



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



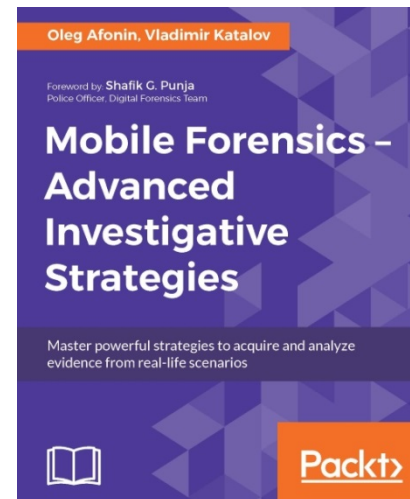
Доступ к зашифрованным данным

- **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



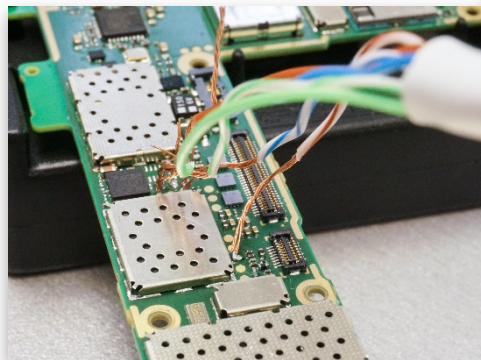
Timeline

- **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 резервными 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



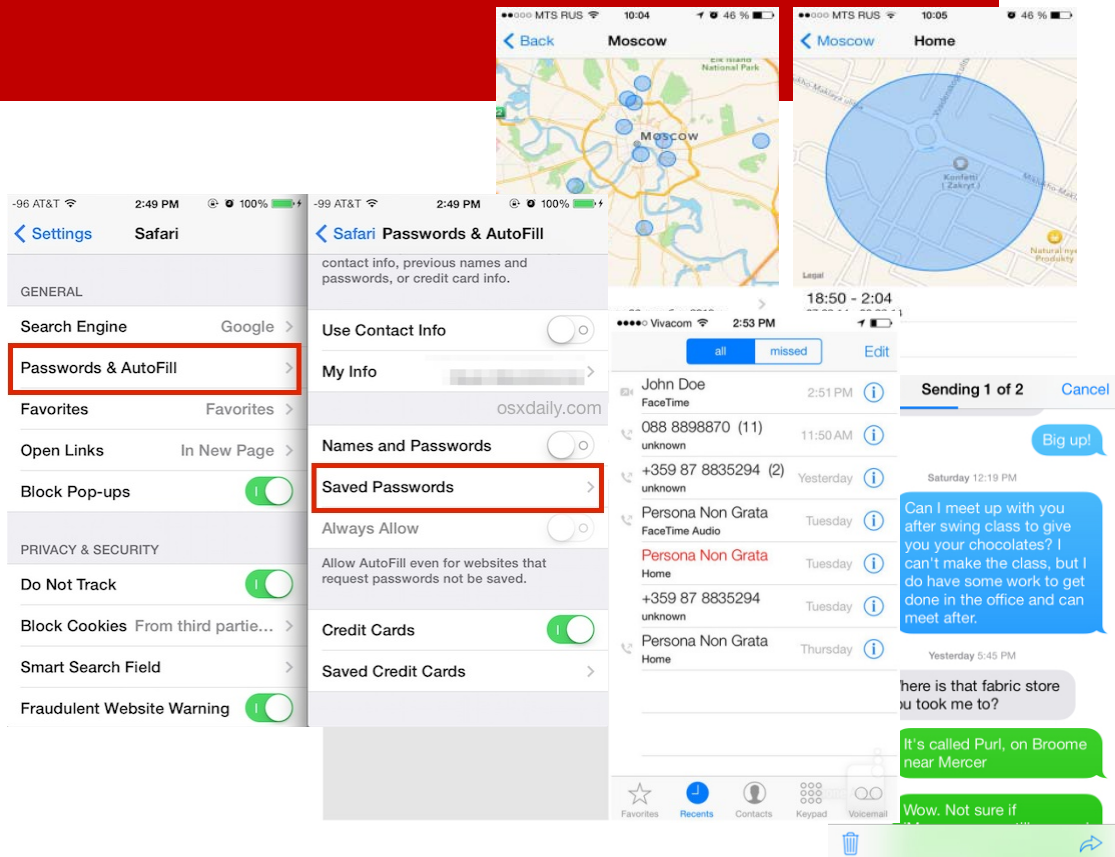
Облако Apple (iCloud)

- 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)

Проблемы:

- 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)



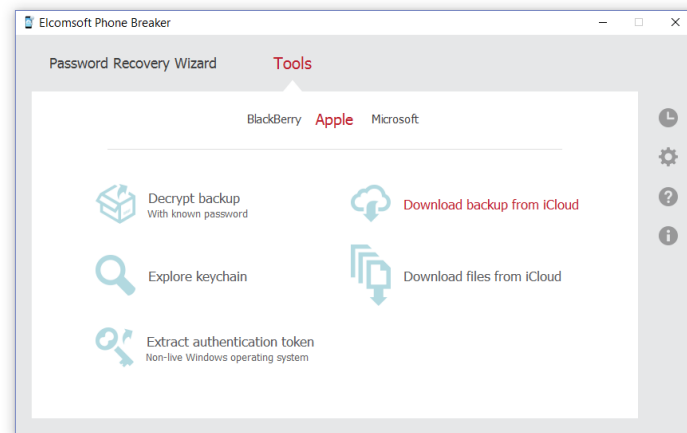
Доступ к данным – это нетривиальная задача

- 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

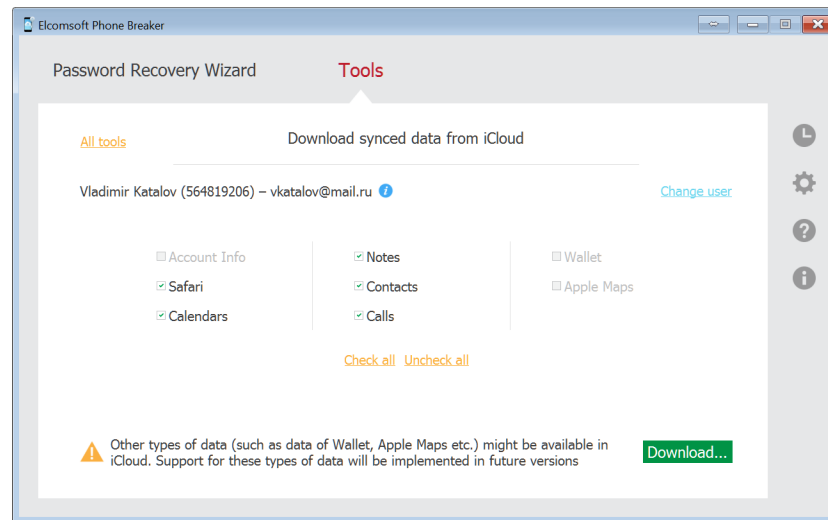
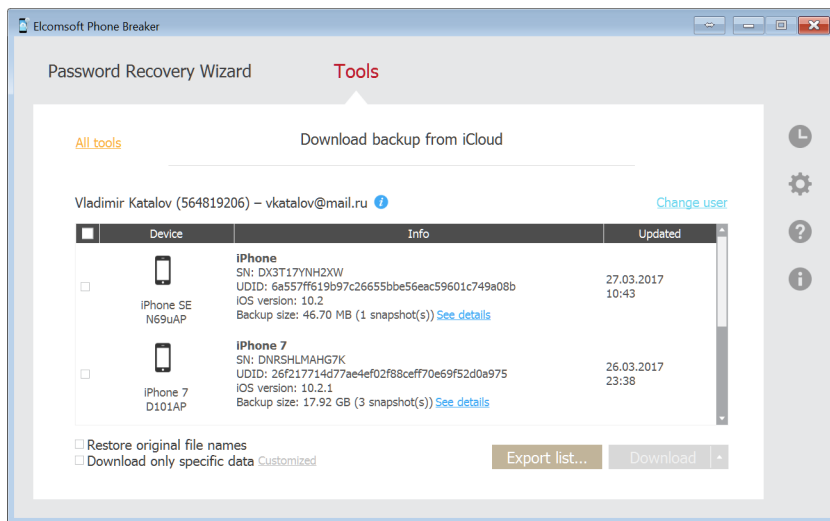


Доступ к Apple iCloud

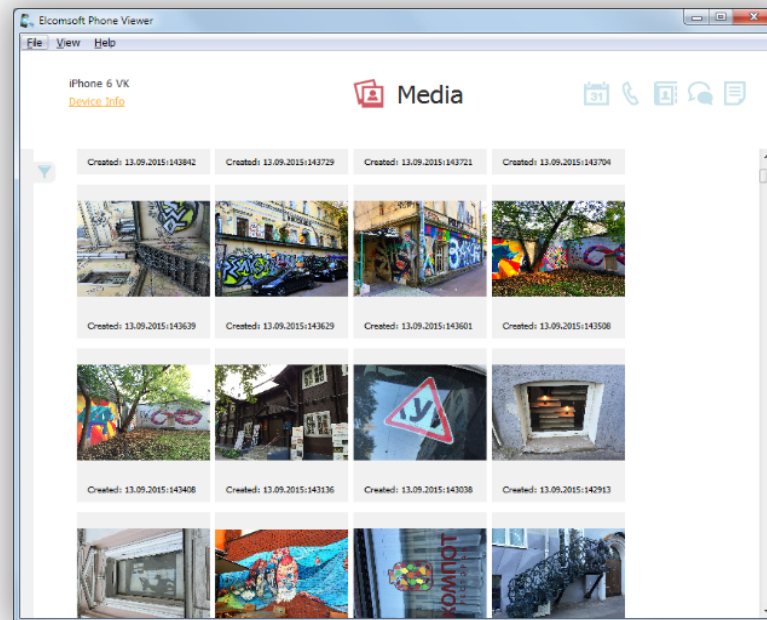
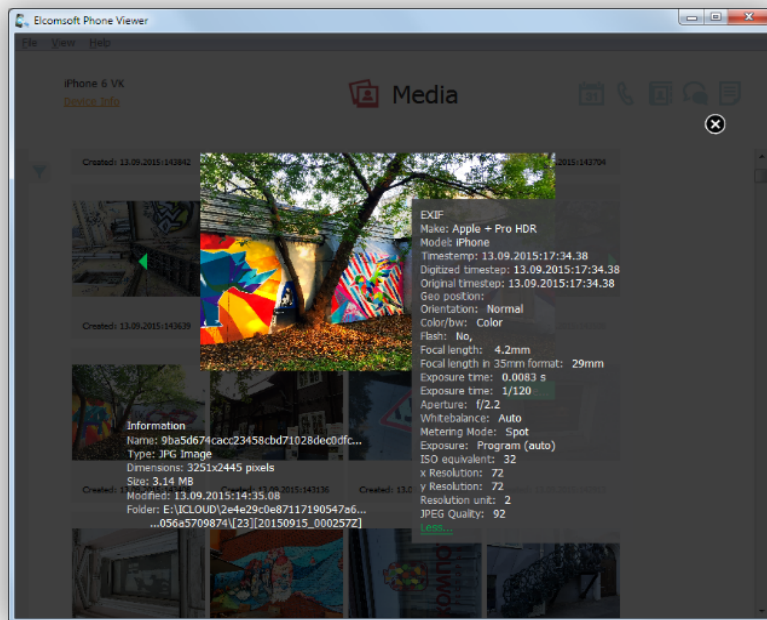
- Возможен выборочный доступ к данным:
 - сообщения
 - журнал звонков
 - адресная книга,
 - заметки
 - календари
 - фото/видео
 - документы
 - данные приложений
 - интернет-активность (история посещений и поиска)
- *По фото можно восстановить данные геолокации*
- *Часто можно получить доступ к облачной «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

Recent security events
Review security events from the past 28 days.

- Changed password
August 15, 12:34 PM
- New iPhone signed in (iPhone 6 VK)
August 4, 9:47 PM

[REVIEW EVENTS](#)

- Приложения

- Dropbox
- Auth
- Chrome
- Remote desktop
- Many more

Recently used devices
Check when and where specific devices have accessed your account.

- Mac
CURRENT DEVICE
- Windows
8 minutes ago
- iPhone 6 VK
39 minutes ago

(+6 more) → + 6 more

[REVIEW DEVICES](#)

Apps connected to your account
Make sure you still use these apps and want to keep them connected.

- Google Chrome
- Chrome Remote Desktop
- Auth
- Dropbox

(+23 more) → + 23 more

[MANAGE APPS](#)

Saved passwords
Manage your passwords from Chrome and Android that are saved with Google Smart Lock.

- 192.168.0.1
- acdsee.com
- adobe.com
- aeroflot.ru

(+76 more) → + 76 more

[MANAGE PASSWORDS](#)

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

Your account, your data.
Download a copy.

Create an archive with your data from Google products.
[Manage archives](#)

Select data to include

Choose the Google products to include in your archive and configure the settings for each product. This archive will only be accessible to you. [Learn more](#)

Product	Details	Select none
+1s		<input checked="" type="checkbox"/>
Blogger	All blogs	<input checked="" type="checkbox"/>
Bookmarks		<input checked="" type="checkbox"/>
Calendar	All calendars	<input checked="" type="checkbox"/>
Contacts	vCard format	<input checked="" type="checkbox"/>
Drive	All files PDF and 3 other formats	<input checked="" type="checkbox"/>
Google Photos	All photo albums	<input checked="" type="checkbox"/>
Google Play Books	All books HTML format	<input checked="" type="checkbox"/>
Google+ Circles	vCard format	<input checked="" type="checkbox"/>
Google+ Pages	All pages HTML format	<input checked="" type="checkbox"/>

Google+ Stream HTML format

Groups

Hangouts

Keep

Location History JSON format

Mail All mail

Maps (your places)

My Maps

Profile

Tasks

Voice

Wallet

YouTube All data types
OPML (RSS) format

[Next](#)

Customize download format



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

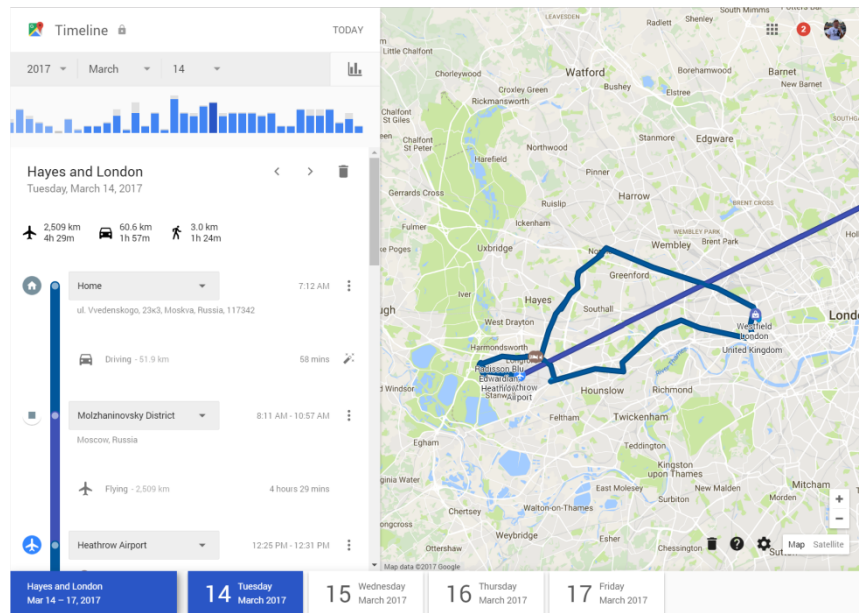
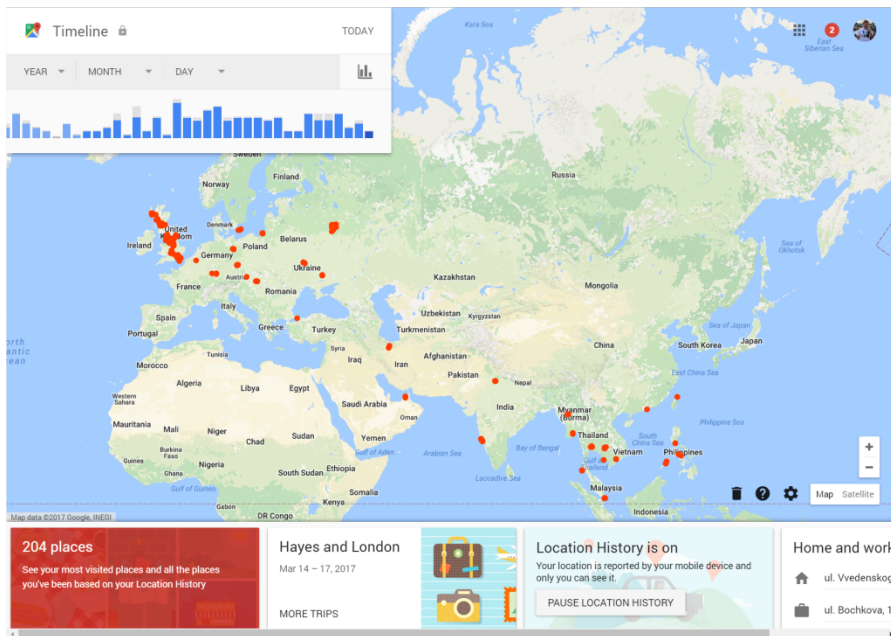
Chrome Sync

Chrome Sync can save your bookmarks, history, passwords, and other settings securely to your Google Account and allow you to access them from Chrome on any device.

The counts below represent all stored items, including those not visible in Chrome.

Apps	Extensions	Settings
7	7	131
Autofill	Omnibox History	Themes
251	185	1
Bookmarks	Passwords 	Open Tabs
236	141	119

Google Timeline



Что можно получить через Elcomsoft Cloud Explorer



Contacts (1264)



Calendars (610)



Calls (0)



Chrome (2739)



Dashboard (7)



Locations (5653)



Mail (34549)



Media (11217)



Google Keep (3)



History (62)



Wi-Fi (66)



Chats (231)



User Info (1)

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

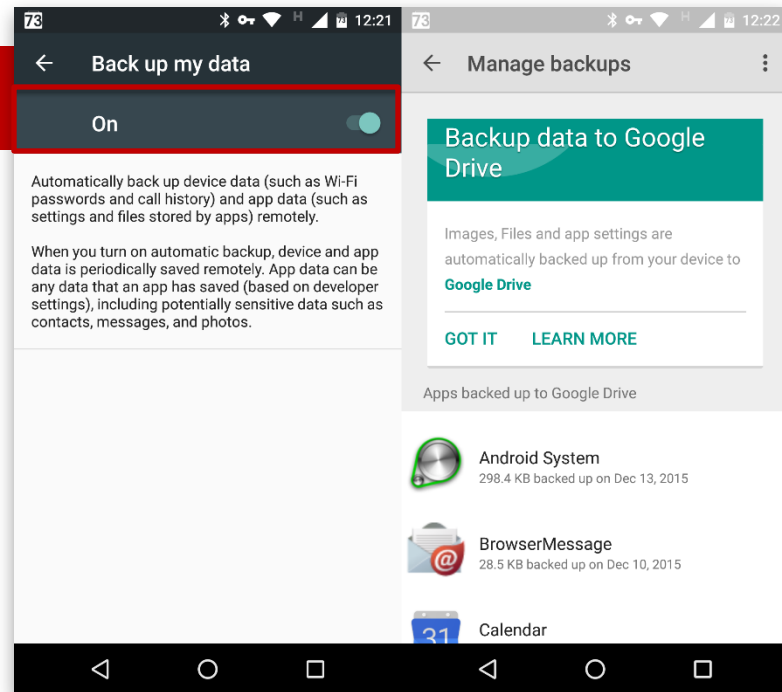
- number of mail threads
- last thread subject
- number of messages in inbox
- last incoming message subject
- number of sent mails
- last sent mail subject

Андроид

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

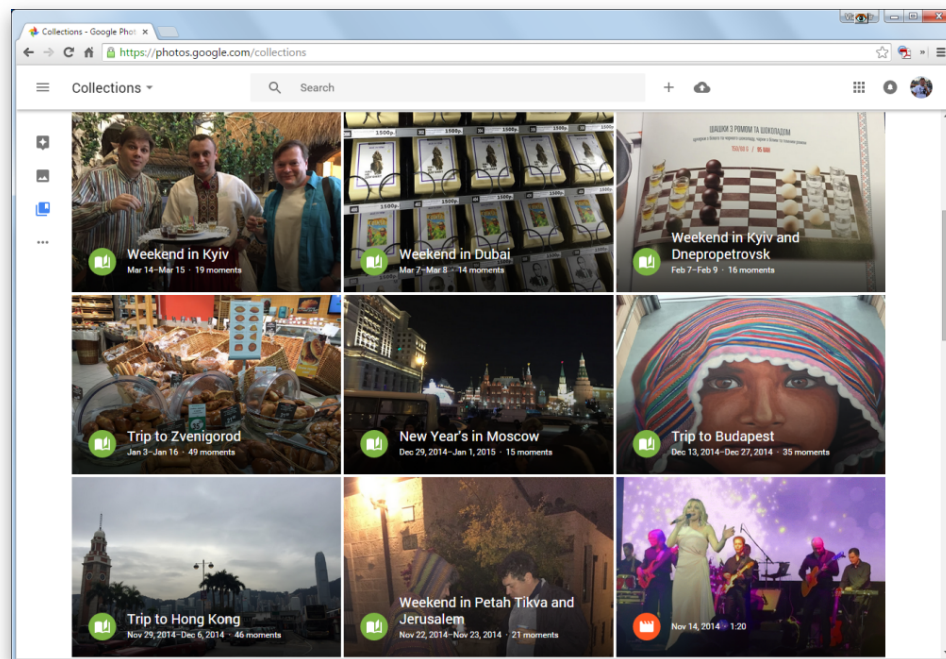
Резервные копии Android

- 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



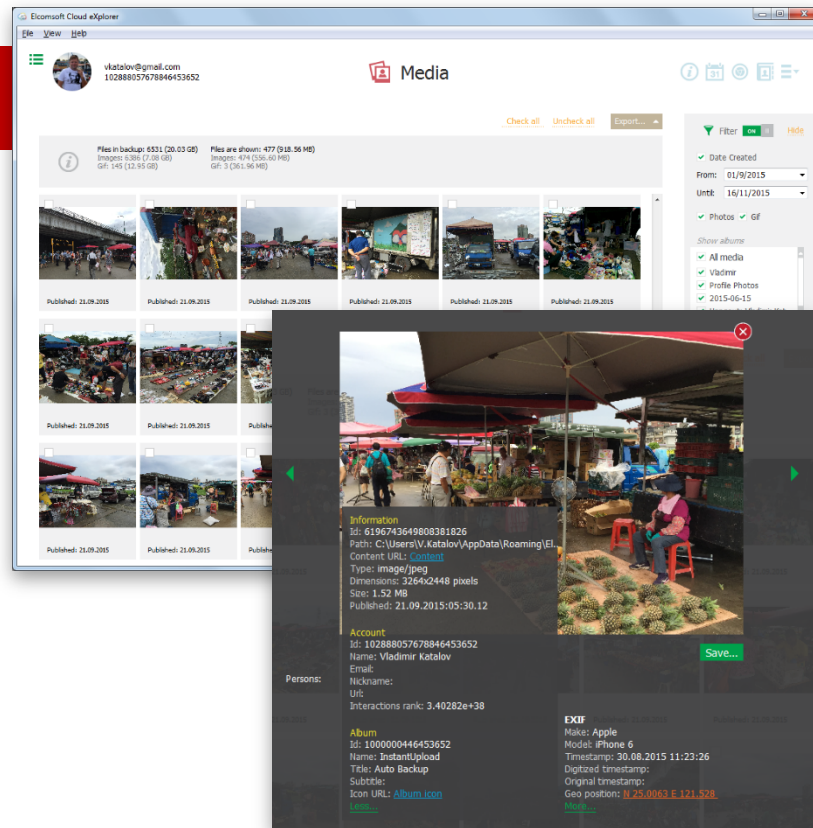
Google Photos

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



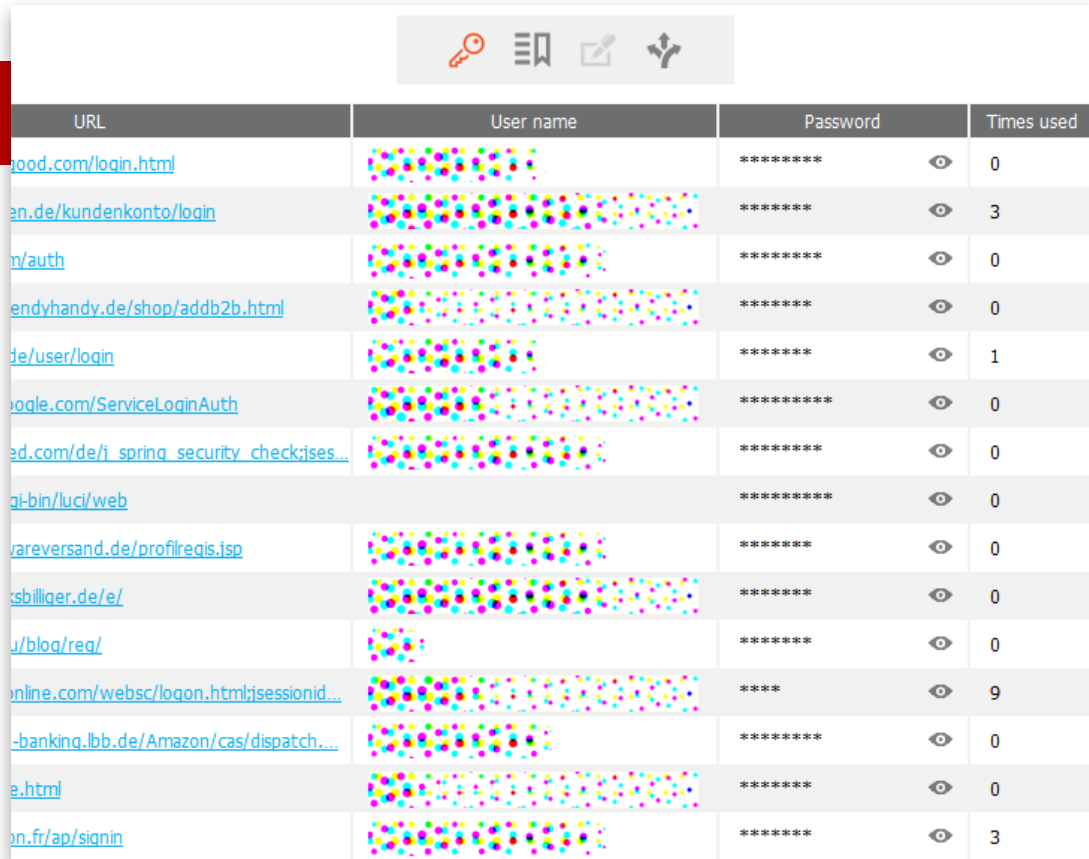
Медиа

- 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

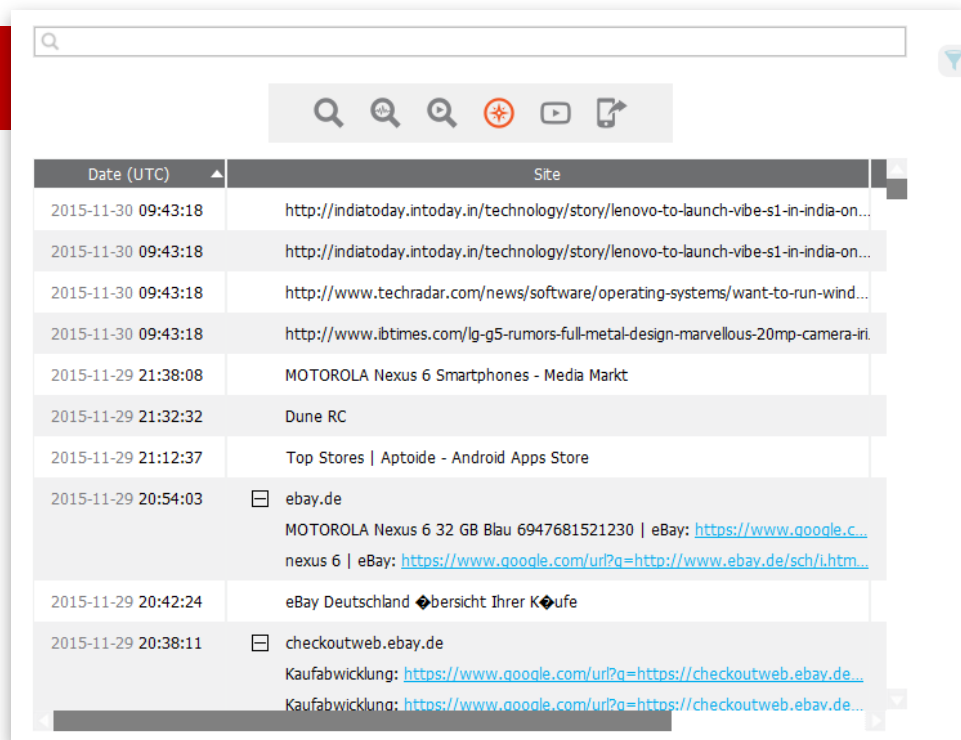
- Данные из Google Chrome
- Пароли синхронизованы между устройствами
- Не только Android
- **Screenshot:** мы маскировали реальные имена пользователей и пароли :)
- Также: закладки, переходы страниц



URL	User name	Password	Times used
ood.com/login.html	[masked]	*****	0
en.de/kundenkonto/login	[masked]	*****	3
n/auth	[masked]	*****	0
endyhandy.de/shop/addb2b.html	[masked]	*****	0
de/user/login	[masked]	*****	1
oogle.com/ServiceLoginAuth	[masked]	*****	0
ed.com/de/i_spring_security_check;jses...	[masked]	*****	0
qi-bin/luci/web	[masked]	*****	0
rareversand.de/profilreqis.jsp	[masked]	*****	0
sbillaer.de/e/	[masked]	*****	0
u/blog/req/	[masked]	*****	0
nline.com/websec/loqon.html;jsessionid...	[masked]	****	9
-banking.lbb.de/Amazon/cas/dispatch...	[masked]	*****	0
e.html	[masked]	*****	0
n.fr/ap/signin	[masked]	*****	3

История поиска

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



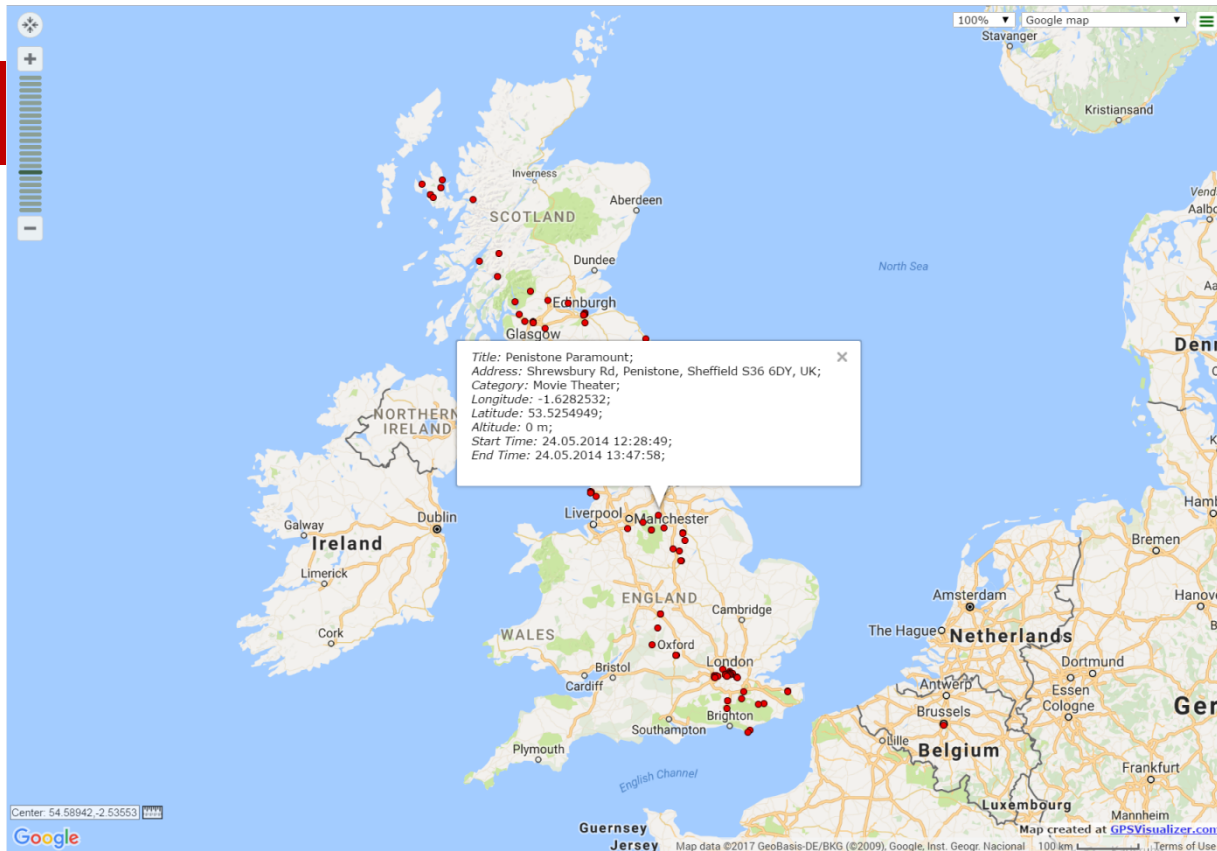
Местоположения: Google Timeline vs. Elcomsoft Cloud Explorer

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

The screenshot displays the Elcomsoft Cloud Explorer interface. On the left, a Google Map shows a geographical area covering parts of Europe and Africa, with red lines indicating movement paths. On the right, the Elcomsoft Cloud Explorer window is open, showing a list of location history entries. The window title is 'Elcomsoft Cloud Explorer' and the user is identified as 'vikatlov@gmail.com' with ID '102888057678846453652'. The interface includes a 'LocationHistory' header, a 'Filter' section, and a table of location data.

Date (UTC +3)	Location
11.12.2015 03:27:32	37.6243954 55.8109671
11.12.2015 03:21:44	37.6243859 55.8109632
11.12.2015 03:17:31	37.6243895 55.8109660
10.12.2015 21:31:21	37.6243922 55.8109645
10.12.2015 21:26:20	37.6243922 55.8109645
10.12.2015 21:22:29	37.6307393 55.8095156
10.12.2015 21:21:17	37.6307392 55.8095126
10.12.2015 21:21:17	37.6243880 55.8109572
10.12.2015 17:32:31	37.6243823 55.8109489
10.12.2015 17:27:29	37.6307393 55.8095156
10.12.2015 17:26:22	37.6307393 55.8095156
10.12.2015 17:22:27	37.6243882 55.8109562
10.12.2015 15:31:15	37.6307393 55.8095156

Местоположения



Экспертиза в мобильных устройствах

Elcomsoft Cloud eXplorer

vkatalov@gmail.com
1028805767844453652

Locations

Places

Locations: 1765
Most recent: 29.03.2017 08:20:04 [55.8285578 37.6213358](#)
Oldest: 14.12.2010 16:27:23 [55.6379560 37.5377720](#)

Start Date	End Date	Title	Category	Address	Coordinates
29.03.2017 08:20:04 (UTC +3)	29.03.2017 14:44:57 (UTC +3)	Ostankinsky District	Other	Moscow, Russia	55.8285578 37.6213358
28.03.2017 20:55:21 (UTC +3)	29.03.2017 07:09:39 (UTC +3)	ul. Vvedenskogo, 23к3	Other	ul. Vvedenskogo, 23...	55.6379560 37.5377720
28.03.2017 14:50:05 (UTC +3)	28.03.2017 19:50:46 (UTC +3)	ul. Bochkova, 11Ac15A	Other	ul. Bochkova, 11Ac1...	55.8109390 37.6248620
28.03.2017 14:22:26 (UTC +3)	28.03.2017 14:30:05 (UTC +3)	Sokolniki District	Other	Moscow, Russia	55.8046147 37.6790236
28.03.2017 10:56:19 (UTC +3)	28.03.2017 14:10:16 (UTC +3)	Konfiders Grupp OOO	Business Managem...	Spartakovskaya pl., ...	55.7762005 37.6781971
27.03.2017 18:43:24 (UTC +3)	28.03.2017 07:10:57 (UTC +3)	ul. Vvedenskogo, 23к3	Other	ul. Vvedenskogo, 23...	55.6379560 37.5377720
27.03.2017 08:17:17 (UTC +3)	27.03.2017 17:09:49 (UTC +3)	ul. Bochkova, 11Ac15A	Other	ul. Bochkova, 11Ac1...	55.8109390 37.6248620
27.03.2017 06:15:28 (UTC +3)	27.03.2017 07:10:16 (UTC +3)	ul. Vvedenskogo, 23к3	Other	ul. Vvedenskogo, 23...	55.6379560 37.5377720
26.03.2017 16:52:59 (UTC +3)	26.03.2017 20:43:18 (UTC +3)	ul. Vvedenskogo, 23к3	Other	ul. Vvedenskogo, 23...	55.6379560 37.5377720
26.03.2017 14:42:23 (UTC +3)	26.03.2017 16:12:01 (UTC +3)	Mari Vanna	Restaurant	Spiridonovskiy per...	55.7626212 37.5955394
26.03.2017 14:03:22 (UTC +3)	26.03.2017 14:10:20 (UTC +3)	Presnensky District	Other	Moscow, Russia	55.7590910 37.5517103
26.03.2017 09:40:41 (UTC +3)	26.03.2017 13:40:16 (UTC +3)	Zamoskvorechye Dist...	Other	Moscow, Russia	55.7334646 37.6323395
26.03.2017 07:30:04 (UTC +3)	26.03.2017 09:19:01 (UTC +3)	ul. Vvedenskogo, 23к3	Other	ul. Vvedenskogo, 23...	55.6379560 37.5377720
26.03.2017 06:51:15 (UTC +3)	26.03.2017 07:11:35 (UTC +3)	Basmanny District	Other	Moscow, Russia	55.7649460 37.6715834

Locations

Routes

Filter: On Hide

Date Created
From: 14.12.2010
Until: 29.03.2017

Category:

- Other
- Restaurant
- Luxury Hotel
- Tourist Attraction
- Hotel
- State Park
- Concert Hall
- Traffic Police Station
- Airport
- Theater Company
- Theme Park
- Parking Garage
- Gastropub
- Tourist Informatio...
- Move Theater
- Casino
- Nature Preserve
- Pub
- National Forest
- Historical Landmark
- Cell Phone Store
- Book Store
- Subway Station
- Beach Resort
- Car Rental Agency
- Ukrainian
- Hospital
- Steak
- Shopping Mall
- Children Polyclinic
- American
- Computer Store

Finish Point	Show Track	Type	Distance, km
5.8114287 37.625...		Driving	32.095
5.6379560 37.537...		Driving	26.835
5.8109390 37.624...		Driving	5.341
5.7904141 37.657...		Walking	2.265
5.7262005 37.678...		Driving	33.062
5.6379560 37.537...		Driving	24.604
5.8109390 37.624...		Driving	28.442
5.6379560 37.537...		Moving	0
5.6395298 37.538...		Moving	0.18
5.6379560 37.537...		Driving	18.656
5.7626212 37.595...		Walking	0.923
5.7644247 37.680...		Driving	8.588
55.6379560 37.537...		Driving	12.484
55.7582349 37.660...		Driving	29.331
55.6382345 37.537...		On the subway	20.573

Type:

- In transit
- Moving
- Cycling
- Walking
- Flying
- Other
- On the subway
- On a bus
- Driving
- On a tram
- On a train
- Basting
- On a ferry
- Motorcycling
- Snowboarding

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!