Windows Password Recovery

Руководство пользователя

Passcape Software

Введение

1 Введение

1.1 О программе

Добро пожаловать в **Windows Password Recovery** - утилиту для анализа сетевой безопасности и восстановления паролей Windows. Windows Password Recovery является единственным программным решением, применяющим самые современные, запатентованные технологии восстановления паролей, разработанные программистами Passcape Software. Например, *Artificial Intelligence* или *Pass-phrase attack*.

Windows Password Recovery обладает рядом достоинств по сравнению с аналогичными продуктами:

Для домашних пользователей - проста и удобна в работе. Позволяет легко восстановить или сбросить забытый пароль любой учетной записи Windows.

Для системных администраторов - аудит паролей выявляет бреши в системе безопасности, помогая администраторам обеспечить надежность и защищенность корпоративной сети, осуществляя проверку уровня защиты операционных систем Windows.

Для экспертов безопасности, государственных и корпоративных структур - производится анализ и аудит политики безопасности системы, выработка рекомендаций по повышению устойчивости парольной защиты операционных систем.

1.2 Особенности и преимущества

- Современный, легко настраиваемый графический интерфейс
- Поддержка 14 различных форматов при загрузке хэшей
- Поддержка паролей NTLM и LM, кэшированных паролей домена, а также Windows PIN.
- Импорт напрямую из реестра или ntds.dit, причем если эти файлы заблокированы системой, программа прочитает и их
- Импорт хэшей с удаленной машины
- Импорт хэшей из теневых копий, точек восстановления, резервных копий реестра
- Импорт хэшей истории паролей
- Может сохранять текущий реестр и базу Active Directory.
- Расшифровка паролей некоторых учетных записей на лету (при локальном импорте)
- Поддержка Active Directory (доменных учетных записей)
- Поддержка учетных записей Microsoft и AzureAD
- Поддержка кэшированных паролей домена
- Поддержка импорта из 32- и 64-х битных систем
- Экспорт хэшей в файл PWDUMP
- Программа имеет в своем арсенале 18 видов различных атак, 10 из которых уникальны, созданные в нашей компании и использующиеся только в нашем программном обеспечении
- Программа поддерживает многопоточность, полностью задействуя возможности современных компьютеров.
- Атака по словарю поддерживает текстовые словари в формате ASCII, UNICODE,UTF8, PCD, RAR и ZIP.
- Большой выбор Онлайн словарей для словарных атак (около 2 Гб)

- Некоторые функции программы, например мутация слов, уникальны. Общее количество правил мутации переваливает за полторы сотни. Такого нет ни в одной аналогичной программе!
- Поддержка неограниченного количества перебираемых хэшей
- Интеллектуальный анализ найденных паролей
- Высокая скорость перебора на современных компьютерах - более 100 млн. п/с на четырехядерных процессорах и **миллиарды паролей в секунду** при использовании GPU.
- Имеются дополнительные инструменты для генерации хэшей, проверки стойкости пароля, создания радужных таблиц и др.
- Набор инструментов для работы со словарями: создание, сортировка, конвертация и др.
- Пополняемые модули расширенного анализа паролей системы: редактор LSA секретов, редактор кэшированных паролей домена, Active Directory и SAM, расшифровщик DPAPI
- Извлечение текстовых паролей из памяти, кэша Windows, из системы Windows Hello и т.п.
- Расширенный генератор отчетов

1.3 Системные требования

Требования
Windows XP или более новая ОС, около 100 Мб на жестком диске, 512 Мб RAM.
Для корректной работы некоторых функций программы, требуются привилегии администратора.
Для запуска GPU атак, требуется видеокарта с поддержкой CUDA 3.0. Видеокарты AMD поддерживаются начиная с 7xxx серии. Intel HD Graphics 4xxx и выше.

Совместимость
При запуске на старых операционных системах (Windows 2000), необходимо самостоятельно скопировать файл GDIPLUS.DLL в каталог программы. Для корректного перебора паролей на видеокартах NVidia требуется Windows XP, для видеокарт AMD Radeon - Windows Vista и выше.

Известные проблемы
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.

Интерфейс программы

2 Интерфейс программы

2.1 Общее описание

Интерфейс программы выполнен в виде Single Document Interface архитектуры, т.е. позволяет работать одновременно только с одним проектом. Работу программы можно условно разбить на 4 этапа:

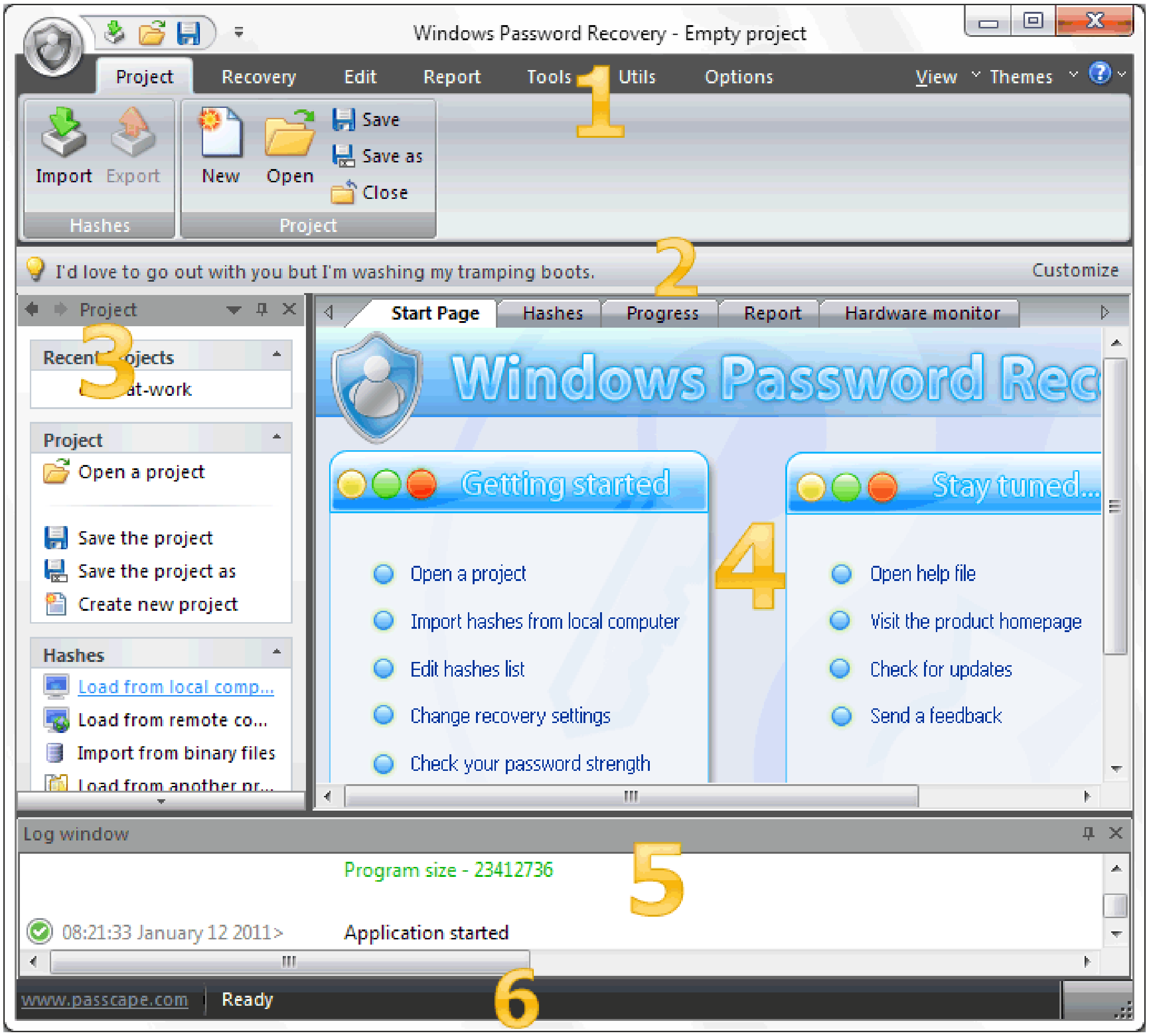
1. Создание проекта
2. Импорт (загрузка) хэшей паролей в проект. Редактирование хэшей: удаление, добавление, выбор и т.д.
3. Расшифровка хэшей. Включает в себя выбор, настройку и запуск выбранной атаки или нескольких атак.
4. Анализ полученных результатов.

Весь интерфейс условно можно разделить на несколько составляющих:

1. Меню программы
2. Information Bar - предназначена для вывода небольшой текстовой информации. Например, подсказок, предупреждений и пр.
3. Task Bar дублирует и дополняет основное меню для обеспечения быстрого доступа к некоторым операциям. Состоит из нескольких вкладок:

- Проект - содержит основные оперции с проектом. Например, открытие, закрытие, создание нового проекта, импорт хэшей.
- Редактирование хэшей. Дублирует наиболее частые операции редактирования.
- Инструменты - включает в себя часы, календарь и калькулятор.

4. Main Window - несет основную нагрузку и состоит из 5 частей. Первая вкладка - окно приветствия. Вторая вкладка содержит список хэшей для анализа и восстановления. Затем идет вкладка состояния (прогресса) текущей атаки и вкладка со статистикой/отчетами. И, наконец, системный монитор.
5. 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.
6. Status Bar - носит информационный характер.



I'd love to go out with you but I'm washing my tramping boots.

```
Program size - 23412736
08:21:33 January 12 2011>        Application started
```

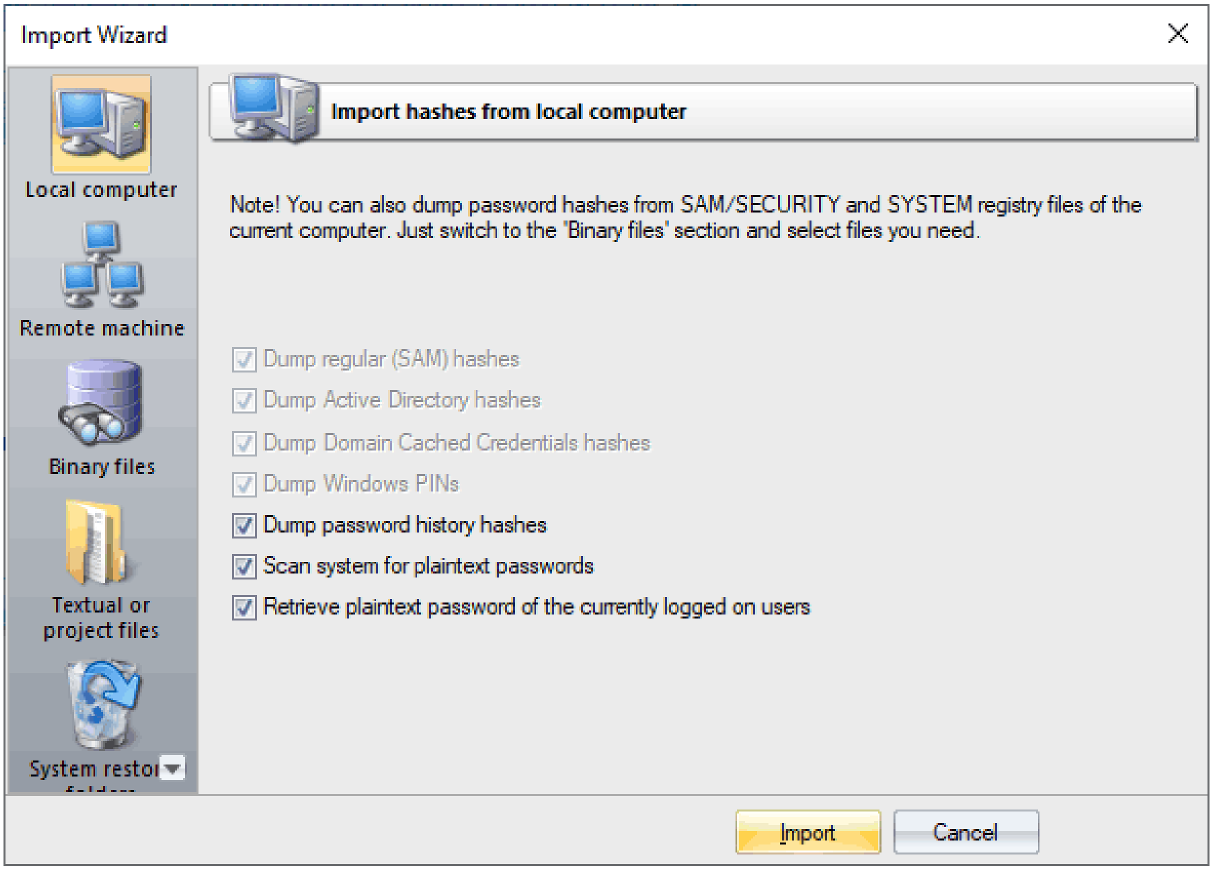
Ready

2.2 Меню Проект

2.2.1 Импорт

Windows Password Recovery предлагает широкий диапазон выбора способов загрузки хэшей в зависимости от ваших возможностей. Всего доступны несколько способов загрузки хэшей паролей в программу.

2.2.1.1 Импорт локальных хэшей



Note! You can also dump password hashes from SAM/SECURITY and SYSTEM registry files of the current computer. Just switch to the 'Binary files' section and select files you need.

☑ Dump regular (SAM) hashes
☑ Dump Active Directory hashes
☑ Dump Domain Cached Credentials hashes
☑ Dump Windows PINs
☑ Dump password history hashes
☑ Scan system for plaintext passwords
☑ Retrieve plaintext password of the currently logged on users

Импорт хэшей из локального компьютера - является наиболее предпочтительным методом, поскольку производится более глубокий анализ системы и паролей в целом. Кроме того, для импортируемых с локалького компьютера хэшей можно проводить продвинутую Интеллектуальную атаку, что позволяет относительно быстро восстанавливать пароли к некоторым учетным записям.

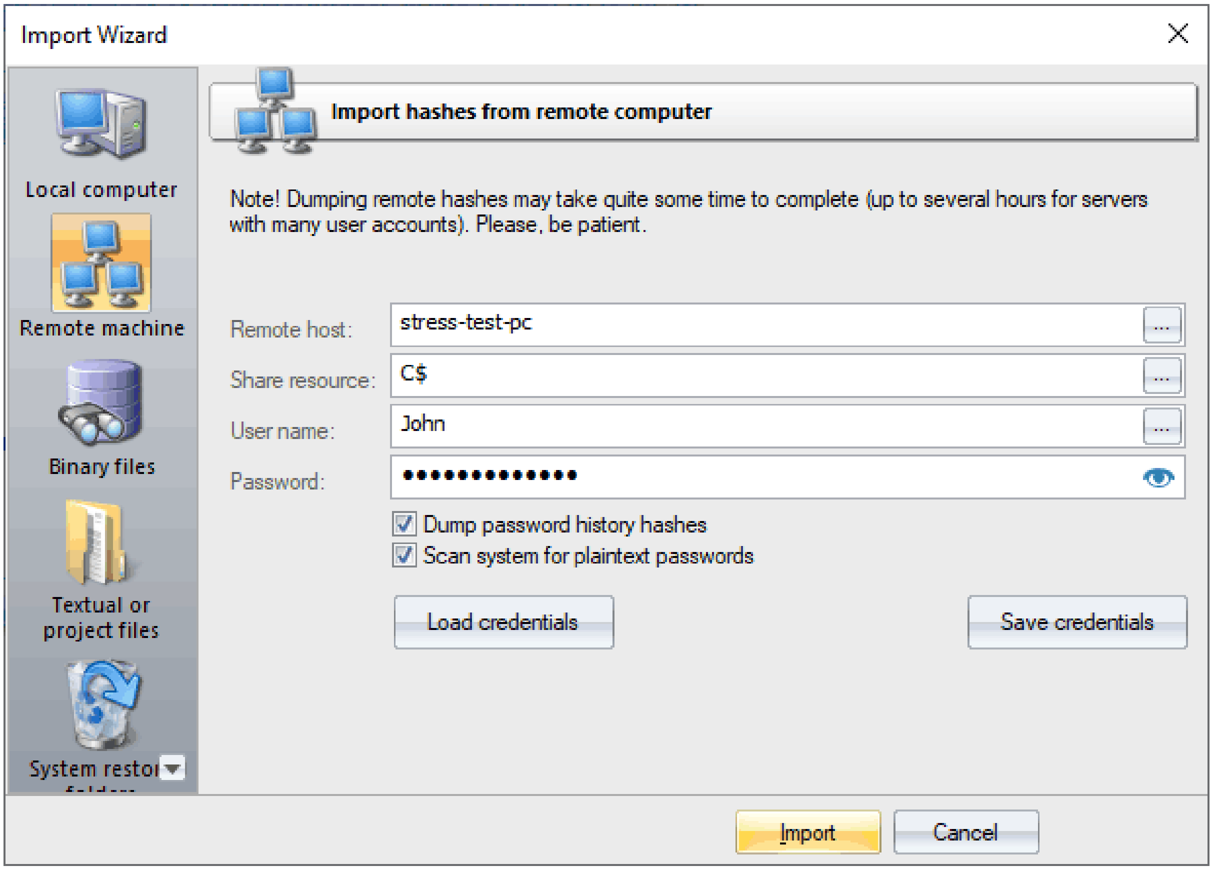
Импорт локальных хэшей работает независимо от того, где локализуются сами хэши: в SAM, SECURITY или в Active Directory. Данный пункт имеет три дополнительные опции: дамп хэшей истории паролей, поиск текстовых паролей, которые хранятся в системе и быстрая расшифровка паролей залогиненых пользователей. Процесс поиска plaintext паролей разбит на 4 части и состоит из непосредственно поиска паролей, которые хранятся в системе, используя обратное шифрование, поиска текстовых паролей системных учетных записей, поиска паролей автозагрузки и дополнительного шага, во время которого происходит анализ некоторых неохваченных учетных записей, пароли к которым также можно выковырять из системы (например, для учетной записи HomeGroupUser$ в Windows 7).

Если отключать опции поиска текстовых паролей нежелетельно, т.к. они позволяют относительно безболезненно и быстро вытаскивать готовые пароли к некоторым учетным записям, то дампом хэшей истории часто бывает полезно пренебречь. Например, если количество импортируемых паролей переваливает за сотни тысяч или даже миллионы. С другой стороны, программа имеет зачатки искусственного интеллекта, поэтому если во время атаки нашелся хотя бы один пароль истории, то она всеми способами попытается восстановить остальные, на основе анализа найденного пароля и предполагаемых предпочтений пользователя.

Одна из последних версий программы впервые в мире научилась вытаскивать хэши истории паролей из файла CREDHIST, поэтому рекомендуется устанавливать эту опцию в большинстве случаев.

Для работы локального импорта требуются привилегии администратора.

2.2.1.2 Импорт хэшей удаленного компьютера



Note! Dumping remote hashes may take quite some time to complete (up to several hours for servers with many user accounts). Please, be patient.

Remote host: stress-test-pc

Share resource: C$

User name: John

Password: ••••••••••••••

☑ Dump password history hashes

☑ Scan system for plaintext passwords

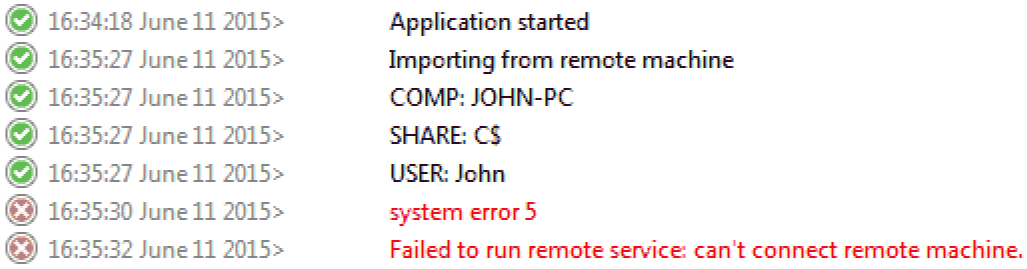
Импорт хэшей с удаленного компьютера. Программа имеет возможность дампа хэшей с удаленного компьютера не прибегая к помощи сторонних утилит. Это не компрометирует удаленную систему, поскольку для доступа к ней необходимы имя пользователя удаленной машины и его пароль.

Дамп с сетевой машины работает следующим образом. Сначала необходимо ввести имя удаленной машины в поле Remote Host. Можно воспользоваться кнопкой [...] для обзора сети. Затем, после того, как выбрали удаленный хост, следует установить ресурс общего доступа (с доступом на чтение и запись), через который будут передаваться данные. Обычно это C$ или ADMIN$. Можно также воспользоваться кнопкой обзора справа от поля ввода. Далее, в два нижних поля вводим имя учетной записи удаленного компьютера и пароль.

Кнопка Save Credentials предназначена для сохранения текущих настроек. Соответственно, с помощью Load Credentials можно загрузить сохраненные настройки, чтобы не вводить их каждый раз вручную. Пароль хранится в зашифрованом виде.

Этот пункт требует привилегий администратора на удаленном ПК!

Однако, иногда могут возникнуть трудности даже с учетной записью Администратора. При этом, при подключении к целевому ПК на базе Windows Vista/7/8/10 возникает следующая ошибка:



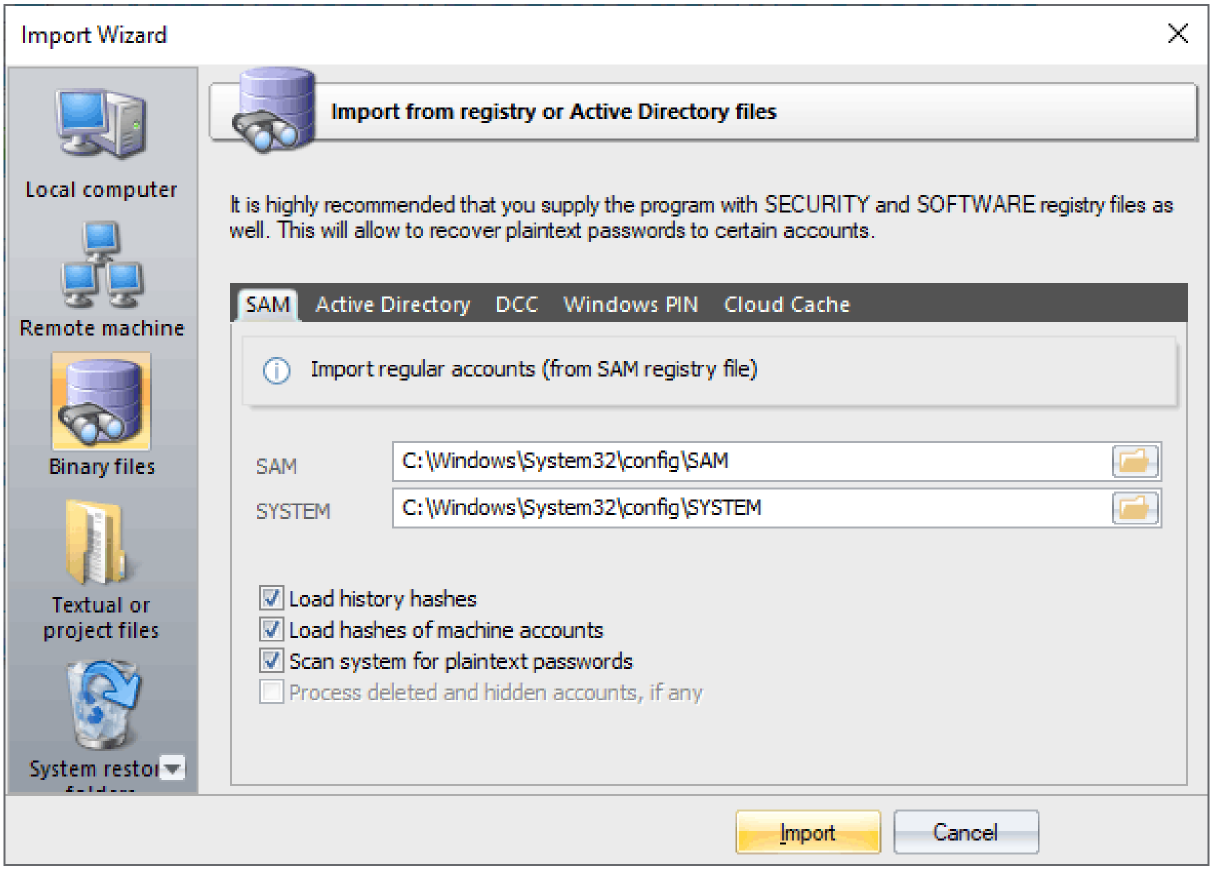
```
✓ 16:34:18 June 11 2015>        Application started
✓ 16:35:27 June 11 2015>        Importing from remote machine
✓ 16:35:27 June 11 2015>        COMP: JOHN-PC
✓ 16:35:27 June 11 2015>        SHARE: C$
✓ 16:35:27 June 11 2015>        USER: John
✗ 16:35:30 June 11 2015>        system error 5
✗ 16:35:32 June 11 2015>        Failed to run remote service: can't connect remote machine.
```

Ошибка номер 5 говорит о том, что доступ запрещен даже несмотря на то, что учетная запись имеет права Админа. Проблема в том, что любое удаленное подключение в Windows Vista и старших операционных системах по-умолчанию понижено в привилегиях и не может выполнять задачи, требующие привилегий Администратора. Документ Microsoft четко говорит об этом:

> *"When a user with an administrator account in a Windows Vista computer's local Security Accounts Manager (SAM) database remotely connects to a Windows Vista computer, the user has no elevation potential on the remote computer and cannot perform administrative tasks. If the user wants to administer the workstation with a SAM account, the user must interactively log on to the computer to be administered."*

Однако, в реестре Windows есть флаг, который позволяет отключить действие, применяемое по-умолчанию ко всем удаленным подключениям. Запустите редактор реестра на целевом ПК и откройте следующий куст:
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\system
Создайте DWORD ключ с именем *LocalAccountTokenFilterPolicy* и присвойте ему значение 1. После этого можно будет спокойно подключаться к любому расшаренному ресурсу.

2.2.1.3 Импорт хэшей из файлов реестра/AD



Import from registry or Active Directory files

It is highly recommended that you supply the program with SECURITY and SOFTWARE registry files as well. This will allow to recover plaintext passwords to certain accounts.

Import regular accounts (from SAM registry file)

SAM C:\Windows\System32\config\SAM

SYSTEM C:\Windows\System32\config\SYSTEM

☑ Load history hashes
☑ Load hashes of machine accounts
☑ Scan system for plaintext passwords
□ Process deleted and hidden accounts, if any

Импорт хэшей из бинарных файлов. Windows Password Recovery умеет вытаскивать хэши паролей напрямую из двоичных файлов. Причем даже из тех, что используются системой, т.е. из заблокированных.

Обычно хэши паролей хранятся в файле реестра SAM или SECURITY, которые располагаются в папке %WINDOWS%\System32\Config. В этом же каталоге находится и реестр SYSTEM, необходимый для расшифровки. Если вы указали путь к реестру текущей системы, то его обработка займет немного больше времени (обычно на несколько секунд).

Парольные хэши учетных записей домена хранятся в базе данных Active Directory, точнее в ее сердце - файле ntds.dit, который обычно лежит в следующем каталоге: %Windows%\ntds. Для расшифровки доменных учетных записей также потребуется файл реестра SYSTEM. Будьте внимательны! Если осуществляется дамп из базы данных AD текущей системы, то это может занять некоторое время, особенно если ntds.dit обладает большим размером.

Программа корректно работает и поддерживает все опции шифрования SYSKEY: Registry SYSKEY, SYSKEY startup diskette, SYSKEY startup password.

Если вы копируете файлы с другой операционной системы, то кроме файлов SAM (ntds.dit) и SYSTEM, крайне рекомендуется копировать также реестр SECURITY и SOFTWARE (они должны находиться в том же каталоге, что и SYSTEM), что позволит быстро расшифровать пароли некоторых ученых записей.

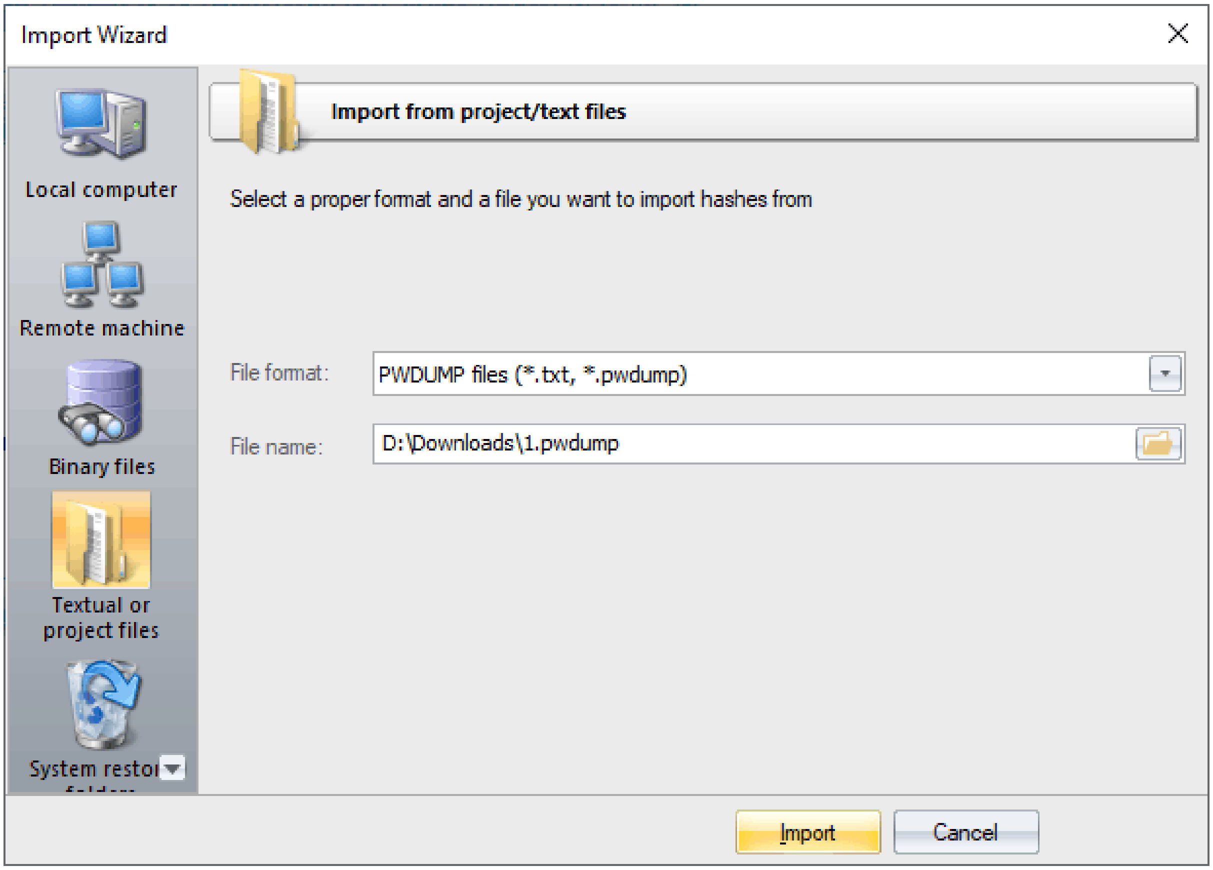
При импорте Windows PIN необходимо указать каталог Windows и папку с профилями пользователей (как правило, C:\Users). Программа сама выполнит поиск необходимых файлов.

Для загрузки кэшированных паролей учетных записей Microsoft или AzureAD, достаточно указать каталог Windows.

В одной из последних версий программы добавлены 4 расширенные опции загрузки хэшей:

1. Загружать/не загружать хэши истории паролей. С одной стороны, отключение загрузки хэшей истории может значительно сократить время обработки входных данных, не загружая ненужные записи. С другой стороны, если во время атаки будут найдены пароли к хэшам истории, это может значительно увеличить шанс угадывания пароля основой учетной записи.
2. Отказаться от загрузки системных учетных записей (имена которых оканчиваются символом $).
3. Отключить модуль поиска оригинальных текстовых паролей, ключей Bitlocker и другой приватной информации.
4. Искать спрятанные и удаленные учетные записи (только при чтении хэшей из Active Directory).

2.2.1.4 Импорт хэшей из других программ



Select a proper format and a file you want to import hashes from

File format: PWDUMP files (*.txt, *.pwdump)

File name: D:\Downloads\1.pwdump

И, наконец, загрузить хэши в проект можно импортировав их из других программ. Поддерживаются следующие форматы:

LM/NTLM хэши

- **PWDUMP** - несмотря на многие недостатки, являющийся стандартом де-факто в форматах хранения хэшей паролей. Важно знать, что этот формат не имеет полноценной поддержки национальных символов. Поэтому, имена пользователей или комментарии

могут отображаться некорректно. Windows Password Recovery поддерживает также текстовые PWDUMP файлы в формате UNICODE.
- **LophtCrack (*.lcs)** - данный формат файлов используется в программе LophtCrack. Windows Password Recovery поддерживает все версии LCS файлов, начиная с v4.
- **Файлы проектов *.hdt**, которые используются в программе Proactive Password Auditor (бывшая PWSEX) фирмы ElcomSoft. Поддерживаются все версии этого формата, начиная с v3.
- ***.hsh файлы**, которые экспортируются программой Proactive System Password Recovery той же небезызвестной фирмы.
- **Файлы хэшей *.lst**, создаваемые программой Cain & Abel. Windows Password Recovery поддерживает lst файлы начиная с версии v.4.9.12. В более ранних версиях LST файлов использовался разделитель ";" вместо "TAB". К сожалению, в самом LST нет маркера, указывающего на версию, поэтому если LST файл не читается, вам, возможно, придется вручную заменить все разделители полей на "TAB".
- ***.winpsw файлы**, создаваемые программой WinPassword, от старой доброй фирмы LastBit. Поддерживаются все версии WINPSW начиная с v6.
- **Файлы проектов SamInside (*.hashes)**. Данный формат похож на текстовый файл PWDUMP, но более гибок, а в качестве разделителя полей использует символ 0x7f вместо двоеточия, что более логично.
- **Файлы проектов InsidePro (*.hashes)**. Данный формат тоже похож на текстовый файл PWDUMP и используется в программе InsidePro.
- **Passcape Universal Configuration Files (*.puc)**. Данный контейнер используется в программе Reset Windows Password и может содержать несколько различных дампов.
- **Просто хэши (*.*).** Обычные хэши в текстовом формате, без разделителей (длина каждой строки 32 или 16 символов).

<u>Кэшированные доменные записи</u>

- **Passcape export/import files (*.peif)**. Этот формат может быть использован для чтения кэшированных записей домена. Формат поддерживается в некоторых программах Passcape software. Например, в Network Password Recovery.
- **Elcomsoft PSPR files (*.dcc)**. Текстовые файлы с кэшированными записями домена.
- **CACHEDUMP files (*.txt or *.cachedump)**. Стандартный агрегатор для хэшей DCC тип 1. Этот формат устарел и содержит несколько ошибок.
- **John The Ripper DCC2 files (*.txt).** Текстовые файлы хэшей DCC тип 2 в формате программы John The Ripper.

<u>Windows Hello PIN</u>

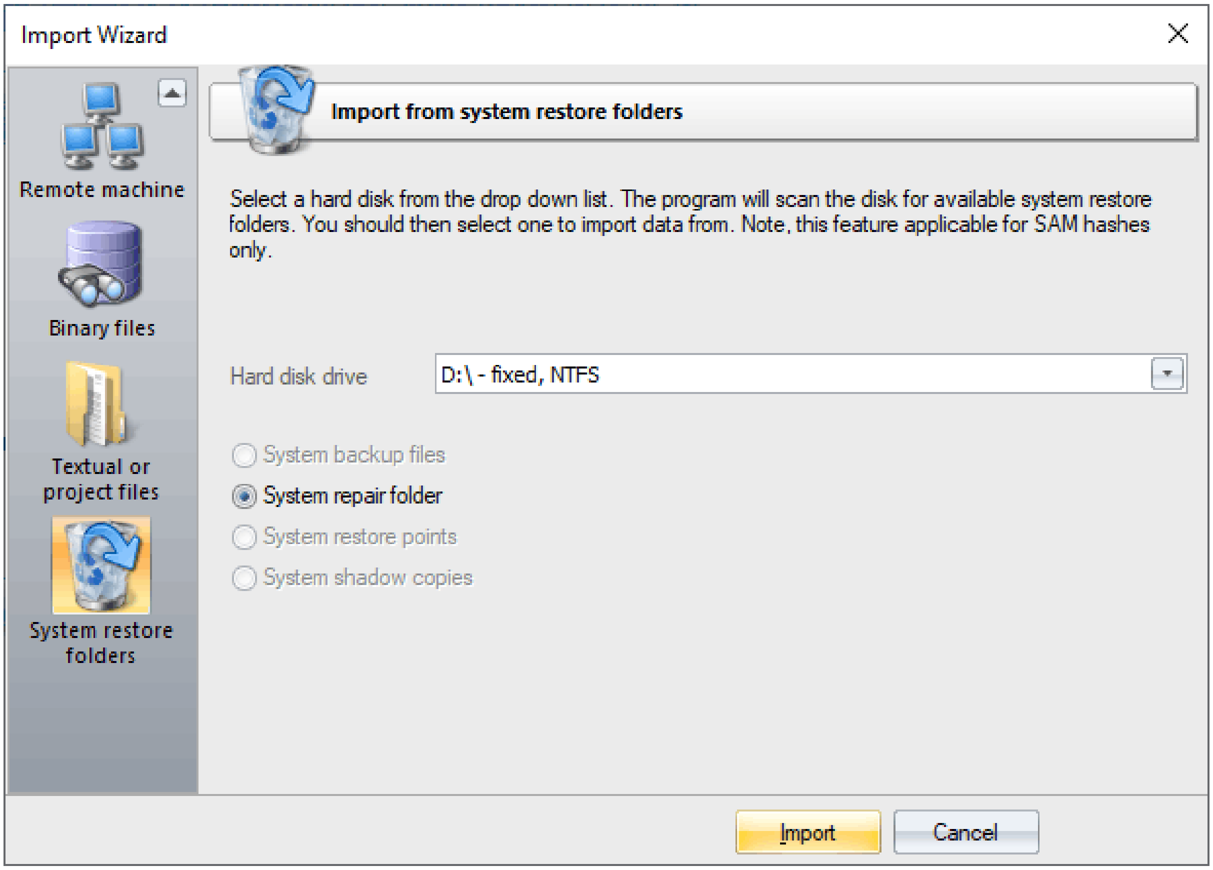
- **Hashcat/Elcomsoft/JtR хэши**, текстовые файлы (обычно с расширением *.pin или *.txt), в которых находятся хэши Windows PIN. Будьте осторожны, этот формат содержит приватные мастер ключи, которые могут скомпрометировать безопасность пользователя.

<u>Все доступные хэши</u>

- **Файлы резервных копий Reset Windows Password**, которые содержат все необходимые файлы для загрузки хэшей SAM, Active Directory, кэшированных паролей домена и Windows PIN, а также некоторые дополнительные данные, участвующие в мгновенной расшифровки этих хэшей. <u>Утилита для поиска и резервного копирования паролей и файлов</u> доступна в бесплатной редакции программы <u>Reset Windows Password</u>.

После импорта хэшей программа автоматически отмечает все загруженные хэши и запускает предварительную атаку. Данное действие опционально и может отключаться из общих настроек. По умолчанию эта опция включена.

2.2.1.5 Импорт хэшей из каталогов восстановления



Import from system restore folders

Select a hard disk from the drop down list. The program will scan the disk for available system restore folders. You should then select one to import data from. Note, this feature applicable for SAM hashes only.

Hard disk drive: D:\ - fixed, NTFS

○ System backup files
● System repair folder
○ System restore points
○ System shadow copies

Другая не менее полезная опция - это импорт хэшей из каталогов восстановления системы. Все, что вам необходимо сделать, это указать путь к одному из дисков. Программа автоматически выполнит поиск каталогов восстановления и, если обнаружит необходимые файлы, выполнит импорт хэшей.

Поиск производится:
Во-первых, в системном каталоге.
Во-вторых, в каталоге %Windows%\Repair, содержащем резервные копии реестра системы.
В-третьих, в каталоге System Volume Information, который используется для отката сделанных в системе изменений.

Корректный импорт хэшей из System Shadow доступен начиная с Windows VIsta. В Windows XP и 2003 используются анализ точек восстановления системы (restore points).

Будьте осторожны, резервные копии файлов реестра могут содержать устаревшие данные!

2.2.2 Экспорт

Все хэши проекта вместе с настройками хранятся в файле проекта (*.wpr), однако для большей гибкости и обеспечении совместимости с другими программами предусмотрена возможность сохранить хэши паролей в PWDUMP или POT файл. Если выбран пункт 'Экспорт в POT файл', то все найденные пароли с соответствующими хэшами (кроме LM) будут сохранены в файл в следующем формате:

хэш:пароль

Если при нажатии на кнопку 'Экспорт в POT файл' удерживается клавиша SHIFT, то выходной формат данных принимает такой вид:
пользователь (rid):пароль

Кодировка паролей - UTF8.

2.2.3 Новый

Сохранение текущего проекта и создание нового.

2.2.4 Открыть

Загрузка/открытие сохраненного ранее проекта. Проекты программы имеют расширение *.wpr и содержат настройки программы и хэши. 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

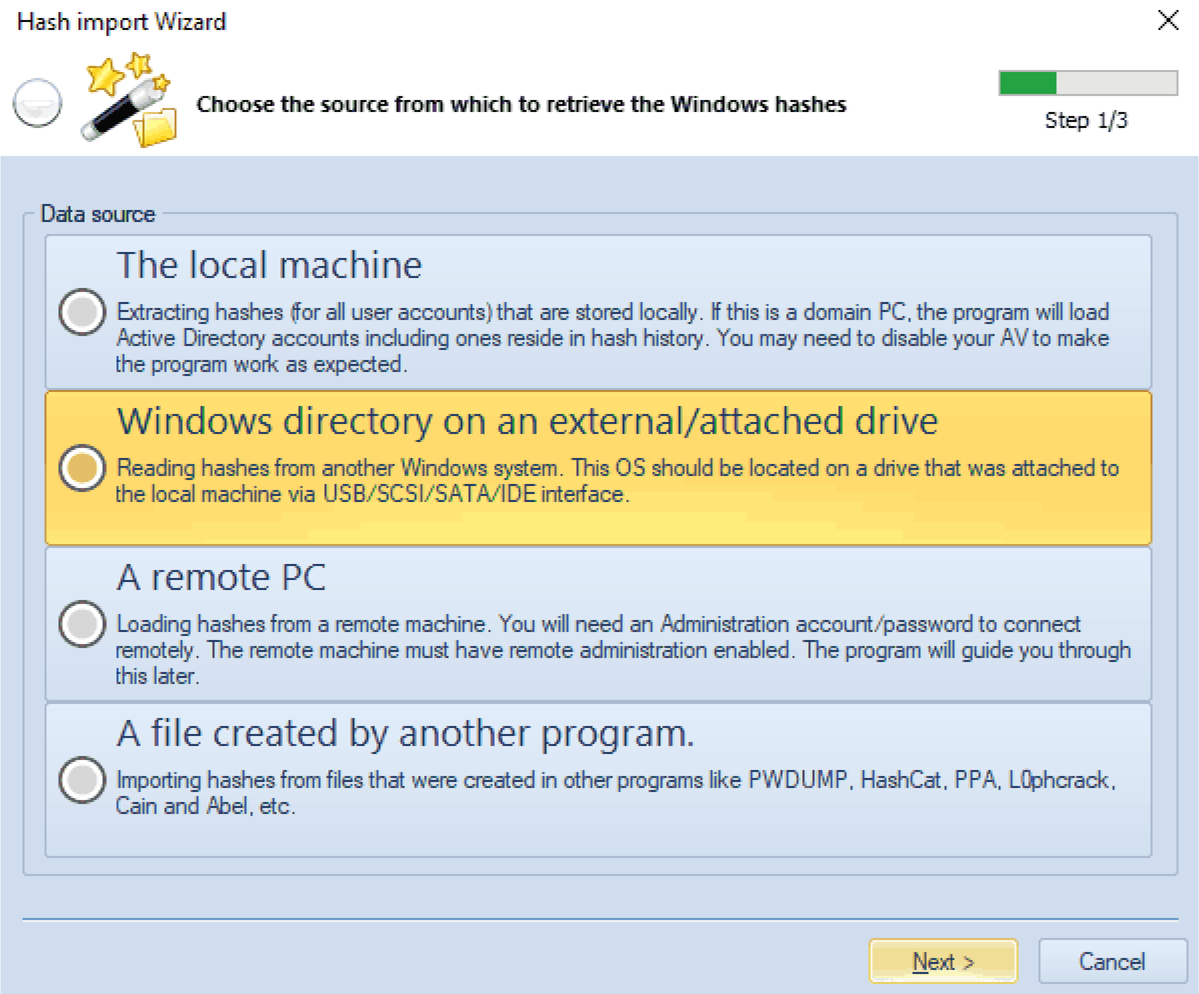
Сохранение текущего проекта под другим именем (переименование).

2.2.7 Закрыть

Закрыть текущий проект.

2.2.8 Мастер импорта

Мастер импорта поможет вам загрузить хэши Windows в программу, не обременяя лишними опциями и вопросами. Например, для загрузки хэшей из другой операционной системы, достаточно указать только каталог Windows. Все остальное программа сделает за вас: определит тип хэшей (локальные или Active Directory), включит режим поиска текстовых паролей на целевом диске, загрузку удаленных учетных записей, хэшей истории, биометрических данных и т.д.
Всего предлагается на выбор 4 источника хэшей: локальный компьютер, чужая операционная система, удаленный компьютер и файл хэшей, созданный в другой программе.



Hash import Wizard

Choose the source from which to retrieve the Windows hashes

Step 1/3

Data source

○ The local machine

Extracting hashes (for all user accounts) that are stored locally. If this is a domain PC, the program will load Active Directory accounts including ones reside in hash history. You may need to disable your AV to make the program work as expected.

● Windows directory on an external/attached drive

Reading hashes from another Windows system. This OS should be located on a drive that was attached to the local machine via USB/SCSI/SATA/IDE interface.

○ A remote PC

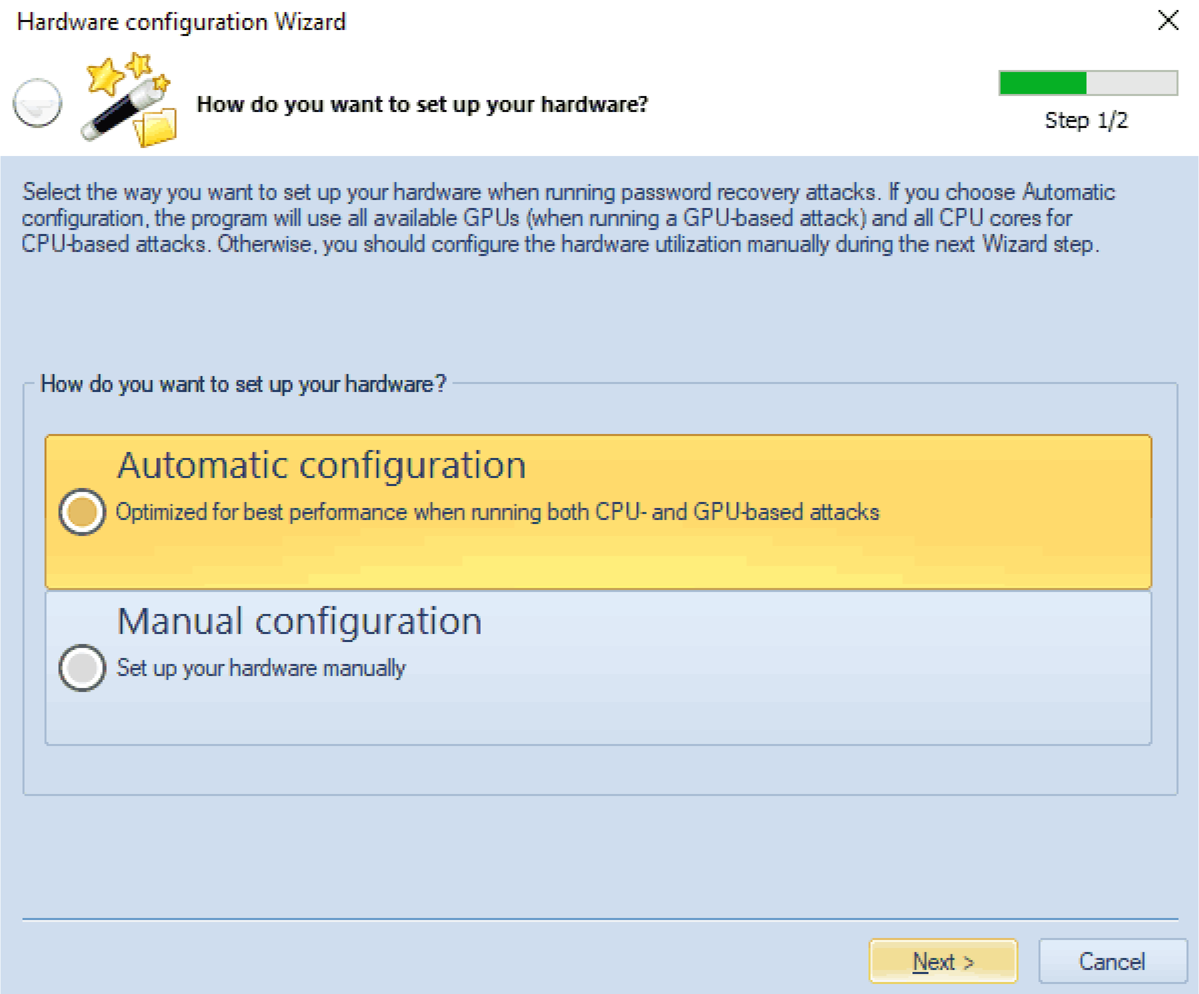
Loading hashes from a remote machine. You will need an Administration account/password to connect remotely. The remote machine must have remote administration enabled. The program will guide you through this later.

○ A file created by another program.

Importing hashes from files that were created in other programs like PWDUMP, HashCat, PPA, L0phcrack, Cain and Abel, etc.

2.2.9 Мастер оборудования

Для настройки оборудования, которое будет использоваться в восстановлении паролей, программа предлагает воспользоваться Мастером оборудования. Автоматический режим определяет конфигурацию, наиболее подходящую для вашего компьютера. Можно также воспользоваться ручной настройкой.
Учтите, если включен автоматический режим, опции процессора и видеокарт в общих настройках будут недоступны до тех пор, пока вы не переключитесь на ручной режим.



Hardware configuration Wizard

How do you want to set up your hardware?

Step 1/2

Select the way you want to set up your hardware when running password recovery attacks. If you choose Automatic configuration, the program will use all available GPUs (when running a GPU-based attack) and all CPU cores for CPU-based attacks. Otherwise, you should configure the hardware utilization manually during the next Wizard step.

How do you want to set up your hardware?

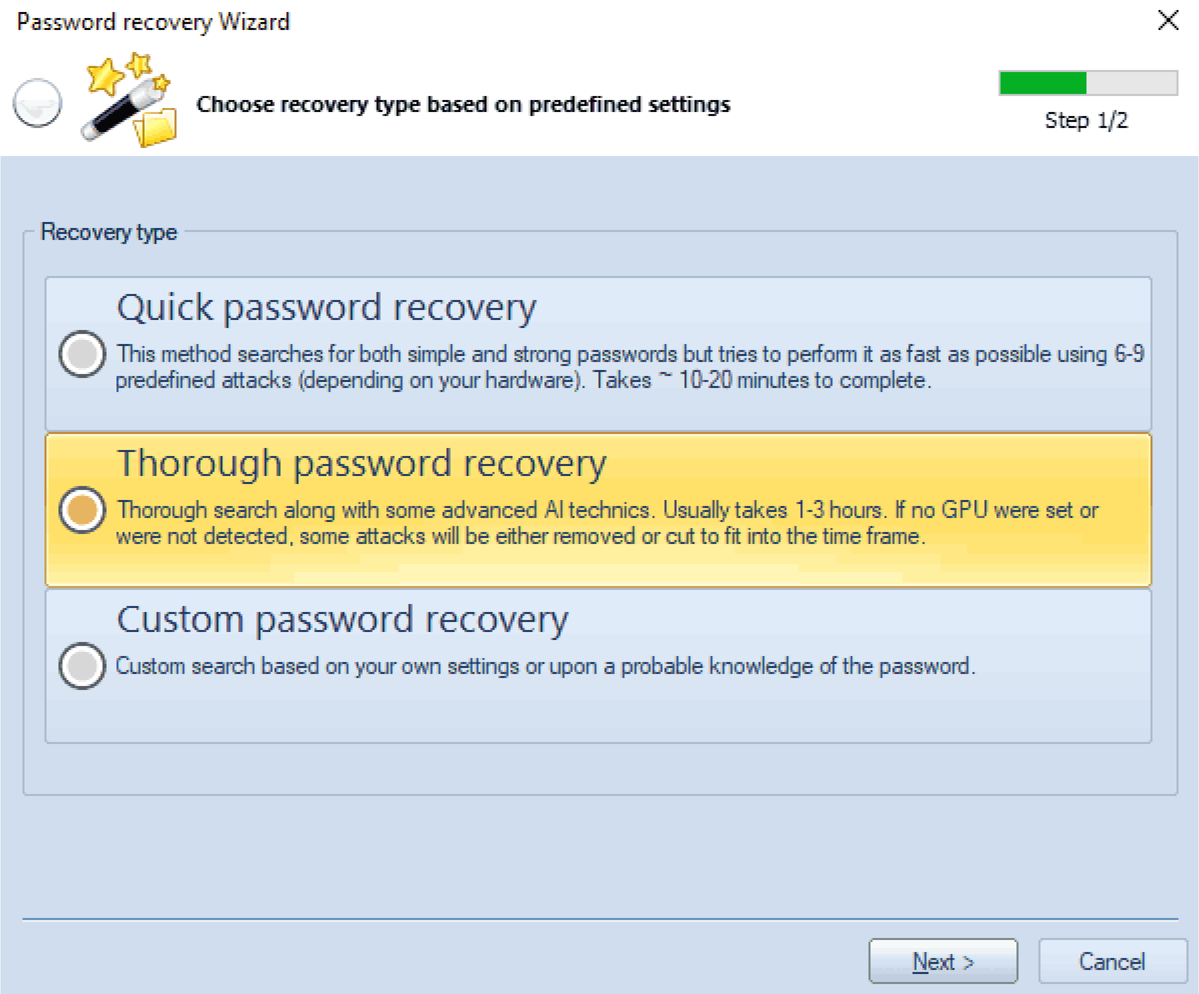
● Automatic configuration
Optimized for best performance when running both CPU- and GPU-based attacks

○ Manual configuration
Set up your hardware manually

2.2.10 Мастер восстановления

Мастер восстановления использует самые лучшие и новейшие алгоритмы восстановления паролей Windows, которые были придуманы за последние несколько лет. И это не просто слова. Вот всего лишь несколько фактов

- Глубина поиска паролей зависит от используемого оборудования.
- Последовательно запускаются несколько атак, оптимально подобранные для поиска паролей разных типов.
- Режим тщательного поиска использует алгоритмы искусственного интеллекта и генерации шаблонов паролей по найденным образцам.
- Режим тщательного поиска находит больше паролей, чем любая аналогичная программа.



Password recovery Wizard

Choose recovery type based on predefined settings

Step 1/2

Recovery type

○ Quick password recovery

This method searches for both simple and strong passwords but tries to perform it as fast as possible using 6-9 predefined attacks (depending on your hardware). Takes ~ 10-20 minutes to complete.

● Thorough password recovery

Thorough search along with some advanced AI technics. Usually takes 1-3 hours. If no GPU were set or were not detected, some attacks will be either removed or cut to fit into the time frame.

○ Custom password recovery

Custom search based on your own settings or upon a probable knowledge of the password.

2.3 Меню Восстановление

Данный пункт меню служит для выбора и запуска атаки. Панель "Атака" позволяет выбрать тип атаки и переключить между атакой на LM/NT/DCC хэши. Имейте в виду, что перед запуском атаки необходимо сначала выбрать/отметить нужные хэши. Это делается из меню **Редактирование - Выбор**. Запуск атаки подразумевает также, что были установлены ее опции (меню **Опции - Опции атаки**).

2.3.1 Запуск

Запуск выбранной атаки. Во время атаки все остальные пункты меню становятся неактивными. Следует отметить, что после окончания атаки запускается специальная функция мутации и анализа найденных паролей. Данная опция по умолчанию включена, но может отключаться из общих настроек.

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.

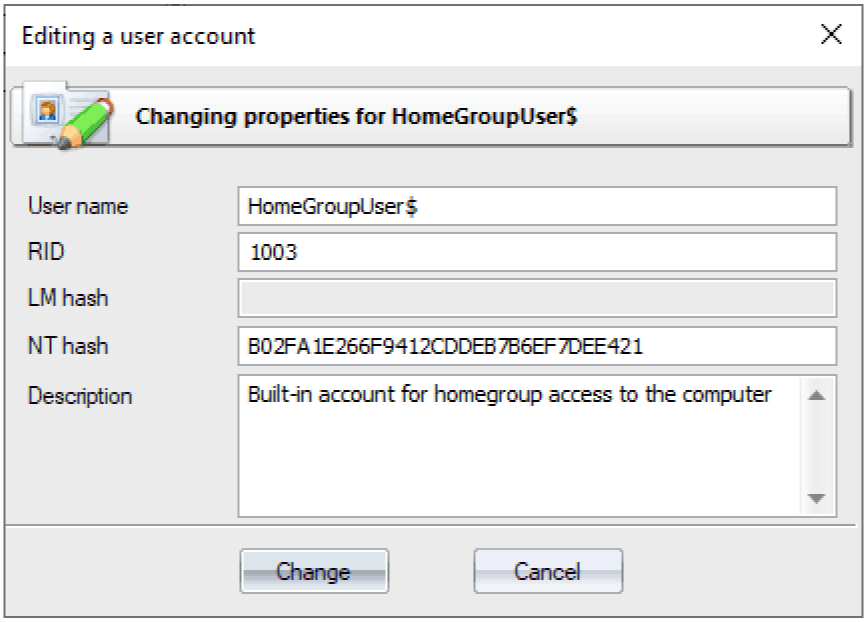
2.3.3 Стоп

Остановка текущей атаки.

2.4 Меню Редактирование

Меню редактирование доступно только при активной вкладе "Хэши" и состоит и четырех элементов: редактирование, копирование, выбор и поиск.

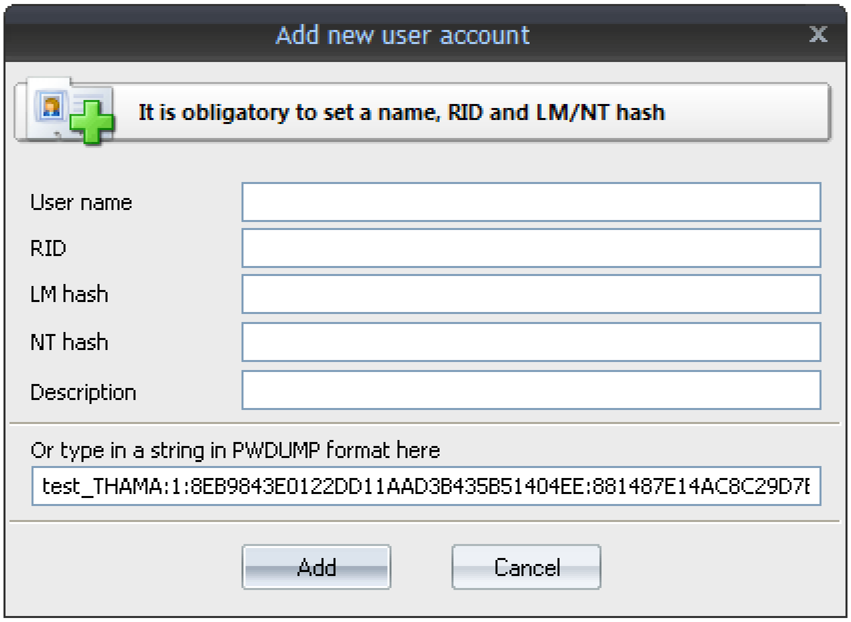
2.4.1 Редактировать



User name: HomeGroupUser$
RID: 1003
LM hash:
NT hash: B02FA1E266F9412CDDEB7B6EF7DEE421
Description: Built-in account for homegroup access to the computer

При выборе этого пункта появляется диалоговое окно, в котором можно в ручном режиме изменить следующие поля текущей выбранной учетной записи: имя пользователя, его RID, LM/NT или DCC хэши, а также комментарий к этой записи.

2.4.2 Добавить



It is obligatory to set a name, RID and LM/NT hash

Or type in a string in PWDUMP format here

test_THAMA:1:8EB9843E0122DD11AAD3B435B51404EE:881487E14AC8C29D7E

Данный пункт предназначен для ручного добавления записи. Имеется возможность вводить целиком строки в формате PWDUMP.

2.4.3 Удалить

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

2.4.4 Сбросить Пароли

Сброс всех найденных паролей из списка.

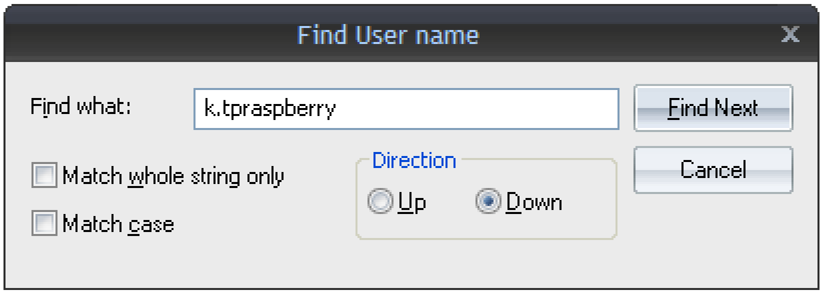
2.4.5 Копировать

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

2.4.6 Выбрать

Выбор хэшей для атаки. Выбранные хэши отмечены галочкой. Если во время атаки найден пароль для выбранного хэша, то отметка этой записи автоматически сбрасывается, а сама запись помечается зеленым цветом. Для выбора NT хэшей, необходимо сначала снять выделение с LM хэшей и наоборот.

2.4.7 Поиск



Find User name

Find what: k.tpraspberry

□ Match whole string only

□ Match case

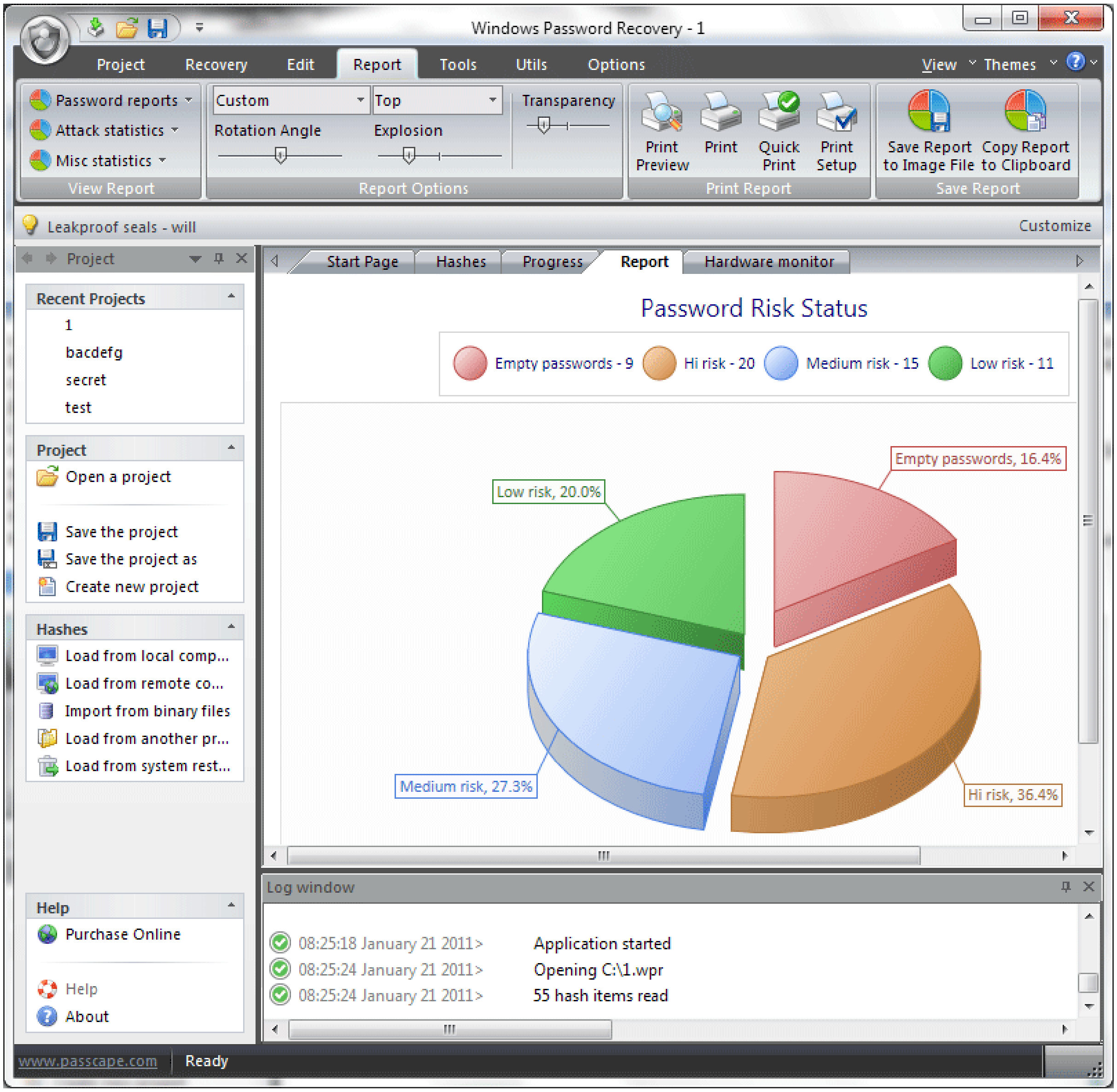
Direction: ○ Up ● Down

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

2.5 Меню Отчеты

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

- Отчеты о паролях
- Статистика атак
- Различная информация
- Статистика учетных записей
- Анализ словарей
- Информация о группах



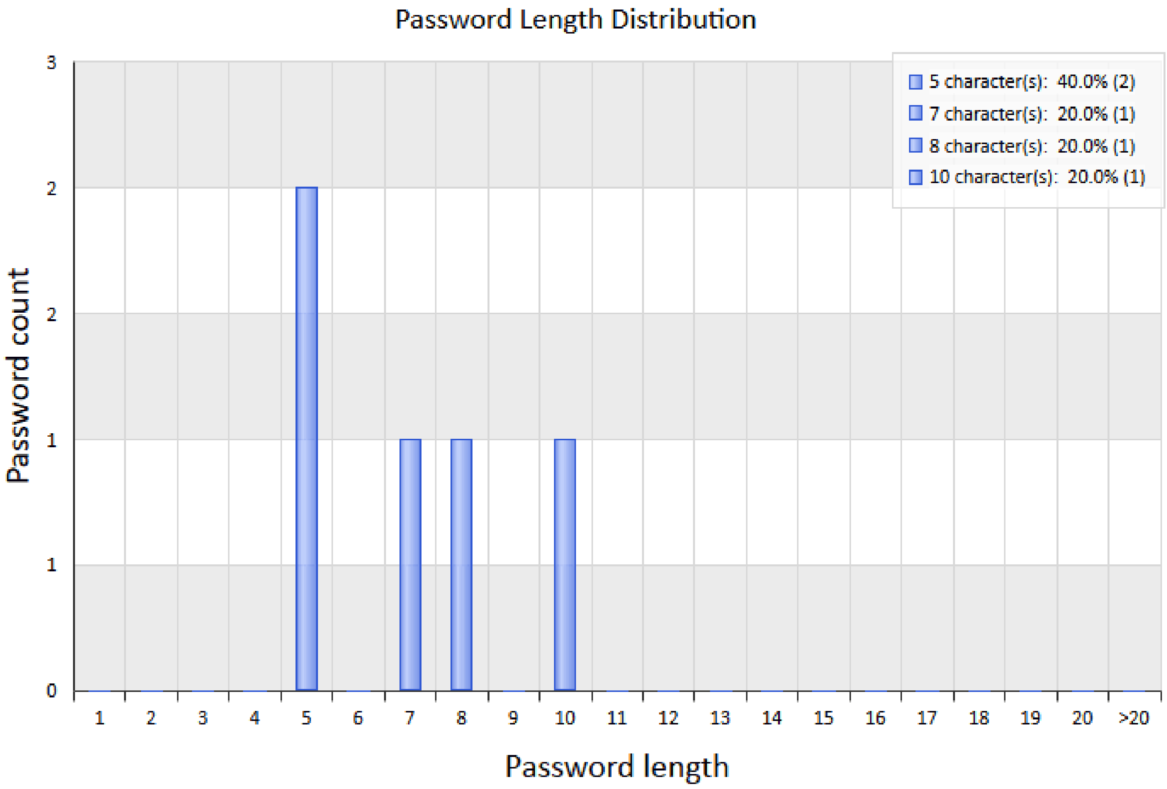
```
08:25:18 January 21 2011>    Application started
08:25:24 January 21 2011>    Opening C:\1.wpr
08:25:24 January 21 2011>    55 hash items read
```

2.5.1 Отчеты о паролях

Отчеты о паролях включают в себя следующие пункты:

- **Парольные риски** - отчет 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
- **Уникальность паролей** - показывает сколько было расшифровано уникальных паролей, а какие расшифрованные пароли используются единожды.
- **Часто используемые пароли** - какие из расшифровываемых паролей используются более одного раза.
- **LM и NT** - соотношение количества LM и NT паролей

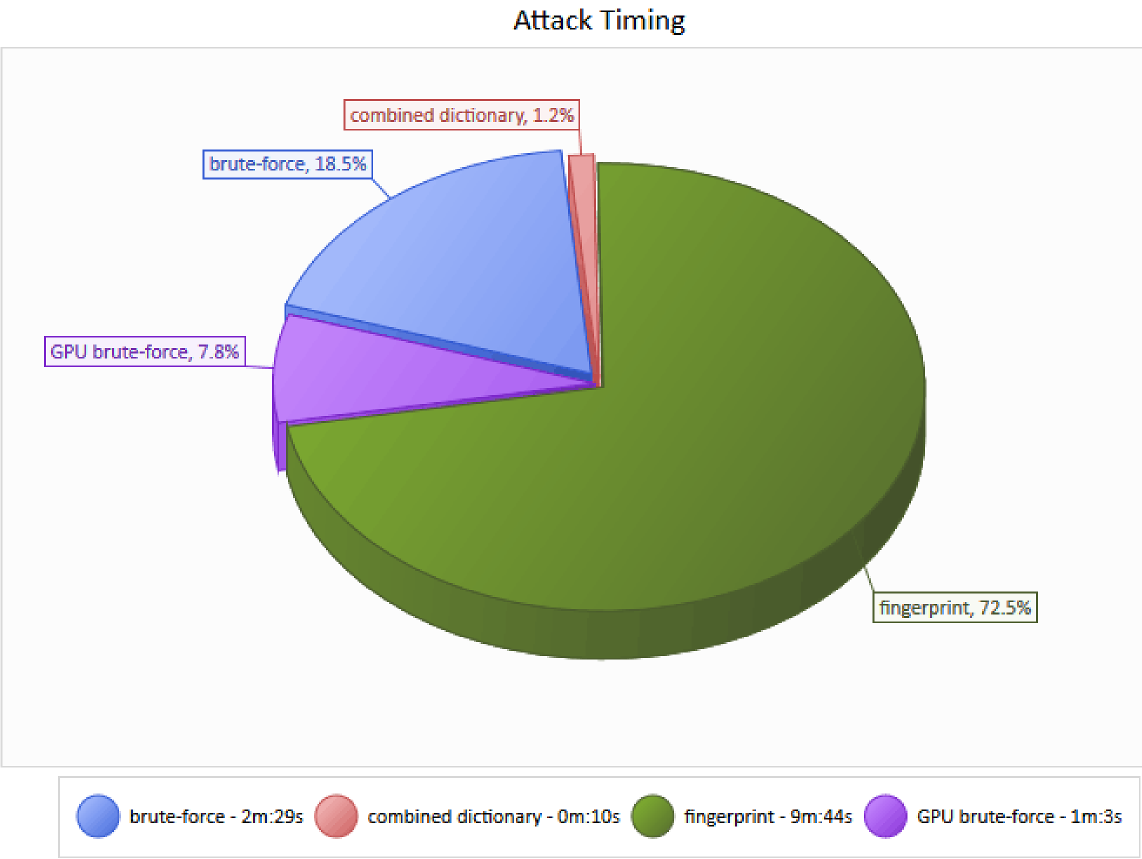
- **Типы хэшей** - типы загруженных учетных записей: обычные (NTLM и LM), кэшированные записи домена, Windows Hello PIN, кэши паролей MSA/AAD
- **Обычные и пароли истории** - соотношение количества обычных паролей и паролей истории (только для хэшей загруженных из SAM\NTDS.DIT файлов, например, импортированных с локального компьютера.
- **Время поиска паролей** - время, затраченное на поиск паролей. Наиболее уязвимые пароли отмечены красной палитрой.
- **Найденные и не найденные** - соотношение количества найденных и не расшифрованных паролей
- **Найденные пароли** - подробный отчет о найденных паролях: сколько из них пустых, сколько частично найдено, сколько полностью восстановлены.



2.5.2 Статистика атак

Статистика атак включает в себя следующие отчеты:

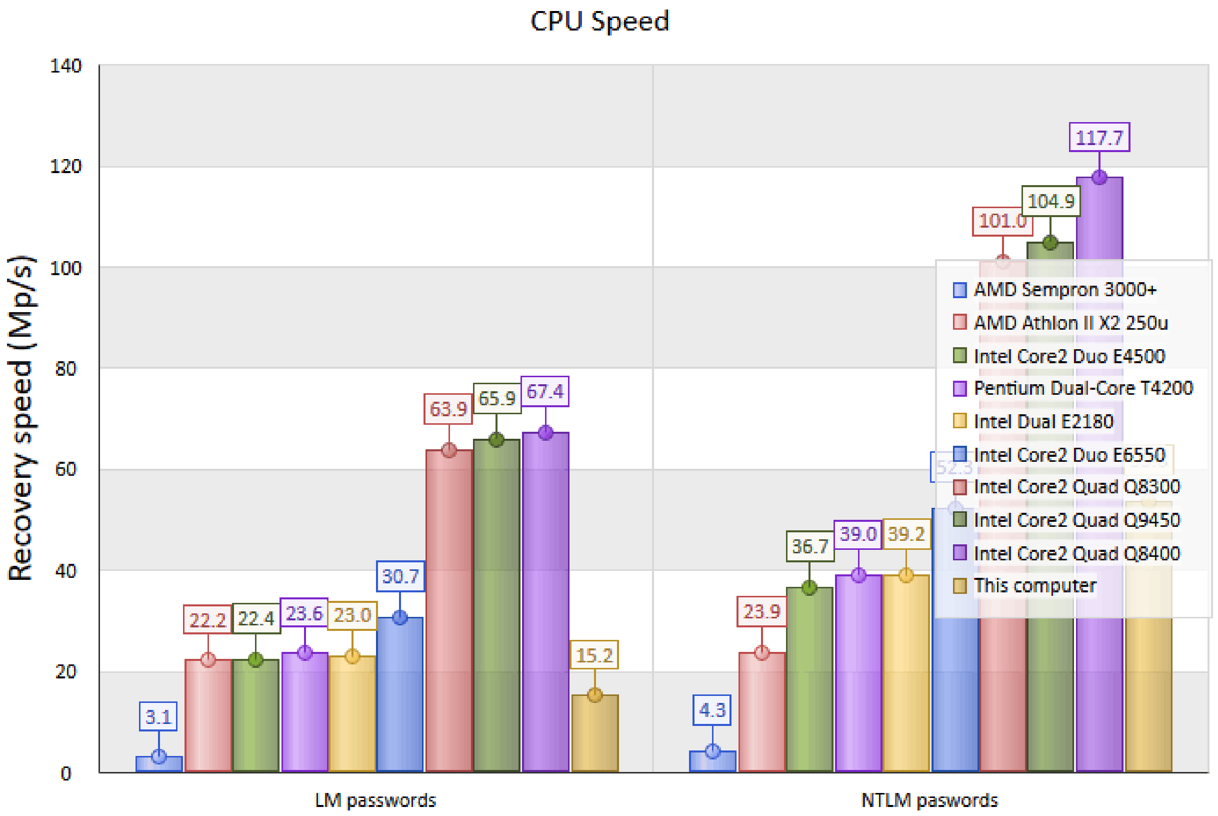
- **Предпочтительная атака** - статистика по количеству и типу запущенных атак
- **Время атаки** - анализ времени, затрачиваемого на каждую атаку
- **Эффективность атаки 1** - анализ эффективности: соотношение затрачиваемого времени к найденым во время атаки паролям
- **Эффективность атаки 2** - анализ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



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. Скорость перебора на процессоре или видеокарте можно измерить при помощи инструмента для измерения стойкости пароля.
- **Взломанные пользователи** - количество взломанных пользователей. Полный список пользователей дополнительно можно сохранить в текстовый файл.
- **Взломанные пользователи и пароли** - список взломанных пользователей с паролями.

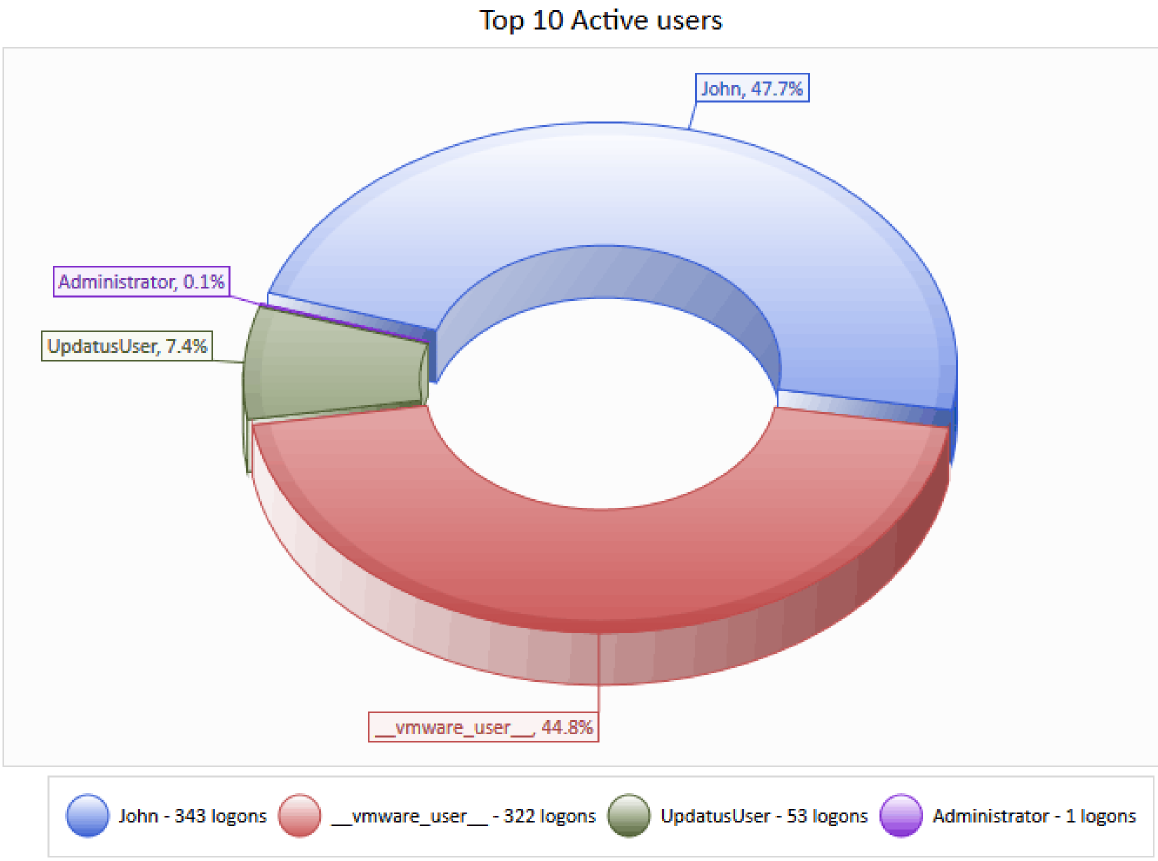


2.5.4 Статистика учетных записей

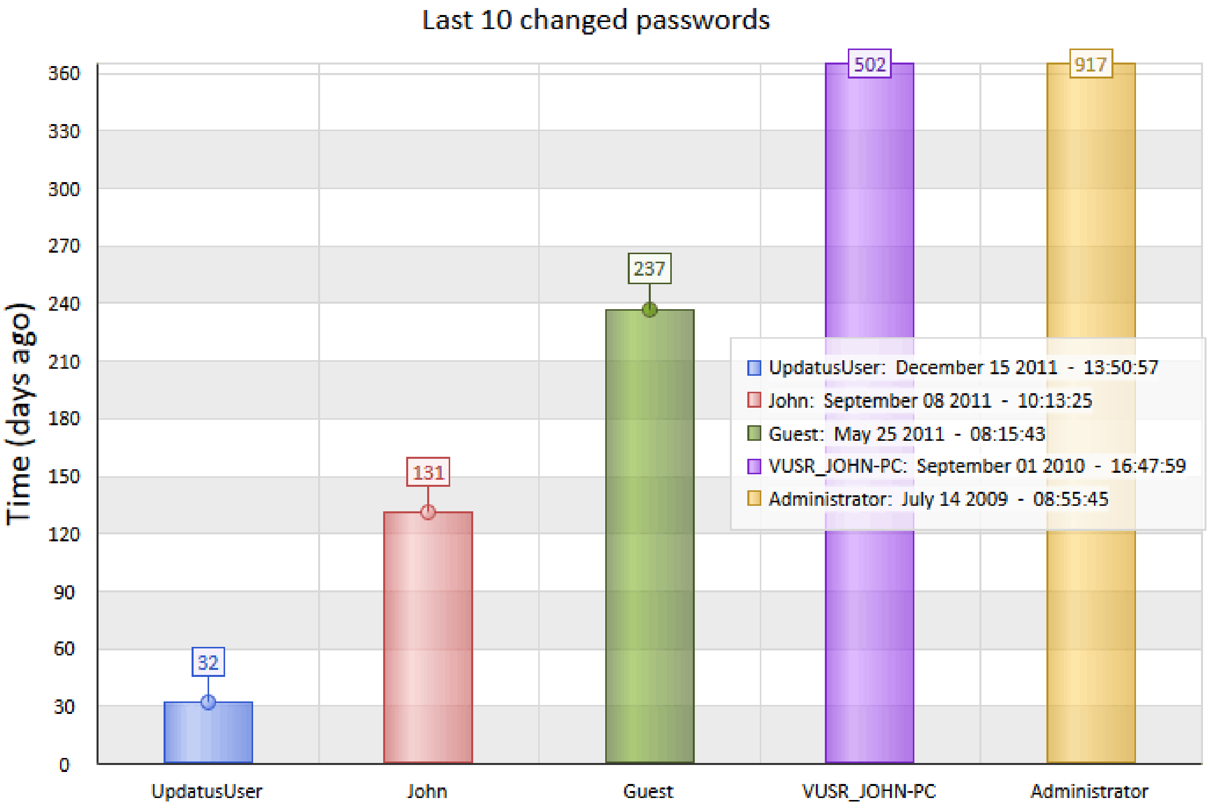
Статистика учетных записей. Отчеты со статистикой доступны как для локальных, так и для доменных учетных записей. Для создания отчета сначала необходимо выбрать источник данных: локальную или внешнюю базу, SAM или Active Directory. В данной категории доступны следующие отчеты:

- **Обычные и отключенные учетные записи.** Этот отчет показывает соотношение обычных или отключенных учетных записей пользователей.
- **Обычные и заблокированные учетки.** Соотношение нормальных и заблокированных\залоченных учетных записей.
- **С паролями - без паролей.** Показывает количество учетных записей с пустыми и с установленными паролями.
- **Типы учетных записей.** Соотношение пользователей и системных учетных записей.
- **Активные и просроченные пароли.** Отчет со статистикой по учетным записям с активными или просроченными паролями.
- **Обычные пароли и с неограниченным сроком действия** - показывает соотношение учетных записей с ограниченным и неограниченным сроком действия паролей.
- **Администраторы и ограниченные пользователя.** Данный отчет выводит сравнительную статистику учетных записей с правами Администратора по отношению к ограниченным учетным записям.
- **Типы учетных записей**. Разделяет все учетные записи на системные, пользовательские, администраторские и т.д.
- **Статус учетной записи**. Этот отчет аналогичен первому за исключением того, что он не выводит дополнительную информацию по именам отключенных учетных записей.

- **10 активных пользователей.** Отчет о 10 самых активных пользователей ОС. Статистика ведется в соответствии со счетчиком входов в систему.
- **Счетчик неверных вводов пароля.** 10 пользователей, имеющих самые большие значения в счетчике неверных вводов пароля.



- **Последние 10 неудачных попыток входа -** показывает список последних 10 пользователей, попытавшихся войти в систему с неправильным паролем.
- **Последние смененные пароли** - список последних 10 пользователей, которые сменили пароль своей учетной записи.
- **Последние 10 входов** - список последних 10 пользователей, которые успешно зашли в систему.
- **Последние 10 выходов -** список последних 10 выходов из системы.
- **Учетные записи с ограниченным сроком** - список 10 учетных записей у которых истекает срок действия.
- **Активность пользователей**. Группирует всех пользователей по дате последнего входа в систему.
- **Срок действия пароля**. Группирует пользователей по дате последней смены или установки пароля.



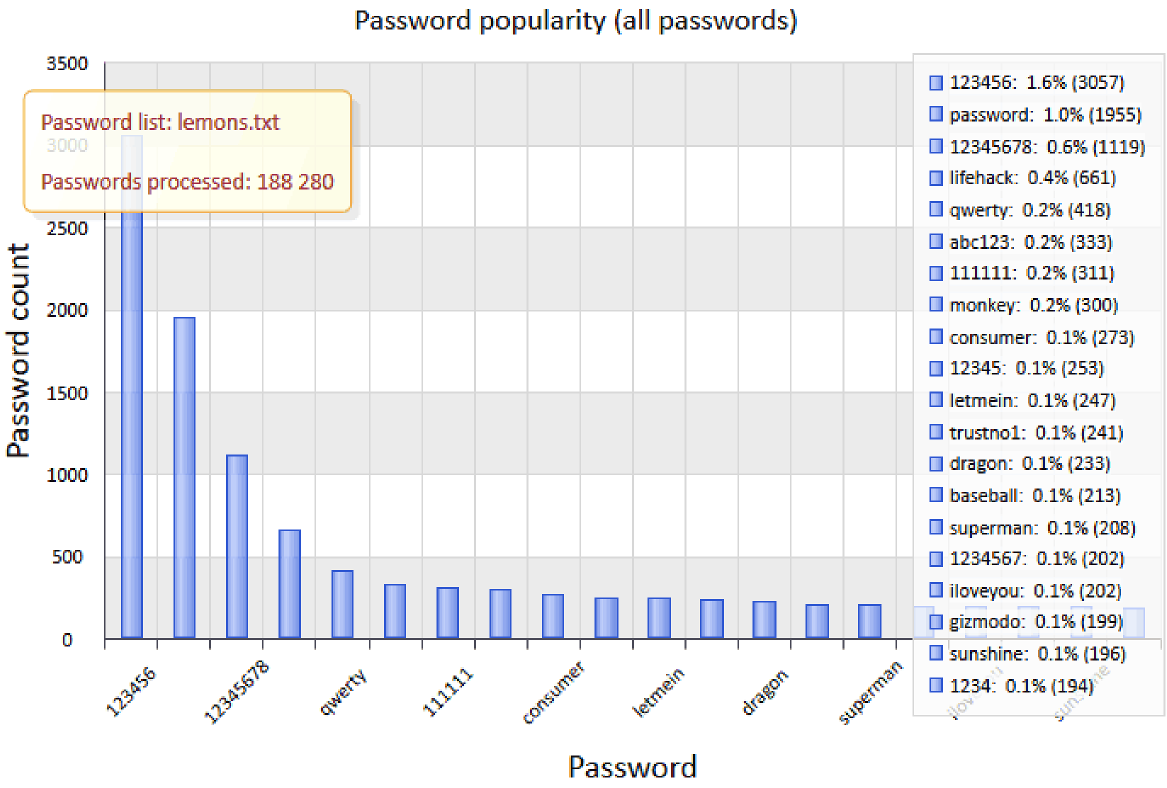
Можно сохранить дополнительную информацию об учетных записях в текстовый файл щелкнув мышью по части отчета.

2.5.5 Анализ словарей

Данные отчеты 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 определенному диапазону, например только для определенной длины. В этом меню доступны следующие отчеты:

- Распределение длин паролей - показывает график распределения длин паролей, т.е. количество паролей, приходящихся на определенную длину.
- Уникальность паролей - состоит ли исходный список из уникальных слов или есть повторяющиеся пароли.
- Популярность паролей - этот отчет 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 четырех 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.

- 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.

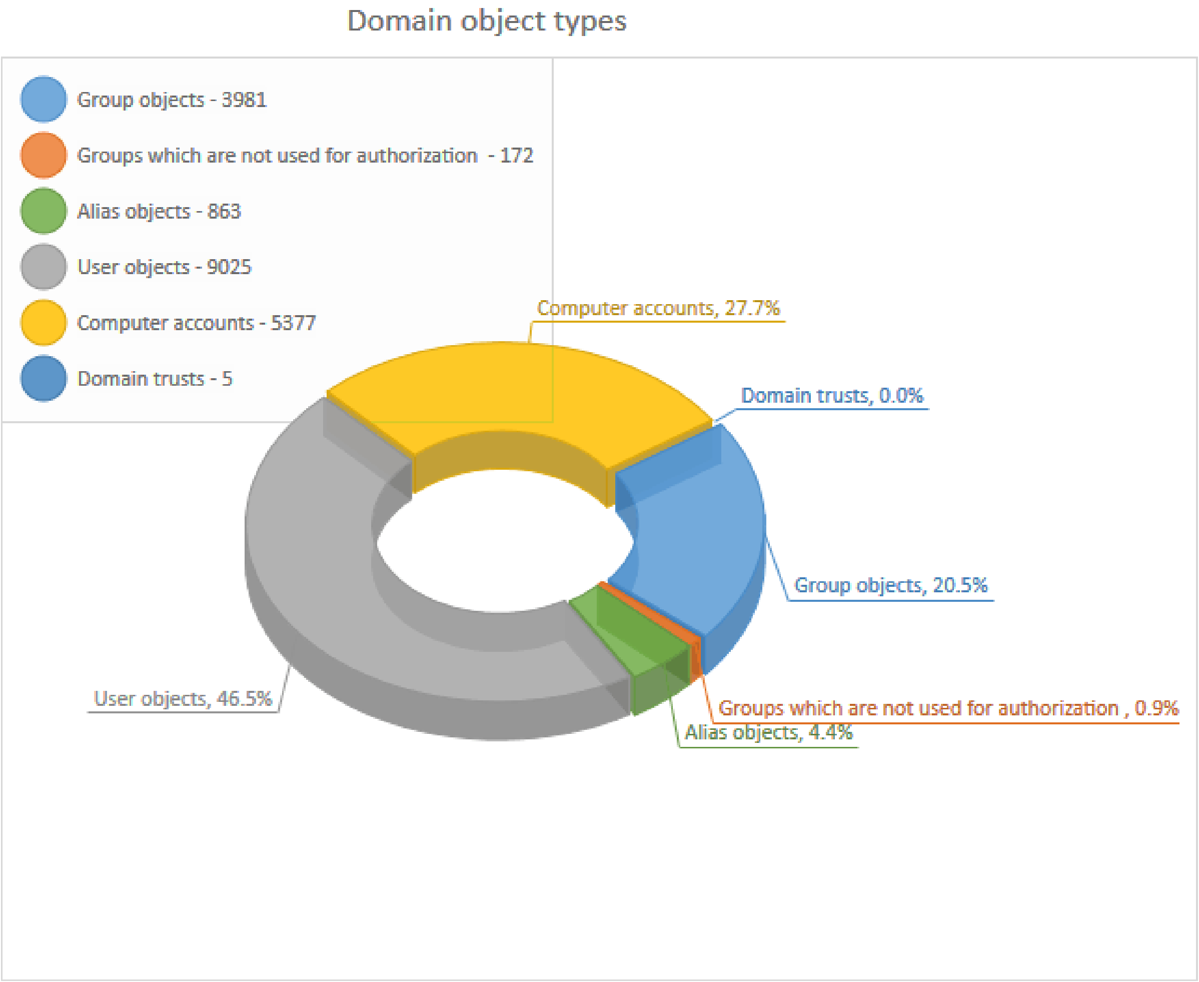


2.5.6 Информация о группах

Данная секция предназначена главным образом для сбора и анализа различной информации о группах и объектах Active Directory. Тем не менее, некоторые отчеты могут использоваться для вывода соответствующей информации о локальных учетных записях, хранящихся в файле реестре SAM. Доступны следующие отчеты:

- **Последние 10 созданных групп.** Последние 10 групп, созданных в домене.
- **Последние 10 измененных групп.** Последние 10 групп, которые подвергались модификации.
- **Типы групп.** Этот отчет показывает соотношение типов, к которым принадлежат групповые учетные записи.

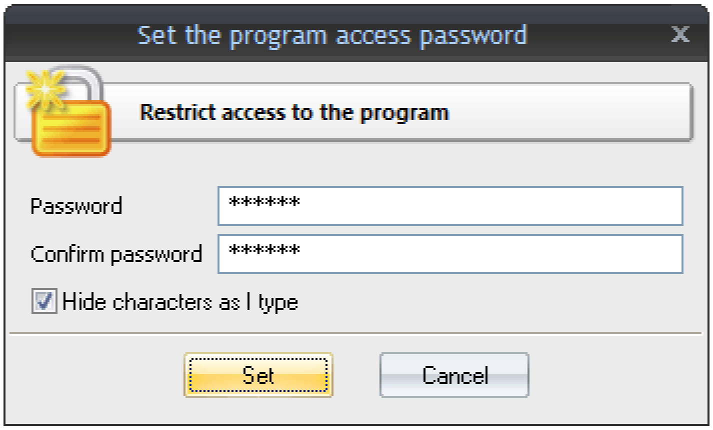
- **Наиболее заполненные группы** - показывает список из 10 групп, содержащих наибольшее количество пользователей.
- **Менее всего заполненные группы** - показывает список из 10 групп с наименьшим количеством пользователей. Группы без пользователей не учитываются.
- **Активные и неактивные группы.** Соотношение активных (содержащих хотя бы одного члена) и неактивных (пустых) групп.
- **Админские и неадминские группы** - выводит соотношение групп с правами Администратора и без таковых.
- **Последние 10 созданных псевдонимов.** Последние 10 псевдонимов, созданных в домене
- **Последние 10 измененных псевдонимов.** 10 псевдонимов, которые подвергались изменениям в последнее время.
- **Типы псевдонимов.** График типов, к которым принадлежат псевдонимы.
- **Наиболее заполненные псевдонимы** - список из 10 псевдонимов, содержащих наибольшее количество пользователей.
- **Наименее всего заполненные псевдонимы** - список из 10 псевдонимов с наименьшим количеством пользователей.
- **Активные и неактивные псевдонимы.** Соотношение активных (содержащих хотя бы одного пользователя) и неактивных (пустых) псевдонимов.
- **Псевдонимы с правами и без прав администратора** - соотношение псевдонимов с правами Администратора и без них.
- **Типы доменных объектов -** статистика по всем типам объектов в домене. Например: пользователи, группы, компьютерные учетные записи, домены доверительных отношений и т.д.



2.6 Меню Инструменты

Инструменты состоят из трех частей: инструменты для разграничения доступа к программе, инструменты для работы с паролями/хэшами и инструменты для создания радужных таблиц.

2.6.1 Доступ к Программе



Set the program access password

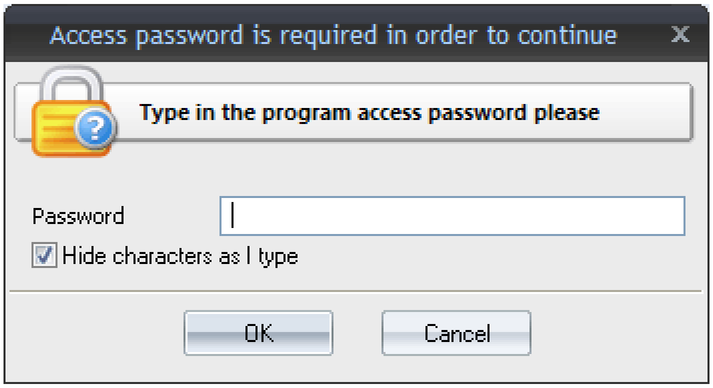
Restrict access to the program

Password: ******

Confirm password: ******

☑ Hide characters as I type

В том случае, если кроме вас к компьютеру или к вашей учетной 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.



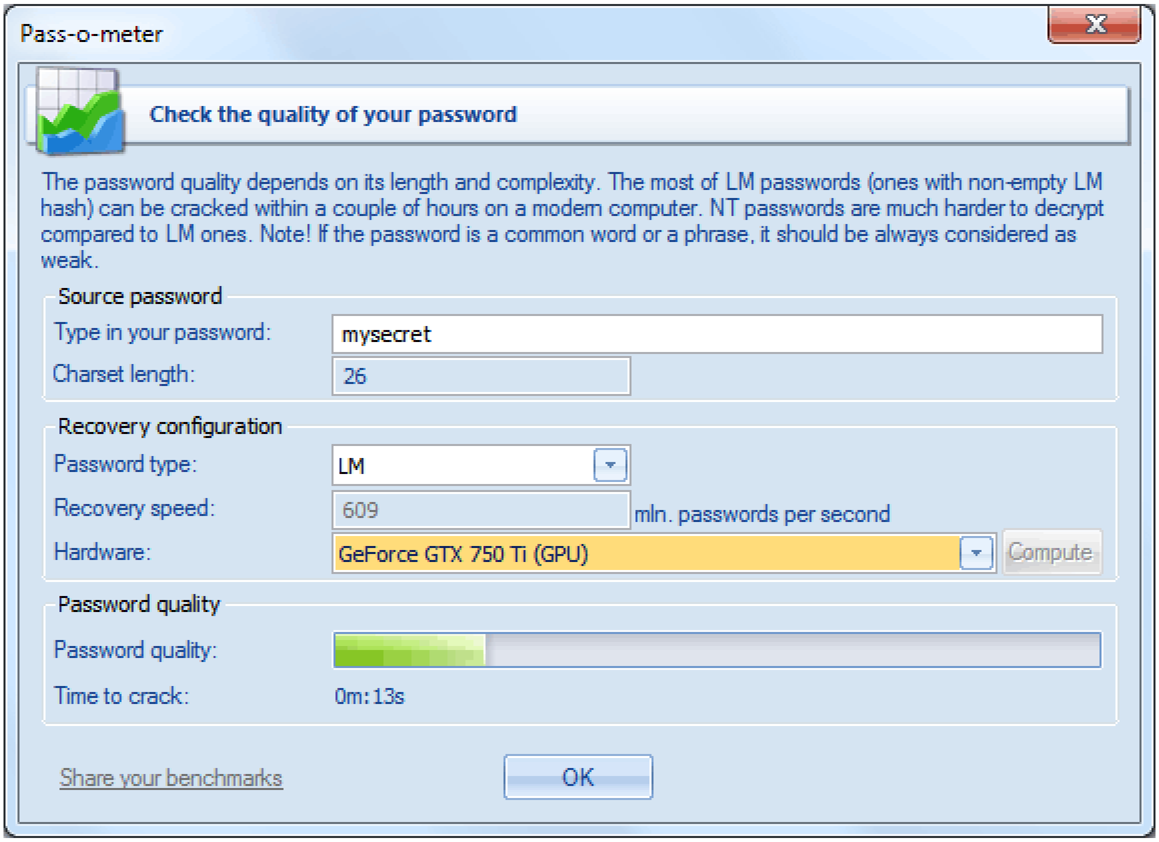
Access password is required in order to continue

Type in the program access password please

Password:

☑ Hide characters as I type

2.6.2 Пасс-о-метр



Pass-o-meter

Check the quality of your password

The password quality depends on its length and complexity. The most of LM passwords (ones with non-empty LM hash) can be cracked within a couple of hours on a modern computer. NT passwords are much harder to decrypt compared to LM ones. Note! If the password is a common word or a phrase, it should be always considered as weak.

Source password

Type in your password: mysecret

Charset length: 26

Recovery configuration

Password type: LM

Recovery speed: 609 mln. passwords per second

Hardware: GeForce GTX 750 Ti (GPU)

Password quality

Password quality:

Time to crack: 0m:13s

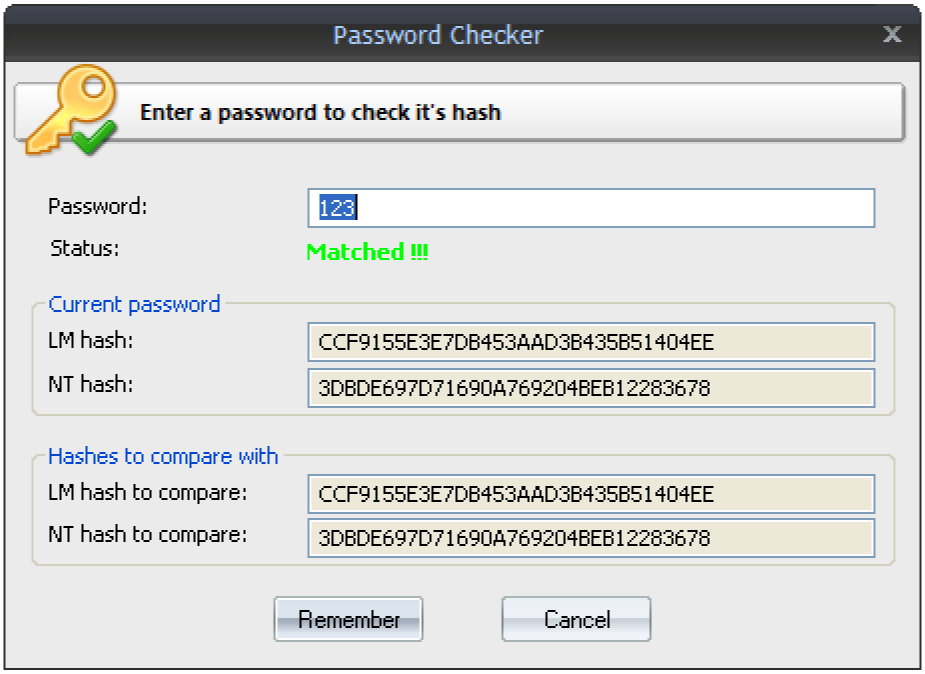
Инструмент для измерения стойкости вашего пароля против взлома. При первом запуске программа попросит провести тест скорости вашего компьютера. Для проверки качества пароля надо:

- Ввести пароль в соответствующее поле ввода
- Выбрать тип хэшей: LM или NT. Помните, что операционные системы начиная с Windows Vista по умолчанию хранят пароли в виде NT хэшей.
- Выбрать тип компьютера. "Этот компьютер" соответствует скорости перебора вашего компьютера.
- 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 **Отчеты**.

Внизу вы увидите качество вашего пароля и сколько времени потребуется для его взлома в выбранной конфигурации. Например, взлом любого LM хэша буквенно-цифрового пароля займет около 10 минут на современном процессоре (при скорости перебора более 100 миллионов паролей в секунду). Скорость перебора пароля на GPU может возрасти еще на порядок.

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

2.6.3 Проверка Пароля



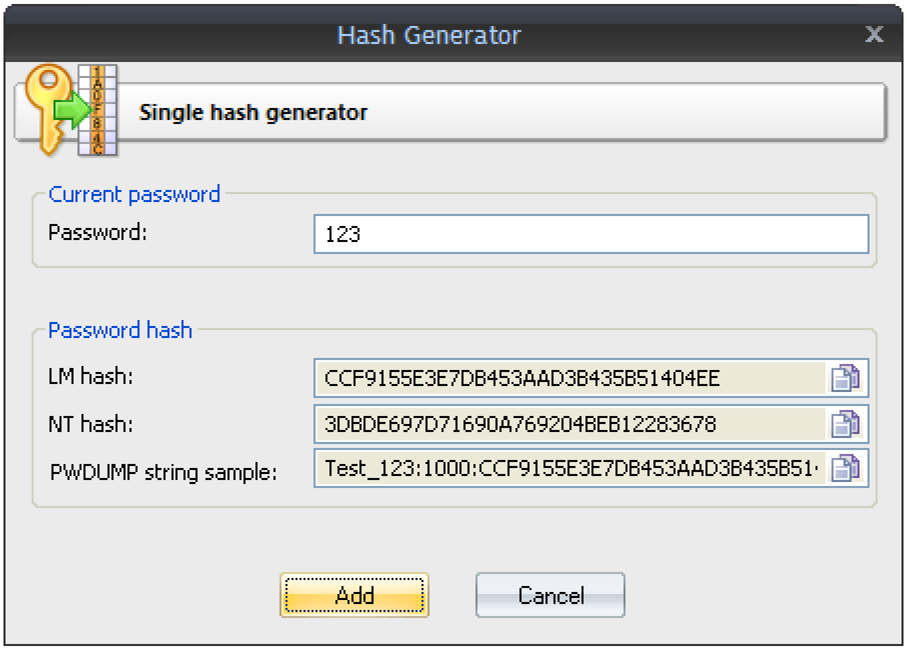
Password: 123
Status: Matched !!!

Current password
LM hash: CCF9155E3E7DB453AAD3B435B51404EE
NT hash: 3DBDE697D71690A769204BEB12283678

Hashes to compare with
LM hash to compare: CCF9155E3E7DB453AAD3B435B51404EE
NT hash to compare: 3DBDE697D71690A769204BEB12283678

Данный инструмент предназначен для ручной проверки пароля выбранного хэша. Проверка пароля часто бывает необходима при проверке валидности того или иного хэша. Например, в том случае, если LM хэш по той или иной причине не соответствует NT хэшу.

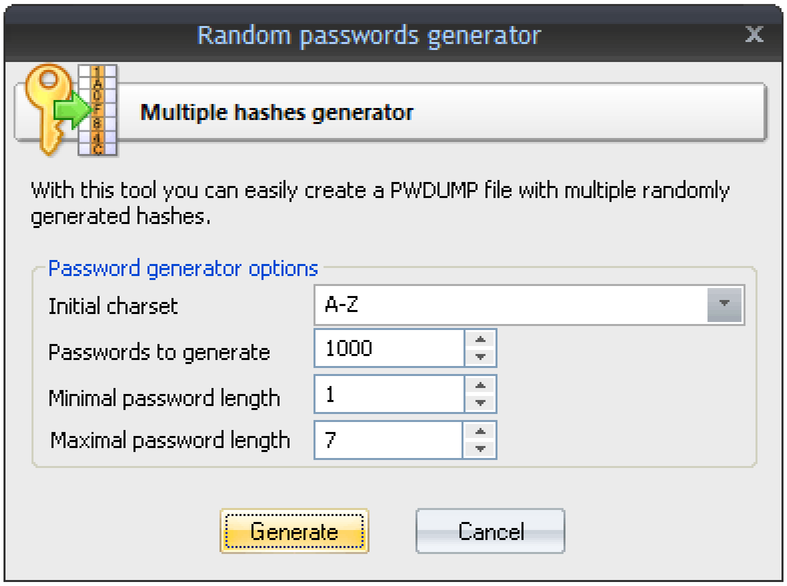
2.6.4 Генератор Хэшей



Current password
Password: 123

Password hash
LM hash: CCF9155E3E7DB453AAD3B435B51404EE
NT hash: 3DBDE697D71690A769204BEB12283678
PWDUMP string sample: Test_123:1000:CCF9155E3E7DB453AAD3B435B51

Генератор одного хэша позволяет быстро сгенерировать тестовую запись для заданного пароля и добавить ее в список хэшей.



Random passwords generator

Multiple hashes generator

With this tool you can easily create a PWDUMP file with multiple randomly generated hashes.

Password generator options

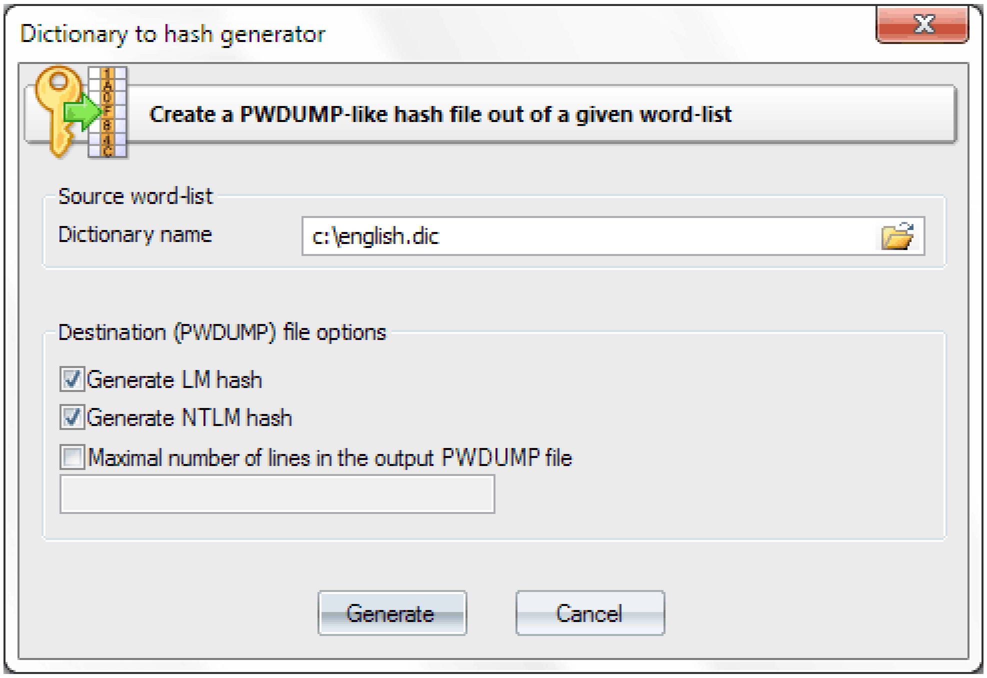
Initial charset: A-Z

Passwords to generate: 1000

Minimal password length: 1

Maximal password length: 7

Если вы хотите создать PWDUMP файл с определенным количеством случайно сгенерированных паролей, то для этого надо воспользоваться инструментом для генерации нескольких хэшей. В диалоге создания хэшей выбираем минимальную и максимальную длину, диапазон символов и общее количество генерируемых паролей.



Dictionary to hash generator

Create a PWDUMP-like hash file out of a given word-list

Source word-list

Dictionary name: c:\english.dic

Destination (PWDUMP) file options

☑ Generate LM hash

☑ Generate NTLM hash

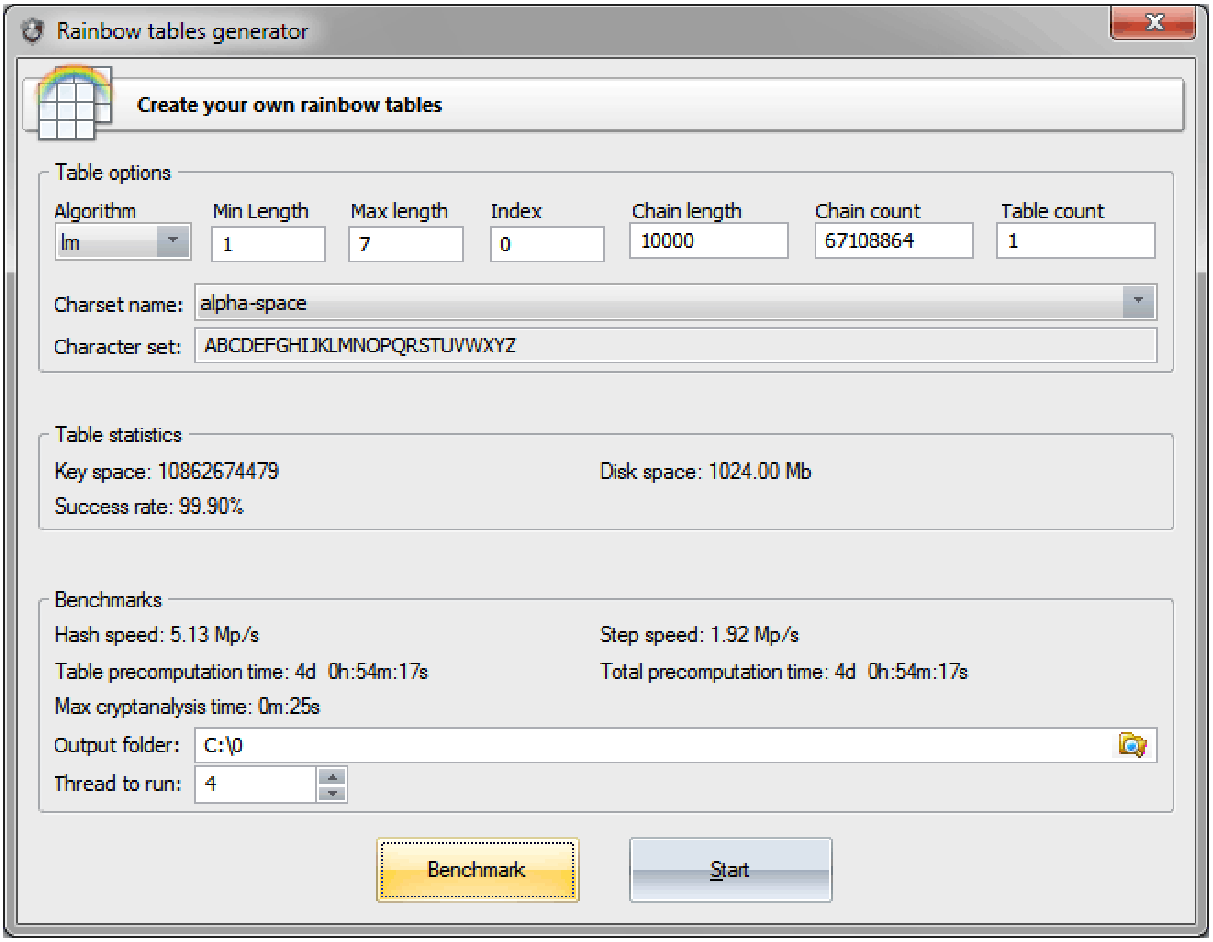
☐ Maximal number of lines in the output PWDUMP file

Иногда бывает необходимо создать тестовый PWDUMP файл с хэшами из уже готовых паролей. В этом случае удобно использовать генератор хэшей по словарю. Интерфейс этого инструмента довольно прост и состоит из диалога, в верхней части которого задается список входных слов для генератора. На их основе будут созданы хэши. В нижней части мы указываем какие именно хэши нам нужны. Можно также ограничить выходной объем создаваемого PWDUMP файла определенным количеством записей.

2.6.5 Создание Радужных Таблиц

Радужные таблицы - это специальные таблицы поиска, используемые для вскрытия паролей, преобразованных при помощи необратимых хэш функций. Примером таких паролей могут служить хэши пользователя (LM или NTLM) в операционной системе Windows.

В программе Windows Password Recovery реализован поиск паролей по радужным таблицам. Для его работы необходимо наличие таблиц, которые можно скачать из Интернет, либо создать самостоятельно при помощи инструмента для генерации RT таблиц.


Rainbow tables generator

Create your own rainbow tables

Table options

Algorithm: lm
Min Length: 1
Max length: 7
Index: 0
Chain length: 10000
Chain count: 67108864
Table count: 1

Charset name: alpha-space
Character set: ABCDEFGHIJKLMNOPQRSTUVWXYZ

Table statistics

Key space: 10862674479
Disk space: 1024.00 Mb
Success rate: 99.90%

Benchmarks

Hash speed: 5.13 Mp/s
Step speed: 1.92 Mp/s
Table precomputation time: 4d 0h:54m:17s
Total precomputation time: 4d 0h:54m:17s
Max cryptanalysis time: 0m:25s

Output folder: C:\0
Thread to run: 4

Перед тем, как начать создание таблиц(ы), важно настроить соответствующие взаимосвязанные опции и найти их наилучшее соотношение. Для этого выберите один из двух алгоритмов (LM или NTLM) и допустимый набор символов. Естественно, чем шире диапазон символов, тем больше паролей будет найдено в атаке по таблицам, но тем больше времени понадобится на их создание и, возможно, тем большего размера они будут.

В поле 'Min length' и 'Max length' задается минимальная и максимальная длина пароля в таблицах поиска. LM пароль в Windows состоит из двух 7 символьных половинок, поэтому максимальная длина пароля при генерации LM таблиц не должна превышать 7 символов.

'Chain Length' (длина цепочки) влияет на следующие параметры таблицы: вероятность нахождения пароля, время генерации таблицы и время подбора одного пароля во время атаки.

От количества цепочек (Chain count) зависит вероятность нахождения пароля, время генерации таблицы и ее размер.

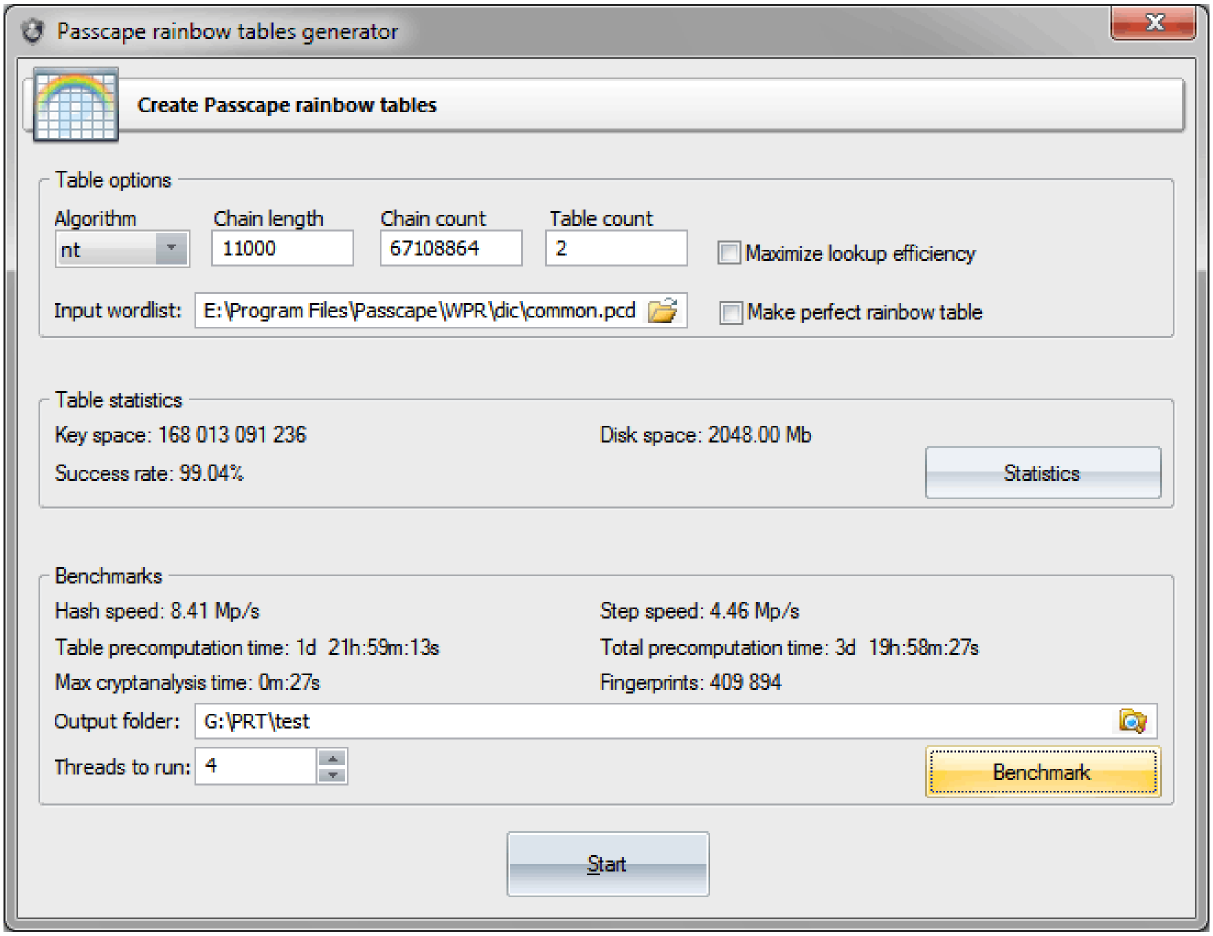
В настоящее время инструмент генерации таблиц не поддерживает таблицы размером более 2 Гб, однако при создании больших таблиц можно увеличивать их количество (параметр 'Table count').

Особенность реализации алгоритма поиска по радужным таблицам состоит в том, что успех нахождения пароля зависит он нескольких параметров, для которых важно найти наилучшее соотношение в зависимости от размера получаемых таблиц, времени их генерации и времени подбора пароля в атаке.

Инструмент генерации таблиц поддерживает многопоточность, поэтому перед началом работы выставите необходимое количество параллельных потоков, которые будут задействованы при создании таблиц.

2.6.6 Создание Радужных Таблиц Passcape

Радужные таблицы Passcape используются для поиска паролей в соответствующей атаке по таблицам Passcape. Для создания таких таблиц и предназначена данная утилита.



Passcape rainbow tables generator

Create Passcape rainbow tables

Table options

Algorithm: nt

Chain length: 11000

Chain count: 67108864

Table count: 2

□ Maximize lookup efficiency

Input wordlist: E:\Program Files\Passcape\WPR\dic\common.pcd

□ Make perfect rainbow table

Table statistics

Key space: 168 013 091 236

Disk space: 2048.00 Mb

Success rate: 99.04%

Benchmarks

Hash speed: 8.41 Mp/s

Step speed: 4.46 Mp/s

Table precomputation time: 1d 21h:59m:13s

Total precomputation time: 3d 19h:58m:27s

Max cryptanalysis time: 0m:27s

Fingerprints: 409 894

Output folder: G:\PRT\test

Threads to run: 4

Перед тем, как начать создание таблиц, укажите исходный словарь, который будет использован для создания банка отпечатков слов, и параметры таблиц:

- Chain Length - (длина цепочки) влияет на вероятность нахождения пароля, время генерации таблицы и время подбора одного пароля во время атаки.
- Количество цепочек (Chain count), от которого зависит вероятность нахождения пароля, время генерации таблицы и ее размер.

В настоящее время инструмент генерации таблиц не поддерживает таблицы размером более 2 Гб, однако при создании больших таблиц можно увеличивать их количество (параметр 'Table count').

Успех нахождения пароля по таблицам зависит он нескольких параметров, для которых важно найти наилучшее соотношение в зависимости от размера получаемых таблиц, времени их генерации и времени криптоанализа, т.е. подбора пароля в атаке.

При генерации таблиц можно также манипулировать двумя дополнительными опциями:

- Maximize password lookup efficiency - позволяет создавать больше отпечатков из исходного словаря, добавляя цифры, клавиатурные и частоупотребляемые комбинации. Эта опция хорошо подходит для небольших словарей.
- Make perfect rainbow table. Как известно, цепочки паролей в радужных таблицам могут сливаться. Это означает бесполезную трату информации, времени, дискового пространства. Выставив соответствующую опцию, можно создавать так называемые perfect tables, где не будет слияний в цепочках паролей. Такие таблицы занимают намного меньше места на диске и подбор пароля по ним осуществляется несколько быстрее. Однако падение вероятности нахождения пароля является неизбежной платой за создание перфектных таблиц. Для того, чтобы нивелировать падение success rate, рекомендуется как минимум удвоить количество цепочек и увеличить число создаваемых таблиц.

Инструмент генерации таблиц поддерживает многопоточность, поэтому перед началом работы выставите необходимое количество параллельных потоков, которые будут задействованы во время работы.

2.6.7 Утилиты для работы со словарями

Довольно скудное количество приемлемых утилит для работы со специализированными словарями паролей, сподвигло 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.

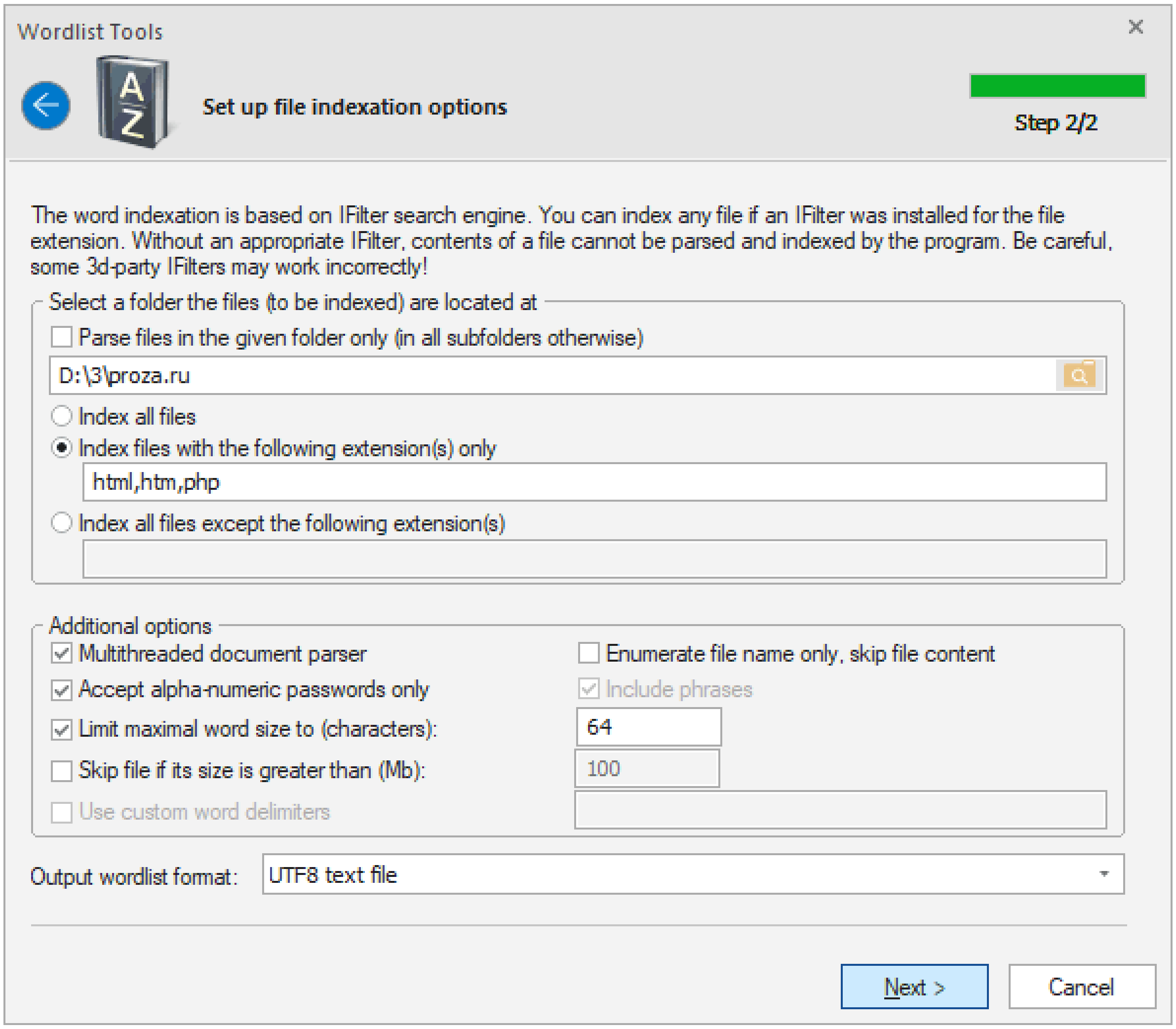
2.6.7.1 Создание словаря путем индексации локальных файлов

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, Windows Password Recovery имеет встроенную поддержку следующих типов файлов:
архивы: *.zip, *,cab, *.rar, *.7z
программы: *.exe, *.dll, *,cpl, *.ocx, *.sys, *.scr, *.drv
текст: *.txt, *.dic, *.udic, *.utf
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 оф. сайта Microsoft.



The word indexation is based on IFilter search engine. You can index any file if an IFilter was installed for the file extension. Without an appropriate IFilter, contents of a file cannot be parsed and indexed by the program. Be careful, some 3d-party IFilters may work incorrectly!

Select a folder the files (to be indexed) are located at

□ Parse files in the given folder only (in all subfolders otherwise)

D:\3\proza.ru

○ Index all files

● Index files with the following extension(s) only

html,htm,php

○ Index all files except the following extension(s)

Additional options

☑ Multithreaded document parser

☑ Accept alpha-numeric passwords only

☑ Limit maximal word size to (characters): 64

□ Skip file if its size is greater than (Mb): 100

□ Use custom word delimiters

□ Enumerate file name only, skip file content

☑ Include phrases

Output wordlist format: UTF8 text file

Настройка этого инструмента состоит из двух групп. В первой группе необходимо установить путь к начальному 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:

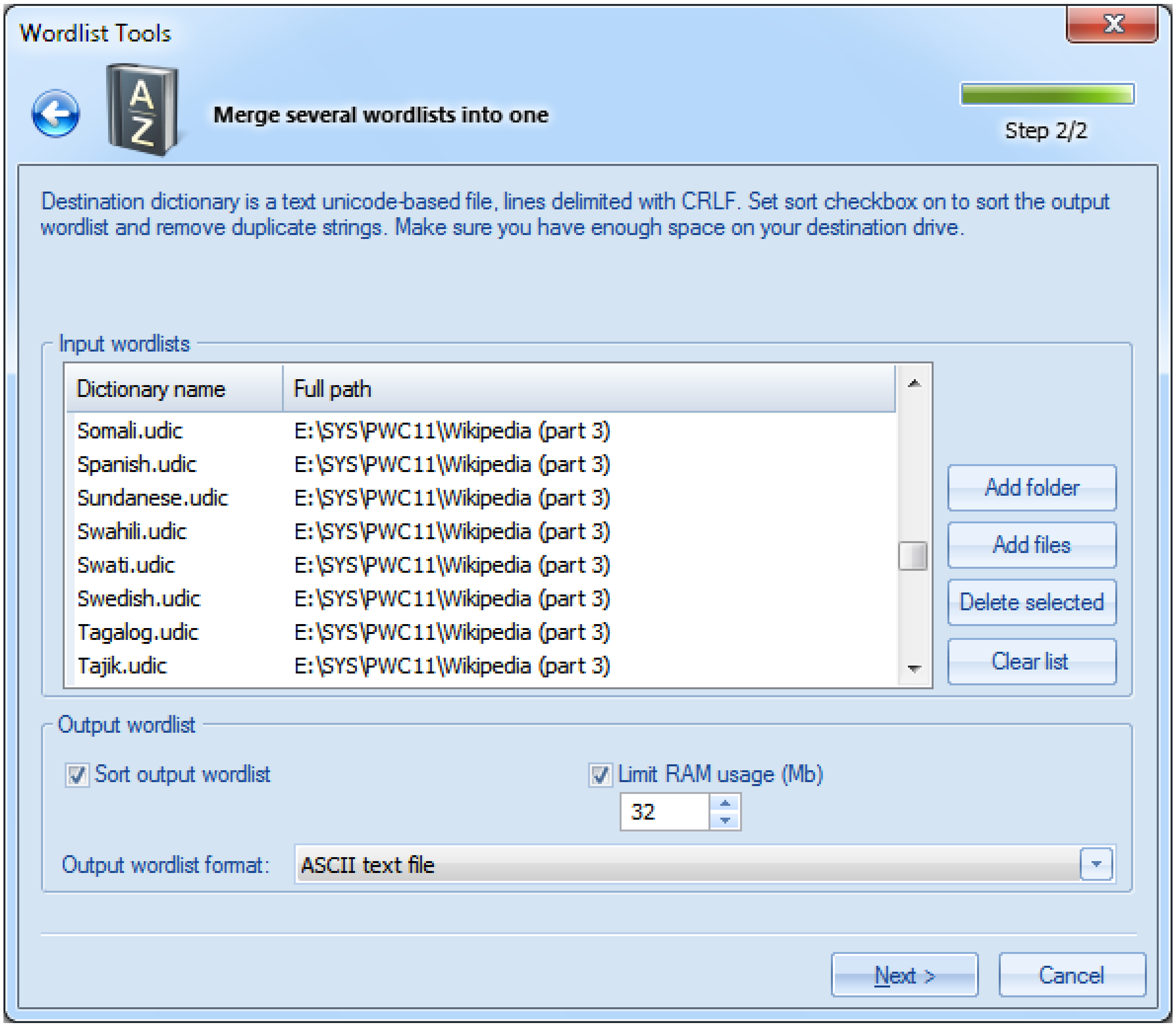
- Многопоточная обработка документов. Эта настройка, если включена, позволяет значительно увеличить скорость создания словарей путем задействования всех ядер процессора при обработке данных.
- Брать только имена файлов, пропускать содержимое. Если включить эту опцию, то для создания словарей программа будет брать только имена найденных файлов, игнорируя их содержимое.
- 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 16-64 знаков. Уменьшение максимальной длины приводит, иногда довольно значительно, к увеличению скорости обработки файлов. Не лишним будет напомнить, что максимальная длина пароля в Windows составляет 128 символов.
- 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 создается 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.

2.6.7.2 Слияние словарей

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



Merge several wordlists into one

Destination dictionary is a text unicode-based file, lines delimited with CRLF. Set sort checkbox on to sort the output wordlist and remove duplicate strings. Make sure you have enough space on your destination drive.

Input wordlists

Dictionary name	Full path
Somali.udic	E:\SYS\PWC11\Wikipedia (part 3)
Spanish.udic	E:\SYS\PWC11\Wikipedia (part 3)
Sundanese.udic	E:\SYS\PWC11\Wikipedia (part 3)
Swahili.udic	E:\SYS\PWC11\Wikipedia (part 3)
Swati.udic	E:\SYS\PWC11\Wikipedia (part 3)
Swedish.udic	E:\SYS\PWC11\Wikipedia (part 3)
Tagalog.udic	E:\SYS\PWC11\Wikipedia (part 3)
Tajik.udic	E:\SYS\PWC11\Wikipedia (part 3)

Output wordlist

☑ Sort output wordlist

☑ Limit RAM usage (Mb): 32

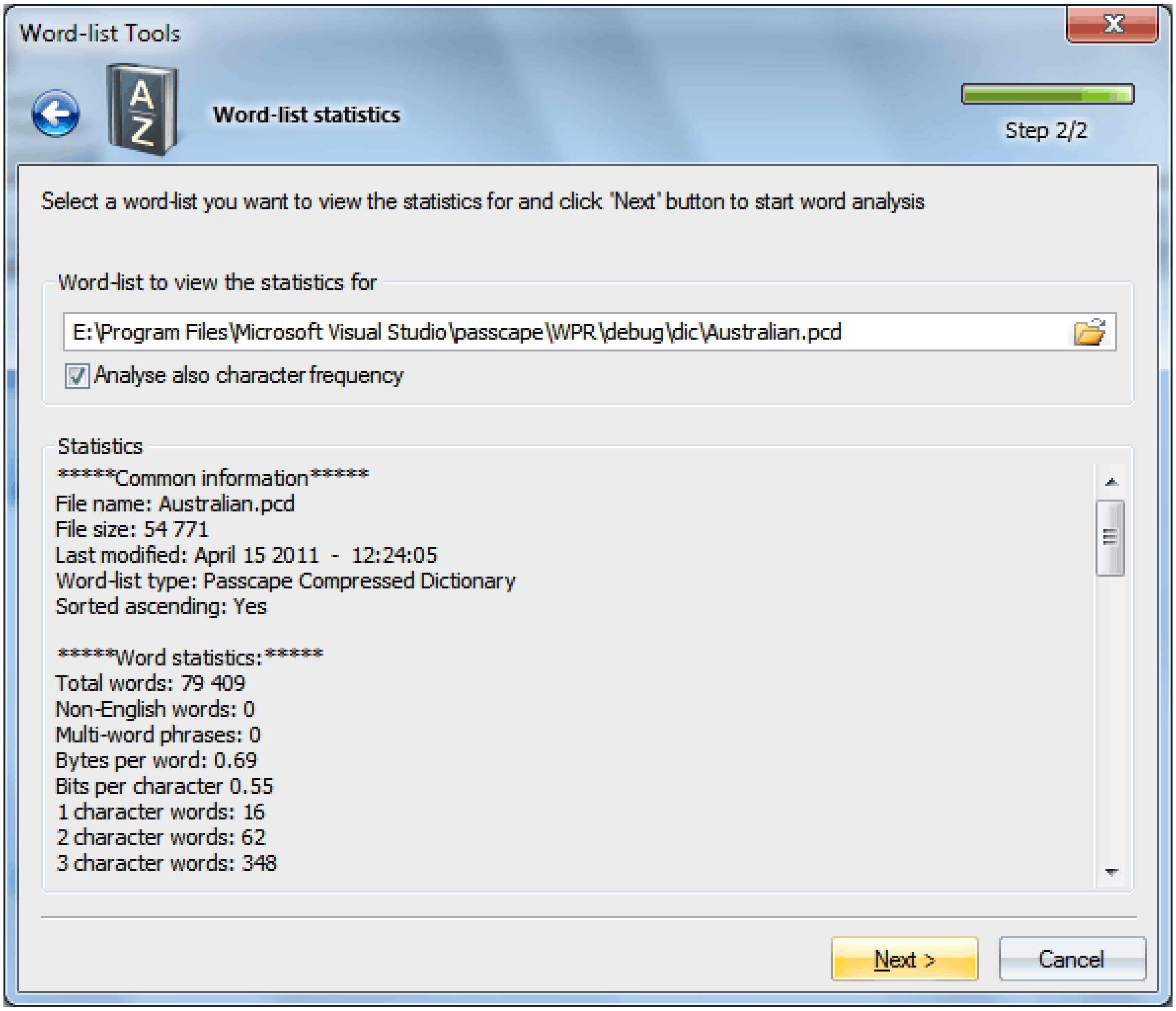
Output wordlist format: ASCII text file

Если опция сортировки выходного словаря не установлена, то слияние происходит путем 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).

2.6.7.3 Анализ словаря

Анализ словаря собирает и показывает следующую статистику:



Select a word-list you want to view the statistics for and click "Next" button to start word analysis

Word-list to view the statistics for

E:\Program Files\Microsoft Visual Studio\passcape\WPR\debug\dic\Australian.pcd

☑ Analyse also character frequency

Statistics

```
*****Common information*****
File name: Australian.pcd
File size: 54 771
Last modified: April 15 2011  -  12:24:05
Word-list type: Passcape Compressed Dictionary
Sorted ascending: Yes

*****Word statistics:*****
Total words: 79 409
Non-English words: 0
Multi-word phrases: 0
Bytes per word: 0.69
Bits per character 0.55
1 character words: 16
2 character words: 62
3 character words: 348
```

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

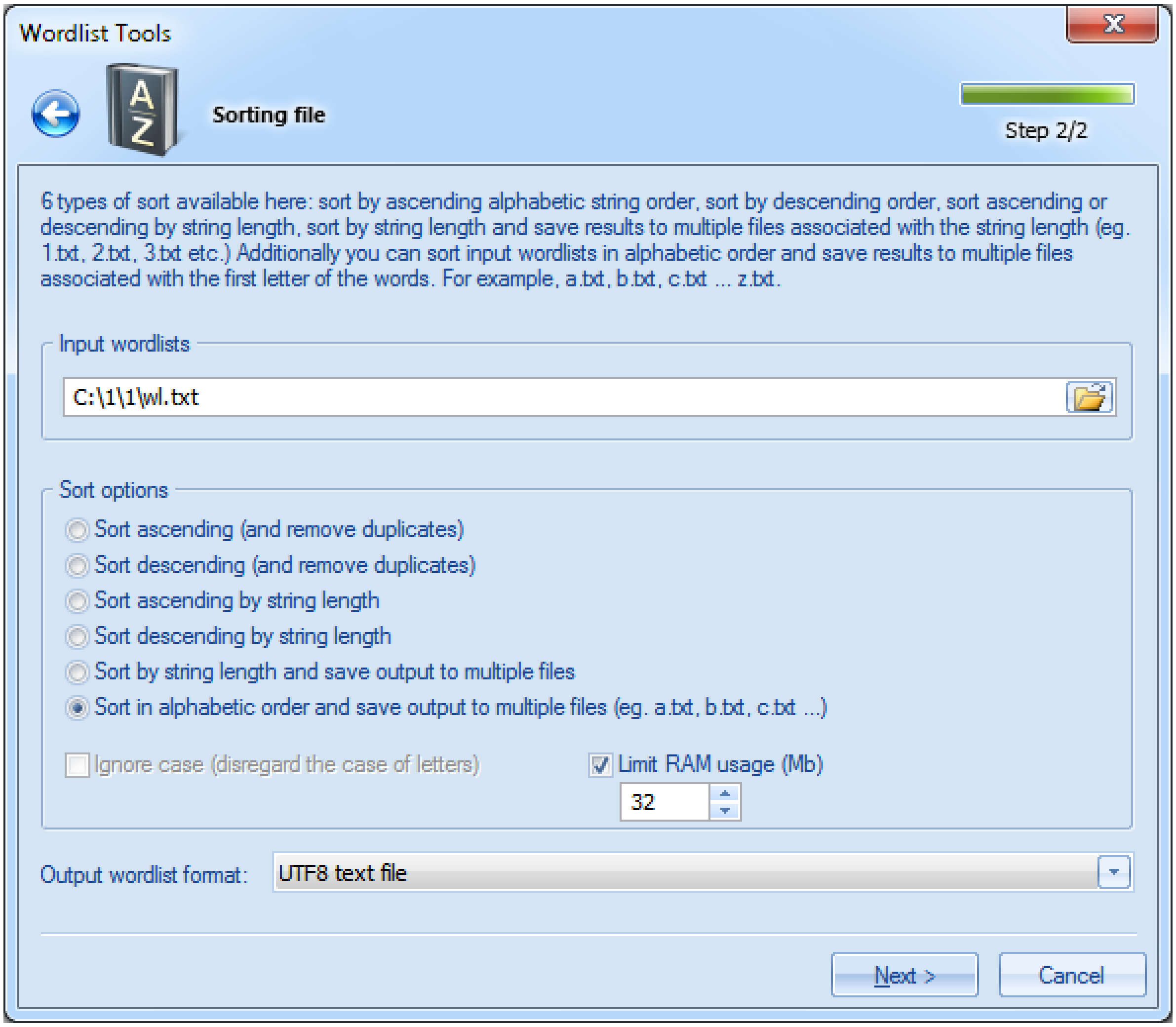
- Общее количество слов
- Количество неанглийских слов
- Количество фраз, т.е. слов, отделенных пробелом
- Количество байт на одно слово, без учета разделителя слов. Показывает среднюю степень сжатия словаря.
- Количество бит на один символ. Показывает реальную степень сжатия словаря. Например, в UNICODE словаре количество бит на букву будет стремиться к 16 (разделитель слов не учитывается при подсчете), 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

2.6.7.4 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.



6 types of sort available here: sort by ascending alphabetic string order, sort by descending order, sort ascending or descending by string length, sort by string length and save results to multiple files associated with the string length (eg. 1.txt, 2.txt, 3.txt etc.) Additionally you can sort input wordlists in alphabetic order and save results to multiple files associated with the first letter of the words. For example, a.txt, b.txt, c.txt ... z.txt.

Input wordlists

C:\1\1\wl.txt

Sort options

○ Sort ascending (and remove duplicates)
○ Sort descending (and remove duplicates)
○ Sort ascending by string length
○ Sort descending by string length
○ Sort by string length and save output to multiple files
● Sort in alphabetic order and save output to multiple files (eg. a.txt, b.txt, c.txt ...)

□ Ignore case (disregard the case of letters)   ☑ Limit RAM usage (Mb) 32

Output wordlist format: UTF8 text file

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 создается 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.

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

Сортировка больших файлов (поддерживаются файлы объемом 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.

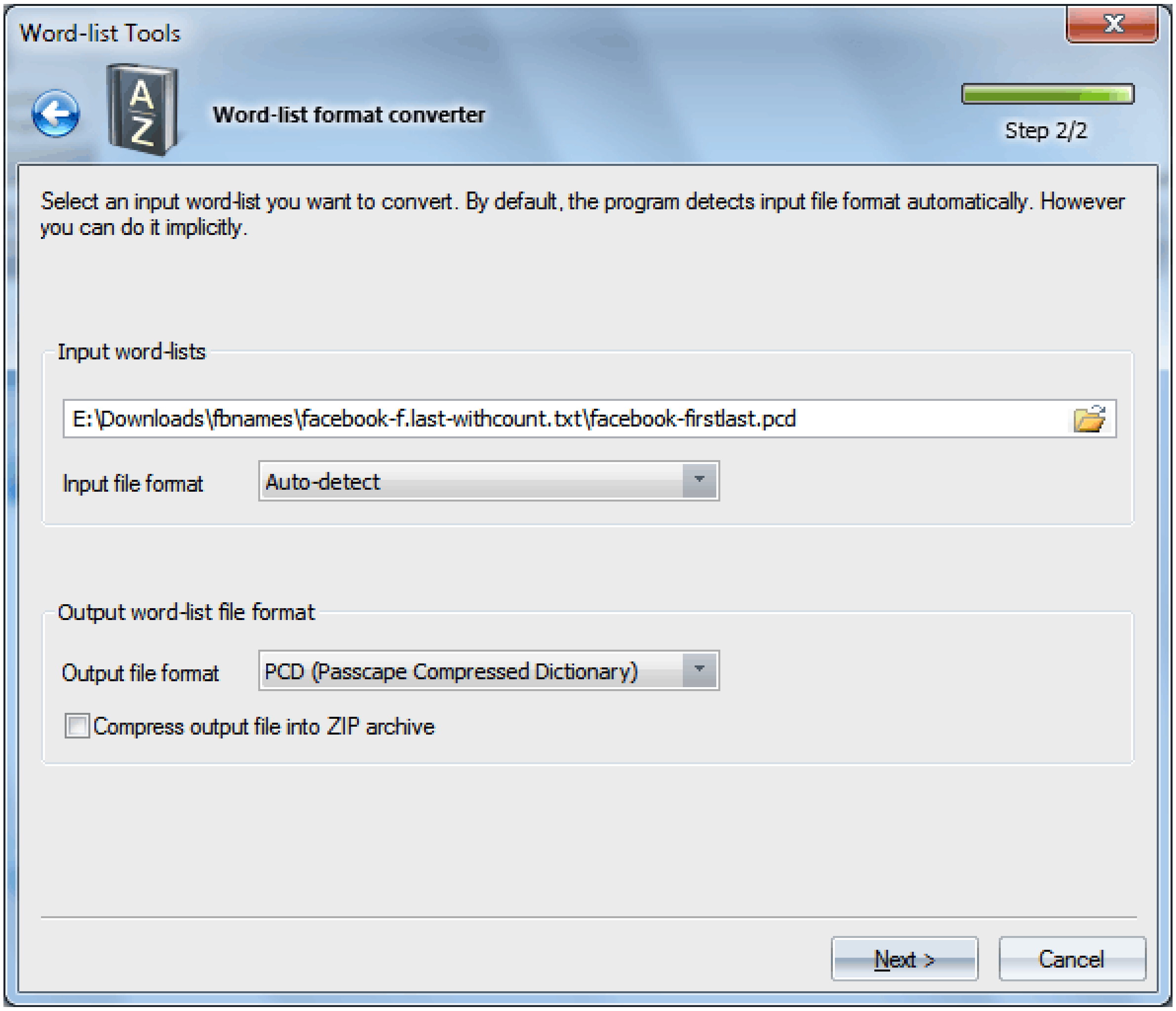
Имя целевого словаря может совпадать с исходным, однако это делать не рекомендуется.

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

2.6.7.5 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 трех вышеупомянутых форматов, программа имеет поддержку своего собственного формата PCD (Passcape Compressed Dictionary), который в большинстве случаев, дает больший выигрыш в размере даже по сравнению со сжатым ZIP архивом.

Создание больших PCD файлов может потребовать значительное время!



Select an input word-list you want to convert. By default, the program detects input file format automatically. However you can do it implicitly.

Input word-lists

E:\Downloads\fbnames\facebook-f.last-withcount.txt\facebook-firstlast.pcd

Input file format: Auto-detect

Output word-list file format

Output file format: PCD (Passcape Compressed Dictionary)

□ Compress output file into ZIP archive

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.

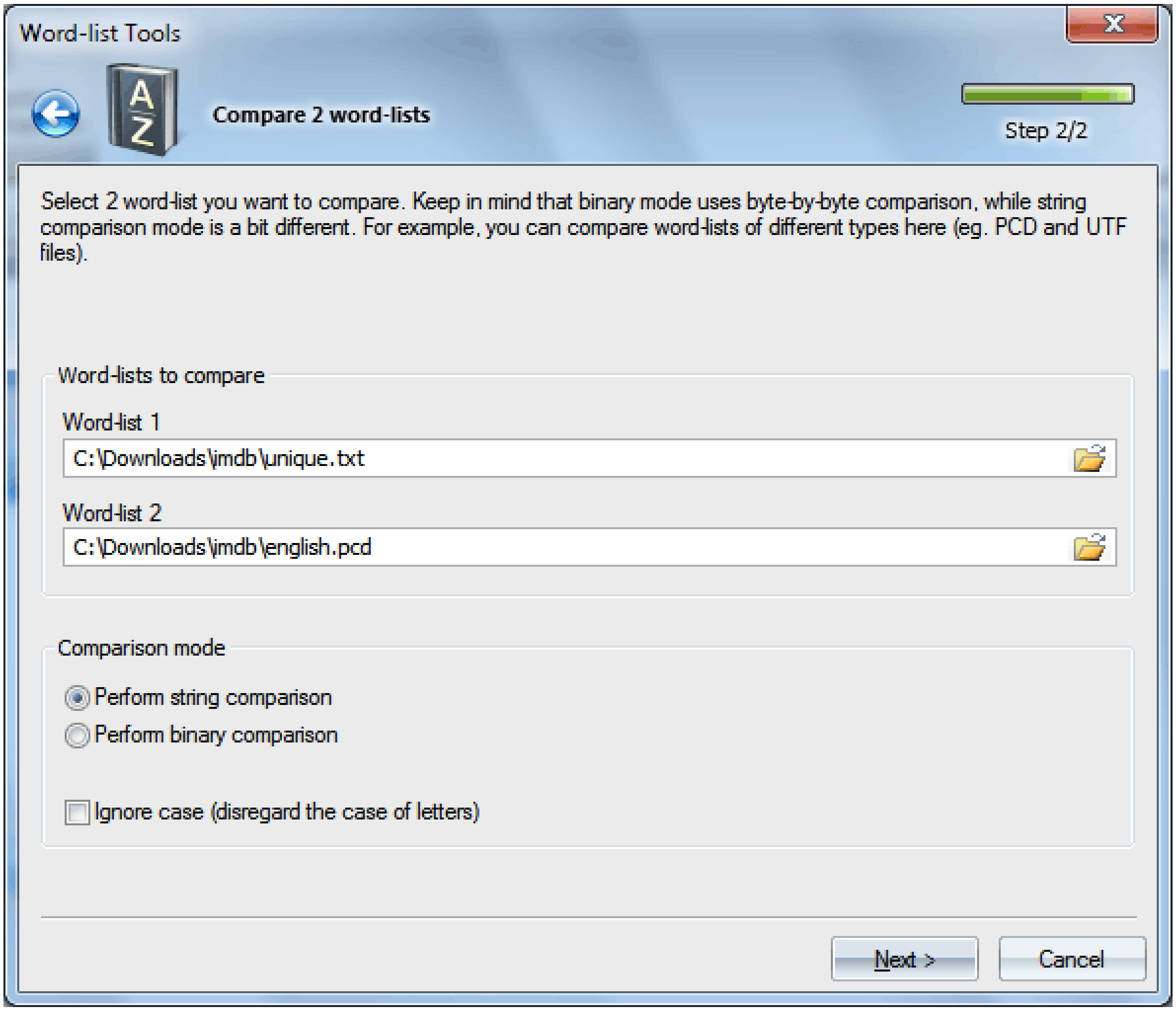
Если формат PCD файла распознается однозначно, то с текстовыми файлами не все так просто. Как правило, текстовые файлы/словари в формате UTF16 или UTF8 имеют в начале двух- или трех-байтовый маркер, описывающий тип файла. Однако, встречаются Юникодные словари без определительных маркеров. Для таких 'тяжелых'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

Целевой словарь аналогично задается одним из четырех описанных выше форматов. Установленная опция компрессии дополнительно сожмет выходной файл в ZIP архив.

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

2.6.7.6 Сравнение словарей

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



Select 2 word-list you want to compare. Keep in mind that binary mode uses byte-by-byte comparison, while string comparison mode is a bit different. For example, you can compare word-lists of different types here (eg. PCD and UTF files).

Word-lists to compare

Word-list 1: C:\Downloads\imdb\unique.txt

Word-list 2: C:\Downloads\imdb\english.pcd

Comparison mode

● Perform string comparison

○ Perform binary comparison

□ Ignore case (disregard the case of letters)

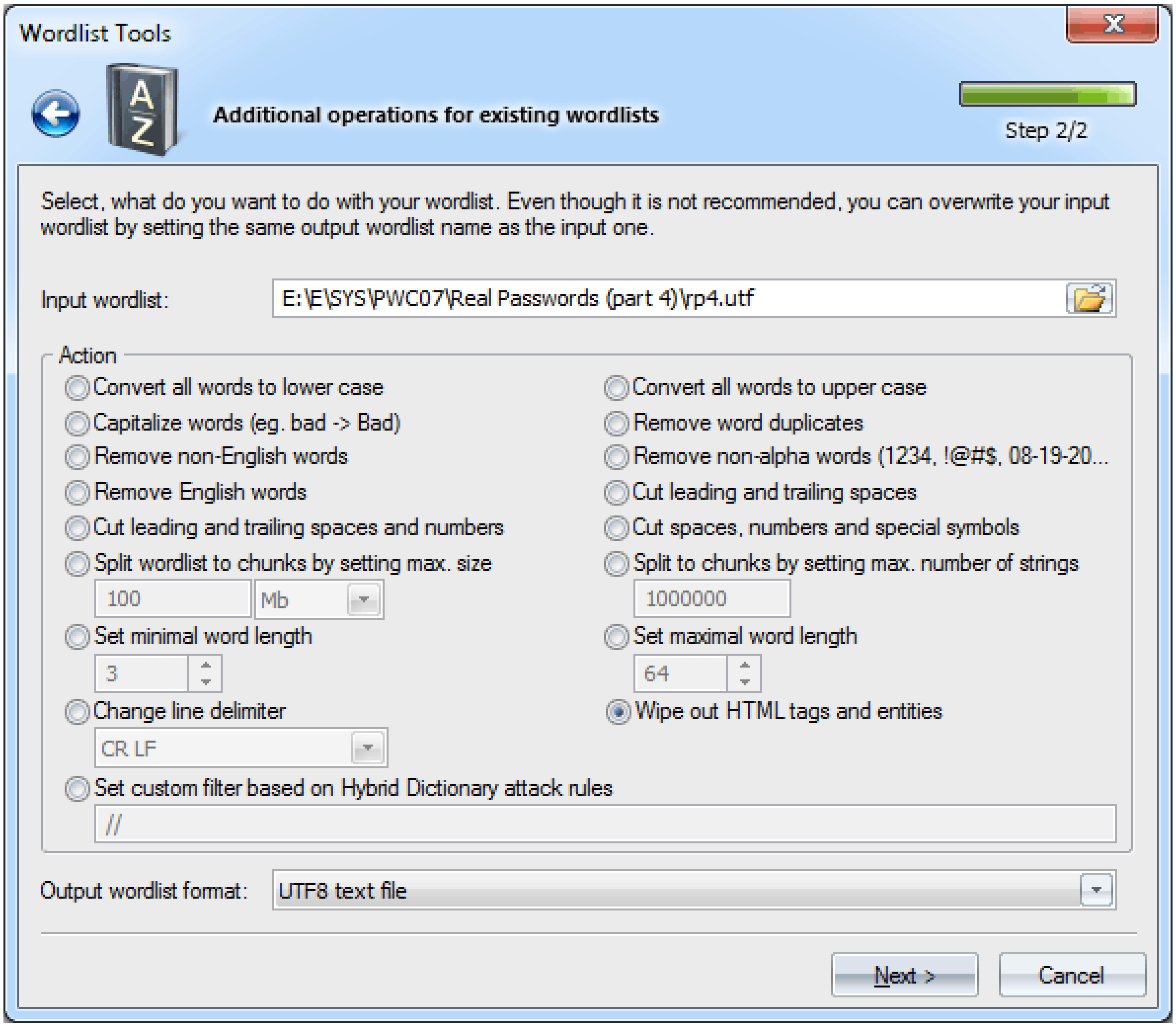
В данном инструменте предусмотрены два режима работы:

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.

2.6.7.7 Дополнительные инструменты

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



Wordlist Tools

Additional operations for existing wordlists

Step 2/2

Select, what do you want to do with your wordlist. Even though it is not recommended, you can overwrite your input wordlist by setting the same output wordlist name as the input one.

Input wordlist: E:\E\SYS\PWC07\Real Passwords (part 4)\rp4.utf

Action

○ Convert all words to lower case
○ Convert all words to upper case
○ Capitalize words (eg. bad -> Bad)
○ Remove word duplicates
○ Remove non-English words
○ Remove non-alpha words (1234, !@#$, 08-19-20...
○ Remove English words
○ Cut leading and trailing spaces
○ Cut leading and trailing spaces and numbers
○ Cut spaces, numbers and special symbols
○ Split wordlist to chunks by setting max. size: 100 Mb
○ Split to chunks by setting max. number of strings: 1000000
○ Set minimal word length: 3
○ Set maximal word length: 64
○ Change line delimiter: CR LF
● Wipe out HTML tags and entities
○ Set custom filter based on Hybrid Dictionary attack rules: //

Output wordlist format: UTF8 text file

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
- Удаление HTML тэгов и мусора. Этот пункт также производит конвертирование HTML объектов. Например, **&amp;** -> **&** или **&#064;** -> **@**
- Установка своего собственного фильтра на основе правил Гибридной Атаки по словарю

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

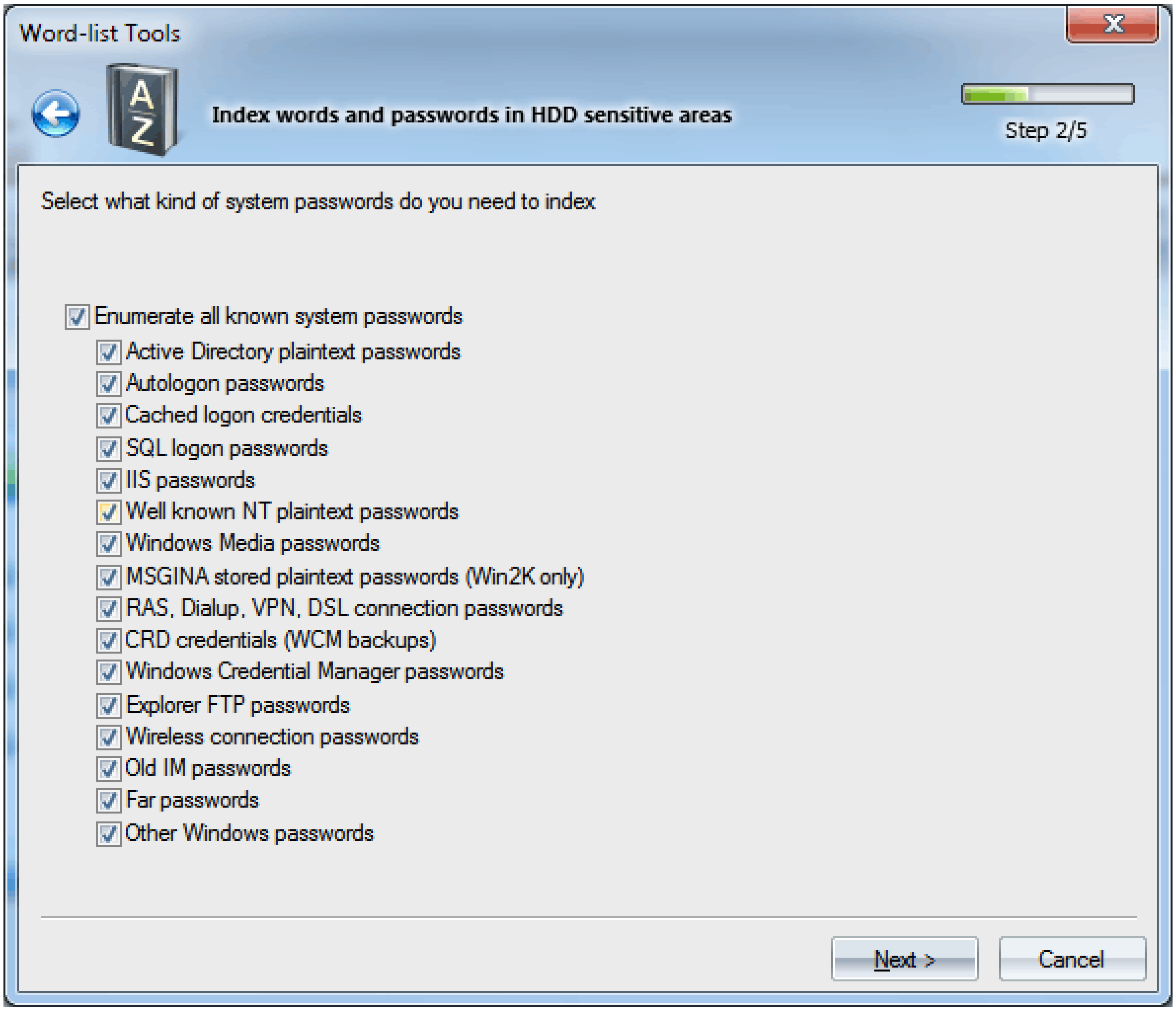
Имена исходного и целевого словаря могут быть одинаковыми (не рекомендуется). При этом исходный словарь будет перезаписан.

2.6.7.8 Индексация жесткого диска

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

Часто пользователи, не отдавая себе отчета, задают одинаковые пароли для учетной 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 учетных записей. Эта технология используется в Интеллектуальной атаке.

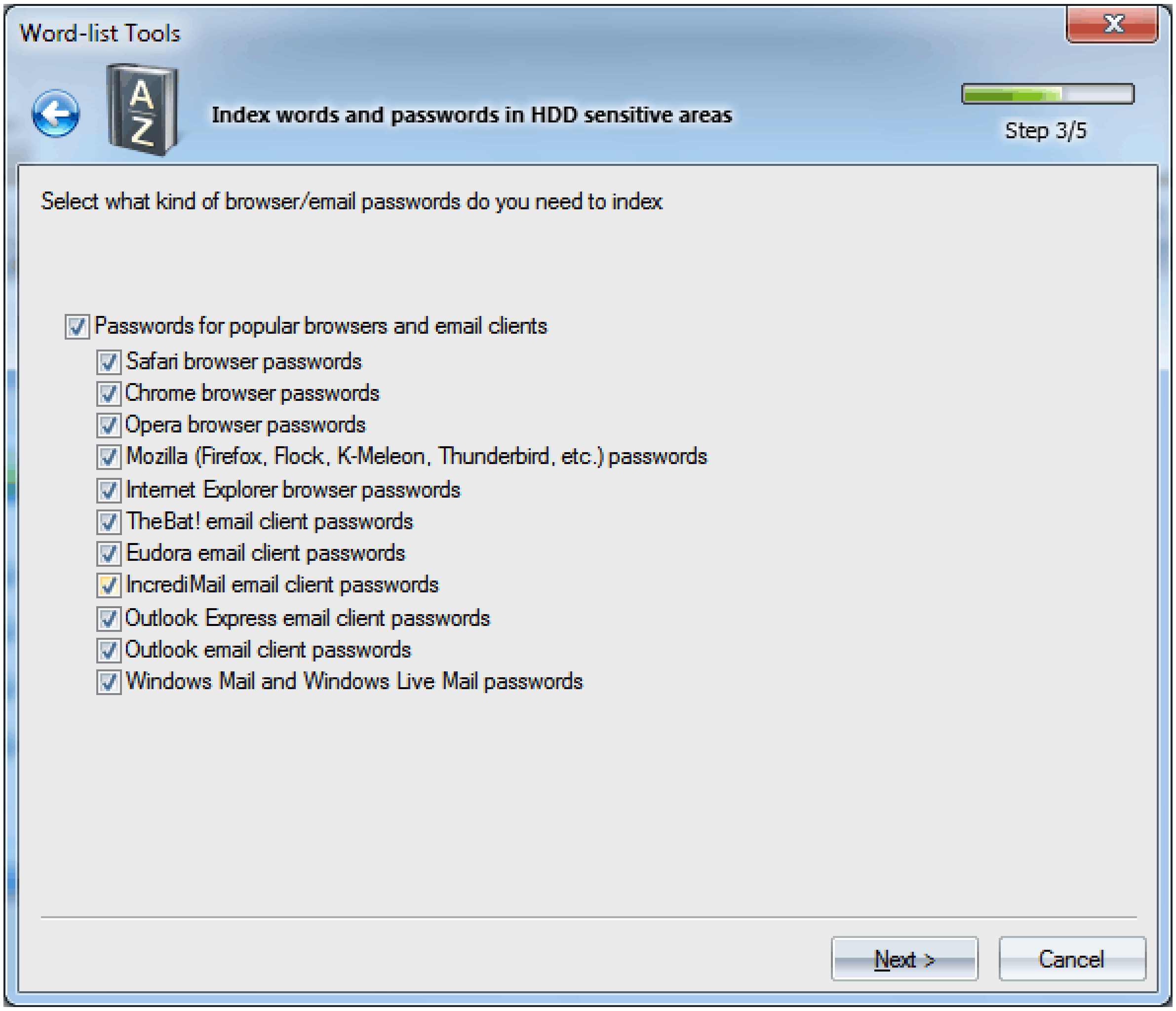
Настройка инструмента условно состоит из четырех частей:



Select what kind of system passwords do you need to index

- ☑ Enumerate all known system passwords
  - ☑ Active Directory plaintext passwords
  - ☑ Autologon passwords
  - ☑ Cached logon credentials
  - ☑ SQL logon passwords
  - ☑ IIS passwords
  - ☑ Well known NT plaintext passwords
  - ☑ Windows Media passwords
  - ☑ MSGINA stored plaintext passwords (Win2K only)
  - ☑ RAS, Dialup, VPN, DSL connection passwords
  - ☑ CRD credentials (WCM backups)
  - ☑ Windows Credential Manager passwords
  - ☑ Explorer FTP passwords
  - ☑ Wireless connection passwords
  - ☑ Old IM passwords
  - ☑ Far passwords
  - ☑ Other Windows passwords

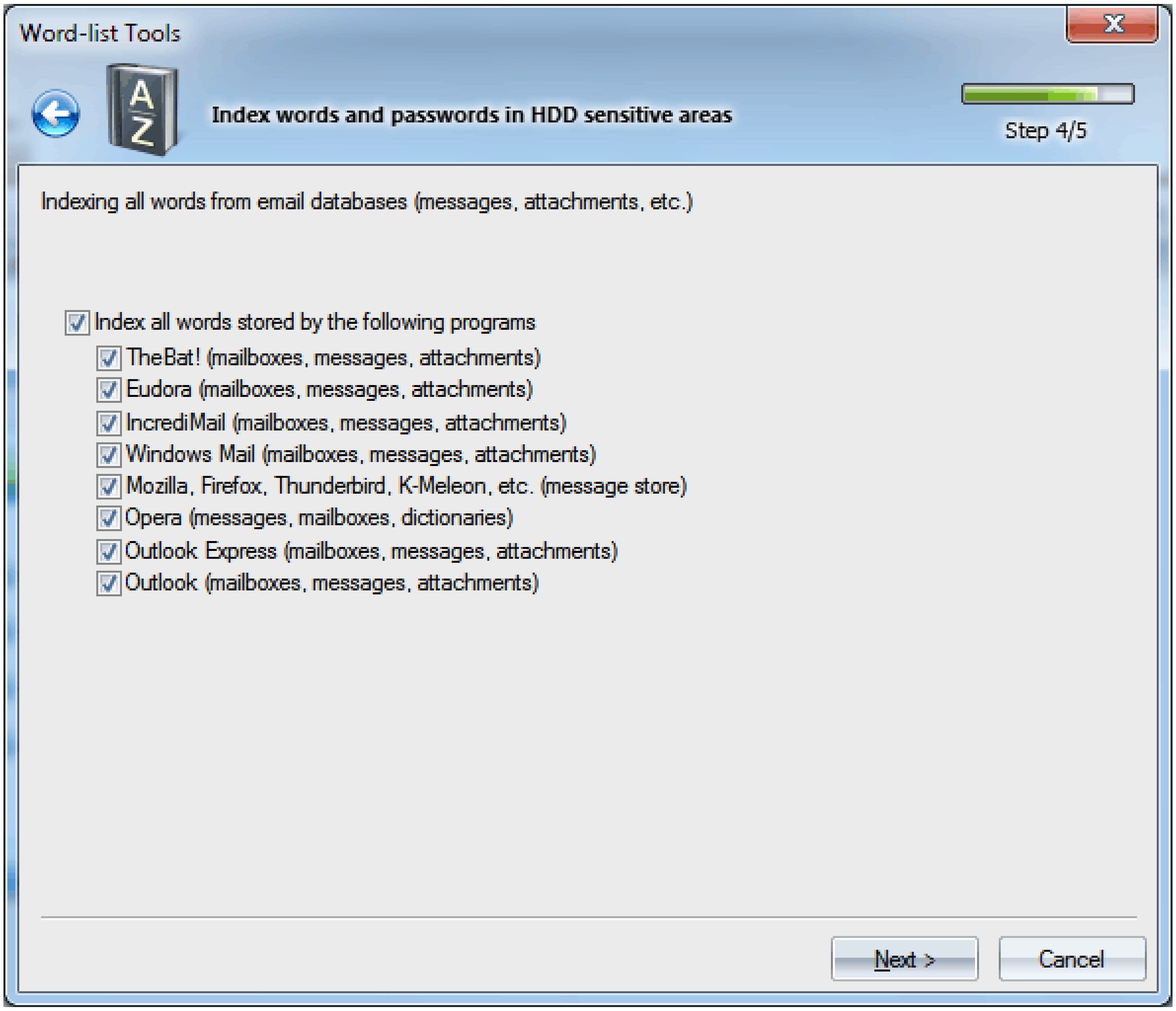
Вначале, необходимо выбрать список системных модулей, которые будут задействованы при создании словаря. Эти модули производят поиск и индексацию следующих видов паролей на жестком диске вашего компьютера: текстовые пароли Active Directory, пароли автозагрузки и кэшированные пароли автозагрузки, SQL, 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.



Select what kind of browser/email passwords do you need to index

- ☑ Passwords for popular browsers and email clients
  - ☑ Safari browser passwords
  - ☑ Chrome browser passwords
  - ☑ Opera browser passwords
  - ☑ Mozilla (Firefox, Flock, K-Meleon, Thunderbird, etc.) passwords
  - ☑ Internet Explorer browser passwords
  - ☑ TheBat! email client passwords
  - ☑ Eudora email client passwords
  - ☑ IncrediMail email client passwords
  - ☑ Outlook Express email client passwords
  - ☑ Outlook email client passwords
  - ☑ Windows Mail and Windows Live Mail passwords

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.



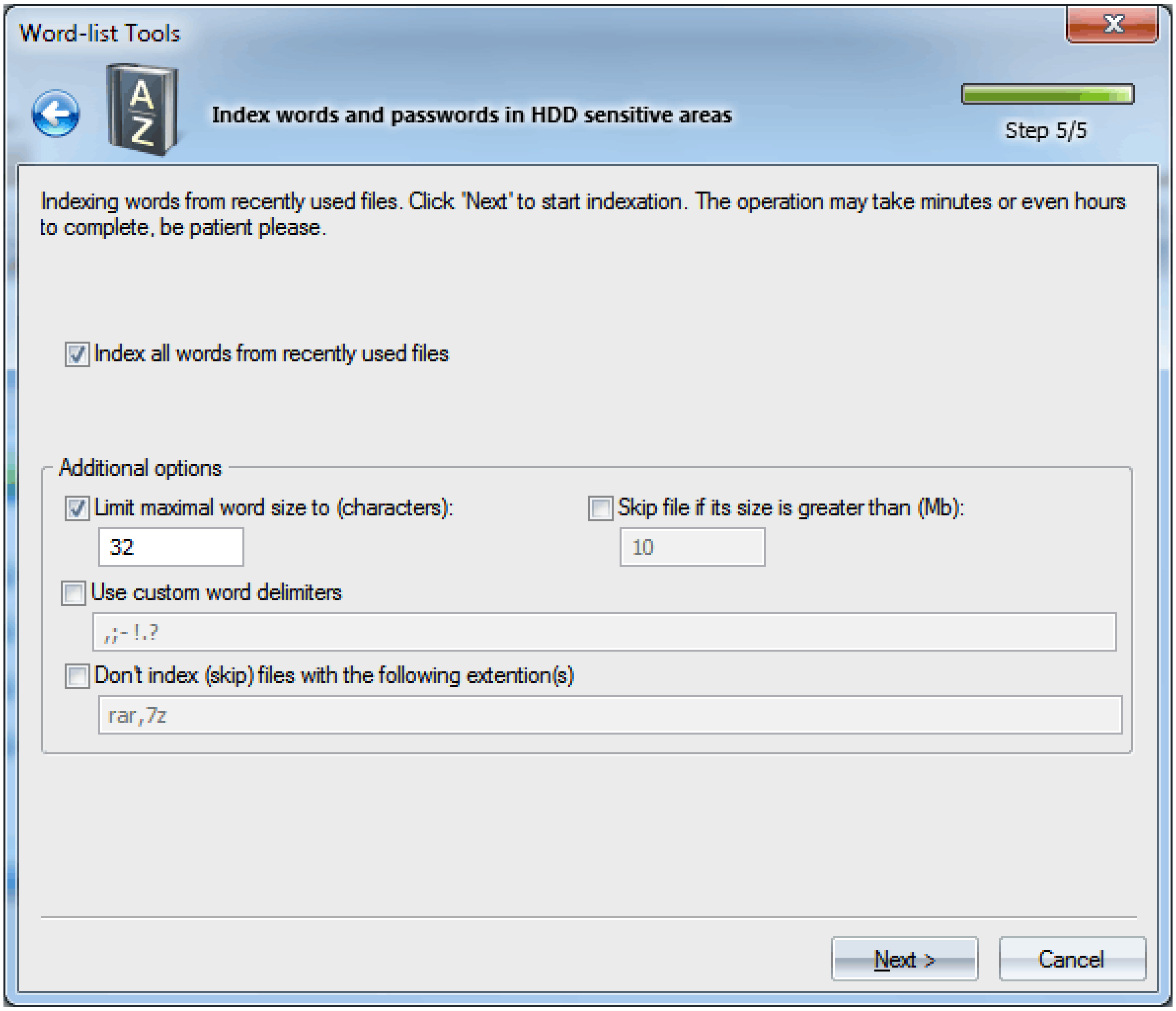
Index words and passwords in HDD sensitive areas

Indexing all words from email databases (messages, attachments, etc.)

☑ Index all words stored by the following programs

- ☑ TheBat! (mailboxes, messages, attachments)
- ☑ Eudora (mailboxes, messages, attachments)
- ☑ IncrediMail (mailboxes, messages, attachments)
- ☑ Windows Mail (mailboxes, messages, attachments)
- ☑ Mozilla, Firefox, Thunderbird, K-Meleon, etc. (message store)
- ☑ Opera (messages, mailboxes, dictionaries)
- ☑ Outlook Express (mailboxes, messages, attachments)
- ☑ Outlook (mailboxes, messages, attachments)

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 учетных 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.



Word-list Tools

Index words and passwords in HDD sensitive areas

Step 5/5

Indexing words from recently used files. Click 'Next' to start indexation. The operation may take minutes or even hours to complete, be patient please.

☑ Index all words from recently used files

Additional options

☑ Limit maximal word size to (characters): 32

☐ Skip file if its size is greater than (Mb): 10

☐ Use custom word delimiters ,;- !.?

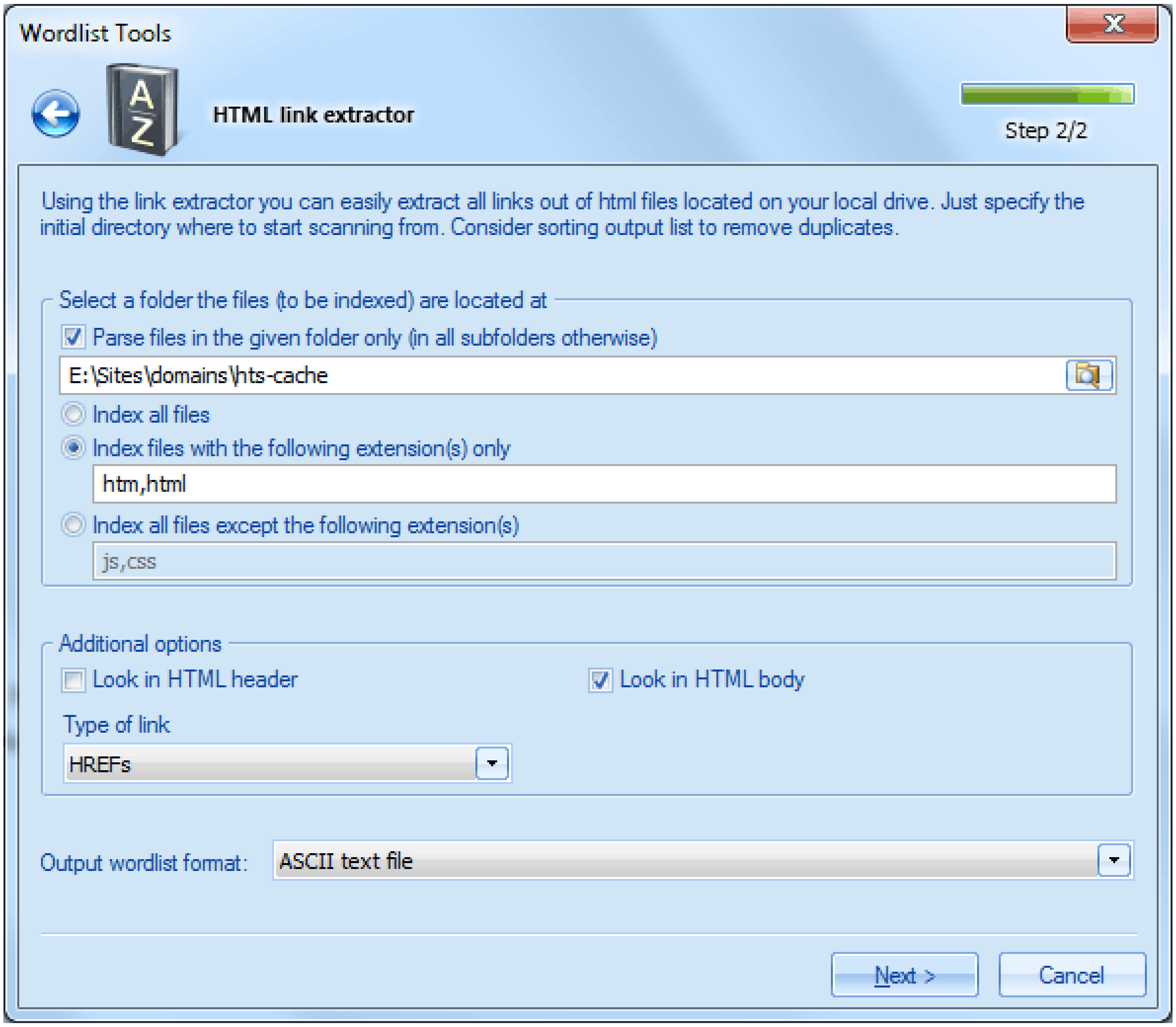
☐ Don't index (skip) files with the following extention(s) rar,7z

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 задается 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>, начнется индексирование.
Имейте в виду, этот процесс может занять значительное время!

2.6.7.9 Поиск HTML ссылок

Эта утилита была разработана для вытаскивания ссылок из HTML файлов.



Wordlist Tools

HTML link extractor

Step 2/2

Using the link extractor you can easily extract all links out of html files located on your local drive. Just specify the initial directory where to start scanning from. Consider sorting output list to remove duplicates.

Select a folder the files (to be indexed) are located at

☑ Parse files in the given folder only (in all subfolders otherwise)

E:\Sites\domains\hts-cache

○ Index all files

● Index files with the following extension(s) only

htm,html

○ Index all files except the following extension(s)

js,css

Additional options

□ Look in HTML header ☑ Look in HTML body

Type of link: HREFs

Output wordlist format: ASCII text file

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.

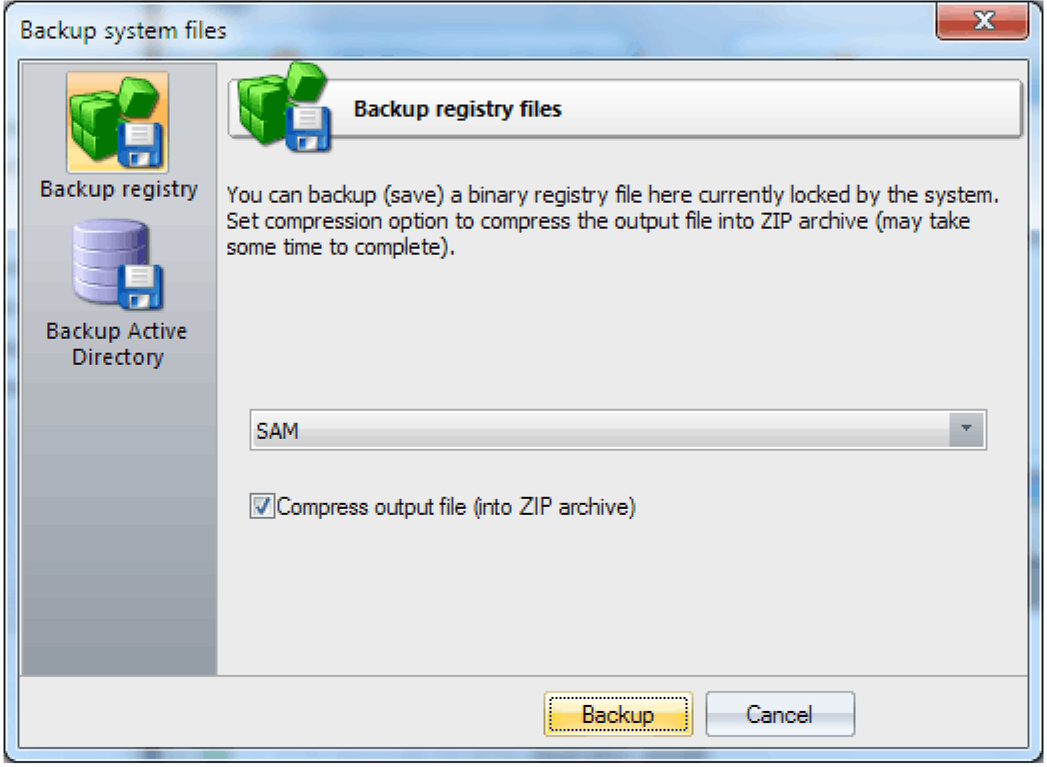
Нажатие кнопки **Next>** запускает процесс поиска, который может занять значительное время. После завершения операции и сохранения найденного списка ссылок на диск, необходимо отсортировать его, чтобы избавиться от дубликатов.

2.7 Меню Утилиты

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

2.7.1 Резервное копирование системных файлов

Инструмент сохранения реестра позволяет легко создать резервные копии рабочих файлов реестра вашей операционной системы. Причем даже если эти файлы заблокирован. Можно установить дополнительную опцию сжатия для создания ZIP архива.

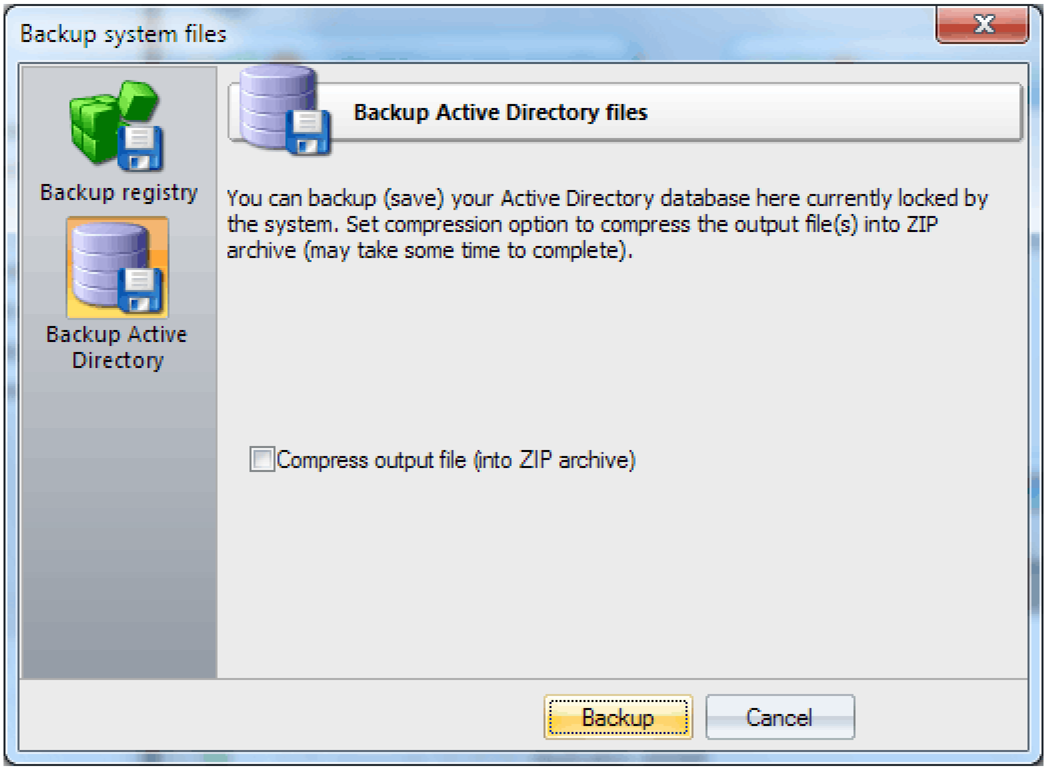


You can backup (save) a binary registry file here currently locked by the system. Set compression option to compress the output file into ZIP archive (may take some time to complete).

SAM

☑ Compress output file (into ZIP archive)

Создание резервной копии Active Directory аналогично реестру. Путь к базе данных Active Directory программа определяет сама.



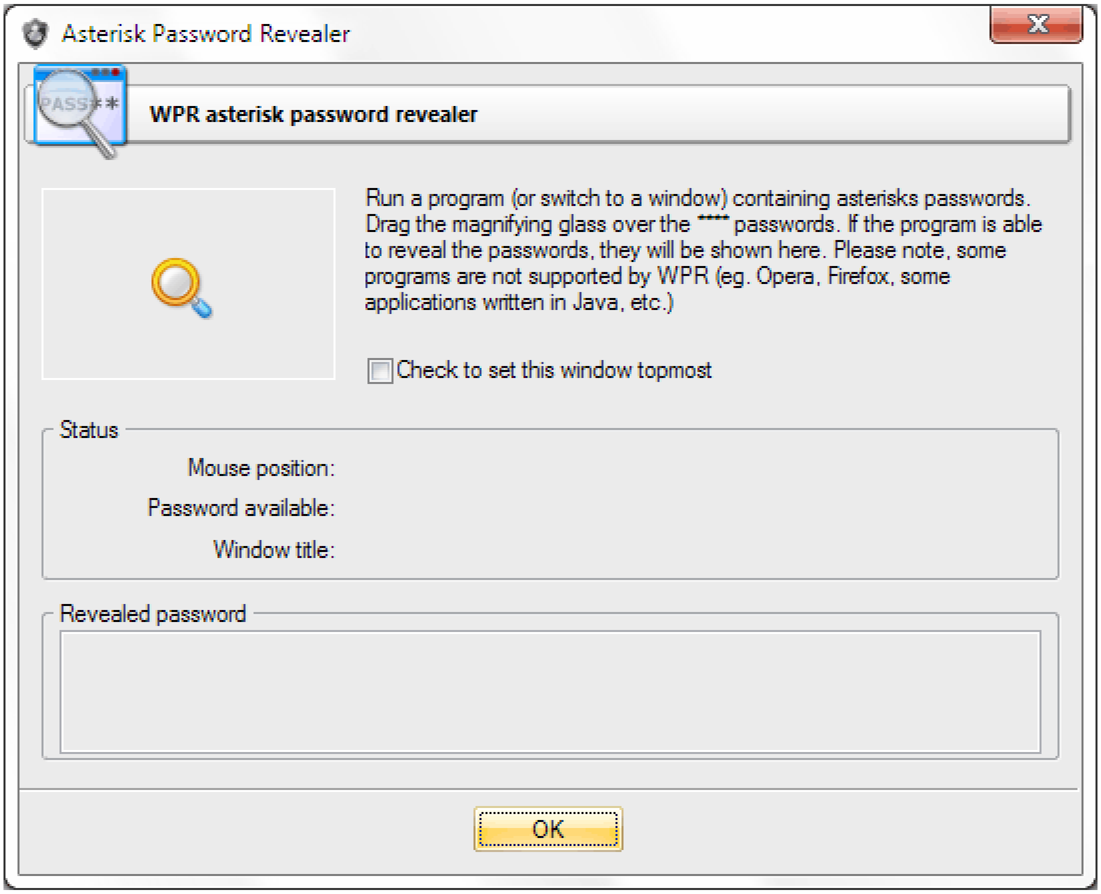
You can backup (save) your Active Directory database here currently locked by the system. Set compression option to compress the output file(s) into ZIP archive (may take some time to complete).

□ Compress output file (into ZIP archive)

Для работы этого инструмента требуются права администратора или backup оператора.

Создание и сохранение резервной копии Active Directory может занять значительное время (несколько десятков минут и даже более для больших баз).

2.7.2 Открыватель паролей за звездочками ***



Run a program (or switch to a window) containing asterisks passwords. Drag the magnifying glass over the **** passwords. If the program is able to reveal the passwords, they will be shown here. Please note, some programs are not supported by WPR (eg. Opera, Firefox, some applications written in Java, etc.)

□ Check to set this window topmost

Status

Mouse position:

Password available:

Window title:

Revealed password

Данный инструмент позволяет открывать пароли, которые прячутся за звездочками. 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 Windows Password Recovery на поле со звездочками.

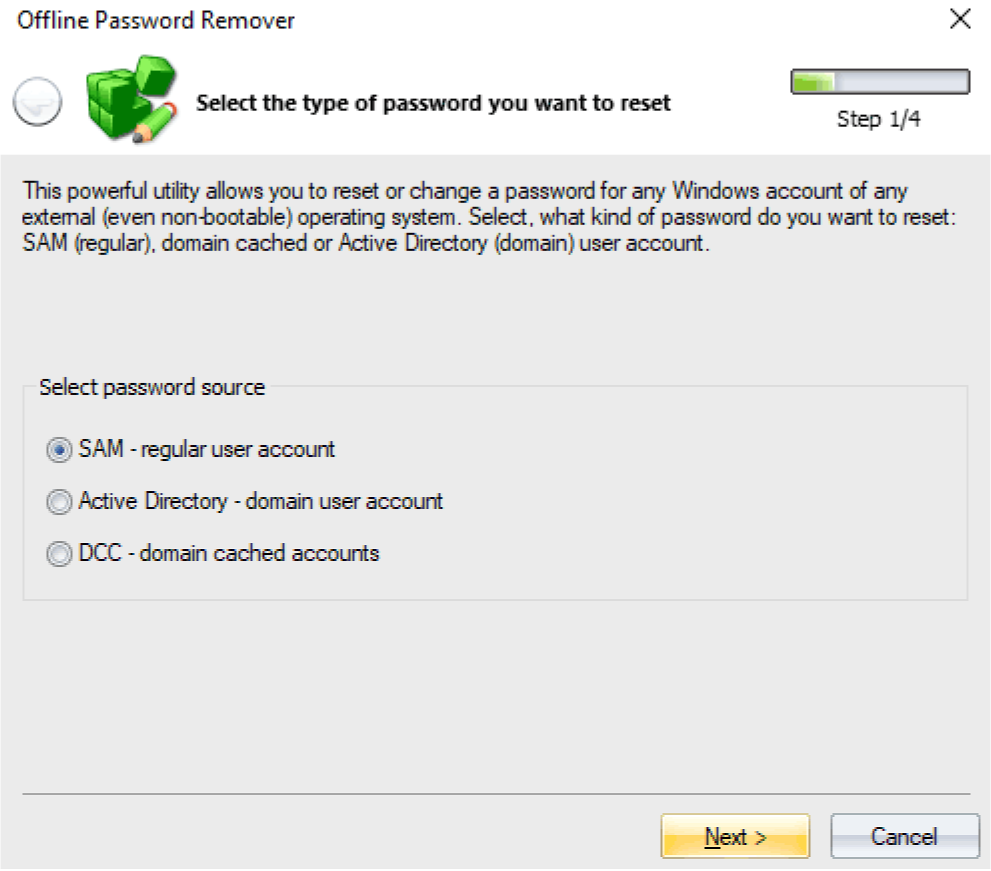
Однако эта утилита имеет ряд ограничений:
Некоторые программы имеют свой собственный GUI, поэтому asterisks revealer не работает на таких программах. К ним относятся браузеры Opera, Mozilla, Firefox и т.д.
Некоторые Веб сайты имеют встроенную защиту, которая за звездочками прячет либо чепуху, либо там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

Для корректной работы этого инструмента требуется наличие привилегий администратора.

2.7.3 Сброс паролей

Полезный плагин для сброса или изменения паролей напрямую в файле реестра SAM/SECURITY или в NTDS.DIT. Например, чтобы получить доступ к заблокированной системе, совсем не обязательно восстанавливать пароль на вход Windows. Достаточно скопировать файлы реестра SAM и SYSTEM, с помощью этого плагина сбросить пароль нужной учетной записи (или сбросить флаг блокировки) и скопировать эти файлы обратно. Плагин сброса паролей выполнен в виде мастера и состоит из 4 шагов:

1. На первом этапе необходимо выбрать источник пароля. Это может быть либо SAM файл - для обычных учетных записей, SECURITY файл - для кэшированных записей домена или NTDS.DIT - для паролей в домене.



Offline Password Remover

Select the type of password you want to reset

Step 1/4

This powerful utility allows you to reset or change a password for any Windows account of any external (even non-bootable) operating system. Select, what kind of password do you want to reset: SAM (regular), domain cached or Active Directory (domain) user account.

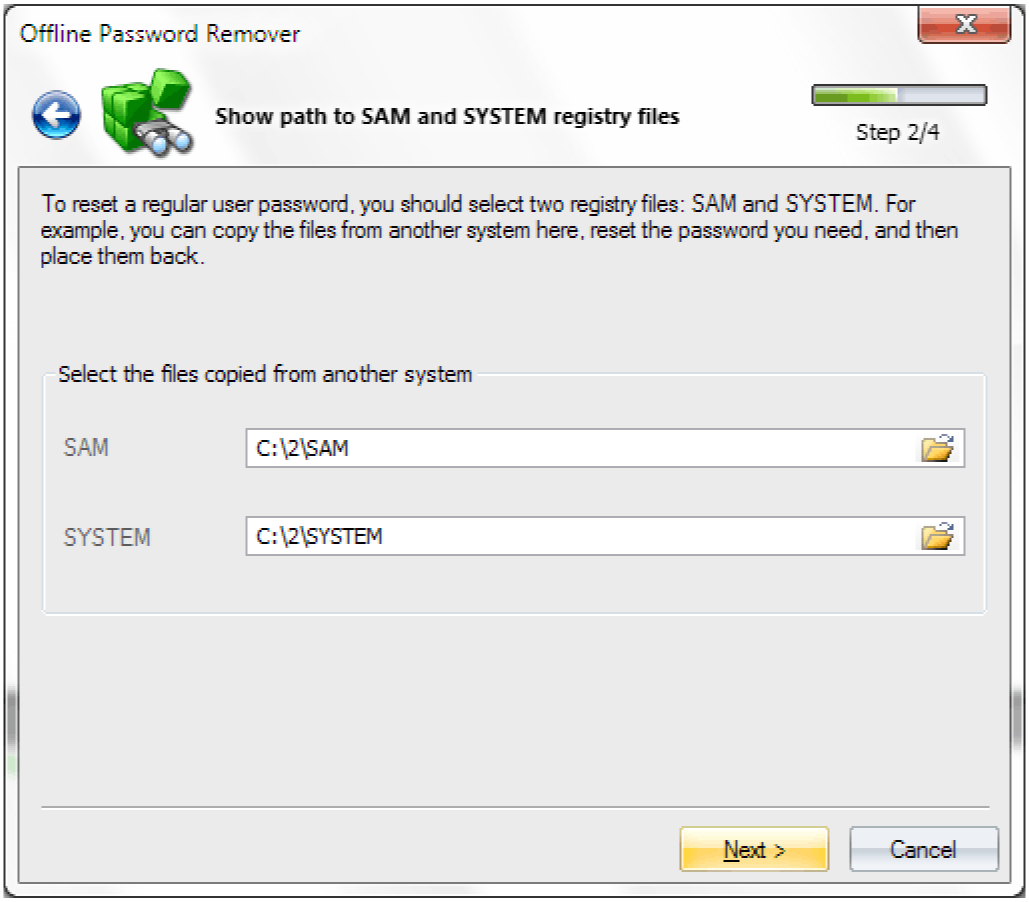
Select password source

● SAM - regular user account

○ Active Directory - domain user account

○ DCC - domain cached accounts

2. На втором шаге мастера нам необходимо указать путь к SAM, SECURITY или NTDS.DIT файлу, а также к файлу реестра SYSTEM. По умолчанию, NTDS.DIT расположен в папке c:\windows\ntds. Файлы реестра лежат в c:\windows\system32\config.



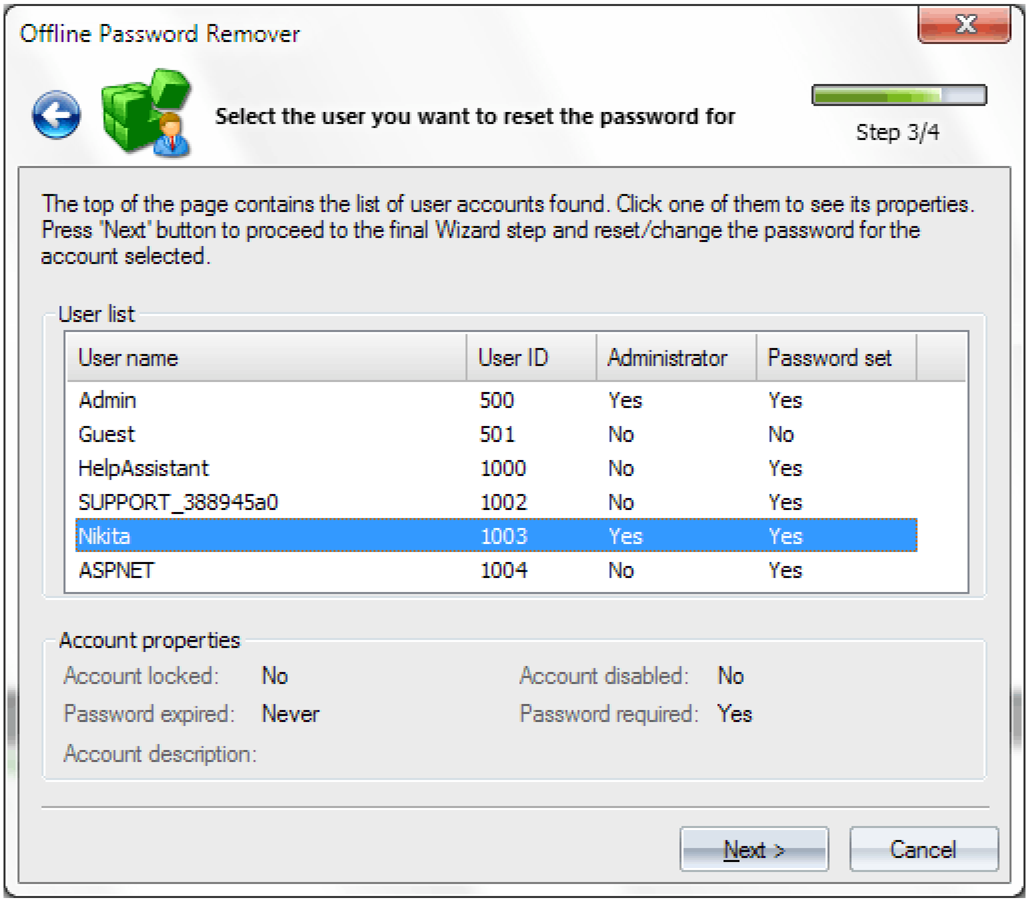
To reset a regular user password, you should select two registry files: SAM and SYSTEM. For example, you can copy the files from another system here, reset the password you need, and then place them back.

Select the files copied from another system

SAM C:\2\SAM

SYSTEM C:\2\SYSTEM

3. На этом шаге нам необходимо выбрать учетную запись, пароль которой необходимо изменить. Выбираем имя пользователя и переходим к последнему шагу.



The top of the page contains the list of user accounts found. Click one of them to see its properties. Press 'Next' button to proceed to the final Wizard step and reset/change the password for the account selected.

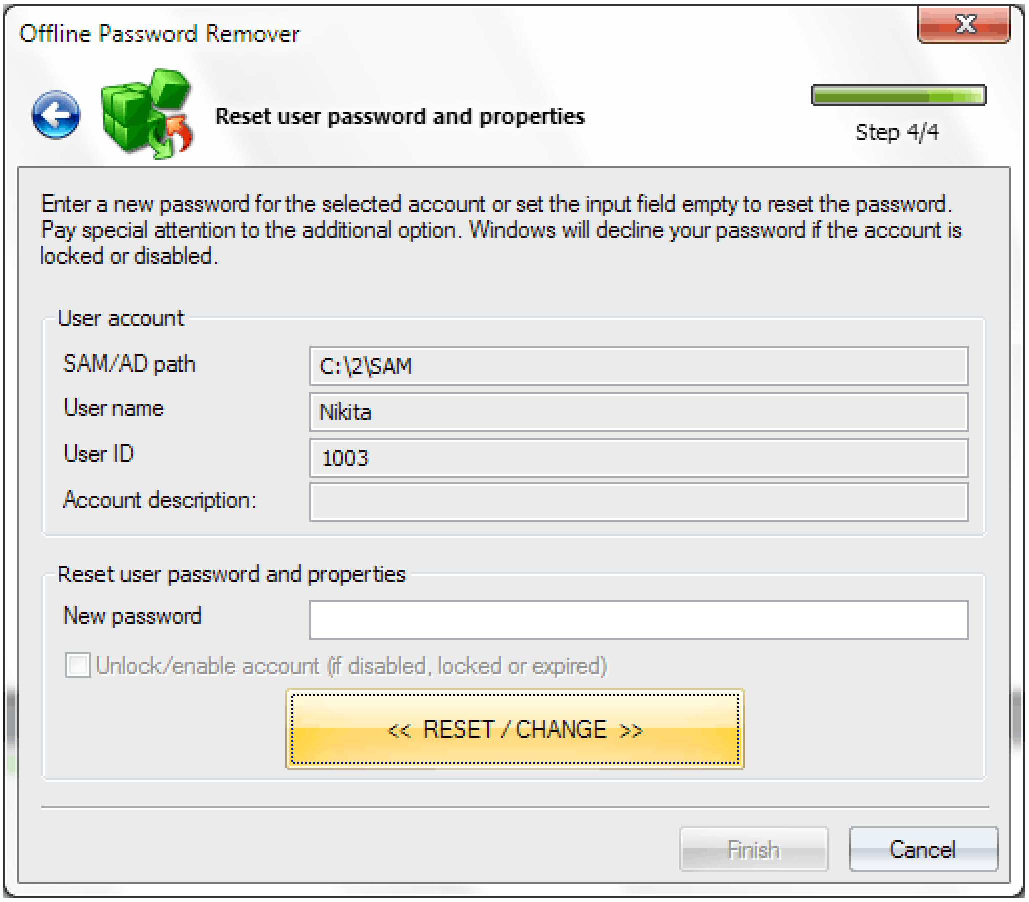
User list

User name	User ID	Administrator	Password set
Admin	500	Yes	Yes
Guest	501	No	No
HelpAssistant	1000	No	Yes
SUPPORT_388945a0	1002	No	Yes
Nikita	1003	Yes	Yes
ASPNET	1004	No	Yes

Account properties

Account locked: No
Account disabled: No
Password expired: Never
Password required: Yes
Account description:

4. Поле ввода 'New password' предназначено для ввода нового пароля (можно оставить его пустым для сброса). Если это поле неактивно, значит пароль учетной записи уже пустой. То же касается и дополнительной опции для разблокировки заблокированных или отключенных учетных записей.



Enter a new password for the selected account or set the input field empty to reset the password. Pay special attention to the additional option. Windows will decline your password if the account is locked or disabled.

User account

SAM/AD path: C:\2\SAM

User name: Nikita

User ID: 1003

Account description:

Reset user password and properties

New password:

□ Unlock/enable account (if disabled, locked or expired)

Перед внесением финальных изменений, не забудьте сохранить ваши SAM, SECURITY или NTDS.DIT файлы!

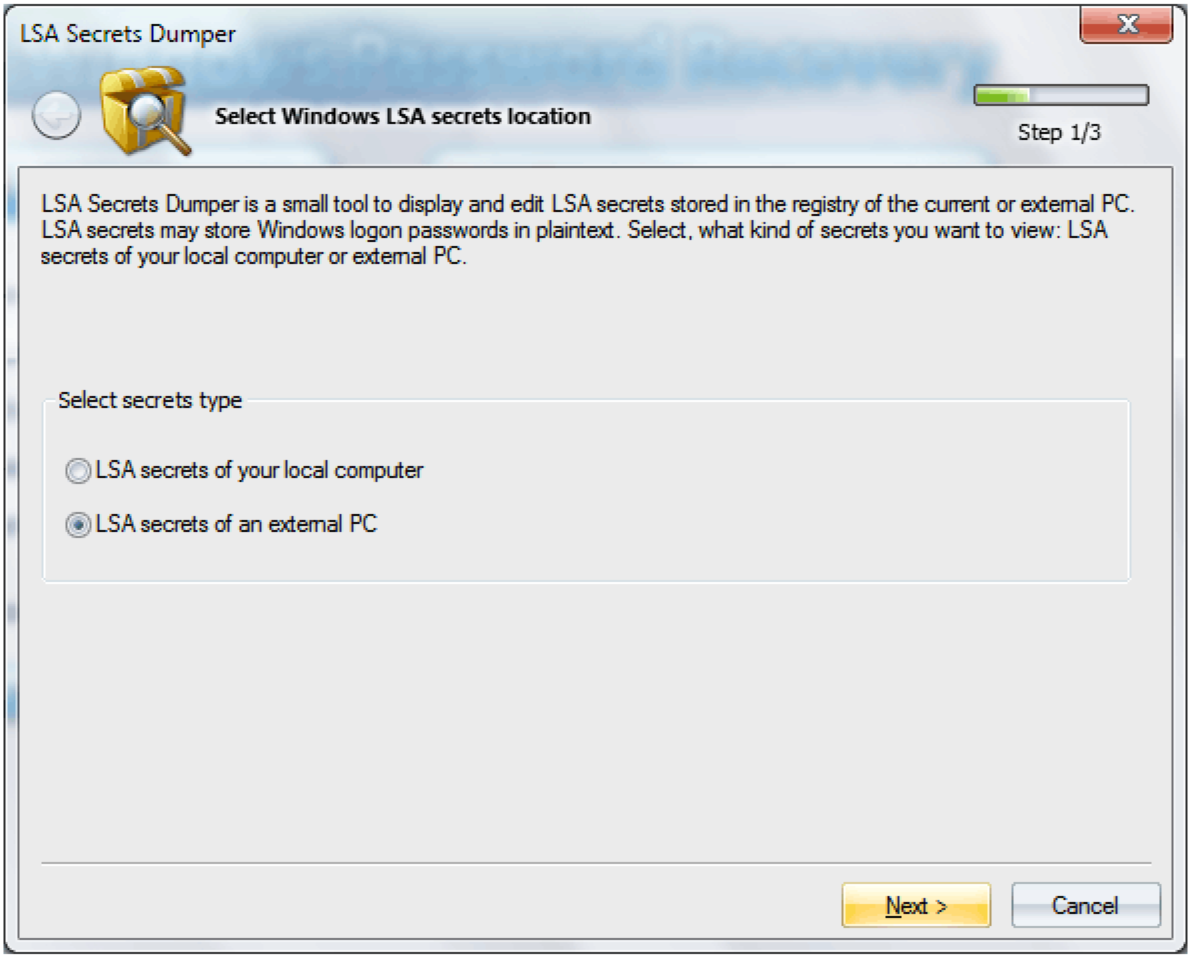
2.7.4 Инструменты Анализа

2.7.4.1 Секреты LSA

LSA секреты - это специальное защищенное хранилище важной информации, которая используется системой Local Security Authority (LSA) в Windows. В секретах могут храниться текстовые пароли пользователей ПК, пароли учетных записей служб (например, требующие запуска в контексте локального пользователя для выполнения определенных задач), пароли Internet Explorer, пароли сетевых подключений RAS, пароли SQL, CISCO, пароли учетной записи SYSTEM, приватные данные пользователя, например, ключи шифрования EFS и многое другое. Например, секрет с именем NL$KM содержит ключ шифрования кэшированных паролей домена, в L$RTMTIMEBOMB хранится время до окончания работы неактивированной копии Windows, и т.д.

WPR плагин для работы с LSA секретами - это небольшая утилита, предназначенная для просмотра, анализа и редактирования секретов LSA. Интерфейс плагина, выполненный в виде Мастера, довольно прост и состоит из трех шагов:

1. Вначале необходимо выбрать тип секретов, с которыми вам предстоит работать. Это могут быть секреты локальной системы, на которой запущена программа, либо секреты другого ПК.



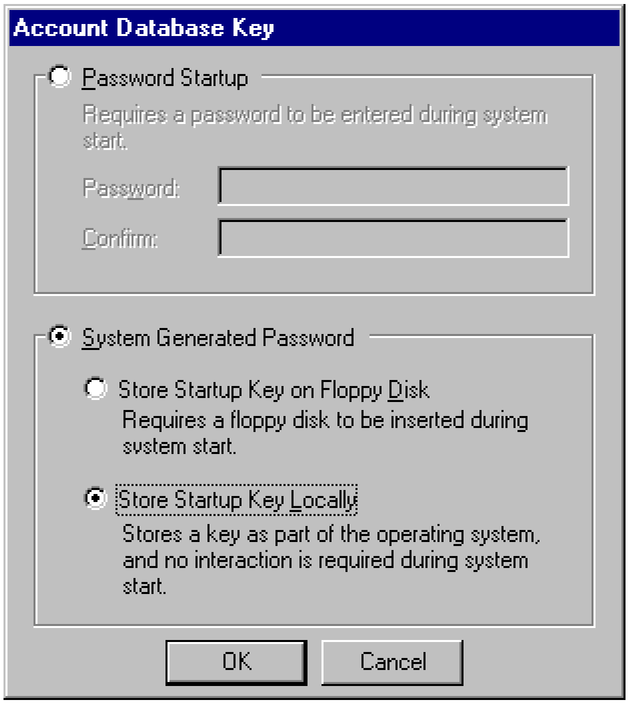
LSA Secrets Dumper is a small tool to display and edit LSA secrets stored in the registry of the current or external PC. LSA secrets may store Windows logon passwords in plaintext. Select, what kind of secrets you want to view: LSA secrets of your local computer or external PC.

Select secrets type

○ LSA secrets of your local computer

● LSA secrets of an external PC

2. При выборе секретов внешнего ПК, вам необходимо указать путь к двум файлам реестра: SYSTEM и SECURITY. В файле SECURITY находятся зашифрованные секреты, а SYSTEM необходим для их расшифровки. Подробнее о шифровании секретов можно ознакомиться в нашей статье. Надо заметить, что в шифровании секретов принимает участие SYSKEY. По умолчанию SYSKEY настроен таким образом, что может быть извлечен из реестра (вот для чего нужен SYSTEM).



○ Password Startup

Requires a password to be entered during system start.

Password:

Confirm:

● System Generated Password

○ Store Startup Key on Floppy Disk

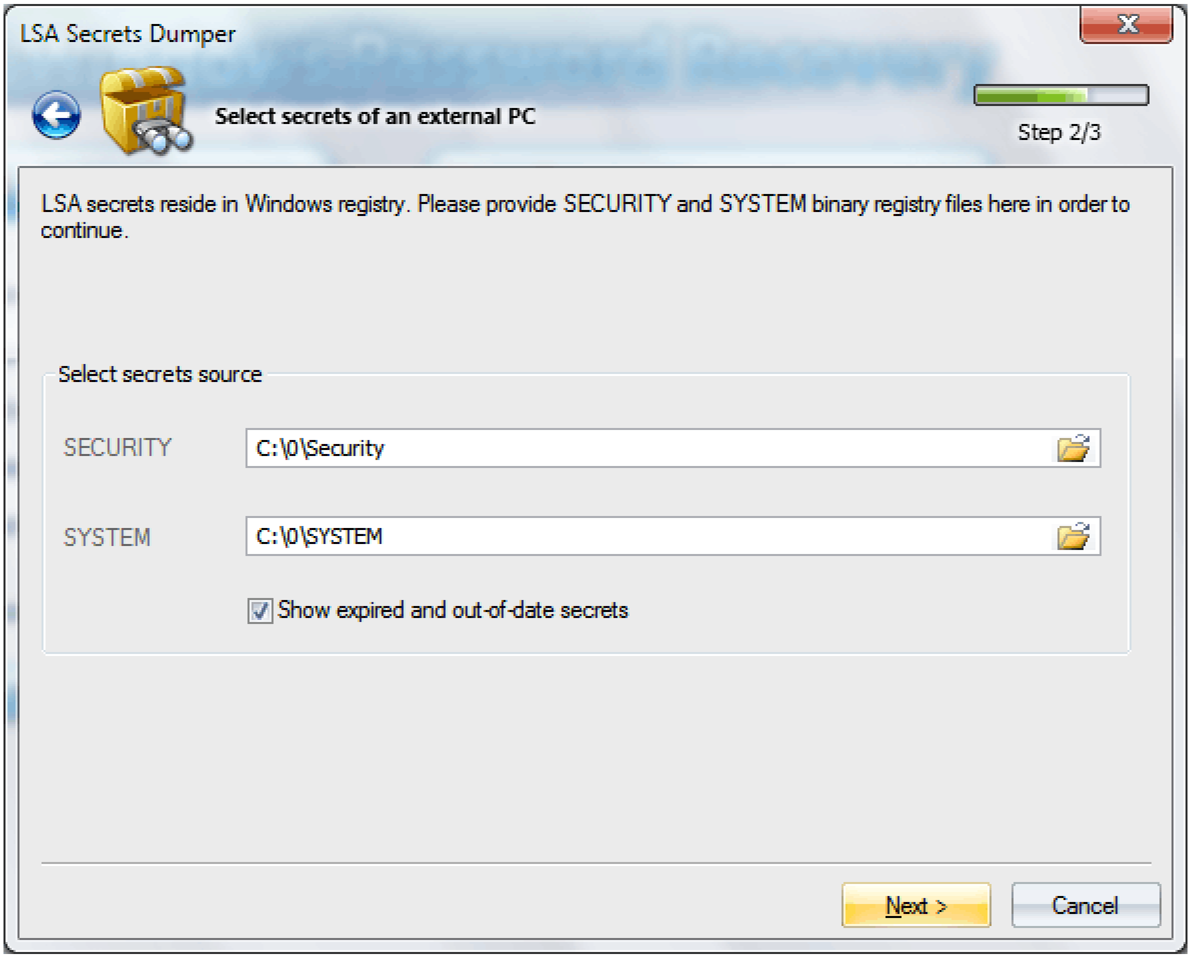
Requires a floppy disk to be inserted during system start.

● Store Startup Key Locally

Stores a key as part of the operating system, and no interaction is required during system start.

В некоторых случаях он может быть настроен иначе: либо храниться на загрузочной дискете, либо генерироваться при вводе пароля во время загрузки операционной системы. Так или иначе, плагин поддерживает все типы шифрования SYSKEY.

Информация, хранимая в секретах, критична для работы всей системы. Поэтому LSA секреты хранятся в двух экземплярах: текущий (активный) и предыдущий (старый). При изменении секрета, происходит следующее: текущий экземпляр откатывается на место старого, а на его место записывается занимает новый, модифицированный секрет. В плагине есть настройка для показа как активных, так и старых секретов.



LSA secrets reside in Windows registry. Please provide SECURITY and SYSTEM binary registry files here in order to continue.

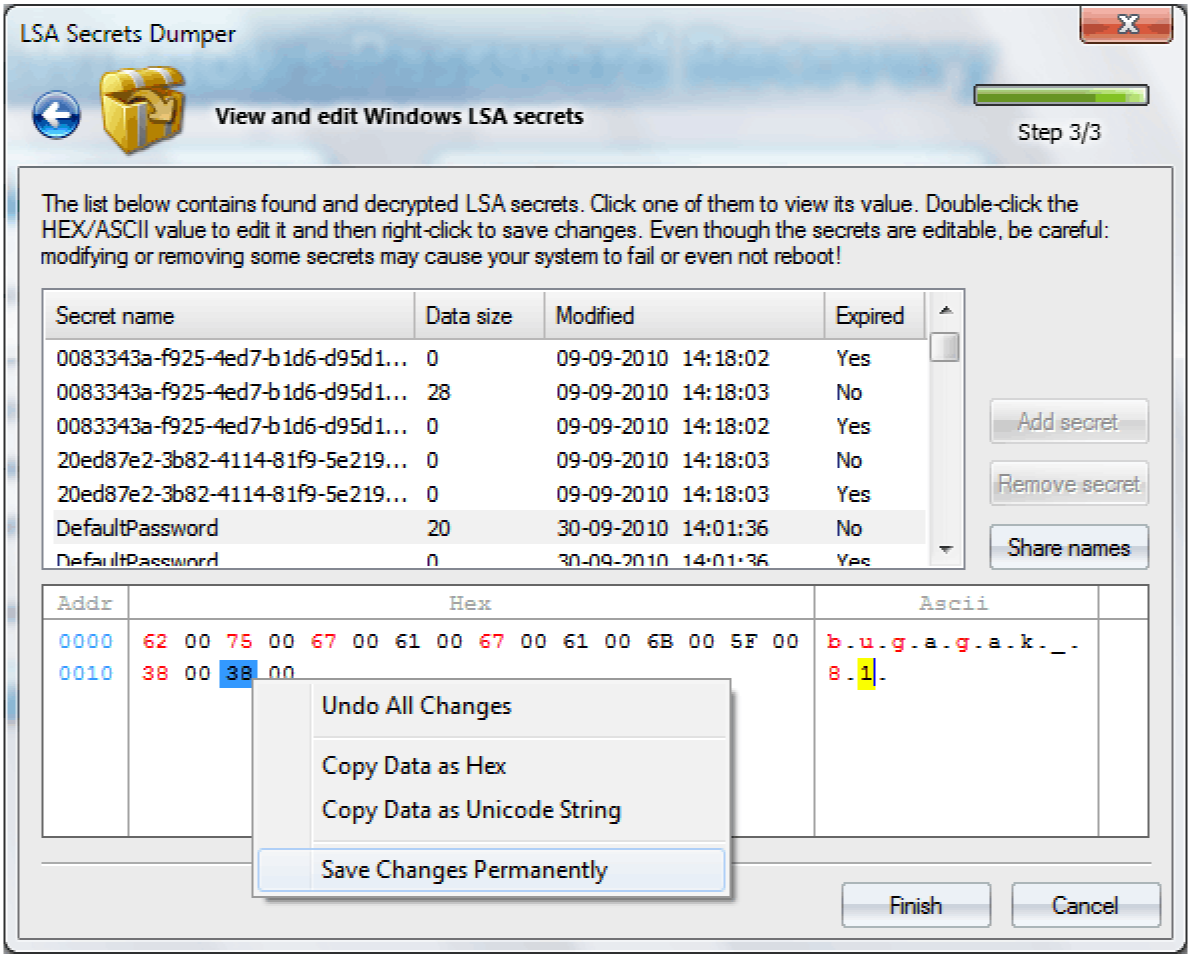
Select secrets source

SECURITY C:\0\Security

SYSTEM C:\0\SYSTEM

☑ Show expired and out-of-date secrets

3. Последний шаг Мастера расшифровывает секреты и отображает их в виде списка. Для того, чтобы показать значение секрета, необходимо щелкнуть мышкой на его имени. Войдите в режим редактирования, дважды щелкнув на одном из символов в поле Hex или Ascii (при этом он должен высветиться желтым цветом), и введите новое значение. В режиме редактирования используйте клавиши управления курсором для перехода к другому символу. Модифицированные значения при этом будут отмечены красным цветом. Для сохранения всех проделанных изменений, щелкните правой кнопкой в поле Hex/Ascii и выберите выберите в меню пункт сохранения.



The list below contains found and decrypted LSA secrets. Click one of them to view its value. Double-click the HEX/ASCII value to edit it and then right-click to save changes. Even though the secrets are editable, be careful: modifying or removing some secrets may cause your system to fail or even not reboot!

Secret name	Data size	Modified	Expired
0083343a-f925-4ed7-b1d6-d95d1...	0	09-09-2010 14:18:02	Yes
0083343a-f925-4ed7-b1d6-d95d1...	28	09-09-2010 14:18:03	No
0083343a-f925-4ed7-b1d6-d95d1...	0	09-09-2010 14:18:02	Yes
20ed87e2-3b82-4114-81f9-5e219...	0	09-09-2010 14:18:03	No
20ed87e2-3b82-4114-81f9-5e219...	0	09-09-2010 14:18:03	Yes
DefaultPassword	20	30-09-2010 14:01:36	No
DefaultPassword	0	30-09-2010 14:01:36	Yes

```
Addr  Hex                                                Ascii
0000  62 00 75 00 67 00 61 00 67 00 61 00 6B 00 5F 00   b.u.g.a.g.a.k._.
0010  38 00 38 00                                        8.1.
```

Учтите, некоторые секреты содержат критическую информацию, поэтому их изменение может привести к нестабильной работе системы или даже к невозможности ее загрузки!

В плагине имеется также возможность добавления или удаления секретов (только для секретов текущей операционной системы). При удалении секрета, не важно, старого или нового, автоматически удаляются оба его экземпляра.

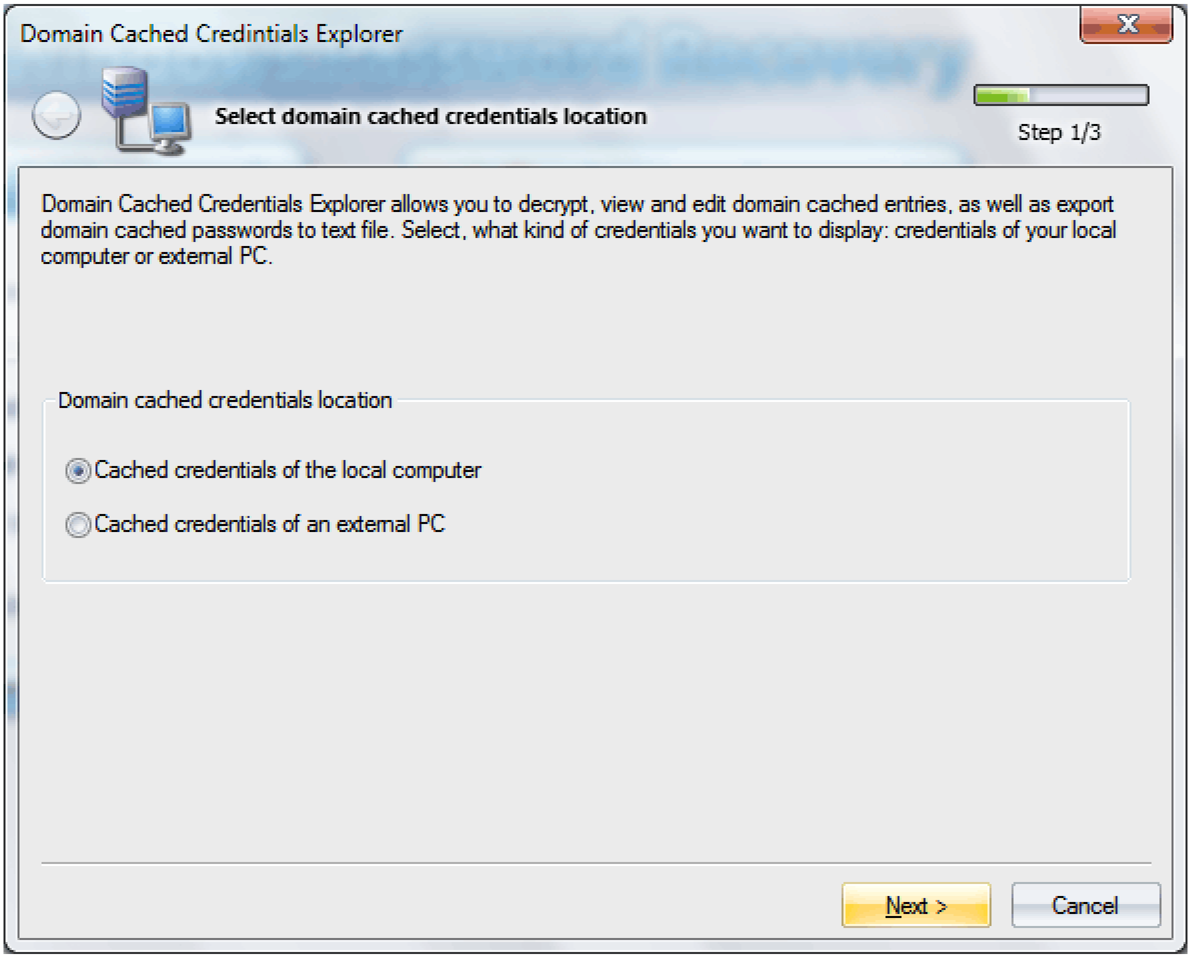
Можно поделиться с разработчиками своими секретами (кнопка Share Names). При этом по электронной почте будут отправлены только имена секретов, без самих данных. Анализ имен секретов поможет нам сделать программу более эффективной.

2.7.4.2 Кэшированные записи домена

Начиная с версии 2.0 в программе появилась возможность чтения кэшированных записей домена. Windows использует кэшированные записи домена для того, чтобы иметь возможность подключаться к серверу даже если сервер для входа по каким-либо причинам недоступен.

Плагин для работы с кэшированными записями домена состоит из трех шагов.

Вначале необходимо определиться, какие записи надо расшифровать: кэшированные записи текущей операционной системы или к.л. другого компьютера.



Select domain cached credentials location

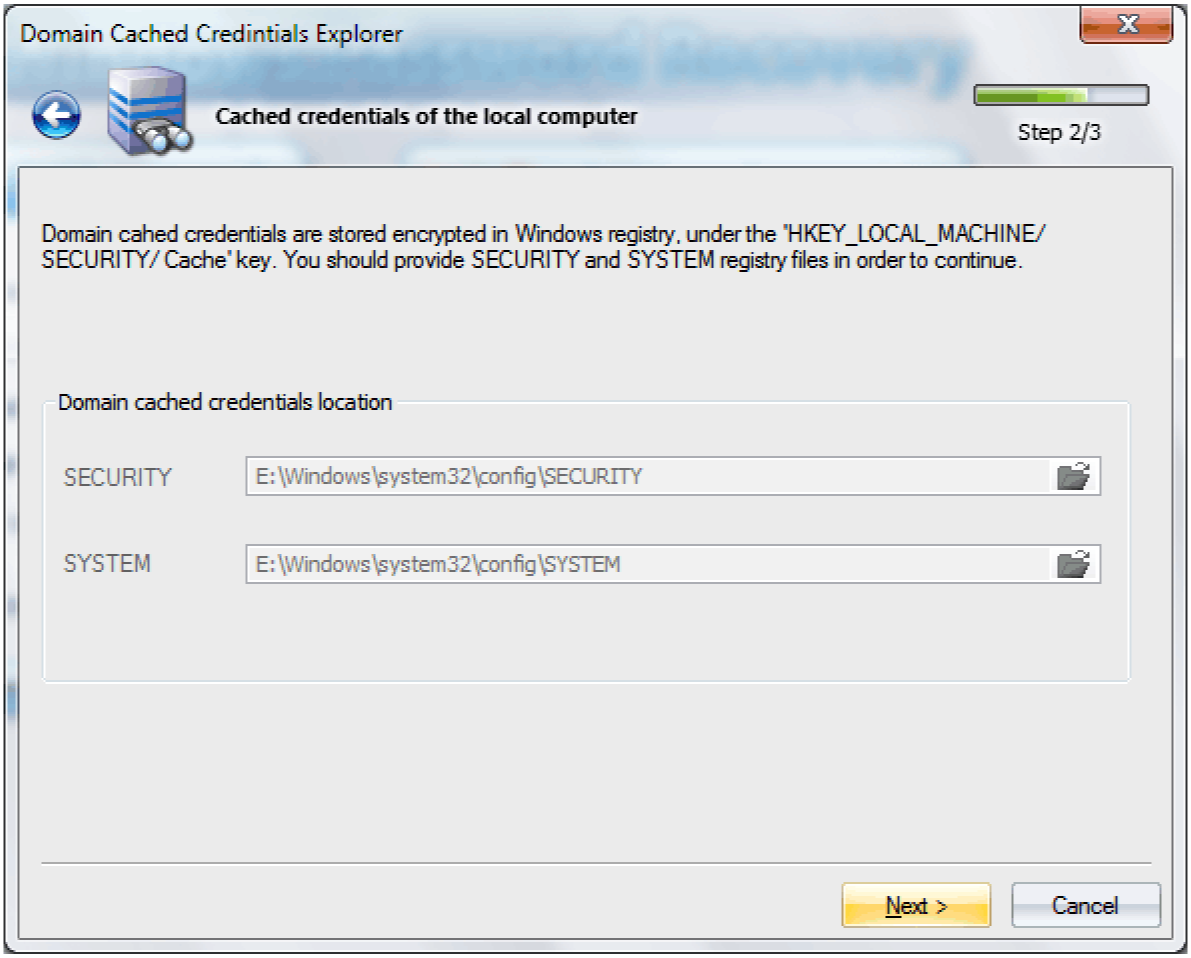
Domain Cached Credentials Explorer allows you to decrypt, view and edit domain cached entries, as well as export domain cached passwords to text file. Select, what kind of credentials you want to display: credentials of your local computer or external PC.

Domain cached credentials location

● Cached credentials of the local computer

○ Cached credentials of an external PC

Кэшированные записи домена хранятся в файле реестра SECURITY. Поэтому, при выборе опции чтения записей внешнего ПК, на следующем шаге Мастера необходимо указать путь к этому файлу, а также к реестру SYSTEM, который участвует в расшифровке записей. Если была выбрана опция чтения кэшированных записей локального компьютера, то на втором шаге мастера программа сама выполнит поиск вышеуказанных файлов. Файлы реестра находятся в папке C:\%WINDIR%\system32\config\, где %WINDIR% - каталог Windows.


Domain Cached Credintials Explorer
Cached credentials of the local computer
Step 2/3

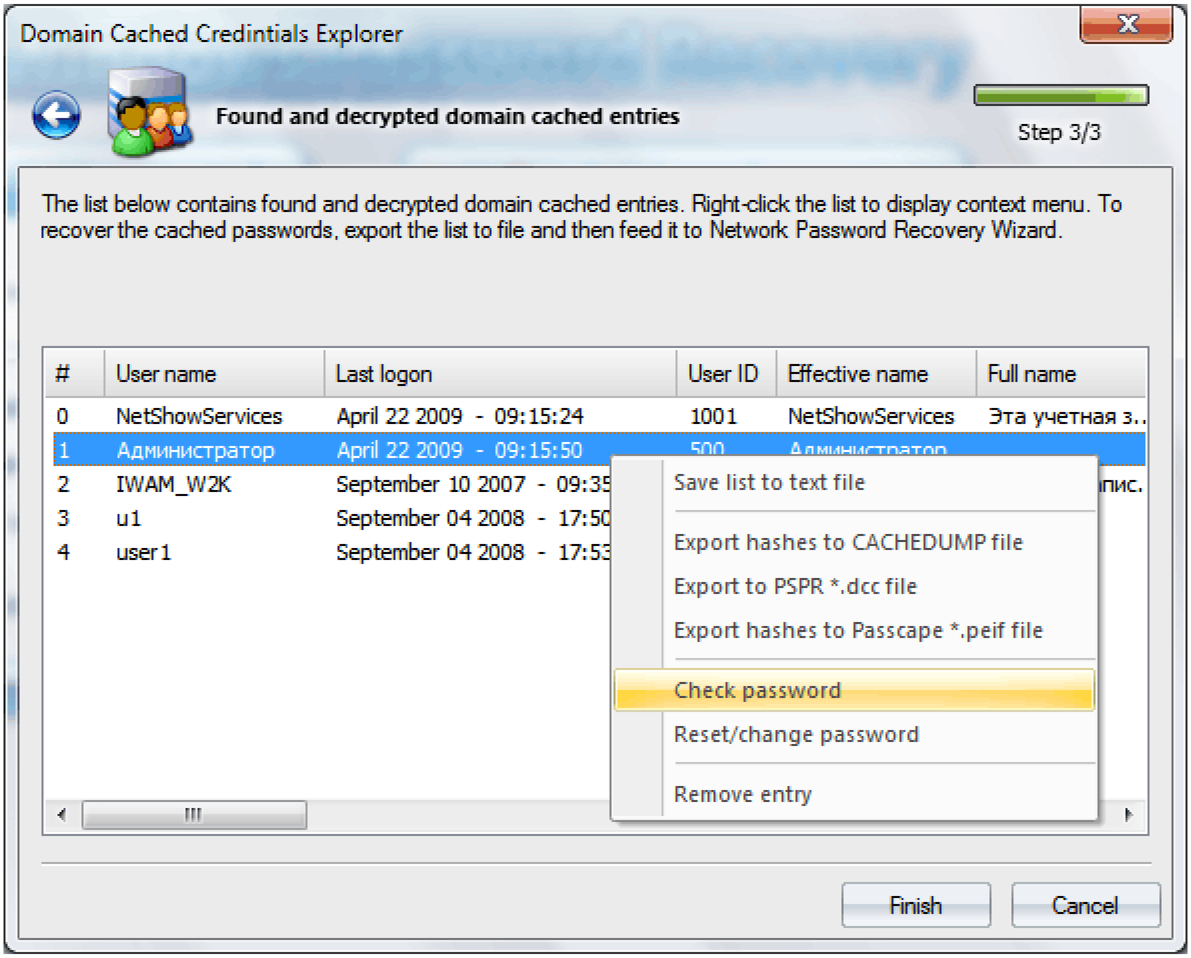
Domain cahed credentials are stored encrypted in Windows registry, under the 'HKEY_LOCAL_MACHINE/ SECURITY/ Cache' key. You should provide SECURITY and SYSTEM registry files in order to continue.

Domain cached credentials location

SECURITY E:\Windows\system32\config\SECURITY

SYSTEM E:\Windows\system32\config\SYSTEM

Если чтение прошло успешно, то в финальном диалоге вы увидите расшифрованные записи домена. Каждая запись имеет несколько атрибутов. Например, имя пользователя, время последнего входа, членство в группах, кэшированные пароль пользователя (точнее хэш).
Щелчок правой кнопкой мыши на списке записей открывает контекстное меню из которого можно:
- сохранить записи со всеми атрибутами в текстовый файл
- экпортировать хэши паролей в формат PWDUMP, *.DCC или *.PEIF файл. Учтите, что PWDUMP формат не совсем корректно хранит записи, поэтому предпочтительнее сохранять хэши паролей в *.DCC или *.PEIF файл.
- проверять или изменять пароль кэшированной записи домена
- удалять запись


Domain Cached Credintials Explorer
Found and decrypted domain cached entries
Step 3/3
Save list to text file
Export hashes to CACHEDUMP file
Export to PSPR *.dcc file
Export hashes to Passcape *.peif file
Check password
Reset/change password
Remove entry
Finish
Cancel

The list below contains found and decrypted domain cached entries. Right-click the list to display context menu. To recover the cached passwords, export the list to file and then feed it to Network Password Recovery Wizard.

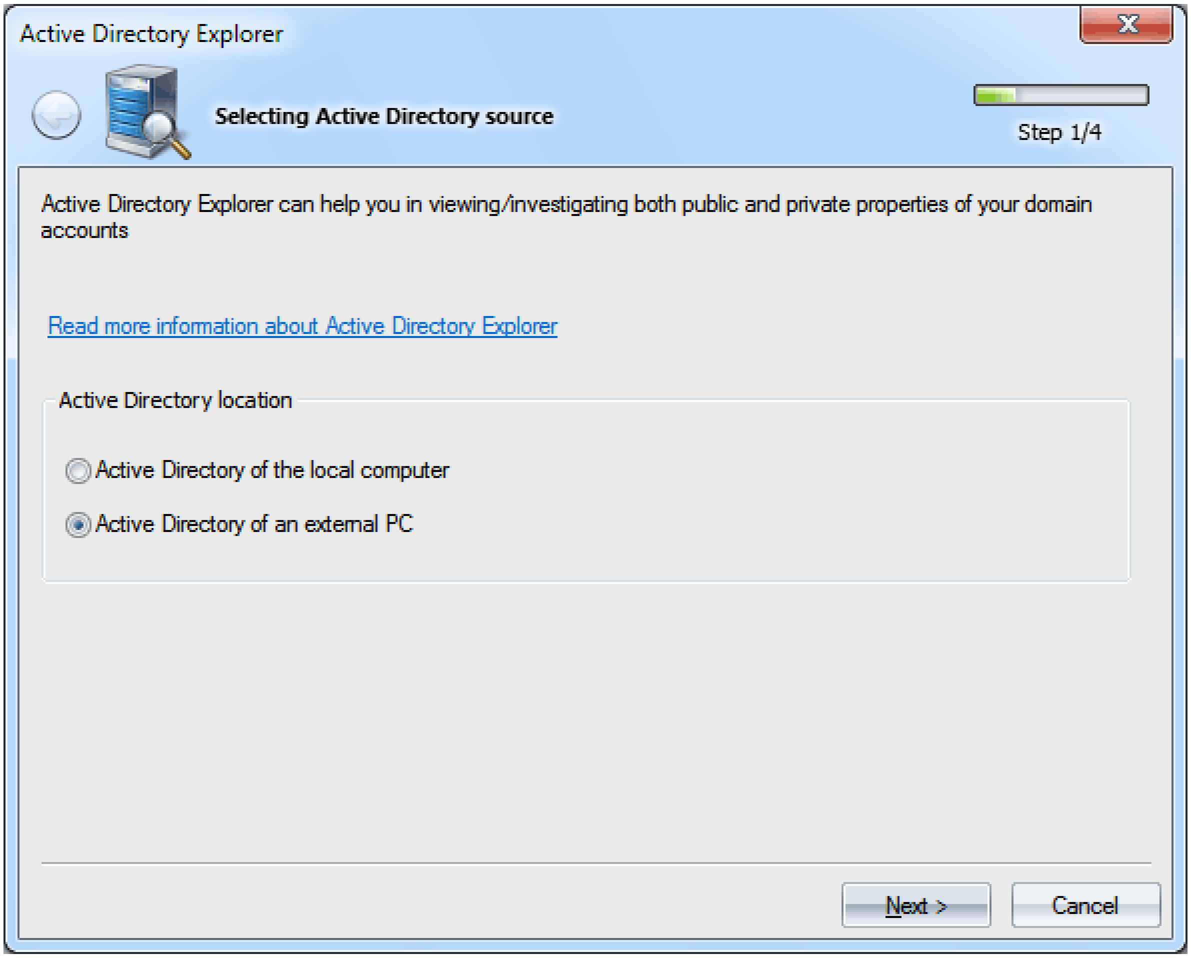
#	User name	Last logon	User ID	Effective name	Full name
0	NetShowServices	April 22 2009 - 09:15:24	1001	NetShowServices	Эта учетная з..
1	Администратор	April 22 2009 - 09:15:50	500	Администратор	
2	IWAM_W2K	September 10 2007 - 09:35			пис.
3	u1	September 04 2008 - 17:50			
4	user1	September 04 2008 - 17:53			

Начиная с версии Windows Password Recovery v13 появилась полная поддержка восстановления паролей кэшированных записей домена. Как первого, так и второго типа.

2.7.4.3 Редактор NTDS.DIT

Редактор Active Directory - это небольшая утилита для просмотра, анализа и редактирования свойств (атрибутов) учетных записей домена, как публичных, так и приватных.

В начале работы необходимо выбрать тип базы данных AD, с которой предстоит работать: локальная или внешняя.



Active Directory Explorer

Selecting Active Directory source

Active Directory Explorer can help you in viewing/investigating both public and private properties of your domain accounts

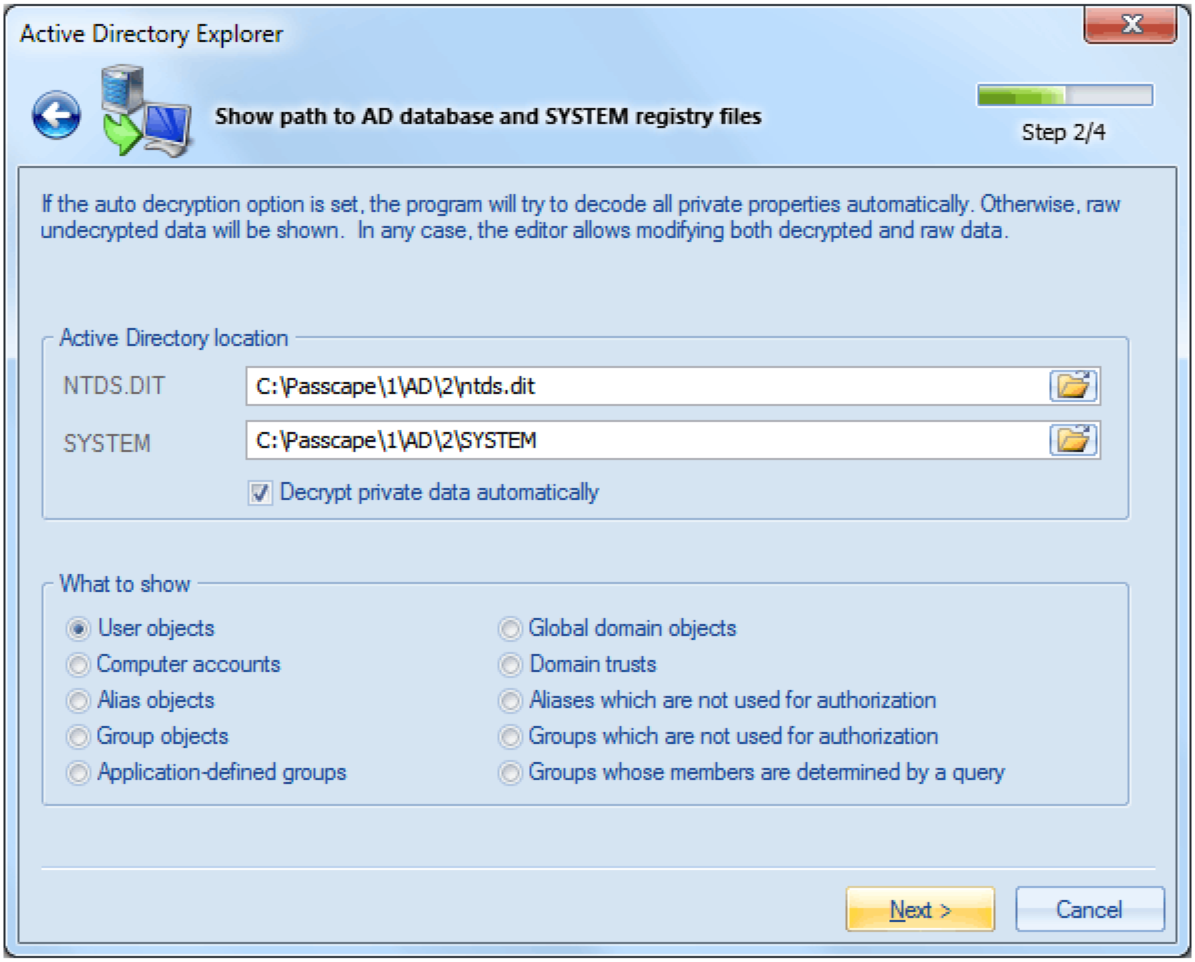
Read more information about Active Directory Explorer

Active Directory location

○ Active Directory of the local computer

● Active Directory of an external PC

При выборе внешней базы данных, следует указать путь к файлу NTDS.DIT и реестру SYSTEM. Последний необходим для расшифровки приватных данных. Если выставлена опция автоматической расшифровки, то все зашифрованные атрибуты учетной записи будут расшифровываться на лету. В любом случае, редактор предоставляет возможность редактирования как расшифрованных, так и сырых данных. В целях безопасности, режим редактирования активен только для внешней базы данных!



Active Directory Explorer

Show path to AD database and SYSTEM registry files

Step 2/4

If the auto decryption option is set, the program will try to decode all private properties automatically. Otherwise, raw undecrypted data will be shown. In any case, the editor allows modifying both decrypted and raw data.

Active Directory location

NTDS.DIT C:\Passcape\1\AD\2\ntds.dit

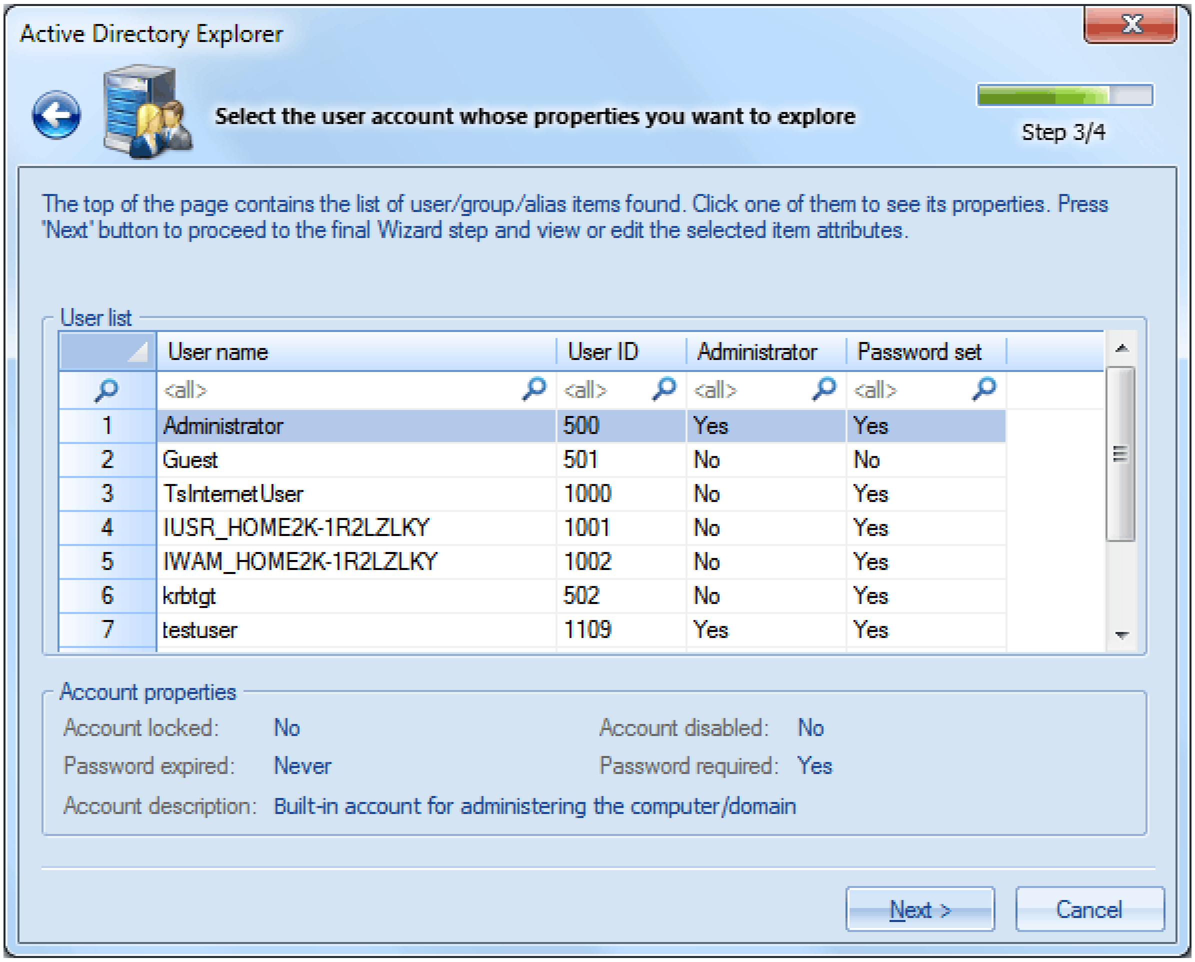
SYSTEM C:\Passcape\1\AD\2\SYSTEM

☑ Decrypt private data automatically

What to show

● User objects
○ Computer accounts
○ Alias objects
○ Group objects
○ Application-defined groups
○ Global domain objects
○ Domain trusts
○ Aliases which are not used for authorization
○ Groups which are not used for authorization
○ Groups whose members are determined by a query

После того, как выбран источник данных, переходим к выбору учетных записей пользователя. Некоторые базы данных Active Directory содержат десятки или даже сотни тысяч учетных записей домена. Для чтения таких больших баз и заполнения списка пользователей может потребоваться некоторое время. Если выбрать одну из записей, то внизу в списке свойств отобразится краткая информация о ней: статус, установлен ли пароль и вышел ли его срок действия, описание учетной записи. Нажатие кнопки 'Далее' запускает процесс сбора и расшифровки всех доступных атрибутов для выбранной записи.



Active Directory Explorer

Select the user account whose properties you want to explore

Step 3/4

The top of the page contains the list of user/group/alias items found. Click one of them to see its properties. Press 'Next' button to proceed to the final Wizard step and view or edit the selected item attributes.

User list

	User name	User ID	Administrator	Password set
	<all>	<all>	<all>	<all>
1	Administrator	500	Yes	Yes
2	Guest	501	No	No
3	TsInternetUser	1000	No	Yes
4	IUSR_HOME2K-1R2LZLKY	1001	No	Yes
5	IWAM_HOME2K-1R2LZLKY	1002	No	Yes
6	krbtgt	502	No	Yes
7	testuser	1109	Yes	Yes

Account properties

Account locked: No
Account disabled: No
Password expired: Never
Password required: Yes
Account description: Built-in account for administering the computer/domain

Каждый атрибут состоит из имени и данных. Например, **Common-Name** содержит имя учетной записи, а в **Unicode-Pwd** хранится хэш пароля. Для более детального описания атрибута, выберите его из списка и кликните по появившейся ссылке в поле с описанием. Двойной щелчок на поле с данными активирует режим редактирования выбранного атрибута учетной записи. После окончания редактирования, правый щелчок мыши открывает контекстное меню, из которого можно отменить сделанные изменения или сохранить их в ntds.dit файл.

Описание некоторых атрибутов учетных записей. Полное описание доступно на сайте Microsoft.

Common-Name
Имя учетной записи.

DBCS-Pwd
Пароль LAN Manager этой учетной записи.

Unicode-Pwd
Пароль пользователя в формате Windows NT OWF (one-way function). Имейте в виду, что получить обратно текстовый пароль из OWF - невозможно.

Lm-Pwd-History

Содержит историю паролей пользователя в формате LAN Manager OWF. Этот атрибут используется для обеспечения совместимости с клиентами LAN Manager 2.x, Windows 95 и Windows 98.

Nt-Pwd-History
История паролей пользователя в формате Windows NT OWF.

Primary-Group-ID
Идентификатор (RID) основной группы пользователя. По умолчанию, это группа Пользователей Домена.

Bad-Pwd-Count
Содержит количество попыток входа в учетную запись с неверным паролем.

Admin-Count
Индикатор принадлежности учетной записи к группе Администраторов (прямо или косвенно).

Logon-Hours
Часы, в которые пользователю разрешен вход в домен.

Last-Logon
Время последнего входа пользователя в домен под этой учетной записью.

Bad-Password-Time
Последний раз, когда пользователь попытался залогиниться с неверным паролем. Это значение хранится в виде 8-байтового числа, представляющего 100 наносекундный интервал, начиная с 1 января 1601 (UTC).

Last-Logon-Timestamp
Дата и время последнего входа пользователя в домен.

Pwd-Last-Set
Дата последнего изменения пароля учетной записи.

Account-Expires
Дата, когда выйдет срок действия этой учетной записи. Значения 0 или 0x7FFFFFFFFFFFFFFF означают, что срок действия учетной записи неограничен.

Supplemental-Credentials
Хранит зашифрованную версию пароля пользователя. Используется при аутентификации.

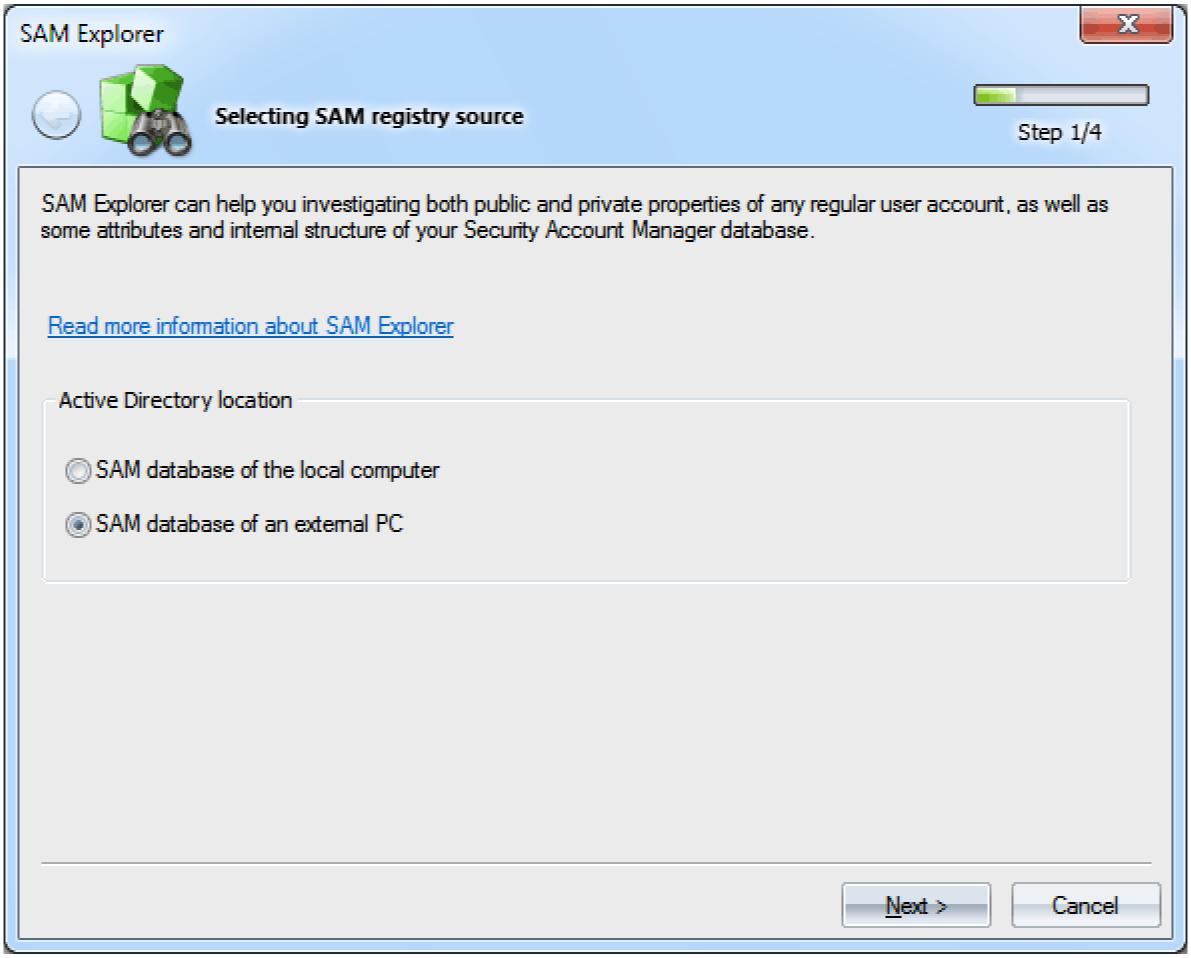
User-Account-Control
Флаг, контролирующий поведение учетной записи. Этот флаг может быть комбинацией одного или нескольких следующих значений:
0x00000001 Учетная запись при входе требует запуска специального скрипта.
0x00000002 Учетная запись отключена.
0x00000008 Требуется домашний каталог.
0x00000010 Учетная запись временно заблокирована.
0x00000020 Пароль на вход не требуется.
0x00000040 Пользователь не имеет права сменить пароль.
0x00000080 Присутствует текстовый пароль.
0x00000100 Эта учетная запись предназначена для пользователей, чья основная учетная запись находится в другом домене.
0x00000200 Учетная запись, представляющая типичного пользователя.
0x00000800 Трастовая учетная запись для системного домена.

0x00001000 Учетная запись компьютера, члена этого домена.
0x00002000 Учетная запись компьютера, системы резервного копирования контроллера домена, члена этого домена.
0x00010000 Срок действия пароля учетной записи неограничен.
0x00020000 Учетная запись MNS.
0x00040000 Вход пользователя осуществляется при помощи смарт карты.
0x00080000 Учетная запись, от имени которой запущен сервис, является доверенной для делегирования Kerberos.
0x00100000 Контекс безопасности пользователя не будет делегироваться сервису даже если учетная запись сервиса является доверенной для делегирования Kerberos.
0x00200000 При генерации ключей шифрования в Kerberos, использовать только алгоритм Data Encryption Standard (DES).
0x00400000 Эта учетная запись для входа не требует пре-аутентификации Kerberos.
0x00800000 Вышел срок действия пароля пользователя.
0x01000000 Учетная запись доступна для делегирования.
0x04000000 Объект является контроллером домена только для чтения (RODC).

2.7.4.4 Редактор SAM

Редактор SAM предназначен для просмотра, анализа и редактирования свойств и статистики учетных записей пользователей Windows. SAM, сокращенно от Security Account Manager, это RPC-сервер, управляющий базой данных учетных записей Windows и выполняющий функции хранения паролей и приватных данных пользователей, группировки логической структуры учетных записей, настройки политики безопасности (например, политики паролей или блокировки учетной записи), сбора статистики (время последнего входа, количества входов, количества некорректных вводов пароля и т.д.) и контроля доступа к базе. База данных SAM хранится в ключе реестра HKEY_LOCAL_MACHINE\SAM\SAM, доступ к которому запрещен всем, кроме системы (даже администраторам). На физическом уровне, база SAM представляет собой двоичный файл реестра с одноименным названием, который расположен в каталоге %WINDIR%\System32\Config, где % WINDIR% - установочный каталог Windows.

В начале работы Мастер предложит выбрать тип базы данных SAM: локальная или внешняя. Учтите, если выбрать локальную базу, то в целях безопасности режим редактировании будет недоступен, база будет открыта только для чтения.



SAM Explorer

Selecting SAM registry source

Step 1/4

SAM Explorer can help you investigating both public and private properties of any regular user account, as well as some attributes and internal structure of your Security Account Manager database.

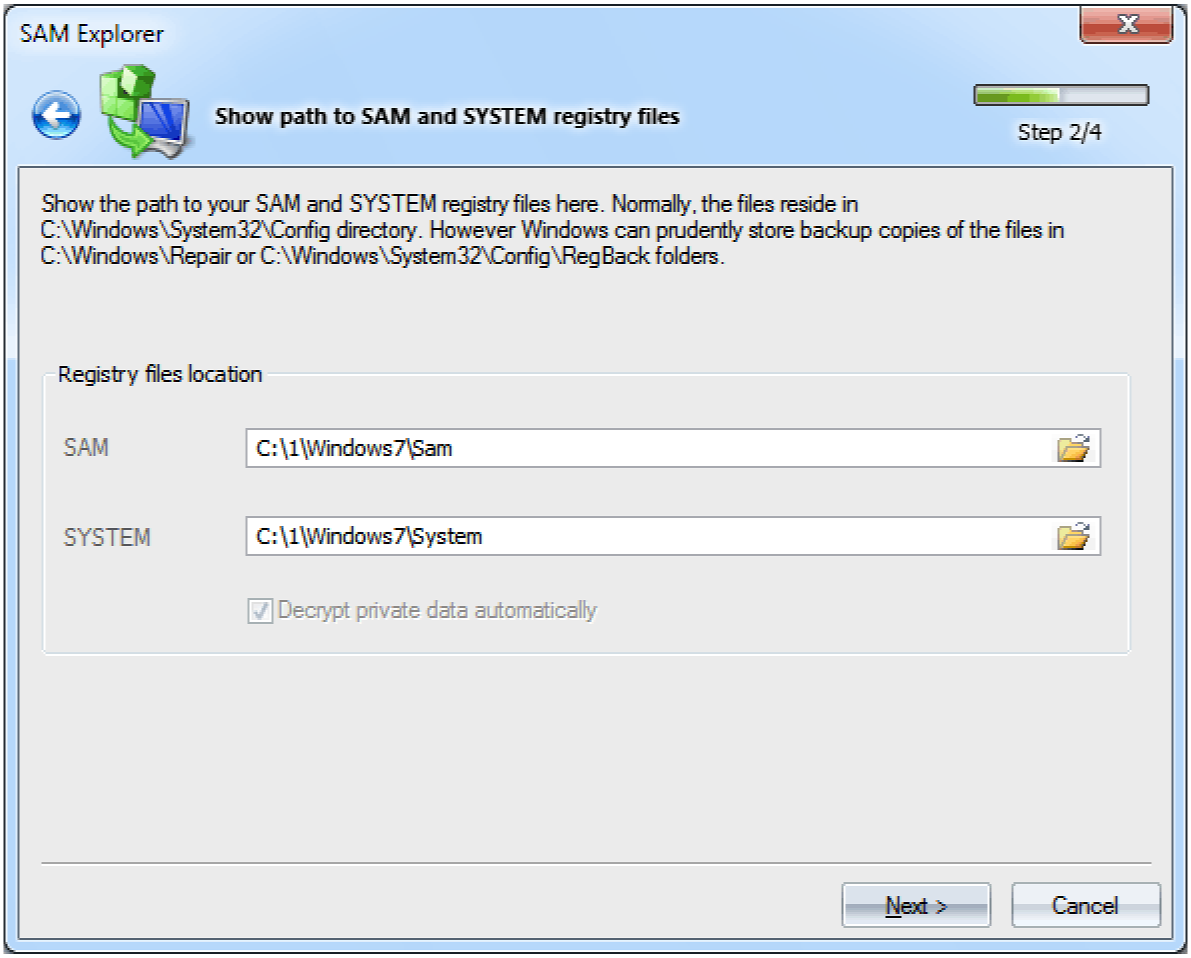
Read more information about SAM Explorer

Active Directory location

○ SAM database of the local computer

● SAM database of an external PC

Если была выбрана база SAM внешнего компьютера, то на втором шаге Мастера необходимо указать путь к реестру SAM и SYSTEM. По умолчанию оба файла находятся в каталоге C:\Windows\System32\Config. Имейте в виду, что система Windows может предусмотрительно сохранять копии файлов реестра в каталогах резервного копирования. Например, C:\Windows\Repair или C:\Windows\ Config\RegBack.



Show the path to your SAM and SYSTEM registry files here. Normally, the files reside in C:\Windows\System32\Config directory. However Windows can prudently store backup copies of the files in C:\Windows\Repair or C:\Windows\System32\Config\RegBack folders.

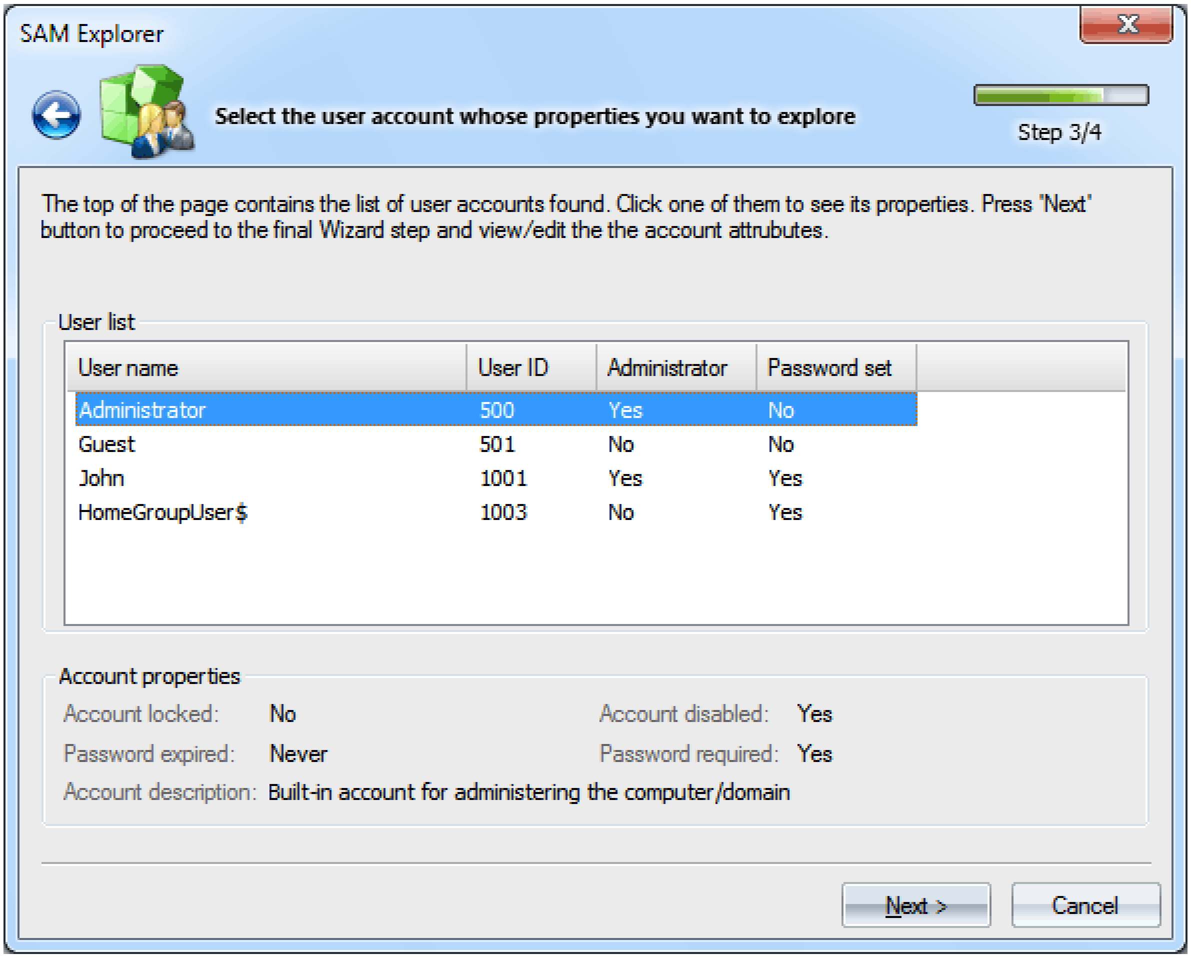
Registry files location

SAM C:\1\Windows7\Sam

SYSTEM C:\1\Windows7\System

☑ Decrypt private data automatically

На третьем этапе переходим к выбору учетной записи, атрибуты которой нам необходимо просмотреть. Выбираем пользователя и жмем Далее.


SAM Explorer
Select the user account whose properties you want to explore
Step 3/4

The top of the page contains the list of user accounts found. Click one of them to see its properties. Press 'Next' button to proceed to the final Wizard step and view/edit the the account attrubutes.

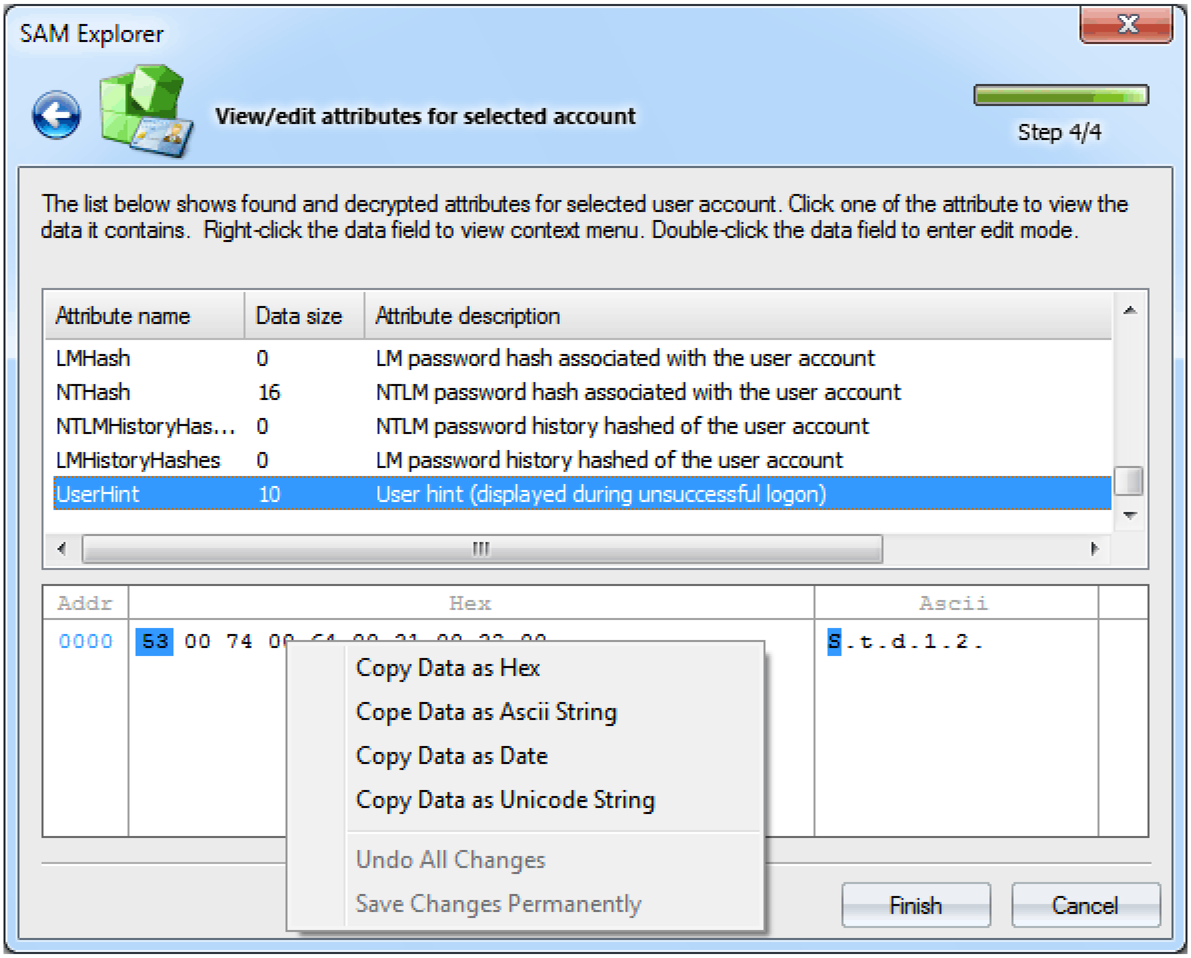
User list

User name	User ID	Administrator	Password set
Administrator	500	Yes	No
Guest	501	No	No
John	1001	Yes	Yes
HomeGroupUser$	1003	No	Yes

Account properties

Account locked: No
Account disabled: Yes
Password expired: Never
Password required: Yes
Account description: Built-in account for administering the computer/domain

В результате получаем список атрибутов для выбранной учетной записи. Если выбрать какой-либо атрибут в списке, то в нижней части редактора будут отображены данные, присущие этому атрибуту. Для входа в режим редактирования, надо дважды щелкнуть на поле с данными, а после завершения выбрать из контекстного меню пункт сохранения сделанных изменений.



The list below shows found and decrypted attributes for selected user account. Click one of the attribute to view the data it contains. Right-click the data field to view context menu. Double-click the data field to enter edit mode.

Attribute name	Data size	Attribute description
LMHash	0	LM password hash associated with the user account
NTHash	16	NTLM password hash associated with the user account
NTLMHistoryHas...	0	NTLM password history hashed of the user account
LMHistoryHashes	0	LM password history hashed of the user account
UserHint	10	User hint (displayed during unsuccessful logon)

```
Addr  Hex                              Ascii
0000  53 00 74 00 64 00 31 00 32 00    S.t.d.1.2.
```

Описание атрибутов учетных записей SAM.

DataRevision
32-битное значение, в котором хранится версия текущей структуры данных. Это значение может быть поделено на два: в первом хранится основной номер версии, во втором - ревизия.

LastLogon
64-битное значение, эквивалент FILETIME, в котором хранится дата и время последнего входа учетной записи в систему.

LastLogoff
64-битное значение, эквивалент FILETIME. Время последнего выхода учетной записи из системы.

PasswordLastSet
64-битное значение, эквивалент FILETIME, дата и время последней смены пароля.

AccountExpires
64-битное значение, эквивалент FILETIME. Дата, когда выйдет срок действия этой учетной записи. Значения 0 или 0x7FFFFFFFFFFFFFFF означают, что срок действия учетной записи неограничен.

LastBadPasswordTime

64-битное значение, эквивалент FILETIME. Последний раз, когда пользователь попытался войти в систему с неверным паролем.

UserID
32-битное значение, представляющее идентификатор (RID) учетной записи.

PrimaryGroupId
32-битное значение, представляющее идентификатор основной группы этой учетной записи.

UserAccountControl
32-битный флаг, контролирующий основные свойства учетной записи. Этот флаг может быть комбинацией одного или нескольких значений:
0x00000001 - учетная запись отключена
0x00000002 - требуется путь к домашнему каталогу пользователя
0x00000004 - пароль для этой учетной записи не требуется
0x00000008 - эта учетная запись предназначена для пользователей, чья основная учетная запись находится в другом домене
0x00000010 - обычная (не системная) учетная запись
0x00000020 - учетная запись MNS
0x00000040 - трастовая учетная запись для системного домена
0x00000080 - учетная запись члена рабочей станции или сервера
0x00000100 - учетная запись контроллера домена
0x00000200 - срок действия пароля пользователя неограничен
0x00000400 - учетная запись заблокирована
0x00000800 - должен присутствовать текстовый пароль пользователя
0x00001000 - вход пользователя осуществляется при помощи смарт карты
0x00002000 - используется протоколом Kerberos
0x00004000 - используется протоколом Kerberos
0x00008000 - используется протоколом Kerberos, учетная запись может использовать только ключи шифрования des-cbc-md5 или des-cbc-crc
0x00010000 - учетная запись для входа не требует пре-аутотентификации Kerberos
0x00020000 - вышел срок действия пароля, при следующем входе пользователю будет предложено ввести новый пароль
0x00040000 - используется протоколом Kerberos
0x00080000 - используется протоколом Kerberos
0x00100000 - объект является контроллером домена только для чтения (RODC)
0x00200000 - использовать шифрование AES, this bit is ignored and used internally

CountryCode
16-битный интернациональный код страны, сопоставленный с учетной записью. Например, код Великобритании - 44 в десятичной нотации.

CodePage
16-битная кодовая страница (в формате кодовой страницы Microsoft), сопоставленная с учетной записью.

BadPasswordCount
16-битный счетчик вводов неверного пароля.

LogonCount
16-битный счетчик удачных входов учетной записи в систему.

AdminCount
Индикатор принадлежности учетной записи к группе Администраторов (прямо или косвенно).

OperatorCount
Индикатор принадлежности учетной записи к группе Операторов.

UserName
Строка в формате Юникод, содержащая имя пользователя этой учетной записи.

FullName
Строка в формате юникод, содержащая полное имя пользователя.

AdminComment
Комментарий администратора, который ассоциируется с этой учетной записью.

UserComment
Второй комментарий пользователя, ассоциирующийся с этой учетной записью.

Parameters
Расширенные параметры пользователя. Программы Microsoft используют это поле для хранения настроек пользователя.

HomeDirectory
Строка Юникод, определяющая путь к домашнему каталогу пользователя учетной записи.

HomeDirectoryDrive
Буква диска для домашнего каталога.

ScriptPath
Содержит путь к скрипту пользователя, запускаемому при входе. Скрипт может быть .CMD, .EXE или .BAT файлом.

ProfilePath
Определяет путь к профилю пользователя.

WorkStations
Имена (разделяемые запятой) рабочих станций, с которых пользователю разрешается вход. Может быть задано но восьми рабочих станций. Установленное значение 0x00000001 во флаге учетной записи, позволяет запретить вход со всех рабочих станций.

LogonHours
21-байтное поле, задающее время, когда пользователь может войти в систему. Каждый бит задает один час в неделе по времени Greenwich Mean Time. Первый бит - воскресенье с 0:00 до 0:59, второй бит - воскресенье с 1:00 до 1:59 и т.д. Имейте в виду, что бит 0 означает воскресенье с 0:00 до 0:59 только во временной зоне GMT. Иначе необходимо сделать поправку на временную зону, в которой находитесь вы. Например, GMT + 3h.

Groups
Список групп к которым принадлежит или не принадлежит учетная запись.

LMHash
Пароль LAN Manager этой учетной записи.

NTHash
Пароль пользователя в формате Windows NT OWF (one-way function).

LMHistoryHashes
Содержит историю паролей пользователя в формате LAN Manager OWF. Этот атрибут используется для обеспечения совместимости с клиентами LAN Manager 2.x, Windows 95 и Windows 98.

NTHistoryHashes
История паролей пользователя в формате Windows NT OWF.

UserHint
Подсказка о пароле, ассоциированная с данной учетной записью (Windows XP и выше).

UserPicture
Рисунок пользователя, ассоциированный с данной учетной записью (Windows Vista и выше).

2.7.4.5 Утилиты для анализа и расшифровки DPAPI

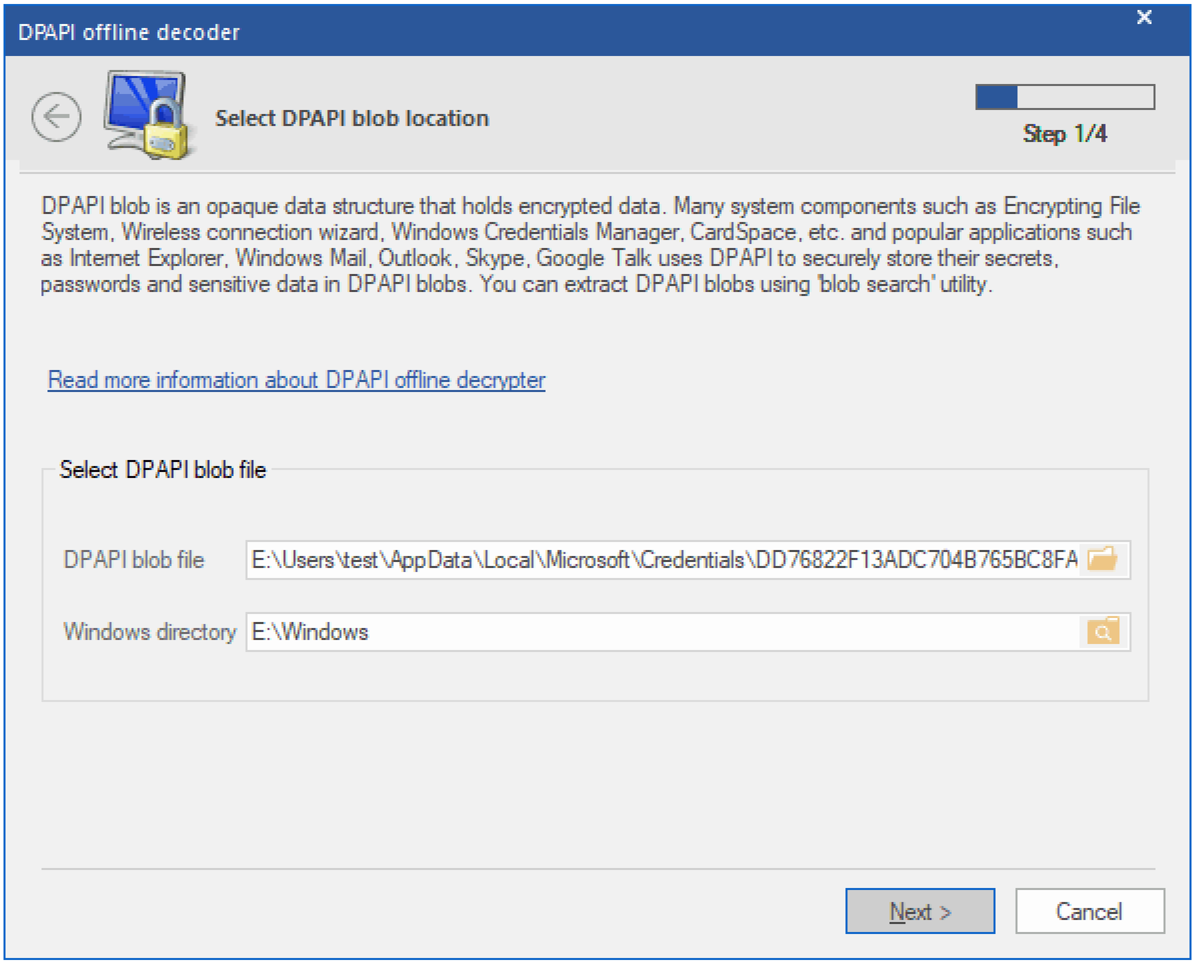
Начиная с Windows 2000, Microsoft стали предоставлять в своих операционных системах специальный интерфейс для защиты данных: Data Protection Application Programming Interface (DPAPI). В настоящее время DPAPI получила очень широкое распространение и используется во многих приложениях и подсистемах Windows. Например, в системе шифрования файлов, для хранения беспроводных паролей сети, в Microsoft Vault, Internet Explorer, Outlook, Skype, Google Chrome и т.д. Эта система стала популярной у программистов в первую очередь благодаря простоте использования, поскольку она состоит всего лишь из пары функций для шифрования и расшифровки данных: CryptProtectData и CryptUnprotectData. Однако несмотря на свою кажущуюся простоту, техническая реализация DPAPI довольно сложна.

Passcape Software (первой в мире!) предлагает набор из 6 инструментов для полноценного анализа и расшифровки данных, зашифрованных при помощи DPAPI. С помощью этих утилит можно:
- Расшифровывать данные DPAPI **для любой** учетной записи
- Выполнять поиск DPAPI объектов на диске
- Расшифровывать объекты DPAPI, зашифрованные под учетной записью **SYSTEM** (например, пароли WiFi)
- Производить анализ и расшифровку Мастер Ключей пользователя
- Проверять пароль пользователя **без** дампа хэшей из SAM или NTDS.DIT
- Расшифровывать хэши истории всех введенных ранее паролей (без использования SAM или NTDS.DIT)

2.7.4.5.1 Расшифровка данных, зашифрованных при помощи DPAPI

Расшифровка данных DPAPI (DPAPI blobs) состоит из четырех шагов мастера.

1. Выбор файла с зашифрованными данными DPAPI



DPAPI blob is an opaque data structure that holds encrypted data. Many system components such as Encrypting File System, Wireless connection wizard, Windows Credentials Manager, CardSpace, etc. and popular applications such as Internet Explorer, Windows Mail, Outlook, Skype, Google Talk uses DPAPI to securely store their secrets, passwords and sensitive data in DPAPI blobs. You can extract DPAPI blobs using 'blob search' utility.

Read more information about DPAPI offline decrypter

Select DPAPI blob file

DPAPI blob file: E:\Users\test\AppData\Local\Microsoft\Credentials\DD76822F13ADC704B765BC8FA

Windows directory: E:\Windows

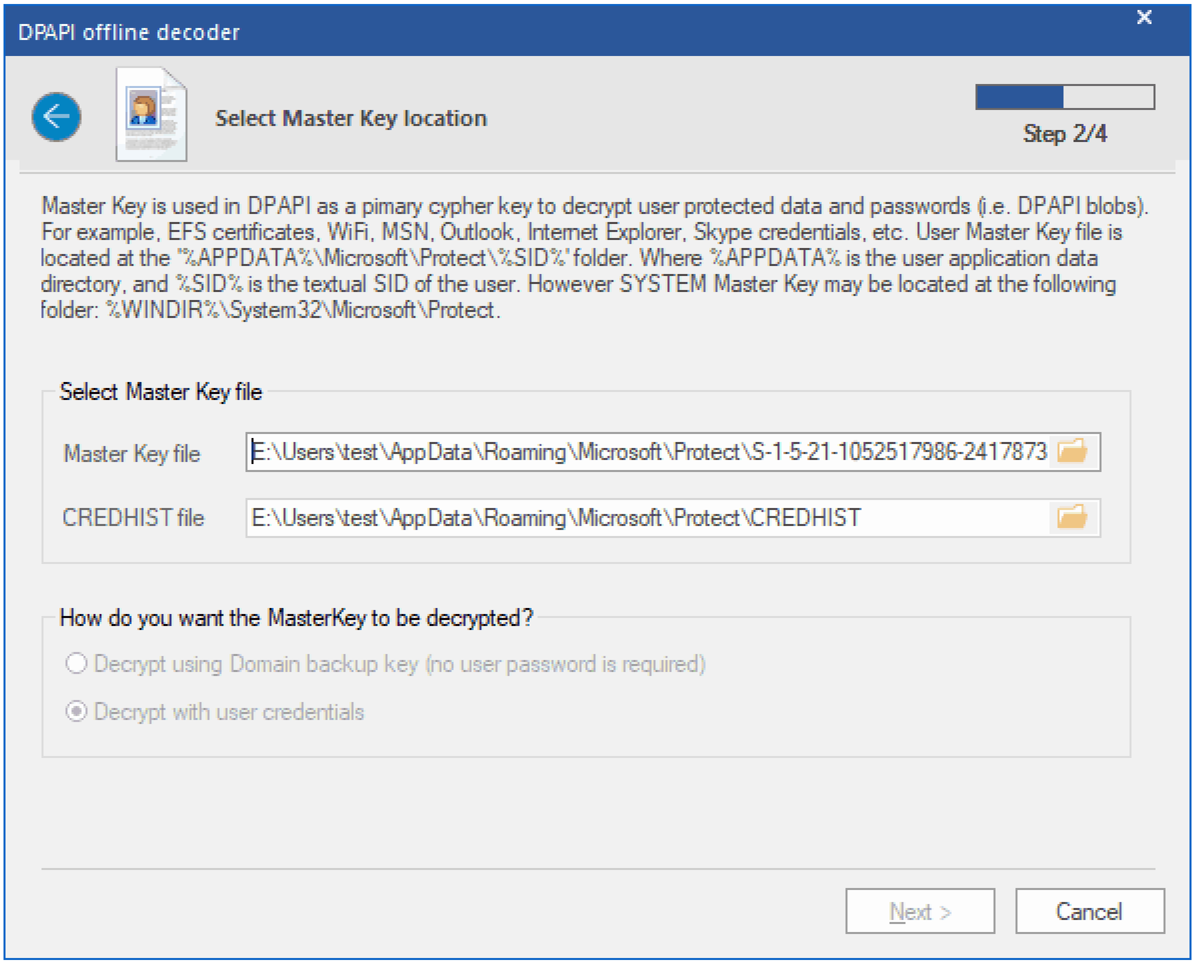
На первом этапе необходимо указать путь к файлу с объектом DPAPI и каталогу Windows. Надо сказать, что сами DPAPI объекты могут храниться в разных местах операционной системы, например, в отдельных xml файлах, в реестре, в Active Directory; и в разных форматах: двоичном, ASCII, UNICODE. Для поиска DPAPI объектов, извлечения и сохранения их в файлы существует специальная утилита. С помощью этой утилиты, к примеру, можно сохранить все DPAPI блобы из реестра пользователя в отдельные файлы.

Ниже указаны места хранения некоторых DPAPI объектов.

- Пароли Internet Explorer, Outlook, WiFi passwords (только для XP): реестр пользователя, **%APPDATA%\ntuser.dat**
- Google Chrome: **%LOCALAPPDATA%\Google\Chrome**
- Пароли WiFi (Windows Vista и выше): **%PROGRAMDATA%\Microsoft\Wlansvc**
- Пароли сетевых соединений (Windows Credential Manager): **%LOCALAPPDATA%\Microsoft\Credentials** или **%APPDATA%\Microsoft\Credentials**

Для выдергивания оттуда DPAPI данных, используйте утилиту поиска.

2. Выбор Мастер Ключа



Master Key is used in DPAPI as a pimary cypher key to decrypt user protected data and passwords (i.e. DPAPI blobs). For example, EFS certificates, WiFi, MSN, Outlook, Internet Explorer, Skype credentials, etc. User Master Key file is located at the "%APPDATA%\Microsoft\Protect\%SID%" folder. Where %APPDATA% is the user application data directory, and %SID% is the textual SID of the user. However SYSTEM Master Key may be located at the following folder: %WINDIR%\System32\Microsoft\Protect.

Select Master Key file

Master Key file: E:\Users\test\AppData\Roaming\Microsoft\Protect\S-1-5-21-1052517986-2417873

CREDHIST file: E:\Users\test\AppData\Roaming\Microsoft\Protect\CREDHIST

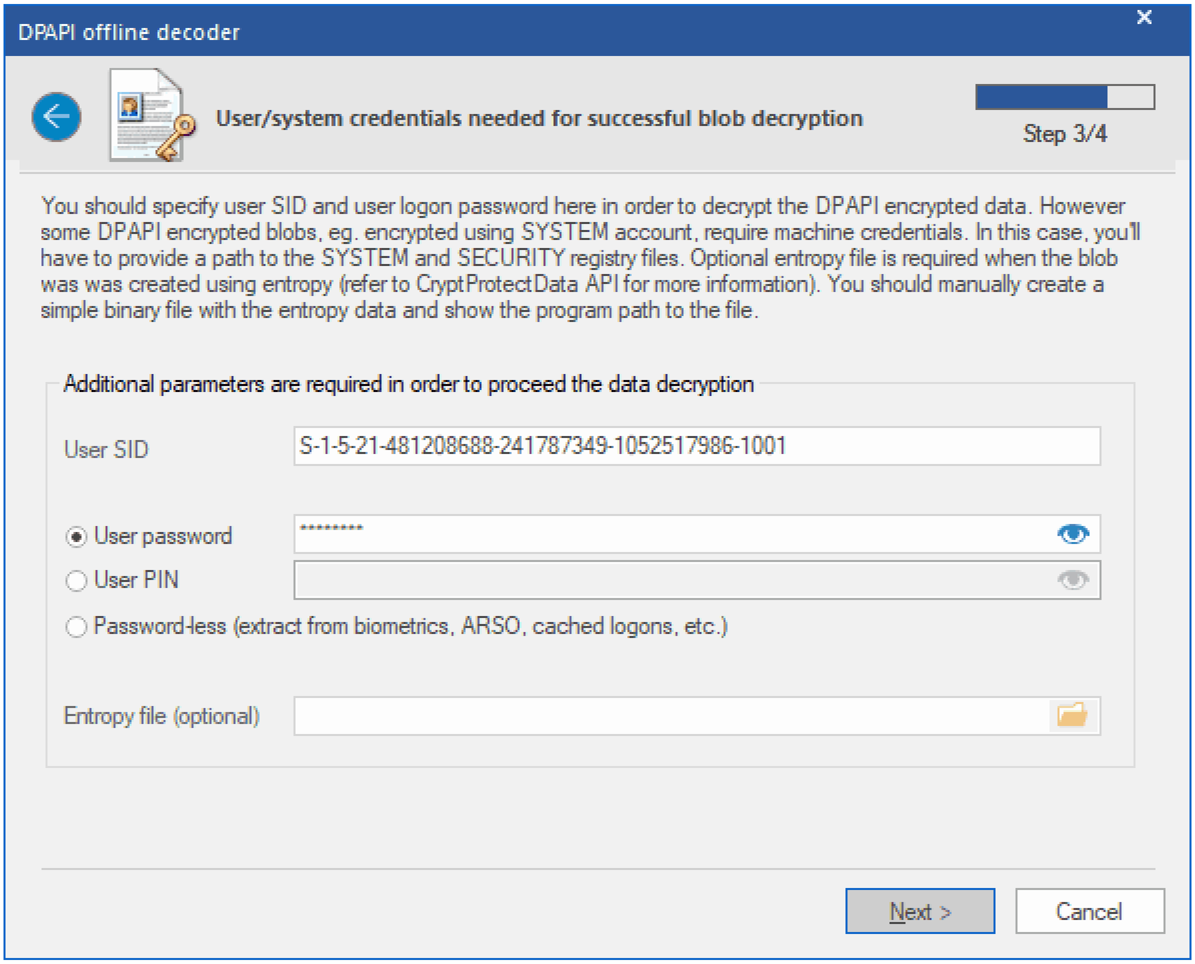
How do you want the MasterKey to be decrypted?

○ Decrypt using Domain backup key (no user password is required)

● Decrypt with user credentials

Мастер ключ представляет собой набор из 64 случайных байт, который используется в качестве первичного ключа при расшифровки DPAPI объектов. Мастер ключ зашифрован с помощью пароля пользователя (либо системы, если это системный Мастер Ключ). Мастер Ключ пользователя всегда располагается в каталоге **%APPDATA%\Microsoft\Protect\%SID%** а Мастер Ключи системной учетной записи хранятся в директории **%SYSTEMDIR%\Microsoft\Protect**. Надо отметить, что Мастер Ключей может быть несколько, а для расшифровки определенного объекта подойдет только один, имя которого хранится внутри DPAPI объекта. При поиске Мастер Ключа, программа может фильтровать ненужные имена. В каталоге **%APPDATA%\Microsoft\Protect** находится и файл **CREDHIST**, который задается опционально, и в большинстве случаев не требуется при расшифровке.

3. Расшифровка Мастер Ключа



User/system credentials needed for successful blob decryption

You should specify user SID and user logon password here in order to decrypt the DPAPI encrypted data. However some DPAPI encrypted blobs, eg. encrypted using SYSTEM account, require machine credentials. In this case, you'll have to provide a path to the SYSTEM and SECURITY registry files. Optional entropy file is required when the blob was was created using entropy (refer to CryptProtectData API for more information). You should manually create a simple binary file with the entropy data and show the program path to the file.

Additional parameters are required in order to proceed the data decryption

User SID: S-1-5-21-481208688-241787349-1052517986-1001

● User password: *********

○ User PIN:

○ Password-less (extract from biometrics, ARSO, cached logons, etc.)

Entropy file (optional):

Для расшифровки Мастер Ключа пользователя необходимо задать как минимум два параметра: пароль пользователя на вход и его идентификатор безопасности (SID), который, как правило, прописан в пути к Мастер Ключу, либо прошит в файле CREDHIST. Так или иначе, WPR вычисляет SID пользователя автоматически. Для расшифровки Мастер Ключа системы, как уже было сказано выше, задавать пароль не имеет смысла, всю необходимую для расшифровки информацию программа получает из двух файлов реестра: SYSTEM и SECURITY. Если при создании DPAPI blob была использована дополнительная энтропия, необходимо самостоятельно создать двоичный файл с энтропией и указать путь к нему. Например, для шифрования паролей Internet Explorer, в качестве энтропии используется имя сайта в формате UNICODE.

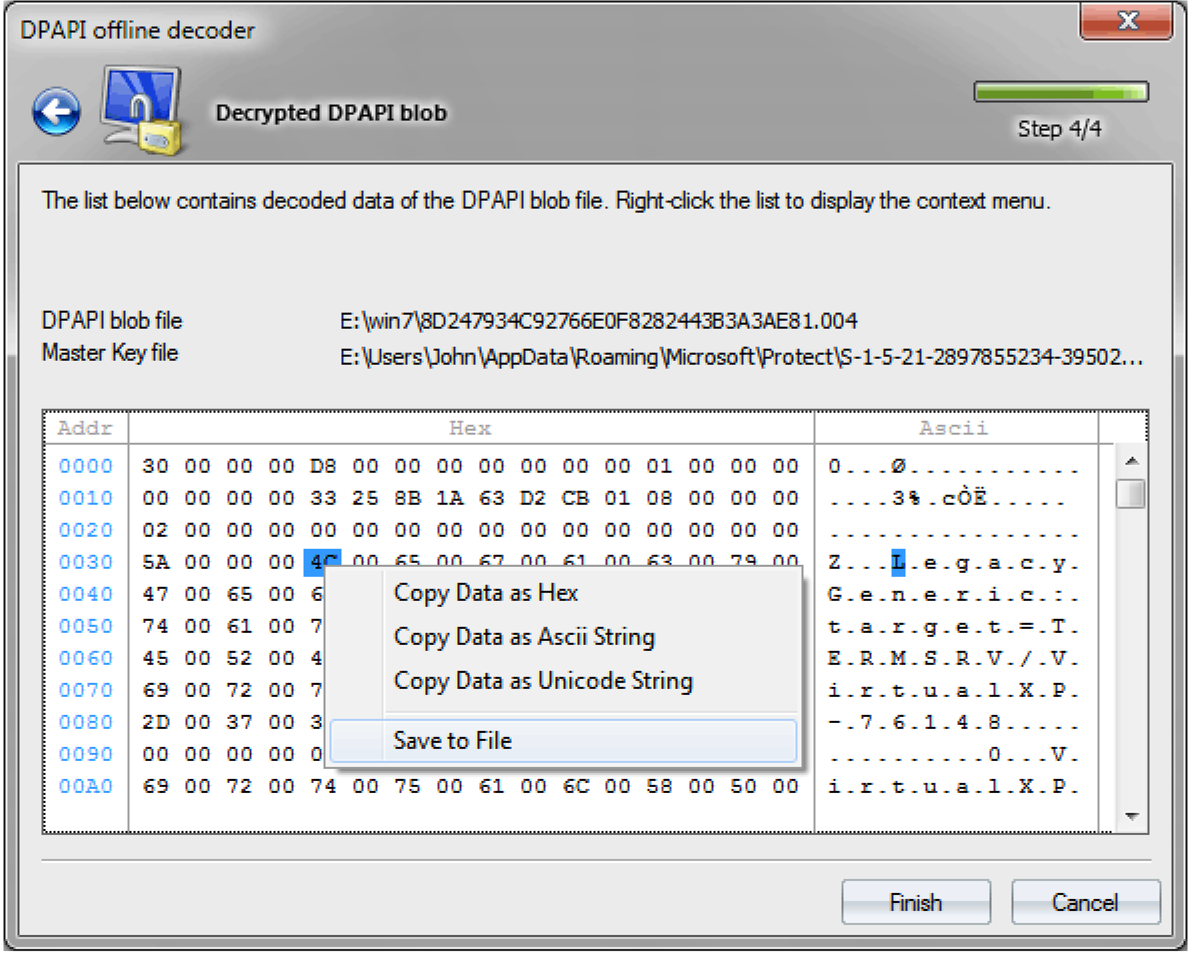
Любопытно, что в Windows 2000 существует серьезная уязвимость благодаря которой для расшифровки любых(!) DPAPI объектов необязательно задавать логон пароль пользователя! Т.е. все данные, защищенные при помощи DPAPI - уязвимы. Это очень серьезная ошибка в реализации DPAPI, о которой знает Microsoft, однако остальные операционные системы лишены этого недостатка. Если при шифровании данных в функции CryptProtectData был указан флаг CRYPTPROTECT_LOCAL_MACHINE, то расшифровка этих данных также возможна без знания пароля на вход пользователя (например, паролей беспроводной сети), но это уже особенности реализации интерфейса и не является ошибкой.

Начиная с версии 9.7, Windows Password Recovery имеет встроенный механизм для обнаружения и использования новых, обнаруженных нами уязвимостей в защите Мастер Ключей DPAPI.

WPR v11.7 поддерживает Trusted Boot Auto-Logon в Windows 10. Если программа обнаруживает, что для пользователя установлен доверенный автоматический вход, для расшифровки данных пароль на вход не потребуется.

В версии WPR v15 появилась пара дополнительных способов расшифровки DPAPI блобов: при помощи PIN, а также автоматическая расшифровка в случае если программа обнаружит использование биометрии, кэшированных паролей и т.д. Для учетных записей, которые используют биометрический вход Windows Hello, возможна расшифровка без знания пароля или PIN кода!

4. Расшифровка данных



DPAPI offline decoder

Decrypted DPAPI blob

Step 4/4

The list below contains decoded data of the DPAPI blob file. Right-click the list to display the context menu.

DPAPI blob file E:\win7\8D247934C92766E0F8282443B3A3AE81.004

Master Key file E:\Users\John\AppData\Roaming\Microsoft\Protect\S-1-5-21-2897855234-39502...

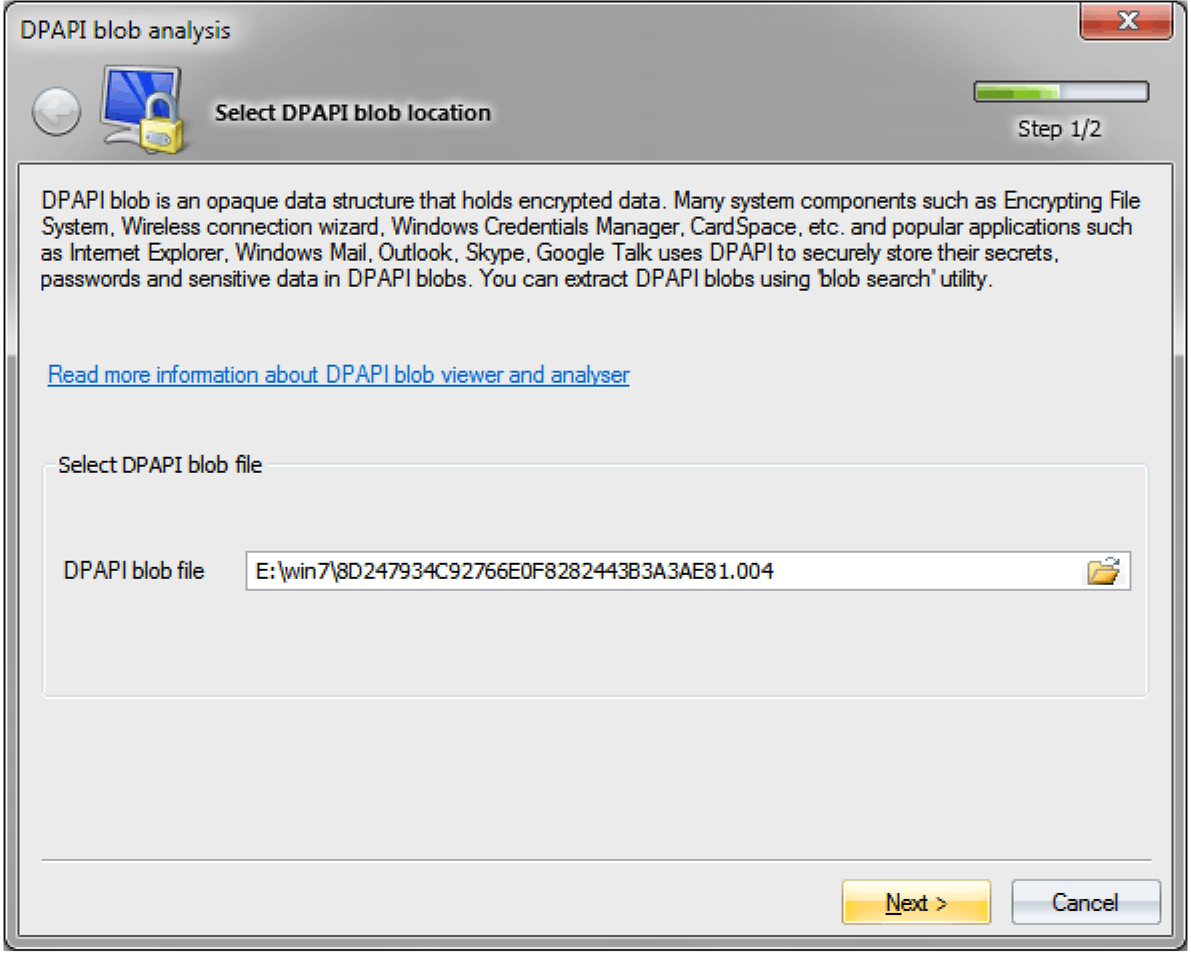
```
Addr  Hex                                                Ascii
0000  30 00 00 00 D8 00 00 00 00 00 00 00 01 00 00 00   0...Ø...........
0010  00 00 00 00 33 25 8B 1A 63 D2 CB 01 08 00 00 00   ....3%.cÒË.....
0020  02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0030  5A 00 00 00 4C 00 65 00 67 00 61 00 63 00 79 00   Z...L.e.g.a.c.y.
0040  47 00 65 00 6                                     G.e.n.e.r.i.c.:.
0050  74 00 61 00 7                                     t.a.r.g.e.t.=.T.
0060  45 00 52 00 4                                     E.R.M.S.R.V./.V.
0070  69 00 72 00 7                                     i.r.t.u.a.l.X.P.
0080  2D 00 37 00 3                                     -.7.6.1.4.8.....
0090  00 00 00 00 0                                     ..........0...V.
00A0  69 00 72 00 74 00 75 00 61 00 6C 00 58 00 50 00   i.r.t.u.a.l.X.P.
```

Имея все необходимое, WPR выполнит расшифровку данных DPAPI объекта, которые затем можно скопировать в буфер обмена или сохранить в файл. Если на финальной стадии расшифровки возникает ошибка, то, скорее всего, вами был неправильно задан или не задан параметр дополнительной энтропии. Например, Internet Explorer и Vista Ftp Manager использует в качестве энтропии исходную страницу, на которой был введен пароль. Windows Credential Manager аналогично использует некоторые строковые константы и т.д.

2.7.4.5.2 Анализ объектов DPAPI (DPAPI blobs)

DPAPI объект (DPAPI blob) - это непрозрачная структура данных, содержащая зашифрованные данные приложения и служебную информацию, необходимую для их расшифровки. Многие программы и подсистемы Windows хранят пароли, секреты и приватные данные в DPAPI объектах. Для создания файлов с DPAPI объектами (и последующего анализа), необходимо воспользоваться нашей утилитой поиска DPAPI структур.

Указываем путь к объекту DPAPI.



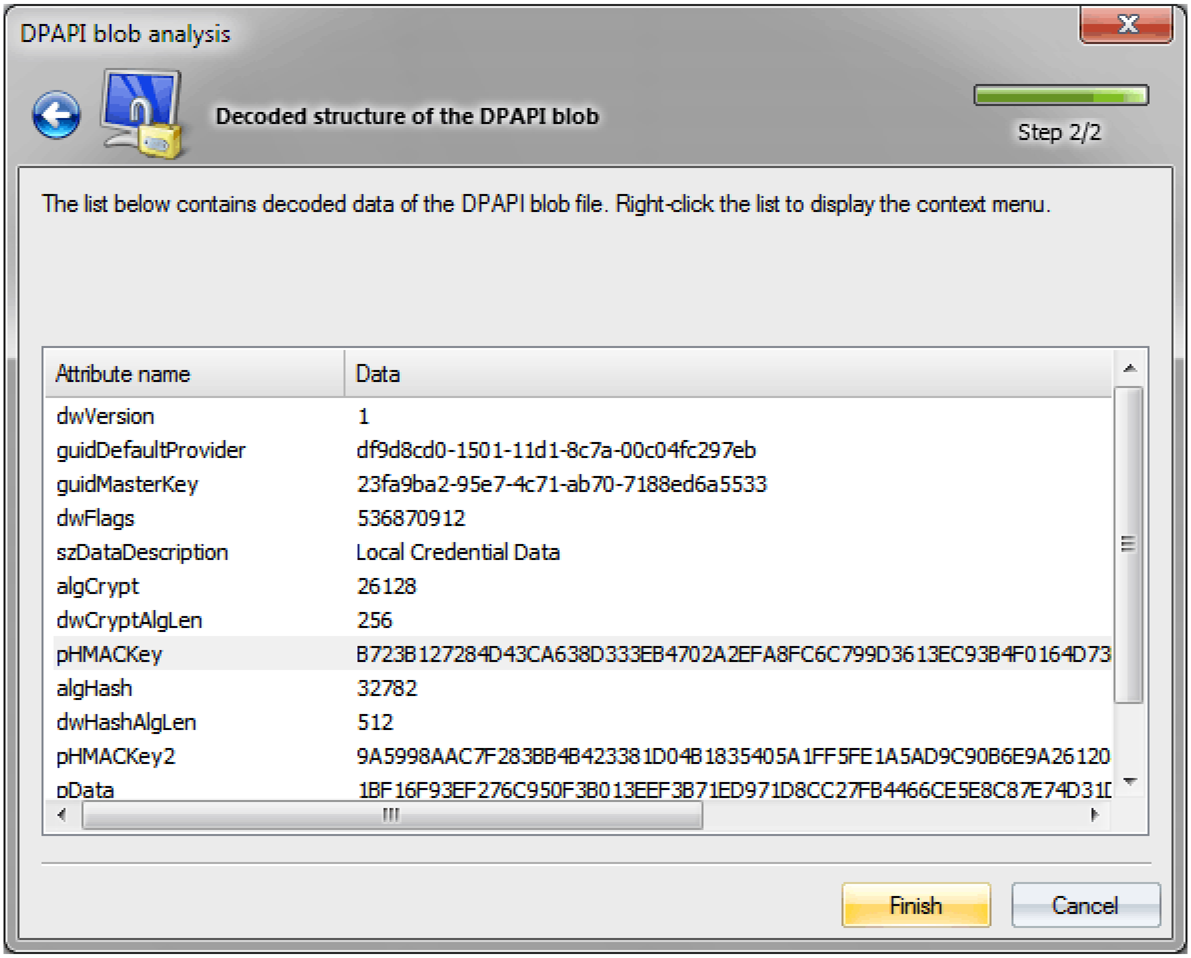
DPAPI blob is an opaque data structure that holds encrypted data. Many system components such as Encrypting File System, Wireless connection wizard, Windows Credentials Manager, CardSpace, etc. and popular applications such as Internet Explorer, Windows Mail, Outlook, Skype, Google Talk uses DPAPI to securely store their secrets, passwords and sensitive data in DPAPI blobs. You can extract DPAPI blobs using 'blob search' utility.

Read more information about DPAPI blob viewer and analyser

Select DPAPI blob file

DPAPI blob file: E:\win7\8D247934C92766E0F8282443B3A3AE81.004

И приступаем к анализу данных.



DPAPI blob analysis

Decoded structure of the DPAPI blob

The list below contains decoded data of the DPAPI blob file. Right-click the list to display the context menu.

Attribute name	Data
dwVersion	1
guidDefaultProvider	df9d8cd0-1501-11d1-8c7a-00c04fc297eb
guidMasterKey	23fa9ba2-95e7-4c71-ab70-7188ed6a5533
dwFlags	536870912
szDataDescription	Local Credential Data
algCrypt	26128
dwCryptAlgLen	256
pHMACKey	B723B127284D43CA638D333EB4702A2EFA8FC6C799D3613EC93B4F0164D73
algHash	32782
dwHashAlgLen	512
pHMACKey2	9A5998AAC7F283BB4B423381D04B1835405A1FF5FE1A5AD9C90B6E9A26120
pData	1BF16F93EF276C950F3B013EEF3B71ED971D8CC27FB4466CE5E8C87E74D31

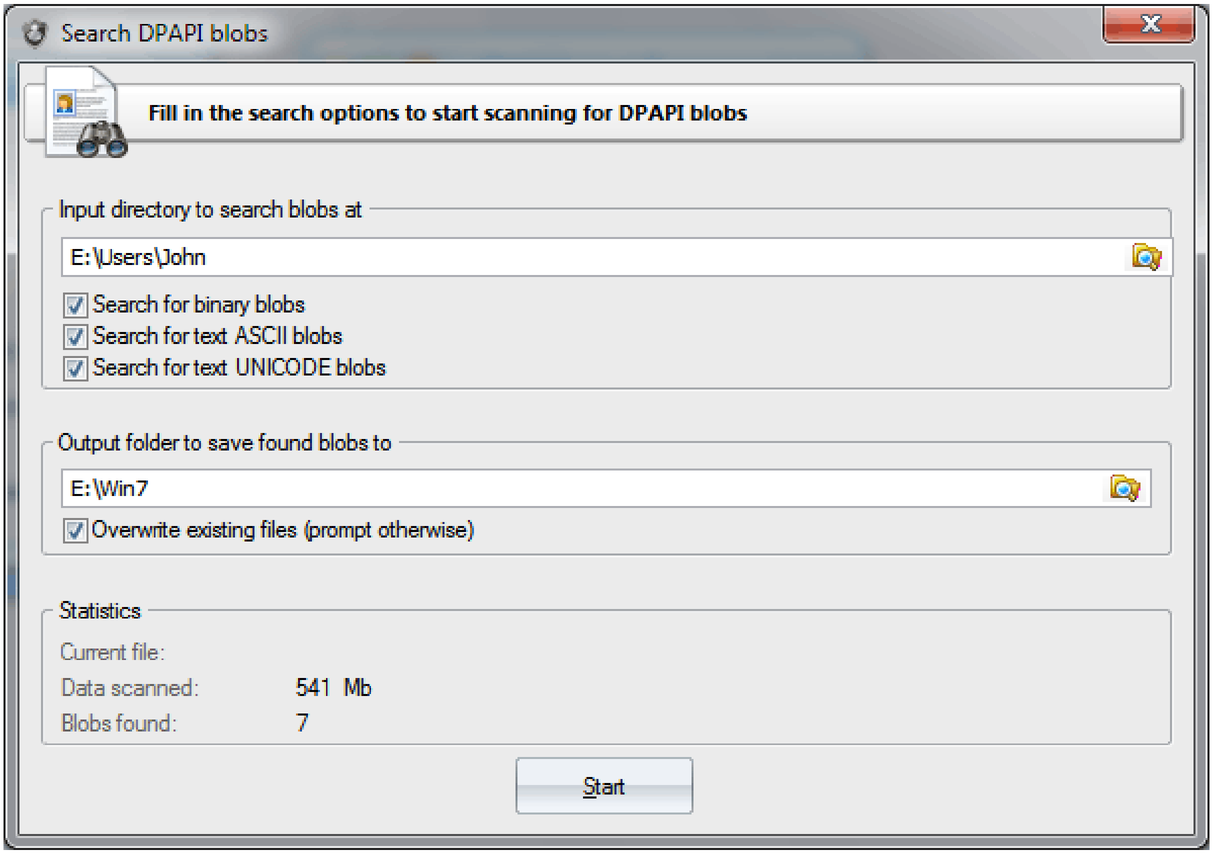
DPAPI объект - это двоичная структура данных, состоящая из следующих друг за другом атрибутов:

- **dwVersion** - версия структуры данных. Текущая версия данных - 1.
- **guidDefaultProvider** - провайдер для шифрования данных, используется в вызовах к функциям шифрования, обеспечивает совместимость версий и организовывает простые криптологические примитивы. Например, в качестве блочного шифра можно задавать Blowfish или RC5. В настоящее время в Windows по умолчанию установлен следующий крипто-провайдер: df9d8cd0-1501-11d1-8c7a-00c04fc297eb, соответствующий ключу реестра HKLM\Microsoft\Cryptography\Protect\Providers\df9d8cd0-1501-11d1-8c7a-00c04fc297eb.
- **guidMasterKey** - GUID Мастер Ключа, с помощью которого зашифрованы данные. Для того, чтобы расшифровать данные в DPAPI объекте, в первую очередь необходимо расшифровать Мастер Ключ, имя которого задано в двоичной структуре guidMasterKey. К объекту DPAPI может быть прикреплен только один Мастер Ключ.
- **dwFlags** - различные флаги. Например установленный бит (dwFlags&4) является индикатором того, что расшифровку данных необходимо производить под учетной записью SYSTEM. Бит (dwFlags&0x20000000) установлен всегда (видимо для обеспечения совместимости).
- **szDataDescription** - описатель данных, который задается опциональным параметром LPCWSTR *szDataDescr* в функции CryptProtectData.
- **algCrypt** - блочный алгоритм шифрования данных. По умолчанию, Windows 7 использует алгоритм AES 256 (что соответствует 0x6610 в шестнадцатеричной или 26128 в десятичной нотации), Windows XP - 3DES, Windows 2000 - RC4.
- **dwCryptAlgLen** - длина ключа шифрования в алгоритме шифрования.
- **pHMACKey** - HMAC ключ 1.
- **pSalt** - соль (опциональный параметр).

- **algHash** - алгоритм хэширования. По умолчанию, Windows 7 использует алгоритм SHA 512, Windows XP и Windows 2000 - SHA1.
- **dwHashAlgLen** - длина хэша в алгоритме хэширования.
- **pHMACKey2** - HMAC ключ 2.
- **pData** - сами зашифрованные данные.
- **pSignHash** - цифровая подпись для проверки целостности данных.

2.7.4.5.3 Поиск объектов DPAPI

Диалог поиска объектов DPAPI довольно тривиален. Все, что необходимо указать, это исходный каталог, в котором будет производиться поиск объектов DPAPI и целевой каталог, куда будут сохраняться найденные объекты. Программа производит поиск как двоичных, так и текстовых объектов.



Fill in the search options to start scanning for DPAPI blobs

Input directory to search blobs at

E:\Users\John

☑ Search for binary blobs
☑ Search for text ASCII blobs
☑ Search for text UNICODE blobs

Output folder to save found blobs to

E:\Win7

☑ Overwrite existing files (prompt otherwise)

Statistics

Current file:
Data scanned: 541 Mb
Blobs found: 7

Пример пути, в которых можно обнаружить файлы, содержащие двоичные объекты DPAPI:
C:\Users\John\AppData\Roaming\Microsoft\Credentials

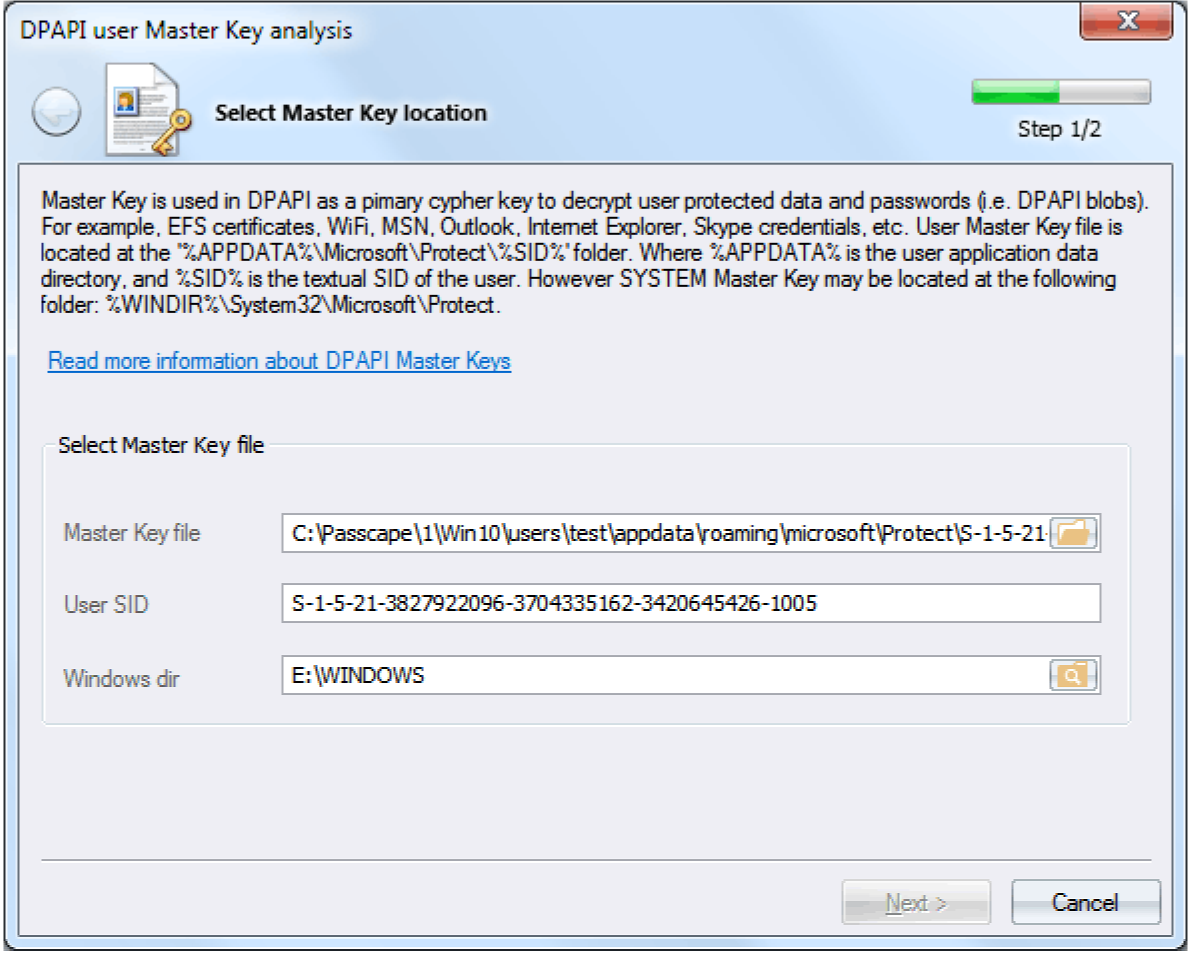
Пример пути, в которых можно обнаружить файлы, содержащие текстовые объекты DPAPI:
C:\ProgramData\Microsoft\Wlansvc

Keep in mind that before searching for blobs in current user's registry files or in the current Active Directory database, you must first back up those files to a separate directory.

2.7.4.5.4 Анализ Мастер Ключа

Мастер Ключ представляет собой 64 байта данных, которые используются в качестве первичного ключа при расшифровке DPAPI объекта. Мастер Ключ пользователя зашифрован при помощи пароля на вход пользователя.

Задаем путь к файлу с Мастер Ключом и прописываем SID пользователя, который программа, как правило, вычисляет автоматически из указанного пути.



Master Key is used in DPAPI as a pimary cypher key to decrypt user protected data and passwords (i.e. DPAPI blobs). For example, EFS certificates, WiFi, MSN, Outlook, Internet Explorer, Skype credentials, etc. User Master Key file is located at the "%APPDATA%\Microsoft\Protect\%SID%" folder. Where %APPDATA% is the user application data directory, and %SID% is the textual SID of the user. However SYSTEM Master Key may be located at the following folder: %WINDIR%\System32\Microsoft\Protect.

Read more information about DPAPI Master Keys

Select Master Key file

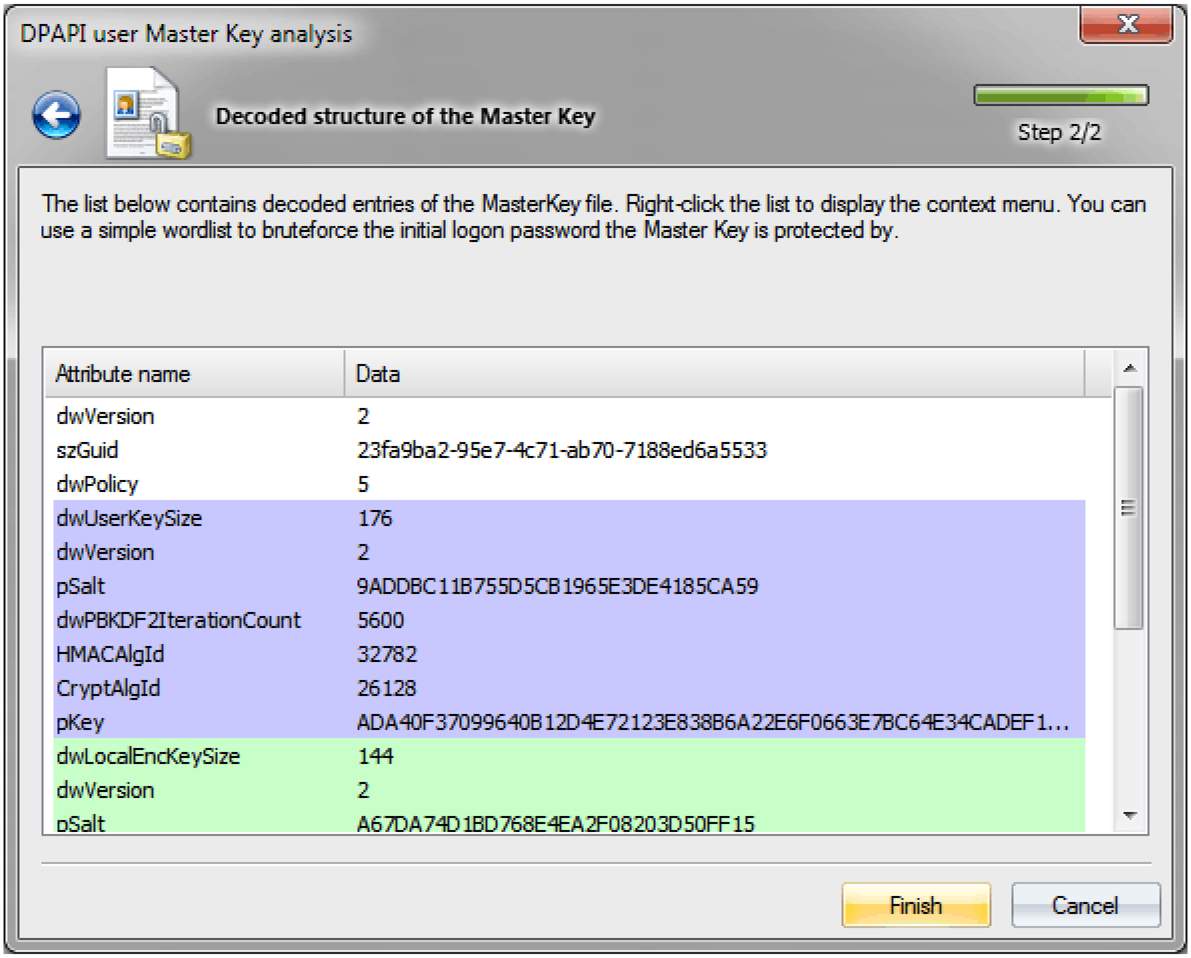
Master Key file: C:\Passcape\1\Win10\users\test\appdata\roaming\microsoft\Protect\S-1-5-21

User SID: S-1-5-21-3827922096-3704335162-3420645426-1005

Windows dir: E:\WINDOWS

Все Мастер Ключи пользователя находятся в папке **%APPDATA%\Microsoft\Protect\%SID%**. Например,
E:\Users\John\AppData\Roaming\Microsoft\Protect\S-1-5-21-2897849034-3956381361-16091305341-1001\23ab9bc1-9397-4cb1-ab74-7166ed6a8713
Мастер Ключи системы складируются в каталоге **%SYSTEMDIR%\Microsoft\Protect**.

Производим анализ Мастер Ключа


DPAPI user Master Key analysis
Decoded structure of the Master Key
Step 2/2
Finish
Cancel

The list below contains decoded entries of the MasterKey file. Right-click the list to display the context menu. You can use a simple wordlist to bruteforce the initial logon password the Master Key is protected by.

Attribute name	Data
dwVersion	2
szGuid	23fa9ba2-95e7-4c71-ab70-7188ed6a5533
dwPolicy	5
dwUserKeySize	176
dwVersion	2
pSalt	9ADDBC11B755D5CB1965E3DE4185CA59
dwPBKDF2IterationCount	5600
HMACAlgId	32782
CryptAlgId	26128
pKey	ADA40F37099640B12D4E72123E838B6A22E6F0663E7BC64E34CADEF1...
dwLocalEncKeySize	144
dwVersion	2
pSalt	A67DA74D1BD768E4EA2F08203D50FF15

Файл с Мастер Ключом представляет собой двоичную структуру, состоящую из служебного заголовка и четырех слотов, а именно:
непосредственно самого Мастер Ключа пользователя, локального ключа шифрования (для расшифровки резервных ключей), локального резервного ключа (для Win2K) или GUID для файла CREDHIST (Windows XP и выше) и резервного ключа домена.

Список со структурой Мастер Ключа состоит из имени атрибута (т.е. двоичного поля) и соответствующего ему значения. Каждая секция выделена своим цветом:

- поле с атрибутами заголовка

🟦 - слот с атрибутами Мастер Ключа пользователя

🟩 - слот с атрибутами Локального Ключа шифрования

🟥 - слот с атрибутами Локального Резервного Ключа или GUID файла CREDHIST

🟨 - слот с атрибутами Резервного Ключа Домена

Теперь немного поподробнее.

Атрибуты заголовка

- **dwVersion** - версия файла с Мастер Ключом.
- **szGuid** - текстовый идентификатор (GUID) мастер ключа. Как правило, он совпадает с именем файла.
- **dwPolicy** - различные флаги. Например, если установлен следующий бит (dwPolicy&4), то при расшифровке ключа используется SHA1 хэш пароля пользователя, иначе MD4. Так в Windows 2000 этот бит сброшен. Установленный бит (dwPolicy&2) говорит о том, что для Мастер Ключа требуется резервное копирование.

Атрибуты Мастер Ключа пользователя

- **dwUserKeySize** - длина текущего слота.
- **dwVersion** - версия структуры данных. В версии 1 используется только атрибут с солью.
- **pSalt** - соль, т.е. случайные 16 байт данных, задействованные в расшифровке Мастер Ключа и предотвращающие взлом данных при помощи атаки по радужным таблицам.
- **dwPBKDF2IterationCount** - количество итераций в функции генерации ключа шифрования PBKDF2.
- **HMACAlgId** - идентификатор алгоритма хэширования.
- **CryptAlgId** - идентификатор блочного шифра.
- **pKey** - зашифрованный Мастер Ключ пользователя.

Атрибуты Локального Ключа шифрования

- **dwLocalEncKeySize** - длина текущего слота.
- **dwVersion** - версия структуры данных. В Win2K используется только атрибут с солью.
- **pSalt** - соль.
- **dwPBKDF2IterationCount** - количество итераций в функции генерации ключа шифрования PBKDF2.
- **HMACAlgId** - идентификатор алгоритма хэширования.
- **CryptAlgId** - идентификатор блочного шифра.
- **pKey** - зашифрованный Локальный Ключ шифрования, который используется для расшифровки Локального Резервного Ключа в Win2K.

Атрибуты Локального Резервного Ключа (Windows 2000)

- **dwLocalKeySize** - длина текущего слота.
- **dwVersion** - версия структуры данных.
- **pSalt** - соль.
- **pKey** - зашифрованный Локальный Резервный Ключ.

Атрибуты GUID для файла CREDHIST (Windows XP и выше)

- **dwLocalKeySize** - длина текущего слота.
- **dwVersion** - версия структуры данных.
- **guidCredHist** - двоичный идентификатор файла CREDHIST.

Атрибуты Резервного Ключа Домена

- **dwDomainKeySize** - длина текущего слота.
- **dwVersion** - версия структуры данных.
- **pSalt** - соль, т.е. случайные 16 байт данных, задействованные в расшифровке Мастер Ключа и предотвращающие взлом данных при помощи атаки по радужным таблицам.
- **dwPBKDF2IterationCount** - количество итераций в функции генерации ключа шифрования PBKDF2.
- **HMACAlgId** - идентификатор алгоритма хэширования.
- **CryptAlgId** - идентификатор блочного шифра.
- **pKey** - зашифрованный Резервный Ключ Домена. Для его расшифровки требуется ключ шифрования домена, хранящийся в базе данных Active Directory.

Для расшифровки Мастер Ключа пользователя требуется знать его пароль на вход или ПИН код. Из контекстного меню анализатора можно проверить пароль или PIN, а также попробовать подобрать его с помощью словаря. Однако, не стоит обольщаться слишком сильно. Если в Windows 2000 скорость подбора исчисляется десятками или даже сотнями тысяч паролей в секунду, то в Windows 7 счет идет уже на единицы. Смотрите таблицу ниже (скорость измерена для одном ядре процессора Intel Q8400 2.66GHz).

ОС	**Алгоритм шифрования**	**Алгоритм хэширования**	**PKCS#5 PBKDF2 rounds**	**Скорость подбора (п/с)**
Windows 2000	RC4	SHA1	1	**95000**
Windows XP	3DES	SHA1	4000	**76**
Windows Vista	3DES	SHA1	24000	**12**
Windows 7	AES256	SHA512	5600	**10**
Windows 10-11	AES256	SHA512	8000	**7**

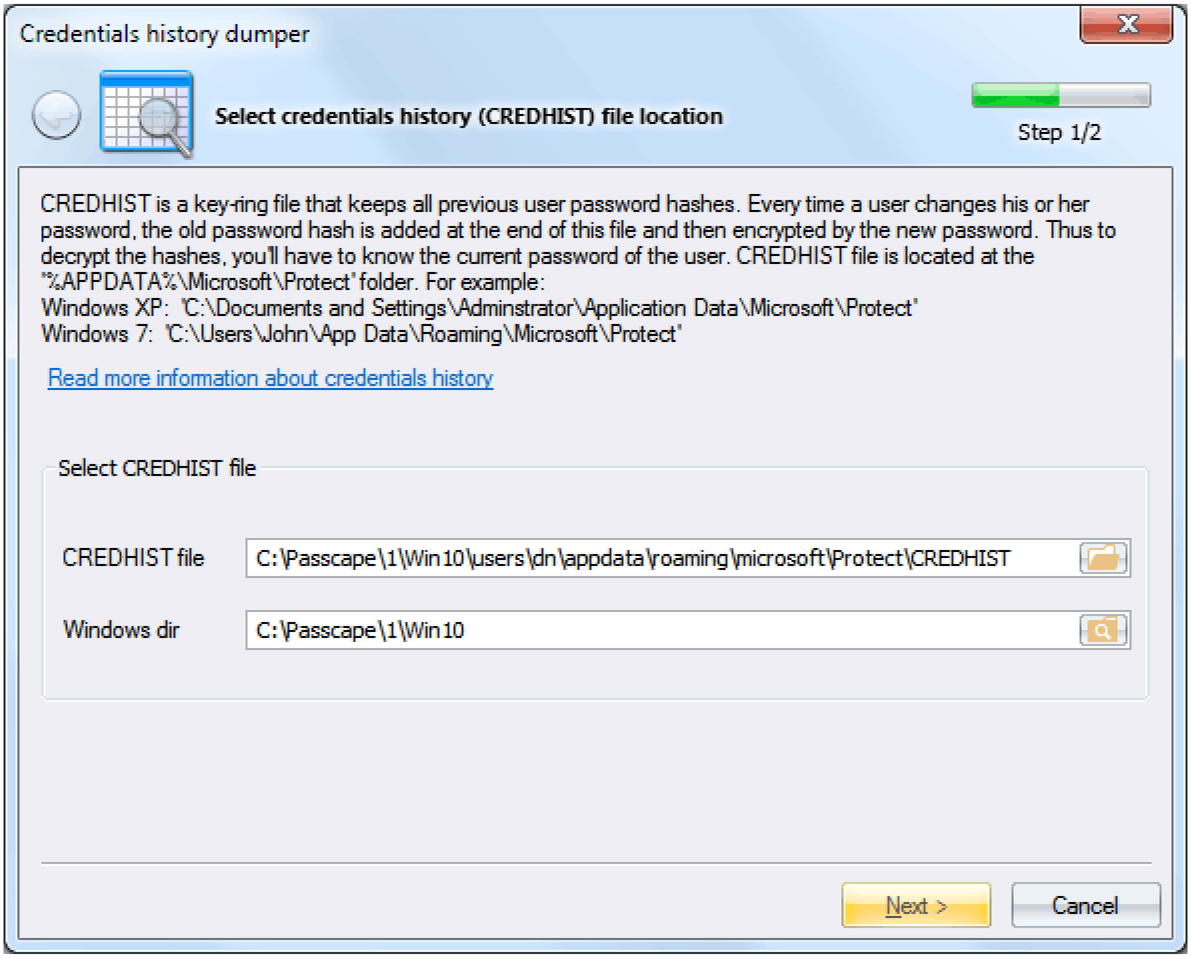
2.7.4.5.5 Дамп хэшей истории паролей из CREDHIST

Из-за особенности реализации DPAPI, для того, чтобы гарантированно расшифровывать все объекты DPAPI, Windows приходится хранить все предыдущие пароли пользователя в системе. История паролей пользователя хранится в следующем файле:
%APPDATA%\Microsoft\Protect\credhist

Все предыдущие пароли пользователя (наряду с некоторой служебной информацией) хранятся в виде пары хэшей: SHA1 и NTLM. Причем, для того, чтобы расшифровать последнюю пару, надо знать хэш текущего пароля пользователя, для расшифровки предыдущих хэшей необходима последняя расшифрованная пара и т.д. по цепочке.

Windows Password Recovery - первая утилита в мире, которая позволяет расшифровывать хэши истории паролей из файлов **CREDHIST**.

Для этого необходимо на первом шаге мастера программы задать путь к файлу CREDHIST и каталогу Windows.



Select credentials history (CREDHIST) file location

CREDHIST is a key-ring file that keeps all previous user password hashes. Every time a user changes his or her password, the old password hash is added at the end of this file and then encrypted by the new password. Thus to decrypt the hashes, you'll have to know the current password of the user. CREDHIST file is located at the "%APPDATA%\Microsoft\Protect" folder. For example:
Windows XP: "C:\Documents and Settings\Adminstrator\Application Data\Microsoft\Protect"
Windows 7: "C:\Users\John\App Data\Roaming\Microsoft\Protect"

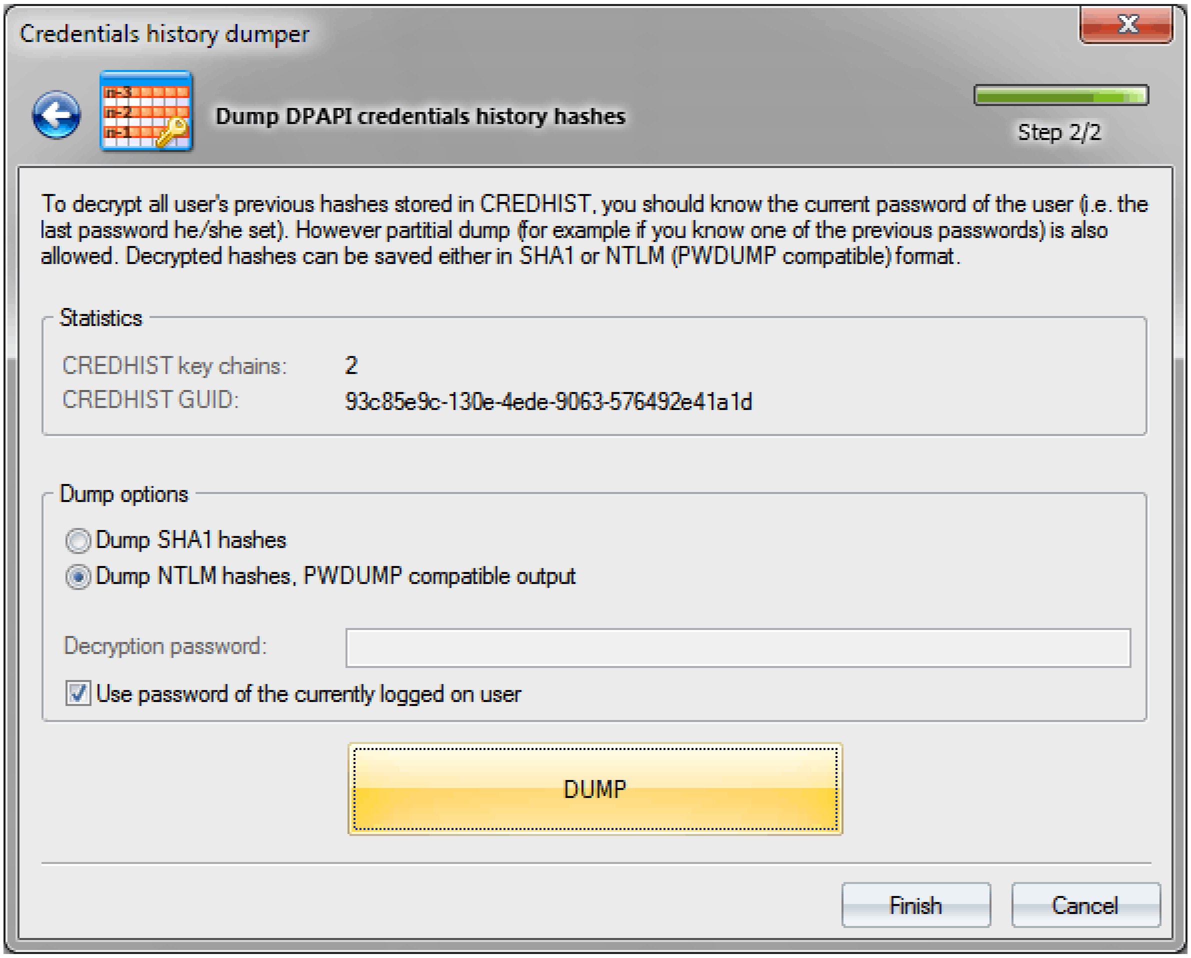
Read more information about credentials history

Select CREDHIST file

CREDHIST file: C:\Passcape\1\Win10\users\dn\appdata\roaming\microsoft\Protect\CREDHIST

Windows dir: C:\Passcape\1\Win10

После этого возможна расшифровка и сохранение хэшей из CREDHIST в текстовый PWDUMP файл, если выбрано сохранение в формате **NTLM**, либо в простой текстовый файл, если выбран формат **SHA1** хэшей.



Credentials history dumper
Dump DPAPI credentials history hashes
Step 2/2

To decrypt all user's previous hashes stored in CREDHIST, you should know the current password of the user (i.e. the last password he/she set). However partitial dump (for example if you know one of the previous passwords) is also allowed. Decrypted hashes can be saved either in SHA1 or NTLM (PWDUMP compatible) format.

Statistics

CREDHIST key chains: 2
CREDHIST GUID: 93c85e9c-130e-4ede-9063-576492e41a1d

Dump options

○ Dump SHA1 hashes
● Dump NTLM hashes, PWDUMP compatible output

Decryption password:

☑ Use password of the currently logged on user

Важно знать, что для расшифровки хэшей CREDHIST необходимо знать текущий пароль пользователя или его PIN. Если производится расшифровка CREDHIST текущего залогиненного пользователя, выставите соответствующую опцию. В этом случае пароль для расшифровки вводить не надо - он будет взят из кэша системы (убедитесь, что Антивирусное ПО, установленное на компьютере, не блокирует доступ к системной памяти).

Программа поддерживает частичную расшифровку хэшей истории. Это означает, что если текущий пароль пользователя неизвестен, но есть один из старых паролей, то программа сможет расшифровать те пароли, которые использовались пользователем ранее, т.е. до того, как был введен этот старый пароль.

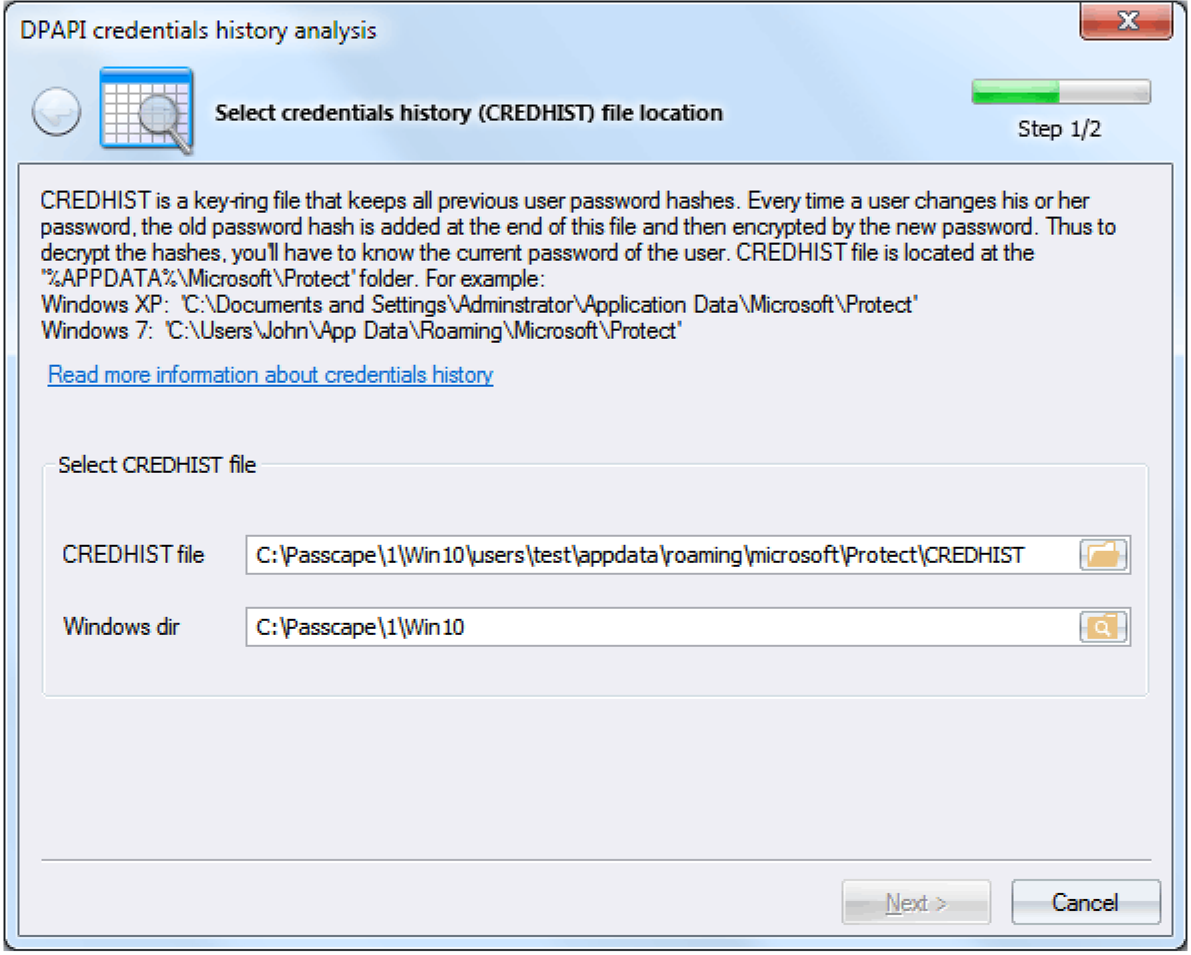
Имейте в виду, в Windows 8 и более поздних операционных системах сохраняемые хэши учетных записей LiveID/Microsoft/AzureAD не совпадают с хэшами паролей.

2.7.4.5.6 Анализ истории паролей (CREDHIST)

CREDHIST - файл истории паролей, выполненный в виде цепочки, каждое звено которой представляют собой хэши предыдущих паролей пользователя. Каждый раз, когда пользователь меняет свой пароль, хэш старого пароля добавляется к концу файла и шифруется новым паролем. Поэтому, чтобы расшифровать все хэши в цепочке, необходимо знать текущий пароль пользователя.

Кроме хэшей, в цепочках хранится другая служебная информация, анализ которой и является целью данной утилиты.

Выбираем файл CREDHIST



DPAPI credentials history analysis
Select credentials history (CREDHIST) file location
Step 1/2

CREDHIST is a key-ring file that keeps all previous user password hashes. Every time a user changes his or her password, the old password hash is added at the end of this file and then encrypted by the new password. Thus to decrypt the hashes, you'll have to know the current password of the user. CREDHIST file is located at the "%APPDATA%\Microsoft\Protect" folder. For example:
Windows XP: 'C:\Documents and Settings\Adminstrator\Application Data\Microsoft\Protect'
Windows 7: 'C:\Users\John\App Data\Roaming\Microsoft\Protect'

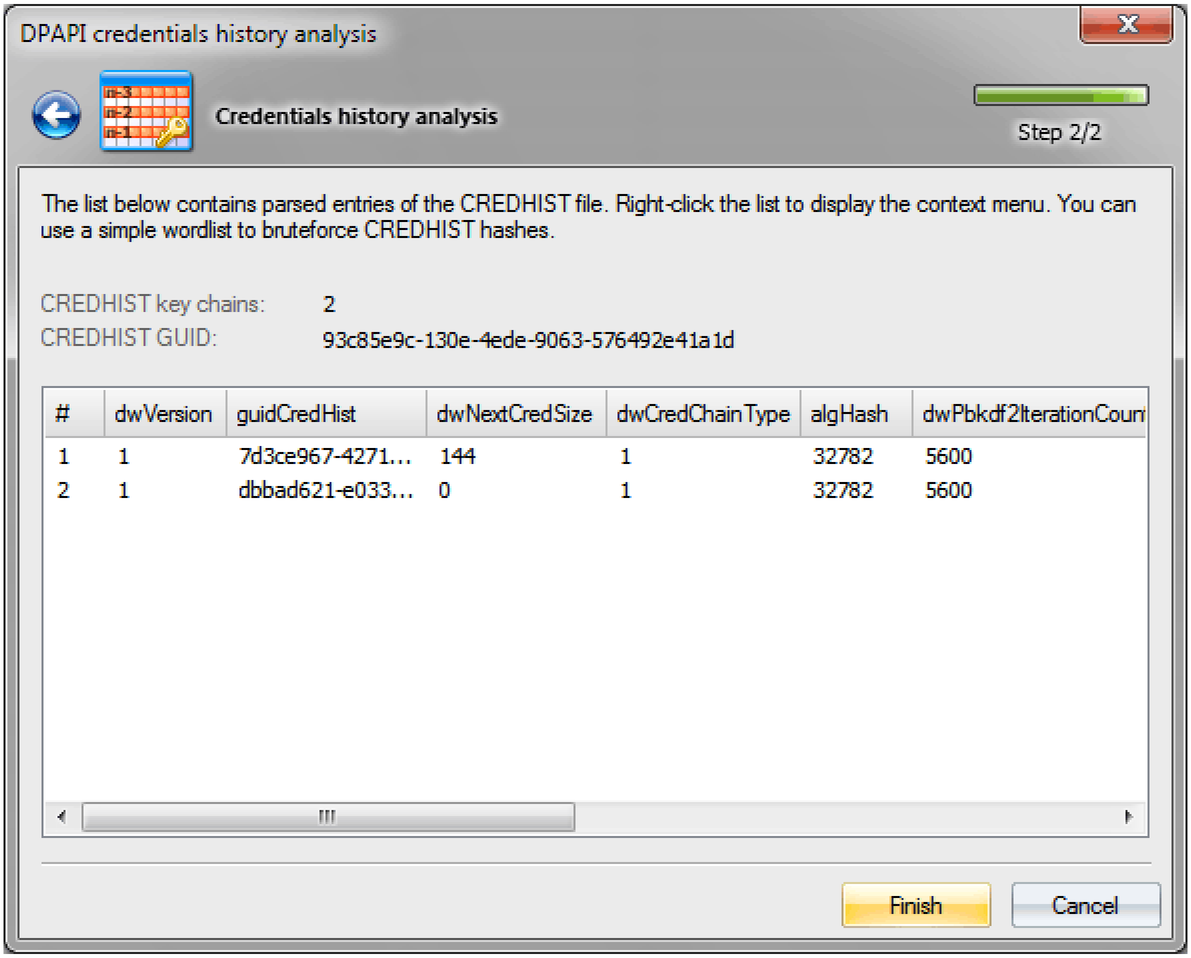
Read more information about credentials history

Select CREDHIST file

CREDHIST file: C:\Passcape\1\Win10\users\test\appdata\roaming\microsoft\Protect\CREDHIST

Windows dir: C:\Passcape\1\Win10

И приступаем к анализу содержимого


DPAPI credentials history analysis
Credentials history analysis
Step 2/2
Finish
Cancel

The list below contains parsed entries of the CREDHIST file. Right-click the list to display the context menu. You can use a simple wordlist to bruteforce CREDHIST hashes.

CREDHIST key chains: 2
CREDHIST GUID: 93c85e9c-130e-4ede-9063-576492e41a1d

#	dwVersion	guidCredHist	dwNextCredSize	dwCredChainType	algHash	dwPbkdf2IterationCoun
1	1	7d3ce967-4271...	144	1	32782	5600
2	1	dbbad621-e033...	0	1	32782	5600

На скриншоте видно, что уникальный идентификатор CREDHIST - 93c85e9c-130e-4ede-9063-576492e41a1d. Именно к этому идентификатору (GUID) прикреплены все мастер ключи пользователя в системе. Число звеньев в цепи хэшей - 2.

Далее в таблице подробно описаны атрибуты и их значения для каждого звена нашего CREDHIST.

<u>Описание атрибутов</u>

- **dwVersion** - версия структуры данных
- **guidLink** - уникальный идентификатор звена
- **dwNextLinkSize** - размер следующего звена
- **dwLinkType** - тип звена
- **algHash** - алгоритм хэширования, который используется в расшифровке звена цепи
- **dwPbkdf2IterationCount** - количество итераций в алгоритме генерации ключа PKCS#5 PBKDF2
- **dwSidSize** - размер описателя безопасности (SID) владельца
- **algCrypt** - алгоритм шифрования
- **dwShaHashSize** - размер SHA1 хэша
- **dwNtHashSize** - размер NTLM хэша
- **pSalt** - соль, используемая при шифровании
- **sidUser** - SID владельца данных
- **pShaHash** - SHA1 хэш
- **pNtHash** - NTLM хэш

Для подбора оригинального пароля CREDHIST, щелкните правой кнопкой на списке атрибутов и в появившемся контекстном меню выберите пункт '*Использовать словарь для проверки пароля...*'. Можно проверять пароль как текущей выбранной записи, так и всех записей. При этом время проверки будет увеличено пропорционально количеству записей (т.е. цепочек).

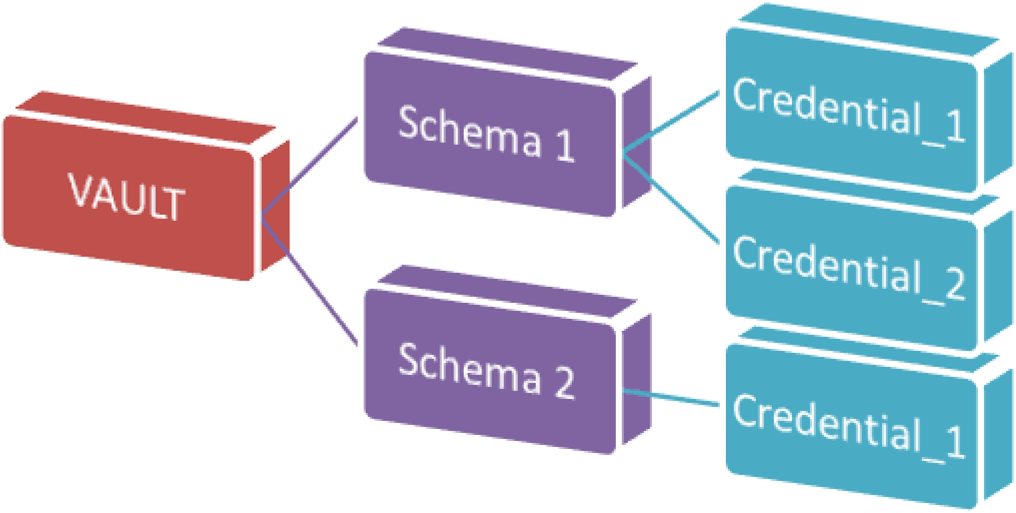
Смотрите сравнительную таблицу скорости подбора оригинального пароля CREDHIST. Скорость измерена для одном ядре процессора Intel Q8400 2.66GHz для ОС, настроенные по умолчанию (например,в Windows 7 количество раундов в PBKDF2 может быть иным).

ОС	**Алгоритм шифрования**	**Алгоритм хэширования**	**Счетчик PBKDF2**	**Скорость подбора (п/с)**
Windows XP	3DES	SHA1	4000	**76**
Windows Vista	3DES	SHA1	24000	**12**
Windows 7	AES256	SHA512	5600	**10**
Windows 10-11	AES256	SHA512	8000	**7**

2.7.4.6 Обозреватель Windows Vault

Что такое Windows Vault

Windows Vault представляет собой защищенное хранилище секретов, паролей и другой персональной информации пользователя и системы. Данные, хранимые в Windows Vault, структуированы и представляют собой набор записей (credentials), принадлежащих определенной схеме Vault.



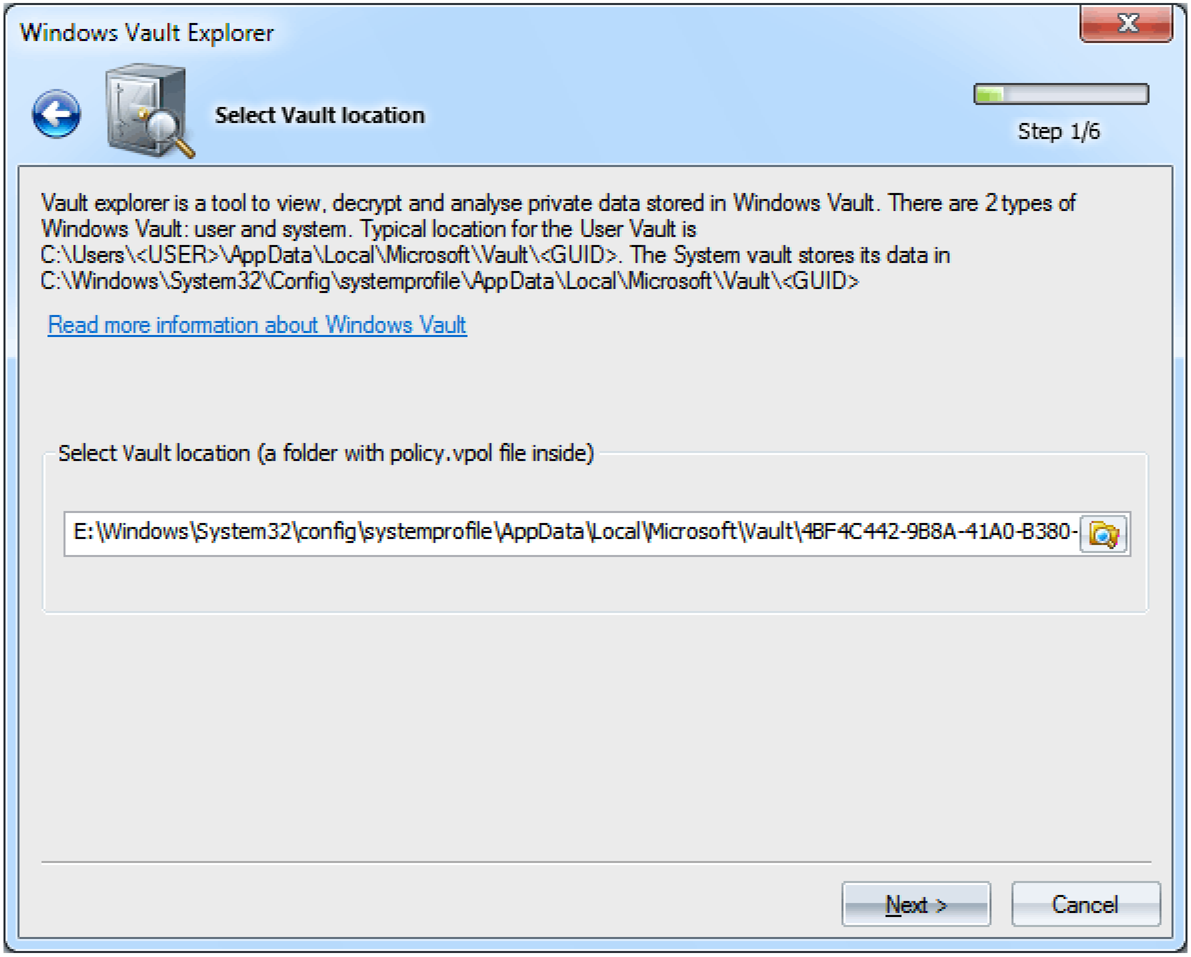
На физическом уровне Vault - это каталог с набором следующих файлов:
Policy.vpol - набор ключей шифрования для записей Vault. Данные ключи могут быть защищены при помощи двух основным методов: с помощью DPAPI, либо с помощью пароля пользователя. Последний тип защиты не используется в Windows 8 и в настоящее время не поддерживается программой.
<GUID>.vsch - схема Vault, содержащая описатели структур, флаги и др. служебную информацию.
<GUID>.vcrd - запись Vault, в которой находятся исходные зашифрованные данные, относящиеся к определенной схеме. Данные могут состоять и, как правило, состоят из нескольких полей.

Обозреватель Windows Vault

Обозреватель Windows Vault представляет собой утилиту для анализа и расшифровки записей Vault в оффлайн режиме. Для этого Мастер расшифровки разбивает весь процесс на несколько последовательных этапов.

1. Поиск каталога Vault
2. Поиск Мастер Ключа пользователя или системы
3. Указание файлов реестра и другой информации, необходимой для расшифровки Мастер Ключа
4. Выбор схемы Vault
5. Поиск записей Vault, принадлежащих выбранной схеме
6. Расшифровка записи

Поиск каталога Vault



Vault explorer is a tool to view, decrypt and analyse private data stored in Windows Vault. There are 2 types of Windows Vault: user and system. Typical location for the User Vault is C:\Users\<USER>\AppData\Local\Microsoft\Vault\<GUID>. The System vault stores its data in C:\Windows\System32\Config\systemprofile\AppData\Local\Microsoft\Vault\<GUID>

Read more information about Windows Vault

Select Vault location (a folder with policy.vpol file inside)

E:\Windows\System32\config\systemprofile\AppData\Local\Microsoft\Vault\4BF4C442-9B8A-41A0-B380-

В настоящее время существует два типа хранилища Vault: системное и пользовательское. Пользовательский Vault может быть расположен в следующих каталогах:

<USER_APP_DATA>\Microsoft\Vault\<GUID>
<USER_LOCAL_APP_DATA>\Microsoft\Vault\<GUID>

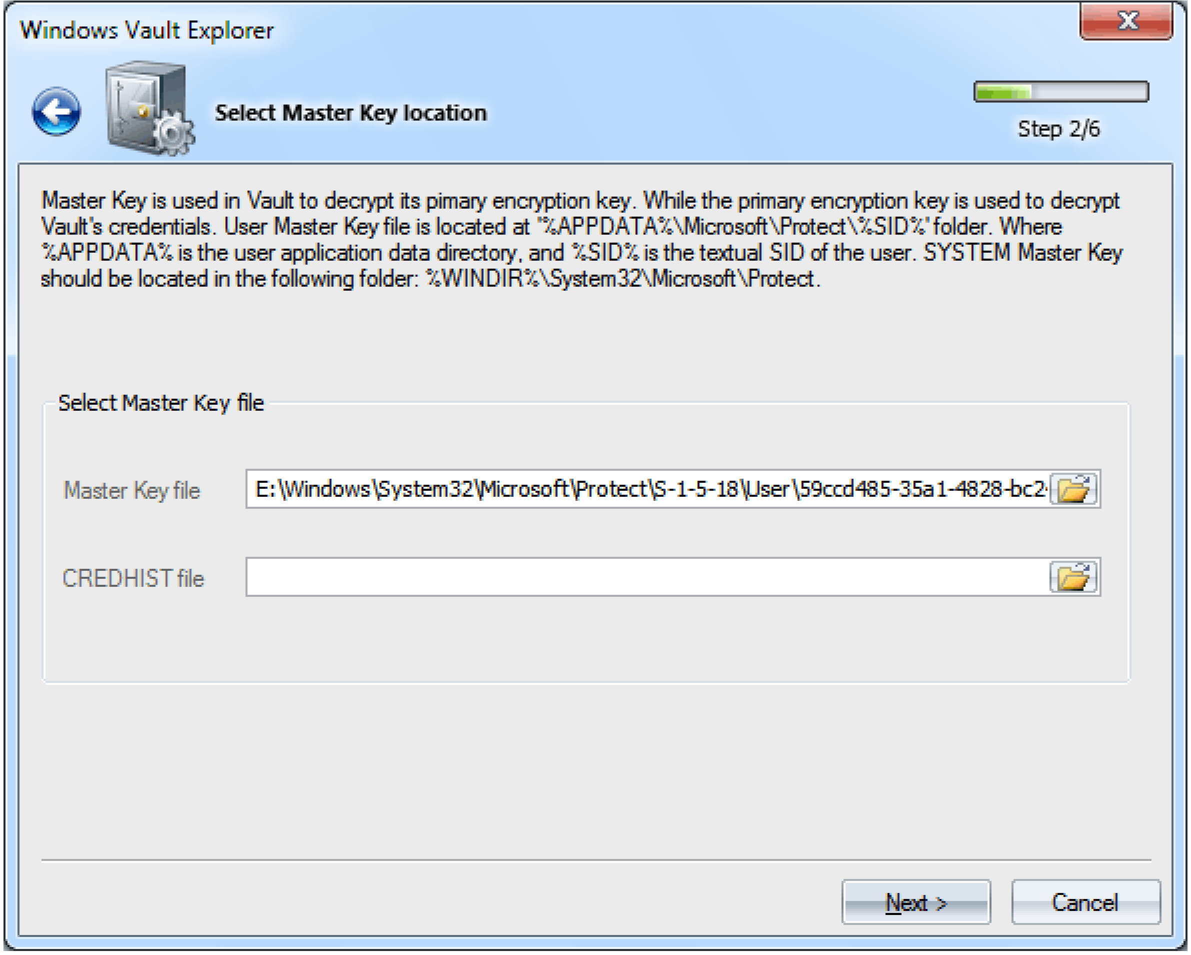
Например,
C:\Users\John\AppData\Local\Microsoft\Vault\18289F5D-9783-43EC-A50D-52DA022B046E
C:\Users\Helen\AppData\Roaming\Microsoft\Vault\4BF4C442-9B8A-41A0-B380-DD4A704DDB28

Системный Vault по-умолчанию расположен в следующих каталогах:

<SYSTEM_APP_DATA>\Microsoft\Vault\<GUID>
<SYSTEM_LOCAL_APP_DATA>\Microsoft\Vault\<GUID>
<PROGRAM_DATA>\Microsoft\Vault\<GUID>
Например,
C:\Windows\System32\config\systemprofile\AppData\Local\Microsoft\Vault\4BF4C442-9B8A-41A0-B380-DD4A704DDB28
C:\Windows\System32\config\systemprofile\AppData\Roaming\Microsoft\Vault\4BF4C442-9B8A-41A0-B380-DD4A704DDB28
C:\ProgramData\Microsoft\Vault\AC658CB4-9126-49BD-B877-31EEDAB3F204

Учтите, некоторые из указанных каталогов имеют системный атрибут, делающий эти каталоги скрытыми.

Выбор Мастер Ключа



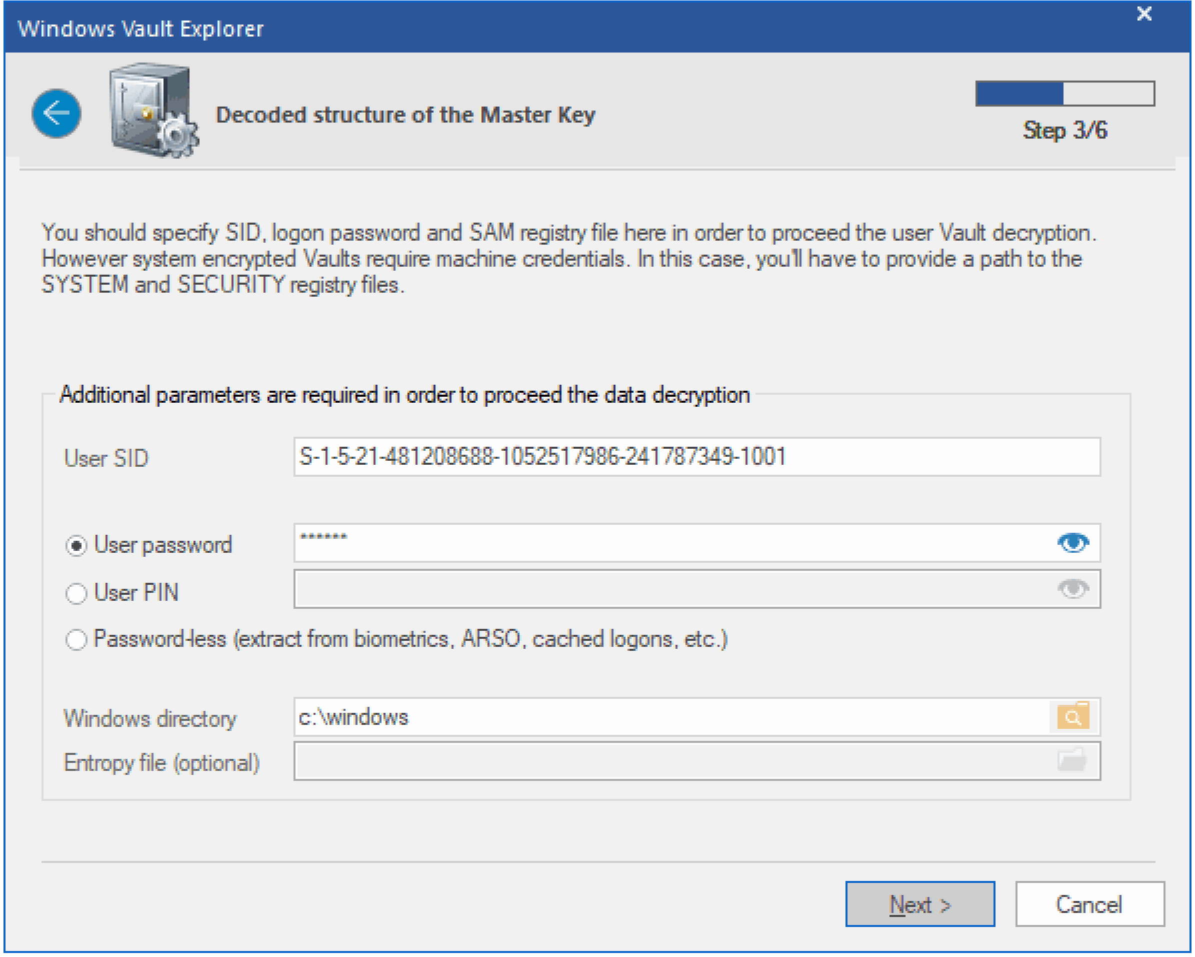
Master Key is used in Vault to decrypt its pimary encryption key. While the primary encryption key is used to decrypt Vault's credentials. User Master Key file is located at "%APPDATA%\Microsoft\Protect\%SID%' folder. Where %APPDATA% is the user application data directory, and %SID% is the textual SID of the user. SYSTEM Master Key should be located in the following folder: %WINDIR%\System32\Microsoft\Protect.

Master Key file: E:\Windows\System32\Microsoft\Protect\S-1-5-18\User\59ccd485-35a1-4828-bc2

CREDHIST file:

После того, как выбран определенный каталог Vault, необходимо указать путь к Мастер Ключу, использующегося в защите ключей шифрования Vault. Мастер Ключ пользователя всегда располагается в каталоге **%APPDATA%\Microsoft\Protect\%SID%**, а Мастер Ключи системной учетной записи хранятся в директории **%SYSTEMDIR%\Microsoft\Protect**. Надо отметить, что Мастер Ключей может быть несколько, а для расшифровки определенного объекта подойдет только один, имя которого хранится внутри файла Policy.vpol. При поиске Мастер Ключа, программа может фильтровать ненужные имена.

Расшифровка Мастер Ключа



You should specify SID, logon password and SAM registry file here in order to proceed the user Vault decryption. However system encrypted Vaults require machine credentials. In this case, you'll have to provide a path to the SYSTEM and SECURITY registry files.

Additional parameters are required in order to proceed the data decryption

User SID: S-1-5-21-481208688-1052517986-241787349-1001

● User password: ******

○ User PIN

○ Password-less (extract from biometrics, ARSO, cached logons, etc.)

Windows directory: c:\windows

Entropy file (optional):

Для расшифровки Мастер Ключа пользователя необходимо задать как минимум два параметра: пароль пользователя на вход и его идентификатор безопасности (SID), который обычно прописан в пути к Мастер Ключу. Программа определяет SID пользователя автоматически. Если это по какой-либо причине сделано не было, укажите его сами. Для расшифровки системного Мастер Ключа задавать пароль не нужно, всю необходимую информацию программа получает из двух файлов реестра: **SYSTEM** и **SECURITY**.

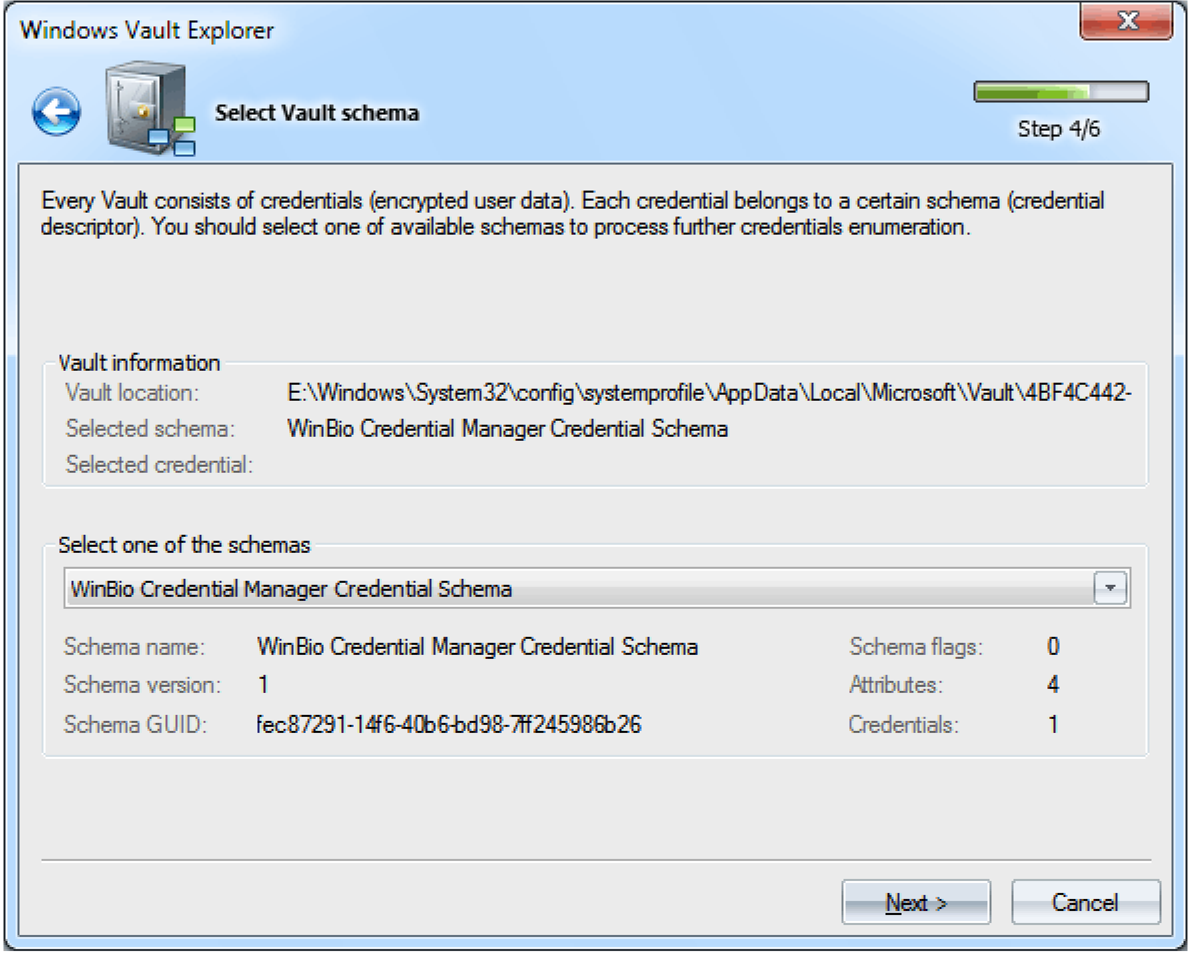
Расшифровка Мастер Ключа пользователя в некоторых случаях требует указания пути к файлу реестра **SAM**. Это необходимо сделать только в том случае, если учетная запись владельца данных Windows 8 имеет тип **LiveID**.

Начиная с версии 9.7, Windows Password Recovery имеет встроенный механизм для обнаружения и использования уязвимости в защите Мастер Ключей DPAPI. Так, для расшифровки _любых_ записей Windows Vault доменного пользователя, пароль владельце больше не обязателен.

WPR v11.7 поддерживает функцию автоматического доверенного входа в систему Windows 10. Если программа обнаруживает, что для пользователя установлен доверенный автоматический вход, для расшифровки данных пароль на вход не потребуется.

WPR v15 поддерживает дополнительные методы расшифровки при помощи биометрии и PIN.

Выбор схемы Vault



Every Vault consists of credentials (encrypted user data). Each credential belongs to a certain schema (credential descriptor). You should select one of available schemas to process further credentials enumeration.

Vault information

Vault location: E:\Windows\System32\config\systemprofile\AppData\Local\Microsoft\Vault\4BF4C442-

Selected schema: WinBio Credential Manager Credential Schema

Selected credential:

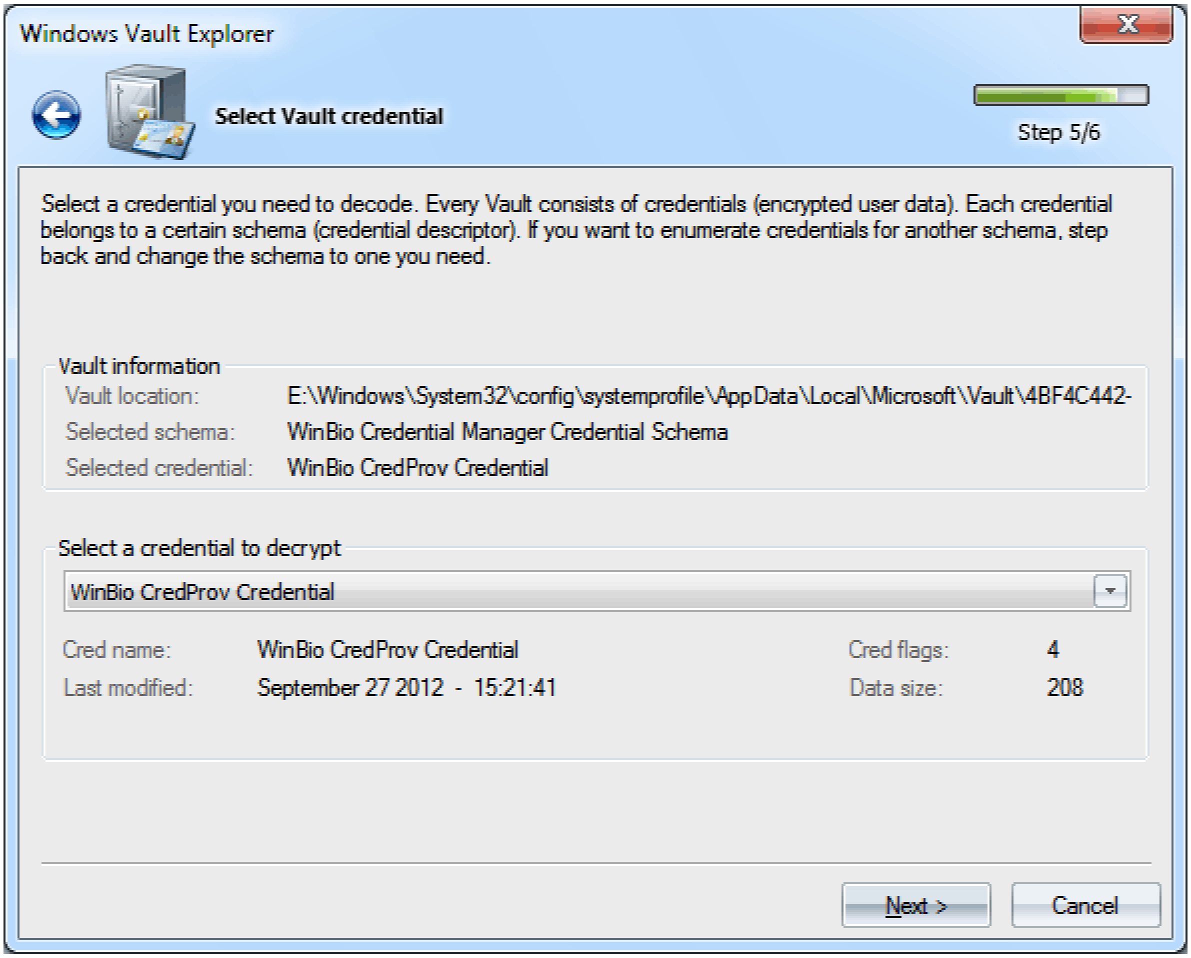
Select one of the schemas

WinBio Credential Manager Credential Schema

Schema name:	WinBio Credential Manager Credential Schema	Schema flags:	0
Schema version:	1	Attributes:	4
Schema GUID:	fec87291-14f6-40b6-bd98-7ff245986b26	Credentials:	1

На четвертом шаге, если предыдущие прошли успешно, программа предложит выбрать из выпадающего списка одну из схем, принадлежащих нашему Vault. Чуть ниже списка показаны общие характеристики выбранной схемы: ее имя, версия, GUID, флаги, количество атрибутов и записей.

Выбор записи Vault



Select a credential you need to decode. Every Vault consists of credentials (encrypted user data). Each credential belongs to a certain schema (credential descriptor). If you want to enumerate credentials for another schema, step back and change the schema to one you need.

Vault information

Vault location: E:\Windows\System32\config\systemprofile\AppData\Local\Microsoft\Vault\4BF4C442-

Selected schema: WinBio Credential Manager Credential Schema

Selected credential: WinBio CredProv Credential

Select a credential to decrypt

WinBio CredProv Credential

Cred name: WinBio CredProv Credential

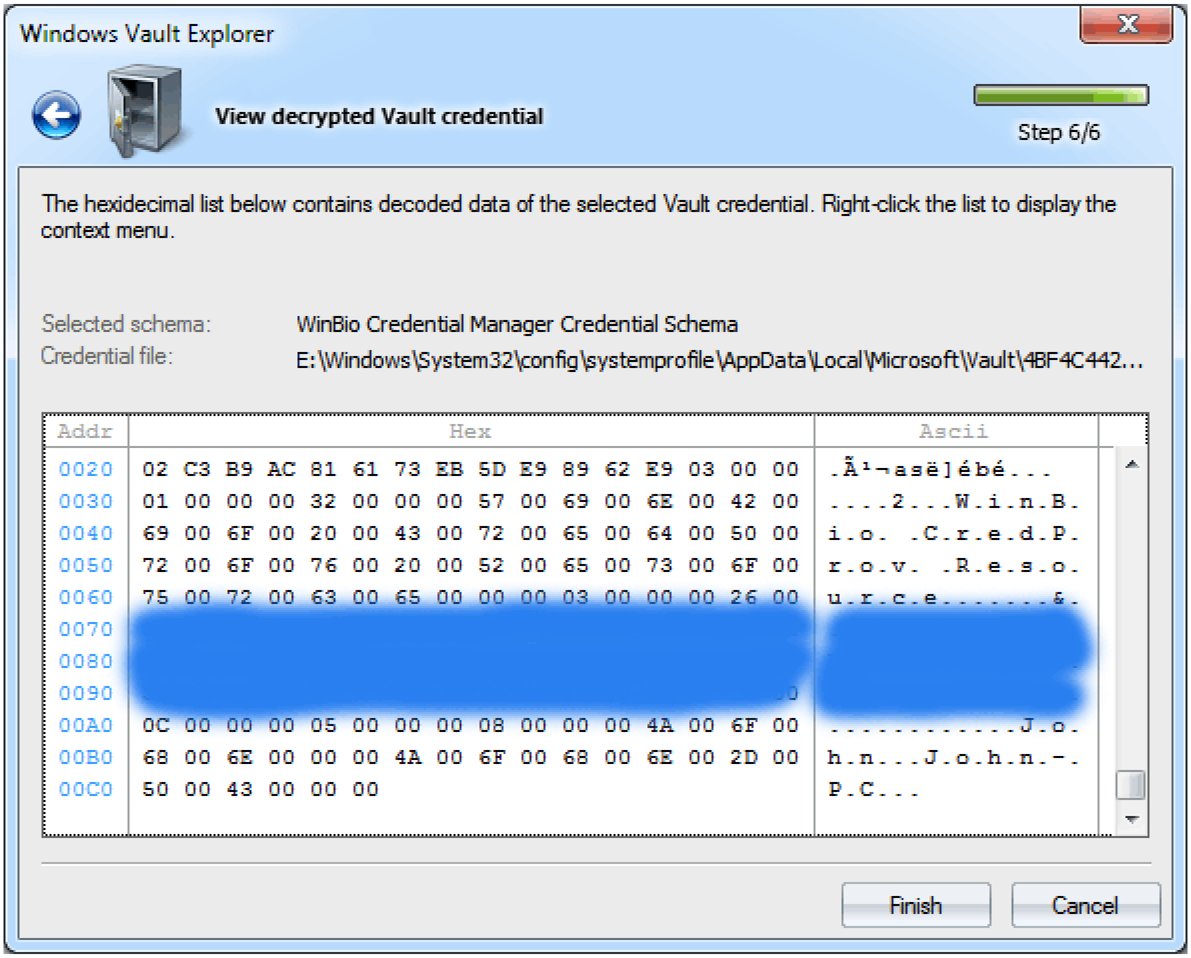
Cred flags: 4

Last modified: September 27 2012 - 15:21:41

Data size: 208

Аналогичным способом выбираем одну из интересующих нас записей, принадлежащих выбранной на предыдущем шаге схеме.

Расшифровка записи Vault



The hexidecimal list below contains decoded data of the selected Vault credential. Right-click the list to display the context menu.

Selected schema: WinBio Credential Manager Credential Schema
Credential file: E:\Windows\System32\config\systemprofile\AppData\Local\Microsoft\Vault\4BF4C442...

```
Addr  Hex                                                Ascii
0020  02 C3 B9 AC 81 61 73 EB 5D E9 89 62 E9 03 00 00   .Ã¹¬asë]ébé...
0030  01 00 00 00 32 00 00 00 57 00 69 00 6E 00 42 00   ....2...W.i.n.B.
0040  69 00 6F 00 20 00 43 00 72 00 65 00 64 00 50 00   i.o. .C.r.e.d.P.
0050  72 00 6F 00 76 00 20 00 52 00 65 00 73 00 6F 00   r.o.v. .R.e.s.o.
0060  75 00 72 00 63 00 65 00 00 00 03 00 00 00 26 00   u.r.c.e.......&.
0070  [redacted]
0080
0090
00A0  0C 00 00 00 05 00 00 00 08 00 00 00 4A 00 6F 00   ............J.o.
00B0  68 00 6E 00 00 00 4A 00 6F 00 68 00 6E 00 2D 00   h.n...J.o.h.n.-.
00C0  50 00 43 00 00 00                                 P.C...
```

Ну и, наконец, финальная стадия, где можно просмотреть расшифрованную запись, скопировать ее в буфер обмена или сохранить в файл для дальнейшего анализа. На рисунке показан расшифрованный пароль (он затерт) учетной записи администратора, настроенной на вход при помощи отпечатка пальцев.

2.7.4.7 Обозреватель Windows Hello

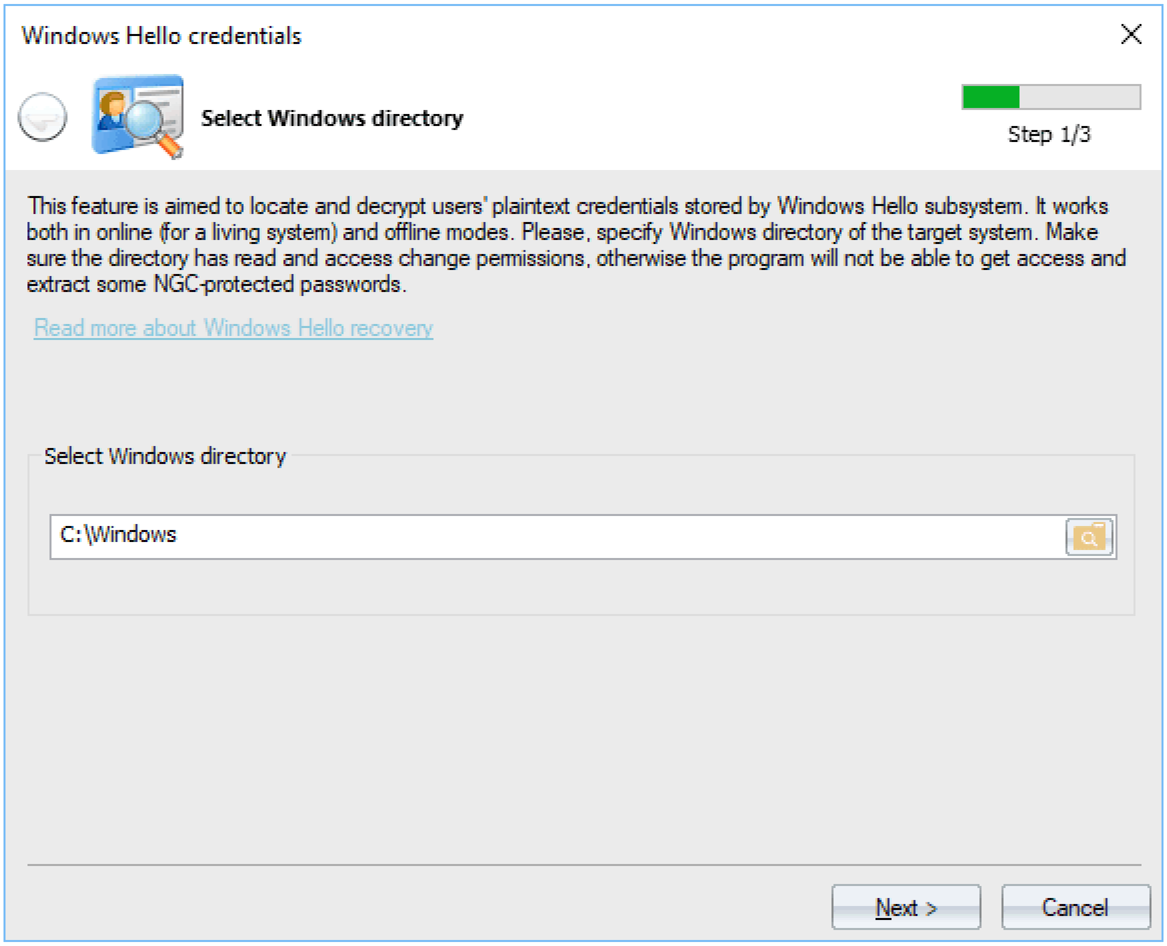
Windows Hello - это сложная система биометрической аутентификациий Windows 10, придуманная в качестве альтернативы паролям. Windows Hello предназначена для удобного и безопасного входа пользователя в систему при помощи распознавания лица, радужной оболочки глаза, отпечатков пальцев или голоса. Предполагается, что такое использование Windows Hello обеспечивает отдельный уровень защиты, так как является уникальным для устройства, на котором настраивается.

Windows Password Recovery предлагает небольшой набор утилит для анализа системы безопасности Windows Hello. Набор включает в себя три утилиты для извлечения паролей пользователей, хранимых в Windows Hello, расшифровки цифровых идентификаторов (например, отпечатков пальцев) и восстановления PIN-кода.

2.7.4.7.1 Пароли Windows Hello

Утилита для поиска и расшифровки паролей пользователей, хранимых в Windows Hello, поддерживает как онлайн, так и оффлайн режимы, обеспечивая работу с данными работающей или любой другой внешней операционной системы. Несмотря на то, что криптография нового поколения (NGC) получилась у Microsoft довольно сложной системой, Passcape Software первой в мире, также, как в случае с DPAPI, сделала практически полный аналог NGC, но с возможностью работы в оффлайн режиме. Это вывело работу с данными Windows Hello на новый, доступный даже неподготовленному пользователю уровень, оставляя все многочисленные и рутинные операции на откуп программе.

1 Задаем каталог Windows



Windows Hello credentials

Select Windows directory

Step 1/3

This feature is aimed to locate and decrypt users' plaintext credentials stored by Windows Hello subsystem. It works both in online (for a living system) and offline modes. Please, specify Windows directory of the target system. Make sure the directory has read and access change permissions, otherwise the program will not be able to get access and extract some NGC-protected passwords.

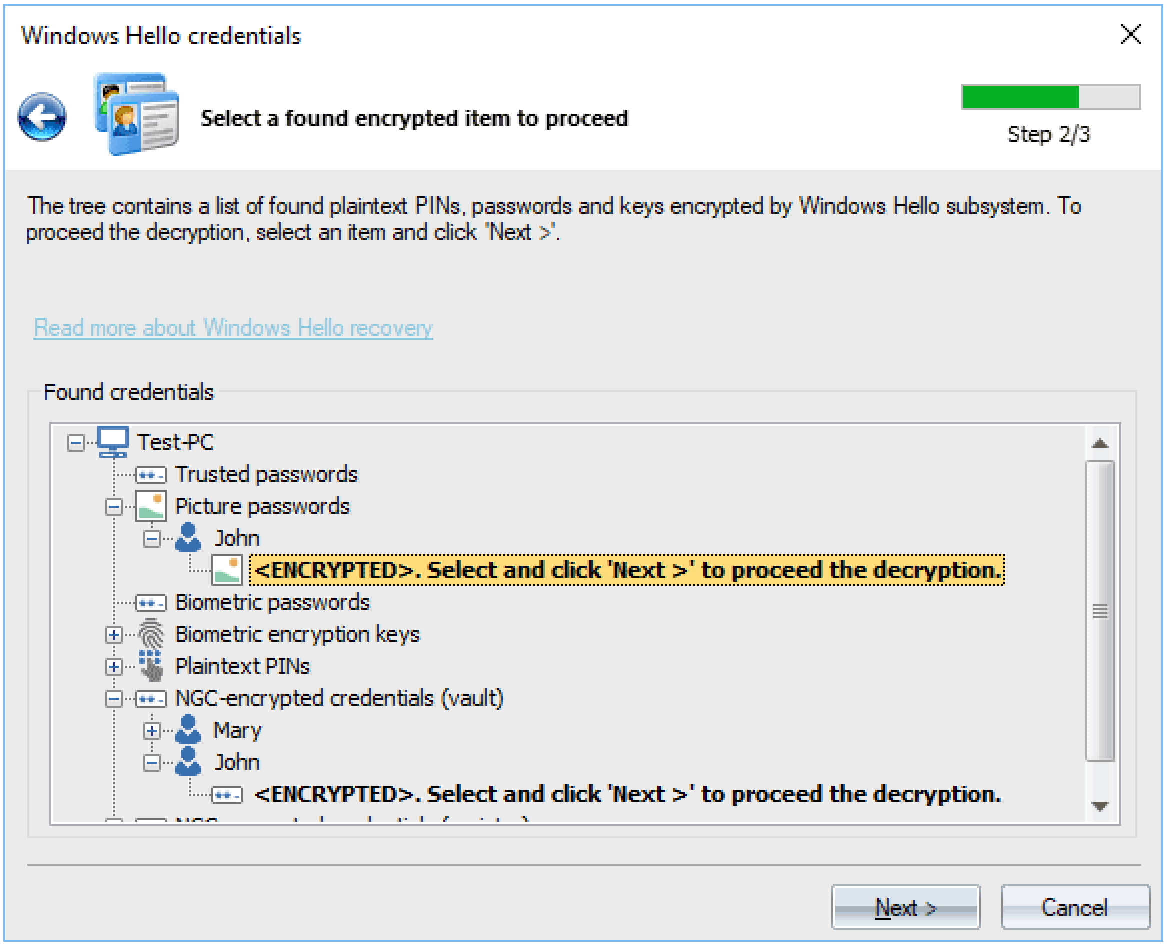
Read more about Windows Hello recovery

Select Windows directory

C:\Windows

Режим работы определяется программой автоматически после того, как будет задан каталог Windows. Каталог Windows содержит папки с ключами шифрования доступ к которым запрещен всем, включая Администраторов. Для извлечения и расшифровки некоторых ключей шифрования необходимо, чтобы каталог был доступен для изменения прав доступа или записи. В противном случае, программа будет не в состоянии расшифровать пароли, защищенные при помощи NGC.

2 Выбор найденных данных



Windows Hello credentials

Select a found encrypted item to proceed

Step 2/3

The tree contains a list of found plaintext PINs, passwords and keys encrypted by Windows Hello subsystem. To proceed the decryption, select an item and click 'Next >'.

Read more about Windows Hello recovery

Found credentials

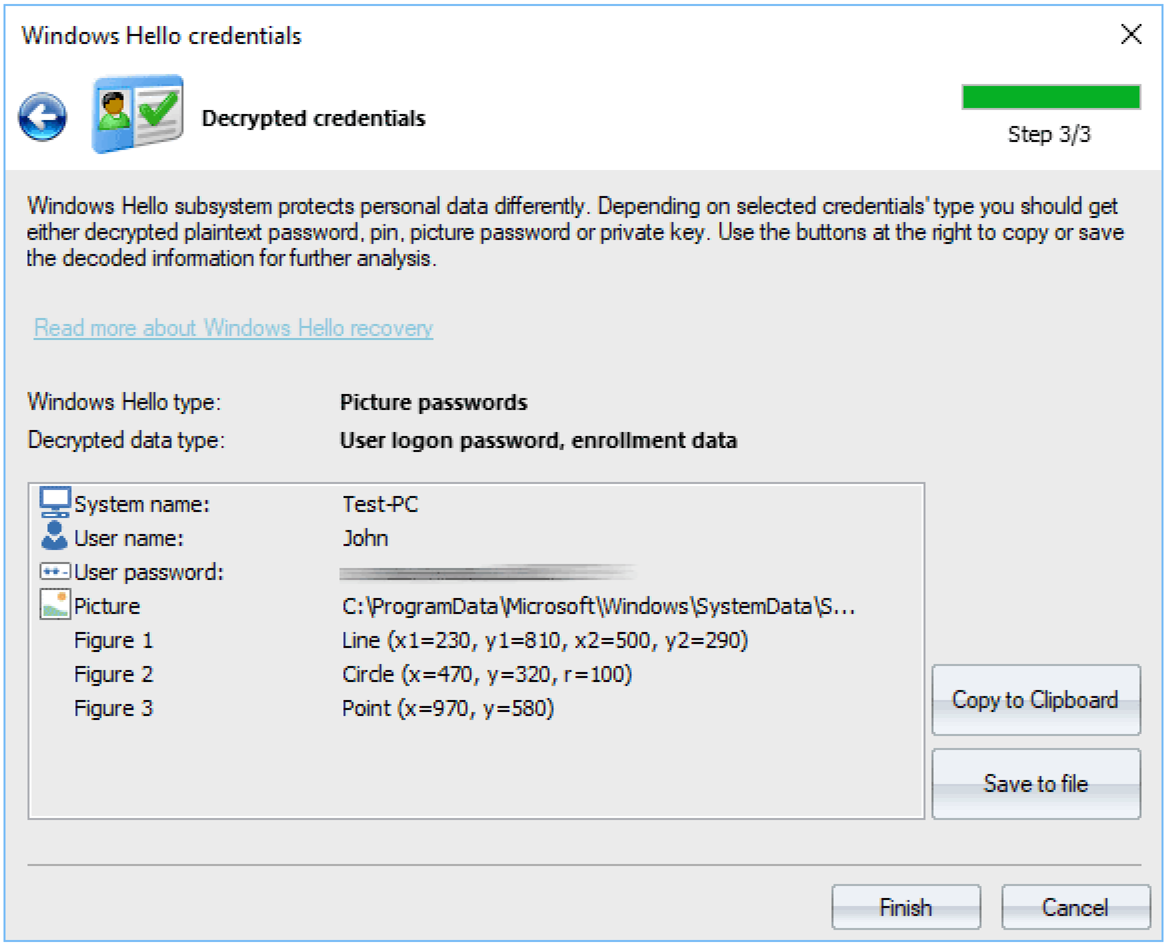
```
Test-PC
  Trusted passwords
  Picture passwords
    John
      <ENCRYPTED>. Select and click 'Next >' to proceed the decryption.
  Biometric passwords
  Biometric encryption keys
  Plaintext PINs
  NGC-encrypted credentials (vault)
    Mary
    John
      <ENCRYPTED>. Select and click 'Next >' to proceed the decryption.
```

На втором шаге мастера программа выводит список всех найденных (и пока зашифрованных) паролей, PIN-кодов и ключей шифрования. Систему Windows Hello разрабатывало определенно несколько команд разработчиков, поскольку персональные данные, ключи и сами алгоритмы шифрования разбросаны по все операционной системе. Программа поддерживает следующие типы извлекаемых данных:

- Графические пароли
- Текстовые пароли пользователей, защищенные при помощи графического пароля
- Биометрические пароли
- Текстовые пароли пользователей, защищенные при помощи биометрического пароля
- Биометрические ключи шифрования
- Текстовые PIN-коды
- История ранее введенных PIN (если включена настройка сохранения)
- Текстовые пароли пользователей, хранимые в Windows Vault и защищенные при помощи NGC
- Текстовые пароли пользователей, хранимые в реестре и защищенные при помощи NGC

Вся найденная информация представлена в виде дерева с привязкой к пользователю. Для финальной расшифровки, дважды щелкните по элементу, выделенному жирным шрифтом.

3 Расшифровка паролей



Windows Hello credentials

Decrypted credentials

Step 3/3

Windows Hello subsystem protects personal data differently. Depending on selected credentials' type you should get either decrypted plaintext password, pin, picture password or private key. Use the buttons at the right to copy or save the decoded information for further analysis.

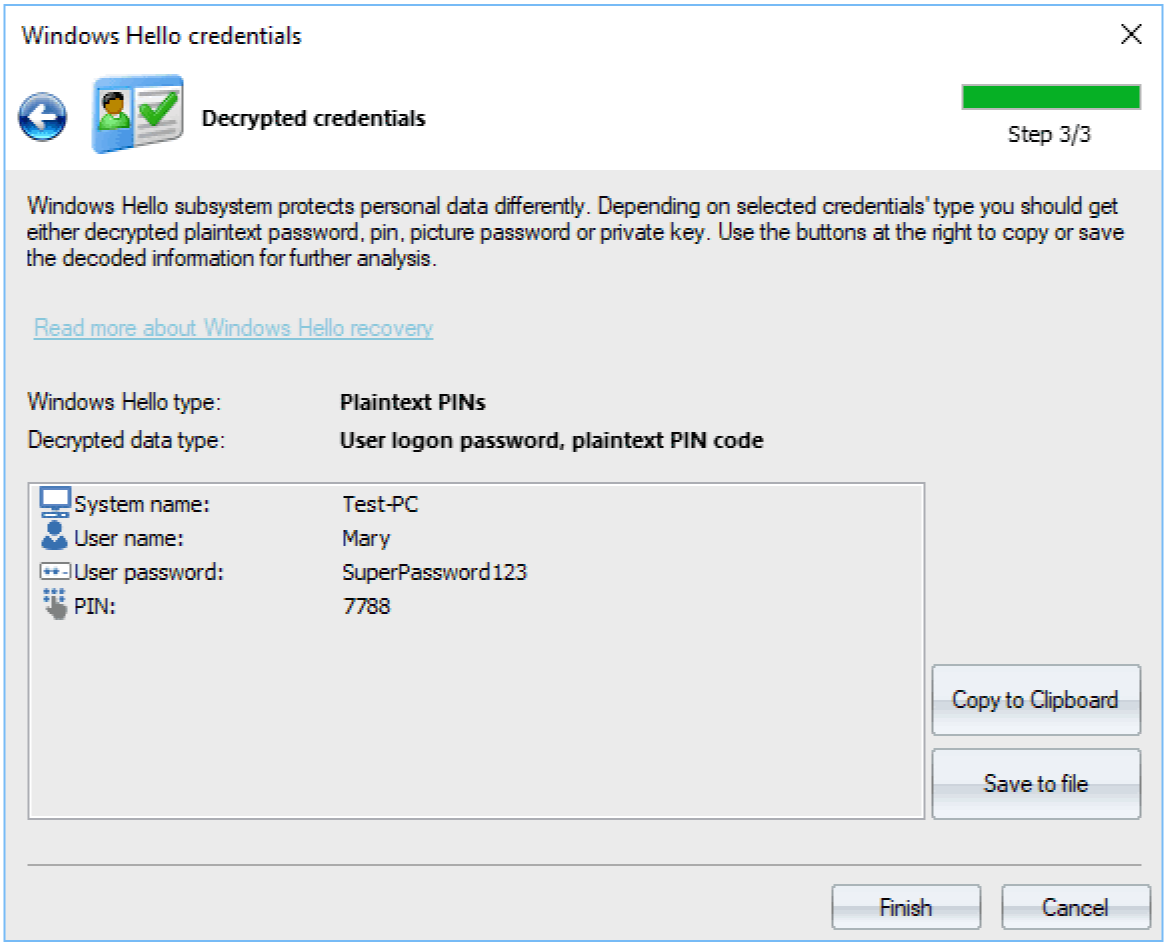
Read more about Windows Hello recovery

Windows Hello type: **Picture passwords**

Decrypted data type: **User logon password, enrollment data**

System name:	Test-PC
User name:	John
User password:	[redacted]
Picture	C:\ProgramData\Microsoft\Windows\SystemData\S...
Figure 1	Line (x1=230, y1=810, x2=500, y2=290)
Figure 2	Circle (x=470, y=320, r=100)
Figure 3	Point (x=970, y=580)

Расшифрованный пароль на вход и графический пароль.



Windows Hello credentials

Decrypted credentials

Step 3/3

Windows Hello subsystem protects personal data differently. Depending on selected credentials' type you should get either decrypted plaintext password, pin, picture password or private key. Use the buttons at the right to copy or save the decoded information for further analysis.

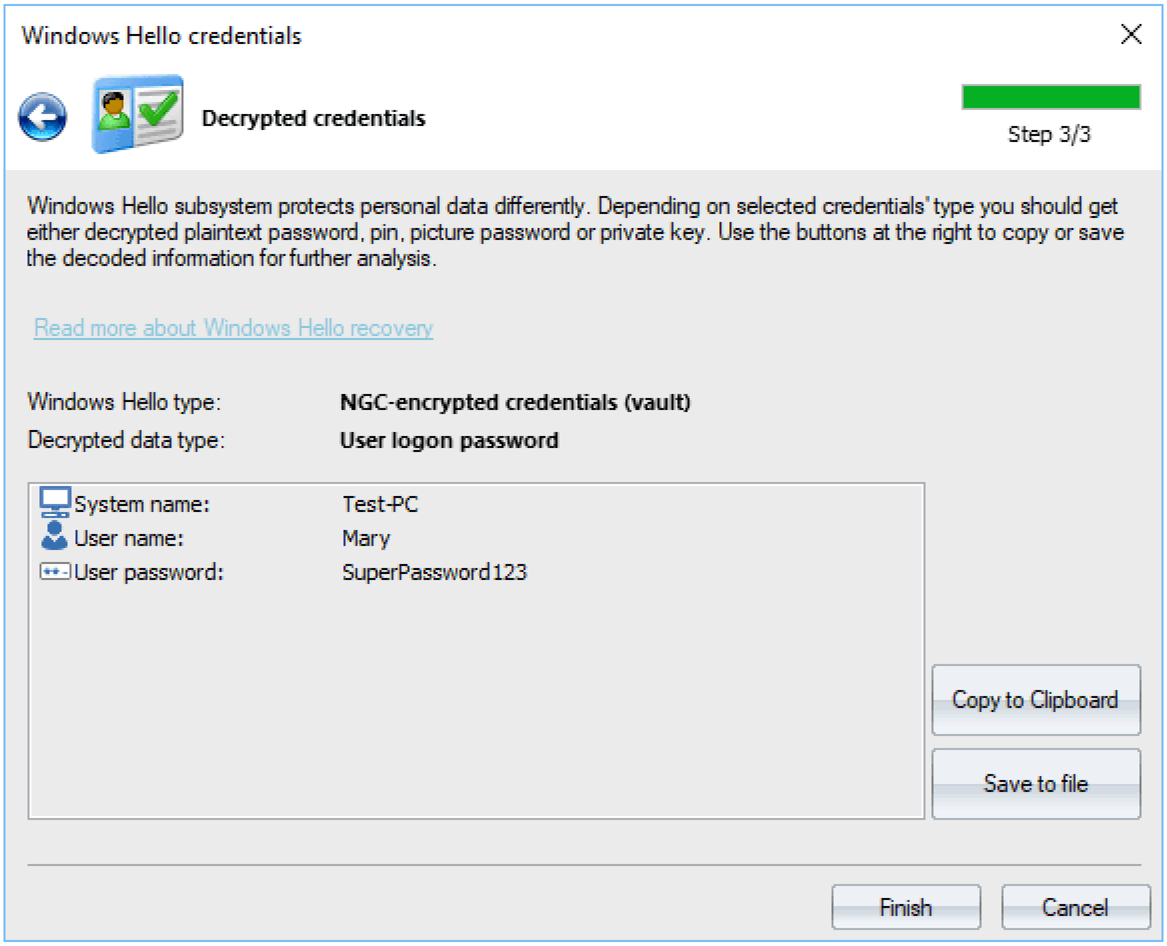
Read more about Windows Hello recovery

Windows Hello type: **Plaintext PINs**

Decrypted data type: **User logon password, plaintext PIN code**

System name:	Test-PC
User name:	Mary
User password:	SuperPassword123
PIN:	7788

Расшифрованный пароль на вход и PIN-код.



Windows Hello credentials

Decrypted credentials

Step 3/3

Windows Hello subsystem protects personal data differently. Depending on selected credentials' type you should get either decrypted plaintext password, pin, picture password or private key. Use the buttons at the right to copy or save the decoded information for further analysis.

Read more about Windows Hello recovery

Windows Hello type: **NGC-encrypted credentials (vault)**

Decrypted data type: **User logon password**

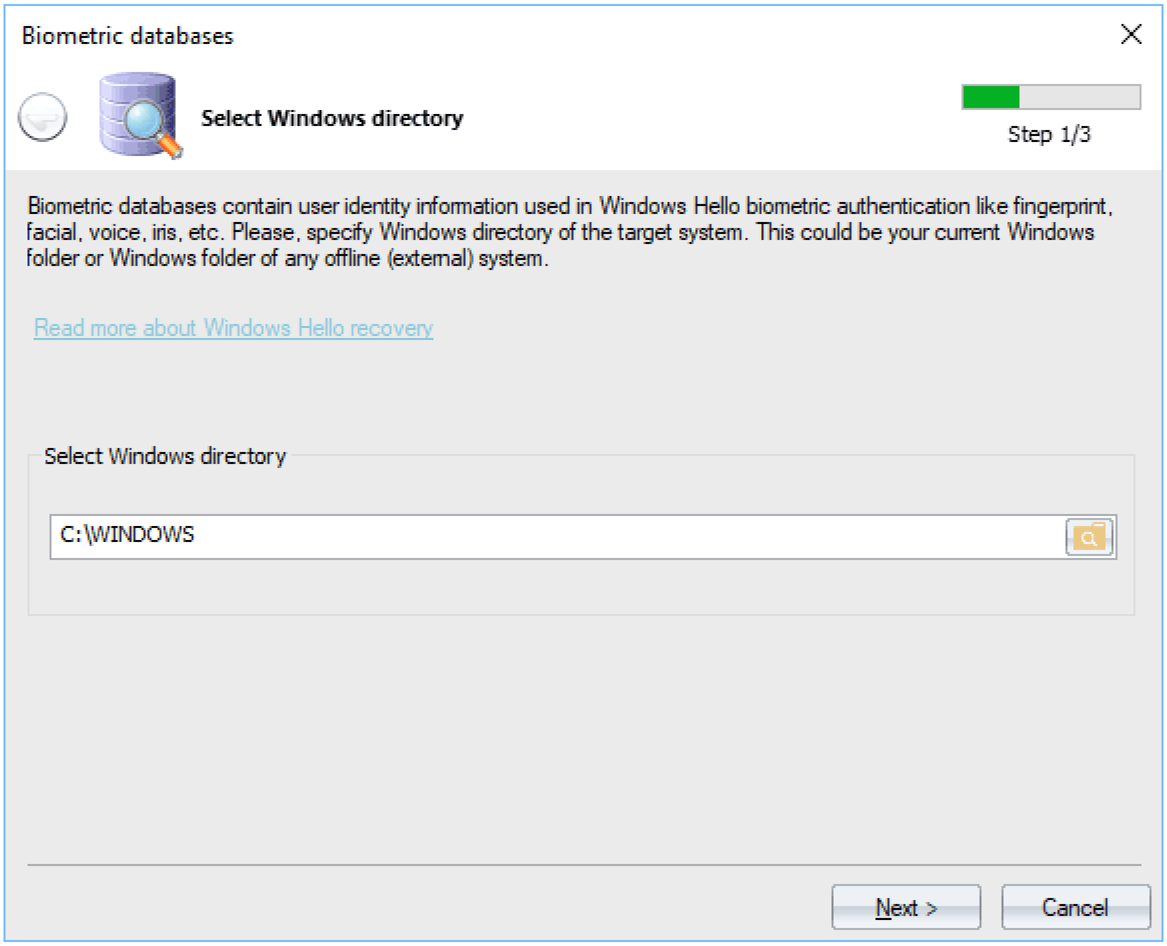
System name: Test-PC
User name: Mary
User password: SuperPassword123

Расшифрованный пароль пользователя.

Имейте в виду, текстовые пароли пользователей, защищенные при помощи NGC, могут быть расшифрованы как биометрическими ключами, так и при помощи PIN-кода. Программа автоматически попытается найти и использовать биометрические ключи шифрования. Если они не найдены, например, биометрический вход не настроен в системе, то в этом случае необходимо предоставить PIN-код.

2.7.4.7.2 Биометрические базы данных

Биометрические базы данных содержат цифровые данные пользователя, используемые в биометрической идентификации Windows Hello: отпечатки пальцев, идентификаторы по лицу, голосу, радужной оболочки и т. д.



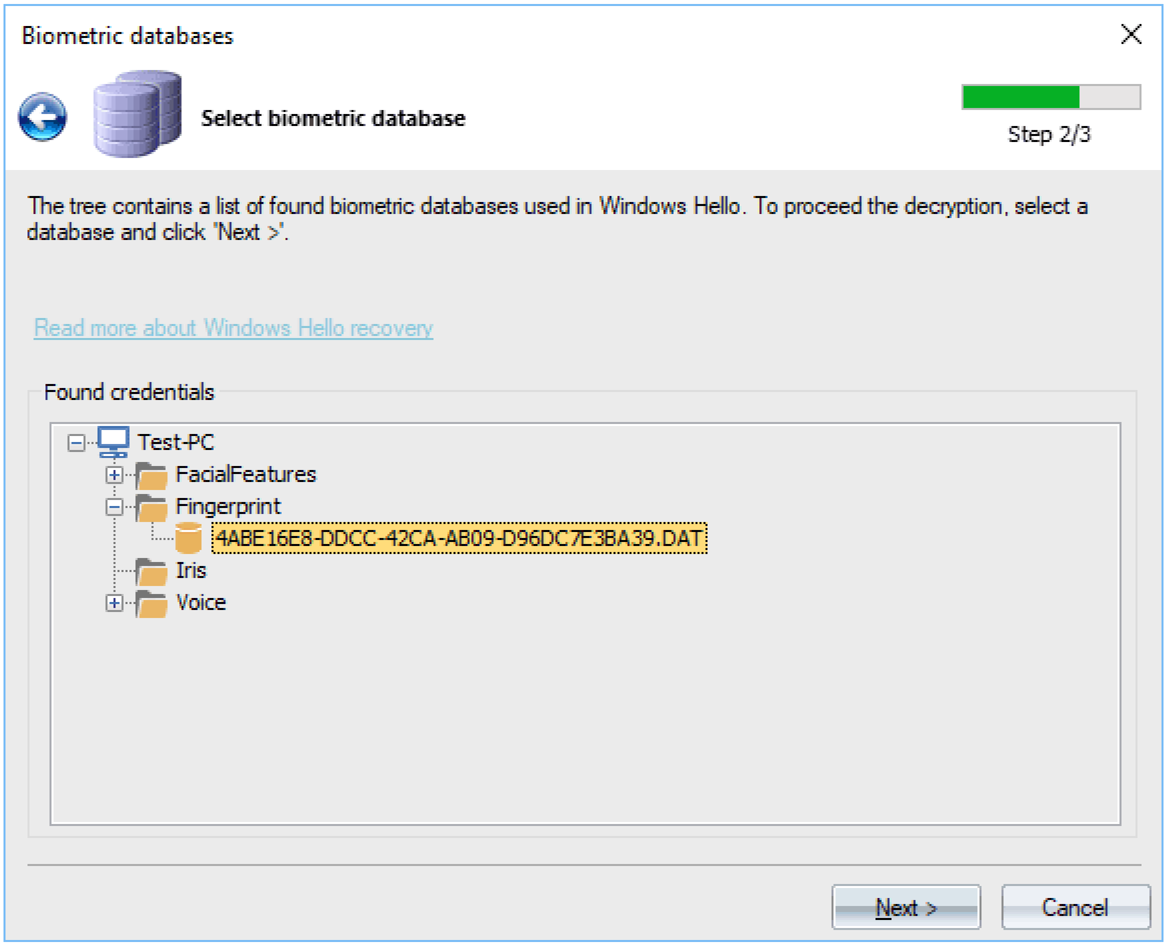
Biometric databases contain user identity information used in Windows Hello biometric authentication like fingerprint, facial, voice, iris, etc. Please, specify Windows directory of the target system. This could be your current Windows folder or Windows folder of any offline (external) system.

Read more about Windows Hello recovery

Select Windows directory

C:\WINDOWS

Для поиска и расшифровки биометрических баз данных, укажите каталог Windows целевой системы. Это может быть папка Windows текущей или любой другой автономной (внешней) операционной системы Windows.



Biometric databases

Select biometric database

Step 2/3

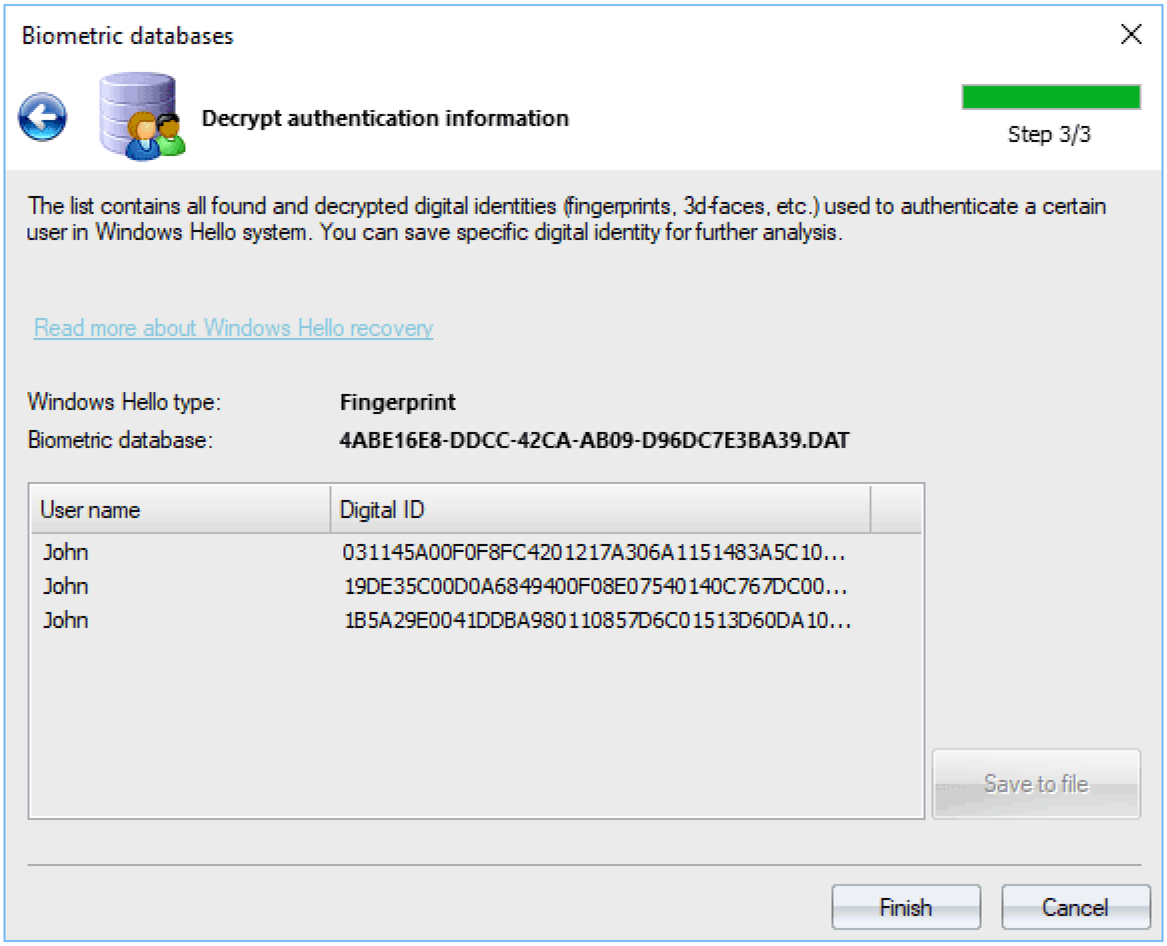
The tree contains a list of found biometric databases used in Windows Hello. To proceed the decryption, select a database and click 'Next >'.

Read more about Windows Hello recovery

Found credentials

- Test-PC
  - FacialFeatures
  - Fingerprint
    - 4ABE16E8-DDCC-42CA-AB09-D96DC7E3BA39.DAT
  - Iris
  - Voice

Для финальной расшифровки, дважды щелкните по найденной базе мышкой.



The list contains all found and decrypted digital identities (fingerprints, 3d-faces, etc.) used to authenticate a certain user in Windows Hello system. You can save specific digital identity for further analysis.

Read more about Windows Hello recovery

Windows Hello type: Fingerprint
Biometric database: 4ABE16E8-DDCC-42CA-AB09-D96DC7E3BA39.DAT

User name	Digital ID
John	031145A00F0F8FC4201217A306A1151483A5C10...
John	19DE35C00D0A6849400F08E07540140C767DC00...
John	1B5A29E0041DDBA980110857D6C01513D60DA10...

Биометрическая база данных содержит найденные и расшифрованные цифровые идентификаторы (отпечатки пальцев, трехмерные лица и т.д.), используемые при идентификации пользователей в системе Windows Hello. Например, если пользователь установил три отпечатка пальцев в Windows Hello, то они будут находиться в соответствующей базе напротив имени пользователя, как показано на картинке.

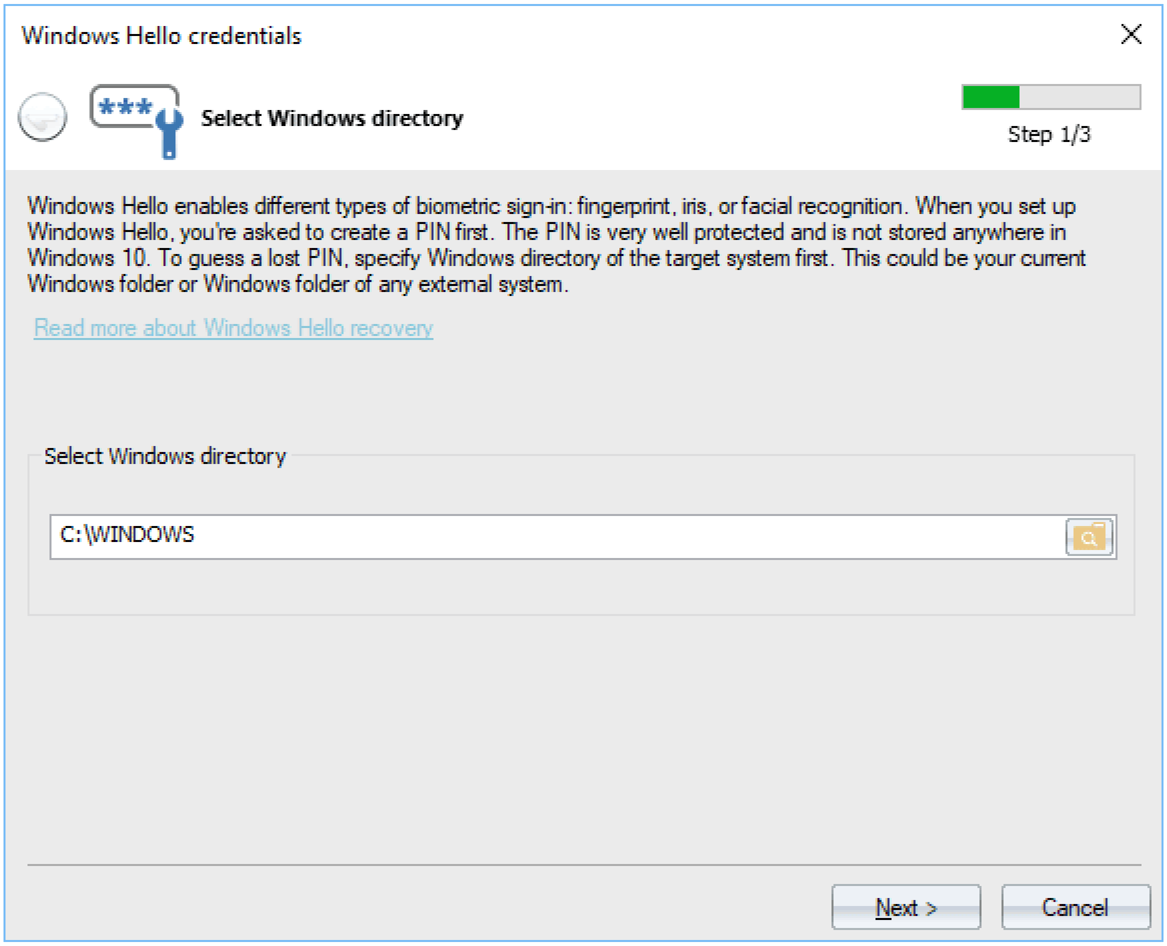
Найденные цифровые идентификаторы можно сохранить в файл для их дальнейшего анализа.

Вопреки заверениям Microsoft, цифровые идентификаторы можно довольно легко перенести или скопировать с одного компьютера на другой. Например, можно создать свой отпечаток пальца на одном компьютере, скопировать его на другой компьютер в чужую учетную запись и затем можно будут зайти в эту учетную запись со своим отпечатком пальца. Из-за серьезного характера данной уязвимости, функция копирования цифровых идентификаторов была отключена в программе.

2.7.4.7.3 Восстановление PIN

Windows Hello позволяет работать с различными типами биометрической аутентификации: по отпечаткам пальцев, радужной оболочки, лицу или голосу. При настройке Windows Hello в первую очередь требуется создать PIN-код. PIN можно использовать как запасной вариант, когда датчик недоступен или не работает должным образом. PIN-код очень хорошо защищен и, начиная с Windows 10, не хранится нигде в системе. Поэтому особенно остро стоит вопрос восстановления забытого PIN-кода.

Чтобы обеспечить синхронизацию данных нескольких устройств (только для учетных записей Microsoft), Microsoft сохраняет копию PIN-кода на своих серверах.



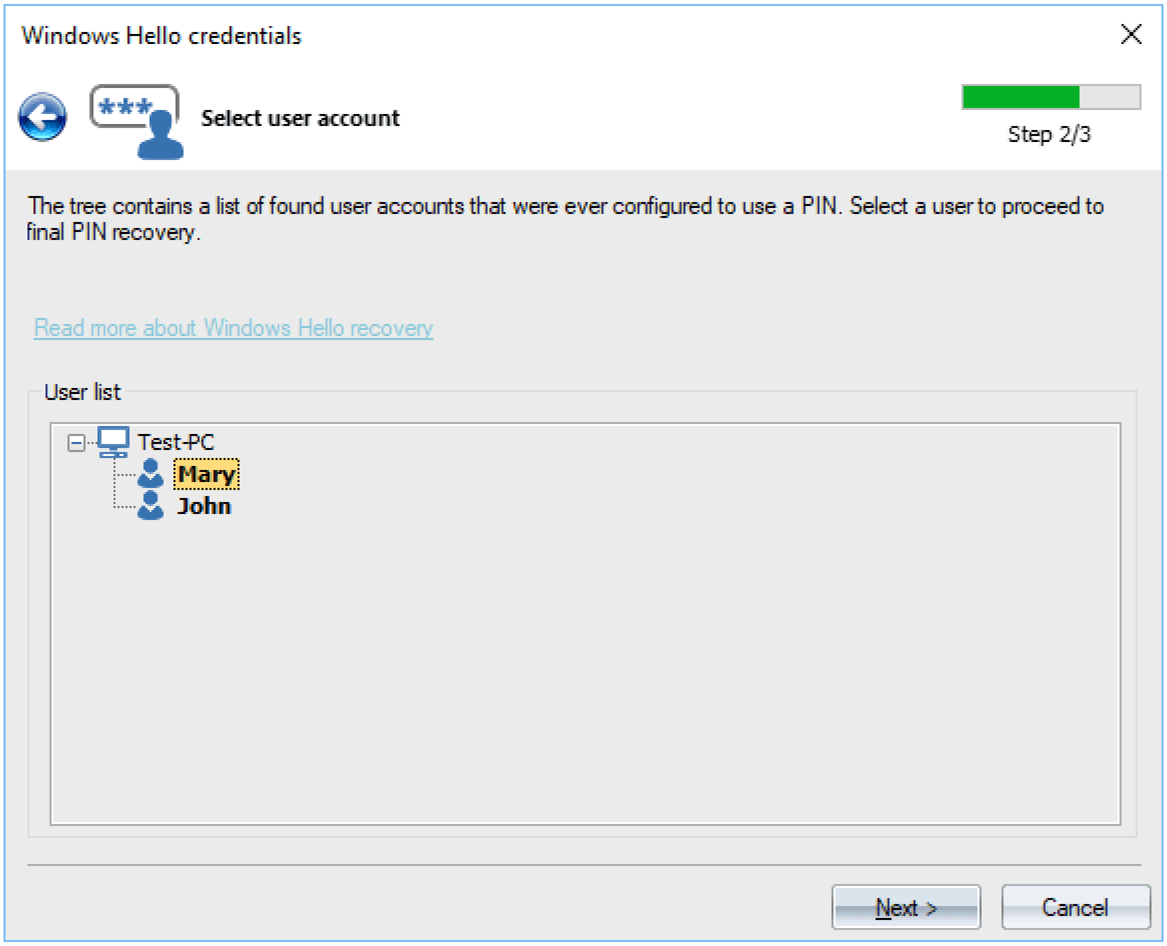
Windows Hello enables different types of biometric sign-in: fingerprint, iris, or facial recognition. When you set up Windows Hello, you're asked to create a PIN first. The PIN is very well protected and is not stored anywhere in Windows 10. To guess a lost PIN, specify Windows directory of the target system first. This could be your current Windows folder or Windows folder of any external system.

Read more about Windows Hello recovery

Select Windows directory

C:\WINDOWS

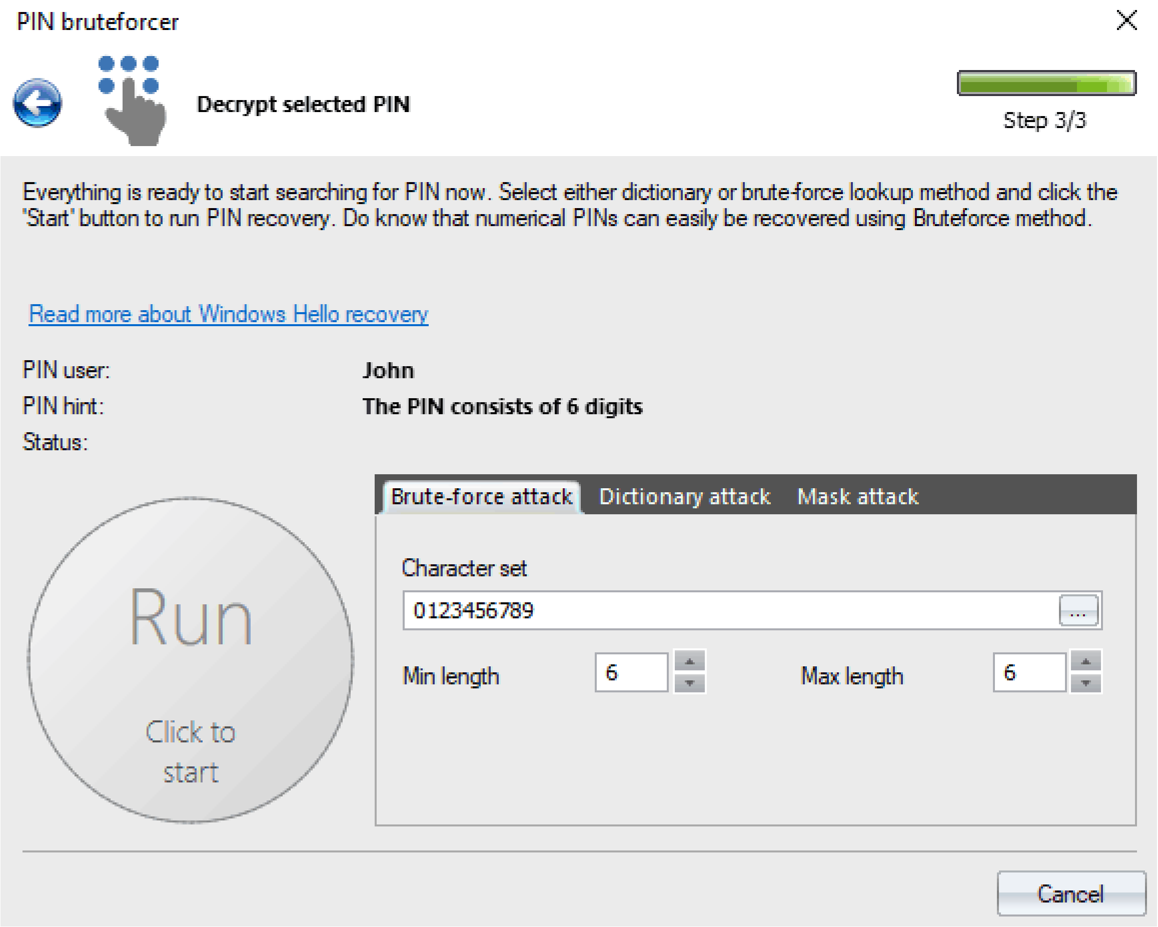
Чтобы начать процесс восстановления, укажите каталог Windows целевой системы. Это может быть папка Windows текущей или любой внешней ОС. Каталог Windows должен быть доступен для изменения прав доступа или записи.


Windows Hello credentials
Select user account
Step 2/3

The tree contains a list of found user accounts that were ever configured to use a PIN. Select a user to proceed to final PIN recovery.

Read more about Windows Hello recovery
User list
Test-PC
Mary
John
Next >
Cancel

На втором шаге мастера восстановления программы выводит список пользователей, которые были настроены на вход в систему при помощи PIN. Выберите необходимую учетную запись для перехода непосредственно к диалогу восстановления.



Everything is ready to start searching for PIN now. Select either dictionary or brute-force lookup method and click the 'Start' button to run PIN recovery. Do know that numerical PINs can easily be recovered using Bruteforce method.

Read more about Windows Hello recovery

PIN user: John
PIN hint: The PIN consists of 6 digits
Status:

Character set: 0123456789
Min length: 6
Max length: 6

Программа поддерживает три метода восстановления PIN: методом прямого перебора, по словарю и по маске. Настройка каждого метода довольно тривиальна. В случае прямого перебора необходимо задать перебираемый набор символов, минимальную и максимальную длину PIN. Для атаки по словарю укажите начальный словарь и уровень мутаций слов в словаре. Атака по маске подразумевает установку маски словаря.

Запуск и остановка выбранной атаки осуществляется при помощи круглой кнопки слева от настроек.

В некоторых случаях программа умеет определять тип используемых символов в PIN-коде. Подсказка появляется в соответствующем поле.

Перебор PIN кодов, зашифрованных при помощи TPM, не поддерживается!

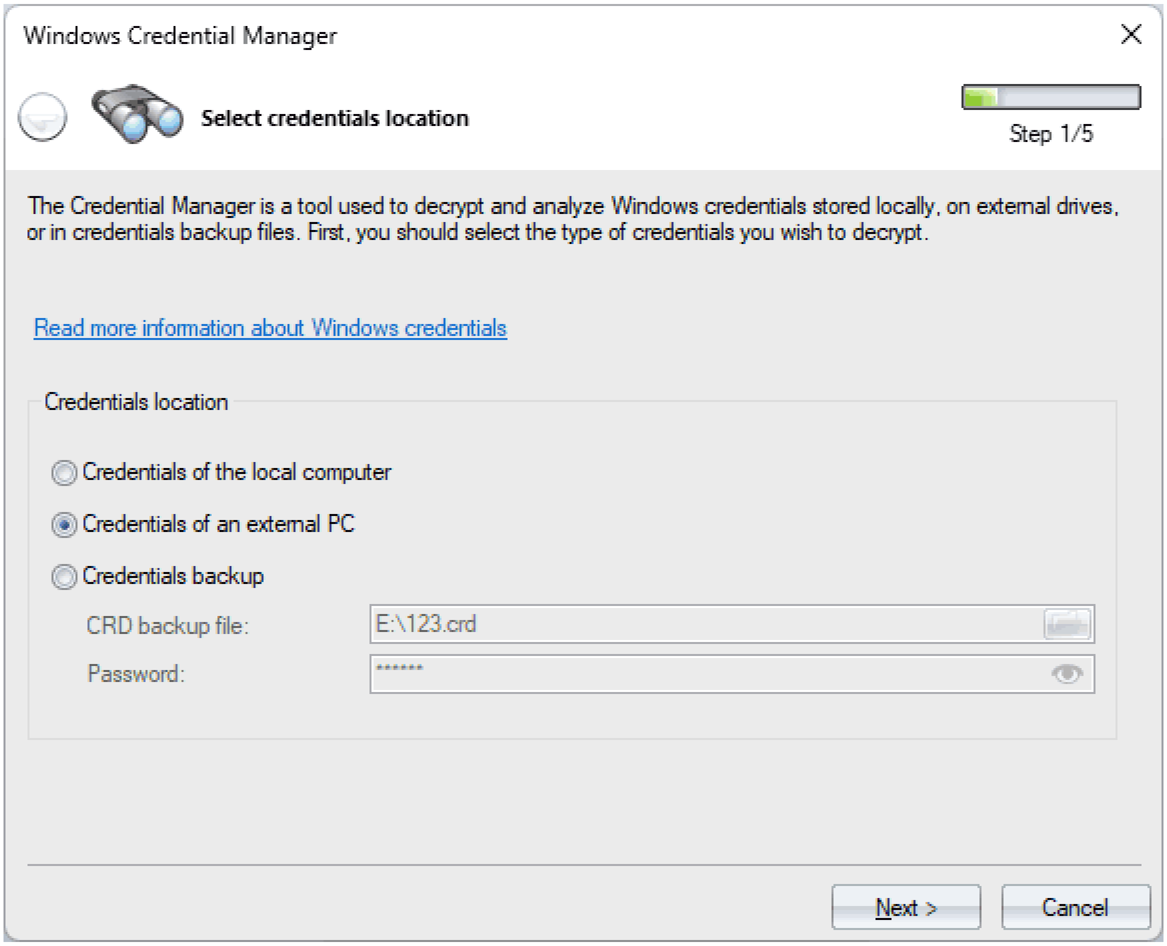
2.7.4.8 Обозреватель паролей Windows Credentials

Windows Credential Manager представляет собой встроенный инструмент, доступный в операционных системах Windows 7 и более поздних версиях. Его основная задача - обеспечить безопасное хранение личных данных и учетных данных пользователей. Credential Manager действует как центральное хранилище, которое позволяет пользователям с легкостью и удобством управлять различными типами учетных данных, такими как сетевые учетные данные, пароли, сертификаты и общие учетные данные. Интерфейс Credential Manager обеспечивает возможность для авторизованных пользователей и приложений манипулировать и получать доступ к хранимым данным. В последних версиях Windows Credential Manager поддерживает синхронизацию учетных данных между устройствами с помощью учетной записи Microsoft, что облегчает доступ к ресурсам на разных системах.

При использовании Credential Manager API (**CredUI** или **CredProv**) сторонние приложения могут извлекать или удалять ранее сохраненные учетные данные, создавать новые или использовать уже сохраненные данные для аутентификации без необходимости многократного запроса у пользователя. Важно отметить, что эти API работают только для аккаунта пользователя, который вошел в систему на текущей системе.

Примечательной особенностью программы является возможность расшифровки учетных данных Windows Credential Manager, путем прямого доступа к данным, без использования API Credential Manager. Это означает, что вы можете получить доступ к расшифрованным паролям любой учетной записи, включая системную, на любом компьютере.

1 Выбор источника данных



The Credential Manager is a tool used to decrypt and analyze Windows credentials stored locally, on external drives, or in credentials backup files. First, you should select the type of credentials you wish to decrypt.

Read more information about Windows credentials

Credentials location

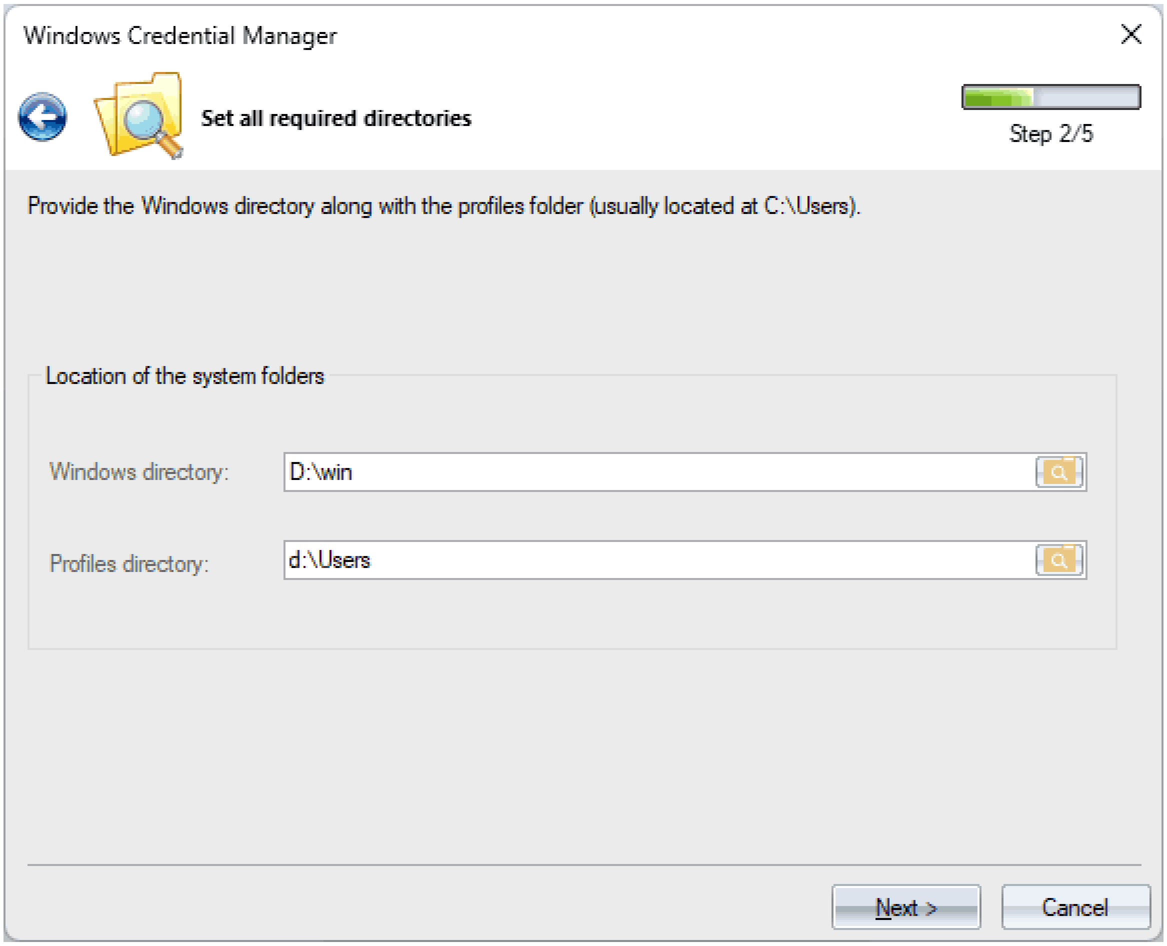
○ Credentials of the local computer
● Credentials of an external PC
○ Credentials backup

CRD backup file: E:\123.crd
Password: ******

Первое окно Мастера расшифровки предлагает выбрать источник данных, которые вы хотите расшифровать. Вам доступны три варианта:

1. Локальный ПК: Выберите этот вариант, чтобы расшифровать пароли Windows Credentials Manager, хранящиеся на вашем текущем компьютере.
2. Внешний ПК: Выберите этот вариант, если вы хотите расшифровать пароли, хранящиеся на внешнем жестком диске.
3. Файл резервной копии: Выберите этот вариант, если у вас есть файл резервной копии паролей Windows Credentials Manager. Файлы резервной копии паролей обычно имеют расширение *.crd и содержат зашифрованные копии всех персональных данных, хранящихся в одном месте. Обычно файлы резервной копии используются для безопасного хранения и передачи учетных данных между системами или для резервного копирования. Если вы знаете пароль, которым был защищен этот *.crd файл, необходимо ввести его для дальнейшей разблокировки и просмотра сохраненных данных .

2 Выбор каталога Windows и папки профилей пользователей



Windows Credential Manager

Set all required directories

Step 2/5

Provide the Windows directory along with the profiles folder (usually located at C:\Users).

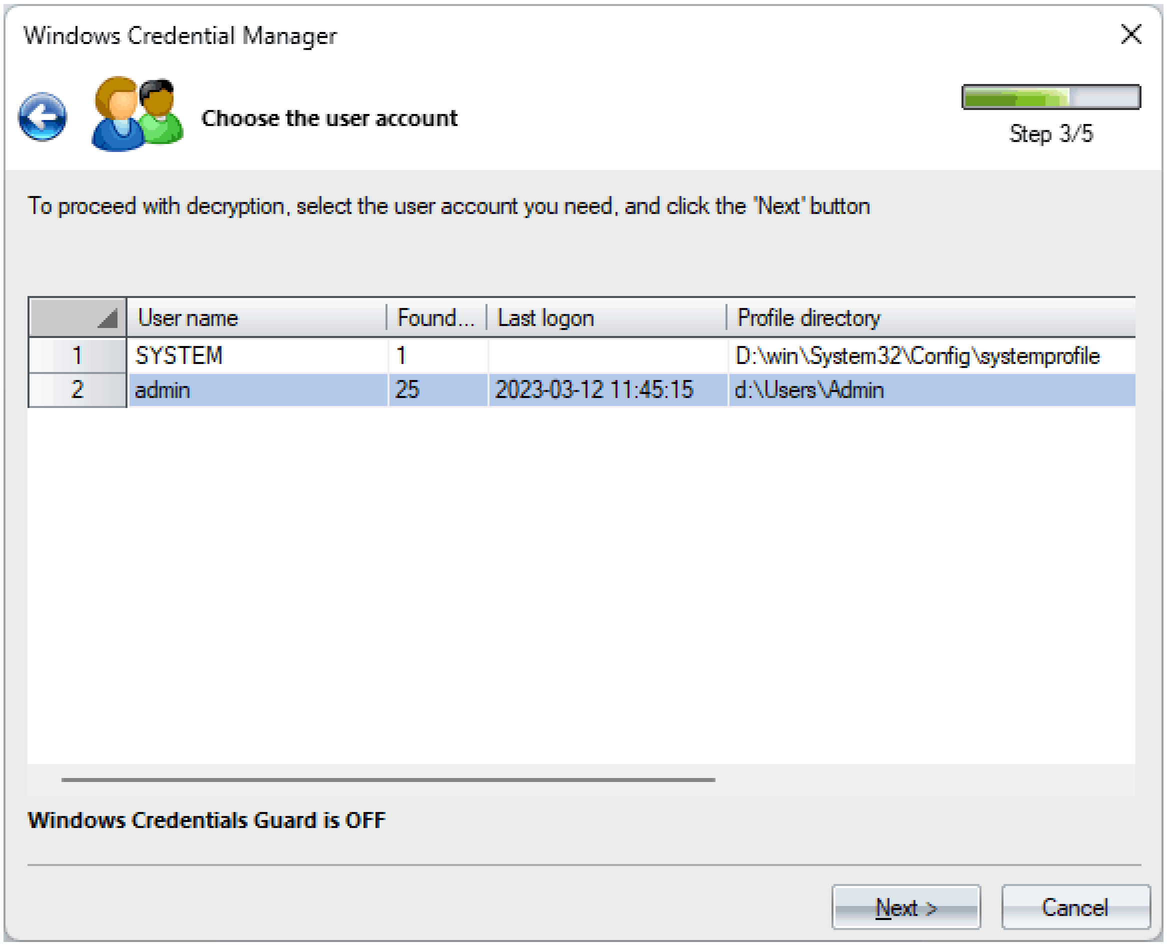
Location of the system folders

Windows directory: D:\win

Profiles directory: d:\Users

Во втором окне Мастера расшифроки, вам необходимо указать расположение каталога Windows и папки профилей пользователя. Эта информация необходима программе, чтобы найти соответствующие файлы и папки, связанные с Credential Manager.

3 Сканирование системы и выбор учетной записи пользователя



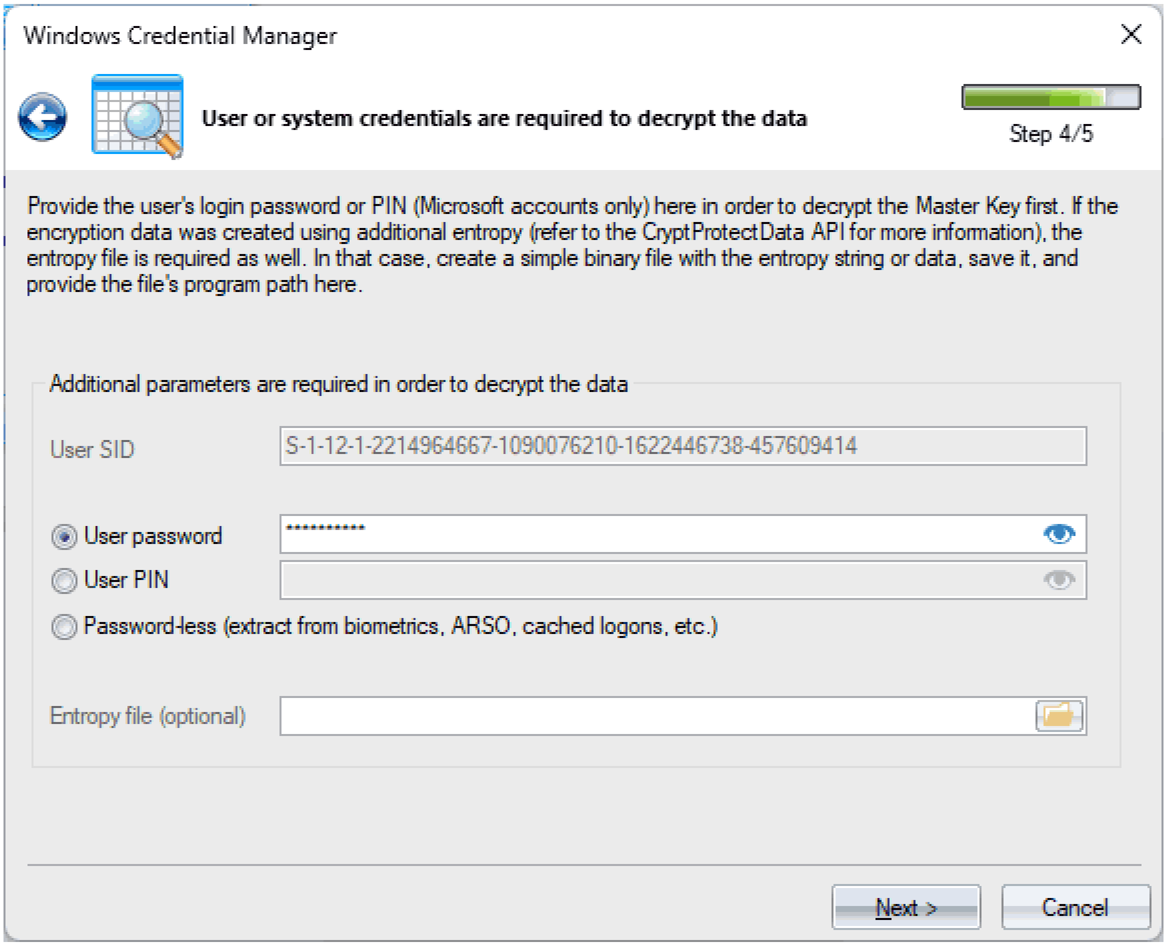
To proceed with decryption, select the user account you need, and click the "Next" button

	User name	Found...	Last logon	Profile directory
1	SYSTEM	1		D:\win\System32\Config\systemprofile
2	admin	25	2023-03-12 11:45:15	d:\Users\Admin

Windows Credentials Guard is OFF

В третьем диалоге Мастера, программа сканирует учетные записи на основе указанных папок и отображает список найденных имен пользователей. Из этого списка выберите учетную запись пользователя, для которой вы хотите выполнить поиск и расшифровку паролей.

4 Ввод пароля пользователя или ПИН-кода



Windows Credential Manager

User or system credentials are required to decrypt the data

Step 4/5

Provide the user's login password or PIN (Microsoft accounts only) here in order to decrypt the Master Key first. If the encryption data was created using additional entropy (refer to the CryptProtectData API for more information), the entropy file is required as well. In that case, create a simple binary file with the entropy string or data, save it, and provide the file's program path here.

Additional parameters are required in order to decrypt the data

User SID: S-1-12-1-2214964667-1090076210-1622446738-457609414

● User password: ***********

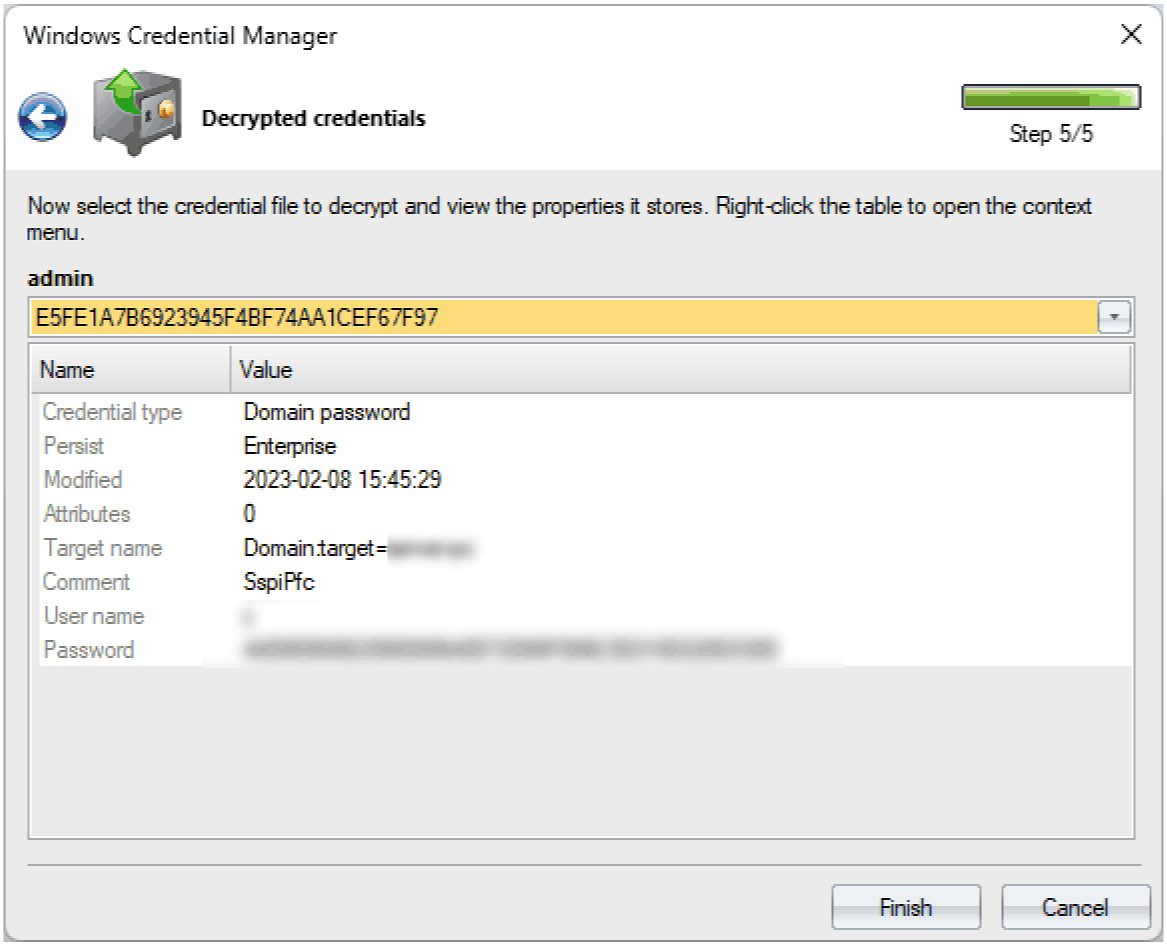
○ User PIN

○ Password-less (extract from biometrics, ARSO, cached logons, etc.)

Entropy file (optional):

После выбора учетной записи пользователя, вам также необходимо будет также указать его пароль или ПИН-код (только для учетной записи Microsoft). Эта информация необходима для расшифровки данных, защищенных при помощи DPAPI. Кроме того, в некоторых случаях стоит попробовать функцию расшифровки без пароля учетной записи. Если программа обнаружит какую-либо чувствительную информацию, такую как биометрия, ARSO, кэшированный вход и т.д., она может быть использована для расшифровки данные без знания пароля пользователя или ПИН-кода.

5 Поиск и расшифровка Windows Credentials



Now select the credential file to decrypt and view the properties it stores. Right-click the table to open the context menu.

admin

E5FE1A7B6923945F4BF74AA1CEF67F97

Name	Value
Credential type	Domain password
Persist	Enterprise
Modified	2023-02-08 15:45:29
Attributes	0
Target name	Domain:target=[redacted]
Comment	SspiPfc
User name	[redacted]
Password	[redacted]

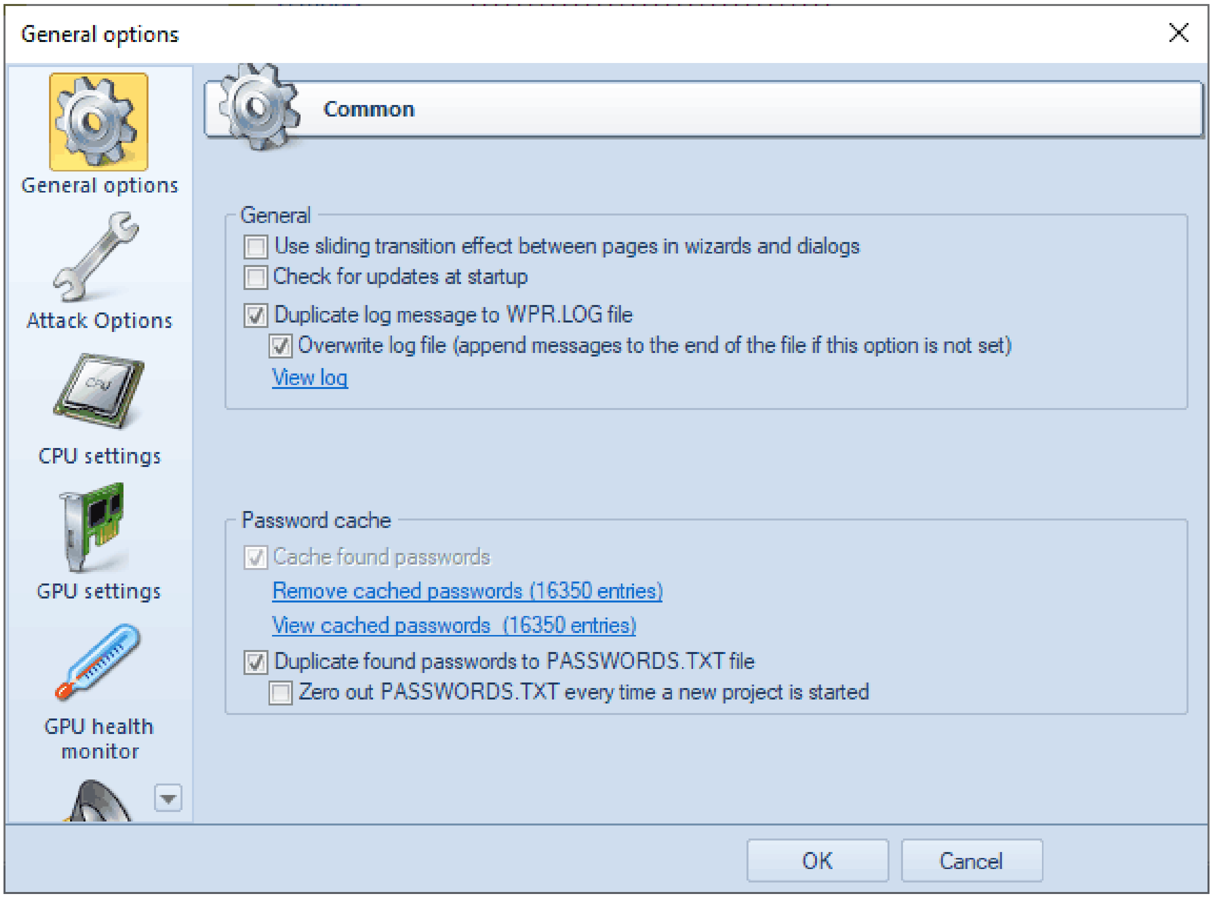
В финальном окне Мастера программа производит поиск всех credentials, которые связанны с выбранной учетной записью пользователя, и расшифровывает их при помощи введенного на предыдущем шаге пароля пользователя или PIN-кода. После завершения процесса расшифровки вы сможете просматривать и анализировать свойства каждой расшифрованной записи, такие как сетевое имя, имя пользователя, пароль и другую доступную информацию.

2.8 Меню Настройки

2.8.1 Общие

Общие настройки разделены на 5 частей.

2.8.1.1 Общие



General options

General

□ Use sliding transition effect between pages in wizards and dialogs

□ Check for updates at startup

☑ Duplicate log message to WPR.LOG file

☑ Overwrite log file (append messages to the end of the file if this option is not set)

View log

Password cache

☑ Cache found passwords

Remove cached passwords (16350 entries)

View cached passwords (16350 entries)

☑ Duplicate found passwords to PASSWORDS.TXT file

□ Zero out PASSWORDS.TXT every time a new project is started

Use sliding transition effect between pages in wizards and dialog
Включение графического эффекта перехода между диалогами.

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

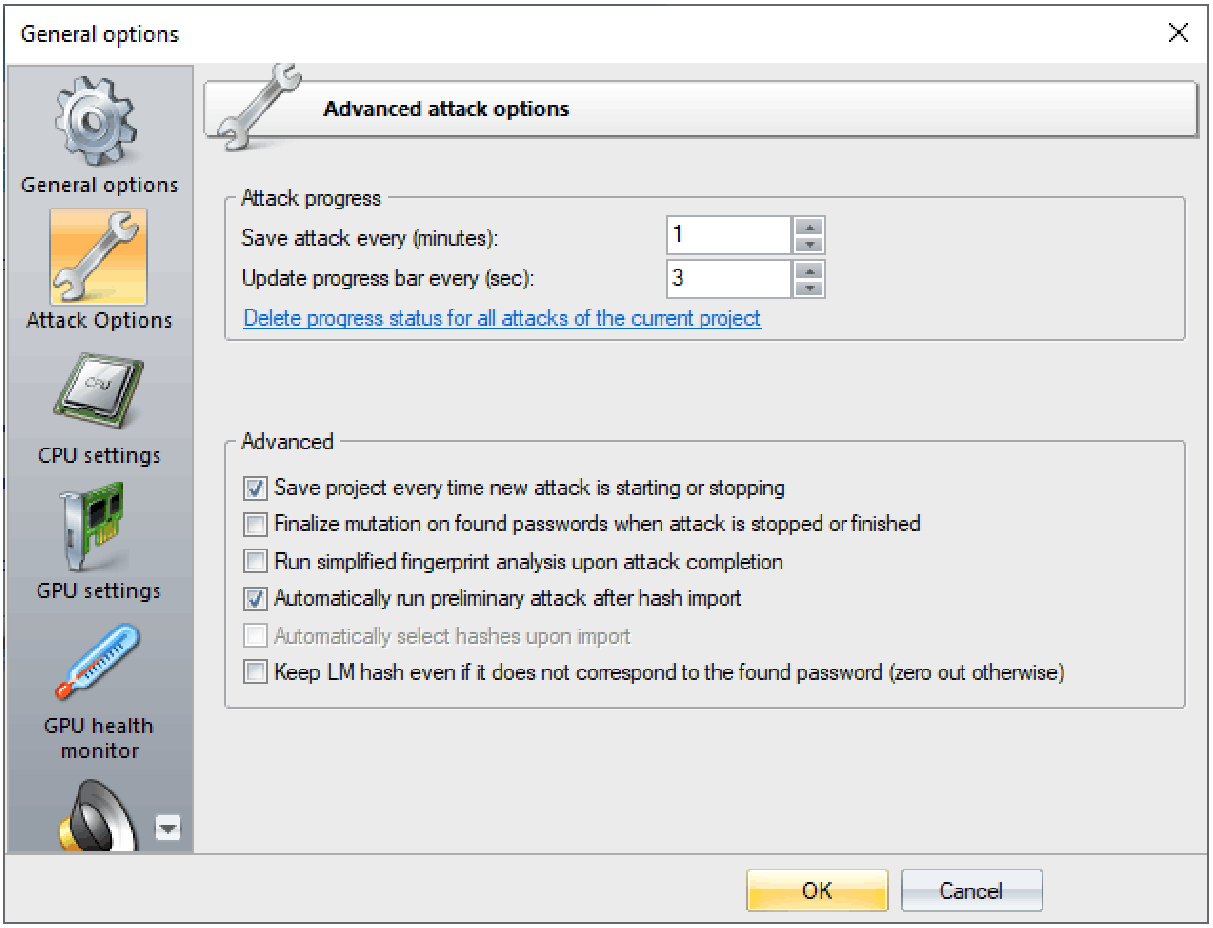
Duplicate log messages to wpr.log file - если установлена эта опция, то все записи журнала событий будут продублированы в файл WPR.LOG. Установка этой опции может повлиять на производительность системы во время анализа большого списка хэшей. Опция полезна в том случае, если программа работает нестабильно или зависает. Файл WPR.LOG расположен в установочном каталоге программы.

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

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.

2.8.1.2 Настройки атак



Advanced attack options

Attack progress

Save attack every (minutes): 1

Update progress bar every (sec): 3

Delete progress status for all attacks of the current project

Advanced

☑ Save project every time new attack is starting or stopping

☐ Finalize mutation on found passwords when attack is stopped or finished

☐ Run simplified fingerprint analysis upon attack completion

☑ Automatically run preliminary attack after hash import

☐ Automatically select hashes upon import

☐ Keep LM hash even if it does not correspond to the found password (zero out otherwise)

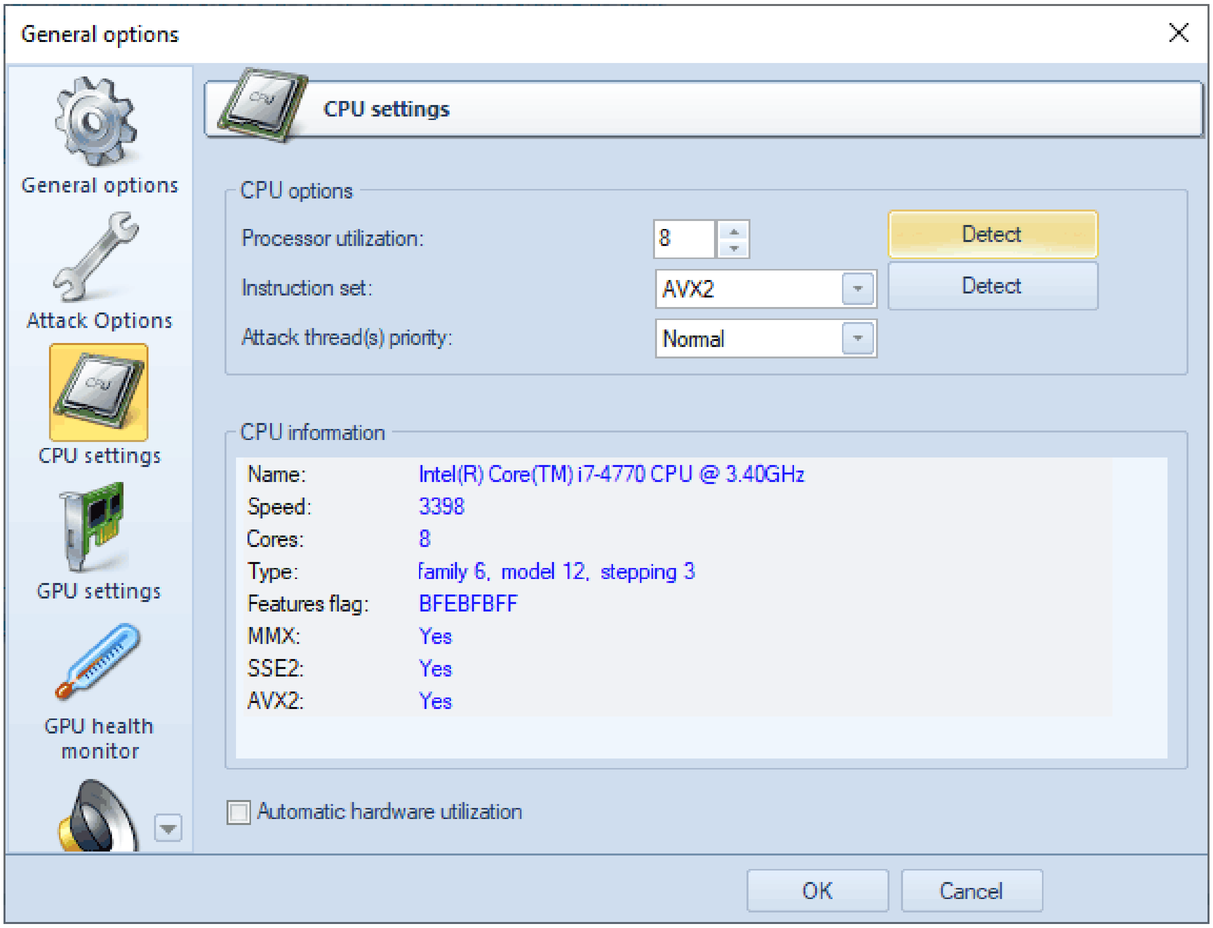
Первая группа настроек позволяет задать интервалы сохранения и обновления текущего состояния атаки. По умолчанию, атака сохраняет свое состояние каждые 5 минут (в последствие, можно продолжить атаку с последнего сохраненного состояния) и обновляет экран каждые 3 секунды.

Дополнительно

- *'Сохранять проект каждый раз...'.* Если установлена, то проект будет сохраняться автоматически каждый раз при запуске или остановке атаки (включая атаки, входящие в групповую атаку).
- *Запускать простую Идентификационную атаку после завершения основной.* Бывает весьма полезна для расшифровки хэшей истории или для большого списка хэшей (если найден хотя бы один пароль).
- *Задействовать модуль анализа и мутации паролей для найденных паролей после окончания атаки.* Данная опция бывает чрезвычайно полезна, например, для расшифровки похожих паролей.

- *Автоматический запуск предварительной атаки после каждого импорта хэшей.* Данная атака позволяет за считанные секунды выявить особо слабые пароли.
- *После импорта хэшей автоматически выделять записи для перебора.* Эта настройка позволяет автоматически отмечать для атаки все хэши после загрузки их в программу.
- *Сохранять LM-хэш, даже если он не соответствует найденному паролю.* В Windows Server 2003 и более поздних серверных операционных системах, если аутентификация LM отключена на сервере, в LM-хэшах хранятся шумовые (случайно созданные) данные. Если эта настройка программы не задана, WPR проверяет соответствующий хэш LM каждый раз, когда найден новый пароль. Как только программа обнаруживает, что LM-хэш не соответствует найденному паролю, она обнуляет слот с LM-хэшем. Если эта настройка включена, программа ничего не делает с неправильными хэшами LM.

2.8.1.3 Настройки CPU



Processor utilization: 8

Instruction set: AVX2

Attack thread(s) priority: Normal

Name:	Intel(R) Core(TM) i7-4770 CPU @ 3.40GHz
Speed:	3398
Cores:	8
Type:	family 6, model 12, stepping 3
Features flag:	BFEBFBFF
MMX:	Yes
SSE2:	Yes
AVX2:	Yes

☐ Automatic hardware utilization

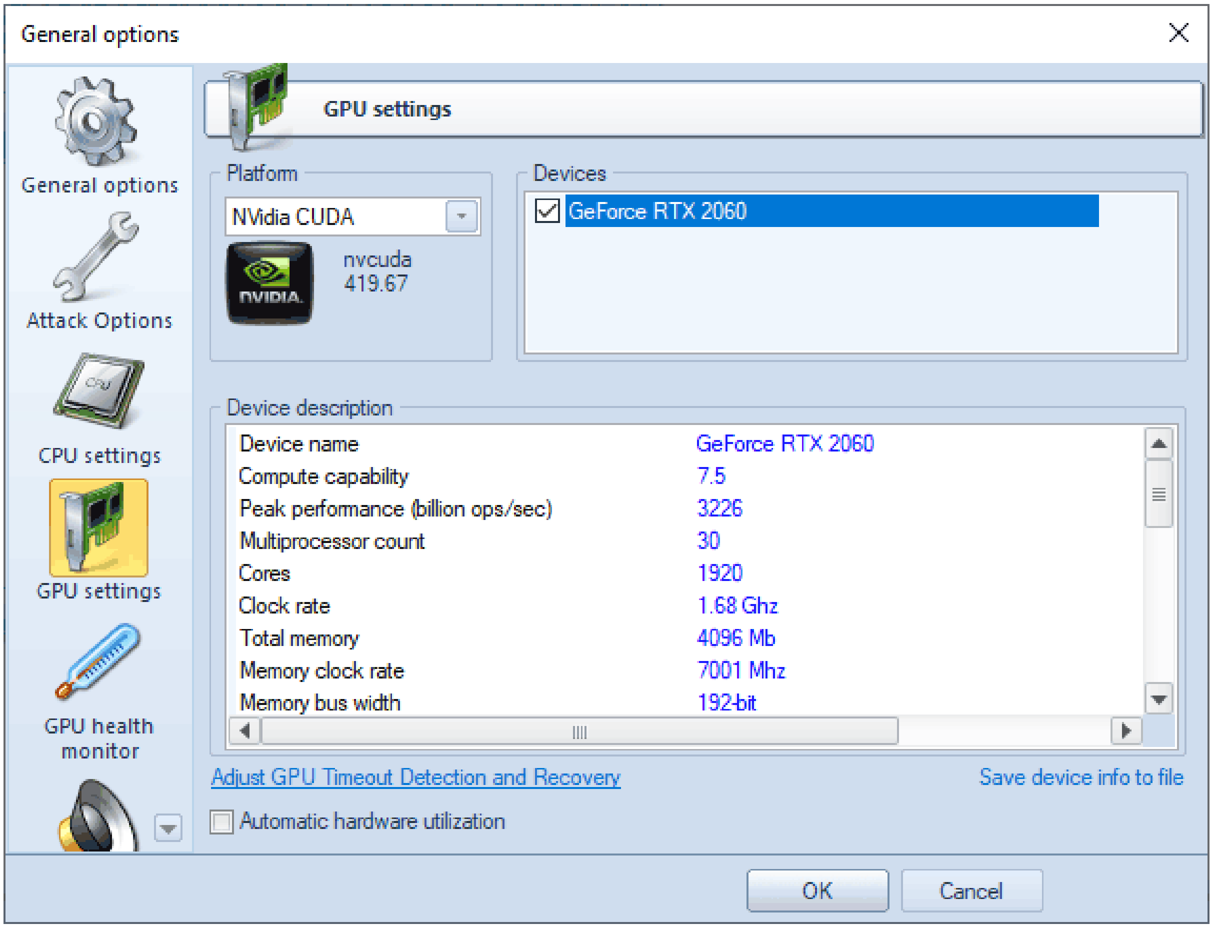
Поскольку большинство атак имеют поддержку многопоточности, то можно задавать количество одновременно выполняемых потоков перебора. В большинстве случаев, оно должно совпадать с количеством ядер процессора. Однако, если в процессоре есть поддержка технологии Hyper-Threading, то можно даже удвоить количество одновременно работающих потоков перебора.

В Windows Password Recovery алгоритмы перебора DES, MD4 и SHA-1 заточены под следующие архитектуры процессора: X86, MMX, SSE2 и AVX2. 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.

Если установлена опция автоматического определения оборудования, то настройки процессора будут недоступны.

2.8.1.4 Настройки GPU



General options

GPU settings

Platform: NVidia CUDA

nvcuda
419.67

Devices:
☑ GeForce RTX 2060

Device description

Device name	GeForce RTX 2060
Compute capability	7.5
Peak performance (billion ops/sec)	3226
Multiprocessor count	30
Cores	1920
Clock rate	1.68 Ghz
Total memory	4096 Mb
Memory clock rate	7001 Mhz
Memory bus width	192-bit

Adjust GPU Timeout Detection and Recovery

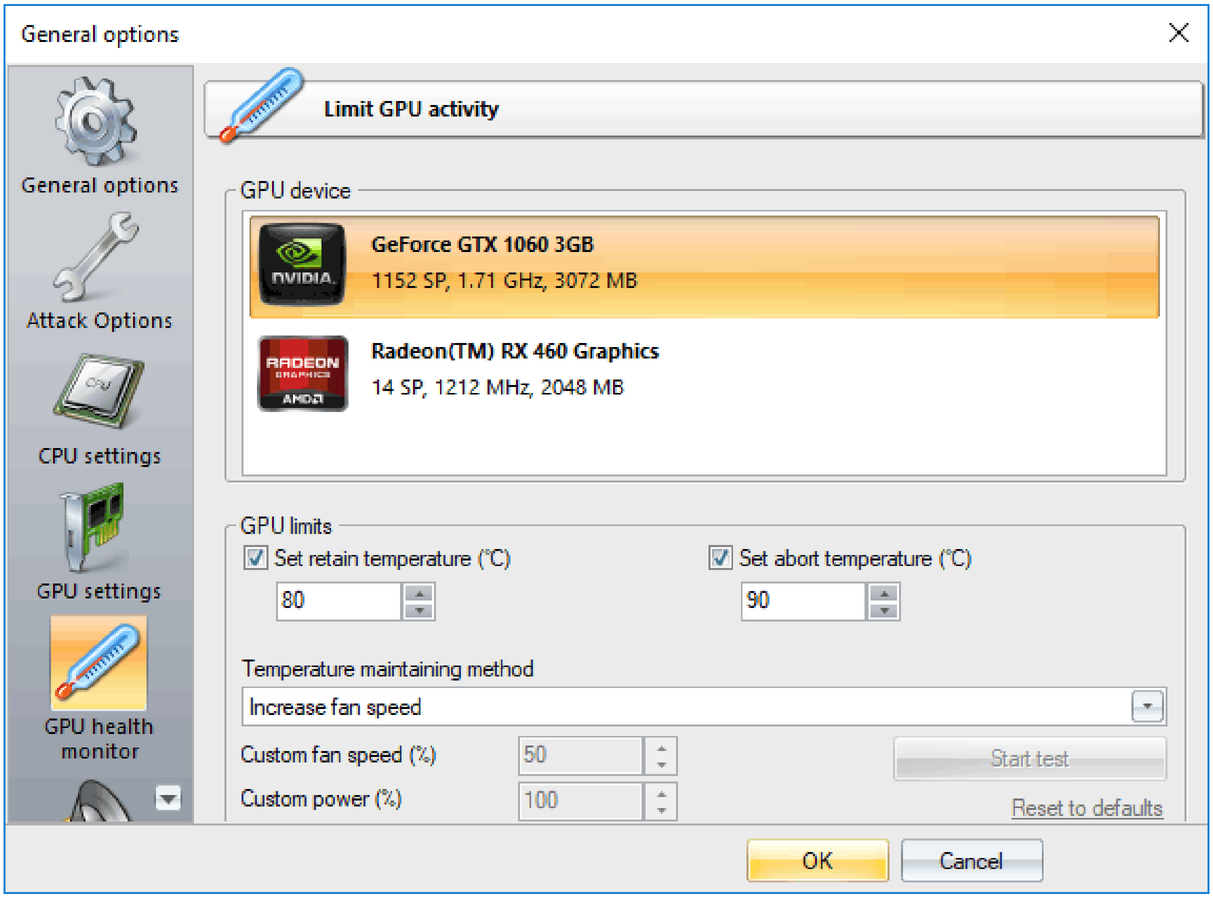
Save device info to file

□ Automatic hardware utilization

Перед запуском атаки на GPU, необходимо выбрать ее в общих настройках программы. Для этого просто поставьте галочку напротив имени видеокарты. Все основные характеристики устройства отображены в нижней таблице.
В программе поддерживаются видеокарты NVidia на платформе CUDA, AMD Radeon и Intel на платформе OpenCL.

Если установлена опция автоматического определения оборудования, то настройки видеокарт будут недоступны.

2.8.1.5 Монитор активности GPU



GPU device

- GeForce GTX 1060 3GB — 1152 SP, 1.71 GHz, 3072 MB
- Radeon(TM) RX 460 Graphics — 14 SP, 1212 MHz, 2048 MB

GPU limits

☑ Set retain temperature (°C): 80

☑ Set abort temperature (°C): 90

Temperature maintaining method: Increase fan speed

Custom fan speed (%): 50

Custom power (%): 100

Монитор активности может быть использован в программе для удержания температуры видеокарт в определенных пределах во время перебора паролей, а также для контроля перегрева и отключения карт в случае достижения критических температур.

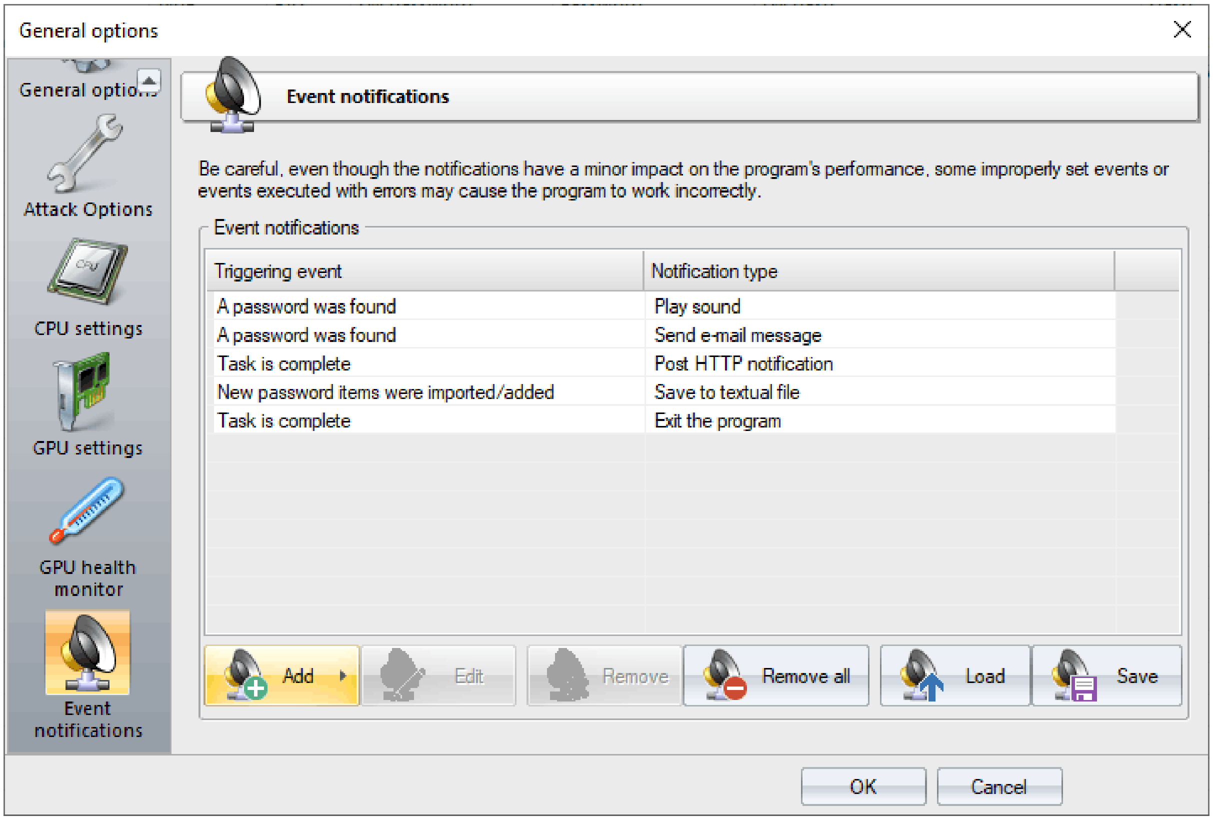
Чтобы задать желаемую температуру GPU, установите соответствующую опцию и задайте значение в градусах. Затем выберите один из методов поддержания температуры:

- **Одновременное увеличение скорости вентилятора и уменьшения частоты графического процессора**. Этот метод можно использовать тогда, когда желательно уменьшить шум от работы вентилятора, но можно пожертвовать незначительным снижением производительности графического процессора.
- **Увеличение скорости вентилятора**. При нагревании GPU выше температуры удержания, скорость вентилятора будет повышаться, при остывании - понижаться. Выбирайте этот метод, если требуется максимальная производительность программы. При выборе этого метода, рекомендуется также задать температуру отключения, чтобы избежать перегрев карты.
- **Уменьшать частоту графического процессора**. Эффективный метод снижения температуры. К недостаткам можно отнести значительное падение производительности в некоторых случаях. Частота процессора автоматически подстраивается под температуру удержания. Скорость работы вентилятора при этом будет определяться системными настройками.
- **Пользовательские настройки** скорости вентилятора и частоты работы графического процессора.

Если установить опцию отключения, то, при достижении выбранной карт установленной температуры, перебор паролей будет прекращен.

Внимание! Для AMD видеокарт поддерживается только опция отключения. Большинство драйверов AMD не позволяют изменять некоторые значения в ручном режиме, имеют многочисленные баги и могут привести к нестабильности системы или даже BSOD. Используйте встроенную утилиту Radeon, чтобы изменить профиль производительности, если это необходимо.

2.8.1.6 Оповещения



Be careful, even though the notifications have a minor impact on the program's performance, some improperly set events or events executed with errors may cause the program to work incorrectly.

Event notifications

Triggering event	Notification type
A password was found	Play sound
A password was found	Send e-mail message
Task is complete	Post HTTP notification
New password items were imported/added	Save to textual file
Task is complete	Exit the program

Для автоматизации процесса восстановления паролей можно использовать уведомления о событиях. Имеется несколько типов событий:

- **Запуск программы**. Программа только что была запущена и готова к работе.
- **Закрытие программы**. Это событие возникает перед самым выходом из программы.
- **Загрузка или создание нового проекта**. Создание пустого проекта также попадает под это событие.
- **Сохранение проекта**. Текущий проект сохранен на диск. Это событие может возникать несколько раз во время атаки, в зависимости от настроек программы.
- **Закрытие проекта**. Пользователь закрыл текущий проект.
- **Запуск задачи**. Была запущена новая задача. Задача включает в себя одну или несколько атак и по крайней мере один элемент пароля.
- **Задача завершена**. Это событие возникает когда пользователь приостановил задачу, все атаки полностью завершены или возникли критические ошибки при выполнении задачи.
- **Добавлены новые парольные элементы**. Пользователь загрузил или добавил один или несколько парольных элементов в текущие проект.

- **Запуск атаки**. Была запущена новая атака. Это событие может возникнуть несколько раз в рамках одной задачи. Например, при запуске пакетной атаки.
- **Атака завершена**. Это событие возникает при успешном или неудачном завершении какой-либо атаки.
- **Найден пароль**. Программа нашла пароль.

Выбрав одно из событий, можно настроить оповещение, которое будет выполняться при срабатывании этого события. Типы оповещений:

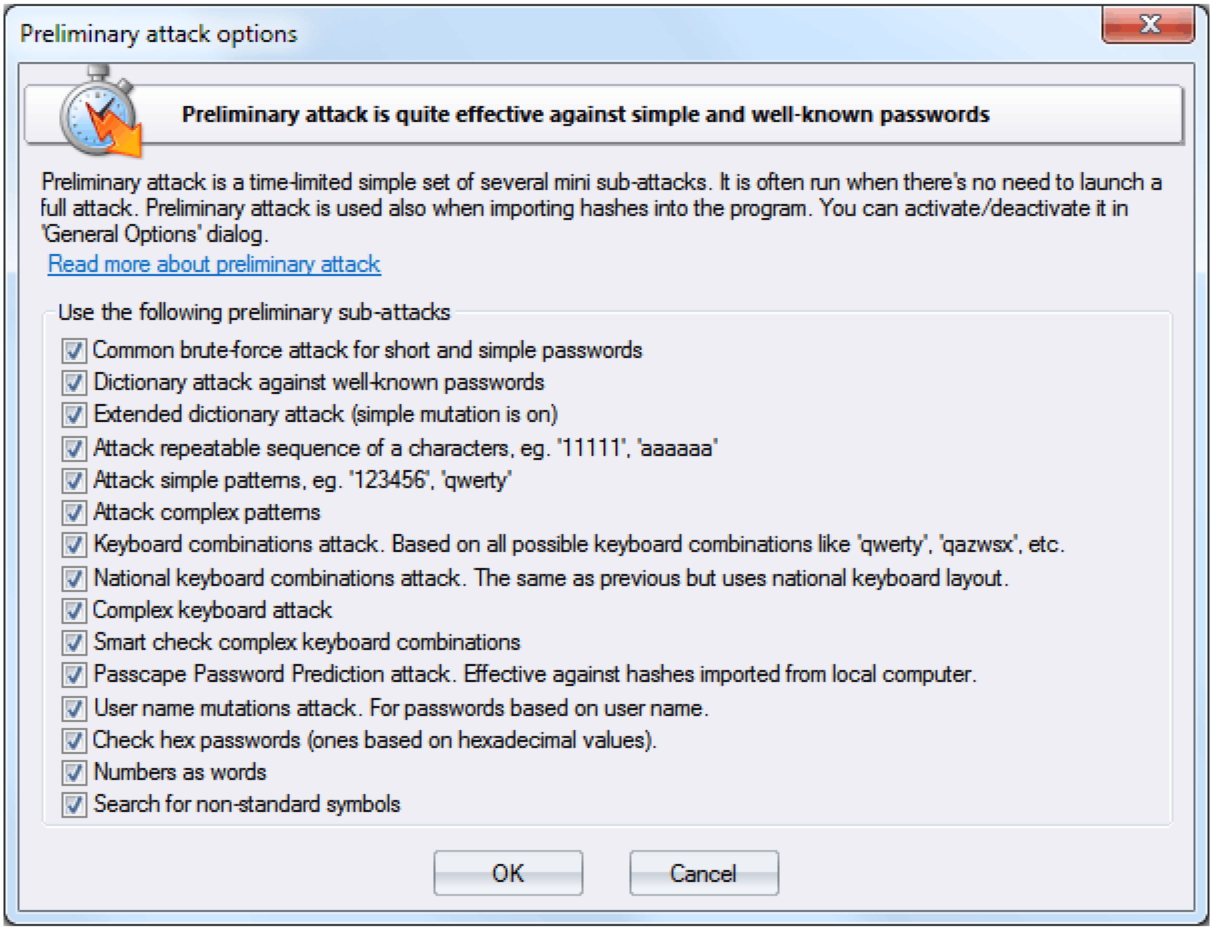
- Проиграть звуковой файл
- Вывести на печать
- Отправка электронного сообщения
- Уведомление по HTTP
- Запуск программы
- Сохранение в текстовый файл
- Сохранение в *.INI файл
- Сохранение в базу данных SQLITE
- Сохранение в *.HTML файл
- Выход из программы
- Выход из системы
- Перезагрузка системы
- Перевод системы в спящий режим

2.8.2 Настройки Атак

2.8.2.1 Предварительная Атака

Предварительная атака (разработана в Passscape 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 1-2 минут или даже быстрее.



Preliminary attack options

Preliminary attack is quite effective against simple and well-known passwords

Preliminary attack is a time-limited simple set of several mini sub-attacks. It is often run when there's no need to launch a full attack. Preliminary attack is used also when importing hashes into the program. You can activate/deactivate it in 'General Options' dialog.

Read more about preliminary attack

Use the following preliminary sub-attacks

- ☑ Common brute-force attack for short and simple passwords
- ☑ Dictionary attack against well-known passwords
- ☑ Extended dictionary attack (simple mutation is on)
- ☑ Attack repeatable sequence of a characters, eg. '11111', 'aaaaaa'
- ☑ Attack simple patterns, eg. '123456', 'qwerty'
- ☑ Attack complex patterns
- ☑ Keyboard combinations attack. Based on all possible keyboard combinations like 'qwerty', 'qazwsx', etc.
- ☑ National keyboard combinations attack. The same as previous but uses national keyboard layout.
- ☑ Complex keyboard attack
- ☑ Smart check complex keyboard combinations
- ☑ Passcape Password Prediction attack. Effective against hashes imported from local computer.
- ☑ User name mutations attack. For passwords based on user name.
- ☑ Check hex passwords (ones based on hexadecimal values).
- ☑ Numbers as words
- ☑ Search for non-standard symbols

Мини-модули предварительной атаки:

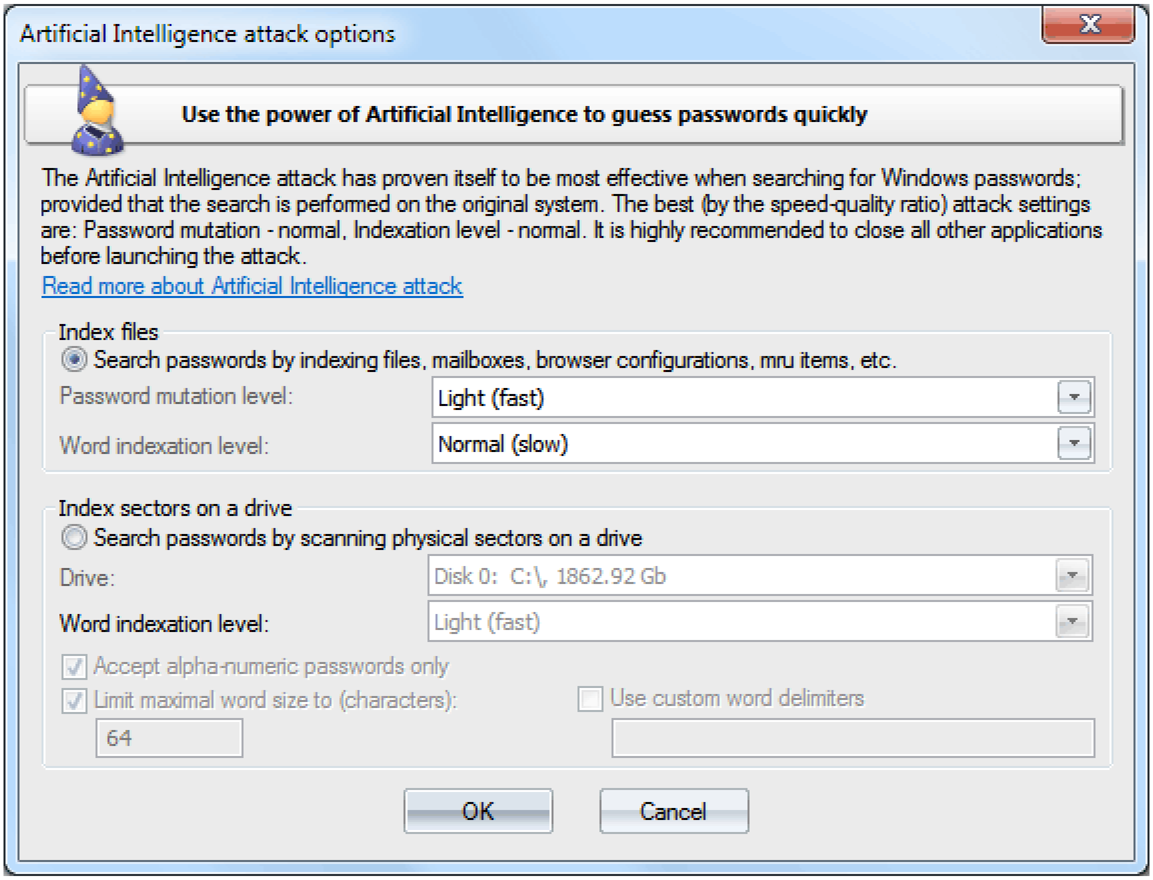
- Простая атака перебором, которая состоит из нескольких небольших атак грубой силой по определенным наборам символов.
- Простая атака по словарю. Быстрая проверка пароля по всем словам внутреннего словаря программы.
- Расширенная атака по словарю. Похожа на простую атаку по словарю, но с использованием нескольких опций мутации.
- Атака на повторяющиеся последовательности. Проверка паролей, состоящих из повторяющихся символов. Например, '1111111' или 'xxxxxxxxxx'.
- Атака на простые образцы, например, '1234567890' или 'йцукен'.
- Атака на сложные образцы. То же что и предыдущий пункт, но для более сложных, составных образцов.
- Клавиатурная атака проверяет всевозможные пароли, привязанные к раскладке клавиатуры: 'qwerty', 'qazwsx', 'asdzxc' и т.д.
- Атака на пароли национальной раскладки клавиатуры. Проверка паролей, созданных на основе национальных раскладок клавиатур.
- Сложная клавиатурная атака аналогична предыдущим двум, но для более сложных, составных паролей клавиатуры и часто употребляемых паролей.
- Предугадывание паролей - наиболее действенный механизм с элементами искусственного интеллекта для угадывания паролей. Известный также как Passcape Password Prediction.
- Атака на пароли, основанные от имени пользователя.
- Атака на шестнадцатеричные формы пароля. Например, 3A79F1
- Атака на цифровые пароли в виде слов
- Поиск коротких паролей, состоящих нестандартных UNICODE символов.

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.

Интеллектуальная атака в основном используется при импорте хэшей с локального компьютера. Атака сканирует локальный компьютер, индексирует и создает список найденных слов и паролей, анализирует их, на основе анализа создает 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 пароли, зашифрованные при помощи хэш функций. 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.



Artificial Intelligence attack options

Use the power of Artificial Intelligence to guess passwords quickly

The Artificial Intelligence attack has proven itself to be most effective when searching for Windows passwords; provided that the search is performed on the original system. The best (by the speed-quality ratio) attack settings are: Password mutation - normal, Indexation level - normal. It is highly recommended to close all other applications before launching the attack.

Read more about Artificial Intelligence attack

Index files

● Search passwords by indexing files, mailboxes, browser configurations, mru items, etc.

Password mutation level: Light (fast)

Word indexation level: Normal (slow)

Index sectors on a drive

○ Search passwords by scanning physical sectors on a drive

Drive: Disk 0: C:\, 1862.92 Gb

Word indexation level: Light (fast)

☑ Accept alpha-numeric passwords only

☑ Limit maximal word size to (characters): 64

□ Use custom word delimiters

Звучит довольно абстрактно, но на практике атака четко 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, введенные когда-либо пользователем. Сюда входят пароли сети, ICQ, электронной почты, FTP, пароли учетных 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 ее 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.

В начале работы атаки программа производит поиск всех известных ей паролей в системе. Для этого существуют 32 мини-модуля для расшифровки паролей системы, почты, браузеров, мессенджеров, архивов и т.д. Затем идет 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.

В среднем, при наименьшем уровне индексации и мутации, время атаки может варьироваться от 1 минуты до 10-15 минут, в зависимости от конфигурации вашей системы, сетевой активности пользователя и других факторов. На домашнем компьютере весь проход занимает, как правило, не более 7-8 минут. 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.

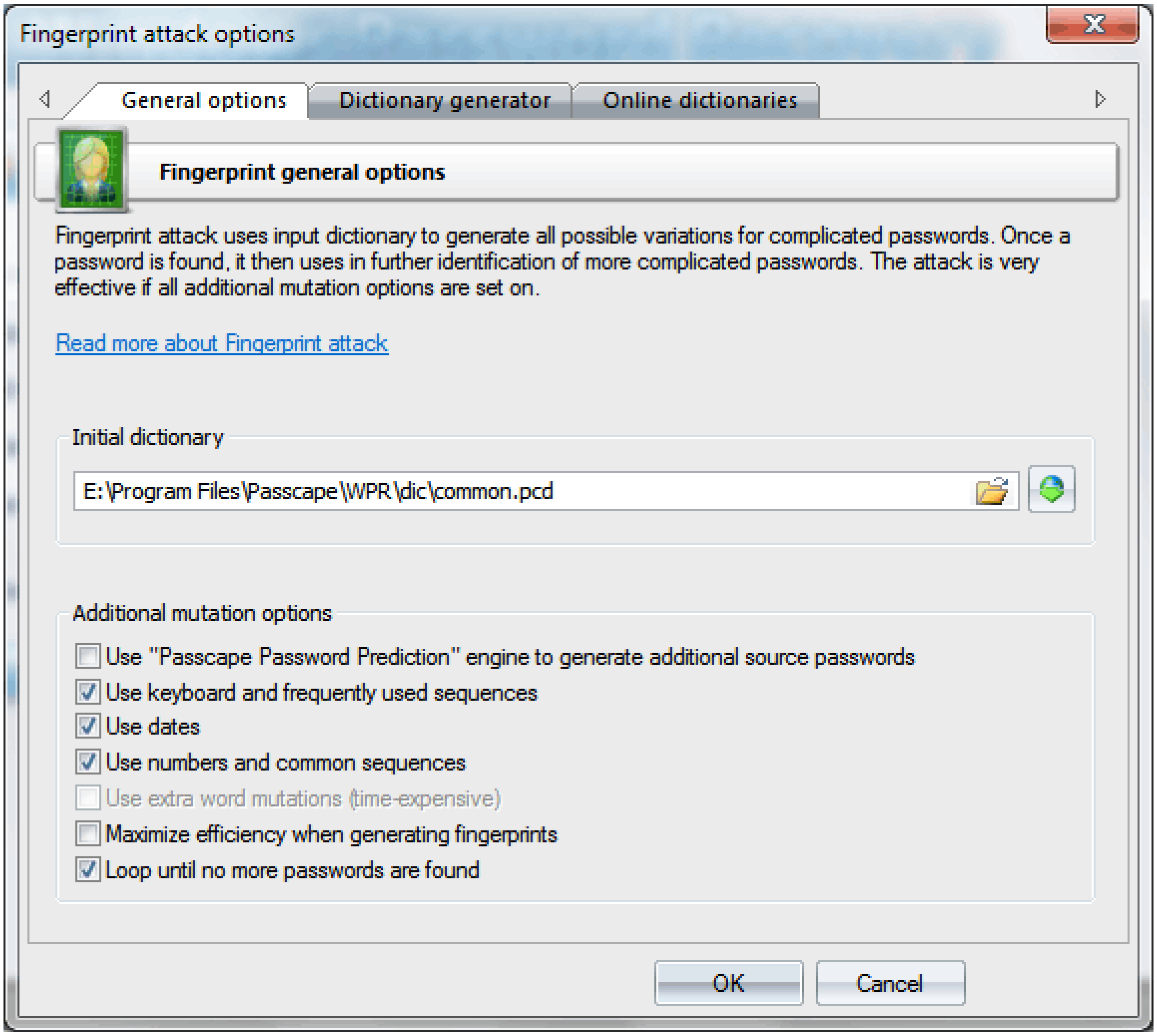
Перед запуском интеллектуальной атаки рекомендуется закрыть все программы. Если интеллектуальная атака протекает очень медленно, можно попробовать удалить кэшированные пароли программы (если их значение переваливает за десяток тысяч).

Начиная с версии Windows Password Recovery 9.5 в Интеллектуальной атаке появился новый режим работы, который производит поиск паролей непосредственно в секторах выбранного диска. Этот режим совместим и с LM, и с NTLM хэшами, позволяя находить как ASCII, так и UNICODE пароли. В этом режиме имеется ряд дополнительных настроек. Например, '*Word Indexation level*' устанавливает уровень дополнительных мутаций всех найденных паролей. Будьте осторожны, сканирование всех секторов целевого диска, с установленной опцией мутации на 'Hard', может занять значительное время. Учтите также, что алгоритм посекторного сканирования неэффективен в случае, если на диске установлено шифрование. Например, при помощи программ Bitlocker или TrueCrypt.

2.8.2.3 Идентификационная Атака

Идентификационная атака (fingerprint attack) - сравнительно свежий инструмент для восстановления сложных паролей, не поддающихся расшифровке в других атаках. Суть ее 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. Если в процессе атаки был найден какой-либо пароль, он участвует в создании новых отпечатков и атака повторяется снова.

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 займет значительное время. Можно использовать словари с национальными паролями, если есть подозрения, что искомый пароль содержит символы в национальной кодировке. В качестве словаря можно (и даже желательно!) использовать уже готовые списки паролей.


Fingerprint attack options
General options
Dictionary generator
Online dictionaries
Fingerprint general options
Read more about Fingerprint attack
OK
Cancel

Fingerprint attack uses input dictionary to generate all possible variations for complicated passwords. Once a password is found, it then uses in further identification of more complicated passwords. The attack is very effective if all additional mutation options are set on.

Initial dictionary

E:\Program Files\Passcape\WPR\dic\common.pcd

Additional mutation options

- □ Use "Passcape Password Prediction" engine to generate additional source passwords
- ☑ Use keyboard and frequently used sequences
- ☑ Use dates
- ☑ Use numbers and common sequences
- □ Use extra word mutations (time-expensive)
- □ Maximize efficiency when generating fingerprints
- ☑ Loop until no more passwords are found

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

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 путем склейки всех отпечатков друг с другом.

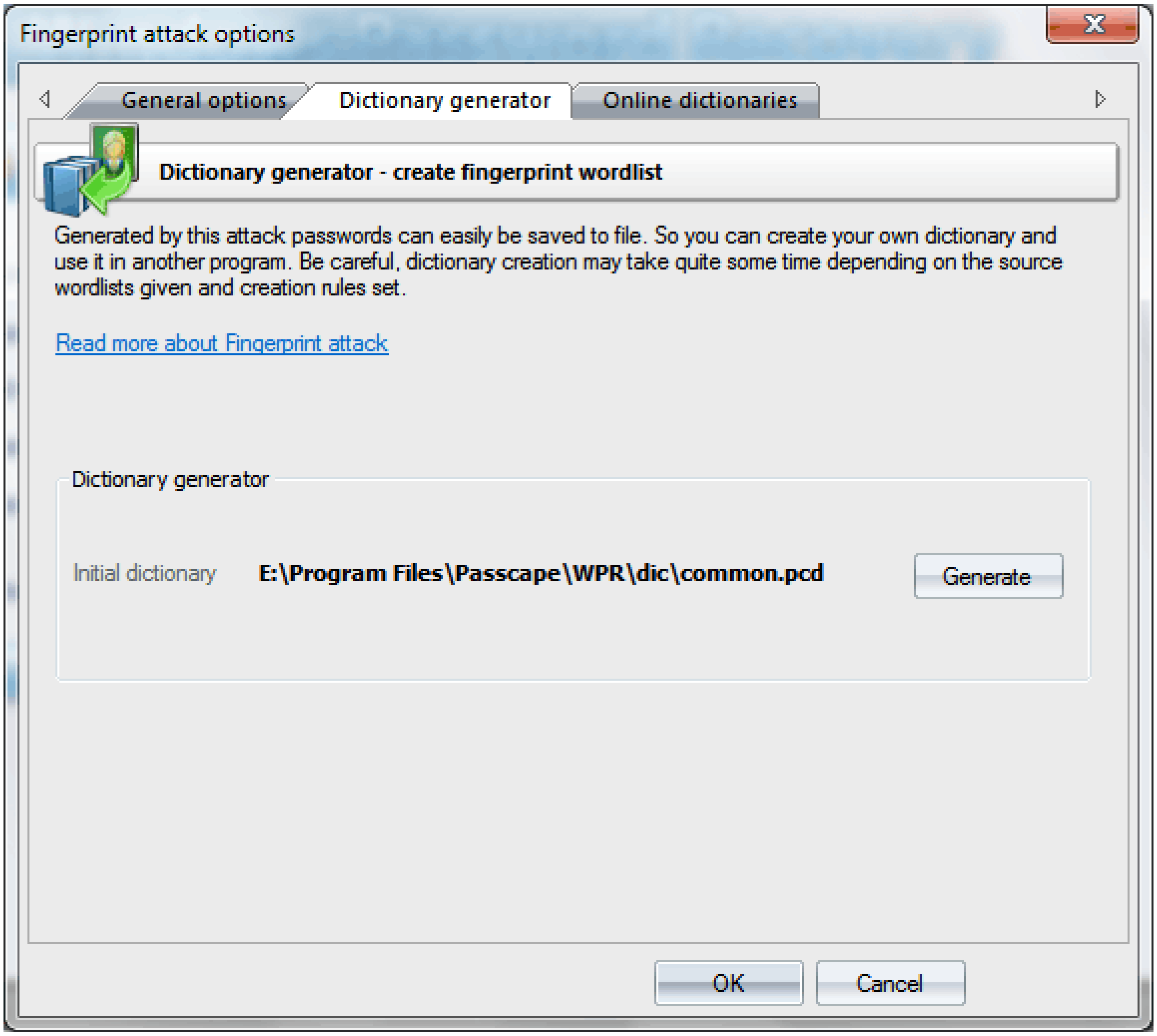
На самом деле, алгоритм генерации отпечатков немного сложнее. Более того, в настройках атаки имеется дополнительная опция **Maximize efficiency when generating fingerprints**, предназначенная для задействования более сложного алгоритма, который позволяет максимизировать эффективность (в ущерб скорости)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

Разберем 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.

Наиболее пристального внимания заслуживает опция **Loop until no more passwords are found**. Вот где идентификационная атака может себя проявить. Работает она таким образом: если во время атаки был найден хотя бы один пароль, по после окончания атаки этот пароль участвует в создании новых отпечатков и атака повторяется сначала. Эта опция хорошо работает на больших списках хэшей, а также на хэшах истории паролей. Следует знать, что установив эту опцию, невозможно будет продолжить атаку с последней запомненной позиции.

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.



Dictionary generator - create fingerprint wordlist

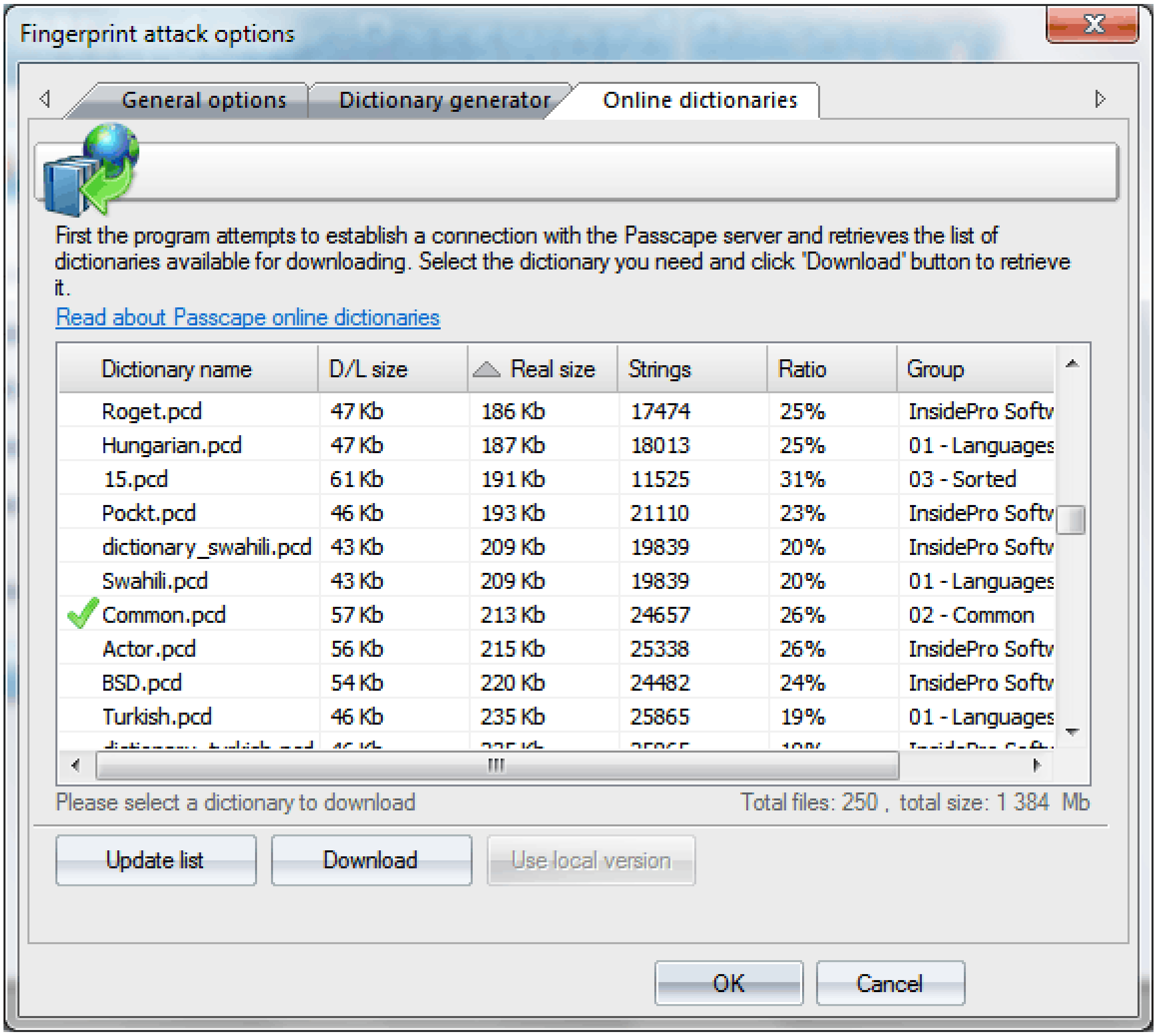
Generated by this attack passwords can easily be saved to file. So you can create your own dictionary and use it in another program. Be careful, dictionary creation may take quite some time depending on the source wordlists given and creation rules set.

Read more about Fingerprint attack

Dictionary generator

Initial dictionary **E:\Program Files\Passcape\WPR\dic\common.pcd**

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



First the program attempts to establish a connection with the Passcape server and retrieves the list of dictionaries available for downloading. Select the dictionary you need and click 'Download' button to retrieve it.

Read about Passcape online dictionaries

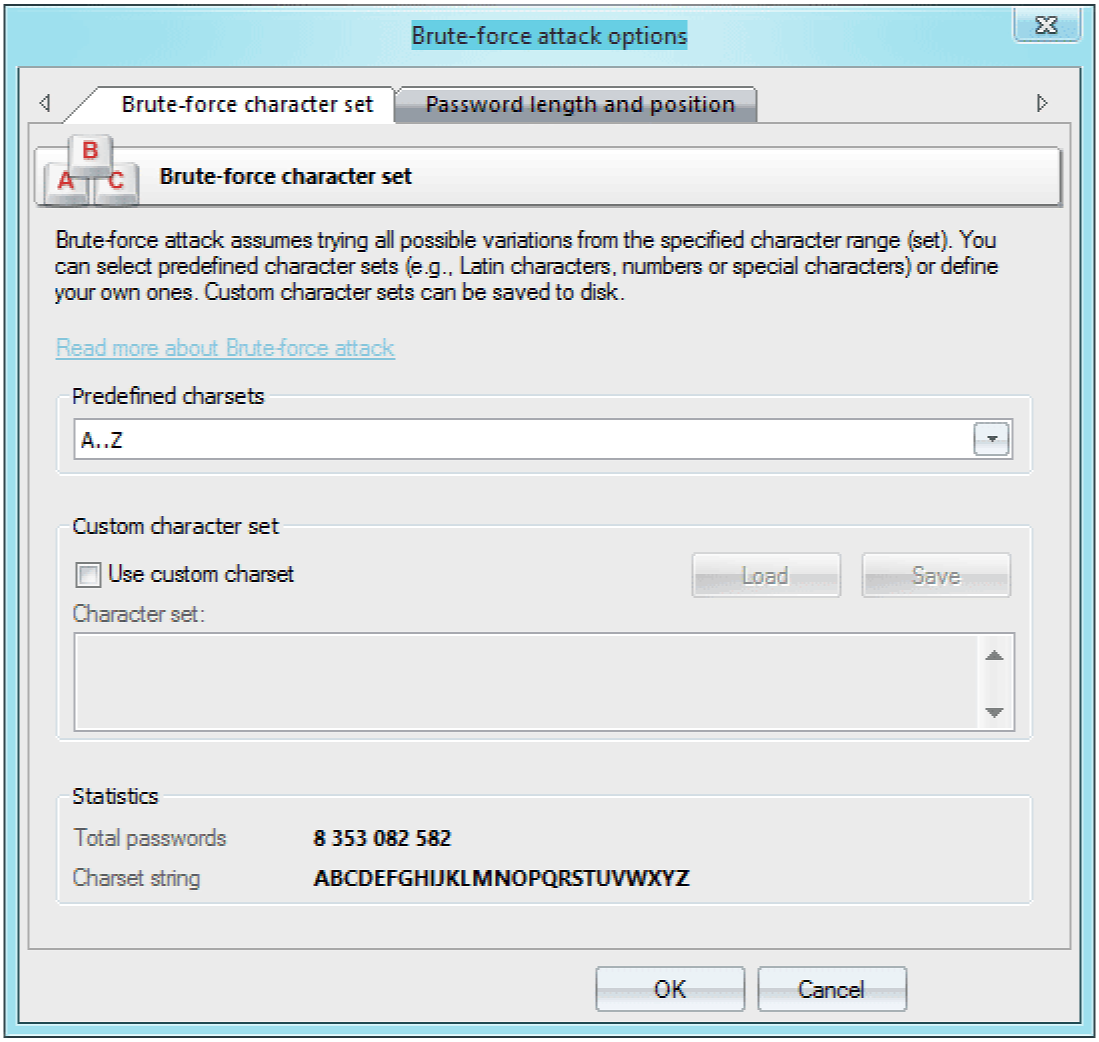
	Dictionary name	D/L size	Real size	Strings	Ratio	Group
	Roget.pcd	47 Kb	186 Kb	17474	25%	InsidePro Softw
	Hungarian.pcd	47 Kb	187 Kb	18013	25%	01 - Languages
	15.pcd	61 Kb	191 Kb	11525	31%	03 - Sorted
	Pockt.pcd	46 Kb	193 Kb	21110	23%	InsidePro Softw
	dictionary_swahili.pcd	43 Kb	209 Kb	19839	20%	InsidePro Softw
	Swahili.pcd	43 Kb	209 Kb	19839	20%	01 - Languages
✓	Common.pcd	57 Kb	213 Kb	24657	26%	02 - Common
	Actor.pcd	56 Kb	215 Kb	25338	26%	InsidePro Softw
	BSD.pcd	54 Kb	220 Kb	24482	24%	InsidePro Softw
	Turkish.pcd	46 Kb	235 Kb	25865	19%	01 - Languages

Please select a dictionary to download Total files: 250 , total size: 1 384 Mb

2.8.2.4 Атака в Лоб (полным перебором)

Полный перебор (или метод 'грубой силы' от англ. brute force) - метод решения задачи путем 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 путем 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 (abcdefghijklmnopqrstuwxyz) для вашей атаки, то потребуется перебрать 217 180 147 158 вариантов для 8-символьного пароля. Эта атака обычно используется только тогда, когда все остальные не увенчались успехом.


Brute-force attack options
Brute-force character set
Password length and position
Brute-force character set

Brute-force attack assumes trying all possible variations from the specified character range (set). You can select predefined character sets (e.g., Latin characters, numbers or special characters) or define your own ones. Custom character sets can be saved to disk.

Read more about Brute-force attack

Predefined charsets: A..Z

Custom character set

☐ Use custom charset

Character set:

Statistics

Total passwords 8 353 082 582

Charset string ABCDEFGHIJKLMNOPQRSTUVWXYZ

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.

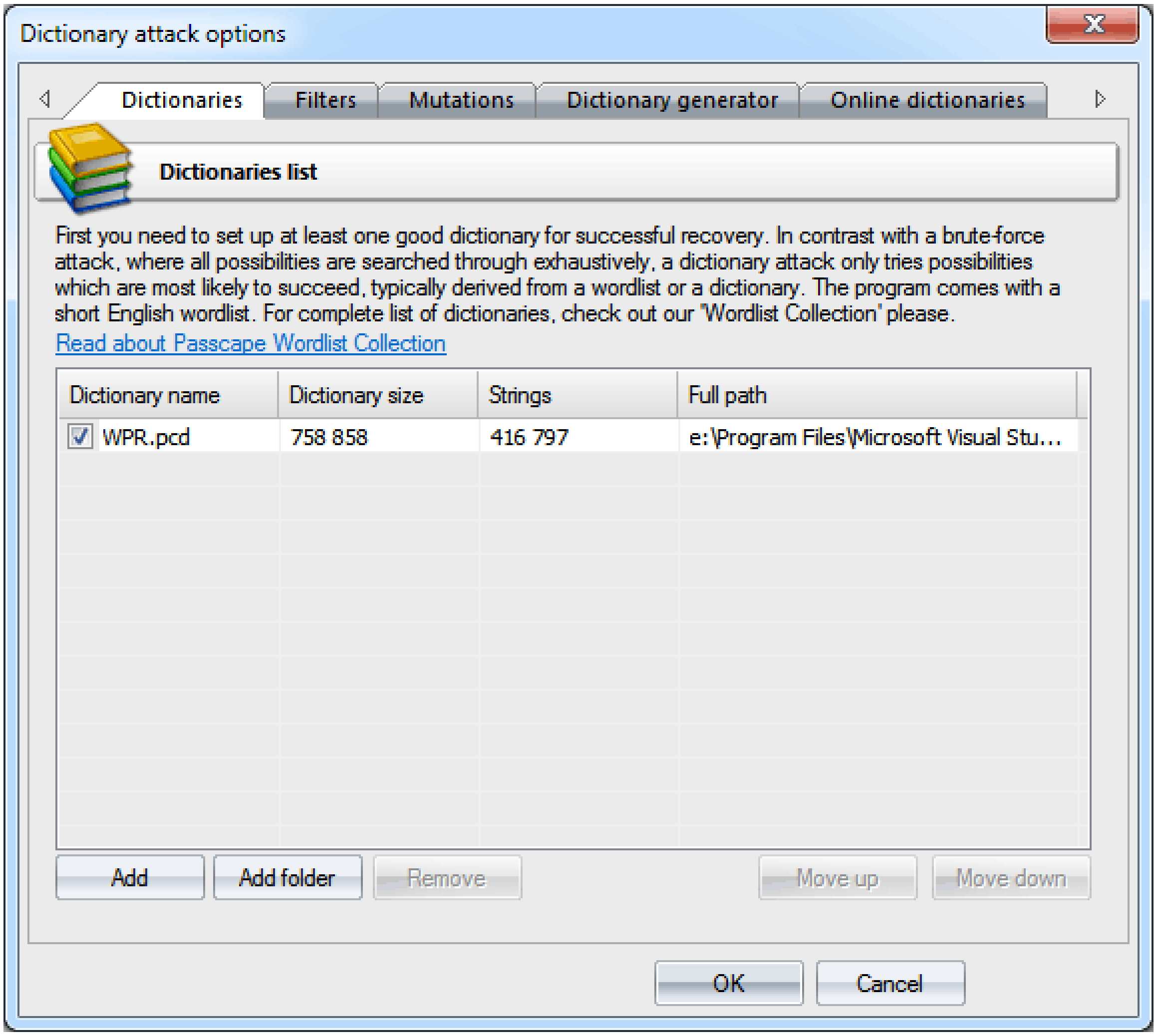
Во второй вкладке необходимо задать минимальную и максимальную длину перебираемых паролей. Важно помнить, что для атаки на LM хэши, максимальная длина не должна превышать 7 символов. Можно также задать и стартовый пароль, с которого начнется перебор. Таблица ниже дает наглядное представление о сложности пароля и зависимости его от длины и набора символов. Подразумевается, что скорость перебора составляет 100 млн. паролей в секунду.

Набор символов	Длина пароля	Пример паролей	Время для полного перебора
A .. Z	5	CRUEL	мгновенно
A .. Z	6	SECRET	3с
A .. Z	7	MONSTER	1м 23с
A .. Z	8	COOLGIRL	36м 11с

A .. Z, 0 .. 9	5	COOL3	мгновенно
A .. Z, 0 .. 9	6	BANG13	22с
A .. Z, 0 .. 9	7	POKER00	13м 26с
A .. Z, 0 .. 9	8	LETMEBE4	8ч 3м 37с
A .. Z, a .. z, 0 .. 9	5	P0k3r	9с
A .. Z, a .. z, 0 .. 9	6	S3cr31	9м 37с
A .. Z, a .. z, 0 .. 9	7	DidIt13	9ч 56м 33с
A .. Z, a .. z, 0 .. 9	8	GoAway99	25д 16ч 26м 34с

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.



First you need to set up at least one good dictionary for successful recovery. In contrast with a brute-force attack, where all possibilities are searched through exhaustively, a dictionary attack only tries possibilities which are most likely to succeed, typically derived from a wordlist or a dictionary. The program comes with a short English wordlist. For complete list of dictionaries, check out our 'Wordlist Collection' please.

Read about Passcape Wordlist Collection

Dictionary name	Dictionary size	Strings	Full path
☑ WPR.pcd	758 858	416 797	e:\Program Files\Microsoft Visual Stu...

Во вкладке **Словари** задается 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 пропустится во время атаки. Вместе с программой поставляется внутренний словарь на 360000 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 введенных символов.

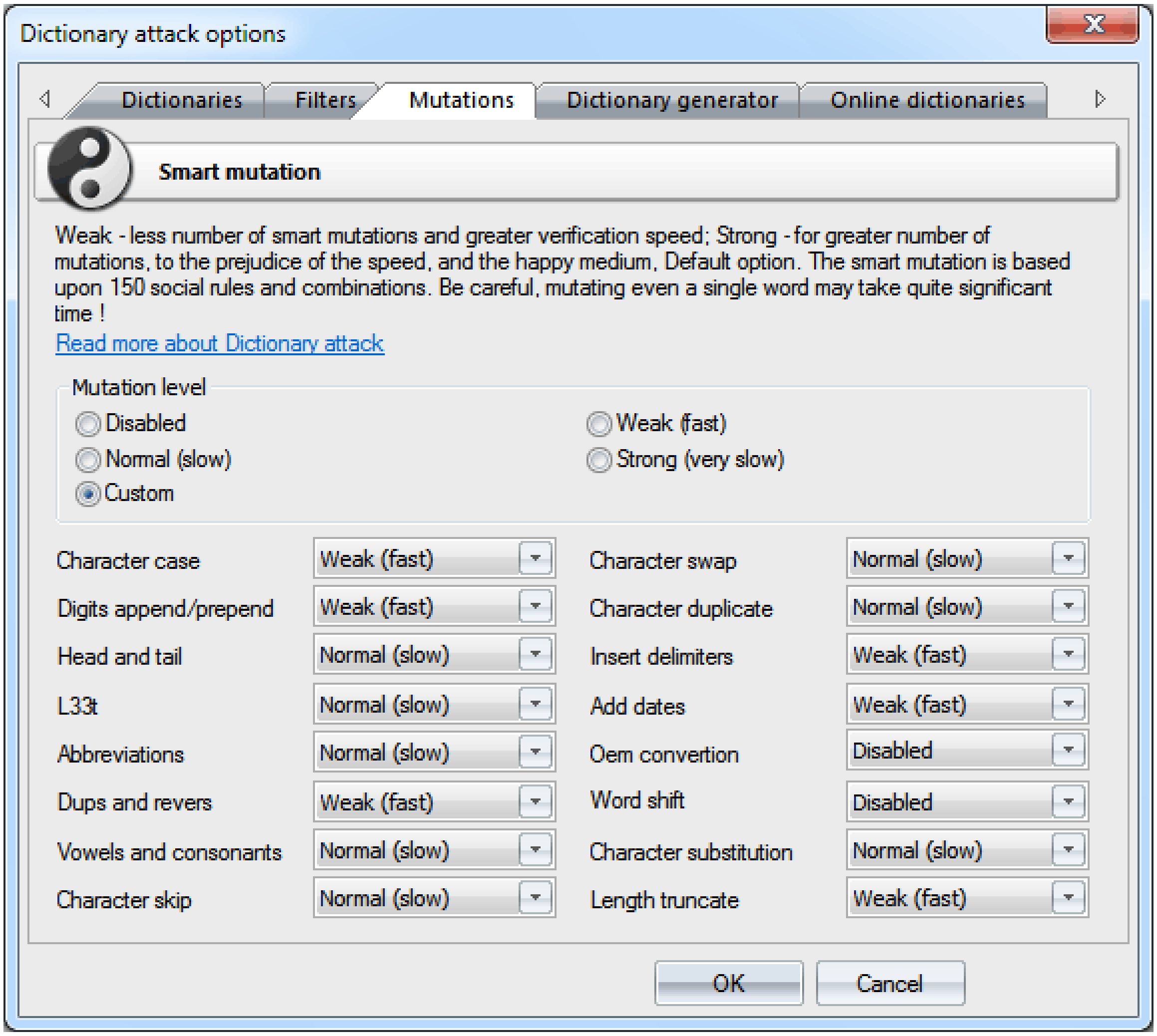
Вкладка **Мутация** предназначена для задания возможных комбинаций перебираемых слов. Например, если задана сильная мутация, то для каждого слова из словаря будет создано несколько сотен аналогов. Например, secret - Secret - s3cr3t - secret123 и т.д. Всего можно задавать три правила для мутации: 'слабо'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

В **Генераторе словарей** можно создавать свои собственные варианты словарей на базе опций первых трех 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

Начиная с версии 4.0 в программе появилась возможность более тонко задавать настройку мутаций в атаке по словарю. Все правила мутации объеденены в 16 основных групп. Вы можете задавать один из трех уровней мутации или отключать ее отдельно для каждой группы.



Smart mutation

Weak - less number of smart mutations and greater verification speed; Strong - for greater number of mutations, to the prejudice of the speed, and the happy medium, Default option. The smart mutation is based upon 150 social rules and combinations. Be careful, mutating even a single word may take quite significant time !

Read more about Dictionary attack

Mutation level

○ Disabled ○ Weak (fast)
○ Normal (slow) ○ Strong (very slow)
● Custom

Character case	Weak (fast)	Character swap	Normal (slow)
Digits append/prepend	Weak (fast)	Character duplicate	Normal (slow)
Head and tail	Normal (slow)	Insert delimiters	Weak (fast)
L33t	Normal (slow)	Add dates	Weak (fast)
Abbreviations	Normal (slow)	Oem convertion	Disabled
Dups and revers	Weak (fast)	Word shift	Disabled
Vowels and consonants	Normal (slow)	Character substitution	Normal (slow)
Character skip	Normal (slow)	Length truncate	Weak (fast)

Например, можно отключить OEM мутации, увеличив в два раза скорость перебора в словарной атаке, если вы уверены, что искомый пароль содержит только латинские символы. Ниже дано краткое описание групп мутаций:

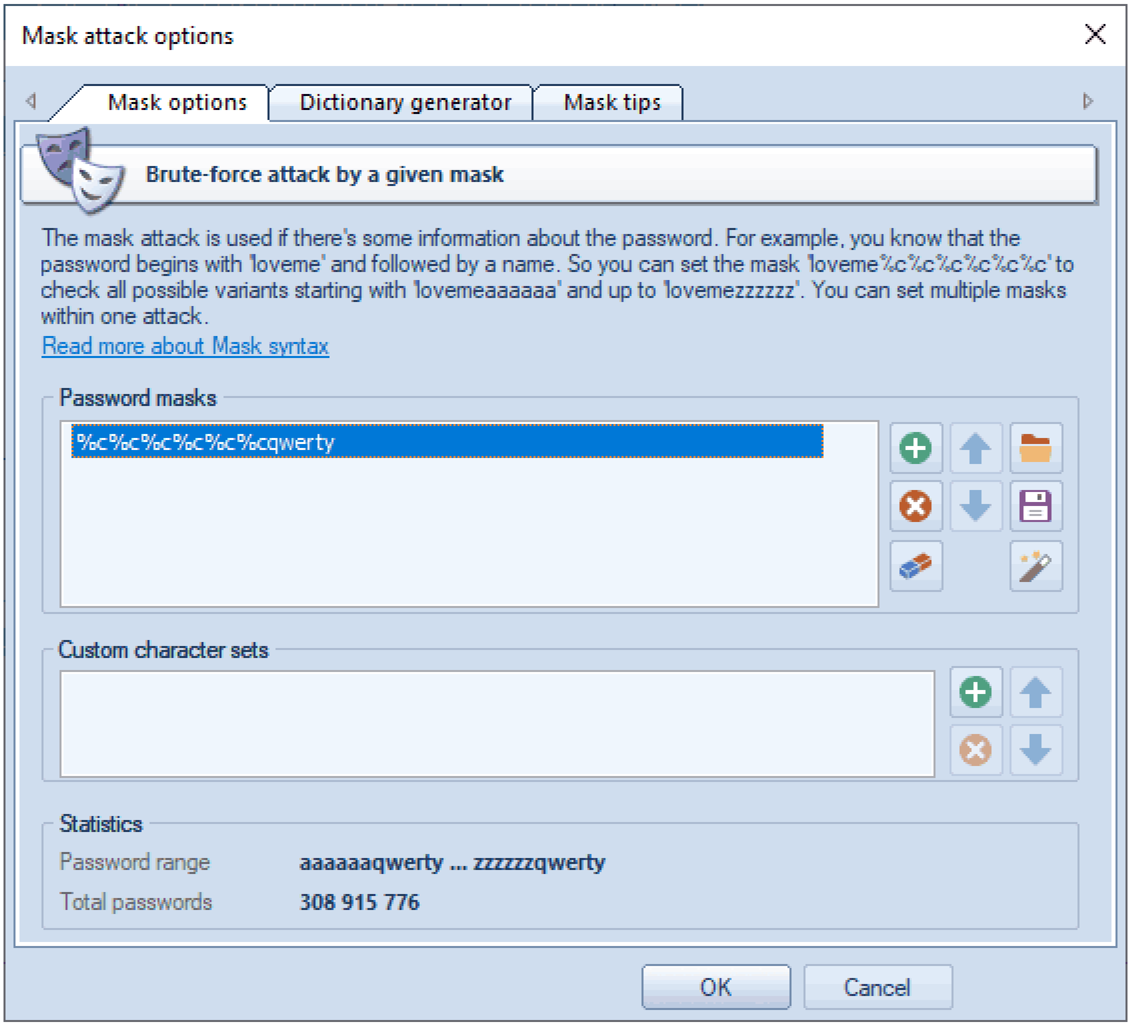
Имя группы	Описание	Примеры (для слова '**password**')	Комментарии
Character case	Проверяет регистр букв в исходном слове.	Password, PassworD, PaSsWoRd	Максимальный (Strong) уровень мутаций НЕ создает всех возможных вариантов регистра букв. Для этой цели можно использовать Гибридную атаку по словаю (см. 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,	#Password#, password12345, 4everPASSWORD, Passwordqwerty	

Имя группы	Описание	Примеры (для слова '**password**')	Комментарии
	абревиатуры, символы, клавиатурные комбинации и т.д.		
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 абревиатруры.	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 **пароль** получится **gfhjkm**.	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.
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'

Имя группы	Описание	Примеры (для слова '**password**')	Комментарии
			может быть заменет 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.



Mask attack options

Brute-force attack by a given mask

The mask attack is used if there's some information about the password. For example, you know that the password begins with 'loveme' and followed by a name. So you can set the mask 'loveme%c%c%c%c%c%c' to check all possible variants starting with 'lovemeaaaaaa' and up to 'lovemezzzzzz'. You can set multiple masks within one attack.

Read more about Mask syntax

Password masks

%c%c%c%c%c%cqwerty

Custom character sets

Statistics

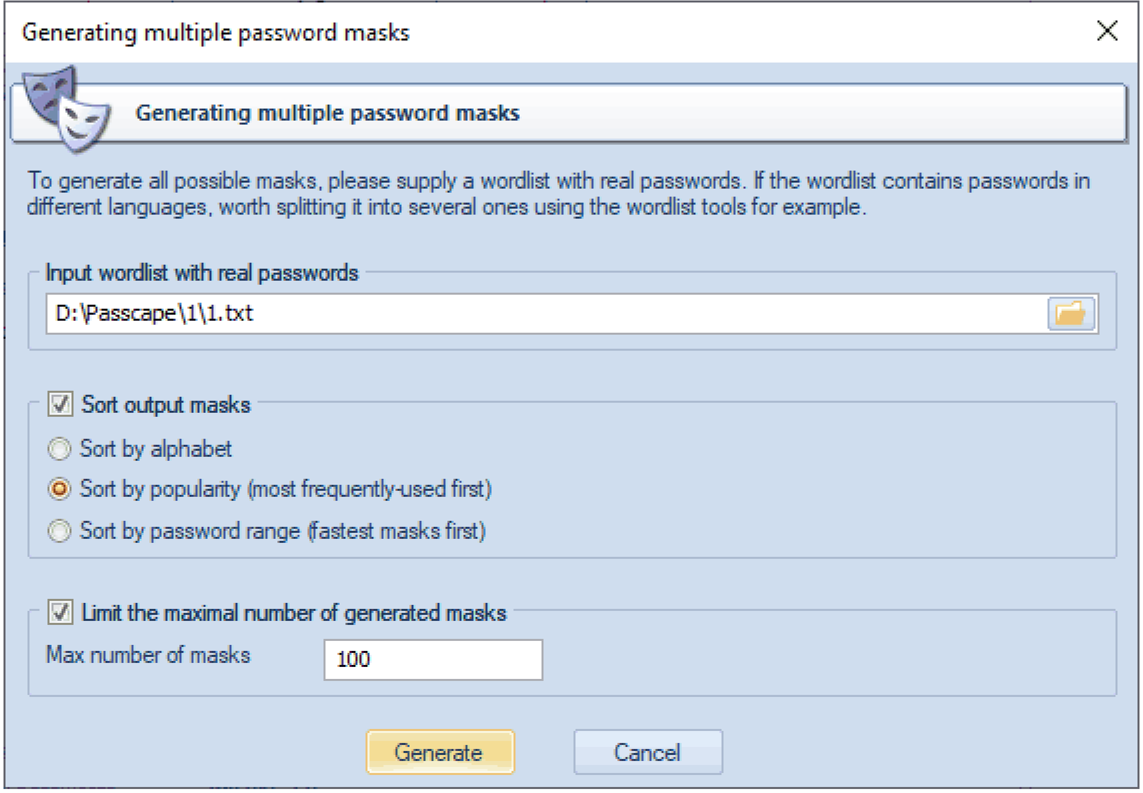
Password range aaaaaaqwerty ... zzzzzzqwerty

Total passwords 308 915 776

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.

Группа опций Password Masks служит для задания масок, по которым будут перебираться пароли. Как правило, если известна часть пароля, достаточно задать одну единственную маску. При выделении маски, группа "статистика" показывает диапазон перебираемых символов и количество паролей, генерируемых при помощи этой маски. Свои маски можно сохранять на диске. Программа позволяет также генерировать словарь по заданной маске или нескольким маскам, однако эта опция доступна не во всех редакциях.

Утилита для генерации масок по словарю с паролями заслуживает отдельного упоминания. Предположим что у вас есть словарь расшифрованных паролей и вы хотели бы сгенерировать шаблоны масок по этим паролям. Нет ничего проще. Запускаем генератор масок и задаем исходный словарь с паролями. Можно отсортировать полученные таким образом маски по алфавиту, популярности или диапазону перебора (вначале самые быстрые).


Generating multiple password masks
Generating multiple password masks
Generate
Cancel

To generate all possible masks, please supply a wordlist with real passwords. If the wordlist contains passwords in different languages, worth splitting it into several ones using the wordlist tools for example.

Input wordlist with real passwords: D:\Passcape\1\1.txt

☑ Sort output masks

○ Sort by alphabet

● Sort by popularity (most frequently-used first)

○ Sort by password range (fastest masks first)

☑ Limit the maximal number of generated masks

Max number of masks: 100

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). Windows Password Recovery 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.

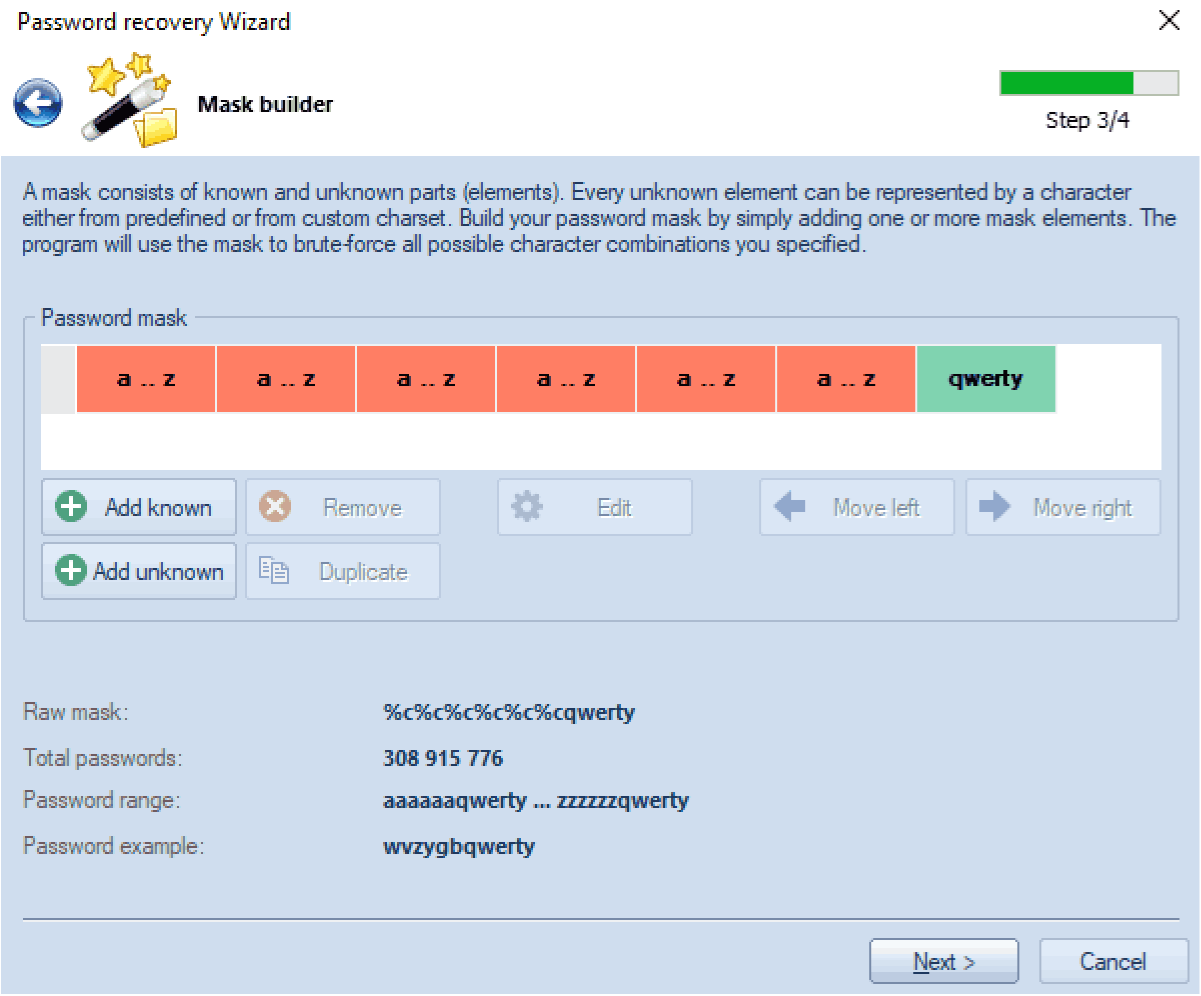
- **%@** малый набор специальных символов (!@#$%^&*()-_+= space). Всего 15 символов.
- **%?** набор всех печатных символов с ASCII кодами от 32 до 127.
- **%*** набор всех ASCII символов с кодами от 1 до 255.
- **%d** одна цифра (0..9).
- **%d(x-y)** последовательность чисел от x до y включительно.
- **%r(x-y)** свой набор символов с последовательными UNICODE кодами от x до y
- **%r(x1-y1,x2-y2...xn-yn)** набор из нескольких непересекающихся последовательностей UNICODE символов.
- **%[1..9]** символ из пользовательского набора 1..9
- **%[1..9](min-max)** пользовательский набор символов переменной длины (от min до max) для перебора. Всего можно задать своих собственных 9 наборов.
- **%%** статический символ %

Примеры:
test%d - парольный ряд test0 .. test9, всего 10 комбинаций
test%d(1980-2007) - test1980 .. test2007, 28 паролей
test%r(0x0600-0x06ff) - test_ .. test_, 256 паролей с арабским символом на конце
%#test%# - _test_..~test~, 1089 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

Перейдя во вторую вкладку настроек, вы можете создать свой собственный словарь по заданной маске и сохранить его на диск. Однако эта опция доступна только в Advanced редакции программы.

Описание синтаксиса и примеры можно посмотреть в третьей вкладке опций.

Если вы чувствуете себя потерянным и уставшим от масочной дребедени, то лучше используйте Mask Builder (в Мастере восстановления паролей), который имеет более удобный графический интерфейс.



A mask consists of known and unknown parts (elements). Every unknown element can be represented by a character either from predefined or from custom charset. Build your password mask by simply adding one or more mask elements. The program will use the mask to brute-force all possible character combinations you specified.

Raw mask: %c%c%c%c%c%cqwerty

Total passwords: 308 915 776

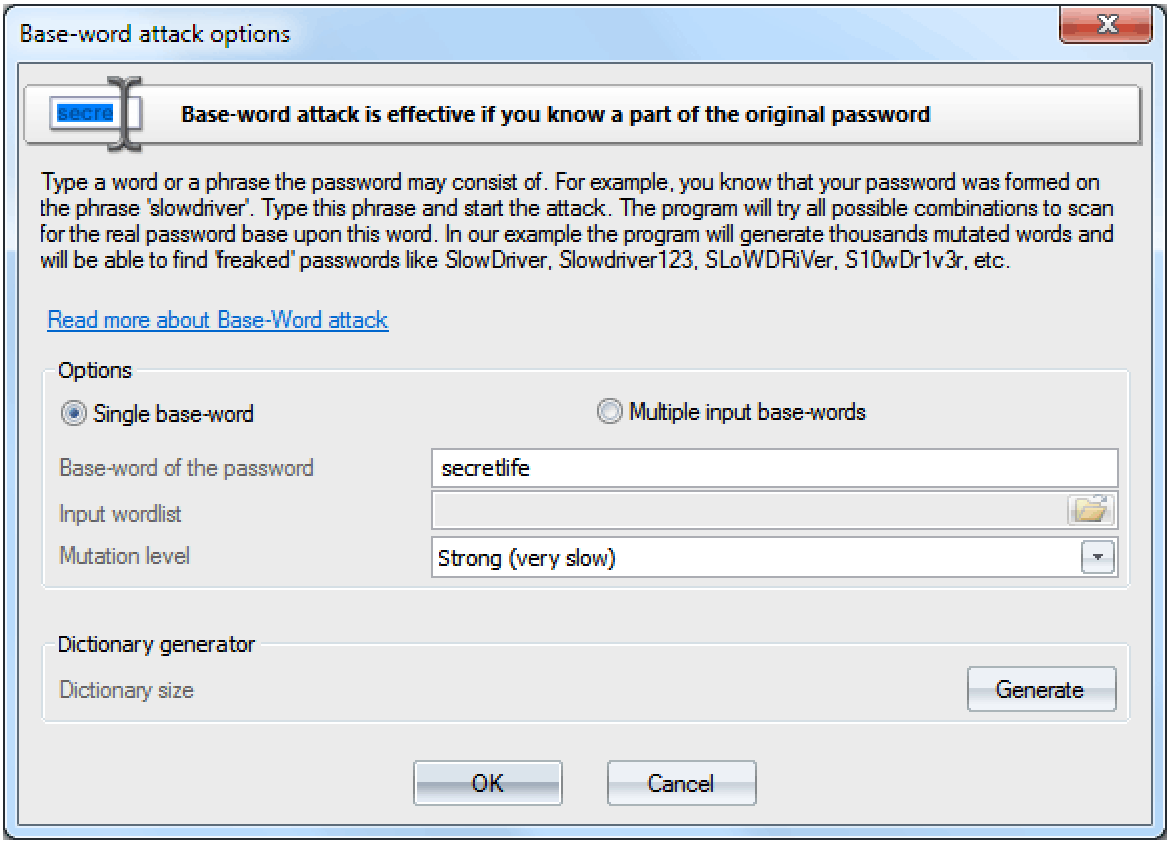
Password range: aaaaaaqwerty ... zzzzzzqwerty

Password example: wvzygbqwerty

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 15 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.


Base-word attack options
secre
Base-word attack is effective if you know a part of the original password

Type a word or a phrase the password may consist of. For example, you know that your password was formed on the phrase 'slowdriver'. Type this phrase and start the attack. The program will try all possible combinations to scan for the real password base upon this word. In our example the program will generate thousands mutated words and will be able to find 'freaked' passwords like SlowDriver, Slowdriver123, SLoWDRiVer, S10wDr1v3r, etc.

Read more about Base-Word attack

Options

● Single base-word ○ Multiple input base-words

Base-word of the password: secretlife

Input wordlist:

Mutation level: Strong (very slow)

Dictionary generator

Dictionary size

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).

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

Начиная с версии Windows Password Recovery 9.5, теперь можно задавать режим множества исходных слов. Этот режим работает практически также, как и словарная атака с максимальным уровнем мутации. Но в отличие от нее, генерируется намного больше возможных комбинаций слов, даже если установлен самый слабый уровень мутаций атаки по ключевому слову. В определенных ситуациях это может быть довольно критично.

2.8.2.8 Комбинированная Атака по Словарям

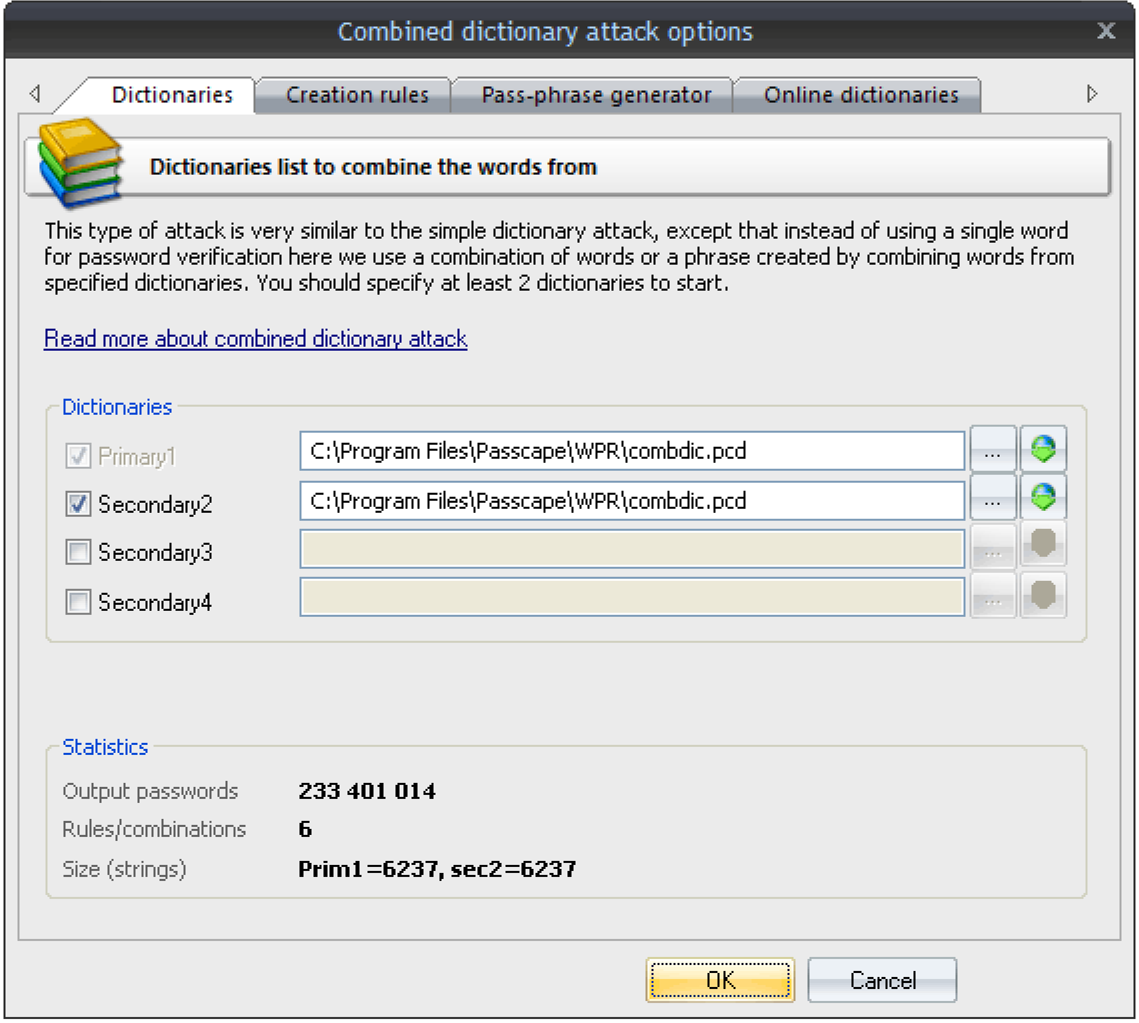
Комбинированная атака по словарям (разработана в Passcape Software) - предназначена для поиска паролей, состоящих из 2,3 или даже 4 слов. Этот вид атаки на сложные и составные пароли очень похож на простую атаку по словарю, за тем лишь исключением, что при проверке пароля используется не одиночное слово, а сочетание слов или фраза, которая создается путем комбинирования слов из заданных словарей. Для ее 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 определенный 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.

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 Passscape.

Словари



Combined dictionary attack options

Dictionaries list to combine the words from

This type of attack is very similar to the simple dictionary attack, except that instead of using a single word for password verification here we use a combination of words or a phrase created by combining words from specified dictionaries. You should specify at least 2 dictionaries to start.

Read more about combined dictionary attack

Dictionaries

☑ Primary1 C:\Program Files\Passcape\WPR\combdic.pcd

☑ Secondary2 C:\Program Files\Passcape\WPR\combdic.pcd

☐ Secondary3

☐ Secondary4

Statistics

Output passwords	233 401 014
Rules/combinations	6
Size (strings)	Prim1=6237, sec2=6237

Алгоритм работы комбинированной атаки довольно прост. Например, если вы задали два словаря, то пароли будут создаваться следующим образом: берется 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.

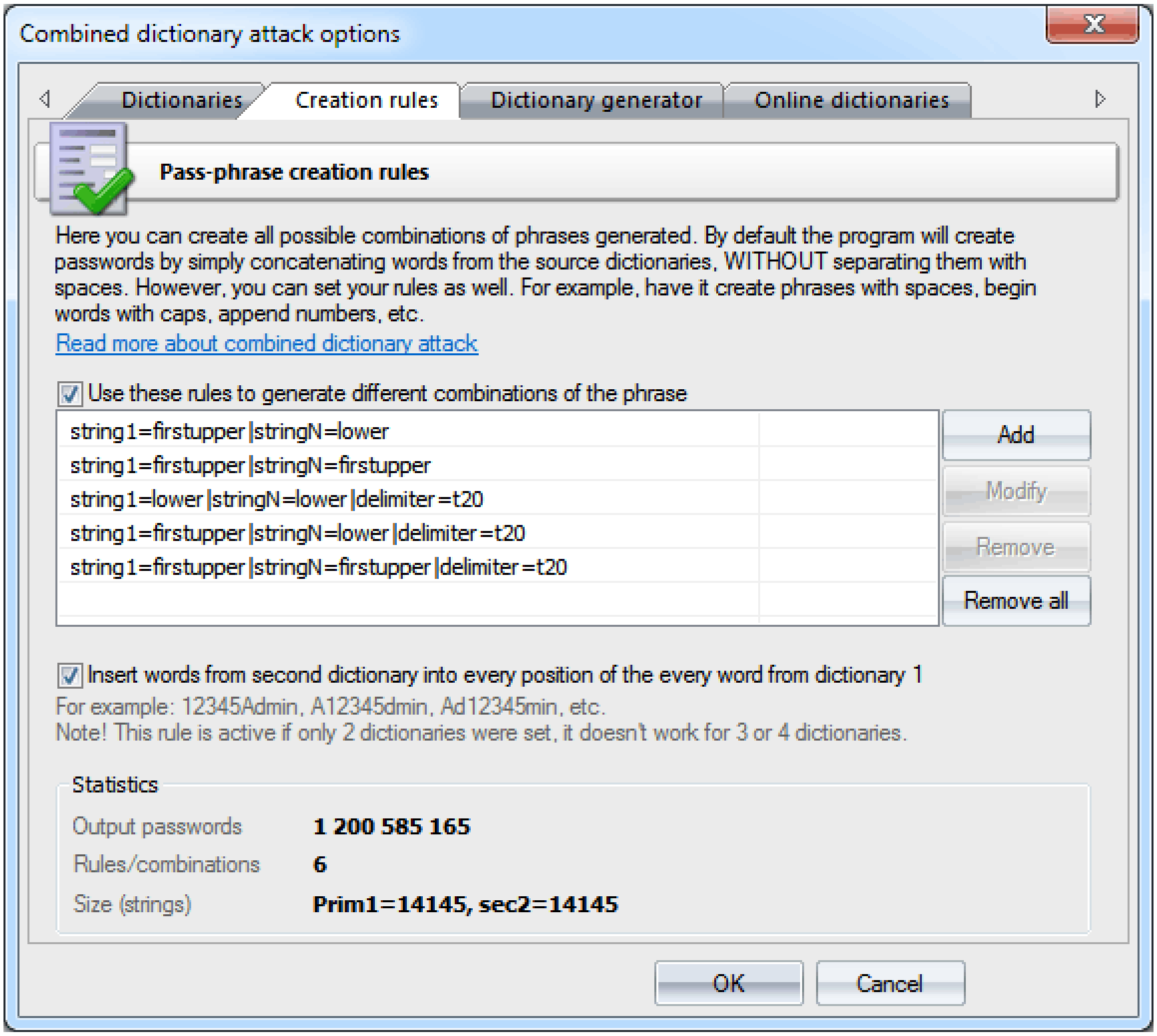
Чтобы понять, как работает комбинированная атака, давайте рассмотрим пару примеров генерации фраз с использованием в первом случае, одного и того же словаря, а во втором случае - двух разных.

1. Предположим, у нас есть один словарь с тремя словами: action, bad и computer. Задаем 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 трех 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".

Пример простой, но показательный. Основная мысль заключается в том, 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



Pass-phrase creation rules

Here you can create all possible combinations of phrases generated. By default the program will create passwords by simply concatenating words from the source dictionaries, WITHOUT separating them with spaces. However, you can set your rules as well. For example, have it create phrases with spaces, begin words with caps, append numbers, etc.

Read more about combined dictionary attack

☑ Use these rules to generate different combinations of the phrase

```
string1=firstupper|stringN=lower
string1=firstupper|stringN=firstupper
string1=lower|stringN=lower|delimiter=t20
string1=firstupper|stringN=lower|delimiter=t20
string1=firstupper|stringN=firstupper|delimiter=t20
```

☑ Insert words from second dictionary into every position of the every word from dictionary 1

For example: 12345Admin, A12345dmin, Ad12345min, etc.
Note! This rule is active if only 2 dictionaries were set, it doesn't work for 3 or 4 dictionaries.

Statistics

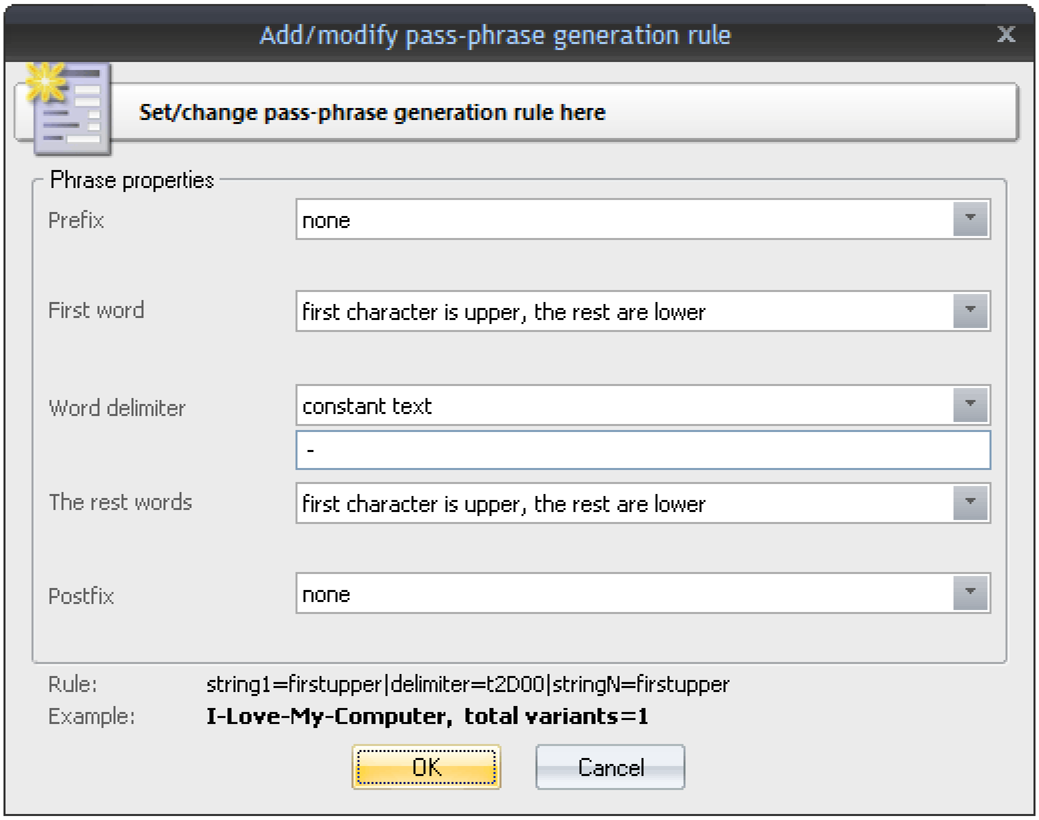
Output passwords	**1 200 585 165**
Rules/combinations	**6**
Size (strings)	**Prim1=14145, sec2=14145**

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 создает пароли путем 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.


Add/modify pass-phrase generation rule
Set/change pass-phrase generation rule here
Phrase properties
OK
Cancel

Prefix: none

First word: first character is upper, the rest are lower

Word delimiter: constant text

-

The rest words: first character is upper, the rest are lower

Postfix: none

Rule: string1=firstupper|delimiter=t2D00|stringN=firstupper

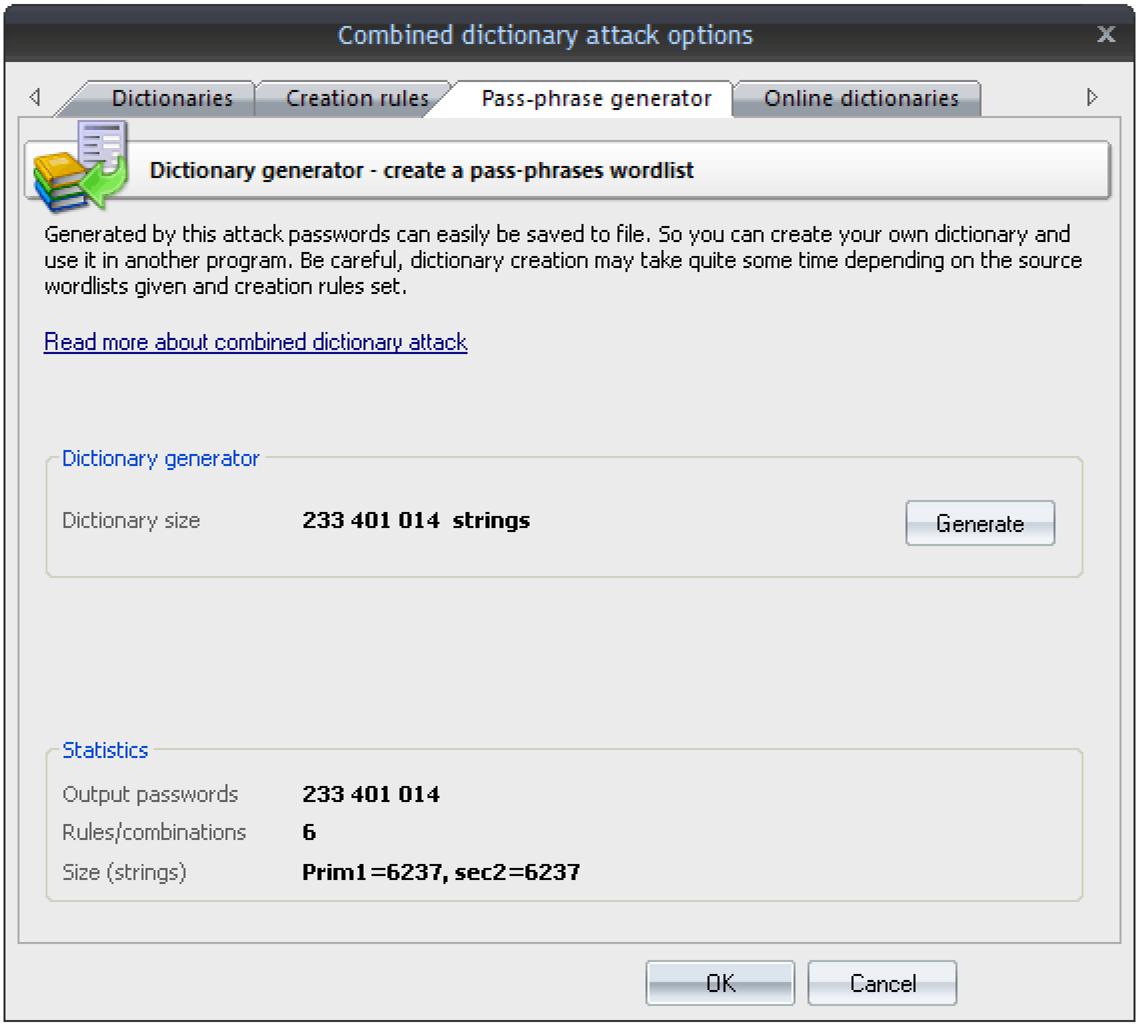
Example: **I-Love-My-Computer, total variants=1**

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



Combined dictionary attack options
Dictionaries
Creation rules
Pass-phrase generator
Online dictionaries
Dictionary generator - create a pass-phrases wordlist

Generated by this attack passwords can easily be saved to file. So you can create your own dictionary and use it in another program. Be careful, dictionary creation may take quite some time depending on the source wordlists given and creation rules set.

Read more about combined dictionary attack

Dictionary generator

Dictionary size 233 401 014 strings

Statistics

Output passwords 233 401 014
Rules/combinations 6
Size (strings) Prim1=6237, sec2=6237

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.

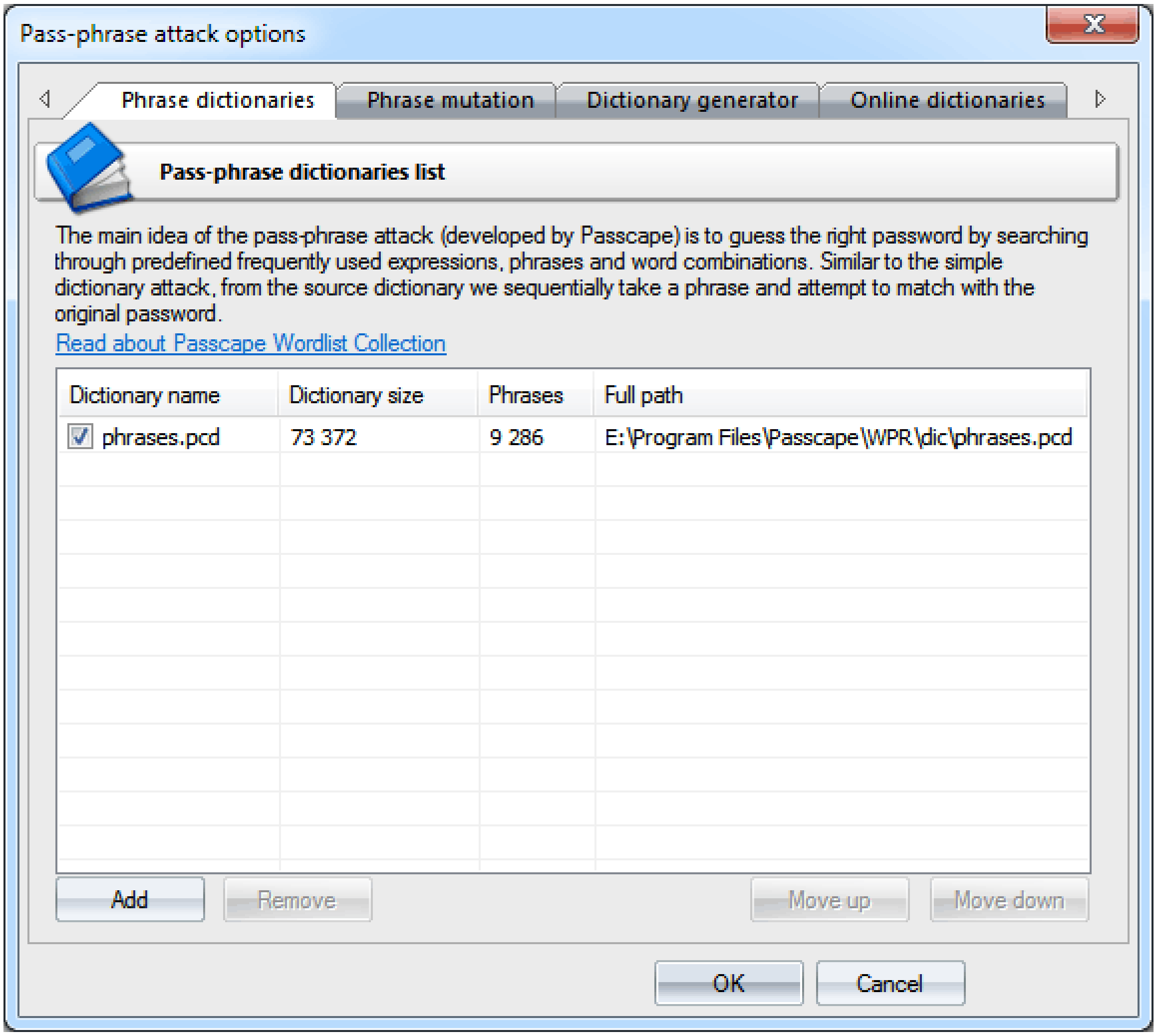
Атака по фразе (разработана в Passcape Software) во многом схожа с простой словарной атакой за тем лишь исключением, что поиск паролей осуществляется не пословно, а пофразно. Подобно атаке по словарю, из исходного словаря поочередно берутся фразы и проверяются на предмет совпадения с исходным паролем.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

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 трудоемкая. Passcape Software дает возможность задействовать целый набор онлайн и оффлайн словарей (всего более 500 Мб), 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 найдете больше нигде в сети!) музыкальные сборники фраз. Есть также библейский сборник, фразы из кино, крылатые и латинские выражения и т.д.

Словари с фразами



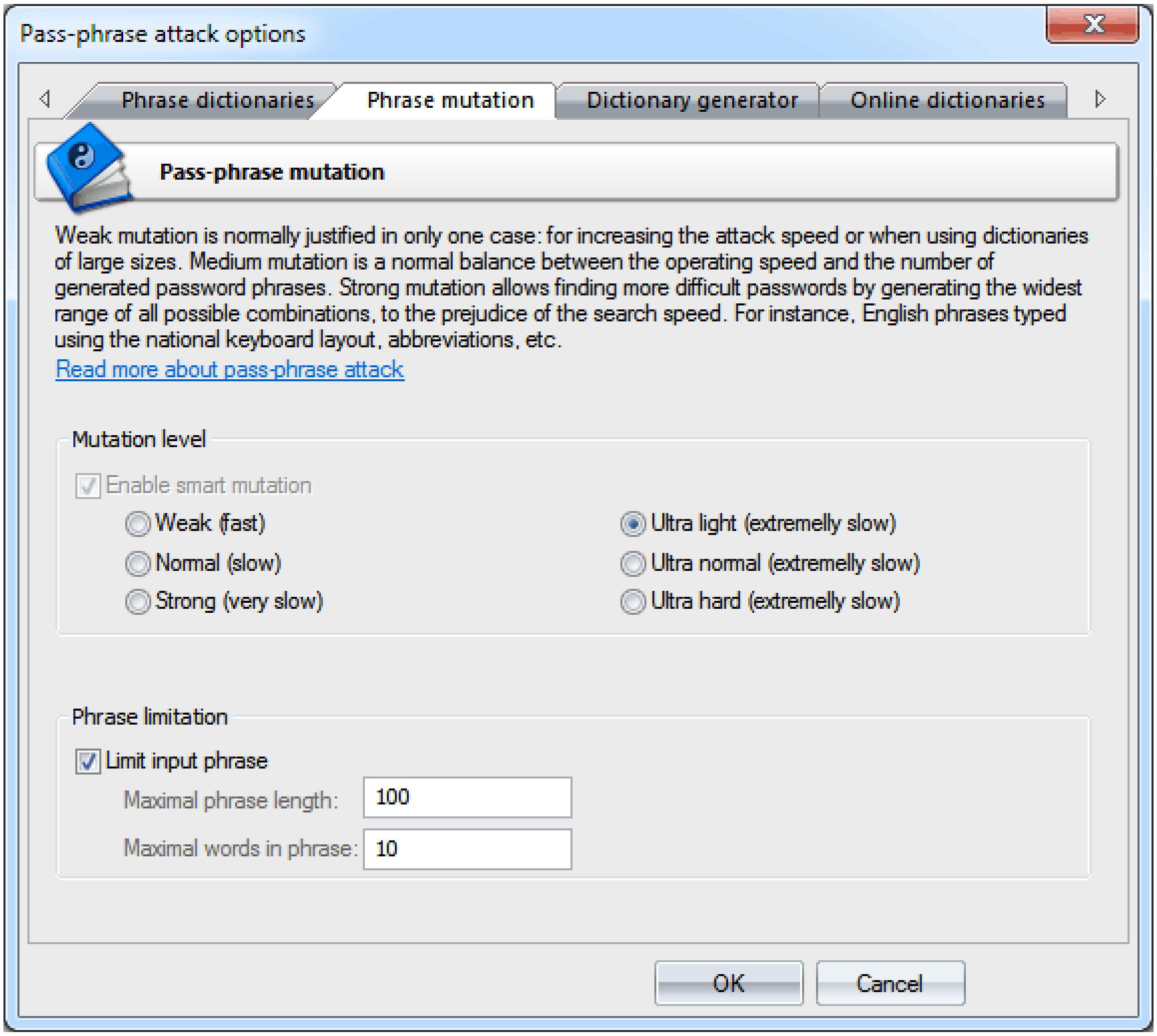
The main idea of the pass-phrase attack (developed by Passcape) is to guess the right password by searching through predefined frequently used expressions, phrases and word combinations. Similar to the simple dictionary attack, from the source dictionary we sequentially take a phrase and attempt to match with the original password.

Read about Passcape Wordlist Collection

Dictionary name	Dictionary size	Phrases	Full path
☑ phrases.pcd	73 372	9 286	E:\Program Files\Passcape\WPR\dic\phrases.pcd

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

Мутация фраз



Weak mutation is normally justified in only one case: for increasing the attack speed or when using dictionaries of large sizes. Medium mutation is a normal balance between the operating speed and the number of generated password phrases. Strong mutation allows finding more difficult passwords by generating the widest range of all possible combinations, to the prejudice of the search speed. For instance, English phrases typed using the national keyboard layout, abbreviations, etc.

Read more about pass-phrase attack

Mutation level

☑ Enable smart mutation

○ Weak (fast) ● Ultra light (extremelly slow)

○ Normal (slow) ○ Ultra normal (extremelly slow)

○ Strong (very slow) ○ Ultra hard (extremelly slow)

Phrase limitation

☑ Limit input phrase

Maximal phrase length: 100

Maximal words in phrase: 10

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. Например, английские фразы, набранные в национальной раскладке клавиатуры, аббревиатуры и т.д.

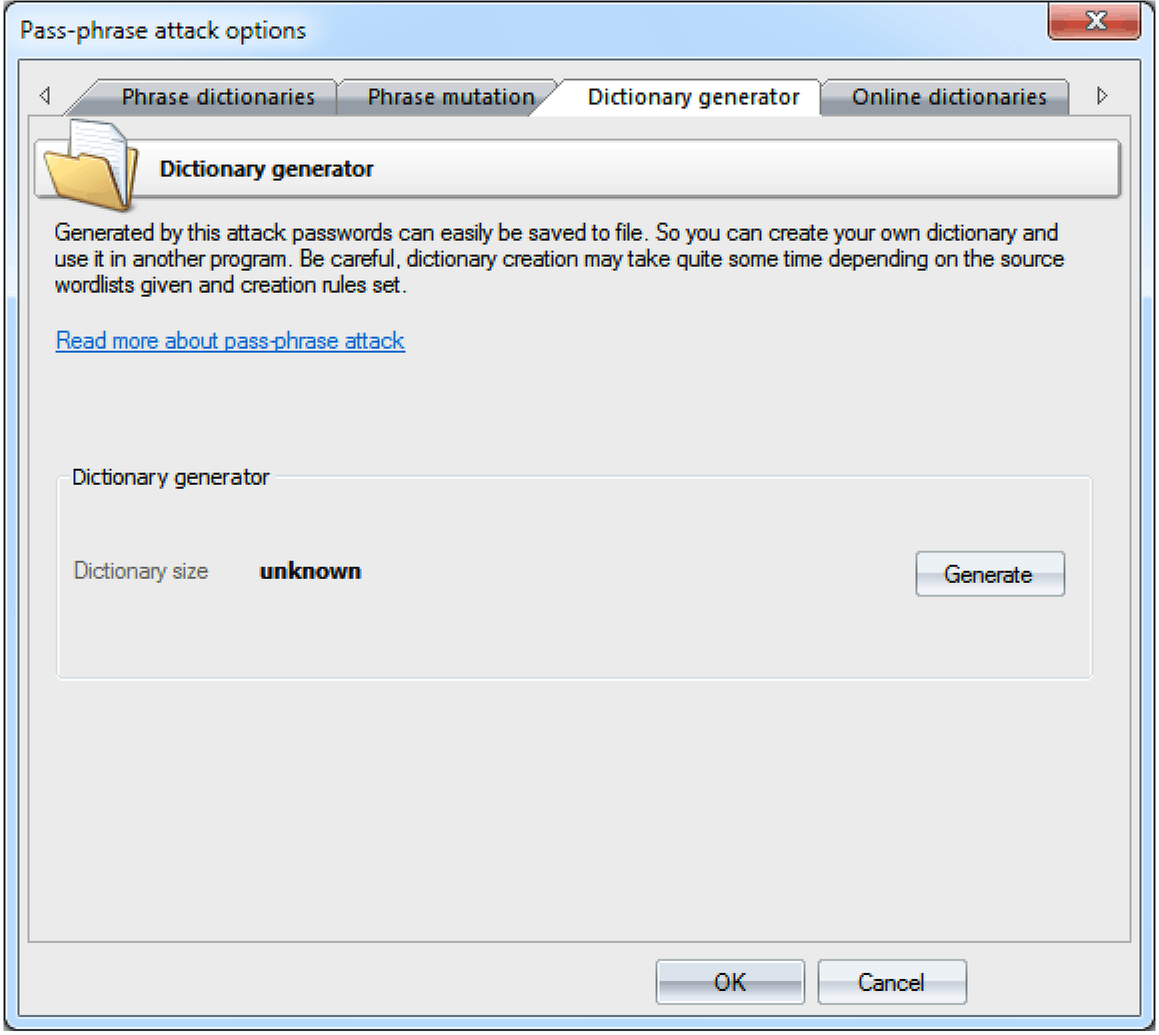
Различия в уровнях мутации:

- 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).
- 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 100 символами и 10 словами.

Генератор словарей

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



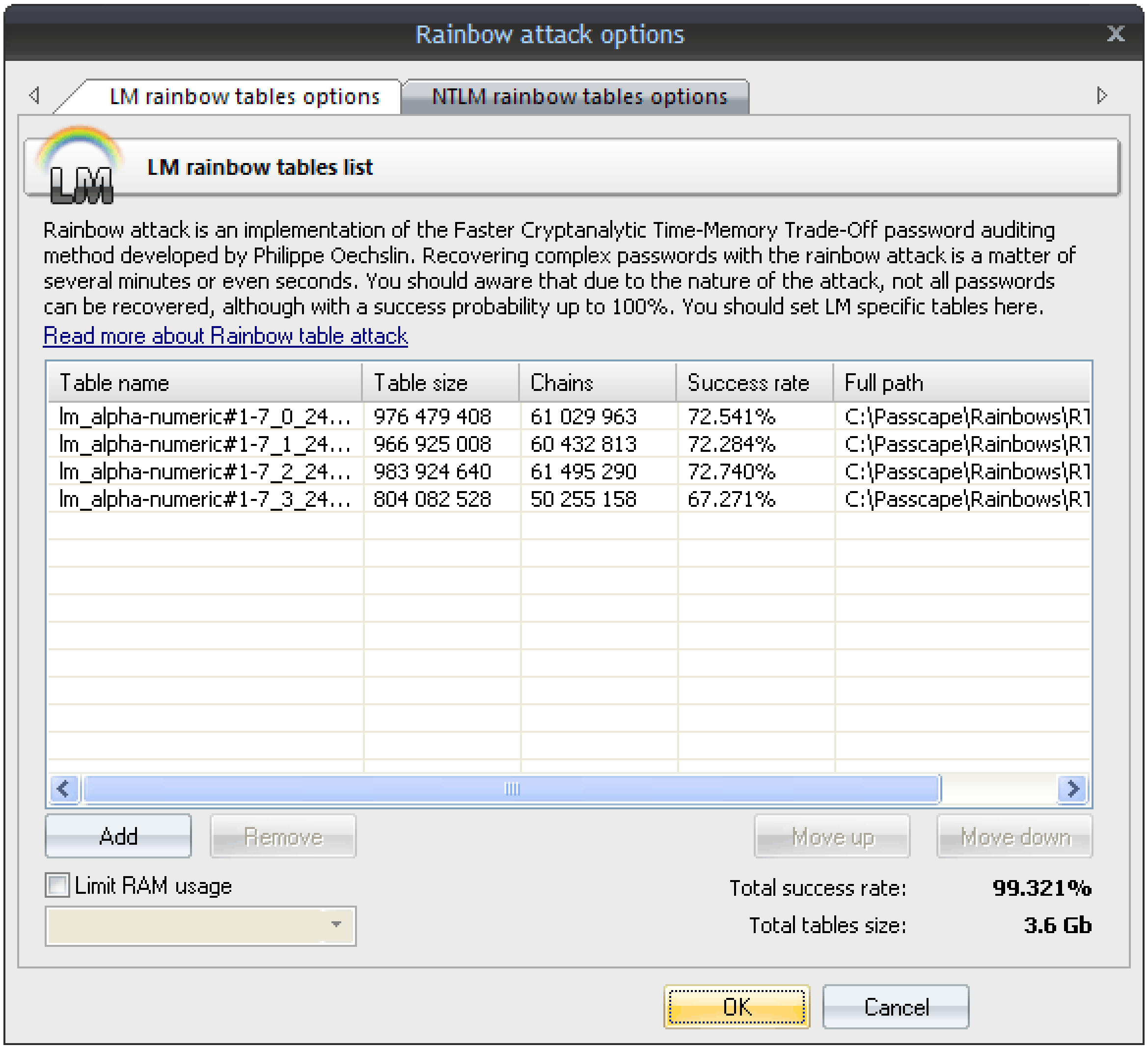
Generated by this attack passwords can easily be saved to file. So you can create your own dictionary and use it in another program. Be careful, dictionary creation may take quite some time depending on the source wordlists given and creation rules set.

Dictionary size unknown

2.8.2.10 Атака по Предвычисленным Таблицам

Радужная таблица (англ. rainbow table) - специальный вариант таблиц поиска, использующий механизм уменьшения времени поиска за счет увеличения занимаемой памяти или time-memory tradeoff. Радужные таблицы используются для вскрытия паролей, преобразованных при помощи необратимой хеш-функции, например, паролей Windows.

Является довольно продвинутым инструментом при аудите паролей. Данный метод был разработан Philippe Oechslin для быстрого поиска паролей по предвычисленным таблицам. Достаточно лишь сказать, что искомый пароль может быт найден за минуты или даже секунды.



Rainbow attack options

Rainbow attack is an implementation of the Faster Cryptanalytic Time-Memory Trade-Off password auditing method developed by Philippe Oechslin. Recovering complex passwords with the rainbow attack is a matter of several minutes or even seconds. You should aware that due to the nature of the attack, not all passwords can be recovered, although with a success probability up to 100%. You should set LM specific tables here.

Read more about Rainbow table attack

Table name	Table size	Chains	Success rate	Full path
lm_alpha-numeric#1-7_0_24...	976 479 408	61 029 963	72.541%	C:\Passcape\Rainbows\R1
lm_alpha-numeric#1-7_1_24...	966 925 008	60 432 813	72.284%	C:\Passcape\Rainbows\R1
lm_alpha-numeric#1-7_2_24...	983 924 640	61 495 290	72.740%	C:\Passcape\Rainbows\R1
lm_alpha-numeric#1-7_3_24...	804 082 528	50 255 158	67.271%	C:\Passcape\Rainbows\R1

□ Limit RAM usage

Total success rate: **99.321%**

Total tables size: **3.6 Gb**

Программа поддерживает стандартные *.rt, а также индексные *.rti и гибридные таблицы, имеется поддержка многопоточности.

Следует также упомянуть, что во время атаки по таблицам не все пароли могут быть найдены, но с вероятностью близкой к 100%, в зависимости от самих таблиц.

Таблицы могут взламывать только ту хеш-функцию, для которой они создавались, то есть таблицы для LM могут взломать только LM хеш.

Опции атаки позволяют ограничить объем используемой памяти для старых компьютеров (атака подразумевает использование большого объема оперативной памяти для вычислений).

2.8.2.11 Гибридная Атака по Словарю

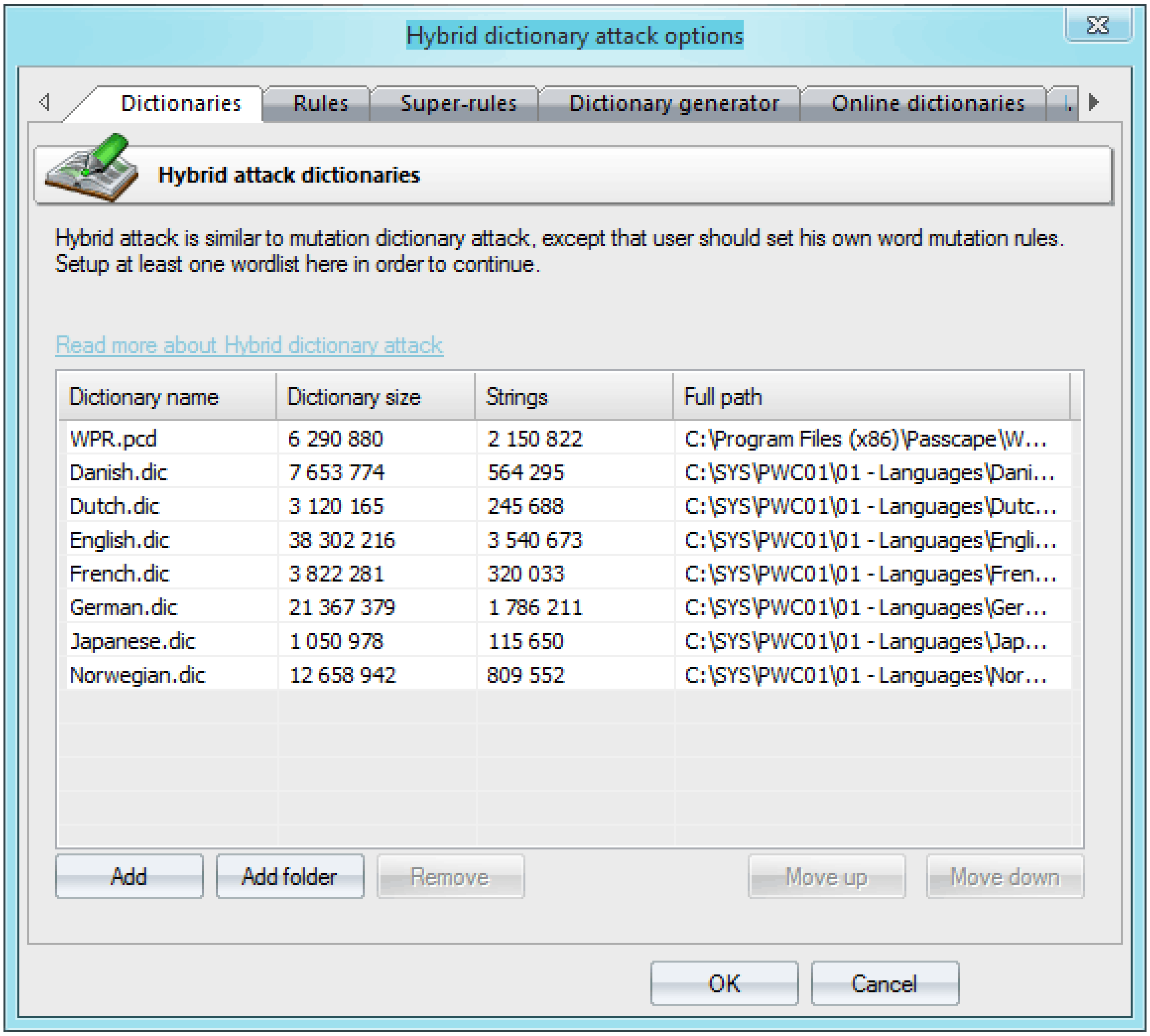
Гибридная атака по словарю - это разновидность простой словарной атаки. Однако в отличие от последней, гибридная атака позволяет пользователю задавать свои собственные правила мутации (вариации) слов и проверять их в качестве исходного пароля. Например, можно перевести первую букву проверяемого пароля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

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.



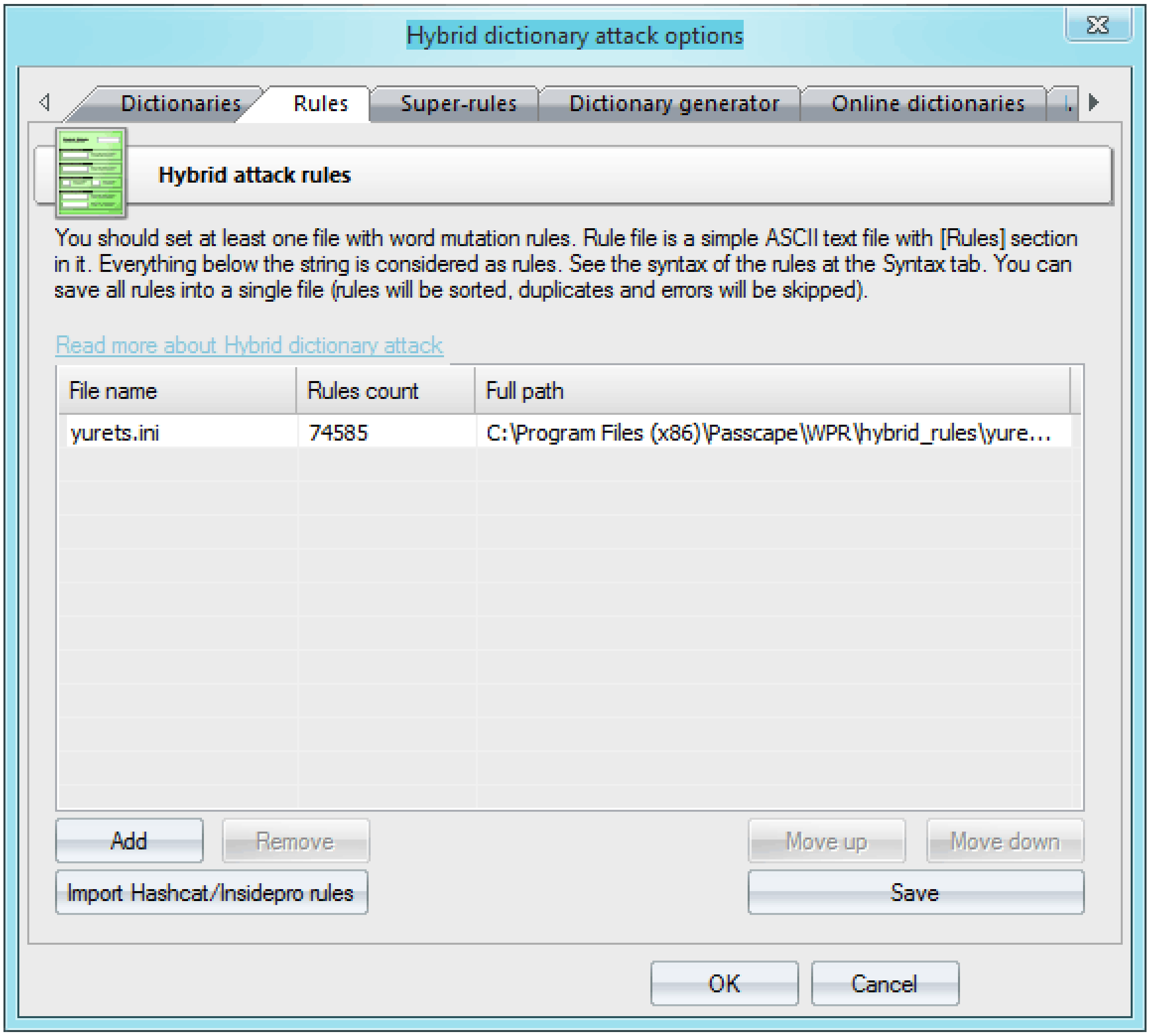
Hybrid attack dictionaries

Hybrid attack is similar to mutation dictionary attack, except that user should set his own word mutation rules. Setup at least one wordlist here in order to continue.

Read more about Hybrid dictionary attack

Dictionary name	Dictionary size	Strings	Full path
WPR.pcd	6 290 880	2 150 822	C:\Program Files (x86)\Passcape\W...
Danish.dic	7 653 774	564 295	C:\SYS\PWC01\01 - Languages\Dani...
Dutch.dic	3 120 165	245 688	C:\SYS\PWC01\01 - Languages\Dutc...
English.dic	38 302 216	3 540 673	C:\SYS\PWC01\01 - Languages\Engli...
French.dic	3 822 281	320 033	C:\SYS\PWC01\01 - Languages\Fren...
German.dic	21 367 379	1 786 211	C:\SYS\PWC01\01 - Languages\Ger...
Japanese.dic	1 050 978	115 650	C:\SYS\PWC01\01 - Languages\Jap...
Norwegian.dic	12 658 942	809 552	C:\SYS\PWC01\01 - Languages\Nor...

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 идет до этой сроки, считается комментариями и игнорируется программой. Все, что после, рассматривается как правила. Каждая строка может содержать несколько правил, применяемых к исходному слову. Исключение составляет правило **aN**. Это правило не должно находиться с другими на одной строке. 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.

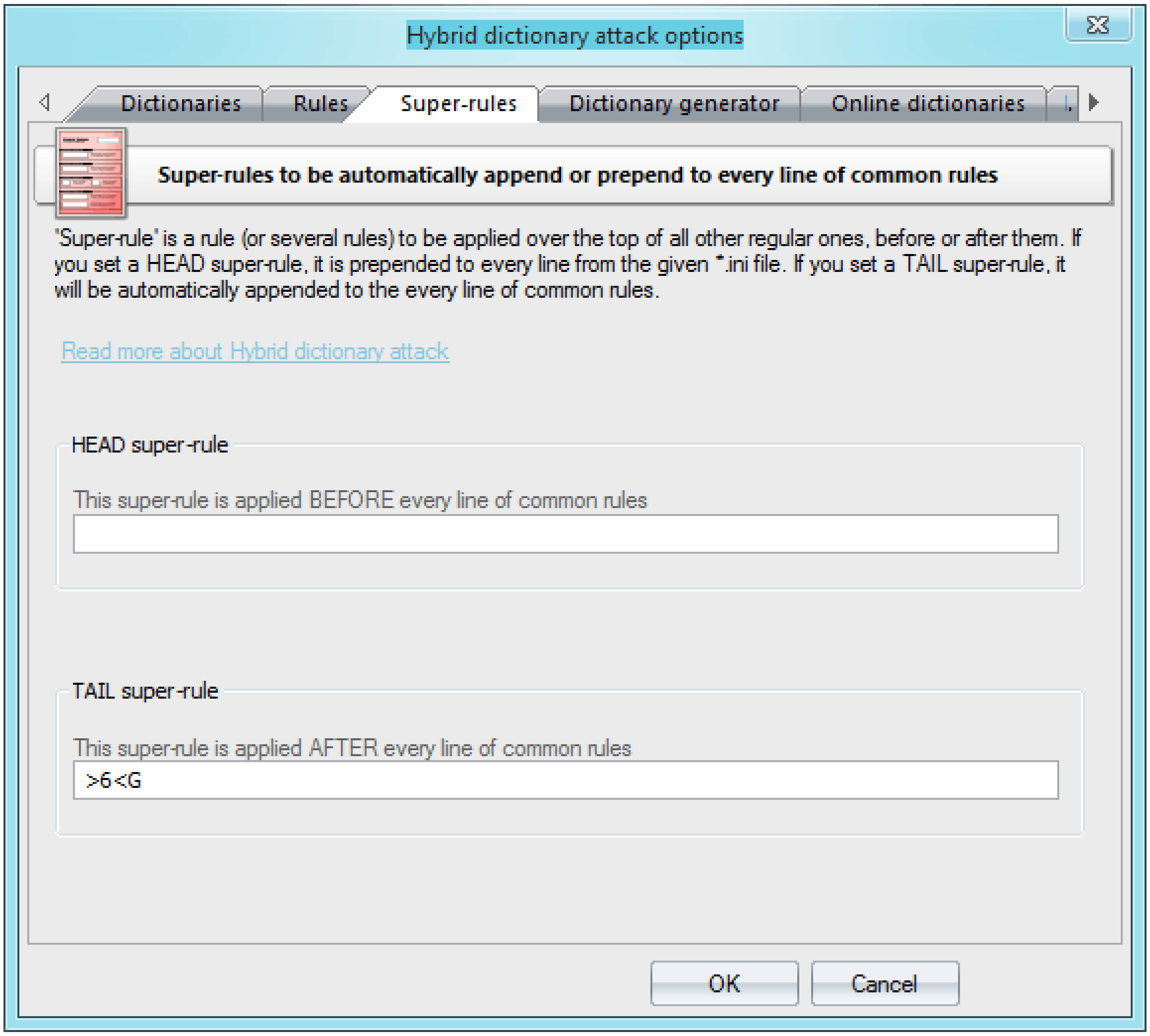


You should set at least one file with word mutation rules. Rule file is a simple ASCII text file with [Rules] section in it. Everything below the string is considered as rules. See the syntax of the rules at the Syntax tab. You can save all rules into a single file (rules will be sorted, duplicates and errors will be skipped).

File name	Rules count	Full path
yurets.ini	74585	C:\Program Files (x86)\Passcape\WPR\hybrid_rules\yure...

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. Еще один пример: если установить начальное супер-правило '>6<G', то до начала обычной мутации будут отклонены все слова меньше 6 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 аккуратны, однако: супер-правило 'aN' может увеличить число генерируемых паролей в сотни или даже тысячи раз!



Super-rules to be automatically append or prepend to every line of common rules

'Super-rule' is a rule (or several rules) to be applied over the top of all other regular ones, before or after them. If you set a HEAD super-rule, it is prepended to every line from the given *.ini file. If you set a TAIL super-rule, it will be automatically appended to the every line of common rules.

Read more about Hybrid dictionary attack

HEAD super-rule

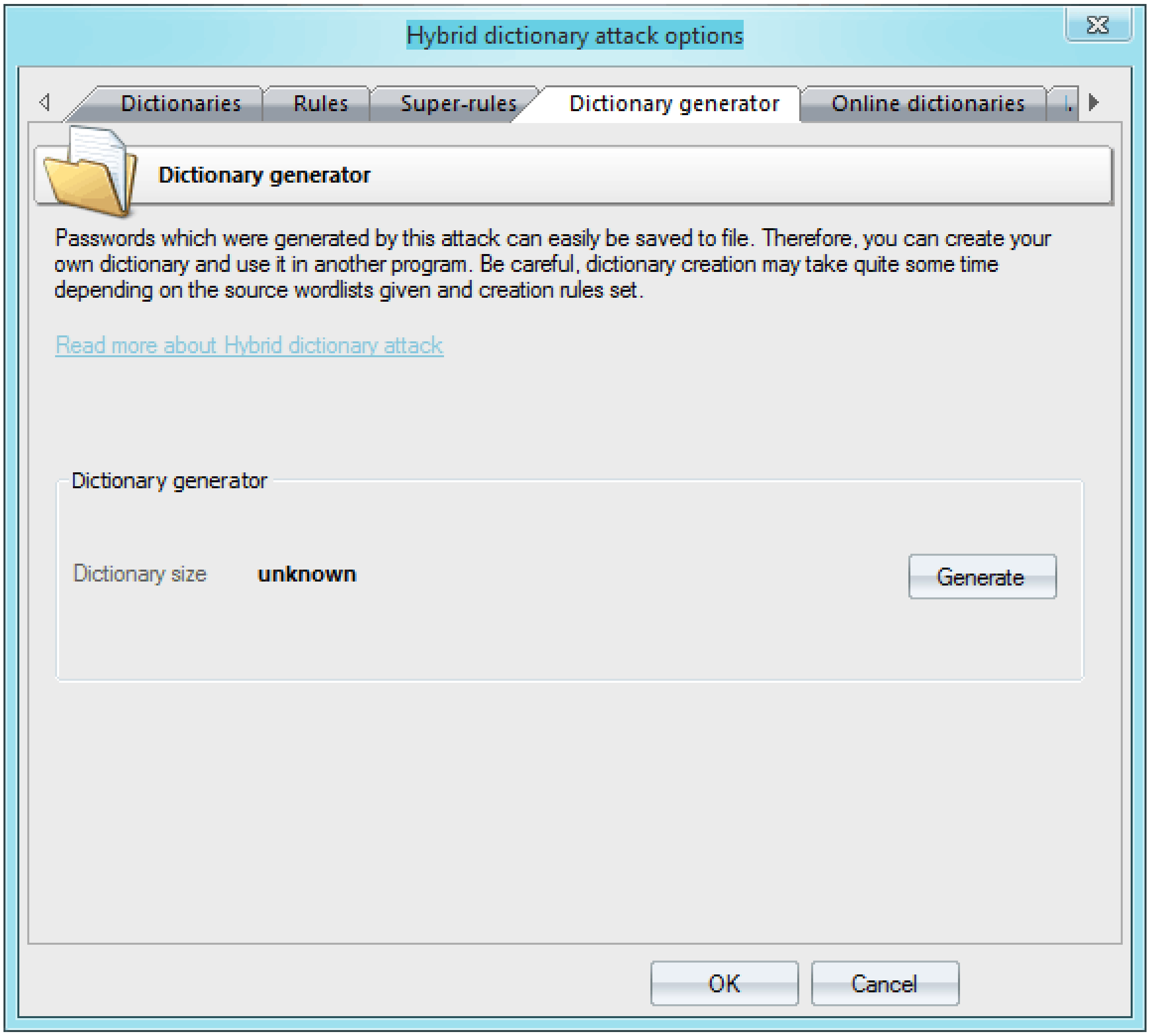
This super-rule is applied BEFORE every line of common rules

TAIL super-rule

This super-rule is applied AFTER every line of common rules

>6<G

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!



Dictionary generator

Passwords which were generated by this attack can easily be saved to file. Therefore, you can create your own dictionary and use it in another program. Be careful, dictionary creation may take quite some time depending on the source wordlists given and creation rules set.

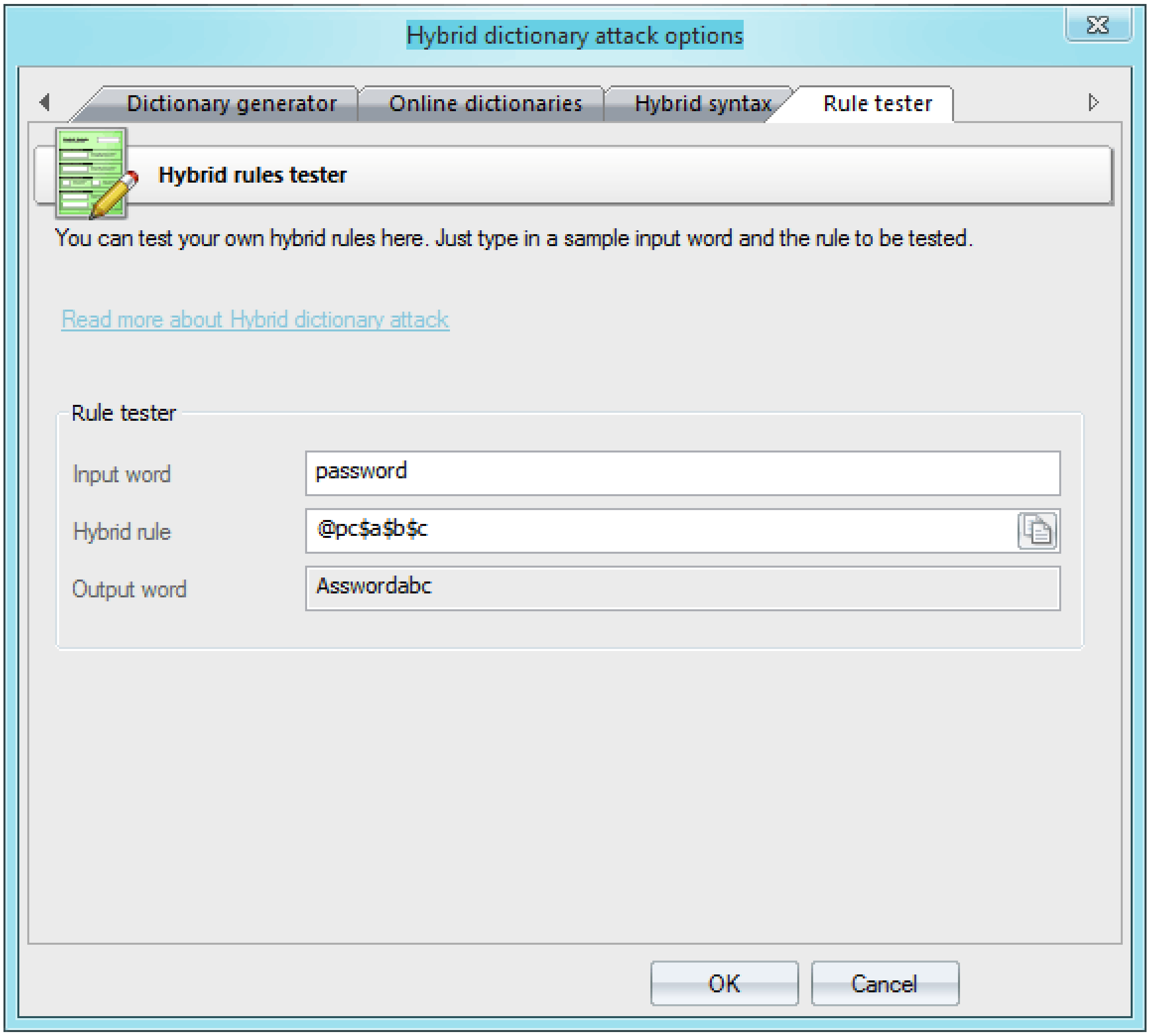
Read more about Hybrid dictionary attack

Dictionary generator

Dictionary size **unknown**

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.



Hybrid rules tester

You can test your own hybrid rules here. Just type in a sample input word and the rule to be tested.

Read more about Hybrid dictionary attack

Rule tester

Input word: password

Hybrid rule: @pc$a$b$c

Output word: Asswordabc

Описание синтаксиса правил гибридной атаки по словарю

Допускается задавать несколько правил на одной строке.
Обработка правил (если их несколько на одной строке) идет 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

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 задает 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	paspasword	Продублировать первые N символов
YN	Y3	password	paswordord	Продублировать последние N символов
zN	z3	password	ppppassword	Дублировать первый символ слова N раз

Правило	Пример	Вход. слово	Выход. слово	Описание правила
ZN	Z3	password	passworddd	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.
RNM+Y	R01+a	password	assword	Удалить символ в позиции N, если символ в позиции M равен Y
RNM-Y	R40-b	password	passord	Удалить символ в позиции N, если символ в позиции M не равен Y

Дополнительно

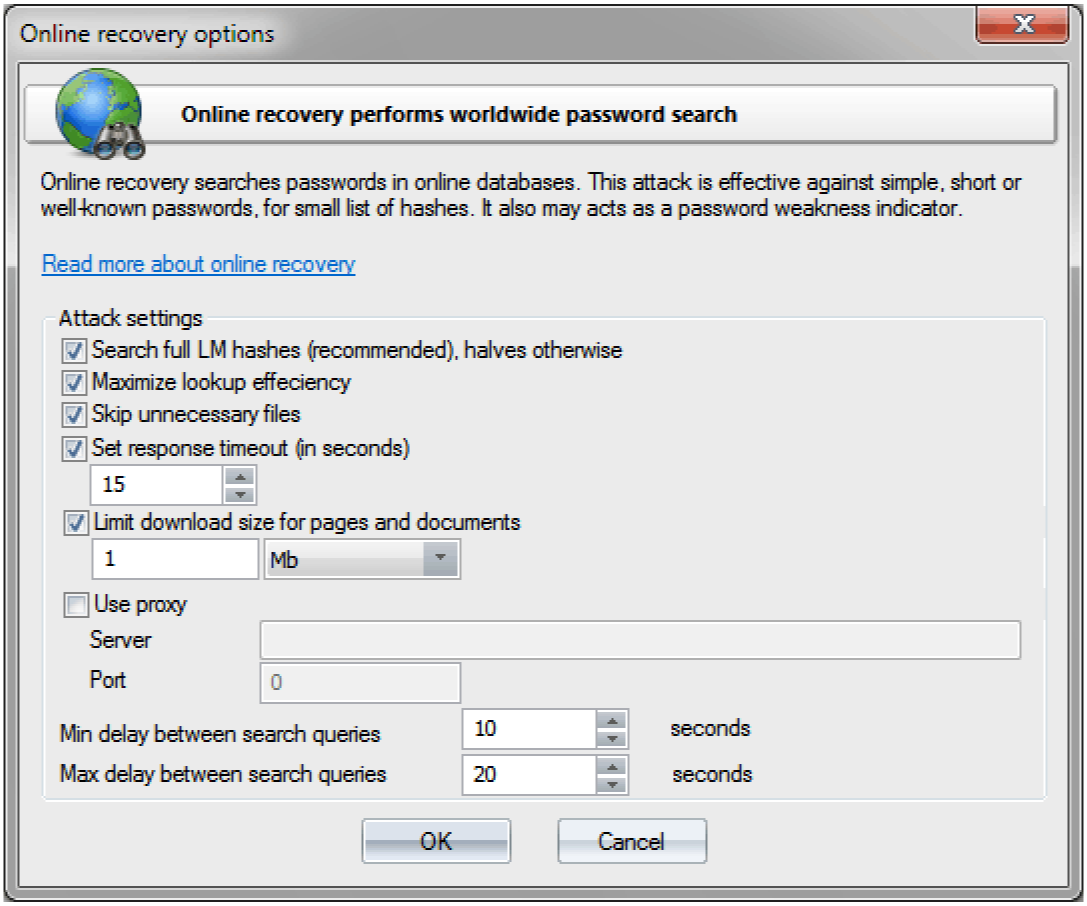
Вместе с дистрибутивом программы поставляется расширенный набор правил мутации паролей:
Файл **hybrid_rules/english_words.ini** содержит набор основных правил для английских паролей.
hybrid_rules/simple_dates.ini - правила с датами, месяцами, временами года и т.д.
hybrid_rules/l33t.ini - правила уродованием 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.

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

2.8.2.12 Онлайн Атака

Онлайн атака (Online recovery) была разработана в Passcape Software и представляет собой улучшенный поиск паролей в Интернете. Для этого программа последовательно для каждого хэша создает специальный запрос в поисковую систему, скачивая найденные файлы с паролем. Онлайн атака довольно медленная, поэтому целесообразно использовать ее на небольшом списке хэшей. Кроме того, найденные пароли, как правило, ограничиваются простыми, словарными и короткими комбинациями. Так или иначе, Онлайн атака бывает довольно полезной. Например, при аудите паролей, как элементарный детектор уязвимости некоторых систем.



Online recovery options

Online recovery performs worldwide password search

Online recovery searches passwords in online databases. This attack is effective against simple, short or well-known passwords, for small list of hashes. It also may acts as a password weakness indicator.

Read more about online recovery

Attack settings

☑ Search full LM hashes (recommended), halves otherwise
☑ Maximize lookup effeciency
☑ Skip unnecessary files
☑ Set response timeout (in seconds)
15
☑ Limit download size for pages and documents
1 Mb
☐ Use proxy
Server
Port 0
Min delay between search queries 10 seconds
Max delay between search queries 20 seconds

Опции Онлайн атаки

- Search full LM hashes - при поиске LM хэшей, использовать весь 16-байтный хэш. Если эта опция не задана, то поиск будет производиться по 8-байтным половинам. Для более результативного поиска, а также чтобы избавиться от некоторого паразитного трафика, рекомендуется всегда устанавливать эту опцию. При поиске NT хэшей, эта опция игнорируется.
- Maximize lookup efficiency - увеличивает вероятность нахождения пароля, не влияя на скорость атаки. Рекомендуется также всегда устанавливать эту опцию.

- Skip unnecessary files - не проверять некоторые необязательные файлы если есть подозрение, что они не содержат пароли.
- Response timeout - установить максимально допустимое время отклика Веб ресурса.
- Limit download size - ограничить размер скачиваемых файлов. Некоторые базы данных хэшей имеют огромный размер, даже несмотря на то, что зачастую в них не содержатся сами пароли. Поэтому для медленных Интернет соединений и для ограничения ненужного трафика, рекомендуется устанавливать лимит по объему скачиваемых страниц. К сожалению, заранее невозможно определить, что содержит скачиваемый материал, поэтому управление этой опцией полностью определяется вашими возможностями и предпочтениями.
- Use proxy - использовать прокси сервер для поиска паролей
- Min/max delay between search queries - минимальная и максимальная задержки между двумя обращениями к поисковому серверу. Некоторые поисковые сервера могут отклонять запросы, если они идут подряд с одного IP адреса через небольшой временной интервал (обычно, менее 10 секунд). Несмотря на то, что Windows Password Recovery имеет встроенный механизм рандомизации запросов, который позволяет значительно уменьшать эту задержку (вплоть до 1 и 2 секунд соответственно), безопасные значения, когда поисковой запрос будет гарантированно обработан сервером, составляют min=15 и max=30 секунд. Естественно, скорость атаки находится в прямой зависимости от этих двух опций.

Будьте аккуратны, Онлайн атака может генерировать много Интернет трафика!

2.8.2.13 Атака по Таблицам Passcape

Радужные таблицы Passcape являются дальнейшим логическим развитием простых предвычисленных таблиц. Они более "заточены" для поиска осмысленных комбинаций и сложных паролей практически неограниченной длины.

Принцип действия простых радужных таблиц

Принцип действия простых радужных таблиц состоит в задании диапазона символов (например, a..z) и максимальной длины пароля. Затем просчитываются все возможные варианты и создаются миллионы цепочек. Каждая цепочка вычисляется по следующей формуле:
P0 -> hash(P0) -> H1 -> R(H1) ->
P1 -> hash(P1) -> H2 -> R(H2) ->
P2 ...
где P - пароль, hash - функция хэширования, R - функция редукции. Таким образом из первоначального пароля с помощью функции хэширования получается хэш, из которого на выходе функции редукции получается следующий пароль и процесс повторяется сначала, что ведет к созданию цепочек. В каждой такой цепочке сохраняется только первоначальное и конечное значение. Хранение только первого и последнего элементов является операцией, ведущей к компромиссу, сохраняя память за счет временных затрат на криптоанализ.

Для восстановления искомого пароля, он подвергается хэшированию и функции редукции, а затем ищется в таблице. Для этого создается цепочка ключей, начиная с *R(Hn)* до максимальной длины цепочки. Если Hn окажется полученным с помощью пароля, использованного при создании таблицы, то мы в итоге получим ключ, соответствующий последнему ключу соответствующей цепочки. Этот последний ключ был сохранен в таблице вместе с первым ключом цепочки. Используя первый ключ цепочки, возможно восстановить всю цепочку – в частности, значение, стоящее перед *R(Hn).* Это и есть тот ключ, который использовался для генерации Hn, т.е. наш искомый пароль.

Принцип действия радужных таблиц Passcape

Поиск с использованием радужных таблица Passcape во многом схож с поиском по простым таблицам. Но в отличие от последних, он является чем-то вроде гибрида идентификационной и простой табличной атаки, где проверка паролей производится не в заданном диапазоне символов, а в диапазоне т.н. отпечатков слов. Суть идентификационной атаки, разработанной в Passcape, сводится к тому что из исходного словаря создается банк отпечатков слов, необходимых для проверки пароля, а во время атаки производится поиск всех возможных вариантов слов, состоящих из двух таких отпечатков.

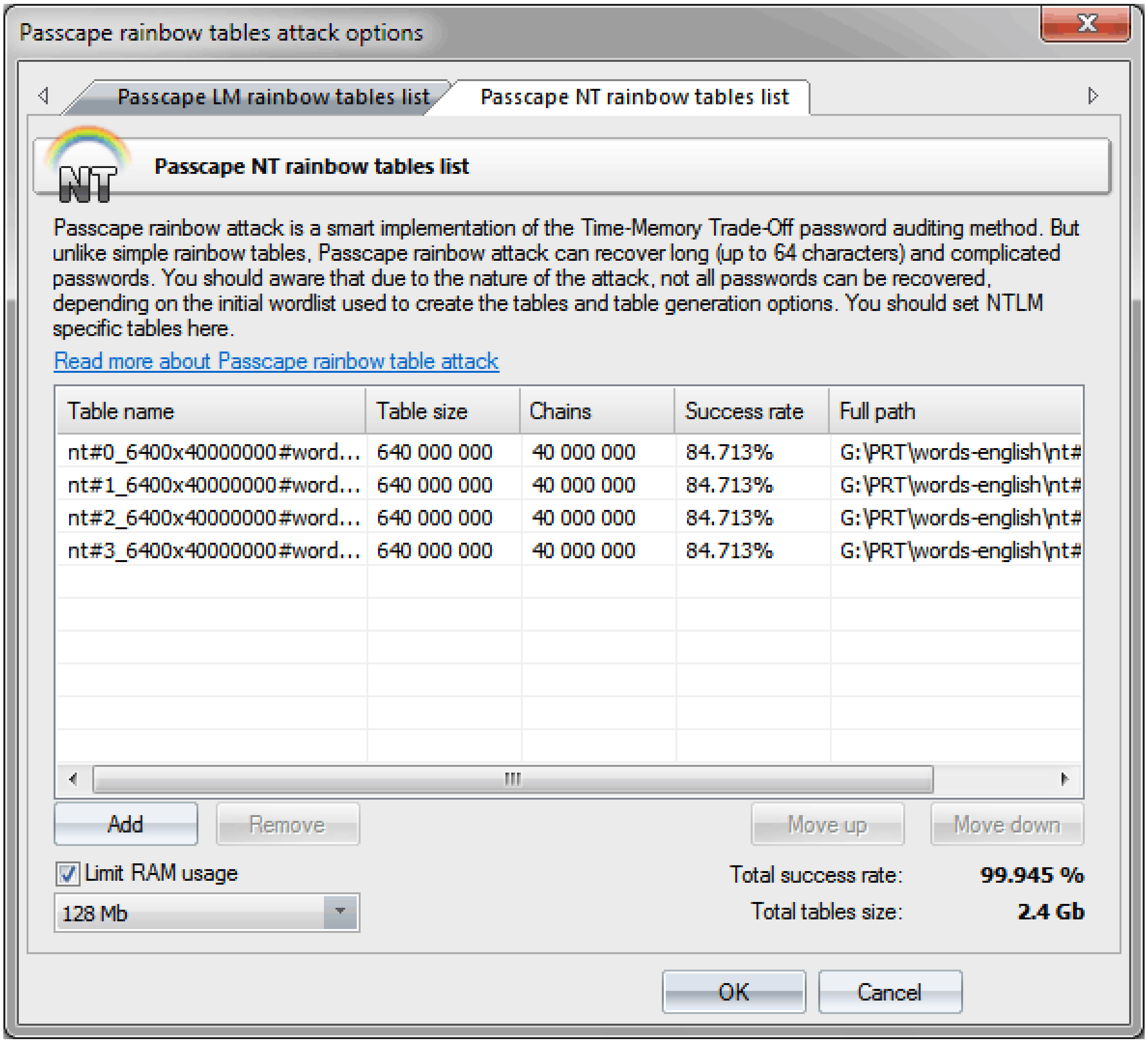
Подобно идентификационной атаке, в радужных таблицах Passcape в начале происходит создание банка отпечатков слов из заданного пользователем словаря. Банк отпечатков слов является аналогом диапазона символов в простых радужных таблицах. Он используется как при генерации Passcape таблиц, так и при проверке пароля. Таким образом, радужная таблица Passcape состоит из одной или нескольких файлов *.prt (непосредственно самих таблиц) и банка отпечатков (*.prti), который может быть задействован только с созданными с помощью него таблицами.

Использование отпечатков слов вместо диапазона символов при создании таблиц имеет ряд преимуществ:
- Длина проверяемых паролей в таблицах Passcape практически неограничена. В отличие от простых радужных таблиц, создание которых для паролей длиной более 9 символов на практике не представляется возможным, в таблицах Passcape с одинаковой долей вероятности можно найти как односимвольный, так и 50-символьный пароль.
- Диапазон символов в обычной таблице сильно влияет на ее критические параметры: чем шире диапазон символов, тем больше должна быть длина цепочки или общее количество цепочек для сохранения success rate (процент успеха при поиске пароля) этой таблицы. В таблице Passcape диапазон символов не влияет на критические параметры таблицы.
- В обычных таблицах имеются определенные сложности при создании таблиц для проверки паролей в национальных кодировках: не все программы корректно работают с такими таблицами, не все могут их создавать. В радужных таблицах Passcape при создании таблиц, например, для русских паролей, достаточно задать исходный словарь на русском языке.
- Поиск паролей в Passcape таблицах осуществляется по более осмысленным комбинациям, однако это в значительной степени зависит от исходного словаря.

К недостаткам радужных таблиц Passcape можно отнести следующее:
- Не все исходные словари одинаково хорошо подойдут для таблиц. Использование больших словарей (как правило, более 1 Мб) генерирует слишком большой банк отпечатков, соответственно, создание таблиц может занять очень много времени и ресурсов.
- Не рекомендуется использовать словари с длинными словами или фразами по причине, сказанной выше.
- Атака по радужным таблицам кушает очень много ресурсов: банк отпечатков должен полностью умещаться в оперативную память компьютера.

Настройки атаки по радужным таблицам Passcape

Опции атаки по радужным таблицам Passcape довольно тривиальны. Необходимо указать один или несколько *.prt таблиц в одном каталоге с которыми должен находиться банк отпечатков (*.prti файл). Поскольку данная атака потребляет больше памяти, чем атака с использованием обычных радужных таблиц, рекомендуется ограничить объем потребляемой памяти, выставив соответствующую опцию.


Passcape rainbow tables attack options
Passcape LM rainbow tables list
Passcape NT rainbow tables list
NT
Add
Remove
Move up
Move down
OK
Cancel

Passcape NT rainbow tables list

Passcape rainbow attack is a smart implementation of the Time-Memory Trade-Off password auditing method. But unlike simple rainbow tables, Passcape rainbow attack can recover long (up to 64 characters) and complicated passwords. You should aware that due to the nature of the attack, not all passwords can be recovered, depending on the initial wordlist used to create the tables and table generation options. You should set NTLM specific tables here.

Read more about Passcape rainbow table attack

Table name	Table size	Chains	Success rate	Full path
nt#0_6400x40000000#word...	640 000 000	40 000 000	84.713%	G:\PRT\words-english\nt#
nt#1_6400x40000000#word...	640 000 000	40 000 000	84.713%	G:\PRT\words-english\nt#
nt#2_6400x40000000#word...	640 000 000	40 000 000	84.713%	G:\PRT\words-english\nt#
nt#3_6400x40000000#word...	640 000 000	40 000 000	84.713%	G:\PRT\words-english\nt#

☑ Limit RAM usage

128 Mb

Total success rate: **99.945 %**

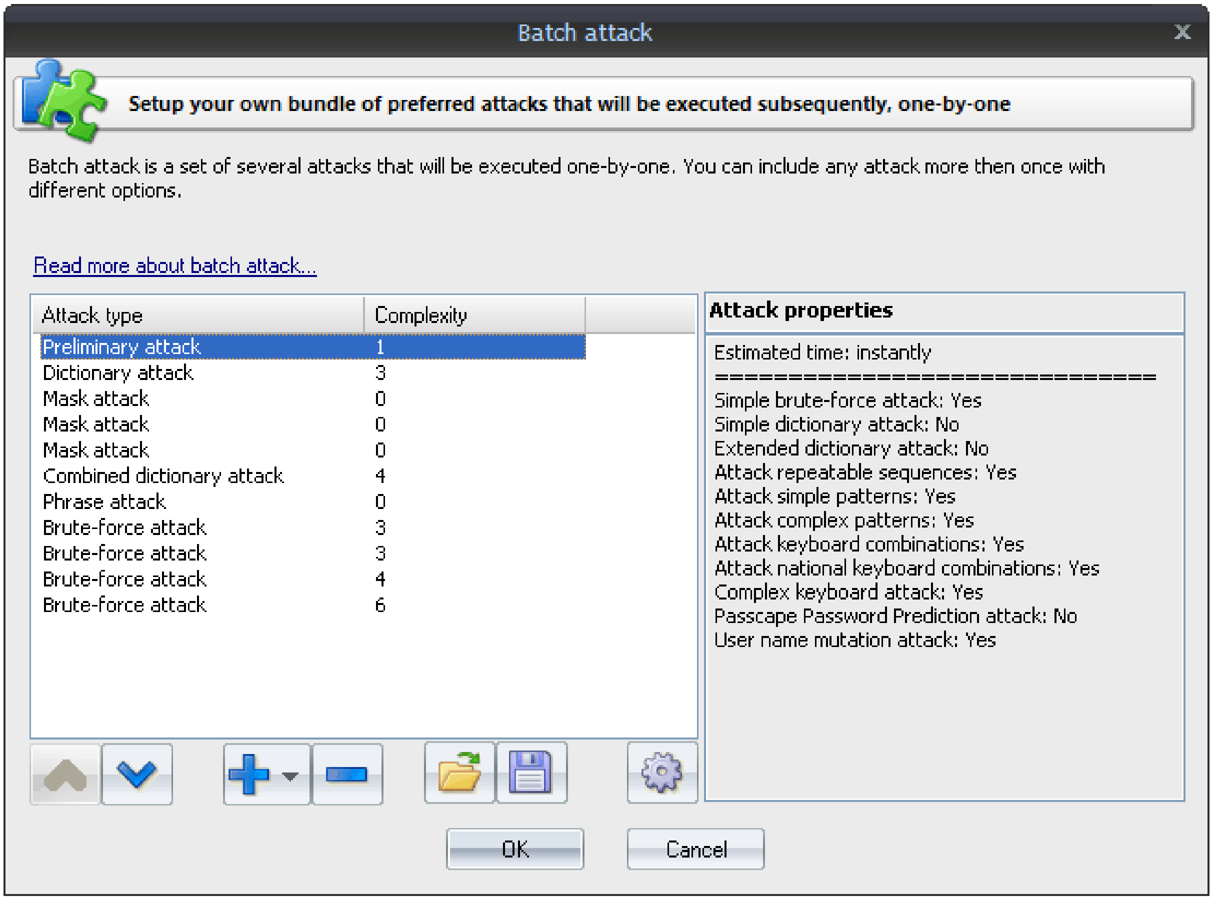
Total tables size: **2.4 Gb**

Таблицы могут взламывать только ту хеш-функцию, для которой они создавались, то есть таблицы для NT могут взломать только NT хеш.

Для создания своих собственных таблиц, воспользуйтесь соответствующим инструментом.
С нашего сайта можно скачать несколько Passcape таблиц для данной атаки.

2.8.2.14 Групповая Атака

Поскольку каждая атака охватывает свой диапазон паролей, то иногда, для полноценной расшифровки парольных хэшей, 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.



Setup your own bundle of preferred attacks that will be executed subsequently, one-by-one

Batch attack is a set of several attacks that will be executed one-by-one. You can include any attack more then once with different options.

Attack type	Complexity
Preliminary attack	1
Dictionary attack	3
Mask attack	0
Mask attack	0
Mask attack	0
Combined dictionary attack	4
Phrase attack	0
Brute-force attack	3
Brute-force attack	3
Brute-force attack	4
Brute-force attack	6

Attack properties

```
Estimated time: instantly
=================================
Simple brute-force attack: Yes
Simple dictionary attack: No
Extended dictionary attack: No
Attack repeatable sequences: Yes
Attack simple patterns: Yes
Attack complex patterns: Yes
Attack keyboard combinations: Yes
Attack national keyboard combinations: Yes
Complex keyboard attack: Yes
Passcape Password Prediction attack: No
User name mutation attack: Yes
```

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 займет ее работа.

2.8.2.15 GPU: Атака перебором

Атака перебором на GPU полностью аналогична атаке простым перебором за тем лишь исключением, что подбор паролей осуществляется не процессором, а графической картой вашего ПК. Не секрет, что производительность современных графических карт на порядок выше процессоров, поэтому их удобно использовать для тяжелых расчетов, в частности при восстановлении паролей. Важно также понимать, что вычисления на графических картах обладает рядом недостатков. Например, некоторые алгоритмы, с большим числом ветвлений и проверок "ложатся" очень плохо на GPU, и в иных случаях, производительность их может быть даже ниже, чем на процессоре.

Так или иначе, но в программе реализована поддержка перебора паролей на GPU. Можно сравнить скоростные характеристики вычислений на GPU и CPU в соответствующем пункте меню программы или представить наглядным образом в меню 'Отчеты'.

Настройка атаки перебором на GPU состоит из трех частей:
1. Выбор набора символов для перебора.
2. Установка длины пароля.

3. Установки графической карты.

Выбор набора символов для перебора

При выборе набора символов для атаки перебором руководствуются в основном эмпирическими соображениями. Например, если предполагаемый пароль состоит из малых Латинских символов и цифр, есть смысл выбрать диапазон 'a-z, 0-9'.

Чем меньше диапазон символов, тем быстрее будет завершена атака.

С другой стороны, всегда есть возможность ошибиться с выбором предполагаемого диапазона символов. Если хотя бы один символ искомого пароля не будет входить в заданный набор символов, этот пароль найден не будет.

Внизу диалога с установками атаки показывается общее количеств паролей, которые соответствуют заданному набору символов и длине пароля.

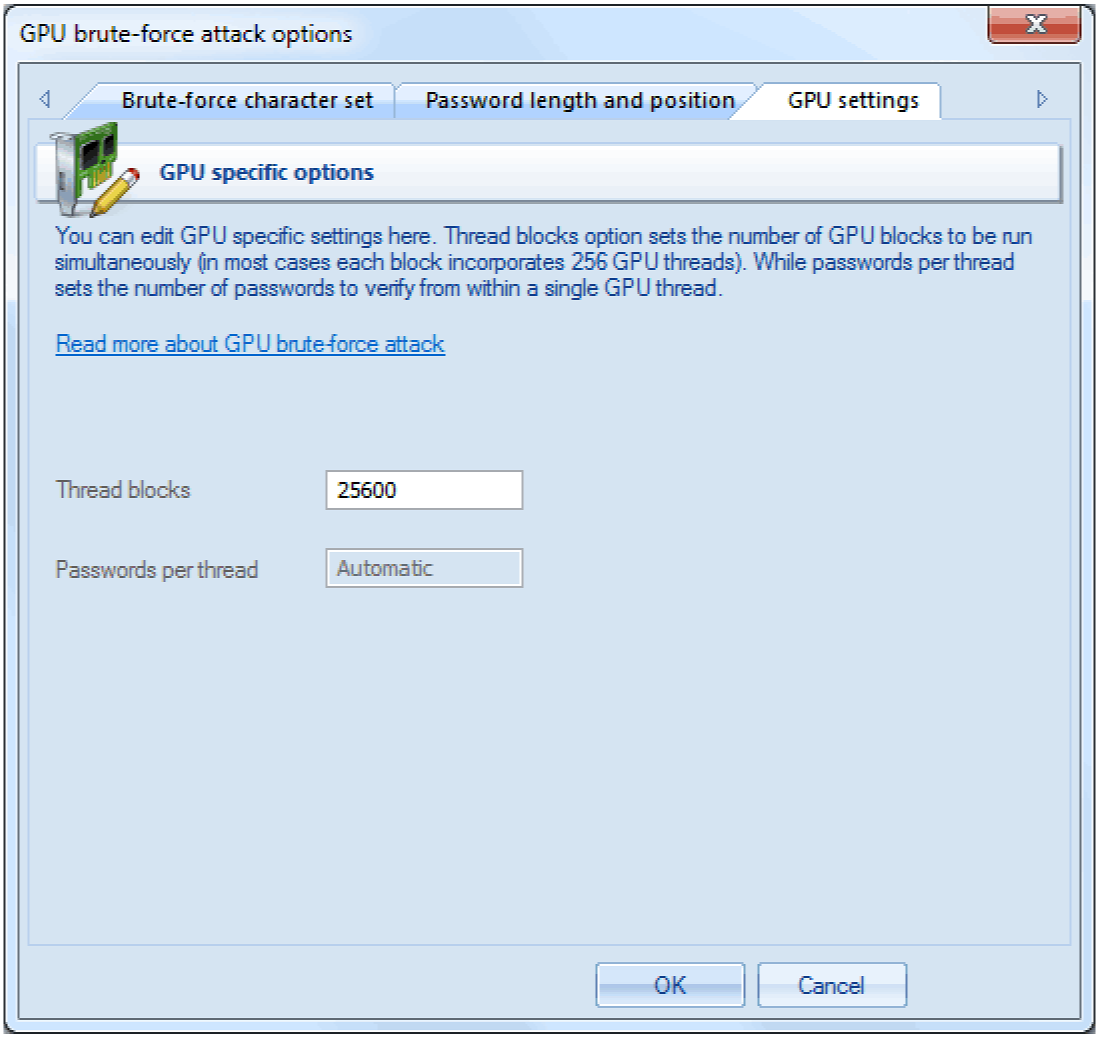
Важно знать, что LM пароли в Windows всегда приводятся в верхний регистр, что значительно сокращает диапазон перебираемых паролей!

Установка длины пароля

Во второй вкладке опций необходимо выставить минимальную и максимальную длину перебираемых паролей. В качестве альтернативы минимальной длины, можно установить исходный пароль, с которого будет начинаться перебор. Максимальная длина LM паролей в ОС Windows равна 7.

Установки графической карты

Перед использованием ее в атаке, графическую карту необходимо выбрать в соответствующем пункте общего меню.


GPU brute-force attack options
Brute-force character set
Password length and position
GPU settings
OK
Cancel

GPU specific options

You can edit GPU specific settings here. Thread blocks option sets the number of GPU blocks to be run simultaneously (in most cases each block incorporates 256 GPU threads). While passwords per thread sets the number of passwords to verify from within a single GPU thread.

Read more about GPU brute-force attack

Thread blocks: 25600

Passwords per thread: Automatic

Настройка графической карты состоит всего из одного параметра:
1. Установка количество параллельных блоков графической карты, в которых будет осуществляться поиск паролей.

Каждый запускаемый на видеокарте блок состоит из 256 потоков. Таким образом, если задать количество блоков равным 25600, то каждый раз на GPU будет запущено 25600*256=6553600 потоков. Установка этого параметра меньше 10000 на современных графических картах в большинстве случаев приводит к снижению производительности.

Если график загрузки видеокарты в системном мониторе имеет ровный, не скачкообразный характер, близкий к 100%, то это значит, что параметр 'Thread blocks' выбран правильно.

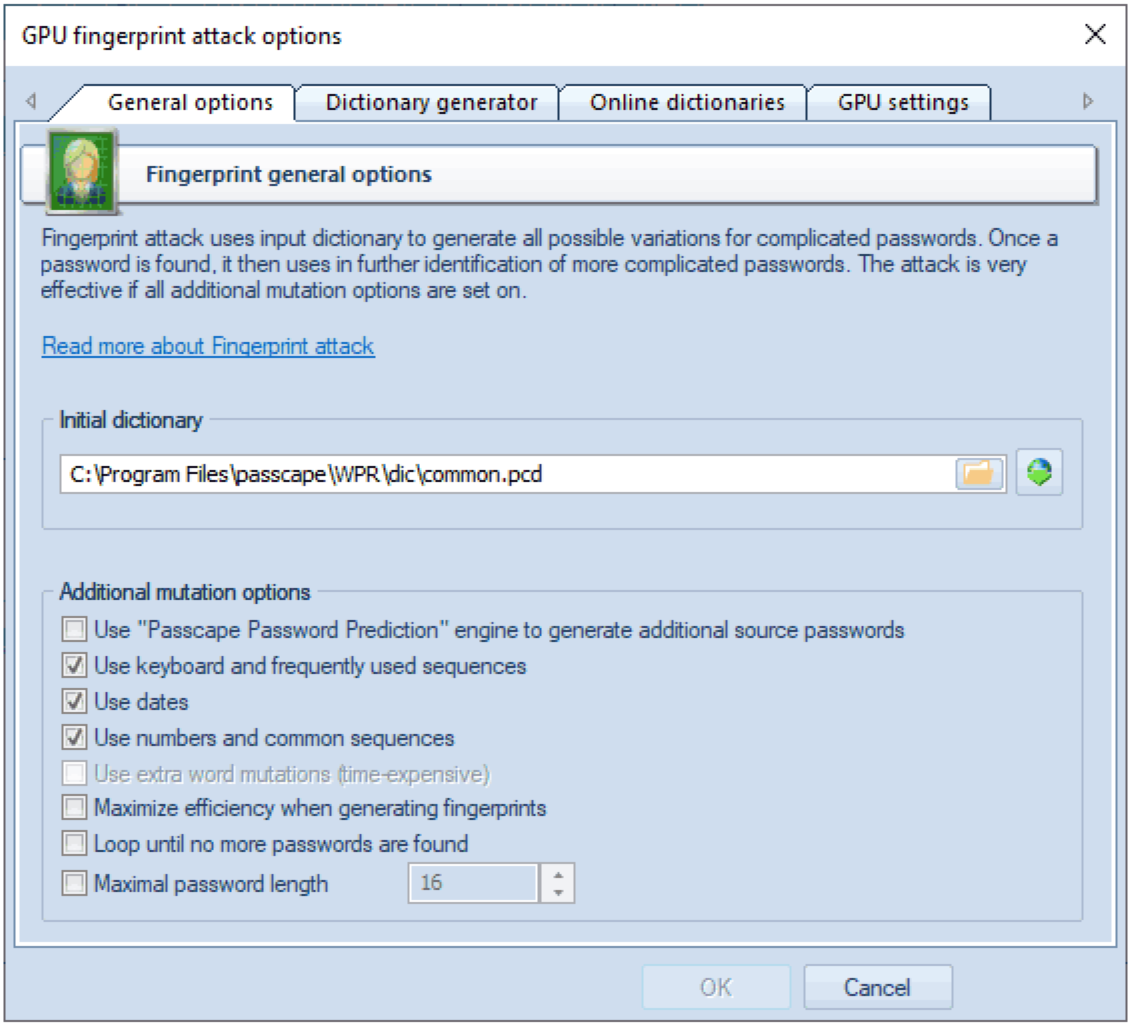
При восстановлении кэшированных паролей домена тип 2 (DCC2) вам, возможно, придется дополнительно изменить параметр '**Thread Blocks**', чтобы обеспечить оптимальную производительность видеокарт.
Слишком большие значения могут привести в зависанию или ошибкам GPU, в зависимости от настроек GPU kernel timeout.

2.8.2.16 GPU: Идентификационная Атака

Идентификационная атака (fingerprint attack) на GPU - новый продвинутый инструмент для восстановления сложных паролей, не поддающихся расшифровке в обычных атаках. Суть ее состоит в том, чтобы для поиска паролей брать не отдельные слова исходного словаря, как в простой словарной атаке, и даже не комбинации слов, как в комбинированной атаке по словарям, а так называемые "отпечатки" (отсюда и название, fingerprint от анл. отпечаток). При этом каждое исходное слово заданного словаря используется для создания нескольких таких отпечатков. Если в процессе атаки был найден какой-либо пароль, он участвует в создании новых отпечатков и атака повторяется снова. Применение вычислений на GPU позволяет значительно увеличить скорость проверки паролей в этой атаке, настройка которой состоит из четырех частей.

Основные настройки атаки

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 займет значительное время. Можно использовать словари с национальными паролями, если есть подозрения, что искомый пароль содержит символы в национальной кодировке. В качестве словаря можно (и даже желательно!) использовать уже готовые списки паролей.



GPU fingerprint attack options

Fingerprint general options

Fingerprint attack uses input dictionary to generate all possible variations for complicated passwords. Once a password is found, it then uses in further identification of more complicated passwords. The attack is very effective if all additional mutation options are set on.

Read more about Fingerprint attack

Initial dictionary

C:\Program Files\passcape\WPR\dic\common.pcd

Additional mutation options

□ Use "Passcape Password Prediction" engine to generate additional source passwords
☑ Use keyboard and frequently used sequences
☑ Use dates
☑ Use numbers and common sequences
□ Use extra word mutations (time-expensive)
□ Maximize efficiency when generating fingerprints
□ Loop until no more passwords are found
□ Maximal password length 16

Отпечатки генерируются следующим образом: каждое слово исходного словаря сначала разбивается на однобуквенные пароли, затем на 2-х буквенные, 3-х и т.д. Например, исходное слово **crazy** программа разбивает на односимвольные отпечатки. Получается:
c
r
a
z
y

Затем на двух символьные:
cr
ra
az
zy

Потом трех:
cra
raz
azy

И, наконец, четырех символьные:

craz
razy

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 путем склейки всех отпечатков друг с другом.

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

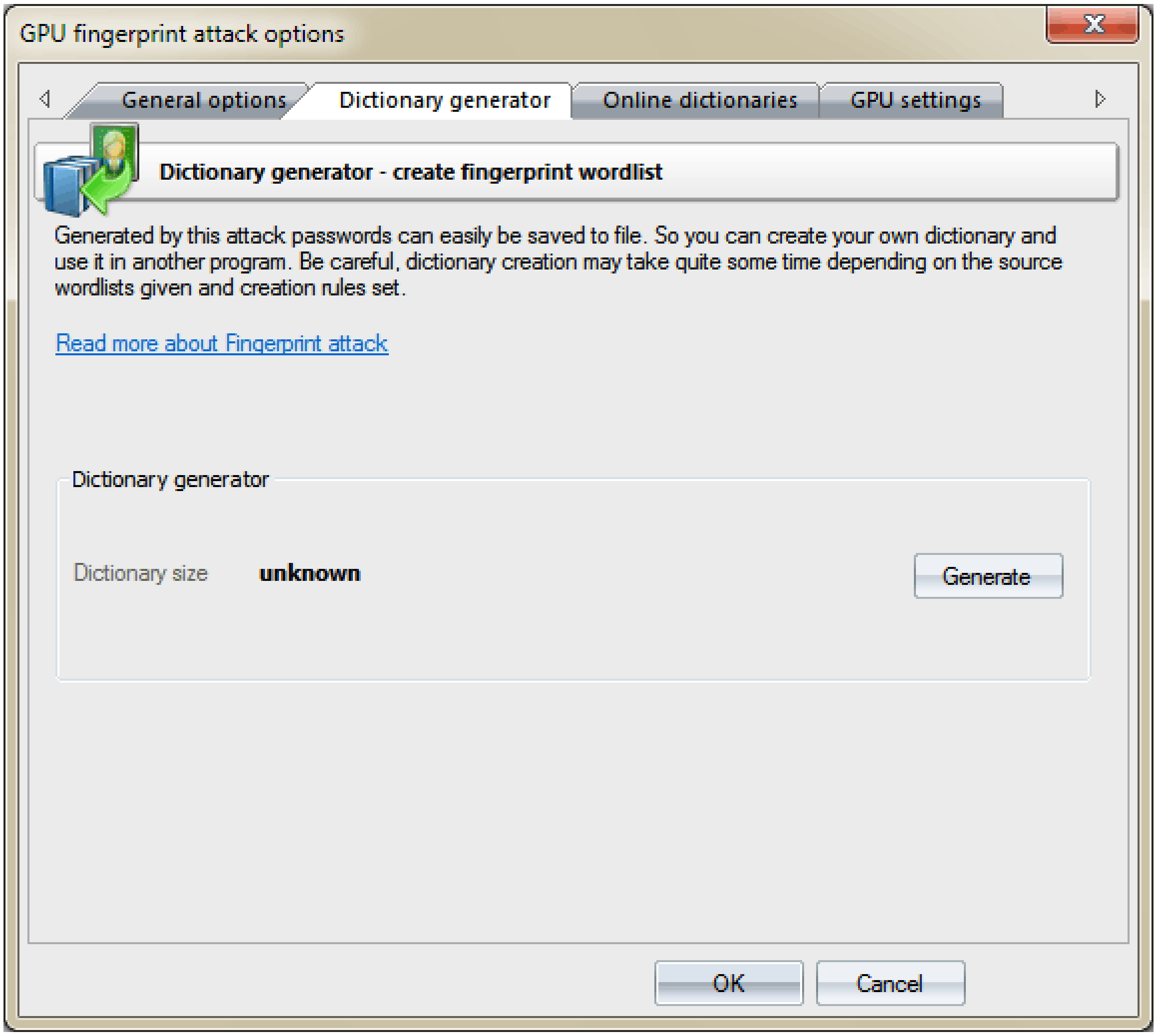
Разберем оставшиеся опции.

- **Use PPP engine to generate additional passwords** - задействовать при создании отпечатков пароли, которые были найдены ранее 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 дополнительно цифры и простые комбинации букв.
- **Maximal password length** - эта опция позволяет ограничить максимальную длину генерируемых паролей. В большинстве случаев это приводит к уменьшению времени работы атаки.

Наиболее пристального внимания заслуживает опция **Loop until no more passwords are found**. Вот где идентификационная атака может себя проявить. Работает она таким образом: если во время атаки был найден хотя бы один пароль, по после окончания атаки этот пароль участвует в создании новых отпечатков и атака повторяется сначала. Эта опция неплохо работает на больших списках хэшей, а также на хэшах с историей паролей. Следует знать, что установив эту опцию, невозможно будет продолжить атаку с последней запомненной позиции.

Генератор словарей

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



Dictionary generator - create fingerprint wordlist

Generated by this attack passwords can easily be saved to file. So you can create your own dictionary and use it in another program. Be careful, dictionary creation may take quite some time depending on the source wordlists given and creation rules set.

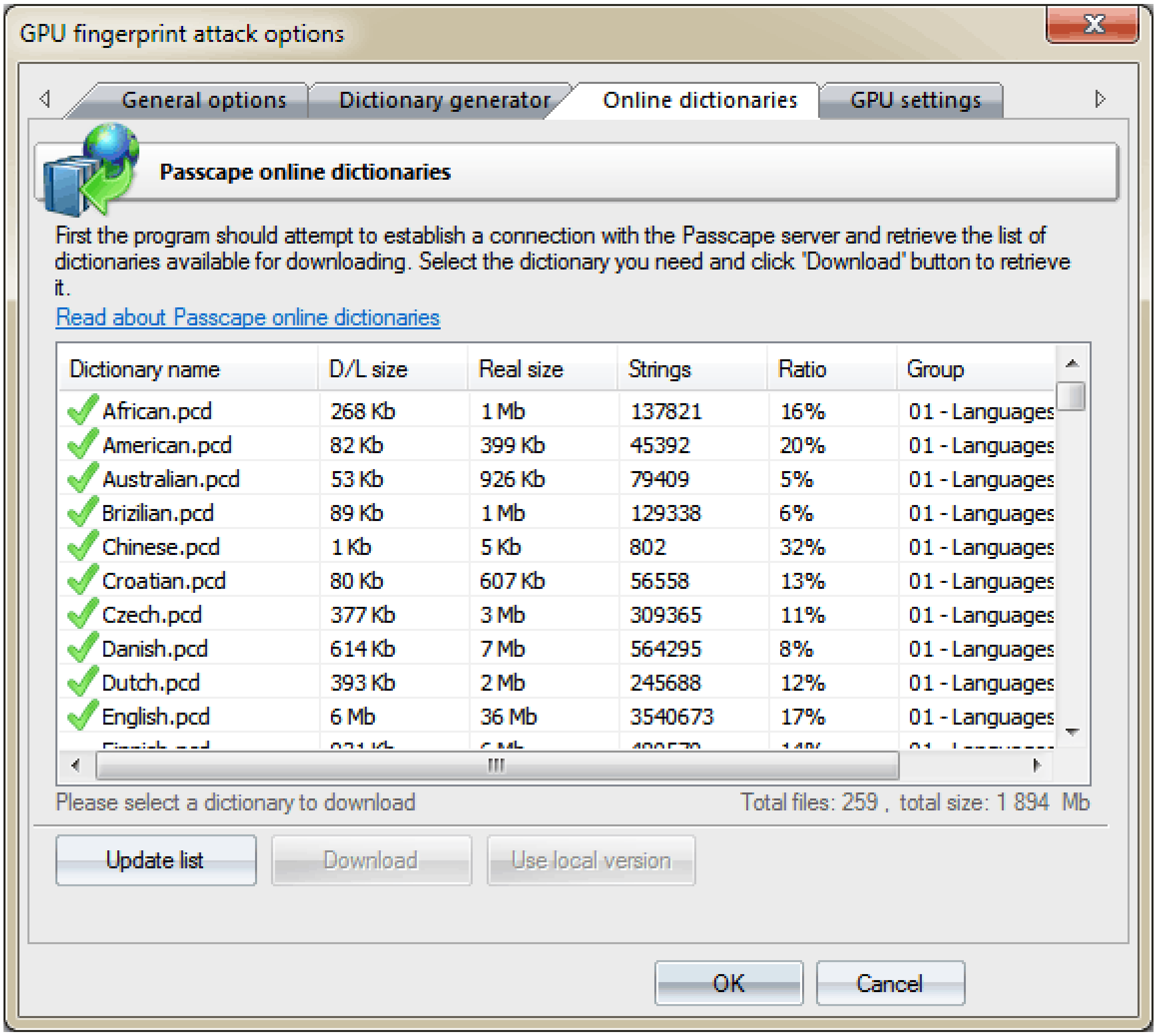
Read more about Fingerprint attack

Dictionary generator

Dictionary size **unknown**

<u>Онлайн словари</u>

В третьей вкладке можно скачать из сети Интернет исходные словари для Идентификационной атаки. Будьте внимательны, не все словари одинаково хорошо подходят для Идентификационной атаки.



Passcape online dictionaries

First the program should attempt to establish a connection with the Passcape server and retrieve the list of dictionaries available for downloading. Select the dictionary you need and click 'Download' button to retrieve it.

Read about Passcape online dictionaries

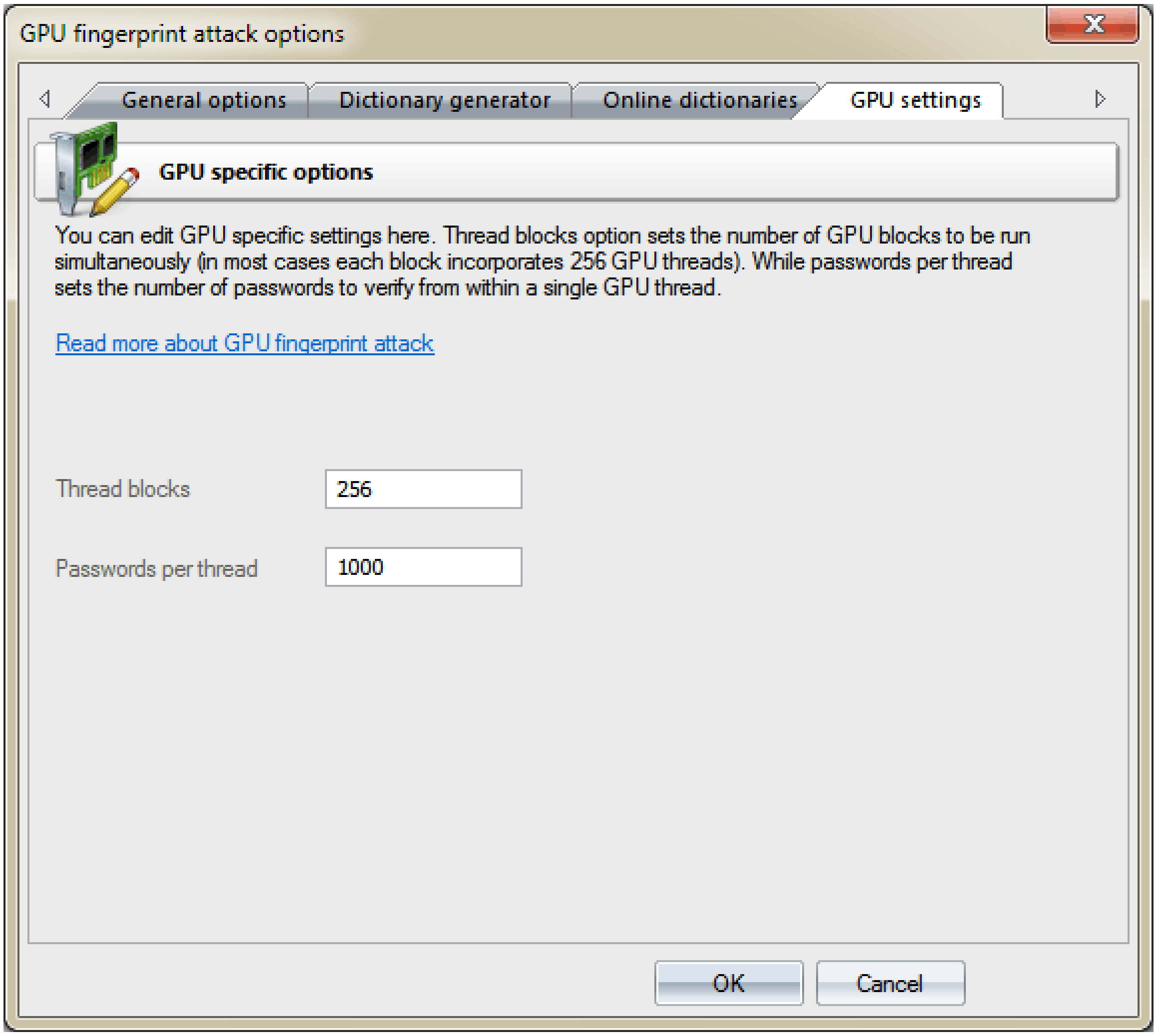
Dictionary name	D/L size	Real size	Strings	Ratio	Group
✓ African.pcd	268 Kb	1 Mb	137821	16%	01 - Languages
✓ American.pcd	82 Kb	399 Kb	45392	20%	01 - Languages
✓ Australian.pcd	53 Kb	926 Kb	79409	5%	01 - Languages
✓ Brizilian.pcd	89 Kb	1 Mb	129338	6%	01 - Languages
✓ Chinese.pcd	1 Kb	5 Kb	802	32%	01 - Languages
✓ Croatian.pcd	80 Kb	607 Kb	56558	13%	01 - Languages
✓ Czech.pcd	377 Kb	3 Mb	309365	11%	01 - Languages
✓ Danish.pcd	614 Kb	7 Mb	564295	8%	01 - Languages
✓ Dutch.pcd	393 Kb	2 Mb	245688	12%	01 - Languages
✓ English.pcd	6 Mb	36 Mb	3540673	17%	01 - Languages
Finnish.pcd	921 Kb	6 Mb	480570	14%	01 - Languages

Please select a dictionary to download

Total files: 259 , total size: 1 894 Mb

Установки графической карты

Перед использованием ее в атаке, графическую карту необходимо выбрать в соответствующем пункте общего меню.



You can edit GPU specific settings here. Thread blocks option sets the number of GPU blocks to be run simultaneously (in most cases each block incorporates 256 GPU threads). While passwords per thread sets the number of passwords to verify from within a single GPU thread.

Read more about GPU fingerprint attack

Thread blocks: 256

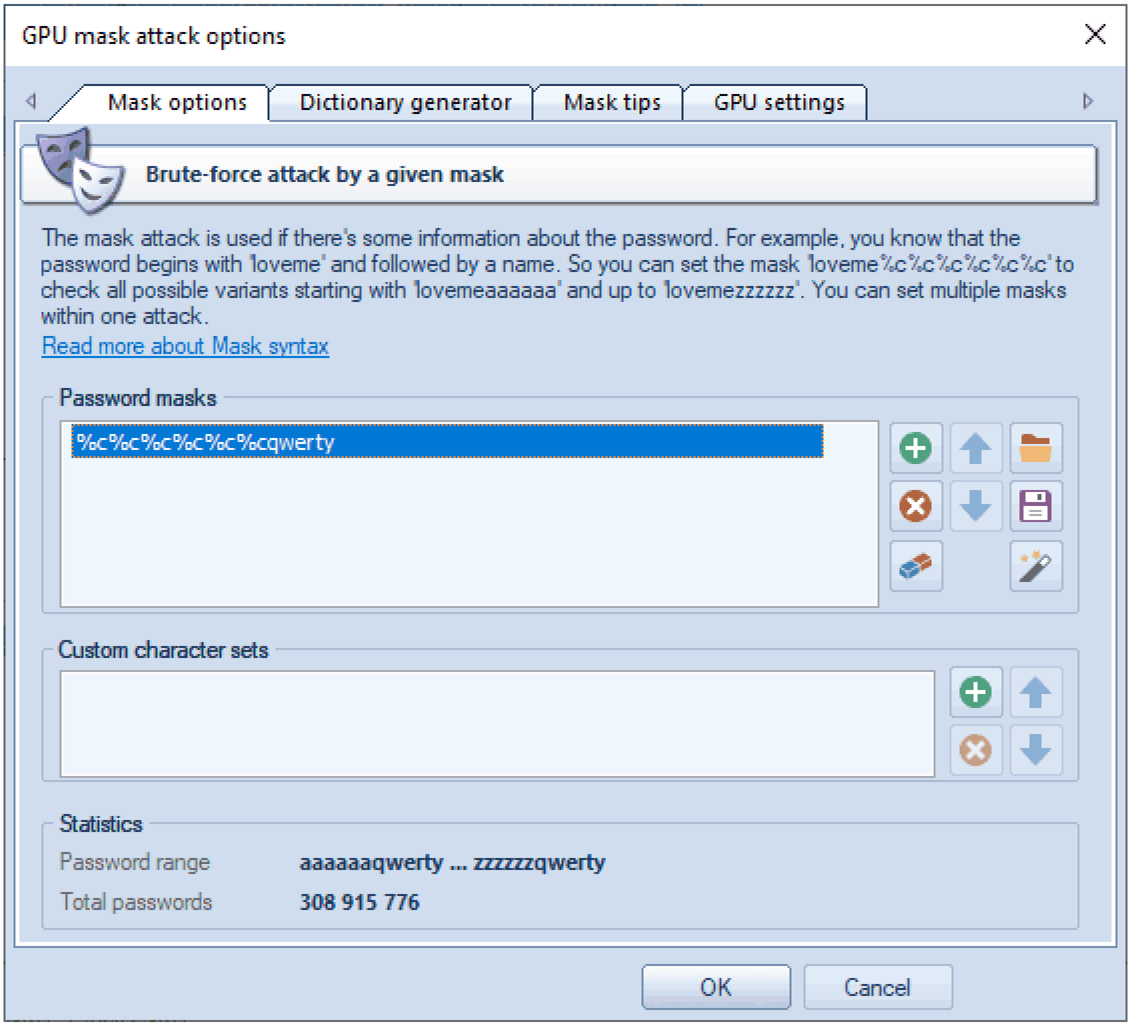
Passwords per thread: 1000

Настройка графической карты состоит из двух частей:
1. Установка количество параллельных блоков графической карты, в которых будет осуществляться поиск паролей. Каждый блок состоит из 256 потоков. Например, если задать количество блоков равным 256, то каждый раз на GPU будет запущено 256*256=65536 потоков. А общее количество проверяемых паролей за один запуск GPU кернела будет составлять 256*ThreadBlocks*PasswordsPerThread, т.е. в нашем случае, 256*256*1000= 65 536 000 паролей. Рекомендуется всегда устанавливать значение **Thread Blocks** кратным 64. Установка этого параметра меньше 256 на современных графических картах в большинстве случаев приводит к снижению производительности.
2. Установка максимального количества паролей, обрабатываемые в одном потоке GPU. Чем выше это значение, тем меньше накладных расходов, связанных с запуском потоков, обработки переменных и т.д. и, соответственно, тем выше скорость перебора. Однако установка слишком большого значения может привести к зависанию компьютера, голубому экрану смерти, либо к тому, что текущая скорость перебора (во вкладке состояния атаки) начинает "плясать". Это связано с тем, что время выполнения задачи на GPU превышает время обновления текущего состояния атаки. Значение по умолчанию для этого параметра составляет 1000.

При восстановлении кэшированных паролей домена тип 2 (DCC2) вам, возможно, придется дополнительно изменить параметр '**Thread Blocks**', чтобы обеспечить оптимальную производительность видеокарт.
'**Password per thread'** не используется и всегда равен 1 при восстановлении паролей DCC2.
Слишком большие значения '**Thread Blocks**' могут привести в зависанию или ошибкам GPU, в зависимости от настроек GPU kernel timeout.

2.8.2.17 GPU: Атака по Маске

Настройка маски
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 и бесполезно, т.к. это может занять годы работы современного ПК. Все, что потребуется, это угадать первые 6 символов искомого пароля. Для этого и существует атака по маске.



The mask attack is used if there's some information about the password. For example, you know that the password begins with 'loveme' and followed by a name. So you can set the mask 'loveme%c%c%c%c%c%c' to check all possible variants starting with 'lovemeaaaaaa' and up to 'lovemezzzzzz'. You can set multiple masks within one attack.
Read more about Mask syntax

Password masks: %c%c%c%c%c%cqwerty

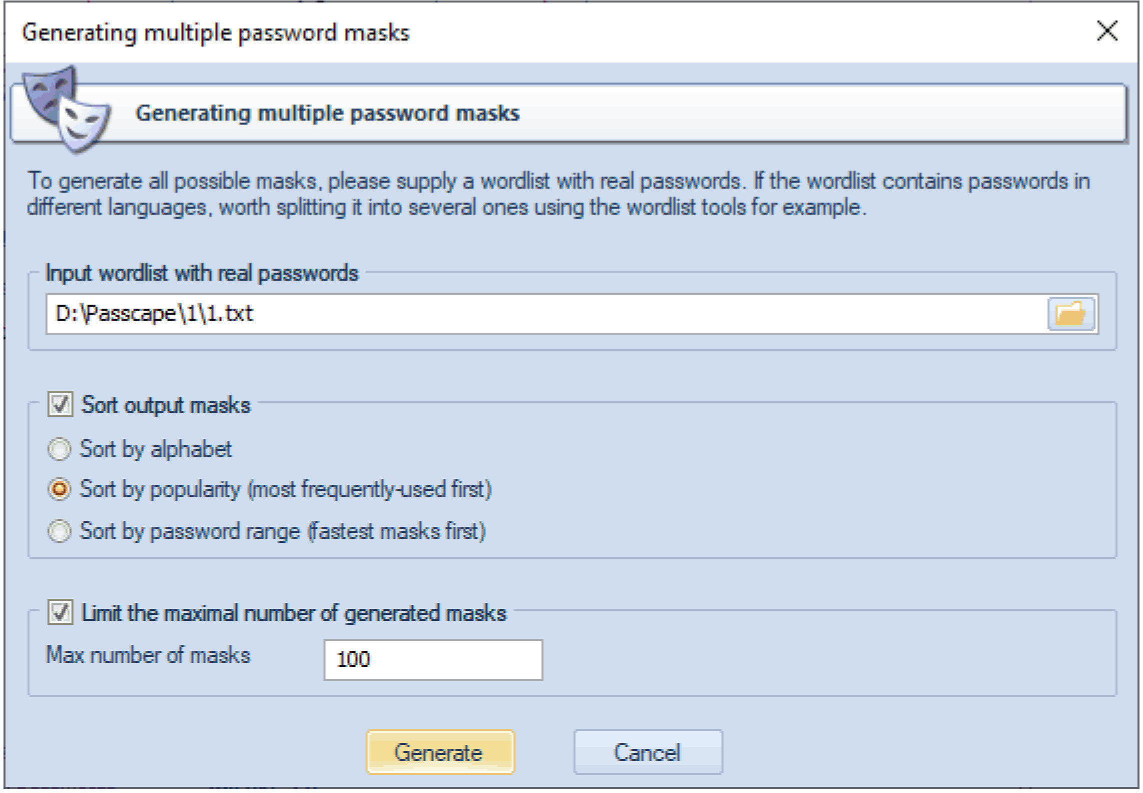
Custom character sets

Statistics
Password range: aaaaaaqwerty ... zzzzzzqwerty
Total passwords: 308 915 776

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.

Группа опций Password Masks служит для задания масок, по которым будут перебираться пароли. Как правило, если известна часть пароля, достаточно задать одну единственную маску. При выделении маски, группа "статистика" показывает диапазон перебираемых символов и количество генерируемых этой маской паролей. Свои маски можно сохранять на диске. Программа позволяет также генерировать словарь по заданной маске или нескольким маскам, однако эта опция доступна не во всех редакциях.

 Утилита для генерации масок по словарю с паролями заслуживает отдельного упоминания. Предположим что у вас есть словарь расшифрованных паролей и вы хотели бы сгенерировать шаблоны масок по этим паролям. Нет ничего проще. Запускаем генератор масок и задаем исходный словарь с паролями. Можно отсортировать полученные таким образом маски по алфавиту, популярности или диапазону перебора (вначале самые быстрые).



Generating multiple password masks

Generating multiple password masks

To generate all possible masks, please supply a wordlist with real passwords. If the wordlist contains passwords in different languages, worth splitting it into several ones using the wordlist tools for example.

Input wordlist with real passwords: D:\Passcape\1\1.txt

☑ Sort output masks

○ Sort by alphabet

● Sort by popularity (most frequently-used first)

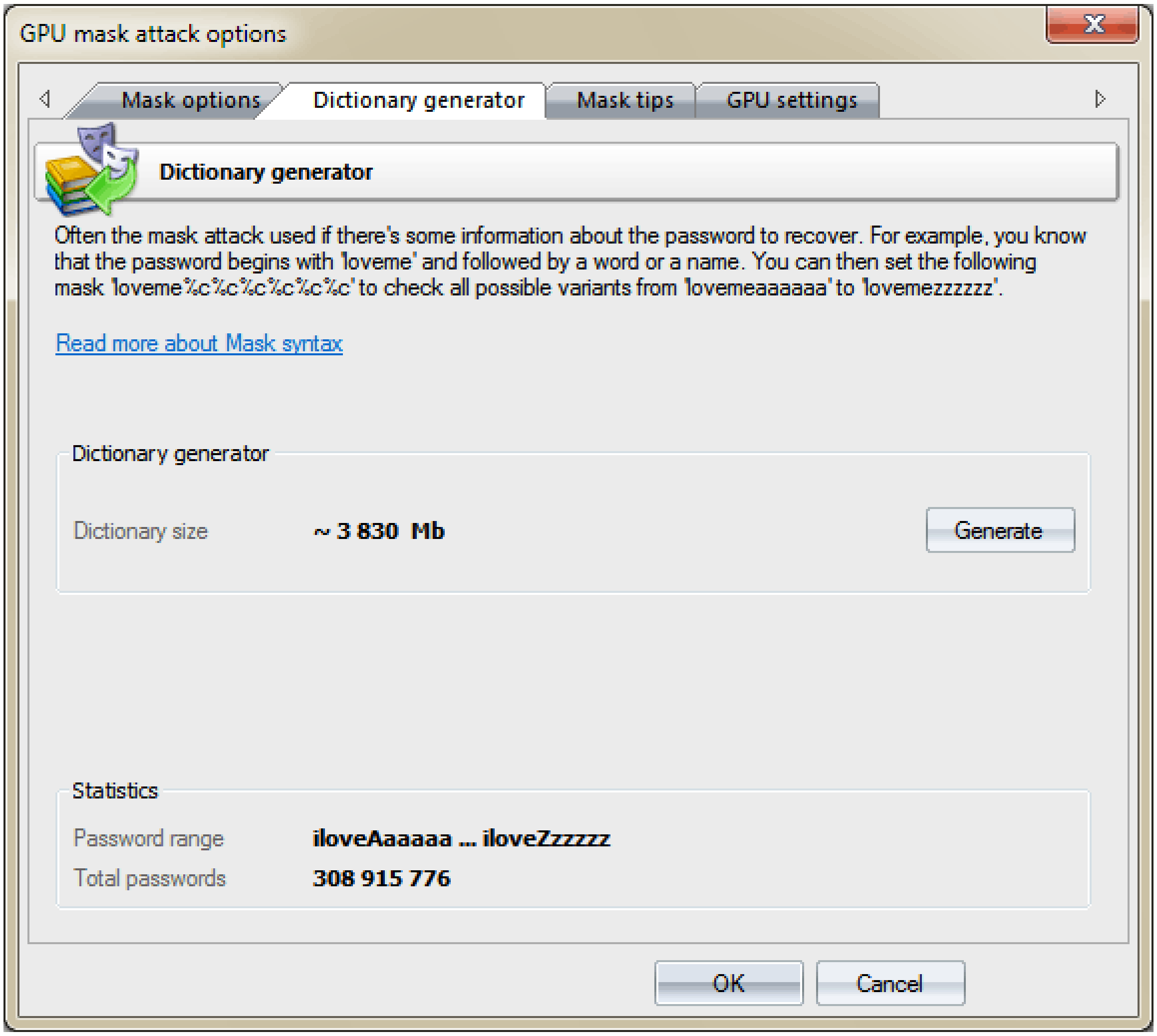
○ Sort by password range (fastest masks first)

☑ Limit the maximal number of generated masks

Max number of masks: 100

Генератор словарей

Перейдя во вторую вкладку настроек, вы можете создать свой собственный словарь по заданной маске и сохранить его на диск. Однако эта опция доступна только в Advanced редакции программы.



Often the mask attack used if there's some information about the password to recover. For example, you know that the password begins with 'loveme' and followed by a word or a name. You can then set the following mask 'loveme%c%c%c%c%c%c' to check all possible variants from 'lovemeaaaaaa' to 'lovemezzzzzz'.

Read more about Mask syntax

Dictionary generator

Dictionary size ~ 3 830 Mb

Statistics

Password range iloveAaaaaa ... iloveZzzzzz

Total passwords 308 915 776

Правила и синтаксис

Описание синтаксиса и примеры можно посмотреть в третьей вкладке опций. 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%d%d%d, то программа сгенерирует 10000 паролей (secret0000, secret0001 .. secret9999). Windows Password Recovery 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.
- **%*** набор всех ASCII символов с кодами от 1 до 255.
- **%d** одна цифра (0..9).
- **%r(x-y)** свой набор символов с последовательными UNICODE кодами от x до y

- **%r(x1-y1,x2-y2...xn-yn)** набор из нескольких непересекающихся последовательностей UNICODE символов.
- **%1[2,3..9]** символ из пользовательского набора 1..9
- **%%** статический символ %

С помощью %r можно задавать наборы для любых национальных кодировок.

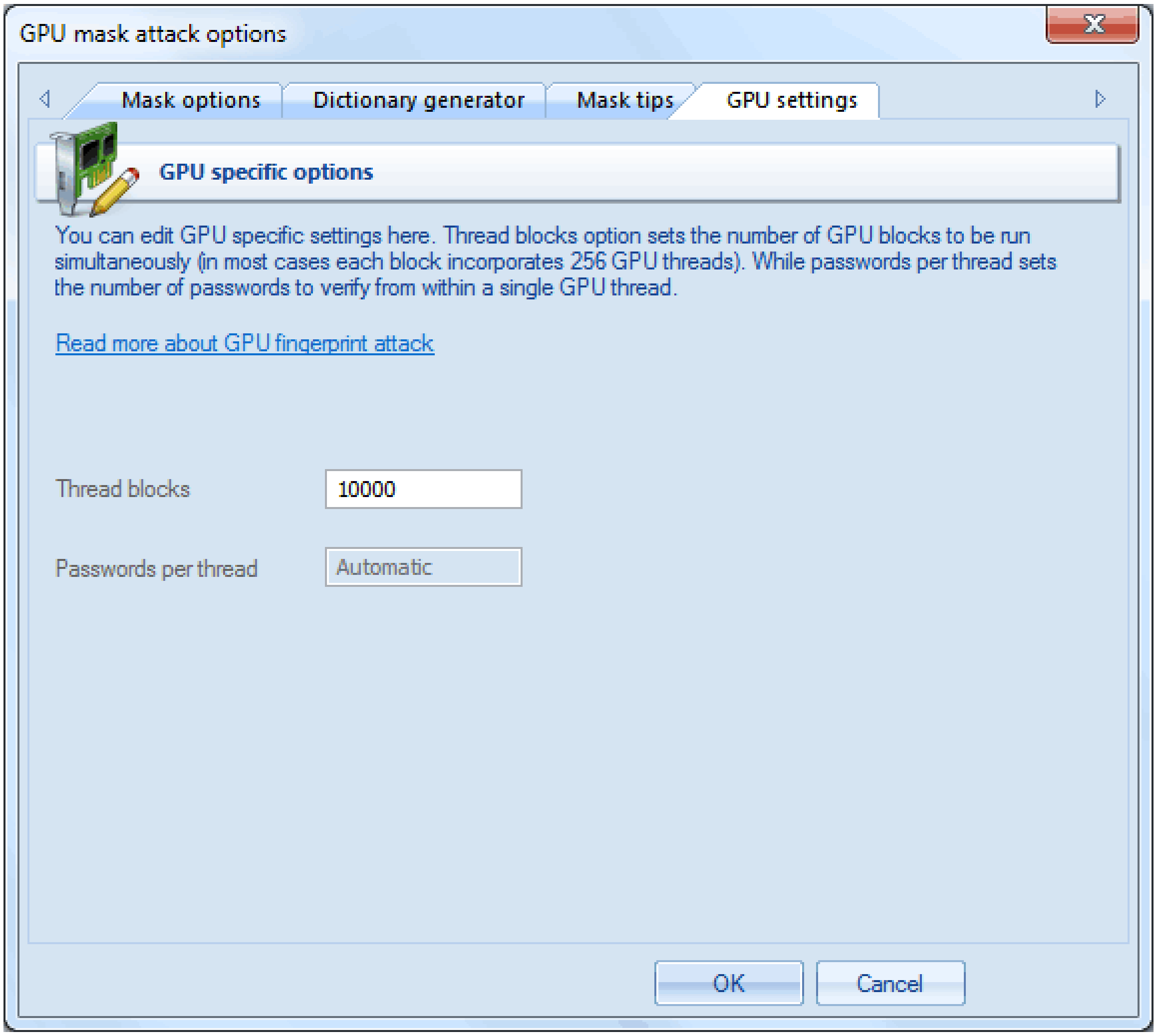
Примеры:
test%d - парольный ряд test0 .. test9, всего 10 комбинаций
test%d%d%d%d - test0000..test9999, 10000 паролей
test%r(0x0600-0x06ff) - test_ .. test_, 256 паролей с арабским символом на конце
%#test%# - _test_..~test~, 1089 паролей
%1%1%1pin%2%2%2 - aaapin000.. zzzpin999, где %1 - это пользовательский набор (a..z), а %2 - второй набор пользователя 0..9
ilove%1%1%1%1%1 - iloveaaaaa .. iloveZZZZZ, %1 - это пользовательский набор (a..z, A..Z)

Синтаксис маски в GPU атаке немного отличается от правил обычной атаки. Главное отличие состоит в том, что в GPU атаке нельзя задавать последовательность чисел от x до y, а также пользовательский набор символов переменной длины. Т.е. следующий синтакс не работает в GPU атаке:

- **%d(x-y)** последовательность чисел от x до y включительно.
- **%1[2,3..9](min-max)** пользовательский набор символов переменной длины (от min до max)

Установки графической карты

Перед использованием ее в атаке, графическую карту необходимо выбрать в соответствующем пункте общего меню.



You can edit GPU specific settings here. Thread blocks option sets the number of GPU blocks to be run simultaneously (in most cases each block incorporates 256 GPU threads). While passwords per thread sets the number of passwords to verify from within a single GPU thread.

Read more about GPU fingerprint attack

Thread blocks: 10000

Passwords per thread: Automatic

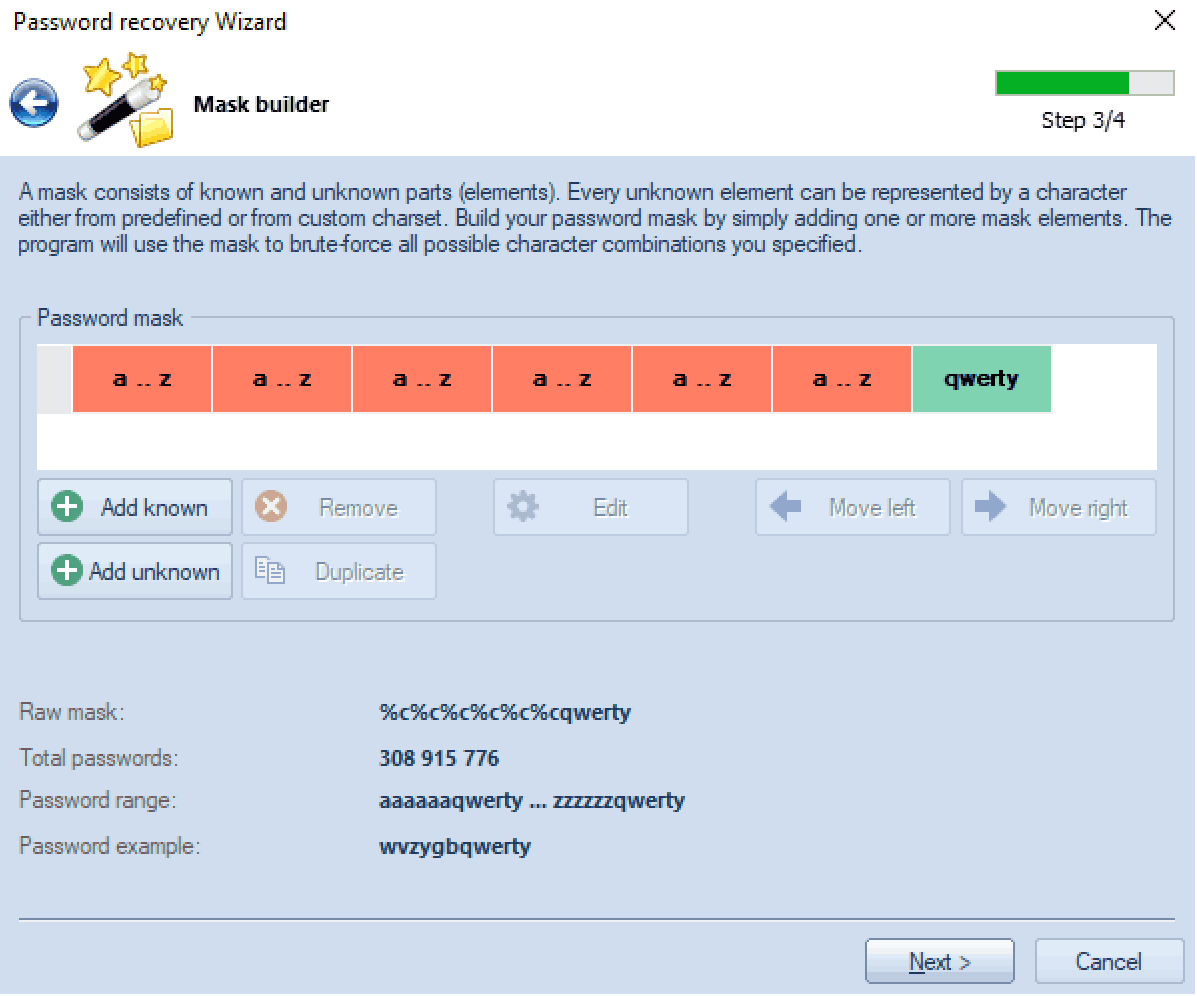
Настройка графической карты состоит всего из одного параметра:
1. Установка количество параллельных блоков графической карты, в которых будет осуществляться поиск паролей.

Каждый запускаемый на видеокарте блок состоит из 256 потоков. Таким образом, если задать количество блоков равным 10000, то каждый раз на GPU будет запущено 10000*256=2560000 потоков. Установка этого параметра меньше 10000 на современных графических картах в большинстве случаев приводит к снижению производительности.

Если график загрузки видеокарты в системном мониторе имеет ровный, не скачкообразный характер, близкий к 100%, то это значит, что параметр 'Thread blocks' выбран правильно.

При восстановлении кэшированных паролей домена тип 2 (DCC2) вам, возможно, придется дополнительно изменить параметр '**Thread Blocks**', чтобы обеспечить оптимальную производительность видеокарт.
Слишком большие значения могут привести в зависанию или ошибкам GPU, в зависимости от настроек GPU kernel timeout.

Если вы чувствуете себя потерянным и уставшим от всех этий масочной дребедени, то лучше используйте Mask Builder (в Мастере восстановления паролей), который имеет гораздо более удобный графический интерфейс.


Password recovery Wizard

Mask builder

Step 3/4

A mask consists of known and unknown parts (elements). Every unknown element can be represented by a character either from predefined or from custom charset. Build your password mask by simply adding one or more mask elements. The program will use the mask to brute-force all possible character combinations you specified.

Password mask

a .. z | a .. z | a .. z | a .. z | a .. z | a .. z | qwerty

Raw mask: %c%c%c%c%c%cqwerty

Total passwords: 308 915 776

Password range: aaaaaaqwerty ... zzzzzzqwerty

Password example: wvzygbqwerty

2.8.2.18 GPU: Атака по словарю (с перебором)

Часто, при создании паролей, пользователи добавляют определенный набор символов в начало, конец или даже в середину слова. Для нахождения такого рода паролей была специально придумана атака по словарю на GPU, которая представляет собой нечто среднее между простой словарной атакой и атакой перебором.

Эта атака работает следующим образом:
- В начале читается очередное слово из исходного словаря.
- В соответствии с заданным диапазоном символов и минимальной/максимальной длиной диапазона, генерируются все возможные варианты.

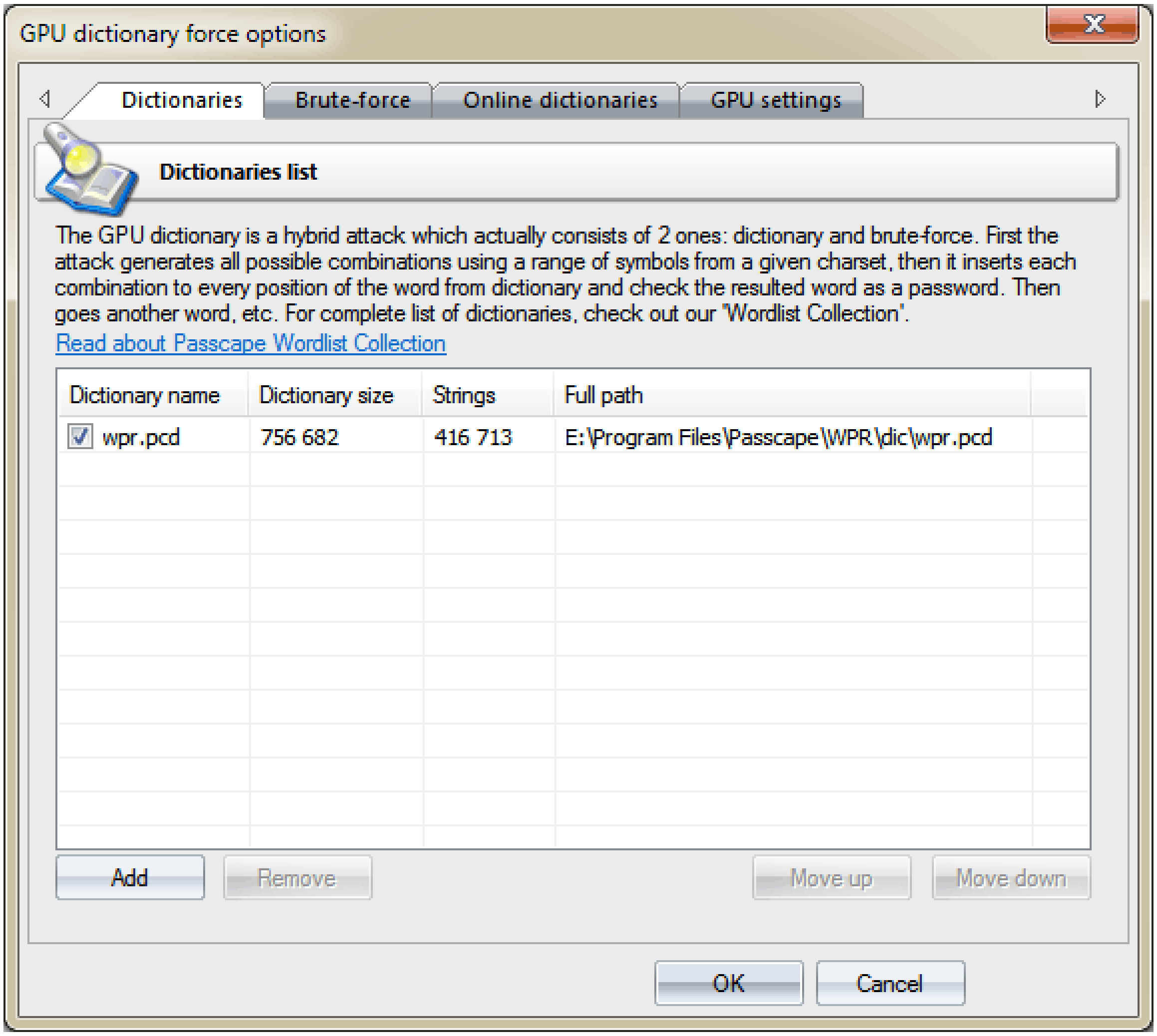
- Эти варианты (символы) вставляются в начало, конец или середину слова. Местоположение в слове, куда будут вставляться генерируемые последовательности может задаваться опционально.
- Полученные таким образом множественные варианты слова проверяются на предмет совпадения с искомым паролем.

Например, если задан диапазон символов для перебора от **0** до **9** и длина этого диапазона от **1** до **2**, то программа создаст 100 вариантов символов: 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11 .. 99. Затем эти последовательности будут добавлены в начало, середину и конец слова. Так, для слова **test**, если последовательности будут вставляться в каждую позицию, программа проверит следующие пароли:
0test, 1test .. 99test
t0est, t1est .. t99est
te0st, te1st .. te99st
tes0t, tes1t .. tes99t
test0, test1 .. test99
Всего - 100*5=500 вариантов.

Рассмотрим подробнее настройки атаки.

Словари

Во вкладке **Словари** задается список словарей для атаки. Поддерживаются текстовые словари в формате ASCII, UNICODE, UTF8, RAR, ZIP, а также зашифрованные\упакованные словари в родном формате PCD, разработанным нашей компанией. Для деактивации словаря достаточно сбросить соответствующую галочку напротив его имени. В этом случае, он будет проигнорирован во время атаки. Вместе с программой поставляется используемый по-умолчанию словарь на 400000 слов. Полный набор из более чем 7.5 Гб словарей можно заказать для доставки на CD, либо использовать online словари.



The GPU dictionary is a hybrid attack which actually consists of 2 ones: dictionary and brute-force. First the attack generates all possible combinations using a range of symbols from a given charset, then it inserts each combination to every position of the word from dictionary and check the resulted word as a password. Then goes another word, etc. For complete list of dictionaries, check out our 'Wordlist Collection'.

Read about Passcape Wordlist Collection

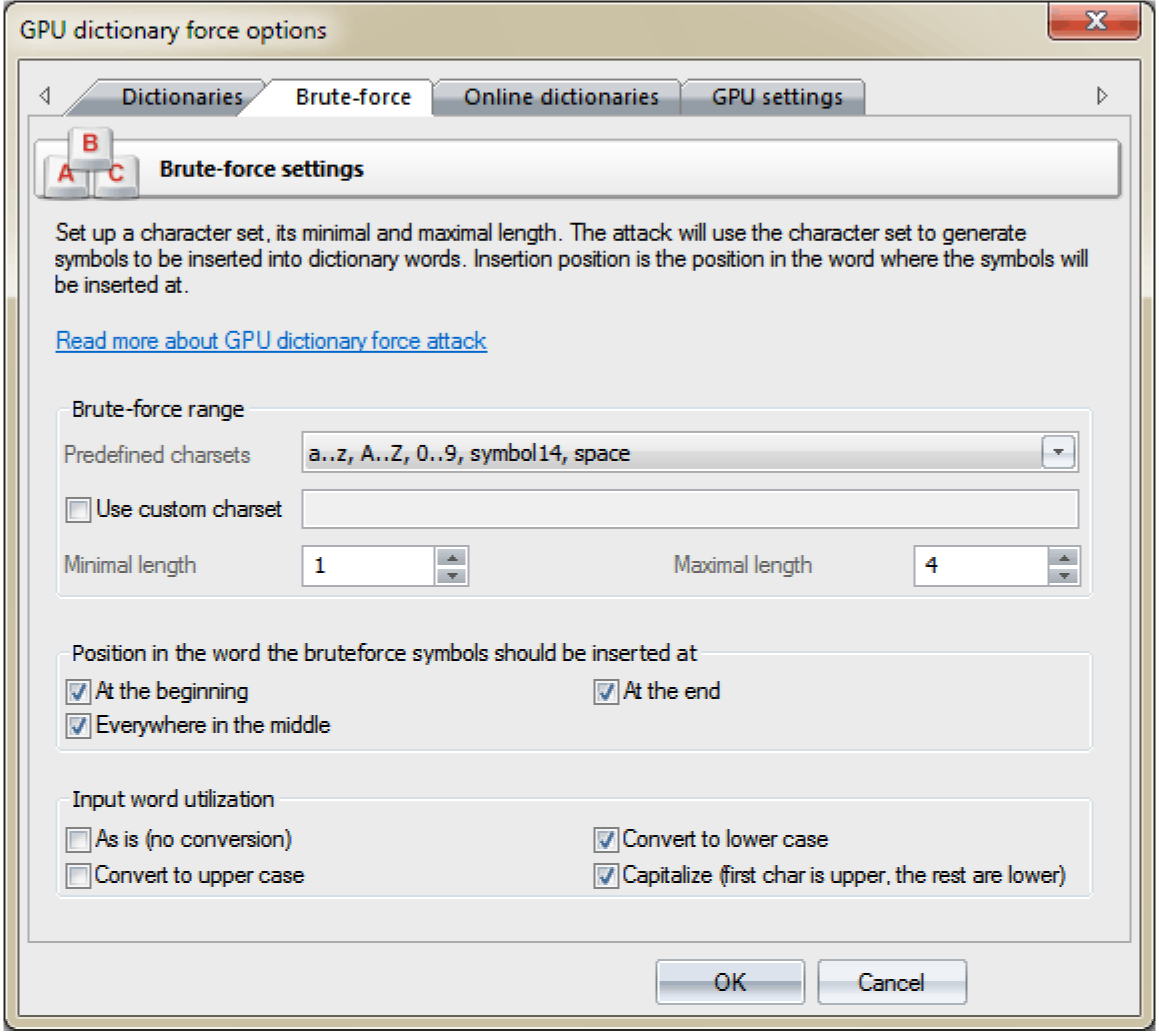
Dictionary name	Dictionary size	Strings	Full path
☑ wpr.pcd	756 682	416 713	E:\Program Files\Passcape\WPR\dic\wpr.pcd

Диапазон для перебора

В этой вкладке необходимо настроить диапазон символов, вставляемый в слова, его минимальную и максимальную длину. При установке диапазона, можно использовать уже имеющиеся заготовки или, установив соответствующую опцию, задавать свой собственный набор. При выборе максимальной длины длины диапазона имейте в виду, что нецелесообразна установка как слишком большого, так и слишком малого значения. Если в первом случае скорость перебора паролей в атаке может упасть до 0, то задание небольшого диапазона перебираемых символов увеличит накладные расходы, связанные с нерациональных использованием вычислительных способностей GPU.

Во второй группе опций необходимо задать местоположение в слове, куда будут вставляться символы перебираемого диапазона.

И, наконец, третья группа настроек отвечает за предварительную обработку слов исходного словаря. Если выставить опцию **As is**, то исходное слово будет использовано как есть, без приведений к верхнему или нижнему регистру букв. Количество перебираемых паролей возрастает прямо пропорционально количеству выставленных в этой группе опций. С другой стороны, программа достаточно умна, чтобы не использовать слова повторно. Например, слово **12345678**, даже если выставлены все опции конвертирования, будет использовано только один раз.



Set up a character set, its minimal and maximal length. The attack will use the character set to generate symbols to be inserted into dictionary words. Insertion position is the position in the word where the symbols will be inserted at.

Read more about GPU dictionary force attack

Brute-force range

Predefined charsets: a..z, A..Z, 0..9, symbol14, space

□ Use custom charset

Minimal length: 1

Maximal length: 4

Position in the word the bruteforce symbols should be inserted at

☑ At the beginning
☑ At the end
☑ Everywhere in the middle

Input word utilization

□ As is (no conversion)
☑ Convert to lower case
□ Convert to upper case
☑ Capitalize (first char is upper, the rest are lower)

Количество перебираемых паролей для одного слова можно рассчитать по следующей формуле:

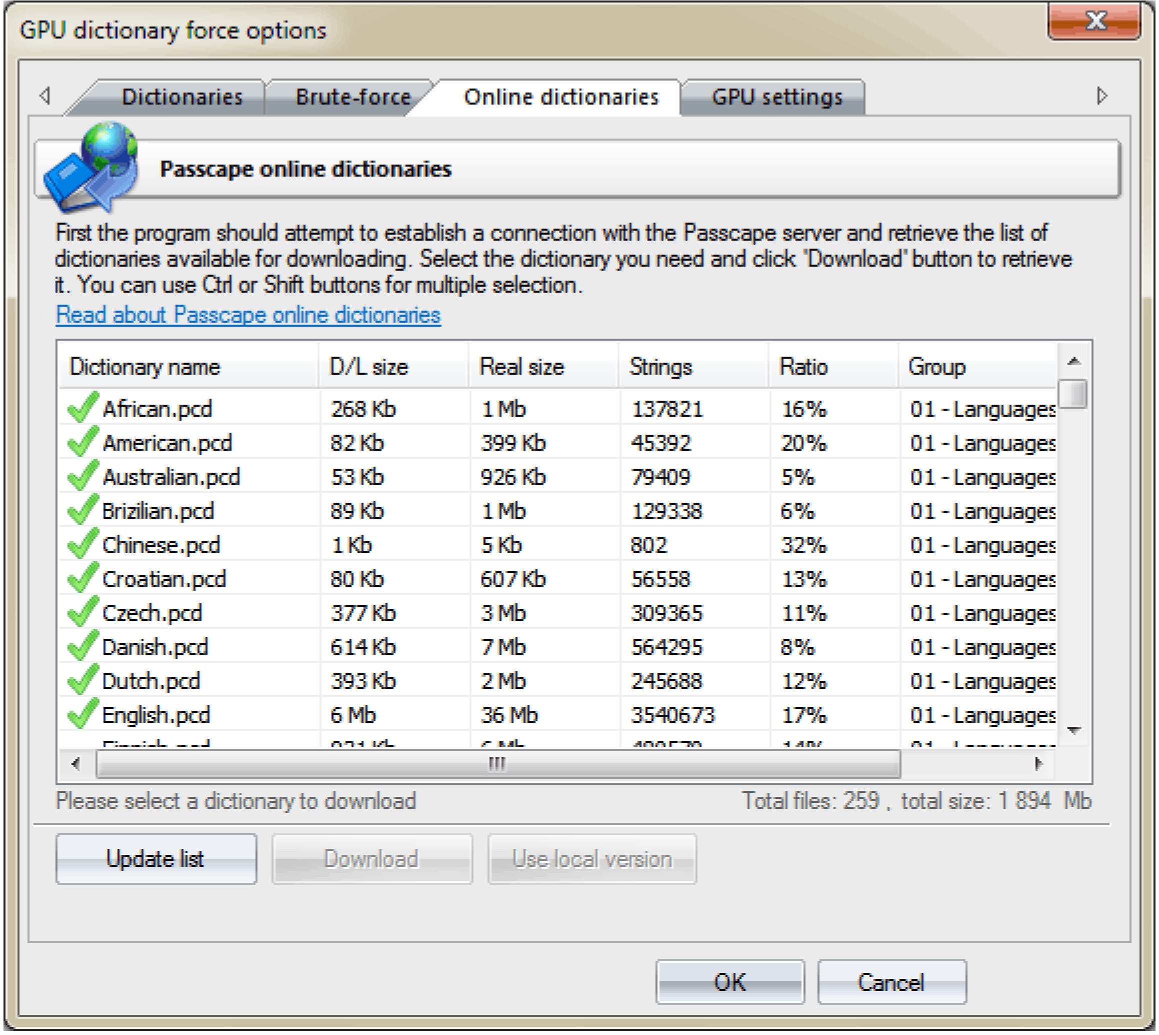
passwords = R * L * K
где
R - диапазон символов, вычисляется по следующей формуле: R = charset_length ^ max_length - charset_length ^ (min_length-1) +1
L - позиции в слове. Рассчитываются так: если задана вставка в середину слова, то L = password_length - 1, затем прибавляем по единице в случае задания вставки в начало или в конец слова.
K - количество установленных опций в группе '**Input word utilization**'.

Например, имеем исходное слово **window** и установленные опции, как на картинке вверху, т.е. диапазон символов **a..z,A..Z,0..9,symbol14,space**, вставка во все позиции, конвертация слова в нижний регистр и капитализация (первая буква заглавная). Подсчитаем количество паролей, которые будут сгенерированы для этого слова:
charset_length = 26+26+10+14+1 = 77
R = 77^4 - 77^0 + 1 = 35153041
L = (6-1) + 1 + 1 = 7

K = 2
passwords = 35153041 * 7 * 2 = **492 142 574**

Онлайн словари

В третьей вкладке можно скачать из сети Интернет исходные словари для Словарной атаки на GPU. По умолчанию используется внутренний словарь на 400000+ слов.



Passcape online dictionaries

First the program should attempt to establish a connection with the Passcape server and retrieve the list of dictionaries available for downloading. Select the dictionary you need and click 'Download' button to retrieve it. You can use Ctrl or Shift buttons for multiple selection.

Read about Passcape online dictionaries

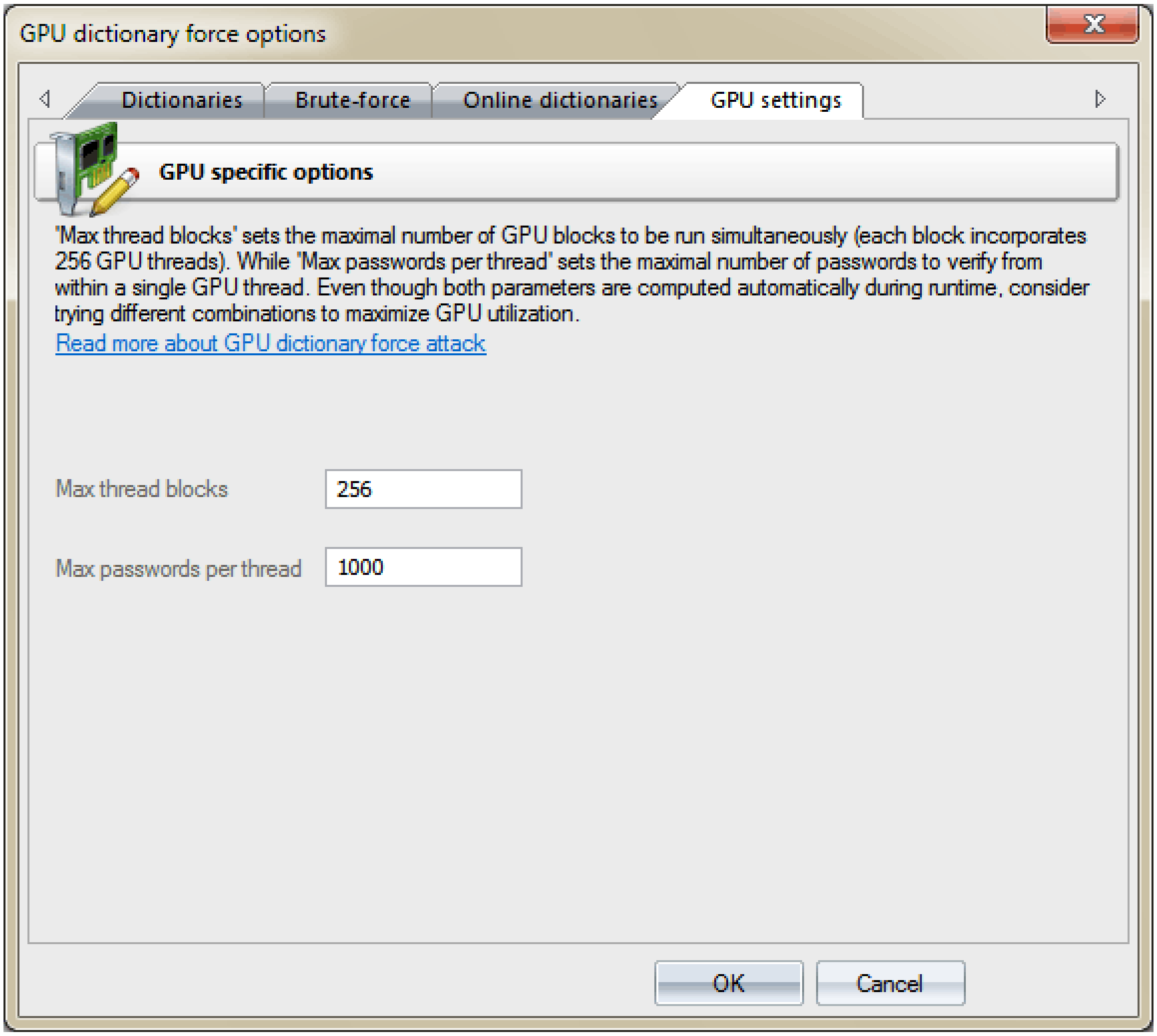
Dictionary name	D/L size	Real size	Strings	Ratio	Group
✓ African.pcd	268 Kb	1 Mb	137821	16%	01 - Languages
✓ American.pcd	82 Kb	399 Kb	45392	20%	01 - Languages
✓ Australian.pcd	53 Kb	926 Kb	79409	5%	01 - Languages
✓ Brizilian.pcd	89 Kb	1 Mb	129338	6%	01 - Languages
✓ Chinese.pcd	1 Kb	5 Kb	802	32%	01 - Languages
✓ Croatian.pcd	80 Kb	607 Kb	56558	13%	01 - Languages
✓ Czech.pcd	377 Kb	3 Mb	309365	11%	01 - Languages
✓ Danish.pcd	614 Kb	7 Mb	564295	8%	01 - Languages
✓ Dutch.pcd	393 Kb	2 Mb	245688	12%	01 - Languages
✓ English.pcd	6 Mb	36 Mb	3540673	17%	01 - Languages

Please select a dictionary to download

Total files: 259 , total size: 1 894 Mb

Установки графической карты

Перед использованием ее в атаке, графическую карту необходимо выбрать в соответствующем пункте общего меню.



'Max thread blocks' sets the maximal number of GPU blocks to be run simultaneously (each block incorporates 256 GPU threads). While 'Max passwords per thread' sets the maximal number of passwords to verify from within a single GPU thread. Even though both parameters are computed automatically during runtime, consider trying different combinations to maximize GPU utilization.

Read more about GPU dictionary force attack

Max thread blocks: 256

Max passwords per thread: 1000

Настройка графической карты состоит из двух частей:
1. Установка количество параллельных блоков графической карты, в которых будет осуществляться поиск паролей. Каждый блок состоит из 256 потоков. Таким образом, если задать количество блоков равным 256, то каждый раз на GPU будет запущено 256*256=65536 потоков. А общее количество проверяемых паролей за один запуск GPU кернела будет составлять 256*ThreadBlocks*PasswordsPerThread, т.е. в нашем случае, 256*256*1000= 65 536 000 паролей. Рекомендуется всегда устанавливать значение **Thread Blocks** кратным 64. Установка этого параметра меньше 256 на современных графических картах в большинстве случаев приводит к снижению производительности.
2. Установка максимального количества паролей, обрабатываемые в одном потоке GPU. Чем выше это значение, тем меньше накладных расходов, связанных с запуском потоков, обработки переменных и т.д. и, соответственно, тем выше скорость перебора. Однако установка слишком большого значения может привести к зависанию компьютера, голубому экрану смерти, либо к тому, что текущая скорость перебора (во вкладке состояния атаки) начинает "плясать". Это связано с тем, что время выполнения задачи на GPU превышает время обновления текущего состояния атаки. Значение по умолчанию для этого параметра составляет 100.

Для обеспечения оптимальной производительности видеокарт при восстановлении кэшированных паролей домена тип 2 (DCC2), возможно, придется дополнительно изменить параметр '**Thread Blocks**'.

'Password per thread' не используется и всегда равен 1 при восстановлении паролей DCC2. Слишком большие значения **'Thread Blocks'** могут привести в зависанию или ошибкам GPU, в зависимости от настроек GPU kernel timeout.

2.8.2.19 GPU: Гибридная Атака по Словарям

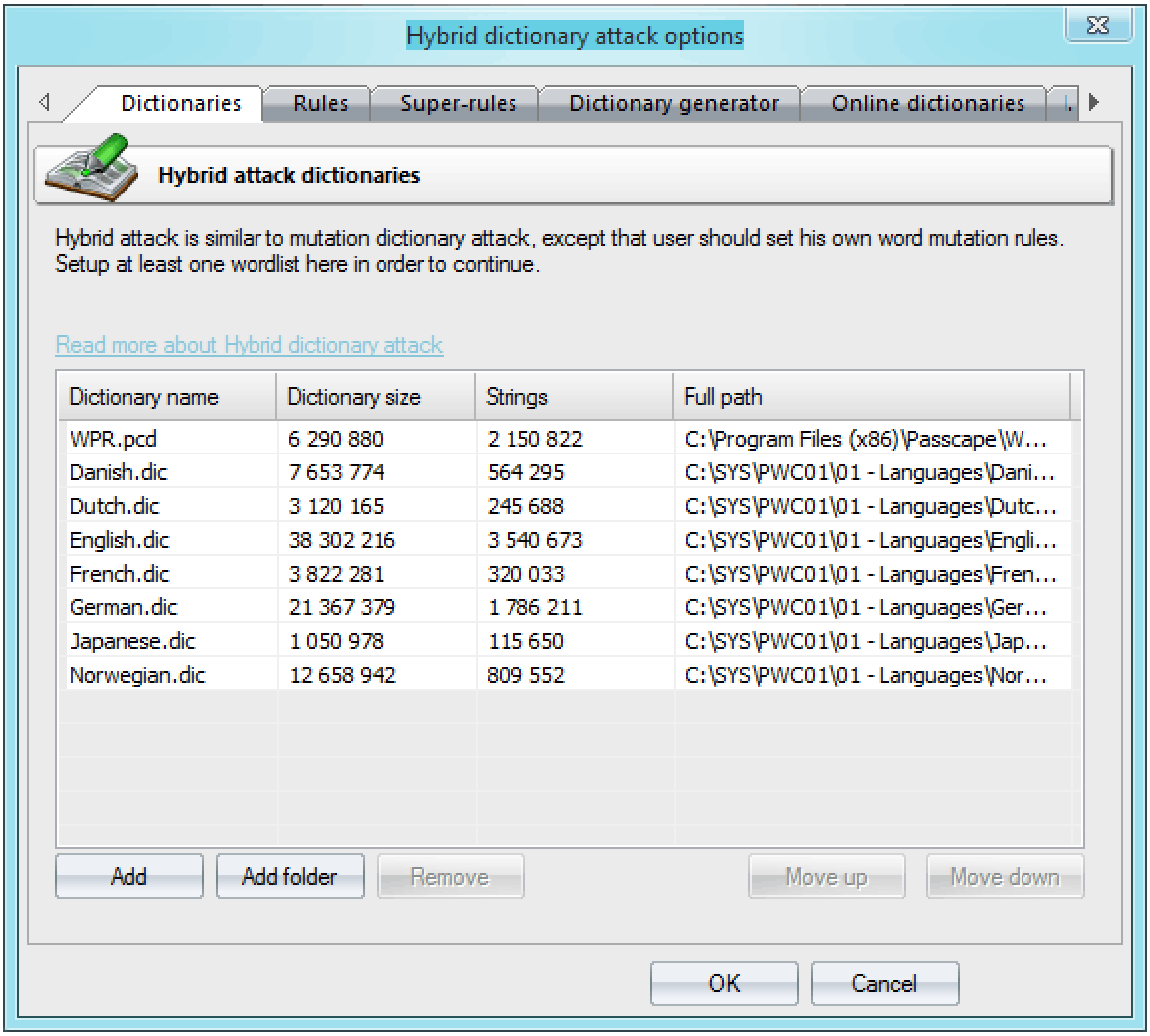
Гибридная атака по словарю на GPU - аналогична простой гибридной атаке за тем лишь исключением, что перебор паролей происходит на видеокарте. Это позволяет увеличить скорость перебора паролей в среднем ~10 раз по сравнению с обычной гибридной атакой. Хотя финальные цифры в значительно степени зависят от настроек атаки и используемого оборудования.

Действия, применяемые к исходным словам словаря, называются правила. К одному исходному слову можно применять несколько правил.

Опции гибридной атаки состоят из восьми вкладок:

1. **Словари** - для задания исходных словарей
2. **Правила** - выбор файлов с наборами правил
3. **Супер-правила -** правила, которые можно применить поверх всех обычных (до или после них)
4. **Генератор словарей**, в которой можно создавать свои собственные словари, получаемые в результате работы этой атаки
5. **Онлайн словари** - для скачивания новых словарей в программу с нашего сайта
6. **Синтаксис атаки** - полное описание всех правил с примерами
7. **Тестер правил** для тестирования и проверки новых правил
8. **Опции GPU**. Настройка параметров для работы GPU.

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



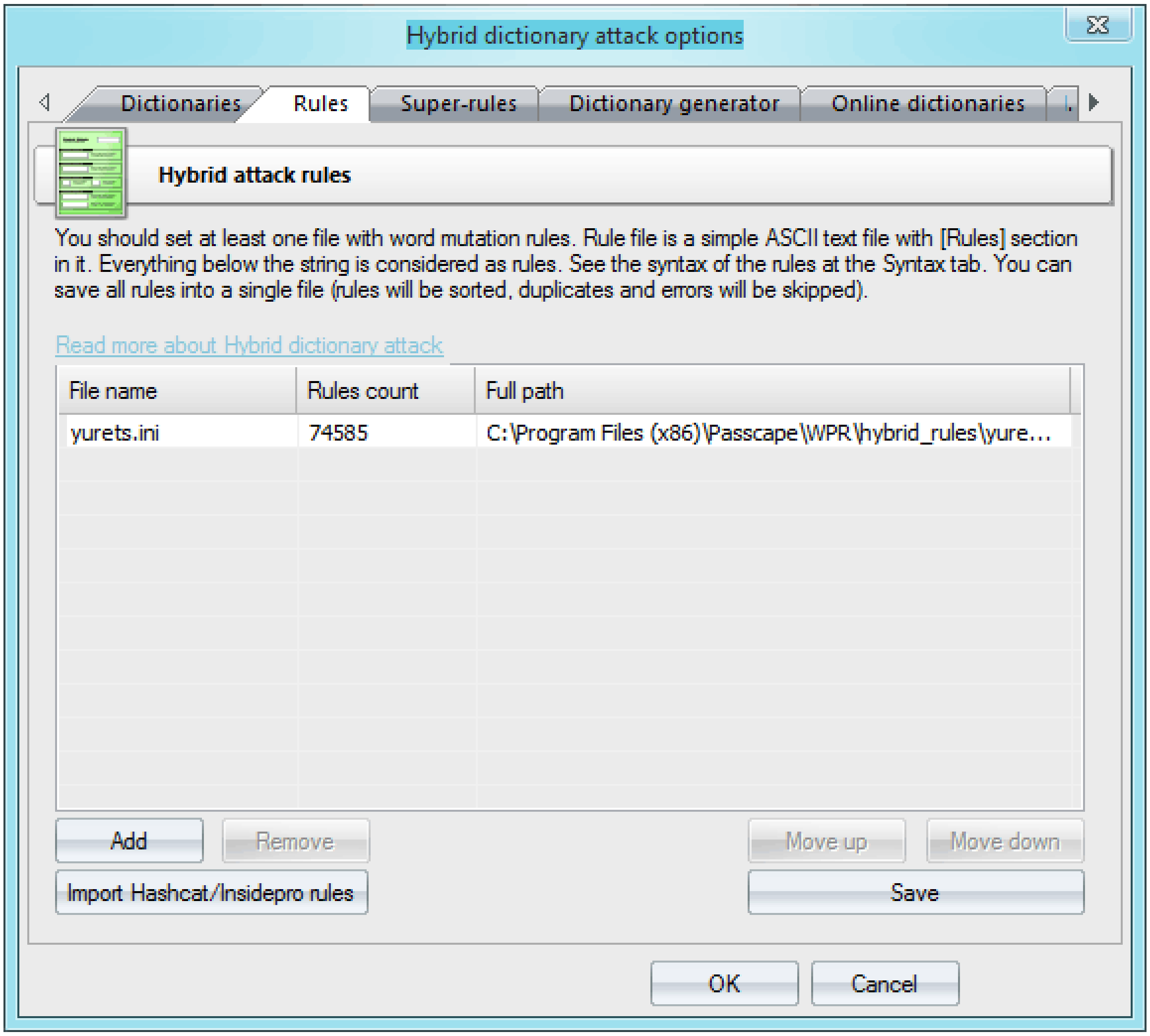
Hybrid attack dictionaries

Hybrid attack is similar to mutation dictionary attack, except that user should set his own word mutation rules. Setup at least one wordlist here in order to continue.

Read more about Hybrid dictionary attack

Dictionary name	Dictionary size	Strings	Full path
WPR.pcd	6 290 880	2 150 822	C:\Program Files (x86)\Passcape\W...
Danish.dic	7 653 774	564 295	C:\SYS\PWC01\01 - Languages\Dani...
Dutch.dic	3 120 165	245 688	C:\SYS\PWC01\01 - Languages\Dutc...
English.dic	38 302 216	3 540 673	C:\SYS\PWC01\01 - Languages\Engli...
French.dic	3 822 281	320 033	C:\SYS\PWC01\01 - Languages\Fren...
German.dic	21 367 379	1 786 211	C:\SYS\PWC01\01 - Languages\Ger...
Japanese.dic	1 050 978	115 650	C:\SYS\PWC01\01 - Languages\Jap...
Norwegian.dic	12 658 942	809 552	C:\SYS\PWC01\01 - Languages\Nor...

Во вкладке *'Правила'* необходимо задать по крайней мере один файл с правилами генерации (мутации) паролей. С программой поставляется несколько файлов, например, **english_words.ini** с более чем 3000 правилами. Формат файла с правилами довольно прост и представляет собой текстовый ASCII файл со строкой **[Rules]**. Все, что идет 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.



Hybrid attack rules

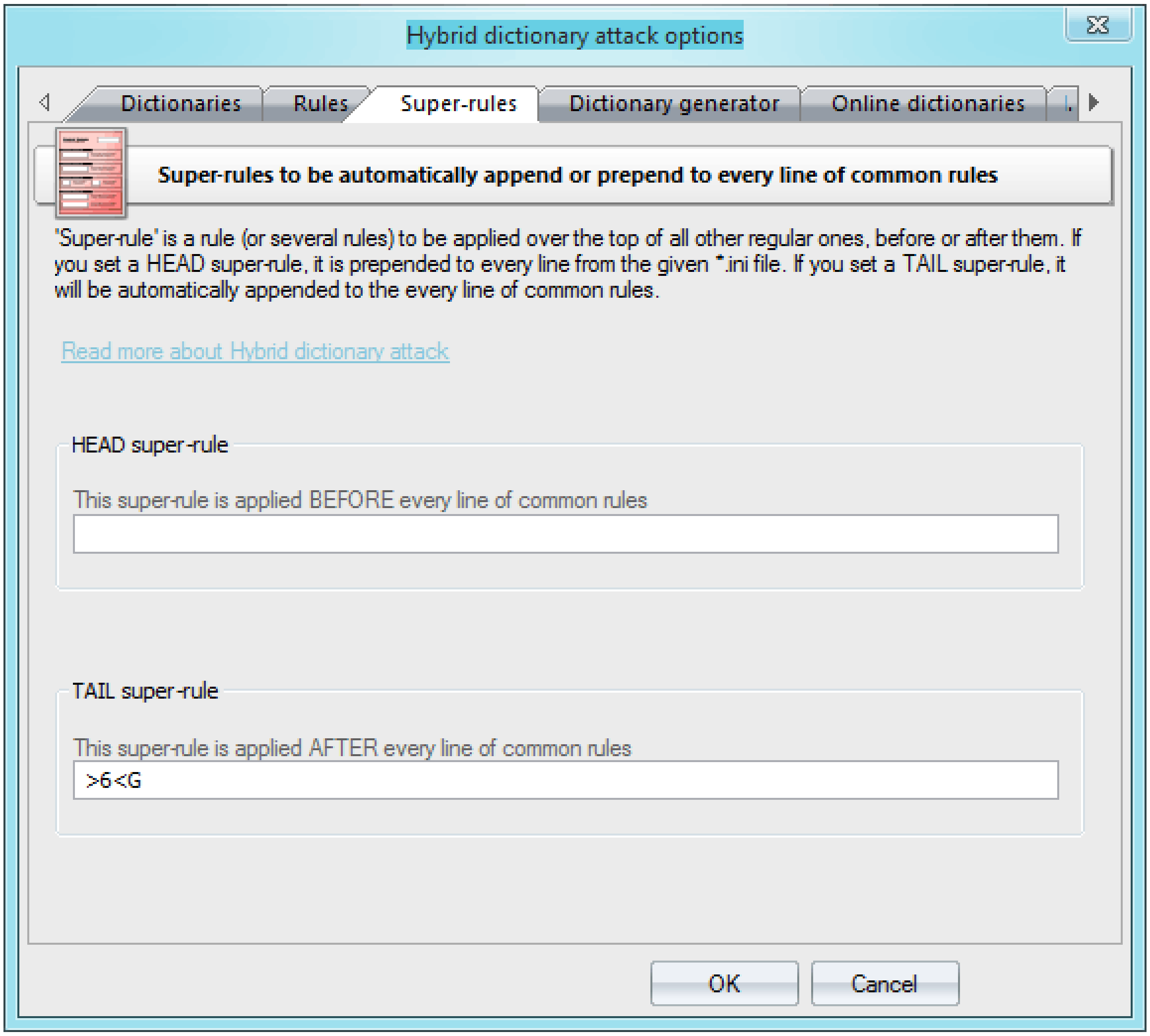
You should set at least one file with word mutation rules. Rule file is a simple ASCII text file with [Rules] section in it. Everything below the string is considered as rules. See the syntax of the rules at the Syntax tab. You can save all rules into a single file (rules will be sorted, duplicates and errors will be skipped).

Read more about Hybrid dictionary attack

File name	Rules count	Full path
yurets.ini	74585	C:\Program Files (x86)\Passcape\WPR\hybrid_rules\yure...

Супер-правило - это одно или несколько правил, которые необходимо применить поверх всех обычных правил. 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. Еще один пример: если установить начальное супер-правило '>6<G', то до начала обычной мутации будут отклонены все слова меньше 6 или больше 16 символов.

Это довольно полезная опция. Если вы решите применить какое-либо правило ко всем строкам заданных *.ini файлов, нет необходимости править в них все текстовые строки. Будьте аккуратны: супер-правило 'aN' может увеличить число генерируемых паролей в сотни или даже тысячи раз!



Super-rules to be automatically append or prepend to every line of common rules

'Super-rule' is a rule (or several rules) to be applied over the top of all other regular ones, before or after them. If you set a HEAD super-rule, it is prepended to every line from the given *.ini file. If you set a TAIL super-rule, it will be automatically appended to the every line of common rules.

Read more about Hybrid dictionary attack

HEAD super-rule

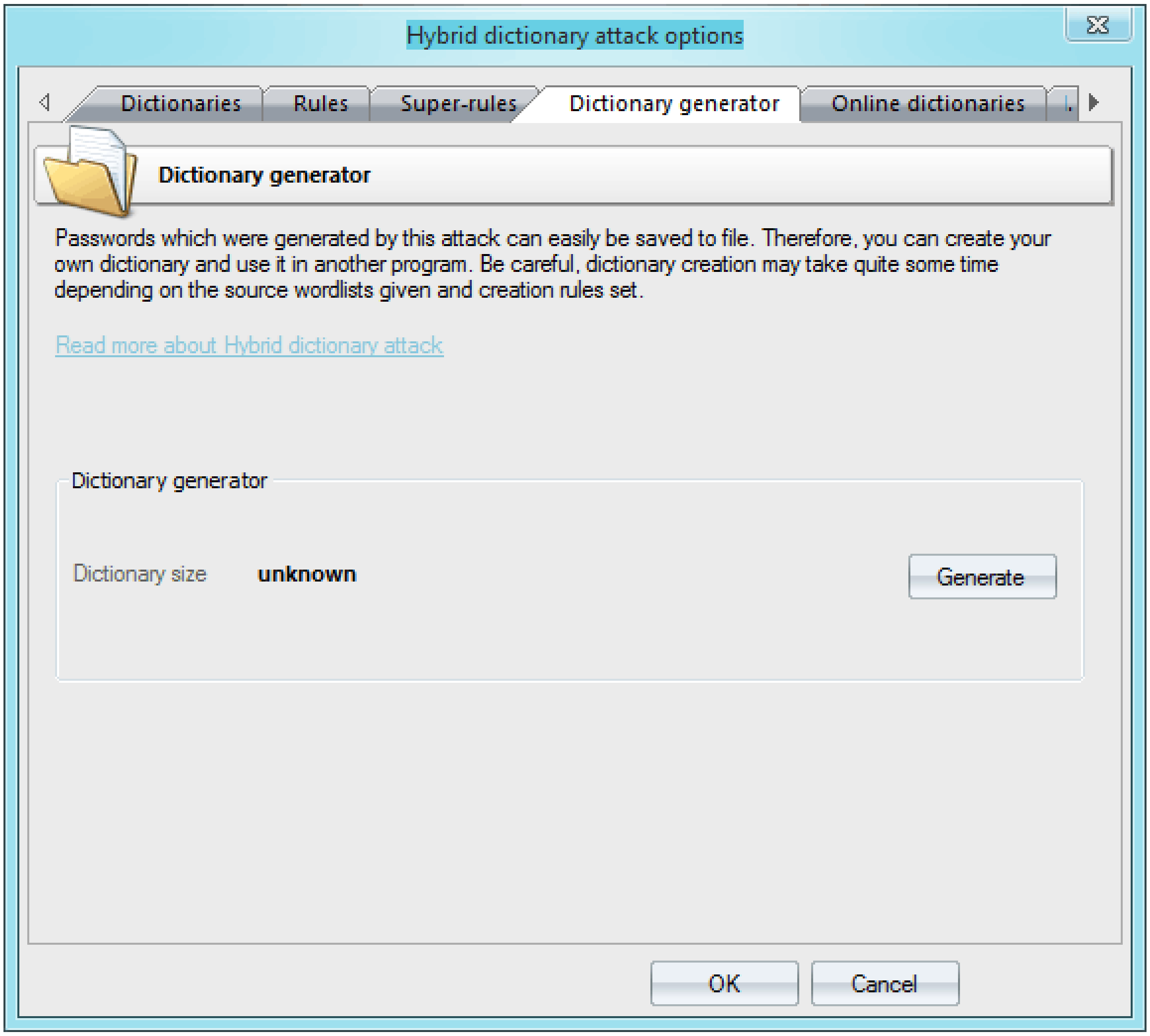
This super-rule is applied BEFORE every line of common rules

TAIL super-rule

This super-rule is applied AFTER every line of common rules

>6<G

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 при условии, что он находится на NTFS разделе диска. Будьте осторожны, процесс создания словаря может занять значительное время!



Dictionary generator

Passwords which were generated by this attack can easily be saved to file. Therefore, you can create your own dictionary and use it in another program. Be careful, dictionary creation may take quite some time depending on the source wordlists given and creation rules set.

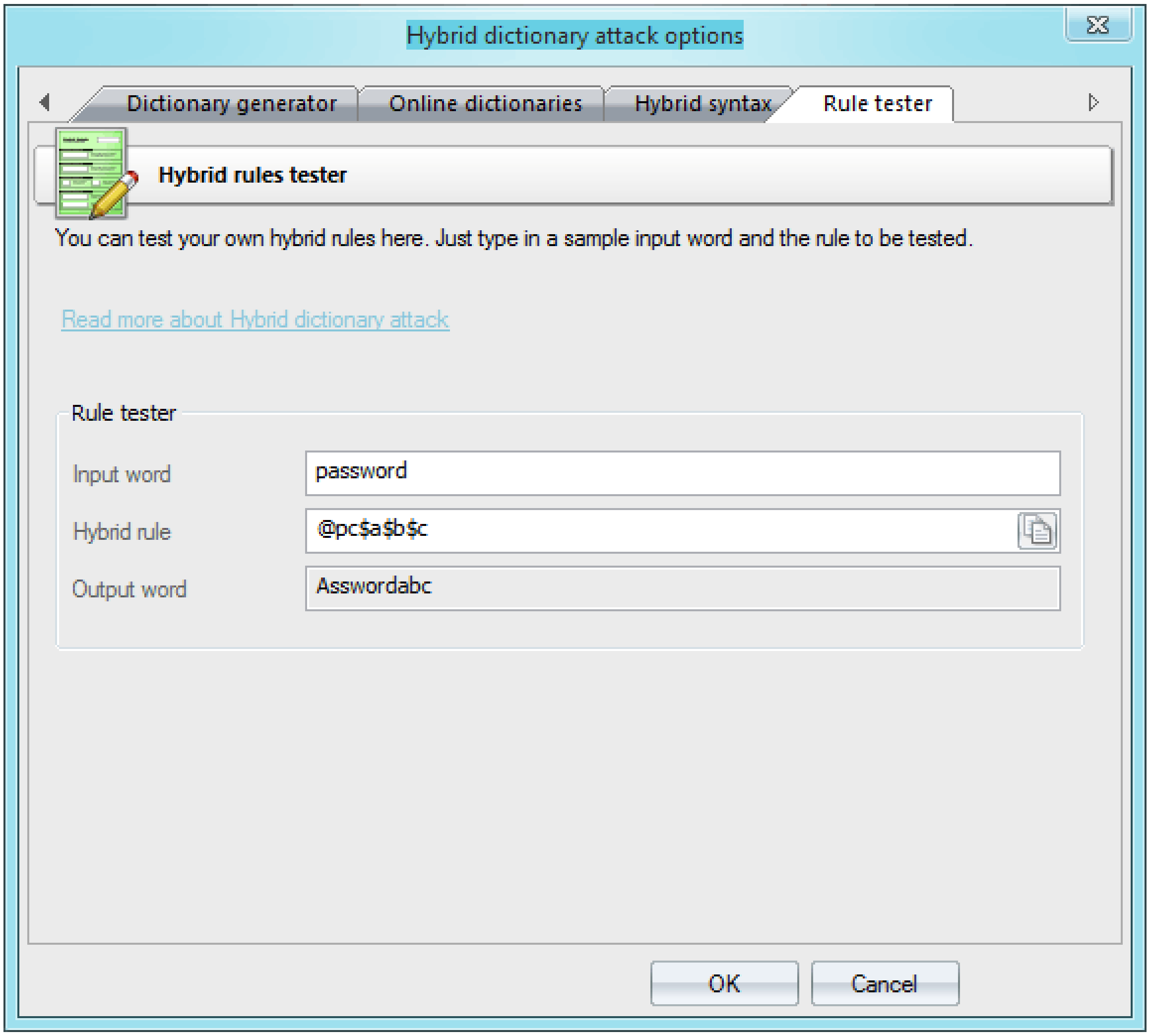
Read more about Hybrid dictionary attack

Dictionary generator

Dictionary size **unknown**

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.



Hybrid rules tester

You can test your own hybrid rules here. Just type in a sample input word and the rule to be tested.

Read more about Hybrid dictionary attack

Rule tester

Input word: password

Hybrid rule: @pc$a$b$c

Output word: Asswordabc

Описание синтаксиса правил гибридной атаки по словарю

Допускается задавать несколько правил на одной строке.
Обработка правил (если их несколько на одной строке) идет 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 коментарием 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.
Следующие правила должны быть последними в строке: aN, ?iN[C], ?i[C], ?oN[C], ?o[C], ?iZ[C], ?oZ[C]
Не меняйте имена стандартных файлов с правилами. Некоторые из них используются программой.
Правила ?iN[C], ?i[C], ?oN[C], ?o[C] ?iZ[C], ?oZ[C] используют следующие встроенные наборы символов (также можно задавать свои собственные):

digits	- 0123456789
loweralpha	- abcdefghijklmnopqrstuwxyz
upperalpha	- ABCDEFGHIJKLMNOPQRSTUVWXYZ
alpha	- abcdefghijklmnopqrstuwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ

special - !@#$%^&*()-_+=~`[]{}|\:;"'<>,.?/ "
loweralphanumeric - abcdefghijklmnopqrstuwxyz0123456789
upperalphanumeric - ABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789
alphanumeric - abcdefghijklmnopqrstuwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789
printable - abcdefghijklmnopqrstuwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789!@#$%^&*()-_+=~`[]{}|\:;"'<>,.? /

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
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

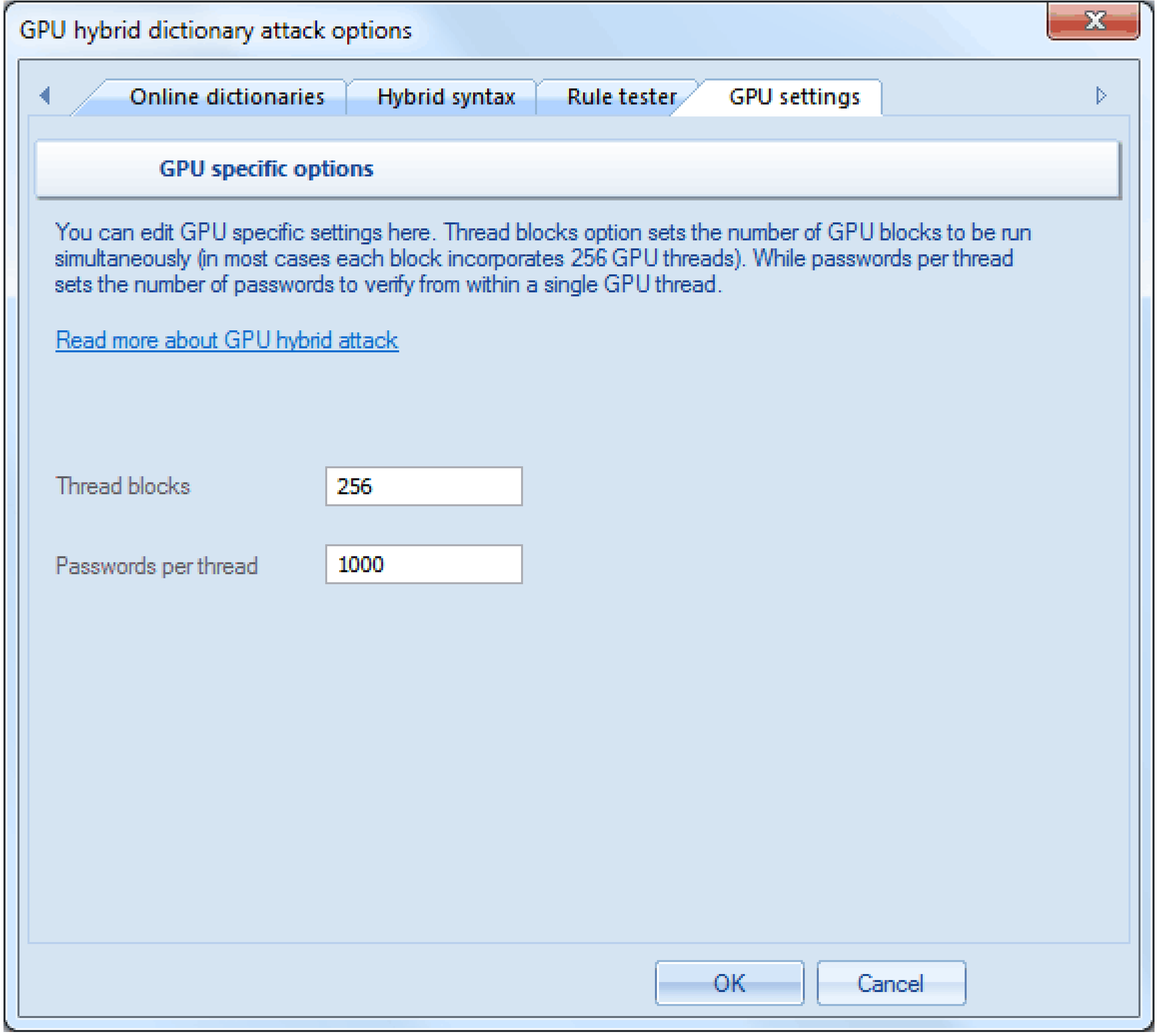
Правило	Пример	Вход. слово	Выход. слово	Описание правила
'N	'4	password	pass	Обрезать слово до длины N
+N	+1	password	pbssword	Увеличить значение ASCII символа в позиции N
-N	-0	password	oassword	Уменьшить значение ASCII символа в позиции N
.N	.4	password	passoord	Заменить символ в позиции N символом 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 задает 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	paspasword	Продублировать первые N символов
YN	Y3	password	paswordord	Продублировать последние N символов
zN	z3	password	ppppassword	Дублировать первый символ слова N раз
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)

Правило	Пример	Вход. слово	Выход. слово	Описание правила
%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.
RNM+Y	R01+a	password	assword	Удалить символ в позиции N, если символ в позиции M равен Y
RNM-Y	R40-b	password	passord	Удалить символ в позиции N, если символ в позиции M не равен Y
? iN[C]	? i0[digits]	password	0password, 1password … 9password	Вставить символ из набора [C] в позицию N входного слова.
? iZ[C]	? iZ[digits]	password	password0, password1 … password9	Вставить символ из набора [C] в последнюю позицию слова.
?i[C]	? i[special]	password	~password, !password … password_, password+	Вставить символ из набора [C] в каждую позицию слова.
? oN[C]	? o1[upperalpha]	password	pAssword, pBssword … pZssword	Перезаписать символ в позиции N символом из набора [C].
? oZ[C]	? oZ[upperalpha]	password	passworA, passworB … passworZ	Перезаписать символ в последней позиции слова символом из набора [C].
?o[C]	?o[-=.]	password	-assword, =assword	Перезаписать символ в каждой позиции слова символом из набора [C].

Правило	Пример	Вход. слово	Выход. слово	Описание правила
			... passwor.	

Установки графической карты

Перед использованием ее в атаке, графическую карту необходимо выбрать в соответствующем пункте общего меню.



You can edit GPU specific settings here. Thread blocks option sets the number of GPU blocks to be run simultaneously (in most cases each block incorporates 256 GPU threads). While passwords per thread sets the number of passwords to verify from within a single GPU thread.

Read more about GPU hybrid attack

Thread blocks: 256

Passwords per thread: 1000

Настройка графической карты состоит из двух частей:

1. Установка количество параллельных блоков графической карты, в которых будет осуществляться поиск паролей. Каждый блок состоит из 256 потоков. Таким образом, если задать количество блоков равным 256, то каждый раз на GPU будет запущено 256*256=65536 потоков. А общее количество проверяемых паролей за один запуск GPU кернела будет составлять 256*ThreadBlocks*PasswordsPerThread, т.е. в нашем случае, 256*256*1000= 65 536 000 паролей. Рекомендуется всегда устанавливать значение **Thread Blocks** кратным 64. Установка этого параметра меньше 256 на современных графических картах в большинстве случаев приводит к снижению производительности.

2. Установка максимального количества паролей, обрабатываемые в одном потоке GPU. Чем выше это значение, тем меньше накладных расходов, связанных с запуском потоков, обработки

переменных и т.д. и, соответственно, тем выше скорость перебора. Однако установка слишком большого значения может привести к зависанию компьютера, голубому экрану смерти, либо к тому, что текущая скорость перебора (во вкладке состояния атаки) начинает "плясать".

Используйте 'тяжелые' правила (например, aN, ?iN, ?oN и т.д.) особенно аккуратно. Эти правила увеличивают количество проверяемых паролей в сотни и даже тысячи раз, что может привести к зависанию системы или неработоспособности программы. Смотрите также опции атак при расшифровке DCC2.

Для обеспечения оптимальной производительности видеокарт при восстановлении кэшированных паролей домена тип 2 (DCC2), возможно, придется дополнительно изменить параметр '**Thread Blocks**'.
'**Password per thread'** не используется и всегда равен 1 при восстановлении паролей DCC2.
Слишком большие значения '**Thread Blocks'** могут привести в зависанию или ошибкам GPU, в зависимости от настроек GPU kernel timeout.

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.

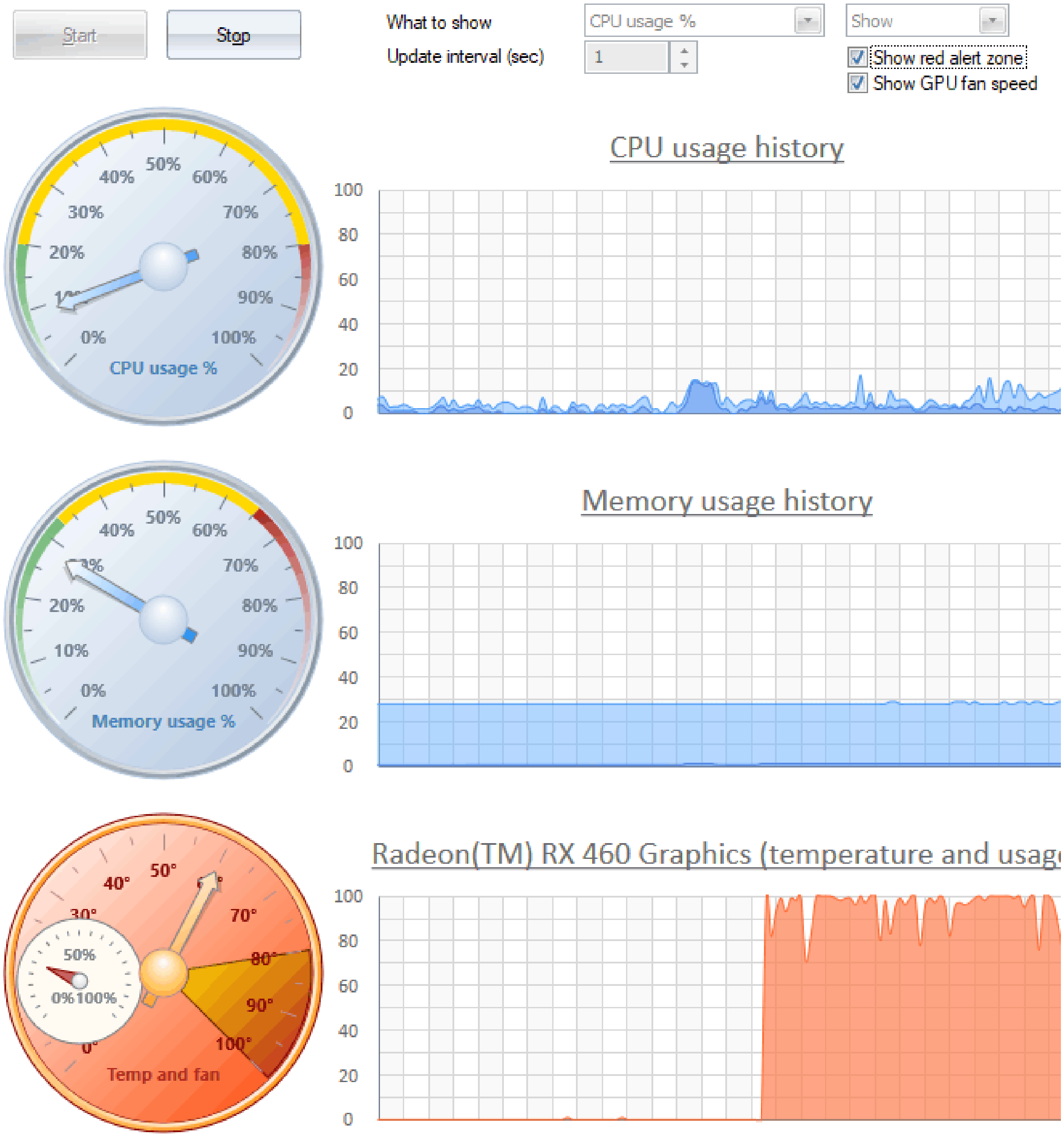
2.10 Меню Темы

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 Windows Password Recovery и др.

2.12 Системный монитор



What to show: CPU usage %
Update interval (sec): 1
Show
☑ Show red alert zone
☑ Show GPU fan speed

В этой вкладке можно посмотреть текущую загруженность процессора, использование физической памяти, температуру и загрузку видеокарт. По умолчанию, интервал обновления составляет 2 секунды. Будьте внимательны, сбор этой статистики тоже отнимает процессорное время, поэтому в "тяжелых" атаках, например, перебором, рекомендуется отключать системный монитор.

Работа с программой

3 Работа с программой

3.1 Атаки на Хэши

В настоящее время, программа использует разные подходы для подбора парольных хэшей Windows:

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 из хэшей, 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 трехсимвольного 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 определенная 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 трехзначное 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 наборы словарей с фразами и словосочетаниями. Данные словари можно скачать только с нашего сайта.

Rainbow attack (разработана Philippe Oechslin). Является современным, продвинутым инструментом для аудите паролей. Данный метод использует предвычисленные таблицы для быстрого поиска паролей.

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 на больших списках хэшей и хэшах истории 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.

Online recovery (впервые разработана в Passcape Software) производит поиск паролей на поисковых серверах Интернет. Неплохо справляется с простыми, короткими и часто-употребляемыми паролями. Из недостатком можно отметить небольшую скорость работы, плохо подходит для больших списков хэшей.

Passcape rainbow tables attack (разработана в Passcape Software). Эта атака является дальнейшим развитием атаки по простым радужным таблицам. Однако подбор паролей в Passcape таблицах осуществляется не в заданном диапазоне символов, а в диапазоне т.н. отпечатков слов, позволяя осуществлять поиск осмысленных комбинаций и сложных паролей практически неограниченной длины.

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

GPU brute-force attack. Атака полным перебором на видеокарте. Используемая в процессе работы графическая карта задается в меню *Общие настройки*.

GPU fingerprint attack. Разработанный нашей компанией, довольно эффективный метод восстановления сложных паролей, которые невозможно подобрать с помощью обычных атак. Перебор паролей осуществляется на графической карте.

GPU mask attack. Этот метод восстановления паролей аналогичен обычной атаке по маске за тем лишь исключением, что подбор паролей осуществляется на графической карте ПК. Соответственно, скорость перебора паролей будет значительно выше.

GPU dictionary-force. Атака по словарю с перебором (разработана нашей компанией), как уже ясно из ее названия, является чем-то средним между словарным и грубым перебором. При этом в каждое слово исходного словаря вставляется диапазон перебираемых символов. Таким образом происходит поиск словарных паролей, в начало, конец или даже середину которых вставлен один или несколько произвольных символов.

GPU Hybrid dictionary attack. Эта атака аналогична простой гибридной атаки за исключением того, что перебор паролей осуществляется на видеокартах.

3.2 Сравнительная Таблица Атак

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

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	Пара 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, не требует	Практически бесполезна для серьезного 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 той же системе, откуда были взяты пароли	Min: 2-3 минуты Max: около часа и более	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 пользователь в своей системе	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)
Полным перебором	Перебор всех возможных комбинаций из заданного набора символов	Зависит от выбранных опций	да	Единственная атака (наряду с атакой по маске), которая гарантированно восстанавливает полностью неизвестный пароль. Хороша для любых коротких и средних паролей	Перебор длинных паролей занимает значительное время. Сложно угадать правильный диапазон перебираемых символов	Может занять века для перебора длинных паролей. Не находит пароли, если неправильно задан набор символов или длина пароля превышает заданную

Словарная	Поиск паролей путем последовательного перебора слов из готовых словарей (списков слов)	Практически мгновенно	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 найдется если неправильно задан набор символов, длина пароля или неправильно задана известная часть исходного пароля
Комбинированная	Проверка сложных паролей (в основе которых два или более слов) путем склейки слов из нескольких словарей	Зависит от выбранных опций	нет	Находит длинные и сложные пароли	Ограниченный набор специализированных словарей, не учитываются особенности не-английских паролей (окончания, суффиксы и т.д.).	Требуется заранее знать, что в основе искомого пароля лежат два или более слов,

					Если задан большой исходный словарь, то атака может занять длительное время	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	Пару секунд (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 некоторое время.	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 часов	нет	Единственная атака против фраз.	Фразы в качестве паролей использует небольшой процент пользователей. Мутация фраз несовершенна, мутация и анализ занимают значительное время. Недостаточно соответствующих словарей, в частности, с неанглийскими фразами и выражениями	Не учитываются особенности языка, ограниченный набор мутаций. Сложность в создании специализированных словарей
По предвычисленным таблицам	Атака на основе предвычисленных таблиц	Обычно несколько минут (секунд) для каждого пароля	Вероятность близкая к 100%, если пароль лежит	В настоящее время одна из лучших атак для восстановления большинства паролей по показателю время/эффективность	Требуются таблицы. Таблицы предвычислений могут занять много места на жестком диске. Длинные пароли с помощью данной атаки	Не может восстанавливать все пароли одновременно, генерация новых таблиц занимает больше

			в заданном диапазоне символов и длины		восстановить невозможно	времени, чем атака полным перебором. Ограниченные возможности восстановления длинных и не-английских паролей
Идентификационная атака	Атака на основе предварительно сгенерированных отпечатков слов из исходного словаря	От нескольких минут до бесконечности, в зависимости от размера исходного словаря	нет	Находит сложные пароли, которые невозможно подобрать в других атаках	Большие словари генерируют такое кол-во отпечатков, которое сложно обработать за разумное время. Успех сильно зависит от качества исходного словаря.	Требует очень много времени, если задать большой словарь
Гибридная по словарю	Аналогично словарной атаке, но каждое слово из словаря подвергается мутациям, которые задает пользователь. Например, можно добавить цифру в конец слова, измененить регистр букв и т.д.	Зависит от количества правил мутаций и размера словаря. Как правило, несколько минут 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
Интернет атака	Производит поиск паролей на поисковых серверах Интернет	В зависимости от установленных опций и скорости Интернет соединен	нет	Неплохой, альтернативный обычным атакам инструмент, для обнаружения простых и часто-употребляемых паролей.	Очень медленная, жрет много Интернет трафика.	Не находит большинство сложных паролей. Работает только при наличии Интернет соединения.

		ия. В среднем, менее минуты для каждого хэша.				
По предвычисленным таблицам Passcape	Атака на основе радужных таблиц Passcape	Обычно несколько минут (секунд) для одного пароля	нет	Одна из лучших атак для восстановления сложных паролей, недоступных для восстановления в других атаках.	Предвычисленные таблицы могут занять много места на жестком диске. Атака по таблицам использует очень много ресурсов компьютера. Для создания таблиц необходимы специально подготовленные словари.	Не может восстанавливать все пароли одновременно, генерация новых таблиц занимает больше времени, чем атака полным перебором. Не все исходные словари одинаково хорошо подходят для создания таблиц.

3.3 Восстановление паролей из хэшей (общая инструкция)

Используйте эту простую инструкцию для восстановления любых паролей в программах Passcape Software. Данная инструкция носит рекомендательный характер и предназначена прежде всего для восстановления паролей, зашифрованных при помощи OWF, например хэшей Windows.

При восстановлении некоторых видов паролей, например паролей пользователей Windows, встает главный вопрос: как наиболее оптимально организовать процесс восстановления, с какой атаки лучше начать для повышения вероятности успешного завершения ?

Для выбора типа и последовательности атак, рекомендуем пользоваться следующим алгоритмом, который применим в большинстве случаев ко всем типам восстанавливаемых паролей:

Во-первых, включите опцию предварительной атаки, если таковая имеется в программе. Она поможет восстановить простые и часто встречающиеся комбинации.

Во-вторых, отметьте несколько хэшей, необходимые расшифровать в первую очередь, и запустите Интернет атаку, которая должна быстро найти простые и часто-употребляемые пароли.

Во-третьих, если вам известно что-либо об искомом пароле, для начала запустите атаку по маске, гибридную атаку по словарю, либо атаку по ключевому слову. Причем, если вам известна часть пароля, лучше использовать атаку по маске. Если вы знаете базовую составляющую пароля или, к примеру, знаете исходное слово пароля, но забыли последовательность заглавных и строчных букв, то вам в первую очередь подойдет атака по ключевому слову.

В-четвертых, если никакой информации об искомом пароле нет, а так чаще всего и бывает, руководствуйтесь следующей последовательностью действий.

1. Запуск интеллектуальной атаки с минимальной мутацией и индексацией. Эта атака работает только для хэшей, импортированных с локального компьютера.
2. Повтор интеллектуальной атаки (если предыдущий шаг не увенчался успехом) с установленными опциями мутации и индексации в normal и deep соответственно.
3. Запуск атаки по предвычисленным таблицам (если таковые имеются в наличии).
4. Запуск атаки по предвычисленным таблицам Passcape.
5. Запуск атаки по словарю с отключенной опции мутации.
6. Запуск атаки по словарю с включенной опции мутации, степень которой зависит от наличия свободного времени и скорости атаки. Для поиска паролей, набранных в национальной раскладке, необходимо выставить опцию сильной мутации.
7. Выбор и загрузка онлайн словарей и повтор шагов 5 - 6.
8. Запуск Гибридной атаки по словарю
9. Повтор Гибридной атаки с дополнительными словарями.
10. Запуск атаки по фразе с выключенной опции мутации.
11. Запуск атаки по фразе с включенной опции мутации, установленной на максимальную эффективность. Это позволит найти даже пароли, набранные в национальной раскладке клавиатуры.
12. Выбор и загрузка онлайн словарей фраз и повтор шагов 10 - 11.
13. Запуск комбинированной атаки по словарям с заданными правилами генерации фраз.
14. Выбор и загрузка онлайн словарей для комбинированной атаки повтор шага 13.
15. Запуск Идентификационной атаки со словарем по умолчанию.
16. Выбор и загрузка онлайн словарей для Идентификационной атаки, изменение опций атаки пре необходимости и повтор шага 15.
17. Выбор и установка набора символов для атаки полным перебором, запуск перебора.
18. При необходимости, выбор нового или дополнение старого набора символов и повтор атаки грубой силой, т.е. шага 17.

На основе данных рекомендаций можно легко создать свои собственные правила для групповой атаки.

3.4 FAQ по паролям Windows

В. Что такое парольная защита?

О. Пожалуй, никто не станет спорить о том, что на сегодняшний день операционные системы на базе Windows NT являются самыми популярными в мире. Это делает их весьма уязвимыми мишенями для различного рода хакеров, взломщиков и недобросовестных пользователей. Широкое распространение глобальной сети только усугубляет ситуацию. Чтобы обеспечить персонализацию хранимых данных пользователя или системы и уберечь их от доступа третьих лиц, была придумана технология парольной защиты. В настоящее время, в операционных системах Windows, парольная защита является основной базовой системой защиты. Доступ к приватным данным в этом случае возможен только при знании оригинального пароля, обычно слова или фразы. На практике это выглядит так: программа или система при попытке доступа к защищенным данным запрашивает текстовый пароль. Этот пароль проверяется с оригинальным значением и, если эти значения совпадают, система разрешает доступ к защищенным ресурсам, иначе отклоняет его. Основной недостаток парольной защиты состоит в том, что программе или системе необходимо где-то хранить оригинальный пароль, чтобы в последствие была возможность сравнивать его с вводимыми значениями.

В. Как хранятся пароли в операционной системе?

О. Но не все так плохо, система Windows NT была разработана таким образом, чтобы не хранить оригинальные, текстовые значения паролей. "Как так?" - спросите вы. А очень просто. Существуют специальные криптографические алгоритмы свертки паролей, которые работают только в одну сторону. Поэтому их еще называют OWF - функции одностороннего преобразования. Грубо говоря, можно получить хэш от пароля, но пароль из хэша не получится. Как это работает в Windows? При создании учетной записи, пользователь вводит начальный пароль, который, однако, не хранится в открытом виде, а хэшируется с помощью OWF функции. Получаемый хэш пароля сохраняется в системе. В дальнейшем, при попытке входа, система запрашивает пользователя пароль, также хэширует его и полученный хэш сравнивает с оригинальным хэшем, сохраненным ранее. Если эти значения совпадают, то пароль, естественно, тоже. Таким образом, оригинальный текстовый пароль не хранится в системе. Более того, существуют и получают распространения новые алгоритмы, которые не хранят даже хэш. Такой алгоритм, к примеру, используется при шифровании паролей Internet Explorer 7-8. Подробнее с ним можно ознакомиться в нашей статье.

В. Как шифруются пароли?

О. Windows NT для хэширования паролей пользователей использует 2 алгоритма: LM, доставщийся нам в наследство от сетей Lan Manager, в основе которого тежит простейшее преобразование DES, и NT, на основе функции хэширования MD4. LM, как более слабый и уязвимый, по умолчанию не поддерживается новейшими системами Windows Vista и Windows 7, однако его можно включить. Более того, прослеживается тенденция его полного исключения или замещения. Важно знать, что при установленной опции хэширования LM (а она по умолчанию включена в Windows XP), все пароли пользователей считаются достаточно уязвимыми. Как правило, для взлома большинства таких паролей требуется несколько минут. NT-хэш лишен недостатков, присущих LM-хэшу. Следовательно, подобрать правильный пароль к известному NT-хэшу значительно сложнее, чем к многострадальному LM. Но имеющаяся тенденция увеличения вычислительных возможностей современных компьютеров, особенно при использовании графических карт, возможно, в скором будущем сделают и этот стандарт уязвимым для потенциальных злоумышленников.

В. Где хранятся хэши паролей?

О. Итак, мы установили, что пароли пользователей в системе Windows преобразуются в специальные значения - хэши. LM и NT хэши имеют фиксированный размер - 16 байт и могут хранится в двух хранилищах: SAM - для обычных учетных записей и Active Directory - учетные записи домена. Обычные учетные записи, содержащие имя пользователя, его пароль и другую служебную информацию, хранятся в реестре Windows NT, а именно файле SAM (от англ. Security Account Manager). Этот файл находится на жестком диске в каталоге %windows%\system32\config. Где %windows% - путь в вашему каталогу Windows. Например, C:\Windows\System32\Config\SAM. Система имеет привилегированный доступ к файлу SAM, поэтому пока она загружена, доступ к файлу запрещен даже администраторам, однако Windows Password Recovery легко обходит это ограничение. Кроме того, несомненный интерес для потенциального взломщика представляют резервная копия файла SAM.SAV и сжатая архивная копия SAM в каталоге %windows%\Repair. Другой способ доступа к файлу SAM - запуск специальной программы с загрузочного диска с последующим копированием файла. Пароли, а точнее хэши, пользователей дополнительно шифруются при помощи утилиты SYSKEY, служебные данные которой находятся в файле реестра SYSTEM. Поэтому для извлечения хэшей из SAM, потребуется также файл SYSTEM, находящийся в той же папке, что и SAM. Учетные записи домена хранятся в базе данных Active Directory. Обычно база данных AD располагается в файле %Windows%\ntds\NTDS.DIT и является сердцем AD. Хэши пользователей шифруются несколько иначе, чем в SAM, но для расшифровки также требуется файл SYSTEM. Доступ к базе также полностью контролируется системой, однако в отличие от SAM, база ntds.dit устойчива к модификации извне.

В. Если все так просто, то почему не запретить доступ всех пользователей к SAM или AD?

О. Так и сделано. По умолчанию, только система имеет доступ к этим файлам. Однако эти ограничения довольно легко обходятся. Например, Windows Password Recovery может импортировать хэши из текущих (заблокированных системой) файлов SAM и AD. Кроме того, система хранит хэши в памяти компьютера для быстрого доступа к ним, поэтому возможен также дамп памяти компьютера.

В. Я не понял, что нужно скопировать с другого компьютера, чтобы расшифровать пароли на своем?

О. Если это обычный компьютер, то следующие файлы: SAM, SYSTEM (а также желательно SECURITY и SOFTWARE). В случае с сервером, нужны эти же файлы и еще ntds.dit.

В. Сколько времени надо чтобы подобрать пароль если известен LM хэш?

О. Самым большим недостатком алгоритма получения LM-хэша является разделение пароля на две части, каждая из которых состоит из 7 символов. Если вводимый пользователем пароль менее 14 символов, то к нему добавляются нули, чтобы получить строку, состоящую из 14 символов. Если пароль пользователя превышает 14 символов, то LM-хэш соответствует пустому паролю. Каждая из 7-символьных половин пароля шифруется отдельно , что значительно упрощает и ускоряет процесс подбора пароля. Другой серьезный недостаток LM-хэша связан с тем, что в процессе шифрования все буквенные символы пароля переводятся в верхний регистр. Т.е. хэши паролей PASSWORD, password, Password или pAsswOrd будут совершенно одинаковыми. Применив brute force атаку отдельно к каждой половине, современные персональные компьютеры могут подобрать численно-цифровой LM-хеш за несколько минут (или даже секунд, при использовании Rainbow атаки). Давайте подсчитаем. Чтобы подобрать пароль методом перебора для любых буквенно-цифровых комбинаций, надо разбить пароль на две части по 7 символов и перебрать 36+36^2+..36^7=80 603 140 212 комбинации. Причем поиск всех хэшей осуществляется одновременно. Скорость перебора в программе Windows Password Recovery на компьютере Intel Core i7 составляет более 100 млн. паролей в секунду. Округлим в сторону уменьшения до 100. 80 603 140 212 / 100 000 000 = 806 секунд. Т.е. мы гарантированно подберем пароль за чуть более 10 минут методом грубого перебора.

В. Можно посмотреть исходники шифрования?

О. Конечно. Примеры исходных кодов доступны на нашем сайте.

В. Сколько времени надо чтобы подобрать пароль если известен NT хэш?

О. С NT хэшами все немного сложнее. NT хэш не имеет недостатков, присущих LM. Поэтому вероятность подбора пароля полностью зависит от его длины и сложности, падая лавинообразно. Даже несмотря на то, что сам по себе алгоритм преобразования NT более быстрый. Рассмотрим следующую таблицу зависимости время перебора пароля от его длины и сложности для скорости перебора 10 миллиардов п/с. Т.е. при переборе на одной топовой (на 2014 год) видеокарте.

Набор символов	Длина пароля	Пример паролей	Время для полного перебора
A .. Z	5	CRUEL	мгновенно

A .. Z	6	SECRET	мгновенно
A .. Z	7	MONSTER	мгновенно
A .. Z	8	COOLGIRL	22с
A .. Z	9	LETMEKNOW	~ 10м
A .. Z, 0 .. 9	5	COOL3	мгновенно
A .. Z, 0 .. 9	6	BANG13	мгновенно
A .. Z, 0 .. 9	7	POKER00	8с
A .. Z, 0 .. 9	8	LETMEBE4	~ 5м
A .. Z, 0 .. 9	9	COOLGIRL1	~ 3ч
A .. Z, a .. z, 0 .. 9	5	P0k3r	мгновенно
A .. Z, a .. z, 0 .. 9	6	S3cr31	~ 10с
A .. Z, a .. z, 0 .. 9	7	DidIt13	~ 6м
A .. Z, a .. z, 0 .. 9	8	GoAway99	~ 6ч
A .. Z, a .. z, 0 .. 9	9	19Sample3	~ 16д

В. Сколько времени надо чтобы узнать NT пароль, если LM пароль известен?
О. Практически, мгновенно.

В. Почему нельзя просто удалить/стереть хэш, т.е. сделать пустой пароль?
О. Почему нельзя? Можно. Например, используя вот эту утилиту. Такой вариант вполне устраивает тех, кому надо любой ценой получить доступ к своей (или чужой, например, соответствующим органам власти) учетной записи. Более того, с помощью вышеупомянутой утилиты можно сделать так: сохранить хэш, сбросить хэш, войти в учетную запись с пустым паролем, произвести необходимые манипуляции, а затем восстановить обратно сохраненный хэш. Но не все так просто. Сбросив пароль и получив доступ к учетной записи, вы не сможете узнать большинство других паролей. Почему? Потому что пароль пользователя участвуется в создании мастер ключа пользователя, применяемый в шифровании DPAPI, EFS и других подсистемах Windows. Т.е., сбросив пароль, вы в дальнейшем не сможете расшифровать следующие данные: файлы, зашифрованные при помощи EFS, пароли учетных записей Outlook, пароли Internet Explorer 7-9, пароли сетевых подключений (RAS, DSL, VPN etc.), сетевые пароли к другим компьютерам, пароли беспроводной сети, MSN Messenger credentials, Google Talk & Google Chrome passwords, Skype и т.д.

В. Другими словами, чтобы расшифровать пароль, например, Internet Explorer, от другой учетной записи, мне сначала нужно узнать пароль этой учетной записи?
О. Совершенно верно.

В. А есть какие-нибудь бэкдоры?
О. Как и везде. Например, пароль учетной записи иногда может храниться к текстовом виде в секретах. Пароли ко многим системным учетным записям также легко расшифровываются.

В. Для этого при импорте хэшей с локального компьютера запрашивается файл реестра SECURITY?
О. Да, основное назначение Security - хранилище т.н. LSA Secrets. В этих секретах (но не только к них) могут храниться plaintext пароли. В Интеллектуальной атаке реализована проверка возможных уязвимостей системы и, как следствие, расшифровка некоторых паролей.

В. А можно при входе в систему вместо пароля подсунуть готовый хэш?
О. Такие программы есть. Действуют они следующим образом: перед загрузкой системы извлекают хэши паролей пользователей SAM. Затем во время загрузки учетной записи, подсовывают известный хэш вместо пароля. Однако последствия этих манипуляций такие же,

как если бы просто сбросить пароль. Т.е. большинство других паролей вы расшифровать не сможете.

В. Что делать, если файл SAM безнадежно испорчен? Можно ли в этом случае восстановить оригинальный пароль?

О. Можно, хотя у вас уже не будет доступа в систему. Можно, например, подобрать пароль по мастер ключу пользователя. В Passcape Software имеются такие наработки. Существуют также кэшированные пароли домена. Если компьютер входит в домен, то по умолчанию имена и хэшированные пароли последних десяти пользователей, регистрировавшихся на этом компьютере, кэшируются в его локальном системном реестре в разделе SECURITY\Policy\Secrets. Можно воспользоваться программой Reset Windows Password для дампа хэшей (их еще называют MSCACHE) с последующей возможной расшифровкой их в Network Password Recovery Wizard или другой аналогичной программе. Но самый простой способ восстановить SAM файл - скопировать его из каталога восстановления или из каталогов отката системы. В программе есть опция загрузки хэшей их этих каталогов.

В. Мне надо получить доступ к учетной записи. Объясните на пальцах чайнику, что и как лучше сделать.

О. Если кратко, есть два способа восстановления доступа к учетной записи.

1. Сбросить пароль, например, сделав его пустым. Для этого есть специальные утилиты, самая мощная и корректная из которых - Reset Windows Password. Принцип ее действия прост: запускаете программу создания загрузочного диска. Создаете с помощью нее загрузочный CD/DVD или USB диск RWP. Далее включаете компьютер с учетной записью, доступ к которой надо получить, и меняете настройки БИОС таким образом, чтобы разрешить загрузку с CD/DVD /USB. На некоторых компьютерах, эта опция уже включена. Загружаетесь с загрузочного диска RWP и, следуя указаниям мастера программы, сбрасываете пароль учетной записи. Все. Теперь можно выполнить вход в систему под этой учетной записью. Однако сброс пароля гарантирует только доступ к учетной записи. Если вам в дальнейшем надо получить доступ к файлам, зашифрованным EFS или восстановить другие пароли (например сетевые), то этот способ не годится.
2. Восстановить оригинальный пароль. Кстати, это может делать и RWP, запуская Интеллектуальную атаку. Однако возможности ее ограничены исключительно слабыми и уязвимыми паролями. Для восстановления оригинального пароля лучше использовать Windows Password Recovery. В этой программе, после импорта хэшей, необходимо выбрать и запустить одну из предлагаемых атак. Если атака не увенчалась успехом, ее можно повторить с измененными параметрами или заменить на другую. Читайте подробнее о том, как выбрать оптимальную атаку на хэши.

В. Где найти словари для атаки по словарям?

О. Искать необязательно. В Windows Password Recovery можно подгружать словари из интернета. На нашем сайте имеется большая подборка словарей.

В. Как сделать пароль "безопаснее"?

О. Обезопасить себя от угадывания пароля потенциальными злоумышленниками можно несколькими способами:

- Не использовать словарные слова (на любом языке), имена, номера, повторяющиеся последовательности букв и цифр, абревиатуры, клавиатурные комбинации, персональную информацию и т.д. Такие пароли подбираются особенно легко.
- Увеличить длину пароля. Однако всему есть разумный предел. Помните, что длина, это еще не главное (впрочем, не только в паролях). В итоге, придумывание длиннющего пароля приведет к тому что очередной пароль будет успешно забыт после бурно проведенных выходных или отпуска. Кроме того, память обычного человека не способна удерживать боле 5-7 паролей одновременно. А ведь есть еще сетевые пароли, пароли Web и т.д.

- Расширить используемый в пароле набор символов. Например, заменить в пароле символ a на @. Использование национальных символов также радикально увеличивает стойкость пароля. Использовать редко встречающиеся символы, например ~. Не стоит использовать сложнозапоминающиеся пароли, состоящие из случайного набора символов, если вы не гений, конечно.
- Не используйте один единственный пароль для входа в Windows, Веб сайтов, сервисов и т.д.
- Если вы боитесь забыть все свои пароли, запишите их в отдельный файл и установите пароль к нему. Хорошая парольная защита, например, использована в архиваторе Rar. Не храните этот файл на локальном компьютере.
- Никогда не вводите свой пароль на чужом компьютере.
- Не стоит записывать пароли на стикерах и приклеивать их к монитору.
- Подумать о дополнительной защите. Например, если установить опцию SYSKEY startup password, то с вероятностью, близкой к 100%, ваши пароли не сможет подобрать ни один парольный взломщик, не угадав начальный пароль SYSKEY.

3.5 FAQ по работе программы

В. Что означают знаки вопроса у LM паролей?
О. Как известно, LM пароль состоит из двух половинок. Если впереди LM пароля стоят 7 знаков вопроса, то это означает, что найдена только вторая половина пароля. Если знаки вопроса стоят позади - то первая.

В. В чем разница между LM и NT паролями? Я нашел оба пароля: MASTERGURU и MasterGuru. Какой из них правильный? Какой мне использовать?
О. Для входа в систему используется NT пароль.

В. При переборе LM пароля, программа ругается и говорит, что урезает длину пароля до 7. Это глюк?
О. Нет. Как известно, LM пароль делится на две 7-символьные половины. Поэтому максимально длина перебираемых LM паролей составляет 7 символов.

В. Я знаю свой NT пароль, но программа его почему-то не находит, почему?
О. NT пароль - регистрозависимый. Возможно, вы задали неправильный диапазон перебираемых символов. Попробуйте проверить пароль вручную в (Tools-Password Checker). Password Checker автоматически подбирает все возможные комбинации заглавных и строчных букв.

В. Я нашел пароль встроенного администратора, но при попытке входа с ним, система сообщает, что пароль неверный. В чем дело?
О. Скорее всего, вы восстановили пароль локального администратора, а ваш компьютер входит в домен. Пароли домена хранятся в Active Directory, в т.ч. и Администратора домена. Попробуйте войти в систему в безопасном режиме.

В. Интересно, во время атаки по словарю нашелся пароль, которого не было в словаре. Как так?
О. Скорее всего, вы установили максимальный уровень мутации, при котором проверяются также словарные слова, набранные не в английском, а в национальном алфавите, в зависимости от раскладки клавиатуры. Например, слово secret в русской раскладке клавиатуры будет соответствовать слову ыускуе. Кроме смены раскладки, включенные мутации могут до неузнаваемости "уродовать" слова. Мутация используется в предварительной, интеллектуальной, словарной, комбинированной атаке, атаке по ключевому слову, а также атаке по фразам.

В. Можно ли в групповой атаке задавать один тип атаки, но с разными настройками?
О. Да, можно.

В. У меня вопрос по онлайн-словарям. Я заметил, что они очень сильно сжаты, сильнее чем любым архиватором. Что это за формат PCD?
О. Это свой собственный формат хранения словарей, разработанный в Passcape, который использует дополнительные алгоритмы оптимизации и шифрования. Некоторые словари, действительно, можно довольно сильно сжать, сильнее чем простым архиватором. Например, словарь Australian.pcd в оригинальном виде занимает 926 Кб, в сжатом - 53 Кб.

В. Я выбрал атаку по словарю, установил средний уровень мутаций. Когда запустил атаку, был неприятно удивлен низкой скоростью, всего несколько тысяч паролей в секунду. Почему так медленно?
О. Скорость атаки по словарю показывается без учета мутации. Например, если в секунду было обработано 1000 слов, то показывается скорость 1000 п/с, хотя в в модуле мутации за это время для каждого слова могло быть создано по 1000 дополнительных слов. Таким образом, реальная скорость перебора в сотни и даже тысячи раз больше.

В. Можно ли в комбинированной атаке по словарям использовать обычные словари?
О. Можно.

В. Я знаю, что пароль начитается со слова blue. Какую атаку мне лучше применить?
О. Можно попробовать атаку по маске. К примеру, вот такая маска blue%c%c%c%c%c%c будет перебирать диапазон от blueaaaaaa до bluezzzzzz включительно. Можно также попробовать комбинированную атаку по словарям. Для этого откройте notepad, наберите стово blue и сохраните, скажем под именем 1.dic. Зайдите в опции комбинированной атаки, введите в качестве основного словаря 1.dic. В качестве вспомогательного - любой другой. Этот вариант будет искать двусложные пароли, например, bluepig, blueberry, bluegirl и т.д. Если задать третий словарь, то поиск будет осуществляться на основе образования трех составляющих. Например, bluecoolgirl, blueblackhash, bluebadboy.

В. Интеллектуальная атака протекает очень медленно, в чем дело?
О. Либо переполнен кэш паролей. В этом случае его надо попробовать очистить. Либо установлена опция глубокой мутации и программа нашла довольно много "подозрительных" слов, т.е. тех слов, которые рассматриваются в качестве потенциальных паролей.

В. Я запускаю перебор, а программа ругается на то, что ей нечего делать. В чем причина?
О. Перед перебором нужно сначала выбрать хэши. Это делается из меню Edit - Select.

В. Что такое Rainbow-таблицы и как их использовать для восстановления паролей?
О. Подробную информацию о таблицах можно получить на сайте https://project-rainbowcrack.com/. Если кратко, то для запуска атаки по таблицам, в опциях атаки необходимо загрузить список *.RT-файлов, содержащих Rainbow-таблицы. Тип таблиц должен совпадать с типом хэшей, выбранных для атаки. Для этого названия файлов с таблицами должны начинаться соответствующим образом: "lm_*.rt" для LM-хэшей, "ntlm_*.rt" для NT-хэшей.

В. У меня постоянно выскакивает ошибка сервиса (Loader error #-1) при работе некоторых модулей программы. Как это исправить?
О. Для чтения хэшей с рабочей системы, выдергиванию тестовых паролей и некоторых других критических операций, Windows Password Recovery активно использует метод DLL inject, внедряя свой код в адресное пространство системы. Некоторое антивирусное ПО блокирует подобную активность. Для обеспечения нормальной работы программы, необходимо повысить уровень доверия программы или убрать ограничения в вашем антивирусном ПО. Если это не помогает,

попробуйте временно отключить антивирусное ПО, предварительно отключив доступ к сети Интернет. Не смотря на кажущуюся простоту, в большинстве случаев эта задача довольно нетривиальна. Например, для отключения антивируса ESET, необходимо перезагрузиться в безопасном режиме по F8, затем через devmgmt.msc отключить следующие драйвера устройств ESET: ehdrv и epfwwfpr.

3.6 GPU FAQ

В: Какие системные требования имеет программа?
О: В настоящее время, программа работает с видеокартами NVidia, имеющими поддержку технологии CUDA 3.0, видеокартами AMD Radeon серии 7xxx и выше, встроенной графикой Intel серии 4xxx и выше. Полный список поддерживаемых CUDA устройств можно найти тут. Совместимые с AMD Radeon видеокарты показаны по следующему адресу: wikipedia.org/wiki/Comparison_of_AMD_graphics_processing_units. Кроме того, необходимо, чтобы были установлены самые свежие драйвера.

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: 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**'.
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 https://www.nvidia.ru/drivers, для AMD карт - https://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 Radeon?
О: https://en.wikipedia.org/wiki/Comparison_of_AMD_graphics_processing_units

В: Где найти инфу о встроенной графике Intel?
О: https://en.wikipedia.org/wiki/Intel_HD_and_Iris_Graphics.

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 надежно и качественно охлаждается, GPU слот в системном блоке и сам системный блок очищен от грязи и пыли. Неразумное использование определенных 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 разъемы для подключения дополнительного питания, убедитесь что все они подключены.

В: Я запустил GPU атаку, но компьютер стал сильно тормозить. Как это исправить?
О: По умолчанию программа настроена на работу с видео картами средней производительности. Это как правило, 256 потоков в блоке, 256 блоков и 1000 паролей на поток. Для старых видеокарт такая конфигурация избыточна и может привести к тормозам. Рекомендуем в настройках атаки уменьшить значение '**Passwords per thread**' до 100 или даже меньше.

В: Как подобрать наилучшие значения 'Thread blocks' и 'Passwords per thread' в настройках GPU атаки?
О: Можно эмпирически, а можно математически. Например, эти значения установлены в 100 и 100, а средняя скорость в атаке составляет 1 миллиард паролей в секунду, то можно посчитать, что за секунду происходит около 390 вызовов подпрограммы графической карты (за один раз обрабатывается обычно 256*ThreadBlocks*PasswordsPerThread паролей). Естественно, чем меньше вызовов, тем меньше накладных расходов, и тем больше скорость атаки. С другой стороны, в секунду должно быть по крайней мере пара обращений к GPU программе. Делаем выводы, вооружаемся калькулятором и вносим соответствующие коррективы. Можно подгонять параметры на глазок, увеличивая эти параметры до тех пор, пока не перестанет расти скорость атаки и не появятся тормоза. Если есть GPU монитор в системе, то он должен показывать как минимум 98-99% загрузку. Кроме того, важно знать еще несколько моментов. Во-первых, нельзя задавать слишком большие суммарные значения в этих параметрах. Это может привести к неработоспособности или зависанию программы. Во-вторых, нежелательно задавать значения меньше 100 в поле '**Password per thread**', т.к. это негативно скажется на производительности атаки для любой графической карты.

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 слотную 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?
О: Есть два решения проблемы: временное и постоянное. В качестве временной меры, попробуйте в настройках атаки уменьшить количество запускаемых GPU блоков или количество паролей, перебираемых в одном GPU потоке. В качестве постоянного решения проблемы, 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 дешевую 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?
О: Да.

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

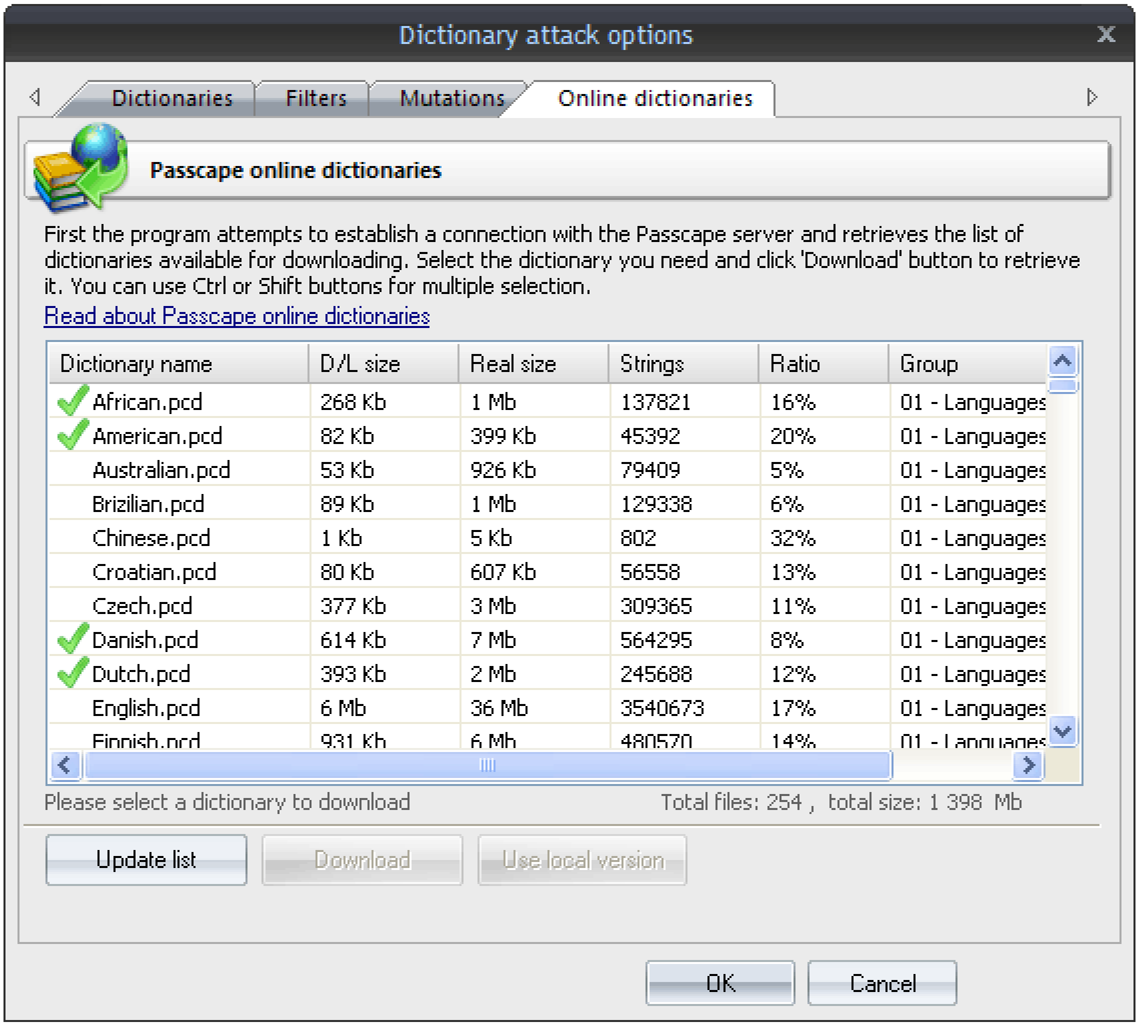
В: Могу ли я использовать одновременно NVidia и AMD видео карты?
О: Да, можете.

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 установить последнюю версию драйвера видеокарты или отдельно компонент ADL. Убедитесь, что видеокарта активна (подключена к активному монитору). Из-за многолетнего бага в драйверах AMD, неактивные видеокарты неправильно функционируют в ADL.

3.7 Загрузка Онлайн Словарей



First the program attempts to establish a connection with the Passcape server and retrieves the list of dictionaries available for downloading. Select the dictionary you need and click 'Download' button to retrieve it. You can use Ctrl or Shift buttons for multiple selection.

Read about Passcape online dictionaries

Dictionary name	D/L size	Real size	Strings	Ratio	Group
✓ African.pcd	268 Kb	1 Mb	137821	16%	01 - Languages
✓ American.pcd	82 Kb	399 Kb	45392	20%	01 - Languages
Australian.pcd	53 Kb	926 Kb	79409	5%	01 - Languages
Brizilian.pcd	89 Kb	1 Mb	129338	6%	01 - Languages
Chinese.pcd	1 Kb	5 Kb	802	32%	01 - Languages
Croatian.pcd	80 Kb	607 Kb	56558	13%	01 - Languages
Czech.pcd	377 Kb	3 Mb	309365	11%	01 - Languages
✓ Danish.pcd	614 Kb	7 Mb	564295	8%	01 - Languages
✓ Dutch.pcd	393 Kb	2 Mb	245688	12%	01 - Languages
English.pcd	6 Mb	36 Mb	3540673	17%	01 - Languages
Finnish.pcd	931 Kb	6 Mb	480570	14%	01 - Languages

Please select a dictionary to download

Total files: 254 , total size: 1 398 Mb

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 объема информации, может потребоваться некоторое время, которое зависит от скорости работы вашего интернет канала.

Все онлайн (а также некоторые дополнительные) словари можно заказать для доставки на CD. Общий объем всех словарей составляет более 6 Гб. Вы также можете поделиться с нами своим собственным словарем, прислав его, или ссылку на него на наш электронный адрес.

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 "Windows 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 of 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.

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.

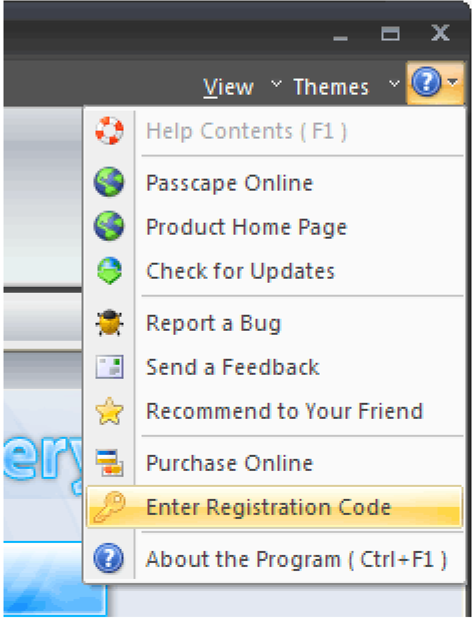
All rights not expressly granted here are reserved by Passcape Software.

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.

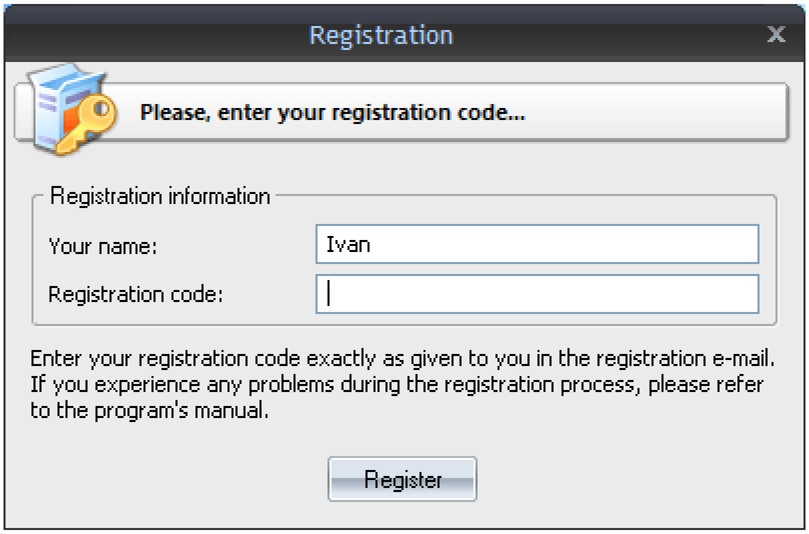
Важно! При заполнении формы оплаты, убедитесь, что указали правильный адрес электронной почты, который не блокирует входящие письма. В противном случае вы будете не в состоянии получить регисрационное письмо.

Для завершения процесса регистрации



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

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



Your name: Ivan

Registration code:

Enter your registration code exactly as given to you in the registration e-mail. If you experience any problems during the registration process, please refer to the program's manual.

4.3 Ограничения ДЕМО версии

Незарегистрированная версия **Windows Password Recovery** показывает только первые три символа расшифровываемых паролей, позволяет работать одновременно с максимум 100 хэшами и имеет ряд других функциональных ограничений.

4.4 Редакции программы

Windows Password Recovery поставляется в трех редакциях: Light, Standard и Advanced. Ниже дано подробное описание ограничений для каждой редакции программы.

ВОЗМОЖНОСТЬ	**Light**	**Standard**	**Advanced**
Поддержка рабочих станций Windows XP - 11	+	+	+
Поддержка серверных ОС Windows 2003 - 2022	+	+	+
Поддержка Windows 64-bit	+	+	+
Поддержка Русской Windows	+	+	+
Поддержка паролей в национальных кодировках	+	+	+
Поддержка многопоточности	+	+	+
Поддержка тем интерфейса	+	+	+
Поддержка хэшей: LM, NTLM, DCC1, DCC2, PIN, CLOUD	+	+	+
Загрузка хэшей с локального компьютера	+	+	+
Загрузка хэшей с удаленного компьютера	-	+	+
Дамп обычных хэшей	+	+	+
Дамп хэшей истории паролей	+	+	+

ВОЗМОЖНОСТЬ	**Light**	**Standard**	**Advanced**
Поиск текстовых паролей	+	+	+
Загрузка хэшей из SAM	+	+	+
Загрузка хэшей из NTDS.DIT	+	+	+
Загрузка хэшей из SECURITY	+	+	+
Импорт хэшей из других программ	+	+	+
Загрузка хэшей из каталогов восстановления системы	+	+	+
Экспорт хэшей в файл PWDUMP	+	+	+
Поддержка облачных учетных записей Microsoft и Azure AD	+	+	+
Поддержка учетных записей без паролей	+	+	+
Обычные атаки	+	+	+
Улучшенные атаки	+	+	+
Умные атаки	+	+	+
Атаки с применением вычислительных способностей GPU	+	+	+
Поддержка нескольких GPU устройств	-	+	+
Групповая атака	-	-	+
Просмотр кэша паролей AI	-	-	+
Умные мутации паролей	+	+	+
Поддержка Онлайн словарей	+	+	+
Поддержка SYSKEY	+	+	+
Поддержка опции SYSKEY startup password	+	+	+
Поддержка опции SYSKEY floppy diskette	+	+	+
Создание словарей в словарной атаке	-	-	+
Создание словарей по маске	-	-	+
Создание словарей по ключевому слову	-	-	+
Создание комбинированных словарей	-	-	+
Создание фразовых словарей	-	-	+
Создание словарей на основе гибридной атаки	-	-	+
Поддержка гибридных и индексных (*.rti) радужных таблиц	+	+	+
Возможность ограничивать доступ к программе	+	+	+
Инструмент измерения стойкости пароля	+	+	+
Проверка хэшей	+	+	+
Генератор хэшей	+	+	+
Генератор случайных хэшей	-	+	+
Генератор хэшей по словарю	-	+	+
Генератор радужных таблиц	+	+	+
Генератор радужных таблиц Passcape	+	+	+
Резервное копирование реестра системы	-	+	+
Резервное копирование базы данных Active Directory	-	-	+
Инструмент для открытия **** паролей	+	+	+
Сброс паролей SAM (обычных учетных записей)	-	-	+
Сброс паролей NTDS.DIT (доменных учетных записей)	-	-	+
Сброс паролей SECURITY (кэшированных записей домена)	-	-	+
Редактор секретов LSA	+	+	+

ВОЗМОЖНОСТЬ	Light	Standard	Advanced
Редактор кэшированных паролей домена	-	+	+
Редактор SAM	-	+	+
Редактор Active Directory	-	-	+
Обозреватель Windows Vault	-	-	+
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	+	+	+
DPAPI: расшифровка объектов DPAPI	*	*	+
DPAPI: анализ объектов DPAPI	+	+	+
DPAPI: поиск объектов DPAPI	+	+	+
DPAPI: анализ Мастер Ключей	*	*	+
DPAPI: дамп хэшей истории паролей	-	-	+
DPAPI: анализ истории паролей DPAPI	*	*	+
Windows Hello: расшифровка паролей пользователей	-	+	+
Windows Hello: расшифровка биометрических баз данных	-	+	+
Windows Hello: восстановление ПИН	-	+	+
Обозреватель паролей Windows Credentials	-	-	+
Системный монитор	+	+	+
Мониторинг активности видеокарт	+	+	+
Отчеты о паролях	-	+	+
Использование ИИ при расшифровке хэшей в режиме Мастера	+	+	+
Запуск в режиме невидимости	+	+	+
Макс. количество хэшей	500	5000	неограничено
14-дневная гарантия возврата денег	+	+	+
Лицензия	персональная	персональная	бизнес
Цена	$65	$345	$895

* - некоторые функции ограничены

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!