Elcomsoft Desktop Forensic Bundle

Руководство Пользователя

Оглавление

Часть I

О наборе программ Desktop Forensic Bundle

1 О наборе программ Desktop Forensic Bundle

Desktop Forensic Bundle - набор программ компании Elcomsoft, предназначенных для восстановления паролей и данных с десктоп-компьютеров и объединенные в единый набор. Эти программы позволяют эксперту открывать защищенные документы, архивы, зашифрованные диски (крипто-контейнеры) и многие другие зашифрованные файлы.

- Перебор паролей поддерживается для нескольких сотен форматов файлов
- Поддерживается аппаратное ускорение перебора паролей с использованием современных видокарт
- Распределенная атака с поддержкой до 10000 рабочих станций

Часть II

Установка программного обеспечения

2 Установка программного обеспечения

Elcomsoft Desktop Forensic Bundle поставляется единым инсталляционным пакетом.

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

Минимальные системные требования для установки:

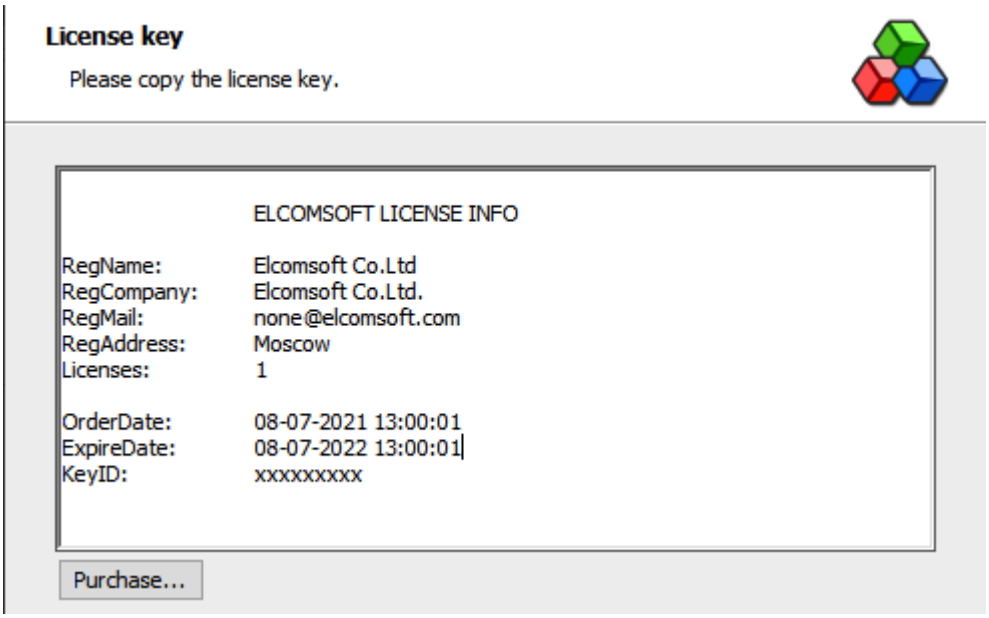
- Компьютер, работающий под операционной системой Windows, начиная от версии 8 и старше
- Свободное место на диске для установки определяется в зависимости от выбранного комплекта компонентов. Полный набор компонентов потребует до 2 гигабайт свободного дискового пространства на жестком диске.

Процесс установки:

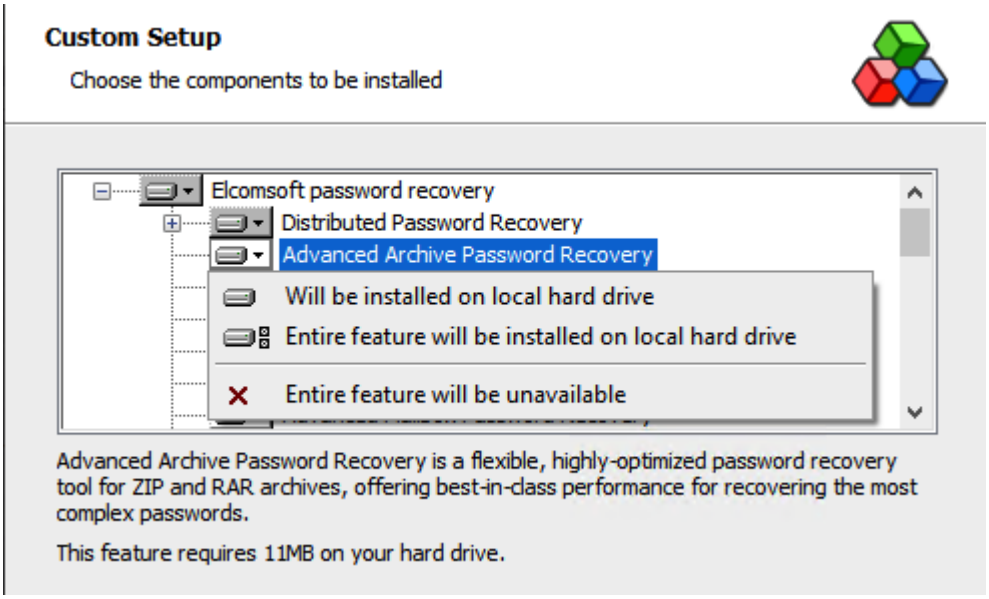
1. Запустите инсталлятор ***eprfd_setup_en.msi***

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 небходимые для установки компоненты



5. Завершите процесс инсталляции выбранных компонентов.

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 невоможно 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 протестированые следующие пароли:
test0
test1
test2
...
test9

John?d(1-2)
Будут протестированые 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@$$w0rd
MIN, AVE, MAX	Меняется только одна буква	password	p@ssword, pa$sword .. passw0rd
AVE, MAX	Меняются все буквы, кроме одной	password	pa$$w0rd, p@s$w0rd, p@$$word ..
MAX	Все возможные изменения, первая буква большая	password	P@$$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	Ih8you, Ihateu
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	psswrd
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	Psswrd
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, Pasword ..
MAX	Удаление одной буквы, все буквы большие	password	ASSWORD, PSSWORD, PASWORD ..

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 .. passwordddddddddd
AVE, MAX	Повторение одной буквы, все буквы маленькие	password	Ppassword, Paassword, Passsword, Passwword ..
MAX	Повторение одной буквы, все буквы большие	password	PPASSWORD, PAASSWORD, PASSSWORD, PASSWWORD ..
MAX	Повторение первой буквы много раз, все буквы маленькие	password	ppassword, pppassword, pppassword .. 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 -> dpasswor
[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 -> ppaasssswwoorrdd
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, атаки по маске и словарю, в то время как атака на основе открытых текстов доступна для определенных архивов ZIP и ARJ. Атака с гарантированным результатом 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

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 («zxcv ...»), диапазон вашего пароля может быть «zxcvbnm,. /» (или заглавными буквами: «ZXCVBNM <>?»). Вы также можете определить оба из них: «zxcvbnm,. / 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 «a» до «z»), его длина равна 5, а пароль начинается с «k», введите «kaaaa». 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.

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). 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
...
PASSWORd
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, 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 и гарантированная WinZip атака 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.

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

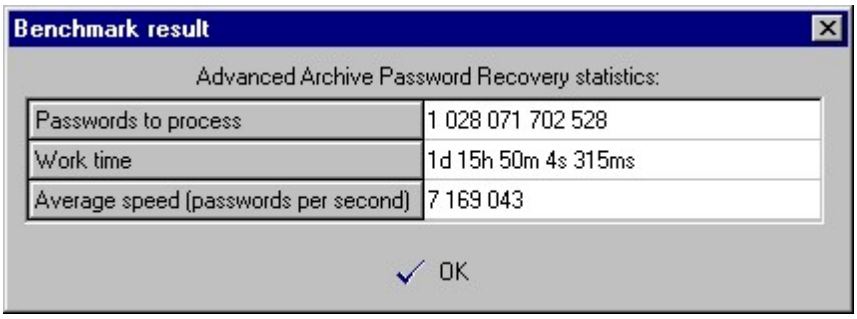
Сохранение и чтение настроек

Вы можете сохранить текущие настройки ARCHPR в файл .AXR. Вы можете восстановить настройки с помощью кнопки «Открыть файл/проект» или перетащив ранее сохраненный файл axr 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 или по маске, 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

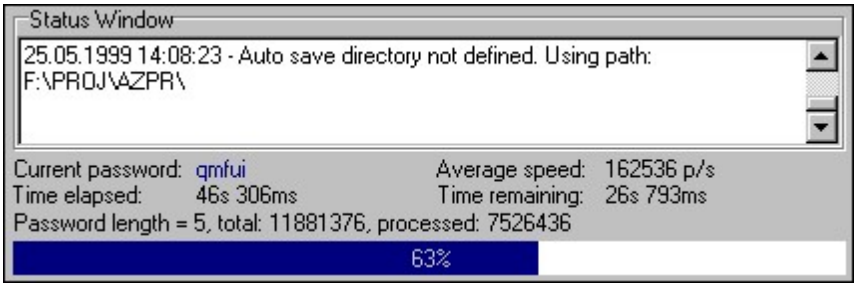
Нажмите "Старт" или F9, чтобы начать атаку. Будет отображен статус программы.

Вы можете остановить и возобновить атаки. Дополнительные сведения см. в разделах «Начать с пароля» и «Сохранение и чтение настроек».

Во время «атаки по известному открытому тексту» 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.

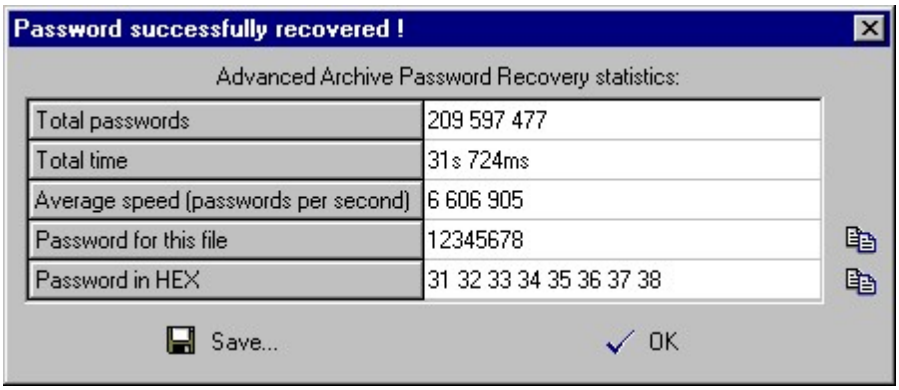
Статус программы

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

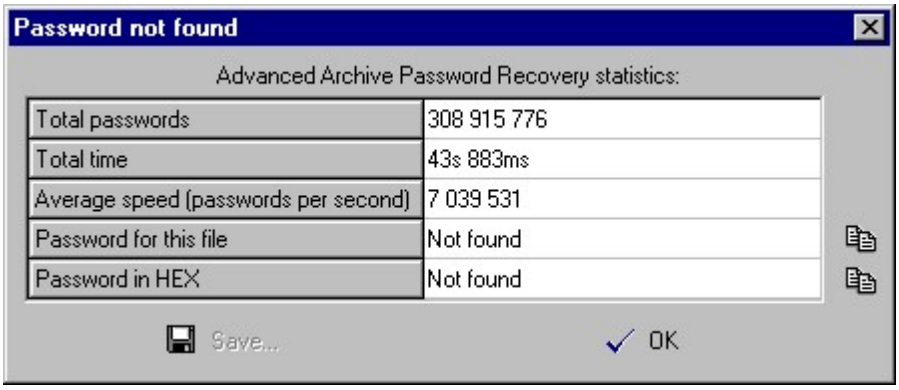
После атаки результат отображается в следующем окне:



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).
- 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, проьел	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:csdepa	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[: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:

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 axr, 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.

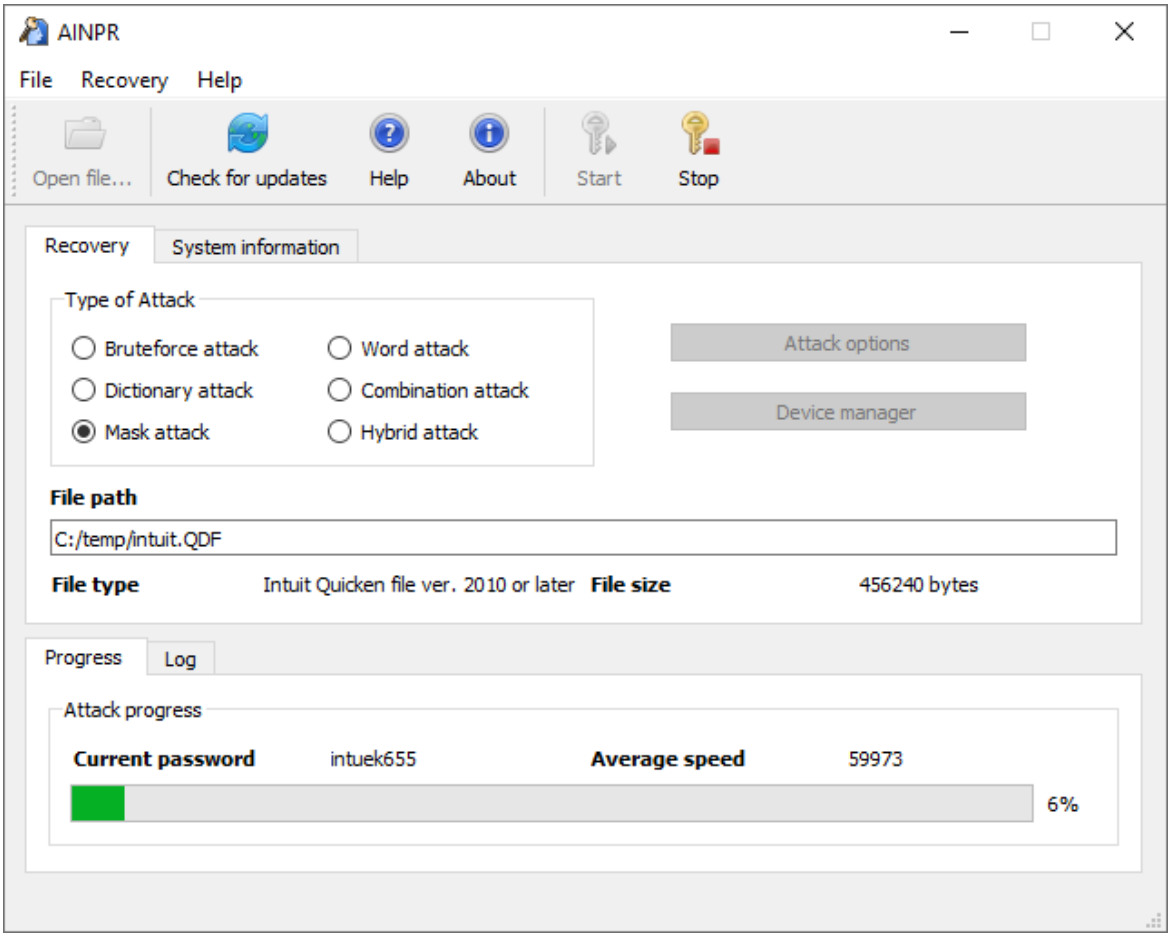
Для получения подробной информации о Quicken и QuickBooks прочтите следующие главы.

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».



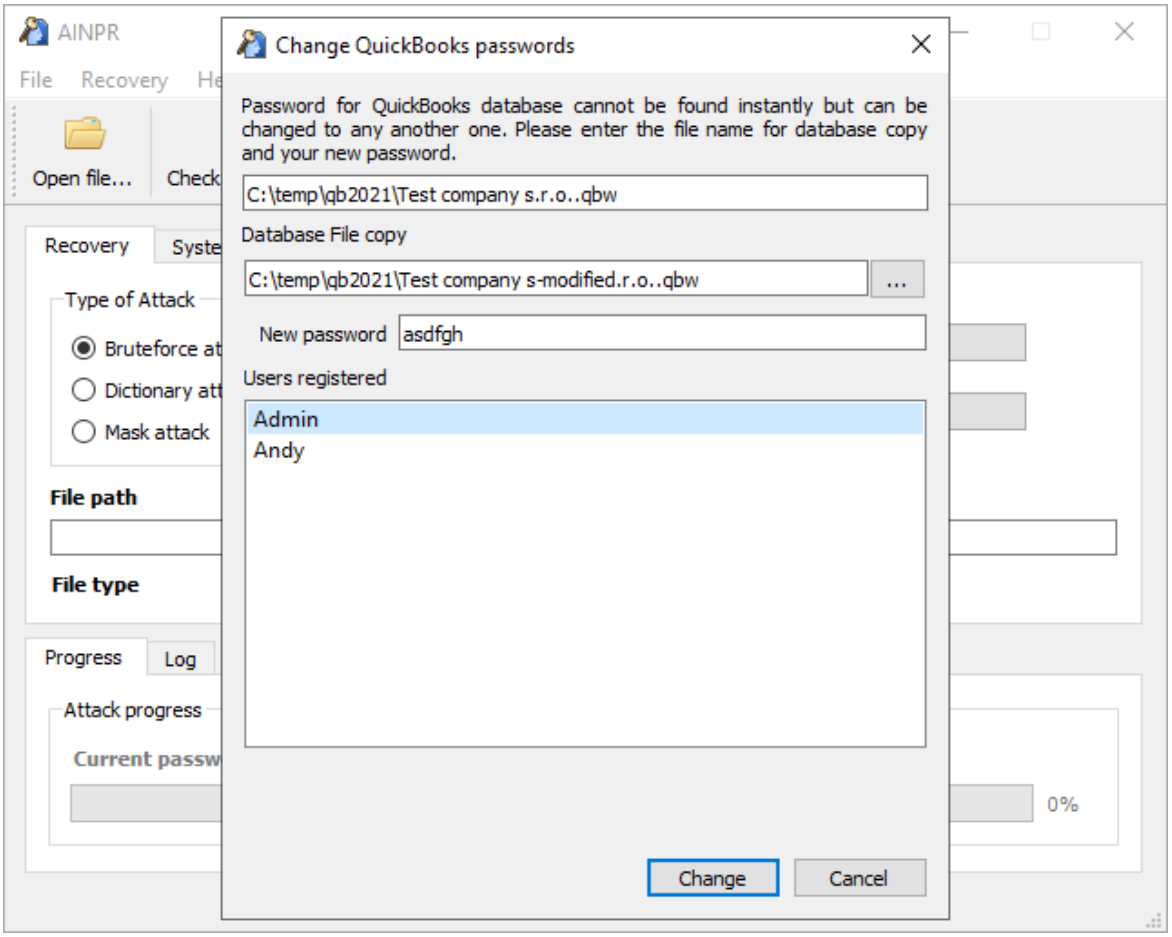
Примечание

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 или вручную; эмулятор почтового сервера: автометически и вручную), Options/Параметры, Help/Справка and Exit/Выход.

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
- ALT-2: Автоматическое восстановление паролей
- ALT-3: Восстановление паролей вручную
- ALT-4: Эмулятор почтового сервера (автоматический режим)
- ALT-5: Эмулятор почтового сервера (ручной режим)

CTRL-2: Параметры
- 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
- 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 потребуется 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 AMBPR.

Эмулятор почтового сервера (ручной режим)

Мы рекомендуем сначала попробовать эмулятор почтового сервера (автоматический режим). 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).

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:

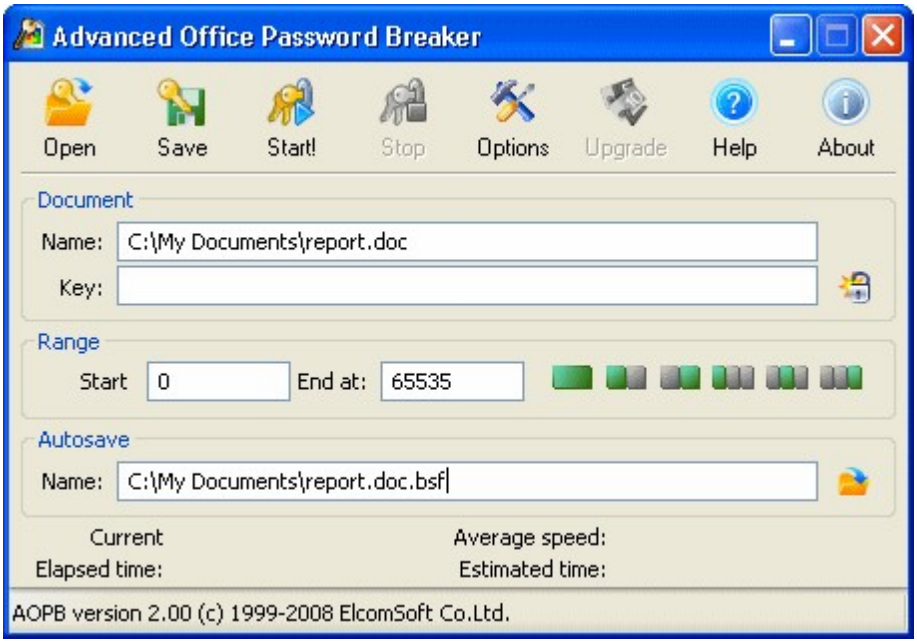
2 ^ 40 = 1,099,511,627,776

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», атака может начаться 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.

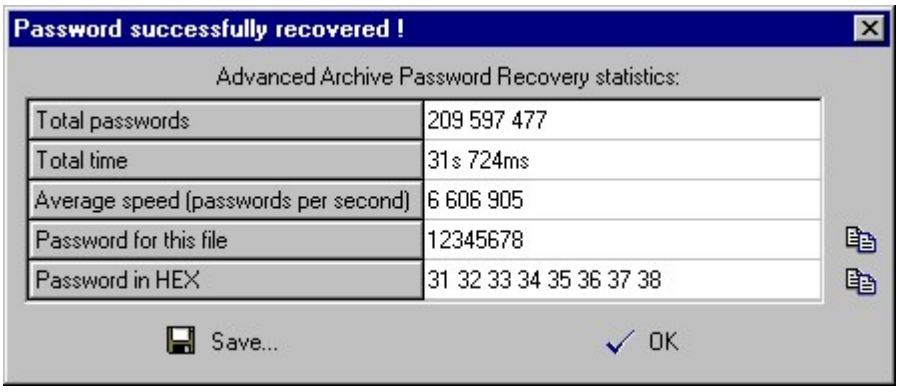
Дождитесь завершения атаки, чтобы расшифровать файл.

Enterprise версия AOPB позволяет ускорить атаку, включив опцию Использовать предварительно вычисленные хэш-таблицы.

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 AOPB 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. AOPB хранит обнаруженные ключи шифрования в реестре Windows на локальном компьютере. Если вы успешно завершили атаку с использованием пробной версии AOPB, 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 AOPB 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_l17000.data
0\t00_l17000.index
1\t01_l17000.data
1\t01_l17000.index
2\t02_l17000.data
2\t02_l17000.index
3\t03_l17000.data
3\t03_l17000.index
4\t04_l17000.data
4\t04_l17000.index
5\t05_l17000.data
5\t05_l17000.index
missing.bin

Для Microsoft Excel:

0x62\0\t00_l12500.data
0x62\0\t00_l12500.index
0x62\1\t01_l12500.data
0x62\1\t01_l12500.index
0x62\2\t02_l12500.data
0x62\2\t02_l12500.index
0x66\0\t00_l12500.data
0x66\0\t00_l12500.index
0x66\1\t01_l12500.data
0x66\1\t01_l12500.index

0x66\2\t02_l12500.data
0x66\2\t02_l12500.index

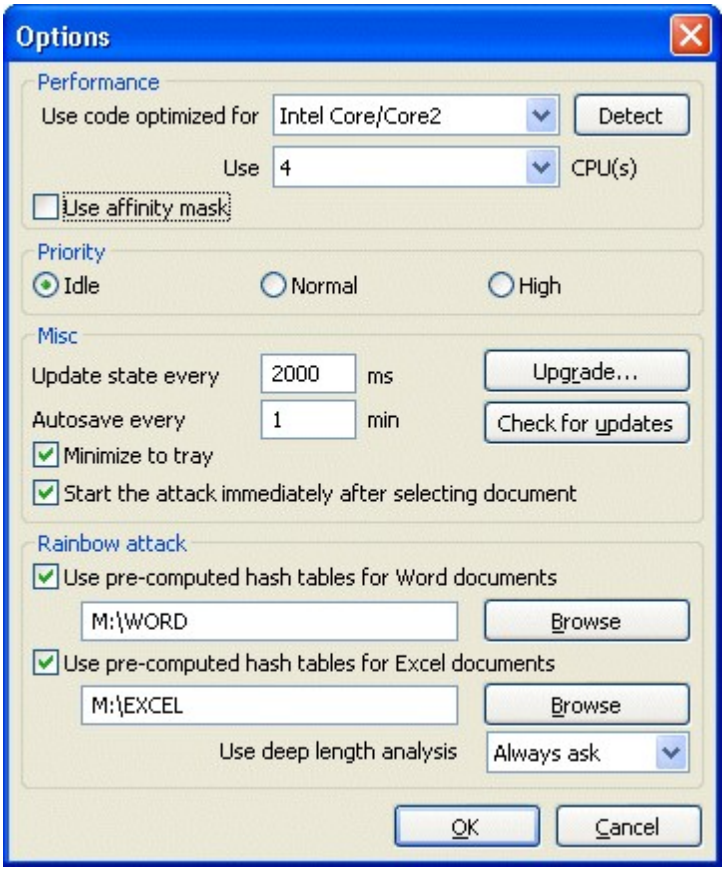
С хеш-таблицами на жестком диске атака может занять от 10 до 30 минут. Если таблицы хранятся на быстром USB-накопителе или SSD-накопителе, большинство атак завершится за секунды, но может занять до 10-15 минут.

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 потребуется 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.

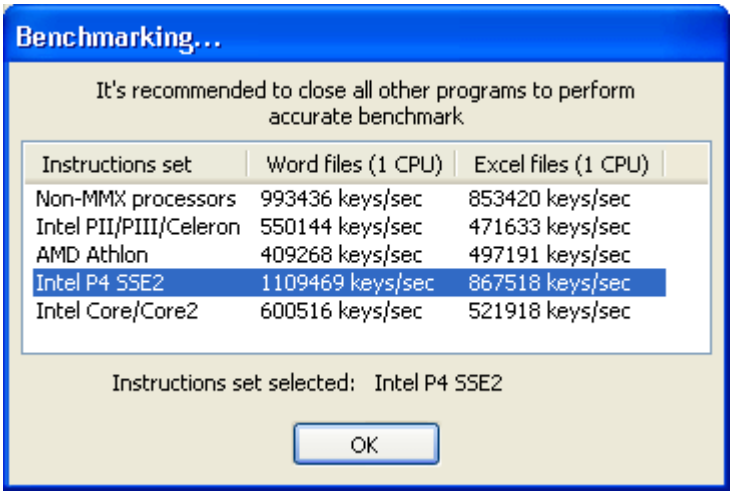
Обратите внимание, что если ключ не найден с помощью предварительно вычисленных таблиц Excel, вы все равно можете расшифровать файл, временно отключив эту опцию и выполнив полный поиск ключа.

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.

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" 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	Да	Да	Да
Пароль на изменения	Да	Да	Да
Пароль защищающий документ	Да	Да	Да
Пароль к VBA Project	Нет	Да	Да
Microsoft® Excel® (версии: 3.0, 4.0, 95, 97, 2000, XP, 2003 - 2019)			
Пароль на открытие	Да	Да	Да
Пароль на изменения	Да	Да	Да
Пароль книги	Да	Да	Да
Общий пароль книги	Да	Да	Да
Пароль листа	Да	Да	Да
Пароль к VBA Project	Нет	Да	Да
Разблокировка надстроек XLA	Нет	Да	Да
Microsoft® Access® (версии: 2.0, 95, 97, 2000, XP, 2003 - 2019)			
Пароль на открытие	Да	Да	Да
Пароли уровней пользователя и группы	Нет	Нет	Да
Database Owner и Security ID	Нет	Нет	Да
Пароль к VBA Project (поддерживается только через обход защиты VBA)	Нет	Нет	Да
Microsoft® Outlook® (версии: 97, 2000, XP, 2003 - 2019)			
Пароль на открытие (PST-файлы)	Нет	Да	Да
Пароль к VBA Project	Нет	Да	Да
Сохранённые пароли к E-Mail аккаунтам	Нет	Да	Да
Microsoft® PowerPoint® (версии: 4.0, 95, 97, 2000, XP, 2003 - 2019)			
Пароль на открытие	Нет	Нет	Да
Пароль на изменения	Нет	Нет	Да
Пароль к VBA Project	Нет	Нет	Да
Microsoft® OneNote® (версии: 2003 с SP1 и новее)			
Пароль на открытие	Нет	Нет	Да
Microsoft® Visio® (версии: 4.0, 5.0, 2000, 2002)			

VBA Project (в некоторых версиях поддерживается только через обход защиты VBA)	Нет	Нет	Да
Microsoft® Publisher			
Пароль к VBA Project	Нет	Нет	Да
Microsoft® Project®			
Пароль на открытие	Нет	Нет	Да
Пароль на изменения	Нет	Нет	Да
Пароль к VBA Project	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	Нет	Нет	Да
Сохранённые пароли к MS Passport	Нет	Нет	Да
Apple iWork (версии: '09 - 2020)			
Пароль на открытие	Нет	Да	Да
All Applications with VBA			
Обход защиты VBA	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**, 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**», чтобы узнать, какие форматы файлов поддерживаются в AOPR.

- **Произошла ошибка.** Отображается окно сообщения об ошибке.

Пожалуйста, ознакомьтесь с **Руководством по паролям**, 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»**.

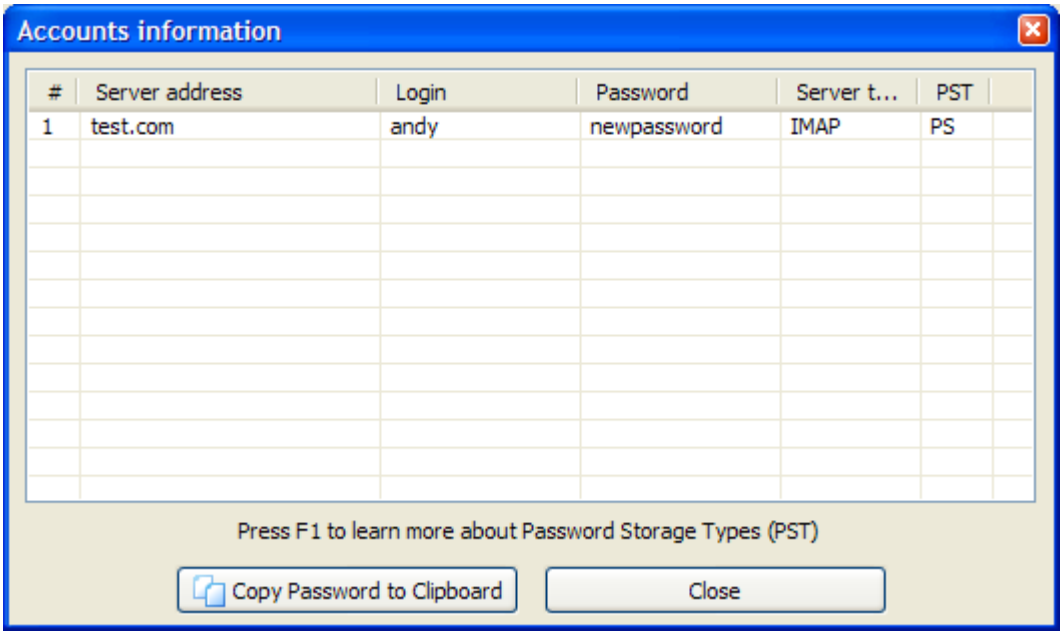
Если у вас уже есть проект, вам будет предложено сохранить его при закрытии программы. Вы можете отключить этот запрос, сняв флажок **«Запрашивать, если проект был изменен»** во вкладке **«Параметры»**.

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.]

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.

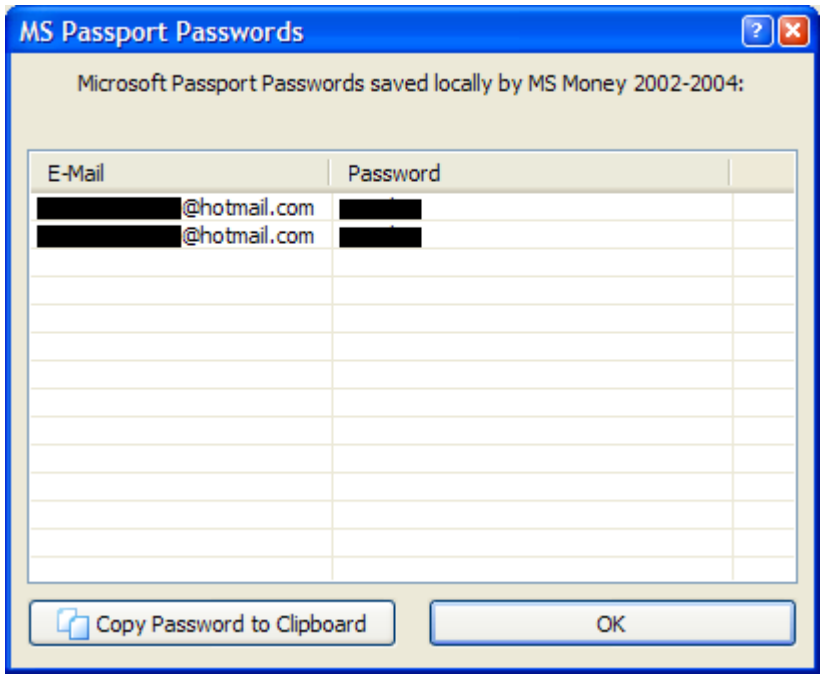
NR - Пароль не был получен. У вас недостаточно прав для разблокировки Защищенного хранилища, или Защищенное хранилище не установлено на компьютере.

NO - Пароль для этой учетной записи отсутствует.

Если тип хранилища **"UN", "ER"** или **"NR"**, отправьте **журнал отладки** в **службу технической поддержки Elcomsoft**.

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

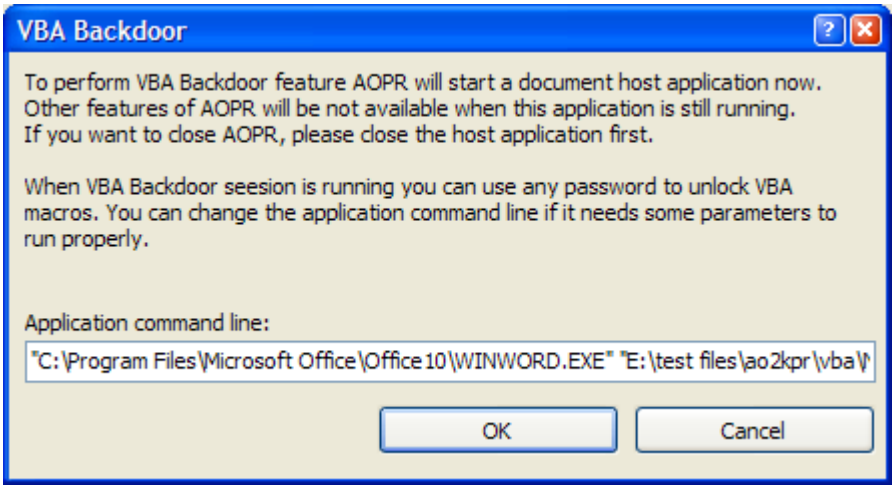
Если у вас есть документ с проектом VBA, который защищён паролем, и у вас есть проблема с восстановлением пароля и/или разблокировкой проекта VBA, вы можете использовать **бэкдор (т.е. обход защиты) VBA**. Данный обход защиты работает для всех приложений, которые могут создавать проекты VBA, а не только 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 VBAProject»**. Вам будет предложено ввести пароль. Введите любой непустой пароль (например, xyz), 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. Он 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**. В отличие от атаки найденных паролей, атака кеша 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 предопределенными наборами символов. Эту атаку

можно включить или отключить с помощью переметра **«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 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), 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 предопределенные 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** (**«aoxppr_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**.

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**. Если пароль документа не может быть мгновенно восстановлен, **AOPR** сначала проверяет кэш паролей.

Имя файла по умолчанию для кеша паролей - **aopr.pwc**. Вы можете **управлять файлами кэша паролей** 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 кеша, нажмите кнопку **«Установить пароль ...»** и введите пароль.

Вы также можете **просмотреть** и **очистить** файл кеша, нажав соответствующие кнопки, или полностью отключить кеш 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)
Пароли на открытие файла Word®/Excel®/PowerPoint® (Office XP и старше)
Пароли на открытие файла Microsoft® Money 2002

Слабые пароли

Пароли на открытие файла Word®/Excel® (слабое шифрование)
Visual Basic for Applications (VBA)

Microsoft® Access®
Общие пароли баз данных Access®, информация о владельце
Пользовательские пароли Access®

Microsoft® Excel®
Документы Excel® - все пароли кроме пароля на открытие файла
Защита надстроек Excel® (XLA)
Pocket Excel®

Microsoft® Word®
Документы Word® - все пароли кроме пароля на открытие

Microsoft® Outlook®

Пароль к файлу личного хранилища Outlook®

Пароли учетных записей электронной почты Outlook®

Microsoft® PowerPoint®

Microsoft® Money

Microsoft® Project

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: 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 совестимое с Office 97/2000

По умолчанию в Microsoft® Office XP методом шифрования является *метод, совместимый с Office 97/2000* . Это проприетарное **шифрование**, 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**, 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 (потоковый 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® Enchanced RSA and AES Cryptographic Provider (Prototype)

Для документов, использующих этот метод шифрования, **AOPR** может запускать те же атаки, что и для **Office 97/2000**, 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**.

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** по словарю и методом полного перебора. В Microsoft Money 2002-2005 все символы пароля начинаются с заглавной буквы (например, «Aaaa» и «AAAA» 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**.

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** в **AOPR**, и пароль будет немедленно **отображен**.

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**, которая позволяет обходить проверку пароля VBA в любом приложении.

Microsoft Access

Общий пароль к базе данных Access, информация о владельце

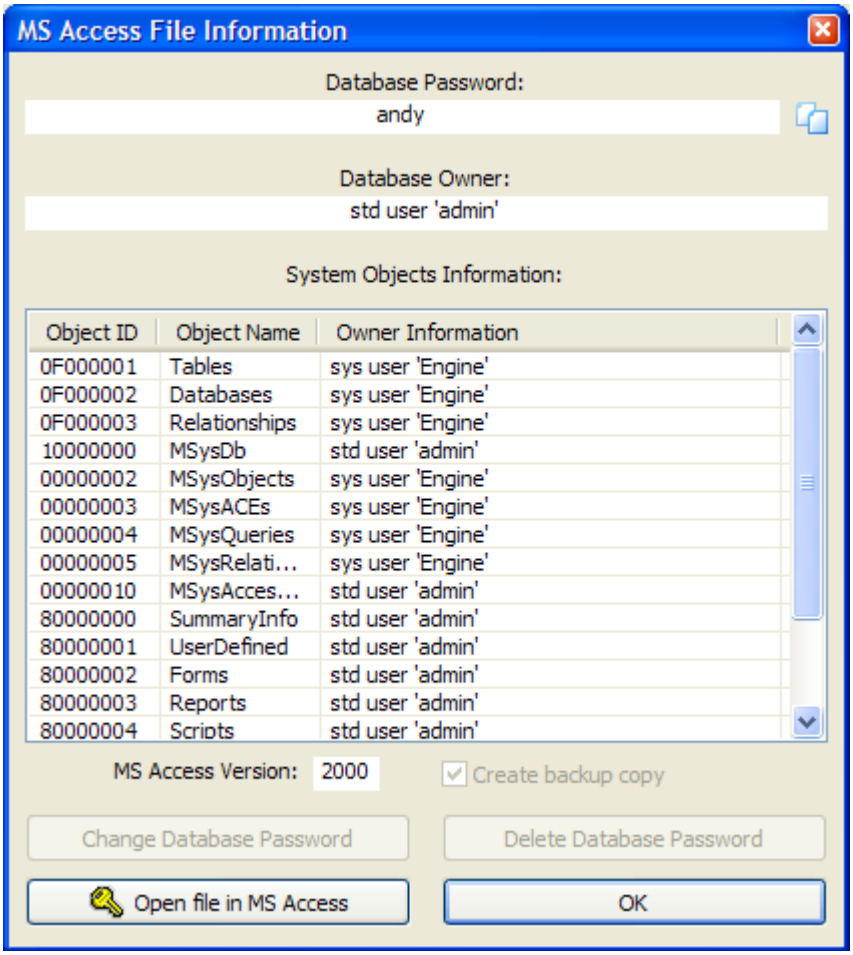
Общий пароль к базе данных Microsoft Access® может быть включен для предотвращения несанкционированного доступа к базе данных. В устаревших версиях Microsoft Access® файл был зашифрован с помощью слабого алгоритма (XOR) и мог быть немедленно восстановлен с помощью AOPR. Access 2007 улучшает защиту паролем,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

При установках **защиты на уровне пользователя** 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 слуедующую информацию:

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

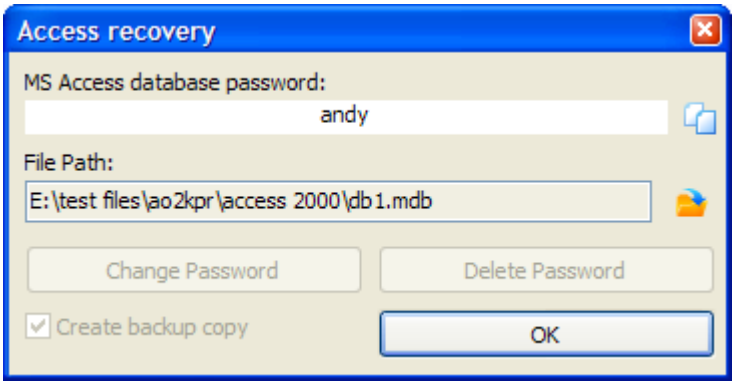
Например:



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**, 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:

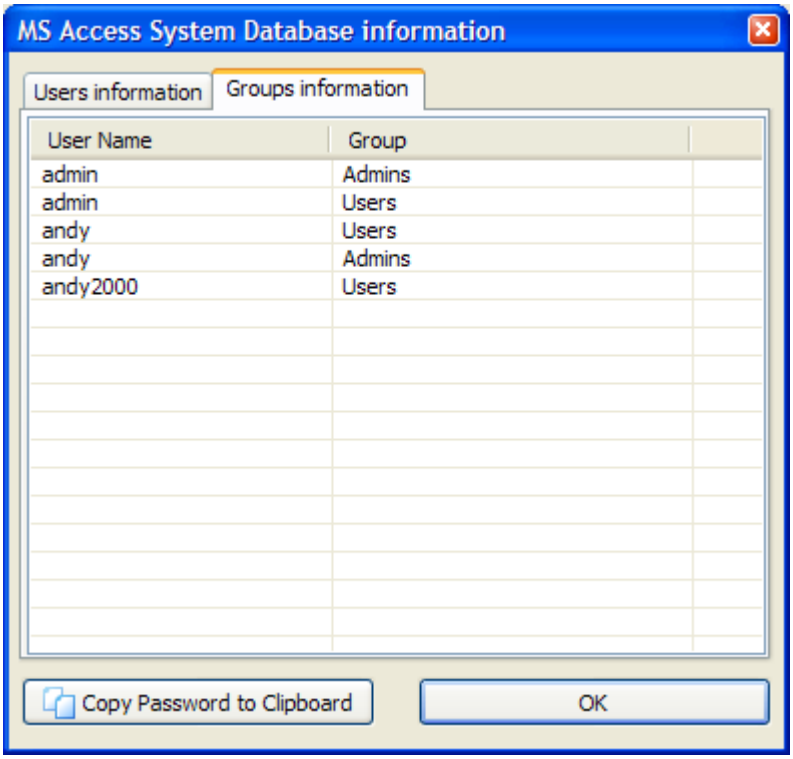
MSACCESS.EXE / пользователь

- 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.

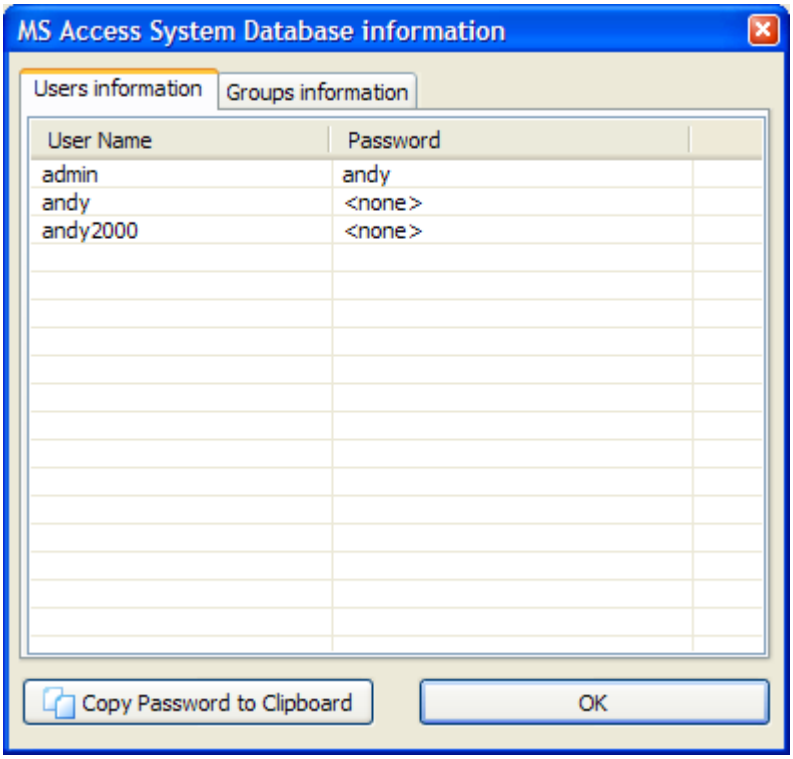
Пользовательские пароли Access

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.:



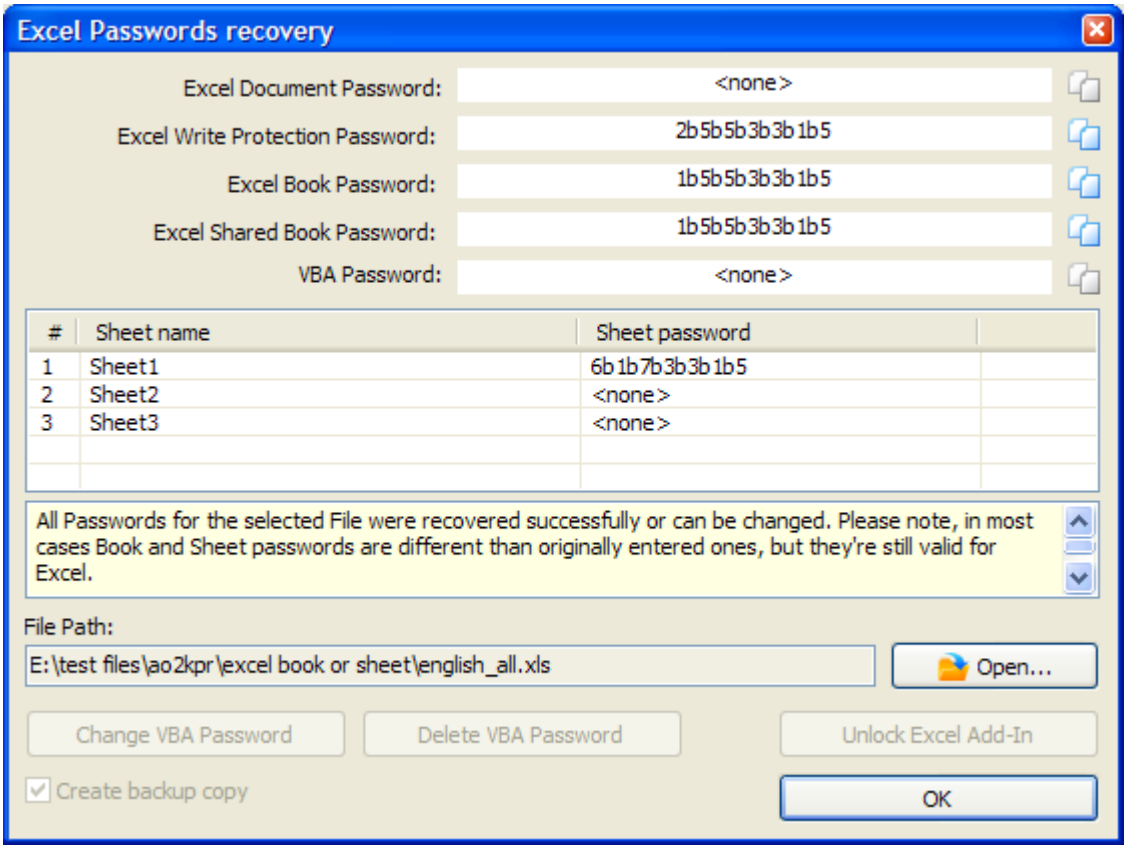
Microsoft Excel

Документ Excel - все пароли кроме пароля на открытие

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

- Пароль на открытие (может быть **стойким** или **слабым**)
- Пароль на изменения (пароль для защиты от записи)
- Пароль на книгу
- Общий пароль книги
- Пароль на лист
- **Пароль к VBA Project**

Все пароли Excel®, кроме **надежного пароля на открытие файла**, 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)**.

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**.

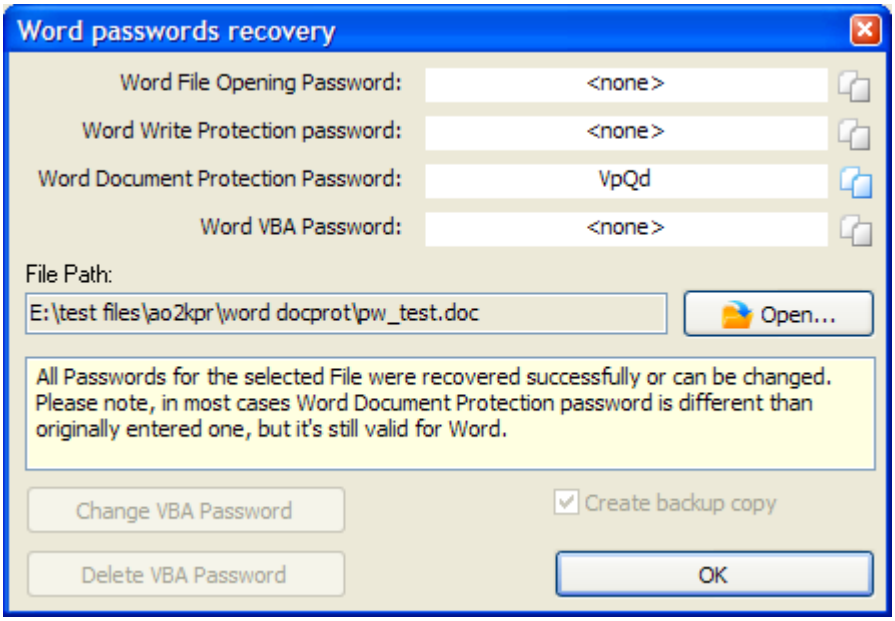
Microsoft Word

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.

Microsoft PowerPoint

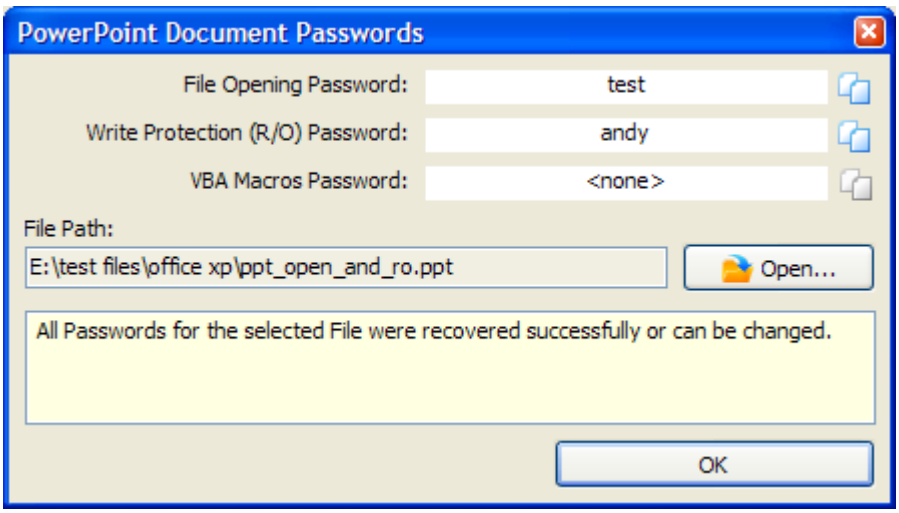
Версии **Microsoft® PowerPoint®** до PowerPoint® XP поддерживают только пароль к **VBA Project**.

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

- **Пароль на открытие**
- Пароль на изменения (Защита от записи)
- **Пароль к проекту VBA**

Пароль на открытие - это стойкий пароль, который можно восстановить **методом полного перебора или атаки по словарю**. **Подробнее об этом пароле.**

Пароль на изменения можно восстановить мгновенно. **Выберите документ** 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** в **AOPR**.

Пароль к базе данных **Microsoft® Money** 2002 и более новых версий нельзя восстановить мгновенно. **Подробнее об этом пароле.**

Microsoft Project

Microsoft® Project поддерживает следующие типы паролей:

- Пароль на открытие
- Пароль на изменения
- **Пароль к проекту VBA**

AOPR мгновенно восстанавливает эти пароли, за исключением пароля к VBA, который можно мгновенно изменить или удалить. Чтобы восстановить пароли MS Project, **откройте файл** 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:

- Запустие 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**, 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**, не отображаются.
- Максимальная длина паролей, которые восстанавливаются мгновенно, ограничена 3 символами.
- Файл журнала не создается.
- **Функция VBA Backdoor** не доступна
- **Пароли VBA** не могут быть изменены или удалены
- Надстройки Excel® (XLA) не могут быть разблокированы
- **Информация о владельце базы данных Access®** не указывается
- Для восстановления пароля можно использовать только один графический процессор

Вы можете **приобрести полную версию** **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.**

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.

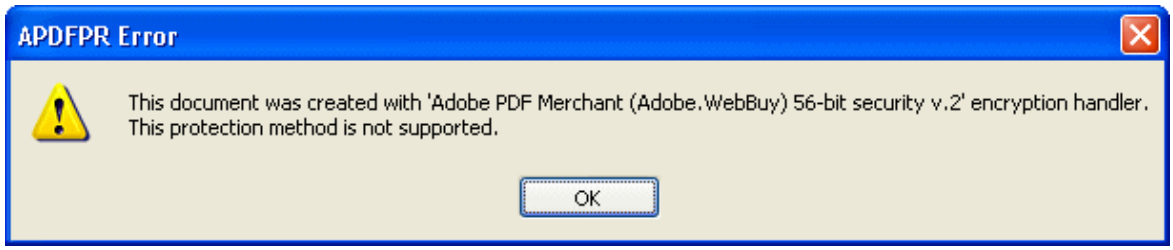
4.7.2 Системные требования

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.

- 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 измененять 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, 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.

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 JScript-код, поля формы и цифровые подписи; иногда они используются для защиты документов. APDFPR также позволяет удалить их.

4.7.3.2 Выбор атаки

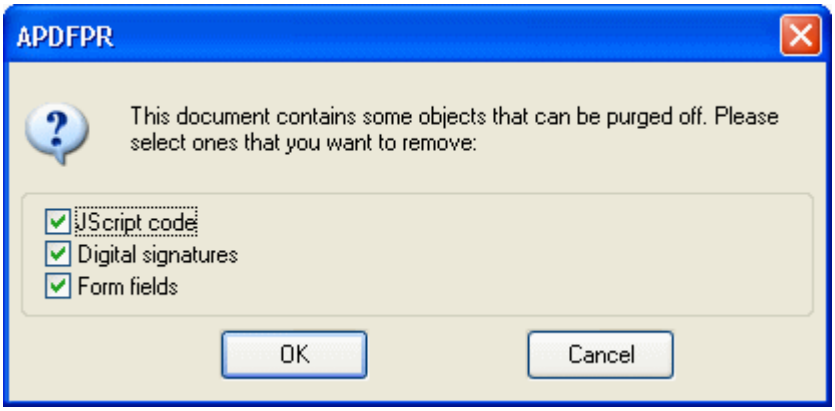
Зашифрованный PDF-файл

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

Если опция 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.

Если файл вообще не зашифрован, но содержит JScript-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), атака по маске (Mask), Атака по словарю (Dictionary) и Поиск ключа (Key search).

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 «a» до «z»), а пароль начинается с «k», введите «kaaaa». 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.

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. 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
...
PASSWORd
PASSWORD

Однако проверка всех этих комбинаций занимает много времени: в приведенном выше примере APDFPR будет проверять 2^8 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_l17000.data
0\t00_l17000.index
1\t01_l17000.data
1\t01_l17000.index
2\t02_l17000.data
2\t02_l17000.index
3\t03_l17000.data
3\t03_l17000.index
4\t04_l17000.data
4\t04_l17000.index
5\t05_l17000.data
5\t05_l17000.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.axr" (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 (tart 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).

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, а затем брутфорс 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.

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

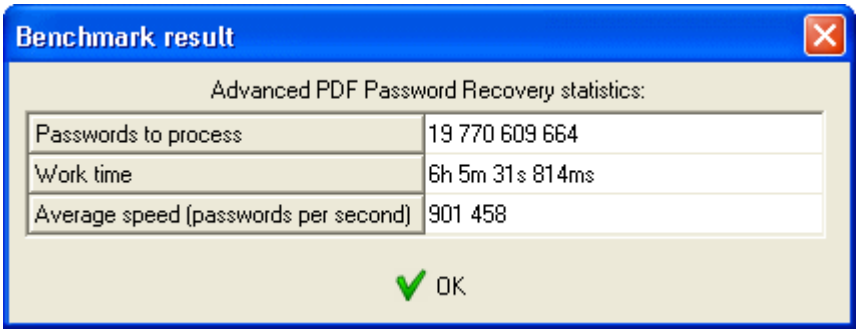
Вы можете сохранить текущие настройки APDFPR в файл AFR с помощью меню [Файл] | [Сохранить проект] или [Сохранить проект как ...] ([File] | [Save Project] или [Save Project as...]). Чтобы открыть проект, выберите [Файл] | [Открыть проект] ([File] | [Open Project]).

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

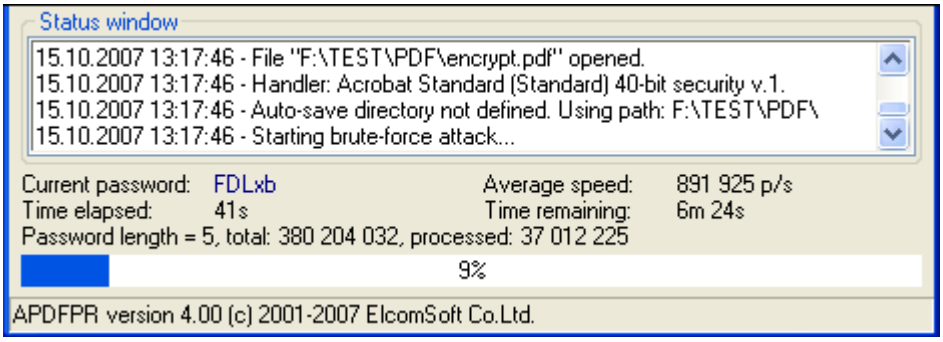
Процесс восстановления

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

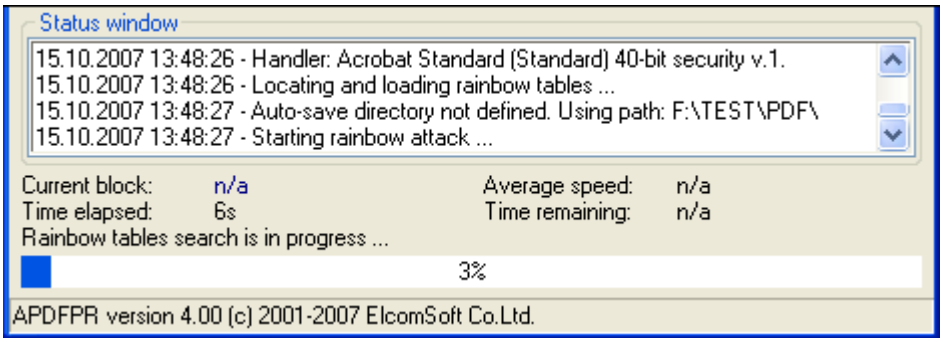
Вы можете в любой момент прервать процесс восстановления, нажав кнопку «Стоп» (Stop) или F10. Чтобы возобновить атаку или сохранить проект, обратитесь к разделам «Начать с пароля» и «Сохранение и чтение настроек».

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:

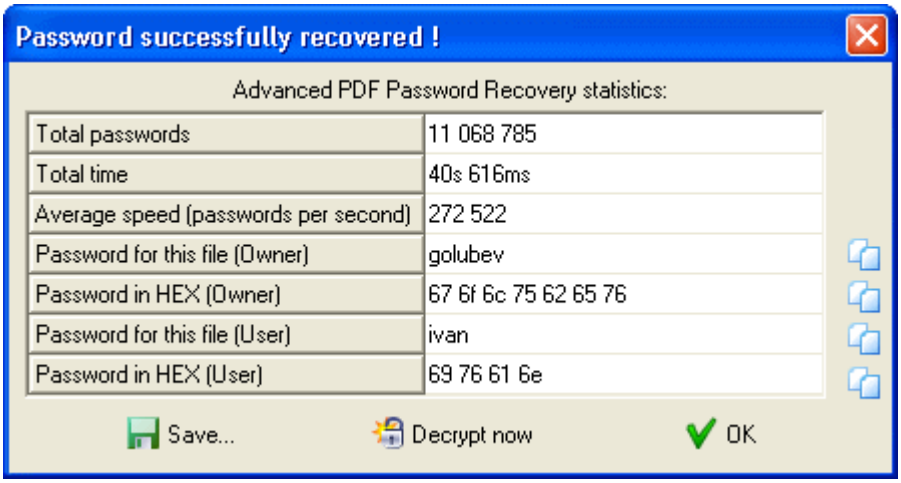


Для атаки с поиском ключа с использованием предварительно вычисленных хэш-таблиц отображается только прошедшее время (*примечание: эта атака обычно занимает не более нескольких минут*):



Результаты

После того, как пароль найден, отображается следующее окно:

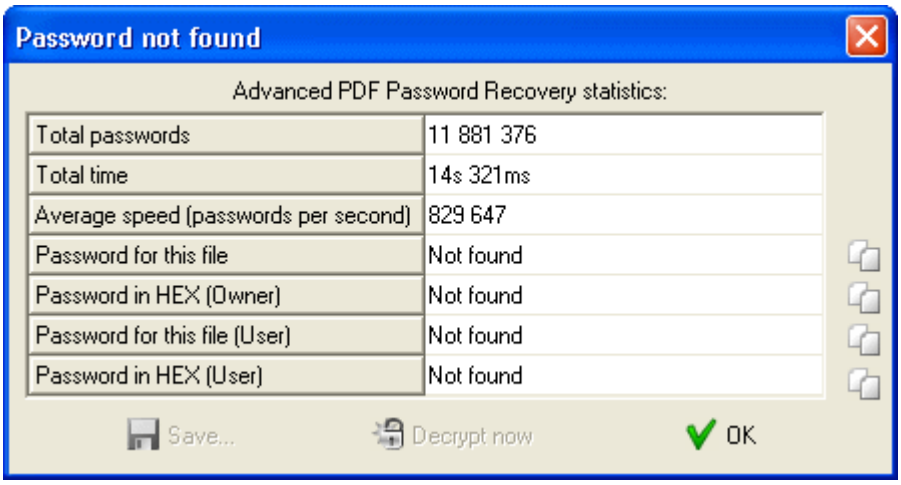


В последней строке отображается пароль в шестнадцатеричной форме, (для удобства, если пароль содержит мультиязычные символы, не поддерживаемые вашей локализацией).

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

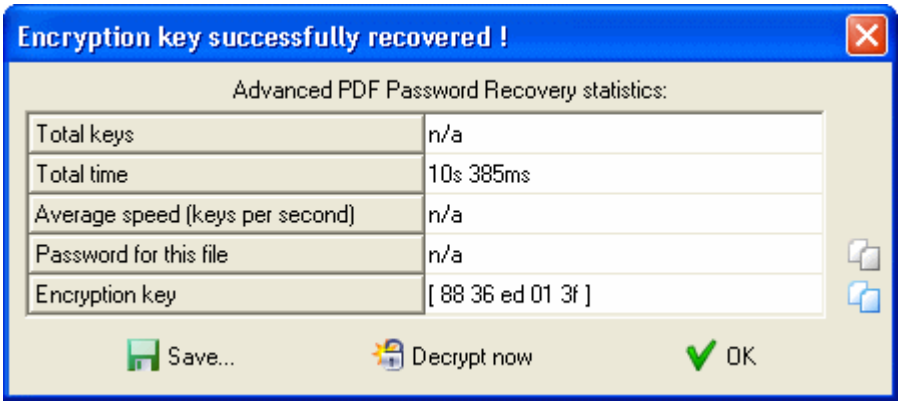
Программа также показывает тип пароля: «пользователь» или «владелец». Чтобы мгновенно расшифровать или сразу же снять защиту с файла с помощью восстановленного пароля, нажмите кнопку «Расшифровать сейчас» (Decrypt now).

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).

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. 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.

-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:csdepa	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 afr-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 удается 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 пароей пользователей и администраторов в Sage PeachTree Accounting, обеспечивая гарантированный мгновенный доступ к защищенному паролем ACT! 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 ACT! (локально или удаленно). Advanced Sage Password Recovery мгновенно обнаруживает паролик документам всех версий ACT! включая последнюю версию (v22). Также есть возможность смены роли учетных записей пользователей с "режима ограниченного доступа" до администратора в ACT! БД.
4. Получения мгновенного доступа к содержимому защищенных паролем документов ACT! (*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 7или выше

4.8.2.2 Восстановление паролей для ACT!

Чтобы восстановить пароли к файлам, созданным в более старых версиях ACT!, нажмите Открыть файл... (Open file...) и выберите Symantec ACT!, затем найдите файлы *.blb или *.mud. Или перетащите ACT!-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.

ACT! 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 ACT! (через драйверы MSSQL ODBC, используемые ACT!) и напрямую. Чтобы использовать первый метод, у вас на локальном ПК должна быть установлена соответствующая версия ACT!, при этом к файлу *.adf можно получить доступ удаленно; второй способ работает даже без ACT!, но не позволяет изменять роли пользователей.

При первом способе нажмите Открыть файл... (Open file...), выберите ACT! 2005-2019 ODBC и найдите файл *.adf (база данных ACT!) Или файл *.pad (информация о базе данных ACT!, - 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 ACT! НЕ на том же компьютере, на котором база данных была открыта в последний раз, мы рекомендуем открыть его в ACT! на этом ПК прежде чем продолжить. Когда ACT! запросит пароль, нажмите Отмена (Cancel), - эти действия позволят ACT! 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 ACT! 2005-2019 прямо из меню и найдите файл *.adf (база данных ACT!). Если этот файл зашифрован именно с ACT!, 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 ACT! 2005..2019 и измените пароль для любого пользователя, новые пароли всегда переведутся в нижний регистр для совместимости с ACT! 2005 (где пароли не чувствительны к регистру). Кроме того, после смены пароля ACT! примет его при первом входе в ACT! с новым паролем, но может попросить изменить его в соответствии с политикой паролей.

ACT! 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 инстансов 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. И 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 WordPerefect): 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\Corel\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.

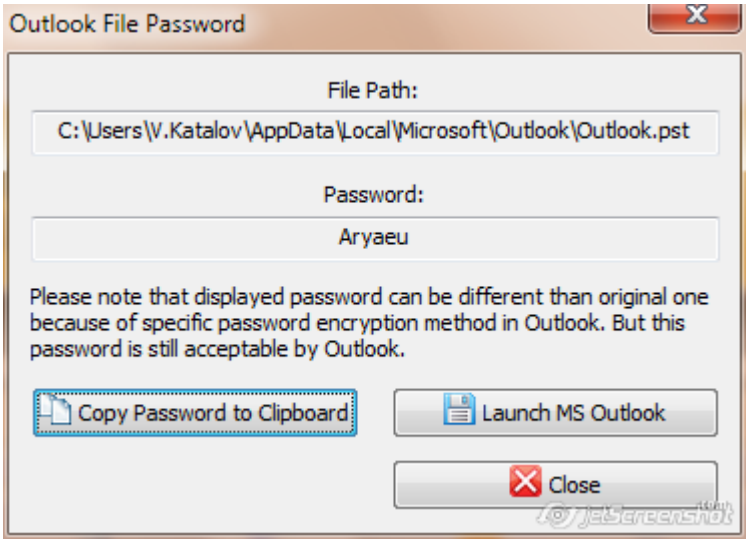
4.11.2 О программе

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.*

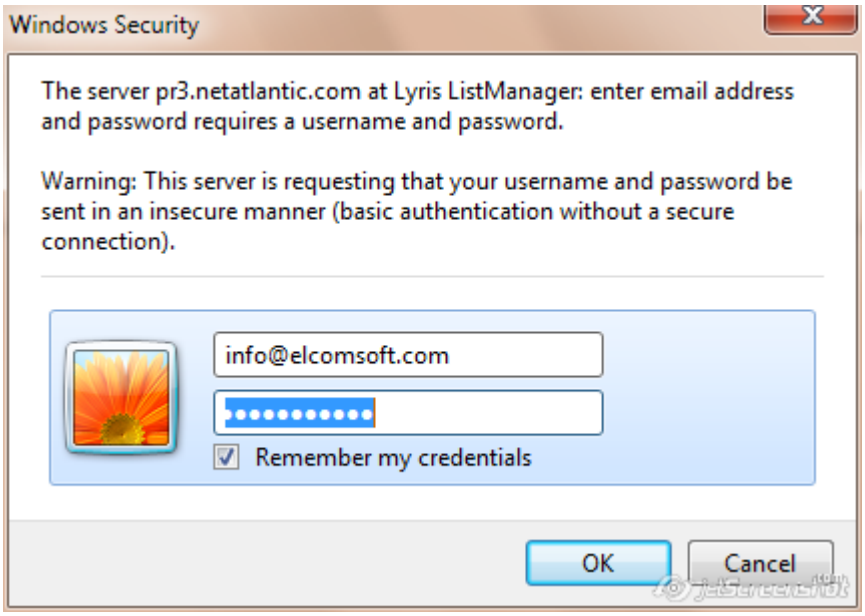


Обратите внимание, что в некоторых случаях пароль, восстановленный EINPB, может не совпадать с исходным паролем. Это ожидаемое поведение из-за алгоритма шифрования, используемого в Outlook. Восстановленный пароль будет принят Outlook, даже если он не соответствует оригиналу.

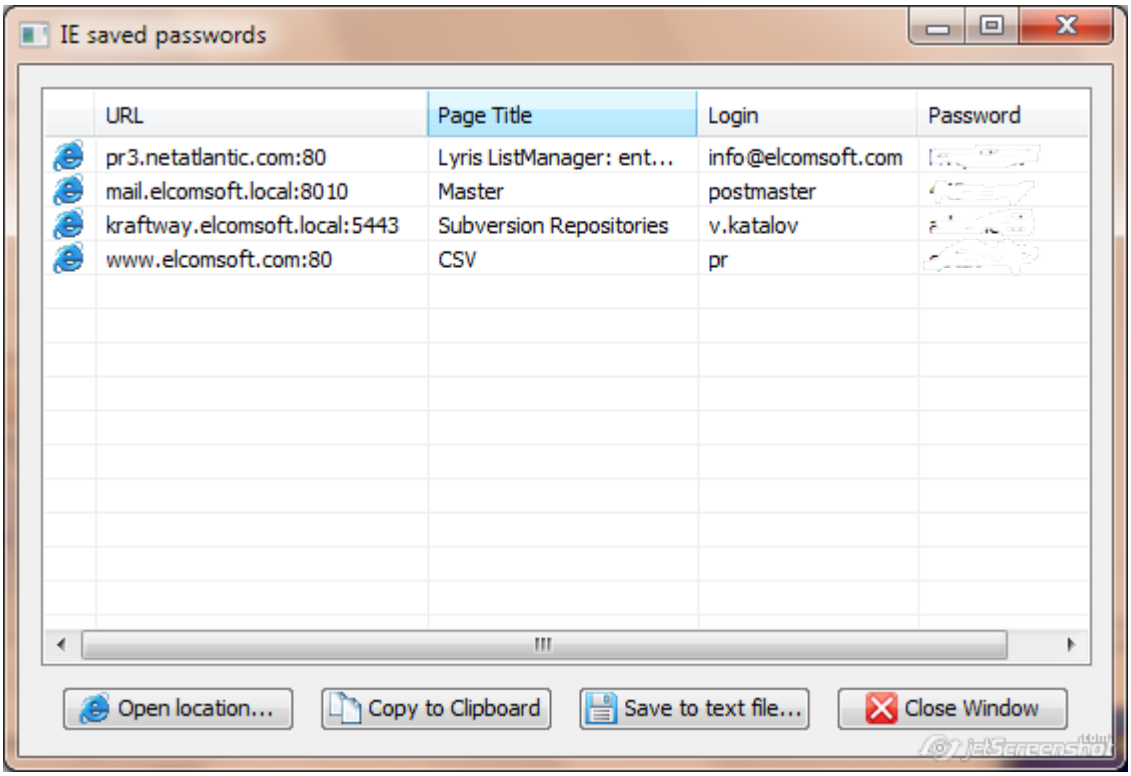
4.11.2.3 Internet Explorer пароли

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):

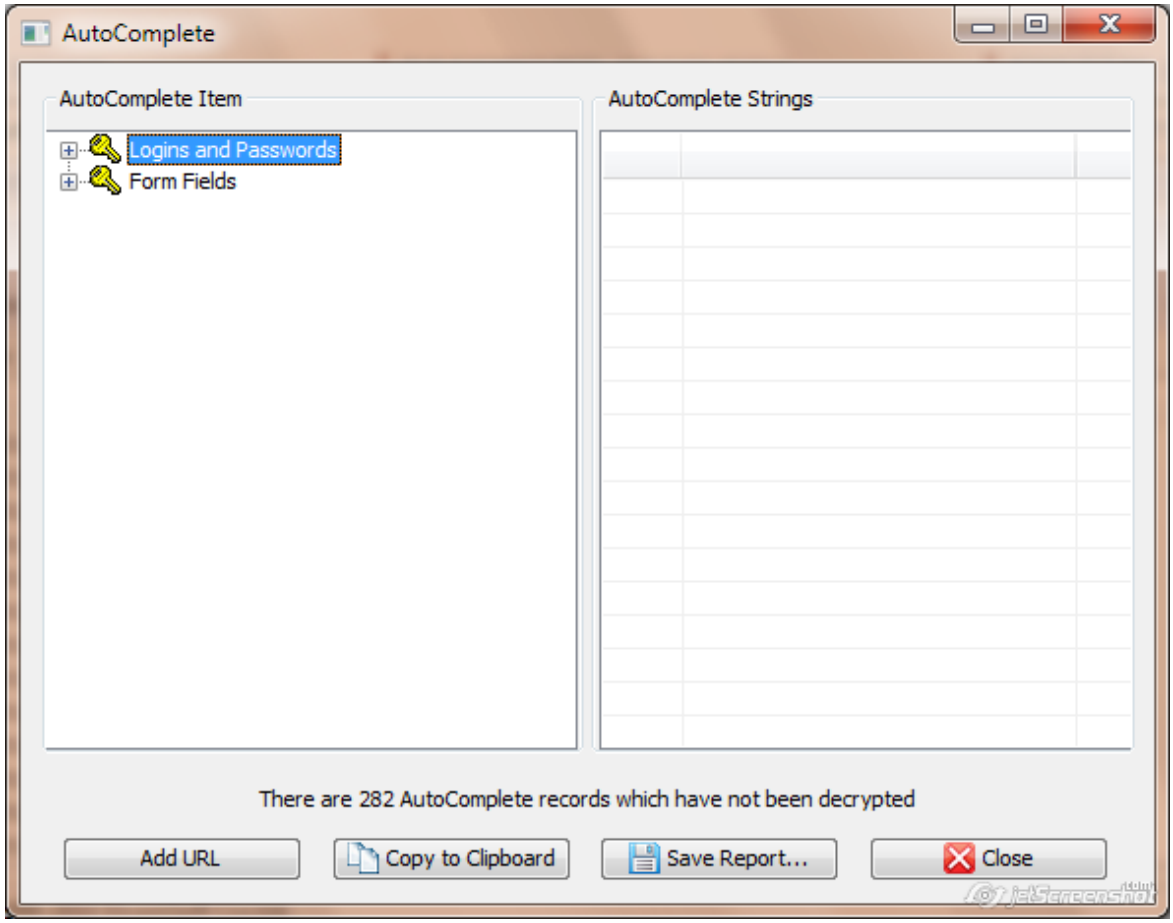


URL-адрес обычно содержит корневой URL. Заголовок страницы - это область, установленная сервером. Для FTP-сайтов он всегда пуст; для веб-сайтов он может содержать заголовок защищенной паролем страницы или имя HTML-файла.

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 «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.

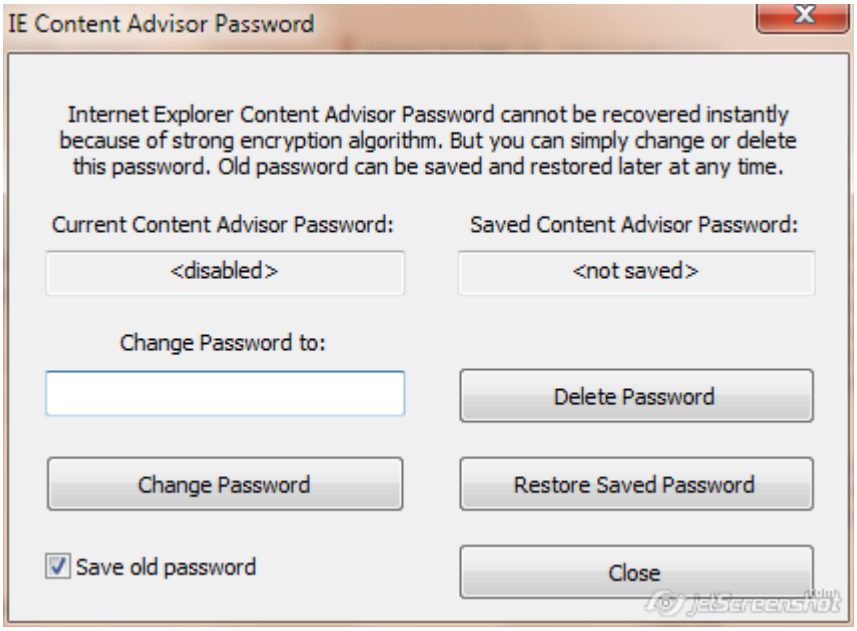
Кнопка «Сохранить отчет» (Save Report) сохраняет всю информацию автозаполнения в текстовый файл Unicode.

Важно: если пароли к некоторым веб-сайтам не отображаются, даже если *включен параметр «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-браузеров, 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).*

Mozila Firefox: обратите внимание, что для восстановления паролей, сохраненных в Mozila 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.

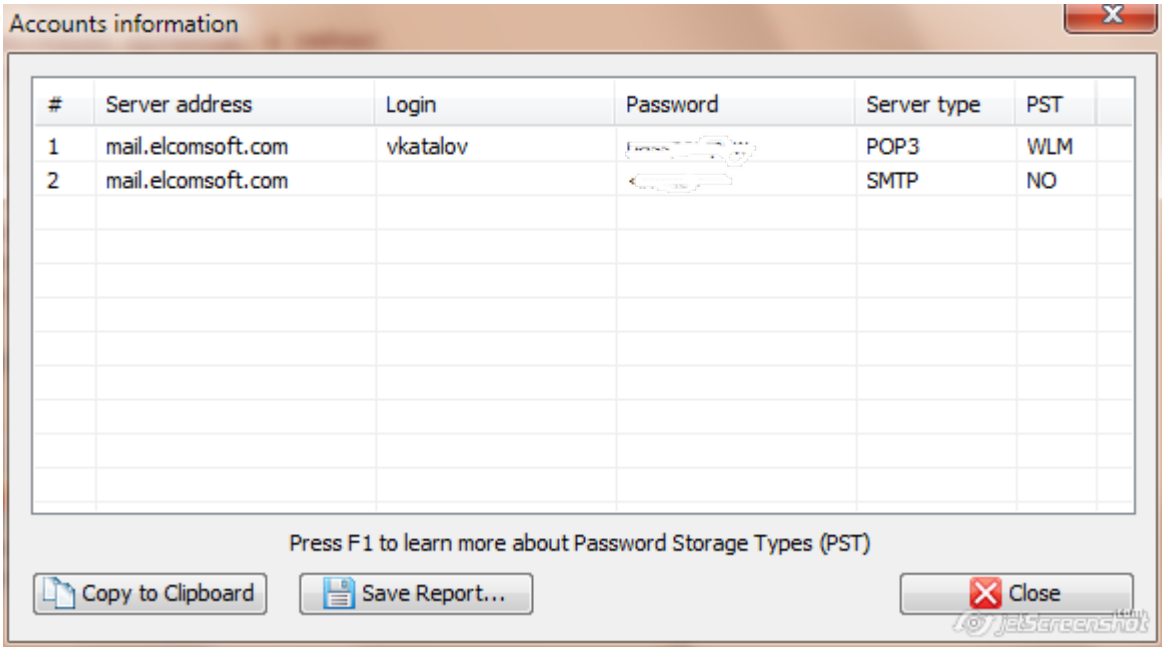
4.11.2.5 Пароли почты и новостей

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

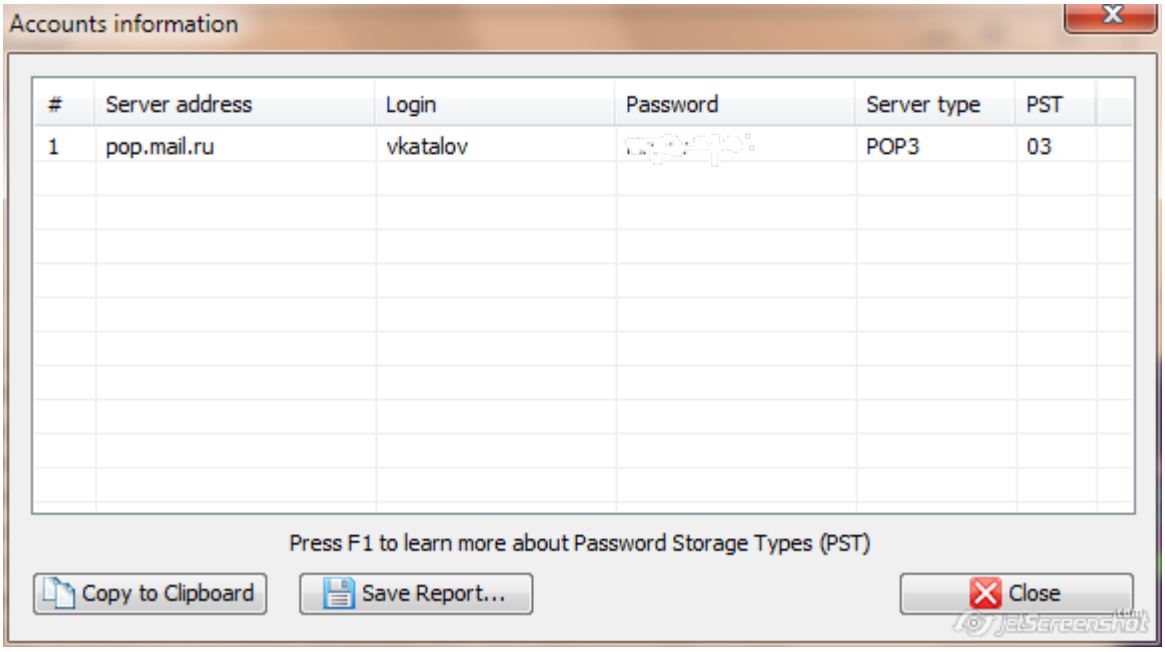
- Аккаунты почты (Outlook Express, Windows Mail и Windows Live Mail, Outlook) - Mail accounts
- Аккаунты новостей (Outlook Express, Windows Mail и Windows Live Mail) - News accounts
- Outlook Express - Identities

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. Для Outlook Express и Windows [Live] Mail:

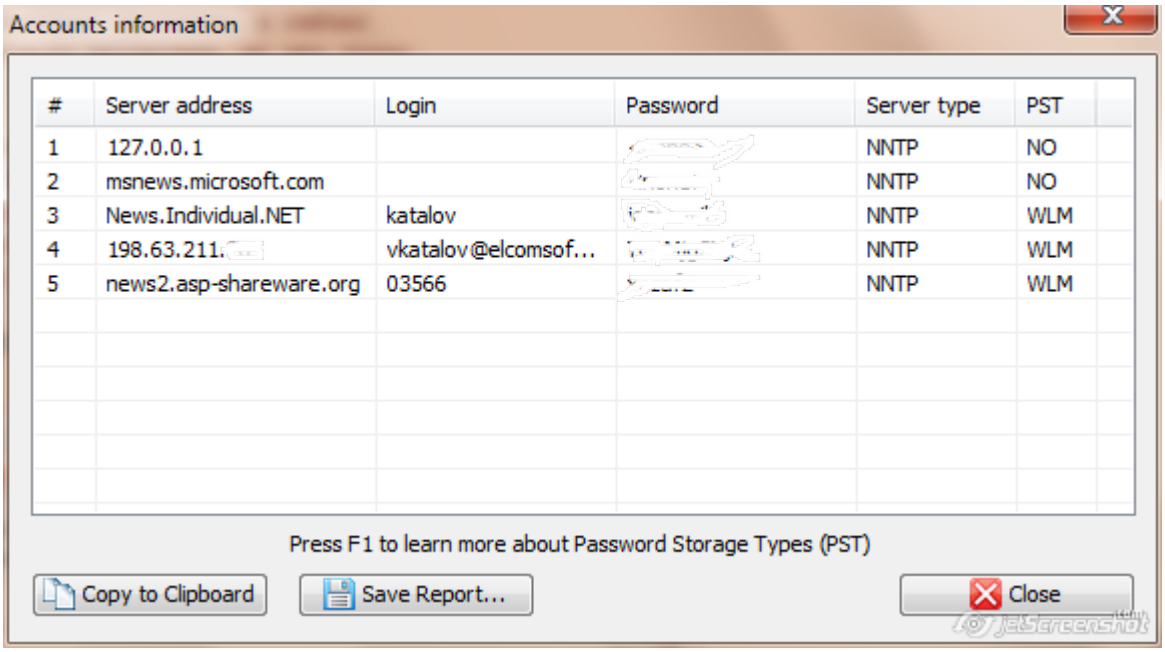


Для Outlook 98, 2000, 2002 / XP, 2003, 2007, 2010 и 2013 (Outlook 97 официально не поддерживается, но все еще может работать) вы также можете восстановить информацию об учетных записях электронной почты, которая в ней хранится (адрес сервера, логин, пароль и тип сервера). Нажмите Учетные записи Outlook (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.

News accounts



Identities

Для индентификаторов 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. Попытайтесь 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. *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 снифферoм 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 снифферoм, 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

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 AipPCap, 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.

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.

Общие настройки (General options)

Когда атака закончится, переключитесь на следующий хеш-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.

Снифер беспроводной сети: установите параметры сниффинга беспроводной сети:

- Установить / переустановить драйвер ESNDISMON
- Сворачивать программу в трэй
- Отображать перехваченные пакеты в .pcap-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

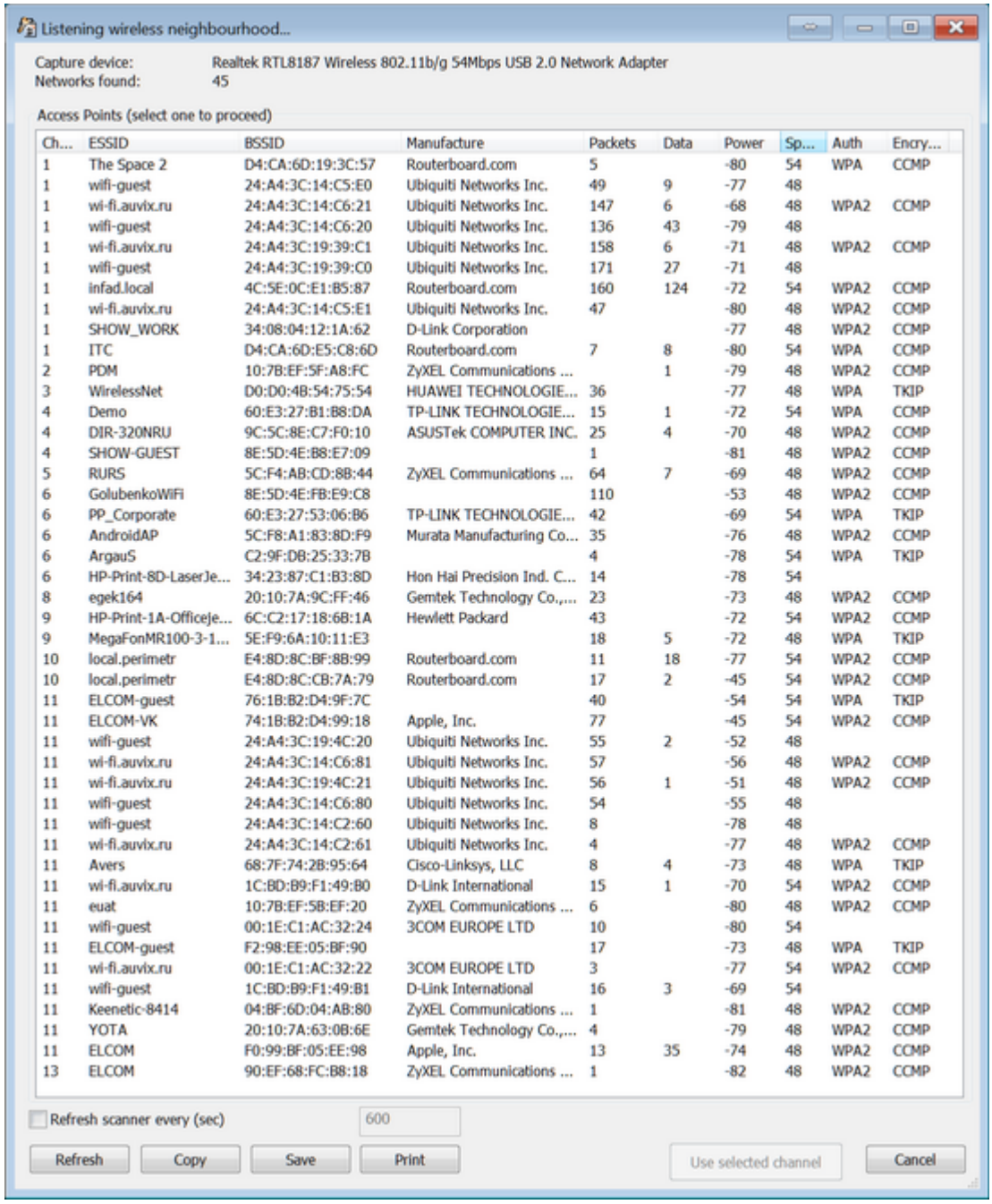
Чтобы начать захват сетевых пакетов, выберите сниффер WiFi на панели инструментов или сниффер AirPCap, если у вас есть адаптер AirPCap. У вас должны быть установлены драйвера; прочтите установка NDIS драйвера для получения более подробной информации.

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).

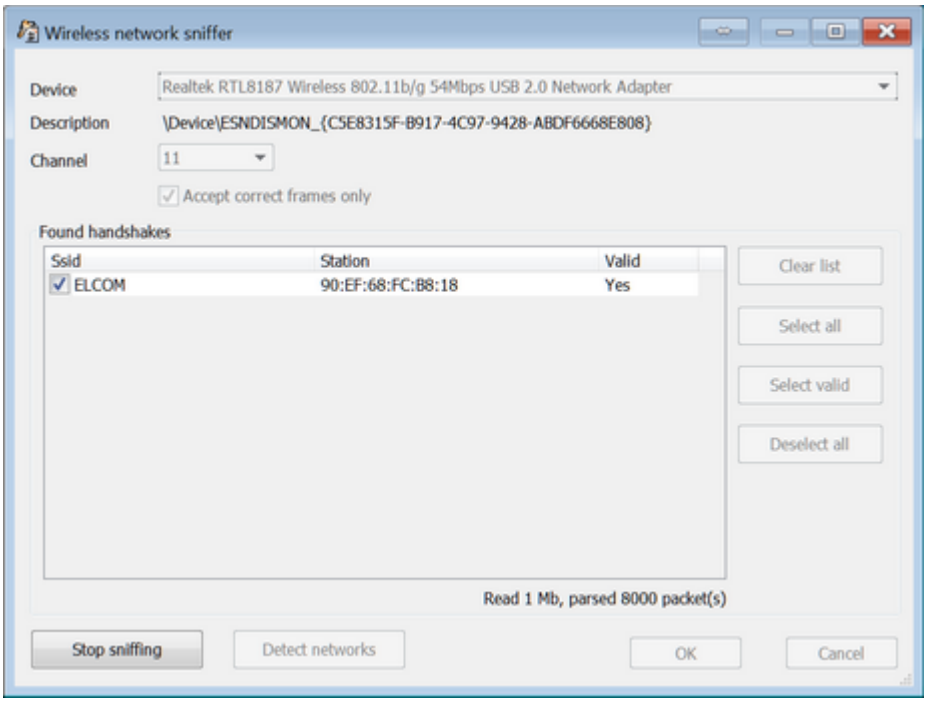
После установки драйверов для адаптера и драйверов NDIS выберите правильное устройство (для адаптеров AipPCap оно обычно указано как \\. \airpcap00 device), выберите канал и нажмите [OK]. Если вы не уверены в канале, нажмите [Определить сети] (Detect networks), и программа начнет мониторинг всех каналов;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



Ch...	ESSID	BSSID	Manufacture	Packets	Data	Power	Sp...	Auth	Encry...
1	The Space 2	D4:CA:6D:19:3C:57	Routerboard.com	5		-80	54	WPA	CCMP
1	wifi-guest	24:A4:3C:14:C5:E0	Ubiquiti Networks Inc.	49	9	-77	48		
1	wi-fi.auvix.ru	24:A4:3C:14:C6:21	Ubiquiti Networks Inc.	147	6	-68	48	WPA2	CCMP
1	wifi-guest	24:A4:3C:14:C6:20	Ubiquiti Networks Inc.	136	43	-79	48		
1	wi-fi.auvix.ru	24:A4:3C:19:39:C1	Ubiquiti Networks Inc.	158	6	-71	48	WPA2	CCMP
1	wifi-guest	24:A4:3C:19:39:C0	Ubiquiti Networks Inc.	171	27	-71	48		
1	infad.local	4C:5E:0C:E1:B5:87	Routerboard.com	160	124	-72	54	WPA2	CCMP
1	wi-fi.auvix.ru	24:A4:3C:14:C5:E1	Ubiquiti Networks Inc.	47		-80	48	WPA2	CCMP
1	SHOW_WORK	34:08:04:12:1A:62	D-Link Corporation			-77	48	WPA2	CCMP
1	ITC	D4:CA:6D:E5:C8:6D	Routerboard.com	7	8	-80	54	WPA	CCMP
2	PDM	10:7B:EF:5F:A8:FC	ZyXEL Communications ...		1	-79	48	WPA2	CCMP
3	WirelessNet	D0:D0:4B:54:75:54	HUAWEI TECHNOLOGIE...	36		-77	48	WPA	TKIP
4	Demo	60:E3:27:B1:B8:DA	TP-LINK TECHNOLOGIE...	15	1	-72	54	WPA	CCMP
4	DIR-320NRU	9C:5C:8E:C7:F0:10	ASUSTek COMPUTER INC.	25	4	-70	48	WPA2	CCMP
4	SHOW-GUEST	8E:5D:4E:B8:E7:09		1		-81	48	WPA2	CCMP
5	RURS	5C:F4:AB:CD:8B:44	ZyXEL Communications ...	64	7	-69	48	WPA2	CCMP
6	GolubenkoWiFi	8E:5D:4E:FB:E9:C8		110		-53	48	WPA2	CCMP
6	PP_Corporate	60:E3:27:53:06:B6	TP-LINK TECHNOLOGIE...	42		-69	54	WPA	TKIP
6	AndroidAP	5C:F8:A1:83:8D:F9	Murata Manufacturing Co...	35		-76	48	WPA2	CCMP
6	ArgauS	C2:9F:DB:25:33:7B		4		-78	54	WPA	TKIP
6	HP-Print-8D-LaserJe...	34:23:87:C1:B3:8D	Hon Hai Precision Ind. C...	14		-78	54		
8	egek164	20:10:7A:9C:FF:46	Gemtek Technology Co.,...	23		-73	48	WPA2	CCMP
9	HP-Print-1A-Officeje...	6C:C2:17:18:6B:1A	Hewlett Packard	43		-72	54	WPA2	CCMP
9	MegaFonMR100-3-1...	5E:F9:6A:10:11:E3		18	5	-72	48	WPA	TKIP
10	local.perimetr	E4:8D:8C:BF:8B:99	Routerboard.com	11	18	-77	54	WPA2	CCMP
10	local.perimetr	E4:8D:8C:CB:7A:79	Routerboard.com	17	2	-45	54	WPA2	CCMP
11	ELCOM-guest	76:1B:B2:D4:9F:7C		40		-54	54	WPA	TKIP
11	ELCOM-VK	74:1B:B2:D4:99:18	Apple, Inc.	77		-45	54	WPA2	CCMP
11	wifi-guest	24:A4:3C:19:4C:20	Ubiquiti Networks Inc.	55	2	-52	48		
11	wi-fi.auvix.ru	24:A4:3C:14:C6:81	Ubiquiti Networks Inc.	57		-56	48	WPA2	CCMP
11	wi-fi.auvix.ru	24:A4:3C:19:4C:21	Ubiquiti Networks Inc.	56	1	-51	48	WPA2	CCMP
11	wifi-guest	24:A4:3C:14:C6:80	Ubiquiti Networks Inc.	54		-55	48		
11	wifi-guest	24:A4:3C:14:C2:60	Ubiquiti Networks Inc.	8		-78	48		
11	wi-fi.auvix.ru	24:A4:3C:14:C2:61	Ubiquiti Networks Inc.	4		-77	48	WPA2	CCMP
11	Avers	68:7F:74:2B:95:64	Cisco-Linksys, LLC	8	4	-73	48	WPA	TKIP
11	wi-fi.auvix.ru	1C:BD:B9:F1:49:B0	D-Link International	15	1	-70	54	WPA2	CCMP
11	euat	10:7B:EF:5B:EF:20	ZyXEL Communications ...	6		-80	48	WPA2	CCMP
11	wifi-guest	00:1E:C1:AC:32:24	3COM EUROPE LTD	10		-80	54		
11	ELCOM-guest	F2:98:EE:05:BF:90		17		-73	48	WPA	TKIP
11	wi-fi.auvix.ru	00:1E:C1:AC:32:22	3COM EUROPE LTD	3		-77	54	WPA2	CCMP
11	wifi-guest	1C:BD:B9:F1:49:B1	D-Link International	16	3	-69	54		
11	Keenetic-8414	04:BF:6D:04:AB:80	ZyXEL Communications ...	1		-81	48	WPA2	CCMP
11	YOTA	20:10:7A:63:0B:6E	Gemtek Technology Co.,...	4		-79	48	WPA2	CCMP
11	ELCOM	F0:99:BF:05:EE:98	Apple, Inc.	13	35	-74	48	WPA2	CCMP
13	ELCOM	90:EF:68:FC:B8:18	ZyXEL Communications ...	1		-82	48	WPA2	CCMP

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 pcap-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 сниффинг» (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 незарегестрированной версии и Регистрация).

Если у вас нет совместимого беспроводного адаптера, есть альтернативные способы импорта необходимых данных. tcpdump - это обычный сниффер 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 снифферов 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 сниффера программа предлагает установить драйвер ESNDISMON. Без драйвера программа не может выполнять сниффинг. 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

4. Перезагрузите систему; это обязательно для большинства адаптеров, даже если не было запроса на перезагрузку.

5. Установите EWSA.

6. Запустите сниффер 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 тут. 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, переформатировании 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 запрещён.

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 зашифрованны 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 aefsdr.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, Scan for encrypted files, Browse for encrypted files и Decrypting files.

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. 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.

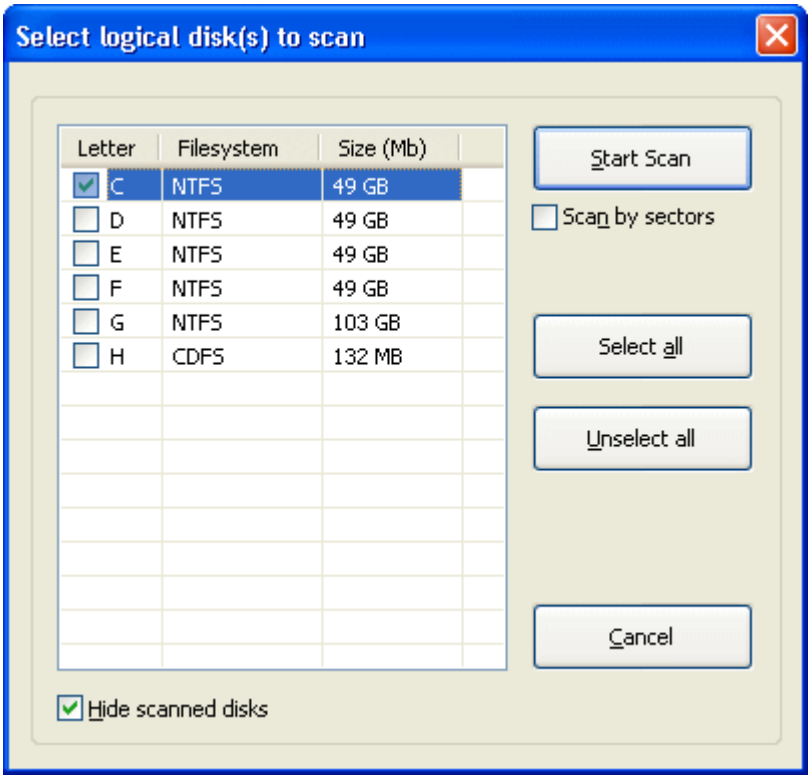
Нажимайте кнопки «Вперёд» и «Назад» для навигации по мастеру; например, вы можете вернуться к одному из предыдущих шагов, чтобы просканировать другой диск на предмет ключей или файлов, или добавить дополнительные пароли, если определенные ключи не были расшифрованы.

5.1.2.4 Поиск ключей шифрования

Введение

Если вы ранее экспортировали закрытый ключ EFS агента восстановления (и у вас есть файл .pfx), нажмите кнопку «Добавить сертификат», найдите файл .pfx и введите его пароль. Теперь AEFSDR может использовать .pfx 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:

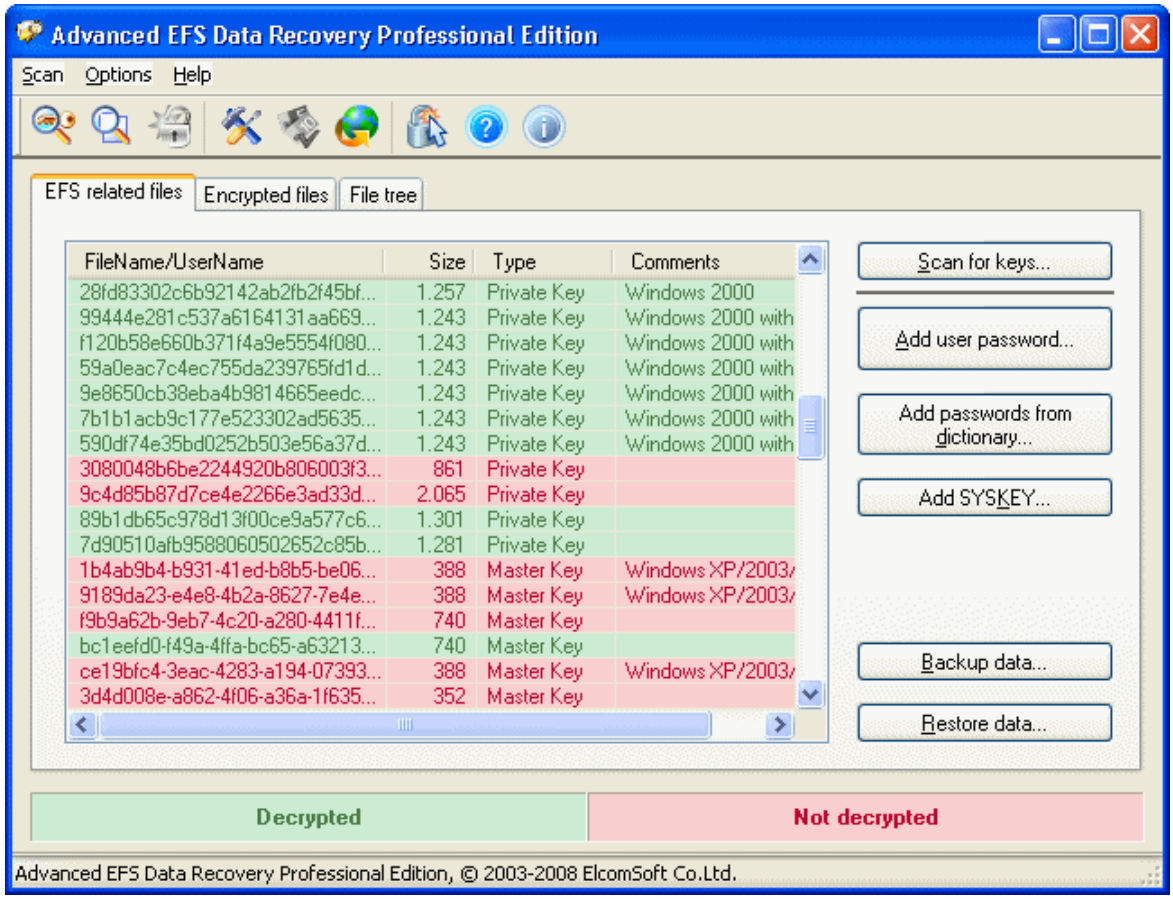


Здесь вы должны выбрать загрузочный диск (загрузочный диск Windows), на котором находятся системный реестр и ключи шифрования. Однако в некоторых случаях ключи шифрования находятся на другом диске. Если вы не уверены, просканируйте несколько дисков.

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 низкогом 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 или Обзор зашифрованных файлов. 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.

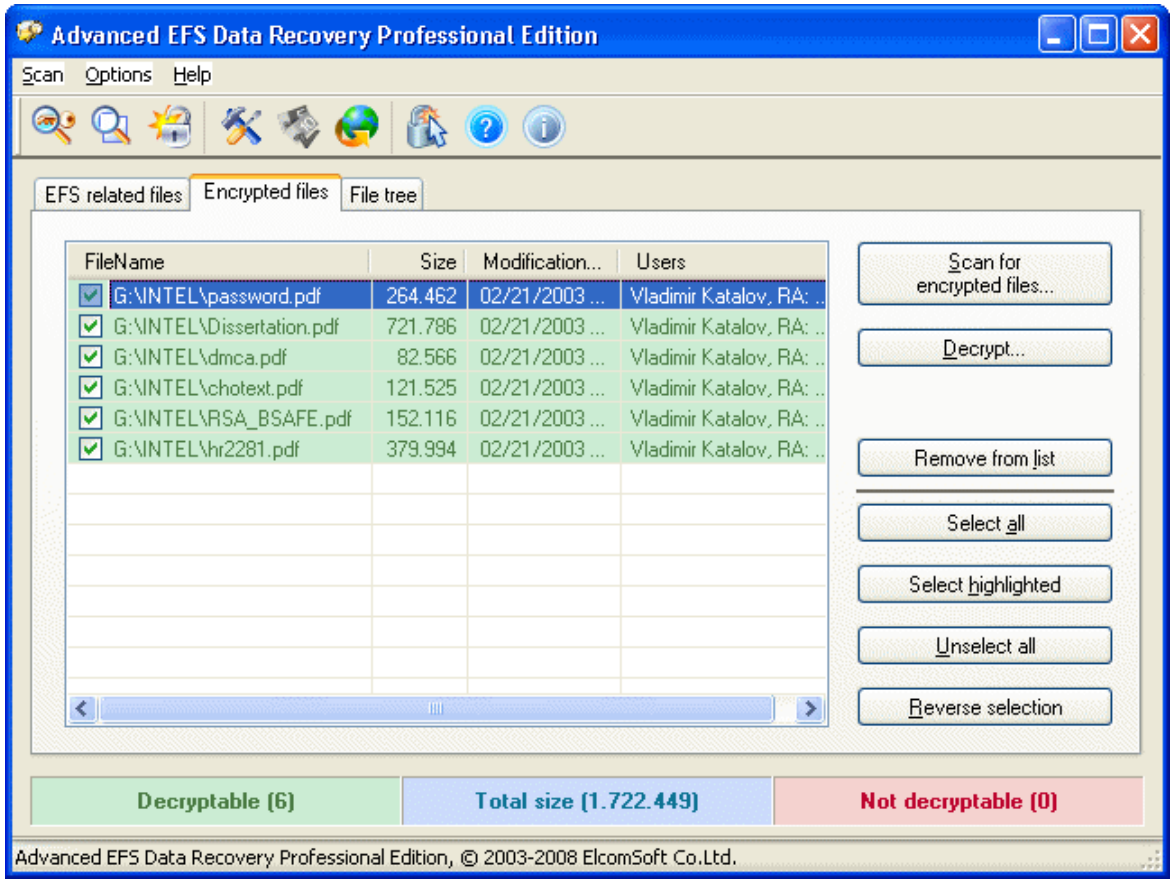
5.1.2.5 Поиск зашифрованных файлов

После того, как ключи найдены и расшифрованы, 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.

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 шифрованная 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

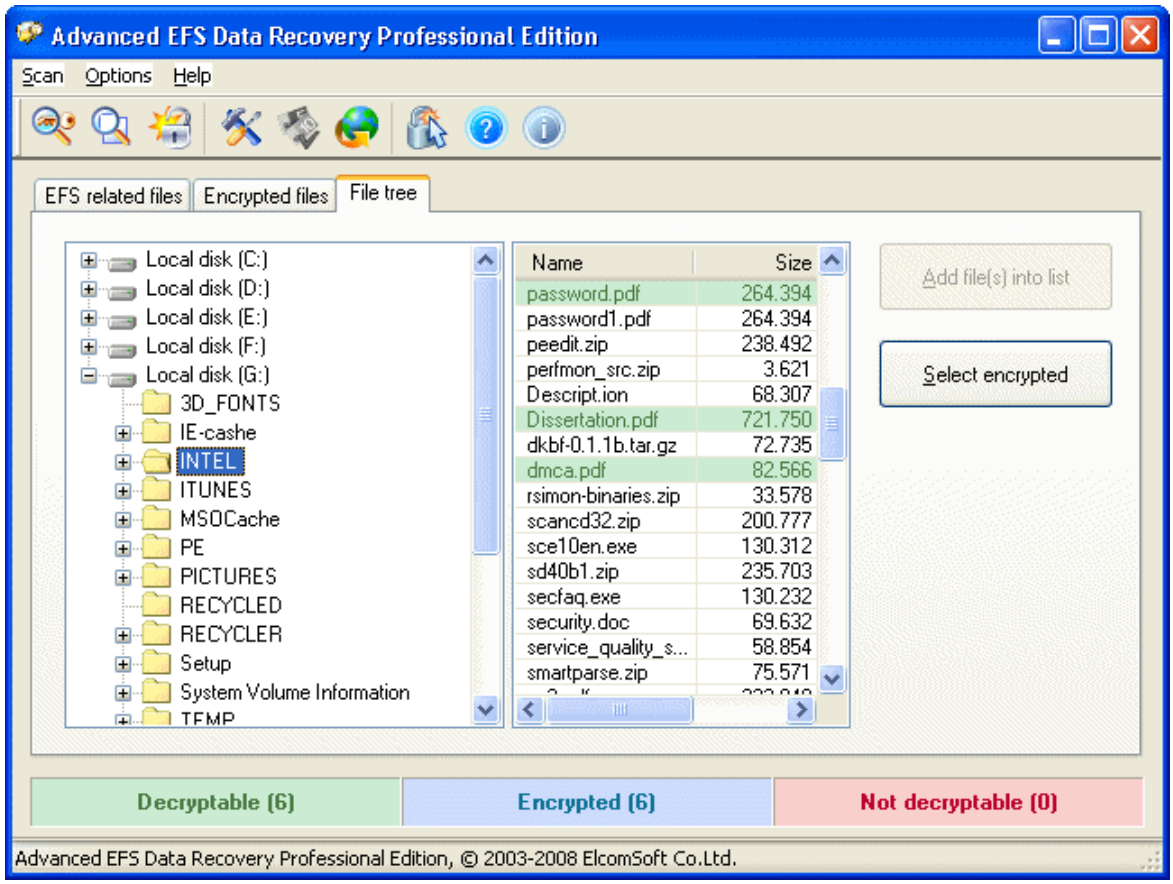
Имя (в данном примере «John Doe») - это имя пользователя, который зашифровал файл. Имена, следующие за аббревиатурой RA: - это агенты восстановления («Ivan Ivanov»), если они существуют.

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 (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.

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.

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), 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 и Обзор зашифрованных файлов) после успешного восстановления ключей, 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 удается 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:

aefsdr.exe -debug_log

В этом случае в корневой папке диска C будет создан aefsdr.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. 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.

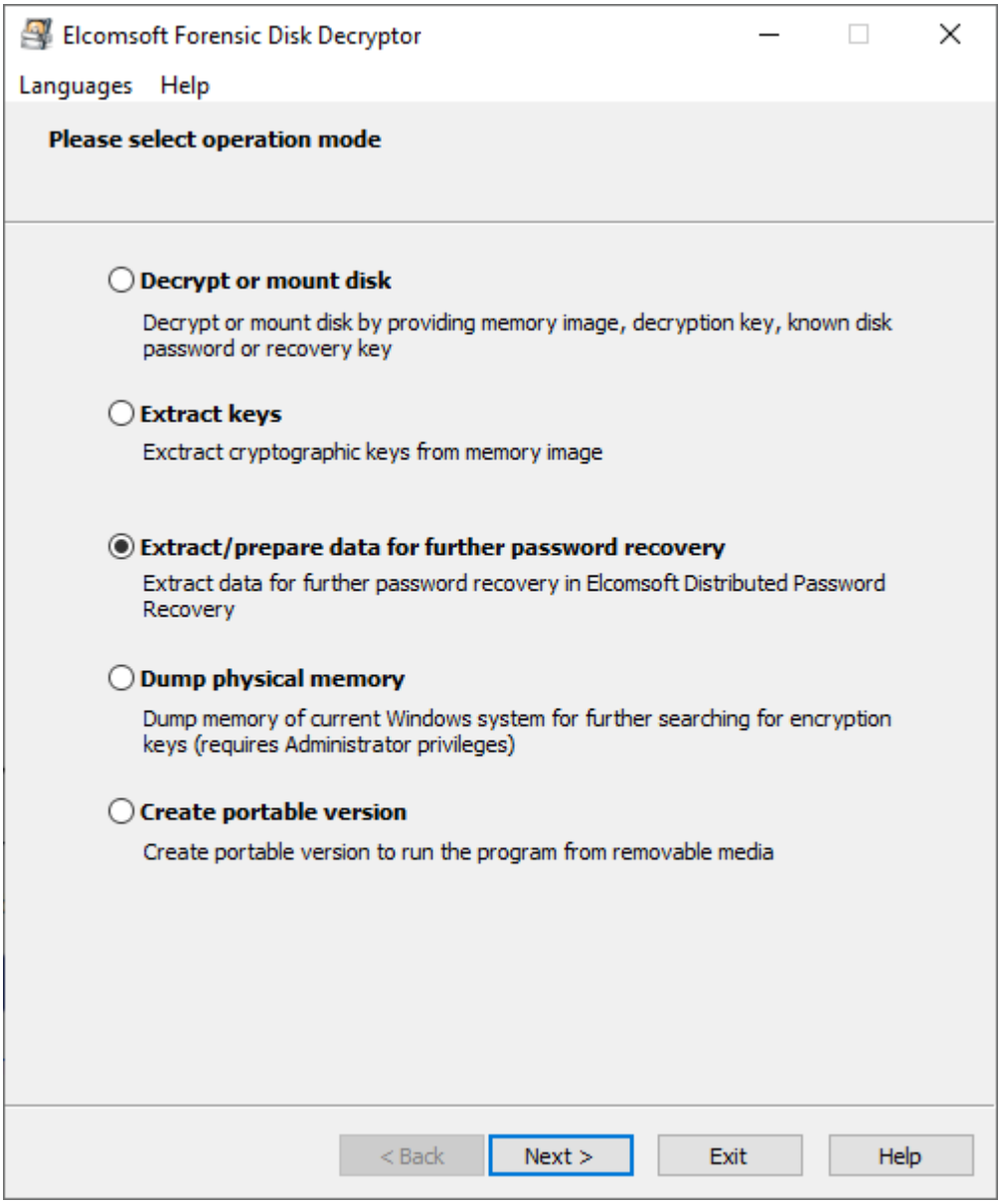
5.2.2 О программе

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.

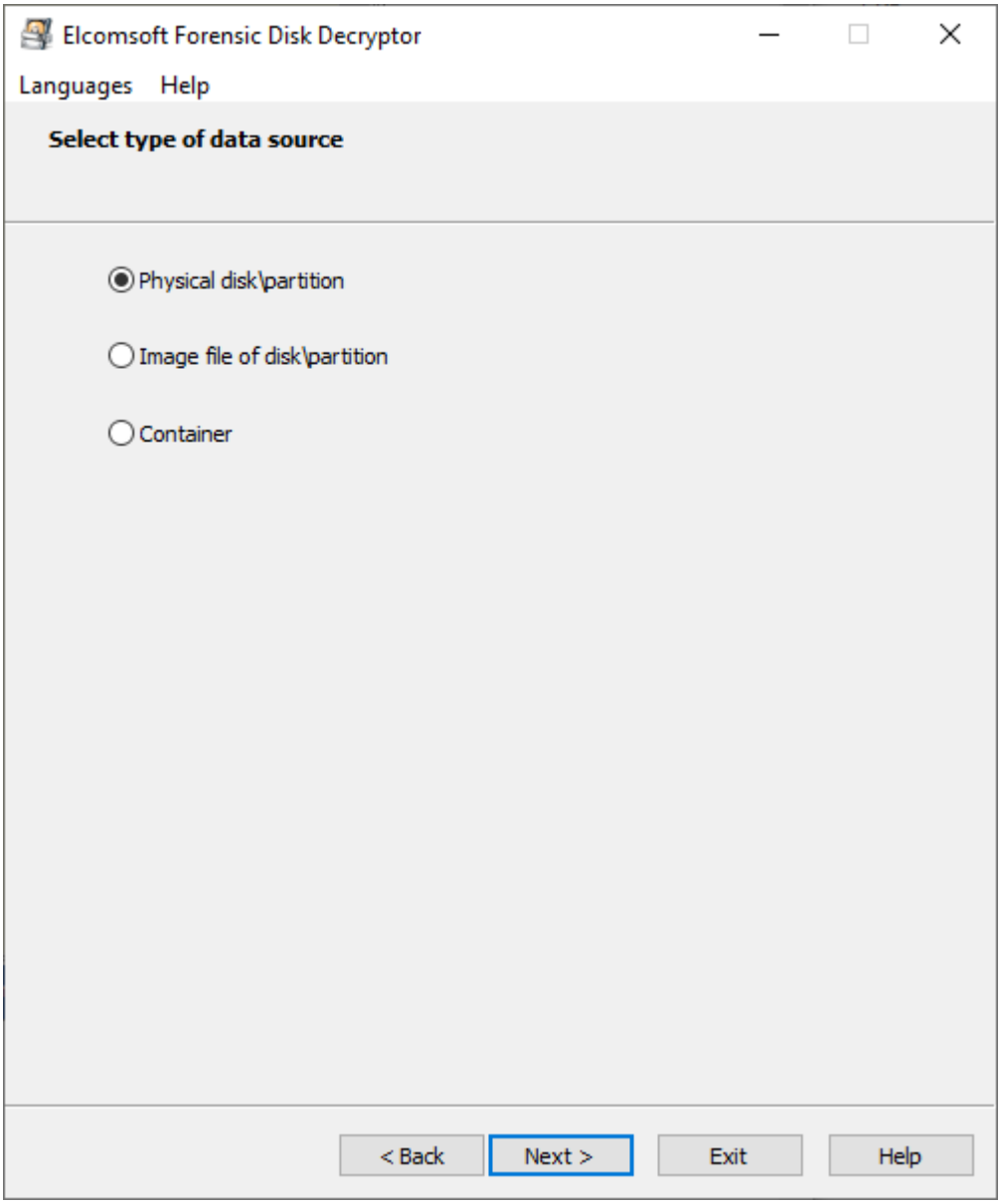
Извлечение ключей (Extract keys)

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.

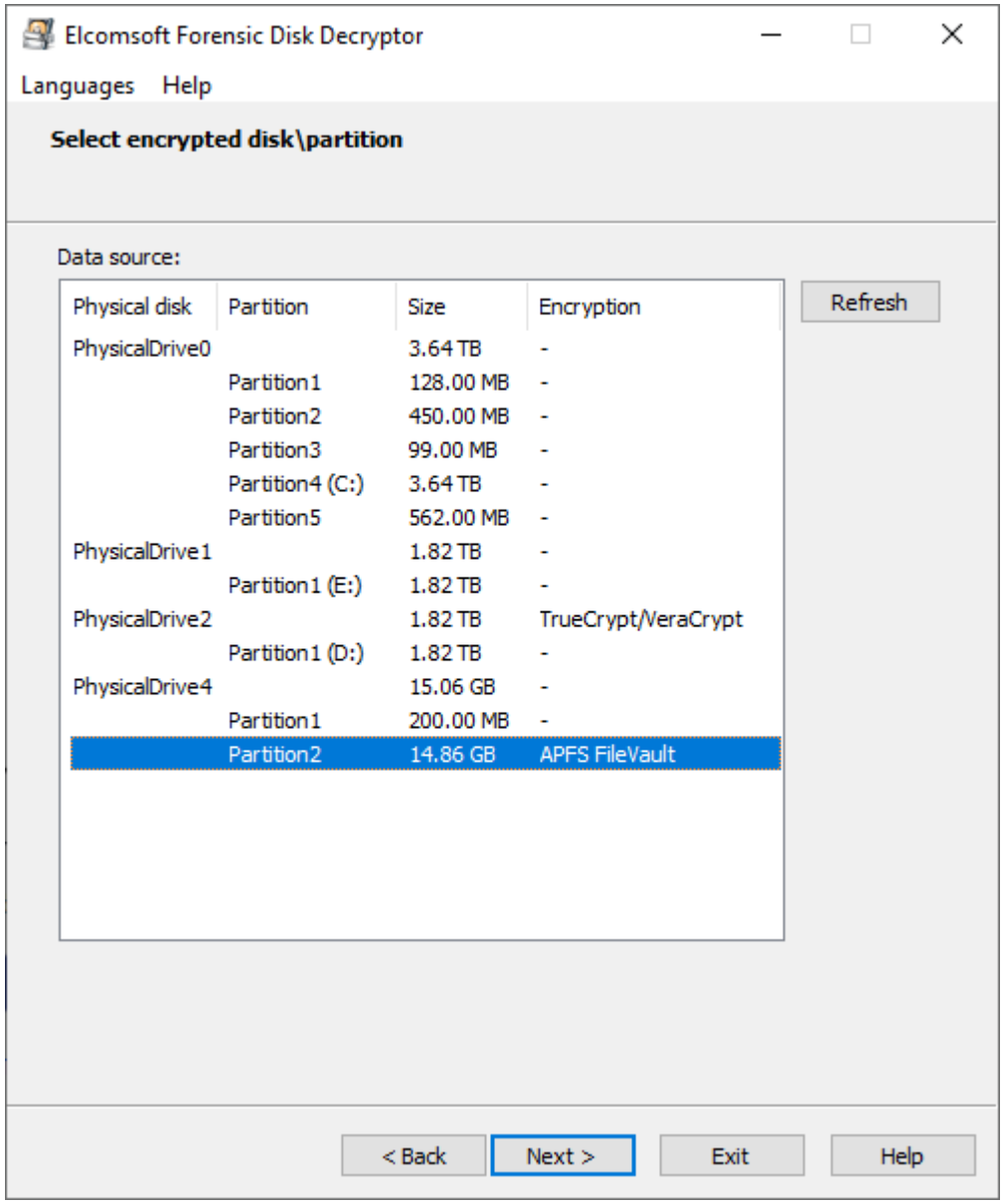
Извлечение/подготовка данных (Extract/prepare data)

Если пароль неизвестен, отсутствуют ключи восстановления, дамп памяти или файл 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:



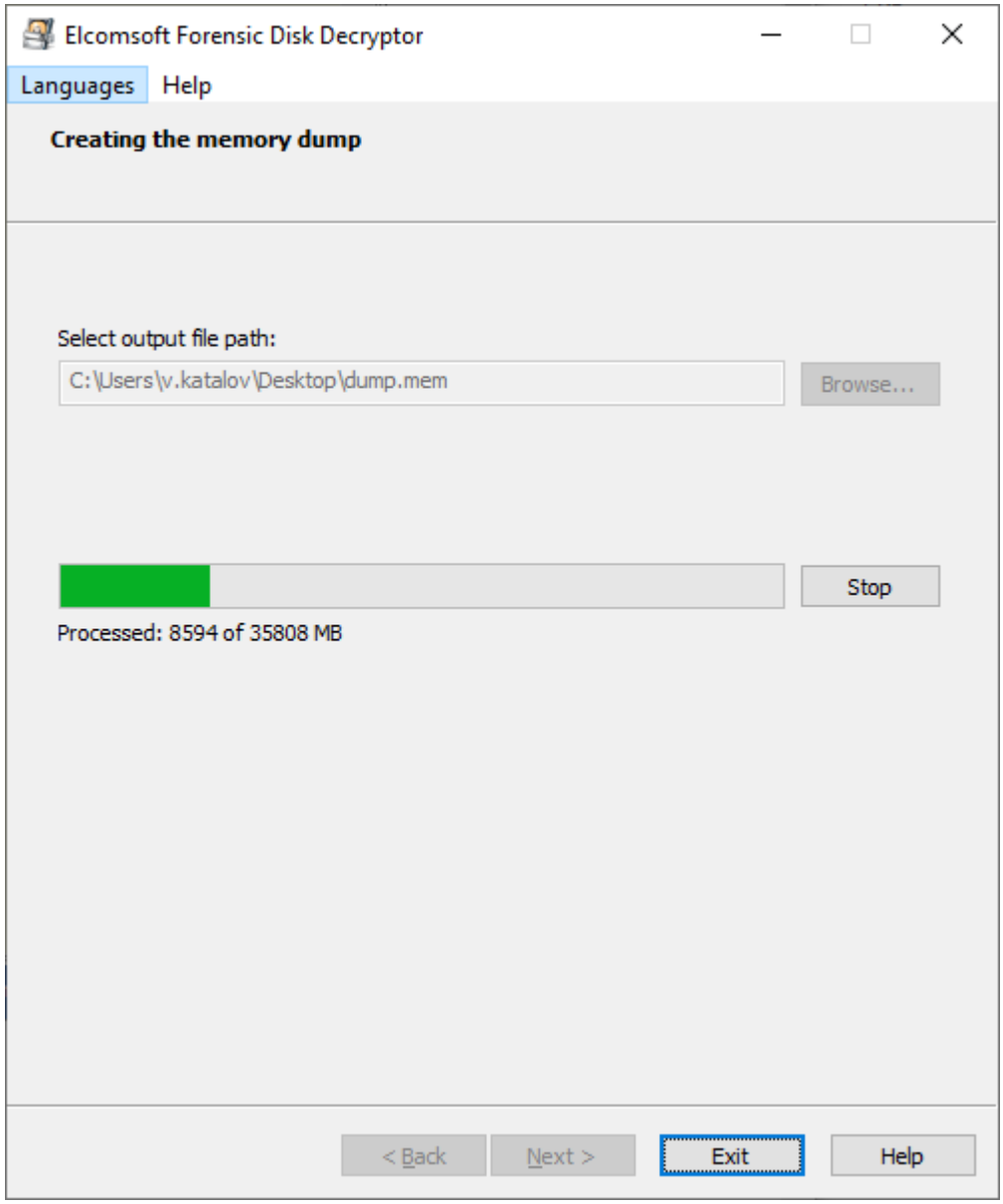
Для первых двух вариантов программа получает список всех доступных разделов и пытается обнаруживить шифрование, если оно есть. Параметр «Контейнер» (Container) предназначен для контейнеров PGP (.pgd) и TrueCrypt/VeraCrypt (во втором варианте он может иметь произвольное расширение).



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)

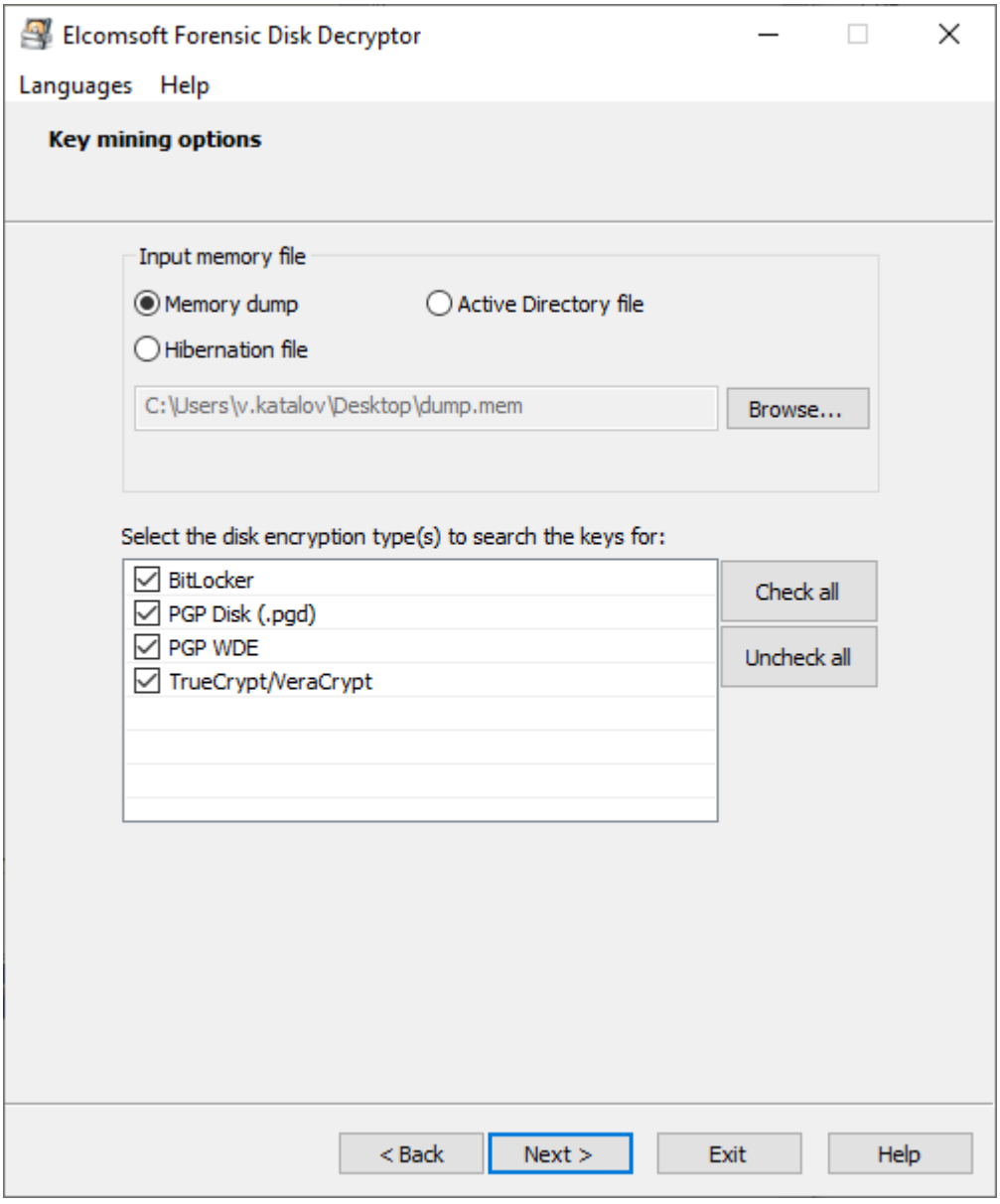
Эта опция позволяет создать портативную версию программы, которая может запускаться со съемного диска. Между обычной и портативной версиями есть следующие различия:

- 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)

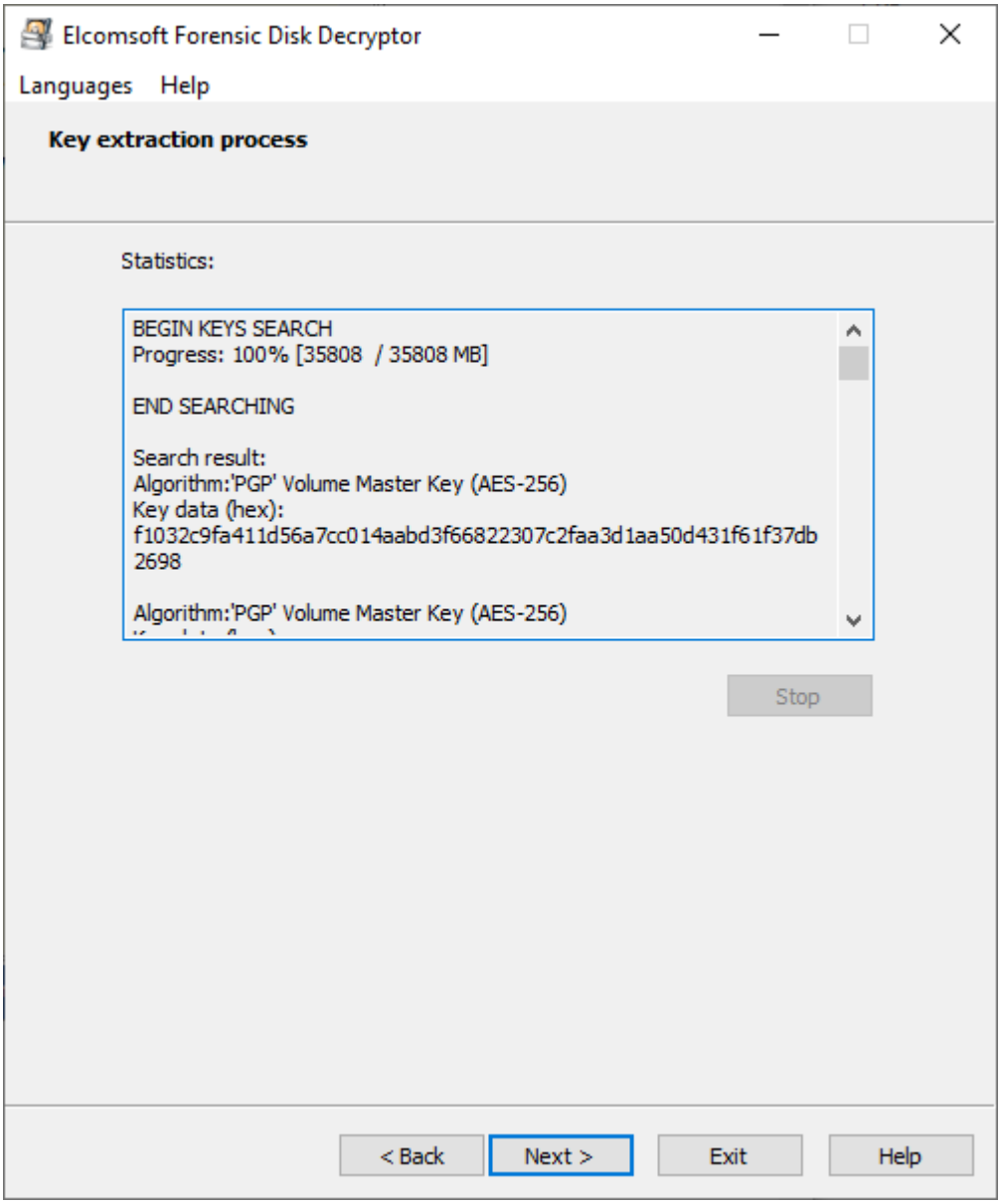
5.2.2.3 Извлечение ключей

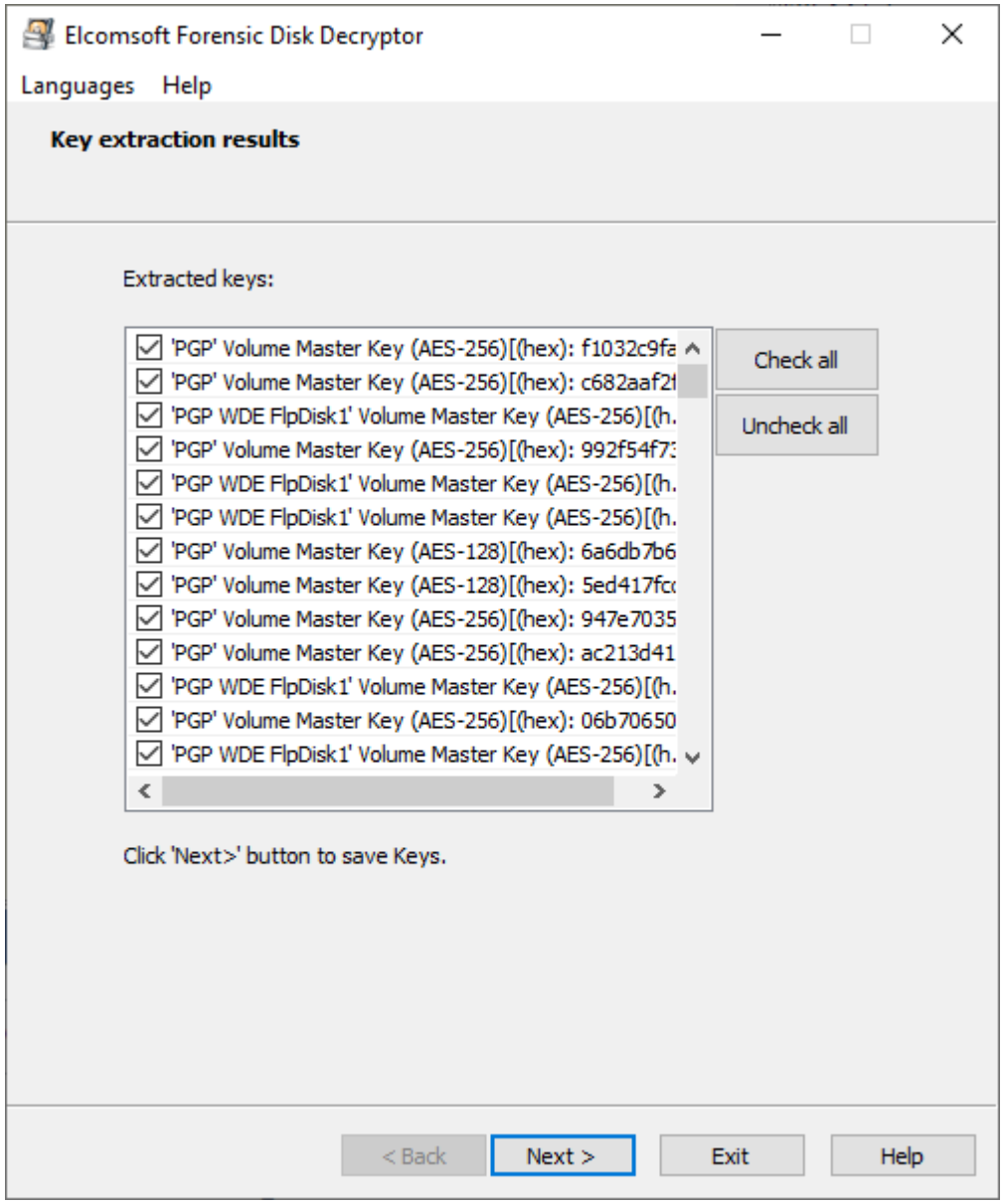
Выберите источник ключей шифрования (дамп памяти (memory dump) или hiberfil.sys) и тип шифрования (BitLocker, PGP или TrueCrypt/VeraCrypt) и нажмите Далее (Next):



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.

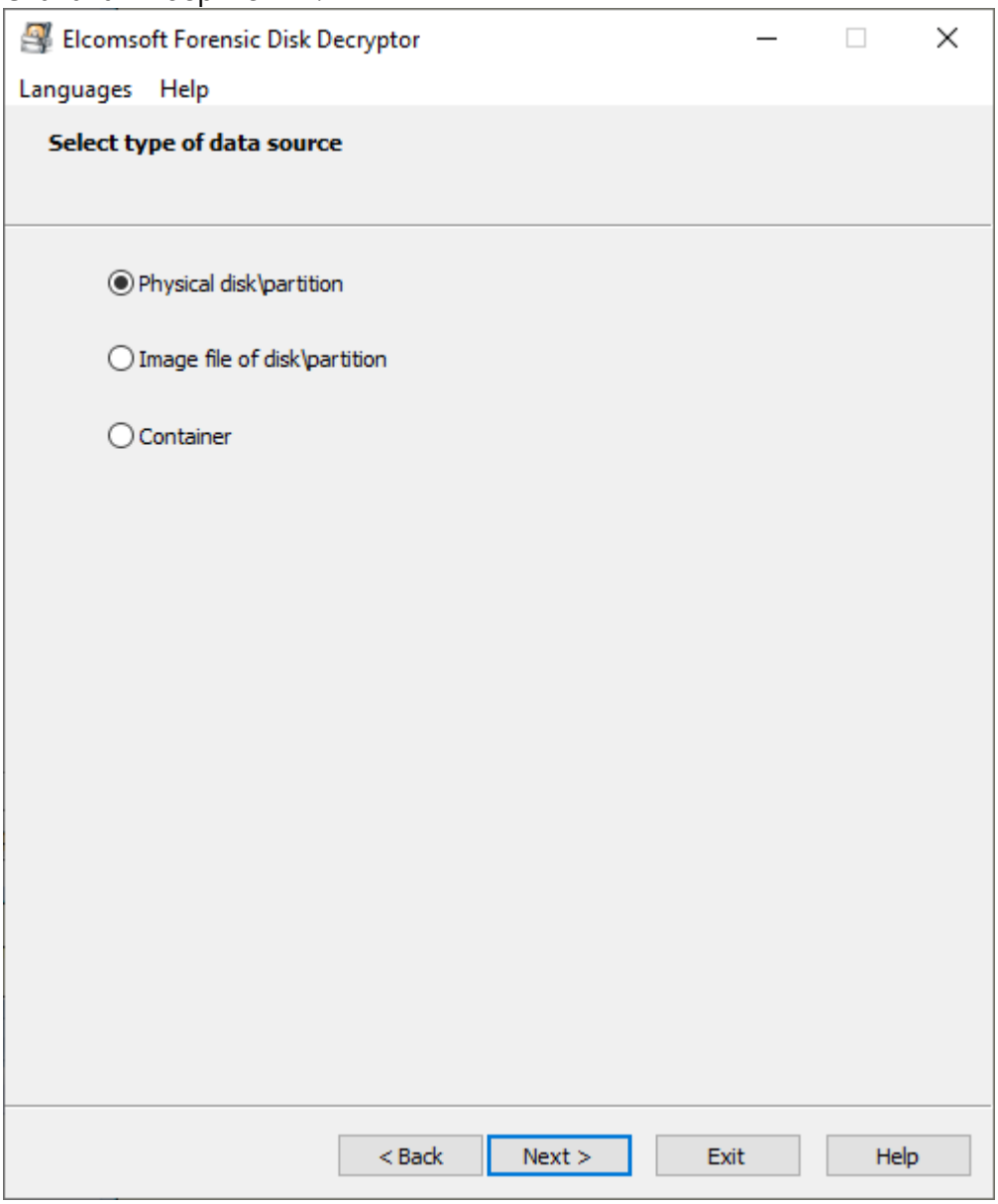
5.2.2.4 Расшифровка и монтирование диска

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

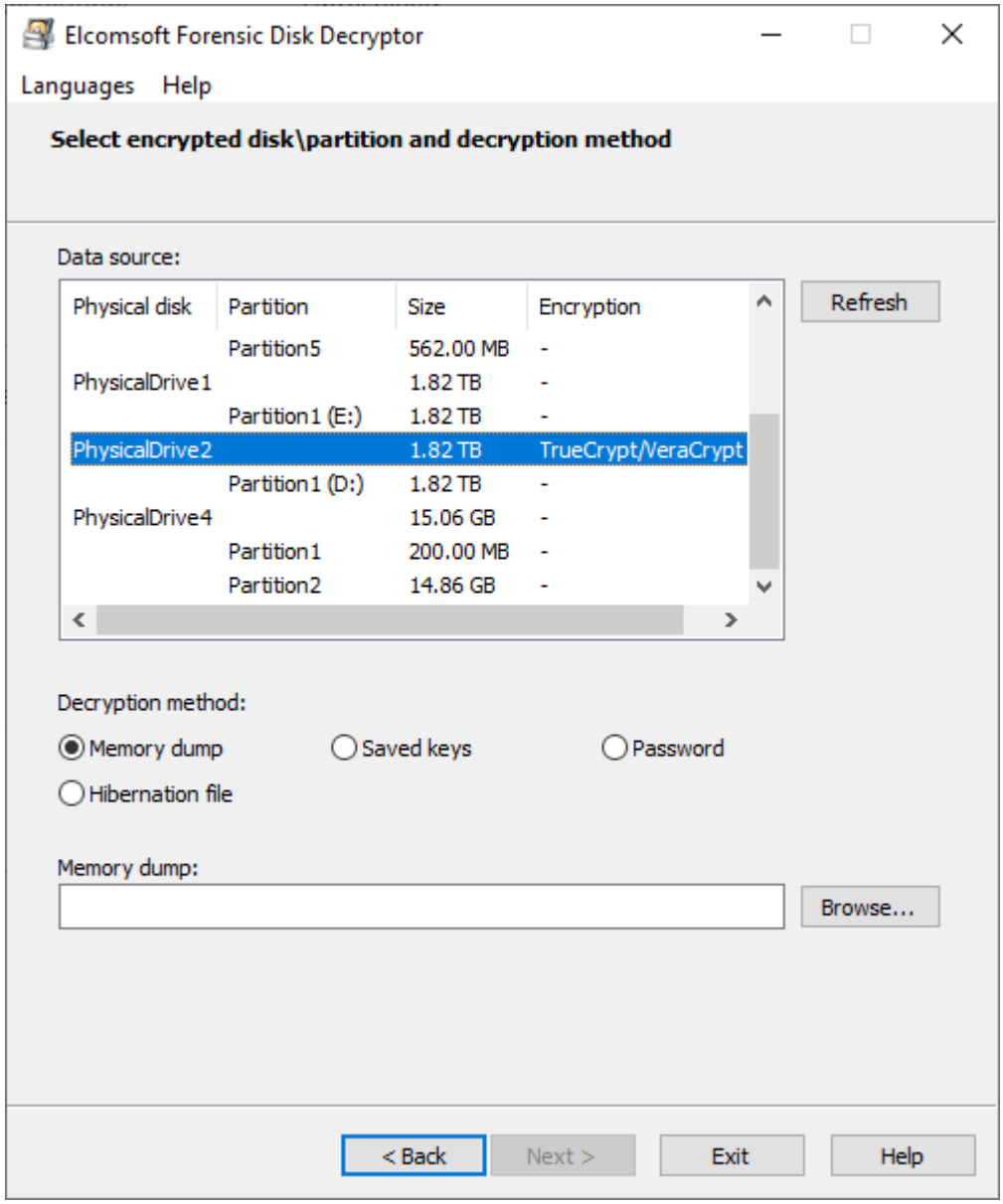
Поддерживаемые образы дисков:

- 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)
- Сохраненные ключи (см. Извлечение ключей)
- Пароль
- Файл гибернации
- Файл Active Directory (только BitLocker)

- Ключ восстановления (для BitLocker, PGP WDE, FileVault2)

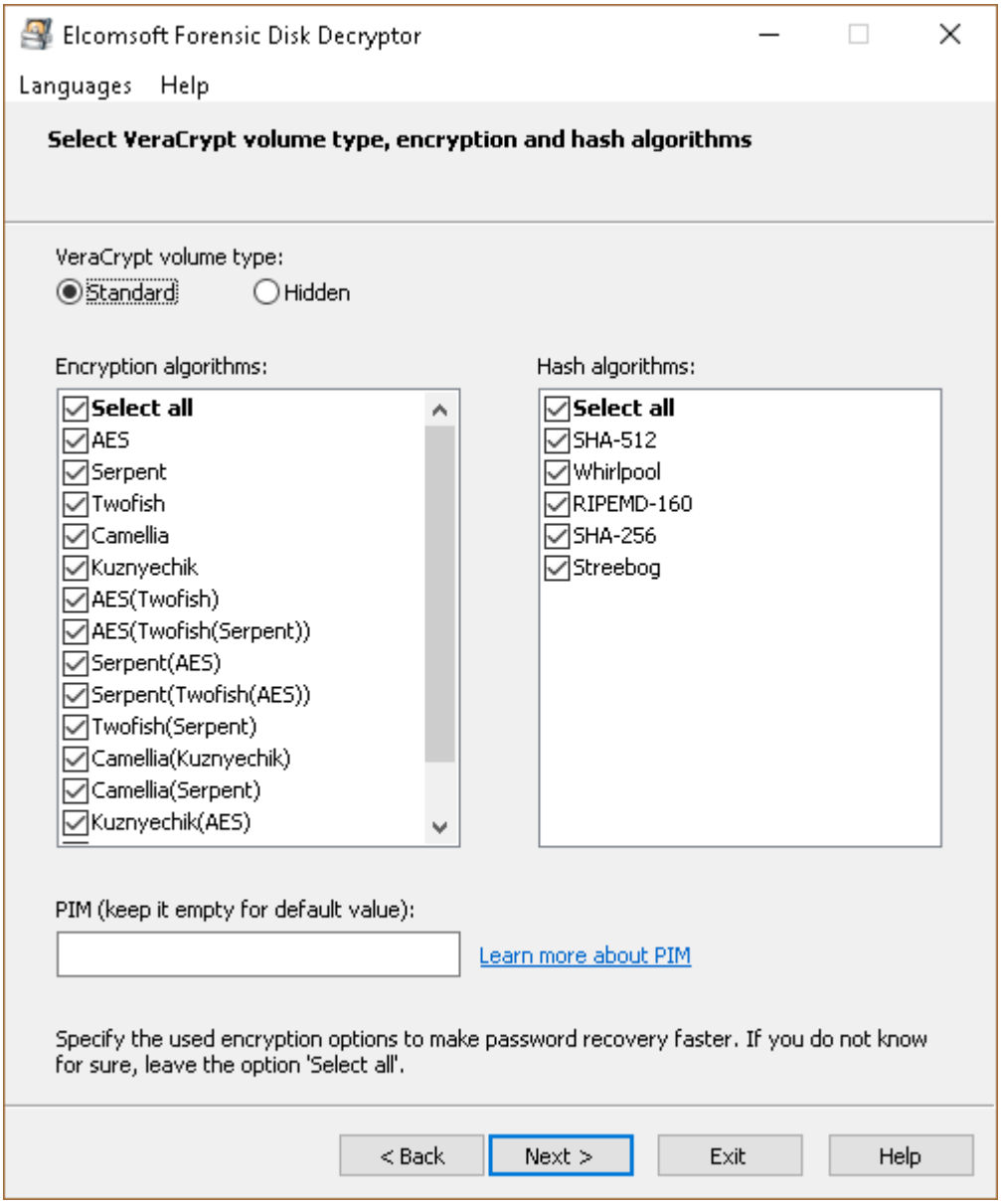
Обратите внимание, что эта функция пока недоступна для разделов APFS, зашифрованных с помощью FileVault2.

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 subsequencial 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

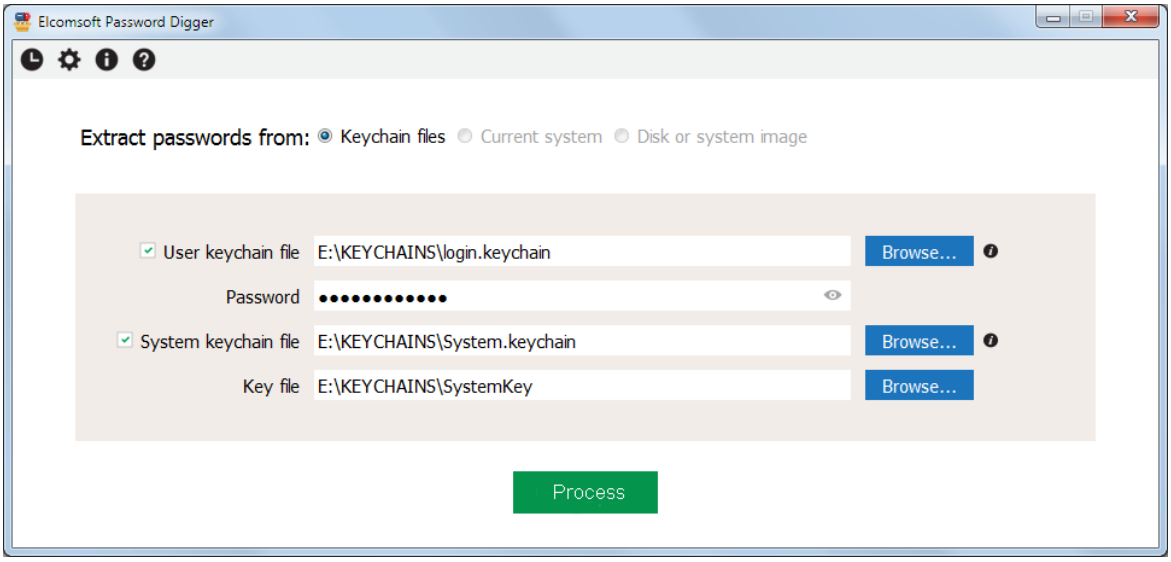
- Windows 7 or above
- about 80 megabytes of free space on hard disk

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 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/wordlist, 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.

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 who's 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 clocking 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 УСТОЙСТВЕ.
- 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:
- Декомприлирование 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 back/wire transfer. European customers are also charged VAT.

More information about all payment options is available at ordering page on ElcomSoft web site:

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, ...

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, предоставленным 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 рекомедуем 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 Съемный (Removeable), 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 загружаться даже с внешнего жесткого диска (USB или FireWire), включая диски размером более 32 ГБ, но некоторые ограничения все еще присутствуют.

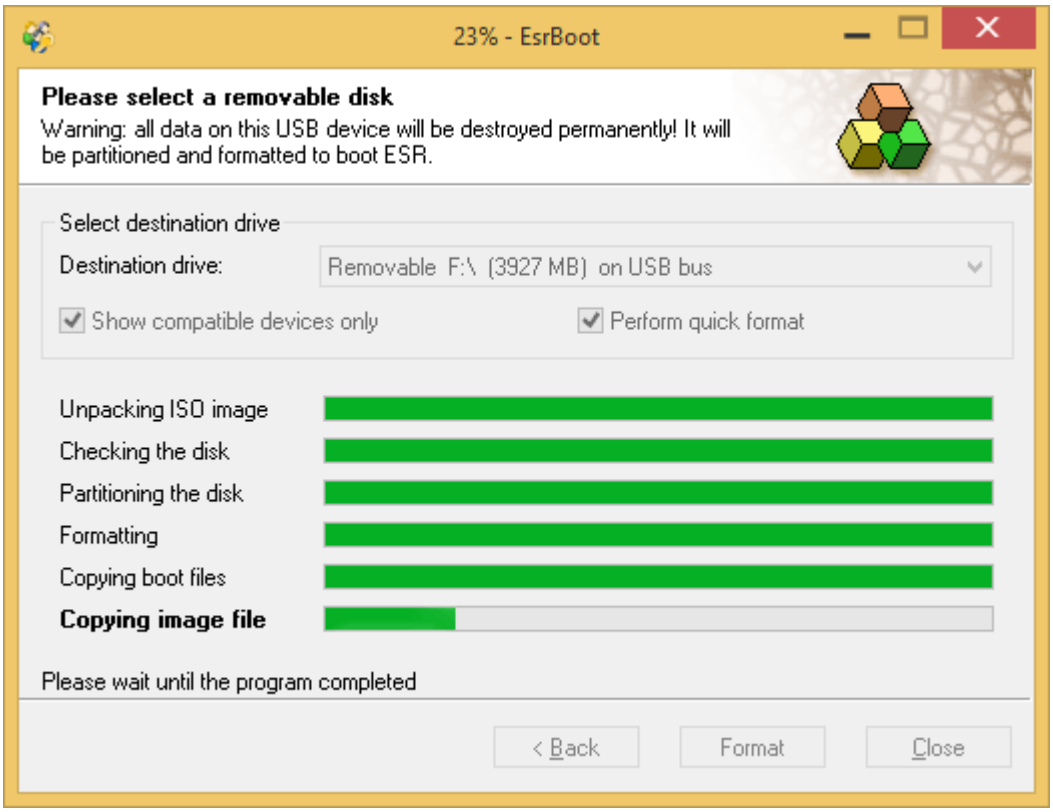
Обратите внимание, что после сброса пароля вы можете потерять доступ к пользовательским: данных для входа на веб-страницах, данным для входа на файловый сервер (file share), данным, зашифрованным с DPAPI, файлам с шифрованием EFS и сертификатам с закрытыми ключами (подписанная / зашифрованная электронная 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).

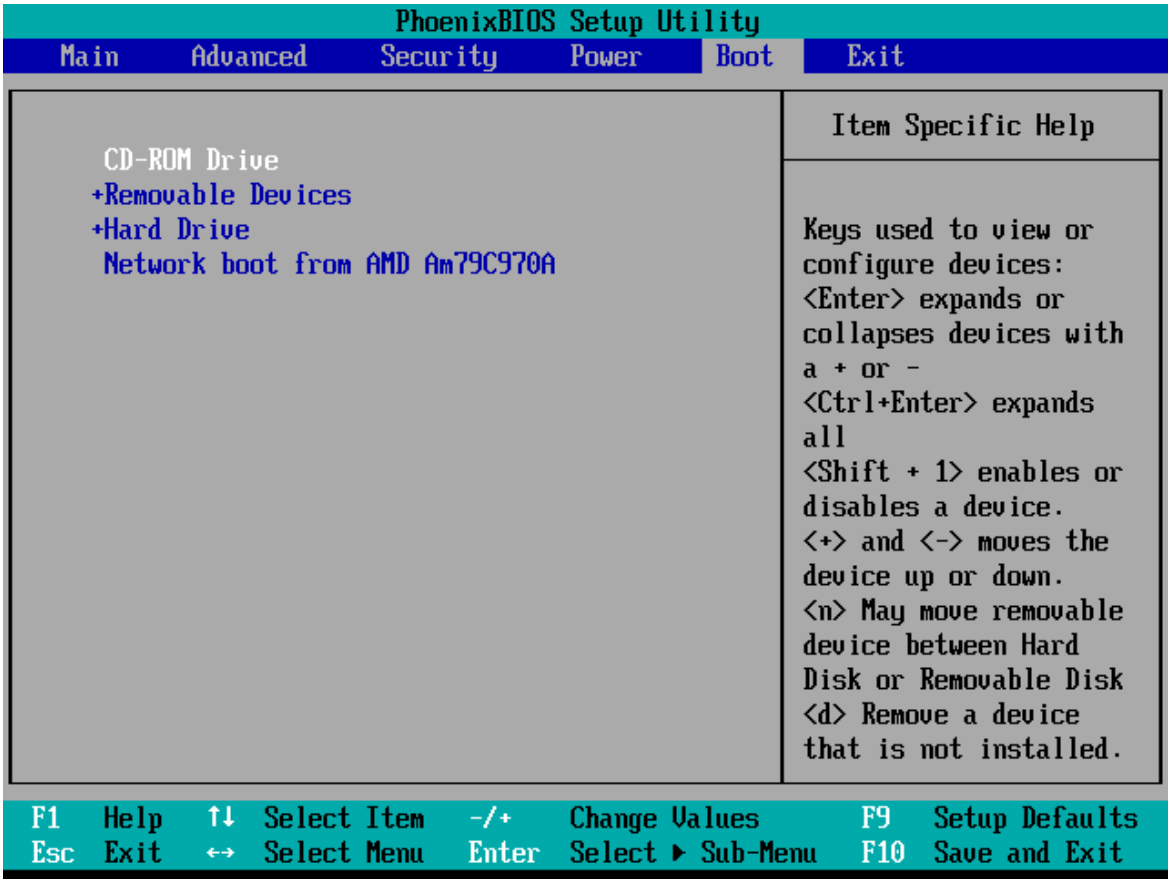
Обратите внимание: при создании загрузочного носителя ESR предлагает на выбор три варианта загрузки: BIOS, UEFI x64 и UEFI x32. Вы должны выбрать подходящий вариант для целевого компьютера. Подавляющее большинство современных компьютеров используют **UEFI x64**, он же в ESR используется по умолчанию. 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.



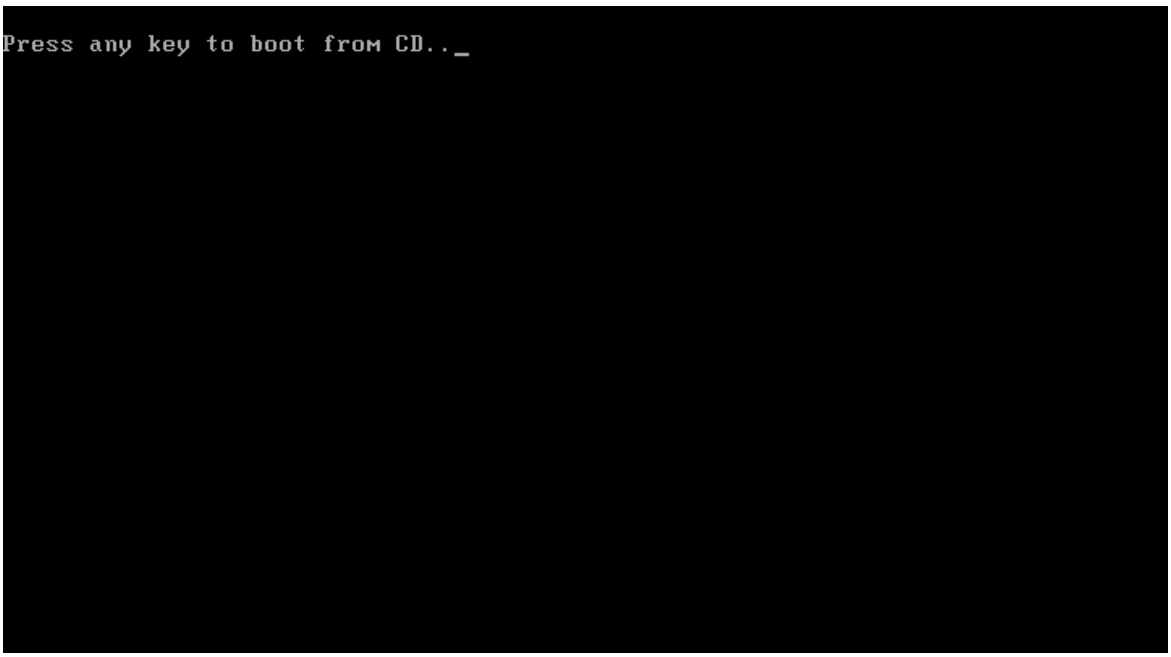
5.4.2.3 Как использовать ESR

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:



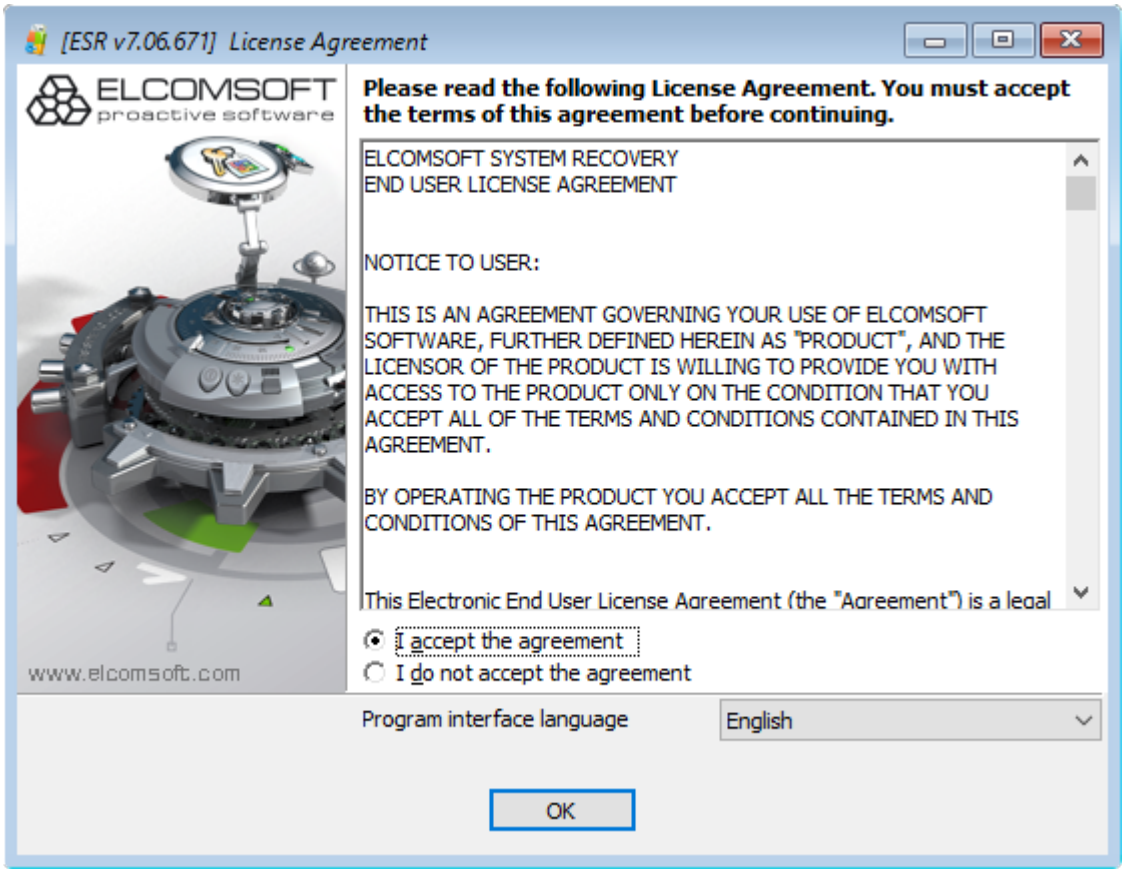
Затем вставьте загрузочный носитель ESR и перезагрузитесь.



Нажмите любую клавишу, и ESR начнет загрузку (создавая RAM-диск и загружая Windows PE):

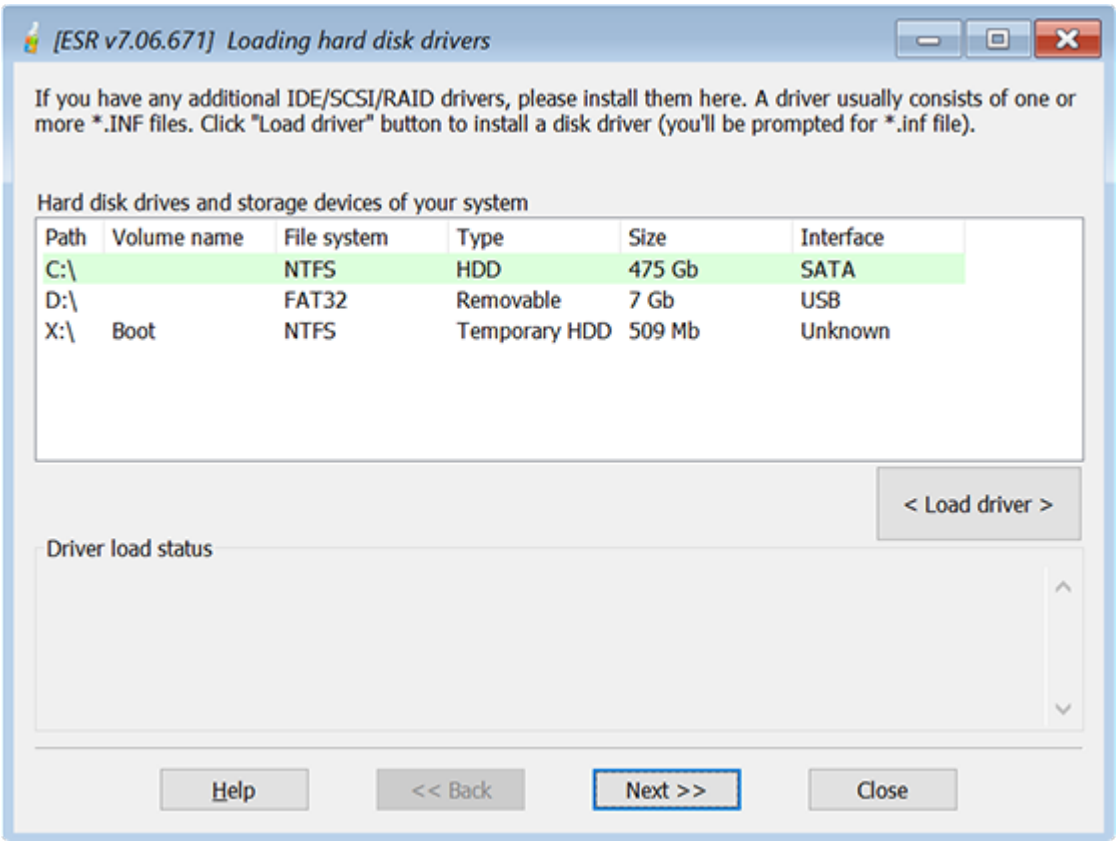
Если вы загружаетесь с USB-устройства, действия в целом, за исключением того, что во время загрузки не будет сообщения «Нажмите любую клавишу...» (Press any key...).

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:



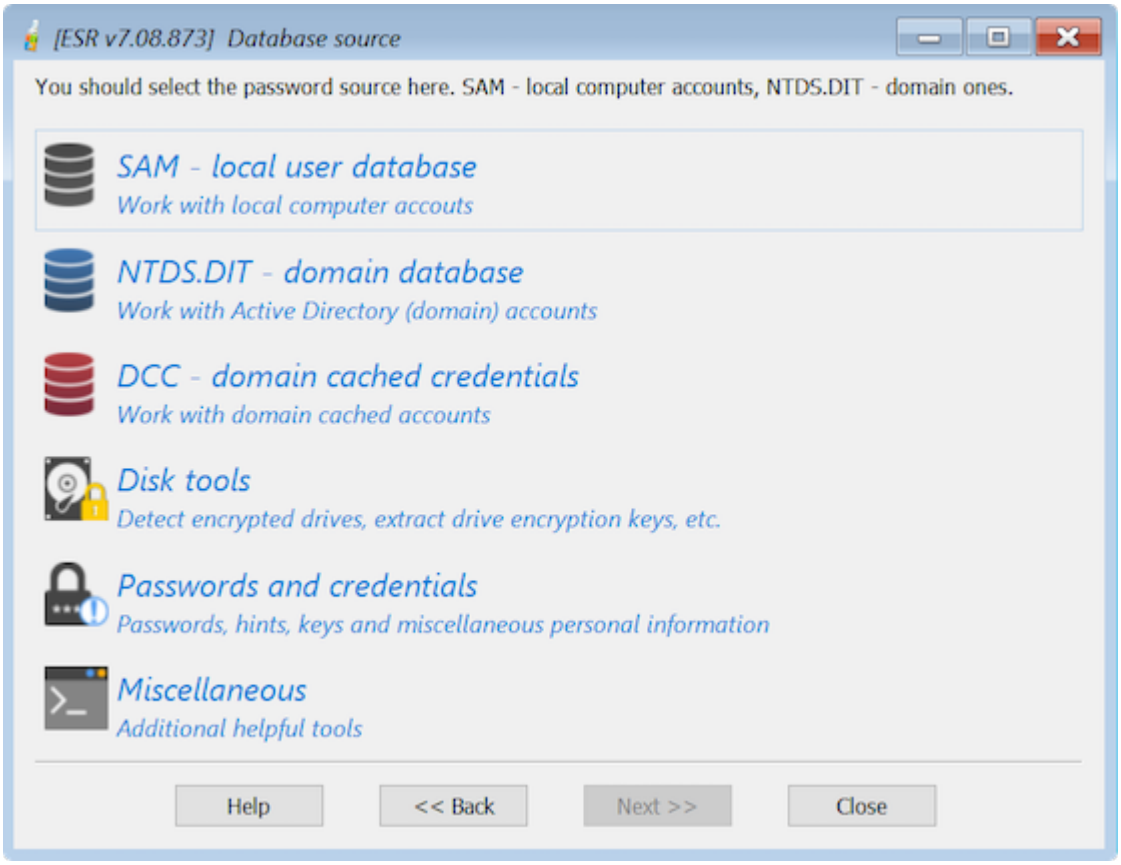
Отобразится список локальных дисков. Если вы не видите системный раздел, нажмите «Загрузить драйвер» и найдите диск, содержащий соответствующие драйверы. ESR загрузит указанный драйвер и обновит список доступных разделов. В окне состояния, где отображается информация о загрузке драйвера появится уведомление об успешной загрузке, если все пройдет хорошо.

ДБ-источник и режим работы

ДБ-источник

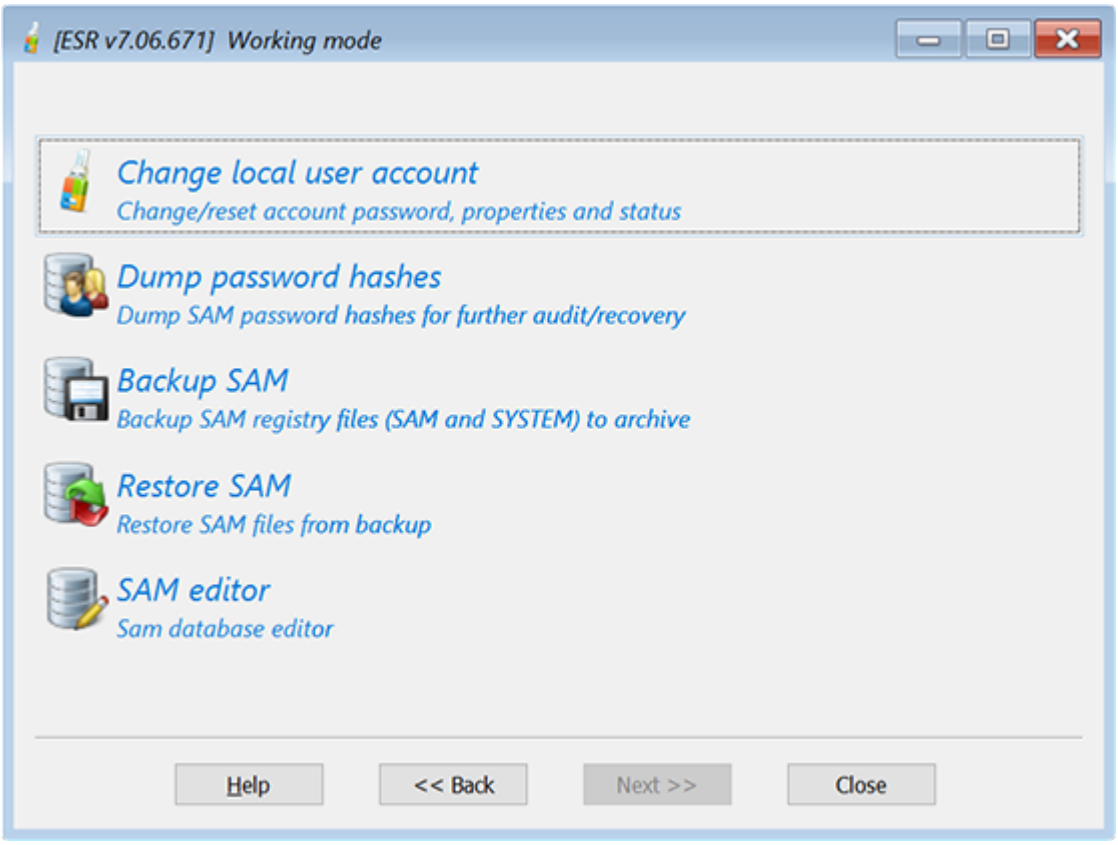
Вы можете выбрать локальные учетные записи и учетные записи Active Directory. Для работы с AD требуется запуск ESR на сервере (domain controller) под управлением Windows Server 2000/2003/2008/2012/2016/2019.

- 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.

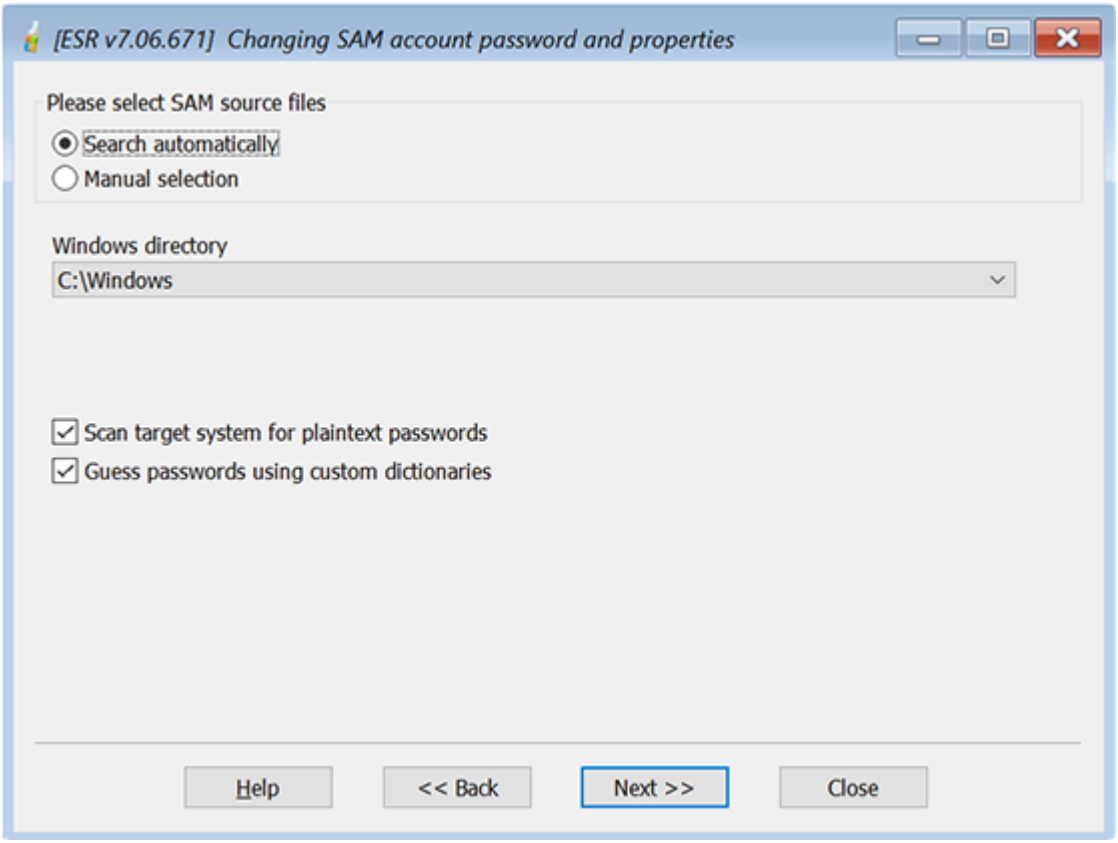
Хэши паролей могут быть сохранены как стандартный файл дампа в ASCII или UNICODE. После сброса программа предлагает открыть файл в Блокноте; **обратите внимание, что если имена пользователей или комментарии**

используют не английский алфавит, они будут отображаться правильно только в UNICODE.

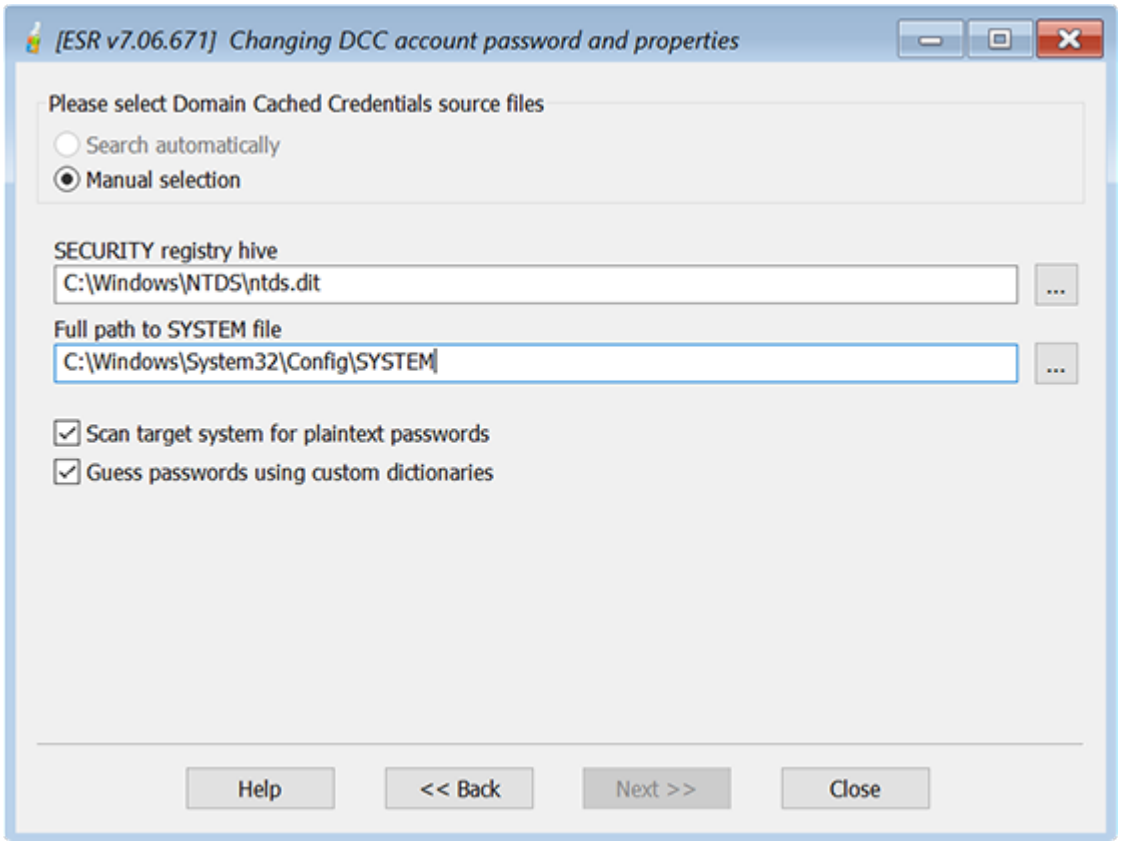
Наконец, редактор базы данных SAM редактор базы данных SAM позволяет редактировать все поля в базе данных SAM, которые содержат расширенные свойства учетных записей локальных пользователей.

Выбор ОС или расположения файлов SAM/AD

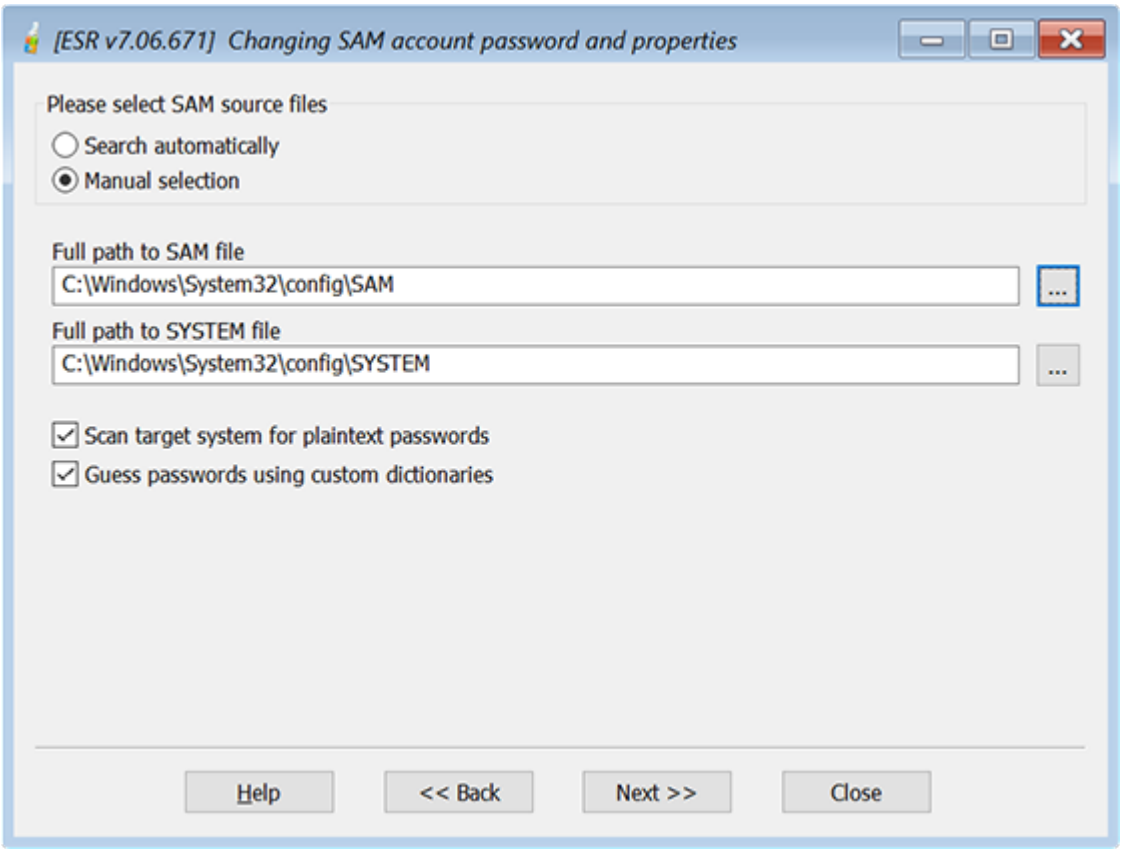
После того, как вы выбрали БД-источник (SAM, DCC или AD) и режим работы, вам будет предложено выбрать операционную систему для работы. Если ваша система использует нестандартные адаптеры запоминающих устройств, такие как SCSI или SAS, которые не поддерживаются ESR, скорее всего вам придется указать драйверы вручную; подробнее в драйверы запоминающих устройств. 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).

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 неполучится извлечь,

и вы не сможете изменить пароли или свойства учетных записей или даже записать хэши паролей в текстовый файл.

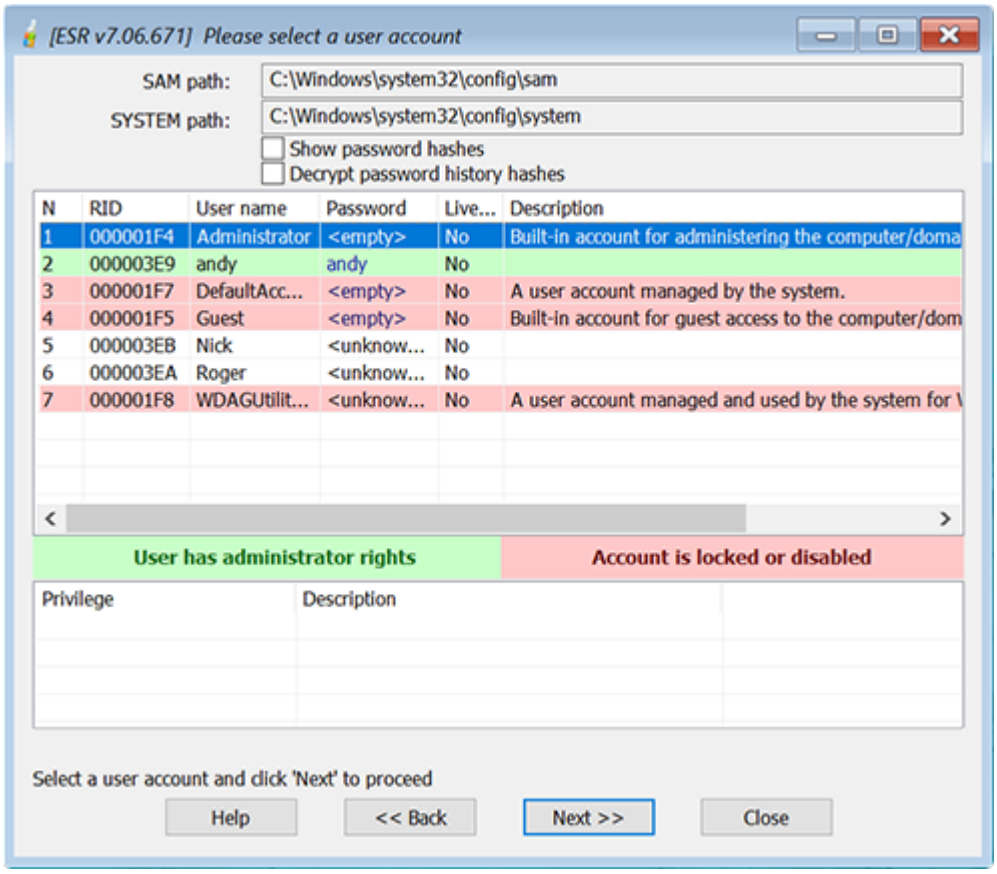
Если вы выбрали опцию «Тестировать короткие и простые пароли» (Test short and simple passwords/), ESR попытается восстановить пароли, используя несколько предопределенных словарных атак и атак методом перебора. Программа также попытается расшифровать пароли, которые могут хранится или быть кэшированы 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», «ааа» 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

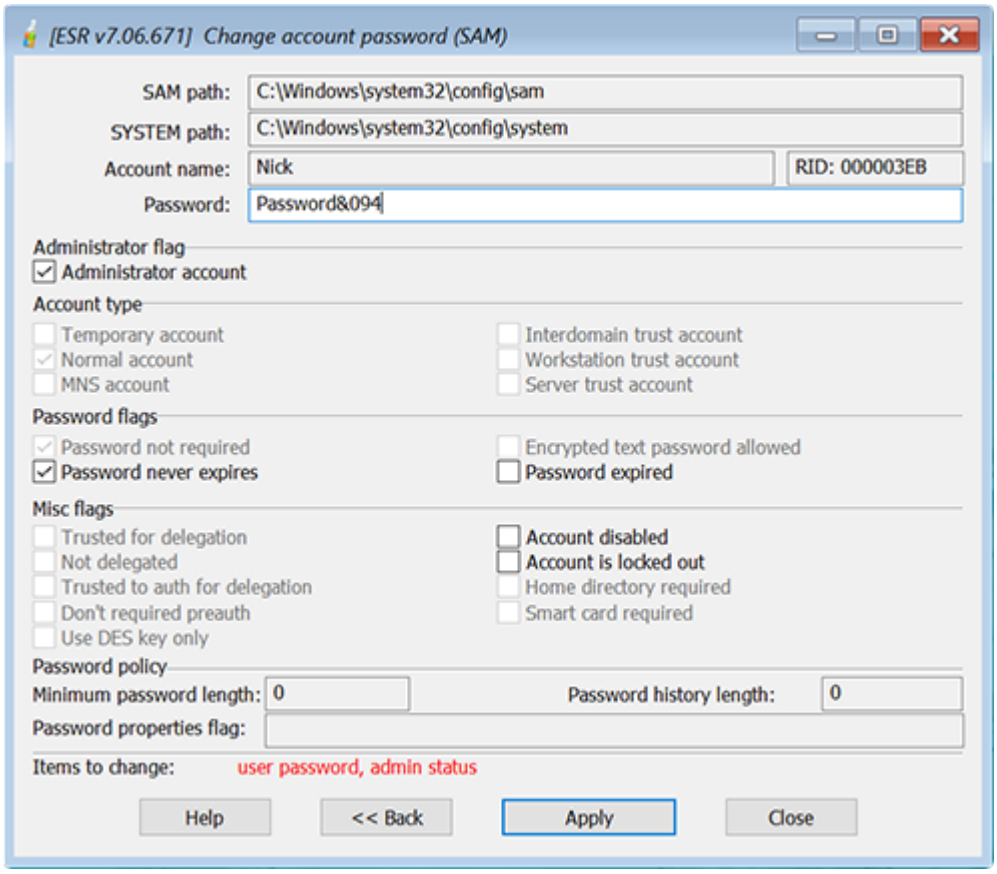
Если вы работаете с локальными (SAM) учетными записями, вам будет представлен список всех локальных учетных записей после выбора операционной системы или файлов SAM и SYSTEM:



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

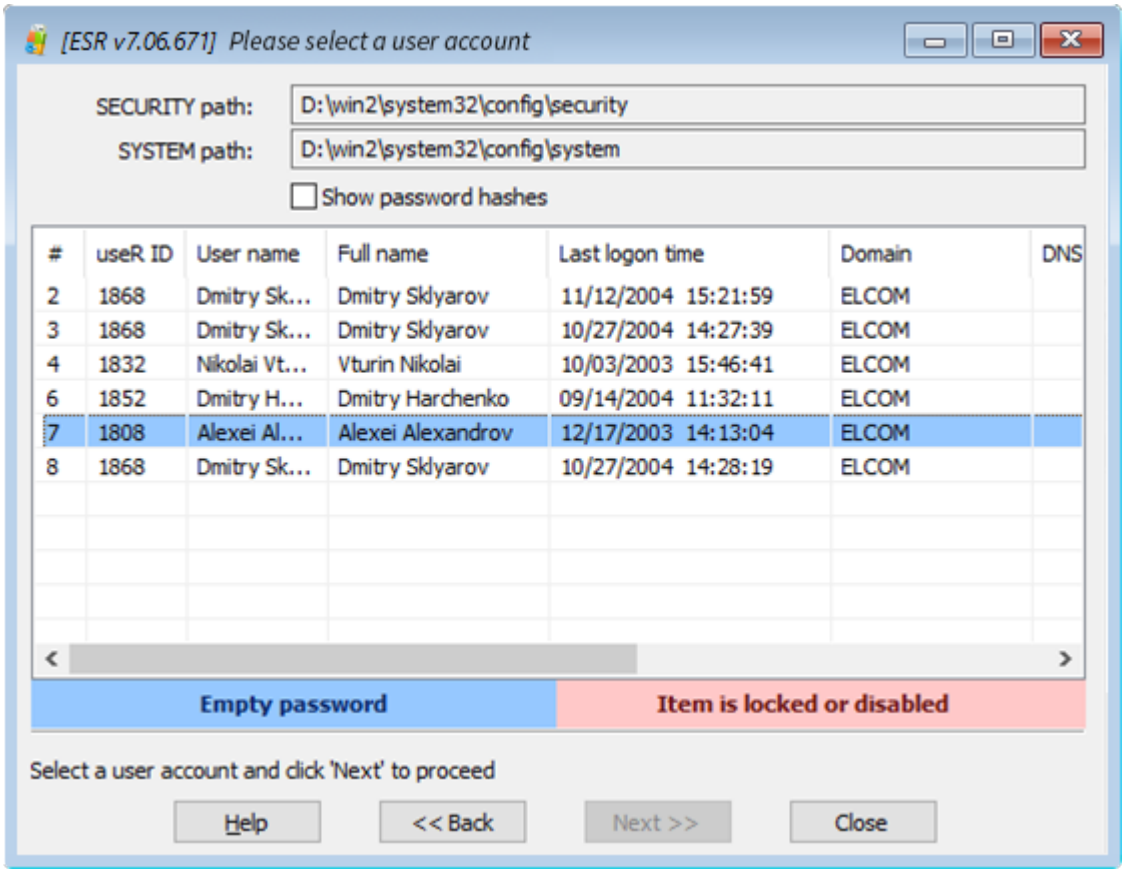
изменять пароль или какие-либо свойства для любых учетных записей в группе пользователей «Гости».

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. 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.).

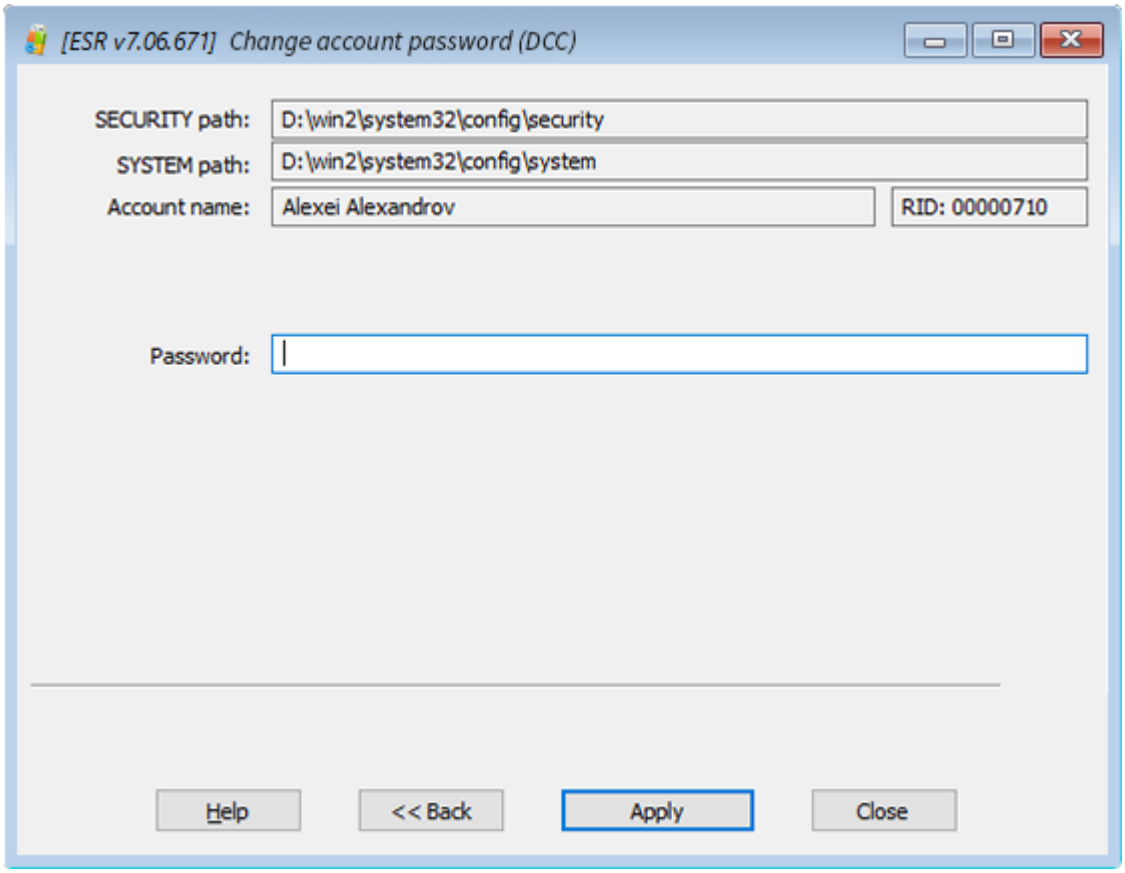
Кэшированные учетные записи домена

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.

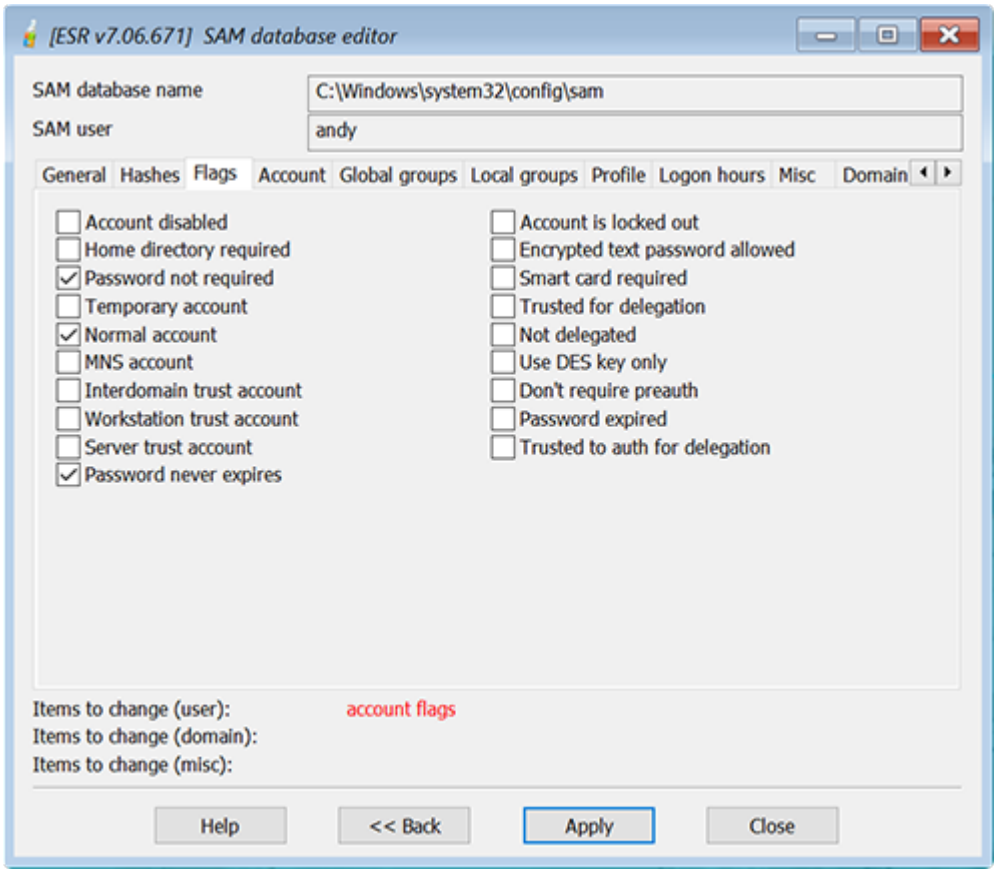


Введите пароль или очистите соответствующее поле ввода, затем нажмите Применить (Apply). Вам будет предложено создать резервную копию файла SECURITY. Перед применением изменений настоятельно рекомендуется сделать резервную копию файла.

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:



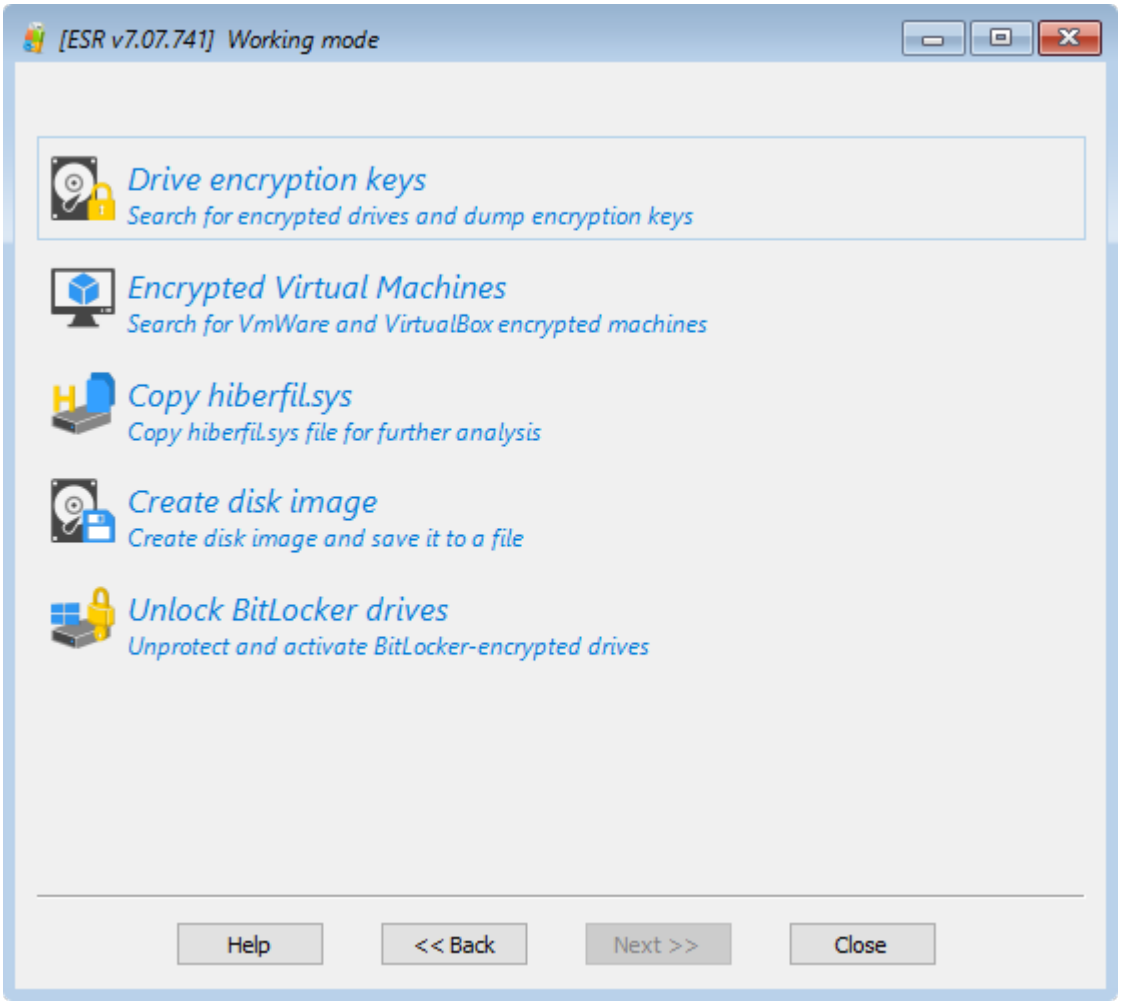
Отображается следующая информация:

- 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

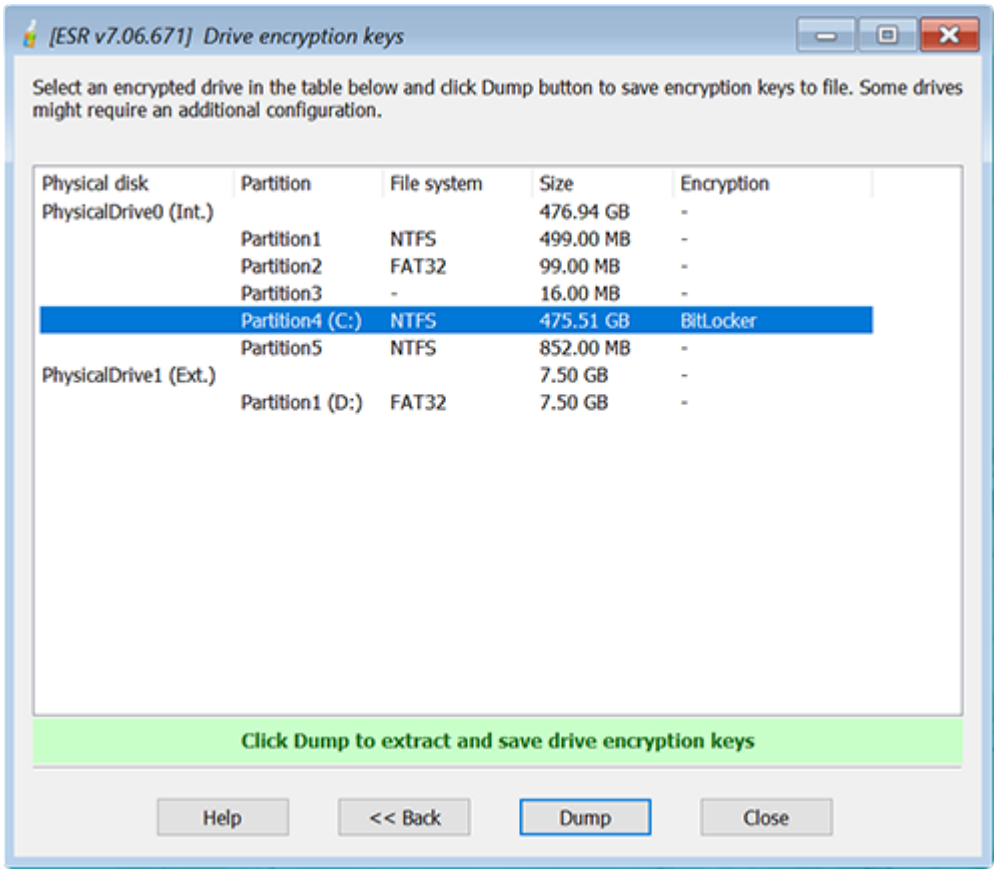
Не рекомендуется редактировать какие-либо поля базы данных SAM, если вы не уверены в том, что делаете.

Инструменты работы с дисками

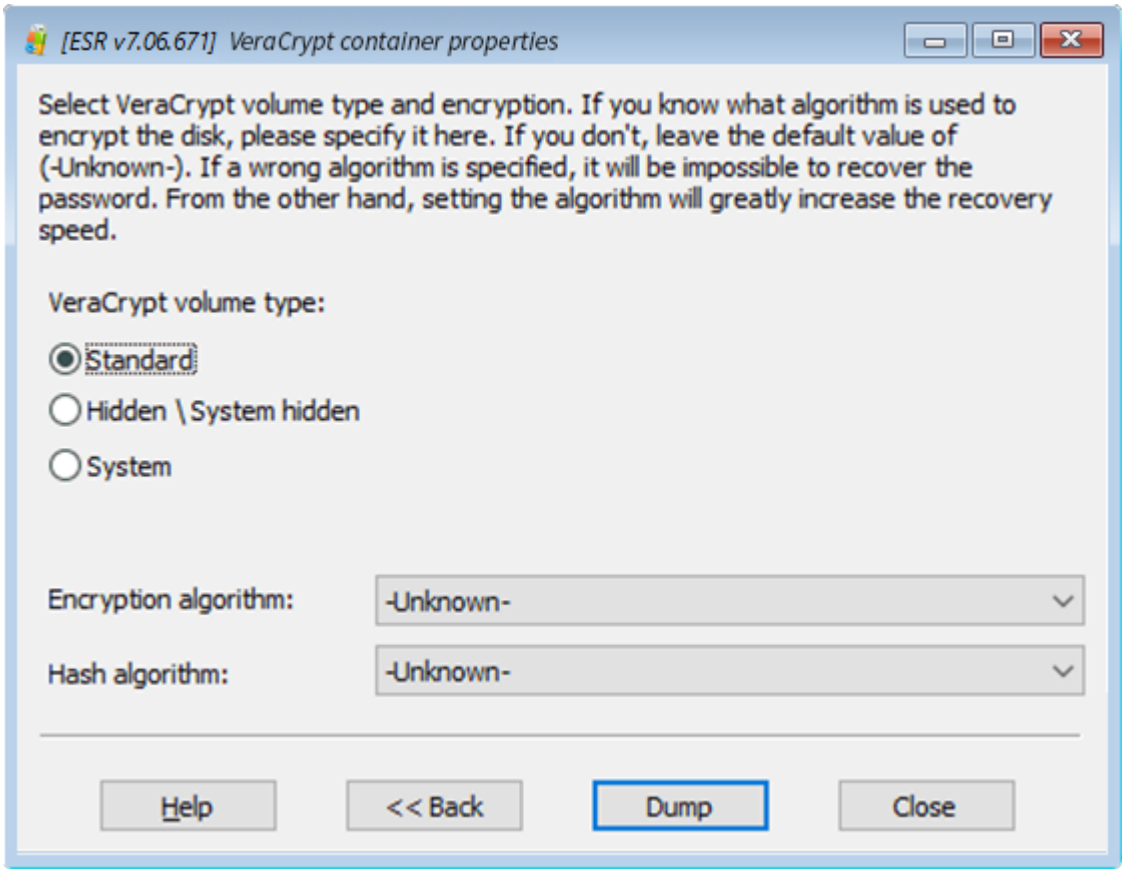
В диалоговом окне «Инструменты работы с дисками» вы можете искать зашифрованные диски или виртуальные машины и создавать дамп ключей шифрования для дальнейшего восстановления с помощью Elcomsoft Distributed Password Recovery или с помощью других программ.
Вы также можете создать образ диска для криминалистического 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

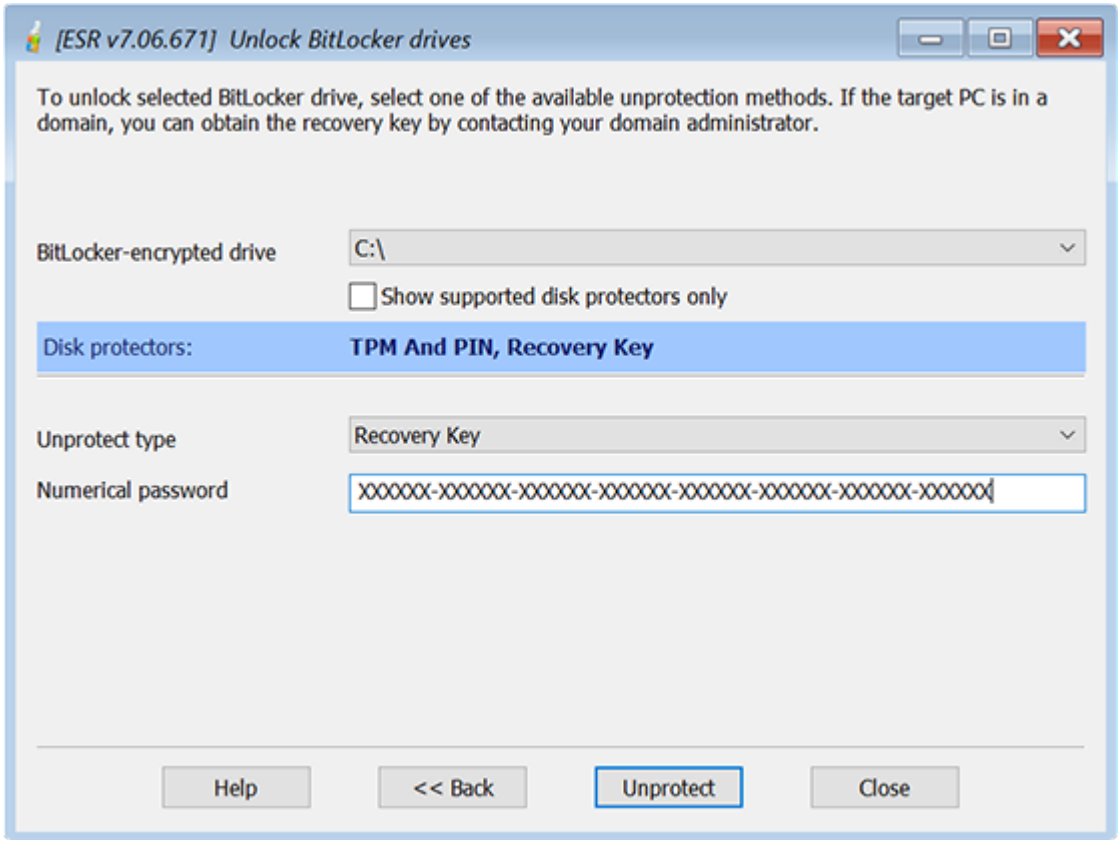
Чтобы использовать диск, зашифрованный с помощью BitLocker, сначала необходимо его разблокировать и смонтировать. Программа поддерживает три основных метода разблокировки диска BitLocker:

- 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.

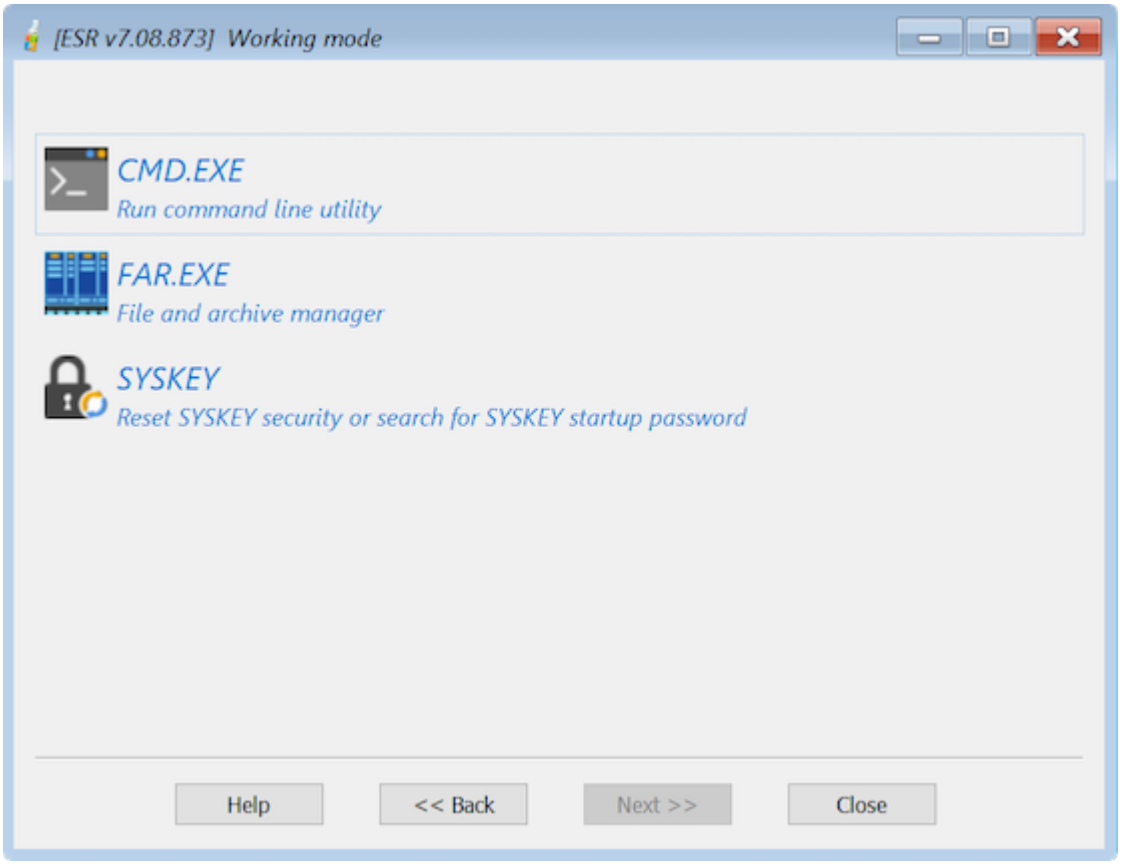


Другое

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 дамп-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, дамп 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 НЕ 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 дамп 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 удается, 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.

Хеш 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) **невозможно получить исходный пароль из хеша**, 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
- найти пароли с такими же хэшами, что и исходные

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, 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 дамп

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

(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).

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).

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 (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 хеш LM недоступен); см. О Windows паролях.

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 пользователей**. 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 хеша (Hash type)

Могут быть созданы хэш-таблицы LM и NTLM; см. О Windows паролях

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-символьная14 (alpha-num-sym14)	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).

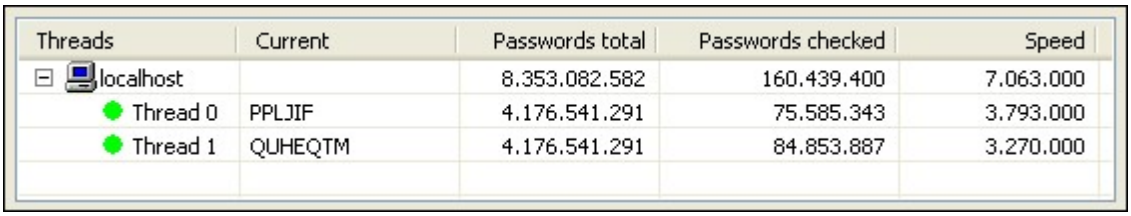
- Прошедшее время (Time elapsed) - время, прошедшее с момента начала атаки.

- 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). 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).

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). Чтобы запустить PPA с определенным количеством потоков, используйте следующую командную строку:

ppa.exe -threads N

где N - количество потоков.

Часть VI

Лицензионное соглашение

6 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 УСТОЙСТВЕ.
- 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:
- Декомприлирование 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 .

Часть VII

Техническая поддержка

7 Техническая поддержка

Портал технической поддержки находится по адресу
https://support.elcomsoft.com

Мы предоставляем техническую поддержку на русском или английском языке. Пожалуйста, заполняйте поля с названием и версией продукта, а также пишите о проблеме максимально подробно, чтобы быстрее получить ответ.

Index

- A -

- B -

- C -

- D -

- E -

- F -

- G -

- H -

- I -

- K -

- L -

- M -

- N -

- O -

- P -

- Q -

- R -

- S -

- T -

- U -

- V -

- W -

- X -

- Y -