Windows Password Recovery

User manual

Passcape Software

Introducción

1 Introducción

1.1 Acerca del programa

Bienvenidos a **Windows Password Recovery**, un analizador de seguridad de red y una utilidad de recuperación de contraseñas de Windows. Windows Password Recovery es la única solución que implementa las tecnologías de recuperación de contraseñas patentadas más avanzadas desarrolladas por los programadores de Passcape Software, como la *Inteligencia Artificial* o el ataque de *frase de contraseña*.

En comparación con productos similares, Windows Password Recovery presenta una serie de ventajas competitivas:

Para usuarios domésticos - fácil configuración y uso. Recupera o restablece fácilmente las contraseñas olvidadas en cualquier cuenta de Windows.

Para los administradores de sistemas - la auditoría de contraseñas revela violaciones de seguridad, lo que ayuda a los administradores a garantizar la confiabilidad y seguridad de la red corporativa. Comprueba el nivel de seguridad de los sistemas operativos Windows.

Para expertos en seguridad forense, industrial y gubernamental - analiza y audita las políticas de seguridad del sistema, emite recomendaciones para mejorar la estabilidad de la protección con contraseña de los sistemas operativos.

1.2 Características y beneficios

- Interfaz gráfica de usuario contemporánea y fácilmente personalizable.
- Soporte para 14 formatos de archivo diferentes al importar hashes.
- Soporte para hashes NTLM, LM, DCC1, DCC2.
- Importar directamente desde el registro de Windows o Active Directory; incluso si los archivos están bloqueados por el sistema, el programa todavía los lee.
- Importar hashes desde equipos remotos.
- Importe hashes desde instantáneas del sistema, puntos de restauración, copia de seguridad y carpetas de reparación.
- Respaldar/guardar archivos de registro local y base de datos de Active Directory.
- Importar hashes del historial de contraseñas.
- Recupere algunas contraseñas de cuenta sobre la marcha (al importar localmente).
- Admite Active Directory (cuentas de dominio).
- Admite credenciales de dominio en caché.
- Soporte de importación desde sistemas x86/x64.
- Exporta hashes al archivo PWDUMP.
- El software utiliza 17 tipos de ataques diferentes; 10 de ellos son únicos, desarrollados por nuestra empresa, implementados sobre tecnologías patentadas.
- El programa es compatible con multithreading, aprovechando al máximo el poder de las computadoras modernas.
- El ataque de diccionario admite diccionarios de texto en los formatos ASCII, UNICODE, UTF8, PCD, RAR y ZIP.
- Amplia selección de diccionarios en línea para ataques de diccionario (aproximadamente 2 GB)

- Algunas de las funciones del programa, por ejemplo, la mutación de palabras, son únicas. Por ejemplo, el número total de reglas de mutación supera los ciento cincuenta. ¡No hay otras características de aplicación similares que!
- Admite un número ilimitado de hashes inspeccionados.
- Análisis inteligente de contraseñas encontradas.
- Alta velocidad de búsqueda en computadoras modernas: más de 100 millones de contraseñas por segundo para CPU de 4 núcleos y miles de millones de contraseñas / seg utilizando la potencia de la GPU.
- Incluye herramientas auxiliares: generador de hash, comprobación de fuerza de contraseña, creación de tablas arcoiris, etc.
- Conjunto de herramientas ampliado para trabajar con listas de palabras: crear, ordenar, convertir, etc.
- Módulos adicionales para forenses e investigadores: editor de secretos LSA, visor de credenciales en caché de dominio, exploradores de Active Directory y SAM, decodificador sin conexión DPAPI.
- Extracción de contraseñas de texto sin cifrar de la memoria, caché de Windows, Windows Hello, secretos ocultos, etc.
- Informes avanzados de contraseñas

Interfaz del programa

2 Interfaz del programa

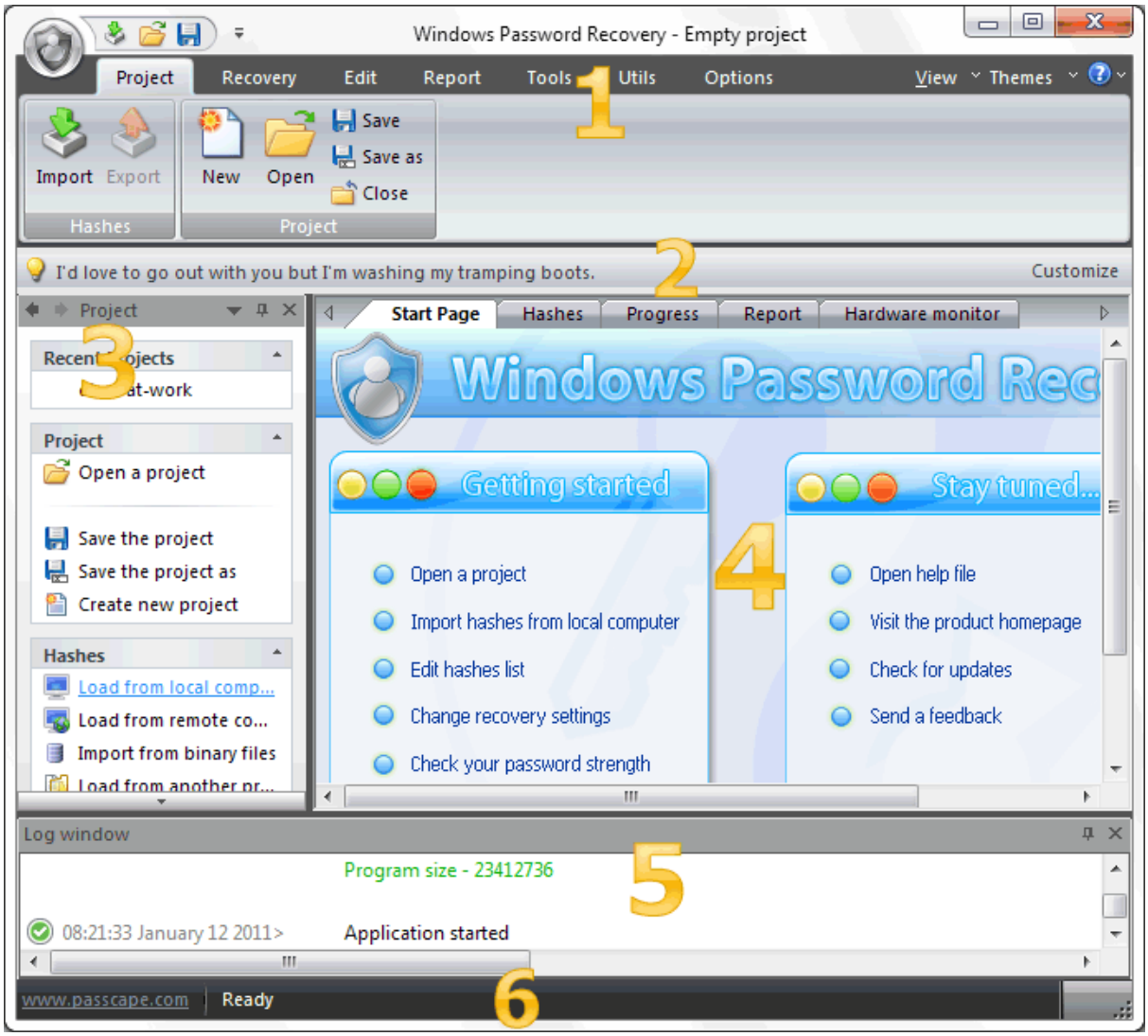
2.1 Visión general

La interfaz del programa se realiza en forma de Interfaz de Documento Único, es decir, permite trabajar con un solo proyecto a la vez. El funcionamiento del programa se puede dividir convencionalmente en 4 etapas:

1. Creación de un proyecto
2. Importación (carga) de hashes de contraseña al proyecto. Edición de los hashes: borrar, añadir, seleccionar, etc.
3. Recuperación de los hashes. Incluye la selección, configuración y lanzamiento de uno o varios ataques seleccionados.
4. Analizando los resultados.

Toda la interfaz se puede dividir convencionalmente en varios componentes:

- Barra de menús
- Barra de información: para mostrar textos informativos breves, como consejos, advertencias, etc.
- Barra de tareas: duplica y complementa la barra de menús, proporcionando un acceso rápido a las operaciones más comunes. Consta de tres partes:
  - Proyecto - incluye las operaciones principales sobre el proyecto, como abrir, cerrar, crear un nuevo proyecto e importar hashes.
  - Editor de hash. Duplica las operaciones de edición más comunes.
  - Herramientas: incluye un reloj, un calendario y una calculadora.
- Ventana principal: soporta la carga principal y consta de 5 partes. La primera pestaña es la ventana de bienvenida. La segunda pestaña contiene la lista de hashes a analizar y recuperar. Luego va una pestaña con el indicador de estado de ataque actual (progreso) y una pestaña con las estadísticas e informes. Y finalmente, una pestaña con el monitor de hardware.
- Ventana de registro: muestra información sobre el estado actual de la aplicación, el funcionamiento actual, etc. El registro del programa se puede copiar en el portapapeles o guardar en un archivo (al hacer clic con el botón derecho se abre el menú correspondiente).
- La barra de estado está diseñada con fines informativos.

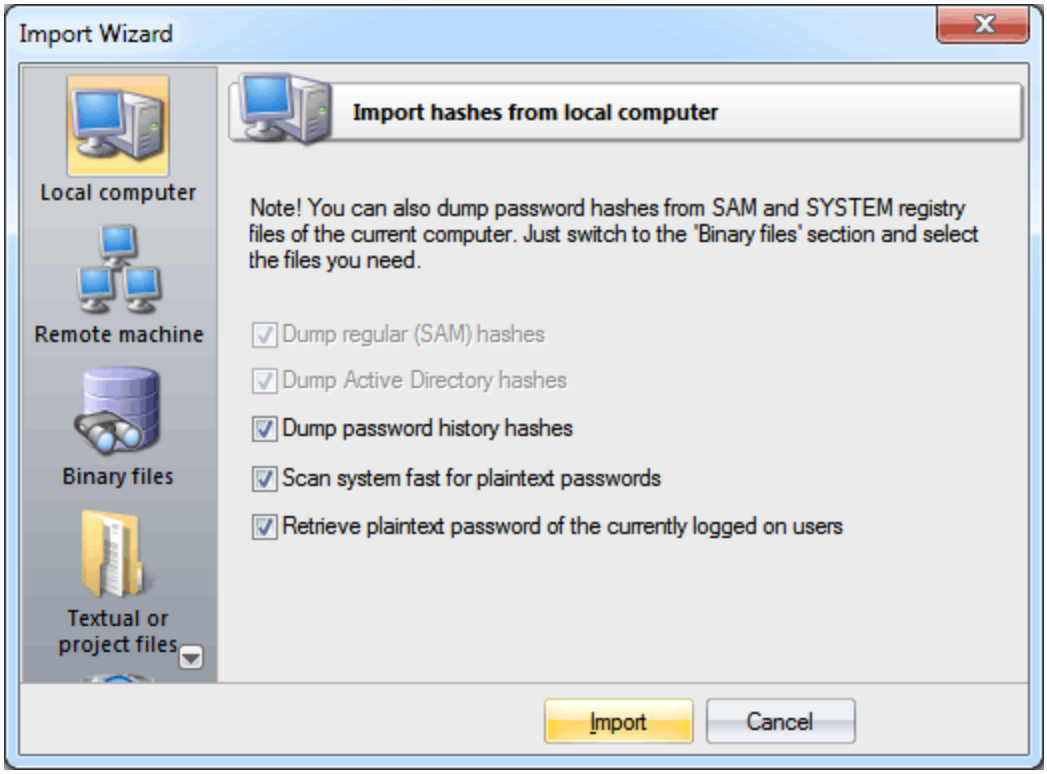


2.2 Menú Proyecto

2.2.1 Importación

Windows Password Recovery ofrece una amplia gama de opciones para cargar hashes en función de sus capacidades. Hay 5 formas principales de importar hashes al programa.

2.2.1.1 Importar hashes locales



Importar hashes desde el equipo local: el método más preferible, ya que implica el análisis general más profundo del sistema y las contraseñas. Además de eso, los hashes que se importan desde la computadora local pueden sufrir el sofisticado *ataque inteligente*, que permite recuperar con relativa rapidez las contraseñas de algunas cuentas.

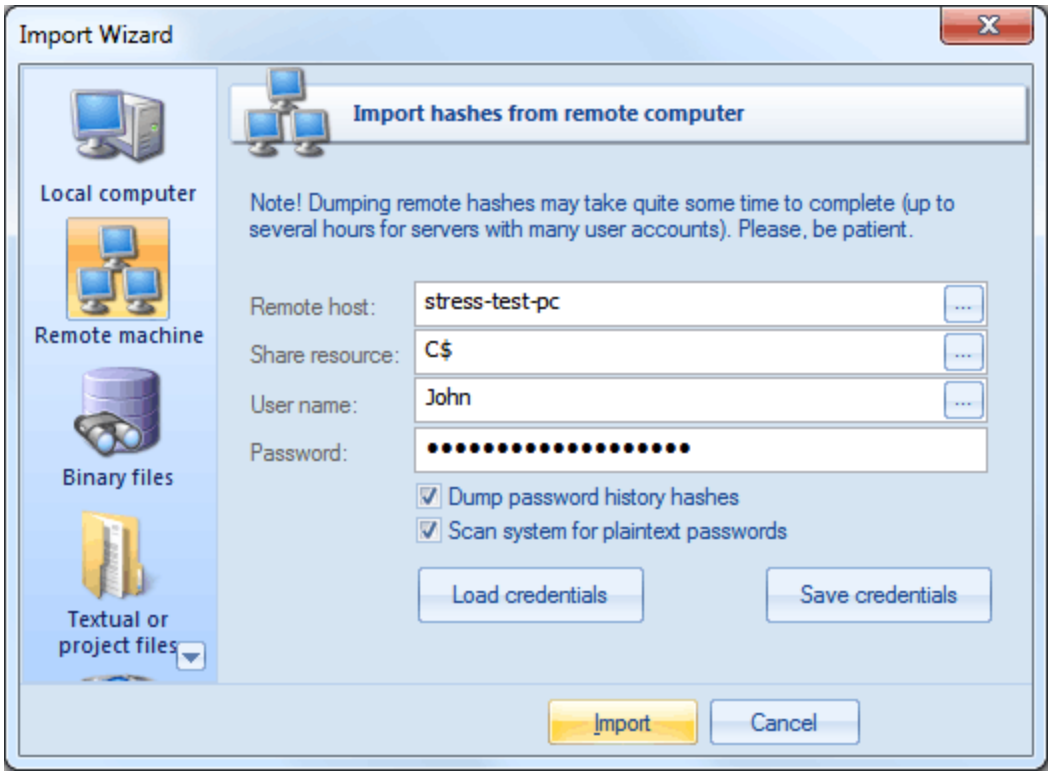
La importación de hashes locales funciona bien independientemente de dónde se localicen los hashes: en SAM, en SECURITY o en Active Directory. Este elemento tiene dos opciones adicionales: volcar hashes del historial de contraseñas y buscar contraseñas de texto sin formato que se almacenan en el sistema. El proceso mismo de búsqueda de contraseñas de texto sin formato se divide en 4 pasos y consiste en la búsqueda real de las contraseñas que se almacenan en el sistema utilizando el cifrado inverso, la búsqueda de las contraseñas de texto para las cuentas del sistema, la búsqueda de contraseñas de inicio y un paso adicional, cuando el programa analiza algunas de las cuentas descubiertas, contraseñas a las que también se puede recuperar del sistema (por ejemplo, para la cuenta HomeGroupUser$ en Windows 7).

Si no se desea deshabilitar las últimas 2 opciones, ya que permite recuperar de manera relativamente indolora y rápida las contraseñas completas de algunas de las cuentas del sistema, el volcado del historial de contraseñas es completamente opuesto: deshabilitarlo a menudo es muy útil. Por ejemplo, cuando el número de contraseñas a importar supera los cientos de miles o incluso millones. Por otro lado, el programa tiene un poder de inteligencia artificial, por lo que si durante un ataque encuentra una de las contraseñas del historial, tomará todo lo posible para recuperar las contraseñas restantes analizando las preferencias del usuario para la contraseña recuperada.

Una de las últimas versiones del programa también puede volcar hashes del historial del usuario desde el archivo DPAPI CREDHIST. Por lo tanto, ahora se recomienda configurar la opción.

La funcionalidad de importación local requiere privilegios administrativos.

2.2.1.2 Importar hashes desde un equipo remoto



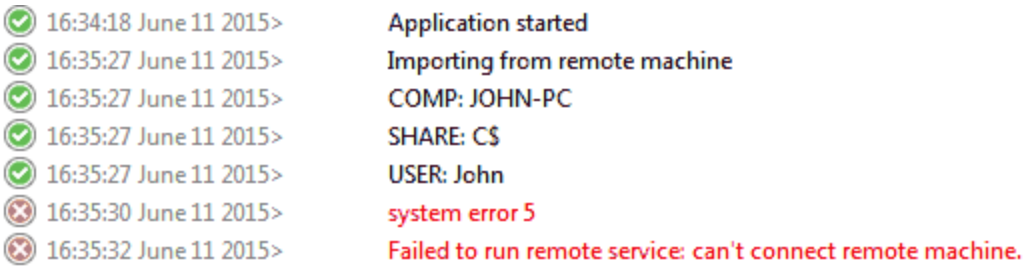
Importar hashes desde un host remoto: El programa tiene medios para volcar hashes desde un host remoto sin emplear utilidades de terceros. Esto no compromete el sistema remoto, ya que aún requiere proporcionar las credenciales para el usuario de host remoto.

El volcado desde un host remoto funciona de la siguiente manera. Primero, debe ingresar el nombre de host remoto en el campo Host remoto. Puede utilizar el botón [...] para navegar por la red. Una vez que haya seleccionado el host remoto, configure un recurso compartido (permitido tanto para leer como para escribir), a través del cual se transmitirán los datos. Por lo general, eso es C$ o ADMIN$. Aquí también, puede aprovechar el botón de exploración a la derecha del cuadro de edición. A continuación, en los dos campos de la parte inferior, escriba el nombre de la cuenta de host remoto y la contraseña.

El botón *'Guardar credenciales'* guarda la configuración actual. Respetuosamente, el botón *'Cargar credenciales'* permite cargar configuraciones existentes, para que no tenga que ingresarlas manualmente cada vez que las necesite. ¡La contraseña se almacena en forma cifrada!

Esta opción de importación también requiere privilegios administrativos en el equipo de destino.

Sin embargo, puede experimentar algunos problemas para conectarse a un equipo remoto, incluso si tiene una cuenta de administrador. Al conexión al PC de destino con Windows Vista/7/8/10, puede obtener el siguiente error:

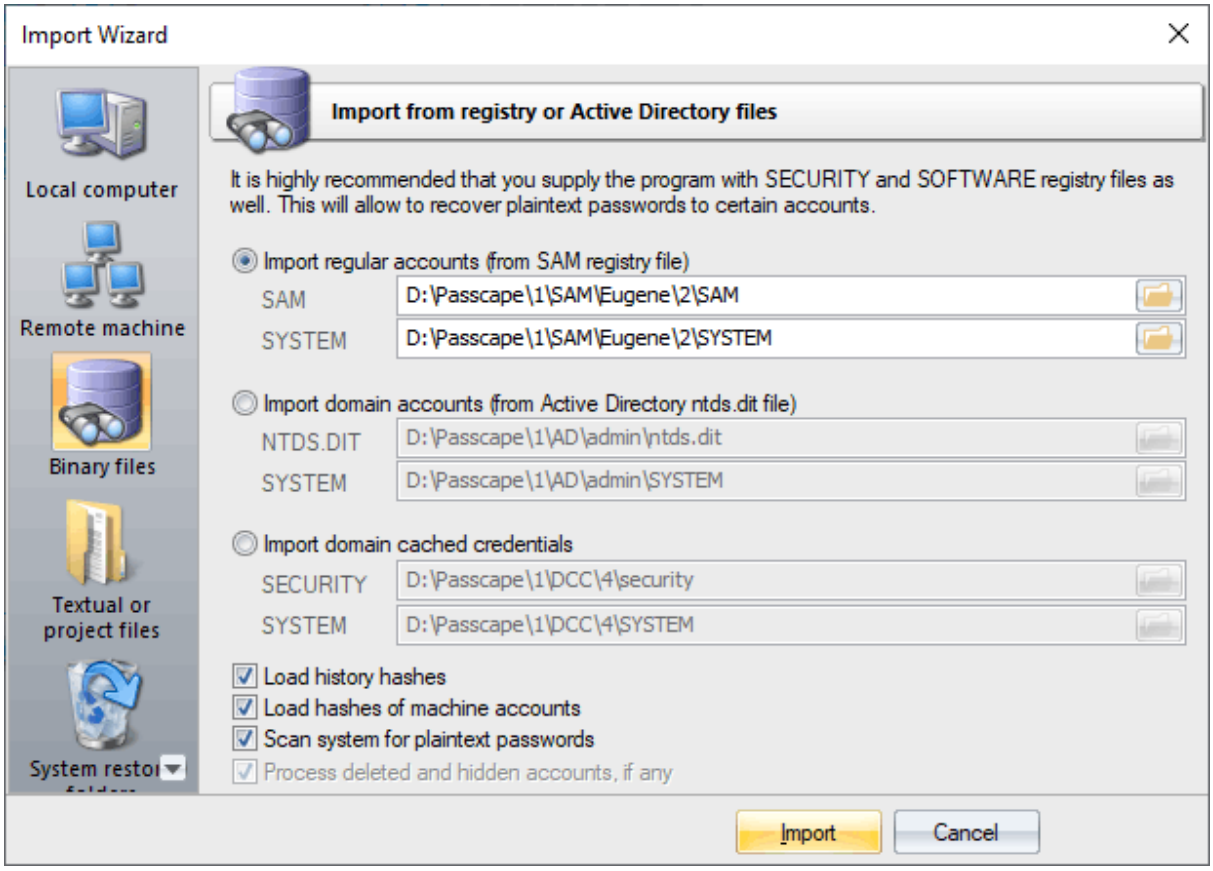


El error 5 indica que se deniega el acceso (incluso si la cuenta de destino tiene privilegios de administrador). El problema es que cualquier conexión remota en Windows Vista y sistemas operativos superiores de forma predeterminada no puede realizar tareas administrativas. La documentación de Microsoft indica claramente lo siguiente:

> *"Cuando un usuario con una cuenta de administrador en la base de datos local del Administrador de cuentas de seguridad (SAM) de un equipo con Windows Vista se conecta de forma remota a un equipo con Windows Vista, el usuario no tiene potencial de elevación en el equipo remoto y no puede realizar tareas administrativas. Si el usuario desea administrar la estación de trabajo con una cuenta SAM, debe iniciar sesión interactivamente en el equipo que se administrará."*

Sin embargo, hay un indicador en el registro de Windows que permite cambiar el comportamiento predeterminado. Simplemente inicie el editor de registro de la PC de destino y abra la siguiente clave: *HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\system*
A continuación, cree un valor DWORD *LocalAccountTokenFilterPolicy* y configúrelo en uno (1). Por lo tanto, podrá conectarse al recurso compartido de administración.

2.2.1.3 Importar hashes desde archivos binarios



Importar hashes desde archivos binarios: Windows Password Recovery puede extraer hashes de contraseña directamente de archivos binarios. Incluso aquellos de ellos que actualmente son utilizados por el sistema (es decir, bloqueados).

Normalmente, los hashes de contraseña se almacenan en archivos de registro SAM o SECURITY, que residen en la carpeta '%WINDOWS\%System32\Config'. La misma carpeta contiene el registro SYSTEM, que es necesario para la recuperación. Si ha especificado la ruta de acceso al registro en el sistema actual, analizarla llevará un poco más de tiempo (normalmente unos segundos).

Los hashes de contraseña para las cuentas de dominio se almacenan en la base de datos de Active Directory; o, para ser más específicos, en el corazón mismo de la misma, en el archivo ntds.dit, que reside en la carpeta: '%Windows%\ntds'. La recuperación de cuentas de dominio también requiere el archivo de registro SYSTEM. ¡Ten cuidado! El volcado desde la base de datos de AD del sistema actual puede llevar algún tiempo, especialmente cuando ntds.dit es de un tamaño considerable.

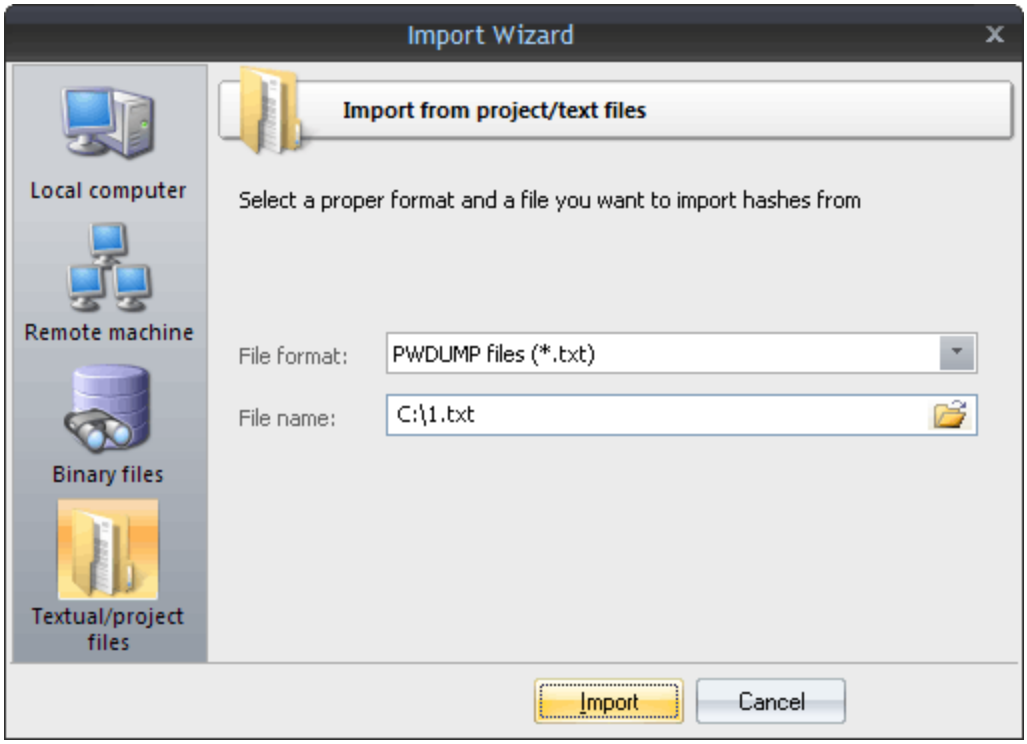
El programa funciona correctamente y es compatible con todas las opciones de cifrado SYSKEY: SYSKEY del registro, disquete de inicio SYSKEY, contraseña de inicio SYSKEY.

Si está copiando los archivos de otro sistema, además de los archivos SAM (ntds.dit) y SYSTEM, también es muy recomendable copiar los archivos de registro SECURITY y SOFTWARE. Deben estar ubicados en la misma carpeta con el archivo SYSTEM. Eso le permitiría recuperar las contraseñas de algunas cuentas de usuario más rápido.

Usando opciones adicionales puedes:

- Activar / desactivar la carga de hashes del historial. Desactivar la carga del historial aumentará el análisis de la base de datos. Por otro lado, al procesar (atacar) hashes, adivinar las contraseñas del historial puede dar una pista para averiguar la contraseña de la cuenta principal a la que pertenecen los hashes.
- Descartar cuentas de máquinas de carga (las que terminan con carácter $).
- Encienda / apague la verificación instantánea de contraseñas de texto sin formato, si las hubiera.

2.2.1.4 Importar desde archivos de proyecto/texto



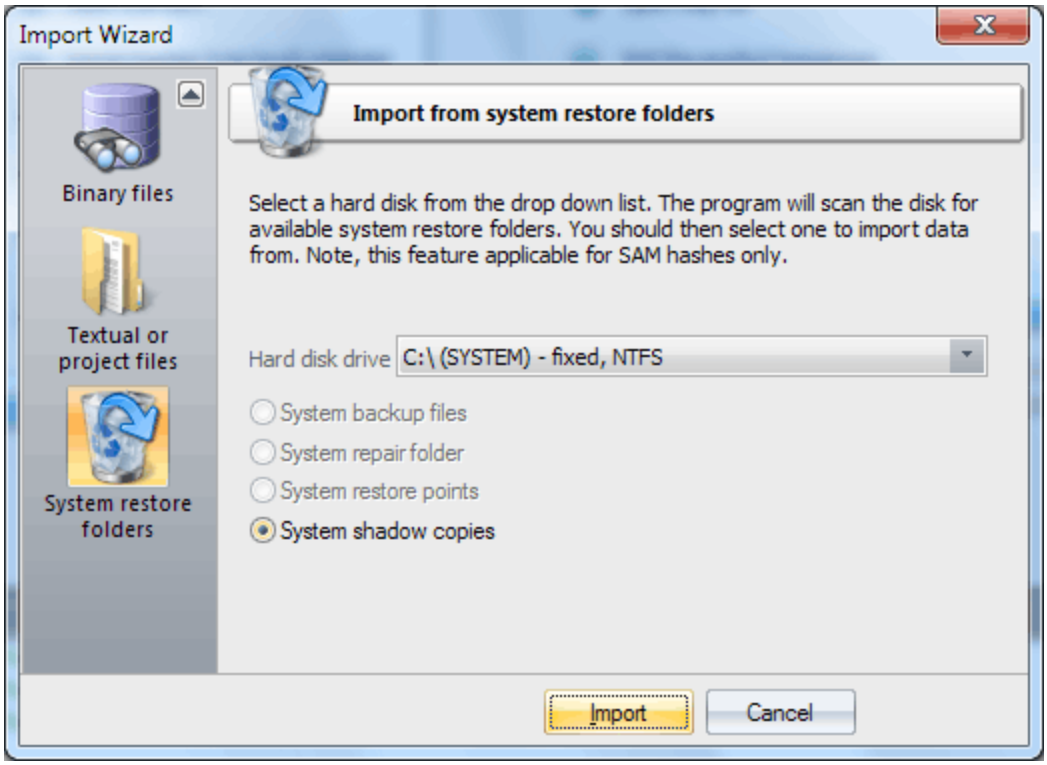
Finalmente, puede cargar los hashes en su proyecto **importándolos desde otras aplicaciones**. El software admite los siguientes formatos:

- **PWDUMP** - a pesar de muchas desventajas, este es un formato estándar de facto para almacenar hashes de contraseña. Nota importante: Este formato no es totalmente compatible con los caracteres nacionales. Por lo tanto, es posible que algunos nombres de usuario o comentarios no se muestren correctamente. Windows Password Recovery también admite archivos PWDUMP textuales en UNICODE.
- **LophtCrack** (*.lcs) - este formato de archivo es utilizado por el software LophtCrack. El programa es compatible con todas las versiones de archivos LCS, comenzando con v4.
- **Archivos de proyecto *.hdt,** que son utilizados por Proactive Password Auditor (solía ser PWSEX) de ElcomSoft. También es compatible con todas las versiones del formato, comenzando con v3.
- ***.hsh**, que son exportados por Proactive System Password Recovery de la misma compañía notoria.
- **Hash lists *.lst**, creado por Cain & Abel. Windows Password Recovery admite archivos lst a partir de v.4.9.12. Las versiones anteriores de los archivos LST usaban el delimitador ';' en lugar de 'TAB'. Desafortunadamente, el archivo LST no tiene un marcador que especifique la versión; por lo tanto, si el archivo LST es ilegible, es posible que tenga que reemplazar manualmente todos los delimitadores de campo con el 'TAB'.

- ***.winpsw** archivos, creados por WinPassword, a partir de LastBit. Soporta todas las versiones de WINPSW, comenzando con v6.
- **Archivos de proyecto SamInside (*.hashes).** Este formato es similar al texto PWDUMP, pero es mas flexible y utiliza el caracter 0x7f en lugar de dos puntos, lo cual es mas razonable.
- **Archivos de proyecto de PasswordPro (*.hashes)**. Este formato es similar al texto PWDUMP, excepto varios cambios. Es utilizado por el producto PasswordsPro.
- **Archivos de configuración universal de Passcape (*.puc).** Este contenedor se utiliza en Reset Windows Password y puede contener varios volcados diferentes.
- **Hashes simples (*.*).** Hashes sin procesar en formato de texto sin formato (32 o 16 caracteres en una línea).
- **Archivos de exportación/importación de Passcape (*.peif).** Este formato contiene credenciales de dominio almacenadas en caché y es utilizado por el software Passcape. Por ejemplo, en Recuperación de contraseña de red.
- **Archivos PSPR de Elcomsoft (*.dcc).** Archivos textuales que contienen credenciales almacenadas en caché de dominio.
- **Archivos CACHEDUMP (*.txt o *.cachedump).** Un marcador de posición estándar para los hashes de tipo 1 de credenciales almacenadas en caché de dominio. Este formato está obsoleto.
- **Archivos DCC2 de John The Ripper (*.txt).** Un formato hash DCC2 utilizado en John The Ripper.

Después de importar hashes, el programa marca automáticamente todos los hashes LM o NT y lanza el ataque preliminar. Esta acción es opcional y se puede desactivar en la configuración general. Esta opción está habilitada de forma predeterminada.

2.2.1.5 Importación de hashes desde carpetas de restauración del sistema



Otra opción, no menos útil, es **importar hashes desde las carpetas de restauración del sistema**. Todo lo que necesitaría para eso es especificar la ruta a uno de los discos. El programa encontrará

automáticamente las carpetas de recuperación y, si encuentra los archivos necesarios, importará los hashes.

La búsqueda se realiza, en primer lugar, en el directorio del sistema. En segundo lugar, en la carpeta '%Windows%\Repair', que normalmente contiene copias de seguridad del registro del sistema. En tercer lugar, en la carpeta 'Información del volumen del sistema', que se utiliza para deshacer los cambios realizados en el sistema. Esta tecnología ha estado disponible desde Windows XP y también se conoce como Restaurar sistema (XP) o Shadow Coping (Vista +).

Sin embargo, tenga cuidado, ¡las copias de seguridad del registro pueden contener datos obsoletos!

2.2.2 Exportar

Todos los hashes del proyecto, junto con la configuración, se almacenan en el archivo del proyecto (*.wpr); sin embargo, en aras de una mayor flexibilidad y compatibilidad con otro software, el programa puede exportar hashes a archivos PWDUMP o POT. Si se elige 'Exportar a POT', todas las contraseñas encontradas junto con los hashes de contraseña correspondientes (excepto los de LM) se guardarán en el archivo en el siguiente formato:
hash:contraseña

Puede modificar el formato de salida predeterminado manteniendo presionada la tecla MAYÚS al hacer clic en 'Exportar a POT'. En ese caso, el formato de salida debería verse así:
user (rid):password

Las contraseñas están codificadas en UTF8.

2.2.3 Nuevo

Guarda el proyecto actual y crea uno nuevo.

2.2.4 Abrir

Carga/abre un nuevo proyecto. Los proyectos de la aplicación tienen la extensión *.wpr y contienen la configuración del programa y los hashes. Sin embargo, para acelerar la velocidad de búsqueda, el programa almacena el estado actual del ataque en un archivo separado "progress.ini".

2.2.5 Guardar

Guarda el proyecto actual. Se recomienda guardar proyectos críticos de vez en cuando.

2.2.6 Guardar como

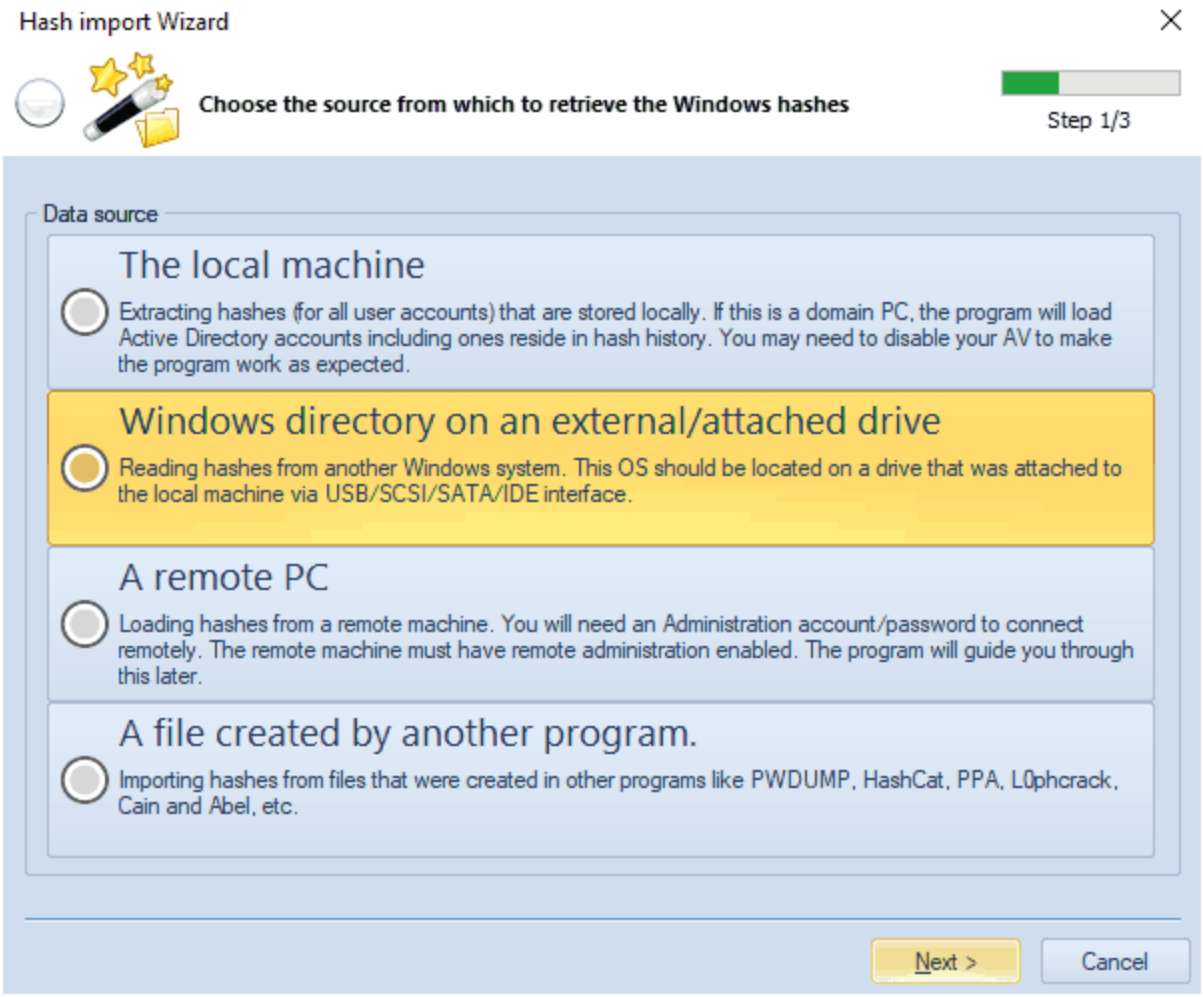
Guarda el proyecto actual con un nombre diferente (le cambia el nombre).

2.2.7 Cerrar

Cierra el proyecto actual.

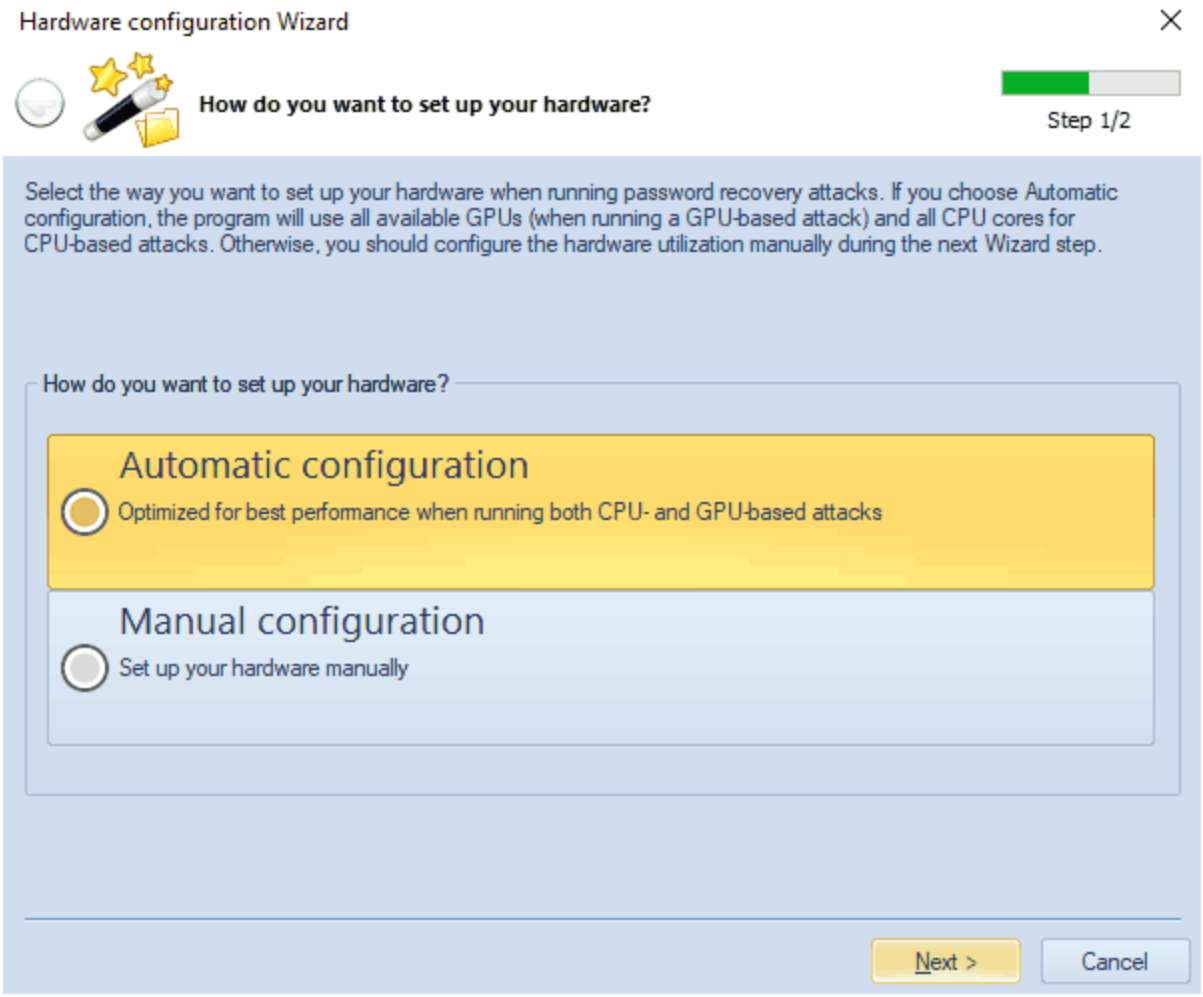
2.2.8 Asistente de importación de hash

El asistente de importación de hash ayuda a cargar hashes de Windows sin sobrecargarlo con opciones y preguntas innecesarias. Por ejemplo, para importar hashes desde otro sistema operativo, todo lo que necesita es especificar el directorio de Origen de Windows. El resto se harán automáticamente. WPR determinará el tipo de hashes (locales o Active Directory), activará el modo de búsqueda de contraseñas de texto sin formato en el disco de destino, cargará cuentas eliminadas / deshabilitadas, hashes de historial, datos biométricos, etc.
Hay 4 fuentes de datos generales para elegir: una computadora local, un sistema operativo externo, una PC remota y un archivo hash creado en otro programa.



2.2.9 Asistente de configuración de hardware

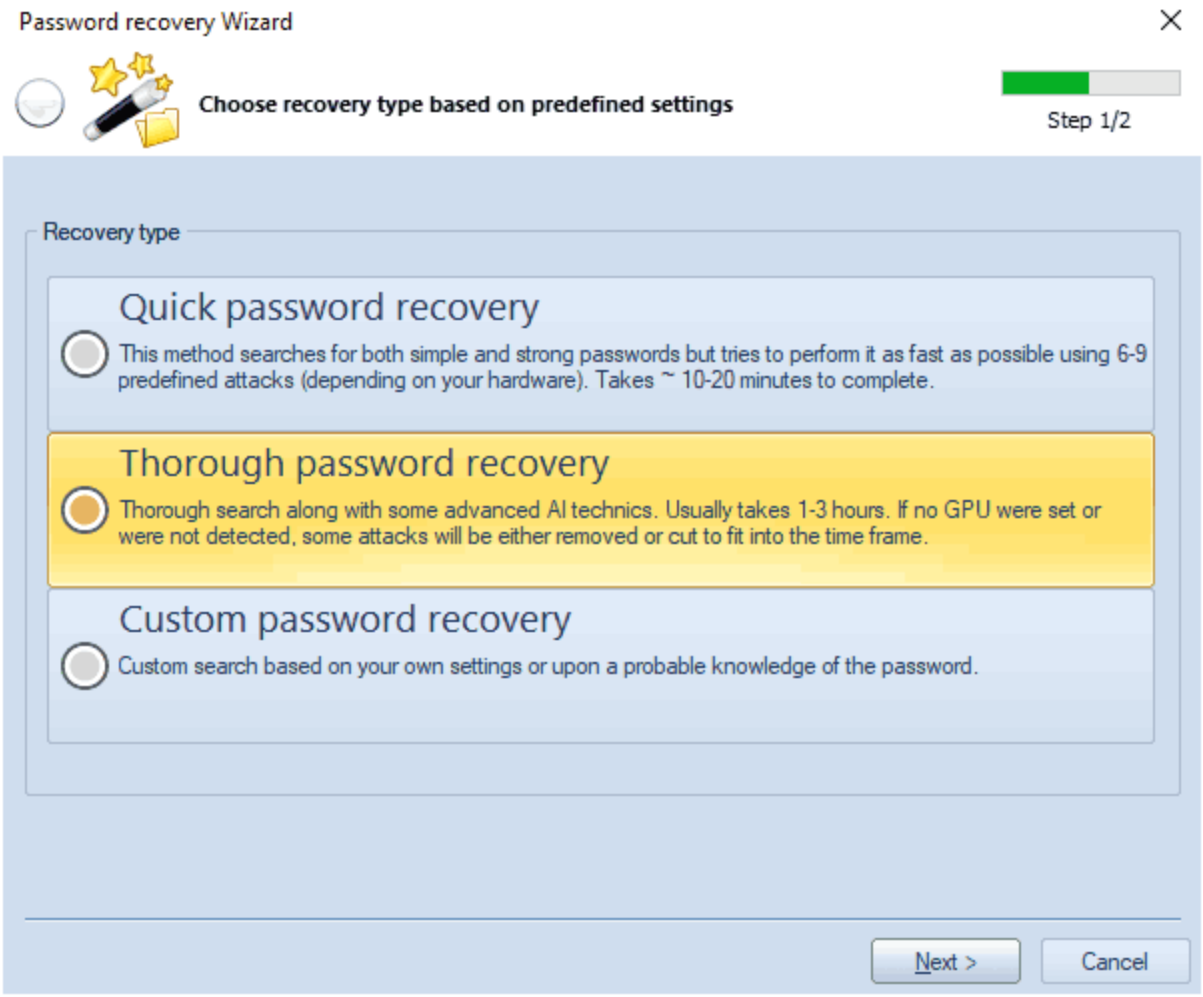
Es una buena idea usar el Asistente de configuración de hardware para configurar el hardware que se utilizará en la recuperación de contraseñas. Puede elegir entre los modos automático y manual. El primer modo automático determina la configuración adecuada para el equipo. Si necesita liberar algunos recursos de CPU / GPU, considere probar el modo manual en su lugar.
Una vez que el modo automático está habilitado, todas las opciones de CPU y GPU (en Opciones generales) no estarán disponibles hasta que vuelva al modo manual.



2.2.10 Asistente de recuperación de contraseña

El asistente de recuperación utiliza los mejores y más actualizados algoritmos de búsqueda de contraseñas que se han inventado en los últimos años. Y no son solo palabras simples. Estos son solo algunos hechos:

- La seguridad de la recuperación de la contraseña depende del hardware utilizado.
- Para lograr el mejor resultado, el programa lanza diferentes ataques que se combinan de manera óptima para buscar diferentes tipos de contraseñas.
- El modo de búsqueda exhaustiva utiliza tanto el poder de la inteligencia artificial como los algoritmos para generar contraseñas basadas en patrones encontrados.
- El modo de búsqueda exhaustiva encuentra más contraseñas que cualquier programa similar.



2.3 Menú de recuperación

Este elemento de menú permite seleccionar y lanzar un ataque. El panel *'Ataque'* permite seleccionar el tipo de ataque y alternar entre los hashes LM o NT atacantes. Tenga en cuenta que antes de lanzar el ataque debe haber seleccionado / marcado los hashes necesarios. Puede hacerlo a través del menú Editar y seleccionar. Al iniciar el ataque, se supone que también ha realizado todos los ajustes necesarios (en el menú **Opciones-Opciones de ataque**).

2.3.1 Ejecutar

Lanza el ataque seleccionado. Cuando el ataque se está ejecutando, todos los demás elementos del menú están deshabilitados. Tenga en cuenta que cuando el ataque ha terminado, el programa ejecuta una rutina especial de análisis de mutaciones y contraseñas sobre las contraseñas encontradas. Esta opción está habilitada de forma predeterminada, pero se puede deshabilitar en la configuración general.

2.3.2 Continuar

Reanuda el ataque desde el último punto almacenado. Recuerde que el último punto almacenado se borra automáticamente cuando se realizan cambios en las opciones del ataque.

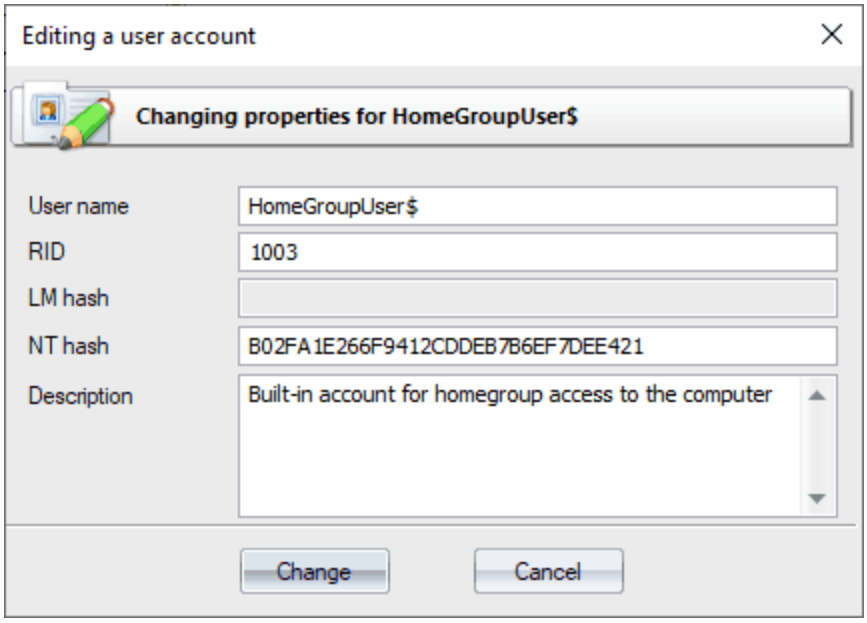
2.3.3 Detener

Pausa el ataque actual.

2.4 Menú Editar

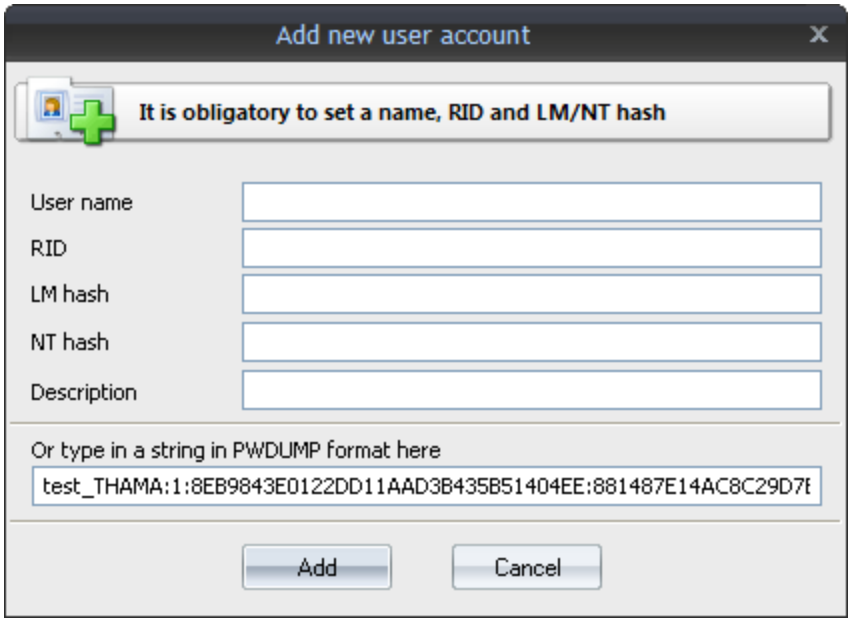
El menú Editar solo está disponible cuando la pestaña '*Hashes*' está activa; incluye cuatro elementos: Editar, Copiar, Seleccionar y Buscar.

2.4.1 Editar



Al seleccionar este elemento, se abre el cuadro de diálogo donde puede editar manualmente los siguientes campos para la cuenta seleccionada: nombre de usuario, RID de usuario, hashes LM/NT o DCC, además del comentario a la cuenta.

2.4.2 Agregar



Este elemento permite agregar elementos manualmente. Permite introducir cadenas tipo PWDUMP.

2.4.3 Borrar

Elimina las entradas de la lista: resaltadas (es decir, la que está debajo del cursor), marcadas o todas a la vez.

2.4.4 Restablecer contraseñas

Elimina todas las contraseñas encontradas de la lista.

2.4.5 Copiar

Copia la entrada actual (resaltada) en el portapapeles de Windows. Copia solo la parte seleccionada de la entrada, no la entrada completa. Por ejemplo, el nombre de usuario o la contraseña encontrada.

2.4.6 Seleccionar

Selecciona los hashes que se atacarían (los que tienen la opción de casilla de verificación está encendida). Si durante el ataque se encuentra la contraseña para el hash seleccionado, la casilla de verificación se borrará automáticamente y el registro se marcará en verde. Para seleccionar los hashes NT, primero debe haber anulado la selección de los hashes LM y al revés.

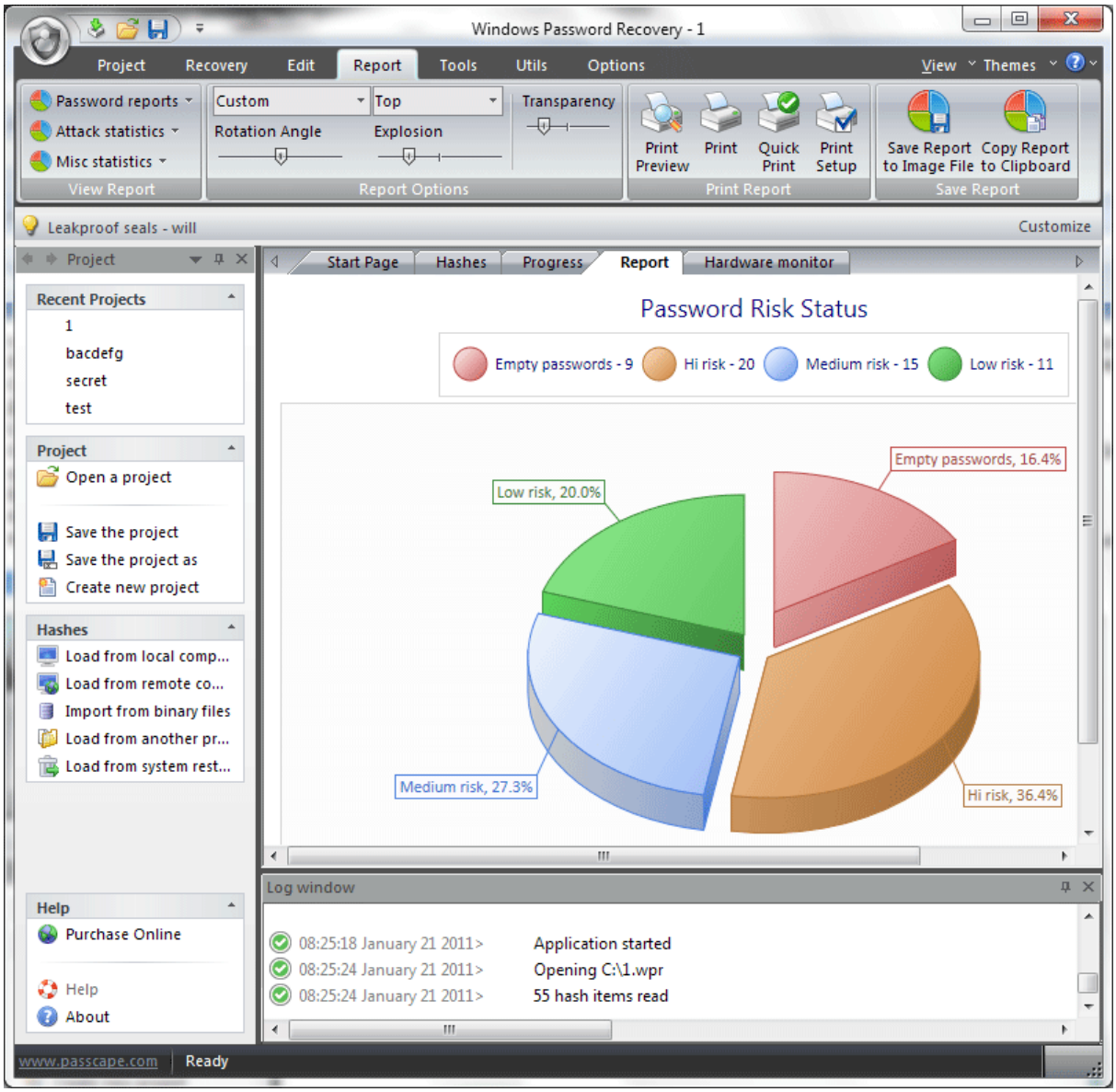
2.4.7 Buscar

Cuando el número de entradas supera los cien miles, encontrar una entrada específica a menudo requiere bastante esfuerzo. Para facilitar el trabajo, el programa ofrece la búsqueda de dos tipos: búsqueda de un campo específico, por ejemplo, nombre de usuario, y búsqueda rápida de entradas en serie. En este último caso, el programa escanea toda la entrada, carácter por carácter.

2.5 Menú Informes

Puede crear, imprimir o guardar uno de los informes del programa aquí. Los siguientes informes están disponibles:

- Informes de contraseñas
- Estadísticas de ataques
- Estadísticas diversas
- Estadísticas de la cuenta
- Análisis de lista de contraseñas
- Información del grupo

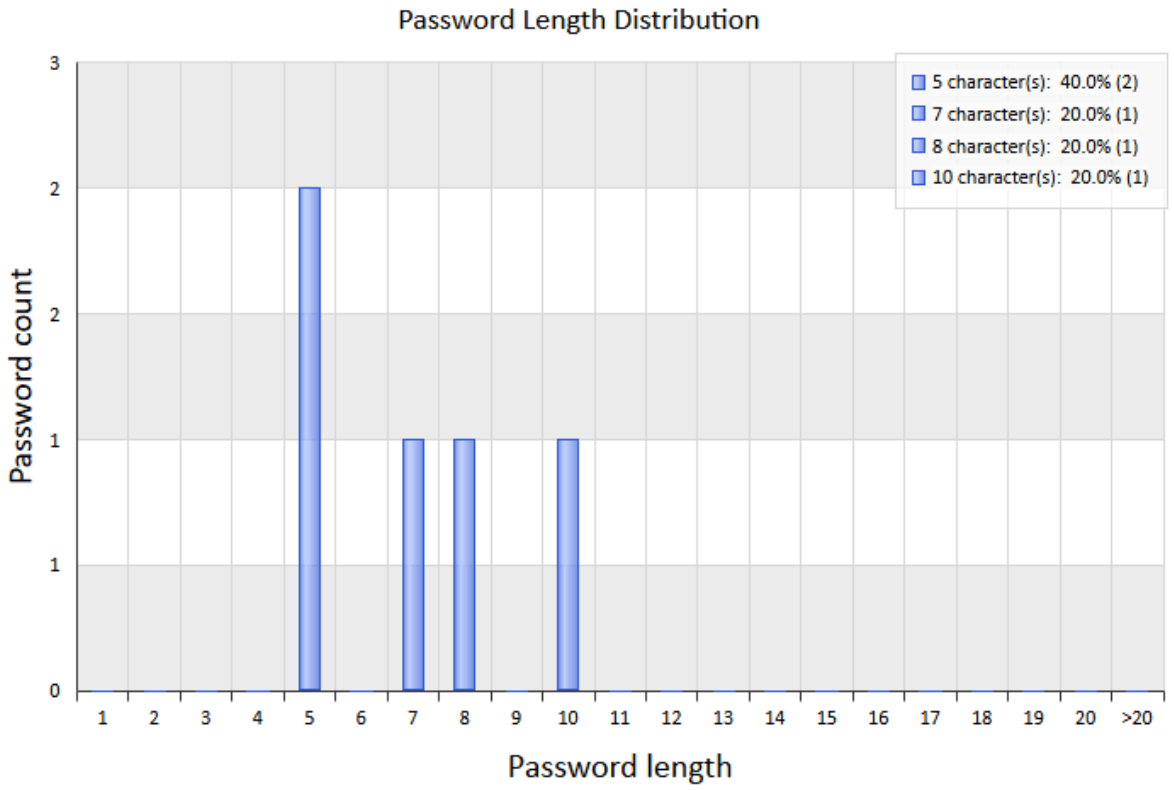


2.5.1 Informes de contraseñas

Los siguientes informes están disponibles aquí

- **Estado de riesgo de la contraseña** - muestra contraseñas vacías, encontradas y no recuperadas
- **Complejidad de la contraseña** - informa del número de contraseñas y varios conjuntos de caracteres que se están auditando
- **Distribución de la longitud de la contraseña** - muestra la longitud total de las contraseñas rotas
- **Singularidad de la contraseña** - este informe muestra un contraseña única contra contraseñas reutilizadas.

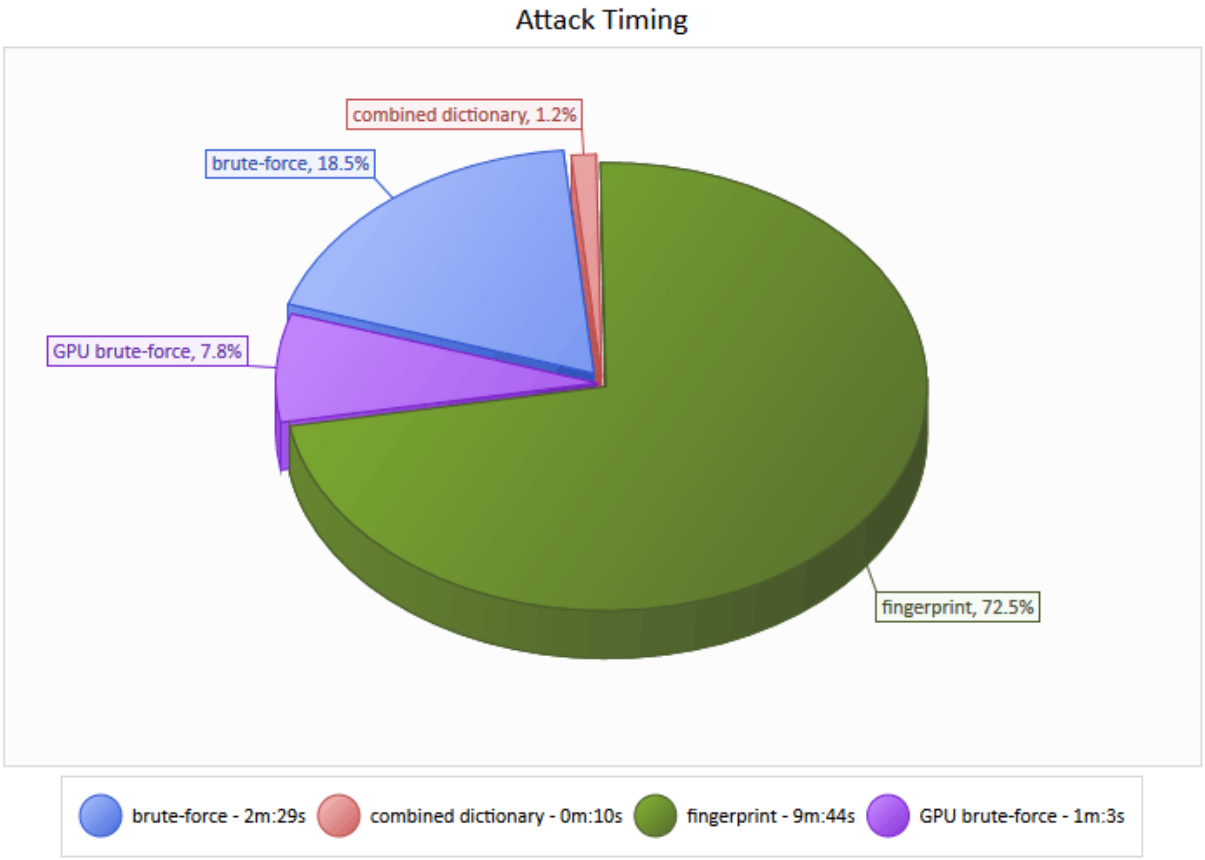
- **Principales contraseñas reutilizadas** - muestra las 20 contraseñas más populares.
- **LM vs NT** - informa del número de hashes LM y NT
- **Contraseñas regulares vs historial** - informa del número de contraseñas comunes y de historial (solo para hashes importados desde SAM/NTDS. Archivos DIT; Eg. importado desde un equipo local)
- **Tiempo de recuperación de contraseña** - tiempo tomado en descifrar una determinada contraseña(s). Las contraseñas más vulnerables están marcadas en una paleta roja.
- **Contraseñas recuperadas vs intactas** - muestra el número de contraseñas descubiertas y no encontradas
- **Contraseñas encontradas** - muestra un informe un poco detallado sobre las contraseñas encontradas



2.5.2 Estadísticas de ataques

Las estadísticas de ataques incluyen los siguientes elementos:

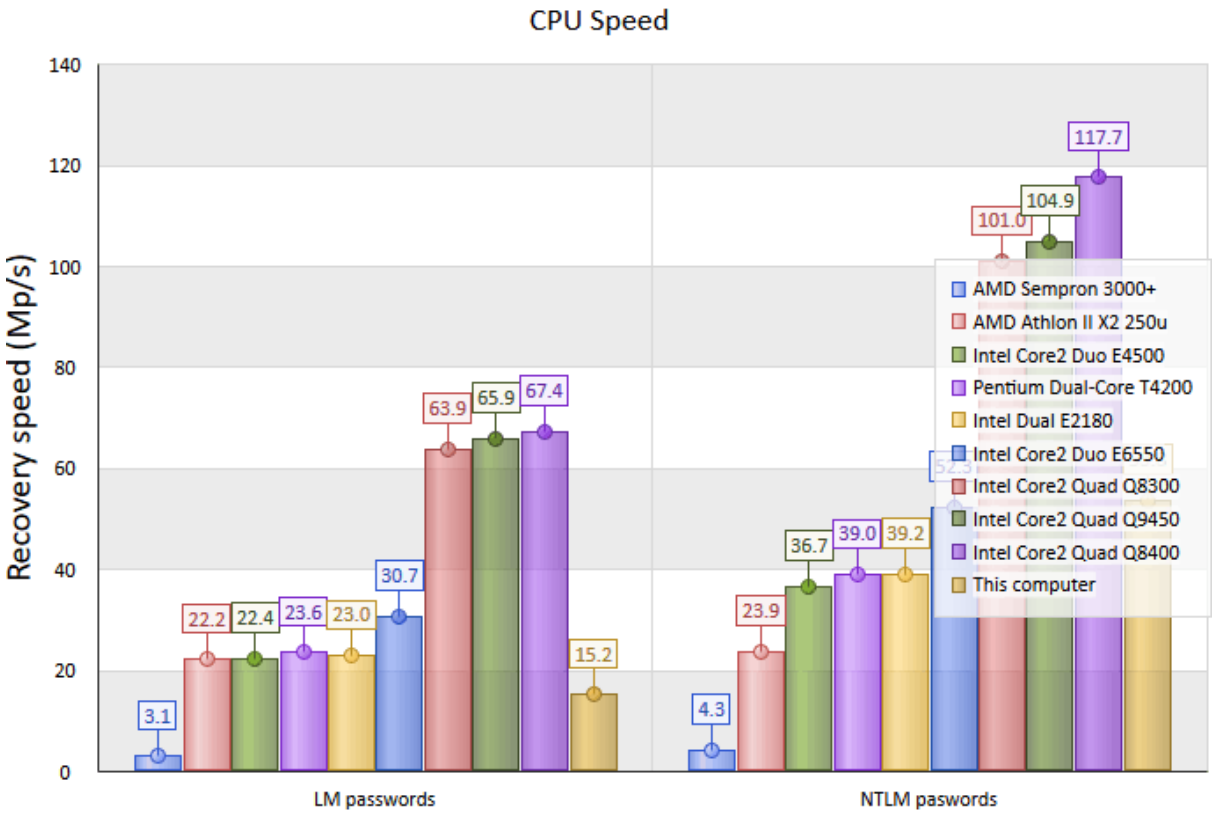
- **Ataque preferido** - estadísticas sobre el número y el tipo de ataques utilizados.
- **Tiempo de ataque** - análisis del tiempo dedicado a cada ataque.
- **Eficiencia del ataque1** - análisis de eficiencia: tiempo empleado frente a contraseñas encontradas durante la relación de ataque.
- **Eficiencia del ataque2** - análisis de eficiencia: eficiencia general para cada ataque.



2.5.3 Estadísticas diversas

Algunas cosas adicionales como:

- **Velocidad de la CPU** - password recovery speed comparison (for brute-force attack).
- **Velocidad de la GPU** - muestra y compara la velocidad de recuperación de contraseña para su dispositivo GPU. Puede comparar el rendimiento de su CPU o GPU utilizando el Herramienta Pass-o-meter.
- **Usuarios crackeados** - muestra el número de usuarios descifrados. La lista completa de cuentas de usuario descifradas se puede guardar en un archivo de texto adicionalmente.
- **Usuarios y contraseñas crackeados** - muestra la lista de cuentas descifradas con contraseñas.

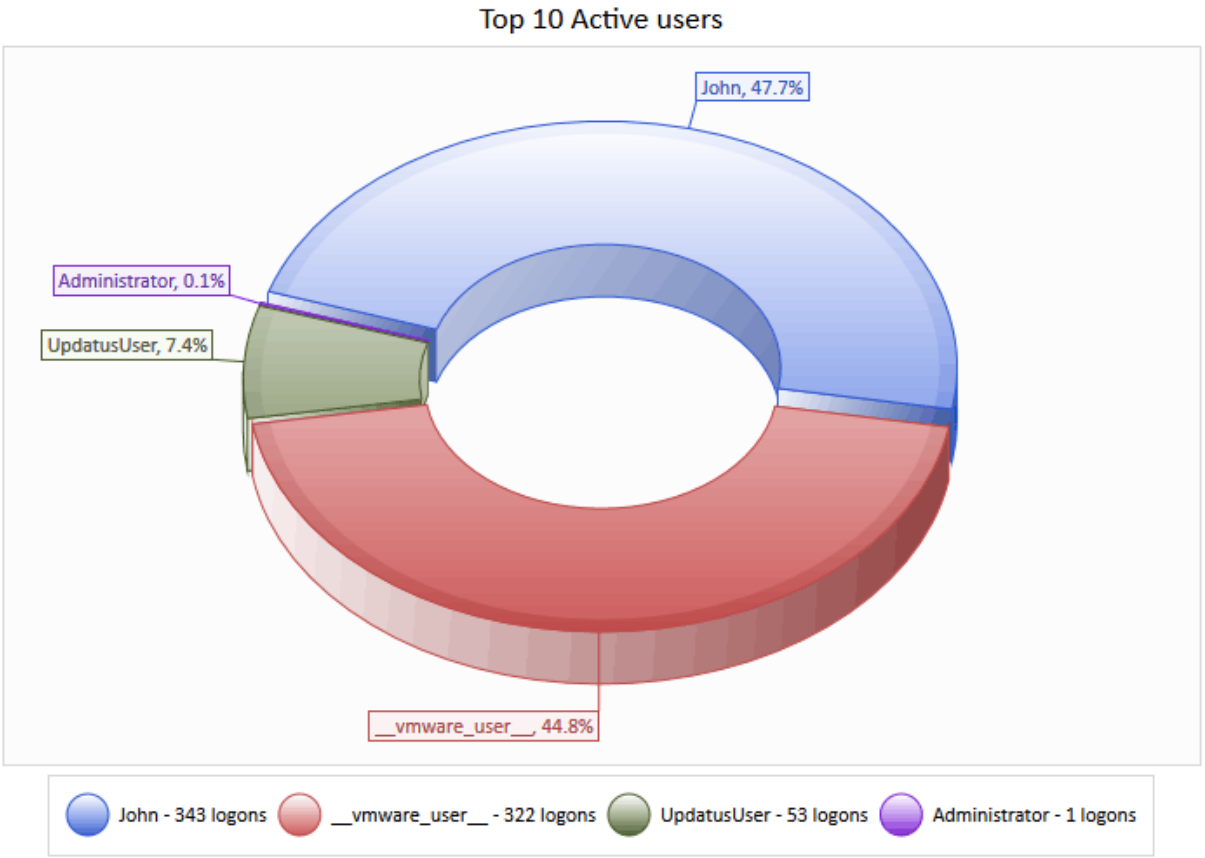


2.5.4 Estadísticas de la cuenta

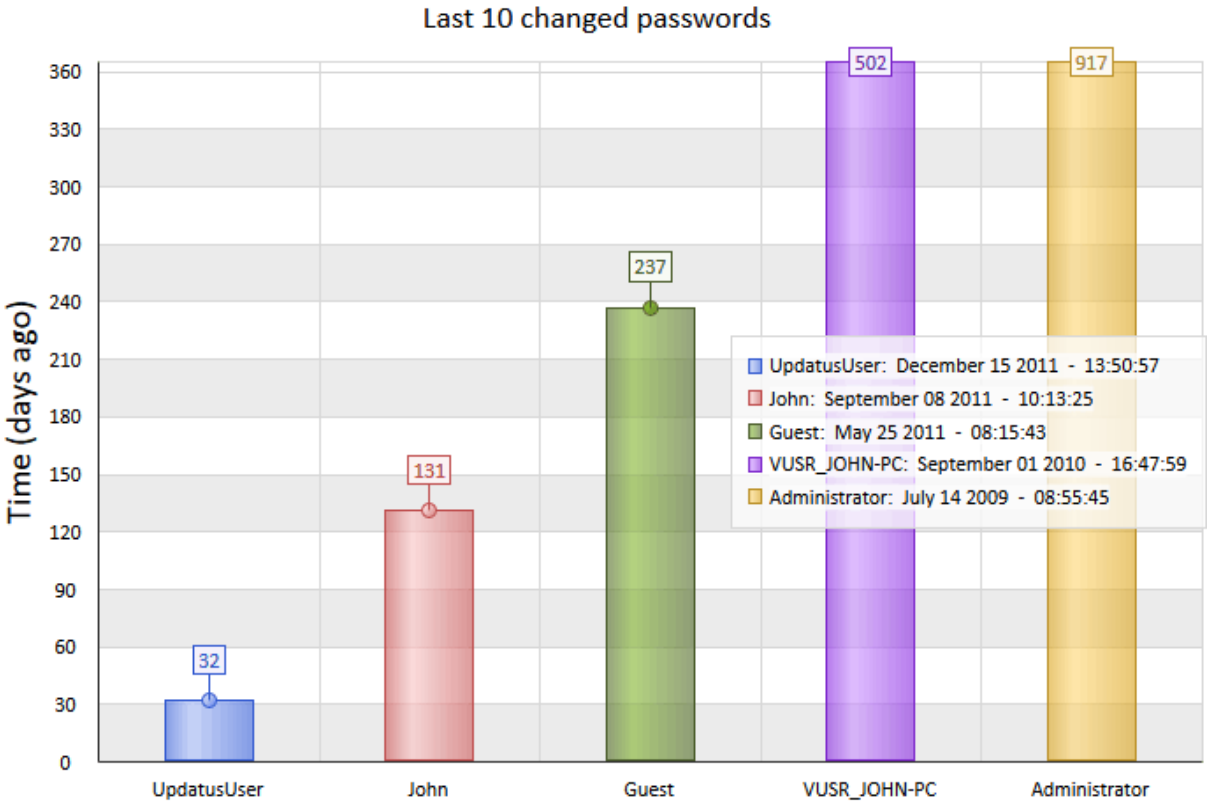
Las estadísticas de cuenta están disponibles tanto para las cuentas locales como para las de dominio. Para generar un informe, primero seleccione el origen de datos: base de datos local o externa, SAM o Active Directory. Estos son los informes disponibles en esta categoría:

- **Cuentas regulares vs. deshabilitadas.** Este informe muestra la proporción de cuentas de usuario regulares vs. deshabilitadas.
- **Cuentas regulares vs. bloqueadas.** Relación entre cuentas regulares vs. bloqueadas/bloqueadas.
- **Con/sin contraseña.** Muestra el número de cuentas con contraseñas en blanco y establecidas.
- **Usuario vs. Cuentas de maquina.** Relación entre las cuentas de usuario y de sistema.
- **Activas vs. contraseñas expiradas.** Informe con estadísticas sobre cuentas con contraseñas activas frente a contraseñas caducadas.
- **Contraseñas regulares vs nunca caducadas** - compara las cuentas de usuario normales con aquellas con la bandera *'La contraseña nunca caduca'* o la contraseña ilimitada establecida en vivo.
- **Administradores vs. usuarios limitados.** Este informe ofrece estadísticas comparativas sobre cuentas con derechos administrativos frente a cuentas de usuario restringidas.
- **Tipos de cuenta.** muestra la cantidad de cuentas de máquina, usuario, administrador, etc.
- **Estado de la cuenta.** muestra las cuentas activas contra las deshabilitadas. El mismo que el primer informe de la lista, pero no contiene ningún panel adicional sobre las cuentas deshabilitadas.
- **Los 10 principales usuarios activos.** Informe sobre los 10 usuarios más activos del sistema operativo. Las estadísticas se recopilan del contador de inicio de sesión de usuario interno del sistema.

- **Inicios de sesión con contraseña incorrecta.** Los 10 usuarios principales con las tasas más altas en el contador de inicio de sesión fallido.



- **Últimos 10 inicios de sesión fallidos** - muestra la lista de cuentas de usuario que intentaron iniciar sesión sin éxito.
- **Últimas 10 contraseñas cambiadas** - muestra la hora de los últimos 10 usuarios que cambiaron sus contraseñas.
- **Últimos 10 inicios de sesión** - muestra la hora de los últimos 10 usuarios que iniciaron sesión correctamente en el sistema.
- **Últimos 10 cierres de sesión** - la hora en la que las últimas 10 cuentas cerraron la sesión.
- **Cuentas por expirar pronto** - cuentas de usuario que caducarán pronto.
- **Actividad de inicio de sesión** - agrupa a los usuarios por el tiempo transcurrido desde el último inicio de sesión en el sistema.
- **Antigüedad de la contraseña -** agrupa a los usuarios por el tiempo transcurrido desde el último conjunto/cambio de contraseña.



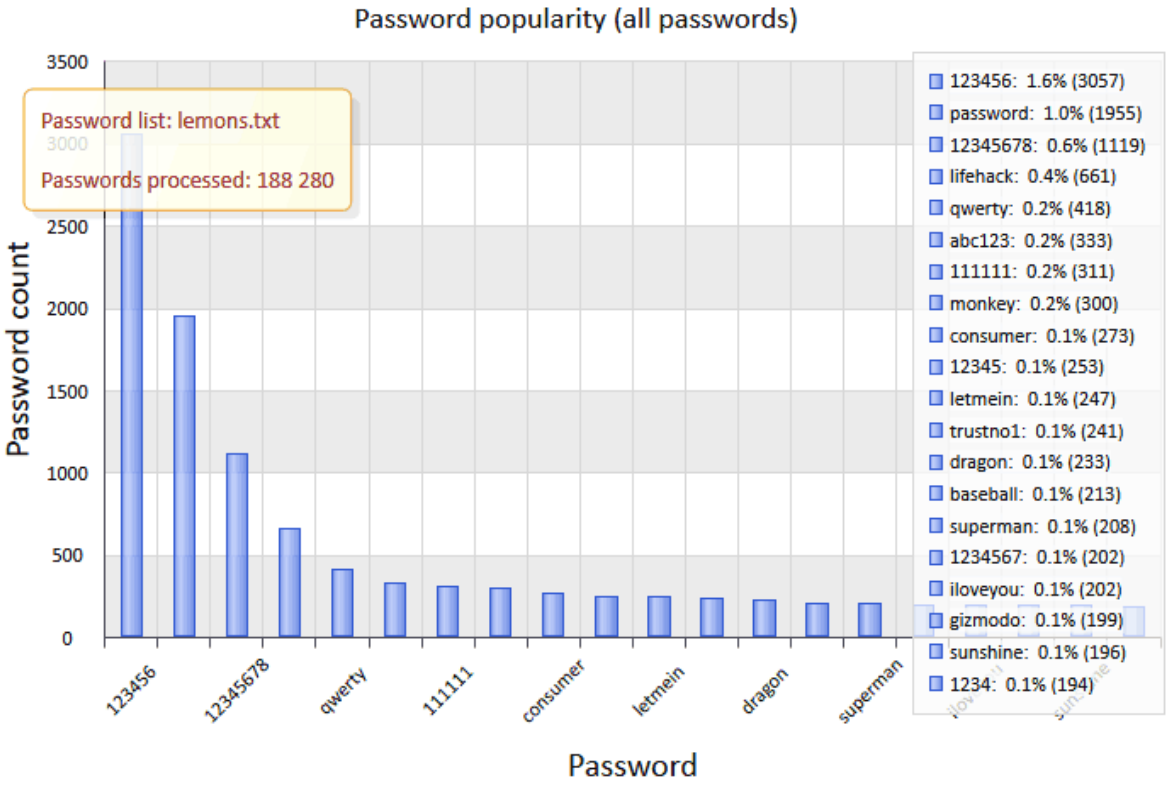
Puede guardar información adicional en un archivo de texto haciendo clic con el botón del mouse en una parte del informe.

2.5.5 Análisis de lista de contraseñas

Password-list reports display various statistics and perform a deep analysis for input wordlists. As a source wordlists you can use, for example, the list of passwords recovered by the program. You can generate reports for all words of the input list as well as for passwords with a certain length only. The following reports are available here:

- **Distribución de la longitud de la contraseña** - muestra la longitud total de la contraseña en una lista de palabras determinada.
- **Singularidad de la contraseña** - este informe muestra un contraseña única contra contraseñas reutilizadas.
- **Popularidad de la contraseña** - muestra las contraseñas más populares y su porcentaje del número total de contraseñas.
- **Formato de contraseña** - estadísticas sobre los 20 formatos más populares. El formato de contraseña se define mediante una máscara de caracteres. Por ejemplo, la máscara DDUUUUDD corresponde a contraseñas que constan de dos dígitos iniciales y dos finales, con cuatro letras mayúsculas en el medio. Puede guardar máscaras de contraseña populares en un archivo para que pueda usarlas fácilmente en un ataque basado en máscaras más adelante.
- **Exclusividad del juego de caracteres** - este informe muestra el número de contraseñas que consisten en un conjunto de caracteres único y el porcentaje de estas contraseñas a las que constan de varias.

- **Diversidad de conjuntos de caracteres** - la proporción porcentual de contraseñas que consta de uno, dos o más juegos de caracteres.
- **Conjuntos de caracteres** - enumera todos los conjuntos de caracteres de los que están hechos
- **Orden del juego de caracteres** - las plantillas de contraseña más populares correspondientes al orden del juego de caracteres. Por ejemplo, la plantilla digit-string-special incluye las siguientes contraseñas: 123password!@#, 1ove*****, y 12monkey^, etc.
- **Frecuencia de caracteres** - estadísticas sobre la frecuencia de caracteres en las palabras de entrada. Se muestran los 20 caracteres más frecuentes.
- **Caracteres únicos** - los 20 caracteres menos frecuentes.
- **Caracteres principales de uso frecuente** - estadísticas sobre las combinaciones más frecuentes de 1 a 3 caracteres al principio de las palabras.
- **Caracteres finales de uso frecuente** - estadísticas sobre las combinaciones más frecuentes de 1 a 5 caracteres al final de las palabras.
- **Combinaciones frecuentes** - las 20 combinaciones más utilizadas de 4 a 8 caracteres.

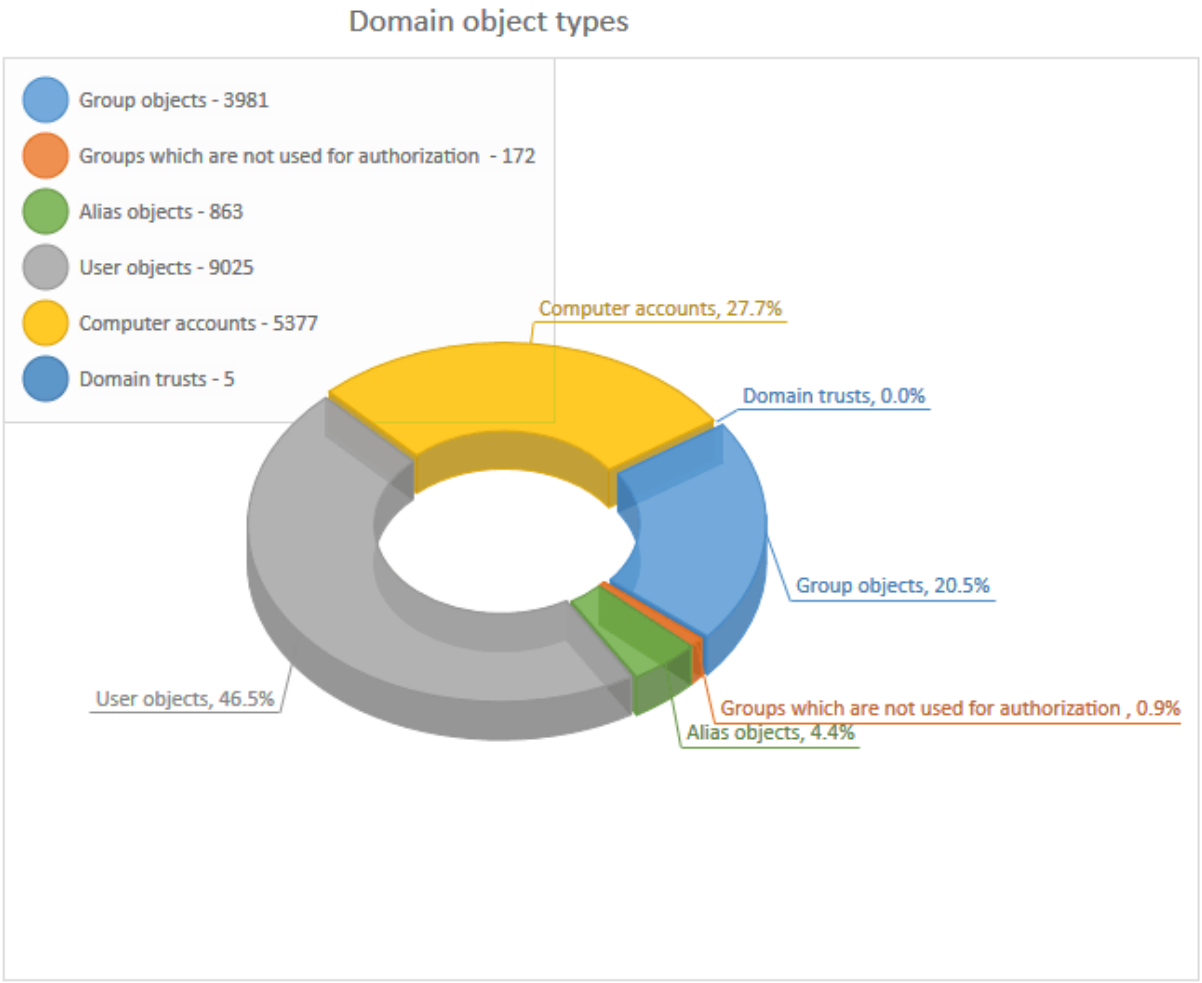


2.5.6 Información del grupo

Esta sección está dirigida principalmente a analizar información diversa sobre grupos y alias de Active Directory. Sin embargo, algunos informes se pueden utilizar para mostrar estadísticas de un EQUIPO local mediante la lectura de información del archivo de registro SAM. Los siguientes informes están disponibles aquí:

- **Últimos 10 grupos creados.** 10 cuentas de grupo creadas recientemente.
- **Últimos 10 grupos modificados.** 10 cuentas de grupo que han cambiado recientemente.
- **Tipos de grupo.** Este informe muestra diferentes tipos a los que pertenecen las cuentas de grupo.
- **Grupos más poblados** - muestra los 10 grupos principales con el mayor número de usuarios.

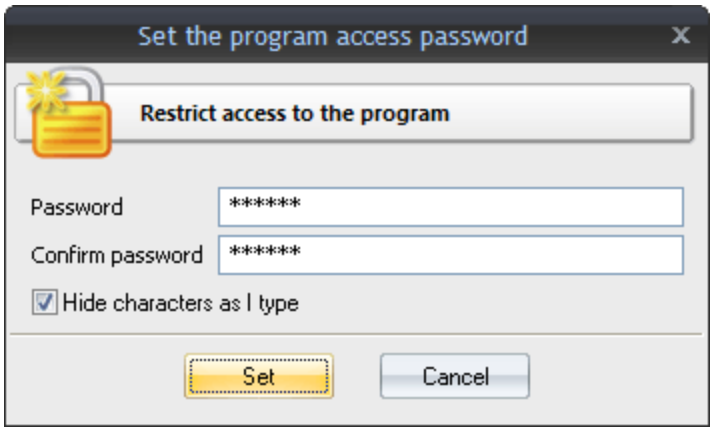
- **Grupos escasamente poblados** - muestra los 10 grupos principales con el menor número de usuarios. Los grupos sin usuarios no se muestran aquí.
- **Grupos activos vs inactivos.** El programa asume que los grupos activos tienen al menos un miembro, mientras que los grupos inactivos no tienen ningún usuario.
- **Grupos de administradores vs no administradores** - muestra estadísticas sobre los privilegios de administrador de los grupos.
- **Últimos 10 alias creados.** 10 cuentas de alias creadas recientemente.
- **Últimos 10 alias modificados.** 10 cuentas de alias modificadas recientemente.
- **Tipos de alias.** Este informe muestra diferentes tipos a los que pertenecen las cuentas de alias.
- **Alias más poblados** - muestra los 10 alias principales con el mayor número de usuarios.
- **Alias escasamente poblados** - muestra los 10 alias principales con el menor número de miembros. No se muestran los alias sin usuarios.
- **Alias activos vs inactivos.** El programa asume que los alias activos tienen al menos un usuario, mientras que los alias inactivos no tienen ningún miembro.
- **Alias de administrador vs no administrador** - muestra cuántos alias tienen privilegios de administrador.
- **Tipos de objetos de dominio** - muestra información sobre todos los objetos encontrados en un dominio. Por ejemplo: usuarios, grupos, cuentas de equipo, confianzas de dominio, etc.



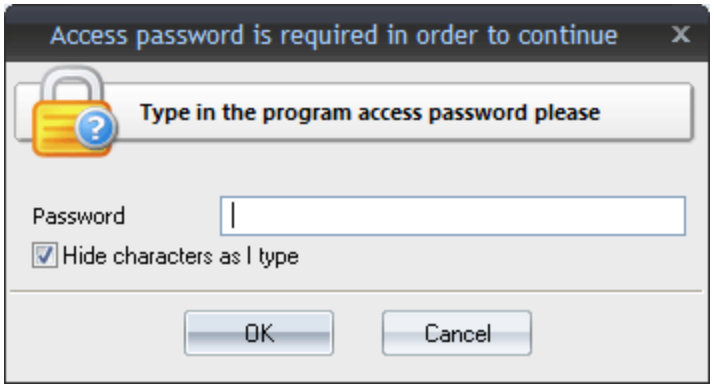
2.6 Menú Herramientas

Las herramientas constan de dos partes: herramientas para controlar el acceso a la aplicación y herramientas para trabajar con contraseñas.

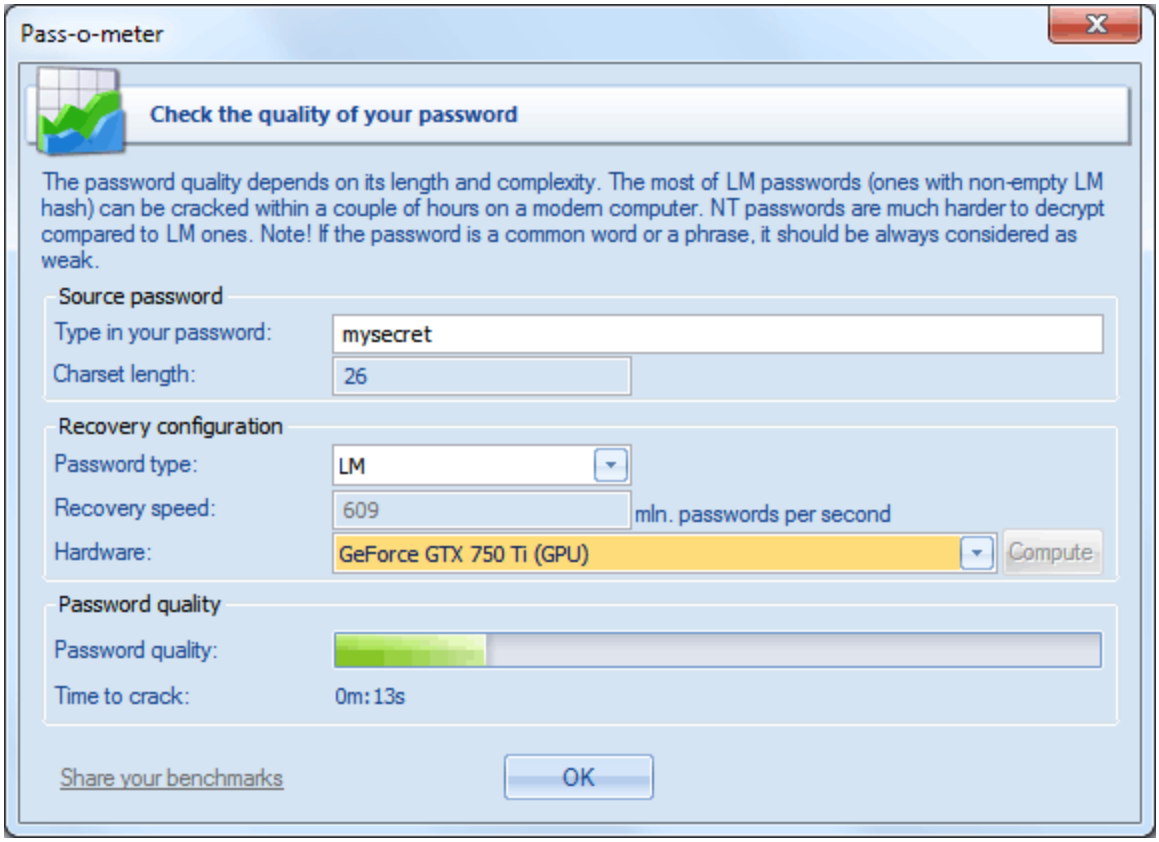
2.6.1 Acceso al programa



Si alguien además de usted puede acceder a su computadora o cuenta, puede proteger la aplicación con contraseña. En este caso, al iniciar el programa, se le pedirá al usuario la contraseña y la aplicación no podrá continuar a menos que se suministre la contraseña válida.



2.6.2 Pass-o-meter



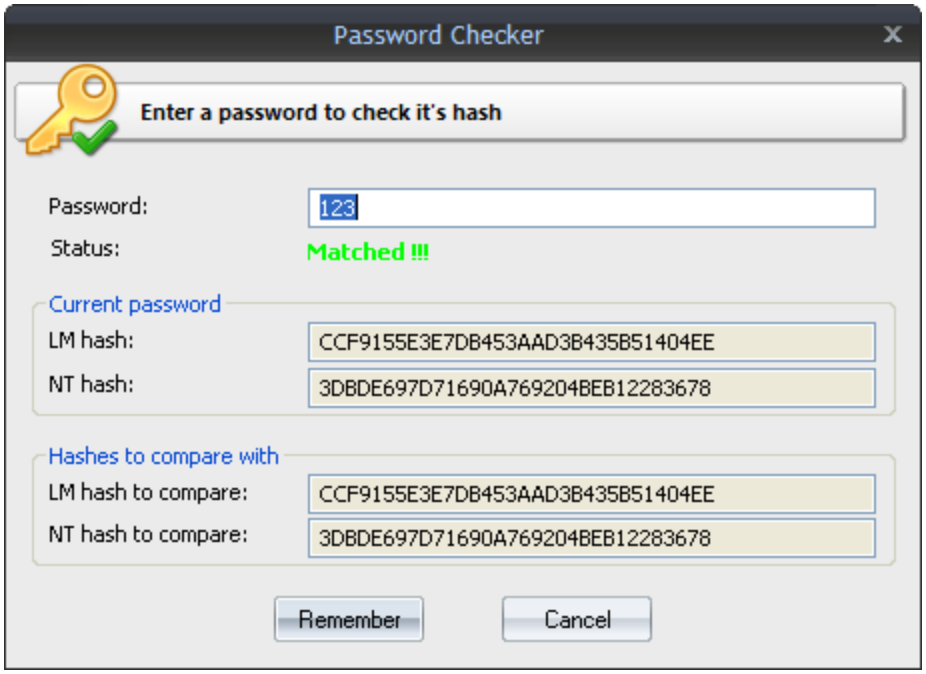
Una herramienta para medir la seguridad de la contraseña. Durante su primer inicio, el programa le pide que pruebe el rendimiento de su computadora. Para comprobar la calidad de una contraseña:

- Introduzca la contraseña en el campo correspondiente.
- Seleccione el tipo de hash: LM o NT. Recuerde que a partir de los sistemas operativos Windows Vista almacenan las contraseñas como hashes NT de forma predeterminada.
- Seleccione el tipo de equipo. *'Esta computadora*' indica la velocidad de búsqueda de su computadora.
- Si desea probar la velocidad de su dispositivo GPU, seleccione *'Esta computadora* (GPU)' en el cuadro combinado '*Hardware*' y haga clic en el botón *'Computar'*. Tenga en cuenta que también puede hacerlo desde el menú Informes.

La calidad de su contraseña, junto con el tiempo que tardaría su computadora con la configuración seleccionada en romperla se mostrará en la parte inferior. Por ejemplo, romper cualquier hash LM de una contraseña alfanumérica tomaría aproximadamente 10 minutos en una CPU moderna (a la velocidad de búsqueda de más de 100 millones de contraseñas por segundo). La velocidad de búsqueda en una GPU puede aumentar en otro orden de magnitud.

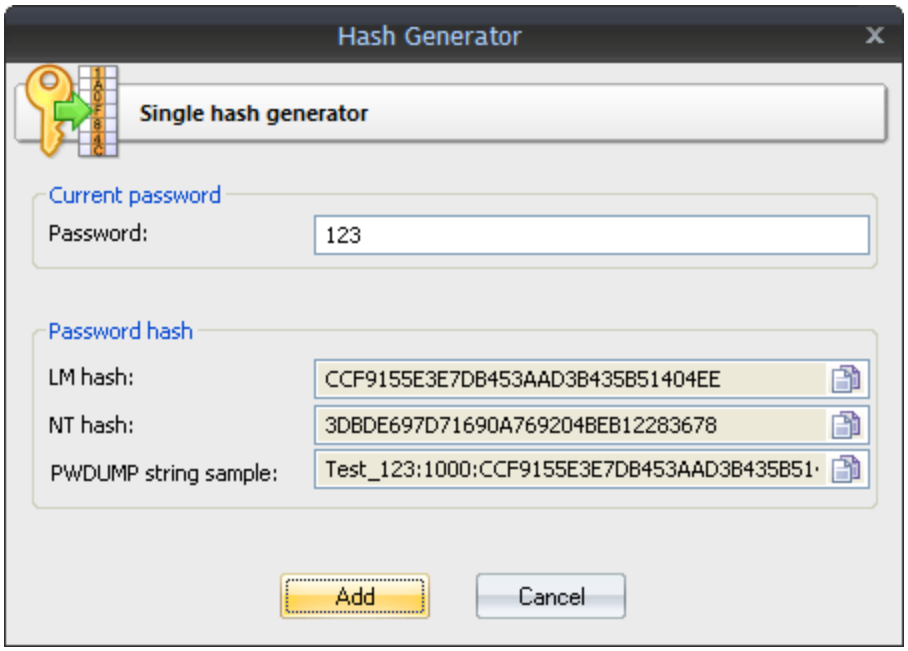
Le agradeceríamos que nos hiciera saber la velocidad que ha alcanzado en su PC.

2.6.3 Comprobador de contraseñas

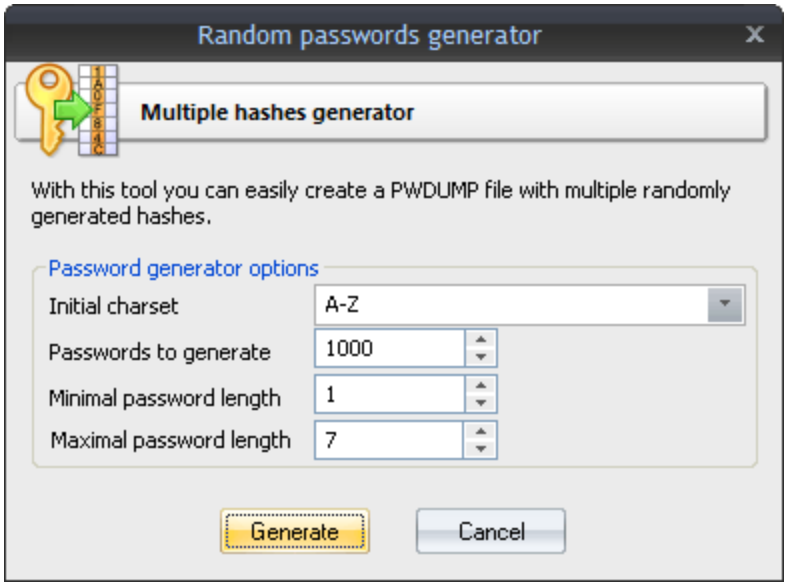


Esta herramienta permite comprobar la contraseña de un hash seleccionado manualmente. La herramienta es a menudo necesaria para validar ciertos hashes. Por ejemplo, cuando un hash LM, por una u otra razón, no coincide con el hash NT de la contraseña.

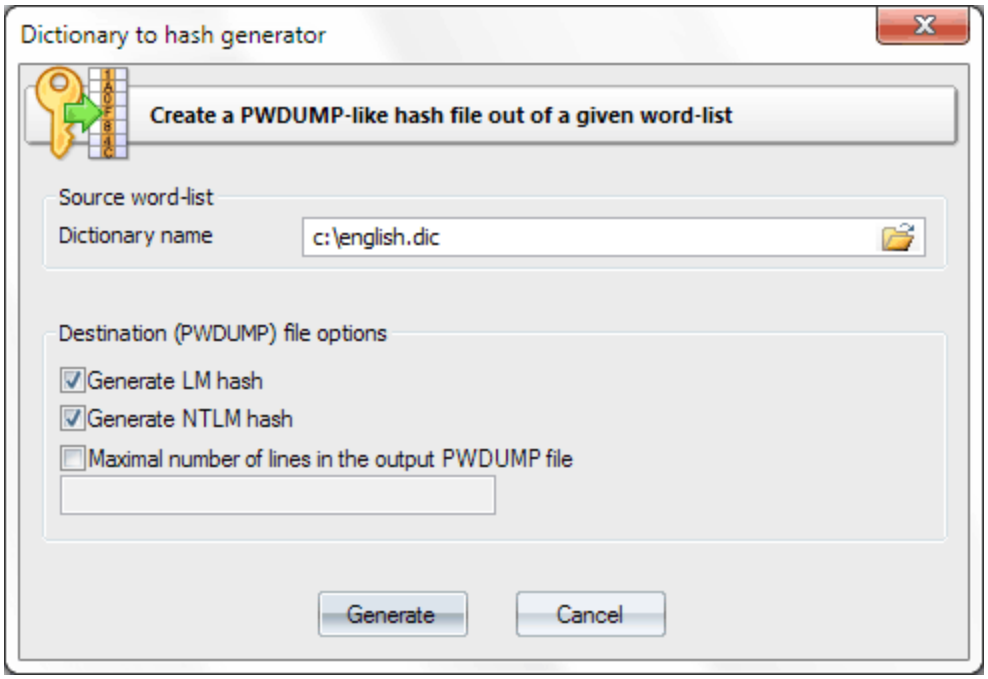
2.6.4 Generador de hash



El generador de hash único permite generar rápidamente una entrada de prueba para una contraseña especificada y agregarla a la lista hash.



Si desea crear un archivo PWDUMP con un número específico de contraseñas generadas aleatoriamente, utilice el generador de hash múltiple. En el nuevo cuadro de diálogo hash, seleccione la longitud mínima y máxima, el intervalo de caracteres y el número total de hashes que se generarán.

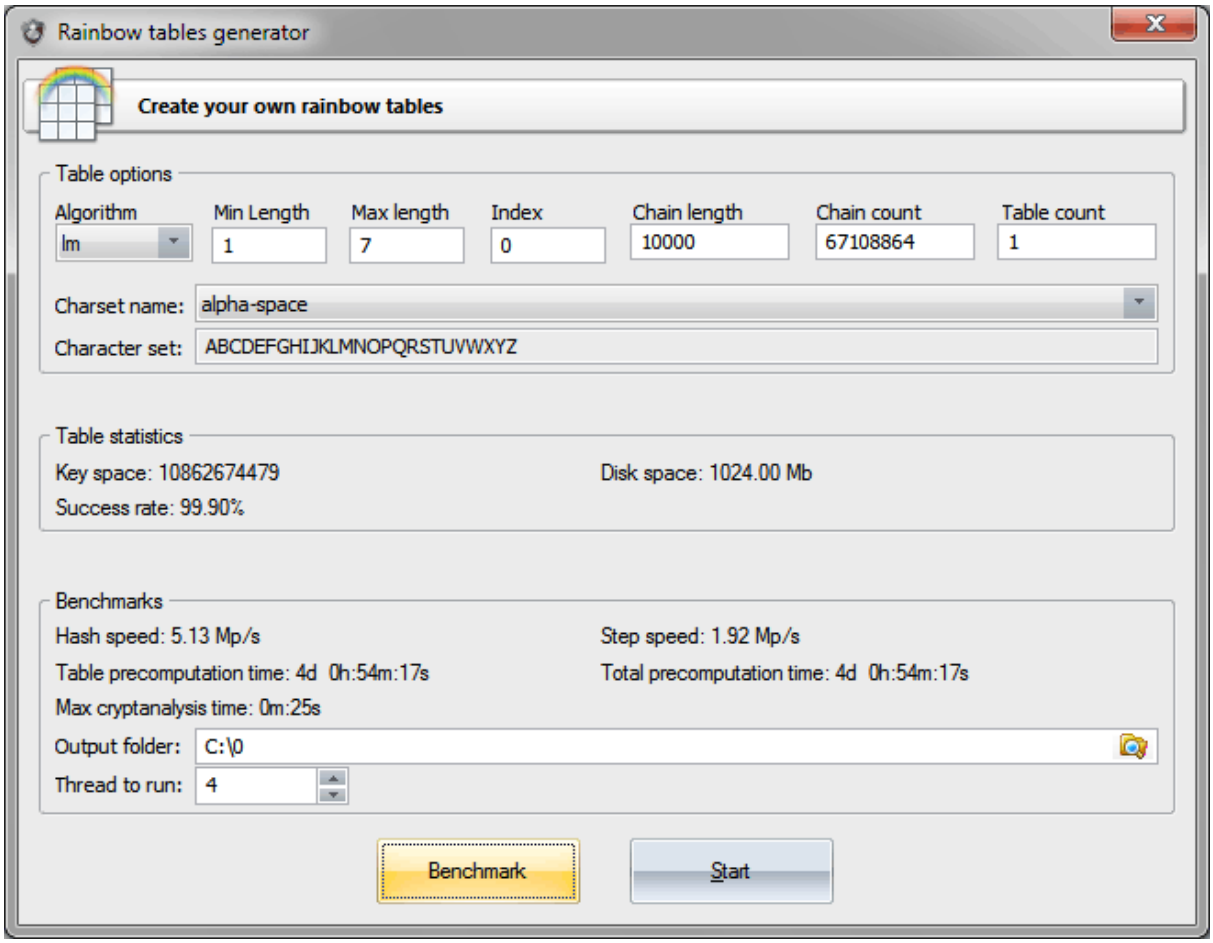


Con el generador de diccionario a hash, puede crear fácilmente un archivo PWDUMP a partir de una lista de palabras determinada. Esta herramienta tiene una serie de opciones adicionales aquí. Por ejemplo, puede limitar el número de elementos hash de salida o crear un archivo PWDUMP solo para hashes NTLM.

2.6.5 Generador de Tablas Rainbow

Las tablas Rainbow son tablas de búsqueda especiales utilizadas para revertir las funciones criptográficas unidireccionales y descifrar contraseñas de texto plano derivadas de las funciones hash. Un ejemplo de tales hashes sería una contraseña de usuario (hashes LM o NTLM) en el sistema operativo Windows.

Windows Password Recovery tiene una implementación de búsqueda de contraseñas mediante tablas Rainbow. Las tablas que requiere se pueden descargar de Internet o crear manualmente con la herramienta de generación RT.



Antes de comenzar a generar sus propias tablas, es importante configurar correctamente las respectivas opciones relacionadas y encontrar su mejor combinación. Primero, seleccione uno de los dos algoritmos (LM o NTLM) que necesita y configure un **conjunto de caracteres** adecuado al que se limitarán las contraseñas. Cuanto más amplio sea el rango de caracteres, más contraseñas se recuperarán en el ataque de la tabla arco iris, pero más tiempo se tardará en precaluar las tablas y, quizás, de mayor tamaño serán.

Las tablas Rainbow se utilizan para recuperar contraseñas de hasta una cierta longitud que debe configurar en los campos **'Longitud mínima'** y **'Longitud máxima'**. Un hash LM en Windows consta

de dos mitades de 7 caracteres; por lo tanto, la longitud máxima de la contraseña que se utilizará al generar tablas LM no debe exceder de 7.

'Longitud de cadena' afecta a los siguientes parámetros de la tabla: tasa de recuperación de contraseña, tiempo de generación de tabla y tiempo que lleva recuperar una sola contraseña por el ataque.

El **recuento de cadenas** afecta la tasa de recuperación de contraseñas, el tiempo de generación de tablas y su tamaño.

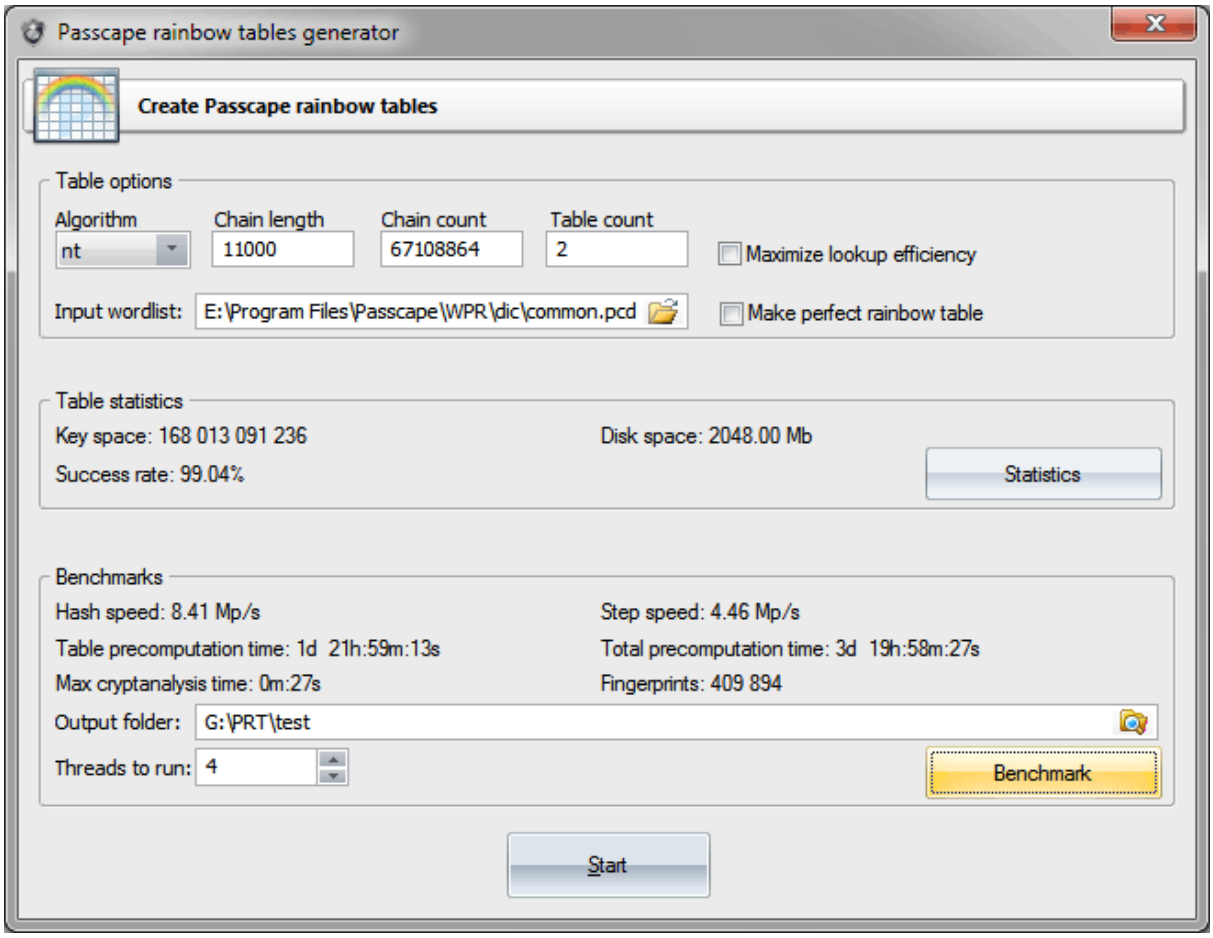
Actualmente, la herramienta de generación RT no admite tablas de más de 2 GB de tamaño; sin embargo, al crear tablas grandes, puede aumentar el número de ellas (opción 'Recuento de tablas').

La peculiaridad de la implementación del algoritmo de búsqueda de tablas arco iris está en el hecho de que el éxito de la recuperación depende de varios parámetros, para los que debe elegir la mejor proporción, dependiendo del tamaño de las tablas, el tiempo que lleva generarlas y el tiempo máximo que lleva encontrar una contraseña en el ataque arcoiris.

La herramienta de generación de tablas admite subprocesos múltiples, por lo que antes de iniciar el preordenamiento, es posible que desee establecer un número adecuado de subprocesos simultáneos que se ejecutarán para crear las tablas.

2.6.6 Generador de Tablas Rainbow Pascape

Las tablas Rainbow de Passcape se utilizan para recuperar contraseñas en ataques de tabla Passcape. Esta herramienta está destinada a crear tales tablas.



Antes de comenzar a generar tablas, debe establecer una lista de palabras que se utilizará para crear una base de datos de impresiones de palabras y especificar los parámetros de la tabla:

- **Longitud de la cadena:** afecta la probabilidad de encontrar contraseñas (por ejemplo, la tasa de éxito), el tiempo de generación de la tabla y el tiempo necesario para buscar una sola contraseña durante el ataque.
- **Recuento de cadenas:** afecta la tasa de éxito, el tiempo de generación de la tabla y su tamaño.

Por el momento, la herramienta de generación de mesas no admite tablas de más de 2 GB de tamaño. Sin embargo, puede crear varias tablas si está trabajando con matrices de datos muy grandes (consulte el parámetro **'Recuento de tablas'**).

El éxito en la recuperación de una contraseña utilizando las tablas depende de varios factores, y es importante que encuentre sus mejores valores dependiendo del tamaño de las tablas con las que trabaja, su tiempo de generación y el tiempo de criptoanálisis, es decir, el tiempo necesario para recuperar una contraseña durante el ataque.

Se utilizan dos opciones adicionales para manipular la eficiencia de la generación de tablas:

- **Maximice la eficiencia de la búsqueda de contraseñas:** le permite generar más huellas de palabras a partir de la lista de palabras de origen agregando números, teclado y combinaciones de uso frecuente. Esta opción funciona bien con listas de palabras pequeñas.
- **Haga una tabla Rainbow perfecta:** como sabrá, las cadenas de contraseñas en las tablas de arco iris pueden fusionarse. Significa que hay un desperdicio de información, tiempo y espacio en disco. Esta opción le permite crear las llamadas 'tablas perfectas' sin cadenas fusionadas. Las tablas perfectas ocupan considerablemente menos espacio en disco y hacen que la recuperación de

contraseñas sea un poco más rápida. Sin embargo, la recompensa de estas ventajas es una menor tasa de éxito en la recuperación de contraseñas. Para compensar esta menor tasa de éxito, debe al menos duplicar el número de cadenas de contraseñas y aumentar el número de tablas generadas.

La herramienta de generación de tablas admite subprocesos múltiples, así que asegúrese de establecer el número necesario de subprocesos simultáneos que ejecutará el programa antes de iniciar el proceso.

2.6.7 Herramienta de lista de palabras

Más bien, un escaso número de herramientas aceptables para trabajar con diccionarios de contraseñas especializados ha inspirado a los desarrolladores de este software a crear su propio kit de herramientas. Con este kit de herramientas, puede crear y editar fácilmente listas de palabras nuevas y existentes, así como usarlas con cualquier aplicación de recuperación de contraseñas.

2.6.7.1 Crear una nueva lista de palabras indexando archivos

Esta herramienta está diseñada para crear una nueva lista de palabras seleccionando (indexando) palabras de archivos locales en su computadora. Por ejemplo, esos podrían ser archivos *.html, *.xml, *.txt, *.doc, así como archivos *.mdb, *.pdf, *.exe, etc.

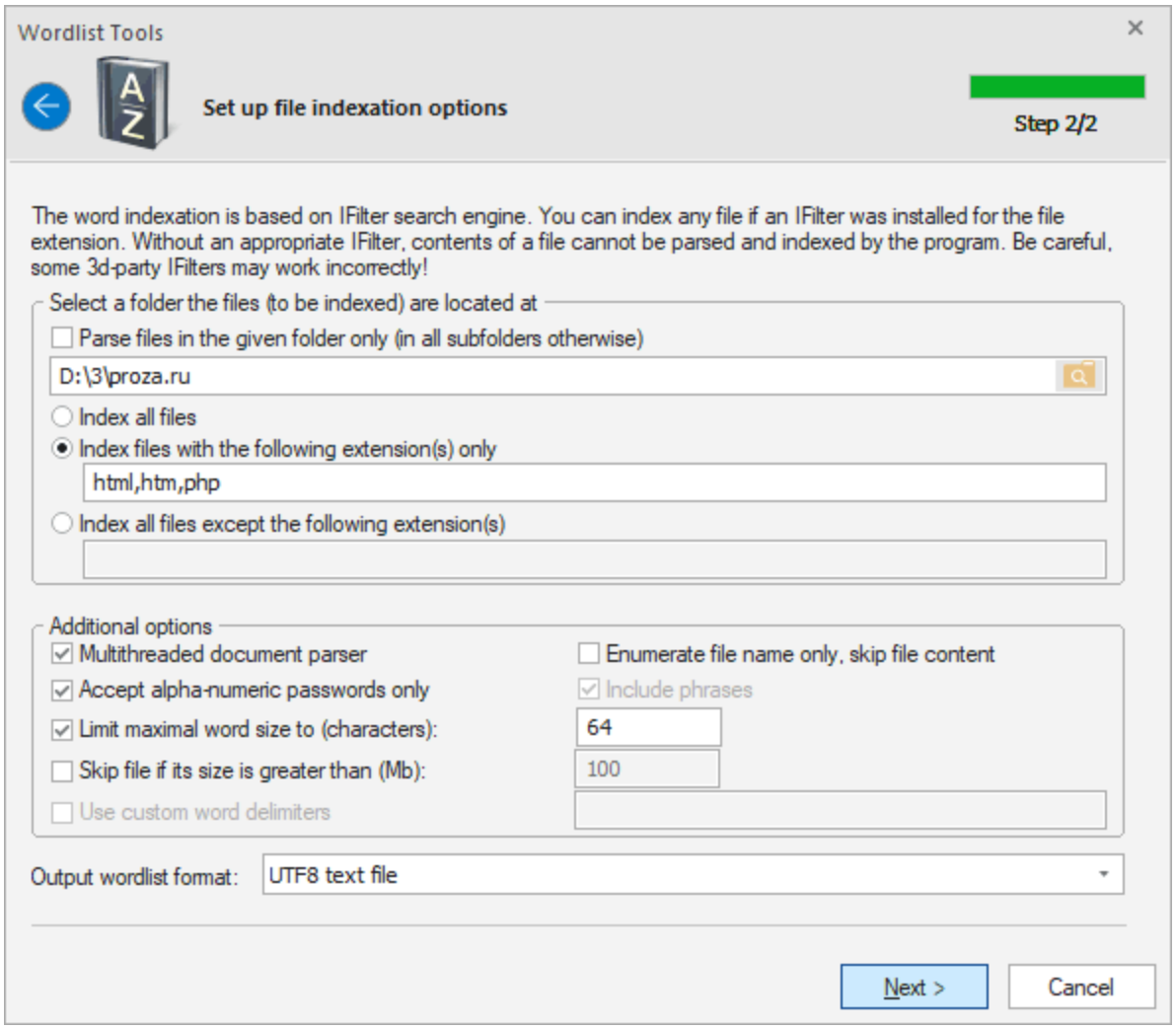
La indexación se basa en la tecnología IFilter, sobre la que puede leer en Wikipedia. La idea de la tecnología, desarrollada por Microsoft, se reduce a la posibilidad de indexar el texto de cualquier archivo, para el que se instala un complemento IFilter apropiado. De esta forma, se podría acceder al texto contenido, por ejemplo, dentro de los archivos *.exe o *.dll, la base de datos del cliente de correo electrónico, etc.

A pesar de que numerosos complementos de IFIlter, tanto comerciales como gratuitos, se pueden encontrar en Internet, Windows Password Recovery tiene soporte interno para los siguientes tipos de archivos:

- Archivos: *.zip, *,cab, *.rar, *.7z
- Programas: *.exe, *.dll, *,cpl, *.ocx, *.sys, *.scr, *.drv
- Texto: *.txt, *.dic, *.udic, *.utf
- Internet: *.html, *.htm

En otras palabras, los archivos con estas extensiones pueden ser analizados por el programa incluso sin un solo IFilter instalado en la computadora.

Windows 7 tiene una herramienta interna de búsqueda en el escritorio de Windows, que tiene una amplia gama de filtros para admitir la mayoría de los documentos populares. En otros sistemas operativos, Windows Desktop Search se puede instalar manualmente; el archivo de instalación se puede descargar desde el sitio web oficial de Microsoft.



Las opciones de configuración de esta herramienta constan de dos grupos. En el primer grupo, debe especificar la ruta a la carpeta inicial, donde necesita indexar los archivos, y seleccionar un método de análisis de archivos, a saber:

- Analice los archivos solo en la carpeta especificada. Si esta opción no está configurada, el programa analiza recursivamente todas las subcarpetas y archivos dentro de ellas.
- Indexar todos los archivos
- Indexar archivos solo con ciertas extensiones
- Indexar todos los archivos excepto ciertas extensiones

Las extensiones de archivo deben escribirse sin el punto y separarse por una coma. Ejemplo: txt,dic,xml,chm,htm

El grupo de opciones adicionales permite personalizar los métodos de análisis de archivos, a saber:

- Analizador de documentos multiproceso. Esta opción, si se configura, acelera drásticamente el proceso de indexación al utilizar tantos núcleos de CPU como tenga su sistema.
- Enumerar sólo el nombre del archivo, omitir el contenido del archivo. Esta opción, si se establece, crea una lista de palabras a partir de los nombres de archivo encontrados. Se ignorará el contenido de los archivos.
- Acepte solo contraseñas alfanuméricas. Si se establece, esta opción omitirá todos los caracteres especiales. Solo se procesarán las contraseñas alfanuméricas.

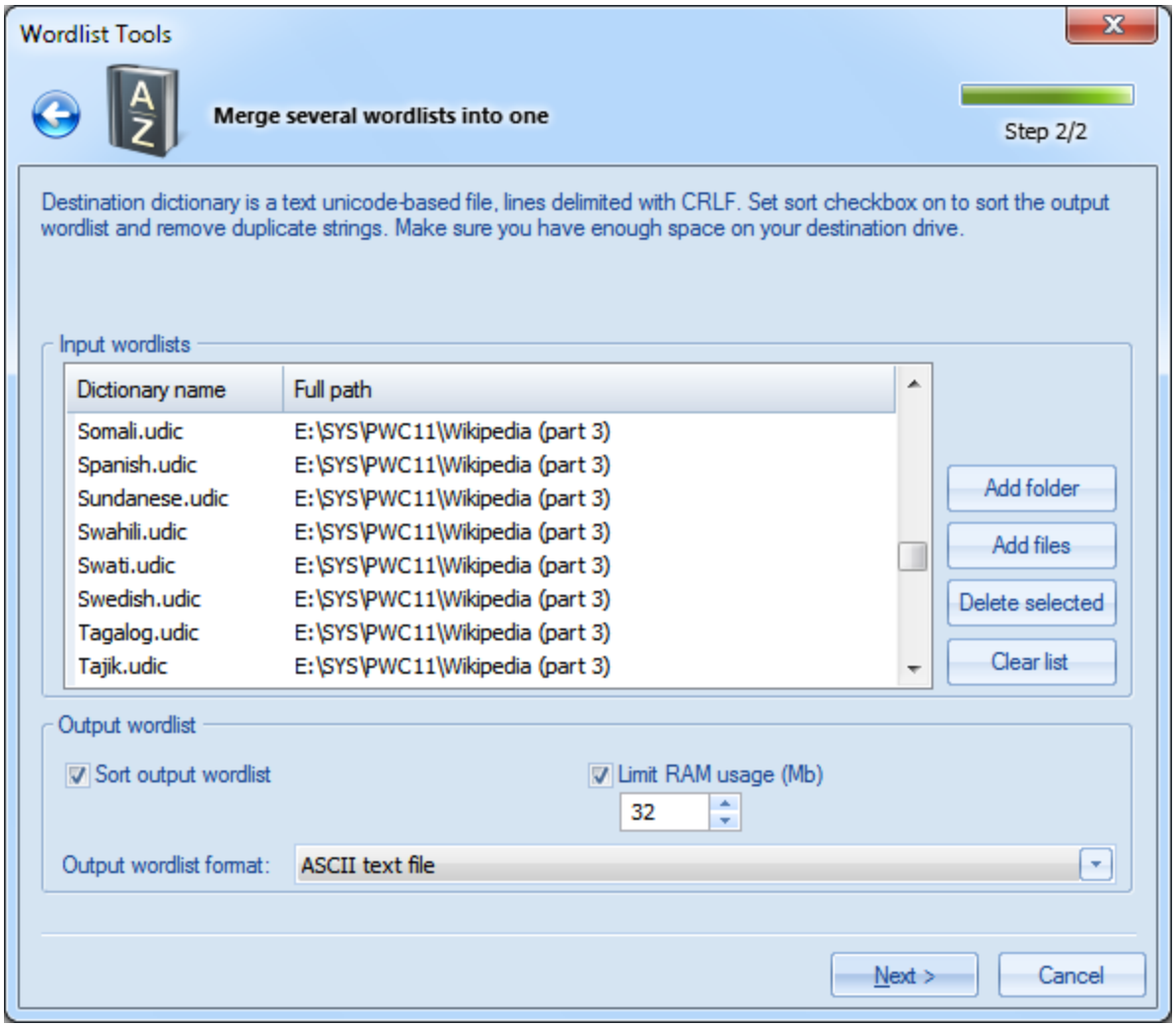
- Incluye frases. Esta opción también permite poner frases en la lista de palabras de destino. Una frase se considera como una cadena de caracteres (de hasta 256 símbolos) con al menos un carácter de espacio en ella.
- Limite el tamaño máximo de las palabras. Se recomienda establecer siempre esta opción. La mejor longitud máxima de palabras en una lista de palabras es de 16-64 caracteres. Cortar la longitud máxima a veces acelera radicalmente el proceso de análisis de archivos. No sería inútil recordar que la longitud máxima de contraseña permitida en Windows es de 128 caracteres.
- Omita archivos con un tamaño superior al especificado. Algunos IFilters tardan mucho en analizar archivos grandes; que puede hacer que el programa se "cuelgue".
- Utilice delimitadores de palabras personalizados. Puede establecer sus propios delimitadores de palabras para analizar archivos. Por ejemplo, podrías usar caracteres como: !" #$%&'()*+,-./:;<=>?@{}[]_ y, por supuesto, espacio.

Al hacer clic en el botón **Siguiente>** se inicia la indexación real, lo que puede llevar un tiempo considerable. En aras de acelerar el proceso, la lista de palabras que se encuentran durante la indexación se crea y se mantiene en la memoria de la computadora; que requiere recursos significativos. Por lo tanto, si obtiene un error de tiempo de ejecución de falta de memoria, intente disminuir la longitud máxima de la palabra o limitar el número de archivos que se analizan y luego intente ejecutarlo nuevamente. Una vez que se completa la operación y las palabras encontradas se guardan en el disco, ordenadas para obtener una lista de palabras verdaderamente valiosa. Se garantiza que las palabras encontradas son únicas, es decir, no contienen duplicados.

Tenga cuidado, algunos filtros de terceros podrían no ejecutarse correctamente y hacer que la aplicación se "bloquee", falle o termine de manera anormal. Por ejemplo, se sabe que algunos filtros para analizar PDF en Windows XP generan errores.

2.6.7.2 Combinar listas de palabras

Una herramienta de combinación de listas de palabras se utiliza cuando necesita combinar dos o más listas de palabras en una.

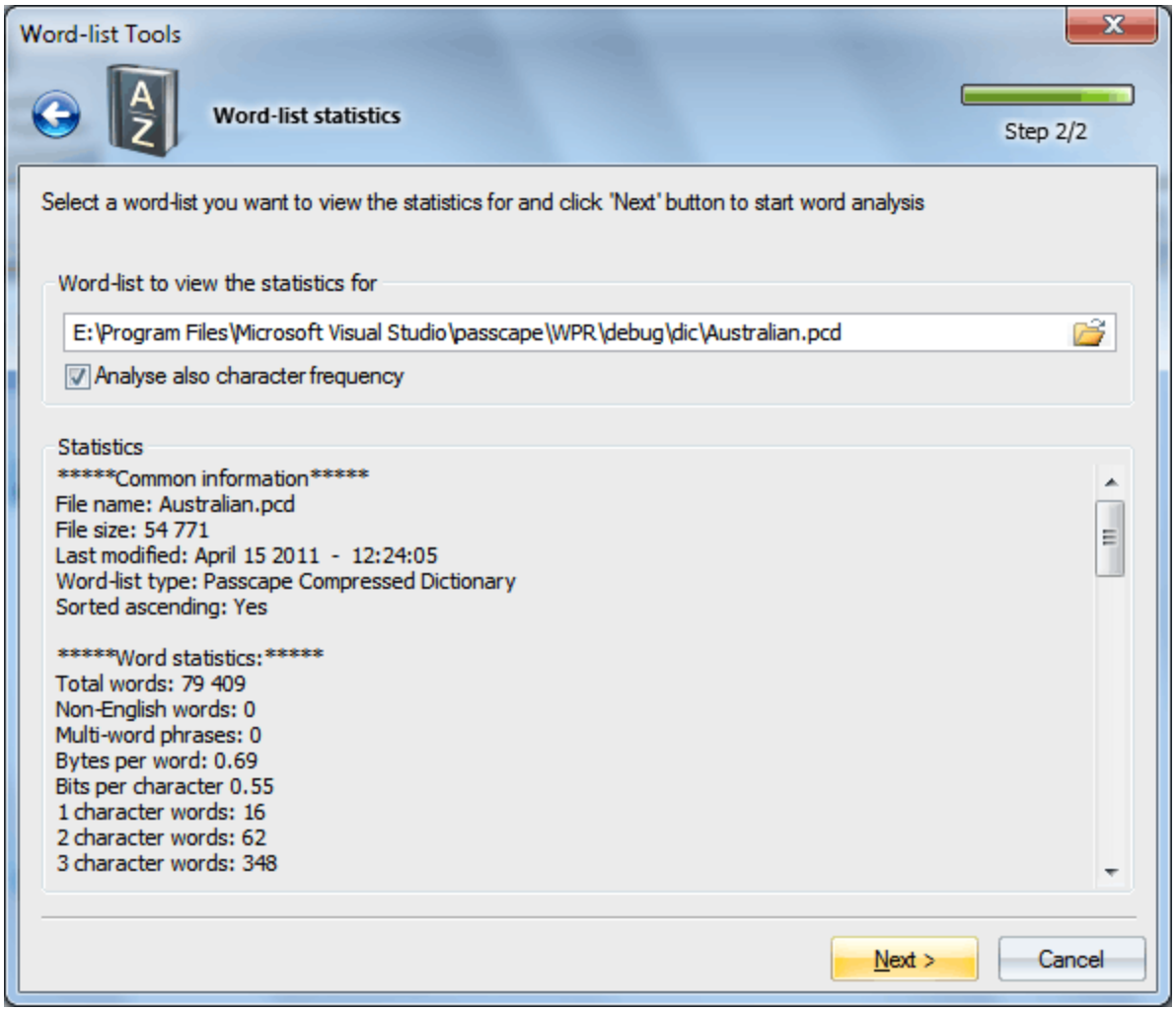


Si la opción **'Ordenar lista de palabras de salida'** no está configurada, la fusión se reduce a simplemente agregar nuevas palabras, sin ordenar o verificar si hay duplicados. En la práctica, sin embargo, más común es la fusión con la clasificación; garantiza que todas las palabras de la lista de palabras de salida estén ordenadas alfabéticamente y sin duplicados.

La clasificación puede requerir una cantidad considerable de memoria; por lo tanto, es apropiado establecer un límite para la cantidad de memoria que puede ser utilizada por el proceso (a expensas de una pequeña disminución de la velocidad de operación).

2.6.7.3 Estadísticas de listas de palabras

El analizador de listas de palabras recopila y muestra las siguientes estadísticas:



Información común
- Nombre del diccionario
- Tamaño en bytes
- Tipo de archivo
- Fecha y hora de la última modificación
- Si está o no ordenado alfabéticamente (la comprobación se realiza solo si el archivo se ordena ascendentemente)

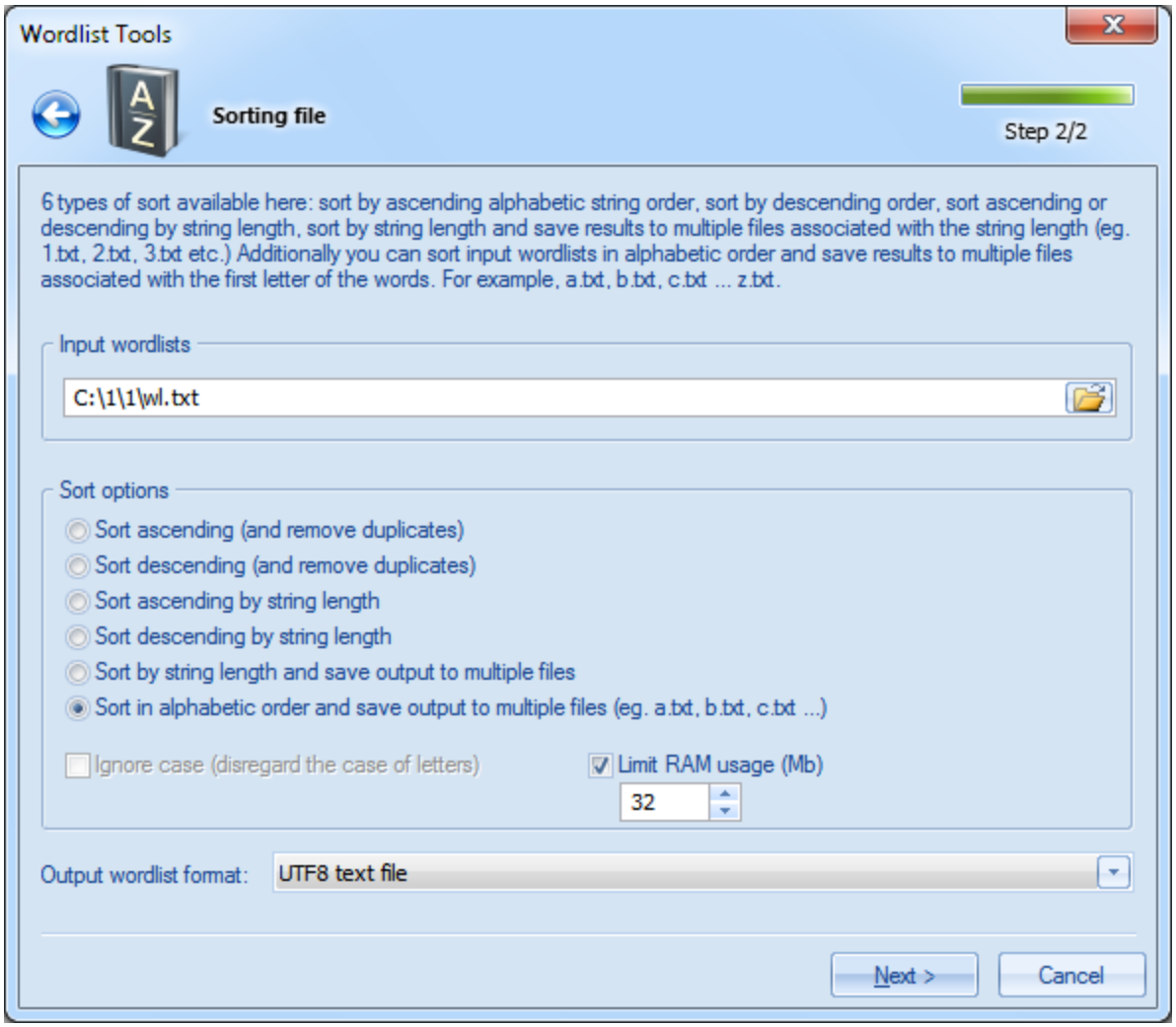
Estadísticas de palabras
- Total de palabras
- Palabras no inglesas
- Frases de varias palabras, es decir, palabras separadas con espacio
- Bytes por palabra, menos delimitador de palabras. Muestra la relación de compresión promedio de la lista de palabras.
- Bits por carácter. Muestra la relación de compresión de la lista de palabras real. Por ejemplo, en UNICODE el valor de bits por carácter tiende a 16 (sin contar el delimitador de palabras), en las listas de palabras ASCII regulares - a 8. En ciertas listas de palabras PCD comprimidas, una letra se puede codificar en menos de 1 bit (ver la captura de pantalla).
- Estadísticas de palabras: cuántas palabras constan de 1, 2, 3, etc. caracteres.

Análisis de frecuencia de caracteres (si se establece la opción respectiva)

- Indica la frecuencia con la que aparece un determinado carácter en una lista de palabras.

2.6.7.4 Ordenar lista de palabras

El kit de herramientas ofrece 6 modos de clasificación de listas de palabras; 4 de ellos son comunes, y 2 se extienden. Los modos de clasificación comunes incluyen ordenar las listas de palabras en orden alfabético (tanto ascendente como descendente) y por longitud de palabra. Al ordenar alfabéticamente o por longitud de palabra, el programa elimina automáticamente los duplicados de palabras.



Además, puede ordenar una lista de palabras por longitud y guardar los resultados en varios archivos, asociados con la longitud de la palabra. Por ejemplo, el archivo 1.txt contendría palabras de 1 carácter, 2.txt - dos caracteres, etc.

El sexto modo de clasificación funciona de manera similar. Al mismo tiempo, el programa ordena la lista de palabras de origen en el orden alfabético y crea varias listas de palabras de destino que se corresponden con la primera letra de la palabra. Por ejemplo, todas las palabras que comienzan con la letra A se escribirían en el archivo A.txt, las palabras que comienzan con B - a B.txt, etc. Debe tener en

cuenta que ciertas palabras pueden comenzar con caracteres que no se pueden usar en un nombre de archivo. En este caso, el programa sugiere automáticamente un reemplazo emitiendo una advertencia apropiada en la ventana de mensajes.

Si se establece la opción 'Ignorar mayúsculas', la clasificación se lleva a cabo independientemente del caso de la letra; es decir, las palabras *malo*, *Malo* o *MALO* se consideran idénticas, con todas las consecuencias resultantes.

El nombre de la lista de palabras de destino puede ser el mismo que el de origen; sin embargo, eso no se recomienda.

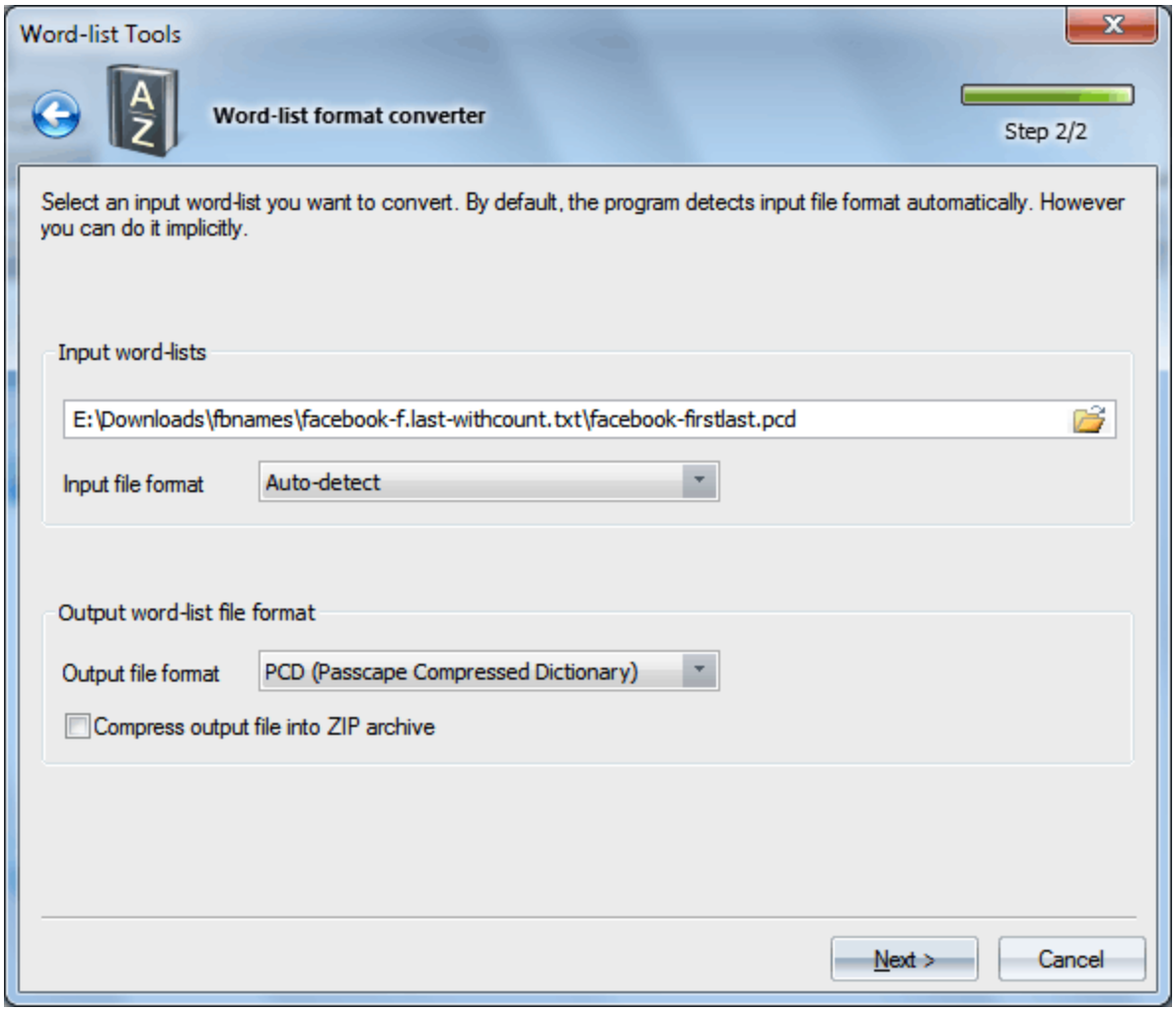
La clasificación de archivos grandes (admite archivos de más de 4 GB) implica un uso intensivo de la RAM; la cantidad de la misma puede estar limitada por la opción respectiva. Para archivos grandes, no se recomienda establecer el límite de memoria inferior a 16 MB, ya que eso puede afectar la velocidad de clasificación.

Durante la clasificación, el programa puede crear archivos auxiliares en la carpeta temporal de la aplicación. Asegúrese de que el disco con la carpeta temporal tenga suficiente espacio para los archivos de intercambio.

2.6.7.5 Convertir/comprimir lista de palabras

Numerosas listas de palabras que se pueden encontrar en Internet suelen estar representadas por tres formatos principales: **ASCII**, **UTF16** (Unicode) y **UTF8**. Con esta herramienta, puede convertir una lista de palabras de un formato a otro y, opcionalmente, comprimir listas de palabras en archivos ZIP. Además de los tres formatos mencionados anteriormente, el programa soporta su propio formato **PCD** (Passcape Compressed Dictionary), que, en la mayoría de los casos, da una mayor ganancia de tamaño incluso en comparación con un archivo ZIP comprimido.

¡Crear archivos PCD grandes puede llevar un tiempo considerable!



La interfaz de usuario de esta herramienta es bastante fácil. En el grupo superior, seleccione la lista de palabras de origen y su formato. De forma predeterminada, el programa detecta el formato del archivo automáticamente, pero también puede especificarlo a mano.

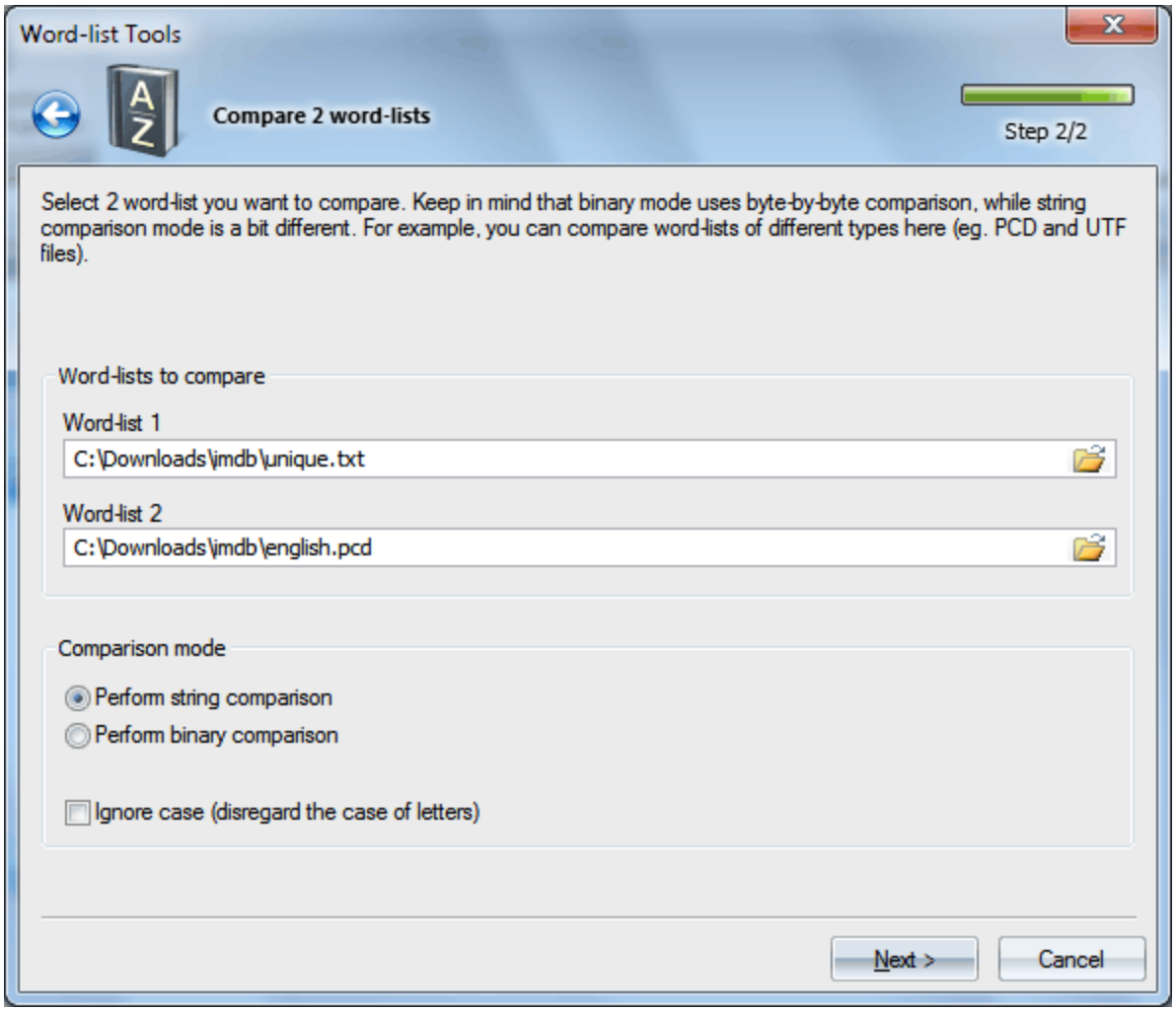
Si bien el formato de un PCD se puede reconocer claramente, con los archivos de texto no es tan fácil. Como regla general, los archivos de texto/listas de palabras en UTF16 o UTF8 comienzan con un marcador de dos o tres bytes que describe el tipo de archivo. Sin embargo, hay listas de palabras Unicode que no tienen ningún marcador de identificación. Para tales casos "difíciles", debe establecer el tipo de archivo de origen manualmente. De lo contrario, el programa, al no poder ver un identificador apropiado, reconoce incorrectamente el archivo como ASCII.

La lista de palabras de destino, de manera similar, se define por uno de los cuatro formatos mencionados anteriormente. Con la opción de compresión establecida, el programa también comprime el archivo en un archivo ZIP.

El nombre de la lista de palabras de destino puede ser el mismo que el de origen; sin embargo, eso no se recomienda.

2.6.7.6 Comparar listas de palabras

A veces, es necesario determinar si dos listas de palabras son idénticas. Para eso está la herramienta de comparación de listas de palabras.



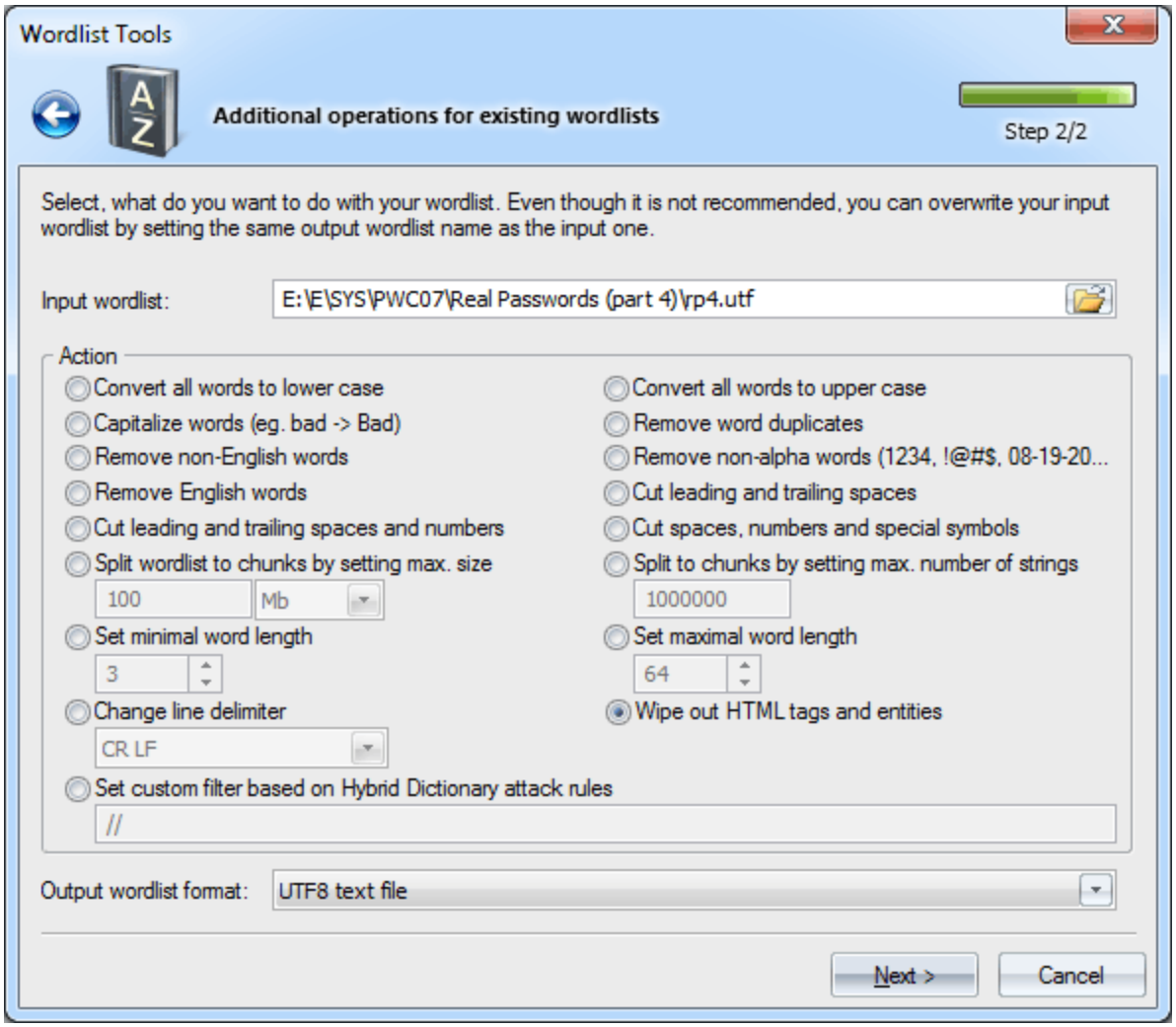
Esta herramienta ofrece dos modos de funcionamiento:

1. Comparación binaria, para comparar archivos por byte
2. Comparación de cadenas, que compara palabras en lugar de bytes. Este modo es notable por su capacidad para comparar listas de palabras de diferentes formatos. Por ejemplo, PCD y UNICODE, o UNICODE y ASCII.

Si se establece la opción Ignorar mayúsculas y minúsculas (solo modo de comparación de cadenas), las palabras *malo* y *Malo* se considerarán idénticas.

2.6.7.7 Operaciones adicionales

Las herramientas adicionales están diseñadas principalmente para editar y ajustar las listas de palabras existentes.



Las herramientas incluyen las siguientes operaciones:

- Convierta todas las palabras de la lista de palabras a minúsculas. Por ejemplo, BAD -> malo.
- Convierte todas las palabras en mayúsculas. Por ejemplo, Bad -> BAD.
- Palabras en mayúsculas: primera letra mayúscula, minúscula todas las demás. Por ejemplo, malo -> malo.
- Elimine los duplicados de palabras.
- Elimine las palabras que no están en inglés.
- Elimine las palabras que consisten completamente en números y / o caracteres especiales. Por ejemplo, 12345, !@#$%, 19-08-10, etc.
- Eliminar palabras en inglés.
- Cortar/quitar espacios de inicio y finales.
- Cortar/eliminar espacios y números de inicio y finales.
- Cortar/eliminar espacios y números y caracteres especiales inicio y finales.
- Divida la lista de palabras en trozos por tamaño máximo.
- Divida la lista de palabras en fragmentos por el recuento máximo de palabras.
- Elimine las palabras de longitud inferior a la especificada.
- Elimine las palabras de longitud superior a la especificada.
- Cambiar delimitador de línea.

- Borra las etiquetas HTML y la papelera. Este menú también convierte entidades HTML en formas legibles por humanos. Por ejemplo, **&** -> **&**, **@** -> @
- Configura tu propio filtro basado en Reglas del diccionario híbrido

Para la lista de palabras de origen, el programa toma archivos ASCII, UTF16, UTF8 y PCD. La lista de palabras de destino puede ser un texto de ASCII, UTF16 o UTF8.

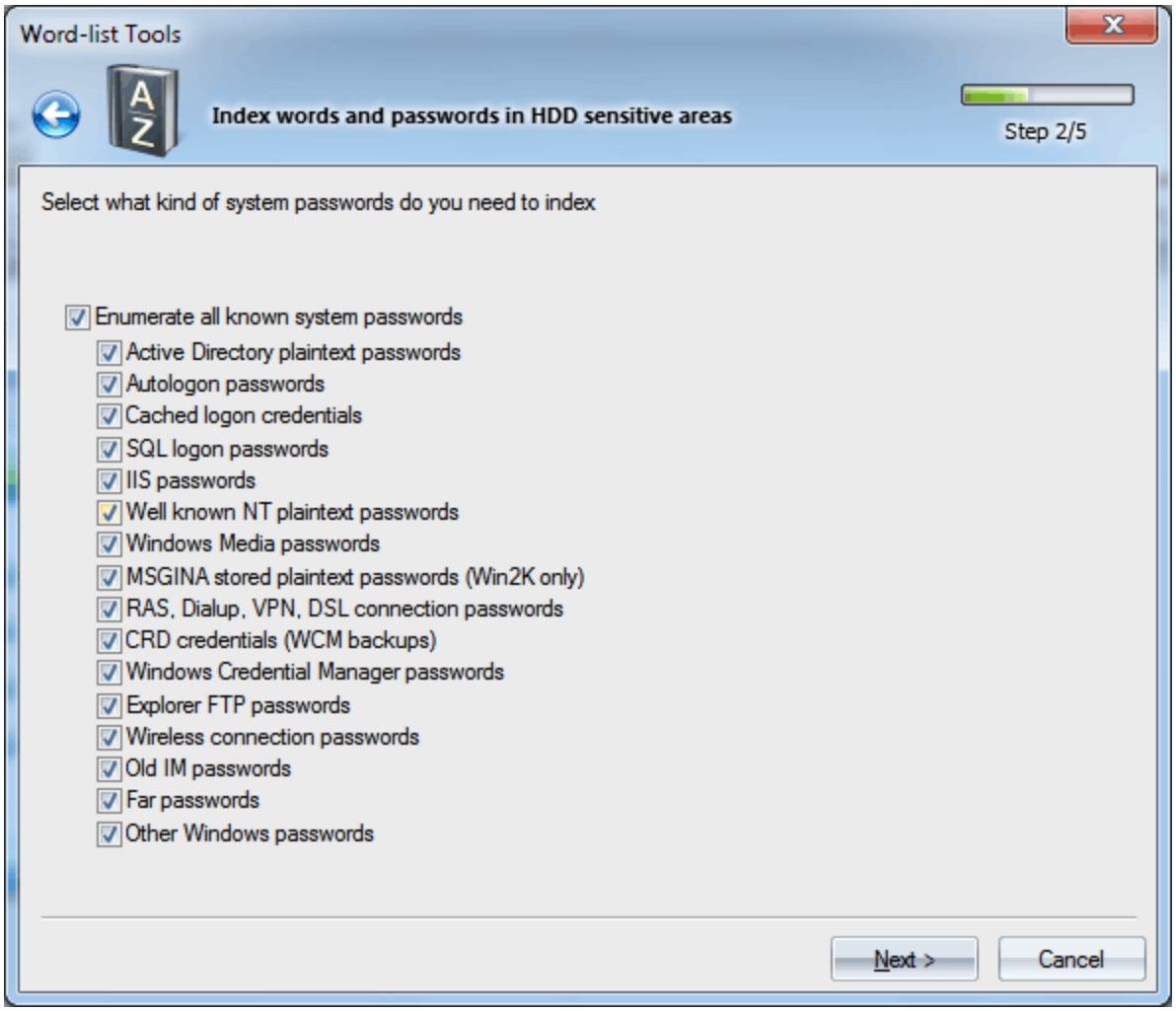
El nombre de la lista de palabras de origen y destino puede ser idéntico (no se recomienda). En este caso, se sobrescribirá la lista de palabras de origen.

2.6.7.8 Indexar áreas sensibles del Disco Duro

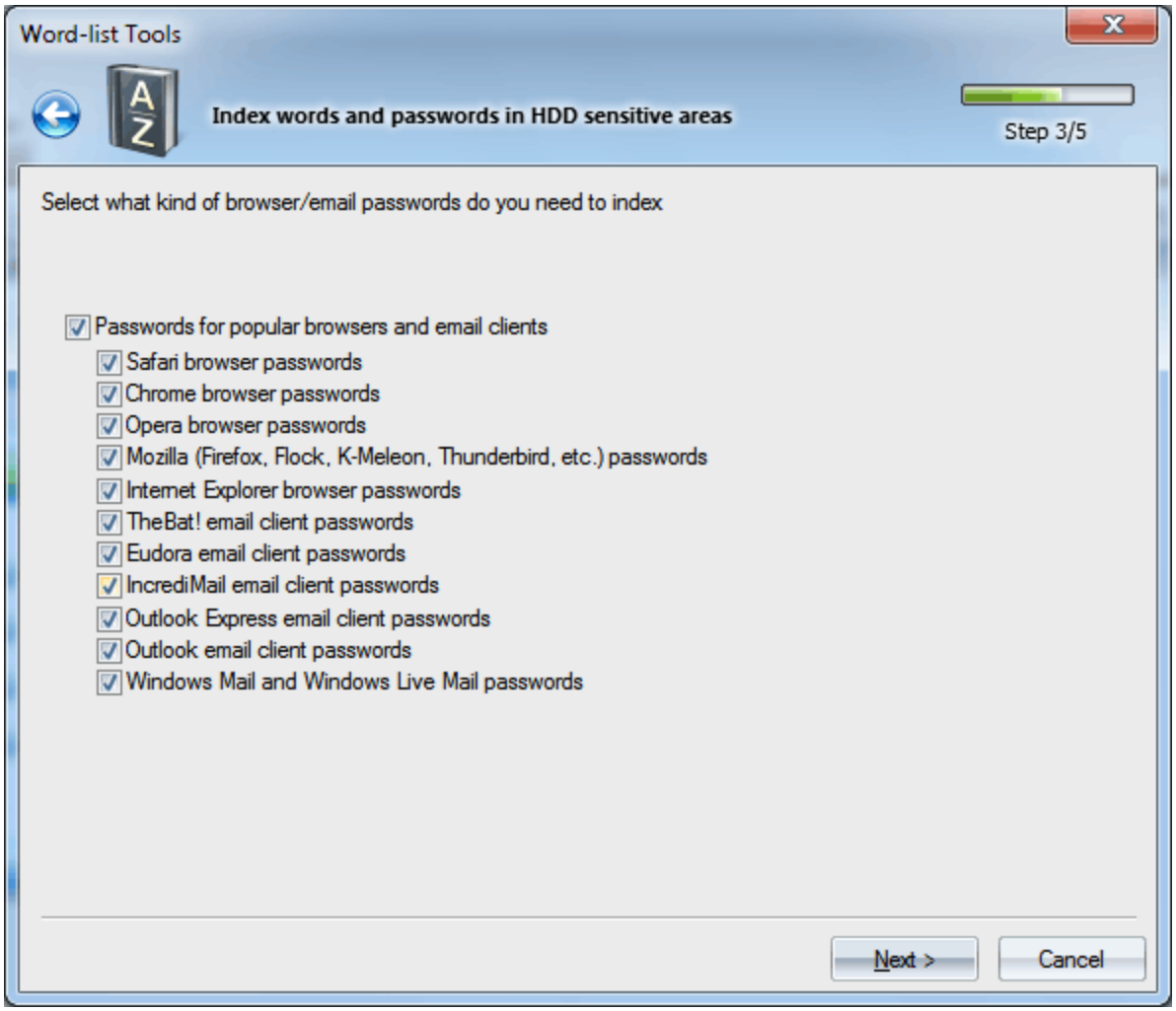
Crear una lista de palabras indexando el disco duro (seguido de un ataque usando esta lista de palabras) es una herramienta bastante útil y sofisticada para descifrar contraseñas a cuentas locales de Windows.

A menudo, los usuarios, instintivamente, establecen las mismas contraseñas para sus cuentas de Windows, Web, ICQ, etc. La idea de esta herramienta es crear una lista de palabras de todas las contraseñas utilizadas anteriormente, mensajes de usuario, palabras de archivos abiertos recientemente, etc. y luego usar la lista de palabras acumulada para buscar contraseñas en las cuentas locales. Esta técnica se dedica al ataque de Inteligencia Artificial.

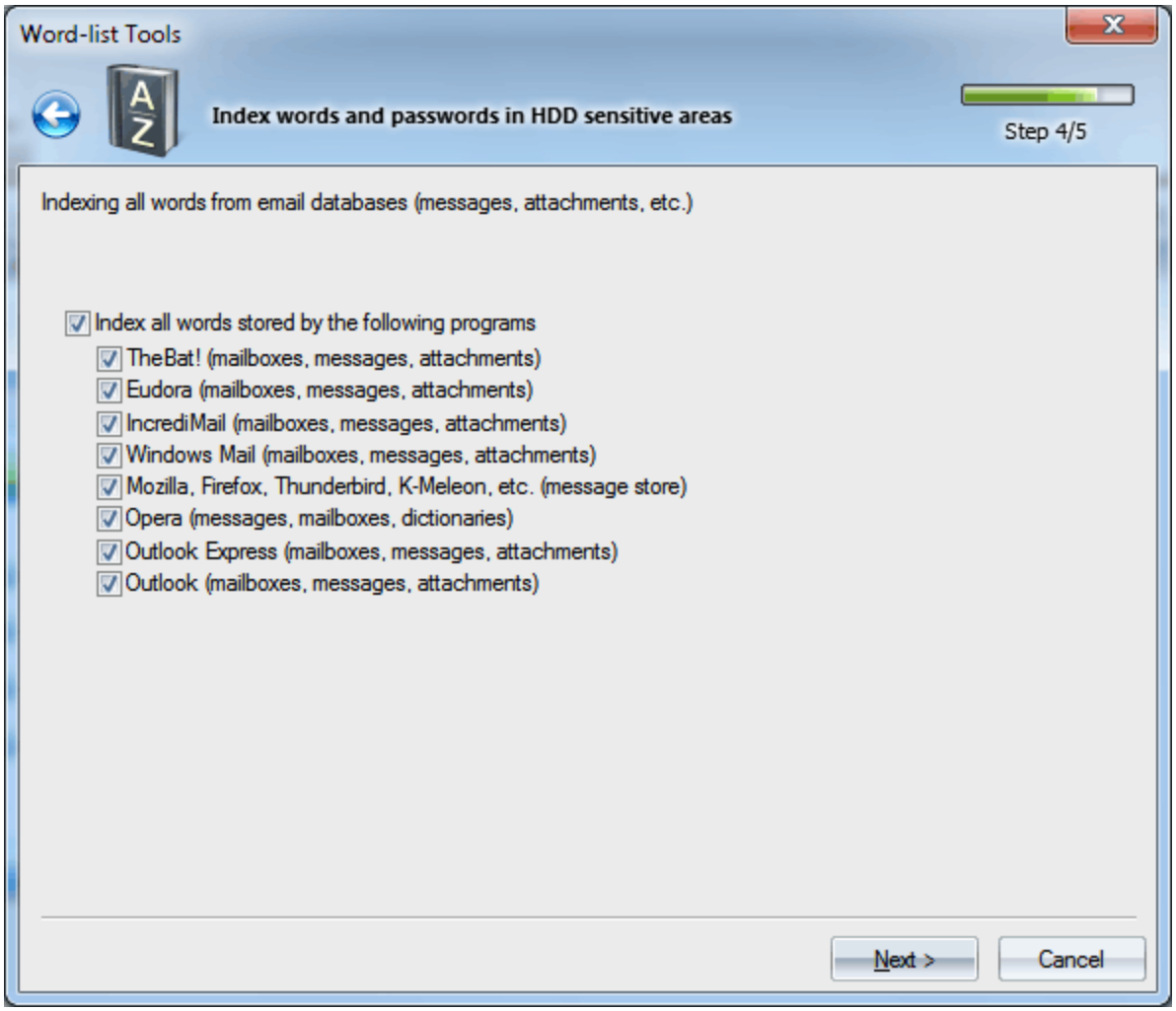
La configuración de la herramienta convencionalmente consta de cuatro partes:



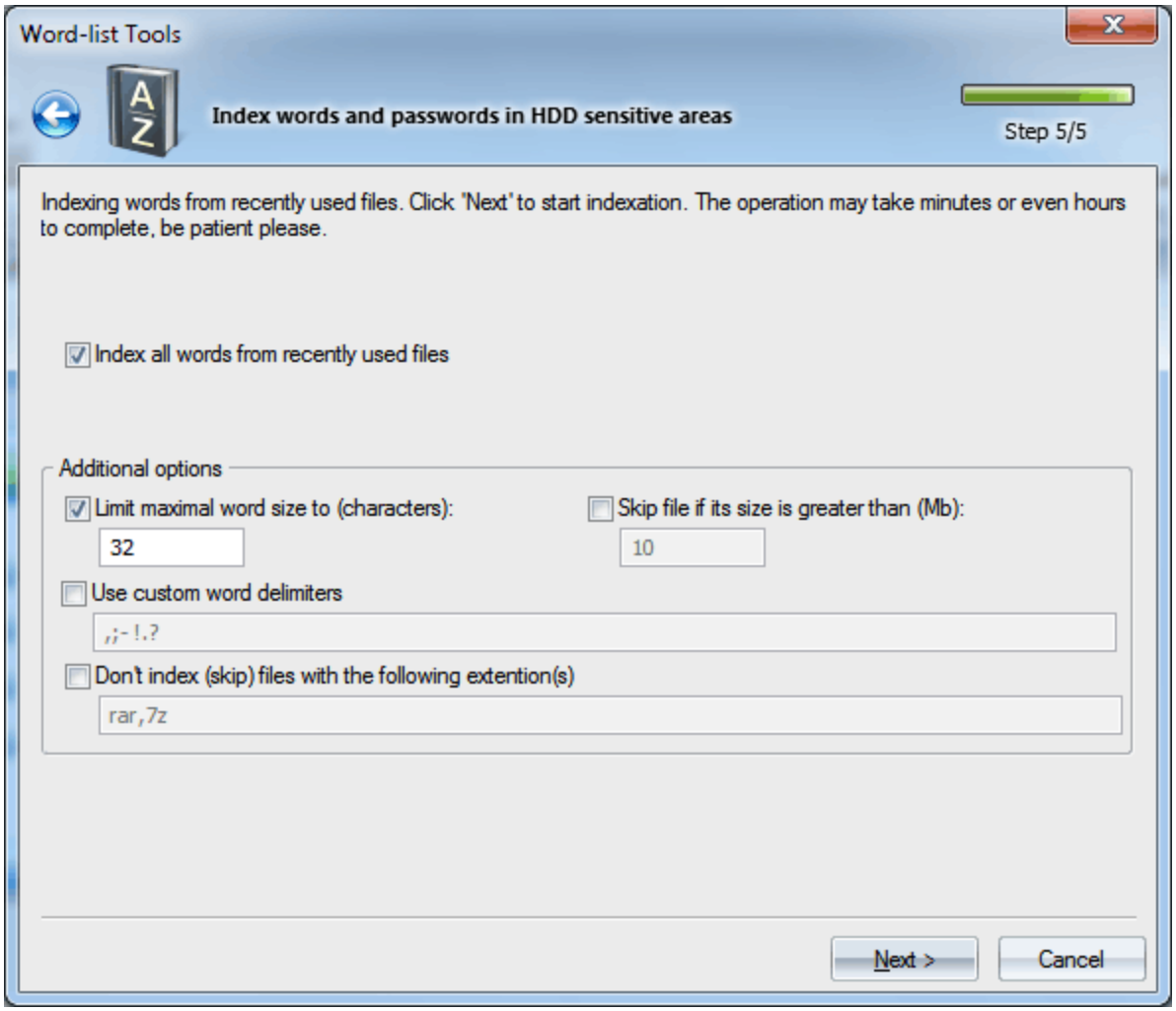
Primero, seleccione los módulos del sistema que se utilizarán al generar la lista de palabras. Estos módulos encuentran e indexan los siguientes tipos de contraseñas en el disco duro de su computadora: contraseñas de texto plano de Active Directory, contraseñas de inicio y contraseñas de inicio almacenadas en caché, SQL, IIS, Windows Media, contraseñas de texto Win2K, RAS, Acceso telefónico, VPN, DSL, WEP, WPA, contraseñas de conexión FTP, contraseñas del Administrador de credenciales de Windows, mensajeros instantáneos, etc. contraseñas.



En la segunda parte de la configuración, seleccione los navegadores y clientes de correo electrónico, contraseñas desde los cuales también se encontrarán y se agregarán a la lista de palabras que se está creando. El programa es compatible con los siguientes navegadores web principales: Safari, Chrome, Opera, navegadores basados en Mozilla (Firefox, K-Meleon, Flock, etc.), Internet Explorer. Los clientes de correo electrónico están representados por: TheBat!, Eudora, IncrediMail, Outlook Express, Outlook, Windows Mail y Windows Live Mail.



Además de simplemente recopilar contraseñas, el programa puede indexar la comunicación por correo electrónico del usuario, escaneando todos los buzones, mensajes, archivos adjuntos, etc. encontrados. La búsqueda en el disco duro se realiza para todas las cuentas de un sistema, por lo que el proceso puede llevar un tiempo considerable, especialmente cuando el sistema aloja a muchos usuarios o cuando las bases de datos de los clientes de correo electrónico son grandes. De una forma u otra, puede habilitar / deshabilitar cada módulo individualmente.



Finalmente, en el último cuadro de diálogo, puede establecer las opciones para indexar palabras de todos los archivos, abiertos recientemente por el usuario actual. Las opciones disponibles incluyen:

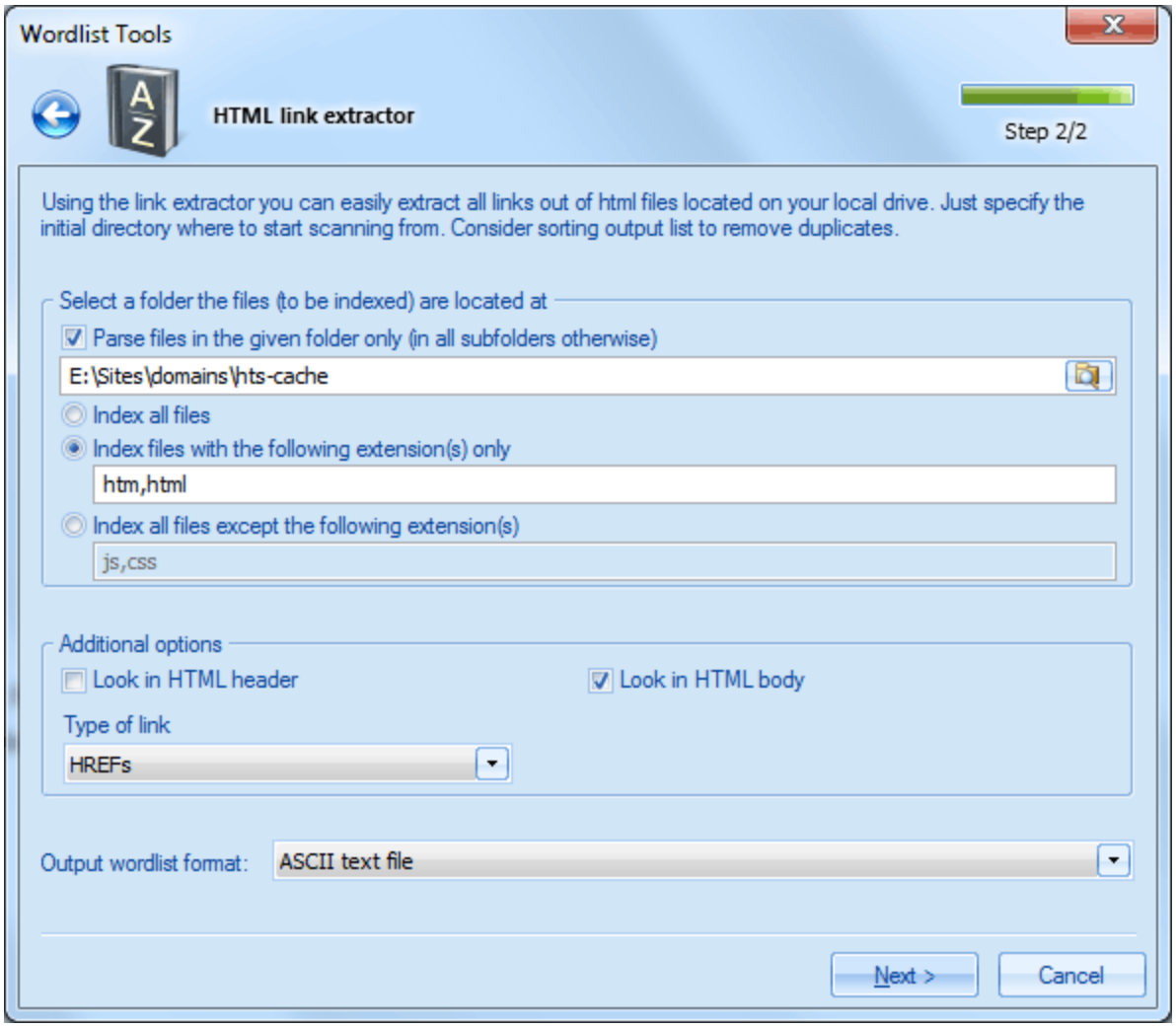
- Establezca la longitud máxima de las palabras que se pueden agregar a la lista de palabras. Se omitirán todas las palabras con una longitud superior al límite especificado.
- Omita archivos con un tamaño superior al especificado. El tamaño se especifica en MB.
- Utilice delimitadores de palabras personalizados. De forma predeterminada, los delimitadores de palabras son todos caracteres no alfabéticos.
- No indexe archivos con extensiones especificadas. Utilice esta opción para omitir archivos que considere innecesarios.

Al hacer clic en el botón **Siguiente>** se inicia el proceso de indexación.

¡Tenga en cuenta que puede llevar un tiempo considerable!

2.6.7.9 Extraer enlaces HTML

Esta herramienta está diseñada para extraer hipervínculos HTML de archivos HTML.



Las opciones de configuración de esta herramienta constan de dos grupos. En el primer grupo, debe establecer una ruta a la carpeta inicial, donde se encuentran los archivos HTML, y seleccionar un método de análisis de archivos, a saber:

- Analice los archivos solo en la carpeta especificada. Si esta opción no está configurada, el programa analiza recursivamente todas las subcarpetas y archivos dentro de ellas.
- Indexar todos los archivos
- Indexar archivos solo con ciertas extensiones
- Indexar todos los archivos excepto ciertas extensiones

De forma predeterminada, la herramienta comprueba solo los archivos *.htm y *.html.

El grupo de opciones adicionales permite establecer el tipo de enlaces, así como dónde buscarlos:

- Buscar en el encabezado HTML
- Buscar en el cuerpo HTML
- Busque enlaces en la etiqueta HREF, la etiqueta SRC o en ambas etiquetas.

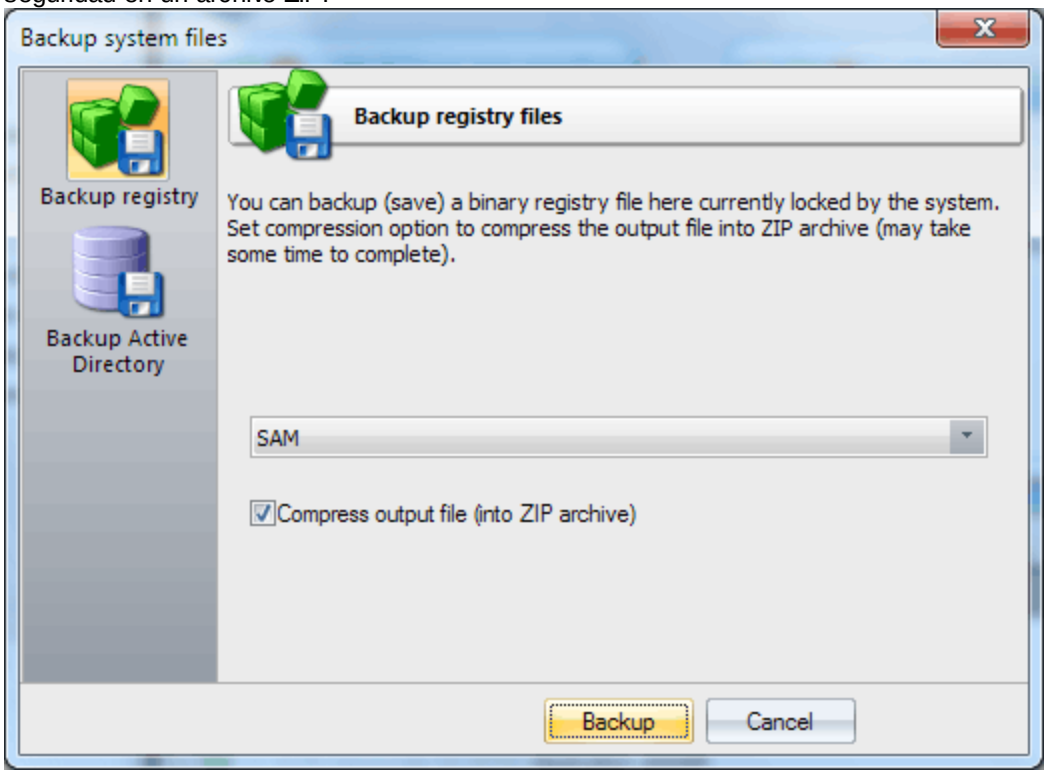
Al hacer clic en el botón **Siguiente>** se inicia la búsqueda, lo que puede llevar un tiempo considerable. Una vez que se complete la operación y los enlaces encontrados se guarden en el disco, considere ordenarlos para obtener un viaje de duplicados.

2.7 Menú Utilidades

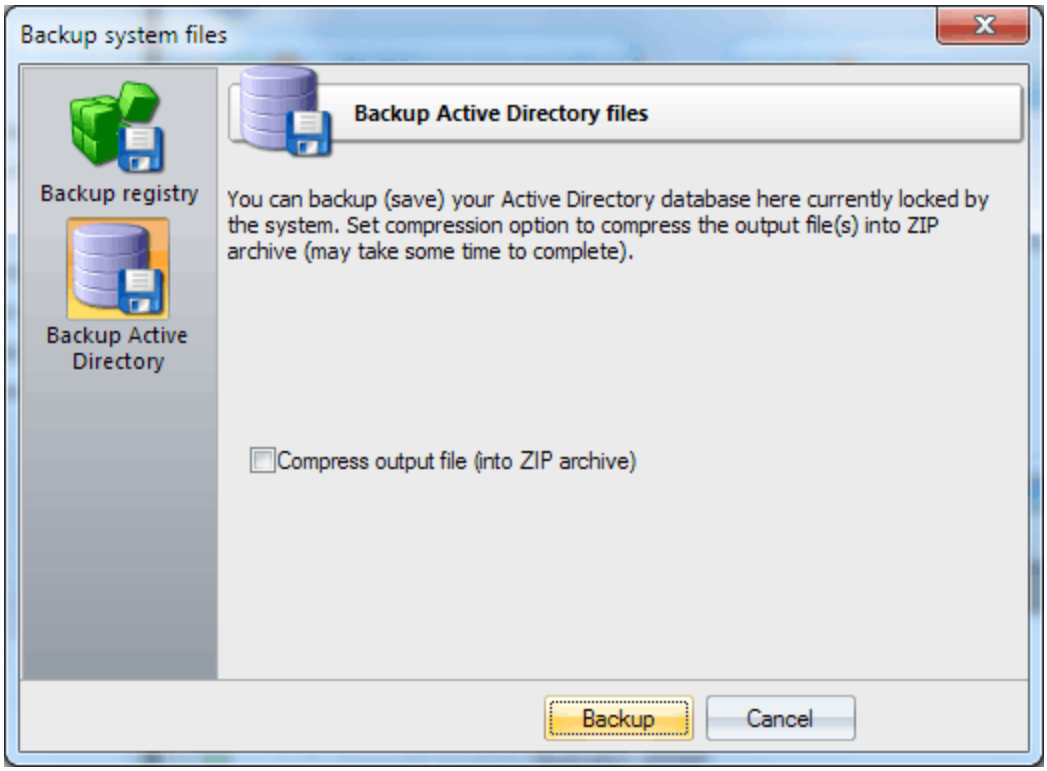
El menú de utilidades consta de complementos adicionales dirigidos principalmente a usuarios avanzados.

2.7.1 Copia de seguridad de archivos del sistema

La herramienta de copia de seguridad del registro permite crear fácilmente una copia de seguridad de su registro de Windows. Incluso si el archivo de registro está bloqueado por el sistema operativo. Puede configurar una opción adicional para ahorrar espacio adicional y comprimir los archivos de copia de seguridad en un archivo ZIP.

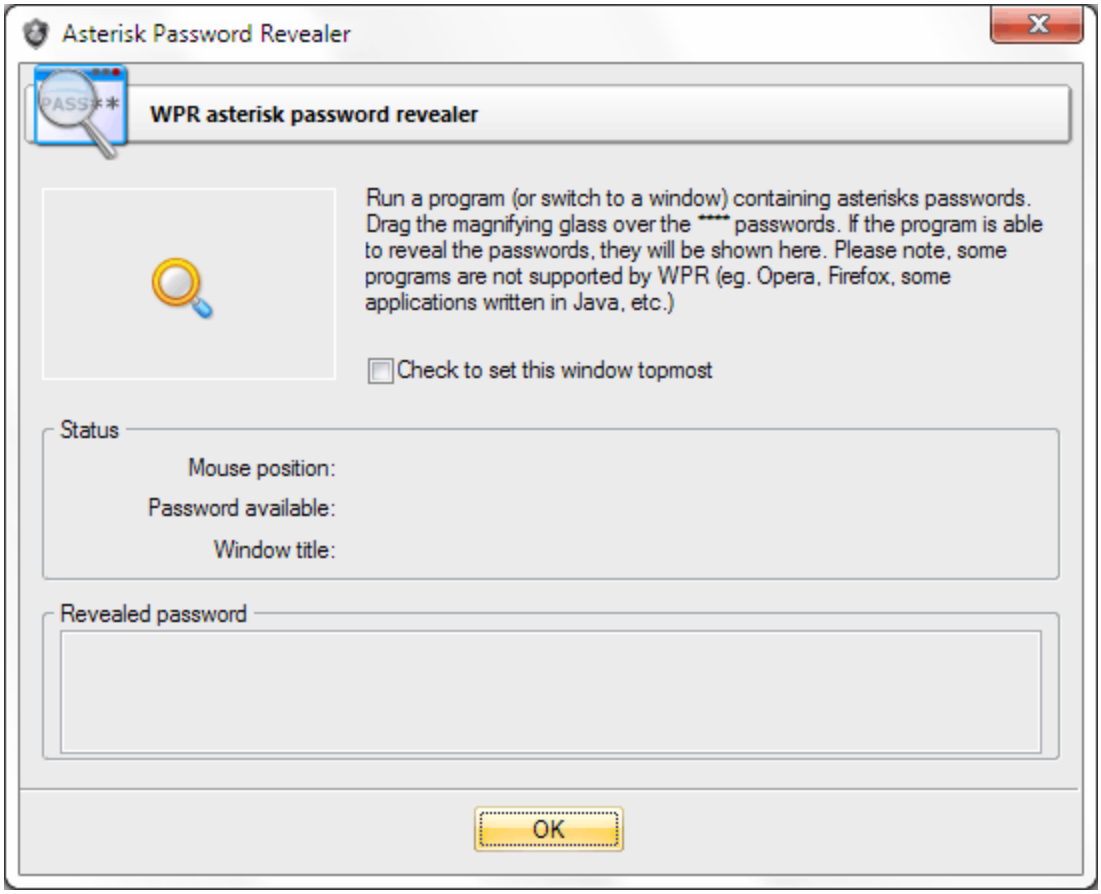


La copia de seguridad de la base de datos de Active Directory es muy similar a la copia de seguridad del Registro, excepto que la ruta de acceso a Active Directory que el programa determina automáticamente.



Se requieren privilegios de administrador u operador de copia de seguridad para ejecutar este complemento.
Crear y guardar la base de datos de Active Directory puede llevar bastante tiempo: minutos o incluso horas para bases de datos enormes.

2.7.2 Revelador de contraseñas en asterisco



Esta herramienta permite recuperar contraseñas ocultas detrás de asteriscos. A menudo es útil cuando necesita recuperar rápidamente una contraseña **** y no tiene las herramientas de recuperación necesarias a mano. Para que la contraseña **** sea visible, debe arrastrar la lupa mágica desde la ventana WPR hasta el campo con asteriscos.

Este método funciona tanto para controles de Windows como para ventanas de Internet Explorer. Sin embargo, tiene una serie de restricciones:

- Algunas aplicaciones tienen su propia GUI y, por lo tanto, es posible que Asterisks Revealer no pueda interactuar con dichas aplicaciones. Estos incluyen Opera, Mozilla, Firefox, etc.
- Algunos sitios web tienen una protección incorporada, que oculta la basura o los asteriscos reales detrás de los caracteres del asterisco * (¡asteriscos ocultos detrás de los asteriscos!).
- En algunos diálogos del sistema Windows, los asteriscos también ocultan el carácter * y no la contraseña real.

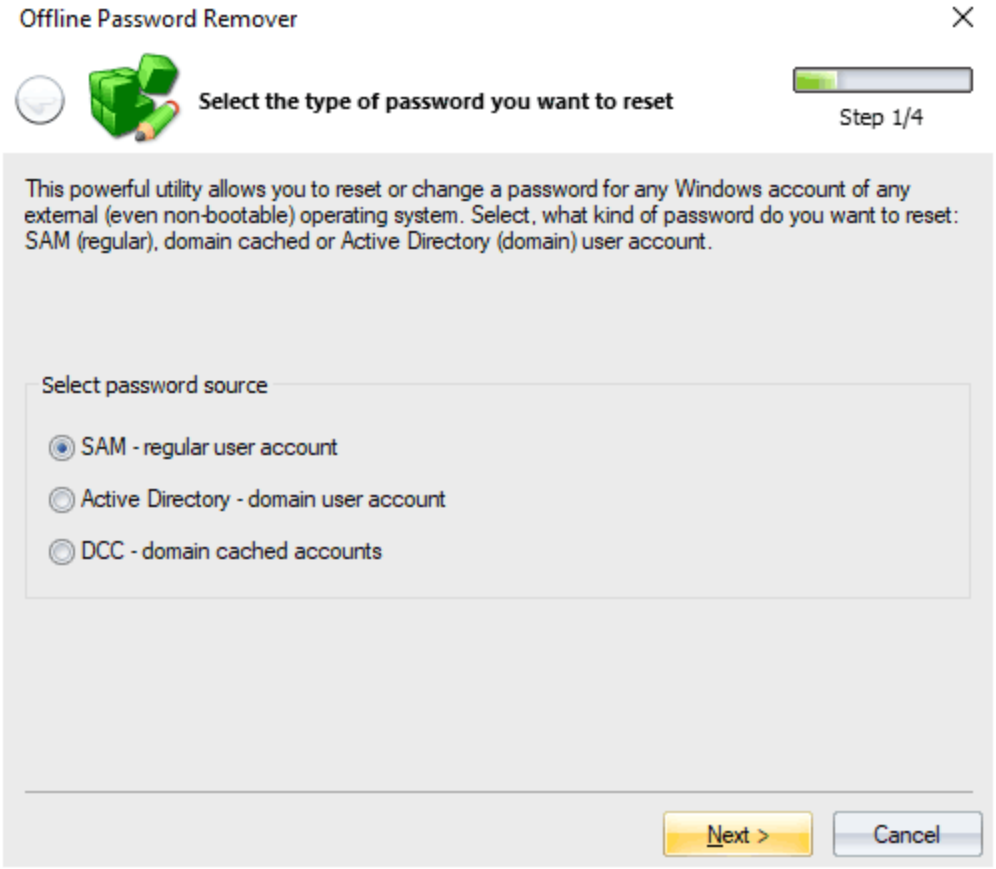
Para garantizar el correcto funcionamiento de esta herramienta, debe tener los privilegios de administrador.

2.7.3 Eliminador de contraseñas sin conexión

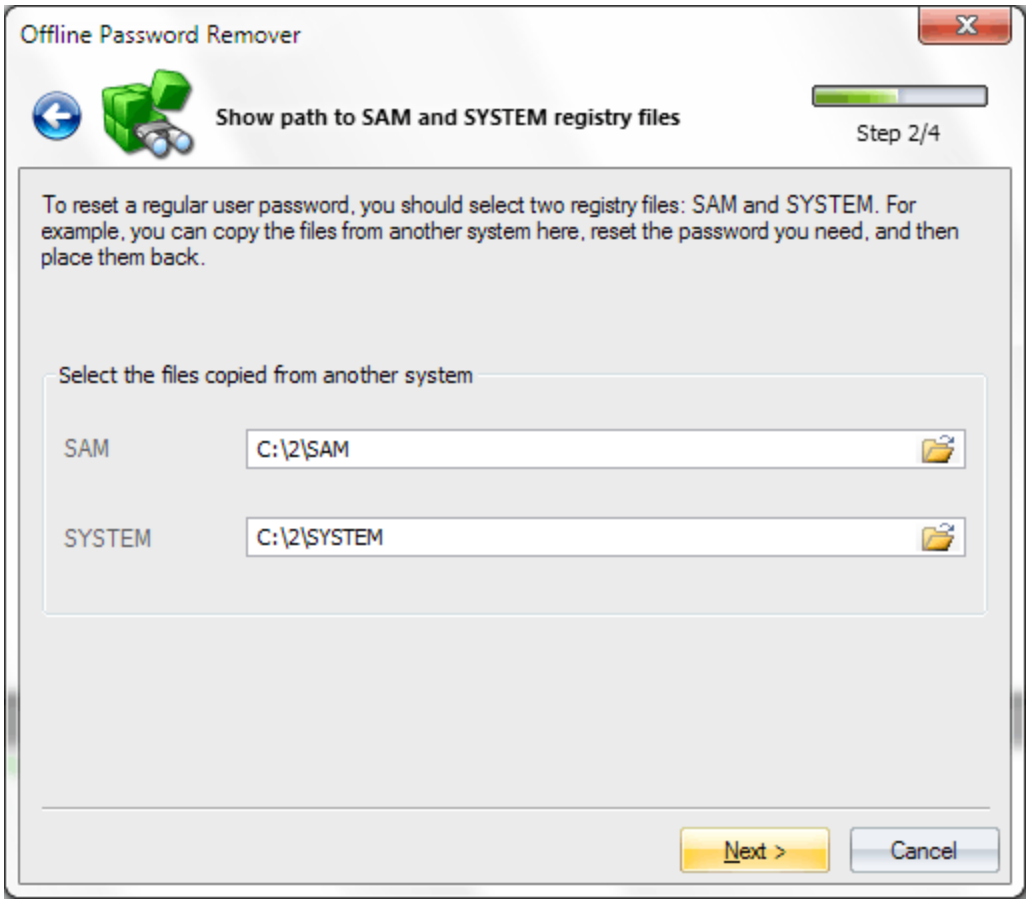
Un complemento útil para eliminar y modificar contraseñas directamente en el archivo de registro SAM/SECURITY o en NTDS. DIT. Por ejemplo, para recuperar el acceso a un sistema bloqueado, no

necesariamente tiene que recuperar la contraseña de inicio de sesión de Windows. En su lugar, puede copiar los archivos de registro SAM y SYSTEM del sistema que no se puede arrancar, usar este complemento para eliminar la contraseña de la cuenta (o borrar la marca de bloqueo) y copiar los archivos de nuevo. El complemento de eliminación de contraseñas se realiza como un asistente y consta de 4 pasos:

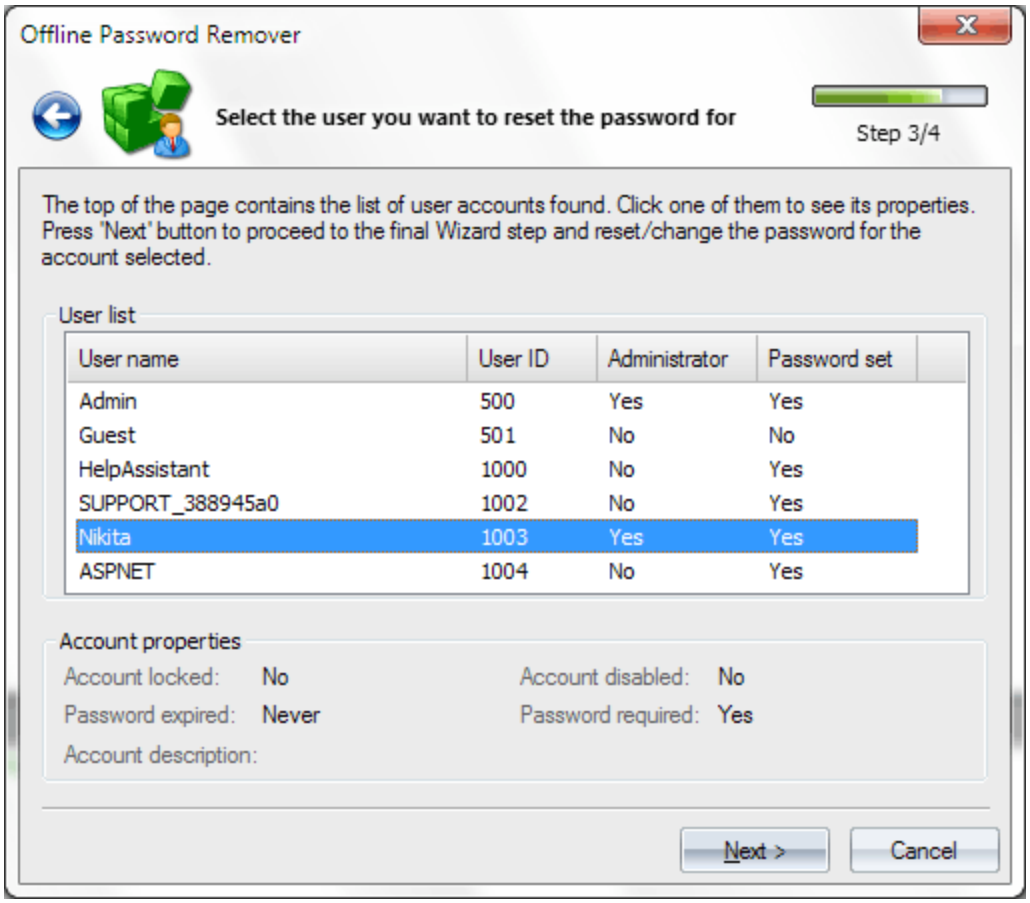
1. En el primer paso, seleccione la fuente de contraseña. Eso podría ser un archivo SAM, para las cuentas normales, DCC, para credenciales en caché de dominio o NTDS. DIT - para eliminar contraseñas en un dominio.



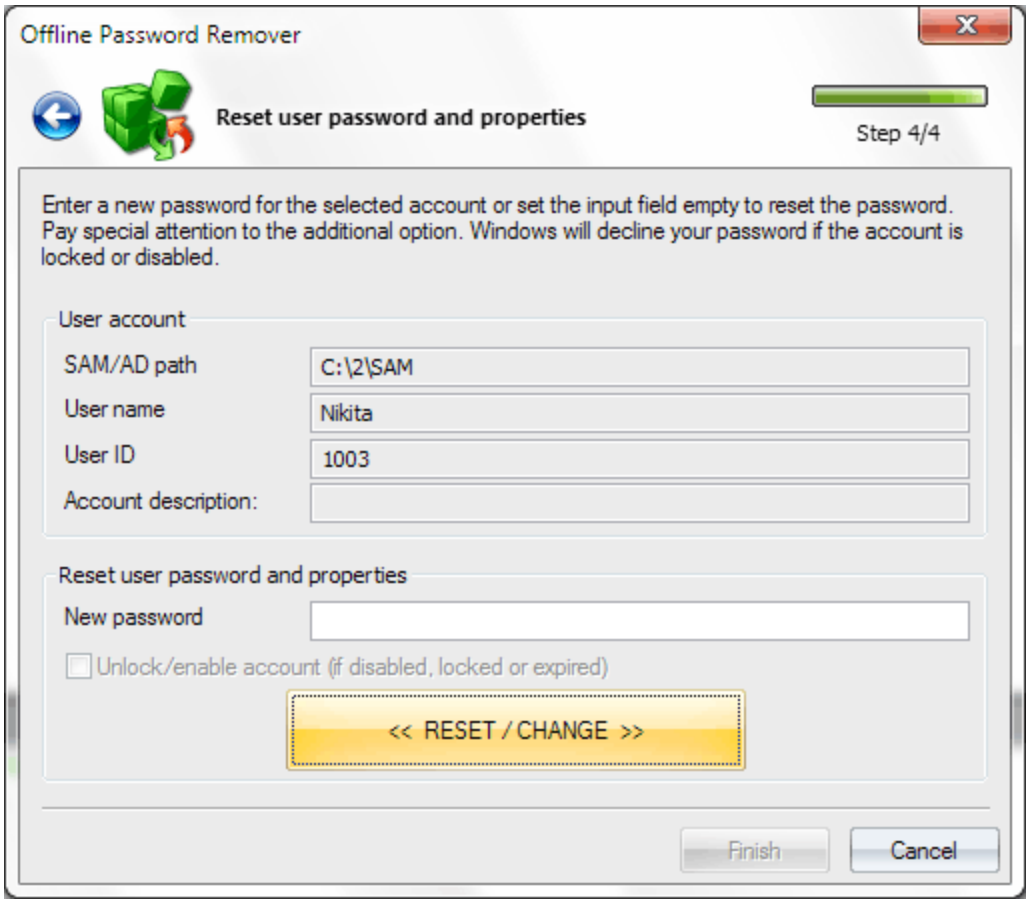
2. En el segundo paso del asistente, especifique la ruta de acceso a SAM, SECURITY o NTDS. DIT junto con el registro SYSTEM. De forma predeterminada, NTDS. DIT se encuentra en c:\windows\ntds. Los archivos del Registro residen en c:\windows\system32\config.



3. En este paso, debemos seleccionar la cuenta para la que necesitamos modificar la contraseña. Seleccione el nombre de usuario y continúe con el paso final.



4. El campo 'Nueva contraseña' está hecho para la nueva contraseña (déjela en blanco para restablecer la contraseña). Si este campo está deshabilitado, significa que la contraseña de esa cuenta ya está vacía. Lo mismo se aplica a la opción avanzada para desbloquear cuentas de usuario bloqueadas o deshabilitadas.



No olvide guardar sus archivos SAM, SECURITY o NTDS. DIT antes de hacer los cambios finales en ellos!

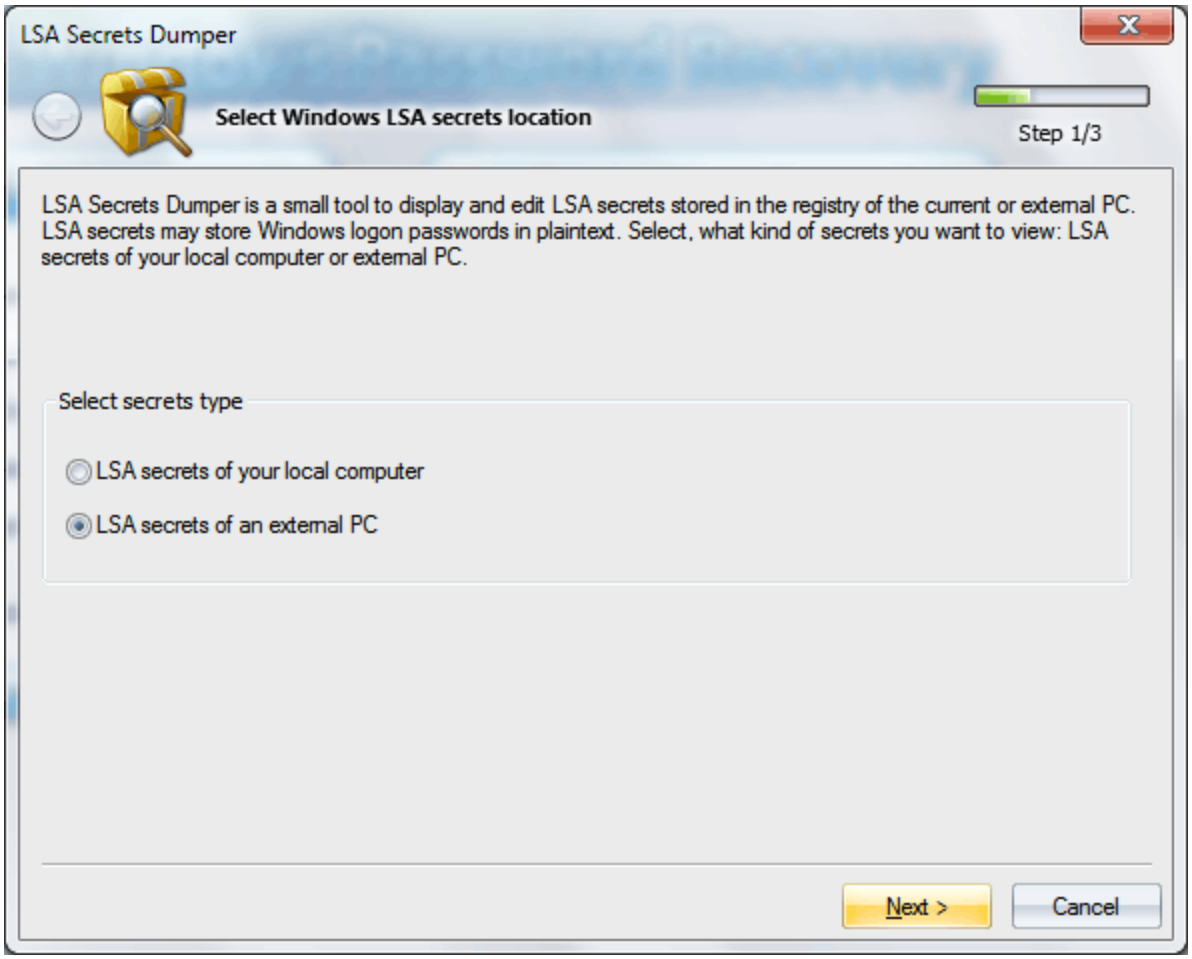
2.7.4 Herramientas forenses

2.7.4.1 Volcador de Secretos LSA

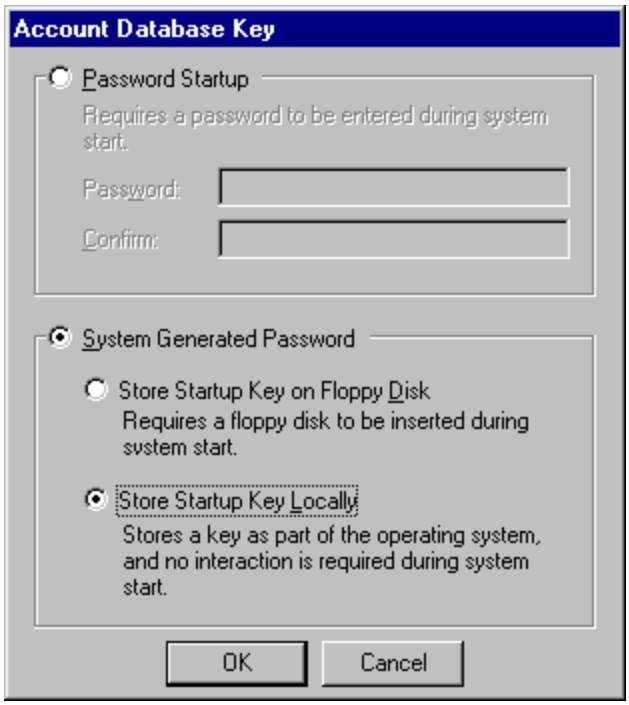
Los secretos LSA son un almacenamiento especialmente protegido para datos importantes utilizados por la Autoridad de Seguridad Local (LSA) en Windows. LSA está diseñado para administrar la política de seguridad local de un sistema, auditar, autenticar, registrar usuarios en el sistema, almacenar datos privados. Los datos confidenciales de los usuarios y del sistema se almacenan en secretos. El acceso a todos los datos secretos está disponible solo para el sistema. Sin embargo, como se muestra a continuación, algunos programas, en particular Windows Password Recovery, permiten anular esta restricción.

El complemento de Windows Password Recovery para manejar secretos LSA es una pequeña herramienta para ver, analizar y editar secretos LSA. La interfaz de usuario impulsada por asistente del complemento es bastante simple y contiene solo tres pasos:

1. Primero, selecciona el tipo de secretos con los que vas a lidiar. Estos pueden ser secretos del sistema local, donde se ejecuta la aplicación, o secretos de una PC externa.

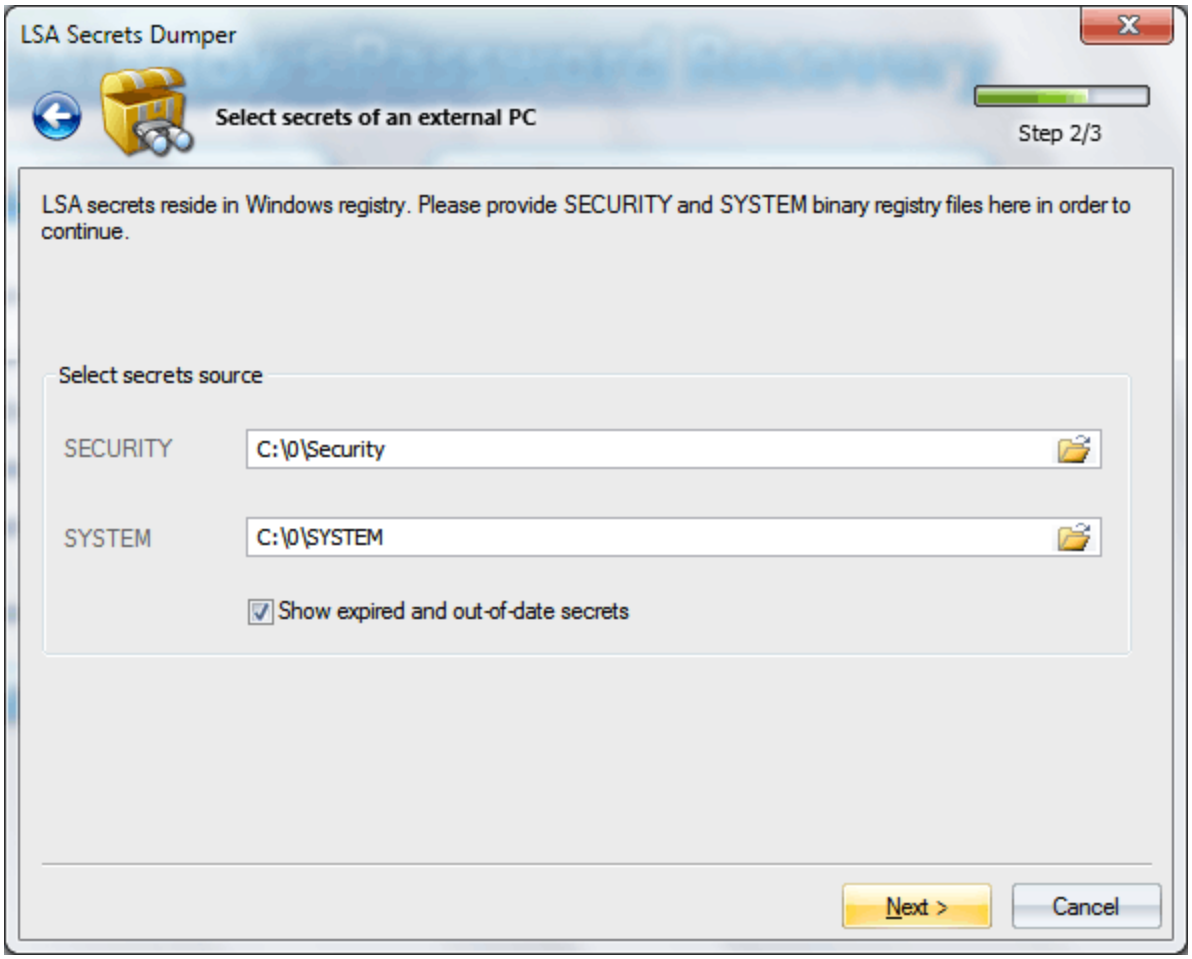


2. Al seleccionar secretos de una PC externa, debe especificar la ruta a dos archivos de registro: SYSTEM y SECURITY. El archivo SECURITY contiene secretos cifrados, y SYSTEM es necesario para descifrarlos. Puede obtener más información sobre el cifrado de secretos en nuestro artículo. Tenga en cuenta que el cifrado de secretos implica SYSKEY. De forma predeterminada, SYSKEY está configurado de la manera en que se puede extraer del registro (para eso está SYSTEM).

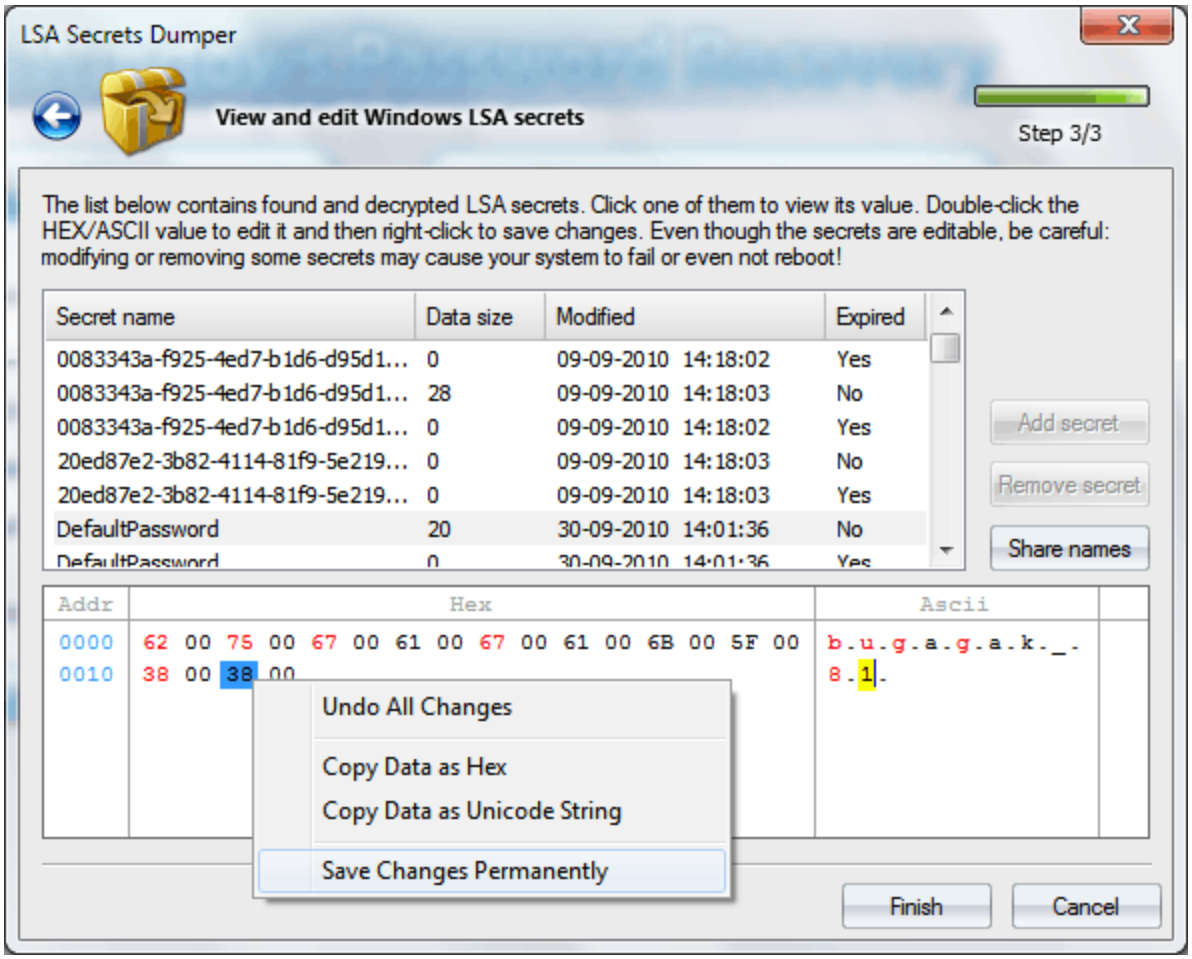


En algunos casos, se puede configurar de otra manera: para que se almacene en un disco de arranque o se derive de la contraseña del usuario cuando se inicie el sistema operativo. De una forma u otra, el plugin admite todos los tipos de cifrado SYSKEY.

Los datos almacenados en secretos son cruciales para el funcionamiento de todo el sistema. Por lo tanto, los secretos de LSA se almacenan en dos copias: actual (activa) y anterior (anterior). La modificación de un secreto coloca su copia actual en la anterior y la reemplaza con el nuevo secreto modificado. El plugin tiene una opción para mostrar secretos activos y anteriores.



3. El último paso del Asistente descifra los secretos y los muestra como una lista. Para mostrar el valor de un secreto, simplemente haga clic en su nombre. Ingrese al modo de edición haciendo doble clic en uno de los caracteres en el campo Hexadeci o Ascii (esto lo marca en amarillo) e ingrese el nuevo valor. En el modo de edición, utilice las teclas del cursor para pasar al siguiente carácter. Los valores modificados se marcan en rojo. Para guardar los cambios, haga clic con el botón derecho en el campo Hex/Ascii y luego seleccione el elemento guardar en el menú que aparece.



Tenga en cuenta que ciertos secretos contienen datos críticos, y modificarlos puede causar inestabilidad del sistema o incluso la imposibilidad de arrancar.

El plugin también permite añadir y eliminar secretos (secretos del sistema operativo actual solamente). Al eliminar un secreto, ya sea antiguo o nuevo, se eliminan automáticamente sus dos copias.

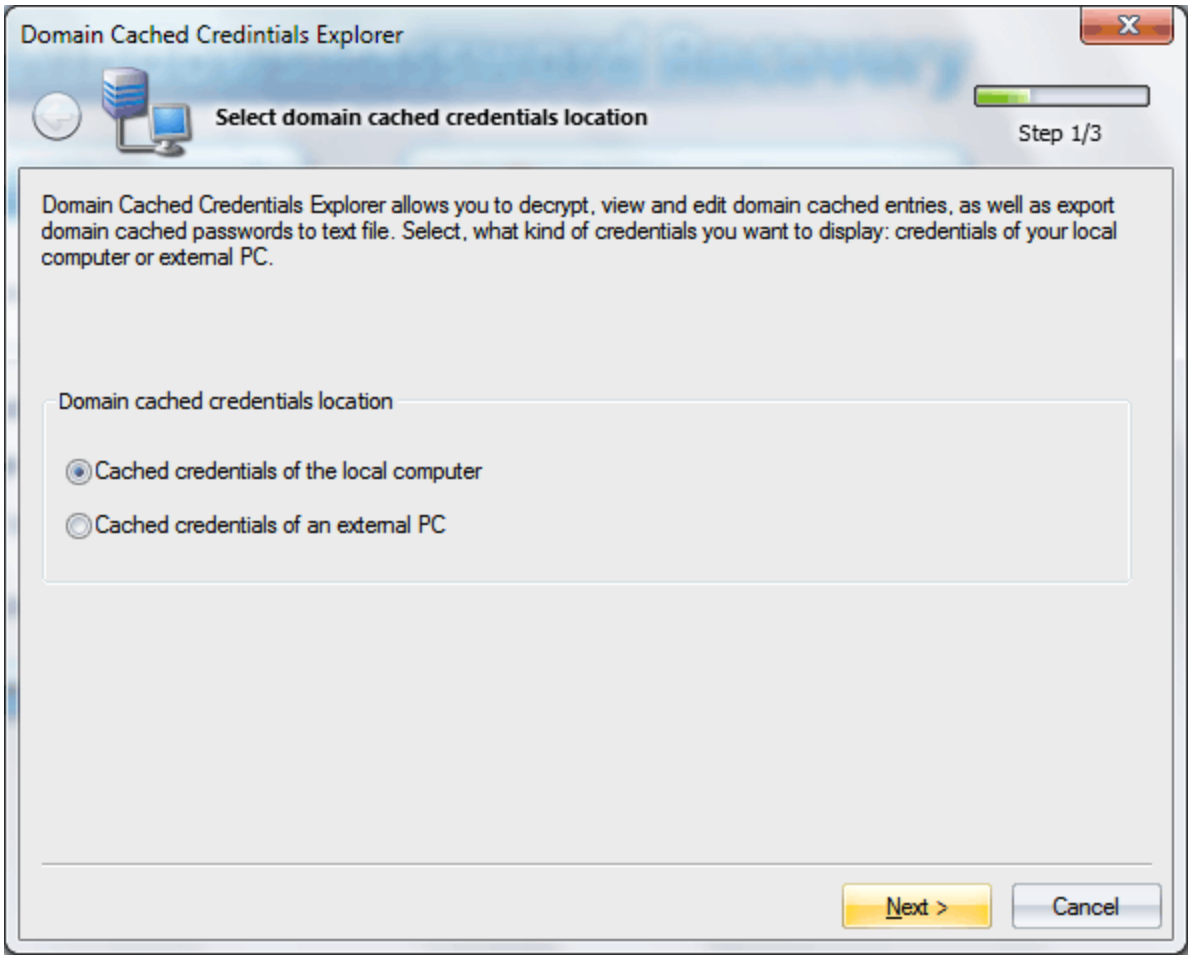
Puede compartir sus secretos con los desarrolladores (botón Compartir nombres). Esto envía por correo electrónico solo los nombres secretos, sin los datos reales. Analizar los nombres secretos nos ayudará a hacer el programa más eficiente.

2.7.4.2 Explorador de credenciales almacenadas en caché de dominio

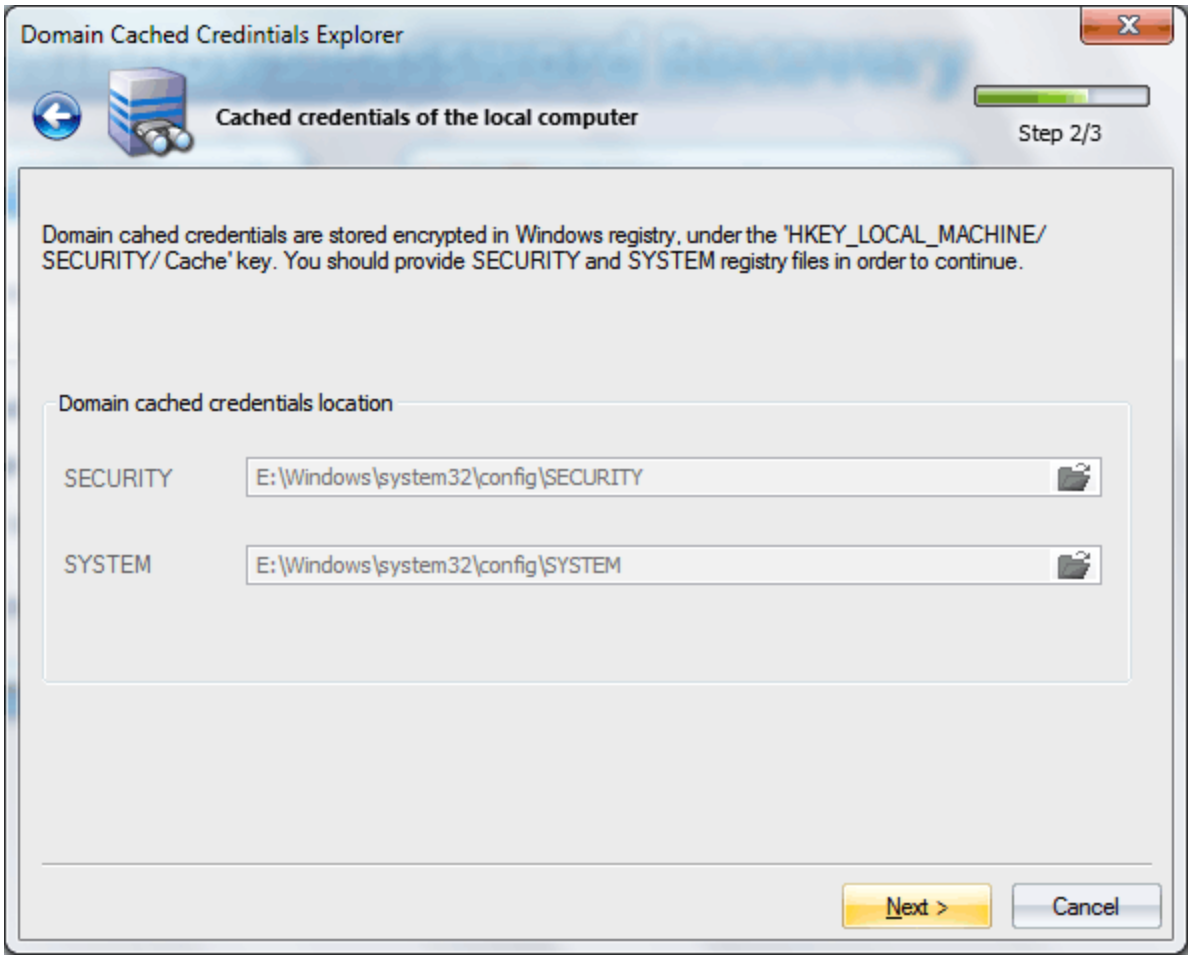
Windows utiliza registros de dominio almacenados en caché para poder conectarse al servidor incluso si el servidor de inicio de sesión no está disponible por cualquier motivo.

El Explorador de credenciales almacenadas en caché de dominio permite descifrar hashes DCC en 3 sencillos pasos:

Primero seleccione el origen de las credenciales: credenciales almacenadas en caché del sistema operativo actual o de otra computadora.

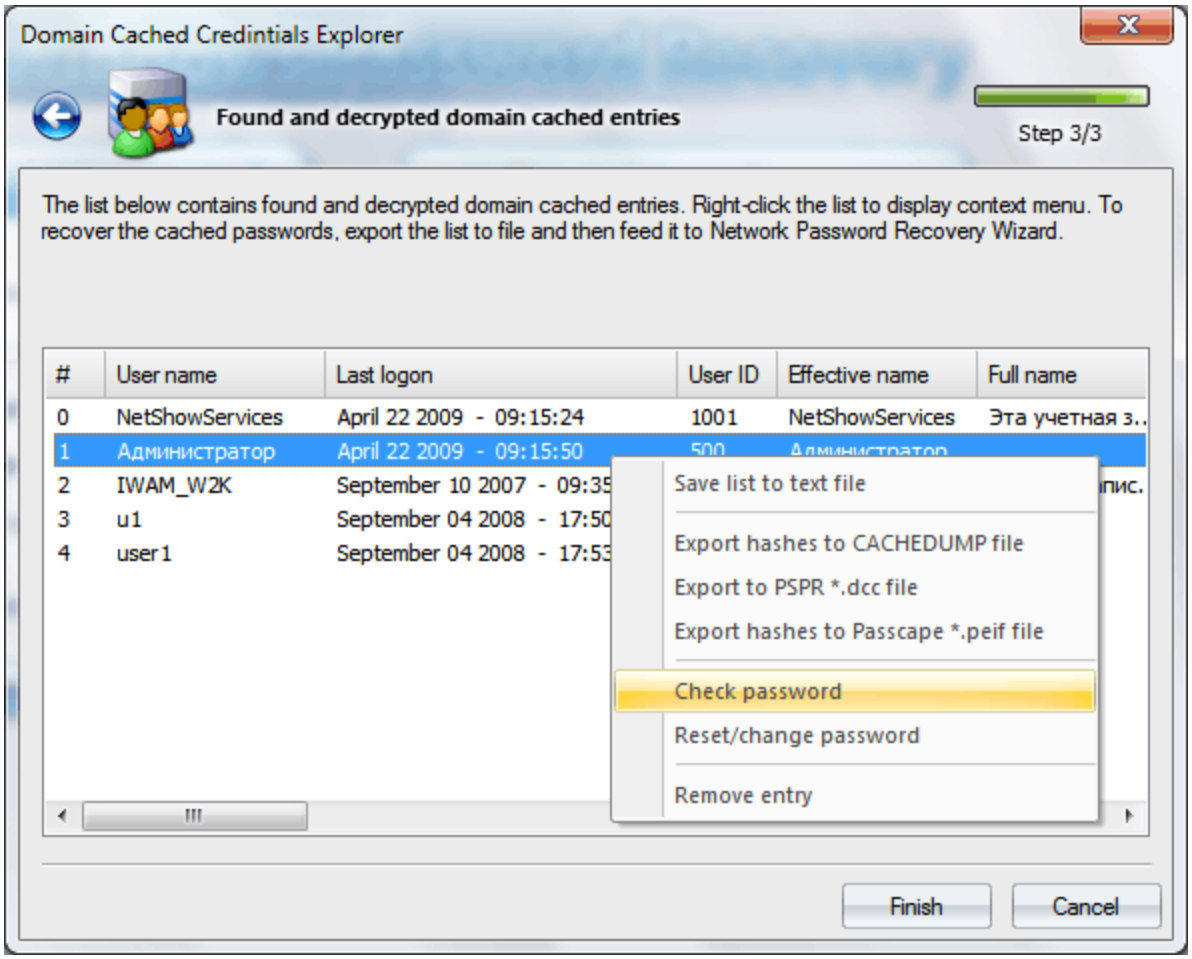


Las credenciales almacenadas en caché de dominio se almacenan en el archivo de registro SECURITY. Por lo tanto, al seleccionar la opción para leer elementos de una PC externa, en el siguiente paso del Asistente, debe especificar la ruta a los archivos de registro SECURITY y SYSTEM utilizados para descifrar los registros. Una vez que se elige la opción de computadora local, el programa debe localizar esos archivos automáticamente. Los archivos del Registro se encuentran en la siguiente carpeta C:\% WINDIR%\system32\config, donde %WINDIR% es el directorio de Windows.



Si la lectura se realizó correctamente, en el cuadro de diálogo final verá las credenciales de dominio descifradas. Cada registro tiene varios atributos. Por ejemplo, nombre de usuario, última hora de inicio de sesión, pertenencia a grupos, contraseña de usuario almacenada en caché (en realidad, hash).

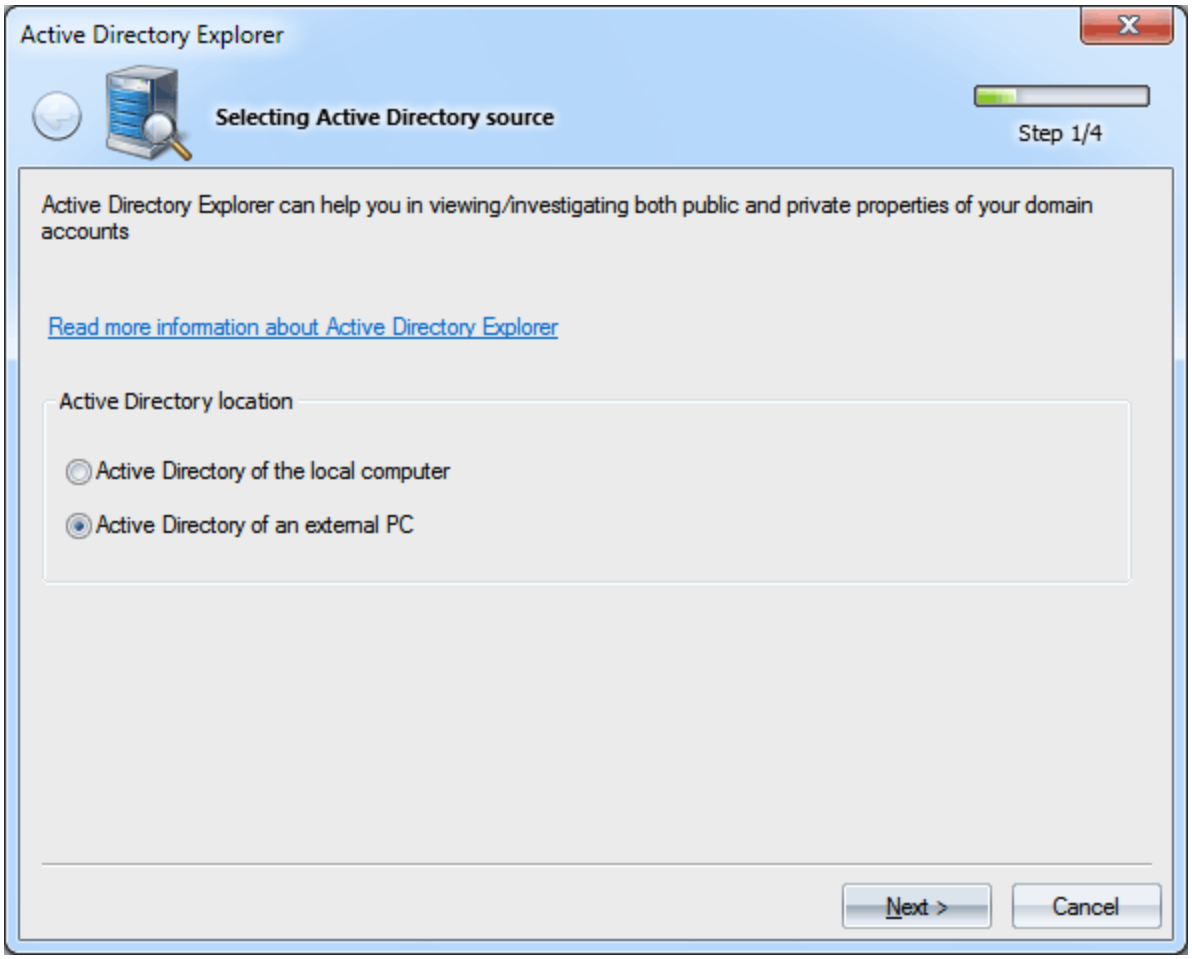
Al hacer clic con el botón derecho en la lista de registros, se abre el menú contextual, que permite:
- Guardar registros con todos los atributos en un archivo de texto.
- Exportar hashes de contraseña a un PWDUMP, *. DCC o *. Archivo PEIF. Tenga en cuenta que el formato PWDUMP almacena los registros de manera no del todo correcta; por lo tanto, es más preferible almacenar hashes de contraseña como *. DCC o *. PEIF archivos.
- Compruebe o edite la contraseña de un registro de dominio almacenado en caché.
- Eliminar registro.



2.7.4.3 Explorador de Active Directory

Explorador de Active Directory es una pequeña utilidad para ver, analizar y editar propiedades (atributos) de cuentas de dominio, tanto públicas como privadas.

Al principio, seleccione el tipo de base de datos de AD con la que va a trabajar: local o externa.

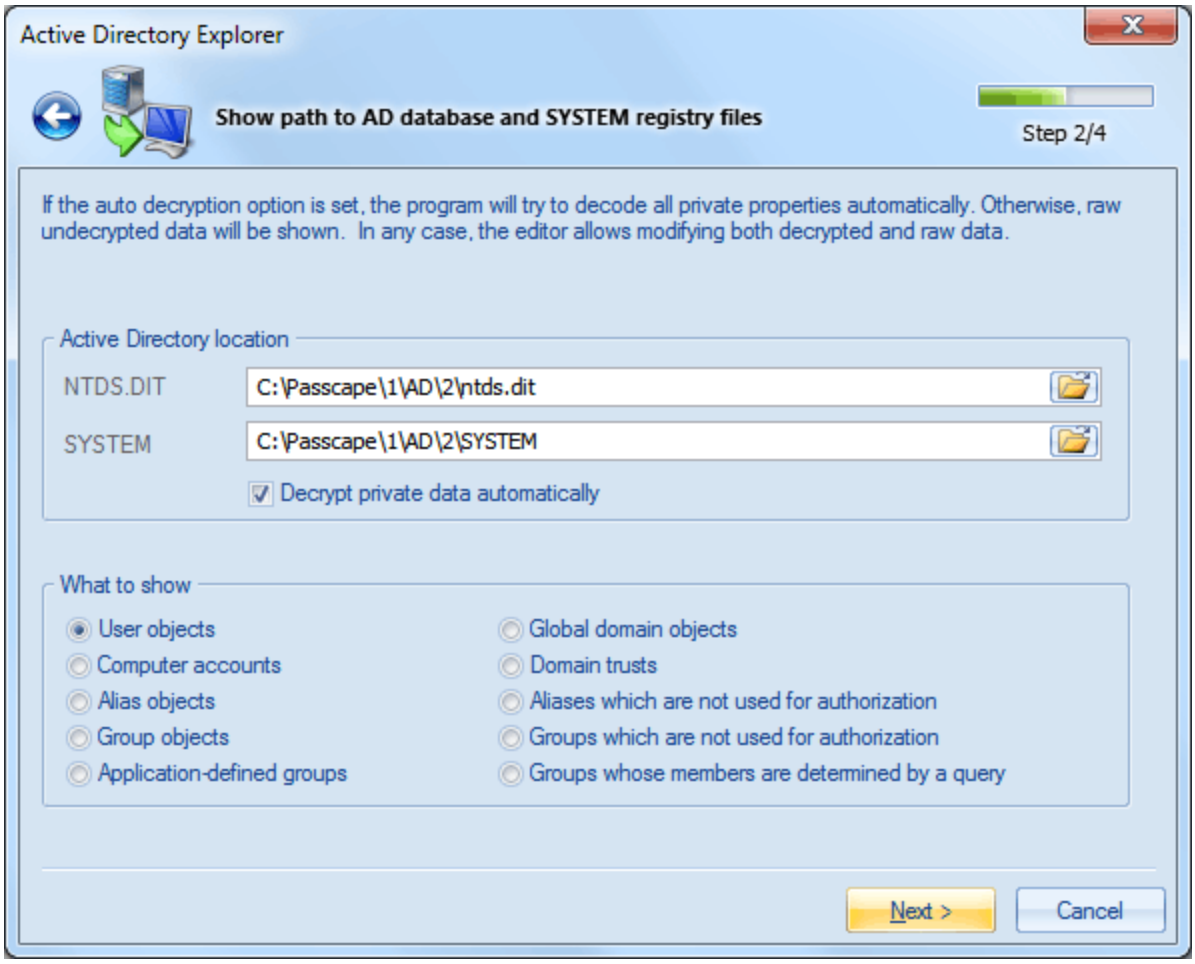


Al seleccionar la base de datos externa, especifique la ruta de acceso al **NTDS.DIT** y al registro **SYSTEM**. Este último es necesario para descifrar datos privados. Si el descifrado automático está habilitado, todos los atributos cifrados de una cuenta se descifrarán sobre la marcha. En cualquier caso, el editor permite editar tanto datos descifrados como sin procesar. Por razones de seguridad, ¡el modo editor solo está disponible para bases de datos externas!

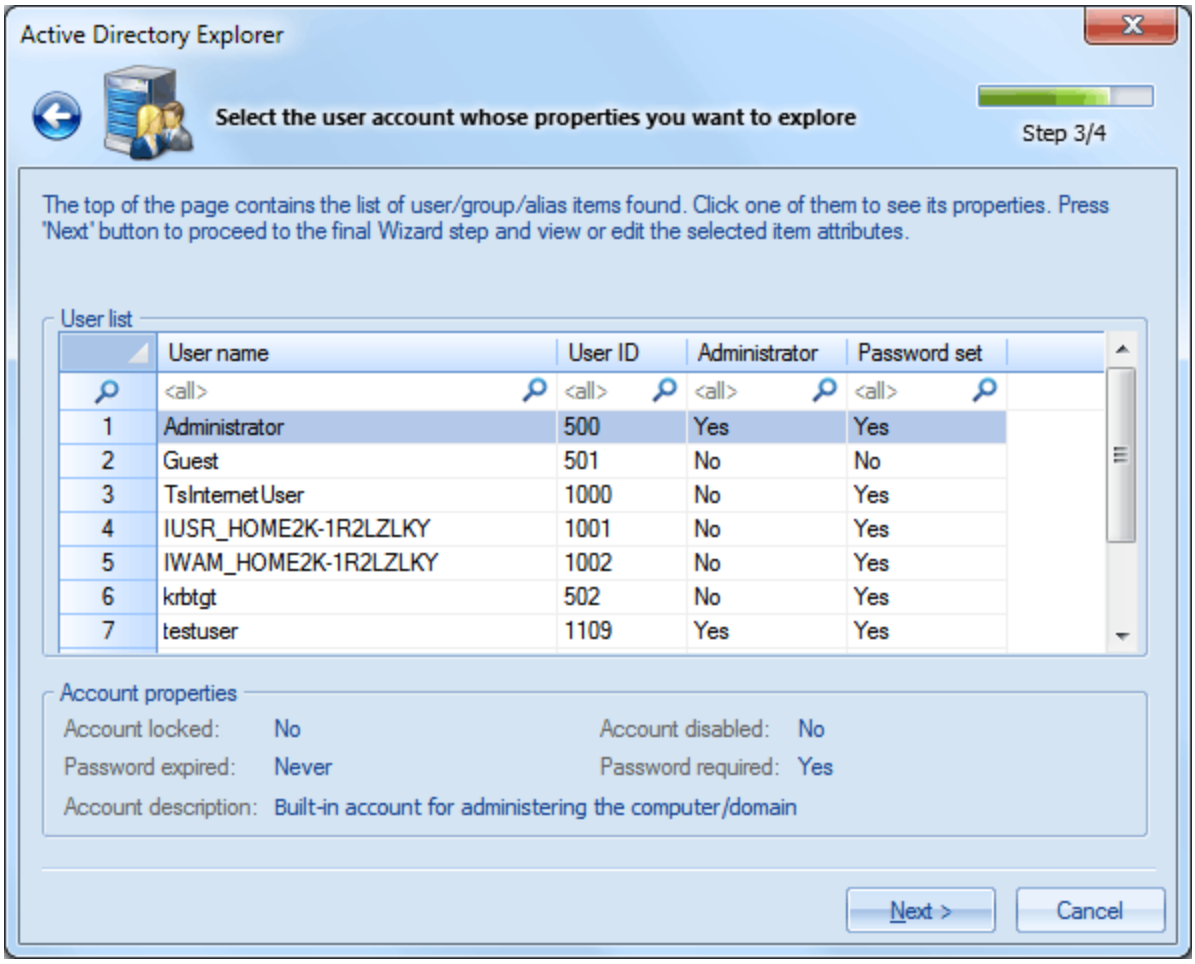
También debe especificar qué objeto desea mostrar. Hay 10 tipos de objetos de dominio. Vea la tabla a continuación.

Objeto de dominio	Descripción
Objeto de usuario	Un objeto de clase usuario. Un objeto de usuario es un objeto principal de seguridad; la entidad de seguridad es una persona o entidad de servicio que se ejecuta en el equipo. El secreto compartido permite que la persona o entidad de servicio se autentique.
Objeto de dominio global	Representa un objeto de dominio típico que no se ajusta a otros tipos.
Cuentas de equipo	Representa un objeto de equipo asociado a equipos cliente o servidor individuales de un dominio de Active Directory.
Confianzas de dominio	Representa un objeto de usuario que se usa para las confianzas de dominio. Un dominio de confianza es un dominio en el que se confía para tomar decisiones de autenticación

Objeto de dominio	Descripción
	para las entidades de seguridad de ese dominio.
Objetos alias	Un grupo de seguridad o distribución que puede contener grupos universales, grupos globales, otros grupos locales de dominio de su propio dominio y cuentas de cualquier dominio del bosque. A los alias se les pueden conceder derechos y permisos en recursos que residen solo en el mismo dominio donde se encuentra el grupo local de dominio.
Alias que no se utilizan para la autorización	Representa un objeto de alias que no se usa para la generación de contexto de autorización.
Agrupar objetos	Objeto de base de datos que representa una colección de objetos de usuario y grupo y tiene un valor de identificador de seguridad (SID).
Grupos que no se utilizan para la autorización	Representa un objeto de grupo que no se usa para la generación de contexto de autorización.
Grupos definidos por la aplicación	Un grupo definido por la aplicación.
Grupos de consultas	Grupo definido por la aplicación cuyos miembros están determinados por los resultados de una consulta.



Una vez seleccionado el origen de datos, pase a seleccionar cuentas. Algunas bases de datos de Active Directory contienen decenas o incluso cientos de miles de registros de dominio. Leer bases de datos tan grandes y completar la lista de usuarios puede llevar algún tiempo. Al seleccionar solo un registro, se muestra una breve información en la parte inferior: estado, si se ha establecido una contraseña y si ha caducado, descripción de la cuenta, etc. Al hacer clic en el botón '*Siguiente* >' se inicia el proceso de recopilación y descifrado de todos los atributos disponibles para el objeto seleccionado.



Cada atributo consta de un nombre y un valor. Por ejemplo, **'Common-Name'** contiene el nombre de la cuenta, y el atributo **'Unicode-Pwd'** almacena su hash de contraseña. Para obtener una descripción más detallada de un atributo, selecciónelo en la lista y luego haga clic en el enlace que aparece en el campo de descripción. Al hacer doble clic en el campo de datos, se abre el atributo seleccionado para editarlo. Cuando haya terminado de editar, haga clic con el botón derecho en el texto para abrir el menú contextual y luego guarde los cambios en el archivo ntds.dit o deséchelos.

Aquí está la descripción de algunos atributos de la cuenta. La descripción completa está disponible en el sitio web de Microsoft.

Common-Name
Nombre de la cuenta.

DBCS-Pwd
Contiene la contraseña de LAN Manager de la cuenta.

Unicode-Pwd
La contraseña del usuario en formato unicode (OWF) de Windows NT. Tenga en cuenta que no puede derivar la contraseña borrada del formulario OWF de la contraseña.

Lm-Pwd-History

Contiene el historial de contraseñas del usuario en formato de función unidirectoria de LAN Manager. El atributo se utiliza para la compatibilidad con clientes de LAN Manager 2.x, Windows 95 y Windows 98.

Nt-Pwd-History
El historial de contraseñas del usuario en formato OWF de Windows NT.

Primary-Group-ID
Identificador relativo (RID) para el grupo principal del usuario. Este es el grupo Usuarios de dominio, de forma predeterminada.

Bad-Pwd-Count
Contiene el número de veces que el usuario intentó iniciar sesión en la cuenta con una contraseña incorrecta.

Admin-Count
Indica que la cuenta es miembro de uno de los grupos administrativos (directa o transitivamente).

Logon-Hours
Las horas en las que el usuario puede iniciar sesión en el dominio.

Last-Logon
La última vez que el usuario inició sesión en la cuenta.

Bad-Password-Time
La última vez que el usuario intentó iniciar sesión en la cuenta con una contraseña no válida. Este valor se almacena como un entero grande de 8 bytes que representa el número de intervalos de 100 nanosegundos desde el 1 de enero de 1601 (UTC).

Last-Logon-Timestamp
Esta es la hora en que el usuario inició sesión por última vez en el dominio.

Pwd-Last-Set
La fecha en que se cambió por última vez la contraseña de esta cuenta.

Account-Expires
La fecha en que caduca la cuenta. Un valor de 0 o 0x7FFFFFFFFFFFFFFF indica que la cuenta nunca caduca.

Supplemental-Credentials
Almacena la versión cifrada de la contraseña del usuario. Se utiliza en la autenticación.

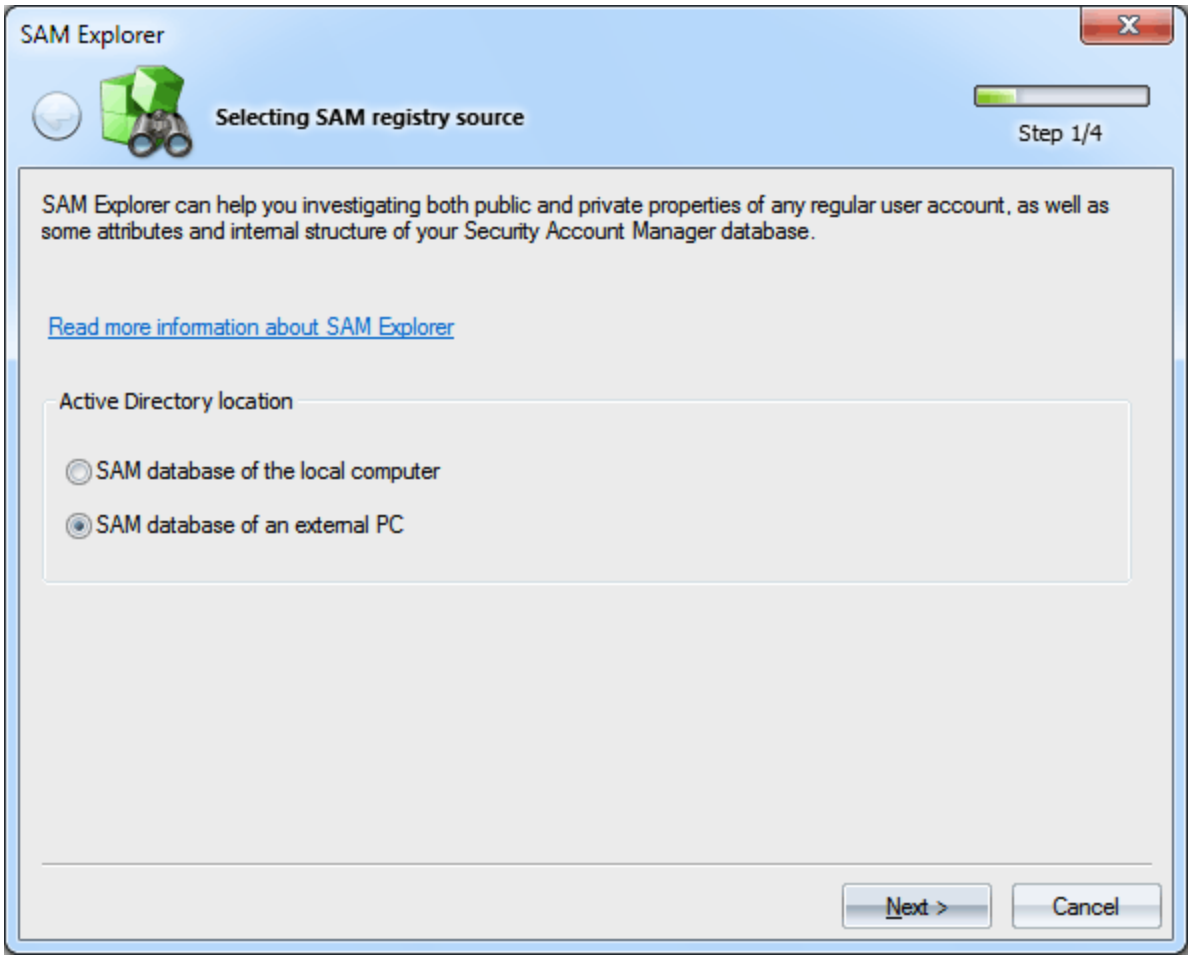
User-Account-Control
Marcas que controlan el comportamiento de la cuenta de usuario. Este valor puede ser una combinación de uno o más de los siguientes valores.
0x00000001 se ejecuta el script de inicio de sesión para la cuenta.
0x00000002 La cuenta está deshabilitada.
0x00000008 se requiere el directorio de inicio.
0x00000010 La cuenta está actualmente bloqueada.
0x00000020 No se requiere contraseña.
0x00000040 El usuario no puede cambiar la contraseña.
0x00000080 La contraseña de texto sin cifrar debe conservarse
0x00000100 Esta es una cuenta para usuarios cuya cuenta principal está en otro dominio.
0x00000200 Este es un tipo de cuenta predeterminado que representa a un usuario típico.
0x00000800 cuenta de confianza para un dominio del sistema que confía en otros dominios.

0x00001000 Esta es una cuenta de equipo para un equipo que es miembro de este dominio.
0x00002000 Esta es una cuenta de equipo para un controlador de dominio de copia de seguridad del sistema que es miembro de este dominio.
0x00010000 La contraseña de esta cuenta nunca caducará.
0x00020000 Esta es una cuenta de inicio de sesión de MNS.
0x00040000 El usuario debe iniciar sesión con una tarjeta inteligente.
0x00080000 La cuenta, en la que se ejecuta un servicio, es de confianza para la delegación Kerberos.
0x00100000 El contexto de seguridad del usuario no se delegará en un servicio, incluso si la cuenta de servicio se establece como de confianza para la delegación Kerberos.
0x00200000 Restringir esta entidad de seguridad para usar solo tipos de cifrado del Estándar de cifrado de datos (DES) para las claves.
0x00400000 Esta cuenta no requiere autenticación previa kerberos para el inicio de sesión.
0x00800000 La contraseña de usuario ha caducado.
0x01000000 La cuenta está habilitada para la delegación. Permite que un servicio que se ejecuta en la cuenta asuma una identidad de cliente y se autentique como ese usuario en otros servidores remotos de la red.
0x04000000 El objeto es un controlador de dominio de solo lectura (RODC)

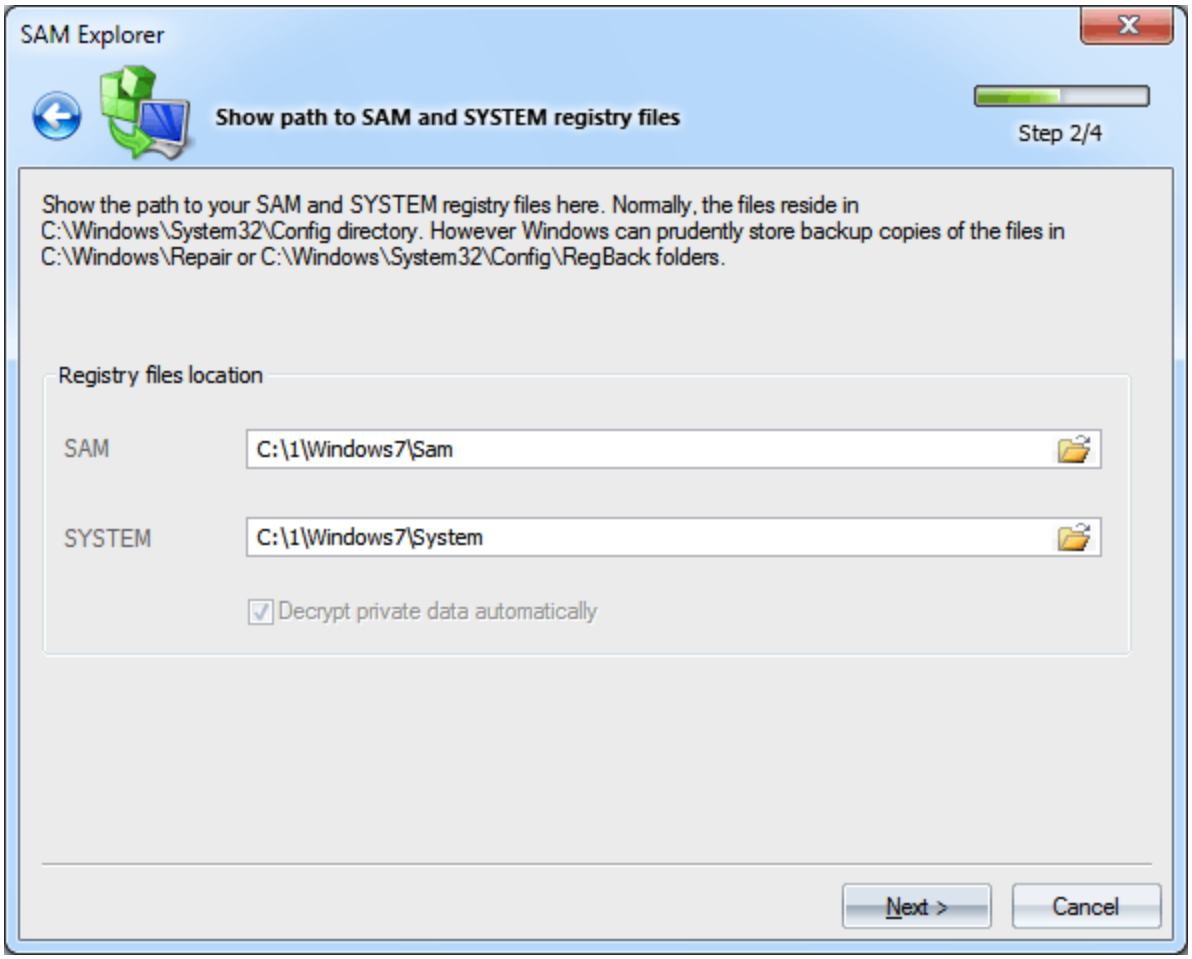
2.7.4.4 Explorador de SAM

Explorador de SAM le permite ver, analizar y editar las propiedades y estadísticas de las cuentas de usuario de Windows. SAM, que es la abreviatura de **Security Account Manager**, es un servidor RPC, que administra la base de datos de cuentas de Windows y almacena contraseñas y datos de usuarios privados, agrupa la estructura lógica de las cuentas, configura la política de seguridad (por ejemplo, contraseña o política de bloqueo de cuentas), recopila estadísticas (última hora de inicio de sesión, recuento de inicio de sesión, recuento de intentos de inicio de sesión fallidos, etc.) y controla el acceso a la base de datos. La base de datos SAM se almacena en el registro (en la clave **HKEY_LOCAL_MACHINE\SAM\SAM**), que es inaccesible para cualquier persona, excepto el sistema (incluso para los administradores). En el nivel físico, la base de datos SAM es un archivo de registro binario con el nombre respectivo, ubicado en %WINDIR%\System32\Config, donde %WINDIR% es la carpeta de instalación de Windows.

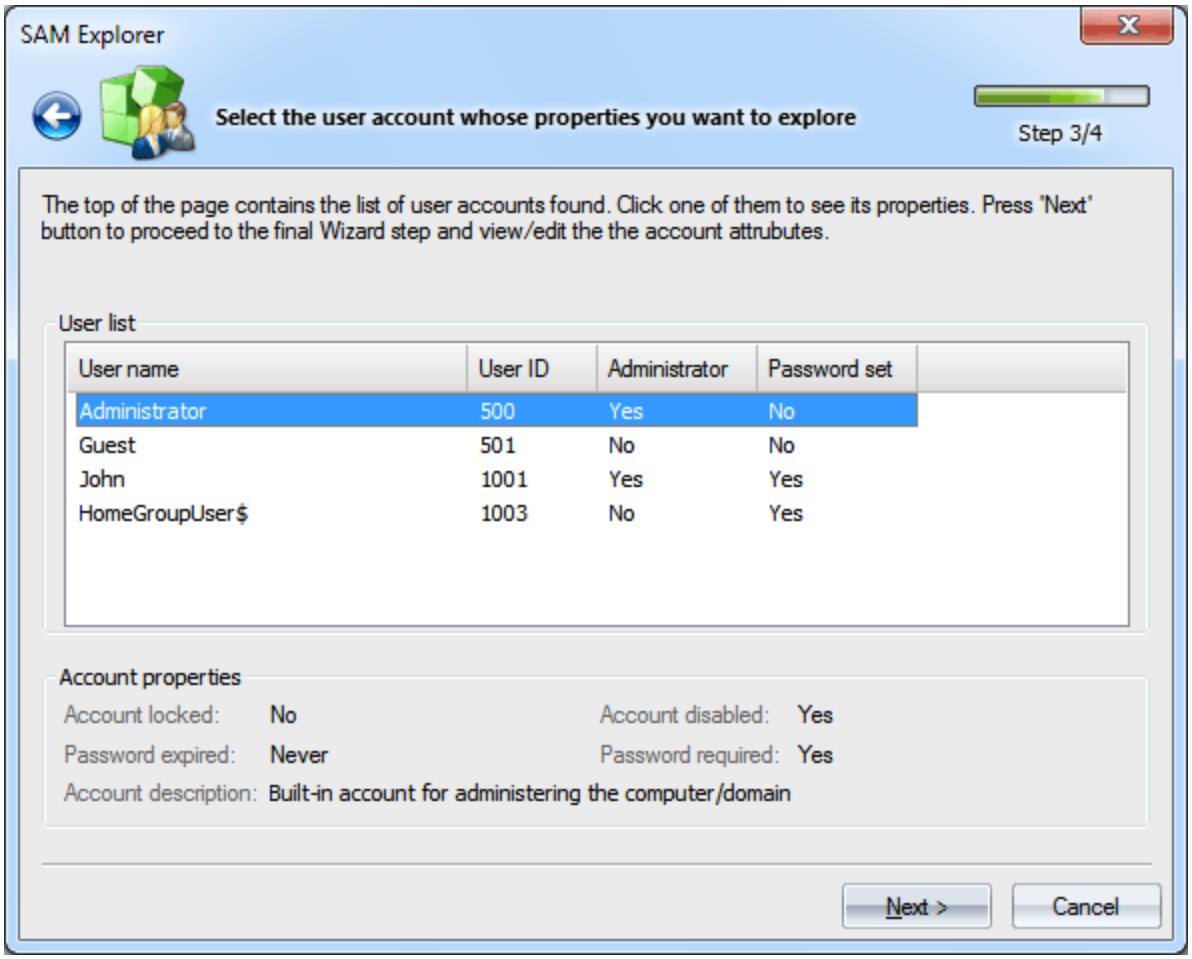
Al principio, el Asistente le pedirá que seleccione el tipo de base de datos SAM: local o externa. Tenga en cuenta: si selecciona una base de datos local, por razones de seguridad, el editor no estará disponible y la base de datos se abrirá en el modo de solo lectura.



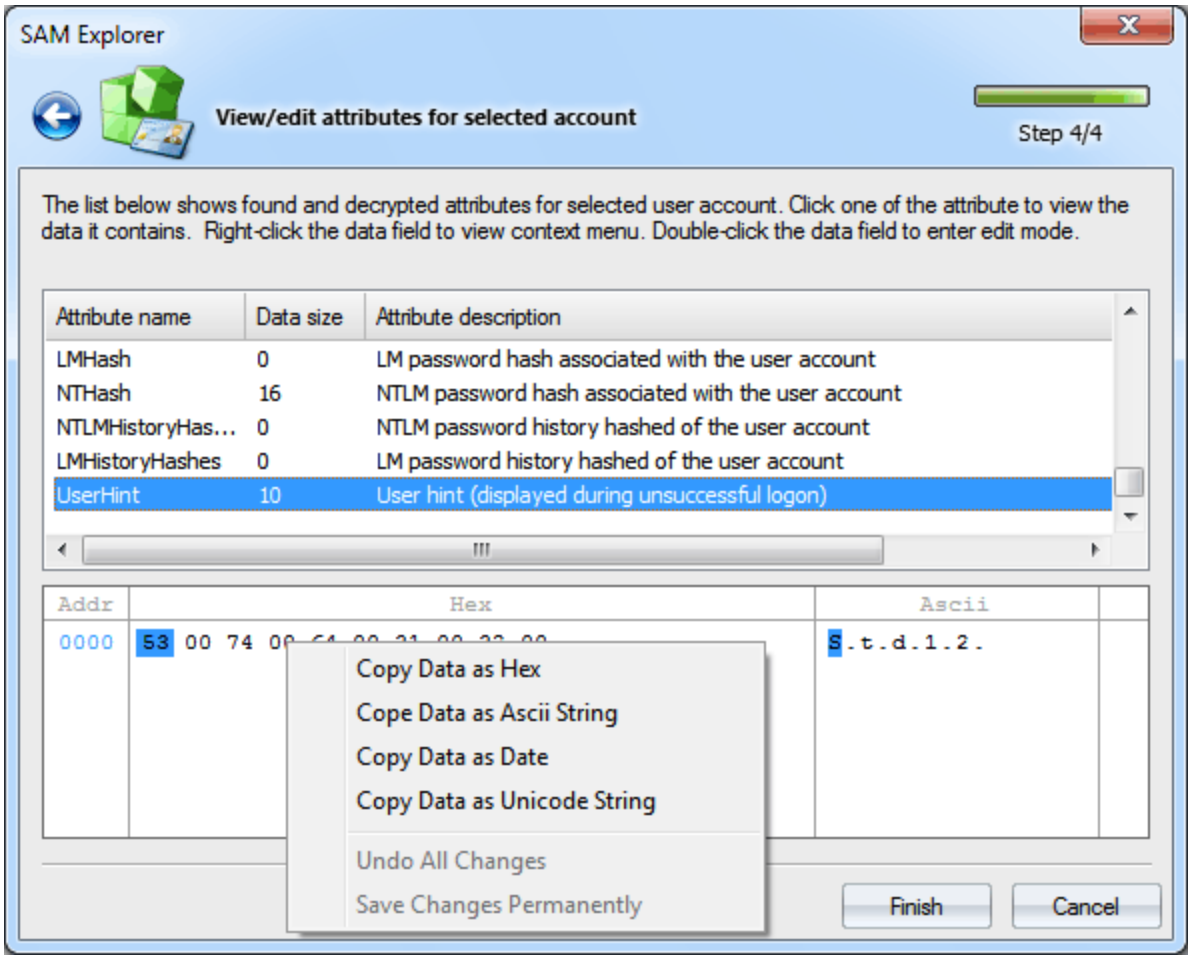
Si selecciona la base de datos SAM en un equipo externo, en el segundo paso del Asistente, especifique la ruta de acceso a los registros SAM y SYSTEM. De forma predeterminada, ambos archivos se encuentran en **C:\Windows\System32\Config**. Tenga en cuenta que Windows puede almacenar providencialmente copias de los archivos del Registro en las carpetas de copia de seguridad, como **C:\Windows\Repair** o **C:\Windows\ Config\RegBack**.



En el tercer paso, continúe seleccionando la cuenta para la que necesita obtener los atributos. Seleccione el usuario y, a continuación, haga clic en Siguiente.



Eso le da la lista de atributos para la cuenta seleccionada. Al seleccionar un determinado atributo en la lista, se muestran los datos comunes a ese atributo en la parte inferior del editor. Para abrirlo para editarlo, haga doble clic en el campo de datos; al finalizar, seleccione el elemento Guardar cambios en el menú contextual



Descripción de los atributos de la cuenta SAM.

DataRevision
Un entero sin firmar de 32 bits que almacena la versión de la estructura de datos. Se divide en 2 WORDs: versión mayor y versión menor.

LastLogon
Un valor de 64 bits, equivalente a un FILETIME, que indica la hora en la que la cuenta inició sesión por última vez.

LastLogoff
Un valor de 64 bits, equivalente a un FILETIME, que indica la hora en la que la cuenta cerró la sesión por última vez.

PasswordLastSet
Un valor de 64 bits, equivalente a un FILETIME, que indica la hora en la que se actualizó por última vez una contraseña.

AccountExpires
Un valor de 64 bits, equivalente a un FILETIME, que indica la hora en la que una cuenta ya no puede iniciar sesión.

LastBadPasswordTime
Un valor de 64 bits, equivalente a un FILETIME, que indica la hora en la que una cuenta intentó iniciar sesión por última vez sin éxito.

UserID
Un entero sin firmar de 32 bits que representa el RID de la cuenta.

PrimaryGroupId
Un entero sin firmar de 32 bits que indica el identificador de grupo principal del recuento.

UserAccountControl
Un indicador de 32 bits que especifica las características de la cuenta.

CountryCode
Un entero sin firmar de 16 bits que indica una preferencia de país específica para este usuario. El espacio de valores es el código de llamada internacional del país. Por ejemplo, el código de país del Reino Unido, en notación decimal, es 44.

CodePage
Un entero sin signo de 16 bits que indica una preferencia de página de códigos específica de este objeto de usuario. El espacio de valores es la designación de la página de códigos de Microsoft.

BadPasswordCount
Un entero sin firmar de 16 bits que indica el número de intentos de contraseña incorrecta.

LogonCount
Un entero sin firmar de 16 bits que indica el número de veces que se ha autenticado la cuenta de usuario.

AdminCount
Un entero sin firmar de 16 bits que indica que la cuenta es miembro de uno de los grupos administrativos (directa o transitivamente).

OperatorCount
Un entero sin firmar de 16 bits que indica que la cuenta es miembro del grupo Operadores.

UserName
Cadena Unicode que especifica el nombre de la cuenta de usuario.

FullName
Cadena Unicode que contiene el nombre completo del usuario.

AdminComment
Comentario del administrador asociado a la cuenta de usuario.

UserComment
Segundo comentario de usuario asociado a la cuenta de usuario.

Parameters
Parámetros de usuario extendidos. Los productos de Microsoft usan este miembro para almacenar información de configuración del usuario.

HomeDirectory

Cadena Unicode que especifica la ruta del directorio principal de la cuenta de usuario.

HomeDirectoryDrive
Especifica la letra de unidad que se va a asignar al directorio principal del usuario con fines de inicio de sesión.

ScriptPath
Cadena Unicode que especifica la ruta de acceso para el archivo de script de inicio de sesión del usuario. El archivo de script puede ser un archivo . CMD, un archivo . EXE o un archivo . Archivo BAT.

ProfilePath
Cadena Unicode que especifica una ruta de acceso al perfil del usuario.

WorkStations
Cadena Unicode que contiene los nombres (separados por comas) de las estaciones de trabajo desde las que el usuario puede iniciar sesión. Se pueden especificar hasta ocho estaciones de trabajo. El indicador de UF_ACCOUNTDISABLE de cuenta permite deshabilitar los inicios de sesión de todas las estaciones de trabajo en esta cuenta.

LogonHours
Cadena de bits de 21 bits que especifica los tiempos durante los cuales el usuario puede iniciar sesión. Cada bit representa una hora única en la semana, en greenwich mean time. El primer bit es domingo, de 0:00 a 0:59; el segundo bit es el domingo, de 1:00 a 1:59; y así sucesivamente. Tenga en cuenta que el bit 0 en la palabra 0 representa el domingo de 0:00 a 0:59 solo si se encuentra en la zona horaria GMT. En todos los demás casos, debe ajustar los bits de acuerdo con el desplazamiento de su zona horaria (por ejemplo, GMT menos 8 horas para la hora estándar del Pacífico).

Groups
Lista de grupos a los que pertenece o no pertenece la cuenta de usuario.

LMHash
Hash de contraseña LM asociado a la cuenta de usuario.

NTHash
Hash de contraseña NTLM asociado a la cuenta de usuario.

LMHistoryHashes
Historial de hashes de contraseñas LM de la cuenta de usuario.

NTHistoryHashes
Historial de contraseñas hasheadas en NTLM de la cuenta de usuario.

UserHint
Sugerencia de usuario (que se muestra durante el inicio de sesión fallido).

UserPicture
Imagen de inicio de sesión asociada a la cuenta.

2.7.4.5 Herramientas DPAPI

A partir de Windows 2000, Microsoft comenzó a equipar sus sistemas operativos con una interfaz especial de protección de datos, **Data Protection Application Programming** Interface (DPAPI). Actualmente DPAPI está muy extendido y se utiliza en muchas aplicaciones y subsistemas de Windows. Por ejemplo, en el sistema de cifrado de archivos, para almacenar contraseñas de redes inalámbricas, en Microsoft Vault y Credential Manager, Internet Explorer, Outlook, Skype, Google Chrome, etc. Este sistema se ha hecho popular entre los programadores en primer lugar por su simplicidad de uso, ya que consta de solo un par de funciones para cifrar y descifrar datos: CryptProtectData y CryptUnprotectData. Sin embargo, a pesar de su aparente simplicidad, la implementación técnica de DPAPI es bastante complicada.

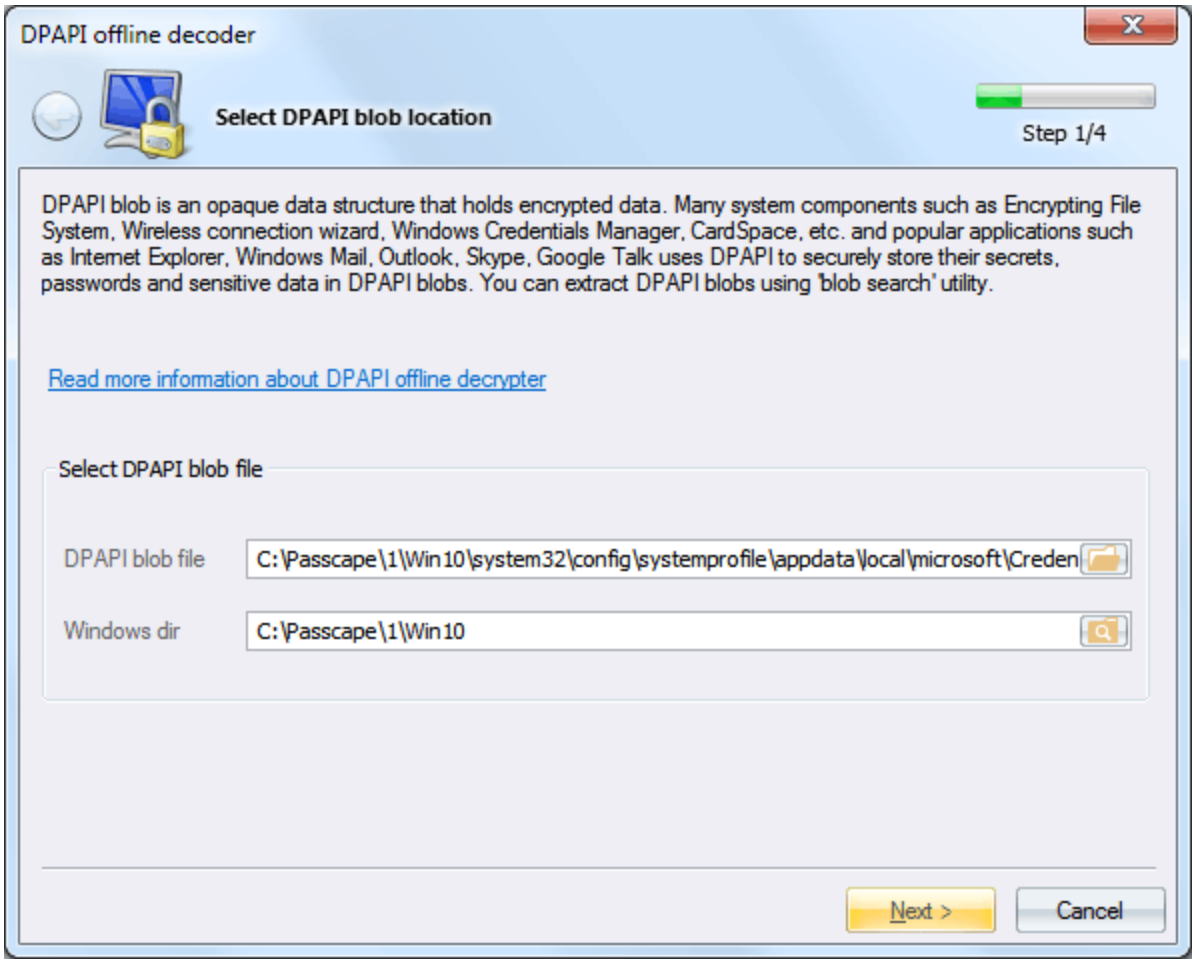
Passcape Software es el primero en el mundo que ofrece un conjunto de 6 herramientas para el análisis exhaustivo y el descifrado de datos cifrados con DPAPI. Estas utilidades le permiten:

- Descifrar blobs DPAPI para cualquier cuenta
- Buscar blobs DPAPI en disco
- Descifrar blobs DPAPI cifrados en la cuenta SYSTEM (por ejemplo, contraseñas WiFi)
- Analizar y descifrar las claves maestras del usuario
- Compruebe la contraseña del usuario sin volcar hashes de SAM o NTDS. DIT
- Descifrar hashes de historial de todas las contraseñas introducidas anteriormente (sin usar SAM o NTDS.DIT)

2.7.4.5.1 Descifrar blob DPAPI

El descifrado de blobs DPAPI consta de cuatro pasos del asistente.

Seleccione el archivo de blobs cifrado DPAPI



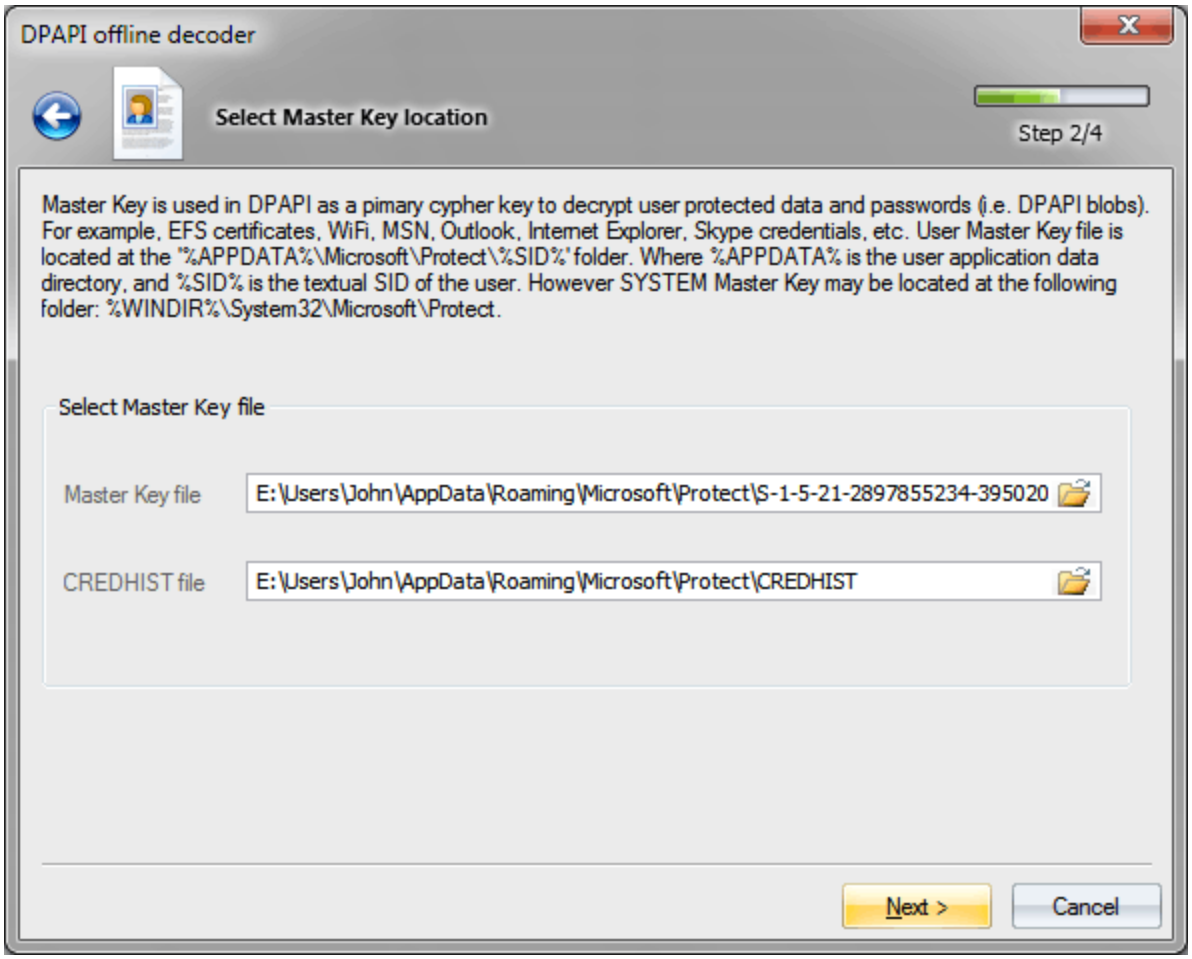
En el primer paso, especifique la ruta de acceso al blob DPAPI y al directorio de Windows. Hay que decir que los objetos DPAPI reales pueden almacenarse en diferentes ubicaciones del sistema operativo; por ejemplo, en archivos XML individuales, en el Registro, en Active Directory; y en diferentes formatos: binario, ASCII, UNICODE. Hay una herramienta especial para localizar, extraer y guardar blobs DPAPI en archivos. Con esa utilidad, por ejemplo, puede guardar todos los blobs DPAPI del registro de un usuario en archivos individuales y usarlos en el programa.

Estas son las ubicaciones de almacenamiento de algunos objetos DPAPI.

- Contraseñas de Internet Explorer y Outlook, contraseñas WIFI (solo XP): registro del usuario, **%APPDATA%\ntuser.dat**
- Google Chrome: **%LOCALAPPDATA%\Google\Chrome**
- Contraseñas WIFI (Windows Vista y superior): **%PROGRAMDATA%\Microsoft\Wlansvc**
- Contraseñas de conexión de red (Administrador de credenciales de Windows): **%LOCALAPPDATA%\Microsoft\Credentials** o **%APPDATA%\Microsoft\Credentials**

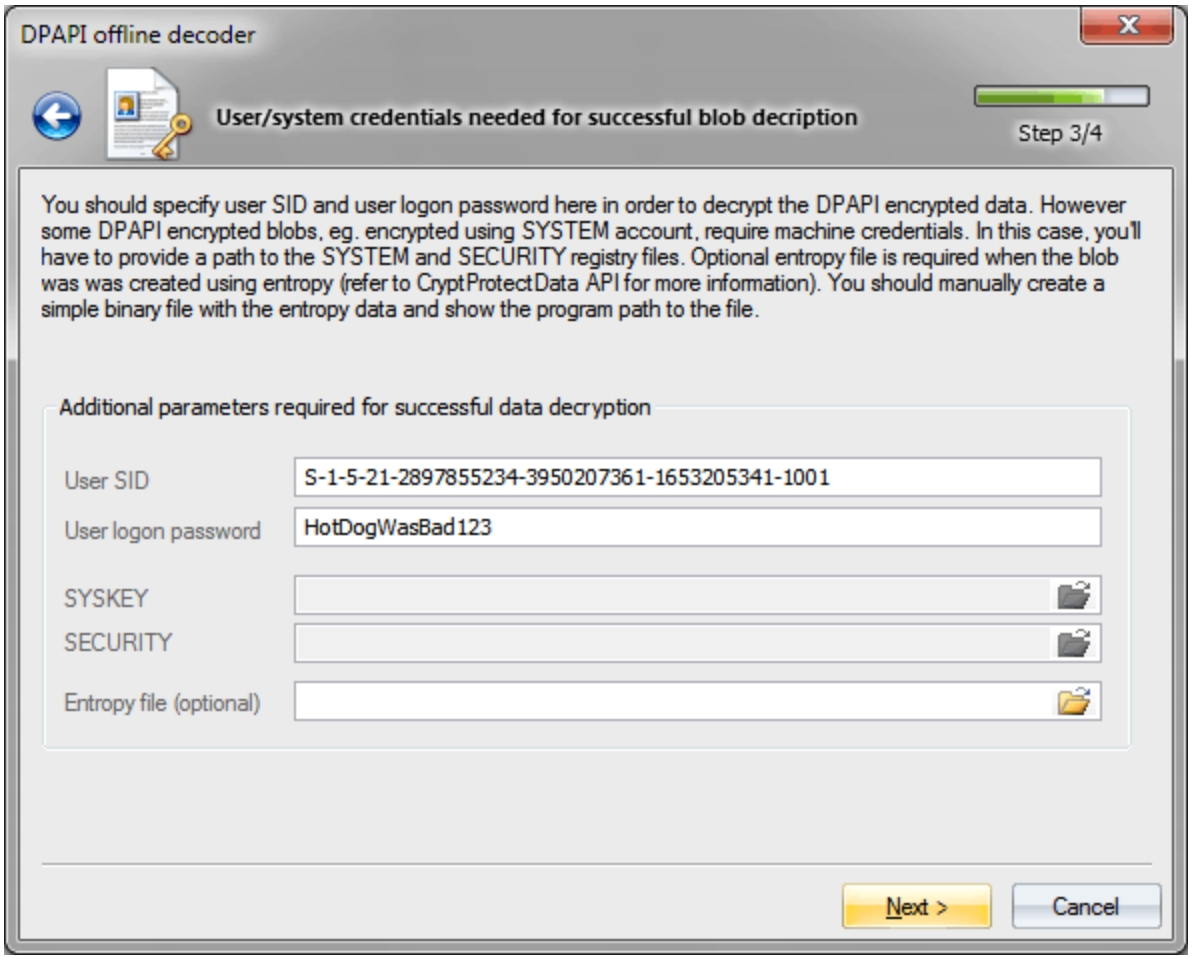
Use la utilidad buscador para extraer datos DPAPI de allí.

Seleccione clave maestra



La clave maestra es un conjunto de 64 bytes aleatorios, que se utiliza como clave principal al descifrar blobs DPAPI. La clave maestra se cifra con la contraseña del usuario (o la contraseña del sistema si se trata de una clave maestra del sistema). La clave maestra del usuario siempre está ubicada en **%APPDATA%\Microsoft\Protect\%SID%**, mientras se almacenan las claves maestras de una cuenta del sistema en **%SYSTEMDIR%\Microsoft\Protect**. Debe tenerse en cuenta que puede haber varias claves maestras, y solo una de ellas es adecuada para descifrar un determinado objeto, el que tiene el nombre almacenado dentro del blob DPAPI. Al buscar una clave maestra, el programa puede filtrar nombres innecesarios. La carpeta **%APPDATA%\Microsoft\Protect** también contiene el archivo **CREDHIST**, que es un parámetro opcional y, en la mayoría de los casos, no es necesario para el descifrado.

Descifrar clave maestra



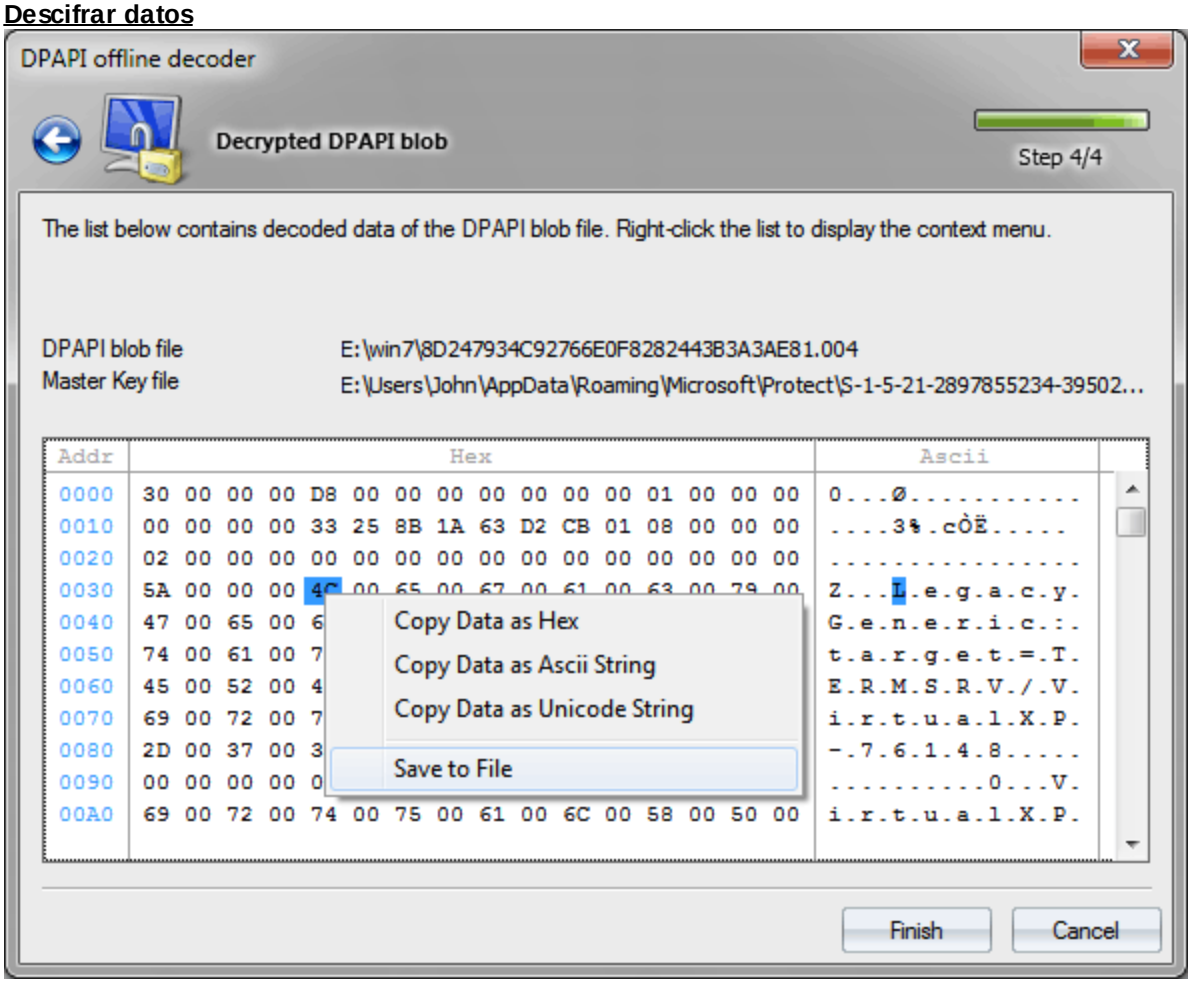
Se deben establecer al menos dos parámetros para descifrar la clave maestra del usuario: la contraseña de inicio de sesión del usuario y su identificador de seguridad (SID), que normalmente se especifica en la ruta a la clave maestra o se muestra en CREDHIST. De una forma u otra, Windows Password Recovery calcula el SID del usuario automáticamente. Para descifrar la clave maestra de un sistema, como ya se ha dicho, establecer una contraseña no tiene sentido, ya que el programa recupera todos los datos necesarios para la recuperación de dos archivos de registro: SYSTEM y SECURITY. Si se utilizó entropía adicional al crear el blob DPAPI, debe crear manualmente el archivo de entropía binaria y especificar la ruta de acceso a él. Por ejemplo, al cifrar contraseñas de Internet Explorer, el nombre del sitio web con formato UNICODE se utiliza como entropía.

Es curioso que Windows 2000 tenga una vulnerabilidad crítica, que permite descifrar cualquier (!) ¡Blob DPAPI en un PC independiente sin especificar necesariamente la contraseña de inicio de sesión del usuario! Es decir, todos los datos protegidos con DPAPI son realmente vulnerables. Esta es una falla importante en la implementación de DPAPI, que es conocida por Microsoft; Sin embargo, otros sistemas operativos no tienen este inconveniente. Si el indicador **CRYPTPROTECT_LOCAL_MACHINE** se estableció en la función CryptProtectData al proteger datos, el descifrado de esos datos también es posible sin la contraseña de inicio de sesión del usuario (por ejemplo, contraseñas de red inalámbrica). Sin embargo, esta es una peculiaridad de una implementación de interfaz y no es un error.

Windows Password Recovery a partir de la versión 9.7 utiliza algunas nuevas vulnerabilidades en la protección de la Clave Maestra en DPAPI que fueron detectadas por nuestra empresa. Por lo tanto, para descifrar una clave maestra de un usuario de dominio, la contraseña de inicio de sesión del propietario ya no es necesaria.

WPR v11.7 es compatible con la función de inicio de sesión automático de arranque de confianza de Windows 10. Si el programa detecta que el inicio de sesión automático de arranque de confianza está configurado para el usuario, no se requiere ninguna contraseña de inicio de sesión para descifrar los datos.

Descifrar datos

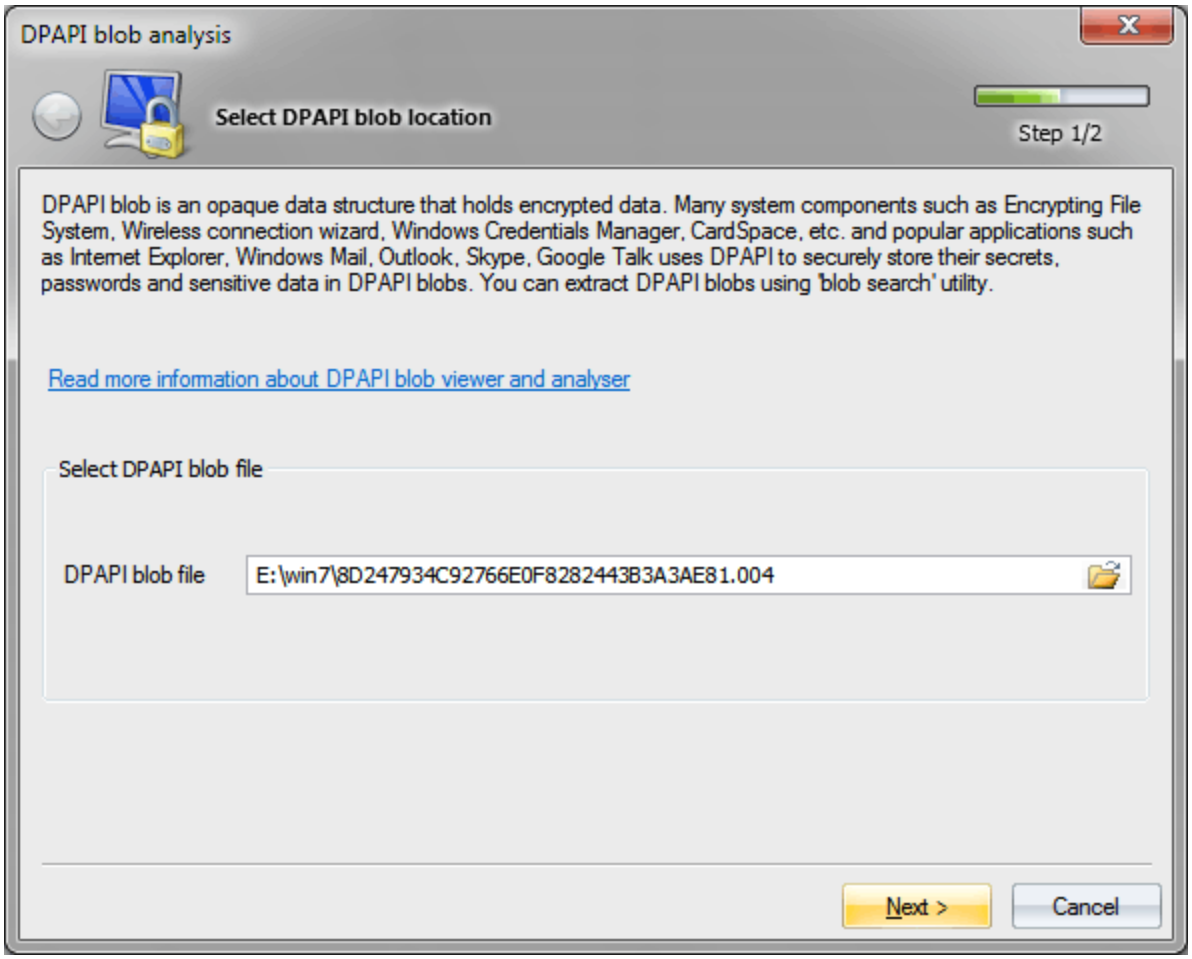


Teniendo todo lo necesario, Windows Password Recovery realiza el descifrado final de los datos de blob DPAPI, que luego puede copiar en el portapapeles o guardar en el archivo. Si el paso final del descifrado termina con un error, lo más probable es que no haya configurado correctamente o no haya establecido en absoluto la entropía adicional. Por ejemplo, Internet Explorer y Vista Ftp Manager utilizan la página de origen donde se introdujo la contraseña como entropía. El Administrador de credenciales de Windows, de manera similar, usa ciertas constantes de cadena, etc.

2.7.4.5.2 Analizar blob DPAPI

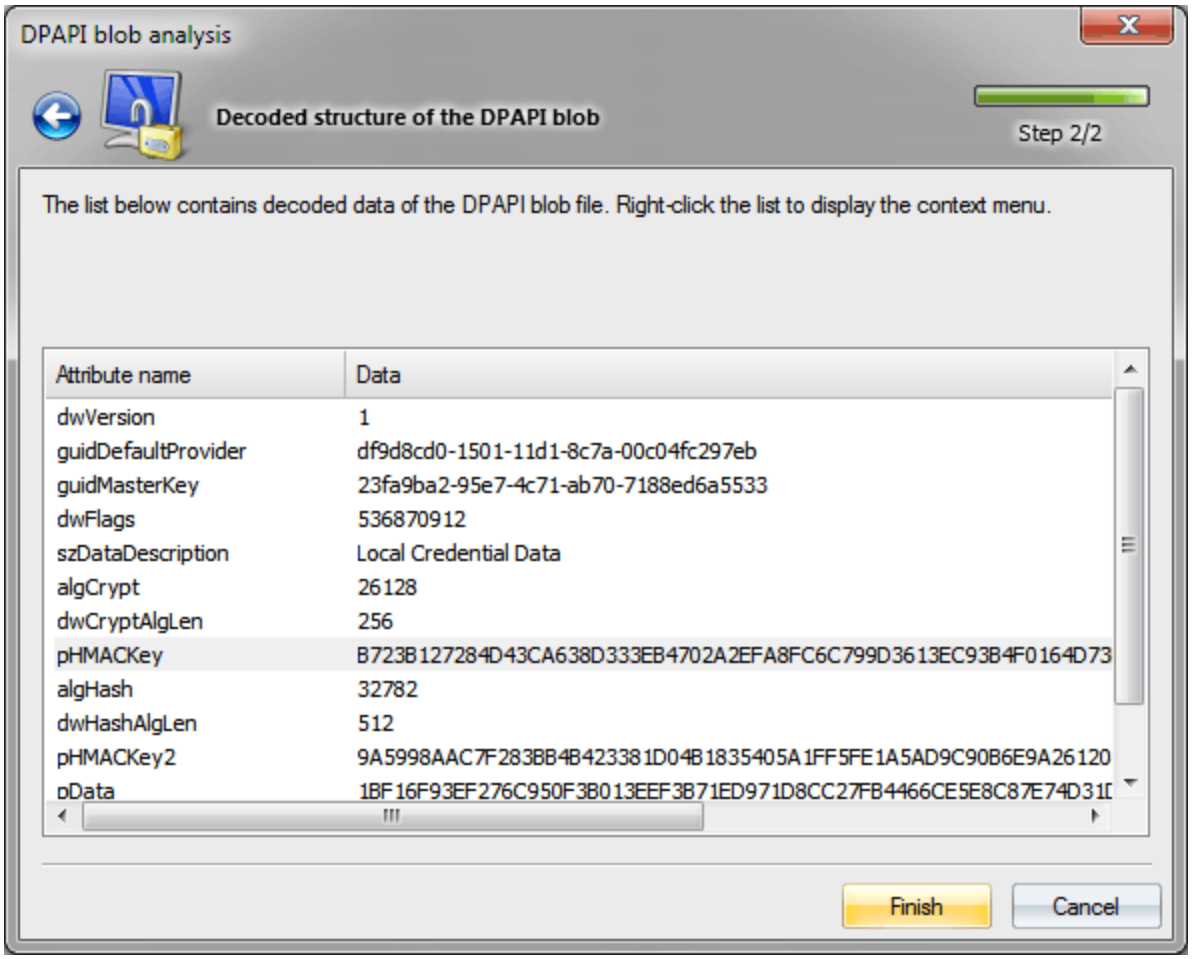
Un blob DPAPI es una estructura binaria opaca, que contiene los datos privados de la aplicación cifrados mediante DPAPI. Muchas aplicaciones y subsistemas de Windows almacenan contraseñas, secretos y datos privados en blobs DPAPI. Para crear archivos con blobs DPAPI (para un análisis más detallado), utilice nuestra Utilidad de búsqueda de blobs DPAPI.

Especificar ruta de acceso al blob DPAPI



Este es el archivo creado por la herramienta de búsqueda de blobs.

Y proceder al análisis de datos



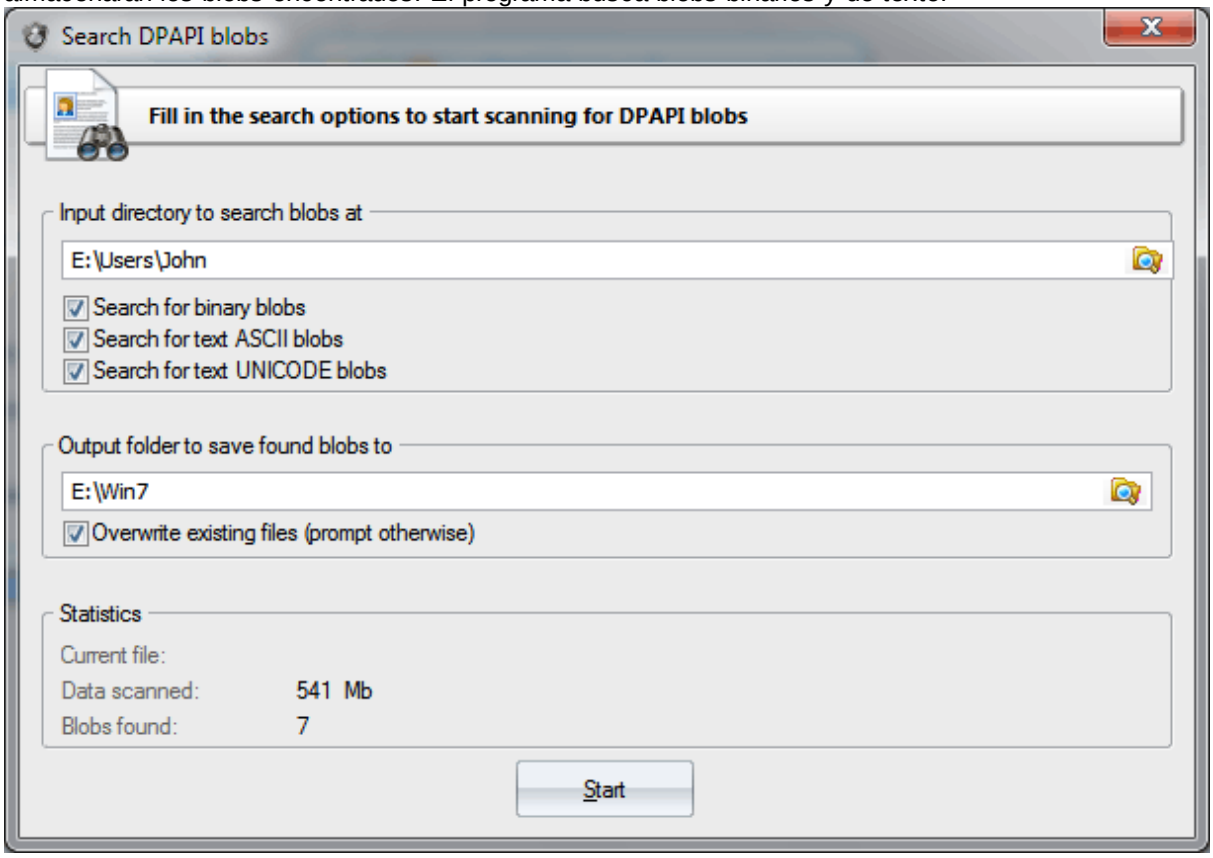
El blob DPAPI es una estructura de datos binaria, que consta de los siguientes atributos consecutivos:

- **dwVersion** — versión de la estructura de datos. Versión actual de los datos - 1.
- **guidDefaultProvider** — El proveedor de cifrado de datos, utilizado en las llamadas a funciones de cifrado, garantiza la compatibilidad de las versiones y organiza primitivas críptológicas simples. Por ejemplo, puede establecer Blowfish o RC5 como un cifrado de bloques. Actualmente, Windows tiene el siguiente proveedor de cifrado predeterminado: **df9d8cd0-1501-11d1-8c7a-00c04fc297eb**, que se corresponde con la clave del Registro HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\Protect\Providers\df9d8cd0-1501-11d1-8c7a-00c04fc297eb.
- **guidMasterKey** — GUID de clave maestra, con el que se cifran los datos. Para descifrar datos dentro de un blob DPAPI, en primer lugar debe descifrar la clave maestra con el nombre establecido en la estructura binaria guidMasterKey. Solo se puede adjuntar una clave maestra a un blob DPAPI.
- **dwFlags** — varias banderas. Por ejemplo, cuando se establece el bit 3, indica que el descifrado de los datos se debe llevar a cabo en la cuenta SYSTEM. El bit (dwFlags&0x20000000) está configurado en todo momento.
- **szDataDescription** — descriptor de datos, que se establece mediante el parámetro opcional LPCWSTR *szDataDescr* en la función CryptProtectData.
- **algCrypt** — algoritmo de cifrado de datos. De forma predeterminada, Windows 7 utiliza AES 256 (que corresponde a 0x6610 en el hexadecimal o 26128 en la notacion decimal), Windows XP - 3DES, Windows 2000 - RC4.
- **dwCryptAlgLen** — longitud de la clave en el algoritmo de cifrado.
- **pHMACKey** — Llave HMAC 1.
- **pSalt** — sal (opcional).

- **algHash** — algoritmo de hasheado. De forma predeterminada, Windows 7 utiliza SHA 512, Windows XP y Windows 2000 - SHA1.
- **dwHashAlgLen** — longitud de hash en la función de hasheado.
- **pHMACKey2** — Llave HMAC 2.
- **pData** — datos cifrados reales.
- **pSignHash** — firma digital para verificar la integridad de los datos.

2.7.4.5.3 Buscar blobs DPAPI

El cuadro de diálogo de búsqueda de blobs DPAPI es bastante trivial. Todo lo que necesita especificar es la carpeta de origen, que el programa buscaría blobs DPAPI, y la carpeta de destino, donde se almacenarán los blobs encontrados. El programa busca blobs binarios y de texto.



Ejemplo de una ruta de acceso, donde puede encontrar archivos, que contienen blobs DPAPI *binarios*:
C:\Users\John\AppData\Roaming\Microsoft\Credentials

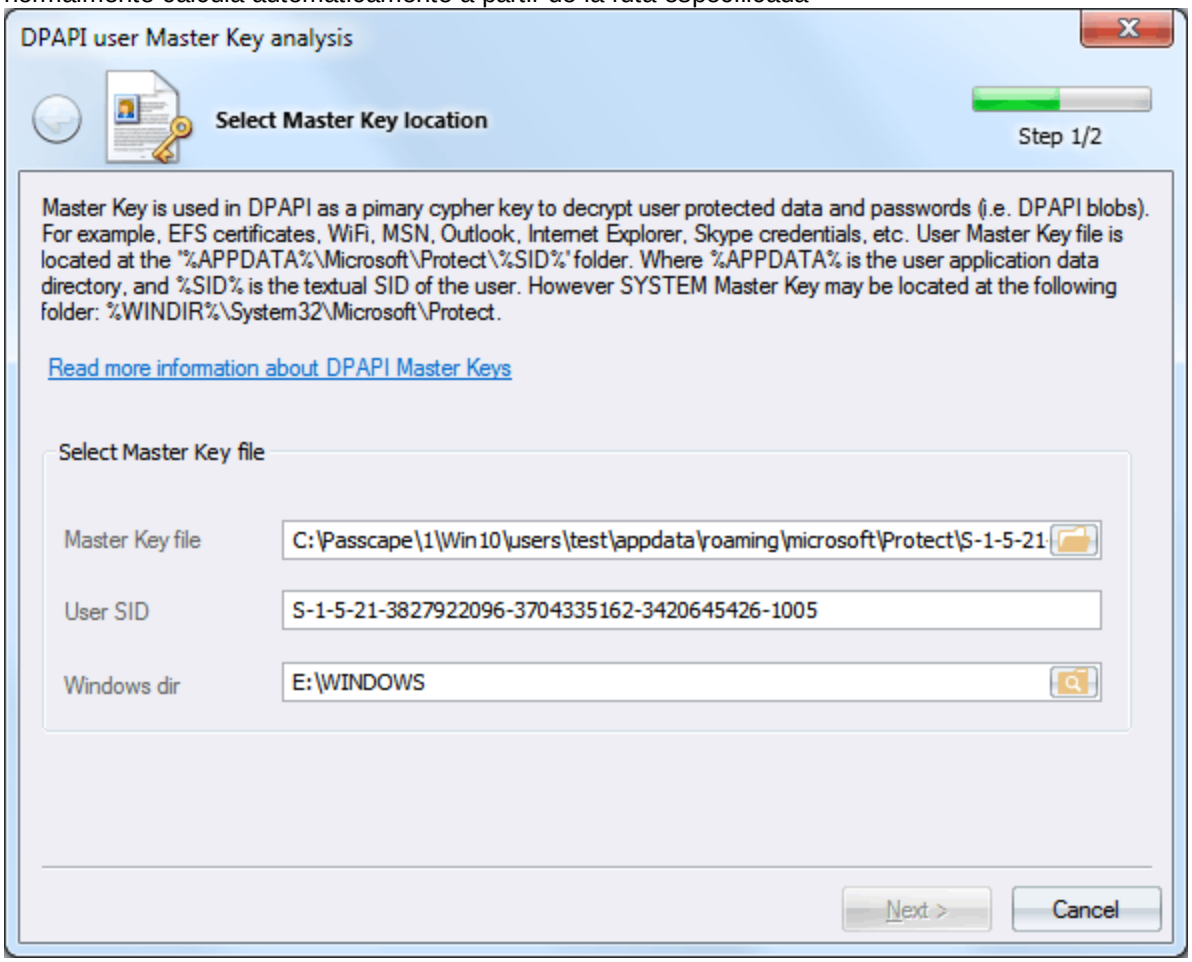
Ejemplo de una ruta de acceso, donde puede encontrar archivos, que contienen blobs DPAPI textuales:
C:\ProgramData\Microsoft\Wlansvc

Tenga en cuenta que si desea buscar blobs en el registro del usuario actual o en la base de datos de Active Directory, primero debe hacer un respaldo de los archivos en un directorio independiente.

2.7.4.5.4 Análisis de claves maestras

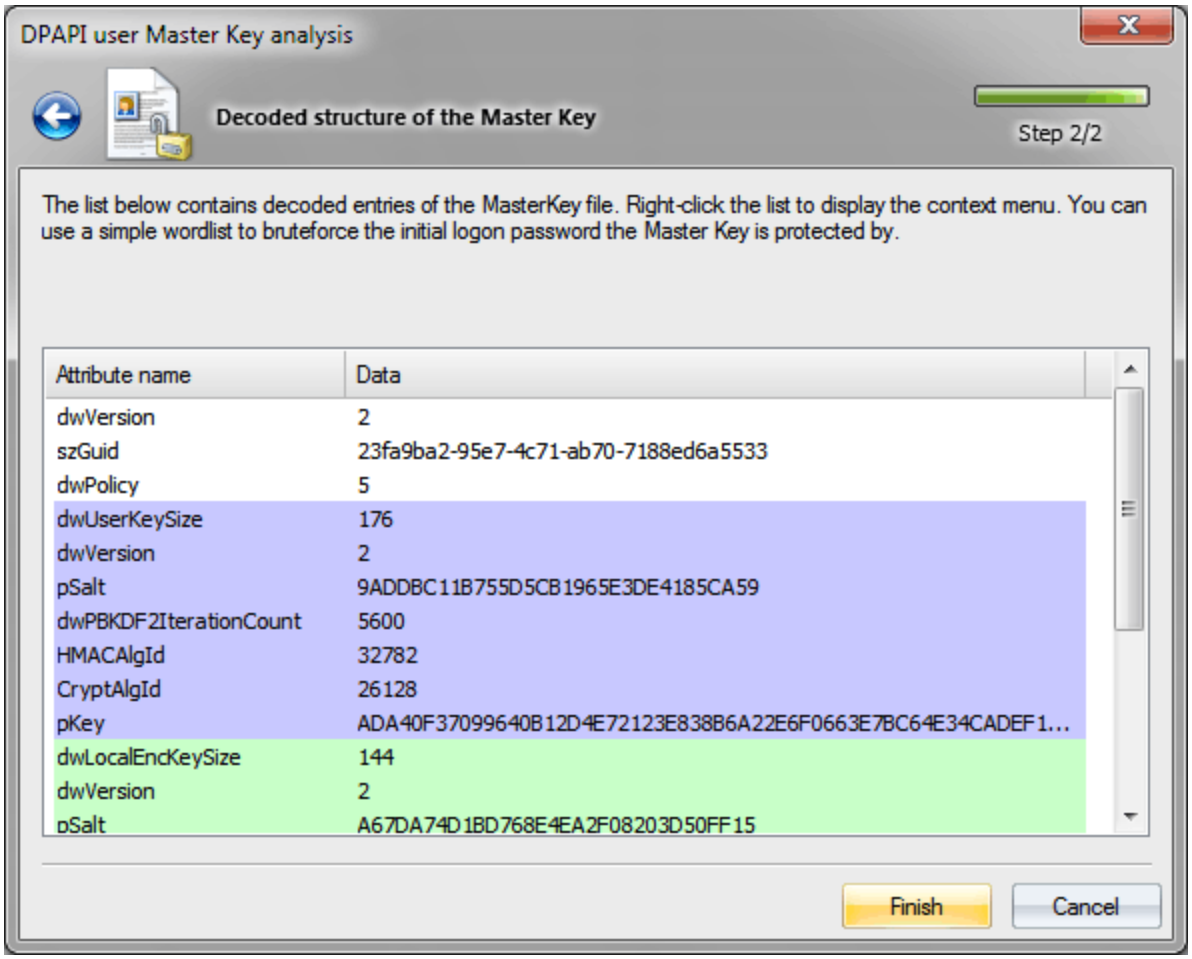
La clave maestra es 64 bytes de datos, que se utilizan como clave principal al descifrar un blob DPAPI. La clave maestra de un usuario se cifra con la contraseña de inicio de sesión del usuario.

Establezca la ruta al archivo de clave maestra y especifique el SID del usuario, que el programa normalmente calcula automáticamente a partir de la ruta especificada



Todas las claves maestras de ese usuario se encuentran en **%APPDATA%\Microsoft\Protect\%SID%**. Por ejemplo,
C:\Users\John\AppData\Roaming\Microsoft\Protect\S-1-5-21-2897849034-3956381361-16091305341-1001\23ab9bc1-9397-4cb1-ab74-7166ed6a8713
Las claves maestras del sistema se almacenan en la carpeta **%SYSTEMDIR%\Microsoft\Protect**.

Análisis de la clave maestra



El archivo de clave maestra es una estructura binaria, que consta de un encabezado de servicio y cuatro ranuras, a saber:
la clave maestra del usuario real, la clave de cifrado local (para desproteger la clave de copia de seguridad local), la clave de copia de seguridad local (en Windows 2000) o el GUID CREDHIST (en Windows XP y versiones posteriores) y la clave de copia de seguridad del dominio.

La lista de estructuras de clave maestra consta de nombres de atributos (es decir, campos binarios) y valores que se corresponden con ellos. Cada sección tiene un color único:

- campo con atributos de encabezado
- ranura con el atributo Clave maestra de los usuarios
- ranura con atributos de clave de cifrado local
- ranura con clave de copia de seguridad local o atributo GUID del archivo CREDHIST
- ranura con atributos de clave de copia de seguridad de dominio

Ahora, un poco más de detalle.

Atributos de encabezado

- **dwVersion** - Versión del archivo de clave maestra.
- **szGuid** - GUID textual de clave maestra. Normalmente coincide con el nombre del archivo.
- **dwPolicy** - varias banderas. Por ejemplo, si se establece el bit 3, el programa utiliza el hash de contraseña SHA1 al descifrar la contraseña del usuario; de lo contrario, utiliza MD4. Así, en Windows 2000 este bit siempre se borra. Un bit 2 establecido nos dice que se requiere una copia de seguridad para la clave maestra.

Atributos de la clave maestra del usuario

- **dwUserKeySize** - longitud de ranura actual.
- **dwVersion** - versión de la estructura de datos. La versión 1 implementa solo el atributo con sal.
- **pSalt** - pSalt - salt, es decir, 16 bytes aleatorios de datos, involucrados en el descifrado de la clave maestra y la prevención de ataques de datos utilizando la tablas rainbow
- **dwPBKDF2IterationCount** - iteraciones en la función de generación de claves de cifrado PBKDF2
- **HMACAlgId** - identificador de algoritmo hash.
- **CryptAlgId** - algoritmo de cifrado utilizado.
- **pKey** - Clave maestra cifrada del usuario.

Atributos de clave de cifrado local

- **dwLocalEncKeySize** - longitud de ranura actual.
- **dwVersion** - versión de la estructura de datos. Win2K utiliza solo un atributo con sal.
- **pSalt** - sal.
- **dwPBKDF2IterationCount** - iteraciones en la función de generación de claves de cifrado PBKDF2.
- **HMACAlgId** - identificador de algoritmo hash.
- **CryptAlgId** - algoritmo de cifrado utilizado.
- **pKey** - clave de cifrado local cifrada, utilizada para descifrar la clave de copia de seguridad local en Windows 2000.

Atributos de clave de copia de seguridad local (Windows 2000)

- **dwLocalKeySize** - longitud de ranura actual.
- **dwVersion** - versión de la estructura de datos.
- **pSalt** - sal.
- **pKey** - Clave de copia de seguridad local cifrada.

Atributos GUID del archivo CREDHIST (Windows XP y versiones superiores)

- **dwLocalKeySize** - longitud de ranura actual.
- **dwVersion** - versión de la estructura de datos.
- **guidCredHist** - Identificador binario del archivo CREDHIST.

Atributos de la clave de copia de seguridad del dominio

- **dwDomainKeySize** - longitud de ranura actual.
- **dwVersion** - versión de la estructura de datos.
- **pSalt** - 16 bytes aleatorios de datos, involucrados en el descifrado de la Clave Maestra y la prevención de hackeos de datos utilizando tablas de arco iris.
- **dwPBKDF2IterationCount** - iteraciones en la función de generación de claves de cifrado PBKDF2.
- **HMACAlgId** - identificador de algoritmo hash.
- **CryptAlgId** - algoritmo de cifrado utilizado.
- **pKey** - Clave de copia de seguridad de dominio cifrada. Su descifrado requiere la clave privada RSA del controlador de dominio, almacenada en la base de datos de Active Directory.

Para descifrar la clave maestra del usuario, debe conocer esa contraseña de inicio de sesión del usuario. Desde el menú contextual, puede verificar la contraseña de esa clave maestra e incluso intentar adivinar una usando un diccionario. Sin embargo, no te halagar demasiado. Mientras que en Windows 2000 la velocidad de búsqueda oscila en decenas e incluso cientos de miles de contraseñas por segundo, en Windows 7 el recuento va por elementos individuales. Consulte la tabla a continuación (la velocidad se mide para un solo núcleo de CPU Intel Q8400 2.66GHz).

Sistema operativo	Algoritmo de cifrado	Función hash	Rondas PKCS#5 PBKDF2	Velocidad de comprobación de contraseña (p/s)
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	AES256	SHA512	8000	**<10**

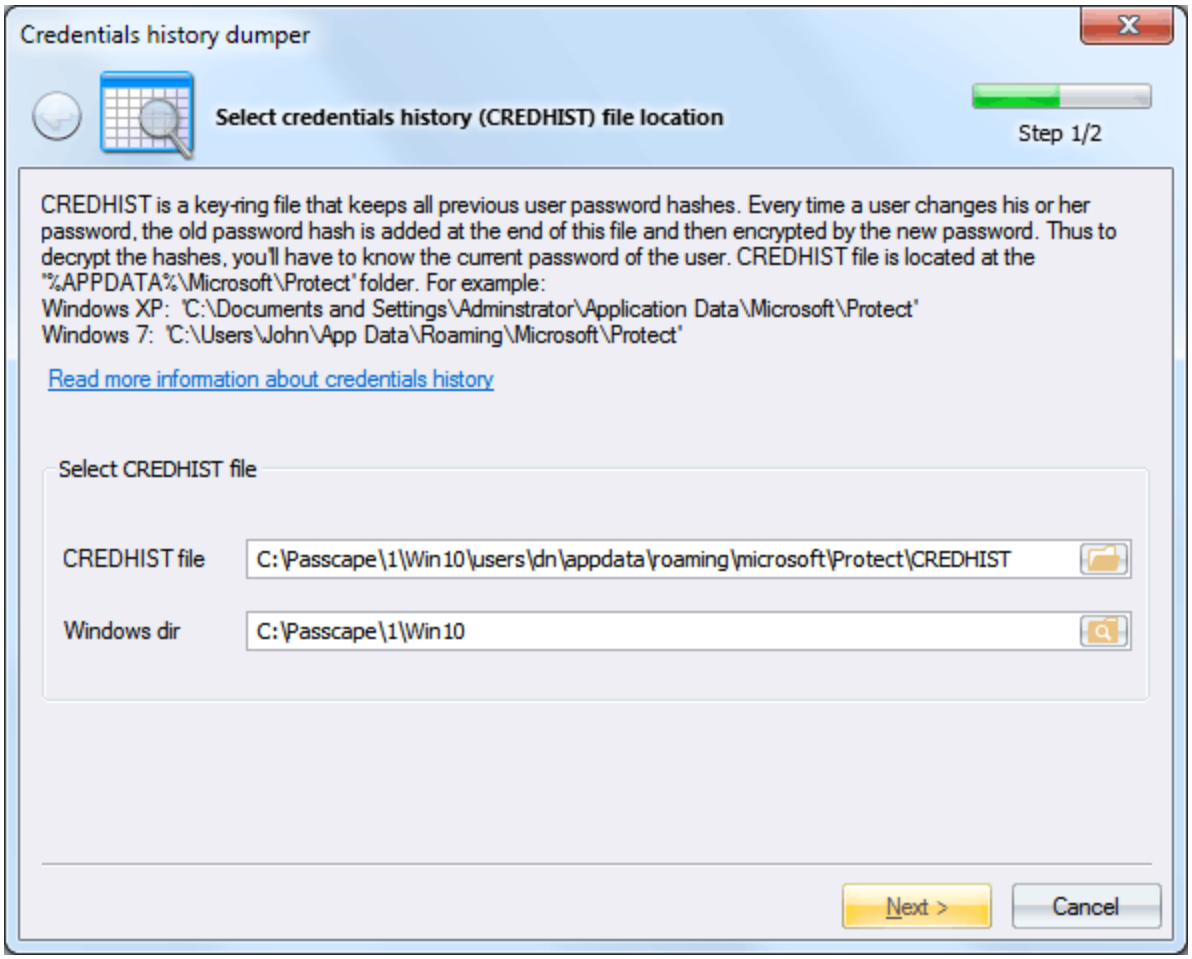
2.7.4.5.5 Volcar hashes del historial de credenciales de usuario

Debido a las peculiaridades de la implementación de DPAPI, para garantizar el descifrado exitoso de todos los blobs de DPAPI, Windows debe almacenar todas las contraseñas anteriores del usuario en el sistema. El historial de contraseñas del usuario se encuentra en el siguiente archivo:
%APPDATA%\Microsoft\Protect\credhist

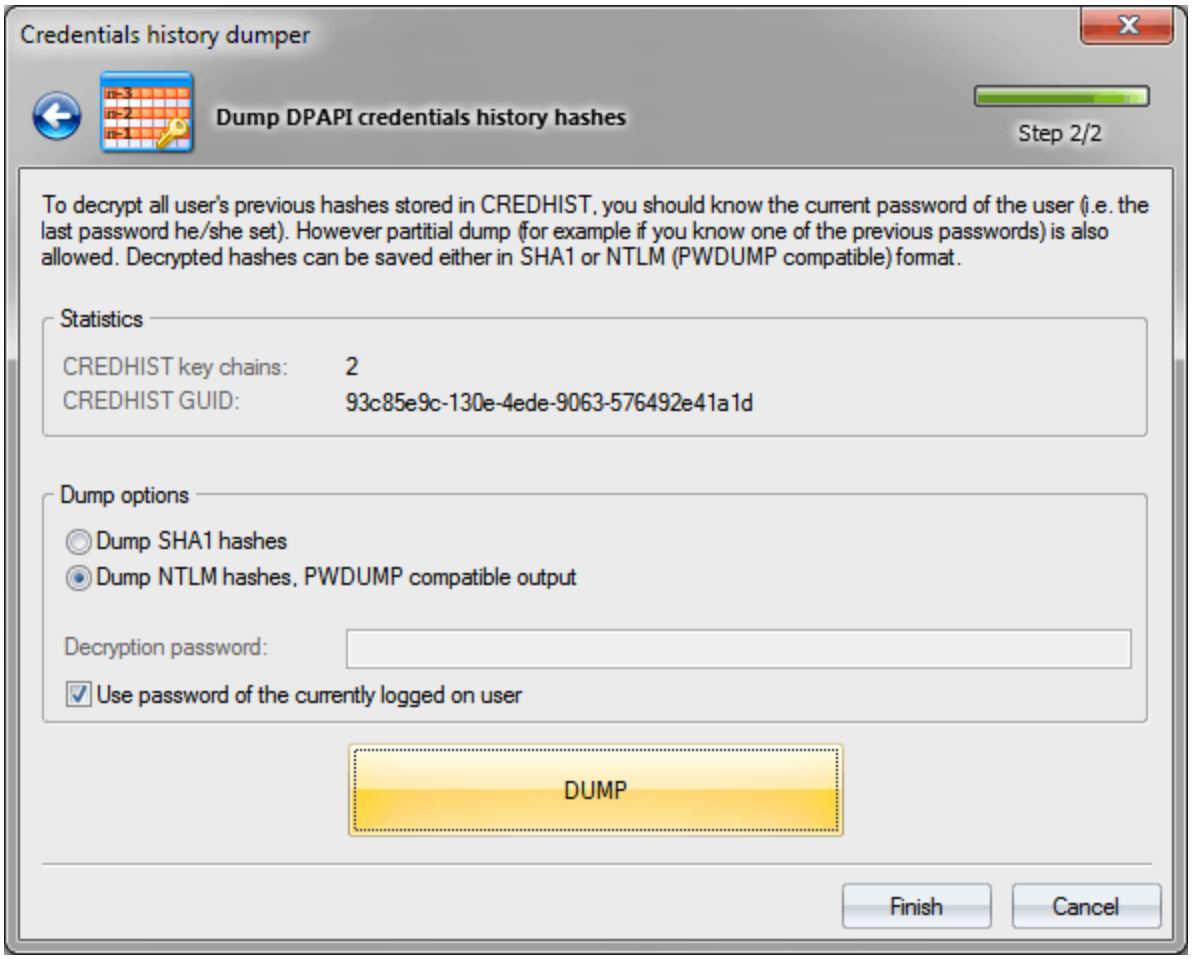
Todas las contraseñas antiguas del usuario (junto con ciertos datos de servicio) se almacenan como pares de hashes: **SHA1** y **NTLM**. Además, para descifrar el último par, debe conocer el hash de la contraseña actual del usuario, para descifrar los hashes anteriores, necesita el último par descifrado, etc., a lo largo de la línea.

Windows Password Recovery es la primera utilidad del mundo, que permite descifrar hashes de historial de contraseñas de archivos CREDHIST.

Para ello, en el primer paso del asistente de la aplicación, especifique la ruta de acceso al archivo CREDHIST y al directorio de Windows.



Luego puede descifrar y guardar hashes de CREDHIST en un archivo textual similar a PWDUMP, si guardar como **NTLM** es seleccionado, o a un archivo de texto sin formato, si el formato de hash **SHA1** se selecciona.



Es importante saber que para descifrar hashes CREDHIST debe conocer la contraseña actual del usuario. Si está descifrando CREDHIST de un usuario que ha iniciado sesión actualmente, asegúrese de establecer la opción respectiva. En este caso, no tendrá que ingresar la contraseña de descifrado, se recuperará de la caché del sistema.

El programa admite el volcado parcial de hashes de historial. Eso significa que si se desconoce la contraseña actual del usuario, pero al menos una de las contraseñas más antiguas está disponible, el programa puede descifrar las contraseñas que el usuario usó anteriormente, es decir, antes de que se ingresara esa contraseña antigua.

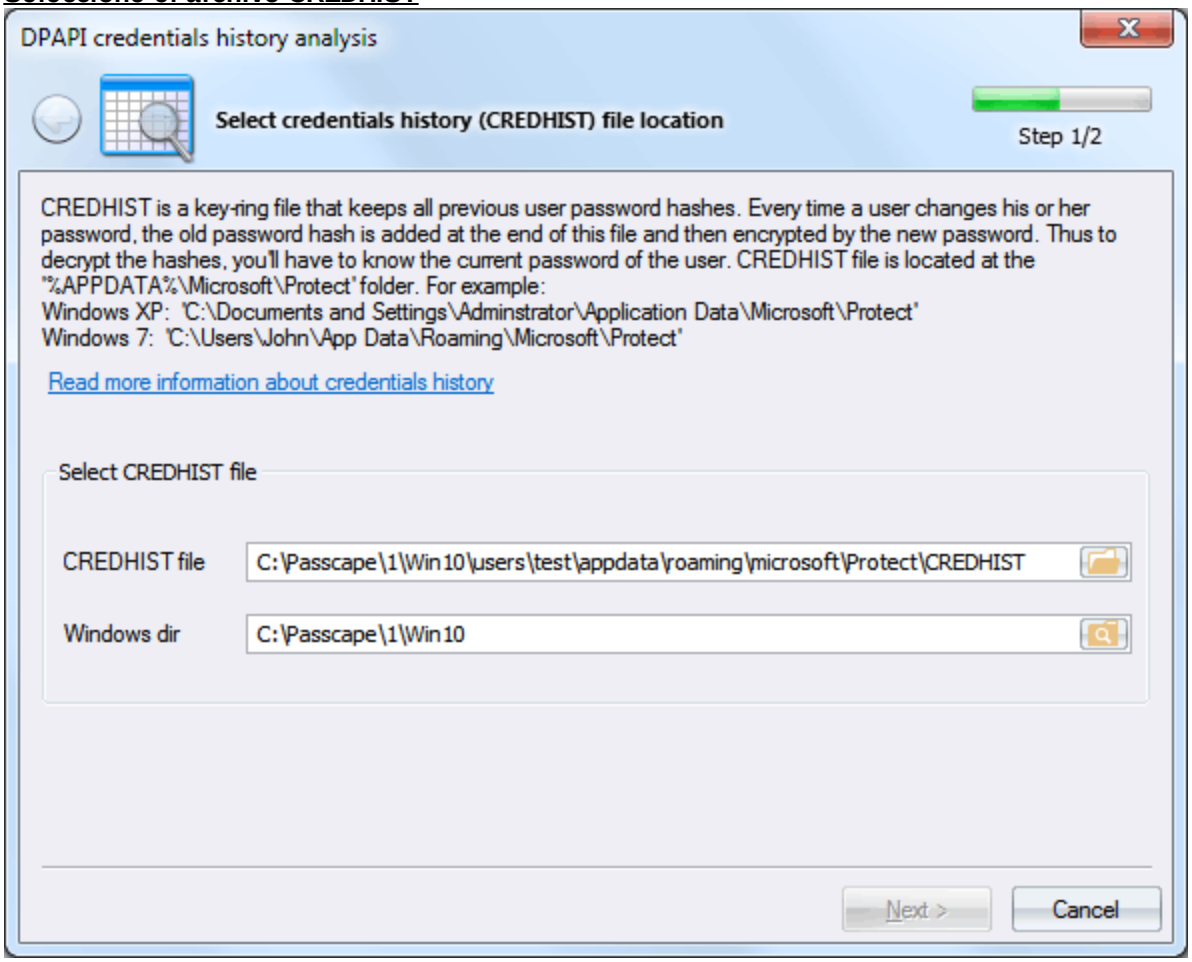
Tenga en cuenta que en los sistemas operativos Windows 8 y versiones posteriores, los hashes volcados para las cuentas de LiveID no corresponden a los derivados de las contraseñas de inicio de sesión de LiveID.

2.7.4.5.6 Analizar el historial de credenciales

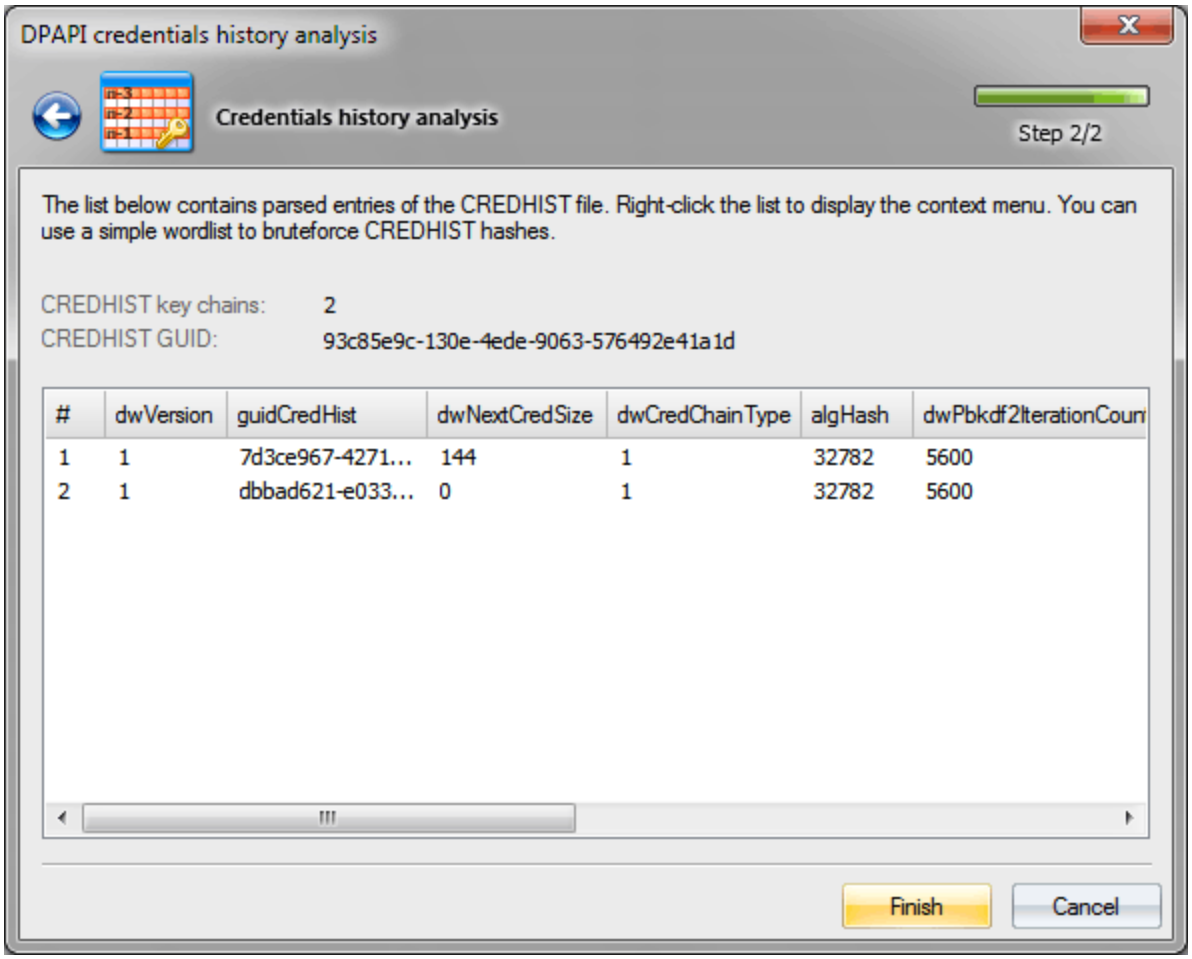
CREDHIST es un archivo de historial de contraseñas, hecho como una cadena, donde cada enlace representa los hashes de contraseña más antiguos del usuario. Cada vez que el usuario cambia la contraseña, el hash de contraseña anterior se anexa al archivo y se cifra con una nueva contraseña. Por lo tanto, para descifrar todos los hashes de una cadena, debe conocer la contraseña actual del usuario.

Junto con los hashes, las cadenas almacenan otros datos de servicio, que también son analizados por esta utilidad.

Seleccione el archivo CREDHIST



Y proceder al análisis de su contenido



En la captura de pantalla, puede ver que el identificador CREDHIST es 93c85e9c-130e-4ede-9063-576492e41a1d. Este es el identificador (GUID) al que se adjuntan todas las claves maestras del usuario en el contexto del propietario de los datos. El número de enlaces en la cadena hash es 2.

La siguiente lista contiene todos los atributos y sus valores para cada enlace de nuestro CREDHIST.

Descripción del atributo

- **dwVersion** - versión de la estructura de datos
- **guidLink** - identificador único de enlace actual
- **dwNextLinkSize** - tamaño del siguiente enlace
- **dwLinkType** - tipo de vínculo
- **algHash** - algoritmo hash utilizado al descifrar el vínculo
- **dwPbkdf2IterationCount** - iteraciones en la rutina de generación de claves PKCS#5 PBKDF2
- **dwSidSize** - tamaño del descriptor de seguridad (SID) del propietario
- **algCrypt** - algoritmo de cifrado
- **dwShaHashSize** - Tamaño de hash SHA1
- **dwNtHashSize** - Tamaño de hash NTLM
- **pSalt** - sal utilizada en el cifrado
- **sidUser** - SID del propietario de los datos
- **pShaHash** - Hash SHA1
- **pNtHash** - Hash NTLM

Para adivinar la contraseña original de CREDHIST, haga clic derecho en los atributos y luego seleccione 'Usar lista de palabras para verificar la contraseña ...' en el menú contextual que aparece. Puede validar la contraseña tanto para los registros seleccionados actualmente como para todos los registros. El tiempo de validación aumenta proporcionalmente al número de registros (es decir, enlaces).

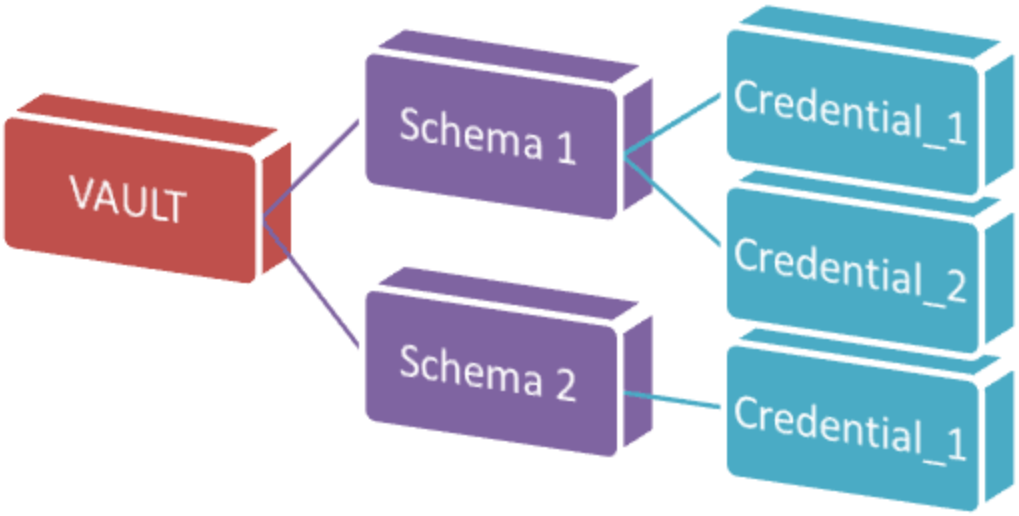
Consulte la tabla comparativa de velocidad de búsqueda de contraseñas CREDHIST original. La velocidad se mide para un solo núcleo de CPU Intel Q8400 2.66GHz para configuraciones predeterminadas del sistema operativo (por ejemplo, en Windows 7 el número de iteraciones en PBKDF2 puede diferir).

Sistema operativo	Algoritmo de cifrado	Función hash	Contador PBKDF2	Velocidad de comprobación de contraseña (p/s)
Windows XP	3DES	SHA1	4000	**76**
Windows Vista	3DES	SHA1	24000	**12**
Windows 7	AES256	SHA512	5600	**10**
Windows 10	AES256	SHA512	8000	**<10**

2.7.4.6 Explorador del Almacén de Windows

Que es el Almacén de Windows

Almacén de Windows es un almacenamiento protegido para secretos de usuario o del sistema, contraseñas, claves de red, contraseña web y otra información personal. Los datos almacenados en el Almacén de Windows están estructurados y representan un conjunto de registros que pertenecen a un determinado esquema del Almacén (véase la imagen siguiente).



En el nivel físico, Almacén es una carpeta basada en disco con un conjunto de los siguientes archivos:
Policy.vpol - conjunto de claves de cifrado para registros de Almacén (credenciales). Estas claves se pueden proteger mediante dos métodos básicos: DPAPI o mediante una contraseña de usuario específica. Este último método de protección no se utiliza en Windows 8 y actualmente no es compatible con el software.

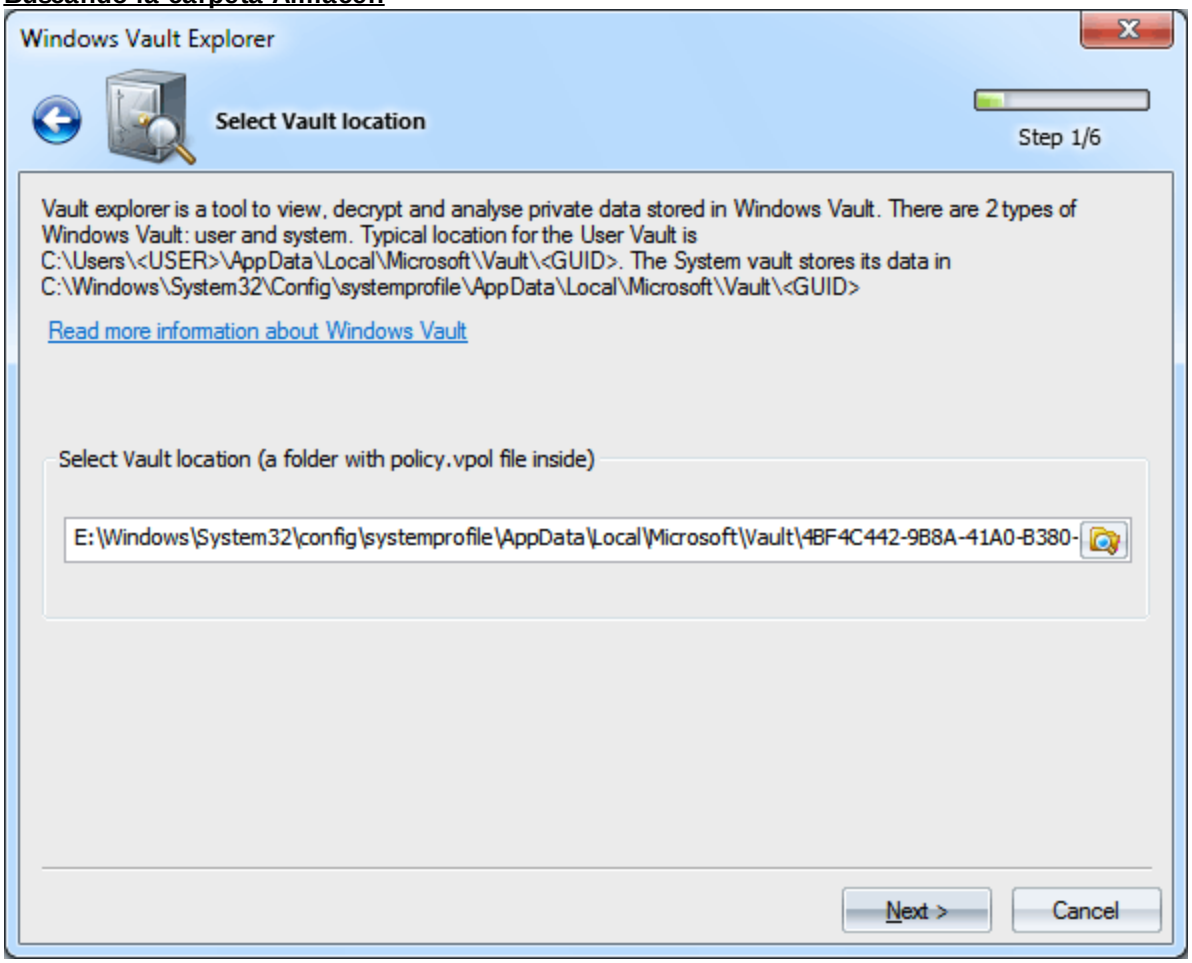
<GUID>.vsch - Esquema de bóveda que contiene descripción de datos, indicadores y otra información del sistema.
<GUID>.vcrd - Credencial de almacén que almacena los datos cifrados originales asociados a un determinado esquema. Los datos pueden consistir y normalmente constan de varios campos. La descripción de los campos se almacena en <GUID>.vsch.

Explorador del Almacén de Windows

El Explorador de Windows Almacén es una utilidad para analizar y descifrar sin conexión las credenciales de Almacén. El Asistente para descifrado divide todo el proceso en los siguientes pasos:

1. Buscando la carpeta Almacén
2. Buscando la clave maestra del usuario o del sistema
3. Configuración de archivos de registro y otra información necesaria para descifrar la clave maestra
4. Selección del esquema de Almacén
5. Búsqueda de registros de Almacén que pertenezcan al esquema seleccionado
6. Descifrar la credencial de Almacén seleccionada

Buscando la carpeta Almacén



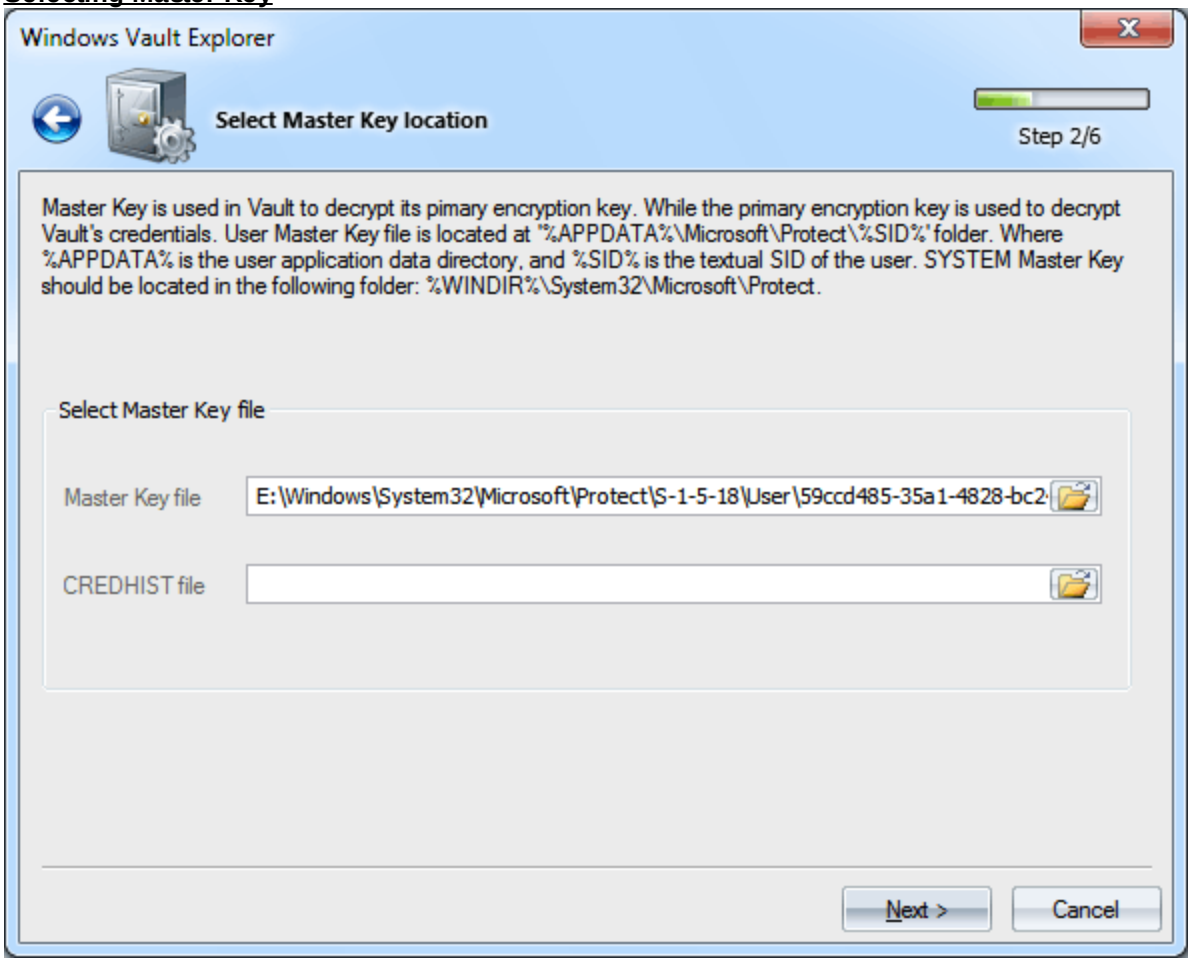
Actualmente hay dos tipos de almacenamiento en Almacén: sistema y usuario. El almacenamiento de Almacén del usuario se puede ubicar en las siguientes carpetas:
<USER_APP_DATA>\Microsoft\Vault\<GUID>
<USER_LOCAL_APP_DATA>\Microsoft\Vault\<GUID>

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

La ubicación predeterminada del almacenamiento de Almacén del sistema es:
<SYSTEM_APP_DATA>\Microsoft\Vault\<GUID>
<SYSTEM_LOCAL_APP_DATA>\Microsoft\Vault\<GUID>
<PROGRAM_DATA>\Microsoft\Vault\<GUID>
Por ejemplo,
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

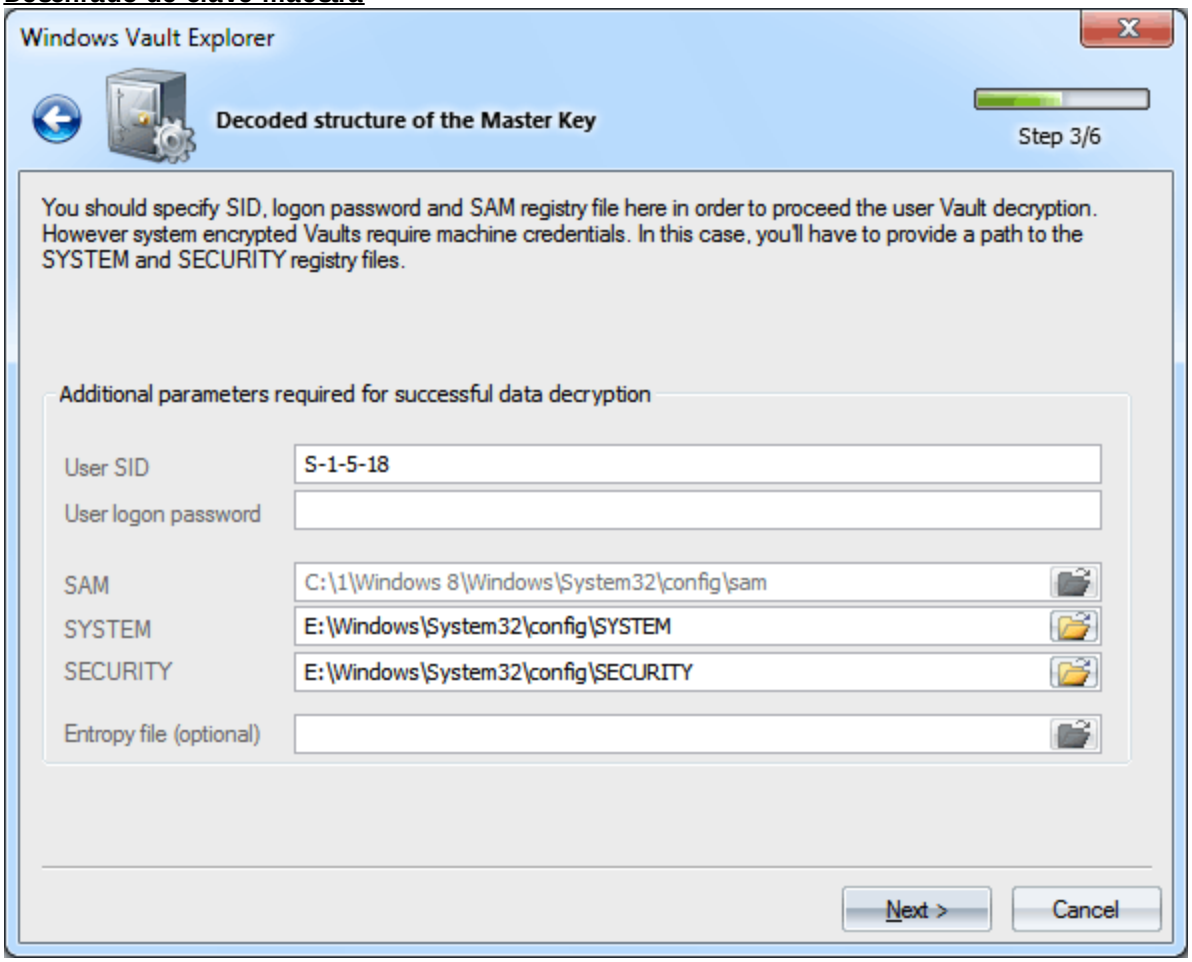
Tenga en cuenta que algunas de las carpetas especificadas tienen el atributo del sistema establecido, lo que hace que estas carpetas se oculten.
Windows tiene VaultCmd.exe utilidad para crear y administrar sus propios almacenamientos de Almacén.

Selecting Master Key



Una vez seleccionada una determinada carpeta de Almacén, debe especificar la ruta a la clave maestra utilizada en la protección de las claves de cifrado de Almacén. La clave maestra del usuario siempre reside en la carpeta **%APPDATA%\Microsoft\Protect\%SID%**, y las claves maestras de la cuenta del sistema se almacenan en **%SYSTEMDIR%\Microsoft\Protect**. Debe tenerse en cuenta que podría haber una serie de claves maestras, mientras que un objeto específico podría descifrarse utilizando solo una clave, cuyo nombre se almacena en el archivo Policy.vpol. Al buscar la clave maestra, el programa puede filtrar nombres innecesarios.

Descifrado de clave maestra

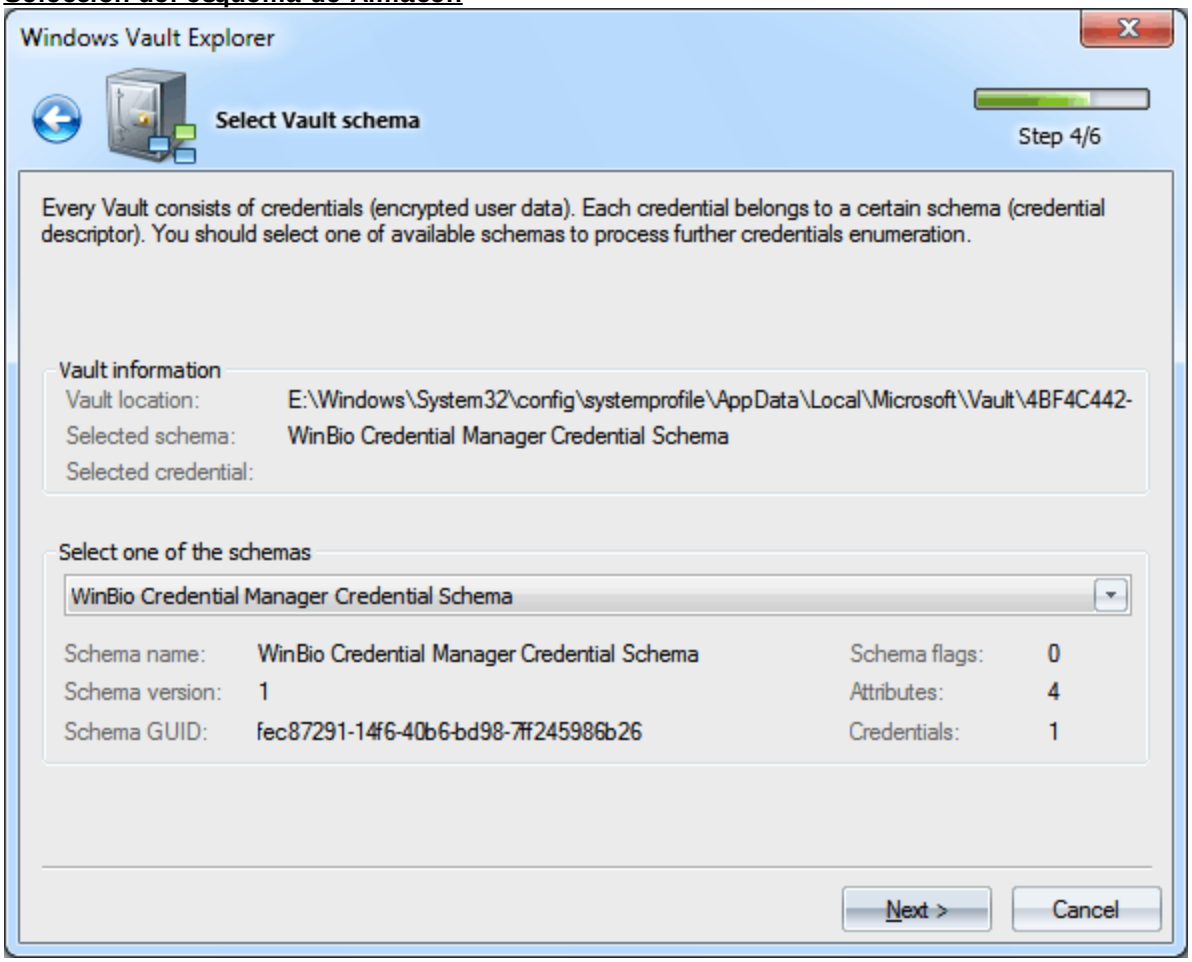


Para descifrar la clave maestra de un usuario, debe proporcionar al menos dos parámetros: la contraseña de inicio de sesión del usuario y su identificador de seguridad (SID), que normalmente se incluye en la ruta a la clave maestra. El programa encuentra el SID del usuario automáticamente. Si eso no se ha hecho por alguna razón, configídalo manualmente. Para descifrar la clave maestra del sistema, no necesitamos especificar la contraseña; el programa extraerá toda la información necesaria de los dos archivos de registro: **SYSTEM** y **SECURITY**.

En algunos casos, el descifrado de la clave maestra requiere especificar la ruta de acceso al archivo de registro **SAM**. Ese es el caso solo cuando la cuenta del propietario de los datos en Windows 8 tiene el tipo **LiveID**.

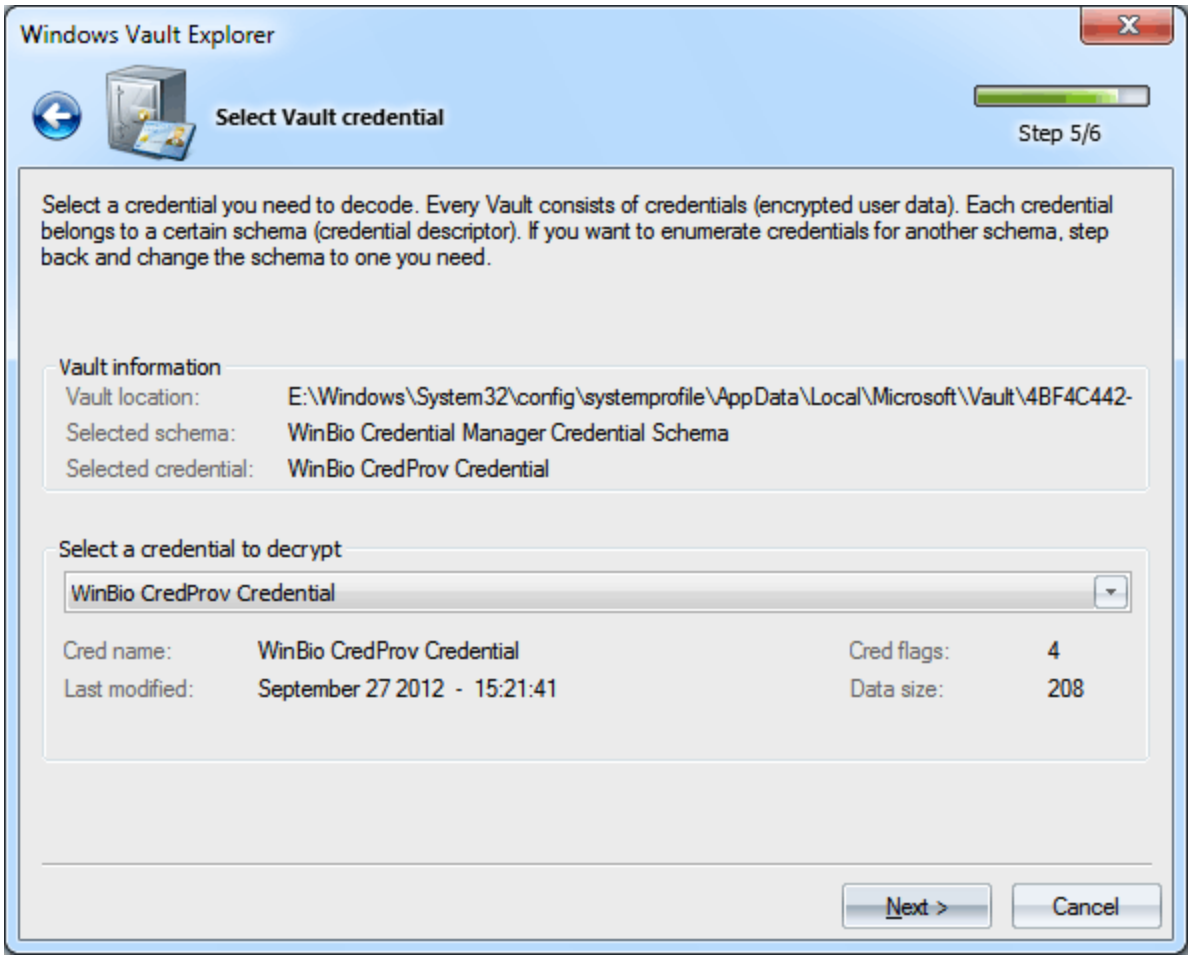
Windows Password Recovery a partir de la versión 9.7 utiliza algunas vulnerabilidades en el cifrado de clave maestra DPAPI. Por lo tanto, para descifrar CUALQUIER entrada de Almacén de un usuario de dominio, la contraseña de inicio de sesión del propietario ya no es necesaria.
WPR v11.7 soporta la característica Inicio de sesión automático de arranque de confianza de Windows 10. Si el programa detecta que el inicio de sesión automático de arranque de confianza está configurado para el usuario, no se requiere ninguna contraseña de inicio de sesión para descifrar los datos.

Selección del esquema de Almacén



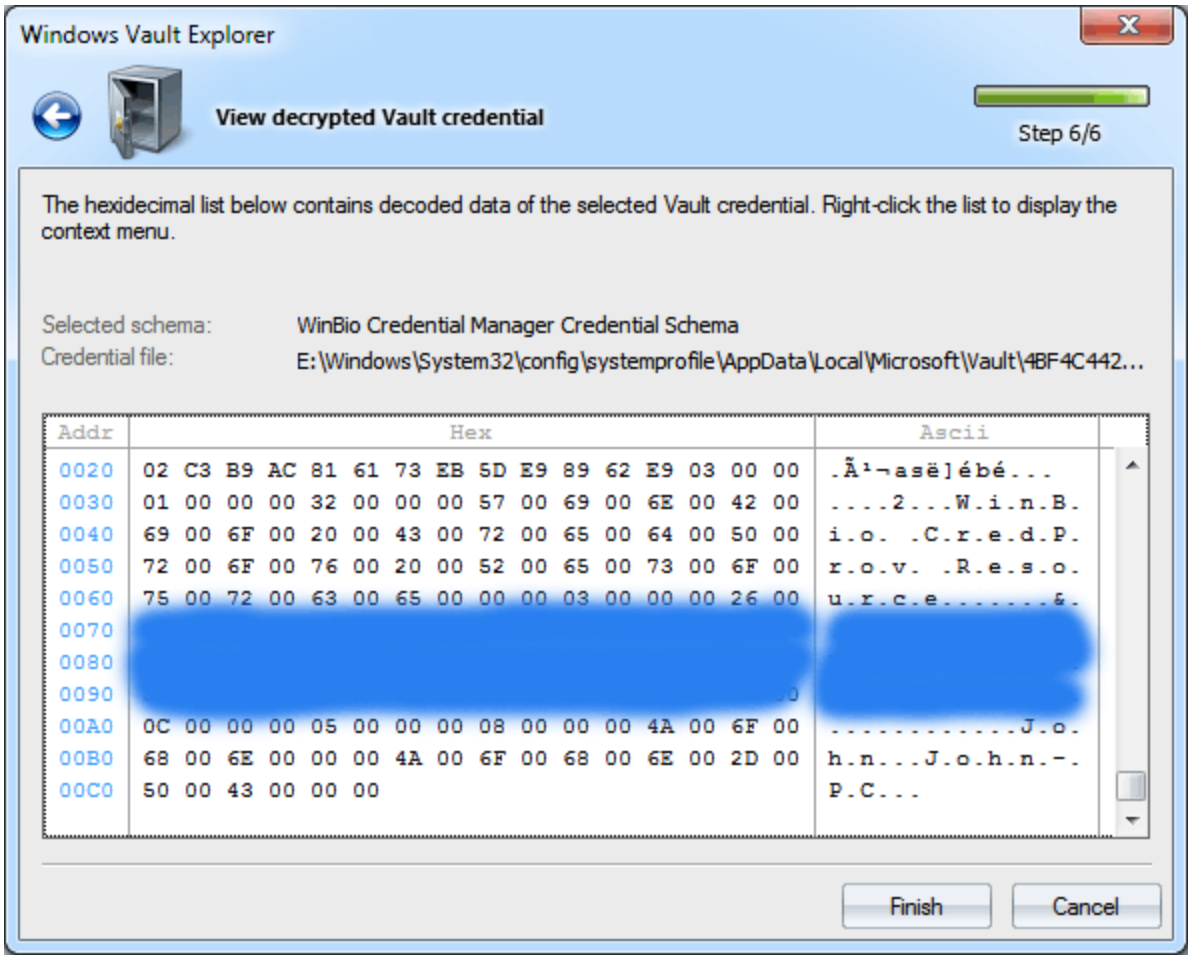
En el cuarto paso, si los anteriores pasaron con éxito, el programa le pedirá que seleccione uno de los esquemas que pertenecen a nuestra Bóveda de la lista desplegable. Justo debajo de la lista, podemos ver las características generales del esquema seleccionado: su nombre, versión, GUID, banderas, número de atributos y credenciales.

Selección de la credencial de Almacén



De manera similar, seleccionamos una de las credenciales de interés que pertenezca al esquema que hemos seleccionado durante el paso anterior.

Descifrado de credenciales de Almacén



Y por último el paso final, donde puede ver el registro descifrado, copiarlo en el portapapeles o guardarlo en un archivo para su posterior análisis. La figura muestra la contraseña de texto sin formato descifrada (está obstruida) de la cuenta de administrador configurada para iniciar sesión utilizando información biométrica (huella digital).

2.7.4.7 Explorador de Windows Hello

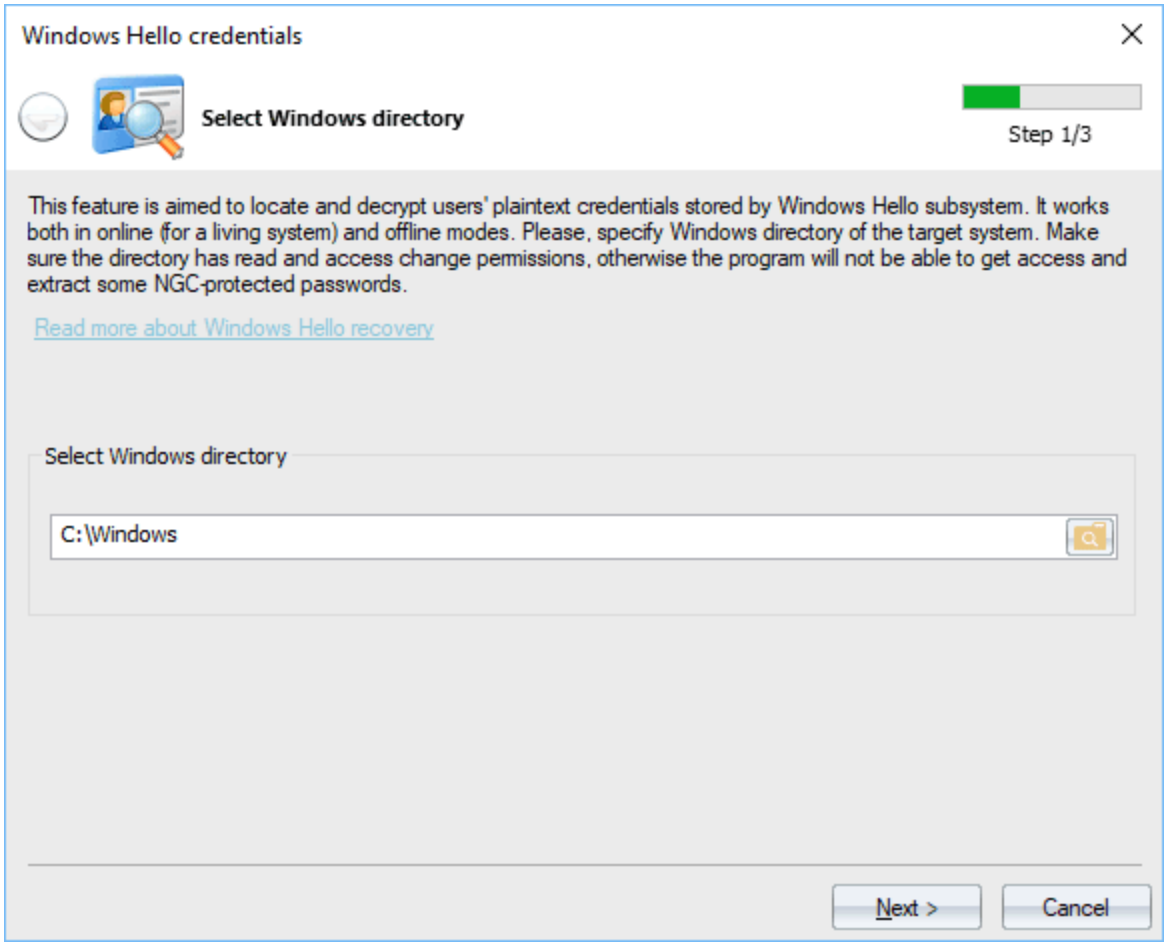
Windows Hello es una nueva tecnología biométrica que permite a los usuarios autenticarse en sus dispositivos Windows 10 con solo una huella digital, escaneo de iris, reconocimiento facial o de voz. Se supone que Windows Hello es más fácil de usar y seguro que usar una contraseña.

Windows Password Recovery tiene un conjunto de utilidades para analizar el sistema de seguridad de Windows Hello. Este kit incluye tres características para Extraer contraseñas de texto sin formato guardadas por el sistema Windows Hello, para descifrar identidades digitales (por ejemplo, huellas dactilares de los usuarios) almacenadas en bases de datos biométricas and Herramienta de recuperación de PIN.

2.7.4.7.1 Credenciales de Windows Hello

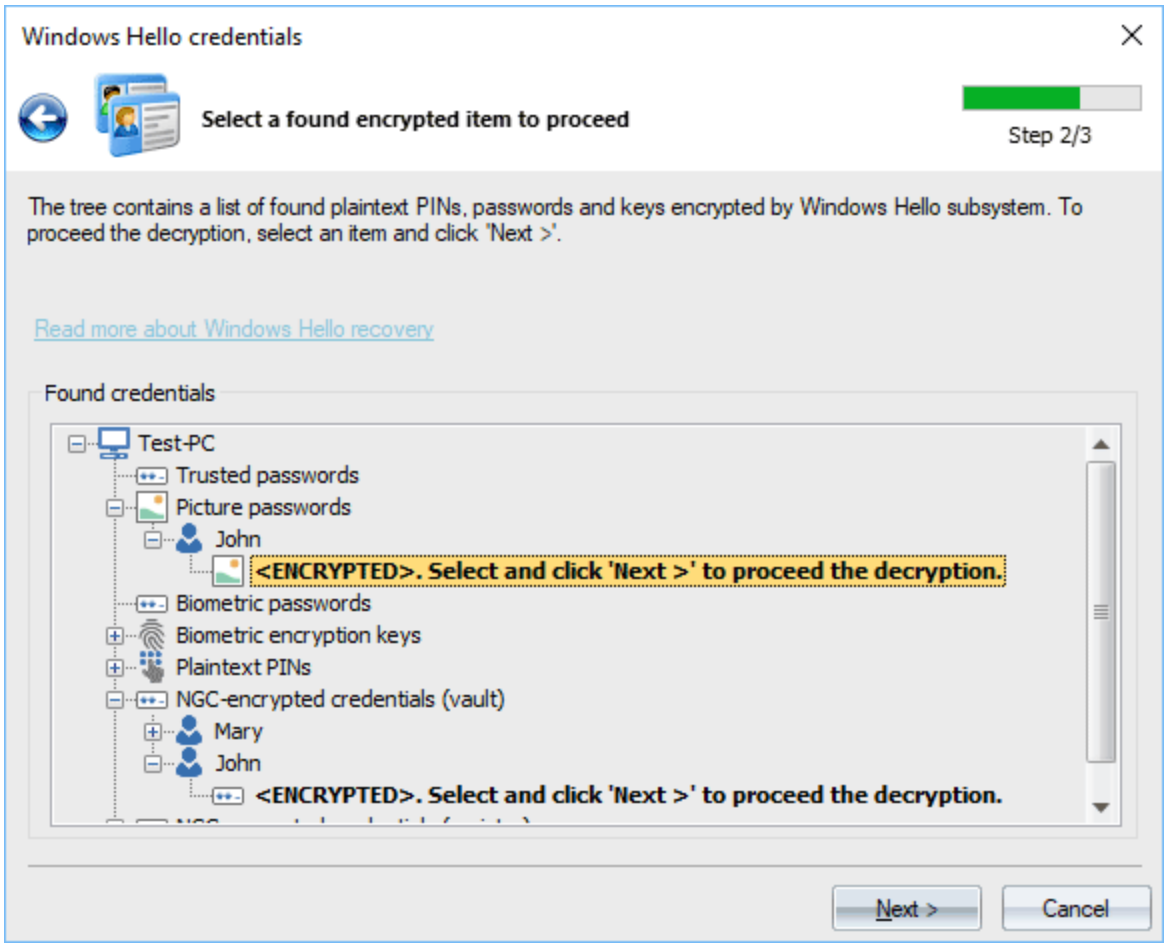
Esta característica tiene como objetivo localizar y descifrar las credenciales de texto sin formato almacenadas por Windows Hello. Windows hello usa la criptografía de próxima generación (NGC o también llamada CNG) para proteger y almacenar los datos privados del usuario y las claves de cifrado. A pesar de que NGC es un sistema muy elaborado y sofisticado (vale la pena mencionar que utiliza incluso algún truco indocumentado para proteger las claves de cifrado y los datos), el software Passcape fue el primero, al igual que en el caso de DPAPI, que lograron crear un conjunto casi idéntico de API pero con soporte para el modo sin conexión. Sí, la herramienta se puede utilizar tanto para un sistema vivo como para cualquier sistema operativo externo. Eso hace que sea fácil trabajar con el programa incluso para un novato, dejando todas las operaciones numerosas y rutinarias al programa..

1 Configuración de la carpeta Windows



El modo de trabajo se detecta automáticamente una vez que se configura un directorio de Windows. La carpeta de Windows contiene archivos y claves de cifrado protegidos para que no se pueda acceder incluso a ellos por parte de los administradores. Para extraer las claves, esta carpeta debe permitir el cambio de acceso o las operaciones de escritura de archivos. De lo contrario, el programa no podrá descifrar contraseñas cifradas con NGC.

2 Selección de datos para descifrar



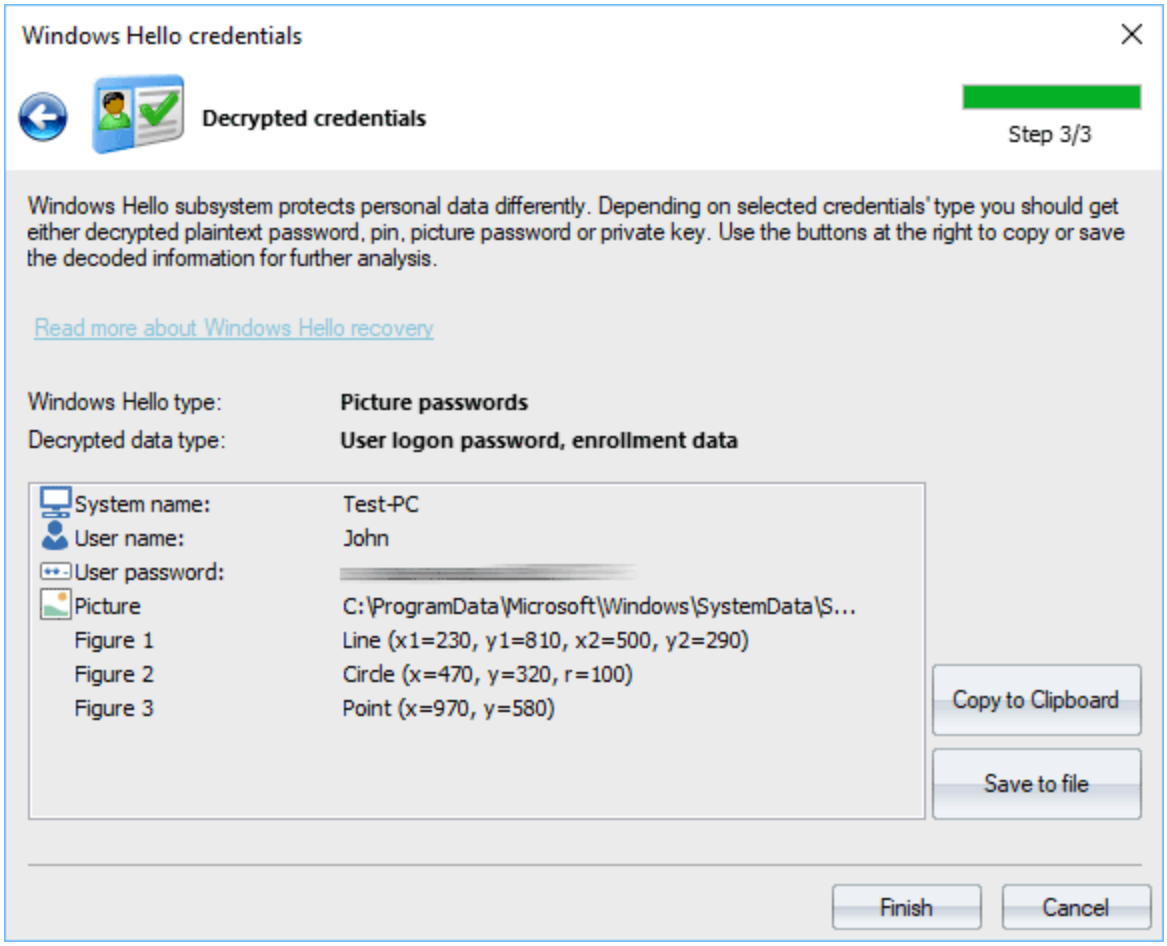
Durante este paso, el programa genera todas las credenciales, claves y PIN encontradas pero aún no descifradas. Definitivamente, Windows Hello fue desarrollado por varios equipos de desarrollo, porque se utilizan múltiples subsistemas de cifrado y todos los datos personales están dispersos por todo el sistema. Actualmente, el programa admite los siguientes tipos de datos:

- Contraseñas de imagen
- Contraseñas de texto sin formato de inicio de sesión protegidas con contraseñas de imagen
- Credenciales biométricas
- Contraseñas de texto sin formato de inicio de sesión protegidas con credenciales biométricas
- Claves de cifrado biométrico
- PIN de texto sin formato
- Historial de PIN (si esta opción está establecida en Windows)
- Contraseñas de texto sin formato de inicio de sesión, almacenadas en el Almacén de Windows y protegidas por NGC
- Contraseñas de texto plano de inicio de sesión, almacenadas en el registro de Windows y protegidas por NGC

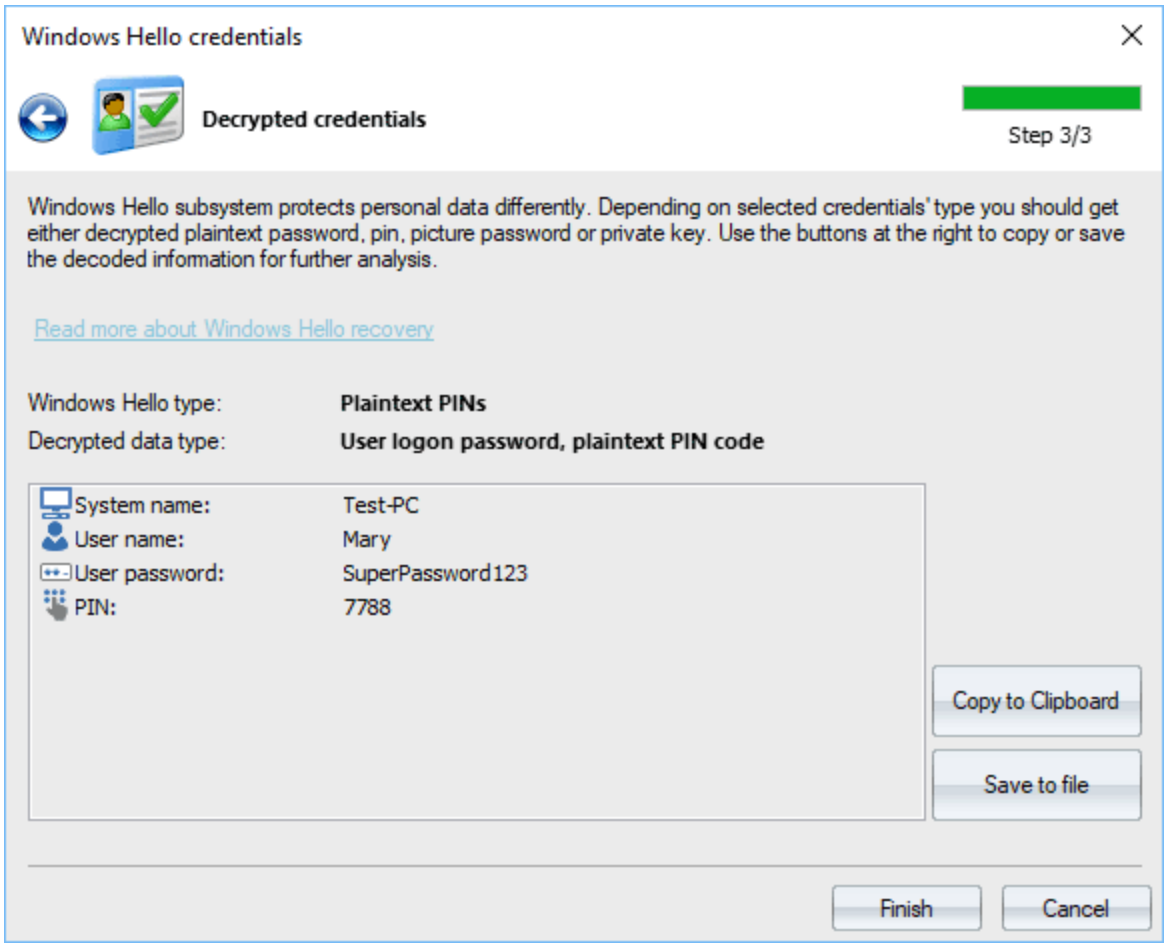
Para finalizar el descifrado, simplemente haga doble clic en un elemento en negrita.

3 Credenciales descifradas

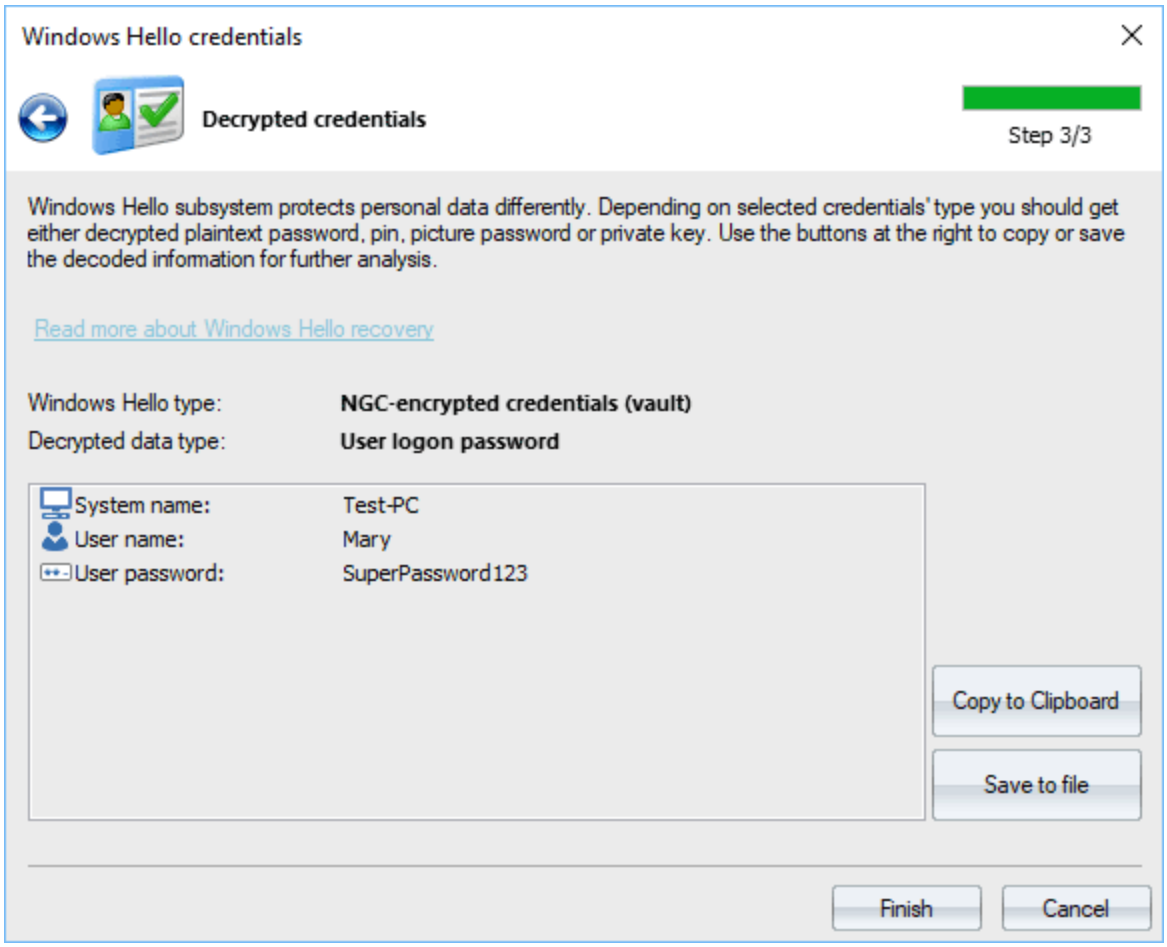
El sistema Windows Hello protege los datos personales de manera diferente. Dependiendo del tipo de credenciales seleccionadas, debe obtener una contraseña de texto sin formato descifrada, un pin, una contraseña de imagen o una clave privada. Utilice los botones de la derecha para copiar o guardar la información decodificada para su posterior análisis.



Contraseña de inicio de sesión descifrada (oculta aquí) y contraseña de imagen.



Contraseña de inicio de sesión y código PIN descifrados.

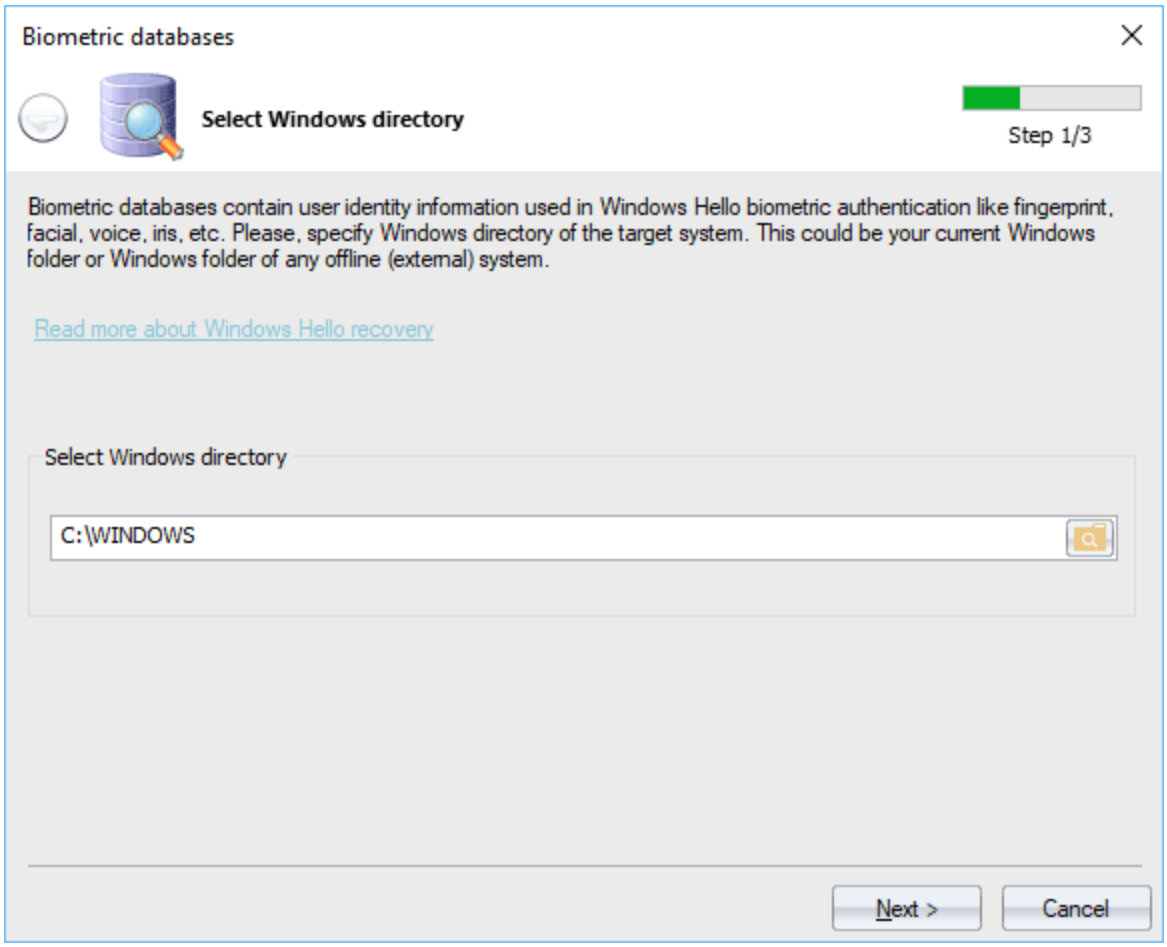


Contraseña de inicio de sesión descifrada para el usuario 'Mary'.

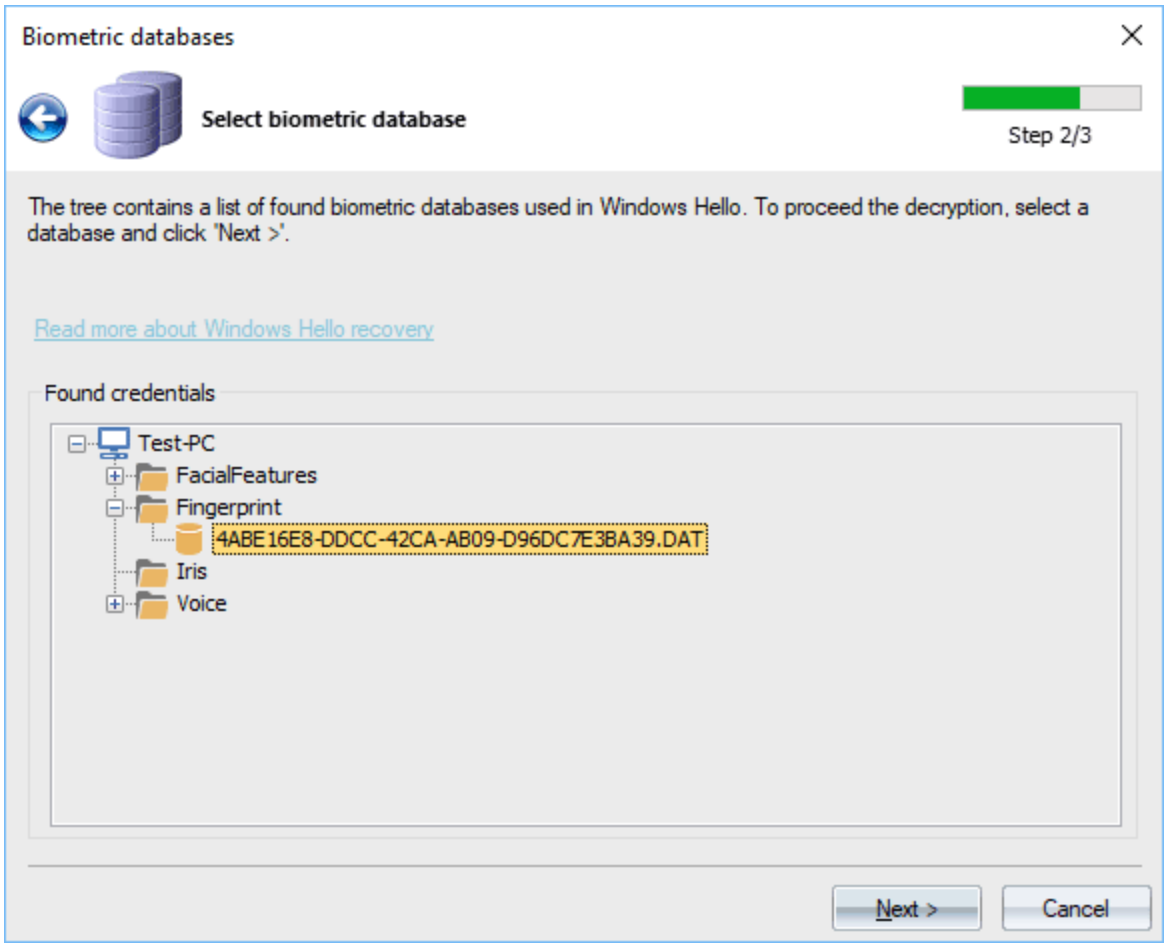
Tenga en cuenta que las contraseñas de texto sin formato protegidas con NGC se pueden descifrar utilizando una clave biométrica o un PIN. El programa primero intenta localizar y usar claves biométricas y si no lo hace (por ejemplo, el inicio de sesión biométrico no se ha configurado), WPR solicita el PIN para poder descifrar los datos.

2.7.4.7.2 Bases de datos biométricas

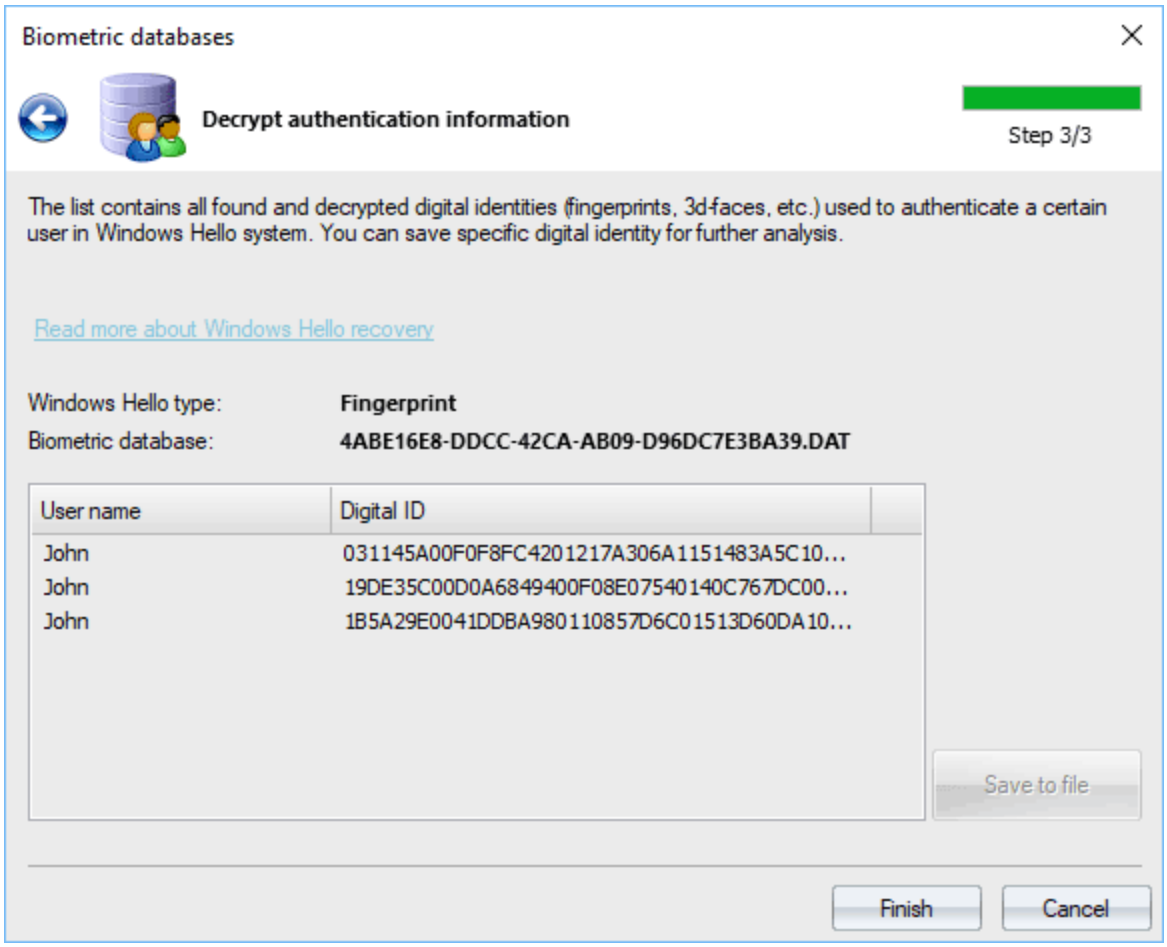
Las bases de datos biométricas contienen identidades digitales que se usan para autenticar a un determinado usuario en el sistema Windows Hello. Esas identidades son huellas dactilares, caras 3D, voz o iris.



Primero debe establecer el directorio de Windows del sistema de destino. Este podría ser el directorio de Windows de su sistema operativo actual o de cualquier sistema operativo externo.



Para descifrar una base de datos, simplemente haga doble clic en ella en la lista.



La base de datos descifrada contiene identidades digitales encontradas y descifradas, como fingerpints, caras 3D, etc. Por ejemplo, si un usuario ha establecido 3 huellas digitales para iniciar sesión en el sistema mediante Windows Hello, las huellas digitales deben descifrarse y generarse a la derecha del nombre del usuario. Al igual que en la imagen de arriba.

Puede guardar los datos digitales para su posterior análisis.

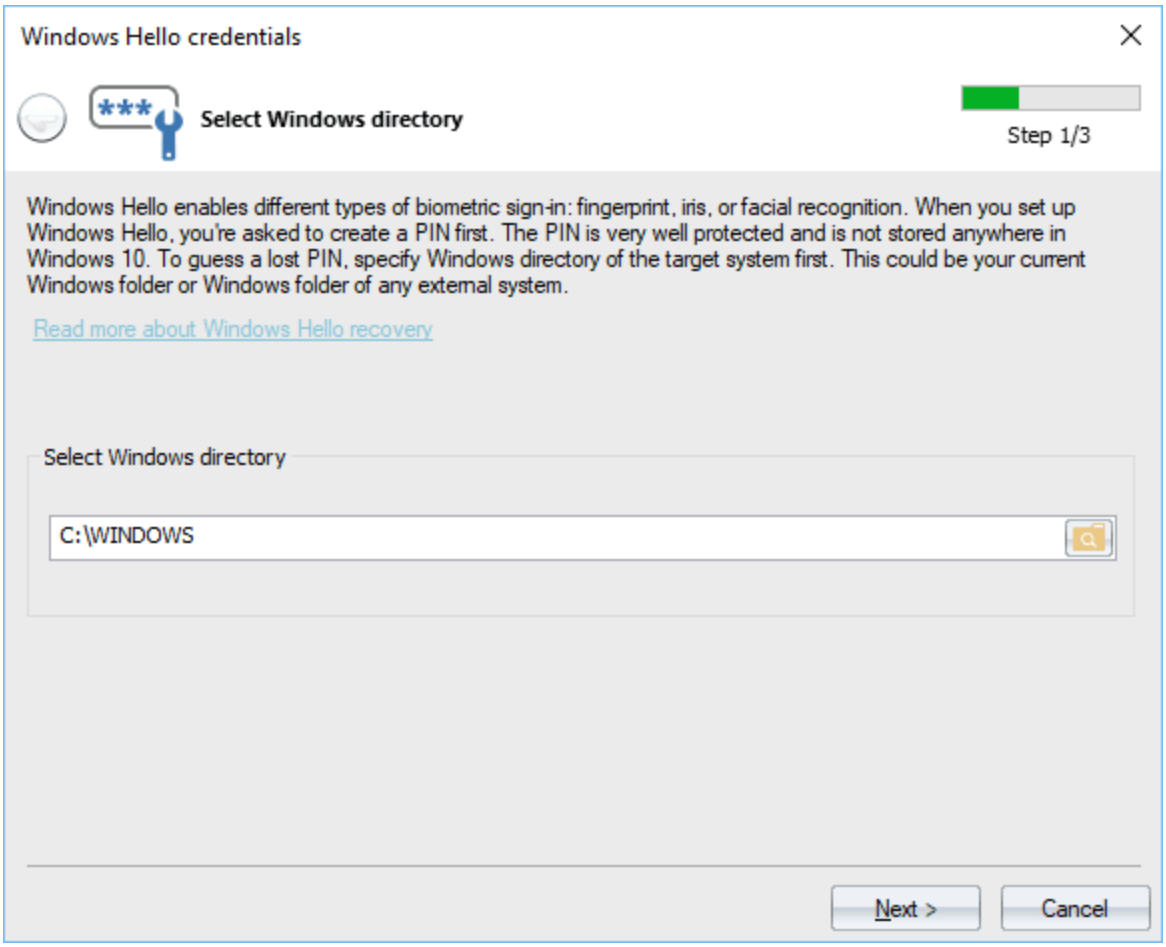
A pesar de la afirmación de Microsoft de extrema seguridad, los ID Digitales están mal protegidos contra la sustitución (a menos que se usen con dispositivos TPM) y se pueden migrar o copiar fácilmente de una PC a otra. Por ejemplo, puede crear su propia huella digital, copiarla en otra PC en otra cuenta de usuario. Luego, simplemente puede iniciar sesión en la cuenta externa usando su propia huella digital. Debido a la gravedad de esta vulnerabilidad que compromete toda la seguridad del sistema, la función de migración de identificadores digitales se deshabilitó en esta versión del programa.

2.7.4.7.3 PIN brute-forcer

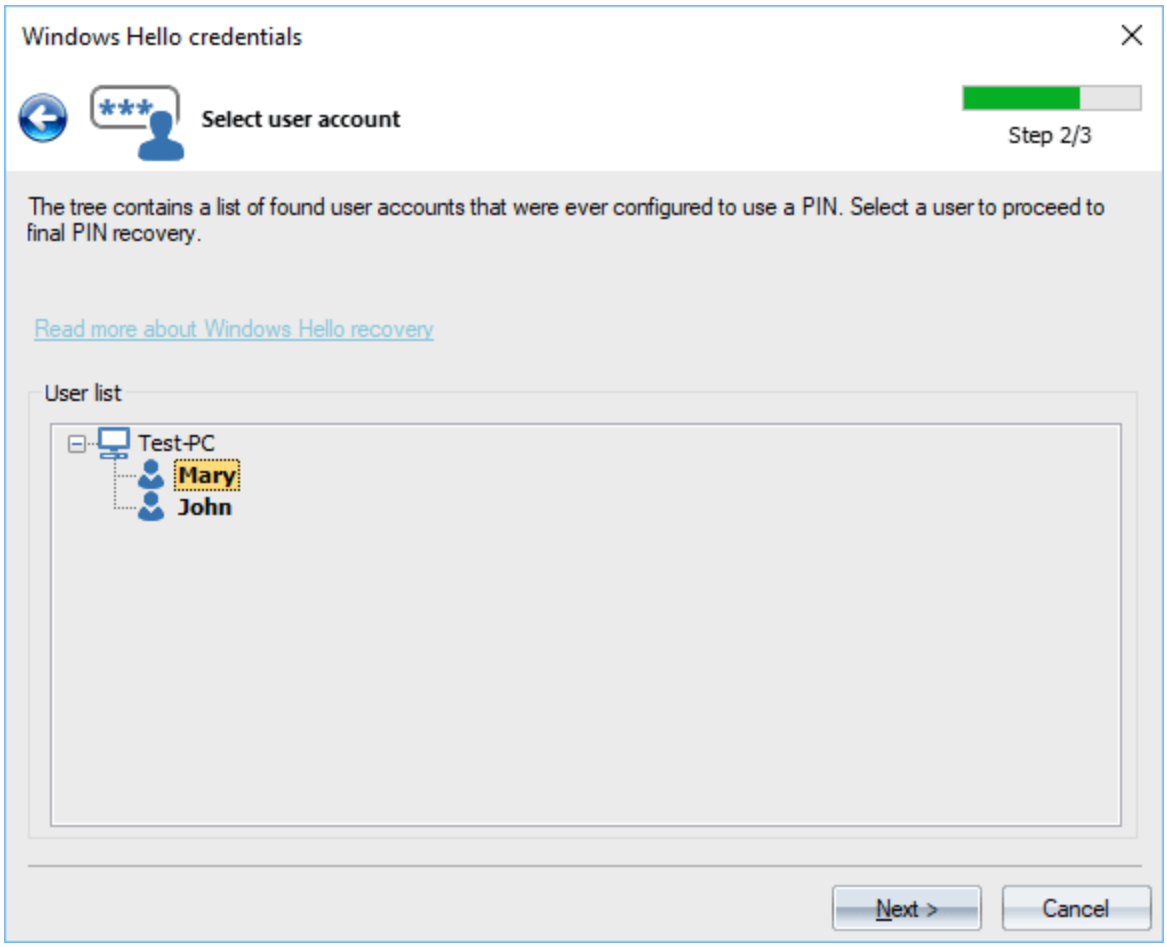
Windows Hello permite diferentes tipos de inicio de sesión biométrico: reconocimiento de huellas dactilares, iris, facial o de voz. Cuando configuras Windows Hello, primero se te pedirá que crees un PIN. El PIN está muy bien protegido y no se almacena en ningún lugar de Windows 10. Sin embargo, se puede descifrar fácilmente en Windows 8. Para adivinar un PIN perdido, primero debe especificar el

directorio de Windows del sistema de destino. Esta podría ser su carpeta actual de Windows o la carpeta de Windows de cualquier sistema externo.

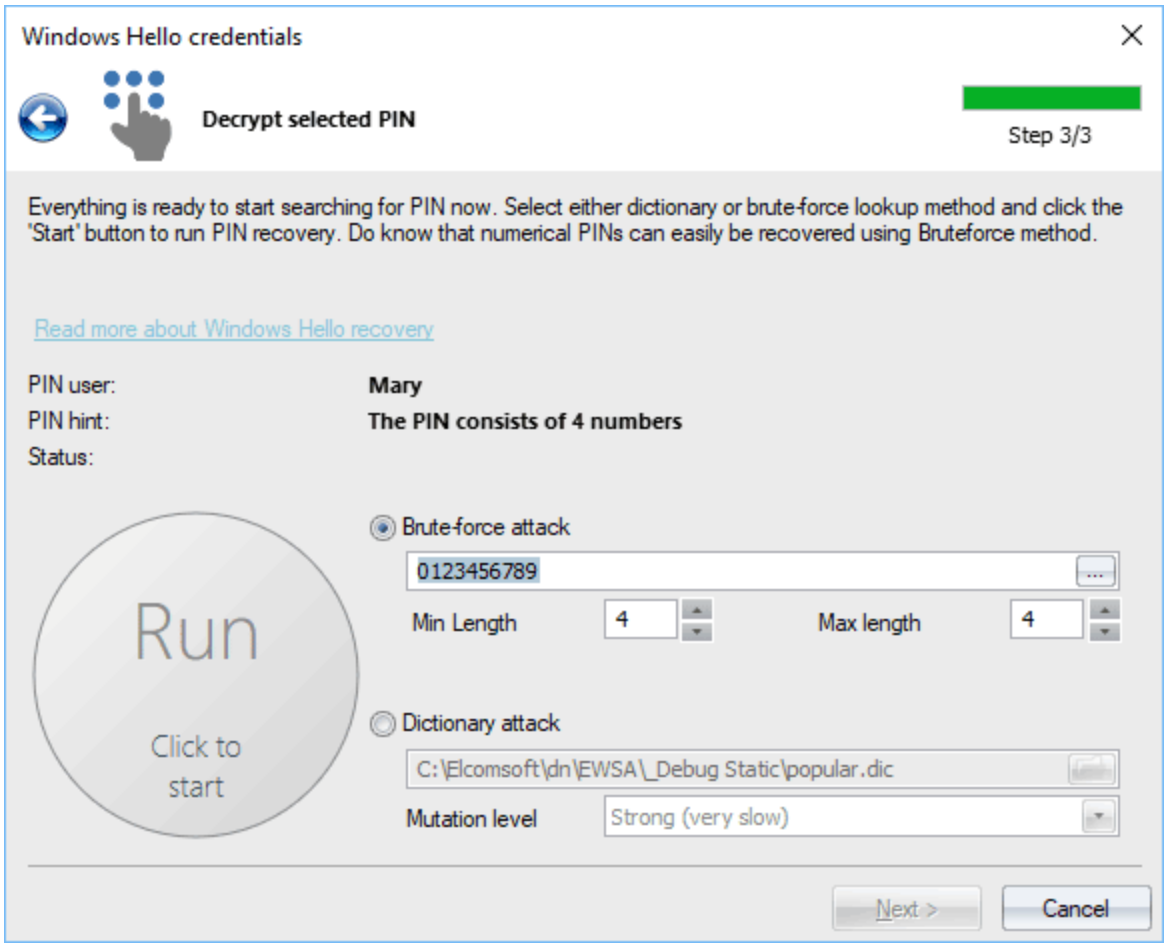
Para proporcionar sincronización de PIN para todos los dispositivos, Microsoft mantiene la copia de su PIN en sus servidores (solo para cuentas de Microsoft).



Primero debe mostrar el directorio de Windows del sistema de destino. Para poder extraer un PIN, el directorio de Windows debe permitir el cambio de acceso o las operaciones de escritura de archivos. En caso de que haya configurado su carpeta actual de Windows, es suficiente ejecutar el programa con privilegios de administrador.



En este paso, el programa muestra todas las cuentas de usuario encontradas que se han configurado para usar PIN para iniciar sesión en el sistema. Simplemente seleccione un usuario y proceda al cuadro de diálogo de recuperación de PIN.



El programa admite dos métodos de recuperación: fuerza bruta y predicción de diccionario. La configuración para cada uno de ellos es bastante trivial. En caso de fuerza bruta, tendrá que configurar un conjunto de caracteres, una longitud de PIN mínima y máxima. Para un ataque de diccionario, simplemente configure una lista de palabras y seleccione el nivel de mutación de palabras que necesita.

Para ejecutar o detener el ataque, use el botón redondo a la izquierda de la configuración.

En ciertos casos, el programa puede detectar el juego de caracteres utilizado para crear un PIN. Si este es tu caso, la sugerencia aparece en el campo correspondiente.

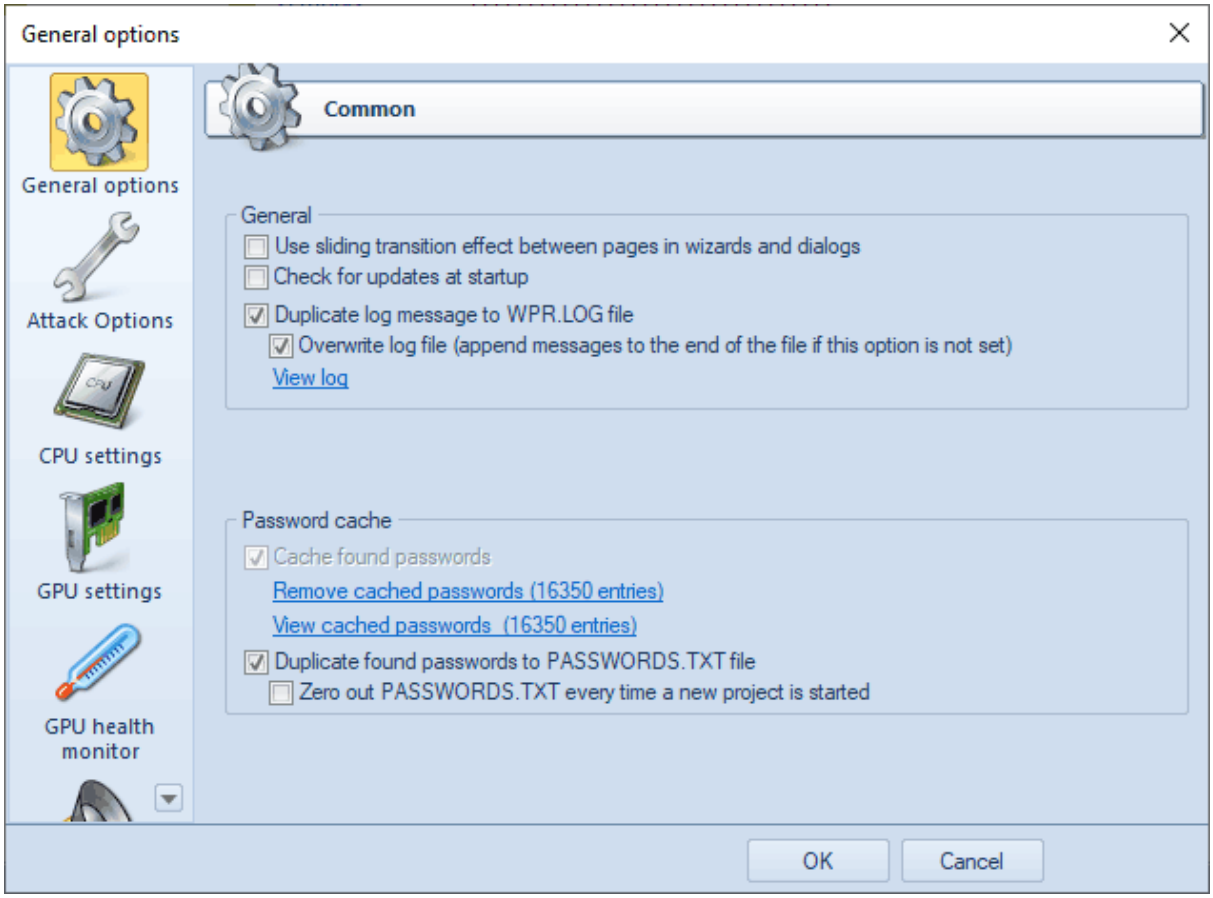
¡Los códigos PIN protegidos con TPM no son compatibles!

2.8 Menú de Opciones

2.8.1 Configuración general

La configuración general se divide en cinco partes.

2.8.1.1 Opciones generales



Usar transiciones deslizantes en asistentes y cuadros de diálogo - permite un efecto de transición gráfico en los cuadros de diálogo.

Compruebe si hay actualizaciones al inicio - compruebe si hay una actualización disponible cada vez que se inicie el programa. La opción solo funciona si la PC está conectada a Internet.

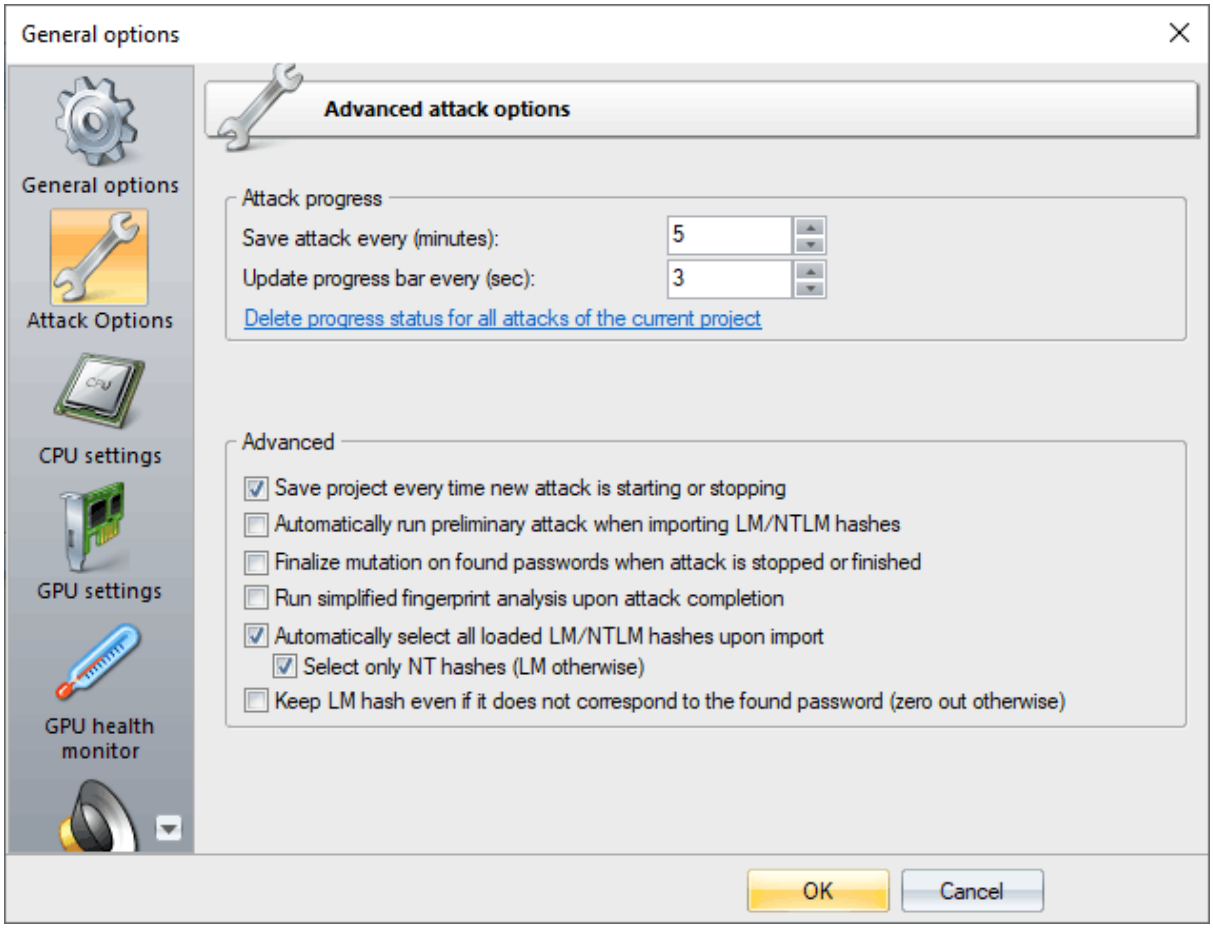
Duplicar mensajes de registro en wpr.log archivo - esta opción, cuando se establece, escribe todos los mensajes que la ventana de registro contiene en WPR. Archivo LOG. Establecer esta opción puede causar una degradación del rendimiento en una gran lista de hashes porque el wpr.log vacía su contenido en el disco cada vez que llega un nuevo mensaje. Sin embargo, puede ser útil cuando el programa se detiene o funciona inestable. WPR. LOG se encuentra en el directorio de instalación del programa.

Sobrescribir archivo de registro - sobrescriba el archivo de registro cada vez que se inicie el programa. De lo contrario, los mensajes nuevos se anexarán al final del archivo de registro.

Caché de contraseñas
Todas las contraseñas encontradas por el programa se almacenan en caché de forma predeterminada. Una cosa muy útil que se dedica a muchos subsistemas. Por ejemplo, en el ataque intelectual o preliminar. Se recomienda eliminar la caché de contraseñas solo en casos de extrema necesidad. Por ejemplo, cuando su número superó los diez mil. En este caso, la velocidad de búsqueda de algunos ataques puede disminuir significativamente.

Además, puede duplicar las contraseñas encontradas en el archivo de texto. Por lo tanto, incluso si el programa falla inesperadamente o en caso de una falla repentina de energía, las contraseñas encontradas garantizados se escribirán en el archivo.

2.8.1.2 Opciones de ataque



Progreso del ataque

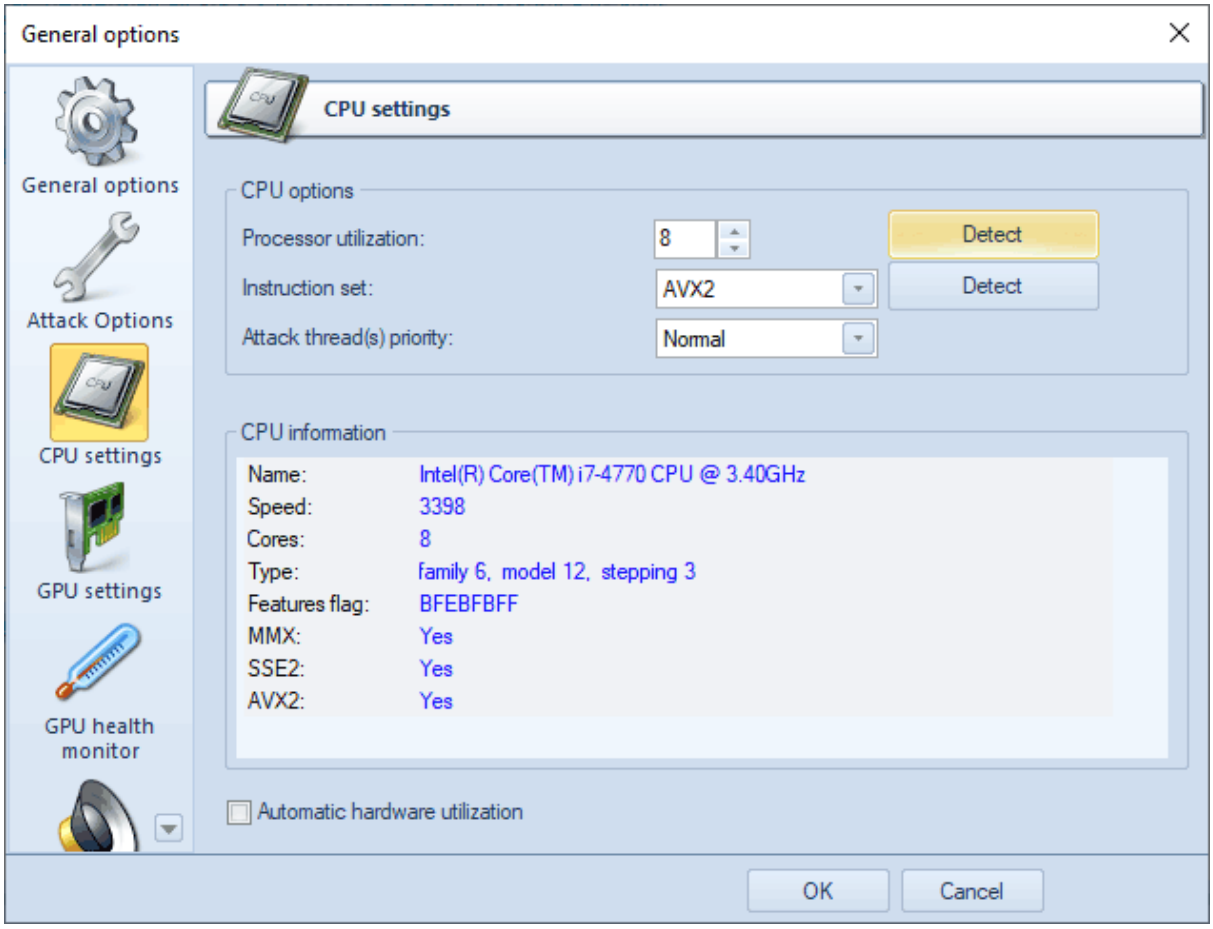
El primer grupo de configuraciones permite establecer los intervalos de guardado y actualización para el estado actual de un ataque. De forma predeterminada, un ataque guarda su estado cada 5 minutos (más adelante, puede reanudar el ataque desde el último punto guardado) y actualiza la pantalla cada 3 segundos.

Avanzado

- *'Guarde el proyecto cada ...'* - establecer esta opción obligará al programa a guardar automáticamente el proyecto cada vez que se inicie o se detenga un nuevo ataque.
- *'Ejecutar automáticamente un ataque preliminar al importar hashes'* - lanzar automáticamente un ataque preliminar al importar. Este ataque recupera contraseñas extremadamente débiles en cuestión de segundos.
- *'Finalizar la mutación en las contraseñas encontradas cuando el ataque se detiene o finaliza'* - activar el módulo de análisis de contraseñas y mutación para contraseñas encontradas después del ataque. Esta opción puede ser extremadamente útil; por ejemplo, para recuperar contraseñas similares.

- *'Ejecute un análisis simplificado de huellas dactilares al finalizar el ataque'* - activar el segundo módulo de análisis. Se lanza al finalizar el ataque, crea un nuevo diccionario de huellas dactilares a partir de contraseñas encontradas, tratando de recuperar más contraseñas. Útil en una gran lista de hashes, hashes de historia, etc.
- *'Seleccione automáticamente todos los hashes cargados al importar'* - seleccionar automáticamente las entradas que se buscarán después de la importación.
- *'Mantener hash LM incluso si no corresponde a la contraseña encontrada'.* Los sistemas operativos Windows Server 2003 y superiores almacenan datos de ruido (creados aleatoriamente) en ranuras LM si la autenticación LM está deshabilitada en el servidor. Si no se establece la configuración de este programa, el WPR comprueba el hash LM apropiado (si existe) cada vez que se encuentra una nueva contraseña. Una vez que el programa detecta que el hash LM no corresponde a la contraseña encontrada, simplemente elimina el hash LM. Si esta configuración está activada, el programa no hace nada con hashes LM incorrectos.

2.8.1.3 Configuración de CPU

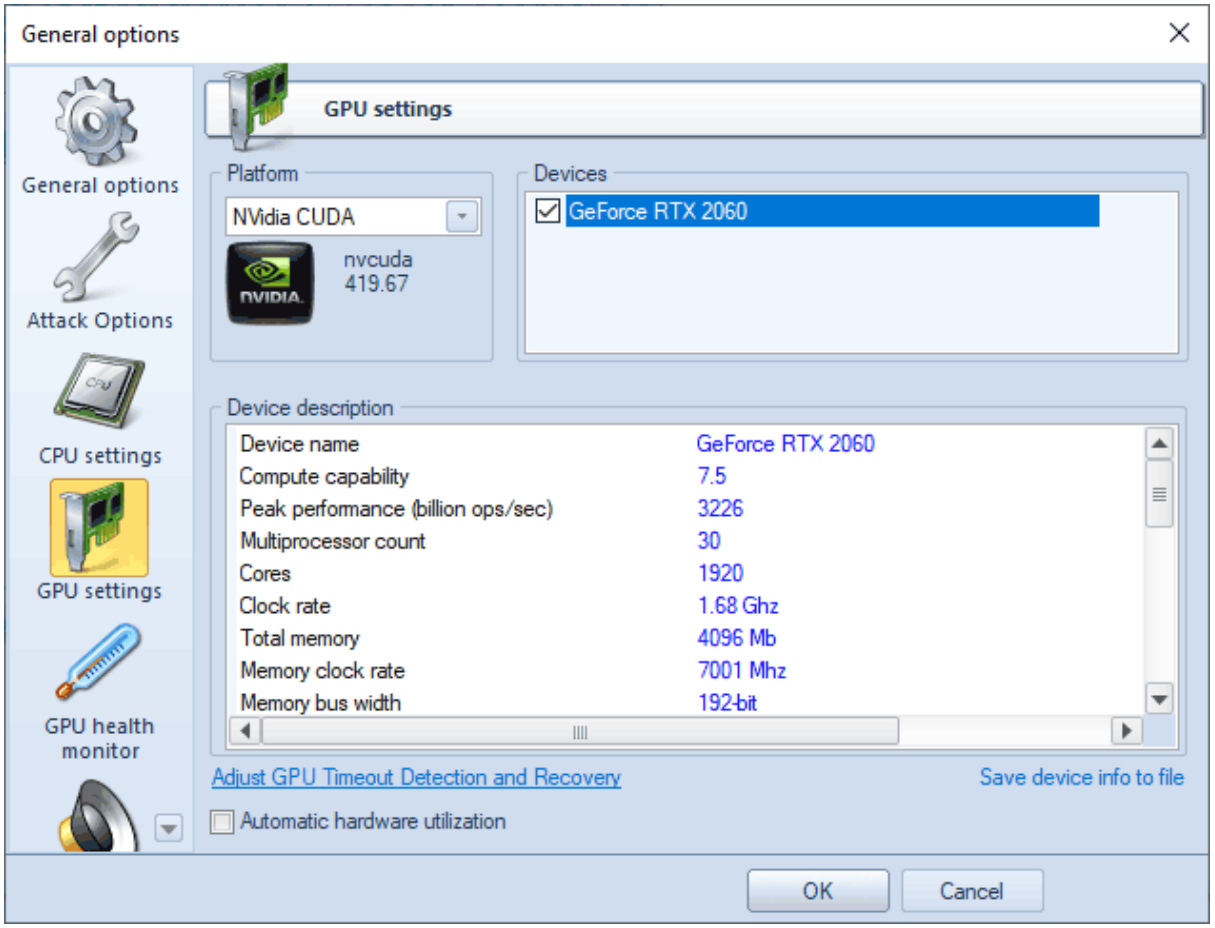


Dado que la mayoría de los ataques admiten subprocesos múltiples, puede establecer el número de subprocesos de búsqueda que se ejecutarán simultáneamente. En la mayoría de los casos, debe coincidir con el número de núcleos en su CPU. Sin embargo, si la CPU admite la tecnología Hyper-Threading, incluso puede duplicar el número de subprocesos de búsqueda que se ejecutan simultáneamente.

Los algoritmos hash DES, MD4 y SHA-1 en Windows Password Recovery están optimizados para las siguientes arquitecturas de CPU: X86, MMX, SSE2 y AVX2. Naturalmente, en las CPU que admiten una arquitectura más nueva, la búsqueda se ejecutaría más rápido.

No se recomienda establecer la prioridad de ataque por encima de lo normal; de lo contrario, puede observar una reducción considerable del rendimiento de todo el sistema.

2.8.1.4 Configuración de GPU

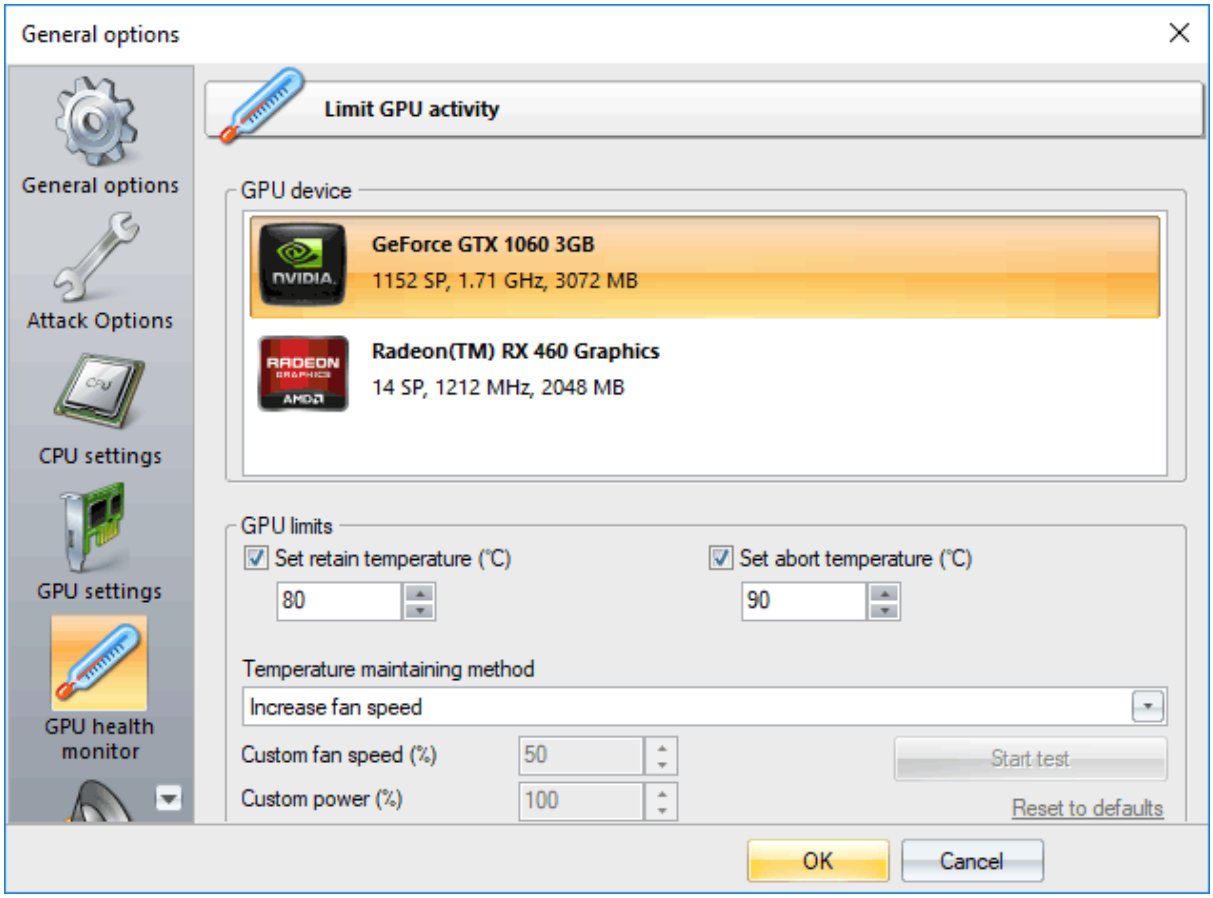


Antes de ejecutar un ataque a una GPU, selecciónela en la configuración general de la aplicación simplemente marcando la casilla de verificación junto al nombre de la GPU. Todas las características principales del dispositivo se muestran en la tabla de propiedades.

El software es compatible con las GPU NVidia (construidas en la plataforma CUDA) y AMD (construidas en la plataforma OpenCL).

The GPU settings are unavailable if automatic hardware utilization is set on.

2.8.1.5 Monitor de estado de GPU



Puede usar el monitor de estado de la GPU para retener una temperatura de gpu a un valor determinado, así como para anular la búsqueda de contraseña en caso de que la temperatura alcance un cierto valor crítico.

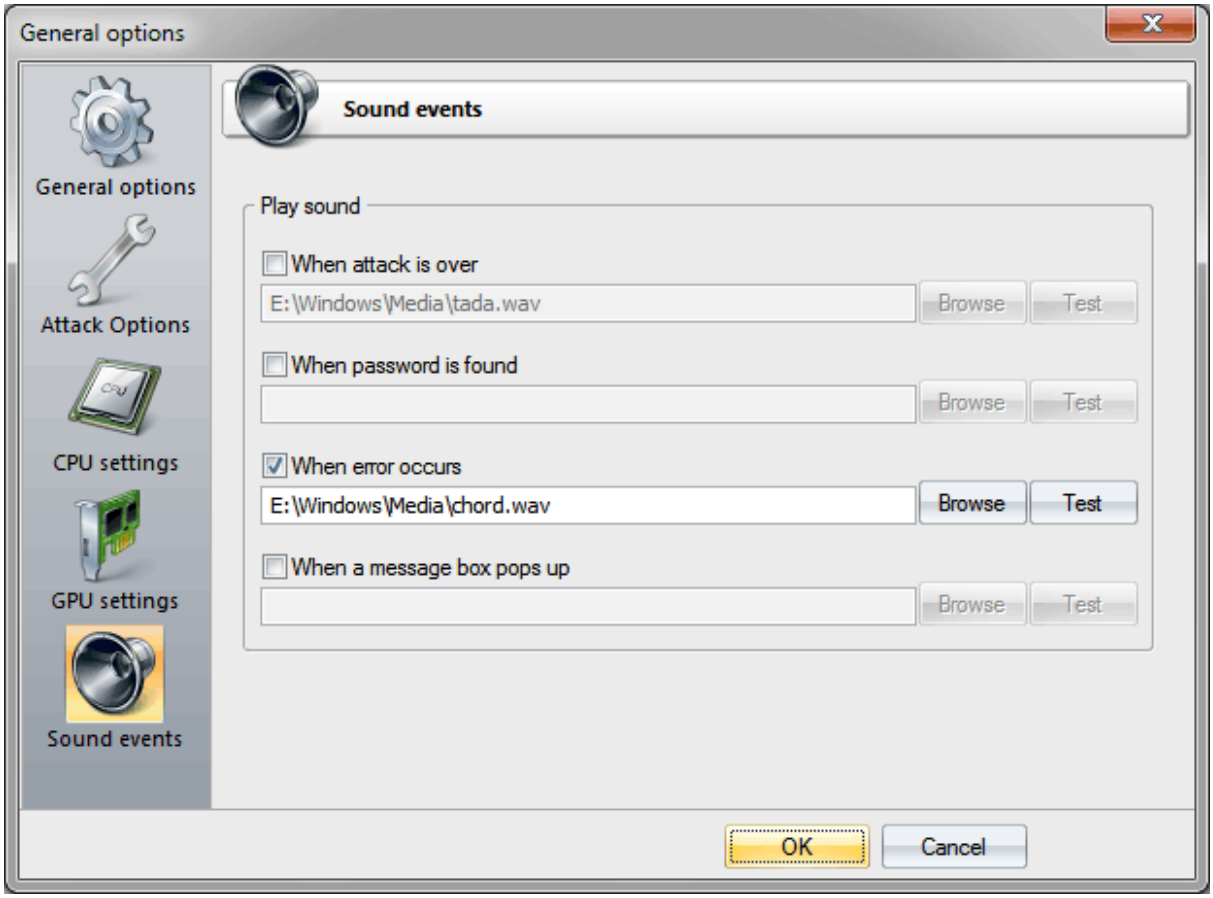
Para establecer la temperatura de retención, seleccione su GPU de la lista de dispositivos disponibles, marque la opción correspondiente y configure su valor en grados Celsius. A continuación, seleccione uno de los métodos de retención:

- **Aumente simultáneamente la velocidad del ventilador y disminuya la potencia de la GPU**. Úselo si desea reducir el ruido del ventilador, pero una ligera disminución en el rendimiento no es un problema para usted.
- **Aumente la velocidad del ventilador**. Cuando se selecciona este método, el programa aumenta la velocidad del ventilador cuando la temperatura excede el límite y disminuye cuando se está enfriando. Úselo cuando necesite el máximo rendimiento. También se recomienda configurar la temperatura de aborto para evitar el sobrecalentamiento de la GPU.
- **Disminuir la potencia de la GPU**. Es bastante efectivo para enfriar la temperatura de una GPU. La frecuencia del procesador de la GPU se ajusta automáticamente a la temperatura de retención, mientras que la velocidad del ventilador estará determinada por la configuración del sistema. La desventaja incluye una caída significativa del rendimiento en ciertos casos.
- **Configuración personalizada** incluyen la velocidad del ventilador definida por el usuario y/o la potencia de la GPU.

Utilice la temperatura de interrupción para dejar de buscar contraseñas una vez que la temperatura de la GPU alcance el límite.

¡Advertencia! Una vez que se selecciona un dispositivo AMD, el programa solo admite la opción de temperatura de interrupción. Los controladores AMD no permiten anular algunos valores manualmente para la mayoría de las tarjetas y tienen numerosos errores que pueden causar inestabilidad del sistema o incluso BSOD. Considere usar la herramienta integrada Radeon para configurar su propio perfil de rendimiento en su lugar.

2.8.1.6 Notificaciones de sonido

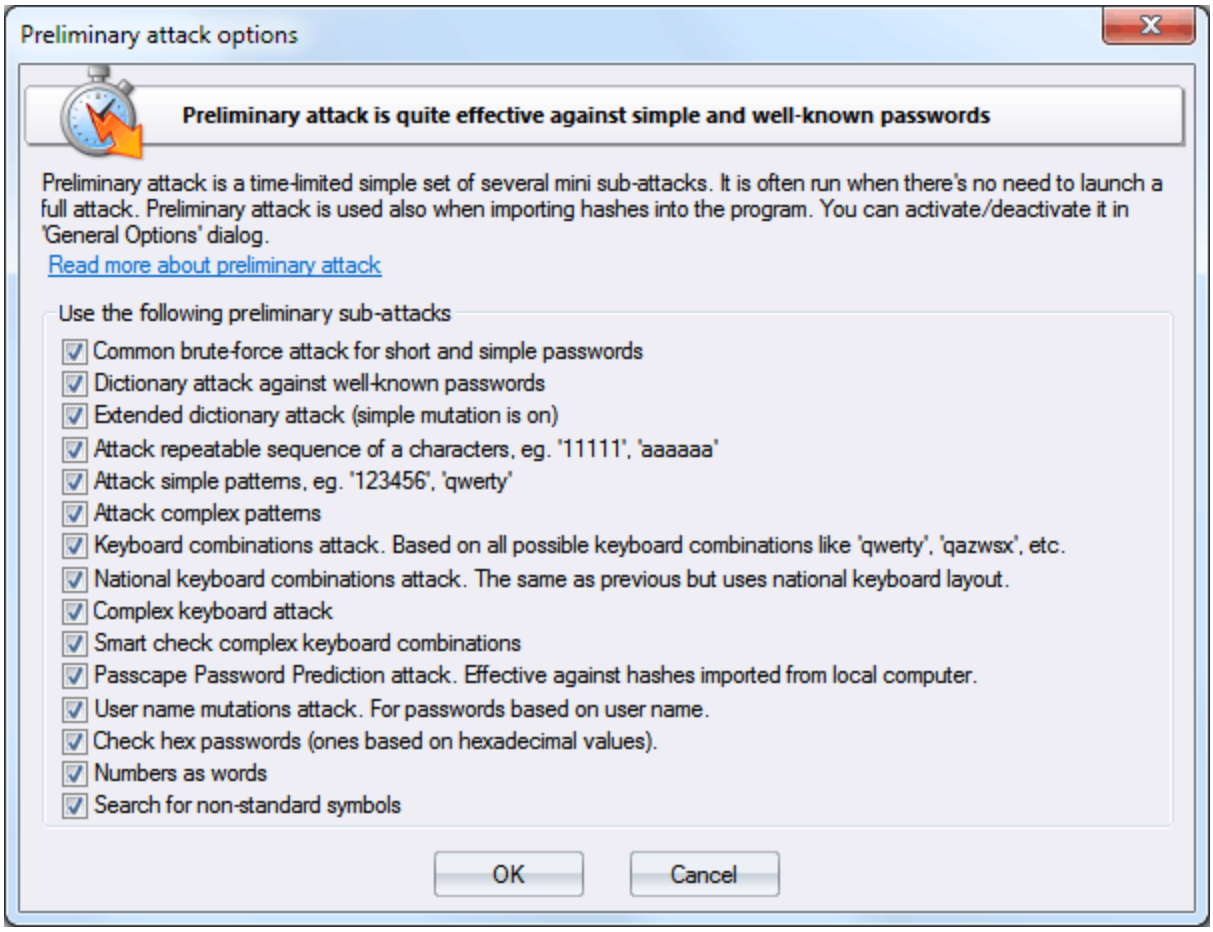


El software permite configurar notificaciones de sonido para ciertos eventos. Por ejemplo, cuando el ataque ha terminado o cuando se encuentra una contraseña.

2.8.2 Configuración de ataque

2.8.2.1 Ataque preliminar

El ataque preliminar (desarrollado en Passcape) es bastante efectivo contra contraseñas cortas, simples, de diccionario, repetitivas, de teclado, etc. y consiste en varios miniataques. Cada miniataque se puede activar/desactivar individualmente.



El ataque preliminar dura unos 10-20 minutos o incluso más rápido. Consiste en al menos los siguientes subataques:

- Ataque común de fuerza bruta. Realiza varios ataques simples de fuerza bruta basados en conjuntos de caracteres predefinidos.
- Ataque de diccionario simple. Verifique rápidamente la contraseña verificando todas las palabras de un diccionario determinado.
- Ataque de diccionario extendido. Es casi lo mismo que el anterior, pero con algunas opciones de mutación inteligentes establecidas.
- Ataque a repetibles. Comprobación de contraseñas como una secuencia repetible de un carácter. Eg. '1111111' o 'xxxxxxx'.
- Ataca patrones simples, como '123456' o 'qwerty'.
- Ataque a patrones complejos. Lo mismo que arriba, para patrones compuestos.
- El ataque de teclado busca contraseñas de teclado y todas las combinaciones posibles. Eg. 'qwer', 'qazwsx', 'asdzxc', etc.
- Ataque de teclado nacional. Lo mismo que anteriormente, pero comprueba las contraseñas escribidas en la distribución del teclado nacional.
- El ataque de teclado complejo es el mismo que los 2 ataques anteriores, para patrones de teclado compuestos.
- El ataque Passcape Password Prediction es la herramienta de predicción de contraseñas más complicada y de última generación.
- Ataque a contraseñas basadas en nombres.
- Ataque a contraseñas hexadecadeciales (por ejemplo, 7A49F3).
- Atacar contraseñas basadas en números (como palabras).

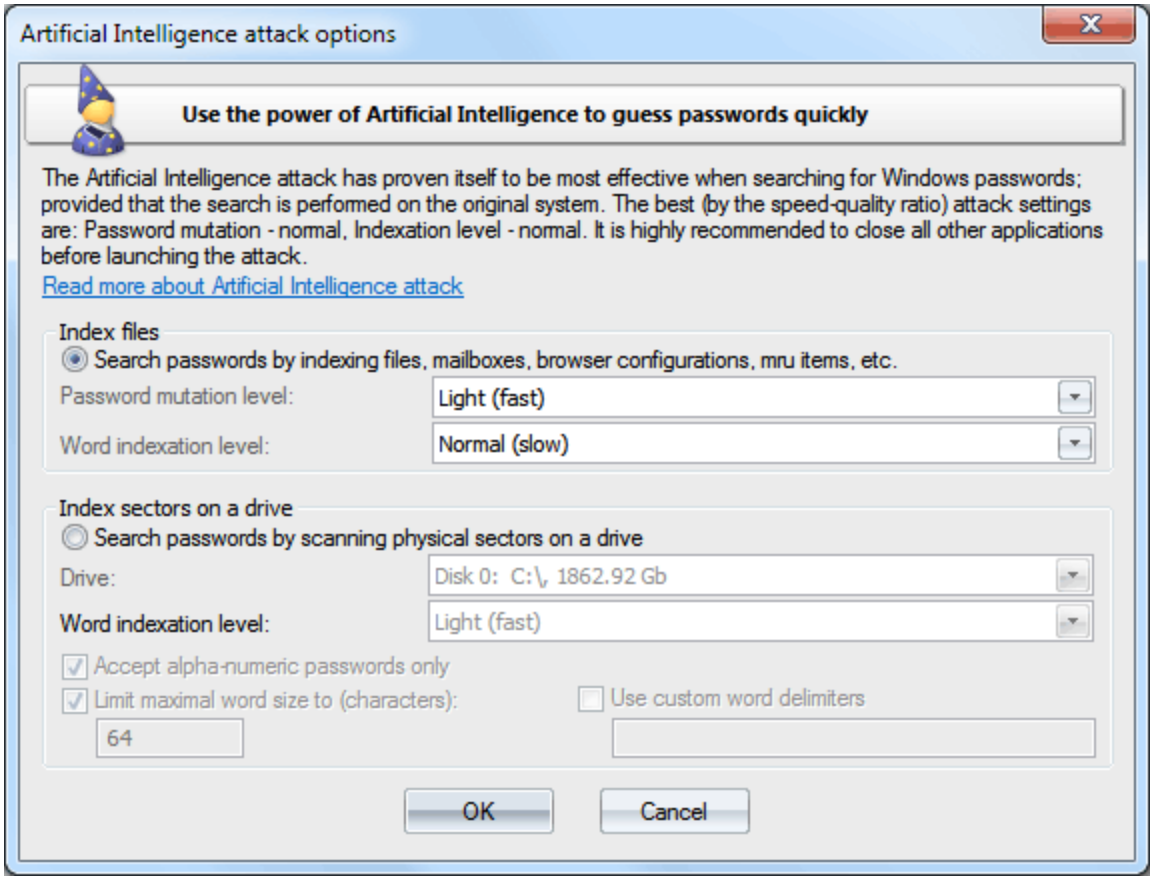
- Busque símbolos no estándar y contraseñas cortas que se crearon con símbolos UNICODE no estándar.

2.8.2.2 Ataque de inteligencia artificial

Artificial Intelligence Attack es un nuevo tipo de ataque desarrollado en nuestra empresa. Se basa en un método de ingeniería social y nunca se ha implementado en aplicaciones de recuperación de contraseñas todavía.

Este se utiliza principalmente cuando los hashes se importan desde el equipo local. El ataque intelectual escanea la computadora local, indexa y crea la lista de palabras y contraseñas encontradas, las analiza, según los resultados del análisis produce las preferencias del usuario, realiza la mutación de las palabras encontradas y, en función de todo eso, intenta recuperar las contraseñas.

Este ataque permite, sin recurrir a cálculos lentos y costosos, recuperar casi instantáneamente ciertas contraseñas cifradas con funciones hash. La idea básica detrás del ataque de Inteligencia Artificial es que un usuario promedio muy a menudo elige palabras y combinaciones de palabras similares o sigue la misma regla de generación de contraseñas al crear sus contraseñas. Con eso en mente, podríamos intentar averiguar esa regla y elegir la contraseña original.



Aunque esto suene algo abstracto, en la realidad el ataque se divide claramente en cuatro pasos sucesivos.

1. Iniciar la recopilación de datos privados. Aquí entra en acción el módulo de recuperación e indexación de contraseñas, que busca todas las contraseñas disponibles y ocultas en el sistema introducidas por el usuario en cualquier momento. Estos incluyen contraseñas de acceso a la red, ICQ, correo electrónico, FTP, contraseñas de cuentas de Windows, contraseñas de servidores, secretos LSA, etc.
2. Inicia el módulo de recopilación e indexación de datos. Durante la ejecución de este paso, analizamos la actividad del usuario (o de todos los usuarios, si el módulo de indexación seleccionado es diferente a Light) en el sistema. A continuación, basándonos en eso, generamos la lista de palabras: contraseñas potenciales seleccionadas de los archivos de texto, archivos, historial de navegadores de Internet, correspondencia por correo electrónico, etc.
3. Incluye el módulo de análisis semántico para la base de datos de contraseñas encontradas y la lista de contraseñas potenciales.
4. En la etapa final, el módulo de análisis de datos realizará la mutación de las palabras e intentará elegir las contraseñas.

Al comienzo del ataque, el programa buscará en el sistema todas las contraseñas que conoce. Para ese propósito, actualmente hay 32 mini módulos para descifrar el sistema, correo, navegador, mensajería, archivo y otras contraseñas. Luego va la indexación de archivos y datos, a lo largo del cual el programa genera un diccionario de ataque potencial. El tercer módulo rompe las contraseñas y las palabras en pedazos, de los cuales en el último módulo ensamblará nuevas combinaciones para elegir y adivinar la contraseña original.

En promedio, con los menores niveles de indexación y mutación, el tiempo de ataque puede variar entre 1 minuto y 10-15 minutos, dependiendo de la actividad de red del usuario. En una computadora doméstica, toda la ruta normalmente no toma más de 2-3 minutos. Naturalmente, cuanto más compleja sea la mutación y el nivel de indexación, más eficiente será la búsqueda. Sin embargo, alcanzar el nivel más alto de indexación y análisis puede llevar horas e incluso días, dependiendo de la velocidad del algoritmo de validación de contraseña y el número de usuarios en el sistema.

El ataque de Inteligencia Artificial ha demostrado ser más efectivo cuando la búsqueda se realiza en el sistema original. Solo hay dos opciones disponibles aquí: profundidad de mutación de contraseña y nivel de indexación de palabras. Las opciones más preferidas para ejecutar un ataque rápido son *Light*:*Light*. Para una búsqueda más profunda (y al mismo tiempo más lenta), establezca estas opciones en *Normal* o incluso *Profundo*. La duración de un ataque intelectual también depende de la configuración de su sistema, la carga de su red y otros factores.

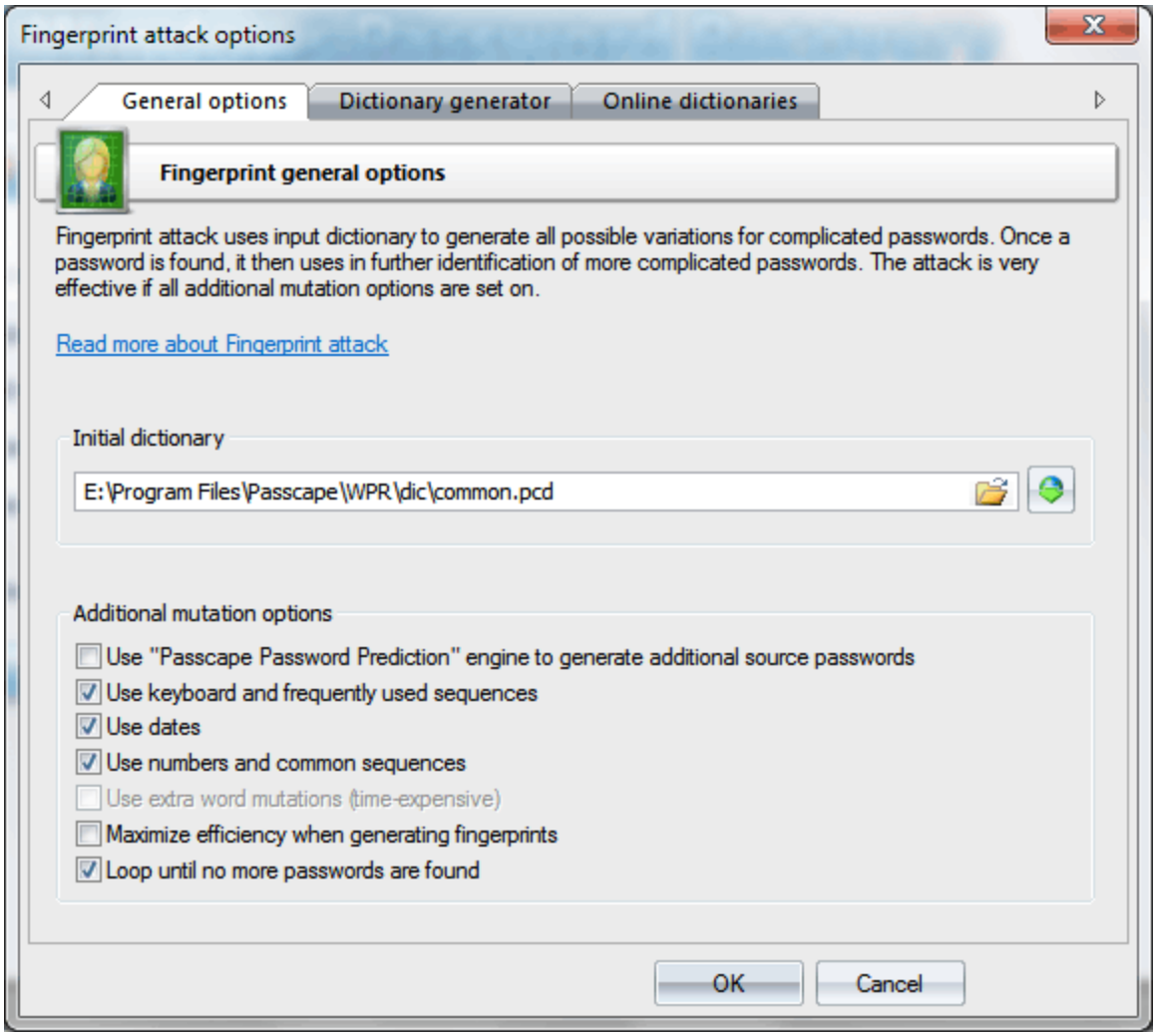
Se recomienda encarecidamente apagar todos los demás programas antes de lanzar el ataque. Si su ataque de Inteligencia Artificial se ejecuta muy lento, es posible que deba eliminar la contraseña almacenada en caché de su programa (por ejemplo, la cantidad total de contraseñas almacenadas en caché supera las 10000).

Windows Password Recovery versión 9.5 ahora viene con una nueva característica que permite la búsqueda de contraseñas mediante la indexación de sectores sin procesar en unidades seleccionadas. Esta característica funciona tanto para hashes LM como NTLM, buscando contraseñas ASCII y UNICODE. Puede cambiar algunas opciones de búsqueda avanzada aquí. Por ejemplo, *'Nivel de indexación de palabras'* establece una mutación adicional en todas las contraseñas encontradas. Tenga cuidado, caminar por todos los sectores de la unidad de destino con esta opción configurada en 'Difícil' puede llevar bastante tiempo. Tenga en cuenta que el algoritmo de escaneo basado en sectores no es efectivo contra las unidades que tienen un cifrado de disco completo establecido. Como Bitlocker o TrueCrypt, por ejemplo.

2.8.2.3 Ataque de huellas dactilares

El ataque de huellas dactilares es una herramienta relativamente nueva para recuperar contraseñas complejas, que no pudieron ser descifradas por otros ataques. La idea del ataque es que aquí, para recuperar una contraseña, no tomamos ni palabras individuales del diccionario de origen, como en el ataque de diccionario, ni siquiera combinaciones de palabras, como en el ataque combinado, sino las llamadas "huellas dactilares". Ahora, cada palabra fuente del diccionario se utiliza para generar varias huellas dactilares. Si se encuentra alguna contraseña durante el ataque, participa en la generación de nuevas huellas dactilares, y el ataque va otra ronda.

Antes de iniciar el ataque, especifique el diccionario de origen que se utilizará para crear el banco de huellas dactilares. El software viene con un diccionario, common.pcd, optimizado para este ataque, pero puede usar el suyo o descargar uno de Internet (pestaña 'Diccionarios en línea'). No hay ciertos requisitos para el diccionario, excepto uno: el diccionario de origen no debe ser demasiado grande; de lo contrario, el ataque tomará un tiempo significativo. Puede utilizar diccionarios con contraseñas nacionales si sospecha que la contraseña buscada contiene caracteres en una codificación nacional.



Esta es la forma de generar huellas dactilares: primero, divida cada palabra del diccionario de origen en contraseñas de un carácter, luego, en 2 caracteres, etc. Por ejemplo, divida la palabra fuente crazy en huellas dactilares de un carácter. Obtenemos:

c
r
a
z
y
Ahora, dos caracteres:
cr
ra
az
zy
A continuación, tres caracteres:
cra
raz
azy
Y, por último, cuatro caracteres:
craz
razy

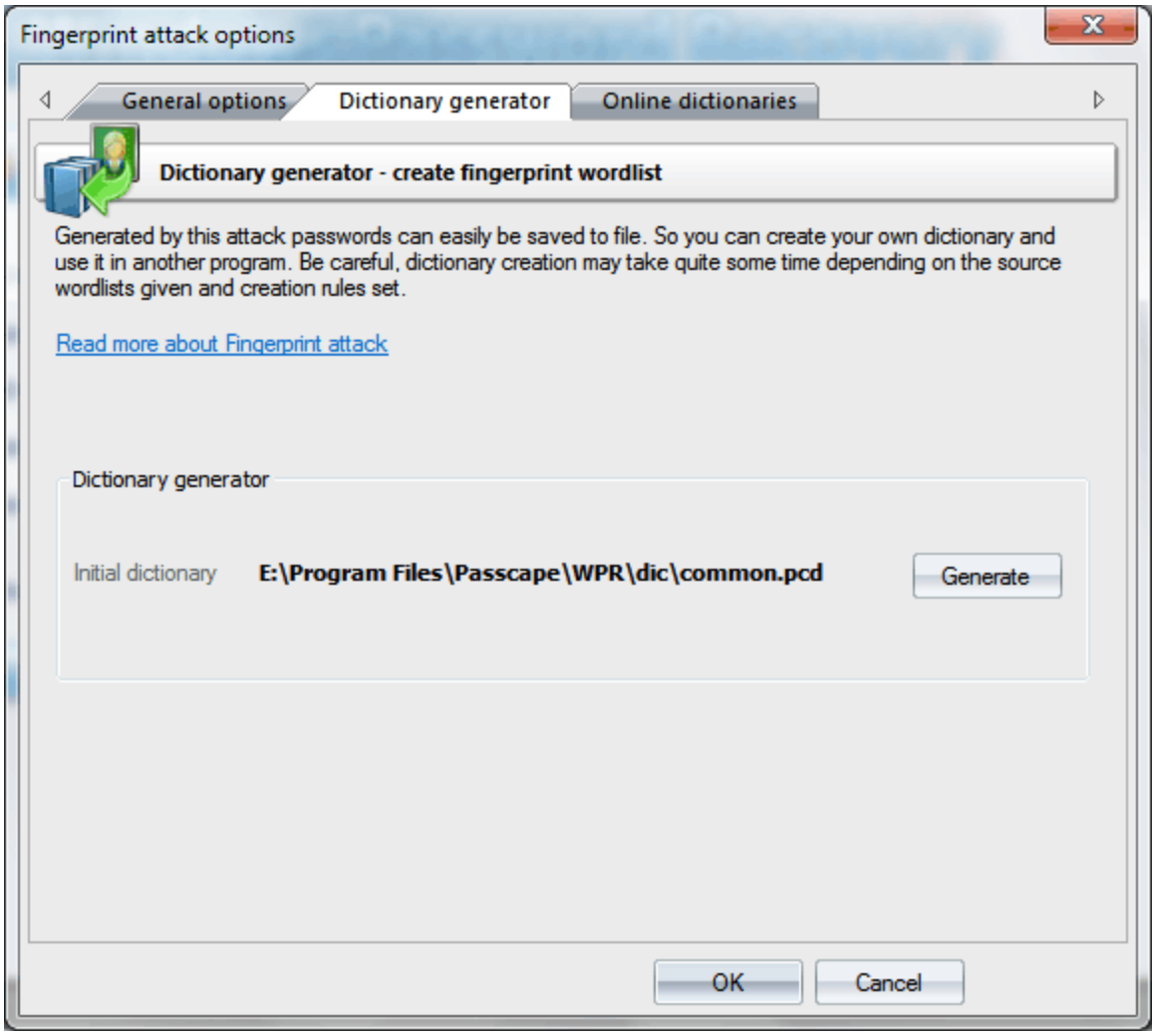
Tenemos 5 + 4 + 3 + 2 = 14 huellas dactilares, sin contar la palabra fuente.
Repita esto para cada palabra del diccionario de origen. Después de esto, todas las huellas dactilares se vuelcan en una sola base de datos, naturalmente, descartando duplicados. Tenemos una base de datos de huellas dactilares que se utilizaría para verificar las contraseñas pegando todas las huellas dactilares entre sí y encontrando la coincidencia.

El algoritmo real de generación de huellas dactilares es mucho más sofisticado. Además, hay una opción en la configuración de ataque, **Maximizar la eficacia al generar huellas dactilares**, que utiliza un algoritmo más sofisticado, que maximiza la eficiencia (a expensas de la velocidad) al generar huellas dactilares adicionales.

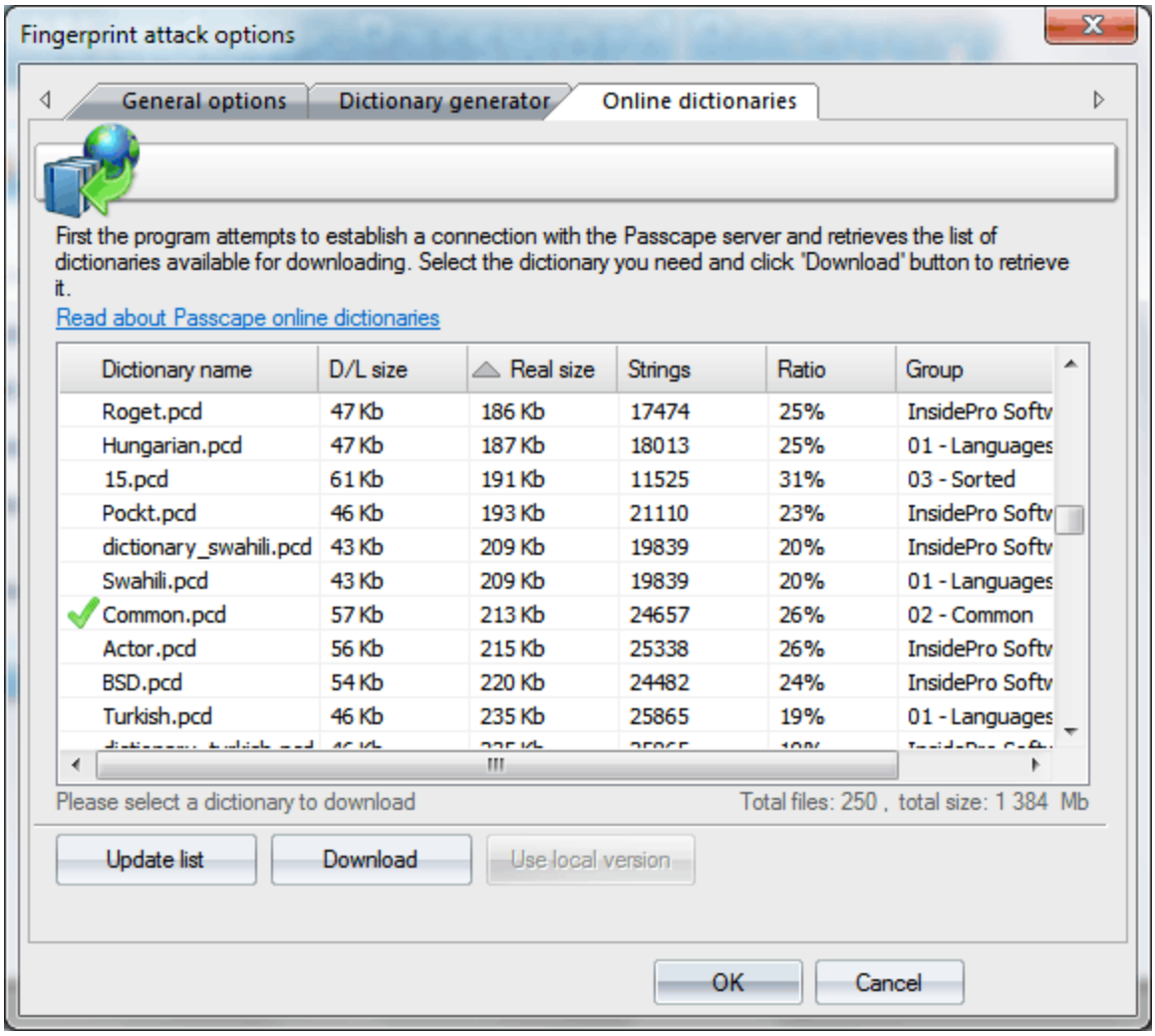
Echemos un vistazo a las opciones restantes.
Usar el motor PPP para generar contraseñas adicionales - utilizar contraseñas encontradas en otros ataques al generar huellas dactilares.
Usar el teclado y usar secuencias con frecuencia - agregue combinaciones de teclado y secuencias comunes al banco de huellas dactilares.
Fechas de uso - añadir fechas a las huellas dactilares.
Usar números y secuencias comunes - usar dígitos y combinaciones simples de letras.

Se debe prestar la atención más cuidadosa a la opción. **Repetir hasta que no se encuentren más contraseñas**. Ahí es donde el ataque de huellas dactilares realmente puede mostrarse. Así es como funciona: si se encuentra al menos una contraseña durante un ataque, cuando el ataque ha terminado, la contraseña participa en la generación de nuevas huellas dactilares y el ataque se ejecuta nuevamente. Esta opción funciona muy bien en grandes listas de hashes y en hashes de historial de contraseñas. Sin embargo, una vez que se establece la opción, no podrá continuar el ataque desde la última posición guardada.

La segunda pestaña con la configuración permite crear y grabar un diccionario personalizado utilizando las opciones actuales de ataque de huellas dactilares. Ten cuidado; ese diccionario puede ocupar mucho espacio en el disco duro de su computadora.



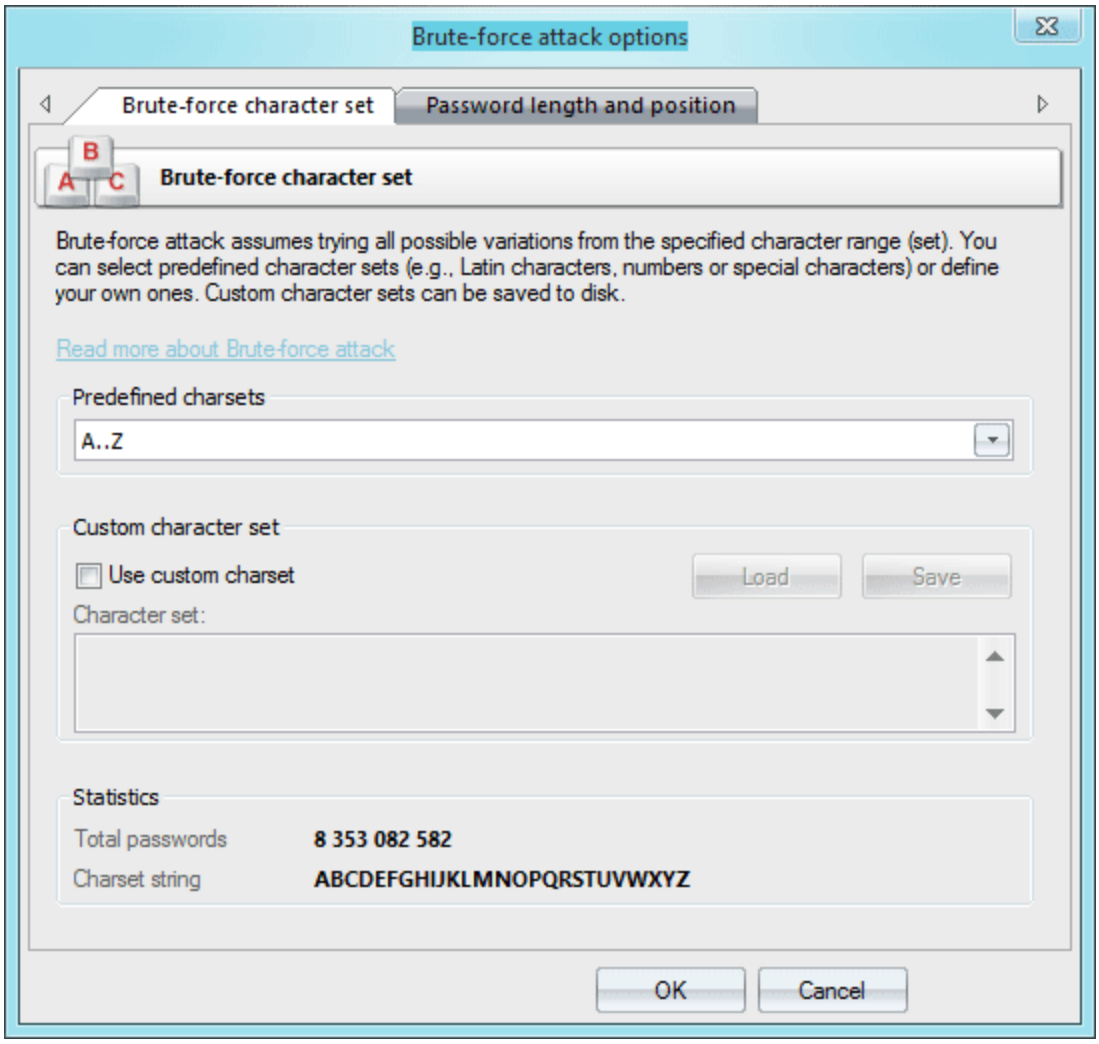
En la tercera pestaña, puede descargar diccionarios de origen para el ataque de huellas dactilares de Internet.



2.8.2.4 Ataque de fuerza bruta (búsqueda exhaustiva)

En criptoanálisis, un ataque de fuerza bruta es un método para derrotar un esquema criptográfico probando una gran cantidad de posibilidades; por ejemplo, trabajar exhaustivamente a través de todas las claves posibles para descifrar un mensaje. Esta definición fue tomada del sitio de Wikipedia.

Bueno, para ponerlo en palabras simples, el ataque de fuerza bruta adivina una contraseña probando todas las variantes probables por un conjunto de caracteres dado. Eg. comprobando toda la combinación en el conjunto de caracteres latinos inferiores, es decir, '*abcdefghijklmnopqrstuvwxyz*'. El ataque de fuerza bruta es muy lento. Por ejemplo, una vez que establezca un conjunto de caracteres latinos inferiores para su ataque de fuerza bruta, tendrá que buscar en 217 180 147 158 variantes para obtener una contraseña de símbolo 1-8. Debe usarse solo si otros ataques no han podido recuperar su contraseña.



The brute-force attack options consist of two tabs.

Las opciones de ataque de fuerza bruta constan de dos pestañas.

La primera pestaña es para establecer el rango de caracteres que se buscarán. Puede utilizar los conjuntos predefinidos o crear los suyos propios. Para definir su propio juego de caracteres, seleccione la opción *'Conjunto de caracteres personalizado'*. Esto habilitará dos campos para definir un juego de caracteres personalizado: el primero - para introducir caracteres ASCII, el segundo - para introducir caracteres no imprimibles. Puede guardar el juego de caracteres personalizado en el disco. El programa viene con varios ejemplos de conjuntos de caracteres definidos por el usuario.

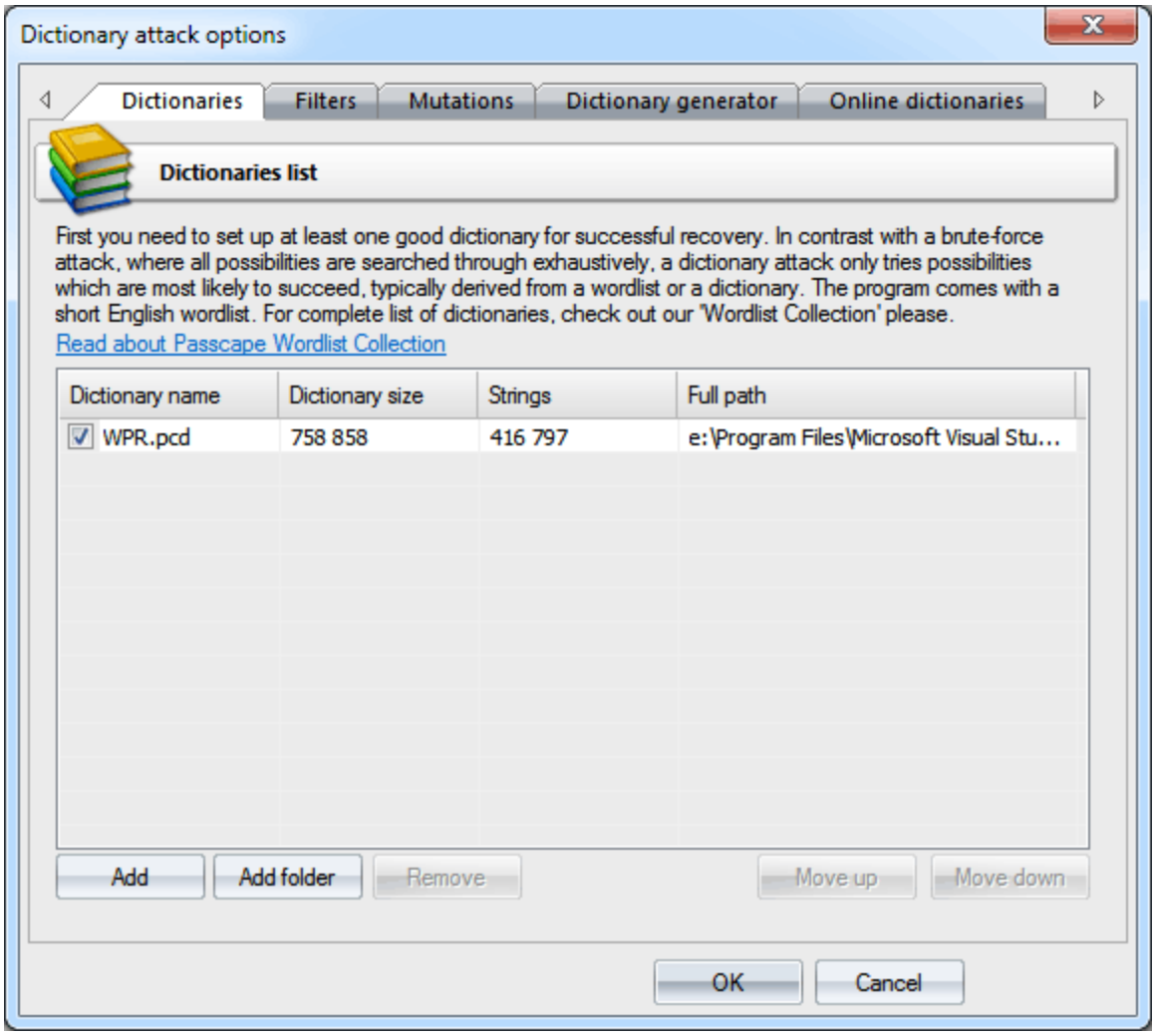
En la segunda pestaña, establezca la longitud mínima y máxima de las contraseñas que se buscarán. Tenga en cuenta que para atacar hashes LM, la longitud máxima de la contraseña no debe exceder los 7 caracteres. También puede establecer una contraseña de inicio, que iniciaría la búsqueda.

A continuación se muestra una tabla que muestra la seguridad de la contraseña dependiendo de la longitud y complejidad de la contraseña. Suponiendo que la velocidad de recuperación es de 100M de contraseñas por segundo.

Juego de caracteres	Longitud de la contraseña	Ejemplo de contraseña	Tiempo para descifrar (búsqueda exhaustiva de fuerza bruta)
A .. Z	5	CRUEL	Al instante
A .. Z	6	SECRET	3s
A .. Z	7	MONSTER	1m 23s
A .. Z	8	COOLGIRL	36m 11s
A .. Z, 0 .. 9	5	COOL3	Al instante
A .. Z, 0 .. 9	6	BANG13	22s
A .. Z, 0 .. 9	7	POKER00	13m 26s
A .. Z, 0 .. 9	8	LETMEBE4	8h 3m 37s
A .. Z, a .. z, 0 .. 9	5	P0k3r	9s
A .. Z, a .. z, 0 .. 9	6	S3cr31	9m 37s
A .. Z, a .. z, 0 .. 9	7	Didlt13	9h 56m 33s
A .. Z, a .. z, 0 .. 9	8	GoAway99	25d 16h 26m 34s

2.8.2.5 Ataque de diccionario

En contraste con un ataque de fuerza bruta, donde todas las posibilidades se buscan exhaustivamente, un ataque de diccionario solo intenta posibilidades que tienen más probabilidades de éxito, generalmente derivadas de una lista de palabras o un diccionario. En general, los ataques de diccionario tienen éxito porque muchas personas tienden a elegir contraseñas que son palabras cortas y únicas en un diccionario, o son variaciones simples que son fáciles de predecir.



En la pestaña *'Diccionarios'*, configure la lista de diccionarios que se utilizarán en el ataque. Se admiten diccionarios de texto plano en los formatos ASCII, UNICODE y UTF8, así como diccionarios cifrados/comprimidos en formato PCD nativo, desarrollados en Passcape Software. La lista de palabras empaquetadas zip y RAR también son compatibles con algunas restricciones. Para desactivar un diccionario, simplemente desactive la casilla de verificación por su nombre. En este caso, el diccionario, aunque permanezca en la lista, se omitirá durante un ataque. El software viene con un diccionario de 360000 palabras. Para obtener una lista completa de diccionarios, por favor consulta nuestra colección de lista de palabras. O puede utilizar nuestros diccionarios en linea como alternativa.

La pestaña '*Filtros*' filtra las palabras de un diccionario por el principio include/exclude. Si el primer filtro, inclusivo, está habilitado, el ataque aceptará solo las palabras que contengan al menos uno de los caracteres introducidos en el filtro. Si se establece el segundo filtro exclusivo, el programa omitirá las palabras que contengan al menos uno de los caracteres introducidos.

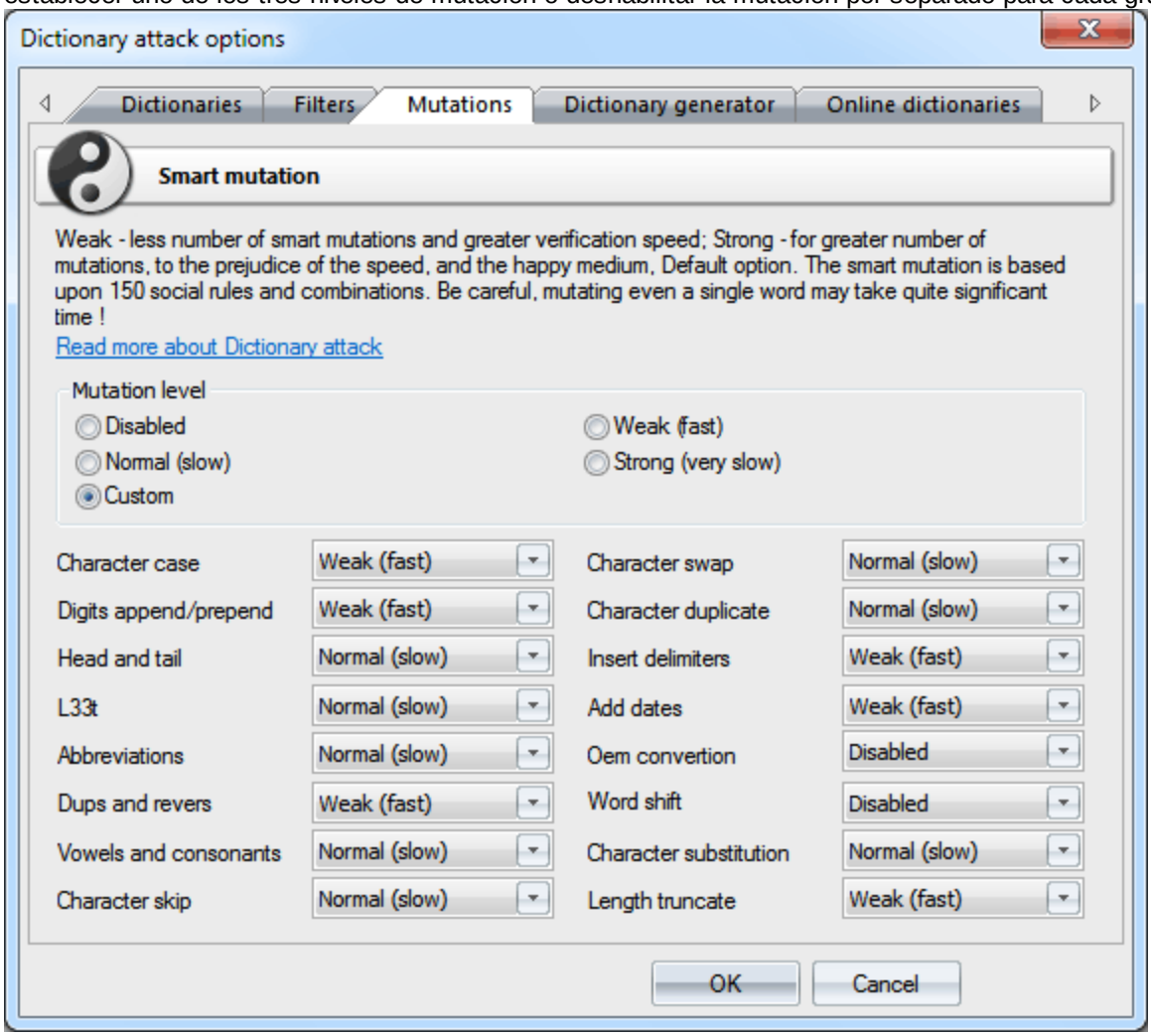
La pestaña '*Mutación*' permite establecer todo tipo de combinaciones posibles de las palabras a buscar. Por ejemplo, si establece una mutación fuerte, el programa creará varios cientos de análogos para cada palabra del diccionario. Por ejemplo, secreto - Secreto - s3cr3t - secret123, y así sucesivamente. Puede configurar hasta tres reglas de mutación: *Débil* - menor número de mutaciones y, a su vez, mayor velocidad de verificación; *Fuerte* - para un mayor número de mutaciones, en perjuicio de la velocidad, y el medio feliz, opción predeterminada (*Normal*).

Puede usar el *Generador de diccionarios* para crear sus propias listas de palabras basadas en las opciones de las tres primeras pestañas.

Diccionarios en línea. El programa tiene una gran característica que permite descargar y utilizar los diccionarios existentes disponibles en el sitio web de Passcape. Hemos acumulado una colección de diccionarios bastante grande: más de 250 artículos. Eso debería deshacerse de la molestia adicional de encontrar el contenido requerido en la red.

Personalización de mutaciones

A partir de la versión 4.0, el programa tiene la capacidad de personalizar la mutación inteligente del ataque del diccionario. Todas las reglas de mutación se agrupan en 16 grupos primarios. Puede establecer uno de los tres niveles de mutación o deshabilitar la mutación por separado para cada grupo.



Por ejemplo, puede desactivar la mutación OEM (y, por lo tanto, duplicar la velocidad de ataque del diccionario) si está seguro de que la contraseña que está buscando solo contiene caracteres latinos. La descripción simple de lo que significan todos estos grupos de mutación se da a continuación:

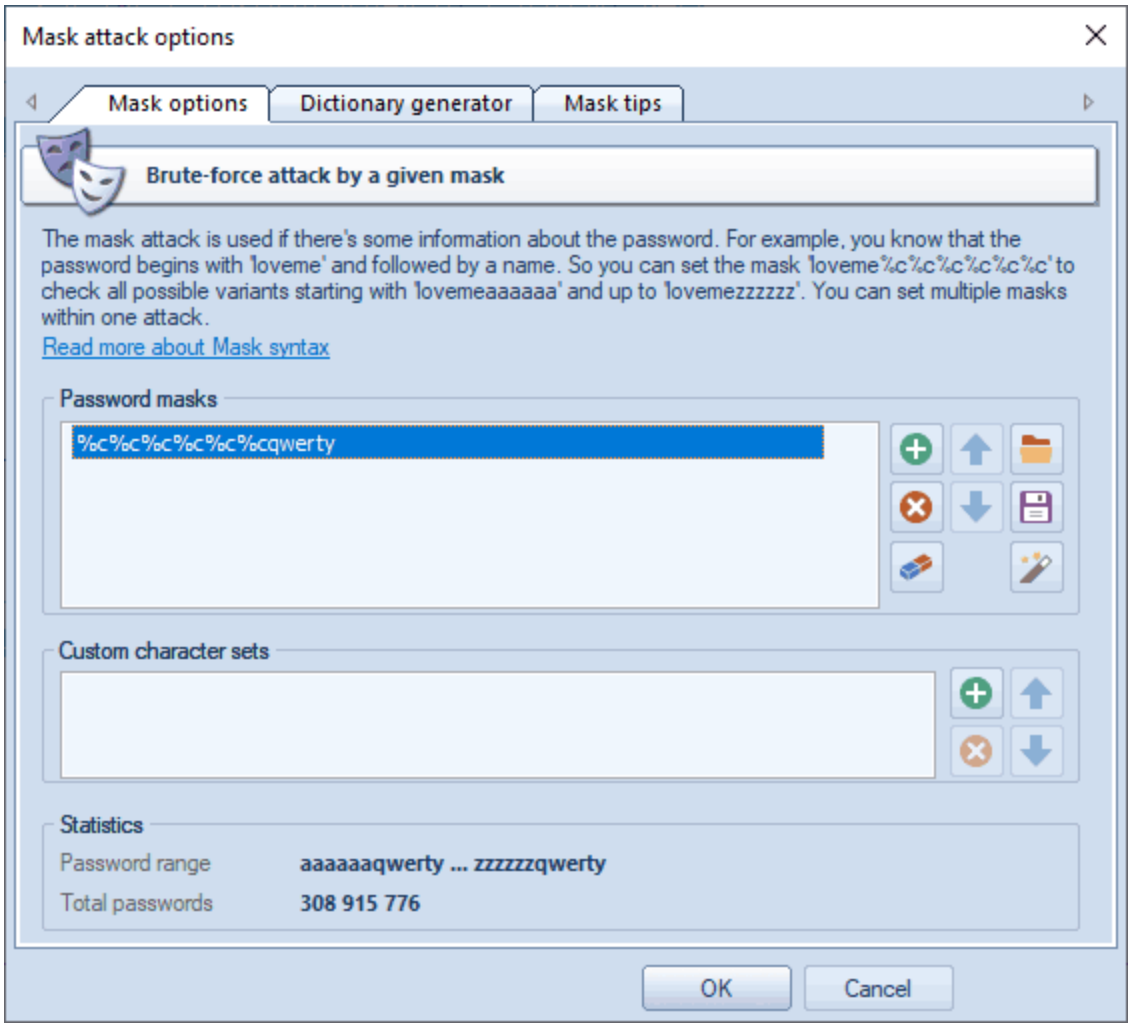
Nombre del grupo	Descripción	Ejemplos (para la palabra '**contraseña**')	Comentarios
Mayúscula en Caracter	Comprueba las combinaciones de mayúsculas y minúsculas de la palabra de entrada.	Password, PasswordD, PaSsWoRd	El nivel máximo (fuerte) del grupo de mutación NO genera todas las combinaciones de casos posibles de palabras de entrada. Para comprobar todas las variantes de casos posibles, considere la posibilidad de utilizar Ataque de diccionario híbrido (regla **aN**)
Anexar/anteponer dígitos	Agrega dígitos al principio o al final de la palabra.	password99, 2Password, PASSWORD3	El nivel máximo agrega 2 dígitos.
Cabeza y cola	Casi lo mismo que el anterior, pero agrega o antepone palabras, abreviaturas, caracteres, combinaciones de teclado, etc.	#Password#, password12345, 4everPASSWORD, Passwordqwerty	
l33t	Crea diferentes combinaciones usando lenguage leet.	p@ssword, P@$$w0rd, P@$$W0RD	
Abreviatura	Convierte varias combinaciones de caracteres (si la palabra inicial contiene alguna) en abreviaturas.	ihateyou -> ih8you, Ih8u	
Duplicados e inverso	Revertir, duplicar la palabra, etc.	drowssap, passwordpassword, PasswordDrowssap	
Vocales y consonantes	Muta vocales y consonantes (solo caracteres en inglés).	Psswrd, PaSSWoRD, pAsswOrd	
Salto de carácter	Omite un solo carácter de la palabra original.	assword, Passwrd, Pasword	
Intercambio de caracteres	Intercambia dos caracteres adyacentes.	apssword, Passowrd	
Duplicado de caracteres	Duplica caracteres.	ppasword, ppaasswwoorrdd, Passwordddd	
Delimitadores	Separa los caracteres con delimitadores.	p.a.s.s.w.o.r.d, P-a-s-s-w-o-r-d	El nivel máximo utiliza 10 delimitadores.
Fechas	Agrega fechas al final de la palabra.	Password2010, password1980	Aunque el motor de mutación puede generar variaciones más complicadas (por ejemplo, password03171998 o Password19710830), esta característica si se desactiva aquí incluso en el nivel máximo de mutación.
Conversión Oem	Convierte la palabra inglesa en otro idioma y viceversa utilizando una distribución de teclado alternativa (segundo idioma del sistema operativo).	Si su sistema operativo tiene 2 idiomas instalados (que sea inglés y ruso), el programa	El programa funciona correctamente para 2 o incluso más idiomas. Por lo tanto, si tiene 5 idiomas instalados localmente

Nombre del grupo	Descripción	Ejemplos (para la palabra '**contraseña**')	Comentarios
		convertirá la palabra inicial **contraseña** en ruso **зфыыцщкв**, y el ruso **пароль** se convertirá en gfhjkm.	(incluido el inglés), habrá 4 encombinaciones diferentes de la palabra de entrada.
Cambio de palabras	Estúpidamente desplaza todos los caracteres de la palabra a la derecha o a la izquierda.	asswordp, dpasswor	
Sustitución de caracteres	Reemplaza un carácter de la palabra inicial.	aoassword, passqord	Esta es una regla bastante útil asumiendo el hecho de que los caracteres para la sustitución se toman de una tabla especial. Por ejemplo, el carácter 's' se sustituirá por los siguientes: 'a', 'w', 'e', 'd', 'x', 'z'. Puede notar que todos estos caracteres se encuentran cerca de 's' en cualquier teclado qwerty.
Longitud truncada	Trunca la longitud de la palabra para sondear todas las combinaciones de longitud posibles.	passwor, passwo, Pass	

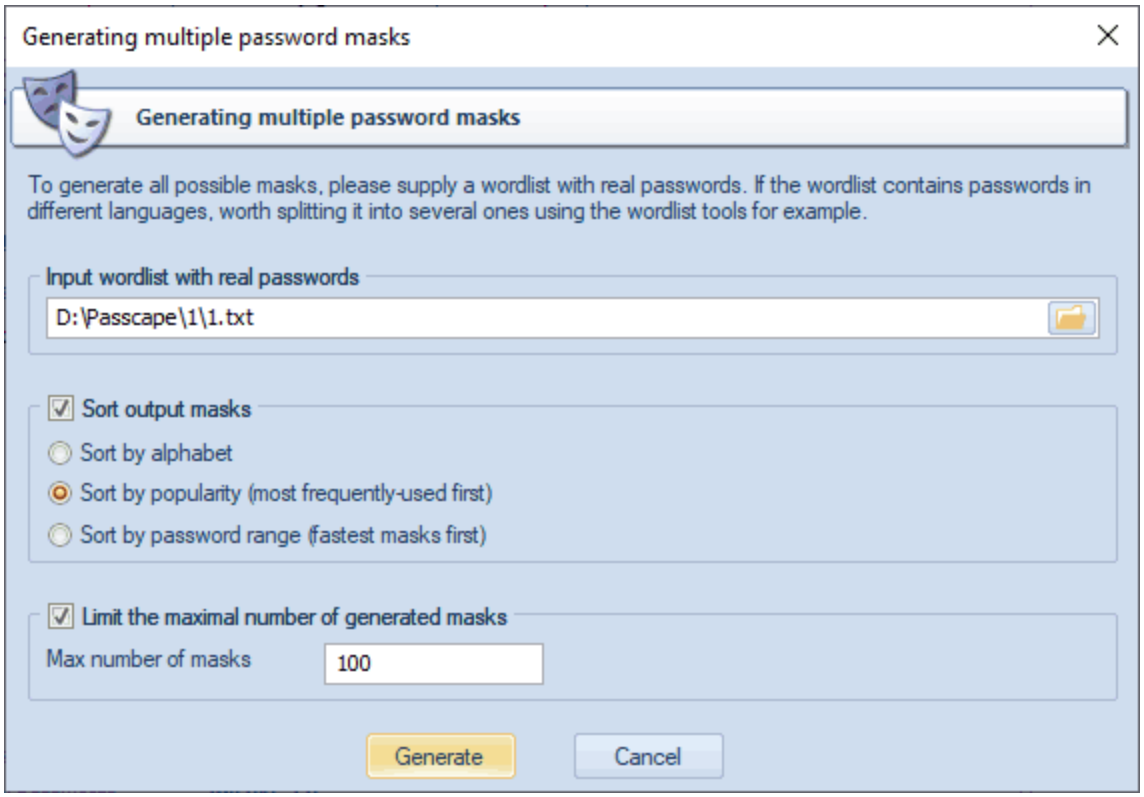
2.8.2.6 Ataque de máscara

Ataque de máscara es una herramienta insustituible cuando conoces un fragmento de la contraseña o tienes algún detalle específico al respecto. Por ejemplo, cuando sabe que la contraseña consta de 12 caracteres y termina con el qwerty, es obvio que buscar en todo el rango de contraseñas de 12 caracteres no es razonable. Todo lo que se requeriría en este caso es elegir los primeros 6 caracteres de la contraseña buscada. Para eso está el ataque con máscara.

En nuestro caso, podríamos definir la siguiente máscara: **%c%c%c%c%c%cqwerty**. Eso significa que el programa verificaría en serie las siguientes combinaciones: aaaaaaqwerty .. zzzzzzqwerty. Si la contraseña original es 'secretqwerty', llega perfectamente a nuestro rango.



El grupo de opciones máscaras de contraseña tiene como objetivo establecer una máscara (o varias), que se utilizarán para generar contraseñas por. En la mayoría de los casos, si conoce una parte de la contraseña, basta con especificar una sola máscara. Cuando se selecciona una máscara, el grupo de estadísticas muestra el rango de contraseñas de salida y el número de contraseñas generadas por esta máscara. Puede guardar sus máscaras en el disco para usarlo en otro proyecto, por ejemplo. El programa también le permite generar diccionarios mediante máscaras dadas.
Supongamos que tiene una lista de contraseñas descifradas y desea generar plantillas de máscara a partir de estas contraseñas. Nada más fácil. Ejecute el generador de máscaras  y muestre la ruta a su lista de contraseñas allí. Puede ordenar las máscaras resultantes alfabéticamente, popularidad o por rango de búsqueda (el más rápido es el primero)



La sintaxis de la máscara es bastante trivial y consiste en caracteres o conjuntos estáticos (no modificables) y dinámicos (modificables). Los caracteres/conjuntos dinámicos siempre tienen un % a la vez Por ejemplo, si establece la máscara secret%d(1-100), el programa generará 100 contraseñas (secret1, secret2: secret100).

Windows Password Recovery admite los siguientes conjuntos de máscaras dinámicas:

- %c caracteres latinos en minúsculas (a.. z), 26 símbolos
- %C caracteres latinos en mayúsculas (A.. Z), 26 símbolos
- %# conjunto completo de caracteres especiales (!.. ~ espacio), total de 33 símbolos
- %@ pequeño conjunto de caracteres especiales (!@#$%^&*()-_+= espacio), 15 símbolos.
- %? todos los caracteres imprimibles con códigos ASCII de 32..127
- %* todos los caracteres ASCII (códigos 1 a 255)
- %d un dígito (0..9)
- %d(x-y) números entre x e y inclusive
- %r(x-y) caracteres definidos por el usuario con códigos UNICODE serie entre x e y
- %r(x1-y1,x2-y2...xn-yn) conjunto de varias secuencias no superpuestas de caracteres UNICODE.
- %[1..9] un carácter del conjunto de caracteres definido por el usuario 1..9
- %[1..9](min-max) rango de longitud variable definido por el usuario (de mínimo a máximo). Puedes configurar hasta 9 tus propios juegos de caracteres personalizados.
- %% carácter estático independiente %

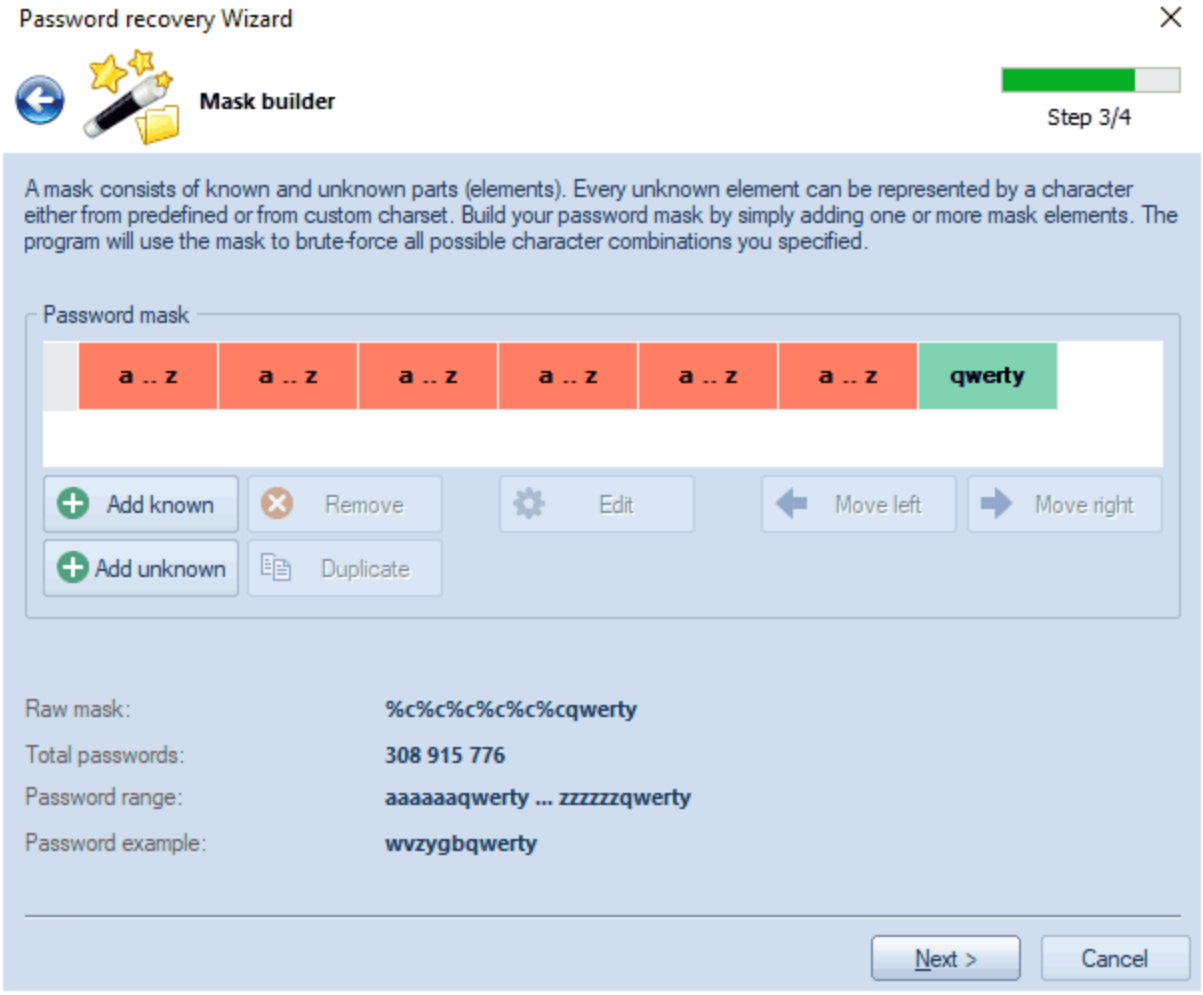
Examples:
test%d - generará el rango de contraseñas test0.. test9, 10 contraseñas en total
test%d(1980-2007) - test1980 .. test2007, 28 contraseñas

test%r(0x0600-0x06ff) - 256 contraseñas con caracteres árabes al final
%#test%# - _prueba_.. ~test~, 1089 contraseñas
admin%1(1-5) - admina.. adminzzzzz, donde %1 es el conjunto de caracteres definido por el usuario 1 (a.. z)
%1%1%1pin%2%2%2 - aaapin000 .. zzzpin999, %1 es el juego de caracteres de usuario a.. z y %2 es el segundo conjunto de caracteres definido por el usuario que contiene los caracteres 0..9

Al cambiar a la pestaña **Generador de diccionarios**, puede generar su propio diccionario mediante una máscara determinada y guardarlo en el disco. Esta función solo está disponible en la edición avanzada del programa.

La tercera pestaña de las opciones de máscara contiene una breve descripción de la sintaxis de la máscara y un par de ejemplos simples.

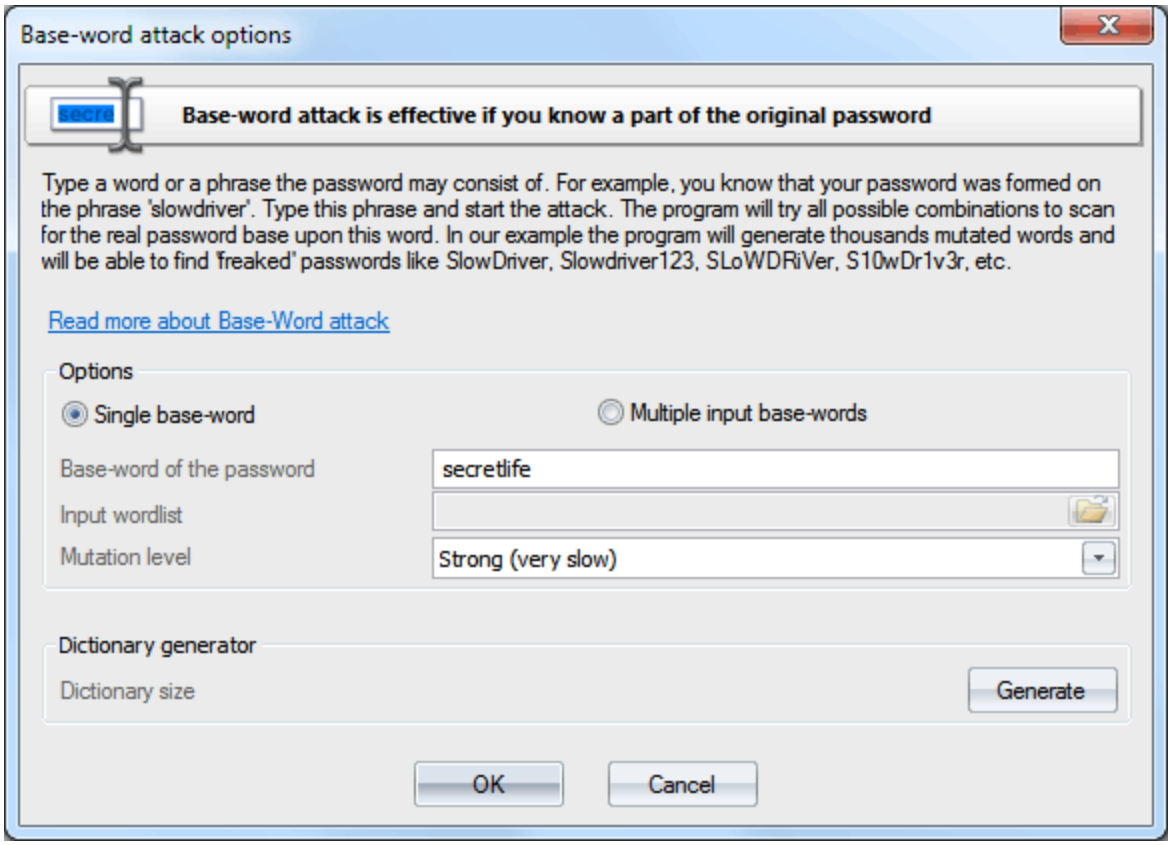
Si se siente perdido y harto de todas estas cosas, use el Mask Builder (en Password Recovery Wizard) que tiene una interfaz gráfica mucho más fácil de usar.



2.8.2.7 Ataque de palabra base

El ataque de palabra base (desarrollado por Passcape) es en muchos aspectos similar al ataque de máscara. Sin embargo, aquí no es necesario configurar la sintaxis; simplemente ingrese la palabra clave, que supuestamente era la palabra base para la contraseña. Es una herramienta de recuperación insustituible cuando conoce una parte de la contraseña o su componente básico. Normalmente, tales casos se disponen a usar ataque de máscara; sin embargo, no siempre permite hacer frente a la tarea establecida. Supongamos que nuestra contraseña fuera '**S10wDr1v3r**'. Tratar de recuperar una contraseña tan complicada utilizando un ataque de fuerza bruta sería un trabajo ingrato, incluso si está bastante seguro de que se basa en la palabra '**slowdriver**'. Estos son los casos en los que el ataque de la palabra base te rescatará.

Con esta herramienta, el programa intentará recuperar la contraseña original, probando todas las combinaciones posibles fundadas en 15 grupos de reglas (un total de más de 150 reglas). Si ingresa '*slowdriver*' en el campo, verá que el programa ha generado varios miles de combinaciones diferentes en esta frase, y una de esas combinaciones podría coincidir con nuestra contraseña.



Si la longitud de la frase de entrada excede de 8-10 caracteres, la mutación puede tomar un tiempo significativo. Si recuerda la contraseña original con precisión y simplemente ha olvidado la secuencia de los caracteres en mayúsculas y minúsculas en ella, puede seleccionar la opción *'Mutar solo mayúsculas y minúsculas'*. Con esta opción seleccionada, el programa generará contraseñas con todas las combinaciones posibles de caracteres en mayúsculas y minúsculas, un total de 2^n contraseñas, donde n - es la longitud de la contraseña. Por ejemplo, para la contraseña '*slowdriver*' el programa generará 2^10=1024 combinaciones diferentes para cada distribución de teclado instalada en su

computadora. También puede generar un diccionario sobre esas mutaciones y guardarlo en un disco (disponible no en todas las ediciones).

Tenga en cuenta que si la longitud de su contraseña supera los 15-16 caracteres, puede llevar bastante tiempo preparar (mutar) la contraseña para el ataque.

En Windows Password Recovery versión 9.5, la recuperación de palabras base se dividió en 2 modos: palabra de entrada única y muchas palabras de entrada. El modo de entradas múltiples actúa como el ataque del diccionario con mutaciones máximas activadas, pero genera muchas más contraseñas (incluso si el nivel de mutación del ataque de palabras base se establece en '*Débil*'), lo que puede ser útil en una determinada situación.

2.8.2.8 Ataque de diccionario combinado

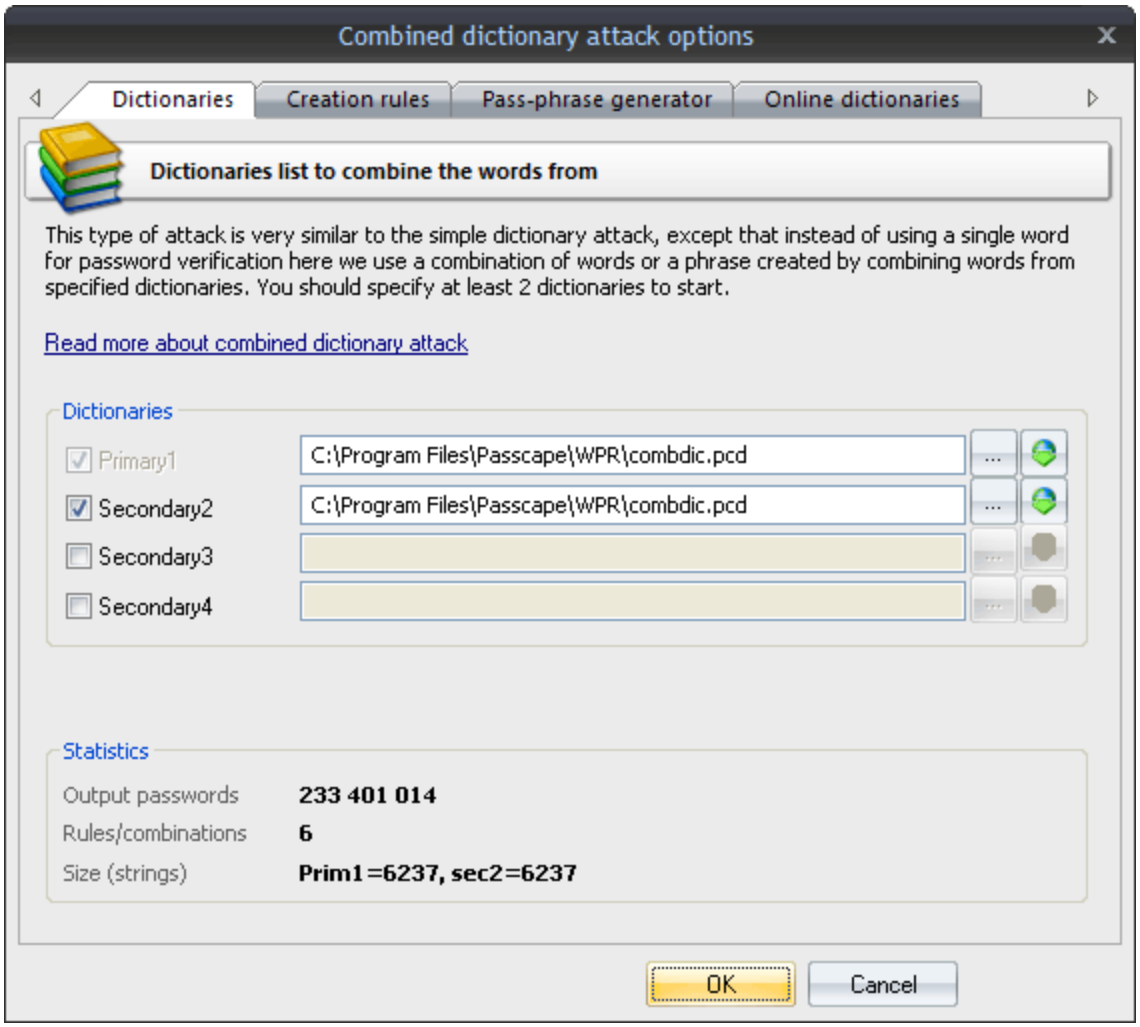
El ataque de diccionario combinado (desarrollado por Passcape Software) es excelente para recuperar contraseñas que constan de 2,3 e incluso 4 palabras. Este tipo de ataque a contraseñas difíciles y compuestas es muy similar al ataque de diccionario simple, excepto que en lugar de usar una sola palabra para la verificación de contraseñas aquí usamos una combinación de palabras o una frase creada combinando palabras de diccionarios específicos. Para utilizar con éxito este ataque, establezca al menos dos diccionarios y las reglas para generar contraseñas. Puede configurar los diccionarios regulares utilizados en el ataque de diccionario simple, pero se recomienda usar diccionarios bastante pequeños con las palabras más comunes. Los diccionarios perfectos para el ataque combinado de frases de contraseña son aquellos que tienen diferentes formas de palabras en ellos; por ejemplo, saltar, saltar, saltar, saltar.

El ataque combinado establece un cierto límite para el número de diccionarios que se pueden usar; eso no es más de 4. Por lo tanto, la limitación general de este ataque es que solo se pueden recuperar frases de contraseña de no más de 4 palabras utilizando este ataque.

Otro inconveniente esencial es la amplia gama de frases generadas. Y, como consecuencia, el aumento proporcional del tiempo dedicado a la validación de una contraseña. Tenga en cuenta que al generar contraseñas que constan de 3 o 4 palabras, el proceso de generación lleva un tiempo considerable.

Si encontrar el diccionario adecuado es difícil, no te preocupes. El software viene con un diccionario especial para el ataque combinado. También puede aprovechar los Diccionarios en linea en la pestaña o el botón correspondiente para descargar dichos diccionarios desde el sitio web de Passcape.

Dictionaries



La forma en que funciona el ataque combinado es realmente simple. Por ejemplo, si ha establecido dos diccionarios, el programa generará las contraseñas de la siguiente manera: tomará la primera palabra del primer diccionario y la pegará con la primera palabra del segundo diccionario, luego con la segunda palabra, y así sucesivamente hasta el final. Luego comprueba la segunda palabra del primer diccionario y sigue la misma ruta, y así sucesivamente.

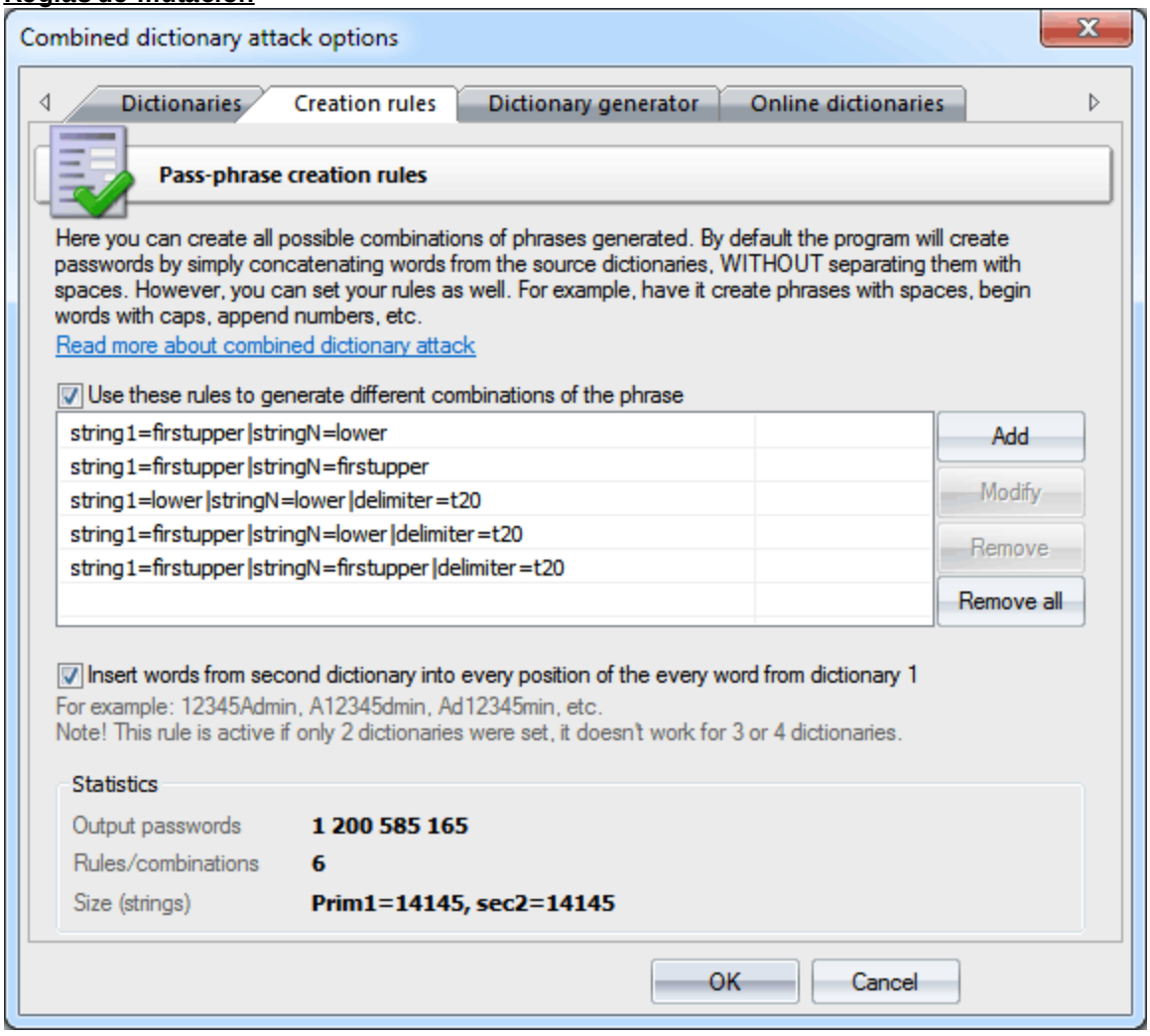
Para entender cómo funciona el ataque combinado, echemos un vistazo a un par de ejemplos de generación de contraseñas que involucran, en el primer caso, el mismo diccionario y en el segundo caso, dos diferentes.

1. Supongamos que tenemos un solo diccionario con tres palabras: acción, malo y computadora. Estableceremos este diccionario como dos fuentes originales: diccionario primario y diccionario secundario2 (ver la figura). Una vez procesados estos diccionarios, a la salida tenemos las siguientes frases (se utilizarán al comprobar la contraseña buscada):
'actionaction', 'actionbad', 'actioncomputer'
'badaction', 'badbad', 'badcomputer'
'computeractio', 'computerbad', 'computercomputer'.
9 frases en total.

2. En el segundo caso, tenemos dos diccionarios diferentes. Por ejemplo, el primer diccionario consta de tres palabras: acción, malo y computadora. El segundo también tiene tres palabras: fecha, águila, fracaso. En este caso, vamos a tener las siguientes frases:
'actiondate', 'actioneagle', 'actionfail'
'baddate', 'badeagle', 'badfail'
'computerdate', 'computereagle', 'computerfail'.

El ejemplo es sencillo pero demostrativo. La idea es que para múltiples fuentes se puede utilizar con éxito tanto un solo diccionario como varios. Todo depende de tu imaginación. El último ejemplo muestra que se debe prestar especial atención al orden de los diccionarios si son diferentes. El orden de las palabras en las frases a crear depende directamente del orden de los diccionarios de origen. En nuestro segundo ejemplo, si intercambiamos los diccionarios primario y secundario, a la salida obtendremos un conjunto de frases completamente diferente.

Reglas de mutación

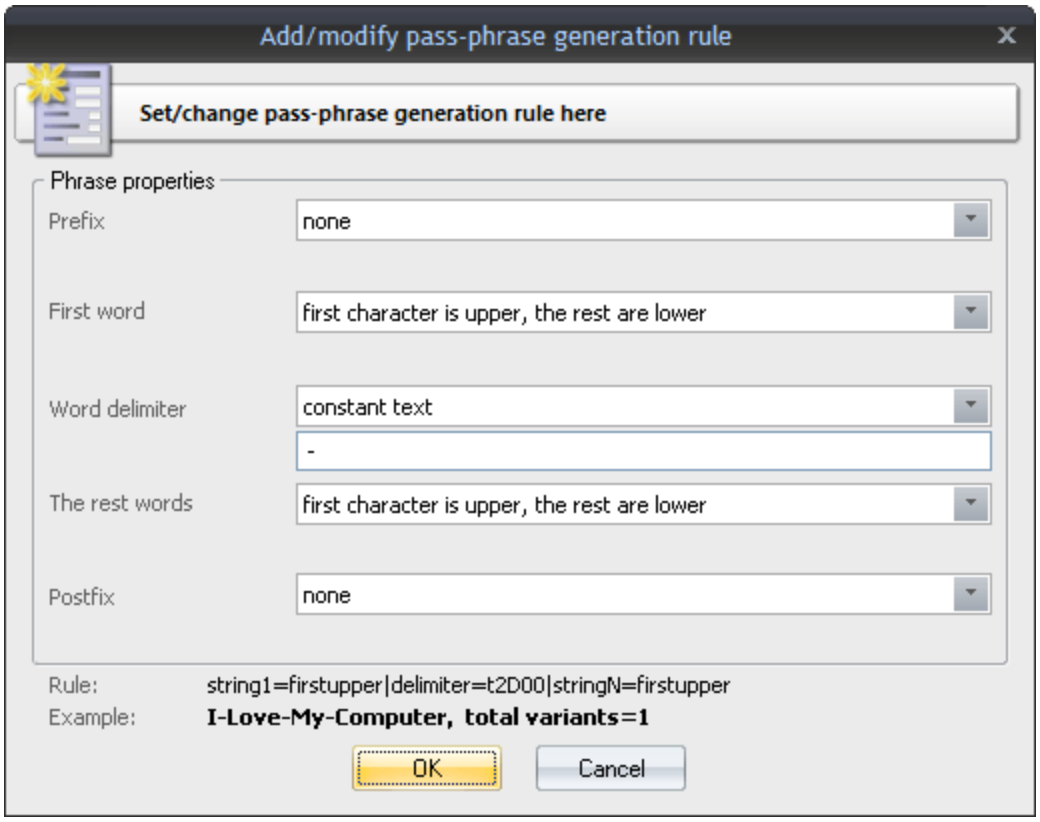


Las contraseñas creadas por el ataque combinado se generan de acuerdo con reglas especiales que se establecerán en la segunda pestaña. De forma predeterminada, cuando las reglas de generación de contraseñas están deshabilitadas, el programa genera contraseñas simplemente pegando las palabras

de los diccionarios, sin separarlas con un espacio. Por ejemplo, de las dos palabras que son 'mi' y 'computadora', obtendrá 'mi computadora'.

Si se establece la opción de inserción de palabras, el programa también crea contraseñas insertando palabras del segundo diccionario en cada posición de la palabra del diccionario 1. Por ejemplo, si la palabra del primer diccionario es Admin, y la palabra del segundo diccionario es **12345**, el programa generará las siguientes contraseñas:
12345Admin
A12345dmin
Ad12345min
Adm12345in
Admi12345n
Y así sucesivamente para todas las palabras del segundo diccionario. Luego va otra palabra del diccionario 1, etc. La opción está activa si solo se establecieron 2 diccionarios.

Las reglas de generación se hacen para ampliar las opciones de búsqueda de contraseñas. Por ejemplo: Mycomputer, MyComputer, MY COMPUTER, my-computer, etc. Existen reglas especiales disponibles para este propósito; no tiene que conocer la sintaxis de ellos, ya que el cuadro de diálogo de creación de reglas de mutación es simple e intuitivo.



Cada regla de mutación consta de cinco elementos:
1. *Prefijo* - texto que aparecerá antes de cada frase. Este elemento puede ser un carácter, una cadena de texto sin formato, un dígito entre 0 y 9 o un número. Por ejemplo, si establece un prefijo de un dígito, las frases creadas con estas reglas se verán de la siguiente manera: '0 aaa bbb', '1 aaa bbb': '9 aaa bbb'.
2. *Primera palabra* - la acción que se realizará sobre la primera palabra de cada frase. Solo hay cuatro opciones. A saber: dejar intacto como está en el diccionario, convertir todos los caracteres a

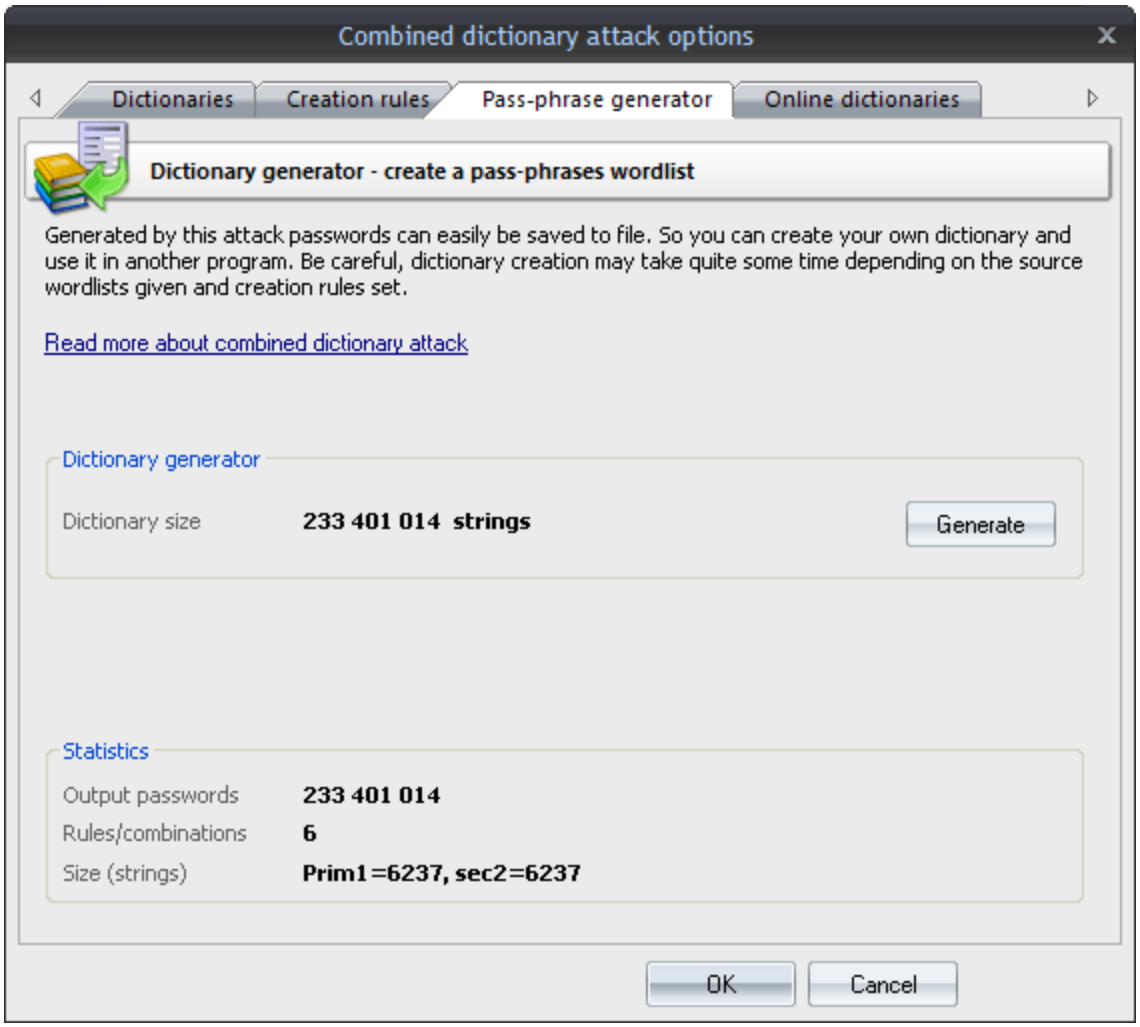
minúsculas, convertir todos los caracteres a mayúsculas o poner en mayúscula solo la primera letra de la palabra.

3. *Separador de palabras* - Puede estar ausente. Entonces todas las palabras serán concatenadas. Ejemplo: 'aaabbb', 'aaaccc', 'aaaddd', etc. De lo contrario, puede establecer un separador personalizado; por ejemplo, el carácter '-': 'aaa-bbb', 'aaa-ccc', 'aaa-ddd'. O puede establecer un rango de caracteres.
4. *Otras palabras* - Con este atributo, de manera similar a 2., puede establecer reglas para las otras palabras de una frase.
5. *Postfix* - texto que finalizará cada frase. Por ejemplo, si establece Postfix en '?' o '?', todas las frases creadas con esta regla tendrán el signo de interrogación al final.

Ciertamente, cuantas más reglas de generación de contraseñas establezca, más posibilidades tendrá de elegir la contraseña correcta. Pero, por otro lado, más tiempo habrás dedicado al ataque.

El grupo 'Estadísticas' muestra el tamaño promedio y recomendado de un diccionario, el número de palabras en los diccionarios de origen, el número total de contraseñas que se generan y otra información útil.

Generador de diccionarios



La tercera pestaña de opciones sirve para crear diccionarios combinados basados en ataques (disponibles no para todas las ediciones).

También puede descargar módulos de diccionario adicionales desde el sitio web de Passcape Software.

2.8.2.9 Ataque de frase de contraseña

Cada vez más usuarios optan por componer sus frases de contraseña de frases enteras, pasajes de poemas, aforismos de películas, aforismos latinos, etc. Intentar recuperar tales contraseñas utilizando las técnicas tradicionales es impensable, incluso con la referencia al avance de la potencia informática de las computadoras modernas. Por lo tanto, la ayuda de recuperación viene con el ataque de frase predefinido y conocido.

El ataque de frase de contraseña es muy similar al ataque de diccionario simple, excepto que aquí la búsqueda de contraseñas va frase por frase en lugar de ir palabra por palabra. La idea principal del ataque es adivinar la contraseña correcta buscando a través de expresiones, frases y combinaciones de palabras predefinidas de uso frecuente.

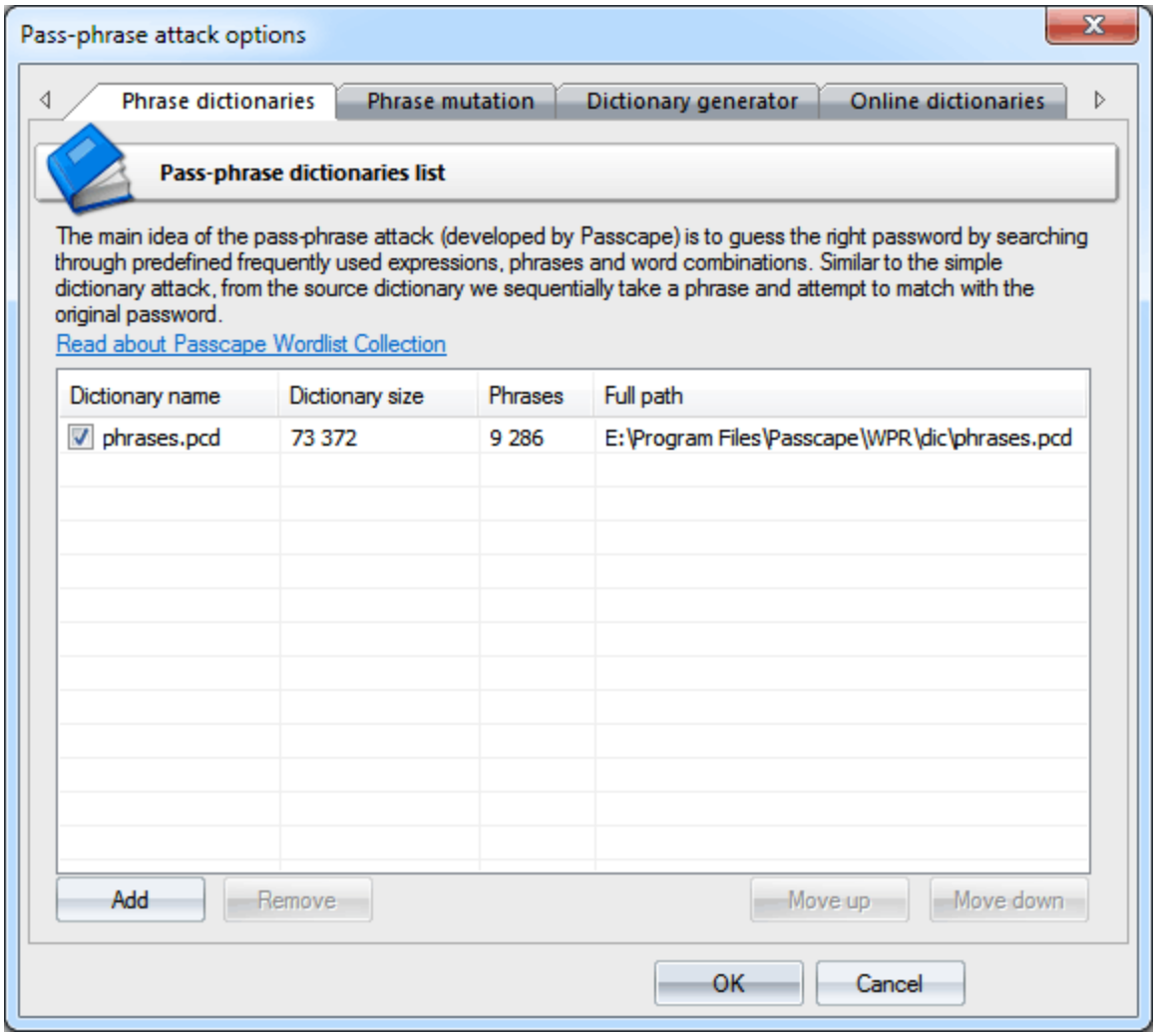
Por ejemplo, si la contraseña buscada está hecha de la frase generalizada 'Ser o no ser', es obvio que este es el único ataque que tiene la virtud de hacer frente a dicha contraseña. Para hacer eso, debe especificar un diccionario especial de frases de contraseña. Un diccionario de frases simple viene con el software, pero también puede descargar los diccionarios en linea que fueron compilados específicamente para este ataque.

No sería una sobreestimación decir que el 99 por ciento del éxito en la recuperación de una contraseña con un ataque de diccionario depende de la calidad de los diccionarios. Lo más probable es que esa sea la razón por la que este tipo de ataques no aparecen en casi ningún descifrador de contraseñas. Passcape Software permite utilizar todo un conjunto de diccionarios online y offline (totalmente más de 500 MB) compilados especialmente para este tipo de ataques.

Por ejemplo, muchos usuarios hacen sus contraseñas de extractos de sus canciones o bandas de música favoritas. Es por eso que hemos creado conjuntos de frases clave especiales y únicas (¡no encontrarás nada así en ninguna parte de la red!) orientadas a la música. También hay un conjunto bíblico, frases de películas, proverbios, etc.

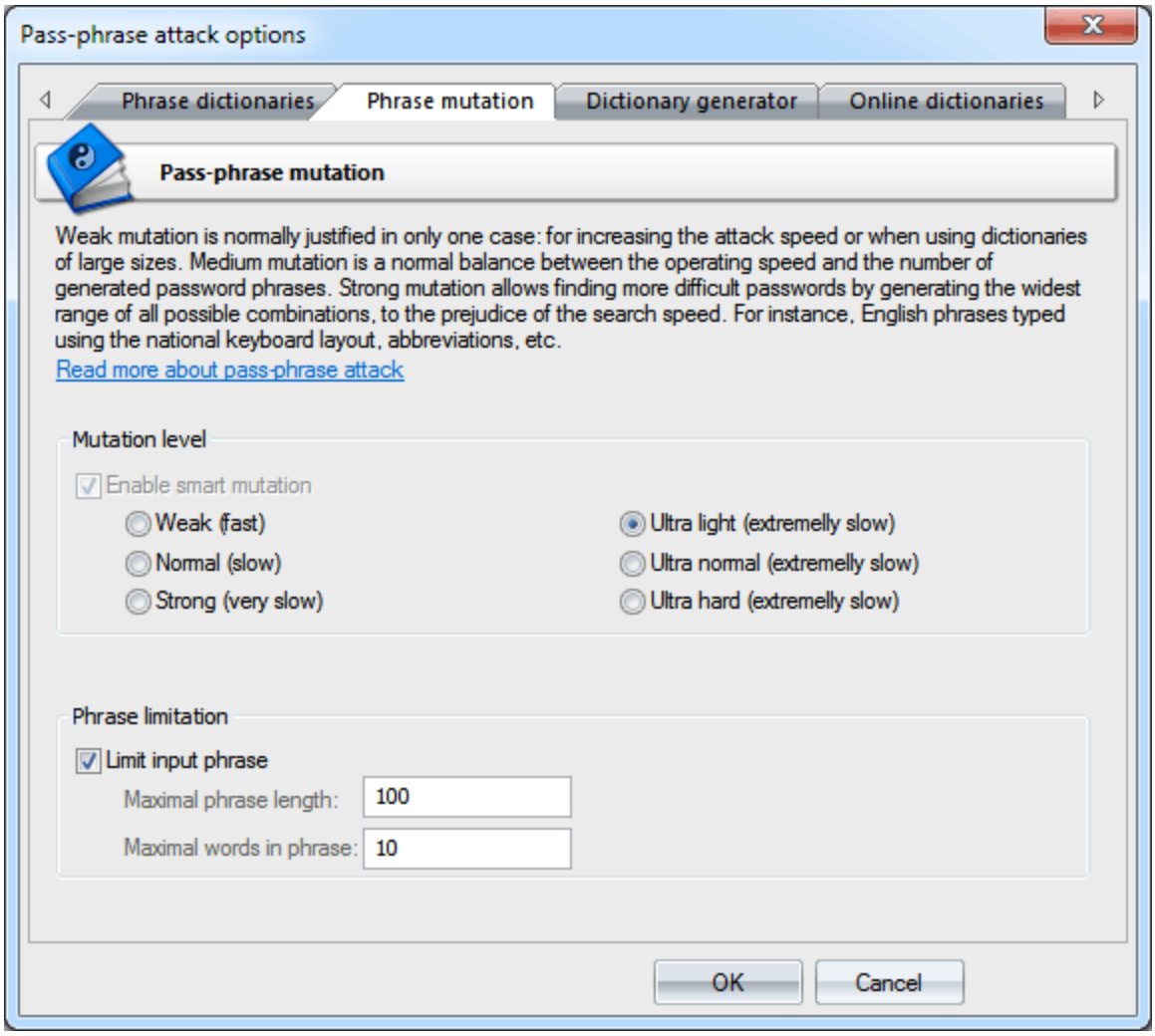
Windows Password Recovery viene con un breve diccionario de frases y aforismos.

Phrase dictionaries



Las opciones de ataque de contraseña-frase repiten casi por completo las opciones de ataque de diccionario simples: aquí, también debe seleccionar uno o varios diccionarios para la fuente de la frase, también permite cargar diccionarios adicionales desde el sitio web de Passcape, y tiene la misma forma de establecer reglas de mutación de frases (creando opciones alternativas).

Mutación de frase



Vale la pena decir más sobre la mutación, ya que como debería haber sabido, la mutación fuerte aumenta significativamente las posibilidades de una recuperación exitosa. La mutación débil normalmente se justifica en un solo caso: para aumentar la velocidad de ataque o cuando se utilizan diccionarios de grandes tamaños. La mutación media es un equilibrio normal entre la velocidad de funcionamiento y el número de frases de contraseña generadas. La mutación fuerte permite encontrar contraseñas más difíciles al generar la gama más amplia de todas las combinaciones posibles, en perjuicio de la velocidad de búsqueda. Cuanto mayor sea el nivel de mutación, más contraseñas cubrirá el ataque. Por ejemplo, frases en inglés mecanografilladas usando la distribución del teclado nacional, abreviaturas, etc.

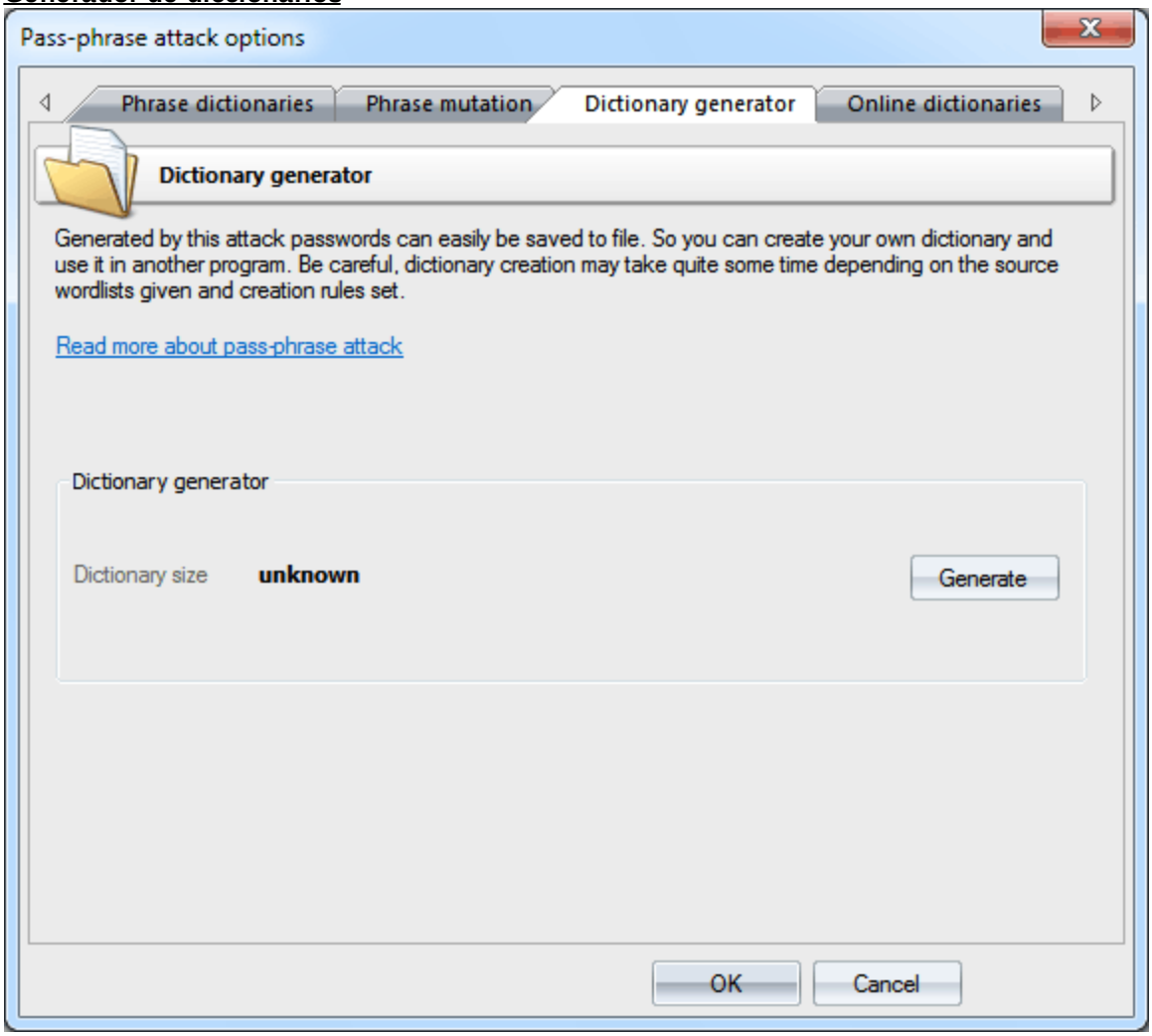
Diferencia importante en los niveles de mutación:

- Débil - mutaciones más simples y rápidas.
- Normal: lo mismo que Débil, pero genera varias mutaciones adicionales y combinaciones de casos.
- Fuerte: lo mismo que normal más mutaciones y contraseñas nacionales (de acuerdo con las distribuciones de teclado instaladas, si las hay).
- Ultra ligero: esta es una mutación de 2 pasos porque cada contraseña generada en modo débil pasa por la segunda ronda de mutación (una utilizada en el modo débil del ataque de diccionario simple).
- Ultra normal - mutación de 2 pasos. Cada contraseña generada en el modo Normal se utiliza como fuente para generar combinaciones adicionales mediante la implementación de un nivel de mutación Normal adicional.

- Ultra duro: cada contraseña generada en modo fuerte se utiliza como fuente para generar combinaciones adicionales mediante el uso de un nivel de mutación fuerte adicional.

¡Ten cuidado! Los modos Ultra generan una gran cantidad de contraseñas, por lo que el ataque puede ejecutarse extremadamente lento. Para acelerar el ataque, considere la posibilidad de configurar límites de frases de entrada. Por ejemplo, puede limitar las frases de entrada a 10 palabras y 100 caracteres.

Generador de diccionarios



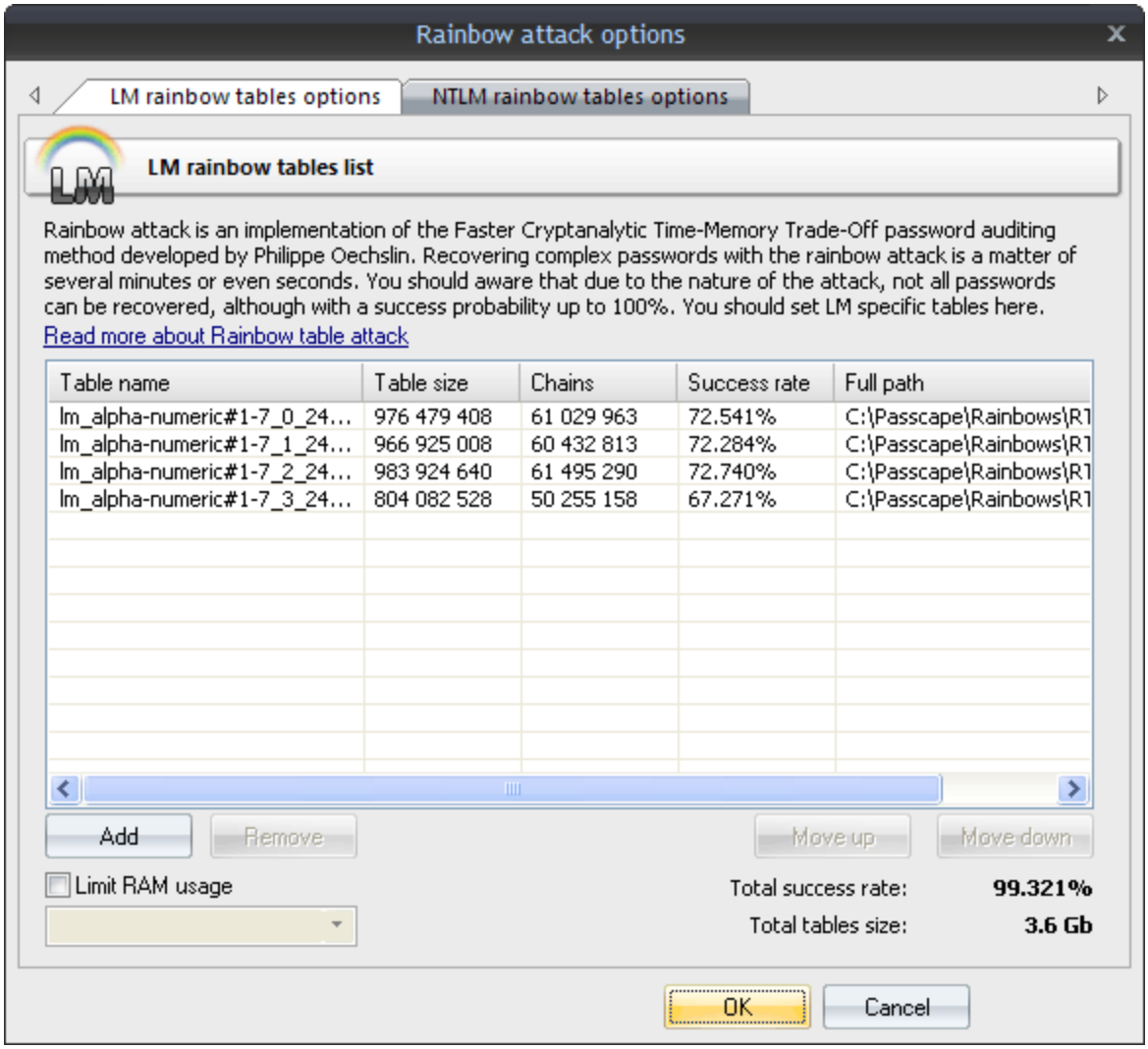
La tercera pestaña se utiliza para crear diccionarios de frases de contraseña.

2.8.2.10 Ataque de tablas Rainbow

Una tabla Rainbow es una tabla de búsqueda que ofrece una compensación de memoria de tiempo utilizada en la recuperación de la contraseña de texto sin formato de un hash de contraseña generado por una función hash, por ejemplo, contraseñas de Windows.

Esta es una herramienta de auditoría de contraseñas bastante sofisticada. Este método fue desarrollado por Philippe Oechslin para la recuperación rápida de la contraseña utilizando tablas precalculadas.

Basta con decir que la contraseña buscada se puede recuperar en cuestión de minutos o incluso segundos.



El programa es compatible con el estándar *.rt, indexado *.rti y tablas híbridas. También se admite multithreading.

Hay que mencionar que rainbow attack no garantiza la recuperación de todas las contraseñas, pero la probabilidad de recuperación es cercana al 100%, dependiendo de las tablas que tengas.

Se puede implementar una tabla de arco iris específica para el hash para el que se creó. Eg. Las tablas específicas de LM deben usarse solo para romper hashes de LM.

Las opciones de ataque permiten limitar la cantidad de RAM que puede utilizar el ataque cuando se utilizan equipos antiguos (el ataque supone utilizar grandes volúmenes de RAM para sus cálculos).

2.8.2.11 Ataque de diccionario híbrido

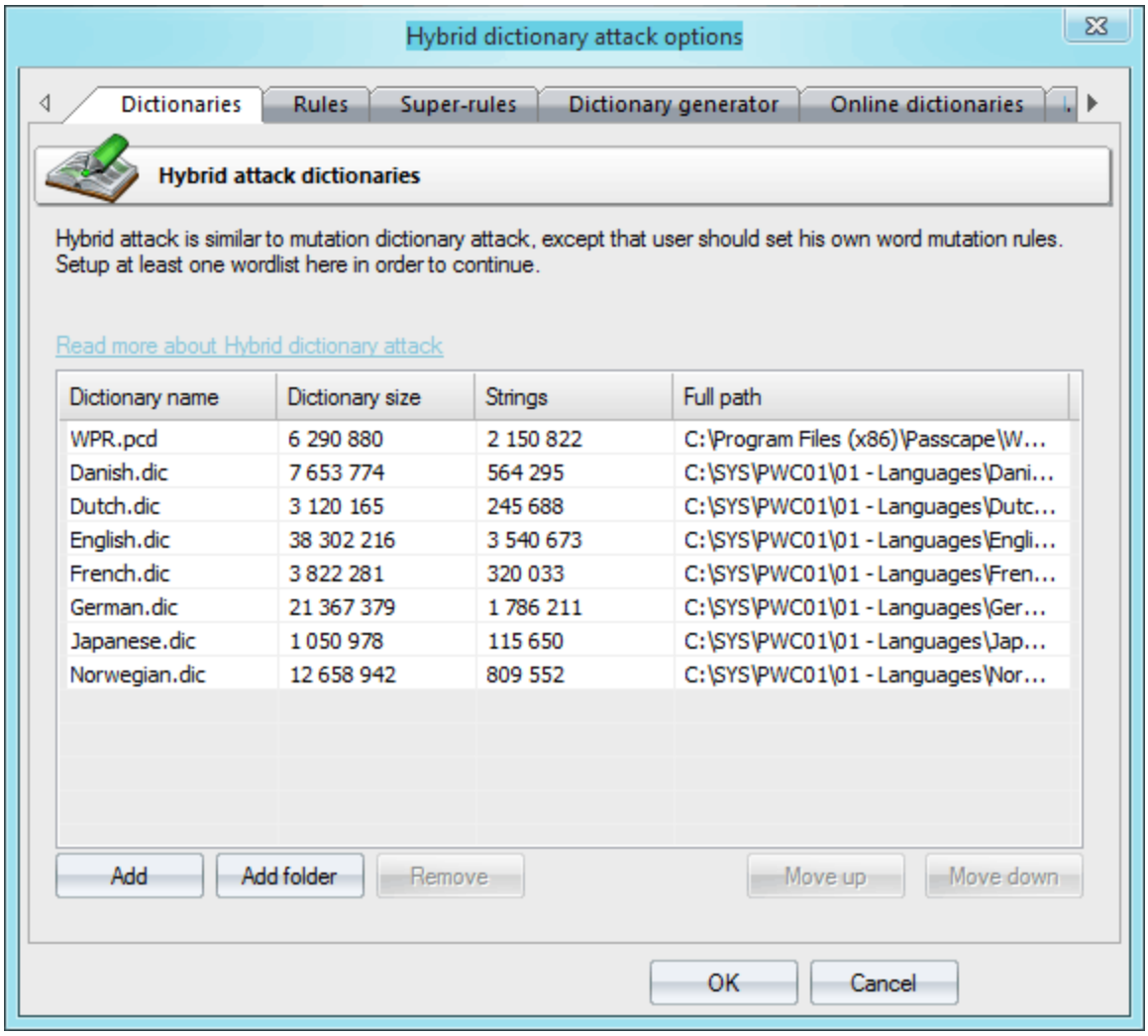
Ataque de diccionario híbrido es una forma de ataque de diccionario simple. Sin embargo, a diferencia de este último, el ataque híbrido permite al usuario establecer sus propias reglas de mutación de palabras (variación) e intentar validar las palabras modificadas como contraseñas de origen. Por ejemplo, el usuario podría poner en mayúscula la primera letra de una contraseña que se está validando, agregar '2' a ella, reemplazar el número 8 con la letra B, O con 0, etc.

Las acciones, realizadas en palabras de origen del diccionario, se denominan reglas. Se pueden aplicar varias reglas a cada palabra de origen. La sintaxis de definición de regla es compatible con el software John the Ripper y PasswordsPro. El autor de este último ha proporcionado amablemente un conjunto extendido de reglas, ligeramente editado, que viene con el kit de distribución para Windows Password Recovery.

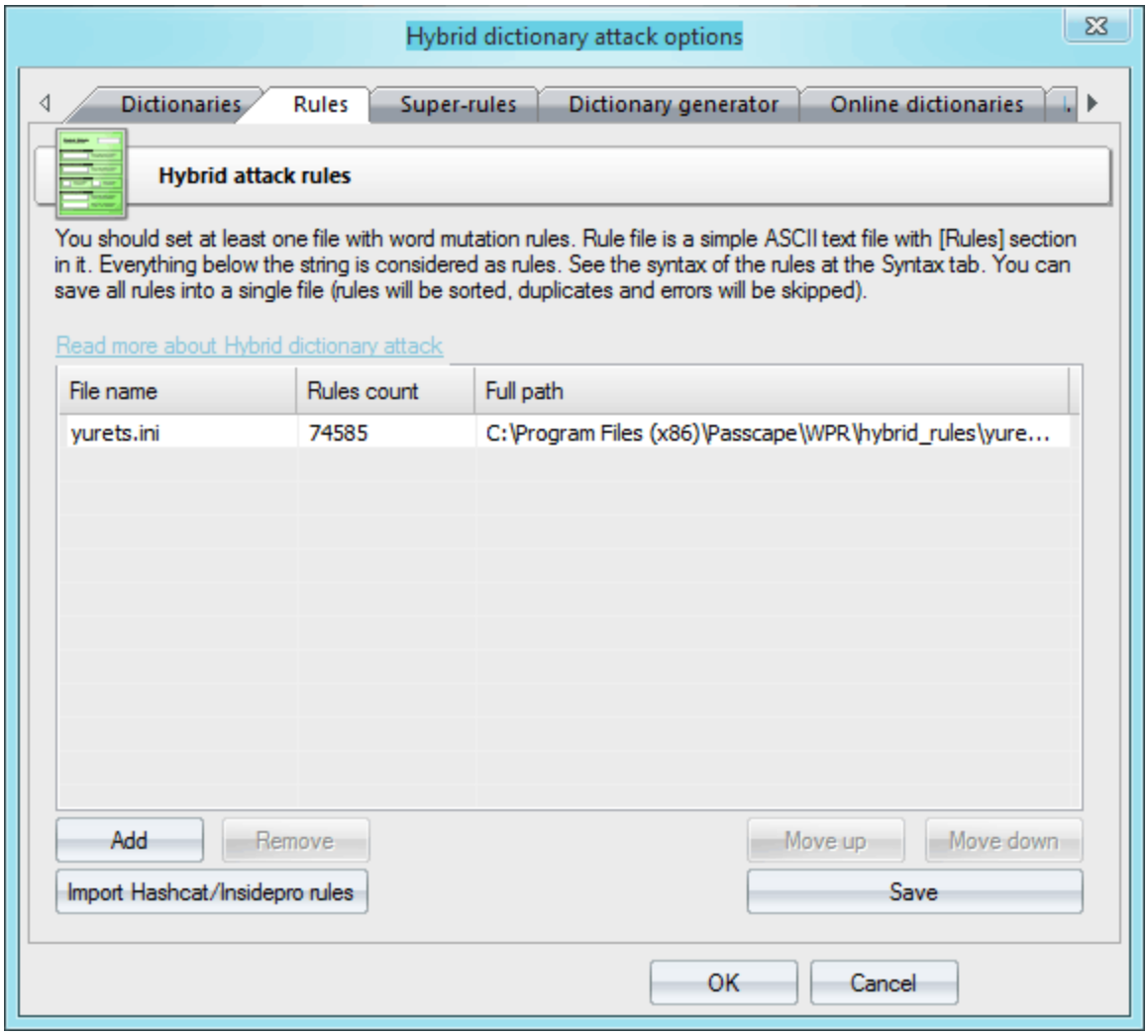
La configuración de ataque del diccionario híbrido se agrupa en 7 pestañas:

1. **Diccionarios** - para configurar diccionarios de origen.
2. **Reglas** - archivos con conjunto de reglas.
3. **Super-reglas** - los que se aplicarán por encima de las reglas regulares
4. **Generador de diccionarios**, donde se pueden crear archivos de palabras obtenidas del ataque híbrido.
5. **Diccionarios en línea** - para descargar nuevos diccionarios a la aplicación.
6. **Sintaxis híbrido** - descripción completa de todas las reglas con ejemplos.
7. **Probador de reglas**, donde puedes probar tus reglas.

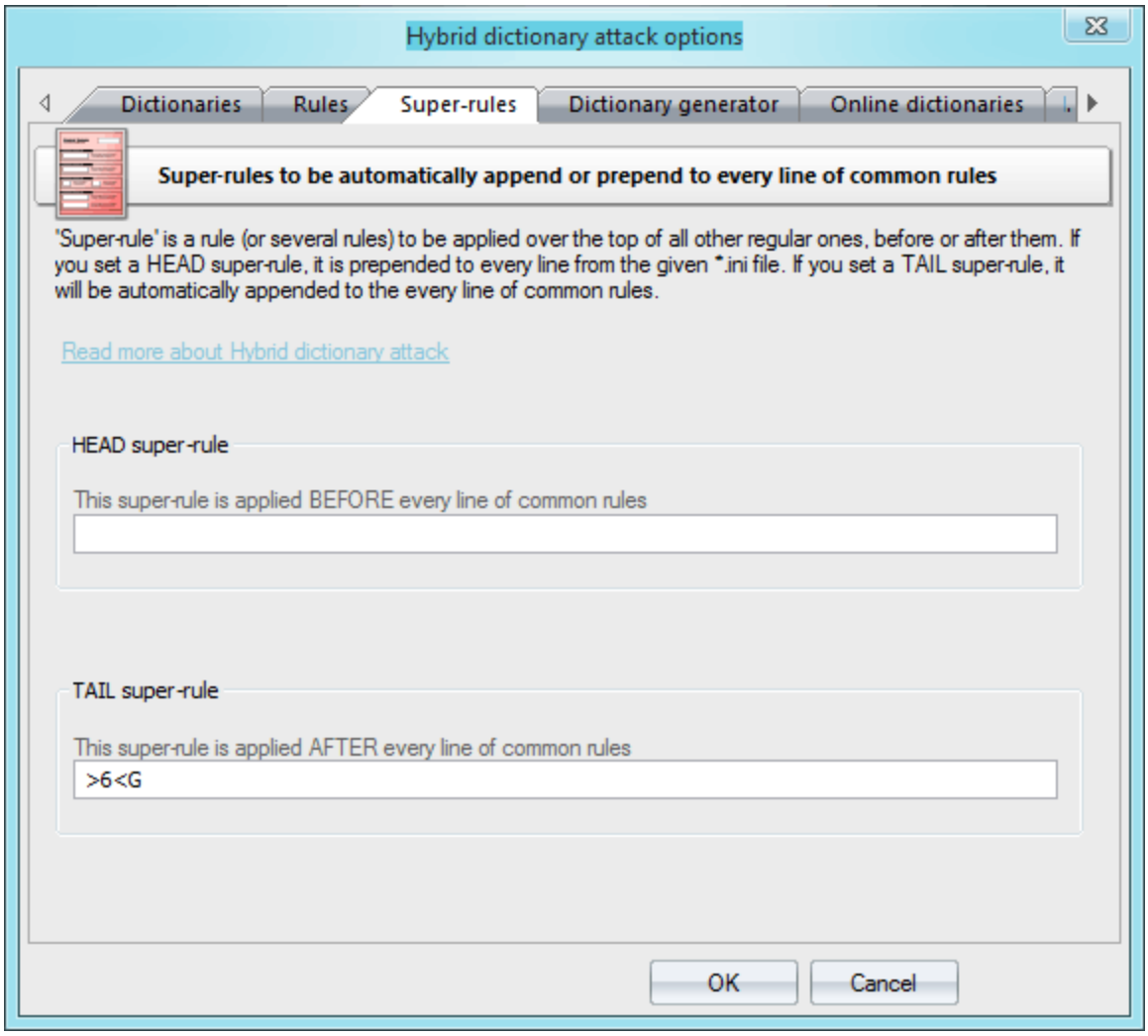
Las listas de palabras que se utilizarán en el ataque se establecen en la primera pestaña. Tradicionalmente, la aplicación admite listas de palabras en formato ASCII, UTF8, UNICODE, PCD, RAR y ZIP. La posición de los archivos en la lista puede ser alterada. Por ejemplo, es posible que desee mover diccionarios más pequeños hacia arriba en la lista o al revés. Durante el ataque, se usarán uno tras otro, de acuerdo con su posición en la lista.



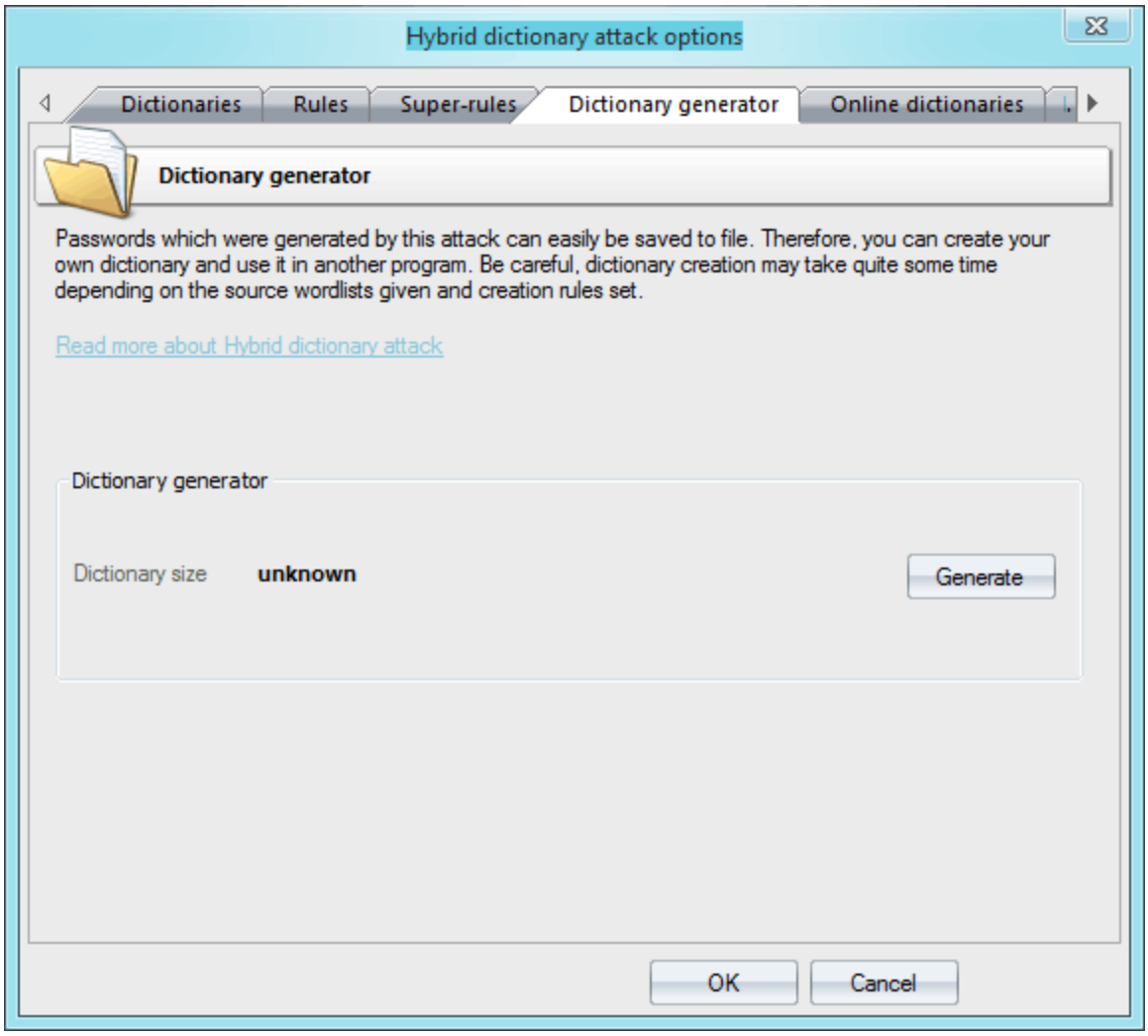
En la pestaña '**Reglas**', defina al menos un archivo con reglas de mutación de contraseña. El formato del archivo de reglas es bastante trivial; es un archivo ASCII de texto sin formato con la cadena **'[Rules]**'. Cualquier cosa por encima de esta cadena se considera como comentarios e ignorada por el programa. Todo lo que va por debajo de esta cadena se considera como reglas. Cada cadena puede contener varias reglas, aplicables a una palabra de origen. La exclusión es la regla **aN**. Esta norma no debe estar en la misma línea que otras normas. Si una cadena contiene varias reglas por palabra, esas reglas se analizan de izquierda a derecha. Por ejemplo, si aplica la regla '@pc$a$b$c' a la palabra de origen 'contraseña', en la salida obtendrá 'Asswordabc'. La longitud máxima de una palabra de salida no puede exceder los 256 caracteres.



Las "**super-reglas**" son una regla (o varias reglas) que se aplican sobre todas las demás reglas regulares, antes o después de ellas. Por ejemplo, puede establecer la superar regla de cola 'a8' para crear todas las combinaciones de casos posibles después de que se haya realizado una mutación común. Por lo tanto, la regla '/asa4' de l33t.ini archivo se convertirá en '/asa4a8', '/csc(' se convertirá en '/csc(a8', etc. Otro ejemplo más: establecer la regla de cabeza '>6<G' le permite omitir todas las palabras de menos de 6 o más de 16 caracteres, antes de comenzar una mutación común. Esta es una característica útil una vez que decida agregar la misma regla a todas las líneas de texto de los archivos *.ini seleccionados. No hay necesidad de modificarlos todos. Sin embargo, tenga cuidado, la superar regla 'aN' puede aumentar drásticamente el número total de contraseñas generadas.

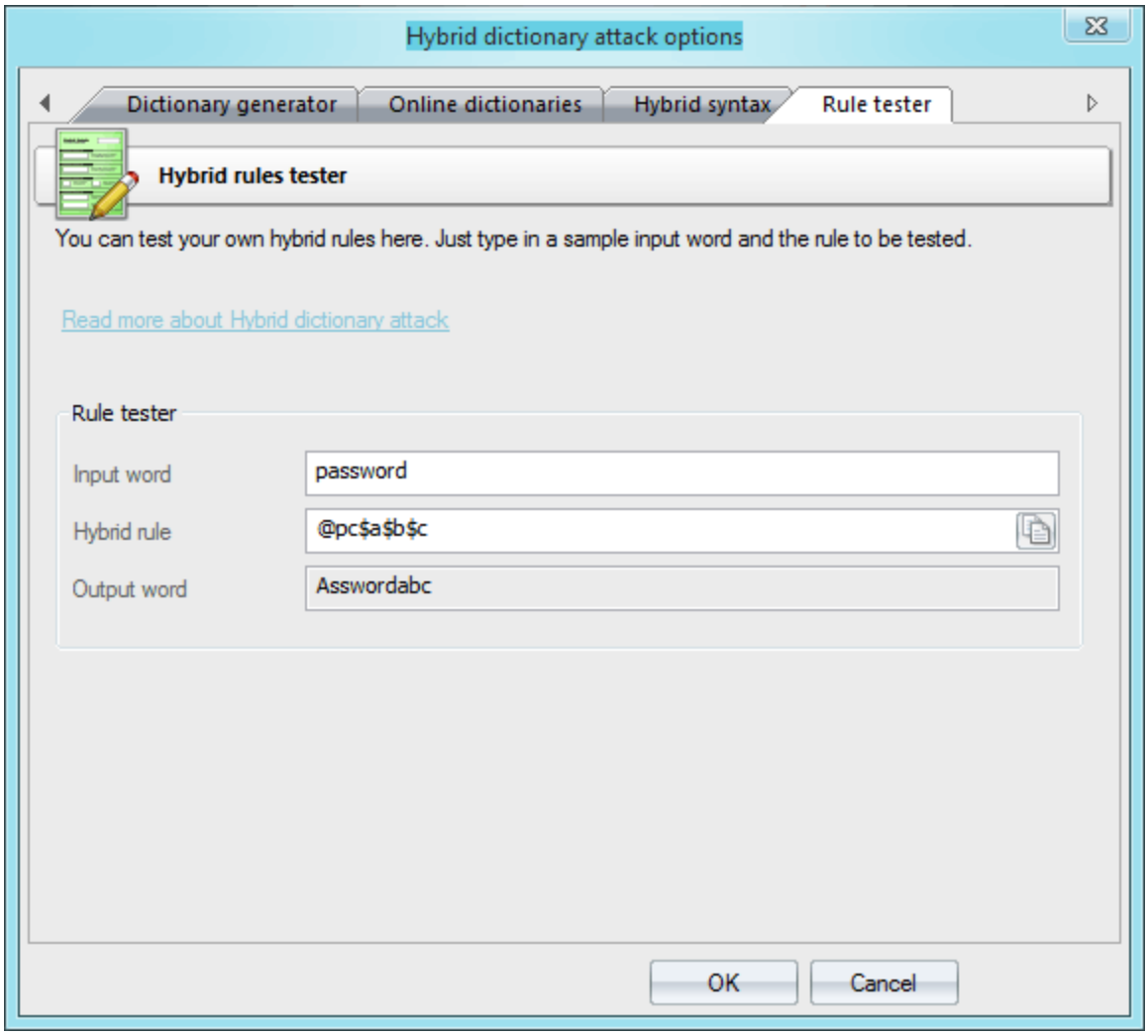


La pestaña **'Generador de diccionarios'** está diseñada para generar diccionarios obtenidos de un ataque. Más adelante, esos diccionarios podrían utilizarse, por ejemplo, en otras aplicaciones. Para generar un diccionario, especifique un diccionario de origen y un conjunto de reglas de mutación para él. El tamaño de un archivo de destino puede superar los 2 GB. ¡Tenga cuidado, el proceso de generación del diccionario puede llevar un tiempo considerable!



Puede descargar listas de palabras adicionales para el ataque utilizando la pestaña 'Diccionarios en linea'

Si desea crear su propio conjunto de reglas, puede utilizar las dos últimas pestañas como fuentes de ayuda. Mientras que la pestaña **'Sintaxis híbrida'** ofrece meras descripciones de las reglas disponibles, en la última pestaña puede probarlas especificando una palabra de origen y una regla para el ataque híbrido. Envíenos sus conjuntos de reglas; si los encontramos interesantes/útiles, los incluiremos en la distribución por defecto del programa.



Descripción de las reglas para el ataque de diccionario híbrido

Se permite establecer varias reglas en una línea.
Las reglas (si las hay) se procesan de izquierda a derecha.
La longitud máxima de la línea está limitada a **256** caracteres.
La longitud máxima de las palabras de salida está limitada a **256** caracteres.
El espacio en blanco se ignora siempre que no se utilice como parámetro.
Una línea que comienza con el carácter # considerado como un comentario.
Todo el texto anterior a la línea «[**Reglas**]» se considera comentario.
N y M siempre comienzan en 0. Para valores mayores de 9 utilice A.. Z (A=10, B=11, etc.).
Las siguientes reglas deben estar en la última posición de una línea: aN, ?iN[C], ?i[C], ?oN[C], ?o[C], ?iZ[C], ?oZ[C].
No cambie los nombres de los archivos de reglas estándar. Algunos son utilizados por el programa.
Las reglas ?iN[C], ?i[C], ?oN[C], ?o[C] ?iZ[C], ?oZ[C] utilizan los siguientes conjuntos de caracteres predefinidos (aunque puede usar conjuntos de caracteres personalizados):

digits	- 0123456789
loweralpha	- abcdefghijklmnopqrstuwxyz
upperalpha	- ABCDEFGHIJKLMNOPQRSTUVWXYZ
alpha	- abcdefghijklmnopqrstuwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ
special	- !@#$%^&*()-_+=~`[]{}|\:;"'<>,.?/ "

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

Rules

Regla	Ejemplo	Entrada	Salida	Descripción
:	:	password	password	No hacer nada con la palabra de entrada
{	{	password	asswordp	Girar la palabra a la izquierda
}	}	password	dpasswor	Girar la palabra a la derecha
[	[	password	assword	Eliminar el primer carácter
]	]	password	passwor	Eliminar el último carácter
c	c	password	Password	Mayúscula inicial
C	C	password	pASSWORD	Anti-mayúsculas (minúsculas el primer carácter, mayúsculas el resto)
d	d	password	passwordpassword	Palabra duplicada
f	f	password	passworddrowssap	Reflejar palabra
k	k	password пароль	зфыыцщкв gfhjkm	Convierta Word usando una distribución de teclado alternativa (primero después de la predeterminada). La regla funciona en ambas direcciones. Por ejemplo, si hay una distribución de teclado rusa instalada previamente en el sistema, la regla debe convertir la palabra 'contraseña' a la rusa 'зфыыцщкв', y la palabra rusa 'пароль' a 'gfhjkm'. Esto es muy útil cuando se buscan contraseñas que no estén en inglés. Si solo hay un idioma instalado en el sistema, la regla no hace nada.
K	K	password	passwodr	Intercambiar los dos últimos caracteres
l	l	password	password	Convertir todos los caracteres en minúsculas
q	q	password	ppaasssswwoorrdd	Duplicar todos los símbolos
r	r	password	drowssap	Palabra inversa
t	t	PassWord	pASSwORD	Alternar mayúsculas y minúsculas de todos los caracteres
u	u	password	PASSWORD	Convertir todos los caracteres en mayúsculas
U	U	my own password	My Own Password	Poner en mayúsculas todas las palabras delimitadas con espacio (en mayúsculas el primer carácter y cada carácter después de un espacio)
V	V	password	PaSSWoRD	Vocales élite

Regla	Ejemplo	Entrada	Salida	Descripción
v	v	password	pASSWoRD	Vocales sin élite
'N	'4	password	pass	Truncar la palabra a N caracteres de longitud
+N	+1	password	pbssword	Carácter de incremento en la posición N por 1 valor ASCII
-N	-0	password	oassword	Carácter de disminución en la posición N por 1
.N	.4	password	passoord	Reemplace el carácter en la posición N por el carácter en la posición N+1
,N	,1	password	ppssword	Reemplace el carácter en la posición N por el carácter en la posición N-1. Donde N > 0.
<N				Rechazar (omitir) la palabra si tiene más de N caracteres de largo
>N				Rechazar (omitir) la palabra si tiene menos de N caracteres de longitud
aN				Compruebe todos los casos de símbolos posibles para la palabra. N es una longitud máxima de la palabra para aplicar esta regla.
DN	D2D2	password	paword	Eliminar el carácter en la posición N
pN	p3	key	keykeykey	Copiar palabra N veces
TN	T1T5	password	pAsswOrd	Alternar mayúsculas y minúsculas del carácter en la posición N
yN	y3	password	paspassword	Duplicar los primeros N caracteres
YN	Y3	password	paswordord	Duplicar los últimos N caracteres
zN	z3	password	ppppassword	Duplicar el primer carácter de la palabra N veces
ZN	Z3	password	passwordddd	Duplicar el último carácter de la palabra N veces
$X	$0$0$7	password	password007	Agregar el carácter X al final de la palabra
^X	^3^2^1	password	123password	Insertar el carácter X al principio de la palabra
@X	@s	password	paword	Quitar todos los caracteres X de la palabra
!X				Rechazar (omitir) la palabra si contiene al menos un carácter X
/X				Rechazar (omitir) la palabra si no contiene el carácter X
(X				Rechazar (omitir) la palabra si el primer carácter no es X
)X				Rechazar (omitir) la palabra si el último carácter no es X
eX	e@	mike@yahoo.com	mike	Extraiga una subcadena que comienza en la posición 0 y termina antes de la primera aparición del carácter X (no haga nada si no se encuentra X)
EX	E@e.	mike@yahoo.com	yahoo	Extraiga una subcadena que comienza justo después de encontrar el primer carácter X y hasta el final de la cadena (no haga nada si no se encuentra X)
%MX				Rechazar (omitir) la palabra si no contiene al menos M instancias del carácter X

Regla	Ejemplo	Entrada	Salida	Descripción
***XY**	*15	password	possward	Intercambiar caracteres en las posiciones X e Y
=NX				Rechazar (omitir) la palabra si el carácter en la posición N no es igual a la X
iNX	i4ai5bi6c	password	passabcword	Inserte el carácter X en la posición N
oNX	o4*o5*	password	pass**rd	Sobrescribir un carácter en la posición N con el carácter X
sXY	ss$so0	password	pa$$w0rd	Reemplazar todos los caracteres X por Y
xNM	x4Z	password	word	Extraiga una subcadena de hasta M caracteres de longitud, a partir de la posición N.
INX-Y	rl0/-/r	google.com	google.com/	Inserte el carácter X en la posición N si el carácter anterior en la posición N no es Y.
INX+Y	rl0.+.r	password.	password..	Inserte el carácter X en la posición N si el carácter anterior en la posición N es Y.
ONX-Y	O0-+p	password	-assword	Si el carácter en la posición N no es Y, sobrescriba con el carácter X.
ONX+Y	O0P+p	password	Password	Si el carácter en la posición N es Y, sobrescriba con el carácter X.
RNM+Y	R01+a	password	assword	Quitar el carácter en la posición N si el carácter en la posición M es Y
RNM-Y	R40-b	password	passord	Quitar el carácter en la posición N si el carácter en la posición M no es Y
?iN[C]	?i0[digits]	password	0password, 1password ... 9password	Inserte un carácter de un conjunto de caracteres [C] en la posición N de la palabra. Donde C debe ser un nombre de conjunto de caracteres predefinido o un conjunto de caracteres personalizado.
?iZ[C]	?iZ[digits]	password	password0, password1 ... password9	Inserte un carácter de un conjunto de caracteres [C] en la última posición de la palabra. Donde C debe ser un nombre de conjunto de caracteres predefinido o un conjunto de caracteres personalizado.
?i[C]	?i[special]	password	~password, !password ... password_, password+	Inserte un carácter de un conjunto de caracteres [C] en cada posición de la palabra. Donde C debe ser un nombre de conjunto de caracteres predefinido o un conjunto de caracteres personalizado.
?oN[C]	?o1[upperalpha]	password	pAssword, pBssword ... pZssword	Sobrescriba un carácter en la posición N con un carácter tomado de un conjunto de caracteres [C]. Donde C debe ser un nombre de conjunto de caracteres predefinido o un conjunto de caracteres personalizado.
?oZ[C]	?oZ[upperalpha]	password	passworA, passworB ... passworZ	Sobrescriba un carácter en la última posición con un carácter tomado de un conjunto de caracteres [C]. Donde C debe ser un nombre de conjunto de caracteres predefinido o un conjunto de caracteres personalizado.

Regla	Ejemplo	Entrada	Salida	Descripción
?o[C]	?o[-=.]	password	-assword, =assword ... passwor.	Sobrescriba un carácter en cada posición de la palabra con un carácter tomado de un conjunto de caracteres [C]. Donde C debe ser un nombre de conjunto de caracteres predefinido o un conjunto de caracteres personalizado.

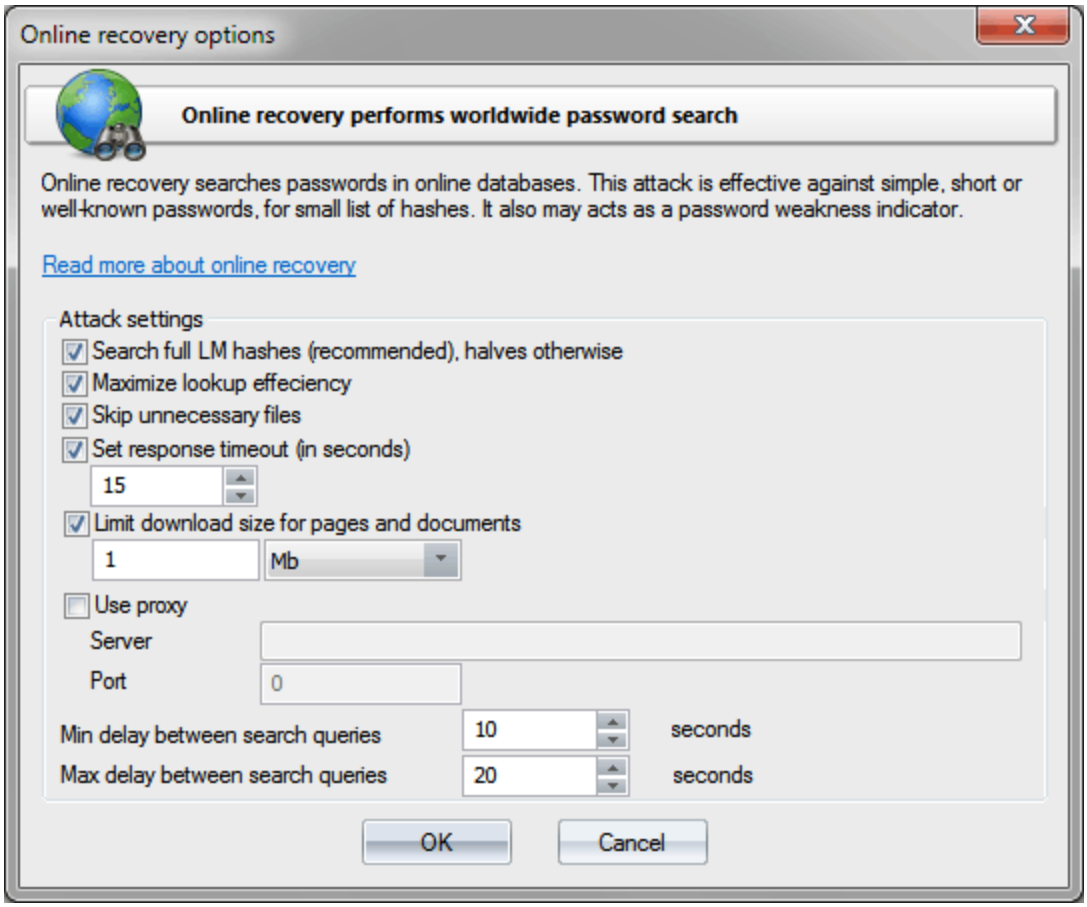
Adicional
El kit de distribución de Windows Password Recovery viene con conjuntos extendidos de reglas de mutación de contraseña:
hybrid_rules/english_words.ini contiene reglas básicas para contraseñas en inglés.
hybrid_rules/nonenglish_words.ini contiene reglas comunes para contraseñas que no son de Eglish.
hybrid_rules/simple_dates.ini - muchas reglas con fechas, meses, estaciones, etc.
hybrid_rules/l33t.ini - reglas para palabras freak (basadas en el diccionario leet). Por ejemplo password->p@$$w0rd
...

¿Busca una forma conveniente de manejar tantas contraseñas como sea posible? Descargue el conjunto completo de más de 180000 reglas ordenadas y sin duplicados..

2.8.2.12 Recuperación en línea

La recuperación en línea (desarrollada por Passcape Software) encuentra contraseñas utilizando servidores de motores de búsqueda de Internet. Se ocupa bastante bien de contraseñas cortas y de uso frecuente. Entre sus inconvenientes se encuentran la baja velocidad de operación y la poca idoneidad para manejar grandes listas hash.

La recuperación en línea ha sido desarrollada por Passcape Software y es un buscador de contraseñas en línea mejorado. Para encontrar contraseñas, el programa envía consecutivamente una solicitud de búsqueda especial para cada hash a un motor de búsqueda y luego descarga los archivos de contraseña encontrados y analiza su contenido. La recuperación en línea es relativamente lenta; por lo tanto, es apropiado para pequeñas listas hash. Además, las contraseñas encontradas suelen limitarse a vocabulario simple y combinaciones cortas. De una forma u otra, este ataque puede ser bastante útil; por ejemplo, al auditar contraseñas, como un simple detector de vulnerabilidades para ciertos sistemas.



Opciones de recuperación en línea

- **Buscar hashes completos de LM** - utilice todo el hash de 16 bits al buscar hashes lm. Si esta opción no está configurada, la búsqueda se llevará a cabo en las mitades de 8 bytes. Para garantizar una búsqueda más eficiente y deshacerse de algo de tráfico perdido, se recomienda que se establezca esta opción. Se ignora al buscar hashes NT.
- **Maximice la eficiencia de la búsqueda** - aumentar la eficiencia de la búsqueda de contraseñas sin afectar la velocidad de ataque. También se recomienda establecer siempre esta opción.
- **Omitir archivos innecesarios** - no compruebe algunos archivos innecesarios si se sospecha que no contienen contraseñas.
- **Tiempo de espera de respuesta** - establezca el tiempo máximo de respuesta de recursos web permitido.
- **Limitar el tamaño de descarga** - limitar el tamaño del archivo de descarga. Algunas bases de datos hash tienen un tamaño enorme, incluso a pesar de que a menudo no contienen contraseñas. Por lo tanto, para conexiones lentas a Internet y para restringir el tráfico perdido, se recomienda establecer un límite en el tamaño de las páginas de descarga. Desafortunadamente, no hay forma de averiguar qué hay en los datos que se descargarán; por lo tanto, esta opción está determinada exclusivamente por sus preferencias y capacidades.
- **Usar proxy** - Utilizar el servidor proxy para buscar contraseñas
- **Retraso mínimo/máximo entre consultas de búsqueda** - retrasos mínimos y máximos entre dos solicitudes consecutivas al servidor de búsqueda. Algunos servidores de búsqueda pueden rechazar las solicitudes de búsqueda si van en serie desde la misma dirección IP con un intervalo de tiempo muy corto (normalmente menos de 10 segundos). A pesar de que Windows Password Recovery tiene un aleatorizador de solicitudes interno, que permite reducir este retraso significativamente (a tan solo 1 y 2 segundos respectivamente), los valores seguros cuando el servidor procesará definitivamente

una solicitud de búsqueda son min = 15 y max = 30 segundos. Ciertamente, la velocidad de ataque depende de estas dos opciones.

¡Ten cuidado! ¡La recuperación en línea puede generar mucho tráfico de Internet!

2.8.2.13 Ataque de tabla Passcape

Passcape Rainbow Tables es el siguiente desarrollo lógico de tablas simples precalculadas. Son los más adecuados para la recuperación de combinaciones significativas y contraseñas complejas de longitud literalmente ilimitada.

El método original de tablas de rainbow simples

El principio de funcionamiento de las tablas de arco iris simples consiste en establecer un rango de caracteres (por ejemplo, a.. z) y la longitud máxima de la contraseña, seguida del cálculo de todas las variantes posibles y la generación de millones de cadenas. Cada cadena se calcula mediante la fórmula:

P0 -> hash(P0) -> H1 -> R(H1) ->
P1 -> hash(P1) -> H2 -> R(H2) ->
P2 ...

donde **P** – contraseña, hash – función hash, **R** – función de reducción. Por lo tanto, a partir de la contraseña original, la función hash produce un hash, que la función de reducción luego convierte en la siguiente contraseña, y el proceso se repite nuevamente y genera cadenas. Cada cadena almacena solo el valor original y final. Almacenar solo el primer y el último hash es una operación que lleva a comprometer y ahorrar memoria a costa del tiempo dedicado al criptoanálisis.

Para recuperar una contraseña buscada, se somete a hasheo y la función de reducción y luego se busca en la tabla. Para ello, se genera un llavero a partir de R(**Hn**) hasta la longitud máxima de la cadena. Si **Hn** se obtiene con la contraseña utilizada al crear la tabla, finalmente obtenemos la clave que coincide con la clave de la cadena respectiva. Esta última clave se guardó en la tabla junto con la primera clave de la cadena. Usando la primera clave de la cadena, podemos recuperar toda la cadena, en particular, el valor justo antes de R(**Hn**). Esa es en realidad la clave que se utilizó para generar **Hn**, nuestra contraseña buscada.

Principio de funcionamiento de las tablas rainbow Passcape

La recuperación con tablas de rainbow de Passcape es más o menos lo mismo que la recuperación con tablas de arco iris simples. Sin embargo, a diferencia de este último, es una especie de híbrido de Huellas dactilares y ataques de tabla simple, donde en lugar de establecer un rango de caracteres específico, las contraseñas se validan dentro de un rango llamado 'huella de palabras'. La idea del ataque Fingerprint desarrollado en Passcape se reduce a sacar de ese diccionario el diccionario fuente y crear un banco de huellas de palabras (huellas dactilares), necesarias para validar la contraseña; luego, durante el ataque, buscamos todas las variantes posibles de palabras que consisten en dos de esas huellas.

Similar al ataque de huellas dactilares, las tablas de rainbow de Passcape primero crean un banco de huellas para las palabras de la lista de palabras de un usuario. El banco de huellas de palabras es un conjunto de caracteres análogo a los de las tablas de rainbow simples. Se utiliza tanto para crear tablas de Passcape como para validar contraseñas. Por lo tanto, una tabla arco iris de Passcape consta de

uno o mas archivos *.prt (las tablas reales) y un banco of huellas de palabras (*.**prti**), que solo se pueden involucrar con las tablas que se crearon con él.

Hay una serie de ventajas en el uso de huellas de palabras en lugar de conjuntos de caracteres al crear tablas:

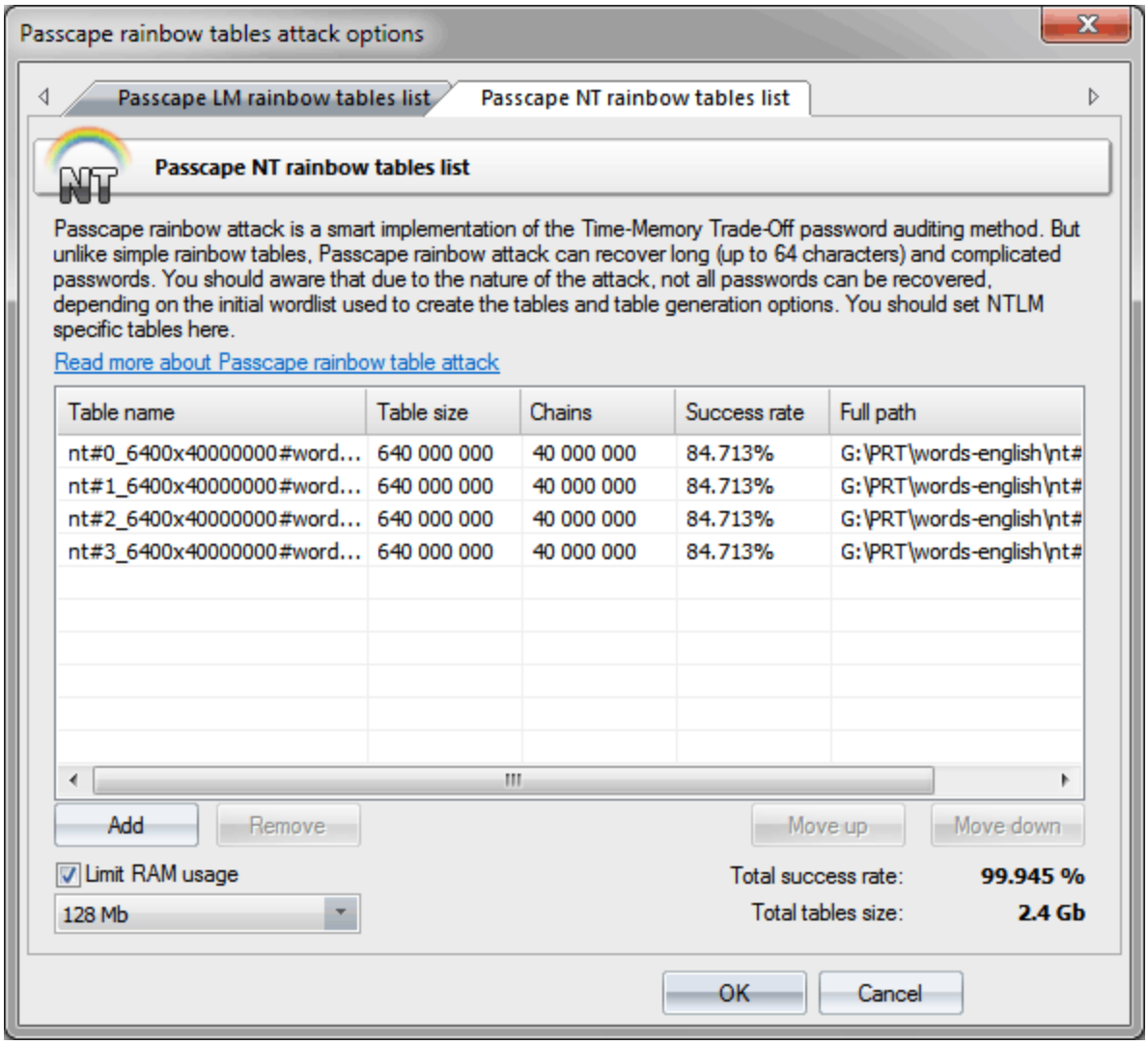
- La longitud de las contraseñas validadas con tablas passcape es literalmente ilimitada. A diferencia de las tablas arco iris simples, que prácticamente no se pueden crear para contraseñas de más de 9 caracteres, con las tablas Passcape se puede recuperar tanto la contraseña de un carácter como la de 50 caracteres con la misma probabilidad.
- El juego de caracteres en la tabla regular afecta en gran medida a sus parámetros críticos: cuanto más amplio sea el rango de caracteres, mayor debe ser la longitud de la cadena o el número total de cadenas para almacenar la tasa de éxito (porcentaje de éxito en la búsqueda de contraseña) de la tabla. En una tabla passcape, un juego de caracteres no afecta a los parámetros críticos de la tabla.
- Las tablas simples tienen ciertas dificultades a la hora de generar tablas para validar contraseñas en conjuntos de caracteres nacionales; no todos los programas manejan correctamente tales tablas, y no todos pueden crearlas. Con las tablas arco iris de Passcape, al generar tablas, por ejemplo, para contraseñas rusas, simplemente se puede especificar el diccionario de origen en ruso.
- Con las tablas de Passcape, las contraseñas se buscan utilizando combinaciones más significativas; sin embargo, eso depende en gran medida del diccionario de origen.

Estos pueden ser referidos como inconvenientes de las tablas rainbow passcape:

- No todos los diccionarios de origen son igualmente adecuados para las tablas. El uso de diccionarios grandes (normalmente mayores de 1 MB) genera un banco de huellas demasiado grande; respectivamente, la creación de tablas puede requerir mucho tiempo y recursos.
- Se desaconseja el uso de diccionarios con palabras o frases largas debido a la razón mencionada anteriormente.
- Rainbow table attack consume una gran cantidad de recursos: el banco de huellas debe ajustarse completamente a la RAM de la computadora.

Configuración de ataque de mesa arco iris de Passcape

Los ajustes de ataque de tabla de rainbow de Passcape son bastante triviales. Especifique una o varias tablas *.prt, que deben residir en el mismo directorio que el banco de huellas (archivo *.prti). Dado que este ataque consume más RAM que el ataque que utiliza tablas de arco iris simples, se recomienda limitar la cantidad de RAM que se puede consumir ajustando la opción respectiva.

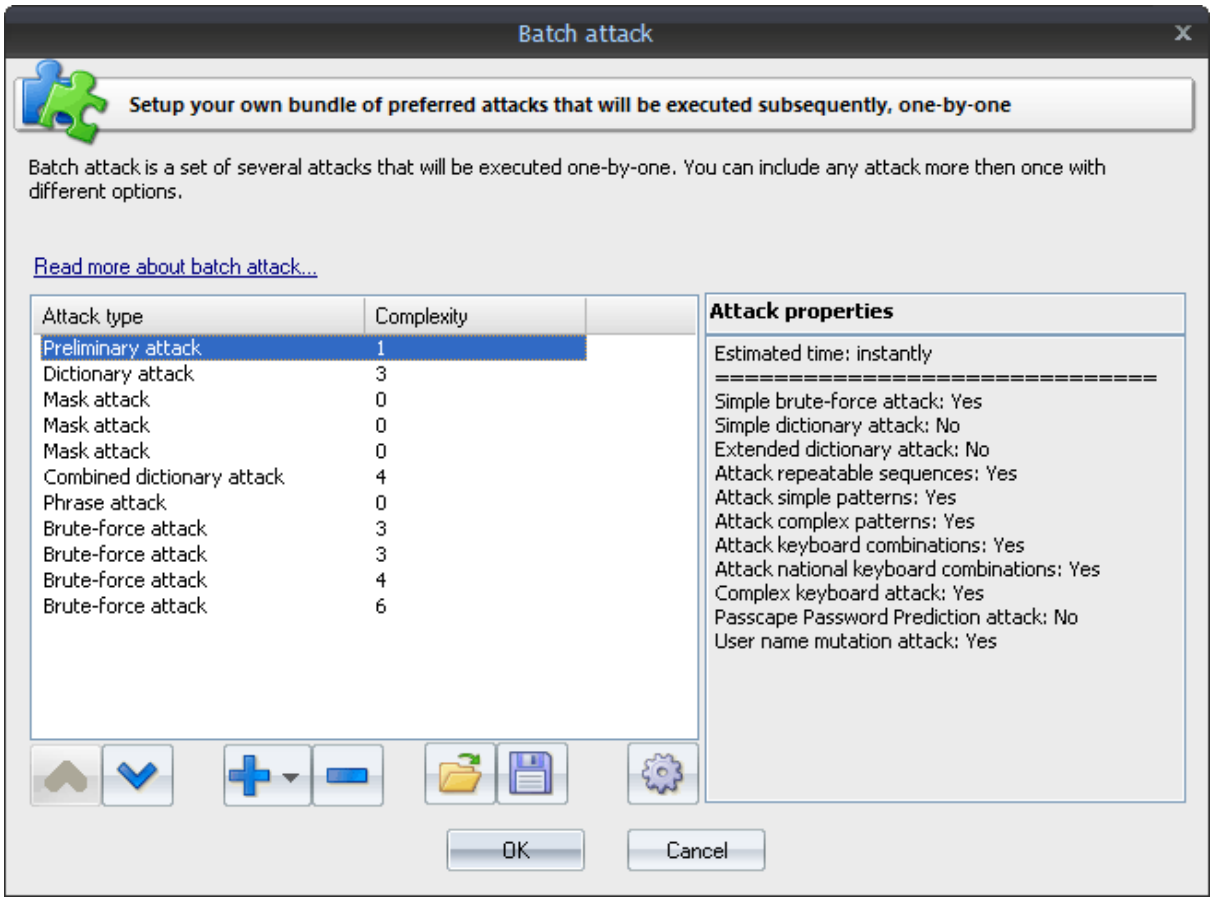


Las tablas solo pueden descifrar la función hash para la que fueron creadas, es decir, ¡las tablas NT solo pueden descifrar el hash NT!

Para crear sus propias tablas, puede aprovechar el herramienta respectiva.
Puede descargar tablas de muestra de Passcape para este ataque desde nuestro sitio web.

2.8.2.14 Ataque por lotes

Dado que cada ataque cubre su propio rango de contraseñas, a veces, para recuperar completamente los hashes de contraseña, debe ejecutar varios ataques diferentes uno tras otro. La idea básica detrás del ataque por lotes (desarrollado por Passcape Software) es crear una lista / lote de ataques para ejecutarse uno tras otro, de modo que pueda lanzar todos esos ataques con un solo clic del mouse y no molestarse con configurar cada uno de ellos individualmente cada vez que los necesite.



Las opciones de ataque por lotes están disponibles como una lista que puede ampliar o cortar (botones [+] y [-]). Cada ataque en la lista se puede mover hacia arriba o hacia abajo (botones [^] y [v]), y su configuración se puede editar. Un lote puede incluir varios ataques del mismo tipo, pero de los ataques puede tener diferentes configuraciones. El panel a la derecha de la entrada seleccionada muestra las propiedades de la entrada seleccionada; especificaciones breves del ataque y el tiempo estimado que tardará el ataque en completarse.

2.8.2.15 GPU: Ataque de fuerza bruta

Un ataque de fuerza bruta de GPU es completamente idéntico a un ataque regular de fuerza bruta, excepto que las contraseñas son buscadas por la unidad de procesamiento de gráficos de su PC en su lugar. No es ningún secreto que el rendimiento de las tarjetas gráficas modernas es un orden de magnitud mayor que el de las CPU; esto los convierte en una herramienta conveniente para cálculos pesados, como la recuperación de contraseñas. Es importante entender que los cálculos que utilizan tarjetas gráficas tienen una serie de desventajas. Por ejemplo, algunos algoritmos con un gran número de saltos condicionales y otras comprobaciones demuestran un rendimiento extremadamente pobre en la GPU, y en ciertos casos puede ser incluso más bajo que en una CPU normal.

De todos modos, el software admite la búsqueda de contraseñas de fuerza bruta utilizando GPU. Puede comparar los indicadores de rendimiento de los cálculos de GPU vs. CPU a través del elemento de menú respectivo de la aplicación o presentarlo visualmente a través del menú '**Informes**'.

La configuración del ataque de fuerza bruta de la GPU consta de tres partes:

1. Elegir un juego de caracteres para la búsqueda.
2. Especificación de la longitud de la contraseña.
3. Configuración de la unidad de procesamiento de gráficos.

Elegir un juego de caracteres para la búsqueda

Al elegir un conjunto de caracteres para un ataque de fuerza bruta, normalmente te guías por consideraciones empíricas. Por ejemplo, si la contraseña esperada consiste en caracteres latinos en minúsculas y dígitos, tiene sentido elegir el rango 'a-z, 0-9'. Cuanto más pequeño sea el conjunto de personajes, antes se completará el ataque.

Por otro lado, siempre existe la posibilidad de hacer una elección incorrecta del conjunto de caracteres esperado. Si al menos un carácter de la contraseña que se va a recuperar no se incluye en el conjunto de caracteres especificado, no se encontrará la contraseña.

En la parte inferior del cuadro de diálogo de configuración de ataque, puede ver el número total de contraseñas que coinciden con el conjunto de caracteres especificado y la longitud de la contraseña.

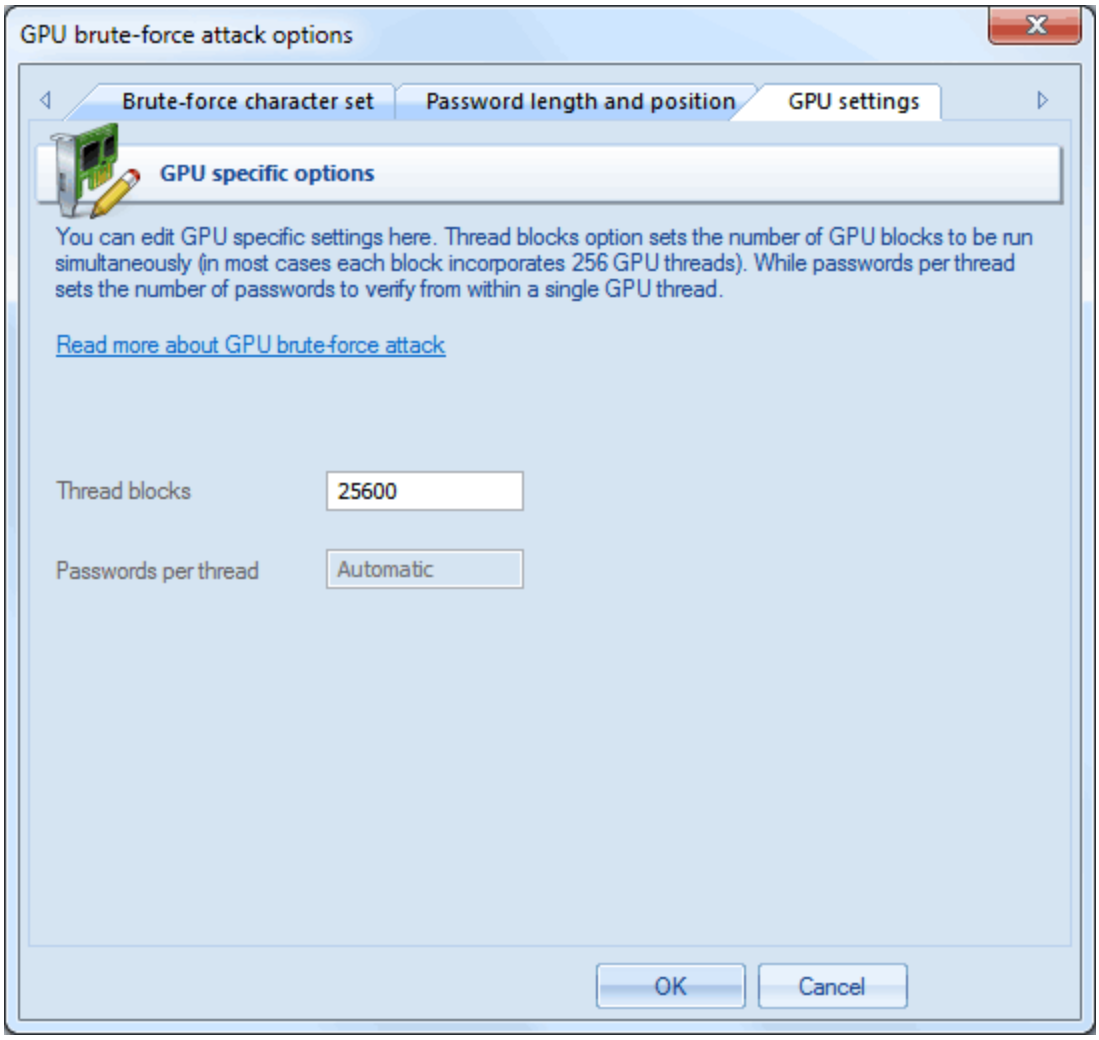
Es importante saber que las contraseñas LM en Windows siempre se convierten a mayúsculas; ¡eso reduce significativamente el rango de contraseñas a buscar!

Especificación de la longitud de la contraseña

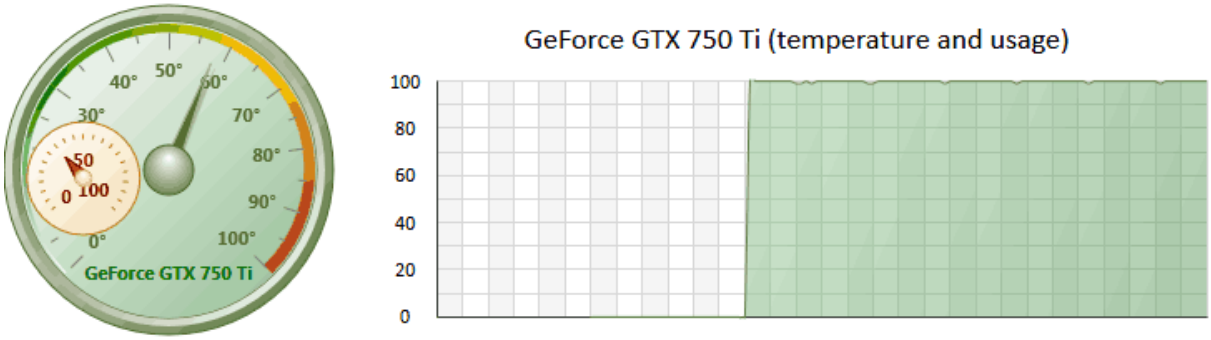
En la segunda pestaña de la página de opciones, establezca la longitud mínima y máxima de las contraseñas buscadas. Como alternativa a la longitud mínima, puede establecer la contraseña de origen, con la que comenzaría la búsqueda. La longitud máxima de LM en los sistemas operativos Windows es 7.

Configuración de la unidad de procesamiento de gráficos

Antes de poder usarlo en un ataque, primero debe seleccionar la tarjeta gráfica en elelemento de menú respectivo.



La configuración de la GPU consta de solo 1 parámetro: el número de bloques de subprocesos que se ejecutarán en la GPU. Cada bloque consta de 256 hilos. Por lo tanto, si establece el número de bloques en 25600, la GPU ejecutará 25600 * 256 = 6553600 subprocesos. Cada subproceso de GPU puede comprobar varias contraseñas. El número total de contraseñas verificadas depende en gran medida de otras opciones. Establecer el parámetro **ThreadBlocks** menor que 10000 en las tarjetas gráficas modernas, en la mayoría de los casos, conduce a un rendimiento deficiente. Para evitar la degradación del rendimiento, después de configurar el parámetro y ejecutar el ataque, asegúrese de que el gráfico de carga de la GPU tenga un gráfico casi 100% simple sin miradas (consulte la captura de pantalla a continuación).

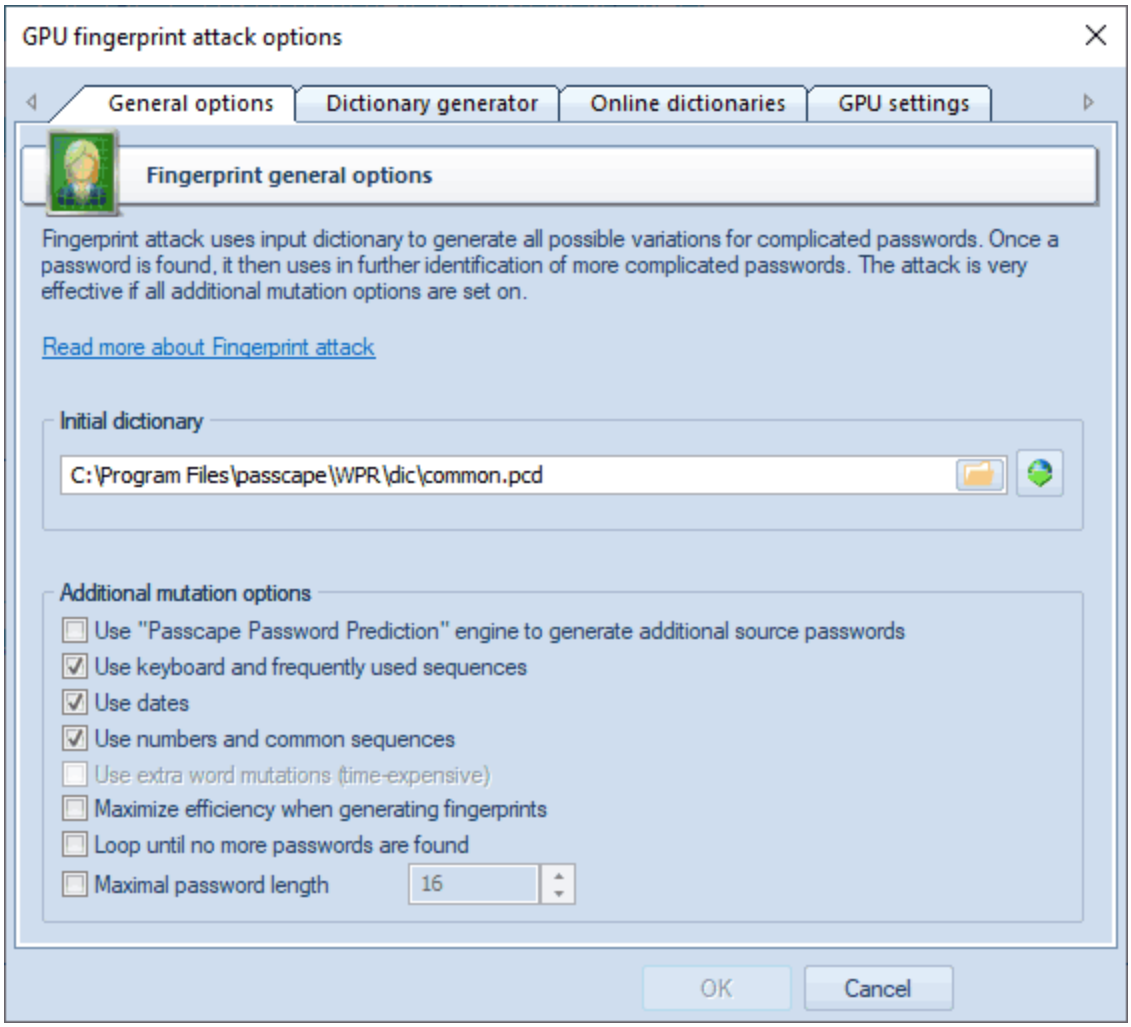


Al ejecutar la recuperación de contraseña para credenciales de dominio almacenadas en caché tipo 2, es posible que deba jugar con esta opción para obtener un mejor rendimiento.
Establecer valores demasiado grandes puede hacer que la GPU se bloquee o genere un error, dependiendo de su Configuración de tiempo de espera del kernel de GPU.

2.8.2.16 GPU: Ataque de huellas dactilares

El ataque de huellas dactilares es una herramienta completamente nueva para recuperar contraseñas complejas, que no se pudieron descifrar de una manera común. La idea del ataque es que aquí, para recuperar una contraseña, no tomamos ni palabras individuales del diccionario de origen, como en el ataque de diccionario, ni siquiera combinaciones de palabras, como en el ataque combinado, sino las llamadas "huellas dactilares". Por lo tanto, cada palabra del diccionario de origen se utiliza para generar varias huellas dactilares. Si se encuentra alguna contraseña durante el ataque, participa en la generación de nuevas huellas dactilares, y el ataque va otra ronda. La implementación de la potencia de cómputo de la GPU permite aumentar drásticamente la velocidad de recuperación. Las opciones de huellas dactilares constan de 4 partes:

Opciones generales
Antes de iniciar el ataque, especifique el diccionario de origen que se utilizará para crear las huellas digitales. El software viene con el diccionario common.pcd, optimizado para este ataque, pero puede usar el suyo o descargar uno de Internet (pestaña 'Diccionarios en línea'). No hay ciertos requisitos para la lista de palabras de origen, excepto uno: no debe ser demasiado grande; de lo contrario, el ataque tomará un tiempo significativo. Puede utilizar diccionarios con contraseñas nacionales si sospecha que la contraseña buscada contiene caracteres en una codificación nacional.



Esta es la forma en que se generan las huellas dactilares: primero, una palabra del diccionario de origen se divide en contraseñas de un carácter, luego, en 2 caracteres, etc. Por ejemplo, la palabra fuente **crazy** se divide en huellas dactilares de un carácter. Así que obtenemos:
c
r
a
z
y

Ahora, en dos caracteres:
cr
ra
az
zy

A continuación, tres caracteres:
cra
raz
azy

Y, por último, cuatro caracteres:

craz
razy

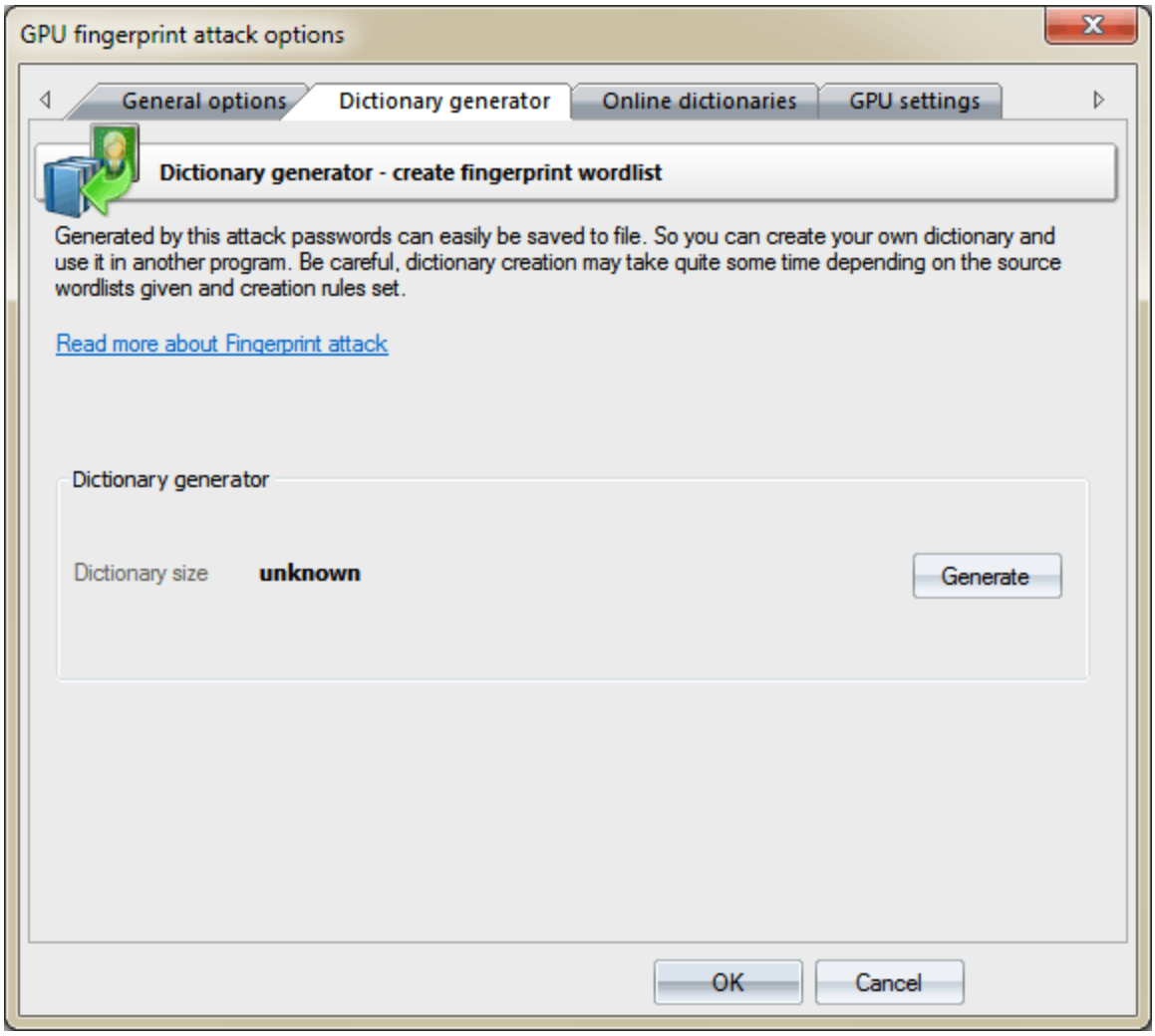
Tenemos 5 + 4 + 3 + 2 = 14 huellas dactilares, sin contar la palabra fuente.
Todas las palabras del diccionario de origen se dividen en huellas dactilares. Después de esto, todas las huellas dactilares se vuelcan en una sola base de datos, naturalmente, descartando duplicados. Así que tenemos una base de datos de huellas dactilares que se utilizaría para verificar las contraseñas pegando todas las huellas dactilares entre sí y encontrando la coincidencia.

El algoritmo real de generación de huellas dactilares es un poco más sofisticado. Además, hay una opción en la configuración de ataque, **Maximizar la eficiencia al generar huellas dactilares**, que maximiza la eficiencia (a expensas de la velocidad) al generar huellas dactilares adicionales.

Echemos un vistazo a las opciones restantes.
- **Usar el motor PPP para generar contraseñas adicionales** - usar contraseñas encontradas en otros ataques al generar huellas dactilares.
- **Usar el teclado y usar secuencias con frecuencia** - Agregar combinaciones de teclado y secuencias comunes al banco de huellas dactilares.
- **Fechas de uso** - agregar fechas a las huellas dactilares.
- **Usar números y secuencias comunes** - utilizar dígitos y combinaciones simples de letras.
- **Longitud máxima de la contraseña** - esta opción permite limitar la longitud máxima de las contraseñas generadas. Como resultado, reduce el tiempo que tarda el ataque.

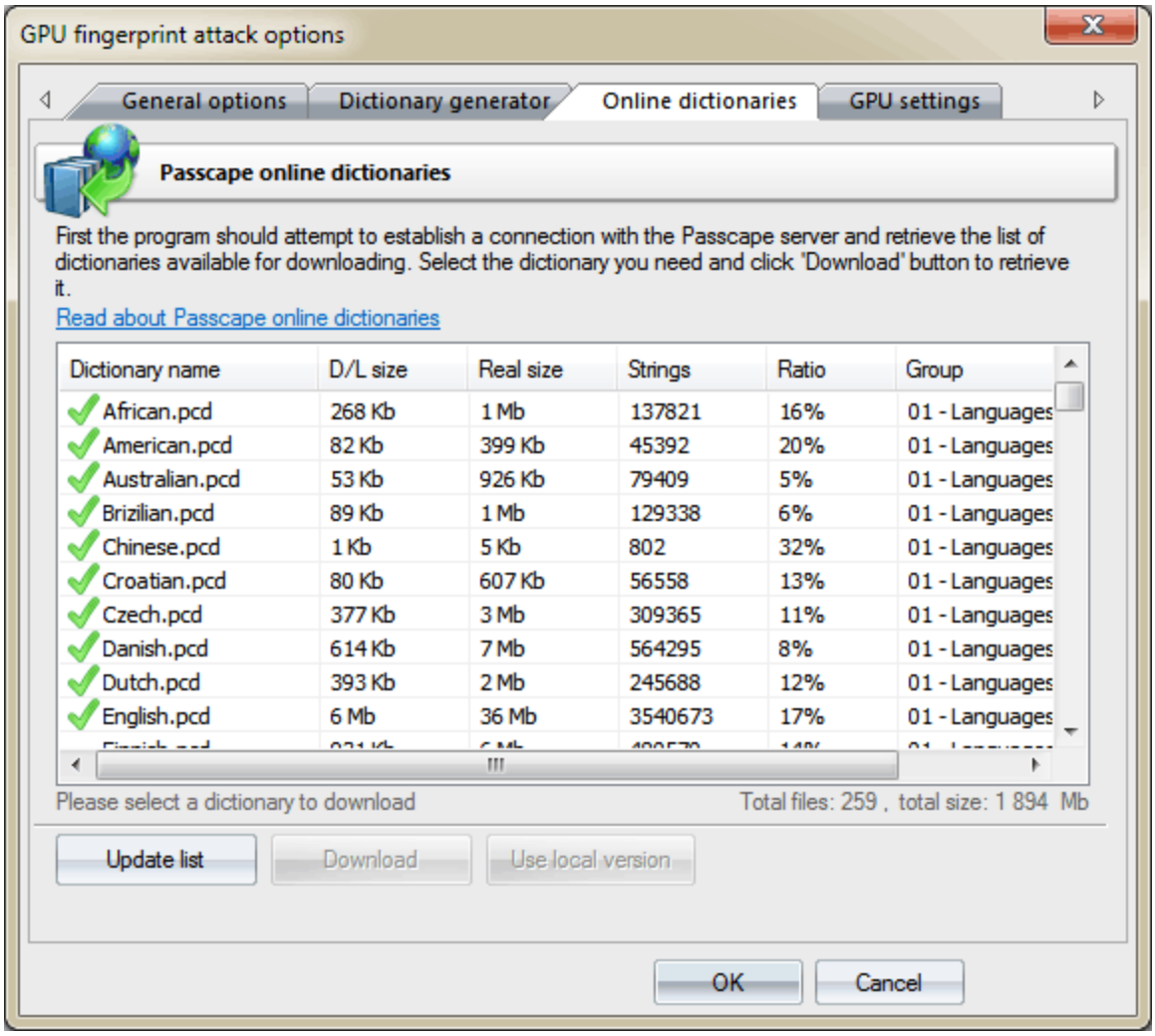
Se debe prestar la atención más cuidadosa a la opción **Repetir hasta que no se encuentren más contraseñas**. Ahí es donde el ataque de huellas dactilares realmente puede mostrarse. Así es como funciona: si se encuentra al menos una contraseña durante un ataque, cuando el ataque ha terminado, la contraseña participa en la generación de nuevas huellas dactilares y el ataque se ejecuta nuevamente. Esta opción funciona muy bien en grandes listas de hashes y en hashes de historial de contraseñas. Sin embargo, una vez que se establece la opción, no podrá continuar el ataque desde la última posición guardada.

Generador de diccionarios
La segunda pestaña con la configuración permite crear y guardar un diccionario personalizado utilizando las opciones actuales del ataque de huellas dactilares. Ten cuidado; el diccionario puede ocupar mucho espacio en la unidad de disco duro de su PC.



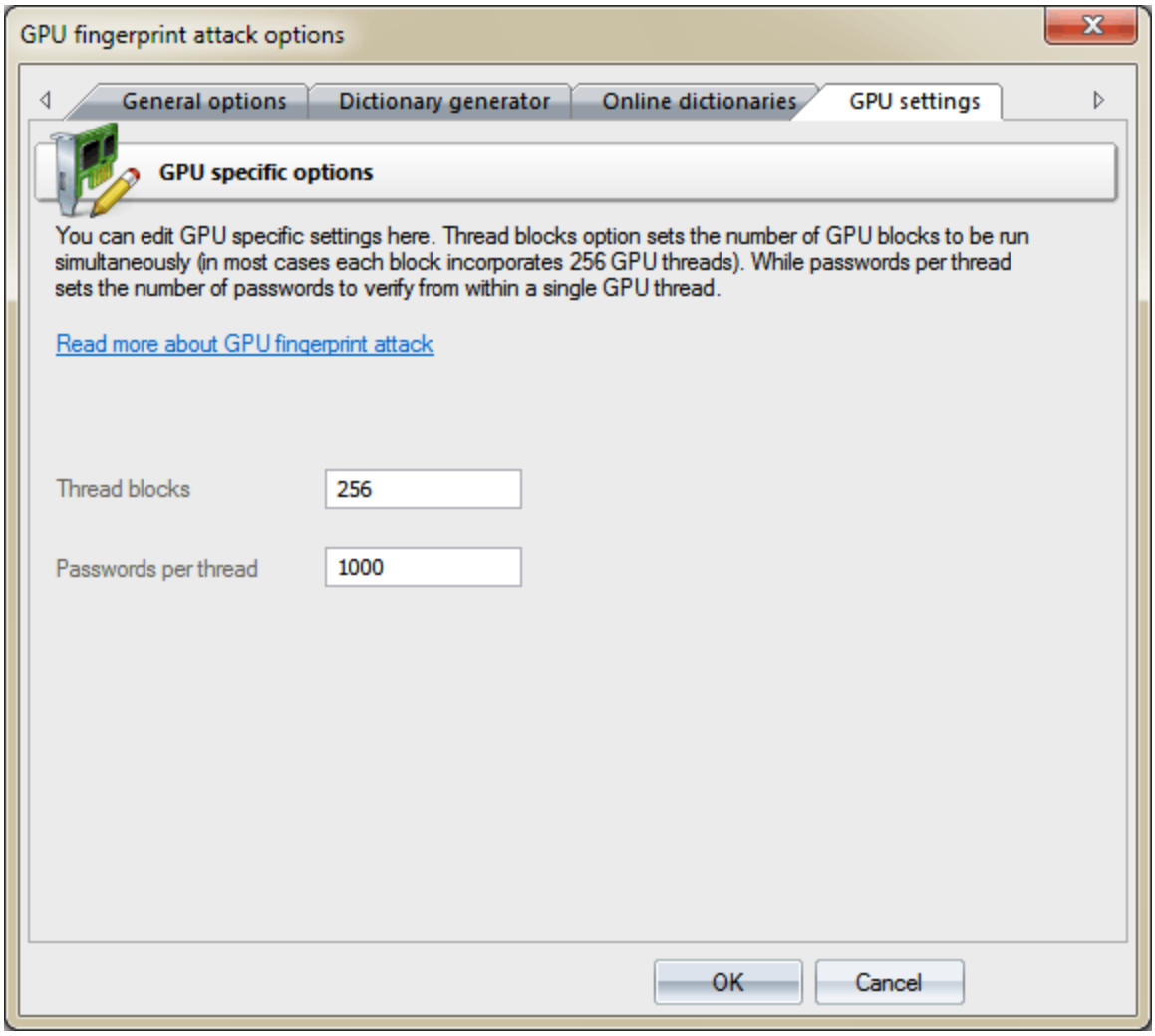
Diccionarios en línea

En la tercera pestaña, puede descargar listas de palabras de origen para el ataque de huellas dactilares de Internet. Tenga cuidado, no todos los diccionarios se adaptan bien para el ataque.



Configuración de GPU

Antes de poder usarlo en un ataque, primero debe seleccionar la tarjeta gráfica en el menú Menú Opciones generales.



La configuración de la GPU es bastante simple y consta de solo dos partes:

1. Establecer el número de bloques de tarjetas gráficas paralelas, donde se buscarían las contraseñas. Normalmente, cada bloque consta de 256 hilos. Por lo tanto, si establece el número de bloques en 256, la GPU ejecutará 256 * 256 = 65536 hilos. El número total de contraseñas verificadas para una llamada al kernel de la GPU será 256*ThreadBlocks*PasswordsPerThread. En nuestro caso 256*256*1000 = 65 536 000 contraseñas. Establecer el parámetro **ThreadBlocks** menor que 256 en las tarjetas gráficas modernas, en la mayoría de los casos, conduce a la degradación del rendimiento.
2. Establecer el número de contraseñas que se buscarán desde un solo subproceso. Cuanto mayor sea el valor, menor será la sobrecarga asociada con el lanzamiento de subprocesos y mayor será la velocidad de búsqueda. Sin embargo, establecer un valor demasiado grande puede bloquear el equipo o causar fluctuaciones significativas en la velocidad de búsqueda actual, que se muestra en la pestaña de estado del ataque. Esto se debe al hecho de que el tiempo de finalización de la tarea en la GPU excede el tiempo requerido para actualizar el estado actual del ataque. Establecer números demasiado grandes puede causar un error del sistema.

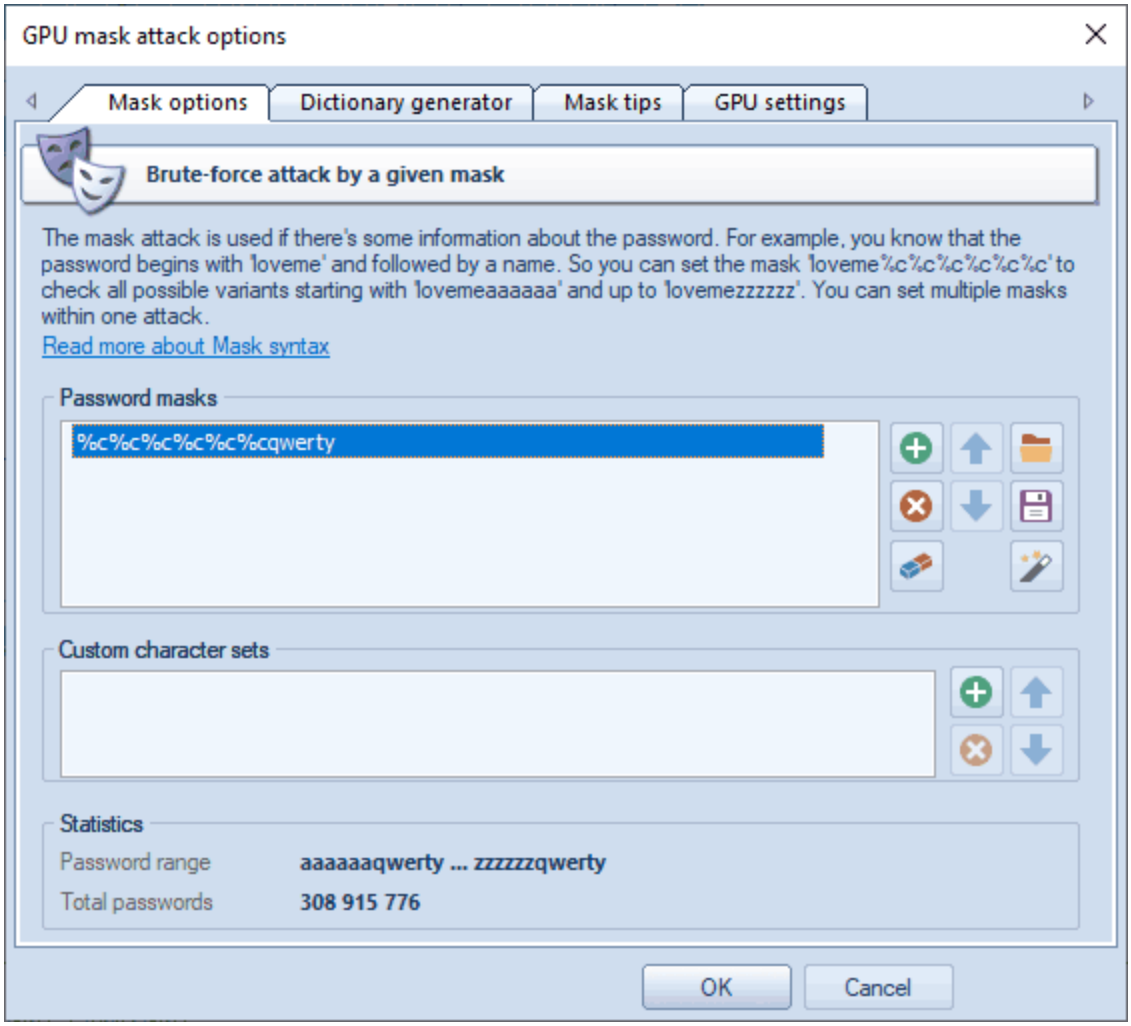
La **contraseña por subproceso** no se usa y siempre se establece en 1 al recuperar las credenciales almacenadas en caché del dominio tipo 2.

Al ejecutar la recuperación de contraseña para credenciales de dominio almacenadas en caché tipo 2, es posible que deba jugar con el parámetro Thread blocks para obtener un mejor rendimiento.
Establecer valores demasiado grandes puede hacer que la GPU se bloquee o genere un error, dependiendo de su Configuración de tiempo de espera del kernel de GPU.

2.8.2.17 GPU: Ataque de máscara

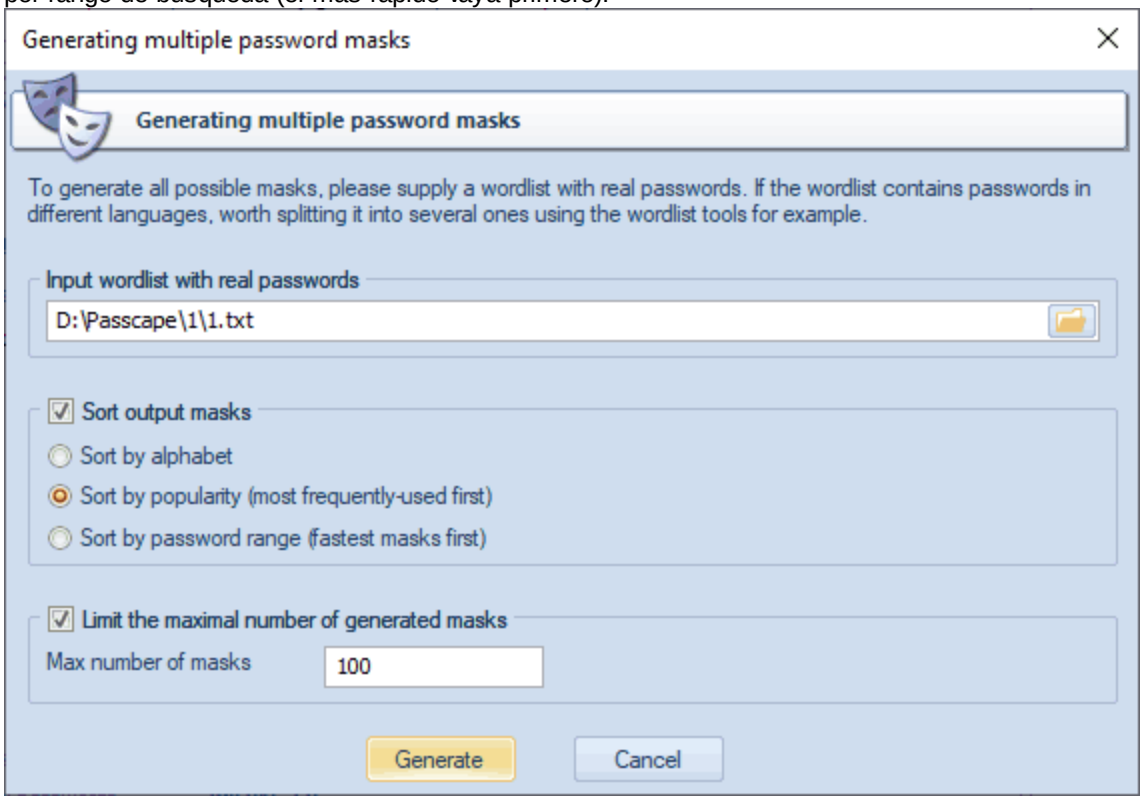
Opciones de máscara

Ataque de máscara es una herramienta insustituible cuando conoces un fragmento de la contraseña o tienes algún detalle específico al respecto. Por ejemplo, cuando sabe que la contraseña consta de 12 caracteres y termina con el qwerty, es obvio que buscar en todo el rango de contraseñas de 12 caracteres no es razonable (e inútil, ya que tarda años en completarse). Todo lo que se requeriría en este caso es adivinar los primeros 6 caracteres de la contraseña buscada. Para eso está el ataque con máscara.



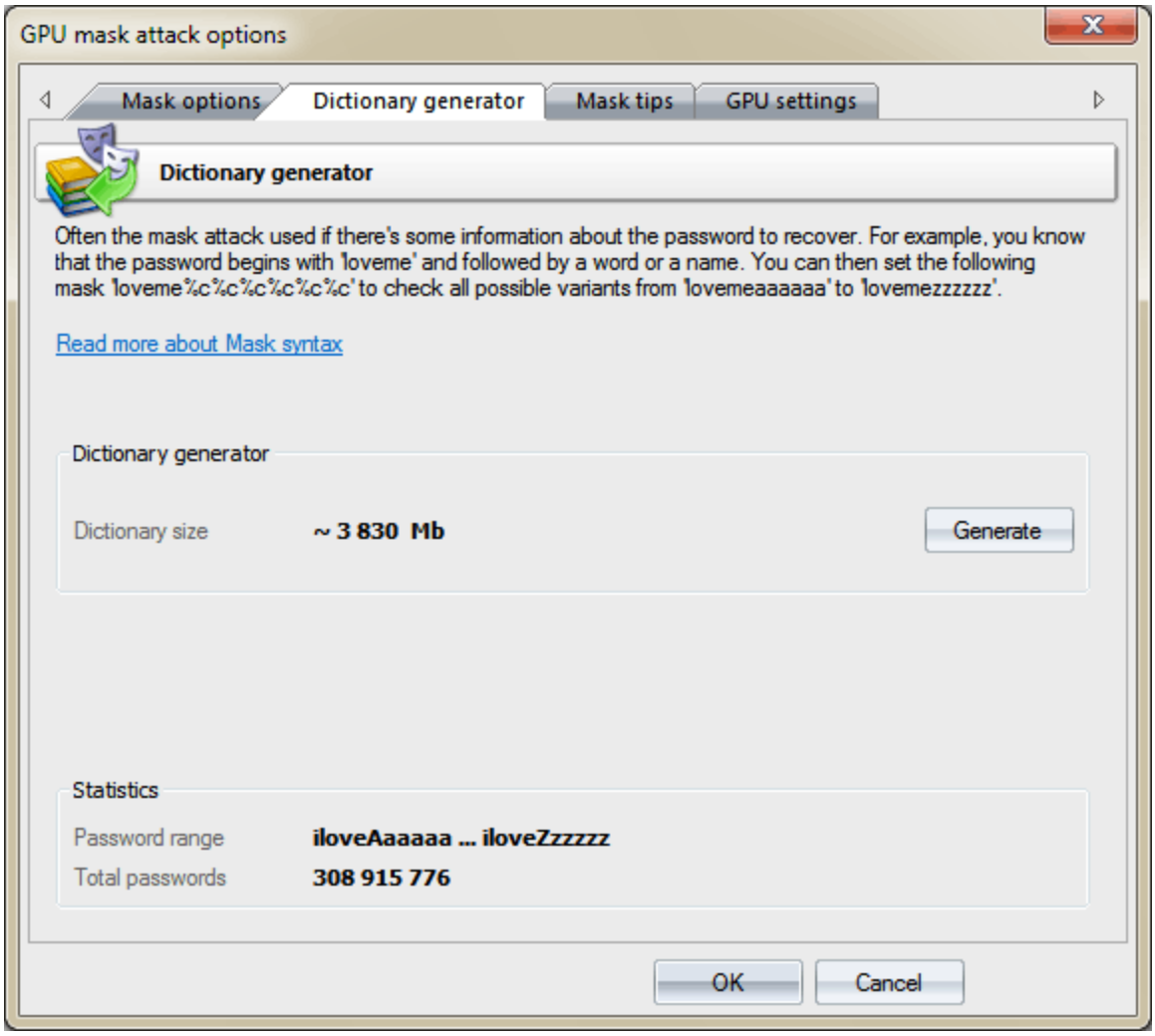
En nuestro caso, podríamos definir la siguiente máscara: **%c%c%c%c%c%cqwerty**. Eso significa que el programa comprobaría sucesivamente las siguientes combinaciones: aaaaaaqwerty, aaaaabqwerty, aaaaacqwerty.. zzzzzzqwerty. Si la contraseña original es '*secretqwerty*', alcanza perfectamente el rango.

El grupo de opciones máscaras de contraseña tiene como objetivo establecer una máscara (o varias), que se utilizarán para generar contraseñas por. En la mayoría de los casos, si conoce una parte de la contraseña, basta con especificar una sola máscara. Cuando se selecciona una máscara, el grupo de estadísticas muestra el rango de contraseñas de salida y el número de contraseñas generadas por esta máscara. Puede guardar sus máscaras en el disco para usarlo en otro proyecto, por ejemplo. El programa también le permite generar diccionarios mediante máscaras dadas.
Supongamos que tiene una lista de contraseñas descifradas y desea generar plantillas de máscara a partir de estas contraseñas. Nada más fácil. Ejecute el generador de máscaras  y muestre la ruta a su lista de contraseñas allí. Puede ordenar las máscaras resultantes alfabéticamente, popularidad o por rango de búsqueda (el más rápido vaya primero).



Generador de diccionarios

Al cambiar a la pestaña **Generador de diccionarios**, puede generar su propio diccionario mediante una máscara determinada y guardarlo en el disco. Esta función solo está disponible en la edición avanzada del programa.



Consejos para máscaras

La tercera pestaña de las opciones de máscara contiene una breve descripción de la sintaxis de la máscara y un par de ejemplos. La sintaxis de la máscara es bastante simple y consiste en caracteres estáticos (no modificables) y dinámicos (modificables). Los caracteres dinámicos siempre tienen un % a la vez Por ejemplo, si establece la máscara **secret%d%d%d%d**, el programa generará 10000 contraseñas (secret0000, secret0001, secret0002 .. secret9999).

Windows Password Recovery admite los siguientes conjuntos de máscaras dinámicas:

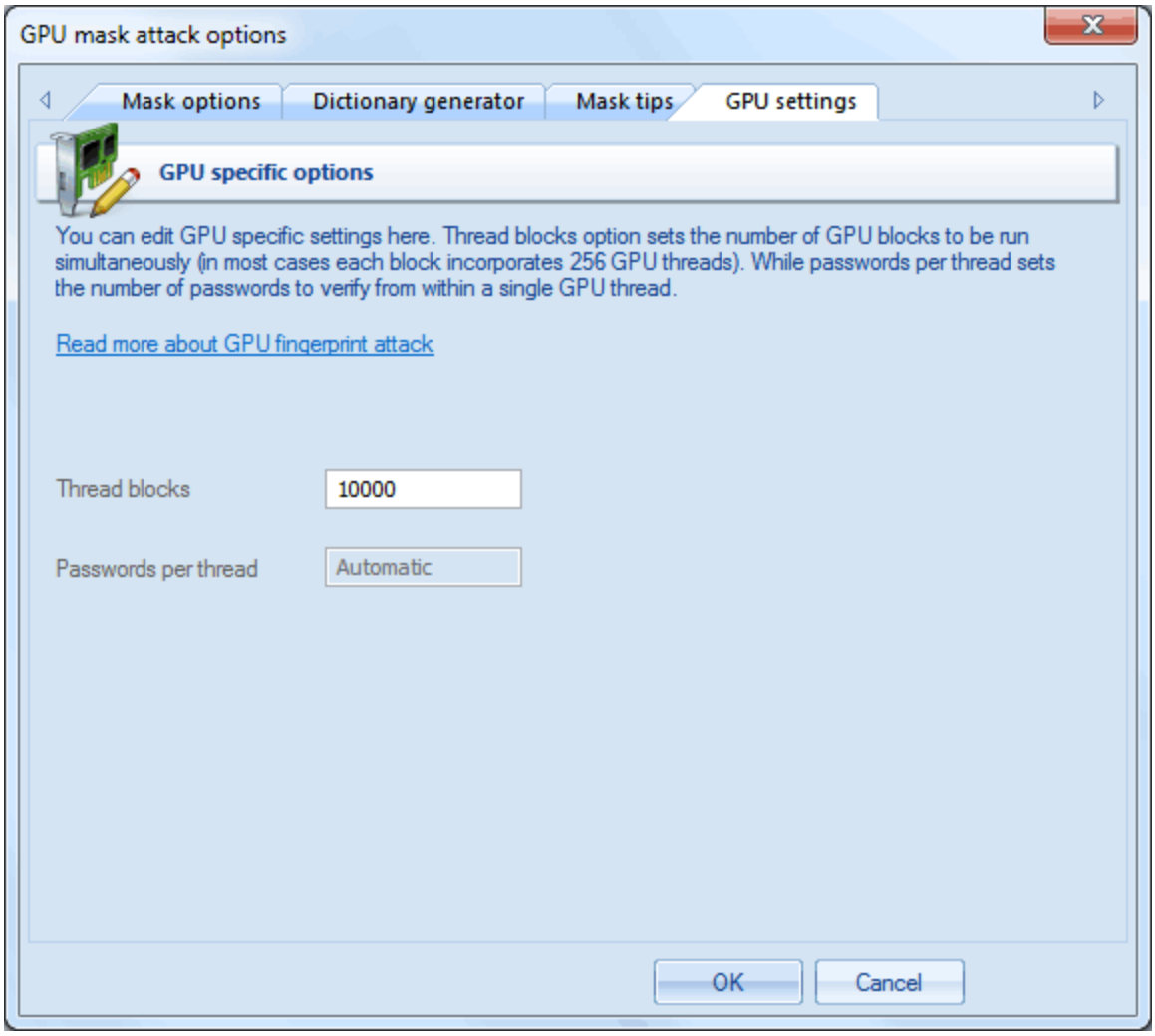
- **%c** caracteres latinos en minúsculas (a.. z), 26 símbolos
- **%C** caracteres latinos en mayúsculas (A.. Z), 26 símbolos
- **%#** conjunto completo de caracteres especiales (!.. ~ espacio), total de 33 símbolos
- **%@** pequeño conjunto de caracteres especiales (!@#$%^&*()-_+= espacio), 15 símbolos
- **%?** todos los caracteres imprimibles con códigos ASCII de 32..127
- **%*** todos los caracteres ASCII (códigos 1 a 255)
- **%d** un dígito (0..9)

- **%r(x-y)** caracteres definidos por el usuario con códigos ASCII serie entre x e y
- **%r(x1-y1,x2-y2...xn-yn)** conjunto de varias secuencias no superpuestas de caracteres ASCII. Útil para definir conjuntos de caracteres personalizados; por ejemplo, de caracteres OEM.
- **%1[2,3..9]** un carácter del conjunto de caracteres definido por el usuario 1..9
- **%%** carácter estático independiente %

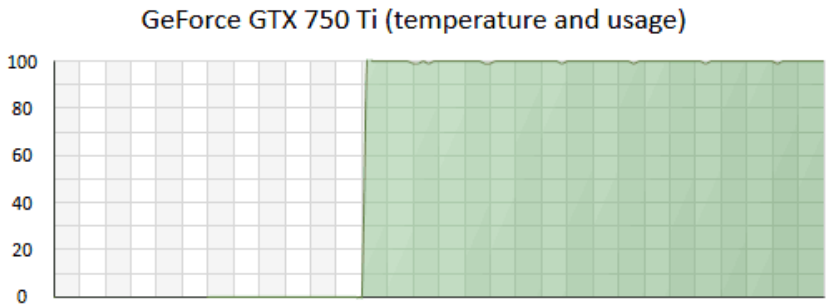
Ejemplos:
test%d - generará el rango de contraseñas test0.. test9, 10 contraseñas en total
test%d%d%d%d - test0000.. test9999, 10000 contraseñas
test%r(0x0600-0x06ff) - test_.. test_, 256 contraseñas con caracteres árabes al final
%#test%# - _test_.. ~test~, 1089 contraseñas
%1%1%1pin%2%2%2 - aaapin000.. zzzpin999, где %1 is user-defined charset 1 (a.. z), y %2- el segundo conjunto de caracteres definido por el usuario 0..9
ilove%1%1%1%1%1 - iloveaaaaa.. iloveZZZZZ, %1 es un conjunto de caracteres de usuario (a.. z, A.. Z)

La sintaxis del ataque de máscara de GPU difiere ligeramente de la utilizada en un ataque de máscara normal. La principal diferencia es que en el ataque basado en GPU no se pueden establecer números entre x e y y no se puede establecer el rango de longitud variable definido por el usuario, es decir, la siguiente sintaxis no funcionará para el ataque de máscara de GPU.:
%d(x-y)
%1[2,3..9](min-max)

Configuración de GPU
Antes de poder usarlo en un ataque, primero debe seleccionar la tarjeta gráfica en el Menú Opciones generales.

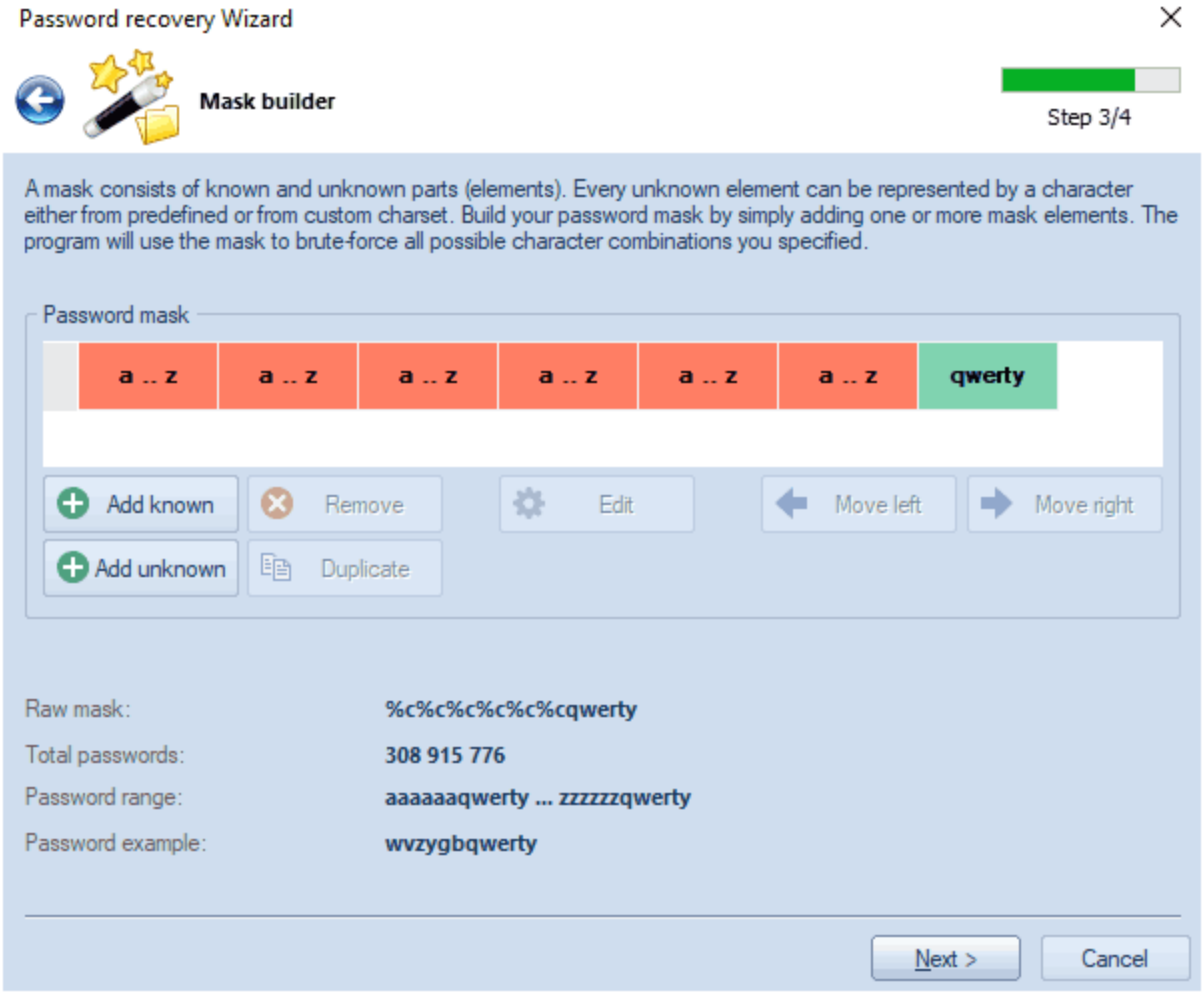


La configuración de GPU para el ataque Mask consta de solo 1 parámetro: el número de bloques de subprocesos que se ejecutarán en una sola llamada a la GPU. Cada bloque consta de 128 o 256 hilos. Por lo tanto, si establece el número de bloques en 10000, la GPU ejecutará 10000 * 256 = 2560000 subprocesos para una llamada al kernel de la GPU. Cada subproceso de GPU puede comprobar varias contraseñas. El número total de contraseñas verificadas depende en gran medida de otras opciones. Establecer el parámetro **ThreadBlocks** menor que 10000, en la mayoría de los casos, conduce a un rendimiento deficiente. Para evitar la degradación del rendimiento, después de configurar el parámetro y ejecutar el ataque, asegúrese de que el gráfico de carga de la GPU tenga un gráfico casi 100% simple sin miradas (consulte la captura de pantalla de NVidia GTX 750Ti que se ejecuta con 15000 bloques).



Al ejecutar la recuperación de contraseña para credenciales de dominio almacenadas en caché tipo 2, es posible que deba jugar con esta opción para obtener un mejor rendimiento.
Establecer valores demasiado grandes puede hacer que la GPU se bloquee o genere un error, dependiendo de su Configuración de tiempo de espera del kernel de GPU..

Si se siente perdido y harto de todas estas cosas, use el Mask Builder (en Password Recovery Wizard) que tiene una interfaz gráfica mucho más fácil de usar.



2.8.2.18 GPU: Ataque de fuerza de diccionario

A menudo, al crear contraseñas, los usuarios agregan ciertos caracteres al principio, al final o incluso a la mitad de la palabra. Para recuperar contraseñas de este tipo específico, hemos ideado un ataque de diccionario basado en GPU, que es algo entre un simple ataque de diccionario y un ataque de fuerza bruta.

Este ataque funciona de la siguiente manera:

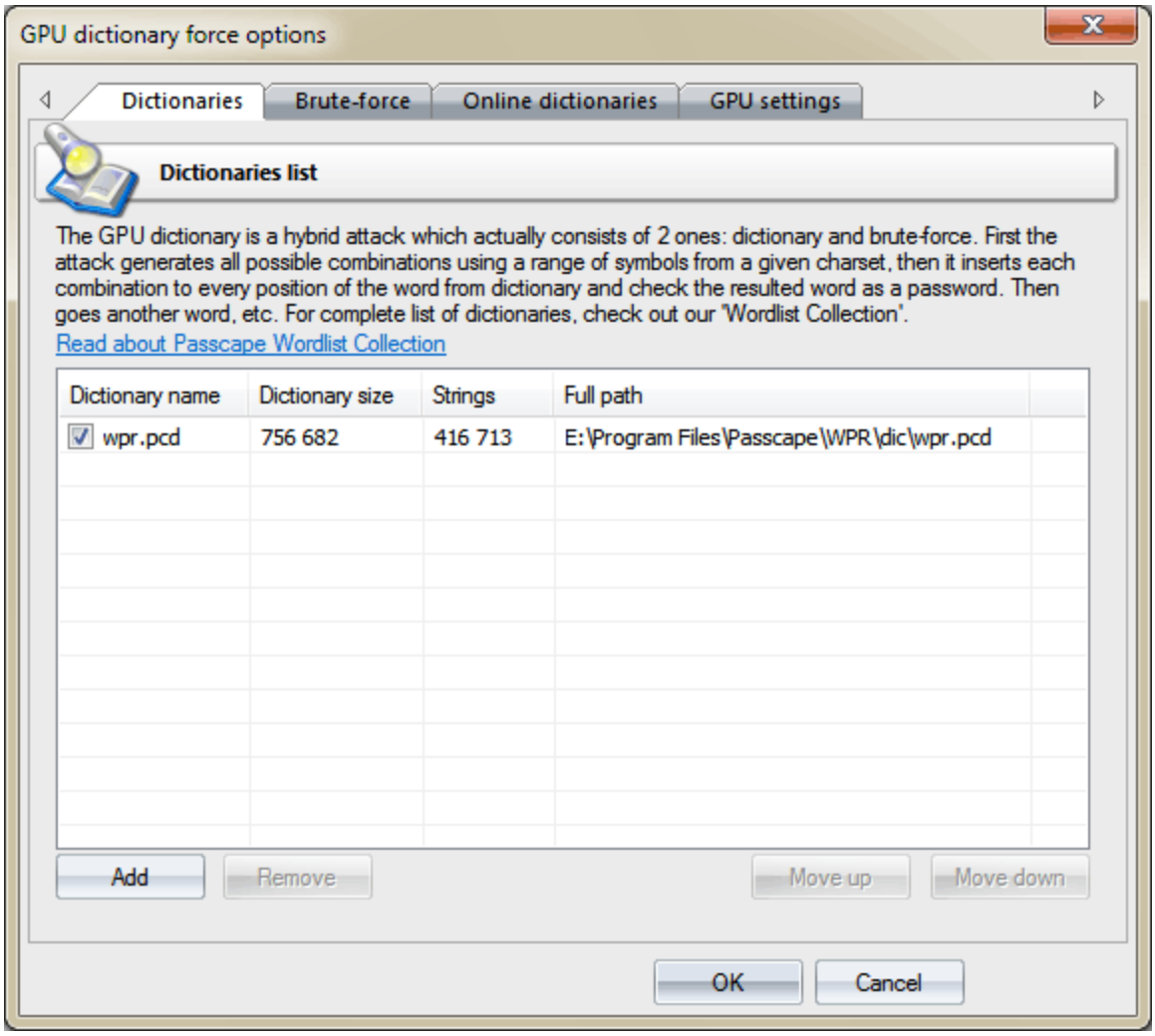
- Lee la primera palabra del diccionario.
- De acuerdo con el juego de caracteres definido y la longitud mínima/máxima del rango de búsqueda, genera todas las variantes posibles.
- Esas variantes (caracteres) se agregan al principio, al final o a la mitad de la palabra. La posición dentro de la palabra, donde se insertarían las secuencias generadas, se puede especificar a su discreción.
- Luego va la siguiente palabra del diccionario, etc.

Por ejemplo, si especificamos un rango de caracteres de búsqueda entre **0** y **9**, y la longitud del rango entre 1 y 2, el programa generará 100 combinaciones: 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11 .. 99. A continuación, estas secuencias se añadirán al principio, a la mitad o al final de la palabra. Por lo tanto, para la prueba de palabras, si las secuencias se van a insertar en cada posición enumerada, el programa verificará las siguientes contraseñas:
0test, 1test.. 99prueba
t0est, t1est.. t99est
te0st, te1st.. te99st
tes0t, tes1t.. tes99t
test0, test1 .. test99
Total - 100* 5 = 500 variantes.

Echemos un vistazo más de cerca a la configuración de ataque.

Dictionaries

En la pestaña Diccionarios, puede especificar la lista de diccionarios que se utilizarán en el ataque. El programa soporta listas de palabras de texto en los siguientes formatos: ASCII, UNICODE, UTF8, RAR, ZIP, así como diccionarios cifrados/empaquetados en el formato PCD nativo, desarrollado por nuestra empresa. Para desactivar un diccionario, simplemente desactive la casilla de verificación por su nombre. Por lo tanto, aunque el diccionario permanezca en la lista, será ignorado por el ataque. El software viene con el diccionario predeterminado de 400000 palabras. Puedes ordenar un juego completo de diccionarios, que tenga más de 6 GB de tamaño, en CD o aproveche los diccionarios disponibles en linea.

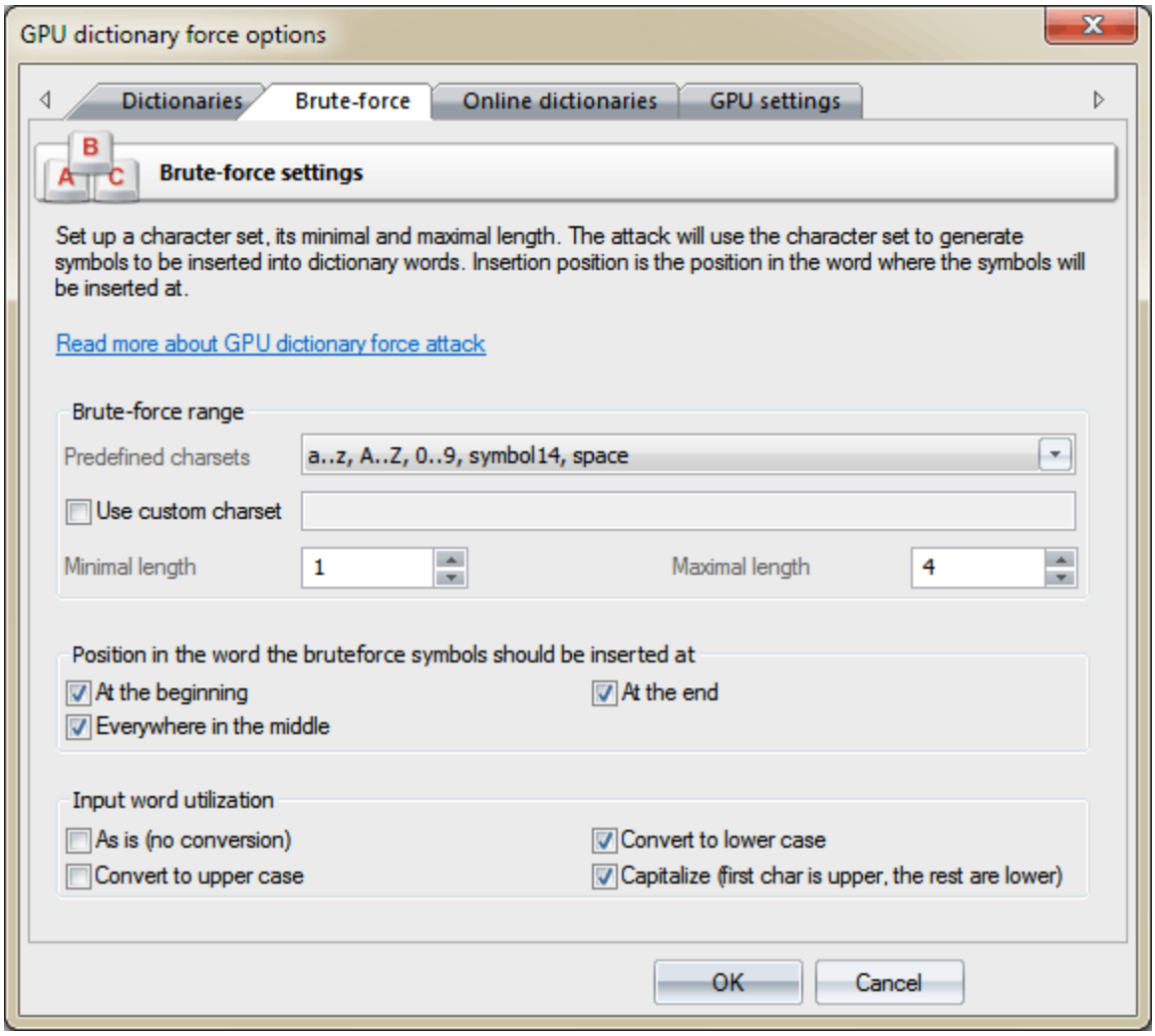


Rango de búsqueda

En esta pestaña, debe configurar el rango de caracteres que se insertará en las palabras base, su longitud mínima y máxima. Al configurar un rango, puede usar las plantillas existentes o, después de haber marcado la casilla de verificación respectiva, definir la suya propia. Al seleccionar la longitud máxima del rango, tenga en cuenta que no es aconsejable especificar un valor demasiado ancho o demasiado pequeño. Mientras que en el primer caso la velocidad de búsqueda de contraseñas puede reducirse a 0, especificar un rango demasiado estrecho de caracteres para buscar aumenta los gastos generales relacionados con el uso irracional de la potencia de cálculo de la GPU.

En el segundo grupo de opciones, especifique la posición en la palabra, donde se insertarían los caracteres del rango buscado.

Y, finalmente, el tercer grupo de configuraciones: estas se encargan de preprocesar las palabras del diccionario de origen. Al seleccionar la opción **Como es** hace que el programa use la palabra de origen tal cual, no convirtiendo a mayúsculas o minúsculas. El número de contraseñas que se buscarán crece en proporción directa al número de opciones especificadas en este grupo. Por otro lado, el programa es lo suficientemente inteligente como para no usar palabras repetidas. Por ejemplo, la palabra **12345678**, incluso si se establecen todas las opciones de conversión, se usará solo una vez.



El número de contraseñas que se buscarán por una sola palabra se puede calcular utilizando la siguiente fórmula:

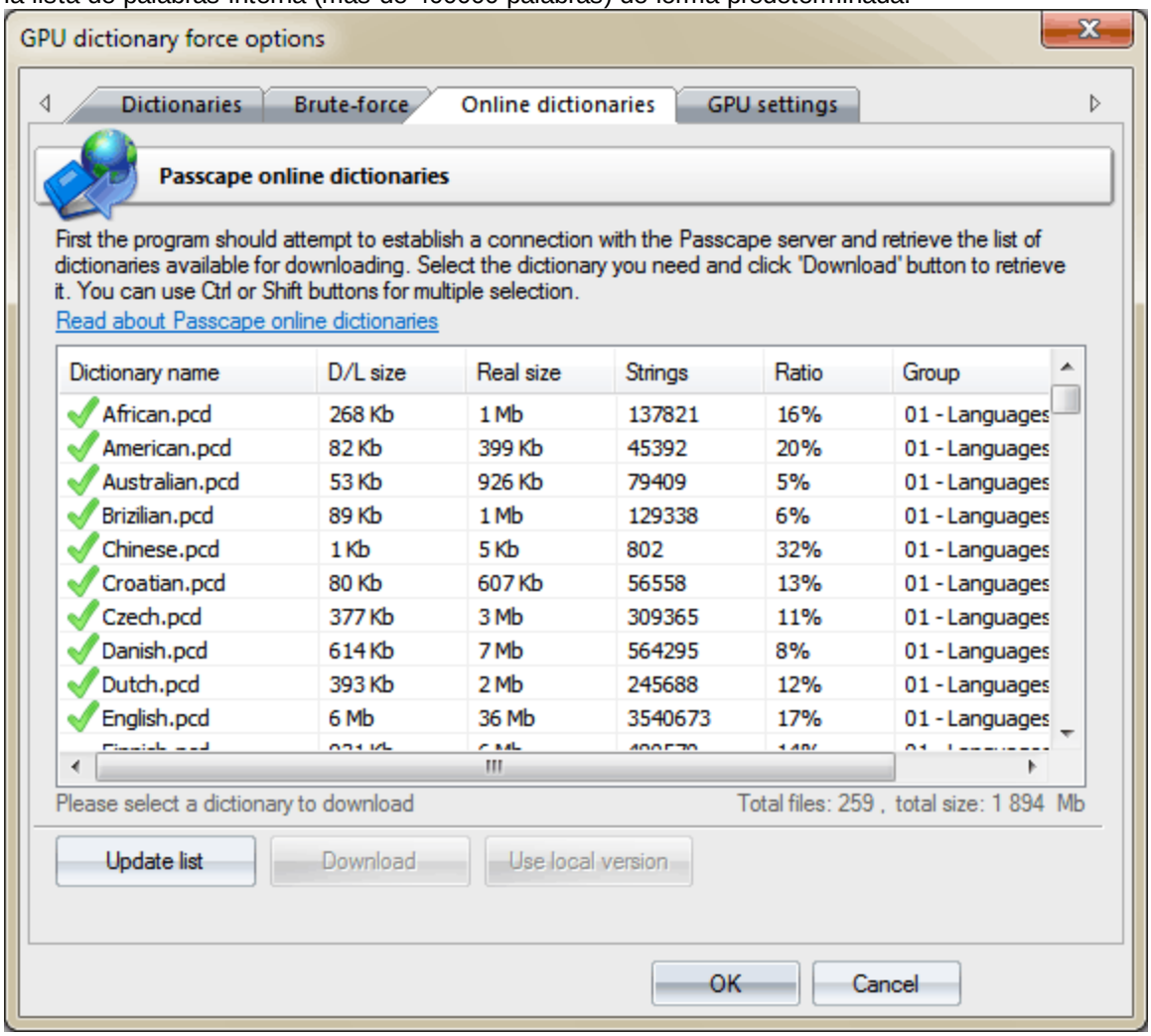
contraseñas = R * L * K
Dónde
R - rango de caracteres, calculado usando la fórmula: R = charset_length ^ max_length - charset_length ^ (min_length-1) +1
L - posiciones en palabra. Calculado de la siguiente manera: si la inserción se realiza en el medio de la palabra, L = password_length - 1; luego agregue más uno si la inserción se realiza al principio y al final de la palabra.
K - número de opciones especificadas en el grupo **'Utilización de palabras de entrada**'.

Por ejemplo, si la palabra de origen que tenemos es **ventana**, y las opciones se especifican como se muestra en la imagen de arriba, es decir, rango de caracteres **a.. z,A.. Z,0..9,symbol14,espacio**, inserción en todas las posiciones, conversión a minúsculas y mayúsculas (primera letra en mayúsculas). Calculemos cuántas contraseñas vamos a comprobar para esta palabra:
charset_length = 26+26+10+14+1 = 77
R = 77^4 - 77^0 + 1 = 35153041
L = (6-1) + 1 + 1 = 7
K = 2

contraseñas = 35153041 * 7 * 2 = **492 142 574**

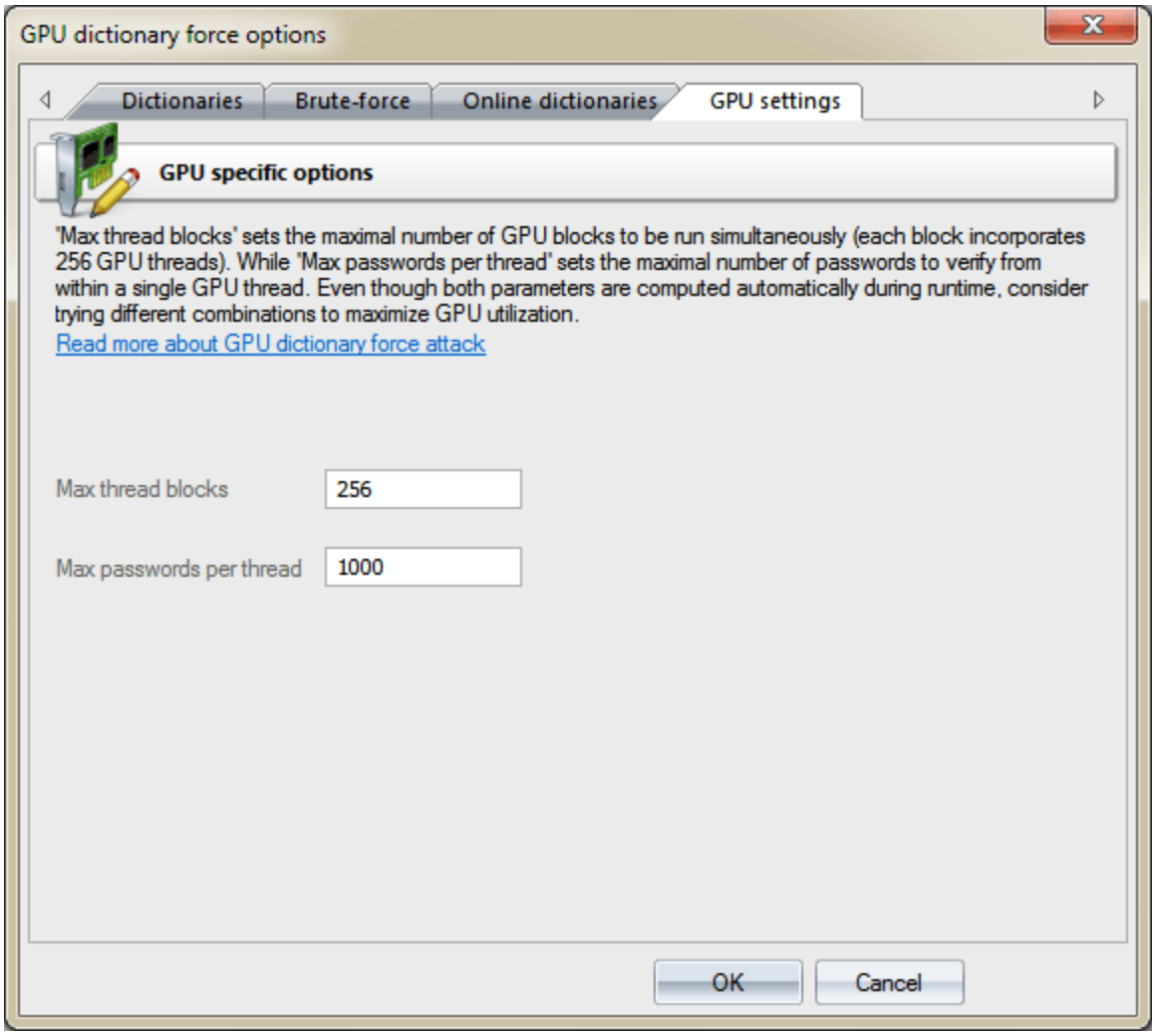
Diccionarios en línea

En la tercera pestaña, puede descargar listas de palabras de origen para el ataque. El programa utiliza la lista de palabras interna (más de 400000 palabras) de forma predeterminada.



Configuración de GPU

Antes de poder usar una GPU en el ataque, primero debe seleccionarla en el respectivo objeto del menú principal.



La configuración de la GPU es bastante simple y consta de solo dos configuraciones:

1. El número de bloques de tarjetas gráficas paralelas, donde se buscarían las contraseñas. Normalmente, cada bloque consta de 256 hilos. Por lo tanto, si establece el número de bloques en 256, la GPU ejecutará 256 * 256 = 65536 hilos. El número total de contraseñas verificadas para una llamada al kernel de la GPU será 256*ThreadBlocks*PasswordsPerThread. En nuestro caso 256*256*1000 = 65 536 000 contraseñas. La configuración de ThreadBlocks menor de 256 en las tarjetas gráficas modernas, en la mayoría de los casos, conduce a la degradación del rendimiento.
2. El número de contraseñas que se buscarán desde un solo subproceso. Cuanto mayor sea el valor, menor será la sobrecarga asociada con el lanzamiento de subprocesos y mayor será la velocidad de búsqueda. Sin embargo, establecer un valor demasiado grande puede bloquear el equipo o causar fluctuaciones significativas en la velocidad de búsqueda actual, que se muestra en la pestaña de estado del ataque. Esto se debe al hecho de que el tiempo de finalización de la tarea en la GPU excede el tiempo requerido para actualizar el estado actual del ataque.

Dependiendo de las opciones que haya especificado, una elección adecuada de la configuración de la GPU puede aumentar drásticamente, a menudo varias veces, la velocidad de búsqueda de contraseñas. Recomendamos jugar con la configuración de la GPU para lograr la máxima utilización de la GPU en este ataque.

La **contraseña máxima por subproceso** no se usa y siempre se establece en 1 al recuperar las credenciales almacenadas en caché del dominio tipo 2.
Al ejecutar la recuperación de contraseña para credenciales almacenadas en caché de dominio tipo 2, es posible que deba jugar con el parámetro **Max thread blocks** para obtener un mejor rendimiento.
Establecer valores demasiado grandes puede hacer que la GPU se bloquee o genere un error, dependiendo de su GPU kernel timeout settings.

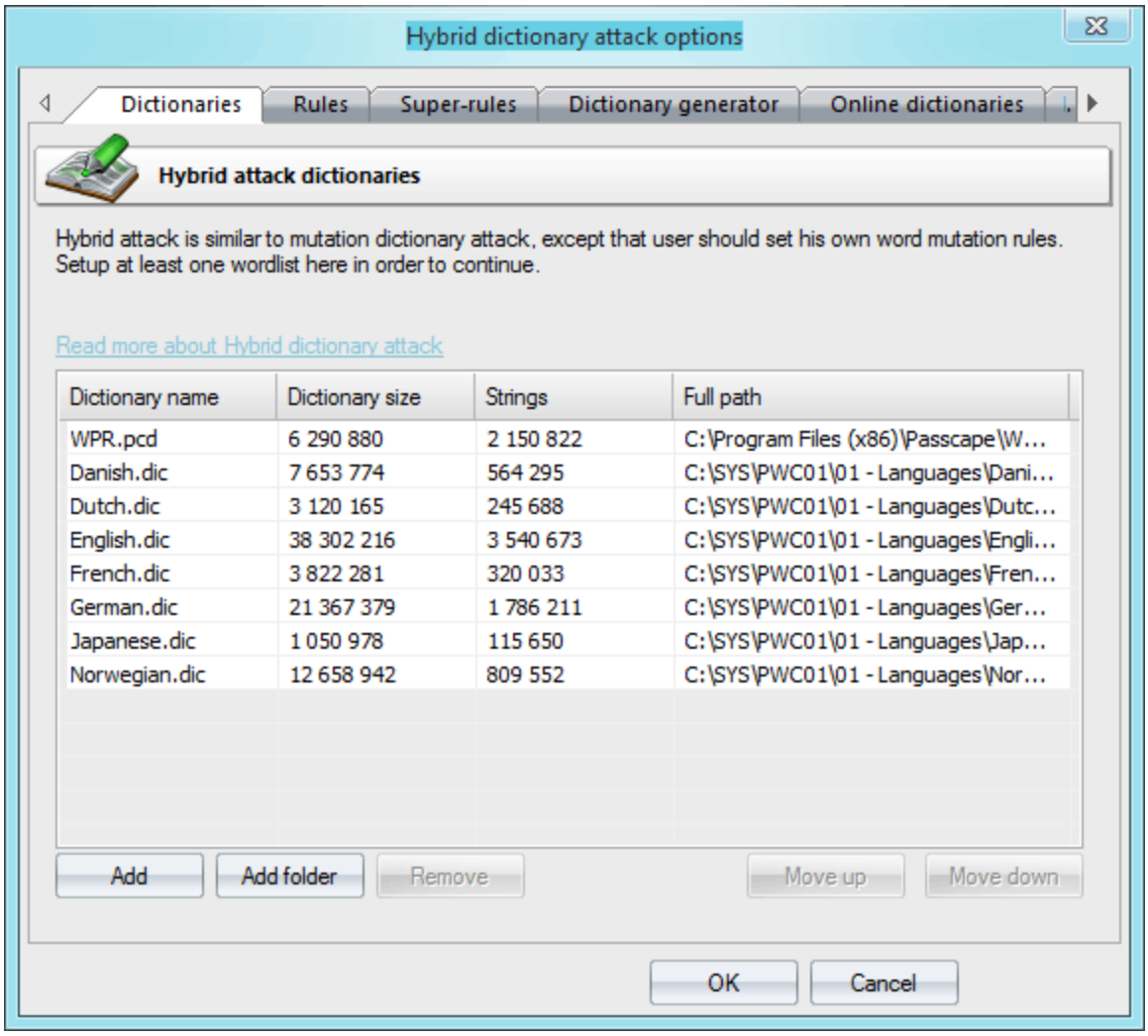
2.8.2.19 GPU: Ataque de diccionario híbrido

El ataque de diccionario híbrido de GPU es más o menos el mismo que el ataque de diccionario híbrido, excepto que utiliza la potencia de su GPU en lugar de la CPU. Eso lo hace extremadamente rápido. Aproximadamente 10 veces más rápido que un simple ataque híbrido. Sin embargo, el valor depende en gran medida de las opciones y el hardware utilizado. El ataque híbrido permite al usuario establecer sus propias reglas de modificación de palabras e intentar validar las palabras de salida modificadas.

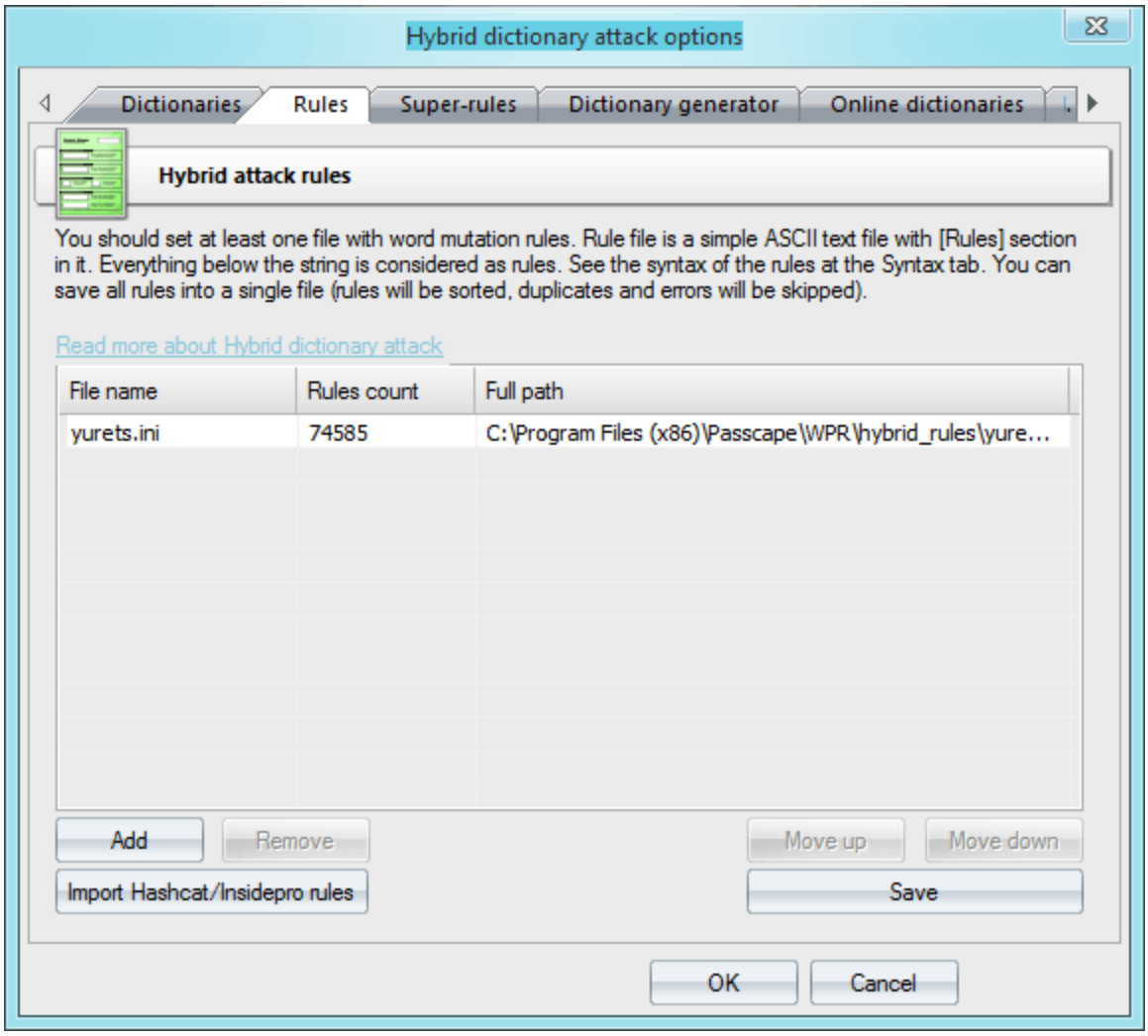
Las acciones, realizadas en palabras de origen del diccionario, se denominan reglas. Se pueden aplicar varias reglas a cada palabra de origen.

La configuración de ataque del diccionario híbrido de GPU se agrupa en ocho pestañas:
1. **Diccionarios** - para configurar diccionarios de origen.
2. **Reglas** - archivos con conjunto de reglas.
3. **Super-reglas** - los que se aplicarán por encima de las reglas regulares
4. **Generador de diccionarios**, donde puede crear archivos de palabras obtenidas del ataque híbrido.
5. **Diccionarios en línea** - para descargar nuevos diccionarios a la aplicación.
6. **Sintaxis de ataque** - descripción completa de todas las reglas con ejemplos.
7. **Probador de reglas**, donde puedes probar tus reglas.
8. **Configuración de GPU** se utiliza para ajustar los parámetros de la GPU.

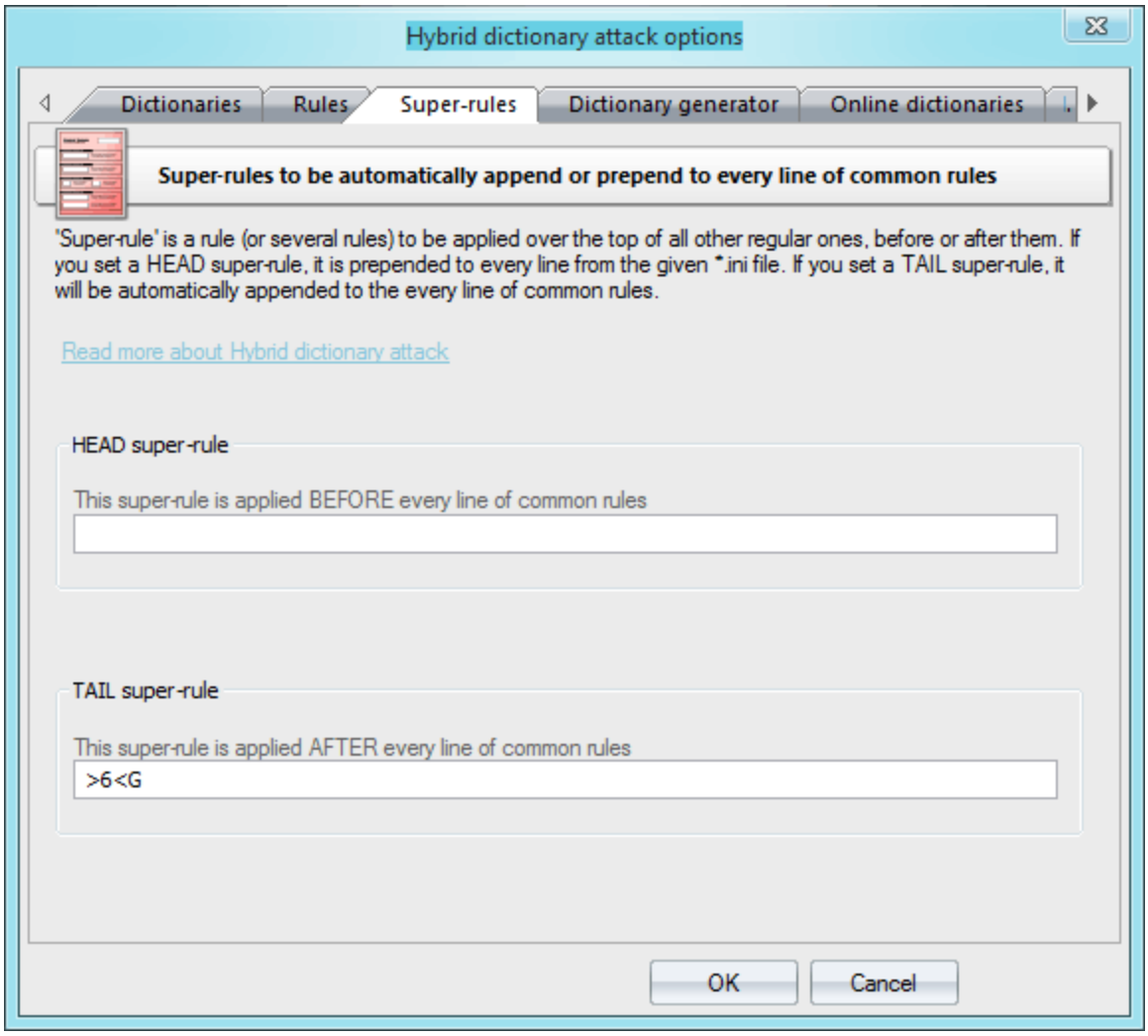
Las listas de palabras que se utilizarán en el ataque se establecen en la primera pestaña. Tradicionalmente, la aplicación admite listas de palabras en formato ASCII, UTF8, UNICODE, PCD, RAR y ZIP. La posición de los archivos en la lista puede ser alterada. Por ejemplo, es posible que desee mover diccionarios más pequeños hacia arriba en la lista o al revés. Durante el ataque, se usarán uno tras otro, de acuerdo con su posición en la lista.



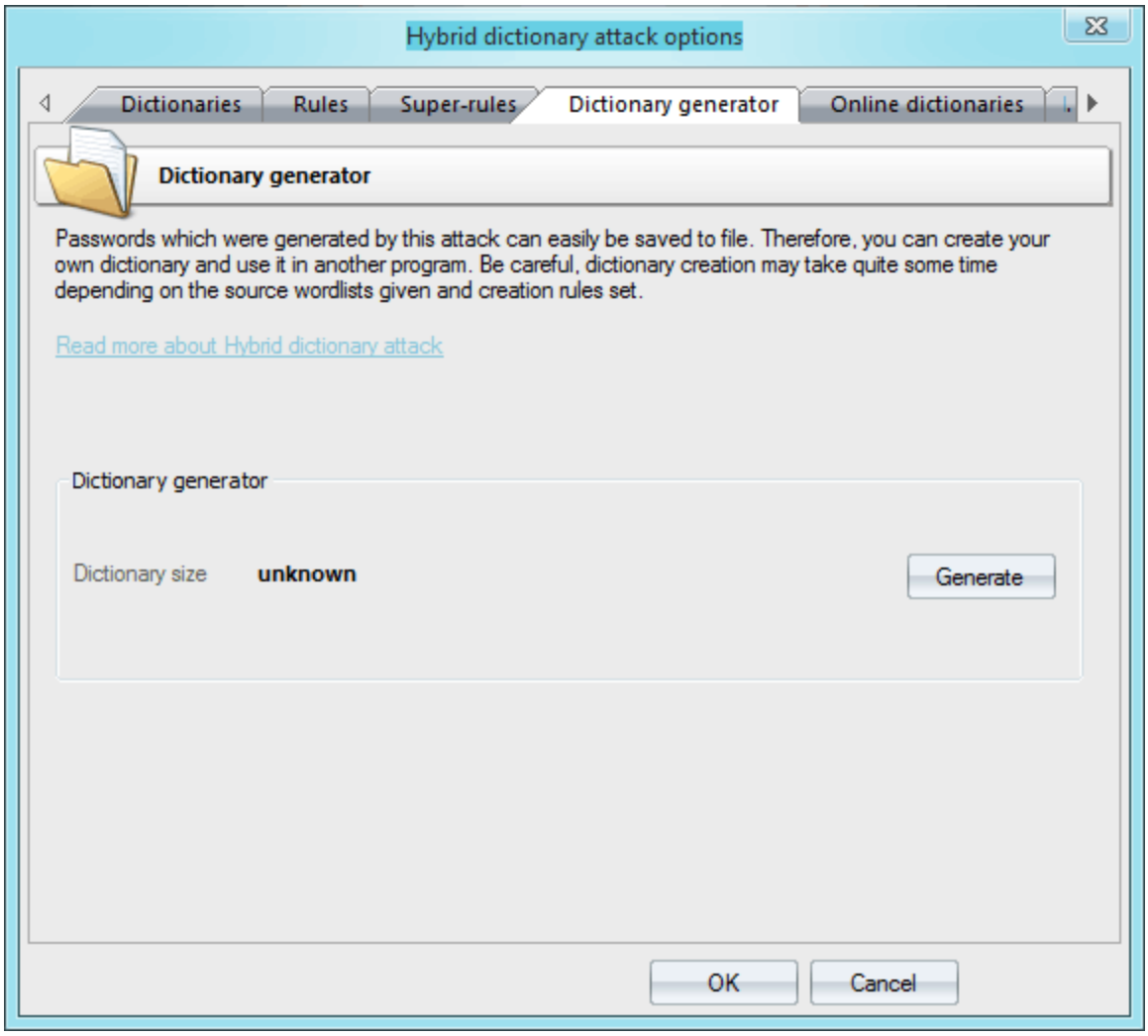
En la pestaña **'Reglas'**, defina al menos un archivo con reglas de mutación de contraseña. El formato del archivo de reglas es bastante trivial; es un archivo ASCII de texto sin formato con la cadena **'[Rules]'**. Cualquier cosa por encima de esta cadena se considera como comentarios e ignorada por el programa. Todo lo que va por debajo de esta cadena se considera como reglas. Cada cadena puede contener varias reglas, aplicables a una palabra de origen. Si una cadena contiene varias reglas por palabra, esas reglas se analizan de izquierda a derecha. Por ejemplo, si aplica la regla '@pc$a$b$c' a la palabra de origen **'contraseña'**, en la salida obtendrá 'Asswordabc'. La longitud máxima de una palabra de salida no puede exceder los 256 caracteres.



'Super-regla' es una regla (o varias reglas) que se aplica sobre todas las demás reglas regulares, antes o después de ellas. Por ejemplo, puede establecer la superar regla de cola 'a8' para crear todas las combinaciones de casos posibles después de que se haya realizado una mutación común. Por lo tanto, la regla '/asa4' de l33t.ini archivo se convertirá en '/asa4a8', '/csc(' se convertirá en '/csc(a8', etc. Otro ejemplo más: establecer la regla de cabeza '>6<G' le permite omitir todas las palabras de menos de 6 o más de 16 caracteres, antes de comenzar una mutación común. Esta es una característica útil una vez que decida agregar la misma regla a todas las líneas de texto de los archivos *.ini seleccionados. No hay necesidad de modificarlos todos. Sin embargo, tenga cuidado, la superar regla 'aN' puede aumentar drásticamente el número total de contraseñas generadas.

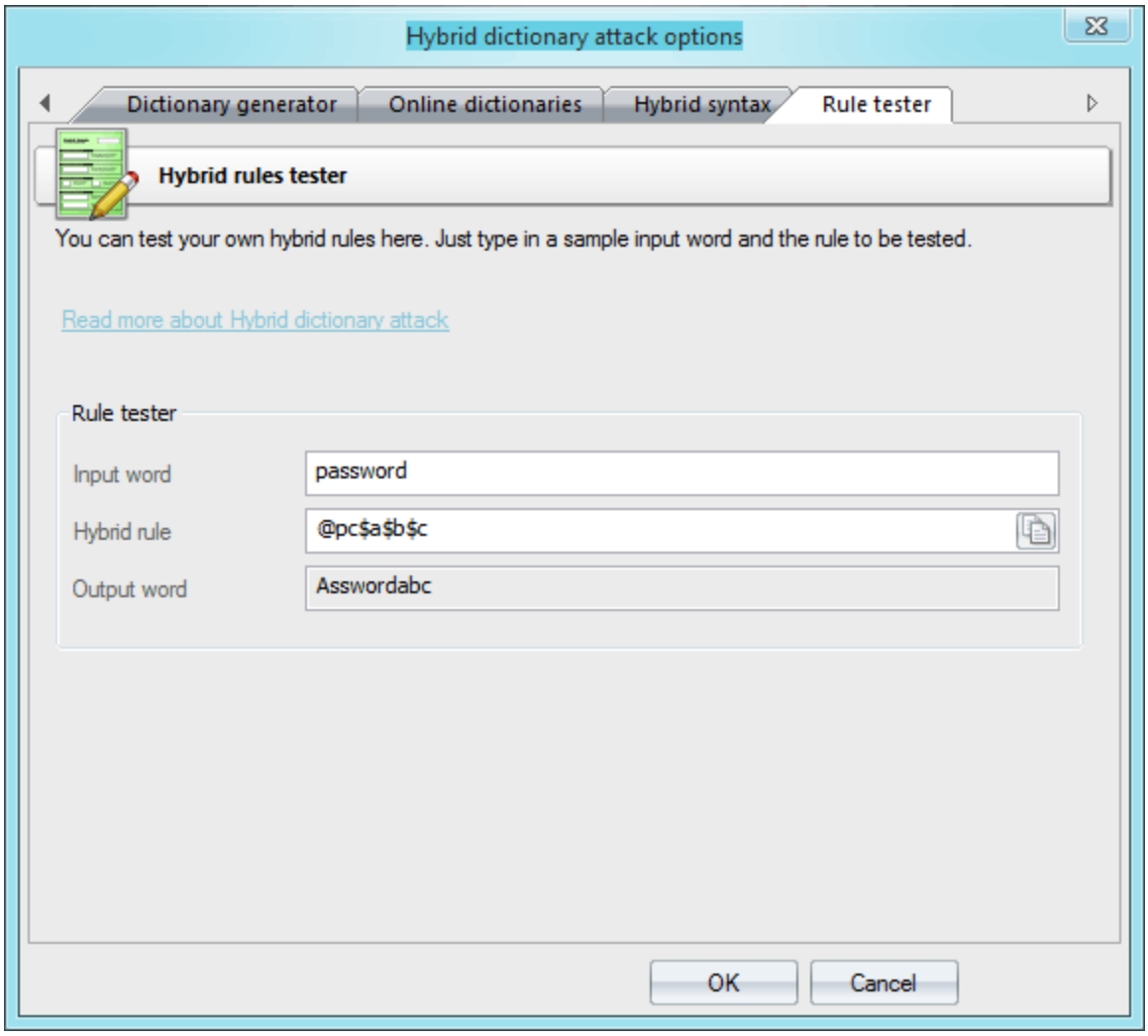


La pestaña **'Generador de diccionarios'** está diseñada para generar diccionarios obtenidos de un ataque. Esos diccionarios personalizados podrían usarse, por ejemplo, en otras aplicaciones. Para generar un diccionario, especifique un diccionario de origen y un conjunto de reglas de mutación para él. El tamaño de un archivo de destino puede superar los 2 GB suponiendo que lo guarde en el disco NTFS. Tenga cuidado, ¡el proceso de generación del diccionario puede tomar mucho tiempo y espacio en disco!



Puede descargar listas de palabras adicionales para el ataque utilizando '[Diccionarios en linea]' tab.

Si desea crear su propio conjunto de reglas, puede usar las dos pestañas siguientes como fuentes de ayuda. Mientras que la pestaña '**Sintaxis**' ofrece meras descripciones de las reglas disponibles, en la pestaña **'Probador de reglas'** puede verificarlas especificando una palabra de origen y una regla. Envíenos sus conjuntos de reglas; si los encontramos interesantes/útiles, los incluiremos en el programa.



Descripción de las reglas para el ataque de diccionario híbrido

Se permite establecer varias reglas en una línea.
Las reglas (si las hay) se procesan de izquierda a derecha.
La longitud máxima de la línea está limitada a 256 caracteres.
La longitud máxima de las palabras de salida está limitada a 256 caracteres.
El espacio en blanco se ignora siempre que no se utilice como parámetro.
Una línea que comienza con el carácter # considerado como un comentario
Todo el texto anterior a la línea «[Reglas]» se considera comentario.
N y M siempre comienzan en 0. Para valores mayores de 9 utilice A.. Z (A=10, B=11, etc.)
Las siguientes reglas deben estar en la última posición de una línea: aN, ?iN[C], ?i[C], ?oN[C], ?o[C], ?iZ[C], ?oZ[C]
No cambie los nombres de los archivos de reglas estándar. Algunos son utilizados por el programa.
?iN[C], ?i[C], ?oN[C], ?o[C] ?iZ[C], ?oZ[C] las reglas utilizan los siguientes conjuntos de caracteres predefinidos (aunque puede usar conjuntos de caracteres personalizados):

digits	- 0123456789
loweralpha	- abcdefghijklmnopqrstuwxyz
upperalpha	- ABCDEFGHIJKLMNOPQRSTUVWXYZ
alpha	- abcdefghijklmnopqrstuwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ
special	- !@#$%^&*()-_+=~`[]{}|\:;"'<>,.?/ "

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

Reglas

Regla	Ejemplo	Entrada	Salida	Descripción
:	:	password	password	No hace nada con la palabra de entrada
{	{	password	asswordp	Gira la palabra a la izquierda
}	}	password	dpasswor	Girar la palabra a la derecha
[	[	password	assword	Eliminar el primer carácter
]	]	password	passwor	Elimine el último carácter
c	c	password	Password	Mayúsculos
C	C	password	pASSWORD	Anti-mayúsculas (minúsculas el primer carácter, mayúsculas el resto)
d	d	password	passwordpassword	Palabra duplicada
f	f	password	passworddrowssap	Reflejar palabra
k	k	password пароль	зфыыцщкв gfhjkm	Convierta Word usando una distribución de teclado alternativa (primero después de la predeterminada). La regla funciona en ambas direcciones. Por ejemplo, si hay una distribución de teclado rusa instalada previamente en el sistema, la regla debe convertir la palabra 'contraseña' a la rusa 'зфыыцщкв', y la palabra rusa 'пароль' a 'gfhjkm'. Esto es muy útil cuando se buscan contraseñas que no estén en inglés. Si solo hay un idioma instalado en el sistema, la regla no hace nada.
K	K	password	passwodr	Intercambiar los dos últimos caracteres
l	l	password	password	Convertir todos los caracteres en minúsculas
q	q	password	ppaasssswwoorrdd	Duplicar todos los símbolos
r	r	password	drowssap	Palabra inversa
t	t	PassWord	pASSwORD	Alternar mayúsculas y minúsculas de todos los caracteres
u	u	password	PASSWORD	Convertir todos los caracteres en mayúsculas
U	U	my own password	My Own Password	Poner en mayúsculas todas las palabras delimitadas con espacio (en mayúsculas el primer carácter y cada carácter después de un espacio)
V	V	password	PaSSWoRD	Vocales élite

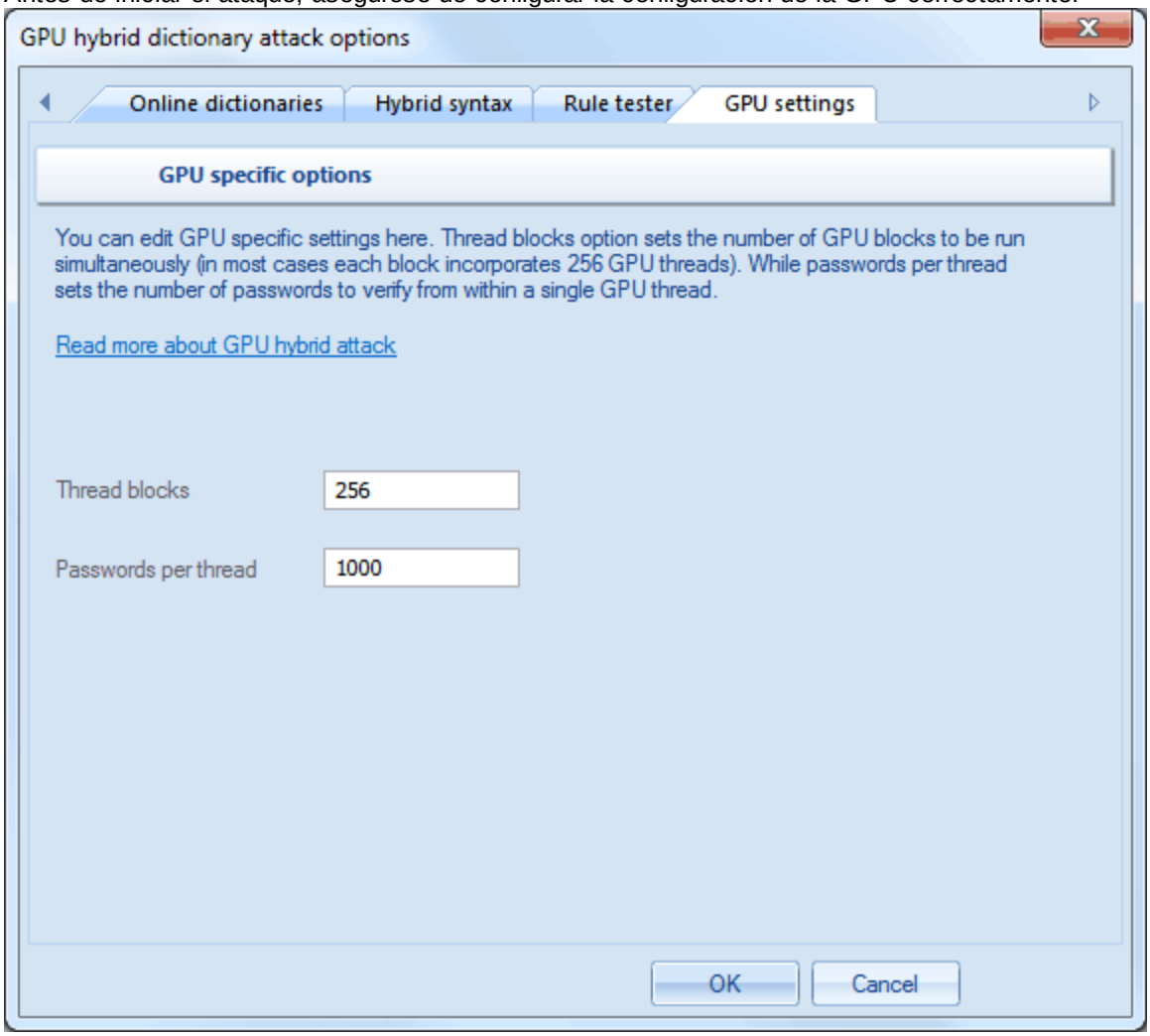
Regla	Ejemplo	Entrada	Salida	Descripción
v	v	password	pASSWoRD	Vocales sin élite
'N	'4	password	pass	Truncar la palabra a N caracteres de longitud
+N	+1	password	pbssword	Carácter de incremento en la posición N por 1 valor ASCII
-N	-0	password	oassword	Carácter de disminución en la posición N por 1
.N	.4	password	passoord	Reemplace el carácter en la posición N por el carácter en la posición N+1
,N	,1	password	ppssword	Reemplace el carácter en la posición N por el carácter en la posición N-1. Donde N > 0.
<N				Rechazar (omitir) la palabra si tiene más de N caracteres de largo
>N				Rechazar (omitir) la palabra si tiene menos de N caracteres de longitud
aN				Compruebe todos los casos de símbolos posibles para la palabra. N es una longitud máxima de la palabra para aplicar esta regla.
DN	D2D2	password	paword	Eliminar el carácter en la posición N
pN	p3	key	keykeykey	Copiar palabra N veces
TN	T1T5	password	pAsswOrd	Alternar mayúsculas y minúsculas del carácter en la posición N
yN	y3	password	paspassword	Duplicar los primeros N caracteres
YN	Y3	password	paswordord	Duplicar los últimos N caracteres
zN	z3	password	ppppassword	Duplicar el primer carácter de la palabra N veces
ZN	Z3	password	passwordddd	Duplicar el último carácter de la palabra N veces
$X	$0$0$7	password	password007	Agregar el carácter X al final de la palabra
^X	^3^2^1	password	123password	Insertar el carácter X al principio de la palabra
@X	@s	password	paword	Quitar todos los caracteres X de la palabra
!X				Rechazar (omitir) la palabra si contiene al menos un carácter X
/X				Rechazar (omitir) la palabra si no contiene el carácter X
(X				Rechazar (omitir) la palabra si el primer carácter no es X
)X				Rechazar (omitir) la palabra si el último carácter no es X
eX	e@	mike@yahoo.com	mike	Extraiga una subcadena que comienza en la posición 0 y termina antes de la primera aparición del carácter X (no haga nada si no se encuentra X)
EX	E@e.	mike@yahoo.com	yahoo	Extraiga una subcadena que comienza justo después de encontrar el primer carácter X y hasta el final de la cadena (no haga nada si no se encuentra X)
%MX				Rechazar (omitir) la palabra si no contiene al menos M instancias del carácter X

Regla	Ejemplo	Entrada	Salida	Descripción
***XY**	*15	password	possward	Intercambiar caracteres en las posiciones X e Y
=NX				Rechazar (omitir) la palabra si el carácter en la posición N no es igual a la X
iNX	i4ai5bi6c	password	passabcword	Inserte el carácter X en la posición N
oNX	o4*o5*	password	pass**rd	Sobrescribir un carácter en la posición N con el carácter X
sXY	ss$so0	password	pa$$w0rd	Reemplazar todos los caracteres X por Y
xNM	x4Z	password	word	Extraiga una subcadena de hasta M caracteres de longitud, a partir de la posición N.
INX-Y	rl0/-/r	google.com	google.com/	Inserte el carácter X en la posición N si el carácter anterior en la posición N no es Y.
INX+Y	rl0.+.r	password.	password..	Inserte el carácter X en la posición N si el carácter anterior en la posición N es Y.
ONX-Y	O0-+p	password	-assword	Si el carácter en la posición N no es Y, sobrescriba con el carácter X.
ONX+Y	O0P+p	password	Password	Si el carácter en la posición N es Y, sobrescriba con el carácter X.
RNM+Y	R01+a	password	assword	Quitar el carácter en la posición N si el carácter en la posición M es Y
RNM-Y	R40-b	password	passord	Quitar el carácter en la posición N si el carácter en la posición M no es Y
?iN[C]	?i0[digits]	password	0password, 1password ... 9password	Inserte un carácter de un conjunto de caracteres [C] en la posición N de la palabra. Donde C debe ser un nombre de conjunto de caracteres predefinido o un conjunto de caracteres personalizado.
?iZ[C]	?iZ[digits]	password	password0, password1 ... password9	Inserte un carácter de un conjunto de caracteres [C] en la última posición de la palabra. Donde C debe ser un nombre de conjunto de caracteres predefinido o un conjunto de caracteres personalizado.
?i[C]	?i[special]	password	~password, !password ... password_, password+	Inserte un carácter de un conjunto de caracteres [C] en cada posición de la palabra. Donde C debe ser un nombre de conjunto de caracteres predefinido o un conjunto de caracteres personalizado.
?oN[C]	?o1[upperalpha]	password	pAssword, pBssword ... pZssword	Sobrescriba un carácter en la posición N con un carácter tomado de un conjunto de caracteres [C]. Donde C debe ser un nombre de conjunto de caracteres predefinido o un conjunto de caracteres personalizado.
?oZ[C]	?oZ[upperalpha]	password	passworA, passworB ... passworZ	Sobrescriba un carácter en la última posición con un carácter tomado de un conjunto de caracteres [C]. Donde C debe ser un nombre de conjunto de caracteres predefinido o un conjunto de caracteres personalizado.

Regla	Ejemplo	Entrada	Salida	Descripción
?o[C]	?o[-=.]	password	-assword, =assword ... passwor.	Sobrescriba un carácter en cada posición de la palabra con un carácter tomado de un conjunto de caracteres [C]. Donde C debe ser un nombre de conjunto de caracteres predefinido o un conjunto de caracteres personalizado.

Configuración de GPU

Antes de iniciar el ataque, asegúrese de configurar la configuración de la GPU correctamente.



La configuración de la GPU es bastante simple y consta de dos parámetros:

1. El número de bloques de GPU que se ejecutarán en una sola llamada a gpu. Cada bloque consta de 256 hilos. Por lo tanto, si establece el número de bloques en 256, la GPU ejecutará 256 * 256 = 65536 hilos. El número total de contraseñas verificadas para una llamada al kernel de la GPU será 256*ThreadBlocks*PasswordsPerThread. En nuestro caso 256*256*1000 = 65 536 000 contraseñas por una llamada a GPU.
2. El número de contraseñas que se buscarán en un solo subproceso de GPU. Cuanto mayor sea el valor, menor será la sobrecarga asociada con el lanzamiento de subprocesos y mayor será la velocidad de búsqueda. Sin embargo, establecer un valor demasiado grande puede bloquear la

computadora, hacer que su GPU no responda o causar fluctuaciones significativas en la velocidad de búsqueda actual, que se muestra en la pestaña de estado del ataque. Esto se debe al hecho de que el tiempo de finalización de la tarea en la GPU excede el tiempo requerido para actualizar el estado actual del ataque.

Tenga cuidado al establecer reglas "pesadas" como aN, ?iN, ?oN, etc. Estas reglas pueden aumentar el número de contraseñas generadas en cien veces y colgar su sistema o hacer que su dispositivo GPU no responda.

Las **contraseñas por subproceso** no se utilizan y siempre se establecen en 1 al recuperar las credenciales almacenadas en caché del dominio, tipo 2.
Al ejecutar la recuperación de contraseña para credenciales de dominio almacenadas en caché tipo 2, es posible que deba jugar con el parámetro Thread blocks para obtener un mejor rendimiento.
Establecer valores demasiado grandes puede hacer que la GPU se bloquee o genere un error, dependiendo de su configuración de tiempo de espera del kernel de GPU.

2.9 Menú Ver

El menú Ver habilita/deshabilita los elementos auxiliares de la interfaz, cambia el idioma de la interfaz, minimiza la aplicación en la bandeja o la ejecuta en el modo invisible.

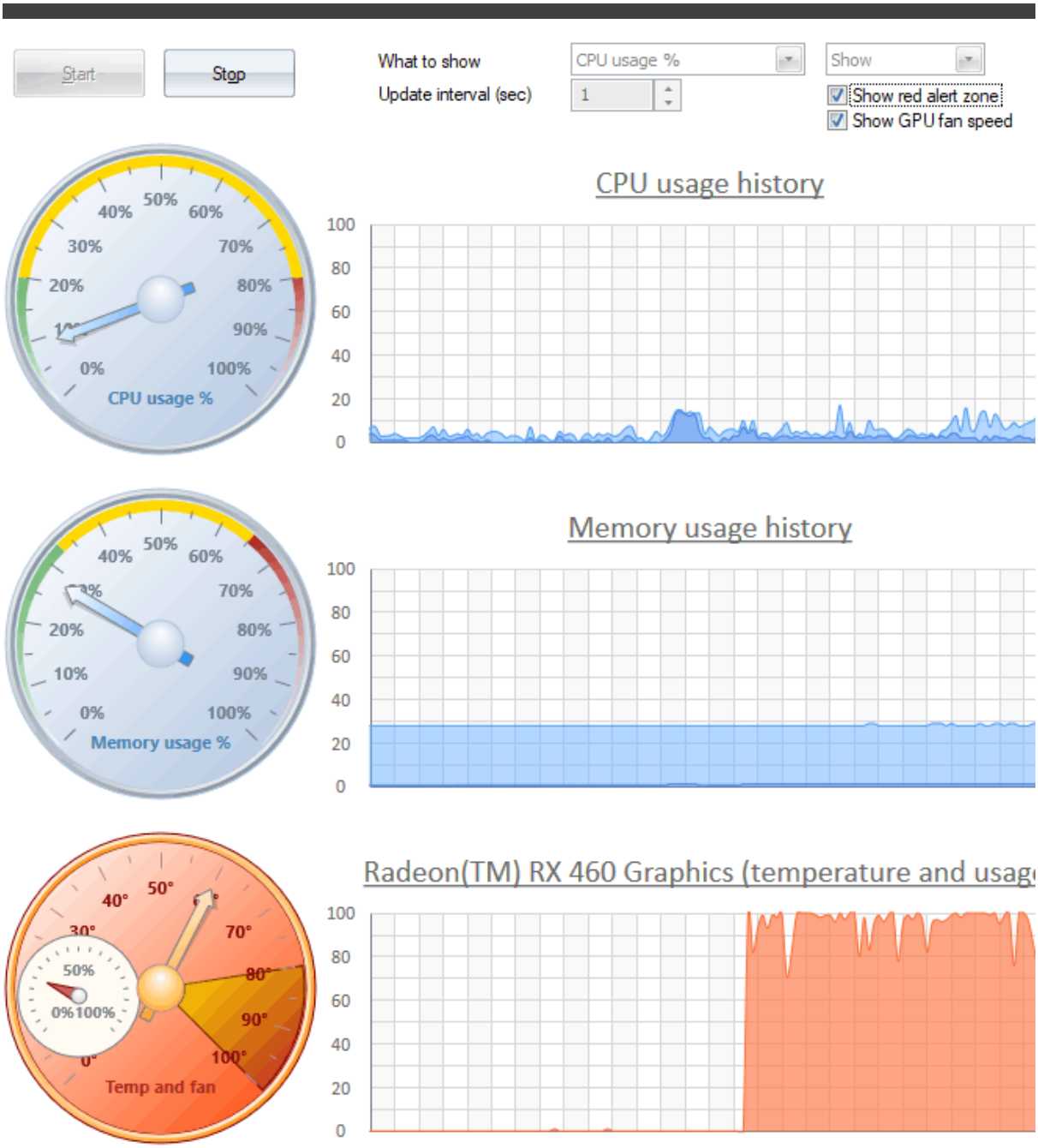
2.10 Menú Temas

Puedes seleccionar aquí uno de los temas que te han gustado o crear tu propio tema.

2.11 Menú Ayuda

En esta sección del menú, puede acceder a los artículos de ayuda sobre el uso del software, visitar la página principal del programa en la Web, verificar la disponibilidad de actualizaciones, enviar un informe de errores, registrar su copia de Windows Password Recovery, etc.

2.12 Monitor de Hardware



En esta pestaña, puede ver la carga actual de la CPU, la utilización de RAM, la temperatura y la carga de la GPU. De forma predeterminada, el intervalo de actualización se establece en 2 segundos. Tenga cuidado: recopilar estas estadísticas también lleva tiempo de CPU; por lo tanto, cuando se ejecutan ataques "pesados", como la fuerza bruta, se recomienda mantener el monitor del sistema deshabilitado.

Trabajando con el programa

3 Trabajando con el programa

3.1 Atacar hashes de Windows

Actualmente el programa puede descifrar hashes de Windows de varias maneras:

Ataque preliminar (desarrollado por Passcape Software) se basa en un método de ingeniería social y consiste en varios subataques. El ataque preliminar es muy rápido y, a menudo, se usa para adivinar contraseñas simples y cortas cuando no hay necesidad de lanzar un ataque totalmente escalable.

Ataque de Inteligencia Artificial - es un nuevo tipo de ataque desarrollado en nuestra empresa. Se basa en un método de ingeniería social y permite, sin recurrir a cálculos lentos y costosos, recuperar casi instantánea e indoloramente ciertas contraseñas.

Ataque de diccionario. Es el método de recuperación más eficiente, cuando el programa prueba cada palabra del diccionario (o diccionarios si hay varios diccionarios) se especifica hasta que encuentra la contraseña original o hasta que la lista de palabras se queda sin palabras. Este método es muy eficiente ya que muchas personas usan palabras o frases regulares para la contraseña. Además este tipo de recuperación se realiza bastante rápido en comparación con el ataque de fuerza bruta, por ejemplo. Diccionarios adicionales y listas de palabras pueden ser descargados en nuestro sitio o pueden ser ordenados en CDs.

Ataque de fuerza bruta prueba todas las combinaciones posibles del rango de caracteres especificado. Por ejemplo, para un rango de tres caracteres de caracteres latinos en minúsculas, verificará todas las combinaciones posibles, comenzando con 'aaa', 'aab', 'aac', y hasta 'zzz'. Este es el ataque más lento, por lo que es realmente ideal para contraseñas cortas.

Ataque de máscara es una variación del ataque de fuerza bruta, excepto que algunos caracteres para encontrar la contraseña permanecen sin cambios, y solo una parte de la contraseña puede cambiar. La sintaxis especial se utiliza para establecer una máscara o regla para encontrar una contraseña.

Ataque de palabra base (desarrollado por Passcape). A primera vista, este tipo de ataque recuerda al que acabamos de describir. Es igual de eficiente si una parte de la contraseña a recuperar es conocida por nosotros. Sin embargo, a diferencia del ataque anterior, aquí no tiene que configurar una máscara, solo proporcione una palabra básica. El programa se encargará del resto. La frase ataque se basa en la experiencia de la ingeniería social para generar un gran número de combinaciones posibles de la contraseña dada.

Ataque de diccionario combinado (desarrollado por Passcape) se utiliza para encontrar contraseñas compuestas. Por ejemplo, 'nothingtodo' o 'me doy por vencido'. Es muy similar al ataque de diccionario, excepto que en lugar de usar una sola palabra para la verificación de contraseñas, utiliza una combinación de palabras creadas combinando palabras de varios diccionarios. Puede crear sus propias reglas de generación de contraseñas.

Ataque de frase (desarrollado por Passcape) es muy eficiente contra contraseñas complejas. La idea es adivinar la contraseña correcta buscando a través de frases y combinaciones de uso frecuente. Puede descargar listas de palabras y diccionarios de frases de contraseña solo desde nuestro sitio.

Ataque arcoiris (desarrollado por Philippe Oechslin). Es una compensación de memoria de tiempo utilizada en la recuperación de la contraseña de texto sin formato de hashes. Este ataque es una herramienta bastante rápida y efectiva para auditar hashes de Windows.

Ataque de huellas dactilares. Desarrollado por Passcape, idea original de Atom. El ataque analiza la lista de palabras de entrada para generar las llamadas "huellas dactilares" utilizadas para recuperar la contraseña. El ataque es bastante efectivo para encontrar contraseñas difíciles para una gran lista de hashes o para hashes del historial de contraseñas.

Ataque de diccionario híbrido es como un simple ataque de diccionario, pero permite al usuario personalizar la mutación de palabras y establecer sus propias reglas de mutación de contraseña. La sintaxis de definición de regla es compatible con algún otro software de recuperación de contraseñas.

Recuperación en línea (desarrollado por Passcape Software) busca contraseñas en bases de datos de Internet. Se ocupa bastante bien de contraseñas simples y de uso frecuente. Su inconveniente es una velocidad de operación bastante baja y una poca idoneidad para manejar grandes listas de hash.

Ataque de tabla rainbow passcape (desarrollado por Passcape Software). Es la próxima generación de tablas precalculadas regulares. El ataque de tabla Passcape es el más adecuado para la recuperación de contraseñas complejas de longitud literalmente ilimitada.

Ataque por lotes (desarrollado en Passcape Software) crea una lista/lote de ataques para ser ejecutados uno por uno, de modo que pueda lanzar todos esos ataques con un solo clic del ratón en lugar de configurar cada uno de ellos individualmente.

Ataque de fuerza bruta de la GPU es completamente idéntico a la fuerza bruta simple, excepto que para adivinar contraseñas, utiliza una tarjeta de video en lugar de cpu. El dispositivo GPU en el que se ejecutará el ataque debe establecerse en *Opciones generales*.

Ataque de huellas dactilares de GPU funciona exactamente de la misma manera que lo hace el simple ataque de huellas dactilares, pero utiliza la potencia de la GPU.

Ataque de máscara de GPU. Este método de recuperación de contraseña es completamente idéntico al ataque de máscara normal, excepto que la adivinación de contraseña es procesada por una tarjeta gráfica de su PC, por lo que la velocidad de recuperación es mucho mayor..

Fuerza de diccionario de GPU. A menudo, al crear contraseñas, los usuarios agregan ciertos símbolos al principio, al final o incluso a la mitad de la palabra. Para recuperar contraseñas de este tipo específico, hemos ideado un ataque de diccionario basado en GPU.

Ataque de diccionario híbrido de GPU. Lo mismo que un simple ataque de diccionario híbrido pero mucho más rápido porque usa GPU.

3.2 Tabla de comparación de ataques

¿Qué ataque es el mejor? ¿Cómo eliges el ataque? Las respuestas a estas preguntas deben encontrarse en la tabla de comparación de ataques.

Ataque	Descripción	Tiempo requerido	Garantizado	Pros	Contras	Limitaciones
Preliminar	Un conjunto de miniataques	Un par de minutos	No	Gran herramienta de búsqueda rápida para	Prácticamente inútil para un análisis	Encuentra principalmente

	ligeros y rápidos para encontrar combinaciones simples, cortas o comunes			la recuperación rápida de contraseñas comunes, simples y cortas, combinaciones de teclado, secuencias repetitivas, etc. Bueno para encontrar contraseñas débiles rápidamente; no requiere ajustes adicionales	serio, al recuperar la mayoría de las contraseñas complejas	contraseñas simples
Inteligencia artificial	La forma más avanzada de recuperar contraseñas, basada en los métodos de ingeniería social.	Mín.: 2-3 minutos, Máx.: más de una hora	No	La mejor herramienta para encontrar contraseñas complejas, que otros métodos no pueden soportar. Funciona muy bien para contraseñas, palabras y combinaciones que el usuario almacenaba en el sistema en cualquier momento en el pasado.	Durante el análisis más eficiente, cuando todas las opciones se establecen al máximo rendimiento, el ataque lleva un tiempo considerable. No encuentra todas las contraseñas.	Eficiente solo cuando se ejecuta en el sistema original (donde se tomaron las contraseñas)
Fuerza bruta	Busca todas las combinaciones posibles dentro de un juego de caracteres especificado	Depende de las opciones	Sí	El único ataque (junto con el ataque de máscara) que está garantizado para recuperar una contraseña completamente desconocida. Bueno para cualquier contraseña corta y mediana	La búsqueda de contraseñas largas lleva un tiempo considerable. Es difícil adivinar el rango correcto de caracteres que se buscarán.	Puede tomar siglos buscar contraseñas largas. No encuentra contraseñas cuando utiliza un juego de caracteres incorrecto o la longitud de la contraseña supera la especificada
Diccionario	Encuentra la contraseña buscando palabras de diccionarios predefinidos (listas de palabras)	Casi al instante	No	Buena y rápida herramienta para recuperar contraseñas comunes	Requiere tener buenos diccionarios, no tiene en cuenta las peculiaridades del idioma y el caso de la letra	Encuentra solo contraseñas comunes
Diccionario con mutación inteligente	Igual que el ataque del diccionario,	Hasta 1000000 veces	No	Bueno para todo tipo de variaciones de contraseñas comunes	La mutación máxima (más efectiva) lleva	No encuentra contraseñas seguras (que

	excepto que aquí cada palabra del diccionario sufre todo tipo de mutaciones. Por ejemplo, agregar números, cambiar mayúsculas y minúsculas, deformar (desplazar) letras, etc.	más lento que un simple ataque de diccionario			un tiempo considerable	no son de diccionario), la mutación lleva un tiempo considerable
Máscara	Busca contraseñas por máscara especificada (regla de generación de contraseñas)	Depende de las opciones	Sí	Garantizado para recuperar la parte restante de una contraseña. Buena opción cuando se conoce alguna parte de la contraseña original.	Requiere tener la parte exacta conocida de la contraseña y su longitud y especificar el conjunto de caracteres correcto para ser buscado	La contraseña no se encontrará si se especifica un juego de caracteres incorrecto, una longitud de contraseña incorrecta o una parte conocida incorrecta de la contraseña de origen
Diccionario combinado	Comprueba contraseñas complejas (compuestas de dos o más palabras) pegando palabras de varios diccionarios	Depende de las opciones	No	El único ataque que encuentra contraseñas largas y complejas	Conjunto limitado de diccionarios específicos de campo, no tiene en cuenta las peculiaridades de las contraseñas no inglesas (terminaciones, sufijos, etc.) Con un diccionario de fuentes grande, el ataque puede llevar un tiempo considerable	Requiere saber de antemano que la contraseña que se busca consta de dos o más palabras; relativamente lento
Diccionario combinado con mutación inteligente	Igual que el ataque combinado, más mutaciones	Depende de las opciones	No	Igual que el ataque anterior	Igual que el ataque anterior. Requiere establecer reglas de mutación adicionales	Igual que el ataque anterior; las mutaciones

					para las contraseñas que se generarán	requieren un tiempo considerable
Palabra base	Aprovecha una palabra base conocida utilizada para componer la contraseña	Un par de segundos si la longitud de la palabra base no supera los 16 caracteres	No	Bueno para los casos en que conocía la contraseña original pero ha olvidado sus variaciones, por ejemplo, mayúsculas y minúsculas o números finales	La mutación para contraseñas largas (más de 16 caracteres) puede llevar algún tiempo	No siempre funciona
Frase	Igual que el ataque del diccionario, excepto que en lugar de una palabra esta comprueba una frase, expresión popular, extractos de canciones, libros, etc.	Desde varios minutos hasta varias horas	No	El único ataque contra las frases de contraseña.	Solo un pequeño porcentaje de usuarios usa frases de contraseña como contraseñas. La mutación de la frase es imperfecta; la mutación y el análisis toman un tiempo considerable. Número insuficiente de diccionarios pertinentes; en particular, con frases y expresiones no inglesas.	No tiene en cuenta las peculiaridades del idioma; elección limitada de mutaciones. Dificultad en la creación de diccionarios especializados.
Tablas arcoiris	Utiliza tablas precalculadas	Por lo general, varios minutos (o incluso segundos) para cada contraseña	Hasta el 100% si la contraseña encaja en el juego de caracteres y la longitud de la contraseña de	Actualmente uno de los mejores ataques para recuperar la mayoría de contraseñas por la relación tiempo/eficiencia	Requiere tablas. Las tablas de precalculamiento pueden ocupar mucho espacio en un disco duro. Es imposible recuperar contraseñas largas usando este ataque.	No se pueden recuperar todas las contraseñas simultáneamente; generar una nueva tabla lleva más tiempo que ejecutar un ataque de fuerza bruta. Capacidades de recuperación limitadas para contraseñas

			la(s) tabla(s)			largas y no inglesas
Huellas dactilares	Basado en huellas dactilares que se generaron a partir de la lista de palabras dada	Desde varias horas hasta varios días (depende del diccionario inicial)	No	Encuentra contraseñas complejas que eran imposibles de recuperar en otros ataques	El diccionario de entrada grande puede generar demasiadas huellas dactilares. El éxito depende del diccionario de entrada.	El ataque tarda demasiado tiempo en completarse al establecer una gran lista de palabras de entrada.
Diccionario híbrido	Es muy similar al ataque de diccionario simple, excepto que las reglas de mutación de contraseña son totalmente personalizables y deben ser establecidas por el usuario.	Depende de la lista de palabras de origen y del contador de reglas. Por lo general, hasta varios minutos para una pequeña lista de palabras.	No	Bueno para todo tipo de variaciones de contraseñas comunes	No se pueden recuperar contraseñas complejas.	No se pueden encontrar contraseñas seguras (que no son de diccionario)
Recuperación en línea	Busca contraseñas a través de Internet	Depende de las opciones establecidas y la velocidad de conexión a Internet. Por lo general, menos de 1 minuto para un	No	Herramienta alternativa bastante agradable para descubrir contraseñas simples y de uso frecuente.	Muy lento, procesa hashes posteriormente, se alimenta mucho de tráfico de Internet.	No encuentra la mayoría de las contraseñas seguras. Funciona solo cuando hay Internet disponible.

		solo hash.				
Tablas Rainbow Passcape	Utiliza tablas precalculadas especialmente formadas para adivinar contraseñas seguras y complicadas	Varios minutos (o incluso segundos) para cada contraseña, dependiendo de los parámetros de la tabla.	No	En realidad es un ataque muy bueno y avanzado para recuperar contraseñas fuertes y complicadas que no se pueden descifrar en otros ataques.	Un buen precálculo de tabla puede tomar mucho espacio en disco y tiempo. La tasa de éxito de la recuperación de contraseñas depende en gran medida de la lista de palabras de entrada.	No se pueden recuperar todas las contraseñas simultáneamente; generar una nueva tabla lleva más tiempo que ejecutar un ataque de fuerza bruta. No todas las listas de palabras iniciales se adaptan bien para crear tablas de Passcape.

3.3 Recuperación de contraseñas de hashes

Utilice esta sencilla instrucción para la recuperación de cualquier contraseña en los programas Passcape. Esta instrucción se ofrece en el formato de recomendación y está destinada principalmente a la recuperación de contraseñas cifradas con OWF; por ejemplo, desde hashes de Windows.

Al recuperar ciertos tipos de contraseñas, la pregunta principal es: ¿Cómo organizar el proceso de recuperación: con qué ataque debo comenzar para aumentar la probabilidad de que se complete con éxito?

Para elegir el tipo y la secuencia de los ataques, aconsejamos seguir este algoritmo, que es aplicable en la mayoría de los casos a todo tipo de contraseñas a recuperar:

Primero, habilite la opción de ataque preliminar, si está disponible. Ayudará a recuperar combinaciones simples y de uso frecuente.

En segundo lugar, seleccione una o varias contraseñas que necesita descifrar en primer lugar y ejecute la recuperación en línea para descubrir contraseñas simples y de uso frecuente.

En tercer lugar, si conoce alguno detalle de la contraseña que está buscando, es mejor probar primero el ataque de máscara o el ataque de palabra base. Específicamente, si conoce una parte de la contraseña, el uso de un ataque de máscara sería más efectivo. Si conoce el componente básico de la contraseña o, por ejemplo, conoce la contraseña pero no recuerda la secuencia de mayúsculas y caracteres en minúsculas, el ataque de palabras base haría mejor el trabajo.

Cuarto, si no hay información sobre la contraseña que está buscando, lo que ocurre con mayor frecuencia, guíese por la siguiente secuencia de pasos:

1. Lanzar un ataque de Inteligencia Artificial con opciones de mutación e indexación puestas a la luz.
2. Si no se encontró la contraseña, inténtelo una vez más con la opción de mutación establecida en nivel normal y la indexación establecida en profundo.
3. Ejecutar un ataque de tabla Rainbow si hay tablas
4. Ejecutar un ataque de tabla Rainbow Passcape.
5. Ejecute el ataque de diccionario con la opción de mutación deshabilitada.
6. Iniciar ataque de diccionario con la opción de mutación habilitada; la profundidad de la mutación depende de la cantidad de tiempo disponible y la velocidad de ataque. Al buscar contraseñas tecleadas en la distribución del teclado nacional, la profundidad de la mutación debe establecerse en fuerte.
7. Seleccione y descargue diccionarios en línea y repita los pasos 5 a 6.
8. Ejecute el ataque de diccionario híbrido.
9. Repita el ataque híbrido utilizando listas de palabras alternativas.
10. Inicie un ataque de frase de contraseña con la opción de mutación desactivada.
11. Inicie el ataque de frase de contraseña con la opción de mutación habilitada y configurada para la máxima productividad. Esto permitirá encontrar incluso contraseñas mecanografilladas en la distribución del teclado nacional.
12. Seleccione y descargue diccionarios de frases de contraseña en línea y repita los pasos 10 a 11.
13. Inicie un ataque de diccionario combinado con reglas de generación de frases definidas.
14. Seleccione y descargue diccionarios en línea para el ataque combinado y repita el paso 13.
15. Ejecute el ataque de huellas dactilares con el diccionario predeterminado.
16. Seleccione y descargue un nuevo diccionario en línea para el ataque de huellas dactilares, ajuste las opciones, configure el nuevo diccionario y repita el paso 15.
17. Seleccione un conjunto de caracteres y la longitud de la contraseña para el ataque de fuerza bruta, inicie el ataque.
18. Si es necesario, seleccione un conjunto de caracteres nuevo o complete el antiguo y repita el ataque de fuerza bruta; es decir, el paso 17.

Sobre la base de las recomendaciones dadas, es fácil crear sus propias reglas para ataque por lotes.

3.4 Preguntas más frecuentes sobre contraseñas de Windows

P. ¿Qué es la protección con contraseña?

R. Tal vez nadie discutiría que los sistemas operativos basados en Windows NT hoy en día son los más populares en todo el mundo. Eso los convierte en objetivos muy vulnerables para varios tipos de hackers, intrusos y usuarios deshonestos. La difusión de la red mundial no hace más que agravar la situación. Para garantizar la personalización de los datos almacenados del usuario o del sistema y protegerlos del acceso no autorizado por parte de terceros, se propuso utilizar la tecnología de protección con contraseña. Actualmente, la protección principal en los sistemas operativos Windows es la protección con contraseña. El acceso a datos privados en este caso solo es posible cuando el usuario conoce la contraseña original, que normalmente es una palabra o frase. Así es como se ve en la vida real: el programa o sistema, en un intento de acceder a datos privados, solicita al usuario las contraseñas de texto. Esa contraseña se compara con la contraseña original y, si los valores coinciden, el sistema permite el acceso a los datos privados; de lo contrario, deniega el acceso. La principal desventaja de la protección con contraseña es que el programa o sistema debe almacenar la contraseña original en algún lugar, con el fin de tener algo con lo que comparar el valor introducido.

P. ¿Cómo almacenan las contraseñas los sistemas operativos?

R. Pero no todo está tan mal; Windows NT se desarrolló de manera que no almacenaría el valor de texto original de la contraseña. "¿Cómo es eso?" Usted puede preguntar. - Muy fácil. Existen algoritmos especiales de envoltura de contraseñas criptográficas que funcionan de una sola manera. Es por eso que a veces se les conoce a OWF- funciones unidirecciones. A grandes rasgos, puede obtener el hash de una contraseña, pero no hay forma de obtener la contraseña de un hash. ¿Cómo funciona en Windows? Al crear una cuenta, el usuario ingresa la contraseña original, que, sin embargo, no se almacena como texto sin formato; en su lugar, se hashe con una función OWF. El hash de contraseña devuelto por la función se almacenará en el sistema. Más adelante, al intentar iniciar sesión, el sistema solicitará al usuario la contraseña; vuelve a hashear la contraseña y luego compara el hash generado con el original que está almacenado en el sistema. Si los dos valores coinciden, las contraseñas, naturalmente, también coinciden. Por lo tanto, la contraseña de texto original no se almacena en el sistema. Además, hay nuevos algoritmos que ni siquiera almacenan hash, y el número de tales algoritmos sigue creciendo. Un algoritmo de este tipo, por ejemplo, se utiliza para cifrar contraseñas en Internet Explorer 7-8. Puedes aprender más al respecto en nuestro artículo

P. ¿Cómo se cifran las contraseñas?

R. Para hashear contraseñas de usuario, Windows NT utiliza dos algoritmos: LM, que hemos heredado de las redes de Lan Manager, que se basa en una conversión DES simple, y NT, basado en la función hash MD4. LM, como el más débil y vulnerable, no es compatible de forma predeterminada con los últimos Windows Vista y Windows 7; sin embargo, aún puede habilitarlo. Además, hay una tendencia a eliminarlo o reemplazarlo por completo. Es importante saber que cuando la opción hash de LM está activada (está habilitada de forma predeterminada en Windows XP), todas las contraseñas de usuario se consideran bastante vulnerables. Descifrar la mayoría de estas contraseñas normalmente toma solo unos minutos. El hash NT está libre de las desventajas, comunes al hash LM. En consecuencia, es mucho más difícil elegir la contraseña correcta para un hash NT conocido que para un hash LM. Pero la tendencia actual de aumentar la potencia de cálculo de las computadoras modernas, especialmente cuando se usa GPU, posiblemente, hará que este estándar sea demasiado vulnerable a los posibles atacantes.

P. ¿Dónde se almacenan los hashes de contraseña?

R. Por lo tanto, hemos descubierto que las contraseñas de usuario en los sistemas Windows se convierten en valores especiales: hashes. Los hashes LM y NT tienen un tamaño fijo - 16 bytes - y se pueden almacenar en dos repositorios: SAM - para las cuentas normales y Active Directory - para las cuentas de dominio.

SAM: Las cuentas normales que contienen nombre de usuario, contraseña y otra información auxiliar se almacenan en el registro de Windows NT; precisamente, en el archivo SAM (Security Account Manager). Ese archivo se encuentra en el disco duro, en la carpeta %windows%\system32\config. % windows% representa la ruta de acceso a la carpeta de Windows. Por ejemplo, C: \Windows\System32\Config\SAM. El sistema tiene acceso prioritario al archivo SAM, por lo que el acceso al archivo se niega a cualquier persona, incluso a los administradores, mientras se carga el sistema; sin embargo, Windows Password Recovery omite esa restricción con facilidad. Además de eso, de gran interés para un potencial atacante sería la copia de seguridad del SAM. SAV y la copia comprimida de SAM en la carpeta %windows%\Repair. Otra forma de acceder al archivo SAM es iniciar un programa especial desde un disco de arranque y, a continuación, copiar el archivo. De todos modos, necesita un acceso físico a la computadora con hashes de contraseña. Las contraseñas de usuario o, para ser precisos, los hashes se cifran adicionalmente con la utilidad SYSKEY, que almacena sus datos de servicio en el archivo de registro SYSTEM. Por lo tanto, para extraer hashes de SAM, también necesitaría el archivo SYSTEM, que se encuentra en la misma carpeta que SAM.

Active Directory: Las cuentas de dominio se almacenan en la base de datos de Active Directory. Normalmente, la base de datos de Active Directory se encuentra en el archivo %Windows%

\ntds\NTDS. DIT; es el núcleo de Active Directory. La forma en que se cifran los hashes de usuario aquí es un poco diferente a la que se encuentra en SAM, pero la recuperación también requeriría el archivo SYSTEM. El acceso a la base de datos también está bajo el control total del sistema; sin embargo, a diferencia de SAM, la base de datos ntds.dit es resistente a las modificaciones del exterior.

P. Si todo es tan fácil, ¿por qué no simplemente denegar el acceso a SAM o Active Directory a todos los usuarios?

R. Así es como se hace. De forma predeterminada, solo el sistema tiene acceso a esos archivos. Sin embargo, estas restricciones pueden ser fácilmente anuladas. Por ejemplo, WPR puede importar hashes de los archivos actuales (bloqueados por el sistema) SAM y AD. Además de eso, el sistema almacena hashes en la memoria de la computadora para acelerar el acceso a ellos, por lo que volcar la memoria de la computadora también es una opción.

P. No lo entendí del todo; ¿Qué necesito copiar desde el ordenador para recuperar las contraseñas?

R. Si se trata de una computadora normal, copie estos archivos: SAM, SYSTEM (también se desean los archivos SECURITY y SOFTWARE). Si se trata de un servidor, necesitará los mismos archivos más uno ntds.dit.

P. ¿Cuánto tiempo se tarda en elegir la contraseña si el hash LM está disponible?

R. La mayor desventaja del algoritmo LM es que divide la contraseña en mitades de 7 caracteres. Si el usuario introduce una contraseña que tiene menos de 14 caracteres, el programa la sigue con ceros para obtener una cadena larga de 14 caracteres. Si la contraseña de usuario supera los 14 caracteres, el hash LM aparece igual que para una contraseña vacía. Cada una de las mitades de 7 caracteres se cifra de forma independiente; que facilita y acelera considerablemente el proceso de recuperación de contraseñas. Otra desventaja importante del hash LM se relaciona con el hecho de que durante el cifrado todos los caracteres alfabéticos de la contraseña se convierten en mayúsculas. En otras palabras, los hashes para PASSWORD, password, Password o pAsswOrd serán completamente idénticos. Al ejecutar un ataque de fuerza bruta contra cada mitad, las computadoras personales modernas pueden elegir un hash LM alfanumérico en unos pocos minutos (o incluso segundos, cuando se usa el ataque Rainbow). Hagamos un poco de cálculo. Para elegir una contraseña para cualquier combinación alfanumérica, necesitamos dividir la contraseña en dos partes largas de 7 caracteres y luego buscar 36 + 32 ^ 2 +. 36^7=80 603 140 212 combinaciones. Además, todos los hashes se buscarán simultáneamente. La velocidad de búsqueda en Windows Password Recovery en una computadora Intel Core i7 es de más de 100 millones de contraseñas por segundo. Redondeémoslo a 100. 80 603 140 212 / 100 000 000 = 806 segundos. Eso significa que tenemos la garantía de obtener la contraseña correcta en poco más de 10 minutos utilizando la fuerza bruta.

P. ¿Puedo ver las fuentes de cifrado?

R. Seguro. Revisemos un programa de cifrado de contraseñas que funciona para el algoritmo LM.

P. ¿Cuánto tiempo se requiere para adivinar la contraseña si se conoce su hash NT?

R. Con los hashes NT es un poco más complicado. El hash NT no tiene las desventajas que son comunes a LM. Por lo tanto, la probabilidad de la recuperación de la contraseña depende completamente de su longitud y complejidad, y cae como una bola de nieve. Incluso a pesar del hecho de que el algoritmo de conversión NT es más rápido. Echemos un vistazo a la siguiente tabla que muestra cómo el tiempo de búsqueda depende de la longitud y complejidad de la contraseña. Suponiendo que la velocidad de recuperación de fuerza bruta es de 10 mil millones de p/s (1 GPU superior en 2014).

Character set	Password length	Password sample	Time to crack
A .. Z	5	CRUEL	instantly

A .. Z	6	SECRET	instantly
A .. Z	7	MONSTER	instantly
A .. Z	8	COOLGIRL	22s
A .. Z	9	LETMEKNOW	~ 10m
A .. Z, 0 .. 9	5	COOL3	instantly
A .. Z, 0 .. 9	6	BANG13	instantly
A .. Z, 0 .. 9	7	POKER00	8s
A .. Z, 0 .. 9	8	LETMEBE4	~ 5m
A .. Z, 0 .. 9	9	COOLGIRL1	~ 3h
A .. Z, a .. z, 0 .. 9	5	P0k3r	instantly
A .. Z, a .. z, 0 .. 9	6	S3cr31	10s
A .. Z, a .. z, 0 .. 9	7	DidIt13	~ 6m
A .. Z, a .. z, 0 .. 9	8	GoAway99	~ 6h
A .. Z, a .. z, 0 .. 9	9	19Sample3	~ 16d

P. ¿Cuánto tiempo se necesita para adivinar la contraseña de NT por su hash LM?
R. Casi al instante.

P. ¿Por qué no puedo simplemente eliminar / eliminar el hash, es decir, establecer una contraseña en blanco?
R. ¿Quién dijo que no podías? Puedes. Por ejemplo, usando esta utilidad. Esta forma está bien para aquellos que necesitan recuperar el acceso a su cuenta (o la de otra persona, por ejemplo, cuando se habla de las autoridades respectivas) a cualquier costo. Además, con la utilidad mencionada anteriormente, puede hacer lo siguiente: recordar el hash, luego restablecer el hash, iniciar sesión en la cuenta con una contraseña vacía, realizar las manipulaciones necesarias con él y luego restaurar el hash recordado. Pero eso no es tan simple como parece. Incluso si ha restablecido la contraseña y ha obtenido acceso a la cuenta, aún no podrá recuperar la mayoría de las otras contraseñas. ¿Por qué? - Porque la contraseña de usuario participa en la creación de la clave maestra del usuario, que se utiliza en el cifrado DPAPI y EFS y otros subsistemas de Windows. En otras palabras, incluso si restablece la contraseña, no podrá recuperar ninguno de los siguientes datos: archivos cifrados con EFS, contraseñas de cuentas de Outlook, contraseñas de Internet Explorer 7-9, contraseñas de conexión de red (RAS, DSL, VPN, etc.), contraseñas de red a otras computadoras, claves de red inalámbricas, credenciales de MSN Messenger, contraseñas de Google Talk y Google Chrome, Skype, etc.

P. Entonces, para recuperar, por ejemplo, una contraseña de Internet Explorer, primero necesitaría obtener la contraseña de la cuenta, ¿verdad?
R. Exactamente.

P. ¿Hay puertas traseras?
R. Como en cualquier otro lugar. Por ejemplo, a veces la contraseña de la cuenta se puede almacenar en el formulario de texto sin formato en los secretos. Las contraseñas de muchas cuentas del sistema también se pueden recuperar con facilidad.

P. ¿Es eso para lo que se solicita el archivo de registro SECURITY al importar hashes desde el equipo local?
R. Sí. El propósito principal de la Seguridad es ser un almacenamiento para los llamados Secretos LSA. Estos secretos (pero no solos) pueden almacenar contraseñas de texto sin formato. El ataque de Inteligencia Artificial implementa un chequeo de posibles vulnerabilidades en el sistema y, como consecuencia, posibilidades de recuperar algunas contraseñas.

P. ¿Puedo colocar un hash existente en lugar de la contraseña al iniciar sesión en el sistema?
R. Hay programas que hacen eso. Así es como funcionan. Antes de arrancar el sistema, extraen hashes de contraseña de usuario de SAM. Luego, al cargar la cuenta, meten el hash conocido en lugar de la contraseña. Sin embargo, el resultado de tales manipulaciones es el mismo que el de simplemente restablecer la contraseña; es decir, no podrá recuperar la mayoría de las otras contraseñas.

P. ¿Qué puedo hacer si el archivo SAM está irremediablemente dañado? ¿Hay alguna manera de recuperar la contraseña original en este caso?
R. Sí, lo hay. Sin embargo, ya no tendrá acceso al sistema. Puede, por ejemplo, elegir la contraseña utilizando la clave maestra del usuario. Passcape Software tiene medios para hacerlo. Si el equipo pertenece a un dominio, los nombres y contraseñas hash de los últimos diez usuarios registrados en el equipo se almacenan en caché en su registro del sistema local, en la sección SECURITY\Policy\Secrets. Puedes aprovechar Reset Windows Password para volcar esos hashes (también se conocen como MSCACHE) y luego atacarlos utilizando Network Password Recovery Wizard.

P. Necesito recuperar el acceso a mi cuenta. ¿Dibujarías una imagen "para tontos": ¿cuál es la mejor manera de hacerlo y cómo lo hago?
R. Brevemente, hay dos formas de recuperar el acceso a una cuenta.
1. Restablecer la contraseña; por ejemplo, dejar la contraseña en blanco. Hay utilidades especiales para hacer eso; el más poderoso es Reset Windows Password. Su principio de funcionamiento es simple. Ejecute un programa de creación de disco de arranque y cree un CD/DVD o disco USB de arranque con Reset Windows Password. A continuación, encienda la computadora con la cuenta a la que necesita para recuperar el acceso y editar la configuración del BIOS para permitir que la computadora arranque desde CD / DVD / USB. Algunos equipos tienen esta opción habilitada de forma predeterminada. Ahora arranca desde el disco de arranque Reset Windows Password y siga las instrucciones del asistente para restablecer la contraseña de la cuenta. Sin embargo, restablecer la contraseña garantiza solo el acceso a la cuenta. Si también necesita recuperar el acceso a archivos cifrados con EFS o recuperar otras contraseñas (por ejemplo, las de red), este método no funcionará por usted.
2. Recupere la contraseña original. Por cierto, eso se puede hacer mediante ese mismo Reset Windows Password, ejecutando el ataque intelectual. Sin embargo, sus capacidades están limitadas solo por contraseñas débiles y vulnerables. Para restaurar la contraseña original, se recomienda usar Windows Password Recovery. En este programa, una vez importados los hashes, selecciona y lanza uno de los ataques propuestos. Si el ataque no tuvo éxito, puede alterar la configuración y ejecutar el ataque o reemplazarlo por otro. Sigue leyendo para descubrir cómo eligir el mejor ataque para tus hashes.

P. ¿Dónde puedo encontrar listas de palabras para ataques de diccionario?
R. No es necesario buscarlo. Puede descargar diccionarios desde Windows Password Recovery. Tenemos un gran conjunto de diccionarios en nuestro sitio web.

P. ¿Cómo hago que mi contraseña sea más segura?
R. Hay varias formas en que puede protegerse de la selección de sus contraseñas por parte de posibles atacantes:
- No utilice palabras del diccionario en ningún idioma, nombres, números, secuencias repetitivas de letras y números, abreviaturas, combinaciones de teclados, información personal, etc. Tales contraseñas se pueden adivinar extremadamente rápido y fácil.
- Aumentar la longitud de la contraseña. Sin embargo, hay un límite razonable para todo. Recuerda que la longitud no es lo principal (aunque no con contraseñas). Finalmente, crear una contraseña demasiado larga hará que la olvide con éxito después de una fiesta de fin de semana o vacaciones. Además de eso, la memoria de un humano promedio no puede contener más de 5-7 contraseñas a la vez. Aún así, hay contraseña de red, contraseña web, etc., que también deben recordarse.

- Extienda el juego de caracteres utilizado en la contrasena. Por ejemplo, reemplace los caracteres 'a' de la contraseña por '@'. El uso de caracteres nacionales también fortalece radicalmente las contraseñas. Usar caracteres poco comunes; por ejemplo, '~'. No use contraseñas difíciles de recordar que consistan en un conjunto aleatorio de caracteres, a menos que sea un genio.
- No utilice la misma contraseña para iniciar sesión en Windows, sitios web, servicios, etc.
- Si tiene problemas para recordar todas sus contraseñas, guárdelas en un archivo separado protegido con contraseña en un lugar seguro. Se implementa una buena protección con contraseña, por ejemplo, en un archivo Rar. No guarde ese archivo en el equipo local.
- Nunca ingrese su contraseña en la computadora de otra persona.
- No es una buena idea escribir sus contraseñas en notas adhesivas y pegarlas en el monitor.
- Piense en una protección adicional. Por ejemplo, si habilita la opción de contraseña de inicio SYSKEY, es probable que ni un solo atacante pueda romper sus contraseñas sin haber adivinado primero la contraseña original de SYSKEY.

3.5 Preguntas frecuentes sobre la recuperación de contraseñas de Windows

P. ¿Qué significan los signos de interrogación en las contraseñas LM?
R. Como ya sabrá, una contraseña LM consta de dos mitades. Si una contraseña LM tiene 7 signos de interrogación principales, eso significa que solo se encuentra la segunda mitad de la contraseña. Los signos de interrogación finales indican la primera mitad de la contraseña recuperada.

P. ¿Cuál es la diferencia entre las contraseñas LM y NT? He encontrado ambas contraseñas: MASTERGURU y MasterGuru. ¿Cuál de ellos es el correcto? ¿Cuál debo usar?
R. Para iniciar sesión en el sistema, debe utilizar la contraseña de NT.

P. Al forzar brutamente una contraseña LM, el programa avisa y trunca la contraseña a 7 caracteres. ¿Es eso un error?
R. No. Como sabes, una contraseña LM se divide en dos mitades de 7 caracteres. Por lo tanto, la longitud máxima de las contraseñas LM forzadas brutas es de 7 caracteres.

P. Conozco mi contraseña de NT, pero el programa no la encuentra por alguna razón. ¿Por qué?
R. La contraseña de NT distingue entre mayúsculas y minúsculas. Tal vez, ha establecido un rango de búsqueda incorrecto. Intente comprobar la contraseña manualmente en (Herramientas-Password Checker). Password Checker comprueba automáticamente todas las combinaciones posibles de caracteres en mayúsculas y minúsculas.

P. He recuperado la contraseña de administrador interno, pero al intentar iniciar sesión con ella, el sistema me dice que la contraseña es incorrecta. ¿Qué ocurre?
R. Lo más probable es que haya recuperado la contraseña del administrador local, mientras que su equipo pertenece a un dominio. Las contraseñas de dominio se almacenan en Active Directory, incluida la contraseña del administrador del dominio. Intente iniciar sesión en el sistema en modo seguro.

P. Durante un ataque de diccionario, he recuperado una contraseña que no estaba en el diccionario. ¿Cómo sucedió eso?
R. Lo más probable es que haya establecido el nivel máximo de mutación, cuando el programa también verifica las palabras del diccionario escribidas en un conjunto de caracteres nacionales no ingleses, dependiendo de la distribución del teclado. Por ejemplo, la palabra 'secreto' mecanografillada con el diseno cirilico producira la palabra 'ыускуе'. Ademas de intercambiar distribuciones de teclado, las

mutaciones activas pueden mutilar las palabras hasta el punto en que son difíciles de reconocer. La mutación se utiliza en los ataques preliminares, intelectuales, de diccionario y combinados, así como en los ataques de palabras y frases clave.

P. En un ataque por lotes, ¿puedo establecer el mismo tipo de ataque pero con diferentes configuraciones?
R. Sí, puedes hacerlo.

P. Tengo una pregunta sobre los diccionarios en línea. He notado que están extremadamente comprimidos, al nivel mayor que los que producen los archivadores. ¿Qué es el formato PCD?
R. Ese es un formato de almacenamiento de diccionario propietario desarrollado en Passcape, que utiliza algoritmos adicionales de optimización y cifrado. De hecho, algunos diccionarios se pueden comprimir más que con un archivador normal. Por ejemplo, el diccionario Australian.pcd en el formato original ocupa 926 KB de espacio, mientras que en el formato comprimido es de solo 53 KB.

P. Elegí ejecutar un ataque de diccionario y establecer el nivel de mutación medio. Cuando lancé el ataque, me sorprendió desagradablemente la baja velocidad, solo unos pocos miles de contraseñas por segundo. ¿Por qué es tan lento?
R. El programa muestra la velocidad de ataque sin mutaciones. Por ejemplo, si se han procesado 1000 palabras en un segundo, muestra 1000 p/s, aunque el módulo de mutación podría haber generado 1000 palabras adicionales por cada palabra durante ese tiempo. Por lo tanto, la velocidad de búsqueda real es cientos o incluso miles de veces mayor que lo que se ve en la pantalla.

P. ¿Puedo usar los diccionarios normales en un ataque de diccionario combinado?
R. Sí, se puede.

P. Sé que la contraseña comienza con "azul". ¿Qué ataque sería el mejor para usar?
R. Puedes probar el ataque de diccionario. Por ejemplo, la máscara blue%c%c%c%c%c%c buscaría el rango desde blueaaaaaa hasta bluezzzzzz.
También puede intentar ejecutar un ataque de diccionario combinado. Para hacer eso, abra el bloc de notas, luego escriba 'azul' y guarde el archivo como, por ejemplo, 1.dic. Luego abra las opciones de ataque combinadas y establezca 1.dic como el diccionario principal y cualquier otro, como el diccionario secundario. De esta manera el programa buscaría palabras disílabas como bluepig, blueberry, bluegirl, etc. Si agrega el tercer diccionario, el programa buscará a través de la combinación de los tres componentes. Por ejemplo, bluecoolgirl, blueblackhash, bluebadboy.

P. El ataque de Inteligencia Artificial va demasiado lento. ¿Qué ocurre?
R. Es porque la caché de contraseñas está llena. En este caso, debe intentar vaciarlo. O porque ha establecido una mutación demasiado profunda, y el programa ha encontrado bastantes palabras "sospechosas"; es decir, las palabras que se consideran como las contraseñas potenciales.

P. Estoy lanzando la fuerza bruta, pero el programa muestra que no tiene nada que ver. ¿Por qué?
R. Antes de lanzar la fuerza bruta, primero debe seleccionar los hashes. Puede hacerlo a través del menú Editar - Seleccionar.

P. ¿Qué son las tablas Rainbow? ¿Y cómo se pueden usar para recuperar contraseñas?
R. Para lanzar un ataque arcoiris, en las opciones de ataque debe cargar el *. RT o *. RTI que contienen tablas Rainbow. El tipo de las tablas debe coincidir con el tipo de hashes seleccionados para el ataque. Por lo tanto, los nombres de los archivos con las tablas deben comenzar correspondientemente: "lm_*.rt" para hashes LM, "ntlm_*.rt" para hashes NT. Puede obtener información adicional y descargar tablas Rainbow en http://project-rainbowcrack.com.

3.6 Preguntas frecuentes sobre GPU

P: ¿Cuáles son los requisitos del sistema para el programa?
R: Actualmente, el programa admite tarjetas de video NVidia con capacidad de cómputo CUDA 3.0 o superior, AMD Radeon al menos serie 7xxx e Intel HD Graphics serie 4xxx o superior. La lista completa de dispositivos compatibles con CUDA se puede encontrar en https://developer.nvidia.com/cuda-gpus. Las tarjetas AMD Radeon compatibles se muestran aquí: https://en.wikipedia.org/wiki/Comparison_of_AMD_graphics_processing_units. También debe tener instalados los controladores de video más recientes.

P: ¿Qué versiones de Windows admite el programa?
R: La aceleración de GPU se admite a partir de Windows XP (GPU NVidia) y Windows Vista (GPU AMD) en sistemas de 32 bits y 64 bits.

P: ¿Cómo sé qué arquitectura admite mi tarjeta de vídeo?
R: Para dispositivos NVidia:
Inicie el programa, abra el menú '*Opciones - Opciones generales*', seleccione la pestaña '*Configuración de GPU*', seleccione la plataforma '*NVidia CUDA*' y elija su tarjeta de video aquí. El campo '*Capacidad de cómputo*' en la sección de descripción debe mostrar su arquitectura de GPU.
Para dispositivos AMD:
Inicie el programa, abra el menú '*Opciones - Opciones generales*', seleccione la pestaña '*Configuración de GPU*', seleccione la plataforma '*AMD OpenCL*' y elija su tarjeta de video aquí. Los campos 'CL_DEVICE_VERSION' y 'CL_DEVICE_OPENCL_C_VERSION' deben mostrar la arquitectura de la GPU compatible.

P: ¿Dónde puedo obtener los controladores de vídeo más recientes?
R: Puede descargar los controladores más recientes en los sitios web de NVidia (https://www.nvidia.ru/drivers) y AMD (https://support.amd.com/us/gpudownload/Pages/index.aspx).

P: ¿Dónde puedo leer más información sobre CUDA?
R: El sitio de Wikipedia es un buen punto de partida para empezar.

P: ¿Dónde puedo leer más información sobre las tarjetas AMD Radeon?
R: https://en.wikipedia.org/wiki/Comparison_of_AMD_graphics_processing_units

P: ¿Dónde puedo leer más información sobre los gráficos Intel?
R: https://en.wikipedia.org/wiki/Intel_HD_and_Iris_Graphics

P: Después de lanzar un ataque basado en GPU, mi computadora se congela o se bloquea en BSOD. ¿Cuál es el problema?
R: El problema puede deberse a las siguientes razones:

- Su tarjeta de video había sido overclockeada y estaba funcionando mal a alta carga. Si ese es el caso, lleve las frecuencias de la memoria / núcleos de video a sus valores predeterminados.
- Enfriamiento insuficiente o ineficaz de su tarjeta. Cuando se lanza un ataque basado en GPU, el programa utiliza la mayor parte de la potencia de la GPU, y la temperatura de la GPU se eleva a un nivel crítico. Asegúrese de que su tarjeta de video esté bien refrigerada, que la ranura de la GPU y la unidad del sistema estén libres de suciedad y polvo. Un uso imprudente de algunas configuraciones de video puede tener un impacto negativo en la temperatura de la tarjeta de video y su estabilidad en condiciones de alta carga. Por ejemplo, algunas aplicaciones reducen la velocidad del ventilador para minimizar el ruido, lo que resulta en una reducción del ruido, pero también aumenta la temperatura central.

- Problema de suministro de energía. Su tarjeta puede consumir mucha energía a plena carga, y es posible que la unidad de fuente de alimentación no pueda manejar una demanda tan alta de energía. Si la tarjeta de vídeo tiene conectores de alimentación adicionales de 6 u 8 pines, asegúrese de que todos estén conectados correctamente.

P: Cuando lanzo un ataque de GPU, mi computadora se ralentiza mucho. ¿Cómo puedo solucionarlo?
R: De forma predeterminada, la aplicación está configurada para usar tarjetas de video de rendimiento medio. Eso suele ser 256 hilos por bloque, 256 bloques y 1000 contraseñas por hilo. Para las tarjetas de video más antiguas, tal configuración es demasiado y puede causar una desaceleración. Considere reducir el valor de "*Contraseñas por subproceso*" a 100 o incluso menos.

P: ¿Cuál es la mejor manera de encontrar valores óptimos de "*Bloques de subprocesos*" y "*Contraseñas por subproceso*" en la configuración de ataque de GPU?
R: Puedes hacerlo empíricamente o haciendo algunas matemáticas. Por ejemplo, si los valores son 100 y 100, y la velocidad promedio de ataque es de 1 mil millones de contraseñas por segundo, puede calcular que el kernel de la GPU se llama aproximadamente 390 veces por segundo (el número de contraseñas calculadas cada vez suele ser 256 * ThreadBlocks * PasswordsPerThread). Naturalmente, cuantas menos llamadas, menos sobrecarga y mayor será la velocidad de ataque. Por otro lado, debe llamar al programa GPU al menos un par de veces por segundo. Así que usa una calculadora y ajusta los parámetros. También puede ajustarlos usando una regla general, es decir, aumentando sus valores hasta que la velocidad de ataque deje de subir y la computadora se ralentí. Si tiene un monitor gpu instalado en su sistema, debe indicar una carga de al menos 98-99 por ciento. Además, es importante saber algunas otras cosas también. Primero, no establezca los valores de resumen de esos parámetros demasiado altos. De lo contrario, su sistema puede funcionar mal o congelarse. En segundo lugar, es mejor que no establezca el valor de "*Contraseñas por hilo*" en menos de 100, ya que afectará negativamente la velocidad de ataque, independientemente del tipo de tarjeta de video que se utilice.

P: ¿El bus PCI-Express tiene algún impacto en el rendimiento?
R: En realidad, este impacto es insignificante. Por lo general, está enmascarado por otros factores. Por lo tanto, la generación de su bus PCI-Express y su rendimiento no importan mucho.

P: ¿Importa la cantidad de memoria de vídeo?
R: No, no es así. Sin embargo, en la mayoría de los casos, su GPU debe tener al menos 256 Mb de memoria de video.

P: Un ataque basado en GPU ralentiza mi PC, por lo que apenas puedo usarlo. ¿Cómo puedo solucionarlo?
R: Hay dos formas de solucionarlo: temporal y permanente. Como solución temporal al problema, vaya a la configuración de ataque e intente reducir el número de bloques de GPU utilizados o el número de contraseñas comprobadas por subproceso de GPU. Como solución permanente, instale un segundo dispositivo de video, siempre que tenga una segunda ranura en su placa base y que su unidad de fuente de alimentación pueda manejar la carga adicional. Por ejemplo, puede usar alguna tarjeta barata como la principal (para mostrar información en su monitor), y una segunda, más potente, para contraseñas de fuerza bruta.

P: Tengo más que tarjetas de video en mi computadora. ¿Puedo usarlos todos para forzar brutamente?
R: Sí. Puedes usar todos o algunos de ellos. Simplemente abra la configuración general y especifique los dispositivos GPU que utilizará el programa.

P: ¿Cuál es el número máximo de dispositivos GPU compatibles con su programa?
R: Depende de su hardware. Aunque el programa admite hasta 255 dispositivos, por lo general, se pueden instalar hasta 8 dispositivos en una placa base de 4 ranuras PCI-E (4 tarjetas de doble GPU).

P: ¿Puedo forzar brutamente contraseñas en dispositivos cuyo rendimiento varía mucho?
R: Sí, puedes.

P: El programa no puede detectar mi tarjeta de vídeo. ¿Qué puedo hacer?
R: Actualiza los controladores de vídeo. Si esto no ayudó, intente extender su escritorio a todos los dispositivos (si tiene más de un dispositivo). Vuelva a conectar el dispositivo a otra ranura PCI-Express.

P: La aplicación no puede usar todas mis GPU.
R: Tendrá que desactivar SLI para poder usar todos los dispositivos.

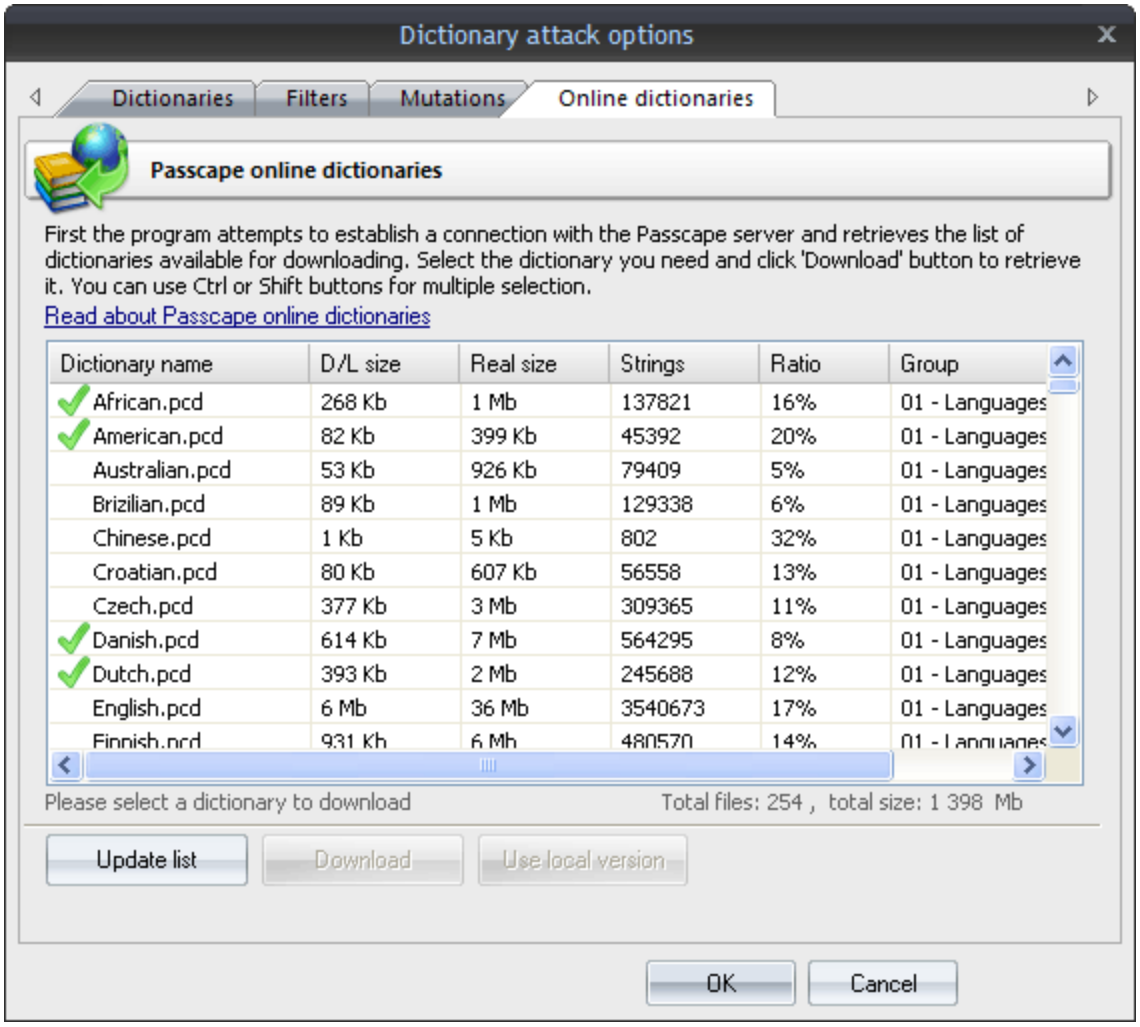
P: ¿Puedo usar dispositivos NVidia, AMD e Intel simultáneamente?
R: Sí, puede usar dispositivos NVidia, AMD e Intel simultáneamente.

P: ¿Cómo puedo comprobar la utilización de mi GPU?
R: Abra la pestaña 'Monitor de hardware'. En el cuadro desplegable 'Qué mostrar', elija el dispositivo que necesita y seleccione 'Mostrar' para mostrarlo. A continuación, puede hacer clic en los botones 'Inicio' o 'Detener' para administrar el monitoreo de hardware. El monitor de GPU muestra la carga del dispositivo (utilización), la temperatura y la velocidad del ventilador.

P: Mi GPU NVidia está ausente en el monitor de hardware.
R: Debe instalar/reinstalar la biblioteca NVAPI. Descargue la biblioteca en https://developer.nvidia.com/nvapi

P: Mi GPU AMD muestra ceros en el monitor de hardware.
R: Instale o reinstale los controladores AMD o el componente ADL más recientes. Asegúrate de que tu dispositivo AMD esté activo (conectado al monitor activo). Los dispositivos no activos no son procesados correctamente por ADL debido a un error en los controladores AMD.

3.7 Diccionarios en línea



El cuadro de diálogo de selección de diccionario en línea es extremadamente simple. Cuando se abre, el programa intenta establecer una conexión con el servidor Passcape y luego recupera y muestra la lista de diccionarios disponibles para descargar.

Seleccione el diccionario que necesita y luego haga clic en el botón '*Descargar*' para recuperarlo y usarlo en el programa.

Algunos de los diccionarios son grandes. Por ejemplo, el tamaño de 'music_songs.pcd' es más de 59 MB en el formato comprimido. Naturalmente, recuperar una cantidad tan grande de datos puede llevar algún tiempo, lo que depende del tamaño del archivo, el ancho de banda de su conexión a Internet y la carga de la red.

Todos los diccionarios en línea (y algunos adicionales) pueden ser ordenados en CD. El tamaño total de todos los diccionarios es de más de 7,5 GB. También puede compartir su propio diccionario con nosotros enviándonos un correo electrónico al diccionario o al enlace donde se puede descargar.

La lista de palabras se utiliza en ataques de diccionario comunes, diccionario combinado y ataques de frase de contraseña.

Licencia y registro

4 Licencia y registro

4.1 Acuerdo de licencia

==========
CONTRATO DE LICENCIA DE SOFTWARE
==========

IMPORTANTE-LEA DETENIDAMENTE: Este es el Acuerdo de licencia de usuario final (el "Acuerdo") es un acuerdo legal entre usted, el usuario final y Passcape Software, el fabricante y el propietario de los derechos de autor, para el uso del producto de software "Windows Password Recovery" ("PROGRAMA").

Todos los derechos de autor del PROGRAMA son propiedad exclusiva de Passcape Software.

El PROGRAMA y cualquier documentación incluida en el paquete de distribución están protegidos por las leyes nacionales de derechos de autor y los tratados internacionales. Cualquier uso no autorizado del PROGRAMA dará lugar a la terminación inmediata y automática de esta licencia y puede dar lugar a un proceso penal y/o civil.

Se le concede una licencia no exclusiva para utilizar el PROGRAMA como se establece en este documento.

Puede utilizar la versión de prueba del PROGRAMA todo el tiempo que desee, pero para acceder a todas las funciones debe comprar la versión completamente funcional. Tras el pago, le proporcionamos el código de registro.

Una vez registrado, se concede al usuario una licencia no exclusiva para utilizar el PROGRAMA en un ordenador a la vez (por cada licencia de usuario único adquirida).

Con la licencia personal, puede utilizar el PROGRAMA como se establece en este Acuerdo para fines no comerciales en entornos no comerciales y no comerciales. Para utilizar el PROGRAMA en un entorno corporativo, gubernamental o empresarial, debe comprar una licencia comercial. Con la licencia comercial, puede ejecutar el PROGRAMA en varios equipos de su organización, sin importar dónde se encuentren.

El PROGRAMA registrado no puede ser alquilado o arrendado, pero puede ser transferido permanentemente junto con la documentación adjunta, si la persona que lo recibe acepta los términos de esta licencia. Si el software es una actualización, la transferencia debe incluir la actualización y todas las versiones anteriores.

No puede crear ninguna copia del PROGRAMA. Puede hacer una (1) copia del PROGRAMA para fines de copia de seguridad y archivo, siempre que, sin embargo, el original y cada copia se mantengan en su posesión o control, y que su uso del PROGRAMA no exceda lo permitido en este Acuerdo.

La versión no registrada (de prueba) del PROGRAMA puede distribuirse libremente, siempre que el paquete de distribución no se modifique. Ninguna persona o empresa puede cobrar una tarifa por la distribución del PROGRAMA sin el permiso por escrito del titular de los derechos de autor.

Usted acepta no modificar, descompilar, desensamblar, realizar ingeniería inversa del PROGRAMA, a menos que dicha actividad esté expresamente permitida por la ley aplicable.

Passcape Software no garantiza que el software sea apto para ningún propósito en particular. Passcape Software renuncia a todas las demás garantías con respecto al PROGRAMA, ya sean expresas o implícitas. Algunas jurisdicciones no permiten la exclusión de garantías implícitas o limitaciones sobre cómo puede durar una garantía implícita, por lo que las limitaciones o exclusiones anteriores pueden no aplicarse a usted.

El programa que se le otorga la licencia es absolutamente legal y puede usarlo siempre que sea el propietario legal de todos los archivos o datos que vaya a recuperar mediante el uso de nuestro PROGRAMA o tenga permiso del propietario legítimo para realizar estos actos. Cualquier uso ilegal de nuestro PROGRAMA será de su exclusiva responsabilidad. En consecuencia, usted afirma que tiene el derecho legal de acceder a todos los datos, información y archivos que han sido ocultados.

Además, usted atestigua que los datos, contraseñas y / o archivos recuperados no se utilizarán para ningún propósito ilegal. Tenga en cuenta que la recuperación de contraseñas y el descifrado de datos subsecúcriplos de archivos no autorizados u obtenidos ilegalmente pueden constituir un robo u otra acción ilícita y pueden resultar en su enjuiciamiento civil y (o) penal.

Todos los derechos no otorgados expresamente aquí están reservados por Passcape Software.

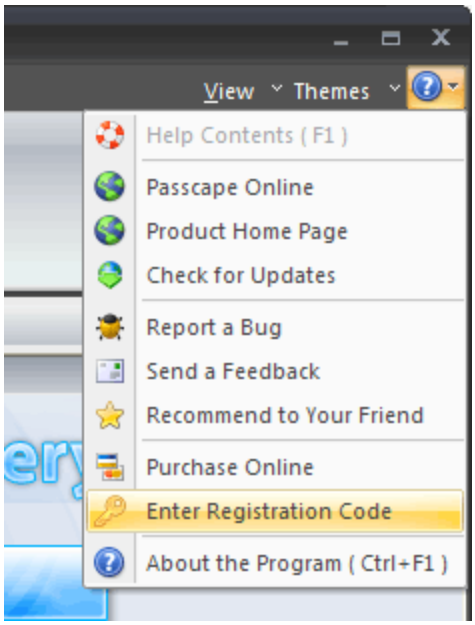
4.2 Registro

El software está disponible en tres ediciones: Light, Standard y Advanced. La lista detallada de características están mostradas aquí. Puede solicitar la versión completamente registrada de Windows Password Recovery a un costo de $ 65 para Light Edition (uso personal), $ 345 para Standard Edition (uso personal) o $ 895 para Advanced Edition (licencia comercial).

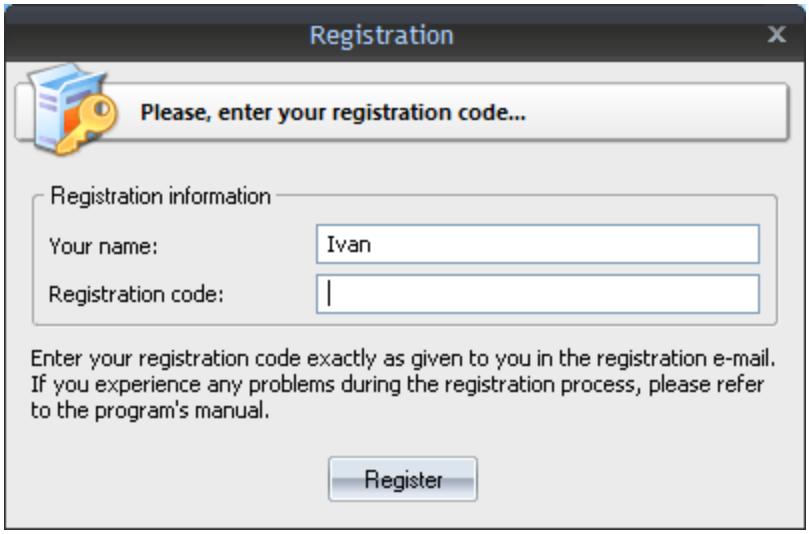
Las instrucciones detalladas para todo tipo de pedidos están disponibles en línea en la Página de pedido de WPR. Los pedidos en línea se cumplen en solo unos minutos las 24 horas del día, los 7 días de la semana. Si compra nuestros productos en línea, recibirá un mensaje de correo electrónico generado automáticamente con los detalles de registro en varios minutos (si el pedido pasa el sistema de verificación de fraude). Sin embargo, algunos pedidos pueden marcarse para el pago manual o como "sospechosos". Esto puede aumentar el tiempo de pedido hasta varias horas.

Importante: al completar el formulario de pedido, verifique que su dirección de correo electrónico sea correcta. Si no es así, no podremos enviarle el código de registro.

Para completar el registro:



- Abra el mensaje de registro y copie el código de registro en el portapapeles de Windows.
- Ejecute el programa, seleccione **Ayuda - Introduzca el código de registro.**
- Escriba su nombre de registro y pegue el código aquí.
- Click en el botón **Registrar** para confirmar.



4.3 Limitación de la versión no registrada

Una versión no registrada de Windows Password Recovery muestra solo los primeros 3 caracteres de las contraseñas recuperadas y tiene algunas limitaciones funcionales. La versión registrada del programa elimina todas las restricciones. Por favor vaya a esta página para ver las restricciones de una determinada edición del programa.

4.4 Ediciones del programa

Windows Password Recovery viene en tres ediciones: Light, Standard y Advanced. La lista detallada de características y la tabla de compatibilidad se muestran a continuación.

CARACTERÍSTICA	Light	Standard	Advanced
Compatibilidad con estaciones de trabajo Windows 2000/XP/Vista/7/8/10	+	+	+
Compatibilidad con servidores Windows 2000/2003/2008/2012/2016/2019	+	+	+
Compatibilidad con Windows de 64 bits	+	+	+
Compatibilidad con versiones de Windows fuera de EE. UU.	+	+	+
Compatibilidad con contraseñas internacionales	+	+	+
Recuperación multiproceso	+	+	+
Compatibilidad con temas de interfaz	+	+	+
Cargar hashes desde el equipo local	+	+	+
Cargar hashes desde el equipo remoto	-	+	+
Volcar hashes regulares	+	+	+
Volcar hashes del historial de contraseñas	+	+	+
Buscar contraseñas de texto sin formato	+	+	+
Cargar hashes desde SAM	+	+	+
Cargar hashes de Active Directory	+	+	+
Cargar hashes almacenados en caché de dominio	+	+	+
Recuperación de contraseña para credenciales almacenadas en caché de dominio	-	+	+
Importar hashes de otros programas	+	+	+
Cargar hashes desde carpetas de restauración del sistema	+	+	+
Exportar hashes al archivo PWDUMP	+	+	+
Ataques comunes	+	+	+
Ataques avanzados	+	+	+
Ataques inteligentes	+	+	+
Ataques basados en GPU	+	+	+
Soporte para múltiples dispositivos GPU	-	+	+
Ataque por lotes	-	-	+
Ver caché de contraseñas de IA	-	-	+
Mutación inteligente de contraseña	+	+	+
Diccionarios en línea	+	+	+
Soporte para SYSKEY	+	+	+
Soporte de descifrado de contraseña de inicio SYSKEY	+	+	+
Soporte de descifrado de disquete SYSKEY	+	+	+
Herramienta generadora de listas de palabras personalizada en ataque de diccionario	-	-	+

CARACTERÍSTICA	Light	Standard	Advanced
Generar diccionarios por máscara	-	-	+
Generar diccionarios por palabra base dada	-	-	+
Generador de diccionarios combinados	-	-	+
Generador de diccionarios de frases de contraseña	-	-	+
Generador de diccionarios de huellas dactilares	-	-	+
Crear listas de palabras basadas en un ataque de diccionario híbrido	-	-	+
Compatibilidad con tablas arco iris híbridas e indexadas (*.rti)	+	+	+
Puede restringir el acceso al programa	+	+	+
Medición de la fuerza de la contraseña	+	+	+
Comprobador de hash	+	+	+
Generador de hash aleatorio	+	+	+
Generador de hashes múltiples	-	+	+
Herramienta de generación de tablas arcoiris	+	+	+
Herramienta de generación de tablas arcoiris Passcape	+	+	+
Diccionario a generador de hash	-	+	+
Archivos de registro del sistema de copia de seguridad	-	+	+
Copia de seguridad de la base de datos de Active Directory	-	-	+
Herramienta de visor de contraseñas en asterisco	+	+	+
Eliminador de contraseñas sin conexión para cuentas de usuario normales	-	-	+
Eliminador de contraseñas sin conexión para cuentas en caché de dominio	-	-	+
Eliminador de contraseñas sin conexión para cuentas de dominio	-	-	+
Volcador de secretos de LSA	+	+	+
Explorador de credenciales almacenadas en caché de dominio	-	+	+
Explorador de SAM	-	+	+
Explorador de Active Directory	-	-	+
Explorador del Almacén de Windows	-	-	+
Herramientas de listas de palabras: crear una lista de palabras indexando archivos	-	+	+
Herramientas de listas de palabras: combinar listas de palabras	+	+	+
Herramientas de listas de palabras: estadísticas de listas de palabras	+	+	+
Herramientas de lista de palabras: ordenar	+	+	+
Herramientas de lista de palabras: conversión/compresión	+	+	+
Herramientas de lista de palabras: comparación de listas de palabras	+	+	+
Herramientas de lista de palabras: operaciones adicionales	+	+	+
Herramientas de lista de palabras: indexación de palabras/contraseñas de áreas sensibles del disco duro	-	-	+
Herramientas de lista de palabras: Extractor de enlaces HTML	+	+	+
DPAPI: recuperación de blobs DPAPI sin conexión	*	*	+
DPAPI: Análisis de blobs DPAPI	+	+	+
DPAPI: búsqueda de blobs DPAPI	+	+	+
DPAPI: Análisis de clave maestra	*	*	+
DPAPI: volcar hashes del historial de contraseñas	-	-	+

CARACTERÍSTICA	Light	Standard	Advanced
DPAPI: analizar el historial de contraseñas	*	*	+
Windows Hello: recuperar credenciales de usuario	-	+	+
Windows Hello: descifrar bases de datos biométricas	-	+	+
Windows Hello: PIN bruteforcer	-	+	+
Monitor de hardware	+	+	+
Monitor de estado de la GPU	+	+	+
Informes de contraseñas	-	+	+
Usar IA al recuperar la contraseña en el modo Asistente	+	+	+
Ejecutar en modo oculto	+	+	+
Máx. cuentas de usuario a la vez	500	5000	ilimitado
Garantía de devolución de dinero de 14 días	+	+	+
Licencia	personal	personal	negocio
Precio	$65	$345	$895

* - uses some restrictions

Soporte técnico

5 Soporte técnico

5.1 Reporte de problemas

Si tiene algún problema, póngase en contacto con nosotros en support@passcape.com. Por favor, infórmenos sobre lo siguiente:

- Nombre completo y versión del programa
- Versión de Windows que incluye Service Pack, OEM e información de idioma, etc.
- Información de registro, si la hubiera.
- Descripción detallada del problema, ya sea un error constante o espontáneo
- Si está informando de un error crítico, adjunte el archivo Crash.log que se guardó durante una sesión de excepción no controlada.

5.2 Sugerencia de características

Si tiene alguna pregunta, comentario o sugerencia sobre el programa o desea obtener más información, envíenos un correo electrónico a info@passcape.com. Por favor, no olvide mencionar el nombre y la versión del programa. También asegúrese de tener instalada la última versión del programa. Sus comentarios nos ayudan a mejorar nuestros productos y trabajar de manera más efectiva.

5.3 Contactos

Por favor, no dude en enviar sus preguntas sobre nuestros productos al correo electrónico support@passcape.com.
Recibirá respuesta durante uno o dos días. Tenga en cuenta que los usuarios registrados tienen prioridad en el soporte técnico.

Si experimenta algún problema durante el proceso de registro, envíe un correo a sales@passcape.com

Estaremos encantados de ayudarle con el registro.

¡Por favor, escriba en inglés!

Puede encontrar otras utilidades de recuperación de contraseña en https://www.passcape.com