PowerPoint Password Recovery

РУКОВОДСТВО ПОЛЬЗОВАТЕЛЯ

Copyright (c) 2024 Passcape Software. All rights reserved.
Passcape Software

1. Введение 5

1.1 О программе ... 6
1.2 Особенности и преимущества ... 6
1.3 Системные требования ... 7

2. Интерфейс программы 8

2.1 Общее описание ... 9
2.2 Меню Проект ... 10
2.2.1 Открыть документ ... 10
2.2.2 Сохранить пароли ... 10
2.2.3 Новый ... 10
2.2.4 Открыть ... 10
2.2.5 Сохранить ... 10
2.2.6 Сохранить Как ... 10
2.2.7 Закрыть ... 11
2.3 Меню Восстановление ... 11
2.3.1 Запуск ... 11
2.3.2 Продолжить ... 11
2.3.3 Стоп ... 11
2.4 Меню Редактирование ... 11
2.4.1 Открыть активный документ ... 11
2.4.2 Удалить ... 12
2.4.3 Удалить защиту ... 12
2.4.4 Копировать ... 12
2.4.5 Выбрать ... 12
2.4.6 Поиск ... 12
2.5 Меню Отчёты ... 13
2.5.1 Отчёты о паролях ... 13
2.5.2 Статистика атак ... 14
2.5.3 Различная информация ... 15
2.5.4 Анализ словарей ... 16
2.6 Меню Инструменты ... 17
2.6.1 Доступ к Программе ... 17
2.6.2 Пасс-о-метр ... 18
2.6.3 Проверка Пароля ... 19
2.7 Меню Утилиты ... 19
2.7.1 Открыватель паролей за звёздочками *** ... 20
2.7.2 Утилиты для работы со словарями ... 20
2.7.2.1 Создание словаря путем индексации локальных файлов ... 21

Copyright (c) 2024 Passcape Software. All rights reserved.

2.7.2.2 Слияние словарей ... 23
2.7.2.3 Анализ словаря ... 24
2.7.2.4 Сортировка словаря ... 26
2.7.2.5 Конвертер словарей ... 27
2.7.2.6 Сравнение словарей ... 28
2.7.2.7 Дополнительные инструменты ... 29
2.7.2.8 Индексация жесткого диска ... 31
2.7.2.9 Поиск HTML ссылок ... 34
2.8 Меню Настройки ... 36
2.8.1 Общие ... 36
2.8.1.1 Общие ... 36
2.8.1.2 Настройки атак ... 37
2.8.1.3 Настройки процессора ... 38
2.8.1.4 Настройки видеокарт ... 39
2.8.1.5 Звуковые События ... 40
2.8.2 Настройки Атак ... 40
2.8.2.1 Предварительная Атака ... 40
2.8.2.2 Интеллектуальная Атака ... 41
2.8.2.3 Идентификационная Атака ... 43
2.8.2.4 Атака в Лоб (полным перебором) ... 46
2.8.2.5 Атака по Словарю ... 47
2.8.2.6 Атака по Маске ... 51
2.8.2.7 Атака по Ключевому Слову ... 53
2.8.2.8 Комбинированная Атака по Словарям ... 54
2.8.2.9 Атака по Фразе ... 59
2.8.2.10 Гибридная Атака по Словарю ... 62
2.8.2.11 Групповая Атака ... 70
2.9 Меню Вид ... 70
2.10 Меню Темы ... 71
2.11 Меню Помощь ... 71
2.12 Системный монитор ... 72
3. Работа с программой 73
3.1 Атаки ... 74
3.2 Сравнительная Таблица Атак ... 75
3.3 GPU FAQ ... 78
3.4 Загрузка Онлайн Словарей ... 81
4. Лицензия и регистрация 83
4.1 Лицензионное соглашение ... 84
4.2 Регистрация ... 85
4.3 Ограничения ДЕМО версии ... 86
4.4 Редакции программы ... 86

Copyright (c) 2024 Passcape Software. All rights reserved.

5. Техническая поддержка 88
5.1 Ошибки и проблемы 89
5.2 Предложения 89
5.3 Контакты 89

Copyright (c) 2024 Passcape Software. All rights reserved.

Введение

1 Введение

1.1 О программе

Добро пожаловать в **PowerPoint Password Recovery** - программу для восстановления забытых паролей Microsoft Office PowerPoint. PowerPoint Password Recovery является современным программным решением, применяющим передовые технологии восстановления паролей, разработанные программистами нашей компании. Например, *Fingerprint attack* или *Pass-phrase recovery*.

Новые стандарты защиты данных в документах Microsoft Office 2007 - 2021 обеспечивают достаточную надёжность персональной информации пользователя. Ранние редакции PowerPoint имели очень слабый алгоритм защиты, слабые пароли были уязвимы и их легко было взломать.

Начиная с PowerPoint 2007, защита документов подверглась значительной ревизии и переделке, начали применяться современные, более стойкие к взлому алгоритмы шифрования AES и SHA-1. В настоящее время, ни один компьютер не может взломать ключ шифрования AES с длиной 128 бит. Начальный пароль при помощи хэш-функции SHA-1 проходит свёртку в 128-битный ключ. При этом используется цикл из 50000 повторов, что приводит к значительному падению скорости взлома пароля (фактически, в те же 50000 раз). PowerPoint 2010 использует аналогичную длину ключа - 128 бит, но количество раундов в цикле преобразования теперь удваивается и составляет 100000. Таким образом, скорость восстановления паролей уменьшается ещё в два раза по сравнению с PowerPoint 2007. По-умолчанию в Microsoft PowerPoint 2013 применено ещё более сильное шифрование даже по сравнению с PowerPoint 2010. Для увеличения стойкости защиты, Microsoft увеличил длину ключа до 256 бит и заменил алгоритм хэширования SHA-1 на более медленный SHA-512.

Таким образом, Microsoft делает каждые последующие выпуски PowePoint все более защищёнными, а перебор, как основной тип восстановления паролей, становится все менее эффективен. С новым стандартом шифрования, применяемым в PowerPoint 2013, о применении простого перебора паролей не может быть и речи. Вот где выходит на сцену **PowerPoint Password Recovery**, с уникальным набором умных атак, разработанных в нашей компании и применяемых исключительно в наших продуктах, что отличают ее от большинства подобных программ. Например, Интеллектуальное восстановление производит анализ сетевой активности пользователя, сканирование жёсткого диска вашего ПК, поиск всех используемых ранее паролей, индексацию всех найденных слов с целью дальнейшего семантического разбора и мутации потенциально возможных вариантов искомого пароля.

1.2 Особенности и преимущества

PowerPoint Password Recovery обладает рядом достоинств по сравнению с аналогичными программами:

- Современный, настраиваемый графический интерфейс.
- Оптимизированные алгоритмы перебора паролей на современных CPU.
- Технология аппаратного ускорения с использованием видеокарт NVIDIA или AMD.
- Более 10 современных типов восстановления паролей, многие из которых разработаны и применяются только в программных продуктах нашей компании.
- Расширенный отчёты для аудита.

Copyright (c) 2024 Passcape Software. All rights reserved.

- Дополнительные инструменты, включая мощный набор утилит для создания и управления словарями. Например, можно создавать свои словари путём индексации файлов на жёстком диске.
- Расшифровка некоторых паролей "на лету".
- Мгновенное удаление/сброс некоторых паролей.
- Восстановление по словарю поддерживает текстовые словари в формате ASCII, UNICODE,UTF8, PCD, RAR и ZIP.
- Большой выбор Онлайн словарей для словарных атак (около 2 Гб), дополнительная коллекция уникальных словарей (более 50 Гб).
- Некоторые функции программы, например мутация слов, уникальны. Общее количество правил мутации переваливает за полторы сотни. Такого нет ни в одной аналогичной программе!
- Гарантированное восстановление пароля для документов MS Office 97-2003 с 40-битным ключом шифрования.

1.3 Системные требования

Требования
Windows XP или более новая ОС, около 50 Мб на жёстком диске, 512 Мб RAM.
Поддержка видеокарт NVidia подразумевает наличие последних драйверов и видеокарты с поддержкой CUDA 3.5 или выше. Для AMD/ATI видео-карт требуется поддержка OpenCL1.2 (все видеокарты, начиная с серии RADEON 7xxx).

Совместимость
Поддерживаются документы Microsoft PowerPoint 97 - 2021

Известные проблемы
При запуске на операционной системе Windows 2000, необходимо самостоятельно скопировать файл GDIPLUS.DLL в каталог программы. Несмотря на то, что программа не содержит вредоносный код, некоторые антивирусы и анти-шпионы могут определять ее как опасную или даже "потенциально нежелательную программу". Это явление, известное как "False Alert", является типичной проблемой для всех продуктов, восстанавливающих пароли.

Copyright (c) 2024 Passcape Software. All rights reserved.

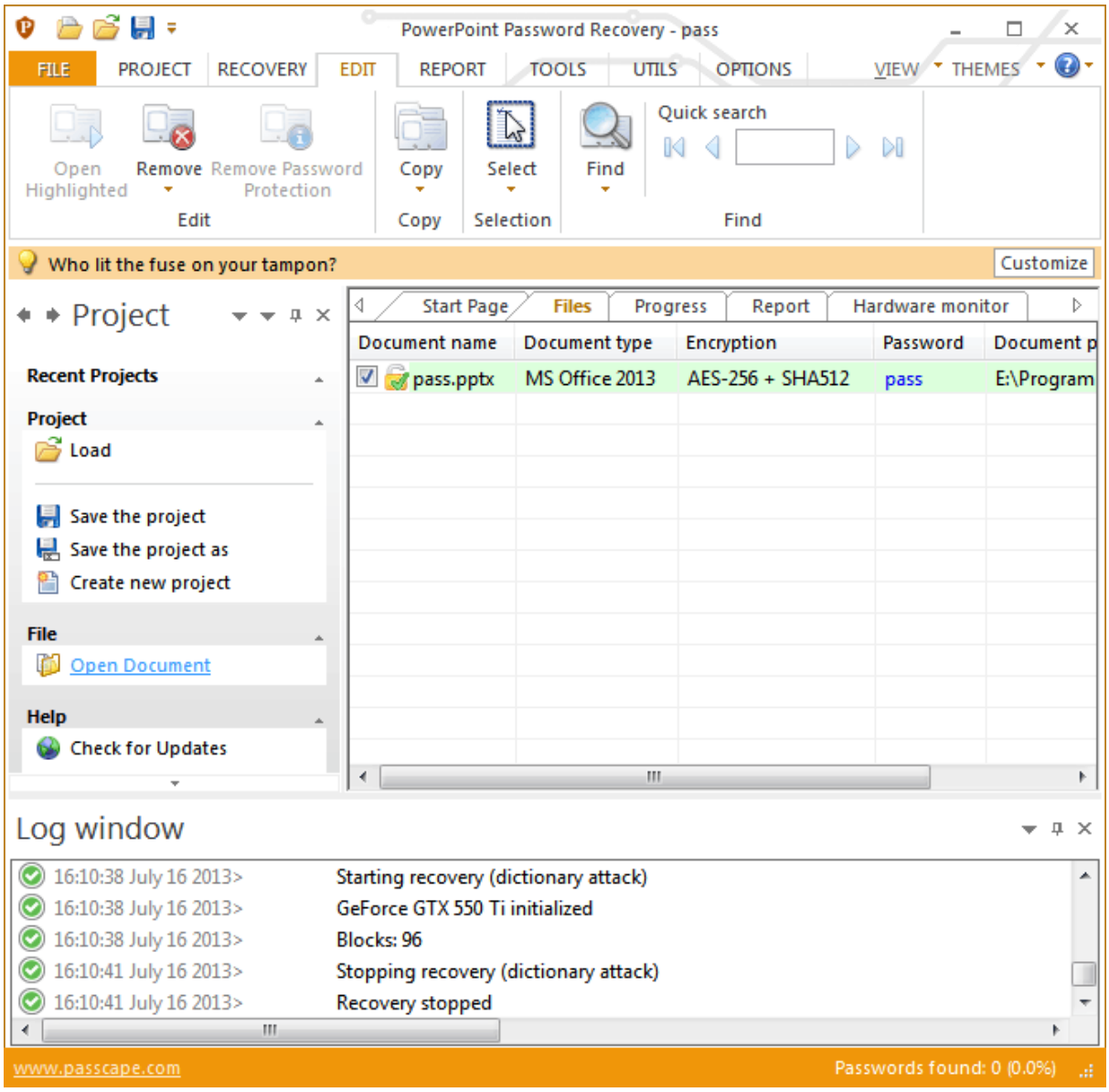
Интерфейс программы

2 Интерфейс программы

2.1 Общее описание

Интерфейс программы выполнен в виде SDI архитектуры, т.е. позволяет работать одновременно только с одним проектом. Работу программы можно условно разбить на несколько этапов:

- Создание проекта.
- Загрузка запароленного документа в проект.
- Настройка опций восстановления, аппаратного ускорения и т.д.
- Расшифровка паролей. Включает в себя выбор, настройку и запуск выбранной атаки или нескольких атак.
- Анализ полученных результатов.



Весь интерфейс условно можно разделить на несколько составляющих:

- Меню программы

Copyright (c) 2024 Passcape Software. All rights reserved.

- Information Bar - предназначена для вывода небольшой текстовой информации. Например, подсказок, предупреждений и пр.
- Task Bar дублирует и дополняет основное меню для обеспечения быстрого доступа к некоторым операциям. Состоит из нескольких вкладок:
- - Проект - содержит основные операции с проектом. Например, открытие, закрытие, создание нового проекта, загрузка документов.
- - Редактирование документов. Дублирует наиболее частые операции редактирования.
- - Инструменты - включает в себя часы, календарь и калькулятор.
- Main Window - несёт основную нагрузку и состоит из нескольких частей. Первая вкладка - окно приветствия. Вторая вкладка содержит список документов для анализа и восстановления. Затем следует вкладка состояния (прогресса) текущей атаки и вкладка со статистикой/отчётами. И, наконец, системный монитор.
- Log Window - необходим для вывода информации о состоянии программы, текущей операции и т.д. Лог программы можно скопировать в буфер или сохранить в файл. Соответствующее меню вызывается щелчком правой кнопки мыши.
- Status Bar - носит информационный характер.

2.2 Меню Проект

2.2.1 Открыть документ

Добавление (загрузка) документа PowerPoint в проект.

2.2.2 Сохранить пароли

Найденные в процессе восстановления пароли можно сохранить в текстовый файл.

2.2.3 Новый

Сохранение текущего проекта и создание нового.

2.2.4 Открыть

Загрузка/открытие сохранённого ранее проекта. Проекты программы имеют расширение *.ppointpr и содержат настройки программы и ссылки на документы. Для увеличения скорости перебора, текущее состояние атаки хранится в отдельном файле progress.ini.

2.2.5 Сохранить

Сохранение текущего проекта. Рекомендуется периодически сохранять критические проекты.

2.2.6 Сохранить Как

Сохранение текущего проекта под другим именем (переименование).

Copyright (c) 2024 Passcape Software. All rights reserved.

2.2.7 Закрыть

Закрыть текущий проект.

2.3 Меню Восстановление

Данный пункт меню служит для выбора и запуска атаки. Имейте в виду, что перед запуском атаки необходимо сначала выбрать/отметить нужный документ в списке. Это делается из меню **Редактирование - Выбор**. Запуск атаки подразумевает также, что были установлены её опции (меню **Опции - Опции атаки**).

2.3.1 Запуск

Запуск выбранной атаки. Во это время все остальные пункты меню становятся неактивными. Следует отметить, что в силу особенности шифрования, перебор паролей возможен только для одного документа, а не всех сразу. Однако в общих настройках можно установить соответствующую опцию для автоматического выбора следующего документа после окончания атаки.

2.3.2 Продолжить

Продолжение атаки с последней запомненной позиции. Необходимо помнить, что после того, как были внесены изменения в опции атаки, последняя запомненная позиция автоматически стирается.

2.3.3 Стоп

Остановка текущей атаки.

2.4 Меню Редактирование

Меню редактирование доступно только при активной вкладке "Файлы" и состоит и четырёх элементов: редактирование, копирование, выбор и поиск.

2.4.1 Открыть активный документ

Открытие выделенного документа в Microsoft Office PowerPoint.

Copyright (c) 2024 Passcape Software. All rights reserved.

2.4.2 Удалить

Удаление записей из списка: высвеченной (т.е. той, на которой находится курсор), отмеченных или сразу всех.

2.4.3 Удалить защиту

Некоторые виды паролей в Microsoft PowerPoint можно не восстанавливать. Можно просто удалить их из документов. Программа поддерживает сброс паролей на редактирование документов PowerPoint и паролей на просмотр и редактирование VBA макросов. Если эти пароли и были заданы одновременно с шифрованием документов, то программа корректно обработает и такой случай. Для этого, после нахождения пароля на открытие, достаточно сохранить документ без шифрования. Пароль на редактирование сбросится автоматически.

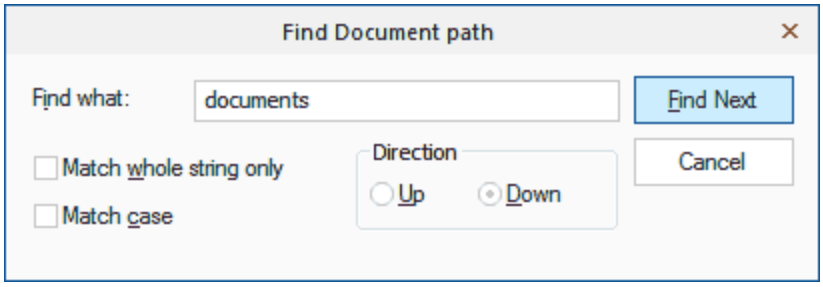
2.4.4 Копировать

Копирование текущей (высвеченной) записи в буфер обмена Windows. Копируется не вся запись целиком, а выбранная часть. Например, имя документа или найденный пароль.

2.4.5 Выбрать

Выбор документа для анализа. Выбранный документ отмечен галочкой. Если во время атаки найден пароль для выбранного документа, то отметка этой записи автоматически сбрасывается, а сама запись помечается зелёным цветом. В программе имеется возможность автоматического запуска атаки на следующий документ в списке.

2.4.6 Поиск



Если количество записей переваливает за сотню, то отыскать нужную запись порой бывает довольно затруднительно. Для этого существует два вида поиска: поиск по заданному полю, например, имени и быстрый поиск последовательных записей. В последнем случае, сканирование будет выполняться последовательно по всем записям целиком.

Copyright (c) 2024 Passcape Software. All rights reserved.

2.5 Меню Отчёты

В этом меню вы можете создать распечатать или сохранить один из отчётов о работе программы. В настоящее время доступны следующие отчёты:

- Отчёты о паролях
- Статистика атак
- Различная информация
- Анализ словарей

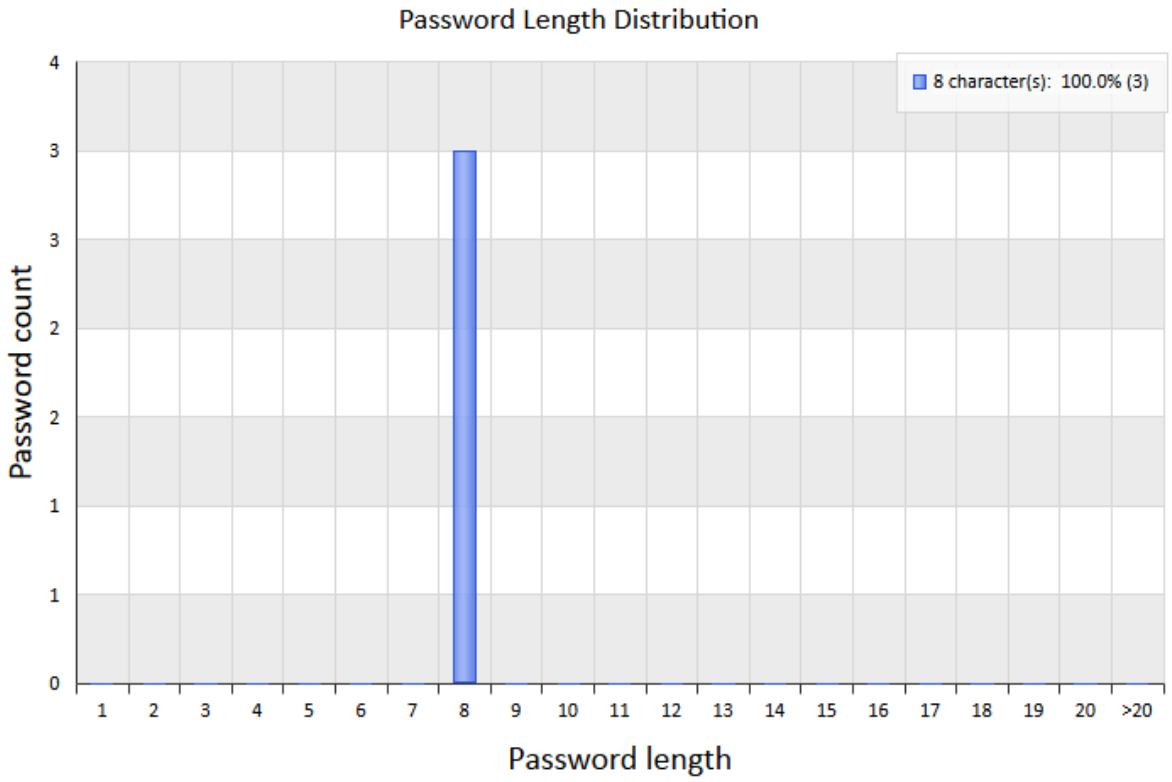
2.5.1 Отчёты о паролях

Отчёты о паролях включают в себя следующие пункты:

- **Парольные риски** - отчёт о найденных паролях: соотношение количества пустых, взломанных и не поддавшихся расшифровке паролей
- **Сложность паролей** - показывает количество восстановленных паролей и диапазон символов из которых они состоят
- **Длина паролей** - распределение длин найденных паролей
- **Время поиска паролей** - время, затраченное на поиск паролей. Наиболее уязвимые пароли отмечены красной палитрой.

Copyright (c) 2024 Passcape Software. All rights reserved.

- **Найденные и не найденные** - соотношение количества найденных и не расшифрованных паролей
- **Найденные пароли** - подробный отчёт о найденных паролях: сколько из них пустых, сколько полностью восстановлены.

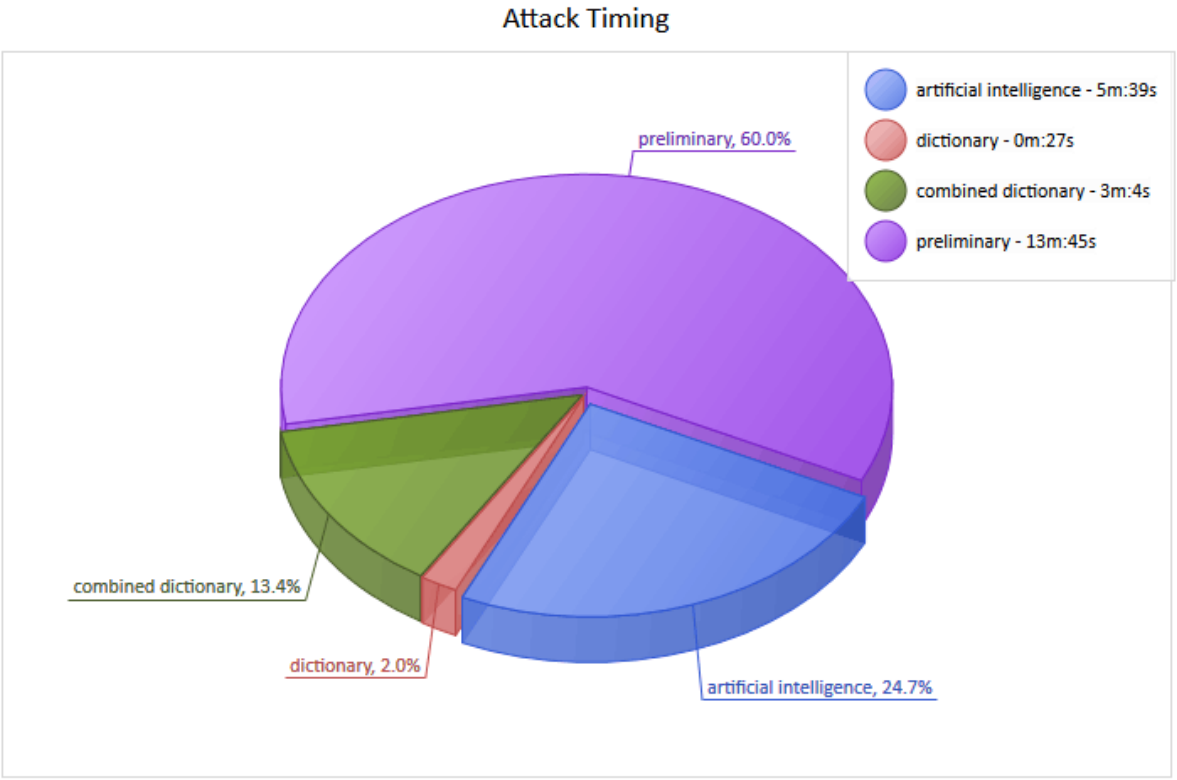


2.5.2 Статистика атак

Статистика атак включает в себя следующие отчёты:

- **Предпочтительная атака** - статистика по количеству и типу запущенных атак
- **Время атаки** - анализ времени, затрачиваемого на каждую атаку
- **Эффективность атаки 1** - анализ эффективности: соотношение затрачиваемого времени к найденным во время атаки паролям
- **Эффективность атаки 2** - анализ эффективности: общая суммарная эффективность каждой атаки

Copyright (c) 2024 Passcape Software. All rights reserved.

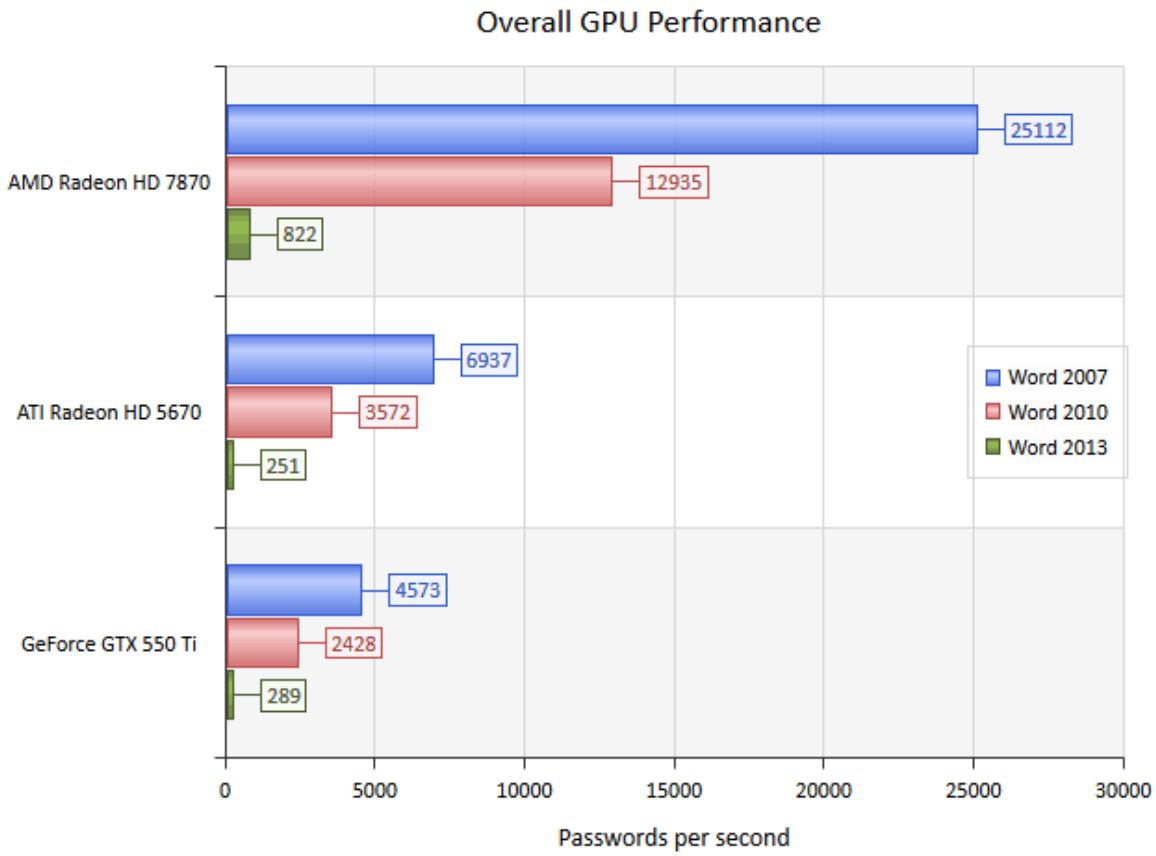


2.5.3 Различная информация

Различная информация состоит из следующих пунктов:

- **Скорость процессора** - сравнение скорости работы вашего процессора.
- **Скорость GPU** - скорость работы графической карты в режиме перебора паролей.
- **Взломанные документы** - количество взломанных документов.
- **Взломанные документы и пароли** - список взломанных документов с паролями.

Copyright (c) 2024 Passcape Software. All rights reserved.



2.5.4 Анализ словарей

Данные отчёты позволяют собирать различную статистику и производить полноценный анализ словарей. В качестве исходных словарей, например, можно использовать список расшифрованных программой паролей. Сбор статистики осуществляется как по всем словам заданного словаря, так и по определённому диапазону, например только для определённой длины. В этом меню доступны следующие отчёты:

- Распределение длин паролей - показывает график распределения длин паролей, т.е. количество паролей, приходящихся на определённую длину.
- Уникальность паролей - состоит ли исходный список из уникальных слов или есть повторяющиеся пароли.
- Популярность паролей - этот отчёт определяет какие пароли являются наиболее популярными, показывает их процент по отношению к общему количеству.
- Формат паролей - вывод статистики 20 наиболее популярных форматов. Формат паролей определяется маской символов. Например, маска DDUUUUDD соответствует всем паролям, состоящим из двух начальных и конечных цифр и четырёх заглавных букв в середине. Популярные форматы паролей можно сохранить в файл, например, чтобы использовать в дальнейшем в атаке по маске.
- Уникальные наборы символов - график паролей, состоящих из одного уникального набора символов и их процентное отношение к паролям, состоящим из нескольких наборов.
- Разнообразие наборов символов - общее процентное соотношение паролей состоящих из одного, двух и т.д. наборов.

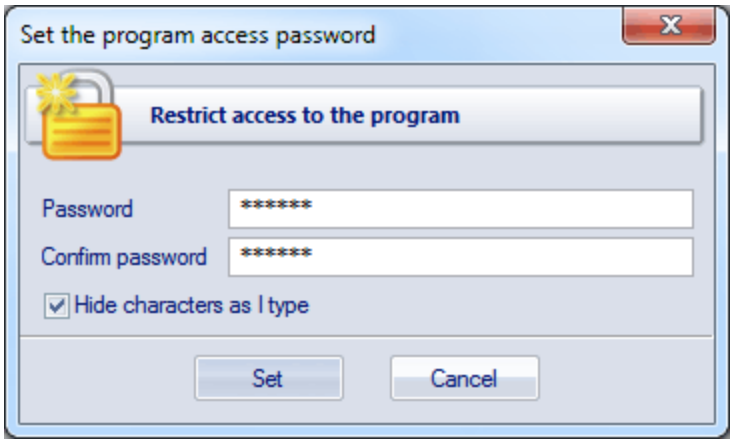
Copyright (c) 2024 Passcape Software. All rights reserved.

- Наборы символов - список всех наборов символов, из которых состоят исходные пароли.
- Порядок наборов символов - определяет наиболее популярные шаблоны паролей в соответствии с порядком наборов символов, используемых в нем. Например в шаблон digit-string-special попадают следующие пароли: 123password!@#, 1ove*****, 12monkey^.
- Частота символов - статистика по частоте встречающихся в исходных словах символов. Отображается 20 самых часто встречающихся символов.
- Уникальность символов - 20 самых редко встречающихся символов.
- Часто встречающиеся символы в начале - статистика по самым часто встречающимся комбинациям (от 1 до 3 символов) в начале слов.
- Часто встречающиеся символы в конце - статистика по самым часто встречающимся комбинациям (от 1 до 5 символов) в конце слов.
- Часто встречающиеся комбинации - 20 самых часто встречающихся комбинаций от 4 до 8 символов.

2.6 Меню Инструменты

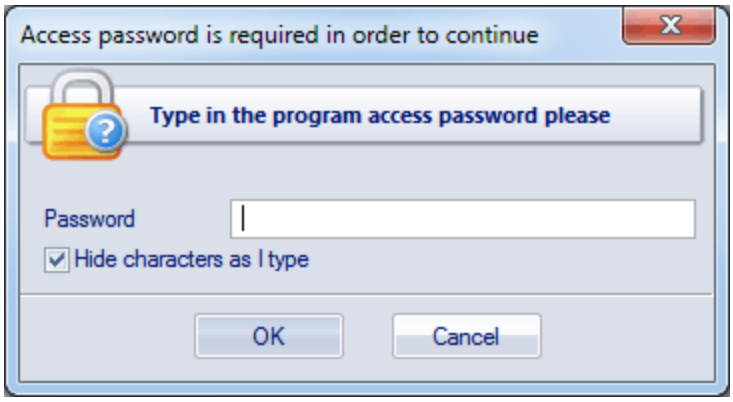
Инструменты состоят из двух частей: инструменты для разграничения доступа к программе и инструменты для работы с паролями.

2.6.1 Доступ к Программе

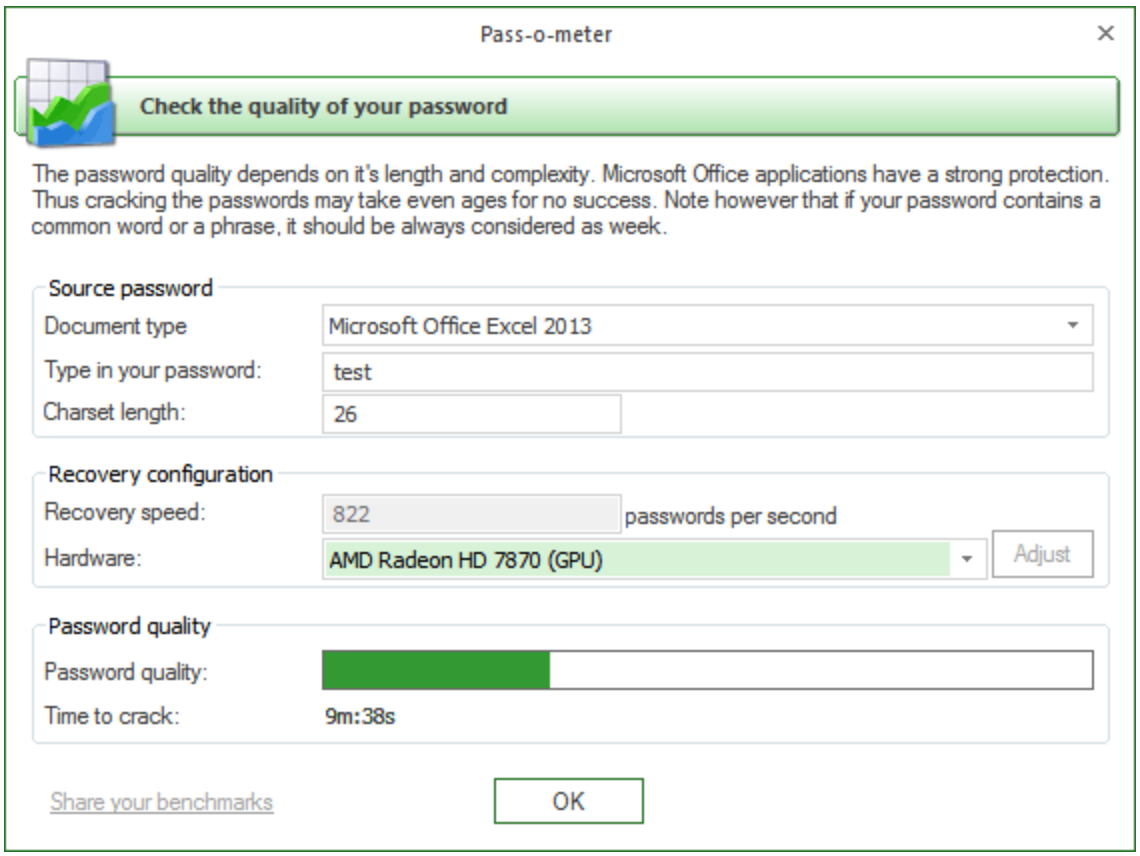


В том случае, если кроме вас к компьютеру или к вашей учётной записи имеет доступ кто-то другой, можно просто установить пароль на программу. В этом случае при запуске программы у пользователя будет запрошен пароль, без которого дальнейшая работа с программой невозможна.

Copyright (c) 2024 Passcape Software. All rights reserved.



2.6.2 Пасс-о-метр



Инструмент для измерения стойкости вашего пароля против взлома. При первом запуске программа попросит провести тест скорости вашего компьютера. Для проверки качества пароля надо:

- Ввести пароль в соответствующее поле ввода
- Выбрать тип документа.
- Выбрать тип железа, используемого для взлома пароля. "Этот компьютер" соответствует скорости перебора вашего компьютера.

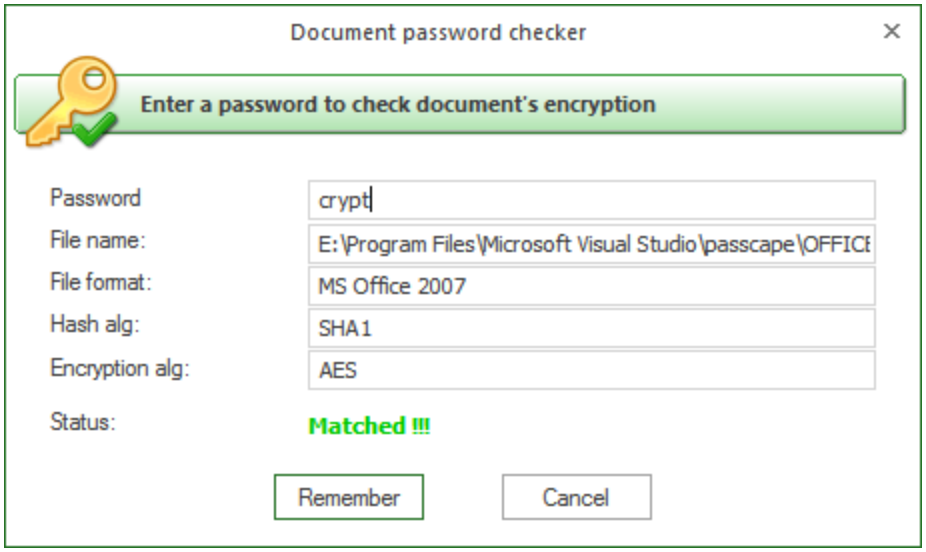
Copyright (c) 2024 Passcape Software. All rights reserved.

- Если вы хотите измерить скорость работы графической карты, из соответствующего выпадающего списка необходимо выбрать пункт "Этот компьютер (видеокарта)" и нажать кнопку "Тест". Измерить скорость работы GPU можно также в соответствующем пункте меню **Отчёты**.

Внизу вы увидите качество вашего пароля и сколько времени потребуется для его взлома в выбранной конфигурации.

Если вы поделитесь с нами скоростью вашего компьютера, мы будем вам очень признательны.

2.6.3 Проверка Пароля



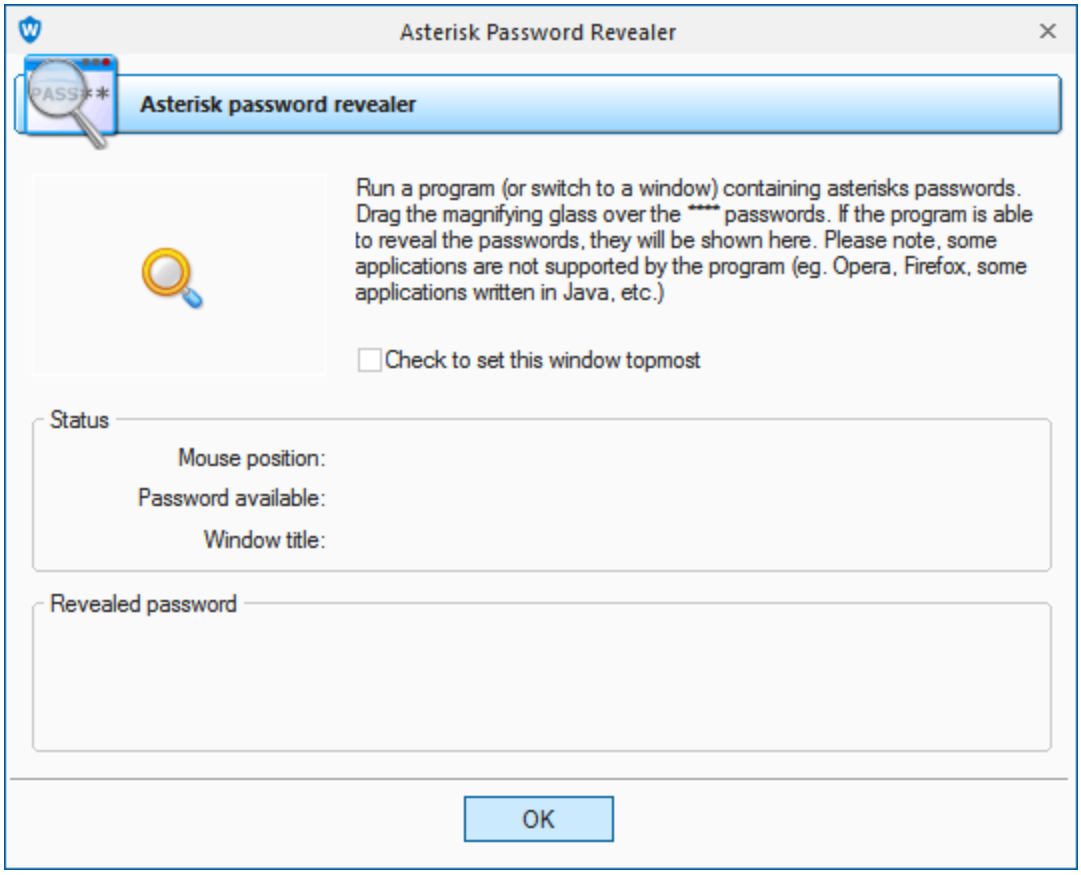
Данный инструмент предназначен для ручной проверки пароля. Это часто бывает необходимо для быстрой проверки того или иного документа.

2.7 Меню Утилиты

Меню Утилиты содержит дополнительные надстройки, предназначенные главным образом для продвинутых пользователей. В ходе развития программы, надстройки пополняются новыми утилитами.

Copyright (c) 2024 Passcape Software. All rights reserved.

2.7.1 Открыватель паролей за звёздочками ***



Данный инструмент позволяет открывать пароли, которые прячутся за звёздочками. Это бывает полезно, когда требуется быстро вспомнить **** пароль, но нет необходимых программ под рукой для его восстановления. Данный инструмент также работает в режиме drag-n-drop: нужно перетащить волшебную лупу из окна программы на поле со звёздочками.

Однако эта утилита имеет ряд ограничений:
Некоторые программы имеют свой собственный GUI, поэтому asterisks revealer не работает на таких программах. К ним относятся браузеры Opera, Mozilla, Firefox и т.д.
Некоторые Веб сайты имеют встроенную защиту, которая за звёздочками прячет либо чепуху, либо там действительно находятся символ * (звёздочки прячутся за звёздочками!). Пример такого сайта - mail.yahoo.com, который хранит зашифрованные пароли в кукисах.
В некоторых системных диалогах Windows, за звёздочками также скрываются символы *, а не настоящий пароль.

Для корректной работы этого инструмента требуется наличие привилегий администратора.

2.7.2 Утилиты для работы со словарями

Довольно скудное количество приемлемых утилит для работы со специализированными словарями паролей, сподвигнуло разработчиков программы на создание своего собственного набора инструментов. С помощью этого набора можно легко создавать новые, редактировать имеющиеся словари и использовать их в любых программах для восстановления паролей.

Copyright (c) 2024 Passcape Software. All rights reserved.

2.7.2.1 Создание словаря путем индексации локальных файлов

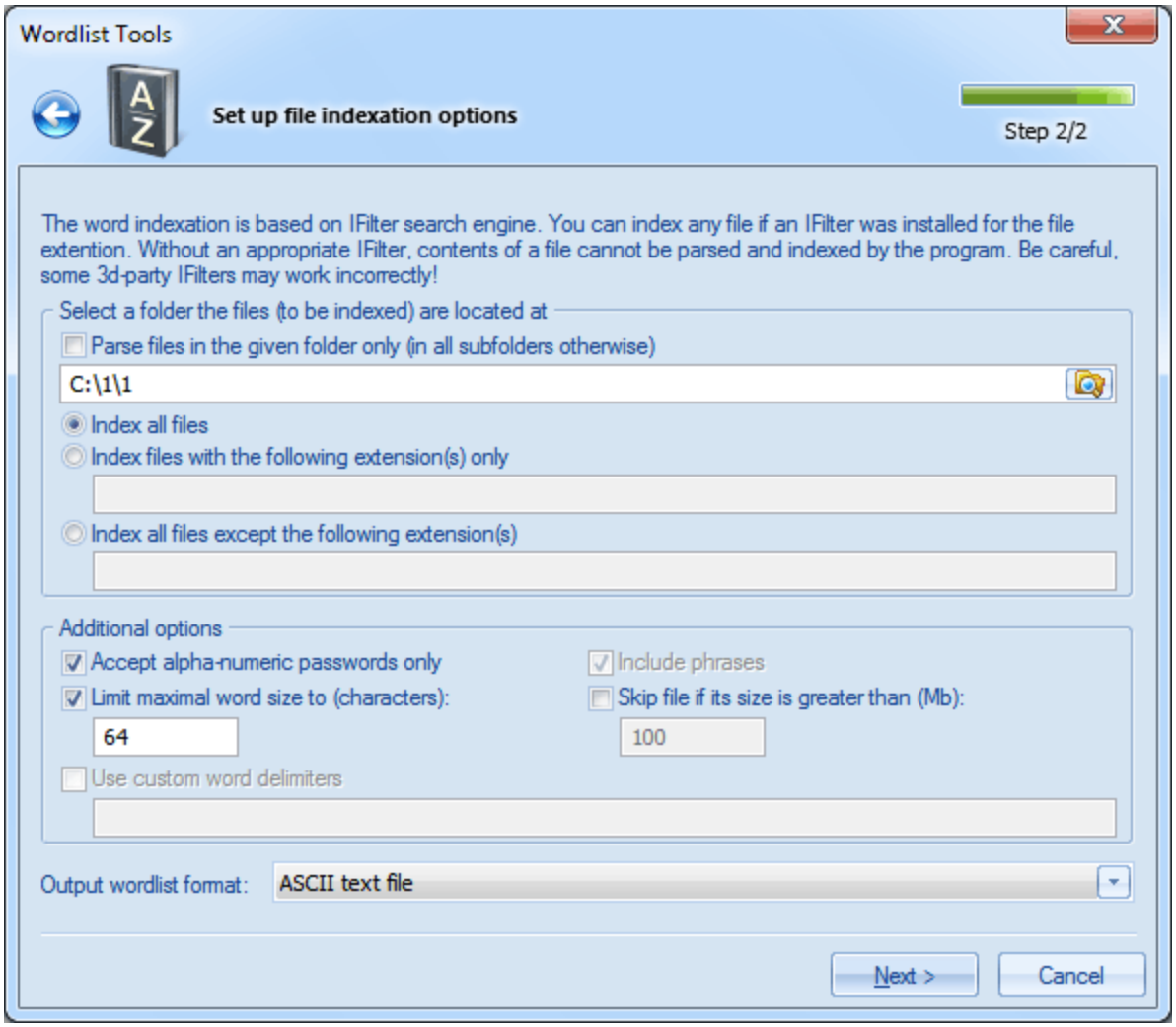
Данный инструмент предназначен для создания нового словаря выборкой (индексацией) слов локальных файлов вашего компьютера. Например, это могут быть *.html, *.xml, *.txt, *.doc файлы, а также *.mdb, *.pdf, *.exe файлы и т.д.

Индексация основана на технологии IFilter, подробнее о которой можно почитать на сайте Wikipedia. Суть этой технологии, разработанной в Microsoft, сводится к тому, чтобы иметь возможность индексировать текст любого файла, для которого установлен соответствующий плагин IFilter. Таким образом, можно получить доступ к тексту, находящемуся, например в файлах *.exe, *.dll, в базе данных почтовых клиентов и т.д.

Несмотря на то, что в Интернете можно найти множество плагинов IFIlter, как коммерческих так и бесплатных, программа имеет встроенную поддержку следующих типов файлов:
архивы: *.zip, *,cab, *.rar
программы: *.exe, *.dll, *,cpl, *.ocx, *.sys, *.scr, *.drv
текст: *.txt, *.dic
internet: *.html, *.htm
Таким образом, файлы с указанными расширениями будут обрабатываться программой даже в том случае, если в системе не установлен ни один IFilter.

Windows 7 имеет встроенный инструмент Windows Desktop Search, обладающий широким набором фильтров для поддержки большинства популярных документов. На других операционных системах, Windows Desktop Search можно установить, скачав его с официального сайта Microsoft.

Copyright (c) 2024 Passcape Software. All rights reserved.



Настройка этого инструмента состоит из двух групп. В первой группе необходимо установить путь к исходному каталогу, файлы в котором необходимо проиндексировать, и задать способ обработки файлов. А именно:

- Обрабатывать файлы только в заданном каталоге. Если эта опция не установлена, то программа подвергнет рекурсивному анализу все вложенные подкаталоги и файлы в них.
- индексировать все файлы
- индексировать только файлы с заданными расширениями
- индексировать все файлы, кроме тех, расширения которых даны

Расширения файлов задаются без точки и отделяются запятой. Например: txt,dic,xml,chm,htm

Группа с дополнительными настройками обеспечивает кастомизацию обработки файлов, а именно:

- Только буквенно-цифровые пароли. Если эта опция установлена, то программа пропустит все специальные символы. Только слова, состоящие из букв и/или цифр будут обрабатываться.
- Включать фразы. Эта опция позволяет обрабатывать и включать в словарь фразы. В данном случае, фраза рассматривается в качестве набора символов (максимальной длины 256) с, как минимум, одним пробелом.
- Ограничить размер слов. Рекомендуется всегда устанавливать эту опцию. Оптимальная максимальная длина слова в словаре составляет 8-64 знаков. Уменьшение максимальной длины приводит, иногда довольно значительно, к увеличению скорости обработки файлов.

Copyright (c) 2024 Passcape Software. All rights reserved.

- Пропускать файлы, если их размер больше заданного. Некоторые IFilter'ы очень долго обрабатывают большие файлы, что может привести к "зависанию" программы.
- Использовать свои собственные разделители слов. При обработке файлов можно задавать свои собственные разделители слов. Например, это могут быть следующие символы: !"#$%&'()*+,-./:;<=>?@{}[]_ и, конечно, пробел.

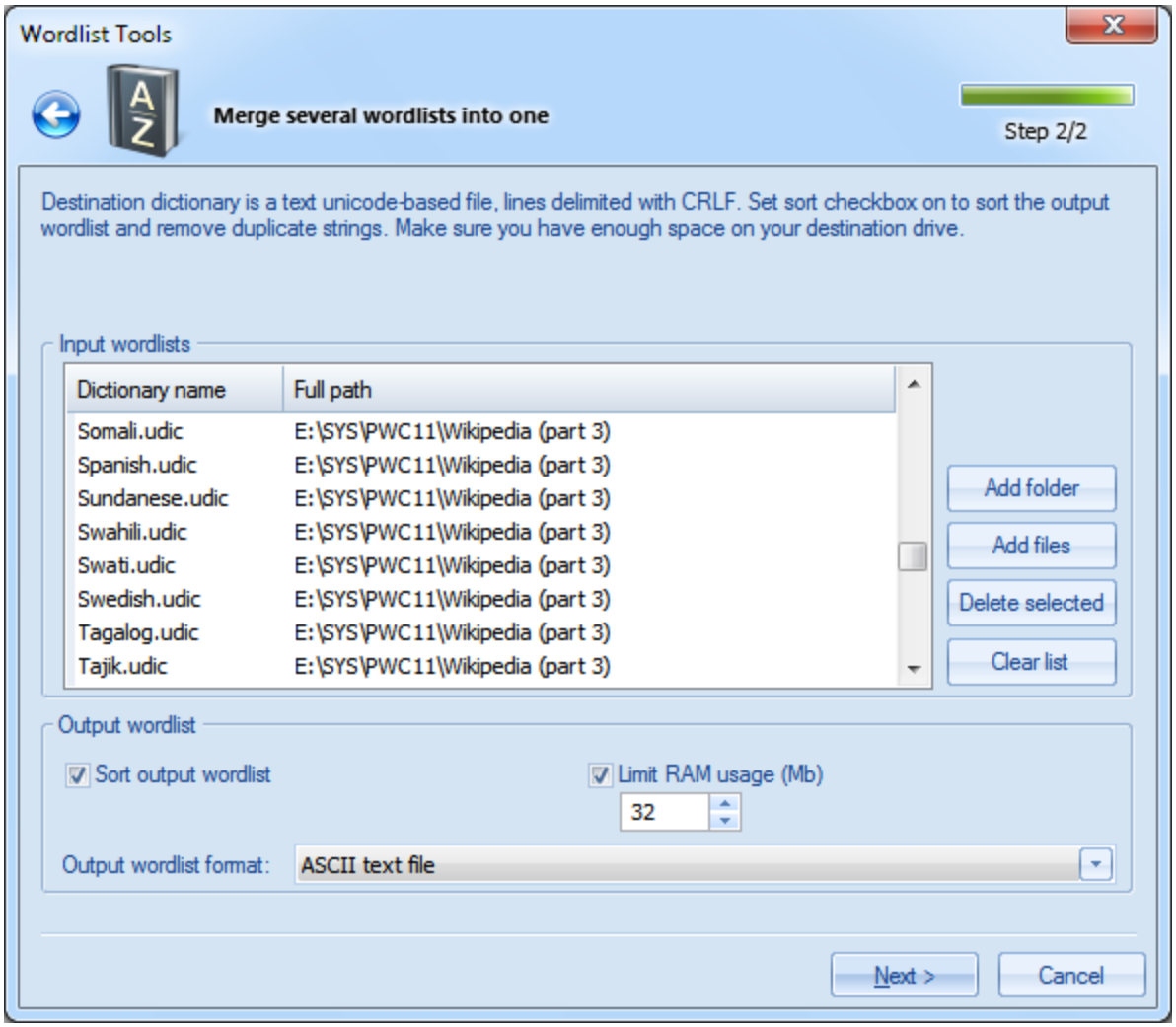
Нажатие кнопки Next> запускает процесс индексации, который может занять значительное время. Для увеличения скорости работы, словарь всех найденных во время индексации слов создаётся в оперативной памяти компьютера, что требует значительных затрат. Если во время работы система выдала ошибку нехватки памяти, попробуйте уменьшить максимальную длину слов или ограничить количество обрабатываемых файлов и повторить все сначала. После завершения операции и сохранения найденных слов на диск, необходимо отсортировать их для получения полноценного словаря. Найденные слова гарантировано уникальны, т.е. не содержат дубликатов.

Будьте осторожны, фильтры некоторых сторонних разработчиков могут работать некорректно, что, как правило, приводит к зависанию, сбою или экстренному выходу из программы. Например, с ошибками работают некоторые фильтры для обработки pdf в системе Windows XP.

2.7.2.2 Слияние словарей

Инструмент слияния словарей используется когда необходимо объединить два или более словаря в один.

Copyright (c) 2024 Passcape Software. All rights reserved.

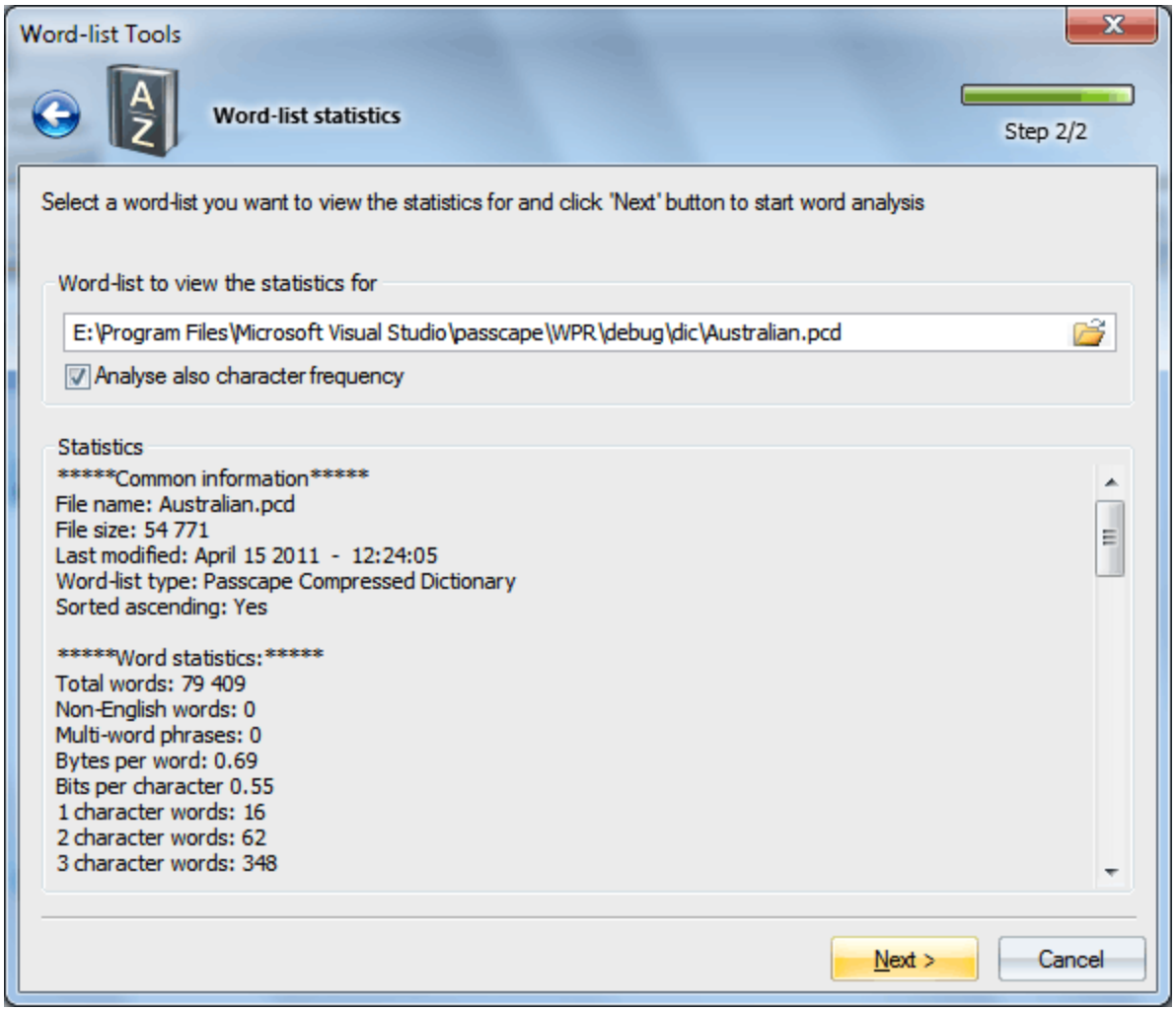


Если опция сортировки выходного словаря не установлена, то слияние происходит путём простого добавления, без сортировки и проверки повторяющихся слов. На практике, однако, более часто используется слияние с установленной опцией сортировки, при которой все слова в выходном словаре будут отсортированы в алфавитном порядке и исключены дубликаты.
Сортировка может отъедать значительное количество оперативной памяти, поэтому целесообразно также устанавливать лимит на используемую память (в небольшой ущерб скорости работы).

2.7.2.3 Анализ словаря

Анализ словаря собирает и показывает следующую статистику:

Copyright (c) 2024 Passcape Software. All rights reserved.



Общая информация

- Имя словаря
- Размер в байтах
- Тип файла
- Время последней модификации
- Отсортирован в алфавитном порядке или нет (проверка производится только если файл отсортирован по возрастанию)

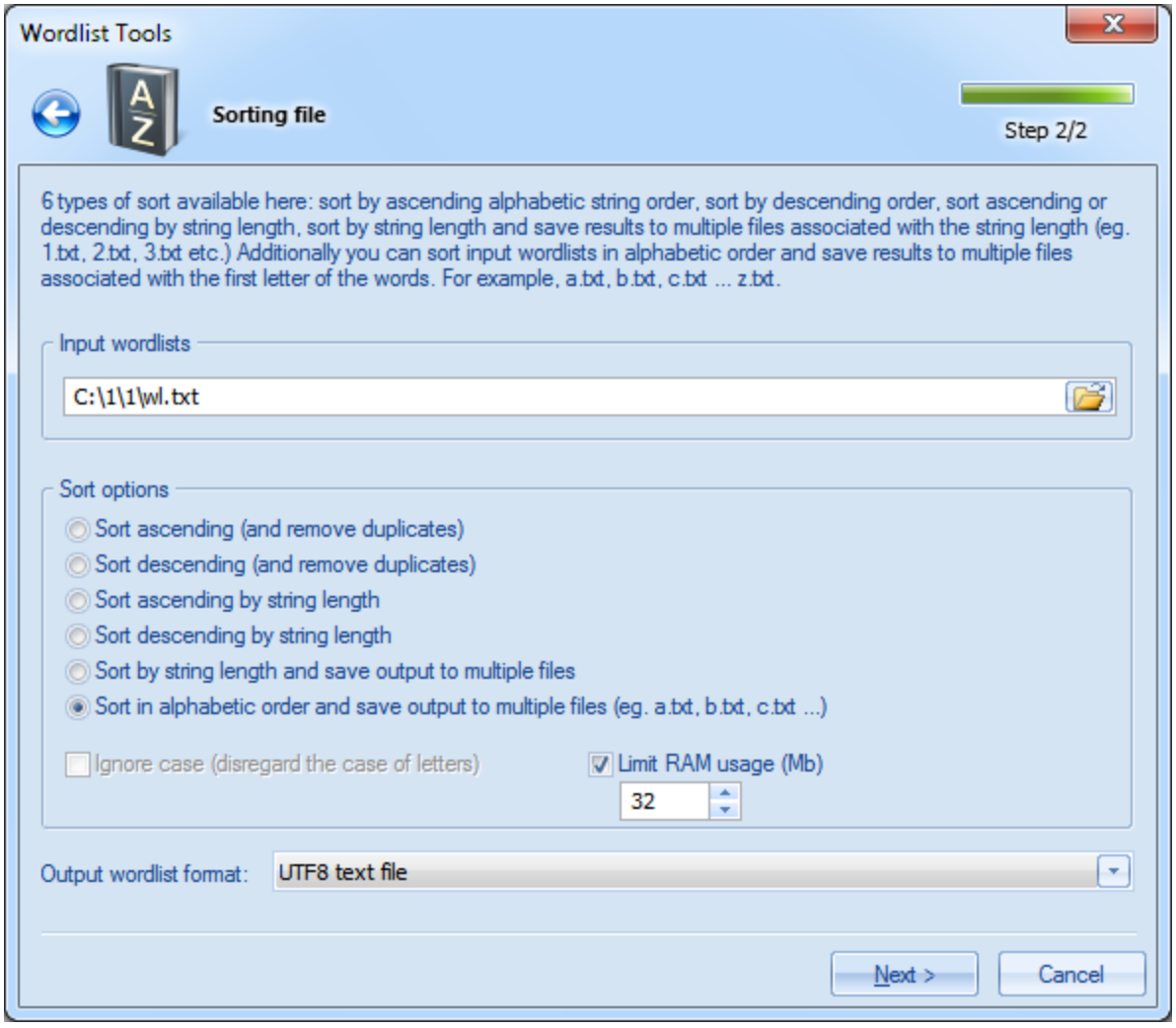
Статистика слов

- Общее количество слов
- Количество неанглийских слов
- Количество фраз, т.е. слов, отделённых пробелом
- Количество байт на одно слово, без учёта разделителя слов. Показывает среднюю степень сжатия словаря.
- Количество бит на один символ. Показывает реальную степень сжатия словаря. Например, в UNICODE словаре количество бит на букву будет стремиться к 16 (разделитель слов не учитывается при подсчёте), в обычных ASCII словарях - к 8. В некоторых сжатых pcd словарях одна буква может кодироваться в менее чем 1 бите (смотрите скриншот).
- Статистика слов - сколько слов, состоящих из 1, 2, 3 и т.д. букв
- Анализ частотности букв (если установлена соответствующая опция)
- Частота, с которой встречается та или иная буква в словаре

Copyright (c) 2024 Passcape Software. All rights reserved.

2.7.2.4 Сортировка словаря

Сортировка списка слов представлена 6 режимами, из которых 4 основных и 2 расширенных. К основным режимам сортировки относится сортировка списка слов в алфавитном порядке (по возрастанию и убыванию) и сортировка по длине слова. Во время сортировки по алфавиту или по длине слова происходит также автоматическое удаление дубликатов слов.



Дополнительно можно отсортировать список слов по длине и сохранить результаты в несколько файлов, которые ассоциируются с длиной слова. Например, в файл 1.txt будут записаны все слова, состоящие из 1 буквы, в 2.txt - из двух букв и т.д.

Аналогично работает и шестой режим сортировки. При этом исходный список сортируется в алфавитном порядке и создаётся несколько целевых словарей, соответствующих первой букве слова. К примеру, все слова, начинающиеся на букву A будут записаны в файл A.txt, слова, начинающиеся с B, - в B.txt и т.д. Следует иметь в виду, что в некоторые слова могут начинаться на символы, которые не могут быть использованы в качестве имени файла. В этом случае, программа автоматически предложит им замену, о чем выдаст соответствующее предупреждение в окне сообщений.

Copyright (c) 2024 Passcape Software. All rights reserved.

Если установлена опция 'игнорировать регистр букв', то сортировка будет происходить без учёта регистра. Т.е. слова bad, Bad или BAD будут считаться одинаковыми, со всеми вытекающими отсюда последствиями.

Сортировка больших файлов (поддерживаются файлы объёмом более 4 Гб) подразумевает интенсивное использование оперативной памяти, объем которой можно лимитировать соответствующей опцией. Для больших файлов, не рекомендуется устанавливать лимит используемой памяти менее 16 Мб, т.к. это может повлиять на быстродействие сортировки.

Имя целевого словаря может совпадать с исходным, однако это делать не рекомендуется.

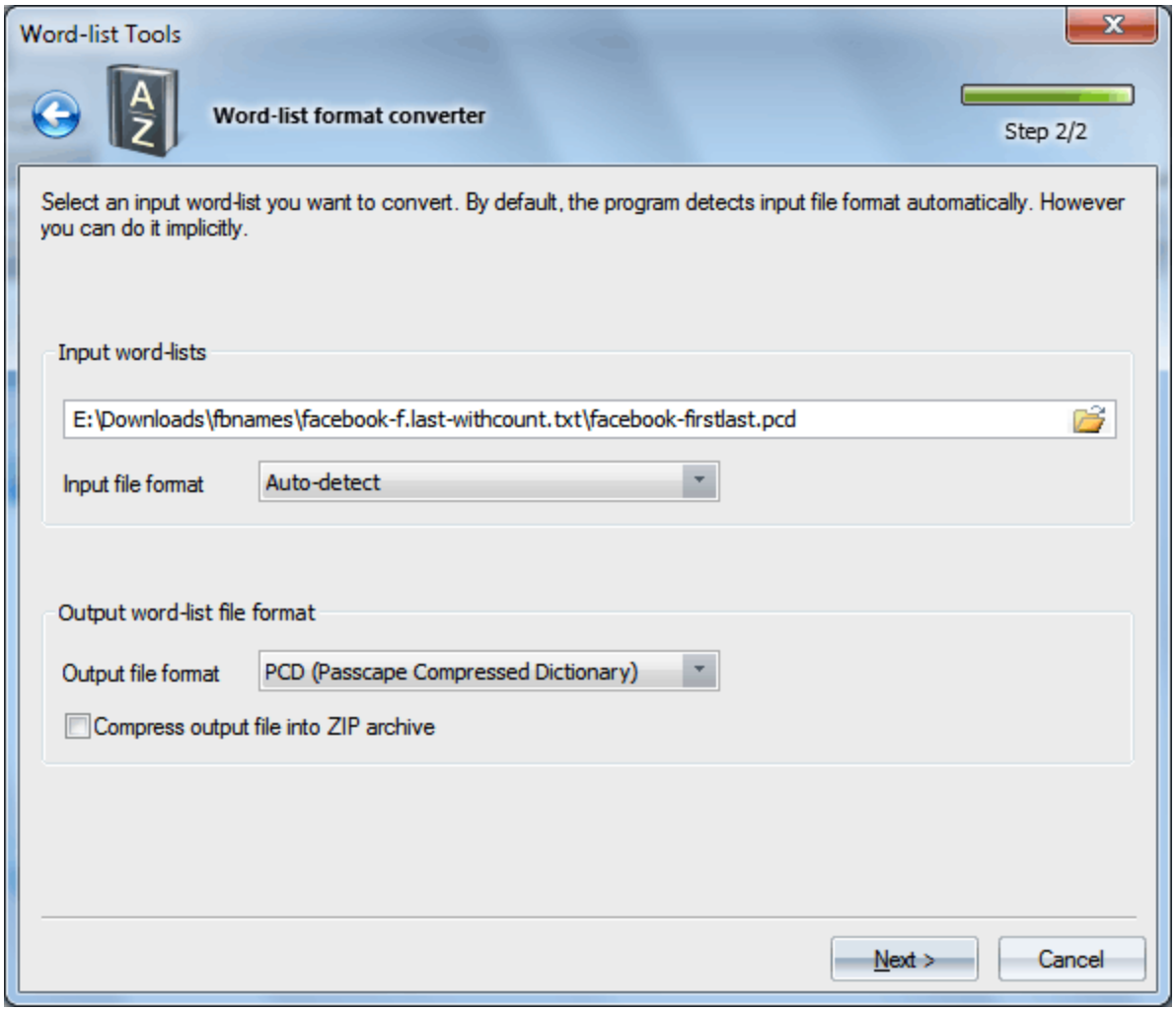
При сортировке могут создаваться вспомогательные файлы во временном каталоге программы.
Убедитесь, что на диске, где расположен временный каталог, достаточно места для своп файлов.

2.7.2.5 Конвертер словарей

Множество словарей, которые можно найти в Интернете, представлены, как правило, тремя основными форматами: ASCII, UTF16 (Unicode) и UTF8. С помощью данного инструмента можно конвертировать словарь из одного формата в другой, а также опционально сжимать их в ZIP файл. Кроме трёх вышеупомянутых форматов, программа имеет поддержку своего собственного формата PCD (Passcape Compressed Dictionary), который в большинстве случаев, даёт больший выигрыш в размере даже по сравнению со сжатым ZIP архивом.

Создание больших PCD файлов может потребовать значительное время!

Copyright (c) 2024 Passcape Software. All rights reserved.



Интерфейс этого инструмента довольно прост. В верхней группе необходимо выбрать исходный словарь и его формат. По умолчанию, программа определяет формат файла самостоятельно, но можно задавать его и непосредственно.

Если формат PCD файла распознаётся однозначно, то с текстовыми файлами не все так просто. Как правило, текстовые файлы/словари в формате UTF16 или UTF8 имеют в начале двух- или трёх-байтовый маркер, описывающий тип файла. Однако, встречаются Юникодные словари без определительных маркеров. Для таких 'тяжёлых' случаев следует выставлять тип исходного файла вручную. Иначе программа, не увидев соответствующий идентификатор, неверно определит файл как ASCII.

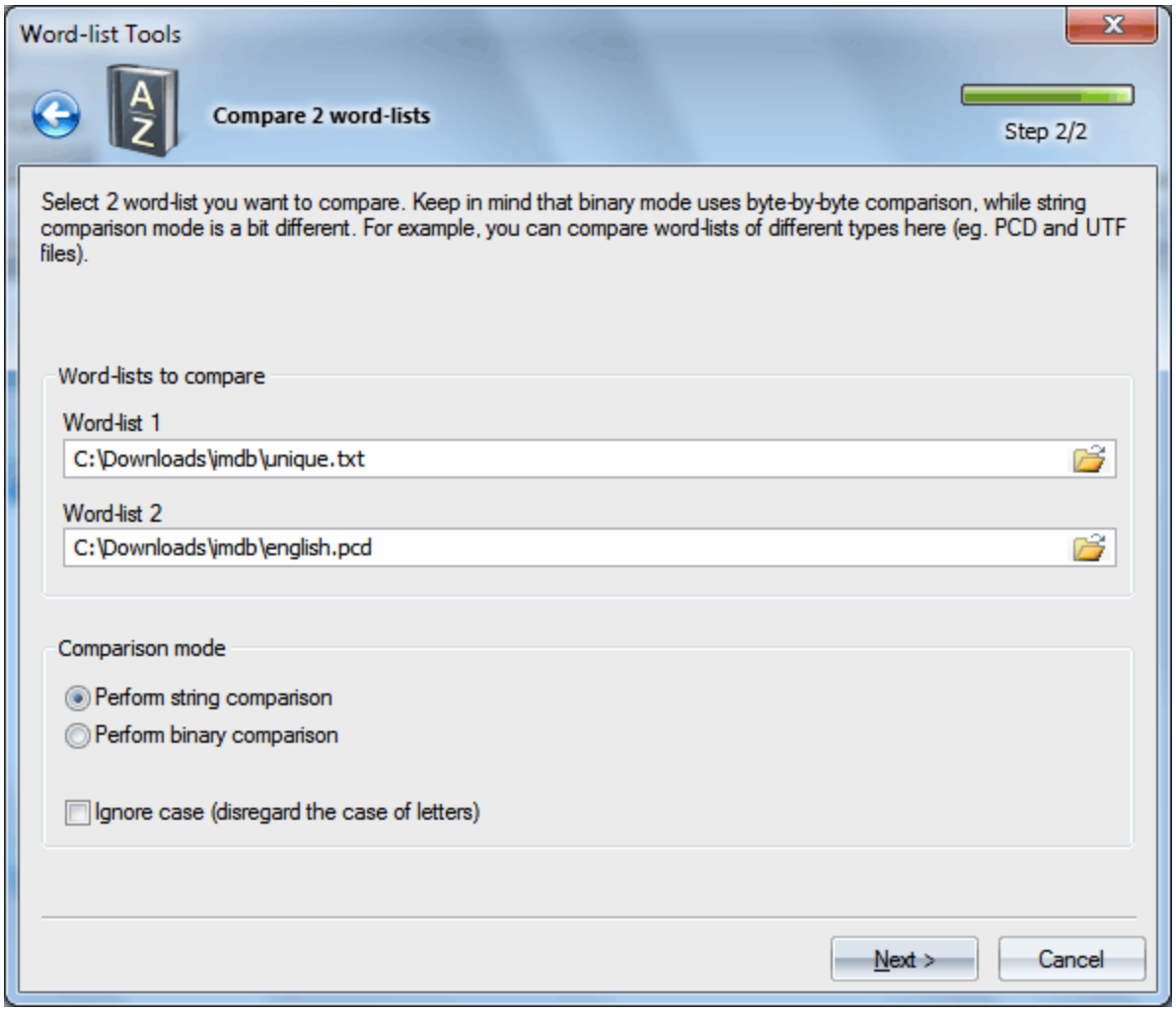
Целевой словарь аналогично задаётся одним из четырёх описанных выше форматов. Установленная опция компрессии дополнительно сожмёт выходной файл в ZIP архив.

Имя целевого словаря может совпадать с исходным, однако это делать не рекомендуется.

2.7.2.6 Сравнение словарей

Иногда требуется определить идентичность двух файлов. Для этого и существует инструмент сравнения словарей.

Copyright (c) 2024 Passcape Software. All rights reserved.



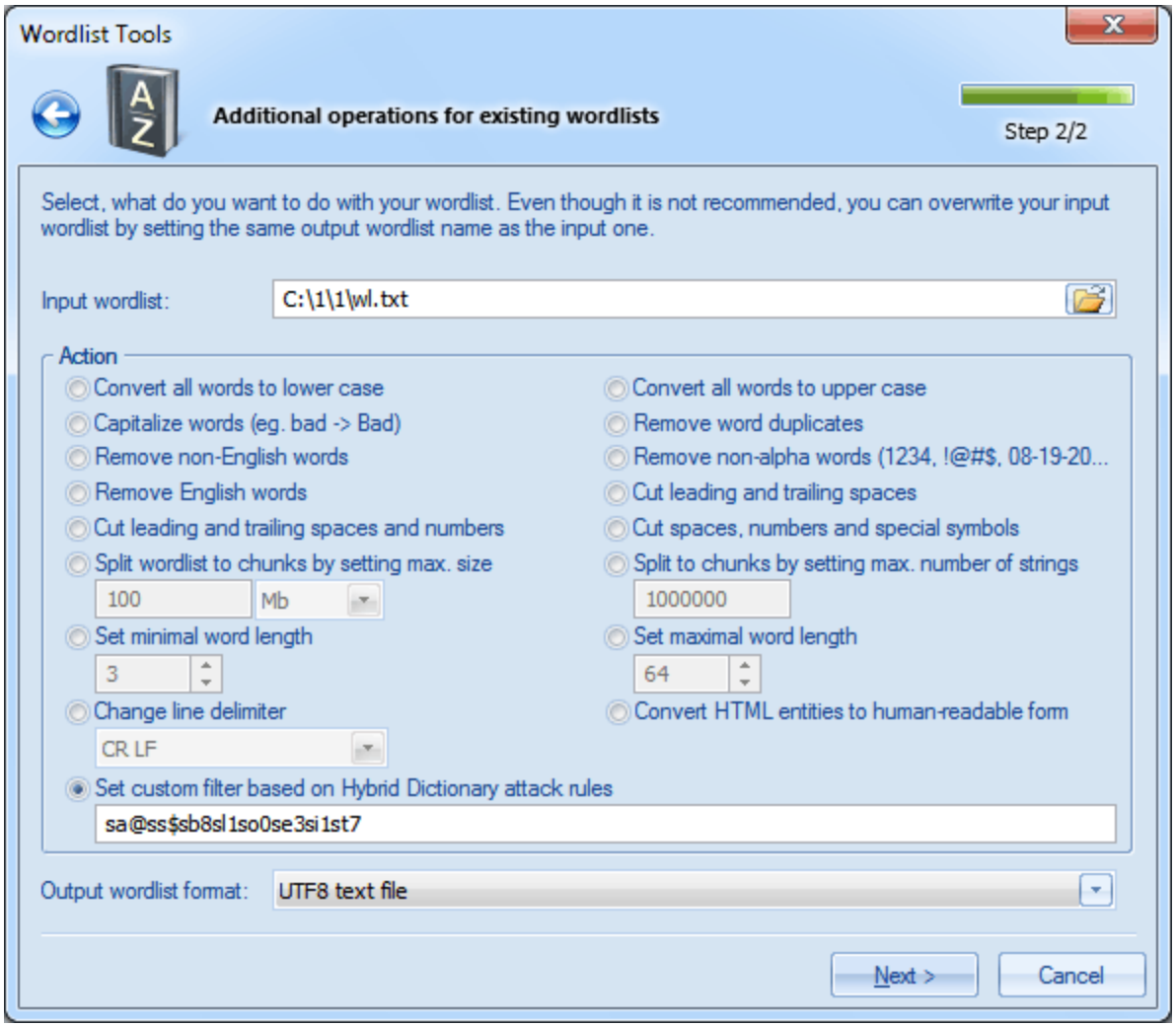
В данном инструменте предусмотрены два режима работы:
1. Двоичное сравнение, для побайтного сравнения файлов
2. Построчное сравнение, которое сравнивает не байты, а слова. Этот режим примечателен тем, что можно задавать словари различных форматов. Например, PCD и UNICODE, или UNICODE и ASCII.

Если установлена опция игнорирования регистра букв (только в режиме построчного сравнения), то, например, слова bad и Bad будут считаться одинаковыми.

2.7.2.7 Дополнительные инструменты

Дополнительные инструменты предназначены главным образом для редактирования и доводки уже готовых словарей.

Copyright (c) 2024 Passcape Software. All rights reserved.



Инструменты включают в себя следующие операции:

- Преобразование всех слов словаря в нижний регистр. Например, BAD -> bad.
- Преобразование слов в верхний регистр. Например, Bad -> BAD.
- Первая буква - заглавная, остальные строчные. Например, bad -> Bad.
- Удаление дубликатов (повторяющихся) слов
- Удаление неанглийских слов
- Удаление слов, целиком состоящих из цифр и/или специальных символов. Например, 12345, !@#$%, 08-19-10 и т.д.
- Удаление английских слов
- Обрезание/удаление пробелов спереди и сзади слова
- Обрезание/удаление пробелов и цифр
- Обрезание/удаление пробелов, цифр и специальных символов
- Разбиение словаря на части по максимальному размеру
- Разбиение словаря на части по максимальному количеству слов
- Удаление слов, меньше заданной длины
- Удаление слов, больше заданной длины
- Изменение разделителя строк
- Конвертер HTML объектов. Например, **&** -> **&** или **@** -> **@**
- Установка своего собственного фильтра на основе правил Гибридной Атаки по словарю

Copyright (c) 2024 Passcape Software. All rights reserved.

В качестве исходного словаря поддерживаются файлы в формате ASCII, UTF16, UTF8 и PCD. Выходной словарь может быть текстом ASCII, UTF16, либо UTF8.

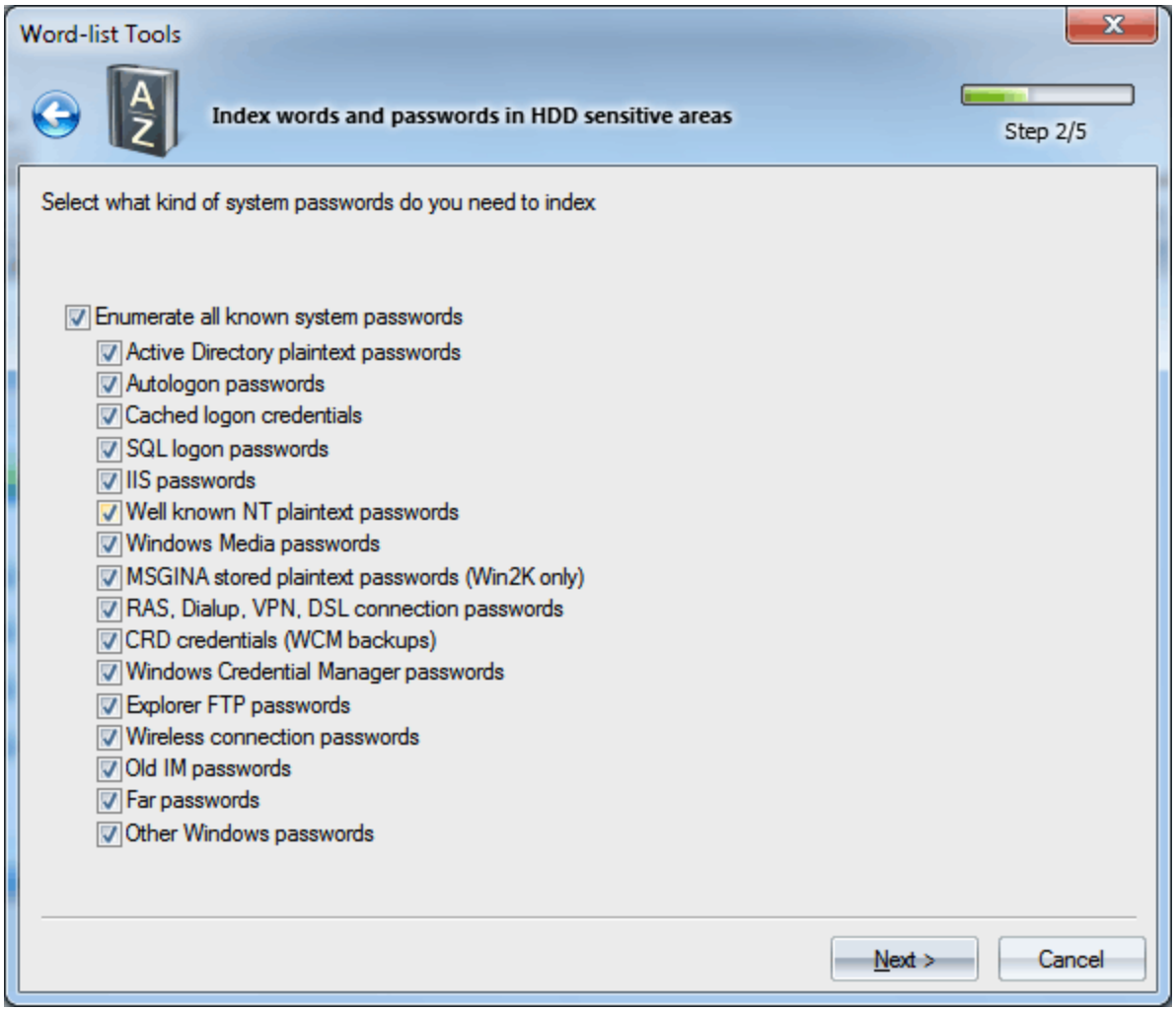
Имена исходного и целевого словаря могут быть одинаковыми (не рекомендуется). При этом исходный словарь будет перезаписан.

2.7.2.8 Индексация жесткого диска

Создание словаря путём индексирования жёсткого диска (с последующей атакой по этому словарю) - это довольно полезный и продвинутый инструмент расшифровки паролей локальных учётных записей Windows.

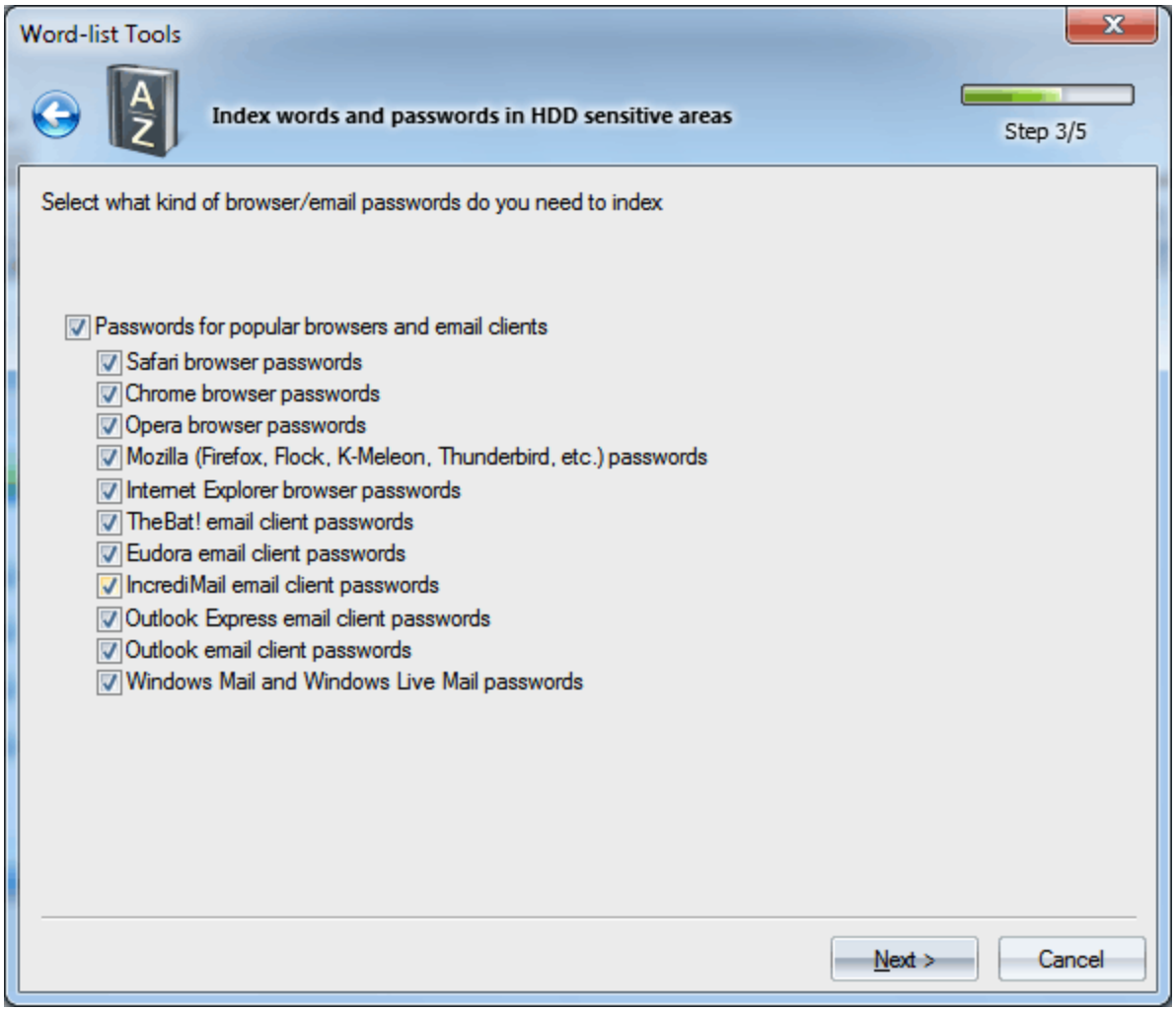
Часто пользователи, не отдавая себе отчёта, задают одинаковые пароли для учётной записи Windows, паролей Web, ICQ и т.д. Смысл данного инструмента состоит в создании словаря всех найденных и использованных ранее паролей, переписки пользователя, слов из последних открываемых файлов и т.д. Впоследствии, собранный словарь можно задействовать для поиска паролей локальных учётных записей. Эта технология используется в Интеллектуальной атаке.

Настройка инструмента условно состоит из четырёх частей:



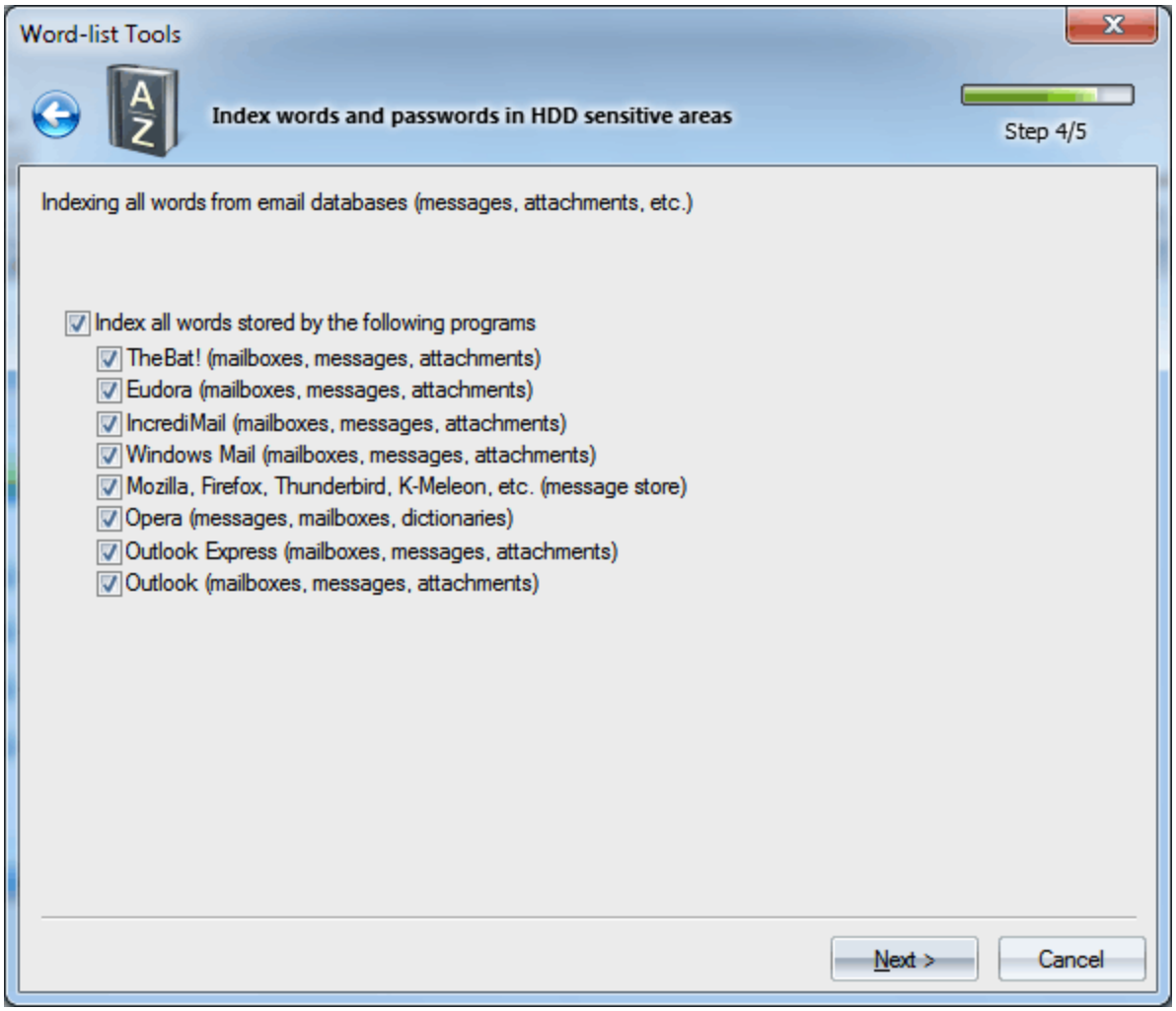
Copyright (c) 2024 Passcape Software. All rights reserved.

Вначале, необходимо выбрать список системных модулей, которые будут задействованы при создании словаря. Эти модули производят поиск и индексацию следующих видов паролей на жёстком диске вашего компьютера: текстовые пароли Active Directory, пароли автозагрузки и кэшированные пароли автозагрузки, SQL, IIS, Windows Media, текстовые пароли Win2K, пароли соединений RAS, Dialup, VPN, DSL, WEP, WPA, FTP, пароли Windows Credential Manager, пароли Instant Messanger'ов и др.



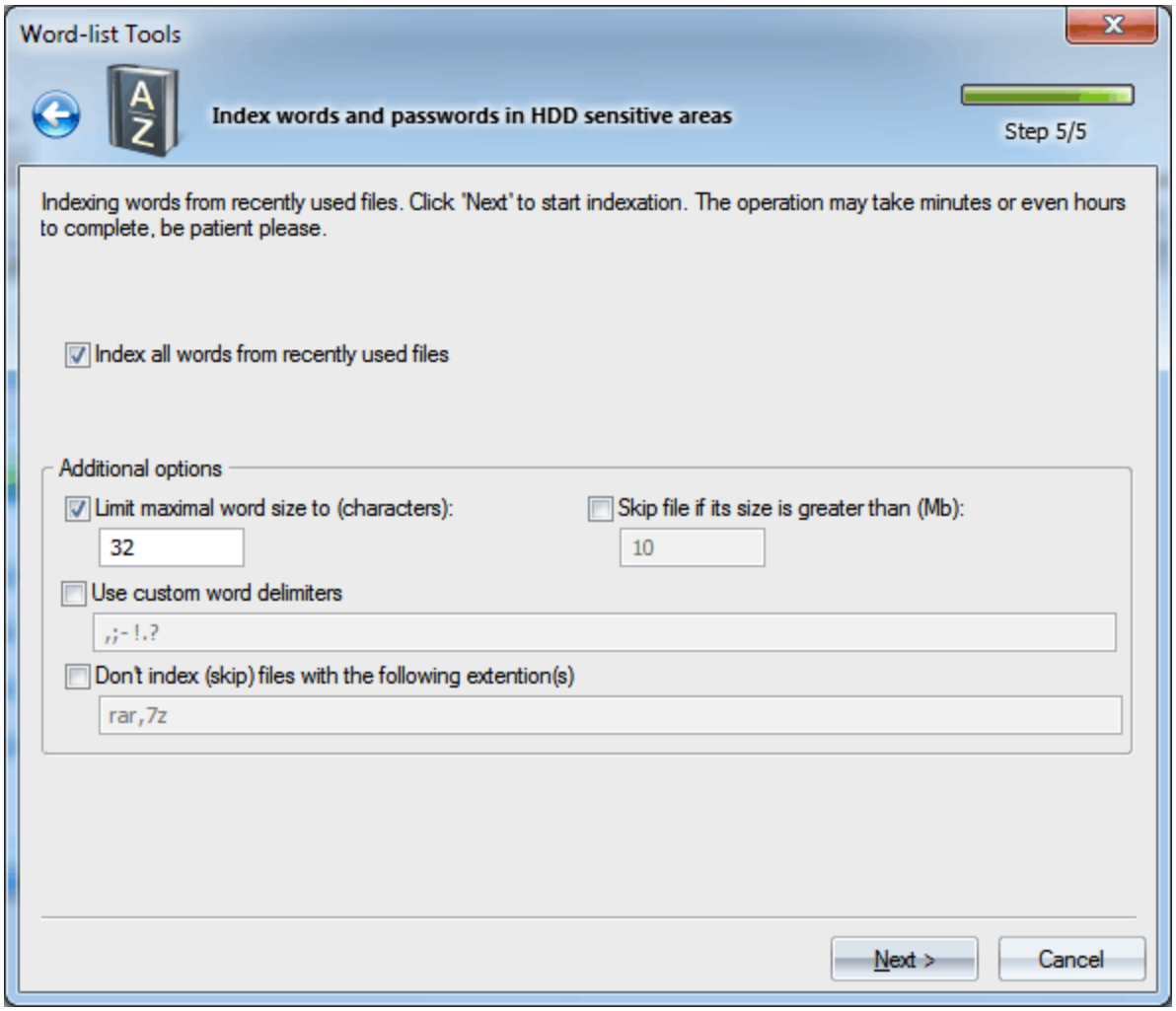
Во второй части настроек необходимо выбрать браузеры и почтовые клиенты, пароли которых также надо найти и добавить в создаваемый словарь. Программа поддерживает основные популярные обозреватели Интернет: Safari, Chrome, Opera, Mozilla браузеры (Firefox, K-Meleon, Flock и т.д.), Internet Explorer. Почтовые клиенты представлены следующими программами: TheBat!, Eudora, IncrediMail, Outlook Express, Outlook, Windows Mail, Windows Live Mail.

Copyright (c) 2024 Passcape Software. All rights reserved.



Кроме сбора паролей, программа может индексировать почтовую переписку пользователя, сканируя все найденные почтовые ящики, сообщения, вложения и т.д. Поиск по диску производится для всех учётных записей системы, так что этот процесс может занять значительное время, особенно, если в системе прописаны много пользователей или базы данных почтовых клиентов - большие. Так или иначе, можно включать/отключать каждый модуль отдельно.

Copyright (c) 2024 Passcape Software. All rights reserved.



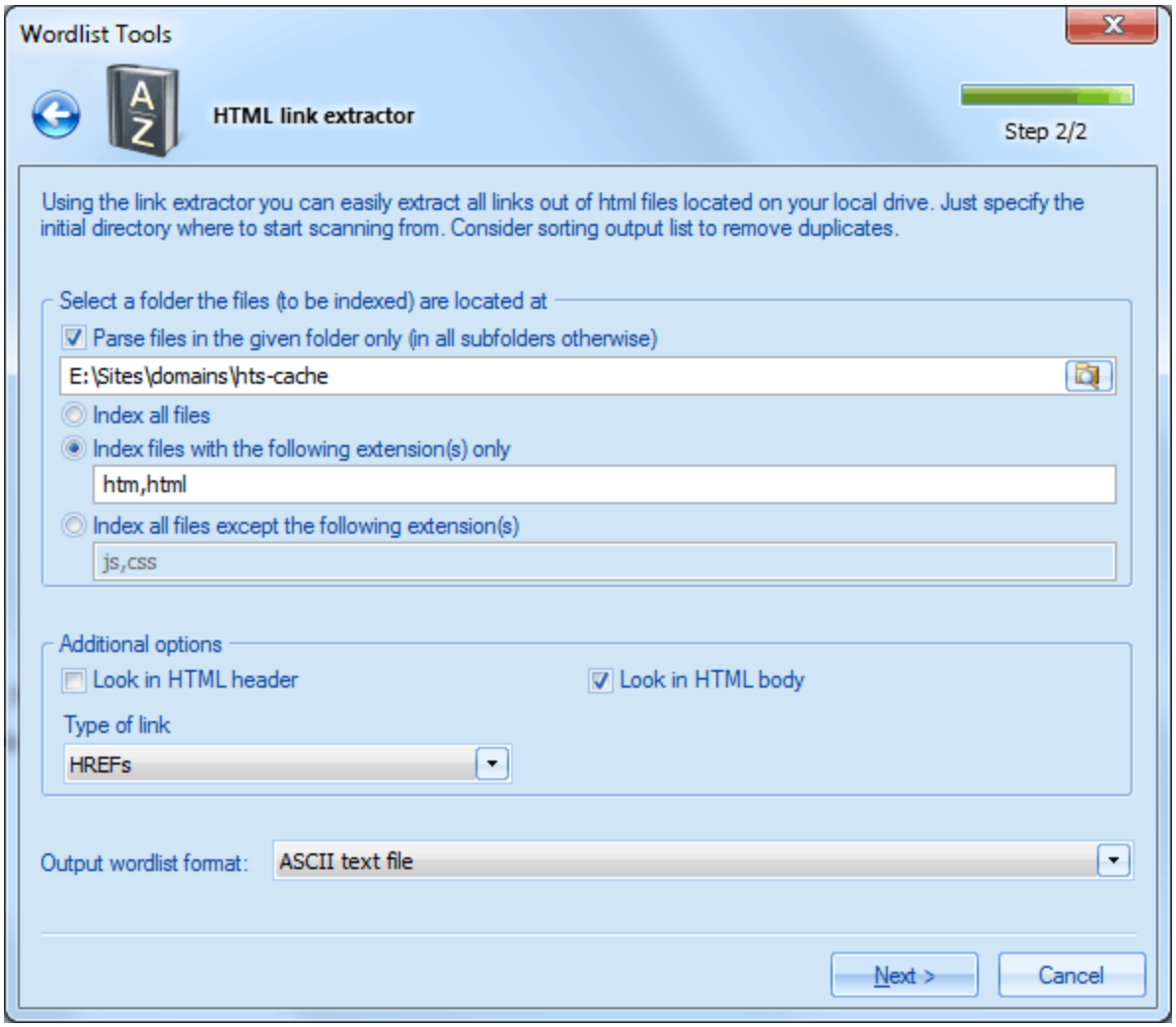
И, наконец, в последнем диалоге имеется возможность задать опции индексирования слов всех последних файлов, открываемых ранее текущим пользователем. Доступны следующие настройки:
- Задать лимит максимальной длины слов, помещаемых в словарь. Все слова, длина которых более заданного лимита, будут пропущены.
- Пропускать файлы, размер которых более заданного. Размер задаётся в Мб.
- Использовать свои разделители слов. По умолчанию, разделителями слов являются все не алфавитные буквы.
- Не индексировать файлы с заданными расширениями. Используйте эту опцию для пропуска ненужных на ваш взгляд файлов.

После нажатия кнопки **Next>**, начнётся индексация.
Имейте в виду, этот процесс может занять значительное время!

2.7.2.9 Поиск HTML ссылок

Эта утилита была разработана для вытаскивания ссылок из HTML файлов.

Copyright (c) 2024 Passcape Software. All rights reserved.



Настройка этого инструмента состоит из двух групп. В первой группе необходимо установить путь к исходному каталогу, в котором необходимо провести поиск, и задать способ обработки файлов. А именно:

- Обрабатывать файлы только в заданном каталоге. Если эта опция не установлена, то программа подвергнет рекурсивному анализу все вложенные подкаталоги и файлы в них.
- индексировать все файлы
- индексировать только файлы с заданными расширениями
- индексировать все файлы, кроме тех, расширения которых даны

По умолчанию, утилита производит поиск ссылок в *.htm и *.html файлах.

Группа с дополнительными настройками устанавливает тип ссылок для поиска и где их необходимо искать:

- Искать в заголовке HTML файлов.
- Искать в теле HTML файлов.
- Искать ссылки в тэге HREF, SRC или в обоих тэгах.

Нажатие кнопки **Next>** запускает процесс поиска, который может занять значительное время. После завершения операции и сохранения найденного списка ссылок на диск, необходимо отсортировать его, чтобы избавиться от дубликатов.

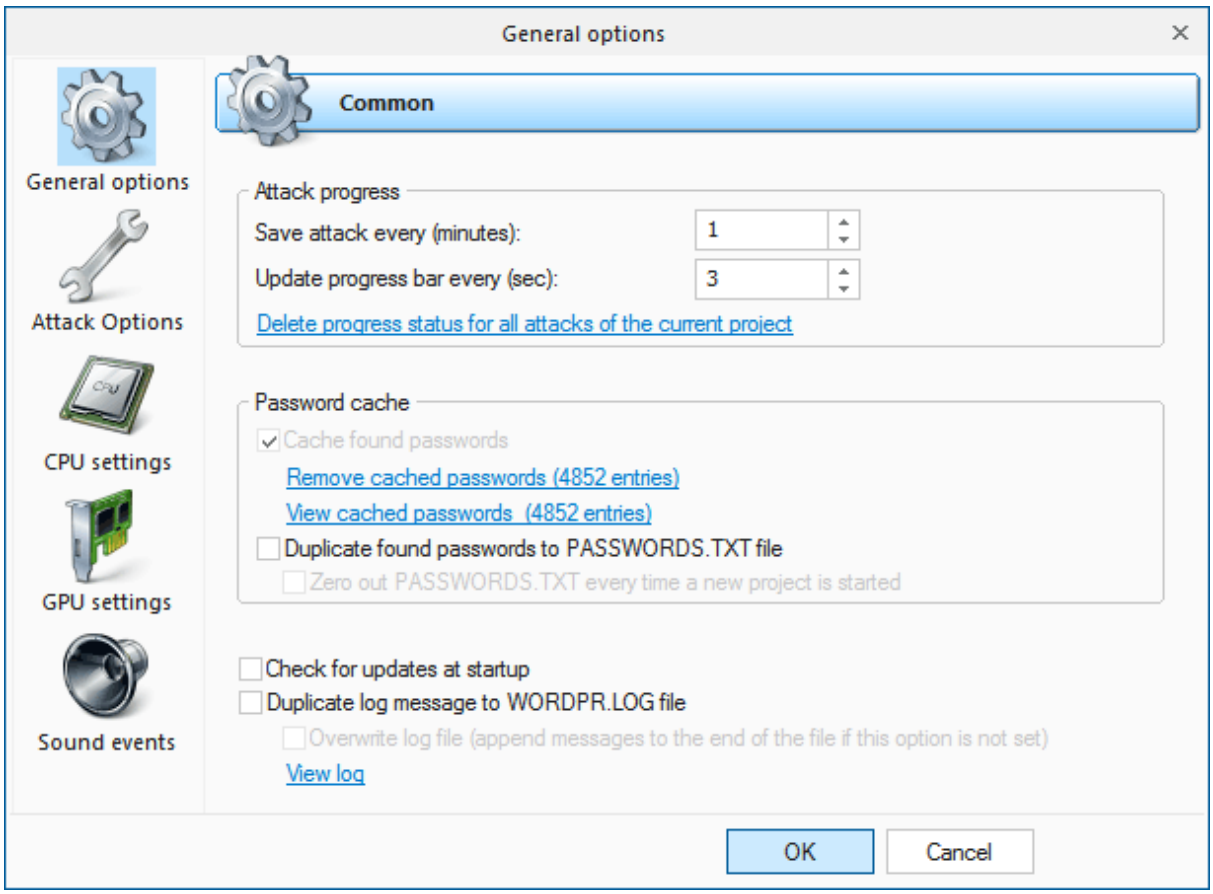
Copyright (c) 2024 Passcape Software. All rights reserved.

2.8 Меню Настройки

2.8.1 Общие

Общие настройки разделены на 5 частей.

2.8.1.1 Общие



Первая группа настроек позволяет задать интервалы сохранения и обновления текущего состояния атаки. По умолчанию, атака сохраняет своё состояние каждые 5 минут (в последствие, можно продолжить атаку с последнего сохранённого состояния) и обновляет экран каждые 3 секунды.

Кэш паролей
Все найденные программой пароли кэшируются по умолчанию. Очень полезная штука, которая задействована во многих подсистемах. Например, в интеллектуальной или предварительной атаке. Рекомендуется удалять кэш паролей только в крайних случаях. Например, когда их количество перевалило за десяток тысяч. В этом случае скорость работы в некоторых атаках значительно падает.
Дополнительно можно установить опцию дублирования найденных паролей в текстовый файл. В случае установки этой опции, например, при непредвиденном сбое в программе или внезапном отключении питания компьютера, все найденные пароли все равно будут сохранены.

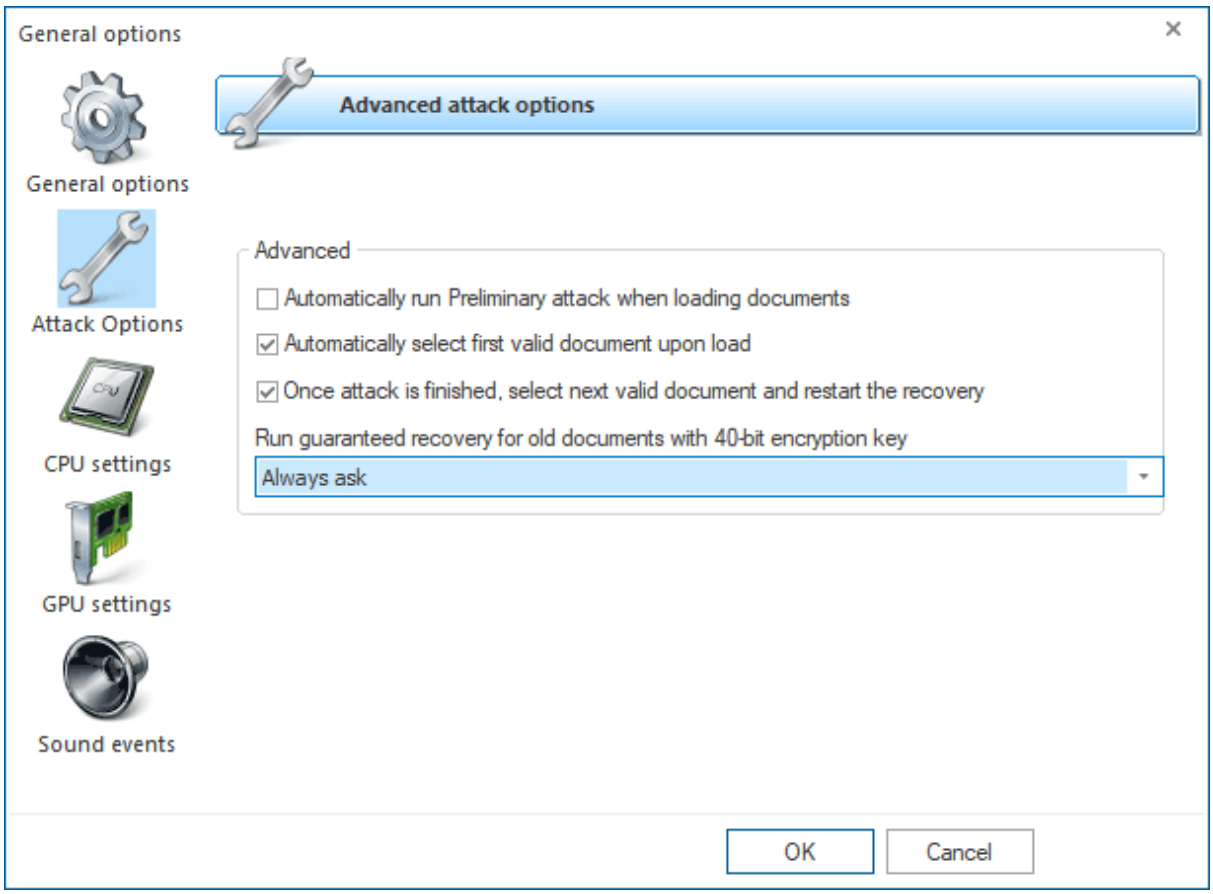
Copyright (c) 2024 Passcape Software. All rights reserved.

Check for updates at startup - проверять наличие обновлений при каждом запуске программы. Эта опция работает только если на компьютере есть активное интернет подключение.

Duplicate log messages to PPOINTPR.LOG file - если установлена эта опция, то все записи журнала событий будут продублированы в файл PPOINTPR.LOG. Опция полезна в том случае, если программа работает нестабильно или зависает. Файл PPOINTPR.LOG расположен в каталоге с программой.

Overwrite log file - перезаписывать PPOINTPR.LOG при каждом запуске программы. Если эта опция не задана, то все новые сообщения будут добавляться в конец файла.

2.8.1.2 Настройки атак



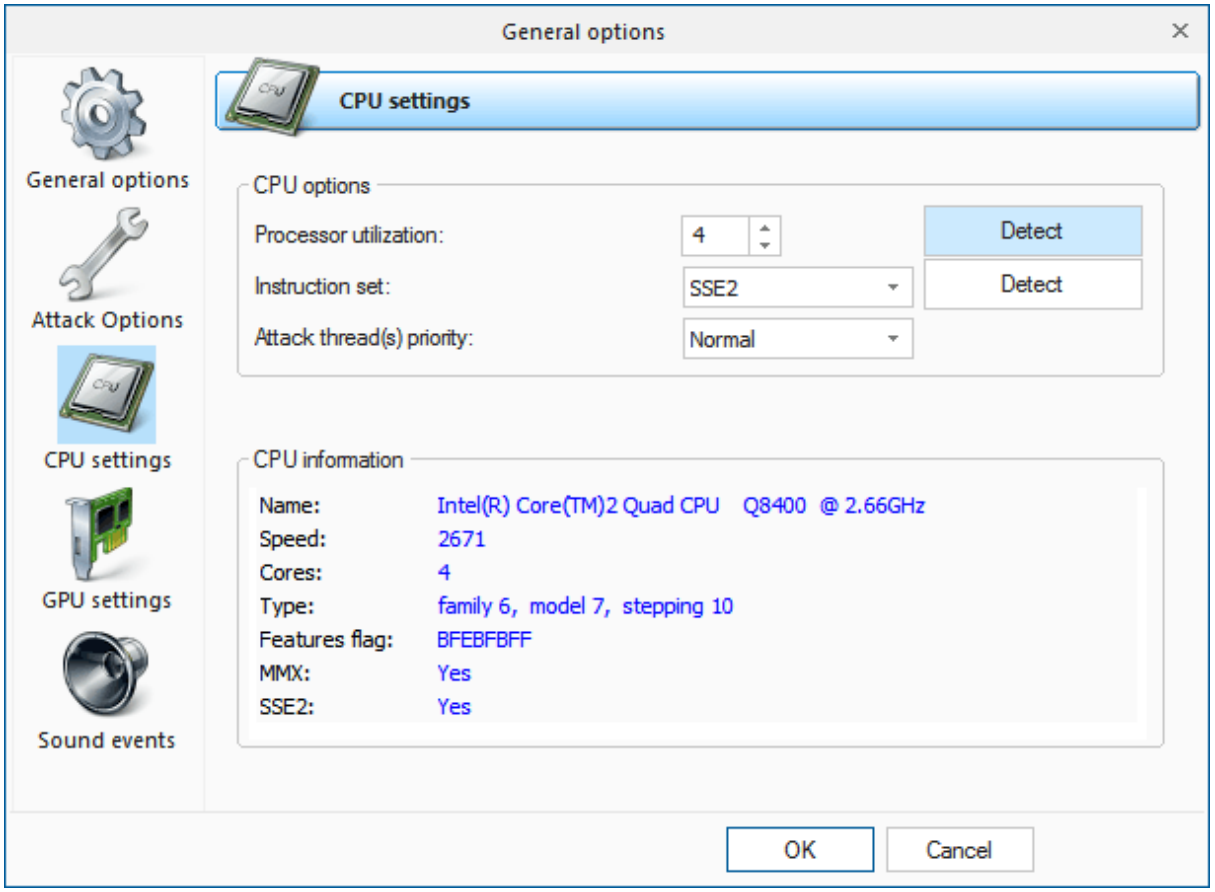
Дополнительно

- *Automatically run preliminary attack when loading documents*. Автоматический запуск Интеллектуальной атаки после каждой загрузки нового документа. Данная атака позволяет за считанные минуты выявить особо слабые пароли.
- *Automatically select first valid document upon import.* Автоматически выбирать первый нерасшифрованный документ для последующего анализа.
- *Once attack is finished, select next valid document and restart the recovery.* Если установлена эта опция, то после того, как атака закончена, не важно, успешно или нет, программа выберет следующую валидную запись в списке документов и автоматически запустит новую атаку.

Copyright (c) 2024 Passcape Software. All rights reserved.

- Run guaranteed recovery for old documents with 40-bit encryption key - что делать, если программа обнаружила документ с 40-битным ключом, который может быть гарантированно расшифрован:
  - всегда запускать гарантированное восстановление пароля. В этом случае программа найдёт коллизию пароля, т.е. пароль, который не будет отличаться от оригинального.
  - никогда не запускать гарантированное восстановление, а запускать обычную (выбранную) атаку
  - всегда спрашивать

2.8.1.3 Настройки процессора



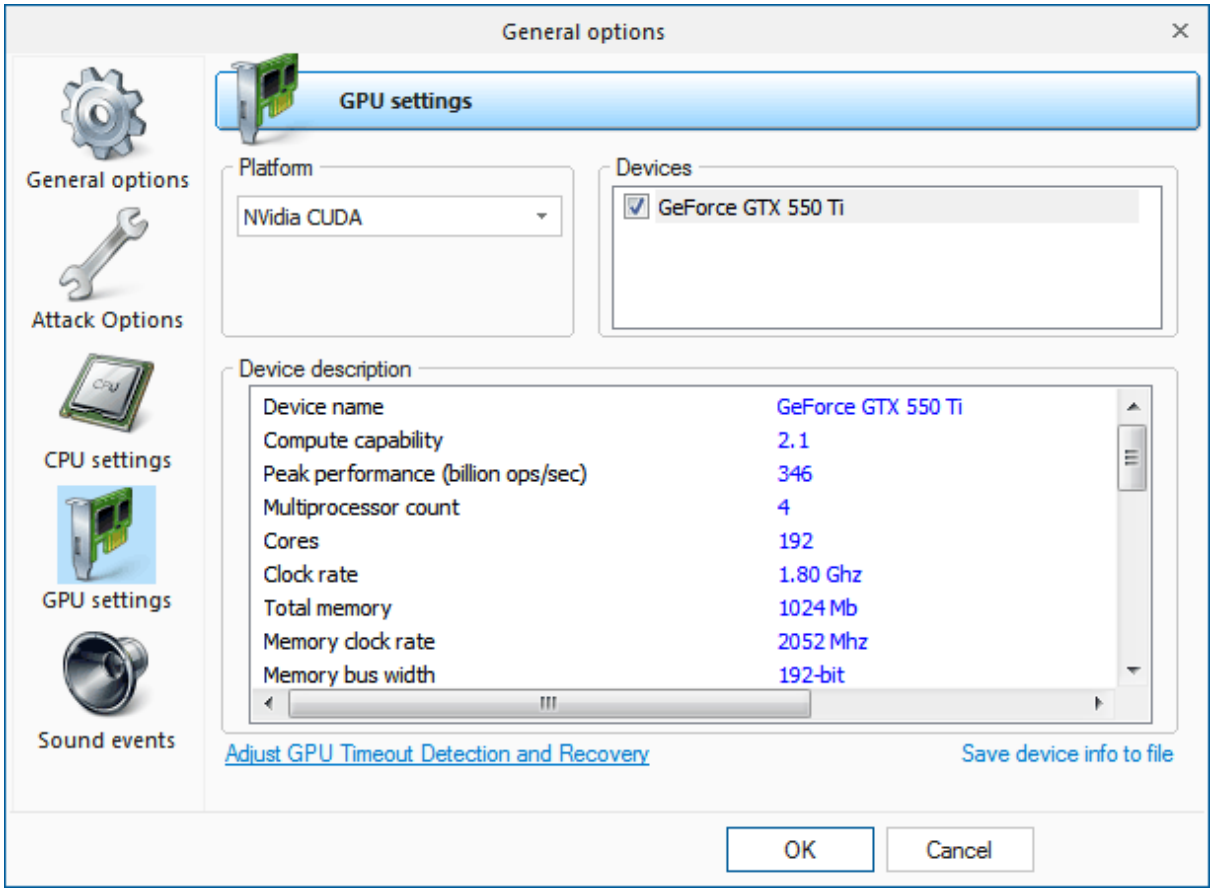
Поскольку большинство атак имеют поддержку многопоточности, то можно задавать количество одновременно выполняемых потоков перебора. В большинстве случаев, оно должно совпадать с количеством ядер процессора. Однако, если происходит поиск паролей с помощью видеокарты, то это значение должно быть уменьшено.

Алгоритмы перебора а программе "заточены" под три архитектуры процессора: X86, MMX и SSE2. Естественно, на процессорах, поддерживающих новую архитектуру, перебор осуществляется быстрее.

Приоритет атаки не рекомендуется задавать выше нормальной, в противном случае можно будет наблюдать значительное снижение производительности всей системы в целом.

Copyright (c) 2024 Passcape Software. All rights reserved.

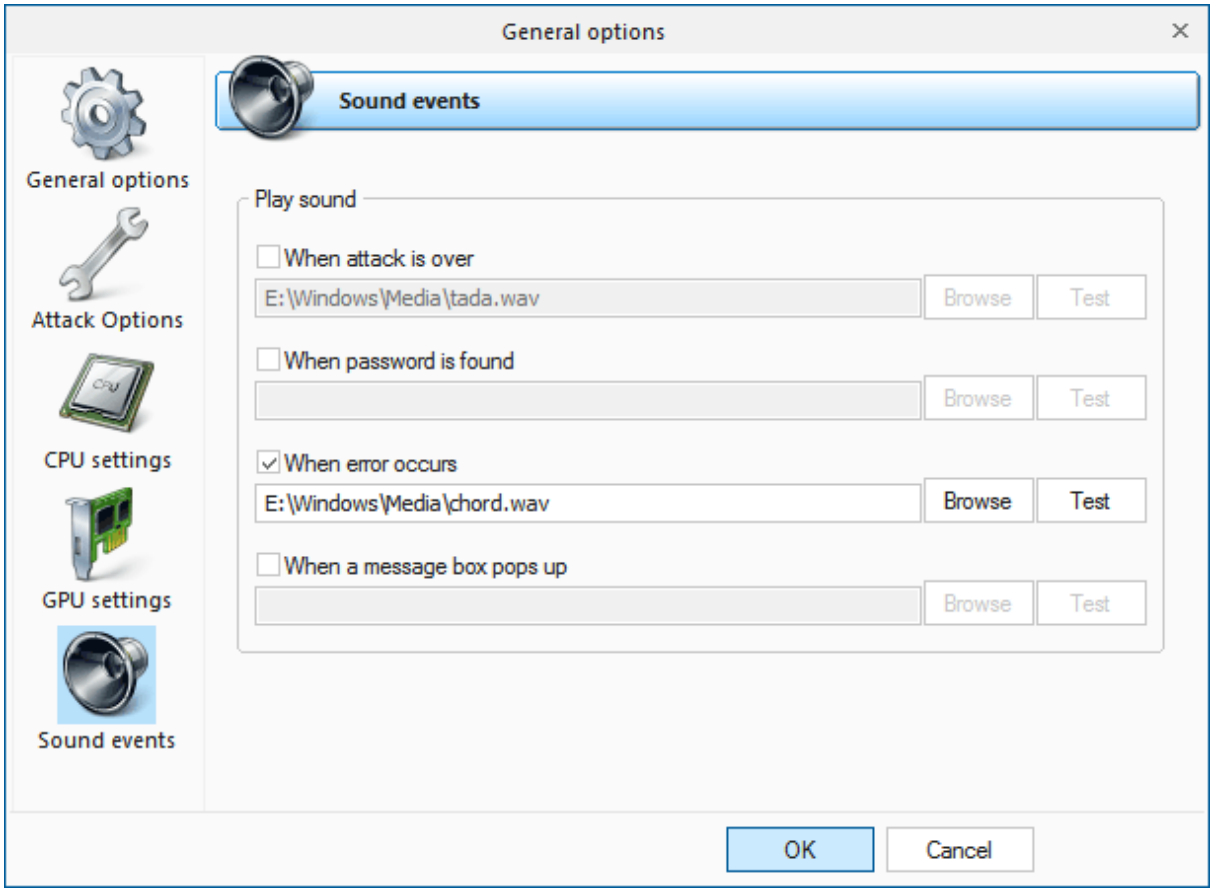
2.8.1.4 Настройки видеокарт



Перед запуском атаки на GPU, необходимо выбрать её в общих настройках программы. Для этого просто поставьте галочку напротив имени видео карты. Все основные характеристики устройства отображены в нижней таблице. Программа поддерживает работу до 255 устройств.

Copyright (c) 2024 Passcape Software. All rights reserved.

2.8.1.5 Звуковые События



В программе имеется возможность задавать звуковые оповещения для определённых событий. Например, по окончании атаки или когда будет найден пароль.

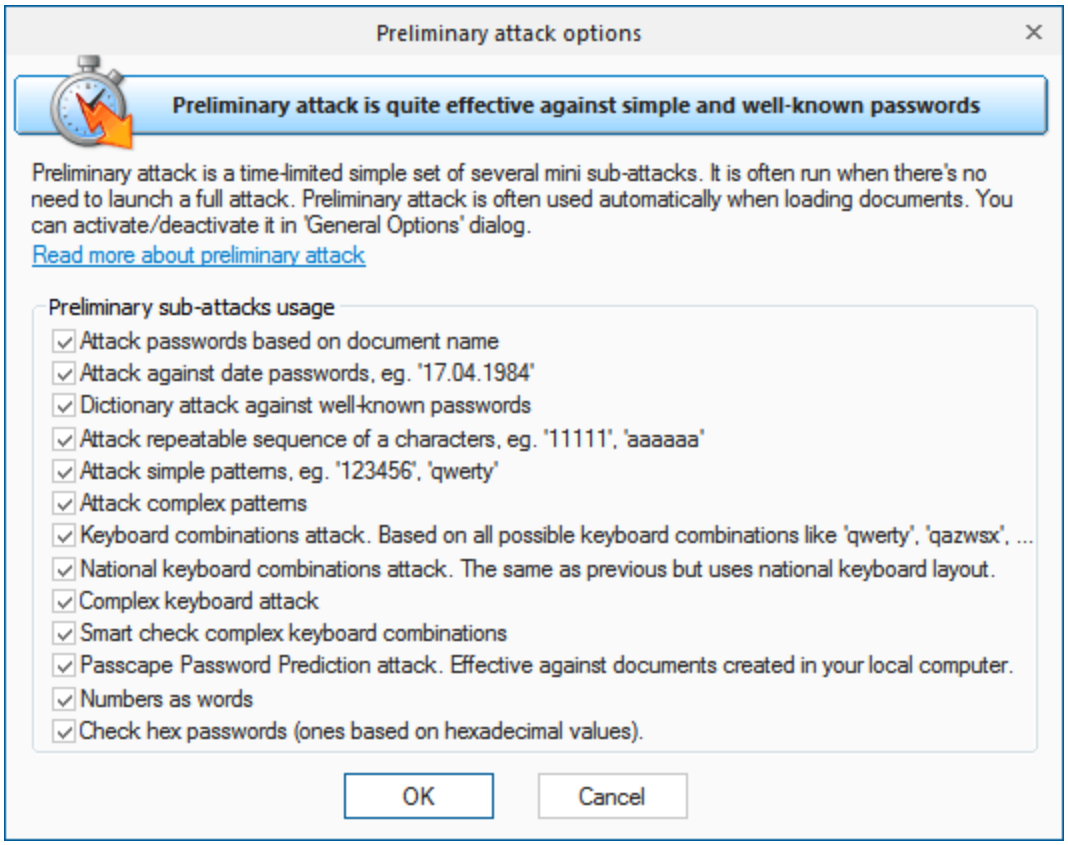
2.8.2 Настройки Атак

2.8.2.1 Предварительная Атака

Предварительная атака (разработана в Passcape Software) довольно эффективна против коротких, простых, словарных, повторяющихся, клавиатурных и т.п. паролей, когда нет необходимости запускать полную атаку. Предварительная атака состоит из нескольких мини атак, каждую из которых можно включать\выключать отдельно.

Как правило, предварительная атака выполняется около 20-30 минут или даже быстрее, в зависимости от типа документа, используемого для восстановления железа и настроек атаки.

Copyright (c) 2024 Passcape Software. All rights reserved.



Мини-модули предварительной атаки:

- Атака на имя документа. Проверка паролей, основанных на имени документа.
- Атака на пароли, которые были созданы на основе дат. Например, 12031992.
- Простая атака по словарю. Быстрая проверка пароля по всем словам внутреннего словаря программы.
- Атака на повторяющиеся последовательности. Проверка паролей, состоящих из повторяющихся символов. Например, '1111111' или 'xxxxxxxxxx'.
- Атака на простые образцы, например, '1234567890' или 'йцукен'.
- Проверка сложных комбинаций, состоящих из нескольких частей.
- Клавиатурная атака проверяет всевозможные пароли, привязанные к раскладке клавиатуры: 'qwerty', 'qazwsx', 'asdzxc' и т.д.
- Аналогично предыдущей, но для интернациональных паролей.
- Сложная клавиатурная атака аналогична предыдущим двум, но для более сложных, составных паролей клавиатуры.
- Улучшенная атака на сложные клавиатурные пароли.
- Предугадывание паролей - наиболее действенный механизм с элементами искусственного интеллекта для угадывания паролей. Известный также как Passcape Password Prediction.
- Атака на цифровые пароли в виде слов.
- Короткие шестнадцатеричные пароли.

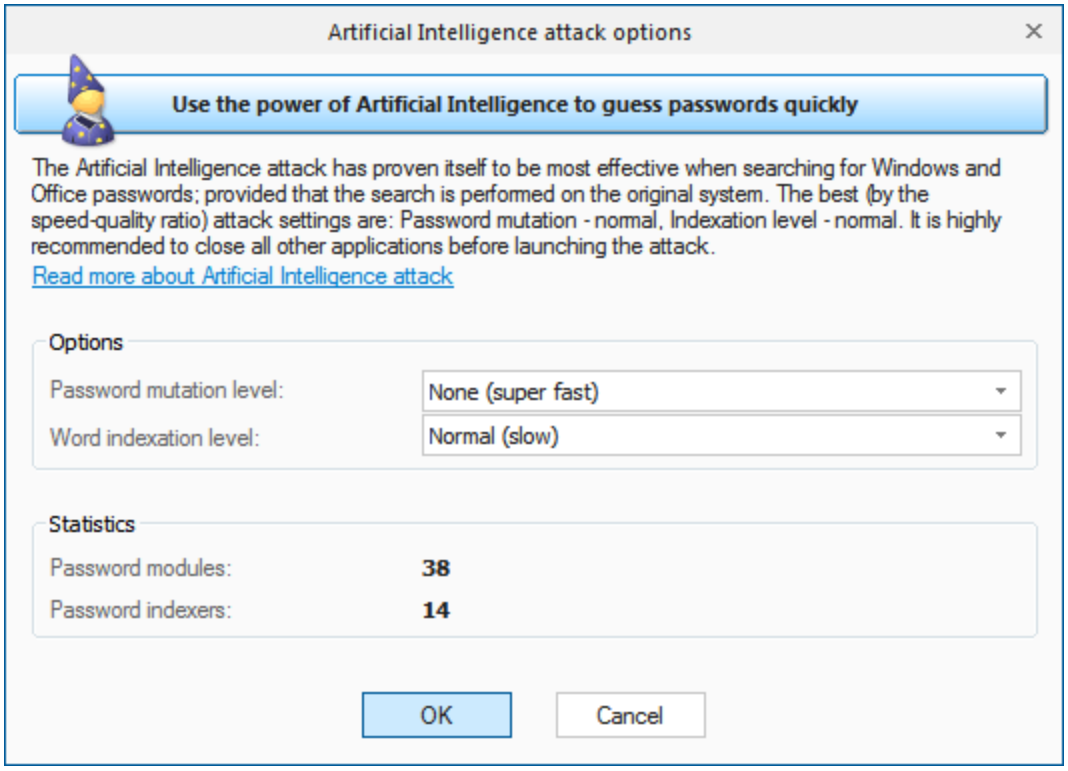
2.8.2.2 Интеллектуальная Атака

Интеллектуальная атака (AI attack или Artificial Intelligence attack) это новый тип атаки, разработанный нашей компанией, основанный на методе социальной инженерии и не применявшийся ранее в программах для восстановления паролей.

Copyright (c) 2024 Passcape Software. All rights reserved.

Интеллектуальная атака в основном используется при проверке паролей, которые были созданы на локальном компьютере. Атака сканирует локальный компьютер, индексирует и создаёт список найденных слов и паролей, анализирует их, на основе анализа создаёт предпочтения пользователя, производит мутацию найденных слов и после этого выполняет подбор паролей.

С помощью данной атаки можно, не прибегая к долгим и затратным вычислениям, практически мгновенно восстанавливать некоторые сложные пароли. Основная идея интеллектуальной атаки состоит в том, что обычный пользователь в качестве своих паролей очень часто выбирает похожие слова и словосочетания или руководствуются одним и тем же правилом создания паролей. Зная это, можно попытаться вычислить это правило и подобрать начальный пароль.



Звучит довольно абстрактно, но на практике атака чётко разбивает свою работу на четыре последовательных шага:

Шаг 1 Начало сбора приватной информации. В действие вступает модуль сбора и индексации паролей, который ищет все доступные и спрятанные в системе пароли, введённые когда-либо пользователем. Сюда входят пароли сети, ICQ, электронной почты, FTP, пароли учётных записей Windows, пароли сервера, LSA Secret и т.д.

Шаг 2 запускает модуль сбора и индексации данных. Во время этого шага анализируется активность пользователя (или всех пользователей, если выбран режим индексации, отличный от Light) в системе. После чего, на её основе происходит создание списка слов - потенциальных паролей, выбранных из текстовых файлов, архивов, истории обозревателей интернет, почтовой переписки и др.

Шаг 3 включает в себя модуль семантического разбора базы найденных паролей и списка потенциальных паролей.

Шаг 4 На заключительном этапе модуль анализа данных производит мутацию слов и подбора паролей.

Copyright (c) 2024 Passcape Software. All rights reserved.

В начале работы атаки программа производит поиск всех известных ей паролей в системе. Для этого существуют 38 мини-модулей для расшифровки паролей системы, почты, браузеров, мессенджеров, архивов и т.д. Затем идёт индексация файлов и данных в ходе которой производится создание потенциального словаря атаки. Третий модуль разбирает найденные пароли и слова по кирпичикам из которых в последнем модуле будут складываться новые сочетания для подбора и угадывания исходного пароля.

Естественно, чем сложнее уровень мутации и индексации, тем эффективнее поиск. Однако наивысший уровень индексации и анализа может занять часы и даже дни в зависимости от скорости алгоритма проверки пароля и количества пользователей в системе.

Наиболее эффективно интеллектуальная атака зарекомендовала себя при условии, что поиск ведется на исходной системе. Доступны всего две опции: глубина мутации паролей и уровень индексации слов. Наиболее предпочтительные варианты для проведения скоростной атаки - Light:Light. Для более глубокого, но и более медленного поиска, следует выставить данные опции в Normal или даже Deep.

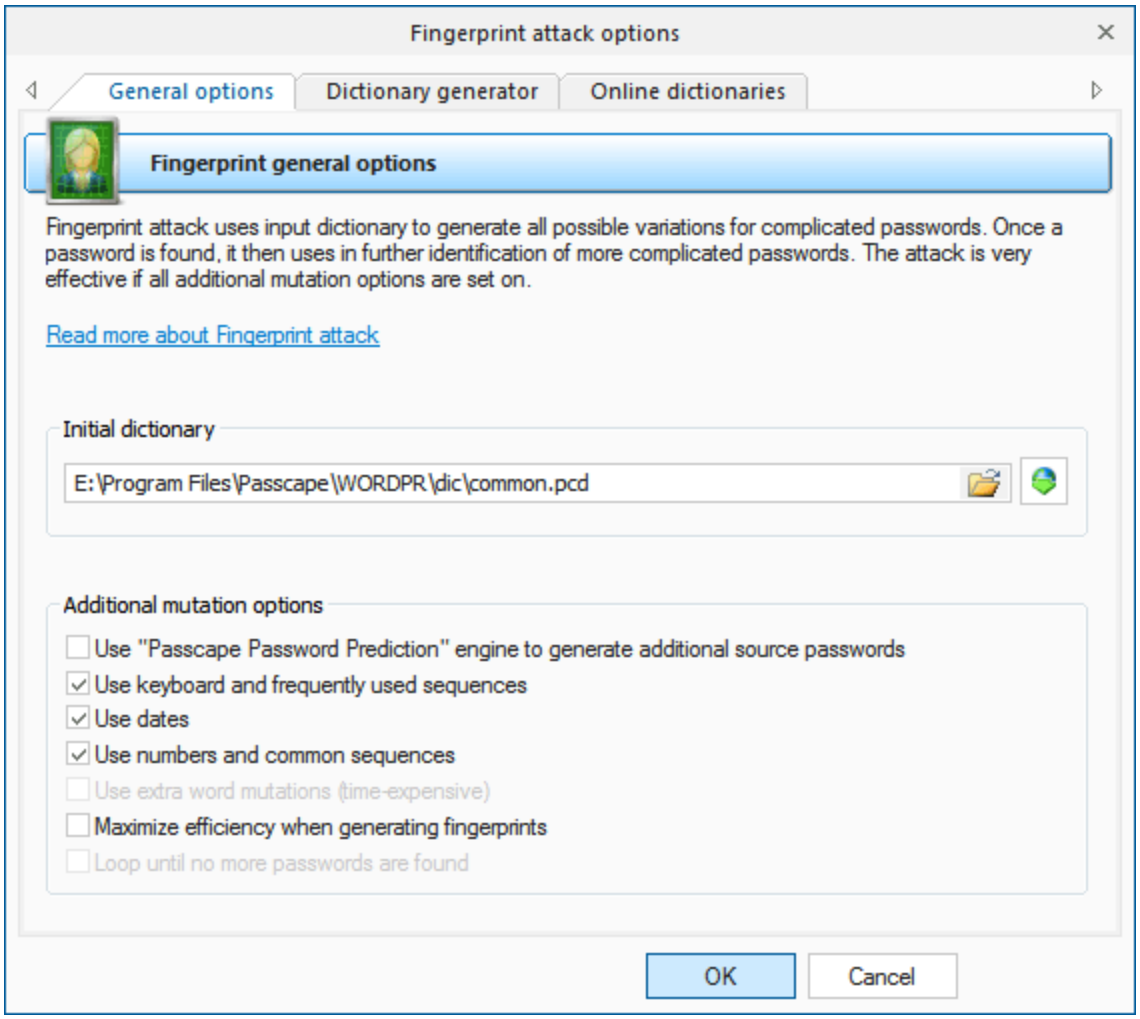
Перед запуском интеллектуальной атаки рекомендуется закрыть все программы.

2.8.2.3 Идентификационная Атака

Идентификационная атака (fingerprint attack) - сравнительно свежий инструмент для восстановления сложных паролей, не поддающихся расшифровке в других атаках. Суть её состоит в том, чтобы для поиска паролей брать не отдельные слова исходного словаря, как в атаке по словарю, и даже не комбинации слов, как в комбинированной атаке, а так называемые "отпечатки". При этом каждое исходное слово словаря используется для создания нескольких отпечатков.

Перед запуском атаки необходимо задать исходный словарь, который будет использоваться для создания банка отпечатков. С программой поставляется словарь common.pcd, оптимизированный для данной атаки, но можно использовать свой или скачать из интернета (вкладка Online dictionaries). Особых требований к словарю нет, кроме одного: исходный словарь не должен быть слишком большим, иначе атака займёт значительное время.В качестве словаря можно (и даже желательно!) использовать уже готовые списки паролей.

Copyright (c) 2024 Passcape Software. All rights reserved.



Отпечатки генерируются так: каждое слово исходного словаря сначала разбивается на однобуквенные пароли, затем на 2-х буквенные и т.д. Например, исходное слово **crazy** разбиваем на односимвольные отпечатки. Получаем:
c
r
a
z
y
Затем на двух символьные:
cr
ra
az
zy
Потом трех:
cra
raz
azy
И, наконец, четырех символьные:
craz
razy

Copyright (c) 2024 Passcape Software. All rights reserved.

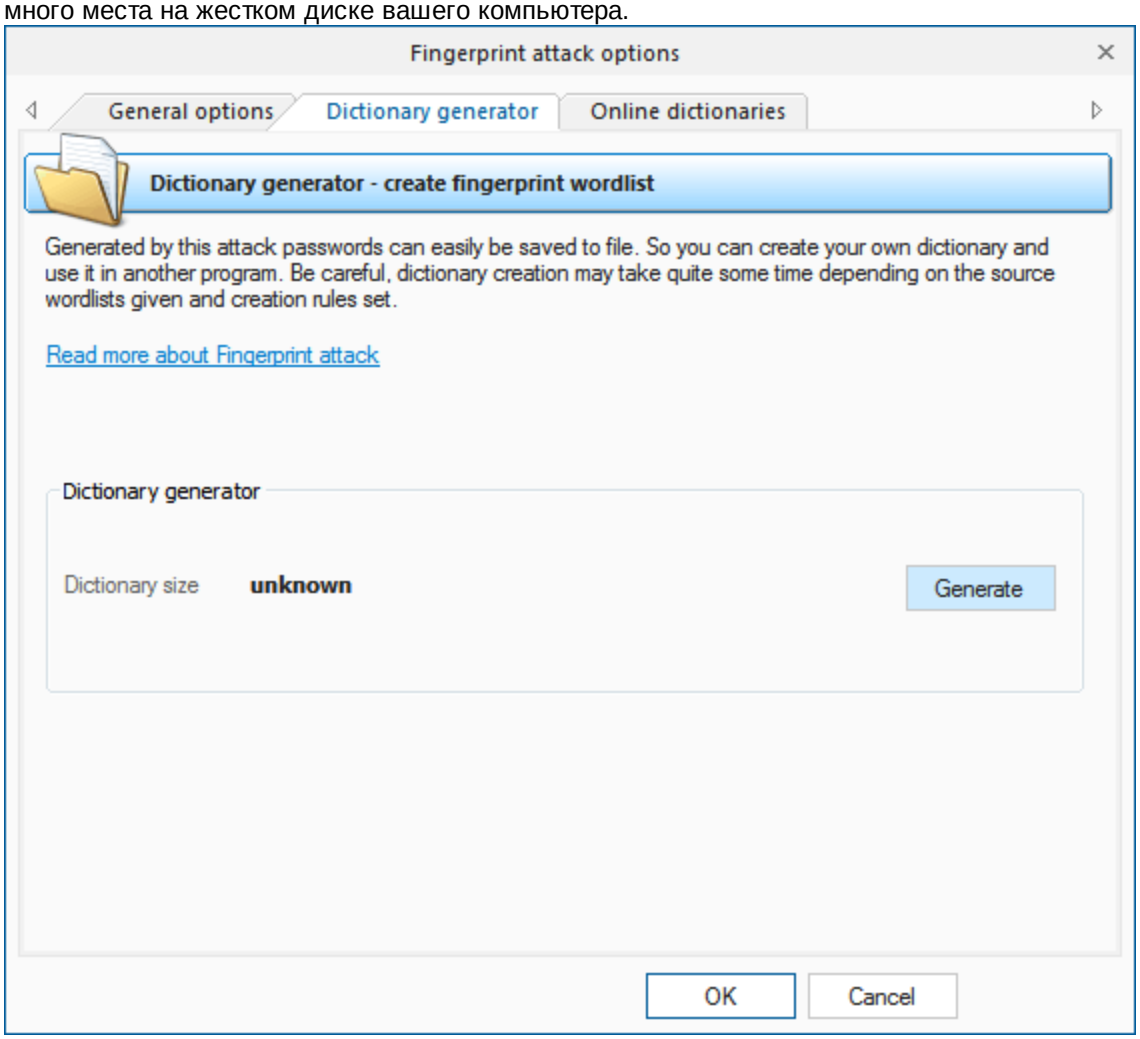
Получилось 5+4+3+2=14 отпечатков, не считая исходного слова.
И так для каждого слова исходного словаря. После этого, все отпечатки сливаются в общую базу, естественно, отбрасывая дубликаты. Получаем базу отпечатков, которые будут использоваться для проверки паролей путём склейки всех отпечатков друг с другом.

На самом деле, алгоритм генерации отпечатков немного сложнее. Более того, в настройках атаки имеется дополнительная опция **Maximize effeciency when generating fingerprints**, предназначенная для задействования более сложного алгоритма, который позволяет максимизировать эффективность (в ущерб скорости) путём создания дополнительных отпечатков.

Разберём оставшиеся опции.

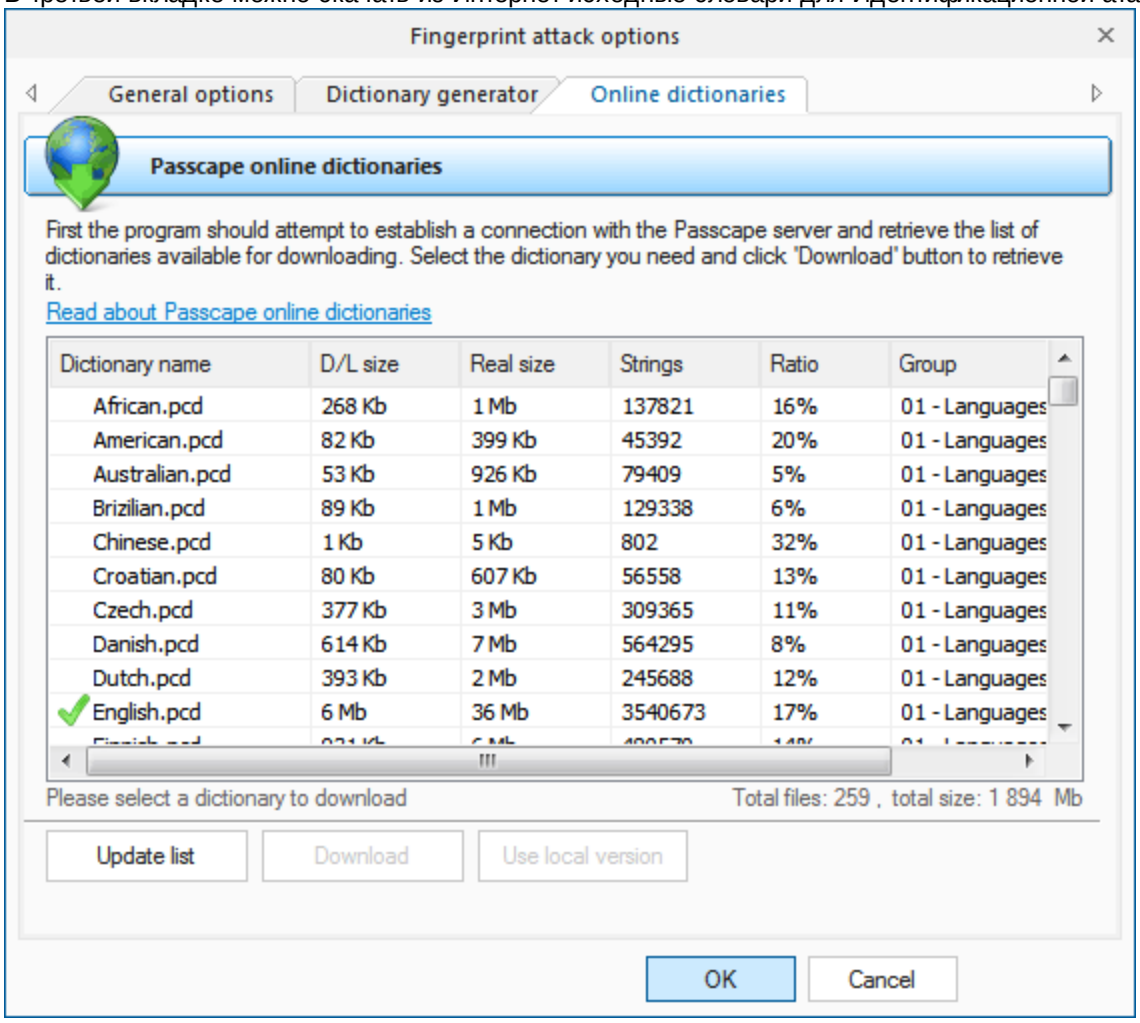
- **Use PPP engine to generate additional passwords** - задействовать при создании отпечатков пароли, которые были найдены в других атаках
- **Use keyboard and frequently use sequences** - добавить в банк отпечатков клавиатурные комбинации и часто повторяющиеся последовательности
- **Use dates** - использовать даты
- **Use numbers and common sequences** - использовать цифры и простые комбинации букв.

Вторая вкладка с настройками позволяет создать и записать свой собственный словарь на основе выставленных опций Идентификационной атаки. Будьте аккуратны, этот словарь может занять много места на жестком диске вашего компьютера.



Copyright (c) 2024 Passcape Software. All rights reserved.

В третьей вкладке можно скачать из Интернет исходные словари для Идентификационной атаки.

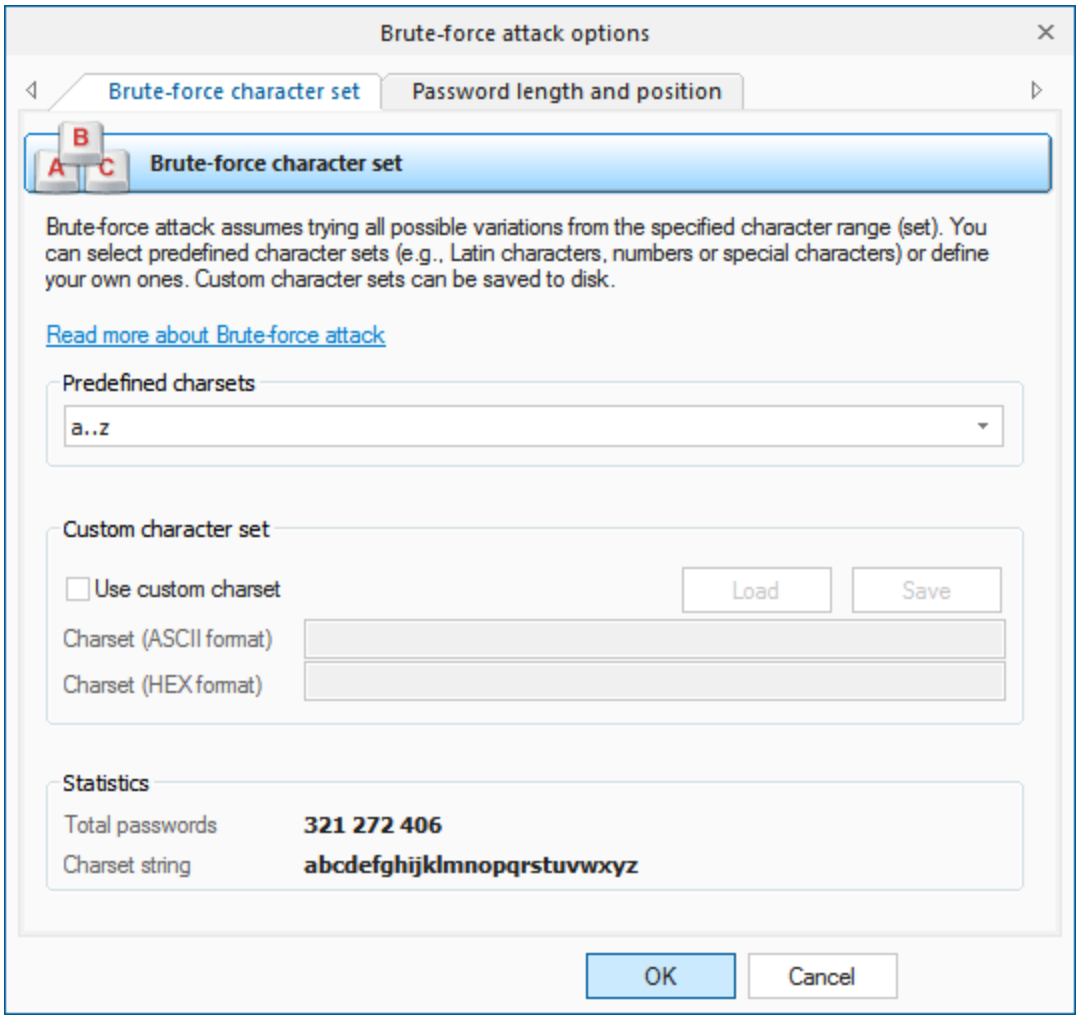


2.8.2.4 Атака в Лоб (полным перебором)

Полный перебор (или метод 'грубой силы' от англ. brute force) - метод решения задачи путём перебора всех возможных вариантов. Сложность полного перебора зависит от размерности пространства всех возможных решений задачи. В криптографии на сложности полного перебора основывается оценка криптостойкости шифров. В частности, шифр считается криптостойким, если не существует метода взлома, существенно более быстрого, чем полный перебор всех ключей.
Это определение атаки грубой силы взято с сайта Википедии.

Выражаясь более простым языком, атака перебором - это угадывание пароля путём перебора всех возможных вариантов на основе длины пароля и заданного набора символов. Атака перебором - самая медленная. К примеру, если вы задали набор из малых Латинских символов (abcdefghijklmnopqrstuvwxyz) для вашей атаки, то потребуется перебрать 208 827 064 576 вариантов для одного 8-символьного пароля. Эта атака обычно используется только тогда, когда все остальные не увенчались успехом.

Copyright (c) 2024 Passcape Software. All rights reserved.



Настройки атаки перебором состоят из двух частей.

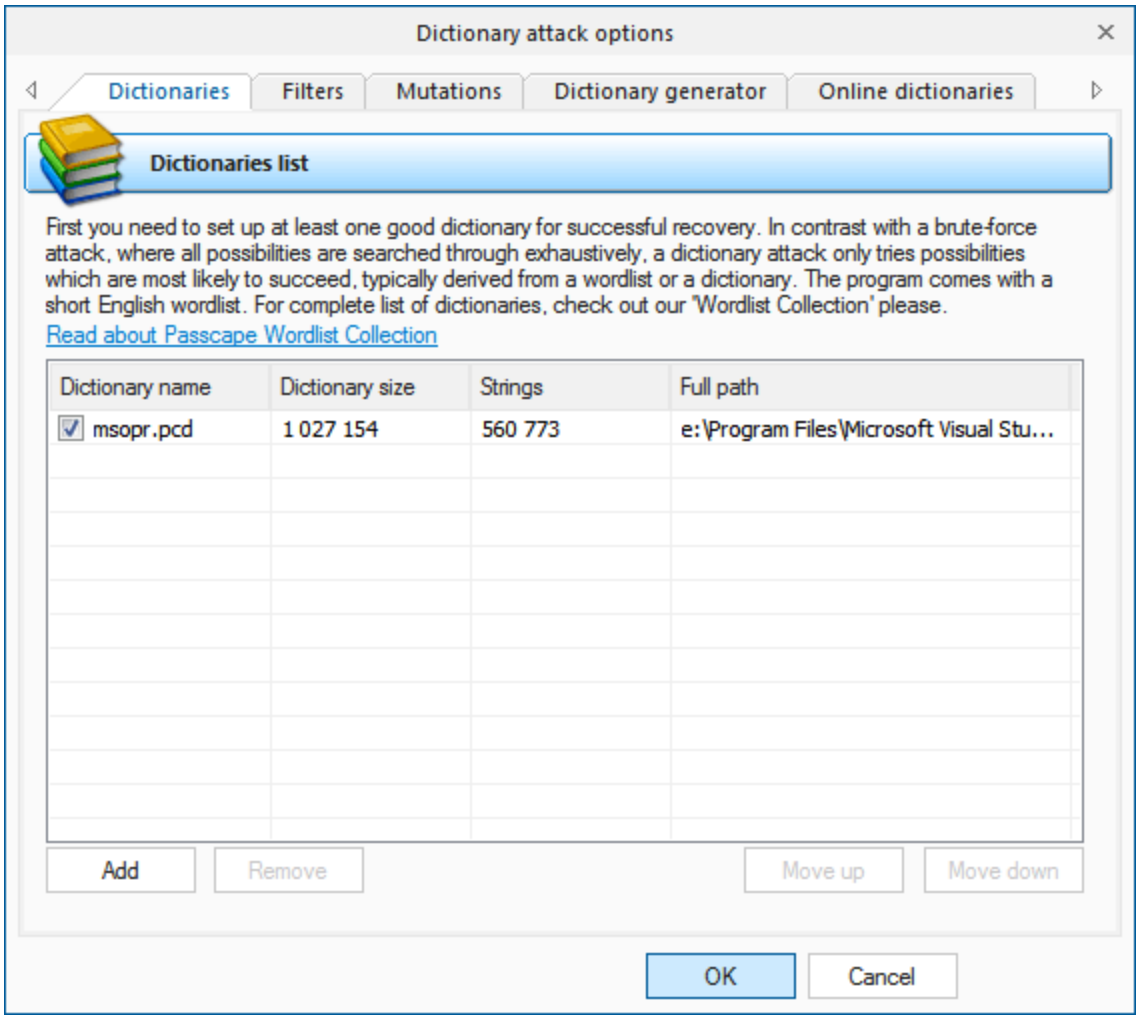
Первая вкладка предназначена для задания диапазона перебираемых символов. Можно выбрать уже готовые заготовки или задать свои собственные. Чтобы задать свой диапазон символов, следует выставить опцию 'Пользовательский набор'. После этого, для формирования своего набора, станут доступны два поля ввода: первое - для ввода ASCII, второе - для ввода непечатных символов. Свой набор можно сохранить на диске.

Во второй вкладке необходимо задать минимальную и максимальную длину перебираемых паролей. Можно также задать и стартовый пароль, с которого начнётся перебор.

2.8.2.5 Атака по Словарю

В отличие от атаки полным перебором, проверяются не все возможные варианты, а лишь уже отобранные до этого и загружаемые из списка слов, или словаря. Этот метод оказывается достаточно эффективным потому, что многие люди выбирают в качестве пароля одиночные слова или их простые вариации.

Copyright (c) 2024 Passcape Software. All rights reserved.



Во вкладке **Словари** задаётся список словарей для атаки. Поддерживаются текстовые словари в формате ASCII, UNICODE, UTF8, RAR, ZIP, а также зашифрованные\упакованные словари в родном формате PCD, разработанным в Passcape Software. Для деактивации словаря достаточно сбросить галочку напротив его имени. В этом случае, он хоть и будет присутствовать в списке, но будет пропущен во время атаки. Вместе с программой поставляется внутренний словарь на несколько десятков тысяч слов. Полный список словарей можно заказать для доставки на CD, либо, как альтернативный вариант, использовать online словари.

Вкладка **Фильтры** фильтрует, т.е. отсекает нежелательные пароли из словаря, по принципу включения или исключения. Если будет задан первый, включающий фильтр, то атака будет принимать только те слова, которые содержат по крайней мере один из символов заданного фильтра. Если будет задан второй, исключающий фильтр, то программа будет пропускать те слова, которые содержат по крайней мере один из введённых символов.

Вкладка **Мутация** предназначена для задания возможных комбинаций перебираемых слов. Например, если задана сильная мутация, то для каждого слова из словаря будет создано несколько сотен аналогов. Например, secret - Secret - s3cr3t - secret123 и т.д. Всего можно задавать три правила для мутации: 'слабо' - меньше мутаций и, соответственно, выше скорость перебора; 'сильно' - для большого количества мутаций в ущерб скорости и промежуточный вариант, используемый по умолчанию.

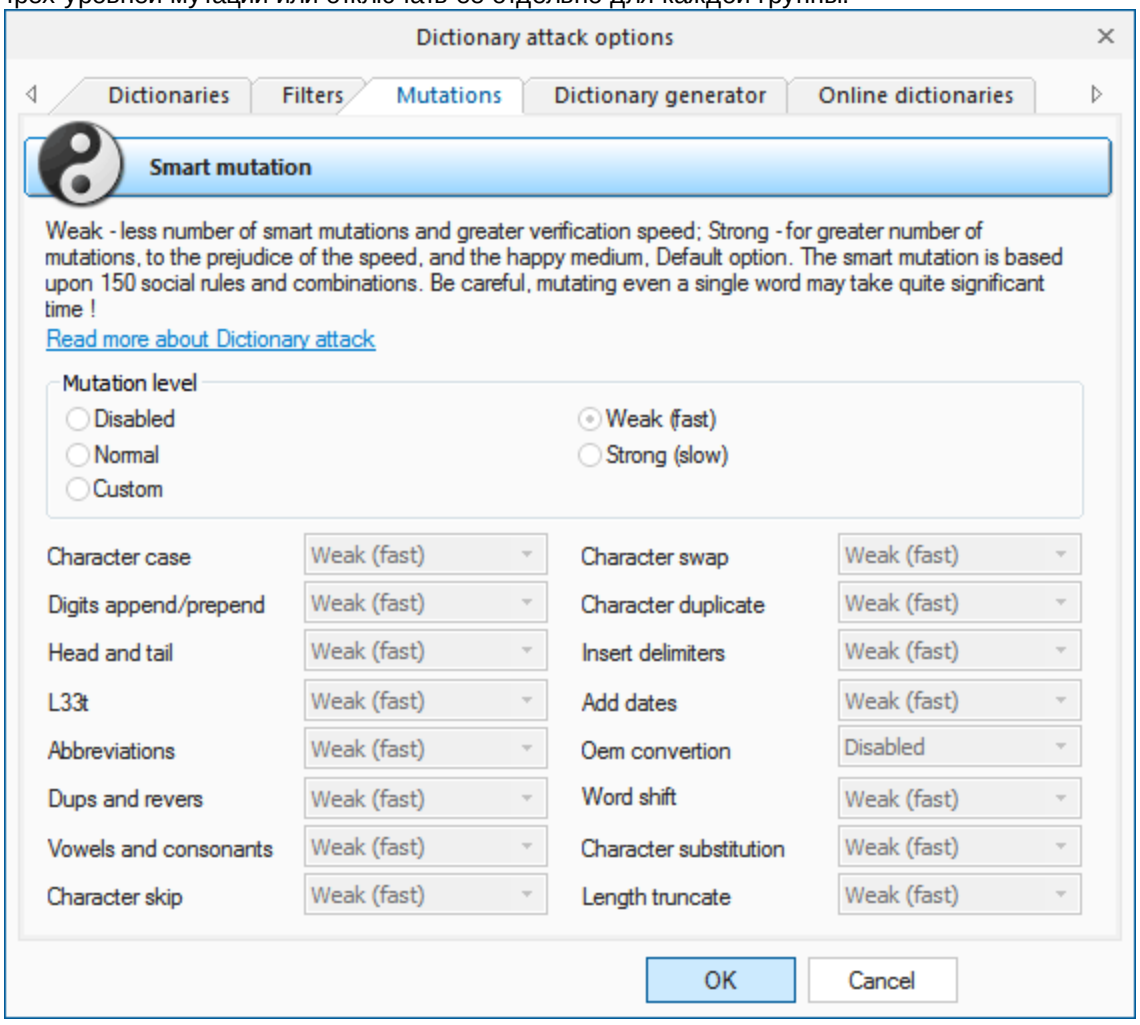
Copyright (c) 2024 Passcape Software. All rights reserved.

В **Генераторе словарей** можно создавать свои собственные варианты словарей на базе опций первых трёх вкладок.

Онлайн словари. В программе имеется замечательная возможность скачать и использовать уже готовые имеющиеся словари с сайта Passcape. Мы собрали достаточно большую коллекцию словарей - более 250. Это должно избавить вас от дополнительных хлопот по поводу поиска соответствующего контента в сети.

Ручная настройка мутации

В программе существует возможность более тонко задавать настройку мутаций в атаке по словарю. Все правила мутации объединены в 16 основных групп. Вы можете задавать один из трёх уровней мутации или отключать её отдельно для каждой группы.



Ниже дано краткое описание групп мутаций:

Имя группы	Описание	Примеры (для слова '**password**')	Комментарии
Character case	Проверяет регистр букв в исходном слове.	Password, PassworD, PaSsWoRd	Максимальный (Strong) уровень мутаций НЕ создаёт всех возможных вариантов регистра букв. Для этой цели можно

Copyright (c) 2024 Passcape Software. All rights reserved.

Имя группы	Описание	Примеры (для слова '**password**')	Комментарии
			использовать Гибридную атаку по словаю (см. правило **aN**).
Digits append/prepend	Добавляет цифры в конец или начало слова.	password99, 2Password, PASSWORD3	Максимальный уровень добавляет две цифры.
Head and tail	Почти тоже самое, что и предыдущая группа, за исключением того, что добавляются не цифры, а слова, аббревиатуры, символы, клавиатурные комбинации и т.д.	#Password#, password12345, 4everPASSWORD, Passwordqwerty	
l33t	Создание различных вариантов слова на основе синтаксиса leet языка.	p@ssword, P@$$w0rd, P@$$W0RD	
Abbreviation	Конвертирует некоторые английские сочетания (если исходное слово содержит таковые) в аббревиатуры.	ihateyou -> ih8you, Ih8u	
Dups and revers	Переворачивает слово, дублирует и т.д.	drowssap, passwordpassword, PasswordDrowssap	
Vowels and consonants	Мутация заглавных и строчных букв (только Английский).	Psswrd, PaSSWoRD, pAsswOrd	
Character skip	Пропуск одной из букв пароля.	assword, Passwrd, Pasword	
Character swap	Обмен двух рядом стоящих букв.	apssword, Passowrd	
Character duplicate	Дублирование букв.	ppasword, ppaasswwoorrdd, Passwordddd	
Delimiters	Отделение букв разделителями.	p.a.s.s.w.o.r.d, P-a-s-s-w-o-r-d	Максимальный уровень использует 10 разделителей.
Dates	Добавление даты в конец слова.	Password2010, password1980	Несмотря на то, что движок мутаций может создавать более сложные варианты дат (например, password03171998 или Password19710830), эта возможность отключена даже для макс. уровня в словарной атаке.
Oem convertion	Конвертирование Английского слова на другой язык или наоборот, используя альтернативную раскладку клавиатуры (т.е. если в системе установлен второй язык).	Если в системе установлены два языка (например, Английский и Русский), программа сконвертирует начальное слово **password** в **зфыыцщкв**, а из Русского слова	Программа корректно работает с двумя и даже более языками. Так, если в системе установлено 5 языков, один из которых Английский, то программа создаст 4 разных варианта слова для этих языков.

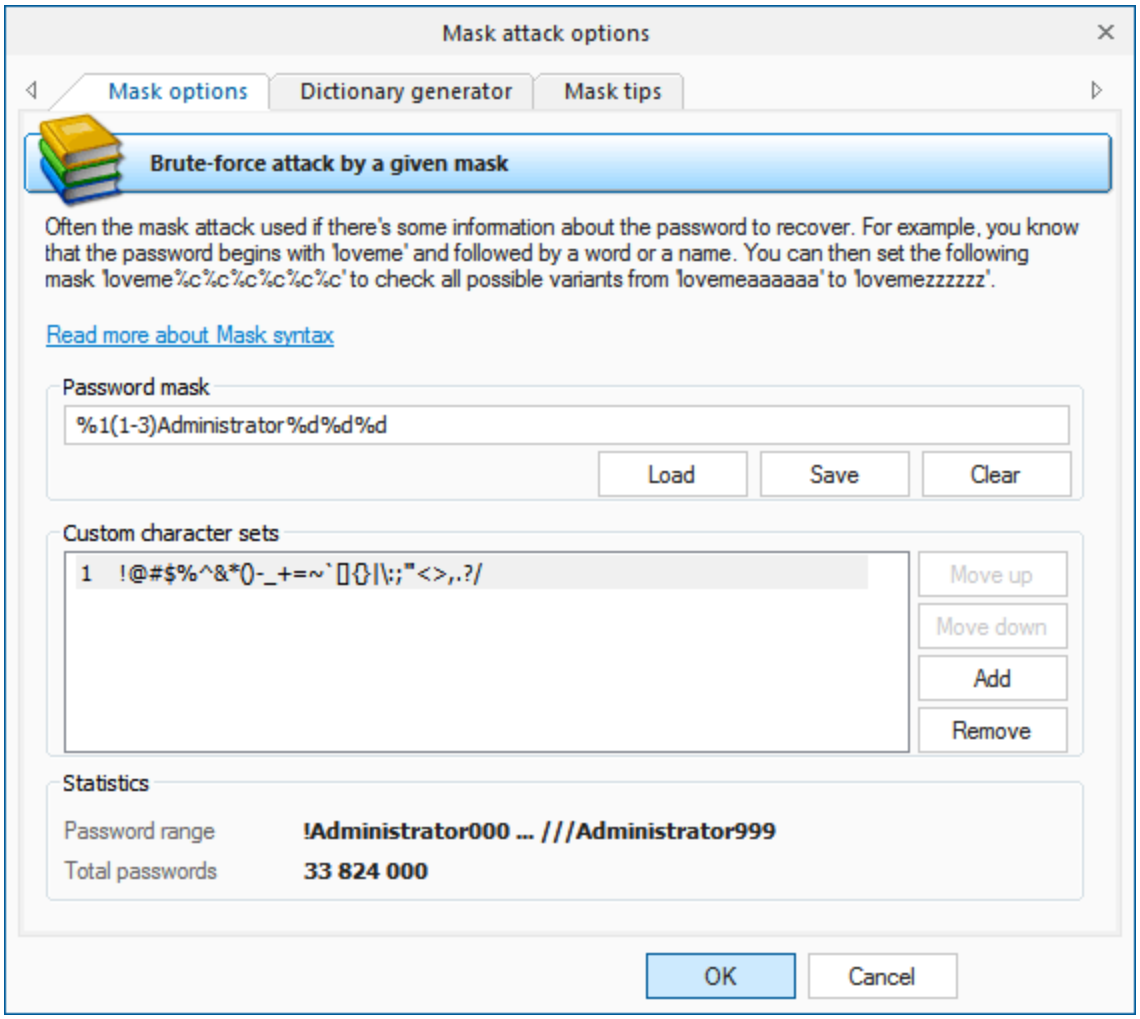
Copyright (c) 2024 Passcape Software. All rights reserved.

Имя группы	Описание	Примеры (для слова '**password**')	Комментарии
		пароль получится **gfhjkm**.	
Word shift	Тупо сдвигает все буквы слова вправо или влево.	asswordp, dpasswor	
Character substitution	Замена букв в исходном слове.	oassword, passqord	Это довольно полезное правило, учитывая тот факт, что символы замены берутся не абы как, а из специальной таблицы. Например, символ 's' может быть заменён следующими: 'a', 'w', 'e', 'd', 'x', 'z'. Заметьте, что все эти символы располагаются рядом с 's' на qwerty клавиатуре.
Length truncate	Обрезание длины слова для проверки всех возможных вариантов.	passwor, passwo, passw	

2.8.2.6 Атака по Маске

Атака по маске - незаменимый инструмент в том случае, если известна часть пароля или имеются какие-либо сведения о нем. Например, если вы знаете, что пароль состоит из 12 символов и заканчивается на qwerty, то очевидно, что перебирать весь 12 символьный диапазон паролей неразумно. Все, что потребуется, это угадать первые 6 символов искомого пароля. Для этого и существует атака по маске.

Copyright (c) 2024 Passcape Software. All rights reserved.



В нашем случае можно задать следующую маску **%c%c%c%c%c%cqwerty**. Это означает, что будут последовательно перебираться все комбинации от aaaaaaqwerty до zzzzzzqwerty. Если первоначальный пароль был secretqwerty, то он успешно попадает в наш диапазон.

Поле ввода служит для задания правила (маски), по которому будут перебираться пароли. Если оно задано правильно, то в группе "статистика" вы увидите диапазон перебираемых символов и количество паролей, генерируемых при помощи этого правила. Свои правила можно сохранять на диске. Программа позволяет также генерировать словарь по заданной маске, однако эта опция доступна не во всех редакциях.

Синтаксис маски довольно тривиален и состоит из статических (неизменяемых) и динамических (меняемых) символов или наборов. Динамические символы\наборы всегда начинаются с **%**. Например, если задать маску secret%d(1-100), то программа сгенерирует 100 паролей (secret1, secret2 .. secret100). Программа поддерживает следующие типы динамических наборов:

- **%c** набор строчных Латинских символов (a .. z). Всего 26 штук.
- **%C** набор заглавных Латинских символов (A .. Z). Всего 26 штук.
- **%#** полный набор специальных символов (! .. ~). 33 символа.
- **%@** малый набор специальных символов (!@#$%^&*()-_+= space). Всего 15 символов.
- **%?** набор всех печатных символов с ASCII кодами от 32 до 127.
- **%d** одна цифра (0..9).

Copyright (c) 2024 Passcape Software. All rights reserved.

- **%d(x-y)** последовательность чисел от x до y включительно.
- **%r(x-y)** свой набор символов с последовательными ASCII кодами от x до y
- **%r(x1-y1,x2-y2...xn-yn)** набор из нескольких непересекающихся последовательностей ASCII символов. При задании %r следует учитывать, что набор заданных OEM символов (код символа больше 127) формируется на основе DOS кодировки.
- **%1[2..9]** символ из пользовательского набора 1..9
- **%1[2..9](min-max)** пользовательский набор символов переменной длины (от min до max) для перебора. Всего можно задать своих собственных 9 наборов.
- **%w(wordlist)** слово из заданного словаря wordlist (можно указывать полный путь)

С помощью %r можно задавать наборы для своих национальных кодировок. Например, маска %r(160-175,241-241,224-239)%l(1)%l(1) создаст парольный ряд из Русских символов ааа .. яяя, всего 33*33*33=35937 паролей.

Примеры:
test%d - сгенерирует парольный ряд test0 .. test9, всего 10 комбинаций
test%d(1980-2007) - test1980 .. test2007, 28 паролей
test%r(48-57,97-122) - test0 .. testz, 36 паролей
admin%1(1-5) - admina .. adminzzzzz, где %1 - это пользовательский набор символов 1 (a..z)
%1%1%1pin%2%2%2 - aaapin000 .. zzzpin999, %1 пользовательский набор символов a..z, а %2 - второй набор, содержащий символы 0..9
%w(c:\dic\names.dic)%d - слово из словаря names.dic с цифрой в конце

Перейдя во вторую вкладку настроек, вы можете создать свой собственный словарь по заданной маске и сохранить его на диск.

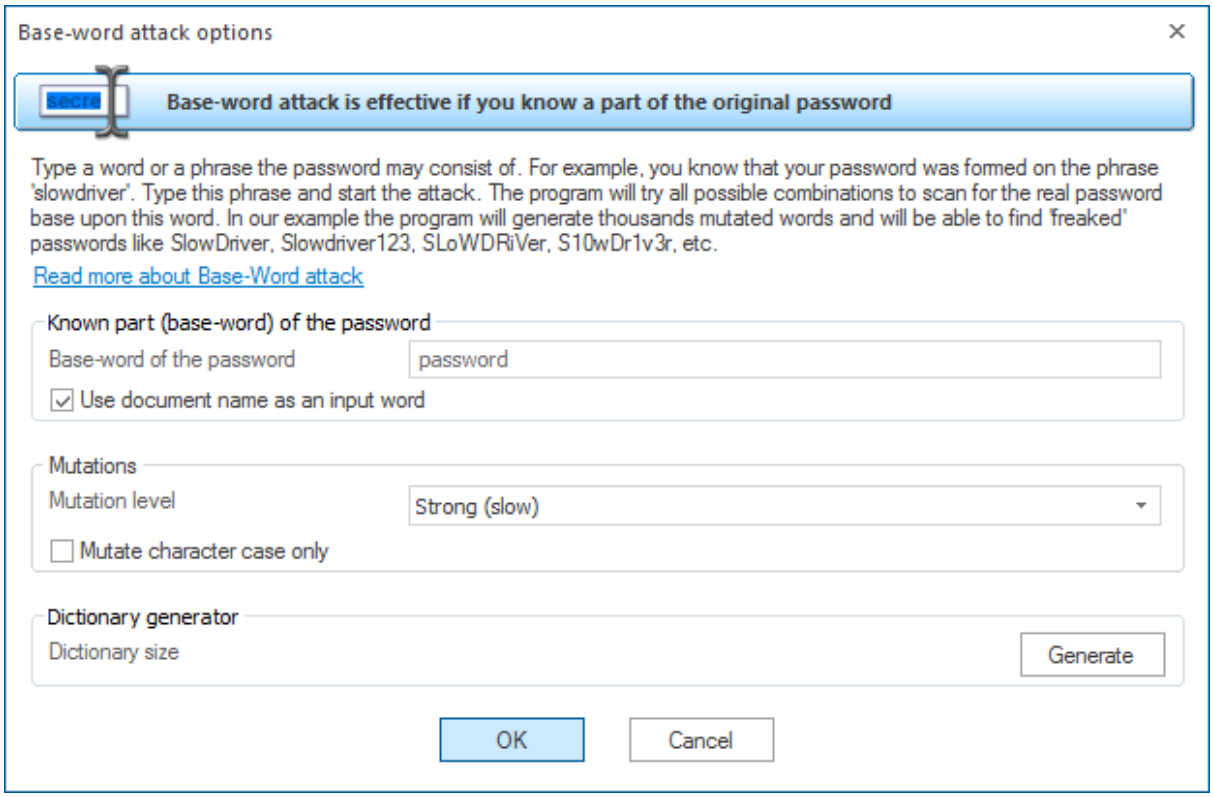
Описание синтаксиса и примеры можно посмотреть в третьей вкладке опций.

2.8.2.7 Атака по Ключевому Слову

Атака по ключевому слову (разработана в Passcape Software) во многом схожа с атакой по маске. Однако тут не надо задавать синтаксис, достаточно ввести ключевое слово на основе которого, как предполагается, был создан пароль. Атака по ключевому слову - незаменимый инструмент, если вам известна часть пароля или его базовая составляющая. Обычно в таких случаях применяется атака по маске, но она не всегда позволяет справиться с поставленной задачей. Допустим, ваш пароль был 'S10wDr1v3r'. Попытаться восстановить такой сложный пароль атакой перебором или по словарю - занятие неблагодарное, даже если вы достаточно хорошо помните, что в его основе лежит слово 'slowdriver'. В таких случаях на помощь может прийти атака по ключевому слову.

При помощи этого инструмента, программа попытается воссоздать исходный пароль, пробуя все возможные комбинации на основе 16 групповых наборов правил мутации (всего более 150 правил) . Если ввести 'slowdriver' в поле ввода, то вы увидите, что это слово подвергнется глубокой мутации и на его основе будет произведено несколько тысяч различных комбинаций, среди которых может оказаться и наш искомый пароль.

Copyright (c) 2024 Passcape Software. All rights reserved.



Вы можете выставить опцию мутации только регистра букв, тогда будут проверены все возможные варианты регистра в этом слове, всего 2^n паролей, где n - длина пароля. Например, для пароля 'slowdriver' программа выдаст 2^10=1024 различных комбинаций для каждого установленного языка в системе. Можно также сгенерировать словарь на основе этих мутаций и записать его на диск (доступно не во всех редакциях).

Установите опцию '*Use document name as an input word*' для того, чтобы программа использовала исходную фразу, основанную от имени документа.

Учтите, если длина фразы превышает 15-16 символов, то для ее мутации может потребоваться значительное время.

2.8.2.8 Комбинированная Атака по Словарям

Комбинированная атака по словарям (разработана в Passcape Software) - предназначена для поиска паролей, состоящих из 2,3 или даже 4 слов. Этот вид атаки на сложные и составные пароли очень похож на простую атаку по словарю, за тем лишь исключением, что при проверке пароля используется не одиночное слово, а сочетание слов или фраза, которая создаётся путём комбинирования слов из заданных словарей. Для её успешной работы необходимо задать как минимум два словаря и правила создания паролей. Можно задавать обычные словари, использующиеся в простой словарной атаке, но рекомендуется указывать небольшие словари с наиболее часто употребляемыми словами. Для комбинированной атаки хорошо подходят словари с различными формами слов. Например: jump, jumper, jumped, jumping.

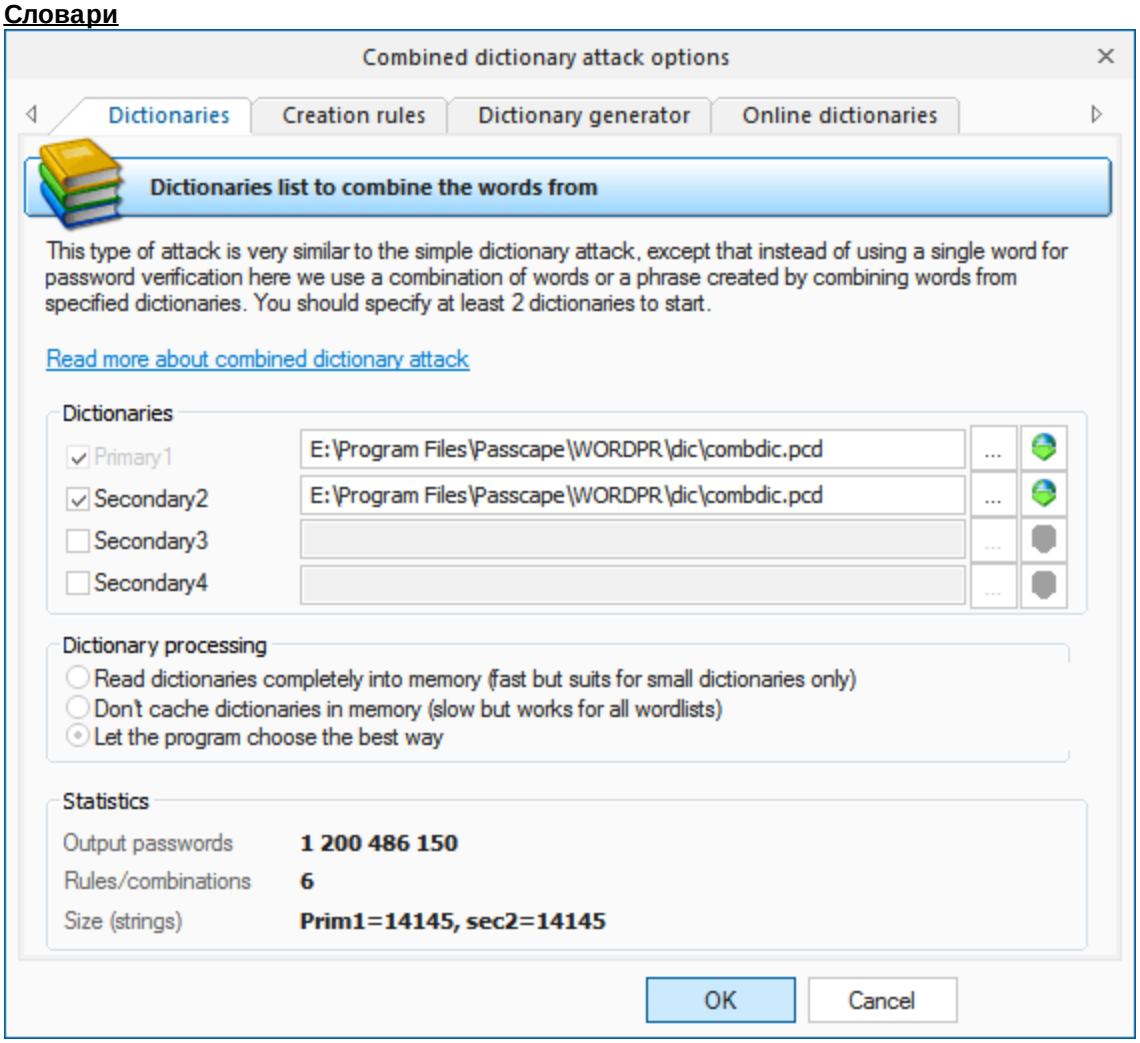
Комбинированная атака накладывает определённый лимит на количество используемых словарей: их может быть не более 4-х. Таким образом, общее ограничение данной атаки состоит в том, что можно восстанавливать парольные фразы, состоящие из не более чем 4-х слов.

Copyright (c) 2024 Passcape Software. All rights reserved.

Другой из существенных недостатков - это большой диапазон генерируемых фраз. И, как следствие этого, пропорциональный рост времени, затрачиваемого на проверку пароля. Поэтому следует учитывать, что при создании паролей, состоящих из 3 или 4 слов, процесс генерации может занять длительное время.

Не беда, если вам затруднительно найти подходящий словарь. С программой поставляется специальный словарь для комбинированной атаки. Можно также воспользоваться вкладкой Онлайн словари или соответствующей кнопкой, для скачивания таких словарей с сайта Passcape.

Словари



Алгоритм работы комбинированной атаки довольно прост. Например, если вы задали два словаря, то пароли будут создаваться следующим образом: берётся первое слово из первого словаря и соединяется с первым словом из второго, затем со вторым словом и т.д. до конца. После этого проверяется второе слово из первого словаря, и т.д.

Чтобы понять, как работает комбинированная атака, давайте рассмотрим пару примеров генерации фраз с использованием в первом случае, одного и того же словаря, а во втором случае - двух разных.

Copyright (c) 2024 Passcape Software. All rights reserved.

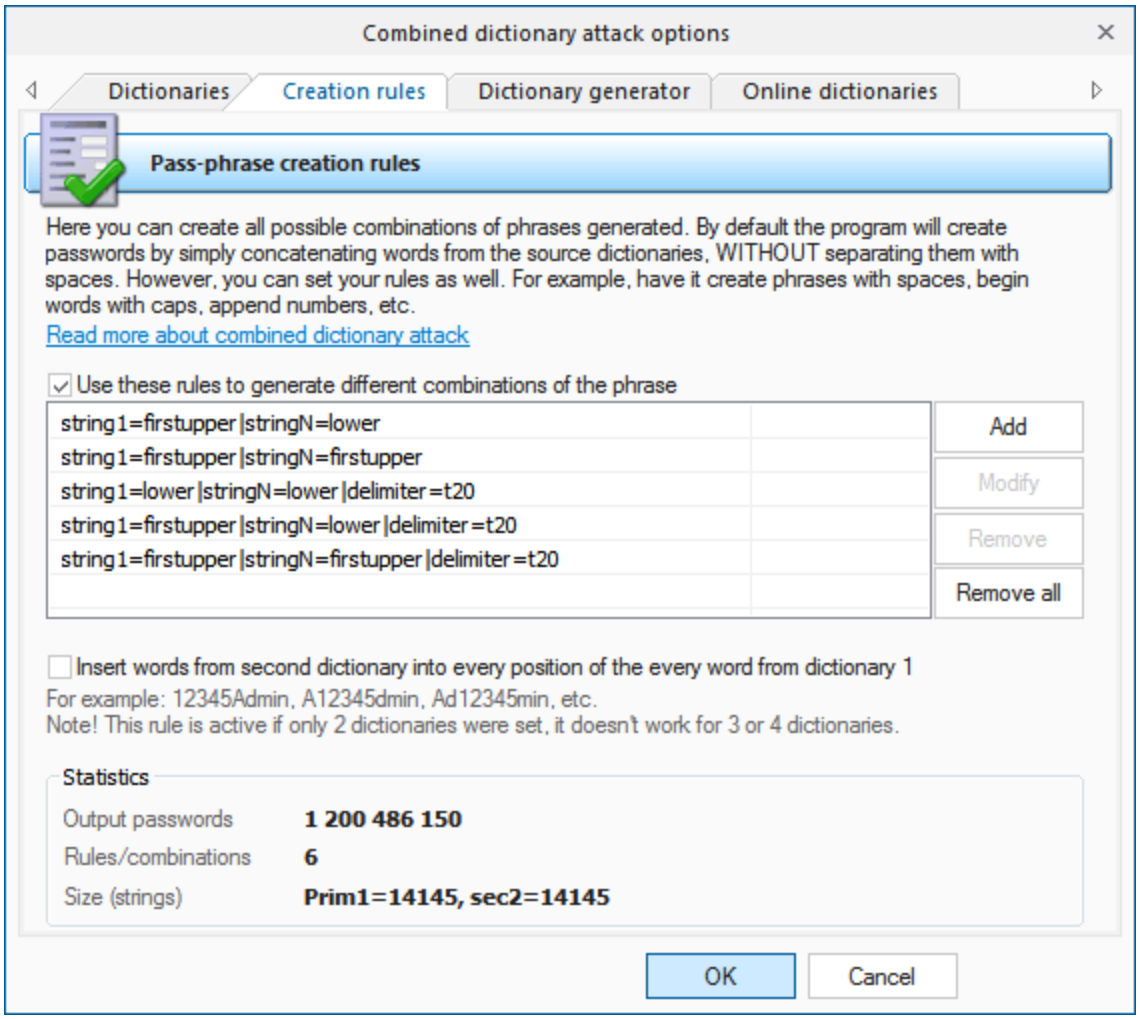
1. Предположим, у нас есть один словарь с тремя словами: action, bad и computer. Задаём этот словарь в качестве двух исходных источников: primary dictionary и additional dictionary1. После обработки этих словарей, на выходе получаем следующие фразы (они будут использоваться при проверке искомого пароля):
"actionaction", "actionbad", "actioncomputer"
"badaction", "badbad", "badcomputer"
"computeraction", "computerbad", "computercomputer".
Всего 9 фраз.

2. Во втором варианте у нас в наличие имеются два разных словаря. Например, первый словарь состоит из трёх слов: action, bad и computer. Во втором - тоже три слова: date, eagle, fail. В данном случае, получаем вот такой список фраз:
"actiondate", "actioneagle", "actionfail"
"baddate", "badeagle", "badfail"
"computerdate", "computereagle", "computerfail".

Важно помнить, что в качестве нескольких источников можно с успехом использовать как один единственный словарь, так и несколько. Все зависит от вашей фантазии. В последнем примере показано, что особое значение следует уделить порядку словарей, если они разные. Порядок слов в создаваемых фразах напрямую зависит от порядка исходных словарей. В нашем втором примере, если поменять местами основной и дополнительный словарь, то на выходе получится совсем другой набор фраз.

Правила генерации паролей

Copyright (c) 2024 Passcape Software. All rights reserved.



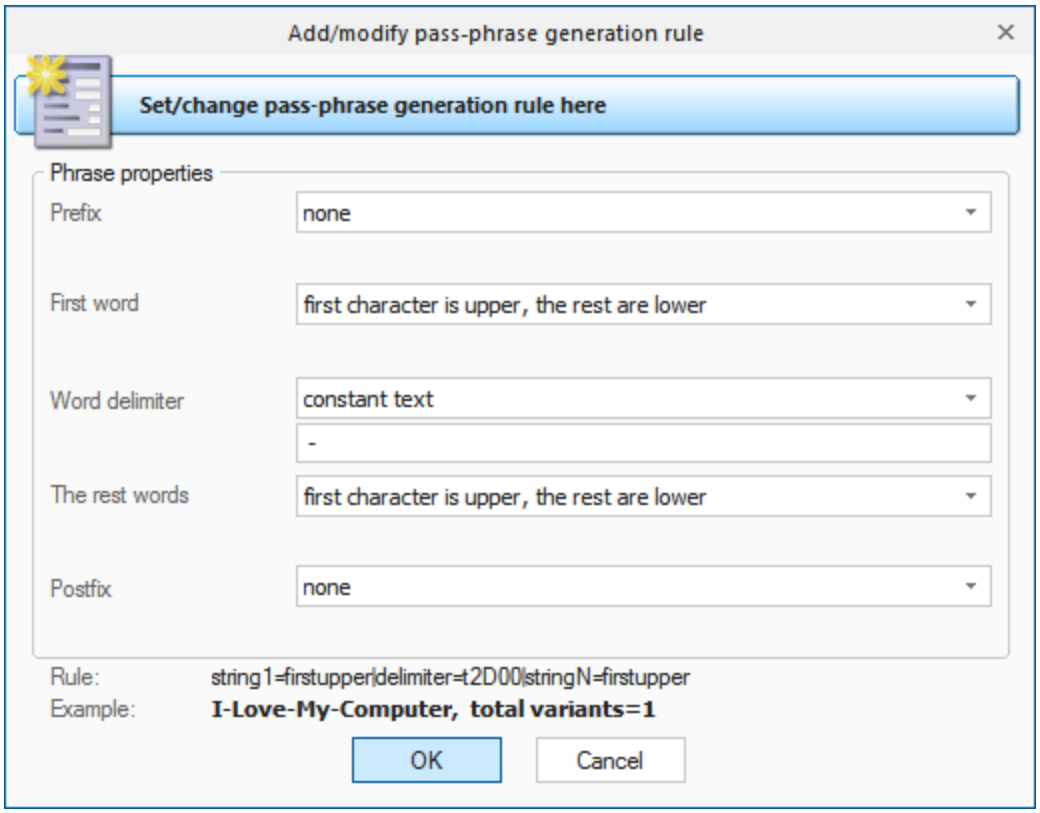
Создаваемые комбинированной атакой пароли генерируются по особым правилам, которые задаются во второй вкладке. По умолчанию, если отключена опция использования правил создания паролей, пароли генерируются простой склейкой слов из словарей без разделения их пробелами. Например, из двух слов my и computer получится mycomputer.

Если задана опция вставки слов, то программа дополнительно создаёт пароли путём вставки слов из второго словаря в каждую позицию слова из первого словаря. Например, если слово первого словаря **Admin**, а второго - **12345**, то программа сгенерирует следующие пароли:
12345Admin
A12345dmin
Ad12345min
Adm12345in
Admi12345n
И так для всех слов. Эта опция активна только если заданы два словаря.

Однако можно задавать и свои варианты мутации. Например, создавать фразы с пробелами, слова начинать с заглавных букв, задавать в конце цифры др. Правила генерации сделаны для того, чтобы максимально расширить поиск возможных вариантов пароля. Например: Mycomputer, MyComputer, MY COMPUTER, my-computer и т.п.

Для этого существует специальные правила, синтаксис которых знать необязательно, потому что диалог создания правил мутации прост и интуитивно понятен.

Copyright (c) 2024 Passcape Software. All rights reserved.



Каждое правило мутации состоит из пяти элементов:

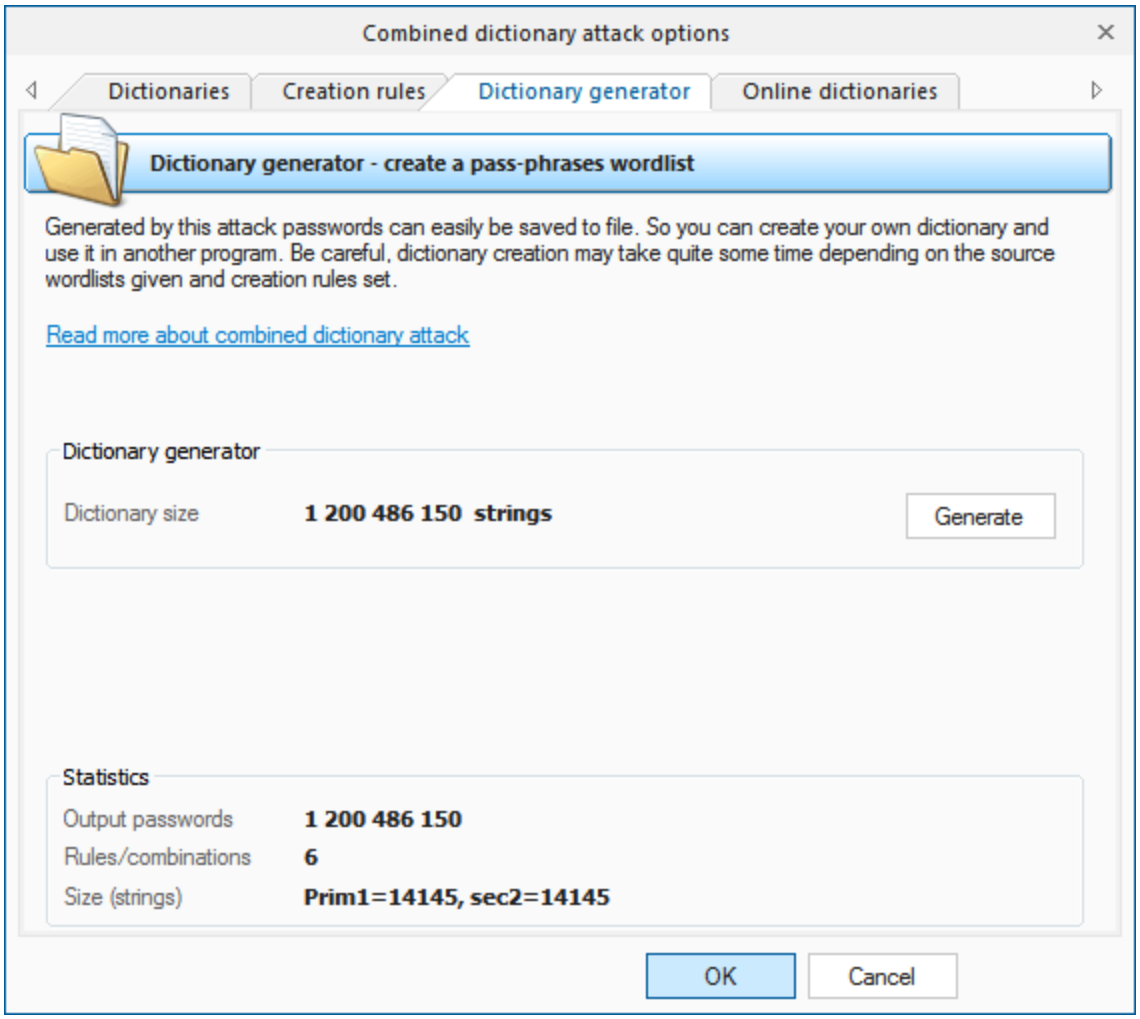
1. Префикс - текст, который будет стоять перед каждой фразой. Этот элемент может быть символом, простой текстовой строкой, цифрой от 0 до 9 или числом. Например, если задать префиксом цифру, то создаваемые с помощью этого правила фразы могут выглядеть следующим образом: "0aaabbb", "1aaabbb" .. "9aaabbb".
2. Первое слово. То, что следует делать с первым словом каждой фразы. Вариантов - всего четыре. А именно: оставлять как есть в словаре, делать строчными все буквы, делать заглавными все буквы или делать заглавной только первую букву слова.
3. Разделитель слов во фразе. Он может отсутствовать. Тогда все слова будут склеены. Например: "aaabbb", "aaaccc","aaaddd" и т.д. Можно задавать свой разделитель, например символ '-'. А можно задать диапазон символов. Тогда все символы из этого диапазона будут проверяться последовательно.
4. Остальные слова. Этим атрибутом, аналогично п.2, можно задавать правила для всех остальных слов фразы.
5. Постфикс - текст, которым будет завершаться каждая фраза. Например, если задать постфиксом символ '?' или ' ?', то все фразы, создаваемые на основе этого правила будут заканчиваться знаком вопроса.

Естественно, чем больше правил создания паролей, тем больше вероятность угадывания искомого пароля, но и тем больше времени потребуется на атаку.

Группа "Статистика" показывает количество слов в исходных словарях, общее количество генерируемых фраз и другую полезную информацию.

Генератор словарей

Copyright (c) 2024 Passcape Software. All rights reserved.



Третья вкладка опций служит для создания словарей на основе комбинированной атаки.

В последней вкладке можно скачать с нашего сервера один или несколько специализированных словарей для этой атаки.

2.8.2.9 Атака по Фразе

Все больше и больше пользователей в качестве своих паролей выбирают целые фразы, отрывки из стихотворений, крылатые выражения из фильмов, латинские афоризмы, текст любимых песен и т.п. Поиск таких паролей традиционными методами - дело немыслимое при развитии вычислительной мощности современных компьютеров. Поэтому на помощь в восстановлении приходит атака по уже готовым и известным фразам.

Атака по фразе (разработана в Passcape Software) во многом схожа с простой словарной атакой за тем лишь исключением, что поиск паролей осуществляется не пословно, а пофразно. Подобно атаке по словарю, из исходного словаря поочередно берутся фразы и проверяются на предмет совпадения с исходным паролем. Атака по фразам - это тот необходимый инструмент в восстановлении паролей, значение которого сложно переоценить.

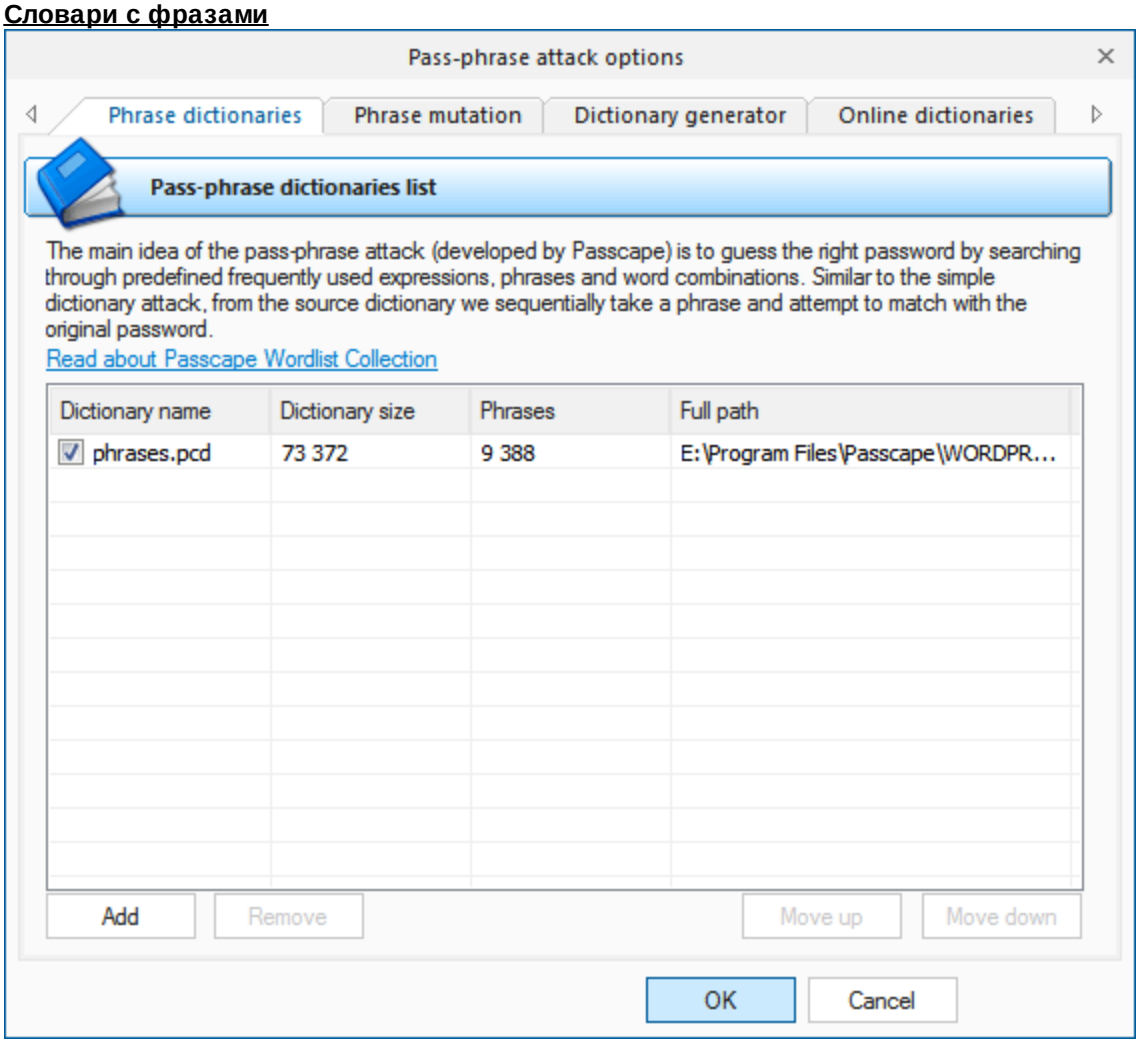
Copyright (c) 2024 Passcape Software. All rights reserved.

Например, если искомый пароль соответствует широко известной фразе 'To be or not to be', то очевидно, что справиться с таким паролем под силу лишь данной атаке. Для этого необходимо указать специальный словарь фраз. Простейший словарь поставляется вместе с программой, но имеется возможность подгрузки Онлайн словарей специально для этой атаки.

Не будет преувеличением сказать, что успех в расшифровке искомого пароля в атаке по фразам на 99 процентов зависит от качества словарей. Скорее всего, именно поэтому данный вид атак не встречается практически ни в одном парольном взломщике: сбор фраз и создание специализированных словарей - задача чрезвычайно трудоёмкая. Passcape Software даёт возможность задействовать целый набор онлайн и оффлайн словарей (всего более 1.5 Гб), специально подготовленных для данного типа атаки.

Например, многие пользователи выбирают пароли в виде отрывков из любимых песен или музыкальных групп. Поэтому мы создали специальные, уникальные (не найдёте больше нигде в сети!) музыкальные сборники фраз. Есть также библейский сборник, фразы из кино, крылатые и латинские выражения и т.д.

Словари с фразами

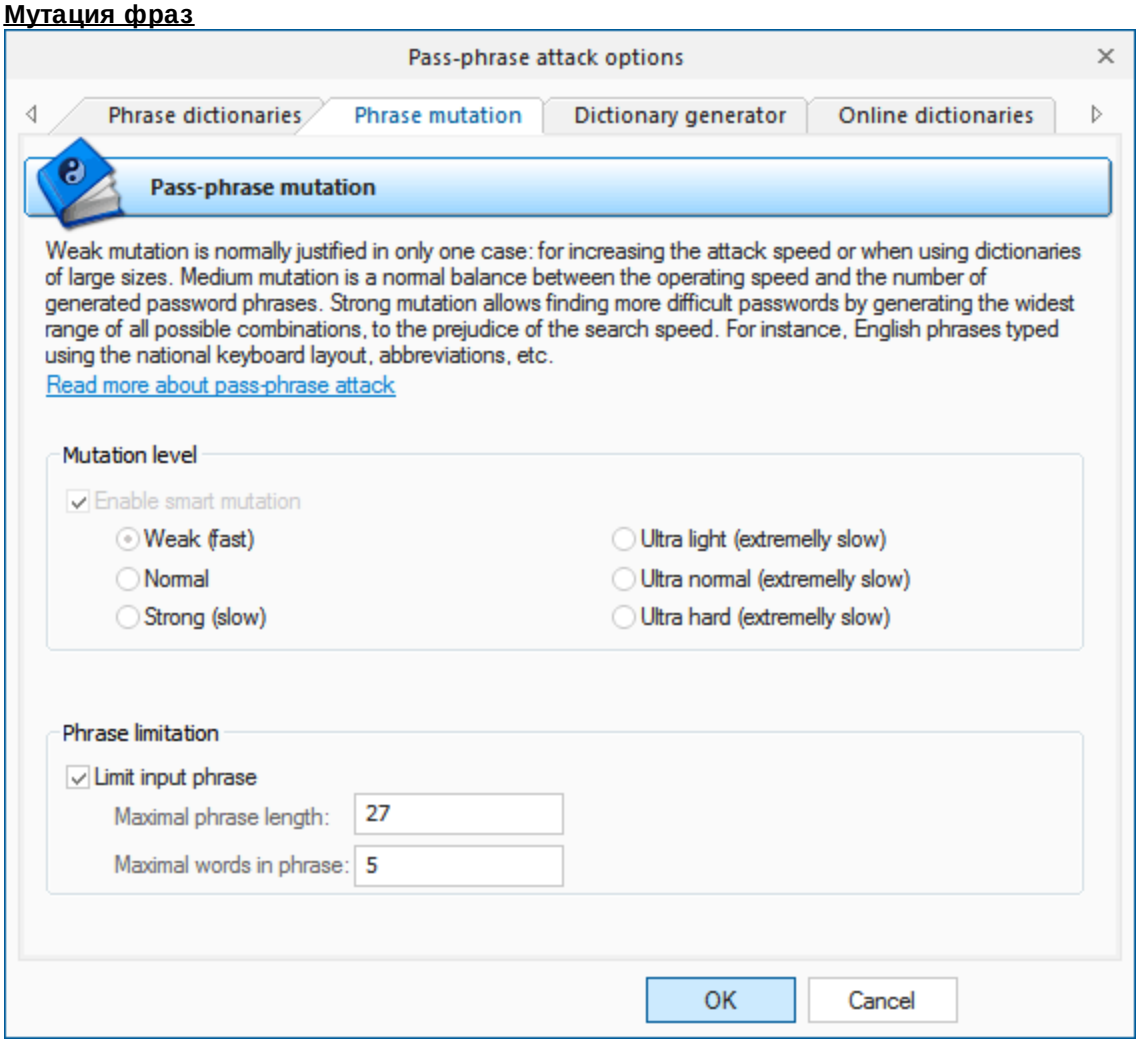


Опции атаки по фразе практически один в один напоминают настройки простого словарного перебора: так же необходимо выбрать один или несколько словарей в качестве источника фраз,

Copyright (c) 2024 Passcape Software. All rights reserved.

также имеется возможность подгружать дополнительные словари с сайта Passcape, аналогично задаются правила мутации (создании альтернативных вариантов) фраз.

Мутация фраз



О мутации следует сказать особо, поскольку, как вам уже наверное должно быть известно, сильная мутация значительно увеличивает шансы на успешное восстановление. Слабая мутация обычно оправдана только в одном случае: для увеличения скорости атаки или при использовании словарей больших размеров. Кроме того, сильная мутация позволяет находить более сложные пароли, генерируя наибольший диапазон всевозможных комбинаций в ущерб скорости перебора. Различия различных уровней мутации:

- Weak - наиболее быстрые и простые мутации.
- Normal - тоже, что и Weak, но с дополнительными мутациями и генерацией нескольких вариантов регистра букв.
- Strong - аналогично Normal с дополнительными мутациями и генерацией национальных паролей (в соответствии с установленной на ПК клавиатурной раскладке, или раскладок, если их несколько).
- Ultra light - каждый генерируемый в режиме Weak пароль подвергается дополнительным простым мутациям (аналогично режиму Weak в простой словарной атаке).
- Ultra normal - каждый генерируемый в режиме Normal пароль подвергается дополнительным простым мутациям (аналогично режиму Normal в простой словарной атаке).

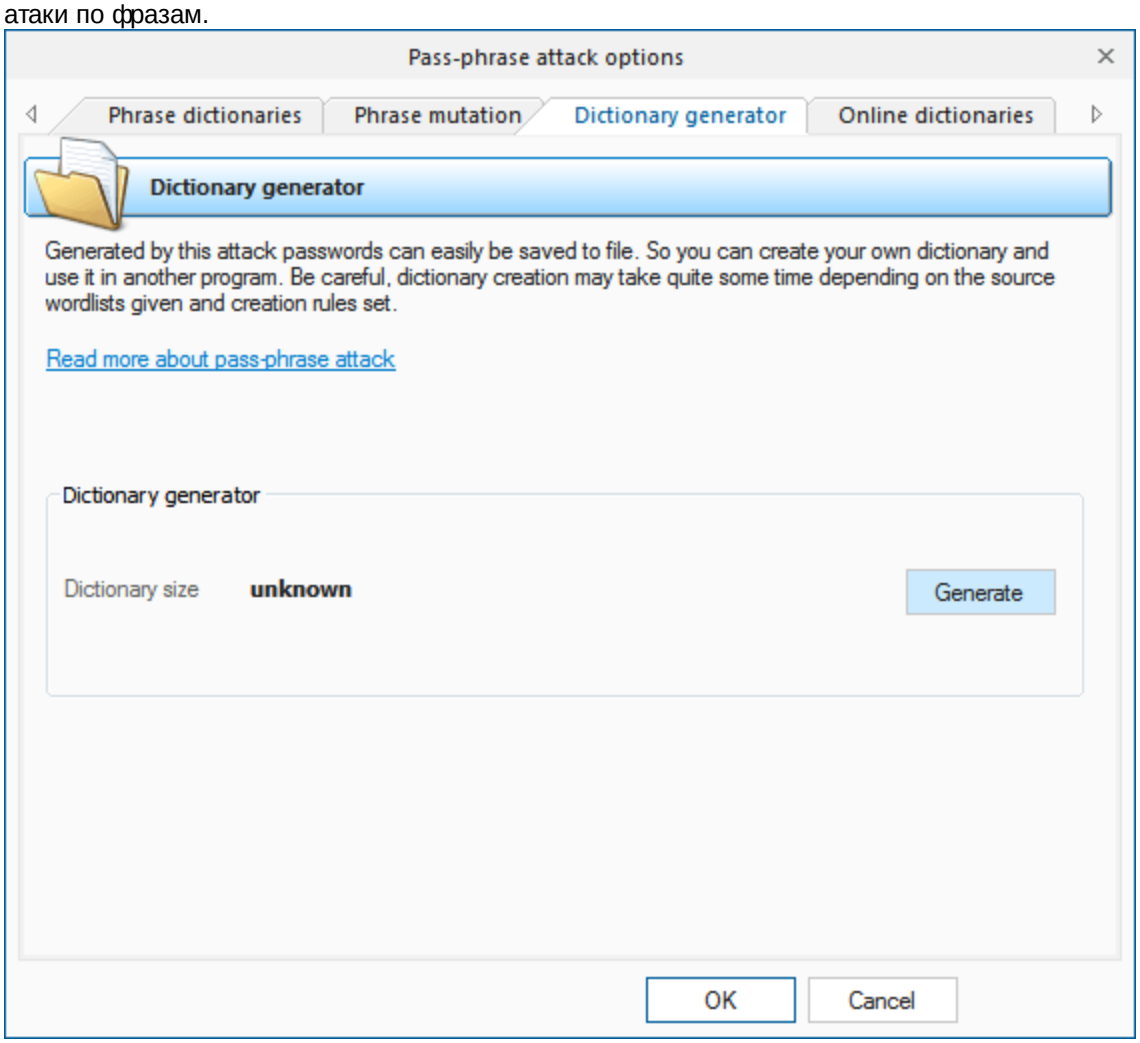
Copyright (c) 2024 Passcape Software. All rights reserved.

- Ultra hard - каждый генерируемый в режиме Strong пароль подвергается дополнительным простым мутациям (аналогично режиму Strong в простой словарной атаке).

Осторожно! В режимах Ultra, из-за большого количества генерируемых вариантов, проверка паролей может происходить очень медленно. Для того, чтобы немного увеличить скорость работы этой атаки в Ultra режимах, можно выставить лимит на размер исходных фраз. Например, ограничить максимальную длину 64 символами и 6 словами.

Генератор словарей

В третьей вкладке настроек можно создать свой словарь фраз на основе установленных опций атаки по фразам.



2.8.2.10 Гибридная Атака по Словарю

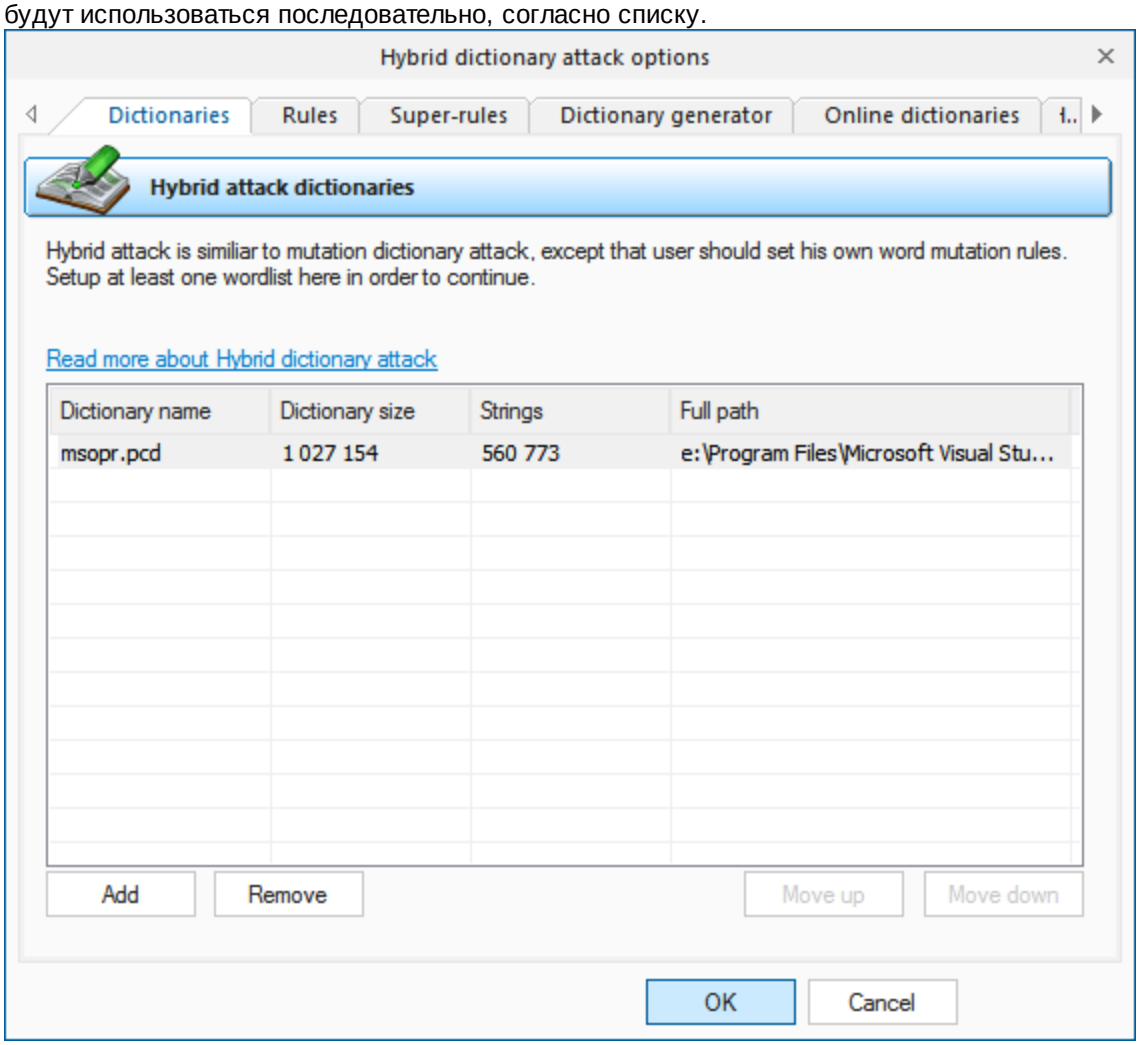
Гибридная атака по словарю - это разновидность простой словарной атаки. Однако в отличие от последней, гибридная атака позволяет пользователю задавать свои собственные правила мутации (вариации) слов и проверять их в качестве исходного пароля. Например, можно перевести первую букву проверяемого пароля в верхний регистр, добавить в конец символ 2, заменить 8 на B, O на 0 и т.д.

Copyright (c) 2024 Passcape Software. All rights reserved.

Действия, применяемые к исходным словам словаря, называются правила. К одному исходному слову можно применять несколько правил. Вместе с дистрибутивом программы поставляется расширенный набор правил мутации паролей.

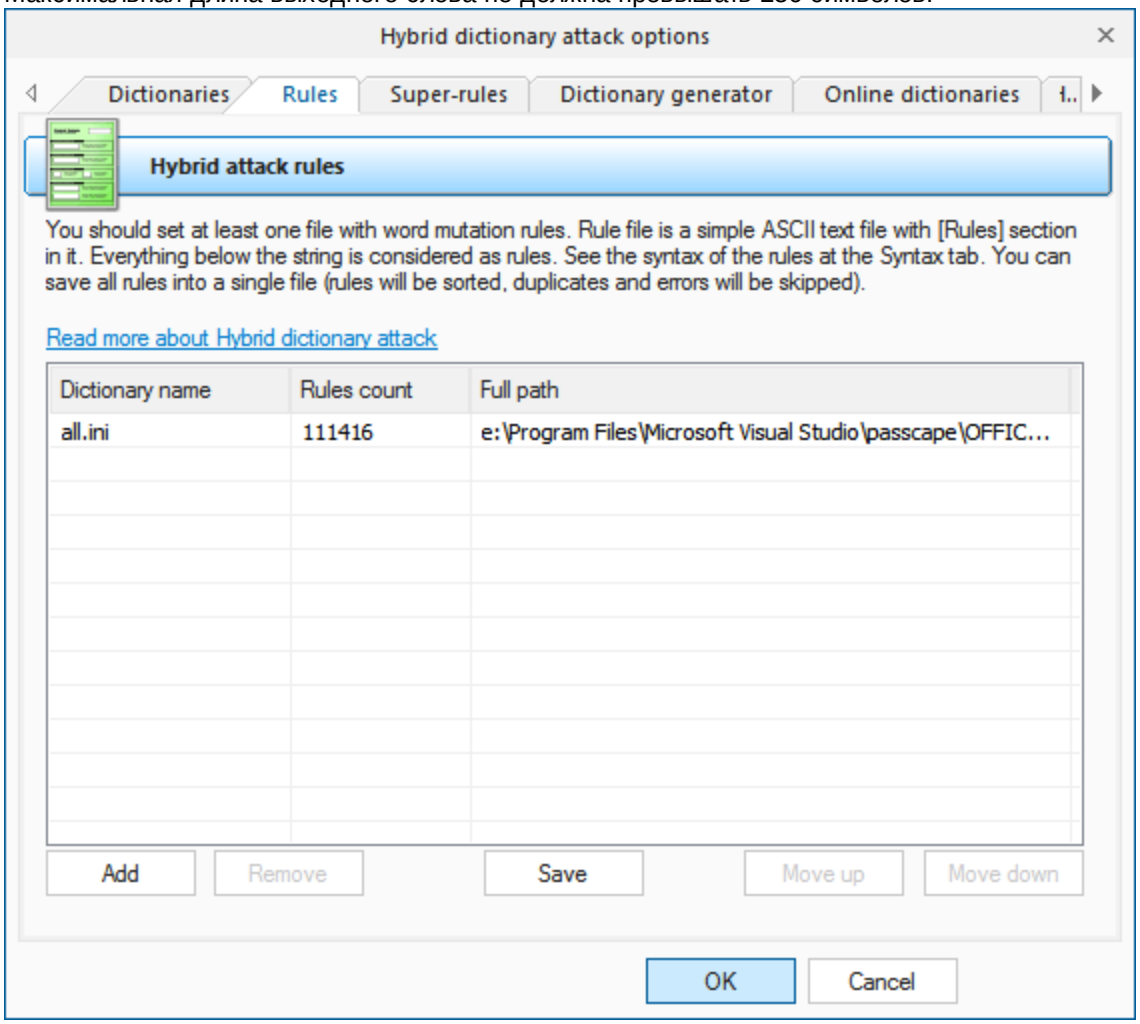
Опции гибридной атаки по словарю разделены на 7 вкладок:
1. **Словари** - для задания исходных словарей
2. **Правила** - файлы с наборами правил
3. **Супер-правила** - правила, которые можно применить поверх всех обычных (до или после них)
4. **Генератор словаря**, в которой можно создавать готовые словари, получаемые в результате работы гибридной атаки
5. **Онлайн словари** - для скачивания новых словарей в программу
6. **Синтаксис атаки** - полное описание всех правил с примерами
7. **Тестер правил** для тестирования собственных правил

Словари для атаки задаются в первой вкладке. Традиционно поддерживаются следующие форматы: ASCII, UTF8, UNICODE, PCD, RAR, ZIP. Порядок файлов в списке можно менять. Например, небольшие словари перемещать в начало списка или наоборот. При этом в атаке они будут использоваться последовательно, согласно списку.



Copyright (c) 2024 Passcape Software. All rights reserved.

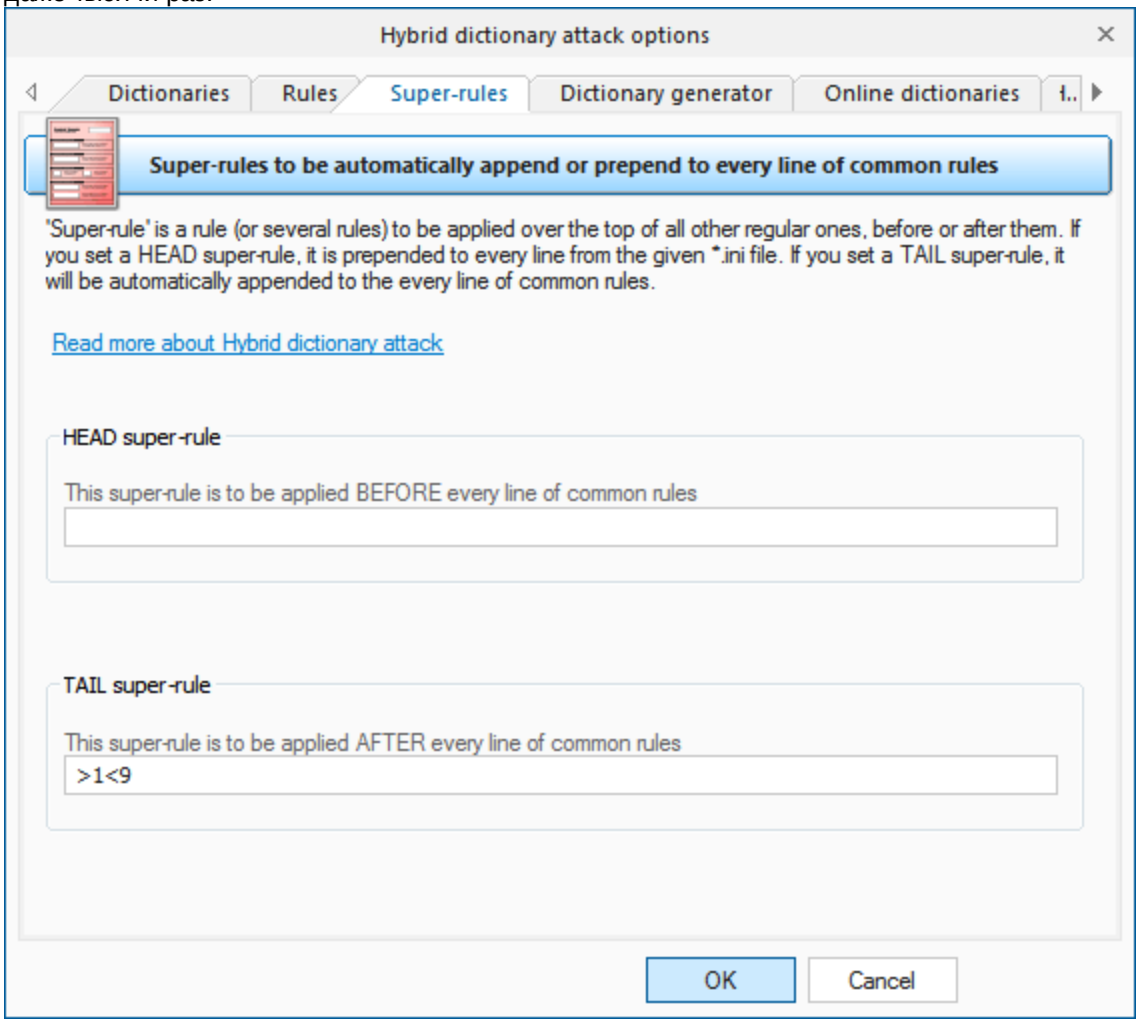
Во вкладке *'Правила'* необходимо задать по крайней мере один файл с правилами мутации паролей. С программой поставляется несколько файлов, например, **english_words.ini** с более чем 3000 правилами. Формат файла с правилами довольно тривиален и представляет собой простой текстовый ASCII файл со строкой **[Rules]**. Все, что идёт до этой сроки, считается комментариями и игнорируется программой. Все, что после, рассматривается как правила. Каждая строка может содержать несколько правил, применяемых к исходному слову. Если строка содержит несколько правил для одного слова, то эти правила обрабатываются слева направо. Например, если к исходному слову 'password' применить правило '@pc$a$b$c', то на выходе получим 'Asswordabc'. Максимальная длина выходного слова не должна превышать 256 символов.



Супер-правило - это одно или несколько правил, которые необходимо применить поверх всех обычных наборов правил. Точнее, до или после них. Например, после отработки обычного правила (или нескольких, если они заданы на одной строке), для того, чтобы сгенерировать все возможные комбинации заглавных и строчных букв, можно задать конечное супер-правило 'a8'. Так правило '/asa4' из файла l33t.ini будет '/asa4a8', а '/csc(' превратится в '/csc(a8', и т.д. Ещё один пример: если установить начальное супер-правило '>8<G', то до начала обычной мутации будут отклонены все слова меньше 8 или больше 16 символов.
Это довольно полезная опция если вы решите применить какое-либо правило ко всем строкам заданных *.ini файлов, поскольку нет нужды править в них все текстовые строки. Будьте

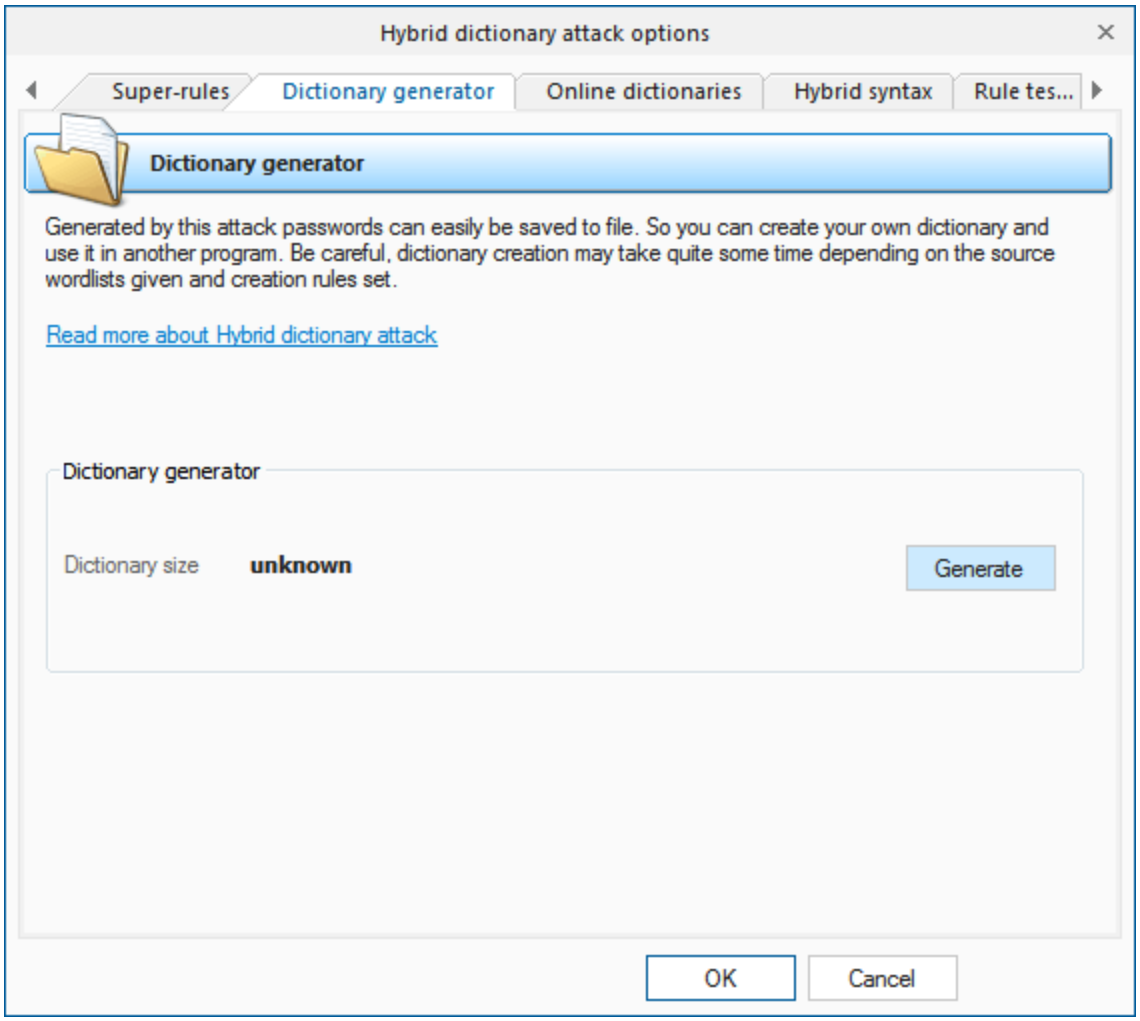
Copyright (c) 2024 Passcape Software. All rights reserved.

аккуратны, однако: супер-правило 'aN' может увеличить число генерируемых паролей в сотни или даже тысячи раз!



Вкладка *'Генератор словаря'* предназначена для создания словарей, получаемых в результате работы этой атаки. В дальнейшем, эти словари, к примеру, можно использовать в других программах. Для создания словаря, задайте исходный словарь и набор правил мутации. Длина генерируемого файла может превышать 2 Гб. Будьте осторожны, процесс создания словаря может занять значительное время!

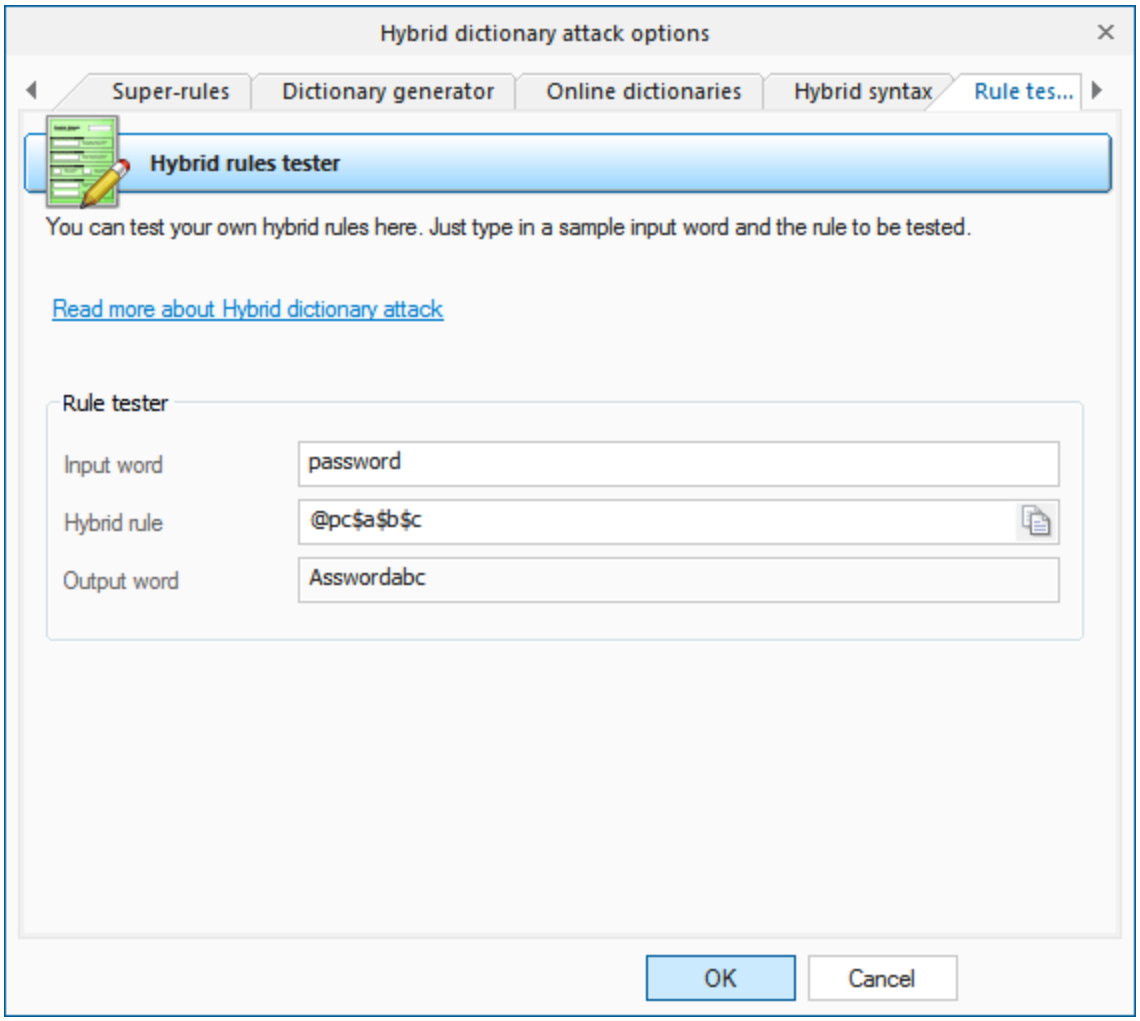
Copyright (c) 2024 Passcape Software. All rights reserved.



Во вкладке 'Онлайн словари' можно скачать с сайта Passcape исходные словари для этой атаки.

Если вы хотите создать свой собственный набор правил, то две последние вкладки можно использовать как помощь. Если во вкладке 'Синтаксис' даны простые описания правил, то в последней кладке можно их протестировать, задав исходное слово и правило для гибридной атаки. Свои наборы правил присылайте нам. Если они покажутся нам интересными/полезными, мы включим их в стандартную поставку программы.

Copyright (c) 2024 Passcape Software. All rights reserved.



Описание синтаксиса правил гибридной атаки по словарю

Допускается задавать несколько правил на одной строке.
Обработка правил (если их несколько на одной строке) идёт слева направо.
Максимальная длина строки - 256 символов.
Максимальная длина выходного слова 256 символов.
Весь текст до строки **[Rules]** считается комментарием и игнорируется.
Строка, начинающаяся символом # считается комментарием и игнорируется.
Пробелы в строках, если они не являются частью правил, игнорируются.
Значения параметров N и M начинаются с 0. Для значений больше 9 используйте A..Z (A=10, B=11 и т.д.). Например, правило 'C ограничивает длину слова 12 символами.

Правила

Правило	Пример	Вход. слово	Выход. слово	Описание правила
:	:	password	password	Ничего не делать со словом
{	{	password	asswordp	Сдвинуть слово влево
}	}	password	dpasswor	Сдвинуть слово вправо
[	[	password	assword	Удалить первый символ слова
]	]	password	passwor	Удалить последний символ слова

Copyright (c) 2024 Passcape Software. All rights reserved.

Правило	Пример	Вход. слово	Выход. слово	Описание правила
c	c	password	Password	Сделать первую букву заглавной
C	C	password	pASSWORD	Первая буква строчная, остальные заглавные
d	d	love	lovelove	Дублировать все слово
f	f	love	loveevol	Отразить (зеркальная перестановка букв)
k	k	password пароль	зфыыцщкв gfhjkm	Конвертировать слово используя альтернативную (первую после установленной по-умолчанию) раскладку клавиатуры. Это правило работает в обоих направлениях. Например, если в системе установлена Русская раскладка клавиатуры, это правило трансформирует слово 'password' в русский эквивалент 'зфыыцщкв', а Русское слово 'пароль' в 'gfhjkm'. Это бывает очень полезно, когда имеем дело с не-английскими паролями. Если в системе установлен только один язык, правило будет проигнорировано.
K	K	password	passwodr	Поменять местами два последних символа
l	l	password	password	Все буквы в нижний регистр
q	q	baby	bbaabbyy	Дублировать все символы в слове
r	r	password	drowssap	Перевернуть слово
t	t	PassWord	pASSwORD	Обратить регистр букв (инверсия регистра)
u	u	password	PASSWORD	Все буквы в верхний регистр
U	U	my own key	My Own Key	Первые буквы всех слов в верхний регистр (подразумевается, что слова разделены пробелом)
V	V	password	PaSSWoRD	Согласные буквы перевести в верхний регистр, гласные - в нижний
v	v	password	pASSWoRD	Согласные буквы перевести в нижний регистр, гласные - в верхний
'N	'4	password	pass	Обрезать слово до длины N
+N	+1	password	pbssword	Увеличить значение ASCII символа в позиции N
-N	-0	password	oassword	Уменьшить значение ASCII символа в позиции N
.N	.4	password	passoord	Заменить символ в позиции N символом в позиции N+1
,N	,1	password	ppssword	Заменить символ в позиции N символом в позиции N-1. Где N > 0.
<N				Отклонить (пропустить) слово если его длина превышает N символов
>N				Отклонить (пропустить) слово если его длина меньше N символов
aN				Проверять все возможные комбинации регистра букв. N задаёт максимальную длину слова, для которого может быть применено это правило.
DN	D2D2	password	paword	Удалить символ в позиции N
pN	p3	key	keykeykey	Копировать слово N раз
TN	T1T5	password	pAsswOrd	Обратить регистр букв в позиции N
yN	y3	password	paspassword	Продублировать первые N символов
YN	Y3	password	paswordord	Продублировать последние N символов
zN	z3	password	ppppassword	Дублировать первый символ слова N раз

Copyright (c) 2024 Passcape Software. All rights reserved.

Правило	Пример	Вход. слово	Выход. слово	Описание правила
ZN	Z3	password	passwordddd	Дублировать последний символ слова N раз
$X	$0$0$7	password	password007	Добавить символ X в конец слова
^X	^3^2^1	password	123password	Вставить символ X в начало слова
@X	@s	password	paword	Удалить все символы X из слова
!X				Отклонить (пропустить) слово если оно содержит по крайней мере один символ X
/X				Отклонить (пропустить) слово если оно не содержит символ X
(X				Отклонить (пропустить) слово если его первый символ не X
)X				Отклонить (пропустить) слово если его последний символ не X
eX	e@	mike@yahoo.com	mike	Извлечь подстроку, начинающуюся с первой позиции и заканчивающуюся перед первым найденным символом X (X не входит)
EX	E@e.	mike@yahoo.com	yahoo	Извлечь подстроку, которая начинается сразу за первым найденным символом X (и до конца строки)
%MX				Отклонить (пропустить) слово если оно не содержит по меньшей мере M символов X
***XY**	*15	password	possward	Поменять местами символы в позициях X и Y
=NX				Отклонить (пропустить) слово если символ в позиции N не X
iNX	i4ai5bi6c	password	passabcword	Вставить символ X в позицию N
oNX	o4*o5*	password	pass**rd	Перезаписать символ в позиции N символом X
sXY	ss$so0	password	pa$$w0rd	Заменить все символы X на Y
xNM	x4Z	password	word	Извлечь подстроку длиной M символов начиная с позиции N
INX-Y	rl0/-/r	google.com	google.com/	Вставить символ X в позицию N, если предыдущий символ в позиции N не равен Y.
INX+Y	rl0.+.r	password.	password..	Вставить символ X в позицию N, если предыдущий символ в позиции N равен Y.
ONX-Y	O0-+p	password	-assword	Если символ в позиции N не равен Y, перезаписать его символом X.
ONX+Y	O0P+p	password	Password	Если символ в позиции N равен Y, перезаписать его символом X.

Дополнительно

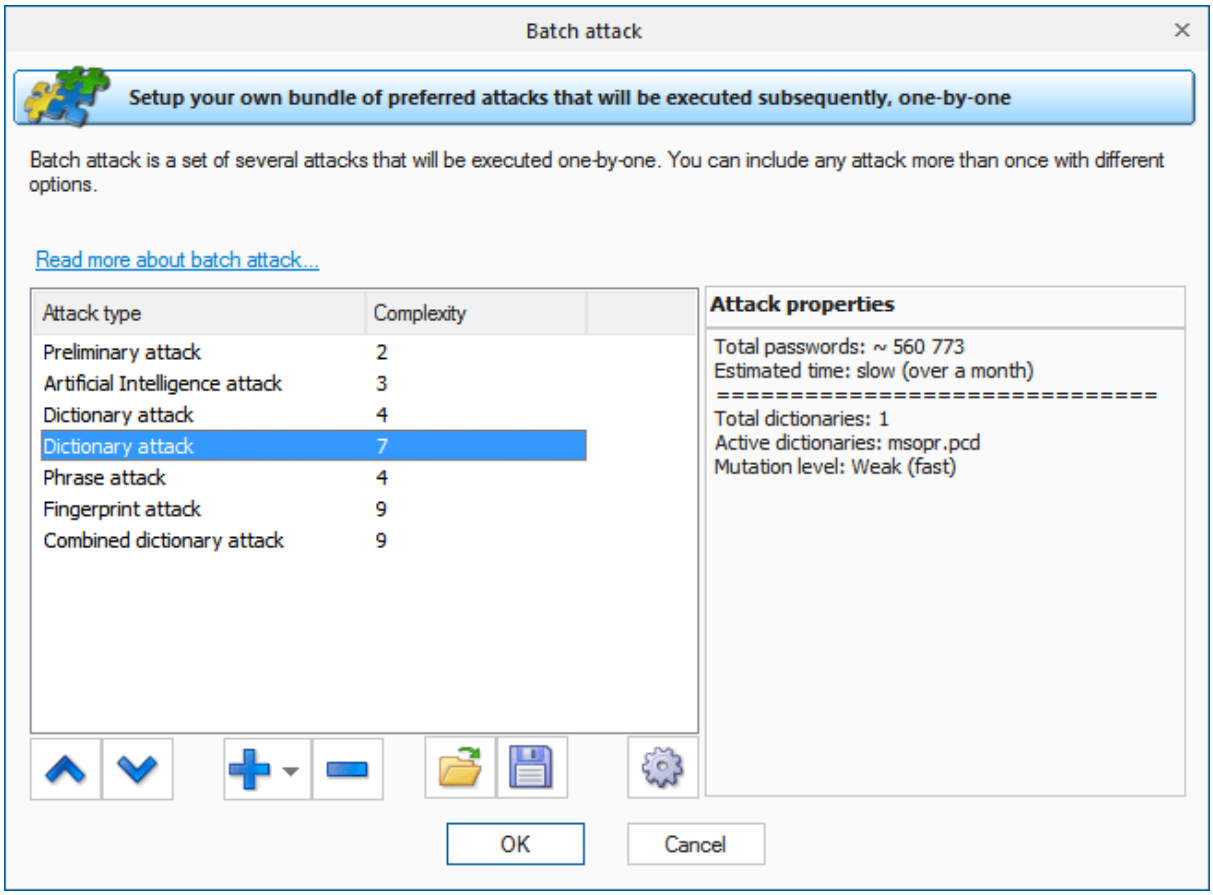
Вместе с дистрибутивом программы поставляется расширенный набор правил мутации паролей:
Файл **hybrid_rules/english_words.ini** содержит набор основных правил для английских паролей.
hybrid_rules/simple_dates.ini - правила с датами, месяцами, временами года и т.д.
hybrid_rules/l33t.ini - правила уродованием слов. Например, password->p@$$w0rd
hybrid_rules/dotcom.ini - правила с интернет доменами
hybrid_rules/numbers.ini - правила с цифрами
hybrid_rules/overwrite.ini - расширенный набор правил для английских слов.

Copyright (c) 2024 Passcape Software. All rights reserved.

Если вам нужен наиболее простой способ охватить как можно больше вариантов паролей, скачайте наш полный набор более чем 180000 правил.

2.8.2.11 Групповая Атака

Поскольку каждая атака охватывает свой диапазон паролей, то иногда, для полноценной расшифровки паролей, необходимо запустить последовательно несколько видов атак. Основная идея групповой атаки, разработанной в Passcape Software, состоит в создании списка/группы из последовательно выполняющихся атак, так, чтобы в последствие запускать все эти атаки одним щелчком, а не настраивать каждый раз по отдельности.



Опции групповой атаки представлены в виде списка, который можно пополнять или укорачивать (кнопки [+] и [-]). Каждую атаку в списке можно двигать вверх-вниз (кнопки [^] и [v]) , а также менять ее настройки. В группу можно включать несколько атак одного вида с разными настройками. Справа от списка атак отображается свойства текущей выбранной записи: краткие характеристики атаки и сколько приблизительно времени займёт её работа.

2.9 Меню Вид

Меню Вид позволяет включать\отключать вспомогательные элементы интерфейса программы, менять язык интерфейса, сворачивать программу в трей или работать в режиме невидимости.

Copyright (c) 2024 Passcape Software. All rights reserved.

2.10 Меню Темы

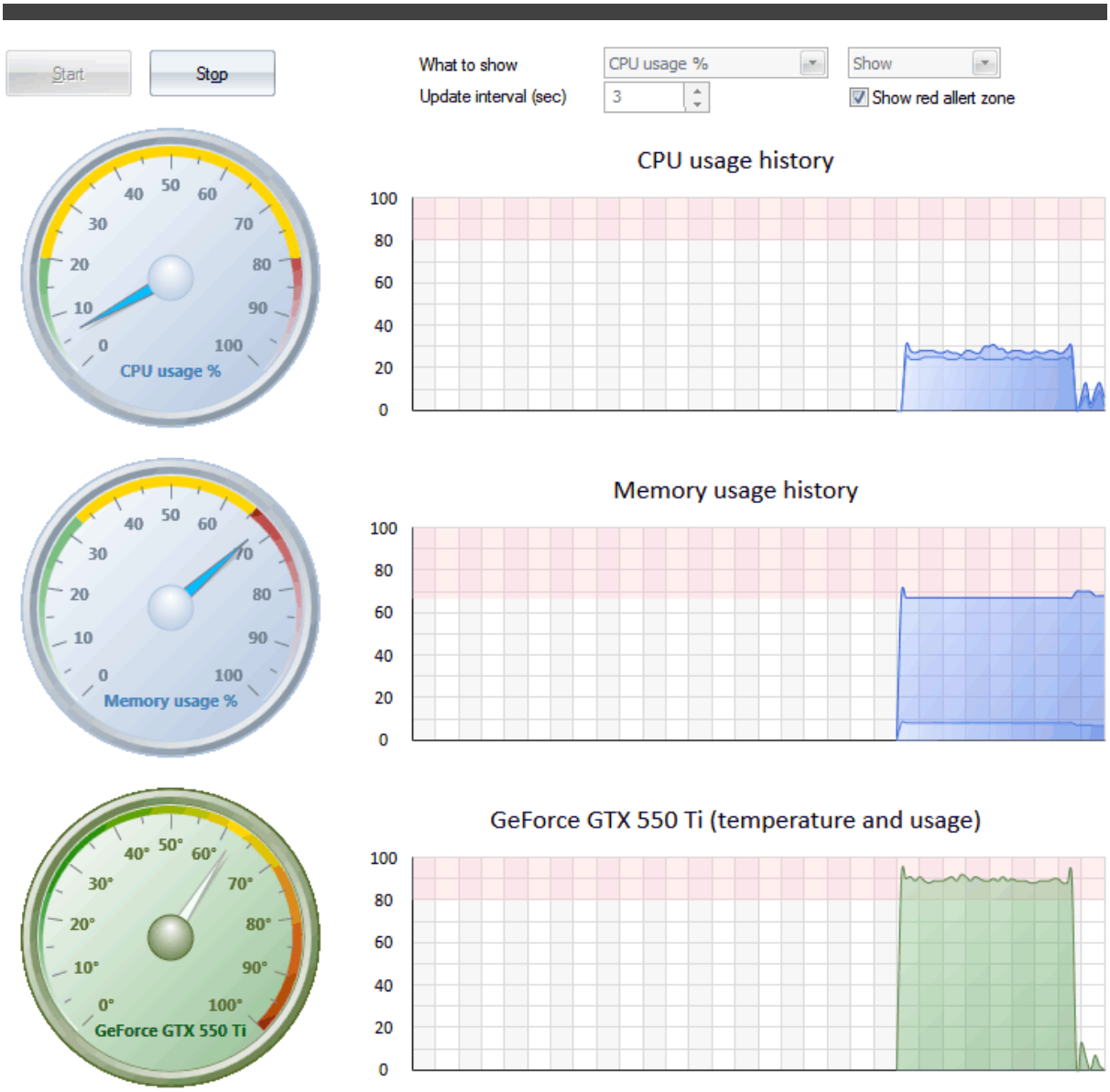
В этом меню можно выбрать одну из понравившихся тем или создать свою собственную.

2.11 Меню Помощь

В этом разделе меню можно вызвать справку о программе, посетить домашнюю страницу программы, проверить обновления, выслать отчет об ошибке, зарегистрировать программу и др.

Copyright (c) 2024 Passcape Software. All rights reserved.

2.12 Системный монитор



В этой вкладке можно посмотреть текущую загруженность процессора, использование физической памяти, температуру и загрузку каждой отдельной видеокарты. По умолчанию, интервал обновления составляет 3 секунды. Будьте внимательны, сбор этой статистики тоже отнимает процессорное время.

Copyright (c) 2024 Passcape Software. All rights reserved.

Работа с программой

3 Работа с программой

3.1 Атаки

В настоящее время, программа использует разные подходы для подбора паролей:

Preliminary attack - предварительная атака (впервые разработана в Passcape Software) представляет собой набор из небольших и быстрых мини атак. Часто предварительная атака запускается, для угадывания простых паролей, если невозможно мгновенное восстановление пароля, а запускать полную атаку (например перебором или по словарю) нет необходимости.

Artificial Intelligence attack - уникальная атака, тоже разработанная в Passcape Software и основанная на методе социальной инженерии. С помощью интеллектуальной атаки можно восстанавливать некоторые пароли, не прибегая к долгим и мучительным вычислениям.

Dictionary attack. Атака по словарю - до сих пор является достаточно эффективным методом восстановления, при котором программа пробует каждое слово из заданного словаря/словарей до тех пор, пока не будет найден искомый пароль или не кончатся слова в списке. Это метод эффективен, потому что многие люди в качестве пароля используют обычные слова. Атака по словарю осуществляется достаточно быстро по сравнению, например, с атакой полным перебором. Дополнительные словари можно скачать с нашего сайта или заказать для доставке на CD.

Brute-force attack. Атака перебором. Одна из немногих атак, гарантирующих восстановления оригинального пароля, при которой используются все возможные комбинации из заданного диапазона символов. Например, для трёхсимвольного диапазона малых латинских символов подбираются все возможные комбинации: 'aaa', 'aab', 'aac'... 'zzz'. Этот тип атак самый медленный. К тому же можно легко ошибиться с выбором оптимального диапазона символов.

Mask attack. Атака по маске является вариацией атаки перебором, за тем лишь исключением, что некоторые символы для нахождения пароля остаются неизменными, а меняется только определённая часть пароля. Эта атака полезна лишь тогда, когда известна какая-нибудь информация об искомом пароле. Например, первые четыре символа в пароле латинские буквы, за которыми следует трёхзначное число. Для задания маски или правила нахождения пароля, используется специально разработанный синтаксис.

Base-word attack (впервые разработана в Passcape Software). На первый взгляд, этот тип атаки похож на предыдущий. Она также эффективна, если известна часть пароля или его составляющая. Но, в отличие от атаки по маске, тут нет необходимости задавать маску, только базовое слово или фразу, если хотите. Все остальное программа берет на себя. Атака по фразе основана на опыте социальной инженерии и использует более 150 правил модификации исходного словосочетания для нахождения большого количества возможных парольных комбинаций.

Combined dictionary attack (впервые разработана в Passcape Software). Комбинированная атака по словарю специально сделана для восстановления паролей, состоящих из нескольких слов. Например, 'nothing to do' или 'ничегонескажу'. Необходимо задать один или несколько словарей, из которых программа, следуя определенным правилам мутации, будет составлять фразы, используемые для нахождения оригинального пароля. Правила создания фраз можно добавлять и редактировать самостоятельно.

Phrase attack (впервые разработана в Passcape Software). Атака по фразе обычно используется для нахождения сложных паролей, состоящих из нескольких слов, используя специальные

Copyright (c) 2024 Passcape Software. All rights reserved.

наборы словарей с фразами и словосочетаниями. Данные словари можно скачать только с нашего сайта.

Fingerprint Attack. Впервые разработана в Passcape Software. Данная атака похоже на комбинированную атаку по словарям, только для поиска паролей используются не слова, а предварительно сгенерированные "отпечатки" слов и найденных в процессе атаки паролей. Довольно эффективна для поиска сложных паролей.

Hybrid dictionary attack это разновидность словарной атаки, позволяющая пользователю задавать свои собственные правила мутации (изменения) слов в словаре и проверять их в качестве исходного пароля.

Batch attack (впервые разработана в Passcape Software). Во время групповой атаки создаётся список из последовательно выполняющихся стационарных атак, так, чтобы в последствие запускать все эти атаки одним щелчком, а не настраивать каждый раз по-отдельности.

Гарантированное восстановление - поиск коллизии пароля. Эта атака гарантированно находит альтернативный пароль, который может отрыть документ с 40-битным ключом шифрования.

3.2 Сравнительная Таблица Атак

Какая атака наиболее оптимальная? Как выбрать атаку? Ответы на эти вопросы должна дать сравнительная таблица атак.

Атака	Описание	Время работы	Гарантия	За	Против	Ограничения
Предварительная	Набор из нескольких мелких и быстрых мини-атак, предназначенных для поиска простых, коротких или часто встречающихся комбинаций	Несколько минут	нет	Хороший инструмент для быстрого обнаружения часто встречающихся, простых, коротких паролей, клавиатурных комбинаций, повторяющихся последовательностей и т.д. Удобна для быстрого поиска слабых паролей	Практически бесполезна для серьёзного анализа, при поиске большинства сложных паролей	Находит только простые пароли
Интеллектуальная	Наиболее продвинутый метод поиска паролей, основанный на методах социальной инженерии. Атака должна проходить на	Min: 5-6 минуты Max: несколько дней	нет	Лучший инструмент для поиска сложных паролей, с которыми другие методы справиться не могут. Хорошо срабатывает для паролей, слов и комбинаций, которые когда-либо сохранял	При наиболее эффективном анализе, когда все опции выставлены по-максимуму, атака занимает значительное время. Находятся не все пароли.	Эффективна только при запуске на оригинальной системе (откуда были взяты пароли)

Copyright (c) 2024 Passcape Software. All rights reserved.

	той же системе, откуда были взяты пароли			пользователь в своей системе		
Полным перебором	Перебор всех возможных комбинаций из заданного набора символов	Минимум - несколько дней	да	Единственная атака (наряду с атакой по маске), которая гарантированно восстанавливает полностью неизвестный пароль.	Перебор длинных паролей занимает нереально много времени. Сложно угадать правильный диапазон перебираемых символов	Может занять века для перебора даже простых паролей. Не находит пароли, если неправильно задан набор символов.
Словарная	Поиск паролей путём последовательного перебора слов из готовых словарей (списков слов)	Пара минут	нет	Хороший и быстрый инструмент для обнаружения часто встречающихся паролей	Требуется наличие хороших словарей, не учитывает особенности языка и регистра букв	Находит только часто употребляемые пароли
Словарная с мутациями	Аналогично словарной атаке, но каждое слово из словаря подвергается всевозможным мутациям. Например, добавлению цифр в конец слова, изменению регистра букв, уродованию (подмены) букв и т.д.	Вплоть до 1000000 раз медленнее простой атаки по словарю	нет	Хороша для всевозможных вариаций часто встречающихся паролей	Максимальная (наиболее эффективная) мутация занимает значительное время	Не находит сложные (не словарные) пароли, мутация занимает значительное время
По маске	Поиск паролей по заданной маске (правилу, по которому создаются пароли)	Зависит от выбранных опций	да	Гарантированно восстанавливает оставшуюся часть пароля. Хороший вариант, если известна часть оригинального пароля	Требуется точно знать известную часть пароля, его длину и указать правильный набор символов для перебора	Пароль не найдётся если неправильно задан набор символов, длина пароля или неправильно задана

Copyright (c) 2024 Passcape Software. All rights reserved.

						известная часть исходного пароля
Комбинированная	Проверка сложных паролей (в основе которых два или более слов) путём склейки слов из нескольких словарей	Зависит от выбранных опций	нет	Находит длинные и сложные пароли	Ограниченный набор специализированных словарей. Если задан большой исходный словарь, то атака может занять длительное время	Требуется заранее знать, что в основе искомого пароля лежат два или более слов, довольно медленная.
Комбинированная с мутациями	Аналогично комбинированной атаке, но с мутациями	Зависит от выбранных опций	нет	Аналогично простой комбинированной атаке	Аналогично простой комбинированной атаке. Требуется задать дополнительные правила мутации создаваемых паролей	Аналогично простой комбинированной атаке. Мутации требуют много времени
По ключевому слову	Атака основанная на том факте, что известно базовое слово, на основе которого был создан пароль	Обычно, несколько минут (если длина базового слова меньше 16)	нет	Хороша в том случае, если вы знали оригинальный пароль, но забыли его вариации (например, регистр букв или цифры на конце слова)	Мутация для длинных паролей (более 16 символов) может занять много времени.	Не всегда срабатывает
По фразе	Аналогична словарной атаке, но в основе проверки лежит не слово, а фраза, крылатое выражение, отрывки из песен, книг и т.д.	От нескольких минут до нескольких дней	нет	Единственная способ восстановить пароли, созданные из фраз.	Фразы в качестве паролей использует небольшой процент пользователей. Мутация фраз несовершенна, мутация и анализ занимают значительное время. Недостаточно соответствующих словарей.	Ограниченный набор мутаций. Сложность в создании специализированных словарей, может занять много времени.
Идентификационная атака	Атака на основе предварительно	От нескольк	нет	Находит сложные пароли, которые	Большие словари генерируют такое	Требует очень много

Copyright (c) 2024 Passcape Software. All rights reserved.

	сгенерированных отпечатков слов из исходного словаря	их минут до бесконечности, в зависимости от размера исходного словаря		невозможно подобрать в других атаках	кол-во отпечатков, которое сложно обработать за разумное время. Успех сильно зависит от качества исходного словаря.	времени, если задать даже небольшой словарь
Гибридная по словарю	Аналогично словарной атаке, но каждое слово из словаря подвергается мутациям, которые задаёт пользователь. Например, можно добавить цифру в конец слова, изменить регистр букв и т.д.	Зависит от количества правил мутаций и размера словаря. Как правило, несколько часов на небольшой словарь.	нет	Хороша для всевозможных вариаций часто встречающихся паролей	Создание своих собственных правил долгое и нудное занятие.	Не находит сложные (не словарные) пароли

3.3 GPU FAQ

В: Какие системные требования имеет программа?
О: В настоящее время, программа работает с видеокартами NVidia, имеющими поддержку технологии CUDA 3.0 и видео картами AMD, начиная с серии Radeon 7xxx. Полный список CUDA-поддерживаемых устройств можно найти по адресу developer.nvidia.com/cuda-gpus. Совместимые карты AMD/ATI показаны на сайте википедии. Кроме того, необходимо, чтобы были установлены самые свежие драйвера.

В: Программа не видит все мои видео карты. Что делать?
О: Обновить драйвера. Если это не помогло, расширьте рабочий стол на все устройства (известный глюк Vista). Попробуйте также воткнуть одно из GPU устройств в другой PCI-Express слот.

В: Как узнать какую архитектуру поддерживает моя видео карта?
О: Для видео карт NVidia: Запустите программу, откройте меню **Options** - **General Options**, вкладку GPU Settings, платформу '**NVidia CUDA**' и выберите видео карту. Внизу в описании основных параметров найдите поле '**Compute capability**'.

Copyright (c) 2024 Passcape Software. All rights reserved.

Для AMD: Откройте меню **Options** - **General Options**, вкладку GPU Settings, платформу '**AMD OpenCL**' и выберите видео карту. Внизу в описании основных параметров найдите поля 'CL_DEVICE_VERSION' and 'CL_DEVICE_OPENCL_C_VERSION'.

В: Где скачать последние версии драйверов?
О: Загрузить последние драйверы с поддержкой CUDA можно с nvidia.ru/drivers, для AMD карт - support.amd.com/us/gpudownload/Pages/index.aspx.

В: Где подробнее почитать о CUDA?
О: Подробнее о этой технологии можно почитать на сайте Википедии.

В: Где подробнее почитать о картах AMD/ATI Radeon?
О: wikipedia.org/wiki/Comparison_of_AMD_graphics_processing_units

Q: Какие версии Windows поддерживаются?
A: Поддержка перебора на видеокартах NVidia осуществляется в ОС Windows начиная с Windows XP, для видеокарт AMD Radeon требуется Windows Vista. Поддерживаются 32- и 64-битные системы.

В: При запуске GPU атаки через некоторое время компьютер зависает или возникает "синий экран смерти" (BSOD). Что это может быть?
О: Как правило, такая ситуация может возникнуть по нескольким причинам:

- Видео карта была разогнана, поэтому при максимальной нагрузке происходит сбой. В этом случае рекомендуется вернуть частоты памяти и ядра в их первоначальные значения.
- Ненадлежащее охлаждение видео карты. При запуске GPU атаки, программа задействует GPU процессор на полною мощность, что приводит к критическому повышению его температуры. Убедитесь, что ваша видео карта надёжно и качественно охлаждается, GPU слот в системном блоке и сам системный блок очищен от грязи и пыли. Неразумное использование определённых настроек видео карт может негативно влиять на температуру и стабильность их работы. Например, некоторые программы для снижения шума видео карт уменьшают частоту вращения вентилятора системы охлаждения, что приводит к уменьшению шума, но одновременно увеличивается рабочая температура.
- Проблемы с питанием. При полной загрузке видео карта потребляет много энергии и ваш блок питания может не выдержать такую нагрузку. Если на GPU имеются разъёмы для подключения дополнительного питания, убедитесь что все они подключены.
- Ещё одна потенциальная причина - установленный лимит на выполнение GPU кернела (GPU kernel execution timeout). При первом обращении к GPU программа предложит вам изменить эти настройки. В противном случае, необходимо настроить параметры WDDM самостоятельно. Например, можно вообще отключить таймаут на исполнение кода GPU.

В: Как влияет на производительность работы программы шина PCI-Express?
О: По сути, это влияние ничтожно и нивелируется другими факторами. Это касается и поколения, и скорости работы PCI-Express.

В: Влияет ли количество видео памяти на производительность?
О: Нет не влияет. Однако в большинстве случаев, видеокарта должна иметь как минимум 256 Мб видео памяти.

В: Какое максимальное количество устройств поддерживается программой?
О: Это зависит от вашего железа. Обычно в 4х-слотовую материнскую плату можно установить до 8 устройств (4 двойные GPU карты). Программно поддерживается до 255 GPU устройств.

В: После запуска GPU атаки, на экране жуткие тормоза. Как от них избавиться?

Copyright (c) 2024 Passcape Software. All rights reserved.

О: Установите в системный блок вторую видео карту, если на материнской плате есть дополнительный разъем и позволяет мощность блока питания. Например, в качестве основной видео карты (для вывода на дисплей) можно использовать любую дешёвую видео карточку. Тогда как вторую, более мощную, можно использовать чисто для перебора паролей.

В: В моей системе несколько видео карт. Могу ли я использовать их все для перебора?
О: Да. Все или некоторые из них. Используемые программой GPU устройства задаются в общих настройках.

В: Могу ли я одновременно брутить на нескольких видео картах с различной производительностью? Например NVidia GT 8600 и AMD Radeon HD 7970?
О: Да.

В: Программа не видит все устройства. Что делать?
О: Необходимо отключить SLI для использования всех устройств.

В: Могу ли я использовать одновременно NVidia и ATI видео карты?
О: Да, можете.

В: Как мне проверить загрузку видео карты?
О: Откройте вкладку '**Hardware Monitor**', в поле '**What to show**' выберите ваш девайс и установите его свойства '**Show**' для отображения в программе. После этого можно, используя кнопки '**Start**' и '**Stop**', управлять мониторингом выбранных устройств. GPU монитор показывает утилизацию (загрузку) видеопроцессора, его температуру и скорость вентилятора.

В: Моя карта NVidia не показывается в системном мониторе. Что делать?
О: Необходимо установить/переустановить библиотеку NVAPI, доступную на сайте https://developer.nvidia.com/nvapi

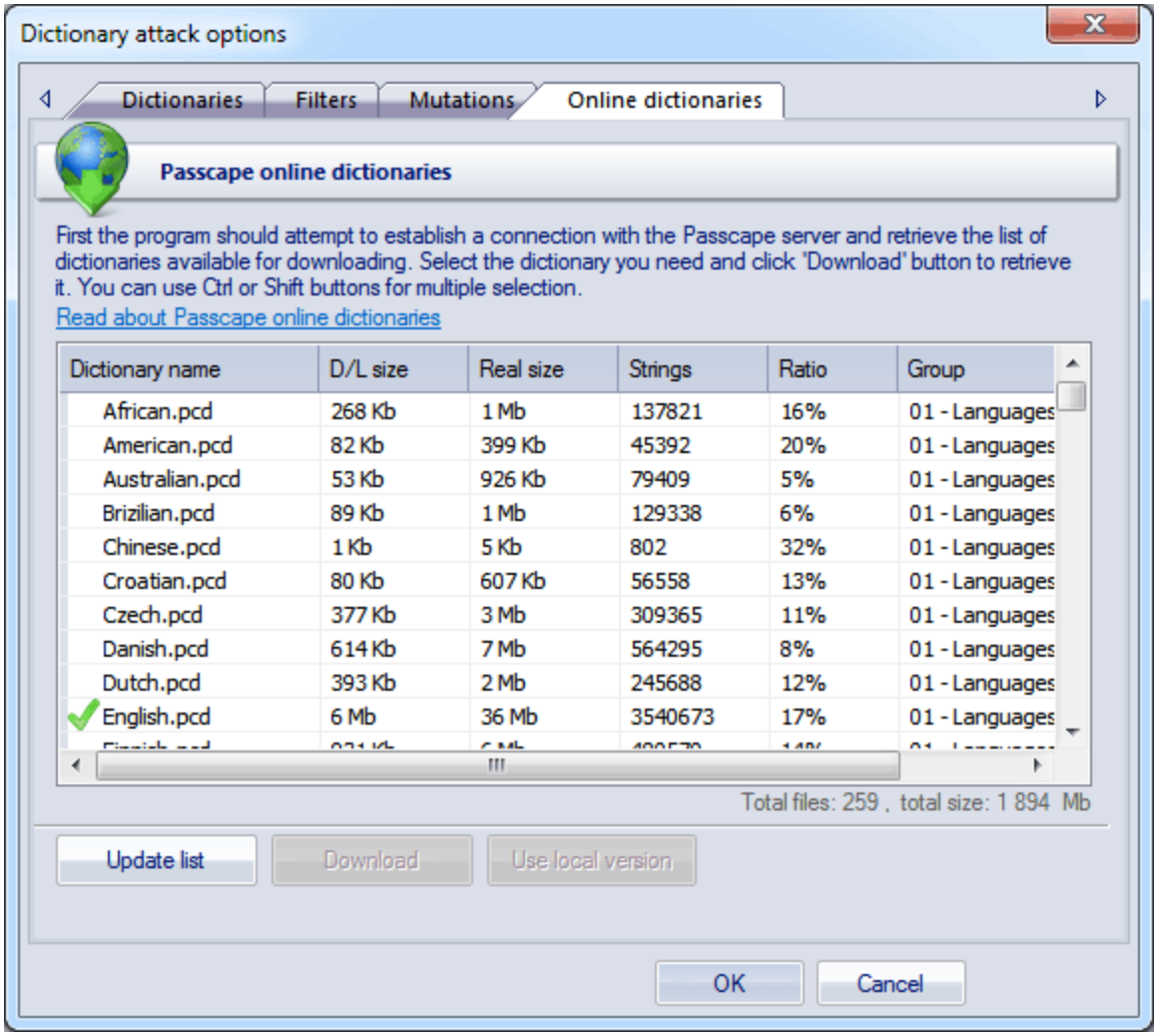
В: Видеокарта AMD Radeon не показывает значения температуры и загрузки GPU в системном мониторе.
О: Необходимо переустановить драйвера видеокарты или отдельно компонент ADL. После успешной переустановки убедитесь, что загрузка и температура GPU корректно отображается и в других программах мониторинга. Например, в Catalyst.

В: Скорость расшифровки паролей намного ниже ожидаемой.
О: В идеале, на каждое графическое ядро должно приходиться свободное ядро процессора. В противном случае, скорость перебора может значительно упасть. Можно также попробовать полностью отключить использование CPU: меню *Options - General Options - CPU Settings*, выставите в поле *Processor Utilization* **0**.

В: Жуткие лаги при бруте паролей к документам PowerPoint 2013 на видеокартах.
О: Это происходит из-за того, что скорость обработки одного блока паролей ниже скорости обновления данных. Т.е. иногда программа может показывать скорость 0 п/с потому что за время обновления (по-умолчанию 3 секунды) очередной блок паролей ещё не был просчитан на видеокарте. При переборе на процессоре этого не происходит, потому что в отличие от GPU, где просчет идет блоками, пароли проверяются последовательно, по одному.

Copyright (c) 2024 Passcape Software. All rights reserved.

3.4 Загрузка Онлайн Словарей



Диалог выбора онлайн словарей чрезвычайно прост в использовании. При его открытии, программа попытается установить связь с сервером Passcape Software, затем скачивает и отображает список доступных для загрузки словарей. Некоторые словари, отмеченные серым цветом, недоступны в демонстрационной версии программы.

Для удобства, можно сортировать список по алфавиту, размеру исходного или сжатого файла, по группе, к которой он принадлежит, и т.д.

Выберите необходимый вам словарь и нажмите кнопку <скачать>, чтобы загрузить и использовать его в программе.

Некоторые словари имеют очень большой размер. Например, размер 'music_songs.pcd' составляет более 59 Мб в сжатом виде. Естественно, для загрузки такого большого объёма информации, может потребоваться некоторое время, которое зависит от скорости работы вашего интернет канала.

Copyright (c) 2024 Passcape Software. All rights reserved.

Все онлайн (а также некоторые дополнительные) словари можно заказать для доставки на CD. Общий объем всех словарей составляет более 10 Гб. Вы также можете поделиться с нами своим собственным словарём, прислав его, или ссылку на него на наш электронный адрес.

Copyright (c) 2024 Passcape Software. All rights reserved.

Лицензия и регистрация

4 Лицензия и регистрация

4.1 Лицензионное соглашение

==========
SOFTWARE LICENSE AGREEMENT
==========

IMPORTANT-READ CAREFULLY: This is the End User License Agreement (the "Agreement") is a legal agreement between you, the end-user, and Passcape Software, the manufacturer and the copyright owner, for the use of the "PowerPoint Password Recovery" software product ("SOFTWARE").

All copyrights to SOFTWARE are exclusively owned by Passcape Software.

The SOFTWARE and any documentation included in the distribution package are protected by national copyright laws and international treaties. Any unauthorized use of the SOFTWARE shall result in immediate and automatic termination of this license and may result in criminal and/or civil prosecution.

You are granted a non-exclusive license to use the SOFTWARE as set forth herein.

You can use trial version of SOFTWARE as long as you want, but to access all functions you must purchase the fully functional version. Upon payment we provide the registration code to you.

Once registered, the user is granted a non-exclusive license to use the SOFTWARE on one computer at a time (for every single-user license purchased).

With the personal license, you can use the SOFTWARE as set forth in this Agreement for non-commercial purposes in non-business, non-commercial environment. To use the SOFTWARE in a corporate, government or business environment, you should purchase a business license. With the business license you can run the SOFTWARE on multiple computers belonging to your organization - no matter where they are located.

The registered SOFTWARE may not be rented or leased, but may be permanently transferred together with the accompanying documentation, if the person receiving it agrees to terms of this license. If the software is an update, the transfer must include the update and all previous versions.

You may not create any copy of the SOFTWARE. You can make one (1) copy the SOFTWARE for backup and archival purposes, provided, however, that the original and each copy is kept in your possession or control, and that your use of the SOFTWARE does not exceed that which is allowed in this Agreement.

The SOFTWARE unregistered (trial) version may be freely distributed, provided that the distribution package is not modified. No person or company may charge a fee for the distribution of the SOFTWARE without written permission from the copyright holder.

You agree not modify, decompile, disassemble, otherwise reverse engineer the SOFTWARE, unless such activity is expressly permitted by applicable law.

Passcape Software does not warrant that the software is fit for any particular purpose. Passcape Software disclaims all other warranties with respect to the SOFTWARE, either express or implied. Some jurisdictions do not allow the exclusion of implied warranties or limitations on how long an implied warranty may last, do the above limitations or exclusions may not apply to you.

Copyright (c) 2024 Passcape Software. All rights reserved.

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.

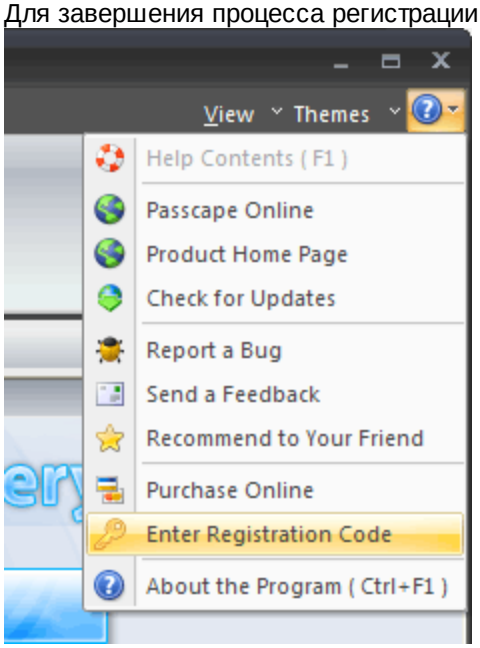
All rights not expressly granted here are reserved by Passcape Software.

4.2 Регистрация

На странице покупки программы можно ознакомиться с подробной инструкцией о процессе покупки, формах оплаты и т.д. Для русскоязычных пользователей имеется возможность оплаты через WebMoney. Интернет заказы обычно обрабатываются в течение нескольких минут, по истечении которых на адрес вашей электронной почты будет выслано регистрационное письмо с кодом программы. Если, после произведения оплаты, вы не получили регистрационное письмо в течение одного-двух бизнес дней, обратитесь, пожалуйста, в службу поддержки.

Важно! При заполнении формы оплаты, убедитесь, что указали правильный адрес электронной почты, который не блокирует входящие письма. В противном случае вы будете не в состоянии получить регистрационное письмо.

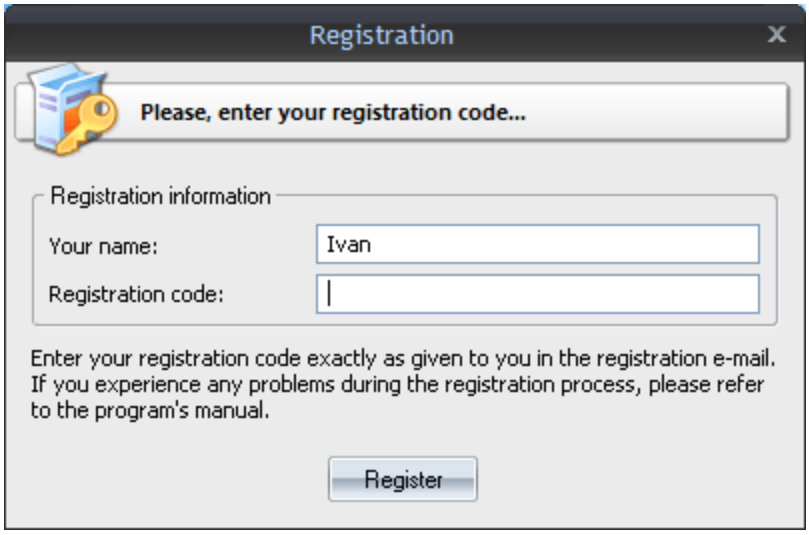
Для завершения процесса регистрации



- Откройте регистрационное письмо и скопируйте код в буфер обмена
- Запустите программу. Выберите меню **Help - Enter Registration Code**
- В появившемся диалоге введите или вставьте из буфера код программы и имя пользователя

Copyright (c) 2024 Passcape Software. All rights reserved.

- Нажмите кнопку **Register** для подтверждения регистрации.



4.3 Ограничения ДЕМО версии

Незарегистрированная версия **PowerPoint Password Recovery** показывает только первые три символа расшифровываемых паролей и имеет ряд других функциональных ограничений.

4.4 Редакции программы

Программа поставляется в двух редакциях: Standard и Professional. Ниже дано подробное описание ограничений для каждой редакции программы.

ВОЗМОЖНОСТЬ	Standard	Professional
Поддержка документов Microsoft PowerPoint 97 - 2021	+	+
Снятие защиты от редактирования контента и VBA макросов в документах PowerPoint 2007 и новее	+	+
Поддержка Windows XP - Windows 10	+	+
Поддержка 64-bit Windows	+	+
Поддержка многопоточности	+	+
Поддержка тем интерфейса	+	+
Поиск текстовых паролей	+	+
Экспорт найденных паролей в текстовый файл	+	+
Обычные атаки	+	+
Улучшенные атаки	+	+
Умные атаки	+	+

Copyright (c) 2024 Passcape Software. All rights reserved.

ВОЗМОЖНОСТЬ	Standard	Professional
Количество поддерживаемых CPU устройств	2	32
Количество поддерживаемых GPU устройств	1	255
Групповая атака	-	+
Просмотр кэша паролей AI	-	+
Создание словарей по маске	-	+
Создание словарей по ключевому слову	-	+
Создание комбинированных словарей	-	+
Создание фразовых словарей	-	+
Создание словарей на основе гибридной атаки	-	+
Создание словарей на основе простой словарной атаки	-	+
Создание словарей на основе идентификационной атаки	-	+
Возможность ограничивать доступ к программе	+	+
Инструмент измерения стойкости пароля	+	+
Загрузка Онлайн словарей	+	+
Ручная проверка паролей	+	+
Инструмент для открытия **** паролей	+	+
Утилиты для словарей: создание словаря индексацией файлов	-	+
Утилиты для словарей: слияние словарей	+	+
Утилиты для словарей: статистика словаря	+	+
Утилиты для словарей: сортировка	+	+
Утилиты для словарей: конвертирование/сжатие словарей	+	+
Утилиты для словарей: сравнение словарей	+	+
Утилиты для словарей: дополнительные операции	+	+
Утилиты для словарей: индексация слов/паролей на жестком диске ПК	-	+
Утилиты для словарей: поиск HTML ссылок	+	+
Гарантированный поиск коллизии пароля (для документов с 40-битным ключом шифрования)	+	+
Системный монитор	+	+
Отч`ты о паролях	-	+
Запуск в режиме невидимости	+	+
14-дневная гарантия возврата денег	+	+
Лицензия	персональная	бизнес

Copyright (c) 2024 Passcape Software. All rights reserved.

Техническая поддержка

5 Техническая поддержка

5.1 Ошибки и проблемы

Если вы обнаружили ошибку в работе программы, напишите письмо на support@passcape.com. Пожалуйста, укажите следующую информацию:

- Полное имя и версия программы
- Версия Windows, наличие привилегий администратора, сетевое окружение
- Регистрационная информация, если есть
- Подробное описание проблемы или ошибки, является ли проблема повторяющейся или спонтанной
- Если это возможно, вышлите скриншот, лог программы и файл **Crash.log**, если имеется.

5.2 Предложения

Если у вас имеются вопросы, комментарии или предложения по работе программы, присылайте их на адрес info@passcape.com. Пожалуйста, не забудьте упомянуть полное название программы и ее версию. Убедитесь также, что у вас установлена последняя версия.

5.3 Контакты

Вопросы по работе программы присылайте только после прочтения FAQ. Адрес тех. поддержки: support@passcape.com.
Мы ответим вам в течение одного-двух дней. Зарегистрированные пользователи имеют приоритет в технической поддержке.

По вопросам регистрации обращайтесь, пожалуйста, по следующему адресу: sales@passcape.com

Пишите на русском или английском языке!

Copyright (c) 2024 Passcape Software. All rights reserved.