# Table of Contents

# I Введение

**Elcomsoft Phone Breaker**

**Elcomsoft Phone Breaker** (**EPB**) предназначен для расшифровки резервных копий iTunes и BlackBerry, скачивания резервных копий и синхронизированных данных из облака iCloud и учётных записей Microsoft Account. В редакции для Windows доступен режим восстановления паролей с аппаратным ускорением, использующим вычислительные ресурсы потребительских видеокарт. Кроме того, в приложении доступен инструмент для расшифровки и просмотра данных из Связки ключей, извлечённых из локальных резервных копий iOS либо скачанных из облака iCloud.

**Примеры использования:**

- Расшифровка локальных резервных копий iOS известным паролем
- Скачивание и расшифровка резервных копий iOS из облака iCloud с использованием данных для входа в учётную запись
- Скачивание синхронизированных данных из облака с использованием данных для входа в учётную запись либо маркера аутентификации
- Расшифровка и просмотр данных Связки ключей, извлечённых из образа файловой системы посредством Elcomsoft iOS Forensic Toolkit либо в резервной копии iOS с известным паролем
- Скачивание Облачной связки ключей из iCloud
- Скачивание из iCloud данных, защищённых сквозным шифрованием (таких, как сообщения SMS/iMessage, данные Здоровья, история браузера и т.п.) при наличии полных данных аутентификации, дополненных кодом блокировки или системным паролем от одного из зарегистрированных в учётной записи устройств
- Расшифровка резервных копий BlackBerry с известным паролем
- Расшифровка резервных копий BlackBerry 10 (до BBOS 10.3.2.2876) с известным паролем от BlackBerry ID
- Скачивание данных из учётных записей Microsoft (контакты, журналы звонков, история браузера и поисковых запросов и т.п.)

**Elcomsoft Phone Viewer**

Elcomsoft Phone Viewer - простой, удобный и компактный инструмент для просмотра информации, извлечённой из устройств под управлением iOS, включая последние версии iPhone и iPad. Продукт поддерживает выходные форматы Elcomsoft Phone Breaker и iOS Forensic Toolkit, а также стандартные форматы резервных копий iTunes. Кроме того, поддерживаются форматы резервных копий BlackBerry 10 и данные, извлечённые из учётных записей Microsoft Account при помощи Elcomsoft Phone Breaker.

Elcomsoft Phone Viewer поддерживает как обычные, так и зашифрованные резервные копии. Для доступа к последним вам понадобится оригинальный пароль.

**Elcomsoft Cloud eXplorer**

**Elcomsoft Cloud eXplorer (ECX)** - инструмент для извлечения и просмотра массивов данных из учётных записей Google. Извлекаются пароли и история посещений браузера, данные местоположения пользователя за весь период существования учётной записи, почтовые сообщения и контакты, заметки Google Keep, закладки, история поисковых запросов, календари и многое другое. Поддерживается аутентификация по паролю и без него при помощи маркеров аутентификации.

Поисковый гигант Google собирает огромное количество информации о зарегистрированных пользователях. Elcomsoft Cloud Explorer позволяет получить доступ к этой информации в программе «одного окна».

**Elcomsoft eXplorer for WhatsApp**

**Elcomsoft eXplorer for WhatsApp** (**EXWA**) - инструмент для извлечения, просмотра и анализа общения пользователей WhatsApp с поддержкой iOS и Android и WhatsApp Business для Android.

**Сценарии использования:**

- Скачивание и расшифровка данных WhatsApp для iOS из резервных копий в iCloud
- Скачивание и расшифровка данных WhatsApp для iOS, которые были синхронизированы в iCloud
- Доступ к контактам, сообщениям, истории звонков и медиа-файлам WhatsApp в резервных копиях iTunes
- Скачивание и расшифровка данных WhatsApp из Google Drive
- Доступ к данным WhatsApp и WhatsApp Business из резервных копий Android
- Доступ к данным WhatsApp и WhatsApp Business непосредственно из устройств под управлением Android

# II Системные требования

**Windows**

- Windows 10, Windows 8.1, Windows 8, Windows 7; Windows Server 2016, Windows Server 2012
- CPU с поддержкой набора инструкций SSE2 (рекомендуется поддержка AES-NI)
- Как минимум 300МБ дискового пространства
- Рекомендуется: одна или несколько видеокарт NVIDIA или AMD либо Tableau TACC1441 (для аппаратного ускорения перебора паролей)

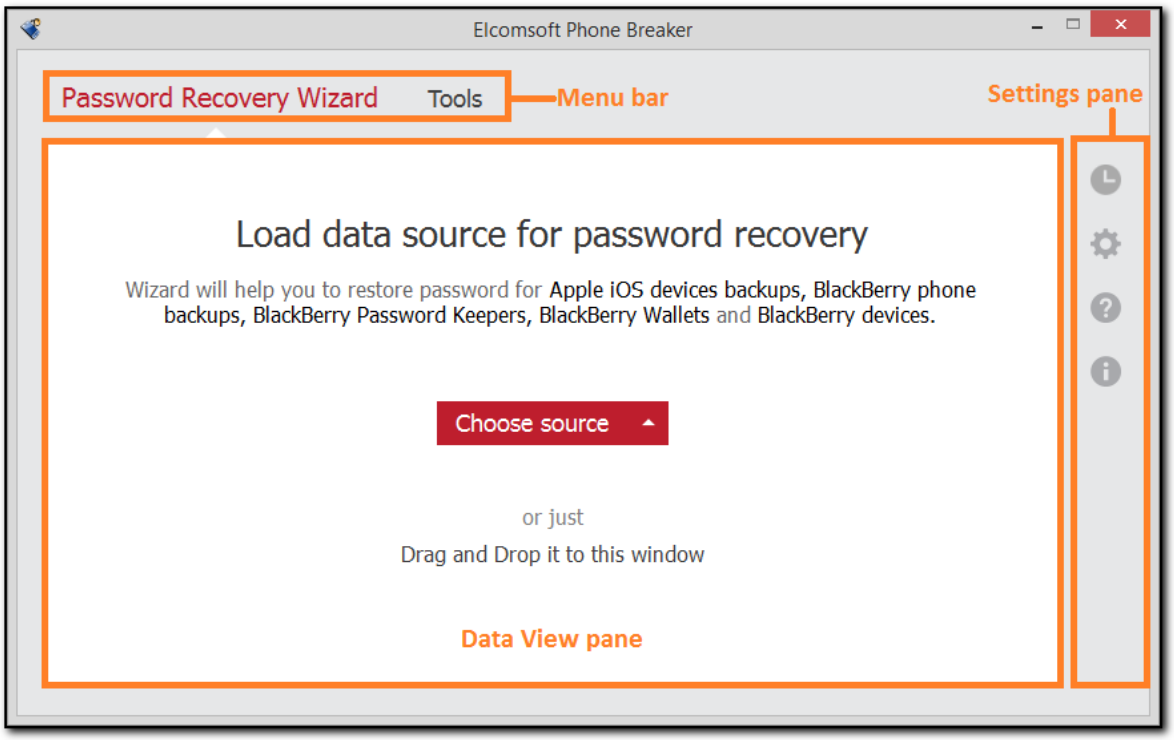
**macOS**

- macOS 10.12 - macOS 10.15
- Как минимум 300МБ дискового пространства

# III Elcomsoft Phone Breaker

## 3.1 Информация о программе

### 3.1.1 Пользовательский интерфейс




Интерфейс Elcomsoft Phone Breaker состоит из следующих элементов:

- **Меню**: доступ к основному функционалу продукта. Доступны следующие вкладки:
  - **Password Recovery Wizard/Мастер Восстановления Паролей**: запуск атаки для восстановления паролей к резервным копиям.
    **Внимание: доступно только в редакции для Windows.**
  - **Tools/Инструменты**: расшифровка резервных копий.
    iOS: скачивание данных из iCloud, расшифровка FileVault, просмотр Связки ключей, извлечение маркеров аутентификации.
    Microsoft Accounts: скачивание данных из учётных записей Microsoft.
- **Область просмотра данных**: здесь отображаются данные в зависимости от выбранной в меню вкладки.
- **Область настроек**: доступны следующие настройки:
  - **Журнал**: список событий, запротоколированных в журнале.

- **Настройки**: настройки аппаратного обеспечения, сетевые настройки, настройки iCloud и настройки шаблонов.
- **Справка**: доступ к документации, проверка обновлений (на macOS), обратная связь, заказ полной версии и ввод регистрационного ключа.
- **О программе**: номер версии и информация о зарегистрированном пользователе.

### 3.1.2 Раздел настроек

В Elcomsoft Phone Breaker доступен ряд настроек.

**Для доступа к настройкам нажмите**  в области настроек.

- **General**

  Общие настройки:

  - **Язык интерфейса / Interface Language**: переключение языка интерфейса между английским и русским. После переключения необходим перезапуск программы.
  - **Заменять системный диалог открытия файла, если установлен Apple iTunes**: если выбрано, диалог открытия файла будет выглядеть так же, как в Apple iTunes (если приложение установлено).
  - **Очищать журнал при запуске:** Удаляет содержимое журнала EPB после перезапуска. Журналы хранятся по следующим путям:
    - **Windows**: *%AppData%\Elcomsoft\Elcomsoft Phone Password Breaker\EPB_<номер_версии_и_ревизии>.log*
    - **macOS**: *~/Users/<username>/Library/Application Support/Elcomsoft Phone Password Breaker/EPB_<номер_версии_и_ревизии>.log.* По умолчанию путь скрыт.

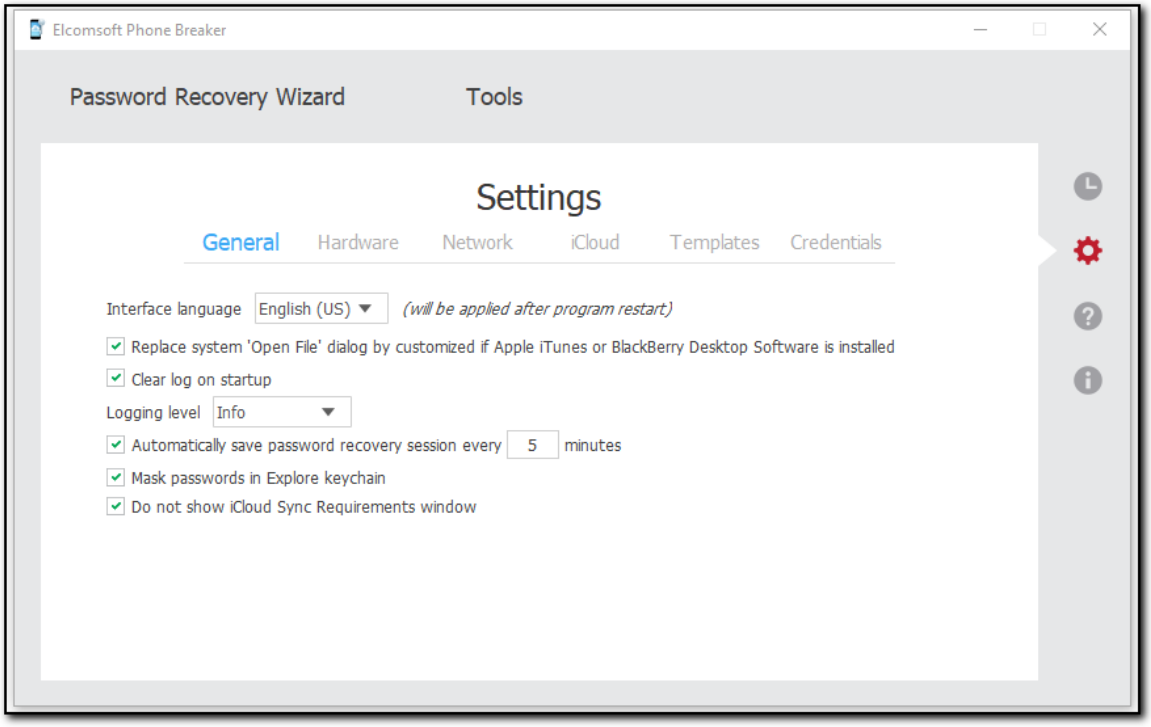
  Вы можете выбрать уровень ведения журнала в списке **Logging Level/Уровень Ведения Журнала**. Он определяет объем информации, которая записывается в журнал: чем выше уровень, тем более подробная информация записывается в файл журнала, но в то же время тем выше нагрузка на систему при ведении журнала. По умолчанию установлен средний уровень.

  Доступны следующие уровни:

| Уровень | Описание |
|---|---|
| None | Журналирование отключено |
| Fatal | Сохраняется только информация о критических ошибках |
| Error | Дополнительно сохраняется информация об ошибках |
| Warning | Дополнительно сохраняются предупреждающие сообщения |
| Info | Дополнительно сохраняются информационные сообщения |
| Debug | Уровень журналирования для отладки |
| Trace | Уровень журналирования для детальной отладки |

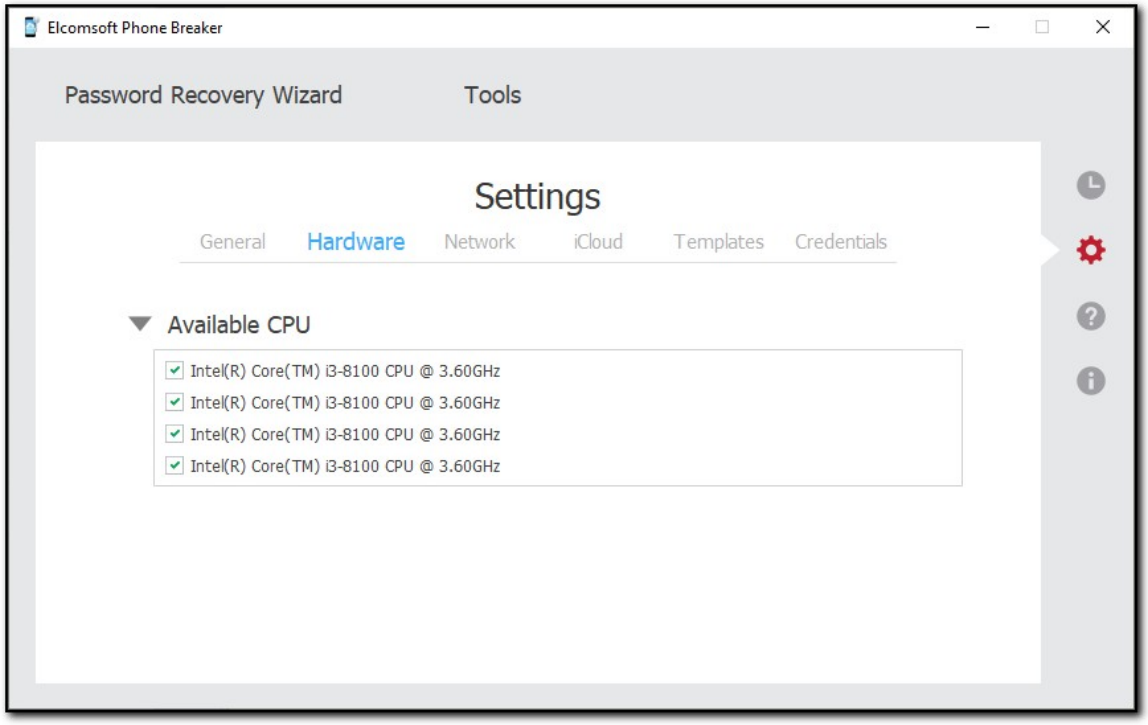
| | |
|---|---|
| Maximum level | Максимальный уровень. Обычно наша служба поддержки рекомендует временно включать именно этот уровень. |

- **Automatically save password recovery session every <> minutes/Автоматически сохранять данные о текущей сессии атаки на пароль каждые <> минут**: автоматическое сохранение данных о текущей сессии атаки на пароль. По умолчанию сохраняются раз в 5 минут.
- **Mask passwords in Explore keychain/Скрыть пароли при просмотре связки ключей**: включает маскировку пароля знаками * при выводе на экран.
- **Do not show iCloud Sync Requirements window/Не показывать окно Требования для iCloud Sync**: пропускает окно iCloud Sync Requirements/Требования для iCloud Sync при скачивании синхронизированных данных из iCloud.




- **Hardware/Оборудование: [доступно только в версии для Windows]**

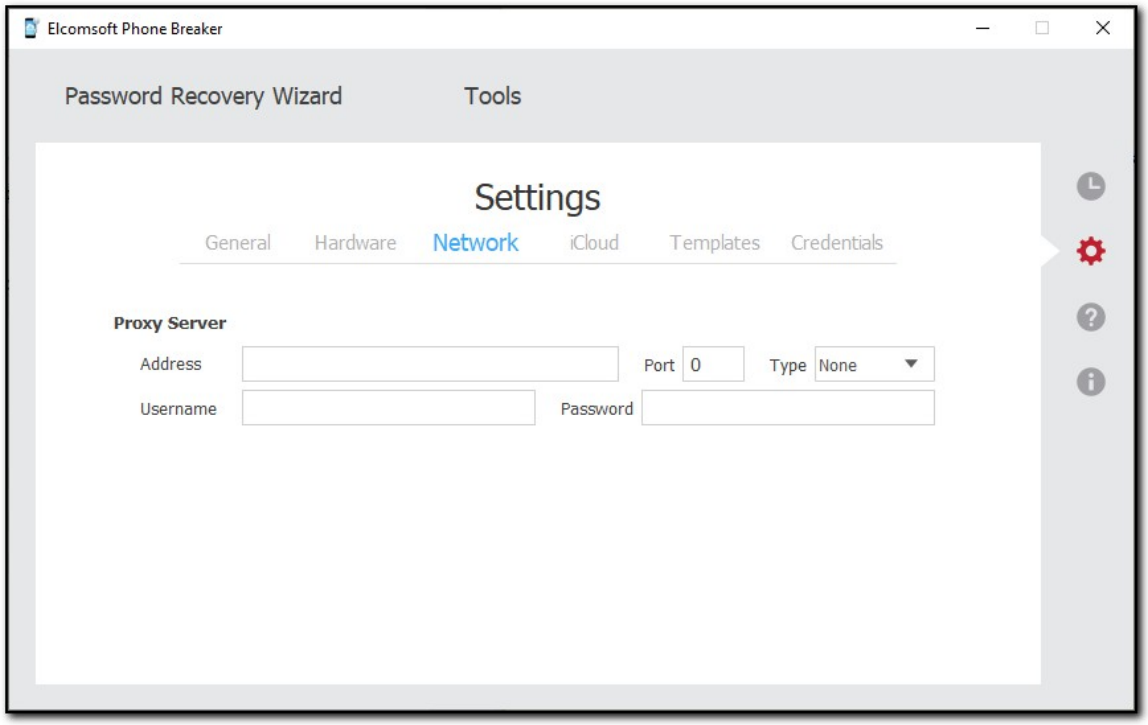
  На странице Hardware/Оборудование указывается количество ядер CPU/ЦПУ и GPU/ГПУ, которые будет использовать EPB.




- **Network/Сетевое Соединение**

  Настройки сетевого соединения и прокси-сервера.

  **Внимание: поддерживаются только сквозные прокси-серверы. Серверы с подменой сертификата не поддерживаются.**




- **iCloud**

  Настройки скачивания из iCloud.

  Для скачивания резервных копий доступны следующие настройки:

  - **Download backups to/Скачать рез. копии в**: выбор папки, в которую будут сохраняться резервные копии.
  - **Restore original file names by default/Восстановить исходные имена файлов по умолчанию**: восстанавливает оригинальные имена файлов (в том виде, в котором файлы хранились на устройстве). Очистка этой опции сохраняет файлы в том виде, в котором они были скачаны (или хранились в резервной копии).

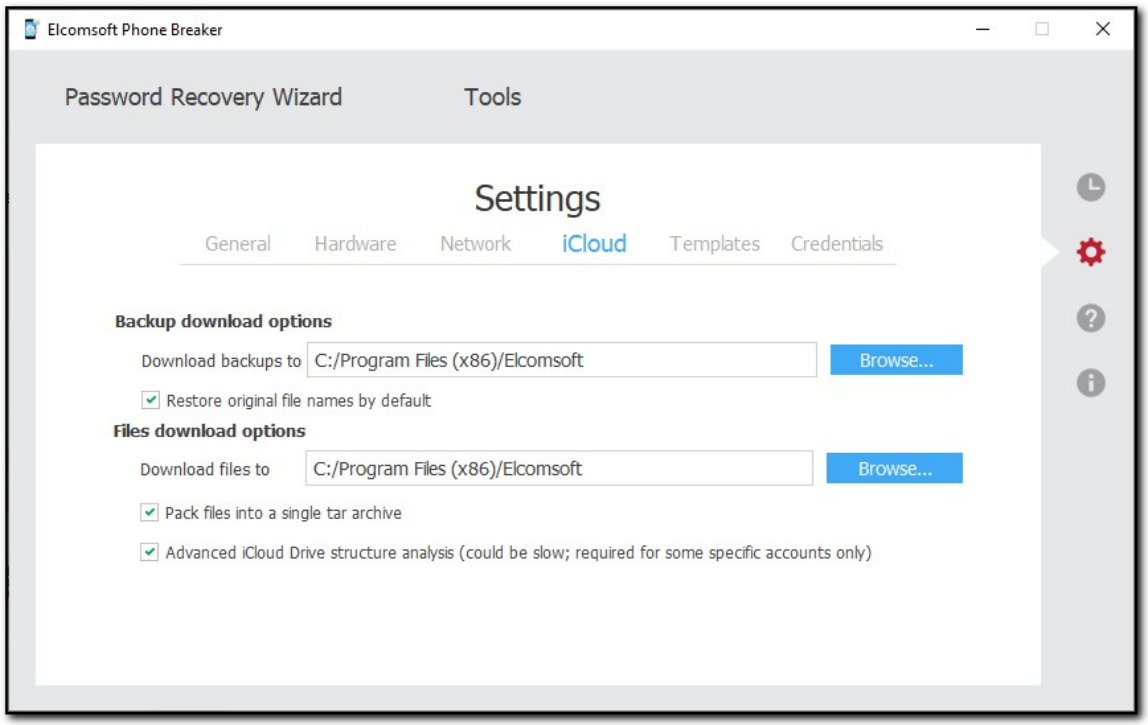
  **Внимание: восстановить оригинальные имена файлов можно в любое время после скачивания данных или расшифровки локальной резервной копии командой Tools/Инструменты -> Apple/Apple -> Decrypt backup/Расшифровать рез. копию, выбрав режим Restore original file names/Восстановить исходные имена файлов.**

  Для скачивания файлов доступны следующие настройки:

  - **Download files to/Скачать файлы в**: путь к папке, в которую будут скачаны файлы.
  - **Pack files into a single tar archive/Сохранить файлы в единый архив формата tar**: файлы будут сохранены в архив.

- **Advanced iCloud Drive structure analysis/Продвинутый анализ данных iCloud Drive**: извлекает дополнительную информацию из данных iCloud Drive и синхронизированных данных iCloud.

**Внимание: если выбрана эта опция, скачивание может занять длительное время. Рекомендуется только в особых случаях.**




- **Templates/Шаблоны [только в версии для Windows]**

  Вкладка **Templates/Шаблоны** позволяет настраивать шаблоны для атаки на пароль. Шаблон включает в себя комбинацию настроек атаки.

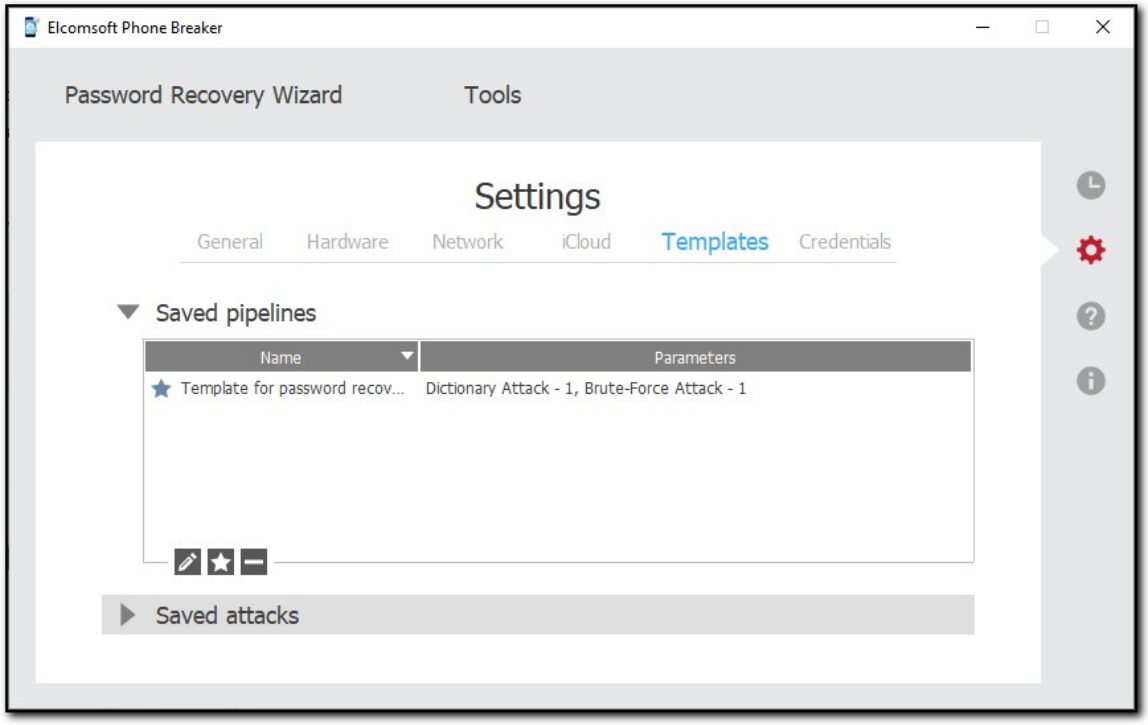
  Процесс восстановления пароля состоит из одной или нескольких атак. Комбинация таких атак носит название очереди атак. Дополнительно см. раздел Password recovery attacks.

  Информацию о шаблонах можно просмотреть в секции **Saved pipelines/Сохранённые конвейеры**. Информацию об отдельных атаках - в секции **Saved attacks/Сохранённые атаки**.

  Чтобы изменить название шаблона, нажмите **Edit/Редактировать** .

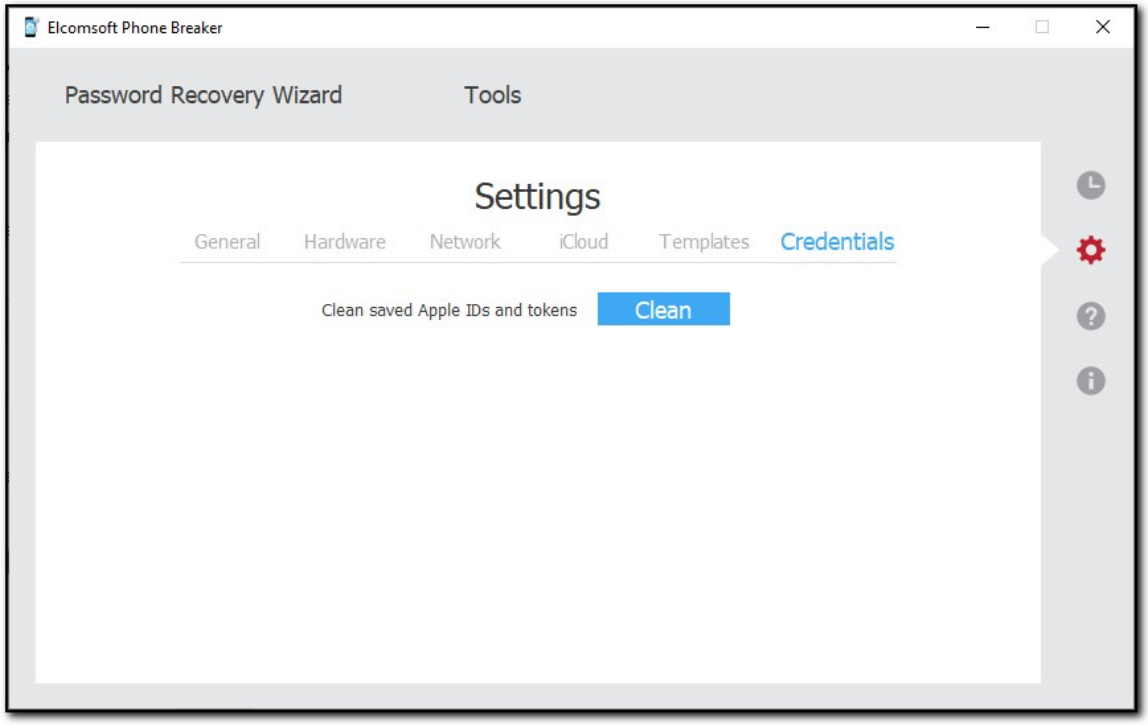
  Установить шаблон по умолчанию можно кнопкой . Шаблон по умолчанию будет использоваться каждый раз, когда вы используете опцию **Password recovery/Восстановление пароля**.

  Удалить шаблон можно кнопкой **Delete/Удалить** .




- **Credentials/Учётные данные**

  Для очистки сохранённых данных для входа в учётную запись (маркеров аутентификации или логина и пароля) нажмите **Clean/Очистить**.




### 3.1.3 [Windows] Аппаратное ускорение

Перебор паролей в версии EPB для Windows можно ускорить с использованием аппаратного ускорения, работающего на современных видеокартах AMD и NVIDIA. Программа может использовать для перебора паролей не только ГП от Nvidia, но и другие графические чипы с универсальной шейдерной архитектурой, выпущенные за последние годы. Это игровые видеокарты Nvidia, начиная с GeForce GTX 4xx и более новые, AMD Radeon серий HD 5000 — HD 8000, AMD R9 и RX и более современные. Поддерживаются также профессиональные видеокарты (все серии Nvidia Quadro и AMD FirePro) и специализированные решения обоих производителей, а также ускорители Tableau. Последние обеспечивают большую скорость перебора в расчете на каждый затраченный ватт энергии.

Для корректного использования аппаратного ускорения убедитесь, что в системе установлены самые свежие версии драйверов NVIDIA или AMD.

Максимальное число поддерживаемых видеоускорителей - 8.

**Внимание: аппаратное ускорение CUDA недоступно при работе через удалённый доступ (RDP).**

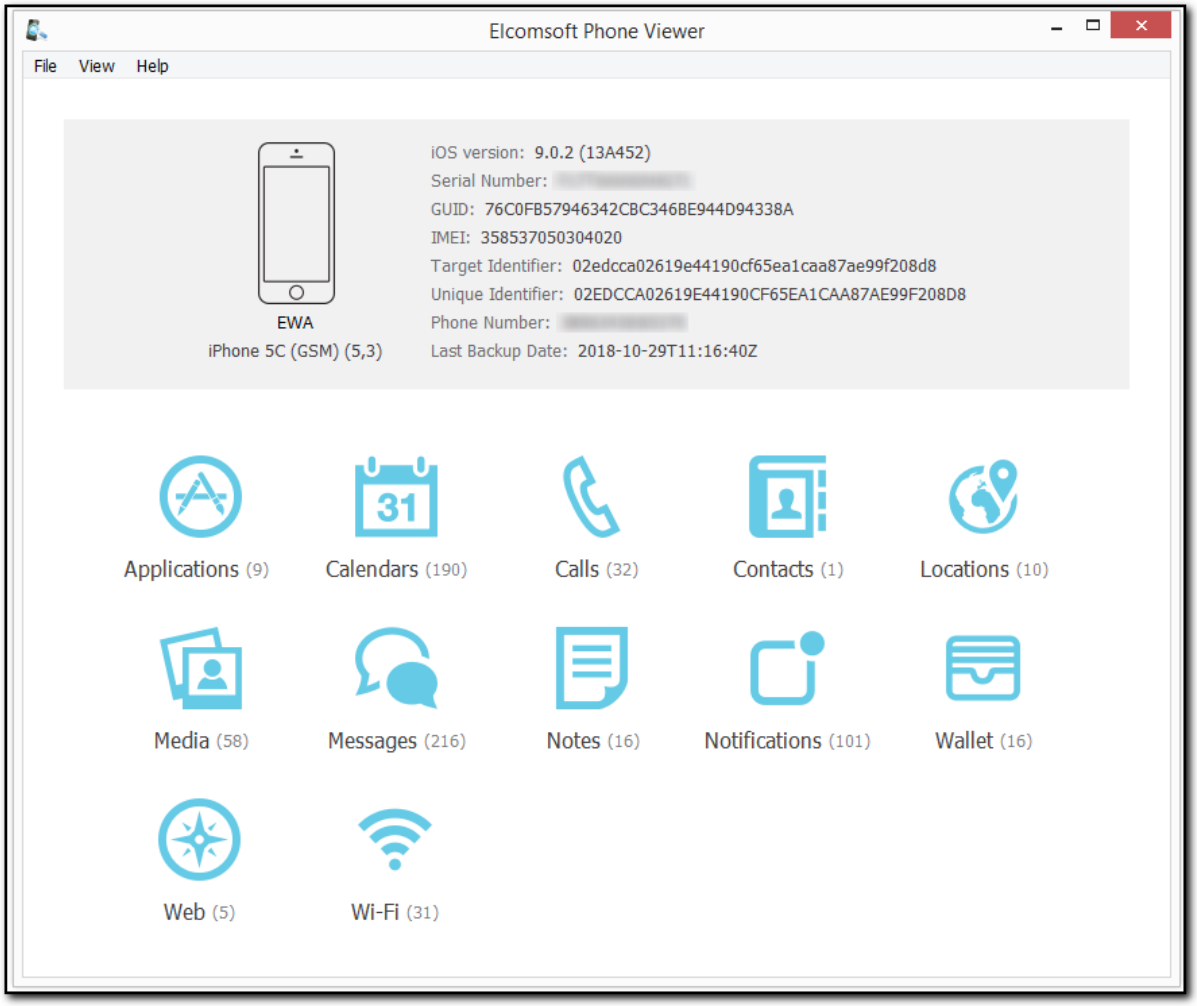
## 3.2 Работа с устройствами Apple

### 3.2.1 Анализ резервных копий iTunes и iCloud

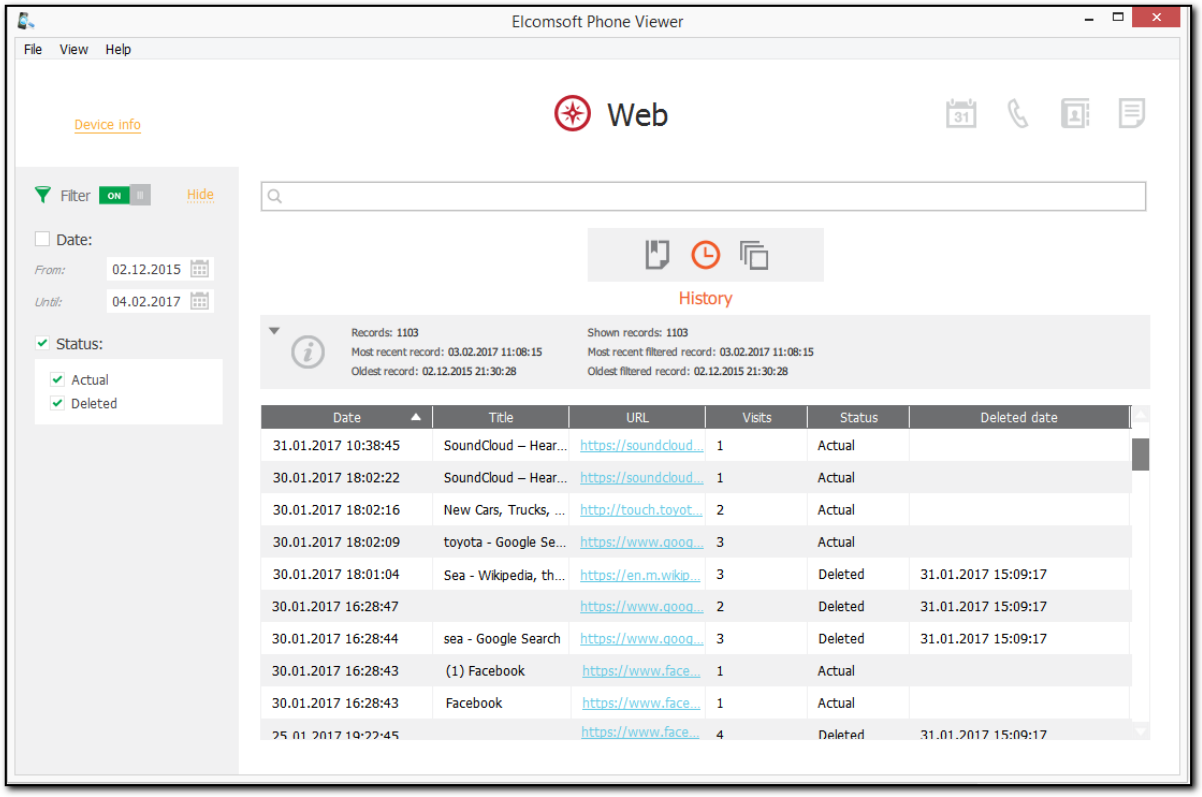
После скачивания из iCloud или расшифровки локальной резервной копии её можно просмотреть посредством утилиты Elcomsoft Phone Viewer. Это единственный инструмент, способный корректно обработать как оригинальные имена файлов, так и восстановленные. Приложение позволяет просматривать многочисленные категории данных, включая:

- Информацию об устройстве: номер модели, серийный номер, номер телефона и т.п.

- Данные из резервной копии: список приложений, календари, контакты, журнал звонков, историю браузера и местоположений, сообщения, заметки и многое другое.




Elcomsoft Phone Viewer обладает рядом возможностей для удобного поиска, анализа и экспорта данных из многочисленных категорий.




Помимо данных, извлечённых из устройств и облачных сервисов Apple, приложение работает с резервными копиями Blackberry 10 и данными из учётных записей Microsoft.

### 3.2.2 Keychain Explorer: анализ Связки ключей

Связка ключей (keychain) содержит как учётные данные пользователей (логины и пароли) для сайтов и приложений, так и разнообразную дополнительную информацию - такую, как маркеры аутентификации, ключи, сертификаты, пароли к точкам доступа Wi-Fi и т.п.

В состав EPB входит удобный инструмент, позволяющий просматривать записи из Связки ключей, полученной из зашифрованной резервной копии или скачанных из облака iCloud.

**Внимание: поддерживаются только резервные копии с паролем, которые были расшифрованы в самом Elcomsoft Phone Breaker. При расшифровке не рекомендуется использовать восстановление оригинальных имён файлов.**

Для доступа к Связке ключей потребуется следующее:

| Тип данных | Требования к извлечению |
|---|---|
| Облачная Связка ключей из iCloud | Данные Apple ID, пароль, код 2FA, код блокировки или пароль от одного из зарегистрированных устройств |
| iTunes (без пароля) | Теоретически доступны с аппаратным ключом, извлекаемым через джейлбрейк |
| iTunes (расшифрован в EPB) | Пароль к резервной копии |
| iTunes (зашифрован) | Пароль к резервной копии |

**EPB** позволяет просматривать данные Облачной связки ключей iCloud Keychain (*iCloud_Keychain.xml* file) и синхронизированных из iCloud данных (*icloud_synced.xml* file).

Также можно просматривать Связку ключей, извлечённую посредством Elcomsoft iOS Forensic Toolkit. Имя файла по умолчанию - *keychaindump.xml*.

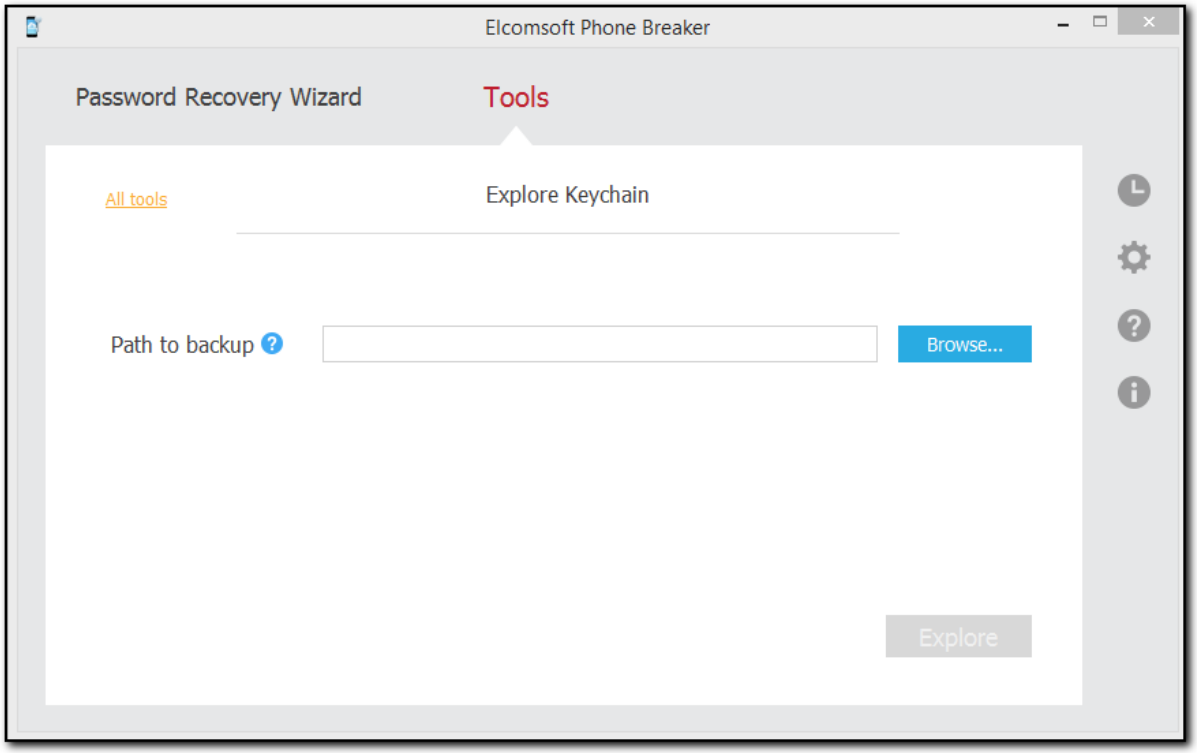
Для анализа Связки ключей:

1. В меню **Tools/Инструменты** выберите вкладку **Apple** и нажмите **Explore keychain/Просмотр связки ключей**.
2. Нажмите **Browse/Обзор** и выберите путь к файлу:

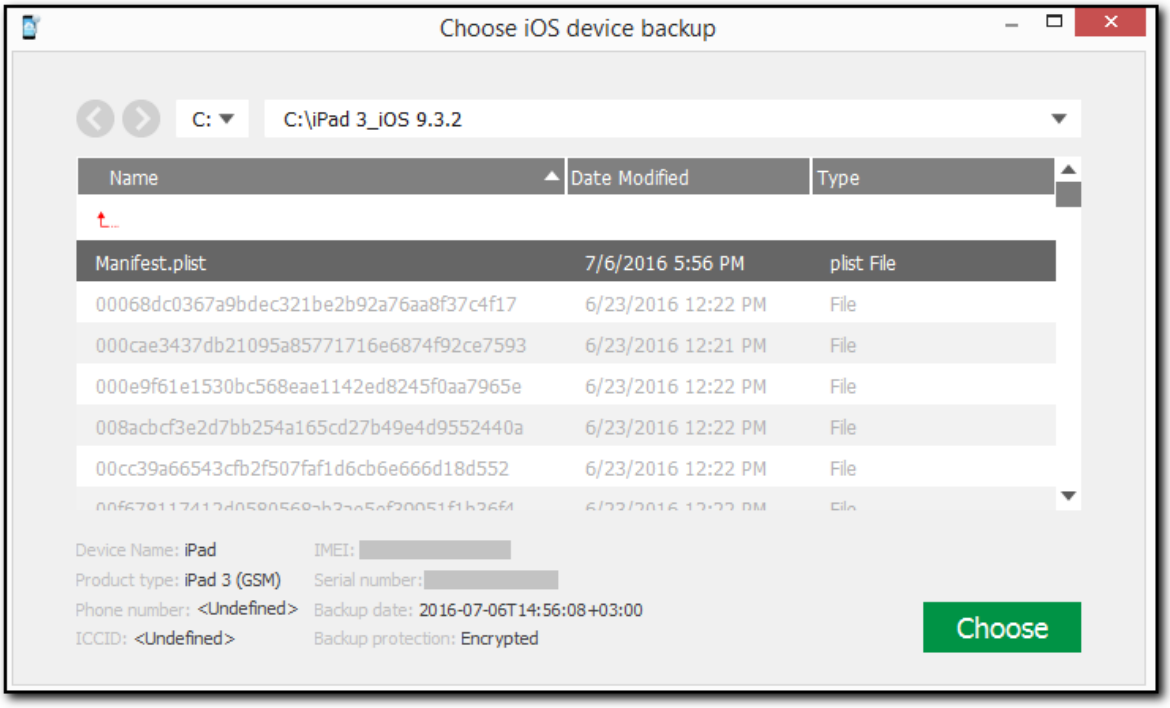
| **Источник данных** | **Имя файла** |
|---|---|
| Резервная копия iTunes | *Manifest.plist* |
| Данные Связки ключей, скачанные при помощи EPB 9.50 и более старых версий | *iCloud_Keychain.xml* |
| Данные Связки ключей, скачанные при помощи EPB 9.60 и более новых версий из синхронизированных данных iCloud | *icloud_synced.xml* |
| Образ данных, извлечённый посредством Elcomsoft iOS Forensic Toolkit | *keychaindump.xml* |

**Внимание: вы можете перетащить нужный файл *Manifest.plist* на окно Explore Keychain/Просмотр связки ключей.**

**Внимание: На macOS 10.14 и более новых версиях, необходимо предоставить EPB полный доступ к диску (Full Disk Access). В противном случае доступ к папке iTunes будет запрещён. Детали в секции Troubleshooting.**

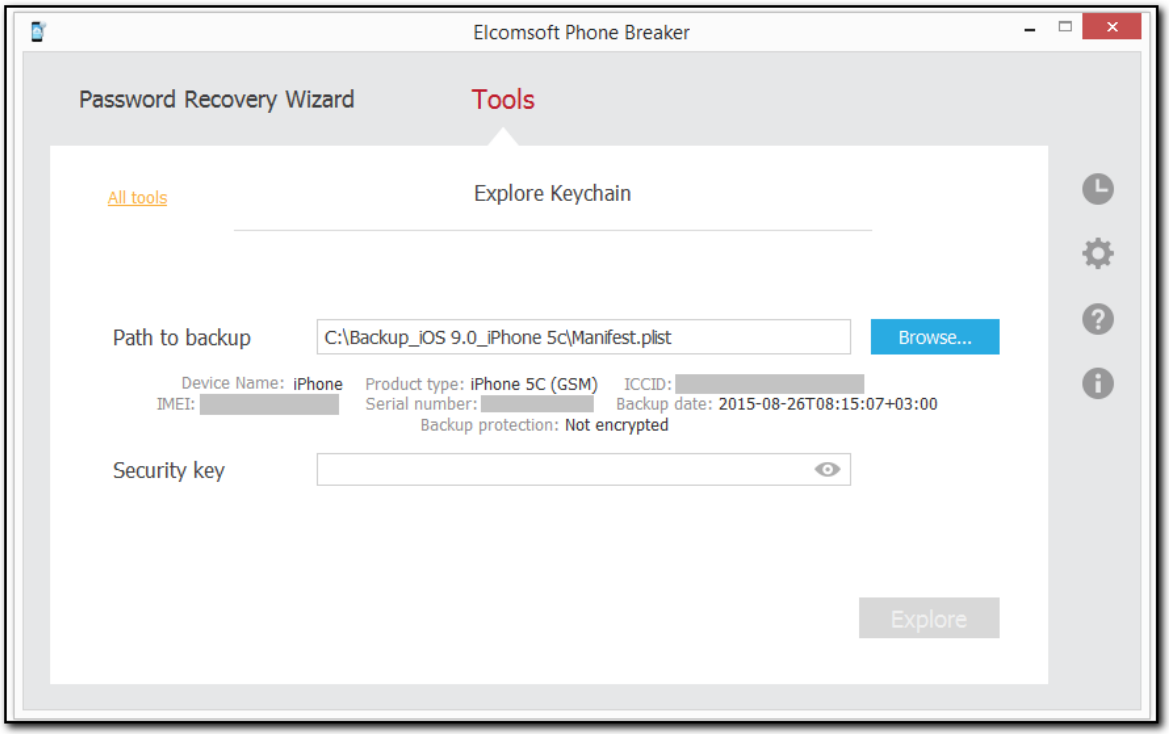



3. Выберите файл и нажмите **Continue/Продолжить**.



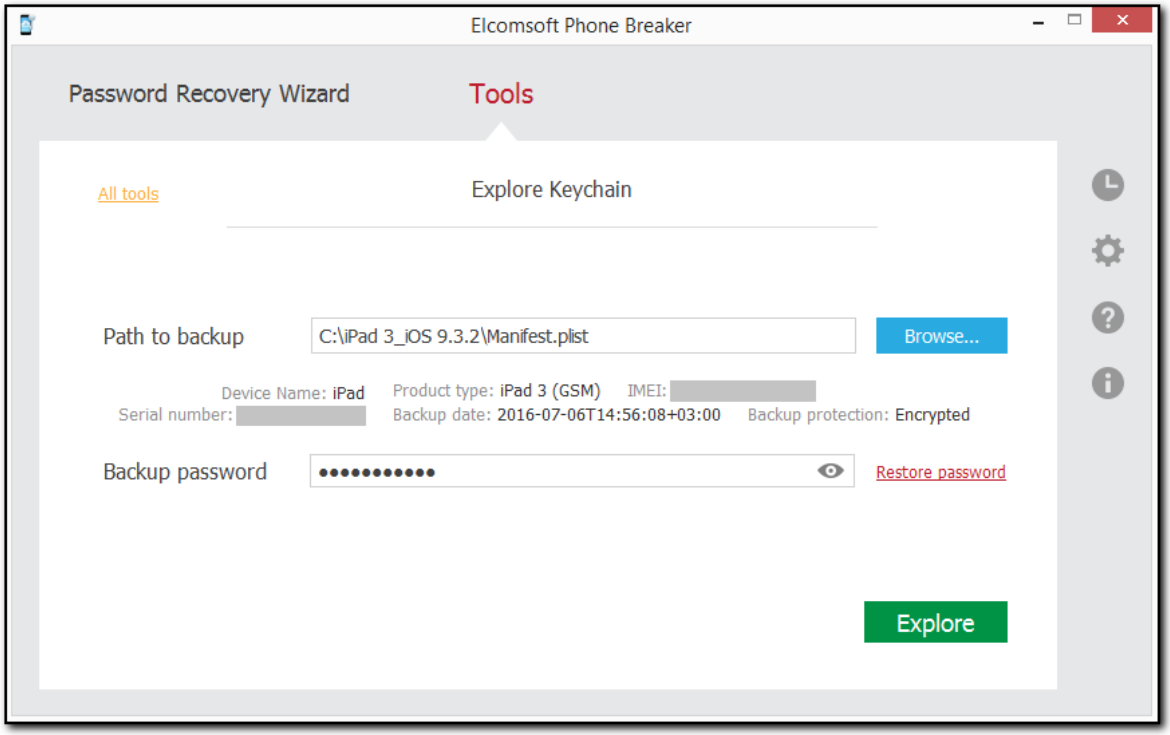

4. В зависимости от того, зашифрована ли резервная копия:

   - **Не зашифрована:** если в вашем распоряжении есть Security key/Код безопасности, извлечённый из устройства, введите его:



- **Зашифрована:** Введите пароль. Для его отображения, нажмите **View/Показать** .

  Если пароль неизвестен, вы можете попытаться его восстановить (восстановление паролей.)




4. Нажмите **Explore/Перейти к просмотру** для просмотра Связки ключей.

5. Записи отображаются по категориям:

| Категория | Общая информация | Информация для категории |
|---|---|---|
| Apple ID | ○ Название: источник данных в Связке ключей<br>○ Дата создания<br>○ Дата последнего изменения | ○ Apple ID (учётная запись)<br>○ Пароль |
| Wi-Fi accounts | | ○ SSID (учётная запись)<br>○ Пароль |
| Mail accounts | | ○ Протокол<br>○ Учётная запись<br>○ Пароль |
| Browser passwords | | ○ Адрес<br>○ Учётная запись<br>○ Пароль |

| | | |
|---|---|---|
| Credit cards | | ○ Название карты<br>○ Имя держателя карты<br>○ Номер карты<br>○ Срок окончания действия |
| DSIDs & Tokens | | ○ Маркер аутентификации<br>○ DSID |
| Other | | Все остальные типы записей |

6. Информация о паролях отображается в древовидной системе:

- **Древовидное отображение**: вид по умолчанию. Можно активировать кликом на icon.

Здесь отображаются все записи, включая те, которые не были расшифрованы.

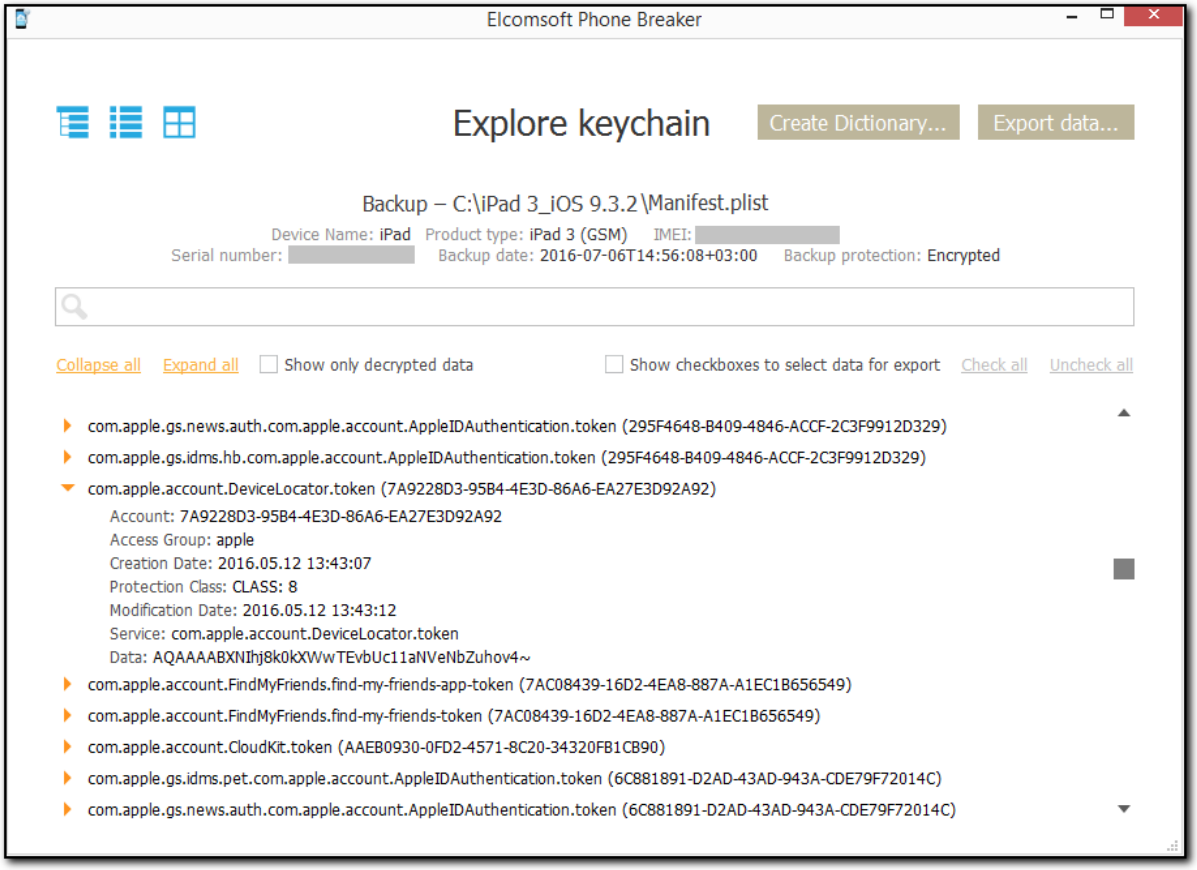
Командой **Show only decrypted data/Показать только расшифров. записи** можно скрыть записи, которые не были расшифрованы. Рекомендуется использовать с целью упрощения анализа.

Кликните по стрелке оранжевого цвета, чтобы раскрыть дополнительную информацию о записи.

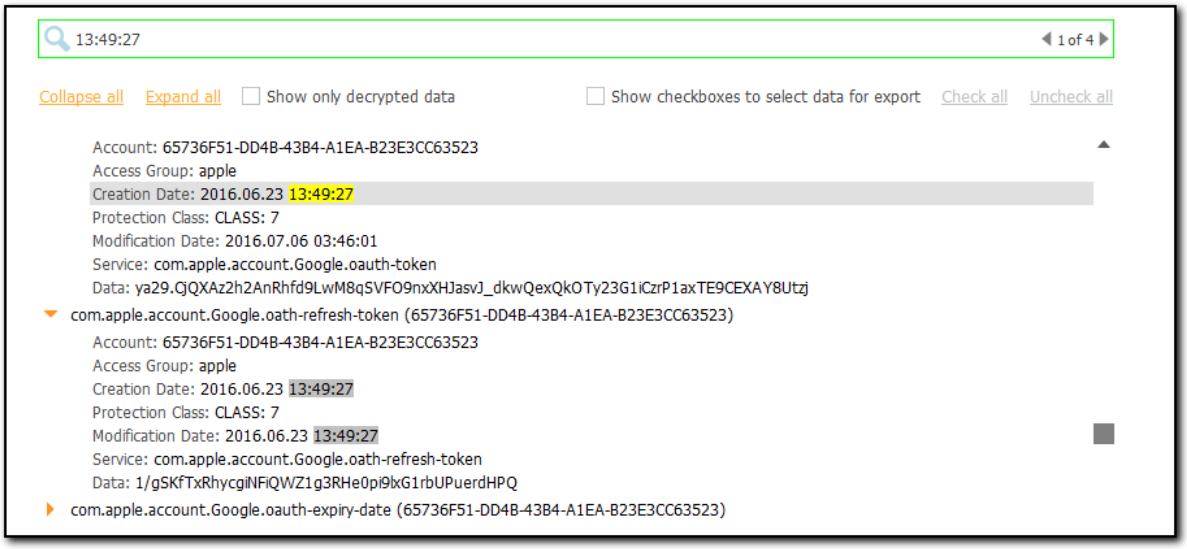
Раскрыть информацию обо всех записях можно командой **Expand all/Развернуть все**.

Свернуть все записи можно командой **Collapse all/Свернуть все.**

Для того, чтобы вместо паролей отображалась маска из символов *, зайдите в настройки EPB Settings и отметьте **Mask passwords in Explore keychain/Скрыть пароли при просмотре связки ключей.**

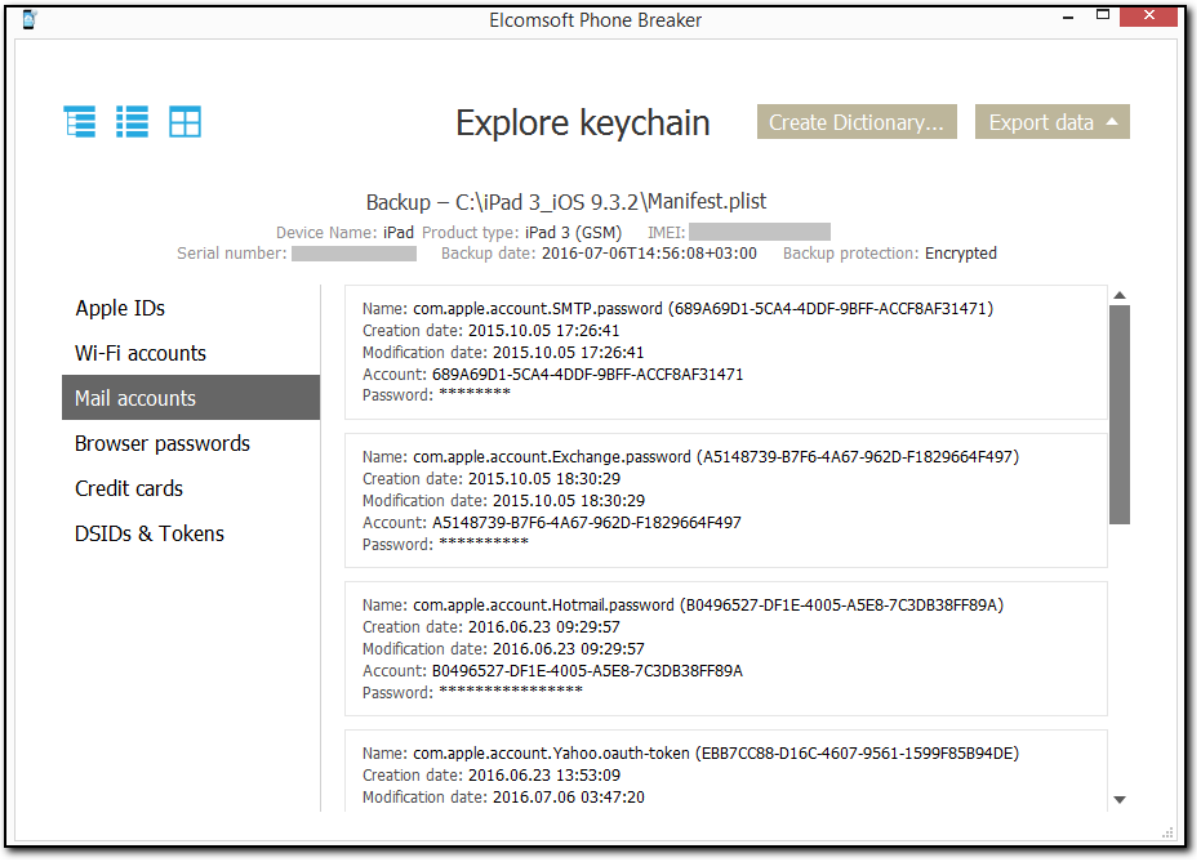



В строке поиска можно вводить поисковые запросы. Если будет найдено больше одной записи, между ними можно переключаться, нажимая на стрелки в окне поиска.



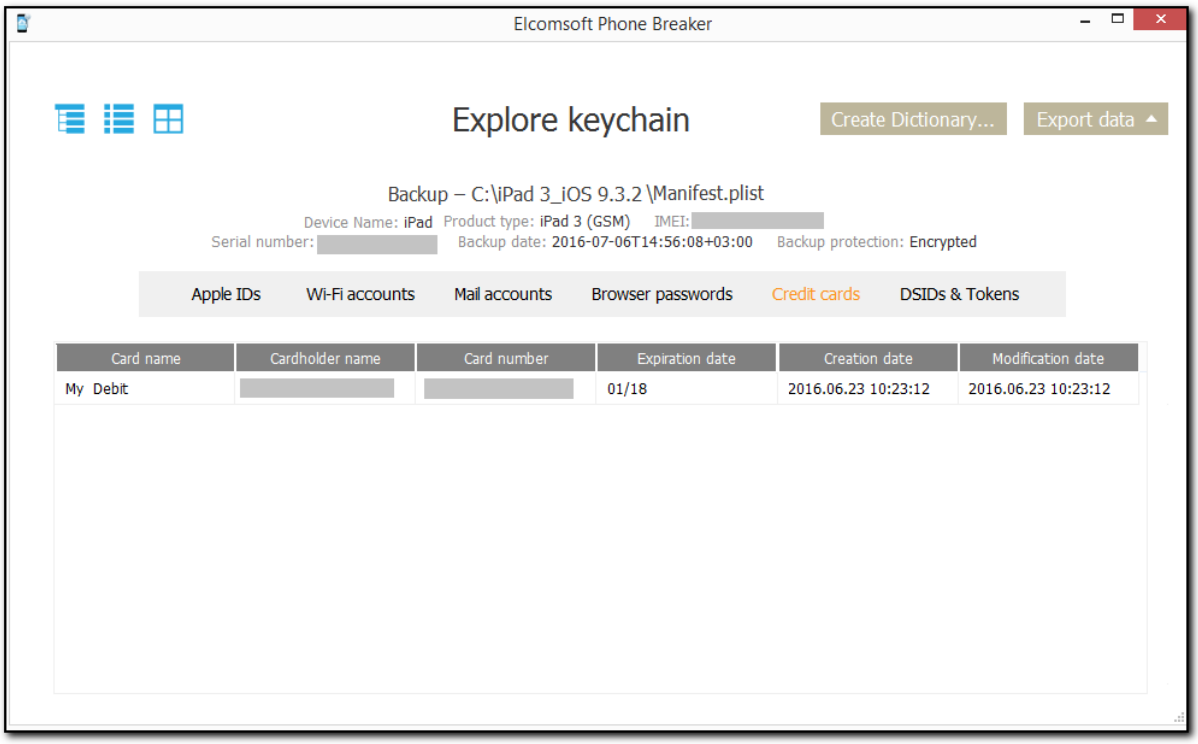

- **Категории:** отображение категорий включается нажатием иконки  .

В этом виде записи выводятся отсортированными по категории.




- **Табличный вид**: активируется иконкой  .

Чтобы отсортировать данные, кликните по заголовке соответствующего столбца.




**Экспорт данных**

Вы можете экспортировать как все данные связки ключей, так и данные из выбранной категории.

**Экспорт данных из окна древовидного просмотра**:

1. Выберите опцию **Show checkboxes to select data for export/Показать опции выбора данных для экспорта.**

2. Отметьте записи, которые хотите экспортировать, либо нажмите **Check All/Выбрать все.**

3. Нажмите **Export Data/Экспортировать** в правом верхнем углу программы и выберите **All/Все** либо **Selected/Выбранные**.

4. Укажите место на диске, куда будут сохранены данные.

5. Нажмите **Save/Сохранить**.

6. Имя файла, в который будут сохранены данные по умолчанию - **keychain_export.xml**.

**Экспорт данных из окна категорий или табличного вида**:

1. Нажмите **Export Data/Экспортировать** в правом верхнем углу программы и выберите **All/Все** либо **Selected/Выбранные**.

2. Укажите место на диске, куда будут сохранены данные.

3.Нажмите **Save/Сохранить**.

4. Имя файла, в который будут сохранены данные по умолчанию - **keychain_export.xml**.

   Имена файлов, в которые сохраняются только отмеченные категории - **keychain_export_<category_name>.xml** либо **keychain_export_<category_name>.csv**.

**Создание словаря**

Из паролей, обнаруженных в Связке ключей, можно создать целевой словарь для атаки на зашифрованные файлы и документы пользователя. Словарь создаётся в текстовом формате.

Чтобы создать словарь, нажмите **Create dictionary/Создать словарь** в верхнем правом углу программы. Укажите путь на диске, куда будет сохранён файл, и нажмите **Save/Сохранить**.

По умолчанию, словарь сохраняется в файле **keychain_passwords.txt.**

## 3.2.3 Резервные копии iTunes

### 3.2.3.1 О резервных копиях iTunes

В приложении Apple iTunes есть возможность создания резервных копий устройств под управлением iOS и iPadOS, включая модели iPhone, iPad и iPod Touch. Содержимое резервных копий может меняться в зависимости от типа и модели устройства, настроек синхронизации iCloud (например, в состав резервной копии могут не попадать фотографии, если пользователь настроил их синхронизацию в облако), а также от версии iOS/iPadOS, под управлением которой оно работает. Актуальную информацию можно получить из статей, опубликованных на сайте Apple:

Сведения о резервных копиях данных iPhone, iPad и iPod touch
Содержимое резервных копий iCloud
Поиск резервных копий iPhone, iPad и iPod touch

Резервные копии могут создаваться как с паролем, так и без него. Если резервная копия создаётся без пароля, то некоторые данные (например, пароли из Связки ключей) будут зашифрованы аппаратным ключом, извлечь который из устройства может быть трудно или невозможно. В резервных копиях с паролем данные будут зашифрованы самим паролем; их можно расшифровать вместе с основной частью резервной копии.

Обратите внимание: резервные копии устройства могут создаваться как приложением Apple iTunes, так и сторонними приложениями - например, Elcomsoft iOS Forensic Toolkit. Их содержимое будет полностью идентичным. Рекомендуем воспользоваться Elcomsoft iOS Forensic Toolkit в силу следующих факторов:

- Дополнительные возможности извлечения: некоторые системные журналы и данные приложений, а также фотографии и медиа-файлы (доступ по отдельному протоколу, независимо от резервных копий и установленного на них пароля)
- Автоматическая установка временного пароля "123" для сохранения максимально полного объёма данных
- Гарантированное отсутствие нежелательной синхронизации исследуемого устройства с компьютером, на котором проводится извлечение (при использовании iTunes синхронизацию необходимо принудительно отключать вручную)

**Внимание**: пароль к резервной копии является свойством устройства (iPhone, iPad, iPod Touch). Если в устройстве установлен пароль на резервные копии, то устройство будет выдавать наружу уже зашифрованные данные независимо от того, какое приложение (iTunes или стороннее)

используется для создания резервной копии. Начиная с iOS 11 этот пароль можно сбросить на самом устройстве, для чего необходимо знать код блокировки экрана устройства.

**Сброс пароля к резервным копиям**

Единожды установленный пароль надёжно защищает уже созданные резервные копии. Сам пароль при этом сохраняется на устройстве. Для сброса пароля телефон должен быть полностью работоспособен, а код блокировки экрана должен быть известен. Для того, чтобы сбросить пароль, воспользуйтесь инструкцией, опубликованной Apple.

*Данные из зашифрованной резервной копии нельзя восстановить без ввода пароля. В iOS 11 или более поздней версии можно создать зашифрованную резервную копию устройства, сбросив пароль. Чтобы сделать это, нужно выполнить следующие действия.*

- *На устройстве iOS выберите «Настройки» > «Основные» > «Сброс».*
- *Нажмите «Сбросить все настройки» и введите пароль ОС iOS.*
- *Следуйте инструкциям по сбросу настроек. Это не затронет данные или пароли пользователей, но приведет к сбросу таких настроек, как уровень яркости дисплея, позиции программ на экране «Домой» и обои. Пароль для шифрования резервных копий также будет удален.*
- *Снова подключите устройство к iTunes и создайте новую зашифрованную резервную копию.*
- *Вы не сможете использовать ранее созданные зашифрованные резервные копии, но можете использовать iTunes для резервного копирования текущих данных и установить новый пароль резервной копии.*

*На устройстве с iOS 10 или более ранней версии сброс пароля невозможен. В этом случае попробуйте выполнить следующие действия.*

- *Если ваше устройство настраивал кто-либо другой, узнайте пароль у него.*
- *Воспользуйтесь резервной копией, созданной с помощью iCloud, а не iTunes. Если у вас нет резервной копии в iCloud, ее можно создать.*
- *Попробуйте воспользоваться более ранней резервной копией в iTunes.*

**Внимание**: если вы воспользуетесь инструкцией по сбросу пароля к резервной копии, с устройства будет удалён код блокировки экрана. Сброс кода блокировки в свою очередь исключает iPhone из «доверенного круга устройств», которые могут синхронизировать в iCloud облачную связку ключей, данные «Здоровья», сообщения и некоторые другие данные. Кроме того, удаление кода блокировки приводит к тому, что с устройства удаляются скачанные сообщения Exchange (если они были) и обнуляется история транзакций Apple Pay. Наконец, после удаления пароля вы более не сможете сбросить или изменить с данного устройства пароль от Apple ID, если на вашей учётной записи активирована двухфакторная аутентификация (точнее, сможете это сделать через браузер, указав старый пароль и пройдя проверку двухфакторной аутентификацией).

Подробнее о защите резервных копий можно прочесть в нашей статье.

На компьютере пользователя резервные копии могут храниться по следующим путям:

- **macOS**: ~/Library/Application Support/MobileSync/Backup/
- **Windows 7, Windows 8, Windows 8.1, and Windows 10**: %appdata% или %USERPROFILE% (если вы загрузили iTunes из Microsoft Store) \Apple Computer\MobileSync\Backup\

В случае, если резервная копия защищена паролем, для его восстановления потребуются файлы **Manifest.plist** и **Manifest.db** (второй из них - начиная с iOS 10 и более современных).

### 3.2.3.2 Резервные копии без пароля

Одна из особенностей резервных копий iTunes без пароля в том, что все имена файлов отображаются в виде хешей SHA-1 от настоящего имени так же, как и путь и домен.

EPB позволяет восстанавливать оригинальные имена файлов в том виде, в котором они отображаются в macOS. В Elcomsoft Phone Viewer можно просматривать содержимое таких резервных копий независимо от того, были ли восстановлены оригинальные имена файлов.

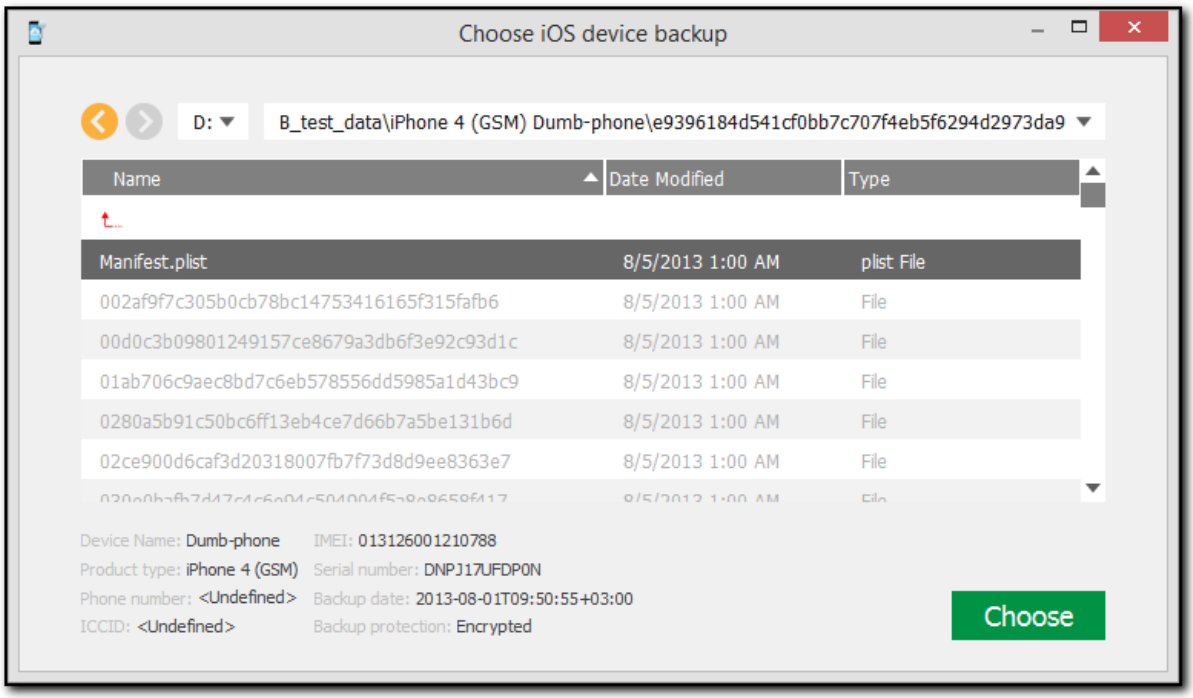
**Для восстановления оригинальных имён файлов** проделайте следующие шаги:

1. В меню **Tools/Инструменты** выберите вкладку **Apple**.
2. Выберите **Decrypt backup/Расшифровать рез. копию.**
3. Выберите файл *Manifest.plist,* перетащив его на окно **Decrypt backup/Расшифровать рез. копию** либо нажмите **Choose backup/Выбрать рез. копию**.

**Внимание: в macOS 10.14 и более новых вам потребуется предоставить привилегию Full Disk Access приложению EPB. Детали в секции Troubleshooting.**

4. Либо выберите файл *Manifest.plist* в открывшемся окне и нажмите **Choose/Выбрать**.

Свойства файлов перечислены в таблице.

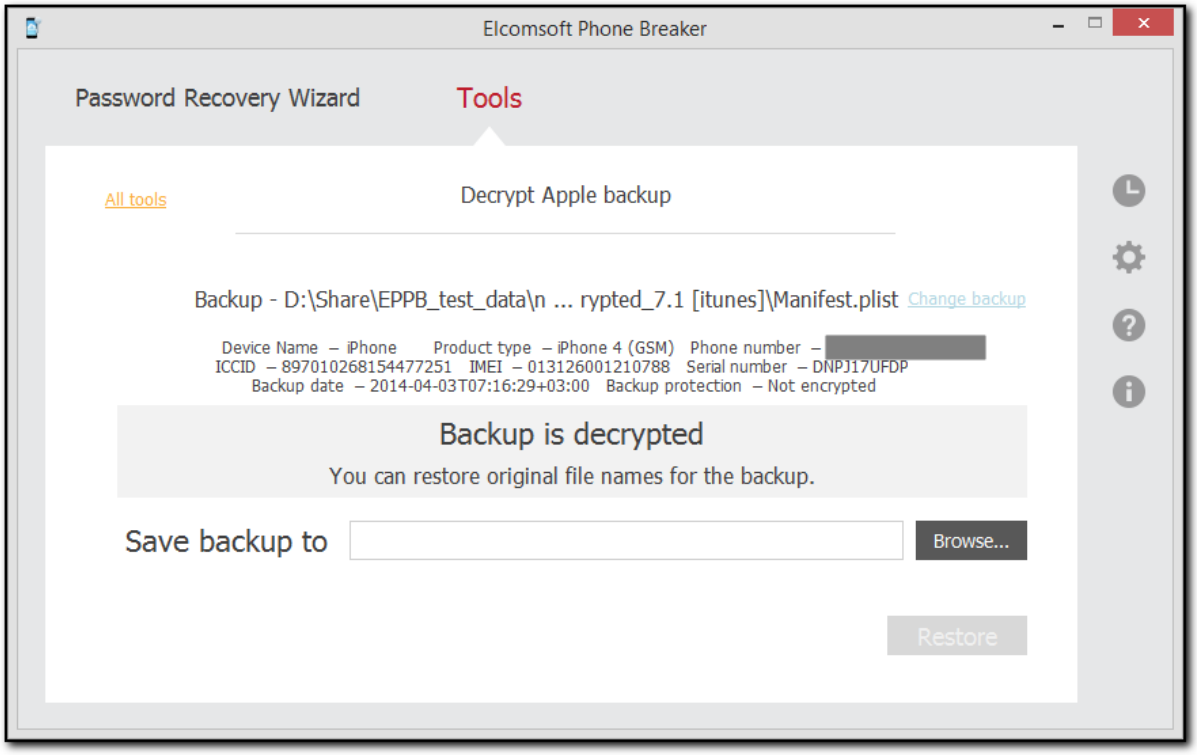



5. После загрузки резервной копии вы сможете просмотреть информацию:
   - **Серийный номер устройства**
   - **Дата создания резервной копии**

- **Тип устройства**

В зависимости от типа устройства может быть доступна и другая информация (IMEI, ICCID, номер телефона и т.п.)

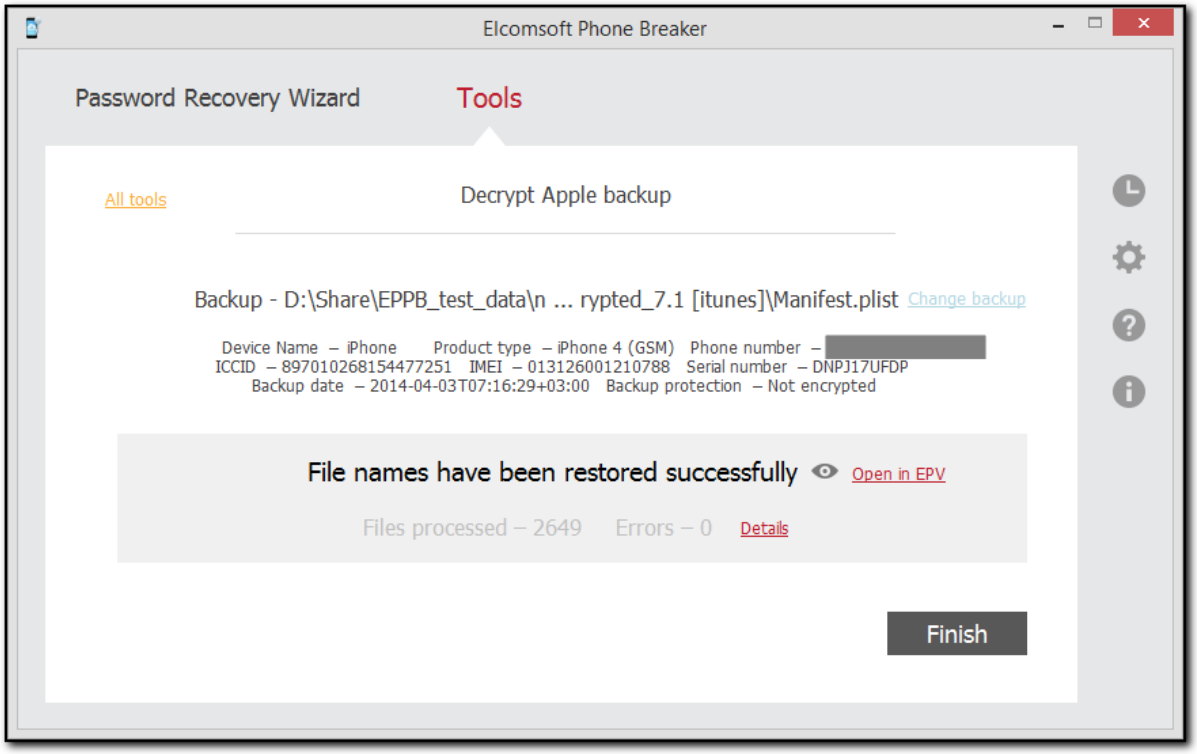
Выбрать другую резервную копию можно, нажав **Change backup/Заменить рез. копию**.




6. Выберите путь, куда будет сохранена резервная копия, и нажмите **Restore/Восстановить**. Имена файлов будут расшифрованы и представлены в том виде, в котором они отображаются в macOS.

**Внимание: путь на диске, куда будет сохраняться резервная копия с восстановленными именами, должен быть пустым.**

7. Начнется процесс расшифровки. Вы можете просмотреть количество обработанных файлов и количество ошибок, полученных при расшифровке.




8. Когда расшифровка закончится, вы можете нажать для просмотра резервной копии.

Если на вашем компьютере установлен Elcomsoft Phone Viewer, вы можете просмотреть содержимое резервной копии, нажав **Open in EPV/Открыть в EPV**.

9. Отчёт доступен нажатием на кнопку **Details/Подробности**.

10. Нажмите **Finish/Завершить**, чтобы закрыть окно.

#### 3.2.3.3 Резервные копии с паролем

EPB позволяет расшифровать зашифрованную резервную копию с известным паролем. После успешного завершения расшифровки вы можете просматривать содержимое резервной копии в Elcomsoft Phone Viewer.

Расшифровка резервной копии доступна только в том случае, если вы знаете пароль к резервной копии, поэтому вам может потребоваться сначала восстановить пароль с помощью EPB для Windows.

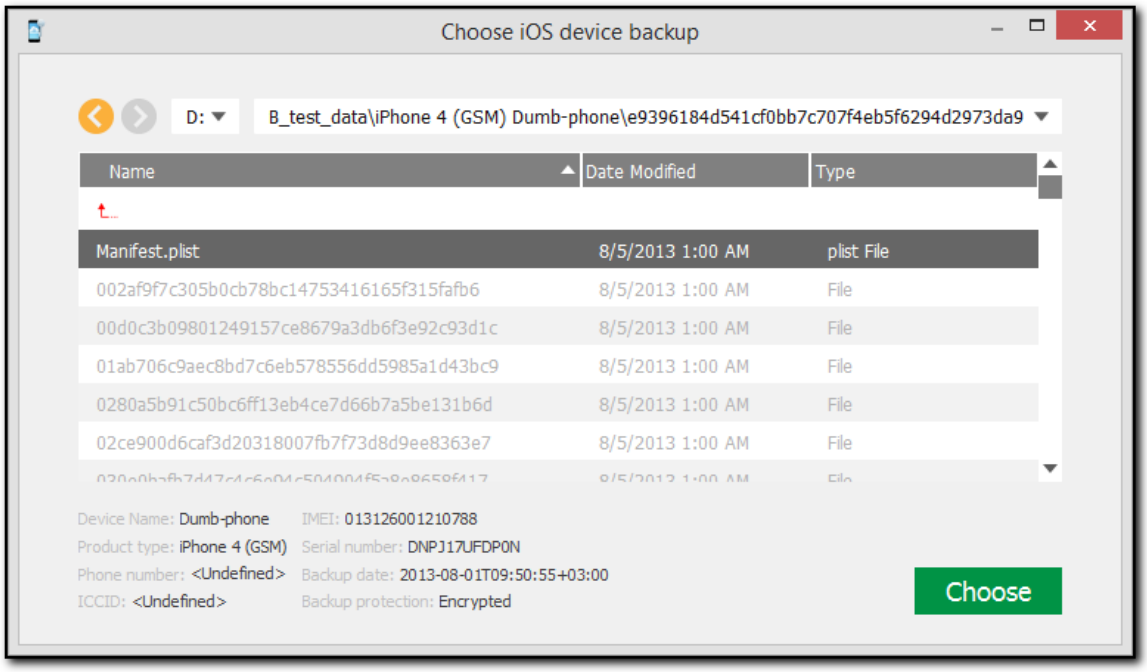
Открыть резервную копию:

1. В меню **Tools/Инструменты** выберите вкладку **Apple**.
2. Выберите **Decrypt backup/Расшифровать рез. копию.**
3. Выберите файл *Manifest.plist,* перетащив его на окно **Decrypt backup/Расшифровать рез. копию** либо кликнув на **Choose backup/Выбрать рез. копию**.

**Внимание: В macOS 10.14 и более новых, предоставьте EPB разрешение Full Disk Access для доступа к папке iTunes. См. раздел Troubleshooting.**

4. В открывшемся окне перейдите к файлу резервной копии, указав путь к файлу в поле пути. Выберите файл Manifest.plist и нажмите **Choose/Выбрать.**

Свойства файла будут показаны в таблице.

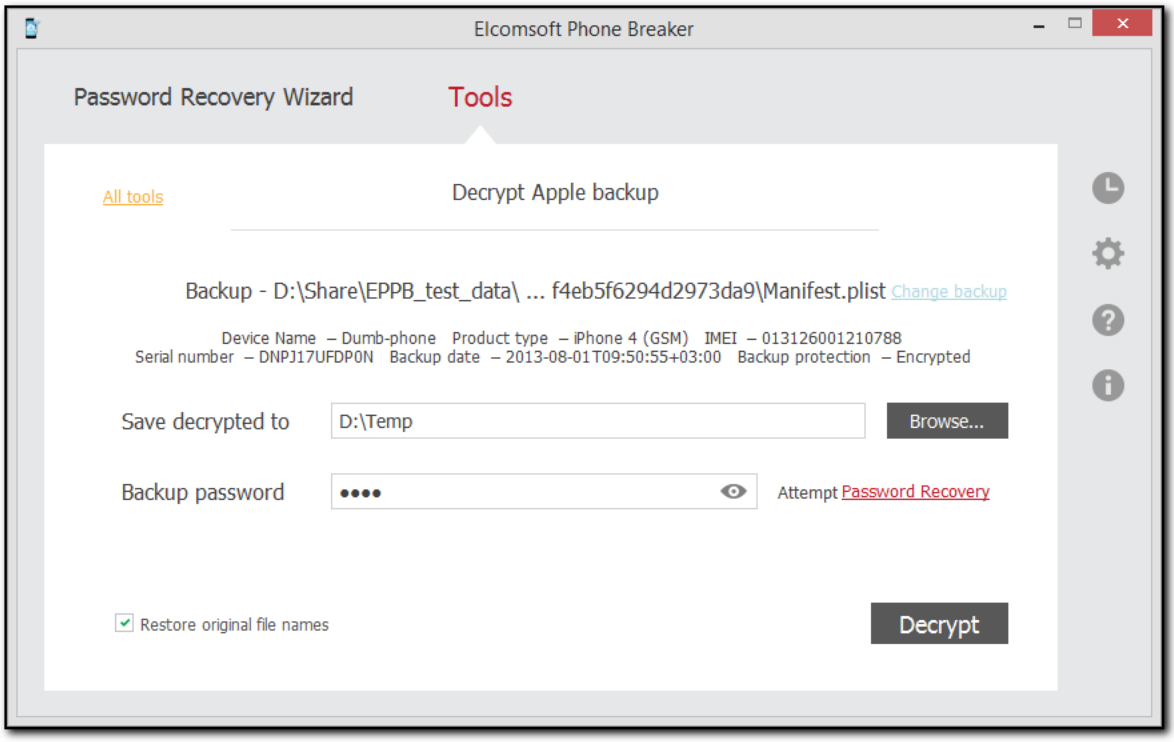



5. После загрузки резервной копии вы сможете просмотреть информацию:

   - **Серийный номер устройства**
   - **Дата создания резервной копии**
   - **Тип устройства**

В зависимости от типа устройства может быть доступна и другая информация (IMEI, ICCID, номер телефона и т.п.)

Выбрать другую резервную копию можно, нажав **Change backup/Заменить рез. копию.**




6. Укажите настройки расшифровки.

   - **Save decrypted to/Сохранить расшифрованные данные в**: путь на диске, куда будет сохраняться расшифрованная резервная копия (должен быть пустым).

   - **Backup password/Пароль к рез. копии**: пароль к резервной копии. Нажмите для снятия маскировки пароля символами (*).

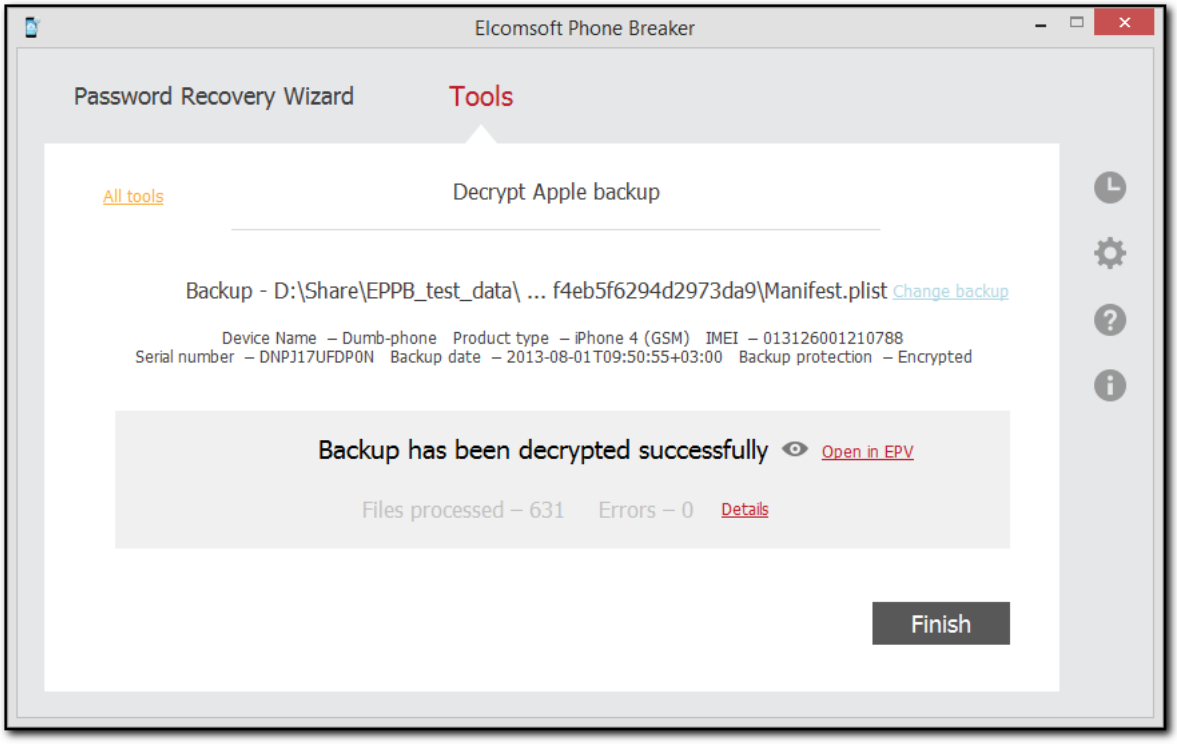
   В EPB для Windows OS доступна опция **Restore password/Восстановить пароль**, позволяющая восстанавливать неизвестные пароли методом перебора.

   - **Restore original file names/Восстановить исходные имена файлов:** восстанавливает оригинальные имена файлов в том виде, в каком они доступны в файловой системе устройства. Если вы планируете работать с расшифрованной резервной копией в стороннем ПО, рекомендуем не использовать эту опцию.

7. Нажмите **Decrypt/Расшифровать.**

8. По окончании расшифровки можно нажать , чтобы определить место на диске, в котором сохранена резервная копия.

Если на вашем компьютере установлена программа Elcomsoft Phone Viewer, вы можете просмотреть содержимое резервной копии, щелкнув ссылку **Open in EPV/Открыть в EPV.**



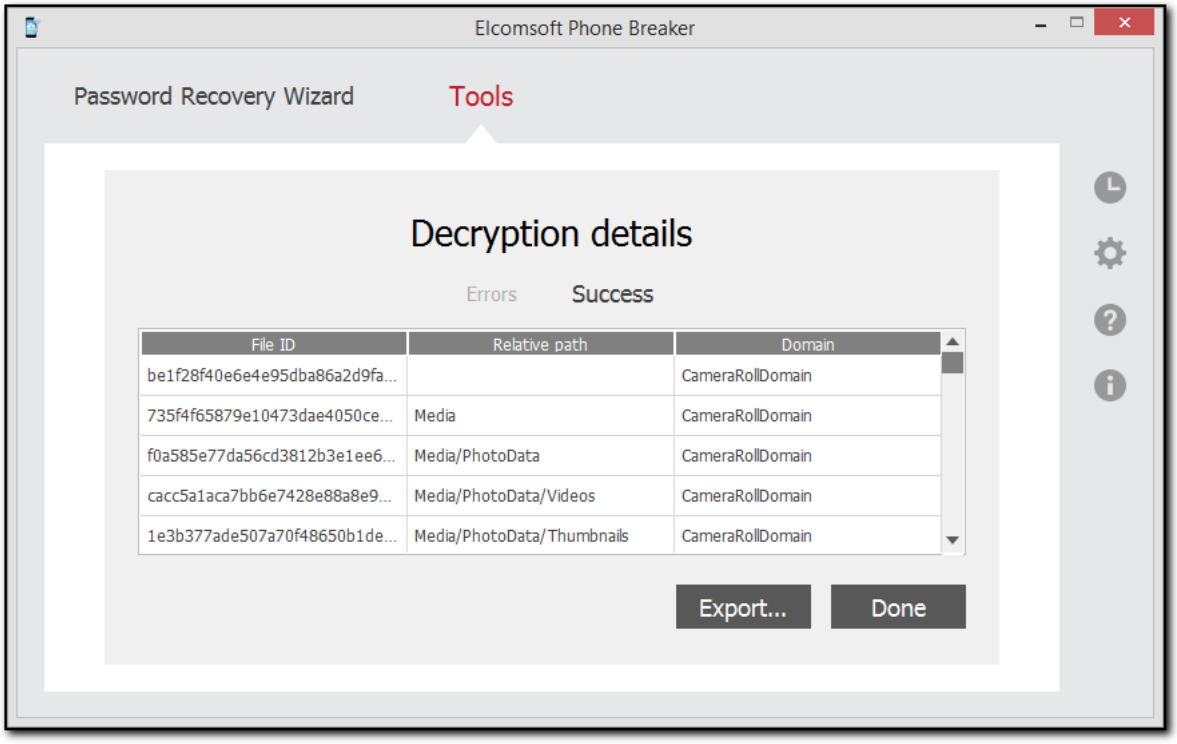

9. Отчёт доступен нажатием на кнопку **Details/Подробности.**

10. Нажмите **Finish/Завершить**, чтобы закрыть окно.

#### 3.2.3.4 Отчёт о расшифровке

В данном отчёте содержится информация о процессе расшифровки, включая ошибки. Открыть отчёт можно командой **Details/Подробности** после завершения расшифровки.

Пример отчёта:




В данные входят:

- **File ID**: Имя файла, состоящее из хэша SHA-1 имени файла, вместе с его путем и доменом.
- **Relative path**: Путь к файлу в указанном домене.
- **Domain**: Имя домена, в котором хранится файл.

Для экспорта отчёта в текстовом формате или в файл XML, нажмите **Export/Экспорт.**

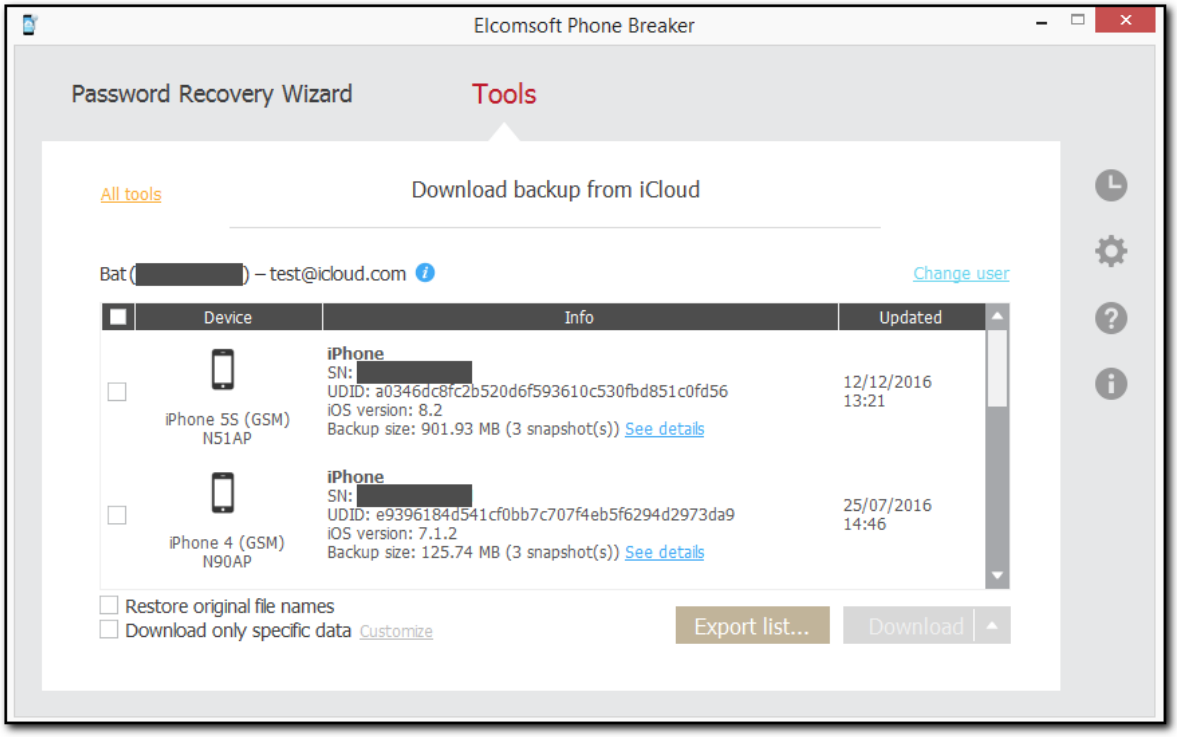
Для выхода нажмите **Done/Готово**.

### 3.2.3.5 Экспорт списка резервных копий

Список резервных копий можно экспортировать в формат XML 1.1.

Чтобы экспортировать список резервных копий устройств iOS в iCloud, выполните следующие действия:

1. Нажмите **Export List/Экспортировать список**.




2. Выберите путь сохранения файла XML.

3. Список будет экспортирован. Информация о каждом устройстве iOS содержит имя устройства, серийный номер, UDID, тип, модель, версию iOS, информацию о последней резервной копии, имя пользователя, идентификатор пользователя и то, включена ли двухэтапная аутентификация.

## 3.2.4 Работа с iCloud

### 3.2.4.1 Резервные копии в iCloud

#### 3.2.4.1.1 Резервные копии в iCloud

Устройства под управлением iOS могут сохранять резервные копии в облаке. Точное содержимое резервной копии в iCloud будет зависеть от множества факторов.

Будут ли создаваться резервные копии в облаке зависит в первую очередь от настройки (**Settings/Настройки | iCloud | Backup & Storage/Резервные копии и хранилище**) в устройстве пользователя. Однако на создание резервных копий влияют и другие факторы: наличие свободного места в учётной записи iCloud пользователя, периодичность подключения, доступность сетей Wi-Fi во время зарядки и т.п.

Для извлечения резервной копии необходимо знать логин и пароль пользователя (Apple ID); для учётных записей с двухфакторной аутентификацией понадобится доступ ко второму фактору. В качестве альтернативы в некоторых случаях можно использовать маркеры аутентификации, которые могут быть доступны на компьютере пользователя.

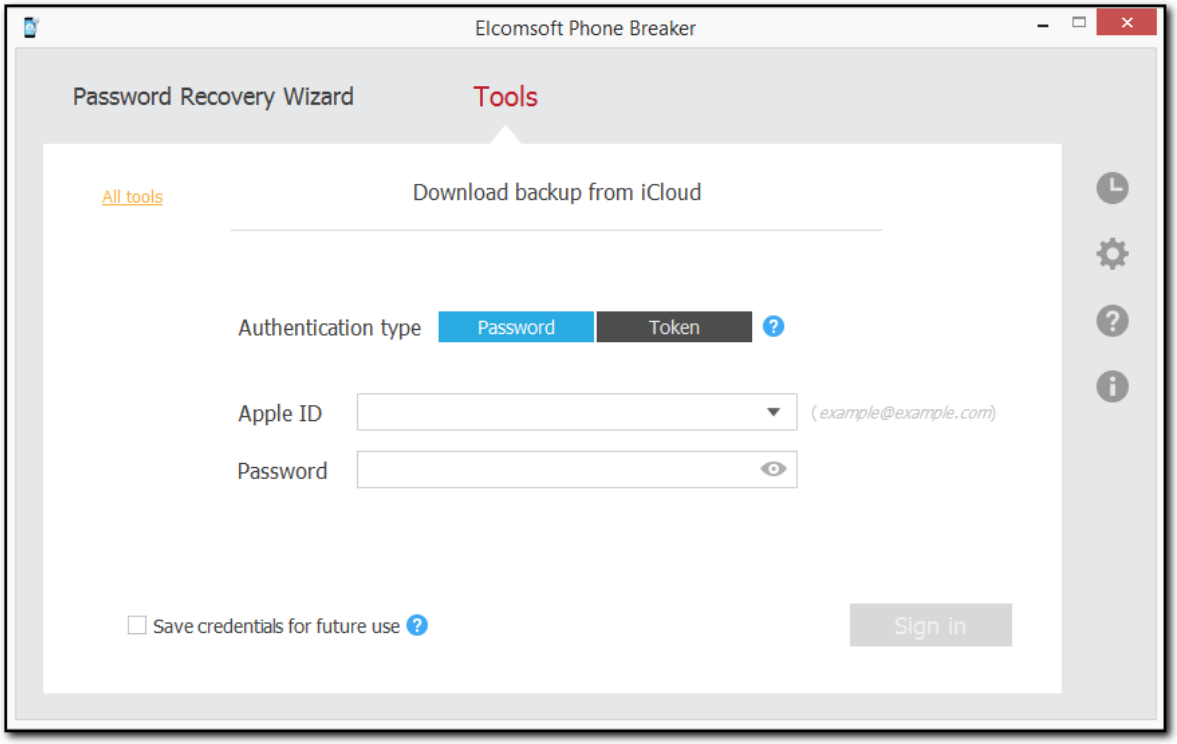
**EPB** сохраняет "облачные" резервные копии в том же формате, который используется iTunes. После расшифровки данных вы сможете просмотреть содержимое в Elcomsoft Phone Viewer.

#### 3.2.4.1.2 Скачивание резервных копий из iCloud

Для скачивания резервной копии проделайте следующие шаги:

1. В меню **Tools/Инструменты** откройте вкладку **Apple**.
2. Выберите **Download backup from iCloud/Скачать рез. копию из iCloud**.
3. Выберите способ аутентификации:
   - **Password/Пароль**: с использованием Apple ID и пароля
   - **Token/Токен**: с использованием маркера аутентификации. Маркер можно извлечь посредством утилиты Elcomsoft Apple Token Extractor, которая входит в поставку. Дополнительно об извлечении маркера: Извлечение маркеров аутентификации.

**Внимание: Сфера применимости маркеров аутентификации ограничена: резервные копии доступны при помощи маркера только для устройств под управлением iOS 11.2 и более старых версий.**




4. Нажмите **Sign in/Войти**.

**Внимание: при вводе Apple ID в неправильном формате будет выведено сообщение об ошибке. Закройте сообщение и введите Apple ID в формате example@example.com.**

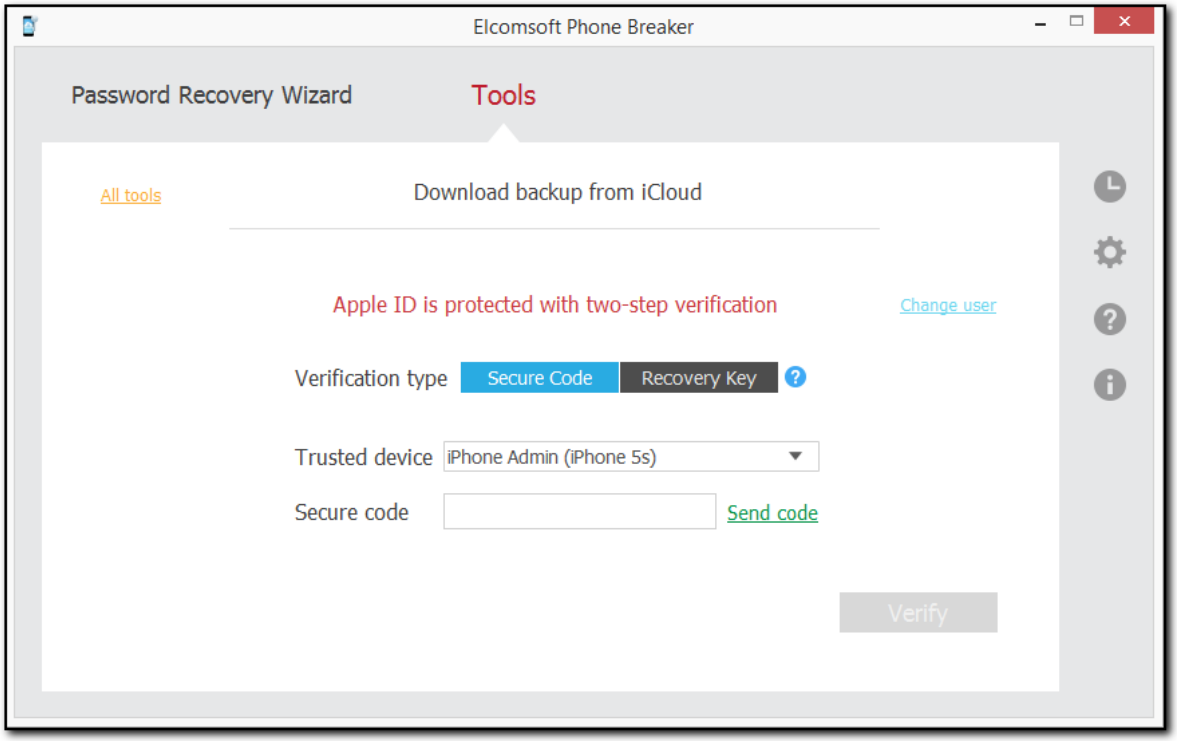
**Внимание: если Apple ID защищен двухфакторной аутентификацией, вам необходимо подтвердить отправку проверочного кода на доверенные устройства или сообщения на телефонный номер.**

Опция **Save credentials for future use/Сохранить учётные данные** позволяет сохранить учётные данные для использования в будущих сессиях.

5. Если Apple ID защищён двухфакторной аутентификацией по методу "**two-step verification**" (старый способ, не используется в современных учётных записях), выберите тип аутентификации:

- **Secure Code/Код проверки: 4-значный** код будет доставлен на доверенное устройство или на телефонный номер в виде SMS. Для получения кода необходимо нажать **Send code/Отправить код**, после чего ввести полученный код в поле **Secure code/Код проверки.**
- **Recovery Key/Ключ восст-я:** 14-значный ключ, полученный в учётной записи Apple (только если используется старая схема Two-step verification).

6. Нажмите **Verify/Проверить.**



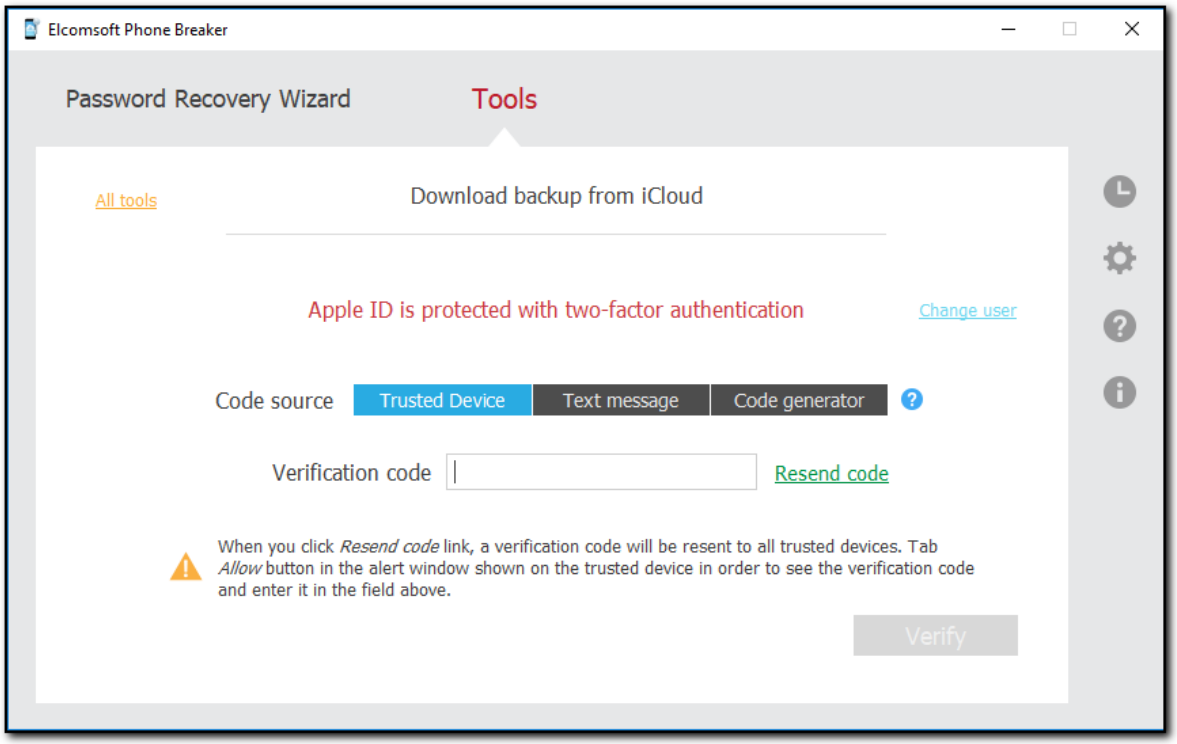

7. Если Apple ID защищён актуальным способом двухфакторной аутентификации (two-factor authentication), вам доступны следующие варианты:

- Выберите доверенное устройство **Trusted Device/Доверенное уст-во**, после чего нажмите **Send code/Отправить код**. Введите полученный 6-значный одноразовый цифровой пароль в поле **Verification code/Код проверки.** Нажмите **Resend code/Отправить код повторно** для инициации повторной доставки кода на все доверенные устройства.
- Выберите **Text message/Текстовое сообщение**, после чего нажмите **Send code/Отправить код**. Введите полученный в виде SMS 6-значный одноразовый цифровой пароль в поле **Verification code/Код проверки.** Нажмите **Resend code/Отправить код повторно** для инициации повторной доставки кода на привязанный номер телефона.

**Внимание: для отправки сообщения требуется macOS 10.12 или более новая.**

**Внимание: аутентификация через SMS доступна только в редакции Forensic.**

- Выберите **Code generator/Генератор кодов** и введите 6-значный код, сгенерированный на устройстве, в поле **Verification code/Код проверки**. Код генерируется в настройках устройства.

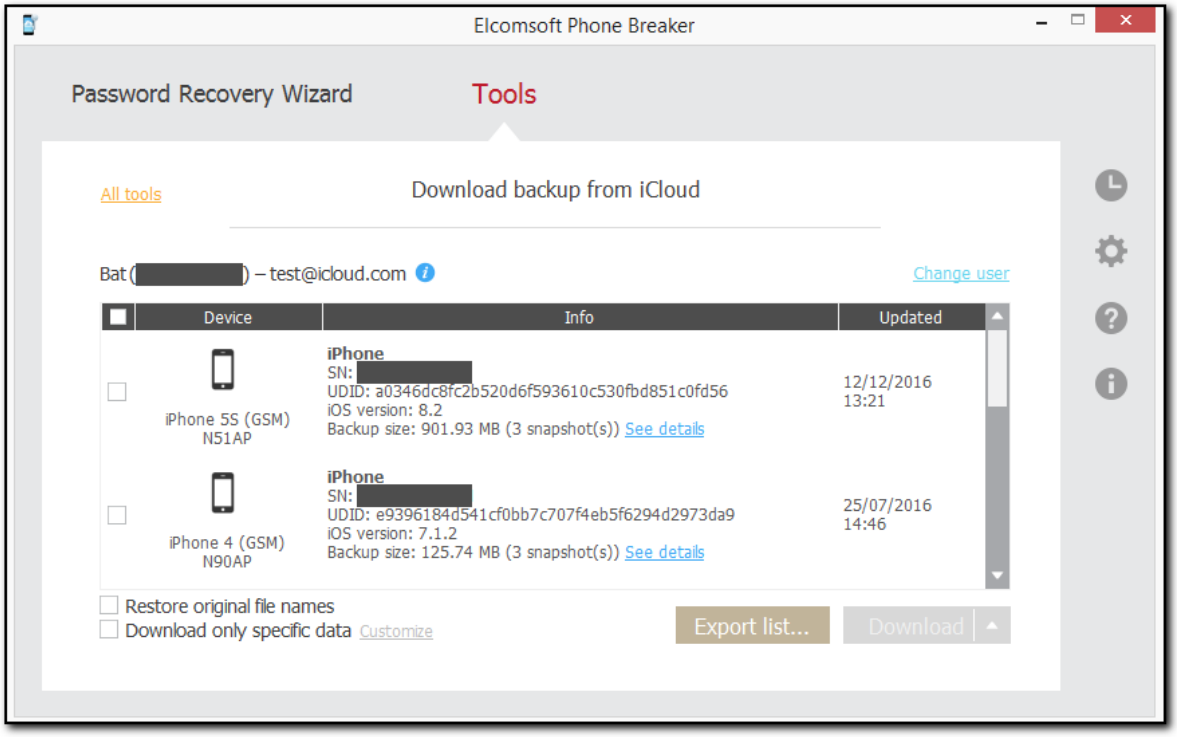



8. Нажмите **Verify/Проверить**.

9. Откроется окно выбора резервной копии.

Вы можете просмотреть имя пользователя, идентификатор пользователя и Apple ID пользователя iCloud, а также список резервных копий, созданных пользователем. По умолчанию отображаются 3 последних резервных копии. Наведите указатель мыши на синий значок i, чтобы просмотреть размер данных.

Чтобы выбрать резервные копии, сделанные другим пользователем iCloud, нажмите **Change user/Выбрать другого пользователя.**

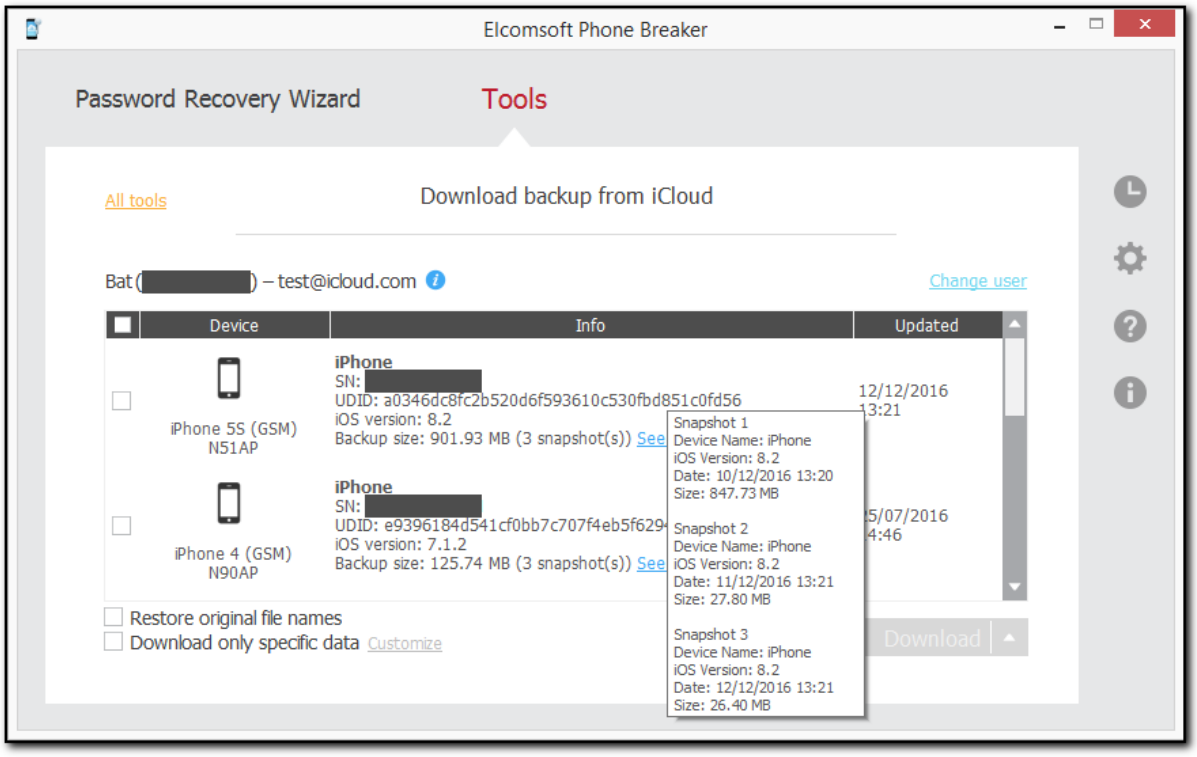



Для всех устройств доступна следующая информация:

- Название устройства
- Модель
- Серийный номер
- Уникальный идентификатор устройства
- Версия iOS
- Дата создания последней резервной копии
- Размер резервной копии

**Внимание: время и дата получаются с устройства.**

Нажмите **See details/См. подробно** для отображения детальной информации.




Для резервных копий доступны данные:

- Имя устройства
- Версия iOS
- Дата, когда была сделана резервная копия
- Размер

**Внимание: Для копий после первой, отображаемый размер - это размер данных, добавленных к моменту сохранения копии, а не полной резервной копии.**

10. Выберите устройство или устройства резервные копии которых вы хотите загрузить, установив флажки слева.

11. Определите параметры для загрузки резервных копий. Наведите указатель мыши на флажки, чтобы просмотреть подсказки для каждого варианта.

- **Restore original file names/Восстановить исходные имена файлов**: Если этот параметр выбран, позволяет сохранять все файлы резервных копий с теми же именами файлов, что и в операционной системе iOS, включая полный путь: например, сообщения (SMS и iMessage) сохраняются как \HomeDomain\Library\SMS\sms.db (формат SQLite). Если он не выбран, резервная копия будет сохранена в том же формате, который iTunes создает при создании локальной резервной копии. В этом случае вы сможете анализировать загруженные резервные копии с помощью Elcomsoft Phone Viewer и сторонних приложений, поддерживающих формат iTunes. Обратите внимание, что эта опция будет включена автоматически, если вы выберете режим селективного скачивания данных.

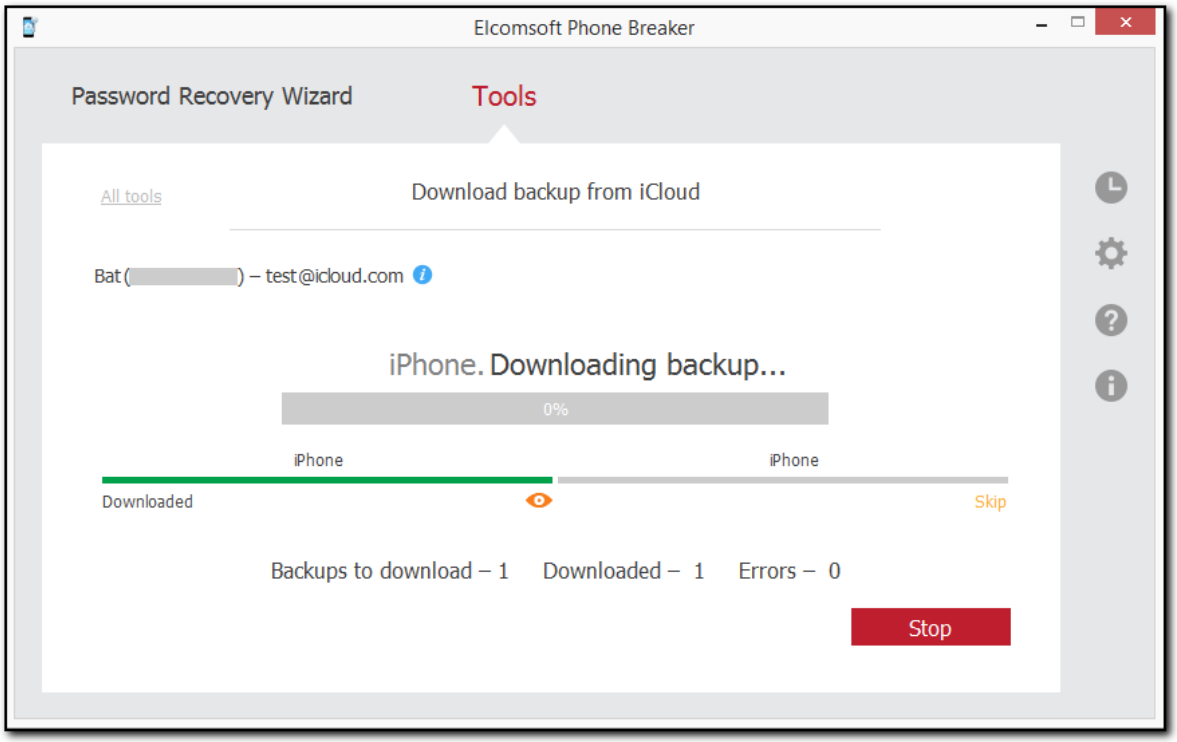
- **Download only specific data/Скачать только выбранные данные**: селективное скачивание данных, позволяющее выбрать категории, которые будут скачаны.

12. Нажмите **Download/Скачать** или **Download to/Скачать в** для скачивания.

13. Выберите папку командой **Select Folder/Выбрать папку.**

**Внимание: маркер аутентификации, который уже нельзя использовать для доступа к резервным копиям, иногда всё ещё можно использовать для доступа к синхронизированным данным.**

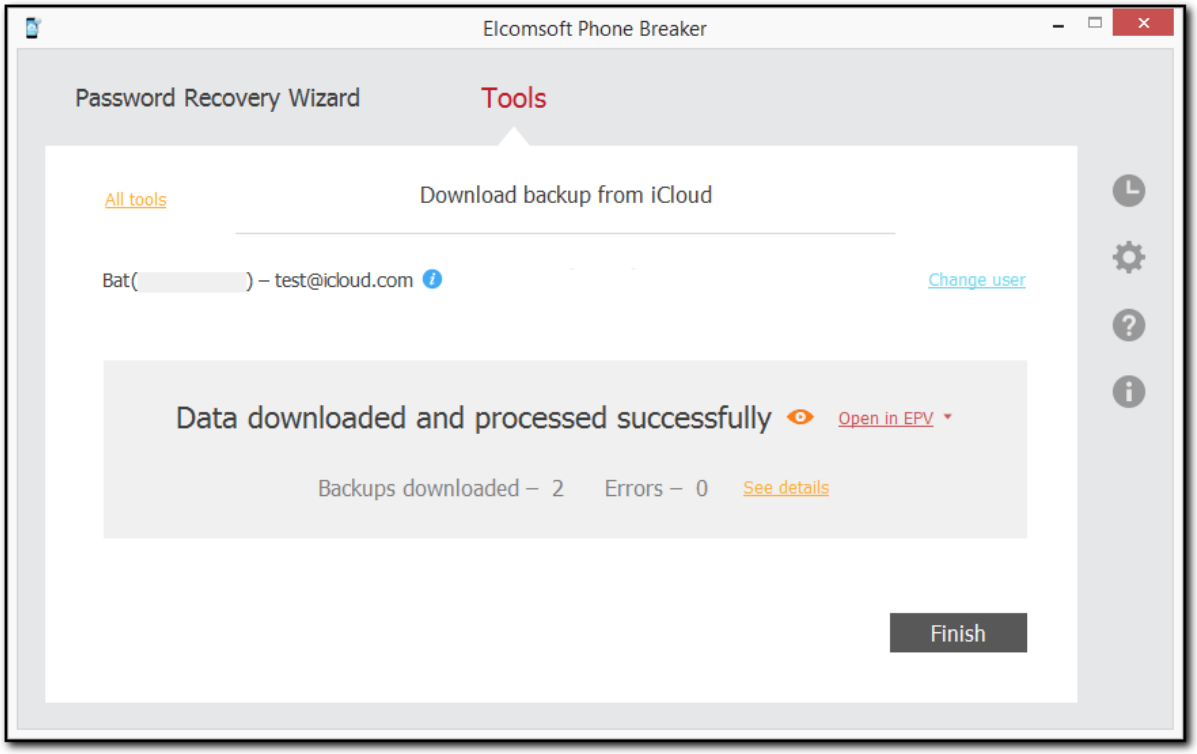
15. Если вы выбрали несколько резервных копий, вы можете нажать Skip/Пропустить, чтобы пропустить загрузку любой из них.




**ПРИМЕЧАНИЕ. Резервные копии, которые еще не были полностью созданы, не будут загружены.**

16. По завершении загрузки нажмите кнопку «Просмотр», чтобы просмотреть резервную копию на локальном компьютере.

Нажмите **Open in EPV/Открыть в EPV** для анализа данных в Elcomsoft Phove Viewer либо запустите Elcomsoft Phove Viewer и откройте скачанные данные.




17. Ссылка **See details/См. подробно** позволяет просмотреть информацию о процессе скачивания.

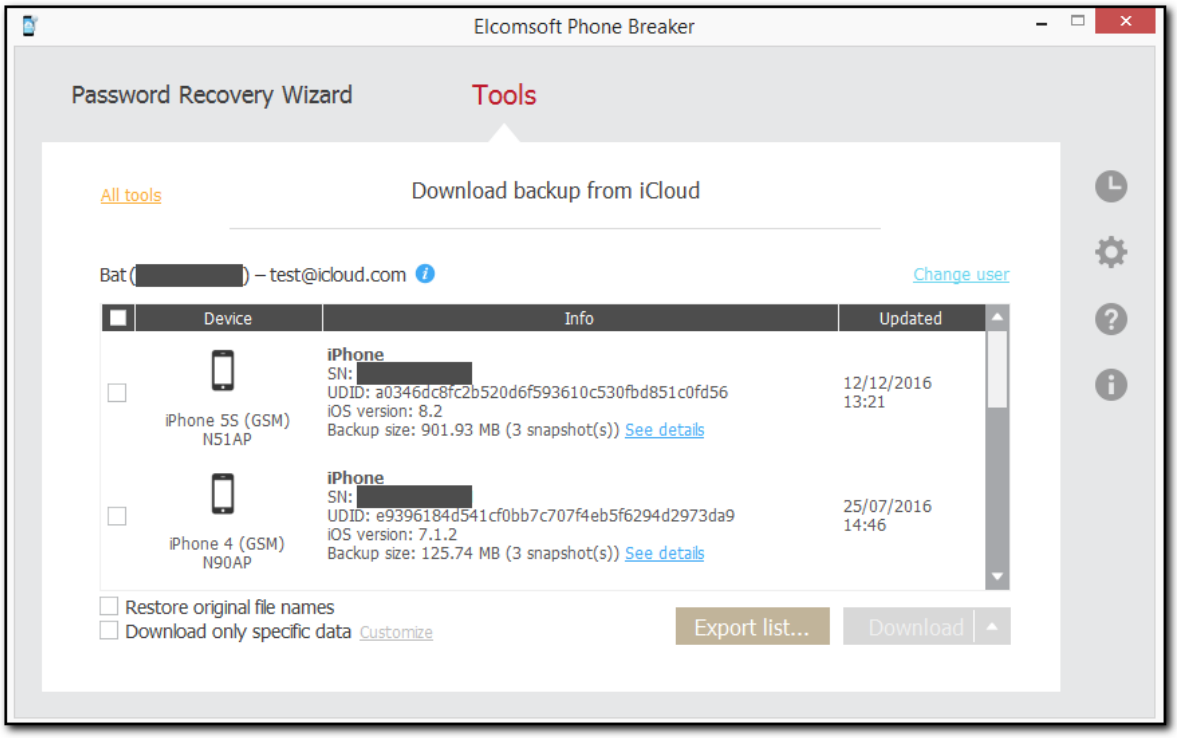
18. Закрыть окно можно кнопкой **Finish/Завершить**.

Обратите внимание, что резервные копии, начиная с iOS 9.x.x и выше, имеют структуру, отличную от резервных копий iOS 8.0 и более ранних версий. Поэтому при наличии нескольких резервных копий разных версий для одного и того же UDID устройства они будут сохранены на локальном компьютере в папке с именем UDID. Однако снимки, принадлежащие разным версиям iOS, будут храниться в разных подпапках:

- Для iOS 8.0 и ниже: в папке с именем в формате [01] [YYYYMMDD_HHMMSS] [R], где [YYYYMMDD_HHMMSS] - дата и отметка времени резервного копирования.
- Для iOS 9.x.x и выше: в папке с именем в виде [A30FD565-3776-4B8E-95AB-B4F06FD930BC] [YYYYMMDD_HHMMSSZ], где [YYYYMMDD_HHMMSSZ] - дата и отметка времени резервного копирования.

#### 3.2.4.1.3 Выборочное скачивание

При скачивании из облака резервных копий доступна опция выборочного скачивания, которая активируется командой **Download only specific data/Скачать только выбранные данные**. Использование этой опции позволяет выбирать, какие категории данных из резервной копии будут скачаны. Её использование позволяет сэкономить время, скачав лишь необходимые для начала работы данные.




Чтобы выбрать категории данных, нажмите **Customize/Настроить**. Обратите внимание, что название ссылки изменится с **Customize/Настроить** на **Customized/Настроено,** а её цвет сменится с **зелёного** на **красный**.

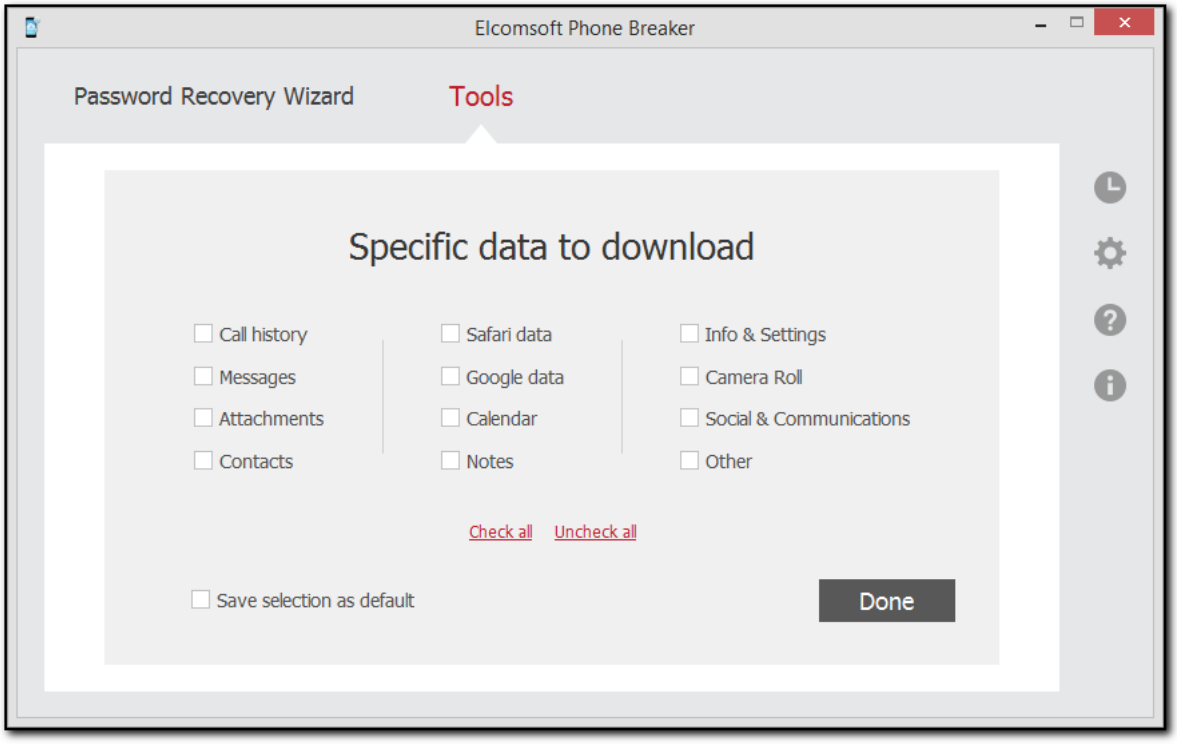
Если не будет выбрано ни одной категории, то будут скачаны только необходимые метаданные, в состав которых входят файлы:

- Info.plist
- Manifest.mbdb / Manifest.db
- Manifest.plist
- Status.plist

Используйте команды **Check All/Выбрать все** и **Uncheck All/Очистить все,** чтобы выделить или снять выделение со всех категорий.

**Внимание: данные часового пояса скачиваются всегда.**

Вы можете сохранить выбранные настройки в качестве настроек по умолчанию, выбрав **Save selections as default/Сохранить настройки по умолчанию**.




Доступны следующие категории:

- **Call History -** история звонков.

Скачиваются данные:
\WirelessDomain\Library\CallHistory* (iOS 7.x и ниже)
\HomeDomain\Library\CallHistoryDB* (iOS 8.x и новее)

- **Messages -** сообщения SMS, iMessages и MMS.

Скачиваются данные:
\HomeDomain\Library\SMS\sms.db
\HomeDomain\Library\SMS\Drafts*

- **Attachments -** вложения к сообщениям.

\MediaDomain\Library\SMS\Attachments*

- **Google data -** данные приложений Google для iOS: Google Earth, Chrome, Maps, YouTube и т.д.

Скачиваются данные:
AppDomain-com.google.b612*
AppDomain-com.google.GoogleDigitalEditions*
AppDomain-com.google.GoogleMobile*
AppDomain-com.google.Blogger*
AppDomain-com.google.chrome.ios*
AppDomain-com.google.coordinate*
AppDomain-com.google.Drive*
AppDomain-com.google.Gmail*
AppDomain-com.google.GoogleBooks*
AppDomain-com.google.GooglePlus*

AppDomain-com.google.GVDialer*
AppDomain-com.google.ios.youtube*
AppDomain-com.google.Maps*
AppDomain-com.google.offers*
AppDomain-com.google.Orkut *
AppDomain-com.google.Translate*
AppDomain-com.google.hangouts*
AppDomain-com.google.Authenticator*

- **Safari data** - история браузера Safari, кэш, cookie, история поисковых запросов.

Скачиваются данные:
\HomeDomain\Library\Safari*
\HomeDomain\Library\Caches*
\HomeDomain\Library\Cookies*
\AppDomain-com.apple.mobilesafari*

- **Contacts -** адресная/телефонная книга.

Скачиваются данные:
\HomeDomain\Library\AddressBook\AddressBook.sqlitedb
\HomeDomain\Library\AddressBook\AddressBookImages.sqlitedb

- **Notes -** заметки.

Скачиваются данные:
\HomeDomain\Library\Notes\notes.idx
\HomeDomain\Library\Notes\notes.sqlite

- **Info & Settings** - настройки устройства.

Скачиваются данные:
\HomeDomain\Library\Accounts*.*
\HomeDomain\Library\ConfigurationProfiles*.*
\HomeDomain\Library\Preferences*.*
\RootDomain\Library\Preferences*.*
\SystemPreferencesDomain*.*
\WirelessDomain\Library\Preferences*.*

- **Calendar -** календари и список событий.

Скачиваются данные:
\HomeDomain\Library\Calendar\Calendar.sqlitedb

- **Camera roll -** фотографии и видео (если сохраняются; включение пользователем iCloud Photo Library отменяет сохранение фотографий в составе резервных копий; фотографии при этом синхронизируются в облако и извлекаются из синхронизированных категорий данных).
\CameraRollDomain*

- **Social & Communications -** данные приложений мгновенного обмена сообщениями, включая Skype, WhatsApp, Viber и т.п., а также некоторых приложений социальных сетей.

Скачиваются данные:
AppDomain-com.viber*
AppDomainPlugin-com.viber.app-share-extension
AppDomainPlugin-com.viber.watchkitextension
AppDomain-com.cardify.tinder*
AppDomain-jp.naver.line*

AppDomainGroup-group.com.linecorp.line*
AppDomain-com.linecorp.line.ipad*
AppDomain-com.tencent.xin*
AppDomain-net.whatsapp.WhatsApp*
AppDomainGroup-group.net.whatsapp.WhatsApp.shared*
AppDomain-com.burbn.instagram*
AppDomain-com.facebook.Facebook*
AppDomain-com.facebook.Messenger*
AppDomain-com.skype.skype*
AppDomain-com.atebits.Tweetie2*
AppDomain-com.linkedin.LinkedIn*
AppDomain-com.naveenium.foursquare*
AppDomain-com.viber*
AppDomain-com.tencent.mQQi*
AppDomain-com.tencent.mqq*
AppDomain-com.blackberry.bbm1*
AppDomain-com.kik.chat*
AppDomain-com.aol.aim*
AppDomain-com.p.pmsn2free*
AppDomain-com.shapeservices.implus*
AppDomain-com.ebuddy.xms*
AppDomain-com.beejive.WLM*
AppDomain-com.beejive.GTalk*
AppDomain-com.beejive.YIM*
AppDomain-com.beejive.AIM*
AppDomain-com.beejive.FacebookIM*
AppDomain-com.ceruleanstudios.trillian.iphone*
AppDomain-com.yahoo.messenger*

- **Other -** пользовательские словари, данные голосовой почты, данные карт Apple, Passbook, почтовые сообщения и т.п.

Скачиваются данные:
\HomeDomain\Library\Keyboard*
\HomeDomain\Library\Passes*
\HomeDomain\Library\Voicemail*
\HomeDomain\Library\Maps*
\HomeDomain\Library\SpringBoard*
\HomeDomain\Library\Mail*
\HomeDomain\Library\WebKit\Databases*
\HomeDomain\Library\DataAccess*
\RootDomain\Library\Caches\locationd*
\KeyboardDomain\Library\Keyboard*

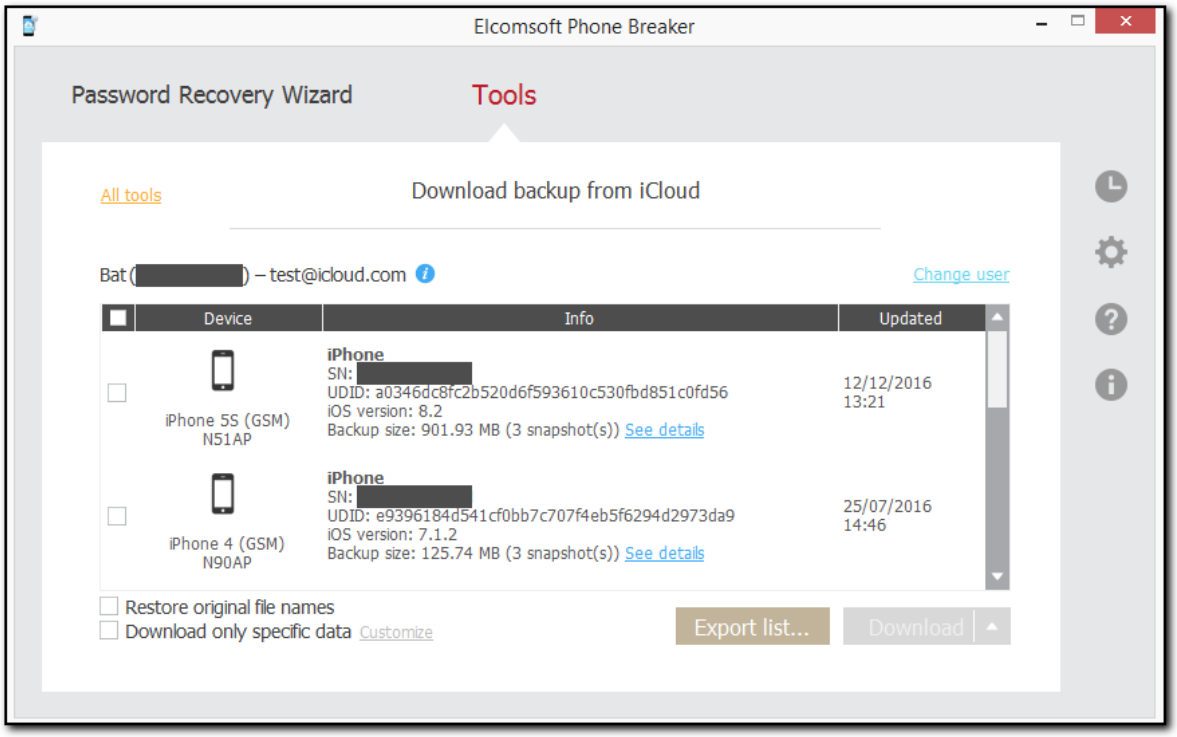
Просмотреть скачанные данные можно в Elcomsoft Phone Viewer.

#### 3.2.4.1.4 Экспорт списка резервных копий

Список резервных копий можно экспортировать в формат XML 1.1.

Чтобы экспортировать список резервных копий устройств iOS в iCloud, выполните следующие действия:

1. Нажмите **Export List/Экспортировать список**.




2. Выберите путь сохранения файла XML.

3. Список будет экспортирован. Информация о каждом устройстве iOS содержит имя устройства, серийный номер, UDID, тип, модель, версию iOS, информацию о последней резервной копии, имя пользователя, идентификатор пользователя и то, включена ли двухэтапная аутентификация.

#### 3.2.4.1.5 Возможные проблемы с загрузкой данных из iCloud

| Проблема | Решение |
|---|---|
| При загрузке резервной копии из iCloud отображается следующее сообщение: **"The requested backup could not be found/Запрашиваемая рез. копия не найдена."**. | Резервная копия, которую вы пытаетесь загрузить, обновлена. Выйдите из системы, затем войдите в iCloud и повторите попытку. |
| Необходимая резервная копия отсутствует в списке элементов для загрузки. | В данный момент создается резервная копия. Она будет доступна, как только будет полностью создана. |
| При загрузке данных из iCloud отображается сообщение: «Условия использования iCloud изменились. Войдите в панель iCloud и примите новые условия, чтобы продолжить работу со службами iCloud». | Условия использования iCloud изменились, и пользователь должен подтвердить их перед использованием iCloud. Войдите в панель iCloud пользователя и примите новые Условия использования.<br>После этого вы сможете работать с данными из iCloud через EPB. |

#### 3.2.4.1.6 Структура резервных копий в iCloud

После загрузки и обработки резервных копий iCloud в целевой папке (iOS 9.x и выше) создаются следующие папки:

*.chunks*
*<device ID>*
*[backup ID][YYYYMMDD_HHMMSSZ]*
*...*
*[backup ID][YYYYMMDD_HHMMSSZ]*
*<device ID>*
*...*

где <device ID> - это уникальный идентификатор устройства, а <backup ID> - это уникальный идентификатор конкретной резервной копии (обычно в iCloud хранится до трех последних резервных копий). [YYYYMMDD_HHMMSSZ] - дата и время создания резервной копии.

Папка .chunks содержит кэш скачиваемых данных, позволяющий возобновить скачивание, если соединение было прервано.

Обратите внимание, что в резервных копиях для iOS 10 и выше каждый файл с невосстановленным именем хранится во вложенной папке, имя которой состоит из первых двух букв имени файла. Например, полный путь к файлу с именем «fd4056e1b33b» будет следующим: *<backup_root>/fd/fd4056e1b33b*

Для iOS 8 и более ранних версий загруженные данные имеют другую структуру:

*.chunks*
*<device id>*
*.keys*
*[01]*
*...*
*[N]*
*[N+1]*
*[01][YYYYMMDD_HHMMSSZ]*
*...*
*[N][YYYYMMDD_HHMMSSZ]*
*[N+1][YYYYMMDD_HHMMSSZ]*

Первые три папки (с номерами, используемыми в качестве имен) также являются необработанными данными. Они хранятся в iCloud, частично преобразованы и уже расшифрованы. Обратите внимание, что резервные копии iCloud являются инкрементными. В большинстве случаев первая папка самая большая (и ее общий размер сравним с объёмом памяти самого устройства), вторая намного меньше, а третья - самая маленькая.

Папки с датой/временем в именах представляют собой полные резервные копии, преобразованные в формат Apple iTunes. Каждый из них имеет примерно такой же размер, как и сама резервная копия (поскольку резервные копии обычно создаются ежедневно, различия невелики). Если вы использовали параметр *Restore original file names/Восстановить исходные имена файлов* либо селективное скачивание, папки с датой/временем также будут иметь суффикс [R] в конце (и размер каждой папки может быть меньше размера резервной копии, потому что не все данные скачиваются).

Таким образом, общий размер, необходимый для хранения всех резервных копий, обычно в пять раз больше, чем размер одной резервной копии.

Независимо от того, используете ли вы параметр *Restore original file names/Восстановить исходные имена файлов*, рекомендуется всегда загружать резервные копии в одну и ту же папку. Не удаляйте папку .chunks до окончания работы с резервными копиями, её наличие позволяет ускорить загрузку.

**Примеры:**

Без ключа *Restore original file names/Восстановить исходные имена файлов*:

.keys
1
19
20
[01][20131124_132403Z]
[19][20131126_130112Z]
[20][20131128_132645Z]

С ключом *Restore original file names/Восстановить исходные имена файлов*:

.keys
1
19
20
[01][20131124_132403Z][R]
[19][20131126_130112Z][R]
[20][20131128_132645Z][R]

Здесь вы получите три резервные копии: созданные 24.11.1013, 26.11.2013 и 28.11.2013. Последние резервные копии находятся в папках [20] [20131128_132645Z] и [20] [20131128_132645Z] [R] соответственно.

Полная резервная копия (в [20] [20131128_132645Z]) содержит множество файлов с именами типа 0ea4ce4cc6e4ce70e34584423b6cfdf6fe87fa, а также всего четыре файла с читаемыми именами:

Info.plist
Manifest.mbdb
Manifest.plist
Status.plist

Это полная резервная копия в формате iTunes. Для просмотра содержимого рекомендуем использовать Elcomsoft Phone Viewer.

Преобразованные резервные копии выглядят логичнее, сохраняя полную структуру папок, а также имена файлов в файловой системе iOS. Большинство данных хранится в базах данных SQLite (.db и .sqlite) и файлах .plist; вы также получаете изображения в PNG и JPEG и т. д.

#### 3.2.4.2 Файлы в iCloud

##### 3.2.4.2.1 Скачивание файлов из iCloud

iCloud хранит файлы, используемые различными приложениями устройств iOS, вместе с другими данными, синхронизированными с iCloud. EPB позволяет скачивать и просматривать эти файлы. Чтобы скачать файлы из iCloud, сделайте следующее:

1. В меню **Tools/Инструменты** выберите вкладку **Apple**.

2. Выберите **Download files from iCloud/Скачать файлы из iCloud.**

3. Далее пройдите аутентификацию. Подробные инструкции даны в разделе **Скачивание резервных копий из iCloud**

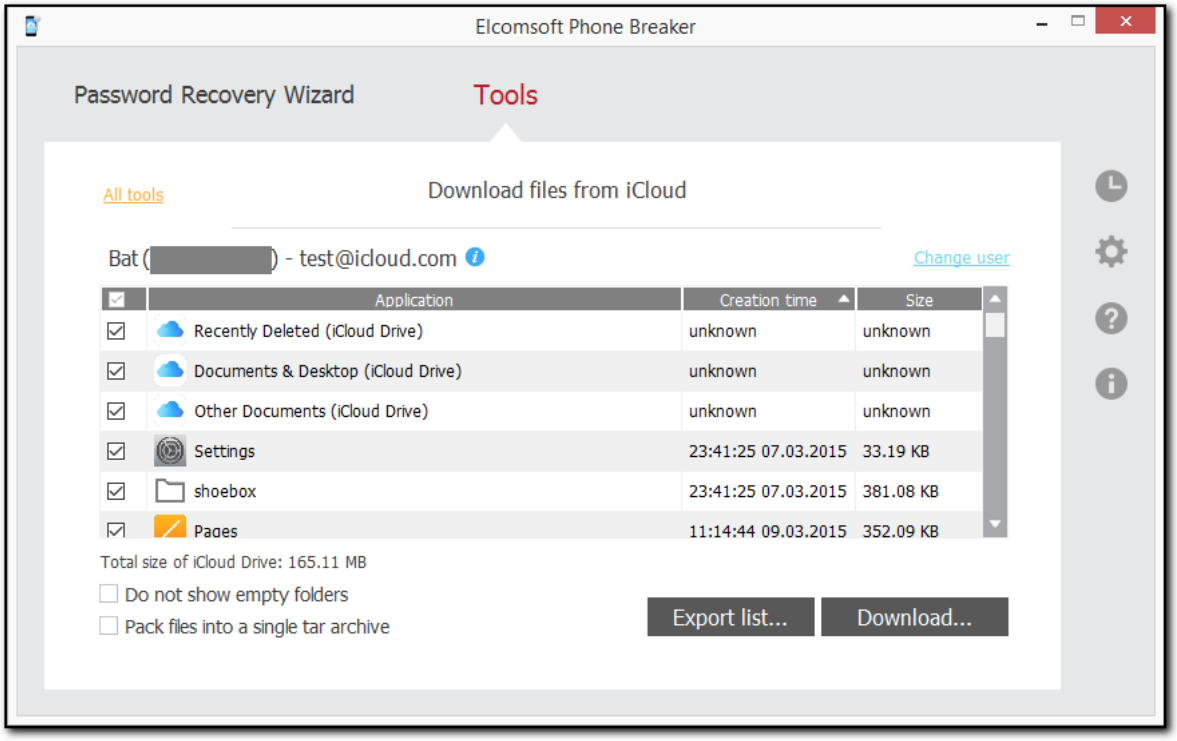
4. Открывается окно со списком доступных файлов. В доступных колонках приводятся данные о приложении, которым был создан файл, времени создания и размере файла или папки.

- Recently Deleted (iCloud Drive): файлы, которые были недавно удалены.
- Documents & Desktop/ (iCloud Drive): содержит папки и файлы из папок Desktop и Documents в iCloud Drive.
- Other Documents (iCloud Drive): прочие файлы из iCloud Drive.

**ПРИМЕЧАНИЕ. Файлы и папки, недоступные для загрузки в текущей версии EPB, отключены и не могут быть выбраны.**

Наведите указатель мыши на значок , чтобы просмотреть объем хранилища и используемый размер.

Чтобы выбрать файлы, созданные другим пользователем iCloud, нажмите **Change user/Заменить пользователя.**




Поддерживаются следующие типы файлов:

- Обычные файлы
- Бандлы iWorks
- Прочие бандлы

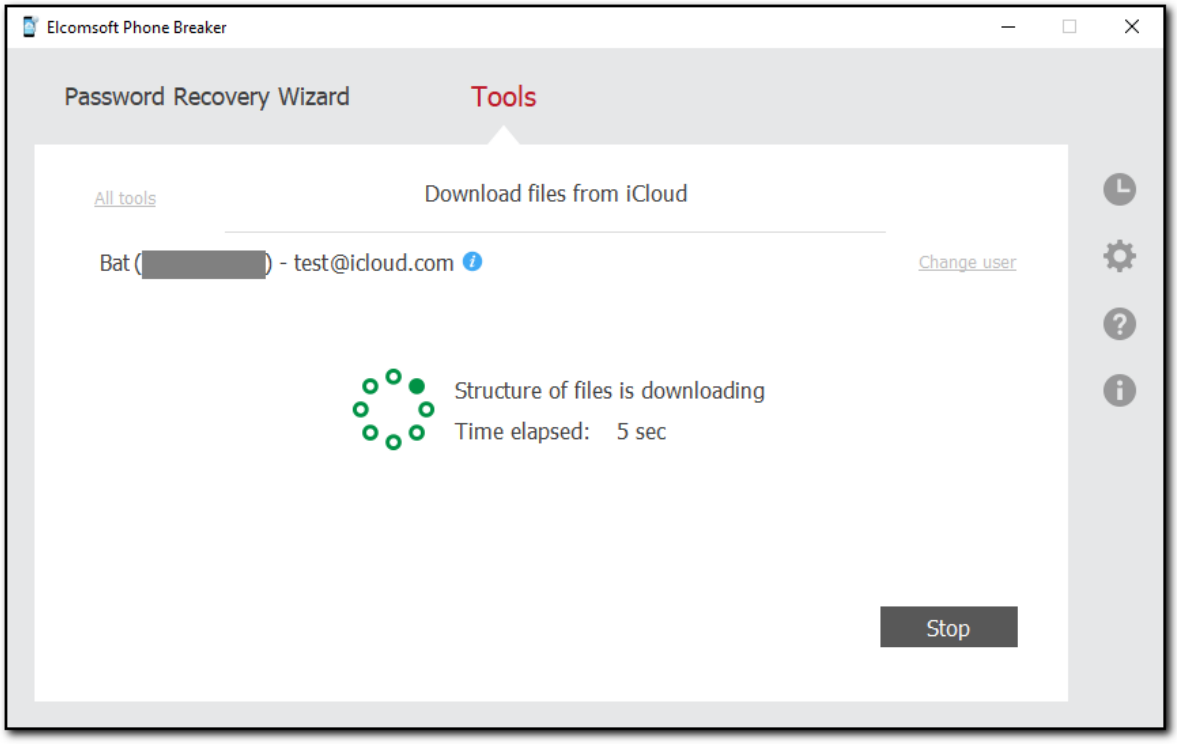
5. Выберите папки и файлы, которые вы хотите загрузить, установив флажки слева. Файлы будут сохранены в оригинальных форматах.

6. Вы можете упаковать все файлы в архив в формате .tar. Для этого выберите опцию **Pack files into a single tar archive/Сохранить файлы в единый архив формата tar.**

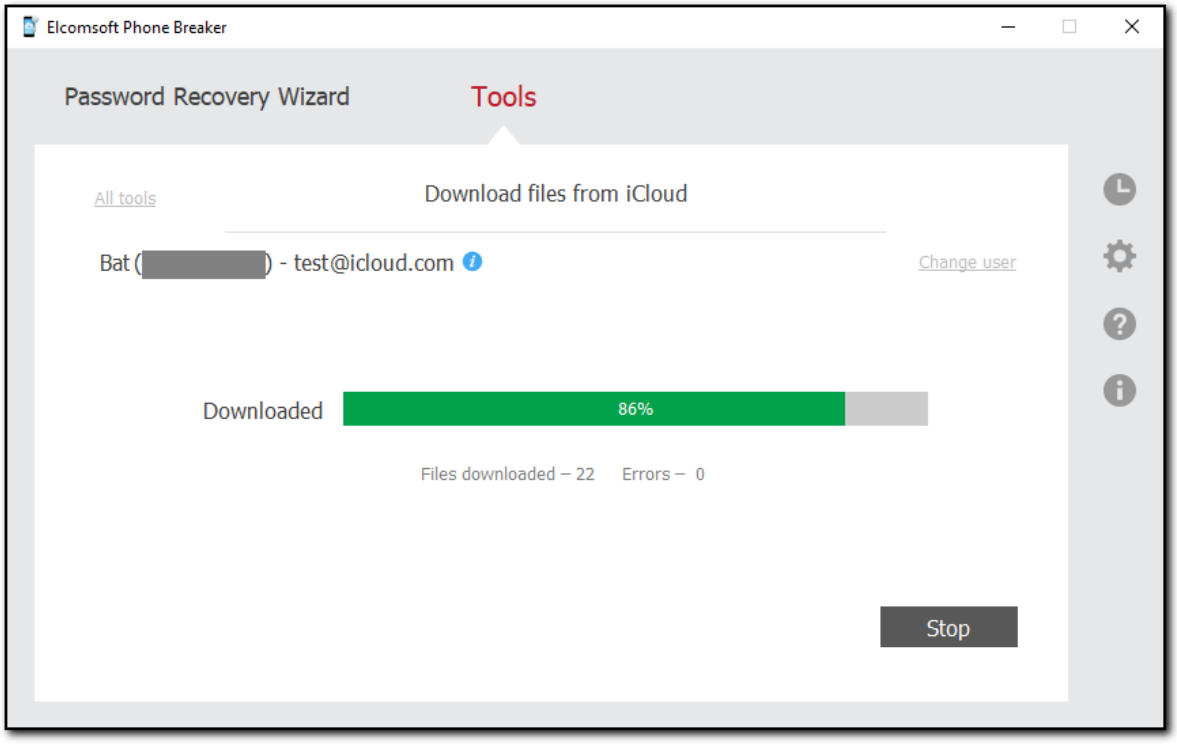
7. Нажмите **Download/Скачать**.

8. Выберите путь на диске для сохранения загруженных данных.

9. Начнется загрузка структуры файлов. На загрузку структуры файлов потребуется время.




10. После загрузки структуры файлов начинается процесс загрузки файлов из iCloud.



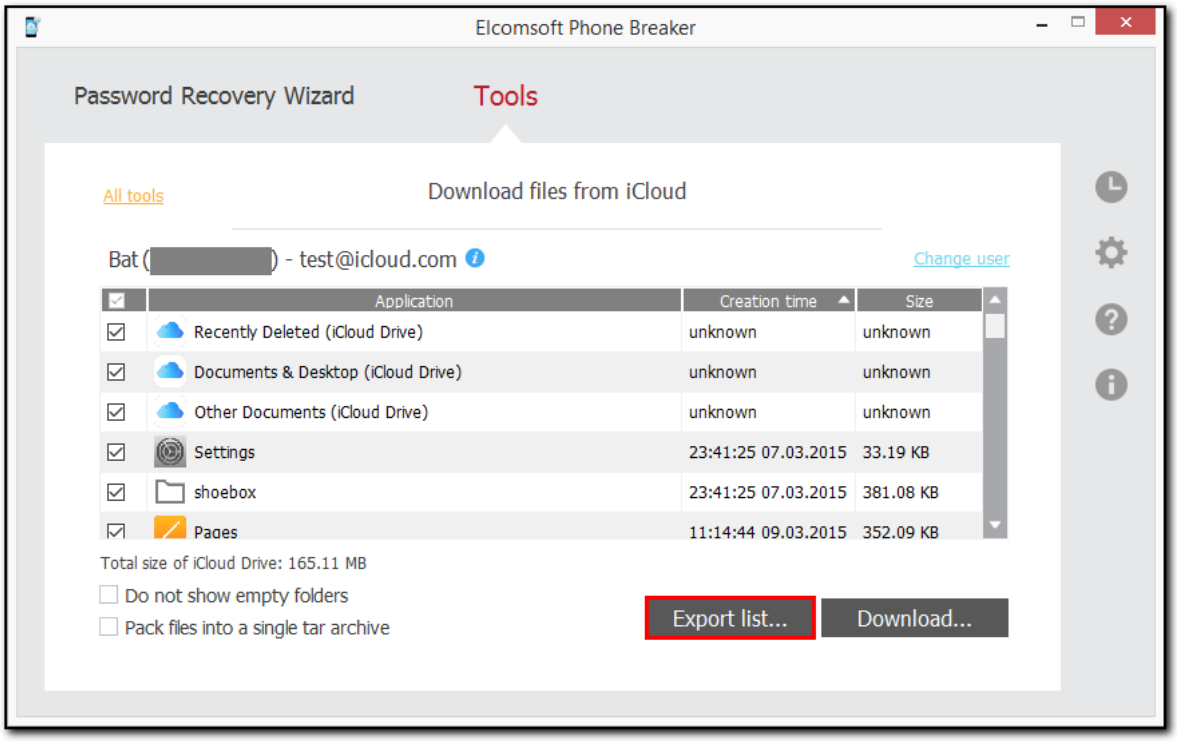

11. Нажмите **Finish/Завершить** для того, чтобы выйти из мастера.

#### 3.2.4.2.2 Экспорт списка файлов в iCloud

EPB позволяет экспортировать список файлов, которые находятся в учётной записи iCloud пользователя, в формат XML.

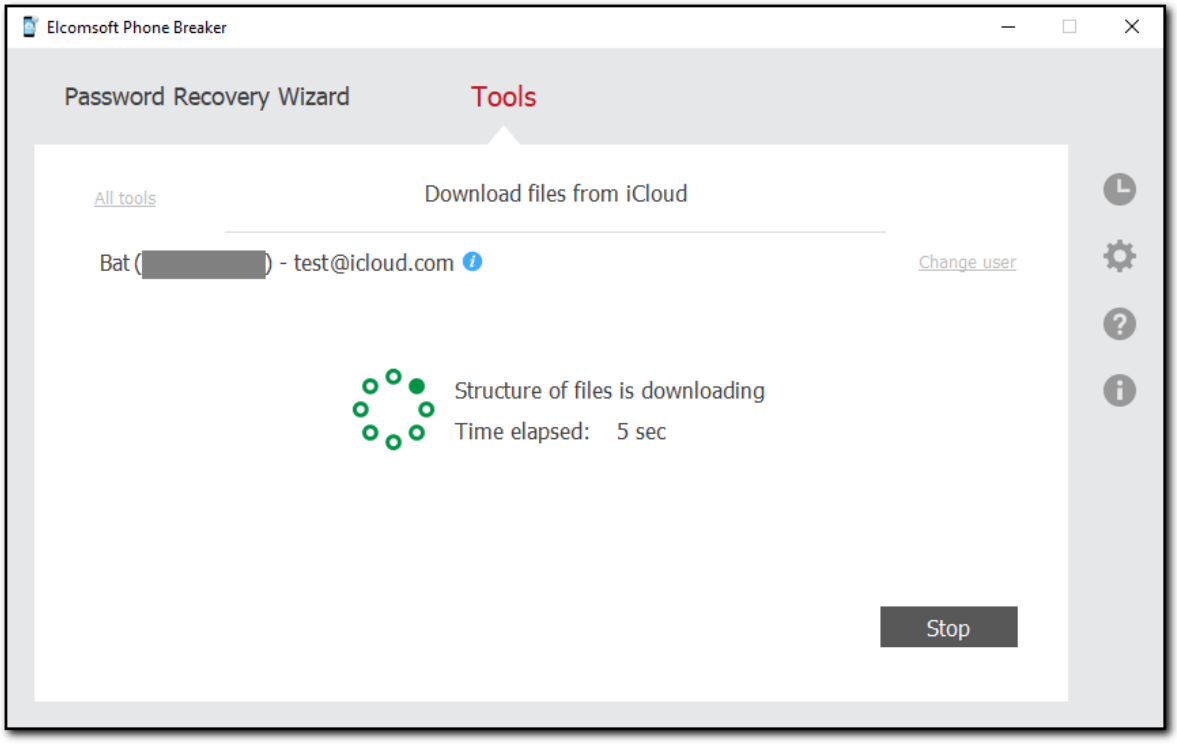
Чтобы экспортировать список файлов в iCloud, сделайте следующее:

1. Нажмите **Export List/Экспортировать список**.




2. Выберите место на диске, куда будет сохраняться файл XML.

3. Программа начнёт операцию экспортирования.




4. По окончании работы нажмите **Finish/Завершить**.

5. Список экспортирован. Информация о каждом файле содержит имя файла, путь к файлу, размер файла в байтах и отметку времени, которая указывает дату и время последней модификации файла.

### 3.2.4.3 Скачивание синхронизированных данных из iCloud

EPB позволяет загружать данные, которые синхронизируются с учетной записью iCloud. Затем эти данные можно просмотреть на вашем компьютере или в Elcomsoft Phone Viewer.

Для скачивания доступны следующие категории:

- Информация об учётной записи
- Карты Apple
- Календарь
- Звонки
- Контакты
- Токен FileVault2
- Здоровье
- Books
- Связка ключей
- Сообщения
- Заметки
- Фотографии
- Данные Safari
- Экранное время
- Голосовые заметки
- Wallet

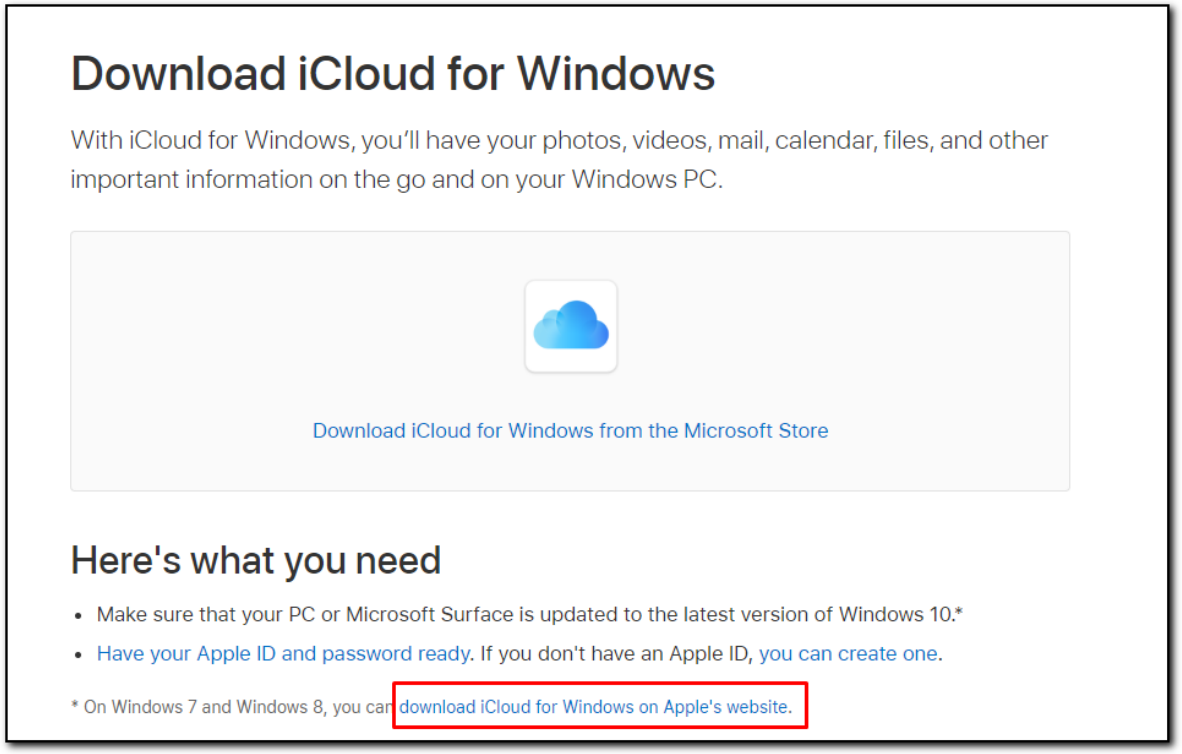
- Wi-Fi

**Требования к системе**

**1**. Для извлечения Связки ключей:

Для **macOS**, требуется macOS 10.12 или новее.

**2**. Для скачивания фотографий установите последнюю версию iCloud for Windows с сайта Apple (https://support.apple.com/ru-ru/HT204283):

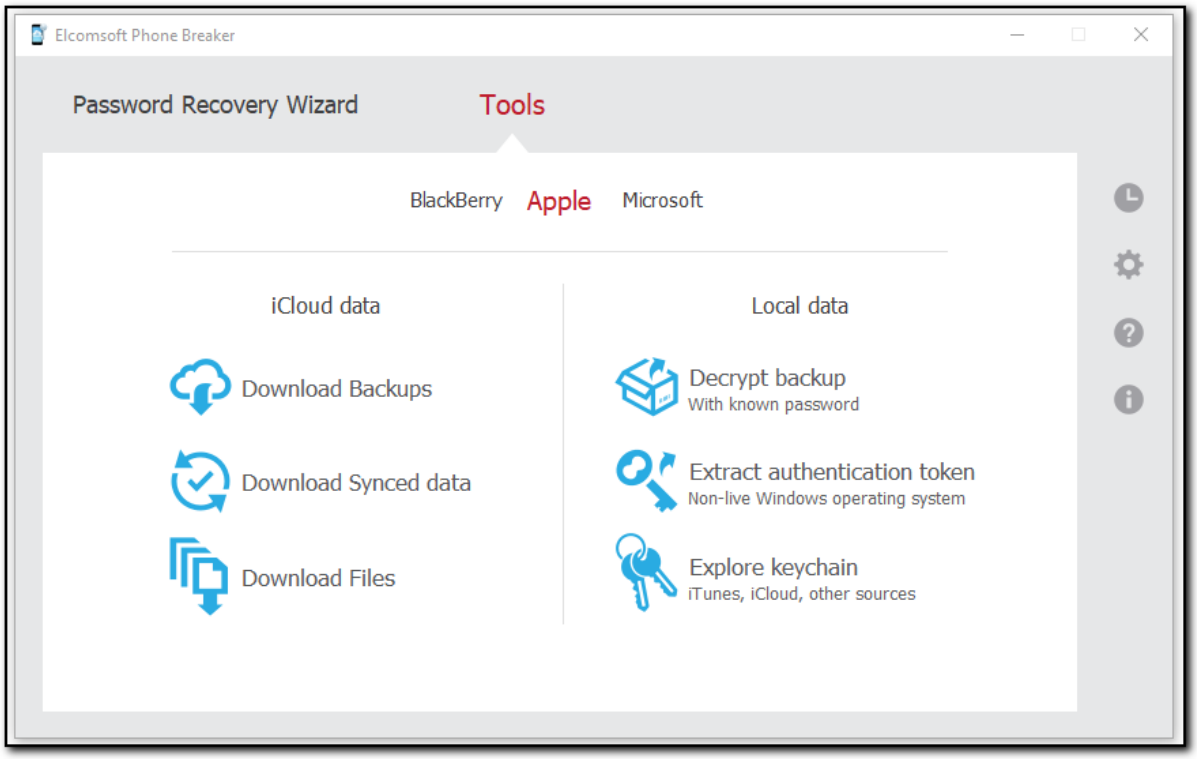



**ПРИМЕЧАНИЕ. Версия iCloud для Windows из Microsoft Store не поддерживается.**

**Для скачивания синхронизированных данных** проделайте следующие шаги:

1. В меню **Tools/Инструменты** выберите вкладку **Apple**.

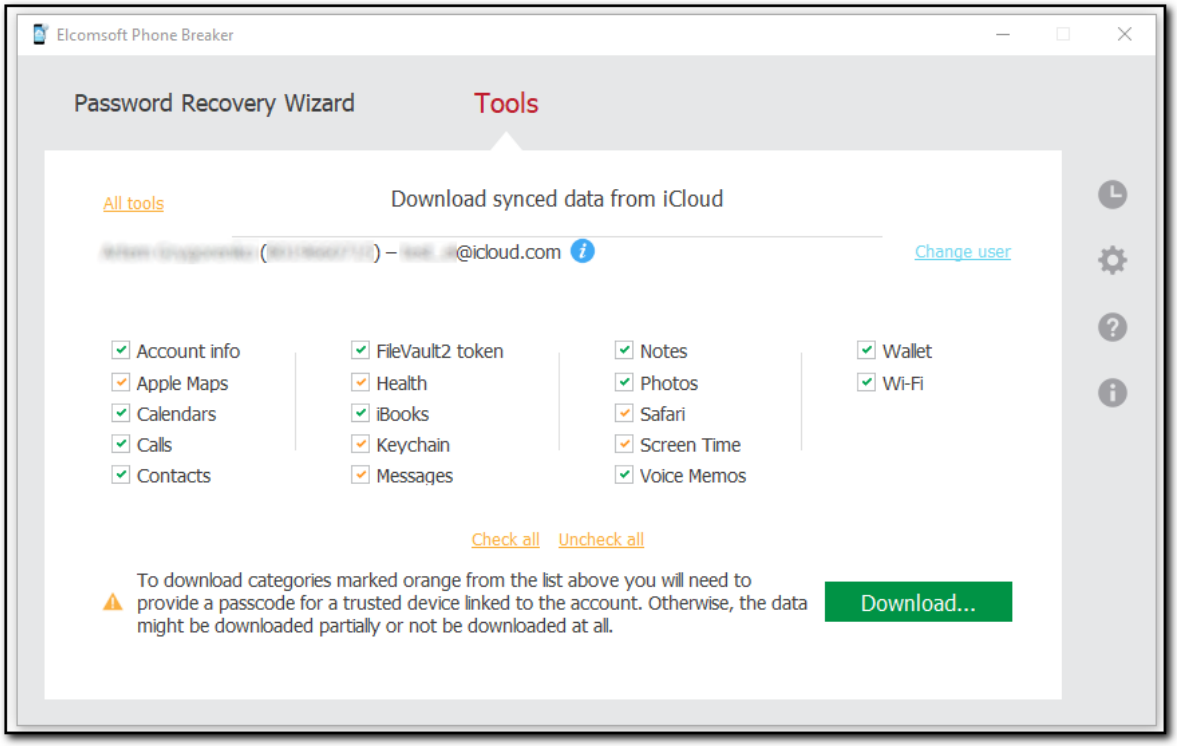
2. Выберите **Download Synced data/Скачать синхронизированные данные**.




3. Пройдите аутентификацию. Подробные инструкции - в разделе Скачивание резервных копий.

4. После успешной авторизации будет выведена информация об имени пользователя, DSID и Apple ID.

**ПРИМЕЧАНИЕ. Чтобы загрузить синхронизированные данные для другого пользователя, нажмите «Change user/Заменить пользователя».**




10. Выберите категории для скачивания и нажмите **Download/Скачать**.

    Обратите внимания на ограничения, связанные со скачиванием следующих категорий: **Account info/Учетная запись**, **Messages/Сообщения**, **Health/Здоровье**, **Screen Time/Экранное Время, Voice Memos/Диктофон**, **Safari** и **Apple Maps/Карты Apple**:

| Категория | Двухфакторная аутентификация | Без двухфакторной аутентификации | Доступ с маркером аутентификации |
|---|---|---|---|
| **Account info** | ✓ | ✓ | – |
| **Messages** | ✓ | – | – |
| **Health** | ✓ | ✓ | Частично (только незашифрованные контейнеры) |
| **Screen Time** | ✓ | – | – |
| **Voice Memos** | ✓ | – | – |
| **Apple Maps** | ✓ | ✓ | Частично (только незашифрованные контейнеры) |
| **Safari** | ✓ | ✓ | Частично (только незашифрованные контейнеры) |

**ПРИМЕЧАНИЕ. Карты Apple Maps (с устройств под управлением iOS 13 и более поздних версий), информация об учетной записи, сообщения, состояние, время экрана, защищенные данные Safari и данные голосовых заметок доступны для загрузки только в редакции Forensic.**

**ПРИМЕЧАНИЕ. Данные Apple Maps с устройств под управлением iOS 13 и более поздних версий можно загрузить только из учетных записей iCloud с двухфакторной аутентификацией после ввода пароля.**

Категория **Messages/Сообщения** содержит сообщения SMS и iMessage, синхронизированные со следующих версий iOS:

- iOS 11.4 и новее
- macOS 10.13.15 и новее

**ПРИМЕЧАНИЕ. При загрузке данных для категорий, отмеченных оранжевым, ключи дешифрования могут стать недействительными или могут не быть сгенерированы в среде, которая поддерживает эти категории данных в iCloud, и данные могут не быть загружены. Убедитесь, что вы вошли в систему с Apple ID на устройстве с последней версией iOS или macOS. Попробуйте выйти и войти в iCloud на устройстве, а затем выключите и снова включите Связку ключей iCloud. Затем попробуйте загрузить сообщения еще раз. Вы также можете попробовать использовать другое доверенное устройство.**

Начиная с версии EPB 6.40, загруженные данные истории Safari включают статус ссылки (актуальный или удаленный) и дату удаления для удаленных записей, которые можно просмотреть в EPV после загрузки. **Доступны данные за последние две недели**.

В категории **Calls/Звонки** доступна информация о звонках за последний месяц.

**ПРИМЕЧАНИЕ. Мы обнаружили, что в свежих версиях iOS синхронизация звонков с облаком может не происходить в рамках политики Apple по синхронизации данных.**

В категорию **Screen Time/Экранное Время** попадает информация с устройств под управлением iOS 12 и новее.

В категории **Voice Memos/Диктофон** содержатся голосовые заметки, которые синхронизируются устройствами под управлением следующих версий ОС:

- iOS 12.x.x и новее
- macOS 10.14 и новее

11. В окне **Select path to download synchronized data/Выбрать путь для скачивания синхронизированных данных** выберите папку для скачивания нажатием **Select Folder/Выбрать папку**.

12. (Только для старых версий iOS) Для старых версий iOS и учётных записей без двухфакторной аутентификации для доступа к категории **Keychain/Связка ключей** вам потребуется ввести **iCloud Security Code/Код безопасности iCloud**, который был создан пользователем в момент первой синхронизации.

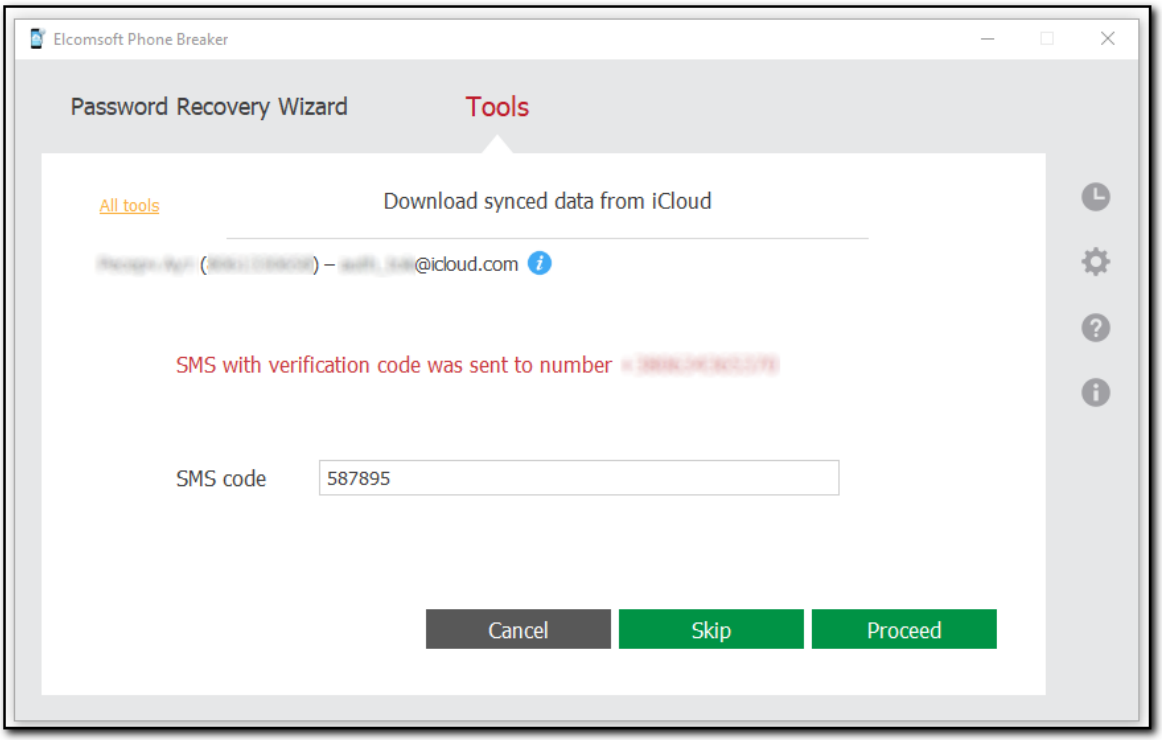
**ПРИМЕЧАНИЕ. В современных условиях iCloud Security Code/Код безопасности iCloud не используется.**

13. (Только для старых версий iOS) Введите код безопасности **iCloud Security Code** и нажмите **Check/Проверить**. SMS-сообщение с кодом подтверждения будет отправлено на номер телефона, с которым связана Связка ключей iCloud.

**ПРИМЕЧАНИЕ. Если вы введете неправильный код безопасности iCloud слишком много раз, ваш доступ к Связке ключей iCloud будет временно заблокирован. Чтобы разблокировать его, вы можете обратиться в службу поддержки Apple. После того как вы разблокируете доступ к Связке ключей iCloud, будьте очень осторожны, вводя правильный код безопасности iCloud. Если вы**

**снова введете его неправильно после того, как ваш доступ к Связке ключей iCloud был разблокирован, данные Связки ключей iCloud будут удалены.**

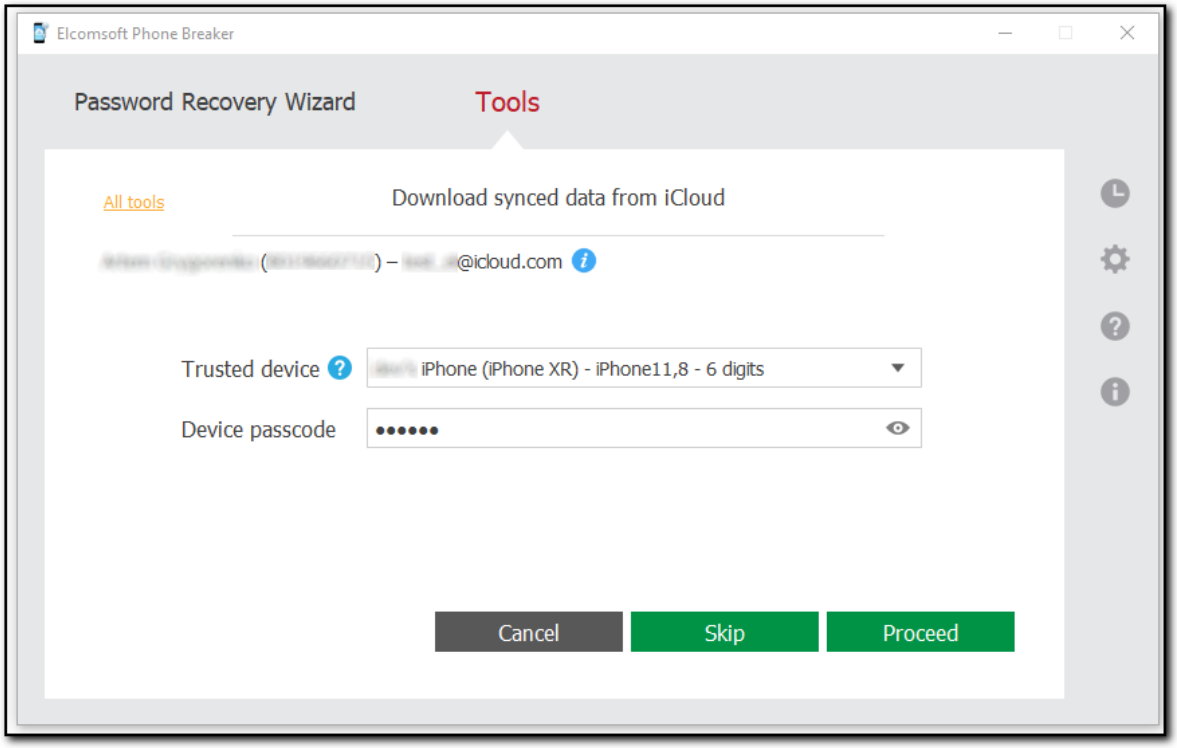
14. (Только для старых версий iOS) Введите полученный в виде SMS код, который был отправлен на предыдущем шаге, и нажмите **Proceed/Продолжить**.



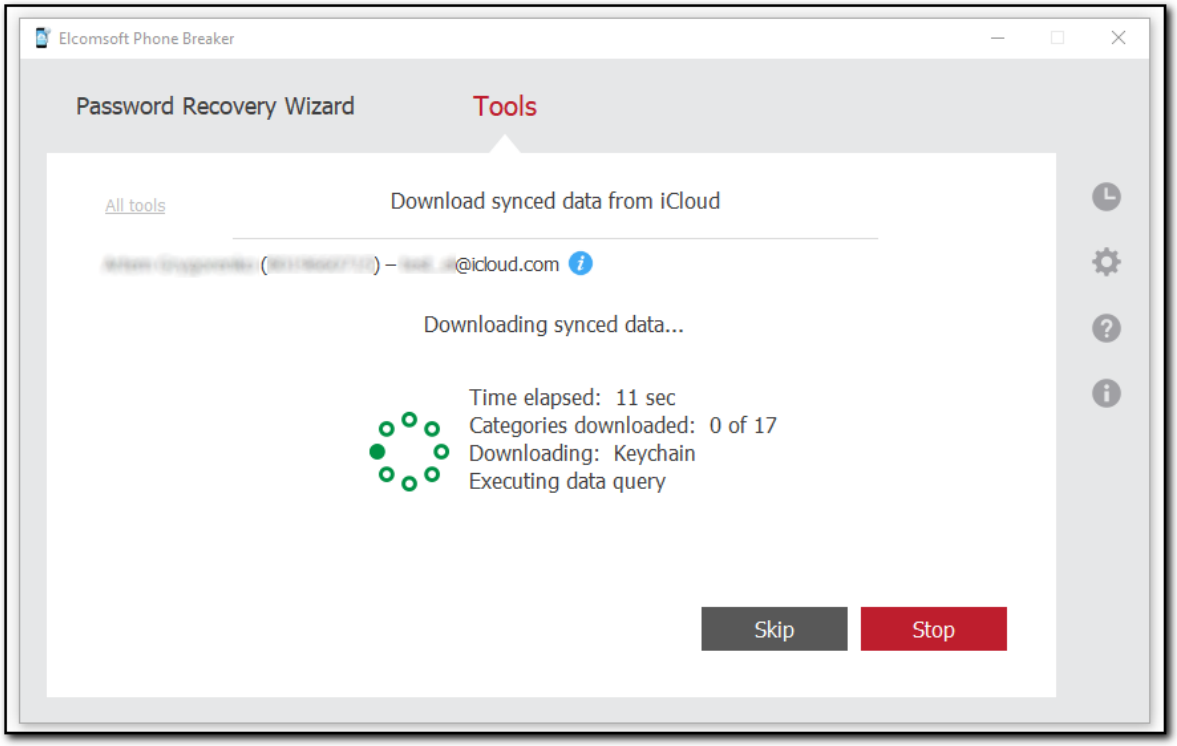

15. Если вы выбрали категории, помеченные оранжевым, для учетной записи с активированной двухфакторной аутентификацией, выберите доверенное устройство и введите пароль (для iOS) или пароль для учетной записи пользователя в операционной системе (для macOS).

**ПРИМЕЧАНИЕ. Если вы не предоставите пароль, данные могут быть загружены частично или не загружены вообще.**

**ПРИМЕЧАНИЕ. Если вы введете неправильный пароль устройства 10 раз, устройство будет заблокировано в EPB. Это не повлияет на само устройство, но вы не сможете использовать его для загрузки данных в EPB. Чтобы разблокировать устройство, вам необходимо изменить его пароль, подтвердить его и снова синхронизировать Связку ключей iCloud с этим устройством. Вы также можете загружать данные, используя другое доверенное устройство и его пароль.**



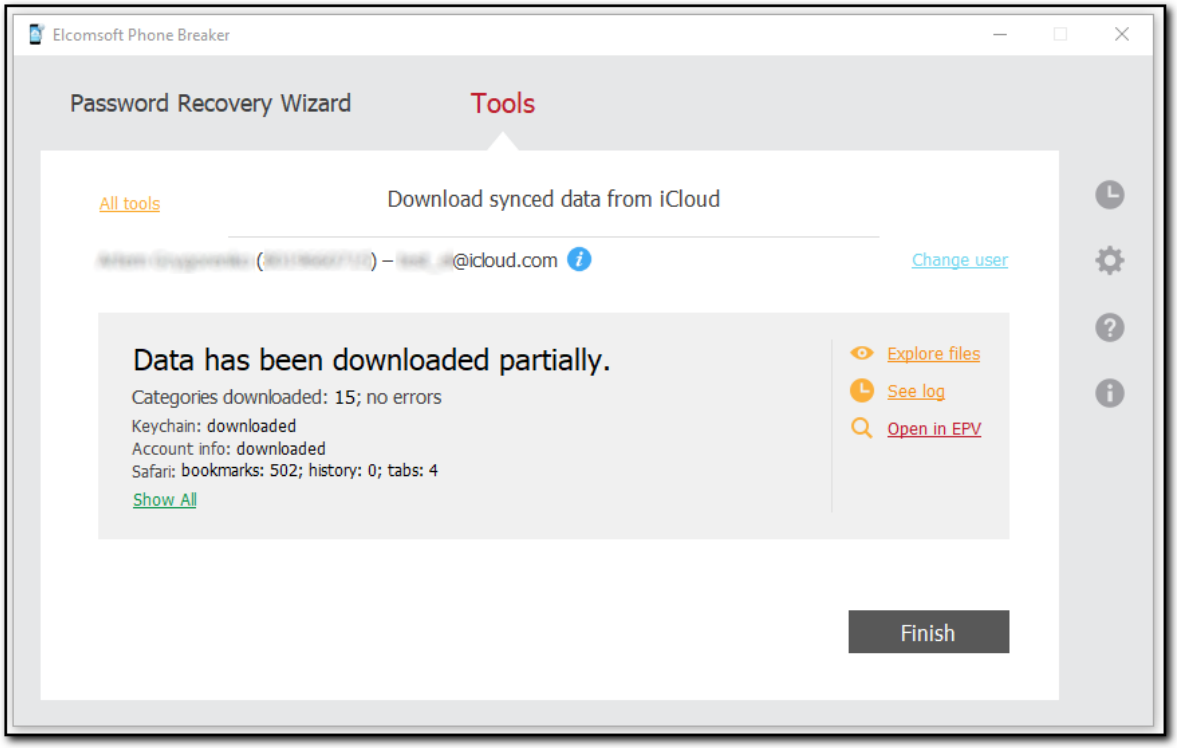

16. Щелкните **Proceed/Продолжить**. Начнется процесс загрузки синхронизированных данных из iCloud. Прогресс отображается в окне программы. Чтобы пропустить загрузку текущей категории, нажмите **Skip/Пропустить**. Чтобы остановить процесс загрузки, нажмите **Stop/Остановить**. (Файлы, загруженные до остановки, доступны для анализа.)




17. Когда загрузка будет завершена, вы увидите следующую информацию:

- Количество загруженных категорий и статус загрузки (без ошибок или с ошибками).
- Количество записей для скачанных категорий.
- Для категорий **Calendars/Календари**, **Calls/Звонки, Apple Maps/Карты Apple, Wi-Fi, Messages/Сообщения, Health/Здоровье, Screen Time/Экранное время** и **Notes/Записи** доступен диапазон дат (от самой ранней до последней записи).

**ПРИМЕЧАНИЕ. Пробная версия Elcomsoft Phone Breaker позволяет загружать только 10 последних звонков, заметки, точки доступа Wi-Fi, избранные в Apple Maps и историю поисковых запросов, а также записи истории Safari.**




Доступны следующие действия:

- **Explore files/Просматривать файлы** - открывает папку со скачанными данными.
- **See log/Смотреть журнал** - открывает журнал сообщений об ошибках в процессе скачивания.
- **Open in EPV/Открыть в EPV** - открывает данные в Elcomsoft Phone Viewer.

**ПРИМЕЧАНИЕ. Эта опция доступна, только если у вас установлен Elcomsoft Phone Viewer 3.10 или более поздняя версия.**

- **Change user/Выбрать др. пользователя** - переключение на другой Apple ID.
- **All tools/Все инструменты** - возврат в окно команд для устройств Apple.
- **Finish/Завершить** - выход из мастера скачивания.

### Просмотр загруженных синхронизированных данных iCloud

Вы можете просматривать загруженные синхронизированные данные iCloud с помощью Elcomsoft Phone Viewer. Для этого нажмите **Open in EPV/Открыть в EPV**.

Вы также можете просмотреть содержимое папки синхронизированных данных iCloud на вашем компьютере. По умолчанию данные скачиваются в папку **iCloud_sync_<apple_id>_<time stamp>**.

**ПРИМЕЧАНИЕ. Отметка времени в имени папки с синхронизированным iCloud соответствует часовому поясу локального компьютера.**

Содержимое папки **iCloud_sync_<apple_id>_<time stamp>**:

- **Account Info** - файлы, относящиеся к данным учётной записи пользователя.
- **AppleMaps** - файл **AppleMaps.db** (база данных Apple Maps).
- **Calendars** - файл **Calendars.db** (база данных календарей).
- **Calls** - файл **calls.db** (база данных звонков).
- **Contacts**:
  - **Contacts.db** - база данных адресной книги.
  - **Vcards** подпапка с карточками контактов.

  **ПРИМЕЧАНИЕ: группы vCards считаются в числе загруженных контактов в EPB. Следовательно, количество контактов, отображаемых в EPB, может быть больше, чем количество контактов, отображаемых в EPV.**
- **FileVault** - файл **filevault2_token.xml** с ключом восстановления зашифрованных дисков macOS в Elcomsoft Forensic Disk Decryptor.
- **Health** - файлы **healthdb.db, healthdb_secure.db, locations.db** и т.п.
- **iBooks** - список скачанных книг.
- **Keychain** - файл Связки ключей **keychain.data**.
- **Messages** - файл **Messages.db** (атрибуты сообщений) и **Attachments** (вложения).
- **Notes** - заметки и атрибуты в файле **Notes.db**.
- **Photos**:
  - **All Photos folder**: папка, в которую были загружены медиафайлы из всех альбомов.
  - **Photos.db**: база данных, в которой хранятся атрибуты медиафайлов.

**ПРИМЕЧАНИЕ. Имена фотографий в папке соответствуют их идентификаторам в iCloud.**

- **Safari** - файл **Safari.db** (база данных, в которой хранятся записи Safari).
- **ScreenTime** - база данных с записями Экранного времени **ScreenTime.db**.
- **VoiceMemos** - список аудиозаписей и база данных **VoiceMemos.db**
- **Wallet** - файлы, имеющие отношение к кошельку Apple Wallet
- **Wifi** - база данных **Wifi.db**
- **CardPhoto.jpg** - изображение владельца учётной записи.
- **icloud_synced.xml** файл, содержащий информацию об Apple ID, времени начала и окончания загрузки и статусе загрузки (успешная, отменена, завершена с ошибками).

### Просмотр загруженных данных Связки ключей iCloud

Вы можете изучить загруженные данные Связки ключей iCloud с помощью Keychain explorer. Перейдите в папку синхронизированных данных с данными связки ключей и откройте файл **icloud_synced.xml** в корне этой папки.

**ПРИМЕЧАНИЕ. Если вы используете EPB 9.50 или более раннюю версию, перейдите в папку с данными Связки ключей iCloud (с именем в следующем формате: iCloud_keychain_account@icloud.com_YYYY.MM.DD_HH-MM-SS) и откройте файл icloud_keychain.xml в корне этой папки.**

## 3.2.5 Маркеры аутентификации iCloud

### 3.2.5.1 Маркеры аутентификации

iCloud позволяет пользователям хранить информацию в облаке. Пользователи macOS могут получить доступ к iCloud без какого-либо дополнительного программного обеспечения, поскольку оно встроено в операционную систему (для iCloud требуется macOS 10.7.2 или новее).

Пользователи iOS могут получить доступ к своим данным и в Windows. В этом случае обмен данными между устройствами iOS и компьютером осуществляется через отдельное приложение iCloud for Windows (доступно для Windows 7 или новее). Это приложение позволяет пользователю работать с данными из iOS на компьютере с Windows.

EPB позволяет извлекать из компьютера пользователя маркер аутентификации, который в некоторых случаях может заменить собой логин и пароль в iCloud. Извлечение маркера аутентификации доступно как в macOS, так и в Windows. Также можно получить маркер аутентификации без входа в фактическую ОС, в которой этот маркер использовался (например, путем подключения образа диска к текущей системе).

**Доступны следующие способы извлечения**

| Operating system | System type | Ways of extraction |
|---|---|---|
| Windows | Система с активной пользовательской сессией | Утилита командной строки (atex.exe). |
| | Диск с системой или образ диска | EPB GUI |
| macOS | Система с активной пользовательской сессией | Утилита командной строки (atex.dmg). |
| | Диск с системой или образ диска | EPB GUI |

**Типы маркеров аутентификации:**

| | iCloud for Windows до v. 7.0 | iCloud for Windows v. 7.0 и новее | macOS до 10.13 | macOS 10.13 и новее |
|---|---|---|---|---|
| Учётная запись с двухфакторной аутентификацией | Маркер аутентификации без ограничений | Маркер аутентификации с ограничениями | Маркер аутентификации без ограничений | Маркер аутентификации с ограничениями |
| Учётная запись без двухфакторной аутентификации | Маркер аутентификации для учётной записи без | Маркер аутентификации для учётной записи без | Маркер аутентификации для учётной записи без | Маркер аутентификации для учётной записи без |

| | | | | |
|---|---|---|---|---|
| | двухфакторной аутентификации | двухфакторной аутентификации | двухфакторной аутентификации | двухфакторной аутентификации |

**Маркеры аутентификации, поддерживаемые в Windows и macOS для загрузки данных через EPB:**

| | Маркер аутентификации без ограничений для учётной записи с двухфакторной аутентификацией | Маркер аутентификации с ограничениями для учётной записи с двухфакторной аутентификацией | Маркер аутентификации для учётной записи без двухфакторной аутентификации |
|---|---|---|---|
| Windows OS | Поддерживается | Не поддерживается | Поддерживается |
| macOS | Поддерживается | Поддерживается | Поддерживается |

**ПРИМЕЧАНИЕ. Маркер аутентификации с ограничениями для учетной записи с двухфакторной аутентификацией действителен только в том случае, если он был извлечен на том же компьютере и под и тем же пользователем, из-под учётной записи которого запущен EPB.**

#### 3.2.5.2 Извлечение маркера аутентификации: Windows

##### 3.2.5.2.1 Извлечение маркера аутентификации: Windows, система с активной пользовательской сесси

Вы можете войти в учетную запись iCloud, не используя логин и пароль. Вместо них можно использовать маркер аутентификации iCloud.

Чтобы извлечь маркер из **текущей системы с активной пользовательской сессией**, вам понадобится **Elcomsoft Apple Token Extractor** для Windows. Этот инструмент поставляется вместе с EPB (файл **atex.exe**). Вы можете найти его в папке установки EPB. Не рекомендуется запускать atex.exe из установочной папки EPB, поскольку может не хватить прав для выполнения извлечения маркера. Скопируйте файл в папку, в которой вы хотите создать файл с маркером аутентификации.

EPB позволяет извлекать маркеры аутентификации для:

- Текущий пользователь iCloud в Windows
- Другие пользователи Windows, использующие iCloud for Windows на данном компьютере
- Пользователи систем, для которых доступен только диск либо его образ (образ необходимо смонтировать на текущем компьютере)

**ПРИМЕЧАНИЕ. Для маркеров, извлеченных с помощью iCloud для Windows 7.3 или новее, для учетных записей с двухфакторной аутентификацией существуют следующие ограничения:**

- **Маркер нельзя использовать для загрузки резервных копий iCloud.**
- **Маркер действителен только в том случае, если он был извлечен на текущем компьютере и пользователь не вышел из iCloud.**

**Системные разрешения, необходимые для доступа к маркерам аутентификации:**

| Маркер аутентификации | Требуемые разрешения |
|---|---|
| Учетная запись iCloud текущего пользователя Windows | Достаточно прав пользователя |
| Учетная запись iCloud другого пользователя Windows | atex.exe необходимо запустить от административного пользователя (если включен UAC) |

**ПРИМЕЧАНИЕ. Когда вы запускаете atex.exe из системной папки или из папки, для изменения которой у вас недостаточно прав, может появиться сообщение Windows User Account Control с запросом разрешения на запуск этой программы.**

Чтобы извлечь токен аутентификации для текущего пользователя iCloud для Windows, выполните следующие действия:

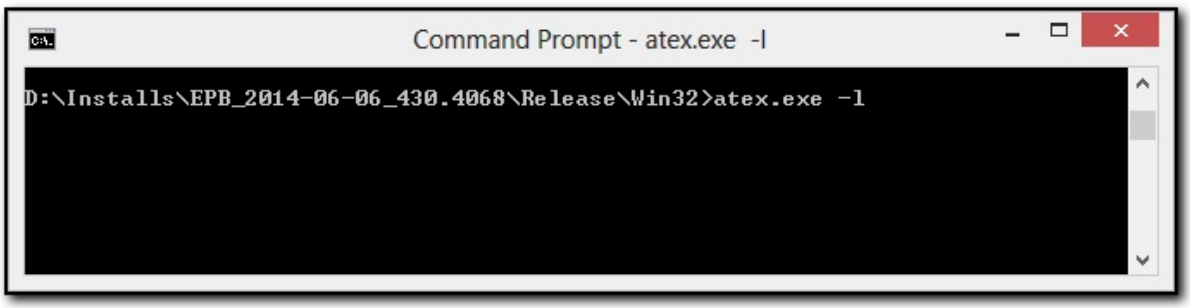
1. Запустите atex.exe. В папке, из которой была запущена утилита, будет создан файл **icloud_token_<timestamp>.txt** . Если у вас недостаточно прав для записи в эту папку, то файл будет создан в папке C:\Users\<имя_пользователя>\AppData\Local\Temp.

В открывшемся консольном окне вы увидите полный путь к файлу. Обратите внимание, что символы Unicode в пути к файлу не поддерживаются.

2. Созданный файл .txt содержит Apple ID текущего пользователя iCloud для Windows и его токен аутентификации.


Чтобы извлечь маркер аутентификации для **другого пользователя Windows**, помимо текущего, выполните следующие действия:

1. Откройте окно командной строки (запустив cmd.exe).
2. Перейдите в папку с файлом atex.exe.
3. Введите команду **atex.exe -l**




4. Выводится список всех пользователей iCloud.


5. Запустите atex.exe с параметром getToken и введите логин локального **пользователя Windows** и пароль для этой учетной записи в следующей форме: **atex.exe --getToken -n <username> -p <password>**

   **Например: atex.exe --getToken -n user1 -p 1234**

6. Будет создан файл "**icloud_token_<timestamp>.txt**" (в том же каталоге, где находится **atex.exe**).

Созданный файл .txt содержит Apple ID текущего пользователя iCloud для Windows и его маркер аутентификации.


**atex.exe - параметры командной строки:**

| **Параметр** | **Значение** |
|---|---|
| **-h** или **[--help]** | Отображает справочное сообщение |
| **-l** или **[--iCloudUserList]** | Отображает имена пользователей iCloud |
| **--getToken -n <username> -p <password>** | Извлекает маркер аутентификации для указанного пользователя. Имя пользователя и пароль следует вводить без скобок. |
| **-n** или **[--username]** | Имя пользователя. Имя пользователя следует вводить без скобок. |
| **-p** или **[--password]** | Пароль пользователя. Пароль следует вводить без скобок. |

#### 3.2.5.2.2 Извлечение маркера аутентификации: Windows, сторонний компьютер или образ диска

EPB позволяет извлекать маркер аутентификации iCloud из неактивной копии Windows, например, путем монтирования образа диска операционной системы, в которой хранится маркер.

**Чтобы извлечь маркер аутентификации iCloud, сделайте следующее:**

1. Смонтируйте образ диска, содержащий маркер аутентификации.

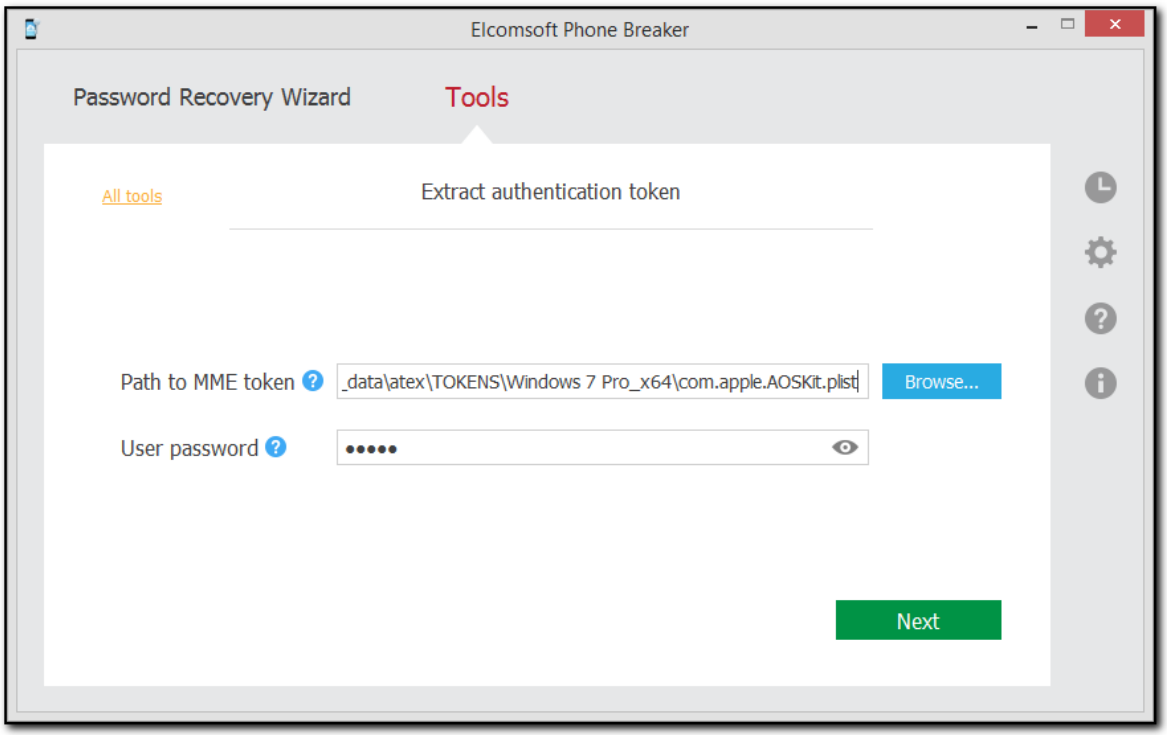
2. Запустите Elcomsoft Phone Breaker.

3. В меню **Tools/Инструменты** выберите вкладку **Apple**.

4. Нажмите **Extract authentication token/Извлечь маркер аутентификации.**

5. Укажите путь и пароль к файлу, содержащему маркер аутентификации:

   - **Path to MME token/Путь к токену**: Укажите путь к файлу **com.apple.AOSKit.plist**. Как правило, файл расположен в папке *%appdata%\Apple Computer\Preferences* в системе Windows.
   - **Password/Пароль**: Укажите пароль того пользователя Windows, маркер которого извлекается.



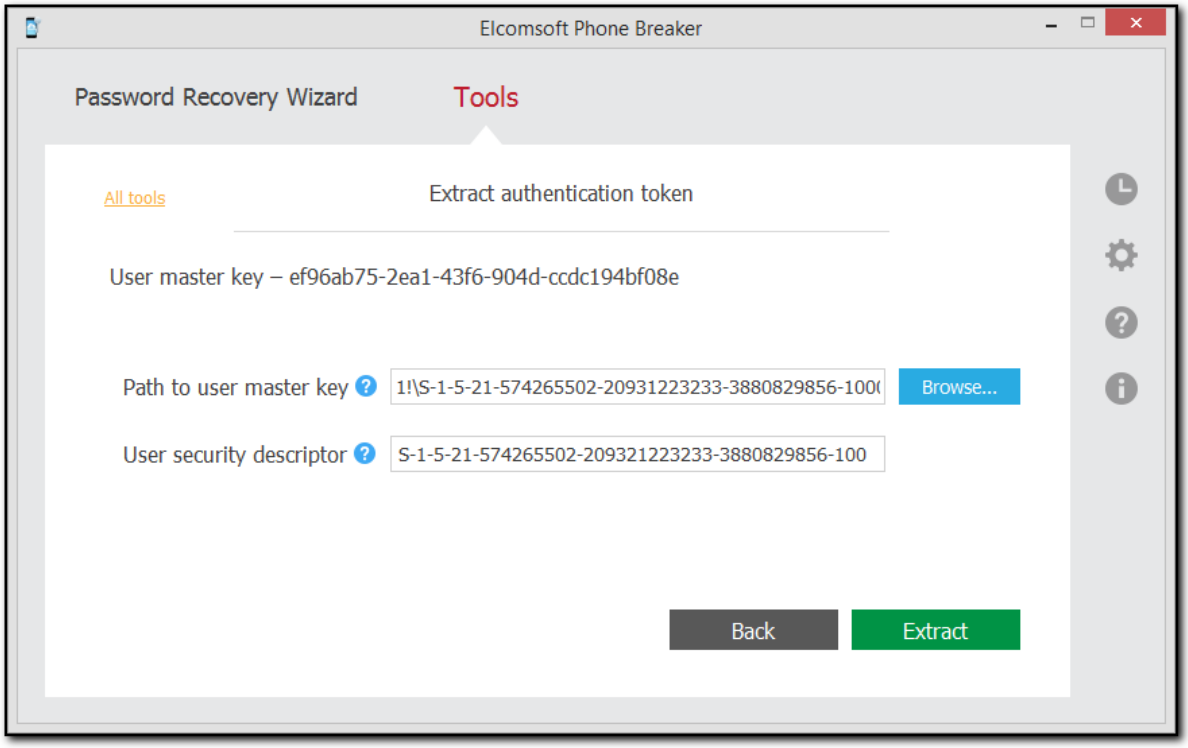

6. Нажмите **Next/Далее**.

7. На следующей странице укажите путь к файлу мастер-ключа пользователя и его SID. Сверху отображается сам мастер-ключ пользователя. Этот ключ используется для расшифровки маркера аутентификации.

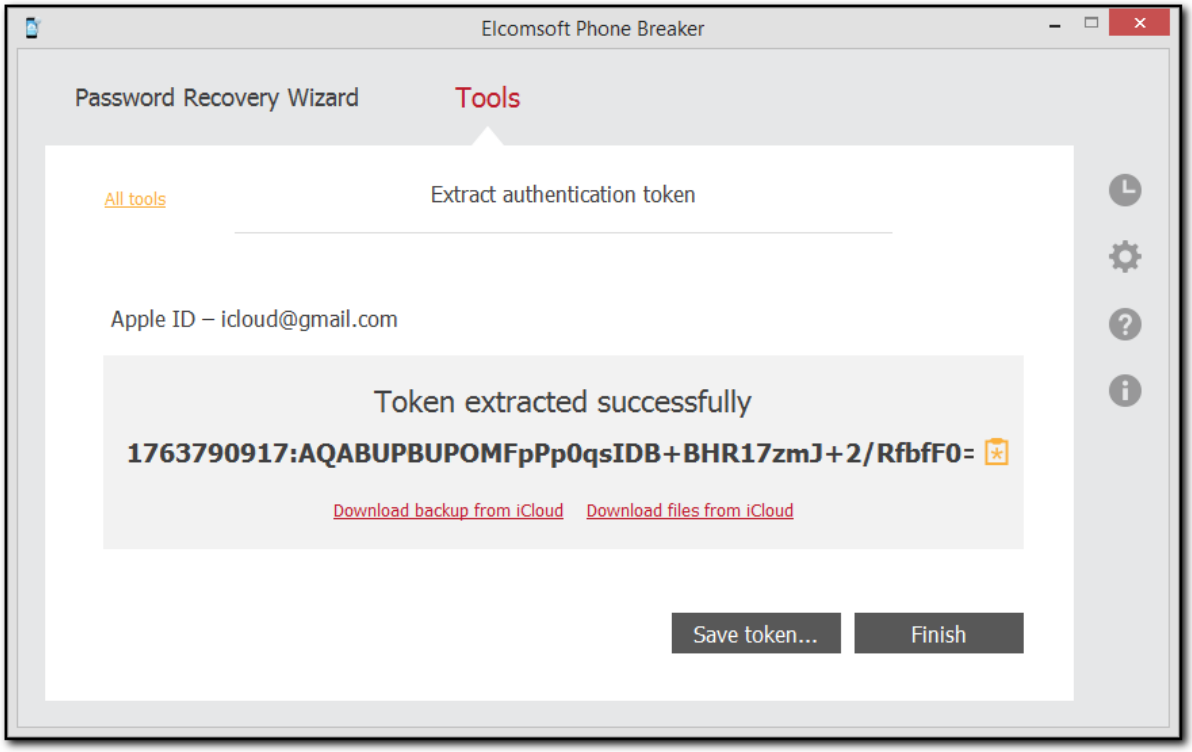
- **Path to user master key/Путь к мастер-ключу пользователя**: Укажите путь на диске к мастер-ключу. По умолчанию мастер-ключ хранится в папке %APPDATA% \Roaming\Microsoft\Protect\<SID>\.

  Обратите внимание, что эта папка обычно скрыта, поэтому вам нужно снять флажок Скрыть защищенные системные файлы (рекомендуется) в Панели управления Windows -> Folder Options -> View.

- **User security descriptor/Дескриптор безопасности пользователя**: Дескриптор безопасности пользователя обычно совпадает с именем папки, содержащей главный ключ пользователя; по умолчанию EPB заполняет это поле автоматически.




8. Нажмите **Extract/Извлечь**.
9. Маркер аутентификации извлекается.




Нажмите **Save token/Сохранить токен** для сохранения найденного маркера в текстовый файл.

Извлечённый маркер можно использовать для аутентификации в iCloud.

#### 3.2.5.3 Извлечение маркера аутентификации: macOS

##### 3.2.5.3.1 Извлечение маркера аутентификации: macOS, система с активной пользовательской сессией

Вы можете войти в учетную запись iCloud, не используя логин и пароль. Вместо них можно использовать маркер аутентификации iCloud.

Для извлечения маркера аутентификации iCloud вам понадобится Elcomsoft Apple Token Extractor для macOS. Этот инструмент поставляется вместе с EPB (файл **atex.dmg**). Вы можете найти его в папке установки EPB.

Elcomsoft Apple Token Extractor поддерживает macOS версий до 10.15.

EPB позволяет извлекать токены аутентификации для:

- Текущего пользователя iCloud
- Других пользователей iCloud
- С диска или образа системы

**Системные разрешения, необходимые для доступа к маркерам аутентификации:**

| Маркер аутентификации | Требуемые разрешения |
|---|---|
| Учетная запись iCloud текущего пользователя macOS | Достаточно прав пользователя |

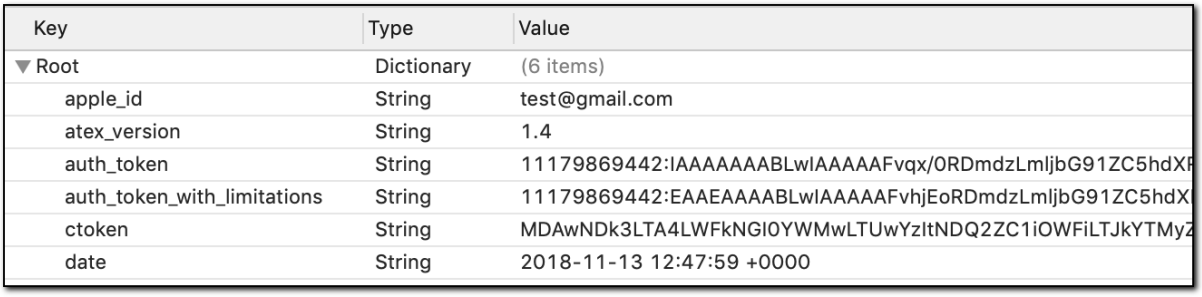
| | |
|---|---|
| Учетная запись iCloud другого пользователя macOS | Требуется **root**-доступ |

**Типы маркеров аутентификации, извлекаемых EPB:**

| | **macOS ниже 10.3** | **macOS 10.3 и выше** |
|---|---|---|
| Учётная запись с двухфакторной аутентификацией | Маркер аутентификации без ограничений | Маркер аутентификации с ограничениями |
| Учётная запись без двухфакторной аутентификации | Маркер аутентификации для учётной записи без двухфакторной аутентификации | Маркер аутентификации для учётной записи без двухфакторной аутентификации |

В файле "**icloud_token_<timestamp>.plist**", который создаётся по результатам извлечения, могут присутствовать следующие типы маркеров:

| **Тип маркера** | **Описание** |
|---|---|
| **auth_token** | **Маркер аутентификации** без ограничений |
| **auth_token_with_limitations** | **Маркер аутентификации** с ограничениями:<br>▪ Маркер нельзя использовать для загрузки резервных копий iCloud..<br>▪ Маркер действителен только в том случае, если он был извлечен на текущем компьютере и пользователь не вышел из iCloud. |
| **ctoken** | Так называемый **Continuation token**. В настоящее время не поддерживается EPB. |



| Key | Type | Value |
|---|---|---|
| ▼ Root | Dictionary | (6 items) |
| apple_id | String | test@gmail.com |
| atex_version | String | 1.4 |
| auth_token | String | 11179869442:IAAAAAAABLwIAAAAAFvqx/0RDmdzLmljbG91ZC5hdXP |
| auth_token_with_limitations | String | 11179869442:EAAEAAAABLwIAAAAAFvhjEoRDmdzLmljbG91ZC5hdX |
| ctoken | String | MDAwNDk3LTA4LWFkNGI0YWMwLTUwYzItNDQ2ZC1iOWFiLTJkYTMyZ |
| date | String | 2018-11-13 12:47:59 +0000 |

Чтобы извлечь маркер аутентификации для текущего пользователя iCloud, выполните следующие действия:

1. Запустите файл atex.dmg.

*ПРИМЕЧАНИЕ. Если Elcomsoft Apple Token Extractor не открывается, см. Подробную информацию в разделе «Устранение неполадок».*

2. Скопируйте файл **atex** из смонтированного образа в папку, в которой вы хотите сохранить файл с токеном аутентификации.

3. Откройте папку с файлом **atex**.

4. Запустите файл **atex**. Будет создан файл "**icloud_token_<timestamp>.plist**", который сохраняется в папке **Users/<*имя_текущего_пользователя*>**.

В открывшемся терминальном окне вы увидите полный путь к созданному файлу.

**ПРИМЕЧАНИЕ. Убедитесь, что на компьютере, на котором извлекается токен, есть подключение к Интернету. В противном случае будет извлечен только маркер с ограничениями.**

5. Файл "**icloud_token_<timestamp>.plist"** содержит маркер аутентификации текущего пользователя iCloud.

Файл "**icloud_token_<timestamp>.plist"** содержит следующие данные:

| Версия macOS | Содержимое файла |
|---|---|
| macOS до 10.12.5 | ▪ Apple ID (apple_id)<br>▪ Маркер аутентификации (auth_token)<br>▪ Continuation token (ctoken)<br>▪ Пароль к Apple ID - иногда |
| macOS 10.3 и выше | ▪ Apple ID (apple_id)<br>▪ Маркер аутентификации (auth_token)<br>▪ Маркер аутентификации с ограничениями (auth_token_with_limitations)<br>▪ Continuation token (ctoken)<br>▪ Password to Apple ID - иногда |

Чтобы извлечь маркер аутентификации для **другого пользователя iCloud**, выполните следующие действия:

1. Запустите atex.dmg.
2. Скопируйте файл **atex** из смонтированного образа в папку, в которую будет сохранён маркер аутентификации.
3. Откройте окно терминала.
4. Перейдите в папку с файлом **atex**.
5. Просмотреть список всех пользователей iCloud можно командой **sudo atex -l** or **sudo atex --iCloudUserList**

   **sudo** используется для эскалации привилегий до root пользователя.
6. Введите пароль пользователя root.
7. Будет выведен список пользователей iCloud.
8. Для извлечения маркера запустите команду **sudo atex --getToken -u <username> -p <password>**

   Пример: **sudo atex --getToken -u mary -p 1234**

   **ПРИМЕЧАНИЕ. Убедитесь, что на компьютере, на котором извлекается токен, есть подключение к Интернету. В противном случае будет извлечен только маркер с ограничениями.**
9. Будет создан файл "**icloud_token_<timestamp>.plist**", сохраняемый в том же каталоге, откуда был запущен **atex**.

В открывшемся окне Терминала вы увидите полный путь к созданному файлу.

10. Файл "**icloud_token_<timestamp>.plist"** содержит маркер аутентификации текущего пользователя iCloud.

Файл "**icloud_token_<timestamp>.plist"** содержит следующие данные:

| Версия macOS | Содержимое файла |
|---|---|
| macOS до 10.12.5 | ▪ Apple ID (apple_id)<br>▪ Маркер аутентификации (auth_token) |

| | |
|---|---|
| | ▪ Continuation token (ctoken)<br>▪ Пароль к Apple ID - иногда |
| macOS 10.3 и выше | ▪ Apple ID (apple_id)<br>▪ Маркер аутентификации (auth_token)<br>▪ Маркер аутентификации с ограничениями (auth_token_with_limitations)<br>▪ Continuation token (ctoken)<br>▪ Password to Apple ID - иногда |

**Параметры командной строки утилиты atex:**

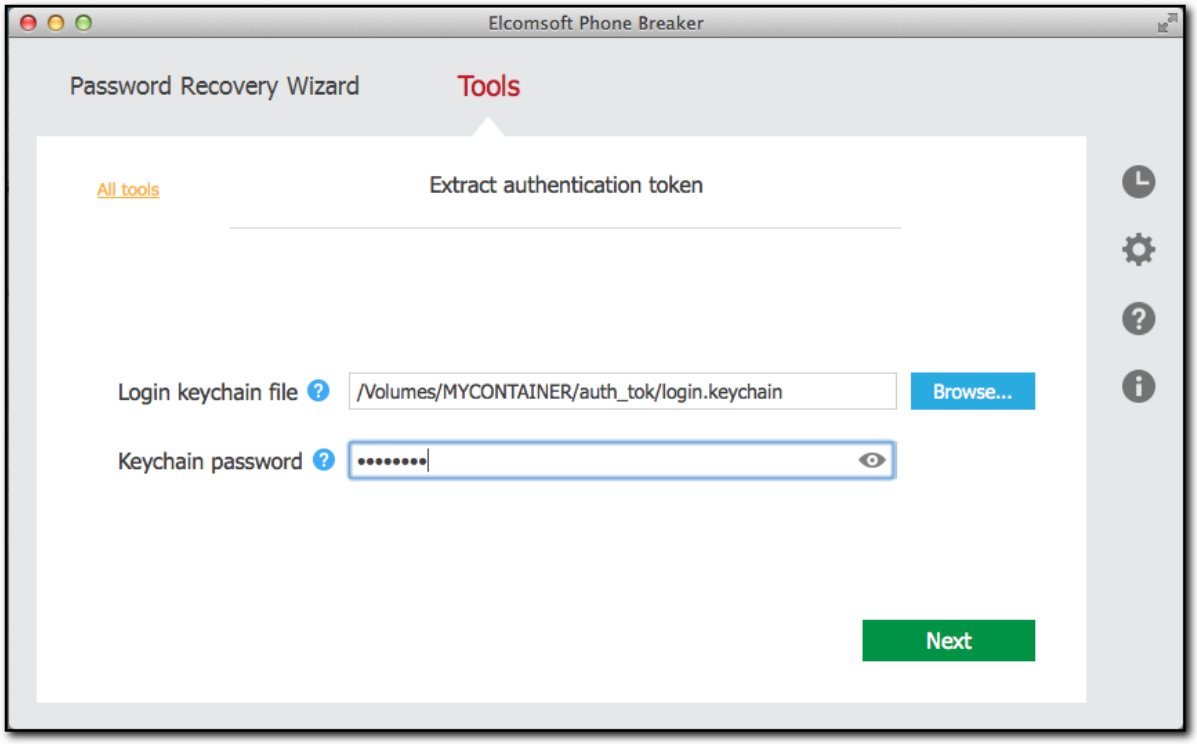
| Параметр | Значение |
|---|---|
| **-h** или **[--help]** | Отображает справочное сообщение |
| **-l** или **[--iCloudUserList]** | Отображает список пользователей iCloud |
| **--getToken -u <username> -p <password>** | Извлекает маркер аутентификации для указанного пользователя. Имя пользователя и пароль следует вводить без скобок. |
| **-u** или **[--username]** | Имя пользователя. Имя пользователя следует вводить без скобок. |
| **-p** или **[--password]** | Пароль пользователя. Пароль следует вводить без скобок. |

#### 3.2.5.3.2 Извлечение маркера аутентификации: macOS, сторонний компьютер или образ диска

EPB позволяет извлекать маркер аутентификации iCloud из неактивной копии macOS, например, путем монтирования образа диска операционной системы, в которой хранится маркер.

**Чтобы извлечь маркер аутентификации iCloud, сделайте следующее:**

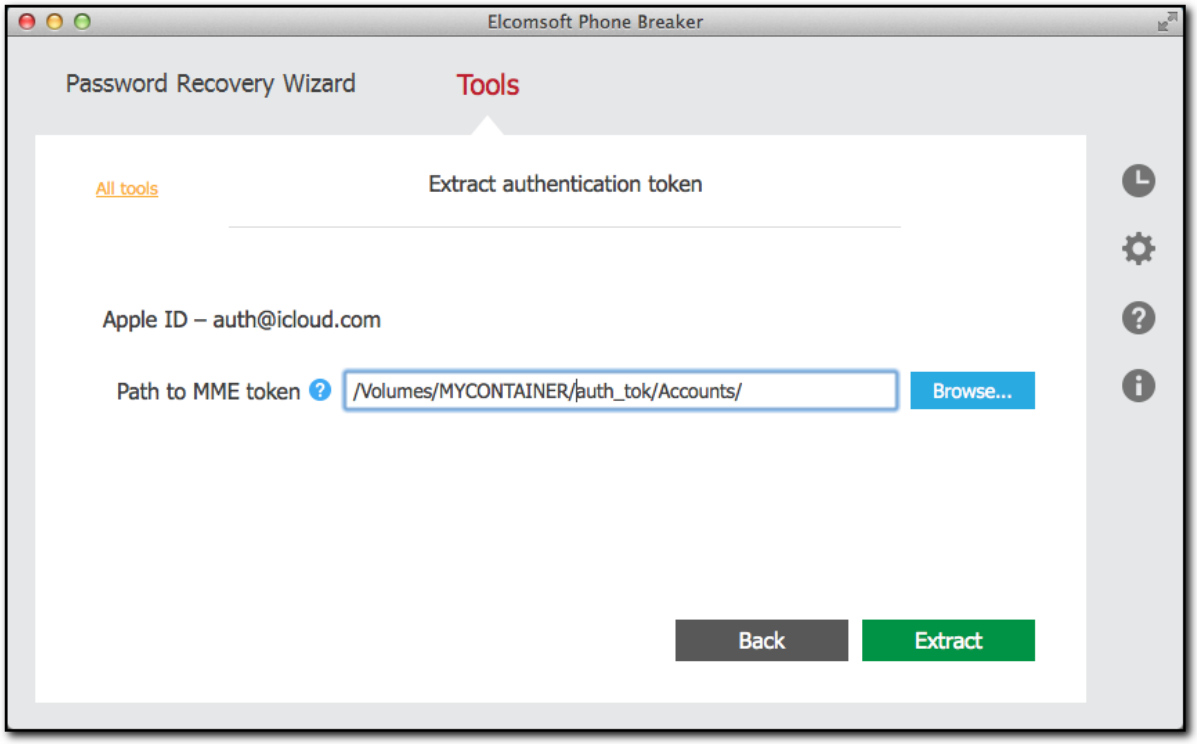
1. Смонтируйте образ диска, содержащий маркер аутентификации.
2. Запустите Elcomsoft Phone Breaker.
3. В меню **Tools/Инструменты** выберите вкладку **Apple**.
4. Нажмите **Extract authentication token/Извлечь маркер аутентификации.**
5. Укажите путь и пароль к файлу, содержащему маркер аутентификации:
   - **Login keychain file/Путь к файлу login.keychain**: Введите путь к файлу login.keychain пользователя, маркер которого вы расшифровываете. По умолчанию он хранится в */Users/<user name>/Library/Keychains/login.keychain*.
   - **Keychain password/Пароль к связке ключей**: Пароль к выбранному login.keychain.




6. Нажмите **Next/Далее**.

7. На следующей странице укажите путь к файлу, содержащему маркер аутентификации. По умолчанию **/Users/<имя пользователя>/Library/Application Support/iCloud/Accounts/**. Имя этого файла представляет собой числовое представление Apple ID пользователя в виде 6-10 цифр.

Apple ID пользователя отображается в верхней части экрана.




8. Нажмите **Extract/Извлечь**.

9. Маркер аутентификации извлекается.

Нажмите **Save token/Сохранить токен** для сохранения строки в файл в формате *.plist.

Извлечённый маркер можно использовать для аутентификации в iCloud.

# 3.3 Работа с данными из Microsoft Account

## 3.3.1 Данные в учётных записях Microsoft

Вы можете загрузить данные учетной записи Microsoft, синхронизированные с устройств или ПК с Windows, на которых пользователь вошел в эту учетную запись. EPB загружает эти данные из облака.

Для доступа к данным необходимы учётные данные - логин и пароль, а также вторичный фактор аутентификации. Доступны следующие категории данных:

- **Контакты**
- **Сообщения SMS**
- **Заметки** (OneNote)
- **Информация о звонках**
- **История поисковых запросов (Bing)**
- **История браузера**

- **История местоположений**
- **Skype**

**ПРИМЕЧАНИЕ. Если вложения Skype (кроме изображений) отправлены более 30 дней назад, они будут удалены с сервера Microsoft и не будут доступны для загрузки через EPB. В этом случае для скачивания будут доступны только метаданные вложений. Более подробную информацию об условиях хранения данных можно найти здесь.** https://support.skype.com/ru/faq/FA34893/kak-dolgo-fayly-i-dannye-ostayutsya-dostupnymi-v-skaype

Загруженные данные сохраняются в архиве, содержащем базы данных с загруженной информацией и файл Manifest.xml, в котором содержится информация о каждом устройстве, связанном с учетной записью, и имя файла для каждого файла базы данных.

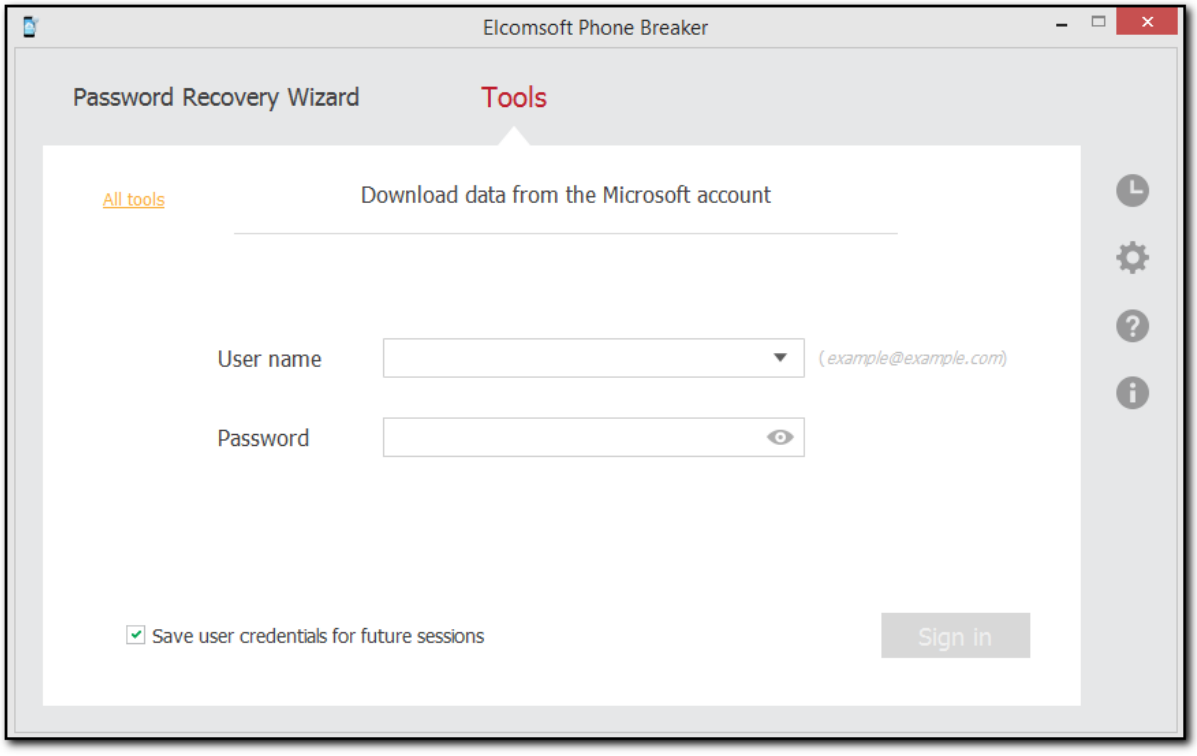
### 3.3.2 Скачивание данных из Microsoft Account

Чтобы загрузить синхронизированные данные учетной записи Microsoft, выполните следующие действия:

1. В меню **Tools/Инструменты** выберите вкладку **Microsoft** и нажмите **Download data from the Microsoft Account/Скачать данные из учётной записи Майкрософт**.

2. Введите имя пользователя и пароль для учетной записи Microsoft.

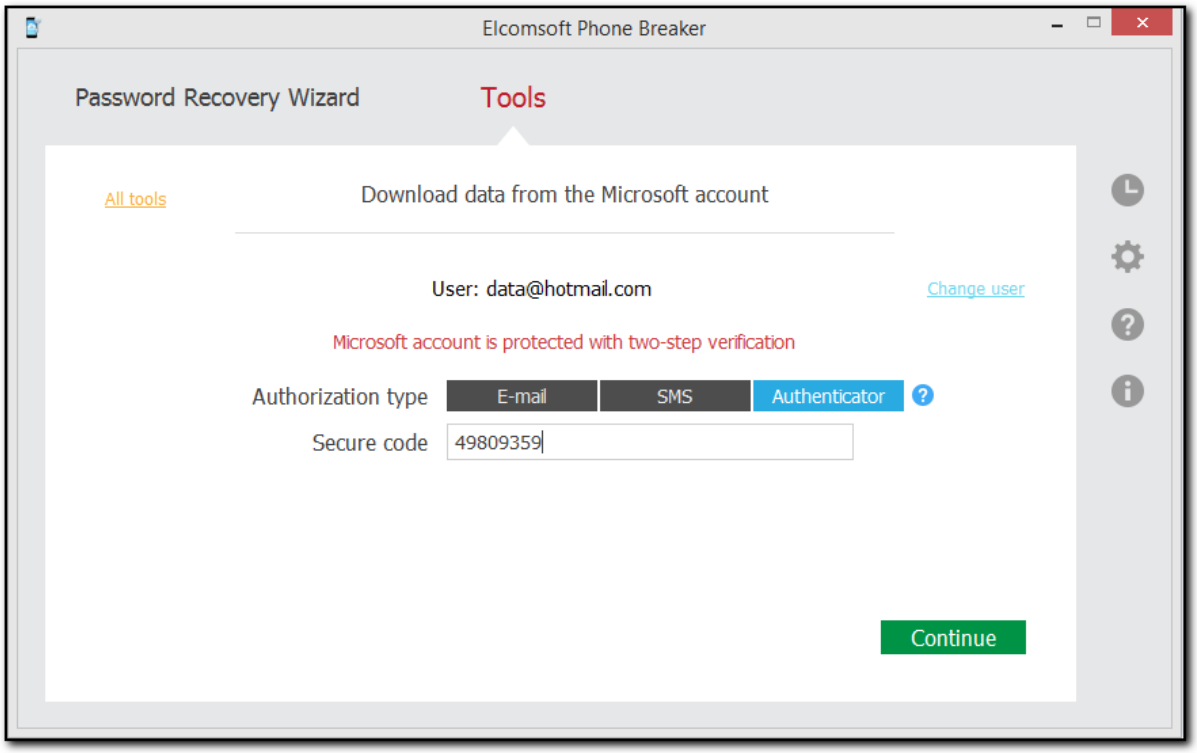
Нажмите **View/Показать** , чтобы снять маскировку символами (*) с пароля.




3. Если учетная запись защищена двухфакторной аутентификацией, вам необходимо ввести дополнительный код безопасности. Поддерживаются следующие типы авторизации:

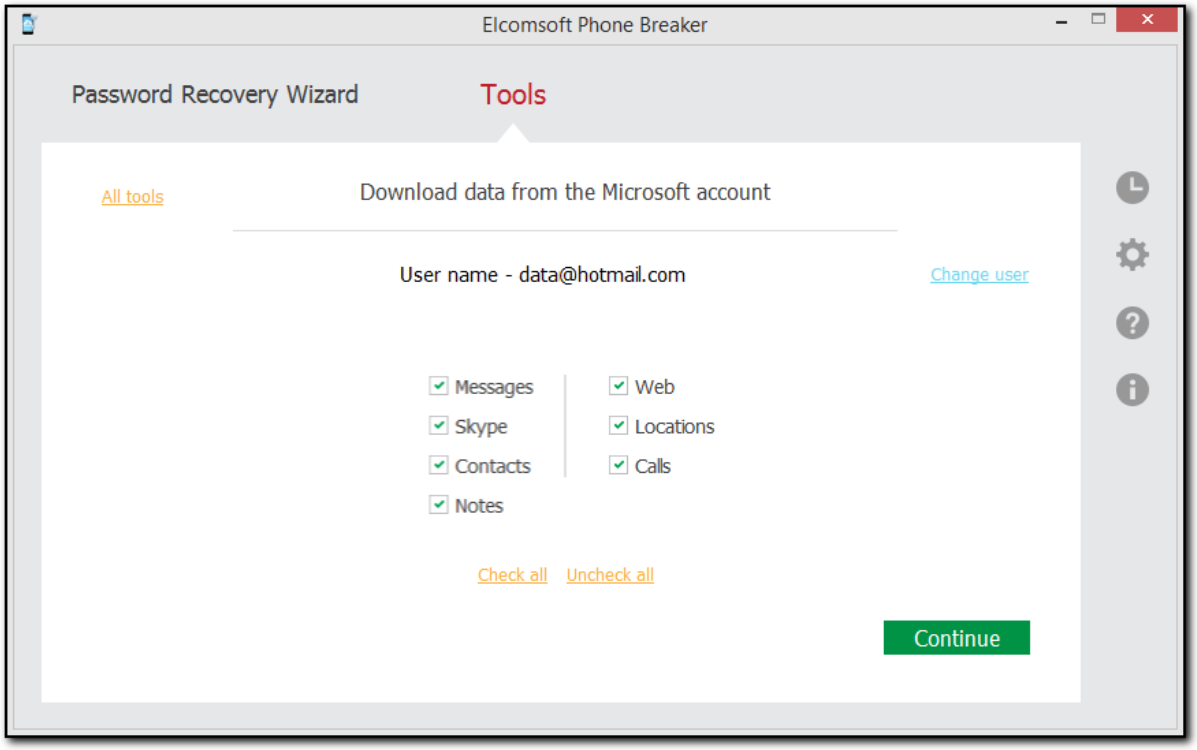
- E-mail
- SMS
- Authenticator: EPB поддерживает 8-значные коды, созданные в стандартном приложении-аутентификаторе Microsoft, и 6-значные коды, созданные в сторонних приложениях.

Выберите тип проверки, введите код безопасности и нажмите **Continue/Продолжить**.

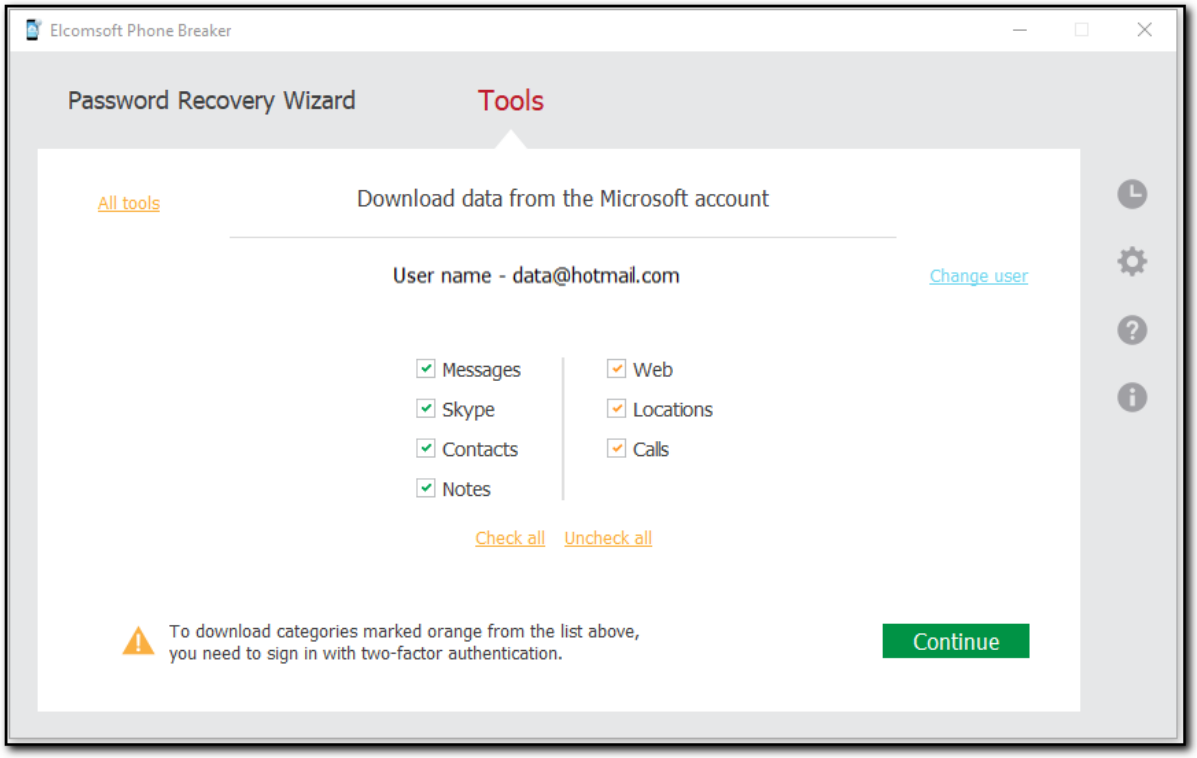



4. Отметьте категории для скачивания и нажмите **Continue/Продолжить**.

Если учетная запись защищена двухфакторной аутентификацией, загрузка начнется немедленно.




Если учетная запись не защищена двухфакторной аутентификацией, то некоторые категории будут доступны только после входа в систему с двухфакторной аутентификацией. Такие категории отмечены оранжевым. В текущей версии EPB есть три таких категории:**Calls/Звонки, Web/Веб-сайты,** и **Locations/Местоположения**.




Если ваша учетная запись не защищена двухфакторной аутентификацией и вы хотите загрузить одну из этих категорий, выберите способ получения кода безопасности:

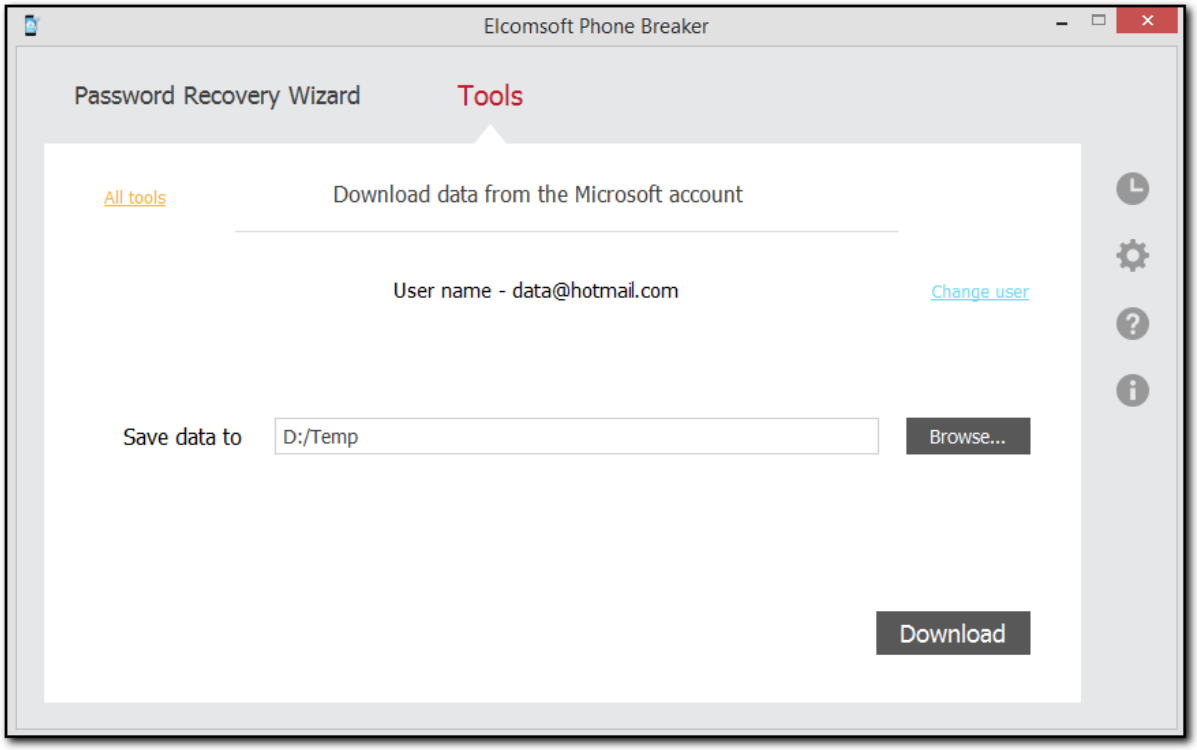
- Доверенный адрес электронной почты
- SMS

Введите номер телефона или адрес и нажмите **Send code/Отправить код**. Вы получите защищенный код на этот адрес электронной почты или номер телефона. Введите полученный код безопасности в поле **Secure code/Код безопасности** и нажмите **Continue/Продолжить**.

5. Выберите место на диске для сохранения данных, загруженных из учетной записи Microsoft.

Для смены пользователя Microsoft, чьи синхронизированные данные вы хотите загрузить, нажмите **Change user/Выбрать др. пользователя**.

Нажмите **Download/Скачать** для начала скачивания.

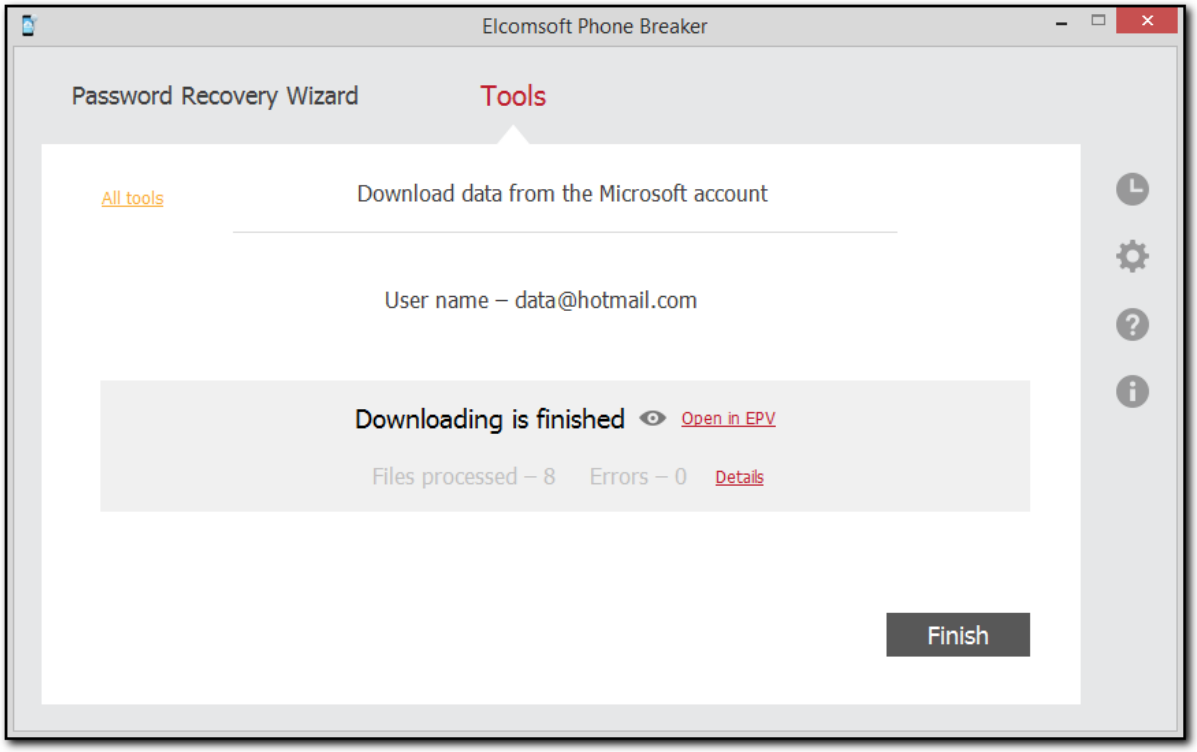



6. Начнется загрузка данных. Вы можете просмотреть количество обработанных файлов и количество ошибок, полученных во время загрузки.

7. Когда загрузка будет завершена, вы можете просмотреть загруженные данные в том месте на локальном компьютере, где они были сохранены, нажав **View/Показать** .

Нажмите **Open in EPV/Открыть в EPV,** чтобы открыть скачанные данные в Elcomsoft Phone Viewer, если он установлен.

Чтобы просмотреть подробную информацию о загруженных файлах и ошибках, возникших во время загрузки, нажмите **Details/Подробности**.




8. Нажмите **Finish/Завершить** для окончания работы.

# 3.4 [Windows] Восстановление паролей

## 3.4.1 Восстановление паролей

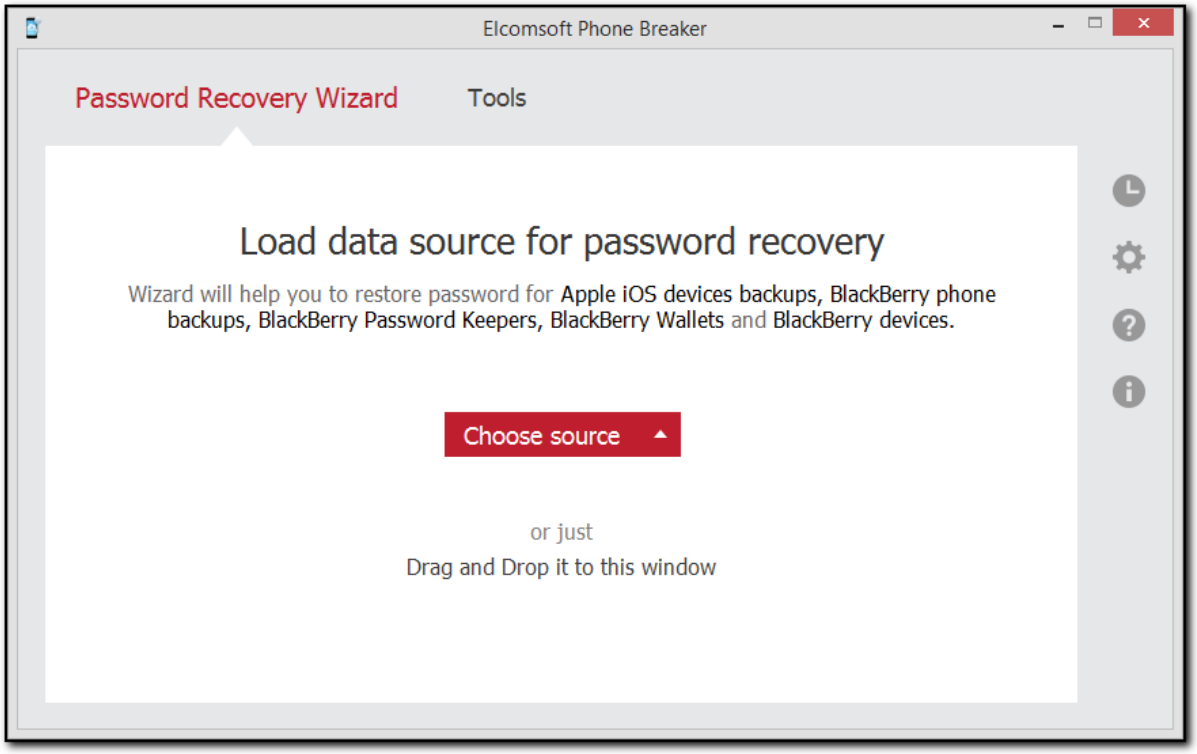
В редакции для Windows доступен функционал восстановления паролей к резервным копиям iTunes

Для настройки атаки необходим файл Manifest.plist (для iOS 10 и новее файл Manifest.db должен находиться в той же папке).

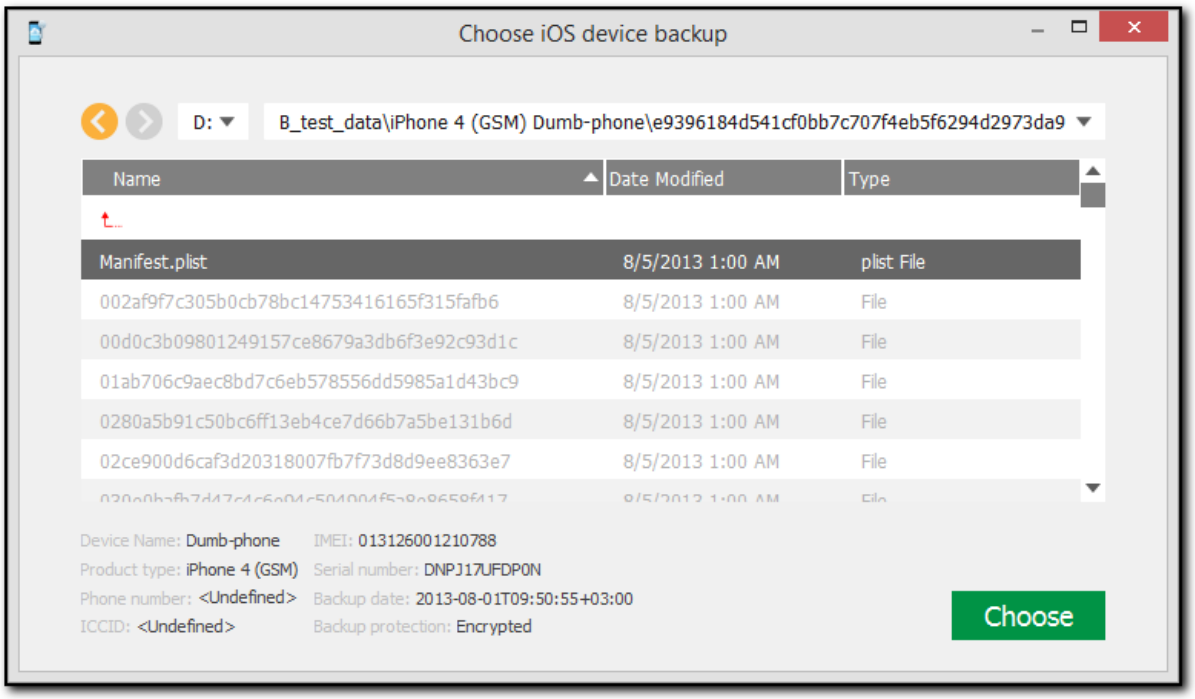
EPB позволяет восстановить пароль методом перебора. Комбинация атак составляет конвейер восстановления.

Для настройки атаки проделайте следующие шаги:

1. Запустите EPB в Windows.
2. Откройте страницу **Password Recovery Wizard/Мастер Восстановления Паролей**.



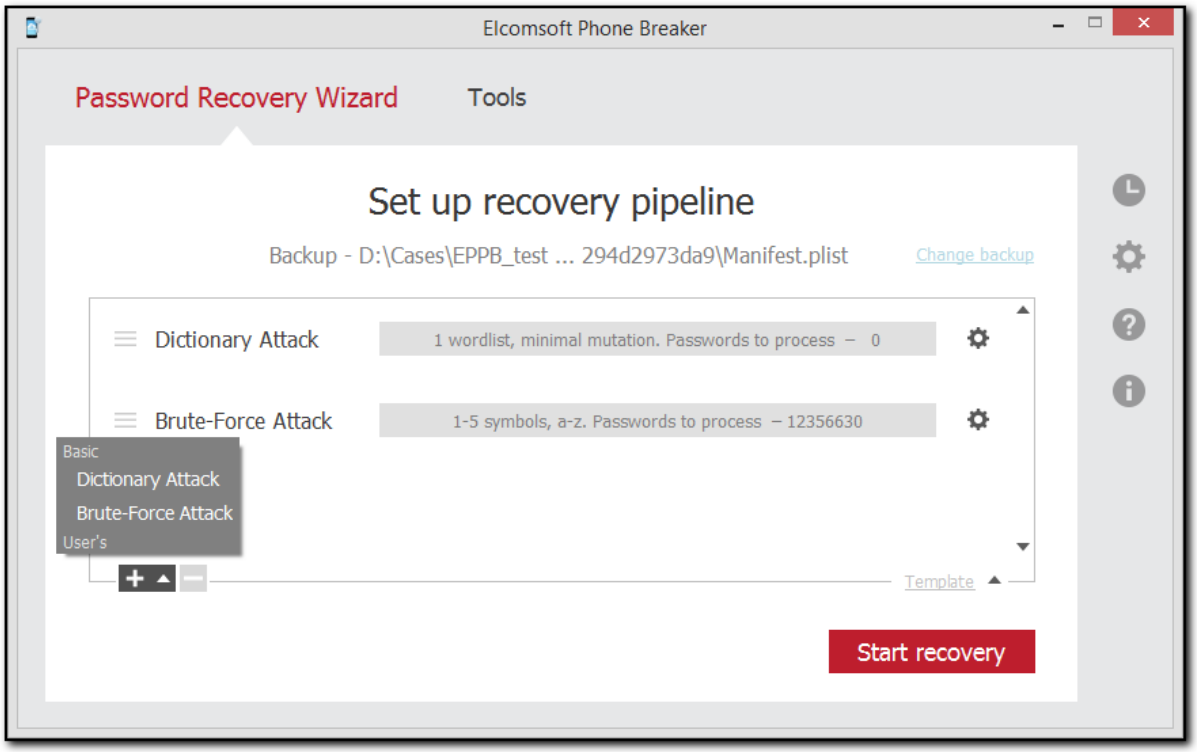

3. Чтобы добавить файл резервной копии или контейнер, перетащите его в окно мастера восстановления пароля или нажмите **Choose source/Выбрать файл** и выберите резервную копию вручную.



4. Когда файл будет добавлен, определите атаки, которые будут использоваться для взлома пароля.

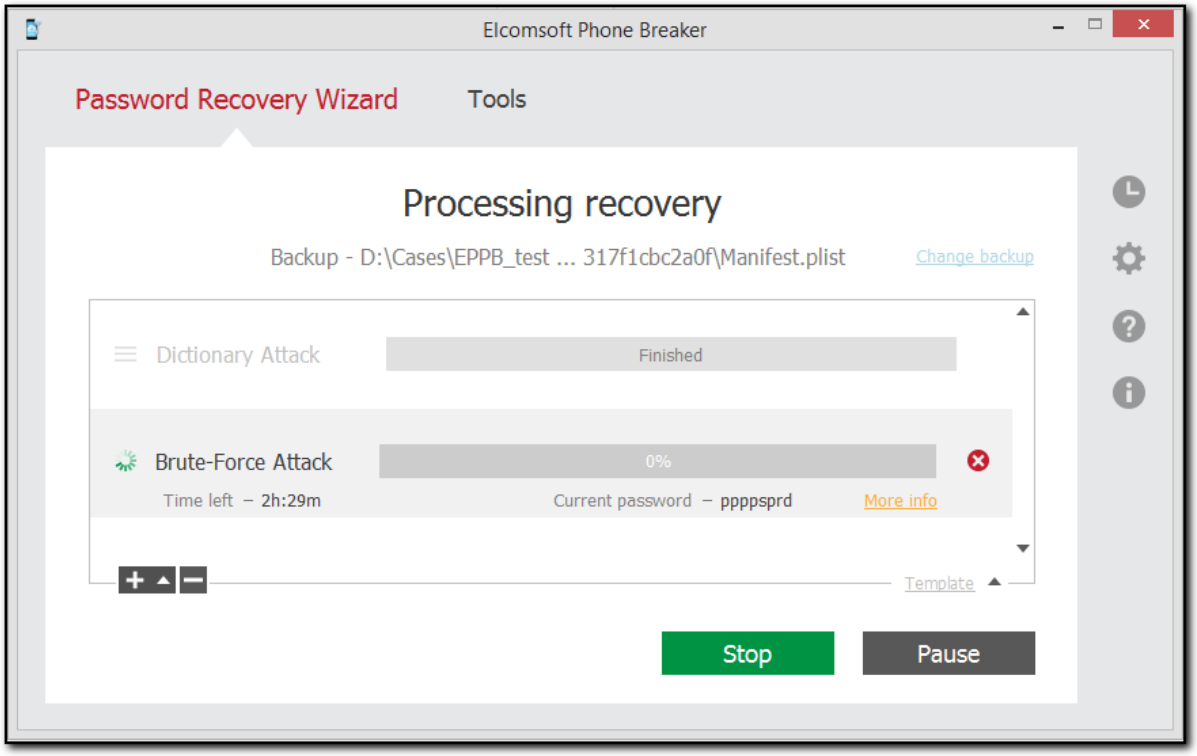
Щелкните на значок плюса «+», чтобы добавить атаки для взлома пароля. По умолчанию в очереди уже добавлены атаки по словарю и атака методом полного перебора. Подробнее об атаках и их настройках см. настройки атак.

Чтобы выбрать другую резервную копию, нажмите **Change backup/Выбрать другую рез. копию**.




5. Нажмите **Start recovery/Начать восстаноление**.

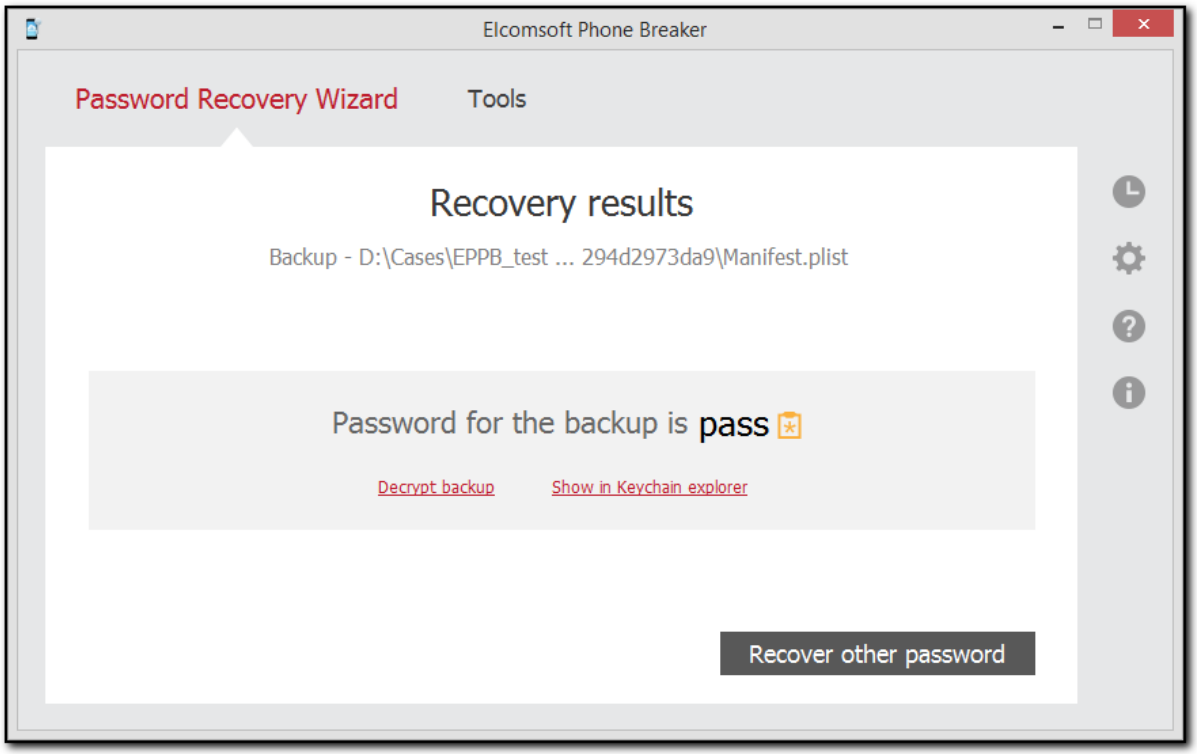
6. Начнется восстановление пароля. Вы можете просмотреть примерное оставшееся время и вариант пароля, который обрабатывается в данный момент.




По кнопке **More Info/Доп. информация** доступна дополнительная информация.

8. Кнопками **Pause/Пауза** и **Stop/Остановить** можно приостановить или прервать атаку.

9. Найденный пароль отображается в окне **Recovery results/Результат восстановления**.




Нажмите **Decrypt backup/Расшифровать рез. копию**, чтобы расшифровать резервную копию найденным паролем.

Просмотреть содержимое Связки ключей можно, нажав на ссылку **Show in Keychain explorer/Показать в просмотрщике связки ключей**. Обратите внимание: все файлы резервных копий должны находиться в той же папке, что и файл Manifest.plist.

Вернуться в окно настроек атаки можно, нажав на кнопку **Recover other password/Восстановить другой пароль**.

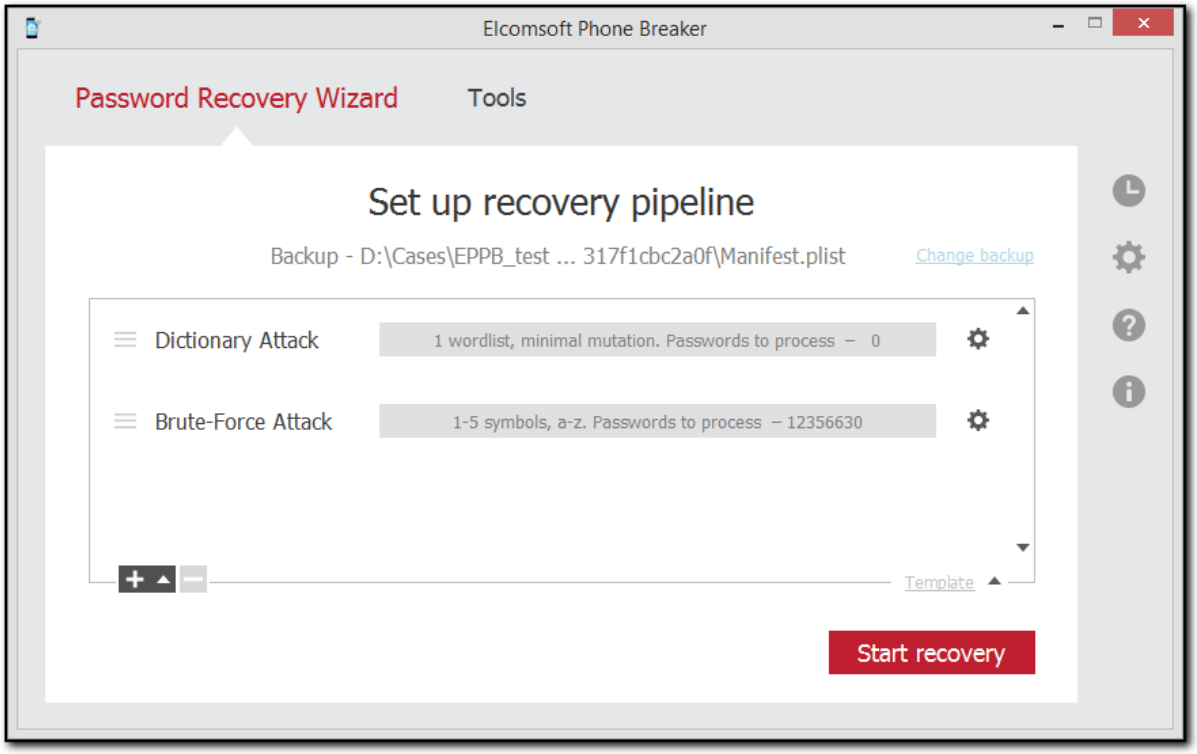
## 3.4.2 Настройка атаки

EPB позволяет восстановить пароль методом перебора. Комбинация атак составляет конвейер восстановления.

**ПРИМЕЧАНИЕ. Восстановление паролей доступно только при использовании EPB в редакции для Windows.**

Доступно два типа атак:

- **Dictionary Attack/Атака по словарю**: в процессе атаки проверяются все вхождения из словаря (текстового файла, в котором в каждой строке содержится слово). Поддерживаются стандартные и сторонние словари.
- **Brute-Force Attack/Метод полного перебора**: проверка всех возможных комбинаций паролей заданного диапазона из заданного набора символов.




Серым цветом выделены текущие настройки атаки, включая количество комбинаций, которые должны быть обработаны во время этой атаки. Чтобы изменить настройки атаки, нажмите .

Задачи проверяются в том порядке, в котором они перечислены. Можно создать несколько задач с возрастающим уровнем сложности. Например, в первую очередь можно проверить простые комбинации, затем средние и только после этого - сложные комбинации.

Кроме того, вы можете использовать шаблоны, чтобы сохранить настройки атаки или загрузить уже существующие.

## 3.4.3 Сохранение сеансов атак

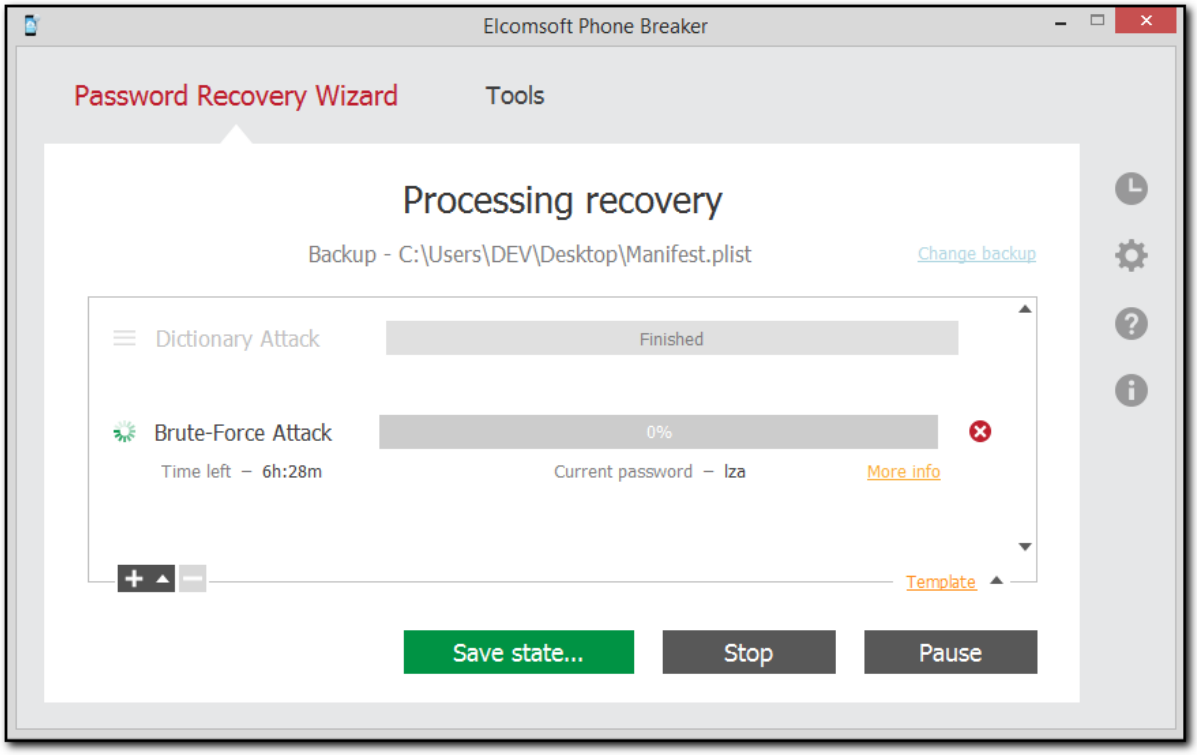
Вы можете сохранять и восстанавливать конвейер и промежуточное состояние сеансов атаки. Сохранение может выполняться вручную или автоматически.

### Сохранение и возобновление сеансов атаки вручную

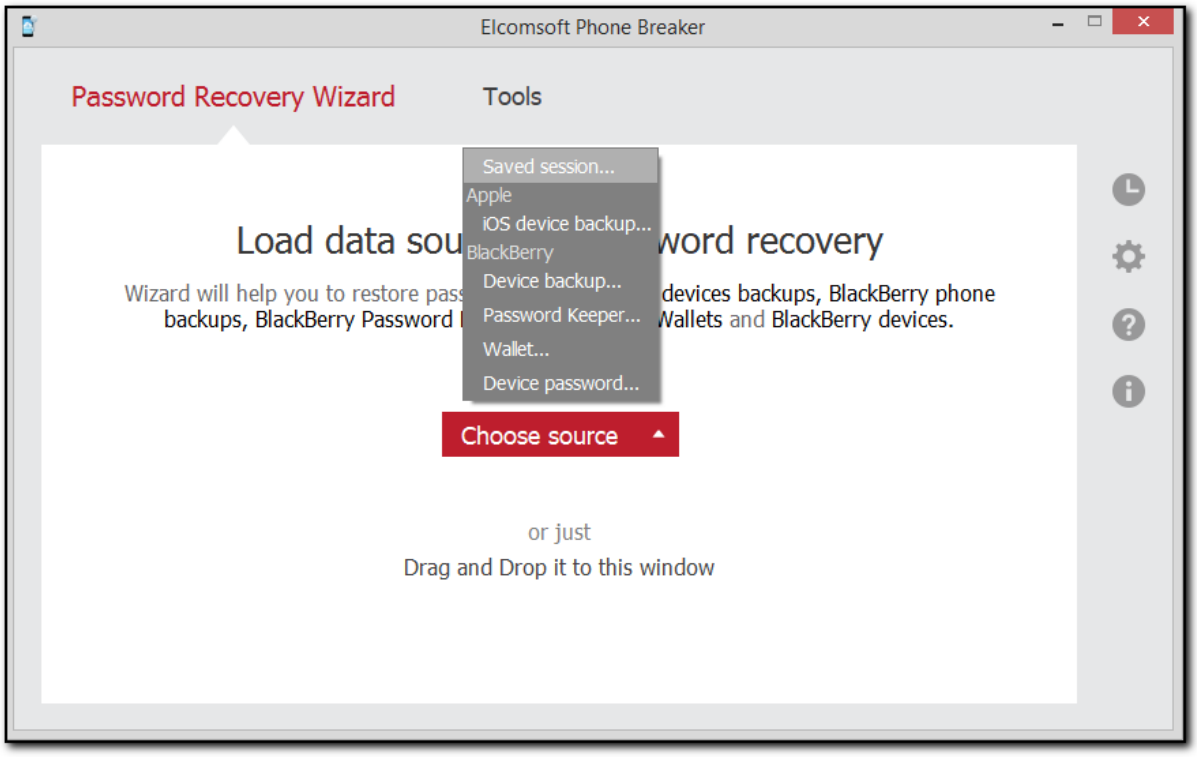
Чтобы сохранить состояние сеанса атаки восстановления пароля вручную, выполните одно из следующих действий:

- нажмите **Pause/Пауза**, после чего нажмите **Save State/Сохранить состояние** и выберите путь к файлу.
- нажмите **Save State/Сохранить состояние** и выберите путь к файлу. В этом случае атака приостанавливается и возобновляется автоматически после сохранения сеанса.

По умолчанию используется папка %USERPROFILE%\Documents. При следующих сохранениях отображается последняя выбранная папка.




Для возобновления сохранённого сеанса нажмите **Saved session/Сохранённая сессия** в главном окне мастера восстановления паролей, после чего выберите файл сохранения. Атака будет продолжена с того момента, на котором она была прервана перед сохранением сеанса.




**Автоматическое сохранение**

Если приложение закрыть до завершения атаки, сеанс атаки будет автоматически сохранён. По умолчанию автоматически сохраненные сеансы хранятся в файле %AppData%\Elcomsoft\Elcomsoft Phone Password Breaker\Sessions\~autosave.epb).

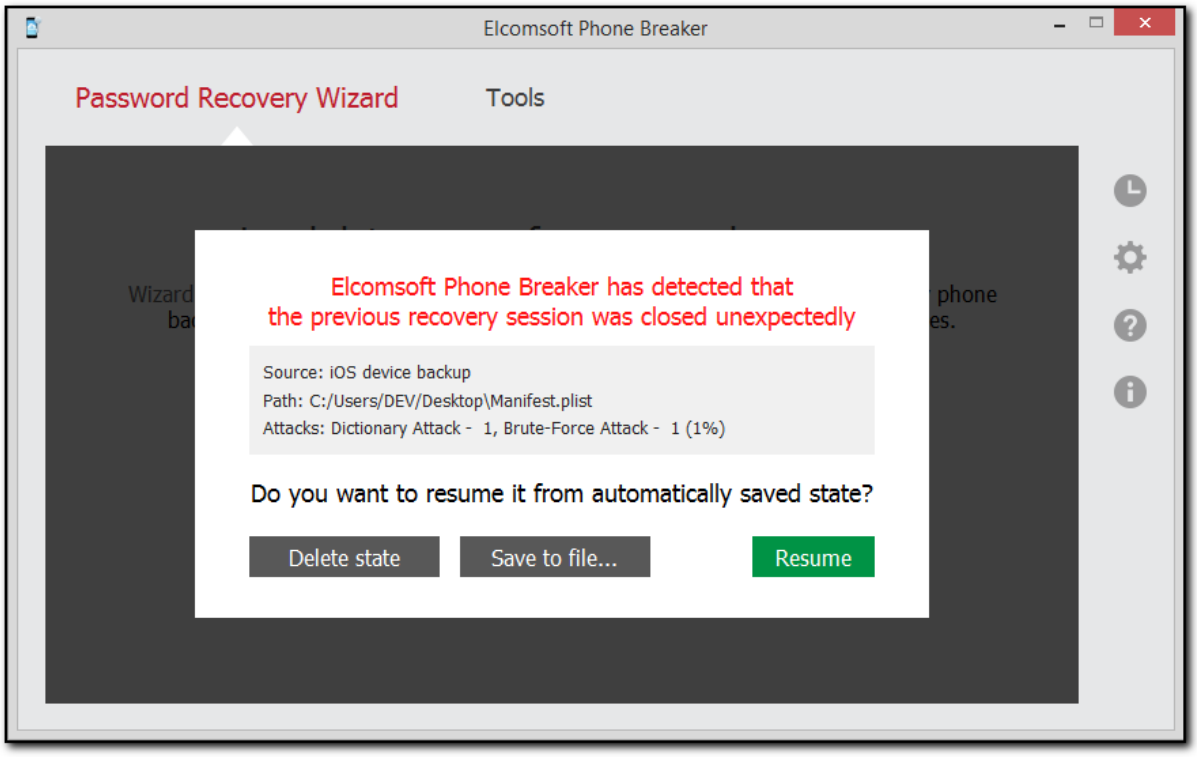
Кроме того, вы можете настроить автоматическое сохранение с заданной периодичностью.
В настройках EPB settings/EPB настройки > General/Основные:

- убедитесь, что опция **Automatically save password recovery session every <> minutes/Автоматически сохранять данные о текущей сессии атаки на пароль каждые <> минут** отмечена (она отмечена по умолчанию).
- установите желаемую частоту автосохранения в интервале от 1 до 180 минут (по умолчанию - каждые 5 минут).

Автоматически сохраненный файл сеанса удаляется при завершении или остановке атаки кнопкой **Stop/Остановить**.

**Возобновление автоматически сохраненных сеансов**

Если приложение было закрыто в процессе атаки, при следующем запуске EPB и выборе мастера восстановления пароля будет предложено возобновить автоматически сохраненный сеанс. В окне отображается информация о настройках и текущем состоянии атаки на момент автоматического сохранения.

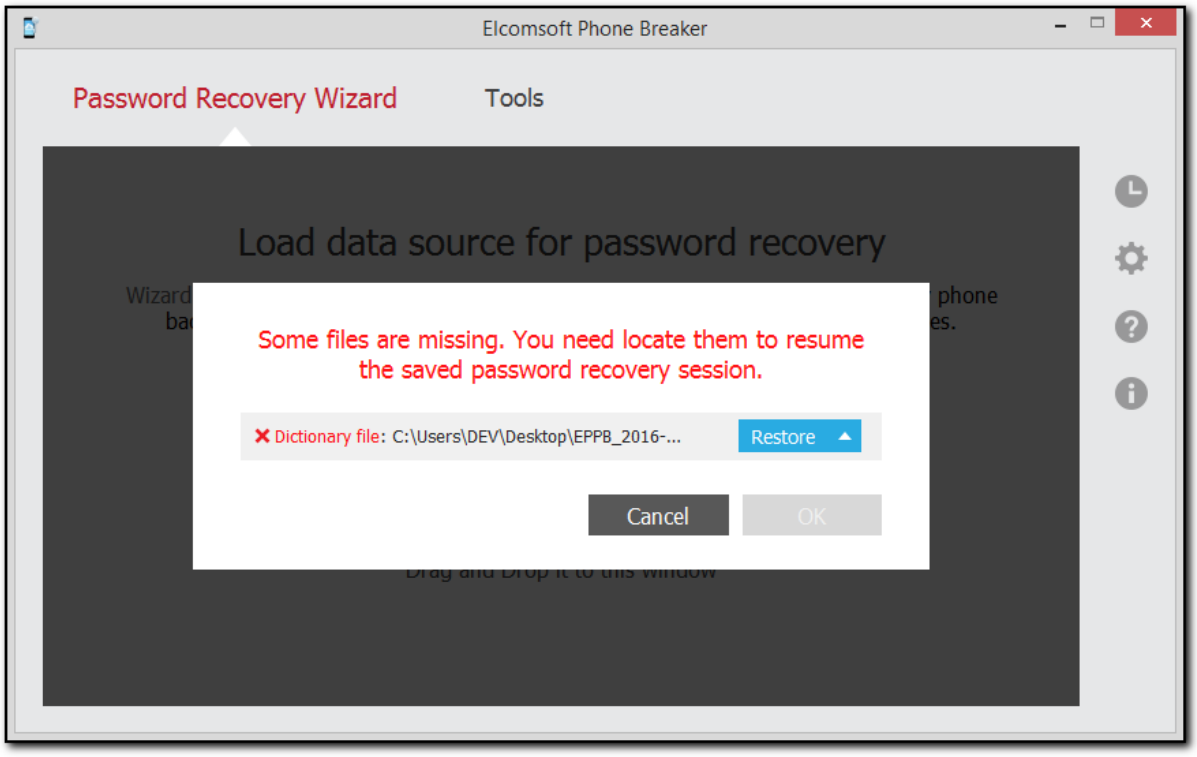



**Resume/Возобновить** восстанавливает сеанс атаки на момент последнего сохранения.
**Save to file/Сохранить в файл** сохраняет сеанс в указанный файл.
**Delete state/Удалить сеанс** удаляет сохранённый сеанс.

### Возобновление сеансов атаки с отсутствующими файлами

Если после перезапуска EPB файл резервной копии или словарь атаки отсутствует, нажмите **Restore/Восстановить** и выберите один из следующих вариантов:

- **Browse/Обзор**: выбрать недостающие файлы.
- **Skip/Пропустить**: возобновить атаку без недостающих файлов.




**Возобновление сеансов атаки в другой среде**

Вы можете возобновить сеанс атаки в другой среде (на другом компьютере под управлением Windows, с другим процессором и видеокартой). Кроме того, если вы приостановите атаку и измените настройки процессора и/или графического процессора на своем компьютере, EPB возобновит атаку с применением новых настроек.

## 3.4.4 Настройка атаки по словарю

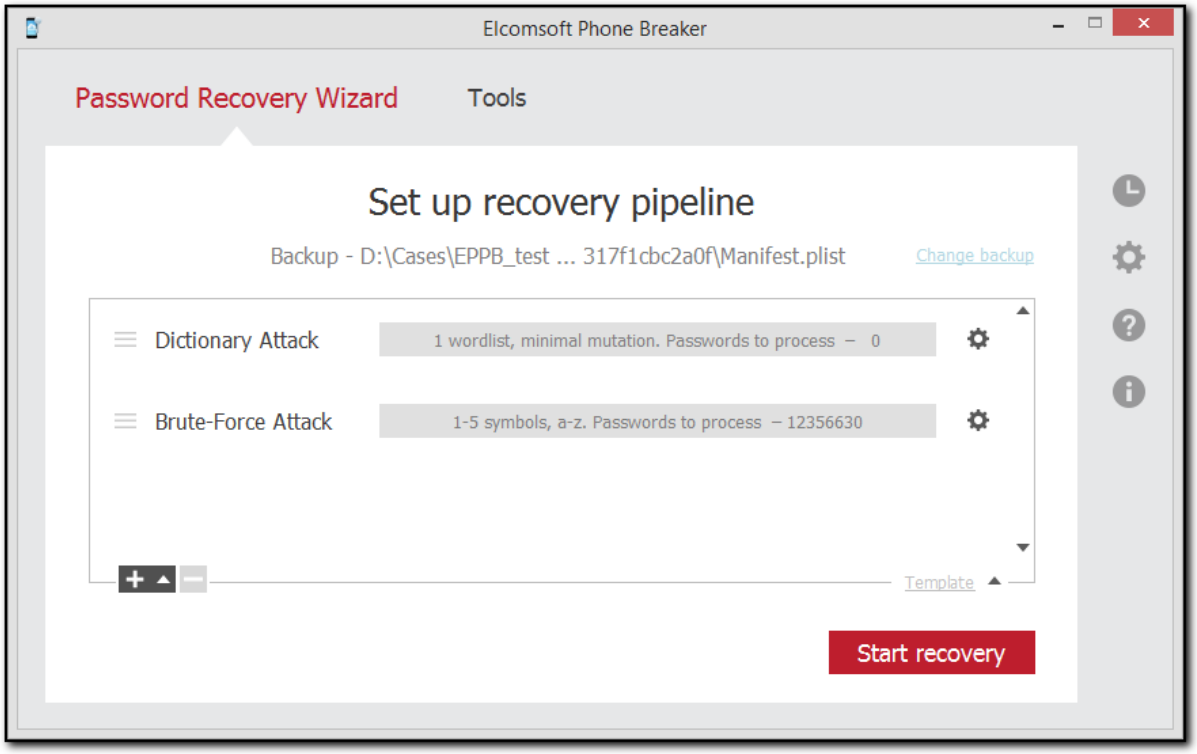
Атаки по словарю позволяют подставлять в качестве вариантов паролей как слова из текстового файла, так и их часто употребимые вариации ("мутации" в терминах EPB). Мутации позволяют подставлять варианты словарных слов, отличающиеся регистром букв, добавлением цифр или дат, перестановками букв и т.д.

В качестве словаря используется текстовый файл, в каждой строке которого содержится по одному слову.

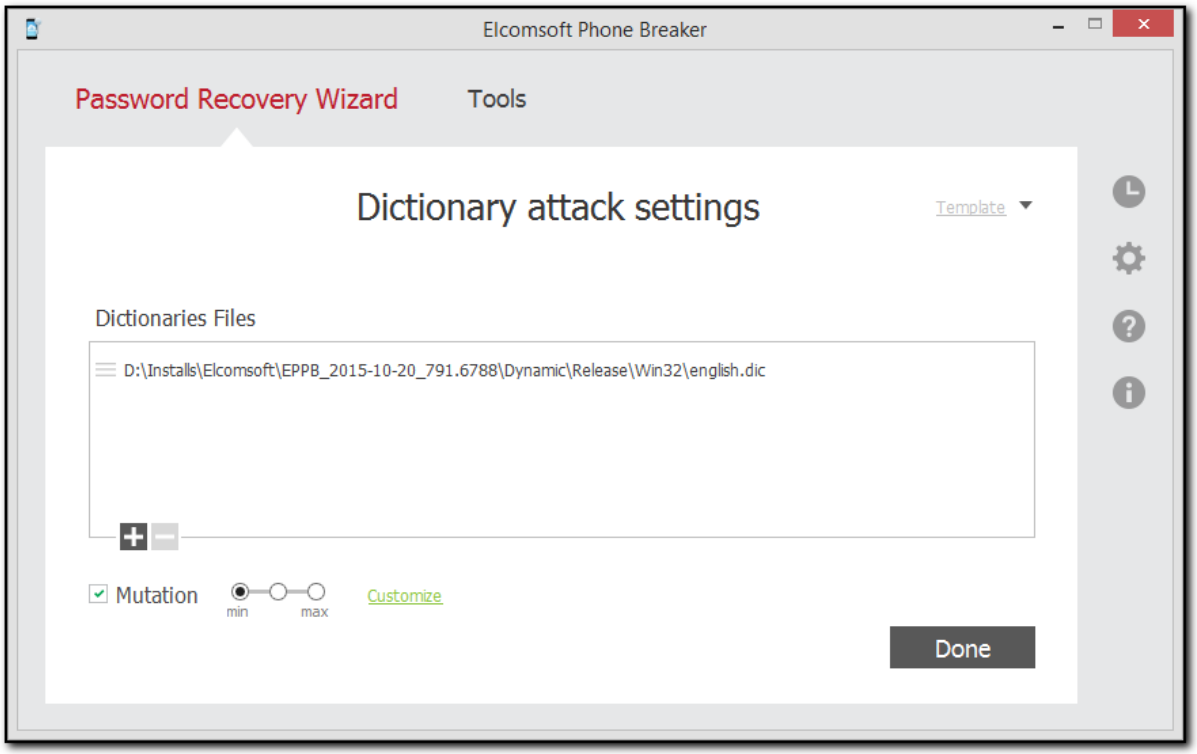
1. **Выбор атаки**

   Чтобы открыть настройки атаки, выберите резервную копию, дважды щелкните **Brute-Force Attack/Метод полного перебора** или нажмите на иконку настроек.

Настройки атаки выделены серым цветом. Они включают количество комбинаций, которое должно быть обработаны в процессе этой атаки, и набор символов, которые будут использоваться.




**2. Окно настроек**



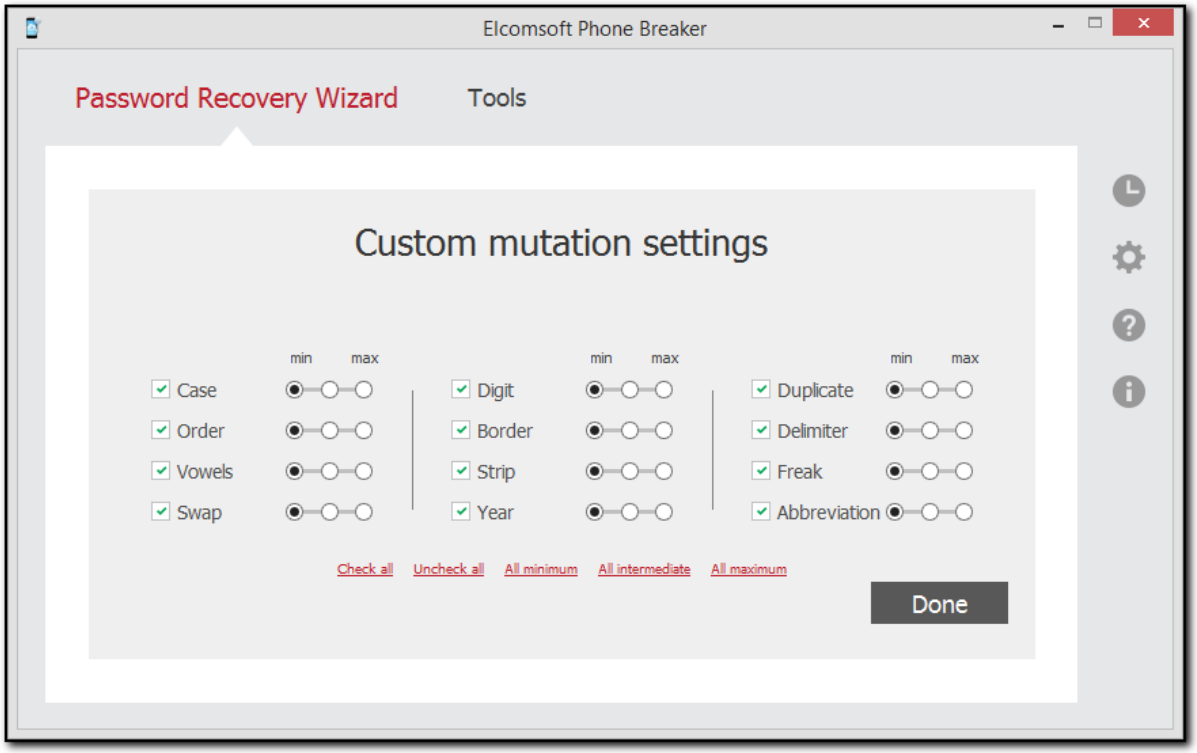
Доступны следующие настройки:

- **Selection of dictionary/Выбор словаря**. Щелкните знак плюса «+», чтобы добавить словарь (текстовый файл, содержащий слова в списке), который будет использоваться для взлома пароля. Щелкните знак минуса «-», чтобы удалить словарь из списка.
- **Mutation/Мутации**. Выбор возможных модификаций словарных слов (вариации или "мутации" паролей):
  - **Minimal/Минимальный**: Минимальный уровень мутаций. Проверяются только пароли в нижнем регистре, а цифры добавляются только в конец пароля.
  - **Intermediate/Средний**: Включает в себя мутации минимального уровня; дополнительно проверяются слова с первой буквой в верхнем регистре.
  - **Maximal/Максимальный**: Включает в себя мутации минимального и среднего уровней; дополнительно проверяются слова, полностью состоящие из букв в верхнем регистре.

По умолчанию мутации применяются ко всем выбранным правилам. Настроить уровень мутаций для каждого правила по отдельности можно, нажав **Customize/Настроить** рядом с выбранной мутацией.

После изменения настроек ссылка **Customize/Настроить** меняет название на **Customized/Настроено,** а её цвет меняется с **зелёного** на **красный**.

**3. Пользовательские настройки мутаций**




Все мутации слов в словаре разделены на несколько наборов. Вы можете выбрать уровень мутации для каждого набора, что позволяет найти нужный баланс между скоростью и эффективностью атаки.

Ниже приводятся примеры паролей, которые будут проверяться в результате выбранной мутации.

Доступны следующие наборы мутаций:

| Название мутации | Описание | Уровни | Примеры |
|---|---|---|---|
| Case | Позволяет проверять слова с прописными и строчными буквами. | • Минимальный уровень проверяет слова в словаре, написанные в нижнем и верхнем регистре, причем первая буква написана в нижнем регистре, а другие - в верхнем регистре.<br>• Средний уровень проверяет все комбинации с минимального уровня, а также первую и последнюю букву слова в верхнем регистре.<br>• Максимальный уровень проверяет комбинации из предыдущих уровней, а также комбинации, каждая вторая буква которых написана в верхнем регистре. | *password, PASSWORD, pASSWORD.*<br>*password, PASSWORD, PassworD.*<br>*password, PASSWORD, PaSsWoRd.* |
| Order | Изменение порядка букв в слове на противоположный, повторение слова, добавление перевернутого слова к исходному слову. | Отличий нет | *password - drowssap passwordpassword, passworddrowssap* |
| Vowels | Удаление гласных или их использование в нижнем или верхнем регистре. | Отличий нет | *psswrd*, *PaSSWoRD*, *pAsswOrd* |
| Swap | Изменение порядка соседних символов в слове. | Отличий нет | *apssword*, *psasword*, *paswsord* |
| Digit | Добавление нескольких цифр в производное (из словаря) в качестве префикса и суффикса. | • Минимальный уровень позволяет добавлять цифры (0-9) в конце слова, проверять строчные слова и слова, начинающиеся с заглавной буквы.<br>• Средний уровень позволяет проверять слова, написанные в верхнем регистре, и слова с цифрами в начале. | *password1, Password1*. |

| Название мутации | Описание | Уровни | Примеры |
|---|---|---|---|
| | | • Максимальный уровень позволяет проверять комбинации в диапазоне от 00 до 99. | *3passsword, 3PASSWORD.* |
| | | | *33password, PASSWORD99* |
| Border | Аналогично мутации Digit, но с добавлением не только цифр, но и наиболее часто используемых символов (например, 123, $$$, 666, qwerty, 007, xxx) в качестве префикса и суффикса. | Отличий нет | *#password#*, *$password$* |
| Strip | Удаление одного символа из словарного слова. | Отличий нет | *assword*, *pssword*, *pasword* |
| Year | Добавление года (1900-2050) в конце слова | Отличий нет | *password1973*, *password2002* |
| Duplicate | Дублирование символов в пароле. | Отличий нет | *ppassword*, *paassword*, *passsword*, *passwword* |
| Delimiter | Добавление разделителей, например. + * - \ / # = \| между символами пароля. | Отличий нет | *p.a.s.s.w.o.r.d*, *p+a+s+s+w+o+r+d*, *p-a-s-s-w-o-r-d* |
| Freak | Замена некоторых символов в пароле символами. | Отличий нет | *p@ssword*, *p@$$word* and *p@$$w0rd* |
| Abbreviation | Проверка некоторых часто используемых сокращений. | Отличий нет | *ihateyou - ih8you*, *loveyou - loveu*, *foryou - 4u.* |

Используйте шаблоны для сохранения настроек атаки.

**Done/Готово** закрывает окно настроек.

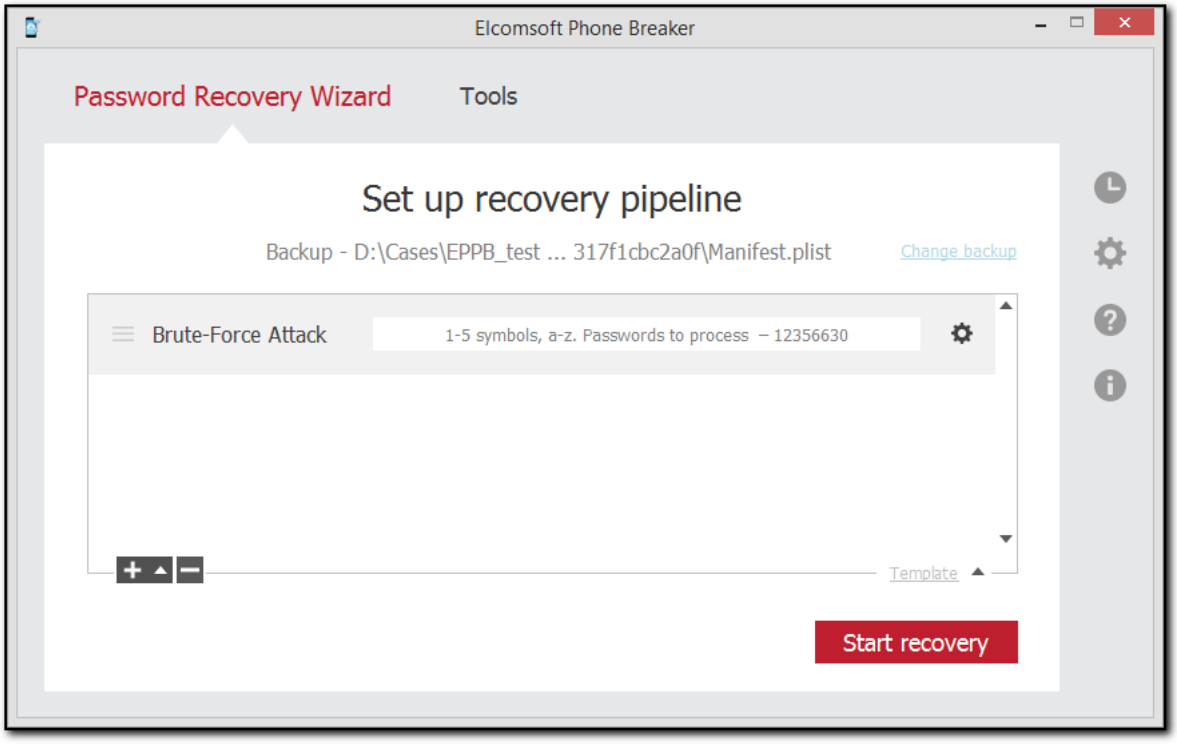
## 3.4.5 Настройка атаки методом полного перебора

Атаки методом полного перебора позволяют проверять все комбинации символов в заданных пределах.

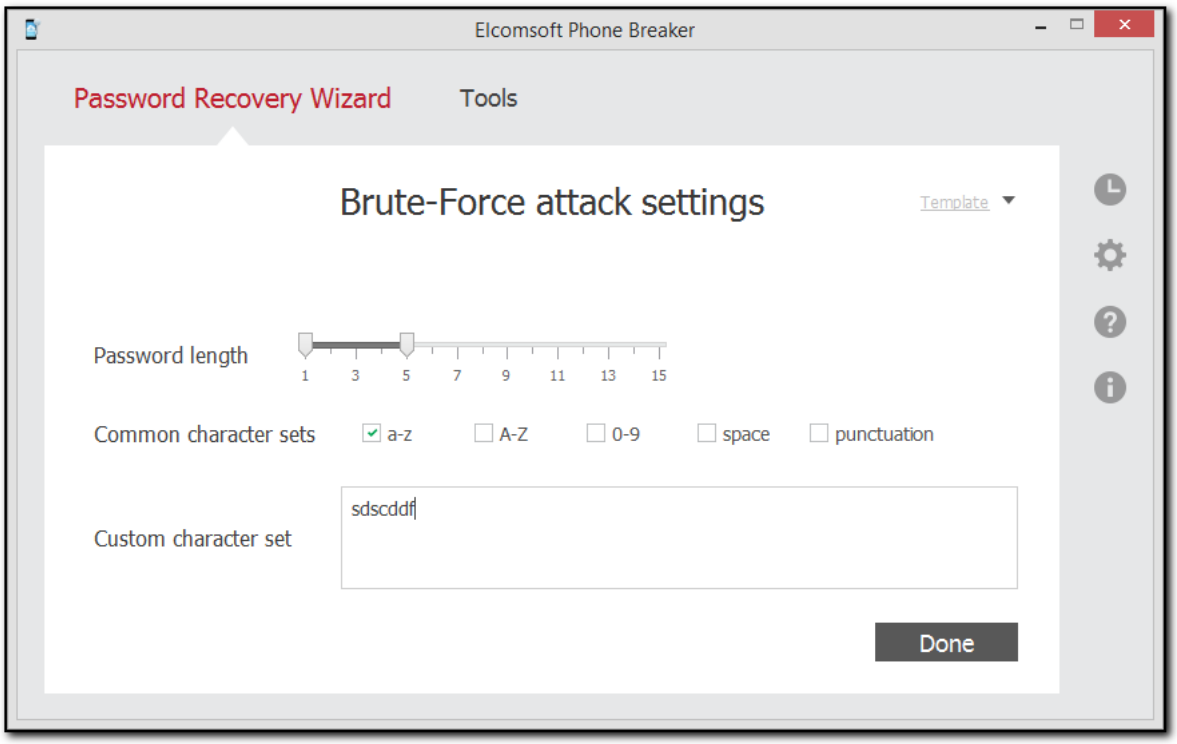
**1. Выбор атаки**

Чтобы открыть настройки атаки, выберите резервную копию, дважды щелкните **Brute-Force Attack/Метод полного перебора** или нажмите на иконку настроек.

Настройки атаки выделены серым цветом. Они включают количество комбинаций, которое должно быть обработаны в процессе этой атаки, и набор символов, которые будут использоваться.




**2. Окно настроек**



Доступны следующие настройки:

- **Password length/Длина пароля**: определяет интервал длины паролей в символах, в рамках которого будут проверяться варианты.
- **Common character sets/Обычные наборы символов**: позволяет выбрать набор символов, которые будут входить в варианты паролей:
  - a-z: буквы латиницы в нижнем регистре.
  - A-Z: буквы латиницы в верхнем регистре.
  - 0-9: цифры от 0 до 9
  - **space/пробел**: знак пробела
  - **punctuation/пунктуация**: знаки препинания
- **Custom character set/Свой набор символов**: позволяет указать дополнительные символы для проверки. Например, все буквы кириллицы в обоих регистрах:

  `абвгдеёжзийклмнопрстуфхцчшщъыьэюяАБВГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯ`.

Используйте шаблоны для сохранения настроек атаки.

**Done/Готово** закрывает окно настроек.

## 3.4.6 Шаблоны

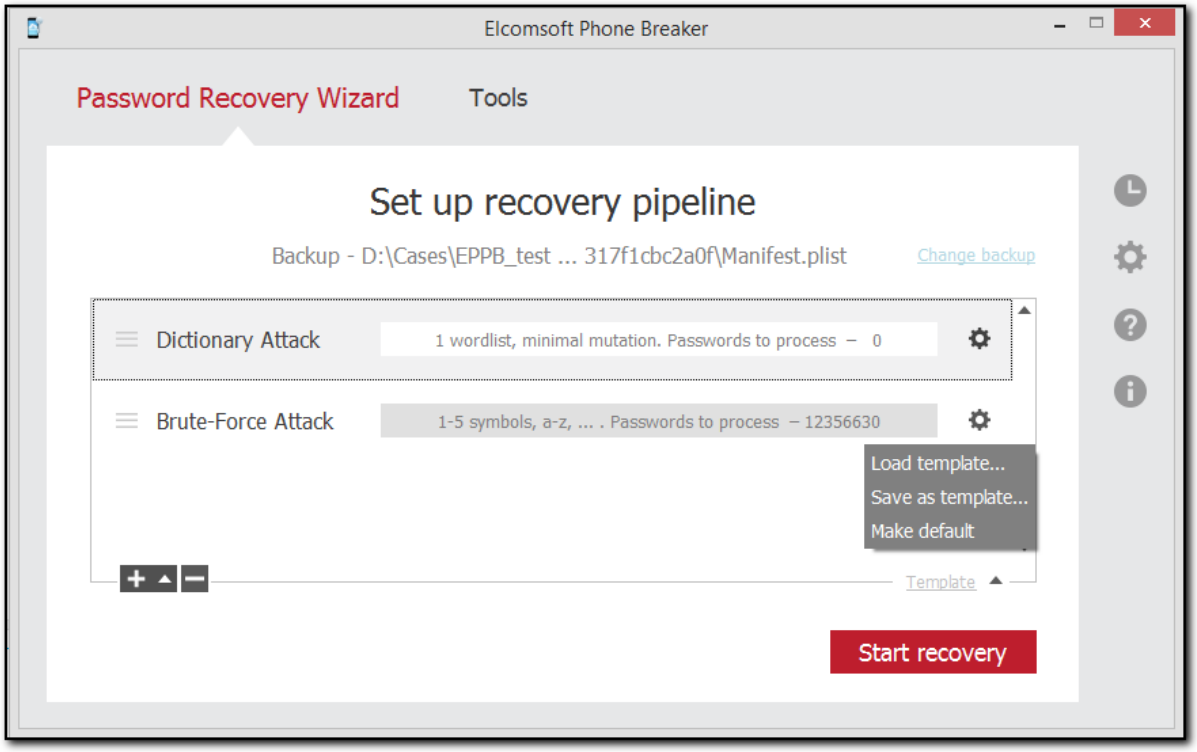
### 3.4.6.1 Сохранение шаблонов

Шаблон - это комбинация настроек конвейера или отдельной атаки, сохраненной в EPB. Шаблоны созданы для упрощения повторного использования определенных настроек при восстановлении паролей к нескольким резервным копиям.

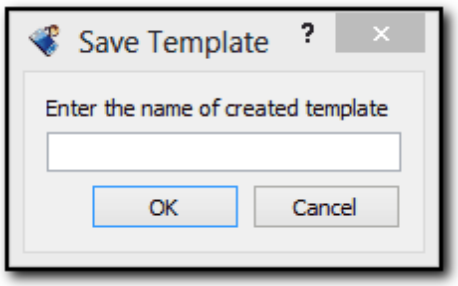
Для сохранения шаблона:

1. Запустите восстановление пароля

2. Выберите **Template/Шаблон - Save as template/Сохранить в шаблоны** на странице **Set up recovery pipeline/Установить конвейер атак**. Чтобы создать шаблон по умолчанию, который будет отображаться в окне **Password recovery/Восстановление пароля**, нажмите **Make default/Сделать настройкой по умолчанию**.



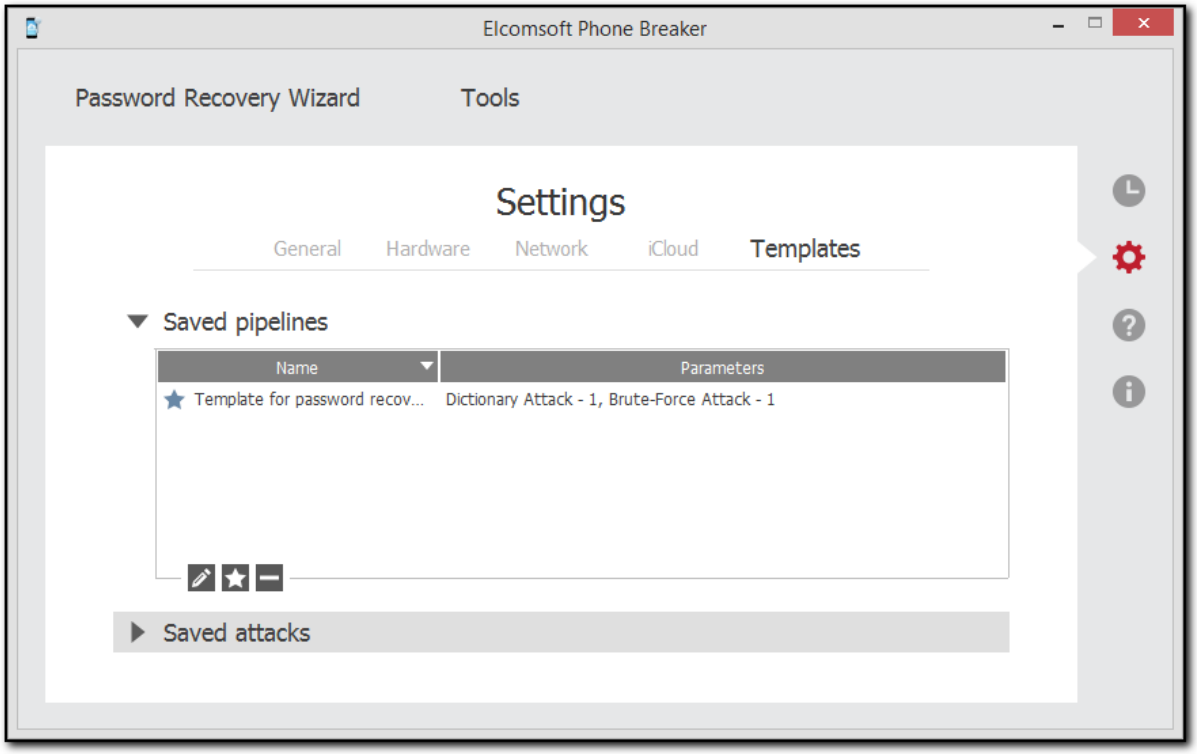

3. В окне **Save Template/Сохранить Шаблон** укажите название шаблона.




Просмотр шаблонов - **Settings/Настройки -> Templates/Шаблоны.**

### 3.4.6.2 Просмотр шаблонов

Для просмотра сохранённых шаблонов откройте окно **Settings/Настройки -> Templates/Шаблоны**.




Информацию о шаблонах конвейеров (комбинации атак) можно посмотреть в разделе **Saved pipelines/Сохранённые конвейеры**. Информация об отдельных атаках отображается в разделе **Saved attacks/Сохранённые атаки**.

Редактирование названия шаблона:

Установка шаблона по умолчанию:

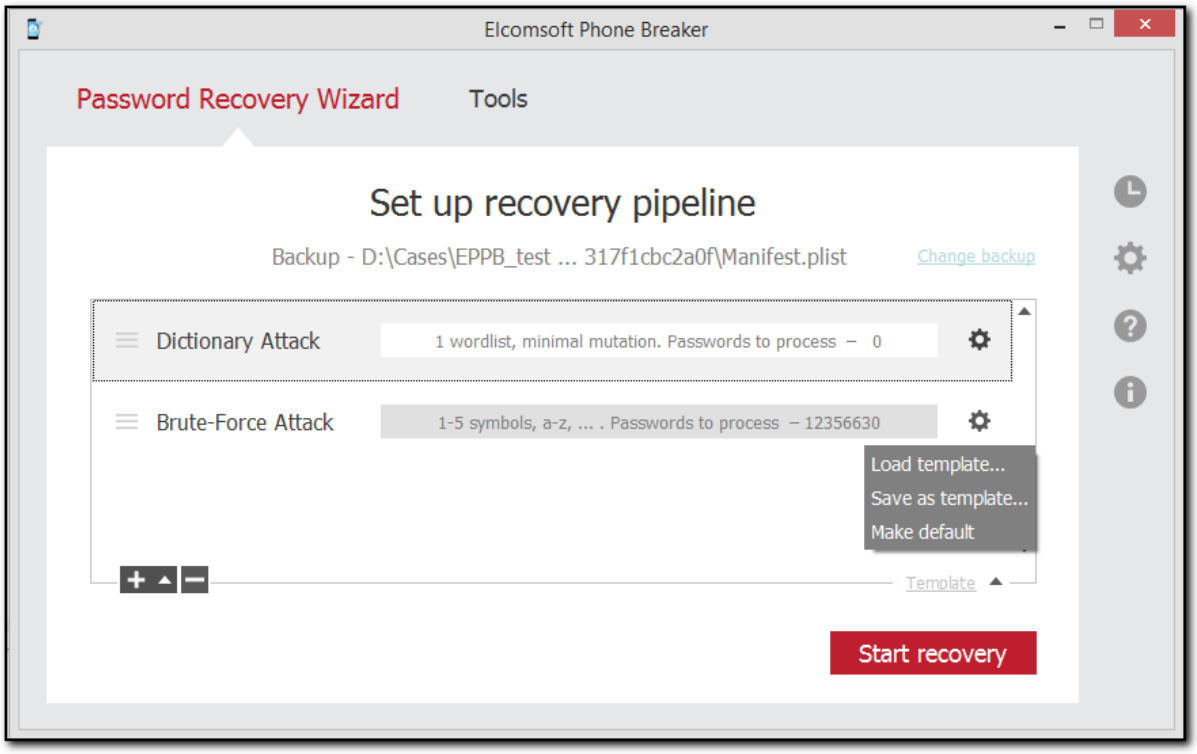
Удаление шаблона:

### 3.4.6.3 Загрузка шаблонов

Для загрузки шаблона:

1. Откройте окно восстановления паролей.

2. Выберите **Template/Шаблон - Load template/Загрузить шаблон** в окне **Set up recovery pipeline/Установить конвейер атак**.




3. Выберите шаблон и нажмите **Load/Загрузить**.


4. Шаблон будет загружен в окне **Set up recovery pipeline/Установить конвейер атак**.

### 3.4.6.4 Использование шаблонов в атаках

Помимо сохранения всего процесса восстановления в шаблоне, вы можете сохранить настройки отдельной атаки.

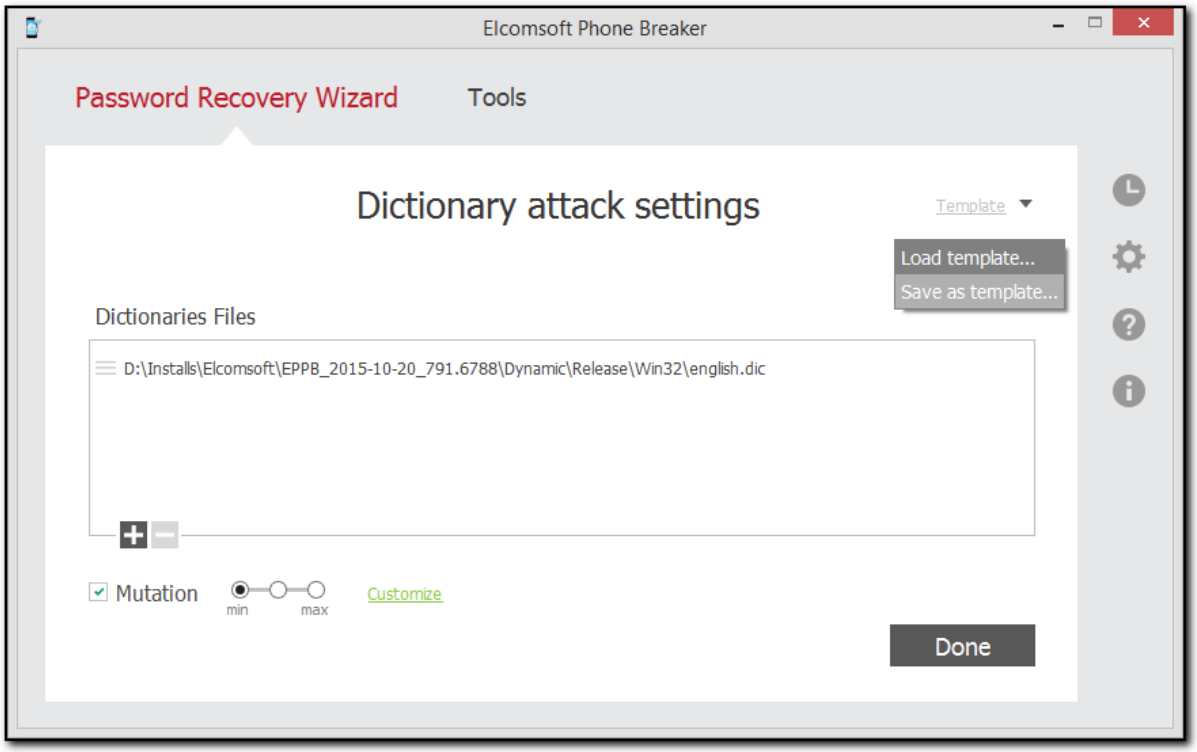
Чтобы сохранить настройки атаки в шаблон, сделайте следующее:

1. Откройте окно восстановления паролей.

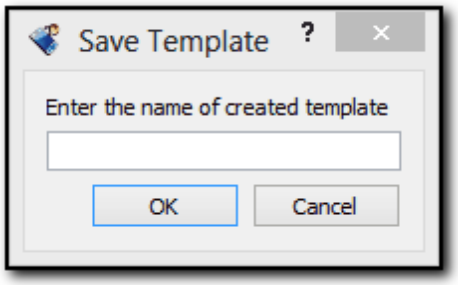
2. Создайте очередь атак.

3. Дважды щелкните определенную атаку или щелкните ⚙ рядом с ней.

4. Нажмите **Template/Шаблон** - > **Save as template/Сохранить в шаблоны** на странице **Attack settings/Настройка атак**.




5. В окне **Save Template/Сохранить Шаблон** укажите название шаблона.



# IV Elcomsoft Phone Viewer

## 4.1 О программе

### 4.1.1 Настройки

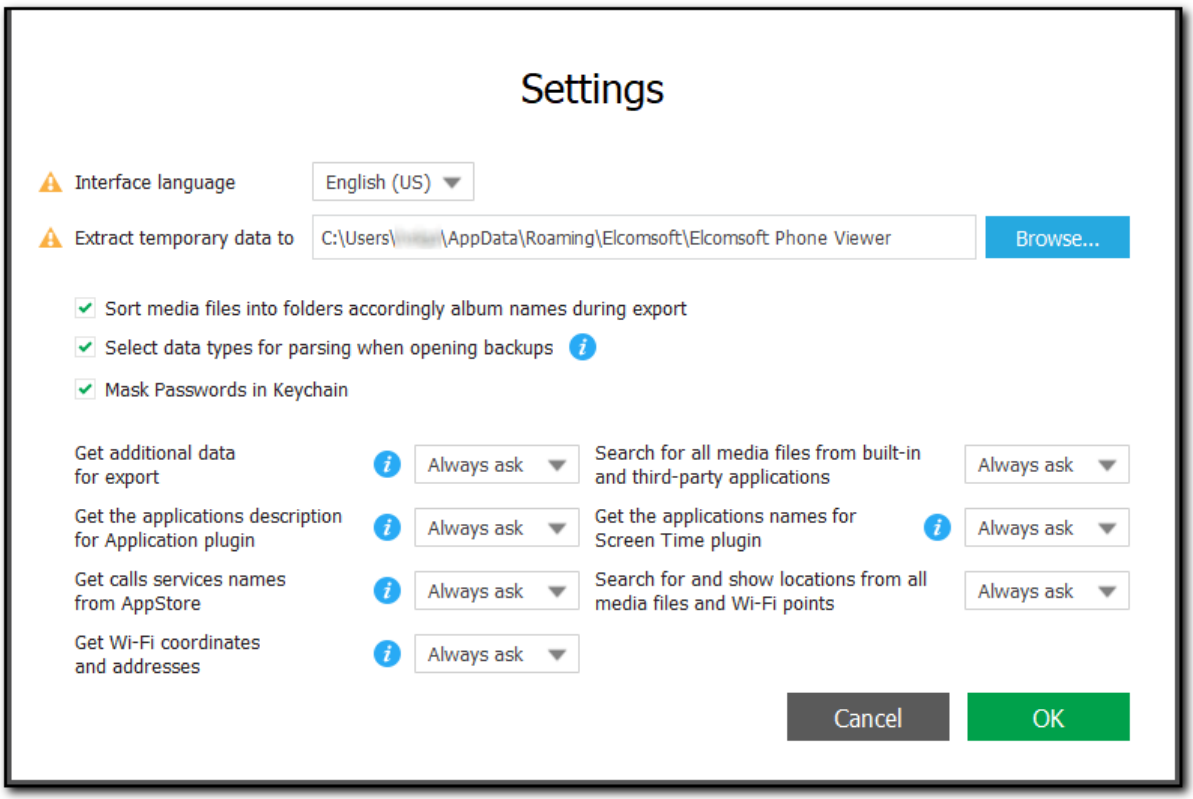
Вы можете переключаться между англоязычным и русскоязычным интерфейсом Elcomsoft Phone Viewer. Изменения вступают в силу после перезапуска приложения.

При расшифровке резервной копии создается ряд файлов, содержащих временные данные. Общий размер временных файлов равен размеру резервной копии.
Вы можете указать папку, в которую будут сохраняться временные данные во время дешифрования резервной копии, в поле **Extract temporary data to/Сохранить временные данные в** в окне **View/Вид - Settings/Настройки**.

Пути по умолчанию:

- **Windows**: *C:\Users\Username\AppData\Roaming\Elcomsoft\Elcomsoft Phone Viewer*
- **macOS**: *~/Users/<username>/Library/Application Support/Elcomsoft/Elcomsoft Phone Viewer*

*Изменения вступят в силу после перезапуска EPV.*



Установите флажок **Sort media files into folders accordingly album names during export/Сортировать медиафайлы по названиям альбомов во время экспорта** для более удобного доступа к экспортированным галереям мультимедиа с большим количеством файлов.

Если выбран этот параметр, изображения и видео будут распределяться по альбомам, аналогичным тем, что есть на устройстве.

### 4.1.2 Поддерживаемые резервные копии Apple

EPV поддерживает разные типы данных:

| Тип данных | Поддержка | Комментарии |
|---|---|---|
| Резервные копии iTunes без пароля | + | |
| Резервные копии iTunes без пароля с восстановленными именами файлов | + | |
| Резервные копии iTunes с паролем | + | Если пароль известен |
| Резервные копии iCloud | + | |
| Частичные резервные копии iCloud (было включено селективное скачивание) | + | Должна быть отмечена хотя бы одна категория данных |
| iCloud Photos | + | Фотографии, скачанные из iCloud, можно просматривать в **Elcomsoft Phone Breaker** |
| Синхронизированные данные iCloud | + | Можно просматривать в **Elcomsoft Phone Breaker**. |
| Образ файловой системы iOS | + | Можно извлечь посредством **Elcomsoft iOS Forensic Toolkit**. |

### 4.1.3 Данные Microsoft Account

EPV поддерживает наборы данных, скачанные при помощи Elcomsoft Phone Breaker из облака Microsoft.

В программе поддерживаются многочисленные типы данных, включая:

- Контакты
- Заметки (Microsoft OneNote)
- Сообщения (SMS)
- История звонков
- История браузера Edge и поисковых запросов Bing
- История местоположения
- Skype

Извлечь данные из Microsoft Account можно при помощи Elcomsoft Phone Breaker.

**Важно**: учётные записи Windows Live с доменом *microsoft.com* не поддерживаются.

## 4.2 Анализ данных Apple

### 4.2.1 Резервные копии iTunes

В состав резервных копий iTunes входят многочисленные и подробные данные о действиях пользователя. Состав резервных копий постоянно меняется; он зависит как от аппаратной

платформы и версии iOS, так и от настроек пользователя. Наконец, на доступность некоторых типов данных зависит от того, зашифрована ли резервная копия паролем.

Актуальная информация о составе резервных копий доступна в следующих статьях на сайте Apple:

Резервное копирование данных на устройствах iPhone, iPad и iPod touch

Сведения о резервных копиях данных iPhone, iPad и iPod touch

Зашифрованные резервные копии на iPhone, iPad или iPod touch

Если не удается создать на компьютере резервную копию данных устройства iOS или iPadOS либо восстановить данные из резервной копии

О местоположении резервных копий на диске рассказано в статье Поиск резервных копий iPhone, iPad и iPod touch:

- **macOS**: ~/Library/Application Support/MobileSync/Backup/
- **Windows 7, Windows 8, Windows 8.1, and Windows 10**: \Users\(username)\AppData\Roaming\Apple Computer\MobileSync\Backup\

Если вы запустите EPV на компьютере, где установлен iTunes, это позволит вам просматривать все хранящиеся там резервные копии.

Зашифрованные резервные копии обозначаются в EPV значком замка, а для их просмотра в EPV потребуется корректный пароль.

### 4.2.2 Резервные копии iCloud

Устройства под управлением iOS могут создавать резервные копии в облаке iCloud.

Так же, как и в случае с локальными резервными копиями, содержимое резервных копий в облаке радикально варьируется в зависимости от множества факторов. Так, многие типы данных, которые попадают в синхронизированный пул, исключаются из резервных копий - либо попадают в них, если пользователь отключит соответствующую настройку. Пример - **iCloud Photos/Фото из iCloud**. Если у пользователя включена синхронизация фотографий в облако, то фотографии не будут включаться в состав резервной копии iCloud, и наоборот. Также пользователь может вручную включать и выключать резервное копирование многочисленных категорий и данных отельных приложений.

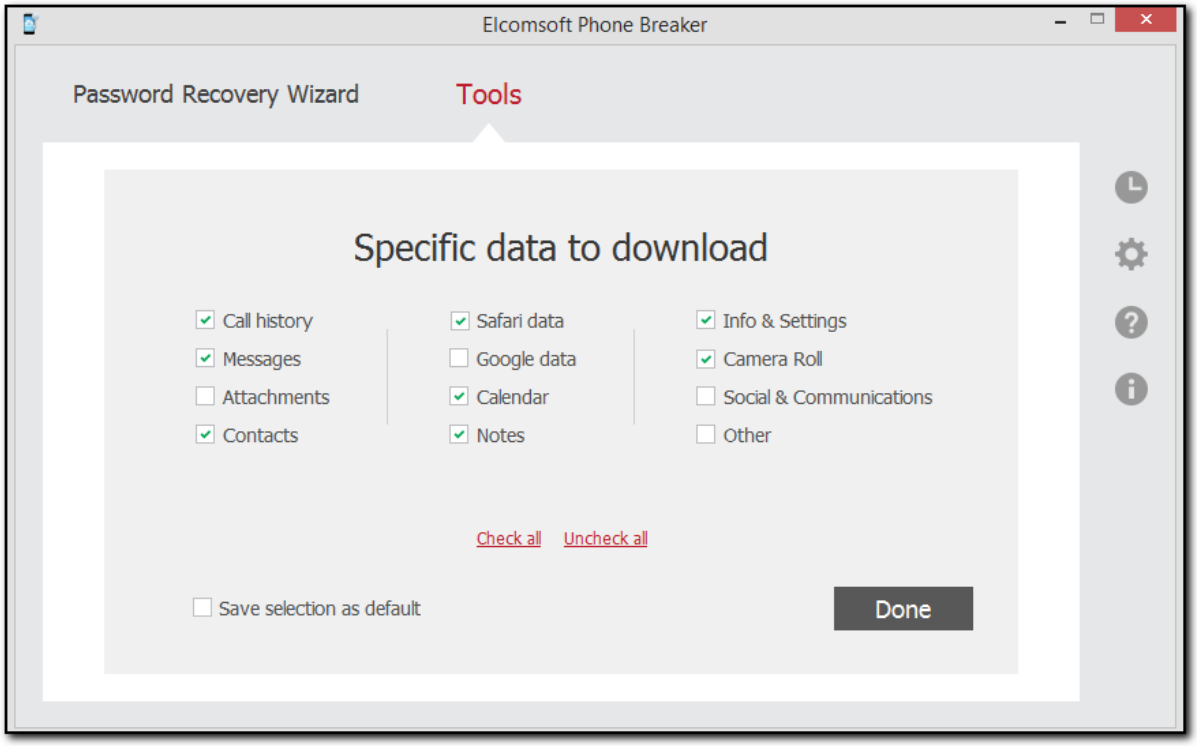
О содержимом резервных копий iCloud можно узнать на сайте Apple:

Содержимое резервных копий iCloud

Обратите внимание: при селективном скачивании данных при помощи Elcomsoft Phone Breaker необходимо отметить как минимум **Info & Settings/Информация и настройки** и ещё хотя бы одну категорию из списка:

- Call history/История звонков
- Messages/Сообщения
- Contacts/Контакты
- Calendar/Календарь

- Notes/Записи
- Safari data/Данные Safari
- Camera Roll/Фотопленка




### 4.2.3 Образ файловой системы iOS

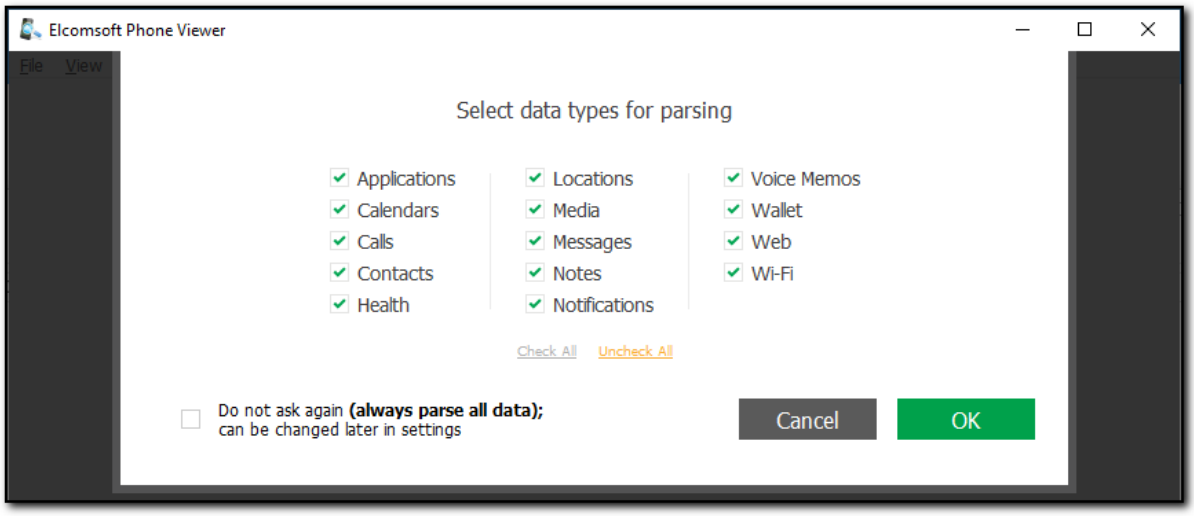
EPV поддерживает анализ образа файловой системы, извлечённого посредством Elcomsoft iOS Forensic Toolkit.

**Elcomsoft iOS Forensic Toolkit (EIFT)** включает в себя инструменты для извлечения образа файловой системы и расшифровки Связки ключей из устройств под управлением iOS и её вариаций (включая iPadOS и TvOS) как с установкой джейлбрейка, так и в ряде случаев без неё.

### 4.2.4 Анализ резервных копий iOS

Открыть резервную копию iOS можно из меню **File/Файл** > **Open/Открыть**, выбрав **iTunes backup/Рез. копия iTunes** либо **iCloud backup/Рез. копия iCloud.** Альтернативный способ - перетащить файл с резервной копией или файл Manifest.plist на главное окно программы.

1. *ПРИМЕЧАНИЕ. В macOS 10.14 и выше необходимо предоставить EPB разрешение на полный доступ к диску, чтобы иметь доступ к папке резервных копий iTunes по умолчанию.*
2. Выберите типы данных для анализа (впоследствии выбор можно изменить в окне настроек).




3. Укажите, должен ли EPV осуществлять поиск медиа-файлов за пределами Camera Roll (впоследствии можно изменить в окне настроек).

После загрузки резервной копии отображается служебная информация об устройстве и учётной записи пользователя:

- Версия iOS
- Серийный номер
- GUID
- IMEI
- Target Identifier
- Unique Identifier (обычно совпадает с предыдущим значением)
- Номер телефона
- Дата создания последней резервной копии
- Пароль Экранного времени или пароль ограничений

*ПРИМЕЧАНИЕ. Пароль ограничений доступен для зашифрованных, незашифрованных и расшифрованных резервных копий iOS 11 и более ранних версий. Пароль Экранного времени доступен для зашифрованных и расшифрованных резервных копий iOS 12.*

Нажмите на иконку соответствующего плагина для анализа соответствующей категории данных.
*ПРИМЕЧАНИЕ. Если базы данных некоторых приложений изменились во время обновления iOS, данные могут не отображаться при попытке просмотреть содержимое некоторых плагинов.*

**Экспорт данных из плагинов**
1. Нажмите **Export/Экспорт**.
2. Выберите данные плагинов, из которых вы хотите экспортировать, или нажмите **Check all/Выбрать все**.
3. При желании включите фильтрацию для экспорта данных за определенный период времени.
4. Нажмите **Export/Экспорт**.
5. Укажите путь, в котором будет сохранен файл с экспортированными данными, и нажмите **Save/Сохранить**.
7. Файл **<имя файла>.xlsx** сохраняется в выбранном месте.

EPV позволяет расшифровать защищенную паролем резервную копию iTunes при условии, что пароль известен.

### 4.2.5 Анализ образа файловой системы

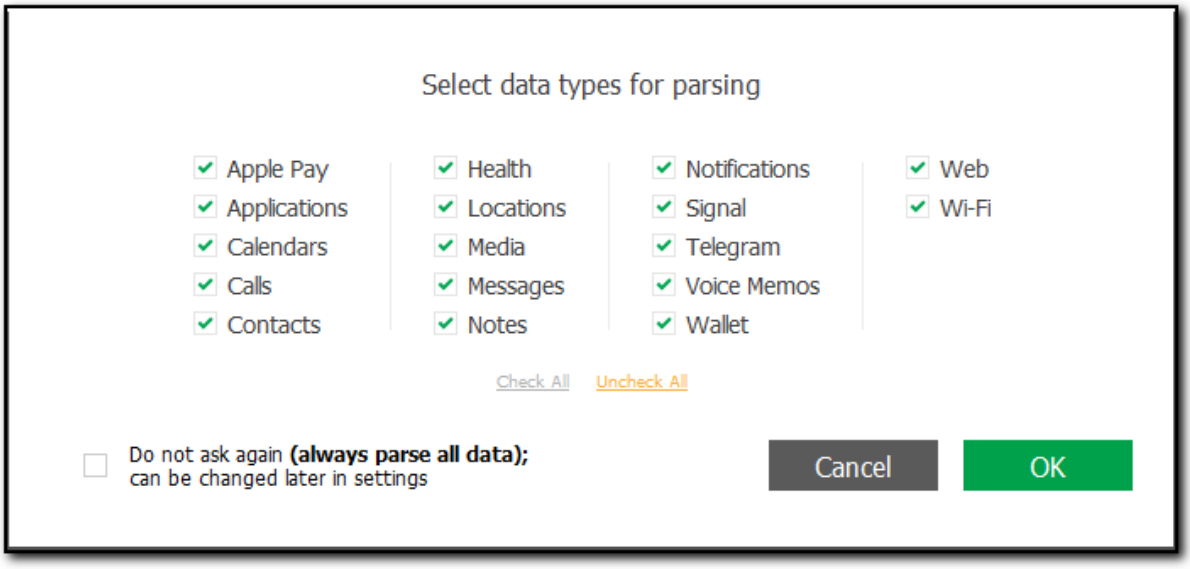
EPV позволяет просматривать содержимое образа файловой системы, извлечённое посредством Elcomsoft iOS Forensic Toolkit (EIFT). Поддерживаются следующие категории данных:

- **Apple Pay/Apple Pay**
- **Applications/Приложения**
- **Calendars/Календари**
- **Calls/Звонки**
- **Contacts/Контакты**
- **Health/Здоровье**
- **Locations/Локации**
- **Media/Медиафайлы**
- **Messages/Сообщения**
- **Notes/Записи**
- **Notifications/Уведомления**
- **Signal/Signal**
- **Telegram/Telegram**
- **Voice Memos/Диктофон**
- **Wallet/Wallet**
- **Web/Веб**
- **Wi-Fi/Wi-Fi**

*ПРИМЕЧАНИЕ: Для ускорения обработки рекомендуем временно отключить **Windows Defender**.*

Чтобы открыть образ файловой системы:

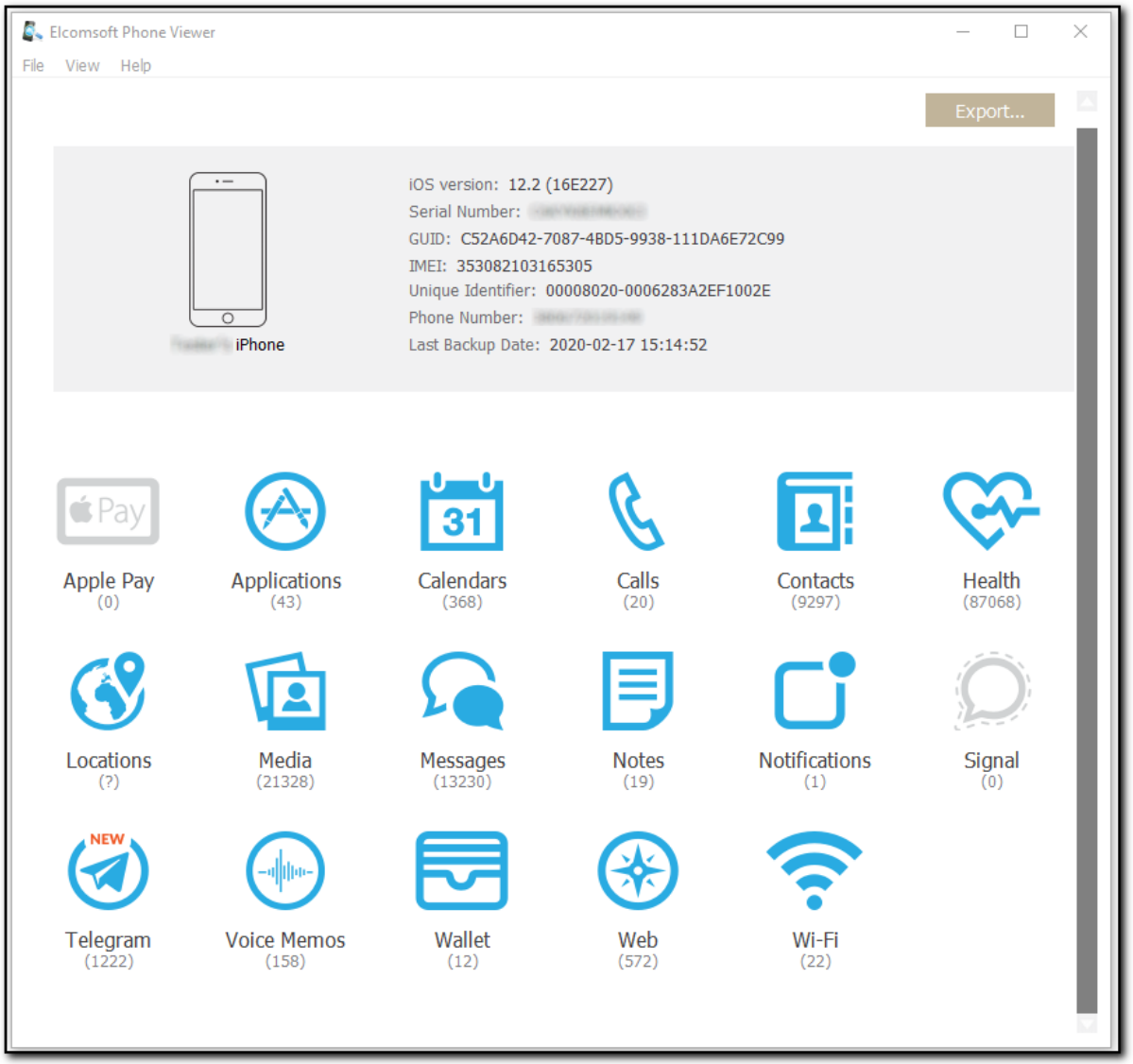
1. Выберите **iOS device image/Образ устройства iOS** в главном окне программы либо выберите **iOS device image/Образ устройства iOS** в меню **File/Файл** > **Open/Открыть** либо перетащите образ файловой системы на главное окно программы.
2. Выберите типы данных для анализа. Впоследствии выбор можно изменить в окне настроек.




3. Укажите, должен ли EPV осуществлять поиск медиа-файлов за пределами Camera Roll (впоследствии можно изменить в окне настроек).

После загрузки данных отображается служебная информация об устройстве и учётной записи пользователя:

- Версия iOS
- Серийный номер
- GUID
- IMEI
- Unique Identifier
- Дата создания последней резервной копии
- Пароль Экранного времени или пароль ограничений




**Экспорт данных из плагинов**

1. Нажмите **Export/Экспорт**.
2. Выберите данные плагинов, из которых вы хотите экспортировать, или нажмите **Check all/Выбрать все**.
3. При желании включите фильтрацию для экспорта данных за определенный период времени.
4. Нажмите **Export/Экспорт**.
5. Укажите путь, в котором будет сохранен файл с экспортированными данными, и нажмите **Save/Сохранить**.
7. Файл **<имя файла>.xlsx** сохраняется в выбранном месте.

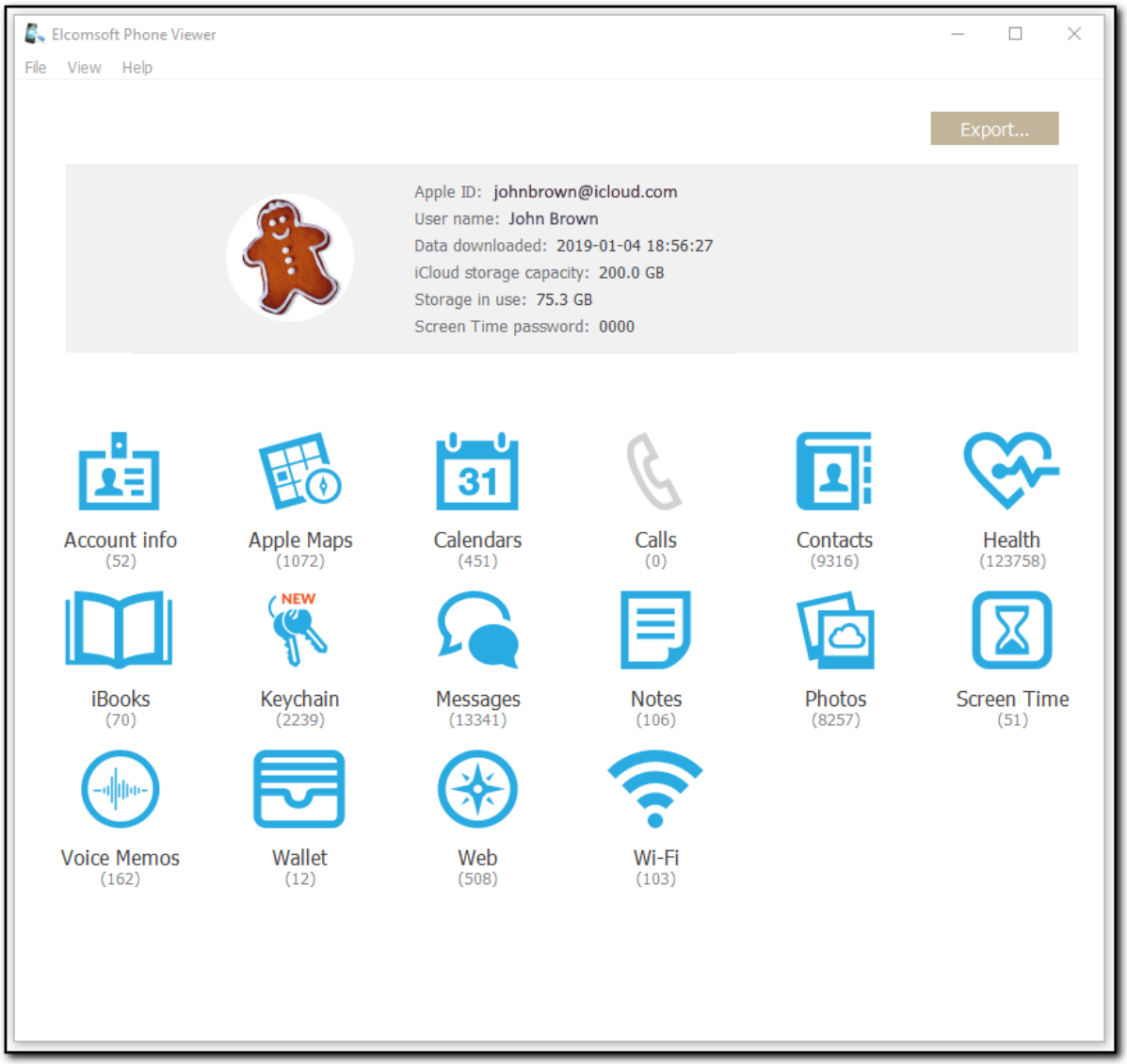
### 4.2.6 Анализ синхронизированных данных iCloud

EPV позволяет просматривать синхронизированные данные, скачанные из облака iCloud посредством Elcomsoft Password Breaker. Поддерживаются следующие категории данных:

- **Account info/Учетная запись**
- **Apple Maps/Карты Apple**
- **Calendars/Календари**
- **Calls/Звонки**
- **Contacts/Контакты**
- **Health/Здоровье**
- **iBooks/iBooks**
- **Keychain/Связка ключей**
- **Messages/Сообщения**
- **Notes/Записи**
- **Photos/Фото**
- **Screen Time/Экранное время**
- **Voice Memos/Диктофон**
- **Wallet/Wallet**
- **Web/Веб**
- **Wi-Fi/Wi-Fi**

Чтобы открыть синхронизированные данные, выберите **iCloud synced data/Синхр. данные iCloud** в главном окне программы либо выберите **iCloud synced data/Синхр. данные iCloud** в меню **File/Файл** > **Open/Открыть** либо перетащите файл **icloud_synced.xml** на главное окно программы.

После загрузки синхронизированных данных отображается информация о учётной записи пользователя:
- Apple ID
- Имя пользователя
- Время и дата скачивания
- Общий объём хранилища пользователя в iCloud
- Объем данных в iCloud
- Пароль Экранного времени




**Экспорт данных из плагинов**

1. Нажмите **Export/Экспорт**.
2. Выберите данные плагинов, из которых вы хотите экспортировать, или нажмите **Check all/Выбрать все**.
3. При желании включите фильтрацию для экспорта данных за определенный период времени.
4. Нажмите **Export/Экспорт**.
5. Укажите путь, в котором будет сохранен файл с экспортированными данными, и нажмите **Save/Сохранить**.
7. Файл **<имя файла>.xlsx** сохраняется в выбранном месте.

# 4.3 Анализ данных Microsoft Account

## 4.3.1 Данные Microsoft Account

Чтобы открыть данные Microsoft Account, скачанные при помощи Elcomsoft Phone Breaker, воспользуйтесь командой **Microsoft account data/Учётные данные Microsoft** из меню **File/Файл** > **Open/Открыть** либо перетащите файл с данными на главное окно EPV.

После того, как данные в резервной копии будут проанализированы, программа отобразит следующую информацию:

- Образ устройства (общий)
- Модель устройства
- Идентификатор устройства
- Номер телефона (при наличии)
- Дата резервного копирования (фактически дата извлечения данных с помощью Elcomsoft Phone Breaker)

ПРИМЕЧАНИЕ. Данные могут содержать информацию с нескольких устройств, подключенных к учётной записи Microsoft. В этом случае вы можете переключаться между устройствами, используя стрелки (слева и / или справа) или зеленую точку в нижней части экрана.

# 4.4 Плагины

## 4.4.1 Просмотр, поиск и анализ данных

Elcomsoft Phone Viewer предназначен для просмотра и анализа данных, извлечённых посредством таких инструментов, как Elcomsoft Phone Breaker и Elcomsoft iOS Forensic Toolkit, а также файлов в стандартных форматах - например, резервных копий в формате iTunes (как с паролем, так и без него) и образов файловой системы, сохранённых в архивах TAR или ZIP.

В зависимости от типа анализируемых данных могут быть доступны те или иные категории. В текущей версии EPV поддерживаются следующие категории, просмотр которых реализован посредством модулей-плагинов:

- Информация об учётной записи
- Apple Pay
- Apple Maps
- Приложения
- Календари
- Журнал звонков
- Контакты
- Здоровье
- Books
- Связка ключей Keychain (только для данных, скачанных из iCloud)
- История местоположений
- Мультимедиа-файлы (фотографии и видео, в том числе из вложений)
- Сообщения
- Заметки
- Уведомления
- Программы мгновенного обмена сообщениями Signal, Skype и Telegram
- Голосовые заметки

- Пароль Экранного времени
- Кошелёк Wallet
- Web
- Wi-Fi

Для данных в плагинах доступны поиск, фильтрация и экспорт.

**Поиск и фильтрация**

Чтобы запустить поиск, введите поисковый запрос в соответствующее поле в окне плагина и нажмите Enter. Результат будет подсвечен жёлтым.

Запуск фильтрации осуществляется нажатием на иконку  .
Нажмите на переключатель, чтобы включить или выключить фильтрацию, после чего настройте фильтрацию (вводом строки текста, указанием диапазона дат и т.п., в зависимости от конкретного плагина).

*ПРИМЕЧАНИЕ. При использовании параметров фильтрации вы сможете просматривать только записи, разрешенные вашим типом лицензии.*

## 4.4.2 Экспорт данных

Большинство расширений поддерживает экспорт данных. Для того, чтобы экспортировать данные той или иной категории, проделайте следующие шаги.

1. В окне соответствующего расширения нажмите **Export/Экспорт**.
2. Выберите **All/Все**, чтобы экспортировать все данные.
3. Выберите файл в окне **Select destination file/Выбрать файл назначения** и укажите путь к файлу.
4. Нажмите **Save/Сохранить**.

В расширениях используются стандартные форматы файлов, включая .xml и .xlsx.

## 4.4.3 Связка ключей

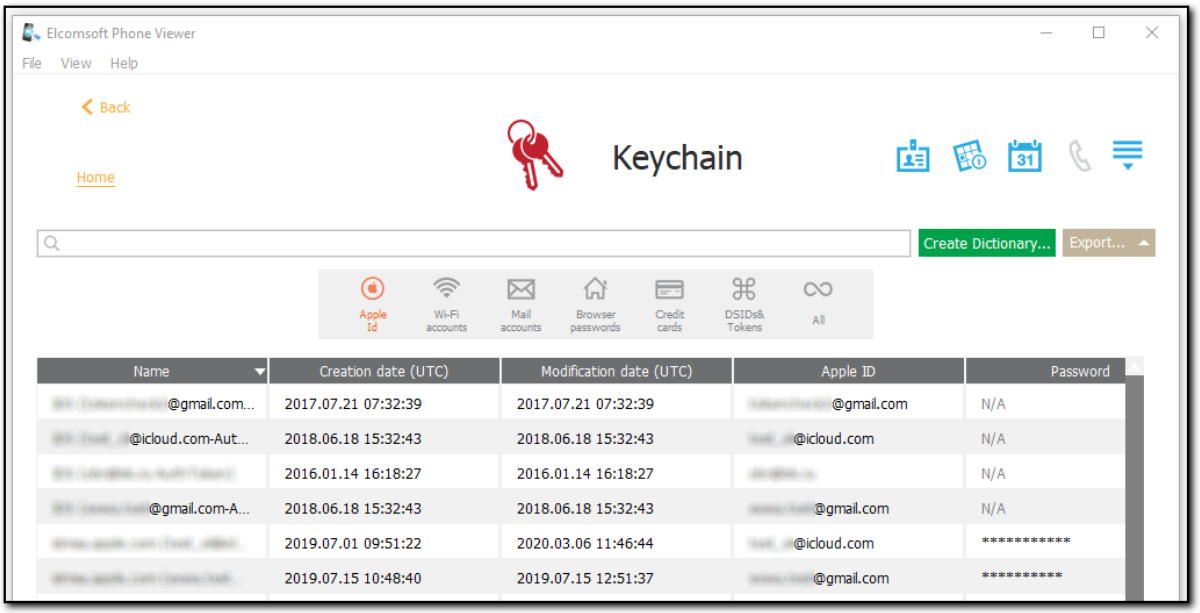
Этот плагин позволяет исследовать данные связки ключей, такие как пароли Apple ID, пароли Wi-Fi, пароли почтовых учетных записей, данные кредитной карты и т.д.

*ПРИМЕЧАНИЕ. Этот плагин доступен только для синхронизированных данных iCloud, загруженных EPB.*

*ПРИМЕЧАНИЕ. Чтобы демаскировать пароли, номера карт, токены и хеш-значения, снимите флажок «Маскировать пароли в связке ключей» в настройках.*

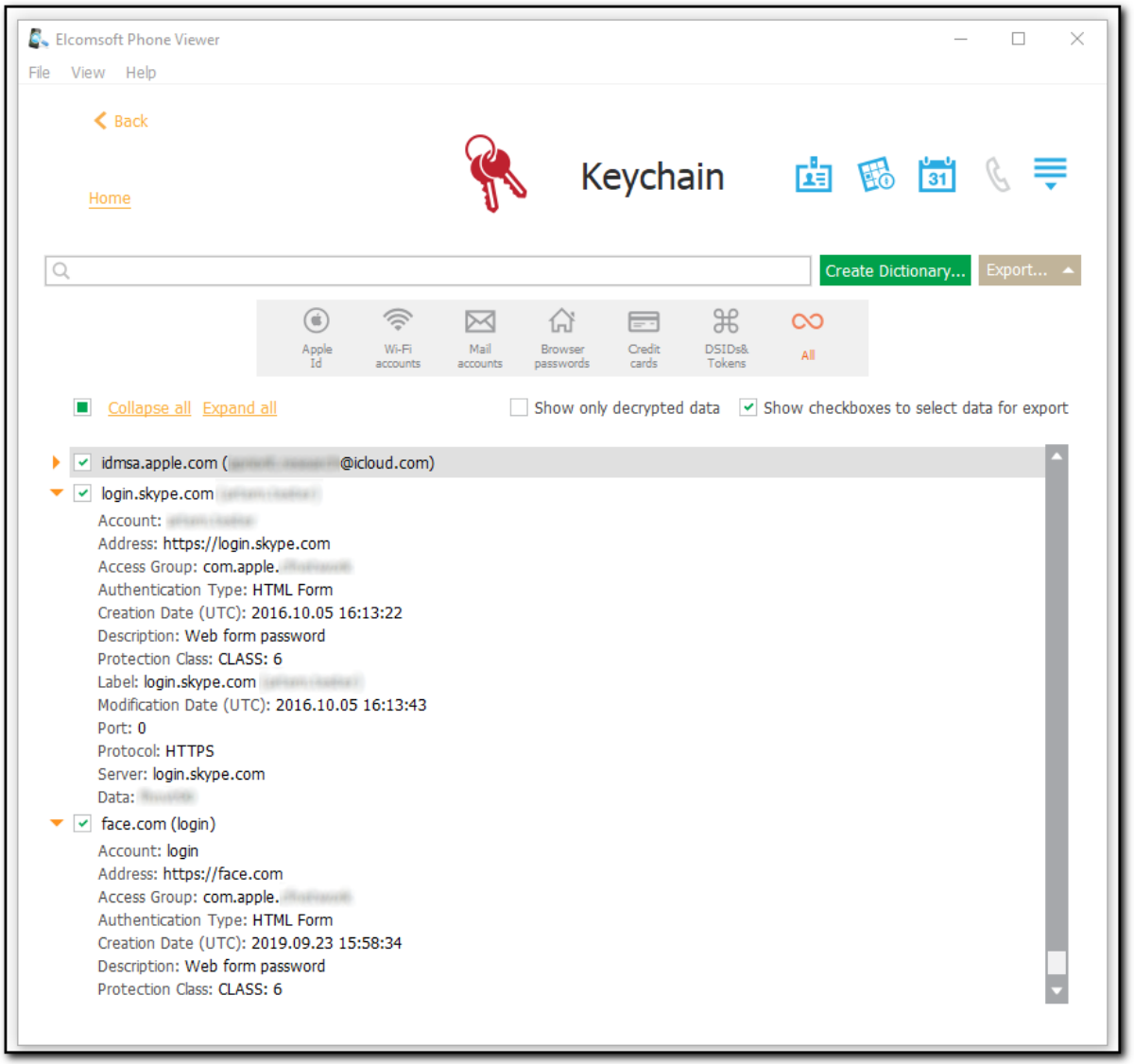
Большинство вкладок (**Wi-Fi accounts/Аккаунты Wi-Fi**, **Mail accounts/Почт. аккаунты**, **Browser passwords/Пароли браузеров** и т.д.) не нуждается в пояснениях. Отдельного упоминания заслуживает две вкладки.

Вкладка **Apple ID** содержит данные, которые относятся к идентификаторам учётной записи Apple (Apple ID). Обратите внимание: на устройстве может одновременно использоваться несколько Apple ID с разными идентификаторами. С высокой вероятностью именно в этой вкладке можно обнаружить пароли и маркеры аутентификации от различных Apple ID пользователя.




Вкладка **All/Все** содержит все доступные данные в древовидном представлении. При исследовании данных доступны следующие опции:

- **Collapse all/Свернуть все** сворачивает все развёрнутые ветки дерева.
- **Expand all/Развернуть все** разворачивает все ветки.
- Иконка разворачивает выбранную ветку.
- **Show only decrypted data/Показать только расшифров. записи** отображает только те записи, которые были успешно расшифрованы (рекомендованный режим).
- **Show checkboxes to select data for export/Показать опции выбора данных для экспорта** позволяет выбирать данные для последующего экспортирования.




### Создание словаря

**EPV** позволяет создавать словари, которые можно использовать для попытки восстановления зашифрованных файлов пользователя.

Для создания словаря:
1. Нажмите **Create Dictionary/Создать словарь.**
2. Откроется окно **Select destination file/Выбрать файл назначения.**
3. Выберите место на диске, куда будет сохранён файл.
4. Нажмите **Save/Сохранить.**
5. Текстовый файл **<file name>.txt** сохраняется.

### Экспорт данных

Для экспорта Связки ключей нажмите **Export/Экспорт** и укажите путь к файлу. Вы сможете выбрать между экспортированием всего содержимого или только выбранных веток. Данные сохраняются в формате **XML**.

### 4.4.4 Доступные данные

В плагинах отображаются данные соответствующих категорий. Ниже перечислены типы данных, доступные для каждого плагина.

### Информация об учётной записи / Account Info

В этой категории содержатся данные, которые относятся к учётной записи пользователя, такие, как логин и пароль, идентификатор учётной записи, наличие двухфакторной аутентификации, время последней смены пароля и др.

*Только для данных, синхронизированных из iCloud.*

### Apple Pay

Плагин Apple Pay позволяет просматривать данные приложения Apple Pay, в том числе информацию о картах и транзакциях.

*ПРИМЕЧАНИЕ. Этот плагин доступен только для образа файловой системы (.tar) устройств iOS с установленным кодом блокировки.*

### Карты / Apple Maps

Плагин Apple Maps позволяет просматривать такую информацию, как подробная история поиска в приложении Карты, информацию о закладках, точках POI и проложенных маршрутах.

*ПРИМЕЧАНИЕ. Этот плагин доступен только для данных, синхронизированных в iCloud.*

### Приложения / Applications

Данный плагин позволяет просматривать информацию о приложениях, установленных на устройстве.

*ПРИМЕЧАНИЕ. Этот плагин доступен только для данных из iOS 7.x.x и более поздних версий.*

При открытии плагина вам будет предложено загрузить дополнительную информацию о приложениях из Интернета. Обратите внимание, что для получения дополнительной информации требуется подключение вашего компьютера к Интернету.

### Календари / Calendars

Здесь можно просмотреть события, запланированные во всех календарях независимо от учетной записи, используемых пользователем устройства. В список входят как разовые, так и регулярные мероприятия, дни рождения, праздники и т.д. Обратите внимание, что для повторяющихся событий/встреч отображается только первый день мероприятия.

## Журнал звонков / Calls

EPV позволяет просматривать историю входящих и исходящих вызовов исследуемого устройства. Вы можете проанализировать полную историю исходящих, входящих, пропущенных и неотвеченных звонков. Доступна информация о том, был ли звонок сделан по телефону или через сторонние сервисы (Skype, WhatsApp, Viber или FaceTime).

## Контакты / Contacts

Этот плагин показывает все контакты из всех адресных книг пользователя. Сюда могут входить как локальные контакты устройства, так и контакты из учетных записей Exchange/Outlook, iCloud, Gmail и другие, если они синхронизированы с устройством. Выберите контакт в левой части панели, и вся доступная для него информация будет показана в правой части.

## Здоровье / Health

Данный плагин позволяет проанализировать данные приложения Здоровье (Apple Health). Это приложение агрегирует большое количество специфических категорий, включающих сведения о физической активности пользователя, циклах сна, особенностях питания и т.д. Обратите внимание: многие категории данных доступны лишь в том случае, если пользователь подключил одно или несколько внешних устройств, совместимых с протоколом HealthKit (например, фитнес-браслет, часы Apple Watch, внешние датчики и т.п.)

ПРИМЕЧАНИЕ. Этот плагин доступен для синхронизированных данных iCloud, образа файловой системы iOS и резервных копий iTunes с паролем.

## Книги / Books

Несмотря на название, данный плагин отображает не только информацию об электронных книгах, приобретённых в официальном магазине Apple, но и файлах, которые пользователь скачал вручную - например, книги в формате ePub или файлы Adobe PDF.

## Связка ключей / Keychain

Этот плагин позволяет исследовать данные связки ключей, такие как пароли Apple ID, пароли Wi-Fi, пароли почтовых учетных записей, данные кредитной карты и т.д. Описанию этого плагина посвящена отдельная глава Связка ключей.

*ПРИМЕЧАНИЕ. Этот плагин доступен только для синхронизированных данных iCloud, загруженных EPB.*

*ПРИМЕЧАНИЕ. Чтобы демаскировать пароли, номера карт, токены и хеш-значения, снимите флажок «Маскировать пароли в связке ключей» в настройках.*

## История местоположений / Locations

Данный плагин отображает одну из самых важных категорий данных - историю местоположений пользователя. Данные о местоположении пользователя извлекаются из резервных копий iOS и образов файловой системы устройств iOS, полученных с помощью Elcomsoft iOS Forensic Toolkit. В зависимости от типа исходных данных (резервная копия или образ файловой системы) данные о местоположении могут извлекаться как из метаданных EXIF фотографий, так и из других источников.

При открытии данного модуля вы сможете выбрать, использовать ли данные о местоположении точек доступа Wi-Fi и других источников, помимо метаданных фотографий. Обратите внимание, что для получения данных о местоположении Wi-Fi в первый раз требуется подключение к Интернету. После загрузки данных о местоположении Wi-Fi они сохраняются в локальный кеш. Процесс скачивания этих данных блокирующий: вы не сможете открывать другие плагины, пока процесс не будет завершен.

В процессе просмотра и анализа данных о местоположении вы сможете использовать как табличное представление, так и визуальное отображение точек на карте.

## Мультимедиа-файлы / Media

Данный плагин предназначен для анализа фотографий и видео, в том числе из вложений, которые извлекаются из резервных копий устройств. Обратите внимание: для анализа фотографий, извлечённых в виде синхронизированных данных из iCloud, предназначен отдельный плагин **Фотографии / Photos**.

## Фотографии / Photos

Данный плагин позволяет анализировать ленту фотографий, скачанную из облака iCloud, если пользователь включил сервис iCloud Photos. Для анализа фото- и видео файлов из резервных копий используйте плагин **Мультимедиа-файлы / Media**.

## Сообщения / Messages

Этот плагин позволяет просматривать историю сообщений пользователя .

В левой части панели отображаются контакты (номер телефона, имя или адрес электронной почты - в зависимости от типа общения).

Вы можете просматривать следующие типы сообщений для каждого контакта:

| Тип сообщений | iOS резервные копии/образ файловой системы | iCloud (синхронизированные данные) | Microsoft Account | Комментарий |
|---|---|---|---|---|
| SMS | + | + | + | |
| MMS | + | + | - | |
| iMessage | + | + | - | |
| Handwriting | + | - | - | Только iOS 10 и выше |
| Digital Touch | + | - | - | Только iOS 10 и выше |
| Reactions | + | - | - | Только iOS 10 и выше |
| Effects | + | - | - | Только iOS 10 и выше |
| Stickers | + | + | - | Только iOS 10 и выше |

Входящие сообщения отображаются в левой части экрана, а исходящие - в правой. Количество сообщений для каждого контакта показано (в скобках). Можно просматривать как обычные, так и групповые чаты.

Смайлы отображаются как в текстах сообщений, так и в контактах (они также поддерживаются другими плагинами).

Для устройств iOS сообщения SMS отображаются зеленым цветом, MMS - серым, а iMessages - синим.

## Заметки / Notes

Для всех заметок отображаются дата и время создания и последнего обновления, папка, в которой она хранится, и первые две строки текста сообщения. Заметки отсортированы по дате последнего изменения.

EPV отображает в том числе удалённые заметки в синхронизированных данных iCloud, загруженных с помощью Elcomsoft Phone Breaker. Удалённые заметки помечаются красным значком корзины и могут принадлежать к следующим папкам:

- **Недавно удалённые**: системная папка, содержащая заметки, удаленные пользователем.
- **Восстановленные**: папка, содержащая заметки, удалённые из папки «Недавно удаленные» на устройстве и восстановленные с помощью EPV.

## Уведомления / Notifications

Этот плагин позволяет просматривать сохранённые в резервных копиях старых версий iOS push-уведомления пользователя, которые используются приложениями для информирования о различных типах обновлений.

*ПРИМЕЧАНИЕ. Этот плагин доступен только для резервных копий iOS 7.x - 10.x следующих типов: iCloud и iTunes (зашифрованные, не зашифрованные и резервные копии с восстановленными именами файлов). Начиная с iOS 11, уведомления перестали сохраняться в резервных копиях.*

## Программы мгновенного обмена сообщениями Signal, Skype и Telegram

Здесь вы сможете просмотреть историю общения пользователя в программах мгновенного обмена сообщениями Signal, Skype и Telegram. Обратите внимание: просмотр истории Signal и секретные чаты Telegram доступны исключительно при анализе образа файловой системы устройства (эти данные не попадают в резервные копии).

## Голосовые заметки / Voice Memos

Этот плагин позволяет просматривать данные встроенного в iOS приложения Voice Memos.

*ПРИМЕЧАНИЕ. Этот плагин доступен для резервных копий iCloud и iTunes iOS 3.1.3 - 12 и выше, образов устройств iOS и синхронизированных данных iCloud (iOS 12 и выше, MacOS 10.14 и выше, watchOS 6 и iPadOS 13).*

## Данные Экранного времени / Screen Time

Этот плагин позволяет вам просматривать информацию системной функции Экранное время / Screen Time. В их состав входят ограничения устройств, время, потраченное на использование приложений, веб-сайтов и т.д.

*ПРИМЕЧАНИЕ. Этот плагин доступен только для синхронизированных данных iCloud 5.x.x и выше.*

### Кошелёк / Wallet

Плагин Wallet позволяет просматривать информацию из приложения Apple Wallet - посадочные талоны, дисконтные и бонусные карты, электронные билеты, брони и т.п.

*ПРИМЕЧАНИЕ. Этот плагин доступен при анализе образов файловой системы устройств iOS, резервных копий iOS и синхронизированных данных iCloud.*

### Web

Данные об активности пользователя в веб-браузерах. Для резервных копий iOS данные берутся из браузера Safari и включают закладки, историю посещений, двадцать последних поисковых запросов и вкладки посещенных страниц. Для данных из учетной записи Microsoft данные берутся из браузера Edge и включают историю посещений и поиска.

### Wi-Fi

Плагин Wi-Fi позволяет просматривать информацию об обнаруженных и сохраненных соединениях Wi-Fi.

*ПРИМЕЧАНИЕ. Только для резервных копий iOS 7.x и выше.*

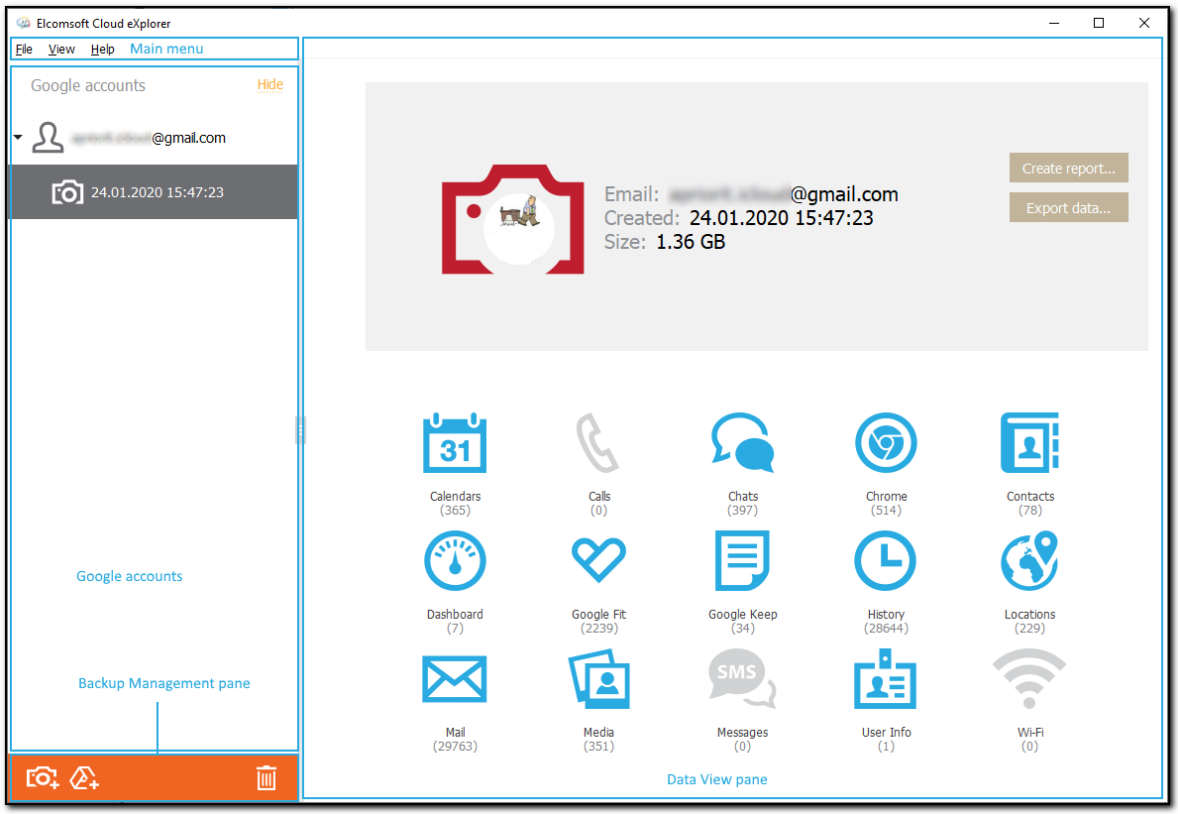
При открытии данного модуля вы сможете запросить данные о местоположении точек доступа Wi-Fi. Обратите внимание, что для этого требуется подключение к Интернету. После загрузки данных о местоположении Wi-Fi они сохраняются в локальный кеш. Процесс скачивания этих данных блокирующий: вы не сможете открывать другие плагины, пока процесс не будет завершен.

# V Elcomsoft Cloud Explorer

## 5.1 О программе

### 5.1.1 Пользовательский интерфейс

Пользовательские интерфейс Elcomsoft Cloud eXplorer состоит из главного меню и нескольких панелей. В панели просмотра данных отображаются скачанные данные; в панели учётных данных Google - данные аккаунтов Google и Google Drive, добавленных в ECX. Наконец, в панели управления резервными копиями отображаются наборы данных, скачанные для каждой учётной записи.

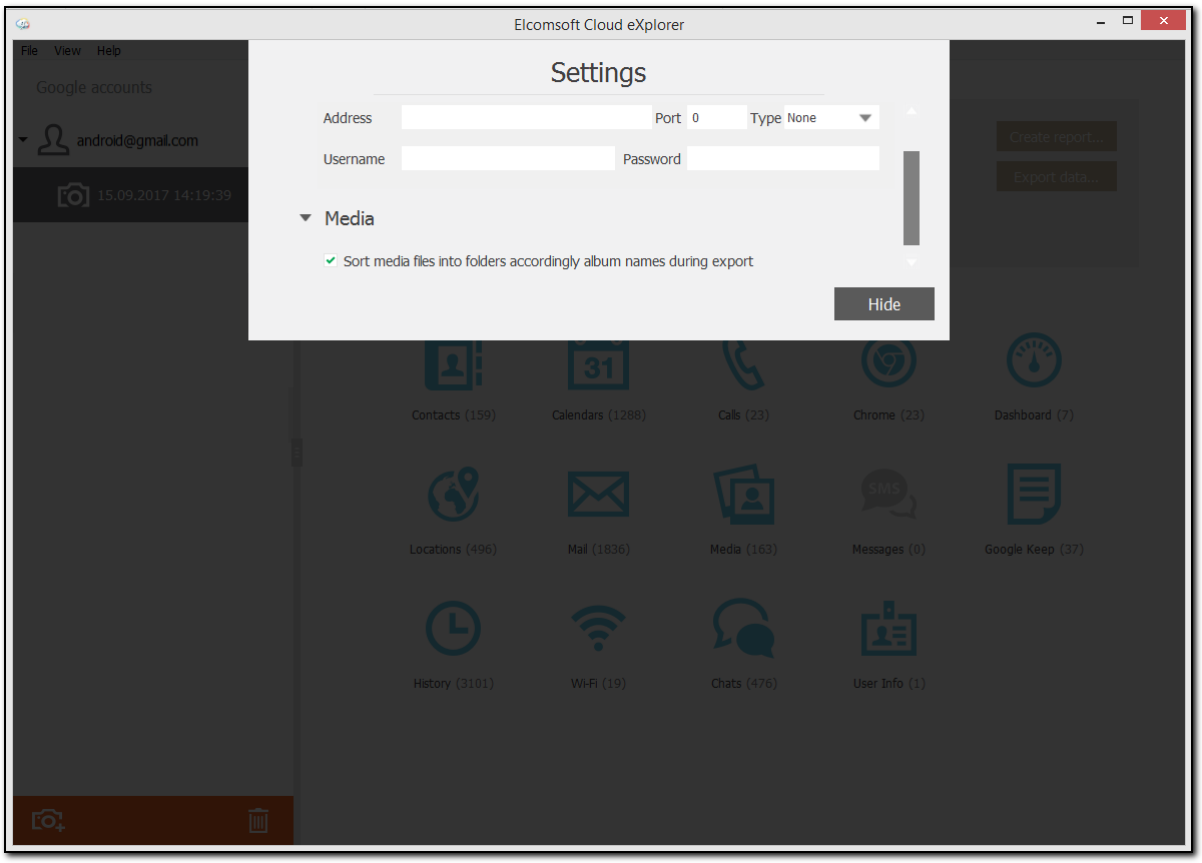



## 5.1.2 Окно настроек

В окне настроек можно указать адрес и настройки прокси-сервера, а также включить или выключить сортировку скачанных медиа-файлов по папкам. Если сортировка включена, то скачанные медиа-файлы будут сохраняться в папках, имена которых будут соответствовать именам альбомов.

Окно настроек доступно в меню **View/Вид - Settings/Настройки.**

**ПРИМЕЧАНИЕ. Поддерживаются только сквозные прокси-серверы. Прокси с подменой сертификата не поддерживаются.**




### 5.1.3 Изменение пути к хранилищу

По умолчанию ECX сохраняет скачанные данные в следующих папках:

- ***Windows:*** *C:\Users**имя_пользователя**\AppData\Elcomsoft\Elcomsoft Cloud eXplorer\Backups*
- ***macOS:*** *~/Library/Application Support/Elcomsoft/Elcomsoft Cloud eXplorer/Backups*

Изменить местоположение этих файлов можно, отредактировав файл *settings.ini,* расположенный в папке ECXL:

***Windows:*** *C:\Users**имя_пользователя**\AppData\Roaming\Elcomsoft\Elcomsoft Cloud eXplorer*

- ***macOS:*** *~/Library/Application Support/Elcomsoft/Elcomsoft Cloud eXplorer*

ПРИМЕЧАНИЕ. Папка AppData по умолчанию скрыта. Убедитесь, что скрытые папки отображаются в вашей системе.

# 5.2 Данные из Google Account

## 5.2.1 Аутентификация

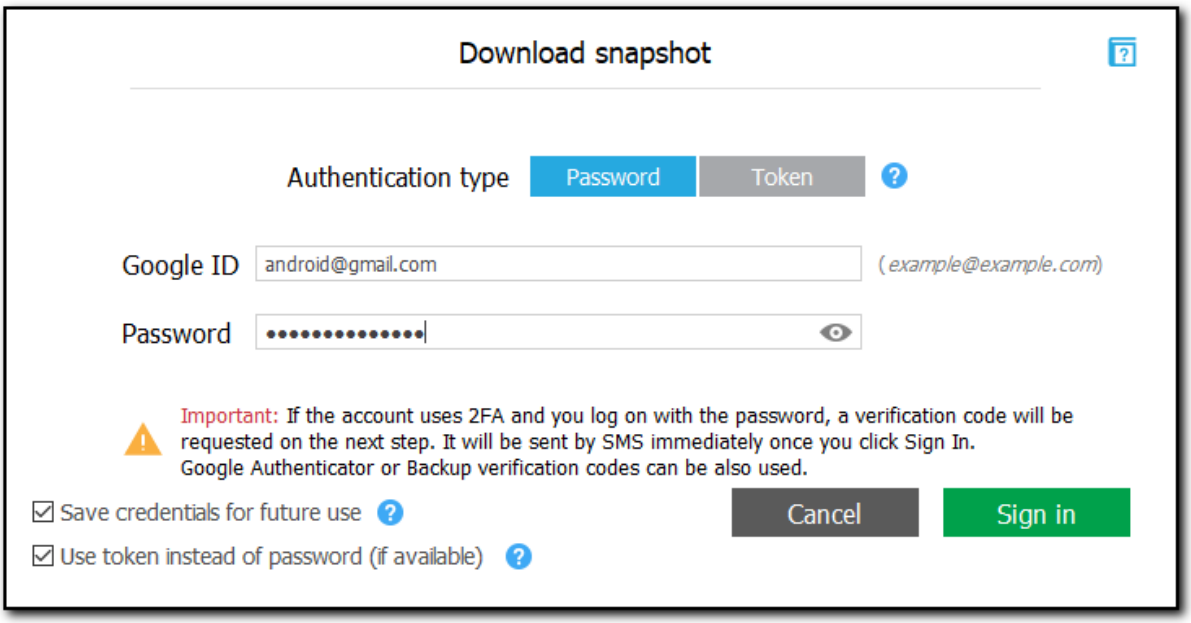
Для скачивания данных вам необходимо пройти аутентификацию в учётную запись пользователя. Процесс аутентификации может различаться в зависимости от настроек безопасности учетной записи Google.

Выберите тип аутентификации: посредством логина и пароля (вкладка **Password/Пароль**) либо маркера аутентификации (вкладка **Token/Токен**).

**Вход при помощи логина и пароля**
Процедура аутентификации не отличается от любой другой процедуры входа в учётную запись при помощи логина и пароля. В качестве логина Google ID чаще всего выступает email-адрес пользователя в формате account@gmail.com.

Если выбрать опцию **Save credentials for future use/Сохранить учётные данные**, ECX сохраняет свой собственный маркер аутентификации для ускорения последующих сессий. Чтобы использовать маркер при следующем входе в эту учетную запись, введите логин и убедитесь, что выбрана опция **Use token instead of password (if available)/Использовать токен вместо пароля (если есть)**. При входе в систему с помощью маркера вам не нужно использовать пароль или проходить двухэтапную проверку.

ПРИМЕЧАНИЕ. ECX не поддерживает учетные записи Google с защитой CAPTCHA. Вы можете подождать некоторое время, пока защита CAPTCHA не будет отключена, после чего попробовать снова войти в систему.

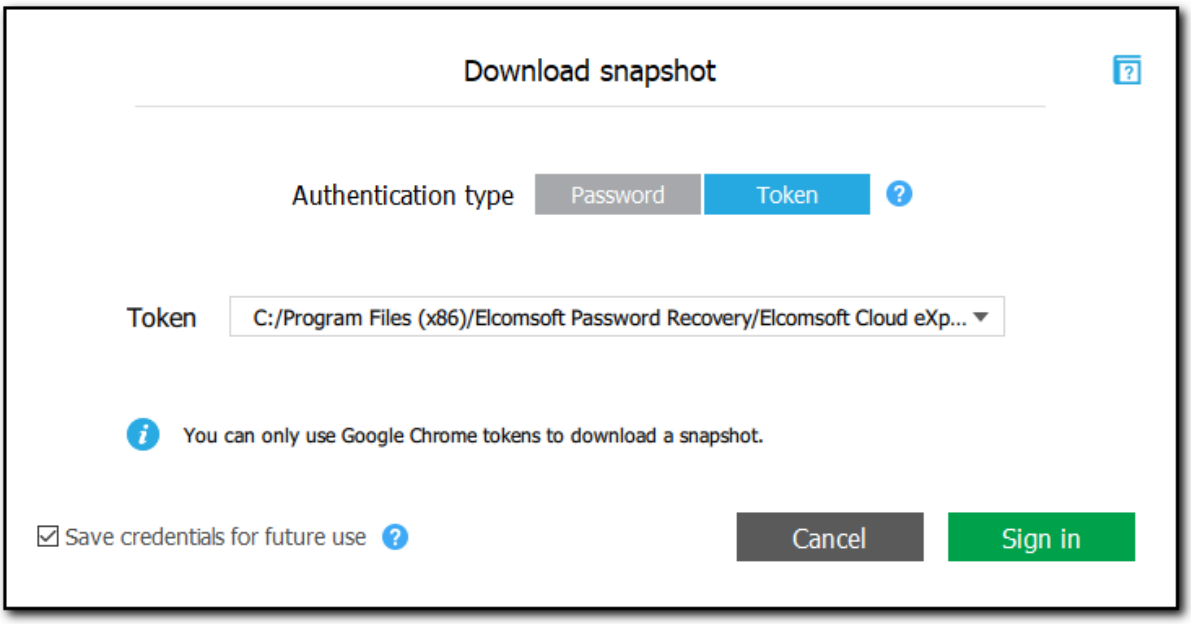



**Вход при помощи маркера аутентификации**
Если вы входите в систему с помощью маркера аутентификации, выберите ранее сохраненный маркер из списка или укажите путь к новому XML-файлу маркера, извлеченному из браузера Google Chrome при помощи утилиты Google Token Extractor (GTEX). По умолчанию этот файл сохраняется в папке, в которой расположен Google Token Extractor.

Когда вы входите в систему с выбранной опцией **Save credentials for future use/Сохранить учётные данные**, ECX сохраняет маркер, и вы можете выбрать его из списка при следующем входе в систему.

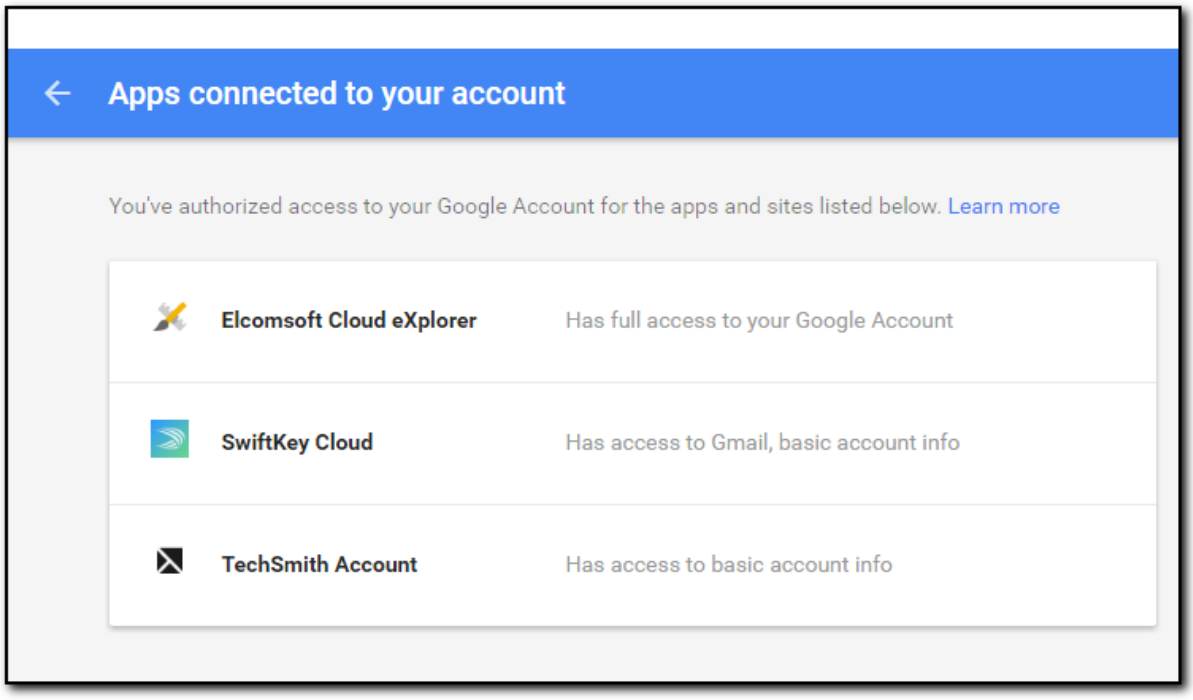
**ПРИМЕЧАНИЕ. Если вы войдете в систему в этом режиме, следующие категории будут недоступны для загрузки: User Info/Информация о пользователе, Contacts/Контакты, Locations/Локации, Media/Медиафайлы, Mail/Почта, Messages/Сообщения.**

**ПРИМЕЧАНИЕ**. Для загрузки данных из учетных записей Google можно использовать только маркеры, извлеченные из браузера Google Chrome.



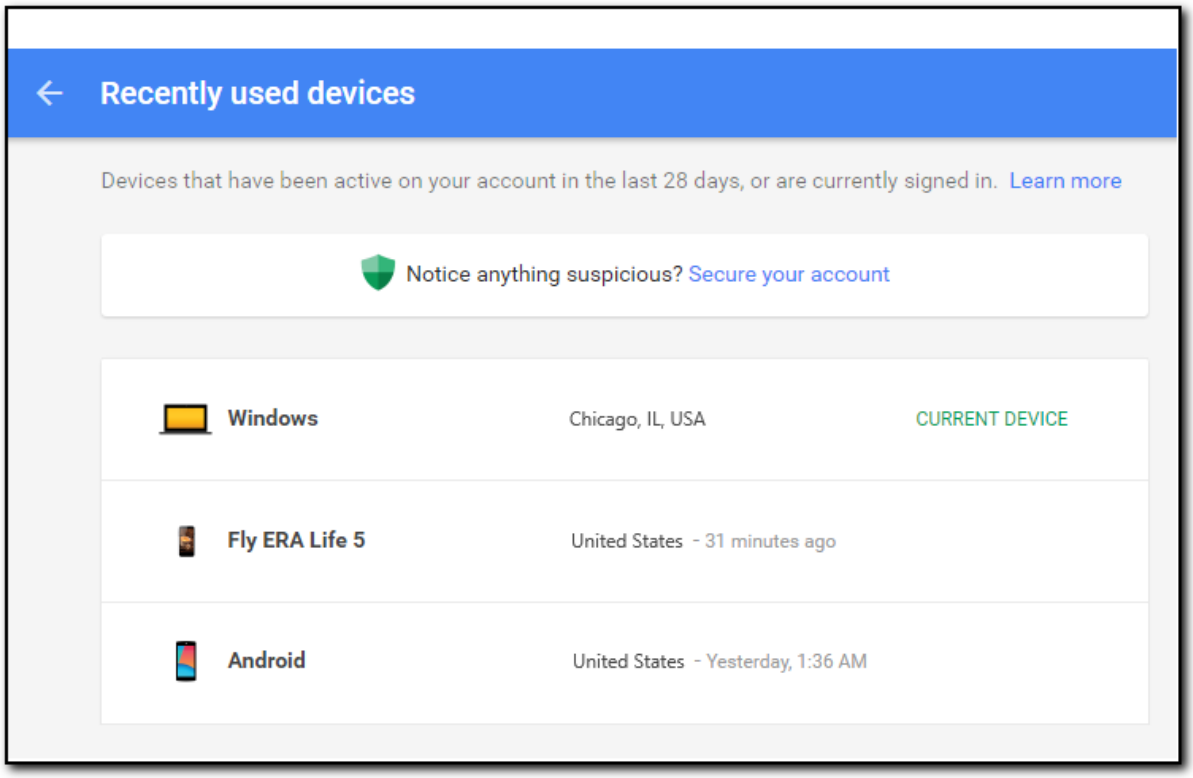

### Уведомления о безопасности

Когда вы входите в систему через ECX, информация об этом входе отображается в учётной записи Google пользователя. Elcomsoft Cloud eXplorer появится в списке приложений и сайтов с авторизованным доступом к учетной записи.




Если вы войдете в систему через ECX, используя логин и пароль, пользователь получит уведомление по электронной почте для той учетной записи Google, в которую вы вошли. Также появится дополнительное уведомление в учетной записи Google в списке недавно использованных устройств. В этом списке упоминания ECX не появится, но в списке устройств, которые недавно вошли в учетную запись, будет устройство с Windows или неизвестной ОС.

Кроме того, в списке появится запись о неизвестном устройстве Android в том случае, если вы загружаете данные из категорий **Calls/Звонки** и **Wi-Fi**.




Наконец, если вы входите в учётную запись с IP-адреса, с которого вы ранее в неё не входили, пользователь получит уведомление по электронной почте с информацией о новом входе.

### 5.2.2 Скачивание динных из Google Account

С помощью ECX вы можете загрузить информацию из учетной записи Google, сохранить ее в виде резервной копии, а затем анализировать её содержимое без подключения к интернету.

Доступны следующие категории:

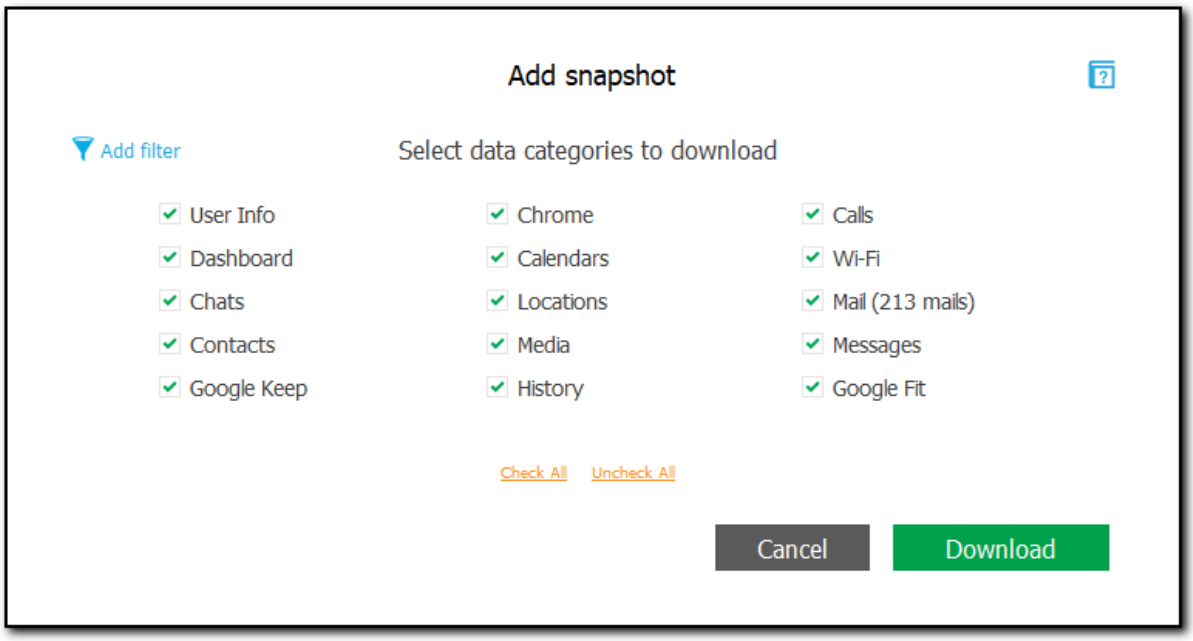
- **User Info/Информация о пользователе**: Данные пользователя учетной записи Google, включая имя, тип учетной записи (лицо или компания), дату рождения, URL-адреса профилей социальных сетей и многое другое.
- **Chats/Чаты**: Чаты в Google Hangouts.
- **Contacts/Контакты**: Контакты пользователя аккаунта Google и вся доступная информация о них.
- **Google Keep**: Заметки Google Keep.
- **Chrome**: Данные Google Chrome, включая пароли, закладки, формы автозаполнения и переходы страниц.
- **Calendars/Календари**: Мероприятия, запланированные в Календаре Google, включая разовые и регулярные мероприятия, дни рождения, праздники и т.д.
- **Dashboard/Дашборд**: Контент Личного кабинета Google, включая следующие данные:
  - устройства, связанные с учетной записью Google.
  - аккаунт Google.
  - история поиска пользователя в Google.
  - активность пользователя на YouTube.
  - подключенные приложения пользователя.
  - история местоположений пользователя и сохраненные места.

  - фотографии пользователя.
  - события календаря пользователя и многое другое.
- **Locations/Локации**: История местоположений пользователя из сервиса Google Timeline.
- **Media/Медиафайлы**: Фотографии пользователя из Google Photos.
- **History/История**: Информация об истории использования сервисов Google, включая историю поиска, историю поиска, историю поиска и просмотра YouTube, историю посещенных веб-сайтов и историю устройства.
- **Mail/Почта**: Почтовые сообщения Gmail.
- **Wi-Fi**: Информация о подключениях Wi-Fi.
- **Calls/Звонки**: Информация об истории звонков пользователя.
- **Messages/Сообщения**: Сообщения SMS.
- **Google Fit**: Данные об активности пользователя, загруженные из Google Fit.

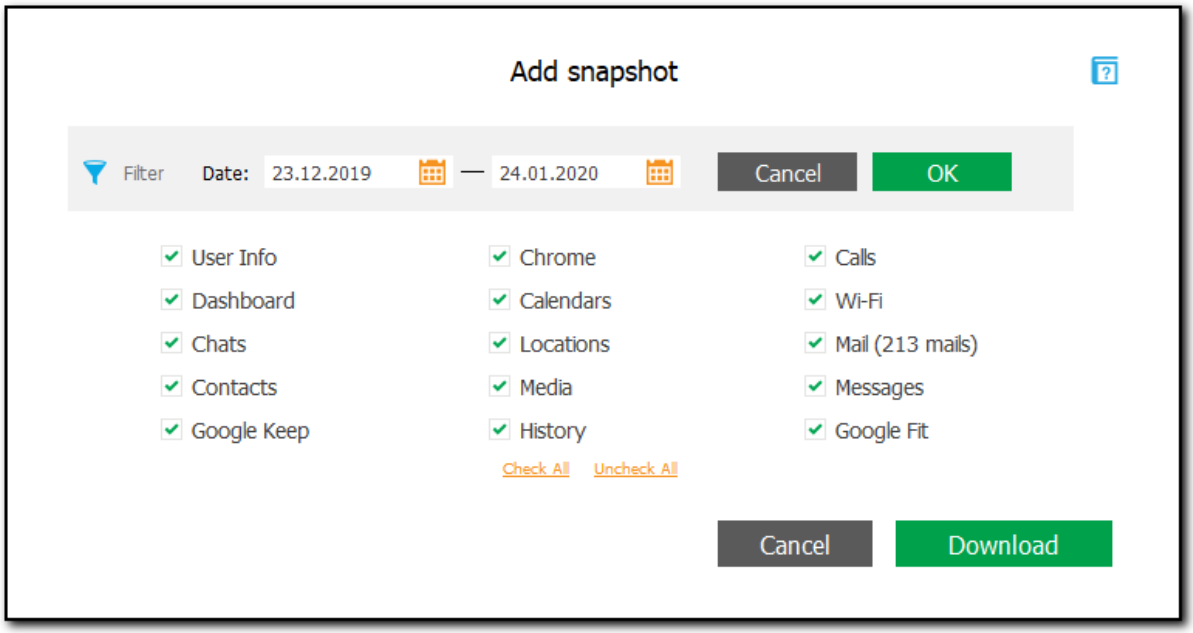
**ПРИМЕЧАНИЕ**. Информация о Wi-Fi, истории звонков и сообщений не будет загружена, если устройство пользователя работает под управлением Android 9.0 и выше и защищено кодом блокировки экрана.

**Чтобы загрузить информацию из аккаунта Google, сделайте следующее:**

1. В меню **File/Файл** нажмите **Add Google Snapshot/Добавить копию Google** либо нажмите  в нижнем левом углу окна ECX.
2. На странице **Download snapshot/Скачать снимок данных** укажите тип авторизации (пароль или маркер).
3. Нажмите **Sign in/Войти**.
4. Выберите категории для скачивания.



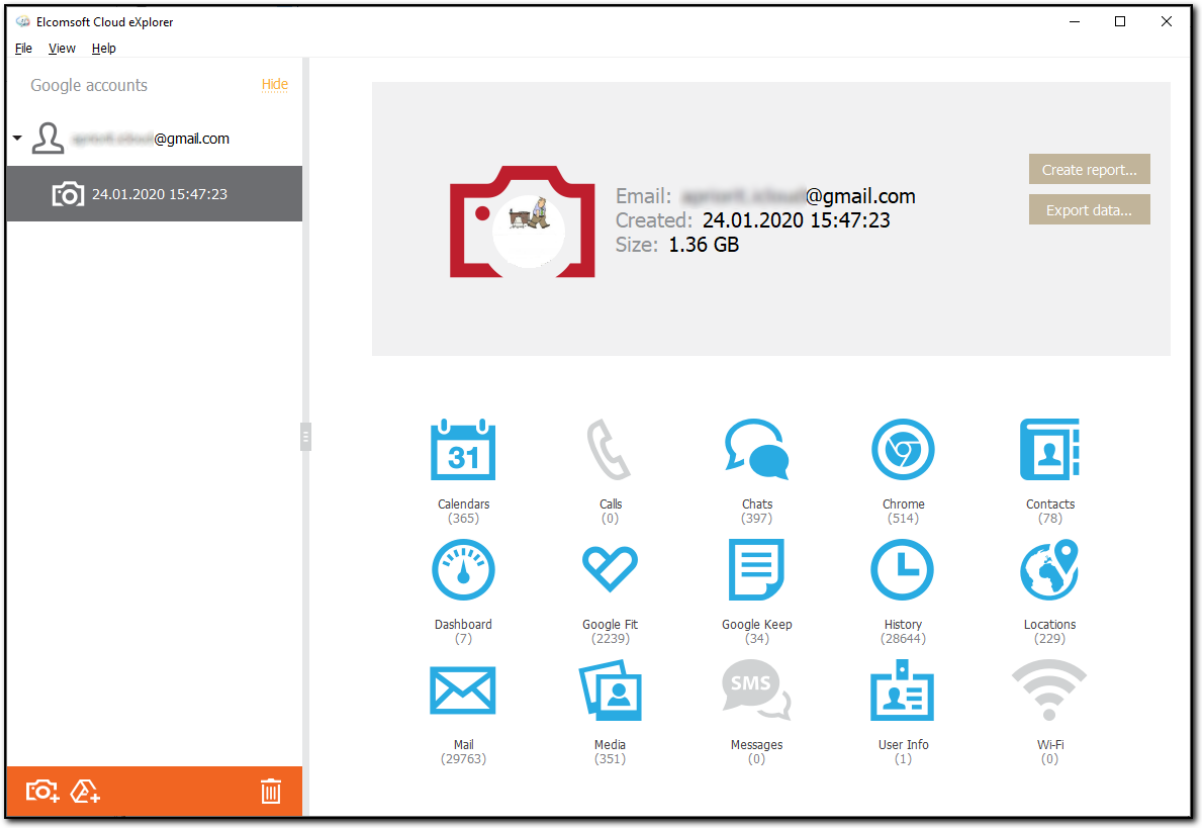

Для категорий **Mail/Почта** и **Media/Медиафайлы** доступна фильтрация  . Вы можете выбрать промежуток времени, за который будут скачаны письма и фотографии пользователя.




5. Нажмите **Download/Скачать.**

**ПРИМЕЧАНИЕ**. Некоторые данные Chrome могут быть зашифрованы с помощью пароля (дополнительную информацию см. на странице https://support.google.com/chrome/answer/1181035). Если вы выбрали загрузку категории данных Chrome, а информация Chrome в вашей учетной записи Google зашифрована паролем, ECX потребует ввести нужный пароль. Если вы введете кодовую фразу, все данные Chrome будут загружены. В обратном случае зашифрованные данные не будут загружены.

В главном окне вы можете увидеть, какие категории данных были загружены в каждую резервную копию, а также сколько записей содержит каждая резервная копия. Категории данных, которые не были выбраны для загрузки, и категории, в которых нет данных, отображаются серым цветом.




**Для удаления учётной записи или резервной копии** выберите запись и нажмите .

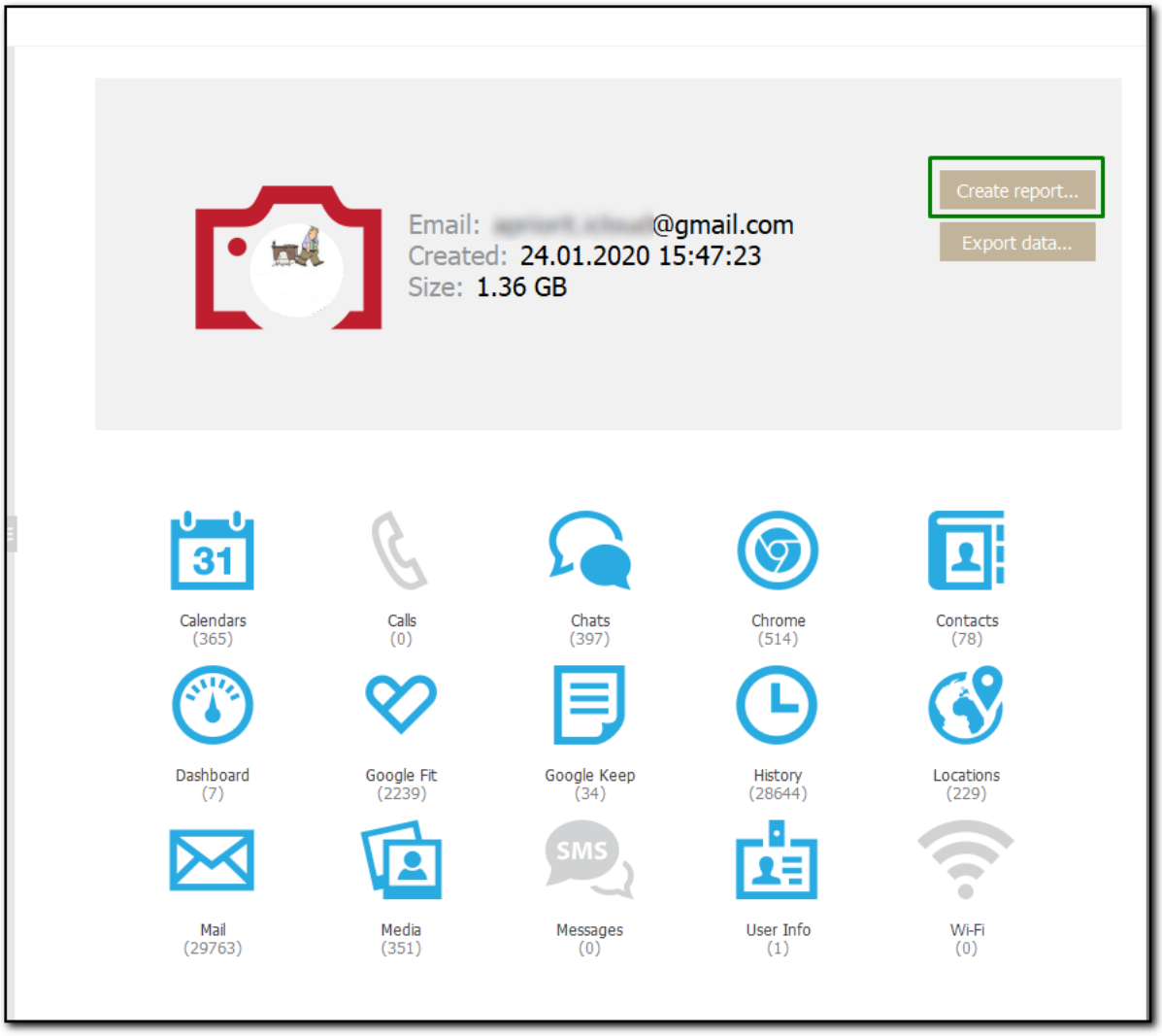
### 5.2.3 Отчёты

ECX поддерживает отчёты в формате html. Вместе с отчетом создается папка, содержащая все вложения.

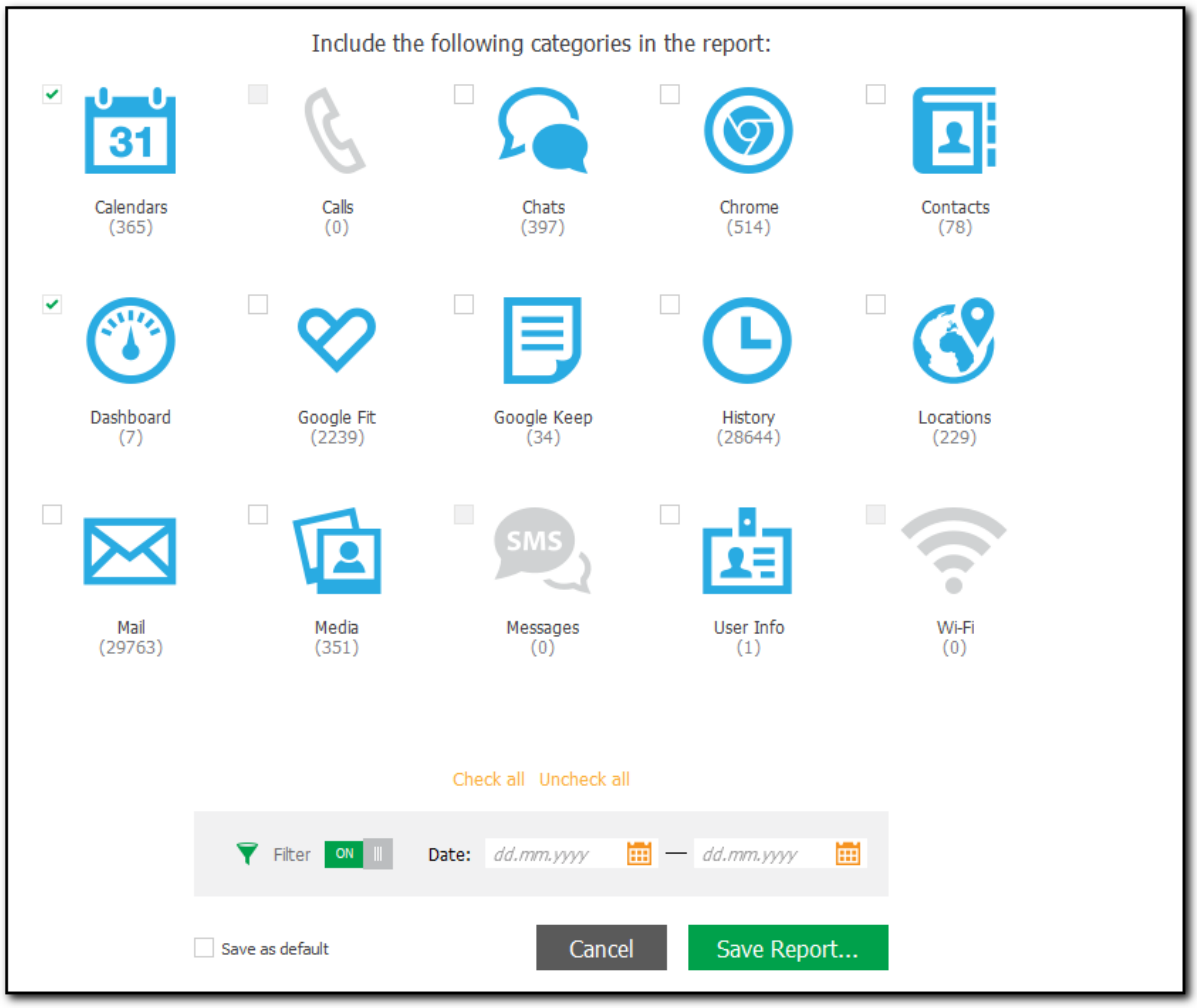
Обратите внимание, что отчеты доступны только в зарегистрированной версии программы.

**Для создания отчёта:**

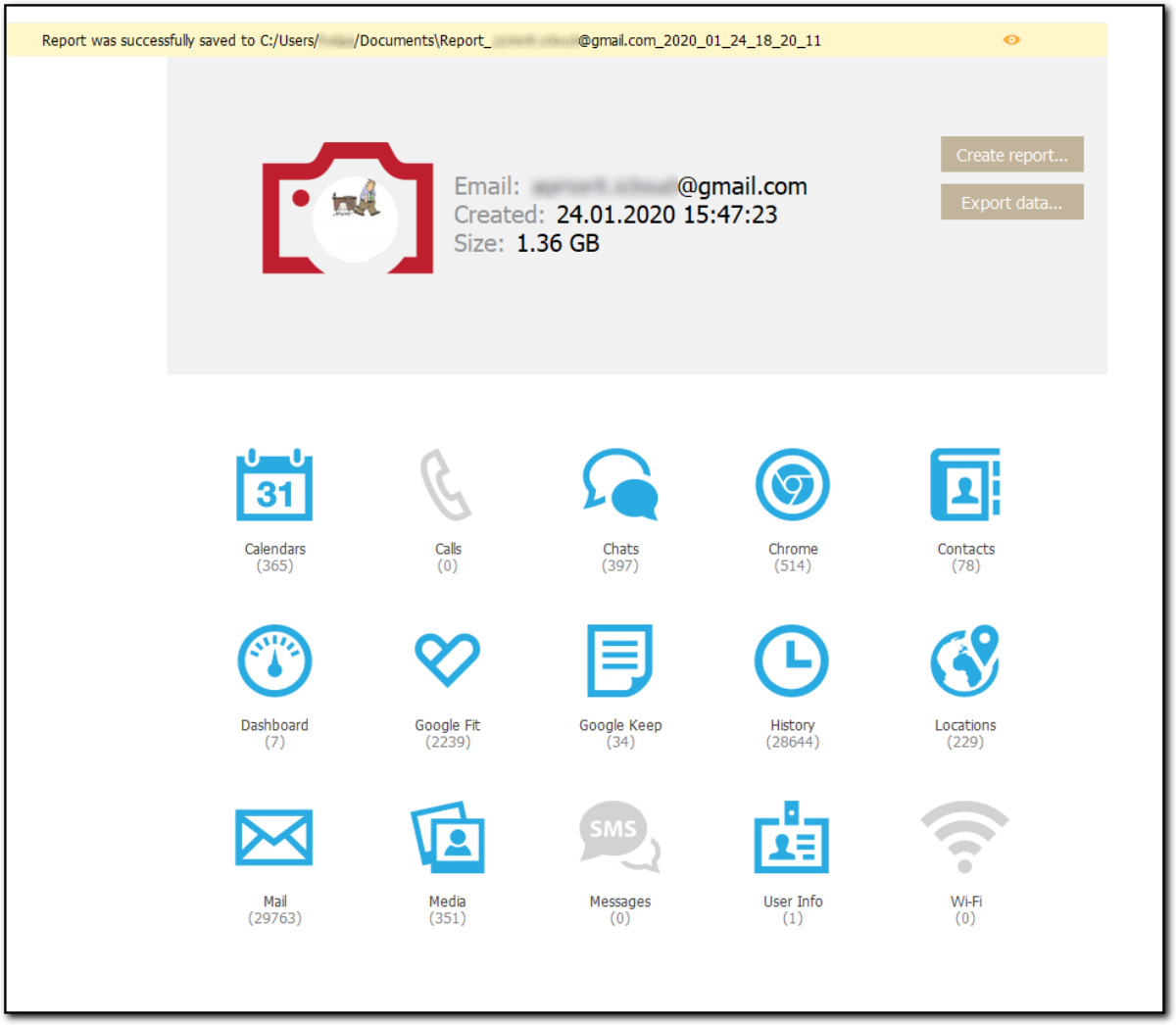
1. В окне просмотра резервной копии нажмите **Create report/Создать отчёт**.




2. Укажите категории данных.
   ПРИМЕЧАНИЕ: Категории **Mail/Почта** и **Google Fit** в текущей версии программы в отчёты не попадают.
3. Определите временной интервал, для которого должен быть создан отчёт.
4. Сохраните отчёт кнопкой **Save Report/Сохранить отчёт**.




Просмотреть отчёт можно, нажав иконку .




В состав отчёта входят:

- Информация об отчете: дата и время создания отчета, временной интервал, который включает отчет, категории данных, которые включены и не включены в отчет.
- Информация о резервной копии: имя учетной записи, дата загрузки резервной копии, размер резервной копии и количество записей в каждой категории данных.
- Информация о записях из каждой категории данных, добавленных в отчет.

### 5.2.4 Экспорт данных

ECX поддерживает экспорт данных в формат XLSX. Сопутствующие файлы сохраняются в ту же папку.

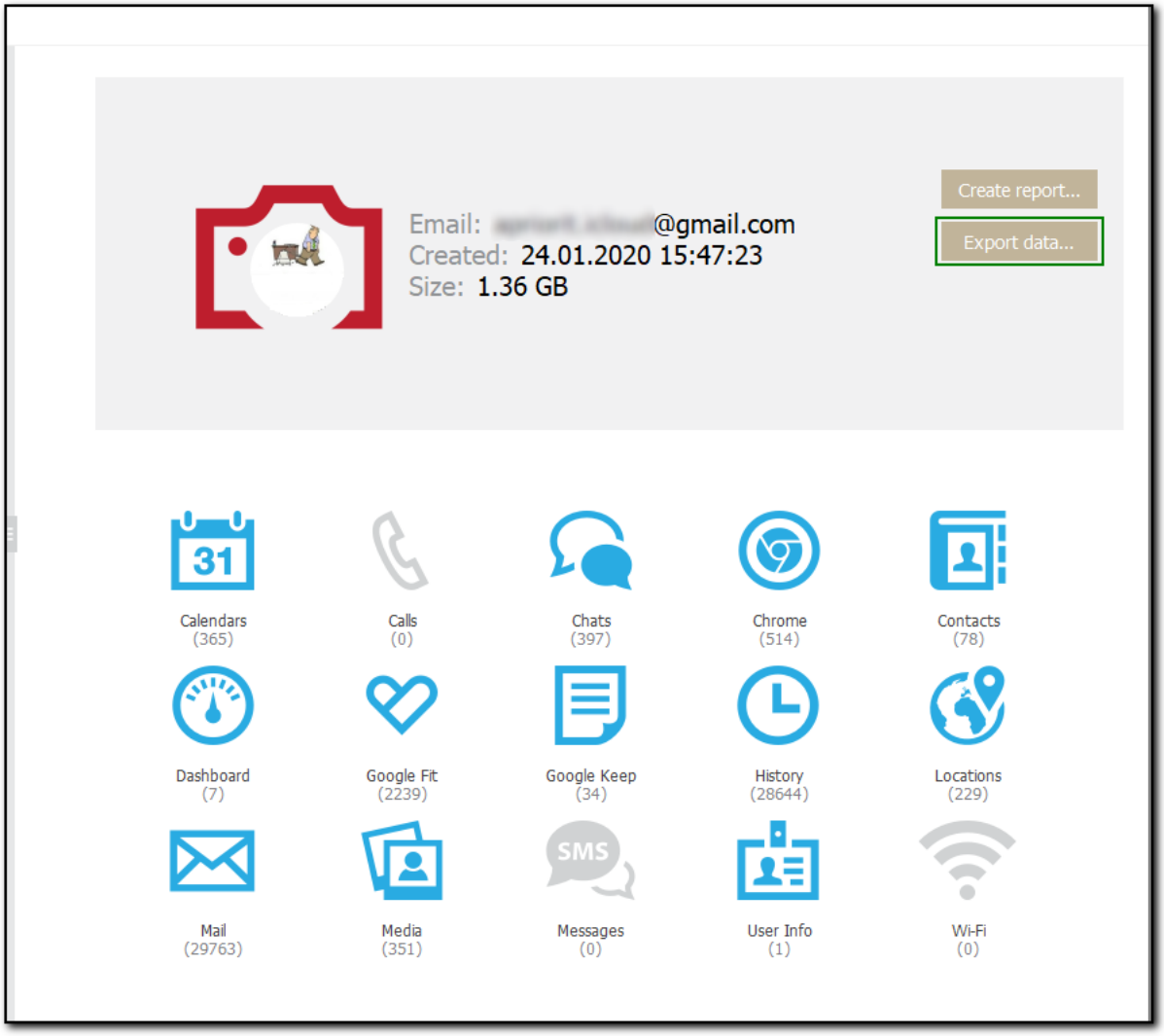
*ПРИМЕЧАНИЕ. Экспорт данных категории **Личный кабинет Google** не поддерживается.*

Вы можете экспортировать как данные из нескольких категорий учётной записи **Google account/Учётная запись Google**, так и данные конкретной категории.

Экспорт доступен только зарегистрированным пользователям.

Для экспорта данных:

1. В разделе информации о резервной копии нажмите **Export data/Экспортировать**.




2. Выберите категории данных для экспорта.
   Категория **Личный кабинет Google (Dashboard)** не может быть экспортирована.
3. Вы можете выбрать период, за который будут экспортированы данные.
4. Нажмите **Export/Экспорт** и укажите путь, в который будут сохраняться данные. Нажмите **Save/Сохранить**.

Просмотреть экспортированные данные можно, нажав .

Вы также можете экспортировать данные любого отдельного плагина:
1. Откройте плагин, нажав на его иконку, и нажмите **Export/Экспорт** рядом с полем ввода.
2. Укажите период, за который будут экспортированы данные, и нажмите **Save/Сохранить**.

Просмотреть экспортированные данные можно, нажав .

### 5.2.5 Двухфакторная аутентификация

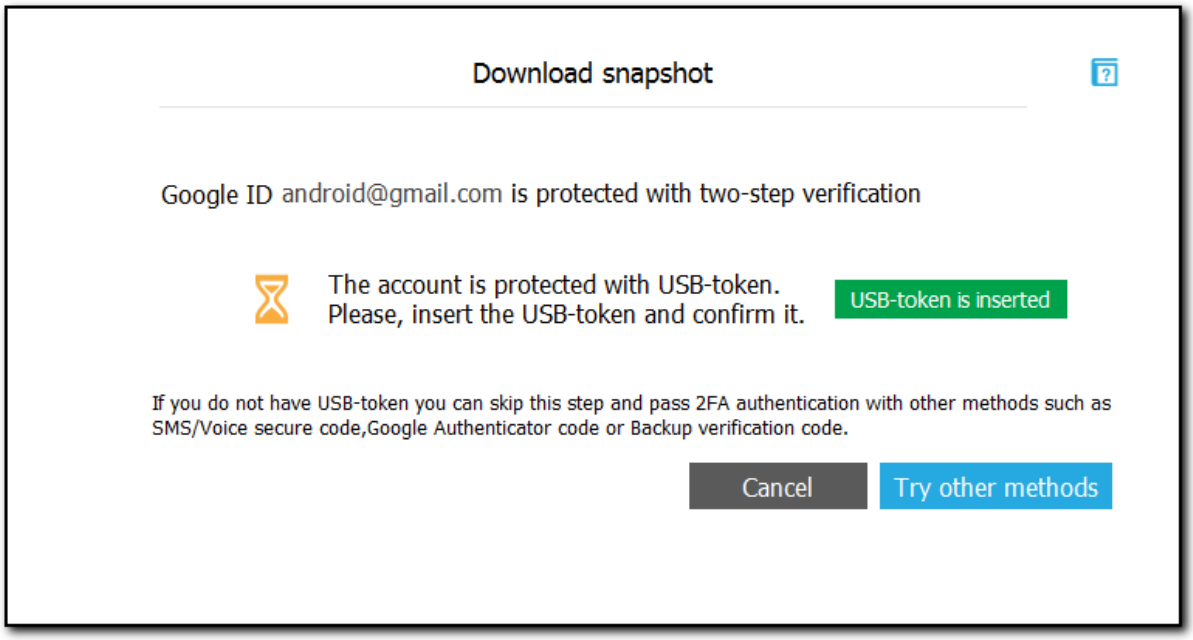
Некоторые учетные записи Google требуют двухэтапной проверки, что означает, что они защищены паролем и одним из дополнительных методов (в зависимости от метода, определенного по умолчанию в настройках безопасности учетной записи Google):

- USB-токен.
- Google Prompt - уведомление, отправленное на доверенное устройство.
- Код, отправленный на доверенный номер телефона в SMS-сообщении.
- Код, сгенерированный в приложении Google Authenticator.
- Один из резервных кодов подтверждения, доступных на странице обзора аккаунтов Google (https://support.google.com/accounts/answer/1187538)

Если учетная запись Google защищена USB-токеном или Google Prompt, используйте ключ безопасности или приложение для прохождения проверки.

**Использование USB-токена**

Если учетная запись защищена USB-токеном, вставьте USB-токен и нажмите кнопку **USB-token is inserted/USB-токен вставлен**.

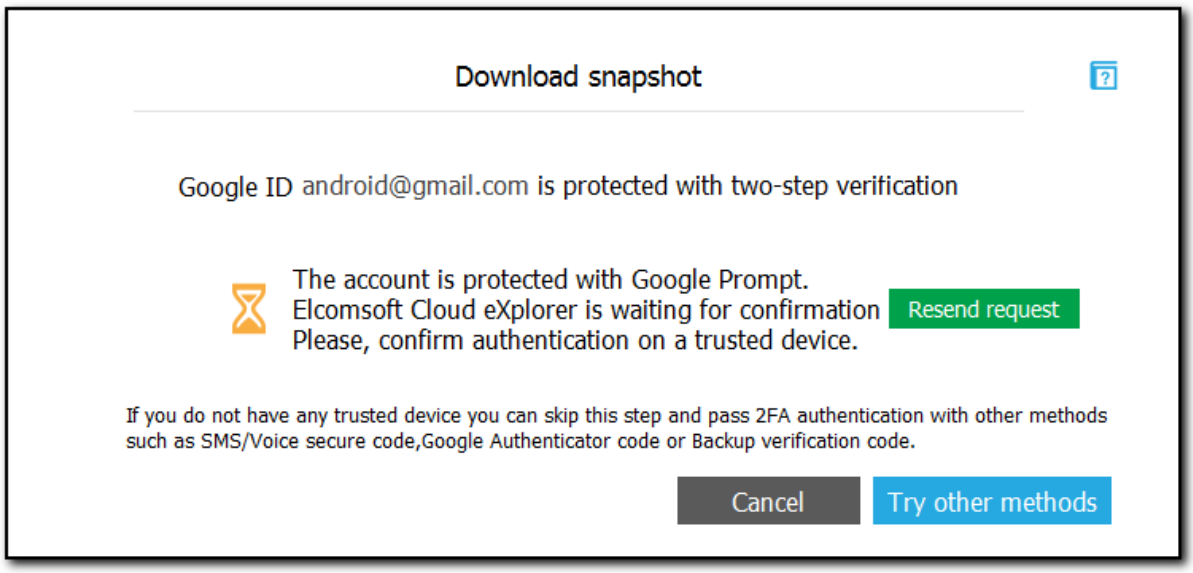



Если USB-токена в вашем распоряжении нет, вы можете попробовать авторизоваться другим способом, нажав на кнопку **Try other methods/Другие способы**.

**Google Prompt**

Если в учётной записи активен Google Prompt, приложение Google выдаст на устройстве пользователя интерактивное всплывающее сообщение. Подтвердите сообщение на устройстве

пользователя. Если сообщение не получено, нажмите **Resend request/Повторный запрос** для его повторной отправки.




**Код через SMS**

Введите цифровой код, доставленный в виде текстового сообщения SMS на доверенный телефонный номер пользователя.

**Коды Google Authenticator**

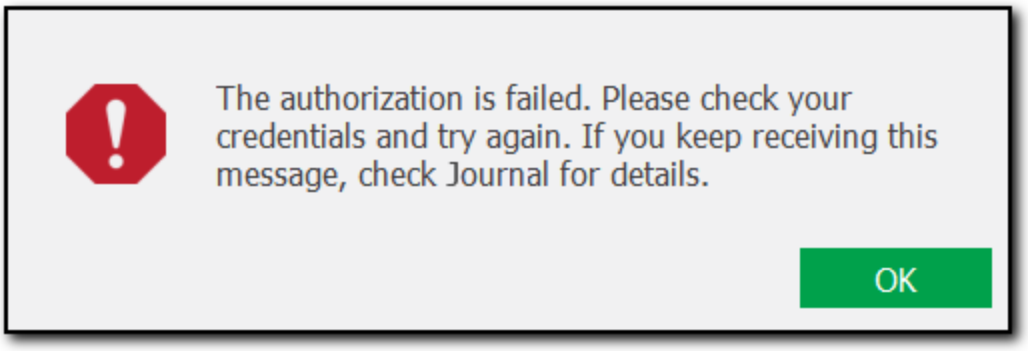
Если у вас есть доступ к приложению Google Authenticator, установленному на устройстве пользователя, вы можете использовать одноразовый код, сгенерированный этим приложением. Обратите внимание: код генерируется по протоколу TOTP (Time-based One Time Password) и действителен в течение 30 секунд.

**Одноразовые резервные коды доступа**

В учётной записи пользователя могут быть доступны одноразовые резервные коды доступа. Получить доступ к этим кодам можно со страницы **Accounts overview/Обзор уч. записей** в учётной записи пользователя. Введите одноразовый резервный код доступа в ECX для прохождения аутентификации.

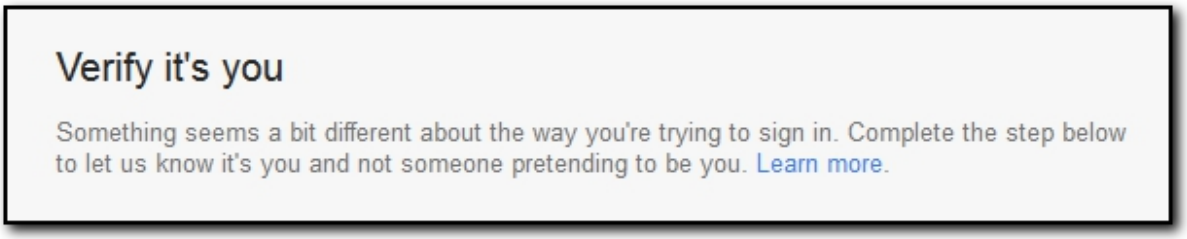
## 5.2.6 Исключения и особые случаи

В процессе входа в Google могут возникать исключительные случаи, когда авторизация не удалась. В этом случае вы получите следующее сообщение:




Авторизация не выполняется в следующих случаях:
- Если вы попытаетесь войти в систему с помощью ECX с нового IP-адреса, который ранее не использовался для входа в Chrome, находясь в той же учетной записи Google.
- Если учетная запись Google использовалась в одном регионе (городе или стране), а вы пытаетесь войти через ECX из другого региона (города или страны).
- Если авторизация выдаёт ошибку в любой другой ситуации, кроме двух описанных выше, обратитесь в нашу службу поддержки.

Если авторизация не удалась, откройте свою учетную запись Google в Google Chrome. Вы увидите уведомление:




Шаги, которые необходимо выполнить для проверки, различаются:
- Если для учетной записи определены и резервный адрес электронной почты, и номер телефона, вы можете выбрать один из них, чтобы получить проверочный код.
- Если для учетной записи определен только адрес электронной почты, вам будет предложено ввести адрес электронной почты, на который будет отправлен проверочный код.
- Если для учетной записи указан только доверенный номер телефона, вам будет предложено выбрать способ получения кода подтверждения (по SMS или по телефону).
- Если для учетной записи не определены ни номер телефона, ни адрес электронной почты, вам будет предложено указать последний город, в котором осуществлялся вход в учетную запись.

После этого попробуйте снова войти в учетную запись Google с помощью ECX.

# 5.3 Данные в Google Drive

## 5.3.1 Вход в Google Drive

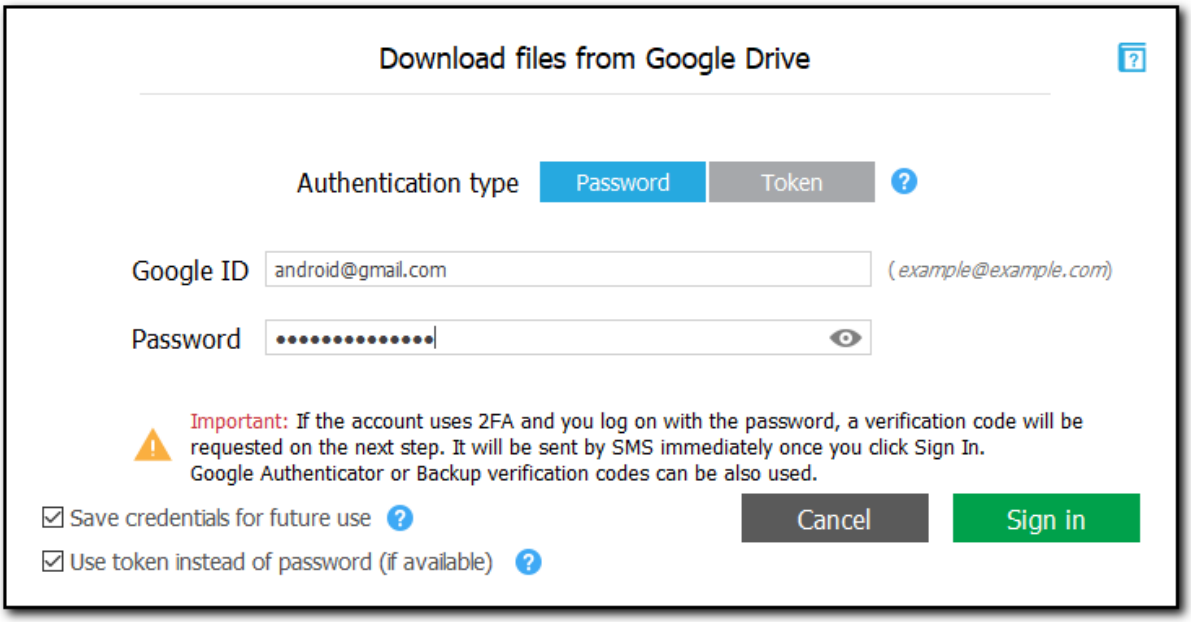
Чтобы загружать файлы с Google Drive, вам необходимо сначала войти в систему. Процесс аутентификации может различаться в зависимости от настроек безопасности учетной записи Google.

Доступны варианты входа по логину и паролю (**Password**) или маркеру аутентификации (**Token**).

**Вход при помощи логина и пароля**
Процедура аутентификации не отличается от любой другой процедуры входа в учётную запись при помощи логина и пароля. В качестве логина Google ID чаще всего выступает email-адрес пользователя в формате account@gmail.com.

Если выбрать опцию **Save credentials for future use/Сохранить учётные данные**, ECX сохраняет свой собственный маркер аутентификации для ускорения последующих сессий. Чтобы использовать маркер при следующем входе в эту учетную запись, введите логин и убедитесь, что выбрана опция **Use token instead of password (if available)/Использовать токен вместо пароля (если есть)**. При входе в систему с помощью маркера вам не нужно использовать пароль или проходить двухэтапную проверку.

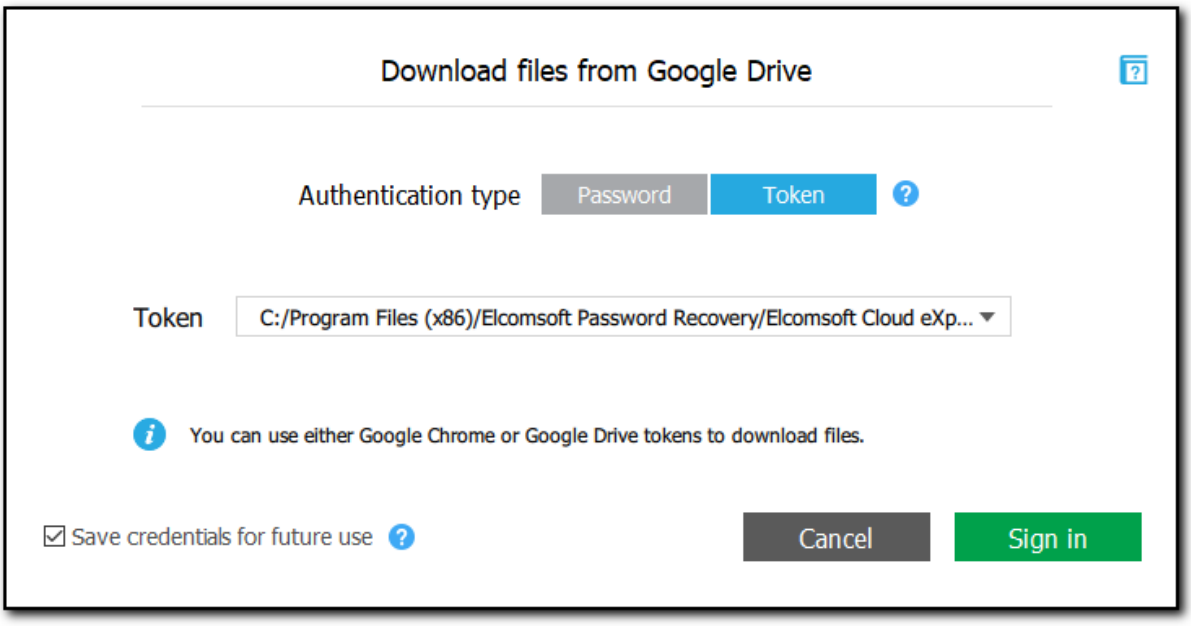
ПРИМЕЧАНИЕ. ECX не поддерживает учетные записи Google с защитой CAPTCHA. Вы можете подождать некоторое время, пока защита CAPTCHA не будет отключена, после чего попробовать снова войти в систему.




**Вход при помощи маркера аутентификации**
Если вы входите в систему с помощью маркера аутентификации, выберите ранее сохраненный маркер из списка или укажите путь к новому XML-файлу маркера, извлеченному из браузера Google Chrome при помощи утилиты Google Token Extractor (GTEX). По умолчанию этот файл сохраняется в папке, в которой расположен Google Token Extractor.

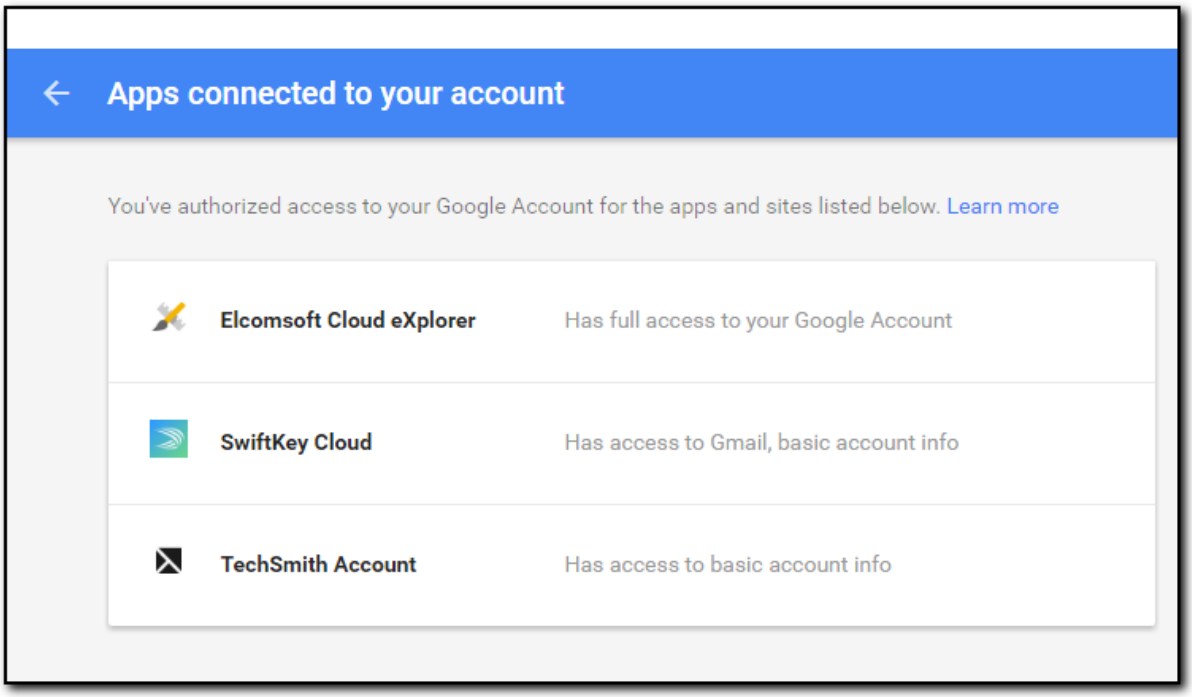
Когда вы входите в систему с выбранной опцией **Save credentials for future use/Сохранить учётные данные**, ECX сохраняет маркер, и вы можете выбрать его из списка при следующем входе в систему.

**ПРИМЕЧАНИЕ**. Для загрузки файлов из Google Drive можно использовать как маркеры, извлеченные из браузера Google Chrome, так и маркеры, которые созданы приложением Google Drive, установленным на компьютере пользователя.




**Уведомления о безопасности**

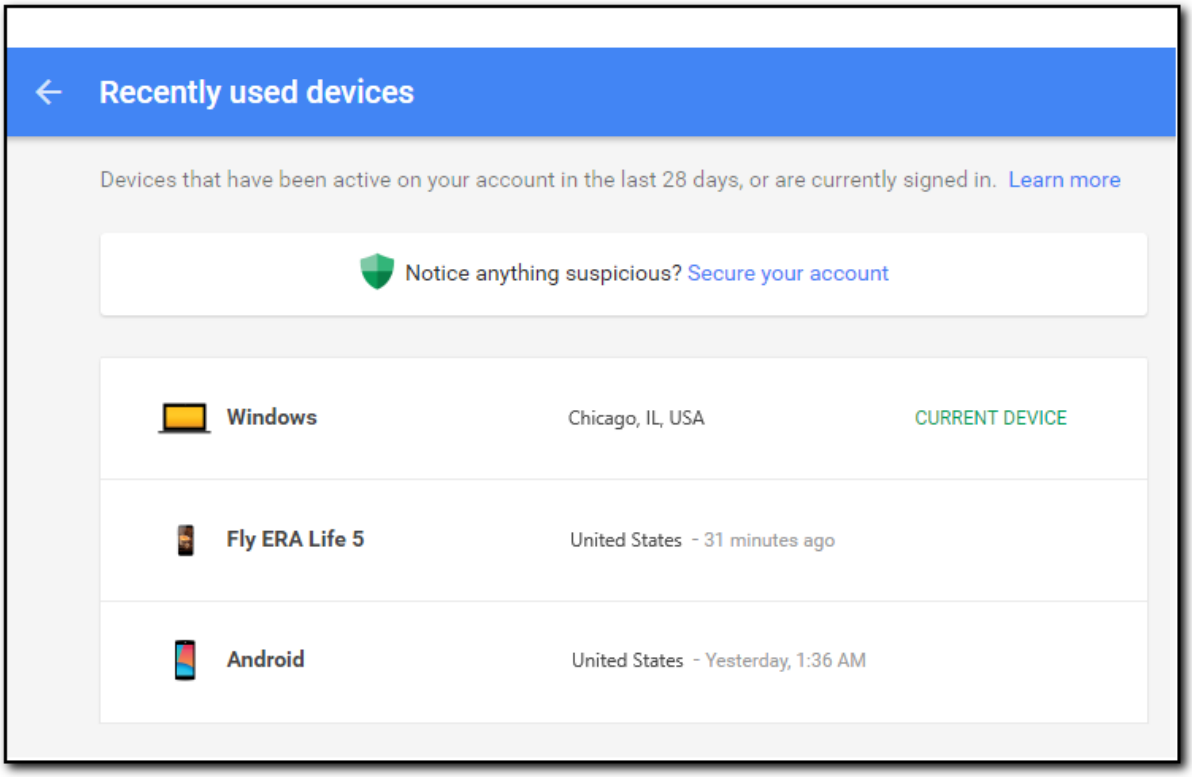
Когда вы входите в систему через ECX, информация об этом входе отображается в учётной записи Google пользователя. Elcomsoft Cloud eXplorer появится в списке приложений и сайтов с авторизованным доступом к учетной записи.




Если вы войдете в систему через ECX, используя логин и пароль, пользователь получит уведомление по электронной почте для той учетной записи Google, в которую вы вошли. Также появится дополнительное уведомление в учетной записи Google в списке недавно использованных

устройств. В этом списке упоминания ECX не появится, но в списке устройств, которые недавно вошли в учетную запись, будет устройство с Windows или неизвестной ОС.

Кроме того, в списке появится запись о неизвестном устройстве Android в том случае, если вы загружаете данные из категорий **Calls/Звонки** и **Wi-Fi**.




Наконец, если вы входите в учётную запись с IP-адреса, с которого вы ранее в неё не входили, пользователь получит уведомление по электронной почте с информацией о новом входе.

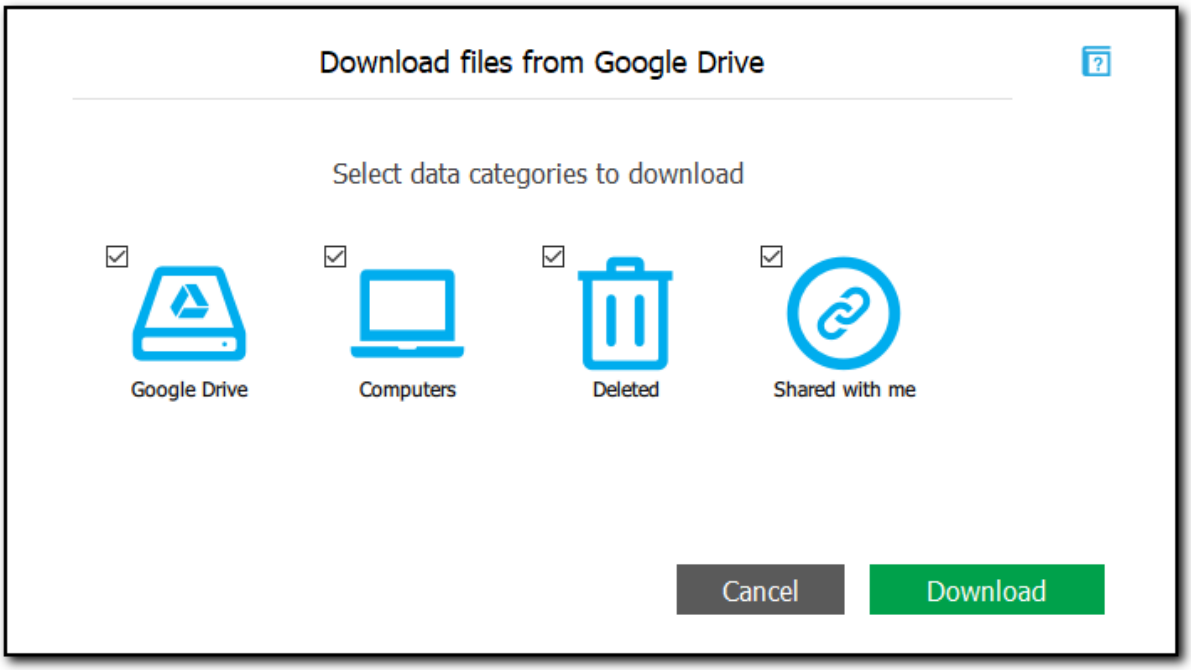
## 5.3.2 Скачивание данных из Google Drive

При скачивании данных из Google Drive доступны следующие категории:

- **Google Drive/Google Диск**: Файлы, которые сохранил пользователь.
- **Computers/Компьютеры:** Файлы, которые были синхронизированы с компьютеров пользователя.
- **Deleted/Удалённые:** Файлы, которые были удалены, но доступны в папке **Trash/Корзина** в Google Drive.
- **Shared with me/Доступные мне:** Файлы, которыми с пользователем поделились другие пользователи.

Для скачивания данных используйте команду **File/Файл - Download files from Google Drive/Скачать с Google Диска** либо иконку  в левой нижней части окна ECX.

После входа в учётную запись вы сможете выбрать категории данных для скачивания. Нажмите **Download/Скачать** для продолжения.

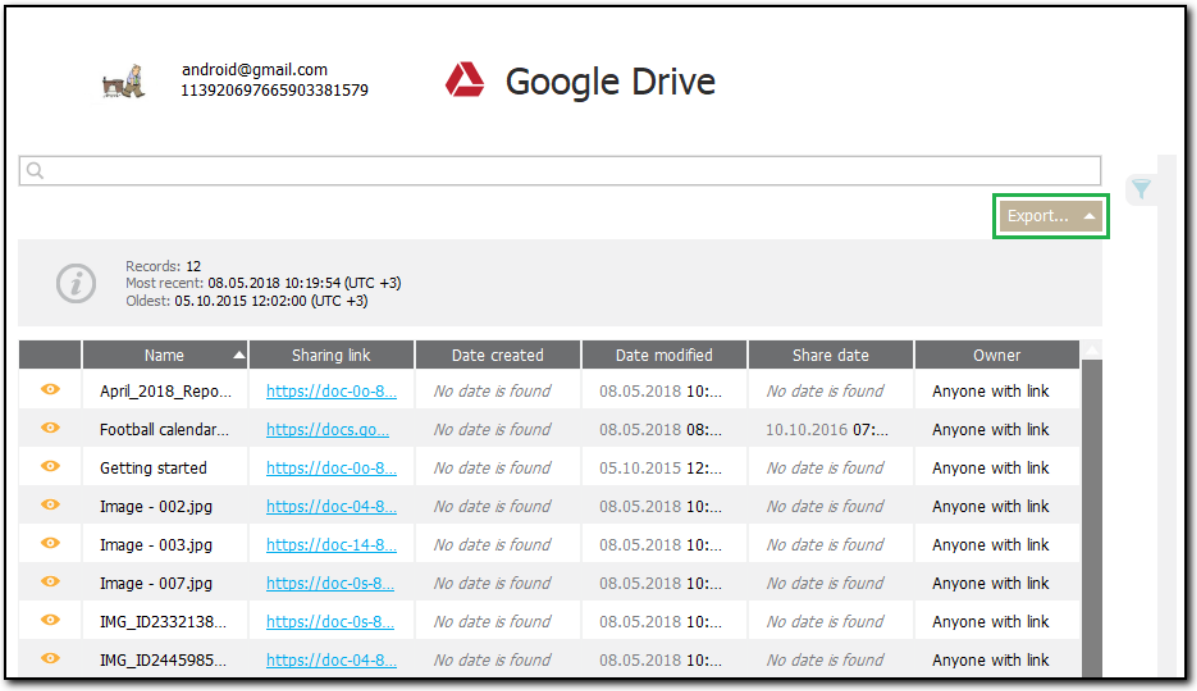



### 5.3.3 Экспорт данных

ECX поддерживает экспорт информации о файлах в Google Drive в формат XLSX.

Экспорт доступен только зарегистрированным пользователям.

Чтобы экспортировать информацию о файлах с Google Drive, сделайте следующее:
1. Откройте резервную копию Google Диска. Щелкните **Export/Экспорт** рядом с полем поиска.




2. Выберите, хотите ли вы экспортировать все или часть данных по определённым критериям.
3. Укажите путь на диске, куда будут сохранены данные.

## 5.4 Извлечение маркеров аутентификации Google

### 5.4.1 О приложении Google Token Extractor

**Google Token Extractor (GTEX)** - это консольная утилита для извлечения маркеров аутентификации в учетные записи Google из активной пользовательской сессии Windows и macOS.

GTEX может извлекать маркеры из браузера Google Chrome и приложения Google Drive (Backup and Sync).

Вы можете использовать маркеры, извлеченные GTEX, для входа в учетную запись пользователя Google, чтобы загрузить данные из учётной записи Google и резервные копии Google Drive.

GTEX поддерживает следующие операционные системы:
- Windows 7, Windows 8, Windows 8.1, Windows 10
- macOS 10.8–10.14

GTEX поддерживает извлечение маркеров из следующих приложений:
- Google Chrome версий 26–64
- Google Backup and Sync 1.32

Извлеченный маркер истекает, если:
- Пользователь отменяет доступ в настройках разрешений аккаунта Google.
- Токен не использовался 6 месяцев.
- Пользователь сменил пароль.

- Пользователь включил или отключил двухэтапную проверку после извлечения маркера.

## 5.4.2 Extracting token on Windows OS

Вход в учетную запись Google требуется для загрузки данных из учетной записи Google и Google Drive. Для входа может быть использована как комбинация логина и пароля, так и маркер аутентификации Google.

Чтобы извлечь маркер аутентификации, вам понадобится Google Token Extractor. Этот инструмент поставляется вместе с ECX (файл GoogleTokenExtractor.exe). Вы можете найти его в папке установки ECX.

Google Token Extractor - портативная утилита, поэтому вы можете скопировать файл GoogleTokenExtractor.exe на USB-накопитель или в папку, в которой вы хотите создать файл с маркером аутентификации.

GTEX может извлекать маркеры из браузера Google Chrome и приложения Google Drive (Backup and Sync).

GTEX позволяет извлекать маркеры аутентификации:

- Текущего авторизованного пользователя Windows
- Других пользователей Windows на текущем компьютере

**Предварительные условия**

Перед извлечением маркера аутентификации убедитесь, что выполнено хотя бы одно из следующих условий:

- Браузер Google Chrome установлен, и как минимум один пользователь вошел в учетную запись Google Chrome. Во время извлечения маркера необходимо закрыть браузер Google Chrome (убедитесь, что в диспетчере задач нет процесса Chrome.exe)
- Приложение Google Backup and Sync установлено, и по крайней мере один пользователь вошел в систему. Приложение можно запустить во время процесса извлечения маркера.

Прежде чем использовать GTEX для извлечения маркера, убедитесь, что подключение к Интернету установлено.

**Привилегии, необходимые для получения маркера аутентификации:**

| Тип маркера | Привилегии |
|---|---|
| Учетная запись Google текущего авторизованного пользователя Windows | Обычные привилегии пользователя |
| Учетная запись Google другого пользователя Windows | GoogleTokenExtractor.exe требует администраторских привилегий (если активирован UAC) |

**ПРИМЕЧАНИЕ. Если вы запустите GoogleTokenExtractor.exe из системной папки или из папки, для изменения которой у вас недостаточно прав, может появиться сообщение UAC с запросом разрешения на запуск этой программы.**

**Чтобы извлечь маркеры аутентификации для текущего пользователя Windows:**

1. Запустите **GoogleTokenExtractor.exe**. В каталоге с программой будет создан файл "**<Windows user>_<Google ID>_<token type>_<timestamp>_<time zone>.xml**".
2. В .xml-файле присутствует следующая информация:
   - GTEX Version - версия утилиты GTEX
   - Platform - платформа (Windows или macOS)
   - Google ID - логин пользователя Google
   - Token - маркер аутентификации
   - Token Type - тип маркера (Google Chrome или Google Drive)
   - Client ID
   - Client Secret
   - Date and time of extraction - дата и время извлечения маркера

**Чтобы извлечь маркеры аутентификации другого пользователя Windows:**

1. Откройте командную строку с правами администратора.
2. Выполните команду **GoogleTokenExtractor.exe --get-users-list**
3. Отобразится список всех локальных пользователей с установленными приложениями Google Chrome и Google Drive.
4. Запустите GoogleTokenExtractor.exe с параметром get-token chrome (для извлечения маркера из Google Chrome) либо get-token drive (для извлечения из приложения Backup and Sync). Введите имя пользователя Windows и пароль от его учетной записи в следующем виде:

**GoogleTokenExtractor.exe --get-token chrome --username <username> --password <password>**

**GoogleTokenExtractor.exe --get-token drive --username <username> --password <password>**

**Пример: GoogleTokenExtractor.exe --get-token chrome --username user1 --password 1234**

Если пароль пустой, введите **""** вместо самого пароля.

**Пример: GoogleTokenExtractor.exe --get-token chrome --username user1 --password ""**

**Список параметров GoogleTokenExtractor.exe:**

| Parameter | Meaning |
|---|---|
| --help | Отображает список всех возможных параметров командной строки и их описания |
| --get-users-list | Отображает список пользователей с установленными приложениями Google Chrome / Backup and Sync. |
| --get-token chrome | Извлекает маркер аутентификации из браузера Google Chrome для текущего пользователя. |
| --get-token drive | Извлекает маркер аутентификации из Backup and Sync для текущего пользователя. |
| --get-token chrome --username <username> --password <password> | Извлекает маркер аутентификации из браузера Google Chrome для указанного пользователя. Имя пользователя и пароль следует вводить без скобок. |

| | |
|---|---|
| --get-token drive --username <username> --password <password> | Извлекает маркер аутентификации из Backup and Sync для указанного пользователя. Имя пользователя и пароль следует вводить без скобок. |
| | Для пользователей с пустым паролем введите "" в качестве значения параметра пароля. |

### 5.4.3 Извлечение маркеров аутентификации: macOS

Вход в учетную запись Google требуется для загрузки данных из учетной записи Google и Google Drive. Для входа может быть использована как комбинация логина и пароля, так и маркер аутентификации Google.

Чтобы извлечь маркер аутентификации, вам понадобится Google Token Extractor. Этот инструмент поставляется вместе с ECX (файл **GoogleTokenExtractor**). Вы можете найти его в папке установки ECX.

GTEX может извлекать маркеры из браузера Google Chrome и приложения Google Drive (Backup and Sync).

GTEX позволяет извлекать маркеры аутентификации:

- Текущего авторизованного пользователя Windows
- Других пользователей Windows на текущем компьютере

**Предварительные условия**

Перед извлечением маркера аутентификации убедитесь, что выполнено хотя бы одно из следующих условий:

- Браузер Google Chrome установлен, и как минимум один пользователь вошел в учетную запись Google Chrome. Во время извлечения маркера необходимо закрыть браузер Google Chrome (убедитесь, что в диспетчере задач нет процесса Chrome.exe)
- Приложение Google Backup and Sync установлено, и по крайней мере один пользователь вошел в систему. Приложение можно запустить во время процесса извлечения маркера.

Прежде чем использовать GTEX для извлечения маркера, убедитесь, что подключение к Интернету установлено.

**Привилегии, необходимые для получения маркера аутентификации:**

| Тип маркера | Привилегии |
|---|---|
| Учетная запись Google текущего авторизованного пользователя системы | Обычные привилегии пользователя |
| Учетная запись Google другого пользователя системы | Требуются привилегии **root** |

**Чтобы извлечь маркеры аутентификации для текущего пользователя macOS:**

1. Запустите файл **GoogleTokenExtractor**. Будет создан файл "**<macOS user>_<Google ID>_<token type>_<timestamp>_<time zone>.xml**" в каталоге /Users/<username>/Documents/.
2. В .xml-файле присутствует следующая информация:

- GTEX Version - версия утилиты GTEX
- Platform - платформа (Windows или macOS)
- Google ID - логин пользователя Google
- Token - маркер аутентификации
- Token Type - тип маркера (Google Chrome или Google Drive)
- Client ID
- Client Secret
- Date and time of extraction - дата и время извлечения маркера

**Чтобы извлечь маркеры аутентификации других пользователей macOS:**

1. Скопируйте **GoogleTokenExtractor** в папку, из которой будет осуществляться работа.
2. Откройте окно терминала / Terminal.
3. Перейдите в каталог с **GoogleTokenExtractor**.
4. Команда **sudo ./GoogleTokenExtractor --get-users-list** выводит список пользователей Google Chrome / Google Drive.

   Команда **sudo** необходима для эскалации привилегий.
5. Введите пароль пользователя **root**.
6. Отобразится список всех пользователей, у которых установлены приложения Google Chrome и Google Drive.
7. Запустите GoogleTokenExtractor.exe с параметром get-token chrome (для извлечения маркера из Google Chrome) либо get-token drive (для извлечения из приложения Backup and Sync). Введите имя пользователя macOS и пароль от его учетной записи в следующем виде:

   **sudo ./GoogleTokenExtractor --get-token chrome --username <username> --password <password>**

   **sudo ./GoogleTokenExtractor --get-token drive --username <username> --password <password>**

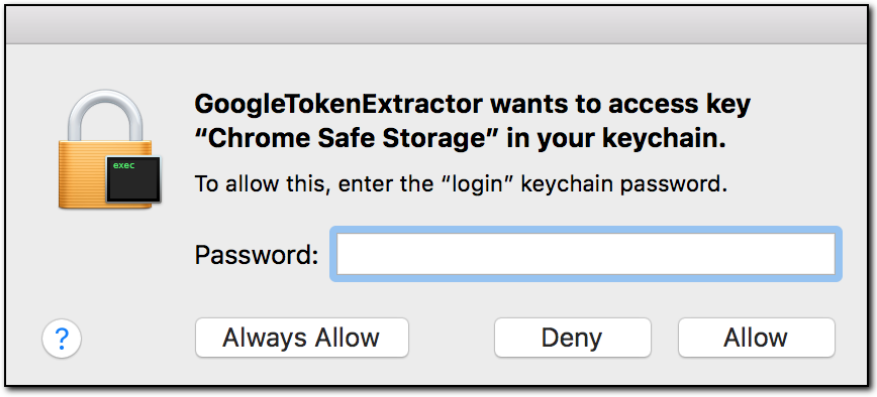
   **Пример: sudo GoogleTokenExtractor --get-token chrome --username user1 --password 1234**

   Если пароль пользователя пустой, используйте вместо него значение **""**.

   **Пример: sudo GoogleTokenExtractor --get-token chrome --username user1 --password ""**

**NOTE: избегайте запуска GoogleTokenExtractor через sudo без параметров.**

8. Введите пароль пользователя.
9. В окне запроса доступа к Связке ключей нажмите **Allow/Разрешить**.




10. В каталоге с программой будет создан файл "**<macOS user>_<Google ID>_<token type>_<timestamp>_<time zone>.xml**".

**Список параметров GoogleTokenExtractor.exe:**

| Parameter | Meaning |
|---|---|
| --help | Отображает список всех возможных параметров командной строки и их описания |
| --get-users-list | Отображает список пользователей с установленными приложениями Google Chrome / Backup and Sync. |
| --get-token chrome | Извлекает маркер аутентификации из браузера Google Chrome для текущего пользователя. |
| --get-token drive | Извлекает маркер аутентификации из Backup and Sync для текущего пользователя. |
| --get-token chrome --username <username> --password <password> | Извлекает маркер аутентификации из браузера Google Chrome для указанного пользователя. Имя пользователя и пароль следует вводить без скобок. |
| --get-token drive --username <username> --password <password> | Извлекает маркер аутентификации из Backup and Sync для указанного пользователя. Имя пользователя и пароль следует вводить без скобок. |
| | Для пользователей с пустым паролем введите "" в качестве значения параметра пароля. |

# 5.5 Плагины

## 5.5.1 Просмотр, поиск и анализ данных

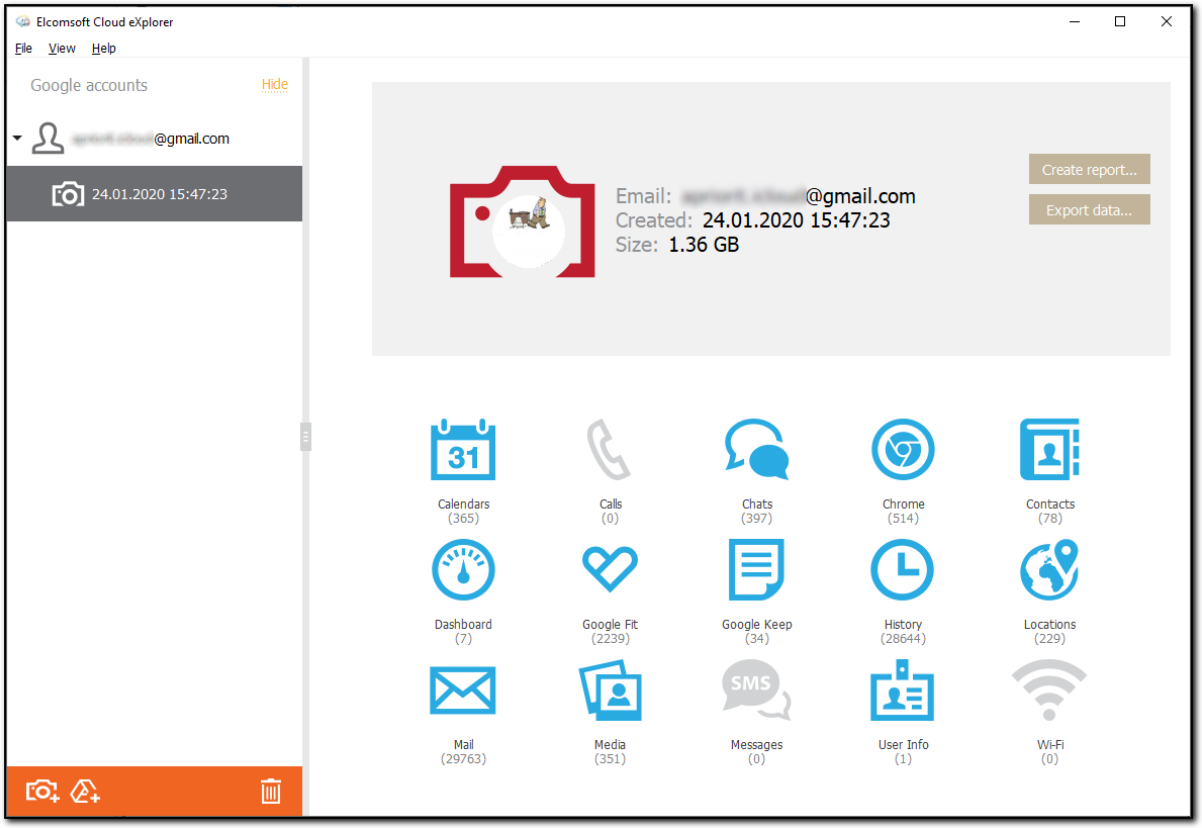
Скачанные в ECX данные можно просматривать при помощи плагинов. Каждый плагин отвечает за собственную категорию данных. Для просмотра категории нажмите на соответствующую иконку в окне просмотра данных.

Вы можете просматривать множество категорий данных. В список входят следующие категории:

- Contacts/Контакты
- Calendars/Календари
- Calls/Звонки
- Chrome
- Mail/Почта

- Media/Медиафайлы
- Messages/Сообщения
- Google Keep
- History/История
- Wi-Fi
- Chats/Чаты
- User Info/Информация о пользователе
- Google Fit
- Google Drive/Google Диск
- Locations/Локации
- Dashboard/Дашборд

Информация о файлах, хранящихся в облачном сервисе Google Drive. В состав данных входят ссылки на загрузку, дата и время создания и последнего изменения файлов и т.п.




**Поиск и фильтрация**

Для большинства категорий доступны поиск и фильтрация данных. Чтобы выполнить поиск, заполните поле поиска и нажмите **Enter/Ввод**. Результаты поиска будут выделены желтым цветом.

Чтобы отфильтровать данные, откройте панель **Filter/Фильтровать**, щелкнув значок справа.

Вы можете экспортировать отфильтрованные данные, выбрав **Export/Экспорт** - **Filtered/Отфильтрованные**.

### 5.5.2 Экспорт данных

Большинство расширений поддерживает экспорт данных. Для того, чтобы экспортировать данные той или иной категории, проделайте следующие шаги.

1. В окне соответствующего расширения нажмите **Export/Эскпорт**.
2. Выберите **All/Все**, чтобы экспортировать все данные.
3. Выберите файл в окне **Select destination file/Выбрать файл назначения** и укажите путь к файлу.
4. Нажмите **Save/Сохранить**.

В расширениях используются стандартные форматы файлов, включая .xml и .xlsx.

### 5.5.3 Доступные данные

Вы можете просматривать множество категорий данных. В список входят:

#### Contacts / Контакты

Информация о контактах из адресной книги пользователя. Избранные контакты помечаются символом звезды.

#### Calendars / Календари

Календари, события, встречи, включая повторяющиеся.

#### Calls / Звонки

Журнал звонков пользователя. Поскольку информация о звонках извлекается из резервных копий устройств под управлением Android, а не из синхронизированных данных, эта категория может быть недоступной, если смартфон пользователя работает под управлением Android 9.0 или более новой, а на устройстве установлен код блокировки экрана (в этом случае резервные копии зашифрованы).

#### Chrome

Данные об активности пользователя в интернет: список посещённых узлов и страниц, закладки, история переходов и поиска, а также сохранённые пароли и формы автозаполнения.

#### Mail / Почта

Скачивает почтовые сообщения и вложения из сервиса Gmail. Для доступа к почте используется собственный API Google, что позволяет проводить предварительную фильтрацию писем до скачивания (например, задавать промежуток, за который должны быть скачаны сообщения).

#### Media / Медиафайлы

Фотографии и видеоролики, извлечённые из сервиса Google Photos с поддержкой разбивки по альбомам.

#### Messages / Сообщения

Сообщения SMS и MMS, скачанные из учётной записи пользователя. Для MMS доступен только текст сообщения.

Эта категория может быть недоступной, если смартфон пользователя работает под управлением Android 9.0 или более новой, а на устройстве установлен код блокировки экрана (в этом случае резервные копии зашифрованы).

### Google Keep

Заметки пользователя из сервиса Google Keep.

### History / История

История активности пользователя из сервиса Google History. Извлекаются следующие категории: история поисковых запросов в Google, история голосовых запросов, включая аудио-файлы, история поиска и просмотров в YouTube, данные об истории открытых веб-страниц и история входа в устройства, в которой перечислены устройства, с которых осуществлялся вход в учётную запись. Для всех категорий доступны дата и время соответствующих записей.

### Wi-Fi

История подключений к точкам доступа Wi-Fi.

Эта категория может быть недоступной, если смартфон пользователя работает под управлением Android 9.0 или более новой, а на устройстве установлен код блокировки экрана (в этом случае резервные копии зашифрованы).

### Chats / Чаты

Чаты Google Hangouts. Включается как текстовое содержимое чатов, так и медиа-файлы.

### User Info / Информация о пользователе

Здесь доступна такая информация о пользователе, как имя, пол, дата рождения, а также опциональные поля - например, профессия, место работы, семейный статус и т.п.

### Google Fit

Данные о физической активности пользователя, которые собирает сервис Google Fit. В набор данных может входить информация о количестве шагов, показания фитнес-браслетов и датчиков, а также данные, которые поставляют в сервис Google Fit сторонние приложения через соответствующие API.

### Google Drive

Информация о файлах, хранящихся в облачном сервисе Google Drive. В состав данных входят ссылки на загрузку, дата и время создания и последнего изменения файлов и т.п.

## 5.5.4 История местоположений - Locations

#### 5.5.4.1 История местоположений

В состав данных истории местоположений входят следующие категории:

### Places / Места

В этом разделе содержится подробная информация о местах и координатах, которые посетил пользователь.

- Дата начала визита
- Дата окончания визита
- Название места
- Категория (например, банк, ресторан, тренажерный зал и т.д.).
- Адрес
- Координаты

Все локации отсортированы по дате, самое последнее - вверху.

Историю местоположений пользователя можно отобразить на карте, просмотрев трек. В браузере откроется карта, на которой будут показаны местоположения пользователя, отмеченные красными точками. Щелкните точку, чтобы просмотреть ее адрес, категорию, координаты, а также дату и время начала/окончания визита.

### Routes / Маршруты

Подробная информация о проложенных пользователем маршрутах включая координаты точек отправления и прибытия, а также всех промежуточных остановок. Кроме того, отображается информация о типе маршрута: общественный транспорт, поездка на автомобиле или велосипеде или пешеходный маршрут.

### Your Places / Ваши места

В этом разделе можно просмотреть места, которые посетил пользователь и/или поставил на них отметку на картах Google.

### Maps / Карты

Здесь можно просмотреть сохраненные пользователем карты Google с дополнительными данными.

## 5.5.5 Личный кабинет Google - Dashboard

Enter topic text here.

#### 5.5.5.1 Личный кабинет Google

В Личном кабинете Google (Google Dashboard) содержится агрегированная статистическая информация об использовании устройств под управлением Android и сервисов Google. Исследование этих данных позволяет получить общее представление о том, какими службами Google, насколько активно, с какой частотой и периодичностью пользуется владелец учётной записи.

Необходимо понимать, что Личный кабинет Google содержит уже обработанные компанией Google данные. Более того, данные соответствующих сервисов в Личный кабинет не попадают - попадает лишь статистическая информация об использовании сервиса. К примеру, для сервиса **Google Drive** можно узнать количество файлов в хранилище, количество удалённых и общих файлов - но не сами файлы и даже не их имена. Аналогичным образом, статистика **YouTube** включает число подписок (обычных и приватных), количество комментариев, а также то, включены или выключены опции сохранения истории просмотра и поиска (но не сама история). Для браузера **Google Chrome** доступны данные о количестве закладок, расширений, паролей и других объектов, а также данные о времени последней синхронизации. Для прочих категорий доступны аналогичные количественные данные.

В состав данных из Личного кабинета (Dashboard) входят статистические данные для следующих категорий:

- Account
- AdSense
- Alerts
- Analytics
- Android
- Blogger
- Books
- Brand Accounts
- Calendars
- Chrome
- Connected Apps
- Contacts
- Device Activity
- Drive
- FeedBurner
- Gmail
- Google Play
- Google Play Music
- Groups
- Keep
- Location History
- Maps
- News
- Package Tracking
- Payments
- Photos
- Search
- Search Console
- Tasks
- YouTube

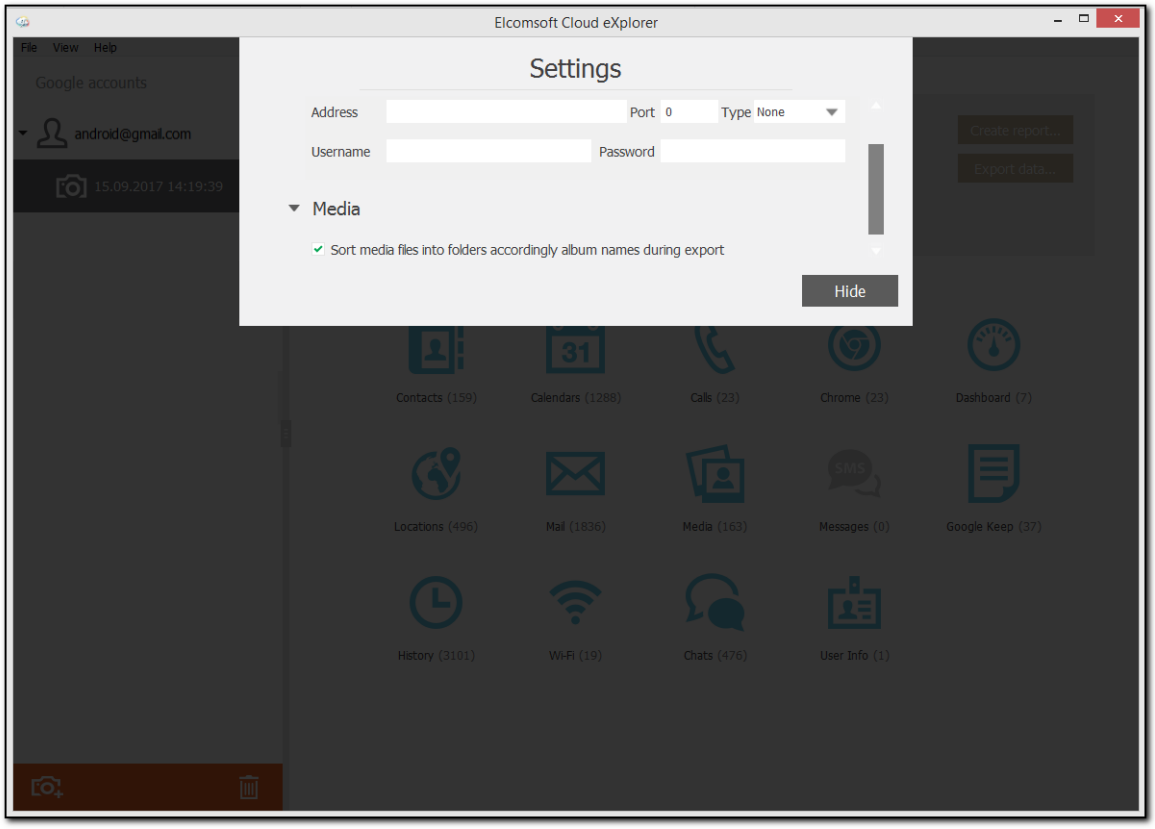
# VI Elcomsoft eXplorer for WhatsApp

## 6.1 О программе

### 6.1.1 Окно настроек

В настройках программы можно указать прокси-сервер для подключения к сети.

**ВНИМАНИЕ: Программа поддерживает только сквозные прокси-серверы. Прокси с подменой сертификата не поддерживаются.**




### 6.1.2 Совместимые устройства

Поддерживаются все устройства линеек iPhone, iPad и iPod Touch с версиями iOS от 6 до 14.0 для всех версий WhatsApp.

Для всех WhatsApp и Android поддерживаются все устройства под управлением Android от 4.0 до 6.0.1 (без root) и 9.0 (только с root-доступом).

### 6.1.3 Изменение пути к файлам

Вы можете изменить путь на диске, в который EXWA будет сохранять скачанные данные. Для этого отредактируйте файл настроек, расположенный по следующему пути:

**\AppData\Roaming\Elcomsoft\Elcomsoft eXplorer for WhatsApp\Setting.ini.**

Укажите желаемый путь на диске с использованием двойных разделителей (\\) и символов латиницы (e.g., **C:\\Users\\jane.smith\\AppData\\Roaming\\Elcomsoft**). Поддерживаются только локальные пути (сетевые папки не поддерживаются).

### 6.1.4 Экспорт данных

EXWA поддерживает экспорт данных в формат XLSX. Вложения и файлы сохраняются в ту же папку. Обратите внимание, что экспорт данных возможен только в зарегистрированной версии продукта. Для того, чтобы экспортировать данные, проделайте следующие шаги.

1. В окне соответствующего **Data View/Просмотр данных** нажмите **Export data/Экспортировать.**
2. Выберите **All/Все**, чтобы экспортировать все данные, либо укажите временной интервал для выборочного экспорта.
3. Выберите файл в окне **Select destination file/Выбрать файл назначения** и укажите путь к файлу.
4. Нажмите **Save/Сохранить**.

## 6.2 Устройства Apple

### 6.2.1 Резервные копии WhatsApp

#### 6.2.1.1 Создание резервной копии WhatsApp

Вы можете создать резервную копию данных WhatsApp как в составе резервной копии устройства в iCloud, так и автономно в iCloud Drive.

**Резервные копии в iCloud**

Чтобы создать резервную копию данных WhatsApp в резервной копии устройства в iCloud, перейдите в **Settings > iCloud > Storage > Manage Storage > This iPhone**. Убедитесь, что переключатель для приложения **WhatsApp** находится в положении "включено".

**Автономные резервные копии в iCloud Drive**

Чтобы немедленно создать резервную копию данных WhatsApp в iCloud Drive, перейдите в **WhatsApp Settings > Chats and Calls > Chat Backup**, а затем нажмите **Back Up Now**.

Вы также можете запланировать автоматическое резервное копирование данных WhatsApp на iCloud Drive. Для этого перейдите в **WhatsApp Settings > Chats and Calls > Chat Backup**, а затем нажмите **Auto Backup** и укажите периодичность резервного копирования.

Требования для создания резервных копий данных WhatsApp в iCloud Drive:
iOS 5.1 или новее.

- Устройство должно быть зарегистрировано в iCloud (Настройки iPhone> iCloud).
- Как в облаке iCloud, так и на iPhone должно быть достаточно свободного места.
- Убедитесь, что следующие настройки включены:
  - Для iOS 7: **Documents & Data (iPhone Settings > iCloud > Documents & Data)**

- Для iOS 8 и новее: **iCloud Drive (iPhone Settings > iCloud > iCloud Drive)**

Дополнительная информация: https://www.whatsapp.com/faq/en/iphone/20888066#backup

#### 6.2.1.2 Маркеры аутентификации

iCloud позволяет пользователям хранить информацию в облаке. Пользователи macOS могут получить доступ к iCloud без какого-либо дополнительного программного обеспечения, поскольку оно встроено в операционную систему (для iCloud требуется macOS 10.7.2 или новее).

**Типы маркеров аутентификации:**

| | **iCloud for Windows до v. 7.0** | **iCloud for Windows v. 7.0 и новее** |
|---|---|---|
| Учётная запись с двухфакторной аутентификацией | Маркер аутентификации без ограничений | Маркер аутентификации с ограничениями |
| Учётная запись без двухфакторной аутентификации | Маркер аутентификации для учётной записи без двухфакторной аутентификации | Маркер аутентификации для учётной записи без двухфакторной аутентификации |

**Маркеры аутентификации, поддерживаемые в Windows и macOS для загрузки данных через EXWA:**

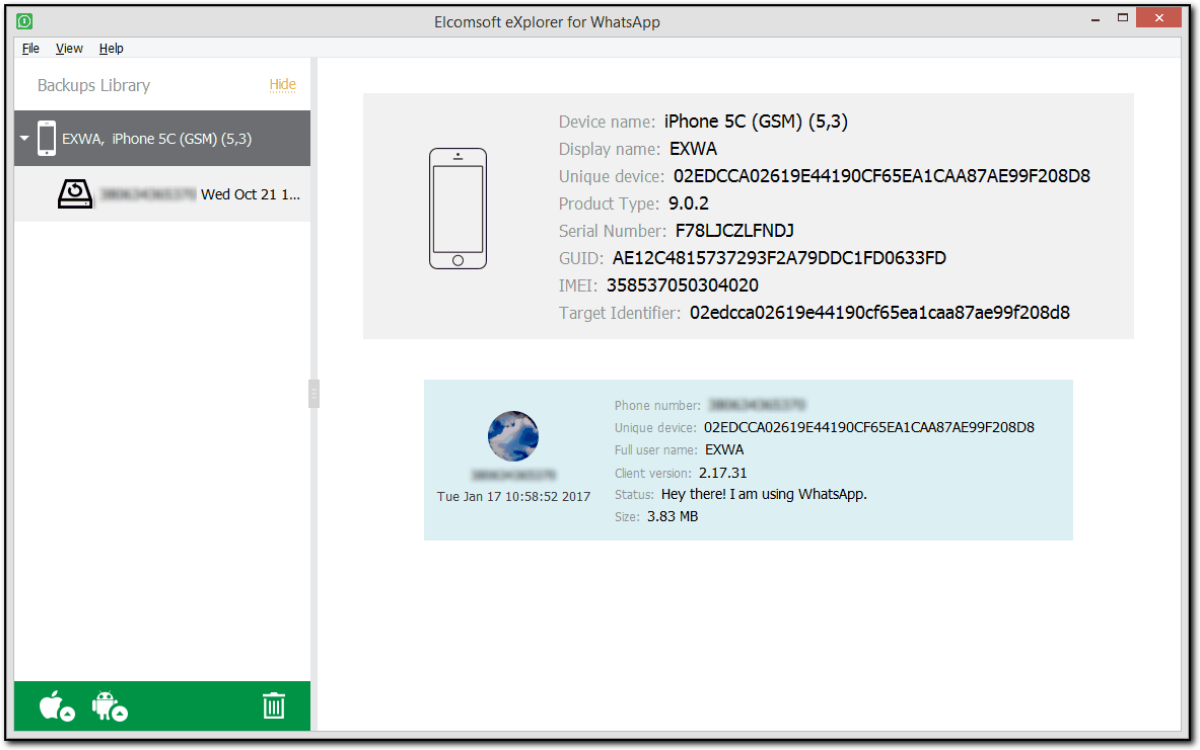
| | **Маркер аутентификации без ограничений для учётной записи с двухфакторной аутентификацией** | **Маркер аутентификации с ограничениями для учётной записи с двухфакторной аутентификацией** | **Маркер аутентификации для учётной записи без двухфакторной аутентификации** |
|---|---|---|---|
| Windows OS | Поддерживается | Не поддерживается | Поддерживается |

## 6.2.2 Adding backups to EXWA

#### 6.2.2.1 Локальные резервные копии

**Как открыть локальную резервную копию**

Данные WhatsApp присутствуют в составе локальных резервных копий в формате iTunes. Для того, чтобы открыть такую резервную копию, нажмите **Acquire data for Apple iOS device/Получить данные для Apple iOS** (иконка  ), затем **Load iTunes/iCloud backup/Загрузка рез. копии из iTunes/iCloud** (иконка  ). Выберите папку с резервной копией и откройте её. Если резервная копия зашифрована, вам потребуется ввести корректный пароль для расшифровки.




**Анализ данных**
Когда вы выбираете целевую резервную копию WhatsApp из списка резервных копий слева, в нижней части окна отображаются все доступные плагины (некоторые из них могут быть отключены, если в резервной копии нет соответствующей информации). Нажмите на один из плагинов, чтобы начать анализ данных.

### 6.2.2.2 Резервные копии в iCloud

**Скачивание резервных копий из iCloud**

Данные WhatsApp присутствуют в составе облачных резервных копий в iCloud. Для того, чтобы открыть такую резервную копию, нажмите **Acquire data for Apple iOS device/Получить данные для Apple iOS** (иконка  ), затем **Download iCloud backup/Скачать рез. копию iCloud** (иконка  ). Выберите папку на диске для сохранения резервной копии. После её скачивания выберите резервную копию из панели в левой части экрана.

Подробная информация о том, как осуществляется авторизация в облако iCloud, доступна в разделе Резервные копии в iCloud.

### 6.2.2.3 Автономные резервные копии в iCloud Drive

## Как скачать автономную резервную копию WhatsApp из iCloud Drive

WhatsApp позволяет создавать автономные резервные копии в iCloud Drive. Для того, чтобы открыть такую резервную копию, нажмите **Acquire data for Apple iOS device/Получить данные**

**для Apple iOS** (иконка ), затем **Download Files from iCloud Drive/Скачать файлы с iCloud Drive** (иконка ).

Подробная информация о том, как осуществляется авторизация в облако iCloud Drive, доступна в разделе Скачивание файлов из iCloud.

Важное отличие автономных резервных копий WhatsApp в iCloud Drive в том, что автономные резервные копии зашифрованы. Ключ шифрования хранится на сервере WhatsApp. Для его получения вам необходима возможность получить SMS с кодом авторизации, для чего можно использовать привязанную SIM-карту пользователя.

Зашифрованные резервные копии отмечены иконкой .
Расшифровка доступна только зарегистрированным пользователям.

Для расшифровки:

1. Выберите резервную копию:


2. Выберите действие:
- **Open/Открыть** откроет резервную копию в состоянии "как есть", с доступом только к медиа-файлам (они хранятся в открытом виде).
- **Decrypt/Расшифровать** позволяет расшифровать резервную копию. Инструкции по расшифровке приводятся ниже.

Для расшифровки доступны два способа:

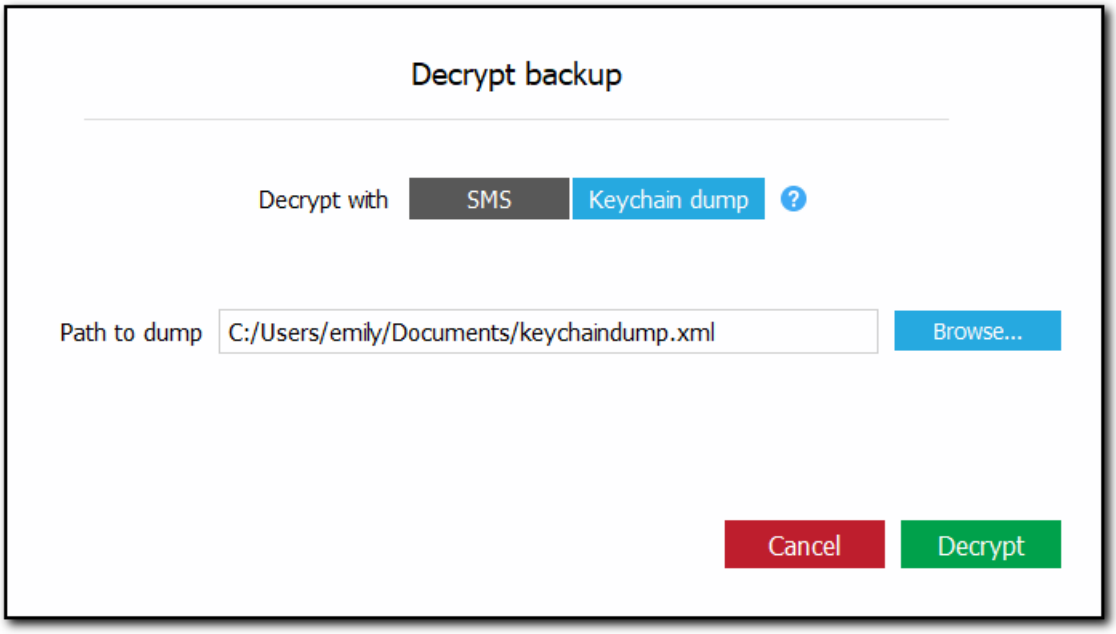
- **SMS**: если у вас есть доступ к SIM-карте пользователя, в поле **Phone number/Номер телефона** введите номер привязанного к WhatsApp телефона и нажмите **Send code/Отправить код**, после чего введите полученный код в поле **Verification code/Код проверки**.

  Если код не был доставлен, нажмите **Resend code/Отправить код повторно**. Вы сможете проделать эту операцию по истечении таймера.

  **ПРИМЕЧАНИЕ. Используя этот тип расшифровки, EXWA не может расшифровать резервную копию, если учетная запись WhatsApp на iOS была защищена двухэтапной проверкой во время создания резервной копии.**

**ПРИМЕЧАНИЕ. Не нажимайте URL-адрес в сообщении с кодом подтверждения. Вы должны ввести код подтверждения вручную, иначе EXWA не будет аутентифицирован в WhatsApp, и вам придется подождать некоторое время, пока не будет отправлен новый код.**


- **Keychain dump/Дамп связки ключей**: в поле **Path to dump/Путь к дампу** введите полный путь к расшифрованному дампу Связки ключей (файл .xml), извлеченному с помощью Elcomsoft iOS Forensic Toolkit (EIFT), или нажмите **Browse/Обзор** и перейдите к файлу.




4. Нажмите **Decrypt/Расшифровать**.

**ПРИМЕЧАНИЕ. Во время расшифровки резервной копии с помощью SMS пользователь выйдет из WhatsApp на устройстве.**

5. После аутентификации EXWA в WhatsApp начинается процесс дешифрования.
Обратите внимание, что после расшифровки резервной копии, связанной с номером телефона, все остальные резервные копии для этого номера телефона будут расшифрованы автоматически после загрузки или при нажатии на резервную копию.
Расшифрованные резервные копии помечаются значком в списке резервных копий.

# 6.3 Устройства Android

## 6.3.1 Данные WhatApp в телефонах Android

EXWA позволяет анализировать данные WhatsApp и WhatsApp Business с некоторых устройств Android.

Загрузка данных WhatsApp с устройств Android доступна как для устройств с root-доступом, так и без него.

Загрузка данных WhatsApp Business с устройств Android доступна только для устройств с root-доступом.

При сохранении данных WhatsApp:

1. Убедитесь, что на устройство установлен root.
2. Скопируйте папку **\data\data\com.whatsapp** с устройства. Обязательно сохраните исходную структуру данных WhatsApp.
3. Запомните путь к файлу **com.whatsapp_preferences.xml** (т.е. **<папка с резервной копией на вашем ПК>\com.whatsapp\shared_prefs**\)
4. Скопируйте папку **\sdcard\WhatsApp** с телефона Android, сохранив исходную структуру данных.
5. Запомните путь к папке **Media (<Папка с резервной копией на вашем ПК>\WhatsApp\Media**).

При сохранении данных WhatsApp Business:

1. Убедитесь, что на устройство установлен root.
2. Скопируйте папку **\data\data\com.whatsapp.w4b** с устройства. Обязательно сохраните исходную структуру данных WhatsApp.
3. Запомните путь к файлу **com.whatsapp.w4b_preferences.xm** (т.е. **<папка с резервной копией на вашем ПК>\com.whatsapp\shared_prefs**\)
4. Скопируйте папку **\sdcard\WhatsApp Business** с телефона Android, сохранив исходную структуру данных.
5. Запомните путь к папке **Media (<Папка с резервной копией на вашем ПК>\WhatsApp Business\Media**).

### 6.3.2 Подключение телефона Android

EXWA позволяет анализировать данные WhatsApp и WhatsApp Business, загруженные непосредственно с устройств Android.

Загрузка данных WhatsApp с устройств Android доступна как для устройств с root-доступом, так и без него.

Загрузка данных WhatsApp Business с устройств Android доступна только для устройств с root-доступом.

Перед загрузкой данных с него нужно включить на устройстве режим отладки по USB:

1. Откройте настройки устройства.
2. Нажмите **About phone** или **About tablet**.
3. Семь раз нажмите надпись **Build number**. Вы увидите сообщение "You are now a developer!".
4. Нажмите **Back**.
5. В настройках Settings > Developer Options > USB Debugging нажмите **USB Debugging**.
6. Нажмите **OK**.

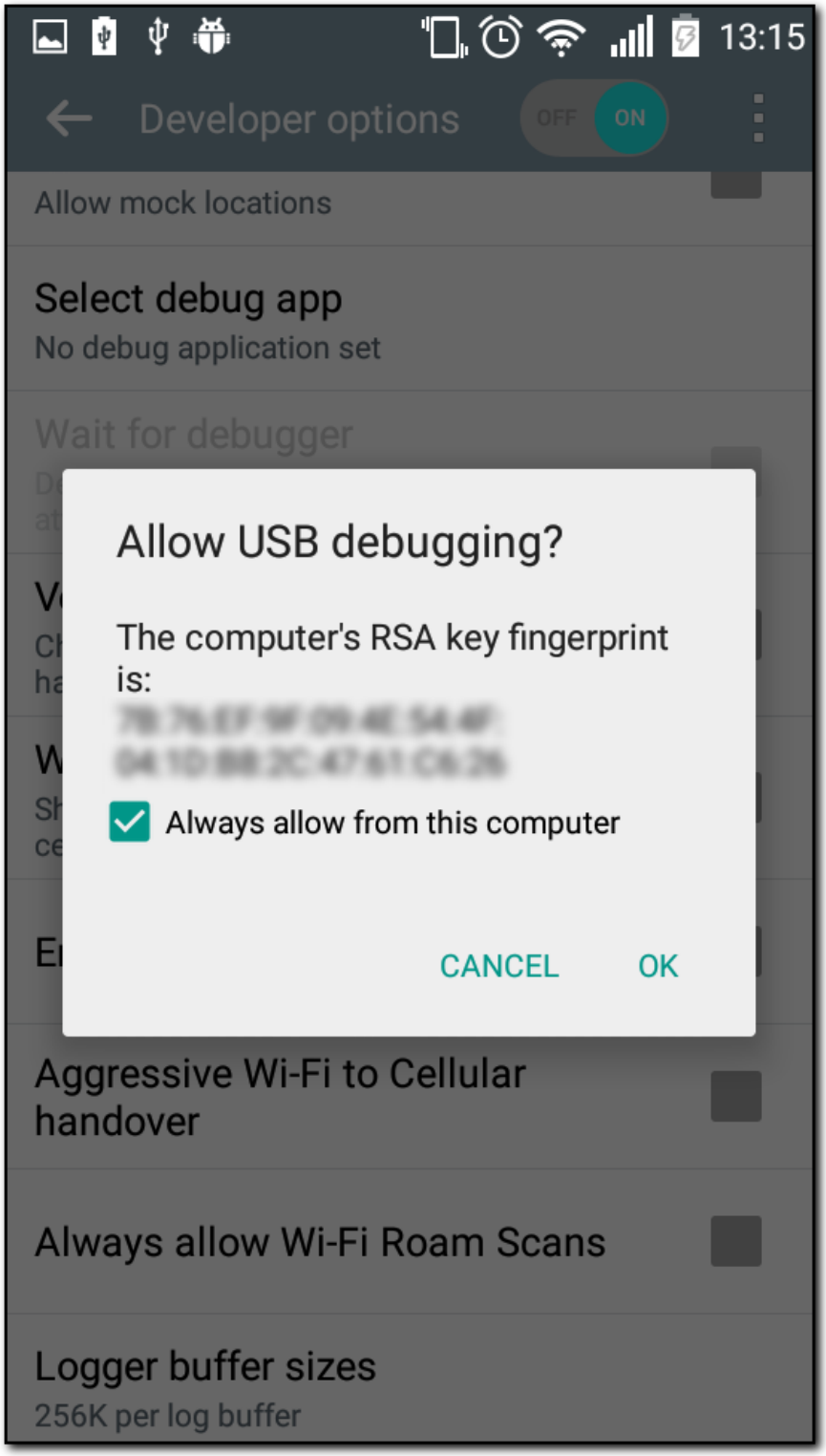
### 6.3.3 Загрузка данных WhatsApp из телефона Android

Подключите телефон к компьютеру и активируйте режим отладки (см. предыдущий раздел).

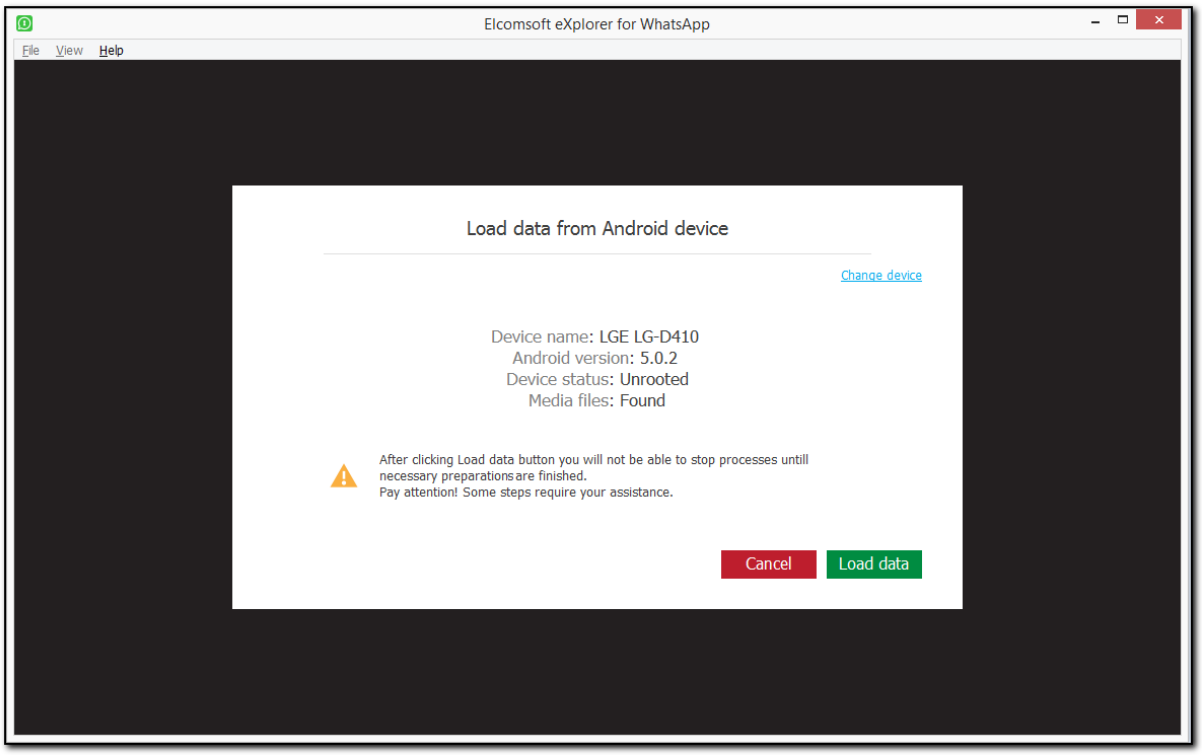
Выберите **Acquire data for Android device/Получить даные для Android** (иконка  ), после чего нажмите **Load from device/Загрузить с устройства**  .

**ПРИМЕЧАНИЕ. Если у вас не установлена последняя версия Java, отобразится сообщение со ссылкой для ее загрузки. Загрузите и установите последнюю версию Java.**

1. Нажмите Выбрать.
2. Подтвердите режим отладки на телефоне:




3. После подключения устройства будет выведена информация о нём:



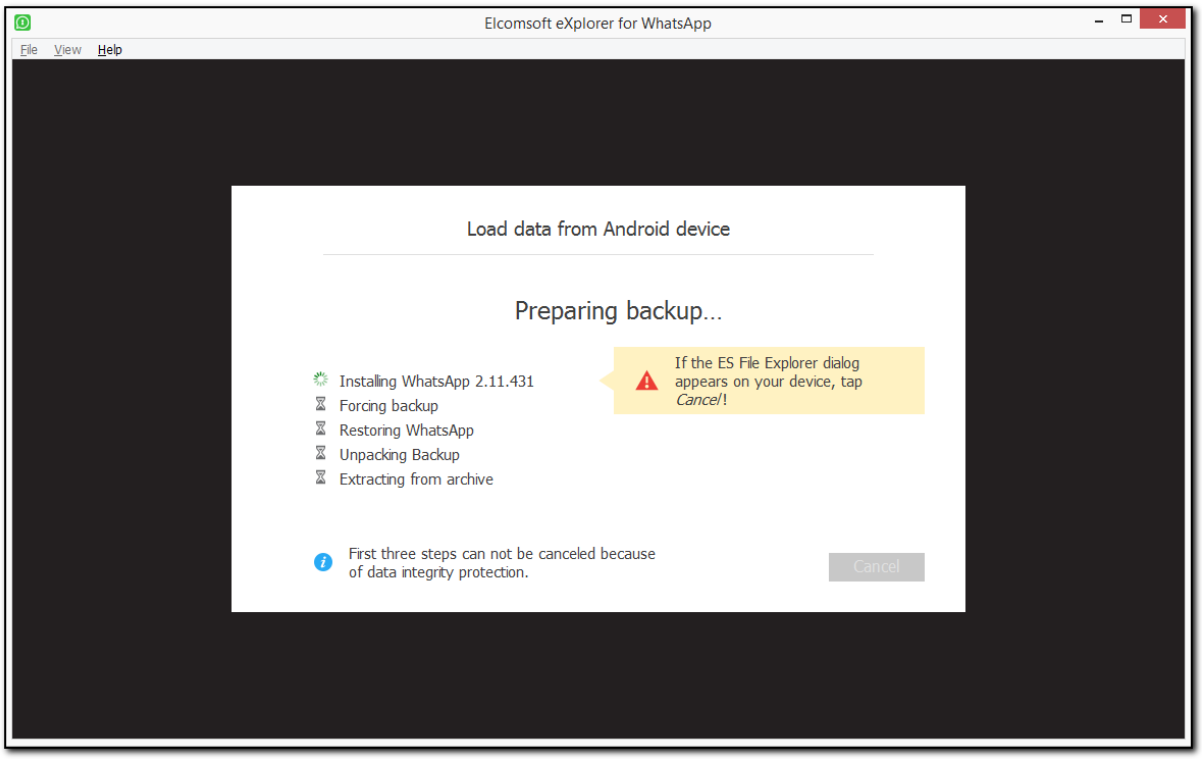

4. Если на устройстве установлены приложения WhatsApp и WhatsApp Business, щелкните значок на кнопке **Load data/Загрузить** и выберите, какие данные вы хотите загрузить. Если вы выберете оба приложения, данные будут отображаться как отдельный снимок для каждого из них.

5. Нажмите **Load data/Загрузить**.

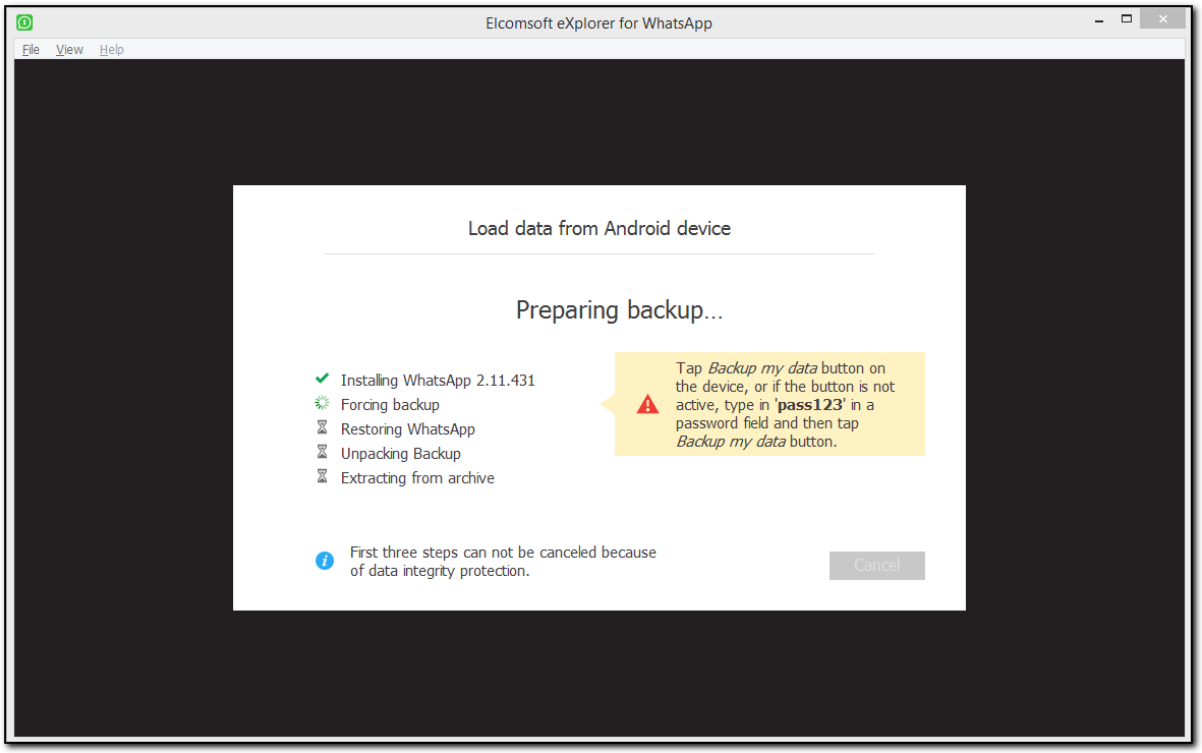
6. Начнется подготовка резервного копирования. Некоторые шаги могут потребовать вашей помощи:

**ПРИМЕЧАНИЕ. Соединение между устройством и компьютером может прерваться во время подготовки из-за состояния демона adbd на устройстве. В этом случае нажмите Check и попробуйте загрузить данные еще раз.**

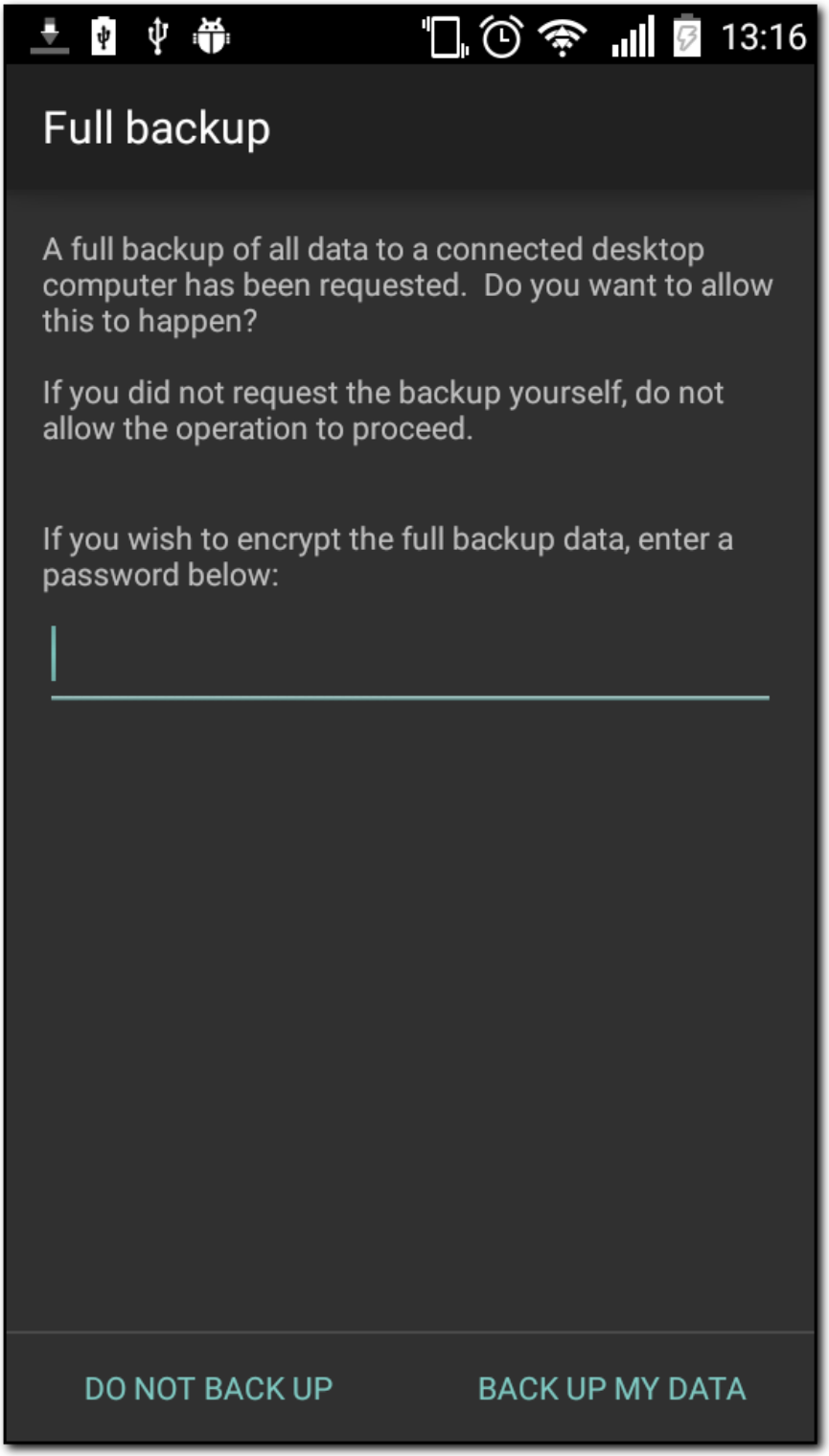
   - **Установка WhatsApp.** Если на устройстве появится диалоговое окно ES File Explorer, коснитесь **Cancel/Отменить**.



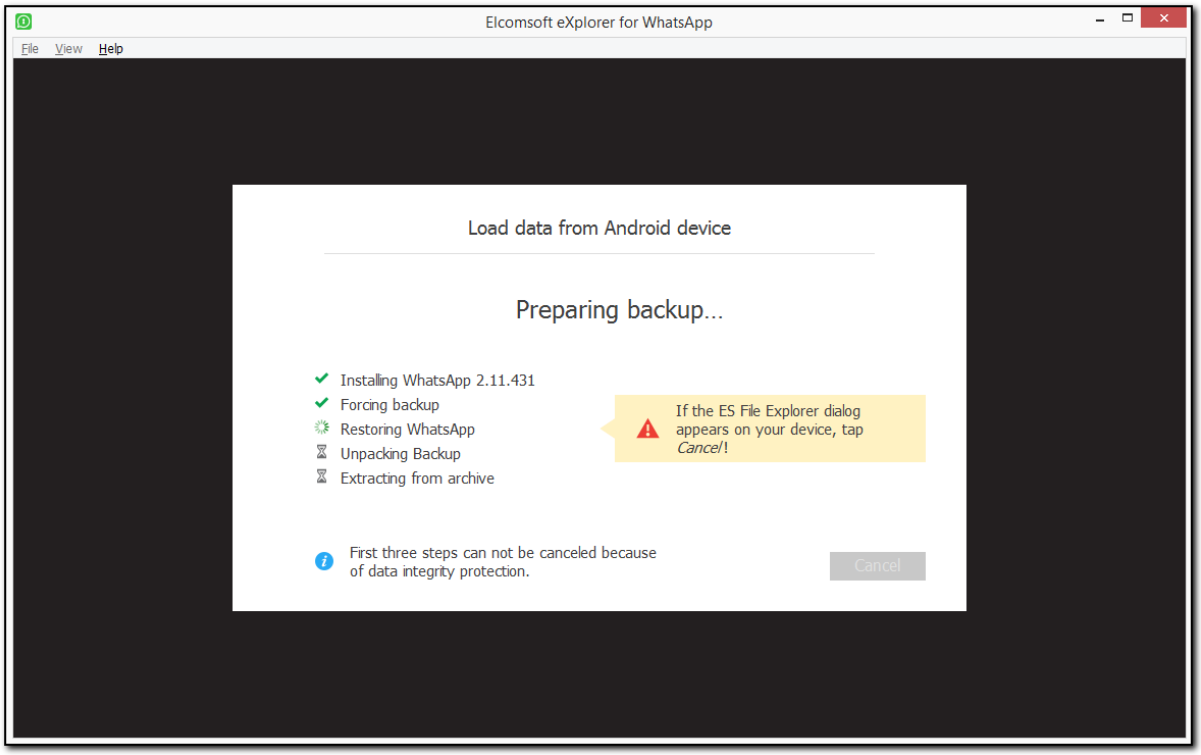

- **Создание резервной копии.**



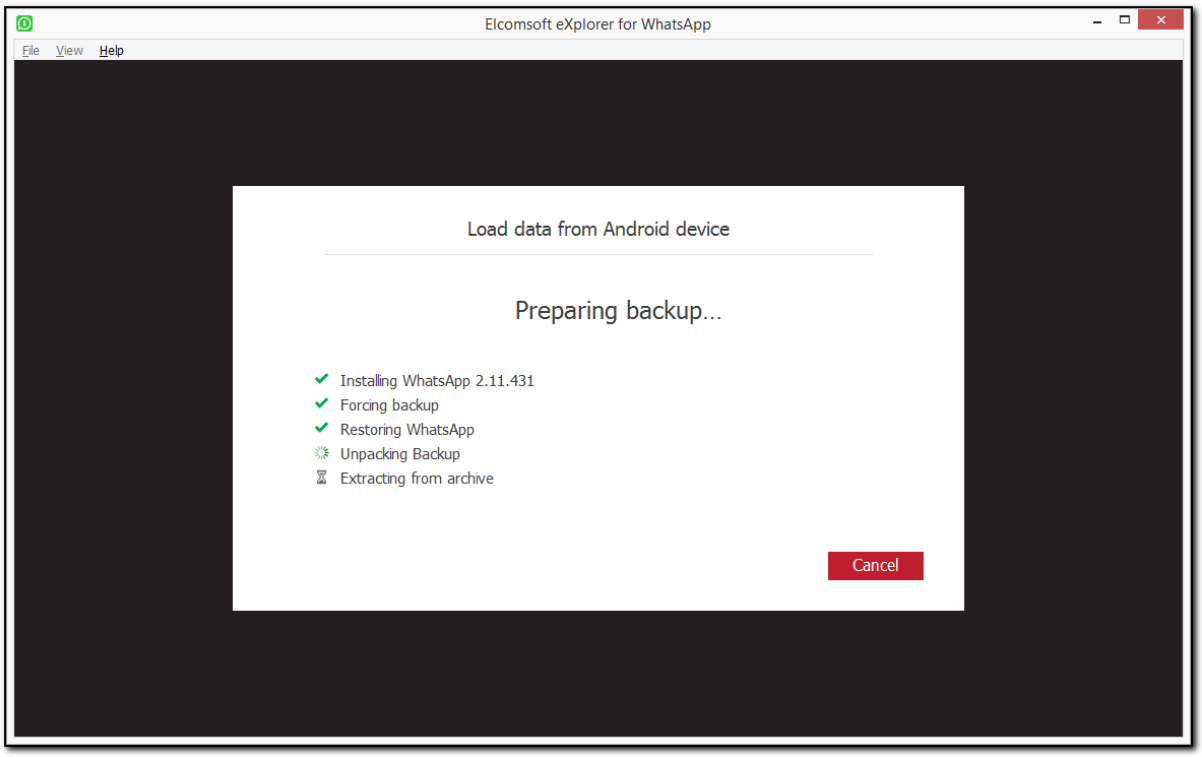
Коснитесь **Backup my data** на телефоне. Если кнопка не активна, введите '**pass123**' в качестве пароля, после чего коснитесь **Backup my data**.



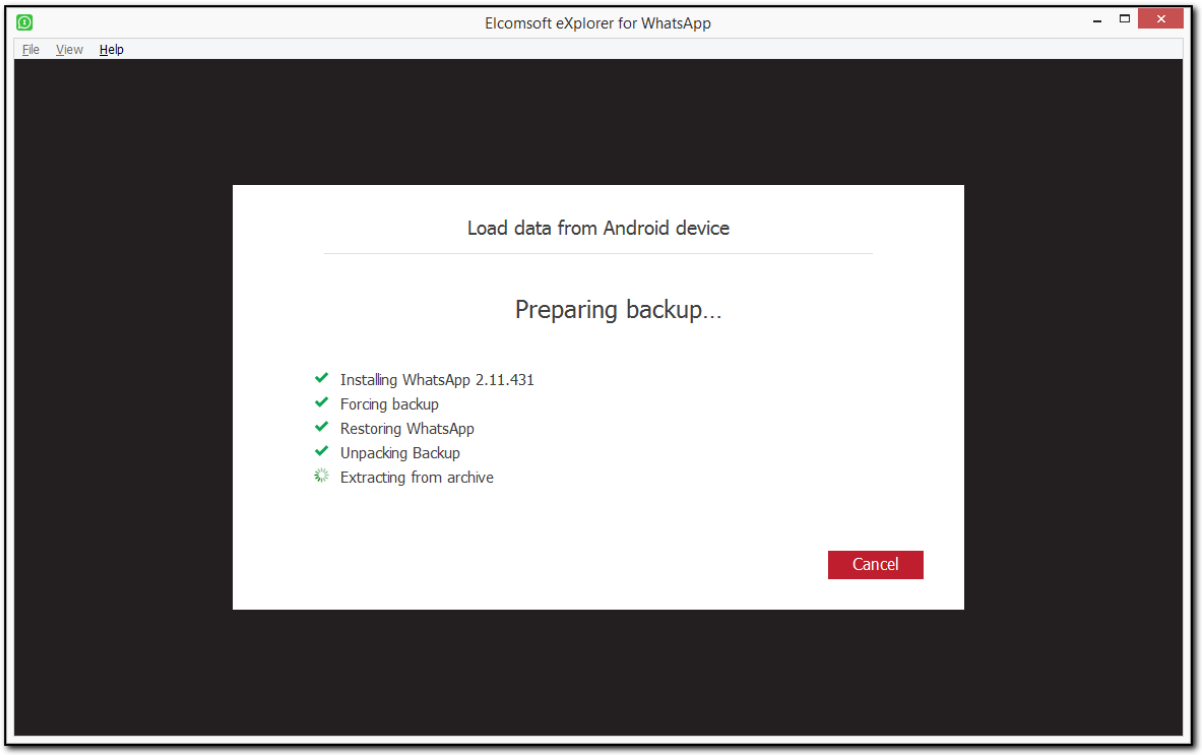
- **Восстановление WhatsApp.** Если на устройстве появится диалоговое окно ES File Explorer, коснитесь **Cancel/Отменить**.



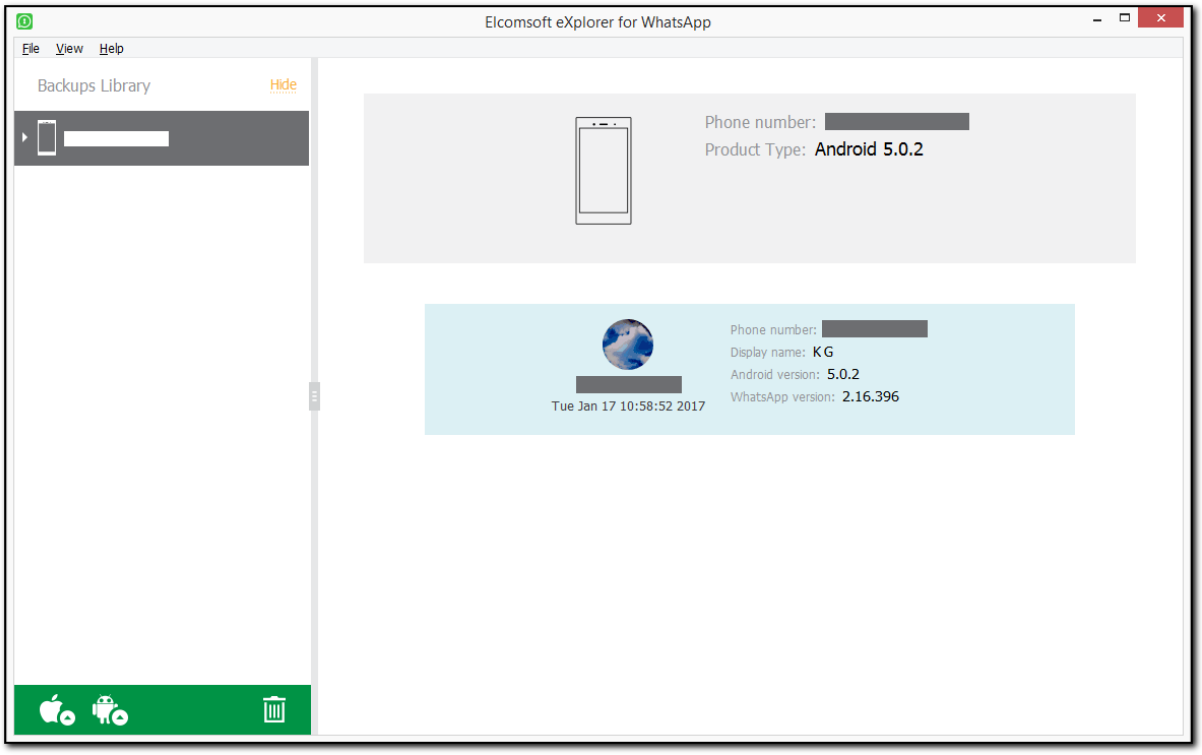

- **Распаковка резервной копии.**




- **Извлечение из архива.**



7. После загрузки резервной копии и обработки данных WhatsApp / WhatsApp Business отображается информация об устройстве.

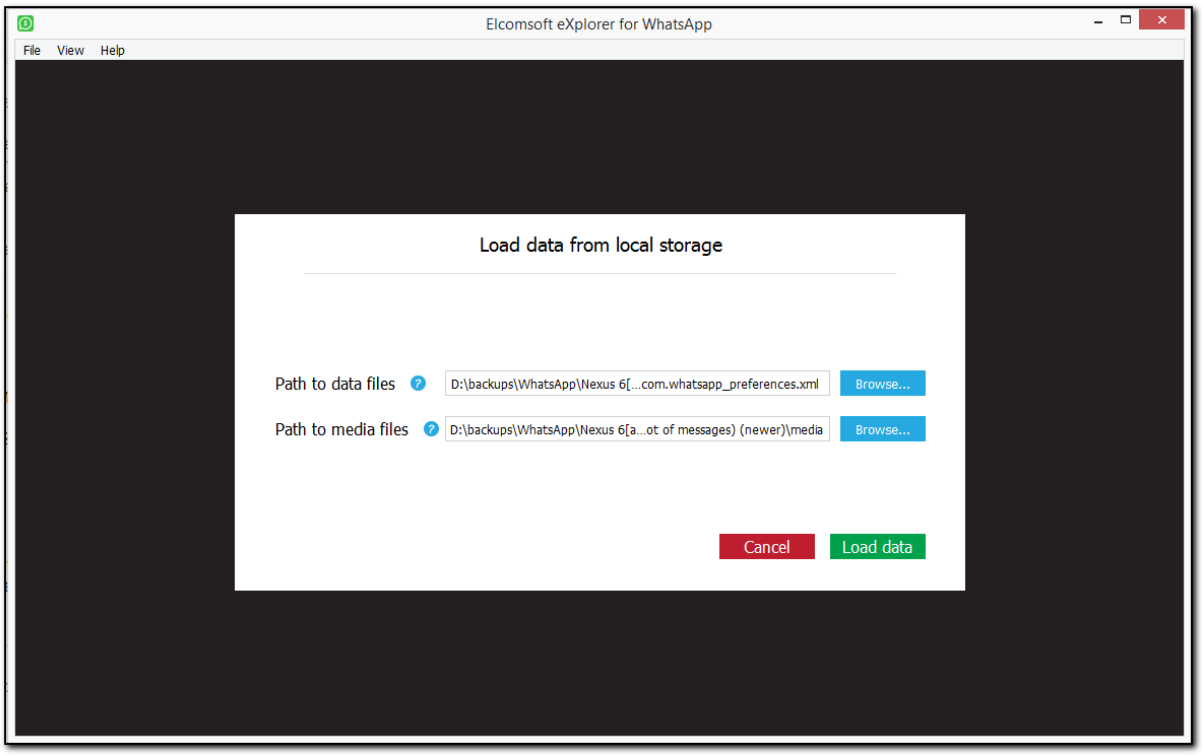



## 6.3.4 Работа с данными WhatsApp из локальной папки

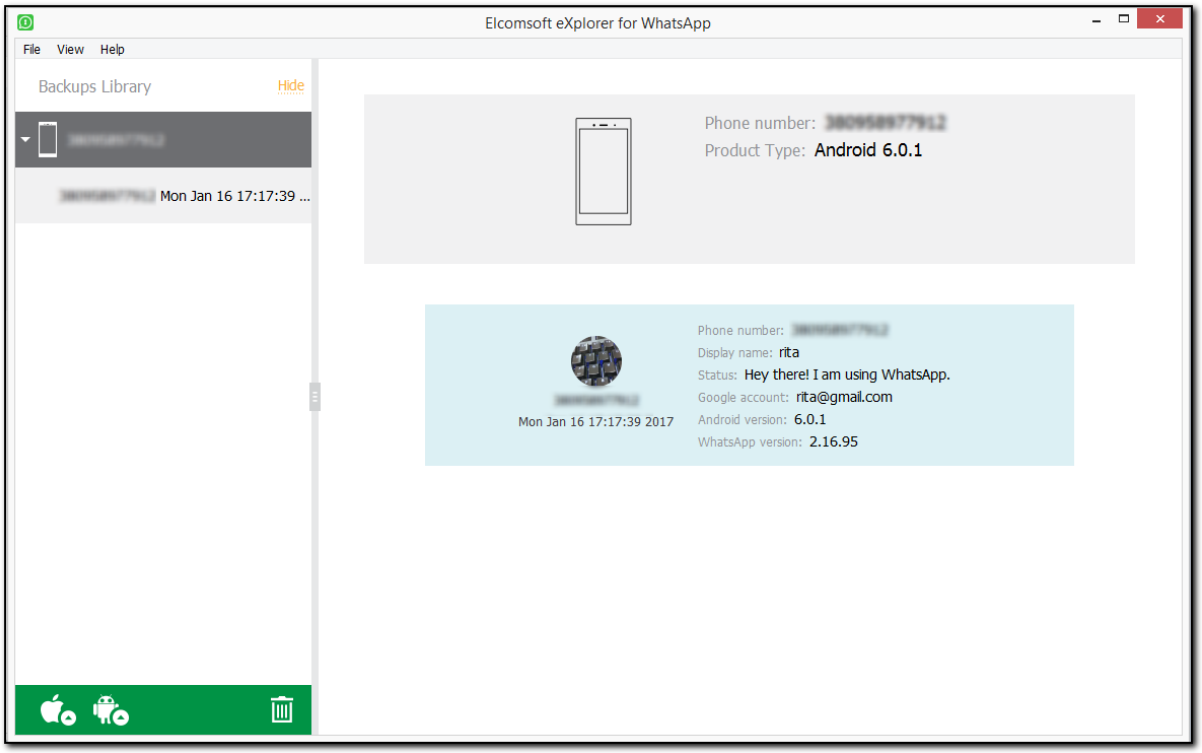
### Загрузка данных WhatsApp из локальной папки

1. Нажмите **Acquire data for Android device/Получить даные для Android** 
2. Нажмите **Load from local storage/Загрузить из локального хранилища**  .
3. Укажите путь к файлу **com.whatsapp_preferences.xml** (WhatsApp) либо **com.whatsapp.w4b_preferences.xml** (WhatsApp Business).

Укажите путь к папке **Media/Медиафайлы** в окне **Path to media files/Путь к медиафайлам**.



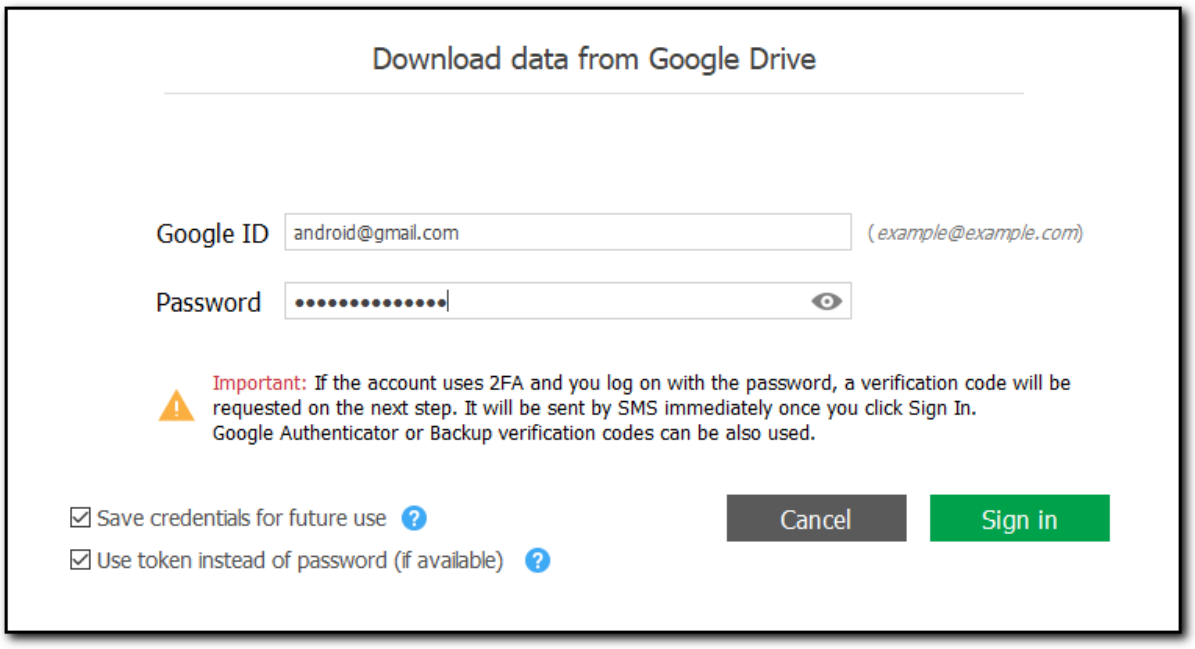

4. Нажмите **Load data/Загрузить**.



### 6.3.5 Загрузка данных WhatsApp из Google Drive

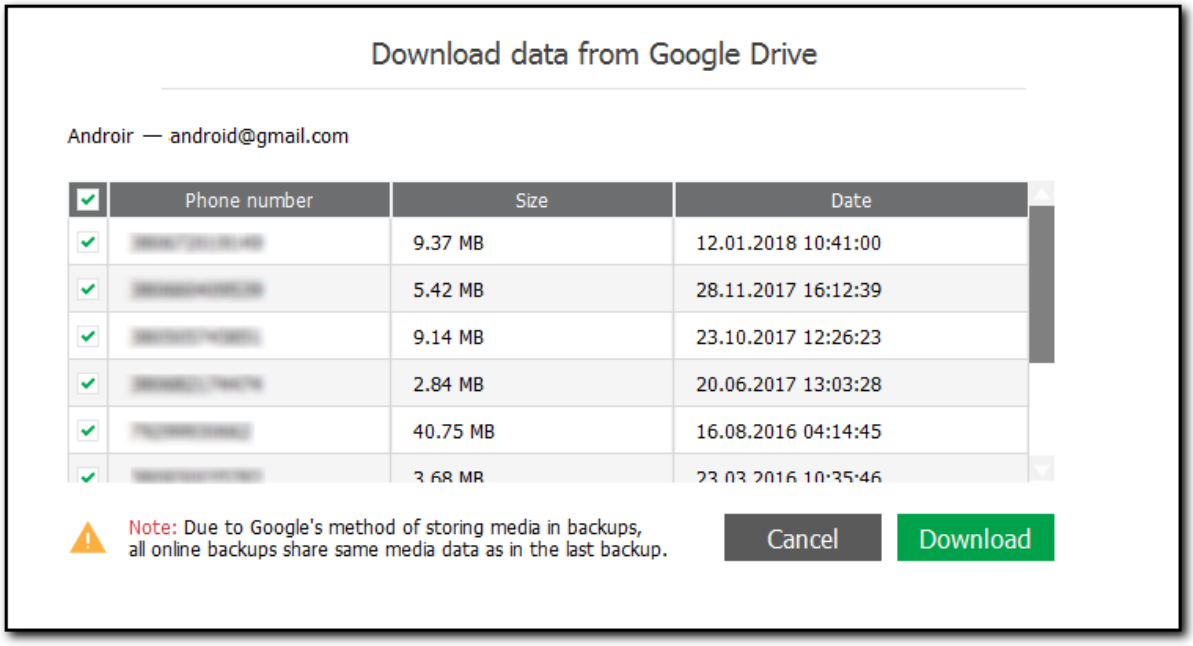
Для загрузки данных WhatsApp из Google Drive, нажмите **Acquire data for Android device/Получить даные для Android**  . После этого нажмите **Download from Google Drive/Скачать с Google Диска**  .

1. Авторизуйтесь в Google Drive по логину и паролю либо посредством маркера аутентификации. Пошаговая инструкция по аутентификации в учётную запись Google в разделе Вход в Google Drive.



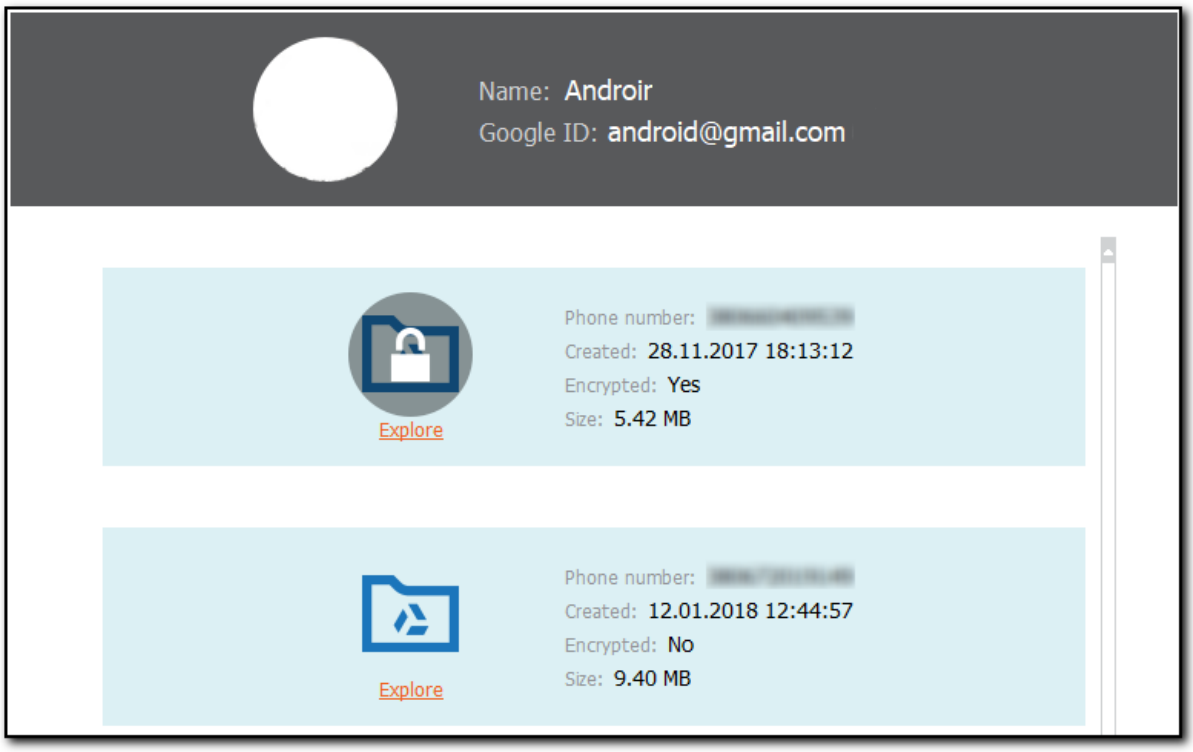

**ПРИМЕЧАНИЕ. EXWA не поддерживает учетные записи Google с защитой CAPTCHA. Вы можете подождать некоторое время, пока защита CAPTCHA не будет отключена, а затем попробуйте снова войти в систему.**

Выберите резервные копии WhatsApp и WhatsApp Business и нажмите **Download/Скачать**.




**ПРИМЕЧАНИЕ. При резервном копировании данных из учетных записей WhatsApp и WhatsApp Business с одним и тем же номером телефона на Google Диск сохраняется только последняя резервная копия. Если вы выполняете резервное копирование данных из учетных записей WhatsApp и WhatsApp Business с разными номерами телефонов, будут созданы две отдельные резервные копии.**

После скачивания резервных копий:



### Зашифрованные резервные копии

Важное отличие автономных резервных копий WhatsApp в iCloud Drive в том, что автономные резервные копии зашифрованы. Ключ шифрования хранится на сервере WhatsApp. Для его получения вам необходима возможность получить SMS с кодом авторизации, для чего можно использовать привязанную SIM-карту пользователя.

Зашифрованные резервные копии отмечены иконкой 🔒.
Расшифровка доступна только зарегистрированным пользователям.

Для расшифровки:

1. Выберите резервную копию:


2. Выберите действие:
   - **Open/Открыть** откроет резервную копию в состоянии "как есть", с доступом только к медиа-файлам (они хранятся в открытом виде).
   - **Decrypt/Расшифровать** позволяет расшифровать резервную копию. Инструкции по расшифровке приводятся ниже.

Для расшифровки доступны два способа:

- **SMS**: если у вас есть доступ к SIM-карте пользователя, в поле **Phone number/Номер телефона** введите номер привязанного к WhatsApp телефона и нажмите **Send code/Отправить код**, после чего введите полученный код в поле **Verification code/Код проверки**.

  Если код не был доставлен, нажмите **Resend code/Отправить код повторно**. Вы сможете проделать эту операцию по истечении таймера.

  **ПРИМЕЧАНИЕ. Не нажимайте URL-адрес в сообщении с кодом подтверждения. Вы должны ввести код подтверждения вручную, иначе EXWA не будет аутентифицирован в WhatsApp, и вам придется подождать некоторое время, пока не будет отправлен новый код.**


4. Нажмите **Decrypt/Расшифровать**.

**ПРИМЕЧАНИЕ. Во время расшифровки резервной копии с помощью SMS пользователь выйдет из WhatsApp на устройстве.**

5. После аутентификации EXWA в WhatsApp начинается процесс дешифрования.
Обратите внимание, что после расшифровки резервной копии, связанной с номером телефона, все остальные резервные копии для этого номера телефона будут расшифрованы автоматически после загрузки или при нажатии на резервную копию.
Расшифрованные резервные копии помечаются значком в списке резервных копий.

## 6.4 Плагины

### 6.4.1 Доступные данные

Полученные данные WhatsApp и WhatsApp Business можно просматривать при помощи плагинов. Каждый плагин отвечает за собственную категорию данных. Для просмотра категории нажмите на соответствующую иконку в окне просмотра данных.

Вы можете просматривать множество категорий данных. В список входят следующие категории:

### Account Info / Учётная запись

Только для WhatsApp Business: данные компании, включая название и адрес.

### Contacts / Контакты

Включает все контакты пользователя, включая их изображения.

## Calls / Звонки

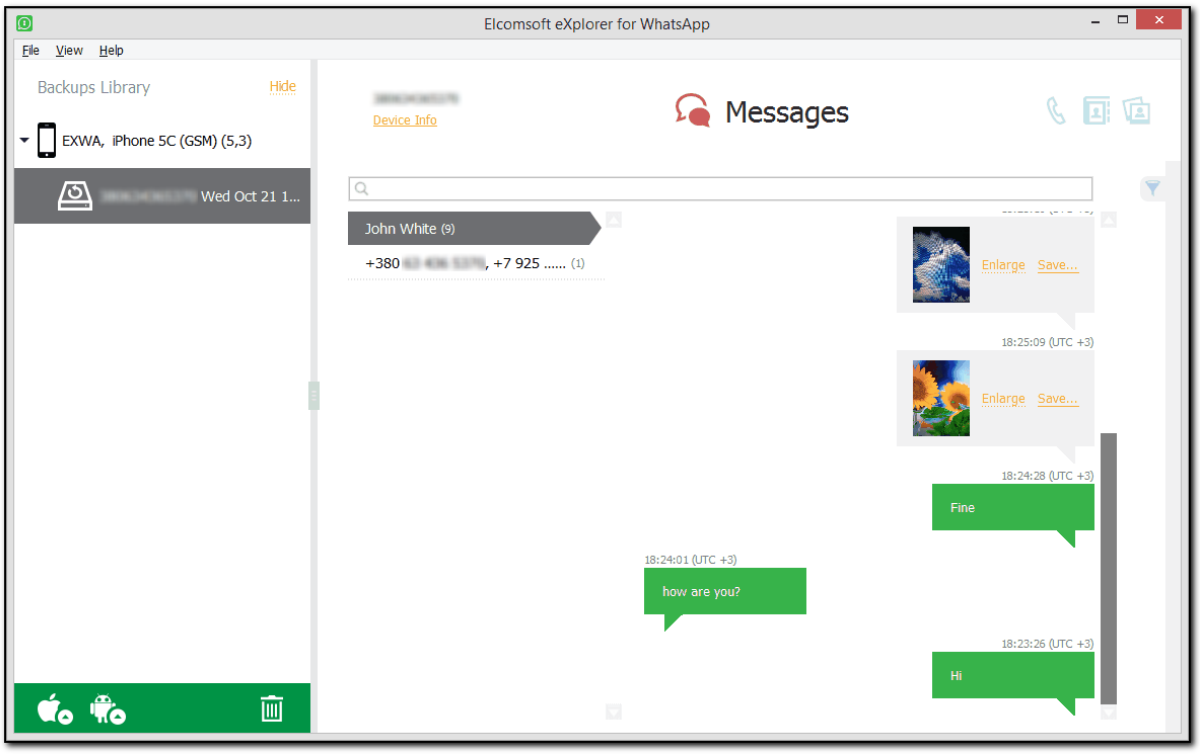
История вызовов исследуемой учетной записи WhatsApp. Вы можете проанализировать полную историю исходящих, входящих, пропущенных и неотвеченных аудио- и видеозвонков.

## Media / Медиафайлы

Все медиа-файлы, отправляемые в чатах WhatsApp, включая изображения, видео (начиная с WhatsApp 2.12.7) и аудиофайлы. Вы также можете просматривать медиафайлы, отправленные определенным контактом.

## Messages / Сообщения

В левой панели окна чатов отображаются в виде списка контактов (номер телефона или имя). Входящие сообщения отображаются слева, а исходящие - справа. Количество сообщений для каждого контакта показано (в скобках). Вы также можете просматривать групповые и архивные чаты, а также системные сообщения.
Смайлы отображаются как в текстах сообщений, так и в контактах.
В резервных копиях WhatsApp Business сообщения и чаты могут быть отмечены значками ярлыков, присвоенных пользователем. Наведите указатель мыши на значок ярлыка, чтобы увидеть его название.



# VII Поддержка и обновления

## 7.1 Контактная информация

Для связи с отделом технической поддержки используйте следующую форму:

https://www.elcomsoft.com/support.html

Все другие запросы (общие вопросы, вопросы продажи и т.п.):

https://www.elcomsoft.com/company.html

Ссылка на скачивание последней версии Mobile forensic Bundle:

https://www.elcomsoft.com/emfb.html

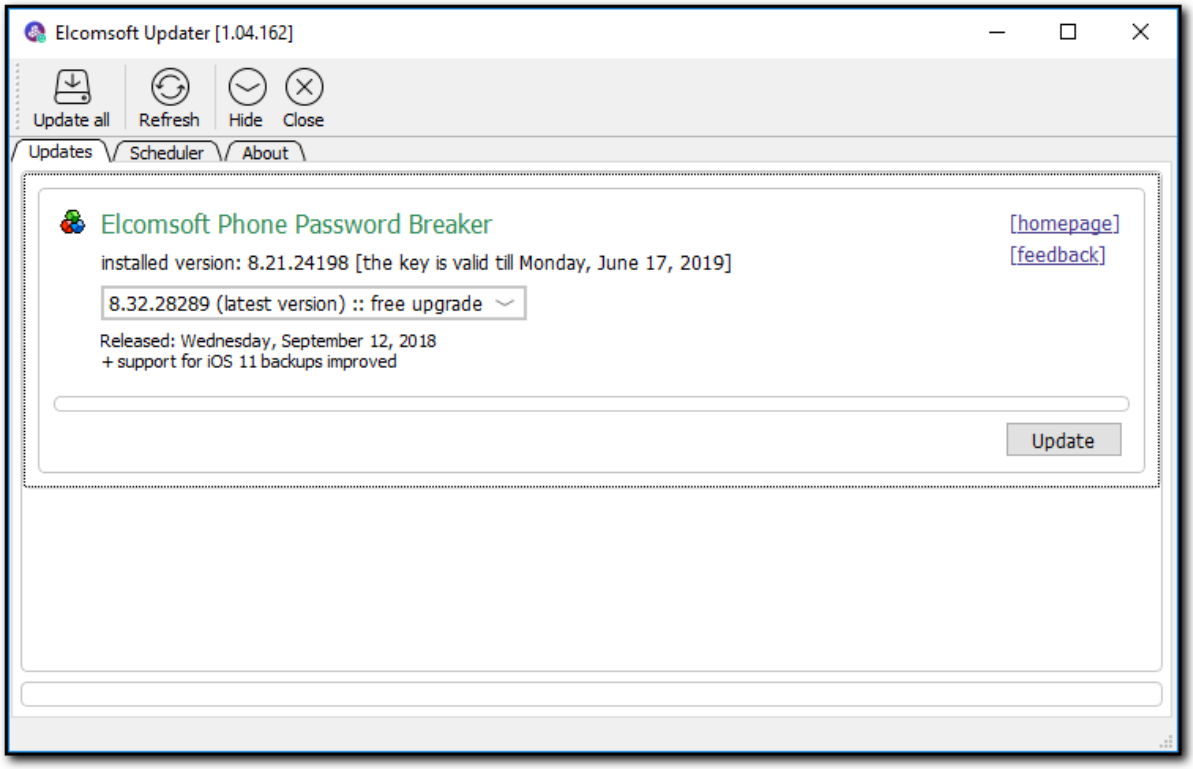
## 7.2 Обновления

Вы можете вручную проверить доступные обновления. Для этого:

1. Запустите **Elcomsoft Updater**.

2. Во вкладке **Updates/Обновления** выберите одно из установленных приложений (например, **Elcomsoft Phone Password Breaker**). Если продукт не присутствует в списке, значит, он либо не установлен на компьютере, либо обновления отсутствуют.

3. Выберите версию приложения из списка и нажмите **Update/Обновить**.



На системах с **macOS** обновления доступны только в ручном режиме. К примеру, для того, чтобы обновить приложение **Elcomsoft Phone Breaker**:

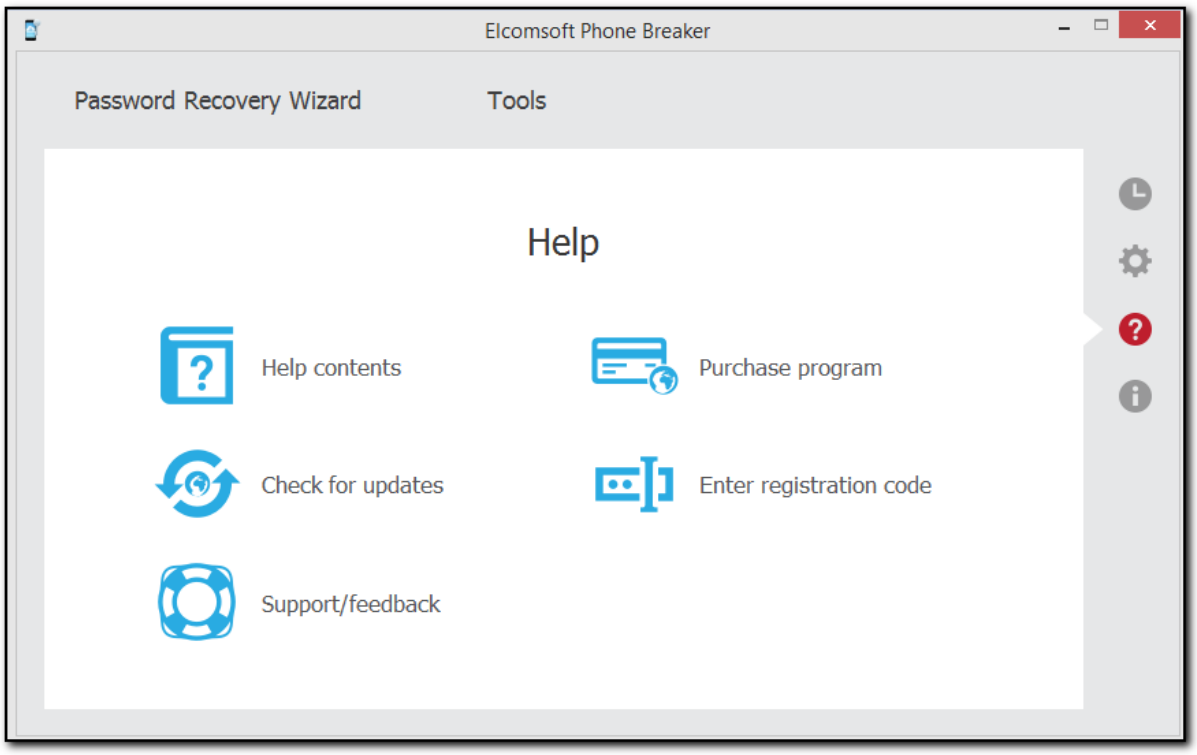
1. В панели **Settings/Настройки** нажмите иконку **Help/Справка**.

2. В открывшейся панели нажмите **Check for updates/Проверка обновлений**.

3. Если обновление доступно, вам будет предложено его скачать. Если обновления отсутствуют, будет выведено соответствующее сообщение.

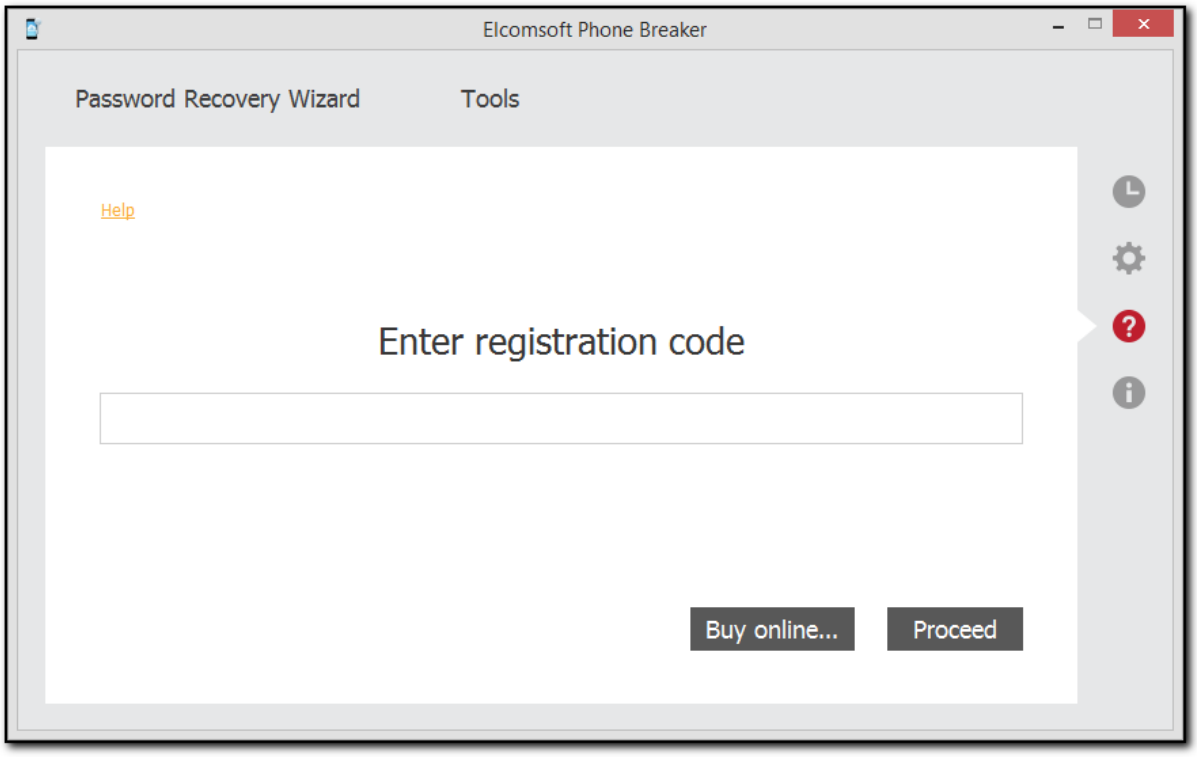
## 7.3 Регистрация

Чтобы приобрести лицензию, воспользуйтесь ссылкой в разделе **Help/Справка** - **Purchase program/Купить программу**. Для Elcomsoft Phone Breaker:




Кроме того, вы можете приобрести любой наш продукт на соответствующей странице с нашего сайта.

Ввести полученный лицензионный ключ можно в окне **Help/Справка** - **Enter registration code/Ввести код регистрации.** Введите полученный ключ в поле **Enter registration code/Введите код регистрации** и нажмите **Proceed/Возобновить**:




## 7.4 Решение проблем

Мы поддерживаем актуальную информация по решению проблем по ссылке Решение проблем