

Elcomsoft Premium Forensic Bundle

Руководство Пользователя

© 2021 ElcomSoft Co.Ltd.

Оглавление

Часть I Введение	13
Часть II Установка программного обеспечения	15
Часть III Основные принципы нахождения паролей	21
1 Основные способы парольной защиты	22
2 Восстановление стойких паролей	22
Прямой перебор (Brute-force)	22
Атака по маске	22
Атака по словарю	24
Словарные мутации	24
Гибридная атака с правилами	30
Часть IV Программы для восстановления паролей	33
1 Advanced Archive Password Recovery	34
Введение	34
Требования	35
Как работать с программой	35
Выбор параметров	35
Открытие архива	35
Тип атаки	35
Параметры диапазона перебора	35
Начать с пароля	36
Маска пароля	36
Длина пароля	36
Параметры словаря	36
Plaintext атака (ZIP)	38
Plaintext атака (ARJ)	38
Гарантированная атака WinZip	39
Пароль из ключей	39
Автосохранение	40
Другие настройки	40
Продвинутые настройки	41
Сохранение и чтение настроек	41
Сохранение и чтение настроек	41
Тест производительности	41
Тест производительности	41
Получение результатов	42
Процесс восстановления	42
Статус программы	42
Результаты	43
Известные ошибки и ограничения	43
Известные ошибки и ограничения	43
Советы и рекомендации	44
Файлы с разными паролями	44
С чего начать	44

Командная строка	44
Благодарности	46
Благодарности	46
2 Advanced Intuit Password Recovery	46
Введение	46
Program information	47
Системные требования	47
Работа с AINPR	47
Пароли Quicken	47
Пароли QuickBooks	48
3 Advanced Lotus Password Recovery	49
Введение	49
Системные требования	50
Работа в программе ALPR	50
4 Advanced Mailbox Password Recovery	50
Введение	50
Системные требования	51
Работа с AMBPR	51
Пользовательский интерфейс	51
Восстановление	52
Поиск почтовых клиентов	52
Автоматическое восстановление паролей	52
Восстановление пароля вручную	52
Эмулятор почтового сервера (автоматический режим)	52
Эмулятор почтового сервера (ручной режим)	53
Параметры	53
Выход	54
5 Advanced Office Password Breaker	54
Введение	54
Системные требования	54
О шифровании Word и Excel	54
Поддерживаемые и неподдерживаемые форматы	55
Работа с AOPB	56
Предисловие	56
Поиск ключа шифрования	56
Расшифровка документа	58
Радужная атака	58
Параметры	60
Интерфейс командной строки	61
6 Advanced Office Password Recovery	62
Введение	62
Подготовка к работе с AOPR	62
Системные требования	62
Поддерживаемые типы файлов и пароли	63
Поддерживаемое оборудование	65
Получение справки и технической поддержки	65
Наши контакты	65
Где приобрести последнюю версию	65
Работа с AOPR	66
Восстановление паролей к документам	66
Выбор файла	66
Анализ результатов	66

Работа с проектами	67
Создание проекта	67
Сохранение проекта	67
Почтовые аккаунты Outlook	67
Восстановление паролей учетных записей электронной почты	67
Типы хранения паролей Outlook®	68
Сохраненные пароли Microsoft Passport	69
Обход защиты VBA	69
Настройка параметров AOPR	70
Тип атаки	70
Предварительная атака	70
Настройка предварительной атаки	71
Общие настройки	72
Другие настройки	72
Кэш паролей	73
О кэше паролей	73
Управление файлами кэша паролей	73
Руководство по паролям	73
Стойкие пароли	74
Пароль на открытие файла Word/Excel (Office 97/2000)	74
Пароль на открытие файла Word/Excel/Pow erPoint (Office XP/2003)	74
Пароль на открытие файла Microsoft OneNote	75
Пароль на открытие файла Microsoft Money 2002+	75
Пароль на открытие файла Office 2007 и более поздних версий	76
Слабые пароли	76
Пароль на открытие файла Word/Excel (слабое шифрование)	76
Visual Basic for Applications (VBA)	76
Microsoft Access	77
Общий пароль к базе данных Access, информация о владельце	77
Пользовательские пароли Access	79
Microsoft Excel	81
Документ Excel - все пароли кроме пароля на открытие	81
Защита надстроек Excel® (XLA)	82
Pocket Excel	82
Microsoft Word	82
Документ Word® - все пароли, кроме пароля на открытие	82
Microsoft Outlook	83
Пароль файла личного хранилища Outlook®	83
Пароли учетных записей электронной почты Outlook®	83
Microsoft Pow erPoint	83
Microsoft Money	84
Microsoft Project	84
Устранение неполадок	84
Создание журнала отладки	84
Пробная версия AOPR и регистрация	85
Ограничения пробной версии	85
Регистрация	85
7 Advanced PDF Password Recovery	85
Введение	85
Системные требования	86
О программе	87
О PDF шифровании	87
Выбор атаки	89
Зашифрованный PDF-файл	89

Типы атак	90
Настройки брутфорса	90
Начать с пароля	90
Маска пароля	91
Длина пароля	91
Опции словарной атаки	91
Поиск ключа	92
Автосохранение	93
Другие параметры	93
Дополнительные параметры	94
Сохранение и чтение настроек	94
Сохранение и чтение настроек	94
Бенчмарки	95
Бенчмарк	95
Получение результата	95
Процесс восстановления	95
Состояние программы	95
Результаты	96
Советы	97
С чего начать	97
Командная строка	98
Сообщения об ошибках	100
8 Advanced Sage Password Recovery	102
Введение	102
О программе	103
Системные требования	103
Восстановление паролей для АСТ!	103
Восстановление паролей для PeachTree/Accounting	104
Другие продукты Sage	104
9 Advanced SQL Password Recovery	104
Введение	104
О программе	105
Системные требования	105
Работа с ASQLPR	105
10 Advanced WordPerfect Office Password Recovery	106
Введение	106
Системные требования	106
Как работать с AWOPR	106
11 Elcomsoft Internet Password Breaker	107
Введение	107
О программе	108
Системные требования	108
Outlook PST пароли	108
Internet Explorer пароли	109
Другие пароли	112
Пароли почты и новостей	113
Типы хранения паролей	115
Опции	115
Отчеты и экспорт паролей	116
12 Elcomsoft Wireless Security Auditor	116
Введение	116
О программе	117

Системные требования	117
О безопасности беспроводных сетей	117
Как работать с EWSA	117
Захват сетевых пакетов	119
Установка NDIS драйвера	122
Аппаратное ускорение	122

Часть V Программы для работы с системой и восстановления данных	123
1 Advanced EFS Data Recovery	124
Введение	124
Работа с AEFSDR	125
Информация о EFS (Encryption File System)	125
Как работает Advanced EFS Data Recovery	126
Режим мастера	127
Поиск ключей шифрования	127
Поиск зашифрованных файлов	131
Обзор зашифрованных файлов	133
Расшифровка файлов	134
Настройки программы	134
Системные требования	135
2 Elcomsoft Forensic Disk Decryptor	136
Введение	136
О программе	137
Системные требования	137
Как работать с EFDD	138
Извлечение ключей	142
Расшифровка и монтирование диска	144
TrueCrypt и VeraCrypt	147
3 Elcomsoft Password Digger	148
Introduction	148
Program information	149
System requirements	149
Working with the program	149
Obtaining keychain files	150
Program options	151
Technical support	151
Contacting us	151
Where to get the latest version	151
License and registration	152
Copyright and license	152
Registration	157
Legal notices	157
4 Elcomsoft System Recovery	159
Введение	159
О программе	161
Важно: О совместимости	161
Создание загрузочного носителя	162
Как использовать ESR	163
Загрузка с CD или USB-устройства	163
Драйверы запоминающих устройств	166
ДБ-источник и режим работы	167

Выбор ОС или расположения файлов SAMAD	170
Учетные записи локальных пользователей	173
Учетные записи AD	176
Кэшированные учетные записи домена	176
Редактор базы данных SAM	178
Инструменты работы с дисками	179
Разблокировать диски от BitLocker	181
Другое	182
5 Proactive Password Auditor	183
Введение	183
Системные требования	184
О программе	185
О Windows паролях	185
Как работать с PPA	185
Получение хэшей паролей	186
Данные аутентификации	188
Взлом паролей	188
Методы взлома паролей	188
Радужная атака	189
Процесс восстановления и результаты	191
Отчеты	192
Настройки программы	193
Часть VI Мобильная криминалистика	195
1 Введение	196
2 Elcomsoft Phone Breaker	198
Информация о программе	198
Пользовательский интерфейс	198
Раздел настроек	199
[Windows] Аппаратное ускорение	205
Работа с устройствами Apple	205
Анализ резервных копий iTunes и iCloud	205
Keychain Explorer: анализ Связки ключей	207
Резервные копии iTunes	215
О резервных копиях iTunes	215
Резервные копии без пароля	217
Резервные копии с паролем	219
Отчёт о расшифровке	222
Экспорт списка резервных копий	223
Работа с iCloud	224
Резервные копии в iCloud	224
Резервные копии в iCloud	224
Скачивание резервных копий из iCloud	225
Выборочное скачивание	231
Экспорт списка резервных копий	235
Возможные проблемы с загрузкой данных из iCloud	236
Структура резервных копий в iCloud	237
Файлы в iCloud	239
Скачивание файлов из iCloud	239
Экспорт списка файлов в iCloud	242
Скачивание синхронизированных данных из iCloud	243
Маркеры аутентификации iCloud	252
Маркеры аутентификации	252

Извлечение маркера аутентификации: Windows	253
Извлечение маркера аутентификации: Windows, система с активной пользовательской сессией	253
Извлечение маркера аутентификации: Windows, сторонний компьютер или образ диска	256
Извлечение маркера аутентификации: macOS	259
Извлечение маркера аутентификации: macOS, система с активной пользовательской сессией	259
Извлечение маркера аутентификации: macOS, сторонний компьютер или образ диска	262
Работа с данными из Microsoft Account	263
Данные в учётных записях Microsoft	263
Скачивание данных из Microsoft Account	264
[Windows] Восстановление паролей	268
Восстановление паролей	268
Настройка атаки	272
Сохранение сеансов атак	273
Настройка атаки по словарю	276
Настройка атаки методом полного перебора	280
Шаблоны	283
Сохранение шаблонов	283
Просмотр шаблонов	284
Загрузка шаблонов	284
Использование шаблонов в атаках	286
3 Elcomsoft Phone Viewer	287
О программе	287
Настройки	287
Поддерживаемые резервные копии Apple	288
Данные Microsoft Account	288
Анализ данных Apple	288
Резервные копии iTunes	288
Резервные копии iCloud	289
Образ файловой системы iOS	290
Анализ резервных копий iOS	290
Анализ образа файловой системы	292
Анализ синхронизированных данных iCloud	295
Анализ данных Microsoft Account	297
Данные Microsoft Account	297
Плагины	297
Просмотр, поиск и анализ данных	297
Экспорт данных	298
Связка ключей	298
Доступные данные	301
4 Elcomsoft Cloud Explorer	306
О программе	306
Пользовательский интерфейс	306
Окно настроек	306
Изменение пути к хранилищу	307
Данные из Google Account	308
Аутентификация	308
Скачивание данных из Google Account	311
Отчёты	314
Экспорт данных	317
Двухфакторная аутентификация	319

Исключения и особые случаи	321
Данные в Google Drive	322
Вход в Google Drive	322
Скачивание данных из Google Drive	325
Экспорт данных	326
Извлечение маркеров аутентификации Google	327
О приложении Google Token Extractor	327
Extracting token on Windows OS	328
Извлечение маркеров аутентификации: macOS	330
Плагины	332
Просмотр, поиск и анализ данных	332
Экспорт данных	334
Доступные данные	334
История местоположений - Locations	336
История местоположений	336
Личный кабинет Google - Dashboard	336
Личный кабинет Google	337
5 Elcomsoft eXplorer for WhatsApp	338
О программе	338
Окно настроек	338
Совместимые устройства	338
Изменение пути к файлам	338
Экспорт данных	339
Устройства Apple	339
Резервные копии WhatsApp	339
Создание резервной копии WhatsApp	339
Маркеры аутентификации	340
Adding backups to EXWA	340
Локальные резервные копии	340
Резервные копии в iCloud	341
Автономные резервные копии в iCloud Drive	341
Устройства Android	344
Данные WhatsApp в телефонах Android	344
Подключение телефона Android	345
Загрузка данных WhatsApp из телефона Android	345
Работа с данными WhatsApp из локальной папки	352
Загрузка данных WhatsApp из Google Drive	353
Плагины	357
Доступные данные	357
6 Elcomsoft iOS Forensic Toolkit	359
Описание продукта	359
Системные требования	359
Использование продукта	359
Совместимость	360
Подготовительный этап	360
Основной экран	361
'I' – Информация об устройстве	363
'R' – Информация об устройстве в режиме восстановления или DFU	364
Логическое извлечение данных	365
'B' – Создание резервной копии	365
'M' – Извлечение медиа-файлов (фото и видео)	367
'S' – Файлы приложений	368
'L' – Журнал crash logs	368

Физическое извлечение данных с помощью джейлбрейка: полная файловая система и извлечение связки ключей	368
Настройка устройства iOS	369
Установка джейлбрейка	369
Извлечение данных	370
Установка OpenSSH	370
Установка запрета блокировки экрана	371
Расшифровка связки ключей keychain	371
Извлечение образа файловой системы	372
Расшифровка связки ключей	372
Извлечения данных с помощью Агента	373
Общая информация и требования	373
Извлечение данных	374
Удаление агента	374
Поддержка устаревших устройств (iPhone 4, 5, 5c)	374
Перевод в режим DFU и установка эксплойта	375
Восстановление кода блокировки экрана	375
Извлечение связки ключей	376
Снятие и расшифровка образа диска	376
Анализ данных	377
Приложение А. Совместимые устройства	377
Приложение В. Инструкции по установке джейлбрейка	379
Приложение С. Проблемы и способы их решения	382

Часть VII Лицензионное соглашение **385**

Index **393**

Часть I

Введение

1 Введение

В состав **Elcomsoft Premium Forensic Bundle** входят все продукты компании из линеек компьютерной и мобильной криминалистики. Каждый продукт поставляется в максимальной редакции. Набор продуктов позволяет восстанавливать доступ к зашифрованным данным и подбирать пароли к защищённым документам за минимально возможное время. Продукты для мобильной криминалистики позволяют извлекать и расшифровывать данные как из физических устройств, так и из локальных резервных копий и облачных сервисов. В состав пакета включены продукты для извлечения, просмотра и анализа данных.

Продукты ElcomSoft базируются на самых современных научных разработках и претендуют на первенство как в области производительности программного кода, так и по соотношению цена-качество.

Часть II

Установка программного обеспечения

2 Установка программного обеспечения

Elcomsoft Premium Forensic Bundle поставляется единым инсталляционным пакетом.

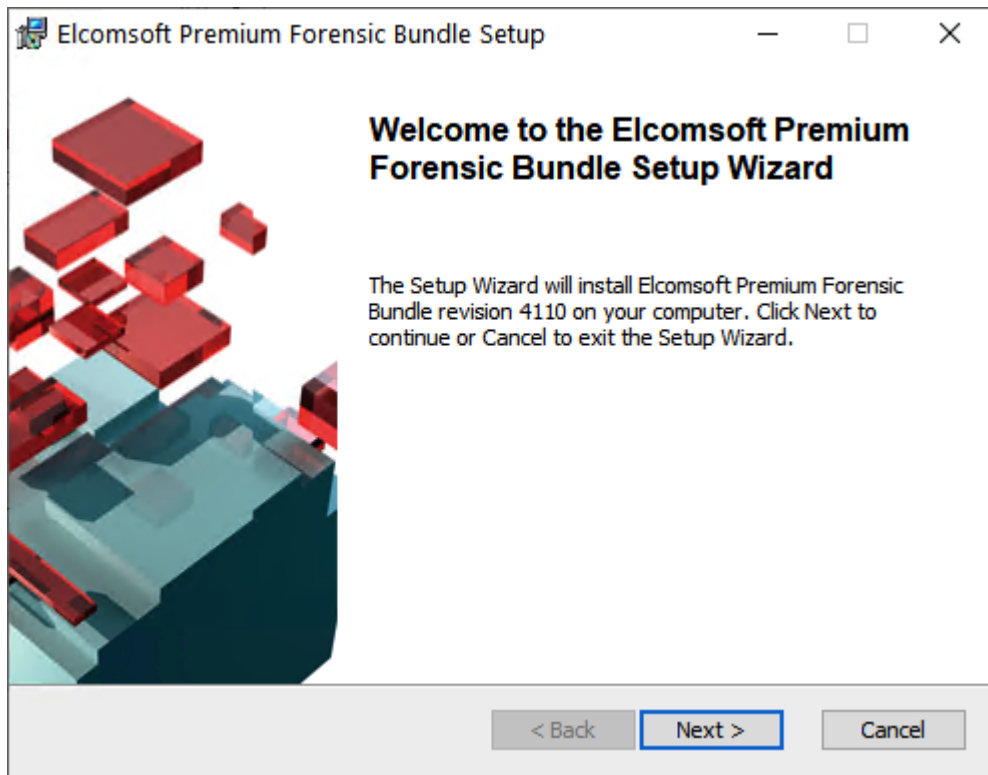
URL для загрузки: https://www.elcomsoft.com/download/eprfp_setup_en.msi

Минимальные системные требования для установки:

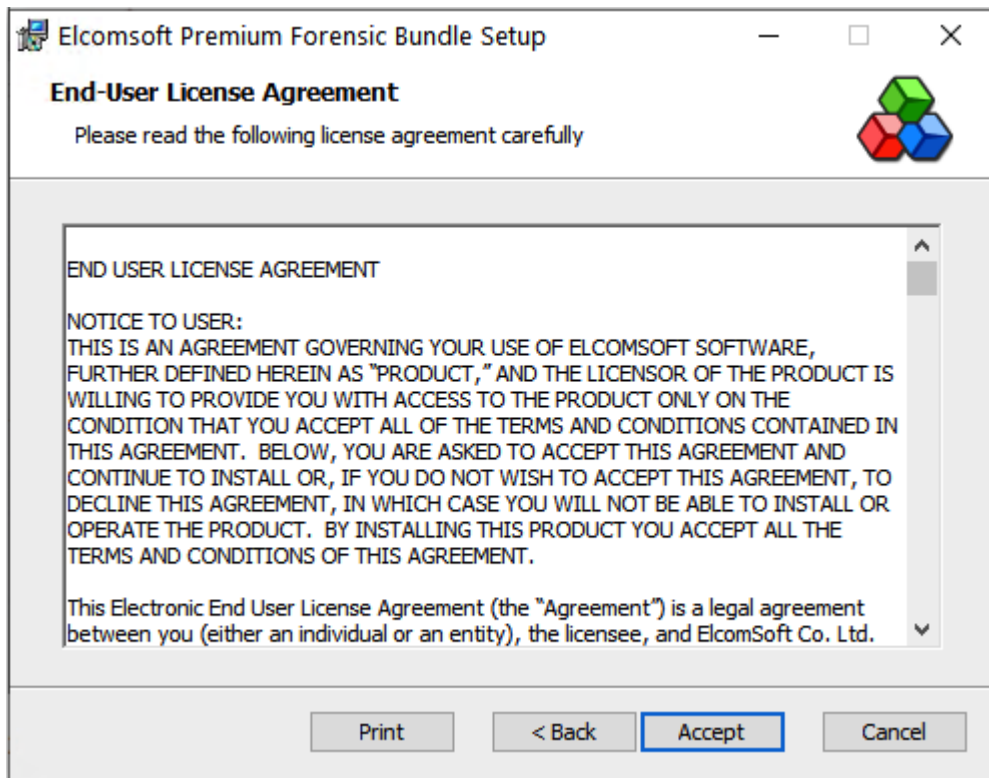
- Компьютер, работающий под операционной системой Windows, начиная от версии 8 и старше
- Свободное место на диске для установки определяется в зависимости от выбранного комплекта компонентов. Полный набор компонентов потребует до 3 гигабайт свободного дискового пространства на жестком диске.

Процесс установки:

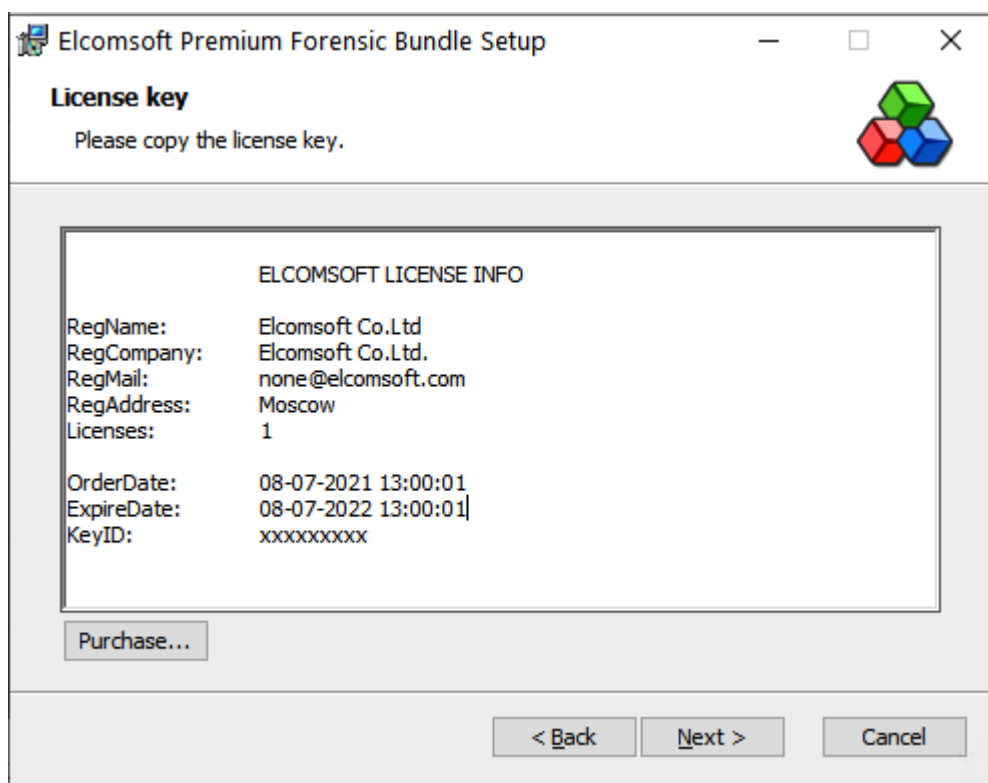
1. Запустите инсталлятор *eprfp_setup_en.msi*



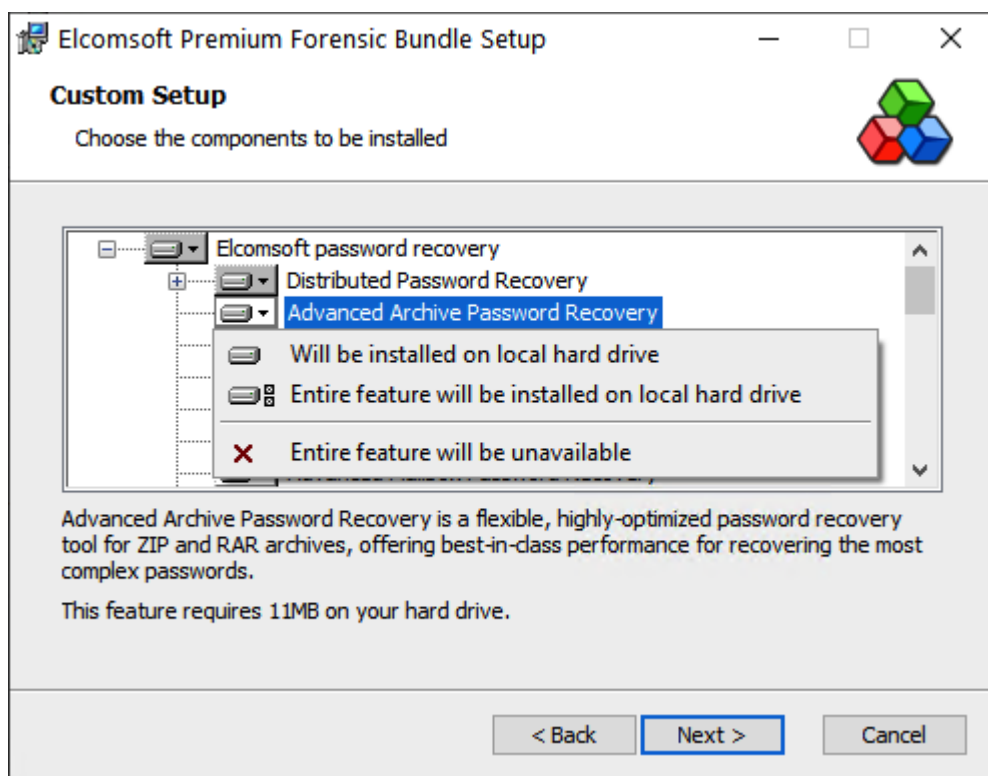
2. Примите условия лицензионного соглашения



3. Скопируйте в буфер обмена **длинный ключ регистрации** и вставьте его в окно с требованием указать ваш лицензионный ключ. Если все было сделано правильно, то вам отобразятся данные по вашей регистрации, как это показано на скриншоте ниже



4. Выберите необходимые для установки компоненты

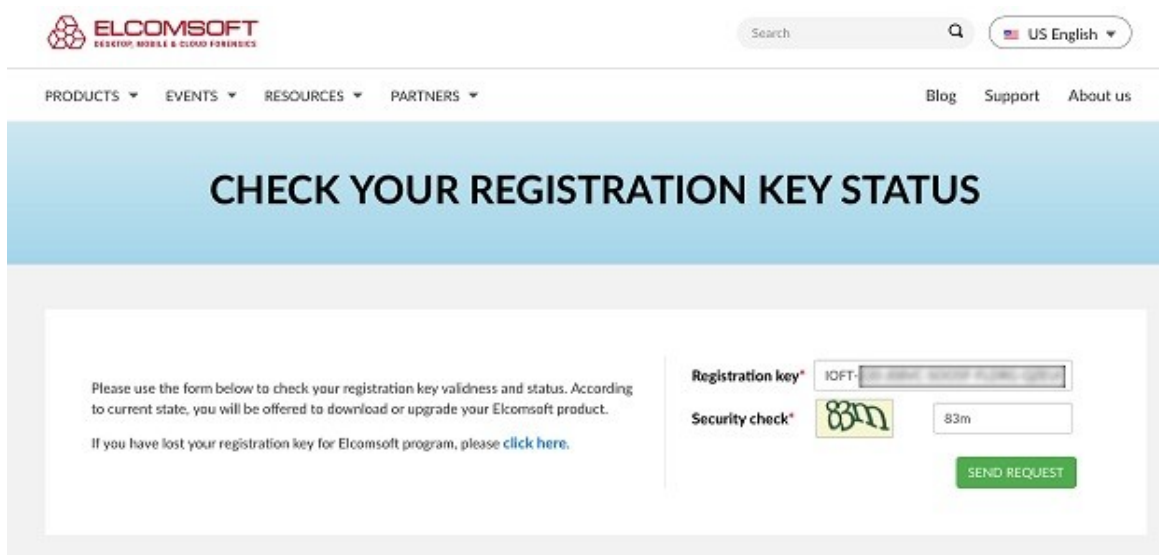


5. Завершите процесс инсталляции выбранных компонентов.

Установка iOS Forensic Toolkit.

Шаг 1: проверка регистрационного ключа онлайн

Пройдите быструю проверку статуса регистрации на [нашем сайте](#), указав Ваш регистрационный ключ программы и правильный код проверки безопасности, затем нажмите «Send request / Отправить запрос» и дождитесь результата.



ELCOMSOFT
DESKTOP, MOBILE & CLOUD FORENSICS

Search [] [] US English []

PRODUCTS [] EVENTS [] RESOURCES [] PARTNERS [] Blog Support About us

CHECK YOUR REGISTRATION KEY STATUS

Please use the form below to check your registration key validness and status. According to current state, you will be offered to download or upgrade your Elcomsoft product.

If you have lost your registration key for Elcomsoft program, please [click here](#).

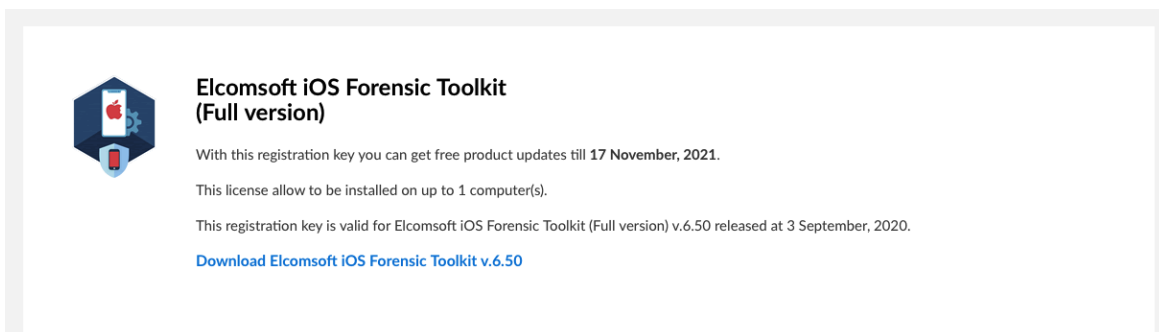
Registration key* IOFT- []


Security check* [] 83m

SEND REQUEST

Шаг 2: проверьте дату истечения срока действия лицензии

Когда появится новое сообщение с подробностями о Вашей лицензии, проверьте дату истечения срока её действия. Также Вам будет предложена ссылка для загрузки последней доступной версии продукта. Кликните по ссылке, чтобы обновить инструментарий.



 **Elcomsoft iOS Forensic Toolkit (Full version)**

With this registration key you can get free product updates till 17 November, 2021.

This license allow to be installed on up to 1 computer(s).

This registration key is valid for Elcomsoft iOS Forensic Toolkit (Full version) v.6.50 released at 3 September, 2020.

[Download Elcomsoft iOS Forensic Toolkit v.6.50](#)

Шаг 3: скачайте и установите последнюю версию Elcomsoft iOS Forensic Toolkit

Выберите необходимую версию продукта, для Windows или macOS, и кликните по соответствующей ссылке. Скачивание начнется немедленно. Также обратите внимание, что

срок действия обеих ссылок истекает через 1 час. После того, как Вы завершили загрузку, используйте предоставленный пароль, чтобы установить программу.



Download Elcomsoft iOS Forensic Toolkit v.6.50

- [Windows Edition](#)
- [MacOS X Edition](#)

Please note, this link valid for one hour only!

Use the password to unpack the archive file

Часть III

**Основные принципы нахождения
паролей**

3 Основные принципы нахождения паролей

3.1 Основные способы парольной защиты

С криминалистической точки зрения все пароли можно разделить на два типа: "быстрые" и "стойкие". Пароль считается "быстрым", если его можно найти, не прибегая к перебору. Если в исследуемых документах есть быстрые пароли, их необходимо найти в первую очередь и использовать для атаки на остальные защищенные документы.

Пароль считается "стойким", если его невозможно найти мгновенно путем вычислений. В этом случае необходимо использовать различные атаки для его восстановления. Этот процесс может быть очень долгим и восстановление не является гарантированным. Desktop Forensic Bundle использует все возможные способы для ускорения нахождения стойких паролей. Наши программы используют ускорение при помощи современных видеокарт. Также возможно использование мутаций при словарной атаке и парольных масок при прямом переборе. Найденные пароли можно сохранить в виде словаря и использовать для дальнейших атак.

3.2 Восстановление стойких паролей

3.2.1 Прямой перебор (Brute-force)

Прямой перебор проверяет все возможные комбинации паролей в определенном диапазоне. Эта атака обычно занимает очень много времени и должна использоваться после того, как все остальные атаки не дали результата. Эта атака имеет два параметра: длина пароля и набор символов.

Примеры

"a-z, длина 3" будут проверены следующие пароли:

aaa
aab
aac
...
zzz

"0-9, длина 5" будут проверены следующие пароли:

00000
00001
00002
...
99999

3.2.2 Атака по маске

Атака по маске может использоваться, если известны какие-то параметры или известные буквы пароля. Маска содержит постоянные и переменные части. Переменные части могут состоять из символов, групп символов и словарных слов. Переменная часть всегда начинается с символа "?".

Синтаксис

- ?? - символ '?'
- ?c - маленькая латинская буква ('a' - 'z')
- ?C - большая латинская буква ('A' - 'Z')
- ?\$ - один спецсимвол из стандартного набора: !@#%&*()-_+= и пробел
- ?@ - один спецсимвол из расширенного набора: !"#%&'()*+,-./:;<=>?@[\\]^_`{|}~ и пробел
- ?# - любой печатный символ в диапазоне 0x20 - 0x7F
- ?d - одна цифра (0 to 9)
- ?w[dictionary_name.udic] - слово из словаря
- ?d(min-max) - число в диапазоне от min до max
- ?1..9(min-max) - символы из пользовательского набора (1-9) с длиной от min до max

Примеры

testmask

Только постоянная часть маски. Будет протестировано только одно слово:

testmask

test?d

Постоянная часть "test", переменная часть "?d". Будут протестированы следующие пароли:

test0

test1

test2

...

test9

John?d(1-2)

Будут протестированы одна-две цифры после постоянной части "John":

John0

John1

...

John9

John00

John01

...

John99

Eva?d(1970-2010)

Добавляем год рождения после постоянной части "Eva":

Eva1970

Eva1971

Eva1972

...

Eva2010

John?w[last_names.udic]

Содержание словаря last_names.udic:

Smith

Doe

Woo

Эта маска подставляет слова из словаря last_names.udic после постоянной части "John":

JohnSmith

JohnDoe

JohnWoo

3.2.3 Атака по словарю

Словарь представляет собой список слов, которые могут быть использованы в качестве паролей. Словари для разных языков входят в комплект поставки Elcomsoft Desktop Forensic Bundle. Мы рекомендуем в первую очередь использовать короткие словари, например "Top 10000 words". Эта атака не займет много времени, однако пароль найдется с довольно большой вероятностью.

3.2.4 Словарные мутации

Каждый пользователь использует свои правила для формирования паролей. Сложные пароли невозможно запомнить, поэтому какой-то набор правил всегда присутствует. Многие используют в качестве пароля свое имя и год рождения, например "John1979" или "Cindy1990". Также пользователи часто меняют регистр букв, надеясь, что это сделает пароль еще более сложным.

При использовании мутацией каждое словарное слово модифицируется с учетом наиболее частных преобразований, используемых пользователями. У каждой мутации есть три уровня: MIN, AVE, MAX.

Case mutation

Изменяет регистр букв.

Уровень	Описание	Слово	Результат
MIN, AVE, MAX	Все маленькие буквы	password	password
MIN, AVE, MAX	Все большие буквы	password	PASSWORD
MIN, AVE, MAX	Первая буква большая	password	Password
MIN, AVE, MAX	Все большие буквы, кроме первой	password	pASSWORD
AVE, MAX	Первая и последняя буквы большие	password	PassworD
MAX	Каждая буква последовательно становится большой	password	Password, pAssword, paSsword .. passworD

Digit mutation

Добавление цифр в начало и конец пароля.

Уровень	Описание	Слово	Результат
MIN, AVE, MAX	Одна цифра на конце слова, все буквы маленькие	password	password0, password1, password2 .. password9
MIN, AVE, MAX	Одна цифра на конце слова, первая буква большая	password	Password0, Password1, Password2 .. Password9
AVE, MAX	Одна цифра на конце слова, все буквы большие	password	PASSWORD0, PASSWORD1, PASSWORD2 .. PASSWORD9
AVE, MAX	Одна цифра в начале слова, все буквы маленькие	password	0password, 1password, 2password .. 9password
AVE, MAX	Одна цифра в начале слова, первая буква большая	password	0Password, 1Password, 2Password .. 9Password
AVE, MAX	Одна цифра в начале слова, все буквы большие	password	0PASSWORD, 1PASSWORD, 2PASSWORD .. 9PASSWORD
MAX	2 цифры на конце слова, все буквы маленькие	password	password00, password01, password02 .. password99
MAX	2 цифры на конце слова, первая буква большая	password	Password00, Password01, Password02 .. Password99
MAX	2 цифры на конце слова, все буквы большие	password	PASSWORD00, PASSWORD01, PASSWORD02 ... PASSWORD99

Border mutation

Добавление к слову часто используемых фраз.

Уровень	Описание	Слово	Результат
MIN, AVE, MAX	Фраза на конце слова, все буквы маленькие	password	password123, passwordxxx, passwordqwer, password000..
MIN, AVE, MAX	Фраза в начале слова, все буквы маленькие	password	123password, xxxpassword, abcpassword, 000password..
AVE, MAX	Символы как префикс и суффикс, все буквы маленькие	password	#password#, -password-, *password* ..

AVE, MAX	Фраза на конце слова, первая буква большая	password	Password123, Passwordxxx, Passwordqwer, Password000..
AVE, MAX	Фраза в начале слова, первая буква большая	password	123Password, xxxPassword, abcPassword, 000Password..
AVE, MAX	Символы как префикс и суффикс, первая буква большая	password	#Password#, -Password-, *Password* ..
MAX	Фраза на конце слова, все буквы большие	password	PASSWORD123, PASSWORDxxx, PASSWORDqwer ...
MAX	Фраза в начале слова, все буквы большие	password	123PASSWORD, xxxPASSWORD, abcPASSWORD ...
MAX	Символы как префикс и суффикс, все буквы большие	password	#PASSWORD#, - PASSWORD-, *PASSWORD* ...

Freak mutation

Изменение символов на похожие ("хакерский жаргон")

Уровень	Описание	Слово	Результат
MIN, AVE, MAX	Все буквы меняются, если есть аналог	password	p@\$w0rd
MIN, AVE, MAX	Меняется только одна буква	password	p@ssword, pa\$sw0rd .. passw0rd
AVE, MAX	Меняются все буквы, кроме одной	password	pa\$\$w0rd, p@s\$w0rd, p@\$sw0rd ..
MAX	Все возможные изменения, первая буква большая	password	P@\$w0rd, p@\$W0rd, p@\$w0rD ..

Abbreviation mutation

Сокращение слов с использованием фонетически похожих цифр.

Уровень	Описание	Слово	Результат
MIN, AVE, MAX	Сокращается одно слово, все буквы маленькие	ihateyou	ih8you, ihateu
MIN, AVE, MAX	Сокращаются все слова, все буквы маленькие	ihateyou	ih8u
AVE, MAX	Сокращается одно слово, первая буква большая	ihateyou	lh8you, lhateu

AVE, MAX	Сокращаются все слова, первая буква большая	ihateyou	Ih8u
MAX	Сокращается одно слово, все буквы большие	ihateyou	IH8YOU, IHATEU
MAX	Сокращаются все слова, все буквы большие	ihateyou	IH8U

Order mutation

Изменение порядка букв в слове, повторение слов.

Уровень	Описание	Слово	Результат
MIN, AVE, MAX	Обратный порядок букв, все буквы маленькие	password	drowssap
MIN, AVE, MAX	Дубликат слова, все буквы маленькие	password	passwordpassword
MIN, AVE, MAX	Дубликат слова с обратным порядком букв, все буквы маленькие	password	passworddrowssap
MIN, AVE, MAX	Тройное повторение слова, все буквы маленькие	password	passwordpasswordpassword
AVE, MAX	Обратный порядок букв, первая буква большая	password	Drowssap
AVE, MAX	Дубликат слова, первая буква большая	password	PasswordPassword
AVE, MAX	Дубликат слова с обратным порядком букв, первая буква большая	password	PasswordDrowssap
AVE, MAX	Тройное повторение слова, первая буква большая	password	PasswordPasswordPassword
MAX	Обратный порядок букв, все буквы большие	password	DROWSSAP
MAX	Дубликат слова, все буквы большие	password	PASSWORDPASSWORD
MAX	Дубликат слова с обратным порядком букв, все буквы большие	password	PASSWORDDROWSSAP
MAX	Тройное повторение слова, все буквы большие	password	PASSWORDPASSWORDPASSWORD

Vowel mutation

Изменение гласных и согласных букв

Уровень	Описание	Слово	Результат
MIN, AVE, MAX	Удаление всех гласных	password	psswrđ

MIN, AVE, MAX	Все согласные большие	password	PaSSWoRD
MIN, AVE, MAX	Все гласные большие	password	pAsswOrd
AVE, MAX	Удаление всех гласных, первая буква большая	password	Psswrđ
MAX	Удаление всех гласных, все буквы большие	password	PSSWRD

Strip mutation

Удаление некоторых символов

Уровень	Описание	Слово	Результат
MIN, AVE, MAX	Удаление одной буквы	password	assword, pssword, pasword ..
AVE, MAX	Удаление одной буквы, первая буква большая	password	assword, Pssword, Password ..
MAX	Удаление одной буквы, все буквы большие	password	ASSWORD, PSSWORD, PASSWORD ..

Swap mutation

Перестановка букв

Уровень	Описание	Слово	Результат
MIN, AVE, MAX	Изменение порядка двух букв, все буквы маленькие	password	apssword, psasword, password ..
AVE, MAX	Изменение порядка двух букв, первая буква большая	password	Apssword, Psasword, Password ..
MAX	Изменение порядка двух букв, все буквы большие	password	APSSWORD, PSASWORD, PASSWORD ..

Duplication mutation

Повторение букв

Уровень	Описание	Слово	Результат
MIN, AVE, MAX	Повторение одной буквы, все буквы маленькие	password	ppassword, paassword, passsword, passwword ..
MIN, AVE, MAX	Повторение последней буквы много раз, все буквы маленькие	password	passwordd, passworddd, passworddd .. passwordddddddd
AVE, MAX	Повторение одной буквы, все буквы маленькие	password	Ppassword, Paassword, Passsword, Passwword ..

MAX	Повторение одной буквы, все буквы большие	password	PPASSWORD, PAASSWORD, PASSSSWORD, PASSWWORD ..
MAX	Повторение первой буквы много раз, все буквы маленькие	password	ppassword, pppassword, ppppassword .. pppppppppassword

Delimiter mutation

Разделение букв специальными символами

Уровень	Описание	Слово	Результат
MIN, AVE, MAX	Вставка символов между буквами, все буквы маленькие	password	p.a.s.s.w.o.r.d, p+a+s+s+w+o+r+d, p*a*s*s*w*o*r*d ..
AVE, MAX	Вставка символов между буквами, первая буква большая	password	P.a.s.s.w.o.r.d, P+a+s+s+w+o+r+d, P*a*s*s*w*o*r*d ..
MAX	Вставка символов между буквами, все буквы большие	password	P.A.S.S.W.O.R.D, P+A+S+S+W+O+R+D, P*A*S*S*W*O*R*D ..

Year mutation

Добавление года в качестве суффикса

Уровень	Описание	Слово	Результат
MIN, AVE, MAX	Год используется как суффикс, все буквы маленькие	password	password1990, password1991 .. password 2020
AVE, MAX	Год используется как суффикс, первая буква большая	password	Password1970, Password1971 .. Password 2020
MAX	Год используется как суффикс, все буквы большие	password	PASSWORD1900, PASSWORD1901 .. PASSWORD 2050

Shift mutation

Сдвиг букв в слове

Уровень	Описание	Слово	Результат
MIN, AVE, MAX	Сдвиг всех букв, все буквы маленькие	password	asswordp, dpasswor
AVE, MAX	Сдвиг всех букв, первая буква большая	password	Asswordp, Dpasswor

AVE, MAX	Сдвиг всех букв, изначально первая буква большая	password	asswordP, dPasswor
MAX	Сдвиг всех букв, все буквы большие	password	ASSWORDP, DPASSWOR

Substitution mutation

Замена букв

Level	Description	Word	Result
MIN, AVE, MAX	Замена буквы на другую, все буквы маленькие	password	oassword, [assword, lassword ..
AVE, MAX	Замена буквы на другую, первая буква большая	password	Oassword, {assword, Lassword ..
MAX	Замена буквы на другую, все буквы большие	password	OASSWORD, {ASSWORD, LASSWORD ..

Length mutation

Ограничение слова по длине

Level	Description	Word	Result
MIN, AVE, MAX	Ограничение справа, все буквы маленькие	password	passwor, passwo, passw ..
MIN, AVE, MAX	Ограничение слева, все буквы маленькие	password	assword, ssword, sword ..
AVE, MAX	Ограничение справа, первая буква большая	password	Passwor, Passwo, Passw ..
AVE, MAX	Ограничение слева, первая буква большая	password	Assword, Ssword, Sword ..
MAX	Ограничение справа, все буквы большие	password	PASSWORD, PASSWO, PASSW ..
MAX	Ограничение слева, все буквы большие	password	ASSWORD, SSWORD, SWORD ..

3.2.5 Гибридная атака с правилами

Гибридная атака является самой мощной среди всего списка атак. Она позволяет строить сложные правила мутации словарных слов. Она может быть использована, когда возможностей предопределенных словарных мутаций недостаточно для поиска пароля. Вы можете построить свои правила для гибридной атаки на основе анализа уже найденных паролей пользователя. Синтаксис правил совместим с популярной программой John the Ripper. Мы также подготовили несколько предопределенных файлов с правилами.

Установка количества букв

В гибридной атаке количество символов устанавливается одной буквой. Числа от 0 до 9 представлены в исходном виде, дальше идут буквы от A до Z. Максимальное количество букв равняется 35 и представлено буквой Z.

Синтаксис правил гибридной атаки

Самое простое правило

: Ничего не делать, использовать слово "как есть"

Изменение регистра букв

- c** Первая буква большая: password -> Password
- C** Первая буква маленькая, остальные большие: password -> pASSWORD
- l** Все буквы маленькие
- u** Все буквы большие
- t** Изменить регистр всех букв: PassWord -> pASSwORD
- aN** Все возможные комбинации больших и маленьких букв. N - максимальная длина слова, к которому будет применено правило.
Это правило не может быть использовано совместно с другими!
- V** Elite мутация гласных: password -> PaSSWoRD
- v** Noelite мутация гласных: password -> pASSWoRD
- TN** Изменить регистр буквы на позиции N.

Циклический сдвиг, удаление, отражение

- {** Циклический сдвиг влево: password -> asswordp
- }** Циклический сдвиг вправо: password -> dpassword
- [** Удалить первую букву: password -> assword
-]** Удалить последнюю букву: password -> password
- DN** Удалить букву на позиции N
- 'N** Обрезать слово до длины N
- f** Отражение: password -> passworddrowssap
- r** Реверс: password -> drowssap

Повторение

- d** Повторение слова: password -> passwordpassword
- q** Повторение символов: password -> ppaasssswwoorrrd
- zN** Повторение первой буквы слова N раз. N = 1 .. 9
- ZN** Повторение последней буквы слова N раз. N = 1 .. 9

Не проверять слово

- <N** Не проверять слово, если его длина больше N.
- >N** Не проверять слово, если его длина меньше N.
- !X** Не проверять слово, если оно содержит символ X
- /X** Не проверять слово, если оно не содержит символ X
- (X** Не проверять слово, если первый символ не X
-)X** Не проверять слово, если последний символ не X
- %MX** Не проверять слово, если оно не содержит символ X как минимум M раз
- =NX** Не проверять слово, если на позиции N не содержится символ X

Вставка, удаление, копирование

- pN** Копировать слово N раз. N = 3 .. 9
- \$X** Добавить символ X в конец слова

- ^X** Добавить символ X в начало слова
- @X** Убрать все символы X из слова
- iNX** Вставить символ X на позицию N
- oNX** Заменить символ на позиции N на символ X
- sXY** Заменить все символы X на Y

Операции с частями строк

- xNM** Извлечь часть строки с позиции N, максимально M символов
- eX** Извлечь часть строки с начала слова до нахождения символа X. Если символ X не найден, слово остается в неизменном виде
- EX** Извлечь часть строки после первого появления символа X.

Другое

- SLN** Побитовый сдвиг влево символа на позиции N
- SRN** Побитовый сдвиг вправо символа на позиции N

Примеры

:c
Password

:
c
password
Password

:soaswv
csoaswv
passvard
Passvard

Часть IV

Программы для восстановления
паролей

4 Программы для восстановления паролей

4.1 Advanced Archive Password Recovery

4.1.1 Введение

Advanced Archive Password Recovery (ARCHPR) восстанавливает пароли и разблокирует зашифрованные архивы, созданные с помощью популярных инструментов сжатия файлов. Гарантированная разблокировка архивов, созданных с помощью WinZip 8.0 и ранее, менее чем за час возможна при использовании недостатка реализации защиты.

ARCHPR обеспечивает максимальную совместимость между различными типами архивов, знает слабые стороны определенных типов защиты и обеспечивает лучшую в своем классе производительность при разблокировке всех типов архивов.

Характеристики и преимущества

- Поддерживает все версии ZIP/PKZip/WinZip, RAR/WinRAR, 7ZIP, а также ARJ/WinARJ и ACE/WinACE (1.x)
- Гарантированное восстановление архивов менее чем за час для ZIP-архивов, созданных с помощью WinZip 8.0 и ранее и содержащих не менее 5 файлов
- Поддерживает архивы размером более 4 ГБ и самораспаковывающиеся архивы
- Поддерживает надежное шифрование AES, которое есть в WinRAR и новых версиях WinZip
- Использует все известные уязвимости и недостатки реализации в различных алгоритмах сжатия для более быстрого восстановления
- Быстрая атака с использованием известного открытого текста восстанавливает определенные архивы ZIP и ARJ за считанные минуты (пользователь должен предоставить хотя бы один незащищенный файл из этого архива)
- Прерывание и возобновление работы в любое время
- Поддерживает фоновую работу за счет использования простоя ЦП
- Атаки по словарю и полным перебором с использованием пользовательских масок и расширенных шаблонов
- Высокооптимизированный низкоуровневый код для оптимальной производительности

Примечание: пароль нигде не хранится в архиве (файлы ZIP / RAR / ARJ / ACE), поэтому его нельзя извлечь или расшифровать. Вместо этого ARCHPR может восстановить его, попробовав все возможные комбинации из заданного диапазона или словаря. Хотя нет гарантии, что пароль будет восстановлен, человеческий фактор играет свою роль, поскольку короткие и/или легко запоминающиеся пароли являются наиболее распространенными.

Программа, на которую вам предоставлена лицензия, является абсолютно законной, и вы можете использовать ее при условии, что вы являетесь законным владельцем всех файлов или данных, которые вы собираетесь восстановить с помощью нашего программного обеспечения, или имеете разрешение законного владельца на выполнение этих действий. Вы несете исключительную ответственность за любое незаконное использование программы. Соответственно, вы подтверждаете, что имеете законное право на доступ ко всем данным, информации и файлам, которые были недоступны.

Вы также подтверждаете, что восстановленные данные, пароли и / или файлы не будут использоваться в каких-либо незаконных целях. Помните, что восстановление пароля и последующее дешифрование данных неавторизованных или иным образом незаконно

полученных файлов может представлять собой кражу или другое противоправное действие и может привести к вашему гражданскому и (или) уголовному преследованию.

4.1.2 Требования

- Windows 7 - Windows 10
- Около 34 МБ ОЗУ для атаки с использованием известного открытого текста ZIP
- Около 260 МБ ОЗУ для обработки архивов RAR 2.9 и 3.x

4.1.3 Как работать с программой

4.1.3.1 Выбор параметров

Открытие архива

Чтобы открыть архив, защищенный паролем, используйте кнопку «Обзор» (или клавишу F3) для выбора или нажмите кнопку «Последние файлы» (с помощью маленькой стрелки вниз), чтобы выбрать файлы из списка недавно открытых файлов. Кроме того, вы можете использовать перетаскивание, чтобы перетащить файл из проводника Windows в окно ARCHPR. Атака начнется немедленно.

Тип атаки

Для всех форматов файлов доступны атаки [методом полного перебора](#)^[35], атаки по маске и [словарю](#)^[36], в то время как атака на основе открытых текстов доступна для определенных архивов [ZIP](#)^[36] и [ARJ](#)^[36]. [Атака с гарантированным результатом](#)^[39] доступна для архивов WinZip 8.0 и более младших версий при наличии 5-и (или более) зашифрованных файлов. Специальная атака [Пароль из ключей/Password from keys](#)^[39] может использоваться в дополнение к атакам методом полного перебора и на основе открытых текстов на определенные ZIP-архивы (подробности читайте в последующих главах).

Параметры диапазона перебора

Заданный набор символов. Вы можете выбрать все заглавные буквы, все строчные буквы, все цифры, все специальные символы и пробелы или все печатные символы (включая все вышеперечисленное). Специальные символы:

!@#%&*()_+<=>,./?[]{}~:;`|'\"

В качестве альтернативы вы можете определить свой собственный набор символов («charset»). Установите флажок «User-defined» и нажмите «Custom charset...». В окне ввода введите все символы диапазона пароля. Например, если пароль содержит символы из нижнего ряда клавиатуры («zxсv...»), диапазон вашего пароля может быть «zxсvbnm,./» (или заглавными буквами: «ZXCVBNM <>?»). Вы также можете определить оба из них: «zxсvbnm,./ ZXCVBNM <>?». Кроме того, вы можете загружать и сохранять пользовательские наборы символов или комбинировать их с помощью кнопки «Add charset from file...».

Обратите внимание на параметр «Конвертировать в OEM кодировку» в «Пользовательский набор символов». Обязательно выберите этот параметр, если пароль содержит какие-либо символы, отличные от английского, и архив был создан с помощью утилиты сжатия на основе DOS, не поддерживающей Unicode (например, PKZIP). В противном случае пароль не будет найден.

Начать с пароля

Эта опция может помочь, если вы знаете первый(е) символ(ы) пароля. Например, если вы уверены, что пароль состоит из маленьких букв (от «а» до «z»), его длина равна 5, а пароль начинается с «k», введите «каааа». Примечание: если вы нажмете «Стоп» во время работы ARCHPR, программа сохранит текущий пароль в главном окне («Начать с»). Вы сможете перезапустить атаку без потери прогресса.

Обратите внимание, что программа проверяет пароли в следующем порядке:

- ЗАГЛАВНЫЕ буквы: 'A'..'Z'
- пробел
- строчные буквы: 'a'..'z')
- цифры: '0'..'9'
- специальные символы: !@#\$%^&*()_+ -= <> , / ? [] { } ~ ; : ' | " \

Вы также можете использовать поле «Закончить на», чтобы установить пароль, на котором ARCHPR должен остановиться. Это может быть полезно, если вы используете несколько компьютеров для атаки одного и того же архива.

Маска пароля

Если вы уже знаете некоторые символы пароля, вы можете указать маску, чтобы уменьшить общее количество проверяемых паролей. Маски доступны только для паролей фиксированной длины.

Пример: если пароль состоит из 8 символов, начинается с «x», заканчивается на «99», а остальные символы - строчные или заглавные буквы, то маска будет «x?????99». Набор символов - Все заглавные и Все строчные.

Если вы знаете, что в пароле встречается символ маски «?», Вы можете выбрать другой символ маски. В этом случае вы можете изменить символ маски с '?' на '#' или '*' и используйте шаблон маски «x#####?» (для символа маски '#') или «x*****?» (для символа маски '*'). Выберите символ маски в [дополнительных параметрах](#)^[41].

Длина пароля

Это один из самых важных параметров, влияющих на продолжительность атак.

Если минимальная и максимальная длина различаются, программа сначала проверяет более короткие пароли. Например, если вы установите минимум 3 и максимум 7, программа будет начинать с паролей из 3 символов, затем пробовать пароли из 4 символов и так далее. Во время работы ARCHPR показывает текущую длину пароля, а также текущий пароль, среднюю скорость, прошедшее и оставшееся время, а также общее и обработанное количество паролей ([статус программы](#)^[42]). Вся эта информация, за исключением средней скорости и прошедшего времени, связана только с текущей длиной пароля.

Параметры словаря

Укажите нужный файл словаря. Кроме того, вы можете выбрать параметры «Умные мутации» или «Попробовать все возможные комбинации заглавных/маленьких букв», что может помочь, если вы не уверены в регистре, в котором был введен пароль. Например, предположим, что следующее слово в словаре - «PASSword». При включенной второй опции программа просто попробует все возможные комбинации регистров, например:

password
 passworD
 passwoRd
 passwoRD
 passwOrd
 ...
 PASSWORDd
 PASSWORD

Однако проверка всех этих комбинаций занимает много времени: в приведенном выше примере ARCHPR будет проверять $2^8 = 256$ слов вместо одного. Умные мутации позволяют исключить ряд маловероятных комбинаций, таким образом проверяться будут следующие слова:

PASSword	(как есть)
passWORD	(в обратном порядке)
password	(все в нижнем регистре)
PASSWORD	(все в верхнем регистре)
Password	(первая заглавная, остальные строчные)
pASSWORD	(первая строчная, остальные заглавные)
PaSSWoRD	(элитный: гласные строчные, согласные заглавные)
pAsswOrd	(неэлитный)
PaSsWoRd	(alt/1)
pAsSwOrD	(alt/2)

Таким образом, умные мутации будут проверять только 10 комбинаций для каждого слова.

Параметр "Стартовая строка #" позволяет начать атаку с заданной строки в словаре; если вы прервете атаку, текущий номер строки будет сохранен.

Параметр «Преобразовать в OEM-кодировку/Convert to OEM encoding» можно использовать, если словарь имеет кодировку ANSI, но ZIP-архив был создан с помощью архиватора DOS (например, PKZIP), поэтому фактический пароль находится в OEM-кодировке. Изменение этого параметра не имеет никакого значения, если все слова в словаре содержат только латинские буквы.

Небольшой, но эффективный словарь поставляется с ARCHPR: english.dic (около 240 000 слов).

Plaintext атака (ZIP)

Атака с использованием известного открытого текста позволяет дешифровать определенные типы зашифрованных архивов ZIP без проведения длительной атаки на исходный пароль. Данная атака применима только к архивам ZIP, зашифрованным с помощью устаревшего шифрования. **ZIP-архивы, зашифрованные с помощью AES-256, не уязвимы для этой атаки.**

Чтобы выполнить атаку с использованием известного открытого текста, необходимо:

- Найти незашифрованный файл, который также существует в архиве, защищенном паролем.
- Сжать его тем же методом и тем же архиватором ZIP, который используется в зашифрованном архиве. Это необходимо, потому что ARCHPR проверяет размеры файлов и контрольные суммы файлов. Однако вы можете использовать атаку с открытым текстом на частичном файле; см. описание ниже.
- Запустите ARCHPR, выберите зашифрованный архив, затем выберите атаку с открытым текстом /plaintext и найдите архив, содержащий незашифрованный файл.

После этого ARCHPR проверит файлы. Если совпадение будет найдено, начнется атака.

ARCHPR может найти или не найти исходный пароль. Если исходный пароль восстановить невозможно, инструмент отобразит только ключи шифрования. В любом случае вы можете использовать эти ключи шифрования для расшифровки ZIP-архива.

Частичный файл

Иногда у вас может быть версия файла с открытым текстом, отличная от версии в зашифрованном архиве. Если вы считаете, что начало простого текстового файла идентично началу зашифрованного, вы можете выполнить так называемую атаку «частичного открытого текста», основанную на первых N символах файла с открытым текстом. Для этого убедитесь, что в архиве, защищенном паролем, хранится только один файл, и только один файл есть архиве с открытым тестом. Запустите атаку, и ARCHPR попросит подтвердить «частичную» атаку. Нажмите «Да» и выберите количество байтов для использования в виде открытого текста. Рекомендуется начать с 1–3 КБ и уменьшить это число, если ARCHPR не может найти ключи шифрования.

Примечания к текущей версии

1. Файл с открытым текстом должен иметь длину не менее 12 байт.
2. Атака на основе открытого текста может быть сохранена только на втором этапе; после перезапуска снова будет выполнен первый этап.
3. Нет оценки времени прохождения первого этапа; однако он не должен длиться дольше нескольких минут.

Plaintext атака (ARJ)

Файлы ARJ имеют относительно надежное шифрование, однако одним из способов взлома защиты ARJ является использование атаки на основе известного открытого текста. Эта атака мгновенная.

Если у вас есть доступ к зашифрованному файлу, созданному архиватором ARJ, и к тому же файлу в незашифрованном виде, вы можете получить исходный пароль. Для проведения атаки

с открытым текстом вам понадобится хотя бы один файл из зашифрованного архива, сжатый, но незашифрованный.

Чтобы выполнить атаку с открытым текстом, надо:

- Найти незашифрованный файл, который также есть в защищенном паролем архиве.
- Сжать его тем же методом, что и в зашифрованном архиве.
- Запустить ARCHPR, выбрать зашифрованный архив, затем выбрать атаку «открытым текстом/plaintext» и найти архив с незашифрованным файлом.

После этого ARCHPR проверит файлы, и если совпадение будет найдено, пароль отобразится мгновенно.

Гарантированная атака WinZip

Эта атака аналогична [атаке с использованием известного открытого текста](#)^[38], но не требует наличия каких-либо файлов из архива. Однако в самом архиве должно быть не менее 5 зашифрованных файлов. Эта атака использует уязвимость, которая существовала в устаревших версиях [WinZip 8.0](#) и ранее или в любом другом архиваторе ZIP, основанном на текущих на тот момент исходниках Info-ZIP.

Обратите внимание, что только WinZip версии 8.0 и более ранних уязвимы для этой атаки из-за использования слабого генератора случайных чисел. В версии 8.1, выпущенной в августе 2001 года, уязвимость была исправлена, и эта атака больше не применима.

Чтобы использовать атаку, выберите архив, затем щелкните «Гарантированная расшифровка WinZip» в раскрывающемся списке «Тип атаки» и нажмите «Старт»; никаких других настроек не требуется. Если архив был создан с помощью другого архиватора или содержит менее 5 файлов, ARCHPR покажет сообщение об ошибке.

Эта атака может сломать около 99,6% поддерживаемых ZIP-архивов, созданных с помощью уязвимой версии WinZip. В одном из 256 случаев (вероятность 0,4%) атака не удастся, даже если архив был создан с помощью уязвимой версии WinZip. ARCHPR может заранее идентифицировать такие архивы и предупреждать сообщением в окне журнала. Но вы все равно можете попробовать использовать атаку, так как идентификация не на 100% верная. Однако, если первый этап атаки завершится без найденных ключей шифрования, вам придется попытаться прибегнуть к другим атакам.

Пароль из ключей

Как отмечалось выше, [атака с использованием известного открытого текста](#)^[38] и [гарантированная WinZip атака](#)^[39] сначала пытаются восстановить ключи шифрования. Как только они появятся, архив можно будет расшифровать, поэтому пароль не требуется. Однако эти атаки также пытаются искать пароли длиной до 10 символов.

Если у вас уже есть ключи шифрования и вы хотите восстановить более длинный пароль, выберите эту атаку в поле "Тип атаки". Введите ключи на вкладке «Plaintext» и установите другие параметры, такие как набор символов (вкладка «Набор/Range») и длину пароля, как если бы вы настраивали атаку методом полного перебора. Рекомендуемая минимальная длина пароля составляет 11 символов (т.к. ARCHPR уже пробовал использовать более короткие пароли ранее), практическая максимальная длина составляет от 15 до 16 символов, в зависимости от набора символов.

Есть некоторые рекомендации относительно параметра "Начать с". Нет необходимости восстанавливать первые 6 символов пароля, поскольку они рассчитываются на основе «хвоста» пароля (седьмой символ и дальше). Таким образом, исходный пароль должен начинаться с 6 звездочек, а значимые позиции - с 7-го символа. Программа начинает поиск правильных комбинаций с конца; например, для 11-значных паролей, содержащих строчные буквы, порядок следующий:

```
*****aaaaa
*****baaaa
...
*****zaaaa
*****zbaaa
....
*****zzaaa
...
*****zzzzz
```

Учтите это при выборе стартового пароля вручную.

Автосохранение

ARCHPR может периодически сохранять свое состояние. Чтобы настроить автоматическое сохранение, отметьте соответствующий параметр и выберите время (в минутах) между сохранениями. Файл восстановления с именем «~archpr.axr» будет создан в той же папке, где находится архив. Вы можете установить другое местоположение и/или имя файла. Файл позволяет возобновить атаку с последнего сохраненного состояния. Этот вариант настоятельно рекомендуется.

Другие настройки

Приоритет: фоновый или высокий

Параметр «Фоновый» позволяет инструменту использовать только неиспользуемые циклы ЦП. Параметр «Высокий» увеличивает приоритет процесса за счет всех других приложений на компьютере.

Свернуть в трей:

Если эта опция включена, окно программы будет свернуто в системный трей.

Вести запись в archpr.log:

Если этот параметр включен, программа сохраняет всю информацию, отображаемую в окне состояния, в файл журнала (archpr.log).

Начать атаку при выборе файла:

Когда этот параметр включен (по умолчанию), программа анализирует файл сразу после его открытия.

Интервал обновления индикатора выполнения:

Интервал в миллисекундах между обновлениями индикатора выполнения и окна состояния; по умолчанию 500.

Язык:

Переключает язык интерфейса. Английский язык интерфейса по умолчанию.

Продвинутые настройки

Использовать известное начало файла для хранимых архивов (шестнадцатеричное):

Если ваш архив содержит один зашифрованный файл, и этот же файл хранится в несжатом виде, использование этой опции помогает сократить время восстановления пароля. Вы должны знать от 1 до 4 байтов в начале файла. Существует множество хорошо известных подписей, например, MZ (шестнадцатеричный: 4D 5A) для исполняемых файлов, PK (шестнадцатеричный: 50 4B 03 04) для файлов ZIP, D0 CF 11 E0 (шестнадцатеричный) для составных документов OLE (например, файлы MS Word/Excel) и т.д.

Всегда использовать оптимизированный движок атаки WinZIP, если вероятность превышает XX% :

Если архив был создан в WinZIP (или другом инструменте ZIP под Windows, основанном на тех же исходниках) и содержит не менее пяти зашифрованных файлов, скорость атаки методом перебора может быть оптимизирована в три раза. ARCHPR попытается автоматически обнаруживать такие файлы с помощью эвристики. Программа рассчитывает значение вероятности, которое основано на количестве файлов в архиве и других факторах. Если оно будет больше 50%, ARCHPR предложит использовать оптимизированную атаку при запуске процесса восстановления. Вы можете включить эту настройку, чтобы оптимизированный движок использовался или не использовался автоматически. 85% - рекомендуемое значение для этой настройки.

Символ маски:

Используется для атаки по [маске](#).^[36]

Использовать код, оптимизированный для:

(Не MMX процессоры / Intel PII/PIII/Celeron / AMD Athlon / Intel P4 SSE2 / Intel Core/Core2): отменяют автоматическое определение ЦП и заставляют ARCHPR использовать код, специально оптимизированный для данных ЦП.

4.1.3.2 Сохранение и чтение настроек

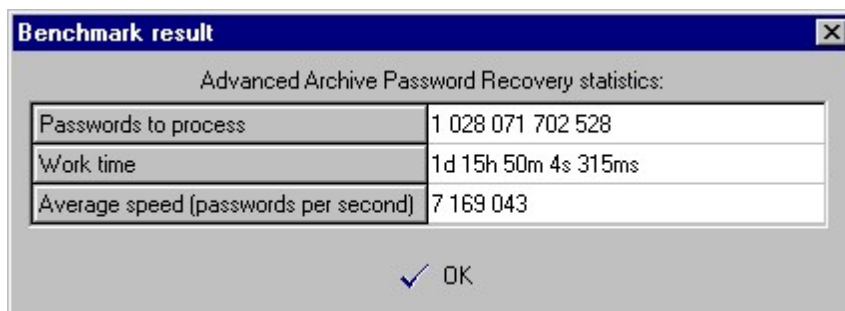
Сохранение и чтение настроек

Вы можете сохранить текущие настройки ARCHPR в файл .AXR. Вы можете восстановить настройки с помощью кнопки «Открыть файл/проект» или перетащив ранее сохраненный файл ахг в окно ARCHPR. Если все настройки верны, атака начнется немедленно.

4.1.3.3 Тест производительности

Тест производительности

Если вы хотите оценить, сколько времени займет атака [методом полного перебора](#)^[35] или [по маске](#)^[36], или протестировать скорость ARCHPR на конкретном архиве, используйте функцию тестирования производительности. Выберите параметры, затем нажмите кнопку "Тест" (рядом с кнопкой "Стоп"). Программа проработает около 10 секунд, а потом покажет некоторую статистику:



4.1.3.4 Получение результатов

Процесс восстановления

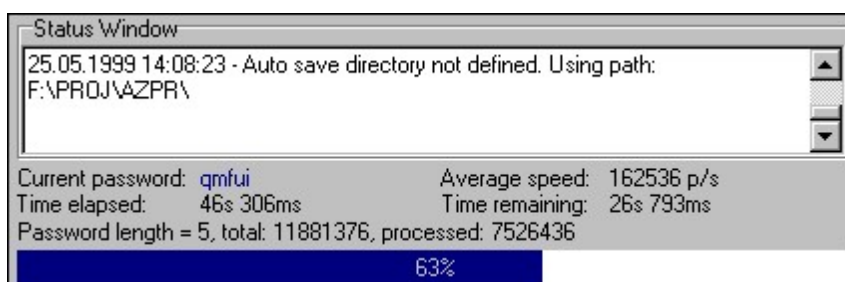
Нажмите "Старт" или F9, чтобы начать атаку. Будет отображен [статус программы](#)^[42].

Вы можете остановить и возобновить атаки. Дополнительные сведения см. в разделах «[Начать с пароля](#)^[36]» и «[Сохранение и чтение настроек](#)^[41]».

Во время «[атаки по известному открытому тексту](#)^[38]» вы можете остановить процесс в любой момент, но возобновление возможно только на втором этапе («поиск ключей»). Возобновление атак с использованием известного открытого текста доступно только в зарегистрированной версии.

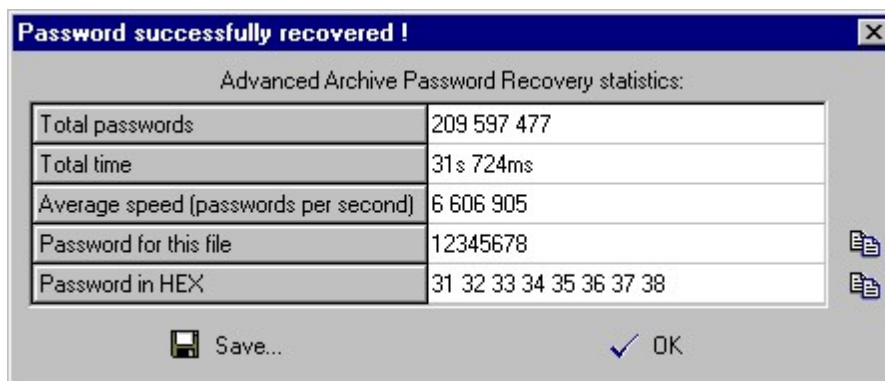
Статус программы

Во время атаки отображается текущий пароль (current password), средняя скорость (average speed), прошедшее время (elapsed time), оставшееся время (remaining time), общее количество паролей заданной длины (total) и количество уже обработанных паролей (processed):



Результаты

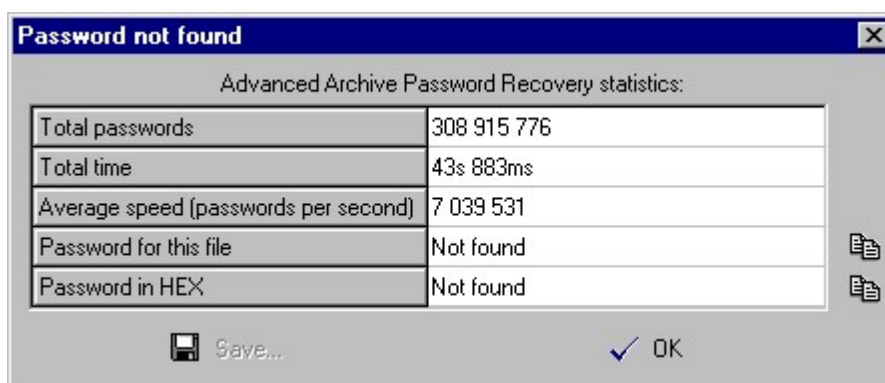
После атаки результат отображается в следующем окне:



В последней строке отображается пароль в шестнадцатеричной форме (HEX), что может быть полезно, если пароль содержит непечатаемые символы.

Вы можете скопировать пароль в буфер обмена с помощью маленького значка справа от поля. Как вариант, вы можете сохранить пароль в файл.

Если инструмент не может найти пароль, отображается следующее окно:



Если вы остановили восстановление, нажав кнопку «Стоп», текущий шаг перебора сохраняется в поле «Начать с». Нажмите кнопку «Старт», чтобы возобновить атаку.

4.1.4 Известные ошибки и ограничения

4.1.4.1 Известные ошибки и ограничения

- Когда файлы в архиве хранятся в зашифрованном виде, но без сжатия, атаки могут выполняться медленнее, чем ожидалось (особенно для больших файлов), потому что требуется расшифровка всего файла (если вы не знаете первые несколько байтов зашифрованного файла).
- Если архив содержит два или более зашифрованных файла, программа предполагает, что все они зашифрованы с одним и тем же паролем (временное решение см. в разделе [Файлы с разными паролями](#)^[44]).
- Программа не поддерживает ZIP-архивы, в которых используется метод сжатия dclimplode (доступен в библиотеке сжатия данных PKWARE).

- Программа не поддерживает Strong Encryption Specification (EFS), доступное в PKZip 5 и выше.

4.1.5 Советы и рекомендации

4.1.5.1 Файлы с разными паролями

Если файлы внутри ZIP-архива зашифрованы разными паролями, ARCHPR может не найти правильный пароль. Обходной путь: (1) надо сделать резервную копию вашего архива; (2) удалить из архива все файлы, кроме зашифрованных одним и тем же паролем (или оставить один файл); и (3) запустить ARCHPR для полученного архива. Как только ARCHPR найдет правильный пароль, создайте последующие архивы с остальными файлами.

4.1.5.2 С чего начать

Вы можете оценить время атаки, выполнив встроенный тест производительности. Пожалуйста, обратитесь к следующей таблице, чтобы узнать количество возможных комбинаций паролей:

Набор символов	Длина	Пароли
Все печатаемые	1..6	742,912,032,768
Цифры, строчные/заглавные, пробел	7	3,938,980,724,736
Цифры, строчные, пробел	8	3,512,479,514,624
Цифры, заглавные, пробел	8	3,512,479,514,624
Цифры	9..11	1,110,999,957,504
Строчные, пробел	9	7,625,596,993,536
Заглавные, пробел	9	7,625,596,993,536

4.1.5.3 Командная строка

Вы можете запустить ARCHPR с параметрами командной строки. Синтаксис:

ARCHPR [switches] [zip/arj/ace/rar-filename]

или

ARCHPR [switches] [axr-filename]

Переключатели разделяются знаком «/» или «-». Если за переключателем следуют значения (например, имя файла, начальный пароль и т. д.), содержащие специальные символы (пробел, точка с запятой, косая черта или тире), его следует заключить в одинарные или двойные кавычки.

Переключатель	Описание	По умолчанию
---------------	----------	--------------

/a:b m d	тип атаки (перебор, маска, словарь)	полный перебор
/c:csdipa	набор символов (заглавные, маленькие, цифры, специальные, пробел, все)	заглавные
/u:chars	набор символов, определяемый пользователем	
/oem	преобразовать в OEM (для пользовательского набора символов и атаки по словарю)	отключено
/sf:pass	начать с пароля	
/endat:pass	закончить на пароле	
/usewz:X	использовать оптимизированную атаку WinZip	
/useknownstart:XX	использовать известные байты в сохраненном файле (от 1 до 4 шестнадцатеричных значений, без пробелов)	
/p[:filename]	имя файла атаки открытым текстом	
/m:mask	маска	
/ms:C	символ маски	?
/min:N	минимальная длина пароля	1
/max:N	максимальная длина пароля	5
/oem	преобразовать в OEM (для пользовательского набора символов и атаки по словарю)	отключено
/useknownstart:XX	использовать известные байты в сохраненном файле (от 1 до 4 шестнадцатеричных значений, без пробелов)	
/d[:filename]	имя файла словаря	
/sm	умные мутации	отключено
/ac	попробовать все возможные комбинации верхнего / нижнего регистра	отключено
/sl:N	начать с строки N	0
/autosave:N	автосохранение каждые N минут; 0 означает отключено	5
/aname:filename	имя файла автосохранения	
/adir:dir	каталог автосохранения	
/idle	работать в фоновом режиме	включено
/high	работать в режиме высокого приоритета	отключено
/dontstart	не запускать атаку, просто загрузить / установить параметры	
/minimize	свернуть программу после запуска атаки	

/smartexit[:filena me]	по завершении атаки записать всю статистику, включая пароль (если он найден), в указанный файл (по умолчанию «cmdline_stats.txt») и выйти из программы.	отключено
---------------------------	---	-----------

Примеры:

archpr.exe /a:b /c:cs /min:3 /max:7 /smartexit test.zip

(атака полным перебором; строчные и заглавные буквы; длина от 3 до 7; сохранить и выйти по окончании)

archpr.exe /a:b /u:12345abcde test.ace

(атака полным перебором с набором символов "12345abcde"; длина: от 1 до 5)

archpr.exe /a:m /c:d /m:june???? /sf:june1000 /high test.rar

(атака по маске с маской "june????"; набор символов: цифры; высокий приоритет)

archpr.exe /d:english.dic /sm /oem /dontstart test.zip

(словарная атака; словарь: "english.dic"; умные мутации; конвертировать слова из ANSI в OEM; загрузить, но не запускать атаку)

archpr.exe /a:p /p:plain.arj test.arj

(атака с известным открытым текстом)

Если в качестве параметра передается файл ахг, программа немедленно загрузит настройки, игнорируя другие настройки, указанные в командной строке, кроме / dontstart, / minimize и / smartexit, и запустит атаку.

4.1.6 Благодарности

4.1.6.1 Благодарности

Многие люди помогли сделать ARCHPR таким, какой он есть, внося предложения, помогая тестировать, сообщая об ошибках и т.д. В частности, мы хотели бы поблагодарить Ирину Каталову, Александра Каталова-младшего, Дмитрия Склярова, Александра Волока, Марко Д'Амато, Джона Тейлора, Паоло Виаппиани, Даррен Паркера, Ричард Дж. Шерин. Особая благодарность Элу Анвею за исправление документации.

Этот продукт включает криптографическое программное обеспечение, написанное [Эриком Янгом](#).

4.2 Advanced Intuit Password Recovery

4.2.1 Введение

Advanced Intuit Password Recovery (AINPR) - программа для восстановления доступа к защищённым паролями документам, созданным в следующих продуктах:

- Quicken (*.qdt, *.qdb, *.qdf)
- QuickBooks (*.qba, *.qbw).

Поддержка документов и паролей на всех языках и кодировках.

Полный и актуальный список поддерживаемых форматов файлов доступен на [странице продукта](#).

Правовая информация

Программа, на которую Вам предоставлена лицензия, является абсолютно законной, и Вы можете использовать её при условии, что Вы являетесь законным владельцем всех файлов или данных, которые Вы собираетесь восстановить с помощью нашего программного обеспечения, или имеете разрешение законного владельца на выполнение этих действий. Вы несёте исключительную ответственность за любое незаконное использование нашего программного обеспечения. Соответственно, Вы подтверждаете, что имеете законное право на доступ ко всем данным, информации и файлам, которые были скрыты.

Вы также подтверждаете, что восстановленные данные, пароли и/или файлы не будут использоваться в каких-либо незаконных целях. Имейте в виду, что восстановление пароля и последующее дешифрование данных неавторизованных или иным образом незаконно полученных файлов может составлять кражу или другое противоправное действие и может привести к вашему гражданскому и (или) уголовному преследованию.

4.2.2 Program information

4.2.2.1 Системные требования

Системные требования:

- Windows 7, 8, 8.1, Windows 10

4.2.2.2 Работа с AINPR

Откройте файл, для которого хотите восстановить пароль, с помощью кнопки «Открыть файл.../Open file...». Тип файла распознается автоматически.

Для получения подробной информации о [Quicken](#)^[47] и [QuickBooks](#)^[48] прочтите следующие главы.

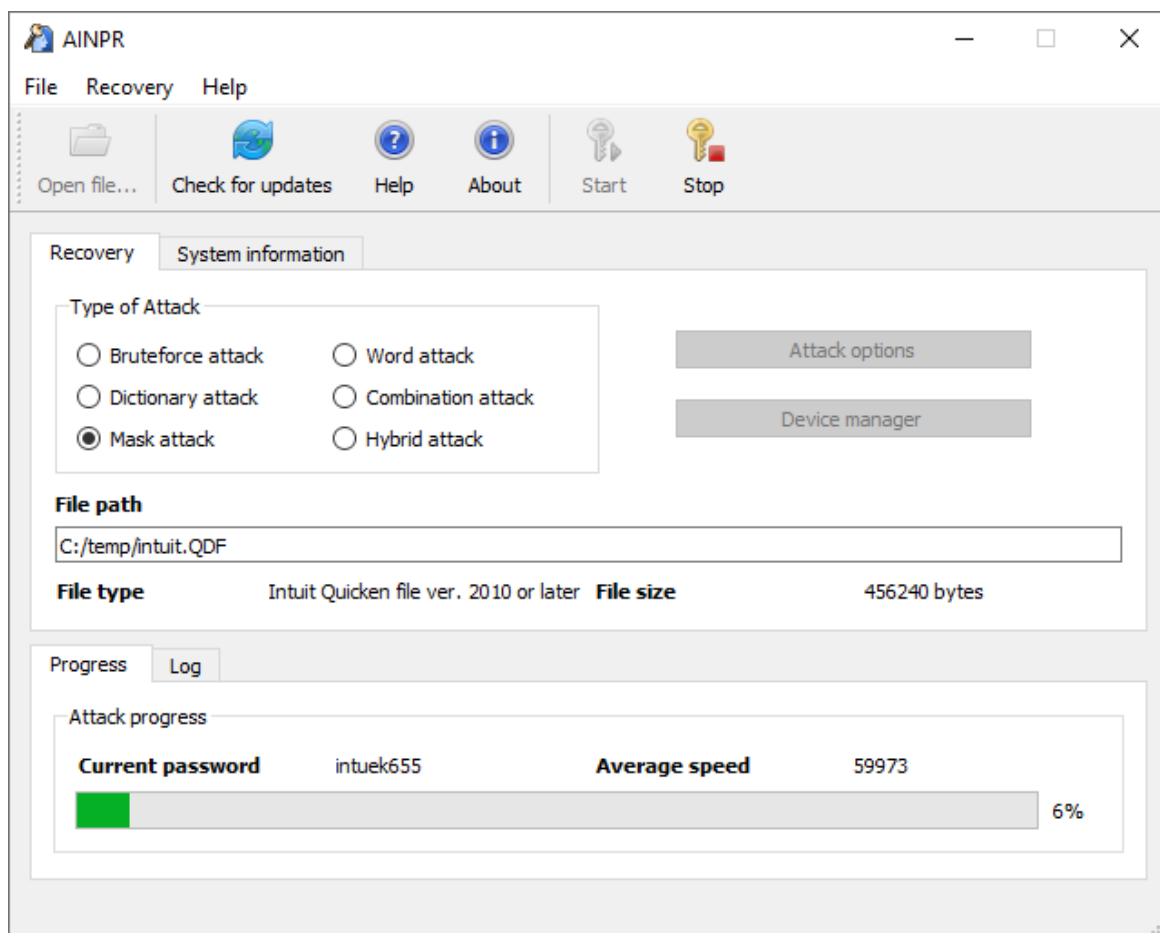
4.2.2.3 Пароли Quicken

Пароль на документ

В последних версиях Quicken (с 2006 по 2020) пароль на открытие файла не может быть восстановлен мгновенно. Единственный способ восстановить пароль - это попробовать подобрать возможные комбинации паролей. Этот процесс называется «атакой». Самая простая атака - это метод полного перебора, который предполагает перебор всех возможных комбинаций паролей в пределах заданного набора символов и заданной длины. Программа также поддерживает сложные атаки, такие как атака по словарю с мутациями или атака по маске. Прочтите [этот документ](#) (англ.), чтобы узнать больше об атаках.

После открытия файла выберите атаку и укажите параметры, затем нажмите кнопку «Пуск/Start», чтобы запустить атаку. Вы также можете выбрать, какие устройства CPU и GPU

будут использоваться для восстановления пароля с помощью кнопки «Диспетчер устройств/Device Manager». Атаку можно остановить в любой момент кнопкой «Стоп/Stop».



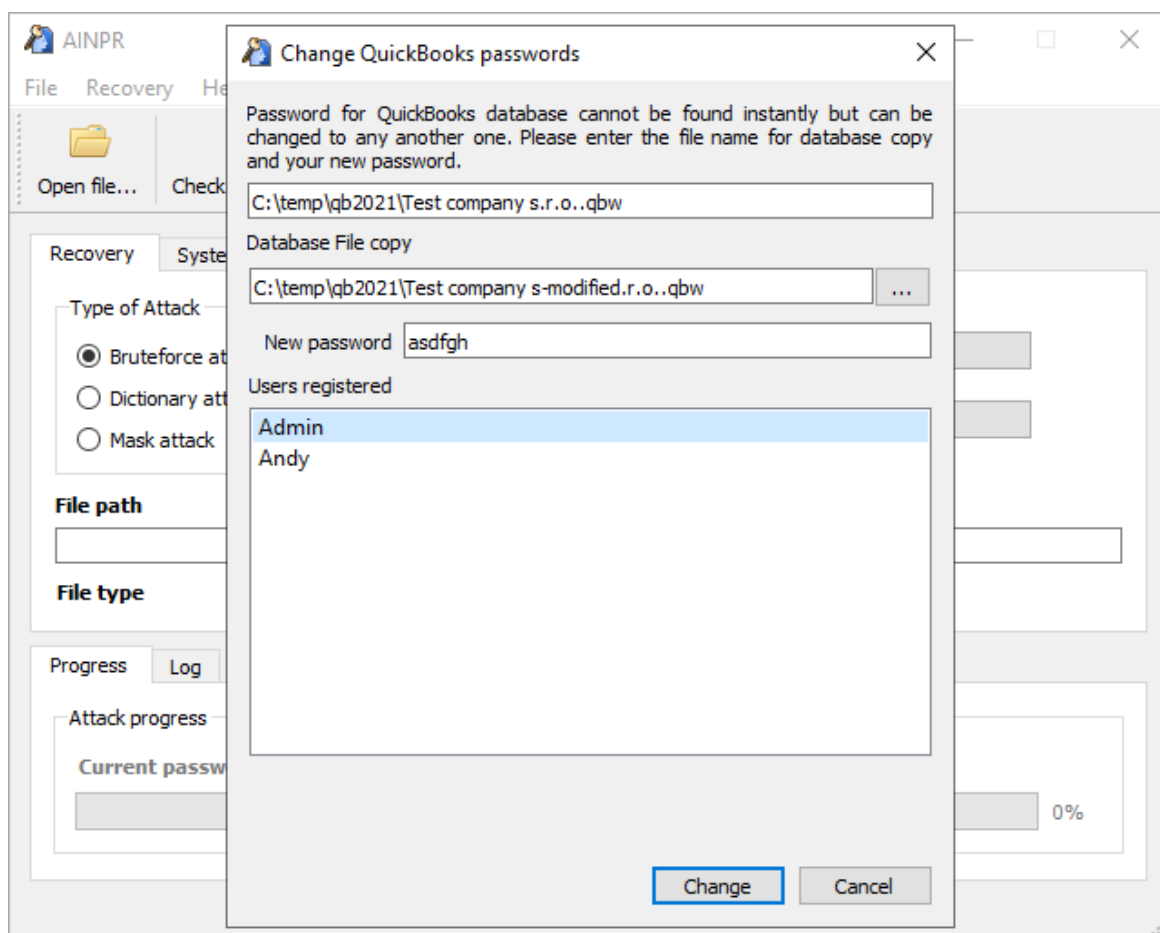
Примечание

Программа была протестирована со всеми версиями Quicken для США, а также с некоторыми версиями для Германии, Канады, Австралии, Новой Зеландии и Испании. Поддержка неамериканских версий не гарантируется.

4.2.2.4 Пароли QuickBooks

Пароль на открытие файла

Для последней версии QuickBooks (с 2006 по 2021 год) пароль на открытие файла не может быть мгновенно восстановлен. Однако вы можете изменить этот пароль и использовать новый пароль для открытия файла. В диалоговом окне смены пароля вы можете указать новое имя файла, путь и новый пароль:



По умолчанию файл с новым паролем сохраняется в том же каталоге. Строка "-modified" будет добавлена к исходному имени файла. Пароли для всех пользователей базы данных QuickBooks будут сброшены на тот же пароль, который вы ввели в поле «Новый пароль/New password».

4.3 Advanced Lotus Password Recovery

4.3.1 Введение

Advanced Lotus Password Recovery позволяет восстановить доступ к документам и учетным записям, защищенным паролем, мгновенно обнаруживая пароли, созданные в любом продукте и любой версии Lotus SmartSuite, а также пароли учетных записей FTP и прокси, заданные в компонентах Lotus SmartSuite. Вы можете восстанавливать пароли любой длины и сложности из Lotus Organizer, Lotus WordPro, Lotus 1-2-3, Lotus Approach и Freelance Graphics.

IBM / Lotus предоставляет возможность защищать документы SmartSuite паролем без предоставления инструментов для восстановления защищённых документов, если пароль будет утерян или забыт. Advanced Lotus Password Recovery - инструмент для мгновенной разблокировки защищенных паролем документов Lotus. Пароли любой длины и сложности можно найти мгновенно, без длительных атак. Advanced Lotus Password Recovery экономит ваше время и обеспечивает гарантированный мгновенный результат.

Программа, на которую вам предоставлена лицензия, является абсолютно законной, и вы можете использовать ее при условии, что вы являетесь законным владельцем всех файлов или данных, которые вы собираетесь восстановить с помощью нашего программного обеспечения, или имеете разрешение законного владельца на выполнение этих действий. Вы несете исключительную ответственность за любое незаконное использование программы. Соответственно, вы подтверждаете, что имеете законное право на доступ ко всем данным, информации и файлам, которые были недоступны.

Вы также подтверждаете, что восстановленные данные, пароли и / или файлы не будут использоваться в каких-либо незаконных целях. Помните, что восстановление пароля и последующее дешифрование данных неавторизованных или иным образом незаконно полученных файлов может представлять собой кражу или другое противоправное действие и может привести к вашему гражданскому и (или) уголовному преследованию.

4.3.2 Системные требования

Поддерживаемые операционные системы: Windows XP и выше, включая Windows 10.

4.3.3 Работа в программе ALPR

Нажмите кнопку «Открыть документ / Open document» и выберите файл, для которого нужно восстановить пароли. Формат файла будет распознан автоматически с соответствующим сообщением в окне «Статус / Status». Если формат файла не поддерживается ALPR, или файл поврежден или заблокирован другим приложением, или если он не защищен паролем, ALPR отобразит сообщение об ошибке. В противном случае пароль будет мгновенно восстановлен и показан в окне сообщения. Пароль также будет отображаться в окне журнала. Для баз данных Approach программа показывает новое окно, в котором отображается пароль файла, а также пароли ко всем группам. Вы можете скопировать пароли в буфер обмена Windows.

Чтобы восстановить пароли к FTP и прокси-серверам, управляемые из любого компонента SmartSuite и хранящиеся в локальной системе, нажмите кнопку «Интернет-пароли Lotus / Lotus internet passwords» на панели инструментов.

4.4 Advanced Mailbox Password Recovery

4.4.1 Введение

Advanced Mailbox Password Recovery (или просто AMBPR) извлекает информацию о логине и пароле, хранящуюся локально из нескольких почтовых клиентов: Microsoft Internet Mail And News, Eudora, TheBat!, TheBat! Voyager, Netscape Navigator/Communicator Mail, Pegasus mail, Calypso mail, FoxMail, Phoenix Mail, IncrediMail, @nyMail, QuickMail Pro, MailThem и MailThem Pro, Opera mail, Kaufman Mail Warrior, Becky! Internet Mail.

Помимо извлечения учетных данных аутентификации из локального хранилища, программа включает в себя эмулятор серверов POP3 и IMAP, который позволяет получить пароль POP3 / IMAP от любого почтового клиента, перехватывая их с помощью атаки типа MITM (man-in-the-middle/ атака посредника). Пароли восстанавливаются мгновенно. Поддерживаются многоязычные пароли.

Программа, на которую вам предоставлена лицензия, является абсолютно законной, и вы можете использовать ее при условии, что вы являетесь законным владельцем всех файлов или данных, которые вы собираетесь восстановить с помощью нашего программного

обеспечения, или имеете разрешение законного владельца на выполнение этих действий. Вы несете исключительную ответственность за любое незаконное использование программы. Соответственно, вы подтверждаете, что имеете законное право на доступ ко всем данным, информации и файлам, которые были недоступны.

Вы также подтверждаете, что восстановленные данные, пароли и / или файлы не будут использоваться в каких-либо незаконных целях. Помните, что восстановление пароля и последующее дешифрование данных неавторизованных или иным образом незаконно полученных файлов может представлять собой кражу или другое противоправное действие и может привести к вашему гражданскому и (или) уголовному преследованию.

4.4.2 Системные требования

Поддерживаемые операционные системы: Windows XP и выше, включая Windows 10.

4.4.3 Работа с AMBPR

4.4.3.1 Пользовательский интерфейс

Меню находится в левой части главного окна. Доступные команды включают Recovery/Восстановление ([автоматически](#)^[52] или [вручную](#)^[52]; эмулятор почтового сервера: [автоматически](#)^[52] и [вручную](#)^[53]), [Options/Параметры](#)^[53], Help/Справка and [Exit/Выход](#)^[54].

Щелкните список правой кнопкой мыши, просмотрите элементы, чтобы открыть контекстное меню.

Используйте CTRL-<цифра>, чтобы выбрать элемент меню высокого уровня, и ALT-<цифра>, чтобы переключиться на элемент нижнего уровня под ним. Поддерживаются следующие горячие клавиши:

CTRL-1: Восстановление

ALT-1: [Поиск почтовых клиентов](#)^[52]

ALT-2: [Автоматическое восстановление паролей](#)^[52]

ALT-3: [Восстановление паролей вручную](#)^[52]

ALT-4: [Эмулятор почтового сервера \(автоматический режим\)](#)^[52]

ALT-5: [Эмулятор почтового сервера \(ручной режим\)](#)^[53]

CTRL-2: [Параметры](#)^[53]

ALT-1: Зарегистрировать программу

ALT-2: Общие настройки

CTRL-3: Справка

ALT-1: Версии и совместимость

ALT-2: О программе

ALT-3: Справка

CTRL-4: [Выход](#)^[54]

ALT-1: Свернуть в трей

ALT-2: Выход в Windows

4.4.3.2 Восстановление

Поиск почтовых клиентов

Сканирует жесткий диск и реестр Windows на предмет поддерживаемых почтовых клиентов. Полный список почтовых клиентов, поддерживаемых инструментом, доступен на странице справки. Для каждого найденного почтового клиента программа показывает его полное имя, версию, адрес электронной почты отправителя, имя и организацию. Выделите и щелкните правой кнопкой мыши элемент контекстного меню, чтобы получить информацию о почтовом клиенте, сохранить, распечатать или скопировать информацию, или обновить список клиентов.

Автоматическое восстановление паролей

Эта команда пытается восстановить все типы паролей от всех почтовых клиентов, обнаруженных на компьютере. Программа показывает имя, тип пароля (POP3, SMTP, IMAP или аккаунт), адрес почтового сервера, если таковой имеется, а также логин и пароль.

Восстановление пароля вручную

Этот параметр следует использовать только по указанию службы технической поддержки. При использовании этой опции выберите почтовый клиент, для которого нужно получить пароли; введите зашифрованную строку или найдите соответствующий файл; и нажмите «Расшифровать/Decrypt».

Обратите внимание, что TheBat! Voyager поддерживается только в ручном режиме. Вы должны указать мастер-пароль, чтобы расшифровать пароли учетных записей.

Эмулятор почтового сервера (автоматический режим)

Если у вас есть почтовый клиент, который напрямую не поддерживается AMBPR, вы можете получить пароль другим способом. Эмулятор почтового сервера реализует "атаку посредника" для перехвата пароля, пока почтовый клиент аутентифицирует соединение.

В лучшем случае этого сценария все, что вам нужно сделать, это нажать кнопку «Подключиться/ Connect». Программа будет одновременно эмулировать серверы POP3 и IMAP4. Запустите свой почтовый клиент (если он уже был запущен, возможно потребуются перезапустить его) и выполните операцию отправки / получения писем. Обратите внимание, что почта не будет получена, потому что почтовый клиент будет подключаться к AMBPR вместо реального почтового сервера. Затем вернитесь в программу AMBPR и проверьте информацию о логине и пароле для учетных записей POP3 и IMAP.

Действуют некоторые ограничения. Во-первых, программе AMBPR нужны адреса почтовых серверов, к которым пытается подключиться почтовый клиент. Программа попытается получить список почтовых серверов автоматически, однако автоматическое обнаружение может не работать для некоторых клиентов. Если определенного почтового сервера нет в списке, нажмите «Добавить сервер/ Add server», чтобы добавить его вручную. Во-вторых, вы можете добавлять серверы по имени или по IP-адресу. Однако, если вы используете IP-адрес, эмуляция будет работать правильно только в том случае, если IP-адрес разрешен.

Также обратите внимание, что этот метод работает только для обычной аутентификации. Некоторые методы аутентификации (например, MD5 APOP) вообще не передают пароль на сервер, поэтому пароль не может быть перехвачен.

По умолчанию AMBPR использует порт 110 для POP3 и порт 143 для IMAP4. Если ваш почтовый клиент использует другие настройки порта, вам придется изменить их в [Параметрах](#) ⁵³ AMBPR.

Эмулятор почтового сервера (ручной режим)

Мы рекомендуем сначала попробовать [эмулятор почтового сервера \(автоматический режим\)](#) ⁵². Только в случае неудачи используйте ручной режим.

Последовательность шагов:

- Выберите эмуляцию POP3 или IMAP
- Нажмите "Подключиться в AMBPR/Connect in AMBPR".
- Запустите почтовый клиент
- Откройте свойства учетной записи в почтовом клиенте
- Обратите внимание на текущий адрес сервера входящей почты (POP3 или IMAP)
- Замените его на localhost или 127.0.0.1
- Сохраните свойства аккаунта
- Подключитесь к Интернету (не требуется для некоторых клиентов)
- Получите почту в почтовом клиенте
- Вернитесь в AMBPR и проверьте пользователя и пароль POP3

Этот метод работает только для обычной аутентификации; в других случаях (например, MD5 APOP) пароль не может быть передан на сервер и не может быть перехвачен.

В отличие от автоматического режима, ручной режим работает только для одной учетной записи POP3 или IMAP4 одновременно.

4.4.3.3 Параметры

Зарегистрируйте программу: после покупки лицензии введите свой регистрационный код в поле ввода и нажмите «Зарегистрироваться/Register».

Общие настройки:

Язык: выберите язык пользовательского интерфейса, затем нажмите «Обновить/Refresh» для обновления.

Если выбрать параметр "Печатать целое окно вместо текста/Print entire windows instead of text", AMBPR будет печатать содержимое текущего окна с помощью кнопки «Печать/Print», а не только текст.

Параметр "Проверять установленные почтовые клиенты при запуске/Check for installed e-mail clients at startup" позволяет программе AMBPR сканировать установленные почтовые клиенты при запуске.

Порт сервера POP3 и порт сервера IMAP: установите номера портов для серверов электронной почты; значения по умолчанию - 110 и 143 соответственно.

4.4.3.4 Выход

Параметр "Свернуть в трей/Minimize to tray" сворачивает программу в трей на панели инструментов Windows. Чтобы вернуть программу в нормальное состояние, дважды щелкните ее значок на панели задач.

Параметр "Выход в Windows/Exit to Windows" закрывает текущий сеанс.

4.5 Advanced Office Password Breaker

4.5.1 Введение

Advanced Office Password Breaker (AOPB) разблокирует защищенные паролем документы Microsoft Word и электронные таблицы Excel в течение гарантированного периода времени вместо взлома и восстановления сложных паролей. Инструмент поддерживает документы и электронные таблицы, созданные с помощью устаревших версий Microsoft Office или сохраненные в режиме совместимости в современных версиях.

В устаревших версиях Microsoft Word и Microsoft Excel для защиты документов использовалось слабое 40-битное шифрование. Этот тип шифрования можно легко взломать с помощью современных компьютеров и соответствующих инструментов. Атака на 40-битные ключи шифрования не только значительно быстрее, чем перебор всех возможных комбинаций букв и цифр, но и гарантирует временные рамки восстановления независимо от того, насколько длинным и сложным был пароль. Enterprise Edition может расшифровать устаревшие документы Word и большинство устаревших файлов Excel за считанные минуты.

4.5.2 Системные требования

- Windows XP или старше
- Около 1 МБ дискового пространства
- Около 8 ГБ дискового пространства для версии Enterprise для хранения предварительно просчитанных таблиц; вместо этого можно использовать быструю USB-флешку ёмкостью 8 ГБ или больше

4.5.3 О шифровании Word и Excel

Microsoft Word® и Microsoft Excel® поддерживают три уровня защиты документов / книг. Пользователь, создающий документ или книгу, имеет разрешение на чтение и запись в документ и контролирует уровень защиты. Существуют три уровня защиты документов:

- Защита от открытия файлов. Word® / Excel® требует, чтобы пользователь ввел пароль, чтобы открыть документ.
- Защита от изменения файла. Word® / Excel® требует, чтобы пользователь ввел пароль, чтобы открыть документ с разрешением на чтение / запись. Если в приглашении пользователь нажимает кнопку «Только для чтения/Read only», Word® / Excel® откроет документ только для чтения.
- Рекомендуемая защита только для чтения. Word® предлагает пользователю открыть документ только для чтения. Если пользователь нажимает Нет в приглашении, Word® / Excel® откроет документ с разрешением на чтение / запись, если документ не имеет другой защиты паролем.

Помимо защиты всего документа Word®, пользователи могут также защитить от несанкционированных изменений определенные элементы, такие как отслеживаемые изменения, комментарии и формы. В Excel® пользователи могут защищать рабочие листы и содержимое заблокированных ячеек, структуру книги, окна в книге, а также ячейки или формулы на листе или элементы на листе диаграммы. Наконец, можно запретить другим пользователям просматривать код, заблокировав проект VBA.

Все средства защиты, кроме пароля на открытие файла, не предназначены для обеспечения должной безопасности. Пароль можно восстановить, удалить или заменить мгновенно. Эти типы паролей не поддерживаются AOPB.

Если используется защита от открытия файлов, Word® и Excel® шифруют защищенные паролем документы с помощью симметричного шифрования, известного как RC4. В устаревших версиях Microsoft Office до Office 97 (например, Office 95, Office 6.0 и т. д.) реализация была слабой и позволяла извлекать и расшифровывать пароль. Такие файлы также не поддерживаются в AOPB.

Для файлов в формате Word® и Excel® 97/2000, включая файлы, сохраненные в Word® / Excel® XP / 2003 с использованием шифрования, совместимого с Office 97/2000, защита от открытия файлов будет довольно сильной. Пароль не может быть восстановлен мгновенно, и наиболее распространенные методы взлома пароля - это атаки полным перебором и по словарю. Однако эти методы не работают, если пароль достаточно длинный и сложный (не основанный на комбинации словарных слов). AOPB поддерживает этот тип защиты, атакуя двоичный ключ шифрования вместо пароля (см. [следующий раздел](#)⁵⁶¹).

Microsoft Office XP ввел шифрование на основе CSP (Поставщики служб шифрования); файлы, зашифрованные таким образом, не поддерживаются в AOPB.

Если AOPB показывает сообщение о том, что такие файлы не поддерживаются, когда вы пытаетесь начать атаку, прочтите главу «Файлы / пароли, которые не поддерживаются» для получения инструкций.

4.5.4 Поддерживаемые и неподдерживаемые форматы

Поддерживаются следующие форматы:

- Word®/Excel® 97/2000 документы, зашифрованные паролем на открытие
- Word®/Excel® XP/2003 сохранённые как совместимые с Office 97/2000, зашифрованные паролем на открытие

Следующие файлы Word® и Excel® не поддерживаются:

- Файлы без защиты от открытия файла (например, защита от изменения файла, защита документа / книги, пароли VBA).
- Файлы, созданные в Office 95 и более ранних версиях
- Файлы, созданные в Office XP / 2003, которые используют любой тип шифрования, кроме совместимого с Office 97/2000.
- Файлы, созданные в Office 2007
- Файлы, созданные на компьютере с французскими (стандартными) языковыми настройками, установленным в Панели управления> Региональные настройки. В то время шифрование

RC4 было запрещено во Франции, и Office 97/2000 / XP мог использовать только слабое шифрование.

Если файл не поддерживается, используйте [Advanced Office Password Recovery](#). Этот инструмент поддерживает все типы файлов, перечисленные выше, используя атаки полным перебором и по словарю.

4.5.5 Работа с AOPB

4.5.5.1 Предисловие

Как отмечалось ранее, файлы Word® / Excel® 97/2000 шифровали файлы с помощью RC4, если использовалась защита от открытия файлов. Самый простой способ взломать пароль - применить атаки полным перебором и по словарю; однако эти методы работают только с короткими и простыми паролями. Для взлома более длинных паролей требуется значительно больше времени. Например, пароль из 10 символов, состоящий из строчных, заглавных букв и цифр, имеет следующее количество возможных комбинаций:

$$(26 + 26 + 10) ^ 10 = 839,299,365,868,340,224$$

AOPB не атакует пароли. Вместо этого он нацелен на 40-битные ключи RC4, которые имеют следующее количество возможных комбинаций:

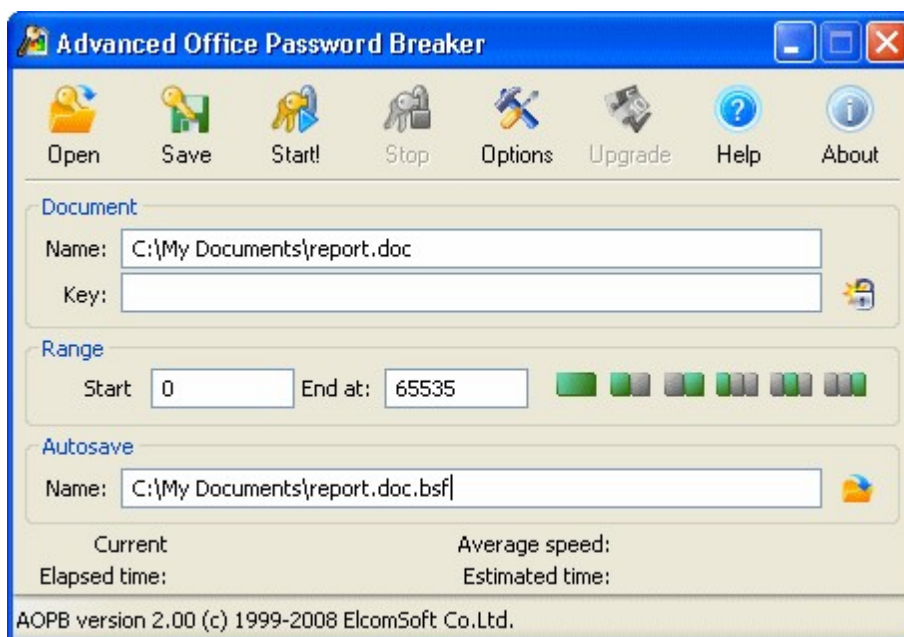
$$2 ^ 40 = 1,099,511,627,776$$

Вместо того, чтобы пробовать все возможные пароли, AOPB пробует все возможные ключи шифрования. Найденный ключ сразу расшифровывает документ, поэтому пароль больше не требуется. Расшифровка не мгновенная, но время восстановления очень разумное (обычно это вопрос нескольких часов). Более того, этот метод обеспечивает 100% успех независимо от длины пароля.

AOPB Enterprise Edition может использовать предварительно вычисленные хэш-таблицы, которые сокращают время поиска ключа до нескольких минут..

4.5.5.2 Поиск ключа шифрования

Чтобы сломать совместимый документ Word® или Excel®, нажмите «Открыть/Open» на панели инструментов. Вы также можете использовать «Открыть/Open» для загрузки ранее сохраненного проекта (*.bsf) с частично завершенной атакой.



В зависимости от настройки, указанной в «[Параметры/Options](#)»^[60], атака может начинаться автоматически. Если этого не произошло, нажмите «[Старт!/Start!](#)», чтобы начать атаку.

Атаку можно в любой момент прервать, нажав «[Стоп/Stop](#)». Во время атаки программа периодически сохраняет промежуточную информацию в файл состояния (.bsf). Вы можете вручную сохранить состояние атаки с помощью кнопки «[Сохранить/Save](#)» на панели инструментов или открыть ранее сохраненный файл с помощью кнопки «[Открыть/Open](#)».

Если опция «Начать атаку сразу после выбора документа» не выбрана, для этих параметров также будут установлены значения по умолчанию.

Вы можете указать диапазон атаки. Диапазон ключей из 1 099 511 627 776 комбинаций разделен на 65 536 блоков, по 16 777 216 ключей в каждом блоке. Поля «Начать с/Start with» и «Закончить на/End at» могут содержать значения от 0 до 65535; укажите соответственно минимум и максимум при запуске атаки. Кнопки справа позволяют выбрать весь диапазон, первую или вторую половину, или одну треть диапазона. Это удобно для разделения задачи между двумя или тремя компьютерами. Затем вы можете выбрать альтернативное имя для файла автосохранения .bsf.

Нажмите «[Старт/Start](#)», и программа начнет поиск ключей шифрования. Статистическая информация будет отображаться во время атаки, включая текущий блок, среднюю скорость (в ключах в секунду), прошедшее время и расчетное время.

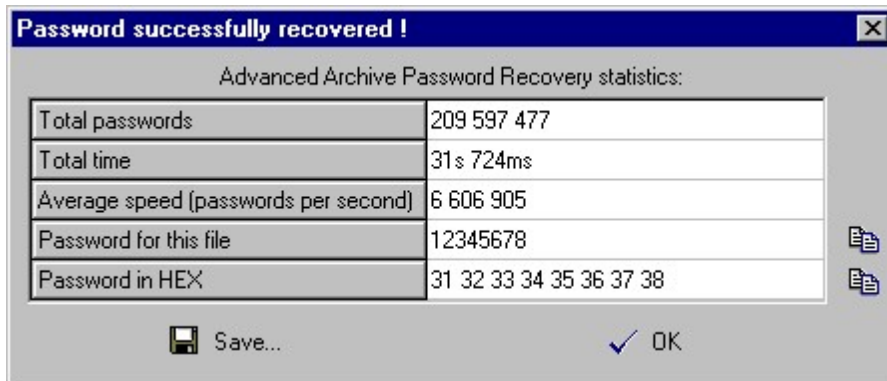
Дождитесь завершения атаки, чтобы [расшифровать файл](#)»^[58].

Enterprise версия AOPB позволяет ускорить атаку, включив опцию [Использовать предварительно вычисленные хэш-таблицы](#)»^[58].

Перед использованием таблиц, поставляемых в редакции Enterprise, мы рекомендуем скопировать их на SSD-накопитель или быстрый USB-накопитель (требуется 8 ГБ свободного места). Хранение хэш-таблиц на жестком диске не рекомендуется из-за значительно меньшей скорости произвольности механических дисков по сравнению с твердотельными носителями. Предварительно вычисленные таблицы гарантируют 100% восстановление документов Microsoft Word, и обеспечивают 97% успешной работы с электронными таблицами Microsoft Excel.

4.5.5.3 Расшифровка документа

Как только ключ шифрования будет найден, появится следующее окно:



В окне отображается общее количество протестированных ключей, прошедшее время, средняя скорость в ключах в секунду и сам ключ шифрования. Нажмите «Сохранить/Save», чтобы сохранить эту информацию в текстовый файл, или нажмите «Расшифровать/Decrypt», чтобы сохранить расшифрованную копию файла Word® или Excel®.

Примечание: если AOPV уже нашел ключ шифрования для определенного файла, но вы попытаетесь снова начать атаку на том же компьютере, вам будет предложено немедленно расшифровать файл или перезапустить атаку. AOPV хранит обнаруженные ключи шифрования в реестре Windows на локальном компьютере. Если вы успешно завершили атаку с использованием пробной версии AOPV, но не расшифровали файл из-за ограничений демонстрационной версии, вы сможете сделать это после покупки полной версии без повторного запуска атаки.

Также обратите внимание, что если у вас есть два или более документов, защищенных одним и тем же паролем, их ключи шифрования будут разными и уникальными, поскольку они основаны на информации, относящейся к конкретному документу. В результате обнаруженный ключ можно использовать только для дешифрования того документа, для которого он был обнаружен.

4.5.5.4 Радужная атака

С Enterprise версией AOPV вы можете ускорить дешифрование поддерживаемых документов Word и около 97% поддерживаемых электронных таблиц Excel, включив параметр «Использовать предварительно вычисленные хэш-таблицы/Use pre-computed hash tables». Нажмите «Обзор/Browse» и выберите папку, в которой расположены таблицы (расположение настраивается отдельно для Word и Excel). Для Microsoft Word папка должна содержать следующие подпапки / файлы:

```
0\t00_I17000.data
0\t00_I17000.index
1\t01_I17000.data
1\t01_I17000.index
2\t02_I17000.data
```

2\t02_I17000.index
3\t03_I17000.data
3\t03_I17000.index
4\t04_I17000.data
4\t04_I17000.index
5\t05_I17000.data
5\t05_I17000.index
missing.bin

Для Microsoft Excel:

0x62\0\t00_I12500.data
0x62\0\t00_I12500.index
0x62\1\t01_I12500.data
0x62\1\t01_I12500.index
0x62\2\t02_I12500.data
0x62\2\t02_I12500.index
0x66\0\t00_I12500.data
0x66\0\t00_I12500.index
0x66\1\t01_I12500.data
0x66\1\t01_I12500.index
0x66\2\t02_I12500.data
0x66\2\t02_I12500.index

С хеш-таблицами на жестком диске атака может занять от 10 до 30 минут. Если таблицы хранятся на быстром USB-накопителе или SSD-накопителе, большинство атак завершится за секунды, но может занять до 10-15 минут.

Параметр «Использовать глубокий анализ длины/Use deep length analysis» помогает контролировать способ обработки файлов Excel. В Excel не каждый файл содержит предсказуемые данные, необходимые для этого метода дешифрования, и некоторые параметры необходимо угадывать. В большинстве случаев требуется только один или два этапа (до нескольких минут каждый), чтобы найти правильные ключи шифрования, но есть вероятность, что параметры были выбраны неправильно, и потребуются больше этапов с другими комбинациями параметров. Процесс может занять час или два. Эта опция определяет, что делать, если ключ не был найден на первом этапе / этапе по умолчанию; выберите "Да/Yes", чтобы всегда выполнять дальнейшие атаки с другим набором параметров; выберите «Всегда спрашивать/Always ask», чтобы сделать выбор только в случае выхода из строя первых этапов; или «Нет/No» в противном случае.

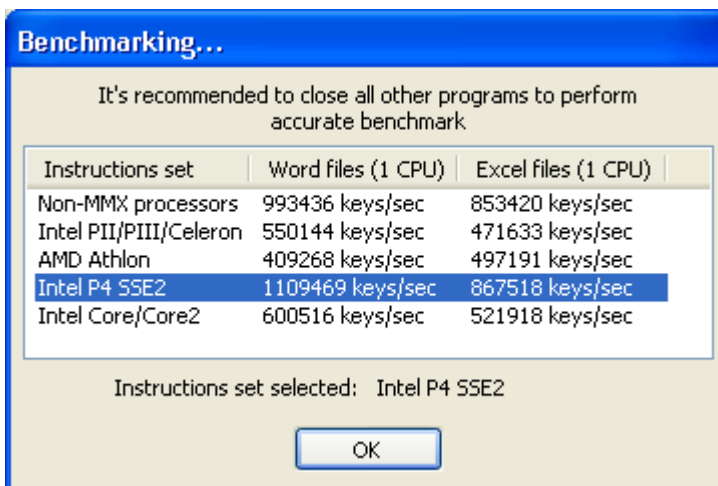
Обратите внимание, что если ключ не найден с помощью предварительно вычисленных таблиц Excel, вы все равно можете расшифровать файл, временно отключив эту опцию и выполнив полный поиск ключа.

Параметры

Кнопка «Параметры/Options» на панели инструментов открывает экран «Параметры/Options».



Программа автоматически определяет расширенные наборы инструкций, поддерживаемые ЦП вашего компьютера. Вы можете отменить выбор, указав набор инструкций после запуска тестирования производительности. Чтобы запустить тестирование, нажмите кнопку «Определить/Detect».



Вы также можете указать количество ядер ЦП, которое AOPB будет разрешено использовать, изменив значение в поле «Использовать ... ЦП/Use ... CPU». Примечание: для некоторых устаревших ЦП, поддерживающих гиперпоточность, настоятельно рекомендуется указать количество физических (не виртуальных) ядер ЦП и выбрать параметр «Использовать маску сходства/Use affinity mask». Для процессоров Pentium 4 Prescott и новее вы можете указать количество виртуальных ядер, что обычно повышает производительность примерно на 30-40%.

Приоритет/Priority (Фоновый / Нормальный / Высокий): укажите приоритет процесса. Для фоновой работы выберите Фоновый/Idle. Нормальный/Normal должен использоваться для работы переднего плана, в то время как опция Высокий/High приоритет отдает приоритет работе AOPB над другими процессами (не рекомендуется).

Автосохранение каждые XX мин: указывает период времени в минутах, по истечении которого AOPB сохранит текущий статус атаки.

Обновлять состояние каждые XX мс: интервал (в миллисекундах) между обновлениями окна состояния, показывающий текущий номер блока, скорость восстановления, прошедшее время и расчетное время. По умолчанию 2000.

Свернуть в трей: если эта опция включена, окно программы исчезнет с рабочего стола Windows при сворачивании окна. Небольшой значок будет создан в области трея на панели задач рядом с системными часами. Дважды щелкните этот значок, чтобы восстановить окно.

Начните атаку сразу после выбора документа: если включено, AOPB начнет поиск ключа шифрования сразу после открытия поддерживаемого документа. В противном случае вам придется нажать кнопку Старт/Start, чтобы начать атаку.

Используйте предварительно вычисленные хеш-таблицы (Enterprise версия): см. [Радужная атака](#)⁵⁸.

Зарегистрироваться/Register: нажмите эту кнопку, чтобы зарегистрировать свою копию AOPB, введя регистрационный код. Если вы уже зарегистрировали AOPB, эта кнопка отображается как «Обновить/Upgrade», что позволяет вам ввести другой код для обновления вашей версии.

Проверить наличие обновлений: проверка обновлений (требуется подключение к Интернету).

4.5.5.5 Интерфейс командной строки

Вы можете запустить программу через командную строку:

aopb.exe [options] <filename>

Доступные варианты:

/minimize OR /m	Сверните программу после запуска атаки
/dontstart OR /ds	Не запускайте атаку, просто загрузите / установите параметры из файла

Единственный обязательный параметр - имя файла. Это имя bsf-файла, в котором хранится имя файла Word® или Excel® для атаки, начальный и конечный блоки. Чтобы создать этот файл, откройте файл Word® / Excel® в AOPB, укажите диапазон блоков и нажмите «Сохранить/Save»

без запуска атаки; проверьте "Поиск ключа шифрования/[Searching for encryption key](#)^[56]" для получения подробной информации. В качестве альтернативы, если у вас уже была запущена атака, вы можете использовать файл автосохранения.

4.6 Advanced Office Password Recovery

4.6.1 Введение

Advanced Office Password Recovery разблокирует документы, созданные с помощью всех версий Microsoft Office, от Microsoft Office 2.0 до Microsoft Office 2019, а также Office 365 и Microsoft 365. Кроме того, инструмент поддерживает множество типов паролей, защищающих документы в форматах OpenDocument и Hangul Office. . Advanced Office Password Recovery может восстанавливать пароли для Microsoft Word, Excel, Access, Outlook, Project, Money, PowerPoint, Visio, Publisher и OneNote, всех приложений OpenOffice и всех приложений, входящих в пакет Hangul / Hancell Office.

Возможности продукта можно разделить на две основные категории: мгновенное снятие защиты паролем и восстановление исходных паролей с помощью атак с использованием графических процессоров.

Мгновенное снятие защиты с документа

Некоторые типы защиты документов могут быть сняты мгновенно и без длительных атак. Многие типы ограничений, такие как «пароль на изменения», «пароль VBA» или «пароль на печать», могут быть мгновенно сняты.

Кроме того, некоторые типы «паролей на открытие» также могут быть удалены мгновенно. Тщательно проанализировав алгоритмы и реализации защиты паролем в различных версиях приложений Microsoft Office, компания Elcomsoft разработала обходные решения, позволяющие мгновенно восстанавливать определенные типы паролей, а не проводить длительные атаки.

Восстанавливает пароли на открытие

При правильной реализации пароль на открытие шифрует всё содержимое документа, что делает невозможным мгновенное снятие пароля. Advanced Office Password Recovery реализует ряд очень сложных атак, включая атаки по словарю, атаки по маске, комбинированные и гибридные атаки. Если ничего не помогает, можно использовать высокооптимизированную атаку методом полного перебора с аппаратным ускорением.

4.6.2 Подготовка к работе с AOPR

4.6.2.1 Системные требования

Для правильной работы **Advanced Office Password Recovery** требуется следующая конфигурация системы:

- Поддерживаемые операционные системы:

Windows® XP
 Windows® Vista
 Windows® 7
 Windows® 8
 Windows® 8.1
 Windows® 10
 Windows® Server 2003
 Windows® Server 2008
 Windows® Server 2008 R2
 Windows® Server 2012
 Windows® Server 2012 R2
 Windows® Server 2016
 Windows® Server 2019

- Около 100 МБ дискового пространства
- Для некоторых функций могут потребоваться права администратора

4.6.2.2 Поддерживаемые типы файлов и пароли

Advanced Office Password Recovery имеет три редакции: **Home** (домашнюю), **Standard** (стандартную) и **Professional** (профессиональную). Список поддерживаемых типов файлов и паролей:

	AOPR Home	AOPR Standard	AOPR Professional
Microsoft® Word® (versions: 2.0, 6.0, 95, 97, 2000, XP, 2003 - 2019)			
Пароль на открытие ⁷⁴	Да	Да	Да
Пароль на изменения ⁸²	Да	Да	Да
Пароль защищающий документ ⁸²	Да	Да	Да
Пароль к VBA Project ⁷⁶	Нет	Да	Да
Microsoft® Excel® (версии: 3.0, 4.0, 95, 97, 2000, XP, 2003 - 2019)			
Пароль на открытие ⁷⁴	Да	Да	Да
Пароль на изменения ⁸¹	Да	Да	Да
Пароль книги ⁸¹	Да	Да	Да
Общий пароль книги ⁸¹	Да	Да	Да
Пароль листа ⁸¹	Да	Да	Да
Пароль к VBA Project ⁷⁶	Нет	Да	Да
Разблокировка надстроек XLA ⁸²	Нет	Да	Да
Microsoft® Access® (версии: 2.0, 95, 97, 2000, XP, 2003 - 2019)			
Пароль на открытие ⁷⁷	Да	Да	Да
Пароли уровней пользователя и группы ⁷⁹	Нет	Нет	Да
Database Owner и Security ID ⁷⁷	Нет	Нет	Да
Пароль к VBA Project ⁷⁶ (поддерживается)	Нет	Нет	Да

только через обход защиты VBA ^[69])			
Microsoft® Outlook® (версии: 97, 2000, XP, 2003 - 2019)			
Пароль на открытие ^[83] (PST-файлы)	Нет	Да	Да
Пароль к VBA Project ^[76]	Нет	Да	Да
Сохранённые пароли к E-Mail аккаунтам ^[83]	Нет	Да	Да
Microsoft® PowerPoint® (версии: 4.0, 95, 97, 2000, XP, 2003 - 2019)			
Пароль на открытие ^[74]	Нет	Нет	Да
Пароль на изменения ^[83]	Нет	Нет	Да
Пароль к VBA Project ^[76]	Нет	Нет	Да
Microsoft® OneNote® (версии: 2003 с SP1 и новее)			
Пароль на открытие ^[75]	Нет	Нет	Да
Microsoft® Visio® (версии: 4.0, 5.0, 2000, 2002)			
VBA Project ^[76] (в некоторых версиях поддерживается только через обход защиты VBA ^[69])	Нет	Нет	Да
Microsoft® Publisher			
Пароль к VBA Project ^[76]	Нет	Нет	Да
Microsoft® Project®			
Пароль на открытие ^[84]	Нет	Нет	Да
Пароль на изменения ^[84]	Нет	Нет	Да
Пароль к VBA Project ^[76]	Нет	Нет	Да
Microsoft® Money (версии: 2.0, 3.0, 4.0, 5.0, 97, 99, 2000, 2002, 2003, 2004, 2005, 2006, 2007, 2008)			
Пароль на открытие ^[84]	Нет	Нет	Да
Сохранённые пароли к MS Passport ^[69]	Нет	Нет	Да
Apple iWork (версии: '09 - 2020)			
Пароль на открытие	Нет	Да	Да
All Applications with VBA			
Обход защиты VBA ^[69]	Нет	Нет	Да
Hangul/Hancom Office Hanword/Word (версии 2010 - 2020)			
Пароль на открытие	Нет	Нет	Да
Hangul/Hancom Office Hancell/Cell (версии 2010 - 2020)			
Пароль на открытие	Нет	Нет	Да
OpenDocument (OpenOffice, LibreOffice)			
Пароль на открытие	Нет	Да	Да
MyOffice (МойОфис)			
Пароль на открытие (совместимый с MS Office)	Да	Да	Да
Пароль на открытие (совместимый с OpenDocument)	Нет	Да	Да

4.6.2.3 Поддерживаемое оборудование

Advanced Office Password Recovery может использовать ядра ЦП и графические карты (ГП) для перебора паролей, которые невозможно найти мгновенно. Количество процессоров и графических процессоров, которые можно использовать для восстановления пароля, зависит от формата файла и версии программы.

Подробную информацию о поддерживаемых графических процессорах можно найти в нашей базе знаний [Knowledge Base](#).

Пробная версия AOPR поддерживает все доступные процессоры и один графический процессор, чтобы продемонстрировать высочайшую скорость восстановления пароля. Количество поддерживаемых ядер ЦП и модулей графического процессора будет зависеть от типа лицензии следующим образом:

	редакция Home	редакция Standard	редакция Professional
Количество поддерживаемых ядер ЦП	1	4	64
Количество поддерживаемых графических процессоров	-	1	64

Обратите внимание, что использование графического процессора (ГПУ) для атаки паролей снижает скорость реакции пользовательского интерфейса Windows. Вы можете использовать диспетчер устройств (расположенный на вкладке «Параметры») для настройки аппаратных ресурсов, которые будут использоваться для атаки.

4.6.2.4 Получение справки и технической поддержки

Наши контакты

Для получения **технической поддержки** используйте следующую форму: <https://support.elcomsoft.com>

С нами можно связаться на русском или английском языке.

Где приобрести последнюю версию

Вы можете скачать последнюю версию **AOPR** по следующей ссылке:

<https://www.elcomsoft.ru/aopr.html>

4.6.3 Работа с AOPR

4.6.3.1 Восстановление паролей к документам

Выбор файла

Нажмите **«Открыть файл»** или **«Файл | Открыть файл»**, чтобы открыть документ для атаки.

Формат файла будет распознан автоматически. Если указанный формат файла не поддерживается в **AOPR**, или если файл поврежден или заблокирован другим приложением, отобразится соответствующее сообщение об ошибке.

Вы можете очистить список последних файлов через меню **«Файл | Очистить историю файлов»**.

Анализ результатов

Следующие сообщения об ошибках и информационные сообщения могут отображаться после открытия и обработки файла.

- **Все или некоторые пароли были восстановлены.** Откроется диалоговое окно с паролями. Поля пароля могут содержать одно из следующих сообщений:
 - **<none>** - пароль не установлен;
 - **<cannot be found instantly>** - пароль не может быть восстановлен мгновенно. Укажите параметры атаки и начните атаку, чтобы восстановить пароль. Вы можете [создать проект](#)^[67], чтобы сохранить параметры атаки в файл.
 - **<can be changed>** - пароль нельзя восстановить, но его можно изменить или удалить. В этом случае диалог с результатами содержит две дополнительные кнопки: **«Изменить пароль»** и **«Удалить пароль»**. Вы можете изменить или удалить пароль, просто нажав эти кнопки. Выбранный файл не должен быть защищен от записи для успешного выполнения этой операции.
 - **<not available>** - пароль восстановить не удалось. Возможные причины:
 - Выбранный формат файла не имеет пароля
 - Пароль для расшифровки документа еще не найден
 - **<error>** - произошла ошибка в процессе восстановления пароля. Появится окно сообщения с более подробной информацией.
 - **<not supported>** - пароль не поддерживается текущей версией AOPR.
 - **<not displayed in trial version>** - пароль найден, но его длина превышает ограничения пробной версии. Вы должны приобрести лицензию, чтобы увидеть этот пароль.

Нажмите **«Копировать в буфер обмена»**, чтобы скопировать пароль в буфер обмена.

- **Формат файла не поддерживается.** Это может произойти, когда вы выбираете файл, формат которого не поддерживается в AOPR. См. [«Поддерживаемые типы файлов и пароли»](#)^[63], чтобы узнать, какие форматы файлов поддерживаются в AOPR.
- **Произошла ошибка.** Отображается окно сообщения об ошибке.

Пожалуйста, ознакомьтесь с [Руководством по паролям](#)^[73], чтобы получить дополнительную информацию о типах паролей.

4.6.3.2 Работа с проектами

Создание проекта

Проект позволяет сохранять и восстанавливать настройки атаки и прогресс. Проект содержит информацию об исходном файле, выбранных параметрах и наборе символов. Файлы проекта полностью автономны и могут передаваться; их можно скопировать на другой компьютер с установленным AOPR без необходимости копировать исходный файл, поскольку **проект содержит всю информацию, необходимую для восстановления пароля.**

Файлы проекта имеют расширение **.AOPR**. По умолчанию имя проекта будет выбрано в соответствии с именем атакуемого файла. Например, если обрабатываемый файл называется «test.doc», имя проекта - «test.aopr».

Сохранение проекта

После загрузки файла вы можете сохранить проект. Имя файла проекта выбирается автоматически на основе имени файла. Если вы хотите использовать другое имя, используйте «**Файл | Сохранить проект как ...**». Если вы не хотите изменять имя проекта, используйте вместо него «**Файл | Сохранить проект**».

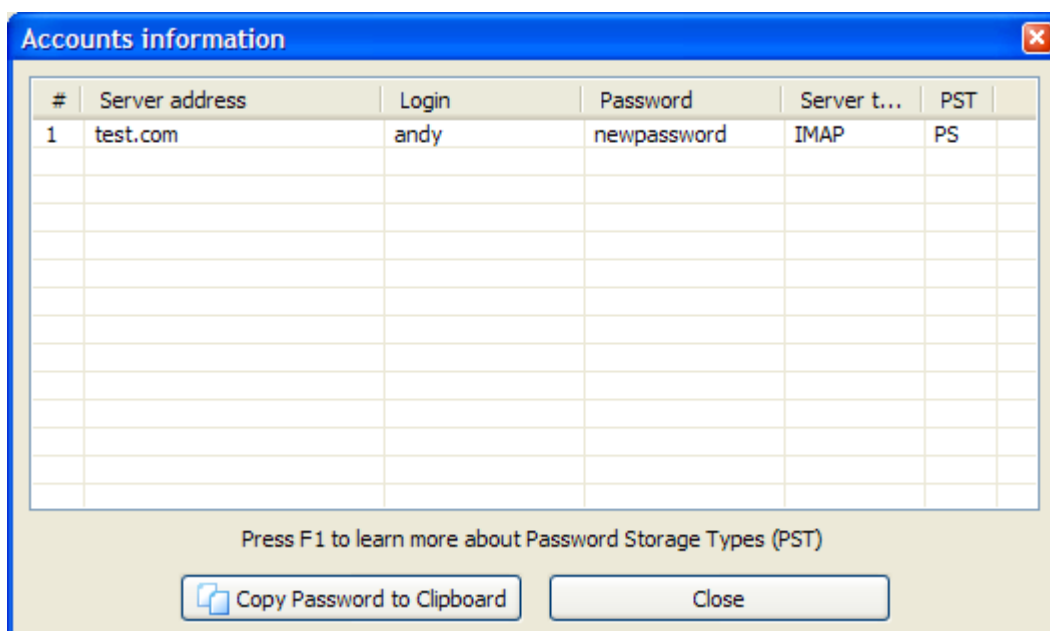
Если у вас уже есть проект, вам будет предложено сохранить его при закрытии программы. Вы можете отключить этот запрос, сняв флажок «**Запрашивать, если проект был изменен**» во вкладке «**Параметры**».

4.6.3.3 Почтовые аккаунты Outlook

Восстановление паролей учетных записей электронной почты

Microsoft® Outlook® email account passwords can be recovered by clicking the "**MS Outlook®**" button or selecting the "**Internet | Outlook® Mail Accounts...**" from the menu.

Если Outlook® установлен и настроена хотя бы одна учетная запись электронной почты, отобразится следующее диалоговое окно:



[Узнать больше о типах хранения паролей.](#)^[68]

Типы хранения паролей Outlook®

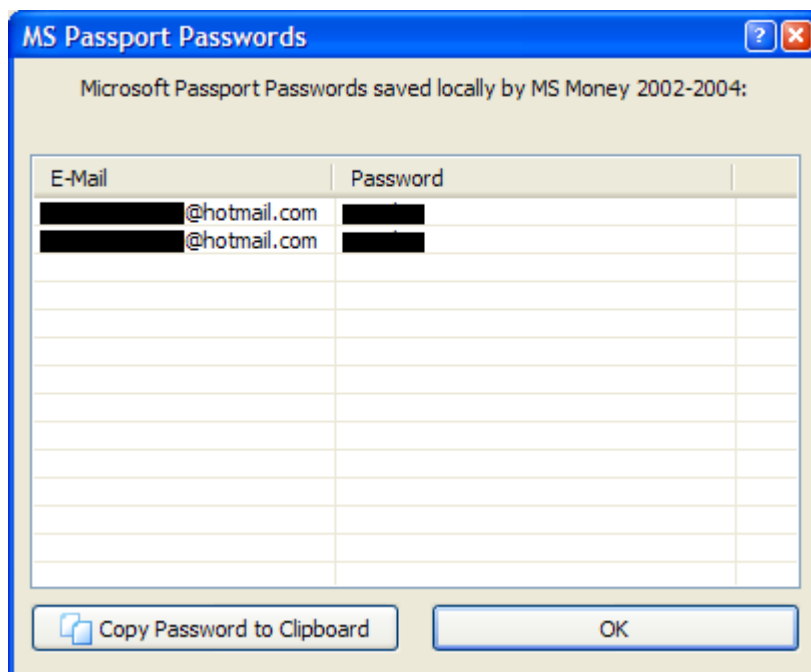
Microsoft® Outlook® хранит пароли учетных записей в Защищенном хранилище. Пароли хранятся в зашифрованном виде в системном реестре. В некоторых случаях AOPR может выдавать ошибку или отображать неправильные пароли. Это может произойти, если системный реестр поврежден, или у вас нет достаточных прав для доступа к некоторым ключам в реестре, или если на вашем компьютере не установлена подсистема защищенного хранилища. Проверка типов хранилища паролей может помочь определить основную причину проблемы. Доступные типы хранения паролей:

- PS** - Пароль успешно получен и сохранен в защищенном хранилище.
- O3** - Пароль хранится в реестре Windows в Outlook® 2003.
- OL** - Пароль успешно получен и сохранен в реестре с использованием слабого алгоритма шифрования.
- NP** - Пароль не найден в защищенном хранилище. В некоторых случаях это указывает на то, что имя пользователя используется в качестве пароля или что подсистема защищенного хранилища повреждена.
- UN** - Неизвестный тип хранилища паролей. Возможно вы используете версию Outlook®, не поддерживаемую в AOPR, или реестр поврежден.
- ER** - Ошибка при получении пароля.
- NR** - Пароль не был получен. У вас недостаточно прав для разблокировки Защищенного хранилища, или Защищенное хранилище не установлено на компьютере.
- NO** - Пароль для этой учетной записи отсутствует.

Если тип хранилища "UN", "ER" или "NR", отправьте [журнал отладки](#)^[84] в [службу технической поддержки Elcomsoft](#)^[65].

4.6.3.4 Сохраненные пароли Microsoft Passport

Чтобы восстановить пароли аутентификации **Microsoft Passport**, хранящиеся локально в **Microsoft® Money**, нажмите кнопку **«MS Passport»**. Если пароли хранятся локально на компьютере, отобразится следующий диалог:



4.6.3.5 Обход защиты VBA

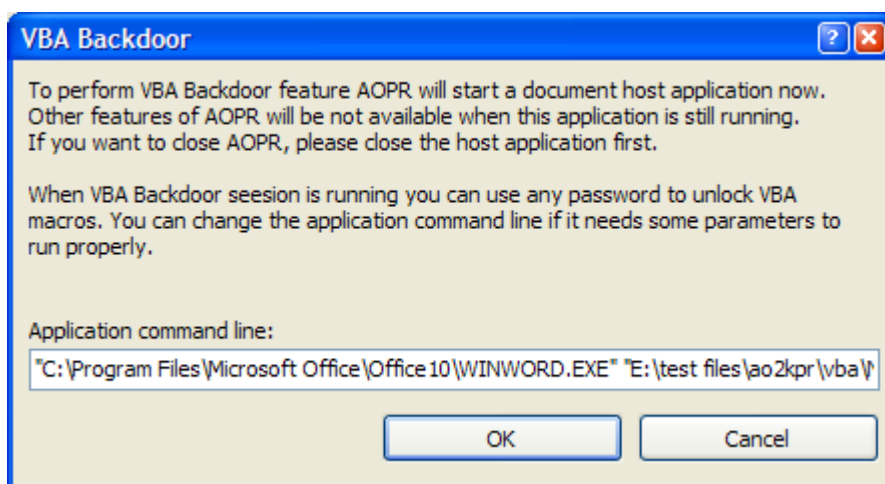
Если у вас есть документ с проектом VBA, который защищён паролем, и у вас есть проблема с восстановлением пароля и/или разблокировкой проекта VBA, вы можете использовать **бэкдор (т.е. обход защиты) VBA**. Данный обход защиты работает для всех приложений, которые могут создавать проекты VBA, а не только для Microsoft® Office. Такие приложения, как Corel WordPerfect Office и AutoCAD, также имеют этот бэкдор.

Эта возможность поможет вам обойти защиту паролем вместо того, чтобы его восстанавливать.

Метод 1

Сначала **закройте все запущенные экземпляры приложений MS Office**.

Нажмите **VBA Backdoor** на панели инструментов **AOPR** (или выберите в меню **VBA Backdoor | Открыть файл через бэкдор**). Прочтите инструкции в диалоговом окне и откройте файл с проектом VBA:



Затем **AOPR** будет использовать специальный метод для загрузки документа в приложение, которое использовалось для создания проекта VBA. В этом приложении (например, Microsoft Word) откройте окно свойств VBA, которое обычно находится в разделе «**Инструменты | Макрос | Редактор Visual Basic**» или «**Инструменты | Свойства VBA Project**». Вам будет предложено ввести пароль. Введите любой непустой пароль (например, хуз), и он будет принят.

Если ваш документ был создан в Microsoft® Office 97, вы можете использовать более старшую версию (например, Office 2000 или Office XP), чтобы снять защиту с проекта, но не наоборот.

Метод 2

Вы можете запустить приложение с поддержкой VBA (например, Word®, Excel®, FrontPage, AutoCad и т. д.) через **AOPR**, используя пункт меню «**VBA Backdoor | Запустить приложение**». Бэкдор будет активирован в запущенном приложении. После этого будет принят любой непустой пароль для проектов VBA, открытых в этом экземпляре.

Обратите внимание, что этот бэкдор поддерживается только для ограниченного числа версий движка VBA (VBE.DLL, VBE6.DLL, VBE7.DLL) до Microsoft® Office 2013 включительно. После запуска приложения **AOPR** отметит в журнале размер и номер версии DLL. Если на вашем компьютере не установлена поддерживаемая версия движка VBA, **AOPR** попытается использовать общий патч, который может не работать при определенных обстоятельствах.

4.6.4 Настройка параметров AOPR

4.6.4.1 Тип атаки

Если пароль не может быть восстановлен мгновенно, необходимо использовать один из типов атаки. Подробное описание доступных атак можно найти в нашей [базе знаний](#).

4.6.4.2 Предварительная атака

Предварительная атака/Preliminary Attack - это набор заранее определенных атак, если пароль не может быть мгновенно восстановлен. Когда эта атака запущена, отображается следующий диалог:



Предварительная атака/Preliminary Attack состоит из четырех независимых атак, которые можно включить или отключить в настройках.

- **Атака найденных паролей.** Эта атака доступна всегда. Она проверяет все пароли, которые были обнаружены в текущем документе, до нахождения текущего пароля. Эта атака помогает быстро обнаруживать повторно используемые пароли.
- **Атака кэша паролей.** Эта атака проверяет [кэш паролей](#)^[73]. В отличие от атаки найденных паролей, атака кэша нацелена на пароли, обнаруженные в других документах. Эту атаку можно включить или отключить с помощью флажка **«Предварительная атака кэша паролей»** во вкладке **«Параметры»**.
- **Предварительная словарная атака.** Выполняет атаку по словарю, используя словарь по умолчанию. Эту атаку можно включить или отключить, установив флажок **«Предварительная атака по словарю»** во вкладке **«Параметры»**.
- **Предварительная атака методом полного перебора.** Выполняет атаку полным перебором с несколькими predetermined наборами символов. Эту атаку можно включить или отключить с помощью параметра **«Предварительная атака методом полного перебора»** на вкладке **«Параметры»**.

Предварительная атака может занять несколько минут. Вы можете остановить его в любой момент, нажав кнопку **«Стоп/Stop»**.

Вы можете [установить свои собственные языки и наборы символов](#)^[71] для предварительной атаки.

4.6.4.3 Настройка предварительной атаки

Каждый раз, когда вы открываете документ в Advanced Office Password Recovery, инструмент выполняет предварительную атаку, если установлен пароль на открытие файла. Эта атака пытается использовать пароли, восстановленные в прошлом (хранящиеся в [кеше паролей](#)^[73]), после чего следует атака по короткому словарю и атаки методом полного перебора.

Атака полным перебором состоит из двух частей:

1. Цифры и латинские символы
2. Национальные символы в зависимости от кодовой страницы Windows

Вы можете установить свои собственные наборы символов и языки для предварительной атаки с помощью файла **«attack.xml»**, который находится в каталоге, где установлен Advanced Office Password Recovery.

Первый раздел этого файла - это языковая карта:

```
<LanguageNameMap>
  <x0411>Japanese</x0411>
  <x0419>Russian</x0419>
  <x0422>Russian</x0422>
  <x0423>Russian</x0423>
</LanguageNameMap>
```

Коды представляют собой [идентификаторы языка](#) Windows. Вы можете присвоить любому LID собственное имя.

Следующий раздел содержит predefined кодировки:

```
<Charsets>
  <LatinAllCaps>ABCDEFGHIJKLMNOPQRSTUVWXYZ</LatinAllCaps>
  <LatinAllSmall>abcdefghijklmnopqrstuvwxyz</LatinAllSmall>
  . . .
</Charsets>
```

Все кодировки являются Unicode, поэтому вы можете определять любые национальные символы.

Последний раздел - «документы». Во всех частях этого раздела есть комментарии о типах документов. Вы можете определить общие наборы символов и наборы символов, относящиеся к системному языку. Каждая запись «атаки» определяет длину пароля и набор символов.

В этом XML-файле вы можете изменить стандартную предварительную атаку и определить собственные наборы символов для любого языка.

4.6.4.4 Общие настройки

Другие настройки

Диспетчер устройств позволяет выбрать оборудование, которое будет использоваться для взлома паролей. По умолчанию AOPR использует все доступные ядра ЦП и графические карты для достижения максимальной производительности.

Включить журнал отладки создает отдельный [файл журнала](#)^[84] («**aoxpr_debug_log.txt**») с подробной информацией для устранения неполадок. Обычно эта опция выключена. Файл будет сохранен в каталоге, указанном в параметре **Папка для файлов журнала**.

Если вы выберете **«Свернуть в трей»**, программа будет свернута в системный трей.

Если вы отключите параметр **«Спрашивать, если проект был изменен»**, AOPR не будет отображать сообщение **«Проект был изменен. Сохранить?»**, когда вы изменяете некоторые параметры и открываете другой проект или создаете новый.

На вкладке «**Параметры**» вы можете включить или отключить [предварительные атаки](#)^[70].

4.6.4.5 Кэш паролей

О кэше паролей

Кэш паролей - это специальное хранилище, предназначенное для хранения всех паролей, обнаруженных с помощью **AOPR**. Записи хранятся в формате Unicode для поддержки международных наборов символов. Для предотвращения несанкционированного доступа к кэшу паролей он сам может быть защищен паролем. Если вы укажете пароль, файл кэша паролей будет зашифрован с помощью RC4. Хеш SHA-1 будет храниться в заголовке файла.

Кэш паролей используется в [предварительной атаке](#)^[70]. Если пароль документа не может быть мгновенно восстановлен, **AOPR** сначала проверяет кэш паролей.

Имя файла по умолчанию для кэша паролей - **aopr.pwc**. Вы можете [управлять файлами кэша паролей](#)^[73] во вкладке «**Кэш паролей**».

Управление файлами кэша паролей

Чтобы указать путь к файлу кэша паролей, нажмите кнопку «**Выбрать файл ...**» и введите имя файла.

Чтобы защитить паролем файл кэша, нажмите кнопку «**Установить пароль ...**» и введите пароль.

Вы также можете **просмотреть** и **очистить** файл кэша, нажав соответствующие кнопки, или полностью отключить кэш с помощью параметра «**Добавить все найденные пароли в кэш**».

4.6.5 Руководство по паролям

Стойкие пароли

[Пароли на открытие файла Word®/Excel® \(Office 97/2000\)](#)^[74]

[Пароли на открытие файла Word®/Excel®/PowerPoint® \(Office XP и старше\)](#)^[74]

[Пароли на открытие файла Microsoft® Money 2002](#)^[75]

Слабые пароли

[Пароли на открытие файла Word®/Excel® \(слабое шифрование\)](#)^[76]

[Visual Basic for Applications \(VBA\)](#)^[76]

Microsoft® Access®

[Общие пароли баз данных Access®, информация о владельце](#)^[77]

[Пользовательские пароли Access®](#)^[79]

Microsoft® Excel®

[Документы Excel® - все пароли кроме пароля на открытие файла](#)^[81]

[Защита надстроек Excel® \(XLA\)](#)^[82]
[Pocket Excel®](#)^[82]

Microsoft® Word®

[Документы Word® - все пароли кроме пароля на открытие](#)^[82]

Microsoft® Outlook®

[Пароль к файлу личного хранилища Outlook®](#)^[83]

[Пароли учетных записей электронной почты Outlook®](#)^[83]

[Microsoft® PowerPoint®](#)^[83]

[Microsoft® Money](#)^[84]

[Microsoft® Project](#)^[84]

4.6.5.1 Стойкие пароли

Пароль на открытие файла Word/Excel (Office 97/2000)

Этот пароль может быть назначен в Microsoft® Word® и Excel® 97 и более поздних версиях.

Пароль на открытие файла в Word® или Excel® 97/2000 шифрует документ с помощью криптографического алгоритма RC4. Microsoft® Office использует хэш MD5 для проверки пароля. Следовательно, этот пароль нельзя восстановить мгновенно.

AOPR может восстановить пароль, используя разные [атаки](#)^[70]: по словарю или методом полного перебора. Для атаки полным перебором укажите длину пароля (до 15 символов) и диапазон пароля (может включать национальные символы). Обратите внимание, что для взлома длинных и сложных паролей может потребоваться распределенная атака (с помощью Elcomsoft Distributed Password Recovery).

Пароль на открытие файла Word/Excel/PowerPoint (Office XP/2003)

Microsoft® Office XP, Office 2003 и более новые версии поддерживают три различных уровня защиты паролем.

Шифрование совместимое с Office 97/2000

По умолчанию в Microsoft® Office XP методом шифрования является *метод, совместимый с Office 97/2000*. Это проприетарное [шифрование](#)^[74], поддерживаемое в Microsoft® Office 97/2000 (Word® и Excel®), которое является алгоритмом по умолчанию для обеспечения обратной совместимости и международной переносимости документов.

Слабое шифрование (XOR)

Этот метод идентичен Office 95 и более ранним [алгоритмам шифрования XOR](#)^[76], которые поддерживаются более ранними версиями Word® и Excel® и по-прежнему используются в

Office 2000, когда региональным стандартом системы является Франция. Это быстрый и простой алгоритм, позволяющий мгновенно восстановить пароль.

Криптопровайдер

Это новый метод шифрования, представленный в Microsoft® Office XP. Поставщик криптографических услуг (CSP) - это независимый программный модуль, который выполняет криптографические алгоритмы для аутентификации, кодирования и шифрования.

Microsoft® разработала несколько различных поставщиков криптографических услуг. Документы Office XP можно зашифровать с помощью любого CSP, поддерживающего RC4 (поточковый шифр) и SHA-1 (алгоритм безопасного хеширования). Мы успешно протестировали **AOPR** на документах, зашифрованных с помощью следующих CSP:

Microsoft® Base Cryptographic Provider
Microsoft® Base DSS and Diffie-Hellman Cryptographic Provider
Microsoft® DH SChannel Cryptographic Provider
Microsoft® Enhanced Cryptographic Provider
Microsoft® Enhanced DSS and Diffie-Hellman Cryptographic Provider
Microsoft® RSA SChannel Cryptographic Provider
Microsoft® Strong Cryptographic Provider
Microsoft® Enhanced RSA and AES Cryptographic Provider (Prototype)

Для документов, использующих этот метод шифрования, **AOPR** может запускать те же атаки, что и для [Office 97/2000](#)^[74], то есть атаки методом полного перебора и по словарю. Если был обнаружен неизвестный CSP (отличный от указанного выше), **AOPR** все еще может восстановить пароль, если CSP соответствует спецификации Microsoft.

Microsoft® PowerPoint® XP и более поздние версии используют исключительно метод шифрования «Криптопровайдер».

Пароль на открытие файла Microsoft OneNote

Microsoft® OneNote® 2003 с пакетом обновления 1 (SP1) и новее позволяет защищать заметки паролем. Этот пароль надежен и не может быть восстановлен мгновенно.

AOPR может восстановить этот пароль с помощью перебора и словарных [атак](#)^[70].

Пароль на открытие файла Microsoft Money 2002+

Этот пароль поддерживается в Microsoft® Money 2002 и более новых версиях. База данных Money зашифрована с использованием алгоритма шифрования RC4. В базе данных хранится только хэш пароля для проверки пароля. Следовательно, этот пароль нельзя восстановить мгновенно.

AOPR может использовать [атаки](#)^[70] по словарю и методом полного перебора. В Microsoft Money 2002-2005 все символы пароля начинаются с заглавной буквы (например, «Аааа» и «АААА» рассматриваются как один и тот же пароль). Поэтому диапазон паролей не может содержать маленькие латинские символы, а набор символов «a - z» отключен. В Money 2006 при использовании аутентификации MS Passport пароль может содержать любые символы.

Money 2003 и более поздние версии могут использовать аутентификацию Microsoft® Passport для открытия базы данных. В этом случае пароль для входа в MS Passport используется в качестве пароля для базы данных. Money 2003 позволяет хранить пароли MS Passport локально. [Эти пароли можно восстановить в AOPR](#)^[69].

Пароль на открытие файла Office 2007 и более поздних версий

Microsoft Office 2007 использует значительно улучшенную систему защиты паролем. Следующие приложения могут установить пароль для открытия файла, который используется для шифрования документа: Microsoft Word, Excel, PowerPoint и Access.

Эти программы используют шифрование AES и хеширование SHA-1. Проверка пароля сделана намеренно медленной, что позволяет восстанавливать только короткие и простые пароли. Microsoft Office 2010 удвоил количество итераций хеширования SHA-1, что в два раза снизило скорость восстановления.

В Office 2013 хеширование SHA-1 заменено на SHA-512, который является более сложным и медленным алгоритмом хеширования.

Для взлома паролей Office 2007+ мы рекомендуем использовать ускорение с помощью графических процессоров. Использование современных видеокарт значительно увеличивает скорость атак. Для взлома более длинных и сложных паролей рассмотрите распределенные атаки с помощью Elcomsoft Distributed Password Recovery.

4.6.5.2 Слабые пароли

Пароль на открытие файла Word/Excel (слабое шифрование)

Этот тип шифрования используется в следующих приложениях:

- Word®/Excel® 95 и более ранние версии
- Word®/Excel® 97/2000 с французскими региональными настройками
- Word®/Excel® XP и новее, выбрав опцию «Слабое шифрование (XOR)».

Когда этот пароль установлен, документ шифруется слабым алгоритмом (XOR). Это позволяет мгновенно восстановить пароль. [Выберите документ](#)^[66] в **AOPR**, и пароль будет немедленно [отображен](#)^[68].

Visual Basic for Applications (VBA)

Microsoft® Visual Basic для приложений (VBA) позволяет использовать пароль для защиты исходного кода. Когда этот пароль установлен, запись пароля добавляется в хранилище макросов VBA. Однако исходный код не зашифрован. VBA 5 шифрует исходный пароль с помощью XOR, а VBA 6 использует SHA-1 для хеширования пароля.

AOPR обнаруживает пароли VBA 5 и позволяет изменять или удалять пароли VBA 6.

Профессиональная версия AOPR предлагает функцию [VBA Backdoor](#)^[69], которая позволяет обходить проверку пароля VBA в любом приложении.

Microsoft Access

Общий пароль к базе данных Access, информация о владельце

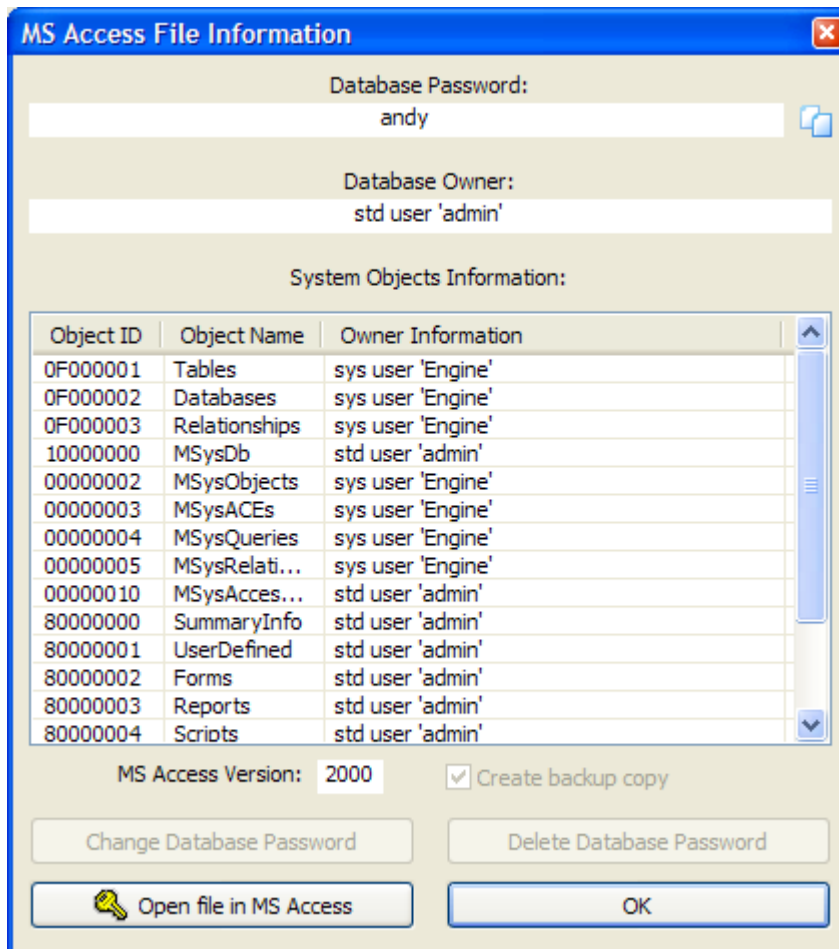
Общий пароль к базе данных Microsoft Access® может быть включен для предотвращения несанкционированного доступа к базе данных. В устаревших версиях Microsoft Access® файл был зашифрован с помощью слабого алгоритма (XOR) и мог быть немедленно восстановлен с помощью AOPR. Access 2007 улучшает защиту паролем, и пароль базы данных может быть восстановлен с помощью атаки по словарю или методом полного перебора.

При установках [защиты на уровне пользователя](#)⁷⁹ пользователи вводят пароль при запуске Microsoft® Access®. Затем Access® считывает файл информации о рабочей группе, в котором каждый пользователь идентифицируется уникальным идентификационным кодом. В информационном файле рабочей группы пользователи идентифицируются как авторизованные отдельные пользователи и как члены определенных групп по их личному идентификатору и паролю.

Для базы данных Access® (*.mdb) с защитой на уровне пользователя, программа показывает следующую информацию:

- версия Access®
- Общий пароль к базе данных
- Информация о владельце базы данных (имя и ID)
- Список объектов и их владельцев

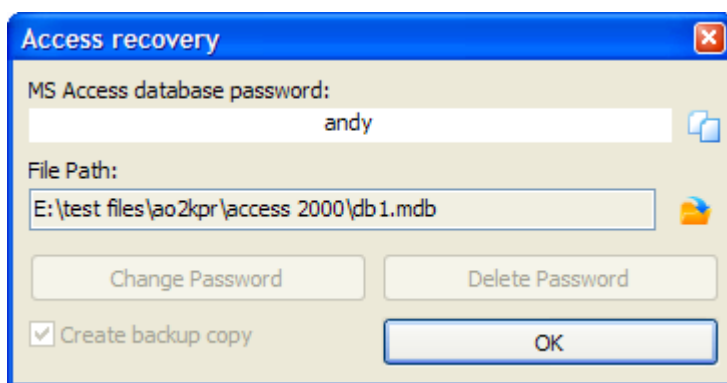
Например:



В большинстве случаев все, что вам нужно, это пароль базы данных, который отображается в верхней части этого окна. Примечание: Access® 2.0 поддерживает только [защиту на уровне пользователя](#)^[79], поэтому пароль базы данных всегда будет пустым для файлов Access® 2.0. Вы можете использовать пароль, указанный в **AOPR**; для файлов Access® 97 вы также можете изменить или удалить его с помощью соответствующих кнопок внизу.

Однако, если в базе данных включена защита на уровне пользователя и файл администрирования рабочей группы (*system.mda* или *system.mdw*) будет недоступен, вам также потребуется информация о владельце базы данных.

Владелец базы данных отображается только в **AOPR Professional**. Стандартная же версия показывает только пароль базы данных:



Чтобы получить доступ к файлу при отсутствии базы данных с защитой на уровне пользователя, выполните следующие действия:

- Запустите MS Access® (та же версия, в которой был создан файл, как показано в AOPR).
- Создайте новую базу данных или откройте существующую незащищенную.
- Перейдите в раздел «Настройка учетных записей» (обычно в меню «**Инструменты | Безопасность | Учетные записи пользователей и групп**»), затем щелкните вкладку «**Пользователи**».
- Создайте нового пользователя с именем, отображаемым в AOPR без кавычек, набрав это имя в раскрывающемся списке «**Имя**» и нажав «**Создать**». Access® откроет новое окно с двумя полями: **Имя** и **Персональный идентификатор**. Во втором поле введите идентификатор, отображаемый в **AOPR**, и нажмите **OK**.
- Закройте окно «**Учетные записи**», нажав **OK**, и выйдите из Access®.
- Запустите Access® из командной строки с параметром / user, то есть:

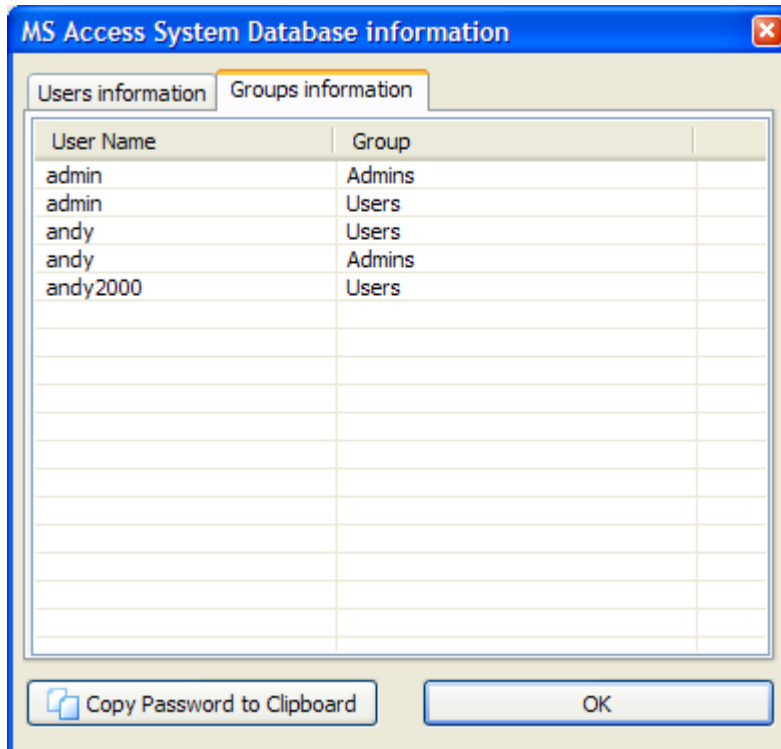
MSACCESS.EXE / пользователь

- Вам будет предложено ввести имя пользователя и пароль. Введите созданное имя и оставьте пароль пустым.
- Теперь откройте защищенную базу данных, и вы должны иметь все необходимые разрешения как владелец базы данных.

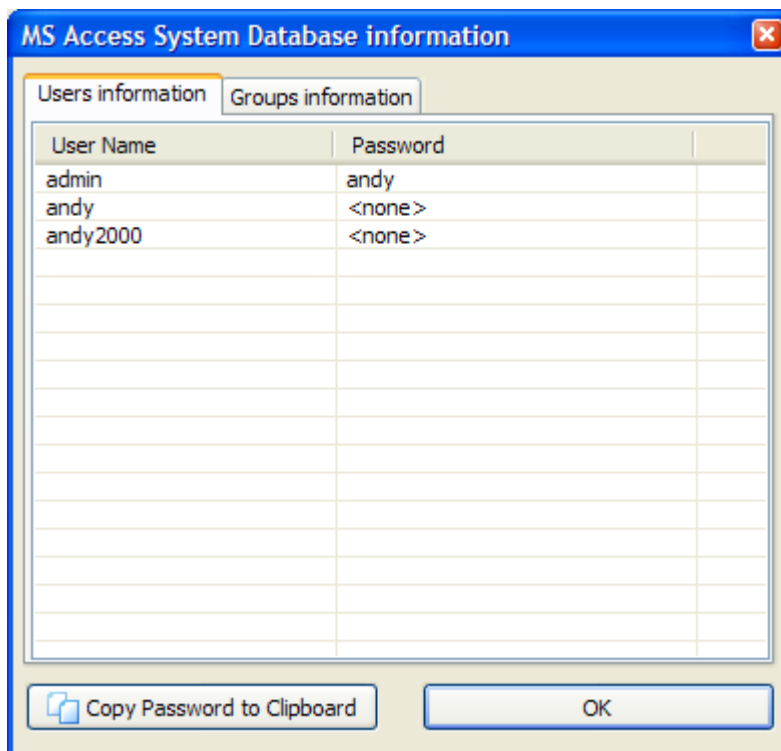
Пользовательские пароли Access

AOPR мгновенно восстанавливает пользовательские пароли Access.

Для баз данных System Access® (обычно *system.mda* или *system.mdw*) программа отображает окно с двумя вкладками: **информация о группах/groups information** и **информация о пользователях/users information**. Первая вкладка показывает, к каким группам принадлежат пользователи:



Вторая отображает пароли для всех пользователей.:



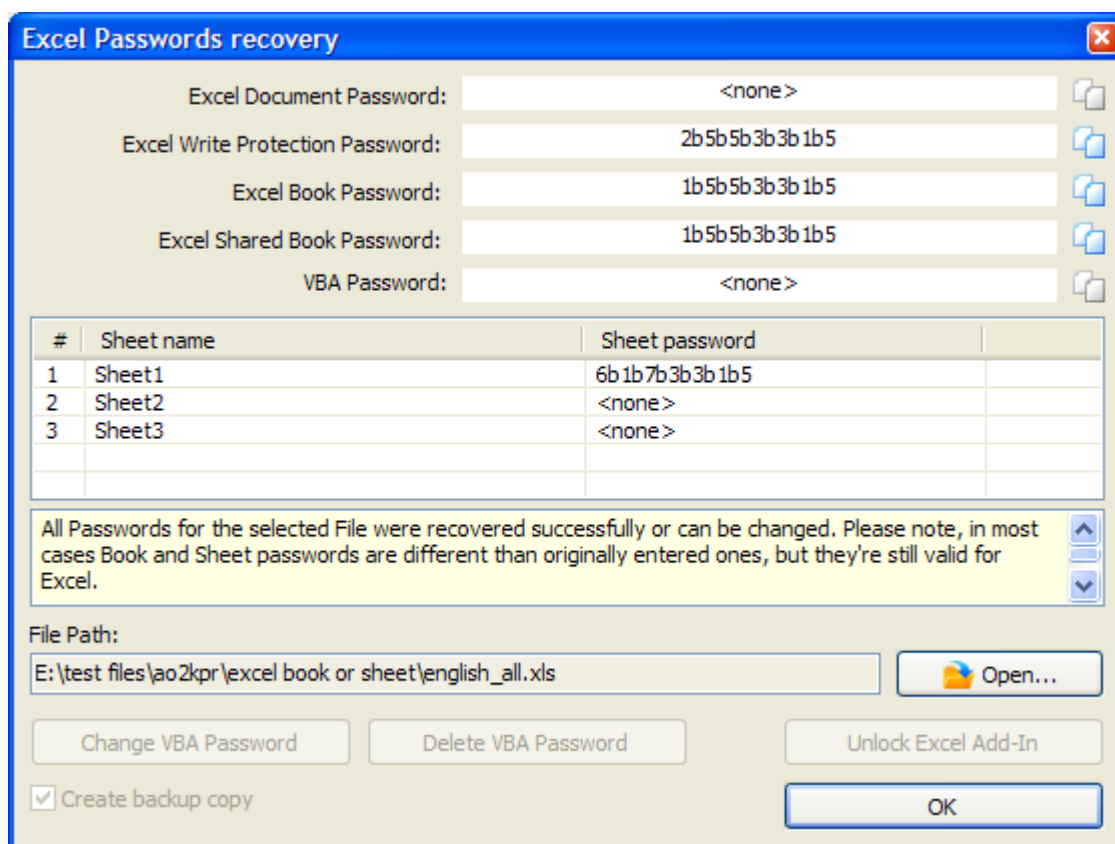
Microsoft Excel

Документ Excel - все пароли кроме пароля на открытие

Документы Microsoft® Excel® можно защитить с помощью следующих типов паролей:

- Пароль на открытие (может быть [стойким](#)^[74] или [слабым](#)^[76])
- Пароль на изменения (пароль для защиты от записи)
- Пароль на книгу
- Общий пароль книги
- Пароль на лист
- [Пароль к VBA Project](#)^[76]

Все пароли Excel®, кроме [надежного пароля на открытие файла](#)^[74], восстанавливаются мгновенно. После открытия документа Excel® программа AOPR отобразит следующий диалог:



Обратите внимание, что некоторые из этих паролей могут отличаться от паролей, изначально установленных в Excel®. Однако Excel® примет эти пароли.

Вы также можете изменить или удалить пароли VBA и [разблокировать надстройку Excel \(XLA\)](#)^[82].

Защита надстроек Excel® (XLA)

Когда документ Excel® сохраняется как надстройка (.XLA), исходный код макроса VBA нельзя просмотреть или изменить. Эта защита реализуется путем установки флага XLA в документе Excel®. AOPR может сбросить этот флаг, и вы получите доступ к источнику макроса VBA. Надстройку XLA можно разблокировать в [диалоговом окне паролей Excel®](#).

Pocket Excel

Файлы **Pocket Excel®** (Windows® CE и Windows® Mobile) могут быть защищены паролем на открытие. Этот пароль хранится в файле и может быть мгновенно восстановлен. Для этого [откройте](#) его в **AOPR**.

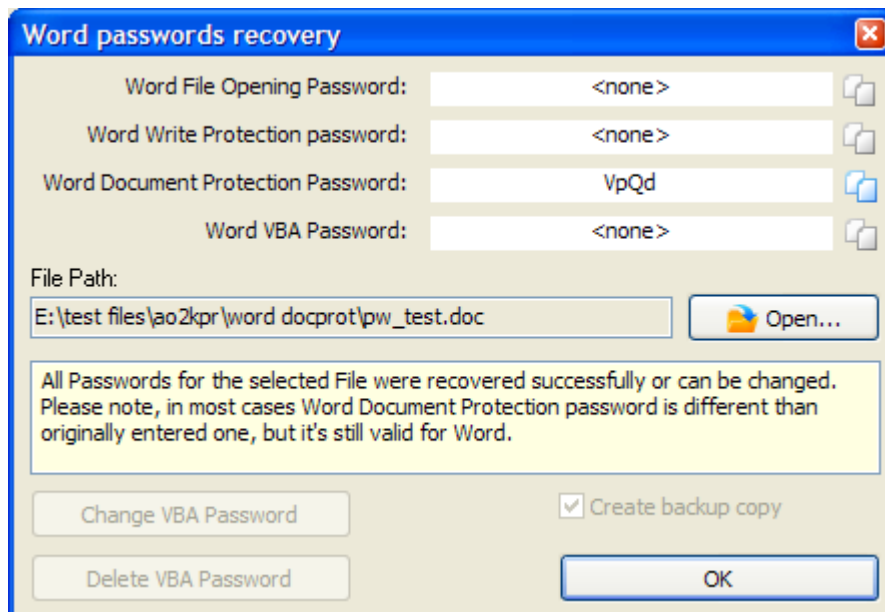
Microsoft Word

Документ Word® - все пароли, кроме пароля на открытие

Документы **Microsoft® Word®** можно защитить с помощью следующих типов паролей:

- Пароль на открытие ([сильный](#) или [слабый](#))
- Пароль на изменения (пароль для защиты от записи)
- Пароль для защиты документа
- [Пароль к проекту VBA](#)

Если выбрать документ Word® в **AOPR**, появляется следующий диалог:



Все пароли, кроме стойкого пароля на открытие файла, восстанавливаются мгновенно. Вы также можете изменить или удалить пароли VBA.

Microsoft Outlook

Пароль файла личного хранилища Outlook®

Microsoft® Outlook® позволяет защитить файл личного хранилища (PST) паролем. Хеш пароля хранится в заголовке файла; содержимое файла не зашифровано, а пароль мгновенно восстанавливается в **AOPR**.

Чтобы восстановить **пароли PST** для Outlook® 97, 98, 2000, 2002 / XP, 2003, 2007 и 2010, откройте файл PST в AOPR. Пароль будет немедленно восстановлен, отображен в окне сообщения и записан в окно журнала.

Обратите внимание, что в некоторых случаях пароль, восстановленный в **AOPR**, отличается от первоначально установленного. Это связано с алгоритмом шифрования, используемым в Outlook®, поскольку исходный пароль не сохраняется в файле. Обратите внимание, что Outlook® примет пароль, который отобразится в программе **AOPR**.

Пароли учетных записей электронной почты Outlook®

Microsoft® Outlook® может хранить пароли к учетным записям электронной почты, если установить параметр «**Сохранить пароль**» в свойствах учетной записи. Эти пароли хранятся в реестре Windows и могут быть расшифрованы в **AOPR**. Пароли учетной записи электронной почты восстанавливаются мгновенно. Обратите внимание, что пароль можно восстановить только в том случае, если он хранится локально в Outlook®. **Пароли, которые не хранятся на локальном компьютере, восстановить невозможно.**

[Подробнее о восстановлении учетных записей электронной почты Outlook® в AOPR](#)^[67].

Microsoft PowerPoint

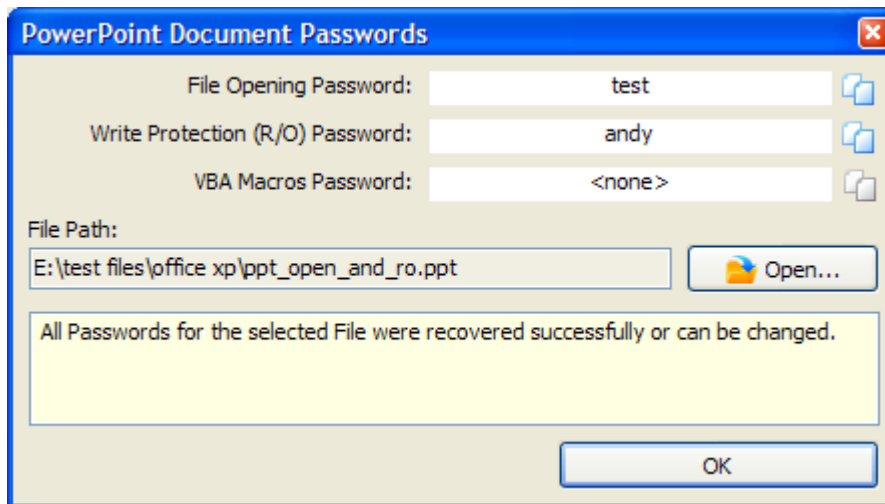
Версии Microsoft® PowerPoint® до PowerPoint® XP поддерживают только пароль к [VBA Project](#)^[76].

PowerPoint® XP и более поздние версии поддерживают следующие типы паролей:

- [Пароль на открытие](#)^[74]
- Пароль на изменения (Защита от записи)
- [Пароль к проекту VBA](#)^[76]

Пароль на открытие - это стойкий пароль, который можно восстановить [методом полного перебора или атаки по словарю](#)^[70]. [Подробнее об этом пароле.](#)^[74]

Пароль на изменения можно восстановить мгновенно. [Выберите документ](#)^[66] в **AOPR**, появится следующее диалоговое окно:



Вы можете скопировать пароль в буфер обмена и открыть файл в PowerPoint®.

Microsoft Money

Microsoft® Money от 3.x до 2000 позволяет установить пароль к базе данных. Этот пароль хранится в базе данных и может быть мгновенно восстановлен, если [открыть файл](#)^[66] в **AOPR**.

Пароль к базе данных **Microsoft® Money** 2002 и более новых версий нельзя восстановить мгновенно. [Подробнее об этом пароле.](#)^[75]

Microsoft Project

Microsoft® Project поддерживает следующие типы паролей:

- Пароль на открытие
- Пароль на изменения
- [Пароль к проекту VBA](#)^[76]

AOPR мгновенно восстанавливает эти пароли, за исключением пароля к VBA, который можно мгновенно изменить или удалить. Чтобы восстановить пароли MS Project, [откройте файл](#)^[66] в **AOPR**.

4.6.6 Устранение неполадок

4.6.6.1 Создание журнала отладки

Функция **журнала отладки/debug log** собирает информацию, необходимую нашей службе поддержки для выявления проблем в процессе восстановления пароля. Чтобы создать журнал отладки, сделайте следующее:

- Запустите AOPR
- Установите флажок **Включить параметры журнала отладки**
- Закройте AOPR и снова запустите

- Выполните действия, вызывающие проблему
- Закройте AOPR

Журнал отладки будет расположен в папке, указанной в поле «**Папка для файлов журнала/ Folder for Log Files**» в **Параметрах**. Имя файла будет «**aopr_debug_log.txt**». Отправьте этот файл в нашу [службу поддержки](#)^[65], и мы постараемся решить проблему.

4.6.7 Пробная версия AOPR и регистрация

4.6.7.1 Ограничения пробной версии

Пробная версия **Advanced Office Password Recovery** имеет следующие ограничения:

- Максимальная длина паролей, восстанавливаемых полным перебором, ограничена 4 символами.
- Пароли длиной более 4 символов, восстановленные с помощью словарной [атаки](#)^[70], не отображаются.
- Максимальная длина паролей, которые восстанавливаются мгновенно, ограничена 3 символами.
- Файл журнала не создается.
- [Функция VBA Backdoor](#)^[69] не доступна
- [Пароли VBA](#)^[76] не могут быть изменены или удалены
- Надстройки Excel® (XLA) не могут быть разблокированы
- [Информация о владельце базы данных Access®](#)^[77] не указывается
- Для восстановления пароля можно использовать только один графический процессор

Вы можете [приобрести полную версию](#)^[85] **Advanced Office Password Recovery**, чтобы снять эти ограничения.

4.6.7.2 Регистрация

Существует три версии **Advanced Office Password Recovery**: Home, Standard и Professional.

Дополнительные сведения о различиях между этими выпусками можно посмотреть [в списке поддерживаемых форматов файлов AOPR](#)^[63].

Вы можете оформить заказ онлайн, используя следующую форму:

<https://www.elcomsoft.ru/purchase/buy.php?product=aopr&ref=DOC>

4.7 Advanced PDF Password Recovery

4.7.1 Введение

Advanced PDF Password Recovery (APDFPR) способен разблокировать [PDF](#)-документы [Adobe Acrobat](#) и мгновенно снимает ограничения на редактирование, печать и копирование. Запатентованная технология **Thunder Tables (tm)** гарантирует восстановление **40-битных**

ключей менее чем за минуту. Для новейшего 256-битного шифрования доступно ускорение на GPU.

Мы предлагаем несколько версий продукта: для бизнеса, для государственных организаций и для простых пользователей.

Стандартная версия (Standard) - идеальный выбор, если у вас есть PDF-файл с наложенными ограничениями, такими как запрет на распечатку/запрет на редактирование данных или копирование данных в буфер обмена. Стандартная версия мгновенно снимет все ограничения и разблокирует защищенный PDF-файл.

Если вы не можете открыть запароленный PDF-файл, ваш выбор - версия Профессиональная (Professional). В нее входит весь функционал Стандартной версии, плюс - позволяет извлекать пароли «владельца» и «пользователя» с помощью брутфорса и словарных атак. Уникальная атака поиска ключа (Key Search) гарантирует восстановление PDF-документов, защищенных 40-битным шифрованием. Ускоренная на GPU и эффективно оптимизированная по скорости, эта атака может восстановить защищенные документы за считанные дни (при использовании на современном многоядерном ПК). Также эта версия позволяет удалить JScript-код, поля формы и цифровые подписи.

Корпоративная версия (Enterprise) еще больше расширяет возможности версии Professional, добавляя уникальную запатентованную технологию Thunder Tables, которая позволяет восстанавливать «пользовательские» пароли за минуту, а не за дни. Технология Thunder Tables использует предварительно вычисленные данные и поддерживает только 40-битное шифрование.

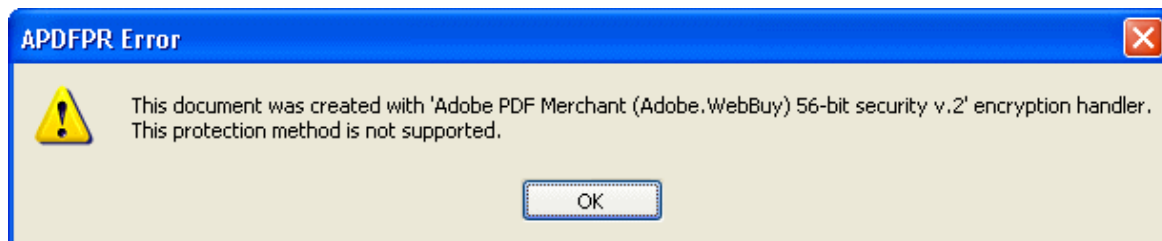
4.7.2 Системные требования

Требования

- Windows XP или выше
- Около 6 МБ дискового пространства
- Корпоративная версия: 4 ГБ дискового пространства (для Thunder Tables)

Ограничения

- PDF-файлы, защищенные с помощью [Digital Rights Management \(DRM\) technology](#) или сторонних плагинов, таких как [FileOpen](#), не могут быть расшифрованы. Если вы попытаетесь начать расшифровку такого файла, APDFPR выдаст сообщение об ошибке:



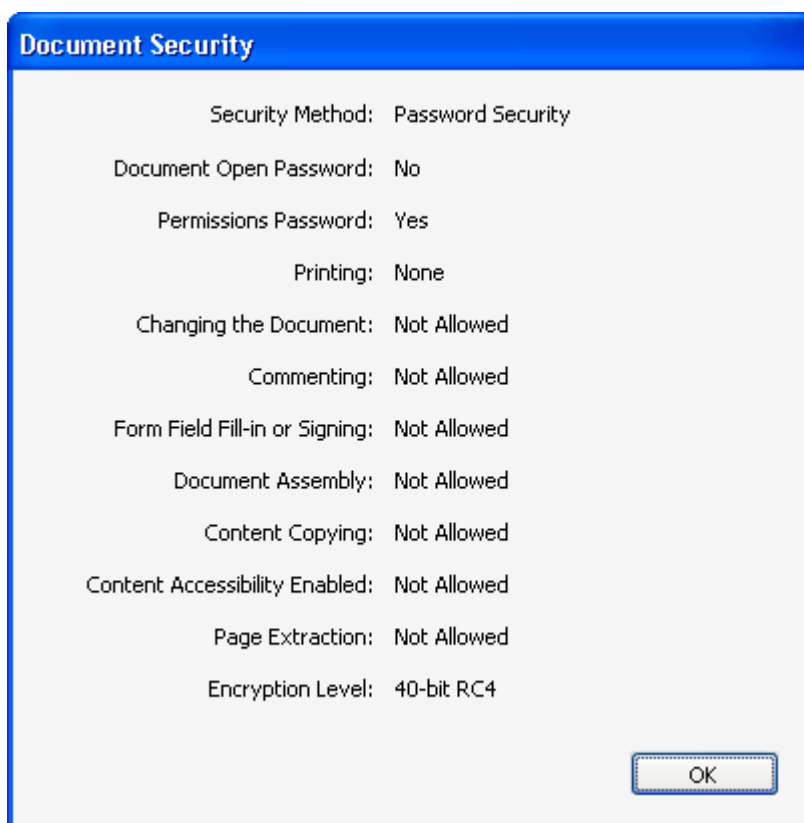
- Брутфорс атака эффективна только против коротких паролей, обычно до 7-8 символов. Восстановление более длинного пароля может занять месяцы или даже годы даже на очень быстром компьютере. В большинстве случаев атака по словарю помогает обнаружить пароль, но если пароль содержит комбинацию букв, цифр и специальных символов, его невозможно восстановить в разумные сроки.
- Если установлен только пароль «владельца» (owner), восстанавливать его не нужно, так как документ можно расшифровать **мгновенно**.
- Файлы, защищенные паролем «пользователя» (user) и 40-битным шифрованием, могут быть разблокированы с помощью атаки "Поиск ключа" - [Key search](#)^[92].
- Если у вас возникли проблемы с открытием поврежденного файла с помощью APDFPR, попробуйте открыть файл в Adobe Acrobat (необходима полная версия, а не приложение Reader) и сохранить копию, не внося никаких изменений. Затем APDFPR можно использовать с копией pdf-файла.

4.7.3 О программе

4.7.3.1 О PDF шифровании

[Adobe Acrobat](#) имеет два уровня защиты с помощью пароля.

Защита документов паролем, ограничивающим доступ, например: пароль «владельца» ("owner"), «безопасности» ("security") или «мастера» ("master") не влияет на возможность открытия и просмотра PDF-файла, но не позволяет пользователям изменять файл, печатать его, выделять текст и графические объекты, копировать элементы в буфер обмена, добавлять или изменять аннотаций, поля формы и т. д. Вы можете просмотреть ограничения в ПО от Adobe, используя Файл | Свойства|Безопасность|Показать подробности (File | Properties, Security, Show Details):



APDFPR может мгновенно снять эти ограничения, если пароль «пользователя» либо не установлен, либо известен.

Кроме того, есть еще «открытый» («пользовательский») пароль. Если он установлен, файл будет зашифрован с помощью надежного алгоритма. Его нельзя открыть, если неизвестен пароль или ключ шифрования. APDFPR может попытаться восстановить этот пароль с помощью атак по словарю и перебора. Кроме того, APDFPR позволяет атаковать пароль «владельца», поскольку дешифрование файла возможно с паролем «пользователя» или «владельца». Даже если оба пароля длинные и сложные, PDF-документы, созданные в устаревших версиях Adobe ПО, можно расшифровать с помощью [атаки по поиску ключа](#)^[92], которая пробует все возможные 40-битные ключи RC4. Это может занять часы или даже дни, но расшифровка **гарантирована**. Предварительно вычисленные хэш-таблицы, поставляемые с APDFPR Enterprise, сокращают время ожидания до нескольких минут.

Обратите внимание, что после сохранения файла в Adobe Acrobat и установки пароля «пользователя», для пароля «владельца» автоматически устанавливается то же значение (но его можно изменить вручную). PDF-файл не может иметь только пароль «пользователя», поэтому он всегда имеет либо пароль «владельца», либо пароли «владельца» и «пользователя» (которые могут быть одинаковыми или разными). Учтите это при выборе [Дополнительных параметров](#)^[94].

PDF-файлы можно защитить с помощью [Digital Rights Management \(DRM\)](#) или сторонних плагинов, таких как [FileOpen](#). APDFPR не поддерживает эти методы защиты.

Обратите внимание, что версии Acrobat с 5 по 8 могут создавать PDF-файлы с улучшенным уровнем безопасности: 56..128-битное RC4-шифрование или 128-битное AES-шифрование. Для

этих файлов защита «владельца» может быть восстановлена мгновенно (как для Adobe Acrobat 4.0 и более старых версий), но и доступны также брутфорс и словарные атаки (значительно медленнее). Атака "поиск по ключу" недоступна. Для файлов Acrobat 9 и более новых версий с 256-битным AES-шифрованием атака «поиском по ключу» недоступна, но скорость атаки полным перебором значительно выше.

Когда запускается атака полным перебором или словарная атака, APDFPR предоставляет дополнительную информацию о типе используемого обработчика безопасности (security handler); окно журнала может содержать следующую запись:

05.04.2002 13:05:51 - File "C:\My Documents\test.pdf" opened.

05.04.2002 13:06:14 - Handler: Acrobat Standard (Standard) 40-bit security v.1.

или

05.04.2002 13:05:51 - Handler: Acrobat Standard (Standard) 128-bit security v.2.

Файлы PDF (даже в незашифрованном виде) могут также содержать дополнительные объекты, такие как JavaScript-код, поля формы и цифровые подписи; иногда они используются для защиты документов. APDFPR также позволяет удалить их.

4.7.3.2 Выбор атаки

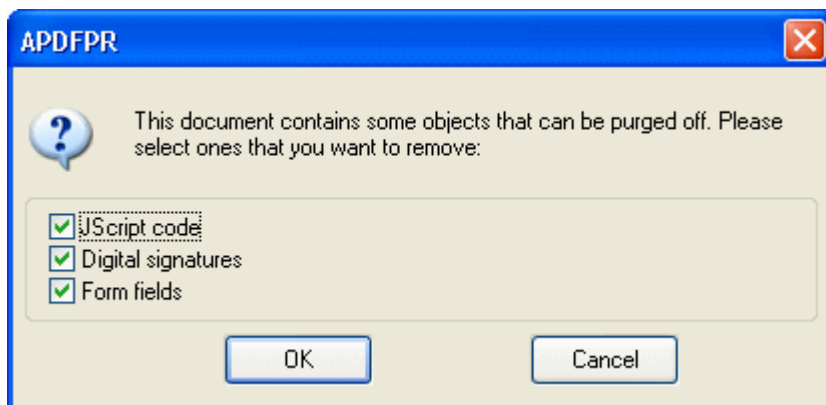
Зашифрованный PDF-файл

Вы можете открыть документ с помощью панели инструментов, меню или перетащив файл в главное окно.

Если [опция](#)^[93] запуска атаки на выбранный файл включена, программа может автоматически снимать ограничения, если используется только пароль для наложения ограничений. Если пароль «пользователя» установлен и неизвестен, выберите другие параметры и вручную запустите атаку.

Если файл зашифрован с помощью НЕстандартного метода, APDFPR отобразит сообщение об ошибке (этот вид шифрования не поддерживается) и сделает соответствующую запись в файл журнала. Если файл поврежден или не может быть открыт по какой-либо другой причине, будет показано соответствующее сообщение об ошибке. Для получения дополнительной информации см. главу [Сообщения об ошибках](#)^[100].

Если файл вообще не зашифрован, но содержит JavaScript-код, поля формы или цифровые подписи, программа предложит удалить любой из этих элементов:



Обратите внимание, что если файл защищен паролем и зашифрован, вам придется сначала его расшифровать, а затем снова загрузить файл в APDFPR, чтобы снять ограничения.

Типы атак

Доступны [Брутфорс \(brute-force\)](#)⁹⁰, атака по маске (Mask), [Атака по словарю \(Dictionary\)](#)⁹¹ и [Поиск ключа \(Key search\)](#)⁹².

Настройки брутфорса

Определяет наборы символов (кодировку) для использования при атаке на пароль: заглавные буквы, строчные буквы, цифры, специальные символы и пробел или все печатаемые символы (включая все перечисленное). Специальные символы следующие:

**!@#%&^&*()_+ -= <> ,./?[]{}~:;`'|" **

Кроме того, вы можете определить свой собственный набор символов (кодировку) с помощью флажка «Определено пользователем» ("User-defined"). Щелкните «Собственная кодировка...» (Custom charset...) и введите символы, которые будут использоваться для взлома пароля. Вы можете загружать и сохранять собственные наборы символов или комбинировать их с помощью кнопки «Добавить кодировку из файла...» (Add charset from file...).

Начать с пароля

Эта опция может помочь, если вы знаете первый (-е) символ (-ы) пароля. Например, если вы знаете, что пароль состоит из пяти (5) строчных букв (от «а» до «z»), а пароль начинается с «k», введите «каааа». Обратите внимание, что если во время атаки вы нажмете «Стоп» (Stop), программа занесет текущий пароль в окно «Начать с пароля» (Start from password). Этот пароль можно использовать позже, чтобы возобновить атаку с той же точки.

Обратите внимание, что программа проверяет пароли в соответствии со следующим порядком символов:

- ЗАГЛАВНЫЕ буквы: "A" .. "Z"
- Пробел
- Строчные буквы: "a" .. "z"
- Цифры: '0' .. '9'
- Специальные символы: !@#%&^&*()_+ -= <> ,./?[]{}~:;`'|" \

Вы также можете использовать поле "Закончить на" (End at), чтобы установить пароль, на котором APDFPR должен останавливаться. Это может быть полезно, если вы атакуете один и тот же документ на нескольких компьютерах и можете разделить диапазон паролей на части.

Маска пароля

Если вы знаете некоторые части пароля, вы можете указать маску, чтобы уменьшить общее количество проверяемых паролей.

Примечание: вы можете установить маску только для паролей фиксированной длины.

Пример: пароль состоит из 8 символов, начинается с «x» и заканчивается «99»; остальная часть пароля состоит из строчных или заглавных букв. Маска будет иметь вид "x?????99", а набор символов (кодировка) - все заглавные и все строчные буквы (All caps, All small). В приведенном выше примере знак "?" обозначает неизвестные символы.

Если вам нужно использовать "?" как часть пароля, вы можете выбрать другой символ маски, например, '#' или '*', и используйте шаблон маски «x#####?» (для символа маски '#') или «x*****?» (для символа маски '*'). Вы можете задать символ маски на странице [Дополнительные параметры](#)^[94].

Длина пароля

Вы можете указать минимальную и максимальную длину пароля.

Если минимальная и максимальная длина не совпадают, программа начинает сперва пробовать более короткие пароли. Например, если минимальная длина составляет 3 символа, а максимальная - 7 символов, программа сначала попробует все трехсимвольные пароли, затем все четырехзначные пароли и так далее. Текущая длина пароля, а также текущий пароль, средняя скорость, прошедшее и оставшееся время, а также общее и обработанное количество паролей отображаются в [Состоянии программы](#)^[95]. Вся эта информация, за исключением средней скорости и прошедшего времени, которые являются глобальными, связана только с текущей длиной пароля.

Опции словарной атаки

Сначала выберите файл словаря (списка слов). Вы также можете выбрать «Умные мутации» (Smart mutations) или «Попробовать все возможные комбинации верхнего и нижнего регистра» (Try all possible upper/lower case combinations). Например, предположим, что следующее слово в списке слов - «PASSWORD». При включенной второй опции программа будет пробовать все возможные комбинации регистров:

```
password
passworD
passwoRd
passwoRD
passwOrd
...
PASSWORDd
PASSWORD
```

Однако проверка всех этих комбинаций занимает много времени: в приведенном выше примере APDFPR будет проверять 2⁸ слов (т.е. 256) вместо одного. С помощью умных

мутаций вы можете исключить ряд редко встречающихся комбинаций; в результате будут проверены только следующие слова:

PASSword	(as is)
passWORD	(reversed)
password	(all lower case)
PASSWORD	(all upper case)
Password	(first uppercase, rest lowercase)
pASSWORD	(first lower case, rest uppercase)
PaSSWoRD	(elite: vowels in lc, others in uc)
pAsswOrd	(noelite)
PaSsWoRd	(alt/1)
pAsSwOrD	(alt/2)

Это дает всего 10 комбинаций на слово.

Опция Начать со строки # (Start line #) позволяет начать атаку с заданной строки в словаре; если вы прервете атаку, текущий номер строки будет записан и сохранен в файле проекта.

В APDFPR включено несколько словарей: english.dic (около 240 000 слов), немецкий и русский словари.

Поиск ключа

Для файлов PDF, созданных с помощью устаревших версий Adobe ПО, вы можете произвести атаку на ключ шифрования вместо атаки на пароль. Это работает только для 40-битных ключей и шифрования RC4.

В файлах PDF 1.2/1.3 (Acrobat 4.x или более ранней версии) длина ключа составляет 40 бит, а общее количество ключей составляет 2^{40} , или 1 099 511 627 776. Ключевое пространство разделено на 65 536 блоков, по 16 777 216 ключей на блок; на современных процессорах процесс восстановления занимает несколько часов.

Укажите начальный блок (Начать с поля ввода - Start from block input) и конечный блок (Закончить на блоке - End at block); значения могут быть от 0 до 65536. Во время атаки программа показывает номер текущего блока, прошедшее время, среднюю скорость (в ключах в секунду), количество уже обработанных ключей и общее количество ключей. Когда ключ найден, программа отображает его и предлагает расшифровать файл. Если вы уже знаете ключ, введите его в поле «Ключ документа» (Document key) и нажмите «Расшифровать» (Decrypt).

Версия Enterprise позволяет ускорить атаку за счет использования предварительно вычисленных хэш-таблиц. Нажмите Выбрать каталог хэшей пользователей (Select user hashes directory) и найдите папку, в которой расположены таблицы. Эта папка должна содержать следующие папки/файлы (Thundertables):

```
0\t00_117000.data
0\t00_117000.index
1\t01_117000.data
1\t01_117000.index
```

2\t02_I17000.data
2\t02_I17000.index
3\t03_I17000.data
3\t03_I17000.index
4\t04_I17000.data
4\t04_I17000.index
5\t05_I17000.data
5\t05_I17000.index
missing.bin

Мы рекомендуем хранить таблицы на SSD-диске или быстрой флешке. В этом случае атака займет от нескольких секунд до нескольких минут. Этот вариант обеспечивает гарантированное восстановление.

Эта атака не применима к PDF-файлам, созданным в Adobe Acrobat 5.0 и более поздних версиях, из-за улучшенного уровня безопасности с использованием ключей шифрования от 56 до 256 бит.

Автосохранение

APDFPR может периодически сохранять свое состояние. Вы можете установить время в минутах между сохранениями. Файл восстановления называется "~apdfpr.axt" (может быть изменен) и находится в той же папке, что и документ. Этот файл помогает восстановить атаку из последнего сохраненного состояния.

Другие параметры

Приоритет (Priority): фоновый (низкий) или высокий. Параметр «Низкий» ("Background") позволяет атаке использовать только неиспользуемые ресурсы ЦП. Параметр «Высокий» увеличивает приоритет процесса, но снижает производительность всех других приложений, работающих на вашем компьютере.

Свернуть в трей (Minimize to tray): если эта опция включена, программа сворачивается в трей на панели задач.

Логгировать в apdfpr.log (Log to apdfpr.log): при включении программа сохраняет всю информацию, отображаемую в окне статуса, в файл журнала.

Интервал обновления индикатора выполнения (Progress bar update interval): устанавливает интервал в миллисекундах между обновлением индикатора выполнения и окна состояния. По умолчанию это 500 мс.

Начать атаку при выборе файла (start attack on file select): когда эта опция включена (по умолчанию), программа анализирует файл сразу после того, как вы его открываете, и советует, что делать дальше.

Язык (Language): выбор языка пользовательского интерфейса из выпадающего списка.

Дополнительные параметры

Искать (Search for): любой пароль (Search for), пароль пользователя (User password) или пароль владельца (Owner password). Выберите этот параметр, чтобы указать программе, какой пароль следует искать (подробнее [О PDF шифровании](#)^[87]).

Возможные сценарии:

- Файл не защищен. Неважно, что вы выберете: при попытке запустить атаку программа это проигнорирует.
- У файла есть только пароль «владельца». Вы получите уведомление о том, что файл можно расшифровать мгновенно, но вы все равно можете искать исходный пароль. Выберите для поиска только пароль владельца (Owner password only); Вы также можете искать через параметр любой пароль (Any password), но скорость будет ниже.
- У вашего файла совпадают пароли "пользователя" и "владельца". Лучшее решение - искать только пароль пользователя, так как это более быстрая атака.
- Оба пароля - «пользователя» и «владельца» - заданы, но они разные. Вы можете искать любой из них или оба одновременно. Имейте в виду, что поиск пароля пользователя - самый быстрый, в то время как атака пароля владельца происходит почти в два раза медленнее. Обратите внимание, что есть вероятность, что один из этих паролей короче/проще другого. Мы рекомендуем сначала установить любой пароль (Any password) (и провести [атаку по словарю](#)^[91], а затем [брутфорс](#)^[90] 5 символов), а затем, если нет результатов, выбрать пароль пользователя (User password) в расширенном диапазоне брутфорса (например, до 7 символов).

Символ маски (Mask symbol): используется для атаки по [Маске](#)^[91].

Использовать код, оптимизированный для (Use code optimized for): (Процессоры без MMX / Intel PII/PIII/Celeron / AMD Athlon / Intel P4 SSE2 / Intel Core/Core2): помогает APDFPR определить оптимизированный для выбранного процессора код. *Обратите внимание, что программа обнаружит ваш процессор и автоматически выберет оптимизацию. Этот параметр отменяет автоматический выбор.*

Диспетчер GPU (GPU Manager): вызывает диспетчер графического процессора (отдельное приложение, устанавливаемое вместе с APDFPR), который позволяет указать, какие графические процессоры программа может использовать для запуска атаки для аппаратного ускорения. Список совместимых видеокарт доступен на сайте [NVIDIA](#). Обратите внимание, что ускорение графического процессора доступно только для файлов PDF с 256-битным шифрованием AES.

4.7.3.3 Сохранение и чтение настроек

Сохранение и чтение настроек

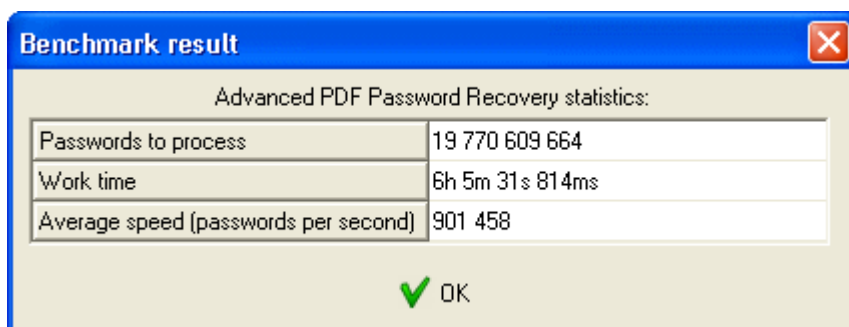
Вы можете сохранить текущие настройки APDFPR в файл AFR с помощью меню [Файл] | [Сохранить проект] или [Сохранить проект как ...] ([File] | [Save Project] или [Save Project as...]). Чтобы открыть проект, выберите [Файл] | [Открыть проект] ([File] | [Open Project]).

Кроме того, вы можете просто перетащить ранее сохраненный файл AFR в окно APDFPR.

4.7.3.4 Бенчмарки

Бенчмарк

Функция Бенчмарк (benchmark) помогает измерить скорость атак на вашу систему примерно за 10 секунд.



4.7.3.5 Получение результата

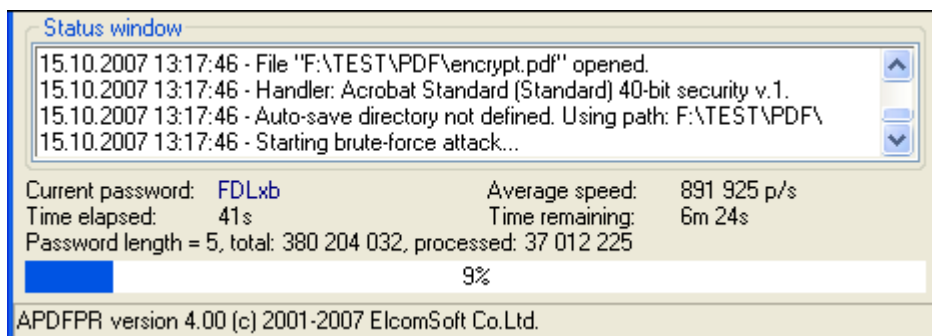
Процесс восстановления

Используйте кнопку Старт (Start) на панели инструментов или нажмите F9, чтобы начать атаку. [Состояние программы](#)^[95] будет отображаться с информацией о количестве уже использованных паролей, прошедшем и предполагаемом времени и т. д.

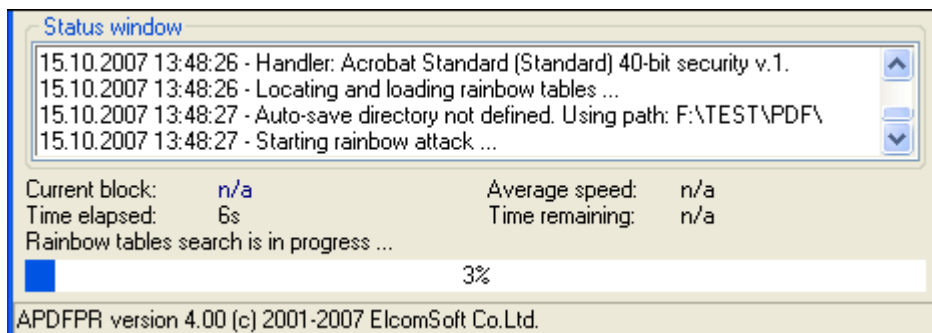
Вы можете в любой момент прервать процесс восстановления, нажав кнопку «Стоп» (Stop) или F10. Чтобы возобновить атаку или сохранить проект, обратитесь к разделам «[Начать с пароля](#)^[90]» и «[Сохранение и чтение настроек](#)^[94]».

Состояние программы

Состояние выполнения включает текущий пробуемый пароль, среднюю скорость, прошедшее время, оставшееся время, общее количество паролей для заданной длины и количество уже обработанных паролей:

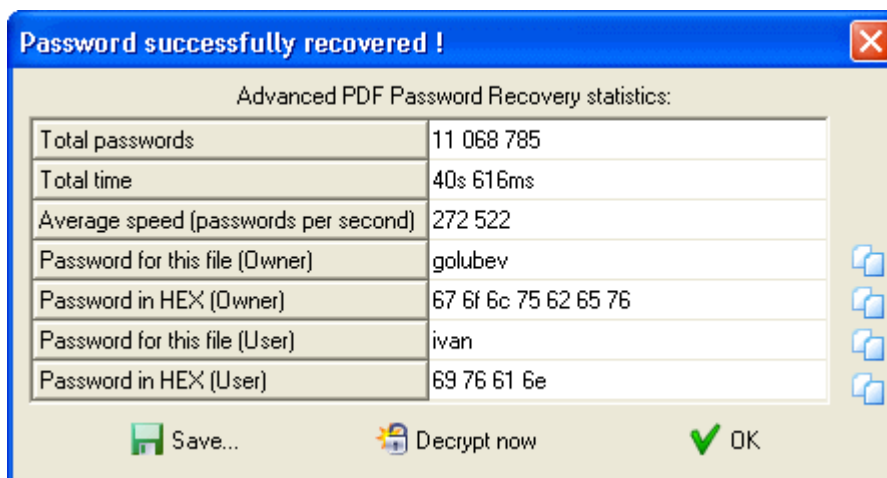


Для атаки с поиском ключа с использованием предварительно вычисленных хэш-таблиц отображается только прошедшее время (*примечание: эта атака обычно занимает не более нескольких минут*):



Результаты

После того, как пароль найден, отображается следующее окно:

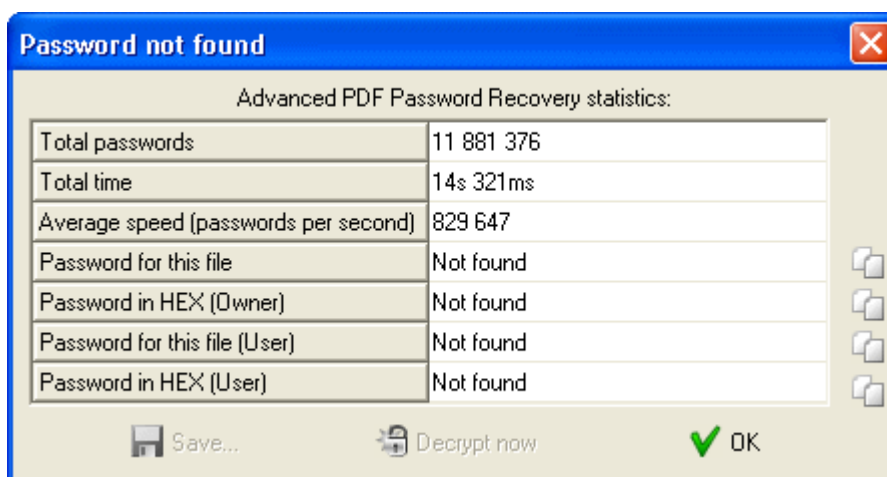


В последней строке отображается пароль в шестнадцатеричной форме, (для удобства, если пароль содержит мультязычные символы, не поддерживаемые вашей локализацией).

Нажмите маленькую кнопку справа от пароля, чтобы скопировать пароль в буфер обмена. Как вариант, вы можете сохранить пароль в файл.

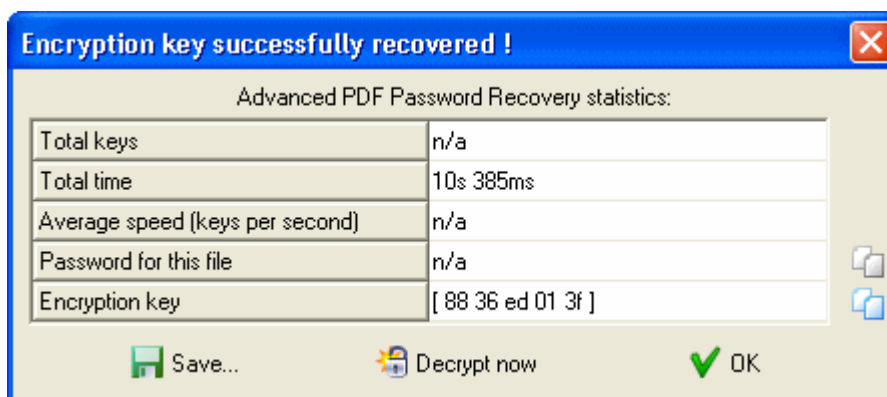
Программа также показывает тип пароля: «пользователь» или «владелец». Чтобы мгновенно расшифровать или сразу же снять защиту с файла с помощью восстановленного пароля, нажмите кнопку «Расшифровать сейчас» (Decrypt now).

Если пароль не был найден, вы увидите следующее окно:



Если атака была остановлена кнопкой «Стоп» (Stop), состояние атаки полным перебором сохраняется в поле «Начать с» (Start from) (для атаки с поиском ключа - в поле «Начать с блока» (Start block)). Вы можете снова нажать кнопку «Старт», чтобы возобновить атаку. Восстановление будет продолжено из последнего сохраненного состояния.

При атаке поиска ключа пароль не восстанавливается. Вместо этого программа показывает ключ шифрования файла, которого достаточно для снятия пароля (и, следовательно, защиты) с данного файла. Для этого нажмите кнопку «Расшифровать сейчас» (Decrypt now):



4.7.4 Советы

4.7.4.1 С чего начать

Если вы не имеете представления о шаблоне пароля или количестве символов пароля, сначала запустите атаку по словарю. Если результатов нет, попробуйте брутфорс до 7 символов или более (чтобы оценить скорость атаки, используйте функцию [Benchmark](#)^[95]).

Если атака полным перебором не удалась, попробуйте использовать другой словарь или отрегулируйте атаку полным перебором.

Если файл использует 40-битное шифрование, запустите атаку поиска по ключу - [Key search attack](#)^[92]. Использование вычисленных хэш-таблиц (APDFPR Enterprise) помогает значительно ускорить поиск ключей.

4.7.4.2 Командная строка

Вы можете запустить APDFPR с параметрами командной строки. Переключатели командной строки доступны для пакетной обработки и отдельных файлов.

Пакетная обработка

Для пакетной обработки используйте следующие параметры:

apdfpr.exe -batch src_path [dest_path] [options]

Параметр -batch является обязательным; в противном случае командная строка будет анализироваться иначе (см. ниже).

src_path	Путь к исходному файлу (-ам); подстановочные знаки разрешены.
dest_path	Путь назначения для расшифрованных файлов. Если не указано, используется тот же путь, что к исходному файлу.
-b	Создавать резервные копии расшифровываемых файлов. Игнорируется, если dest_path не равен src_path.
-p=xxx	Если программа встречает файл, заблокированный паролем «пользователя», она пытается расшифровать его, используя заданный пароль («xxx»).
-q	Тихий режим; игнорирует файлы с "пользовательскими" паролями, если пароль, указанный в опции -p, не совпадает или опция -p не используется.
-t	Сохраняет дату и время расшифрованного файла такими же, как и в оригинальном.
-l=log_path	Создает файл журнала («log_path»; должно быть имя файла).
-w	Бесшумная работа. Программа закрывается, когда все файлы обработаны; главное окно скрыто; возвращается последняя ошибка (или 0, если ошибок не было).

Параметры, заключенные в квадратные скобки, необязательны; единственный обязательный параметр - это исходный путь.

Если src_file начинается с символа «@», он рассматривается как имя файла, содержащего список обрабатываемых PDF-документов, по одному в каждой строке.

Если исходный или целевой путь содержит пробелы, его необходимо заключить в двойные кавычки.

Пароль может содержать специальные символы, но они должны быть представлены в шестнадцатеричной форме с префиксом «%». Например, пробел представлен как 20 в шестнадцатеричном формате, поэтому, если пароль - «my pass», соответствующая опция командной строки будет:

-p=my%20pass

Сам символ % заменяется на %25.

-w можно использовать, если вы вызываете APDFPR из другой программы. Когда все файлы, указанные в командной строке, будут обработаны, APDFPR завершится с соответствующим [кодом ошибки](#) ¹⁰⁰.

-l указывает программе создать файл журнала. Новые записи добавляются в существующий файл журнала. Если путь содержит пробелы, его следует заключить в двойные кавычки. Обратите внимание, что если вы укажете src_path как *.* , Файл журнала не будет создан в той же папке, потому что имя файла журнала также будет соответствовать заданной маске, создавая рекурсию. В этом случае используйте маску, например *.PDF, и/или создайте файл журнала в другой папке.

Примеры:

```
apdfpr.exe -batch doc??.pdf
```

```
apdfpr.exe -batch "c:\my documents\manuals\*.pdf" "c:\my documents\decrypted\" -q
```

```
apdfpr.exe -batch @list.txt -b -p=LockSmith -w -l="C:\Program Files\apdfpr_log.txt"
```

Восстановление пароля пользователя/владельца

Как правило, синтаксис следующий:

```
apdfpr.exe [switches] [pdf-filename]
```

Если у вас уже есть проект, вы можете использовать имя проекта вместо имени PDF-файла:

```
apdfpr.exe [switches] [afr-filename]
```

Переключатели обозначаются знаком «/» или «-». Значения, содержащие специальные символы (пробел, точка с запятой, косая черта или тире), должны быть заключены в одинарные или двойные кавычки.

Переключатели	Описание	Стандартные значения
/a:b m d	тип атаки (перебор, маска, словарь)	перебор
/pass:u o a	пароль для поиска (пароль пользователя, владельца, любой)	пароль пользователя
/nommx	не использовать инструкции MMX	отключено
/c:csdapa	набор символов (заглавные, маленькие, цифры, специальные, пробел, все)	заглавные
/u:chars	использовать собственную кодировку	
/sf:pass	начать с пароля	
/m:mask	маска	
/ms:C	символ маски	?
/min:N	минимальная длина пароля	1
/max:N	максимальная длина пароля	5
/d[:filename]	имя файла словаря	
/sm	умные мутации	отключено

/ac	пробовать все возможные комбинации верхнего/нижнего регистра	отключено
/sl:N	начать с строки N	0
/autosave:N	автосохранение каждые N минут; 0 означает отключено	5
/aname:filename	имя файла автосохранения	
/adir:dir	каталог автосохранения	
/idle	запуск с низким приоритетом	включено
/high	Запуск с высоким приоритетом	отключено
/dontstart	не запускайте атаку, только загрузить/задать параметры	
/minimize	свернуть программу после запуска атаки	
/smartexit[:filename]	по завершении атаки записать всю статистику, включая пароль (если он найден), в указанный файл (по умолчанию «cmdline_stats.txt») и выйти из программы.	отключено

Примеры:

apdfpr.exe /a:b /pass:u /c:cs /min:3 /max:7 /smartexit test.pdf

(атака полным перебором; пароль пользователя; строчные и заглавные буквы; длина от 3 до 7; сохранение и выход по завершении)

apdfpr.exe /a:b /u:12345abcde test.pdf

(атака полным перебором с набором символов "12345abcde"; длина: от 1 до 5)

apdfpr.exe /a:m /pass:a /c:d /m:june???? /sf:june1000 /high test.pdf

(атака по маске с маской вида "june????"; любой пароль; кодировка: только цифры; высокий приоритет)

apdfpr.exe /d:english.dic /sm /dontstart test.pdf

(атака по словарю; словарь: "english.dic"; умные мутации; преобразование слов из ANSI в OEM; не запускать)

Если параметром является аф-файл, программа загрузит настройки из этого файла, игнорируя другие настройки, указанные в командной строке, кроме /dontstart, /minimize и /smartexit, и запустит атаку.

4.7.4.3 Сообщения об ошибках

Если есть проблема с PDF-файлом, который вы пытаетесь расшифровать, APDFPR отображает сообщение об ошибке, например

Не удается открыть файл C:\My documents\report.pdf. Ошибка 105
(*Can't open file C:\My documents\report.pdf. Error 105*)

Таблица кодов ошибок:

	Код ошибки	Описание ошибки
--	------------	-----------------

0	PDFERR_OK	Нет ошибок
1	PDFERR_NO_STARTXREF	Нет ссылки на таблицу объектов
2	PDFERR_BAD_STARTXREF	Неверная ссылка на таблицу объектов
3	PDFERR_NOREF	Нет таблицы объектов или она пустая
4	PDFERR_BAD_XREF	Неверная таблица объектов
5	PDFERR_NO_TRAILER	Нет трейлера документа
6	PDFERR_BAD_TRAILER	Неправильный трейлер документа
7	PDFERR_NO_OBJ	Не найден объект
8	PDFERR_BAD_OBJ	Неверный формат объекта
9	PDFERR_NO_ENDOBJ	Не найден конец объекта
10	PDFERR_UNEXPECTED_LEX	Неожиданная лексема
11	PDFERR_NAME_EXPECTED	Нет имени
12	PDFERR_NO_TRAILER_DICT	Нет трейлера словаря
13	PDFERR_NO_STREAM_DICT	Нет потокового словаря
14	PDFERR_NO_STREAM_LEN	Не задана длина потока
15	PDFERR_BAD_STREAM_LEN	Неверный формат длины потока
16	PDFERR_NO_ENDSTREAM	Не найден конец потока
20	PDFERR_NO_LEX	Лексема не найдена
21	PDFERR_UNK_LEX	Неизвестная лексема
30	PDFERR_BAD_NUMBER	Неверный формат числа
31	PDFERR_BAD_STRING	Неверный формат строки
32	PDFERR_BAD_HEXSTR	Недопустимый формат шестнадцатеричной строки.
33	PDFERR_BAD_NAME	Неверный формат имени
34	PDFERR_BAD_KEYWORD	Неверный формат ключевого слова
35	PDFERR_UNK_KEYWORD	Неизвестное ключевое слово
101	PDFERR_ALREADY_OPENED	Документ уже загружен
102	PDFERR_CANT_OPEN	Невозможно открыть документ
103	PDFERR_CANT_CREATE_MAP	Невозможно сопоставить файл
104	PDFERR_CANT_MAP_VIEW	Невозможно просмотреть карту файлов
105	PDFERR_NO_HEADER	Нет заголовка PDF-файла
1001	PDFERR_NO_ENCRYPT	Документ не зашифрован
1002	PDFERR_NO_PDEF	Документ не загружен
1003	PDFERR_BAD_REF	Неверная ссылка на объект шифрования (Encryption Object)

1004		PDFERR_BAD_OBJ	Неверный или недействительный объект шифрования (Encryption Object)
1005		PDFERR_WRONG_FILTER	Неподдерживаемый объект шифрования (Encryption Object)
1006		PDFERR_WRONG_VER	Неподдерживаемая версия шифрования (Unsupported Encryption Version)
1007		PDFERR_WRONG_REV	Неподдерживаемая версия шифрования (Unsupported Encryption Revision)
1008		PDFERR_WRONG_OWNER	Неверный формат Ключа Владельца (OwnerKey)
1009		PDFERR_WRONG_USER	Неверный формат Ключа Пользователя (UserKey)
1010		PDFERR_WRONG_PERM	Неверный формат разрешений
1011		PDFERR_NO_ID	Не удастся найти DocumentID
1012		PDFERR_BAD_ID	Неверный формат DocumentID

4.8 Advanced Sage Password Recovery

4.8.1 Введение

Advanced Sage Password Recovery используется для:

1. Нахождения паролем пользователей и администраторов в Sage PeachTree Accounting, обеспечивая гарантированный мгновенный доступ к защищенному паролем АСТ! документу. Advanced Sage Password Recovery работает локально и удаленно и не требует локального доступа для восстановления пароля. Пользователи могут запускать Advanced Sage Password Recovery с любого компьютера в той же сети с доступом к защищенной паролем удаленной базе данных, чтобы мгновенно разблокировать пароль.
2. Получения доступа к заблокированным базам данных Sage PeachTree Accounting, мгновенно вытаскивая пароли пользователей и администраторов. Advanced Sage Password Recovery отображает все пароли пользователей и администраторов во всех версиях Sage PeachTree Accounting, независимо от длины и сложности паролей. Пароли предоставляются в виде обычного текста **мгновенно**. Программа также поддерживает учетные записи Sage 50, Sage Instant Accounts и Sage Simply Accounting.
3. Восстановления или замены пароля, защищающего файлы BLB, MUD и ADF/PAD, созданные с помощью АСТ! (локально или удаленно). Advanced Sage Password Recovery мгновенно обнаруживает паролик документам всех версий АСТ! включая последнюю версию (v22). Также есть возможность смены роли учетных записей пользователей с "режима ограниченного доступа" до администратора в АСТ! БД.
4. Получения мгновенного доступа к содержимому защищенных паролем документов АСТ! (*гарантировано!*). Advanced Sage Password Recovery мгновенно отображает пароли в виде простого текста, независимо от их длины, сложности или кодировки. Никаких времязатратных атак или дополнительных настроек не требуется! Просто откройте документ с помощью Advanced Sage Password Recovery, и вы сможете сбросить или отобразить пароль в ту же секунду!

4.8.2 О программе

4.8.2.1 Системные требования

- Windows 7 или выше

4.8.2.2 Восстановление паролей для АСТ!

Чтобы восстановить пароли к файлам, созданным в более старых версиях АСТ!, нажмите Открыть файл... (Open file...) и выберите Symantec АСТ!, затем найдите файлы *.blb или *.mud. Или перетащите АСТ!-файл из проводника Windows в окно ASAPR. Программа выведет список пользователей с правами доступа, а также их пароли и роли/уровень безопасности (например, Administrator, Standard, Manager, Browse, Restricted). Вы можете скопировать или сохранить пароль или использовать кнопку «Изменить уровень» (Change Level), чтобы изменить уровень безопасности для выбранного пользователя.

АСТ! 2005..2019 (от [Best Software/Sage/Swiftpage](#)) основан на Microsoft SQL Server Engine и зашифрован; для него пароли невозможно восстановить мгновенно. Однако их можно изменить или удалить. ASAPR предоставляет два способа сделать это: через сам АСТ! (через драйверы MSSQL ODBC, используемые АСТ!) и напрямую. Чтобы использовать первый метод, у вас на локальном ПК должна быть установлена соответствующая версия АСТ!, при этом к файлу *.adf можно получить доступ удаленно; второй способ работает даже без АСТ!, но не позволяет изменять роли пользователей.

При первом способе нажмите Открыть файл... (Open file...), выберите АСТ! 2005-2019 ODBC и найдите файл *.adf (база данных АСТ!) Или файл *.rad (информация о базе данных АСТ!, - может находиться на другом компьютере в локальной сети). ASAPR выдаст список пользователей с их ролями. Выделите пользователя, для которого нужно изменить пароль, нажмите «Изменить пароль» (Change password) и введите новый пароль для этого пользователя (используйте пустой пароль, чтобы снять защиту). Вы также можете изменить роль выбранного пользователя.

Если вы собираетесь работать с БД АСТ! НЕ на том же компьютере, на котором база данных была открыта в последний раз, мы рекомендуем открыть его в АСТ! на этом ПК прежде чем продолжить. Когда АСТ! запросит пароль, нажмите Отмена (Cancel), - эти действия позволят АСТ! внести изменения в файлы конфигурации. После этого откройте базу данных в ASAPR, чтобы изменить пароль (пароли). Если вы не выполните эти шаги, восстановление может работать некорректно.

Второй способ: выберите АСТ! 2005-2019 прямо из меню и найдите файл *.adf (база данных АСТ!). Если этот файл зашифрован именно с АСТ!, ASAPR предложит остановить службу SQL; в противном случае файл не будет доступен/разблокирован. Последующие шаги аналогичны первому способу, но вы не сможете выбрать новый пароль; вместо этого новый пароль сгенерируется автоматически.

Также обратите внимание, что если вы работаете с АСТ! 2005..2019 и измените пароль для любого пользователя, новые пароли всегда переведутся в нижний регистр для совместимости с АСТ! 2005 (где пароли не чувствительны к регистру). Кроме того, после смены пароля АСТ! примет его при первом входе в АСТ! с новым паролем, но может попросить изменить его в соответствии с политикой паролей.

АСТ! может сохранить пароль в системном реестре. ASAPR имеет возможность извлечь и расшифровать его с помощью команды Проверить реестр (Check Registry). Если последний пароль был сохранен, он будет найден и отображен.

4.8.2.3 Восстановление паролей для PeachTree/Accounting

Нажмите Открыть файл... (Open file...) и выберите один из следующих пунктов в зависимости от продукта:

- 50 Accounting (Peachtree)
- 50 Accounts
- 50 Accounting Canadian Edition (Simply Accounting)

Для Peachtree найдите PERMISS.DAT из БД PeachTree, для которой вы хотите восстановить пароль. Будет показан список имен пользователей и их паролей.

Для учетных записей Sage 50 (ранее Sage Line 50) и ее упрощенной версии Sage Instant Accounts восстанавливается только пароль для встроенного пользователя MANAGER. Как только вы войдете в систему как этот пользователь (MANAGER), вы сможете просматривать или изменять пароли для всех других пользователей. Найдите SETUP.DTA, расположенный в соответствующей папке; пароль будет восстановлен мгновенно.

Для Sage Simply Accounting восстанавливаются все пароли пользователей. Для версии 2008 и новее пароли хранятся в файле с именем «ibdata1»; в более старых версиях для этой цели используются файлы *.SDW. Найдите файл соответствующий номеру версии, и вам мгновенно будут показаны пароли для всех пользователей.

4.8.2.4 Другие продукты Sage

Для Sage 50cloud Accounts (ранее Sage Line 50, 50 Accounts) и его упрощенной версии, Sage Instant Accounts восстанавливаются только MANAGER-пароли. Войдите в систему как MANAGER, чтобы просмотреть или изменить пароли для всех других пользователей. Нажмите "Открыть файл..." (Open file..) и выберите 50 учетных записей 2004..2019 (50 Accounts 2004..2019), затем найдите файл SETUP.DTA, расположенный в соответствующей папке; пароль будет восстановлен мгновенно.

Для Sage Simply Accounting восстанавливаются все пароли пользователей. Для версий с 2008 по 2011 пароли хранятся в «ibdata1», тогда как в более старых версиях для этой цели используются файлы *.SDW. Нажмите "Открыть файл..." (Open file..) и выберите 50 Accounting (Peachtree) 2002..2021, затем найдите один из файлов, упомянутых выше, в соответствии с версией. Вам будут показаны пароли для всех пользователей.

4.9 Advanced SQL Password Recovery

4.9.1 Введение

Advanced SQL Password Recovery может изменить пароль от баз данных Microsoft SQL Server 2000-2019 для любого пользователя или администратора, что позволяет получить гарантированный мгновенный доступ к защищенным паролем базам данных SQL Server. Advanced SQL Password Recovery работает как с установленным SQL Server, так и без него. Он обращается к файлу master.mdf напрямую, независимо от того, запущен или установлен SQL Server.

Advanced SQL Password Recovery предлагает удобную работу - фактически одним щелчком мыши и без изменения конфигурации или дополнительных настроек. Если у вас запущен MS SQL, Advanced SQL Password Recovery автоматически обнаружит и остановит службу. В том числе если у вас есть несколько экземпляров MS SQL Server - он также остановит службу.

Advanced SQL Password Recovery полностью безопасен для ваших файлов. Он автоматически создает резервную копию вашей исходной базы данных. Независимо от длины и сложности паролей Advanced SQL Password Recovery может мгновенно заменить или сбросить эти пароли. Никаких длительных атак и дополнительных настроек! Advanced SQL Password Recovery легко заменит пароли на любом языке и в любой кодировке.

Данная программа, на которую вам предоставлена лицензия, соответствует законодательству и является абсолютно легальной. Используя ее, вы ничего не нарушаете при условии, что вы являетесь законным владельцем всех файлов или данных, которые вы собираетесь восстановить с помощью нашего программного обеспечения, или имеете разрешение законного владельца на выполнение этих действий. Вы несете исключительную ответственность за любое незаконное использование нашего программного обеспечения. Соответственно, вы подтверждаете, что имеете законное право на доступ ко всем данным, информации и файлам, которые были скрыты.

Вы также подтверждаете, что восстановленные данные, пароли и/или файлы не будут использоваться в каких-либо незаконных целях. Имейте в виду, что восстановление пароля и последующее дешифрование данных из незаконно полученных файлов может представлять собой кражу или другое противоправное действие и может привести к вашему гражданскому и (или) уголовному преследованию.

4.9.2 О программе

4.9.2.1 Системные требования

- Windows 7 и выше

4.9.2.2 Работа с ASQLPR

Microsoft SQL Server Engine использует надежное шифрование, потому пароли не могут быть восстановлены мгновенно. Однако их можно тут же изменить или удалить. Нажмите "Открыть файл..." (Open file...) и найдите файл с именем master.mdf. ASQLPR покажет список пользователей; выделите пользователя, для которого хотите изменить пароль, нажмите «Изменить пароль» (Change password) и введите новый. Ввод пустой строки удаляет пароль.

Важно: MSSQL может использовать два разных режима аутентификации, которые можно выбрать во время установки: режим аутентификации Windows и смешанный режим. Режим Windows аутентификации включает Windows-аутентификацию и отключает аутентификацию со стороны SQL сервера. Смешанный режим включает как аутентификацию Windows, так и аутентификацию SQL Сервера. При использовании аутентификации SQL Сервер в SQL Server создаются учетные записи, не основанные на аккаунтах в Windows. Имя пользователя, и пароль создаются с помощью SQL Server и хранятся в нем же. Пользователи, подключающиеся с использованием аутентификации SQL Server, должны предоставлять свои учетные данные (логин и пароль) при каждом подключении. Обратите внимание, что ASQLPR поддерживает только базы данных, использующие смешанный режим, то есть аутентификацию SQL Server.

4.10 Advanced WordPerfect Office Password Recovery

4.10.1 Введение

Advanced WordPerfect Office Password Recovery (AWOPR) обеспечивает гарантированное восстановление пароля, благодаря быстрому нахождению паролей к документам, созданным с помощью любой версии Corel WordPerfect Office (до Office X5), а также паролей к учетным записям Corel WordPerfect Lightning. Инструмент может **мгновенно** находить пароли любой длины и сложности для документов WordPerfect, Quattro Pro и Paradox.

Corel защищает документы WordPerfect Office с помощью пароля, но не предлагает инструментов для восстановления заблокированных документов, если вы потеряете или забудете пароль. Advanced WordPerfect Office Password Recovery создан для пользователей Corel WordPerfect, предоставляя удобный инструмент для восстановления документов и учетных записей, защищенных паролем.

4.10.2 Системные требования

- Windows Windows XP или выше

4.10.3 Как работать с AWOPR

Чтобы разблокировать документ, откройте его в AWOPR. Вы также можете перетащить файл в главное окно. Для поддерживаемых типов файлов пароль будет отображаться **мгновенно**.

WordPerfect

Для файлов WordPerfect 5.x пароль восстанавливается мгновенно, если он не содержит символов, отличных от символов американской раскладки. Если это так, пароль как таковой не может быть восстановлен. Но вместо этого вы можете мгновенно расшифровать защищенный файл.

Для файлов WordPerfect 6.x..13 поддерживаются два режима защиты: стандартный и расширенный. Восстановление двухэтапное. На первом этапе инструмент находит требуемые ключи. На втором этапе он пытается восстановить исходный пароль (это может занять несколько секунд или минут в зависимости от набора символов). Поддерживаются следующие наборы символов (как определено WordPerfect): ASCII, "мультинациональный", кириллица, греческий и иврит (AWOPR пробует их последовательно один за другим). Если пароль не удалось найти, вы можете вместо этого расшифровать сам файл. Хотя восстановление гарантировано, поиск ключа может занять от нескольких минут до нескольких часов. Если вы прервете атаку, вы сможете возобновить ее с последнего автоматически сохраненного состояния.

Для режима расширенного шифрования (версии с 6.x по X5/15) AWOPR может расшифровывать пароли любой длины, содержащие любые символы из наборов символов, упомянутых выше, и в любой комбинации. Восстановление большинства паролей происходит практически **мгновенно**. Однако, если пароль очень длинный и содержит символы из разных наборов символов, процесс восстановления может занять до нескольких минут.

Paradox

В большинстве случаев AWOPR создает 8-значный пароль «коллизии» ('collision'), который будет отличаться от заданного пользователем пароля в документе Paradox. Этот пароль, даже если он отличается от оригинала, успешно разблокирует БД.

Восстановление происходит мгновенно. В некоторых редких случаях атака может длиться несколько секунд.

QuattroPro

Пароли QuattroPro восстанавливаются мгновенно независимо от версии QuattroPro. Если восстановленный пароль содержит непечатаемые символы, возможно, вы не сможете ввести его в QuattroPro. В этом случае AWOPR позволит расшифровать файл; этот шаг не является обязательным.

WordPerfect Lightning

Чтобы получить информацию, связанную с учетной записью WordPerfect Lightning (домен, имя пользователя и пароль), нажмите «Открыть файл» (Open file) и выберите в меню WordPerfect Lightning. Затем найдите файл *.ini, расположенный в по адресу:

%Documents and Settings%\<user name>\Application Data\Core\WordPerfect Lightning

Обратите внимание, что пароль можно восстановить только в том случае, если он был сохранен (был выбран параметр «Запомнить мой пароль» (Remember my password) в WordPerfect Lightning), и только если вы вошли в систему под той же учетной записью пользователя Windows, из которой был осуществлен доступ к учетной записи WordPerfect Lightning.

4.11 Elcomsoft Internet Password Breaker

4.11.1 Введение

Elcomsoft Internet Password Breaker мгновенно обнаруживает пароли к веб-сайтам, идентификационные данные и почту, хранящиеся в различных приложениях. Поддерживаются все версии Internet Explorer, Microsoft Edge Chromium, Microsoft Edge Legacy, Firefox, Safari, Google Chrome, Chromium, Opera, Yandex, браузер QQ, браузер UC, браузер Tor, браузер 360 Safe и все версии Microsoft Outlook, Outlook Express, Windows Mail и Windows Live Mail.

Elcomsoft Internet Password Breaker поможет вам получить информацию о логине и пароле на самых разных ресурсах.

Elcomsoft Internet Password Breaker извлекает логины и пароли к веб-сайтам, "раскрывает" информацию автозаполнения (включая формы логин-пароля). Пароли в Apple Safari, Google Chrome, Mozilla Firefox и Opera можно получить одним щелчком мыши. Для Internet Explorer 7+ **EINPB** позволяет анализировать историю URL-адресов для определения последних посещенных веб-сайтов и извлекать информацию о паролях, хранящуюся для этих веб-сайтов. Для IE он сможет извлекать сохраненные пароли и информацию автозаполнения для всех веб-сайтов, включая клиенты веб-почты, Amazon, LinkedIn, LiveJournal и различные социальные сети.

Elcomsoft Internet Password Breaker извлекает сохраненную информацию о паролях из Microsoft Outlook, Outlook Express, Windows Mail и Windows Live Mail, включая пароли Microsoft Passport. Он также позволяет получить доступ ко всем типам паролей почтовых учетных записей, включая пароли, защищающие POP3, IMAP, SMTP и NNTP аккаунты, а также пароли, защищающие идентификационные данные пользователей. Для всех версий Microsoft Outlook **EINPB** также будет извлекать пароли к почтовым учетным записям и пароли, защищающие файлы PST.

Если на ПК установлено несколько продуктов или существует несколько идентификаторов пользователей, **Elcomsoft Internet Password Breaker** автоматически обнаружит все идентификационные данные и все файлы PST и автоматически восстановит все пароли ко всем установленным продуктам.

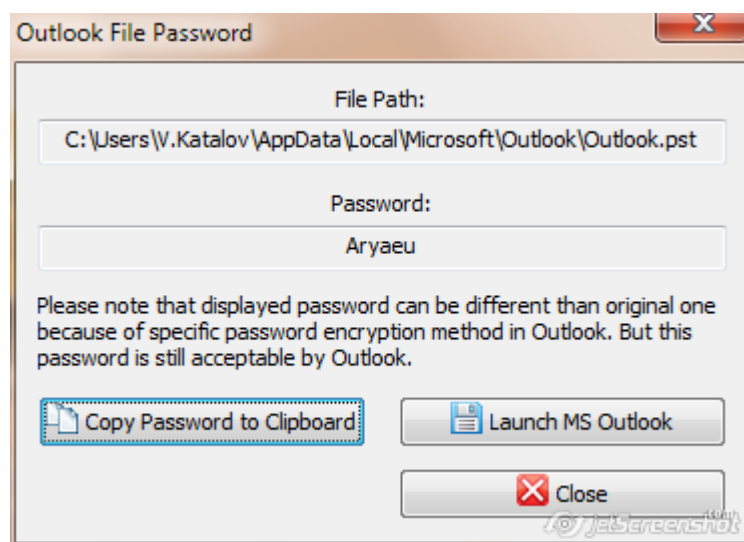
4.11.2 О программе

4.11.2.1 Системные требования

- Windows XP или выше
- Подключение к Интернету (для загрузки веб-страниц из истории IE)

4.11.2.2 Outlook PST пароли

Чтобы извлечь пароли из файлов PST (Outlook 97, 98, 2000, 2002 / XP, 2003, 2007, 2010, 2013, 2016, 2019), используйте кнопку «Открыть файл PST» (Open PST file) и выберите соответствующий файл PST. Пароль будет немедленно восстановлен, показан в окне сообщения и записан в окно журнала. *Вы можете скопировать пароль в буфер обмена, запустить Outlook из EINPB и вставить пароль из буфера обмена, чтобы избежать ошибок при вводе.*

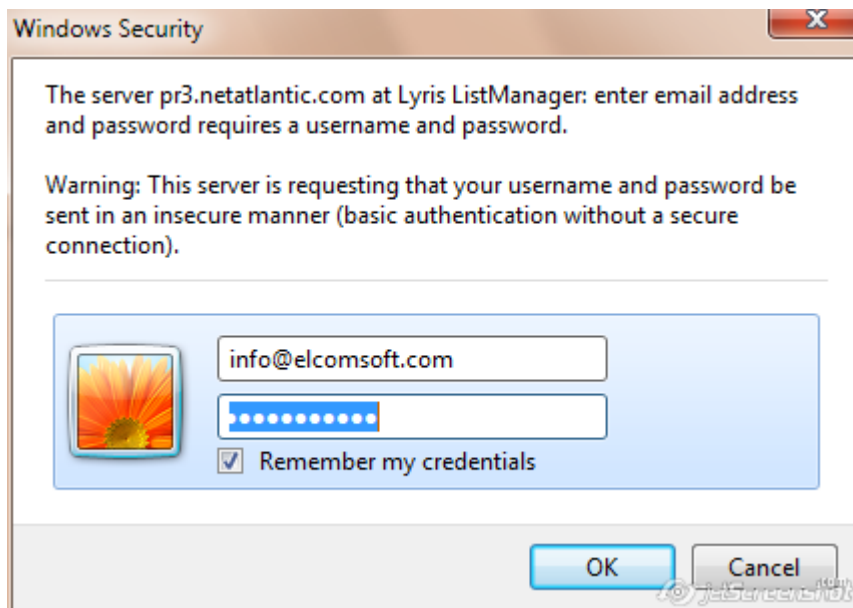


Обратите внимание, что в некоторых случаях пароль, восстановленный EINPB, может не совпадать с исходным паролем. Это ожидаемое поведение из-за алгоритма шифрования, используемого в Outlook. Восстановленный пароль будет принят Outlook, даже если он не соответствует оригиналу.

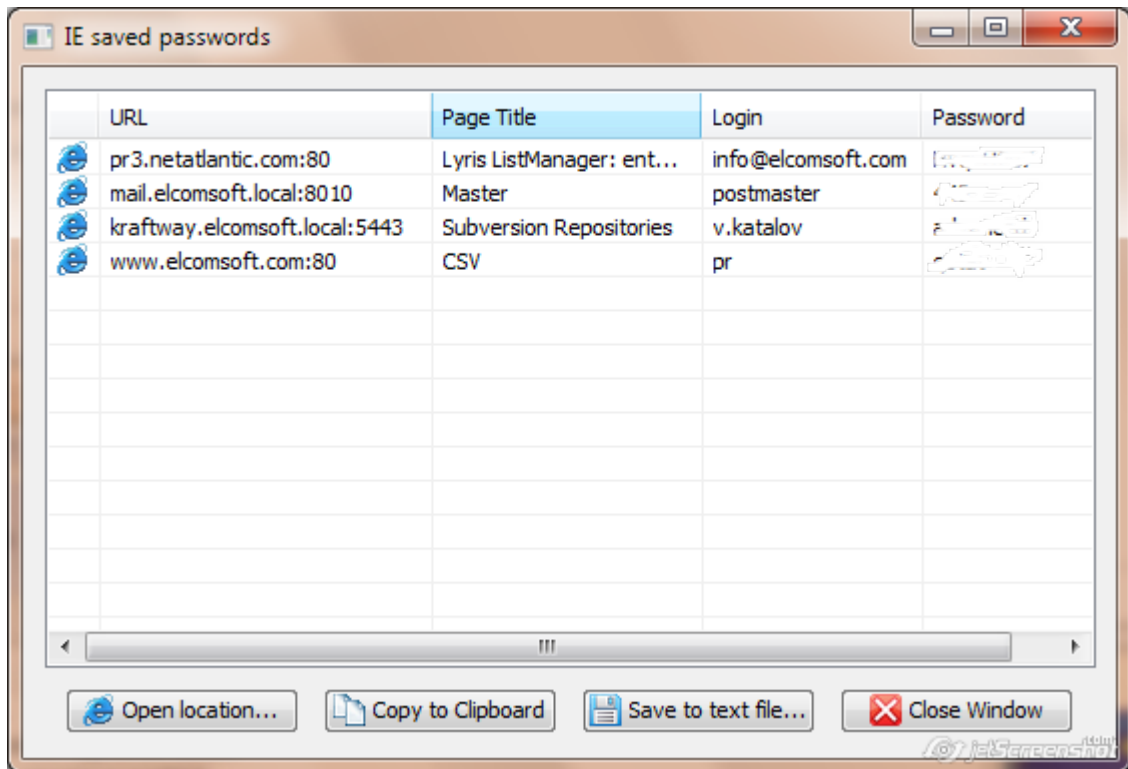
4.11.2.3 Internet Explorer пароли

IE пароли (IE Passwords)

В Internet Explorer есть функция - хранить пароли веб-сайтов:



Чтобы вывести список сохраненных паролей, нажмите "Веб-пароли" (Web Passwords) и выберите "Пароль IE" (IE Password) или выберите Web Explorer | Пароли IE (Web Explorer | IE Passwords) в меню (на скриншоте пароли скрыты):

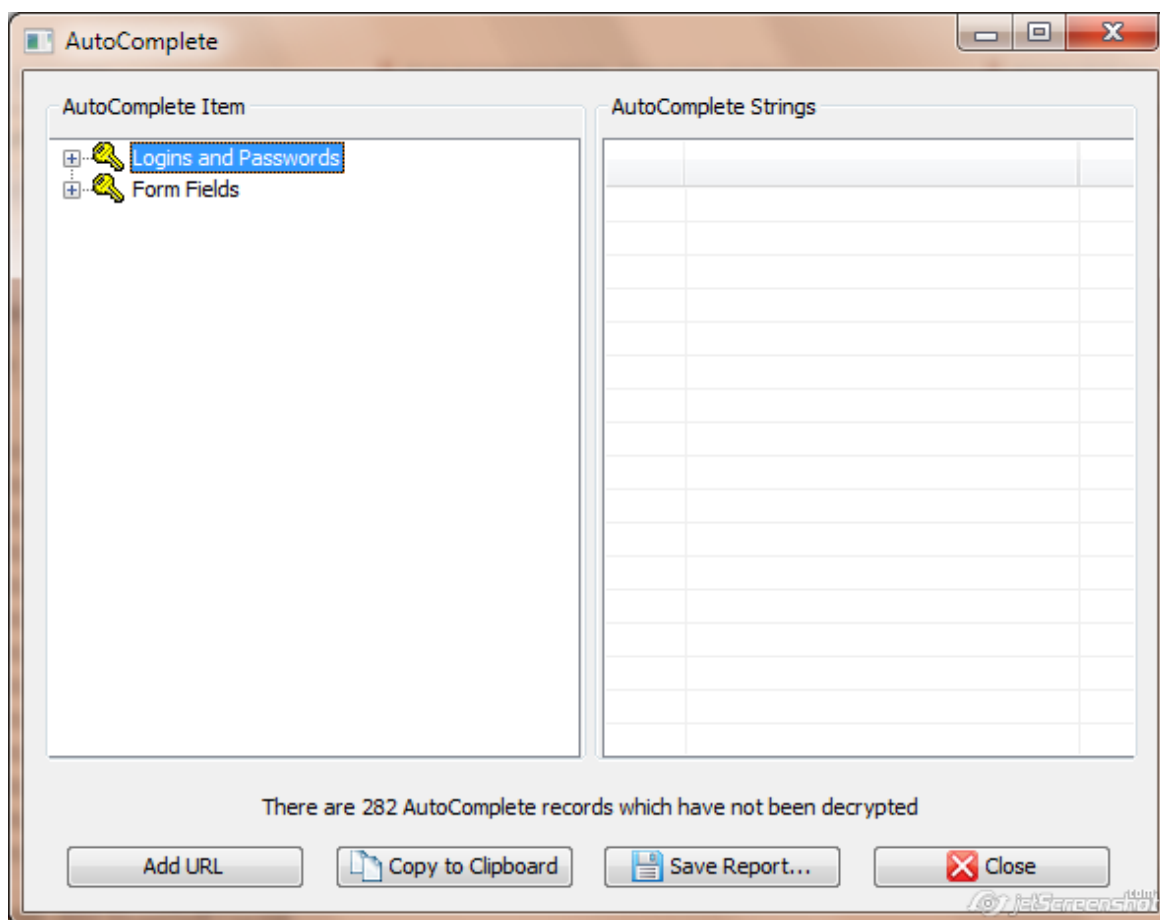


URL-адрес обычно содержит корневой URL. Заголовок страницы - это область, установленная сервером. Для FTP-сайтов он всегда пуст; для веб-сайтов он может содержать заголовок защищенной паролем страницы или имя HTML-файла.

Вы можете сохранить учетные данные для аутентификации в текстовый файл с помощью кнопки "Сохранить в текстовый файл" (Save to text file..). Для экспорта только паролей используйте вместо этого кнопку «Экспорт» (Export) на панели инструментов.

Автозаполнение IE (IE AutoComplete)

Для доступа к информации автозаполнения используйте Веб-пароли | Автозаполнение IE (Web passwords | IE AutoComplete) на панели инструментов или выберите Веб-браузеры | Автозаполнение IE (Web browsers | IE AutoComplete) из меню:



Обратите внимание, что если у вас много сохраненных строк автозаполнения (несколько сотен или больше), вам, возможно, придется подождать несколько секунд, прежде чем появится окно. Примечание. Если включен [параметр](#) ^[115] «Загрузка веб-страниц из истории IE» (Loading web pages from IE history), этот процесс может занять больше времени, особенно если у вас медленное подключение к Интернету.

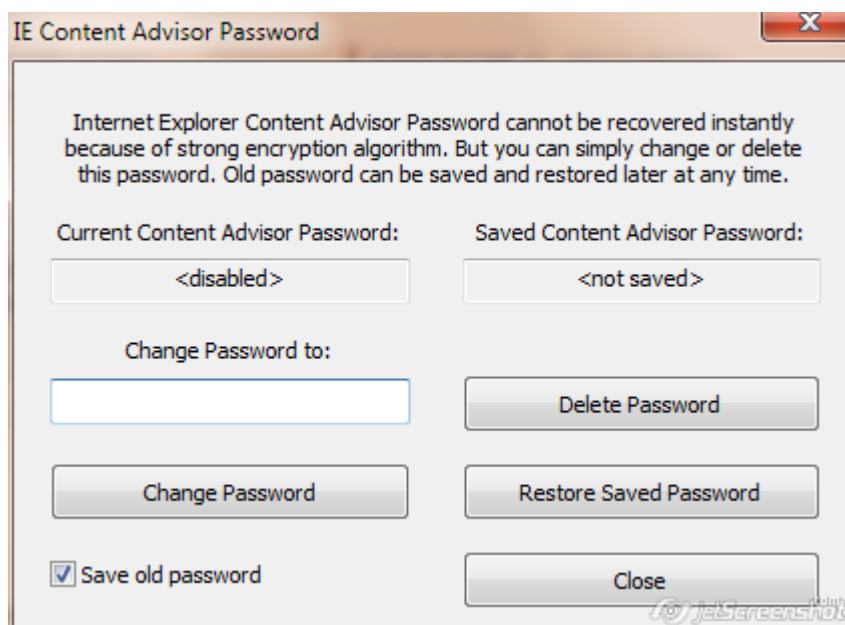
Для каждой записи в разделе слева «Логины и пароли» (Logins and Passwords) вы увидите одну или две строки на правой панели. Первая запись указывает имя для входа, а вторая - пароль. Если вторая запись отсутствует, это означает, что пароль не сохранен.

Кнопка «Сохранить отчет» (Save Report) сохраняет всю информацию автозаполнения в текстовый файл Unicode.

Важно: если пароли к некоторым веб-сайтам не отображаются, даже если включен [параметр](#) ^[115] «Загрузка веб-страниц из истории IE» (Loading web pages from IE history), это не обязательно означает, что пароль не был сохранен. Это может означать, что URL-адрес этих страниц неизвестен программе (что является необходимым для успешного дешифрования). Вы можете попробовать ввести соответствующую ссылку вручную с помощью кнопки «Добавить URL»; если пароль был сохранен для введенной вами ссылки, он будет расшифрован и отображен.

IE Content Advisor

EINPB позволяет удалить или изменить пароль к IE Content Advisor, если он включен. Нажмите Advisor на панели инструментов (или воспользуйтесь меню Веб-браузеры | IE Content Advisor (Web Browsers | IE Content Advisor menu)):



Если установлен пароль к Content Advisor, в поле "Текущий Content Advisor Пароль" (Current Content Advisor Password) будет отображаться значение <включено> (<enabled>). Вы можете изменить пароль или удалить его. Если вы хотите иметь возможность восстановить исходный пароль, включите опцию «Сохранить старый пароль» (Save old password) (и при необходимости используйте «Восстановить сохраненный пароль» (Restore Saved Password)). После того, как вы установили новый пароль, вы можете открыть Content Advisor и отключить его или изменить его настройки.

Обратите внимание, что пароль необходимо менять и удалять, когда Internet Explorer не запущен. В некоторых случаях вам может потребоваться перезагрузить компьютер, чтобы изменения вступили в силу.

4.11.2.4 Другие пароли

EINPB может восстанавливать пароли, сохраненные в различных веб-браузерах, например Mozilla Firefox, Opera, Google Chrome и многих других. Выберите соответствующий веб-браузер в меню Веб-браузеры (Web Browsers) или нажмите кнопку Веб-пароли (Web Passwords) на панели инструментов. *Обратите внимание, что вы можете извлекать пароли из всех веб-браузеров, установленных на компьютере, с помощью команд «Отчет» или «Экспорт» (Report или Export).*

Mozilla Firefox: обратите внимание, что для восстановления паролей, сохраненных в Mozilla Firefox, необходимо установить браузер Firefox. Если пароли защищены мастер-паролем, вы должны сначала удалить его в настройках Firefox. Если вы не знаете мастер-пароль, вам нужно сначала восстановить его с помощью [Elcomsoft Distributed Password Recovery](#).

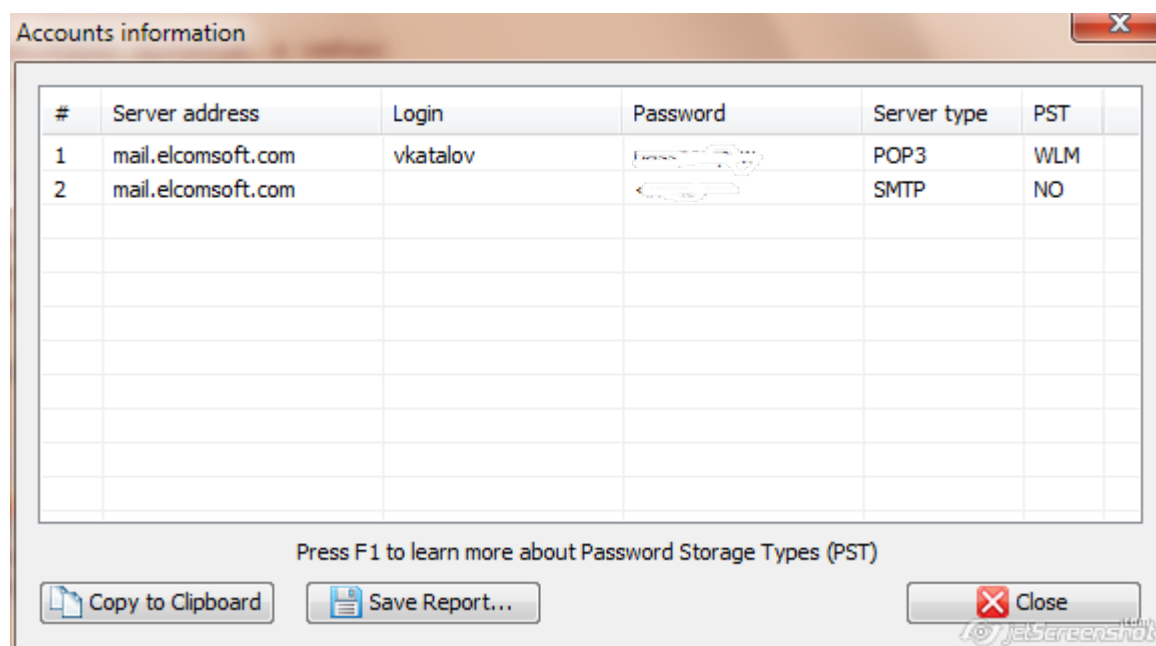
4.11.2.5 Пароли почты и новостей

На панели инструментов есть три кнопки, связанные с почтой и новостями:

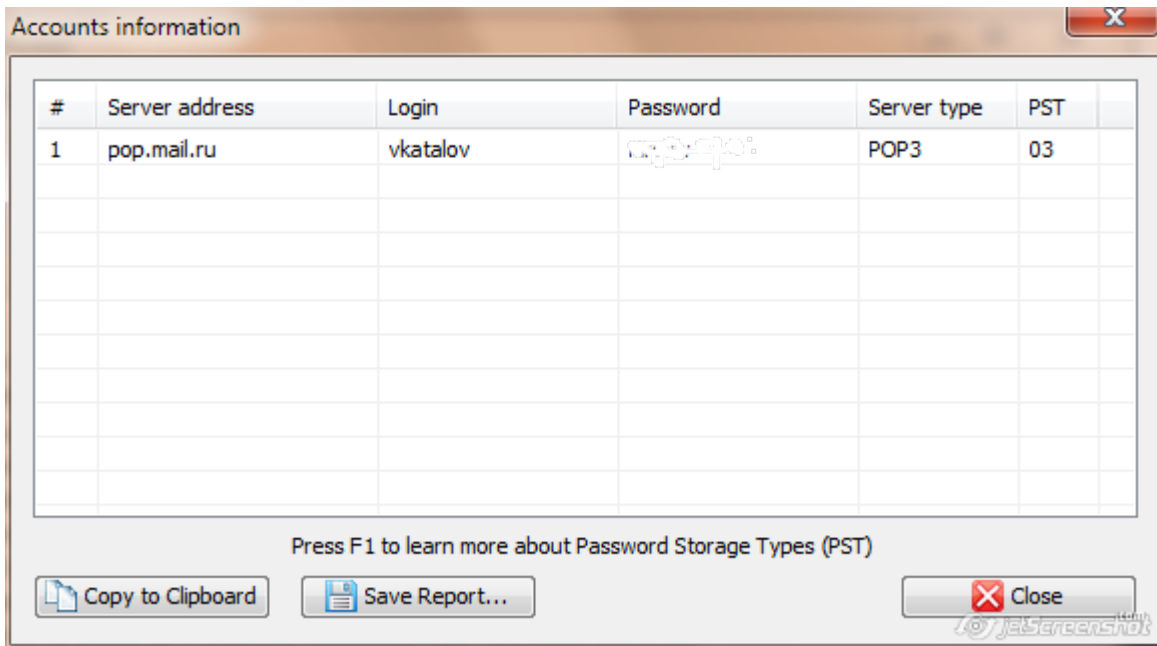
- Аккаунты почты (Outlook Express, Windows Mail и Windows Live Mail, Outlook) - Mail accounts
- Аккаунты новостей (Outlook Express, Windows Mail и Windows Live Mail) - News accounts
- Outlook Express - Identities

Mail accounts

Для каждой учетной записи электронной почты и новостей EINPB показывает адрес сервера, логин и пароль; Обычно последние два поля отображаются как <отсутствует> (<none>) для новостей, что означает, что для подключения к данному серверу не требуется логин/пароль. Кроме того, программа показывает тип сервера (NNTP для учетных записей новостей; POP3, IMAP4, HTTP и SMTP для учетных записей электронной почты) и [тип хранилища паролей](#)^[115]. Для Outlook Express и Windows [Live] Mail:

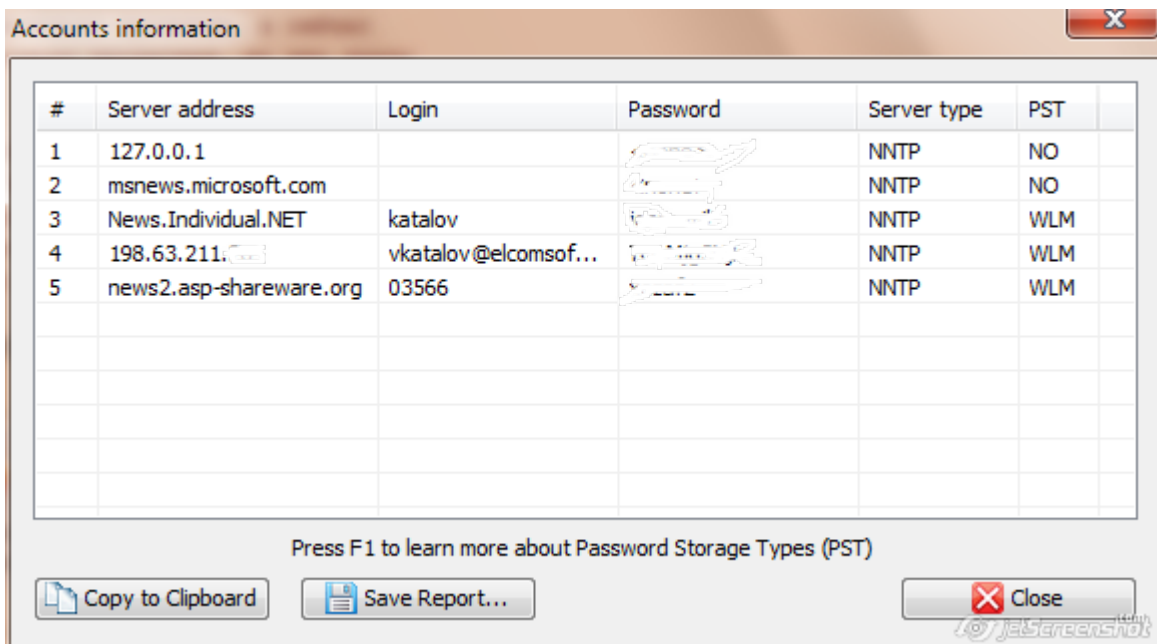


Для Outlook 98, 2000, 2002 / XP, 2003, 2007, 2010 и 2013 (Outlook 97 официально не поддерживается, но все еще может работать) вы также можете восстановить информацию об учетных записях электронной почты, которая в ней хранится (адрес сервера, логин, пароль и тип сервера). Нажмите Учетные записи Outlook (Outlook Accounts) на панели инструментов. Если Outlook установлен и имеет хотя бы одну учетную запись электронной почты, EINPB откроет новое окно с соответствующими полями. Оттуда для любой учетной записи вы можете скопировать пароль в буфер обмена, нажав соответствующую кнопку внизу:



Кроме того, программа показывает тип сервера (POP3, IMAP4, SMTP или HTTP) и [тип хранилища паролей](#)¹¹³.

News accounts



Identities

Для идентификаторов EINPB показывает список комбинаций имен и паролей.

Всю информацию, отображаемую EINPB (адрес, логин-пароль), можно сохранить в текстовый файл с помощью кнопки «Сохранить отчет» (Save Report).

Если у вас возникла проблема при попытке получить пароли для почты, новостей или личных данных, вы можете использовать режим отладки. Чтобы включить режим отладки, выберите Параметры | Настройки в меню (Options | Settings) установите флажок «Включить ведение журнала» (Enable logging) и выберите путь к файлу журнала. Попробуйте восстановить пароли еще раз и отправьте нам этот файл журнала. *Журнал не содержит паролей или какой-либо личной информации.*

4.11.2.6 Типы хранения паролей

Обычно Microsoft Outlook Express хранит все пароли в зашифрованном виде в защищенном хранилище системы (Protected Storage), в других областях реестра или в специальном наборе файлов учетных данных на диске. В редких случаях некоторые пароли могут отображаться некорректно. Следующая таблица типов хранения паролей поможет вам устранить проблему, если таковая возникла.

PS	Пароль успешно получен и хранится в Защищенном хранилище (Protected Storage).
OL	Пароль успешно извлечен и хранится в системном реестре с использованием устаревшего слабого алгоритма шифрования.
O97	Outlook 97; пароль хранится в MAPI.
NP	Пароль не найден в защищенном хранилище (Protected Storage). В некоторых случаях это указывает на то, что имя пользователя используется в качестве пароля или что подсистема защищенного хранилища повреждена.
UN	Неизвестный тип хранилища паролей (Unknown Password Storage Type). Может означать неподдерживаемую версию Outlook Express или поврежденный системный реестр.
ER	Ошибка при получении пароля.
NR	Пароль не получен. Недостаточно прав для разблокировки Защищенного хранилища, или Защищенное хранилище не установлено на компьютере.
NO	Пароль для этой учетной записи отсутствует.
WM	Windows Mail
WLM	Windows Live Mail

Если Тип хранилища - «UN», «ER» или «NR», отправьте журнал отладки (debug log) (см. «Параметры») в службу поддержки ElcomSoft.

4.11.2.7 Опции

Параметр «Включить ведение журнала» (Enable logging) можно использовать, если у вас возникли проблемы с доступом к паролям или программа не работает должным образом. Отправьте нам файл журнала, созданный EINPB, и мы рассмотрим проблему.

Включите опцию "Загрузка веб-страниц из истории IE" (Loading web pages from IE history), чтобы восстановить содержимое полей формы залогинивания и пароли для [Internet Explorer](#)¹⁰⁹. **Обратите внимание, что эта опция замедляет доступ к истории IE, и это может занять несколько часов!**

4.11.2.8 Отчеты и экспорт паролей

Используйте кнопку «Создать отчет» (Create Report) на панели инструментов или выберите [Файл] | [Создать отчет для всех] ([File] | [Create Report for All]) в меню, чтобы экспортировать все обнаруженные учетные данные для аутентификации в текстовый файл. Адреса, логины и пароли для всех записей, найденных на компьютере, будут экспортированы, за исключением строк автозаполнения.

В качестве альтернативы вы можете извлечь дедуплицированный и отсортированный список паролей (без остальных данных). Это помогает создать собственный список слов - словарь паролей. Используйте кнопку «Экспорт паролей» (Export Passwords) на панели инструментов или в меню [Файл] | [Экспорт паролей] ([File] | [Export Passwords]). Пароли сохраняются в формате Unicode, по одному в каждой строке. Этот словарь можно использовать в ПО для восстановления паролей, например в [Distributed Password Recovery](#).

4.12 Elcomsoft Wireless Security Auditor

4.12.1 Введение

Elcomsoft Wireless Security Auditor (EWSA) - это инструмент для сетевых администраторов и ИТ-безопасников, позволяющий проводить аудит безопасности беспроводных сетей путем попыток взлома паролей Wi-Fi. Встроенный сниффер Wi-Fi и использование графического процессора обеспечивают максимальную производительность атак на пароли WPA / WPA2-PSK. Elcomsoft Wireless Security Auditor поддерживает словарные атаки с расширенными возможностями - мутациями. Встроенный беспроводной сниффер позволяет перехватывать беспроводной трафик с помощью обычных Wi-Fi адаптеров, а также AirPC арадаптеров. Продукт может принимать стандартные логи tcpdump, поддерживаемые также любым сниффером Wi-Fi.

Периодический аудит сетевой безопасности необходим для обеспечения кибербезопасности. Беспроводные сети могут обеспечить достаточную безопасность только при правильной настройке. Поддерживая стандарты безопасности WPA и WPA2, Elcomsoft Wireless Security Auditor может выполнять аудит всех видов Wi-Fi сетей, посредством попытки взлома-восстановления WPA-PSK (Pre-Shared Key) и WPA2-PSK паролей.

Elcomsoft Wireless Security Auditor поставляется со специализированным Wi-Fi сниффером, который может работать с обычными Wi-Fi адаптерами через NDIS драйвер (32-битная и 64-битная версии в комплекте). Также поддерживаются AirPCap адаптеры. Встроенный беспроводной сниффер перехватывает пакет рукопожатия (handshake packet), необходимый для начала атаки. Для включения сниффинга Wi-Fi сетей необходимы драйверы WinPCap.

Запатентованное ElcomSoft ускорение на графическом процессоре позволяет подбирать Wi-Fi пароли в несколько сотен раз быстрее за счет использования огромной вычислительной мощности современных видеокарт от NVIDIA и AMD. Ускорение с помощью графического процессора обеспечивает производительность уровня суперкомпьютеров с минимальными вложениями. Несколько видеокарт можно использовать вместе для еще более быстрого результата.

Elcomsoft Wireless Security Auditor поддерживает полностью автоматическое и ручное управление, позволяя вручную вводить хэши паролей и SSID сети. Получая все SSID и хэши паролей из пакетов рукопожатия (handshake packet), Elcomsoft Wireless Security Auditor позволяет выбрать, какой из них нужно восстановить. Для проверки сетевой безопасности от атак "изнутри" Elcomsoft Wireless Security Auditor может автоматически импортировать

сохраненные хэши паролей, полученные с помощью [Elcomsoft Proactive System Password Recovery](#).

4.12.2 О программе

4.12.2.1 Системные требования

- Windows 7 или выше
- [AirPcap адаптер](#) (рекомендуется); или иной совместимый Wi-Fi адаптер; или файл дампа в 'tcpdump' формате с пакетами рукопожатия (handshake packages)
- Опционально: поддерживаемая [NVIDIA или AMD/ATI карта](#)^[122]

4.12.2.2 О безопасности беспроводных сетей

Безопасность беспроводных сетей основана на стандарте [IEEE 802.1X](#) (IEEE Стандарт). Этот стандарт определяет два типа шифрования: [WEP](#) и [WPA \(WPA2\)](#). Всего определено два режима WPA / WPA2: общий ключ (pre-shared key) и [RADIUS](#).

Режим pre-shared key (PSK, также известный как персональный режим) предназначен для домашних сетей и сетей небольших офисов; каждый пользователь должен ввести фразу-пароль, содержащую от 8 до 63 печатных символов. Хеш-функция, включающая SSID, преобразует пароль в хеш-значение, которое передается в процессе «рукопожатия». Нет простого способа получить пароль в текстовой форме из хэша, но пароль все же можно взломать-восстановить, выполнив атаку методом перебора или по словарю

4.12.2.3 Как работать с EWSA

Входные данные

EWSA (только в Про-версии) содержит встроенный сетевой сниффер, который поддерживает адаптеры AirPcap, а также большинство современных «универсальных» пользовательских моделей. Если вы используете AirPcap, вам необходимо установить его собственные драйверы; со сторонними адаптерами необходимо установить специальные драйверы NDIS, входящие в комплект EWSA.

EWSA также поддерживает следующие входные данные:

- tcpdump логи
- Tamos CommView логи
- PSPR логи
- Локальный реестр (Local Registry)
- Ручной ввод

Дополнительные сведения об использовании встроенного сниффера и импорте данных из журналов tcpdump и Tamos CommView смотрите в разделе [Захват сетевых пакетов](#)^[119].

Кроме того вы можете импортировать данные из логов PSPR ([Proactive System Password Recovery](#)). При использовании с [WZC \(Wireless Zero Configuration\)](#), программа может сохранять хеш пароля WPA-PSK в текстовый файл (нажмите «Экспорт» в «Доп функции | Беспроводная

сеть»). EWSA также может выгружать хэши паролей из локального реестра (используйте меню «Дамп хэшей Windows WPAPSK»). Обратите внимание, что ни PSPR, ни EWSA не могут извлекать хэши в ситуации, когда беспроводная конфигурация управляется сторонней (предоставляемой поставщиком) утилитой вместо WZC.

Наконец, вы можете добавить хэш пароля вручную.

Настройки программы (Program options)

Настройки ЦП (CPU Options)

Использование процессора: нужно задать количество процессоров или ядер процессора для запуска атаки. Нажмите Автоопределение, чтобы задать этот параметр автоматически в соответствии с количеством установленных процессоров. В поле «Сводка» (Summary) отображается дополнительная информация об ОС, имени компьютера, имени пользователя, правах администратора и ЦП.

Ускорители (Accelerators)

В поле «Доступные устройства» отображается информация о совместимых видеокартах или аппаратных ускорителях, которые EWSA может использовать для ускорения атак. Если установлено несколько карт, будут показаны все; щелкните, чтобы просмотреть дополнительную информацию, и установите флажок «Информация об устройстве»; нажмите «Информация о драйверах», чтобы получить дополнительную информацию об установленных видеодрайверах. Для получения дополнительной информации ознакомьтесь с разделом [Аппаратное ускорение](#)^[122].

Общие настройки (General options)

Когда атака закончится, переключитесь на следующий хэш-элемент и перезапустите атаку: если этот флажок установлен, программа начнет работать над следующим "рукопожатием" после того, как текущее будет полностью обработано (независимо от результата).

Логгирование (журнал): указывает точность ведения журнала: сообщения-уведомления, предупреждения, сообщения об ошибках. Вы можете также скопировать все сообщения журнала в файл.

Автосохранение: установите интервал для автоматического сохранения состояния атаки. Если программа вылетает по какой-либо причине, при следующем запуске вы сможете восстановить атаку с последней сохраненной точки. Состояние также сохраняется, когда пароль найден, атака остановлена или запущена, а также при некоторых других событиях.

Сниффер беспроводной сети: установите параметры sniffing беспроводной сети:

- Установить / переустановить драйвер ESNDISMON
- Сворачивать программу в трэй
- Отображать перехваченные пакеты в .rsar-файле (добавляет надежности в случае сбоя)
- Возможность отключения службы WLAN при запуске сниффера; помогает с некоторыми адаптерами в Windows 7
- Варианты деаутентификации (только при наличии двух и более адаптеров)

4.12.2.4 Захват сетевых пакетов

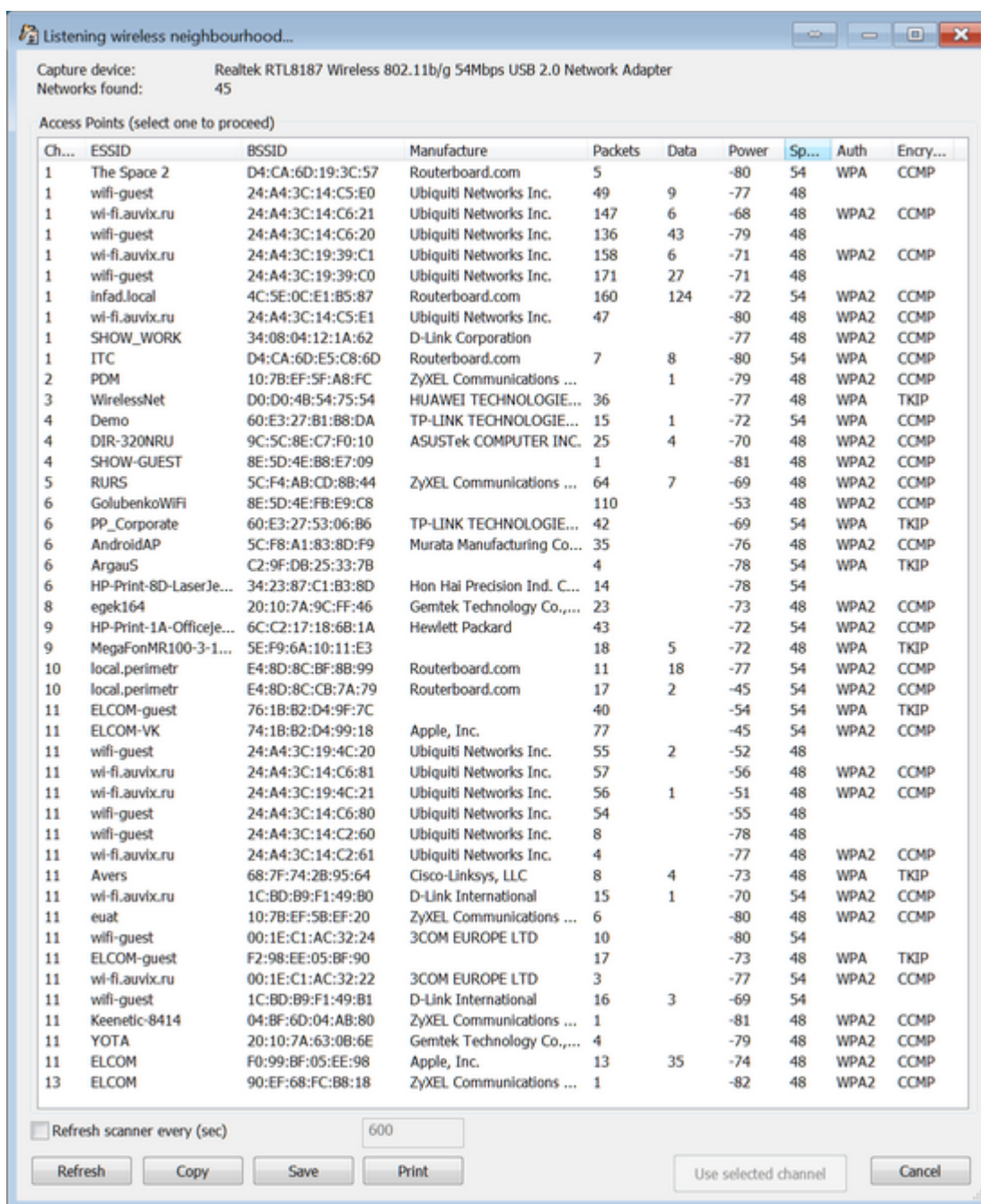
Чтобы начать захват сетевых пакетов, выберите сниффер WiFi на панели инструментов или сниффер AirPCap, если у вас есть адаптер AirPCap. У вас должны быть установлены драйвера; прочтите [установка NDIS драйвера](#)^[122] для получения более подробной информации.

Что касается совместимости адаптеров, то это зависит от качества драйверов соответствующего адаптера. Вкратце:

- Большинство адаптеров Alfa (например, AWUSS036H) совместимы
- Большинство адаптеров Intel (используемых во многих ноутбуках) несовместимы
- Неоднозначные результаты с адаптерами TP-Link: они обычно лучше работают с драйверами, поставляемыми производителем чипсета, а не с TP-Link; те, которые мы протестировали и показали работоспособность: TL-WN7200ND, TL-WN822N, TL-WN722
- Atheros: в основном совместимы (проверено: AR9002WB, AR9485, AR5BW222, AR56x), но есть проблемы с некоторыми конкретными адаптерами (например, невозможность захвата пакетов или даже BSOD)

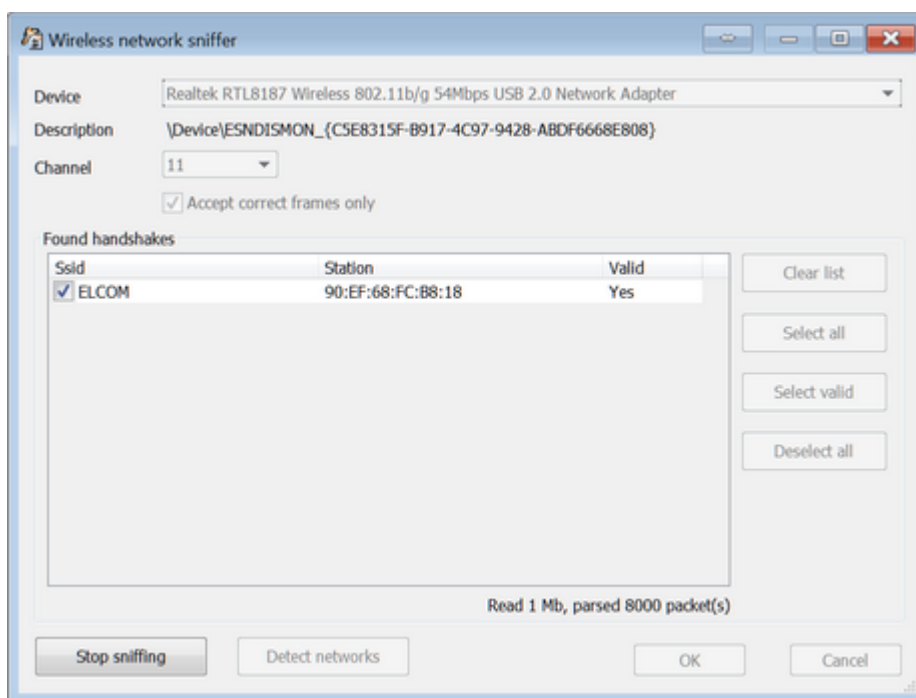
Нет никакого «золотого правила». Даже "универсальные" безымянные адаптеры могут работать правильно, если вы найдете стабильный драйвер, который не вызывает сбой программы (или системы).

После установки драйверов для адаптера и драйверов NDIS выберите правильное устройство (для адаптеров AirPCap оно обычно указано как \\.\airpcap00 device), выберите канал и нажмите [OK]. Если вы не уверены в канале, нажмите [Определить сети] (Detect networks), и программа начнет мониторинг всех каналов; вы можете в любой момент нажать Сохранить, чтобы сохранить список доступных сетей:



Выберите точку доступа и нажмите Использовать выбранное (Use selected channel). Программа начнет мониторинг выбранного канала во всех беспроводных сетях в радиусе действия. Вы также можете мониторить несколько каналов одновременно, нажав кнопку «Несколько» (Multiple). В этом случае программа будет мониторить все каналы один за другим. Обратите внимание, что, если вы используете эту опцию, вы можете пропустить подходящие рукопожатия на в данный момент неактивных каналах, пока программа мониторит другой канал.

После захвата пакетов "рукопожатия" они отображаются в программе:



Все перехваченные пакеты можно отобразить в rсар-файл (для дальнейшего анализа в стороннем ПО). Если эта опция включена, автоматически включается защита от потерянных пакетов "рукопожатия".

Обратите внимание, что некоторые адаптеры могут работать правильно, только если отключен параметр "Принимать только правильные фреймы".

Получив "рукопожатие", нажмите «Прекратить sniffing» (Stop sniffing) и «OK». Теперь вы можете начать процесс взлома-восстановления. Обратите внимание, что если вы используете пробную или стандартную версию, пакеты будут захвачены, но вы не сможете импортировать их для дальнейшего восстановления пароля; эта функция доступна только в Про-версии (подробнее смотрите в Ограничения незарегистрированной версии и Регистрация).

Если у вас нет совместимого беспроводного адаптера, есть альтернативные способы импорта необходимых данных. tcpdump - это обычный sniffер пакетов, который позволяет пользователю перехватывать и отображать TCP / IP и другие пакеты, передаваемые или получаемые по сети, к которой подключен компьютер. Он был написан несколькими людьми, работающими в Лаборатории Лоуренса Беркли; теперь распространяется под лицензией на свободное программное обеспечение и работает в большинстве Unix-подобных операционных систем. Также есть порты tcpdump для Windows.

Примеры существующих sniffеров пакетов, которые могут экспортировать пакеты в формате tcpdump: [airodump-ng](#), [OmniPeek](#).

Захваченные данные должны содержать полное подтверждение ("рукопожатие") аутентификации от реального клиента и точки доступа. Обратите внимание, что программа не работает с пакетами, в которых тип ссылки - LINKTYPE_ETHERNET (они поступают из проводных, а не беспроводных сетей).

4.12.2.5 Установка NDIS драйвера

При первом запуске sniffера программа предлагает установить драйвер ESNDISMON. Без драйвера программа не может выполнять sniffing. Вы можете просмотреть установленные драйверы (включая дату установки), выбрав [Параметры] | [Общие параметры] | [Сниффер беспроводной сети], а также установить / переустановить драйвер.

Чтобы убедиться, что драйверы установлены правильно, выполните следующие действия:

1. Убедитесь, что у вас есть совместимый адаптер.
2. Удалите драйверы WinPCap и AirPCap, если они у вас уже есть в системе.
3. Вставьте адаптер и установите драйвер, предоставленный производителем. НЕ используйте драйверы, поставляемые с Windows: чаще всего они несовместимы. Мы рекомендуем найти и установить драйверы чипсета.

Если вы используете адаптер AirPCap, установите его собственные драйверы с веб-сайта поставщика:

<https://support.riverbed.com/content/support/software/steelcentral-npm/airpcap.html>¹²²

4. Перезагрузите систему; это обязательно для большинства адаптеров, даже если не было запроса на перезагрузку.
5. Установите EWSA.
6. Запустите sniffер Wi-Fi или AirPCap, в зависимости от адаптера. EWSA предложит установить драйвер ESSNDISMON.
7. Если адаптер по-прежнему не работает, установите ESNDISMON вручную:
 - Откройте Центр управления сетями и общим доступом
 - Выберите настройки адаптера
 - Щелкните на адаптер правой кнопкой мыши и выберите Свойства.
 - Нажмите "Установить", выберите "Службы", затем "Добавить".
 - Нажмите Установить с локального диска и выберите путь к драйверу ESNDISMON (.inf-файл, в зависимости от версии системы и 32/64); драйверы находятся в папке «Драйверы» в папке установки программы.

4.12.2.6 Аппаратное ускорение

EWSA поддерживает аппаратное ускорение для практически всех современных [NVIDIA](#) и [AMD](#) видеокарт.

Вы можете использовать NVIDIA [GeForce](#) или [Quadro/Tesla](#) видеокарты. Полный список поддерживаемых карт [здесь](#). Если у вас несколько карт, вам нужно отключить [SLI](#) (масштабируемый интерфейс связи) (или в драйвере или физически отключить карту). EWSA также поддерживает ускорение с картами [AMD Radeon](#) и встроенными [Intel HD и Iris graphics](#).

Независимо от того, есть ли у вас карта NVIDIA или AMD для использования с EWSA, у вас также должны быть установлены последние версии драйверов. Программа была протестирована с 8 картами, но технически она поддерживает большее количество карт.

Часть V

**Программы для работы с системой и
восстановления данных**

5 Программы для работы с системой и восстановления данных

5.1 Advanced EFS Data Recovery

5.1.1 Введение

Advanced EFS Data Recovery (AEFSDR) восстанавливает зашифрованные с помощью Encrypting File System (EFS) файлы и папки и работает во всех версиях Windows 2000, XP, Windows Server 2003, Windows Vista, Windows 7, 8, 8.1, Windows Server 2008, Windows Server 2012, and Windows 10. Восстановление возможно даже в случаях, когда система повреждена, не загружается или когда уничтожены некоторые ключи шифрования.

Microsoft Encrypting File System (EFS) является составной частью операционных систем Microsoft Windows, позволяющей защищать данные от несанкционированного доступа даже в тех случаях, когда злоумышленник завладел компьютером или накопителями с хранящимися на них зашифрованными данными.

Потерять доступ к файлам, защищенным EFS, можно при переустановке Windows поверх старой версии, реформатировании системного раздела или переносе диска с зашифрованными данными на новый компьютер.

Advanced EFS Data Recovery быстро и эффективно расшифровывает данные, защищенные средствами EFS. Сканируя диск сектор за сектором, Advanced EFS Data Recovery обнаруживает зашифрованные файлы и доступные ключи шифрования, после чего дешифрует обнаруженные файлы, даже если какие-то ключи шифрования были утеряны.

Advanced EFS Data Recovery восстанавливает ставшие недоступными вследствие ошибок администрирования зашифрованные данные. Примеры таких ошибок: удаление учётных записей пользователей, отсутствие агентов восстановления данных (Data Recovery Authorities) или их неправильное конфигурирование, некорректный перенос учётных записей в другой домен, а также перенос дисков с зашифрованными данными между компьютерами.

Программа, на которую Вам предоставлена лицензия, является абсолютно законной, и Вы можете использовать её при условии, что Вы являетесь законным владельцем всех файлов или данных, которые Вы собираетесь восстановить с помощью нашего программного обеспечения, или имеете разрешение законного владельца на выполнение этих действий. Вы несёте исключительную ответственность за любое незаконное использование нашего программного обеспечения. Соответственно, Вы подтверждаете, что имеете законное право на доступ ко всем данным, информации и файлам, которые были скрыты.

Вы также подтверждаете, что восстановленные данные, пароли и/или файлы не будут использоваться в каких-либо незаконных целях. Имейте в виду, что восстановление пароля и последующее дешифрование данных неавторизованных или иным образом незаконно полученных файлов может составлять кражу или другое противоправное действие и может привести к вашему гражданскому и (или) уголовному преследованию.

5.1.2 Работа с AEFSDR

5.1.2.1 Информация о EFS (Encryption File System)

Система шифрования данных Encrypting File System (EFS) включена в Windows 2000 (Professional, все версии Server), Windows XP (Professional), Windows Server 2003/2008/2012, Windows Vista (Business, Ultimate, Enterprise), Windows 7 (Professional, Enterprise, Ultimate), Windows 8, 8.1 и Windows 10. Система EFS предоставляет основную технологию шифрования на диске файлов NTFS. EFS, в частности, решает проблемы безопасности, связанные с возможностью получения доступа к файлам NTFS независимо от прав доступа с помощью инструментов, доступных в других операционных системах.

Подробнее в документации [Microsoft TechNet](#):

Функции безопасности, такие как аутентификация при входе в систему или права доступа к файлам, защищают сетевые ресурсы от несанкционированного доступа. Однако любой, у кого есть физический доступ к компьютеру, например, к украденному ноутбуку, может установить на этот компьютер новую операционную систему и обойти защиту существующей операционной системы. Таким образом могут быть раскрыты конфиденциальные данные. Шифрование конфиденциальных файлов с помощью EFS добавляет еще один уровень безопасности. Когда файлы зашифрованы, их данные защищены, даже если злоумышленник имеет полный доступ к хранилищу данных компьютера.

Только авторизованные пользователи и назначенные агенты восстановления данных могут расшифровать зашифрованные файлы. Другие системные учетные записи, у которых есть разрешения для файла - даже разрешение на владение - не могут открыть файл без авторизации. Даже учетная запись администратора не может открыть файл, если эта учетная запись не назначена агентом восстановления данных. Если неавторизованный пользователь попытается открыть зашифрованный файл, доступ будет запрещен.

Сценарии использования EFS

EFS позволяет пользователям защитить информацию от несанкционированного физического доступа к их компьютеру. EFS особенно полезен для защиты конфиденциальных данных на портативных компьютерах или на компьютерах, совместно используемых несколькими пользователями. Оба типа систем уязвимы для атак с помощью методов, позволяющих обойти ограничения списков контроля доступа (ACL). В общей системе злоумышленник может получить доступ, запустив другую операционную систему. Злоумышленник также может украсть компьютер, удалить жесткий диск(и), поместить диск(и) в другую систему и получить доступ к сохраненным файлам. Однако файлы, зашифрованные EFS, отображаются как неразборчивые символы, если у злоумышленника нет ключа дешифрования.

Поскольку EFS тесно интегрирована с NTFS, шифрование и дешифрование файлов прозрачны. Когда пользователи открывают файл, он расшифровывается EFS по мере чтения данных с диска. Когда они сохраняют файл, EFS шифрует данные при записи на диск. Авторизованные пользователи могут даже не осознавать, что файлы зашифрованы, потому что они могут работать с файлами, как обычно.

В конфигурации по умолчанию EFS позволяет пользователям без особых усилий начинать шифрование файлов с «Моего компьютера». С точки зрения пользователя, шифрование файла - это просто вопрос установки атрибута файла. Атрибут шифрования также можно установить для папки с файлами. Это означает, что любой файл, созданный или добавленный в папку, автоматически шифруется.

Как работает EFS

1. EFS использует пару открытого и закрытого ключей и ключ шифрования для каждого файла для шифрования и дешифрования данных. Когда пользователь шифрует файл, EFS генерирует ключ шифрования файла (FEK) для шифрования данных. FEK зашифровывается открытым ключом пользователя, а затем зашифрованный FEK сохраняется вместе с файлом.
2. Файлы могут быть помечены для шифрования различными способами. Пользователь может установить атрибут шифрования для файла с помощью дополнительных свойств файла в папке «Мой компьютер», сохранив файл в папке с файлами, настроенной для шифрования, или с помощью служебной программы командной строки Cipher.exe. EFS также можно настроить так, чтобы пользователи могли зашифровать или расшифровать файл из контекстного меню, доступ к которому можно получить, щелкнув файл правой кнопкой мыши.
3. Чтобы окончательно удалить шифрование, пользователь открывает файл, удаляет атрибут шифрования или расшифровывает файл с помощью команды cipher. EFS расшифровывает FEK с помощью закрытого ключа пользователя, а затем расшифровывает данные с помощью FEK.

Дополнительную информацию можно получить в Microsoft:

- [The Encrypting File System](#)
- [File encryption](#)

5.1.2.2 Как работает Advanced EFS Data Recovery

Существует несколько типичных сценариев использования Advanced EFS Data Recovery:

- Вы хотите получить доступ к файлам на внутреннем диске(ах), и у вас есть учетная запись администратора или права администратора. Однако некоторые сертификаты повреждены, и стандартные методы, доступные в операционной системе, не работают, или некоторые файлы были зашифрованы другими пользователями, и их пароли неизвестны.
- Операционная система не загружается, или у вас нет учетной записи с правами администратора.
- Вы работаете с диском с файлами, которые были зашифрованы на другом компьютере.
- Система была переустановлена.

В первом случае никаких дополнительных действий перед установкой AEFSDR не требуется. Если вы не можете загрузиться с диска, содержащего зашифрованные файлы, установите AEFSDR на компьютер с Windows, на котором у вас есть права администратора. В последнем случае подключите анализируемый диск к новой системе.

Примечание: если вы запускаете AEFSDR в Windows Vista или Windows 7, используя учетную запись с правами администратора, но не учётную запись самого администратора, вы можете увидеть следующее сообщение об ошибке:

Невозможно получить прямой доступ к логическому диску!

Для использования этой программы у вас должны быть права администратора.

Проблема может быть частью UAC (Контроль учетных записей пользователей), который в некоторых случаях работает некорректно. В качестве обходного пути щелкните правой кнопкой

мыши aefsd.exe и выберите во всплывающем меню «Запуск от имени администратора». Возможно, вам потребуется предоставить учетные данные администратора.

Программа может делать следующее:

- Поиск ключей шифрования (на уровне файла или сектора).
- Попытаться расшифровать все закрытые ключи, доступные в системе.
- Находить расшифрованные файлы на выбранных разделах и пытаться расшифровать их ключи шифрования FEK.
- Расшифровать файлы, используя ключи FEK, полученные на предыдущих шагах.

Если вы ранее экспортировали закрытый ключ EFS агента восстановления (подробности см. в [KB241201](#)), но по какой-то причине не можете импортировать его обратно, AEFSDR может использовать его напрямую. В этом случае вам не нужно искать ключи шифрования.

Все шаги подробно описаны в следующих главах: [Scan for encryption keys](#)^[127], [Scan for encrypted files](#)^[131], [Browse for encrypted files](#)^[133] и [Decrypting files](#)^[134].

Самый простой способ использовать инструмент - запустить режим мастера. Если соответствующий параметр включен, режим мастера отображается автоматически при запуске инструмента. Кроме того, вы можете вызвать его в любое время, нажав кнопку «Мастер» на панели инструментов.

5.1.2.3 Режим мастера

Режим мастера проведет вас через все шаги, описанные в разделе [как работает AEFSDR](#)^[126]. Обычно это следующие шаги:

- Выберите логические диски для поиска ключей (по умолчанию проверяются все диски)
- Добавьте имя (имена) пользователя и пароль (пароли) для расшифровки ключей
- Выберите логические диски для поиска зашифрованных файлов (по умолчанию проверяются все диски NTFS)
- Выберите файлы для расшифровки

В любой момент вы можете переключиться в экспертный режим, нажав кнопку на экране мастера. Ваши текущие результаты (найденные ключи или файлы) не будут потеряны. Вы можете отключить опцию "Показывать Мастера при запуске", когда мастер уже запущен. Это не закроет мастера, но в следующий раз программа запустится в экспертном режиме.

Нажимайте кнопки «Вперёд» и «Назад» для навигации по мастеру; например, вы можете вернуться к одному из предыдущих шагов, чтобы просканировать другой диск на предмет ключей или файлов, или добавить дополнительные пароли, если определенные ключи не были расшифрованы.

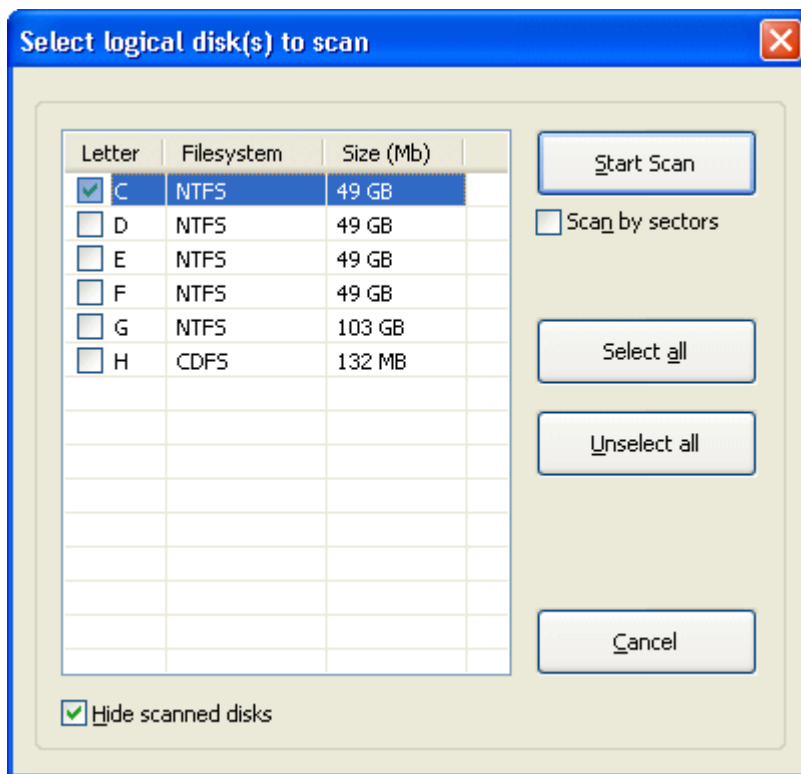
5.1.2.4 Поиск ключей шифрования

Введение

Если вы ранее экспортировали закрытый ключ EFS агента восстановления (и у вас есть файл .rpx), нажмите кнопку «Добавить сертификат», найдите файл .rpx и введите его пароль. Теперь AEFSDR может использовать .rpx для восстановления / дешифрования файлов. В этом случае

вам не нужно будет сканировать ваш диск (диски) на предмет ключей шифрования, как описано ниже.

Начните с поиска ключей шифрования. На вкладке файлов, связанных с EFS, нажмите **Искать ключи...** (или выберите в меню **Поиск | Искать ключи...**; или нажмите кнопку **Искать ключи...** на панели инструментов). Программа отобразит список локальных логических дисков с указанием их размеров и файловых систем:

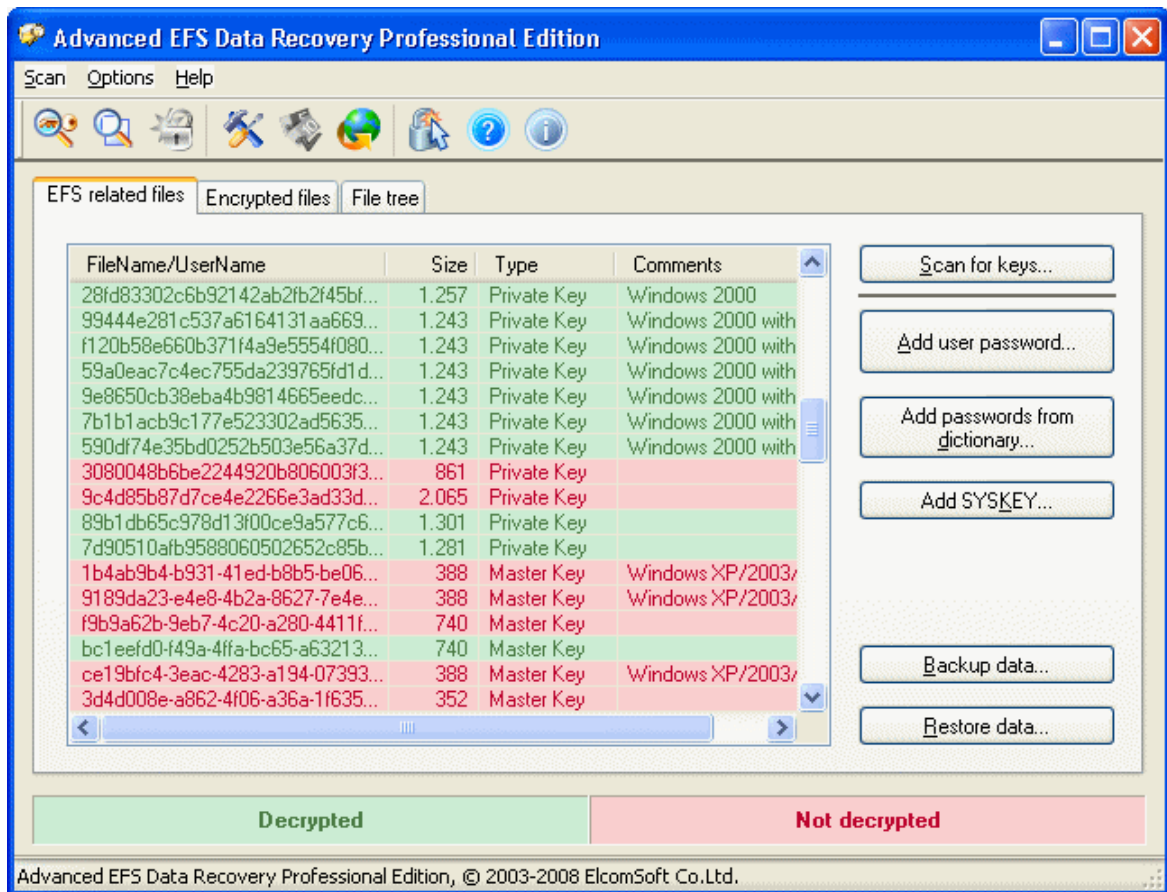


Здесь вы должны выбрать загрузочный диск (загрузочный диск Windows), на котором находятся системный реестр и ключи шифрования. Однако в некоторых случаях ключи шифрования находятся на другом диске. Если вы не уверены, просканируйте несколько дисков.

Выбрав параметр **Сканировать посекторно**, вы можете сканировать диск(и) на более низком уровне, сектор за сектором, чтобы найти ключи, которые были удалены, или которые остались после форматирования диска. Обратите внимание, что этот тип сканирования медленнее, чем обычный, поэтому мы рекомендуем выполнить первое сканирование с отключенной этой опцией и использовать опцию сканирования на низком уровне, только если ключи не были найдены при обычном сканировании.

Обратите внимание на опцию **Спрятать просканированные диски** внизу. Если эта опция включена (по умолчанию) и вы уже просканировали несколько дисков во время текущего сеанса программы, эти диски не будут отображаться в этом окне, поскольку все ключи уже найдены. Если вы хотите отобразить все диски, доступные в системе, отключите эту опцию.

При нажатии кнопки **Начать сканирование** программа просканирует данный(е) диск(и) с целью файлов, необходимых для расшифровки данных:



Вот эти файлы:

- Ключи шифрования
- SYSTEM-реестр
- SAM-реестр

Обычно существует несколько ключей шифрования (фактическое количество может варьироваться в зависимости от количества пользователей в системе) и несколько копий файлов реестра SYSTEM и SAM (активная копия и две или более резервных копии); хотя бы по одной копии каждого реестра.

Если какой-либо из этих компонентов отсутствует, это означает, что либо вы выбрали неправильный диск (в этом случае просто отсканируйте правильный диск, либо все диски, тогда необходимые данные, если они будут найдены, будут добавлены в уже созданный список), либо компоненты недоступны вообще (если, например, они были удалены вручную, или на диске есть физические ошибки).

Ключи шифрования в этом списке всегда красного или зеленого цвета. Зеленый цвет означает, что ключ был успешно расшифрован; или если ключ красный - расшифровка не удалась.

Последний столбец на этом экране, **Комментарии**, показывает дополнительную информацию о ключах шифрования (в какой конкретной версии Windows они были созданы) и режиме SYSKEY (см. ниже).

Возможные проблемы

Если некоторые ключи не были расшифрованы (т.е. они красные), не паникуйте. Возможно, эти ключи вообще не нужны, и вы можете сразу перейти ко второму шагу - [Поиск зашифрованных файлов](#)^[131] или [Обзор зашифрованных файлов](#)^[133]. И только если AEFSDR не сможет расшифровать нужные вам файлы, вернитесь к файлам, связанным с EFS, и попытайтесь решить проблему, как описано ниже.

Шифрование паролем (Windows XP/2003/Vista/2008/7) или защита SYSKEY (Windows 2000)

Во-первых, если файлы были зашифрованы в Windows XP или более поздней версии, вы должны указать пароль (для входа в систему) пользователя, который зашифровал файл(ы), или пароль Агента восстановления. Нажмите кнопку **Добавить пароль пользователя...** и введите имя пользователя и пароль (в виде текста или в шестнадцатеричном формате / UNICODE). Имя пользователя, на самом деле, значения не имеет (имеет значение только пароль), поэтому введите его только для справки. Добавлять пустой пароль не нужно.

Обратите внимание, что вы можете добавить более одного имени/пароля, и после добавления каждого из них AEFSDR попытается расшифровать все ключи, перечисленные на этой вкладке - в случае успеха цвет изменится с красного на зеленый. Кроме того, вы можете использовать опцию **Добавить пароли из словаря...** и загрузить списки паролей из текстового файла. Этот файл должен содержать только пароли, по одному на строку, без имен пользователей (которые на самом деле не имеют значения). Не рекомендуется использовать большие списки слов (более нескольких сотен записей), особенно в Windows XP и более поздних версиях и/или при наличии большого количества ключей шифрования, поскольку это занимает много времени.

В Windows 2000 пароль обычно не требуется, пока не будет использована расширенная защита SYSKEY (дополнительную информацию см. здесь [How to use the SysKey utility to secure the Windows Security Accounts Manager database](#)). Есть три возможных варианта SYSKEY:

- Пароль при запуске: пароль необходим для разблокировки ключа запуска при каждом запуске компьютера.
- Сохранить ключ запуска на гибком диске: SYSKEY создает новый ключ запуска и сохраняет его на гибком диске. Эта дискета вставляется каждый раз при запуске компьютера.
- Хранить ключ запуска локально: это настройка по умолчанию. Сохраняя ключ запуска на локальном жестком диске, Windows может получить к нему доступ во время запуска без дальнейшего вмешательства.

AEFSDR должен работать нормально, если в системе, с которой вы работаете, использовалась последняя (по умолчанию) опция, т.е. ключи должны расшифровываться автоматически. Но если ключ запуска хранится (был) на гибком диске или был выбран пароль запуска, программа просто не сможет расшифровать некоторые ключи. В этом случае вы должны указать пароль (как в Windows XP / 2003, см. выше). В качестве альтернативы, если у вас есть дискета с ключом запуска или вы знаете пароль запуска, вы можете добавить их в программу, нажав кнопку **Добавить SYSKEY...** Вы можете добавить несколько паролей или ключей с помощью этой функции (но по одному за раз). Обратите внимание, однако, что после добавления SYSKEY вам придется повторно сканировать ключи шифрования.

Пароль был изменен после шифрования

После изменения пароля домена вы можете получить сообщение об ошибке при попытке получить доступ к защищенным данным. Эта проблема возникает из-за того, что защищенные данные зашифрованы с использованием хэша, основанного на вашем пароле. Когда вы меняете свой пароль в домене, данные не шифруются повторно с новым паролем, пока вы впервые не получите доступ к данным. Если вы попытаетесь получить доступ к данным в первый раз, когда вы отключены от домена, с контроллером домена не удастся связаться. Следовательно, невозможно получить доступ к данным и повторно зашифровать их с новым паролем.

По умолчанию AEFSDR должен по-прежнему иметь возможность расшифровывать ключи шифрования (и, следовательно, защищенные данные), но если нет, используйте тот же прием, что и для проблемы защиты SYSKEY, то есть путем добавления пароля (паролей) пользователя. Если вы их не знаете, попробуйте решение, описанное в следующей статье базы знаний Майкрософт:

[You Cannot Access Protected Data After You Change Your Password](#)

Компьютер является частью домена

Политика восстановления предусматривает, что человек должен быть назначен агентом восстановления. Локальная политика восстановления по умолчанию создается автоматически, когда учетная запись администратора входит в компьютер в первый раз. Когда это происходит, этот администратор становится агентом восстановления по умолчанию. В некоторых ситуациях первый администратор, входящий в Windows 2000, не является учетной записью локального администратора. Соответствующая статья базы знаний Майкрософт:

[The Local Administrator Is Not Always the Default Encrypting File System Recovery Agent](#)

Если локальный администратор является агентом восстановления ваших данных по умолчанию, AEFSDR будет работать правильно. Если нет (как описано в упомянутой выше статье), вам придется добавить пароли пользователей для расшифровки ключей (см. выше).

Резервное копирование/восстановление расшифрованных ключей

Когда/если ключи шифрования (и другие данные, относящиеся к EFS) были найдены и расшифрованы программой, рекомендуется сохранить их для будущего использования - чтобы избежать повторного сканирования диска или на тот случай, если некоторые данные будут изменены. Нажмите кнопку **Сохранить данные...** в AEFSDR и выберите имя файла, чтобы сохранить то, что вы восстановили. Когда вы будете использовать AEFSDR в следующий раз, вы сможете получить все ключи, нажав кнопку **Загрузить данные...**, вместо повторного сканирования диска, добавления паролей пользователей и т. д.

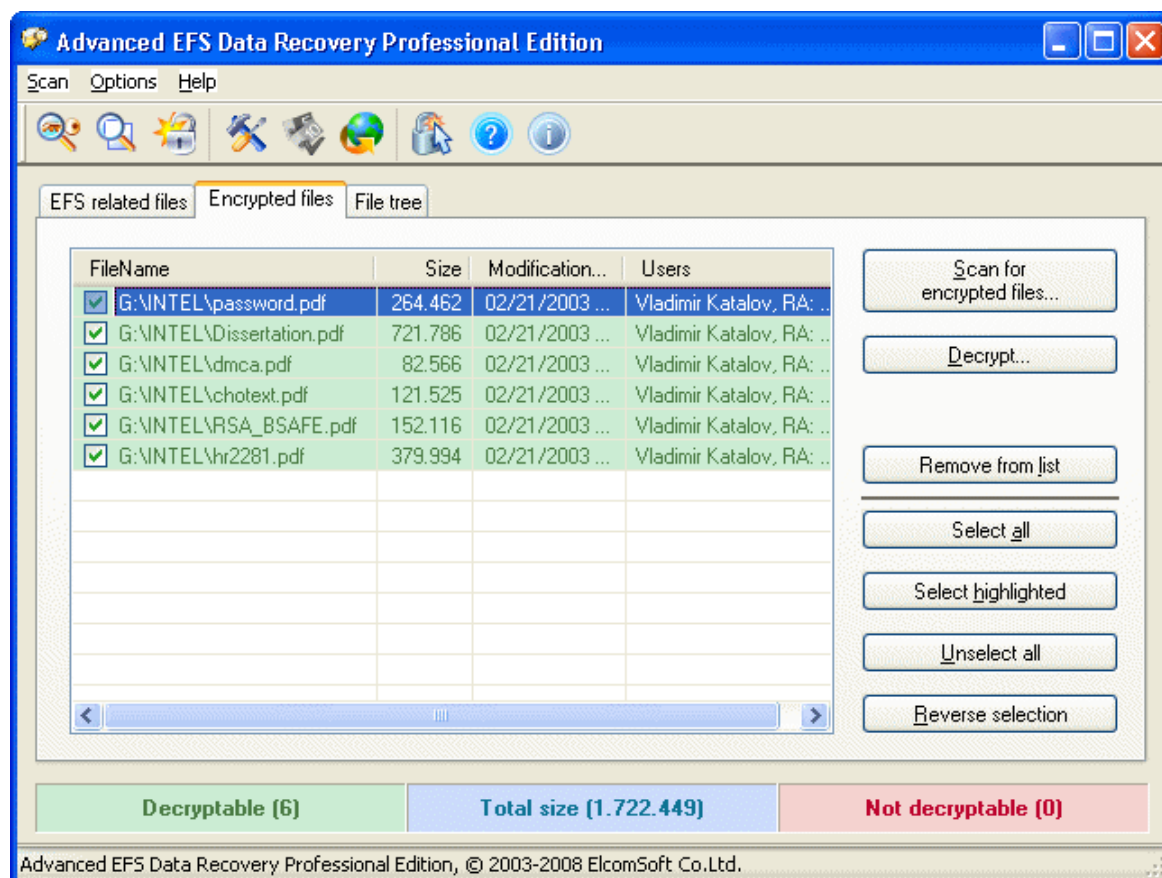
5.1.2.5 Поиск зашифрованных файлов

После того, как ключи [найжены и расшифрованы](#)^[127], вы готовы к расшифровке файлов. Если вы уже знаете, какие файлы зашифрованы и где они находятся, пропустите этот шаг и перейдите непосредственно к [Обзору зашифрованных файлов](#)^[133].

В противном случае перейдите на вкладку **Зашифрованные файлы** в AEFSDR. Там нажмите кнопку **Искать зашифрованные файлы** (или выберите в меню **Поиск | Искать зашифрованные файлы**; или нажмите кнопку **Искать зашифрованные файлы** на панели

инструментов). Программа предложит вам выбрать диск(и) для поиска зашифрованных файлов примерно так же, как при сканировании диска для поиска ключей шифрования. Здесь будут перечислены только диски NTFS, поскольку зашифрованная файловая система доступна только на томах NTFS.

Выберите диски, которые нужно сканировать, и нажмите кнопку **Начать сканирование**. Обратите внимание: если выбранные диски большие и содержат большое количество файлов, этот процесс может занять несколько минут или даже часов. Как только программа находит зашифрованные файлы, она сразу же добавляет их в список. По окончании сканирования вы должны получить полный список зашифрованных файлов, содержащий имя файла (с полным путем), размер в байтах и дату модификации.



Последний столбец (Пользователь) гласит следующее:

John Doe, RA: Ivan Ivanov

Имя (в данном примере «John Doe») - это имя пользователя, который зашифровал файл. Имена, следующие за аббревиатурой RA: - это агенты восстановления («Ivan Ivanov»), если они существуют.

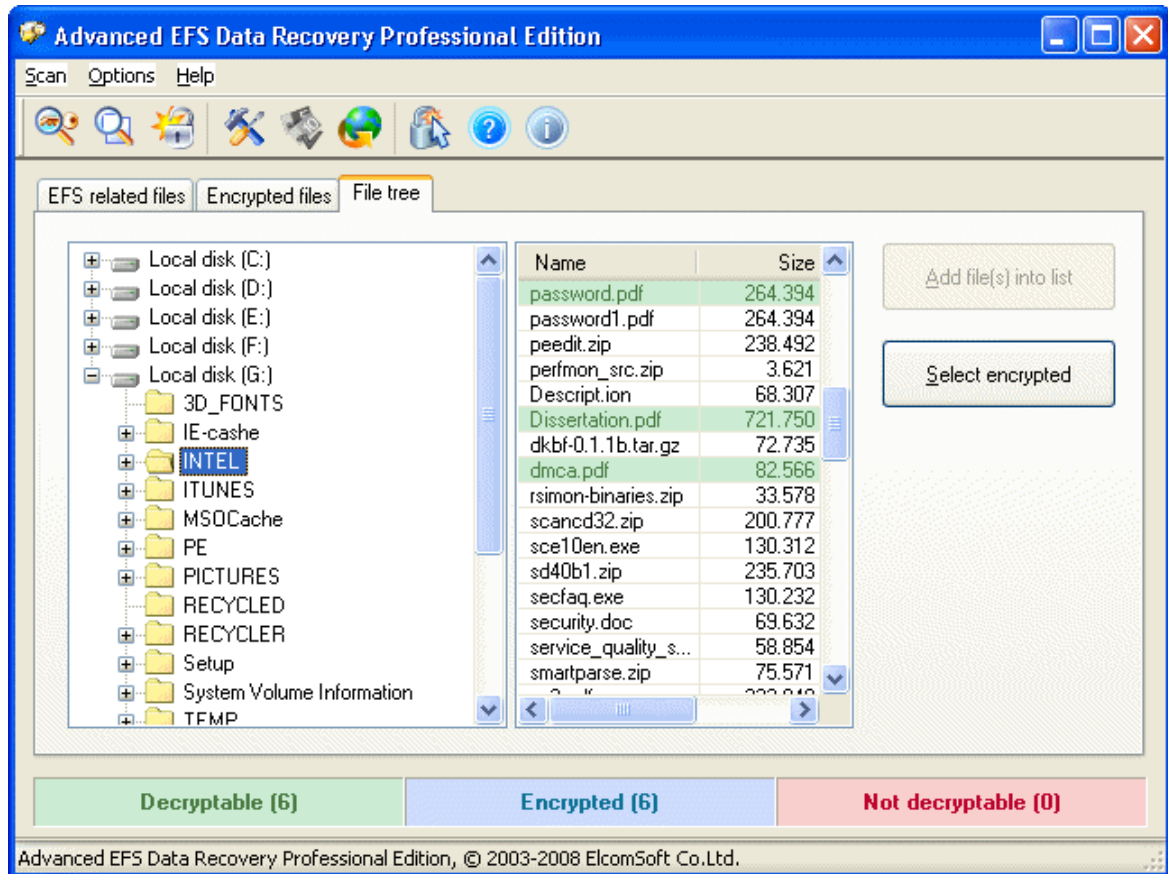
Файлы в этом списке будут выделены зеленым или красным в зависимости от того, можно ли расшифровать файл или нет. Если необходимые файлы не могут быть расшифрованы, вам необходимо снова выполнить [поиск ключей шифрования](#)^[127] (например, просканировав другой раздел и/или добавив SYSKEY или паролей пользователей). Для файлов, зашифрованных в

Windows XP, вы всегда должны добавлять пароли пользователей; в противном случае ключи (и, следовательно, файлы) вообще невозможно расшифровать.

Когда все зашифрованные файлы найдены, их можно [расшифровать](#)¹³⁴.

5.1.2.6 Обзор зашифрованных файлов

Если вы уже знаете местоположение и имена зашифрованных файлов, перейдите на вкладку **Дерево файлов**. Работа здесь аналогична работе с проводником Windows. Дерево дисков и папок расположено в левой панели (примечание: только разделы NTFS), а в правой панели отображается список файлов.



Когда вы меняете или выбираете папку слева, в правой панели AEFSDR отображает имена файлов. Зашифрованные файлы изначально помечаются синим цветом, и инструмент выполняет фоновый анализ того, можно ли расшифровать эти файлы с помощью уже восстановленных ключей. Расшифровываемые файлы отмечены зеленым, а файлы, которые нельзя расшифровать, выделены красным.

Выберите файлы, которые нужно расшифровать, и нажмите **Добавить файл(ы) в список** (или используйте **Выделить зашифрованные файлы**, чтобы добавить все зашифрованные файлы сразу). Файлы будут добавлены в список во вкладке **Зашифрованные файлы**. Вы также можете щелкнуть правой кнопкой мыши любую папку на левой панели и выбрать **Искать зашифрованные файлы (рекурсивно)**, чтобы искать зашифрованные файлы только в выбранной папке и ее подпапках. Повторите эти шаги для файлов, которые нужно расшифровать, и вы готовы к [расшифровке](#)¹³⁴.

Примечание: когда вы открываете эту вкладку впервые после запуска программы, программа может перестать отвечать на запросы в течение нескольких секунд. Это нормально. Инструмент проверяет все логические диски в системе, анализирует файловые системы и строит дерево файлов и папок. Однако, если программа не отвечает в течение нескольких минут, принудительно закройте ее с помощью диспетчера задач и перезапустите с включенным ведением журнала (подробности см. в разделе [Настройки программы](#)^[134]), затем снова переключитесь во вкладку **Дерево файлов** и закройте инструмент. Будет создан файл журнала; Вы можете отправить его нам для анализа. Файл журнала может быть большим, поэтому перед отправкой сохраните его в ZIP или RAR.

5.1.2.7 Расшифровка файлов

Когда у вас будет полный список зашифрованных файлов (см. [Поиск зашифрованных файлов](#)^[131] и [Обзор зашифрованных файлов](#)^[133]) после успешного [восстановления ключей](#)^[127], вы можете начать процесс дешифрования.

Во вкладке **Зашифрованные файлы** выберите файлы для дешифрования. Отметьте файлы для расшифровки. Используйте кнопки **Выбрать все**, **Выбрать подсвеченные**, **Снять выделение со всех** и **Инвертировать выделение** для выполнения массовых операций. Обратите внимание, что можно расшифровать только файлы, выделенные зеленым; красные не могут быть выбраны. **Удалить из списка** удаляет выбранные файлы со страницы.

Затем нажмите кнопку **Дешифровать** (или **Дешифровать файлы** на панели инструментов). AEFSDR предложит вам указать целевой путь. По этому пути инструмент создает подпапки с такими именами, как AEFSDR_X_DECRYPTED, где «X» - буква диска для раздела, из которого вы дешифруете файлы. В этой подпапке будет воссоздан полный исходный путь. Расшифровка выполняется относительно медленно, поэтому проявите терпение. Программа покажет индикатор выполнения и имена дешифруемых файлов.

Мы настоятельно рекомендуем сохранять дешифруемые файлы в NTFS-раздел. Использование раздела FAT32 в качестве целевого может вызвать непредвиденные ошибки.

Перед удалением исходных (зашифрованных) файлов убедитесь, что все файлы были успешно расшифрованы.

Примечание: тестовая версия AEFSDR расшифровывает только первые 512 байт каждого файла, дополняя остальное содержимое нулями. Пожалуйста, зарегистрируйте свою копию, чтобы получить полную версию.

5.1.2.8 Настройки программы

Журнальный файл

Используйте эту опцию, если что-то пойдет не так, например если программе не удастся просканировать выбранный раздел, или некоторые файлы не могут быть расшифрованы и т. д. Укажите имя файла для сохранения отладочной информации и выберите один из следующих вариантов в поле со списком:

- Отключено
- Перезаписать существующий файл
- Перезаписать существующий файл (отладка)
- Добавить в существующий файл

- Добавить в существующий файл (отладка)

Наша служба технической поддержки может попросить вас отправить файл журнала. Журнал отладки гораздо более подробный и может быть большим (до нескольких мегабайт).

Вы можете принудительно перейти в режим отладки, используя параметр командной строки - debug_log и запустив программу как:

```
aefsd.exe -debug_log
```

В этом случае в корневой папке диска C будет создан aefsd.log: это может быть полезно для выявления серьезных проблем, например когда программа не запускается вообще.

Вы также можете установить максимальный размер файла журнала (в мегабайтах). Когда предел будет достигнут, программа прекратит записи. Установите этот параметр на ноль для неограниченного доступа.

Приоритет процесса

Вы можете переключаться между высоким, нормальным и низким приоритетом.

Рекомендуемая настройка - Нормальный, но если вы хотите запустить программу в фоновом режиме, который будет потреблять только циклы простоя ЦП, вы можете выбрать Низкий. Если вы хотите повысить производительность AEFSDR, выберите Высокий, но имейте в виду, что это снизит производительность всех других приложений, работающих на вашем компьютере.

Использовать простые пароли для расшифровки master-ключей

Если эта опция включена, AEFSDR попытается расшифровать главные ключи, используя 100 самых популярных паролей. Обратите внимание, что это может замедлить начальную расшифровку в системах Windows Vista и новее.

Показывать Мастера при запуске

Если включено (по умолчанию), программа всегда запускается в режиме [мастера](#)¹²⁷. Чтобы запустить программу в экспертном режиме, снимите этот флажок.

Анализировать удаленные файлы

Если этот параметр включен, программа также будет сканировать удаленные зашифрованные файлы.

5.1.2.9 Системные требования

- Windows 2000 и выше
- Права администратора (для прямого доступа к диску)

Известные проблемы и ограничения

- Программа может расшифровать защищенные файлы только в том случае, если ключи шифрования все еще существуют в системе и не были уничтожены.
- Поддерживаются только базовые (в отличие от динамических) тома NTFS.
- Для всех систем, кроме Windows 2000, для дешифрования необходим пароль пользователя, который зашифровал файлы, или соответствующий агент восстановления.

5.2 Elcomsoft Forensic Disk Decryptor

5.2.1 Введение

Elcomsoft Forensic Disk Decryptor (EFDD) предоставляет простой способ в режиме реального времени получить полный доступ к информации, хранящейся в криптоконтейнерах. Поддерживая десктопные и портативные версии популярного ПО для шифрования дисков, EFDD может расшифровать все файлы и папки, хранящиеся в криптоконтейнерах, или смонтировать зашифрованные тома в виде новых дисков для обеспечения мгновенного доступа. Ключи дешифрования можно получить, проанализировав файлы гибернации или дампы памяти (функция сброса памяти встроена в продукт) или с помощью атаки FireWire. Программа также может расшифровывать или монтировать диски, если известен пароль или имеется ключ восстановления.

Инструмент обеспечивает почти мгновенное получение доступа к содержимому зашифрованных томов. При полной расшифровке расшифровывается все содержимое защищенного диска, предоставляя исследователям полный и неограниченный доступ ко всей информации, хранящейся на зашифрованных томах. Для быстрого доступа к защищенной информации в режиме реального времени зашифрованный том можно смонтировать (он отобразится как новый диск с новой буквой). В этом режиме файлы будут расшифровываться "на лету".

Elcomsoft Forensic Disk Decryptor поддерживает три способа получения ключей дешифрования, используемых для получения доступа к содержимому зашифрованных контейнеров. В зависимости от того, работает компьютер или выключен, заблокирован или разблокирован, ключи могут быть получены путем анализа дампа памяти или файла гибернации или путем выполнения атаки FireWire для получения "живого" дампа памяти. Чтобы получить ключи дешифрования, зашифрованный том должен быть смонтирован на ПК.

Elcomsoft Forensic Disk Decryptor поддерживает флеш-накопители и съемные носители, зашифрованные с помощью BitLocker-to-Go, а также распознает зашифрованные тома и полное шифрование диска всех поддерживаемых типов. Также поддерживаются образы дисков Raw (DD) и EnCase (.E01).

Поддерживаемые криптоконтейнеры:

- BitLocker
- PGP (шифрование тома и всего диска)
- TrueCrypt
- VeraCrypt
- LUKS (только извлечение хэша пароля)
- BestCrypt (только извлечение хэша пароля)

Данная программа, на которую вам предоставлена лицензия, соответствует законодательству и является абсолютно легальной. Используя ее, вы ничего не нарушаете при условии, что вы являетесь законным владельцем всех файлов или данных, которые вы собираетесь восстановить с помощью нашего программного обеспечения, или имеете разрешение законного владельца на выполнение этих действий. Вы несете исключительную

ответственность за любое незаконное использование нашего программного обеспечения. Соответственно, вы подтверждаете, что имеете законное право на доступ ко всем данным, информации и файлам, которые были скрыты.

Вы также подтверждаете, что восстановленные данные, пароли и/или файлы не будут использоваться в каких-либо незаконных целях. Имейте в виду, что восстановление пароля и последующее дешифрование данных из незаконно полученных файлов может представлять собой кражу или другое противоправное действие и может привести к вашему гражданскому и (или) уголовному преследованию.

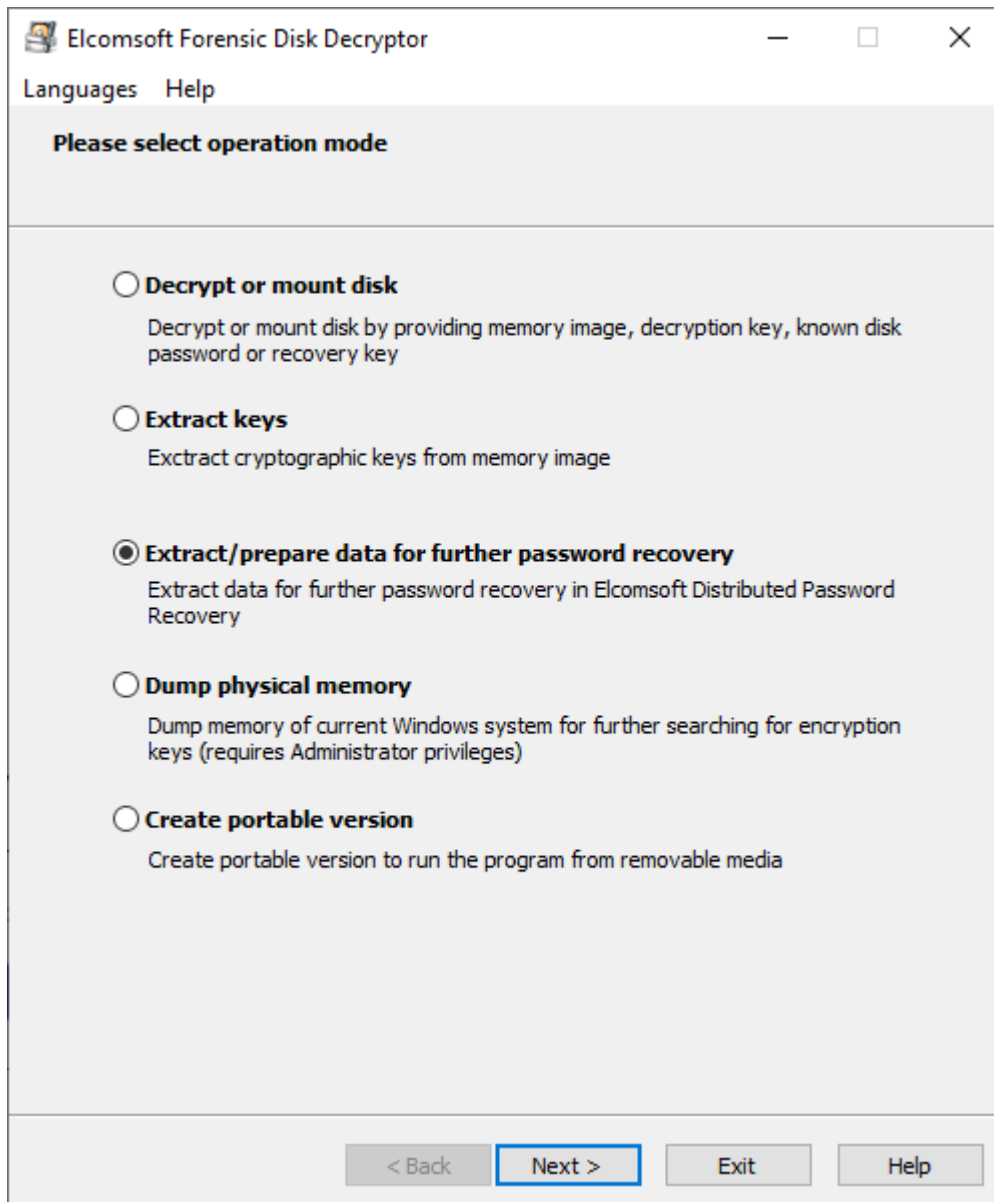
5.2.2 О программе

5.2.2.1 Системные требования

- Windows 7 или выше
- Для всех поддерживаемых зашифрованных дисков / крипто-контейнеров: образ оперативной памяти или файл гибернации, содержащий ключи шифрования диска (созданные при подключении зашифрованного диска) или же сам пароль
- Для BitLocker и PGP: ключ восстановления
- Для BitLocker: база данных Active Directory (ntds.dit)
- Для контейнеров, зашифрованных FileVault2: токен восстановления из iCloud или локально сохраненный ключ восстановления или пароль (только для разделов HFS+; для APFS поддерживается только генерация данных для дальнейшего восстановления пароля)
- Для образов VHD и VHDX: Windows 8.1 или выше

5.2.2.2 Как работать с EFDD

На главном экране EFDD доступны следующие функции:



Расшифровка и монтирование диска (Decrypt or mount a disk)

Подобро описано в [Расшифровка и монтирование диска](#)^[144].

Извлечение ключей (Extract keys)

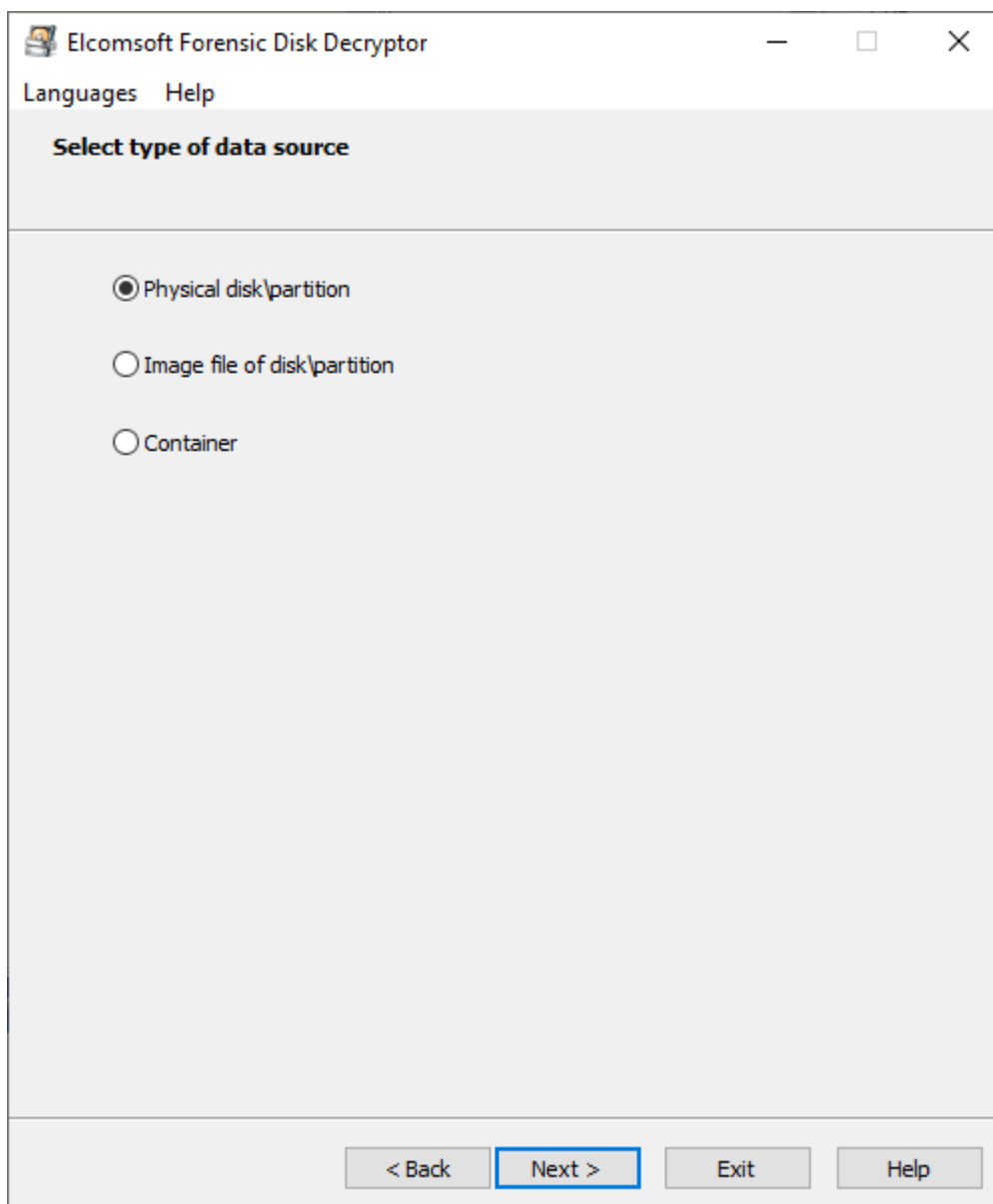
После того, как диск смонтирован в систему (тем самым разблокирован), система сохраняет ключи шифрования в оперативной памяти (ОЗУ), позволяя извлекать или получать ключи из

дампа памяти или файла гибернации (если система находится в гибернации с зашифрованными дисками, которые при этом смонтированы). Подробнее в [Извлечение ключей](#) ^[142].

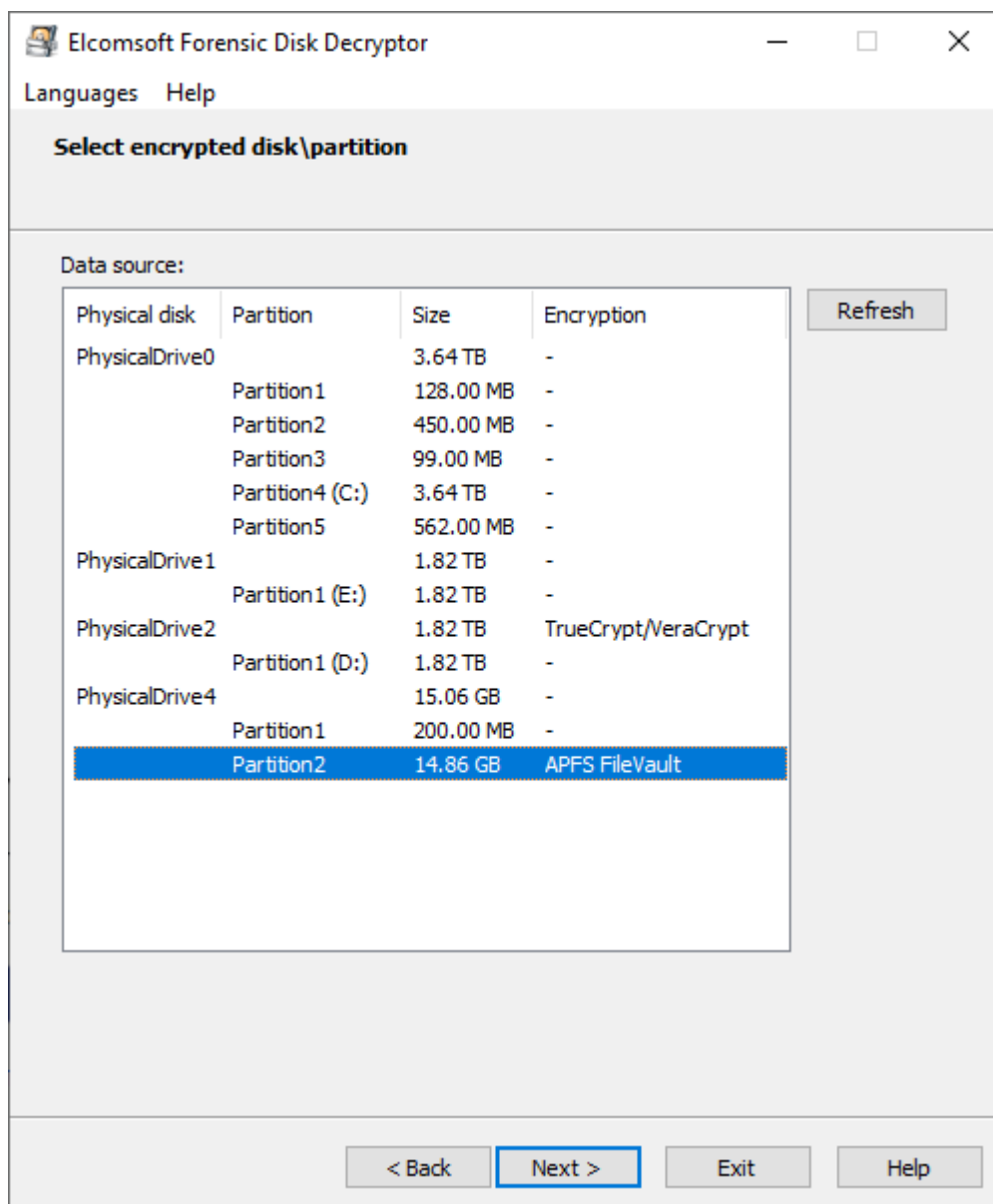
Извлечение/подготовка данных (Extract/prepare data)

Если пароль неизвестен, отсутствуют ключи восстановления, дампы памяти или файлы гибернации, остается единственный вариант - восстановить исходный пароль с помощью довольно долгой по времени брутфорс-атаки или словарной атаки. EFDD позволяет извлекать данные, необходимые для восстановления пароля. Вы можете использовать эти данные в программе [Distributed Password Recovery](#) для эффективного взлома паролей.

Сначала выберите источник данных:



Для первых двух вариантов программа получает список всех доступных разделов и пытается обнаружить шифрование, если оно есть. Параметр «Контейнер» (Container) предназначен для контейнеров PGP (.pgd) и TrueCrypt/VeraCrypt (во втором варианте он может иметь произвольное расширение).

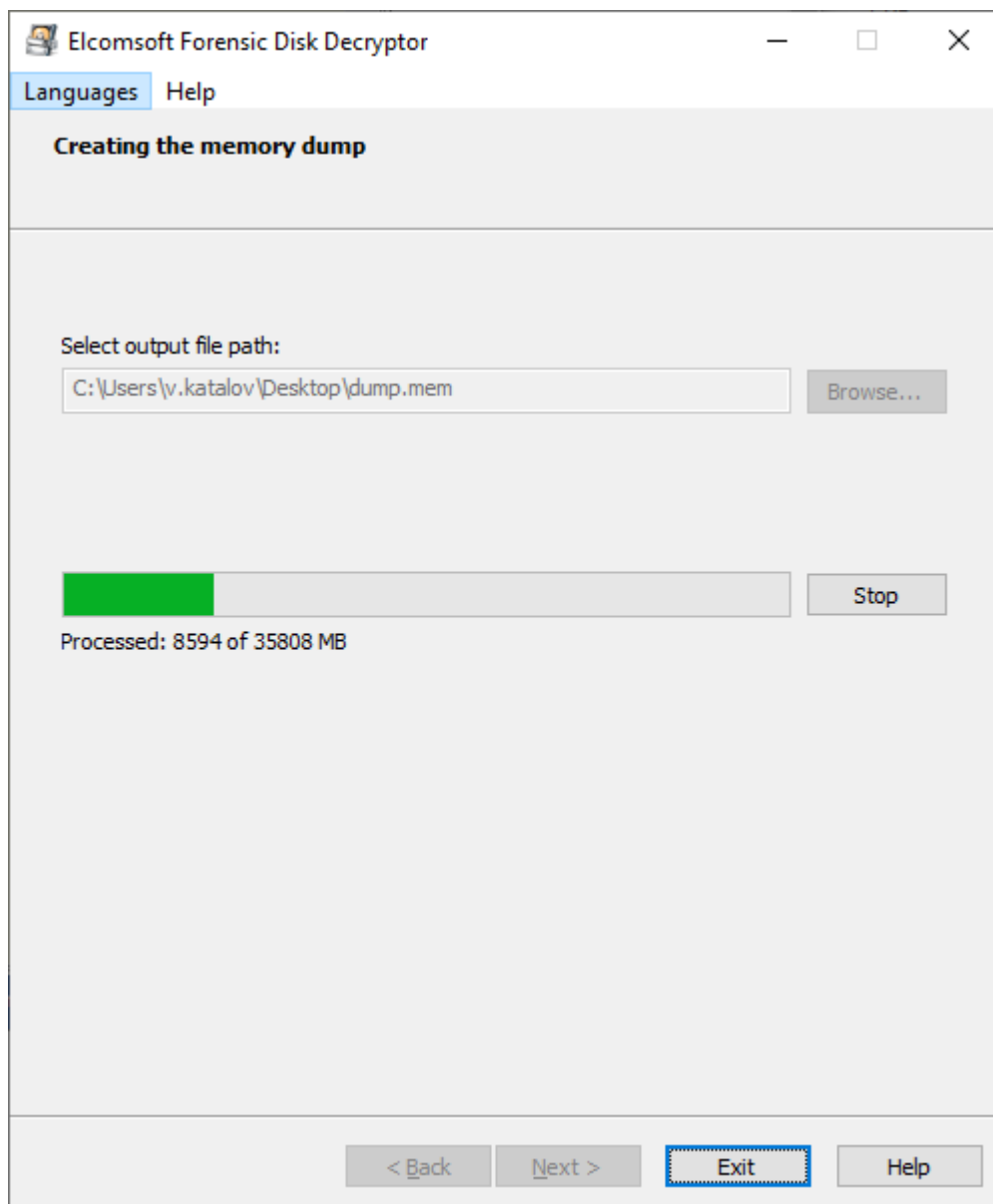


Данные, извлеченные с помощью EFDD, можно в дальнейшем использовать для восстановления пароля с помощью [Distributed Password Recovery](#).

Дамп памяти (Dump physical memory)

После того, как диск смонтирован в систему (разблокирован), система сохраняет ключи шифрования в ОЗУ. Если у вас есть доступ к активной системе, в этом случае ключи можно

вытащить простым способом. Выберите файл, в который нужно сделать дамп памяти, и нажмите Старт (Start). Для этой операции требуются права администратора.



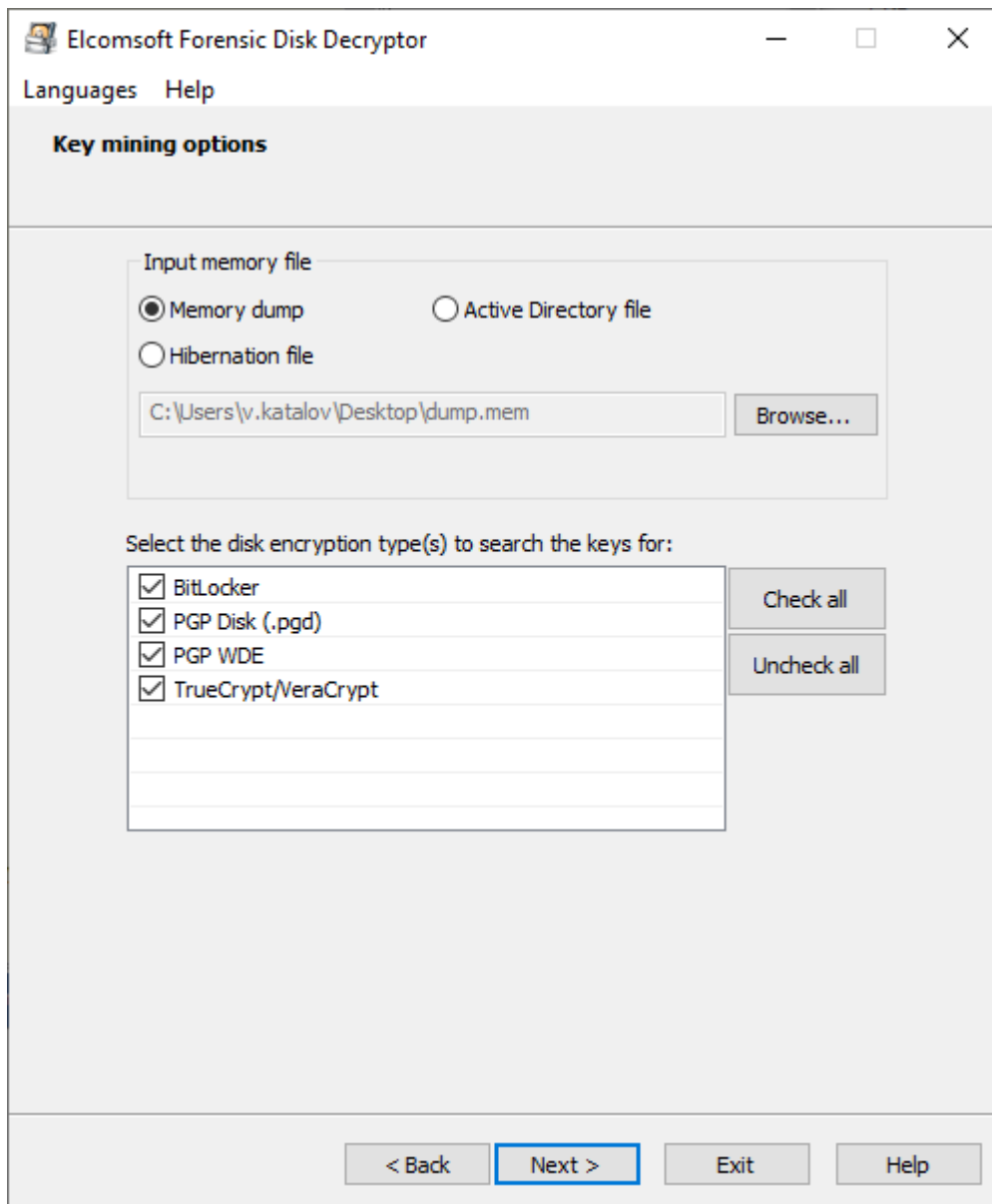
Создать портативную версию (Create portable version)

Эта опция позволяет создать портативную версию программы, которая может запускаться со съемного диска. Между обычной и портативной версиями есть следующие различия:

- Портативная версия не требует установки; запустите 'efdd.exe' для работы
- Портативная версия не включает возможность создания другой портативной версии.
- Портативная версия не может монтировать диски (может только расшифровать)

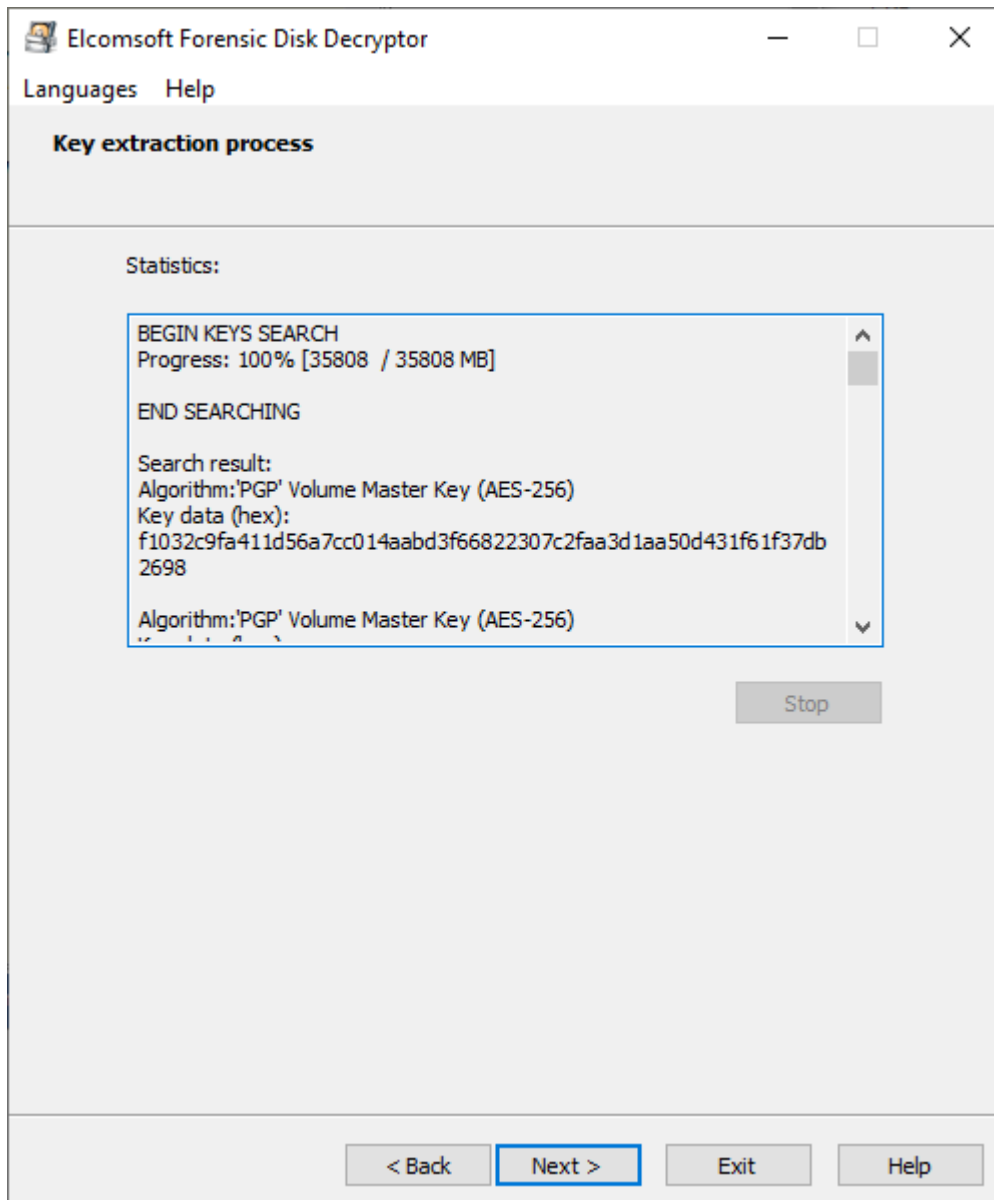
5.2.2.3 Извлечение ключей

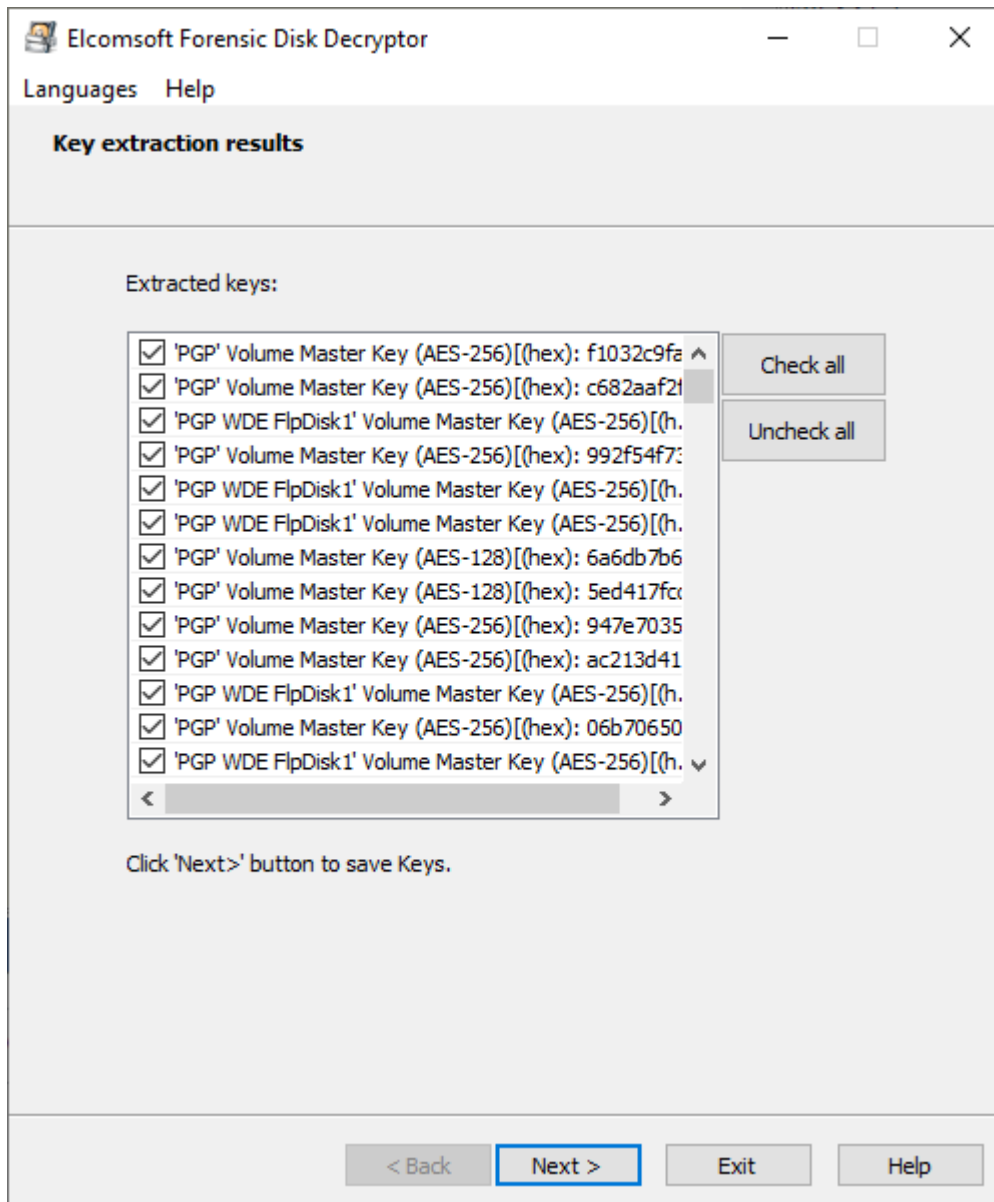
Выберите источник ключей шифрования (дамп памяти (memory dump) или hiberfil.sys) и тип шифрования (BitLocker, PGP или TrueCrypt/VeraCrypt) и нажмите Далее (Next):



Вы также можете выбрать Active Directory (файл ntds.dit) в качестве источника; в настоящее время AD поддерживается только для ключей восстановления к BitLocker.

После завершения процесса поиска отобразится список ключей. Вы можете сохранить их в файл для дальнейшего использования.





Обратите внимание, что зашифрованный диск должен быть подключен к системе при создании дампа (или когда компьютер переведен в состояние гибернации); в противном случае ключи не сохраняются в памяти.

Поиск ключей - это трудоемкий процесс, поэтому рекомендуется ограничить поиск конкретными типами ключей.

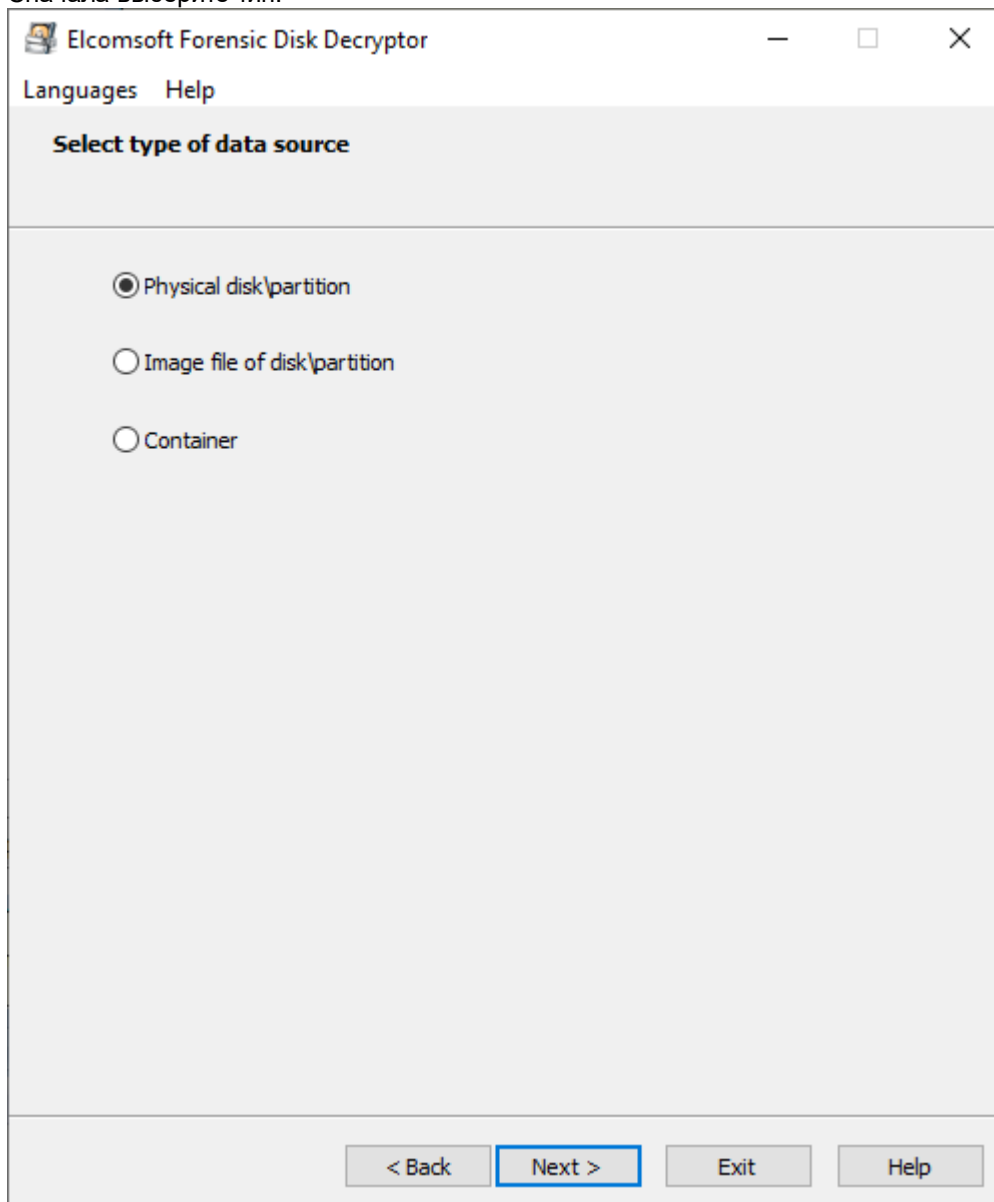
5.2.2.4 Расшифровка и монтирование диска

EFDD поддерживает физические диски, образы дисков и крипто-контейнеры.

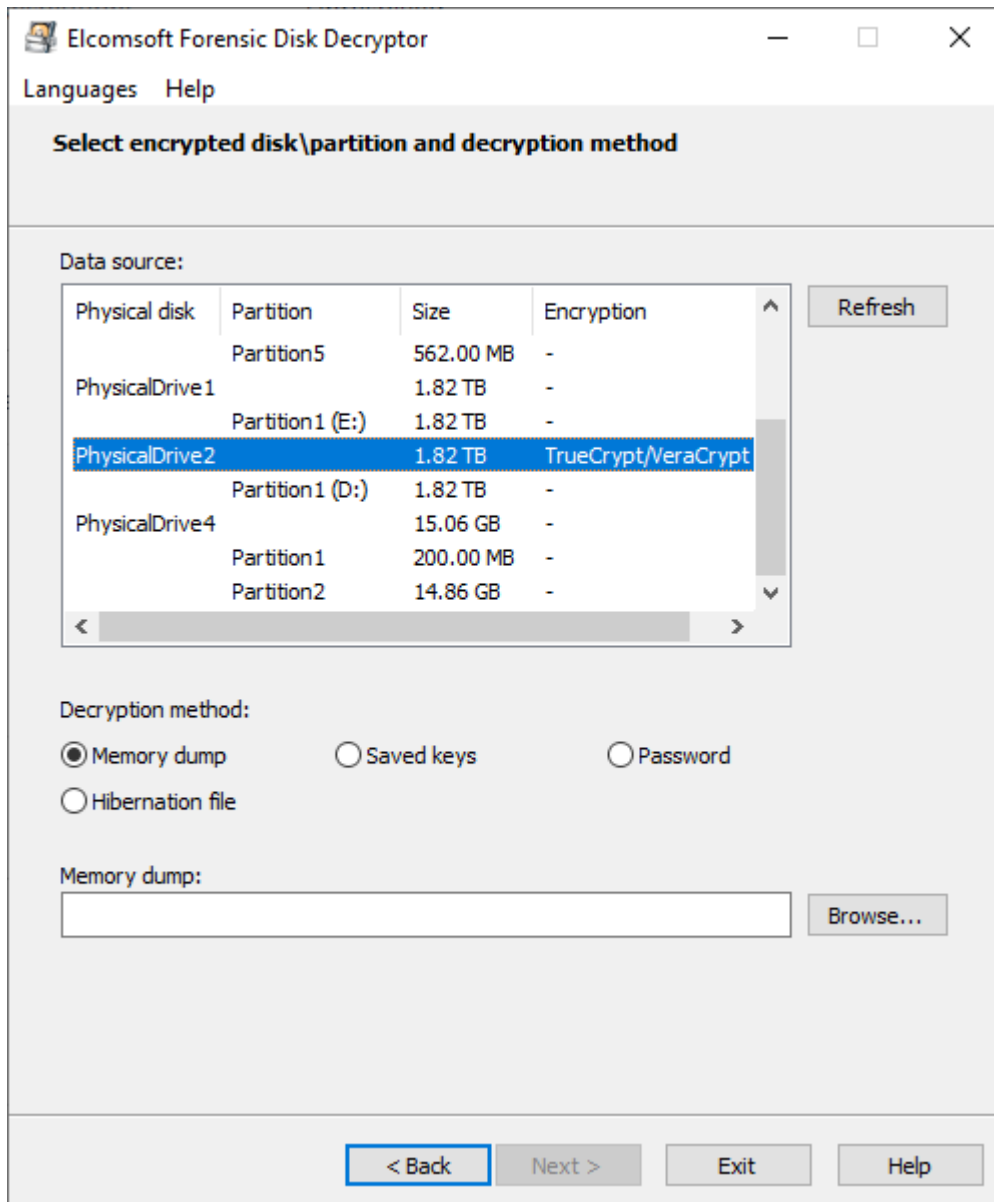
Поддерживаемые образы дисков:

- RAW/DD
- EnCase .E01
- VHD/VHDX (для работы с этими образами требуется Windows 8.1 или выше)

Сначала выберите тип:



EFDD выводит подключенные устройства хранения и разделы, автоматически определяя тип шифрования:



Вы можете либо расшифровать, либо смонтировать раздел для немедленного доступа. Последнее реализуется через [ImDisk virtual disk driver](#) установленный на ПК вместе с EFDD.

Требуется что-то одно из списка:

- Дамп памяти (см. [Извлечение ключей](#)^[142])
- Сохраненные ключи (см. [Извлечение ключей](#)^[142])
- Пароль
- Файл гибернации
- Файл Active Directory (только BitLocker)
- Ключ восстановления (для BitLocker, PGP WDE, FileVault2)

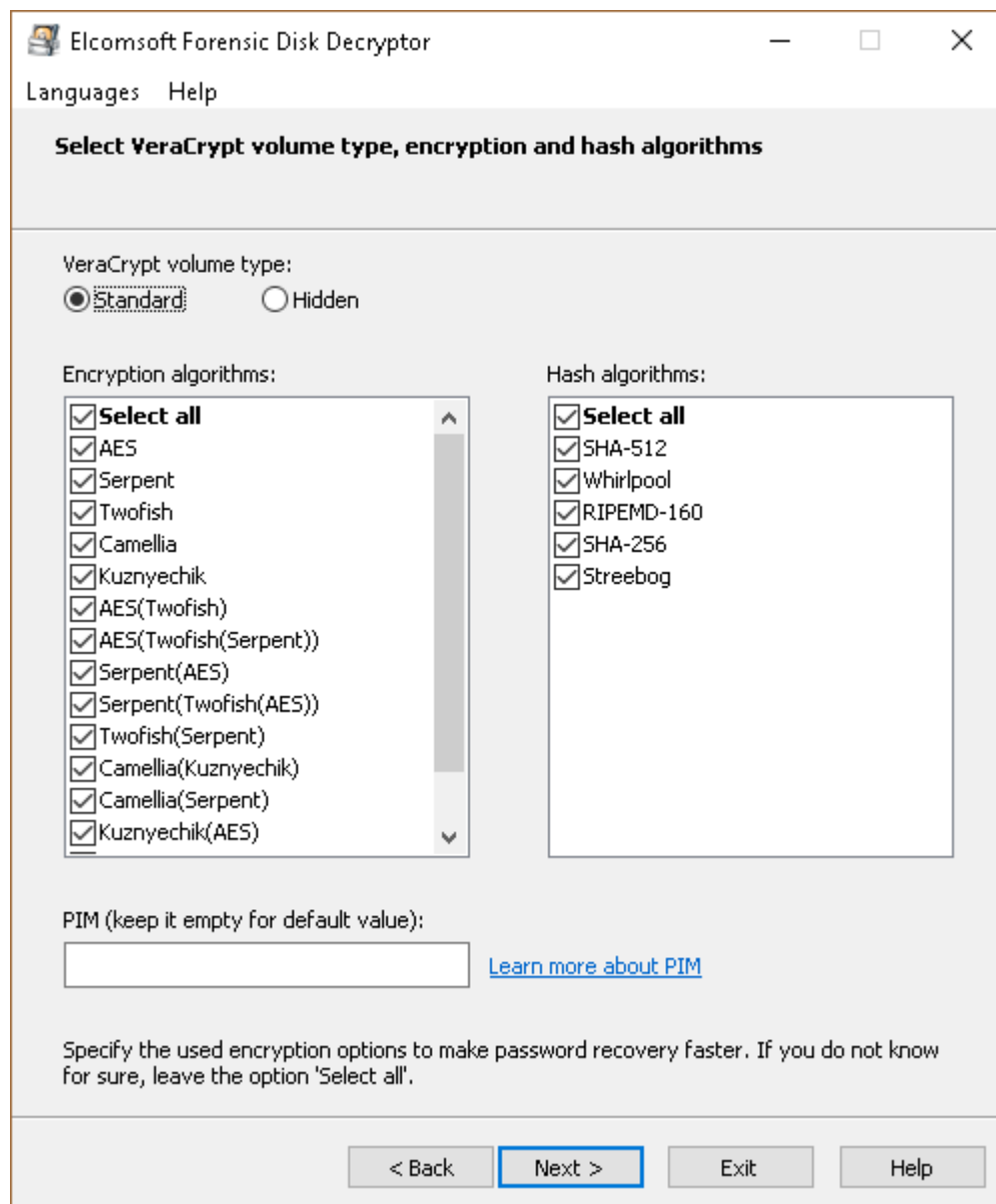
Обратите внимание, что эта функция пока недоступна для разделов APFS, зашифрованных с помощью FileVault2.

5.2.2.5 TrueCrypt и VeraCrypt

Выбор алгоритма шифрования и алгоритма хеширования

При создании файла контейнера или образа пользователь может выбрать дополнительный алгоритм шифрования и алгоритм хеширования.

Если вы знаете алгоритм шифрования или алгоритм хеширования для выбранного контейнера или файла-образа, укажите эти данные в соответствующем окне, - это значительно ускорит процесс дешифрования. Для VeraCrypt имеет смысл указать PIM, если вы знаете, как с ним работать (см. PIM далее).



PIM

PIM (Personal Iterations Multiplier) - это значение, определяющее количество итераций, используемых при выводе ключа заголовка в соответствии с формулами.

Чтобы зашифровать системный раздел, который не использует SHA-512 или Whirlpool (быстрее, но менее безопасно): количество итераций = PIM x 2048

Чтобы зашифровать несистемный раздел или системное шифрование, использующее SHA-512 или Whirlpool (медленнее, но безопаснее): количество итераций = 15000 + (PIM x 1000)

Указывать PIM не обязательно. Если значение PIM оставить равным нулю, будет использоваться значение по умолчанию:

Чтобы зашифровать системный раздел, который использует SHA-256: количество итераций = 200000

Чтобы зашифровать системный раздел, который использует RIPEMD-160: количество итераций = 327661

Чтобы зашифровать несистемный раздел и стандартные крипто-контейнеры, в которых используется RIPEMD-160: количество итераций = 655331

Чтобы зашифровать несистемный раздел и стандартные контейнеры, использующие SHA-256, SHA-512 или Whirlpool: количество итераций = 500000

PIM используется в VeraCrypt с версии 1.12.

5.3 Elcomsoft Password Digger

5.3.1 Introduction

Elcomsoft Phone Digger (EPD) is a Windows tool to decrypt information stored in Mac OS X keychain. The tool dumps the content of an encrypted keychain into a plain XML file for easy viewing and analysis. One-click dictionary building offers the ability to dump all passwords from the keychain into a plain text file, producing a custom dictionary for password recovery tools. A custom dictionary containing all user passwords can be used to speed up password recovery when breaking encrypted documents or backups. Both system and user keychains can be decrypted.

Mac OS X uses keychain to manage system-wide and user passwords. System passwords are stored in the system keychain and include Wi-Fi passwords.

User keychain can contain highly sensitive authentication information such as passwords to Web sites and accounts (including the user's Apple ID password), VPN, RDP, FTP and SSH passwords, passwords to mail accounts including Gmail and Microsoft Exchange, passwords to network shares, and iWork document passwords. Third-party applications can store sensitive information in the keychain. In addition, the keychain may contain private keys, certificates, authentication tokens, and secure notes. Information stored in the keychain is securely encrypted.

While Apple provides Keychain Access, a built-in utility for viewing keychain items, using Keychain Access is less than convenient as the user has to re-enter the password for accessing each individual record.

Elcomsoft Phone Digger dumps information from Mac OS keychain into a plain, decrypted XML file that can be imported into any XML-enabled tool including Microsoft Excel for easily viewing keychain items.

The program that is licensed to you is absolutely legal and you can use it provided that you are the legal owner of all files or data you are going to recover through the use of our software or have permission from the legitimate owner to perform these acts. Any illegal use of our software will be solely your responsibility. Accordingly, you affirm that you have the legal right to access all data, information and files that have been hidden.

You further attest that the recovered data, passwords and/or files will not be used for any illegal purpose. Be aware password recovery and the subsequential data decryption of unauthorized or otherwise illegally obtained files may constitute theft or another wrongful action and may result in your civil and (or) criminal prosecution.

5.3.2 Program information

5.3.2.1 System requirements

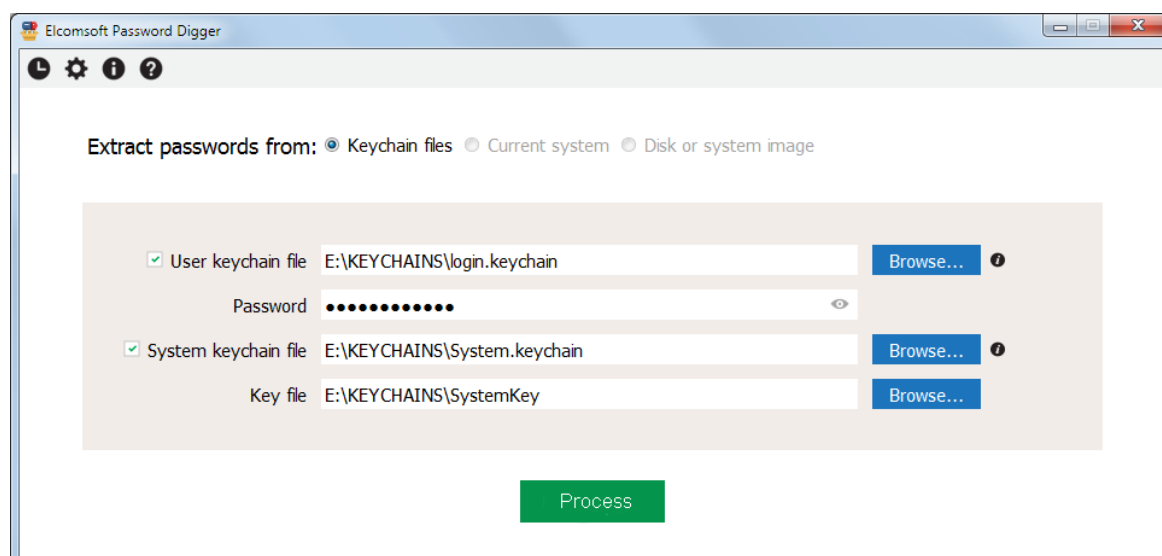
- Windows 7 or above
- about 80 megabytes of free space on hard disk

5.3.2.2 Working with the program

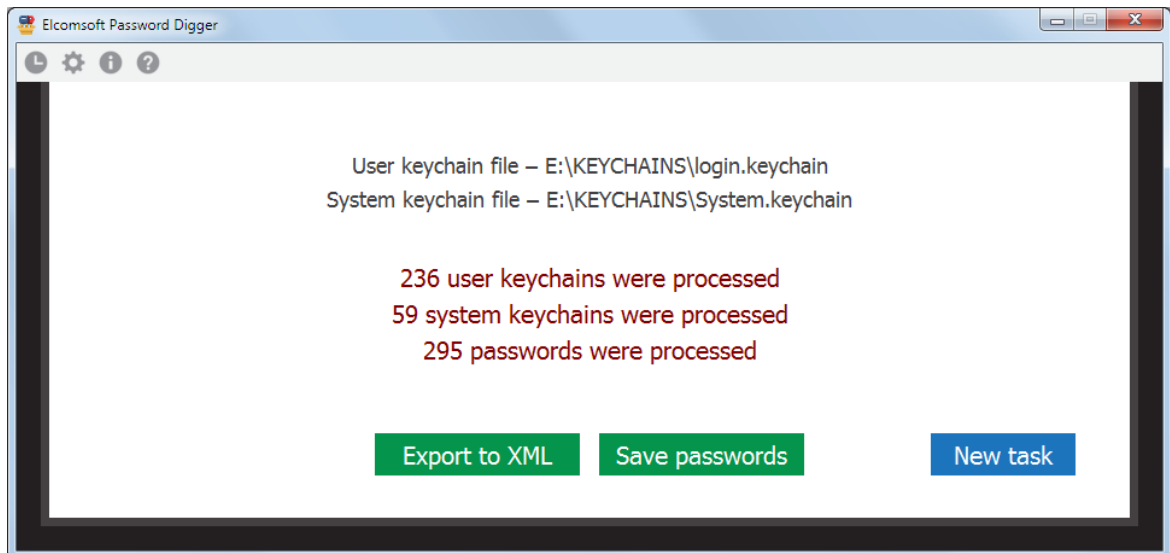
On the main program screen, select the following:

path to user keychain file (login.keychain)
user's password (if set)
path to system keychain file
path to system key file

For more information how/where to get them, please consult [Obtaining keychain files](#) ¹⁵⁰ chapter.



Once the files are selected (you can work with just the user's keychain, or system keychain, or both), please *Process*; if password is not correct, the program will not let you to proceed. The next screen shows how many records are processed in each file:



There you can export all records either to XML file (suitable for further analysis and/or reporting), or save just the passwords, so generating something like a dictionary/w ordlist, e.g. to perform dictionary attacks with other software. The text file with password is sorted alphabetically (with the duplicates removed). XML file contains all the records from the keychains, including not just the passwords, but also the encryption keys, tokens etc, until you set the "Ignore non-password data in XML output" [option](#)^[15].

5.3.2.3 Obtaining keychain files

In order to decrypt the keychain with **EPD**, the first thing you'll need is the keychain itself. In Mac OS, keychain is stored in several physical files. Yet another file holds the decryption key for the system keychain. You'll need all of these in order to gain full access to encrypted information.

If you're acquiring keychain files from a live Mac OS X system, do the following.

- Make a new folder on the desktop (e.g. "KEYCHAINS")
- Open Terminal and issue the following command

```
cd Desktop/KEYCHAINS
```

- Copy the following files into the current folder ("KEYCHAINS"):

```
cp /Users/<username>/Library/Keychains/login.keychain-db .
cp /Library/Keychains/System.keychain .
sudo cp /private/var/db/SystemKey .
```

User's keychain name is "login.keychain-db" on macOS X 10.12 and 10.13, and "login.keychain" on older versions of macOS.

Note that you need superuser access in order to extract SystemKey, a file that contains encryption metadata for decrypting system keychain. You'll be prompted for a password.

Also note there is a final dot at the end of each "copy" command. This is not a formatting error; the dot means that the file is to be copied into the current folder ("KEYCHAINS" in our case).

<user name> is the name of the user whose keychain you are about to extract (currently logged in user is displayed before the "\$" sign).

- Transfer the content of the “KEYCHAINS” folder to the Windows PC where you have **EPD** installed; you may be prompted to enter your Mac administrator's password again (because of special permissions set on *SystemKey* file).

If you have a disk image instead of the live system, extracting files is easier since you won't need superuser access or admin password. Just mount the disk image and use your favorite file manager to copy the required files to your Windows computer.

Mounting the disk image is normally not a problem. If you're dealing with a DMG image, Mac OS has built-in tools to mount it. If the disk image is in EnCase .E01 format, you'll need to use third-party tools to mount the image, such as [AccessData FTK Imager](#) or [GetData Forensic Imager](#).

5.3.2.4 Program options

Apart from the program that records just the main steps you perform in the program (and which is visible right from the program interface by clicking the top-left button on the tool bar), you can set the program to create the log file. By default, logging is disabled; you can set this option to *Normal* (in that case, log will contain just the basic information such as opening/closing the file, decryption started/completed etc) or *Debug* (so including more information, that may help us to locate and fix the problem in an unlucky case if occurs).

The log file is stored in %APPDATA%\Elcomsoft\Password Digger folder.

Ignore non-password data in XML output option allows to filter the items from the keychains that are not actually passwords. That includes encryption keys, certificates, authentication tokens, date/time stamps, and some other data such as UUIDs. Please note that this option affects XML output only; if you export to the text files, the data is always filtered there.

5.3.3 Technical support

5.3.3.1 Contacting us

For technical support, as well as all other requests (general questions, sales, legal) please contact us through the web form located at:

<https://support.elcomsoft.com>

Our fax numbers:

+1 866 448-2703 (US and Canada, toll-free)

+44 870 831-2983 (UK)

+49 18054820050734 (Germany)

Please write in **English** language only.

5.3.3.2 Where to get the latest version

The latest version of **EPD** is always available at:

https://www.elcomsoft.com/purchase/buy.php?product=epd&ref=ELCOM_PROG_PAGE

Other password recovery products (for ZIP and RAR archives, all versions of Microsoft Office; Lotus WordPro, 1-2-3, Approach and Organizer; Adobe Acrobat PDF; Corel Paradox, WordPerfect and QuattroPro; Intuit Quicken and QuickBooks; Microsoft SQL; Sage ACT! and accounting products; email clients such as TheBat!, Eudora, Pegasus etc; instant messengers; Windows 2000/XP/2003/Vista/2008/Windows 7 Encrypting File System on NTFS; Windows logon passwords; Windows PWL/RAS/dial-up/VPN/shares/asterisked passwords; WPA passwords; iTunes and BlackBerry backups and more) are available from our web site at:

<http://www.elcomsoft.com/products.html>

5.3.4 License and registration

5.3.4.1 Copyright and license

Общество с ограниченной ответственностью «ЭлкомСофт», адрес: 12985, Москва, ул. Звездный бульвар д. 21, стр.1, этаж 6, помещение I, комнаты № 17, 17д, 17е, которое является обладателем исключительного права на определенные программы для ЭВМ или компьютерные программы (далее «Программы»), в дальнейшем именуемое Лицензиар, с одной стороны, и Вы – физическое или юридическое лицо, указанное в конкретном Заказе, приобретающее право использования Программы (Программ), в дальнейшем «Вы» или «Лицензиат» и далее совместно именуемые «Стороны» или каждый отдельно – «Сторона» соглашаются заключить лицензионный договор на использование Программы (Программ) на следующих условиях и в следующем порядке.

- Лицензиар является обладателем исключительного права на Программу (Программы), охраняемую авторским правом, а также обладателем иных исключительных прав на результаты интеллектуальной деятельности и средства индивидуализации, связанные с Программой, включая, но не ограничиваясь, исключительное право на ноу-хау.
- Настоящий договор («Договор») является лицензионным договором на использование программ для ЭВМ в форме договора присоединения в значении статьи 428 Гражданского Кодекса Российской Федерации и заключается в соответствии с п.5 статьи 1286 Гражданского Кодекса.
- Если Вы приобретаете право использования Программы у третьего лица (дистрибьютора, реселлера или иного уполномоченного Лицензиаром лица), настоящий Договор регулирует использование Вами Программы в дополнение к договору между Вами и таким третьим лицом.
- Начало использования Вами Программы означает Ваше согласие на заключение настоящего Договора.
- **ВНИМАТЕЛЬНО ПРОЧИТАЙТЕ УСЛОВИЯ НАСТОЯЩЕГО ДОГОВОРА ПЕРЕД УСТАНОВКОЙ ПРОГРАММЫ НА ВАШЕМ УСТРОЙСТВЕ.**
- **ЕСЛИ ВЫ НЕ СОГЛАСНЫ С УСЛОВИЯМИ НАСТОЯЩЕГО ДОГОВОРА, НЕ УСТАНАВЛИВАЙТЕ ПРОГРАММУ НА ВАШЕМ УСТРОЙСТВЕ.**
- Под началом использования понимается установка (инсталляция) Программы на компьютере (устройстве) Лицензиата.

1. Основные термины

Программа (Программы) – программа для ЭВМ ООО «ЭлкомСофт», право на использование которой Вы получаете на основании настоящего Договора и которая указана в конкретном Заказе.

Регистрационный Код - генерируемый Лицензиаром уникальный код, позволяющий осуществлять полнофункциональное использование Программы без временных и иных ограничений.

Ознакомительная Версия – версия Программы, имеющая временные или иные ограничения по использованию/функционалу, предназначенная для оценки возможностей Программы Лицензиатом.

Использование – установка (инсталляция) Программы на технических средствах Лицензиата, а также осуществление действий, связанных с функционированием Программы в соответствии с ее назначением и документацией в зависимости от Типа Лицензии.

Обновления – новые версии Программы.

Декомпилирование – преобразование объектного кода в исходный текст.

Документация – инструкции по использованию Программы, иные текстовые файлы, входящие в дистрибутив Программы, которые Лицензиат получает при установке Программы.

Экземпляр Программы – копия Программы, включая Документацию.

Тип Лицензии – конкретный вид лицензии, определяющий пределы использования Программы Лицензиатом, включая количество устройств (рабочих мест), на которых Лицензиат имеет право использовать Программу одновременно. Типы Лицензии указаны на Интернет сайте Лицензиара <https://www.elcomsoft.ru> в разделе «Продукты» - <https://www.elcomsoft.ru/products.html>, а также в конкретном Заказе.

Типы Лицензии могут время от времени изменяться и все изменения будут опубликованы на Интернет сайте Лицензиара.

Заказ – заказ на получение права использования Программы (Программ), составленный и направляемый Лицензиару в письменной или иной форме (включая через Интернет сайт Лицензиара), в котором указана конкретная Программа (Программы), право на использование которой получает Лицензиат, Тип Лицензии, срок предоставления права использования, размер лицензионного вознаграждения и иные условия, связанные с использованием Программы и получением Лицензиатом права использования Программы. Заказ является приложением к настоящему Договору.

2. Предмет Договора. Объем лицензии.

2.1. Лицензиату предоставляется право использования Программы в пределах, установленных настоящим Договором за вознаграждение, указанное в Заказе, следующими способами на условиях простой неисключительной лицензии:

- В рамках настоящего Договора Лицензиат получает право Использовать Программу только на разрешенном количестве технических устройств в соответствии с Типом Лицензии и иными условиями, определенными в Типе Лицензии и указанными в Заказе. Право Использования предоставляется Лицензиату на срок, указанный в Заказе.

- Если Лицензиат устанавливает Ознакомительную Версию Программы, то Лицензиат имеет право использования Программы безвозмездно на срок, который может быть указан на Интернет сайте Лицензиара или в Заказе и / или с ограниченным функционалом.

2.2. Декомпилирование. Лицензиат имеет право декомпилировать Программу, т.е. воспроизвести и преобразовать объектный код в исходный текст при одновременном соблюдении следующих условий:

- Декомпилирование необходимо для достижения способности к взаимодействию независимо разработанной Лицензиатом программы с другими программами, которые могут взаимодействовать с декомпилируемой программой;

- информация, необходимая для достижения способности к взаимодействию, ранее не была доступна Лицензиату из других источников. Лицензиат обязан сначала запросить эту информацию у Лицензиара и только если Лицензиар не предоставит такую информацию Лицензиату, последний имеет право декомпилировать Программу;

- Эти действия осуществляются в отношении только тех частей декомпилируемой Программы, которые необходимы для достижения способности к взаимодействию;

- Информация, полученная в результате декомпилирования, может использоваться исключительно для достижения способности к взаимодействию независимо разработанной программы с другими программами, не может передаваться иным лицам, за исключением случаев, когда это необходимо для достижения способности к взаимодействию независимо разработанной программы для ЭВМ с другими программами, а также не может использоваться для разработки программы для ЭВМ, по своему виду существенно схожей с декомпилируемой Программой, или для осуществления другого действия, нарушающего исключительное право на Программу.

Никакое иное декомпилирование Программы, кроме случая, указанного выше, не разрешено Лицензиату.

2.3. Запрещается вносить какие-либо изменения в Программу без предварительного письменного разрешения Лицензиара. Если Программа или ее часть предоставлена в форме исходного текста, запрещается без предварительного письменного согласия Лицензиара, любая передача и предоставление такого исходного текста третьим лицам, за исключением

случаев, когда это прямо разрешено какой либо дополнительной лицензией, регулирующей использование такого исходного текста.

2.4. Любое иное использование Программы, не разрешенное настоящим Договором, прямо запрещено. Лицензиату не предоставлены никакие права, кроме прямо указанных в настоящем Договоре.

2.5. Лицензиат не имеет права передавать экземпляр Программы любым третьим лицам, а также передавать право Использования Программы любым третьим лицам без предварительного письменного согласия Лицензиара.

2.6. Лицензиар предоставляет Лицензиату Регистрационный Код по электронной почте не позднее трех (3) рабочих дней после выплаты вознаграждения, указанного в Заказе, Лицензиару.

2.7. Лицензиату предоставляется право Использования Обновлений, которые будут выпущены в свет Лицензиаром в течение двенадцати месяцев со дня предоставления Лицензиату Регистрационного Кода либо иного срока, который указан в Заказе, в объеме и на условиях, указанных в настоящем разделе 2 Договора, за исключением случаев, если предоставление Обновлений будет сопровождаться иным лицензионным договором. Дополнительные условия и порядок предоставления Обновлений могут быть указаны на Интернет сайте Лицензиара или в Заказе.

Для использования любых обновлений, которые будут выпущены в свет по истечении двенадцати месяцев с указанной даты, Лицензиат должен выплатить Лицензиару дополнительное вознаграждение за предоставление права использования Обновлений в соответствии с информацией, указанной на Интернет сайте Лицензиара или в Заказе.

3. Регистрационный Код. Конфиденциальность Регистрационного Кода

3.1. Регистрационный Код является конфиденциальной информацией Лицензиара и является ноу-хау Лицензиара. Соответствующие положения о ноу-хау и защите информации, составляющей коммерческую тайну, законодательства РФ применяются к Регистрационному Коду.

3.2. Лицензиат обязуется использовать Регистрационный Код только в целях, определенных настоящим Договором, исключительно для обеспечения возможности Использования Программы в соответствии с настоящим Договором в зависимости от Типа Лицензии и информации, указанной в Заказе.

Лицензиат обязуется не передавать и предоставлять его третьим лицам любым способом без предварительного письменного согласия Лицензиара, в том числе не размещать Регистрационный Код на любых Интернет – сайтах.

4. Обязанности Лицензиара по технической поддержке

4.1. Лицензиар обязан оказывать техническую поддержку Лицензиату в течение двенадцати месяцев со дня предоставления Лицензиату Регистрационного Кода, в объеме и на условиях, указанных ниже.

4.2. Обязательства Лицензиара по технической поддержке включают в себя ответы на вопросы по электронной почте: support@elcomsoft.com, а также через специальный раздел по технической поддержке на Интернет сайте Лицензиара на странице:

<https://support.elcomsoft.com> . Техническая поддержка, кроме ответов на вопросы, также включает в себя исправление ошибок.

Дополнительные условия выполнения Лицензиаром обязанностей по технической поддержке могут указываться на Интернет сайте Лицензиара на странице <https://support.elcomsoft.com> .

4.3. Техническая поддержка предоставляется в рабочие дни в Российской Федерации за исключением выходных и праздничных дней.

5. Ограничения. Использование в соответствии с законодательством.

5.1. Лицензиат обязуется использовать Программу и любую информацию, полученную в результате такого использования, только в соответствии с законодательством РФ, других

стран, а также положений международного права. Лицензиат обязуется не использовать Программу и любую информацию, полученную в результате использования Программы, с какой-либо противоправной целью, включая незаконный доступ к информации третьих лиц, или в целях, противоречащих принципам этики, гуманности и морали.

Все лицензируемые Вам Программы являются полностью легальными и Вы имеете право их использования, при условии, что Вы являетесь законным владельцем всех файлов и данных, которые Вы собираетесь восстановить или доступ к которым Вы собираетесь получить при помощи Программ, Вы являетесь законным владельцем любых устройств или учетных записей, доступ к которым Вы собираетесь получить при помощи Программ или у Вас есть соответствующее разрешение законного владельца на выполнение указанных действий или у Вас есть такое право на основании Вашего национального законодательства (например, Вы представляете правоохранительные органы или иные компетентные органы государства, которые имеют право получения доступа к информации и данным и такой доступ необходим в ходе проведения действий и процедур, предусмотренных законодательством).

Любое использование Программ в нарушение законодательства является только Вашей ответственностью.

Вы подтверждаете, что у Вас есть законное право получить доступ ко всем данным, информации и файлам, которые закрыты.

Вы также подтверждаете, что восстановленные или полученные иным образом данные, пароли и/или файлы не будут использованы в каких-либо противозаконных целях.

Вы осознаете, что несанкционированное восстановление паролей и иных данных или несанкционированный доступ к информации и данным может являться преступлением или правонарушением и может привести к разным видам ответственности.

5.2. С целью предотвращения незаконного использования Программа может установить на Вашем устройстве технические меры защиты авторских прав и иных прав на результаты интеллектуальной деятельности. Данные меры будут использованы с целью контроля использования Программы и любых Обновлений в соответствии с настоящим Договором. В результате установки таких технических мер Лицензиар не будет получать никакой персональной информации (включая персональные данные) о Лицензиате.

5.3. Уведомления об авторских правах. Программа может содержать уведомления о принадлежности исключительного права на нее Лицензиару и иные уведомления об исключительных правах. Вы не имеете право удалять или изменять каким-либо образом такие уведомления и информацию.

6. Вознаграждение

6.1. Вознаграждение за право использования указано в Заказе на конкретную Программу (Программы).

7. Ограниченная гарантия

7.1. Лицензиар гарантирует, что Программа будет функционировать в соответствии с Документацией на Программу при условии соблюдения порядка ее использования, предусмотренного Документацией и настоящей Лицензией в течение 90 (девяносто) дней со дня получения Лицензиатом Регистрационного Ключа.

Функционирование с незначительными отступлениями от Документации не считаются дефектами.

7.2. Данная гарантия недействительна, если использование Программы осуществляется с нарушениями правил и требований, указанных в Документации и с нарушениями настоящего Договора и/или законодательства, включая внесение любых изменений в Программу без согласия Лицензиара.

7.3. Лицензиар не предоставляет никаких иных гарантий кроме указанной выше и не несет никакой материальной ответственности за любые убытки Лицензиата, включая упущенную выгоду, вытекающие из использования или невозможности использования Программы, не получения Лицензиатом какого-либо результата от использования Программы, не связанные с

нарушением Лицензиаром настоящей гарантии и обязательств по технической поддержке, указанных в Договоре.

7.4. Единственным средством защиты Лицензиата в случае нарушения указанной выше гарантии является: а) возврат выплаченного вознаграждения или б) замена дефектного носителя, если Программа предоставлена на материальном носителе или в) исправление ошибок в течение разумного периода времени. В случае претензий к функционированию Программы Лицензиат обязан направить Лицензиару максимально полную информацию о проблеме, включая информацию об устройстве (устройствах) Лицензиата, на которых используется Программа, информацию об иных программах, используемых Лицензиатом, которые могут повлиять на функционирование Программы, информацию о любых файлах, документах и материалах, в связи с которыми Лицензиат использует Программу и любую иную информацию, запрошенную Лицензиаром.

Указанная в настоящем разделе 7 гарантия не применяется в случае не предоставления Лицензиатом полной информации о проблеме по запросу Лицензиара.

8. Интеллектуальная собственность Лицензиара

8.1. Программа и вся Документация на нее являются объектом авторского права и охраняются авторским правом, а именно частью 4 Гражданского Кодекса РФ и международными соглашениями в области авторского права, а также иными положениями законодательства об интеллектуальных правах (интеллектуальной собственности). Программы, принципы и способы, связанные с Программой, также могут охраняться как объекты патентного права, включая, но не ограничиваясь, изобретения, в РФ и иных странах.

8.2. Исходный текст (код) Программ и Регистрационный Код являются ноу-хау и информацией, составляющей коммерческую тайну Лицензиара.

8.3. Лицензиат не приобретает никаких прав на Программу, кроме тех, которые прямо указаны в настоящем Договоре. Лицензиату предоставлена ограниченная неисключительная лицензия на Программу в пределах настоящего Договора.

9. Ответственность за нарушение Договора

9.1. В случае нарушения обязательств по сохранению конфиденциальности Регистрационного Кода Лицензиат возмещает Лицензиару убытки в полном размере, включая упущенную выгоду.

9.2. Ответственность за нарушение иных обязательств Сторон определяется в соответствии с законодательством Российской Федерации.

10. Срок действия Договора

10.1. Датой заключения настоящего Договора считается дата оплаты вознаграждения за предоставление права использования Программы. Договор действует на срок, указанный в конкретном Заказе.

Договор применяется к отношениям Сторон, возникшим со дня начала использования Программы в соответствии с преамбулой Договора.

10.2. Лицензиар имеет право отказаться от исполнения Договора и расторгнуть Договор в случае нарушения Лицензиатом условий использования Программ, установленных настоящим Договором, включая, но не ограничиваясь условия, установленные в разделе 2 Договора, а также нарушения обязательств по сохранению конфиденциальности Регистрационного Кода, установленного в разделе 3 Договора или нарушения Лицензиатом иных обязательств по настоящему Договору. В таком случае Лицензиар уведомляет Лицензиата о расторжении Договора, и Договор считается прекращенным с даты направления уведомления по электронной почте по адресу Лицензиата, указанному в Заказе или иным образом.

10.3. После расторжения или прекращения Договора по любому основанию Лицензиат не имеет права использовать Программу каким-либо образом и должен немедленно удалить все экземпляры Программ и незамедлительно уведомить об этом Лицензиара по электронной почте по адресу: info@elcomsoft.com.

11. Публичность

11.1. Лицензиат настоящим соглашается, и Лицензиар имеет право публично ссылаться на тот факт, что Лицензиат является его клиентом (пользователем - Лицензиатом), в том числе ссылаться на Лицензиата и на факт использования Программы Лицензиатом в маркетинговых материалах, аналитических и иных материалах и пресс-релизах, не раскрывая какой-либо конфиденциальной информации Лицензиата.

11.2. Лицензиат имеет право отказать Лицензиару в реализации указанного выше в 11.1 права на публичность либо отозвать свое согласие на такое использование, направив сообщение по электронной почте по адресу: info@elcomsoft.com с указанием в теме письма «Отзыв согласия на Публичность».

12. Заключительные и переходные положения

12.1. Ссылки на соответствующие страницы Интернет сайта Лицензиара включены в настоящий Договор как его части и (или) приложения к нему. Положения и условия, размещенные на соответствующих страницах Интернет сайта Лицензиара, применяются к использованию Программы Лицензиатом.

12.2. В случае, если компетентный суд признает какое-либо из условий настоящего Договора недействительными, Договор продолжает действовать в остальной части.

12.3. К настоящему Договору применяется материальное право Российской Федерации без отсылки к нормам международного частного права.

Любые споры, вытекающие из настоящего Договора, подлежат рассмотрению в компетентном суде г. Москвы.

12.4. Настоящий Договор также размещен на Интернет – сайте Лицензиара по адресу:

https://www.elcomsoft.ru/Elcomsoft_EULA_ru.pdf.

5.3.4.2 Registration

Free trial version of **EPD** shows only some first symbols of decrypted passwords.

You can place an order online using the following order form:

https://www.elcomsoft.com/purchase/buy.php?product=epd&ref=ELCOM_PROG_PAGE

Please note that there are some small processing charges for orders placed by fax, by check/money order or with bank/wire transfer. European customers are also charged VAT.

More information about all payment options is available at ordering page on EcomSoft website:

https://www.elcomsoft.com/purchase/buy.php?product=epd&ref=ELCOM_PROG_PAGE

On payment approval (for online orders, usually within a few minutes), we'll send you the registration key which will remove all limitations of the unregistered version.

5.3.4.3 Legal notices

Qt, LGPL, ...

Copyright (c) 1998-2011 The OpenSSL Project. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgment: "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (<http://www.openssl.org/>)"
4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.
5. Products derived from this software may not be called "OpenSSL" nor may "OpenSSL" appear in their names without prior written permission of the OpenSSL Project.
6. Redistributions of any form whatsoever must retain the following acknowledgment: "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (<http://www.openssl.org/>)"

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT "AS IS" AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

=====

This product includes cryptographic software written by Eric Young (eyay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

Copyright (C) 1995-2004 Jean-loup Gailly and Mark Adler

This software is provided 'as-is', without any express or implied warranty. In no event will the authors be held liable for any damages arising from the use of this software.

Permission is granted to anyone to use this software for any purpose, including commercial applications, and to alter it and redistribute it freely, subject to the following restrictions:

1. The origin of this software must not be misrepresented; you must not claim that you wrote the original software. If you use this software in a product, an acknowledgment in the product documentation would be appreciated but is not required.
2. Altered source versions must be plainly marked as such, and must not be misrepresented as being the original software.
3. This notice may not be removed or altered from any source distribution.

Jean-loup Gailly jloup@gzip.org
 Mark Adler madler@alumni.caltech.edu

Copyright (c) 1996 - 2012, Daniel Stenberg, <daniel@haxx.se>.

All rights reserved.

Permission to use, copy, modify, and distribute this software for any purpose with or without fee is hereby granted, provided that the above copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OF THIRD PARTY RIGHTS. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Except as contained in this notice, the name of a copyright holder shall not be used in advertising or otherwise to promote the sale, use or other dealings in this Software without prior written authorization of the copyright holder.

Copyright 2008, Google Inc.

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

* Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

* Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

* Neither the name of Google Inc. nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Code generated by the Protocol Buffer compiler is owned by the owner of the input file used when generating it. This code is not standalone and requires a support library to be linked with it. This support library is itself covered by the above license.

5.4 Elcomsoft System Recovery

5.4.1 Введение

Elcomsoft System Recovery помогает системным администраторам сбрасывать или восстанавливать пароли к локальным учетным записям Windows и учетной записи Microsoft (во всех версиях Windows), давать права администратора любой учетной записи пользователя, сбрасывать пароли с истекшим сроком действия или экспортировать хэши паролей для восстановления в автономном режиме. Программа может обнаруживать следы шифрования и создавать образы дисков для криминалистической экспертизы. Elcomsoft System Recovery поставляется с загрузочной средой Windows PE.

Характеристики и преимущества

- Загрузочная среда Windows PE (Preinstallation Environment) по лицензии Microsoft
- Восстанавливает или сбрасывает пароли пользователей и администраторов
- Восстановление исходного пароля может предоставить автоматический доступ к файлам, зашифрованным с использованием EFS.
- Разблокирует и дает доступ учетным записям пользователей и администраторов.
- Назначает права администратора любой учетной записи пользователя
- Сбрасывает или отключает параметры истечения срока действия пароля
- Широкая совместимость с оборудованием и встроенная поддержка FAT и NTFS
- Естественный графический интерфейс Windows для удобной работы

- Поддерживает Windows NT 4, Windows 2000, Windows XP, Windows Vista, Windows 7, Windows 8 / 8.1, Windows 10
- Поддерживает Windows Server 2000/2003/2008/2012/2016/2019 (включая пароль администратора домена и пароли всех пользователей)
- Поддерживает US и локализованные версии Windows, а также мультиязычные имена пользователей и пароли.
- Автоматически определяет все установки ОС Windows
- Возможность сбрасывать хешированные пароли из файлов SAM / SYSTEM или из БД Active Directory для дальнейшего анализа и восстановления пароля в автономном режиме
- Возможность сбросить кэшированные учетные данные домена
- Дамп ключей шифрования для защищенных дисков
- Поддерживает учетные записи Microsoft Live!
- Сбрасывает или ищет SYSKEY пароль
- Сброс пароля для кэшированных учетных записей домена
- Дамп ключей шифрования диска
- Разблокирует диски, зашифрованные с помощью BitLocker
- Находит зашифрованные виртуальные машины и извлекает метаданные шифрования для последующего восстановления пароля
- Создает образы дисков или разделов для криминалистического анализа

Готов к загрузке, мгновенная разблокировка

Elcomsoft System Recovery поставляется в виде программы, которая позволяет быстро создать загрузочный диск (CD или USB). Не нужно создавать доступ к установочным дискам Windows, чтобы их сделать. ElcomSoft лицензировала среду предустановки Windows (Windows PE) непосредственно у Microsoft, что позволяет компании распространять полностью рабочую загрузочную среду Windows на основе Windows 10.

Если в вашей учетной записи Windows нет файлов, зашифрованных с помощью EFS, вариант мгновенной разблокировки - самый быстрый и простой способ получить доступ к учетным записям пользователей и администраторов. Elcomsoft System Recovery сбрасывает забытые пароли, используя новый пароль, предоставленный вами, что позволяет мгновенно войти в систему без трудоемких операций по восстановлению пароля.

Широкая совместимость

Загрузочная среда Elcomsoft System Recovery поддерживает множество аппаратных компонентов, включая самые популярные контроллеры жестких дисков, благодаря встроенным драйверам Windows. В отличие от различных сред эмуляции, Elcomsoft System Recovery полностью совместим с последними версиями файловых систем Microsoft, включая последние версии FAT (FAT32, exFAT) и NTFS.

Восстанавливает уникальные пароли

Elcomsoft System Recovery может восстановить уникальный пароль с помощью стандартных паролей и словарных атак. Elcomsoft System Recovery проверяет места, где кэшируются системные пароли, часто позволяя мгновенно восстановить пароль.

Автономное восстановление паролей стало возможным благодаря выгрузке хешированных паролей из файлов SAM / SYSTEM или базы данных Active Directory для дальнейшего анализа в автономном режиме. Мы рекомендуем использовать для восстановления системных паролей

наш продукт - [Elcomsoft Distributed Password Recovery](#) - поддерживающий вычисления на графических процессорах.

5.4.2 О программе

5.4.2.1 Важно: О совместимости

- Вы можете просматривать или изменять свойства учетной записи (Аккаунт Администратора, Аккаунт заблокирован / отключен, Срок действия пароля истек, Срок действия пароля не истечет) только для локальных учетных записей пользователей, *но не для учетных записей AD*.
- Некоторым компьютерам могут потребоваться сторонние драйверы запоминающих устройств (для RAID, SCSI, SAS и подобных устройств хранения). Вы можете загрузить дополнительные драйверы после загрузки ESR с USB-накопителя или использовать драйверы, поставляемые с программой.
- Если вы используете read-only носитель для загрузки ESR (например, CD / DVD), вы не сможете сохранить хэши паролей обратно на загрузочный диск. Используйте другой носитель для сохранения файлов.

Elcomsoft System Recovery совместим с современными и устаревшими компьютерами. Хотя современные компьютеры оснащены UEFI, все еще встречаются ПК, на которых используется устаревшая версия BIOS. Некоторые производители, поставляющие более новые ПК с UEFI, все еще используют термин «BIOS», чтобы избежать путаницы. Однако подавляющее большинство компьютеров, проданных за последнее десятилетие, оснащены UEFI вместо BIOS.

Если на вашем компьютере работает UEFI, особых требований к загрузочному носителю нет. Однако, если вы анализируете устаревший ПК, оснащенный BIOS, вам необходимо создать загрузочный носитель размером не более 32 ГБ. Есть некоторые другие ограничения, о которых следует помнить при анализе устаревших компьютеров с BIOS.

При создании загрузочного носителя ESR предлагает на выбор три варианта загрузки: BIOS, UEFI x64 и UEFI x32. Вы должны выбрать подходящий вариант для целевого компьютера. Подавляющее большинство современных компьютеров используют **UEFI x64**, он же в ESR используется по умолчанию. Для устаревших ПК выберите **BIOS**. Последний вариант, **UEFI x32**, используется в особых случаях: для тонких-и-легких устройств и неттопов, построенных на определенных поколениях платформы Intel Atom, которые, хотя и поддерживают 64-битные инструкции, ограничены 32-битными.

Требования для загрузки устаревших компьютеров - загрузки с BIOS

Существуют особые требования при загрузке с USB-носителя для компьютеров с устаревшей BIOS (как это определено у Microsoft для Windows PE).

- Размер USB-носителя не может быть меньше 256 мегабайт.
- Размер USB-носителя не может превышать 32 ГБ.
- USB-носитель должен быть типа Съёмный (Removable), а не Встроенный (Fixed).
- USB-носитель должен быть первым в списке загрузочных устройств в BIOS.
- BIOS компьютера должен поддерживать расширенное прерывание BIOS INT 13h (xINT13) для USB-носителя.
- BIOS компьютера должен поддерживать загрузку с USB-носителя.
- USB-контроллер компьютера должен поддерживать bulk-only transport (BOT).

Обратите внимание, что эти требования не распространяются на достаточно современные компьютеры с UEFI. (Для информации) производители начали использовать UEFI вместо BIOS примерно в 2007 году.

ESR был разработан с расчетом на максимальную совместимость и по идее должен иметь возможность загрузаться даже с внешнего жесткого диска (USB или FireWire), включая диски размером более 32 ГБ, но некоторые ограничения все еще присутствуют.

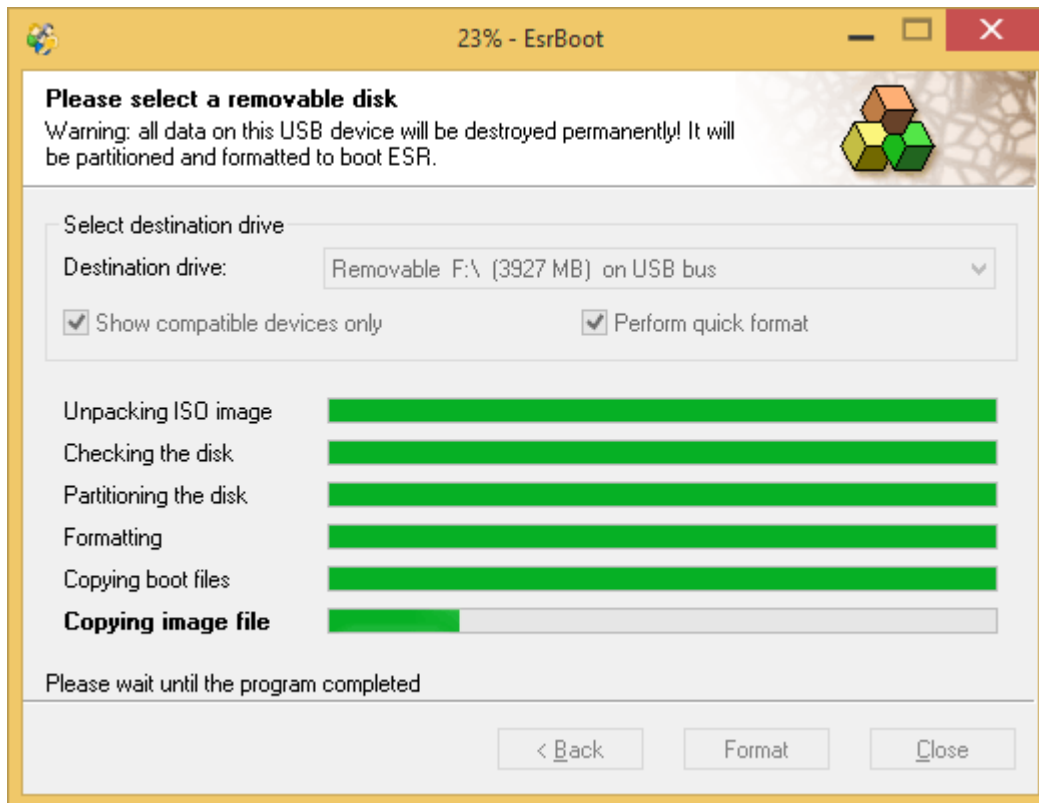
Обратите внимание, что после сброса пароля вы можете потерять доступ к пользовательским: данным для входа на веб-страницах, данным для входа на файловый сервер (file share), данным, зашифрованным с DPAPI, файлам с шифрованием EFS и сертификатам с закрытыми ключами (подписанная / зашифрованная электронная почта).

5.4.2.2 Создание загрузочного носителя

Чтобы создать загрузочный USB-носитель, запустите утилиту ESRBOOT и выполните несколько простых шагов:

- Примите лицензионное соглашение ElcomSoft
- Введите свой лицензионный ключ
- Выберите вариант создания загрузочного USB-накопителя.
- Вставьте USB-устройство, которое вы собираетесь сделать загрузочным (**предупреждение: все данные на этом диске будут удалены!**)
- Выберите USB-устройство в выпадающем списке в Destination drive. Выберите Показать только совместимые устройства (Show compatible devices only), чтобы отфильтровать внутренние устройства хранения; и не выбирайте, только если ESRBOOT не показывает ваш съемный диск.
- Программа проверяет, можно ли настроить устройство для загрузки ESR; создает специальный раздел; создает логический диск; форматирует диск; делает этот диск загрузочным; затем копирует файлы (Windows PE и ESR т. е. сам себя).

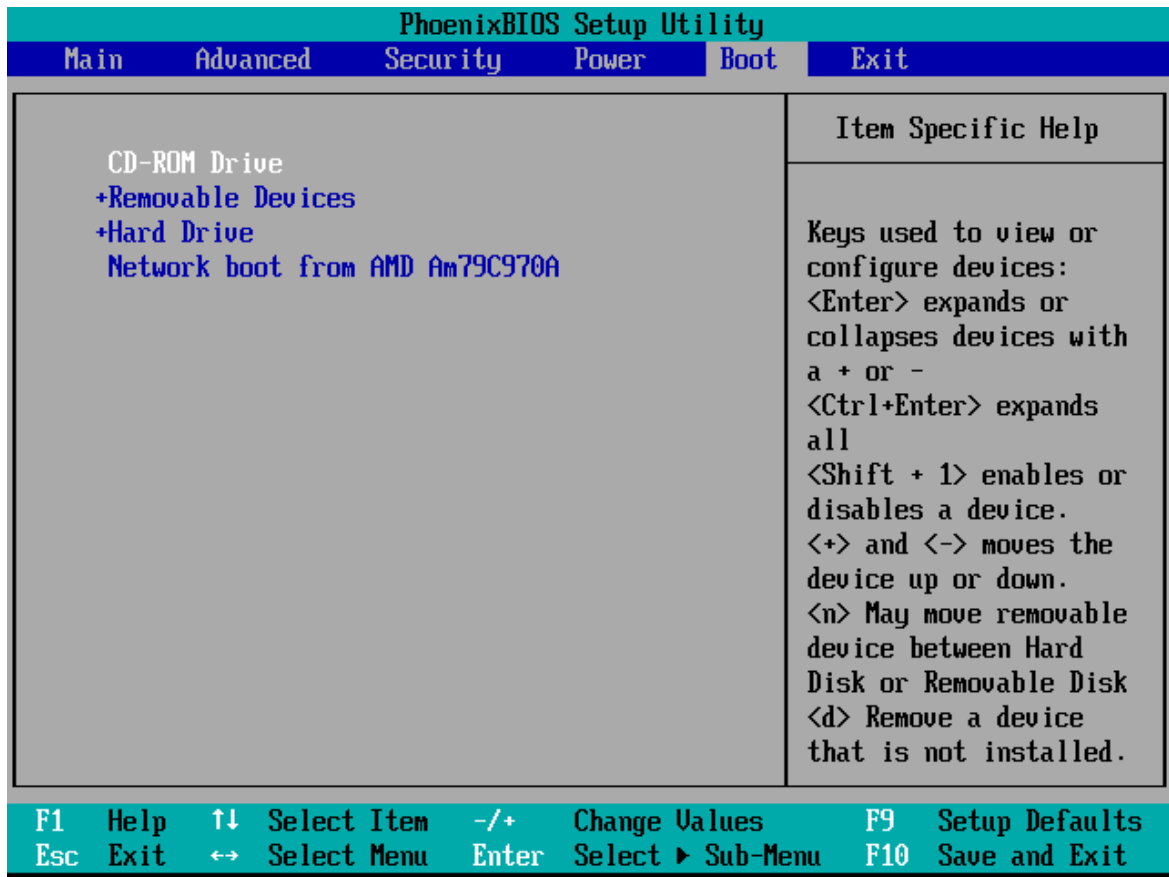
Обратите внимание: при создании загрузочного носителя ESR предлагает на выбор три варианта загрузки: BIOS, UEFI x64 и UEFI x32. Вы должны выбрать подходящий вариант для целевого компьютера. Подавляющее большинство современных компьютеров используют **UEFI x64**, он же в ESR используется по умолчанию. Для устаревших ПК выберите **BIOS**. Последний вариант, **UEFI x32**, используется в особых случаях: для тонких-и-легких устройств и неттопов, построенных на определенных поколениях платформы Intel Atom, которые, хотя и поддерживают 64-битные инструкции, ограничены 32-битными.



5.4.2.3 Как использовать ESR

Загрузка с CD или USB-устройства

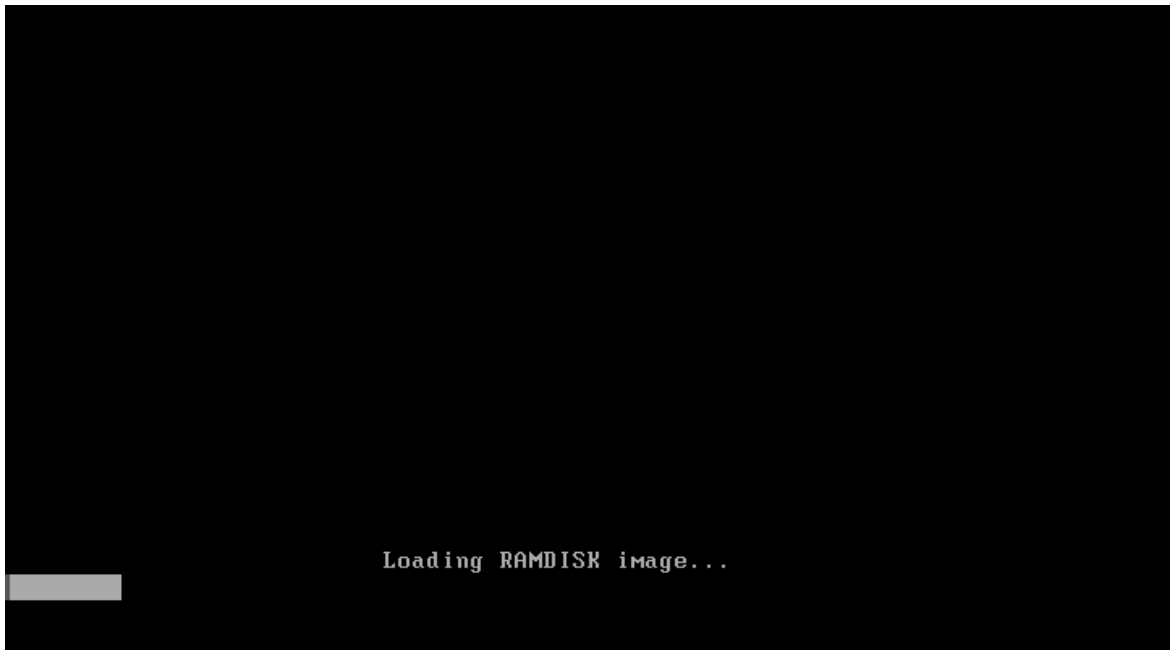
Чтобы загрузить компьютер с CD или USB, внесите соответствующие изменения в BIOS или UEFI-shell так, чтобы дисковод или USB-устройство отображалось как первое в списке загрузочных устройств:



Затем вставьте загрузочный носитель ESR и перезагрузитесь.

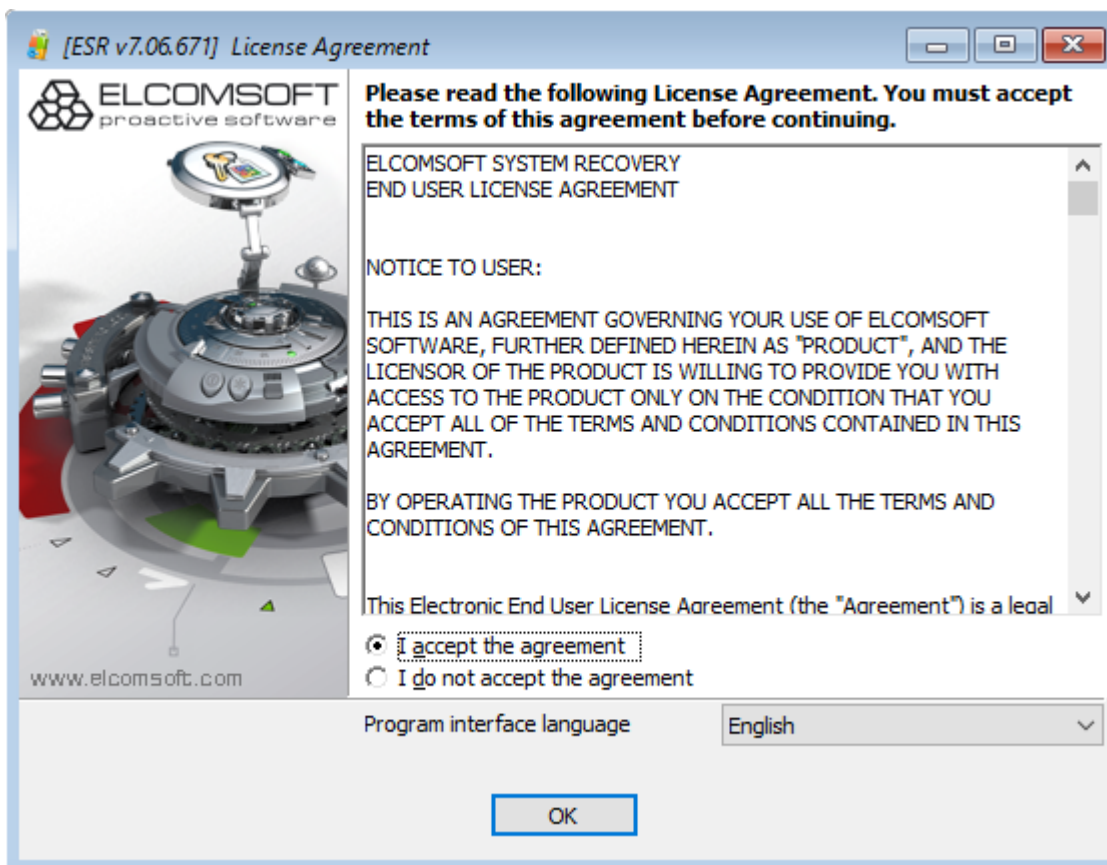


Нажмите любую клавишу, и ESR начнет загрузку (создавая RAM-диск и загружая Windows PE):



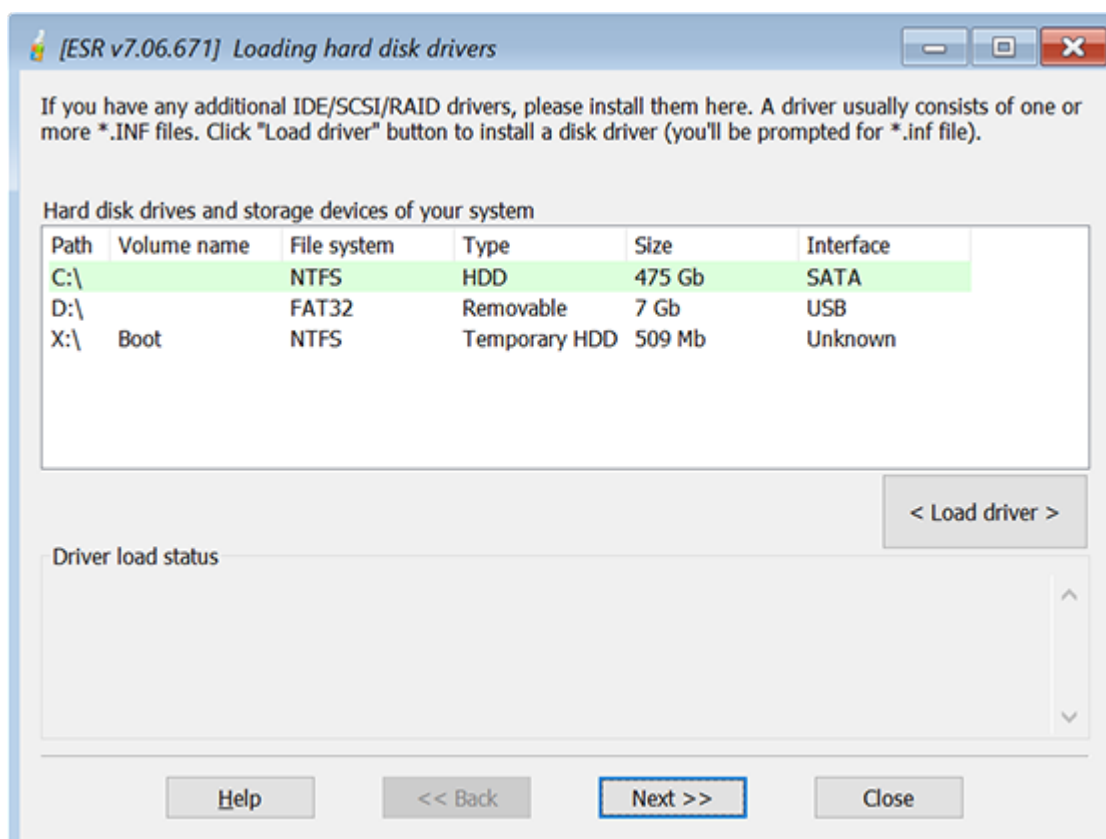
Если вы загружаетесь с USB-устройства, действия в целом, за исключением того, что во время загрузки не будет сообщения «Нажмите любую клавишу...» (Press any key...).

При загрузке ESR вам будет представлено лицензионное соглашение; нажмите "принять" (I accept the agreement), чтобы продолжить:



Драйверы запоминающих устройств

Если в вашей системе используется нестандартный адаптер запоминающего устройства (например, в некоторых случаях это SerialATA, SCSI, RAID или SAS), вам может потребоваться указать соответствующие драйверы вручную:



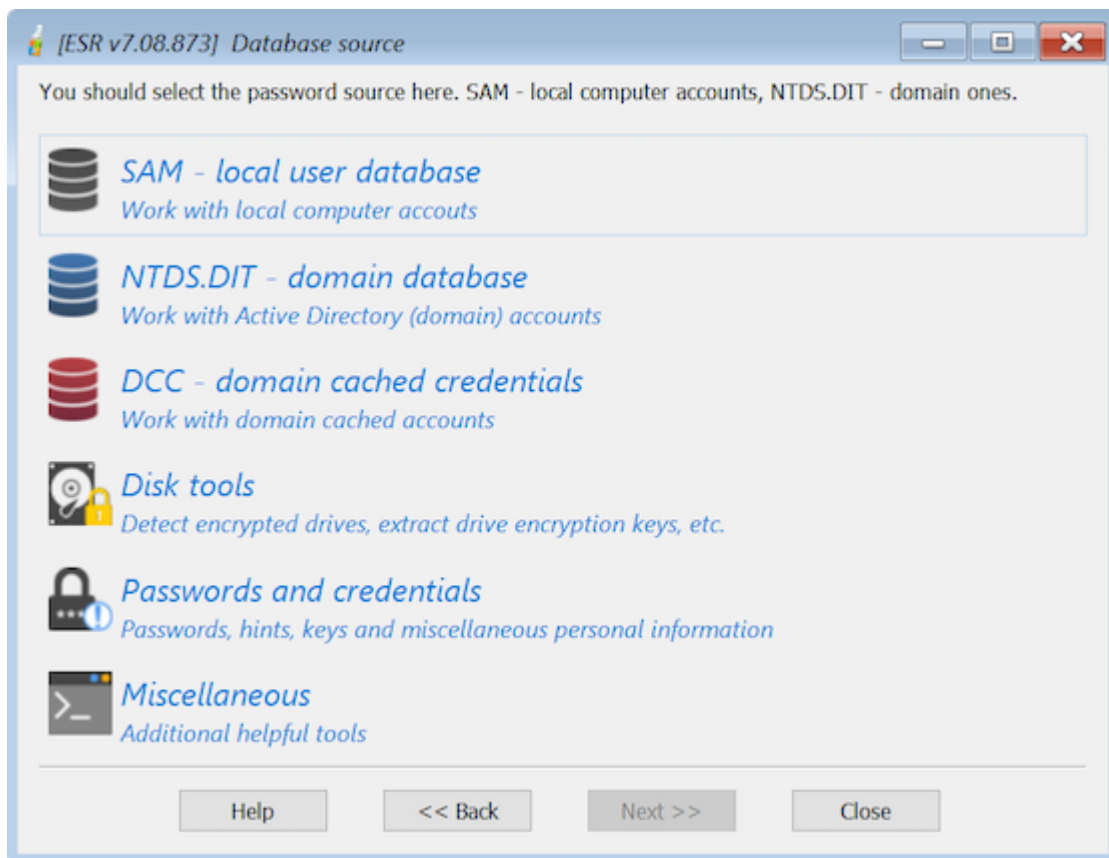
Отобразится список локальных дисков. Если вы не видите системный раздел, нажмите «Загрузить драйвер» и найдите диск, содержащий соответствующие драйверы. ESR загрузит указанный драйвер и обновит список доступных разделов. В окне состояния, где отображается информация о загрузке драйвера появится уведомление об успешной загрузке, если все пройдет хорошо.

ДБ-источник и режим работы

ДБ-источник

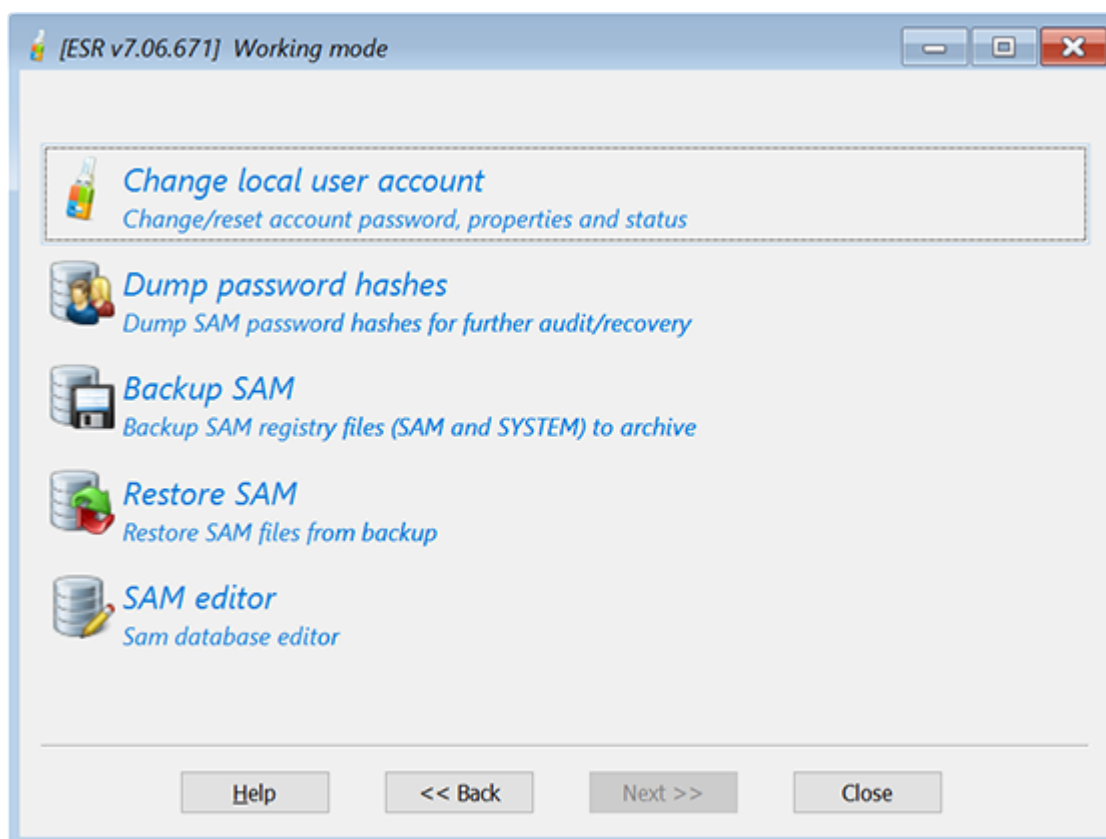
Вы можете выбрать локальные учетные записи и учетные записи Active Directory. Для работы с AD требуется запуск ESR на сервере (domain controller) под управлением Windows Server 2000/2003/2008/2012/2016/2019.

- Работа с локальными учетными записями (SAM)
- Работа с учетными записями Active Directory (ntds.dit)
- Работа с кешированными учетными записями домена
- Инструменты для поиска ключей шифрования дисков
- Дополнительные утилиты



Режим работы

- Изменение пароля и свойств аккаунта
- Дамп хэшей паролей для дальнейшего аудита / восстановления
- Резервное копирование реестра или Active Directory для архивации
- Восстановление реестра или AD из резервной копии
- Редактор базы данных SAM
- Сброс пароля DSRM



Если вы уже изменили свойства учетной записи или пароль (/пароли) и хотите отменить изменения, выберите последний вариант: «Восстановить реестр или AD из резервной копии» (Restore Registry or AD from backup). Вам будет предложено указать расположение резервной копии реестра Windows или базы данных AD.

В противном случае выберите "Изменить пароль и свойства учетной записи" (Change account password and properties) (для изменения / сброса паролей для учетных записей пользователей, разблокировки отключенных или заблокированных учетных записей и т. д.) Или "Дамп хэшей паролей" (Dump password hashes), чтобы выгрузить хэши паролей из AD или реестра в текстовый файл для дальнейшего анализа/восстановления в [Proactive Password Auditor](#) или [Elcomsoft Distributed Password Recovery](#). Наконец, вы можете создать резервную копию реестра (SAM, SECURITY и SYSTEM) или базы данных Active Directory (ntds.dit).

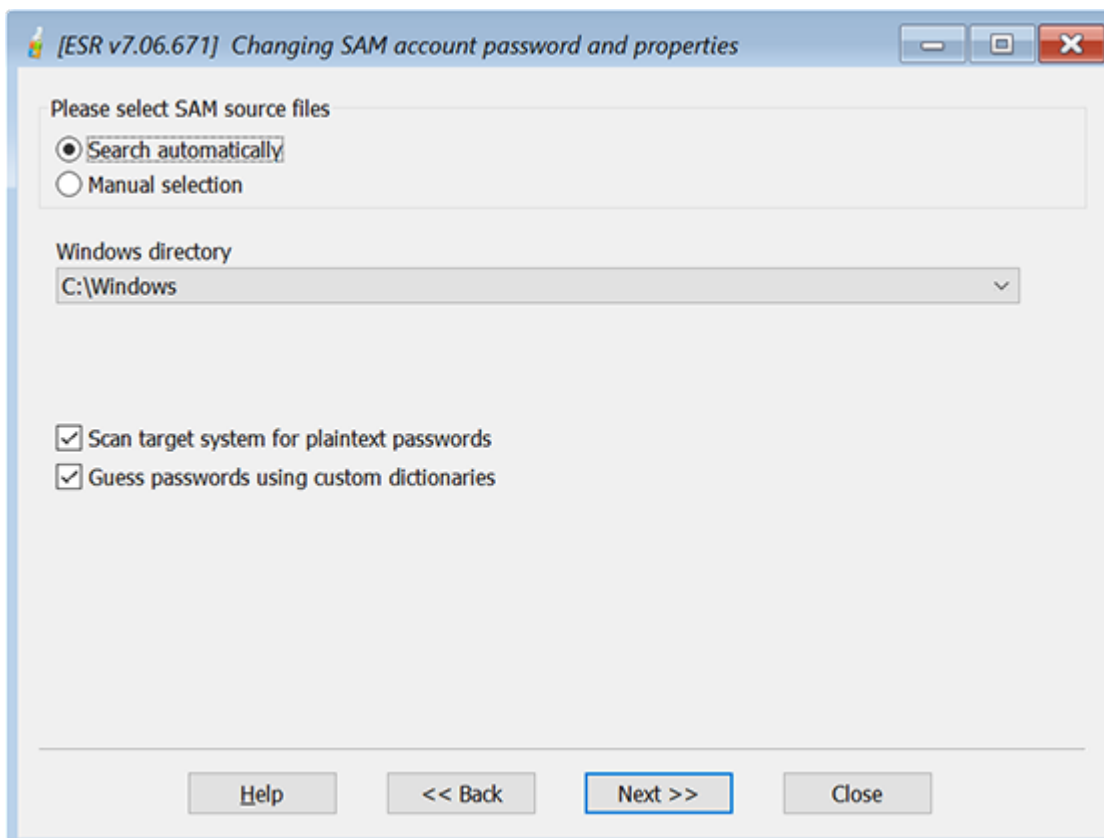
Когда вы дампаете локальные хэши паролей из SAM, хэши истории паролей также извлекаются и сохраняются в файле дампа.

Хэши паролей могут быть сохранены как стандартный файл дампа в ASCII или UNICODE. После сброса программа предлагает открыть файл в Блокноте; **обратите внимание, что если имена пользователей или комментарии используют не английский алфавит, они будут отображаться правильно только в UNICODE.**

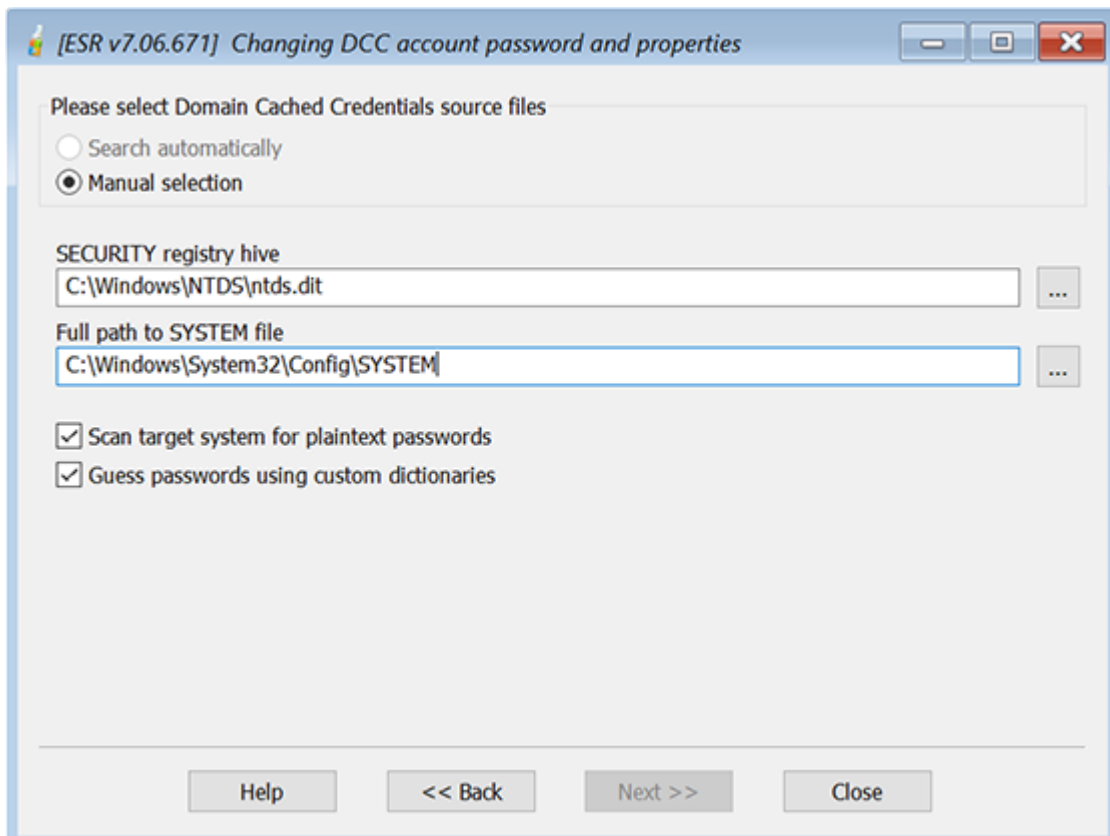
Наконец, [редактор базы данных SAM](#)¹⁷⁸ редактор базы данных SAM позволяет редактировать все поля в базе данных SAM, которые содержат расширенные свойства учетных записей локальных пользователей.

Выбор ОС или расположения файлов SAM/AD

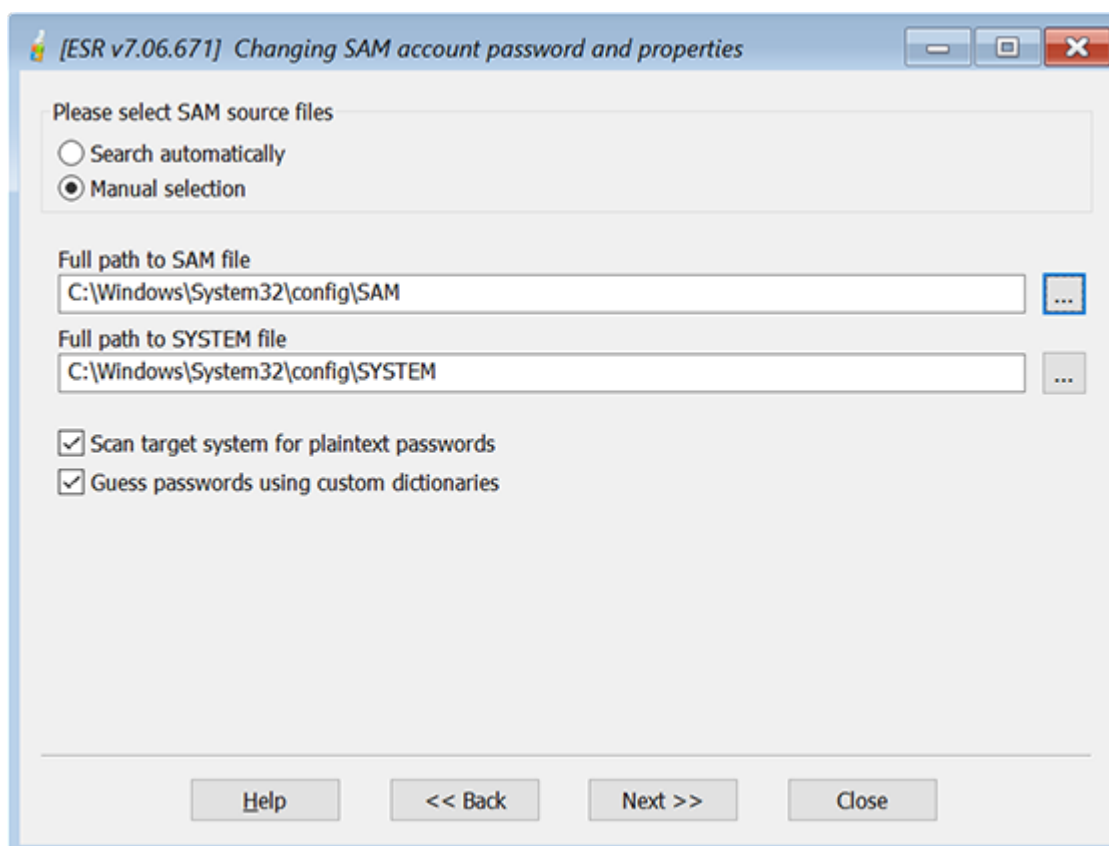
После того, как вы выбрали БД-источник (SAM, DCC или AD) и режим работы, вам будет предложено выбрать операционную систему для работы. Если ваша система использует нестандартные адаптеры запоминающих устройств, такие как SCSI или SAS, которые не поддерживаются ESR, скорее всего вам придется указать драйверы вручную; подробнее в [драйверы запоминающих устройств](#)^[166]. При выборе "Авто" (Search automatically) вы можете выбрать системную папку из выпадающего списка:



При выборе "Вручную" (Manual selection) необходимо самостоятельно выбрать расположение базы данных AD и файла системного реестра (SYSTEM Registry file или SYSTEM) с помощью кнопки [...] справа:



Либо выберите расположение файлов SAM, SECURITY и SYSTEM:



В ручном режиме мы рекомендуем сначала выбрать расположение файла SYSTEM, чтобы расположение SAM / SECURITY (или AD) было заполнено автоматически. Расположение файлов SAM, SECURITY и SYSTEM по умолчанию следующее:

```
%WINDOWS%\SYSTEM32\CONFIG\
```

База данных AD (ntds.dit) обычно хранится в папке:

```
%WINDOWS%\NTDS\
```

Если вы не видите локальные диски при просмотре файлов SAM / SECURITY / SYSTEM / AD, это может означать, что у вас не установлены необходимые драйверы, такие как SerialATA, SCSI или RAID. Возможно, вам потребуется указать их во время процесса загрузки (подробнее в [Загрузка с CD или UDB-устройств](#)¹⁶³).

Если ваша система использует нестандартный режим SYSKEY (т.е. SYSKEY не хранится в реестре), программа запросит у вас пароль запуска ОС или дискету SYSKEY. Если не предоставить что-то из этого, хэши паролей не получится извлечь, и вы не сможете изменить пароли или свойства учетных записей или даже записать хэши паролей в текстовый файл.

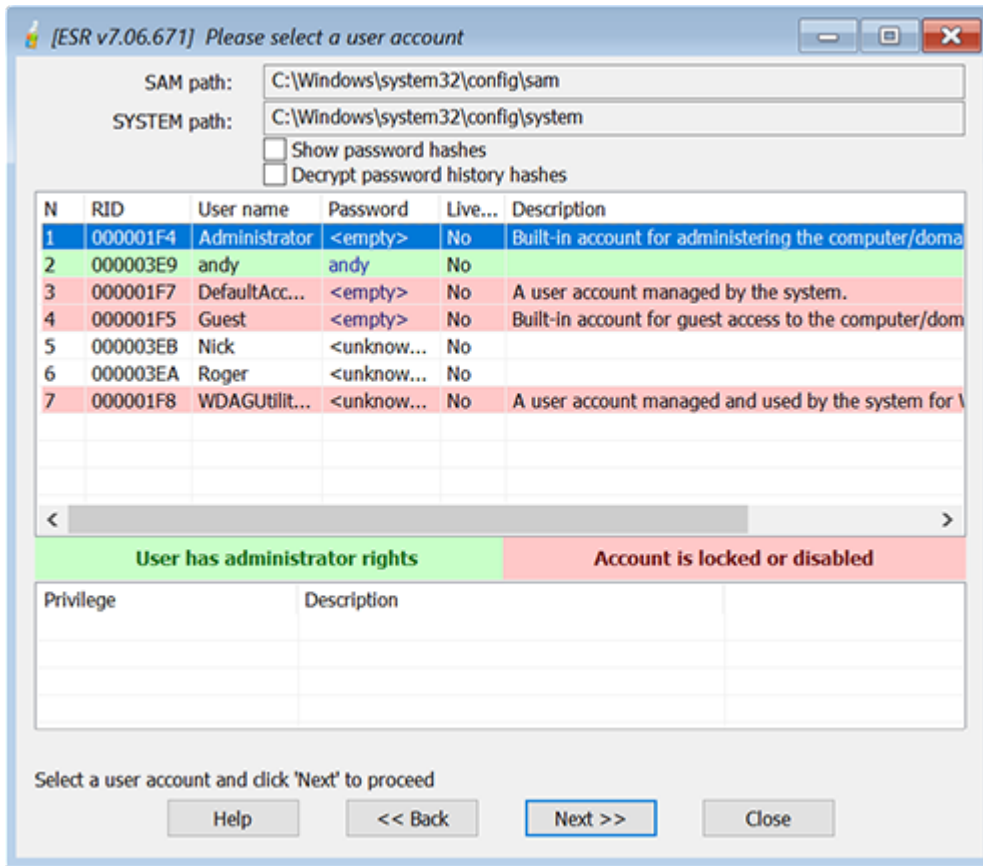
Если вы выбрали опцию «Тестировать короткие и простые пароли» (Test short and simple passwords/), ESR попытается восстановить пароли, используя несколько predefined словарных атак и атак методом перебора. Программа также попытается расшифровать пароли, которые могут храниться или быть кэшированы в других файлах. Хотя эта атака не возьмет большинство паролей, она занимает всего несколько минут и помогает в восстановлении коротких и простых пароли. Программа проверит следующие пароли:

- Очевидные комбинации, такие как пароли, совпадающие с логинами
- Хранимые пароли от dial-up
- Пароли из SECURITY в реестре
- Пароли от некоторых браузеров, которые можно расшифровать мгновенно
- LM пароли
 - 4 символа (заглавные буквы, цифры, 16 символов)
 - Пароли из словаря
 - Пароли из словаря с одной цифрой в конце
- NTLM пароли
 - 4 символа (строчные буквы, цифры, 16 символов)
 - 4 символа (строчные буквы, заглавные буквы)
 - 5 знаков (строчные буквы)
 - 5 знаков (заглавные буквы)
 - 7 знаков (цифры)
 - 3 символа (все символы)
 - Пароли из словаря
 - Повторяющиеся комбинации (например, «00000», «aaa» и т. д.)
 - Комбинации клавиатуры (например, qwerty)
 - Комбинации клавиатур на штатной (OEM) раскладке

После этого программа создаст несколько различных мутаций для паролей, найденных на предыдущих шагах, и попытается применить их ко всем учетным записям.

Учетные записи локальных пользователей

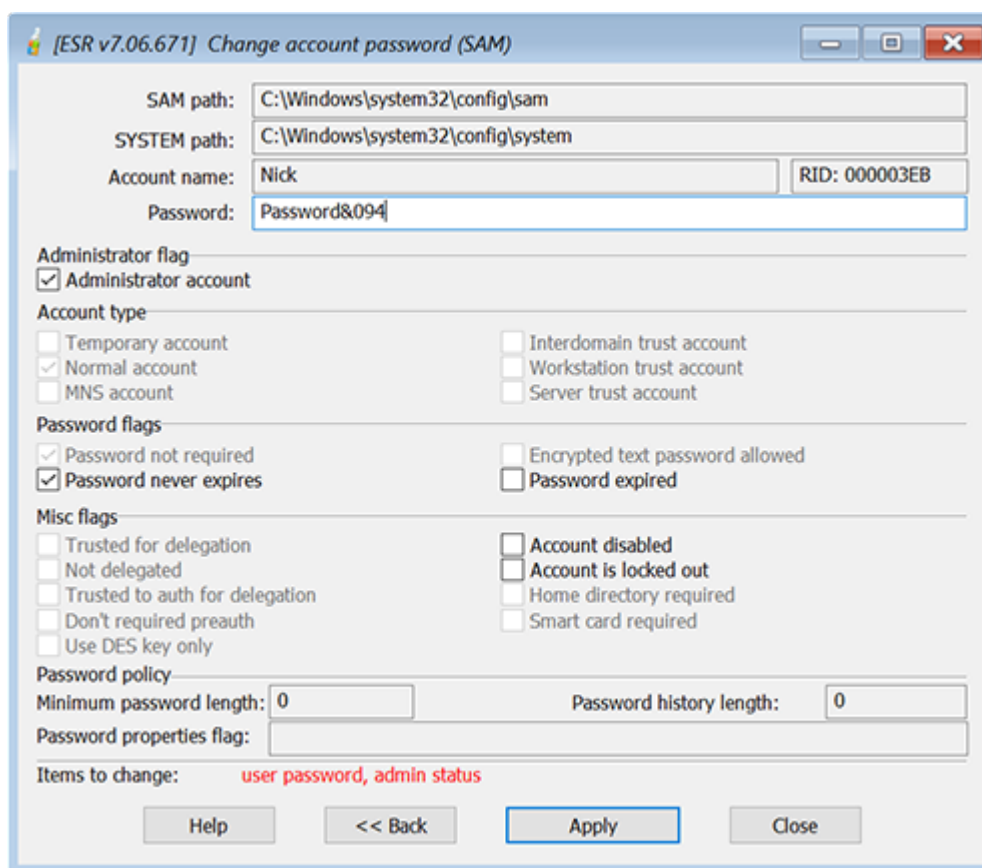
Если вы работаете с локальными (SAM) учетными записями, вам будет представлен список всех локальных учетных записей после выбора операционной системы или файлов SAM и SYSTEM:



Учетные записи с правами администратора выделены зеленым. Учетные записи, которые заблокированы или отключены, - красным.

Вы можете включить опцию Показать хэши паролей (Show password hashes), чтобы увидеть хэши LM и NTLM для всех учетных записей с непустыми паролями, и включить опцию Показать историю паролей (Show password history), чтобы увидеть старые доступные записи (если в системе было включено сохранение истории паролей).

Выберите учетную запись, для которой вы хотите изменить пароль или свойства, и нажмите Далее>> (Next):



Здесь вы можете сбросить / изменить пароль, а также следующие свойства учетной записи:

- Учетная запись администратора
- Срок действия пароля никогда не истечет
- Срок действия пароля истек
- Учетная запись отключена
- Аккаунт заблокирован

После внесения изменений нажмите Применить (Apply). Вам будет предложено указать расположение и имя резервной копии базы данных SAM.

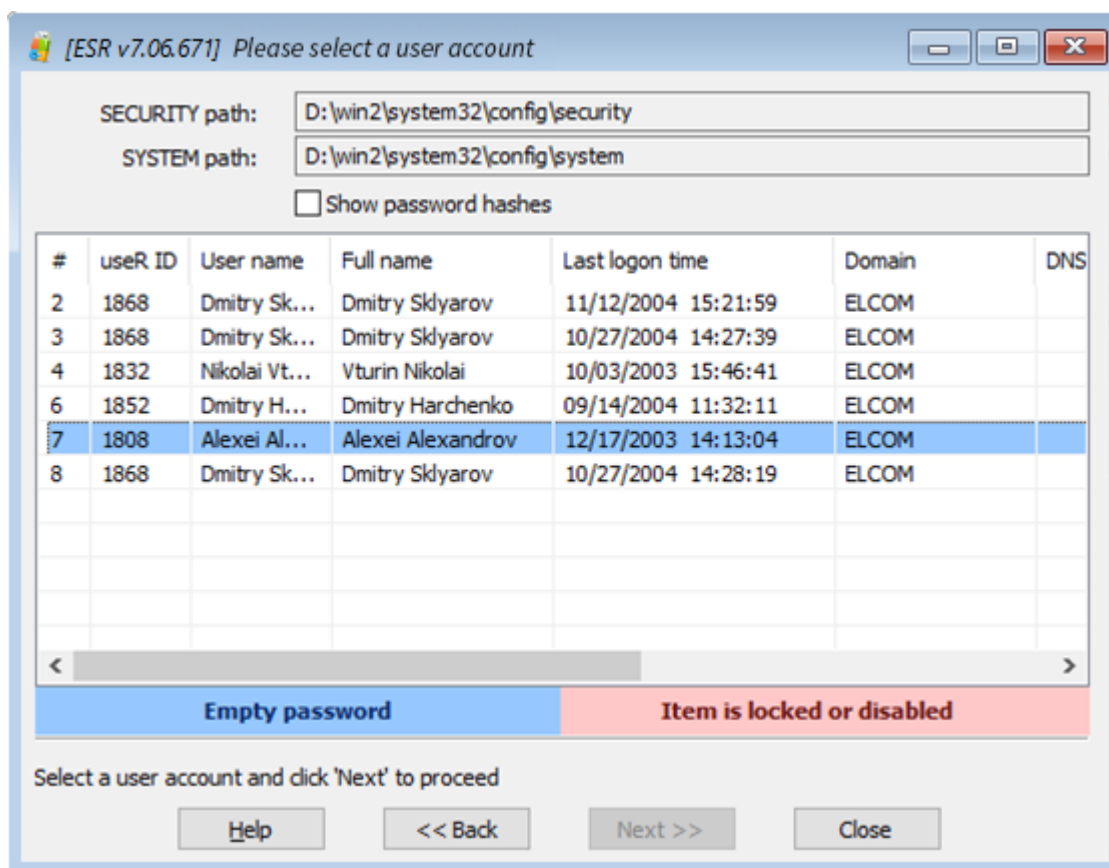
Важно: не сбрасывайте пароль, оставляя его пустым. В целях безопасности выберите новый, при чем достаточно сложный пароль. Обратите внимание, что может быть применена локальная политика безопасности. В таком случае вы хоть и сможете установить несовместимый или даже пустой пароль, но вы не сможете войти в систему с этим новым паролем, если он не соответствует политике паролей. Наконец, вы не можете предоставить права администратора встроенным учетным записям, таким как Гость (Guest); Также не рекомендуется изменять пароль или какие-либо свойства для любых учетных записей в группе пользователей «Гости».

Учетные записи AD

Если вы работаете с учетными записями Active Directory, программа выдаст список всех учетных записей Active Directory вместе с их свойствами. Здесь вы сможете сбросить пароль для любого пользователя Active Directory (включая администратора домена), так же как для [локальных учетных записей пользователей](#)^[173]. Однако вы не сможете изменить какие-либо свойства учетной записи (например: сделать учетную запись Администратора или задать свойство Срок действия пароля никогда не истечет и т. д.).

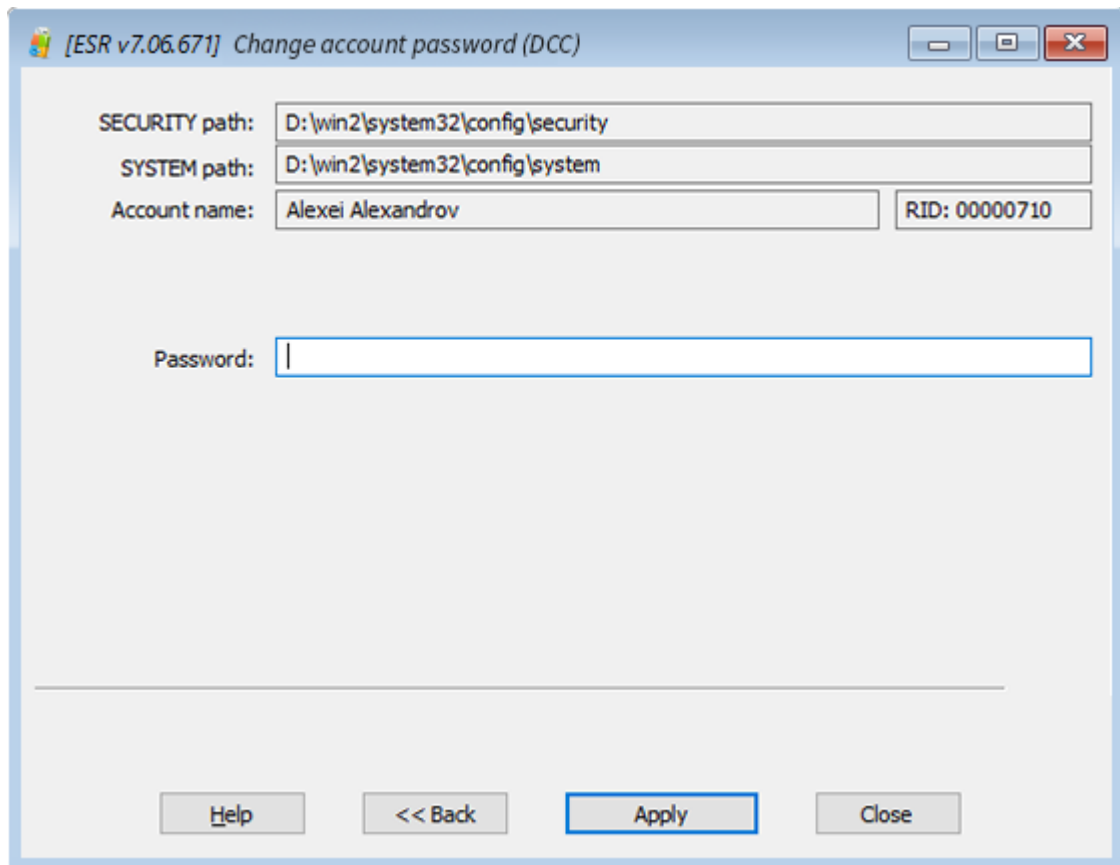
Кэшированные учетные записи домена

После выбора директории Windows (или файлов SECURITY и SYSTEM) программа начнет поиск и расшифровку кэшированных записей домена и отобразит список кэшированных учетных записей пользователей.



Учетные записи с пустыми паролями выделены синим цветом. Учетные записи, которые заблокированы или отключены, - красные.

Выберите учетную запись, пароль для которой нужно изменить, и нажмите Далее >> (Next), чтобы перейти к следующему шагу.

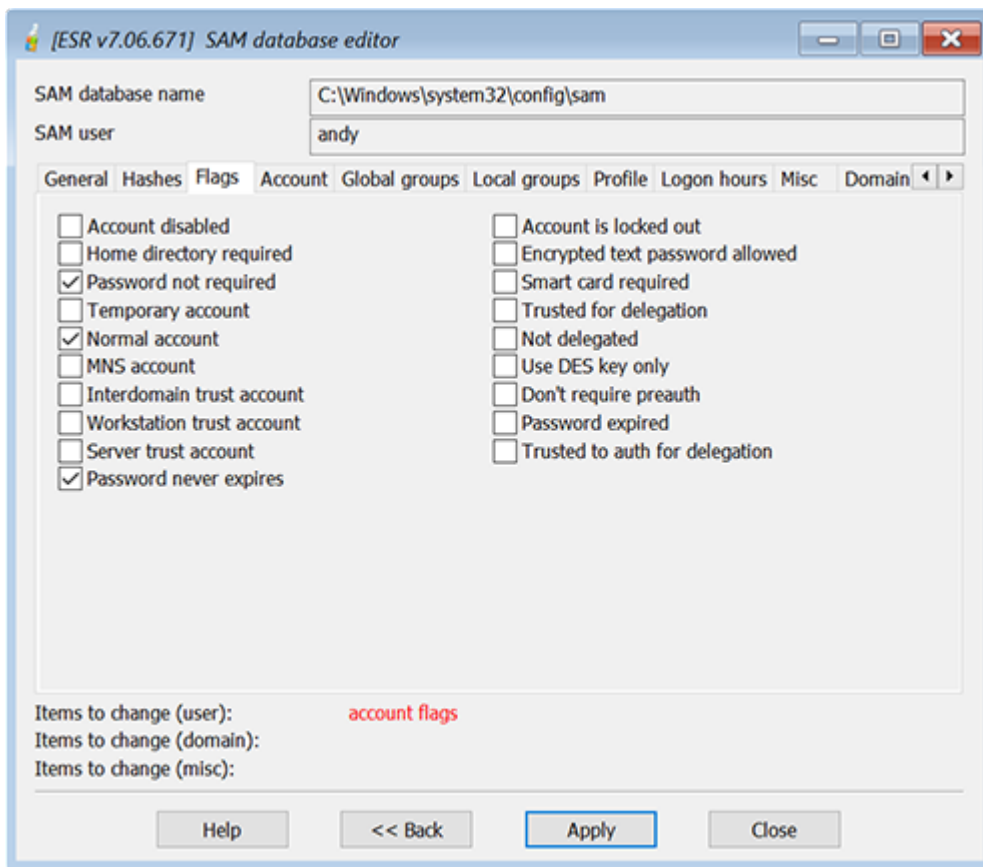


Введите пароль или очистите соответствующее поле ввода, затем нажмите Применить (Apply). Вам будет предложено создать резервную копию файла SECURITY. Перед применением изменений настоятельно рекомендуется сделать резервную копию файла.

Чтобы войти в учетную запись домена после сброса пароля, вам необходимо отключить соединение с доменом. В противном случае Windows не будет использовать кэшированные данные для входа.

Редактор базы данных SAM

Редактор базы данных SAM позволяет просматривать и изменять большинство свойств локальных учетных записей пользователей:



Отображается следующая информация:

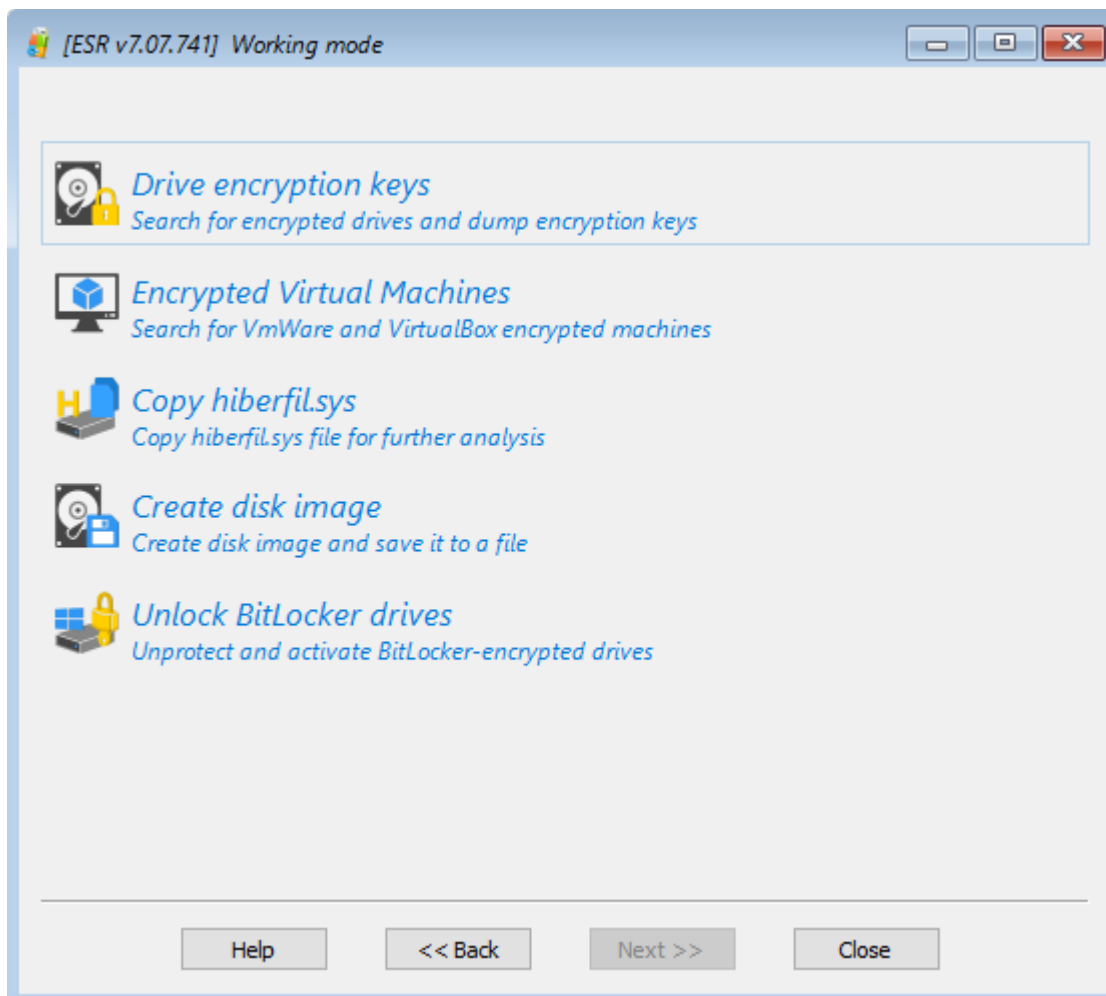
- Общие (имя пользователя, полное имя, комментарий, ID пользователя)
- Хеши (LM и NTLM)
- Флаги (Flags) (основные свойства учетной записи пользователя)
- Учетная запись (время последнего входа и выхода, последний установленный пароль, истечение срока действия учетной записи, последний неверный пароль)
- Глобальные и локальные группы
- Профиль (домашняя директория, путь к скрипту / профилю)
- Часы входа в систему
- Другое (версия базы данных SAM, код страны, кодовая страница и т. д.)
- Информация о домене, свойства, в т. ч. свойства пароля

Не рекомендуется редактировать какие-либо поля базы данных SAM, если вы не уверены в том, что делаете.

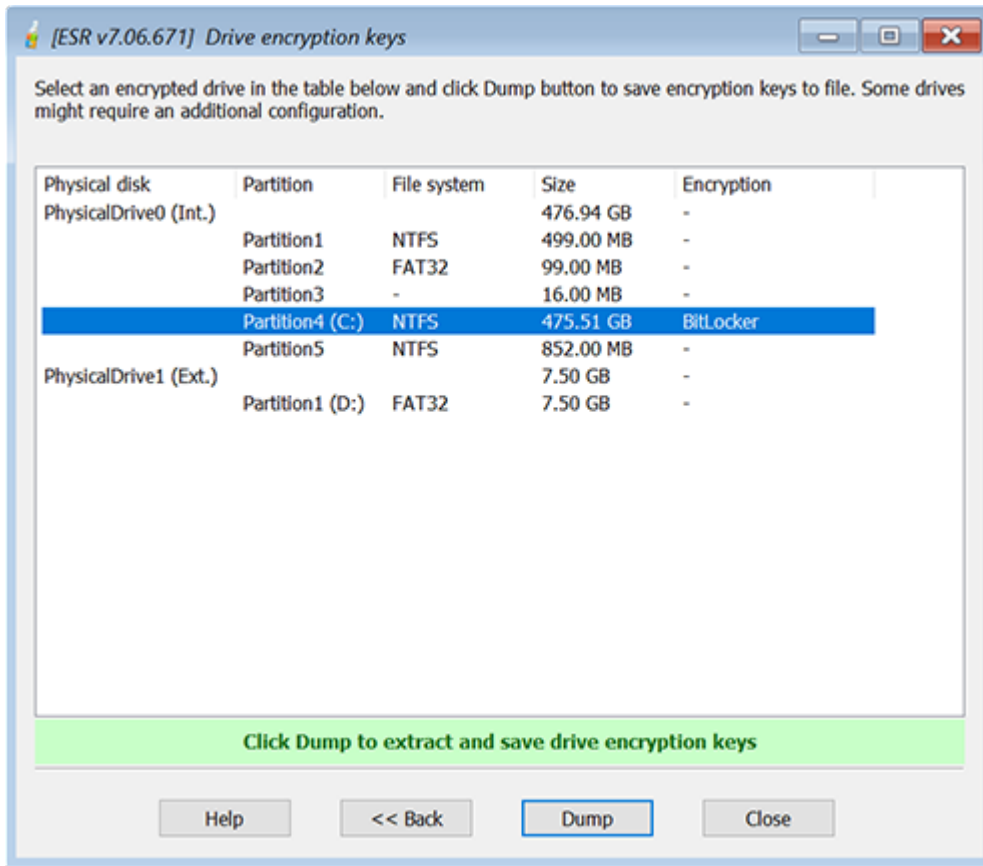
Инструменты работы с дисками

В диалоговом окне «Инструменты работы с дисками» вы можете искать зашифрованные диски или виртуальные машины и создавать дампы ключей шифрования для дальнейшего восстановления с помощью Elcomsoft Distributed Password Recovery или с помощью других программ.

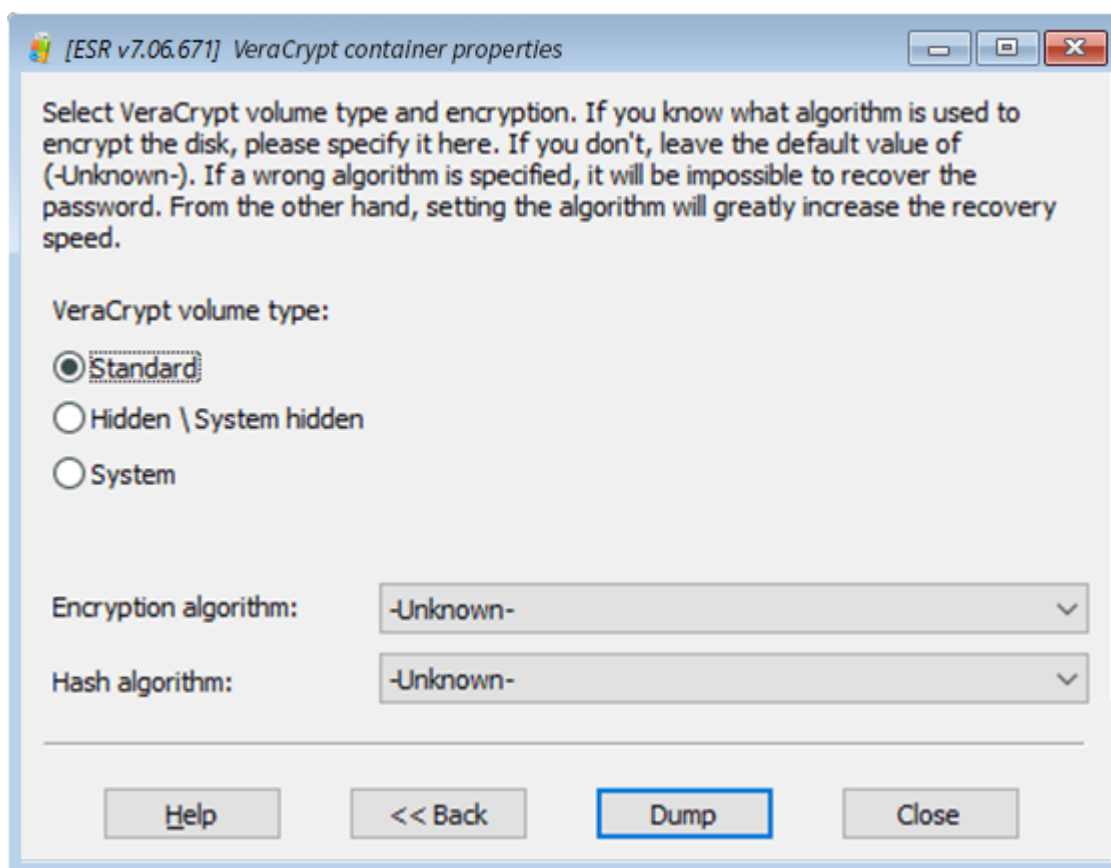
Вы также можете создать образ диска для криминалистического анализа (forensic disk).



Как только программа обнаружит зашифрованный диск, выберите его из списка и нажмите Дамп (Dump), чтобы сохранить ключи шифрования диска.



Диски TrueCrypt / VeraCrypt требуют дополнительной настройки. Возможно, вам потребуется вручную задать алгоритмы шифрования для более быстрого восстановления.



Программа поддерживает следующие типы шифрования:

- BitLocker
- PGP Диски
- PGP WDE
- TrueCrypt
- VeraCrypt
- FileVault
- LUKS

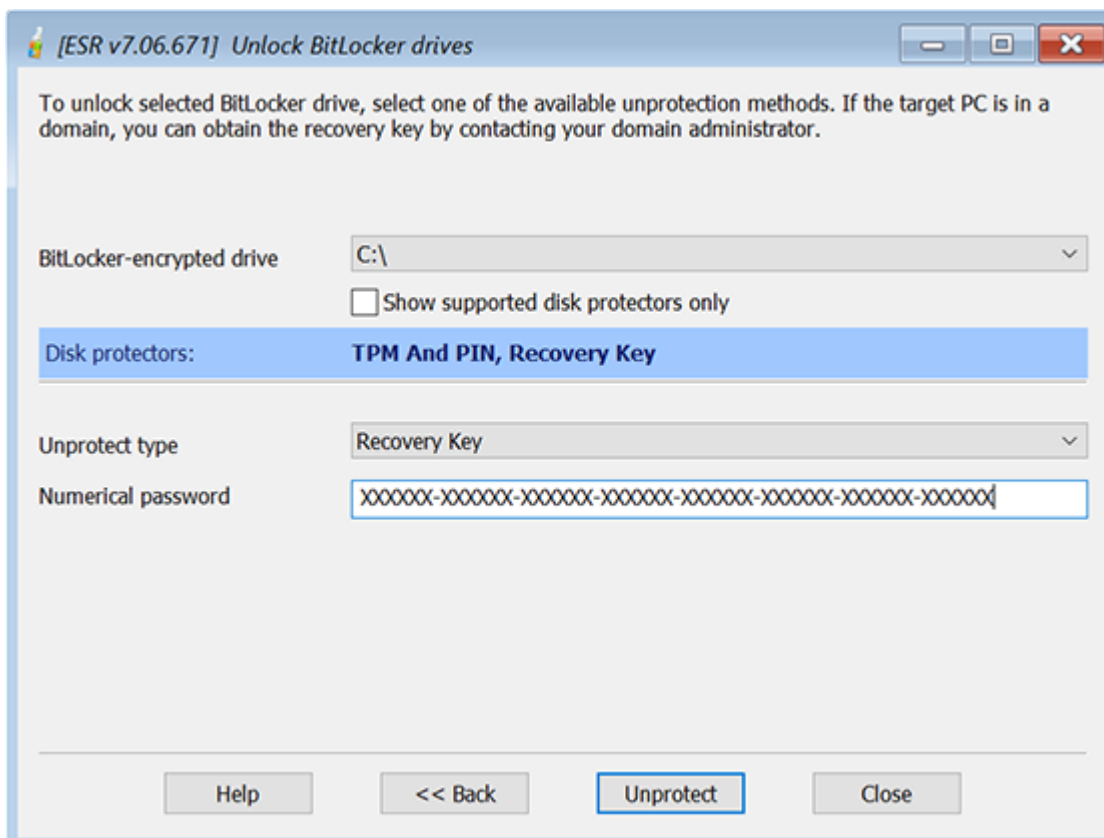
Разблокировать диски от BitLocker

Чтобы использовать диск, зашифрованный с помощью BitLocker, сначала необходимо его разблокировать и смонтировать. Программа поддерживает три основных метода разблокировки диска BitLocker:

- Ключ восстановления. Этот метод используется по умолчанию. Windows генерирует 48-значный цифровой ключ восстановления каждый раз, когда пользователь запускает BitLocker шифрование.
- Пароль. Простой буквенно-цифровой пароль, который используется для разблокировки дисков, зашифрованных с помощью BitLocker, в дополнение к ключу восстановления.
- Ключ USB. Двоичный файл, обычно с расширением * .bek, который хранится на внешнем диске (например, USB).

Если целевой компьютер является частью доменной организации, вы также можете получить ключ восстановления, связавшись с администратором домена.

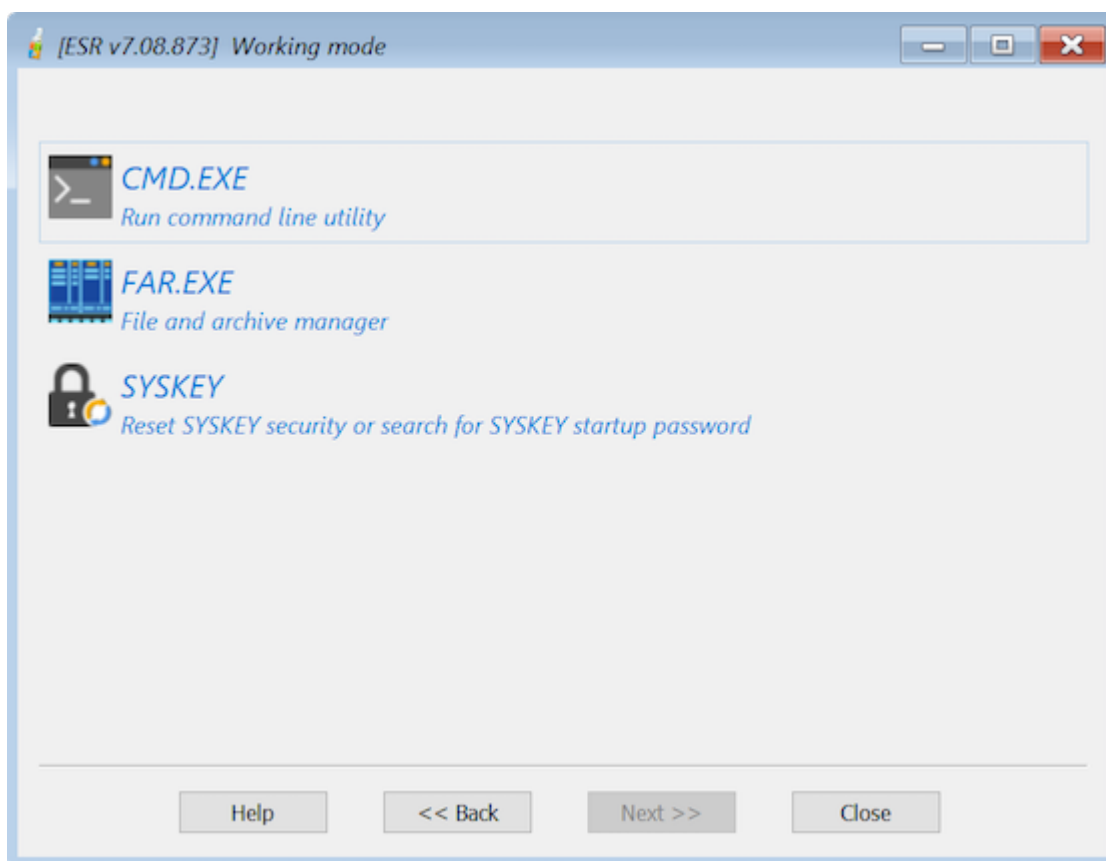
После того, как выбранный диск BitLocker будет разблокирован, программа расшифровывает и подключает диск, позволяя вам получить доступ к данным, хранящимся на этом диске.



Другое

Доступны дополнительные инструменты:

- CMD.EXE - командная строка. Вы можете использовать ее для дополнительных операций, таких как копирование файлов или запуск встроенных инструментов WinPE.
- Подсказки паролей (Password hints) - эта функция отображает подсказки локальных пользователей, обнаруженных в анализируемой системе. Это применимо только к локальным (SAM) учетным записям.
- SYSKEY - позволяет сбросить или восстановить Syskey пароль.



5.5 Proactive Password Auditor

5.5.1 Введение

Proactive Password Auditor - это инструмент для системных администраторов и ИТ-безопасников, позволяющий проводить аудит политики безопасности организации, проверять безопасность сети и восстанавливать пароли учетных записей. Инструмент помогает точно узнать, насколько безопасна сеть, запустив полномасштабную атаку на пароли учетных записей. Обнаруживая незащищенные пароли, Proactive Password Auditor тем самым оценивает безопасность сети.

Не все политики безопасности одинаково успешны на практике. Один единственный слабый пароль становится слабым звеном в цепочке, которая ставит под угрозу безопасность всей сети. Корпоративные пользователи часто используют слишком короткие или слишком простые пароли. Эти пароли легко запомнить, но по сути они небезопасны.

Proactive Password Auditor определяет безопасность вашей сети, пытаясь проникнуть в нее посредством одного из взломанных паролей. Если за определенное время разблокируется хотя бы одна учетная запись, это свидетельствует об уязвимости всей сети. Если сеть выдерживает атаки в течение всего периода времени пока срок действия пароля не истек, политика безопасности паролей считается достаточно строгой.

Восстановление утерянных и забытых паролей к учетным записям пользователей - еще одна цель Proactive Password Auditor. Анализируя хэши паролей и восстанавливая пароли

(предоставляя их текстовую версию), Proactive Password Auditor позволяет получать доступ и входить в учетные записи пользователей, открывая файлы и папки, зашифрованные с помощью EFS-шифрования. Широкий спектр доступных атак - от словарных атак до брутфорса - позволяет восстанавливать пароли по сети, в то время как атака Rainbow (использующая радужные таблицы) восстанавливает до 95% паролей за считанные минуты. *К счастью, Rainbow-атаку невозможно выполнить извне!*

Proactive Password Auditor™ может анализировать бинарные значения в реестре и извлеченные дампы-файлы, что позволяет восстанавливать пароль в автономном режиме. Proactive Password Auditor работает в Windows 2000, XP, Vista, 7, 8, Windows Server 2003/2008/2012.

5.5.2 Системные требования

- Windows 2000, Windows XP, Windows Vista, Windows 7, Windows 8, Windows Server 2003/2008/2012 (32-разрядная или 64-разрядная)

Обратите внимание, что некоторые функции (например, дампы хэшей паролей из памяти или реестра) доступны только с правами администратора. Если права администратора недоступны, или если пароль администратора утерян, забыт или срок его действия истек, или если учетная запись администратора заблокирована или отключена, вы можете использовать [Elcomsoft System Recovery](#) для сброса или изменения паролей для любых локальных учетных записей пользователей или учетных записей Active Directory, для включения/разблокировки отключенных/заблокированных учетных записей, для дампа хэшей паролей с выгрузкой в текстовый файл и т.д.

Дополнительные требования для дампа хэшей паролей из памяти:

- Значение RestrictAnonymous должно быть установлено как 0 или 1 в следующем ключе:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\LSA

Удаленный доступ к реестру для пользователей домена HE должен быть ограничен следующим ключом:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurePipeServers\winreg

- И на локальном, и на удаленном компьютерах должен быть включен общий доступ к файлам и принтерам (т.е. сервисы рабочих станций и сервера).
- Удаленная система должна иметь общий ресурс Admin\$ (скрытый общий ресурс, который сопоставляется с каталогом \windows) или другой общий ресурс с такими же свойствами.

Проблемы с Windows XP/Windows Server 2003: если удаленный компьютер, на котором вы собираетесь делать дампы хэшей паролей, работает под управлением Windows XP SP2+ или Windows Server 2003+, для параметра "Сетевой доступ: Безопасность и общий доступ" для локальных пользователей политику безопасности следует установить как "Classic" - локальные пользователи входят в систему со своими данными. Это можно сделать с помощью редактора групповой политики (gpedit.msc) в следующей ветви: *Панель управления\Все элементы панели управления\Администрирование\Локальная политика безопасности\Конфигурация компьютера\Конфигурация Windows\Параметры безопасности\Локальные политики\Параметры безопасности*

Если по какой-либо причине PPA не может выполнить дамп с удаленного компьютера, попробуйте подключиться к ресурсу ADMIN\$ вручную в проводнике Windows: *Нажмите Win+E. Выберите "Этот компьютер" на панели слева. Затем на вкладке "Компьютер" выберите "Подключить сетевой диск". В списке "Диск" выберите букву диска. В поле "Папка" введите путь к папке или компьютеру либо выберите "Обзор", чтобы найти папку или компьютер. Чтобы подключать сетевой диск при каждом входе в систему, установите флажок "Восстанавливать подключение при входе в систему". Нажмите "Готово".*

Если соединение установлено успешно, PPA будет работать; в противном случае вам может потребоваться проверить настройки файловой системы на удаленном компьютере. Если ручное подключение к ADMIN\$ также не удастся, это означает, что общий ресурс ADMIN\$ не включен, или для политики безопасности, описанной выше, задано значение «Только гость» - локальные пользователи аутентифицируются как гость, или вы используете неверные учетные данные.

В доменной среде рекомендуется запускать PPA под учетной записью администратора домена.

5.5.3 О программе

5.5.3.1 О Windows паролях

Вместо того, чтобы хранить пароль учетной записи пользователя в виде простого текста, Windows генерирует и сохраняет одно из двух различных представлений пароля, т.н. «хэши». Когда вы устанавливаете или меняете пароль для аккаунта на пароль, содержащий менее 15 символов, Windows генерирует как LAN Manager (LM), так и Windows NT (NTLM) хэши пароля. Эти хэши хранятся в локальной базе данных Security Account Manager (SAM) или в Active Directory.

Хэш NTLM на самом деле является MD4-хешем от исходного пароля (в UNICODE) длиной 16 байт. Теоретически длина пароля ограничена 128 символами.

LM-хэш по сравнению с NTLM-хешем считается более слабым, но он необходим для обратной совместимости с клиентами Windows 9x и обычно используется для авторизации удаленного подключения к данной машине. Чтобы сгенерировать хэш LM, система преобразует пароль из UNICODE в ANSI (по одному байту на символ) и переводит все символы в верхний регистр. После этого пароль делится на две части (по 7 символов в каждой, при необходимости дополняемые нулями). Каждая часть используется в качестве ключа DES-шифрования (для шифрования заранее определенной константы), а результаты шифрования сохраняются в системе (объединяются в одно 16-байтовое значение). Таким образом, если система использует LM-аутентификацию (и поэтому доступны LM-хэши), реальная **сложность** пароля составляет всего 7 символов, и пароль из 14 символов ненамного сильнее, чем пароль из 7 символов.

5.5.3.2 Как работать с PPA

Из-за природы алгоритмов хеширования (см. [О Windows паролях](#)¹⁸⁵) **невозможно получить исходный пароль из хэша**, будь то LM или NTLM. Тем не менее, все еще можно найти пароль, используя брутфорс-атаки и атаки по словарю, проверяя все возможные пароли в заданном диапазоне или пробуя слова из списка слов, соответственно. Итак, чтобы получить пароли, необходимо:

- [найти хэши пароля](#)¹⁸⁶
- [найти пароли с такими же хэшами, что и исходные](#)¹⁸⁸

Поскольку хеширование основано на довольно-таки надежных алгоритмах (DES и MD4), поиск правильного пароля может оказаться времязатратным. Но поскольку большинство пользователей предпочитают легкозапоминающиеся пароли, брутфорс и атаки по словарю часто являются наиболее эффективными методами, для поиска пароля. Таким образом, надежность пароля зависит от того, сколько символов в нем, насколько хорошо пароль аккуратно хранится владельцем и насколько сложно его угадать.

В настоящее время существует несколько [типов атак](#)¹⁸⁶, основанных на угадывании слабых паролей: с использованием словарных атак, брутфорса и радужных атак.

5.5.3.3 Получение хэшей паролей

PPA поддерживает несколько различных методов получения хэшей паролей. Они описаны ниже.

DUMP файл (DUMP file)

Есть несколько сторонних инструментов, которые могут создавать файлы дампа с хешами паролей, например `pwdump`, `pwdump2`, `pwdump3` и `samdump`. Файлы, созданные этими инструментами, имеют следующий формат:

```
user_name:user_id:LM_hash: ntlm_hash:comment:user_home_directory:
```

PPA может принимать эти типы файлов в качестве входных данных.

Локальный реестр (Local Registry)

Во всех системах, которые не используют Active Directory, хэши паролей хранятся в системном реестре, и программа может извлекать их из реестра, даже если они зашифрованы с помощью SYSKEY.

Файлы реестра (Registry files (SAM, SYSTEM))

Программа может извлекать хэши паролей прямо из файлов реестра: SAM и SYSTEM. Вам нужно будет выбрать эти два файла (или только файл SAM, если это файл из старой NT-системы, которая не использует защиту SYSKEY: в этом случае установите флажок "Не использовать SYSKEY" (Don't use SYSKEY)). Если SYSKEY был сгенерирован из пароля запуска системы или сохранен на внешнем носителе, вам нужно будет указать этот пароль или внешний носитель, соответственно. Обратите внимание, что с помощью этой функции вы не можете выполнить дампы из файлов SAM и SYSTEM, которые в настоящее время используются (по адресу `WINDOWS\SYSTEM32\config`), потому что в данный момент они будут заблокированы операционной системой.

Однако вы можете сделать копии этих файлов, загрузившись в альтернативную операционную систему, например, в другую установку Windows или, как другой способ - подключить жесткий диск, на котором расположены эти файлы, в качестве дополнительного диска к другой рабочей станции Windows.

ОЗУ локального компьютера (Local computer RAM)

Если у вас есть права администратора на машине, на которой вы запускаете PPA, вы можете выгружать хэши паролей из его памяти. Этот метод работает независимо от режима SYSKEY и получает хэши для всех пользователей, включая пользователей Active Directory.

ОЗУ удаленного компьютера (Remote computer RAM)

Этот метод аналогичен предыдущему, но позволяет дампать хэши с любого удаленного компьютера в вашей локальной сети: сервера или рабочей станции, с Active Directory или без нее. Нажмите кнопку «Просмотр» (Browse) и выберите компьютер(-ы), с которых вы хотите сделать дамп хэшей. После получения хэшей паролей PPA покажет следующую информацию:

- Имя пользователя - User name
- Компьютер - Computer
- ID пользователя - User ID
- Тип хэша - Hash type (LM или LM+NTLM)
- LM-хэш - LM hash
- NT-хэш - NT hash
- Пароль - Password
- Время аудита - Audit time
- Состояние (отключен или заблокирован) - Status (disabled or locked)
- Описание - Description

Щелкните правой кнопкой мыши на заголовок любого столбца, чтобы включить/отключить отображение любого из этих полей в интерфейсе программы.

Обратите внимание, что для получения хэшей паролей с любого удаленного компьютера PPA должен иметь права администратора на удаленной машине. Сперва он попытается войти в систему с текущими учетными данными (теми, с которыми была запущена программа), затем с [сохраненными учетными данными](#)^[188] (если есть соответствующая запись), и если эти методы не сработают, он запросит имя пользователя и пароль. Если данный компьютер является контроллером домена, вы должны предоставить учетные данные администратора домена (см. в разделе [Системные требования](#)^[184]).

Когда вы делаете дамп или открываете хэши паролей с помощью любого из описанных выше методов, PPA запускает (по умолчанию) т.н. быструю предварительную атаку, которая занимает несколько секунд, но может автоматически восстанавливать короткие и простые пароли. (см. в разделе [Опции предварительной атаки](#)^[193]).

Перед атакой, когда пароли еще не восстановлены, пароли отображаются либо как <отсутствует> (<empty>) (если пароль для данной учетной записи не установлен), либо как <неизвестный> (<unknown>). После предварительной атаки некоторые <неизвестные> (<unknown>) пароли могут быть восстановлены и отображены.

Выберите учетные записи пользователей, для которых вы хотите выполнить аудит паролей, выберите метод атаки и начните саму атаку. **Вы не сможете проверить следующие учетные записи:**

- Аккаунты с пустыми паролями
- Учетные записи, которые превышают лимит пробной версии PPA или в соответствии с приобретенной лицензией (эти учетные записи неактивны)

Соответствующее сообщение будет выведено в окне журнала (и в файле журнала) соответственно:

- Пароль пользователя «Гость» пуст, восстановление для этого пользователя недоступно. - Password of user "Guest" is empty, recovery for this user is disabled
- Восстановление для этого пользователя недоступно (номер пользователя 101) - Recovery for this user is disabled (number of user 101)

5.5.3.4 Данные аутентификации

PPA позволяет управлять учетными данными и сохранять их для любого количества компьютеров, на которых вы проводите аудит.

Выберите пункт «Учетные данные» (Credentials) в меню «Параметры» (Options), и вы получите список компьютеров для управления (это пустой список, если вы только начали работу с программой). Нажмите кнопку «Добавить» (Add), найдите компьютер, для которого нужно сохранить учетные данные, и нажмите «Выбрать» (Select). На следующем экране вы должны ввести:

- Домен/компьютер (Domain/computer). Вы уже выбрали его на предыдущем шаге, но вы все равно можете нажать «Выбрать» (Select), чтобы выбрать другой.
- Имя ресурса (Resource name). PPA будет подключаться к данному ресурсу для загрузки настраиваемой службы, которая будет сбрасывать хэши паролей. Нажмите "Выбрать" (Select), чтобы просмотреть список общих ресурсов на выбранном компьютере (если на это есть права).
- Имя пользователя (User name). Имя пользователя, имеющего права администратора на данном компьютере. Нажмите "Выбрать" (Select), чтобы получить список локальных пользователей, и, если необходимо, кнопку "Пользователи домена" (Domain users) на следующем экране, чтобы выбрать одну из учетных записей пользователей домена для любого выбранного контроллера домена.
- Пароль (Password). Пароль пользователя, выбранного на предыдущем шаге.

*Обратите внимание, что если вы вводите имя ресурса и имя пользователя вручную, PPA проверит их, так же как и пароль, **только при аудите конкретного компьютера**. Если что-то пойдет не так (ресурс недоступен, пользователь не найден или пароль не совпадает), вам будет предложено исправить эти поля, и, если обновленная информация верна, она будет сохранена.*

5.5.3.5 Взлом паролей

Методы взлома паролей

PPA поддерживает различные методы восстановления пароля: атака по словарю, брутфорс и [радужная атака](#)^[189] (подробнее см. в следующих разделах). После выбора метода атаки на второй вкладке в главном окне будут отображены параметры, подходящие для выбранного метода.

Кроме того, вам нужно выбрать LM-атаку или NTLM-атаку, в зависимости от используемого метода аутентификации, то есть типов доступных хэшей паролей. После получения хэшей паролей в поле "Тип хэша" (Hash type) отображается либо LM + NTLM (что означает, что присутствуют хэши LM и NTLM), либо NTLM (если хэш LM недоступен); см. [O Windows паролях](#)^[185].

Если некоторые пользователи указаны с типом хэша LM + NTLM, рекомендуется начать с LM-атаки. Обе атаки выполняются примерно с одинаковой скоростью, но, как уже отмечалось, эффективная длина пароля для LM-хэша ограничена 7 символами, а LM-пароли всегда вводятся в верхнем регистре. Таким образом, вы можете завершить LM-атаку для всех 14-значных паролей за относительно быстрое время (от нескольких минут до нескольких часов, в зависимости от выбранного набора символов и скорости вашего процессора).

Однако для всех пользователей с NTLM-хешем вам все равно придется запускать NTLM-атаку.

Обратите внимание, что **вы можете проводить атаку одновременно на нескольких пользователях**. Из-за слабой реализации хеширования паролей (в см. без соли), примерно одинаковое время уйдет, чтобы попробовать один и тот же пароль для одного пользователя, 100 пользователей или 10 000 пользователей. Выберите всех пользователей с одинаковым типом хэша (LM или LM + NTLM) для проведения наиболее эффективной атаки. Чтобы выбрать учетные записи пользователей для восстановления, поставьте галочки слева от имен пользователей; вы также можете использовать контекстное меню или горячие клавиши: Ctrl+A для выбора всех пользователей, Ctrl-U для снятия выделения.

После восстановления паролей учетные записи с известными/восстановленными (или пустыми) паролями отображаются красным цветом, а в столбце "Время аудита" (Audit time) отображается общее время, потраченное на эту учетную запись/пароль.

Радужная атака

Радужная атака - это реализация метода [Faster Cryptanalytic Time-Memory Trade-Off](#), разработанного доктором Филиппом Охслином. Идея состоит в том, чтобы заранее (только один раз) сгенерировать хеш-таблицы паролей, а в процессе аудита/восстановления искать хеш-значения в этих предварительно вычисленных таблицах. Этот процесс значительно сокращает необходимое время, особенно для сложных паролей. Из-за характера этой атаки некоторые пароли не могут быть восстановлены; однако вы можете использовать радужные таблицы с большой вероятностью успешного нахождения пароля.

Чтобы получить доступ к настройкам радужной атаки, переключите тип атаки на радужную (Rainbow) и щелкните вкладку радужной атаки (Rainbow attack). Нажмите кнопку "Список радужных таблиц" (Rainbow tables list) и найдите таблицы для дальнейшей атаки (вы можете добавить сразу несколько таблиц), вы можете удалять таблицы из списка и перемещать их вверх и вниз; по завершении нажмите "Закрыть" (Close) и приступайте к самой атаке.

Программа также поддерживает индексированные радужные таблицы, доступные по адресу <http://www.freerainbowtables.com>.

Чтобы создать свои собственные таблицы, нажмите кнопку «Сгенерировать таблицы» (Generate tables).

Тип хэша (Hash type)

Могут быть созданы хеш-таблицы LM и NTLM; см. [О Windows паролях](#) ¹⁸⁵

Длина пароля (Password length)

Минимум и максимум; обычно от 1 до 7 (чтобы покрыть все пространство паролей для хэшей LM). Однако, если вы хотите проверять только 6-символьные пароли (и вторую половину паролей длиной от 8 до 15 символов), вы можете создать более эффективные и все же относительно небольшие таблицы для длины от 1 до 6.

Кодировка (Charset)

Доступные варианты:

- буквенный (alpha): только заглавные буквы (26)
- буквенный-пробел (alpha-space): заглавные буквы плюс пробел (27)
- буквенно-цифровой (alpha-numeric): заглавные буквы плюс цифры (36)
- буквенно-числовой-пробел (alpha-numeric-space): заглавные буквы плюс цифры и пробел (37)
- буквенно-числовой-символьный14 (alpha-numeric-symbol14): заглавные буквы, цифры и 14 наиболее распространенных символов: ! @ # \$ % ^ & * () - _ + = (50)
- буквенно-числовой-символьный14-пробел (alpha-numeric-symbol14-space): заглавные буквы, цифры, пробел и 14 наиболее распространенных символов: ! @ # \$ % ^ & * () - _ + = (51)
- все (all): заглавные буквы, цифры и 32 печатных символа, включая пробел (69)

Длина цепи (Chain length)

Обычные значения от 1000 до 10000. Когда это значение увеличивается, вы получаете большую вероятность успеха, но большее время генерации и криптоанализа.

Счетчик цепи (Chain count)

Счетчик цепи влияет на размер таблицы (и, следовательно, на дисковое пространство), вероятность успеха и время генерации (*но не на время криптоанализа*).

Количество таблиц и индексов (Number of tables and Indexes)

Количество таблиц для создания или индексы таблиц, если вы распределяете процесс создания таблиц по нескольким компьютерам. Чем больше у вас таблиц, тем выше вероятность успеха. Например, если одна таблица дает вероятность 60% (0,6), две таблицы дают $1 - (1 - 0,6) * (1 - 0,6) = 0,84$ (84%). С тремя такими таблицами вероятность уже равна $1 - (1 - 0,6)^3 = 0,936$ (93,6%). Но, конечно, резко увеличивается в объеме и занятое таблицами пространство.

Папка вывода (Output folder)

Нажмите кнопку «Обзор» (Browse), чтобы выбрать папку для сохранения сгенерированных таблиц (перед запуском процесса создания убедитесь, что в ней достаточно свободного места).

Как только все параметры выбраны, PPA немедленно вычисляет пространство ключей (общее количество паролей в заданном диапазоне; фактически, это зависит только от набора символов и длины пароля), дисковое пространство (размер каждой таблицы, умноженный на количество таблиц), и вероятность успеха. Вы также можете запустить тест: нажмите "Старт" (Start), и PPA рассчитает скорость вашего компьютера при этих операциях, а также время предварительного

вычисления таблицы, общее время предварительного вычисления и максимальное время криптоанализа.

Есть несколько стандартных конфигураций (для LM-хэша, длина от 1 до 7; время рассчитывается для процессора Pentium 4 3.0ГГц), которые вы можете использовать, например:

	#1	#2	#3	#4
Кодировка (Charset)	Буквенная (alpha)	Буквенно-цифровая (alpha-numeric)	Буквенно-цифрово-символьная ¹⁴ (alpha-num-sym ¹⁴)	Все (all)
Длина цепи (Chain length)	2,100	2,400	12,000	20,000
(Счетчик цепи) Chain count	8,000,000	40,000,000	40,000,000	100,000,000
Таблиц (Tables)	5	7	13	20
Вероятность успеха (Success rate)	99.9%	99.9%	99.9%	99,3%
Общее пространство (Total space)	640 Мб	4,480 Мб	8,320 Мб	32,000 Мб
Макс. время генерации (Max gen. time)	17час	5д 14час	52д	332д
Макс. Время анализа (Max analysis time)	7 с	14 с	11 мин	48 мин

Для последней конфигурации (с полным набором символов) таблицы занимали около 32 гигабайт и требовалось 369 дней для создания, но с такими таблицами любой пароль можно восстановить примерно за час с вероятностью 99,3%. Обычно восстановление таких паролей с помощью брутфорса занимает до 3 недель.

Процесс восстановления и результаты

Когда все параметры выбраны, нажмите кнопку "Старт" (Start) на панели инструментов или выберите Восстановление | Старт (Recovery | Start) в меню "Восстановление" (recovery) и ждите. Во время атаки программа покажет следующую информацию:

- Текущий пароль (Current password) - последний проверенный пароль
- Найдено NT-паролей (NT passwords found) - количество уже найденных NT-паролей. Второе число - это общее количество пользователей, выбранных для текущей атаки.
- Проверено паролей (Passwords checked) - общее количество паролей, проверенных с момента начала атаки.

- Всего паролей (Passwords total) - общее количество паролей, которые нужно попробовать, в соответствии с выбранными параметрами для текущей длины (которая указана в скобках).
- Прошедшее время (Time elapsed) - время, прошедшее с момента начала атаки.
- Оставшееся время (Time left) - время до момента, когда все пароли будут проверены (или атака завершится раньше при нахождении верного пароля) в зависимости от текущей скорости.
- Скорость (Текущая/Средняя) (Speed (Cur/Avg)) - указывает, сколько паролей в секунду проверяет программа (текущих и средних с начала атаки).

Как только программа находит пароли для выбранных пользователей, она сразу показывает их в главном окне. Для LM-атаки программа будет искать каждую половину пароля независимо друг от друга, поэтому может быть вариант, когда она нашла только первую или вторую; когда обе половины будут найдены, программа восстанавливает полный (NT) пароль и "убирает" данного пользователя из проверяемых. Вся информация о восстановленных паролях (в т.ч. о его половинках) записывается (вместе с метками времени) в окно журнала и в файл журнала (если выбрана соответствующая опция).

Брутфорс и словарная атаки являются многопоточными, чтобы использовать все ресурсы SMP-систем, многоядерных процессоров и процессоров с технологией HyperThreading. По умолчанию PPA запускает столько потоков, сколько процессоров (включая «виртуальные» процессоры), установлено в системе. Вы можете изменить количество потоков с помощью параметра командной строки (см. [Опции](#)¹⁹³). Если задействовано более одного потока (Threads), вы можете нажать "Показать подробности" (Show details), чтобы увидеть состояние всех потоков: текущий пароль, общее количество паролей, количество проверенных паролей и скорость, а также общие значения для всех потоков вместе:

Threads	Current	Passwords total	Passwords checked	Speed
localhost		8.353.082.582	160.439.400	7.063.000
● Thread 0	PPLJIF	4.176.541.291	75.585.343	3.793.000
● Thread 1	QUHEQTM	4.176.541.291	84.853.887	3.270.000

5.5.3.6 Отчеты

Когда атака запущена или после ее завершения, вы можете просматривать и сохранять отчеты. Воспользуйтесь кнопкой «Отчеты...» (Reports...) или «Проект» | «Отчеты...» (Project | Reports...) в меню. Доступны следующие отчеты:

Пароли пользователей (Users passwords)

Этот отчет создается в виде CSV-файла (значения, разделенные запятыми), где каждая строка включает имя пользователя, LM-пароль (он разделен пополам; если половина LM-пароля не найдена, она отображается в виде вопросительных знаков) и NT-пароль (при наличии). Такой отчет можно импортировать в любую программу, поддерживающую формат CSV (например, Microsoft Excel), для дальнейшего анализа или построения диаграмм.

Нажмите Параметры (Options), чтобы настроить поля, которые включают: имя пользователя, идентификатор пользователя, компьютер и т. д. (Полный список доступных полей см. в разделе ОЗУ удаленного компьютера (Remote computer RAM) в главе [Получение хэшей паролей](#)^[186]).

Пароли ко времени (Passwords by time (running total))

Это графический отчет, который показывает текущее количество восстановленных паролей; его также можно скопировать в буфер обмена или сохранить как файл формата .BMP.

Вы также можете сохранить отчет в виде XML-файла. В Параметрах (Options) установите поля, которые вы хотите распечатать в выходной файл; вы также можете указать, сохранять ли все учетные записи или только те, для которых были найдены пароли. Для каждой учетной записи PPA записывает следующие данные:

- Надежность пароля (Password Strength): слабая - Weak (восстановление возможно менее чем за один день), сильная - Strong (от одного дня до одной недели) или очень сильная - Very Strong (более одной недели)
- Набор символов пароля (Password Charset): буквенный - Alpha, цифровой - Numeric и т. д.
- Метод аудита пароля: предварительная атака - Preliminary attack, брутфорс - Bruteforce attack, атака по словарю - Dictionary attack или радужная атака - Rainbow attack.
- Распределение длины пароля (Password Length Distribution)

5.5.3.7 Настройки программы

Сохранять настройки каждые (N минут) (Save setup every (minutes))

Сохраняет текущие настройки каждые N минут. *Настоятельно рекомендуется включить эту опцию.*

Интервал обновления индикатора выполнения (мс) (Progress bar update interval (ms))

Позволяет установить интервал (в миллисекундах) между обновлением индикатора выполнения и окна состояния; по умолчанию 500.

Скрыть найденные пароли (Hide found passwords)

Если эта опция включена, пароли маскируются звездочками.

Журнал (Log file)

Если этот параметр включен, программа сохраняет информацию, отображаемую в окне состояния, в файл журнала (ppa.log).

Свернуть в трей (Minimize to tray)

Сворачивает окно в трей.

Приоритет (Priority)

Нормальный (Normal) или высокий (high). Установка для этого параметра значения «Высокий» относительно увеличивает производительность, но это серьезно сказывается на быстродействии вашего компьютера.

Опции предварительной атаки (Preliminary attack options)

- Атака через информацию о пользователе (User info attack): проверить, не совпадают ли пароли с именами пользователей
- Атака через информацию в Windows (Windows info attack): восстановление кэшированных паролей (для пользователей HelpAssistant, VUSR_*, IIS_* и т. д.), пароля для автоматического входа в систему, и пароля, сохраненного в памяти процесса WinLogon
- Атака из кэша паролей (Password cache attack): проверка паролей по «внутреннему» словарю/списку слов, созданному из паролей, которые были найдены во время предыдущих сессий.
- Простая атака по словарю (Simple dictionary attack): атака с использованием небольшого, но эффективного встроенного в PPA словаря
- Простая брутфорс-атака (Simple brute-force attack): атака перебором паролей длиной до трех символов

Первые три атаки очень быстрые, последняя обычно занимает несколько секунд (до нескольких минут на медленных компьютерах с большим количеством учетных записей).

Язык (Language)

Переключает язык пользовательского интерфейса.

Поддерживаемые параметры командной строки: имя проекта - project name (файл .hdt) и количество потоков - the number of threads (см. [Процесс восстановления и результаты](#)^[191]). Чтобы запустить PPA с определенным количеством потоков, используйте следующую командную строку:

```
ppa.exe -threads N
```

где N - количество потоков.

Часть VI

Мобильная криминалистика

6 Мобильная криминалистика

6.1 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.

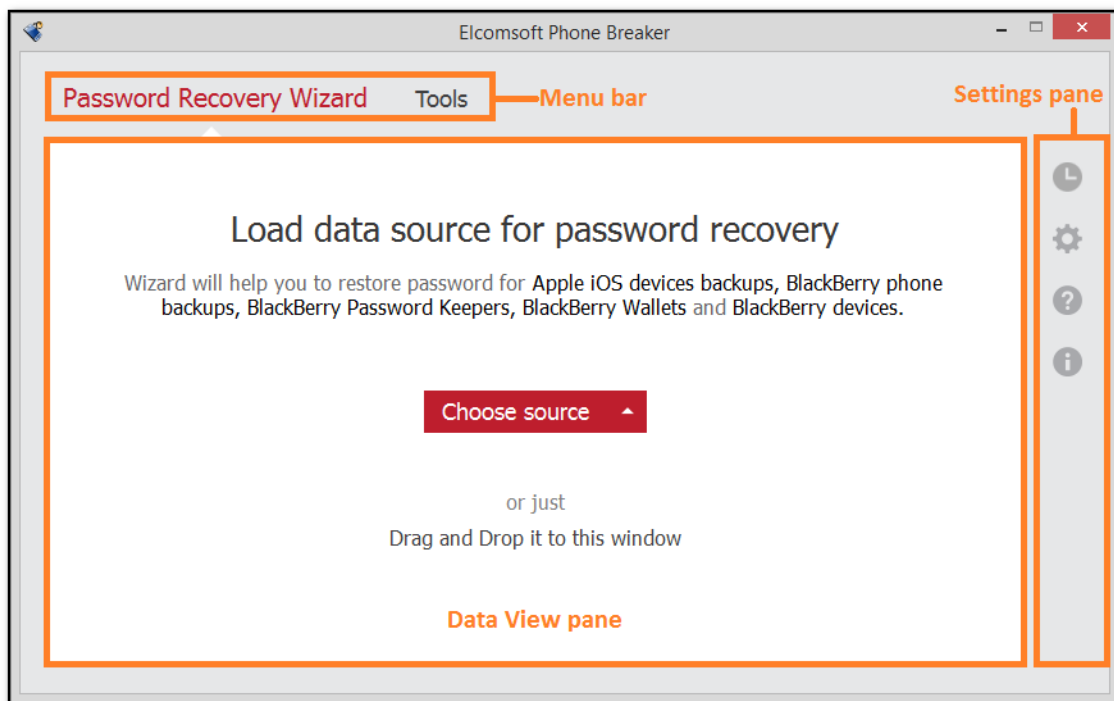
Сценарии использования:

- 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

6.2 Elcomsoft Phone Breaker

6.2.1 Информация о программе

6.2.1.1 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](#)^[225], расшифровка FileVault, просмотр [Связки ключей](#)^[207], извлечение [маркеров аутентификации](#)^[252].
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, заprotoколированных 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.

6.2.1.2 Раздел настроек

В Elcomsoft Phone Breaker доступен ряд настроек.

Для доступа к настройкам нажмите  в области настроек.

• General

Общие настройки:

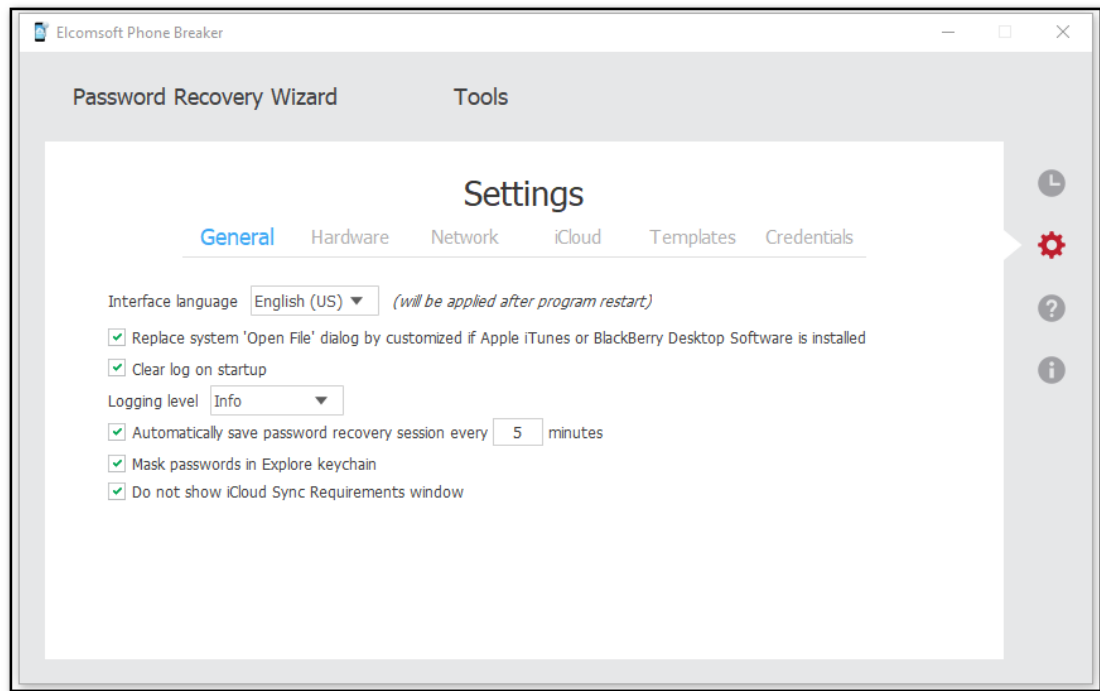
- **Язык интерфейса / Interface Language:** переключение языка интерфейса между английским и русским. После переключения необходимо перезапуск программы.
- **Заменять системный диалог открытия файла, если установлен Apple iTunes:** если выбрано, диалог открытия файла будет выглядеть так же, как в Apple 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_u_ревизии>.log
 - **macOS:** ~/Users/<username>/Library/Application Support/Elcomsoft Phone Password Breaker/EPB_<номер_версии_u_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:

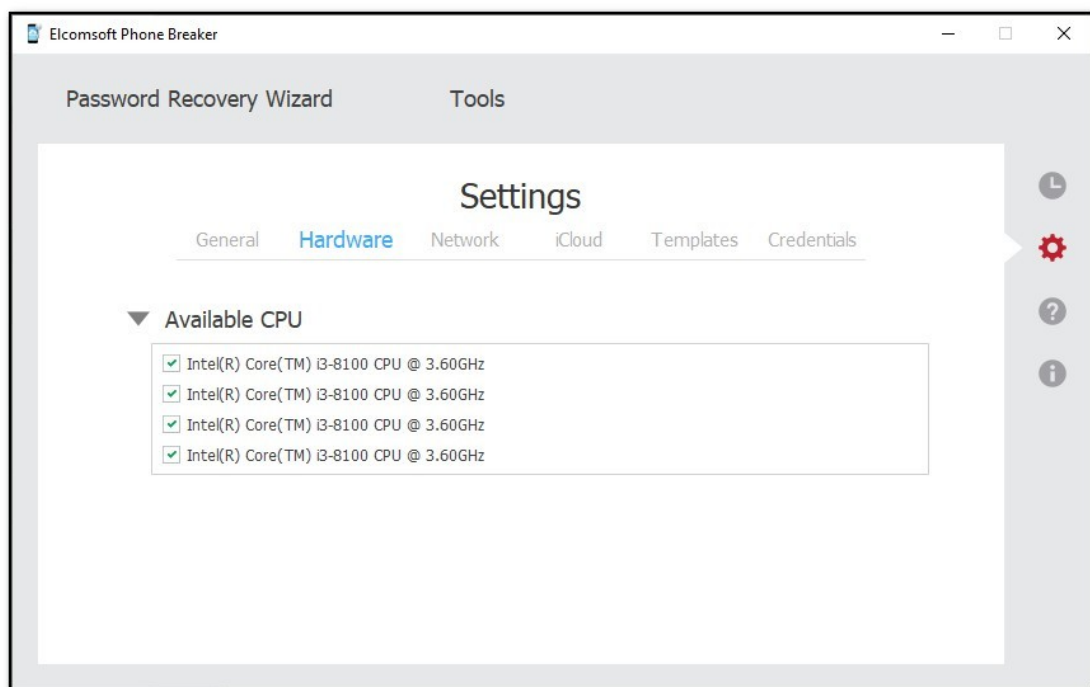
Уровень	Описание
None	Журналирование отключено
Fatal	Сохраняется только информация о критических ошибках
Error	Дополнительно сохраняется информация об ошибках
Warning	Дополнительно сохраняются предупреждающие сообщения
Info	Дополнительно сохраняются информационные сообщения
Debug	Уровень журналирования 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]**

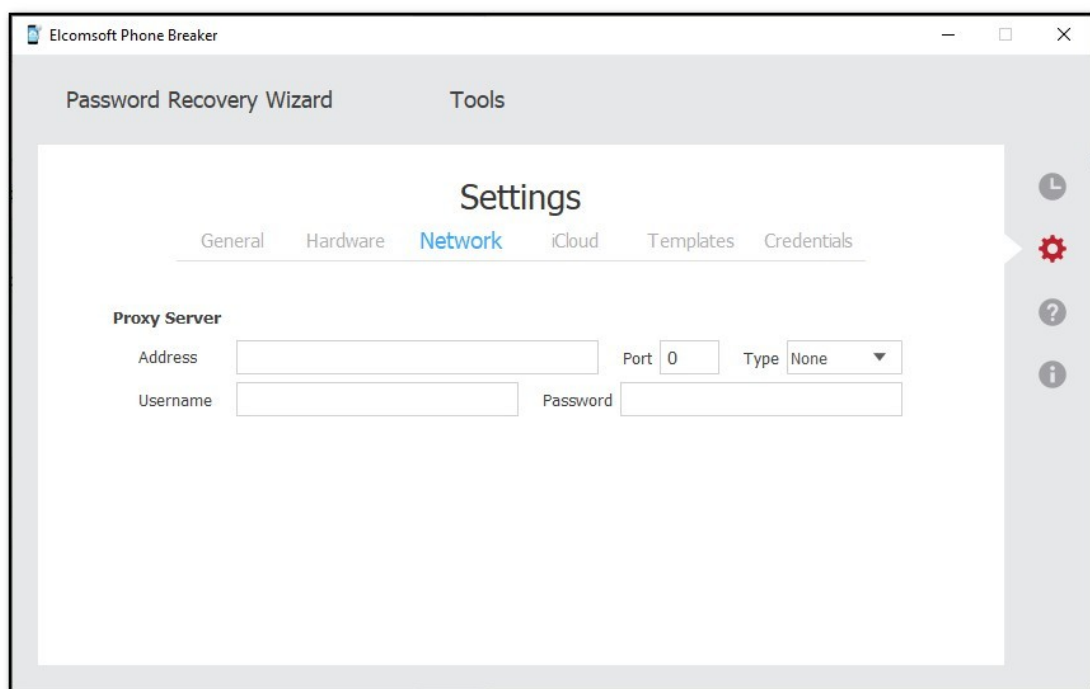
На странице Hardware/Оборудование указывается количество ядер CPU/ЦПУ и GPU/ГПУ, которые будет использовать EPB.



- **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).

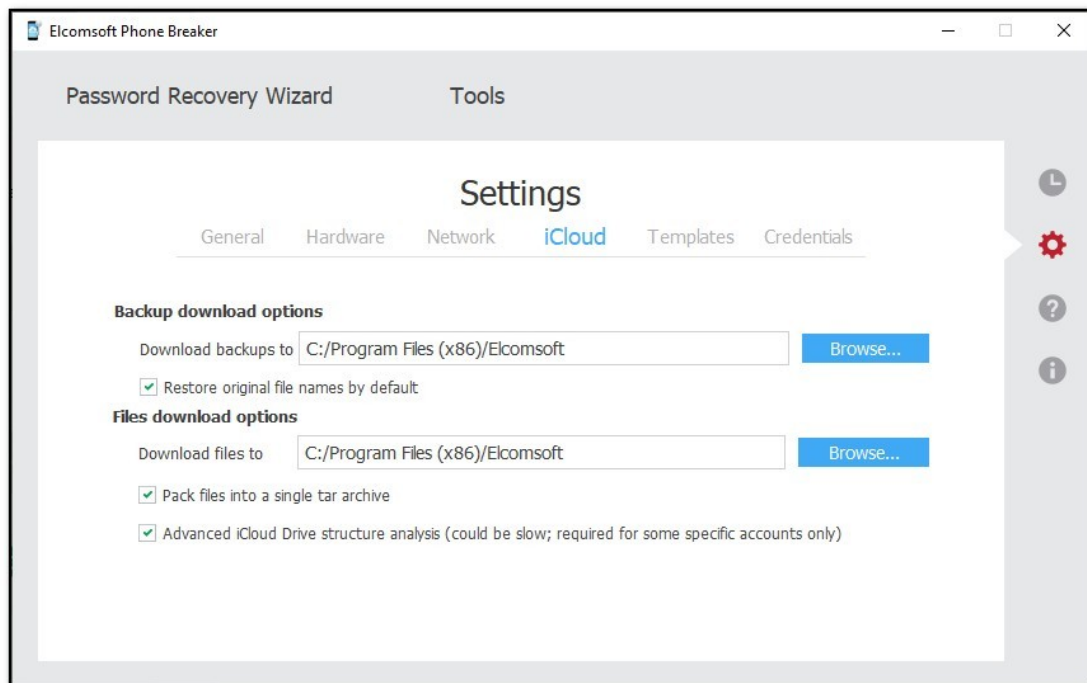
Внимание: восстановить оригинальные имена файлов можно в любое время после скачивания данных или расшифровки локальной резервной копии командой **Tools/Инструменты -> Apple/Apple -> Decrypt backup/Расшифровать рез. копию, выбрав режим Restore original file names/Восстановить исходные имена файлов.**

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](#)^[283] для атаки на пароль. Шаблон включает в себя комбинацию настроек атаки.

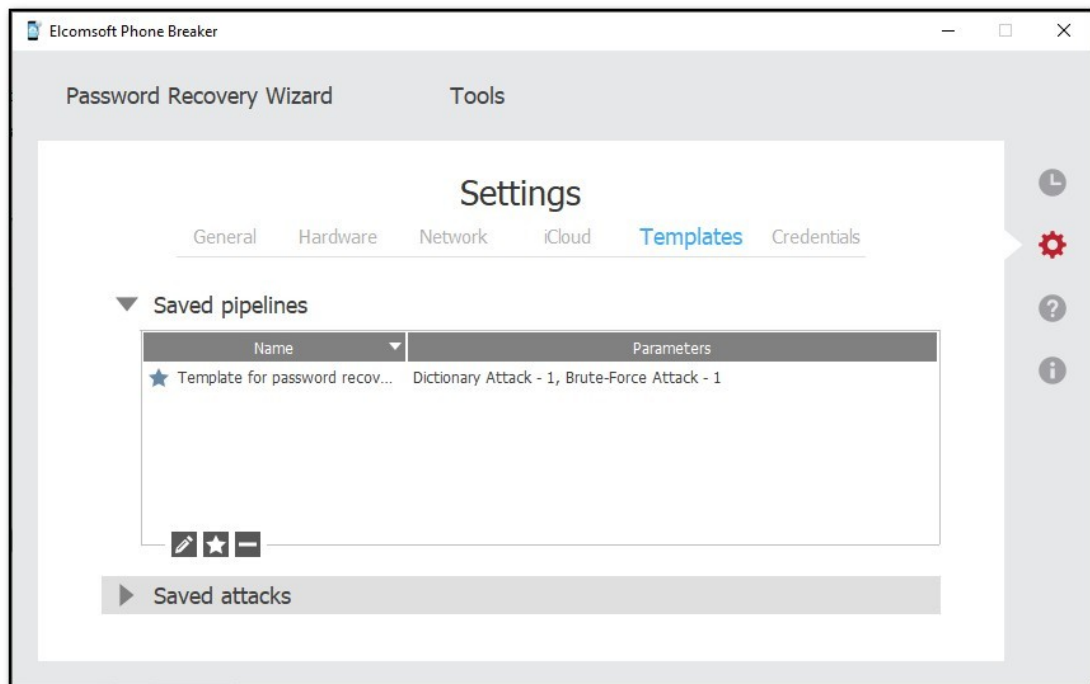
Процесс восстановления пароля состоит из одной или нескольких атак. Комбинация таких атак носит название очереди атак. Дополнительно см. раздел [Password recovery attacks](#)^[272].

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** .

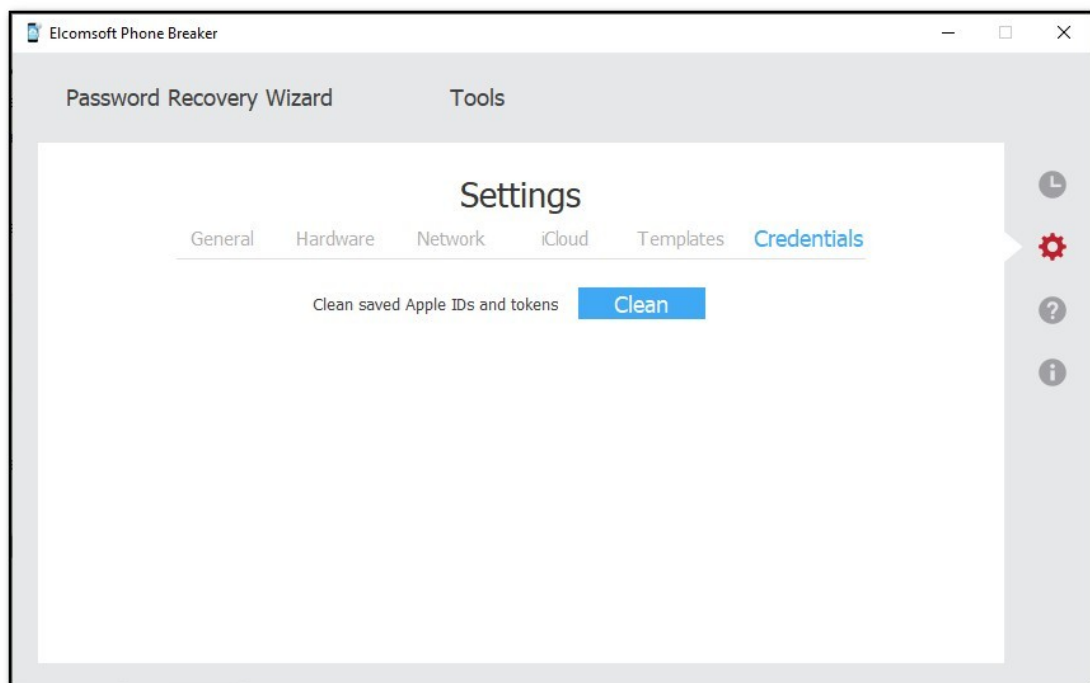
Установить шаблон по умолчанию можно кнопкой . Шаблон по умолчанию будет использоваться каждый раз, когда вы используете опцию **Password recovery/Восстановление пароля**.

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**.



6.2.1.3 [Windows] Аппаратное ускорение

Перебор паролей в версии EPV 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.

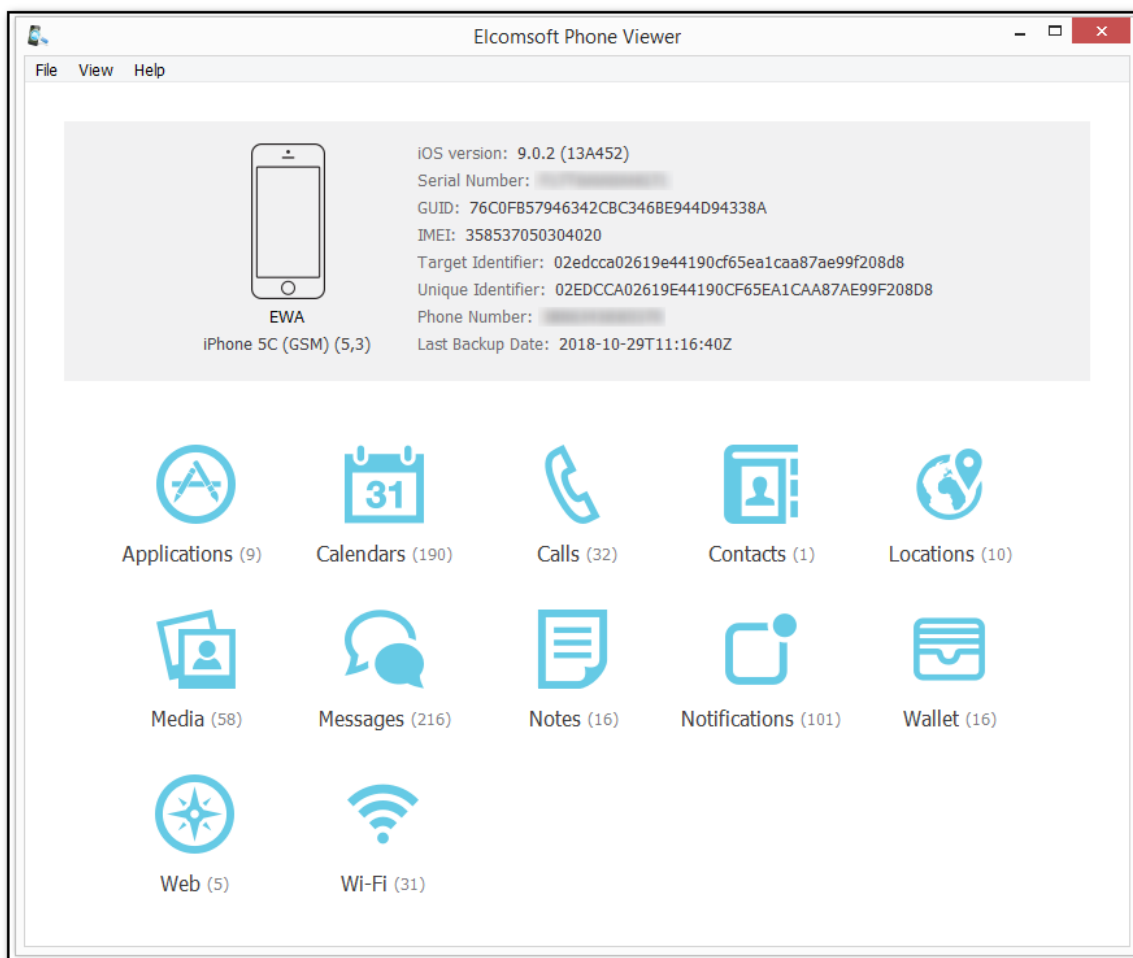
Внимание: аппаратное ускорение CUDA недоступно при работе через удалённый доступ (RDP).

6.2.2 Работа с устройствами Apple

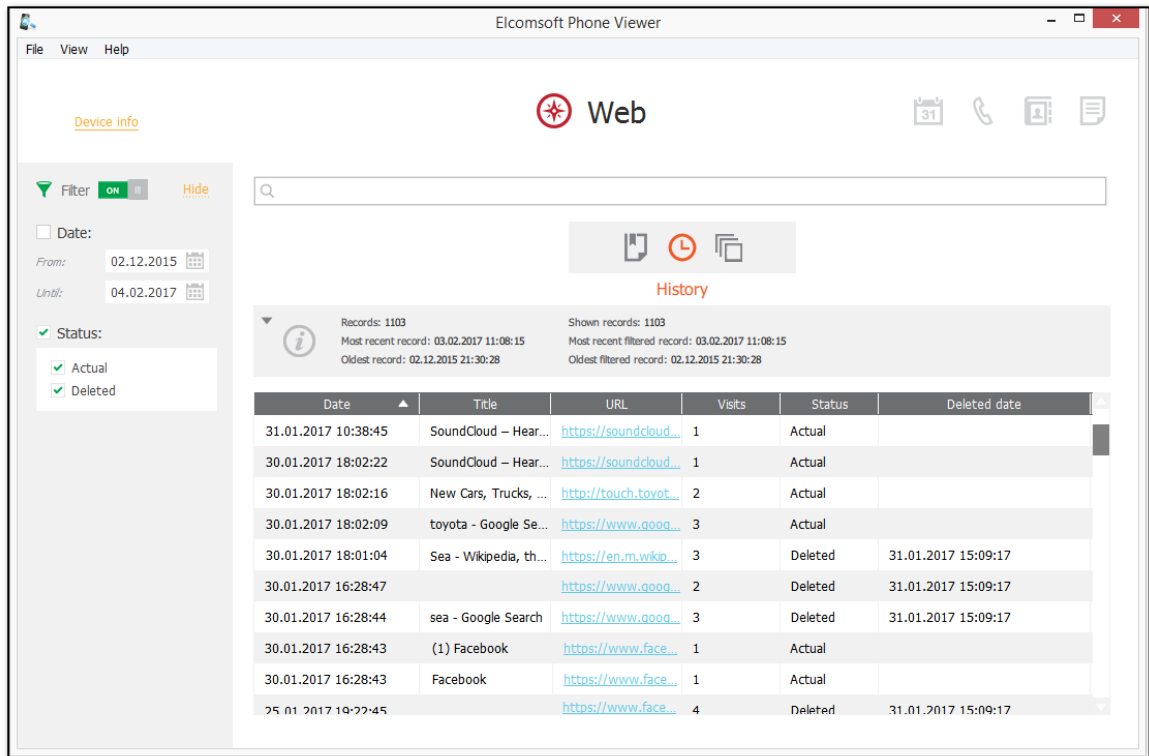
6.2.2.1 Анализ резервных копий iTunes и iCloud

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.

6.2.2.2 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 ЕРВ 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 ЕРВ)	Пароль к резервной копии
iTunes (зашифрован)	Пароль к резервной копии

ЕРВ позволяет просматривать данные Облачной связки ключей iCloud Keychain (*iCloud_Keychain.xml* file) и синхронизированных из [iCloud](#) ^[243] данных (*icloud_synced.xml* file).

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

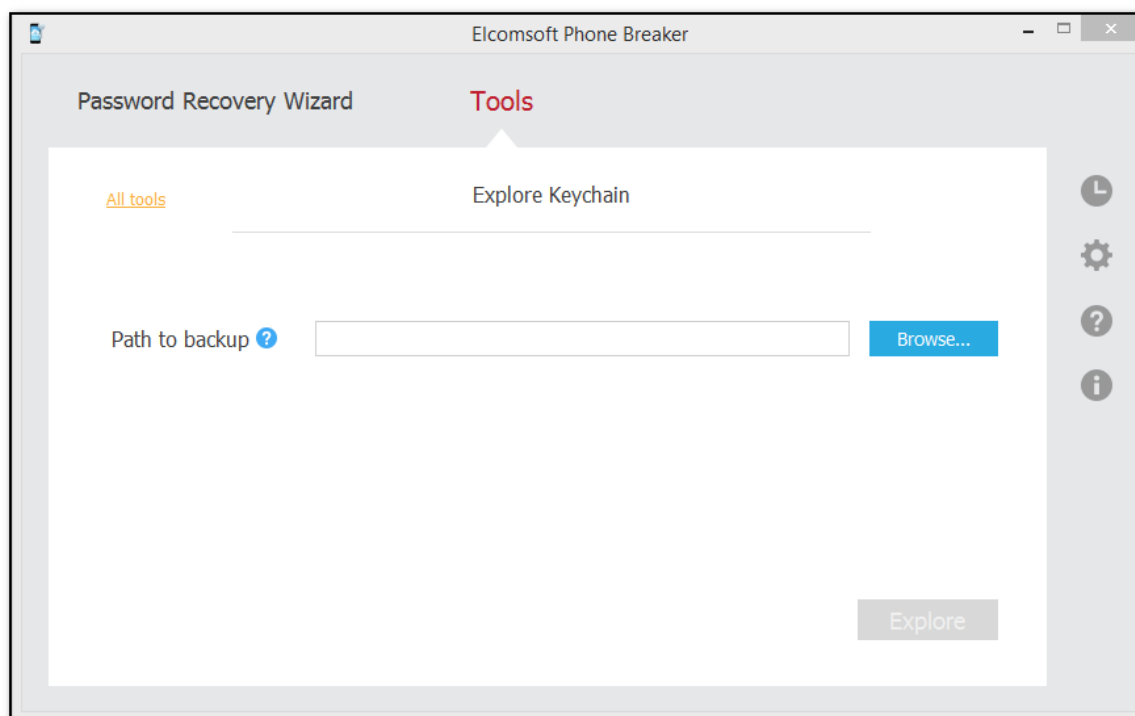
Для анализа Связки ключей:

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

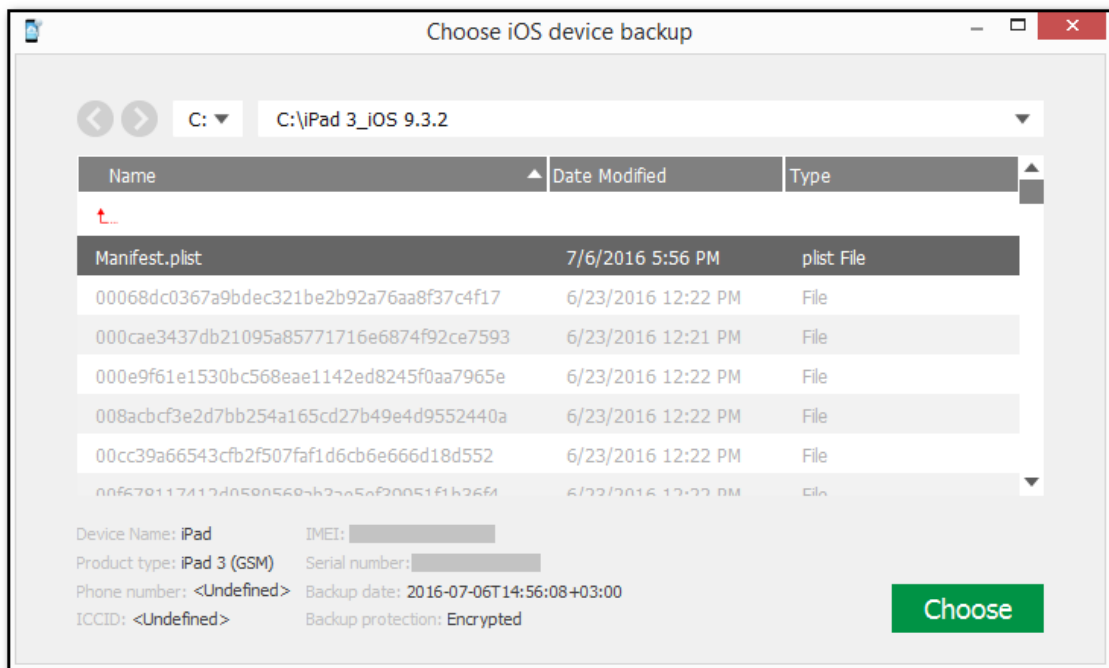
Источник данных	Имя файла
Резервная копия iTunes	<i>Manifest.plist</i>
Данные Связки ключей, скачанные при помощи EPB 9.50 и более старых версий	<i>iCloud_Keychain.xml</i>
Данные Связки ключей, скачанные при помощи EPB 9.60 и более новых версий из синхронизированных данных iCloud ²⁴³	<i>icloud_synced.xml</i>
Образ данных, извлечённый посредством Elcomsoft iOS Forensic Toolkit	<i>keychaindump.xml</i>

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**.

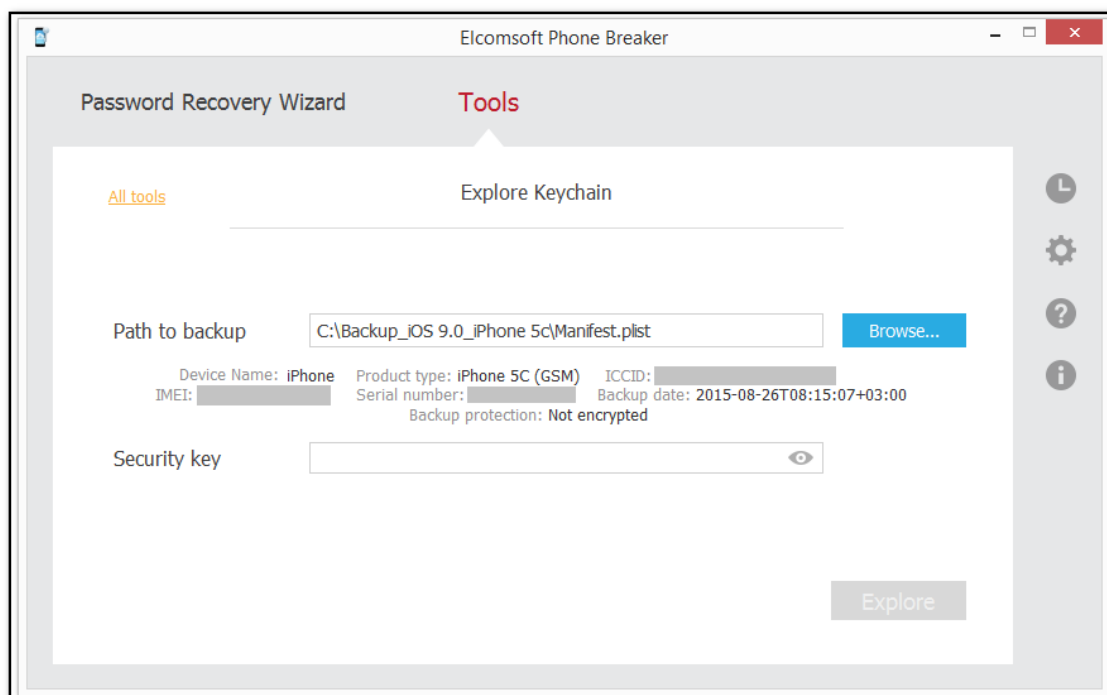



3. Выберите файл и нажмите **Continue/Продолжить**.



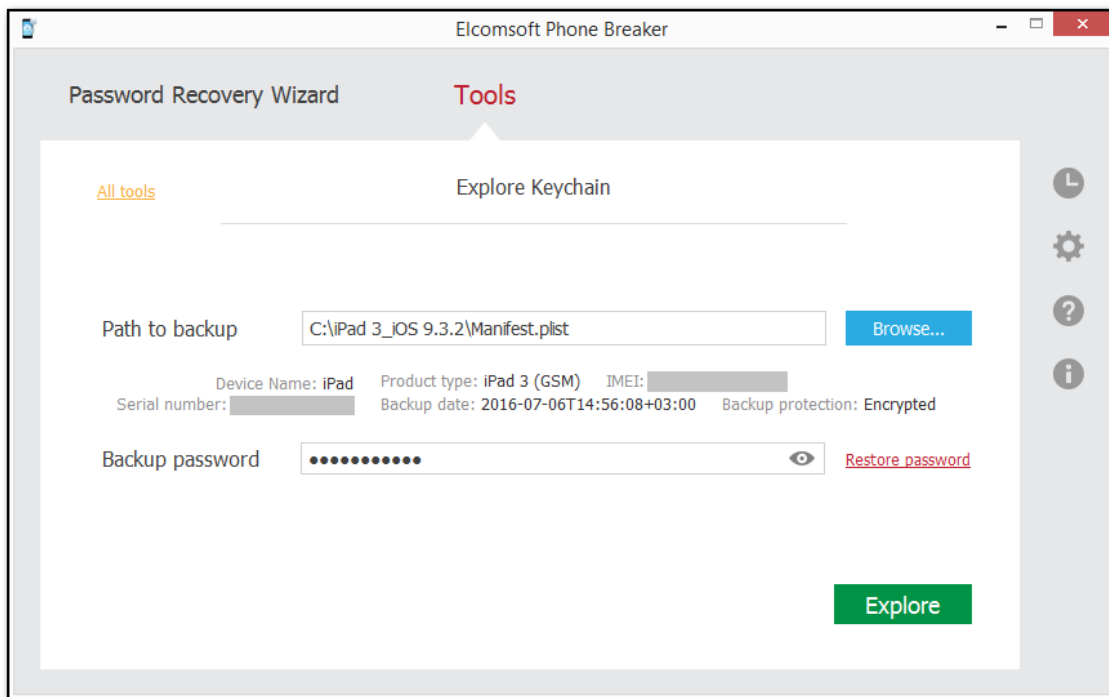
4. В зависимости от того, зашифрована ли резервная копия:

- **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](#)²⁶⁸.)



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

5. Записи отображаются по категориям:

Категория	Общая информация	Информация для категории
Apple ID	<ul style="list-style-type: none"> ○ Название: источник данных в Связке ключей 	<ul style="list-style-type: none"> ○ Apple ID (учётная запись) ○ Пароль
Wi-Fi accounts	<ul style="list-style-type: none"> ○ Дата создания ○ Дата последнего изменения 	<ul style="list-style-type: none"> ○ SSID (учётная запись) ○ Пароль
Mail accounts		<ul style="list-style-type: none"> ○ Протокол ○ Учётная запись ○ Пароль
Browser passwords		<ul style="list-style-type: none"> ○ Адрес ○ Учётная запись ○ Пароль
Credit cards		<ul style="list-style-type: none"> ○ Название карты

		<ul style="list-style-type: none"> ○ Имя держателя карты ○ Номер карты ○ Срок окончания действия
DSIDs & Tokens		<ul style="list-style-type: none"> ○ Маркер аутентификации ○ 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.

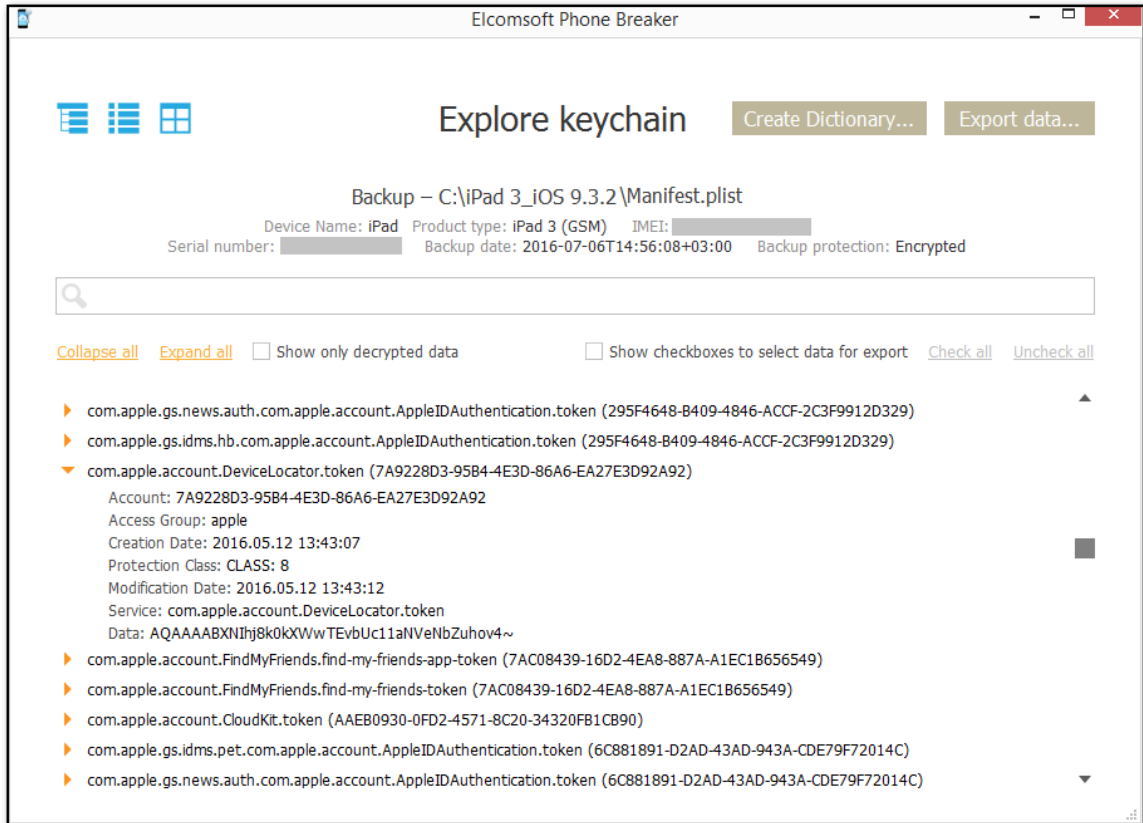
Командой **Show only decrypted data/Показать только расшифров. записи** можно скрыть записи, которые не были расшифрованы. Рекомендуется использовать с целью упрощения анализа.

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

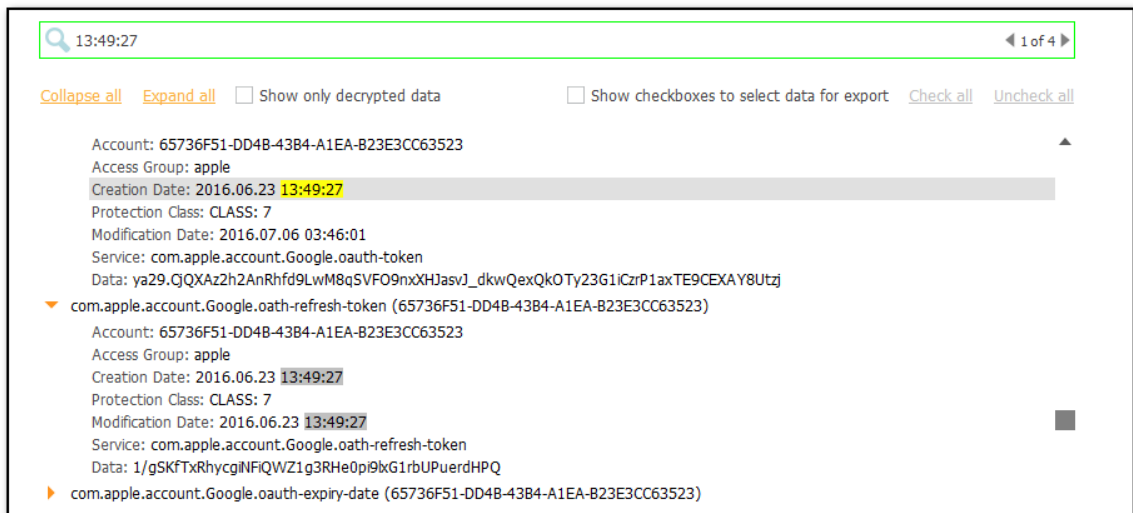
Раскрыть информацию обо всех записях можно командой **Expand all/Развернуть все**.

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

Для того, чтобы вместо паролей отображалась маска из символов *, зайдите в настройки [EPB Settings](#)¹⁹⁹ и отметьте **Mask passwords in Explore keychain/Скрыть пароли при просмотре связки ключей**.

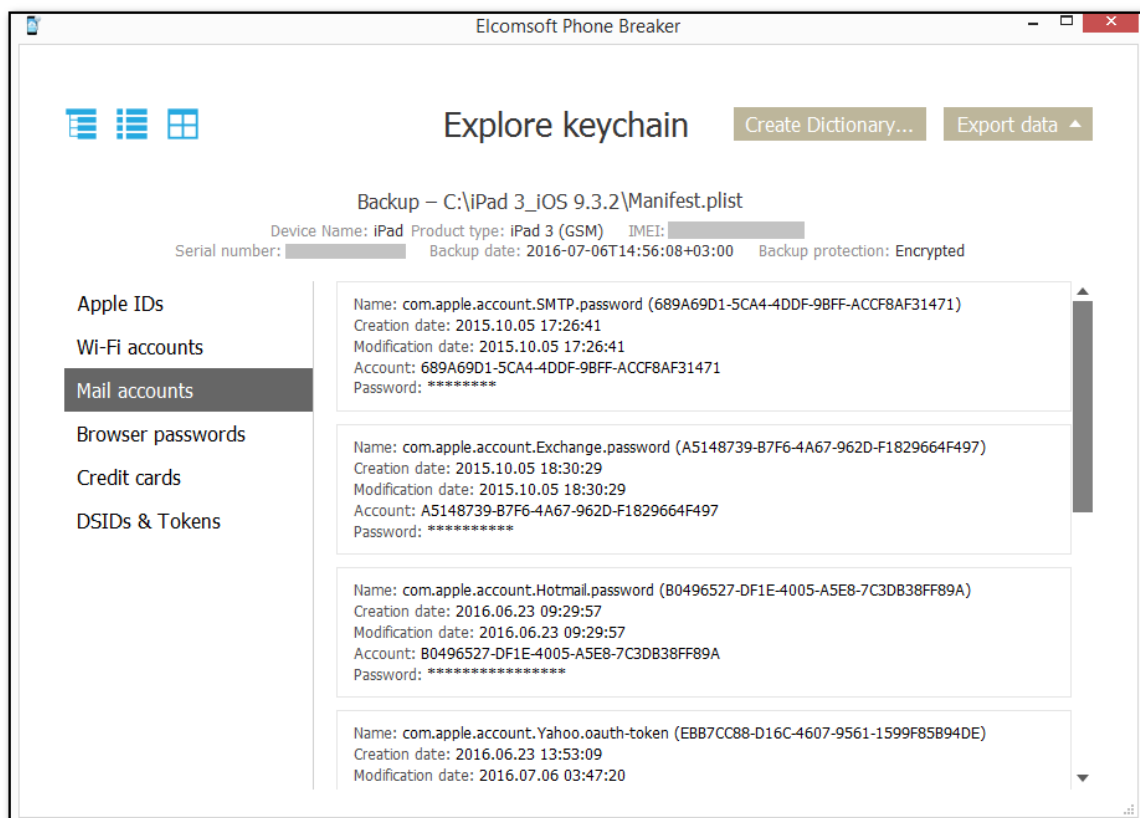



В строке поиска можно вводить поисковые запросы. Если будет найдено больше одной записи, между ними можно переключаться, нажимая на стрелки в окне поиска.



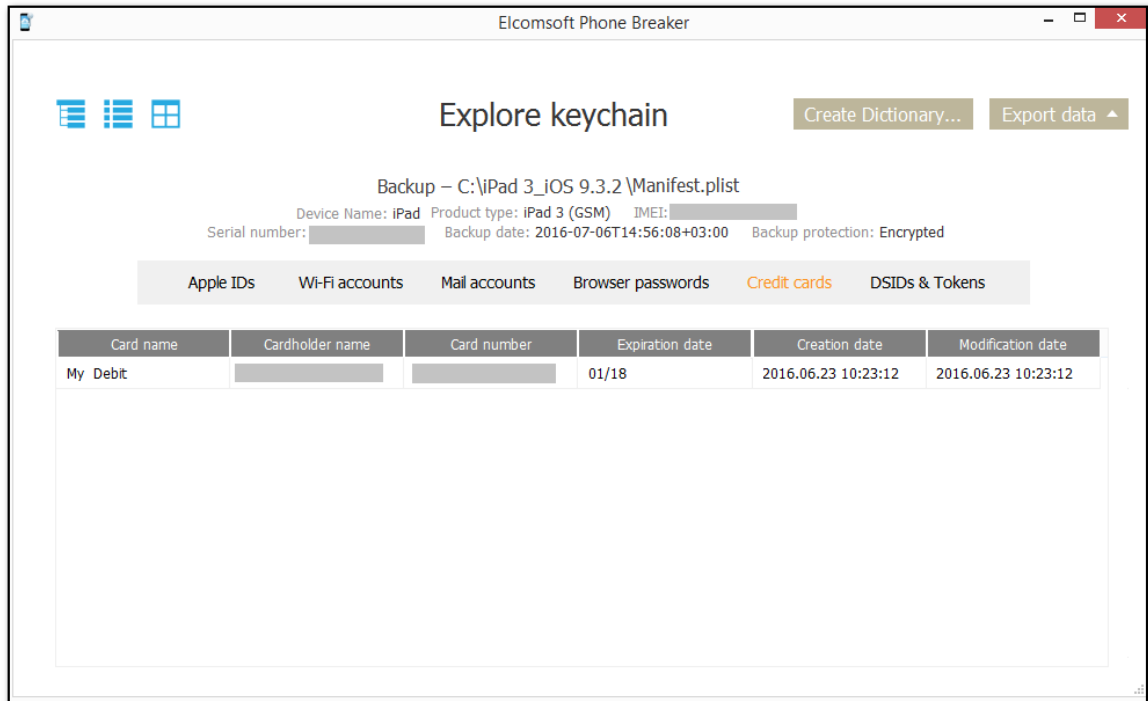
- **Категории:** отображение категорий включается нажатием иконки .

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**.

6.2.2.3 Резервные копии iTunes

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%\Apple Computer\MobileSync\Backup\ (если вы загрузили iTunes из Microsoft Store)

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).

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.

EPV 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.

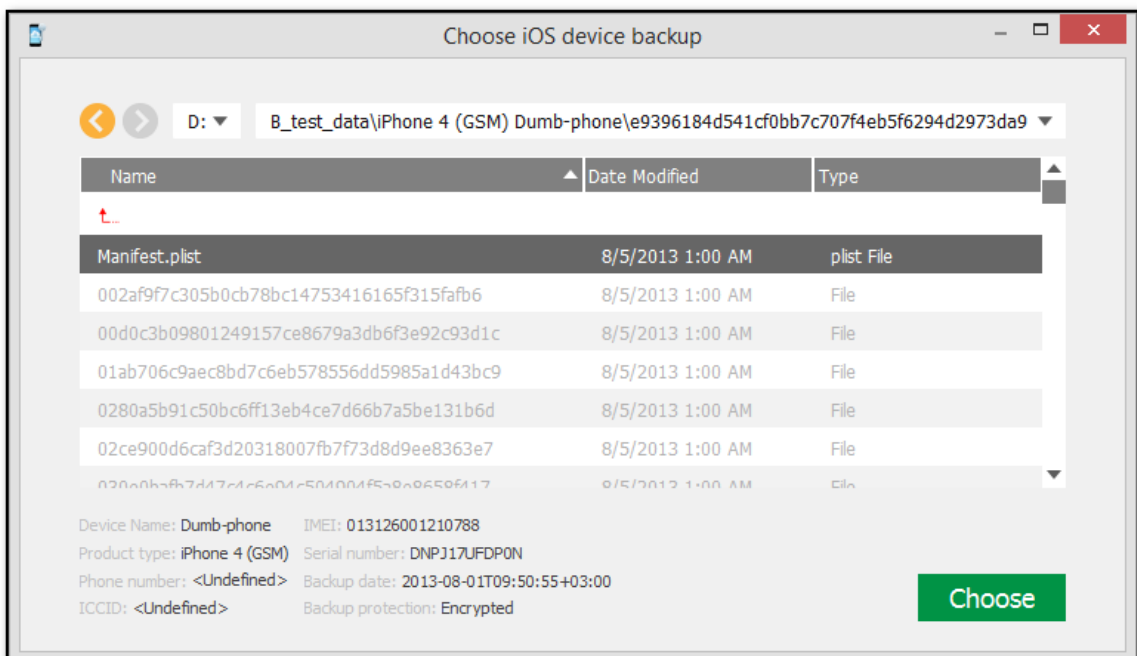
Для восстановления оригинальных имён файлов проделайте следующие шаги:

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 EPV. Детали в секции **Troubleshooting**.

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

Свойства файлов перечислены в таблице.

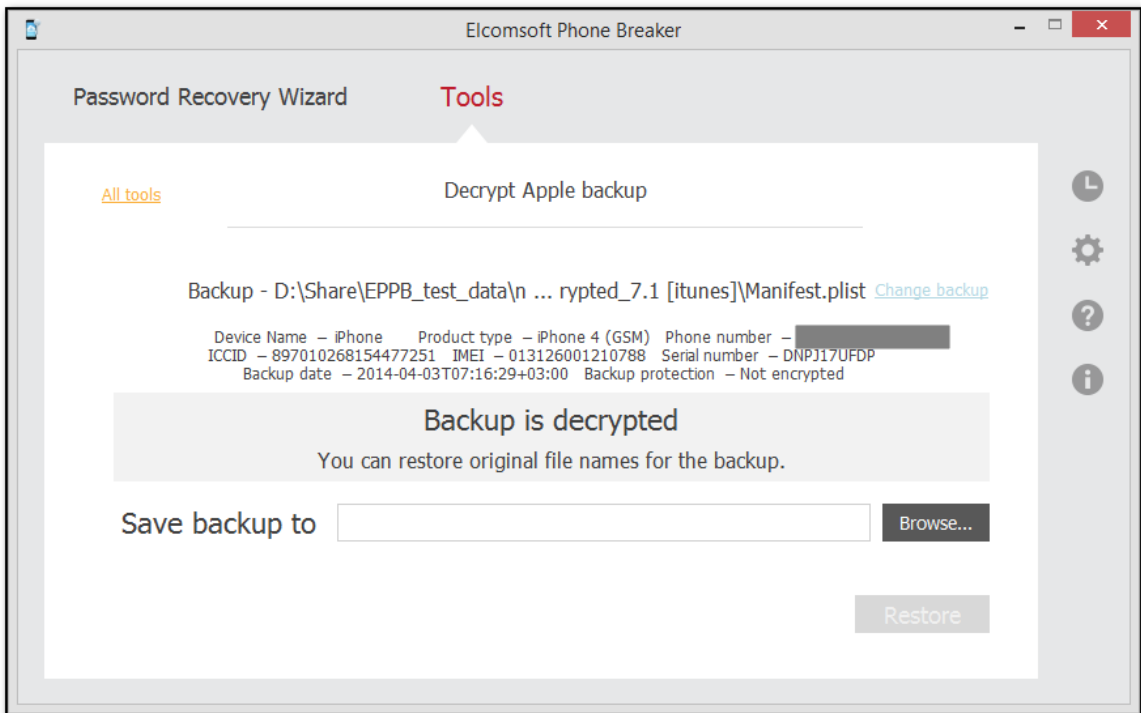


5. После загрузки резервной копии вы сможете просмотреть информацию:

- **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.)

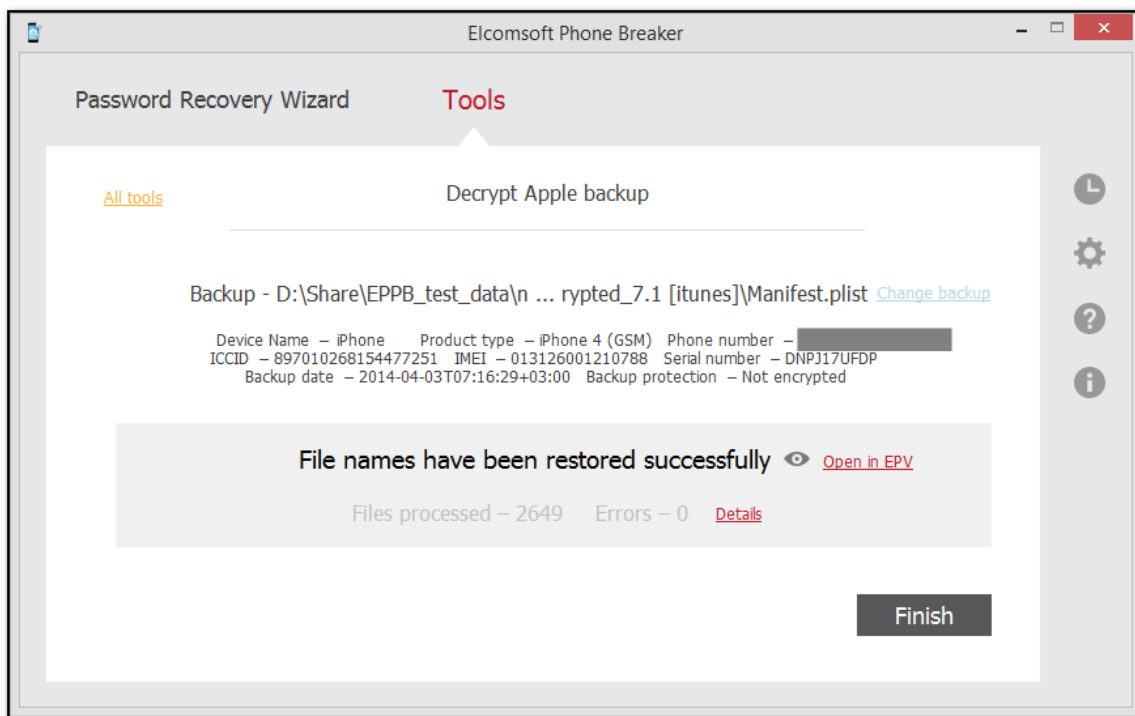
Выбрать другую резервную копию можно, нажав **Change backup/Заменить рез. копию**.




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](#) ²²² доступен нажатием на кнопку **Details/Подобности**.

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

Резервные копии с паролем

EPV 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.

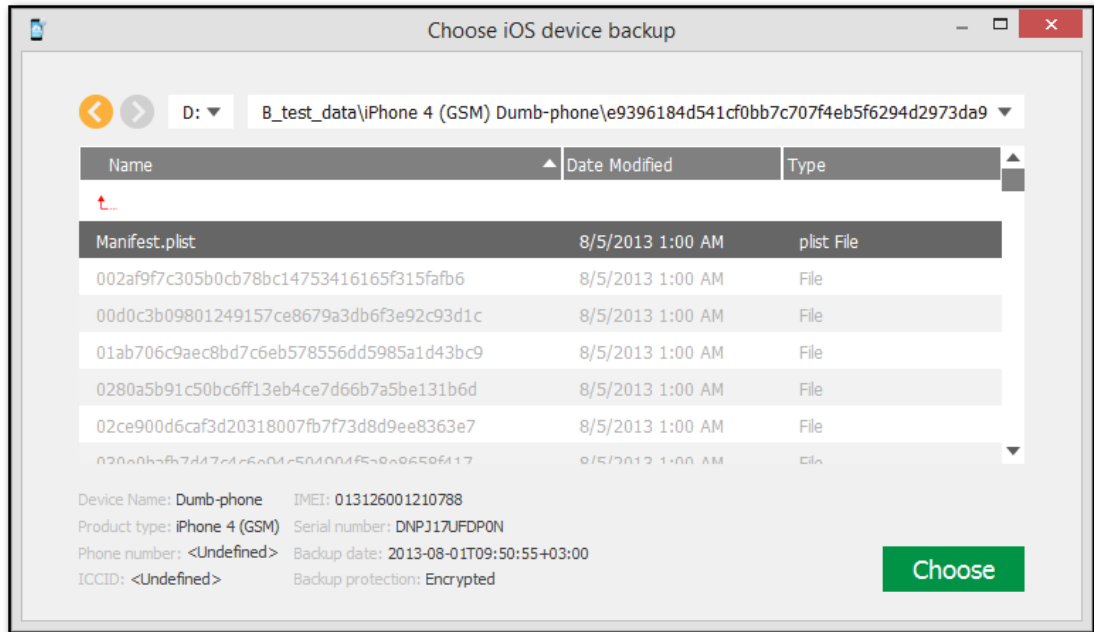
Открыть резервную копию:

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.

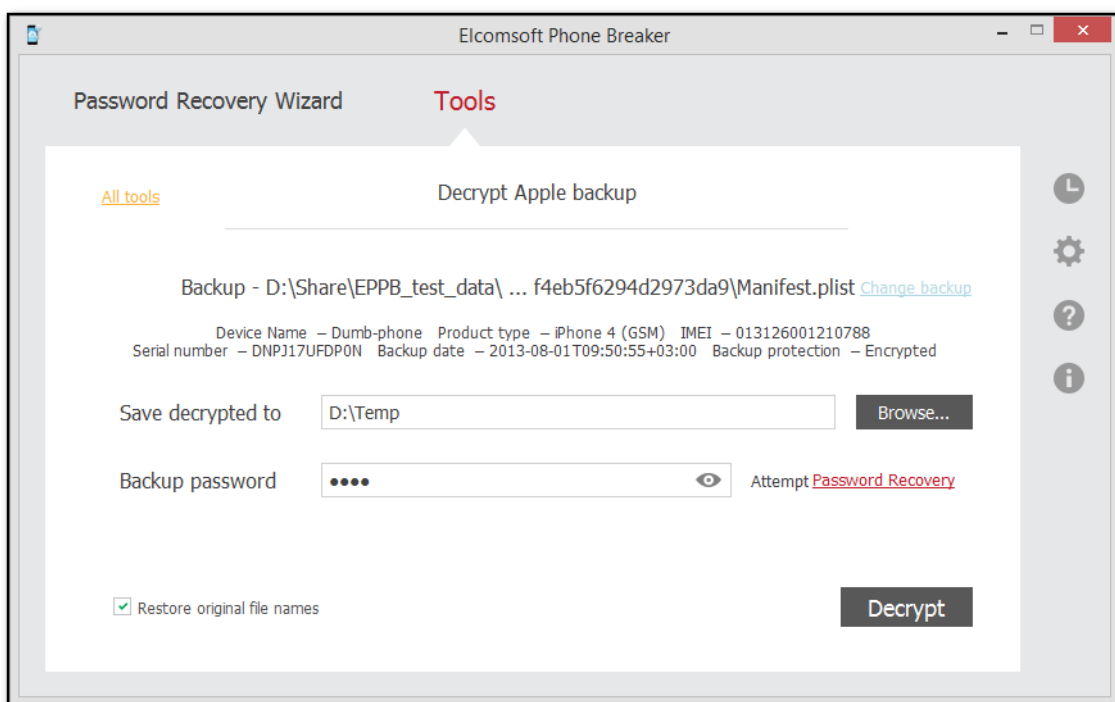


5. После загрузки резервной копии вы сможете просмотреть информацию:


- **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 (*).

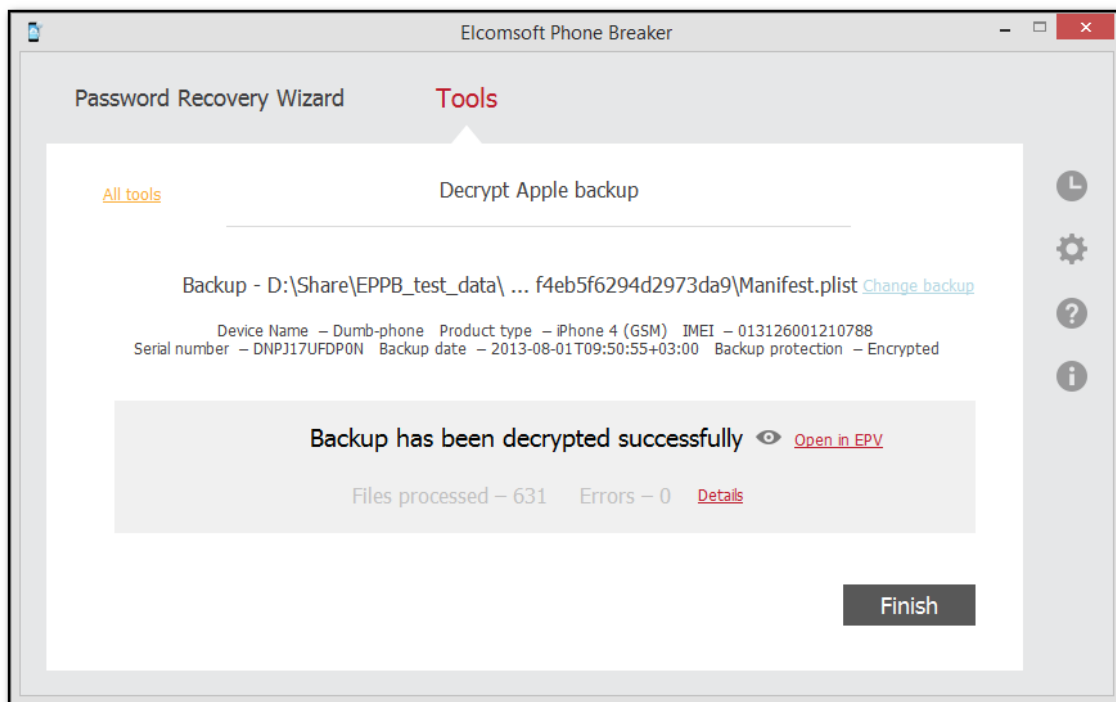
В EPB для Windows OS доступна опция **Restore password/Восстановить пароль**, позволяющая восстанавливать неизвестные пароли методом перебора.

- **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**.



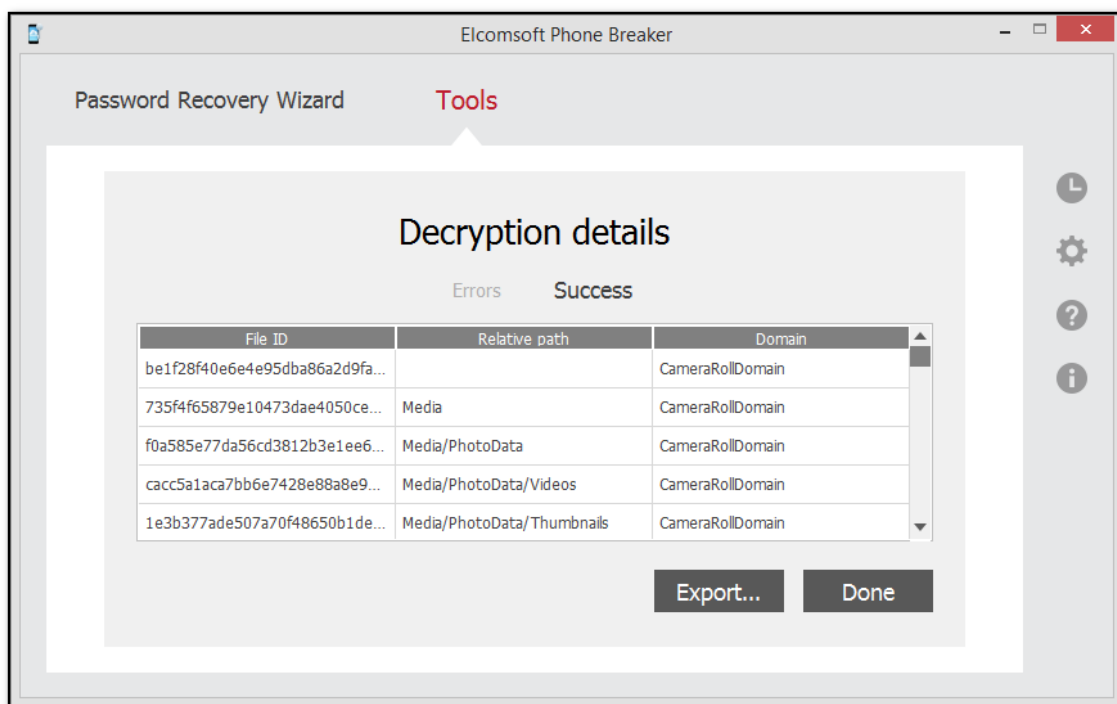
9. [Отчёт](#) ²²² доступен нажатием на кнопку **Details/Подобности**.

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

Отчёт о расшифровке

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

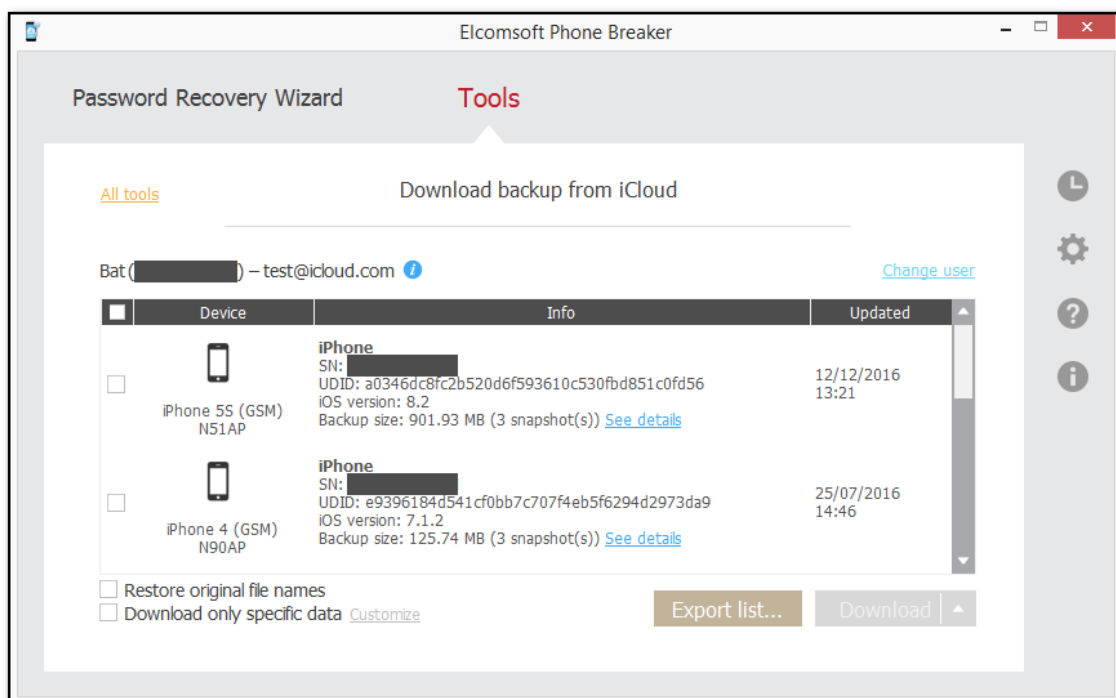
Для выхода нажмите **Done/Готово**.

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.

6.2.2.4 Работа с iCloud

Резервные копии в iCloud

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](#)^[252], которые могут быть доступны на компьютере пользователя.

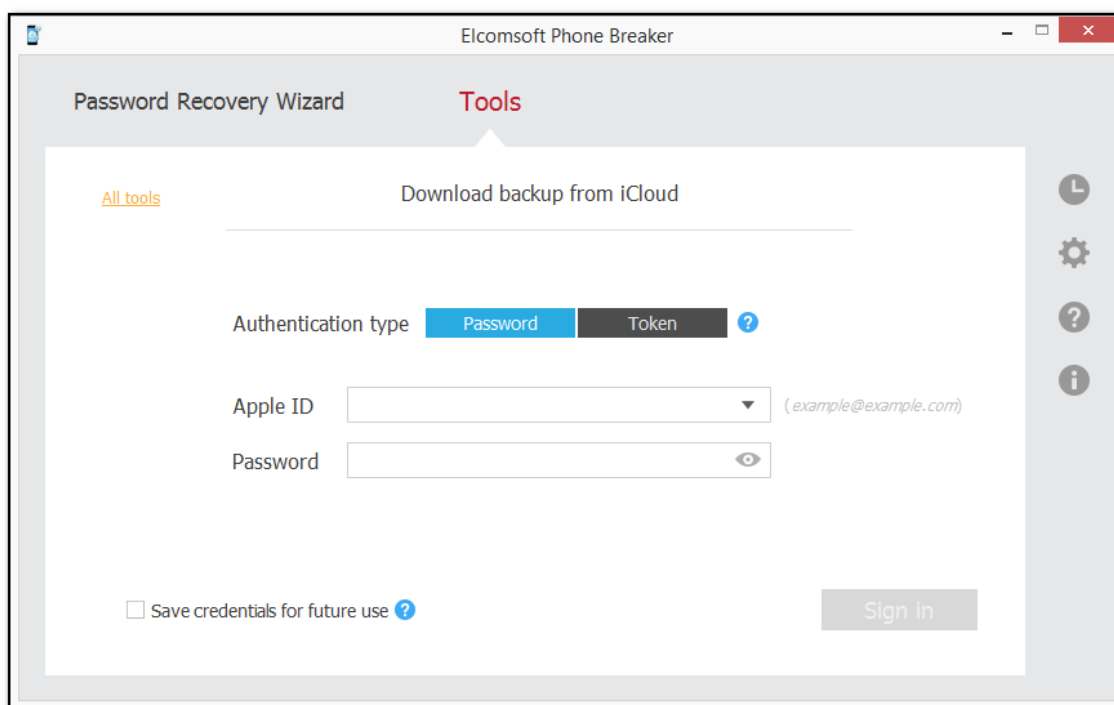
EPB сохраняет "облачные" резервные копии в том же формате, который используется iTunes. После расшифровки данных вы сможете [просмотреть содержимое](#)^[205] в Elcomsoft Phone Viewer.

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](#) [252].

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](#).

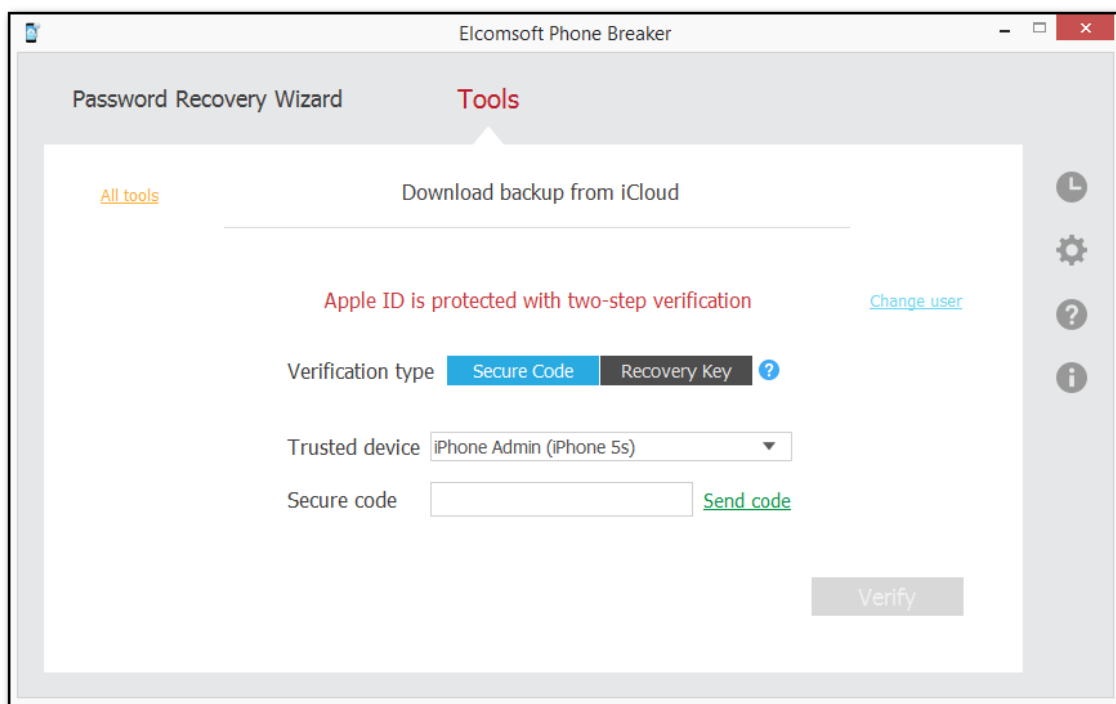
Внимание: если Apple ID защищен двухфакторной аутентификацией, вам необходимо подтвердить отправку проверочного кода на доверенные устройства или сообщения на телефонный номер.

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**.



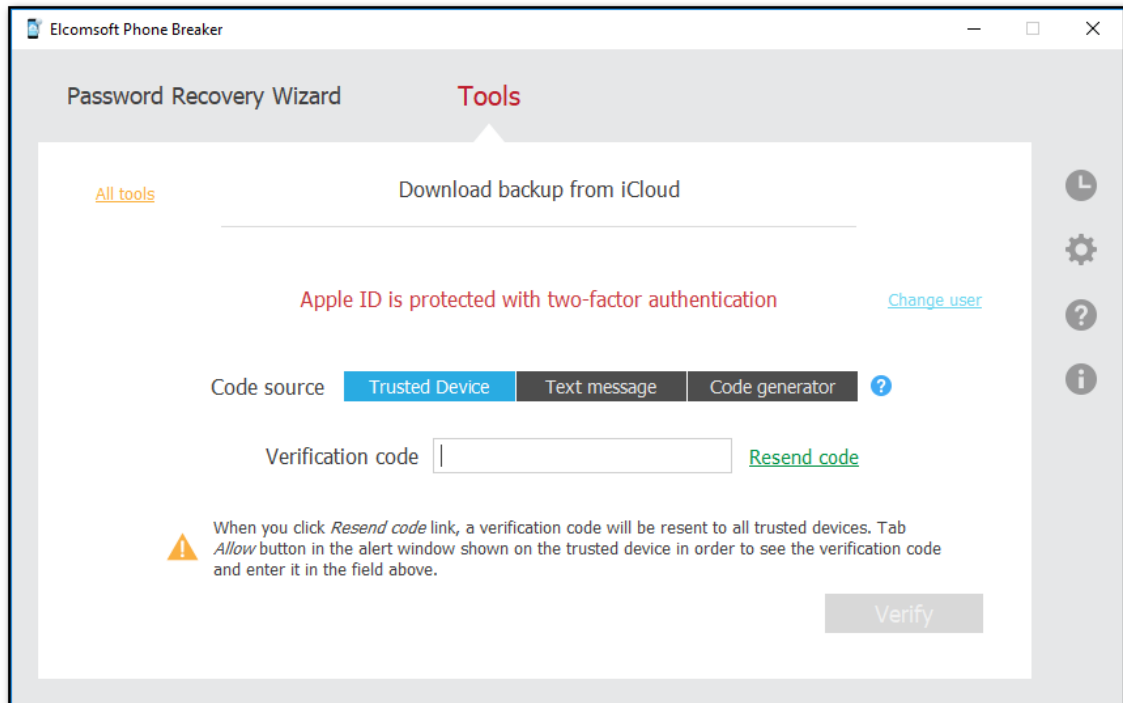
7. Если Apple ID защищён актуальным способом двухфакторной аутентификации (two-factor authentication), вам доступны следующие варианты:

- 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.

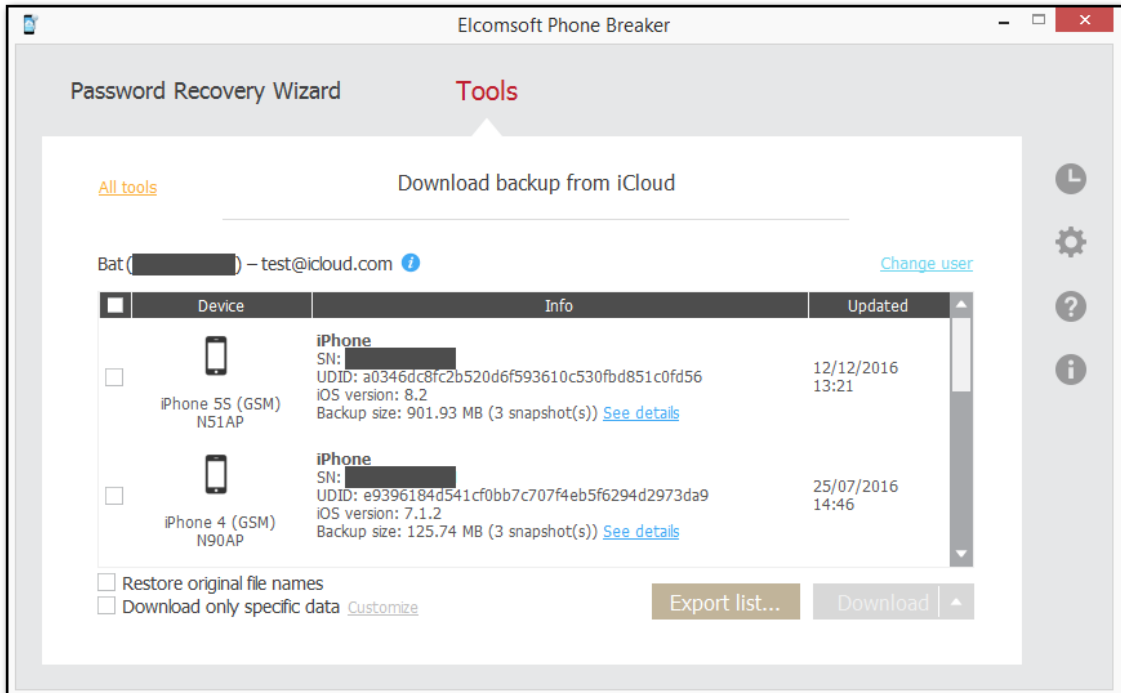


8. Нажмите **Verify/Проверить**.

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**.

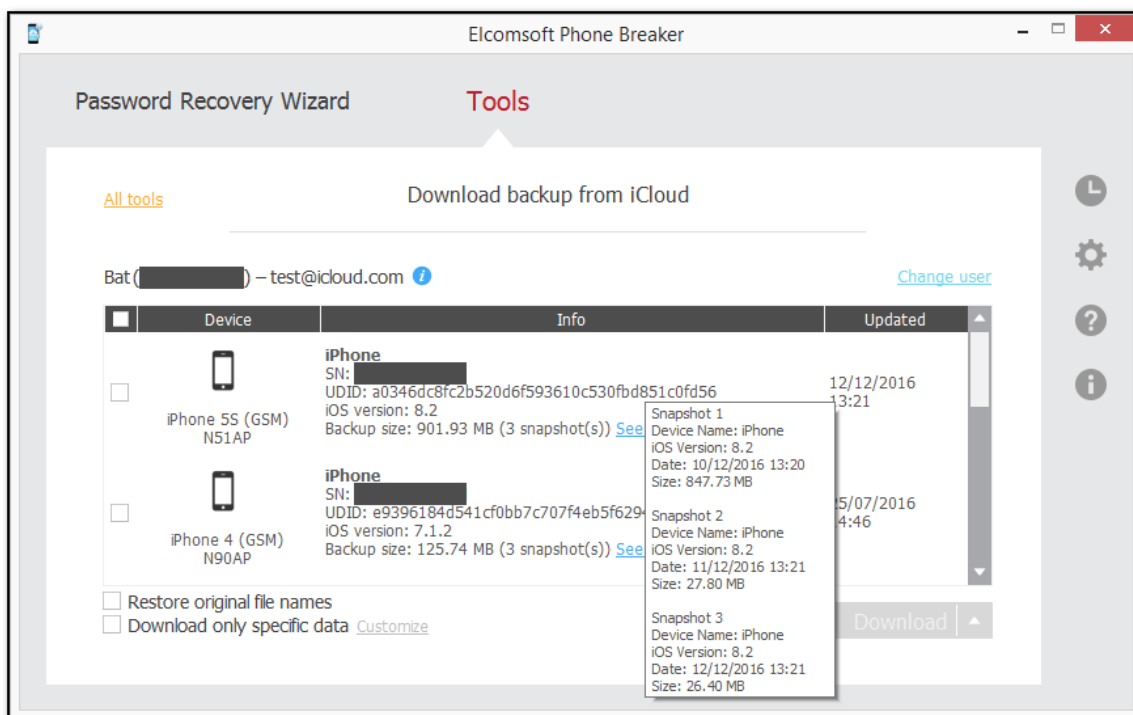


Для всех устройств доступна следующая информация:

- 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.

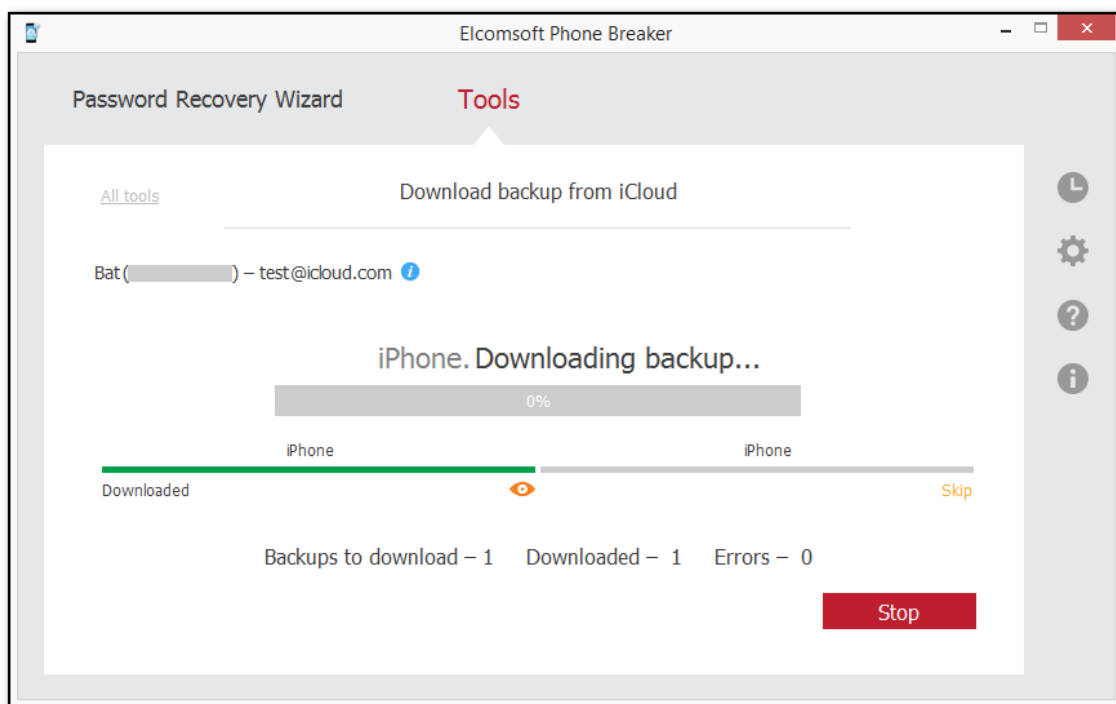
- **Download only specific data/Скачать только выбранные данные:** селективное скачивание данных, позволяющее выбрать категории, которые будут скачаны.

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.

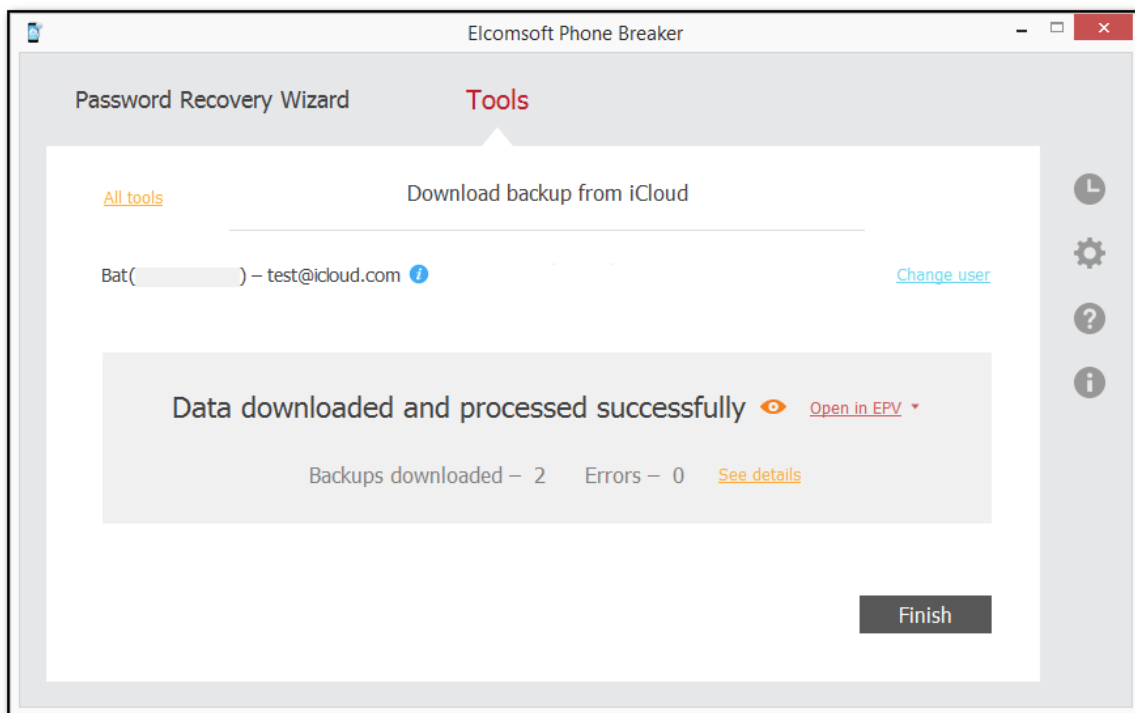
15. Если вы выбрали несколько резервных копий, вы можете нажать Skip/Пропустить, чтобы пропустить загрузку любой из них.



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 Phone Viewer либо запустите Elcomsoft Phone Viewer и откройте скачанные данные.



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

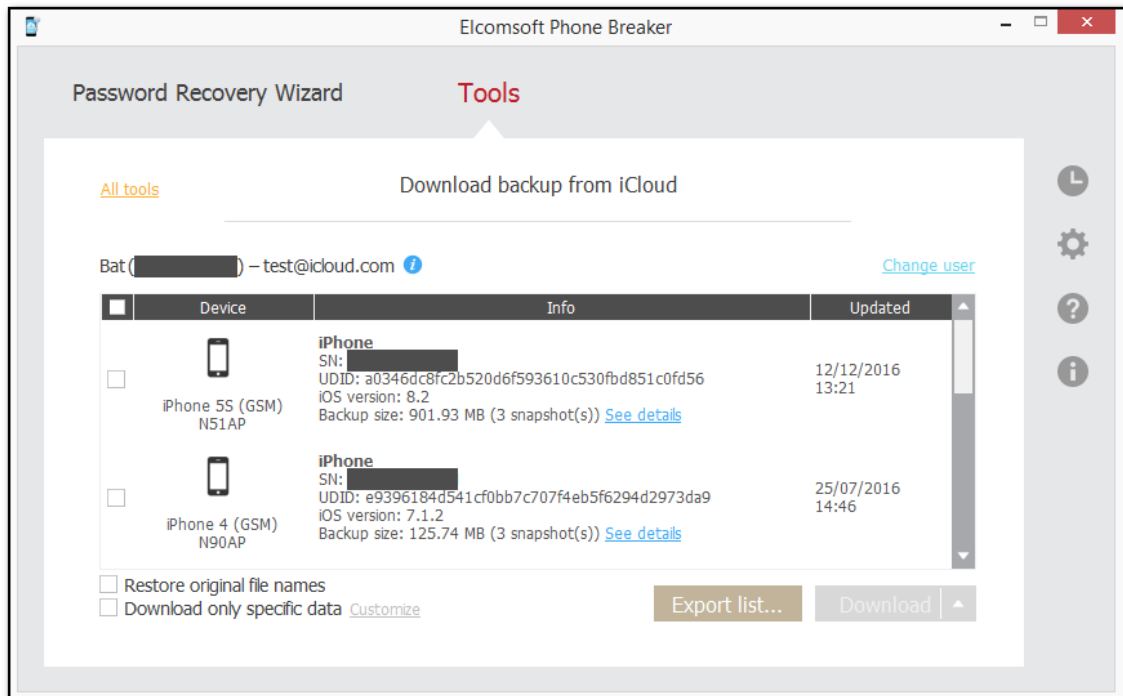
18. Закреть окно можно кнопкой **Finish/Завершить**.

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.

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**.

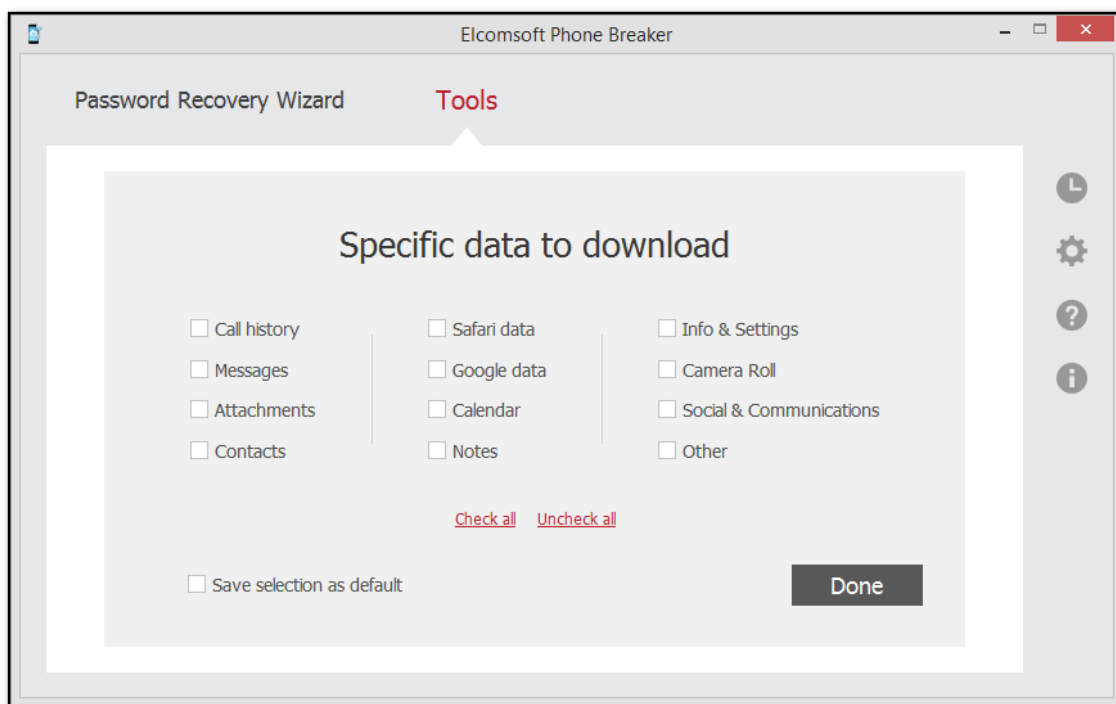
Если не будет выбрано ни одной категории, то будут скачаны только необходимые метаданные, в состав которых входят файлы:

- 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:

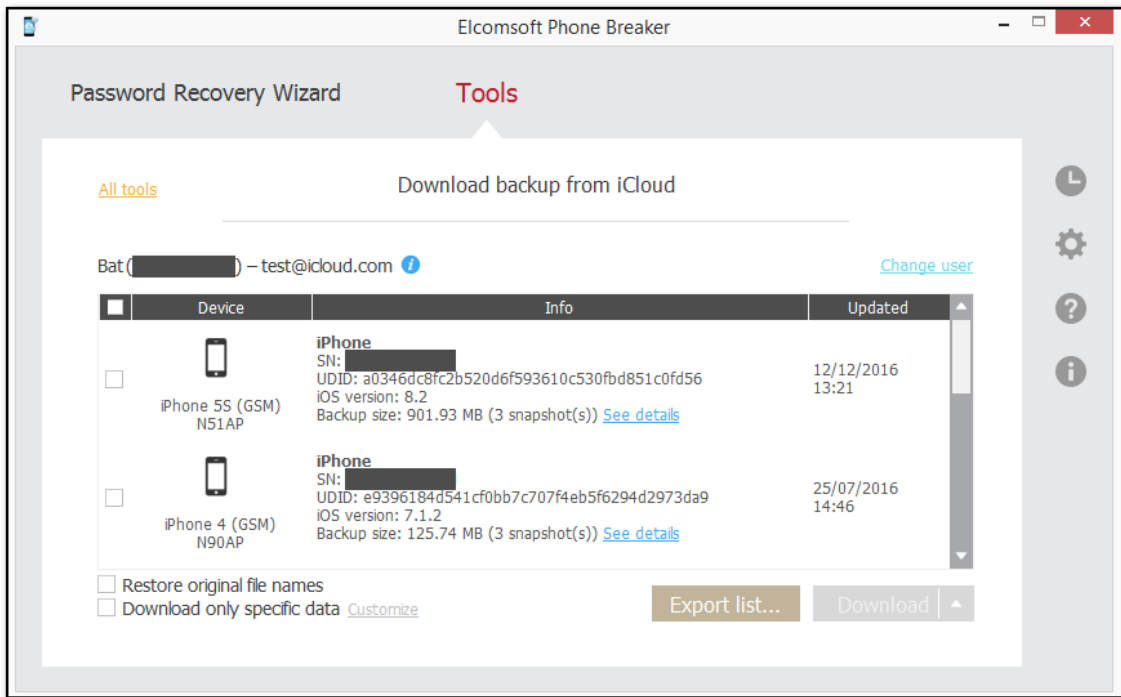
\HomeDomain\Library\Keyboard\
\HomeDomain\Library\Passes\
\HomeDomain\Library\Voicemail\
\HomeDomain\Library\Maps\
\HomeDomain\Library\SpringBoard\
\HomeDomain\Library\Mail\
\HomeDomain\Library\WebKit\Databases\
\HomeDomain\Library\DataAccess\
\RootDomain\Library\Caches\locationd\
\KeyboardDomain\Library\Keyboard

Просмотреть скачанные данные можно в Elcomsoft Phone Viewer.

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.

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. После этого вы сможете работать с данными из iCloud через EPB.

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 невозстановленным именем хранится во вложенной папке, имя которой состоит из первых двух букв имени файла. Например, полный путь к файлу с именем «fd4056e1b33b» будет следующим:

```
<back up_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 объемом 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 24.11.2013, 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 `0ea4ce4cc6e4ce70e34584423b6cfd6f6e87fa`, 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.

Файлы в iCloud

Скачивание файлов из iCloud

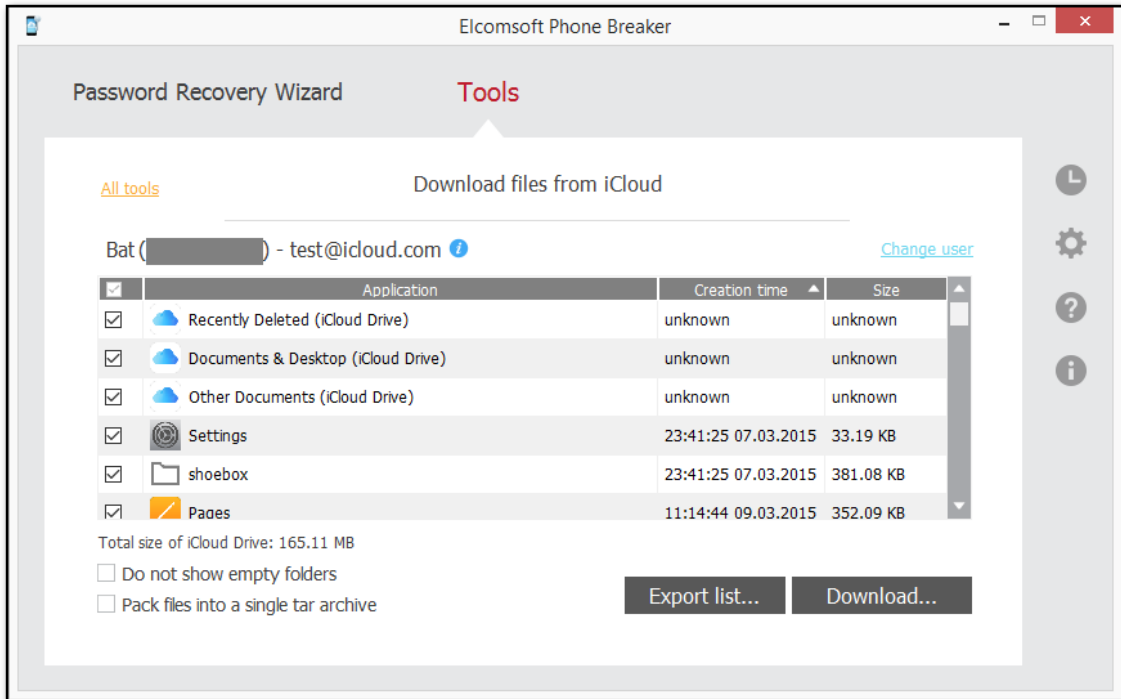
iCloud хранит файлы, используемые различными приложениями устройств iOS, вместе с другими данными, синхронизированными с iCloud. EРВ позволяет скачивать и просматривать эти файлы. Чтобы скачать файлы из iCloud, сделайте следующее:

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](#)^[225]
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 EРВ, 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

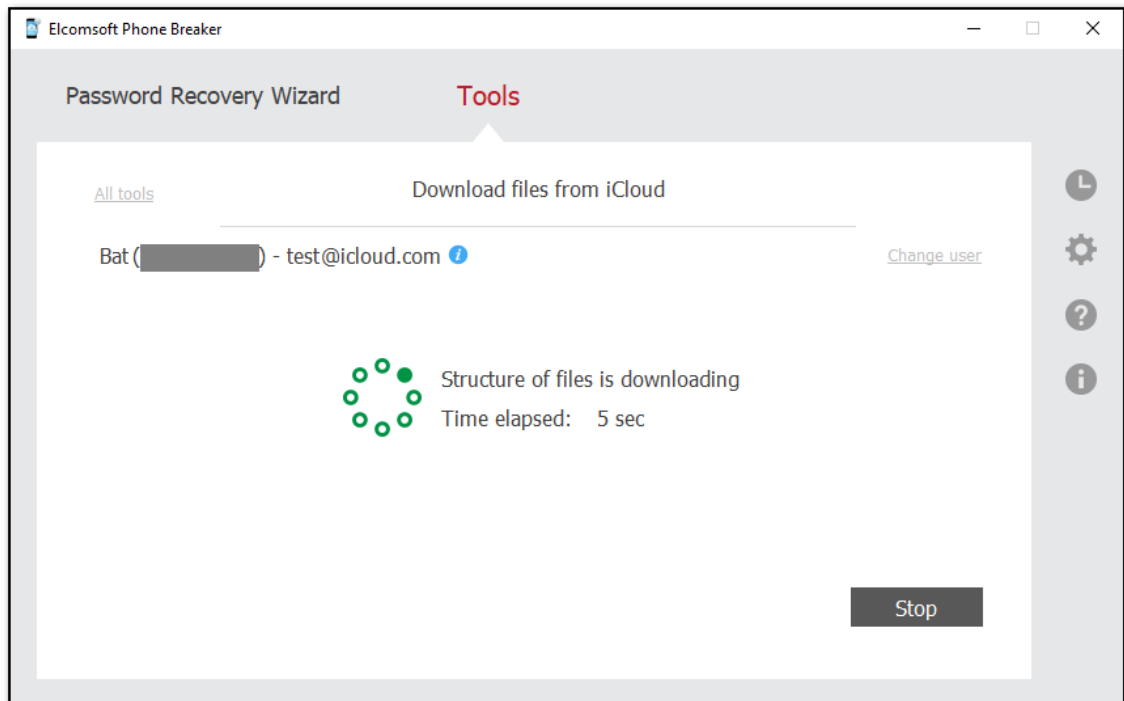
5. Выберите папки и файлы, которые вы хотите загрузить, установив флажки слева. Файлы будут сохранены в оригинальных форматах.

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**.

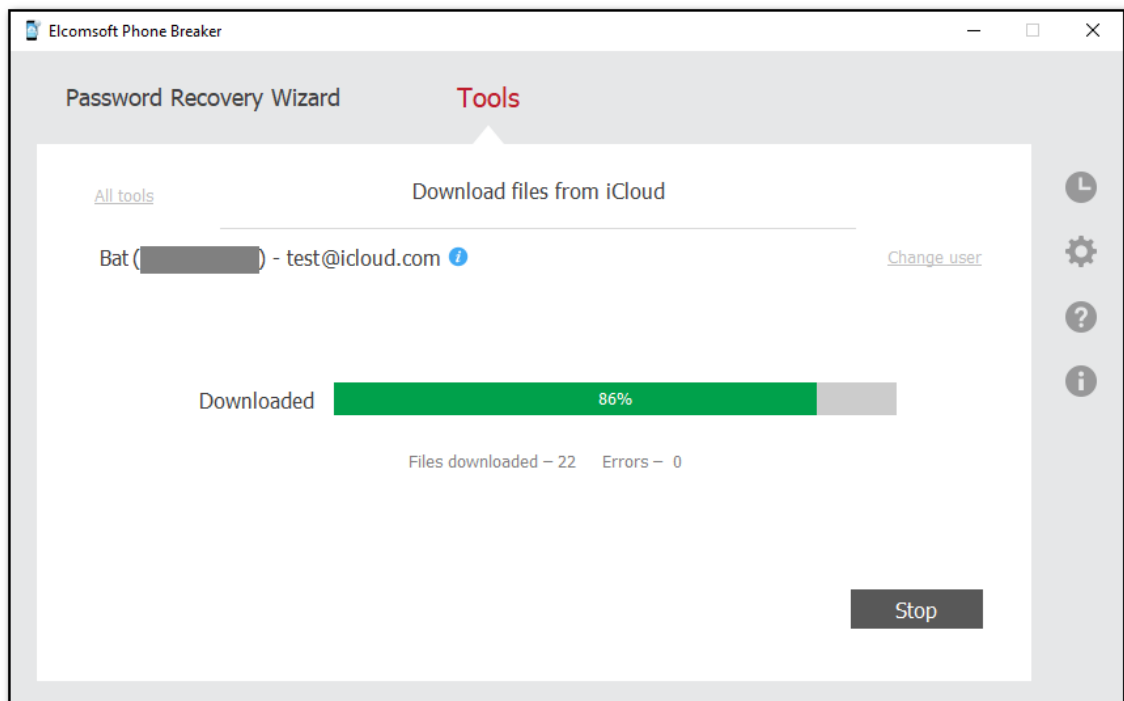
7. Нажмите **Download/Скачать**.

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.



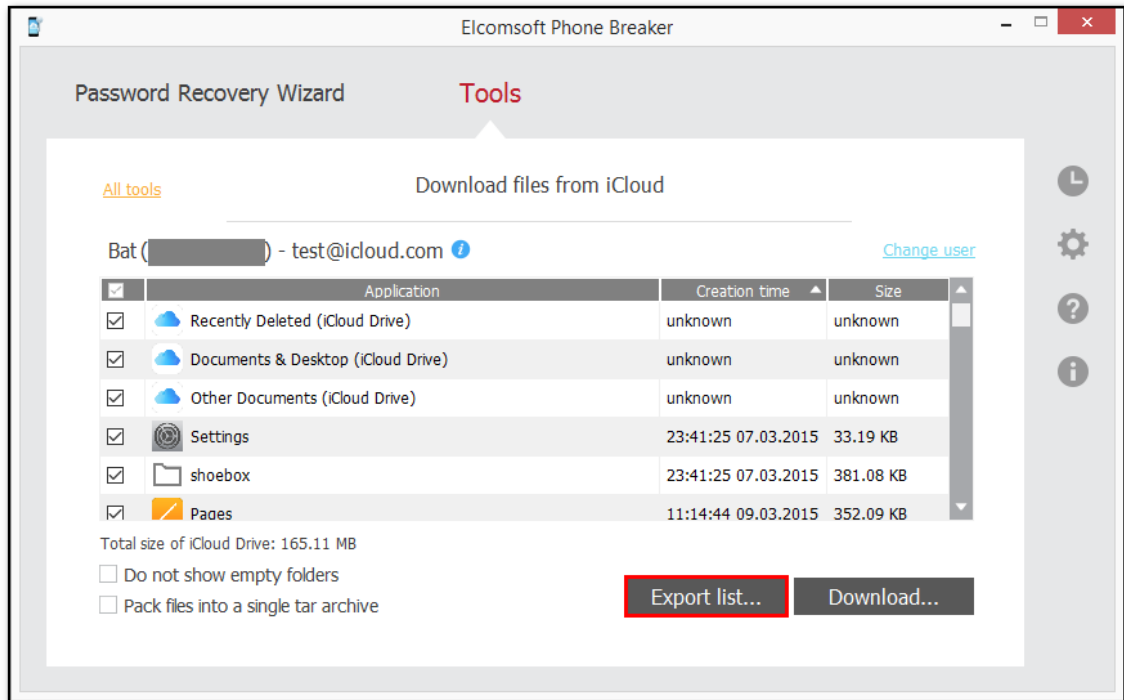
11. Нажмите **Finish/Завершить** для того, чтобы выйти из мастера.

Экспорт списка файлов в iCloud

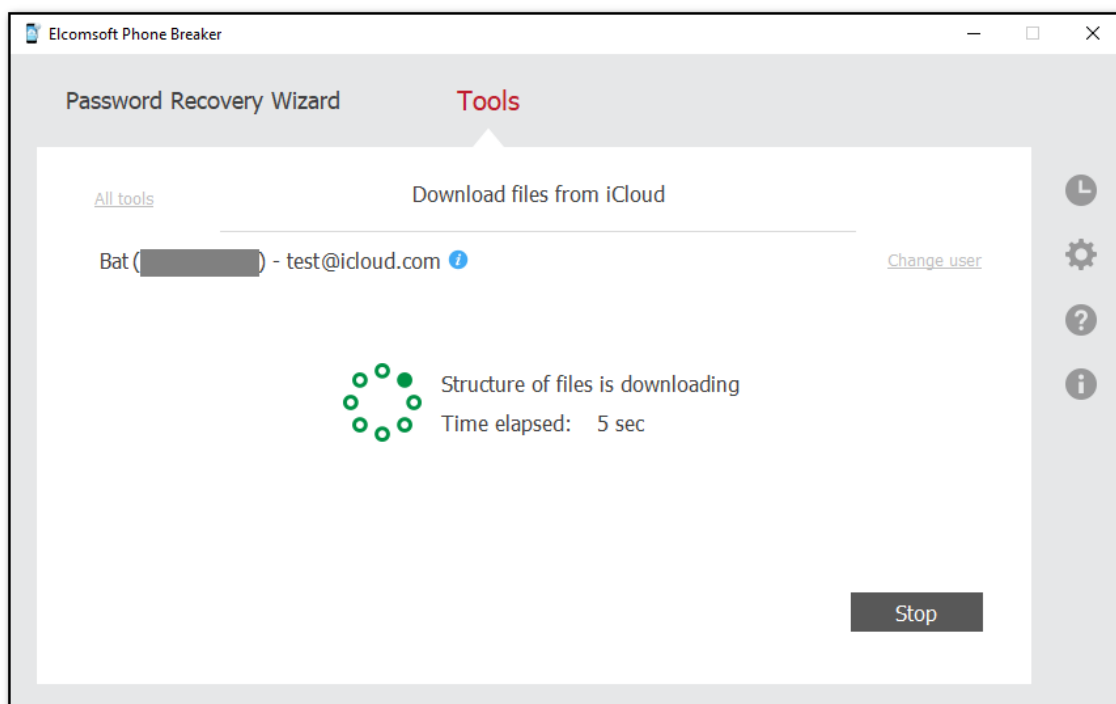
ЕРВ позволяет экспортировать список файлов, которые находятся в учётной записи iCloud пользователя, в формат XML.

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.

Скачивание синхронизированных данных из iCloud

ЕРВ 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>):

Download iCloud for Windows

With iCloud for Windows, you'll have your photos, videos, mail, calendar, files, and other important information on the go and on your Windows PC.



[Download iCloud for Windows from the Microsoft Store](#)

Here's what you need

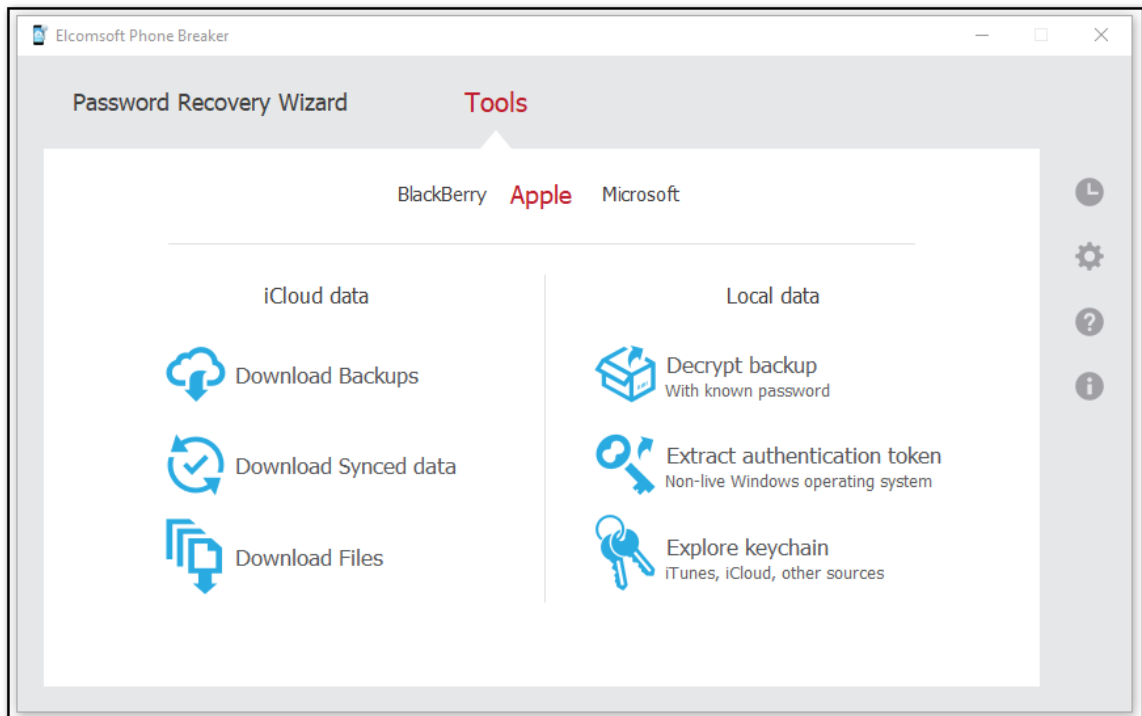
- Make sure that your PC or Microsoft Surface is updated to the latest version of Windows 10.*
- [Have your Apple ID and password ready](#). If you don't have an Apple ID, [you can create one](#).

* On Windows 7 and Windows 8, you can [download iCloud for Windows on Apple's website](#).

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

Для скачивания синхронизированных данных проделайте следующие шаги:

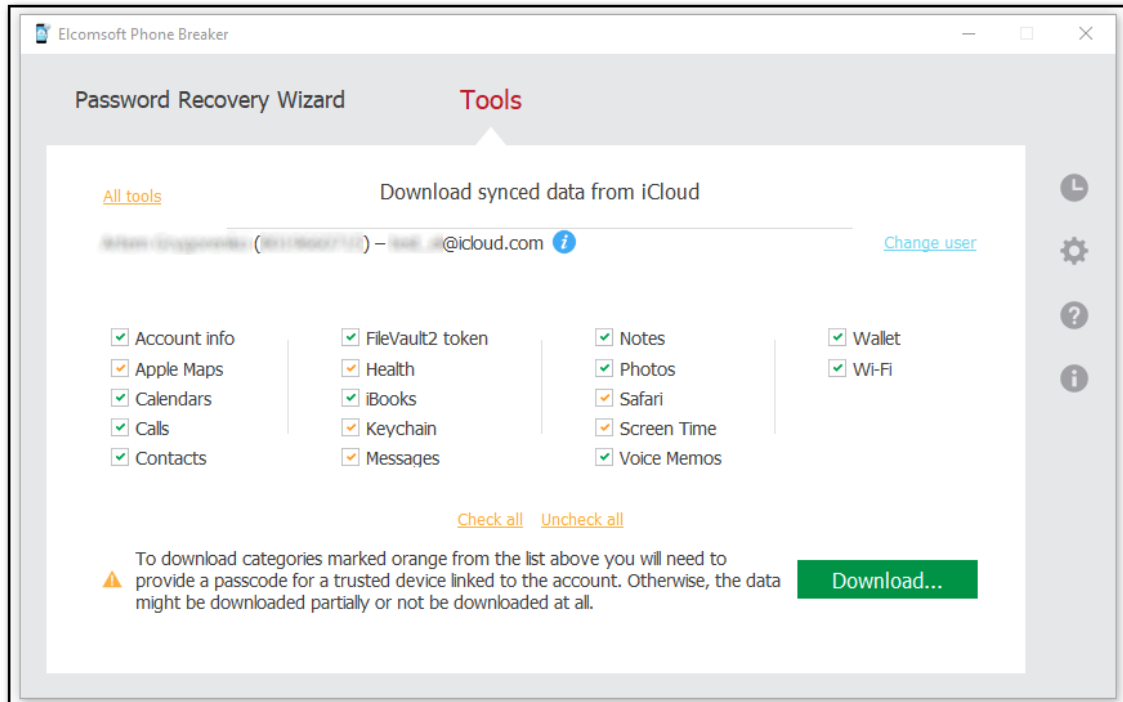
1. В меню **Tools/Инструменты** выберите вкладку **Apple**.
2. Выберите **Download Synced data/Скачать синхронизированные данные**.



3. Пройдите аутентификацию. Подробные инструкции - в разделе [Скачивание резервных копий](#)^[228].

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 EPV 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 учетных 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.

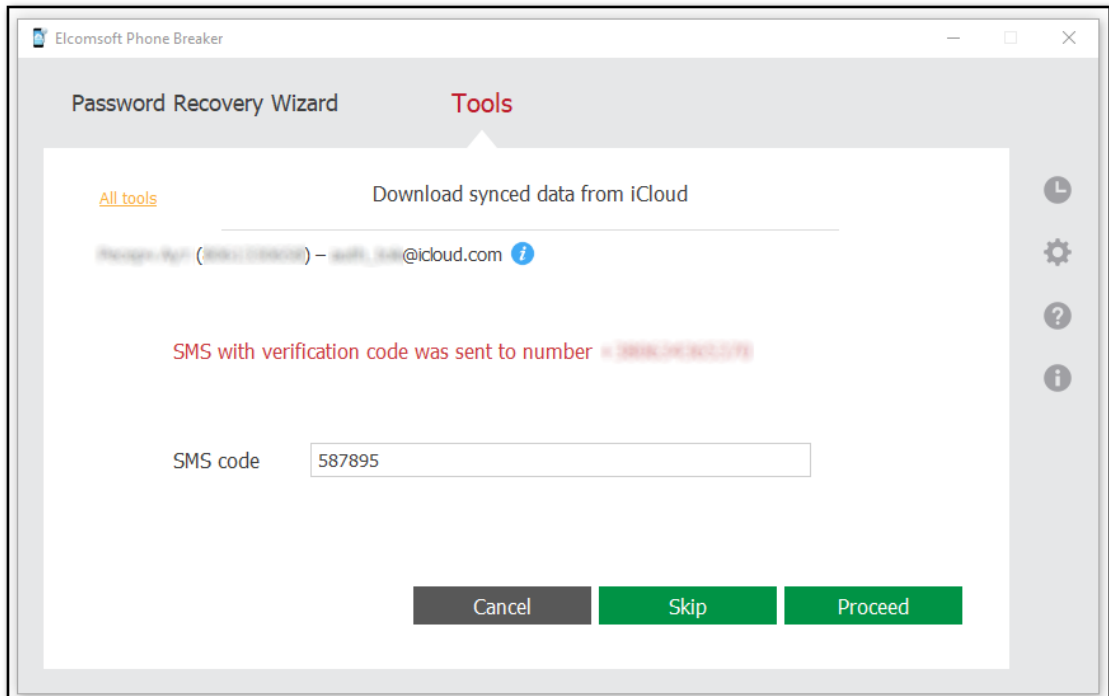
ПРИМЕЧАНИЕ. В современных условиях iCloud Security Code/Код безопасности iCloud не используется.

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.

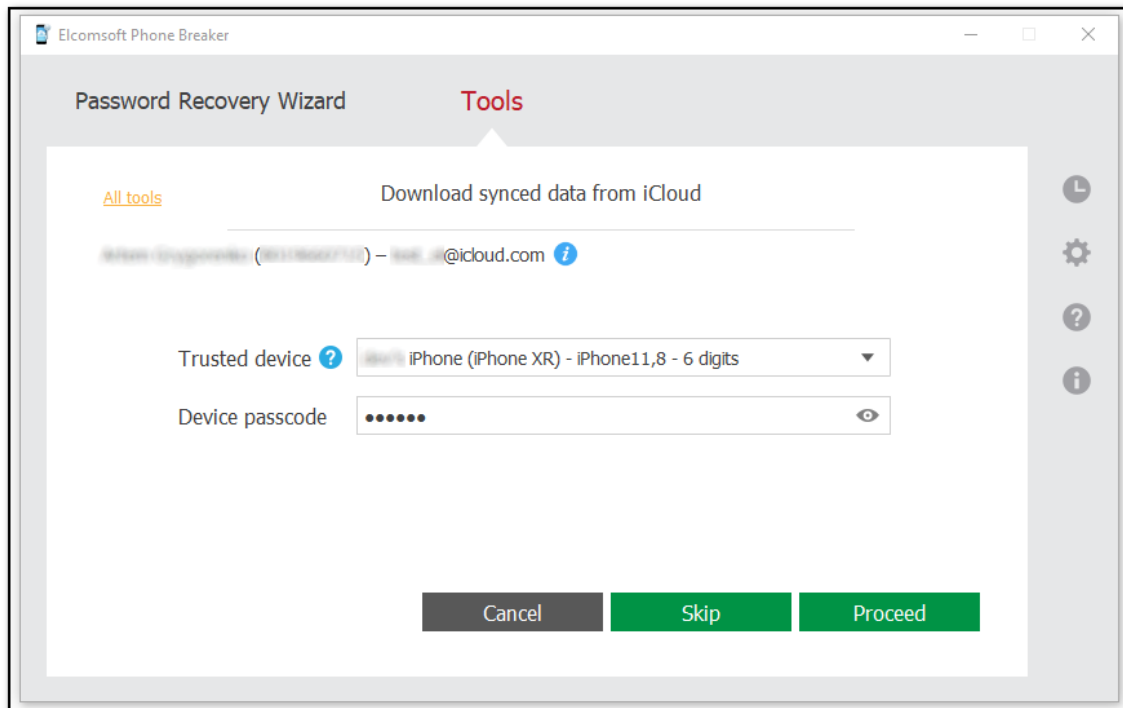
14. (Только для старых версий iOS) Введите полученный в виде SMS код, который был отправлен на предыдущем шаге, и нажмите **Proceed/Продолжить**.



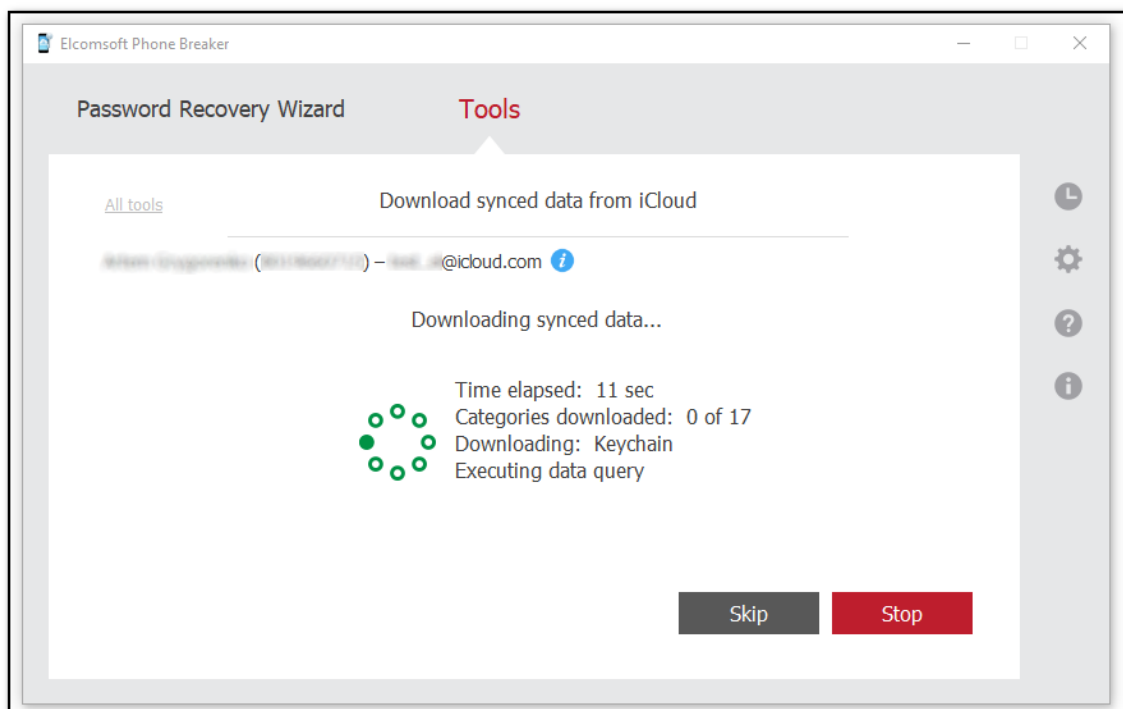
15. Если вы выбрали категории, помеченные оранжевым, для учетной записи с активированной двухфакторной аутентификацией, выберите доверенное устройство и введите пароль (для iOS) или пароль для учетной записи пользователя в операционной системе (для macOS).

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 ЕРВ. Это не повлияет на само устройство, но вы не сможете использовать его для загрузки данных в ЕРВ. 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.



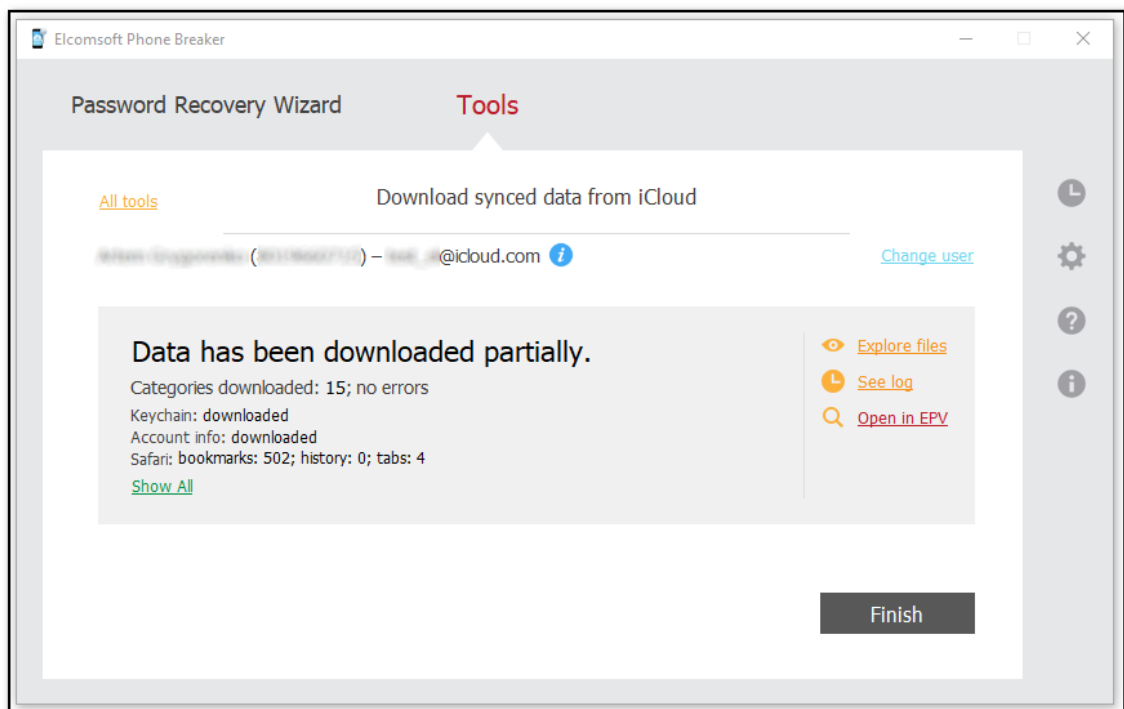
16. Щелкните **Proceed/Продолжить**. Начнется процесс загрузки синхронизированных данных из iCloud. Прогресс отображается в окне программы. Чтобы пропустить загрузку текущей категории, нажмите **Skip/Пропустить**. Чтобы остановить процесс загрузки, нажмите **Stop/Остановить**. (Файлы, загруженные до 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 EPV. Следовательно, количество контактов, отображаемых в EPV, 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](#)^[207]. 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_НН-ММ-СС**) и откройте файл **icloud_keychain.xml** в корне этой папки.

6.2.2.5 Маркеры аутентификации iCloud

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 ^[253] командной строки (atex.exe).
	Диск с системой или образ диска	EPB GUI ^[256]
macOS	Система с активной пользовательской сессией	Утилита ^[259] командной строки (atex.dmg).
	Диск с системой или образ диска	EPB GUI ^[262]

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 двухфакторной аутентификации	Маркер аутентификации для учётной записи 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 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 учётной 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.

Извлечение маркера аутентификации: Windows**Извлечение маркера аутентификации: Windows, система с активной пользовательской сессией**

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](#)^[256] (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)

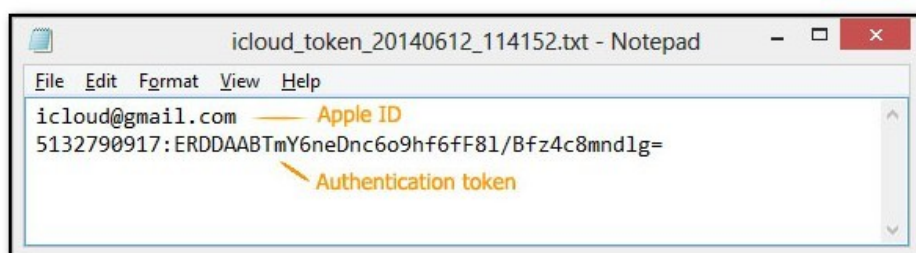
ПРИМЕЧАНИЕ. Когда вы запускаете atex.exe из системной папки или из папки, для изменения которой у вас недостаточно прав, может появиться сообщение Windows User Account Control с запросом разрешения на запуск этой программы.

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.

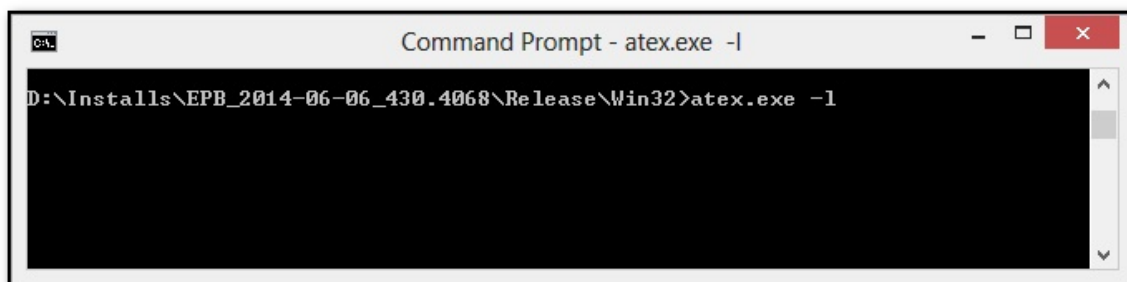
В открывшемся консольном окне вы увидите полный путь к файлу. Обратите внимание, что символы Unicode в пути к файлу не поддерживаются.

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.

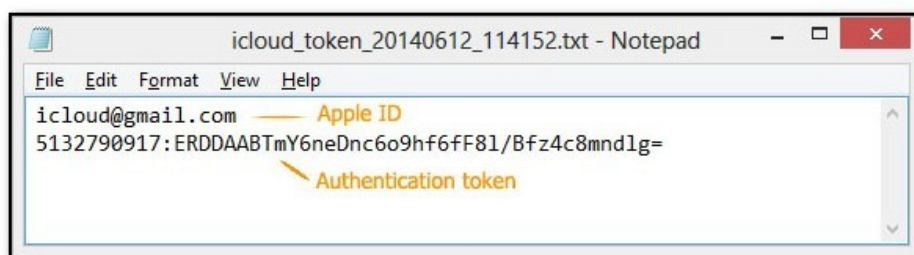


5. Запустите atex.exe с параметром getToken и введите логин локального **пользователя Windows** и пароль для этой учетной записи в следующей форме: **atex.exe --getToken -n <username> -p <password>**

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

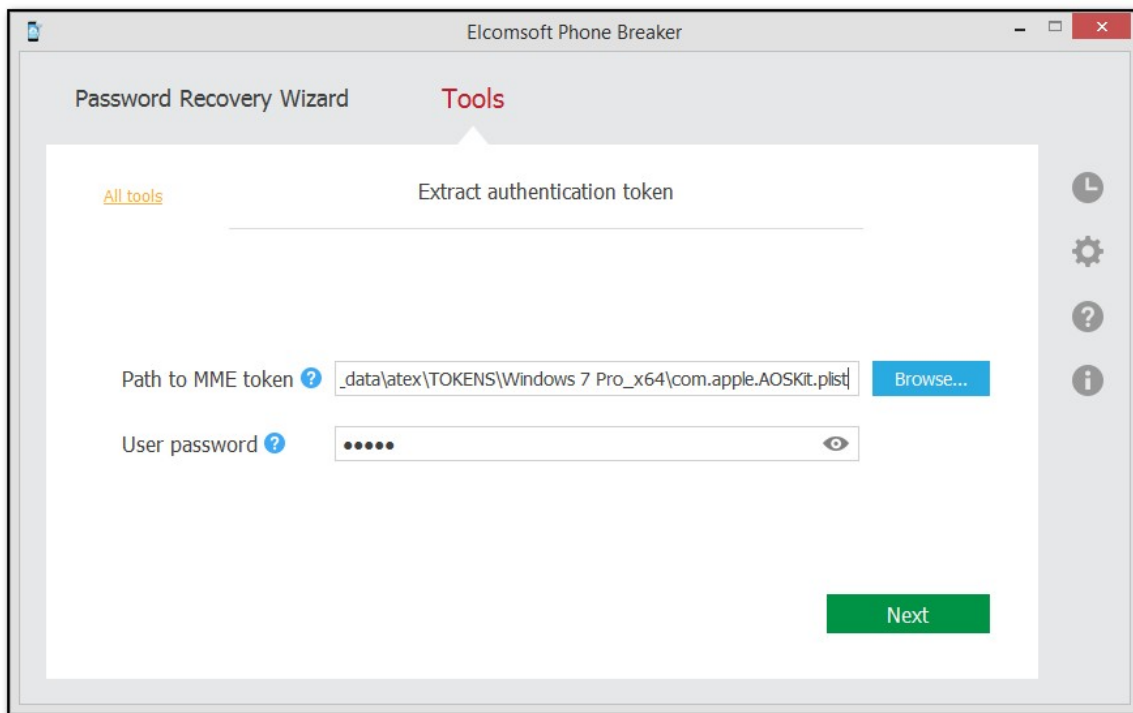
--getToken -n <username> -p <password>	Извлекает маркер аутентификации для указанного пользователя. Имя пользователя и пароль следует вводить без скобок.
-n или [--username]	Имя пользователя. Имя пользователя следует вводить без скобок.
-p или [--password]	Пароль пользователя. Пароль следует вводить без скобок.

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 токenu:** 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.



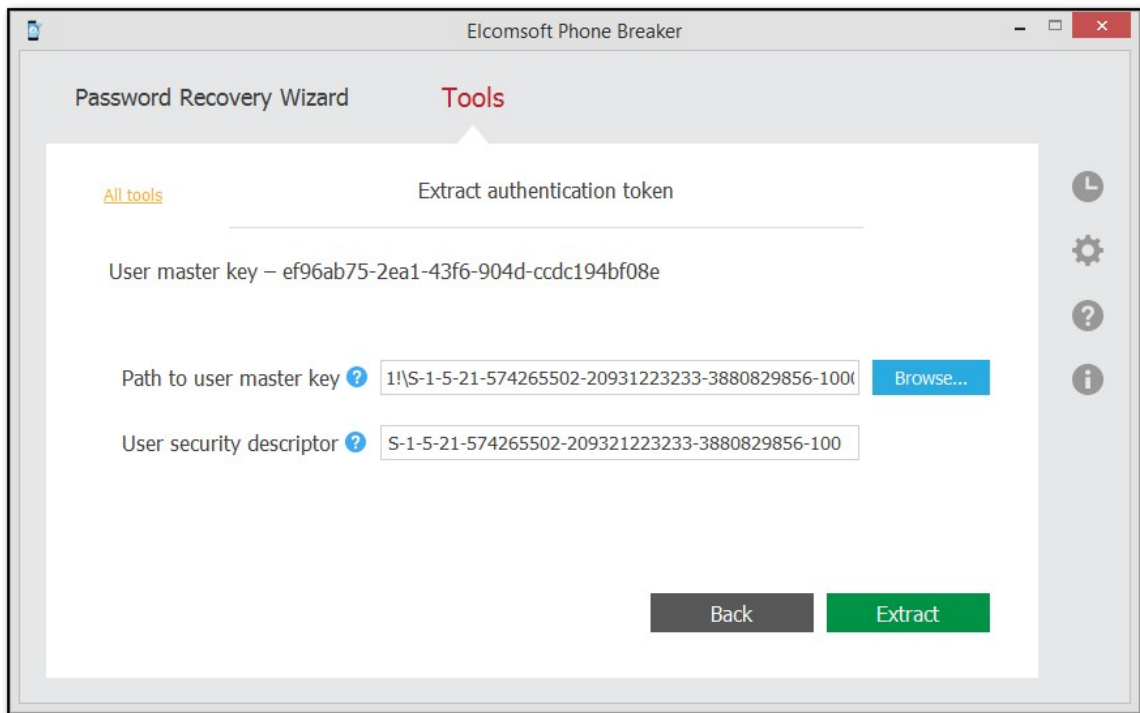
6. Нажмите **Next/Далее**.

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.

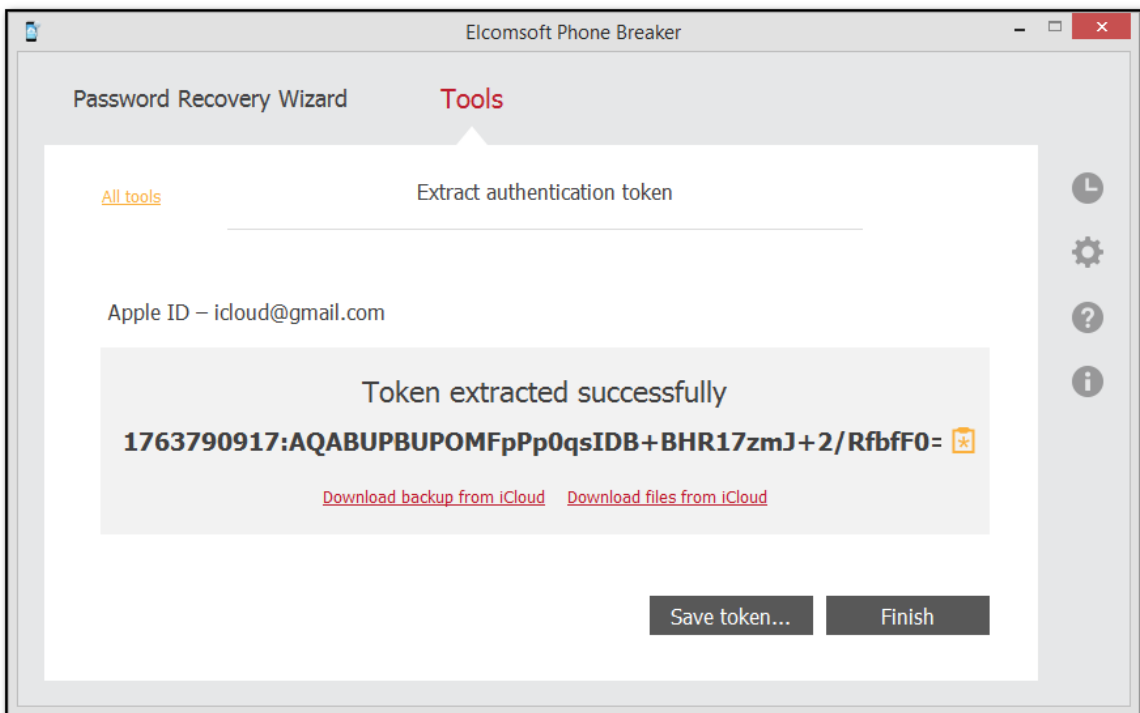
- **Path to user master key/Путь к мастер-ключу пользователя:** Укажите путь на диске к мастер-ключу. По умолчанию мастер-ключ хранится в папке %APPDATA%\Roaming\Microsoft\Protect\\.

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.

Извлечение маркера аутентификации: macOS

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](#) ²⁶²

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: <ul style="list-style-type: none"> ▪ Маркер нельзя использовать для загрузки резервных копий iCloud..

	<ul style="list-style-type: none"> ▪ 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:IAAAAAABLWIAAAAFvqx/ORDmdzLmljbG91ZC5hdXp
auth_token_with_limitations	String	11179869442:EAAEAAAABLWIAAAAFvhjEoRDmdzLmljbG91ZC5hdXp
ctoken	String	MDAwNDk3LTA4LWFkNGlOYWwLTUwYzltNDQ2ZC1iOWFiLTJkYTYz
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	<ul style="list-style-type: none"> ▪ Apple ID (apple_id) ▪ Маркер аутентификации (auth_token) ▪ Continuation token (ctoken) ▪ Пароль к Apple ID - иногда
macOS 10.3 и выше	<ul style="list-style-type: none"> ▪ Apple ID (apple_id) ▪ Маркер аутентификации (auth_token) ▪ Маркер аутентификации с ограничениями (auth_token_with_limitations) ▪ Continuation token (ctoken) ▪ 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	<ul style="list-style-type: none"> ▪ Apple ID (<code>apple_id</code>) ▪ Маркер аутентификации (<code>auth_token</code>) ▪ Continuation token (<code>ctoken</code>) ▪ Пароль к Apple ID - иногда
macOS 10.3 и выше	<ul style="list-style-type: none"> ▪ Apple ID (<code>apple_id</code>) ▪ Маркер аутентификации (<code>auth_token</code>) ▪ Маркер аутентификации с ограничениями (<code>auth_token_with_limitations</code>) ▪ Continuation token (<code>ctoken</code>) ▪ Password to Apple ID - иногда

Параметры командной строки утилиты `atex`:

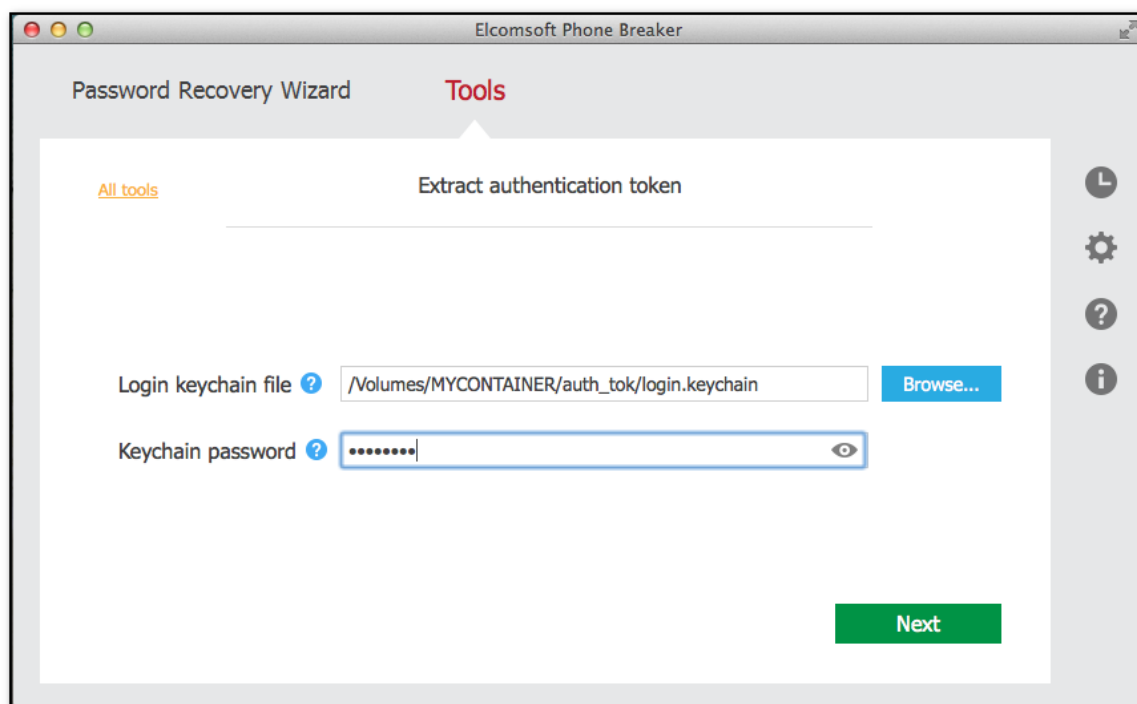
Параметр	Значение
<code>-h</code> или <code>[-help]</code>	Отображает справочное сообщение
<code>-l</code> или <code>[-iCloudUserList]</code>	Отображает список пользователей iCloud
<code>--getToken -u <username> -p <password></code>	Извлекает маркер аутентификации для указанного пользователя. Имя пользователя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

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.

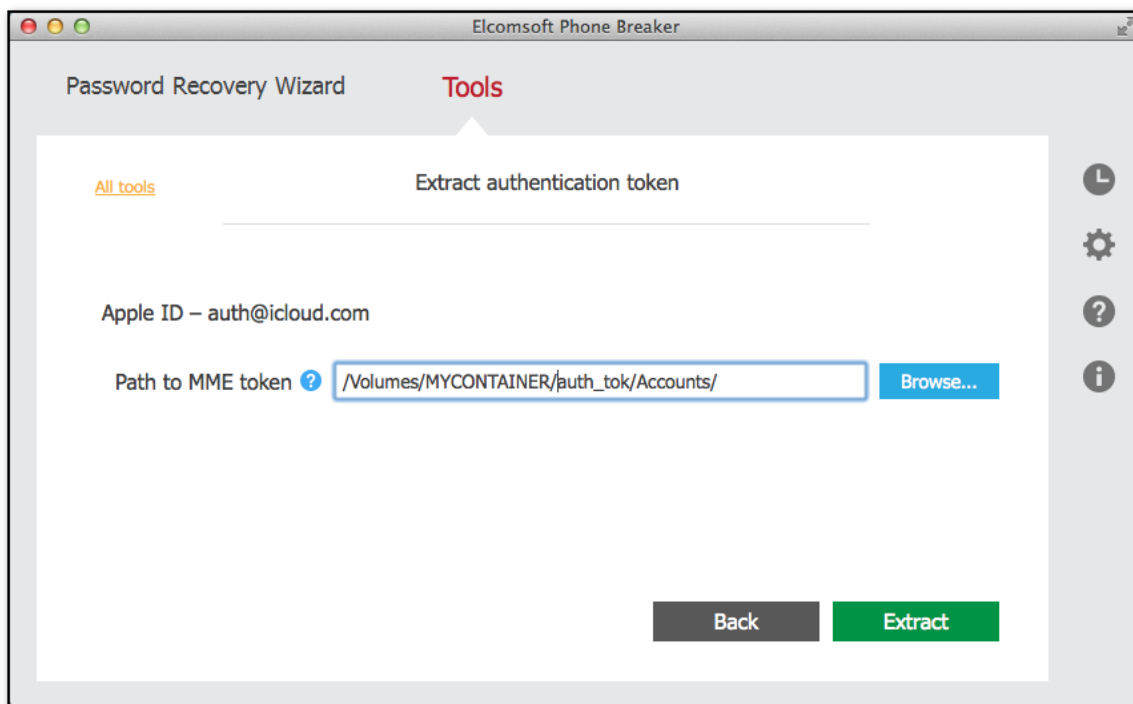


6. Нажмите **Next/Далее**.

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.

6.2.3 Работа с данными из Microsoft Account

6.2.3.1 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-skype>

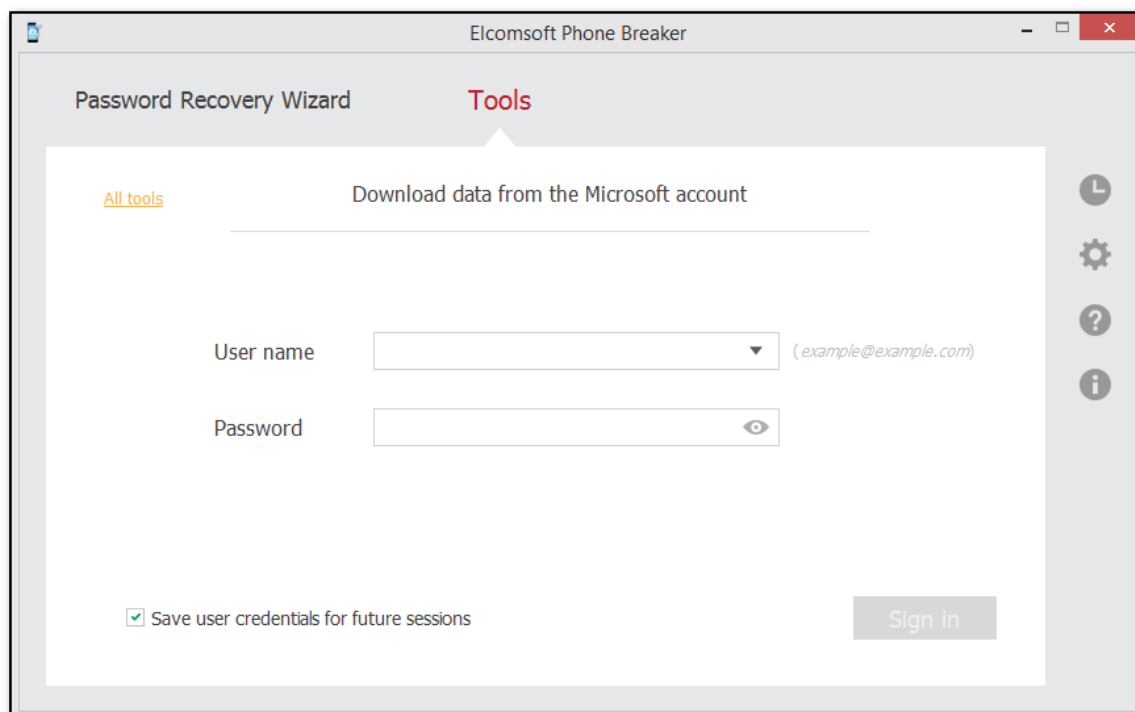
Загруженные данные сохраняются в архиве, содержащем базы данных с загруженной информацией и файл Manifest.xml, в котором содержится информация о каждом устройстве, связанном с учетной записью, и имя файла для каждого файла базы данных.

6.2.3.2 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.

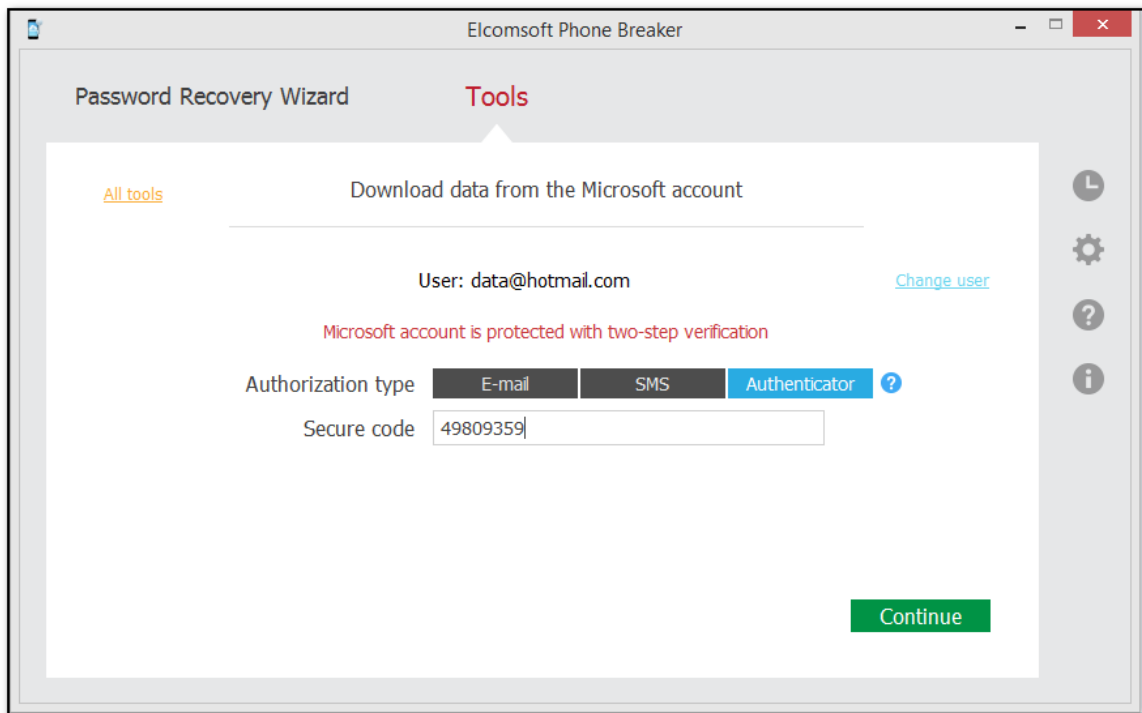
Нажмите **View/Показать**  , чтобы снять маскировку символами (*) с пароля.



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

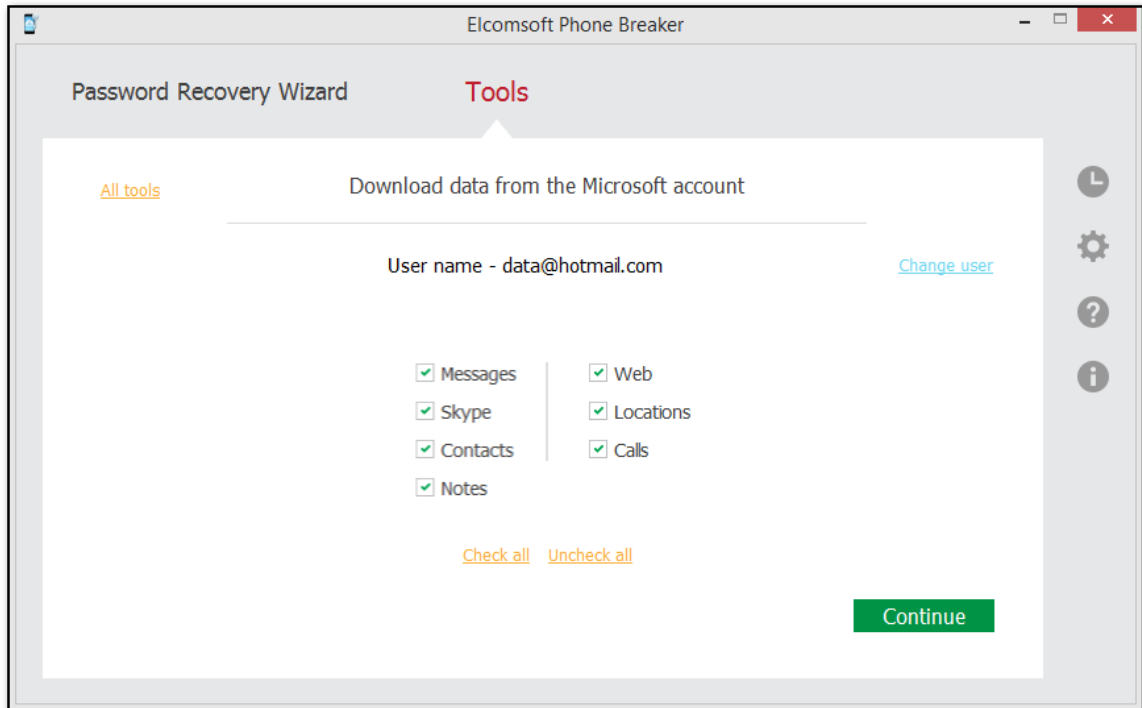
- E-mail
- SMS
- Authenticator: EPB поддерживает 8-значные коды, созданные в стандартном приложении-аутентификаторе Microsoft, и 6-значные коды, созданные в сторонних приложениях.

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

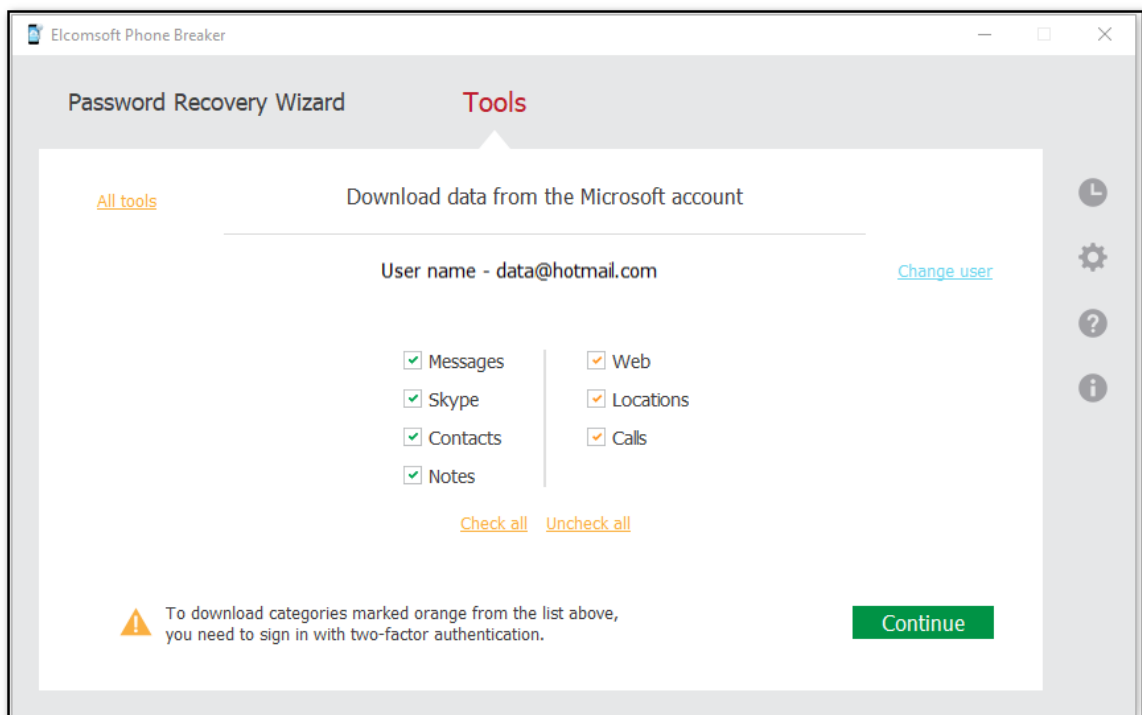


4. Отметьте категории для скачивания и нажмите **Continue/Продолжить**.

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:

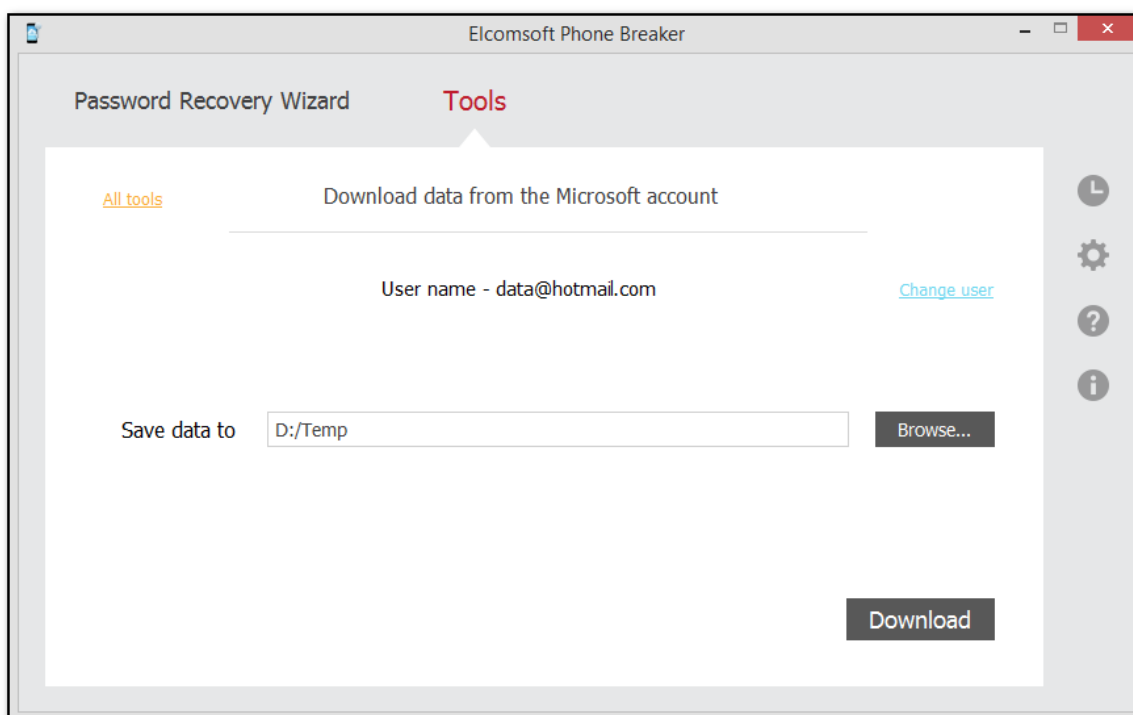
- Доверенный адрес электронной почты
- SMS

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.

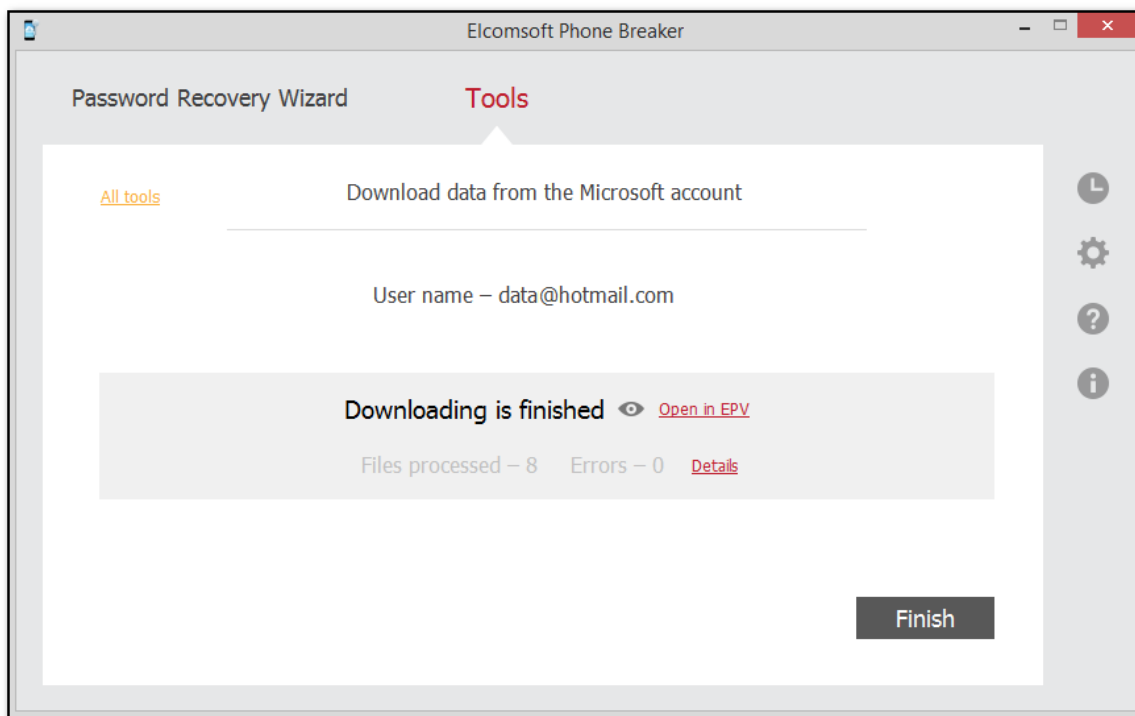


6. Начнется загрузка данных. Вы можете просмотреть количество обработанных файлов и количество ошибок, полученных во время загрузки.

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.

6.2.4 [Windows] Восстановление паролей

6.2.4.1 Восстановление паролей

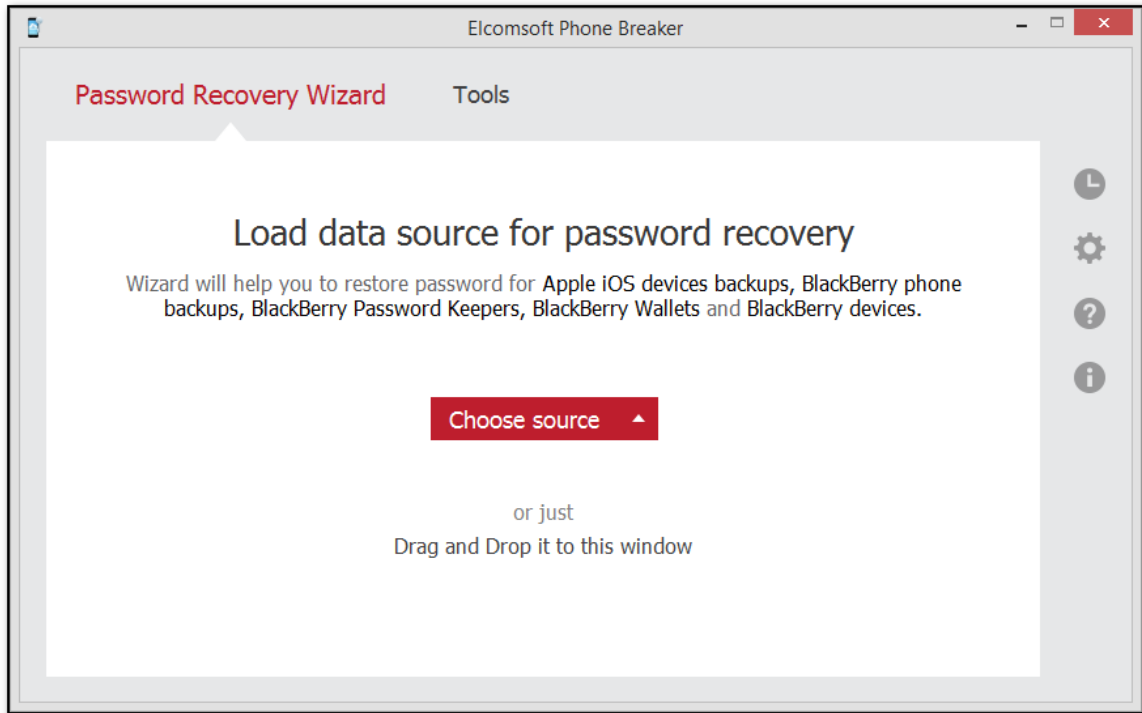
В редакции для Windows доступен функционал восстановления паролей к [резервным копиям iTunes](#) ^[215]

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

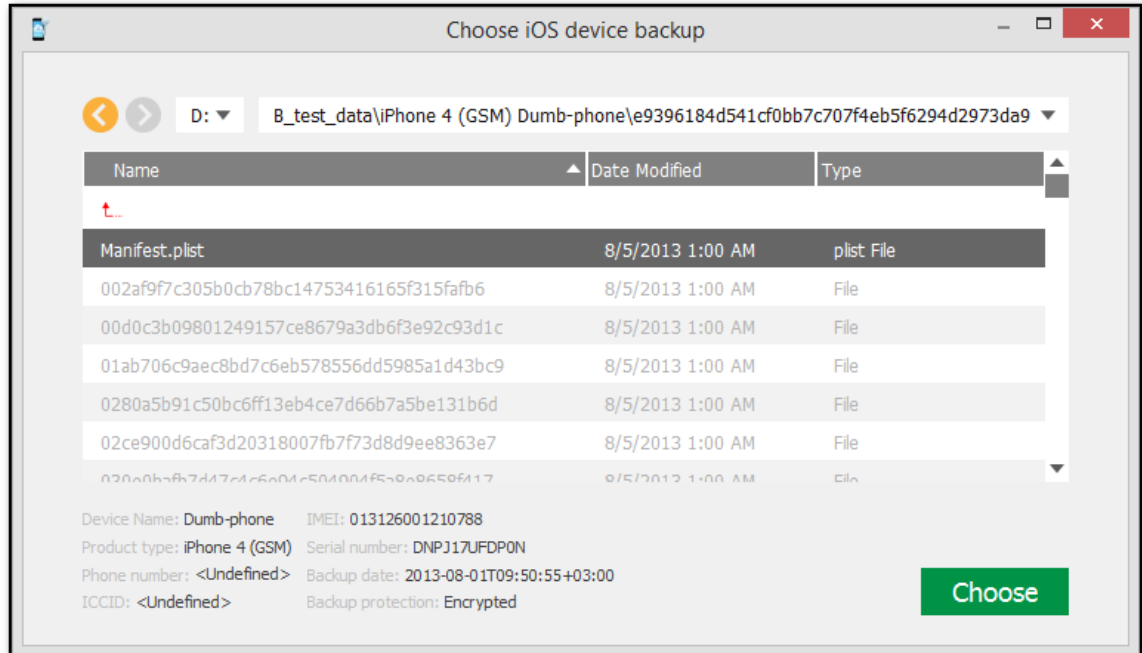
EPB позволяет восстановить пароль методом перебора. Комбинация атак составляет конвейер восстановления.

Для настройки атаки проделайте следующие шаги:

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



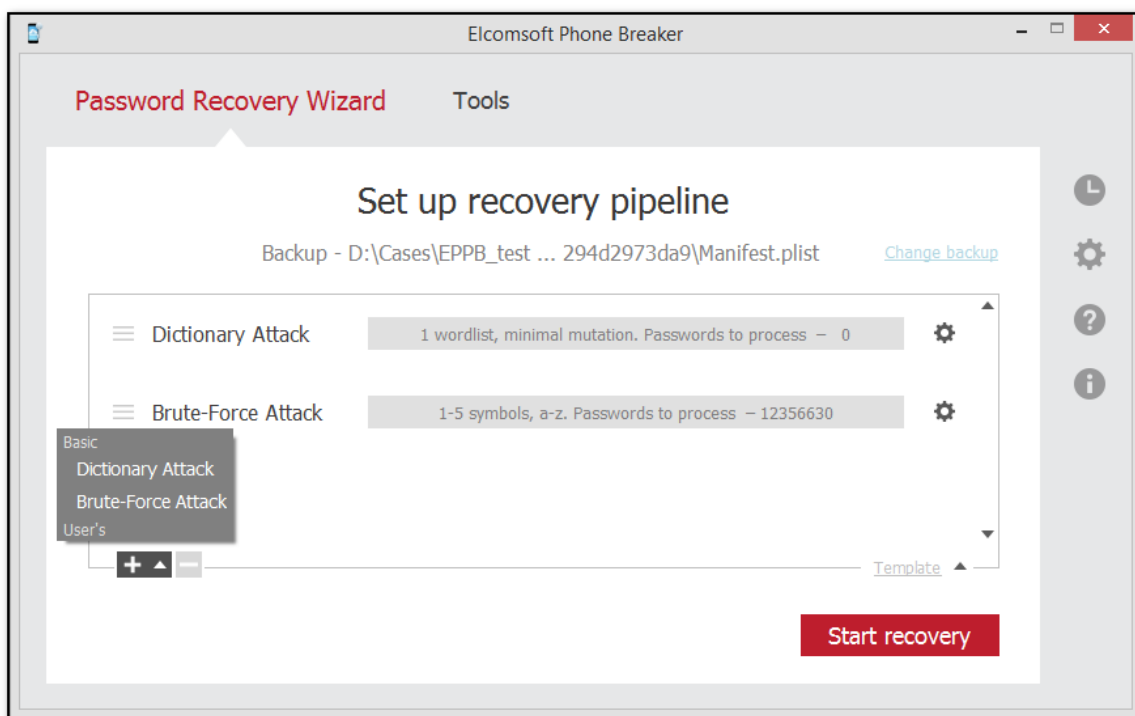
3. Чтобы добавить файл резервной копии или контейнер, перетащите его в окно мастера восстановления пароля или нажмите **Choose source/Выбрать файл** и выберите резервную копию вручную.



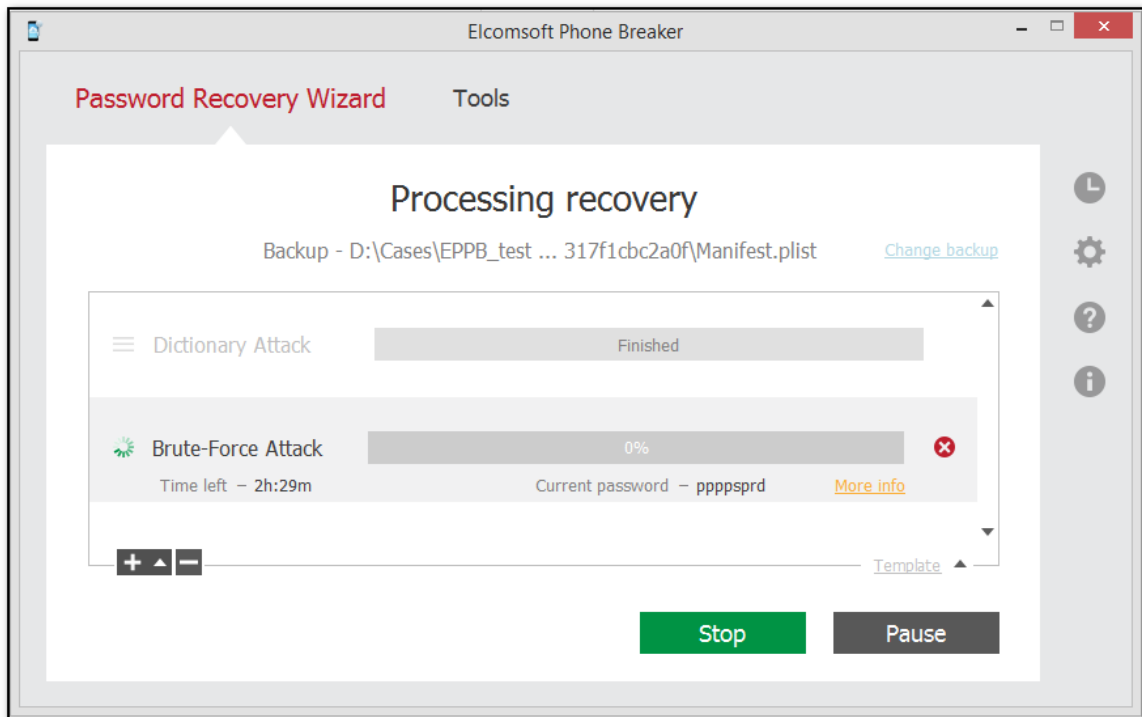
4. Когда файл будет добавлен, определите атаки, которые будут использоваться для взлома пароля.

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](#)^[272].

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



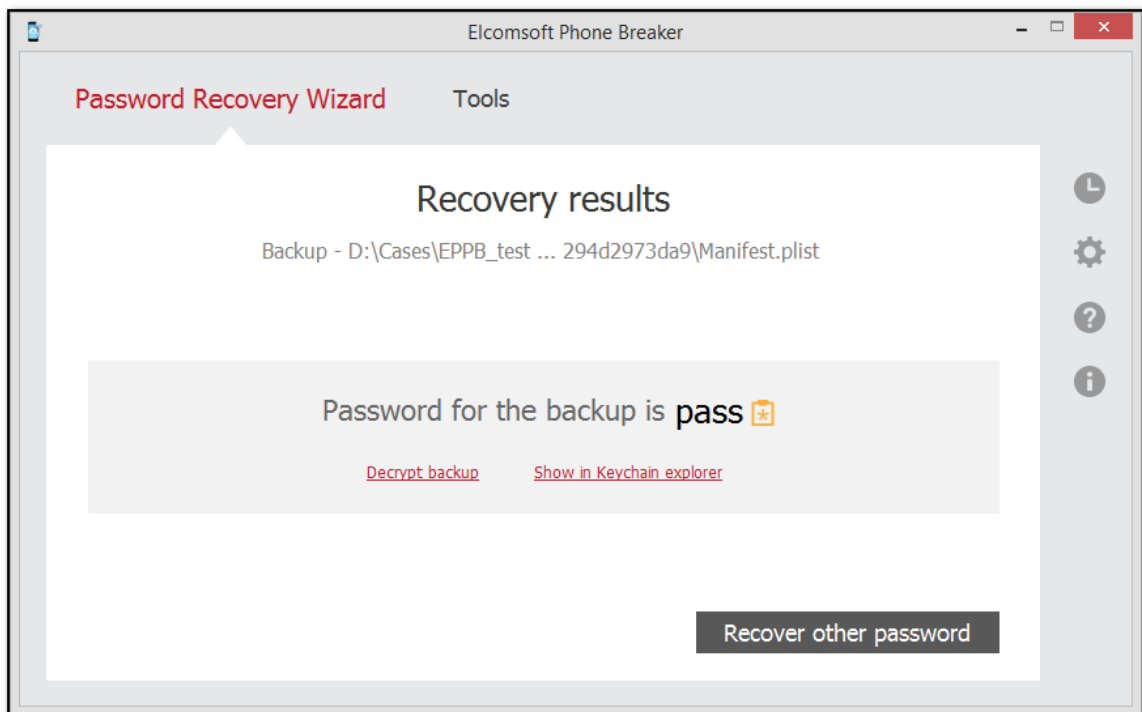
5. Нажмите **Start recovery/Начать восстановление**.
6. Начнется восстановление пароля. Вы можете просмотреть примерное оставшееся время и вариант пароля, который обрабатывается в данный момент.



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**.

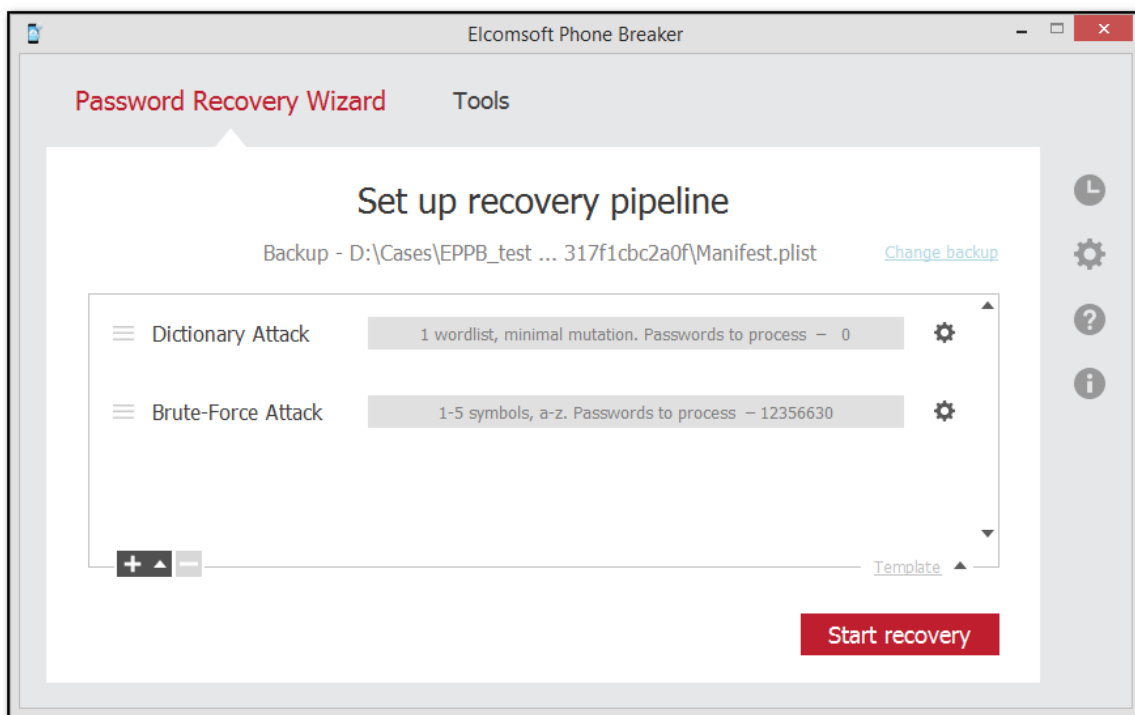
6.2.4.2 Настройка атаки


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](#)²⁸³, чтобы сохранить настройки атаки или загрузить уже существующие.

6.2.4.3 Сохранение сеансов атак

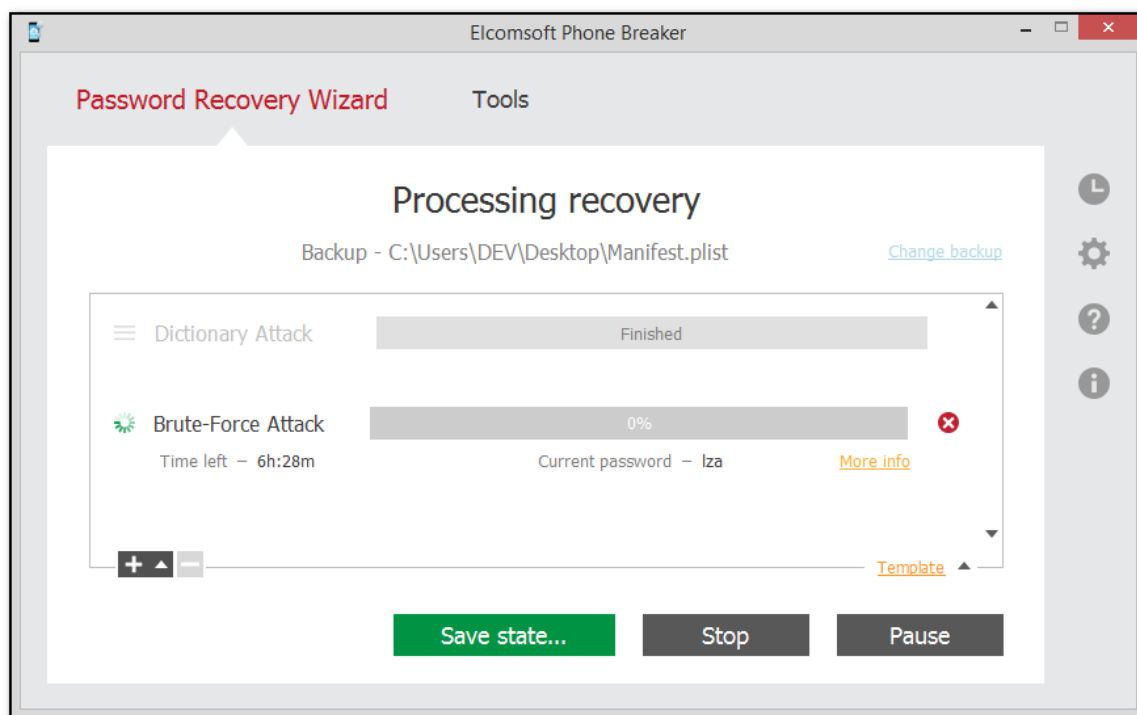
Вы можете сохранять и восстанавливать конвейер и промежуточное состояние сеансов атаки. Сохранение может выполняться вручную или автоматически.

Сохранение и возобновление сеансов атаки вручную

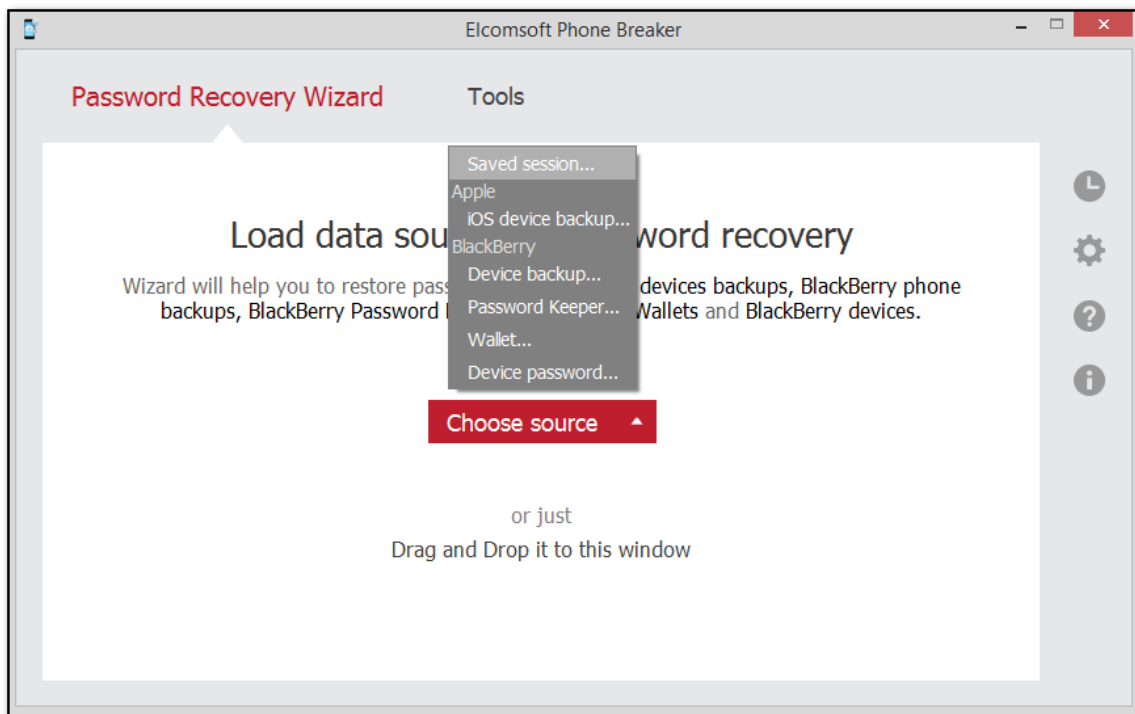
Чтобы сохранить состояние сеанса атаки восстановления пароля вручную, выполните одно из следующих действий:

- 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](#) ¹⁹⁹:

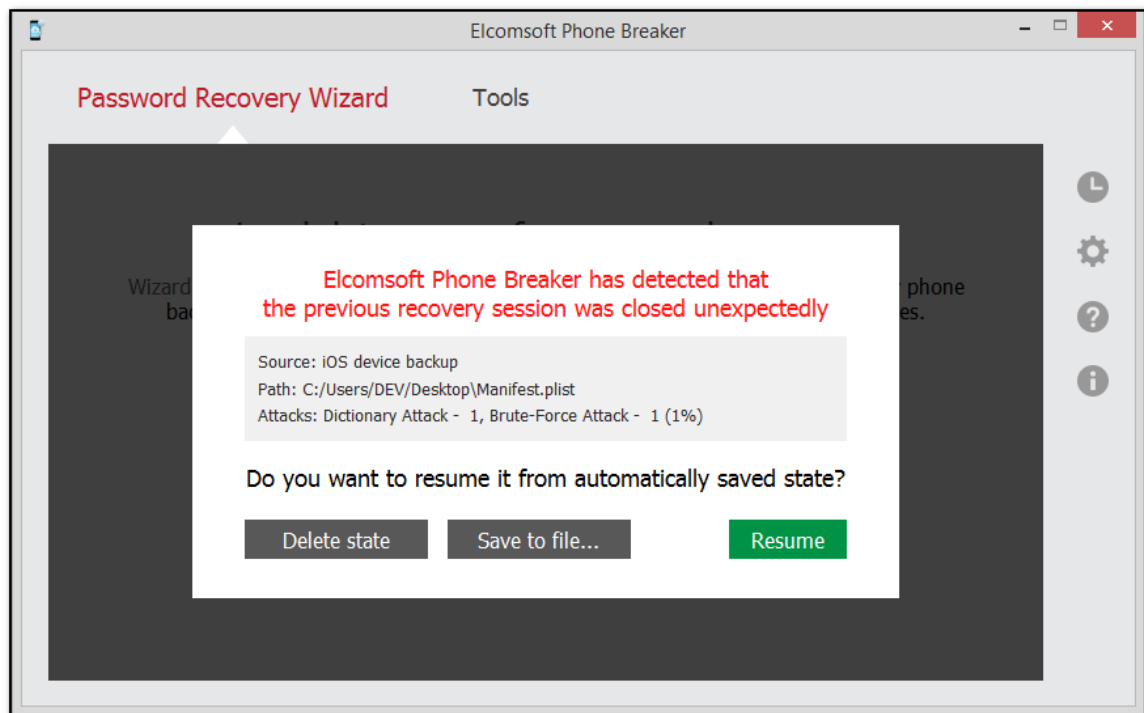
- убедитесь, что опция **Automatically save password recovery session every <> minutes/Автоматически сохранять данные о текущей сессии атаки на пароль каждые <> минут** отмечена (она отмечена по умолчанию).
- установите желаемую частоту автосохранения в интервале от 1 до 180 минут (по умолчанию - каждые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

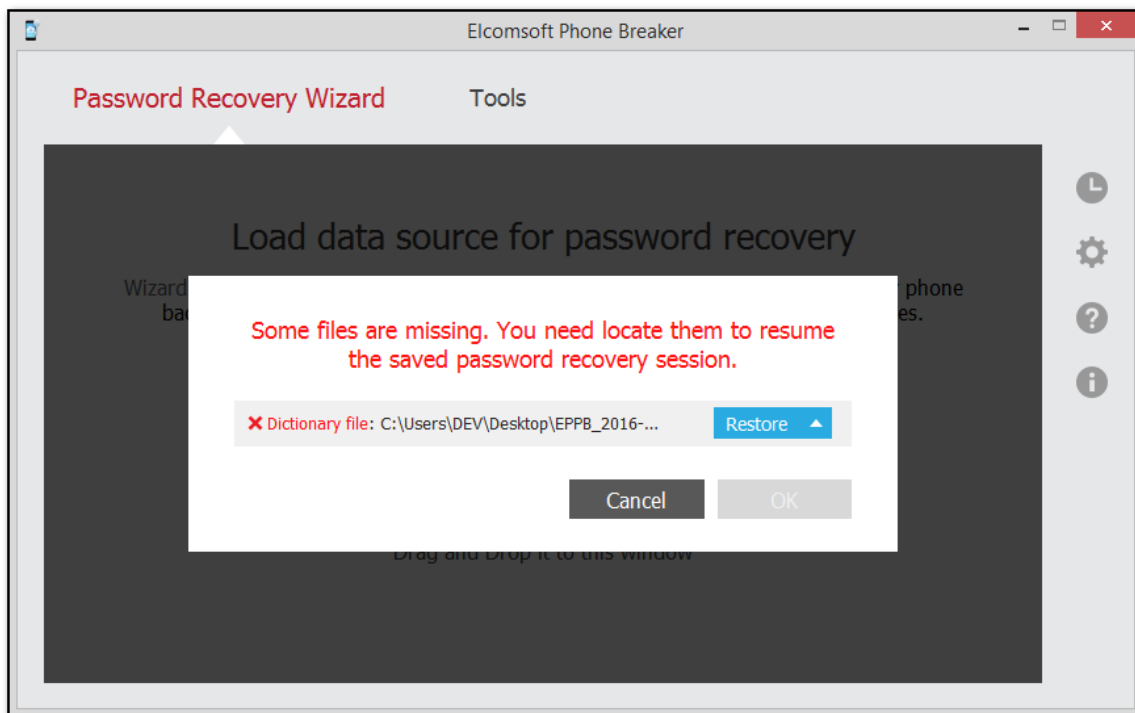


Resume/Возобновить восстанавливает сеанс атаки на момент последнего сохранения.
Save to file/Сохранить в файл сохраняет сеанс в указанный файл.
Delete state/Удалить сеанс удаляет сохранённый сеанс.

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.

6.2.4.4 Настройка атаки по словарю

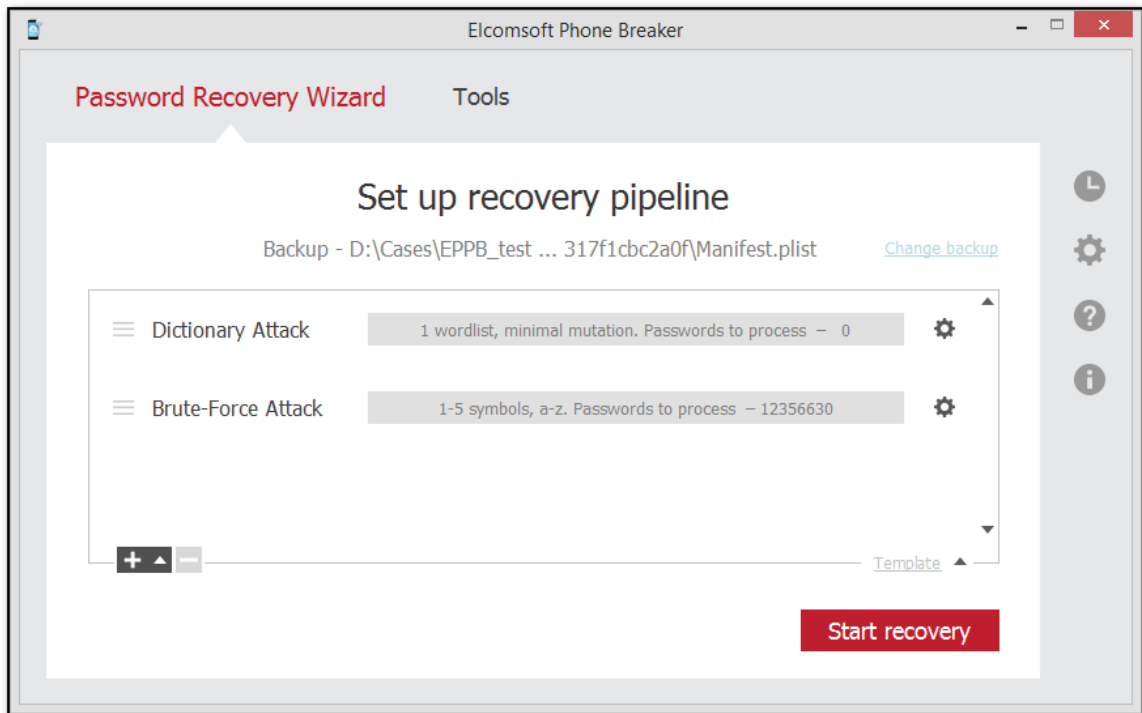
Атаки по словарю позволяют подставлять в качестве вариантов паролей как слова из текстового файла, так и их часто употребляемые вариации ("мутации" в терминах EPB). Мутации позволяют подставлять варианты словарных слов, отличающиеся регистром букв, добавлением цифр или дат, перестановками букв и т.д.

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

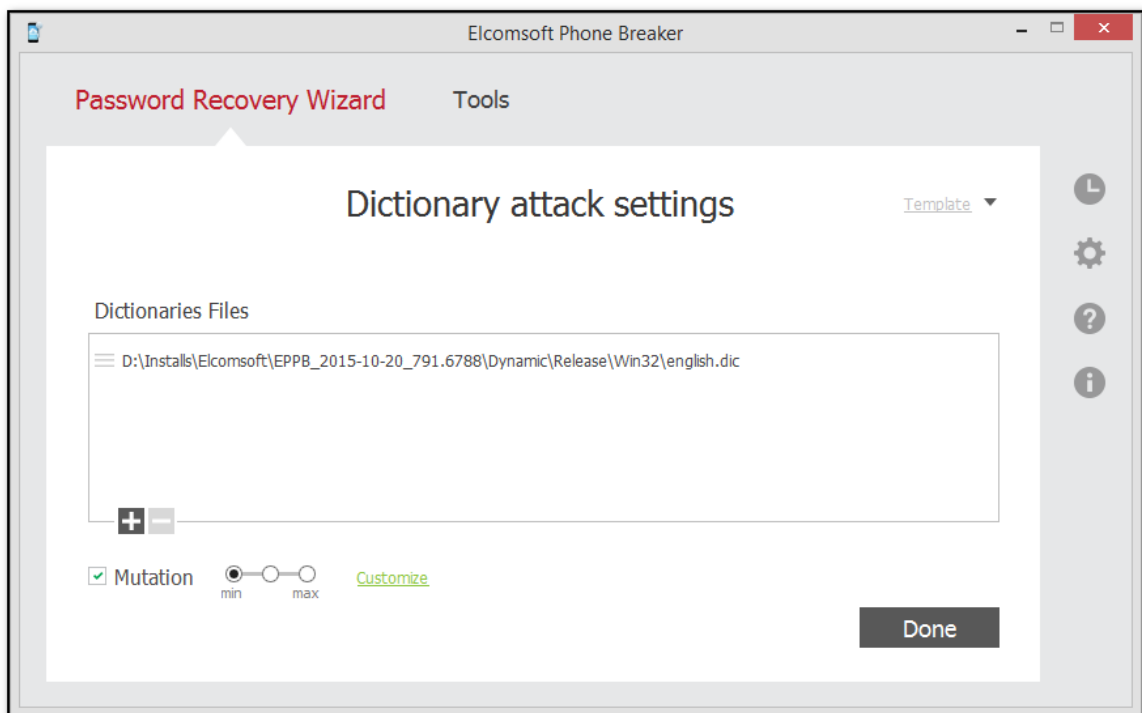
1. Выбор атаки

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 обработано в процессе этой атаки, и набор символов, которые будут использоваться.



2. Окно настроек



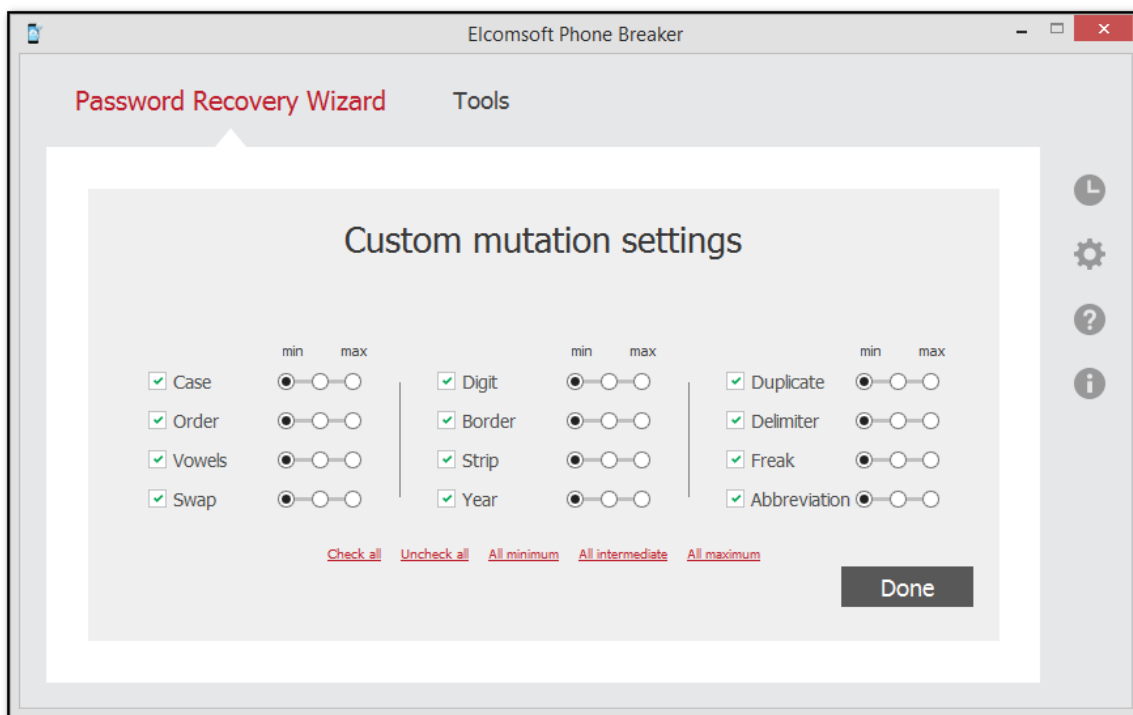
Доступны следующие настройки:

- **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.	<ul style="list-style-type: none"> Минимальный уровень проверяет слова в словаре, написанные в нижнем и верхнем регистре, причем первая буква написана в нижнем регистре, а другие - в верхнем регистре. Средний уровень проверяет все комбинации с минимального уровня, а также первую и последнюю букву слова в верхнем регистре. Максимальный уровень проверяет комбинации из предыдущих уровней, а также комбинации, каждая вторая буква которых написана в верхнем регистре. 	<p><i>password, PASSWORD, pASSWORD.</i></p> <p><i>password, PASSWORD, PasswOrd.</i></p> <p><i>password, PASSWORD, PaSsWoRd.</i></p>
Order	Изменение порядка букв в слове на противоположный, повторение слова, добавление перевернутого слова к исходному слову.	Отличий нет	<i>password - drowssap passwordpassword, passworddrowssap</i>
Vowels	Удаление гласных или их использование в нижнем или верхнем регистре.	Отличий нет	<i>psswrD, PaSSWoRD, pAsswOrd</i>
Swap	Изменение порядка соседних символов в слове.	Отличий нет	<i>apssword, psasword, paswsord</i>
Digit	Добавление нескольких цифр в производное (из словаря) в качестве префикса и суффикса.	<ul style="list-style-type: none"> Минимальный уровень позволяет добавлять цифры (0-9) в конце слова, проверять строчные слова и слова, начинающиеся с заглавной буквы. Средний уровень позволяет проверять слова, написанные 	<i>password1, Password1.</i>

Название мутации	Описание	Уровни	Примеры
		в верхнем регистре, и слова с цифрами в начале. <ul style="list-style-type: none"> Максимальный уровень позволяет проверять комбинации в диапазоне от 00 до 99. 	<i>3password,</i> <i>3PASSWORD.</i> <i>33password,</i> <i>PASSWORD99</i>
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	<i>#password#, \$password\$</i>
Strip	Удаление одного символа из словарного слова.	Отличий нет	<i>assword, pssword,</i> <i>password</i>
Year	Добавление года (1900-2050) в конце слова	Отличий нет	<i>password1973,</i> <i>password2002</i>
Duplicate	Дублирование символов в пароле.	Отличий нет	<i>ppassword, paassword,</i> <i>passsword, passwword</i>
Delimiter	Добавление разделителей, например. + * - \ / # = между символами пароля.	Отличий нет	<i>p.a.s.s.w.o.r.d,</i> <i>p+a+s+s+w+o+r+d,</i> <i>p-a-s-s-w-o-r-d</i>
Freak	Замена некоторых символов в пароле символами.	Отличий нет	<i>p@ssword, p@\$s\$word</i> <i>and p@\$s\$w0rd</i>
Abbreviation	Проверка некоторых часто используемых сокращений.	Отличий нет	<i>ihateyou - ih8you,</i> <i>loveyou - loveu, foryou - 4u.</i>

Используйте [шаблоны](#) ²⁸⁶ для сохранения настроек атаки.

Done/Готово закрывает окно настроек.

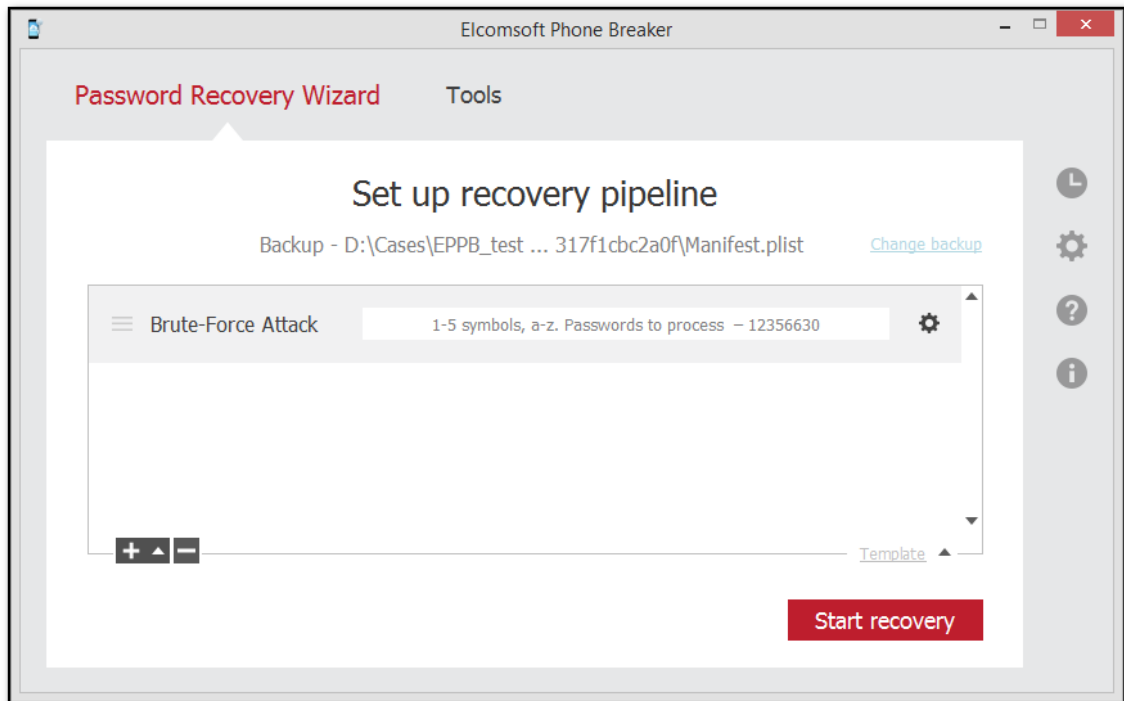
6.2.4.5 Настройка атаки методом полного перебора

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

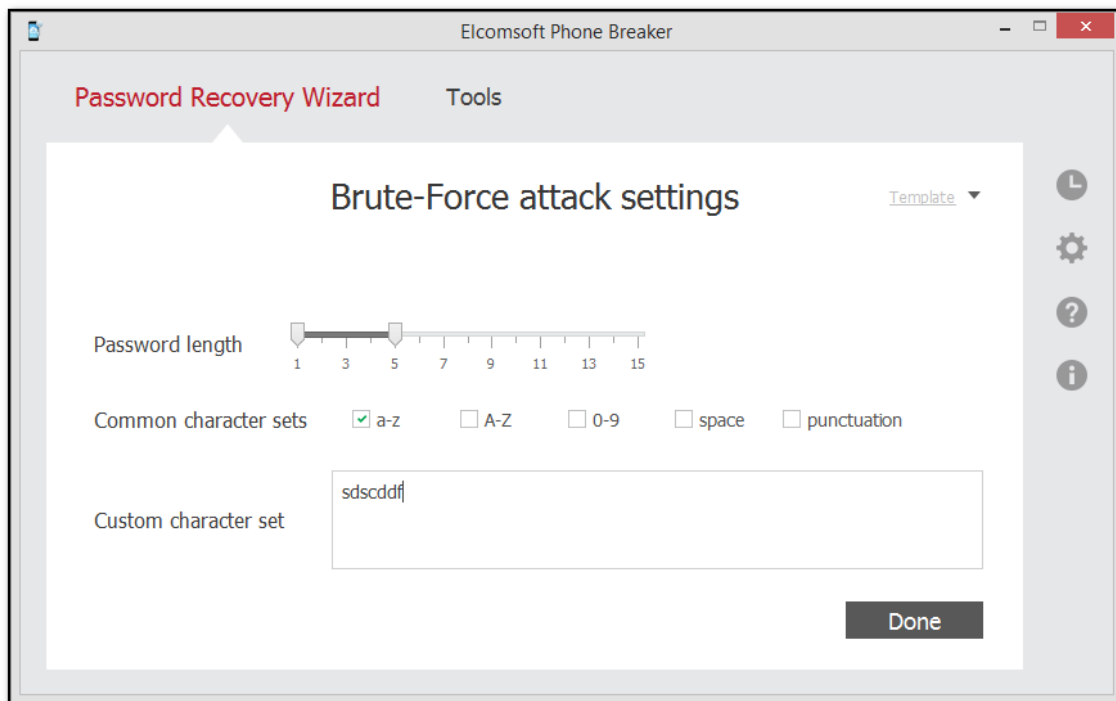
1. Выбор атаки

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 обработано 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:

абвгдеёжзийклмнопрстуфхцчшщъыьэюяАБВГДЕЖЗИЙКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯ.

Используйте [шаблоны](#) ^[286] для сохранения настроек атаки.

Done/Готово закрывает окно настроек.

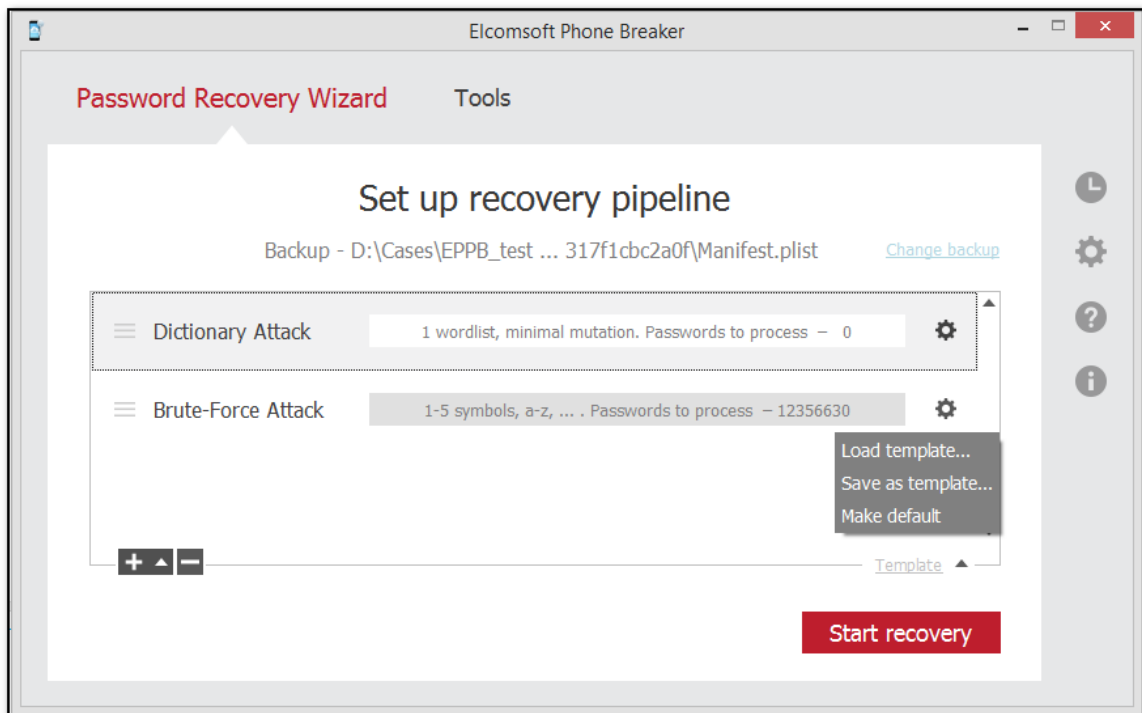
6.2.4.6 Шаблоны

Сохранение шаблонов

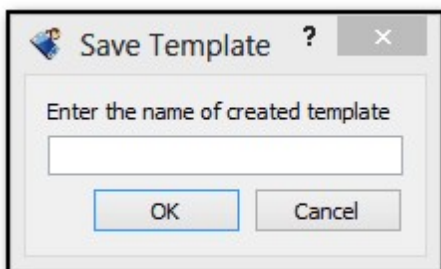
Шаблон - это комбинация настроек конвейера или отдельной атаки, сохраненной в EPB. Шаблоны созданы для упрощения повторного использования определенных настроек при восстановлении паролей к нескольким резервным копиям.

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**.



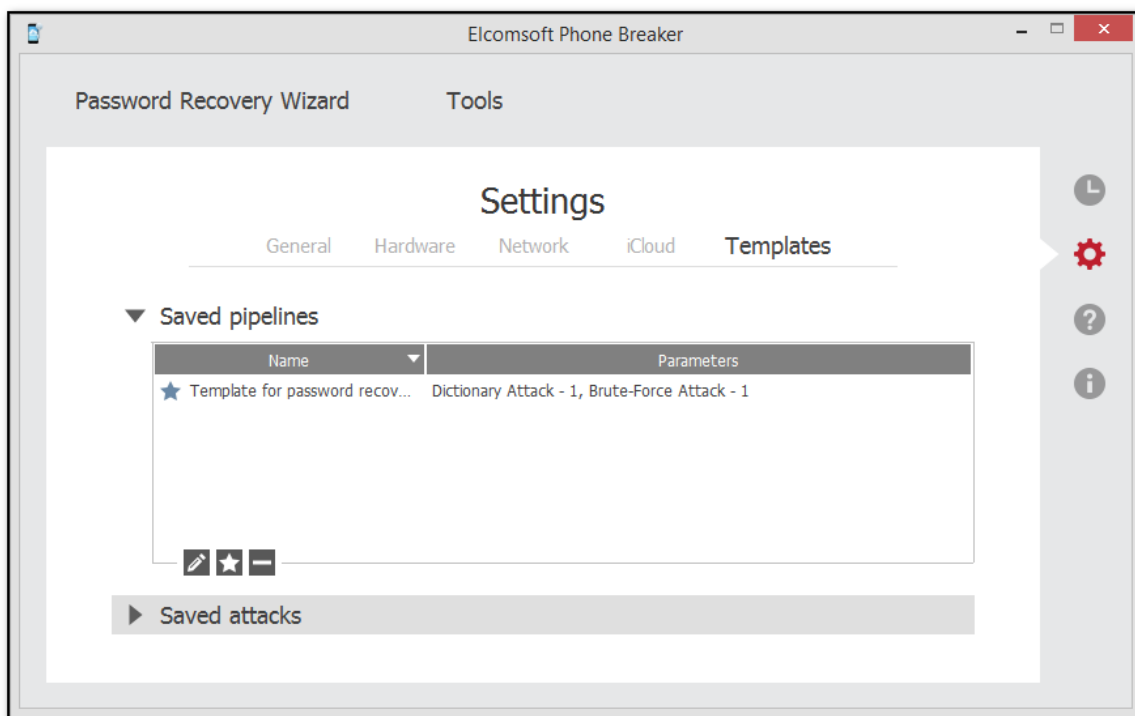
3. В окне **Save Template/Сохранить Шаблон** укажите название шаблона.



[Просмотр шаблонов](#) ²⁸⁴ - Settings/Настройки -> Templates/Шаблоны.


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: 

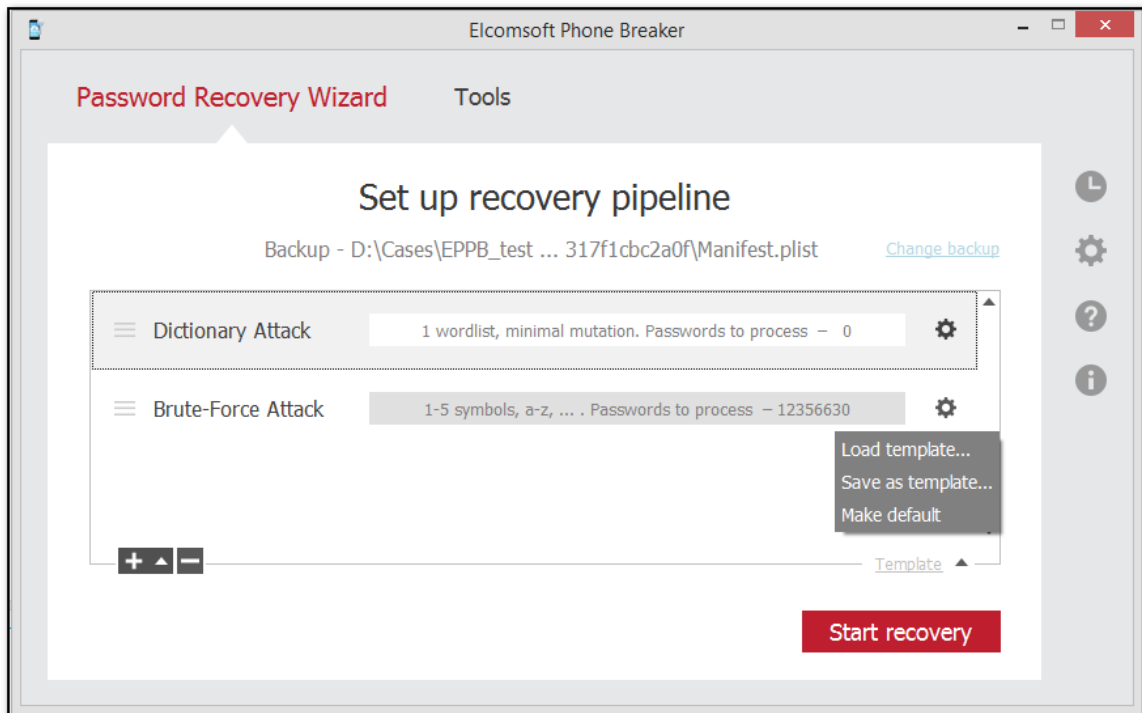
Установка шаблона по умолчанию: 

Удаление шаблона: 

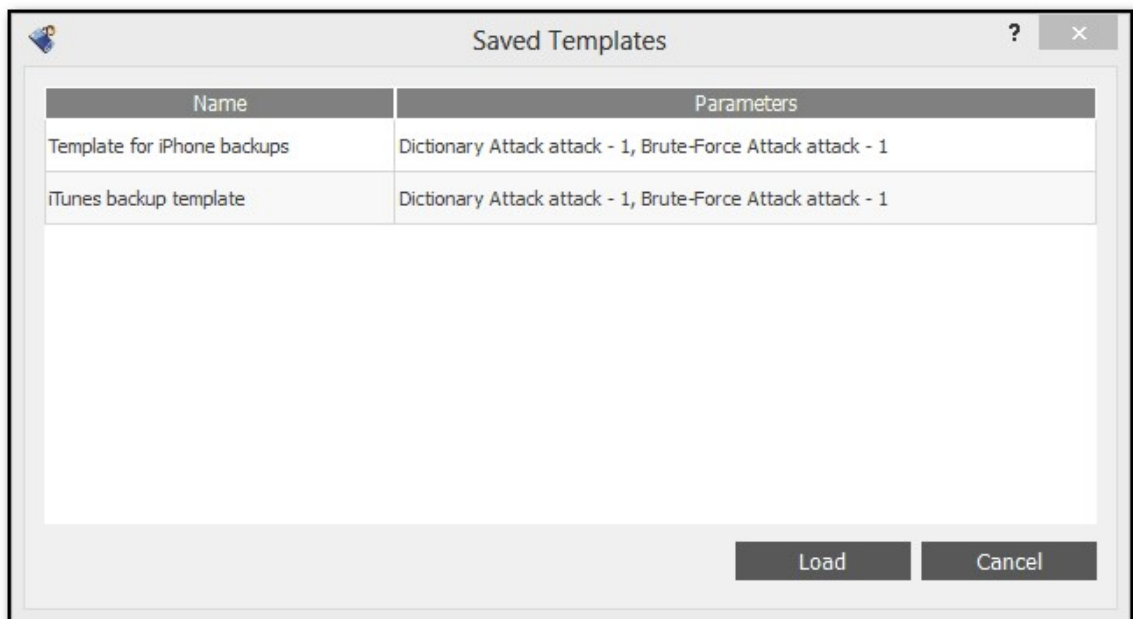
Загрузка шаблонов

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**.




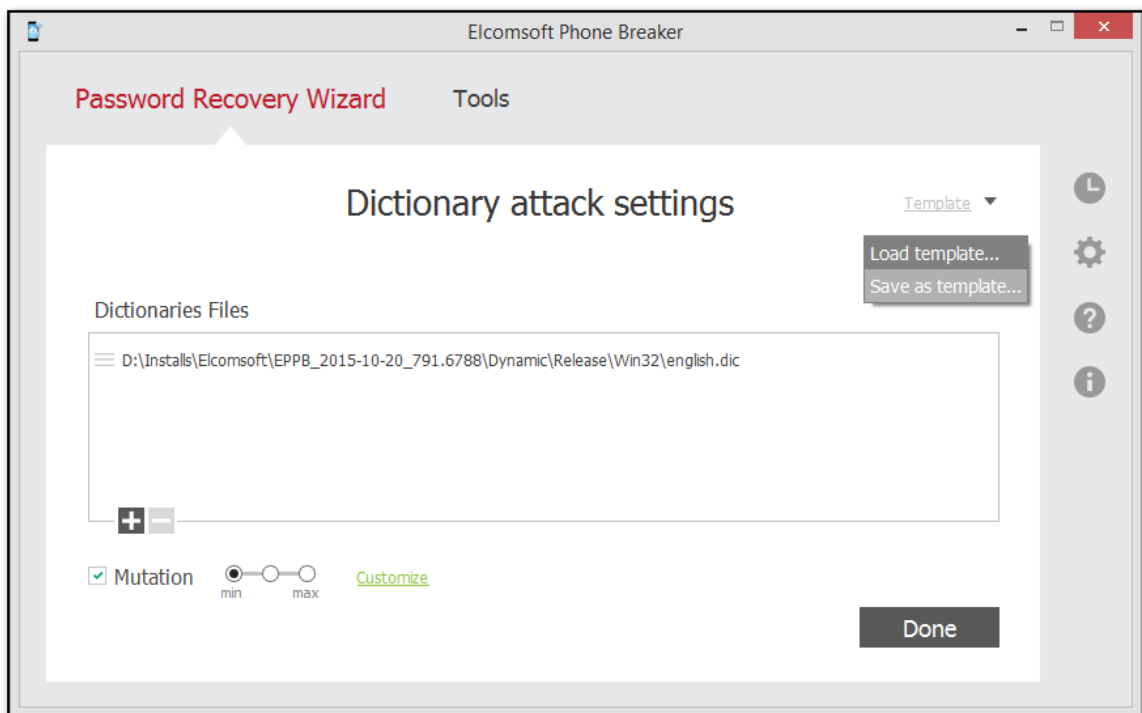
4. Шаблон будет загружен в окне **Set up recovery pipeline/Установить конвейер атак**.

Использование шаблонов в атаках

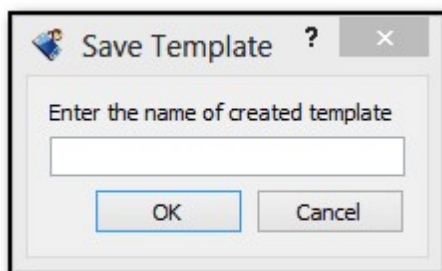
Помимо сохранения всего процесса восстановления в шаблоне, вы можете сохранить настройки отдельной атаки.

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.



6.3 Elcomsoft Phone Viewer

6.3.1 О программе

6.3.1.1 Настройки

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

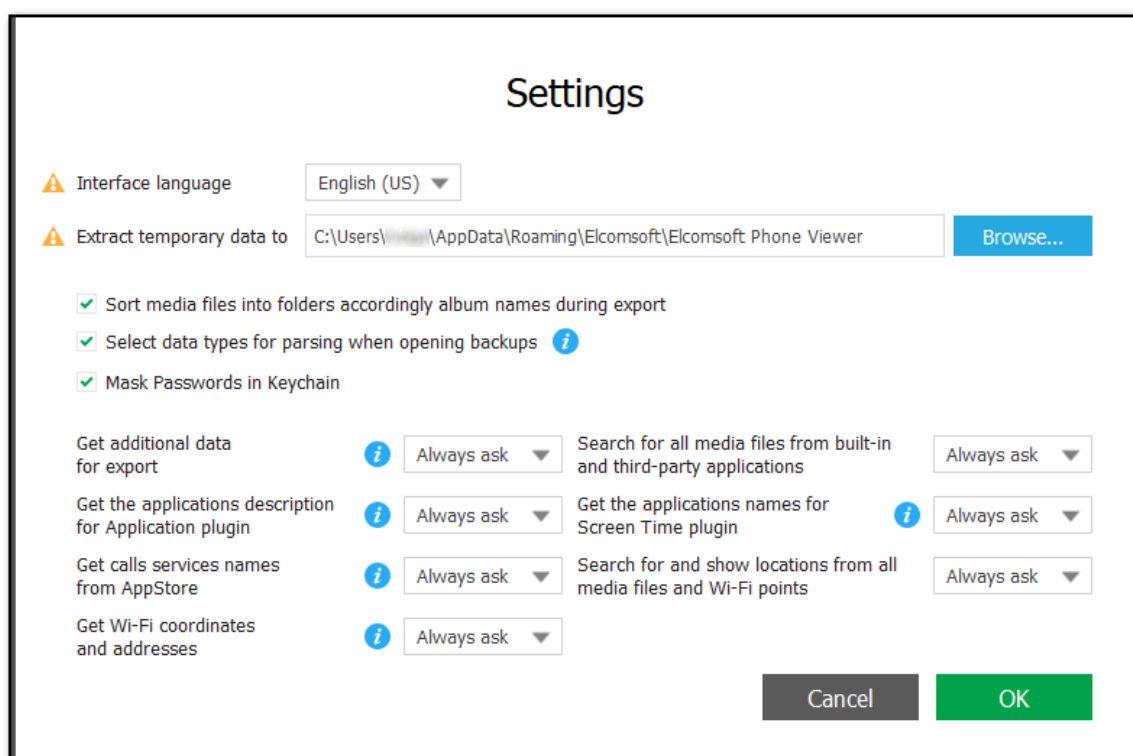
При расшифровке резервной копии создается ряд файлов, содержащих временные данные. Общий размер временных файлов равен размеру резервной копии.

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.

6.3.1.2 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 .

6.3.1.3 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.

6.3.2 Анализ данных Apple

6.3.2.1 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 удастся 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.

6.3.2.2 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 отдельных приложений.

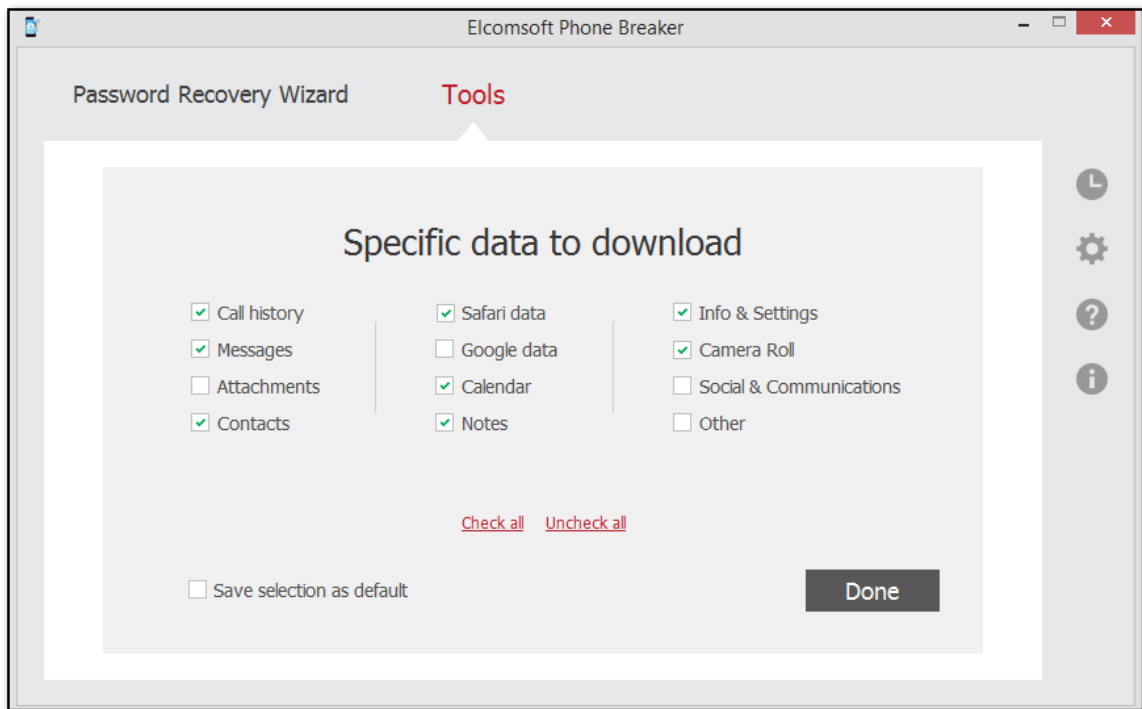
О содержимом резервных копий iCloud можно узнать на сайте Apple:

[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



6.3.2.3 Образ файловой системы iOS

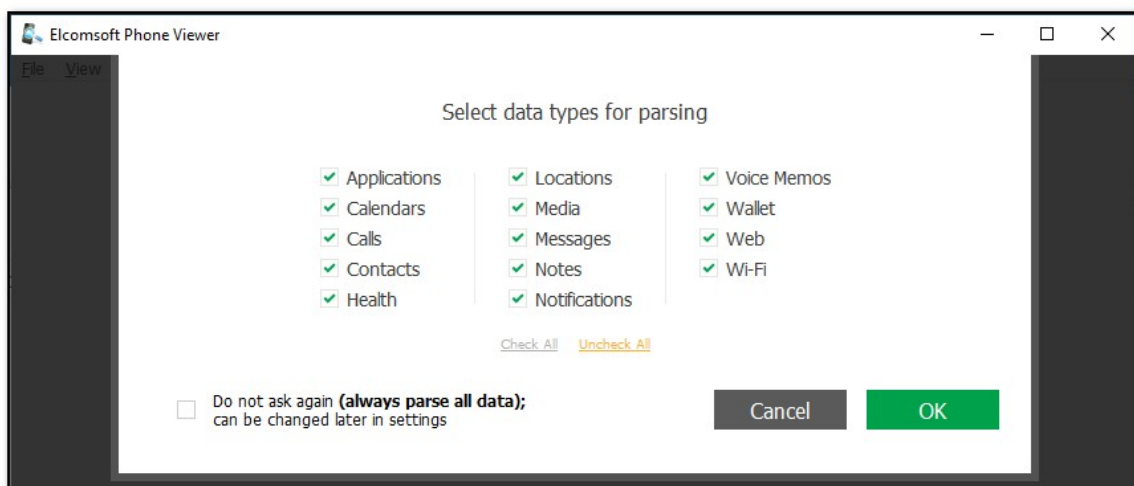
EPV поддерживает анализ образа файловой системы, извлечённого посредством [Elcomsoft iOS Forensic Toolkit](#).

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.

6.3.2.4 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 EPV 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.

6.3.2.5 Анализ образа файловой системы

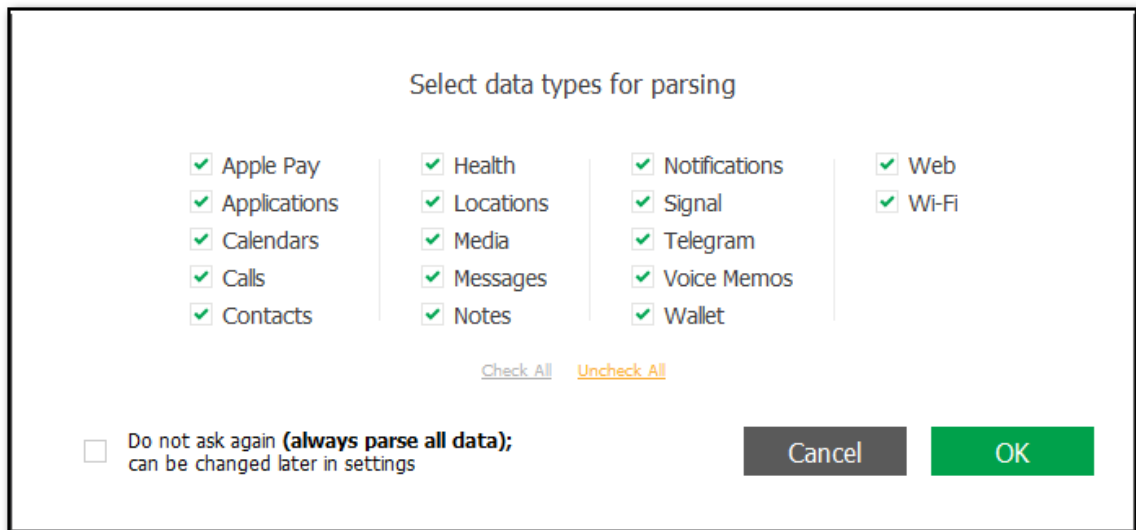
EPV позволяет просматривать содержимое образа файловой системы, извлечённое посредством [Elcomsoft iOS Forensic Toolkit](#) (EIFT). Поддерживаются следующие категории данных:

- **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:

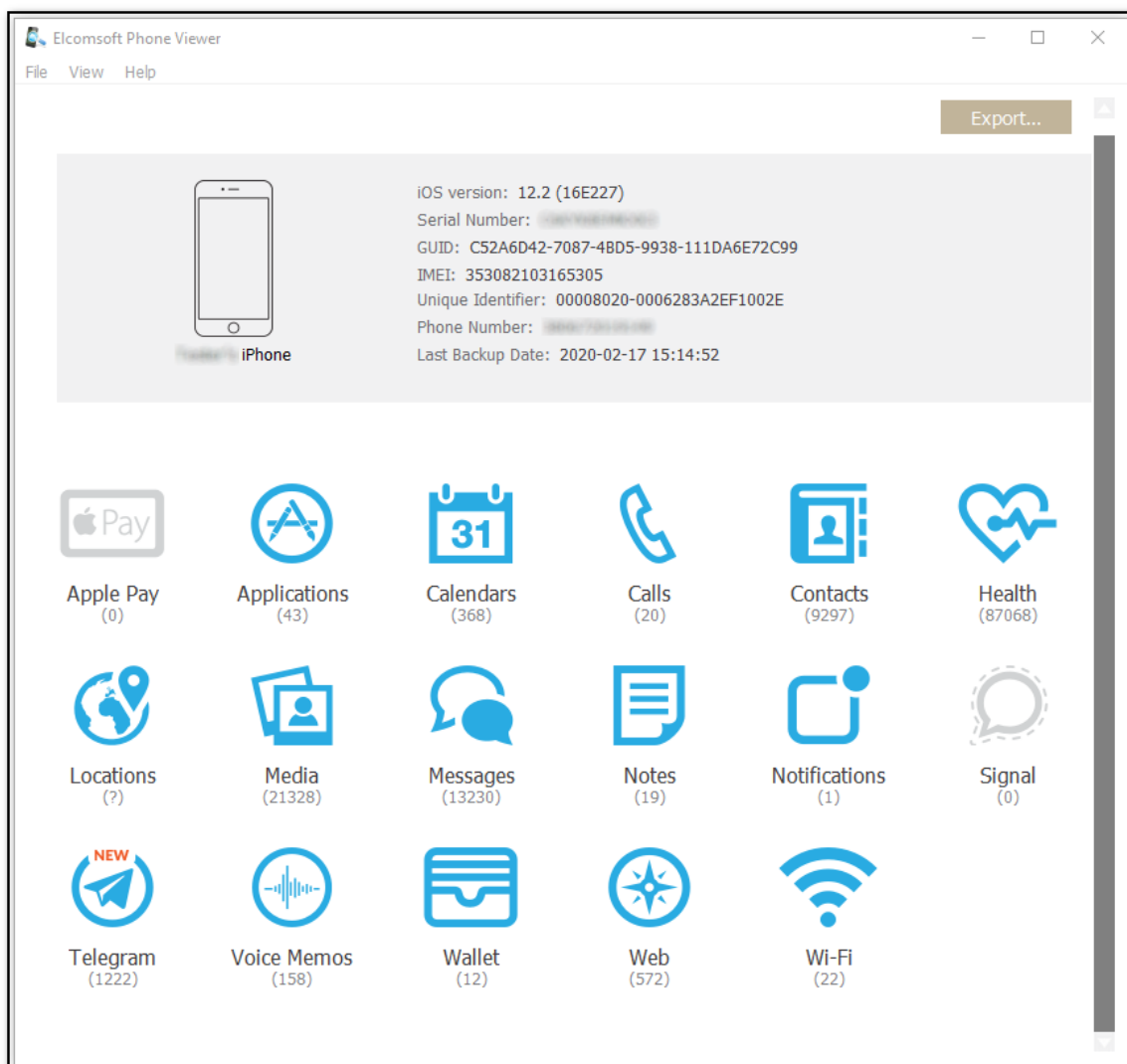
1. Выберите **iOS device image/Образ устройства iOS** в главном окне программы либо выберите **iOS device image/Образ устройства iOS** в меню **File/Файл > Open/Открыть** либо перетащите образ файловой системы на главное окно программы.
2. Выберите типы данных для анализа. Впоследствии выбор можно изменить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

6.3.2.6 Анализ синхронизированных данных iCloud

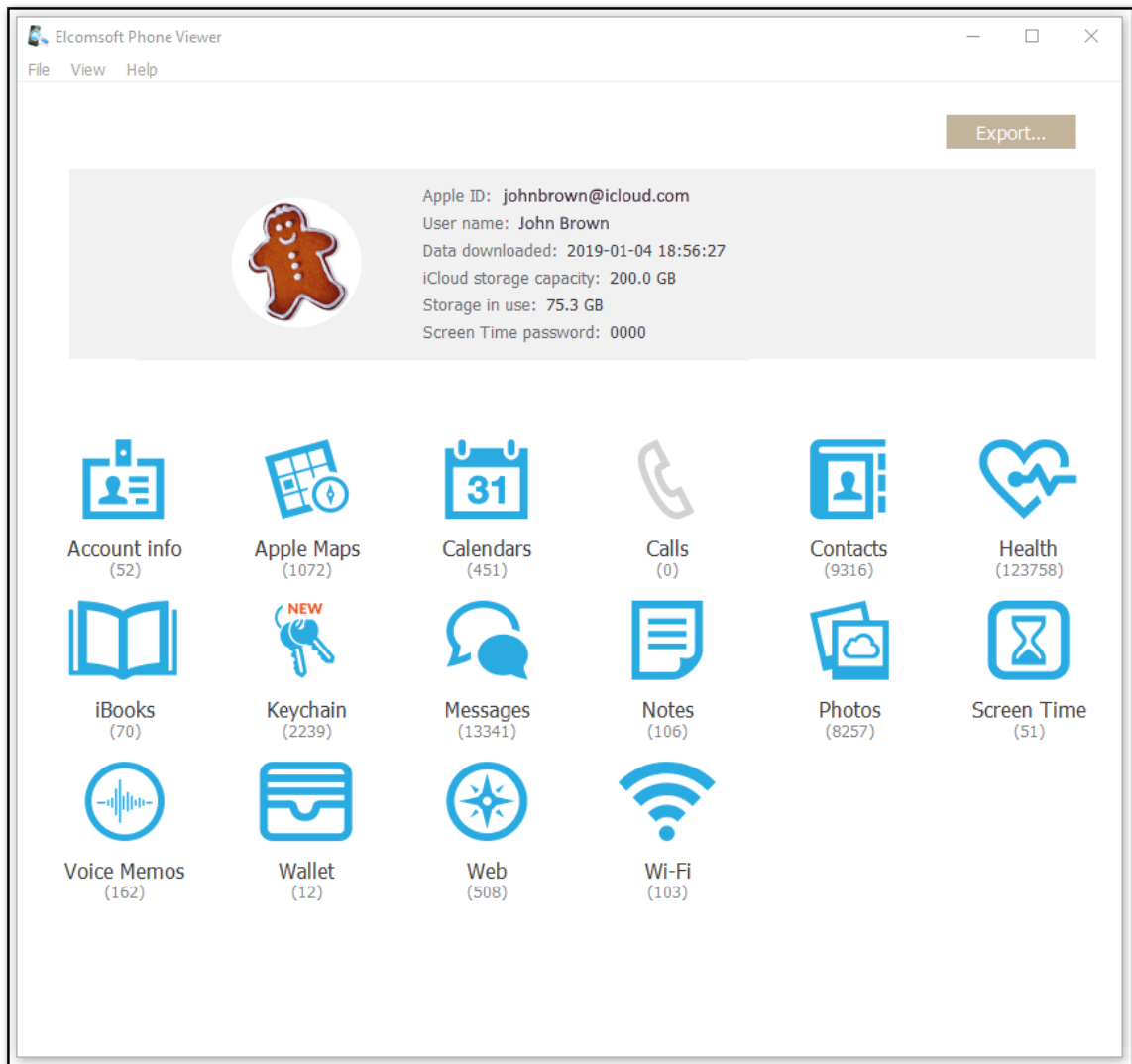
EPV позволяет просматривать синхронизированные данные, скачанные из облака iCloud посредством [Elcomsoft Password Breaker](#). Поддерживаются следующие категории данных:

- 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
- Объём 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.

6.3.3 Анализ данных Microsoft Account

6.3.3.1 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.

6.3.4 Плагины

6.3.4.1 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.

6.3.4.2 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.

6.3.4.3 Связка ключей

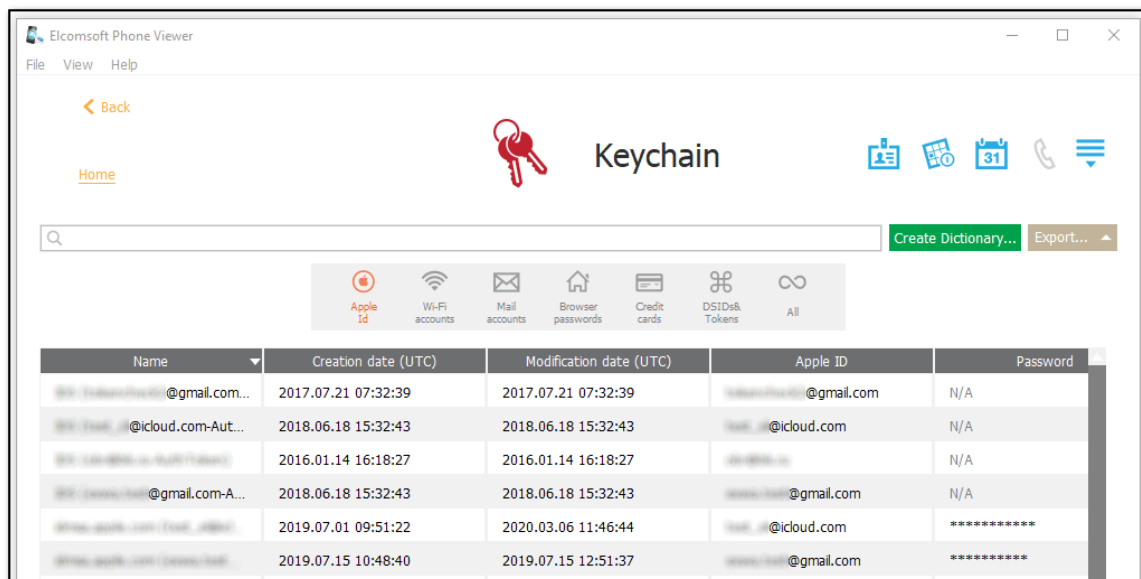
Этот плагин позволяет исследовать данные связки ключей, такие как пароли Apple ID, пароли Wi-Fi, пароли почтовых учетных записей, данные кредитной карты и т.д.

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.

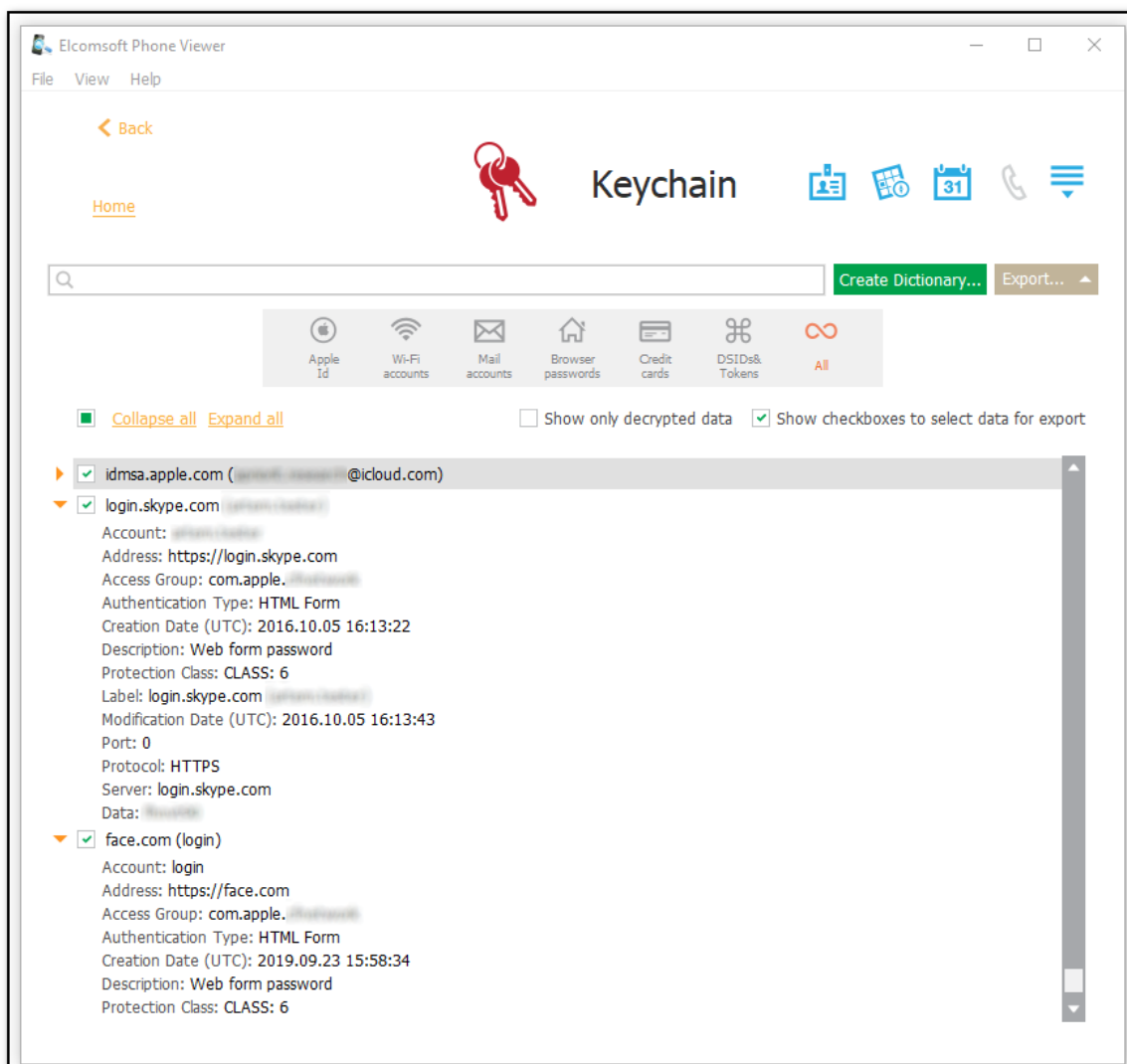
Большинство вкладок (**Wi-Fi accounts/Аккаунты Wi-Fi, Mail accounts/Почт. аккаунты, Browser passwords/Пароли браузеров** и т.д.) не нуждается в пояснениях. Отдельного упоминания заслуживает две вкладки.

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**.

6.3.4.4 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](#)^[298].

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

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.

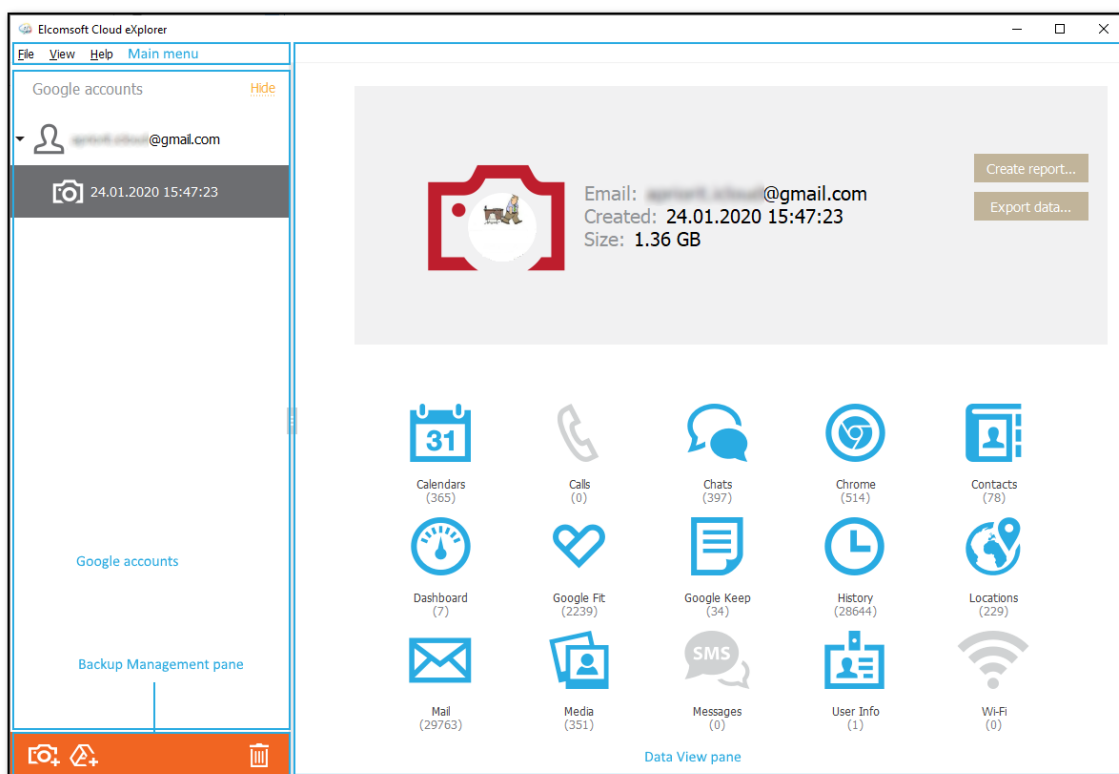
При открытии данного модуля вы сможете запросить данные о местоположении точек доступа Wi-Fi. Обратите внимание, что для этого требуется подключение к Интернету. После загрузки данных о местоположении Wi-Fi они сохраняются в локальный кеш. Процесс скачивания этих данных блокирующий: вы не сможете открывать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

6.4 Elcomsoft Cloud Explorer

6.4.1 О программе

6.4.1.1 Пользовательский интерфейс

Пользовательский 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 ЕСХ. Наконец, в панели управления резервными копиями отображаются наборы данных, скачанные для каждой учётной записи.

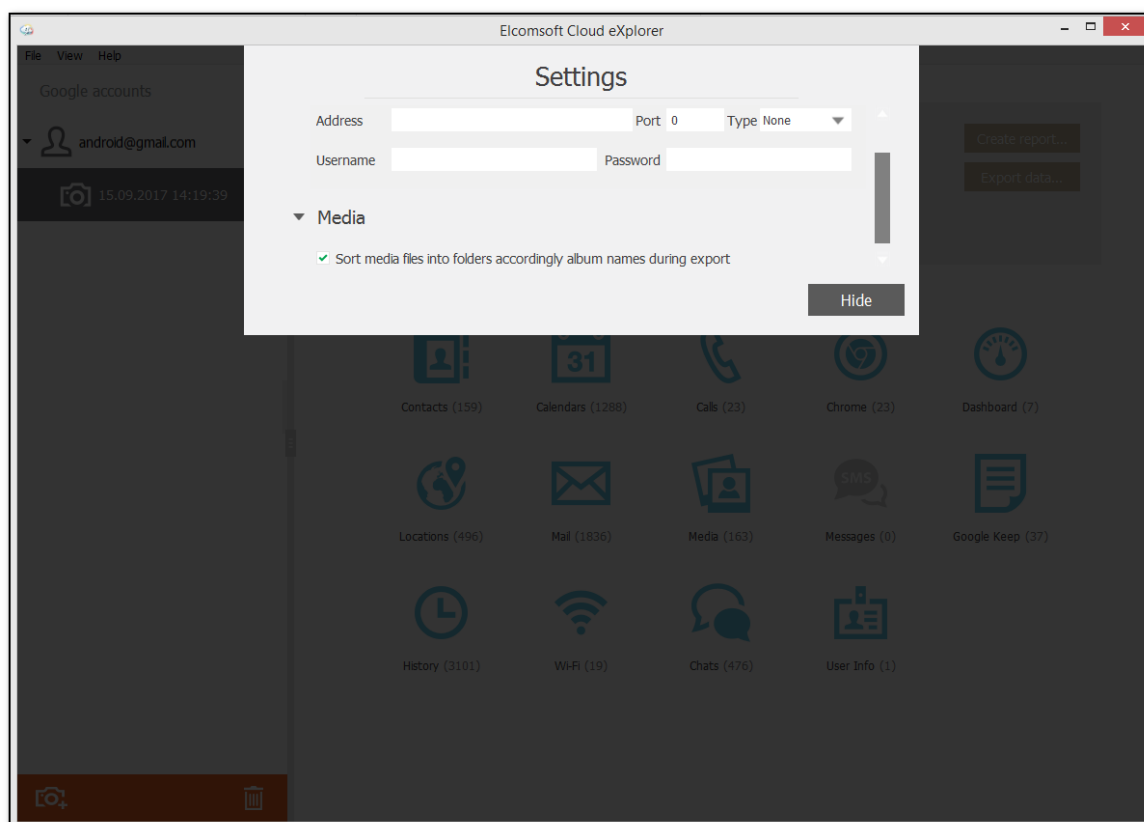


6.4.1.2 Окно настроек

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 подменной сертификата не поддерживаются.



6.4.1.3 Изменение пути к хранилищу

По умолчанию ECX сохраняет скачанные данные в следующих папках:

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

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.

6.4.2 Данные из Google Account

6.4.2.1 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**, EСХ 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. EСХ 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.

The screenshot shows a dialog box titled "Download snapshot" with a help icon in the top right corner. Below the title bar, there are two tabs for "Authentication type": "Password" (selected) and "Token". Below the tabs are two input fields: "Google ID" containing "android@gmail.com" and "Password" with masked characters. To the right of the Google ID field is a placeholder "(example@example.com)". Below the password field is an eye icon. A warning message with a yellow triangle icon states: "Important: If the account uses 2FA and you log on with the password, a verification code will be requested on the next step. It will be sent by SMS immediately once you click Sign In. Google Authenticator or Backup verification codes can be also used." At the bottom, there are two checked checkboxes: "Save credentials for future use" and "Use token instead of password (if available)". To the right of the checkboxes are "Cancel" and "Sign in" buttons.

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.

Download snapshot

Authentication type Password Token ?

Token C:/Program Files (x86)/Elcomsoft Password Recovery/Elcomsoft Cloud eXp... ▼

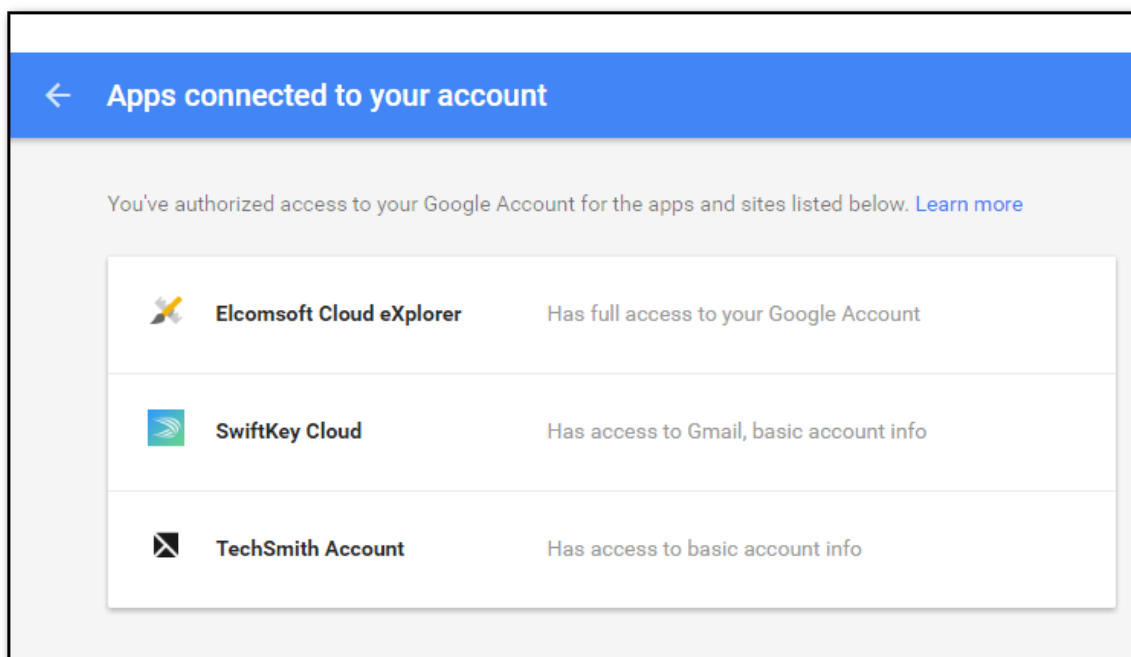
i You can only use Google Chrome tokens to download a snapshot.

Save credentials for future use ?

Cancel Sign in

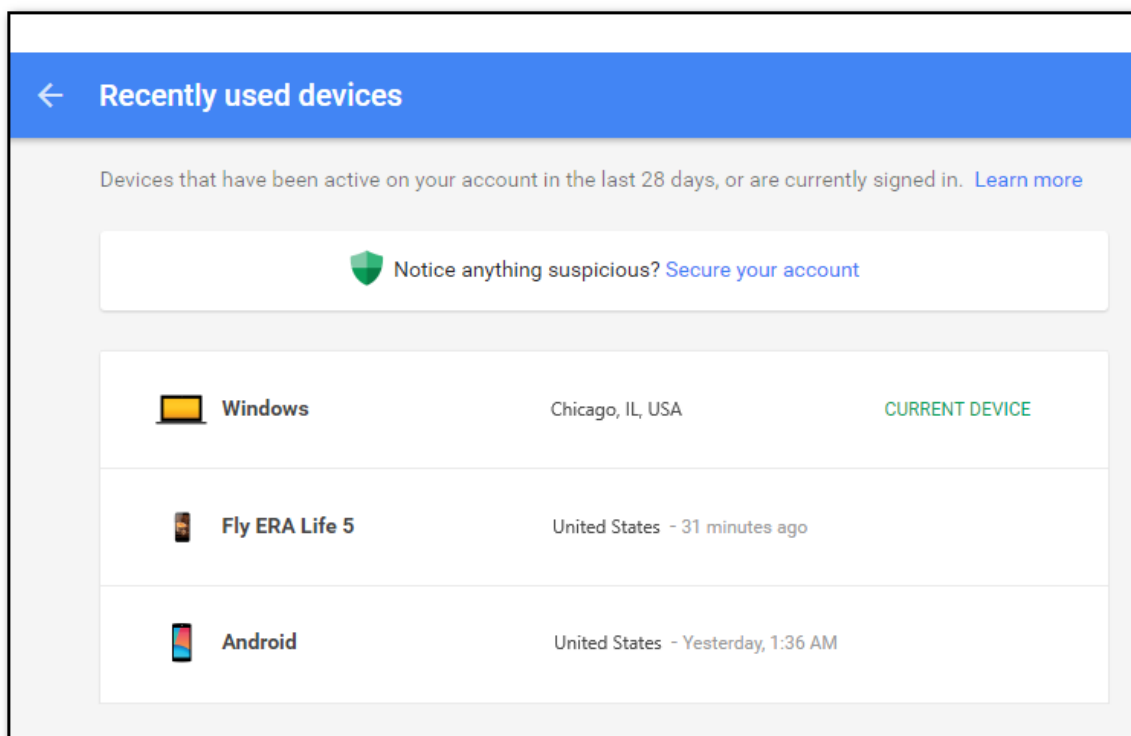
Уведомления о безопасности

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 учётной 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 появятся, 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.

6.4.2.2 Скачивание данных из Google Account

С помощью EСХ 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.

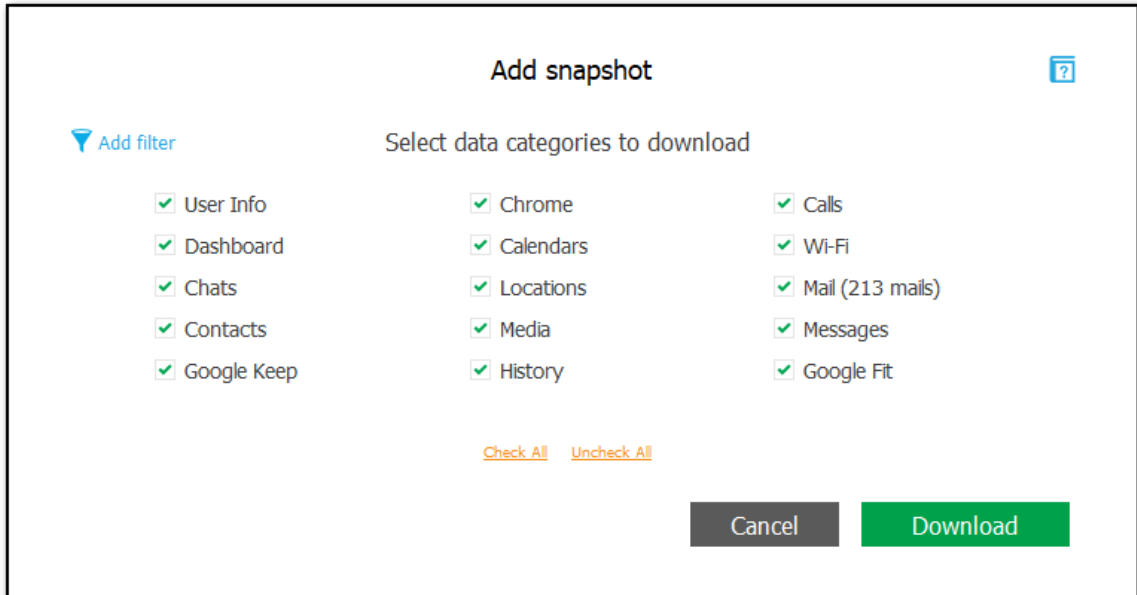
Чтобы загрузить информацию из аккаунта Google, сделайте следующее:


1. В меню **File/Файл** нажмите **Add Google Snapshot/Добавить копию Google** либо нажмите

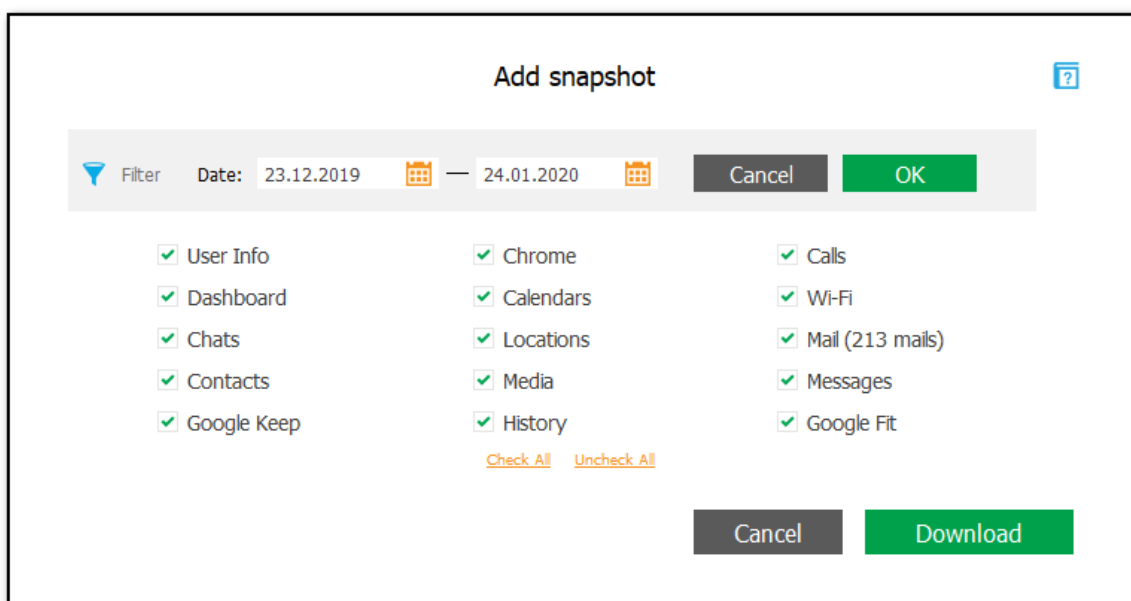


в нижнем левом углу окна ECX

2. На странице **Download snapshot/Скачать снимок данных** укажите тип авторизации (пароль или маркер).
3. Нажмите **Sign in/Войти**.
4. Выберите категории для скачивания.



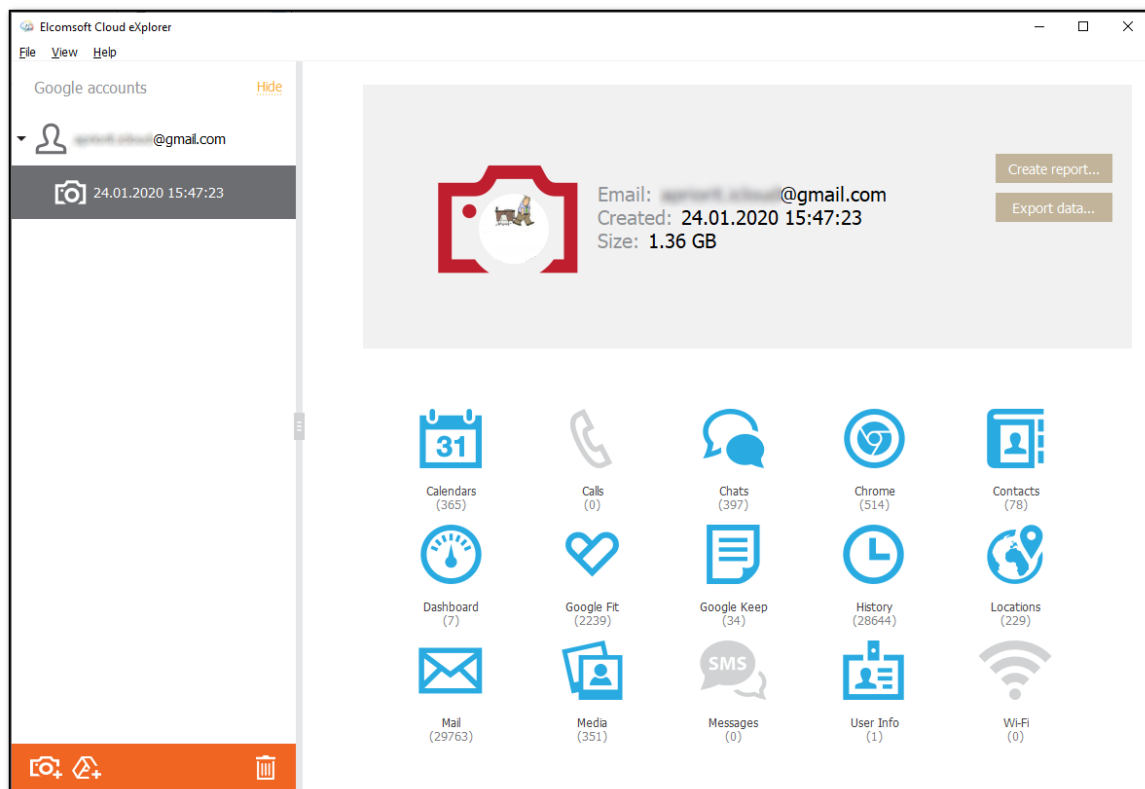
Для категорий **Mail/Почта** и **Media/Медиафайлы** доступна фильтрация . Вы можете выбрать промежуток времени, за который будут скачаны письма и фотографии пользователя.



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, EСХ 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 .

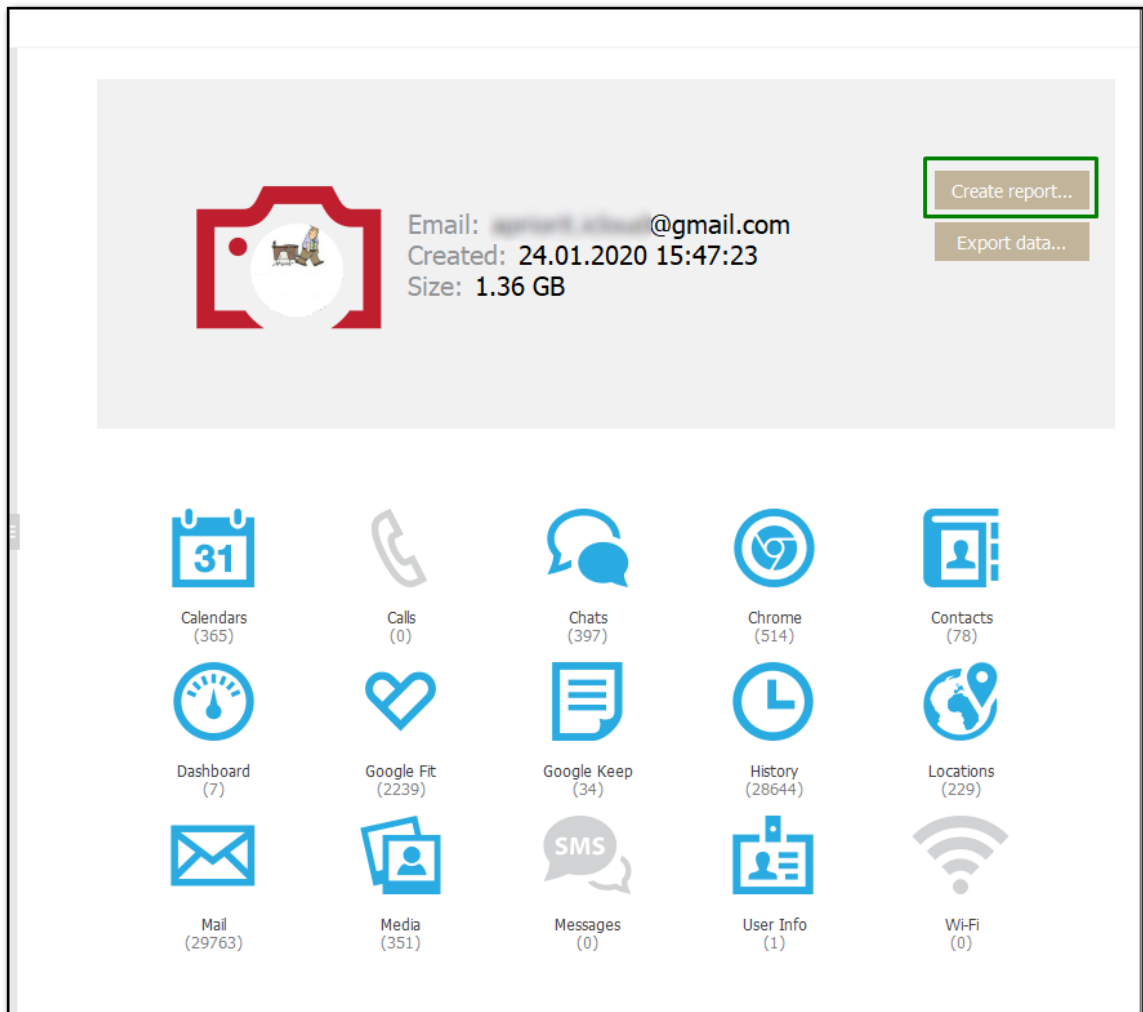
6.4.2.3 Отчёты

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**.


Include the following categories in the report:

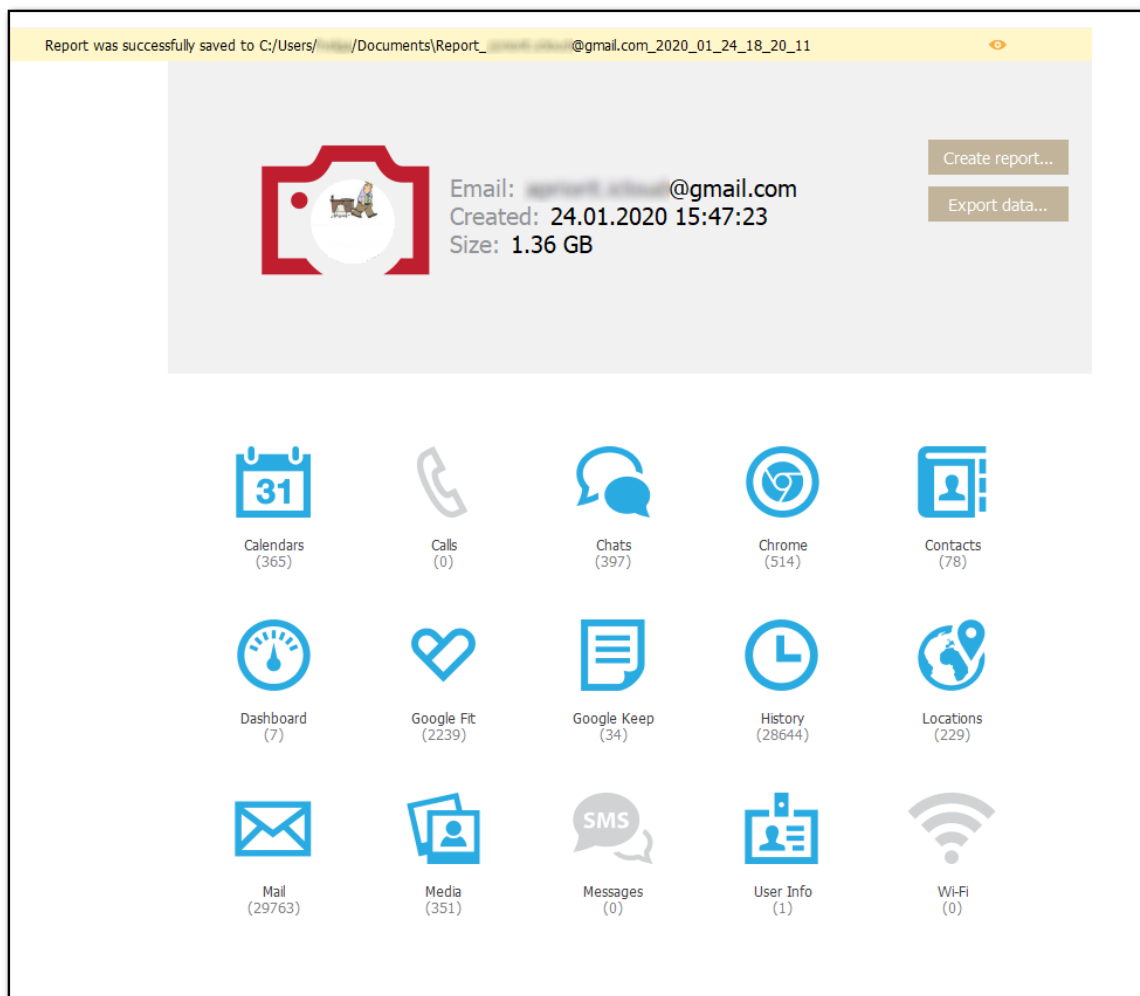
<input checked="" type="checkbox"/>  Calendars (365)	<input type="checkbox"/>  Calls (0)	<input type="checkbox"/>  Chats (397)	<input type="checkbox"/>  Chrome (514)	<input type="checkbox"/>  Contacts (78)
<input checked="" type="checkbox"/>  Dashboard (7)	<input type="checkbox"/>  Google Fit (2239)	<input type="checkbox"/>  Google Keep (34)	<input type="checkbox"/>  History (28644)	<input type="checkbox"/>  Locations (229)
<input type="checkbox"/>  Mail (29763)	<input type="checkbox"/>  Media (351)	<input type="checkbox"/>  Messages (0)	<input type="checkbox"/>  User Info (1)	<input type="checkbox"/>  Wi-Fi (0)

[Check all](#) [Uncheck all](#)

Filter **ON** Date:

Save as default

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.

6.4.2.4 Экспорт данных

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

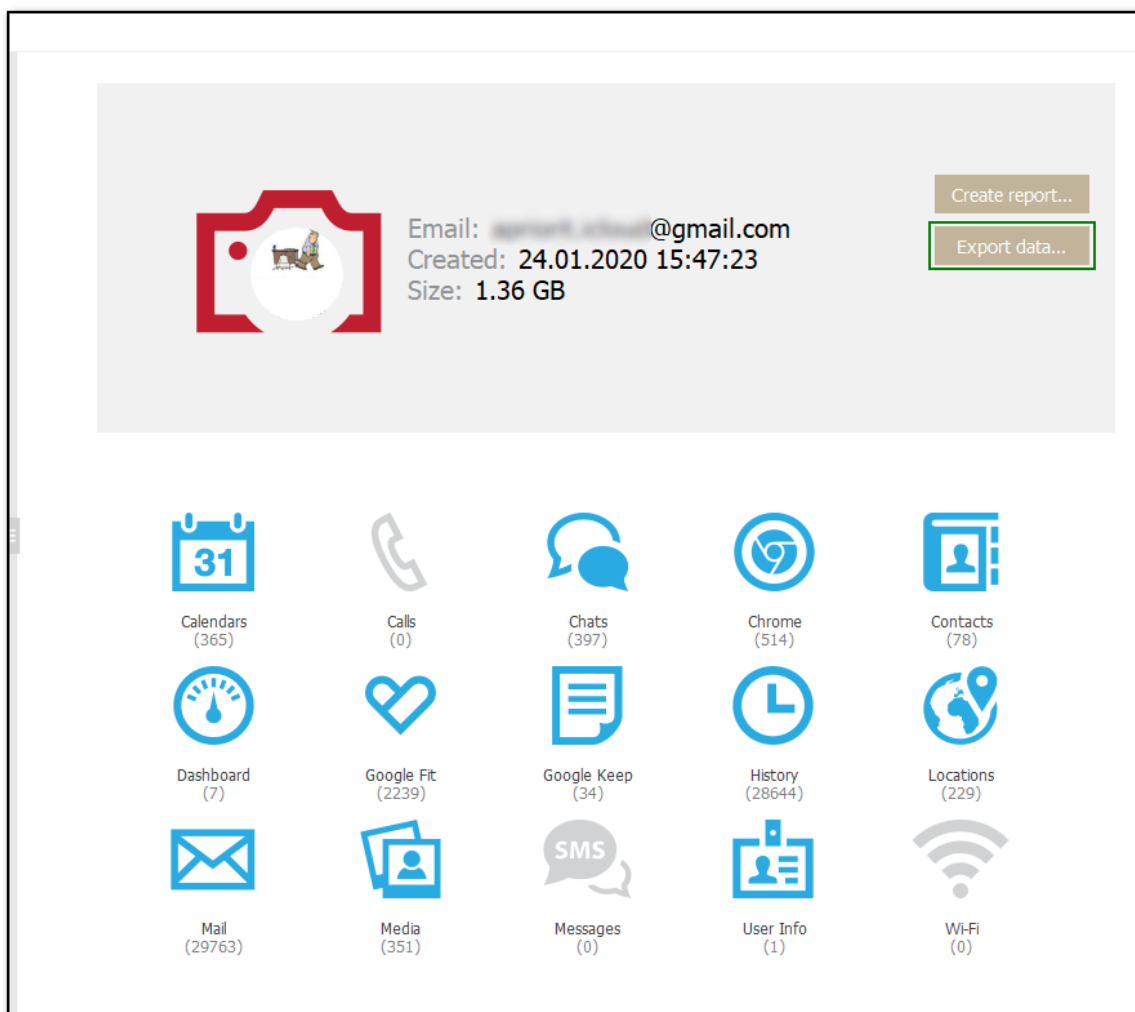
*ПРИМЕЧАНИЕ. Экспорт данных категории **Личный кабинет Google** не поддерживается.*

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 .

6.4.2.5 Двухфакторная аутентификация

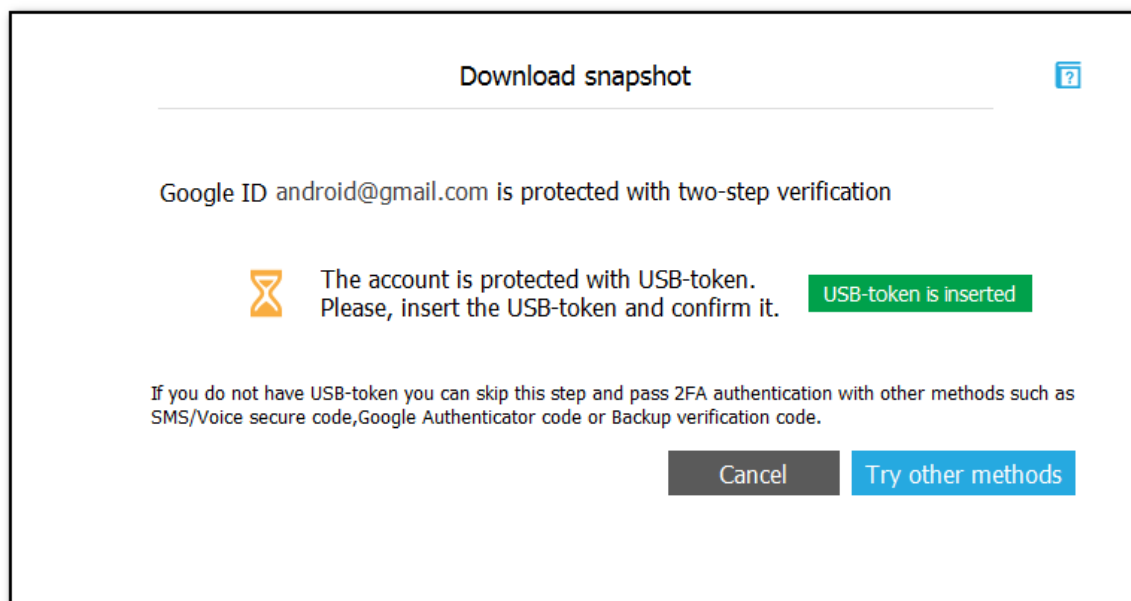
Некоторые учетные записи Google требуют двухэтапной проверки, что означает, что они защищены паролем и одним из дополнительных методов (в зависимости от метода, определенного по умолчанию в настройках безопасности учетной записи Google):

- 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

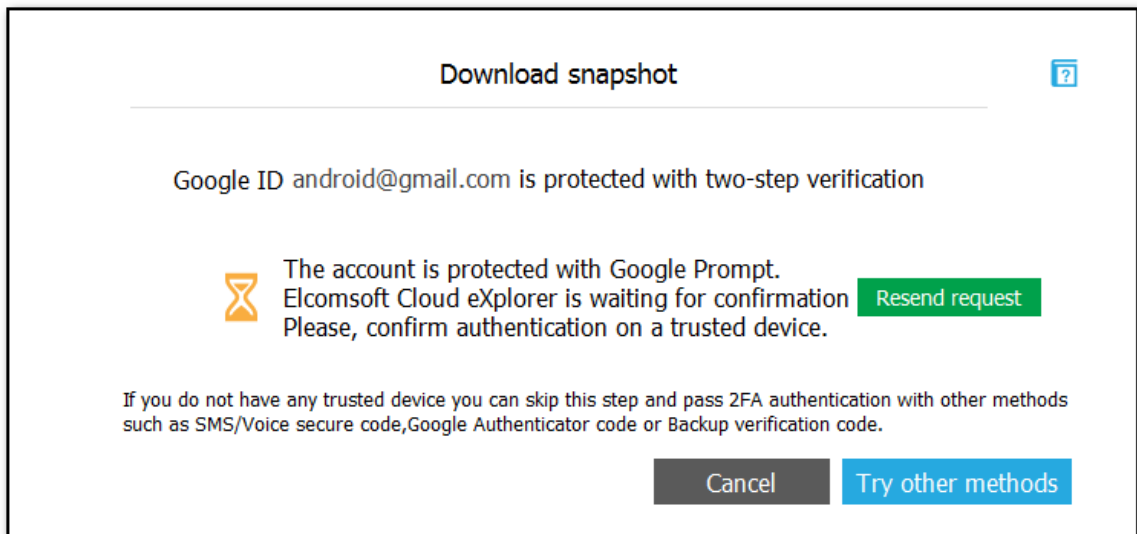
Если учетная запись защищена USB-токеном, вставьте USB-токен и нажмите кнопку **USB-token is inserted/USB-токен вставлен**.



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

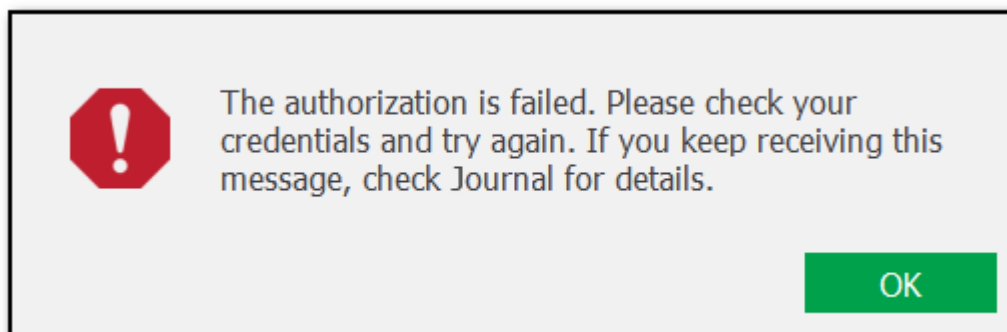
Если у вас есть доступ к приложению Google Authenticator, установленному на устройстве пользователя, вы можете использовать одноразовый код, сгенерированный этим приложением. Обратите внимание: код генерируется по протоколу TOTP (Time-based One Time Password) и действителен в течение 30 секунд.

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 ЕСХ для прохождения аутентификации.

6.4.2.6 Исключения и особые случаи

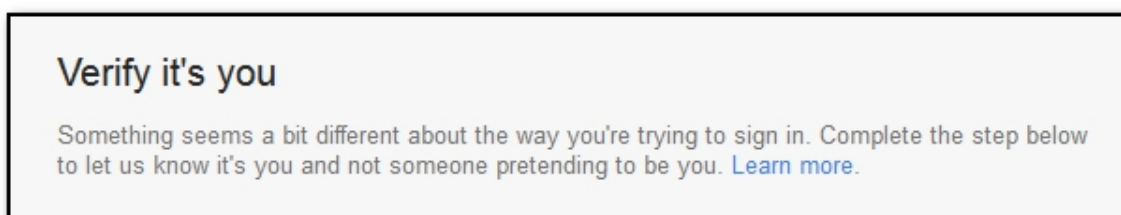
В процессе входа в Google могут возникать исключительные случаи, когда авторизация не удалась. В этом случае вы получите следующее сообщение:



Авторизация не выполняется в следующих случаях:

- Если вы попытаетесь войти в систему с помощью ЕСХ 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 ЕСХ 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 ЕСХ.

6.4.3 Данные в Google Drive

6.4.3.1 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 учетную 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 учетные 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.

Download files from Google Drive

Authentication type: Password (selected), Token

Google ID: android@gmail.com (example@example.com)

Password: [masked]

Important: If the account uses 2FA and you log on with the password, a verification code will be requested on the next step. It will be sent by SMS immediately once you click Sign In. Google Authenticator or Backup verification codes can be also used.

Save credentials for future use

Use token instead of password (if available)

Buttons: Cancel, Sign in

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.

Download files from Google Drive

Authentication type Password Token ?

Token C:/Program Files (x86)/Elcomsoft Password Recovery/Elcomsoft Cloud eXp... ▾

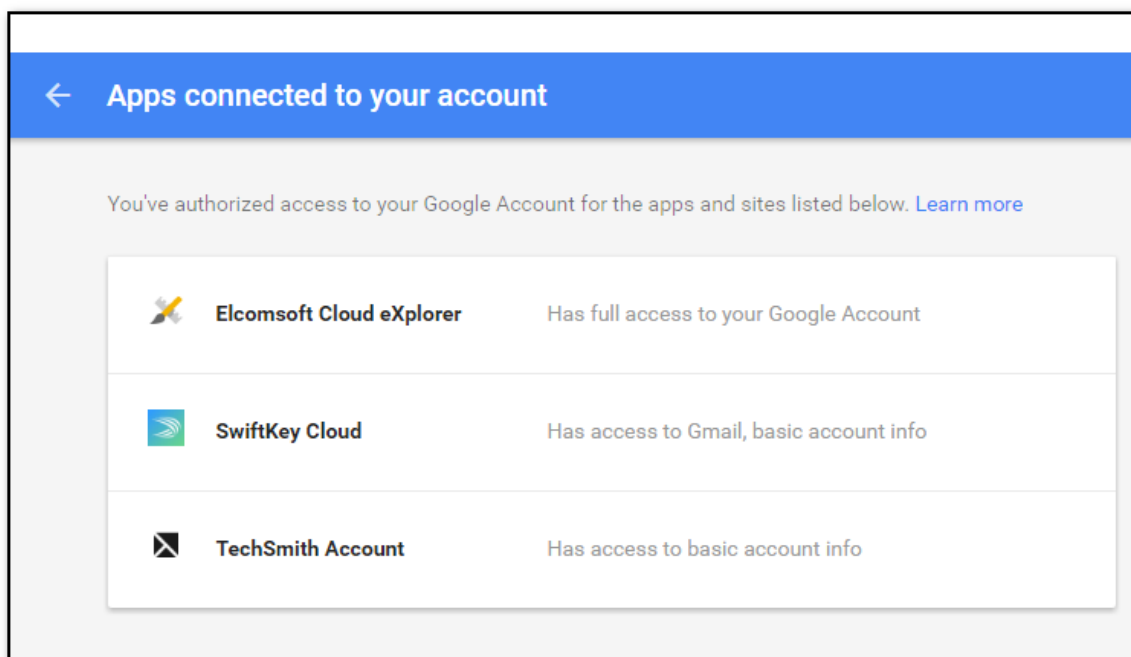
i You can use either Google Chrome or Google Drive tokens to download files.

Save credentials for future use ?

Cancel Sign in

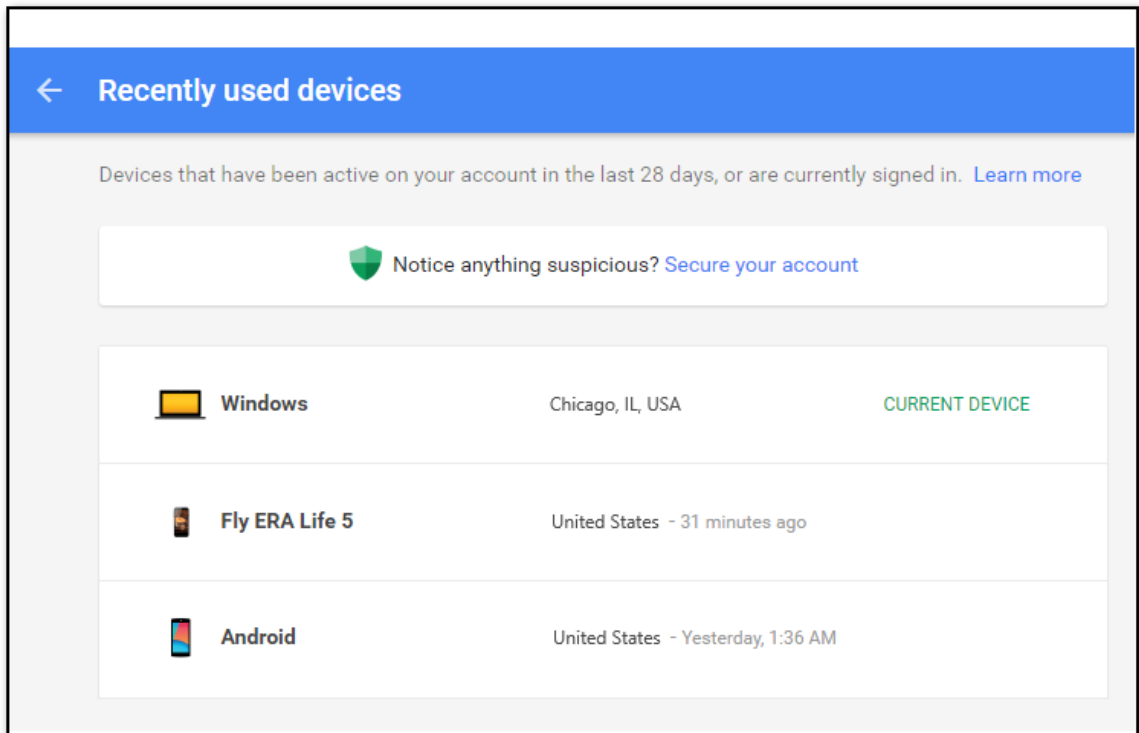
Уведомления о безопасности

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 учётной 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 появятся, 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.

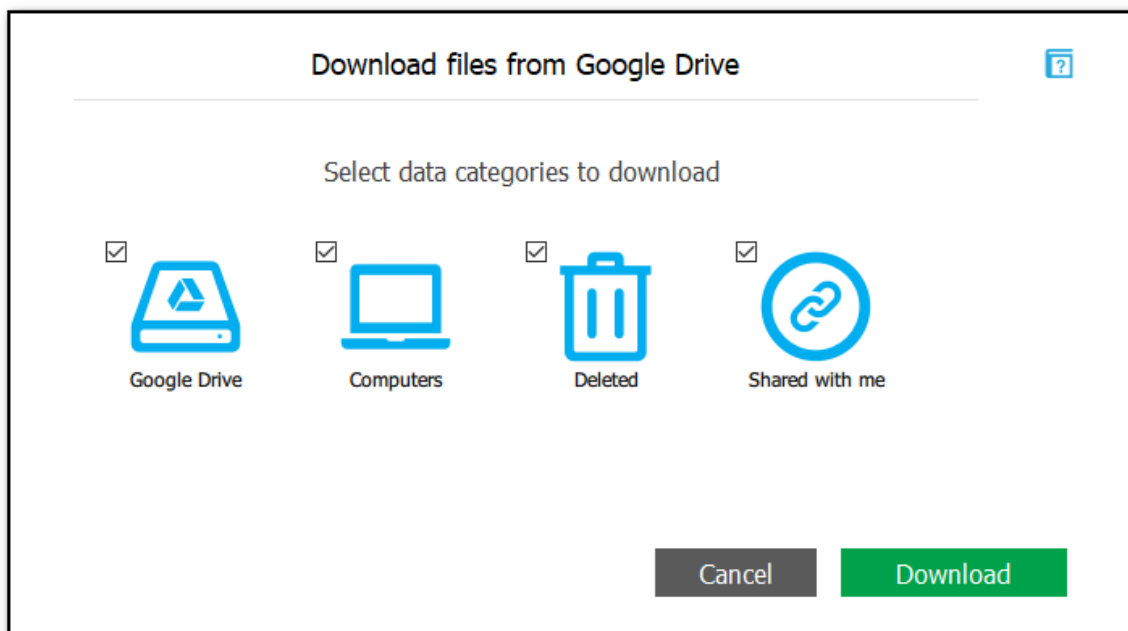
6.4.3.2 Скачивание данных из Google Drive

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.



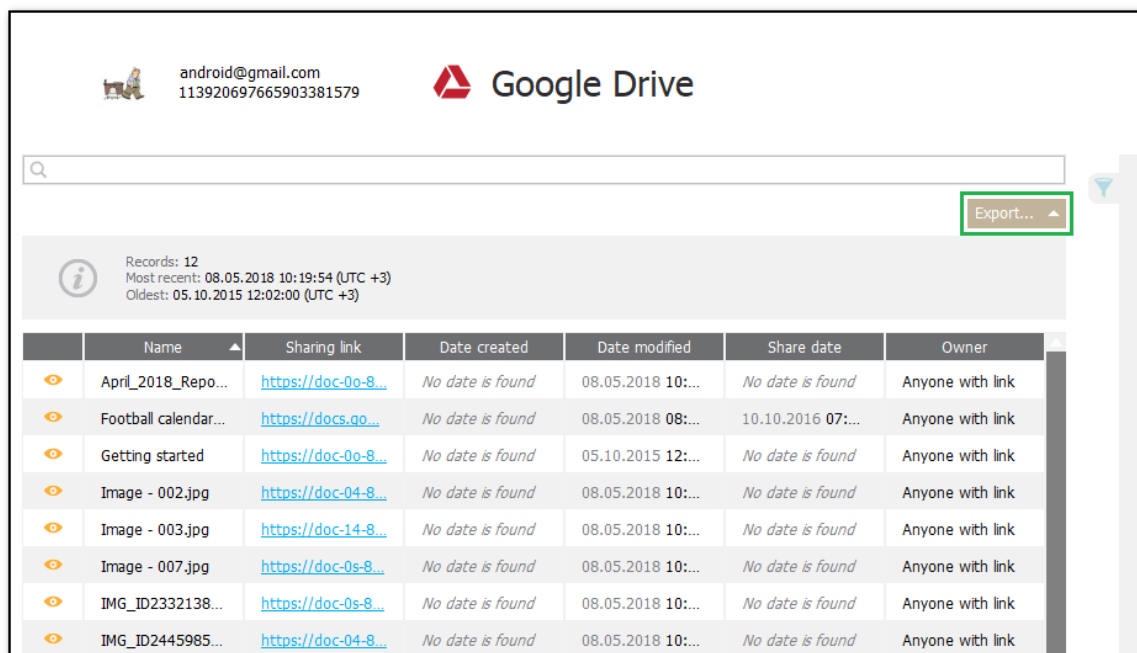
6.4.3.3 Экспорт данных

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.



The screenshot shows the Google Drive interface for a user named android@gmail.com. At the top, there is a search bar and an 'Export...' button highlighted with a green box. Below the search bar, there is a summary of records: 12 records, most recent from 08.05.2018 10:19:54 (UTC +3), and oldest from 05.10.2015 12:02:00 (UTC +3). The main part of the interface is a table listing files with columns for Name, Sharing link, Date created, Date modified, Share date, and Owner.

	Name	Sharing link	Date created	Date modified	Share date	Owner
📁	April_2018_Repo...	https://doc-0a-8...	No date is found	08.05.2018 10:...	No date is found	Anyone with link
📁	Football calendar...	https://docs.go...	No date is found	08.05.2018 08:...	10.10.2016 07:...	Anyone with link
📁	Getting started	https://doc-0a-8...	No date is found	05.10.2015 12:...	No date is found	Anyone with link
📁	Image - 002.jpg	https://doc-04-8...	No date is found	08.05.2018 10:...	No date is found	Anyone with link
📁	Image - 003.jpg	https://doc-14-8...	No date is found	08.05.2018 10:...	No date is found	Anyone with link
📁	Image - 007.jpg	https://doc-0a-8...	No date is found	08.05.2018 10:...	No date is found	Anyone with link
📁	IMG_ID2332138...	https://doc-0a-8...	No date is found	08.05.2018 10:...	No date is found	Anyone with link
📁	IMG_ID2445985...	https://doc-04-8...	No date is found	08.05.2018 10:...	No date is found	Anyone with link

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

6.4.4 Извлечение маркеров аутентификации Google

6.4.4.1 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.

6.4.4.2 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.	

6.4.4.3 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>
```

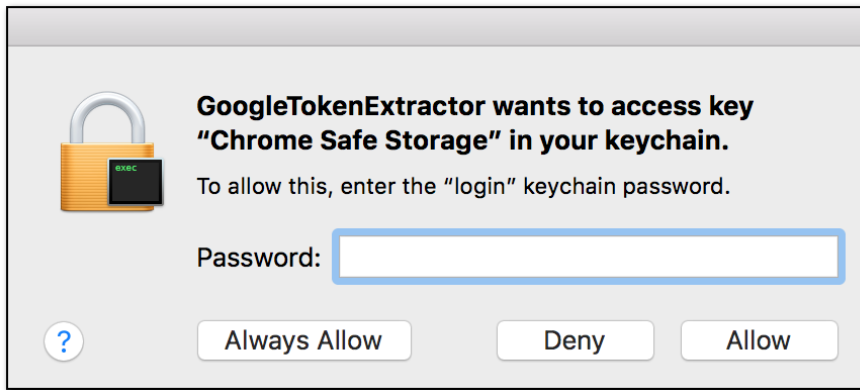
Пример: sudo GoogleTokenExtractor --get-token chrome --username user1 --password 1234

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.	

6.4.5 Плагины

6.4.5.1 Просмотр, поиск и анализ данных

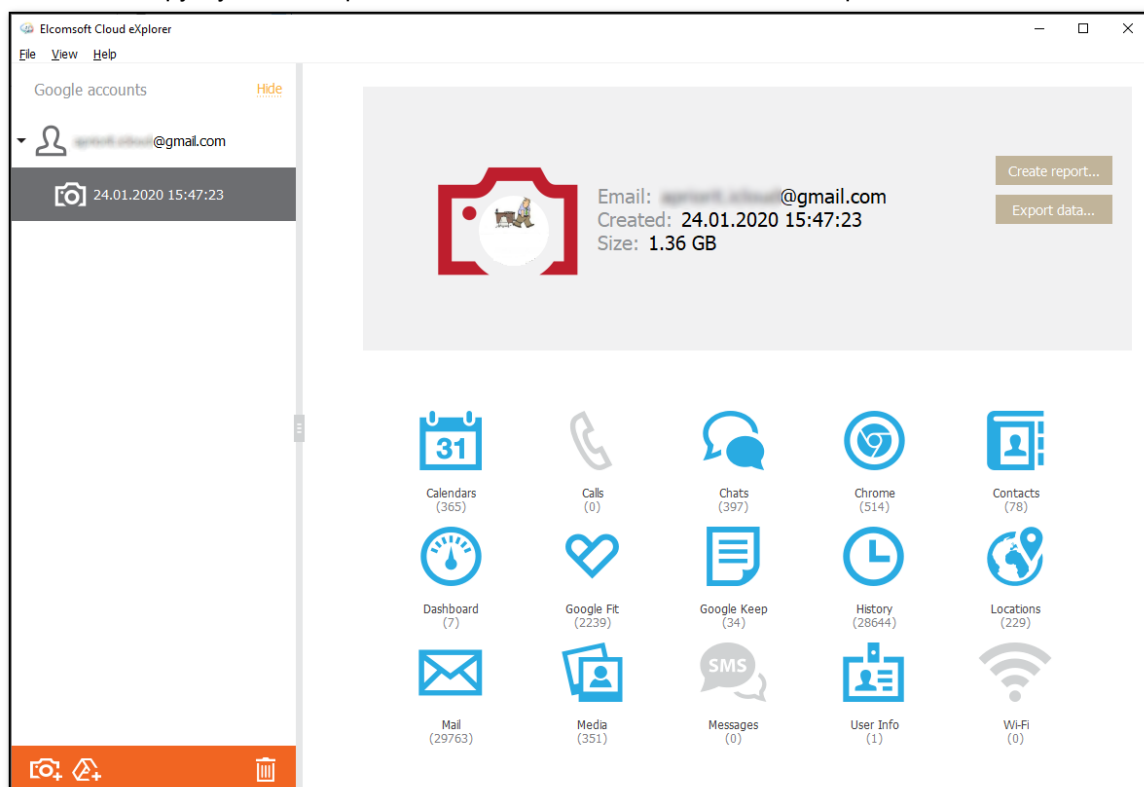
Скачанные в ЕСХ данные можно просматривать при помощи плагинов. Каждый плагин отвечает за собственную категорию данных. Для просмотра категории нажмите на соответствующую иконку в окне просмотра данных.

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**.

6.4.5.2 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/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.

6.4.5.3 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.

6.4.5.4 История местоположений - Locations

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.

6.4.5.5 Личный кабинет Google - Dashboard

Enter topic text here.

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

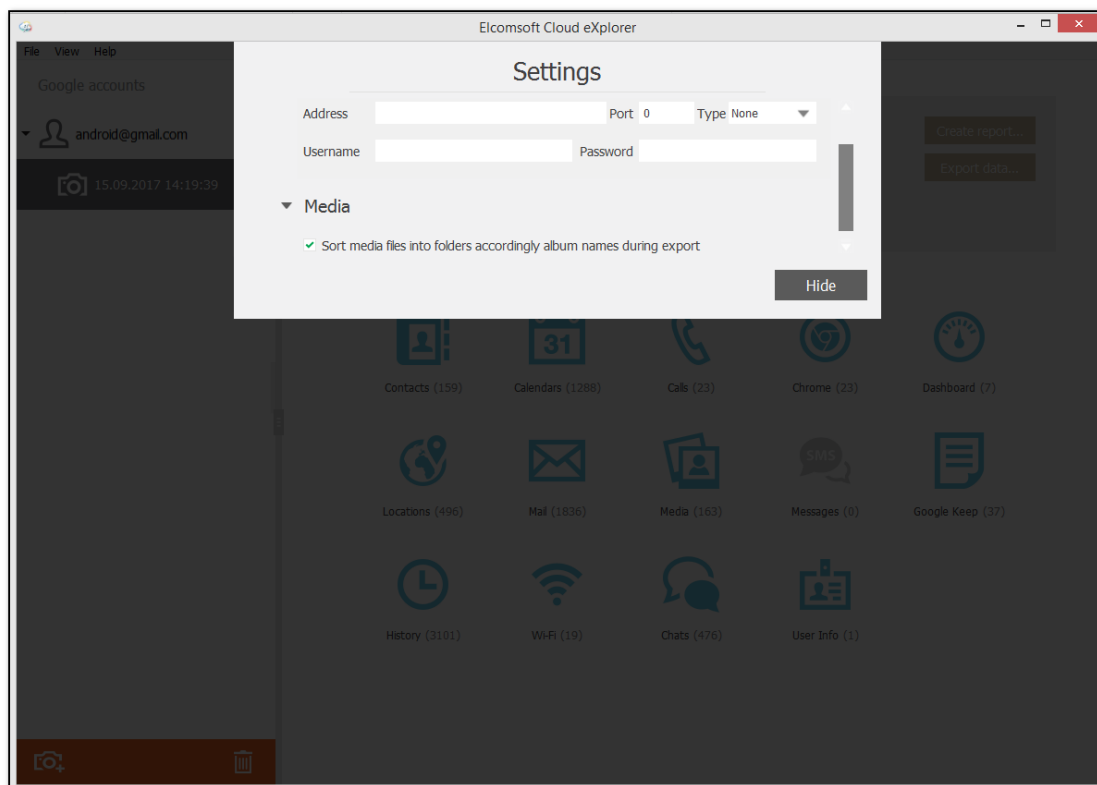
6.5 Elcomsoft eXplorer for WhatsApp

6.5.1 О программе

6.5.1.1 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.



6.5.1.2 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).

6.5.1.3 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).

6.5.1.4 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**.

6.5.2 Устройства Apple

6.5.2.1 Резервные копии WhatsApp

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>

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


6.5.2.2 Adding backups to EXWA

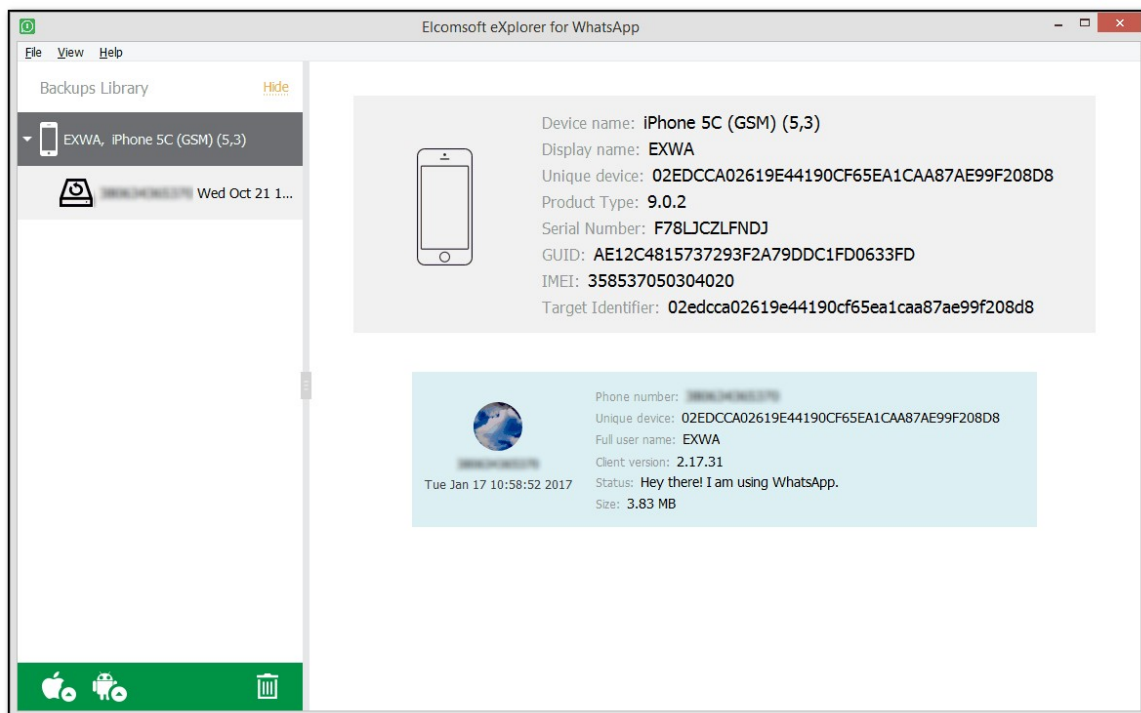
Локальные резервные копии

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.

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](#)^[341].

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 ).

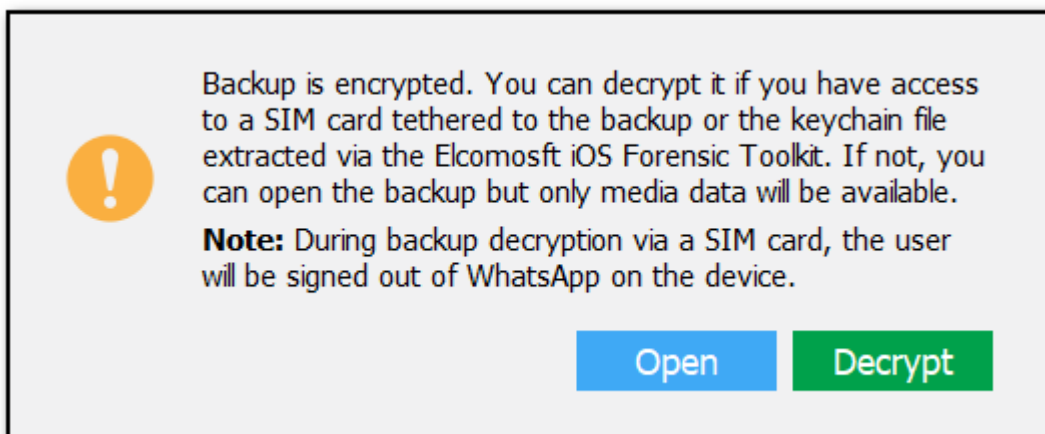
Подробная информация о том, как осуществляется авторизация в облако iCloud Drive, доступна в разделе [Скачивание файлов из iCloud](#)^[239].

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:

- **Открыть/Открыть** откроет резервную копию в состоянии "как есть", с доступом только к медиа-файлам (они хранятся в открытом виде).
- **Расшифровать/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.

Decrypt backup

Decrypt with **SMS** Keychain dump ?

Phone number

Verification code [Resend code](#) 00:01:04

Note: you will be logged out of WhatsApp on your device. To continue using WhatsApp on your device, you will have to sign in again after obtaining the key with the program.

Cancel **Decrypt**

- **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.

Decrypt backup

Decrypt with SMS **Keychain dump** ?

Path to dump **Browse...**

Cancel **Decrypt**

4. Нажмите **Дешифровать/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.

6.5.3 Устройства Android

6.5.3.1 Данные WhatsApp 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.xml` (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)**.

6.5.3.2 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**.

6.5.3.3 Загрузка данных WhatsApp из телефона Android

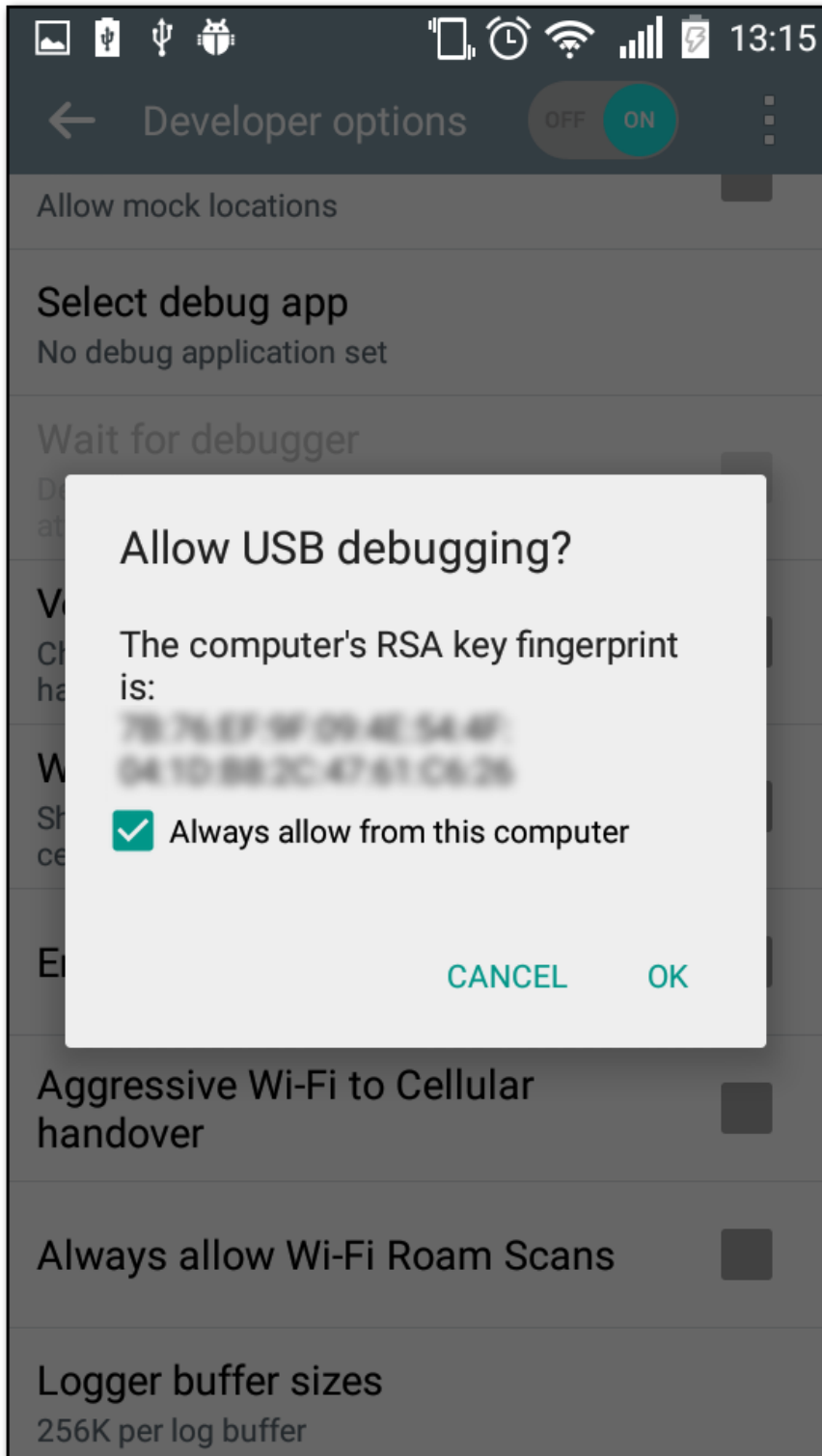
Подключите телефон к компьютеру и активируйте режим отладки (см. предыдущий раздел).

Выберите **Acquire data for Android device/Получить данные для Android** (иконка ,

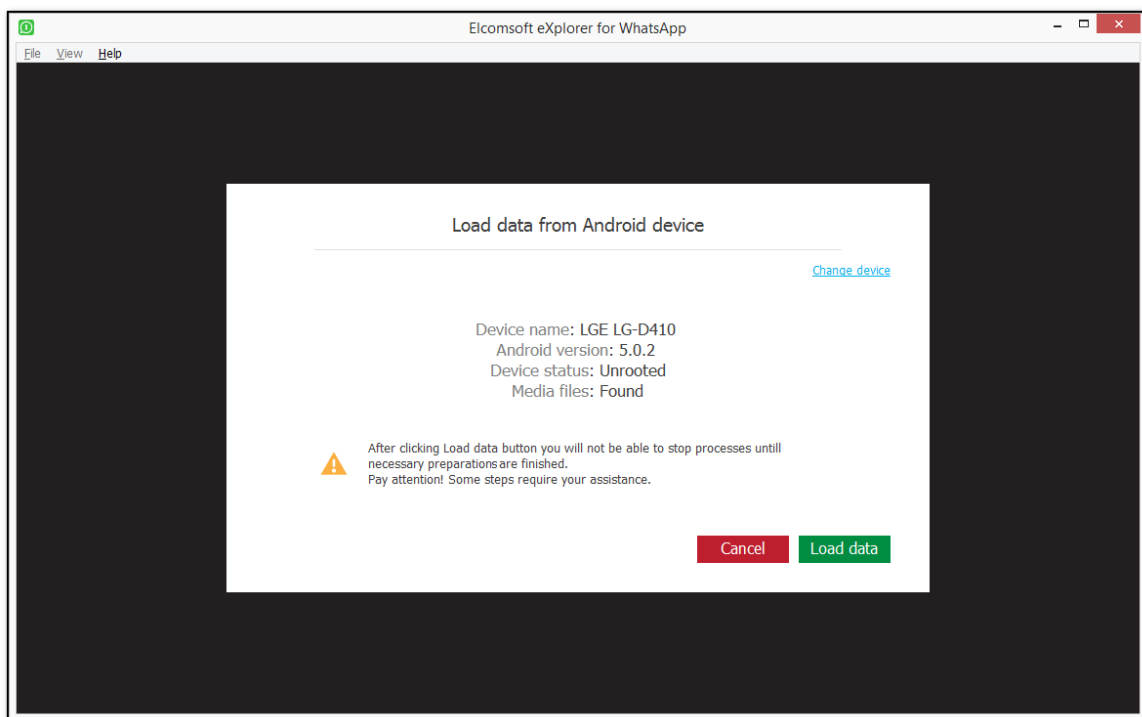
после чего нажмите **Load from device/Загрузить с устройства** .


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:



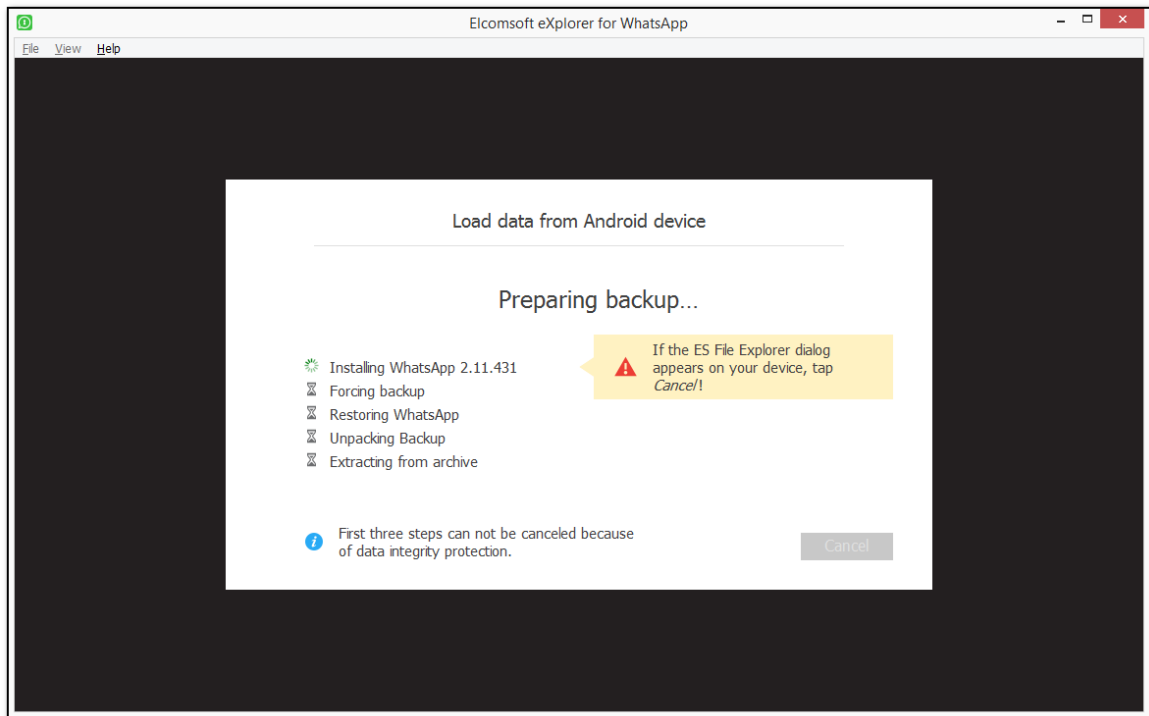
3. После подключения устройства будет выведена информация о нём:



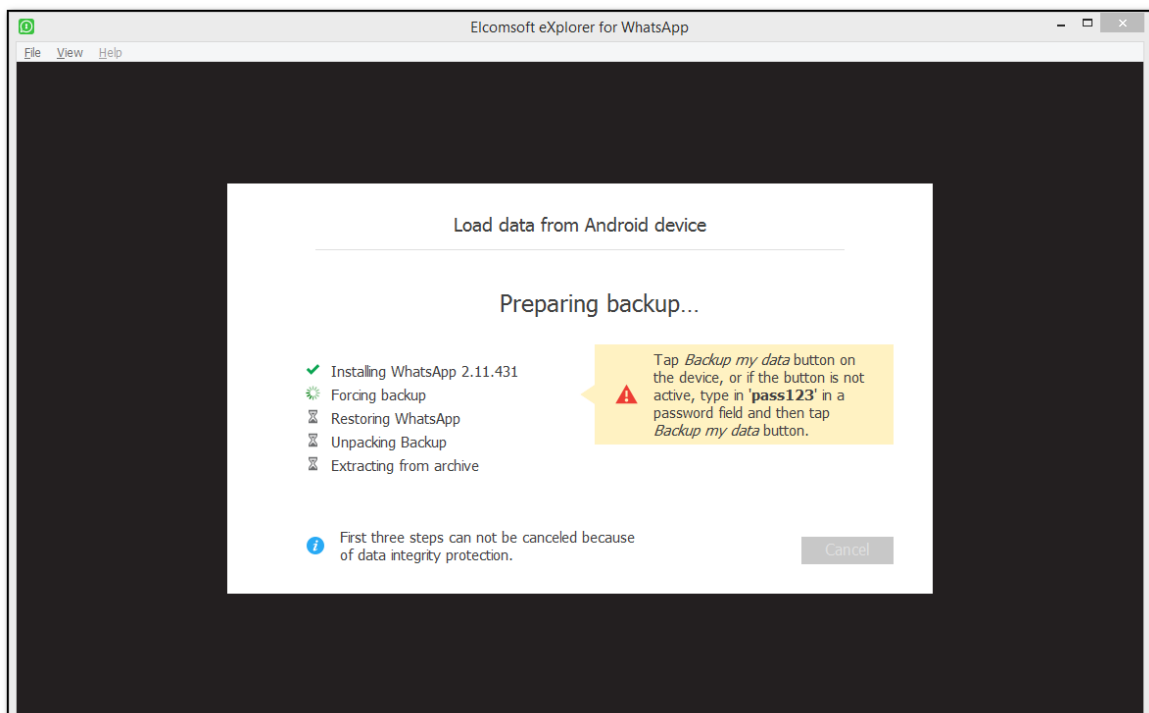
4. Если на устройстве установлены приложения WhatsApp и WhatsApp Business, щелкните значок  на кнопке **Load data/Загрузить** и выберите, какие данные вы хотите загрузить. Если вы выберете оба приложения, данные будут отображаться как отдельный снимок для каждого из них.
5. Нажмите **Load data/Загрузить**.
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 `adb` на устройстве. В этом случае нажмите **Check** и попробуйте загрузить данные еще раз.

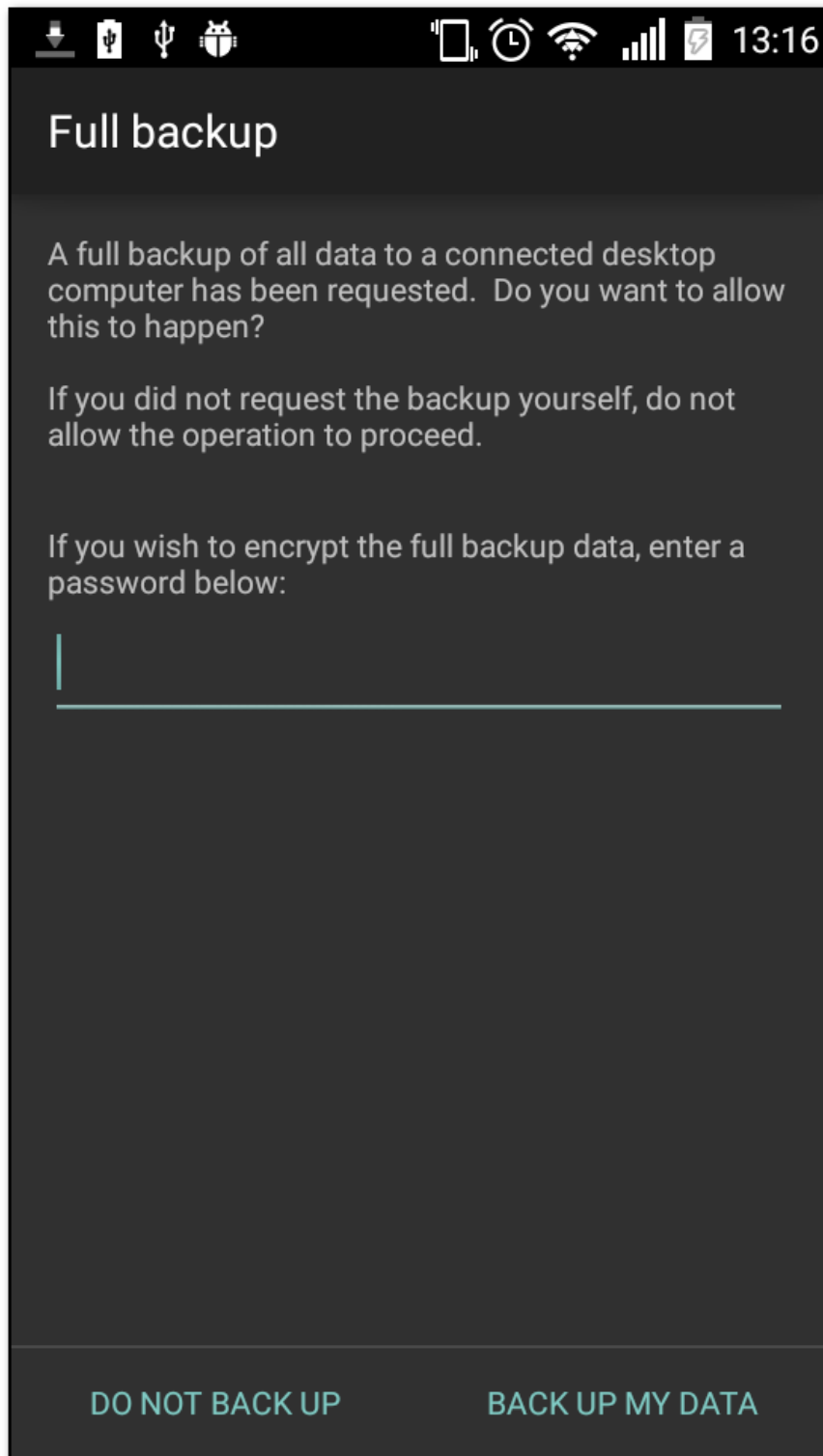
- **Установка WhatsApp.** Если на устройстве появится диалоговое окно ES File Explorer, коснитесь **Cancel/Отменить**.



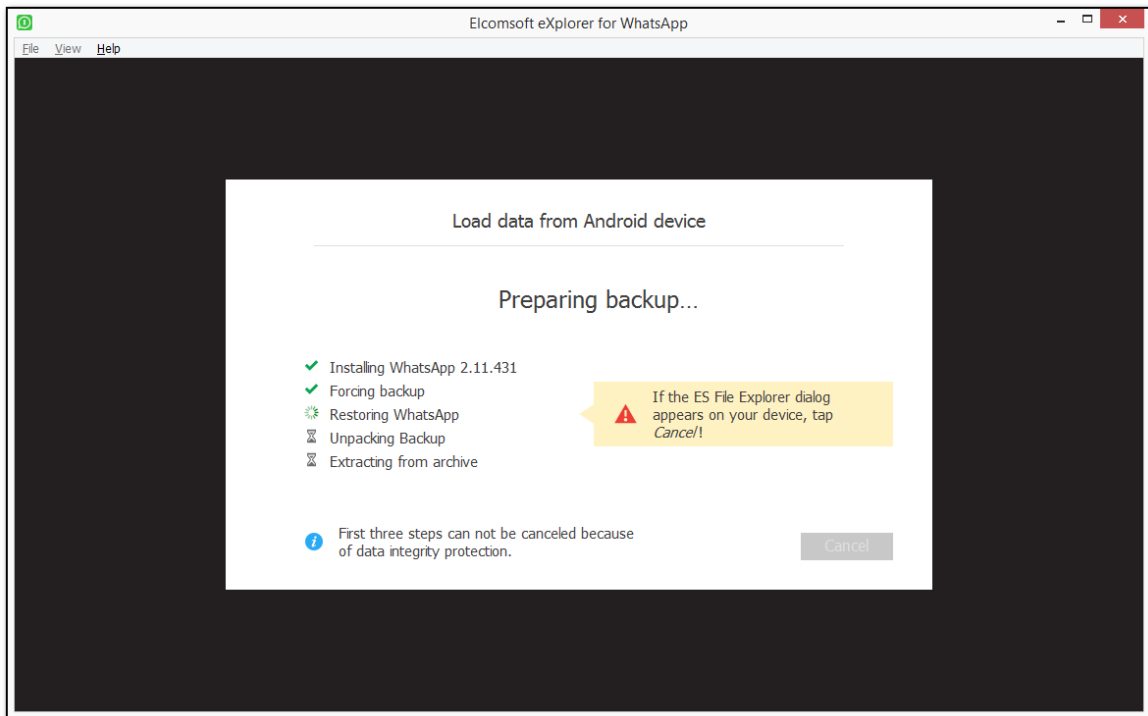
○ **Создание резервной копии.**



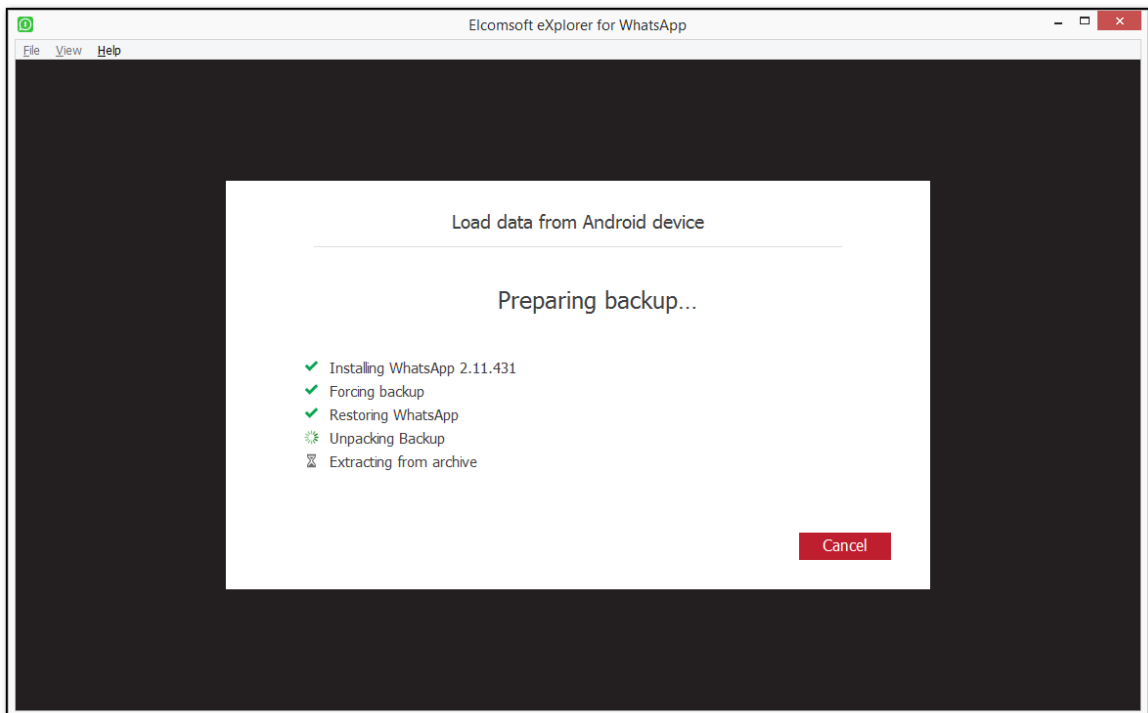
Коснитесь **Backup my data** на телефоне. Если кнопка не активна, введите **'pass123'** в качестве пароля, после чего коснитесь **Backup my data**.



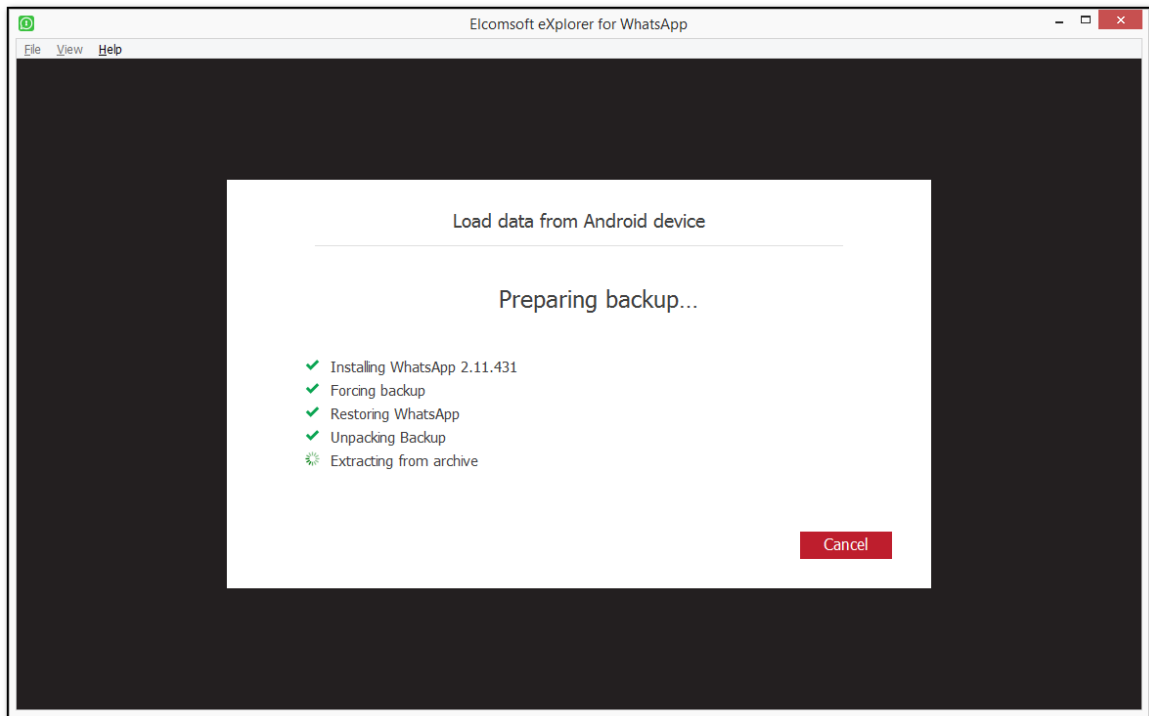
- **Восстановление WhatsApp.** Если на устройстве появится диалоговое окно ES File Explorer, коснитесь **Cancel/Отменить**.



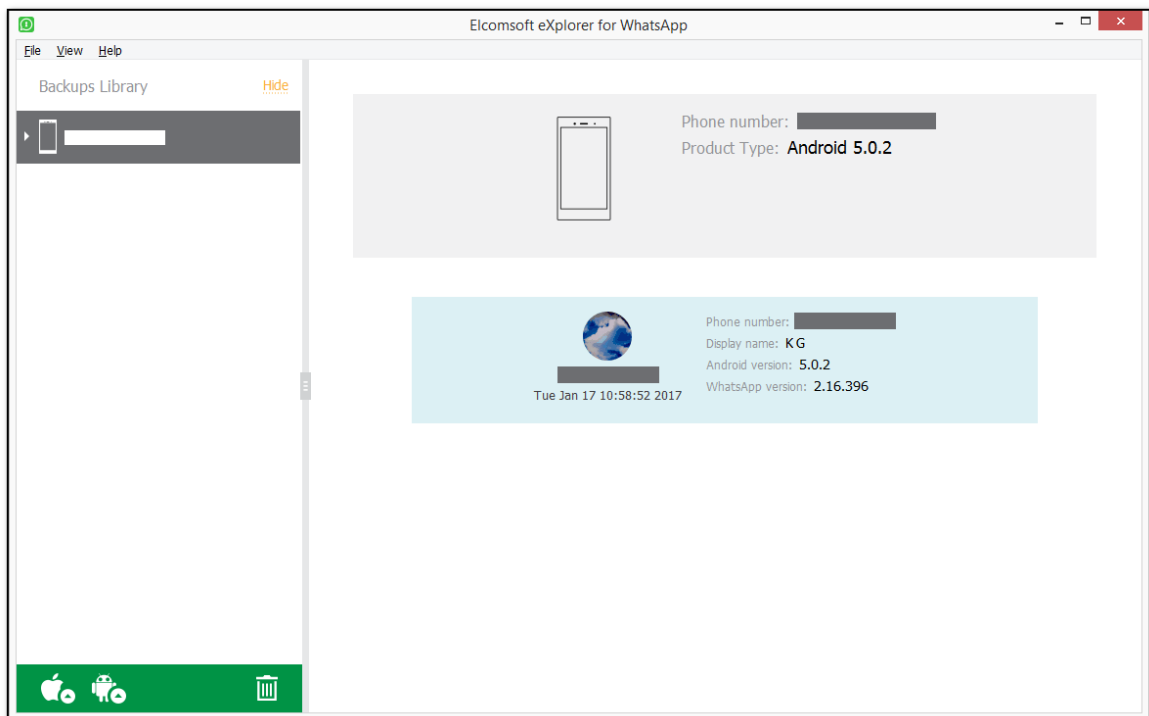
○ **Распаковка резервной копии.**



○ **Извлечение из архива.**





7. После загрузки резервной копии и обработки данных WhatsApp / WhatsApp Business отображается информация об устройстве.

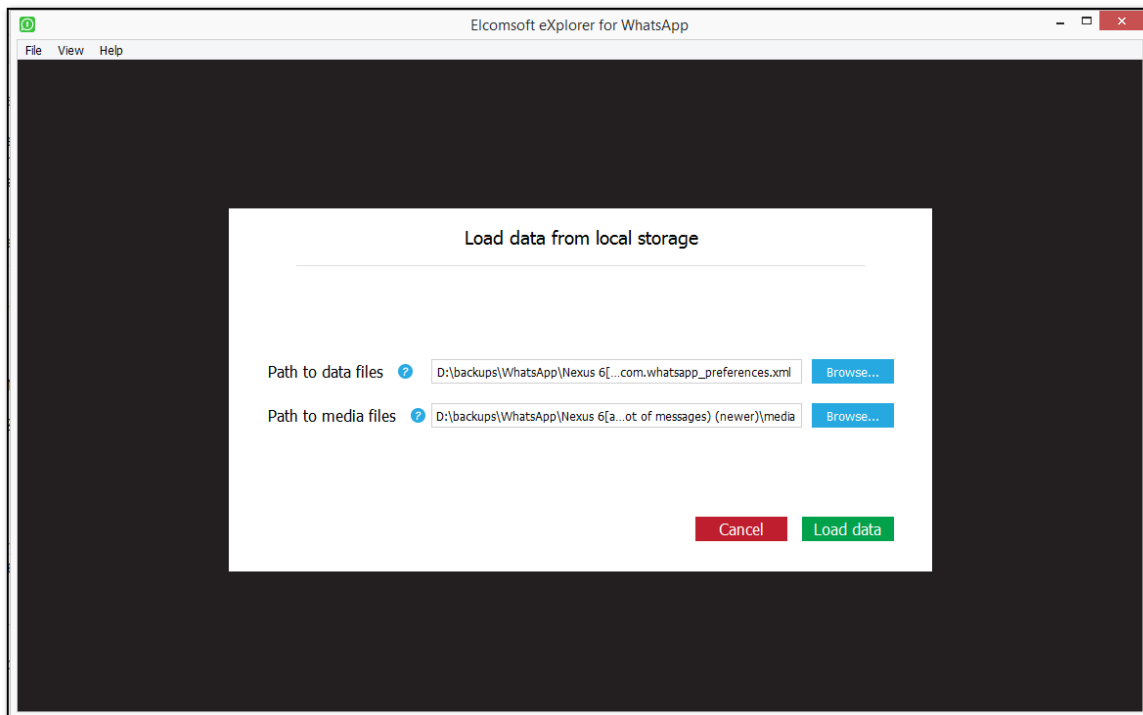


6.5.3.4 Работа с данными WhatsApp из локальной папки

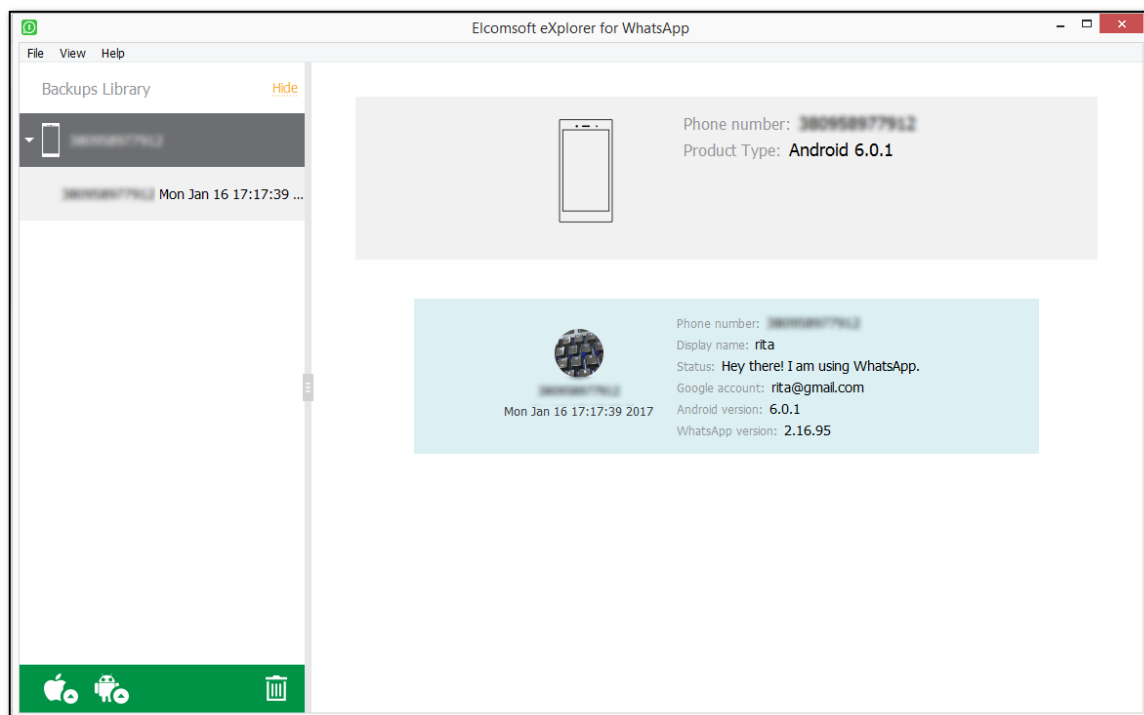
Загрузка данных WhatsApp из локальной папки

1. Нажмите **Acquire data for Android device/Получить данные 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**.



6.5.3.5 Загрузка данных WhatsApp из Google Drive

Для загрузки данных WhatsApp из Google Drive, нажмите **Acquire data for Android device/Получить данные 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](#)³²².

Download data from Google Drive

Google ID (example@example.com)

Password

Important: If the account uses 2FA and you log on with the password, a verification code will be requested on the next step. It will be sent by SMS immediately once you click Sign In. Google Authenticator or Backup verification codes can be also used.

Save credentials for future use ?

Use token instead of password (if available) ?

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**.

Download data from Google Drive

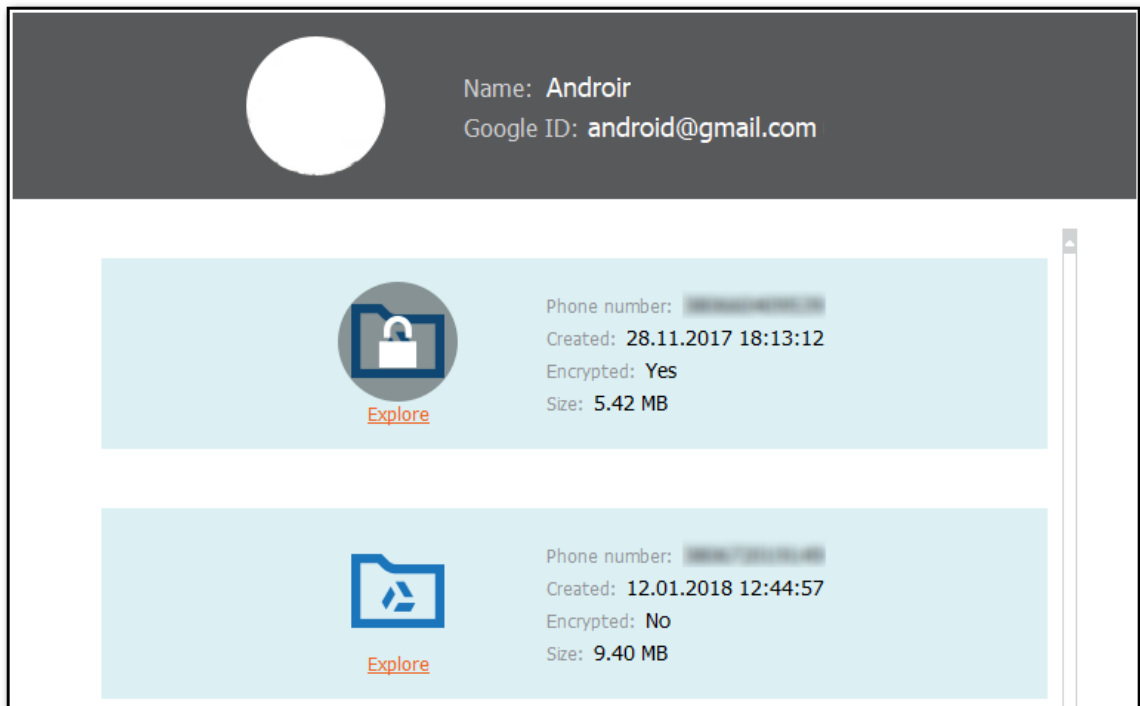
Androir — android@gmail.com

<input checked="" type="checkbox"/>	Phone number	Size	Date
<input checked="" type="checkbox"/>	XXXXXXXXXX	9.37 MB	12.01.2018 10:41:00
<input checked="" type="checkbox"/>	XXXXXXXXXX	5.42 MB	28.11.2017 16:12:39
<input checked="" type="checkbox"/>	XXXXXXXXXX	9.14 MB	23.10.2017 12:26:23
<input checked="" type="checkbox"/>	XXXXXXXXXX	2.84 MB	20.06.2017 13:03:28
<input checked="" type="checkbox"/>	XXXXXXXXXX	40.75 MB	16.08.2016 04:14:45
<input checked="" type="checkbox"/>	XXXXXXXXXX	3.68 MB	23.03.2016 10:35:46

Note: Due to Google's method of storing media in backups, all online backups share same media data as in the last backup.

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:



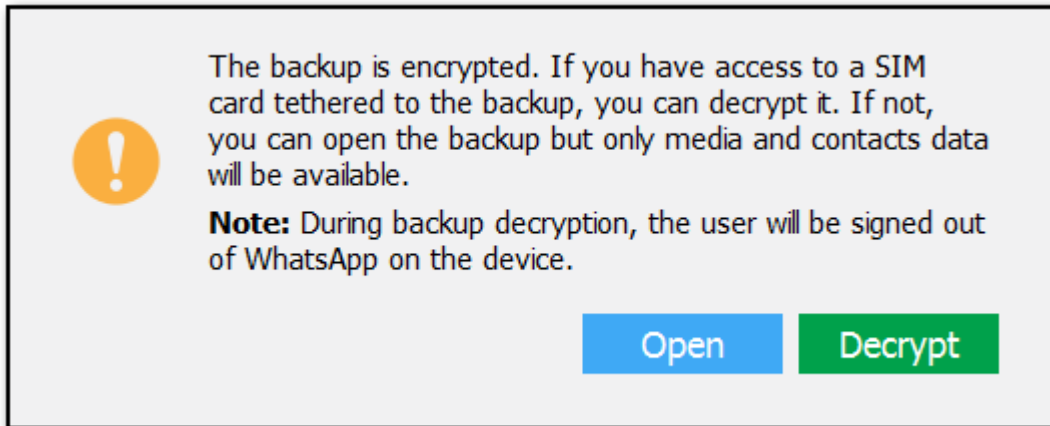
Зашифрованные резервные копии

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:

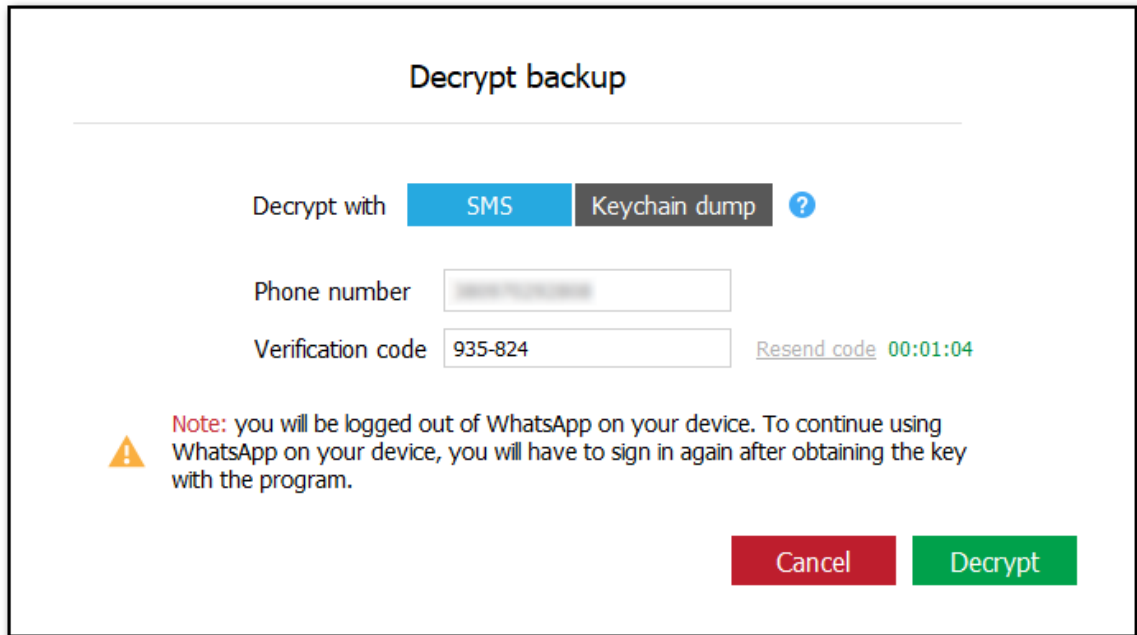
- **Open/Открыть** откроет резервную копию в состоянии "как есть", с доступом только к медиа-файлам (они хранятся в открытом виде).
- **Decrypt/Расшифровать** позволяет расшифровать резервную копию. Инструкции по расшифровке приводятся ниже.

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.

6.5.4 Плагины

6.5.4.1 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

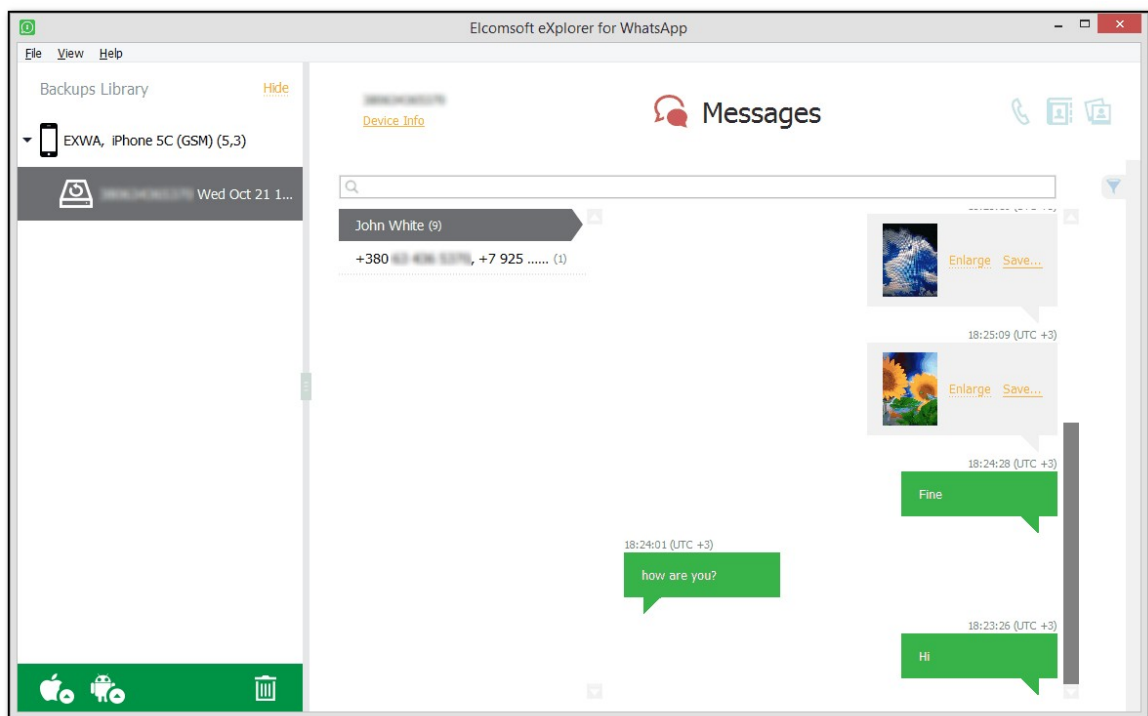
Все медиа-файлы, отправляемые в чатах WhatsApp, включая изображения, видео (начиная с WhatsApp 2.12.7) и аудиофайлы. Вы также можете просматривать медиафайлы, отправленные определенным контактом.

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 ярлычков, присвоенных пользователем. Наведите указатель мыши на значок ярлычка, чтобы увидеть его название.



6.6 Elcomsoft iOS Forensic Toolkit

6.6.1 Описание продукта

Elcomsoft iOS Forensic Toolkit – инструментарий для извлечения данных из мобильных устройств под управлением Apple iOS. Для 64-разрядных устройств (iPhone 5s и более новых моделей, iPad Mini 2+, iPad Air, iPad Pro) извлечение данных выполняется в виде снятия полного образа файловой системы (TAR) и дешифрования связки ключей, если доступен джейлбрейк или комбинация модели устройства и версии iOS поддерживается агентом сбора данных (**Приложение А. Поддерживаемые устройства**). Логическое извлечение данных доступно для всех моделей устройств и версий iOS с джейлбрейком или без него. Для устройств с действительным файлом блокировки (запись сопряжения iTunes) логическое извлечение данных возможно даже без пароля.

В версии для macOS (и только в ней) присутствует поддержка устройств iPhone 4, iPhone 5 и iPhone 5s. Для этих устройств поддерживается восстановление пароля блокировки и физическое извлечение данных (снятие и расшифровка образа раздела данных, расшифровка Связки ключей).

Наконец, версия для Мак также позволяет извлекать полную файловую систему и связку ключей из устройств, подверженных эксплойту checkm8. Пока это функционал находится в стадии бэта-тестирования, он описан в отдельном руководстве ([eiff_checkm8_ru.pdf](#)).

6.6.2 Системные требования

Для работы Elcomsoft iOS Forensic Toolkit требуется персональный компьютер под управлением Windows версий от 7 до 10, macOS версий от 10.13 (High Sierra) до 10.15 (Catalina) включительно. На компьютере должно быть установлено приложение Apple iTunes последней версии.

6.6.3 Использование продукта

В состав продукта входит электронный ключ с интерфейсом USB. Данный ключ должен быть установлен в USB порт компьютера в течение всего времени работы с продуктом.

Внимательно ознакомьтесь с информацией из этого документа перед началом работы. Во время работы рекомендуем обращать внимание на информацию, выводимую в окно приложения.

Для корректной работы необходимо запустить приложение **Elcomsoft iOS Forensic Toolkit** из меню Start (Windows) или папки Applications (macOS); несмотря на то, что приложение консольное (скрипт *Toolkit.cmd* для Windows или *Toolkit.command* для macOS), такой запуск необходим для корректной установки привилегий и папок по умолчанию для извлекаемых данных, поэтому не запускайте скрипты напрямую.

6.6.3.1 Совместимость

Технология физического извлечения данных позволяет извлекать большее количество информации в сравнении с альтернативными технологиями. В то же время, возможность использования данной технологии имеет ряд ограничений. Меры безопасности Apple заставляют использовать jailbreak для извлечения данных. Использование Secure Enclave в 64-разрядных устройствах (iPhone 5s и более новые) ещё сильнее ограничивает возможности физического извлечения: для установки jailbreak и работы приложения требуется код разблокировки устройства (для чего необходимо его предварительно ввести). Для определенных комбинаций устройства и версии iOS доступно извлечение данных с помощью агента без джейлбрейка. Полная информация о совместимости – в таблице **Appendix A. Supported devices**

6.6.3.2 Подготовительный этап

Перед началом работы ознакомьтесь с информацией о различиях в методах извлечения данных между устройствами и версиями iOS разных поколений. Для работы инструментария со многими устройствами необходима установка джейлбрейка. Альтернативное извлечение данных с помощью агента доступно для ограниченного круга устройств (подробности см. в таблице совместимости).

Внимание: Перед началом работы обязательно переведите устройство в режим полёта (Airplane mode) для предотвращения удалённой блокировки или стирания устройства; на компьютере, с которого происходит извлечение, интернет необходим только для установки *Агента*.

Подготовка к работе: Убедитесь, что устройство под управлением iOS полностью заряжено. Вам потребуется исправный кабель Lightning, инструментарий Elcomsoft iOS Forensic Toolkit и установленный в USB-порт электронный ключ от инструментария.

Обратите внимание:

- Для определенных устройств (*Приложение A. Поддерживаемые устройства*) доступно извлечение данных с помощью Агента, при этом установка джейлбрейка НЕ требуется. Для всех других устройств требуется джейлбрейк, как указано ниже.
- Если извлечение данных с помощью Агента недоступно для данной комбинации аппаратного обеспечения и версии iOS, необходимо установить джейлбрейк и OpenSSH или Dropbear SSH для работы с iPhone 5s и более новыми устройствами. Обратите внимание, что некоторые джейлбрейки уже включают SSH-клиент, однако во многих случаях (например, unc0ver джейлбрейк) **необходимо вручную включить SSH** в настройках джейлбрейка во время его установки.
- Физическое извлечение данных из 64-разрядных устройств Apple включает копирование файловой системы и связки ключей (keychain), а не копирование всего диска. Пароль на устройство не может быть восстановлен, поэтому работать можно только с тем устройством, для которого пароль не установлен или известен.

6.6.3.3 Основной экран

Elcomsoft iOS Forensic Toolkit использует окно командной строки: приложение Terminal (macOS) или cmd.exe (Windows). Для управления инструментарием используется текстовое меню.

Для начала работы с iOS Forensic Toolkit запустите приложение командной строки.

- o **Toolkit.cmd** (Windows) или **Toolkit.command** (macOS)

Данные файлы расположены в каталоге установки инструментария. Основной экран приложения выглядит следующим образом:

у вас есть доступ к файлу блокировки (lockdown) с не истёкшим сроком действия с компьютера пользователя.

Извлечение данных с использованием *Агента* поддерживается для ограниченного числа устройств. В настоящее время *Агент* может быть установлен на устройствах iOS, список которых приведён в **Приложении А**. Извлечение данных с помощью *Агента* похоже на извлечение данных с помощью джейлбрейка с полным извлечением файловой системы и расшифровкой связки ключей. Однако извлечение данных с использованием *Агента* является более безопасным, более надёжным и оставляет меньше следов по сравнению с установкой джейлбрейка.

Логическое извлечение данных

I DEVICE INFO	- Сохранить в файл доступную информацию об устройстве
R RECOVERY INFO	- Информация об устройстве в режиме DFU / Recovery.
B BACKUP	- Создать резервную копию устройства
M MEDIA	- Копировать медиа-файлы (фото и видео)
S SHARED	- Извлечь файлы приложений
L LOGS	- Копировать системный журнал crash logs

Physical acquisition

D DISABLE LOCK	- Отключить блокировку экрана (до первой перезагрузки)
K KEYCHAIN	- Извлечь и расшифровать связку ключей keychain
F FILE SYSTEM	- Создать образ файловой системы устройства в TAR

Агент (ограниченная совместимость)

1 INSTALL	- Установить агент
2 KEYCHAIN	- Расшифровать связку ключей
3 FILE SYSTEM	- Создать образ файловой системы устройства в TAR
4 FILE SYSTEM (USER)	- Скопировать пользовательский раздел (TAR)
5 UNINSTALL	- Удалить агента

Legacy devices acquisition

A LEGACY	- Восстановление кода блокировки экрана, физическое извлечение для iPhone 4, 5 и 5c
X EXT	- Выход из программы

Инструментарий сохраняет отчёт о всех выполняемых действиях в виде текстового журнала. Соответствующий файл создаётся в каталоге продукта каждый раз при его запуске. Название файла создаётся на основе текущего времени в формате UTC: **YYYYMMDD_hhmmssZlog**.

6.6.3.4 'I' – Информация об устройстве

Извлекает информацию об устройстве и сохраняет её в файл `ideviceinfo.plist` в формате XML.

macOS: файл сохраняется в домашнем каталоге пользователя (Finder | Go | Home).

Данная команда поддерживает все устройства под управлением iOS независимо от версии, наличия или отсутствия джейлбрейка, при разблокированном и заблокированном экране. Разблокированные устройства (в том числе при помощи lockdown-файла) и устройства с установленным джейлбрейком возвращают более подробную информацию.

Устройства iOS без джейлбрейка налагают жёсткие ограничения на то, что можно извлечь. Разблокировка устройства (при помощи пароля или с помощью Touch ID) или использование записи блокировки (запись о сопряжении) открывает доступ к более полной информации по сравнению с заблокированным устройством.

Инструмент сможет извлечь больше информации, если возможно разблокировать устройство iOS с помощью Touch ID или пароля; для устройств iOS 11+ вероятнее всего понадобится пароль. Кроме того, вы можете использовать записи сопряжения iTunes (файл «блокировки» устройства).

Внимание: срок действия записей блокировки может истечь в зависимости от версии iOS на устройстве. Версии iOS более ранние, чем iOS 11, по-видимому, не имеют установленного срока действия для файлов блокировки, в то время как в iOS 11/12/13 срок действия файлов блокировки истекает после некоторого периода бездействия, обычно 30 дней. Кроме того, даже действительные файлы блокировки не могут использоваться, если устройство не было разблокировано хотя бы один раз после перезагрузки. Изменение пароля **не** делает старую запись о сопряжении недействительной.

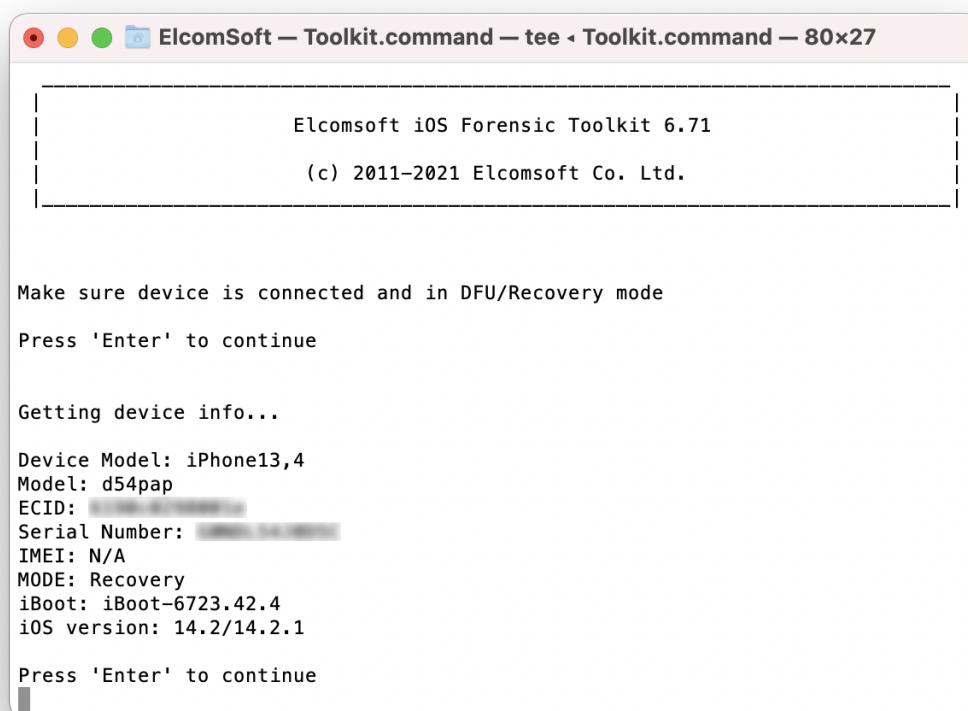
Команда «Информация» (“Info”) выдаст полезную информацию даже без записи блокировки, но полученный файл будет содержать ограниченный набор данных, включая имя устройства, модель, версию iOS, Mac-адрес адаптеров Wi-Fi и т. д.

Если предоставляется действительная запись блокировки с неистекшим сроком действия, доступно больше данных, включая номер телефона, Mac-адрес адаптера Bluetooth, ICCI / IMEI / IMSI, часовой пояс устройства, а также сведения об установке пароля резервного копирования iTunes, и включена ли опция резервного копирования в iCloud; дата / время создания последних резервных копий iTunes и iCloud; общее и свободное пространство на устройствах; информация о часовом поясе устройства и региональных настройках.

В случае, если устройство было разблокировано хотя бы один раз после последней перезагрузки (After First Unlock, AFU), можно будет получить резервную копию устройства, используя тот же файл блокировки (см. ниже). Кроме того, будет создана пара файлов (*applications.txt* и *applications.xml*). Файл *application.txt* содержит список всех приложений, установленных на устройствах, включая номера версий. Файл *applications.xml* включает в себя более подробную информацию о каждом приложении.

6.6.3.5 ‘R’ – Информация об устройстве в режиме восстановления или DFU

Команда «R» возвращает ограниченный набор данных об устройстве, находящемся в режиме DFU (обновление прошивки устройства) или режиме восстановления (Recovery). Подключите устройство и выберите «R»; отображается вся доступная информация, включая название модели, ECID, серийный номер, IMEI и UDID, а также версия загрузчика, и версия (или диапазон версий) iOS. Обратите внимание, что некоторые из этих данных могут быть недоступны в зависимости от модели устройства и режима:



```
Elcomsoft iOS Forensic Toolkit 6.71
(c) 2011-2021 Elcomsoft Co. Ltd.

Make sure device is connected and in DFU/Recovery mode
Press 'Enter' to continue

Getting device info...

Device Model: iPhone13,4
Model: d54pap
ECID: ██████████
Serial Number: ██████████
IMEI: N/A
MODE: Recovery
iBoot: iBoot-6723.42.4
iOS version: 14.2/14.2.1

Press 'Enter' to continue
```

6.6.3.6 Логическое извлечение данных

В iOS Forensic Toolkit предусмотрена возможность создания резервной копии данных устройства через механизм, аналогичный тому, что используется в iTunes. **Настоятельно рекомендуем** создавать резервные копии перед тем, как приступить к процедурам установки джейлбрейка и физического извлечения данных. Резервная копия может использоваться для логического извлечения данных.

‘В’ – Создание резервной копии

Для создания резервной копии требуется наличие Apple iTunes на компьютере или хотя бы «Apple Mobile Device Support» (драйвер из пакета iTunes). Если же пароль на резервную копию не установлен, инструментарий установит временный пароль «123» с целью расшифровки keychain. После завершения операции временный пароль будет автоматически сброшен.

Вы сможете создать резервную копию с любого устройства под управлением iOS при условии, что устройство было разблокировано хотя бы раз после включения или перезагрузки.

Внимание: после перезагрузки или выключения устройства обязательно разблокируйте его. При первом разблокировании устройства будет запущен сервис `com.apple.mobilebackup2`, который используется для создания резервных копий.

Для создания резервной копии используйте команду “B” на основном экране инструментария.

Внимание: для последующей расшифровки некоторых данных из резервных копий, защищённых паролем, программа установит временный пароль “123”. Вы сможете использовать этот пароль для расшифровки резервной копии, а также при просмотре данных с использованием Elcomsoft Phone Viewer. В случае, если пользователь установил собственный пароль на резервные копии, который неизвестен, вам потребуется подобрать оригинальный пароль при помощи Elcomsoft Phone Breaker.

Чтобы изменить пароль на резервное копирование, iOS 13 запрашивает пароль блокировки экрана устройства. Если у вас нет пароля блокировки экрана, при помощи которого можно получить данные, защищённые с помощью записи блокировки экрана, то резервное копирование может быть создано только «как есть», с паролем или без пароля, в соответствии с настройками устройства.

Анализ защищенных паролем резервных копий Apple позволяет получить доступ к элементам из связки ключей keychain. Резервные копии, созданные без пароля, по большей части не зашифрованы; однако связка ключей keychain зашифрована аппаратным ключом, поэтому данные связки ключей не будут доступны.

Если пароль на резервную копию уже установлен (и неизвестен), вы можете вернуться в главное меню, не создавая копию.

Прежде чем создать резервную копию, разблокируйте устройство с помощью кода блокировки экрана, отпечатка пальца или файла lockdown.

Важно: Начиная с iOS 8, получение резервной копии возможно только в том случае, если устройство iOS было разблокировано паролем хотя бы один раз после загрузки (After First Unlock, AFU). По этой причине, если вы обнаружите, что iPhone включен, хотя и заблокирован, **не выключайте его**. Вместо этого изолируйте его от беспроводных сетей, поместив его в сумку Фарадея, и не позволяйте ему выключаться или полностью разряжаться, подключая его к зарядному устройству (подойдёт переносной блок питания в сумке Фарадея, пока вы не перенесёте устройство в лабораторию). Это даст вам время для поиска на компьютерах пользователя записи о блокировке (lockdown).

Если невозможно разблокировать устройство кодом блокировки, по отпечатку пальца или Face ID, используйте файл lockdown, извлечённый из компьютера пользователя. Файл lockdown создаётся при подключении устройства iOS к компьютеру пользователя, если пользователь подтвердит доверенный статус компьютера (подтвердив диалоговое окно «Trust this computer» на разблокированном устройстве). Использование файлов lockdown автоматизирует процесс разблокирования устройства в последующих сессиях.

Необходимо извлечь правильную запись блокировки с компьютера пользователя, чтобы использовать её для логического извлечения данных с помощью Elcomsoft iOS Forensic Toolkit. Записи lockdown по умолчанию хранятся в следующих каталогах:

Windows Vista, Windows 7, 8, 10: %ProgramData%\Apple\Lockdown

Пример:

C:\ProgramData\Apple\Lockdown\6f3a363e89aaf8e8bd293ee839485730344edba1.plist

Windows XP: %AllUsersProfile%\Application Data\Apple\Lockdown

Пример:

C:\Documents and Settings\All Users\Application
Data\Apple\Lockdown\6f3a363e89aaf8e8bd293ee839485730344edba1.plist

macOS: /private/var/db/lockdown

Операционная система macOS Sierra (10.12) и более новые защищают доступ к депонированным ключам средствами системы. Для работы с ключами необходимо предоставить доступ к папке /var/db/lockdown для текущего пользователя, например:

```
sudo chmod 755 /private/var/db/lockdown
```

На macOS 10.15 (Catalina) папка lockdown дополнительно защищена, и даже у администратора нет к ней доступа. Однако вы можете временно отключить SIP (System Integrity Protection), либо извлечь нужные файлы из криминалистического образа диска.

Внимание: Депонированные ключи остаются действительными даже после изменения пароля; однако, начиная с iOS 8 все существующие депонированные ключи станут недействительными при сбросе настроек к заводским. В iOS 8 срок действия записей блокировки не истекает, если они явно не отменены пользователем. В iOS 11 установлены правила истечения срока действия записи блокировки; в iOS 9, если запись сопряжения не использовалась более шести месяцев, срок её действия истекает. Период действия записи сокращен до 30 дней в iOS 11 или более поздних версиях.

Дополнительная информация:

<https://support.apple.com/en-us/HT203887>

Резервные копии, создаваемые при помощи Elcomsoft iOS Forensic Toolkit, создаются в стандартном для iTunes формате. Их можно открыть во множестве криминалистических приложений, в том числе в программе Elcomsoft Phone Viewer.

Рекомендация: Вы можете переименовать файл lockdown, указав более короткое имя файла для удобства работы. Вам нужно будет ввести путь к этому файлу в программе iOS Forensic Toolkit.

‘М’ – Извлечение медиа-файлов (фото и видео)

Для извлечения медиа-файлов (фотографий и видео) необходимо выполнение тех же условий, что и для расшифровки резервных копий (устройство должно быть разблокировано либо должна быть доступна запись lockdown). В то же время, наличие или отсутствие пароля на резервные копии никак не влияет на возможность извлечения медиа-файлов.

В режиме «М» извлекаются фотографии и видеоролики, а также информация о редактировании файлов. В фотографиях, как правило, доступны теги EXIF, в которых содержится информация о местоположении устройства в момент фотографирования. Кроме того, могут извлекаться музыкальные файлы, которые были скачаны на устройство.

Для устройств, не имеющих установленных доверенных отношений с компьютером, потребуется использование lockdown-записи. По умолчанию файлы сохраняются в каталог

“AFC”, который будет создан в текущем каталоге (Windows) или домашней папке пользователя в macOS.

‘S’ – Файлы приложений

Извлечение файлов приложений работает схожим образом с извлечением медиа-файлов: устройство должно быть разблокировано либо должна быть доступна запись lockdown, наличие или отсутствие пароля на резервные копии не имеет значения.

Файлы приложений ([HT201301](#)) сохраняются в каталог “Shared”, который будет создан в текущем каталоге (Windows) или домашней папке пользователя в macOS. Пустые папки приложений не копируются.

В старых версиях iOS (до iOS 8.3) копируются данные всех приложений независимо от значения атрибутов доступности.

‘L’ – Журнал crash logs

Журналы crash logs и диагностики – важная часть информации, доступной в устройствах под управлением iOS. Файлы журналов не попадают в резервные копии, и могут быть извлечены только непосредственно из самого устройства. Для доступа к журналам crash logs используйте команду “L”: Copy crash logs.

С точки зрения эксперта, интерес представляют следующие данные:

- Список установленных приложений (PowerLog, Security, OnDemand)
- Имя пользователя в iTunes (itunesstored.2.log, значение не всегда определено)
- Название файлов вложений (журналы MobileMail)
- Список сетей Wi-Fi и история последних подключений (Wi-Fi logs)
- Список удалённых приложений (существует вероятность обнаружить журналы crash logs для приложений, которые не установлены в системе; это даёт возможность утверждать, что такое приложение было установлено и использовалось ранее, по крайней мере до момента последнего события из crash logs)

На основе журналов crash logs возможно построение ленты событий, основанных на дате и времени, извлечённых из журналов.

Несмотря на то, что в резервной копии iOS содержится значительно больший объём данных, информация из журналов crash logs (такая как удалённые приложения и журналы соединений с Wi-Fi) в резервные копии не попадает.

Журналы crash logs извлекаются из устройств, для которых установлены доверенные отношения с компьютером либо доступна запись lockdown. Для извлечения журналов необходимо, чтобы устройство было разблокировано кодом блокировки хотя бы единожды после включения или перезагрузки.

6.6.3.7 Физическое извлечение данных с помощью джейлбрейка: полная файловая система и извлечение связки ключей

Программа Elcomsoft iOS Forensic Toolkit обеспечивает возможность ограниченного физического извлечения данных из 64-разрядных устройств под управлением iOS.

ВАЖНО: В этом разделе рассматривается метод, требующий установки джейлбрейка. Если исследуемое устройство попадает в категорию устройств, поддерживаемых для извлечения данных с помощью Агента (**Приложение А. Поддерживаемые устройства**), мы настоятельно рекомендуем использование Агента.

Процесс извлечения данных из 64-разрядных устройств имеет ряд ограничений в сравнении с более старыми устройствами. Новый метод извлекает образ файловой системы, сохраняя содержимое устройства в единый архив TAR (tarball).

В лабораторных условиях скорости извлечения данных составляют около 15-20 МБ/с, используя метод «джейлбрейк». Метод «Агент» обеспечивает максимальную скорость, возможную на устройстве без дополнительной нагрузки (25+ МБ/с).

Дополнительная информация о работе с jailbreak в **Приложении В**. Для устранения неполадок, пожалуйста, прочитайте **Приложение С**.

Настройка устройства iOS

Обязательно выполните все следующие шаги для подготовки устройства iOS к физическому извлечению данных.

1. Убедитесь, что на устройство установлен джейлбрейк. Физическое извлечение данных из 64-битных устройств является возможным только для устройств iPhone, iPad и iPod с установленным джейлбрейком. Если джейлбрейк не установлен, перейдите к следующему разделу.
2. Если SSH-сервер не установлен, установите OpenSSH из [Cydia](#) или следуйте этим [инструкциям](#).
3. Разблокируйте устройство, указав правильный пароль.
4. Переключите устройство в «Авиарежим» и отключите все подключения к интернету (беспроводному и проводному) на рабочем столе.

Для устройств с установленным джейлбрейком *checkra1n* возможно частичное извлечение файловой системы.

Установка джейлбрейка

Физическое извлечение данных из более новых устройств iOS (iPhone 5S и всех более новых 64-разрядных моделей вплоть до iPhone Xr / Xs) возможно, только если на них установлен джейлбрейк. Поскольку количество iOS-устройств с уже установленным джейлбрейком крайне мало, в большинстве случаев придется устанавливать джейлбрейк в лаборатории.

Важно: для джейлбрейка устройств под управлением iOS 8+ и новее потребуется предоставить правильный пароль на устройство (для всех, кроме джейлбрейка *checkra1n*). Кроме того, возможно потребуется создать новую учётную запись Apple ID, чтобы подписать IPA для джейлбрейка и загрузить его на устройство. Некоторые джейлбрейки требуют отключения Find My Phone, в то время как другие джейлбрейки работают, даже если Find My Phone активен. Рекомендуется использовать сертификат разработчика (чтобы избежать верификации сертификата, которая требует активного подключения к интернету).

Установка джейлбрейка сильно зависит от версии iOS на устройстве. В целом, большинство устройств Apple используют текущую версию iOS. Джейлбрейк может быть недоступен для

самой последней версии iOS, и в этом случае возможности извлечения данных будут сильно ограничены.

Elcomsoft iOS Forensic Toolkit поддерживает множество вариантов джейлбрейка, подробности см. в **Приложении В**.

Установка джейлбрейка на устройство с ОС iOS 8 и новее - это трудоёмкий процесс без гарантированного результата. В зависимости от версии iOS может потребоваться выполнение дополнительных шагов. Установка и устранение неполадок джейлбрейка не является частью этого руководства.

Чтобы сделать джейлбрейк устройства iOS, необходимо отключить несколько уровней защиты. Для этого вероятно потребуется указать правильный пароль к Apple ID и ввести правильный пароль на устройство (если включен один или оба уровня защиты).

Обратите внимание, что некоторые джейлбрейки для iOS 9+ являются полупривязанными (или полутвязанными). Если устройство будет перезагружено, придется снова запустить джейлбрейк на устройстве iOS. Процесс установки джейлбрейка отличается от одного к другому; обратитесь к документации для получения более подробной информации.

Извлечение данных

1. Запустите iOS Forensic Toolkit. Возможно, вам предварительно понадобится изменить пароль для root и/или номер ssh-порта для соединения; см. Приложение С.
2. Разблокируйте устройство кодом блокировки и выполните в программе iOS Forensic Toolkit команду «**D**» **DISABLE LOCK**. В результате автоматическая блокировка устройства будет отключена. Это необходимо для корректного извлечения данных, поскольку устройство должно оставаться разблокированным в течение всего времени работы iOS Forensic Toolkit.
3. Выполните команду «**F**» **FILE SYSTEM** из основного меню приложения. Данная функция извлекает образ файловой системы устройства (файлы и структуру каталогов) с данными приложений в виде архива в формате TAR. База данных связки ключей также будет извлечена; однако она не будет расшифрована, так как ключи дешифрования связки ключей недоступны на 64-битных устройствах.
4. Укажите имя файла для архива, в который будут сохранены данные.
5. Дождитесь окончания процесса. Это может занять некоторое время, особенно при извлечении информации из устройств с большим объемом данных (до нескольких часов).
6. После окончания процесса отключите устройство от компьютера и переходите к анализу данных.

По умолчанию архив tarball сохраняется в файл с именем {UDID}_timestamp.rar.

Установка OpenSSH

Для физического извлечения данных необходим OpenSSH, если джейлбрейк не поставляется с собственным SSH сервером. Некоторые утилиты jailbreak поставляются со встроенным SSH сервером Dropbear, работающим обычно на портах 22.

Если в состав jailbreak сервер SSH не входит, то для дальнейшей работы потребуется установить приложение OpenSSH на исследуемое устройство. Приложение OpenSSH доступно из депозитария Cydia <https://cydia.saurik.com/openssh.html>, также есть возможность

непосредственной установки: <http://www.cydiaos.com/install-openssh-on-iphone-ipod-without-cydia/>

Установка запрета блокировки экрана

Для успешного извлечения данных экран исследуемого устройства должен быть разблокирован в течение всего времени работы программы. Иногда экран устройства можно разблокировать путем ручной настройки параметра «блокировать после», выбрав опцию «никогда», однако известно, что некоторые политики безопасности отключают параметр «никогда». Для того, чтобы запретить автоматическую блокировку экрана исследуемого устройства, в программе Elcomsoft iOS Forensic Toolkit существует команда «D» **DISABLE LOCK**. В результате автоматическая блокировка устройства будет отключена до первой перезагрузки.

Для функции отключения блокировки экрана используется компактная утилита, которая автоматически устанавливается на устройство, запускается, обрабатывает и автоматически удаляется с устройства. В редких случаях автоматическое удаление с устройства может не сработать.

Внимание: если iPhone/iPad находится в режиме Low Power Mode, отключение блокировки экрана не сработает. В таком случае необходимо вручную отключить Low Power Mode на устройстве, перейдя в Settings > Battery и переключив соответствующую настройку.

Внимание: этот шаг НЕ нужен, если выполняется извлечение данных в режиме BFU (Before First Unlock), когда пароль неизвестен.

Расшифровка связки ключей keychain

В защищённом хранилище keychain система хранит наиболее важные данные устройств iPhone, iPod Touch и iPad. С каждой новой версией iOS в keychain переносится всё больше информации. Данные из keychain хранятся на зашифрованном дисковом разделе, и дополнительно зашифрованы с помощью аппаратного ключа. В зависимости от версии iOS в keychain могут храниться пароли и маркеры аутентификации от учётных записей пользователя, пароли от электронной почты, от Wi-Fi, финансовая информация, документы и т.п.

Расшифровка keychain происходит моментально. Для расшифровки keychain используйте команду «K» Keychain на основном экране программы Elcomsoft iOS Forensic Toolkit. Эта функция также работает с установленным джейлбрейком *checkra1n*, когда пароль неизвестен, хотя при этом будет извлечено только очень ограниченное количество записей связки ключей.

Keychain сохраняется в файл *keychain_{UDID}_timestamp.xml* в текущем каталоге (Windows) или домашнем каталоге пользователя (macOS). Для просмотра рекомендуется использовать [Elcomsoft Phone Breaker](#).

Для извлечения keychain на компьютере должно быть установлено приложение iTunes. Также требуется наличие доверенных отношений устройства с компьютером либо наличие lockdown-файла.

Для извлечения и расшифровки keychain используется компактная утилита, которая автоматически устанавливается на устройство, запускается, получает и передаёт данные и автоматически с устройства удаляется. В редких случаях автоматическое удаление с устройства может не сработать.

Важно: для успешного извлечения данных связки ключей `keychain` экран устройства должен быть разблокирован в течение всего времени работы. В процессе извлечения данных может возникнуть необходимость разблокировать устройство. Инструмент извлечения связки ключей `keychain` пытается обнаружить подобные запросы и приостанавливает процесс до тех пор, пока устройство не будет разблокировано. Иногда запрос на разблокировку может быть не обнаружен, в этом случае просто разблокируйте устройство (с помощью пароля или Touch ID / Face ID) и продолжайте.

Извлечение образа файловой системы

Внимание: перед началом работы переключите устройство в авиарежим (Airplane mode). Если в пределах досягаемости есть другие устройства под управлением iOS, рекомендуем деактивировать на них подключение к Wi-Fi.

Данный вид извлечения данных позволяет сохранить образ файловой системы устройства в формате UNIX tarball (архив TAR). В отличие от побитового копирования дискового пространства, здесь извлекаются только файлы и структура каталогов.

Необходимо задать имя файла для сохранения образа файловой системы; по умолчанию это `{UDID}_timestamp.tar`. Если вы не укажете полный путь, файл будет сохранен в текущем каталоге (Windows) или в домашнем каталоге текущего пользователя (macOS).

Внимание: максимальный размер файла, поддерживаемый файловой системой FAT32, составляет 4 ГБ. Система FAT32 часто используется для форматирования накопителей USB, карт памяти и внешних дисков. Размер архива, извлекаемого из устройства iOS, может существенно превышать максимальный размер файла на FAT32. Перед началом работы убедитесь, что используемый накопитель отформатирован в exFAT, NTFS, APFS или HFS+.

После указания имени файла начинается процесс создания образа. Извлечение данных может занять длительное время в зависимости от модели устройства и объема пользовательских данных. Во время работы выводится информация о прогрессе.

Если извлечение данных выполняется в режиме BFU (Before First Unlock) с помощью джейлбрейка `checkra1n` на устройстве с неизвестным паролем, извлекается только ограниченный объем данных.

Расшифровка связки ключей

Elcomsoft iOS Forensic Toolkit позволяет извлекать и дешифровать связку ключей `keychain`, извлекая все записи, включая записи с атрибутом «только для этого устройства». Используйте команду «**К**» `Keychain`, чтобы извлечь и расшифровать записи связки ключей.

Обратите внимание, что для извлечения записей связки ключей необходимо ввести пароль на устройство (биометрическая аутентификация с использованием Touch ID или Face ID также может использоваться).

6.6.3.8 Извлечения данных с помощью Агента

Elcomsoft iOS Forensic Toolkit позволяет полностью извлекать файловую систему и дешифровать связку ключей на ограниченном ряде устройств Apple, перечисленных в Приложении А. Поддерживаемые устройства.

ВАЖНО: В этом разделе рассматривается извлечение данных с помощью Агента без джейлбрейка, доступное для ограниченного ряда устройств без джейлбрейка. Данный метод наиболее оптимален для этих устройств, поскольку получение данных с помощью Агента является более безопасным и более надёжным методом сбора данных.

Процесс извлечения данных с помощью Агента отличается от методов на основе джейлбрейка тем, что он не требует установки стороннего джейлбрейка. Недостатком этого метода является ограниченный диапазон поддерживаемых устройств (**Приложение А. Поддерживаемые устройства**) и необходимость использовать Apple ID, зарегистрированный в программе Apple Developer Program, для подписи агента.

В тестовых лабораторных условиях скорость записи данных превышает 1 ГБ / мин. Скорость получения данных может быть значительно выше и зависеть только от типа устройства iOS.

Общая информация и требования

Сбор данных с помощью агента в целом аналогичен сбору данных с помощью джейлбрейка с разницей в том, что для агента джейлбрейк не требуется. Для получения информации о совместимости смотрите **Приложение А. Поддерживаемые устройства**. Этот метод практически не вносит изменений в устройство, и в отличие от джейлбрейка, совершенно безопасен в использовании.

Для использования этого метода, необходимо установить специальный Агент на устройство. Агент - это небольшое приложение, которое получает привилегии root, считывает всю файловую систему, получает и дешифрует связку ключей и отправляет выходные данные на компьютер эксперта, где запущен iOS Forensic Toolkit.

Для установки Агента под Windows, необходимо иметь платную учетную запись разработчика Apple (зарегистрироваться можно [здесь](#)). В Apple ID, подключенном к этой учетной записи, должна быть включена двухфакторная аутентификация. Кроме того, необходимо установить пароль для конкретного приложения (app-specific password) в своей учетной записи Apple и использовать этот пароль для конкретного приложения вместо обычного пароля Apple ID во время установки Агента.

На системах под управлением macOS можно использовать как учётные записи разработчика, так и обычные. При этом в качестве пароля при использовании двухфакторной аутентификации всегда надо вводить обычный (а не специфичный для приложения) пароль, и проходить вторичную аутентификацию путём ввода кода, который будет послан на доверенное устройство.

Важно: В учетную запись разработчика можно добавить до 100 устройств любого типа (например, 100 iPhone и 100 iPad). Для обычных учётных записей агент может быть установлен только на 3 устройства для каждой из них, но вы можете использовать временные (вновь созданные) Apple ID.

Агент не использует SSH, поскольку использует собственный протокол связи с меньшими издержками и большей надежностью.

Установка

Команда «1» (Установить агент) устанавливает Агент на исследуемое устройство. Необходимо ввести учётные данные (Apple ID и пароль; на Windows – тот, который был установлен для приложения, на macOS – «обычный», а затем пройти двухфакторную аутентификацию с использованием доверенного устройства).

После установки, если вы использовали учётную запись разработчика, запустите Агент на исследуемом устройстве iOS и продолжите работу на рабочем компьютере. При использовании обычной учётной записи вам понадобится пройти дополнительный шаг: разрешить (на устройстве) возможность запуска агента путём подтверждения сертификата в настройках. Для этого нужно временно пустить устройство в интернет, но чтобы оно не начало синхронизироваться (и тем более, чтобы не сработало удалённая блокировка), необходимо настроить соединение так, чтобы был доступ только к серверу `ppq.apple.com` (порт 443) и ничему более.

Извлечение данных

Шаги извлечения данных в основном такие же, как для устройств с джейлбрейком, за исключением того, что нет необходимости использовать команду «D» (Отключить блокировку). Просто оставьте Агент (приложение iOS) работающим на переднем плане. Обратите внимание, что для извлечения данных с помощью Агента используются команды «2» и «3» вместо «K» и «F».

Удаление агента

Удалите приложение Агент с устройства после завершения извлечения данных. Используйте команду «5» (Удалить), чтобы удалить приложение. Это не обязательно, но оставляет меньше следов на исследуемом устройстве.

6.6.3.9 Поддержка устаревших устройств (iPhone 4, 5, 5c)

Выберите пункт 'A' для доступа к функционалу подбора кода блокировки и физического извлечения для iPhone 4, 5 и 5c (см. Приложение A для информации о совместимых устройствах). Требования:

- macOS (под Windows эта функция недоступна).
- Прямое соединение телефона с компьютером без использования USB хаба
- Если на Маке есть только порты USB-C, используйте адаптер-переходник с USB-C на USB-A и кабель USB-A – Lightning. Не используйте кабели USB-C – Lightning.
- Устройство должно быть заряжено как минимум до 20%.

Доступные варианты действий:

- [1] Put device in DFU mode (перевести телефон в режим DFU)
- [2] Exploit device (произвести эксплойт)
- [3] Recover passcode (взломать пароль блокировки экрана)
- [4] Extract keychain (извлечь связку ключей)
- [5] Image user partition (снять образ раздела данных)

- [6] Decrypt image (расшифровать снятый образ раздела данных)
- [7] Reboot device (перезагрузить устройство для выхода из режима DFU)

Перевод в режим DFU и установка эксплойта

На первом шаге необходимо ввести устройство в режим DFU. Сделать это можно только вручную. Первая опция [1] поможет вам произвести нужные шаги. Существует несколько вариантов, но мы рекомендуем такую последовательность:

- Начальное состояние: телефон должен быть выключен и не подключен к компьютеру.
- Нажмите кнопку *Home* (единственную/центральную на лицевой панели), и удерживая её, подключите кабель Lightning. Отпустите *Home*, когда на экране устройства появится картинка «Подключитесь к iTunes».
- Одновременно нажмите *Home* и *Sleep/Power* (кнопка блокировки на верхнем торце устройства) и удерживайте их 8 секунд (на некоторое время на экране появится логотип Apple).
- Отпустите кнопку *Sleep/Power*, но продолжайте удерживать *Home* ещё 8 секунд

Если всё сделано правильно, экран аппарата останется чёрным, а в iTunes или Finder (в зависимости от используемой версии macOS) телефон появится как *iPhone in recovery mode* (режим восстановления). Всё готово к следующим шагам, которые уже автоматизированы.

Когда устройство находится в DFU-режиме, выберите вторую команду для эксплойта устройства путём загрузки в оперативную память специальной версии прошивки, использующей уязвимость. Процесс абсолютно безопасен, не затрагивает пользовательские данные и не оставляет следов на устройстве. Но в зависимости от ряда факторов (включая такие, как качество кабеля), эта операция не всегда бывает успешной. Просто повторите попытку. Вам понадобится сначала перезагрузить устройство в обычном режиме путём нажатия и удерживания обеих кнопок в течение примерно 8 секунд, после чего пройдите все шаги заново, начиная с выключения устройства.

Восстановление кода блокировки экрана

Если операция эксплойта прошла успешно и смонтирован пользовательский раздел (об этом будет выведено сообщение), можно приступить к взлому пароля. Выберите один из доступных вариантов (4 или 6 цифр). Атака для iPhone 5 или 5s займёт максимум 12 минут или 21 час соответственно, обычно существенно быстрее. На iPhone 4 атака работает в 2.5 раза медленнее. Перебор алфавитно-цифровых паролей произвольной длины рекомендуется проводить с использованием словаря. Словарь, составленный из 100,000 часто используемых паролей, доступен в комплекте поставки.

Обратите внимание: часть информации будет доступна, даже если пароль восстановить не удалось.

После успешного нахождения пароля перезагрузите устройство в обычном режиме путём выбора последней команды.

- [1] Recover 4-digit passcode – восстановление паролей из 4 цифр
- [2] Recover 6-digit passcode – восстановление паролей из 6 цифр
- [3] Perform a wordlist attack – восстановление паролей произвольной длины
- [4] Set custom passcode recovery parameters – атака с собственными настройками

Вы можете проверить тип кода блокировки, загрузив устройство в обычном режиме. Тип пароля отображается на экране устройства. Важно выбрать правильный вариант, чтобы исключить проверку комбинаций, которые не могли быть использованы.

С помощью словарной атаки вы можете попробовать восстановить более длинные и сложные коды блокировки. Словари используются в текстовом формате, по одному слову в строке. В поставку продукта входит словарь из 100,000 часто употребляемых паролей. Наконец, вы можете самостоятельно параметры атаки, выбрав команду [4]. В этом режиме вы сможете указать длину пароля и набор символов, которые может содержать код блокировки.

Извлечение связки ключей

Этот шаг [4] является обязательным независимо от того, установлен ли код блокировки и известен ли он. Если код блокировки установлен, вам будет предложено его ввести. Отсутствие правильного пароля приведёт к двум важным последствиям:

- Большую часть записей из связки ключей (например, пароли от веб-сайтов) расшифровать не удастся.
- Не удастся расшифровать часть файлов на следующем шаге.

В результате работы команды будет создано два файла:

- {device ID}.keys
- {device ID}_keychain_timestamp.xml

Снятие и расшифровка образа диска

Создание образа диска (только раздела пользовательских данных) работает независимо от того, был ли установлен и известен ли код блокировки (при условии, что установка эксплойта прошла успешно). Большая часть файлов в устройстве зашифрована, поэтому, если код блокировки установлен и неизвестен, могут быть доступны только метаданные (структура папок, имена файлов, размеры и временные метки).

На первом шаге создайте образ диска «как есть» командой [5], а затем расшифруйте его командой [6]. На этапе дешифрования вам будет предложено указать файл с ключами, ранее извлечёнными командой [4]. В процессе расшифровки отобразится общее количество файлов, а также число незашифрованных файлов и таких зашифрованных файлов, которые могут быть расшифрованы с помощью предоставленных ключей. Последнее число зависит от двух факторов:

- Версия iOS
- Известен ли код блокировки

В iOS 4–7 большинство файлов можно расшифровать, даже если код блокировки неизвестен. В iOS 8–10 ситуация обратная, и большинство файлов можно расшифровать, только если вы укажете код блокировки устройства.

В процессе снятия образа диска будет создан следующий файл:

- {device ID}_user.dmg

После расшифровки создаются следующие файлы:

- {device ID}_decrypted_{timestamp}.dmg
- {device ID}_not_encrypted_{timestamp}.txt
- {device ID}_decryptable_{timestamp}.txt
- {device ID}_undecryptable_{timestamp}.txt

Первый файл — это расшифрованный образ диска; остальные три — это листинги файловой системы. «Незашифрованные» (not_encrypted) файлы копируются как есть; «дешифруемые» (decryptable) файлы расшифровываются с использованием ключей, полученных на предыдущем шаге; наконец, «нерасшифровываемые» (undecryptable) файлы — это файлы, которые невозможно расшифровать из-за отсутствия кода блокировки устройства (эти файлы будут пустыми, если код доступа не установлен или был указан).

6.6.3.10 Анализ данных

Для просмотра и анализа извлечённых методом физического анализа данных рекомендуем воспользоваться программой [Elcomsoft Phone Viewer](#) или другим инструментом, поддерживающим формат .tar, а для просмотра паролей из keychain — программой [Elcomsoft Phone Breaker](#). Также возможен ручной анализ файловой системы. Для анализа в ручном режиме потребуется распаковать или смонтировать образ раздела данных или файловой системы. Процесс рекомендуется проводить на компьютере под управлением UNIX или macOS.

6.6.4 Приложение А. Совместимые устройства

Инструментарий Elcomsoft iOS Forensic Toolkit поддерживает все 64-разрядные модели устройств под управлением iOS и ряд 32-разрядных. Физическое извлечение данных (файловая система) для этих моделей имеет ряд ограничений. Для получения файловой системы и связки ключей устройство должно быть с установленным джейлбрейком (или иметь возможность установки) либо поддерживаться Агентом извлечения (см. ниже); пароль должен быть известен. Вы должны иметь возможность разблокировать устройство и держать его разблокированным в течение всего процесса извлечения файловой системы.

Логический анализ (извлекаются резервные копии, медиафайлы, файлы приложений, журналы диагностики) поддерживается для всех моделей iPhone, iPad, iPod Touch, Apple TV и Apple Watch, для всех версий iOS. Для Apple TV и Apple Watch резервное копирование недоступно. Для Apple Watch (с 1-го по 5-е поколения) и Apple TV 4K требуется специальный адаптер.

Логический анализ — единственный метод, доступный для моделей, несовместимых с Агентом извлечения, для которых недоступен джейлбрейк.

Список совместимости для работы с Агентом

Агент-экстрактор является рекомендованным для современных устройств методом извлечения, и совместим со следующими комбинациями устройств и версий iOS:

- iPhone 5s, iPhone 6, iPhone 6s Plus, iPad Mini 2 и 3, iPad Air (1 поколения): **iOS 9-12.5.2**
- iPhone 6s до iPhone X, iPad 5 и 6 поколения, iPad Pro 1 и 2 поколения: **iOS/iPadOS 9.0 - 14.3**

- iPhone Xr, Xs, Xs Max, iPad Mini 5, iPad Air 3 поколения, iPad Pro 3 и 4 поколения, iPod Touch 7 поколения: **iOS/iPadOS 12.0 - 14.3**
- iPhone 11, 11 Pro, 11 Pro Max, iPhone SE (2020), iPhone 12, iPhone 12 Mini, iPhone 12 Pro, iPhone 12 Pro Max, iPad Air 4 поколения: **iOS 13.0 - 14.3**

Извлечение файловой системы и связки ключей с джейлбрейком

Устройство должно быть взломано (доступен джейлбрейк), код блокировки должен быть известен. Вы должны иметь возможность разблокировать устройство и оставить его разблокированным в течение всего процесса получения файловой системы. Поддерживаемые устройства:

- iPhone 5S, 6/Plus, 6S/Plus, 7/Plus, 8/Plus, iPhone X, iPhone Xr, iPhone Xs, iPhone Xs Max, iPhone 11, iPhone 11 Pro, iPhone 11 Pro Max, iPhone SE2 (2020)
- iPad Air, iPad Pro, iPad 6+, iPad Mini 2+
- Apple TV (от 2 поколения до версии 4K)

Этот метод зависит от наличия джейлбрейка (установка джейлбрейка должна быть выполнена до анализа), подробности см. в **Приложении В**.

При использовании *checkra1n* возможно частичное извлечение файловой системы и связки ключей в режиме BFU (Before First Unlock, до первой разблокировки) с неизвестным паролем, но с учётом ограничений *checkra1n*:

- Поддерживаются только некоторые комбинации аппаратных платформ и версий iOS

Взлом пароля блокировки экрана и физическое извлечение данных

Полное физическое извлечение (взлом кода блокировки, извлечение связки ключей, создание образа и расшифровка пользовательского раздела) доступно только в macOS.

Поддерживаемые версии iOS: от 6.0 до 10.3.4, поддерживаемые модели:

- iPhone 4 (iOS 4.0 - iOS 7.1.2)
 - iPhone3,1 (GSM): A1332
 - iPhone3,2 (GSM Rev. A): A1332
 - iPhone3,3 (CDMA): A1349
- iPhone 5 (iOS 6.0 - iOS 10.3.4)
 - iPhone5,1 (GSM): A1428
 - iPhone5,2 (GSM+CDMA): A1429, A1442
- iPhone 5c: (iOS 7.0 - iOS 10.3.3)
 - iPhone5,3 (GSM): A1456, A1532
 - iPhone5,4 (Global): A1507, A1516, A1526, A1529

Примечания:

- Физическое извлечение данных (извлечение файловой системы и дешифрование связки ключей) обычно возможно только для устройств с джейлбрейком и поэтому зависит от доступности джейлбрейка (установка джейлбрейка должна быть выполнена до процедуры извлечения данных)
- Некоторые устройства также поддерживают извлечение полной файловой системы и связки ключей keychain с использованием метода «Агента»

- Между двумя методами извлечения данных (джейлбрейк и агент) всегда выбирайте «агент», если версия iOS поддерживается
- Если джейлбрейк недоступен, а извлечение данных с помощью агента невозможно, возможно только логическое извлечение данных
- Некоторые комбинации аппаратного и программного обеспечения iOS, поддерживают неполное извлечение файловой системы и извлечение связки ключей в режиме BFU (Before First Unlock) с неизвестным паролем
- Для Apple TV и Apple Watch резервное копирование недоступно
- Устройства Apple Watch (первое-пятое поколения) поддерживают только логическое извлечение и требуют использования специального адаптера IBUS

Информация о моделях и версиях iOS, к которым применим метод извлечения checkm8, приведена в соответствующем отдельном руководстве.

6.6.5 Приложение В. Инструкции по установке джейлбрейка

Извлечение образа файловой системы из устройств iPhone 5s и более новых доступно исключительно посредством низкоуровневого доступа, предоставить который может только джейлбрейк. Процесс установки jailbreak не даёт гарантии неизменности данных. Более того, установка джейлбрейка неизбежно модифицирует системный раздел устройства и некоторые данные в пользовательском разделе. При сборе доказательной базы важно тщательно документировать все шаги.

Невозможно установить джейлбрейк на устройство, заблокированное неизвестным паролем. Однако, если устройство не заблокировано или пароль на устройство известен, рекомендуется сначала выполнить логическое извлечение данных, а только затем пытаться установить джейлбрейк и получить полную файловую систему.

Для того, чтобы снять образ файловой системы, на устройстве должен быть установлен сервер SSH, в качестве которого может быть использован как встроенный в jailbreak сервер SSH (обычно Dropbear), так и установленный из Cydia пакет OpenSSH. При использовании встроенного сервера Dropbear обращайте внимание на номер порта, на котором запущен сервис. Обычно используется порт 22 или 2222; указать номер порта можно при запуске iOS Forensic Toolkit. Если в составе jailbreak сервер SSH отсутствует, вам потребуется вручную установить пакет OpenSSH из Cydia.

При использовании jailbreak, полученных из непроверенных источников, существует риск заражения устройства потенциально вредными приложениями. Чтобы избежать подобного развития событий, рекомендуем скачивать файлы jailbreak по тем ссылкам, которые мы приводим ниже.

Мы протестировали iOS Forensic Toolkit со многими версиями jailbreak. Ниже находится список совместимых с iOS Forensic Toolkit утилит jailbreak, ссылки на скачивание и обнаруженные нами в процессе тестирования особенности установки и работы jailbreak.

iOS: 7.0 – 7.0.6

наименование: evasi0n7

ссылка: <http://www.iphonehacks.com/download-evasi0n7>

поддерживаемые устройства: iPhone 5s

особенности: сохраняет работоспособность после перезагрузки; рекомендуется снятие пароля блокировки; требуется установка OpenSSH из Cydia

iOS: 7.1 – 7.1.2

наименование: Pangu7

ссылка: <http://www.iphonhacks.com/download-pangu-jailbreak>

поддерживаемые устройства: iPhone 5s

особенности: сохраняет работоспособность после перезагрузки; требуется установка OpenSSH из Cydia

iOS: 8.0 – 8.4

наименование: TaiG

ссылка: <http://www.taig.com/en/>

поддерживаемые устройства: iPhone 5s, 6, 6 Plus

рекомендации: TaiG 1.2.1 для версий iOS 8.0-8.1.2; TaiG 2.4.5 для версий iOS 8.1.3-8.4

iOS: 9.0 – 9.1

наименование: Pangu

ссылка: <http://en.9.pangu.io/>

поддерживаемые устройства: iPhone 5s, 6, 6s, 6/6s Plus, SE

iOS: 9.2 – 9.3.3

наименование: Pangu64

ссылка: <http://en.pangu.io/>

поддерживаемые устройства: iPhone 5s, 6, 6s, 6/6s Plus, SE

iOS: 10.0 – 10.3.3

наименование: Meridian

ссылка: <https://meridian.sparkes.zone/>

поддерживаемые устройства: iPhone 5s, 6, 6s, 6/6s Plus, SE, iPhone 7/Plus

iOS: 13.0 to 13.7

наименование: Odyssey

jailbreak link: <https://theodyssey.dev/>

поддерживаемые устройства: от iPhone 6s до iPhone 11

iOS: 11.0 - 14.3

наименование: unc0ver

ссылка: <https://unc0ver.dev>

совместимые устройства: от iPhone 5s до iPhone 12; есть версия для Apple TV 4 и 4K

особенности: включите опцию установки OpenSSH в настройках джейлбрейка; для устройств на базе A12-A14 работа не очень стабильна

iOS: 12.3 - 14.4

наименование: checkra1n

ссылка: <https://checkra.in/>

совместимые устройства: от iPhone 5s до iPhone X, большинство iPad; для iPhone 8/X под управлением iOS 14 требуется предварительно удалить пасскод

особенности: есть поддержка tvOS; установка через режим DFU; возможно частичное извлечение данных из устройств с неизвестных пасскодом

Проверка наличия сервера SSH на устройстве

Для того, чтобы проверить работоспособность и доступность сервера SSH, запустите iOS Forensic Toolkit командой `Toolkit.command` (macOS) либо `Toolkit.cmd` (Windows). В момент запуска должно установиться туннельное соединение по протоколу SSH через порт 22 (для старых версий джейлбрейка *Meridian* вы должны указать порт 2222; для некоторых версий джейлбрейка *checkra1n* используются порт 44) на устройстве и порт 3022 на `localhost`. Используйте клиент SSH на компьютере для соединения с `localhost` через порт 3022. Пример команды:

```
ssh -p 3022  
root@localhost
```

Если сессия SSH успешно установлена или если запрашивается пароль, а также если выводится сообщение «key fingerprint mismatch error» («ошибка несоответствия отпечатка пальца»), сервер SSH успешно запущен. Если соединение не может быть установлено или отклонено, сервер SSH не запущен или не установлен. В этом случае установите OpenSSH из Cydia, установленном на устройстве. Некоторые джейлбрейки не включают Cydia, но SSH-клиент уже может быть встроен.

Смена пароля для пользователя root

По умолчанию, пароль `root` в iOS - `alpine`. В случаях, когда этот пароль не срабатывает, вам может потребоваться сменить пароль. Используйте приложение iExplorer или подобное для редактирования файла `/private/etc/master.passwd`, чтобы строка, соответствующая `root` выглядела в точности следующим образом:

```
root:/smx7MYTQIi2M:0:0::0:0:System Administrator:/var/root:/bin/sh
```

После сохранения файла `master.passwd` пароль `root` будет изменён на `alpine`. Теперь можно установить сессию SSH с устройством.

Работа с устройствами без джейлбрейка

Физическое извлечение данных (файловой системы) из устройств iPhone 5s и более новых без джейлбрейка возможно только при использовании *Агента* для определённых комбинаций моделей устройств и версий iOS.

Кроме того, вы можете выполнить логическое извлечение данных. Благодаря логическому извлечению данных можно создать свежую локальную резервную копию, извлечь файлы мультимедиа и общие файлы и получить доступ к журналам `crash log`. Если на устройстве установлен неизвестный пароль резервного копирования, можно попытаться восстановить его с помощью программы Elcomsoft Phone Password Breaker (<https://www.elcomsoft.com/eppb.html>).

Важно: в iOS 11/12/13, пароль на резервную копию может быть просто удален с устройства при сбросе настроек системы. Для этого понадобится пароль на устройство (а также пароль «Ограничений» или «Экранного времени», если они установлены) для сброса пароля резервного копирования. Обратите внимание, что при сбросе настроек также удаляется пароль на устройство, что может незначительно повлиять на некоторые пользовательские данные (такие как транзакции Apple Pay, кэшированная почта из учетных записей Exchange и т.д.).

6.6.6 Приложение С. Проблемы и способы их решения

Редактирование скрипта

Изменение некоторых настроек программы требует ручного редактирования скрипта. В версии для Windows он находится тут (необходимы привилегии Администратора для сохранения изменений):

```
C:\Program Files (x86)\Elcomsoft Password Recovery\Elcomsoft iOS  
Forensic Toolkit\Toolkit.cmd
```

В версии для macOS вызовите контекстное меню (по правой кнопке мыши) для приложения *Elcomsoft iOS Forensic Toolkit* в папке *Applications* и выберите *Browse Contents*, затем откройте файл по следующему пути:

```
Contents/Resources/macosx/Toolkit.sh
```

Редактируйте скрипт с осторожностью, только если вы точно знаете, что делаете.

SSH и пароль root

При возникновении ошибок работы с устройством убедитесь, что OpenSSH установлен (и вы использовали правильный номер порта) и запущен. Убедитесь, что пароль root - "alpine". Если установлен другой пароль, задайте его в переменной SSH в скрипте продукта.

BFU извлечение

По умолчанию *checkra1n* использует порт 44 вместо стандартного 22. Если вы производите BFU-извлечение из устройства с неизвестным пасскодом (или обычное извлечение, но без установки Cydia и OpenSSH), задайте порт 44 в переменной `IPORT` в скрипте продукта, и перезапустите продукт.

Извлечение с помощью агента

- macOS: используйте обычный пароль (не специфичный для приложений); понадобится проходить двухфакторную аутентификацию с помощью доверенного устройства; можно работать как через учётную запись разработчика, так и обычную
- Windows: используйте пароль, специфичный для приложения (его надо создать заранее)

Параметры учётной записи (Apple ID и пароль, а также идентификатор команды при использовании учётной записи разработчика) можно задать параметрами в скрипте продукта: `AGENT_ID`, `AGENT_PASSWORD` and `AGENT_TEAMID`.

Ещё одна опция для этого метода извлечения связана с максимальным размером файлов, который копируются из файловой системы устройства. По умолчанию это 512 ГБ, что более чем достаточно в большинстве случаев; однако, иногда файловая система устройства незначительно повреждена, и размер некоторых файлов возвращается некорректно (превышает все разумные пределы), что вызывает проблемы при копировании. Вы можете установить максимальный размер копируемых файлов путём добавления параметра `--max_file_size=`, указав далее размер в килобайтах, мегабайтах или гигабайтах (к/М/Г).

Параметр надо добавить в вызов вспомогательного приложения AcquisitionClient (без расширения в macOS или .exe в Windows), где оно вызывается с опцией `--image parameter` (в двух местах). В результате строка будет выглядеть примерно так (пример для macOS, в данном случае размер ограничен 8 гигабайтами):

```
"$AGENTDIR"/AcquisitionClient --image --max_file_size=8G -p "$outdir"
```

Wi-Fi

Настоятельно рекомендуем переводить устройство в полётный режим или отключать Wi-Fi до начала работы. Если инструментарий выводит сообщение "Device connected: {UDID}", при этом показывается более одного устройства, при работе инструментария могут возникать ошибки.

Решение: переключите устройство в авиарежим. Кроме того, на рабочем столе, на котором вы запускаете EIFT, должны быть отключены соединения с Wi-Fi и Ethernet. Соединение с интернет может понадобиться только для установки агента.

Стабильность и соединение

Убедитесь, что компьютер не перейдёт в режим сна или гибернации во время работы инструментария. Если используется портативное устройство (ноутбук), НЕ отключайте его от сети и НЕ подключайте к сети. В противном случае соединение может прерваться, и вам придётся начинать весь процесс с начала.

Часть VII

Лицензионное соглашение

7 Лицензионное соглашение

Лицензионный договор на использование программ для ЭВМ «ЭлкомСофт»

Общество с ограниченной ответственностью «ЭлкомСофт», адрес: 12985, Москва, ул. Звездный бульвар д. 21, стр.1, этаж 6, помещение I, комнаты № 17, 17д, 17е, которое является обладателем исключительного права на определенные программы для ЭВМ или компьютерные программы (далее «Программы»), в дальнейшем именуемое Лицензиар, с одной стороны, и Вы – физическое или юридическое лицо, указанное в конкретном Заказе, приобретающее право использования Программы (Программ), в дальнейшем «Вы» или «Лицензиат» и далее совместно именуемые «Стороны» или каждый отдельно – «Сторона» соглашаются заключить лицензионный договор на использование Программы (Программ) на следующих условиях и в следующем порядке.

- Лицензиар является обладателем исключительного права на Программу (Программы), охраняемую авторским правом, а также обладателем иных исключительных прав на результаты интеллектуальной деятельности и средства индивидуализации, связанные с Программой, включая, но не ограничиваясь, исключительное право на ноу-хау.
- Настоящий договор («Договор») является лицензионным договором на использование программ для ЭВМ в форме договора присоединения в значении статьи 428 Гражданского Кодекса Российской Федерации и заключается в соответствии с п.5 статьи 1286 Гражданского Кодекса.
- Если Вы приобретаете право использования Программы у третьего лица (дистрибьютора, реселлера или иного уполномоченного Лицензиаром лица), настоящий Договор регулирует использование Вами Программы в дополнение к договору между Вами и таким третьим лицом.
- Начало использования Вами Программы означает Ваше согласие на заключение настоящего Договора.
- **ВНИМАТЕЛЬНО ПРОЧИТАЙТЕ УСЛОВИЯ НАСТОЯЩЕГО ДОГОВОРА ПЕРЕД УСТАНОВКОЙ ПРОГРАММЫ НА ВАШЕМ УСТРОЙСТВЕ.**
- **ЕСЛИ ВЫ НЕ СОГЛАСНЫ С УСЛОВИЯМИ НАСТОЯЩЕГО ДОГОВОРА, НЕ УСТАНОВЛИВАЙТЕ ПРОГРАММУ НА ВАШЕМ УСТРОЙСТВЕ.**
- Под началом использования понимается установка (инсталляция) Программы на компьютере (устройстве) Лицензиата.

1. Основные термины

Программа (Программы) – программа для ЭВМ ООО «ЭлкомСофт», право на использование которой Вы получаете на основании настоящего Договора и которая указана в конкретном Заказе.

Регистрационный Код - генерируемый Лицензиаром уникальный код, позволяющий осуществлять полнофункциональное использование Программы без временных и иных ограничений.

Ознакомительная Версия – версия Программы, имеющая временные или иные ограничения по использованию/функционалу, предназначенная для оценки возможностей Программы Лицензиатом.

Использование – установка (инсталляция) Программы на технических средствах Лицензиата, а также осуществление действий, связанных с функционированием Программы в соответствии с ее назначением и документацией в зависимости от Типа Лицензии.

Обновления – новые версии Программы.

Декомпилирование – преобразование объектного кода в исходный текст.

Документация – инструкции по использованию Программы, иные текстовые файлы, входящие в дистрибутив Программы, которые Лицензиат получает при установке Программы.

Экземпляр Программы – копия Программы, включая Документацию.

Тип Лицензии – конкретный вид лицензии, определяющий пределы использования Программы Лицензиатом, включая количество устройств (рабочих мест), на которых Лицензиат имеет право использовать Программу одновременно. Типы Лицензии указаны на Интернет сайте Лицензиара <https://www.elcomsoft.ru> в разделе «Продукты» - <https://www.elcomsoft.ru/products.html>, а также в конкретном Заказе.

Типы Лицензии могут время от времени изменяться и все изменения будут опубликованы на Интернет сайте Лицензиара.

Заказ – заказ на получение права использования Программы (Программ), составленный и направляемый Лицензиару в письменной или иной форме (включая через Интернет сайт Лицензиара), в котором указана конкретная Программа (Программы), право на использование которой получает Лицензиат, Тип Лицензии, срок предоставления права использования, размер лицензионного вознаграждения и иные условия, связанные с использованием Программы и получением Лицензиатом права использования Программы. Заказ является приложением к настоящему Договору.

2. Предмет Договора. Объем лицензии.

2.1. Лицензиату предоставляется право использования Программы в пределах, установленных настоящим Договором за вознаграждение, указанное в Заказе, следующими способами на условиях простой неисключительной лицензии:

- В рамках настоящего Договора Лицензиат получает право Использовать Программу только на разрешенном количестве технических устройств в соответствии с Типом Лицензии и иными условиями, определенными в Типе Лицензии и указанными в Заказе. Право Использования предоставляется Лицензиату на срок, указанный в Заказе.
- Если Лицензиат устанавливает Ознакомительную Версию Программы, то Лицензиат имеет право использования Программы безвозмездно на срок, который может быть указан на Интернет сайте Лицензиара или в Заказе и / или с ограниченным функционалом.

2.2. Декомпилирование. Лицензиат имеет право декомпилировать Программу, т.е. воспроизвести и преобразовать объектный код в исходный текст при одновременном соблюдении следующих условий:

- Декомпилирование необходимо для достижения способности к взаимодействию независимо разработанной Лицензиатом программы с другими программами, которые могут взаимодействовать с декомпилируемой программой;
- информация, необходимая для достижения способности к взаимодействию, ранее не была доступна Лицензиату из других источников. Лицензиат обязан сначала запросить эту информацию у Лицензиара и только если Лицензиар не предоставит такую информацию Лицензиату, последний имеет право декомпилировать Программу;

- Эти действия осуществляются в отношении только тех частей декомпилируемой Программы, которые необходимы для достижения способности к взаимодействию;
- Информация, полученная в результате декомпилирования, может использоваться исключительно для достижения способности к взаимодействию независимо разработанной программы с другими программами, не может передаваться иным лицам, за исключением случаев, когда это необходимо для достижения способности к взаимодействию независимо разработанной программы для ЭВМ с другими программами, а также не может использоваться для разработки программы для ЭВМ, по своему виду существенно схожей с декомпилируемой Программой, или для осуществления другого действия, нарушающего исключительное право на Программу.

Никакое иное декомпилирование Программы, кроме случая, указанного выше, не разрешено Лицензиату.

2.3. Запрещается вносить какие-либо изменения в Программу без предварительного письменного разрешения Лицензиара. Если Программа или ее часть предоставлена в форме исходного текста, запрещается без предварительного письменного согласия Лицензиара, любая передача и предоставление такого исходного текста третьим лицам, за исключением случаев, когда это прямо разрешено какой либо дополнительной лицензией, регулирующей использование такого исходного текста.

2.4. Любое иное использование Программы, не разрешенное настоящим Договором, прямо запрещено. Лицензиату не предоставлены никакие права, кроме прямо указанных в настоящем Договоре.

2.5. Лицензиат не имеет права передавать экземпляр Программы любым третьим лицам, а также передавать право Использования Программы любым третьим лицам без предварительного письменного согласия Лицензиара.

2.6. Лицензиар предоставляет Лицензиату Регистрационный Код по электронной почте не позднее трех (3) рабочих дней после выплаты вознаграждения, указанного в Заказе, Лицензиару.

2.7. Лицензиату предоставляется право Использования Обновлений, которые будут выпущены в свет Лицензиаром в течение двенадцати месяцев со дня предоставления Лицензиату Регистрационного Кода либо иного срока, который указан в Заказе, в объеме и на условиях, указанных в настоящем разделе 2 Договора, за исключением случаев, если предоставление Обновлений будет сопровождаться иным лицензионным договором. Дополнительные условия и порядок предоставления Обновлений могут быть указаны на Интернет сайте Лицензиара или в Заказе.

Для использования любых обновлений, которые будут выпущены в свет по истечении двенадцати месяцев с указанной даты, Лицензиат должен выплатить Лицензиару дополнительное вознаграждение за предоставление права использования Обновлений в соответствии с информацией, указанной на Интернет сайте Лицензиара или в Заказе.

3. Регистрационный Код. Конфиденциальность Регистрационного Кода

3.1. Регистрационный Код является конфиденциальной информацией Лицензиара и является ноу-хау Лицензиара. Соответствующие положения о ноу-хау и защите информации, составляющей коммерческую тайну, законодательства РФ применяются к Регистрационному Коду.

3.2. Лицензиат обязуется использовать Регистрационный Код только в целях, определенных настоящим Договором, исключительно для обеспечения возможности Использования Программы в соответствии с настоящим Договором в зависимости от Типа Лицензии и информации, указанной в Заказе.

Лицензиат обязуется не передавать и предоставлять его третьим лицам любым способом без предварительного письменного согласия Лицензиара, в том числе не размещать Регистрационный Код на любых Интернет – сайтах.

4. Обязанности Лицензиара по технической поддержке

4.1. Лицензиар обязан оказывать техническую поддержку Лицензиату в течение двенадцати месяцев со дня предоставления Лицензиату Регистрационного Кода, в объеме и на условиях, указанных ниже.

4.2. Обязательства Лицензиара по технической поддержке включают в себя ответы на вопросы по электронной почте: support@elcomsoft.com, а также через специальный раздел по технической поддержке на Интернет сайте Лицензиара на странице: <https://support.elcomsoft.com>. Техническая поддержка, кроме ответов на вопросы, также включает в себя исправление ошибок.

Дополнительные условия выполнения Лицензиаром обязанностей по технической поддержке могут указываться на Интернет сайте Лицензиара на странице <https://support.elcomsoft.com>.

4.3. Техническая поддержка предоставляется в рабочие дни в Российской Федерации за исключением выходных и праздничных дней.

5. Ограничения. Использование в соответствии с законодательством.

5.1. Лицензиат обязуется использовать Программу и любую информацию, полученную в результате такого использования, только в соответствии с законодательством РФ, других стран, а также положений международного права. Лицензиат обязуется не использовать Программу и любую информацию, полученную в результате использования Программы, с какой-либо противоправной целью, включая незаконный доступ к информации третьих лиц, или в целях, противоречащих принципам этики, гуманности и морали.

Все лицензируемые Вам Программы являются полностью легальными и Вы имеете право их использования, при условии, что Вы являетесь законным владельцем всех файлов и данных, которые Вы собираетесь восстановить или доступ к которым Вы собираетесь получить при помощи Программ, Вы являетесь законным владельцем любых устройств или учетных записей, доступ к которым Вы собираетесь получить при помощи Программ или у Вас есть соответствующее разрешение законного владельца на выполнение указанных действий или у Вас есть такое право на основании Вашего национального законодательства (например, Вы представляете правоохранительные органы или иные компетентные органы государства, которые имеют право получения доступа к информации и данным и такой доступ необходим в ходе проведения действий и процедур, предусмотренных законодательством).

Любое использование Программ в нарушение законодательства является только Вашей ответственностью.

Вы подтверждаете, что у Вас есть законное право получить доступ ко всем данным, информации и файлам, которые закрыты.

Вы также подтверждаете, что восстановленные или полученные иным образом данные, пароли и/или файлы не будут использованы в каких-либо противозаконных целях.

Вы осознаете, что несанкционированное восстановление паролей и иных данных или несанкционированный доступ к информации и данным может являться преступлением или правонарушением и может привести к разным видам ответственности.

5.2. С целью предотвращения незаконного использования Программа может установить на Вашем устройстве технические меры защиты авторских прав и иных прав на результаты интеллектуальной деятельности. Данные меры будут использованы с целью контроля использования Программы и любых Обновлений в соответствии с настоящим Договором. В результате установки таких технических мер Лицензиар не будет получать никакой персональной информации (включая персональные данные) о Лицензиате.

5.3. Уведомления об авторских правах. Программа может содержать уведомления о принадлежности исключительного права на нее Лицензиару и иные уведомления об исключительных правах. Вы не имеете право удалять или изменять каким-либо образом такие уведомления и информацию.

6. Вознаграждение

6.1. Вознаграждение за право использования указано в Заказе на конкретную Программу (Программы).

7. Ограниченная гарантия

7.1. Лицензиар гарантирует, что Программа будет функционировать в соответствии с Документацией на Программу при условии соблюдения порядка ее использования, предусмотренного Документацией и настоящей Лицензией в течение 90 (девяносто) дней со дня получения Лицензиатом Регистрационного Ключа.

Функционирование с незначительными отступлениями от Документации не считаются дефектами.

7.2. Данная гарантия недействительна, если использование Программы осуществляется с нарушениями правил и требований, указанных в Документации и с нарушениями настоящего Договора и/или законодательства, включая внесение любых изменений в Программу без согласия Лицензиара.

7.3. Лицензиар не предоставляет никаких иных гарантий кроме указанной выше и не несет никакой материальной ответственности за любые убытки Лицензиата, включая упущенную выгоду, вытекающие из использования или невозможности использования Программы, не получения Лицензиатом какого-либо результата от использования Программы, не связанные с нарушением Лицензиаром настоящей гарантии и обязательств по технической поддержке, указанных в Договоре.

7.4. Единственным средством защиты Лицензиата в случае нарушения указанной выше гарантии является: а) возврат выплаченного вознаграждения или б) замена дефектного носителя, если Программа предоставлена на материальном носителе или в) исправление ошибок в течение разумного периода времени. В случае претензий к функционированию Программы Лицензиат обязан направить Лицензиару максимально полную информацию о проблеме, включая информацию об устройстве (устройствах) Лицензиата, на которых используется Программа, информацию об иных программах, используемых Лицензиатом,

которые могут повлиять на функционирование Программы, информацию о любых файлах, документах и материалах, в связи с которыми Лицензиат использует Программу и любую иную информацию, запрошенную Лицензиаром.

Указанная в настоящем разделе 7 гарантия не применяется в случае не предоставления Лицензиатом полной информации о проблеме по запросу Лицензиара.

8. Интеллектуальная собственность Лицензиара

8.1. Программа и вся Документация на нее являются объектом авторского права и охраняются авторским правом, а именно частью 4 Гражданского Кодекса РФ и международными соглашениями в области авторского права, а также иными положениями законодательства об интеллектуальных правах (интеллектуальной собственности). Программы, принципы и способы, связанные с Программой, также могут охраняться как объекты патентного права, включая, но не ограничиваясь, изобретения, в РФ и иных странах.

8.2. Исходный текст (код) Программ и Регистрационный Код являются ноу-хау и информацией, составляющей коммерческую тайну Лицензиара.

8.3. Лицензиат не приобретает никаких прав на Программу, кроме тех, которые прямо указаны в настоящем Договоре. Лицензиату предоставлена ограниченная неисключительная лицензия на Программу в пределах настоящего Договора.

9. Ответственность за нарушение Договора

9.1. В случае нарушения обязательств по сохранению конфиденциальности Регистрационного Кода Лицензиат возмещает Лицензиару убытки в полном размере, включая упущенную выгоду.

9.2. Ответственность за нарушение иных обязательств Сторон определяется в соответствии с законодательством Российской Федерации.

10. Срок действия Договора

10.1. Датой заключения настоящего Договора считается дата оплаты вознаграждения за предоставление права использования Программы. Договор действует на срок, указанный в конкретном Заказе.

Договор применяется к отношениям Сторон, возникшим со дня начала использования Программы в соответствии с преамбулой Договора.

10.2. Лицензиар имеет право отказаться от исполнения Договора и расторгнуть Договор в случае нарушения Лицензиатом условий использования Программ, установленных настоящим Договором, включая, но не ограничиваясь условия, установленные в разделе 2 Договора, а также нарушения обязательств по сохранению конфиденциальности Регистрационного Кода, установленного в разделе 3 Договора или нарушения Лицензиатом иных обязательств по настоящему Договору. В таком случае Лицензиар уведомляет Лицензиата о расторжении Договора, и Договор считается прекращенным с даты направления уведомления по электронной почте по адресу Лицензиата, указанному в Заказе или иным образом.

10.3. После расторжения или прекращения Договора по любому основанию Лицензиат не имеет права использовать Программу каким-либо образом и должен немедленно удалить все

экземпляры Программ и незамедлительно уведомить об этом Лицензиара по электронной почте по адресу: info@elcomsoft.com.

11. Публичность

11.1. Лицензиат настоящим соглашается, и Лицензиар имеет право публично ссылаться на тот факт, что Лицензиат является его клиентом (пользователем - Лицензиатом), в том числе ссылаться на Лицензиата и на факт использования Программы Лицензиатом в маркетинговых материалах, аналитических и иных материалах и пресс-релизах, не раскрывая какой-либо конфиденциальной информации Лицензиата.

11.2. Лицензиат имеет право отказать Лицензиару в реализации указанного выше в 11.1 права на публичность либо отозвать свое согласие на такое использование, направив сообщение по электронной почте по адресу: info@elcomsoft.com с указанием в теме письма «Отзыв согласия на Публичность».

12. Заключительные и переходные положения

12.1. Ссылки на соответствующие страницы Интернет сайта Лицензиара включены в настоящий Договор как его части и (или) приложения к нему. Положения и условия, размещенные на соответствующих страницах Интернет сайта Лицензиара, применяются к использованию Программы Лицензиатом.

12.2. В случае, если компетентный суд признает какое-либо из условий настоящего Договора недействительными, Договор продолжает действовать в остальной части.

12.3. К настоящему Договору применяется материальное право Российской Федерации без отсылки к нормам международного частного права.

Любые споры, вытекающие из настоящего Договора, подлежат рассмотрению в компетентном суде г. Москвы.

12.4. Настоящий Договор также размещен на Интернет – сайте Лицензиара по адресу: https://www.elcomsoft.ru/Elcomsoft_EULA_ru.pdf.

Index

- A -

About PDF encryption 87
About Windows passwords 185
About Word and Excel encryption 54
Access Database Password 77
Access Owner Information 77
Access User-Level Passwords 79
Account disabled 173
Account is locked out 173
Accounts database source 167
Acknowledgements 46
Active Directory 167, 176
AD 167
Administrator account 173
Advanced options 41, 94
AOL password 113
Automatic passwords recovery 52
Auto-save 40, 93

- B -

Benchmark 41, 95
BIOS 162, 163
boot 163
Brute-force range options 35, 90
Buy 85

- C -

Command line 44, 98
Command line interface 61
Contacting us 65, 151
Copyright and license 152
Creating Debug Log 84
Creating the project 67
Credentials 188
Cryptographic Service Provider 74
CSP 74

- D -

Debug Log creation 84
Decrypting files 134
Decrypting the document 58
Dictionary options 36, 91
Domain 188
Download the latest version 65
drivers 163

- E -

EFS 125
Elcomsoft System Recovery 159
Encrypted PDF file 89
Encrypting File System 125
Error messages 100
ESR 159
Excel Add-In unlocking 82
Excel Book Password 81
Excel Document Passwords 81
Excel Password to Modify 81
Excel Shared Book Password 81
Excel Sheet Passwords 81
Exit 54

- F -

File encryption 125
Files with different passwords 44
French versions of Word/Excel 76

- G -

Getting results 66
Guaranteed WinZip attack 39

- H -

hotmail password 113
How the program works 185

- I -

identity password 113

IE 109
 IE password 109
 Internet Explorer 109
 Internet Explorer password 109
 Introduction 34, 46, 49, 50, 54, 62, 85, 102, 104,
 106, 107, 116, 124, 136, 148, 159, 183

- K -

KB241201 126
 Key search 92
 Known bugs and limitations 43
 Known plaintext attack (ARJ) 38

- L -

Language 167
 Limitations 161
 Limitations of Trial version 85
 LM hash 186
 local accounts 167

- M -

mail 113
 mail password 113
 Mail server emulator (auto mode) 52
 Mail server emulator (manual mode) 53
 Managing Password Cache Files 73
 Manual passwords recovery 52
 mass-storage 163
 Microsoft Outlook 108
 Microsoft Passport Passwords 75
 Microsoft Policy Regarding Missing or Invalid
 Passwords 62
 Money 2002 Password to Open 75
 Money Passwords 84
 MS Passport stored Passwords 69

- N -

news 113
 NNTP password 113
 ntds.dit 170
 NTFS 125
 NTLM hash 186

- O -

Obtaining password hashes 186
 Office XP Passwords 74
 OneNote 75
 Operating system 170
 Options 53, 193
 Other options 40, 72, 93
 Outlook E-Mail Account Passwords 83
 Outlook E-Mail Accounts 67
 Outlook Personal Storage 83
 Outlook PST 108
 Outlook PST File Password 83

- P -

password 173
 Password Cache 73
 Password cracking methods 188
 Password expired 173
 Password from keys 39
 Password length 36, 91
 Password mask 36, 91
 Password never expires 173
 Password Storage Types (PST) 68
 Password-encrypted file 35
 Pocket Excel Password 82
 PowerPoint Password to Modify 83
 PowerPoint Passwords 83
 Precompiled hashes 189
 Preinstallation Environment 159
 Preliminary Attack 70
 Price list 85
 Program options 60, 72, 134
 Program status 42, 95
 Project Passwords 84
 Purchase 85
 PWDUMP 186

- Q -

Quicken 2001 and below 47

- R -

RAID 163
Rainbow attack 189
Recovering process 95
Recovery process and results 191
Registration 85, 157
Registry 186
Reports 192
Requirements 35, 47, 50, 51, 54, 86, 103, 105, 106, 108, 117, 135, 137, 149, 161, 184
Resource name 188

- S -

SAM 170, 186
Save and Read setup 41, 94
Saving your project 67
Scan for encrypted files 131
Scan for encryption keys 127
SCSI 163
Search for email clients 52
Searching for encryption key 56
Selecting File 66
SerialATA 163
Several words before 56
Start from password 36, 90
Supported File Types 63
Supported Passwords 63
SYSTEM 170, 186
System Requirements 62

- T -

Technical Support 65
The password is 43
Time-Memory Trade-Off 189
Type of attack 35, 70, 90

- U -

UFD 162
USB flash drive 162
User interface 51

- V -

VBA 76
VBA Backdoor 69
Visual Basic for Applications 76

- W -

Weak Encryption 76
web mail 113
web mail password 113
webmail 113
webmail password 113
What to start from 44, 97
Where to get the latest version 65, 151
Windows Live Mail password 113
Windows Mail password 113
Windows PE 159
Wizard 127
Word Document Passwords 82
Word Document Protection Password 82
Word Password to Modify 82
Word/Excel 95 Passwords 76
Word/Excel 97/2000 encryption 74
Word/Excel 97/2000 Password to Open (strong) 74
Word/Excel Password to Open (weak) 76
Word/Excel/PowerPoint XP Password to Open 74
Working mode 167
Working with ACTPR 103
Working with AINPR 47
Working with ALPR 50
Working with ASQLPR 105
Working with AWOPR 106
Working with Password Cache 73

- X -

XLA unlock 82

- Y -

Yahoo password 113