Windows Password Recovery

Manuel d'utilisation

Passcape Software

Traduit le 07/06/2018

Introduction

1 Introduction

1.1 À propos du logiciel

Bienvenue dans **Windows Password Recovery**, un analyseur de sécurité réseau et un utilitaire de récupération de mots de passe Windows. Windows Password Recovery est la seule solution qui implémente la plus avancée, brevetée de technologies de récupérations de mots de passe développées par les programmeurs de Passcape Software, comme *l'Intelligence Artificielle* ou *l'attaque par phrases de mots de passe*.

Comparé à des logiciels similaires, Windows Password Recovery dispose d'un certain nombre d'avantages compétitifs:

Pour les utilisateurs personnels - facilité d'utilisation et de configuration. Récupérations facilitées ou la réinitialisation des mots de passe oubliés pour tous les comptes Windows.

Pour les administrateurs système - audit de mots de passe révèle les brèches de sécurités, aide les administrateurs à assurer la fiabilité et la sécurité du réseau d'entreprise. Vérifier le niveau de sécurité des systèmes d'exploitations Windows.

Pour les enquêteurs, les experts en sécurité industrielle et gouvernementale - analyse et audit les règles de sécurité système ('policies'), émet des recommandations sur l'amélioration de la stabilité de la protection par mots de passe des systèmes d'exploitation.

1.2 Fonctionnalités et avantages

- Interface utilisateur graphique, moderne, facilement personnalisable.
- Chargement de hachages à partir de 9 programmes différents.
- Importation directe à partir de SAM ou ntds.dit; même si les fichiers sont verrouillés par le système, le programme continuera de les lire.
- Importation de hachages à partir d'ordinateurs distants.
- Importation de hachages à partir de copies système ('shadow'), de points de restauration, de répertoires de sauvegardes ou de réparations.
- Possibilité de sauvegarder\enregistrer les fichiers locaux de la base de registre et de la base de données de l'Active Directory.
- Importation de hachages d'historiques de mots de passe.
- Récupération des mots de passe de certains comptes à la volée (lors de l'importation locale).
- Support de l'Active Directory (comptes de Domaine).
- Support de l'importation à partir de systèmes 64-bits.
- Exportation de hachages vers le fichier PWDUMP.
- Le logiciel possède 17 sortes d'attaques différentes; 10 d'entre elles sont unique, développé par notre entreprise, mise en œuvre à partir de technologies brevetées.
- Le programme supporte le multi-tâche, utilisant toute la puissance des ordinateurs récents.
- L'attaque par Dictionnaires supporte les dictionnaires textes aux formats ASCII, UNICODE,UTF8, PCD, RAR et ZIP.
- Large choix de dictionnaires en ligne pour les attaques de dictionnaires (environ 2 Go).
- Certaines fonctionnalités du programme - ex: la mutation de mots - sont unique. Par exemple, le nombre total de règles de mutations excède les 150. Aucun autre logiciel ne possède cela !
- Support d'un nombre illimité de hachages inspectés, analysés.
- Analyse intelligente des mots de passe trouvés.
- Vitesse élevé de recherche avec les ordinateurs récents - plus de 100 millions de mots de passe par secondes pour un CPU 4 cœurs et plus de 1 milliard de mots de passe en utilisant la puissance des GPUs.
- Outils complémentaires inclus: générateur de hachages, test de la force de mots de passe, création de tables Arc-en-ciel, etc.

- Jeux d'outils étendus pour travailler avec les listes de mots: création, tri, conversion, etc.
- Ajout de modules pour les enquêteurs et les chercheurs: éditeur de secrets LSA, visionneuse d'infos d'identification de connexion de Domaine en cache, explorateurs d'Active Directory et SAM, décodeur hors-ligne DPAPI.
- Rapports avancés de mots de passe.

Interface du programme

2 Interface du programme

2.1 Vue générale

L'interface du programme est réalisée sous la forme d'une architecture (mono-document), par ex, cela permets de ne travailler que sur un seul projet à la fois. Le fonctionnement du programme peut être divisé en 4 niveaux:

- Création d'un projet
- Importation (chargement) des hachages de mot de passe dans le projet. Éditer les hachages: suppression, ajouter, sélectionner, etc.
- Récupération des hachages. Incluant la sélection, configuration et l'exécution d'une ou plusieurs attaques sélectionnées.
- Analyse des résultats.

L'interface dans son ensemble peut être divisée en plusieurs composants:

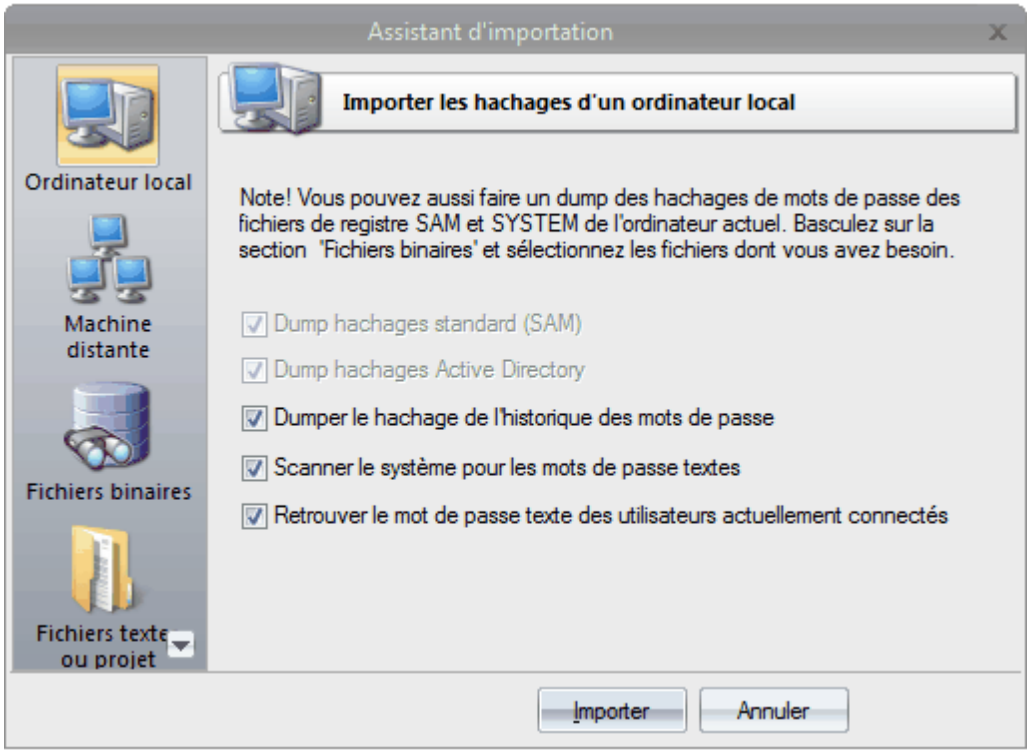
1. La barre de menus
2. La barre d'informations - pour l'affichage de courts textes d'informations - comme les astuces, les alertes, etc.
3. La barre de tâches - reproduit et complémente la barre de menu, fournissant un accès rapide à la plupart des fonctionnalités. Elle est constituée de trois parties:
   - Projet - incluant les principales fonctions tout au long du projet - comme l'ouverture, fermeture, création de nouveau projet, et l'importation des hachages.
   - Éditeur de Hachages. Reproduit la plupart des actions d'éditions.
   - Outils - incluant une horloge, un calendrier, et une calculatrice.
4. La fenêtre principale - supporte l'essentiel du travail et est constituée de 5 parties. Le premier onglet est la fenêtre d'accueil. Le second onglet contient la liste des hachages à analyser ou récupérer. L'onglet suivant, contient l'indicateur de l'attaque en cours (progression) et un autre onglet, les statistiques et les rapports. Pour finir - un onglet contient le moniteur système (matériel).
5. La fenêtre des journaux (logs) - Affiche les informations de l'état actuel du programme, de l'opération en cours, etc. Le journal du programme peut être copié dans le presse-papiers ou enregistrer dans un fichier (un clic droit ouvre le menu correspondant).
6. La barre de statut a pour fonction de fournir des informations.

2.2 Menu Projet

2.2.1 Importer

Windows Password Recovery offre un large choix d'options pour charger les hachages (hashes) en fonction de vos possibilités. Il y a 5 possibilités principales pour importer des hachages (hashes) dans le programme.

2.2.1.1 Importer des hachages locaux



Importer les hachages d'un ordinateur local - méthode préférable, qui implique une analyse générale, en profondeur, du système et des mots de passe. Hormis cela, les hachages qui sont importées à partir de l'ordinateur local peuvent être soumis à la sophistiquée *attaque intelligente*, qui permets de récupérer, relativement rapidement, les mots de passe de certains comptes.

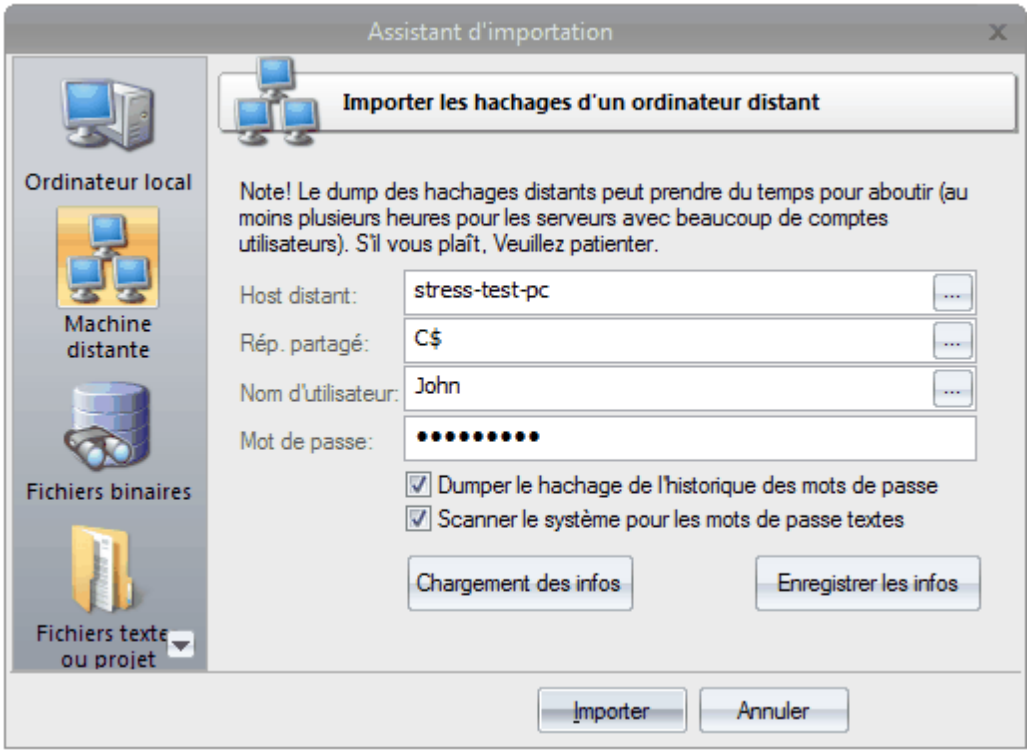
Importer des hachages locaux fonctionne bien quelque soit l'emplacement où sont situés les hachages: dans le SAM ou dans l'Active Directory. Cette fonction a deux options supplémentaires: le "dumping" de hachages d'historiques de mots de passe et la recherche de mots de passe en clair stockés dans le système.
Le processus de recherche pour les mots de passe en clair est divisé en 4 étapes et consiste en une recherche de mots de passe qui sont stockés dans le système utilisant le décryptage inverse, une recherche de mots de passe texte pour les comptes système, une recherche pour les mots de passe de démarrage et une étape supplémentaire, lorsque le programme analyse des comptes découverts, les mots de passe qui peuvent aussi être récupérés à partir du système (par exemple, pour le compte HomeGroupUser$ dans Windows 7).

Si la désactivation des deux dernières options n'est pas souhaitées, comme cela permets de réduire la charge et récupérer rapidement les mots de passe de certains comptes système, le dump de l'historique des mots de passe est complètement à l'opposé - il est désactivé, c'est souvent très utile. Par exemple, lorsque le nombre de mots de passe à importer excède la centaine de milliers ou souvent des millions. En revanche le programme possède une puissante intelligence artificielle, du coup, si pendant une attaque, il trouve un des mots de passe de l'historique, il s'efforcera de récupérer les mots de passe restants en analysant les préférences de l'utilisateur pour le mot de passe récupéré.

La dernière version du programme peut aussi dumper les hachages de l'historique de l'utilisateur à partir du fichier DPAPI CREDHIST. Il est donc recommandé, maintenant, d'activer cette option.

La fonction d"importation locale nécessite les droits d'administrateur.

2.2.1.2 Importer les hachages d'un ordinateur distant



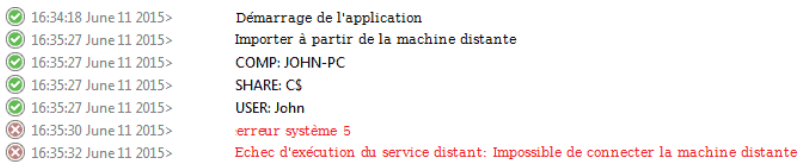
Importer les hachages d'un ordinateur distant. Le programme possède la capacité de dumper les hachages d'un ordinateur distant sans utiliser un utilitaire tierce. Cela n'endommage pas le système distant, étant donné qu'il faut fournir les informations d'identification de l'utilisateur de l'hôte distant.

Le dump d'un ordinateur distant fonctionne de la façon suivante. Premièrement, vous devez entrer le nom du host dans le champ "Host distant". Vous pouvez utiliser le bouton [...] pour parcourir le réseau. Une fois que vous avez choisi le host distant, renseignez le champ pour le répertoire partagé (Rép. partagé) permettant la lecture et l'écriture, à travers lequel les données seront transmises.
Habituellement, cela peut être C$ ou ADMIN$. Ici aussi, vous pouvez vous servir du bouton pour parcourir le système à droite la zone texte. Ensuite, dans les deux champs du bas, entrez le nom et le mot de passe du compte du host distant.

Le bouton "Enregistrer les infos" sauvegarde les paramètres. Tout comme le bouton "Chargement des infos" permets le chargement de paramètres existants, vous évitant ainsi de les saisir manuellement chaque fois que vous en avez besoin. Le mot de passe est stocké sous un format crypté !

Cette option d'importation nécessite aussi les droits d'administrateur, sur le PC source des fichiers.

Vous pouvez, cependant, avoir des problèmes de connexion sur le PC distant, même si vous avez un compte Administrateur. Lors de la connexion sur un PC sous Windows Vista/7/8/10, vous pouvez avoir l'erreur suivante:



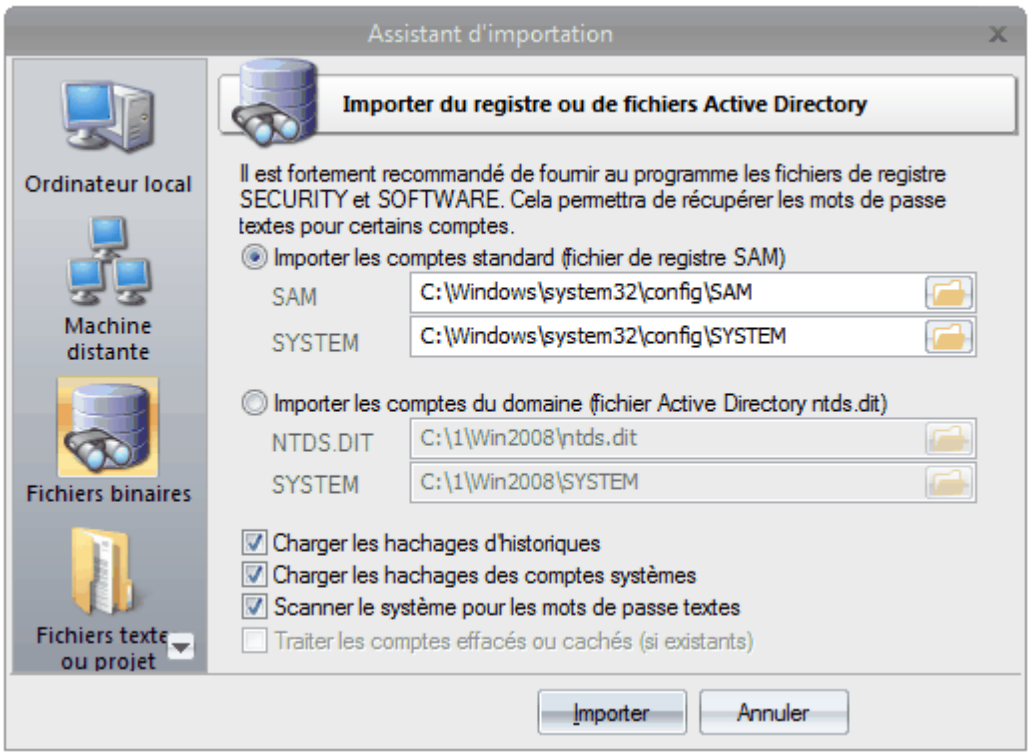
L'erreur 5 indique que l'accès a été refusé (même si le compte de destination a les privilèges d'administrateur). Le problème vient du fait que pour toute connexion distante dans Windows Vista et les OS supérieurs par défaut il n'est pas possible de réaliser des tâches d'administrateur. La documentation de Microsoft explique la situation de la manière suivante:

"Lorsqu'un utilisateur avec un compte administrateur sur un ordinateur local avec Windows Vista, avec une base de données SAM (locale), se connecte à un ordinateur sous Windows Vista, l'utilisateur n'a pas d'élévation des privilèges sur l'ordinateur distant et du coup ne peut pas effectuer des tâches d'administrations. Si l'utilisateur veut administrer une station (distante) avec un compte SAM (local), l'utilisateur doit se connecter sur l'ordinateur distant pour l'administrer."

Il y a, cependant, un paramètre dans la base de registre Windows qui permets de changer cette fonction par défaut. Exécutez l'éditeur de la base de registre et ouvrez la clé suivante:
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\system

Puis créez la valeur *LocalAccountTokenFilterPolicy* (type DWORD) et paramétrez la à un (1). Ainsi vous serez capable de vous connecter à l'administrateur partagé.

2.2.1.3 Importer des hachages à partir de fichiers binaires



Importer des hachages à partir de fichiers binaires. Windows Password Recovery peut extraire des hachages de mots de passe directement de fichiers binaires. Ce type de fichiers étant habituellement utilisés par le système et donc verrouillés.

Normalement, les hachages de mots de passe sont stockés dans le fichier SAM de la base de registre, qui réside dans le répertoire "%WINDOWS%\System32\Config". Le même répertoire contient le fichier de registre SYSTEM, qui est nécessaire pour la récupération. Si vous avez indiqué le chemin de la base de registre dans le système, l'analyse sera légèrement plus longue (normalement de quelques secondes).

Les hachages de mots de passe pour les comptes de domaine sont stockés dans la base de données de l'Active Directory; ou, plus être plus précis, dans le cœur de celle-ci, dans le fichier ntds.dit, qui réside dans le répertoire: "%Windows%\ntds".

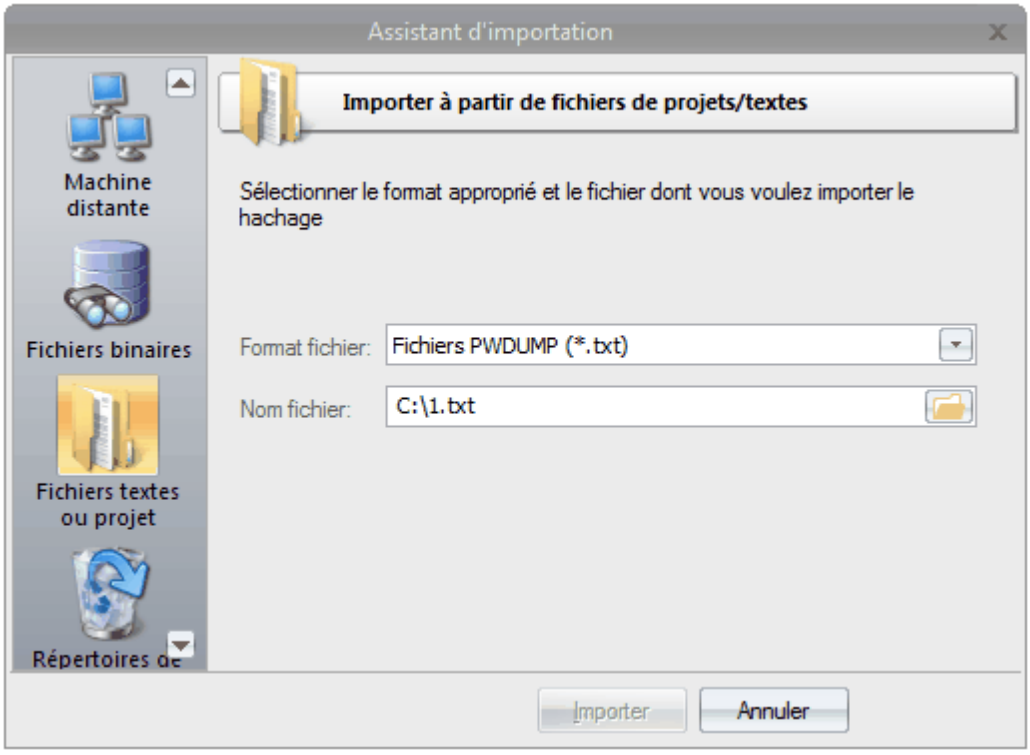
La récupération des comptes de domaine nécessite également, le fichier SYSTEM de registre. Attention !! Le dump à partir de la base de donnée de l'AD du système en cours peut prendre du temps, spécialement lorsque le le fichier ntds.dit a une taille importante.

Le programme fonctionne correctement et supporte toutes les options de cryptage de SYSKEY: Registre SYSKEY, disquette de démarrage SYSKEY, mot de passe de démarrage SYSKEY.

Si vous copiez les fichiers à partir d'un autre système, hormis les fichiers SAM (ntds.dit) et SYSTEM, il est aussi, fortement recommandé, de copier les fichiers de registre SECURITY et SOFTWARE (qui doivent être situé dans le même répertoire que le fichier SYSTEM); Ce qui vous permettra de récupérer, rapidement, les mots de passe des autres comptes d'utilisateurs.

En utilisant les options complémentaires vous pouvez:
- Activer/désactiver le chargement des hachages d'historiques. Désactiver le chargement de l'historique améliorera l'analyse de la base de données. D'un autre coté, lorsque le processus (d'attaque) des hachages, trouvera les mots de passe de l'historique cela pourra donner un indice pour déterminer le mot de passe des hachages du compte principal.
- Désactiver le chargement des comptes machine (ayant un $ comme caractère à la fin).
- Activer/désactiver la vérification rapide des mots de passe en clair, si ils existent.

2.2.1.4 Importer à partir de fichiers de projet/textes



Pour terminer, vous pouvez charger les hachages dans votre projet **en les important d'autres applications.** Le logiciel supporte les formats suivants:

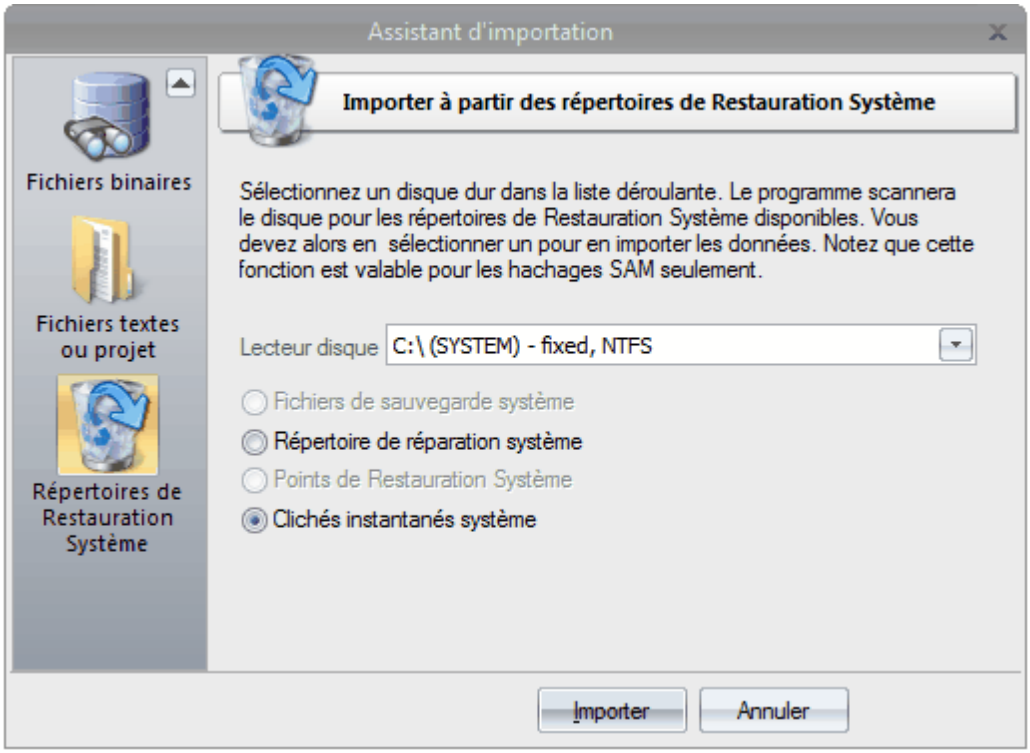
- **PWDUMP** - malgré plusieurs inconvénients, c'est le format standard pour stocker les hachages de mots de passe. Remarque importante: Ce format ne supporte pas complètement les caractères nationaux. Du coup, certains noms d'utilisateurs et des commentaires peuvent ne pas être affichés correctement. Windows Password Recovery supporte aussi les fichiers texte PWDUMP en UNICODE.
- **LophtCrack (*.lcs)** - ce format est utilisé par le logiciel LophtCrack. Le programme WPR supporte toutes les versions de fichiers LCS, commençant avec v4.
- **Fichiers projet *.hdt**, sont utilisés par Proactive Password Auditor (utilisé pour être des PWSEX) de ElcomSoft. WPR supporte, aussi, toute les versions du format commençant par v3.
- **Fichiers *.hsh**, qui sont exportés par Proactive System Password Recovery, célèbre entreprise bien connu pour son logiciel.
- **Listes de Hachages (Hash) *.lst**, créées par Cain & Abel. Windows Password Recovery supporte les fichiers LST à partir de la version v.4.9.12. les versions précédentes de fichiers LST utilisent le point virgule " ; " comme délimiteur à la place des tabulations " TAB ". Malheureusement, le fichier LST ne possède pas d'indication sur la version; malgré tout, si le fichier est illisible, vous pouvez remplacer manuellement tout les délimiteurs de champs par une tabulation " TAB ".
- **Fichiers *.winpsw**, créés par WinPassword, du fameux logiciel LastBit. Le support est assuré de toutes

les versions, à partir de la version v6.

- **Fichiers de projet SamInside (*.hashes)**. Ce format est similaire au fichier texte PWDUMP, mais il est plus souple d'emploi et utilise le caractere 0x7f a la place d'une virgule, ce qui plus logique.
- **Fichiers de projet PasswordPro (*.hashes)**. Ce format est similaire au fichier texte PWDUMP, excepté plusieurs modifications. Il peut être utilisé par le logiciel de chez PasswordsPro.
- **Fichier de Configuration Universel (*.puc)**. Ce fichier est utilisé par le logiciel Reset Windows Password et peut contenir plusieurs différents types de "dumps".
- **Hachages en "clair" (*.*)**. Hachages bruts au format texte (32 ou 16 caractères sur une ligne).

Après l'importation des hachages, le programme marque automatiquement tous les hachages LM et NT et exécute une attaque préliminaire. Cette action est optionnelle et peut être désactivée dans les paramètres généraux de configuration. Cette option est activée par défaut.

2.2.1.5 Importer des hachages de répertoires des restaurations système



Encore une option, et non pas la moins inutile, qui est **l'importation des hachages à partir des répertoires de la Restauration Système**. Tout ce que vous devez savoir est que vous devez, seulement, indiquez le chemin (path) d'un des disques durs. Le programme trouvera, automatiquement, les répertoires de restaurations et, si il trouve les fichiers nécessaires, il importera les hachages.

La recherche est réalisée dans l'ordre suivant:

1. Dans le répertoire système.
2. Dans le répertoire "%Windows%\Repair%", qui contient normalement les sauvegardes de la base de registre du système.
3. Dans le répertoire du "System Volume Information", qui est utilisé pour annuler les modifications réalisées dans le système. Cette technologie est disponible depuis Windows XP et est aussi connu sous le nom Système de restauration (XP) ou Copie Shadow (Vista+).

Attention, tout de même, les sauvegardes de registre peuvent contenir des données obsolètes !

2.2.2 Exporter

Tous les hachages de projets, ainsi que les paramètres, sont stockés dans un fichier de projet (*.wpr); Toutefois, pour une meilleure flexibilité et compatibilité avec d'autres logiciels, le programme peut exporter les hachages dans un fichier PWDUMP ou POT. Si l'exportation vers un fichier POT' est choisie, tous les mots de passe avec les hachages NTLM correspondant seront sauvegardés dans le fichier sous le format suivant:
hachage:mot de passe

Vous pouvez modifier le format d'exportation par défaut en maintenant appuyé, la touche "Shift" de votre clavier lorsque vous cliquez sur "Exporter dans un fichier POT".
Le contenu du fichier sera sous la forme:
utilisateur (rid): mot de passe

Les mots de passe seront encodés au format UTF8.

2.2.3 Nouveau

Enregistre le projet en cours et en crée un nouveau.

2.2.4 Ouvrir

Charge/ouvre un nouveau projet. Les projets du logiciel ont une extension *.wpr et contiennent les paramètres du logiciel et les hachages. Toutefois, pour accélérer la recherche, le programme stocke l'état actuel de la progression de l'attaque dans un fichier ".ini".

2.2.5 Enregistrer

Enregistre le projet en cours. Il est recommandé d'enregistrer les projets importants de temps en temps.

2.2.6 Enregistrer sous

Enregistre le projet en cours sous un nom différent (renomme le projet).

2.2.7 Fermer

Ferme le projet en cours.

2.3 Menu de récupération

Ce menu permets de sélectionner et de lancer une attaque. Le panneau *"Attaque"* permets de choisir le type d'attaque et de basculer entre les hachages LM ou NT. Pensez, avant de lancer l'attaque, à sélectionner/marquer les hachages concernés, en utilisant le menu **"Éditer -> Sélectionner"**. Le lancement d'une attaque suppose que vous avez effectué tous les paramétrages (dans menu **"Options--> Options d'Attaques"**).

2.3.1 Démarrer

Exécute l'attaque sélectionnée. Pendant l'exécution de l'attaque, les autres éléments du menu sont désactivés.
Lorsque l'attaque sera terminée, le programme lancera une routine spéciale de mutation et d'analyse de mots de passe pour les mots de passe trouvés. Cette option est activée par défaut, mais peut être désactivée dans les paramètres généraux.

2.3.2 Reprendre

Reprends l'attaque à partir du dernier point enregistré. Gardez en mémoire, que le dernier point mémorisé est automatiquement effacé, lorsque des modifications sont faites dans les options d'attaques.

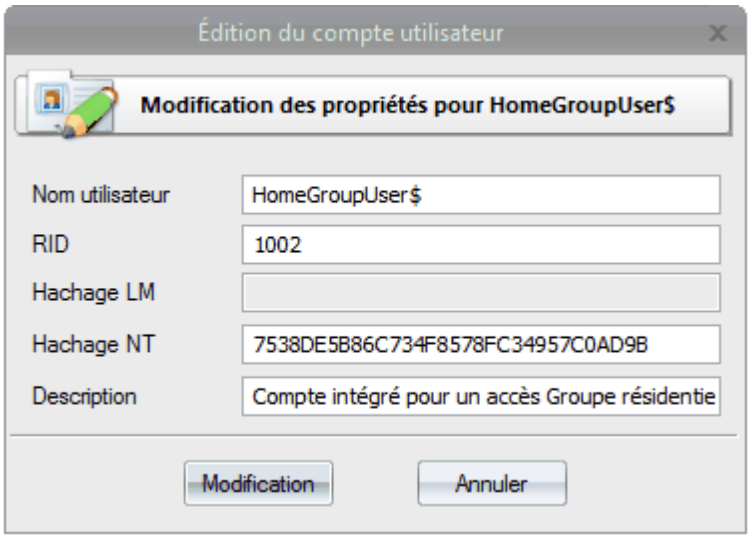
2.3.3 Arrêter

Arrête l'attaque en cours.

2.4 Menu Editer

Le menu Éditer est disponible seulement lorsque l'onglet "Hachages" est actif; incluant 4 groupes d'éléments: Éditer, Copier, Sélectionner et Rechercher.

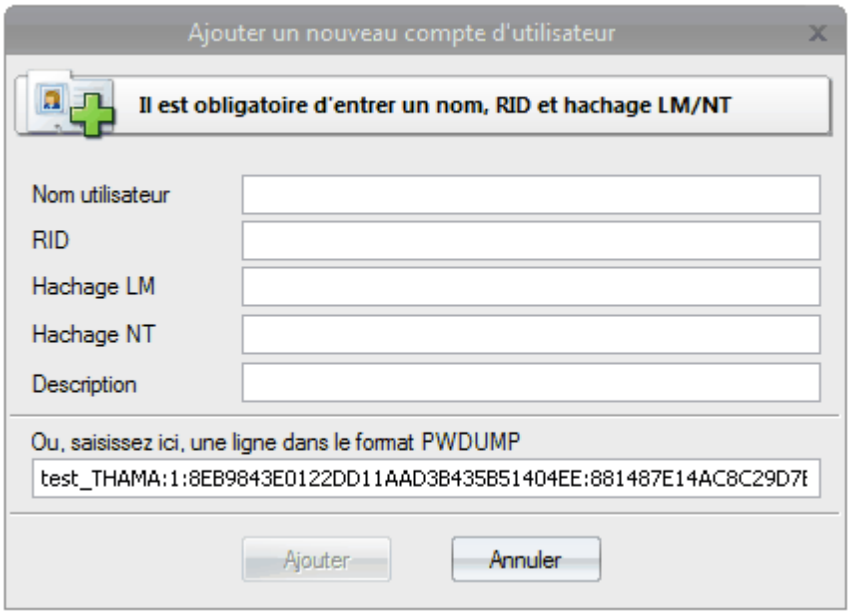
2.4.1 Editer la ligne surlignée



La sélection de cet élément ouvre une boite de dialogue où vous pouvez manuellement éditer les champs suivants pour le compte sélectionné:

- Nom de l'utilisateur RID de l'utilisateur
- Les hachages LM et NT
- Le commentaire du compte.

2.4.2 Ajouter un nouveau



Permets l'ajout, manuellement, d'un nouveau compte d'utilisateur. Cette boite de dialogue permets de saisir des chaînes de caractères au format PWDUMP.

2.4.3 Supprimer

Supprime les entrées de la liste surlignées (par ex. celles qui sont sous le curseur), marquée ou la totalité.

2.4.4 Réinitialiser les mots de passe

Supprime tous les mots de passe de la liste.

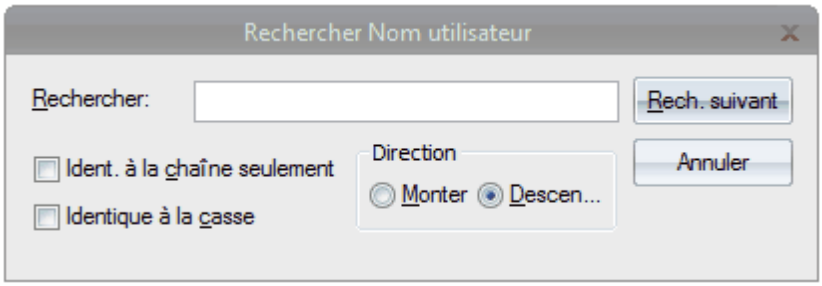
2.4.5 Copier

Copie la ligne (surlignée) dans le Presse-papiers de Windows. Seulement, la partie sélectionnée est copiée, et non pas la ligne complète. Par exemple, le nom de l'utilisateur ou le mot de passe trouvé.

2.4.6 Sélectionner

Sélectionne les hachages qui doivent être attaquées (ceux dont la case est cochée). Si durant l'attaque, le mot de passe pour le hachage sélectionné, est trouvé, la case sera automatiquement décochée, et la ligne sera surlignée en vert. Pour sélectionner les hachages NT, vous devez, en premier, désélectionner le hachages LM, et l'inverse pour les hachages LM.

2.4.7 Rechercher



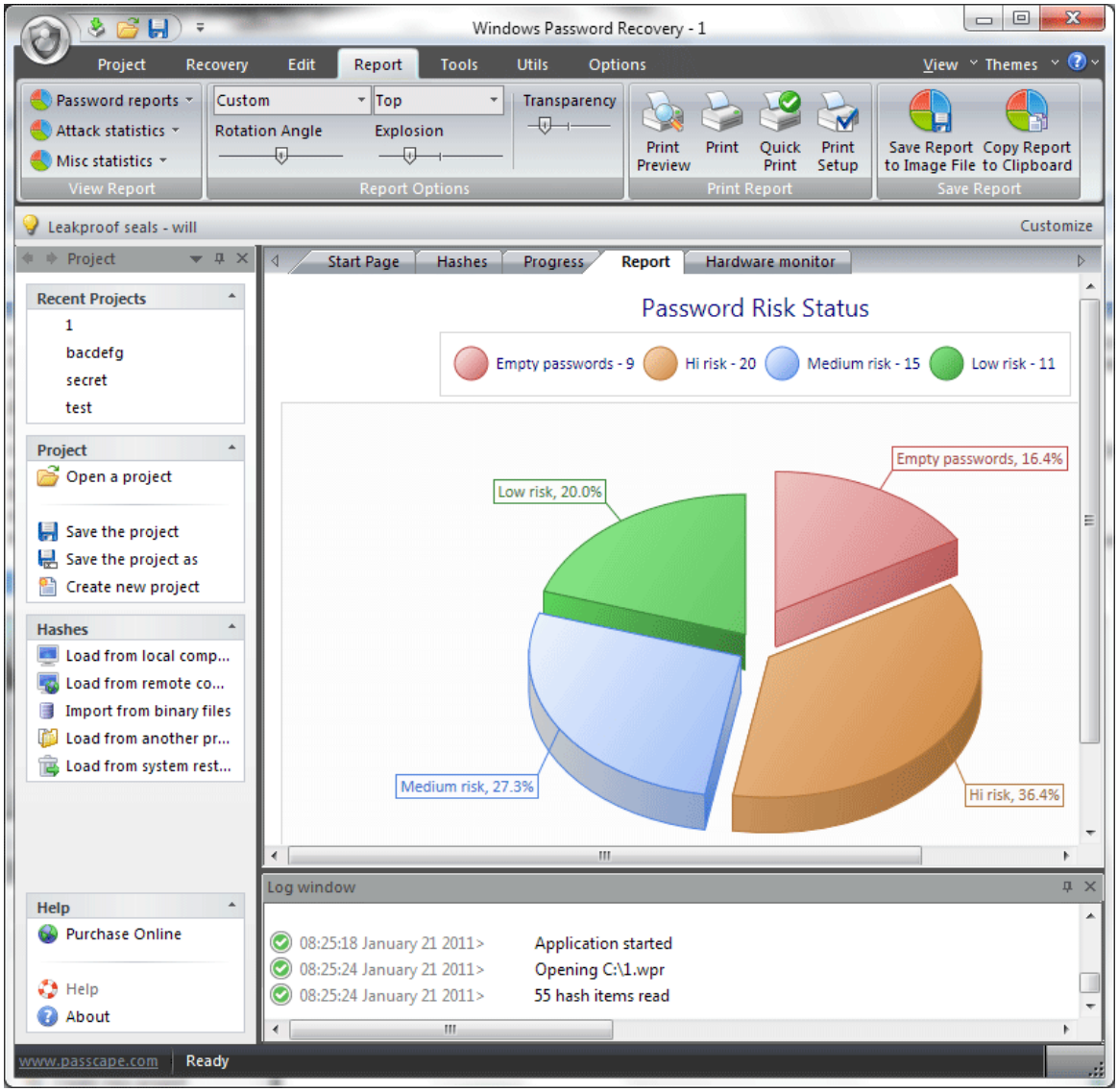
Lorsque le nombre d'entrées excède une centaine de milliers, trouver une entrée spécifique prends souvent plus d'efforts.
Pour réaliser ce travail facilement, le programme propose une recherche de deux types:

- Une recherche d'un champ spécifique (ex: un nom d'utilisateur)
- Une recherche rapide d'une série d'entrées. Le programme scanne l'intégralité de l'entrée, caractère par caractère.

2.5 Menu Rapports

Vous pouvez créer, imprimer ou enregistrer un des rapports du programme ici. Les rapports suivants sont disponibles:

- Rapports de mots de passe
- Statistiques d'attaque
- Statistiques divers
- Statistiques de comptes
- Analyse de liste de mots de passe
- Informations de groupes



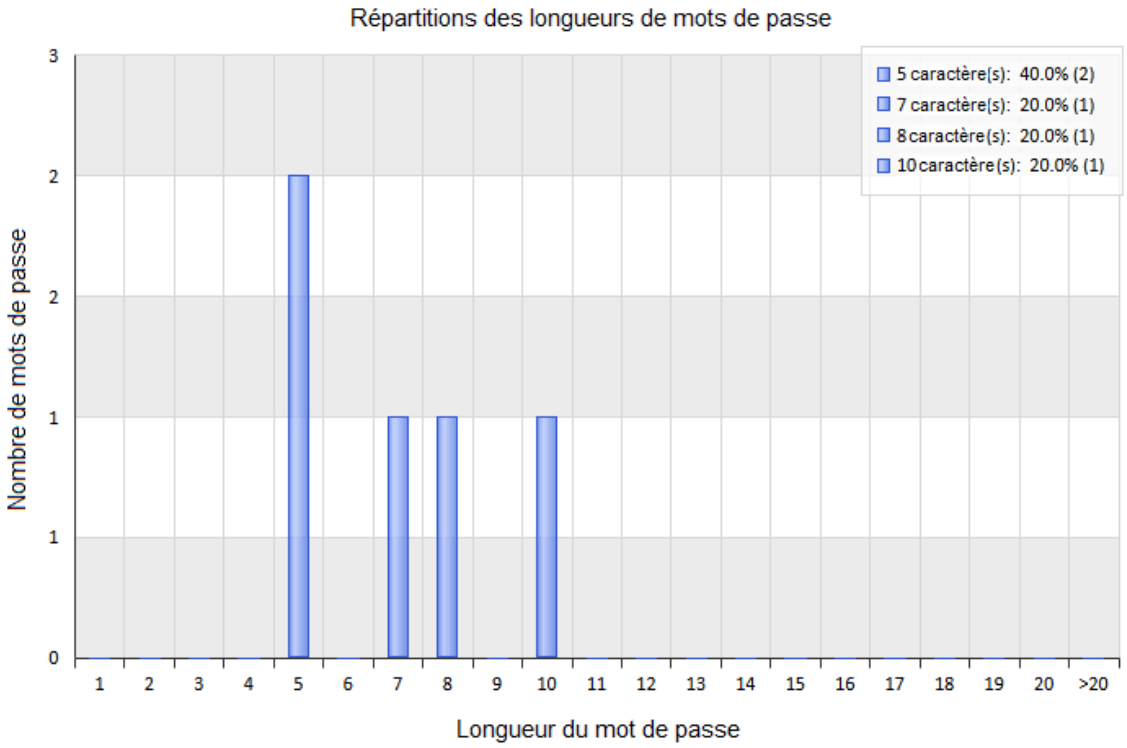
2.5.1 Rapports de mots de passe

Les rapports suivants sont disponibles ici:

- **Statut de risques de mots de passe** - Affiche les mots de passe vides, trouvés, et non découverts.
- **Complexité de mots de passe** - Rapporte le nombre de mots de passe et les différents caractères audités.
- **Répartition de longueur des mots de passe** - Affiche un résumé de la longueur des mots de passe cassés.
- **Mot de passe unique** - Ce rapport affiche un graphique des mots de passe unique comparé à ceux réutilisés.
- **Top des mots de passe réutilisés** - Affiche le top 20 des mots de passe les plus populaires.
- **LM par rapport NT** - Rapporte le nombre de hachages LM et NT.
- **Mots de passe habituels par rapport à l'historique** - Rapporte le nombre de mots de passe communs

et de l'historique (seulement pour les hachages importés des fichiers SAM\NTDS.DIT; ex. importés à partir de l'ordinateur local)

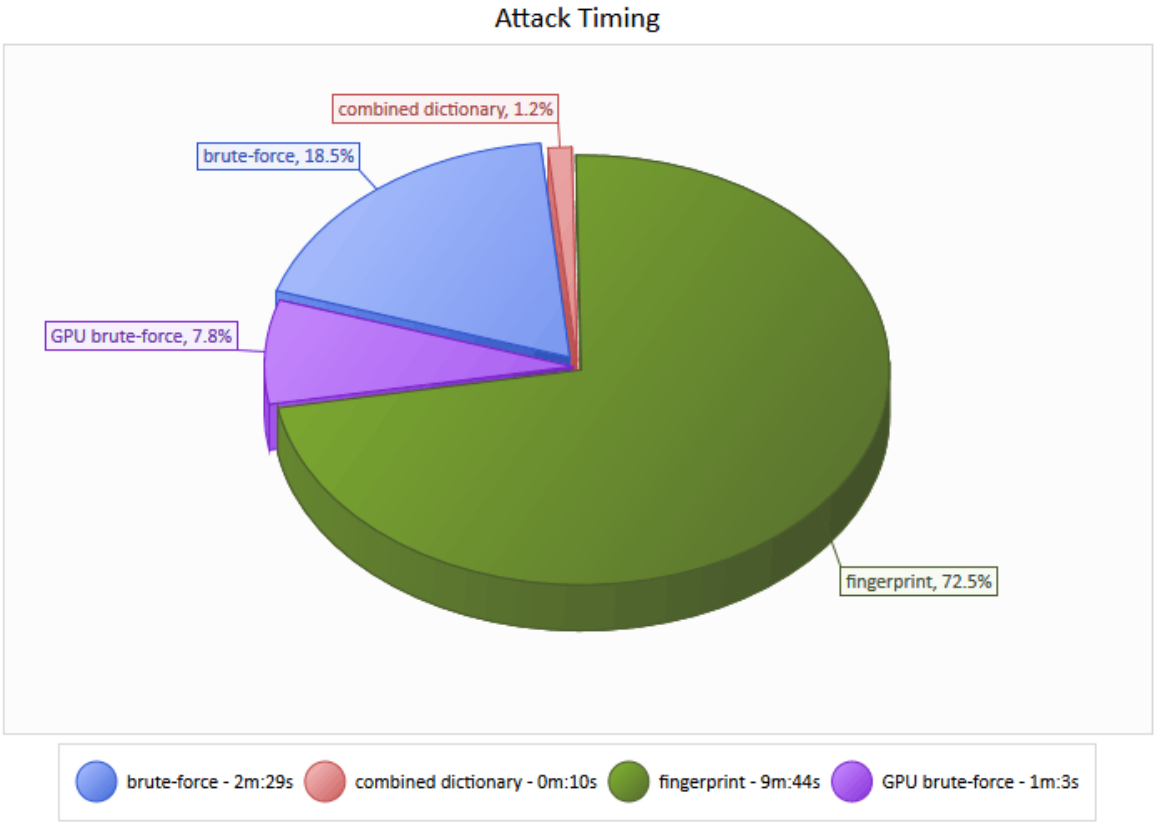
- **Temps de récupération de mots de passe** - Temps pour cracker un/des mot(s) de passe, en particulier. Les mots de passe les plus vulnérables sont marqués en rouge.
- **Mots de passe récupérés par rapport à ceux non découverts** - Affiche le nombre de mots de passe découverts et non découverts.
- **Mots de passe trouvés** - Affiche un rapport détaillé sur les mots de passe trouvés.



2.5.2 Statistiques d'attaques

Les statistiques d'attaques inclues les éléments suivants:

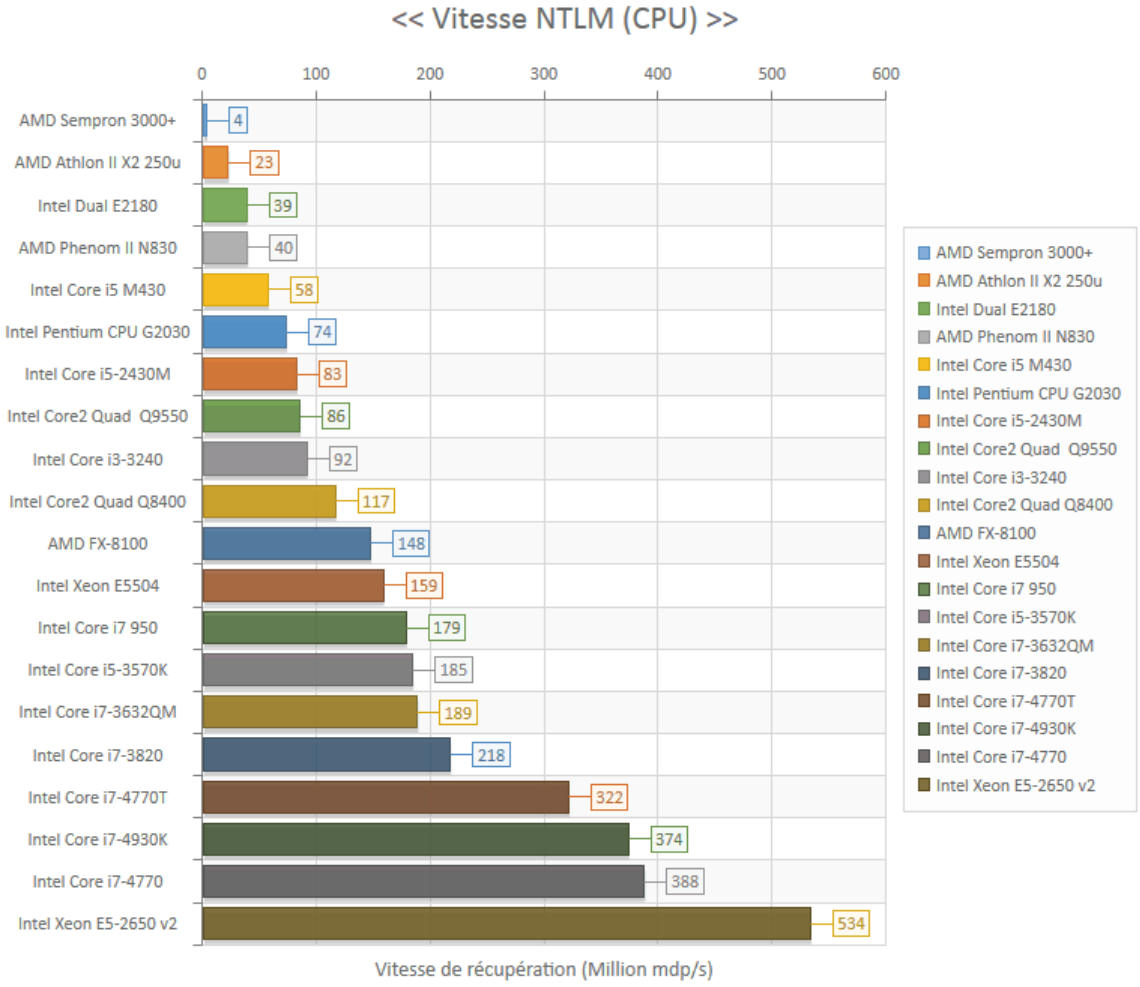
- **Attaques préférées** - Statistiques sur le nombre et le type d'attaques utilisées.
- **Durée des attaques** - Analyse le temps pris pour chaque attaque.
- **Efficacité de l'attaque (vitesse)** - Analyse d'efficacité: ratio du temps d'une attaque par rapport aux mots de passe trouvés.
- **Efficacité de l'attaque (générale)** - Analyse d'efficacité: efficacité générale pour chaque attaque.



2.5.3 Statistiques divers

Quelques statistiques complémentaires comme:

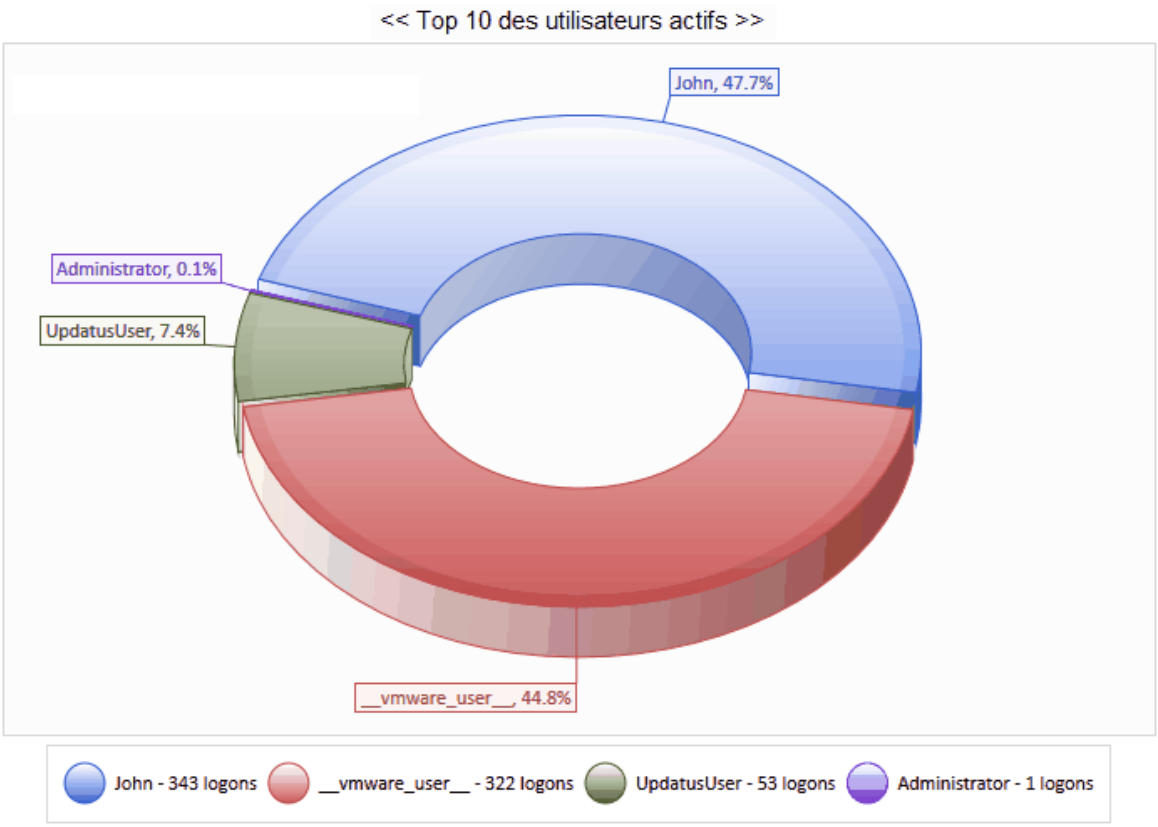
- **Vitesse CPU** - Comparaison de vitesses de récupérations de mots de passe (pour l'attaque par force-brute).
- **Vitesse GPU** - Affiche et compare la vitesse de récupération de mots de passe pour votre périphérique GPU. Vous pouvez mesurer la performance de votre CPU ou GPU en utilisant l'outil Pass-o-meter.
- **Utilisateurs crackés** - Affiche le nombre d'utilisateurs crackés. La liste complète des comptes d'utilisateurs crackés peut être, également, enregistrée dans un fichier texte.
- **Utilisateurs et mots de passe crackés** - Affiche la liste des comptes crackés avec les mots de passe.



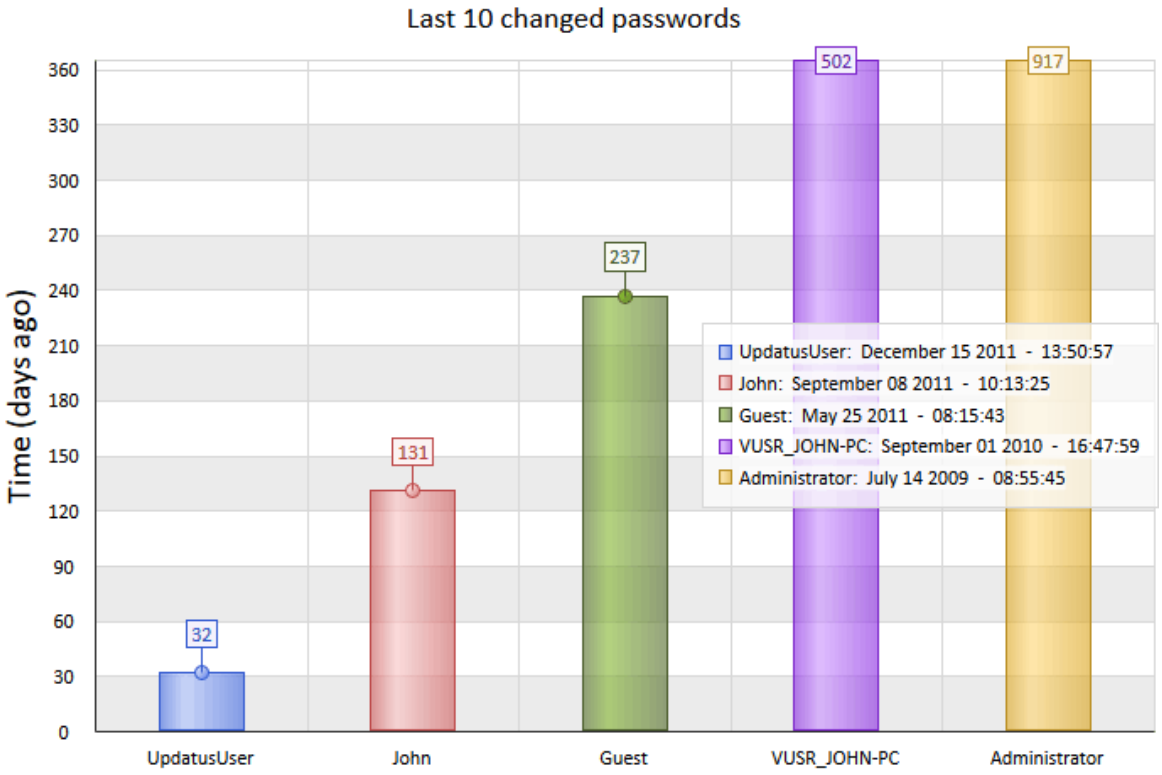
2.5.4 Statistiques de comptes

Les statistiques de compte sont disponibles pour les comptes locaux et de Domaine. Pour générer un rapport, sélectionner en premier les données source: base de données locales ou externes, SAM ou Active Directory. Ces rapports sont disponibles dans les catégories suivantes:

- **Comptes standard vs. désactivés.** Ce rapport affiche le ratio des comptes utilisateur standard par rapport à ceux désactivés.
- **Comptes standard vs. verrouillés.** Ratio des comptes standard vs. bloqués\verrouillés.
- **Avec/sans mots de passe.** Affiche le nombre de compte qui possède ou non un mot de passe.
- **Comptes utilisateurs vs. machine.** Ratio des comptes utilisateurs vs. systèmes.
- **Mots de passe actifs vs. expirés.** Rapport avec les statistiques sur les comptes actifs vs. expirés.
- **Mots de passe standard vs. sans expiration** - Compare les comptes utilisateurs standard par rapport à ceux qui ont un indicateur (flag) de "Mot de passe n'expirant pas" ou une date d'expiration du mot de passe illimitée.
- **Utilisateurs administrateurs vs. limités.** Ce rapport donne des statistiques comparatifs sur les comptes utilisateurs avec les droits administrateur vs. ceux restreints.
- **Types de comptes.** Affiche le nombre de comptes machines, utilisateurs, administrateurs, etc.
- **Statut des comptes.** Affiche les comptes actifs et désactivés. Identique au premier rapport mais n'affiche pas dans un panneau, à gauche, du graphique, les comptes désactivés.
- **Top 10 des utilisateurs les plus actifs.** Rapport sur les utilisateurs les 10 plus actifs. Les statistiques sont recueillies à partir du compteur interne du système d'identification des utilisateurs.
- **Erreurs de mots de passe d'identifications.** Top 10 des utilisateurs avec le compteur le plus haut taux d'erreurs d'identification de connexions.



- **10 derniers échecs de connexions de session** - Affiche la liste des utilisateurs de comptes ayant échoué lors de leur dernière tentative de connexion.
- **10 derniers mots de passe modifiés** - Affiche le temps écoulé (nombres de jours), des 10 utilisateurs qui ont modifié leur mots de passe.
- **10 dernières connexions de session** - Affiche le temps passé (nombres de jours), des 10 utilisateurs qui ont eu un échec de connexion au système.
- **10 dernières déconnexions de session** - Affiche le temps écoulé depuis la déconnexion des 10 derniers comptes.
- **Comptes qui expirent prochainement** - Utilisateurs dont le compte va bientôt expirer.
- **Activités de connexions -** Groupes d'utilisateurs en fonction du temps passé depuis leur dernière connexion au système.
- **Ancienneté du mot de passe -** Groupes d'utilisateurs en fonction du temps passé depuis leur dernière modification/changement de leur mot de passe.

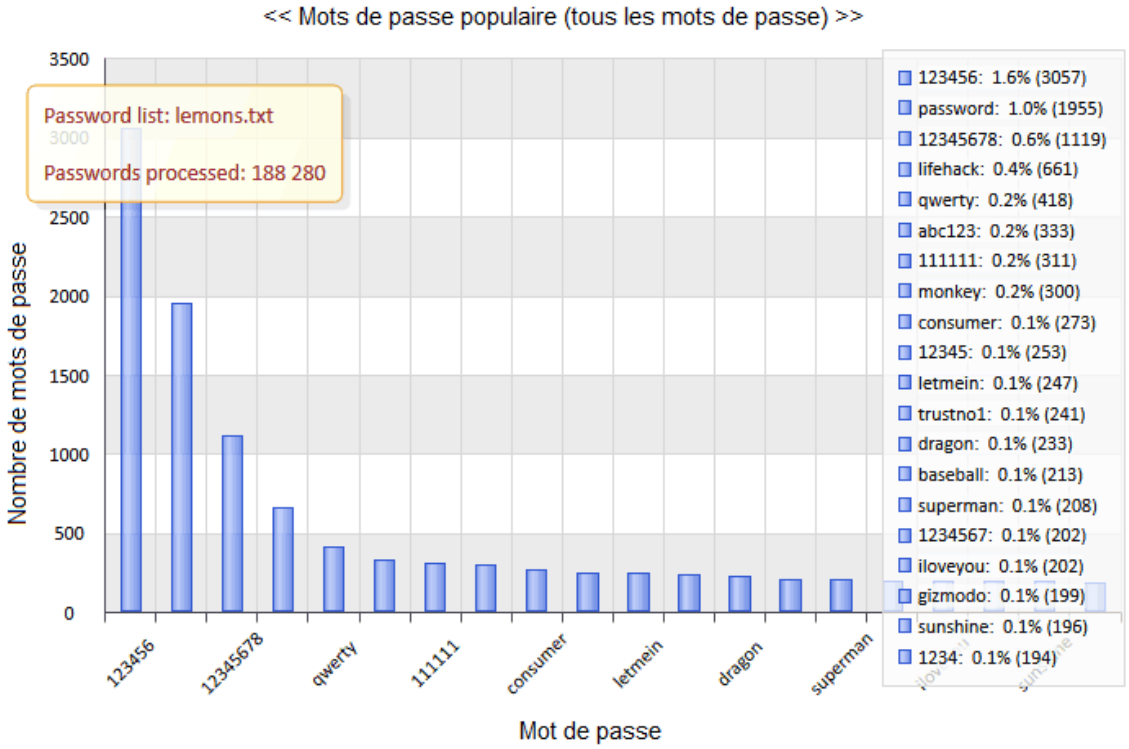


2.5.5 Analyse "liste de mots de passe"

Les rapports de "liste de mots de passe" affiche différents statistiques et réalisent une analyse en profondeur pour la liste des mots sources. Vous pouvez comme source de "listes de mots de passe", par exemple, utiliser la liste des mots de passe récupérée par le programme.
Vous pouvez générer des rapports pour tous les mots dans le liste ainsi que pour les mots de passe ayant, uniquement une certaine longueur.
Les rapports suivants sont disponibles, dans ce menu:

- **Répartition de la longueur des mots de passe** - Affiche une vue globale de la longueur d'un mot de passe dans une liste de mots de passe choisie.
- **Mots de passe uniques** - Ce rapport affiche un graphique des mots de passe unique comparés à ceux identiques.
- **Mots de passe populaires** - Affiche les mots de passe les plus populaire et leur pourcentage du nombre total de mots de passe.
- **Formats de mots de passe** - Statistiques des 20 plus populaires formats. Par exemple, le masque DDUUUUDD corresponds aux mots de passe constitués de deux chiffres au début et à la fin, avec quatre lettres capitales au milieu. Vous pouvez sauvegarder les masques de mots de passe populaires dans un fichier qui peut ainsi être utilisé, plus facilement ultérieurement, dans une attaque à base de masques.
- **Exclusivité des jeux de caractères** - Ce rapport affiche le nombre de mots de passe constitués d'un jeu unique de caractères et le pourcentage de ces mots de passe constitués de plusieurs jeu de caractères.
- **Diversité des jeux de caractères** - Le pourcentage des mots de passe constitués d'un, de deux, ou de plusieurs jeux de caractères.
- **Jeux de caractères** - Liste de tous les jeux de caractères réalisées à partir des mots de passe saisies.
- **Ordre des jeux de caractères** - les modèles les plus populaires correspondent à l'ordre des jeux de caractères. Par exemple, le modèle *chiffre-chaine spéciale* inclut les mots de passe suivants: 123password!@#, 1ove*****, et 12monkey^, etc.
- **Fréquence des caractères** - Statistiques sur la fréquence des caractères des mots entrées. Les 20 plus fréquents caractères sont affichés.
- **Caractères uniques** - Affiche les 20 caractères plus fréquents.

- **Caractères fréquemment utilisés à l'avant** - Statistiques des combinaisons les plus fréquentes de 1 à 3 caractères au début des mots.
- **Caractères fréquemment utilisés à l'arrière** - Statistiques des combinaisons les plus fréquentes de 1 à 5 caractères à la fin des mots.
- **Combinaisons fréquentes** - Les 20 combinaisons utilisées, les plus fréquentes, de 4 à 8 caractères.

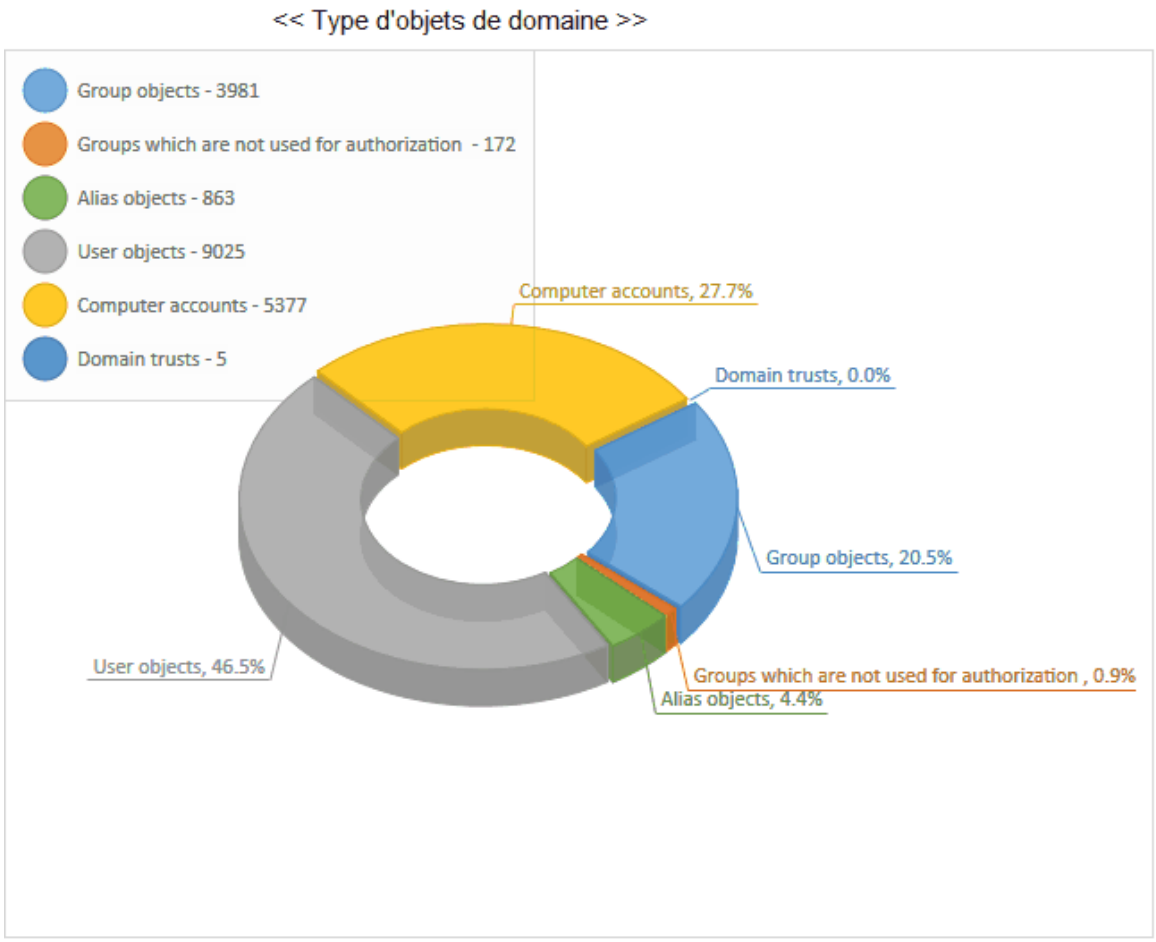


2.5.6 Informations de groupes

Cette section possède principalement des outils pour analyser diverses informations sur les groupes et alias de l'Active Directory. Des rapports peuvent toutefois être utilisés pour afficher des statistiques du PC local, les informations étant obtenues à partir du fichier SAM de la base de registre.
Les rapports suivants sont disponibles dans ce menu:

- **10 derniers groupes créés** - 10 groupes de comptes qui ont été créé récemment.
- **10 derniers groupes modifiés** - 10 groupes de comptes modifiés récemment.
- **Types de groupes** - Ce rapport affiche les différents types de groupes.
- **Groupes les plus populaires** - Affiche le top 10 des groupes ayant le plus grand nombre d'utilisateurs.
- **Groupes les moins utilisés** - Affiche le top 10 des groupes ayant le plus petit nombre d'utilisateurs. Les groupes sans utilisateur ne sont pas affichés dans ce rapport.
- **Groupes actifs vs ceux inactifs** - Le programme suppose que les groupes actifs ont au moins un membre tandis que les groupes inactifs n'ont pas de membre.
- **Groupes Admin vs ceux non-Admin** - Affiche les statistiques sur les privilèges des administrateurs du groupe.
- **10 derniers alias créés** - 10 alias de comptes récemment créés.
- **10 derniers alias modifiés** - 10 alias de comptes récemment modifiés.
- **Types d'alias** - Ce rapport affiche les différents types d'alias de comptes.
- **Alias les plus populaires** - Affiche le top 10 avec le plus grand nombre d'utilisateurs.
- **Alias les moins utilisés** - Affiche le top 10 avec le moins grand nombre d'utilisateurs. Les alias sans utilisateur ne sont pas affichés.
- **Alias actifs vs inactifs** - Le programme suppose que les alias actifs ont au moins un utilisateur tandis que les alias inactifs n'ont pas de membre.
- **Alias Admin vs ceux non-Admin** - Affiche les nombre d'alias ayant les privilèges d'Administrateurs.

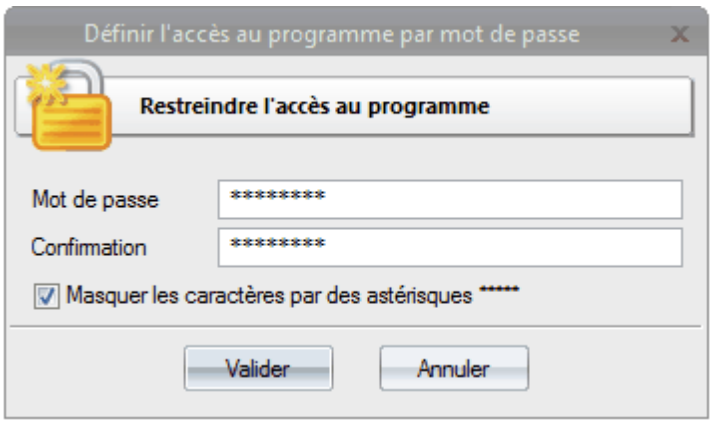
- **Types d'objets de Domaine** - Affiche les informations sur les objets trouvés dans un Domaine. Par exemple: comptes d'utilisateurs, de groupes, de l'ordinateur, domaines de confiance, etc.



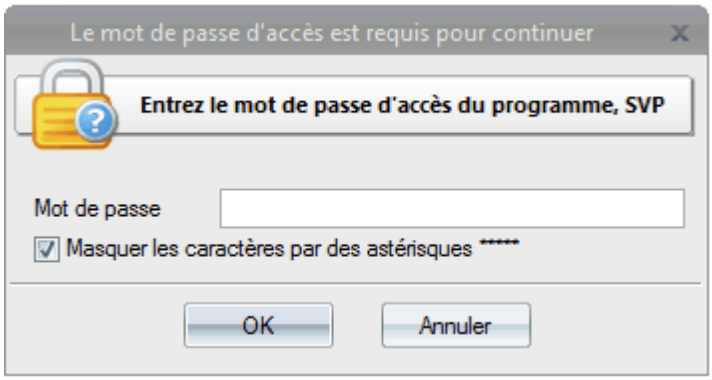
2.6 Menu Outils

Il y a deux sortes d'outils: Les outils pour le contrôle de l'accès à l'application et les outils pour travailler avec les mots de passe.

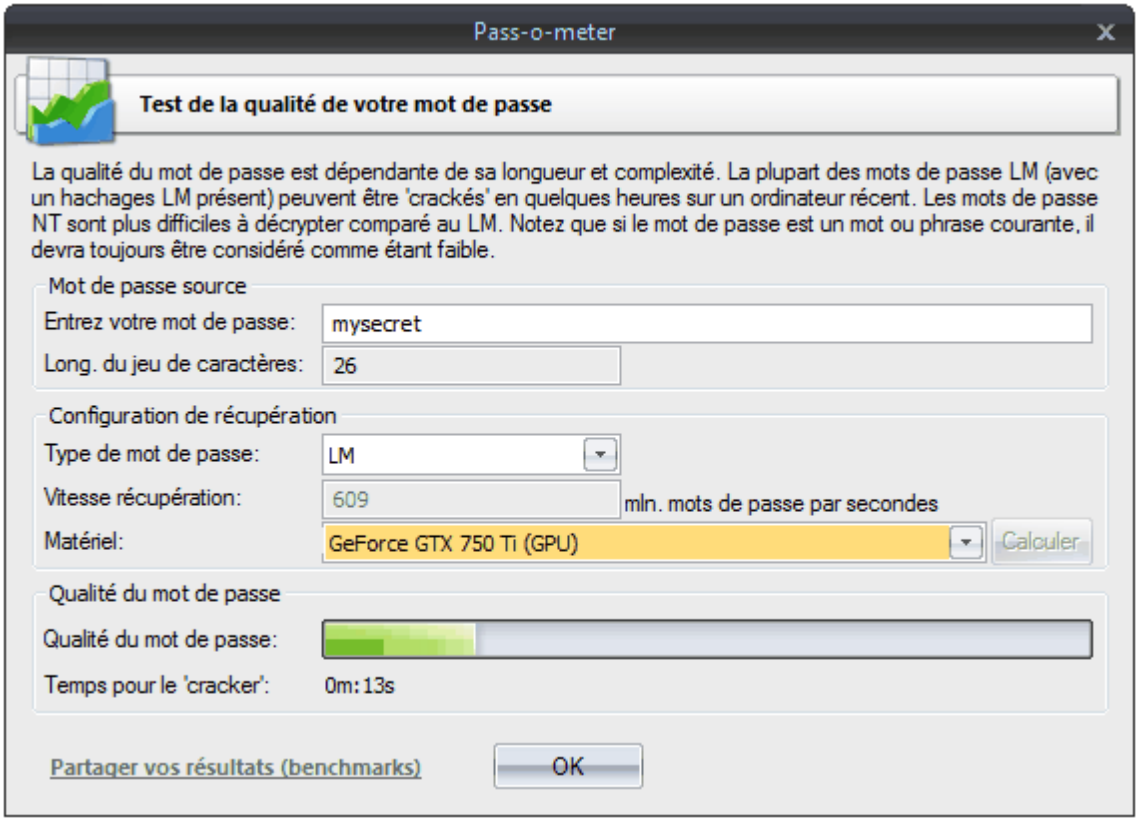
2.6.1 Accès au programme



Si quelqu'un en votre absence, peut accéder à votre ordinateur ou votre compte, vous pouvez protéger par mot de passe le logiciel. Dans ce cas, lors du démarrage du logiciel, l'utilisateur devra saisir le mot de passe. Le logiciel ne pourra pas être utilisé si le mot de passe fourni est invalide.



2.6.2 Pass-o-meter



Cet outil permets de mesurer la "force" ou complexité du mot de passe. Lors du premier démarrage, le programme demande de tester la performance de l'ordinateur.
Différentes étapes pour tester la qualité d'un mot de passe sont nécessaires:

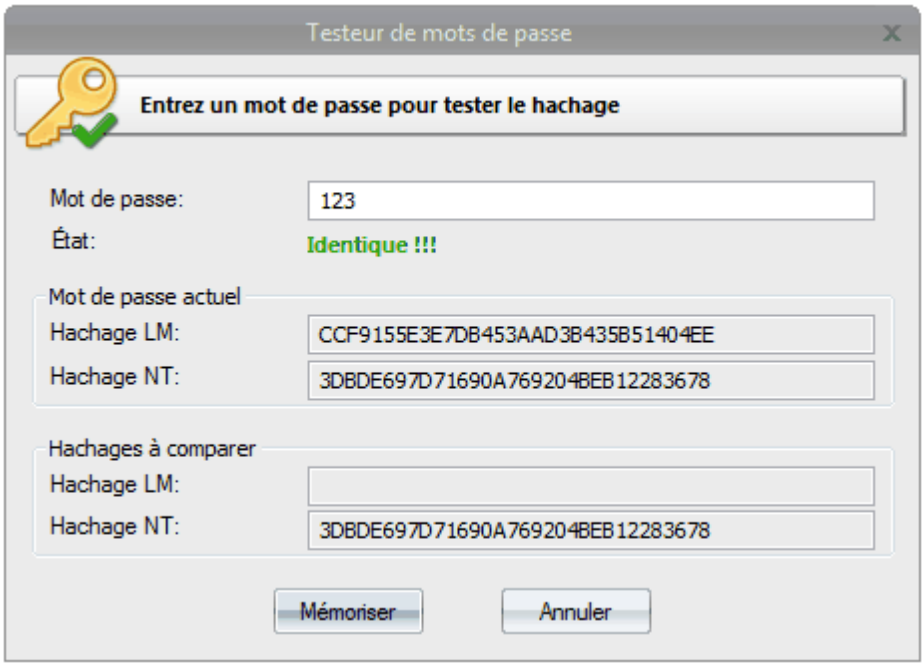
- Saisir le mot de passe dans le champ correspondant.
- Sélectionner le type de hachage: LM ou NT. Notez, que les systèmes d'exploitations avec Windows Vista stockent les mots de passe sous la forme de hachages NT par défaut.
- Sélectionner le type d'ordinateur. "*Cet ordinateur*" indique la vitesse de recherche de votre propre ordinateur.
- Si vous voulez tester la vitesse de votre périphérique GPU, sélectionnez "Cet ordinateur (GPU)" à partir de la liste déroulante "*Matériel*" et cliquez sur le bouton "*Calculer*". Notez que vous pouvez aussi le faire à partir du menu "Rapports".

La qualité de votre mot de passe, en fonction du temps que prendra votre ordinateur pour le "casser", avec

la configuration sélectionnée, sera affichée en dessous.
Par exemple, "casser" un hachage LM d'un mot de passe alphanumérique, prendra à peu près 10 minutes avec un processeur récent (avec une vitesse de recherche de mots de passe supérieure à 100 mln. par secondes). La vitesse de recherche avec un GPU peut dépasser largement cet ordre de grandeur.

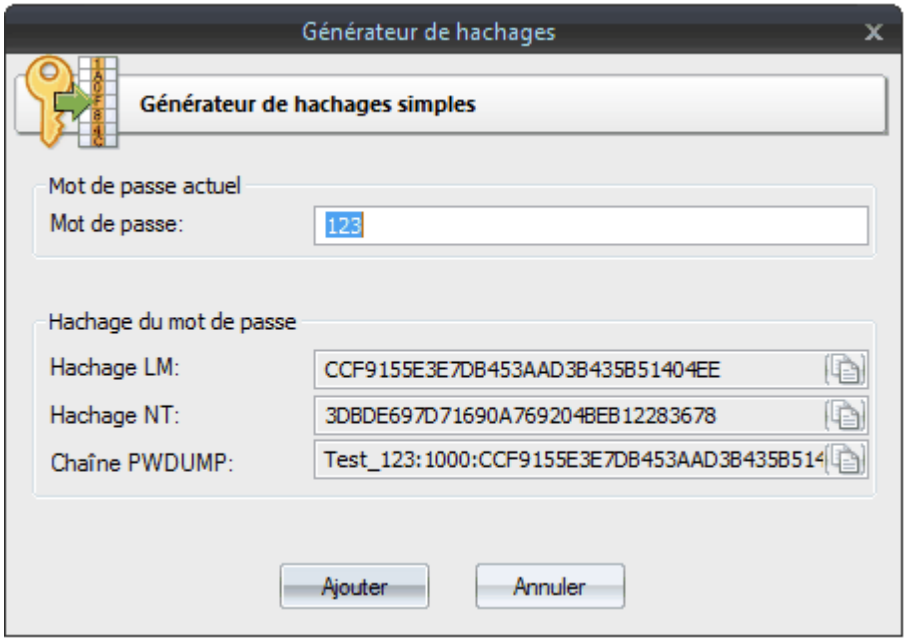
Nous vous remercions par avance, si vous nous faites parvenir les vitesses atteintes par votre PC.

2.6.3 Testeur de mots de passe

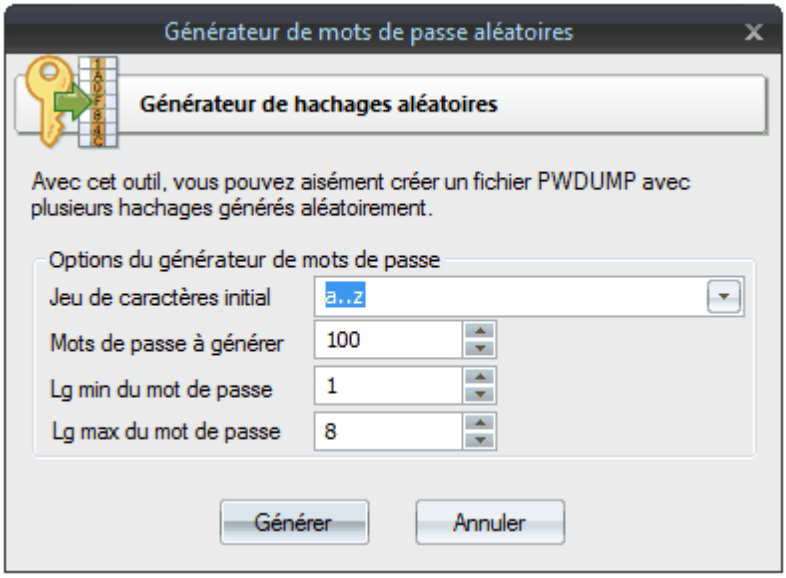


Cet outil permets de tester un mot de passe manuellement un hachage. Cet outil est souvent nécessaire pour valider certains hachages. Par exemple, lorsqu'un hachage LM, pour une ou plusieurs raisons, ne corresponds pas au mot de passe du hachage NT.

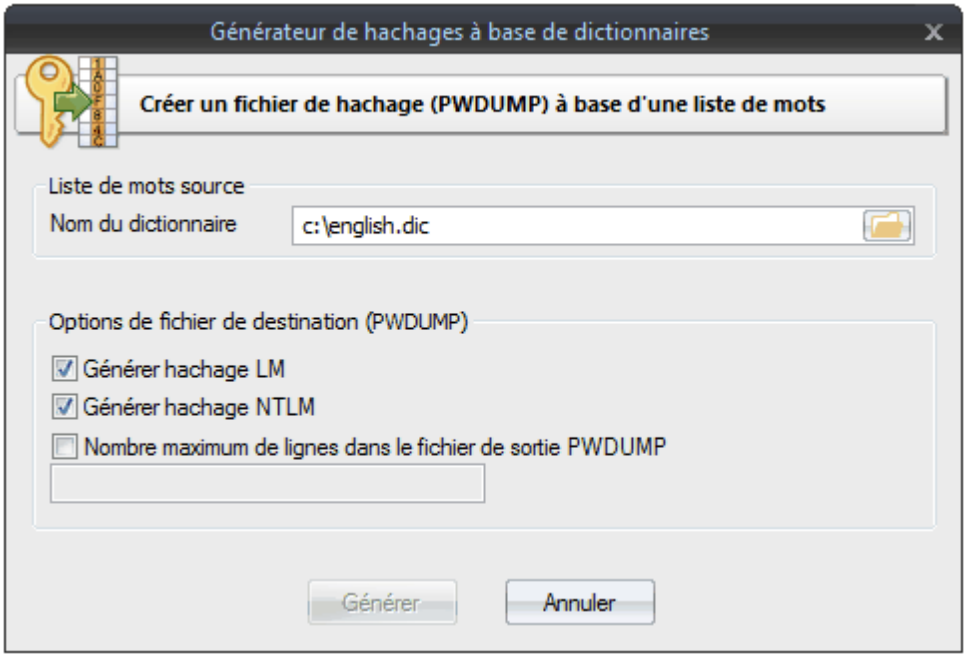
2.6.4 Générateur de hachages



Ce générateur de simple hachage permets de générer rapidement une entrée de test pour un mot de passe spécifique et l'ajouter à la liste des hachages.



Si vous voulez créer un fichier PWDUMP avec un nombre de mots de passe générés aléatoirement, utilisez le générateur de multiples hachages.
Dans la nouvelle fenêtre de dialogue du hachage, entrez la longueur minimum et maximum, la plage de caractères et le nombre total de hachages à générer.

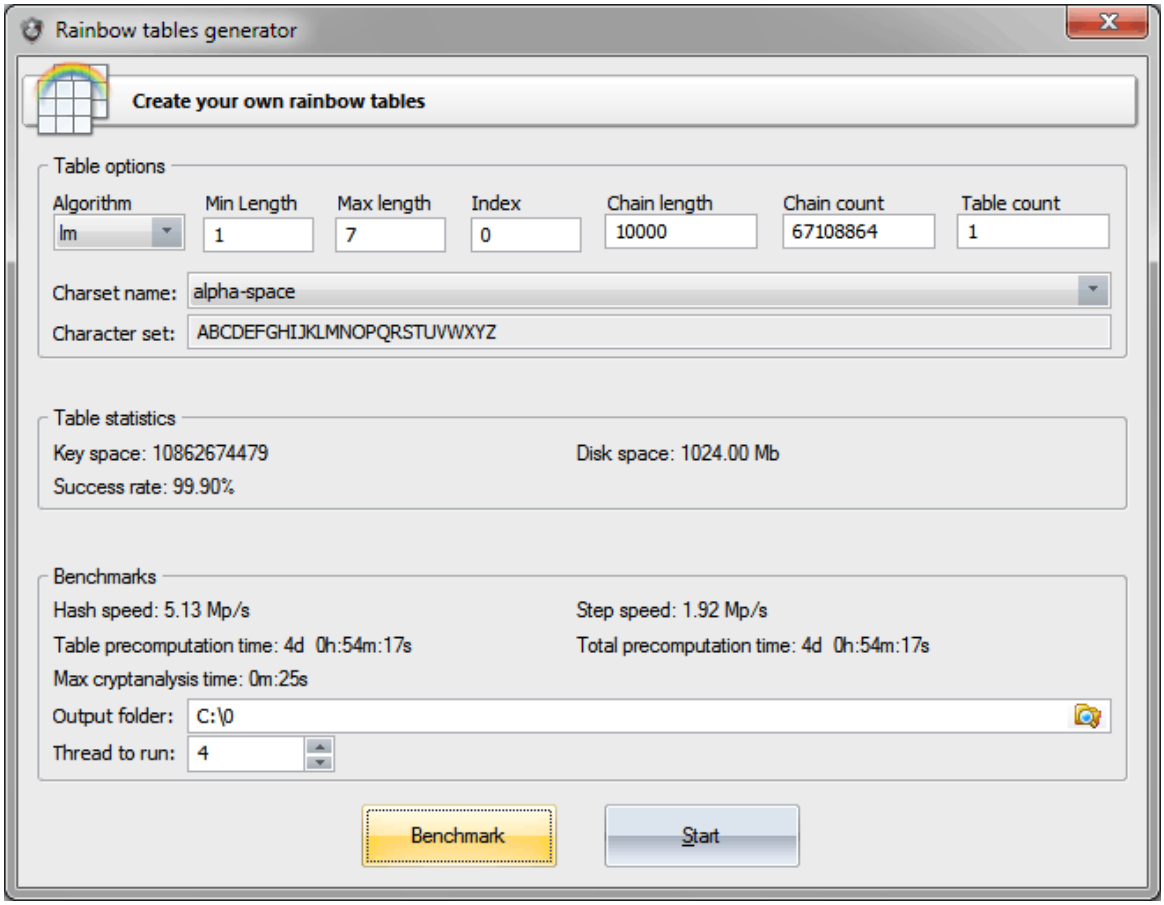


Avec le générateur de hachages à base de dictionnaire, vous pouvez créer facilement un fichier de sortie à partir d'une liste de mots.
Cet outil a des options complémentaires. Par exemple, vous pouvez limiter le nombre de hachages en sortie ou uniquement créer un fichier PWDUMP pour les hachages NTLM.

2.6.5 Générateur de Rainbow Tables

Les rainbow tables sont des tables de recherches spéciales utilisées pour la cryptographie inverse. Les fonctions "One-Way" et les mots de passe sont "crackés" en dérivant à partir des fonctions de hachages. Un exemple de telles tables serait le mot de passe de l'utilisateur (hachages LM ou NTLM) dans l'OS Windows.

Windows Password Recovery possède une recherche implémentée utilisant les rainbow tables. Les tables nécessaires peuvent être téléchargés à partir d'Internet ou être créées manuellement avec l'outil, générateur de rainbow tables.



Avant de démarrer la génération de vos propres tables, il est important de configurer correctement les options et de trouver la meilleure combinaison.
En premier, sélectionnez un des deux algorithmes (LM ou NTLM) dont vous avez besoin et configurez le **nom du jeu** de caractères dont peut être constitué les mots de passe. Plus le jeu de caractères sera grand, plus grand sera le nombre de mots de passe récupérés dans une attaque rainbow. Mais plus long sera le temps pour pré-calculer les tables et, peut-être plus grande sera sa taille.

Les rainbow tables sont utilisées pour récupérer les mots de passe jusqu'à une certaine longueur, définie dans les champs "**Long. min**" et "**Long. max**".
Un hachage dans Windows est constitué de deux moitiés de 7 caractères; cependant la longueur maximum du mot de passe à utiliser lors de la génération des tables LM ne doit pas excéder 7 caractères.

"**Long. de chaînes**" influe sur les paramètres suivant de la table: taux de récupération de mot de passe, temps de génération de la table, et le temps pour récupérer un seul mot de passe avec cette attaque.

"Nbre de chaînes" influe sur le taux de récupération du mot de passe, le temps de génération, et sa taille.

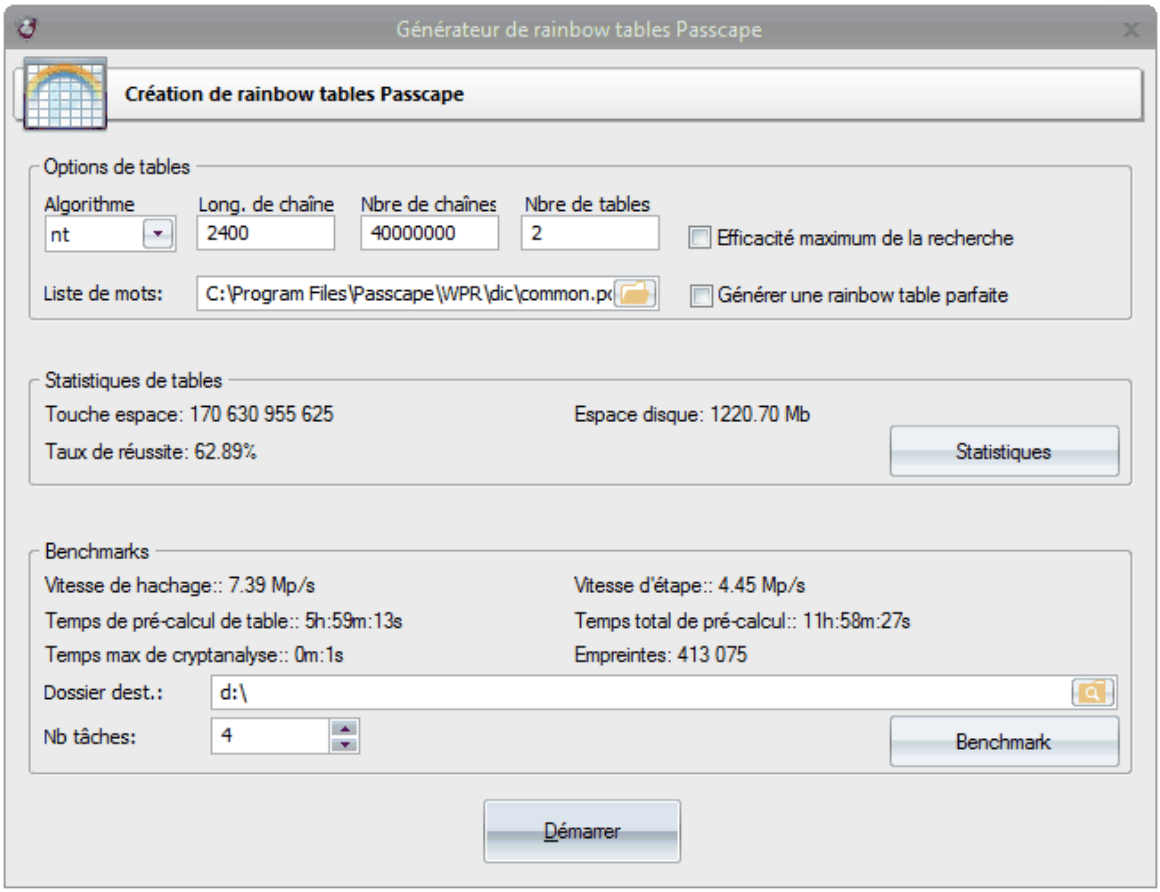
Normalement, Le générateur de Rainbow Tables ne supporte pas les tables d'une taille supérieure à 2 Go; cependant, lors de la création de tables grandes tailles, vous pouvez augmenter son nombre(option "**Nbre de tables**").

La particularité de l'algorithme de recherche à base de rainbow tables réside dans le succès de la récupération qui dépends de plusieurs paramètres, comme le meilleur rapport, en fonction de la taille des tables, le temps pour les générer et le temps maximum pour trouver un mot de passe dans une attaque Rainbow.

L'outil de génération de tables supporte le multi-taches, donc, avant de lancer un pré-calcul, vous devez définir un nombre approprié de cœurs à exécuter pour créer les tables.

2.6.6 Générateur de Rainbow Tables Pascape

Les Rainbow Tables Passcape sont utilisées pour la récupération de mots de passe dans les attaques avec une table Passcape.
Cet outil est utilisé pour créer ce type de tables.



Avant de démarrer la génération de tables, vous devez définir une liste de mots qui doit être utilisée pour la création d'une base de données de mots imprimable et indiquer les paramètres de la table:

- **Long. de chaîne**: influe sur la probabilité de trouver les mots de passe (ex. taux de réussite), le temps de génération de la table et le temps nécessaire pour la recherche d'un seul mot de passe pendant l'attaque.
- **Nbre de chaînes**: influe sur le taux de réussite, le temps de génération de la table et sa taille.

Actuellement, l'outil générateur de table ne supporte pas les tables d'une taille supérieure à 2 Go. Cependant, vous pouvez créer plusieurs tables si vous travaillez avec de très large volumes de données (voir le paramètre "**Nbre de tables**").

Réussir une récupération d'un mot de passe en utilisant des tables dépends de plusieurs facteurs. Et il est important que vous trouviez les meilleurs valeurs en fonction de la taille des tables, influant sur le temps de génération et de cryptanalyse - qui corresponds au temps nécessaire pour récupérer un mot de passe lors d'une attaque.

Deux options complémentaires sont utilisées pour modifier l'efficacité la génération de tables:
- **Efficacité maximum de la recherche**: permets de générer plus de "mots-imprimable" à partir d'une liste de mots comme source en ajoutant des nombres, des claviers et et des combinaisons fréquemment utilisées. Cette option fonctionne très bien avec de petites listes de mots.
- **Générer une Rainbow Table parfaite**: comme vous le savez, les chaînes de mots de passe dans les Rainbow tables peuvent être fusionnées. Cela veut dire qu'il y a des informations inutiles, du temps et de l'espace disque perdu. Cette option, vous permets de créer des tables dites "parfaites" avec aucune chaîne fusionnée. Les tables "parfaites" occupe nettement moins d'espace disque et permettent une

vitesse de récupération un peu plus rapide. Cependant, le prix à payer pour ces avantages est un plus faible taux de récupération de mots de passe. Pour compenser ce faible taux, vous devez au moins, doubler le nombre de chaînes de mots de passe et augmenter le nombre de tables générées.

L'outil de génération de tables supporte le multi-taches, donc assurez vous d'avoir défini le nombre nécessaire de cœurs à exécuter par le programme avant de démarrer le processus de génération de tables.

2.6.7 Outils de listes de mots

Face au peu d'outils pour travailler avec des dictionnaires spécifiques de mots de passe, cela a inspiré les développeurs pour créer leur propre jeu d'outils.

Avec ce kit d'outils, vous pouvez facilement créer de nouvelles listes de mots ou les éditer, tout comme les utiliser avec toutes les applications de récupération de mots de passe.

2.6.7.1 Créer une nouvelle liste de mots en indexant des fichiers

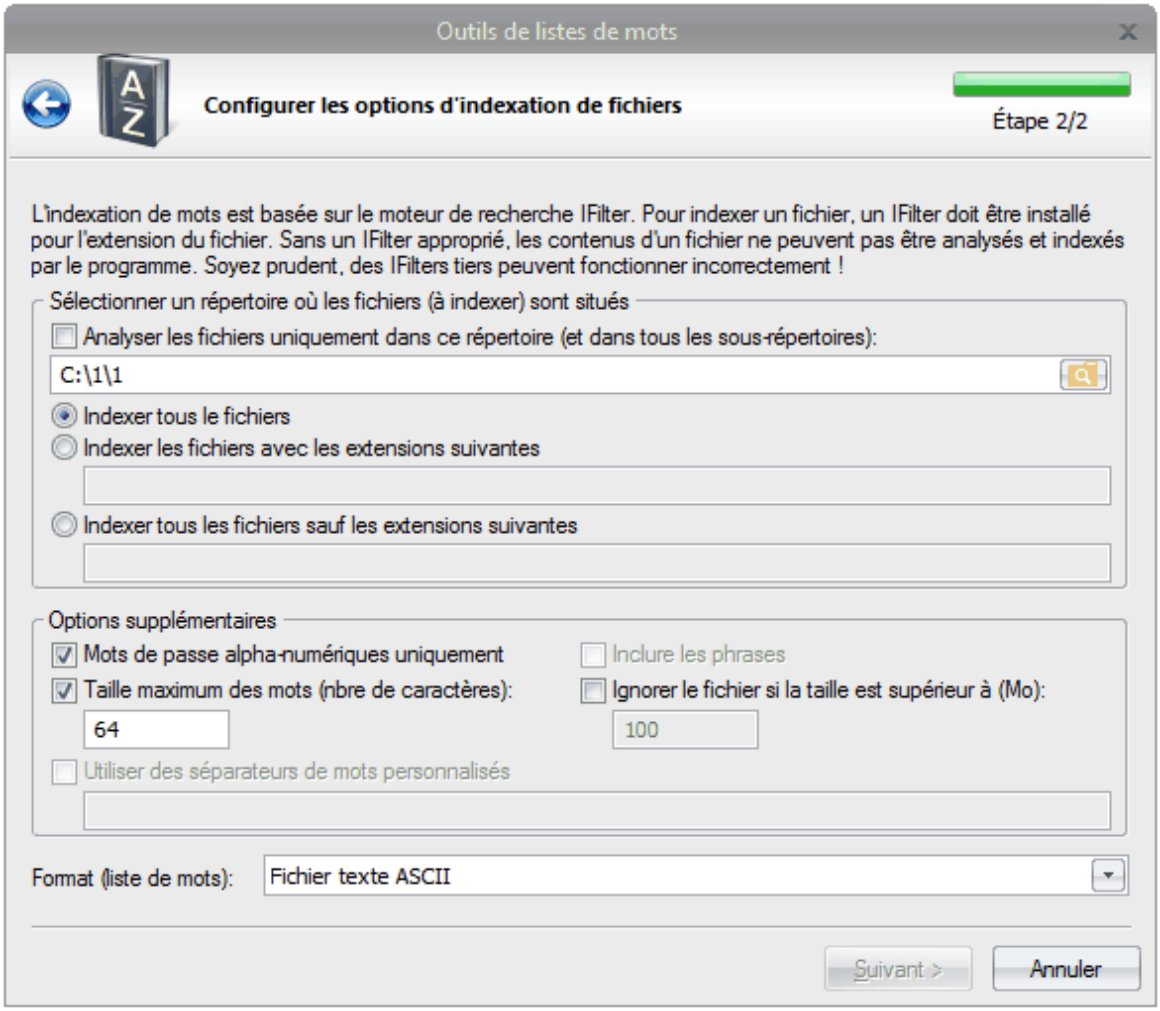
Ce outil est conçu pour créer une nouvelle liste de mots en sélectionnant (indexant) des mots de fichiers locaux de votre ordinateur. Par exemple, les fichiers peuvent de types: *.html, *.xml, *.txt, *.doc, *.mdb, *.pdf, *.exe, etc.

L'indexation est basée sur la technologie **IFilter** (consulter l'article Ifilter sur Wikipedia pour en savoir plus). Cette idée de technologie, a été développé par Microsoft, permettant l'indexation de textes de tous les fichiers, à partir du moment que le plugin approprié soit installé.
De cette façon, vous pouvez accéder au texte contenu, par exemple, dans les fichiers *.exe ou *.dll, base de données de logiciels d'e-mails, etc.

En dépit du fait, que le nombre de plugins IFIlter, gratuit ou payant, peuvent être trouvés sur Internet, Windows Password Recovery supporte en interne les types de fichiers suivants:
- Archive: *.zip, *,cab, *.rar
- Programme: *.exe, *.dll, *,cpl, *.ocx, *.sys, *.scr, *.drv
- Texte: *.txt, *.dic
- Internet: *.html, *.htm

Ce qui veut dire, que les fichiers avec ces extensions, peuvent être analysés par le programme sans qu'un plugin IFilter soit installé sur l'ordinateur.

Windows 7 possède un outil interne "Windows Desktop Search", qui possède une grande variété de filtres supportant la majorité des documents les plus populaire. Dans les autres systèmes d'exploitations, Windows Desktop Search peut être installés manuellement; le fichier d'installation peut être téléchargé à partir du site officiel de Microsoft.



Les options de configuration pour cet outil sont divisées en deux groupes. Dans le premier groupe, vous pouvez configurer le répertoire source, où sont situés les fichiers à indexer, et sélectionner une méthode d'analyse, suivante:

- Analyse de fichiers uniquement dans un répertoire sélectionné. Si cette option n'est pas définie, le programme analysera récursivement, tous les sous-répertoires et les fichiers qui y sont contenus.
- Indexe tous les fichiers.
- Indexe les fichiers avec, seulement, certaines extensions.
- Indexe tous les fichiers exceptés certaines extensions.

Les extensions de fichiers doivent être saisis sans le point et être séparées par une virgule. Exemple: txt,dic,xml,chm,htm.

Le groupe d'options complémentaires permets de personnaliser, les méthodes de recherches de fichiers, suivantes:

- Accepte uniquement les mots de passe alpha-numériques. Si cette option est activée, elle ignorera tous les caractères spéciaux. Seulement les mots de passe alpha-numériques seront traités.
- Inclus les phrases. Cette option permets, également, de mettre des phrases dans la liste de mots de destination. Une phrase sera considérée comme une chaîne de caractères (jusqu'à 256 symboles), incluant au moins, un espace (caractère).
- Taille limite maximum pour un mot. Il est toujours recommandé de définir cette option. La longueur maximum optimale pour un mot dans une liste de mots est entre 16 et 64 caractères. Réduire la longueur maximum accélère, quelquefois, radicalement, la vitesse de recherche de fichiers.Il faut rappeler, pour mémoire, que la longueur maximum permise pour un mot de passe dans Windows, est de 128 caractères.
- Sautés les fichiers ayant une taille supérieure à celle spécifiée. Certains IFilters prennent

beaucoup temps pour analyser les fichiers de tailles importantes; ce qui peut amener le programme à se figer et ne plus répondre.

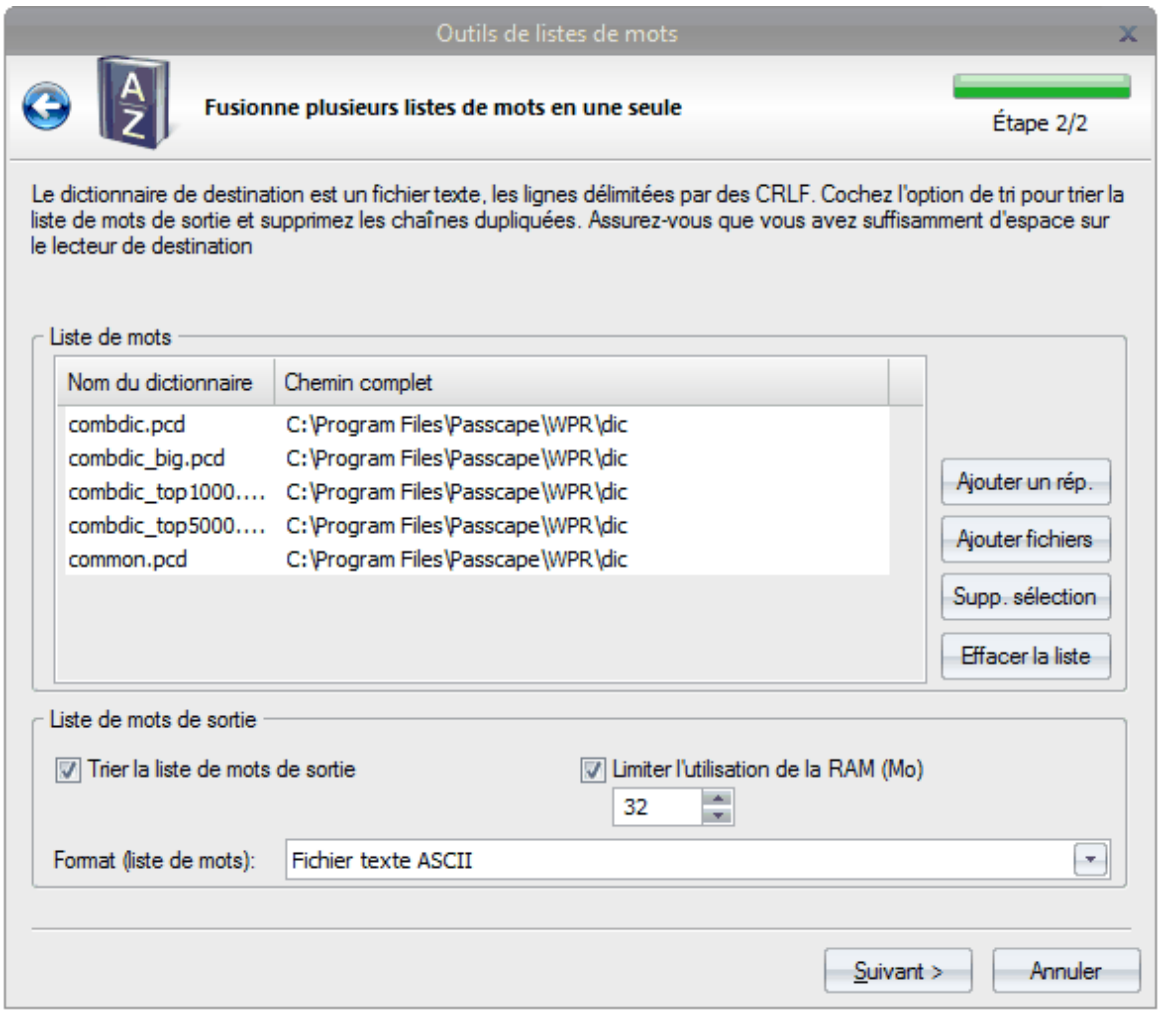
- Utiliser des séparateurs de mots personnalisés. Vous pouvez définir vos propres séparateurs lors de l'analyse de fichiers. Par exemple, vous pouvez utilisez des caractères tels que: !"#$%&'()*+,-./:;<=>?@{}[]_ et bien sûr, un espace.

Cliquez sur le bouton **Suivant>** exécute l'indexation sélectionnée, qui peut prendre énormément de temps. Pour bien améliorer la vitesse d'exécution, la liste des mots trouvés durant l'indexation est créée et conservée dans la mémoire de l'ordinateur; ce qui nécessite des ressources suffisantes. Donc, si vous avez une erreur de routine suite à un manque de mémoire, essayez de réduire la longueur maximum des mots ou limitez le nombre de fichiers qui doivent être analysés et essayez d'exécuter à nouveau l'indexation. Une fois, cette opération terminée, et que les les mots trouvés ont été enregistré sur le disque dur, soit triés pour obtenir une liste de mots pertinente. Les mots trouvés sont garantis d'être unique et de ne pas contenir de doublons.

Attention, certains filtres tiers peuvent ne pas fonctionner correctement et créer un blocage, un "gel" ou une fin anormale de l'application. Par exemple, certains filtres d'analyse de fichiers PDF dans Windows XP sont connus pour générer des erreurs.

2.6.7.2 Fusionner des listes de mots

Cet outil de fusion de listes de mots est utilisé lorsque vous avez besoin de combiner deux ou plusieurs listes de mots en une seule.



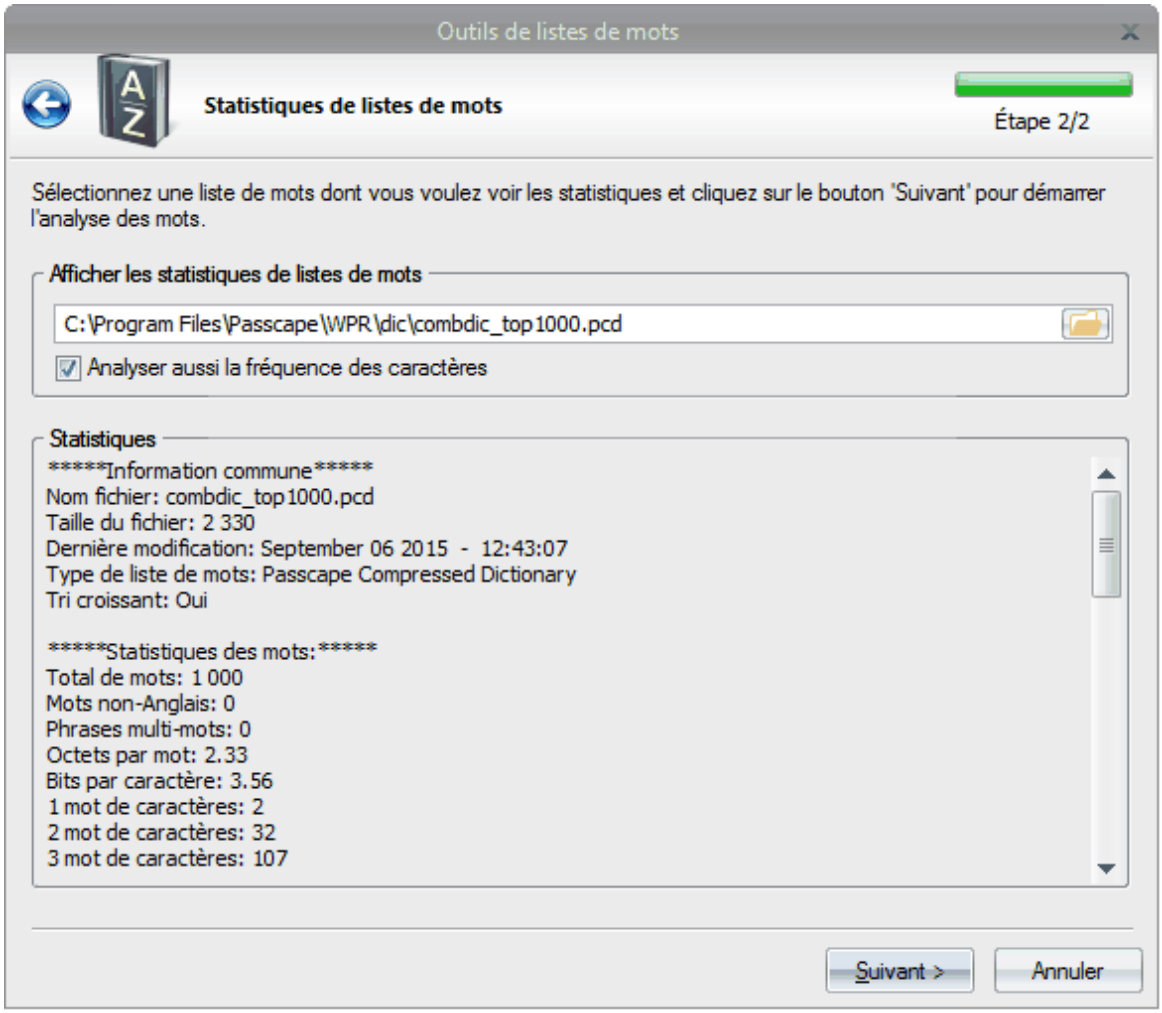
Si l'option "**Trier la liste de mots de sortie**" n'est pas cochée, la fusion des nouveaux mots se fera

par le simple ajout à la liste, sans tri ou vérification des doublons. Dans la pratique, il est plus courant de fusionner avec un tri; ce qui permets d'avoir une liste avec tous les mots triés dans l'ordre alphabétique et sans doublon.

Le tri peut prendre énormément de mémoire; toutefois, il est recommandé de limiter la quantité de mémoire qui peut être utilisé (malgré la légère réduction de la vitesse d'exécution que cela engendre).

2.6.7.3 Statistiques de listes de mots

L'analyseur de listes de mots collecte et affiche les statistiques suivants:



Informations communes:
- Nom du dictionnaire
- Taille en octets
- Type du fichier
- Date et heure de la dernière modification
- Tri alphabétique ou non (la vérification est faite uniquement si le fichier est trié de façon croissante)

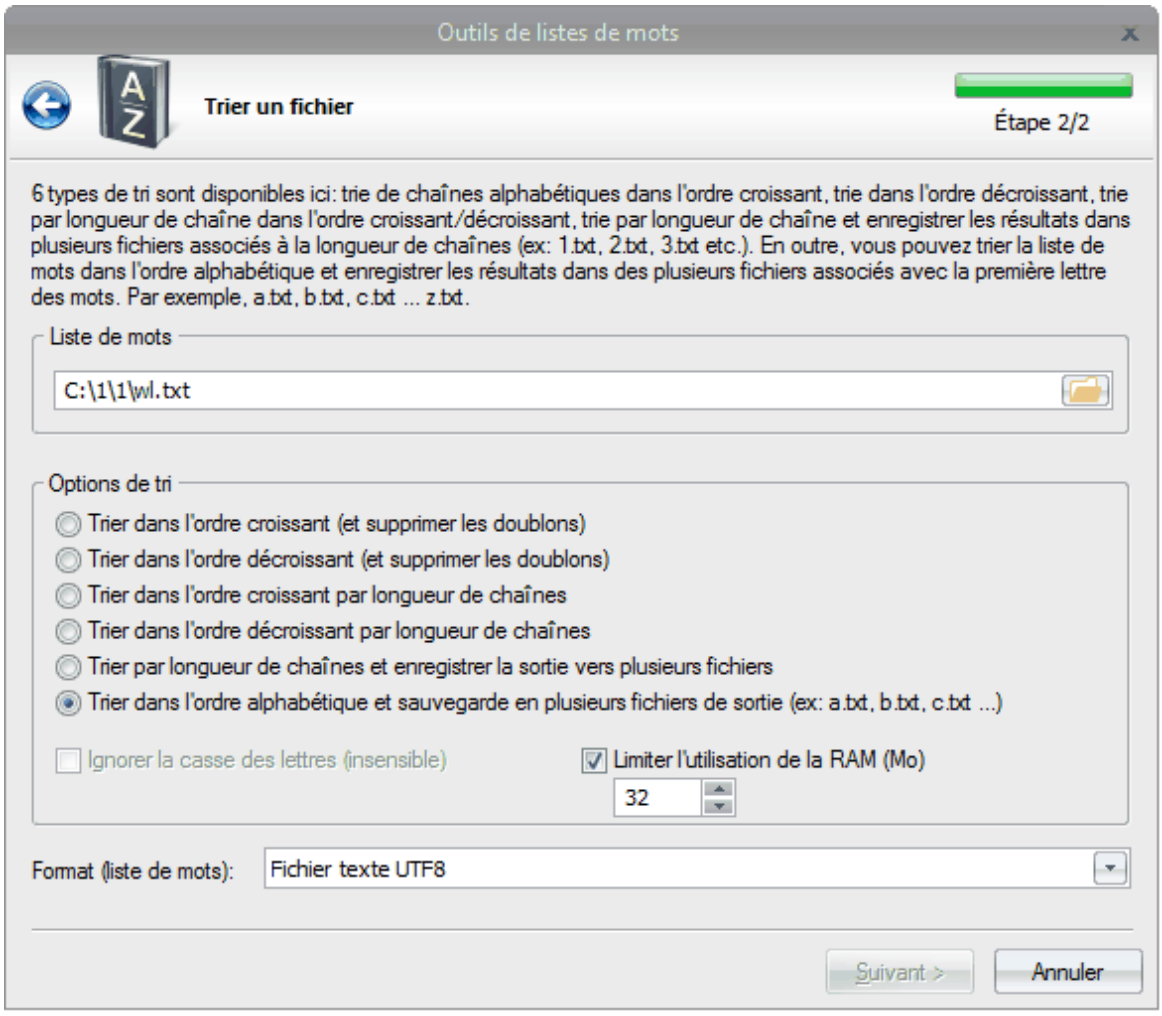
Statistiques de mots:
- Total de mots
- Mots non-Anglais
- Phrases multi-mots, par ex, les mots séparés par un espace.
- Octets par mot, moins les séparateurs de mots. Affiche le taux de compression moyen de la liste de mots.
- Bits par caractère. Affiche le taux réel de compression de la liste de mots. Par exemple, en UNICODE, la valeur des bits par caractère tend vers 16 (excluant les séparateurs de mots), pour les listes de mots

classique en ASCII - vers 8. Dans certaines listes de mots PCD compressées, une lettre peut être codée par moins d'un bit.
- Statistiques de mots - nombre de mots constitués de 1, 2, 3, etc. caractères.

Analyse de la fréquence des caractères (si l'option correspondante est cochée)
- Indique la fréquence d'utilisation d'un caractère, en particulier, dans la liste de mots.

2.6.7.4 Tri d'une liste de mots

Cet ensemble d'outils offre 6 modes de tri de listes de mots: 4 parmi eux sont communs, et 2 sont étendus. Les modes communs de tri inclus le tri de liste de mots dans l'ordre alphabétique (croissant et décroissant) et par longueur des mots. Lors du tri alphabétique ou par longueur des mots, le programme supprime automatiquement les mots en doubles.



En complément, vous pouvez trier une liste de mots par longueur et enregistrer les résultats dans plusieurs fichiers, associé à la longueur des mots. Par exemple, le fichier 1.txt contiendra les mots de 1 caractère, 2.txt - deux caractères, etc.

Le sixième mode de tri fonctionne de façon similaire. En même temps, le programme trie la liste source de mots dans l'ordre alphabétique et crée plusieurs listes de mots cibles qui correspondent à la première lettre du mot. Par exemple, tous les mots commençants par la lettre A sont enregistrer dans un fichier A.txt, les mots commençants par B - dans B.txt, etc.
Vous devez gardez en mémoire que certains mots peuvent commencer par des caractères qui ne peuvent pas être utilisés pour un nom de fichier. Dans ce cas, le programme proposera un nom de remplacement, par l'affichage d'un message d'avertissement.

Si l'option "**Ignorer la casse**" est cochée, le tri est sans tenir compte de la casse des lettres; par ex., les mots *bad*, *Bad* or *BAD* sont considérés comme identiques, avec toutes les conséquences qui en découlent.

Le nom de destination de la liste de mots peut être le même que la source, cependant, cela n'est pas recommandé.

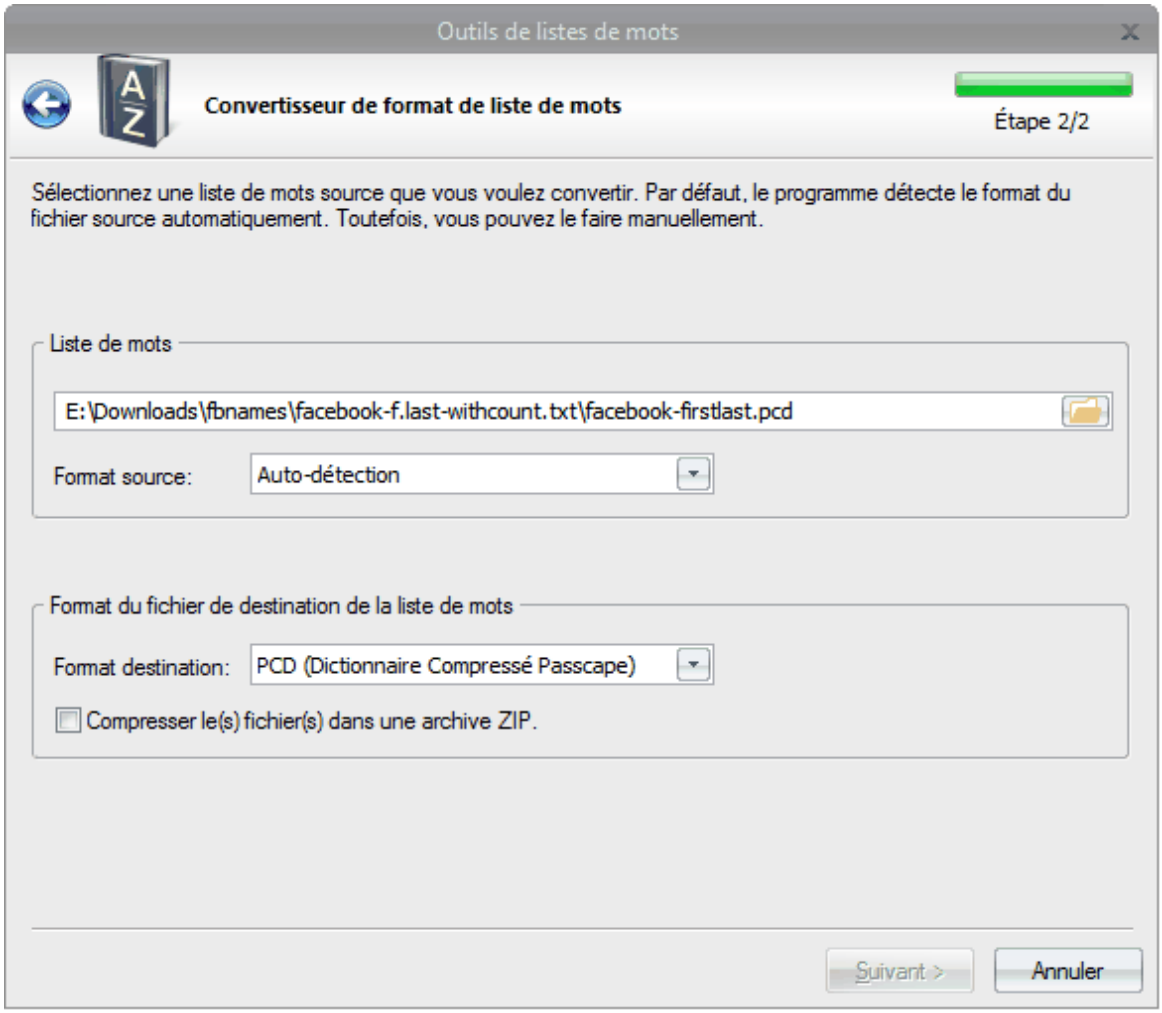
Le tri de fichiers importants (supporte les fichiers supérieurs à 4Go) requière une utilisation importante de RAM; sachant que le nombre peut être limité par l'option correspondante. Pour les fichiers importants, il n'est pas recommandé de définir la mémoire minimum, en dessous de 16Mo, comme cela affecte la vitesse de tri.

Pendant le tri, le programme peut créer accessoirement, des fichiers dans le répertoire temporaire de l'application. Assurez-vous que le disque du répertoire temporaire contient suffisamment de place pour les fichiers d'échanges (swap).

2.6.7.5 Convertir/compresser une liste de mots

Un grand nombre de listes de mots peuvent être trouvées sur Internet qui sont divisées en trois formats principaux: **ASCII**, **UTF16** (Unicode) et **UTF8**. Avec cet outil, vous pouvez convertir une liste de mots d'un format en un autre et en option comprimer les listes de mots en fichiers ZIP. Derrière ces trois formats, mentionnés précédemment, le programme supporte son propre format: **PCD** (Passcape Compressed Dictionnary), lequel, dans la majorité des cas, apporte un meilleur gain de taille comparé à un fichier d'archive ZIP.

Créer de larges fichiers PCD peut prendre énormément de temps !



L'interface utilisateur de cet outil est très conviviale. Dans la partie supérieure, sélectionnez la liste de mots source et son format. Par défaut, le programme détecte le format de fichiers automatiquement, mais vous pouvez aussi le choisir manuellement.

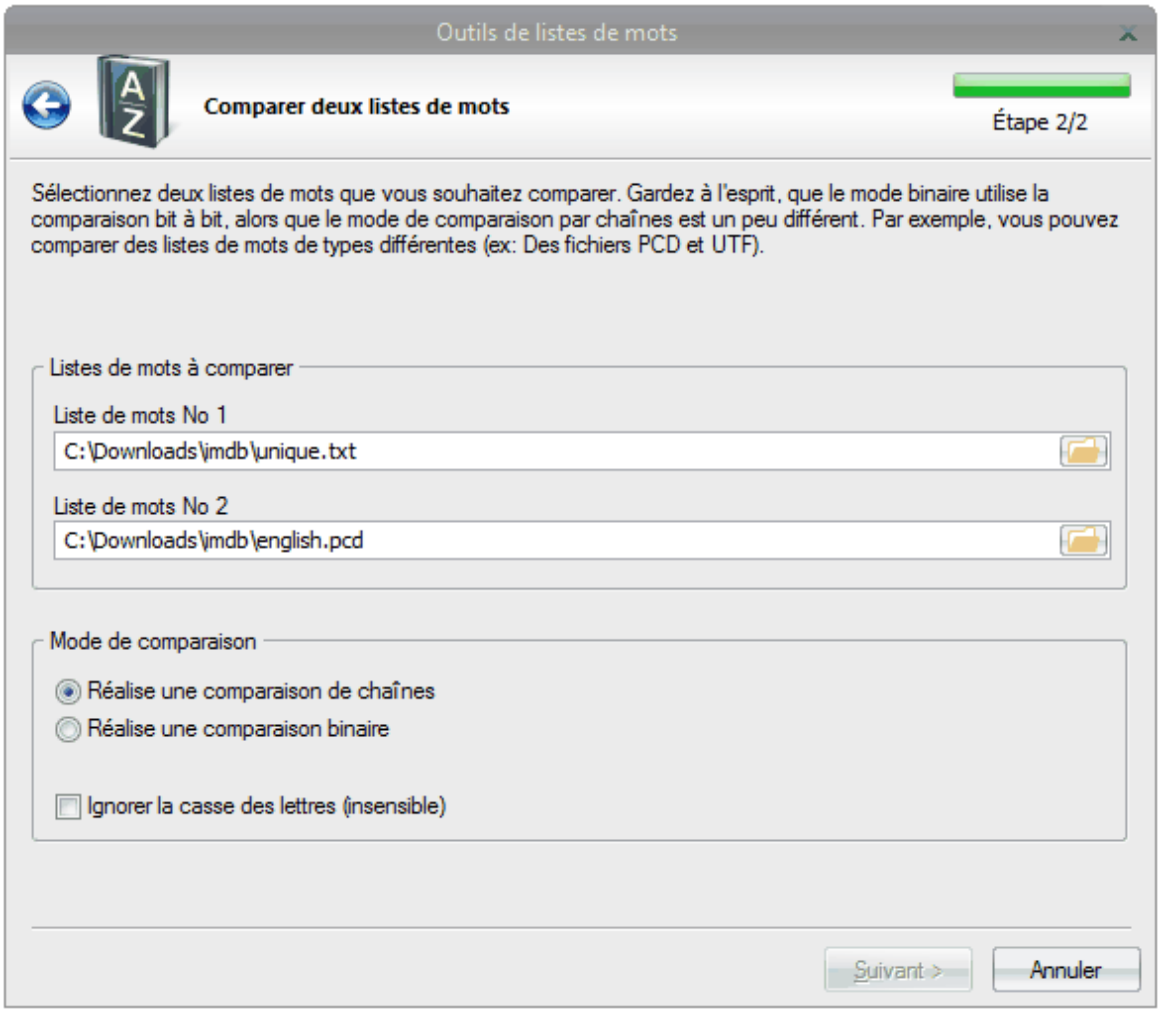
Alors que le format PCD peut être facilement reconnu, avec les fichiers texte ce n'est pas le cas. En règle générale, les fichiers/listes de mots en UTF16 ou UTF8 qui commencent avec un marqueur de deux- ou trois-bits représentent le type du fichier. Cependant, il y a des listes de mots Unicode qui n'ont pas de marqueurs d'identifications. Pour certains cas "difficiles", vous devez définir le type de fichier source manuellement. Sinon, le programme sera incapable de voir l'identificateur approprié, reconnaissant le fichier incorrectement comme de type ASCII.

La liste de mots de destination, est définie avec un des quatre formats mentionnés précédemment. Lorsque l'option de compression est cochée, le programme en complément, comprime le fichier dans une archive ZIP.

Le nom de la liste de mots de destination peut être le même que celui source; cependant, cela n'est pas recommandé.

2.6.7.6 Comparer des listes de mots

Parfois, il est nécessaire de savoir si deux listes de mots sont identiques. Cet outil de comparaison de listes de mots est conçu à cet effet.

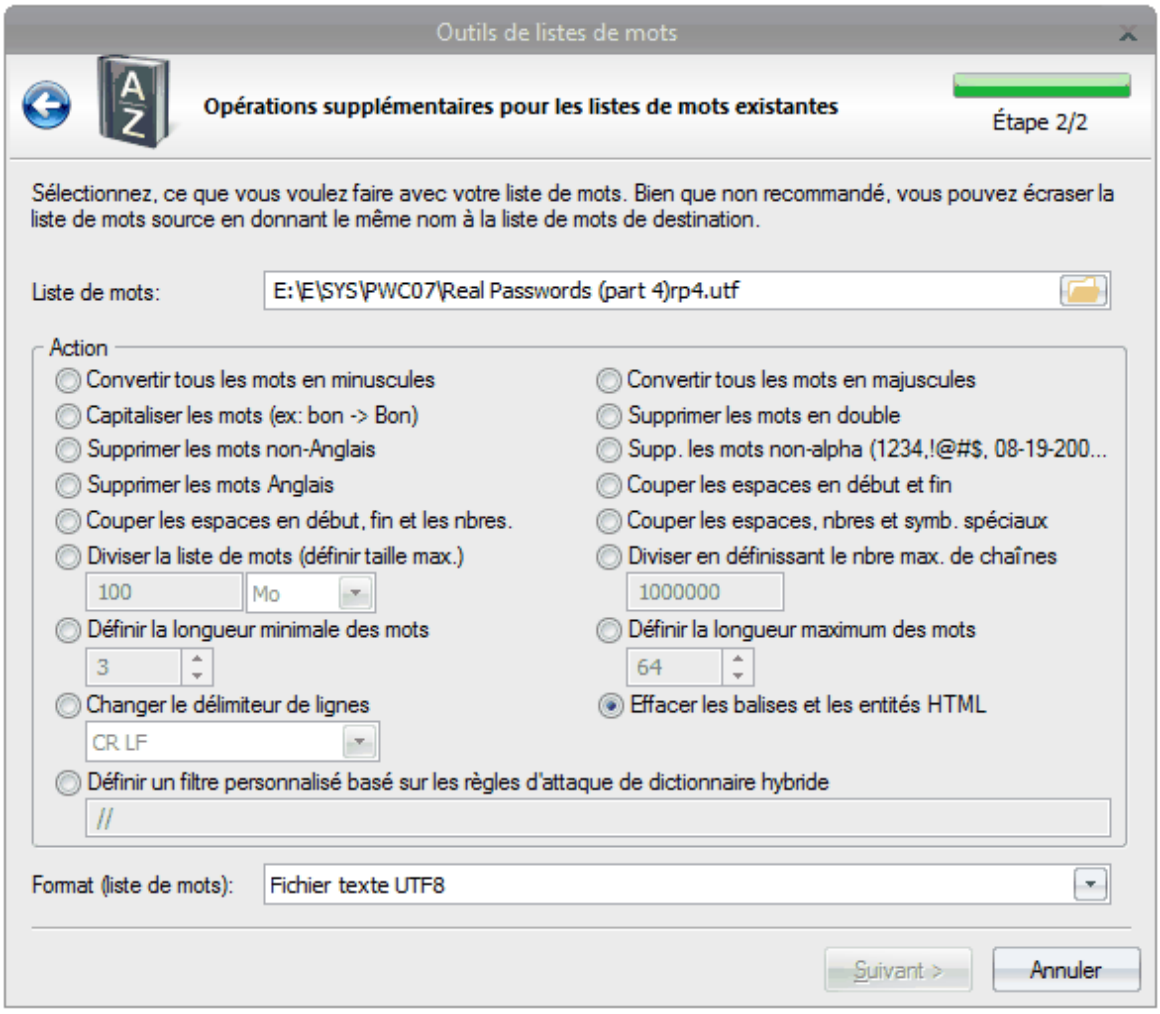


Cet outil possède deux modes de fonctionnement:
1. Comparaison binaire, pour la comparaison de fichiers bit à bit.
2. Comparaison de chaînes, qui compare les mots au lieu des bits. Ce mode est remarquable pour sa capacité à comparer des listes de mots de différents formats. Par exemple, PCD et UNICODE, ou UNICODE et ASCII.

Si la case "**Ignorer la casse**" est cochée (uniquement, pour le mode de comparaison de chaînes), par exemple, les mots *bad* et *Bad* seront considérés comme identiques.

2.6.7.7 Opérations complémentaires

Ces outils complémentaires sont conçus principalement pour éditer et ajuster les listes de mots déjà existantes.



Les outils inclus les actions suivantes:
- Convertir tous les mots en minuscule. Par exemple, BAD -> bad.
- Convertir tous les mots en majuscule. Par exemple, Bad -> BAD.
- Capitaliser les mots - majuscule pour la première lettre, minuscule pour les autres. Par exemple, bad -> Bad.
- Supprimer les mots en doublons.
- Supprimer les mots non-Anglais.
- Supprimer les mots qui sont entièrement constitués de nombres et/ou de caractères spéciaux. Par exemple, 12345, !@#$%, 08-19-10, etc.
- Supprimer les mots Anglais.
- Couper/supprimer les espaces en début et fin.
- Couper/supprimer les espaces en début, fin et les nombres.

- Couper/Supprimer les espaces en début, fin, les nombres et les caractères spéciaux.
- Diviser la liste de mots en morceaux de tailles maximum.
- Diviser la liste de mots en morceaux d'un nombre maximum de chaînes.
- Supprimer les mots dont la longueur est plus petite que celle spécifiée.
- Supprimer les mots dont la longueur est plus grande que celle spécifiée.
- Changer le délimiteur de lignes.
- Nettoie les balises HTML. Cet outil converti également les entités HTML dans un format lisible. Par exemple, **&** -> **&**, **@** -> @
- Défini votre propre filtre basé sur les règles du Dictionnaire Hybride.

Comme liste de mots source, le programme accepte les fichiers ASCII, UTF16, UTF8 et PCD.

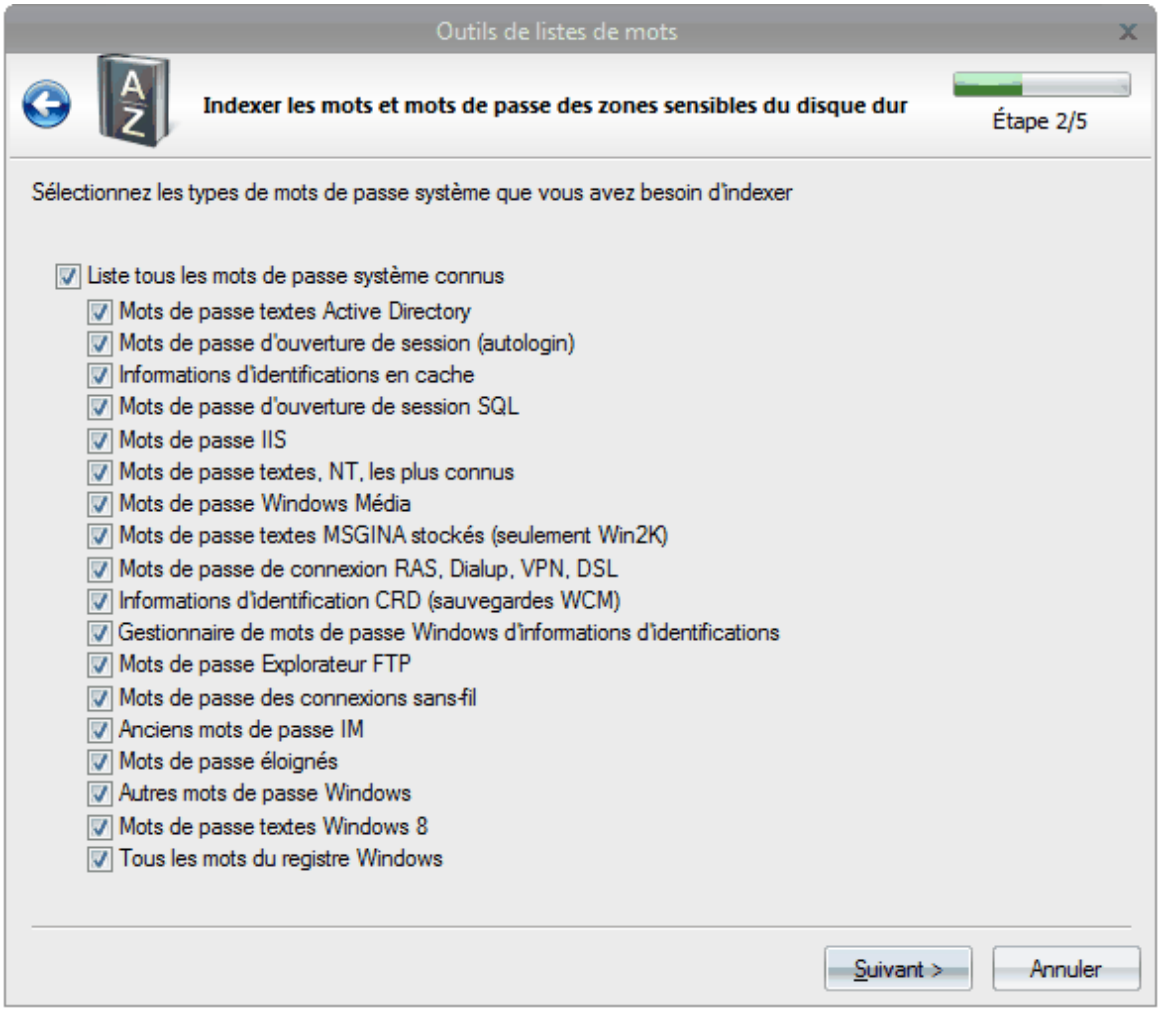
Le nom de la liste de mots source et de destination peut être identique (cela n'est pas recommandé). Dans ce cas, la liste de mots source sera remplacée par celle de destination (écrasée), lors de l'enregistrement sur le disque.

2.6.7.8 Indexer des zones sensibles du disque dur

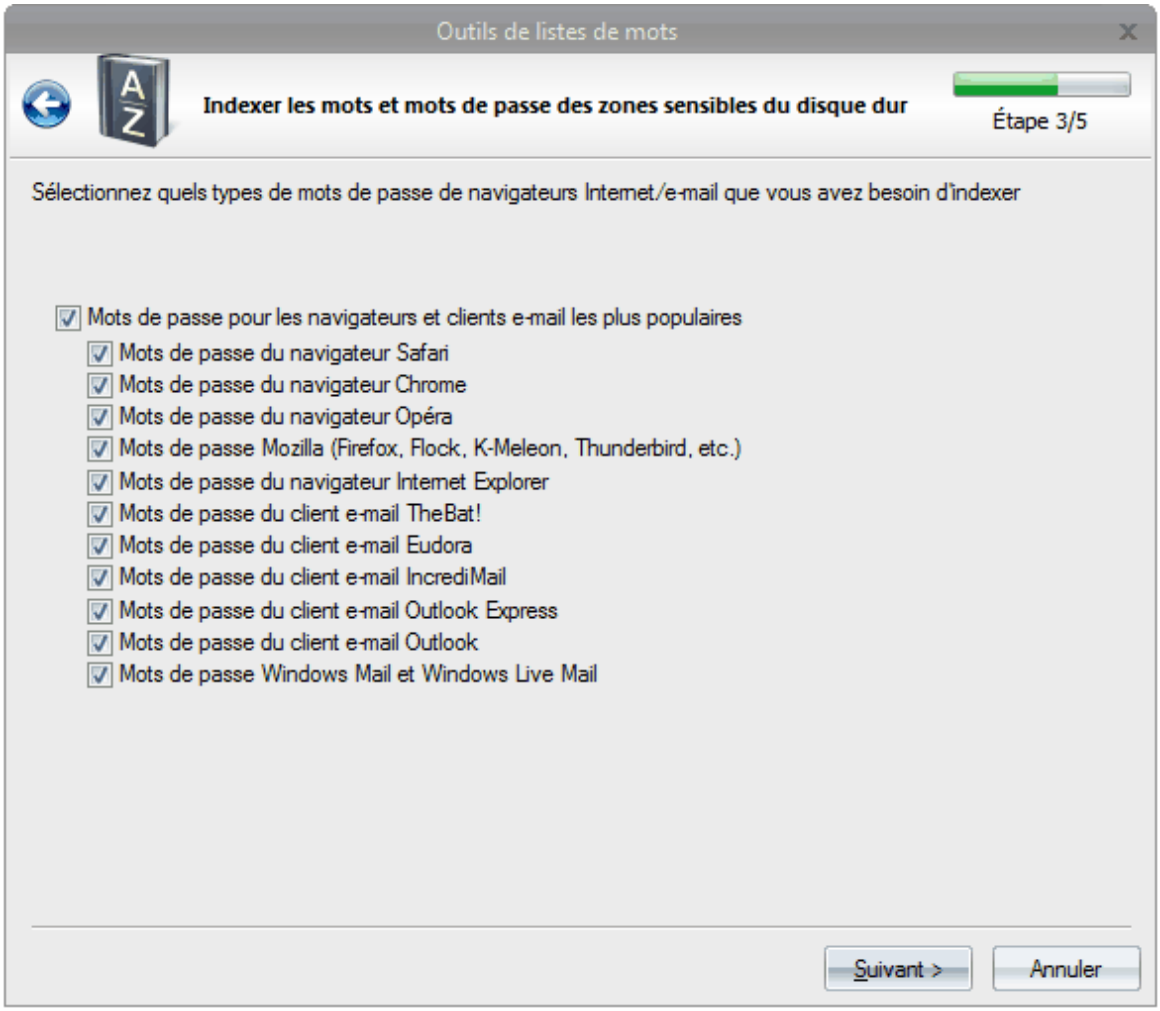
La création d'une liste de mots en indexant le disque dur (suivi par une attaque utilisant cette liste de mots) est très utile et est un outil sophistiqué pour décrypter les mots de passe des comptes locaux de Windows.

Couramment, les utilisateurs, attribuent le même mot de passe pour leurs comptes Windows, Web, ICQ, etc. L'idée de cet outil est de créer une liste de mots avec tous les mots de passe déjà utilisés, messages d'utilisateurs. Les mots provenant des anciens fichiers ouverts, etc. et ensuite d'utiliser cette liste de mots accumulées pour la recherche des mots de passe des comptes locaux. Cette technique est utilisée dans l'attaque par Intelligence Artificielle.

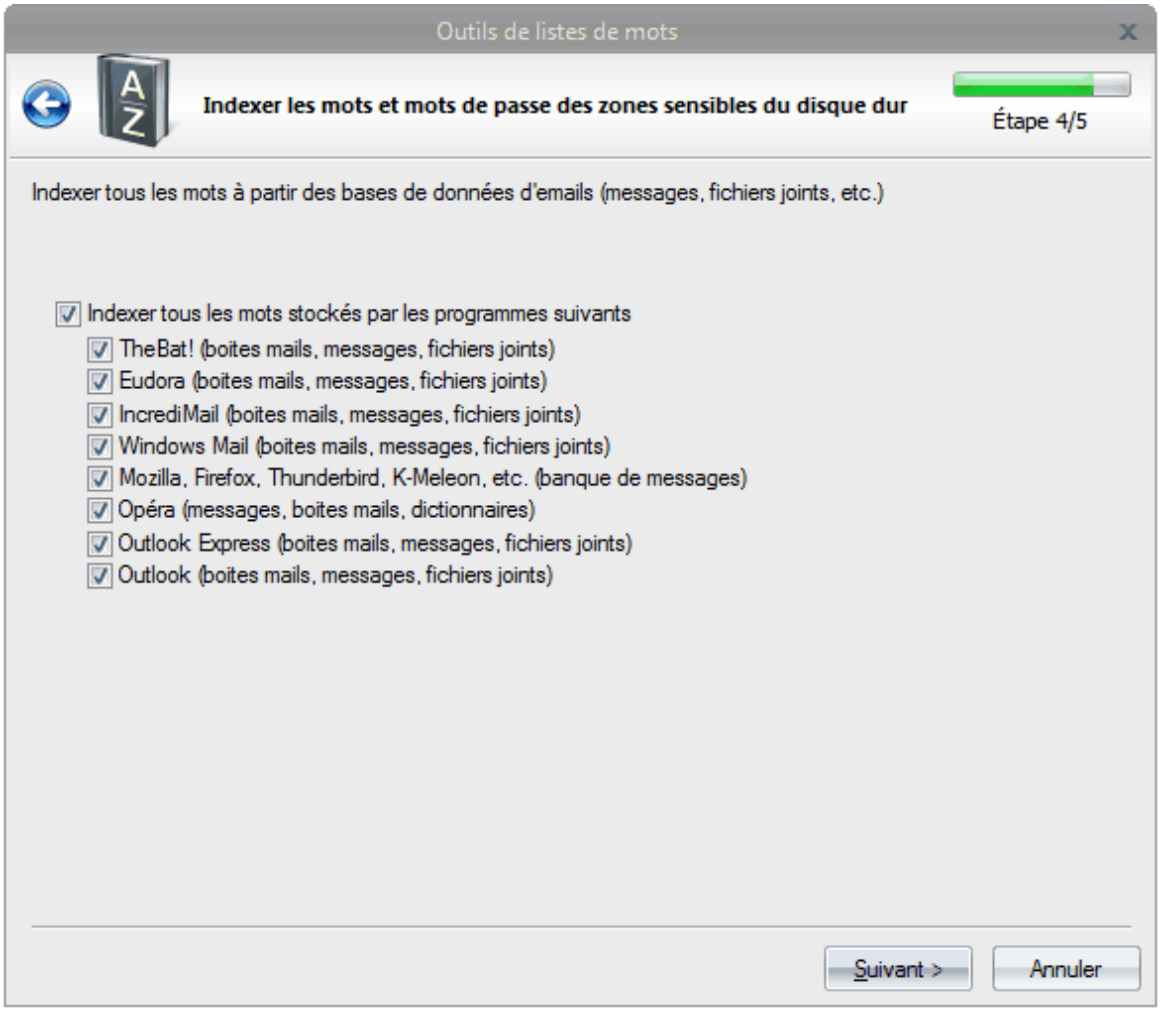
La configuration de cet outil est constituée, classiquement, de quatre parties (étapes):



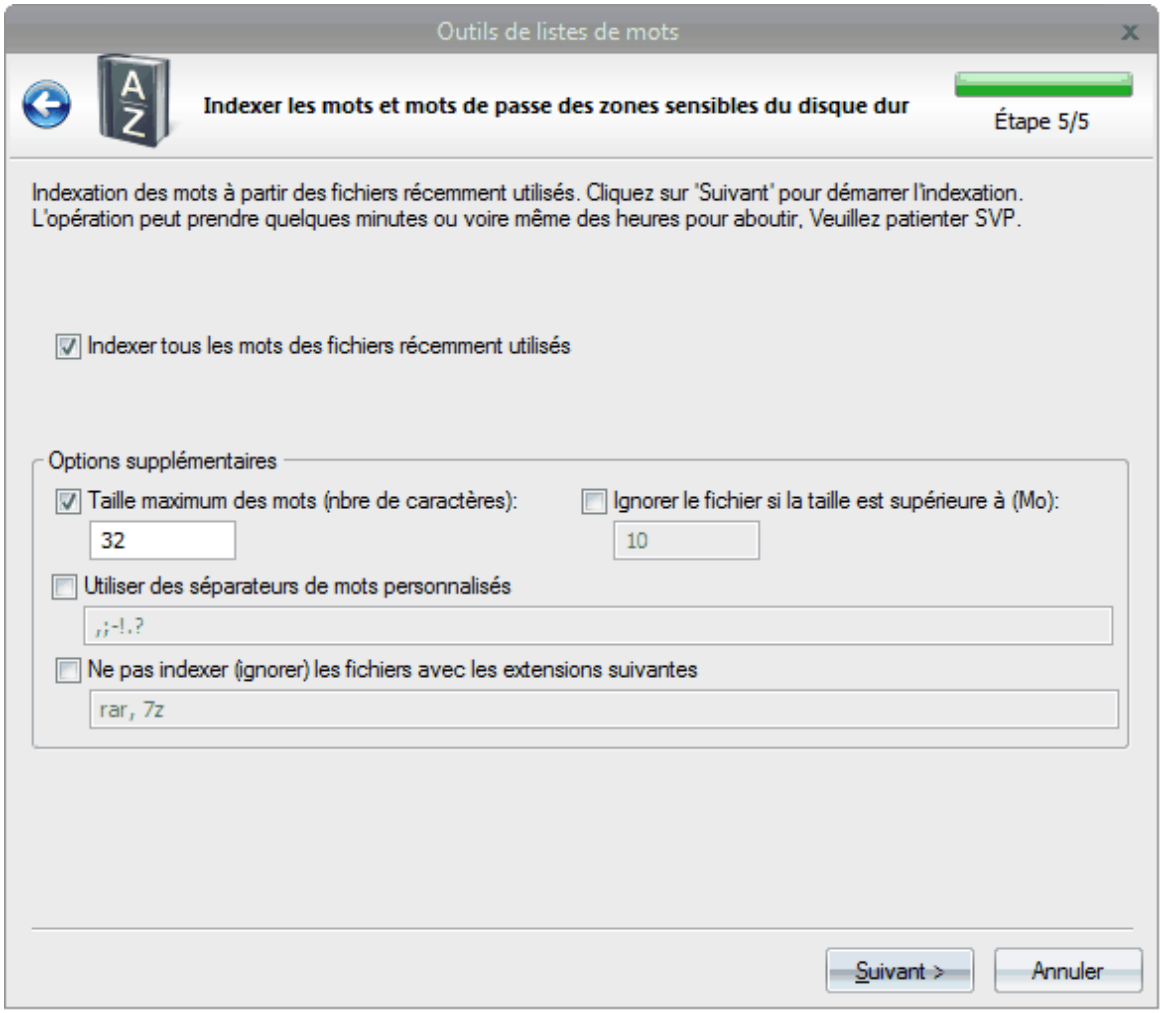
Premièrement, sélectionner les modules système qui doivent être utilisés lors de la génération de la liste de mots. Ces modules recherchent et indexent les types de mots de passe suivants du disque dur de votre ordinateur: Les mots de passe en clair de l'Active Directory, les mots de passe de démarrage, les mots de passe du cache de démarrage, SQL, IIS, Windows Media, les mots de passe texte Win2K, RAS, Dialup, VPN, DSL, WEP, WPA, les mots de passe de connexions FTP, les mots de passe du gestionnaire de d'identifications Windows (Windows Credential Manager), Instant Messengers, et les autres mots de passe.



Dans la seconde partie de configuration, sélectionnez les navigateurs et les clients e-mail, à partir desquels les mots de passe doivent être trouvés et être ajoutés à la liste des mots qui va être créée.
Le programme supporte la majorité des navigateurs Web suivants: Safari, Chrome, Opera, navigateurs basé sur Mozilla (Firefox, K-Meleon, Flock, etc.), Internet Explorer.
Les clients e-mail suivants: TheBat!, Eudora, IncrediMail, Outlook Express, Outlook, Windows Mail, et Windows Live Mail.



Hormis les mots de passe collectés, le programme peut indexer les conversations d'utilisateurs par e-mails, en scannant toutes les boîtes d'e-mails trouvées, messages, fichiers joints, etc. La recherche est réalisée sur tout le disque dur, pour tous les comptes du système, du coup le processus peut prendre un temps considérable, spécialement lorsqu'il contient beaucoup d'utilisateurs ou quand les bases de données des clients d'e-mails sont importantes. En fonction de vos besoins, vous pouvez activer/ désactiver chaque module individuellement.



Finalement, dans le dernier dialogue, vous définir les options pour indexer les mots de tous les fichiers, récemment ouvert par l'utilisateur en cours.
Les options disponibles sont:

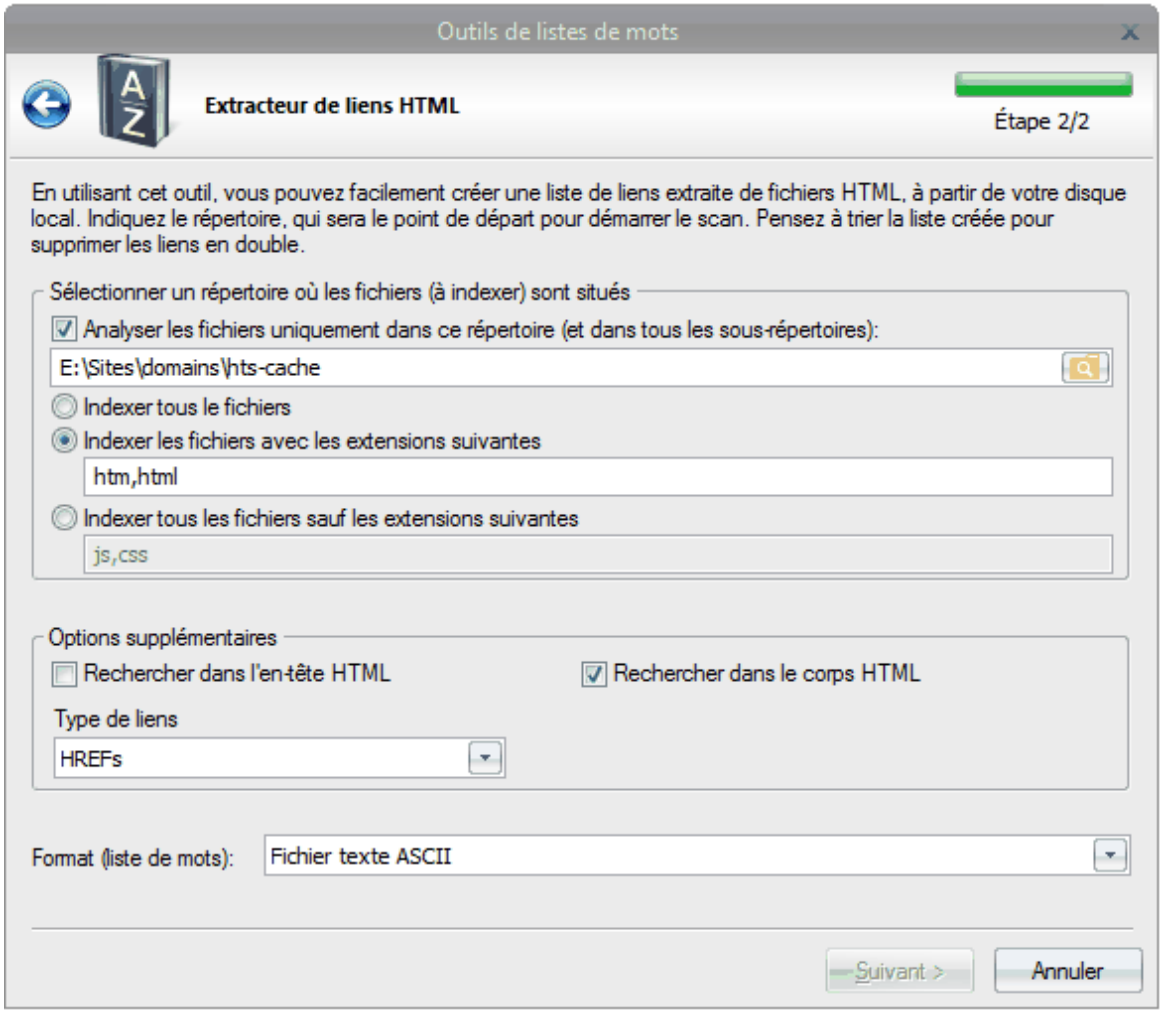
- Définir la longueur maximum des mots qui doivent être ajoutés dans la liste de mots. Tous les mots avec une taille supérieure à celle spécifiée ne seront pas ajoutés dans la liste de mots.
- Ignorer les fichiers ayant une taille supérieure à la taille définie. La taille est définie en Mo.
- Utiliser des délimiteurs de mots personnalisés. Par défaut, les délimiteurs de mots sont tous des caractères non-alphabétiques.
- Ne pas indexer les fichiers avec les extensions spécifiées. Utilisez cette option pour ignorer (sauter) les fichiers que vous considérez comme inutiles.

Cliquez sur le bouton **Suivant>** pour démarrer le processus d'indexation.

Gardez en mémoire que ce processus peut prendre un temps considérable !

2.6.7.9 Extraire les liens HTML

Cet outil est conçu pour extraire les liens hypertexte HTML de fichiers HTML.



Les options de configuration pour cet outil sont constituées en deux groupes. Dans le premier groupe, vous devez définir le chemin du répertoire, où sont localisés les fichiers HTML, et sélectionner une méthode de recherche de fichiers, dans la liste suivante:

- Rechercher les fichiers, uniquement, dans le répertoire spécifié. Si cette option n'est pas cochée, le programme analysera récursivement tous les sous-répertoires et les fichiers s'y trouvant.
- Indexer tous les fichiers.
- Indexer, uniquement, les fichiers avec certaines extensions.
- Indexer tous les fichiers, excepté certains fichiers.

Par défaut, l'outil vérifie, uniquement, les fichiers *.htm et *.html.

Le options complémentaires de ce groupe permettent de définir le type de lien, comme par ex: où les rechercher:

- Rechercher dans l'en-tête HTML.
- Rechercher dans le corps HTML.
- Rechercher les liens dans les balises HREF, SRC ou dans les deux.

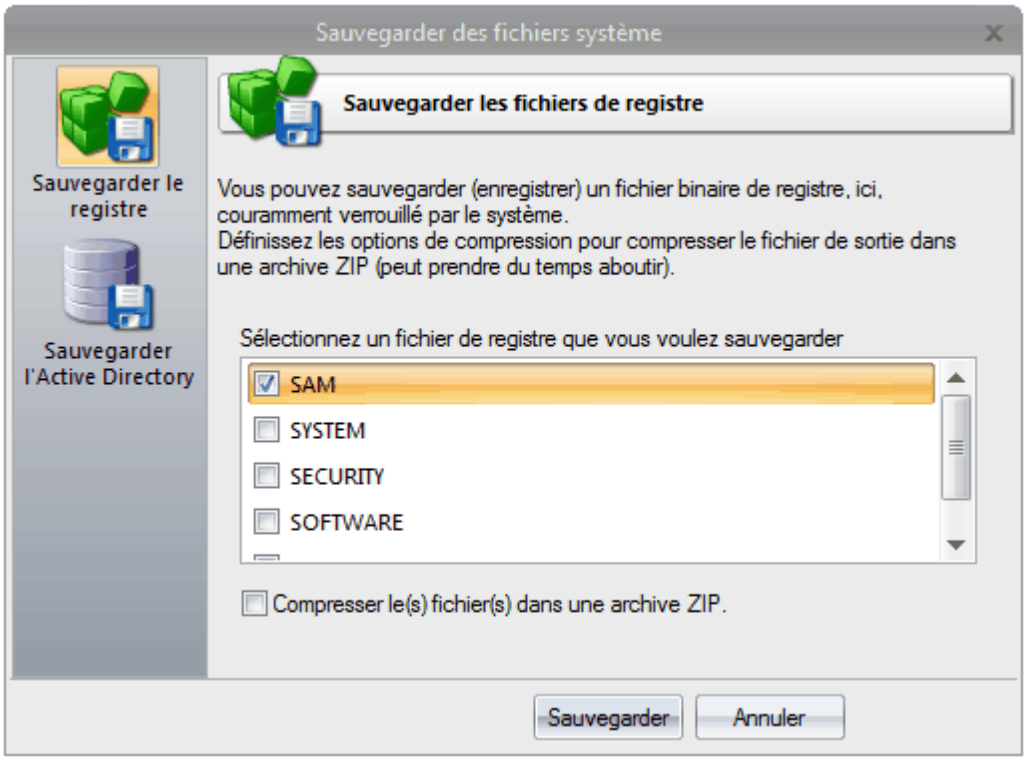
Cliquez sur le bouton **Suivant>** pour démarrer la recherche, qui peut prendre un temps considérable. Une fois, l'opération terminée, et que les liens trouvés ont été enregistrés dans le disque dur, pensez à les trier pour supprimer tous les doublons.

2.7 Menu Utilitaires

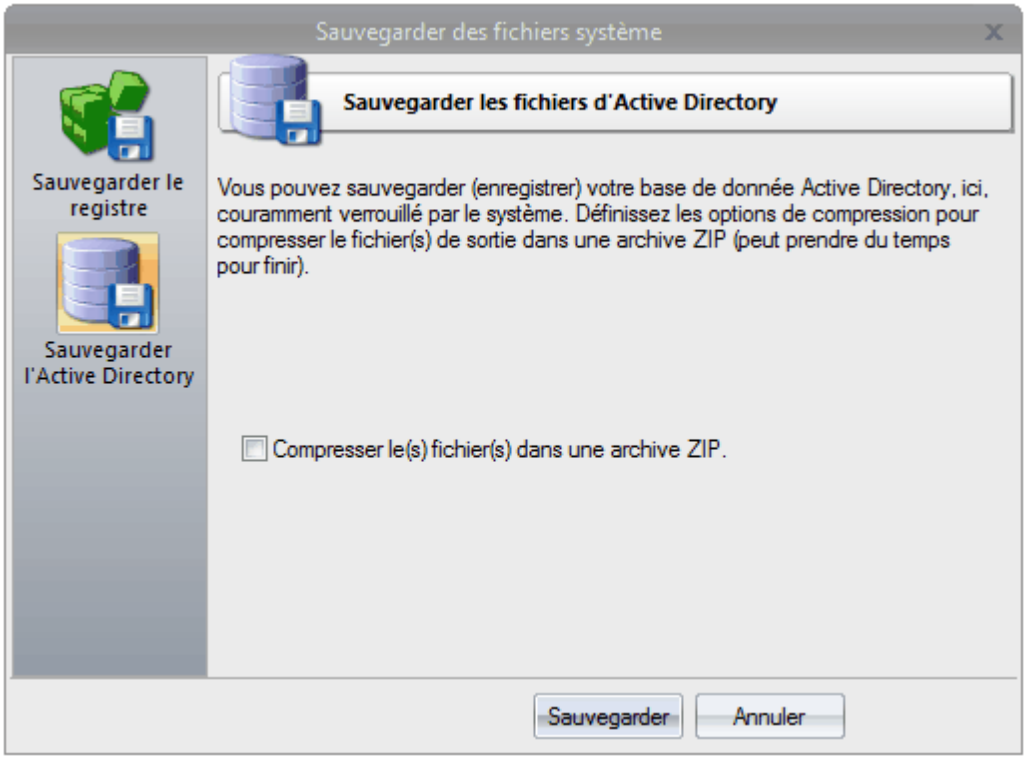
Le menu des utilitaires est constitué d'outils complémentaires principalement pour les utilisateurs avancés.

2.7.1 Sauvegarder des fichiers système

Cet outil de sauvegarde de la base de registre permets, facilement, de créer une copie de sauvegarde de votre base de registre Windows.
La plupart du temps, les fichiers de la base de registre sont verrouillés par le système d'exploitation. Vous pouvez définir des options supplémentaires pour sauver de l'espace disque et compresser les fichiers de sauvegardes dans une archive ZIP.

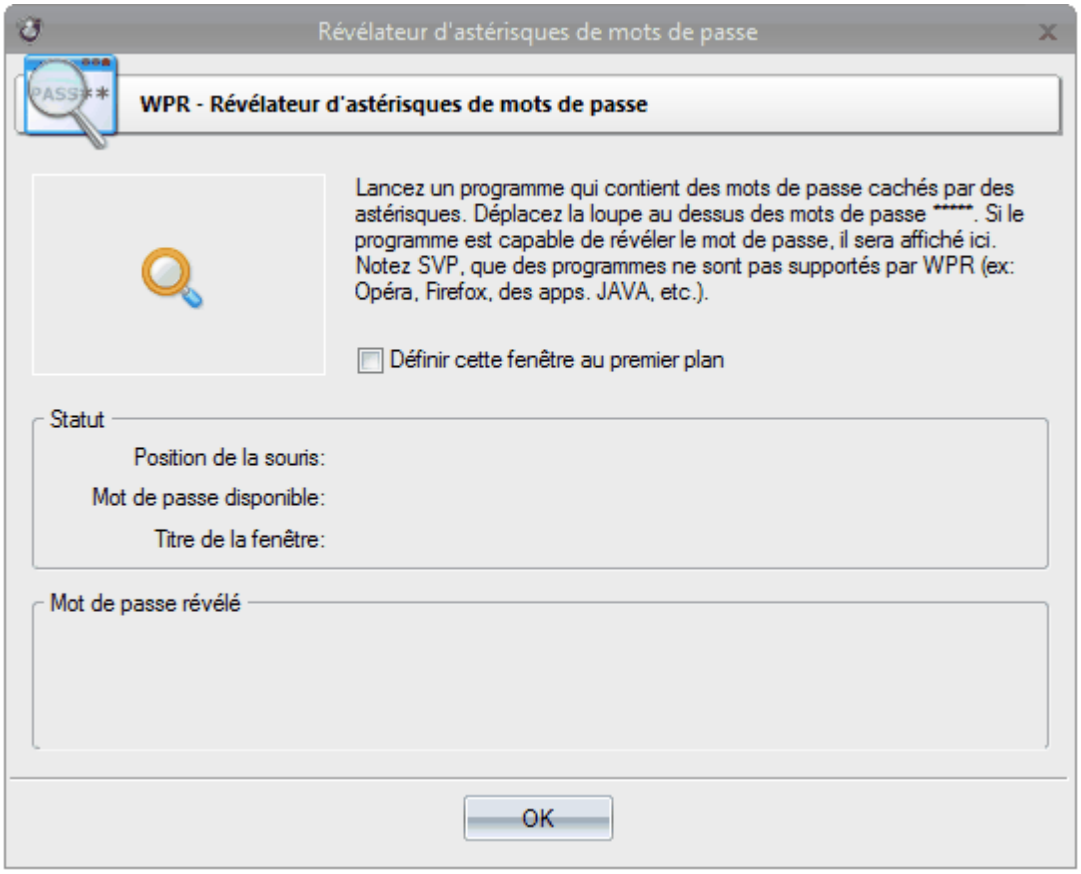


Sauvegarder la base de donnée de l'Active Directory est très similaire à la sauvegarde de la base de registre, excepté le fait que le chemin de l'Active Directory est déterminé automatiquement par le programme.



Les privilèges Administrateur ou d'Opérateurs de Sauvegarde sont nécessaire pour exécuter ce plug-in.
Créer et enregistrer la base de données de l'Active Directory peut prendre du temps: des minutes ou plusieurs heures pour les bases de données imposantes.

2.7.2 Révélateur d'astérisques de mots de passe



Cet outil permets de récupérer les mots de passe cachés derrière les astérisques. c'est souvent utile lorsque vous avez besoin de se rappeler rapidement un mot de passe caché par des **** et que vous n'avez pas nécessairement les outils de récupérations sous la main. Pour rendre le mot de passe sous les **** visibles, vous devez déplacer la loupe magique de la fenêtre de WPR dans le champ avec les astérisques.

Cette méthode fonctionne pour les fenêtres des contrôles Windows et d'Internet Explorer. Elle a aussi un nombre de restrictions avec:

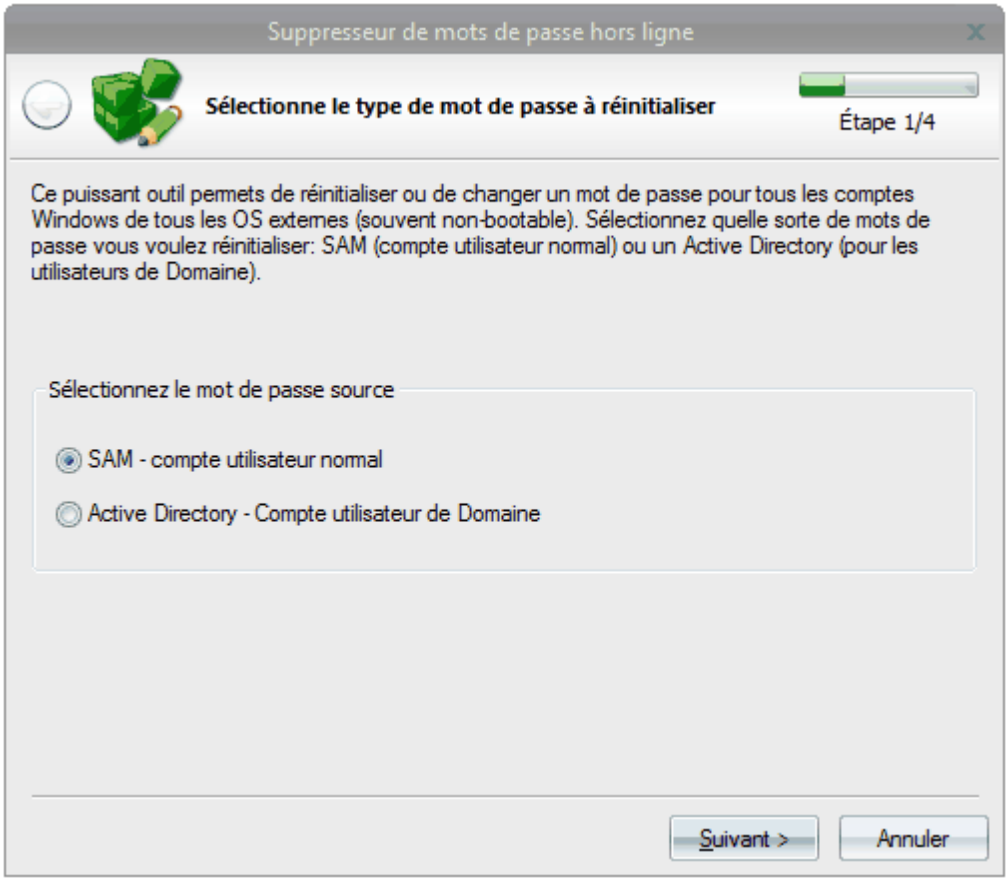
- Des applications qui ont leur propre GUI, et donc, le Révélateur d'Astérisques peut être incapable d'interagir avec ce type d'applications, comme Opéra, Mozilla, Firefox, etc.
- Certains sites Web possèdent une protection intégrée, qui cache l'espace de stockage ou les astérisques derrière les astérisques des caractères * (les astérisques cachés derrière des astérisques !).
- Dans certains dialogues système de Windows, également, le caractère * est caché et n'affiche pas le mot de passe réel.

Pour que cet outil fonctionne correctement, vous devez possédez des privilèges d'administrateur.

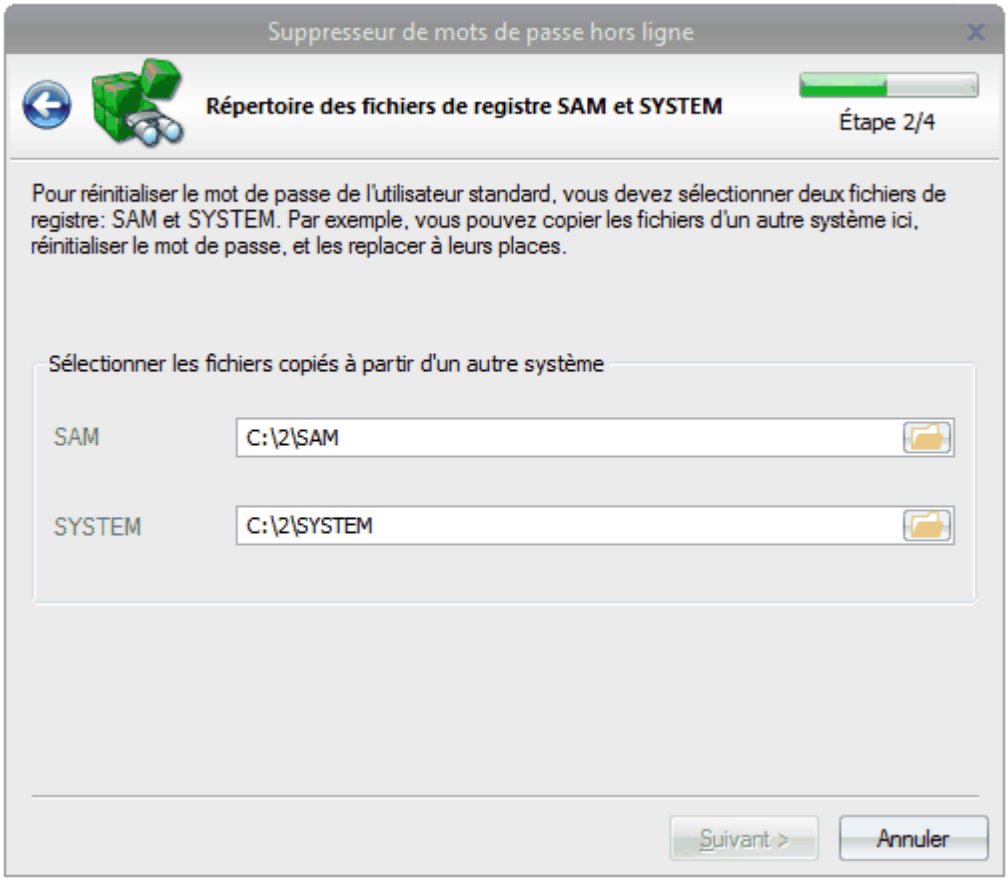
2.7.3 Suppresseur de mots de passe hors ligne

Ce plug-in très utile, permets de supprimer et de modifier les mots de passe directement dans le fichier de la base de registre SAM ou dans le fichier NTDS.DIT. Par exemple, pour récupérer l'accès à un système verrouillé, vous n'a pas besoin, nécessairement, de récupérer le mot de passe d'identification de connexion de Windows (login). A la place, vous pouvez copier les fichiers de base de registre SAM et SYSTEM du système verrouillé, utilisez le plug-in pour supprimer le mot de passe pour le compte (ou désactiver le paramètre de verrouillage (flag)) et copier à nouveau les fichiers sur le système verrouillé. Le plug-in suppresseur de mots de passe appairait sous forme d'un assistant, constitué de quatre étapes:

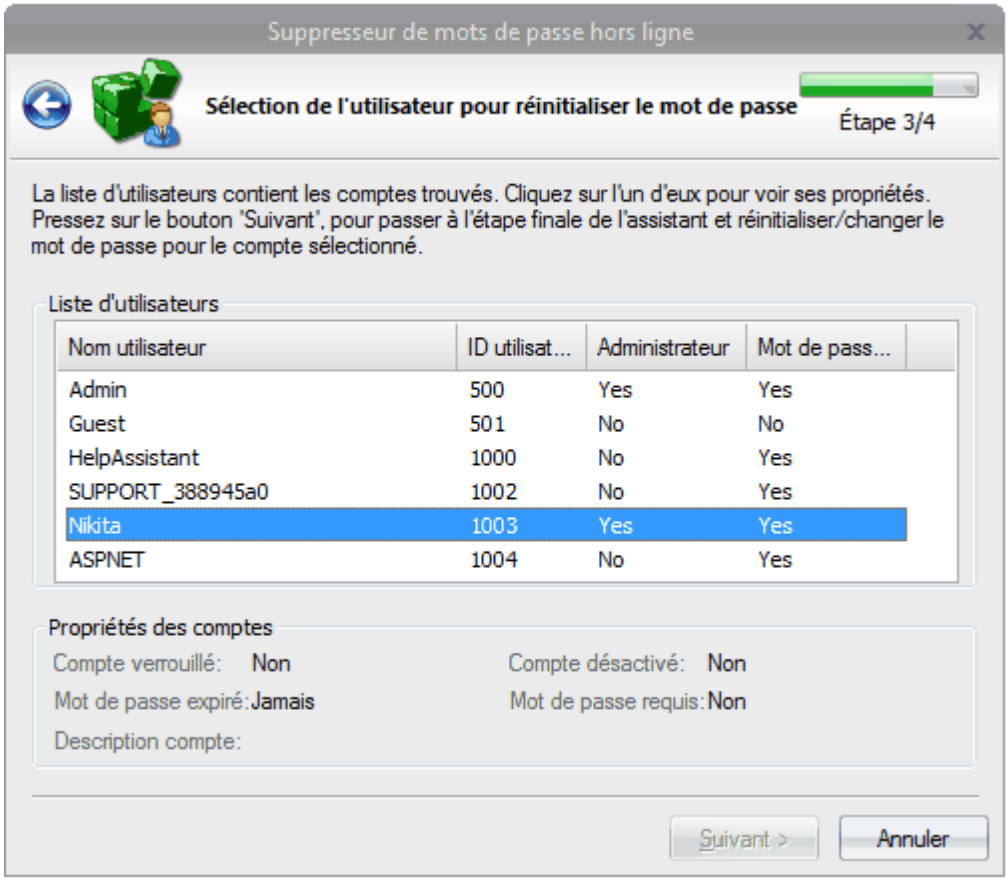
1. A la première étape, sélectionnez le mot de passe source. Cela peut être soit un fichier SAM pour les comptes ordinaires - ou un fichier NTDIS.DIT - pour supprimer les mots de passe dans un Domaine.



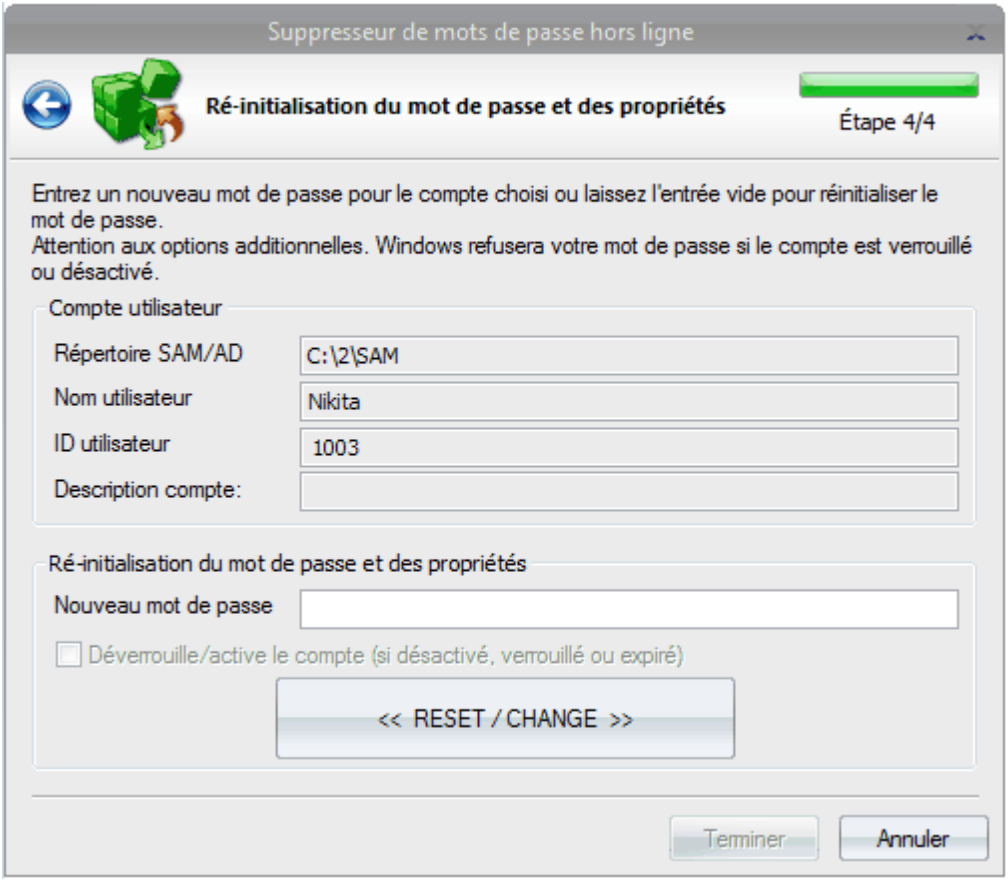
2. A la deuxième étape de l'assistant, indiquez le chemin des fichiers SAM/NTDS.DIT et du fichier SYSTEM de la base de registre. Par défaut, NTDS.DIT est situé dans le répertoire c:\windows\ntds. Les fichiers de la base de registre sont situés dans le répertoire c:\windows\system32\config.



3. Dans cette étape, vous devez sélectionner le compte dont vous souhaiter modifier le mot de passe. Sélectionnez le nom de l'utilisateur et passer à l'étape suivante finale.



4. Le champ '**Nouveau mot de passe**' est utiliser pour saisir le nouveau mot de passe (laissez ce champ vide pour réinitialiser le mot de passe). Si le champ est désactivé (grisé), cela signifie que le mot de passe pour ce compte est déjà vide. La même chose s'applique à l'option avancée pour déverrouiller les comptes d'utilisateurs bloqués ou les désactiver.



N'oubliez pas d'enregistrer vos fichiers SAM ou NTDS.DIT avant de les modifier définitivement !

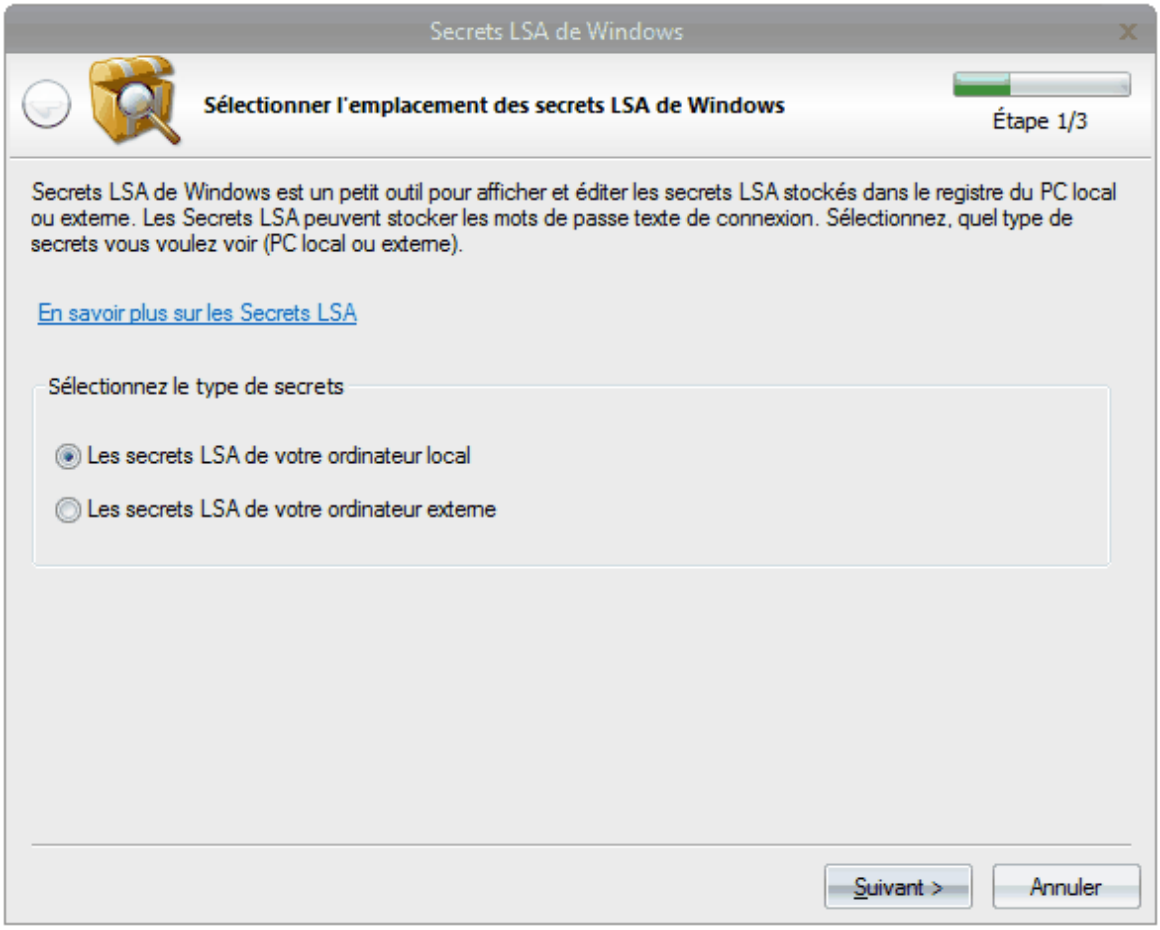
2.7.4 Outils d'analyses

2.7.4.1 Secrets LSA de Windows

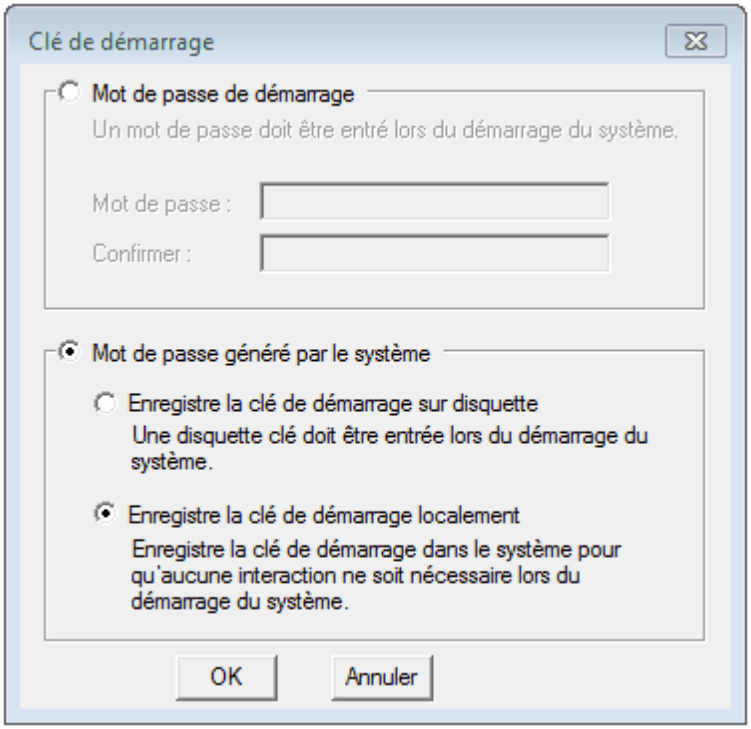
Les secrets LSA sont un espace spécial de stockage pour les données importantes utilisées par le Local Security Authority (LSA) dans Windows. LSA est conçu pour gérer le la politique locale de sécurité du système, des audits, des authentifications, des connexions d'utilisateurs sur le système, le stockage de données privées. Les données sensibles des l'utilisateurs et du système sont stockées dans les "secrets". L'accès à toutes les données secrètes sont disponibles uniquement pour le système. Cependant, comme on le voit plus bas, certains programmes, en particulier Windows Password Recovery, permettent d'outrepasser cette protection.

Le plugin Windows Password Recovery, pour le manipulation des secrets LSA, est un petit outil pour les visualiser, les analyser et les éditer. Ce plugin possède un assistant qui vous guidera, relativement simple, en trois étapes:

1. En premier, sélectionnez le type de secrets que vous souhaitez traiter. Ils peuvent être des secrets du système local, où le programme WPR est exécuté, ou des secrets d'un PC externe.

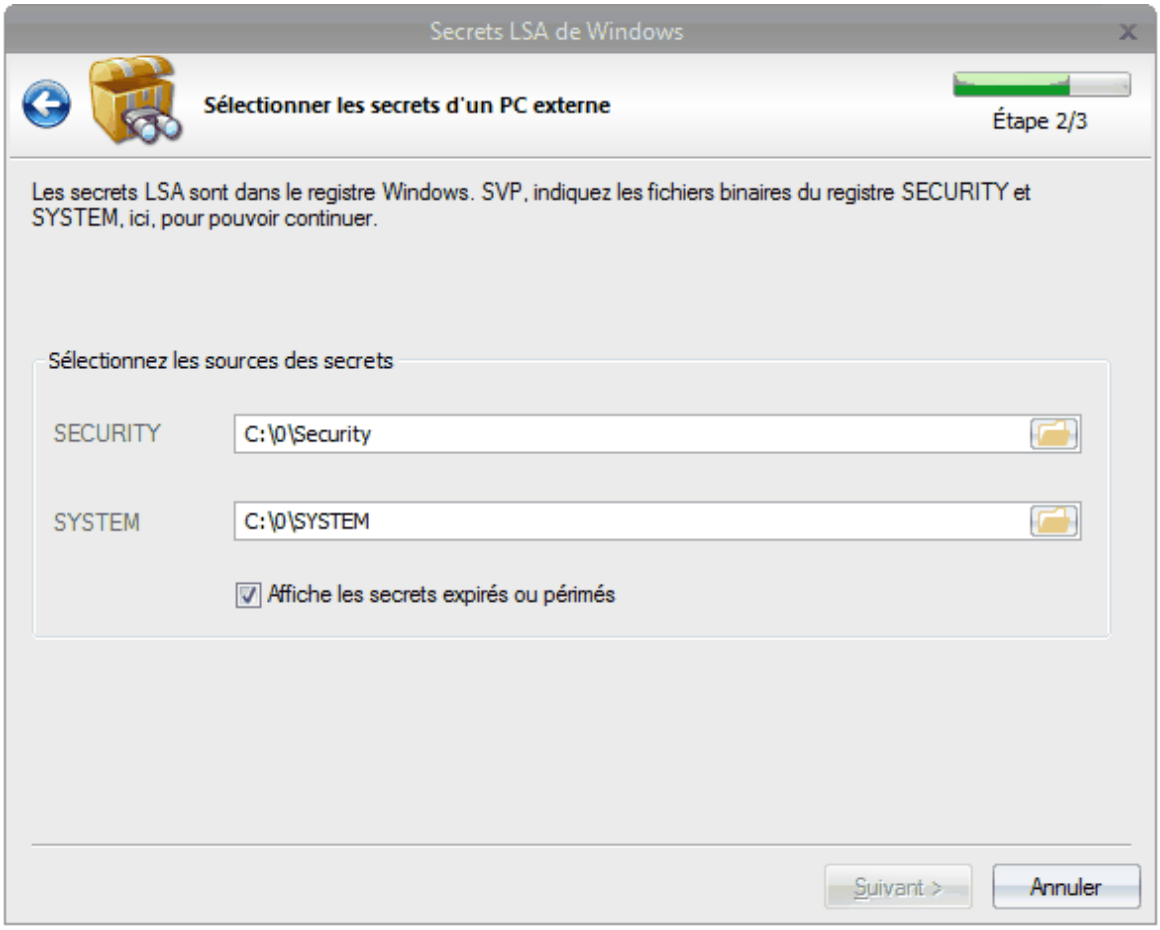


2. Lors de la sélection de secrets d'un PC externe, vous devez spécifier le chemin des deux fichiers de la base de registre: SYSTEM et SECURITY. Le fichier SECURITY contient des secrets cryptés, et SYSTEM est nécessaire pour les décrypter. Vous pouvez trouver plus d'informations sur les décryptages de secrets dans notre article. Notez, SVP, que le cryptage de secrets fait appel à SYSKEY. Par défaut, SYSKEY est configuré de manière a être extrait de la base de registre (qui est le rôle de SYSTEM).

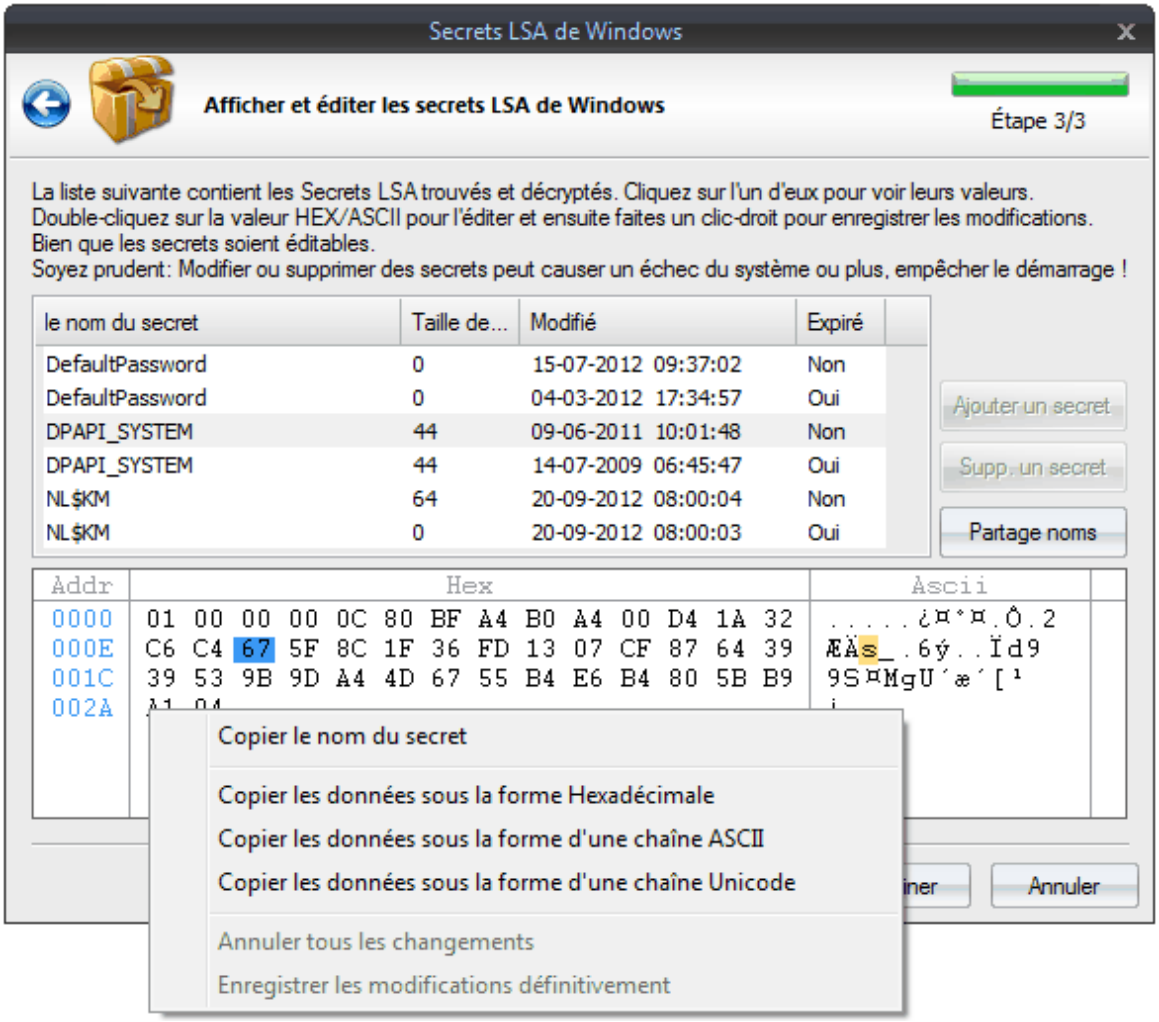


Dans certains cas, il peut être configuré de plusieurs façons: pour être stocké sur un disque de démarrage ou dérivé du mot de passe de l'utilisateur lors du démarrage de l'OS. Quelque soit la façon, le plugin supporte tous les types de cryptage de SYSKEY.

Les données stockées dans les secrets sont cruciales pour le fonctionnement du système complet. Toutefois, les secrets LSA sont stockés dans deux copies: actuelle (active) et précédente (ancienne). la modification d'un secret le place dans la copie précédente et le remplace par le nouveau secret modifié. Le plugin possède une option pour visualiser les secrets dans la copie active et précédente.



3. La dernière étape de l'assistant décrypte les secrets et les affichent sous forme de listes. Pour afficher la valeur d'un secret, il suffit de cliquer sur son nom. Entrez dans le mode d'édition en double-cliquant sur un des caractères Hexadécimal ou ASCII (le marquant en jaune), ensuite saisissez la nouvelle valeur. Dans le mode d'édition, utilisez les touches du curseur pour vous déplacer vers le nouveau caractère. Les valeurs modifiées sont marquées en rouge. Pour enregistrer les modifications, faites un clic-droit sur le champ HEX/ASCII et ensuite enregistrer l'élément avec le menu qui s'affiche.



Gardez à l'esprit que certains des secrets contiennent des données critiques, et leurs modifications peuvent créer une instabilité du système ou parfois une impossibilité de démarrer le système !

Le plugin permets aussi d'ajouter ou de supprimer des secrets (pour les secrets du système d'exploitation en cours seulement). La suppression d'un secret, qu'il soit ancien ou nouveau, supprime automatiquement les deux copies.

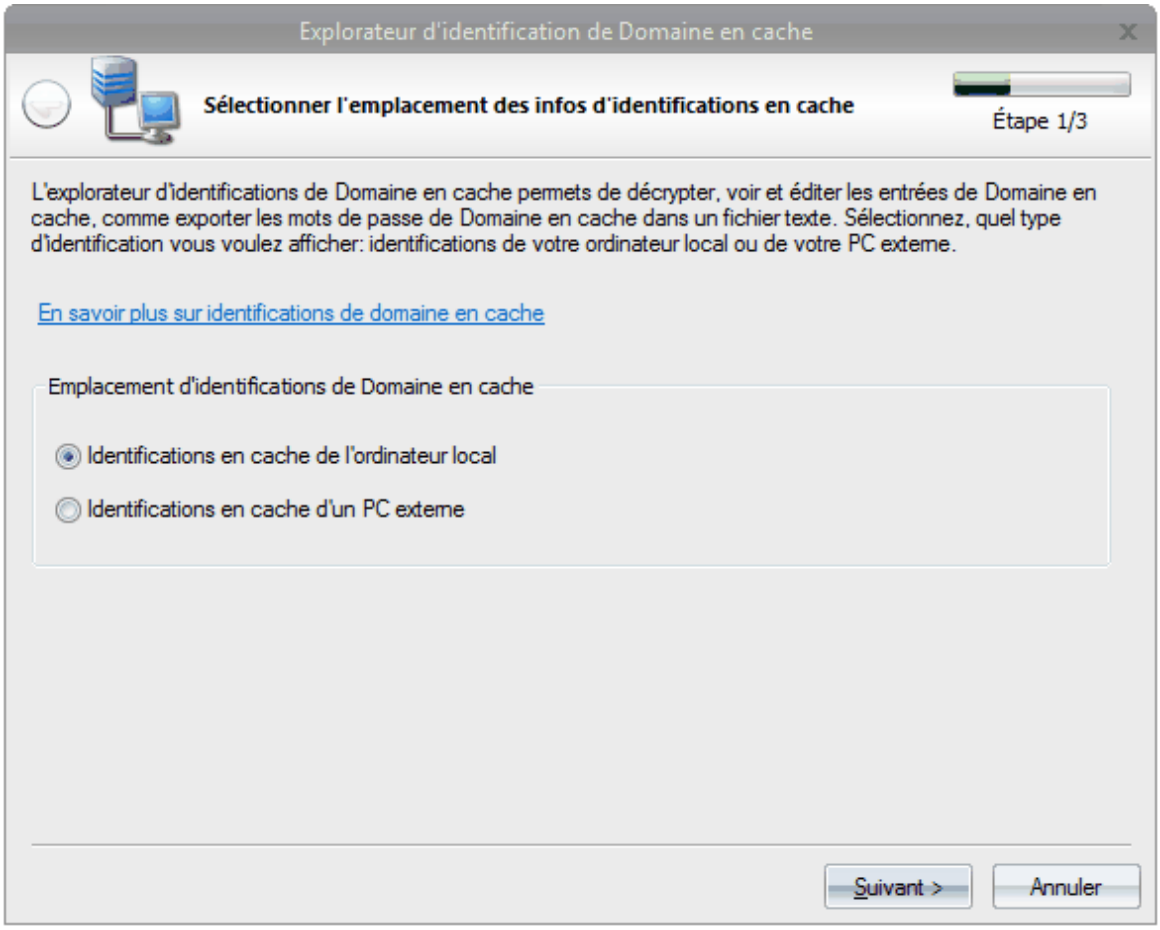
Vous pouvez partager vos secrets avec les développeurs (Bouton "Partage noms"). Ces e-mails contiennent uniquement les noms des secrets, sans les données actuelles. L'analyse des noms des secrets nous permets de rendre le programme plus efficace.

2.7.4.2 Explorateur d'informations d'identifications de domaine en cache

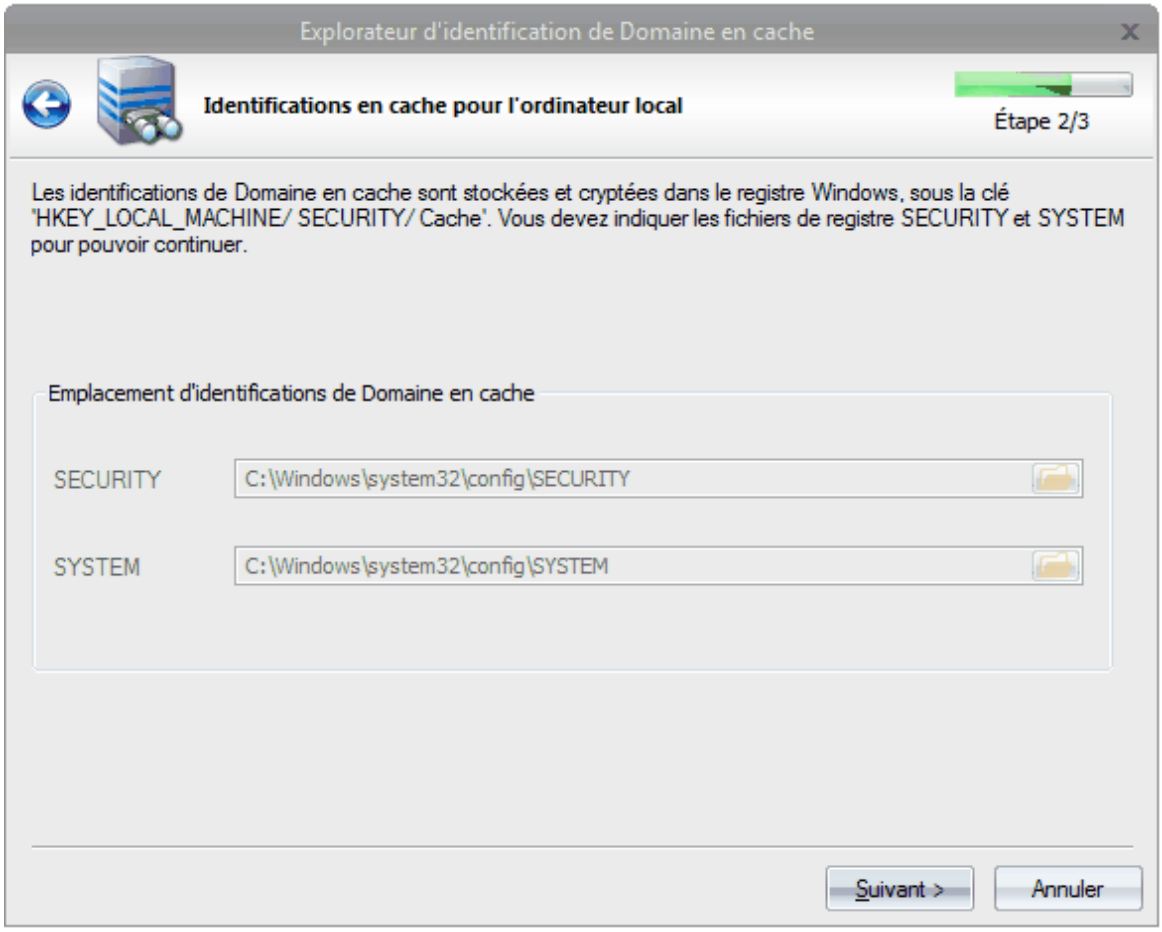
A partir de la version 2.0, le programme permets la lecture des enregistrements de domaine en cache. Windows utilise les enregistrements de domaine en cache pour lui permettre de se connecter au serveur même si les informations de de connexion sont indisponibles quelques soient les raisons.

Le plugin pour la manipulation des enregistrements de domaine en cache est constitué de trois étapes:

En premier, il faut décider, quels enregistrements doivent être décryptés: ceux du système d'exploitation courant ou d'un autre ordinateur.

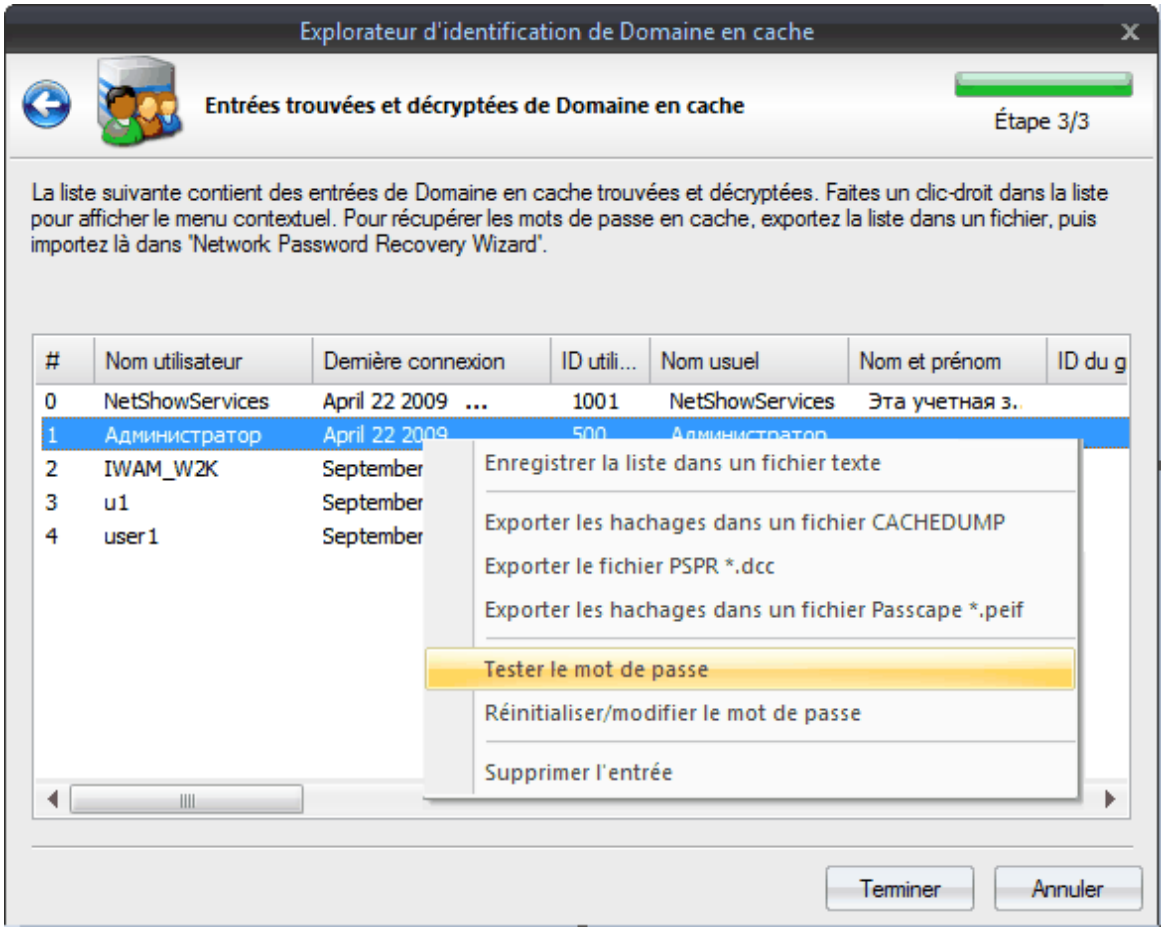


Les enregistrements de domaine en cache sont stockés dans fichier SECURITY de la base de registre. Par conséquent, lors de la sélection de l'option pour lire les enregistrements à partir d'un PC externe, à l'étape suivante de l'assistant, vous devez indiquer les deux chemins de SECURITY et SYSTEM de la base de registre utilisés pour le décryptage des enregistrements.
Si vous choisissez l'autre option de lecture des enregistrements en cache de l'ordinateur local, à la seconde étape de l'assistant, le programme localisera automatiquement ces fichiers. Les fichiers de la base de registre se trouvant dans le répertoire, connu suivant: C:\%WINDIR%\system32\config\, ou %WINDIR% est le répertoire de Windows.



Si la lecture est réalisée avec succès, à l'étape finale de l'assistant, s'affichera les enregistrements de domaine décryptés. Chaque enregistrement possède plusieurs attributs. Par exemple, le nom de l'utilisateur, le temps depuis la dernière connexion, le groupe de travail, le mot de passe de l'utilisateur en cache (actuel, et le hash).

Un clic-droit sur la liste des enregistrements ouvre le menu contextuel, qui permets les actions suivantes:
- Enregistrer les données avec tous les attributs dans un fichier texte.
- Exporter les hachages de mots de passe dans un fichier PWDUMP, *.DCC ou *.PEIF. Notez, que le format PWDUMP stocke les enregistrements de façon imparfaite; cependant, il est préférable de stocker les hachages de mots de passe dans des fichiers *.DCC ou *.PEIF.
- Tester ou éditer le mot de passe pour un enregistrement de domaine en cache.
- Supprimer un enregistrement.

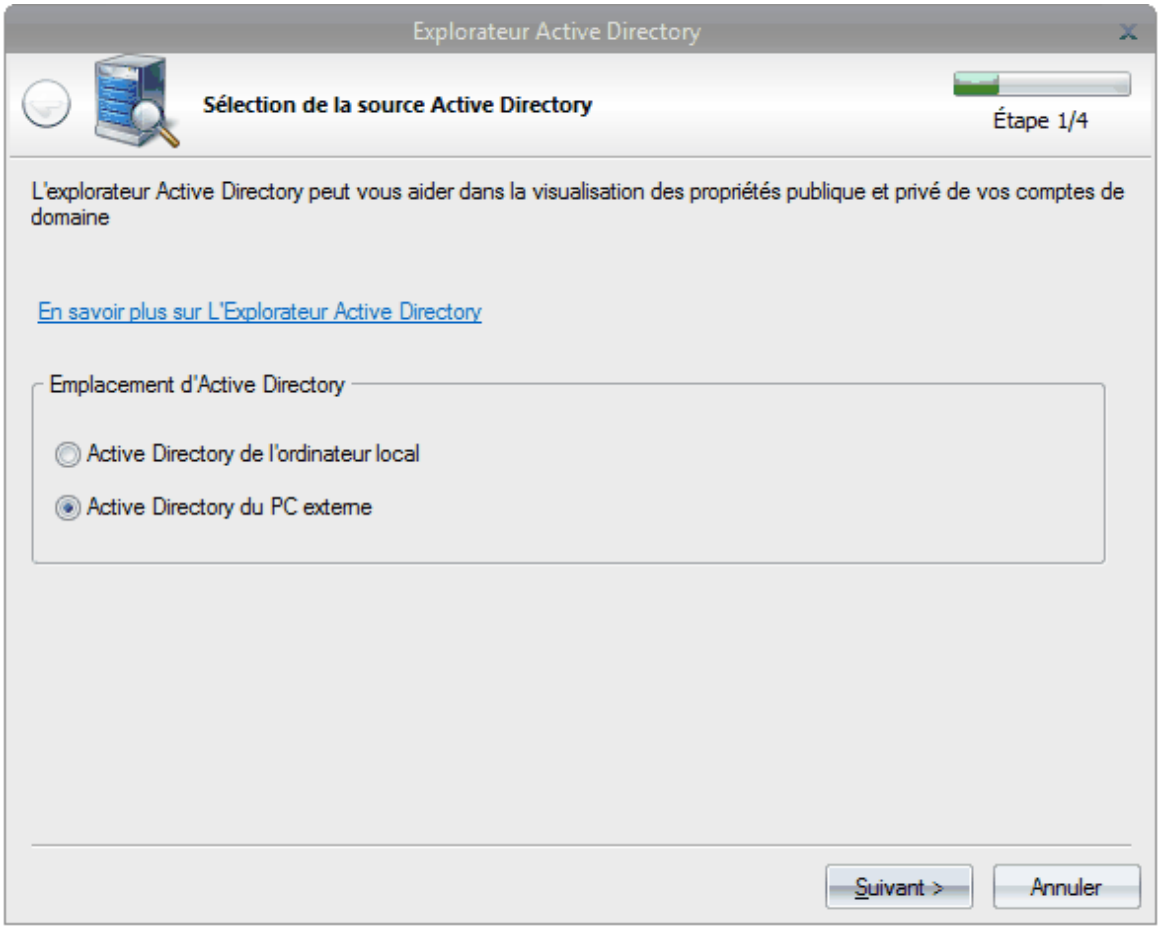


Pour récupérer un mot de passe de domaine en cache, il est préférable d'utiliser Network Password Recovery Wizard; avec les hachages exportés dans un des fichiers au format indiqué précédemment.

2.7.4.3 Explorateur Active Directory

L'explorateur d'Active Directory est un petit utilitaire pour visualiser, analyser et éditer les propriétés (attributs) des comptes de domaine, qu'ils soient publiques ou privés.

Dans un premier temps, sélectionnez le type de base de données de l'Active Directory avec lequel vous souhaitez travailler: local ou externe.

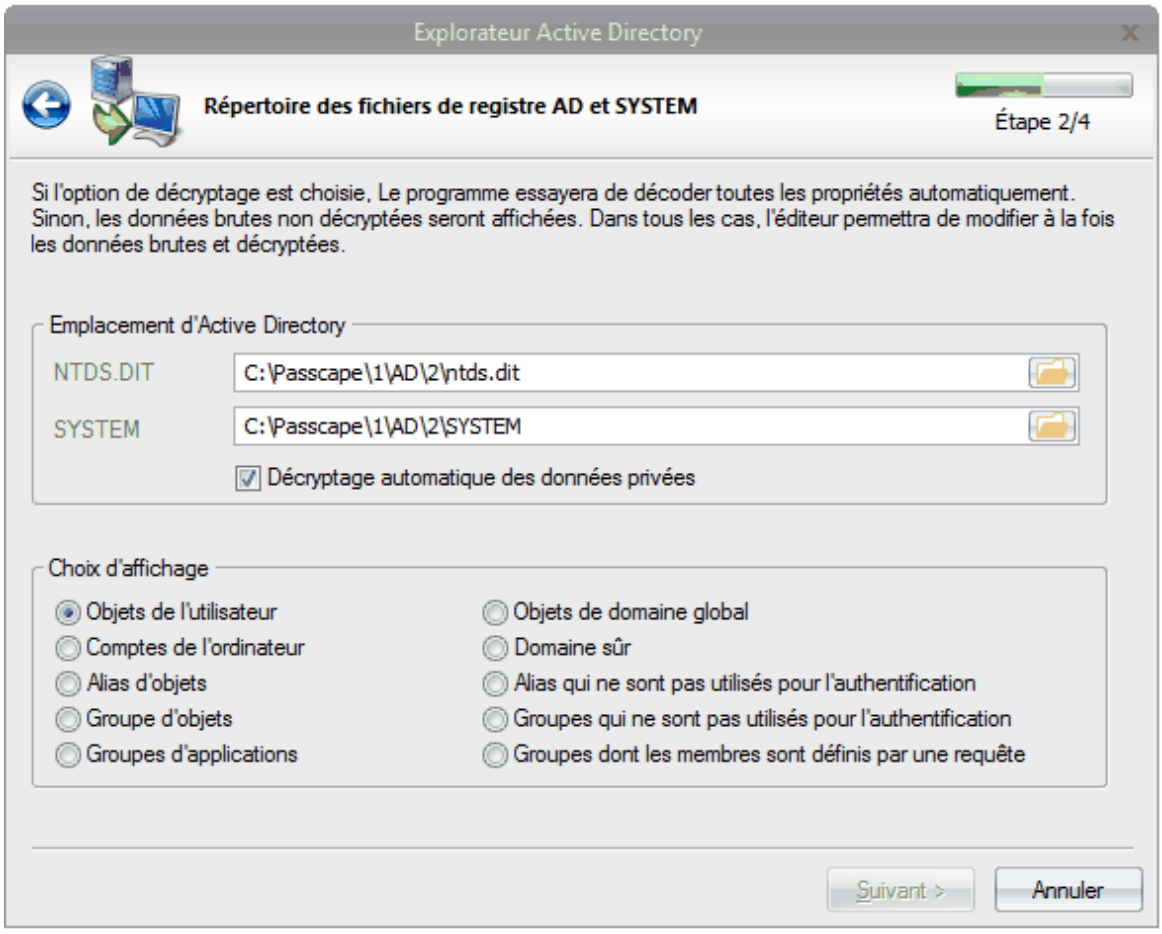


Lors de la sélection d'une base de données externe, indiquez le chemin du fichier **NTDS.DIT** et **SYSTEM** de la base de registre. Ce dernier étant requis pour décrypter les données privées. Si le décryptage automatique est activé, tous les attributs de cryptage d'un compte seront décryptés à la volée. Dans tous les cas, l'éditeur permets l'édition des données brutes et décryptées. Pour des raisons de sécurité, le mode de l'éditeur est disponible que pour les base de données externes !

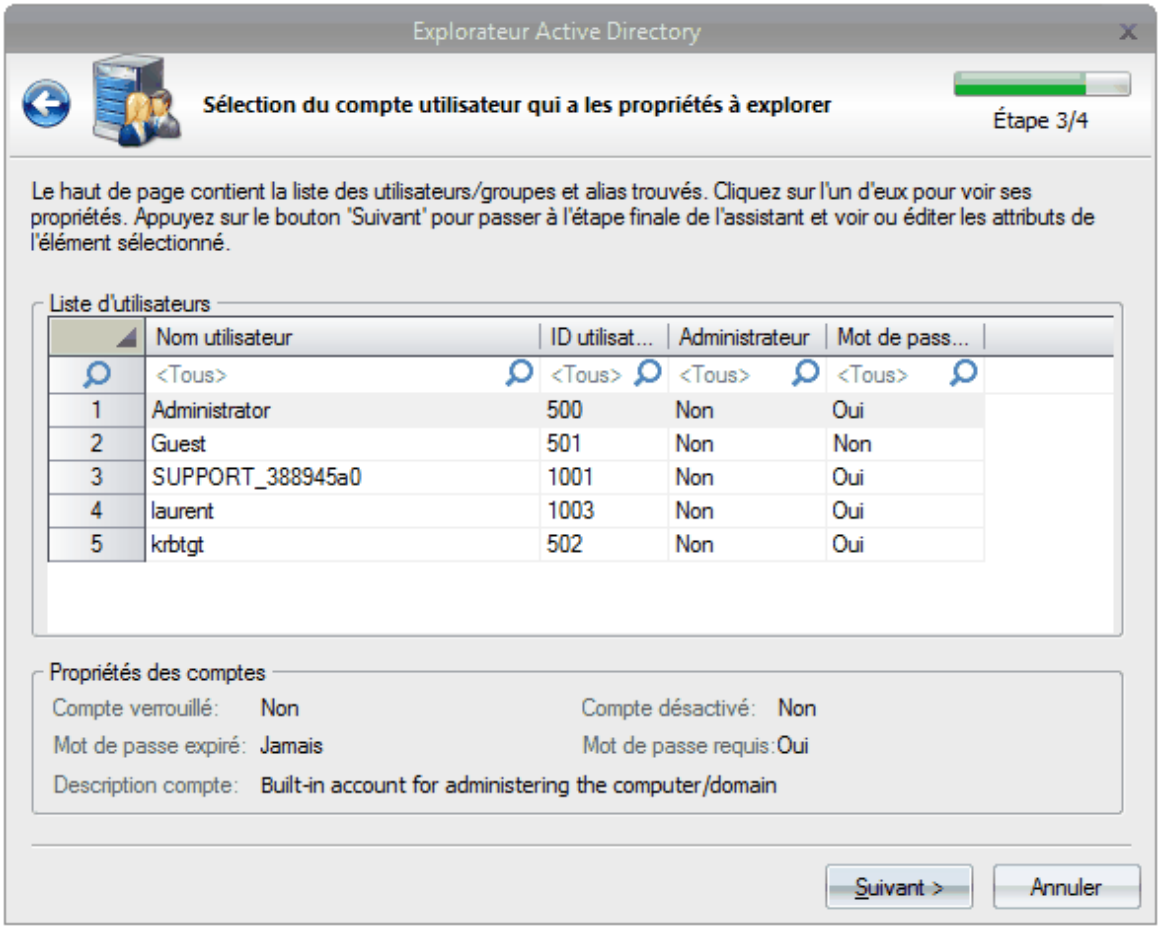
Vous devez indiquer quel objet vous voulez afficher. Il y a 10 types d'objets de domaine. Voir la table suivante:

Objet de domaine	Description
Objet d'utilisateur	Un objet de classe utilisateur. Un objet d'utilisateur est un objet principal de sécurité; le principal est une personne ou une entité de service exécuté sur l'ordinateur. Le secret partagé permets à la personne ou à l'entité de service de s'authentifier elle-même.
Objet global de domaine	Représente un objet typique de domaine qui n'est pas conforme à d'autres types.
Compte d'ordinateurs	Représente un objet d'ordinateur qui est associé avec un client individuel ou des serveurs dans un domaine Active Directory.
Domaine de confiance	Représente un objet d'utilisateur qui est utilisé pour les domaines de confiance. Un domaine de confiance est un domaine qui a été vérifié pour permettre de prendre des décisions d'authentification pour les directeurs de sécurité dans ce domaine.
Objets d'alias	Un groupe de sécurité ou de distribution peut contenir plusieurs groupes universels, des groupes globaux, autres groupes de domaine locaux à partir du propre domaine, et les comptes à partir de tous les domaines dans la forêt. Les alias peuvent accorder les droits et les permissions des ressources qui résident uniquement dans le même groupe local du domaine ou ils sont situés.
Alias qui ne sont pas	Représente un objet d'alias qui n'est pas utilisé pour générer un contexte d'autorisation.

Objet de domaine	Description
utilisés pour les autorisations	
Objets de groupes	Une base de données d'objet qui représente un ensemble d'utilisateur, d'objets de groupes et une valeur d'identifiant de sécurité (SID).
Groupes qui ne sont pas utilisés pour les autorisations	Représente un objet de groupe qui n'est pas utilisé pour générer un texte d'autorisation.
Groupes définis par l'application	Un groupe défini par une application.
Groupes de recherche	Un groupe défini par une application dont les membres sont déterminés par le résultat d'une recherche.



Une fois que la source des données est choisie, passez à l'étape suivante pour sélectionner les comptes. Certaines bases de données de l'Active Directory contiennent des dizaines ou souvent des centaines de milliers d'enregistrements de domaine. Lire une si grande base de données et remplir la liste des utilisateurs peut prendre du temps. Sélectionnez un enregistrement pour afficher un résumé des informations: statut, si un mot de passe est défini, si il est expiré, la description du compte, etc. Cliquez sur le bouton "Suivant>" pour lancer le processus pour collecter et décrypter tous les attributs disponibles pour l'objet sélectionné.



Chaque attribut est constitué d'un nom et d'une valeur. Par exemple, '**Common-Name**' contient le nom du compte, et l'attribut '**Unicode-Pwd**' stocke le hachage du mot de passe. Pour plus de détails sur la description d'un attribut, sélectionnez le dans la liste, puis cliquez sur la ligne qui apparaît dans le champ de la description. En double-cliquant sur le champ de données, cela ouvre l'attribut sélectionné pour l'édition. Lorsque l'édition est terminée, faire un clic-droit sur le texte pour ouvrir le menu contextuel et enregistrer les modifications dans le fichier ntds.dit ou pour les annuler.

Ci-dessous vous trouverez la description des attributs de certains comptes. La description complète est disponible sur le site web de Microsoft.

Common-Name
Le nom du compte.

DBCS-Pwd
Contient le mot de passe du gestionnaire LAN du compte.

Unicode-Pwd
Le mot de passe de l'utilisateur dans Windows NT, format à sens unique (OWF). Notez que vous ne pouvez pas dériver le mot de passe en clair à partir de cette forme de mot de passe OWF.

Lm-Pwd-History
Contient l'historique du mot de passe d'un utilisateur dans le gestionnaire LAN, format à sens unique. L'attribut est utilisé pour la compatibilité avec les clients du gestionnaire LAN 2.x, Windows 95, et Windows 98.

Nt-Pwd-History
Historique de mots de passe d'un utilisateur dans le format Windows NT OWF.

Primary-Group-ID

Identificateur relatif (RID) pour le groupe principal d'un utilisateur. C'est le groupe des Utilisateurs du Domaine, par défaut.

Bad-Pwd-Count
Contient le nombre de fois que l'utilisateur a essayé de se connecter au compte en utilisant un mot de passe incorrect.

Admin-Count
Indique que le compte est membre d'un des groupes d'Administration (directement ou transitivement).

Logon-Hours
Heure à laquelle l'utilisateur a été autorisé à ce connecter au domaine.

Last-Logon
Heure à laquelle l'utilisateur s'est connecté à son compte pour la dernière fois.

Bad-Password-Time
Dernière heure où l'utilisateur a tenté de se connecter à son compte avec un mot de passe invalide. Cette valeur est stockée comme un entier de 8 bits de large qui représente le nombre d'intervalles de 100 nanosecondes depuis le 1 Janvier 1601.

Last-Logon-Timestamp
Heure à laquelle l'utilisateur s'est connecté la dernière fois au domaine.

Pwd-Last-Set
Date à laquelle le mot de passe de ce compte a été changé pour la dernière fois.

Account-Expires
Date à laquelle le compte expirera. Une valeur de 0 ou 0x7FFFFFFFFFFFFFFF indique que le compte n'expirera jamais.

Supplemental-Credentials
Stocke la version cryptée du mot de passe de l'utilisateur. Utilisé lors de l'authentification.

User-Account-Control
Paramètres contrôlant la gestion du compte de l'utilisateur. Cette valeur peut être une combinaison d'une ou plusieurs valeurs parmis celles qui suivent:
0x00000001 Script de connexion a été exécuté pour ce compte.
0x00000002 Le compte est désactivé.
0x00000008 Le répertoire racine est nécessaire.
0x00000010 Le compte est actuellement verrouillé.
0x00000020 Aucun mot de passe est requis.
0x00000040 L'utilisateur ne peut pas changer le mot de passe.
0x00000080 Le mot de passe texte est permanent.
0x00000100 Ce compte est pour les utilisateurs qui n'ont pas de compte principal dans un autre domaine.
0x00000200 C'est un type de compte par défaut qui représente un utilisateur standard.
0x00000800 Compte de confiance pour un système de domaine, qui confie d'autres domaines.
0x00001000 C'est le compte d'un ordinateur qui est membre de ce domaine.
0x00002000 C'est le compte d'un ordinateur contrôleur de sauvegarde système du domaine qui en est membre.
0x00010000 Le mot de passe pour ce compte n'expirera jamais.
0x00020000 Compte de connexion MNS.
0x00040000 L'utilisateur doit utiliser une carte à puce pour se connecter.
0x00080000 Le compte, sous lequel le service s'exécute, a été vérifié pour la délégation Kerberos.
0x00100000 Le contexte de sécurité de l'utilisateur ne sera pas délégué à un service même si le compte du service a été défini comme de confiance pour la délégation Kerberos.
0x00200000 Restreint le principal d'utiliser uniquement, pour les clés, les types de cryptages de Data Encryption Standard (DES).
0x00400000 Ce compte ne nécessite pas de pré-authentification Kerberos pour la connexion.
0x00800000 Le mot de passe de l'utilisateur a expiré.

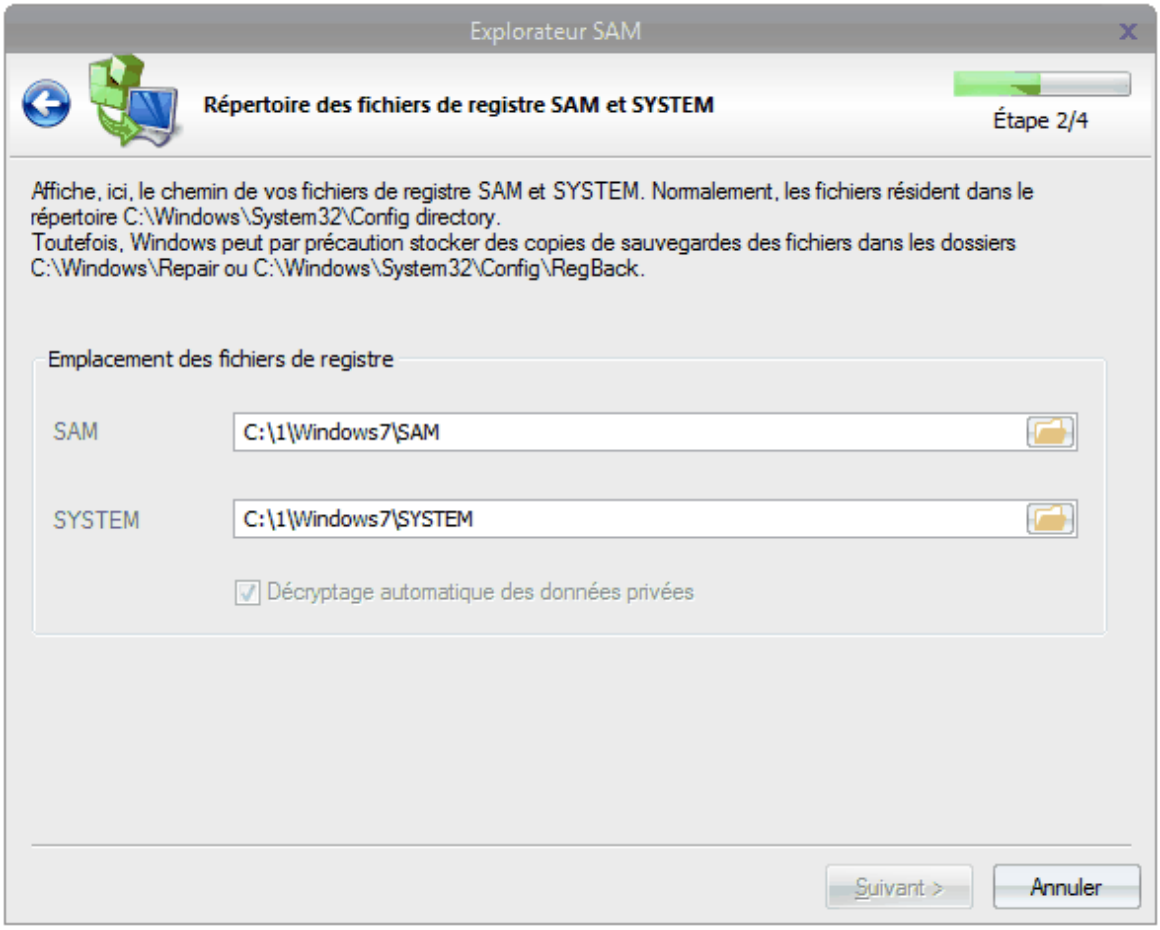
0x01000000 Le compte est activé pour la délégation. Activer un service s'exécutant sous le compte présume de l'identité du client et son authentification comme un utilisateur aux autres serveurs sur le réseau.
0x04000000 Cet objet est un contrôleur de domaine en lecture seul (RODC)

2.7.4.4 Explorateur SAM

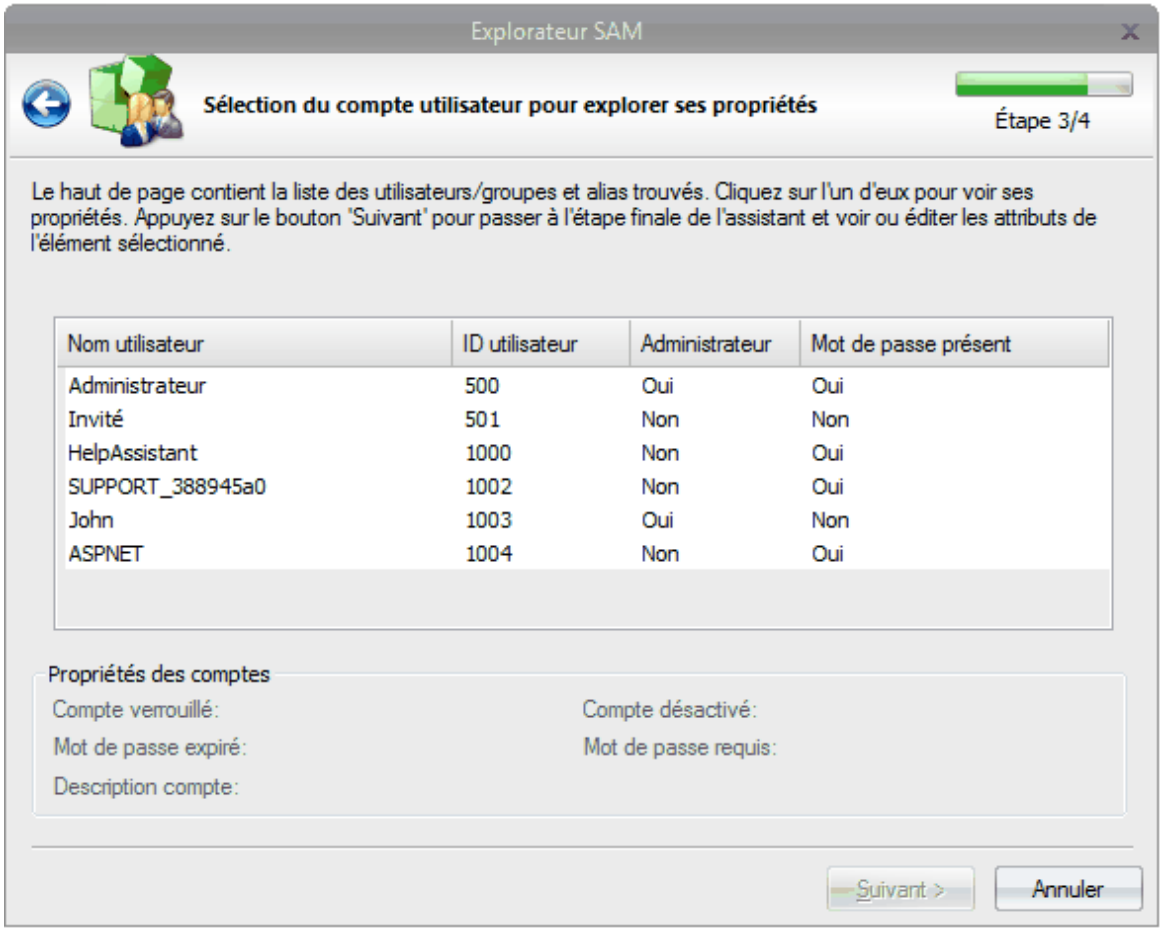
L'explorateur SAM permets de visualiser, analyser et éditer les propriétés et les statistiques des comptes des utilisateurs Windows. SAM, le diminutif de **Security Account Manager**, est un serveur RPC, qui gère la base de données des comptes Windows, stocke les mots de passe/données privées, les groupes de structures logiques de comptes, configure les stratégies de sécurité (ex: stratégie des mots de passe et du blocage de comptes), collecte de statistiques (dernière heure de connexion, nombre de connexion, nombre de connexion ayant échoué, etc.) et contrôle des accès à la base de données.
La base de données SAM est stocké dans la base de registre (sous la clé **HKEY_LOCAL_MACHINE\SAM\SAM**), cette dernière étant inaccessible pour tout le monde, excepté pour le système (administrateurs). Au niveau physique, la base de données SAM est un fichier binaire de la base de registre avec le nom qui lui corresponds, située dans le répertoire %WINDIR%\System32\Config, où %WINDIR% est le répertoire d'installation Windows.

Dans un premier temps, l'assistant vous demandera de sélectionner le type de base de données: locale ou externe. Notez: si vous sélectionnez une base de données locale, pour des raisons de sécurité, l'éditeur ne sera pas disponible, ce qui signifie que la base de données sera ouverte en lecture seule.

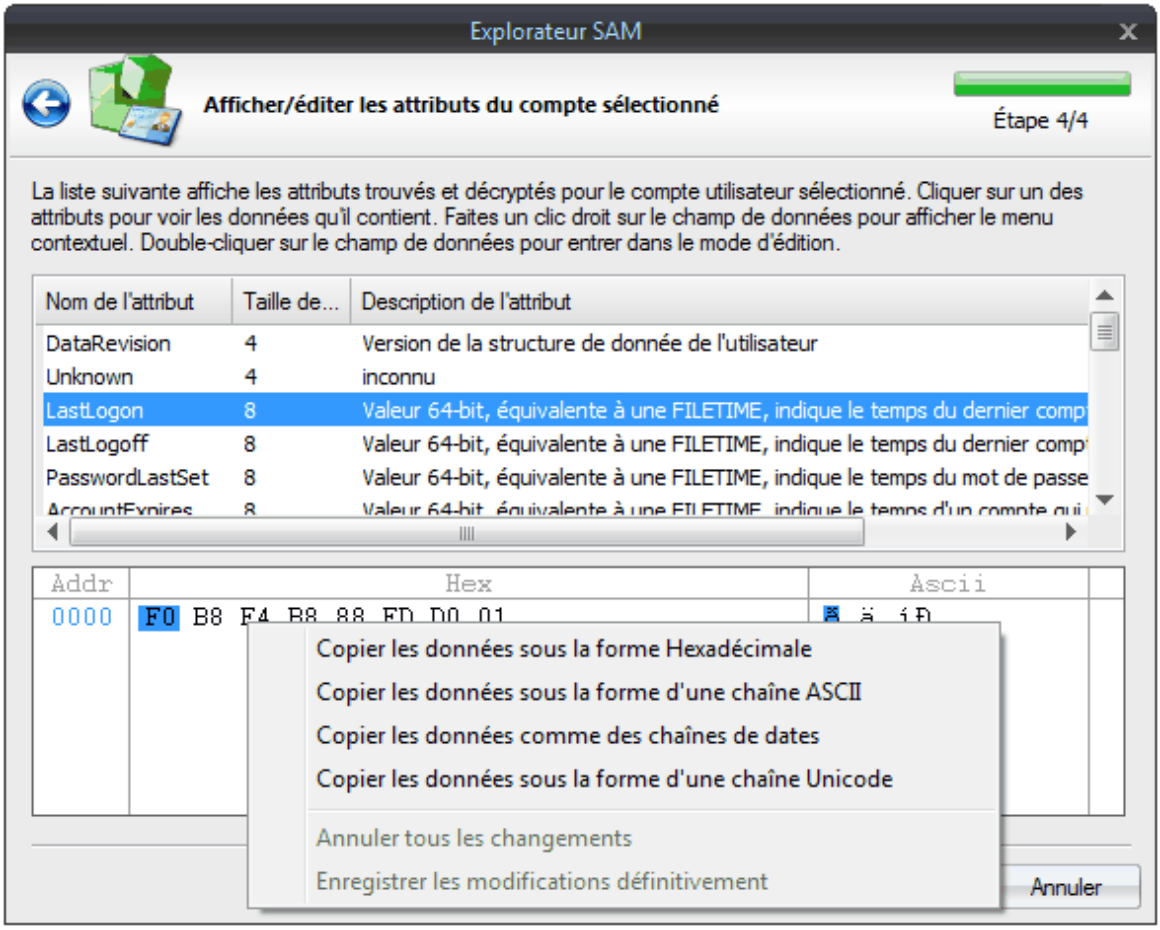
Si vous sélectionnez une base de données SAM d'un ordinateur externe, à la deuxième étape de l'assistant, vous devrez indiquer le chemin de la base de registre SAM et SYSTEM.
Par défaut, les deux fichiers sont localisés dans le répertoire **C:\Windows\System32\Config**. Gardez en tête, que Windows peut par précaution stocker des copies des fichiers de la base de registre dans les dossiers de sauvegarde, comme: **C:\Windows\Repair** ou **C:\Windows\ Config\RegBack**.



A la troisième étape, sélectionnez le compte dont vous voulez obtenir les attributs. Sélectionner l'utilisateur, puis cliquez sur "Suivant".



Affichant une liste des attributs pour le compte sélectionné. La sélection d'un attribut de la liste affiche ses données en bas de l'éditeur. Pour activer l'édition, double-cliquez sur le champ de données, puis une fois terminé, enregistrez les éléments modifiés (avec le menu contextuel).



Description des attributs SAM de comptes

DataRevision
Entier de 32-bits non signé stockant la version de la structure de données. Il est divisé en 2 WORDs: la version principale et la version mineure.

LastLogon
Valeur de 64-bits, équivalent à une FILETIME, indiquant l'heure de la dernière connexion au compte.

LastLogoff
Valeur de 64-bits, équivalent à une FILETIME, indiquant l'heure de la dernière connexion au compte.

PasswordLastSet
Valeur de 64-bits, équivalent à une FILETIME, indiquant l'heure de la dernière mise à jour du mot de passe.

AccountExpires
Valeur de 64-bits, équivalent à une FILETIME, indiquant l'heure où il n'est plus possible de de se connecter à un compte.

LastBadPasswordTime
Valeur de 64-bits, équivalent à une FILETIME, indiquant l'heure où la connexion à un compte a echoué (accès refusé).

UserID
Entier de 32-bits non signé représentant le RID d'un compte.

PrimaryGroupId

Entier de 32-bits non signé représentant l'ID du groupe principal d'un compte.

UserAccountControl
Flag de 32 bits spécifiant les caractéristiques du compte.

CountryCode
Entier de 16-bits non signé représentant le pays de préférence de l'utilisateur. La valeur est le code international du pays. Par exemple, le code du Royaume-Uni de pays, en notation décimale, est de 44.

CodePage
Entier de 16-bits non signé représentant la préférence de code de page pour l'utilisateur. La valeur est le code de page Microsoft.

BadPasswordCount
Entier de 16-bits non signé représentant le nombre de mots de passe erronés essayés.

LogonCount
Entier de 16-bits non signé représentant le nombre de fois que le compte de l'utilisateur s'est connecté.

AdminCount
Entier de 16-bits non signé représentant le compte comme étant membre d'un des groupes administrateurs (direct ou indirect).

OperatorCount
Entier de 16-bits non signé représentant le compte comme étant un membre du groupe utilisateurs.

UserName
Chaîne Unicode qui spécifie le nom du compte utilisateur.

FullName
Chaîne Unicode qui contient le nom complet de l'utilisateur.

AdminComment
Commentaire de l'administrateur associé avec le compte utilisateur.

UserComment
Commentaire de l'utilisateur associé avec le compte utilisateur.

Parameters
Paramètres utilisateur étendus. Les produits Microsoft utilisent ce membre pour stocker des informations de configuration de l'utilisateur.

HomeDirectory
Chaîne Unicode spécifiant le chemin du répertoire racine pour le compte de l'utilisateur.

HomeDirectoryDrive
Indique la lettre de lecteur à attribuer au répertoire racine de l'utilisateur pour l'ouverture de sessions.

ScriptPath
Chaîne Unicode spécifiant le chemin pour le fichier de script d'ouverture de session de l'utilisateur. Le fichier de script peut être un fichier .CMD, un fichier .exe ou un fichier .BAT.

ProfilePath
Chaîne Unicode qui spécifie un chemin d'accès au profil de l'utilisateur.

WorkStations
Chaîne Unicode qui contient les noms (séparés par des virgules) de postes de travail à partir de laquelle l'utilisateur peut se connecter. Jusqu'à huit postes de travail peuvent être spécifiés. Le flag du compte UF_ACCOUNTDISABLE permet de désactiver les connexions de tous les postes de travail de ce compte.

LogonHours

Chaîne de bits 21 octets qui spécifie les périodes durant lesquelles l'utilisateur peut se connecter. Chaque bit représente une heure unique dans la semaine, à l'heure de Greenwich. Le premier bit est le dimanche, de 00 heures à 00h59; le second bit est dimanche, de 01:00 à 01:59; et ainsi de suite. Notez que le bit 0 dans le mot 0 représente dimanche midi de 0:00 à 00h59 seulement si vous êtes dans le fuseau horaire GMT. Dans tous les autres cas, vous devez ajuster les bits selon votre temps de décalage horaire (par exemple, GMT moins 8 heures pour Pacific Standard Time).

Groups
Liste des groupes auxquels le compte d'utilisateur appartient ou pas.

LMHash
Hash du mot de passe LM associé au compte d'utilisateur.

NTHash
Hash du mot de passe NTLM associé au compte d'utilisateur.

LMHistoryHashes
Hachage de l'historique du mot de passe LM du compte de l'utilisateur.

NTHistoryHashes
Hachage de l'historique du mot de passe NTLM du compte de l'utilisateur.

UserHint
Astuce de l'utilisateur (affiché lorsque la connexion échoue).

UserPicture
Image de connexion associée au compte.

2.7.4.5 Utilitaires DPAPI

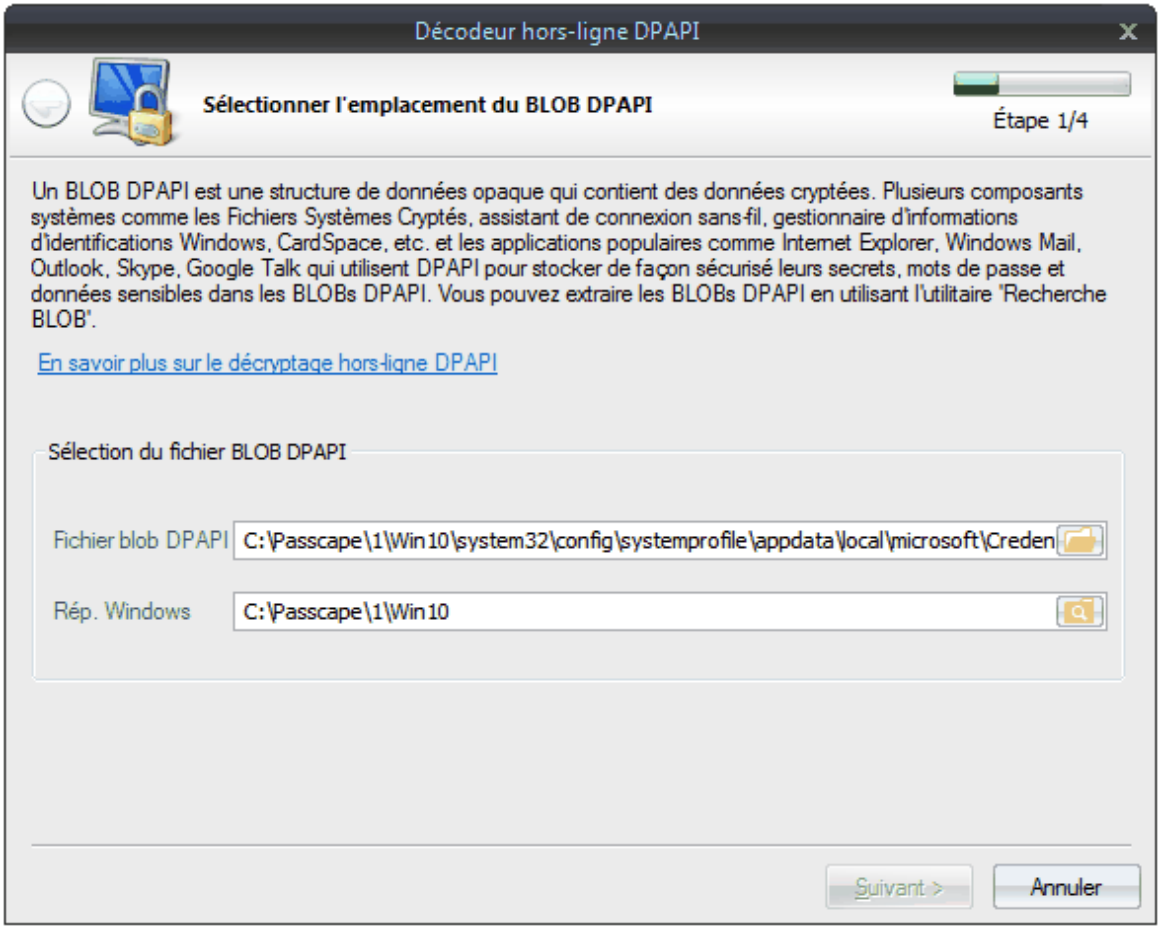
À partir de Windows 2000, Microsoft a commencé à équiper leurs systèmes d'exploitation avec une interface spéciale de protection des données, la protection des données Application Programming Interface (de DPAPI). Actuellement, DPAPI est très largement répandu et utilisé dans de nombreuses applications et sous-systèmes Windows. Par exemple, dans le système de cryptage de fichiers, pour stocker les mots de passe du réseau sans fil, dans le coffre Microsoft et le gestionnaire d'accès, Internet Explorer, Outlook, Skype, Google Chrome, etc. Ce système est devenu populaire parmi les programmeurs d'abord pour sa simplicité d'utilisation, car il se compose de juste un couple de fonctions de cryptage et de décryptage des données: CryptProtectData et CryptUnprotectData. Cependant, malgré son apparente simplicitée, la mise en œuvre technique des DPAPI est assez compliquée.

Passcape Software est le premier dans le monde qui offre un ensemble de 6 outils pour l'analyse et le décryptage des données complètes, chiffrés avec DPAPI. Ces utilitaires vous permettent de:
Décryptage de blobs DPAPI pour tous les comptes
- Recherche de blobs DPAPI sur le disque
- Décryptage de blobs DPAPI cryptés dans le compte SYSTEM (ex mots de passe WiFi)
- Analyze et décryptage de clés des utilisateurs
- Test de mots de passe utilisateur sans extraire les hachages de SAM ou NTDS.DIT
- Décryptage de l'historique de hachages de tous les mots de passes entrés précédemment (sans utiliser SAM ou NTDS.DIT)

2.7.4.5.1 Décryptage de blobs DPAPI

Le décryptage des blobs DPAPI est constitué d'un assistant en quatre étapes.

Sélection d'un fichier blob crypté DPAPI



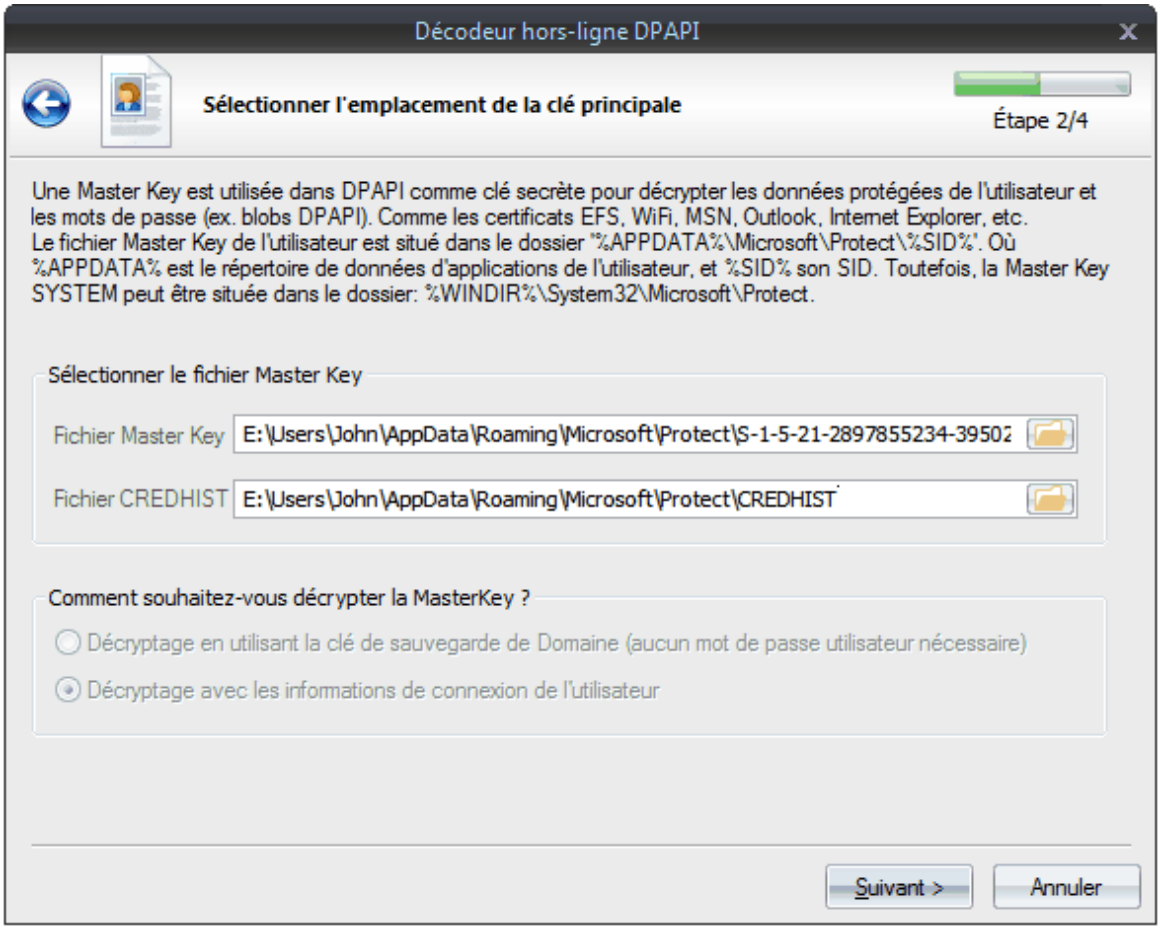
A la première étape, spécifiez le chemin du blob de DPAPI et le répertoire Windows. Il faut savoir que l'actuel DPAPI peut être stocké dans des emplacements différents du système d'exploitation; par exemple, dans des fichiers XML individuels, dans le registre, dans Active Directory; et dans différents formats: binaire, ASCII, UNICODE. Il y a un outil spécial qui permet de localiser, d'extraire et sauver les blobs DPAPI dans des fichiers. Avec cet utilitaire, par exemple, vous pouvez enregistrer tous les blobs DPAPI de registre d'un utilisateur dans des fichiers individuels et les utiliser dans le programme.

Liste des différents emplacements de stockage pour certains objets DPAPI:

- Mots de passe d'Internet Explorer et de Outlook, mots de passe WiFi (XP only): base de registre de l'utilisateur, **%APPDATA%\ntuser.dat**
- Google Chrome: **%LOCALAPPDATA%\Google\Chrome**
- Mots de passe WiFi (Windows Vista et supérieur): **%PROGRAMDATA%\Microsoft\Wlansvc**
- Mots de passe de connexions réseaux (Gestionnaire d'identification Windows): **%LOCALAPPDATA%\Microsoft\Credentials** or **%APPDATA%\Microsoft\Credentials**

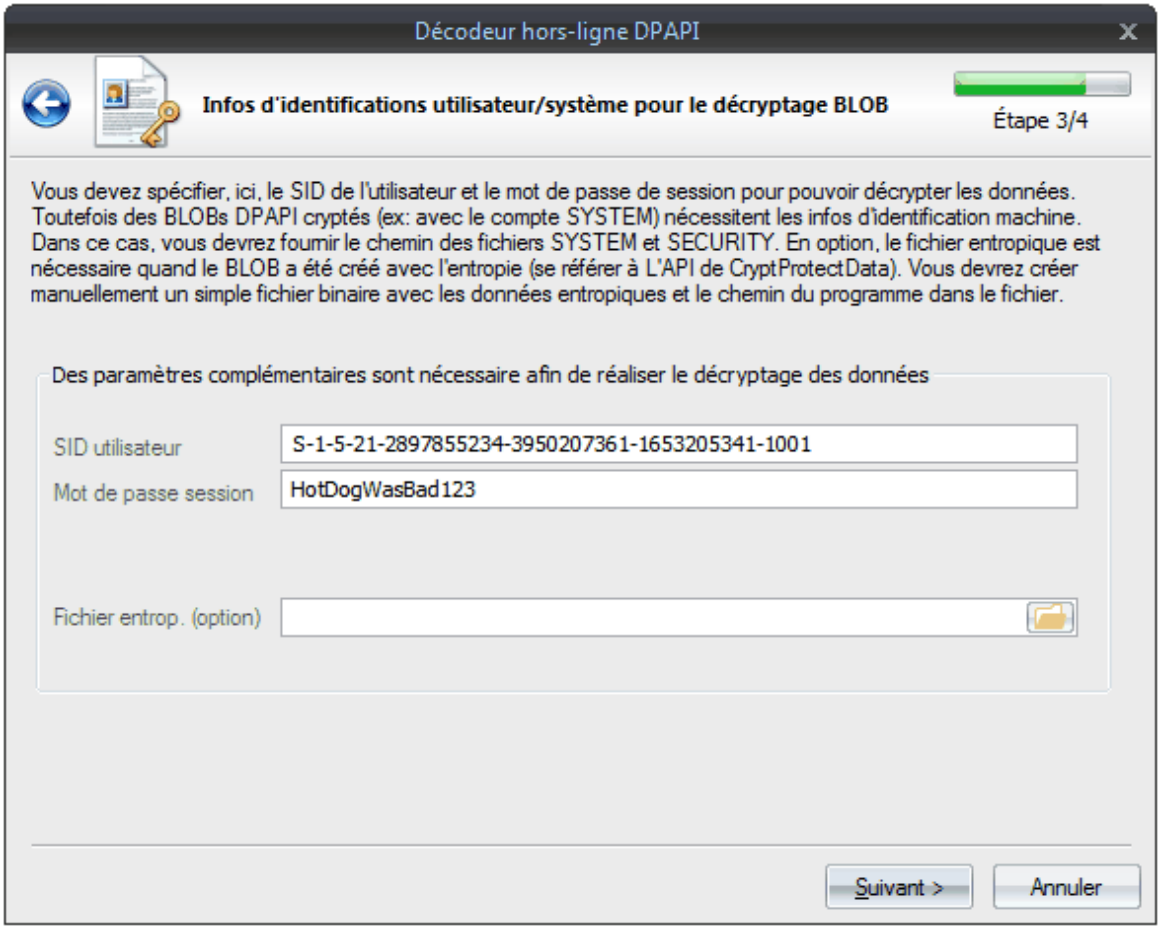
Utilisez l'utilitaire de recherche pour extraire les données DPAPI à partir d'ici.

Sélection de la Master Key



La Master Key est un ensemble de 64 octets aléatoires, utilisée comme clé principale lors du décryptage des blobs DPAPI. La Master Key est cryptée avec le mot de passe de l'utilisateur (ou du mot de passe système dans le cas de la Master Key). La Master Key est toujours localisé dans le répertoire **%APPDATA%\Microsoft\Protect\%SID%**, alors que les Master Keys des comptes du système sont stockées dans le répertoire **%SYSTEMDIR%\Microsoft\Protect**.
Il faut noter qu'il peut y avoir plusieurs Master Keys, et seulement une d'elles est adaptée pour décrypter un objet en particulier, l'un d'entre eux avec le nom stocké dans le blob DPAPI.
Lors de la recherche d'une Master Key, le programme peut supprimer les noms inutiles. Le répertoire **%APPDATA%\Microsoft\Protect** contient aussi le fichier **CREDHIST**, qui est un paramètre optionnel, et dans la majorité des cas n'est pas nécessaire pour le décryptage.

Décryptage de la Master Key

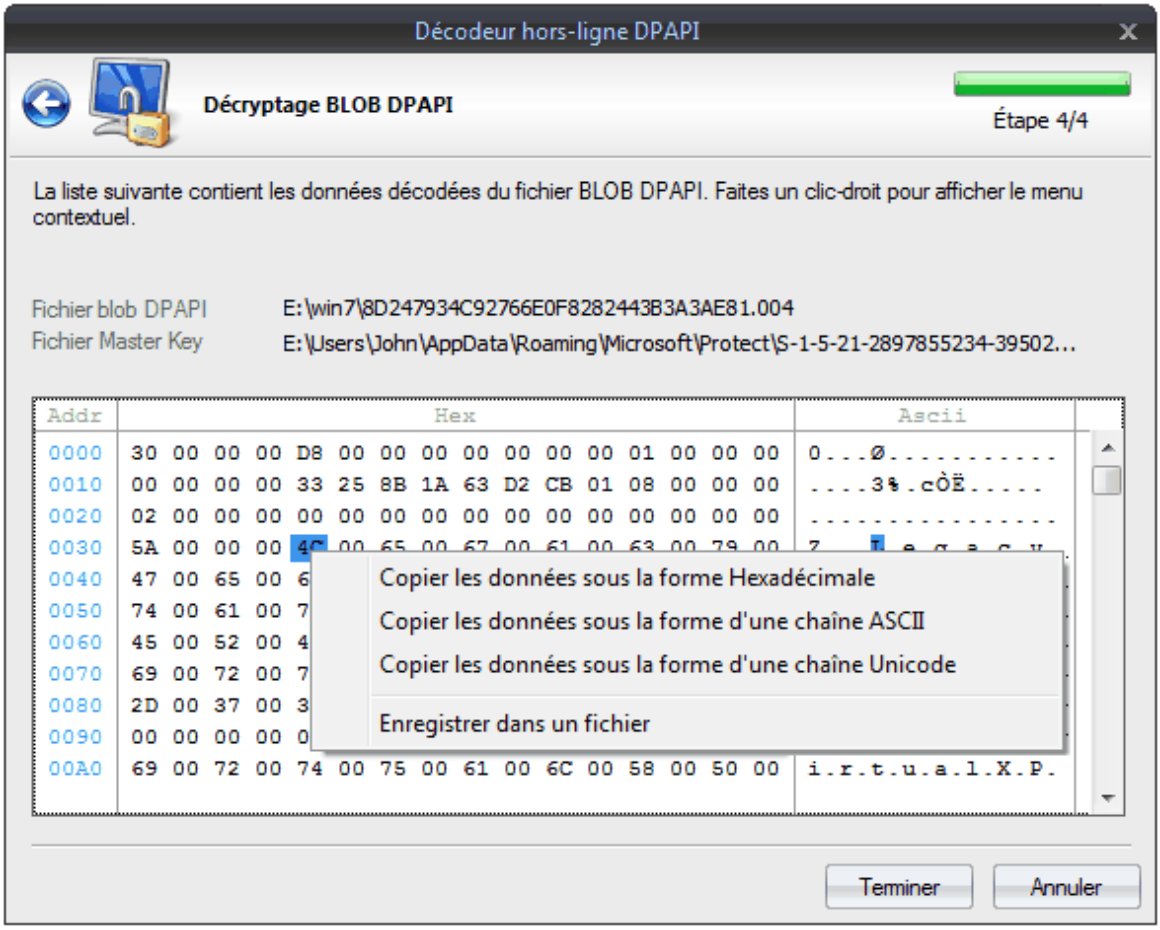


Au moins deux paramètres doivent être définis afin de décrypter la Master Key de l'utilisateur: le mot de passe d'ouverture de session de l'utilisateur et de son identifiant de sécurité (SID), qui est normalement spécifié dans le chemin (répertoire) de la Master Key ou inscrit dans CREDHIST. D'une façon ou l'autre, la Récupération de Mot de passe Windows calcule automatiquement le SID de l'utilisateur. Pour décrypter la Master Key d'un système, comme il a déjà été dit, définir un mot n'a pas de sens, comme le programme récupère toutes les données nécessaires à la récupération à partir de deux fichiers du registre: SYSTEM et SECURITY.
Si entropie supplémentaire a été utilisé lors de la création du blob de DPAPI, vous devez créer manuellement le fichier d'entropie binaire et spécifier le chemin d'accès. Par exemple, lors du cryptage des mots de passe d'Internet Explorer, le nom du site au format Unicode est utilisé comme entropie.

Il est curieux que Windows 2000 a une vulnérabilité critique, qui permet le décryptage de tout (!) blob DPAPI sur un PC, hors domaine, sans nécessairement préciser le mot de passe d'ouverture de session de l'utilisateur !
Par exemple, toutes les données protégées avec DPAPI sont actuellement vulnérables. Ceci est un défaut majeur dans la mise en œuvre de DPAPI, qui est connu par Microsoft; cependant, d'autres systèmes d'exploitation ne présente pas cet inconvénient. Si le flag **CRYPTPROTECT_LOCAL_MACHINE** a été défini dans la fonction CryptProtectData lors de la protection des données, le décryptage de ces données est également possible sans le mot de passe d'ouverture de session de l'utilisateur (par exemple, les mots de passe réseau sans fil). Cependant, ceci est une particularité d'une mise en œuvre de l'interface et pas un bug.

La Récupération de Mot de passe Windows démarre à partir de la version 9.7, utilise de nouvelles vulnérabilités dans la protection de la Master Key DPAPI qui sont détectées par notre entreprise. Ainsi, pour décrypter une Master Key d'un utilisateur de domaine, le mot de passe du propriétaire d'ouverture de session n'est plus nécessaire.

Décryptage des données

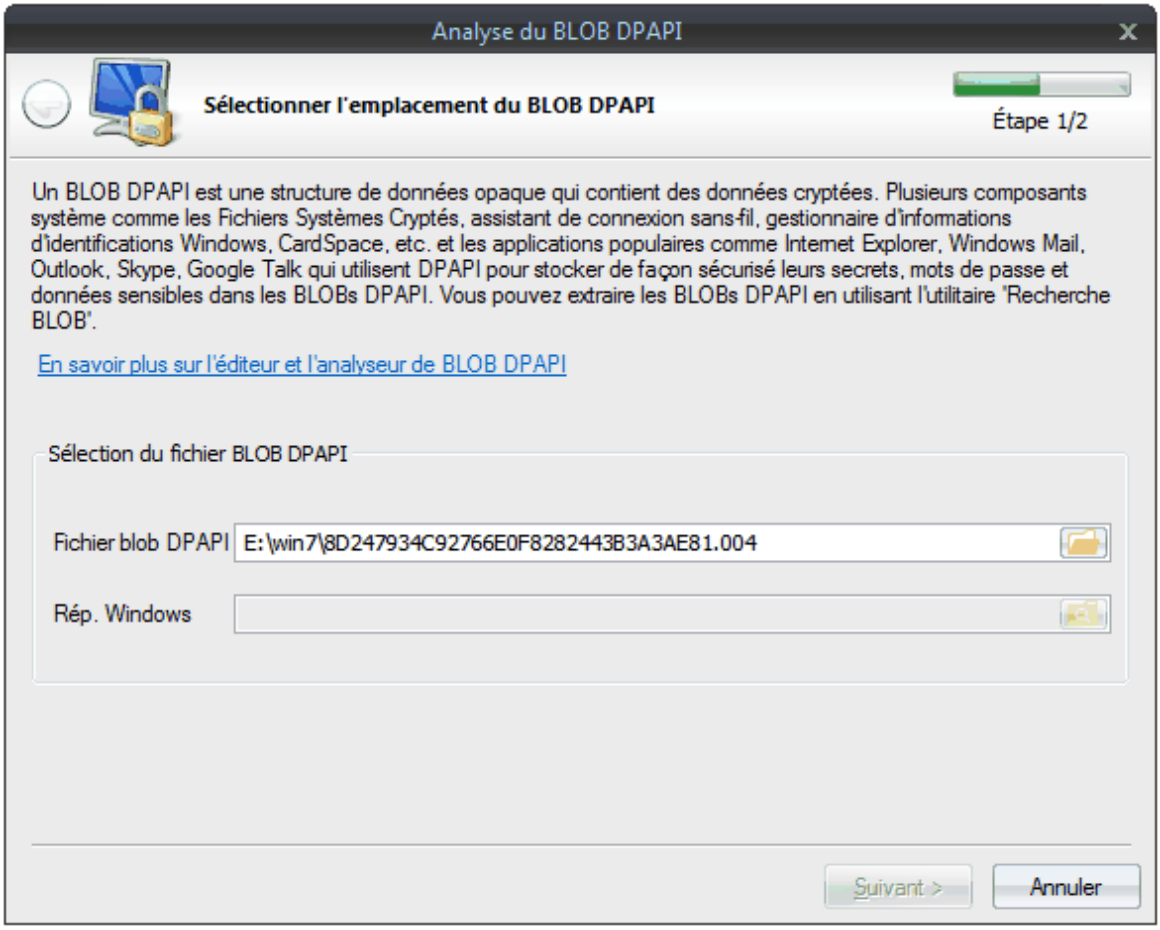


Une fois toutes les informations réunies, la Récupération de Mot de passe Windows effectue le décryptage final des données de blob DPAPI, que vous pouvez ensuite copier dans le presse-papiers ou enregistrer dans un fichier.
Si l'étape finale du décryptage se termine avec une erreur, il est plus que probable que vous n'avez pas défini correctement ou pas du tout, l'entropie supplémentaire. Par exemple, Internet Explorer et Vista FTP Manager utilise la page source où le mot de passe a été saisi comme entropie. Le gestionnaire d'identification de Windows, de manière similaire, utilise certaines constantes de chaîne, et ainsi de suite.

2.7.4.5.2 Analyse de blobs DPAPI

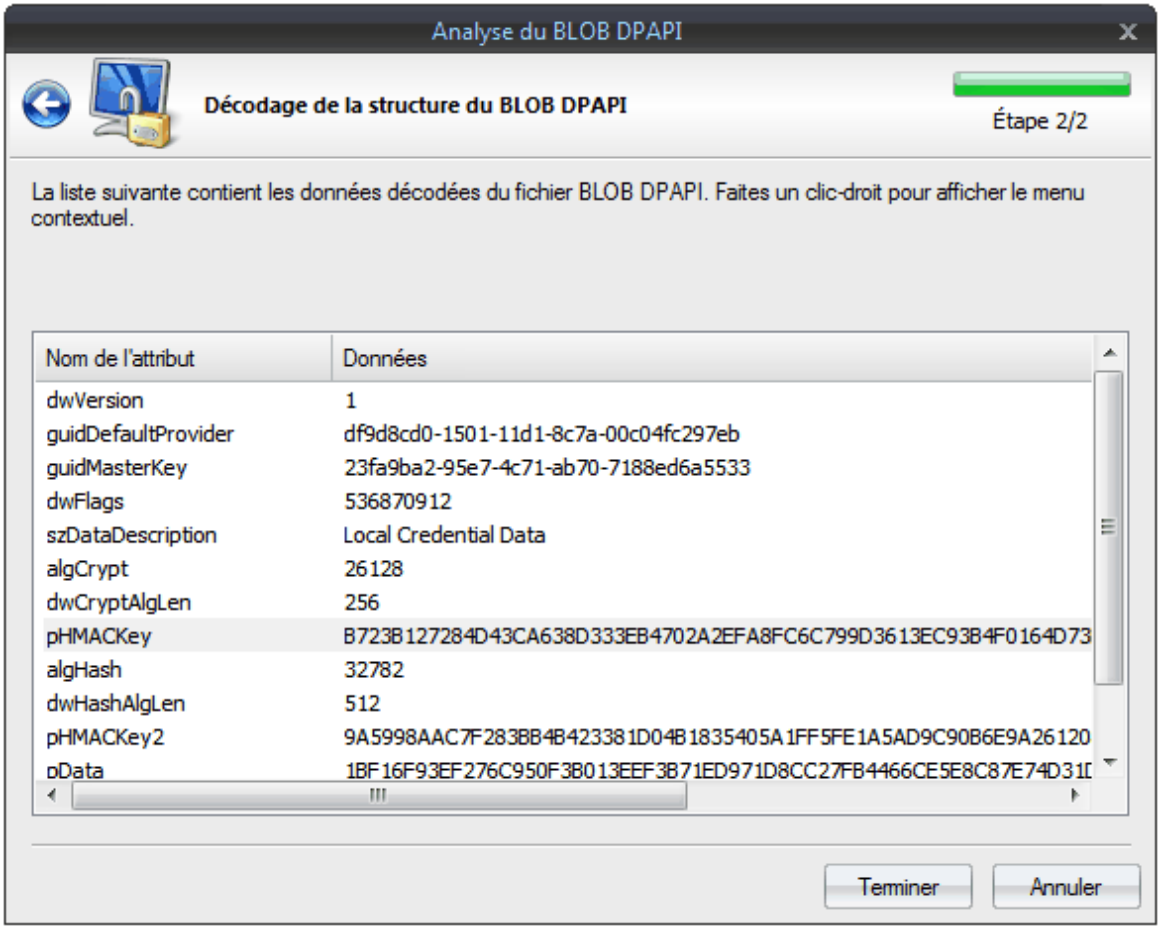
Un blob DPAPI est une structure binaire opaque, qui contient des données privées des applications cryptées utilisant DPAPI. Plusieurs applications Windows et sous-systèmes stockent les mots de passe, les secrets et les données privées dans les blobs DPAPI. Pour créer les fichiers avec les blobs DPAPI (pour de futures analyses), utilisez notre utilitaire de recherche de blobs DPAPI.

Sélection du chemin du blob DPAPI



C'est un fichier qui a été créé par l'outil de recherche de blobs.

Ensuite procédez à l'analyse des données

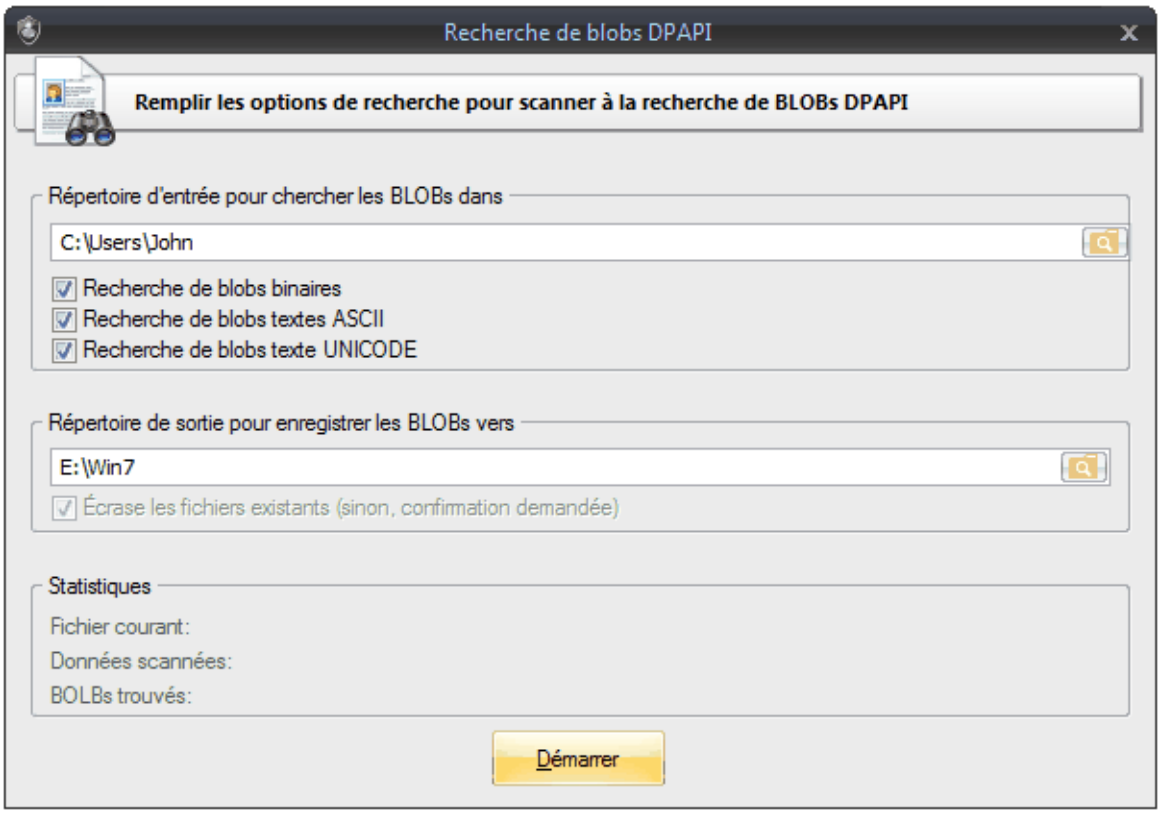


Un blob DPAPI est une structure de données binaire, qui est constituée des attributs consécutifs suivants:

- **dwVersion** — version de la structure de données. Version des données actuelle - 1.
- **guidDefaultProvider** — fournisseur de cryptage de données, utilisé dans les appels de fonctions de cryptage, assure la compatibilité des versions et organise les primitives cryptologiques simples. Par exemple, vous pouvez définir Blowfish ou RC5 comme un chiffrement par bloc. Actuellement, Windows dispose du fournisseur de cryptage par défaut suivant: df9d8cd0-1501-11d1-8c7a-00c04fc297eb, qui correspond à la clé de RegistreHKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\Protect \Providers\df9d8cd0-1501-11d1-8c7a-00c04fc297eb.
- **guidMasterKey** — Master Key GUID, avec laquelle les données sont cryptés. Pour décrypter les données dans le blob DPAPI, en premier vous devez décrypter la Master Key avec avec le nom défini dans la structure binaire guidMasterKey. Seulement une Master Key peut être liée à un blob DPAPI.
- **dwFlags** — divers flags. Par exemple, lorsque le bit 3 est activé, cela indique que le décryptage des données doit être effectué sous le compte SYSTEM. Le bit (dwFlags & 0x20000000) est défini à tout moment.
- **szDataDescription** — descripteur de données, qui est définie par le paramètre facultatif LPCWSTR *szDataDescr* dans la fonction CryptProtectData.
- **algCrypt** — algorithme de cryptage de données. Par défaut, Windows 7 utilise AES 256 (ce qui correspond a 0x6610 en hexadecimal ou 26128 dans la notation decimale), Windows XP - 3DES, Windows 2000 - RC4.
- **dwCryptAlgLen** — longueur de la clé de l'algorithme de chiffrement.
- **pHMACKey** — clé HMAC 1.
- **pSalt** — sel (optionnel).
- **algHash** — algorithme de hachage. Par défaut, Windows 7 utilise SHA 512, Windows XP et Windows 2000 - SHA1.
- **dwHashAlgLen** — longueur hachage dans la fonction de hachage.
- **pHMACKey2** — clé HMAC 2.
- **pData** — données cryptées actuelle.
- **pSignHash** — signature digitale pour la vérification de l'intégrité des données.

2.7.4.5.3 Recherche de blobs DPAPI

La boîte de dialogue de recherche de blob DPAPI est plutôt trivial. Tout ce que vous devez spécifier est le répertoire source, que le programme devra chercher pour les blobs DPAPI, et le répertoire de destination, où les blobs trouvés sont stockés. Le programme recherche les blobs binaires et textes.



Exemple d'un chemin, où vous pouvez trouvez des fichiers, contenant des blobs DPAPI binaires:
C:\Users\John\AppData\Roaming\Microsoft\Credentials

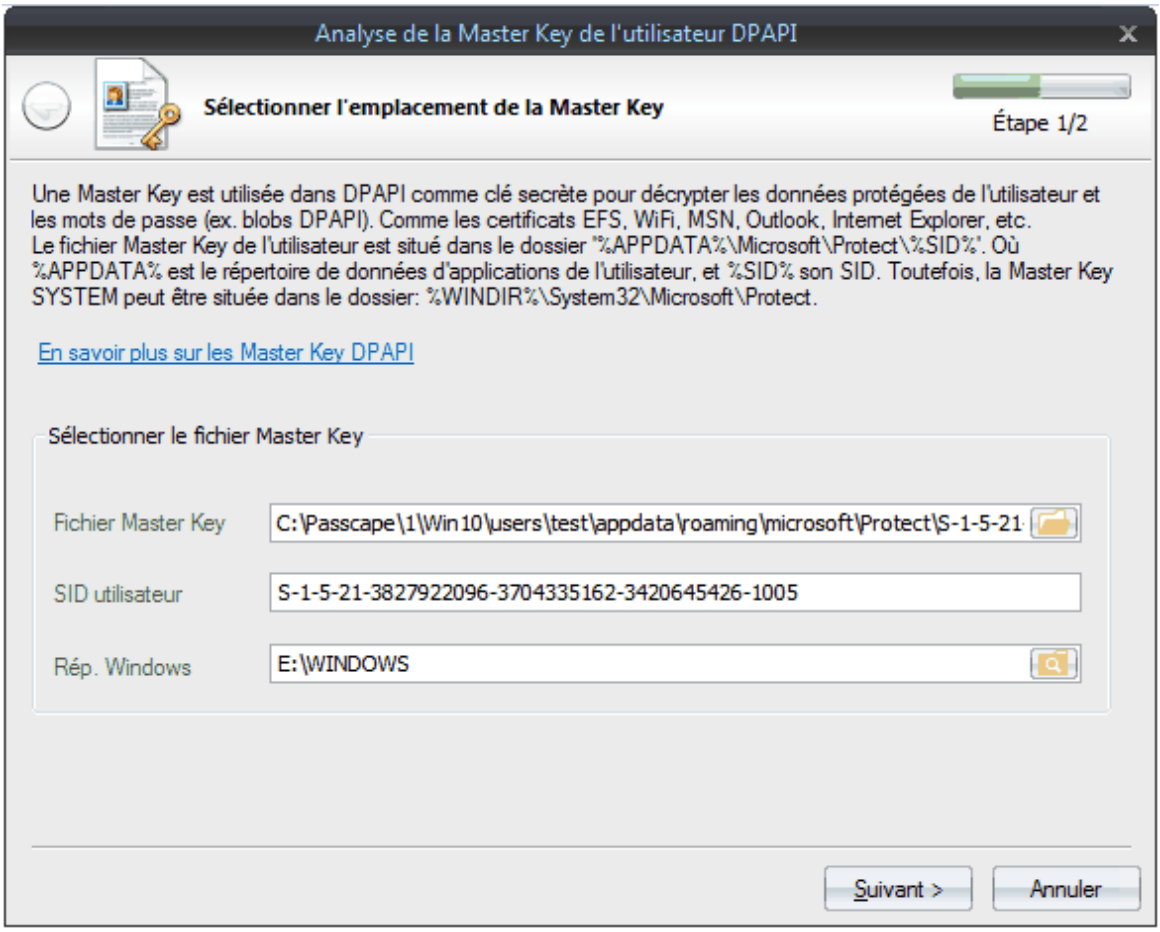
Exemple d'un chemin, où vous pouvez trouvez des fichiers, contenant des blobs DPAPI textes:
C:\ProgramData\Microsoft\Wlansvc

Gardez à l'esprit que si vous rechercher des blobs dans le registre de l'utilisateur ou dans la bse de données de l'Active Directory, vous devez en premier sauvegarder les fichiers dans un autre répertoire.

2.7.4.5.4 Analyse de Master Key

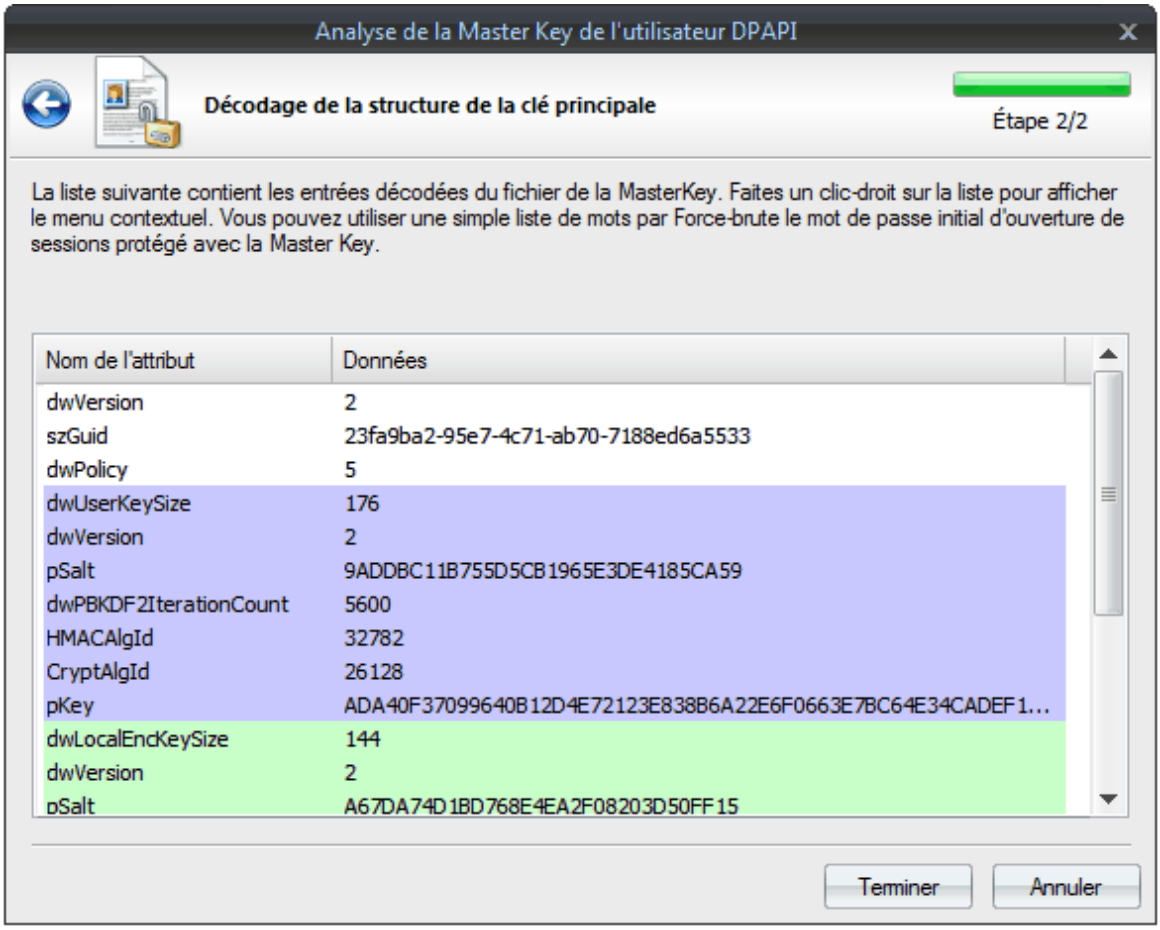
La Master Key est un jeu de 64 octets de données, qui sont utilisés comme clé primaire lors du décryptage d'un blob de DPAPI. La Master Key d'un utilisateur est cryptée avec le mot de passe d'ouverture de session de l'utilisateur.

Définissez le chemin du fichier de la Master Key et spécifiez le SID de l'utilisateur, que le programme calcule, normalement automatiquement, à partir du chemin d'accès spécifié.



Toutes les Master Keys des utilisateurs sont localisées dans le répertoire **%APPDATA%\Microsoft\Protect\%SID%**.
Par exemple, C:\Users\John\AppData\Roaming\Microsoft\Protect\S-1-5-21-2897849034-3956381361-16091305341-1001\23ab9bc1-9397-4cb1-ab74-7166ed6a8713
Les Master Keys du Système sont stockées dans le répertoire **%SYSTEMDIR%\Microsoft\Protect.**

Analyse de la Master Key



Le fichier de la Master Key file est une structure binaire, qui est constituée d'un en-tête d'un service et de quatre emplacements, à savoir:
la Master Key de l'utilisateur actuel, la clé de cryptage locale (pour la suppression de la protection de clé de sauvegarde locale), la clé de sauvegarde locale (sous Windows 2000) ou CREDHIST GUID (sous Windows XP et supérieur) et la clé de sauvegarde de domaine.

La liste de la structure de la Master Key est constituée des attributs des noms (ex: champs binaires) et les valeurs qui correspondent avec eux. Chaque section est de couleur unique:
- champ avec les attributs d'en-têtes
- emplacement avec les attributs de la Master de l'utilisateur
- emplacement avec les attributs de la Clé de Cryptage Locale
- emplacement avec la Clé de Sauvegarde Locale ou l'attribut GUID du fichier CREDHIST
- emplacement avec les attributs de la Clé de Sauvegarde de Domaine

Voyant, maintenant, un peu plus de détails:

Header attributes
- **dwVersion** - version du fichier de la Master Key.
- **szGuid** - GUID texte de la Master Key. Il corresponds normalement au nom du fichier.
- **dwPolicy** - divers flags. Par exemple, si le bit 3 est actif, le programme utilise le hachage SHA1 du mot de passe lors du décryptage du mot de passe de l'utilisateur; sinon, il utilisera le MD4. Ainsi, dans Windows 2000 ce bit est toujours effacé. L'activation du bit 2 nous informe que la sauvegarde est exige pour la Master Key.
-

Attributs de la Master Key de l'utilisateur
- **dwUserKeySize** - longueur de l'emplacement.
- **dwVersion** - version de la structure de données. La version 1 implémente seulement l'attribut de 'salt'.
- **pSalt** - pSalt - 'salt', par ex: 16 octets aléatoire de données, impliqué dans le décryptage de la Master Key et la prévention des attaques de données en utilisant des tables Arc en ciel.
- **dwPBKDF2IterationCount** - itérations dans la fonction pour générer la clé de cryptage PBKDF2.
- **HMACAlgId** - identifiant de l'algorithme de hachage.

- **CryptAlgId** - algorithme de cryptage utilisé.
- **pKey** - Master Key crypté de l'utilisateur.

Local Encryption Key attributes
- **dwLocalEncKeySize** - longueur de l'emplacement.
- **dwVersion** - version de la structure de données. Win2K utilise seulement un attribut de 'salt'.
- **pSalt** - 'salt'.
- **dwPBKDF2IterationCount** - itérations dans la fonction pour générer la clé de cryptage PBKDF2.
- **HMACAlgId** - identifiant de l'algorithme de hachage.
- **CryptAlgId** - algorithme de cryptage utilisé.
- **pKey** - Clé de Cryptage Locale, utilisée pour le décryptage de la Clé de Sauvegarde Locale dans Windows 2000.

Local Backup Key attributes (Windows 2000)
- **dwLocalKeySize** - longueur de l'emplacement.
- **dwVersion** - version de la structure de données.
- **pSalt** - 'salt'.
- **pKey** - Clé de Backup Local cryptée.

CREDHIST file's GUID attributes (Windows XP et supérieur)
- **dwLocalKeySize** - longueur de l'emplacement.
- **dwVersion** - version de la structure de données.
- **guidCredHist** - Identifiant du fichier binaire CREDHIST.

Domain Backup Key attributes
- **dwDomainKeySize** - longueur de l'emplacement.
- **dwVersion** - version de la structure de données.
- **pSalt** - 16 octets aléatoire de données, impliqué dans le décryptage de la Master Key et la prévention des attaques de données en utilisant des tables Arc en ciel.
- **dwPBKDF2IterationCount** - itérations dans la fonction pour générer la clé de cryptage PBKDF2.
- **HMACAlgId** - identifiant de l'algorithme de hachage.
- **CryptAlgId** - algorithme de cryptage utilisé.
- **pKey** - Clé de Backup de Domaine cryptée. Son décryptage nécessite la clé privée RSA du contrôleur de Domaine, stockée dans la base de données de l'Active Directory.

Pour décrypter la Master Key de l'utilisateur, vous devez connaître le mot de passe d'ouverture de session. A partir du menu contextuel, vous pouvez vérifier le mot de passe de la Master Key et même essayer d'en deviner un en utilisant un dictionnaire. Cependant, ne vous flattez pas trop. Tandis que dans Windows 2000, la vitesse de recherche varie en dizaines et même en centaines de milliers de mots de passe par seconde, dans Windows 7, le nombre varie seulement de quelques éléments. Voir le tableau ci-dessous (la vitesse est mesurée pour un single-cœur du processeur Intel Q8400 à 2,66 GHz).

Système d'exploitation	Algorithme de cryptage	Type de hachage	PKCS#5 PBKDF2 rounds	Vitesse de test du mot de passe (mp/sec)
Windows 2000	RC4	SHA1	1	**95000**
Windows XP	3DES	SHA1	4000	**76**
Windows Vista	3DES	SHA1	24000	**12**
Windows 7	AES256	SHA512	5600	**10**

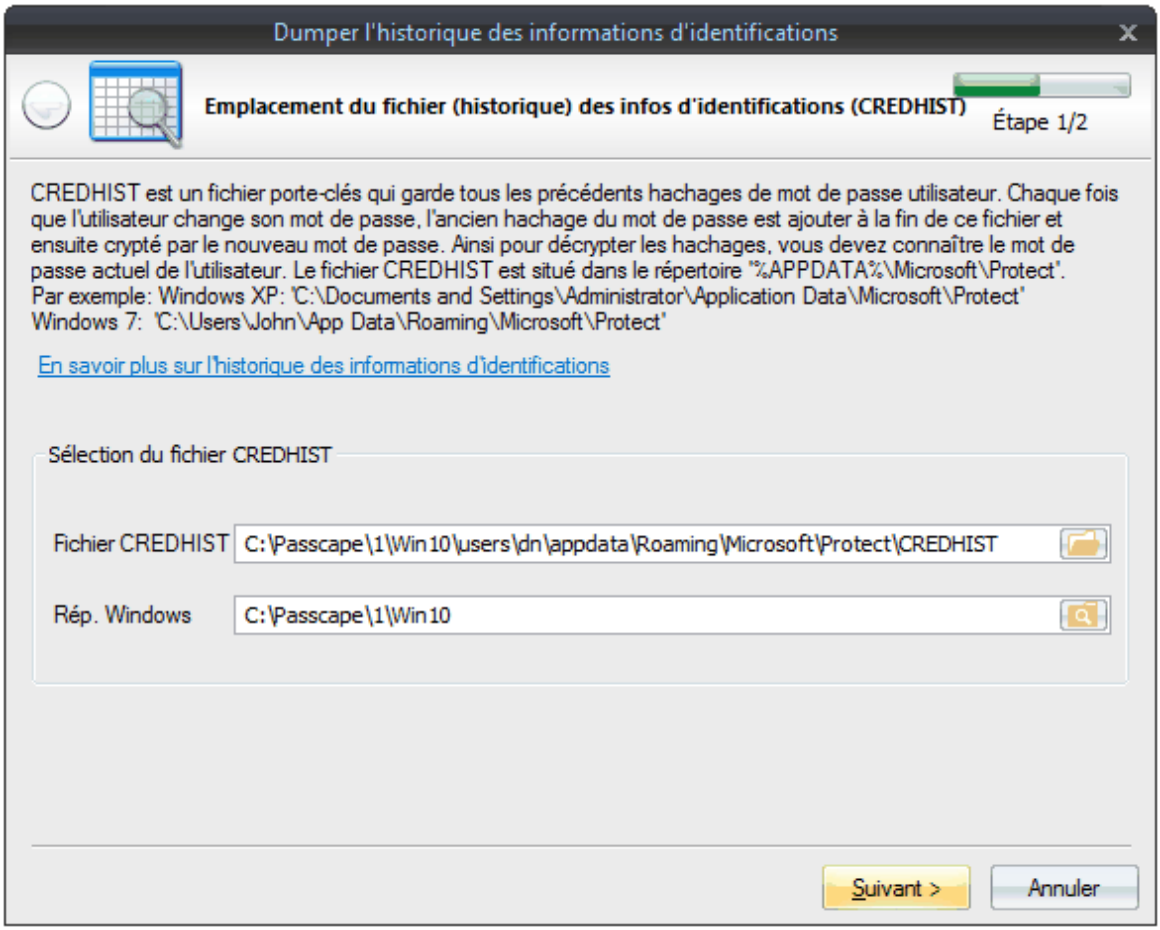
2.7.4.5.5 Dump de hachages de l'historique des infos d'identifications d'utilisateur

En raison des spécificités de l'implémentation DPAPI, pour garantir le décryptage complet de tous les blobs DPAPI, Windows doit stocker tous les mots de passe des utilisateurs dans le système. L'historique de mots de passe des utilisateurs est stocké dans le fichier suivant: **%APPDATA%\Microsoft\Protect\CREDHIST**

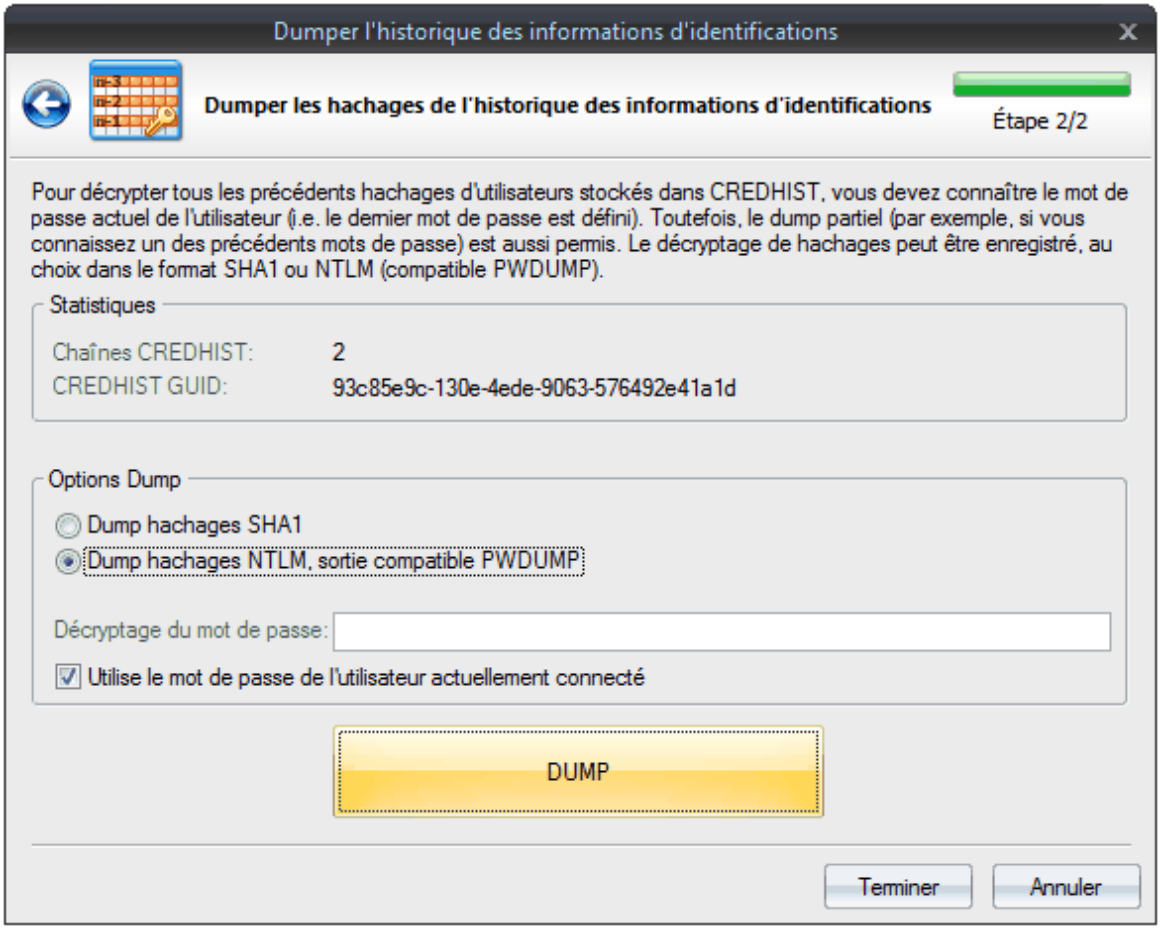
Tous les anciens mots de passe des utilisateurs (avec données de service) sont stockés en pairs de hachages: **SHA1** et **NTLM**. De plus, afin de décrypter la dernière paire, vous devez connaître le hachage du mot de passe de l'utilisateur actuel, pour décrypter les précédents hachages, et vous en avez besoin pour décrypter la dernière paire, et ainsi de suite.

Windows Password Recovery est le premier utilitaire dans le monde, qui permets de décrypter les hachages de l'historique de mots de passe à partir des fichiers CREDHIST.

Pour réaliser cela, à la première étape de l'assistant, vous devez indiquez le chemin de votre fichier CREDHIST et du répertoire Windows.



Ensuite vous pouvez décrypter et sauvegarder les hachages provenant du fichier CREDHIST, dans un fichier de type PWDUMP texte, si la sauvegarde **NTLM** est sélectionnée, ou dans un fichier texte si le format de hachage **SHA1** est choisi.



Il est important de savoir que pour pouvoir décrypter les hachages CREDHIST, vous devez connaître le mot de passe de l'utilisateur actuel. Si vous décryptez CREDHIST d'un utilisateur actuellement connecté, assurez-vous de cochez la case correspondante pour cette option.
Dans ce cas, vous n'aurez pas besoin de saisir le mot de passe de décryptage, il sera récupéré à partir du cache système.

Le programme supporte le dump partiel des hachages de l'historique. Cela signifie que si le mot de passe de l'utilisateur actuel est inconnu, mais au moins l'un des anciens mots de passe est disponible, le programme peut décrypter les mots de passe de l'utilisateur utilisé plus tôt, par ex. avant que l'ancien mot de passe soit saisi.

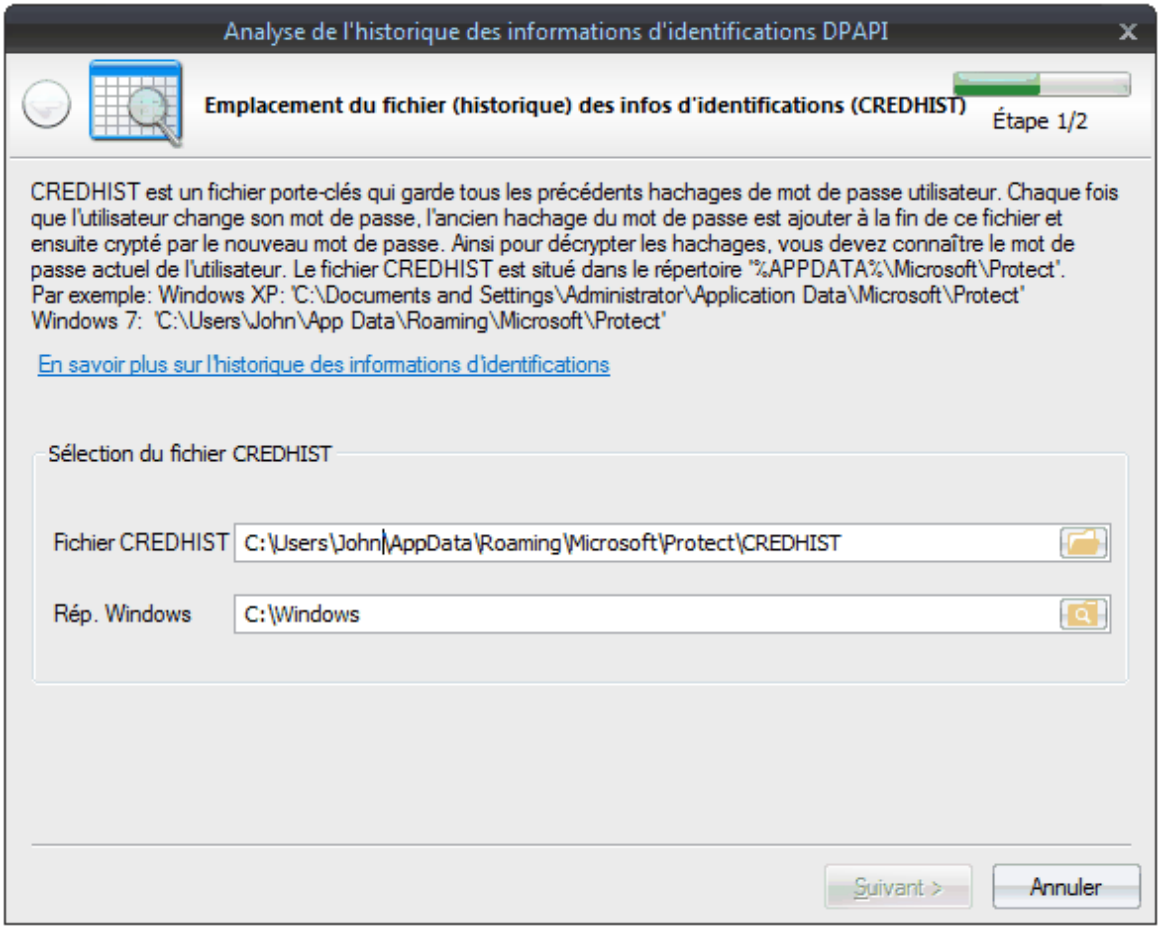
Faites attention, dans Windows 8 et les OS supérieurs, les hachages dumpés pour les comptes LiveID ne correspondent pas à ceux dérivés des mots de passe LiveID de connexion.

2.7.4.5.6 Analyse de l'historique des infos d'identifications

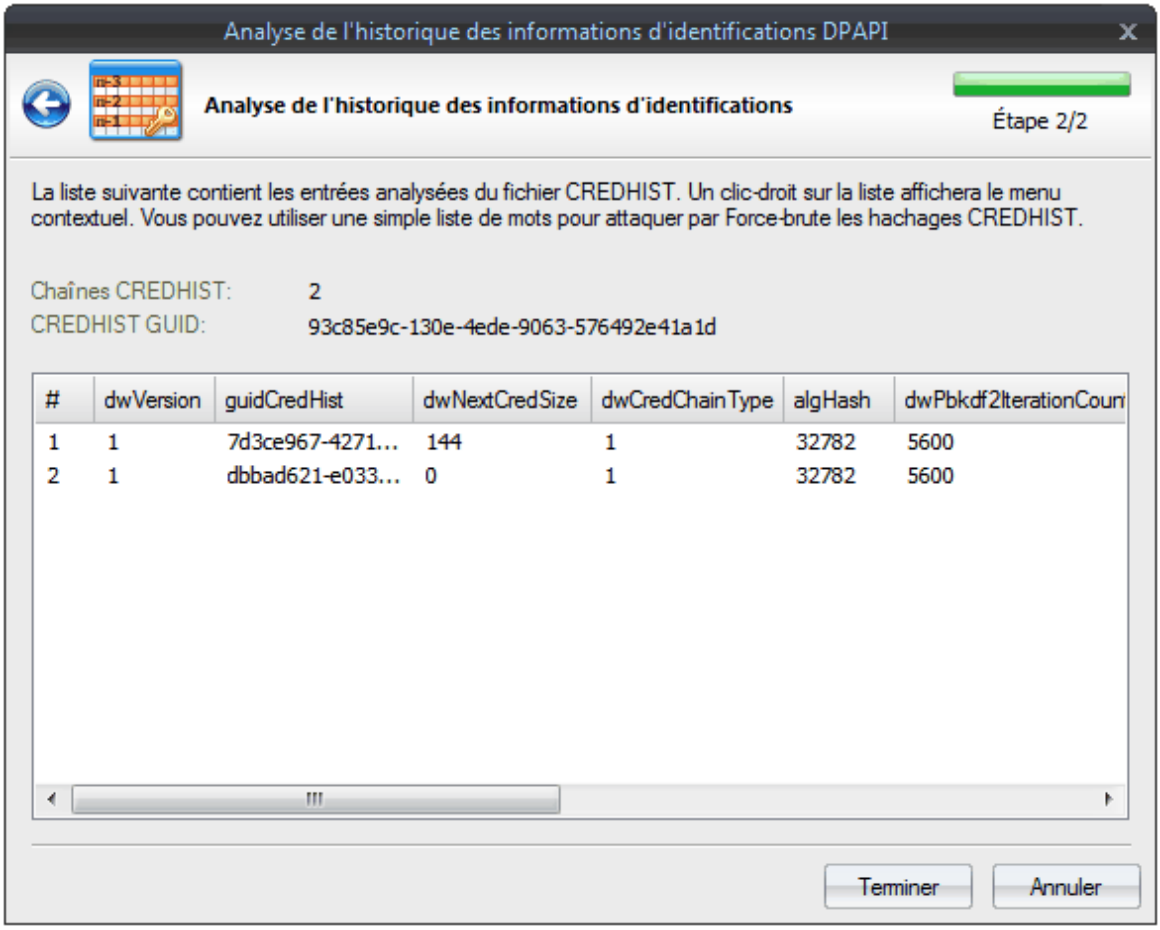
CREDHIST est un fichier d'historique de mots de passe, construit sous la forme d'une chaîne, ou chaque lien représente les hachages des anciens mots de passe.
Chaque fois que l'utilisateur change le mot de passe, l'ancien hachage du mot de passe est ajouté au fichier et crypté avec le nouveau de passe.
Cependant, pour décrypter tous les hachages dans une chaîne, vous devez connaître le mot de passe de l'utilisateur actuel.

Concernant les hachages, les chaînes stockent d'autres données de service, lesquelles sont aussi analysées par cet utilitaire.

Sélection du fichier CREDHIST



Analyse du contenu



Dans cette capture d'écran, on peut voir que l'identificateur CREDHIST est 93c85e9c-130e-4ede-9063-576492e41a1d. C'est l'identificateur (GUID) des Master Keys des utilisateurs qui sont liées au propriétaire des données. Le nombre de liens dans la chaîne de hachages est de 2.

La liste suivante contient tous les attributs et leurs valeurs pour chaque lien de votre CREDHIST.

Description des attributs

- **dwVersion** - version de la structure de données
- **guidLink** - lien actuel de l'identifiant unique
- **dwNextLinkSize** - taille du prochain lien
- **dwLinkType** - type de lien
- **algHash** - algorithme de hachage utilisé pour le décryptage du lien
- **dwPbkdf2IterationCount** - itérations dans la routine pour générer la clé PKCS#5 PBKDF2
- **dwSidSize** - taille du descripteur de sécurité propriétaire (SID)
- **algCrypt** - algorithme de cryptage
- **dwShaHashSize** - taille du hachage SHA1
- **dwNtHashSize** - taille du hachage NTLM
- **pSalt** - "salt" utilisé pour le cryptage
- **sidUser** - SID du propriétaire des données
- **pShaHash** - hachage SHA1
- **pNtHash** - hachage NTLM

Pour découvrir le mot de passe d'origine CREDHIST, faites un clic-droit sur les attributs puis sélectionnez '*Utiliser la liste de mots pour tester le mot de passe...*' dans le menu contextuel qui s'affiche. Vous pouvez valider un mot de passe pour la ligne ou tous ceux sélectionnés. Le temps de validation s'accroît proportionnellement au nombre d'enregistrements (par ex: le nombre de liens).

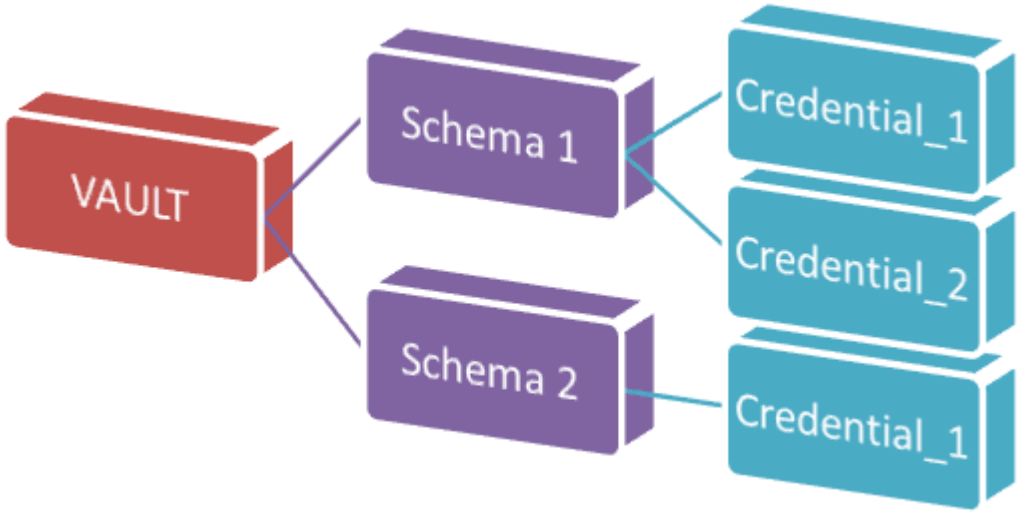
La table de comparaison, ci dessous, montre des vitesses de recherche de mots de passe CREDHIST. La vitesse est mesurée avec un CPU simple cœur Intel Q8400 2.66GHz pour des configurations d'OS par défaut. 'par exemple, dans Windows 7 le nombre d'itérations dans PBKDF2 peut être différent).

Système d'exploitation OS	Algorithme de cryptage	Type de hachage	Compteur PBKDF2	Vitesse de test de mot de passe (mdp/s)
Windows XP	3DES	SHA1	4000	**76**
Windows Vista	3DES	SHA1	24000	**12**
Windows 7	AES256	SHA512	5600	**10**

2.7.4.6 Explorateur du Coffre Windows

Tout sur le Coffre Windows

Le Coffre Windows est un espace de stockage protégé de l'utilisateur ou du système pour les secrets, les mots de passe, les clés réseaux, les mots de passe Web et d'autres informations confidentielles. Les données stockées dans le Coffre Windows sont structurées et composées d'un ensemble d'enregistrements appartenant à une structure particulière de Coffre (voir l'image suivante).



Au niveau physique, le Coffre est un répertoire du disque contenant les fichiers suivants:
Policy.vpol - jeu de clés de cryptage pour les enregistrements du Coffre (infos d'identifications). Ces clés peuvent être protégées en utilisant deux méthodes différentes: soit par le DPAPI ou avec un mot de passe utilisateur spécifique. la dernière méthode de protection n'est pas utilisée dans Windows 8 et n'est pas habituellement supportée par le logicielle.
<GUID>.vsch - le schéma du Coffre contient la description des données, des flags et autres informations système.
<GUID>.vcrd - Vault credential stocke les données cryptées associées à un schéma particulier. Les données peuvent être ou normalement constituées de plusieurs champs. La description de ces champs est stockée dans <GUID>.vsch.

Explorateur de Coffre Windows

Explorateur de Coffre Windows est un utilitaire pour l'analyse hors-ligne et le décryptage d'informations d'identifications du Coffre. L'assistant de décryptage découpe l'ensemble du processus en les différentes étapes suivantes:
1. Sélection du répertoire du Coffre
2. Sélection de la Master Key des utilisateurs et du système
3. Décryptage de la Master Key - sélection des fichiers de la base de registre et autres informations nécessaires pour le décryptage
4. Sélection du schéma du Coffre
5. Sélection de l'enregistrement correspondant au schéma choisi
6. Décryptage de l'info d'identification sélectionnée du Coffre

Sélection du répertoire du Coffre

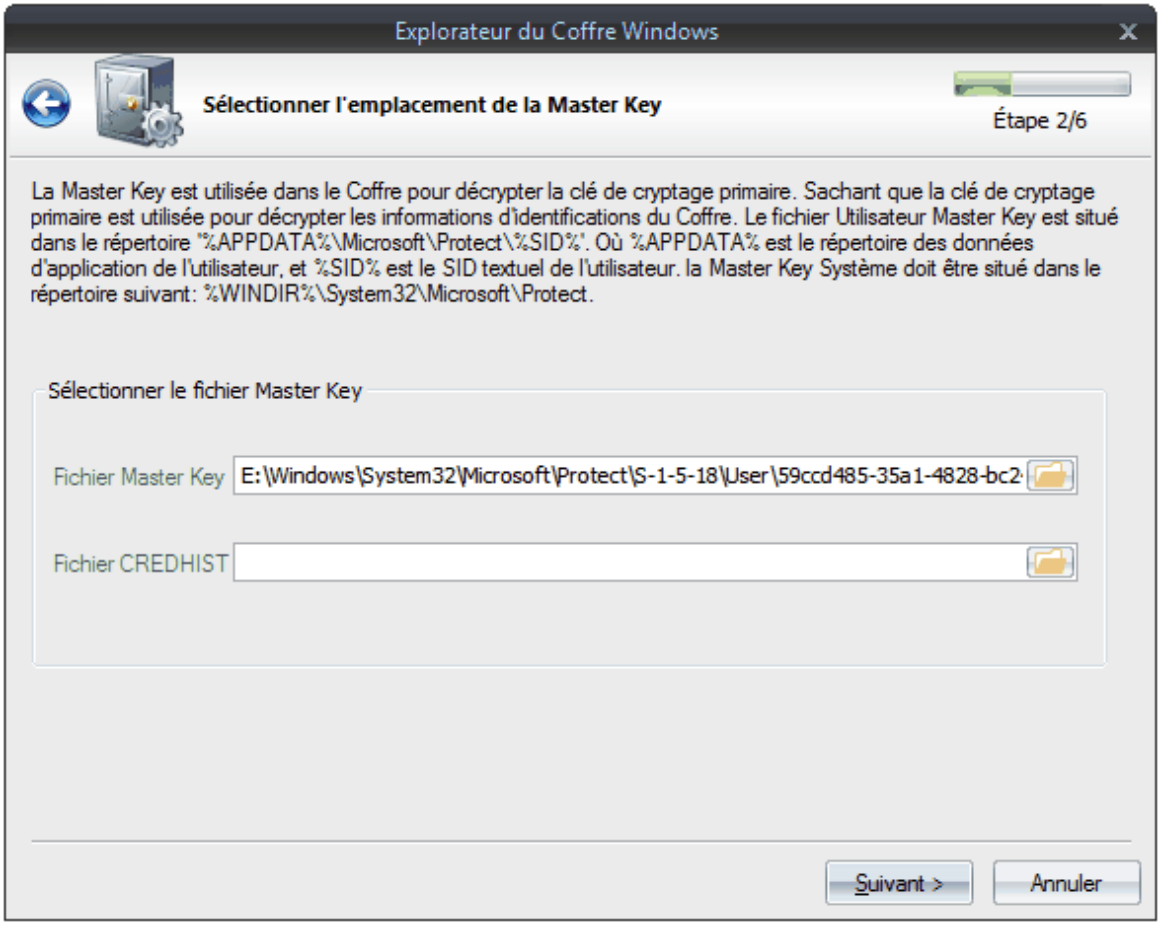
Il y a deux types de Coffre de stockage: système et utilisateur.

Le Coffre de l'utilisateur peut être situé dans les répertoires suivants:
<USER_APP_DATA>\Microsoft\Vault\<GUID>
<USER_LOCAL_APP_DATA>\Microsoft\Vault\<GUID>
Exemples de répertoires:
C:\Users\John\AppData\Local\Microsoft\Vault\18289F5D-9783-43EC-A50D-52DA022B046E
C:\Users\Helen\AppData\Roaming\Microsoft\Vault\4BF4C442-9B8A-41A0-B380-DD4A704DDB28

L'emplacement par défaut du Coffre du système est:
<SYSTEM_APP_DATA>\Microsoft\Vault\<GUID>
<SYSTEM_LOCAL_APP_DATA>\Microsoft\Vault\<GUID>
<PROGRAM_DATA>\Microsoft\Vault\<GUID>
Exemples de répertoires:
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

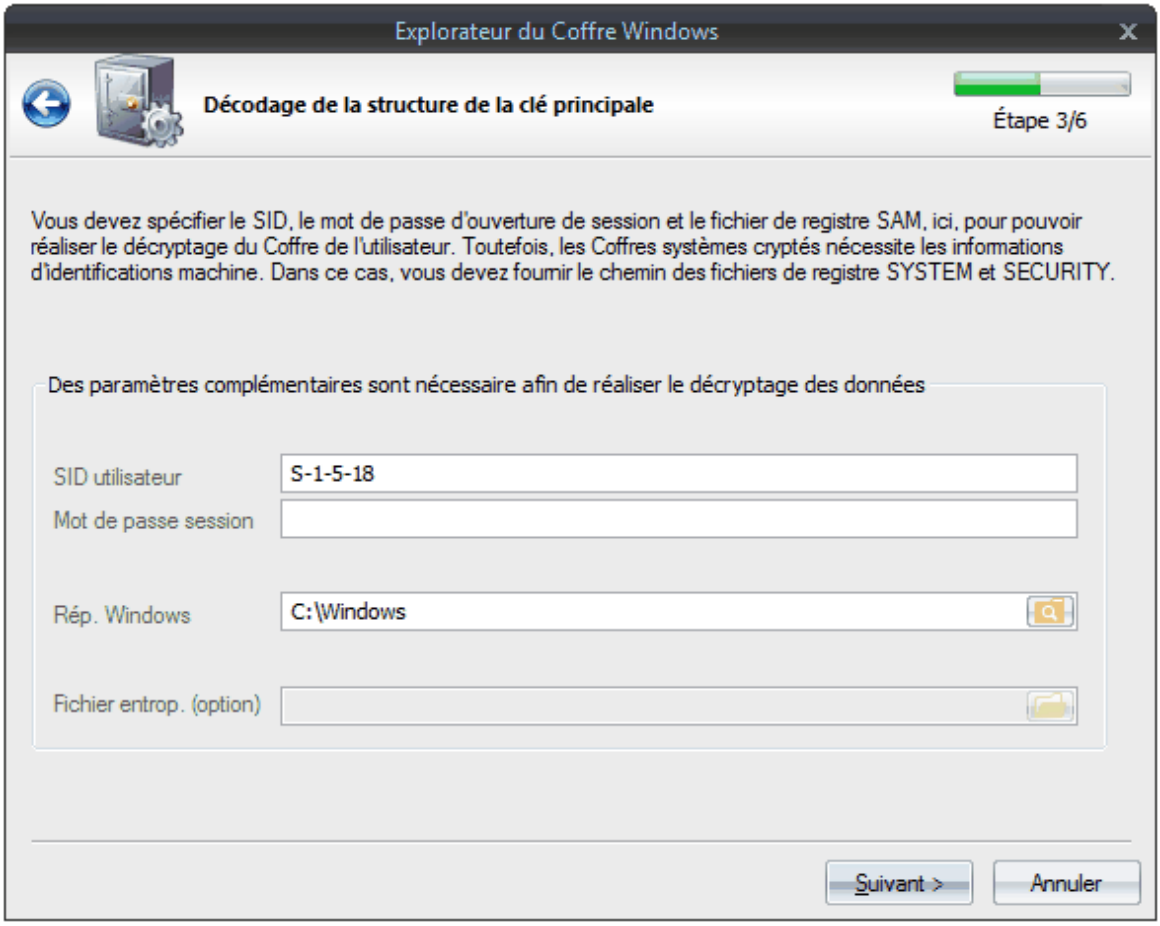
Notez, que certains des répertoires cités ont des attributs système activés, qui définis ces répertoires comme cachés.
Windows possède un utilitaire, sous le nom de VaultCmd, pour créer et gérer vos Coffres de stockages.

Sélection de la Master Key



Une fois qu'un répertoire du Coffre est sélectionné, vous devez indiquer le chemin de la Master Key utilisée pour la protection des clés de cryptage. La Master Key de l'utilisateur est toujours située dans le répertoire **%APPDATA%\Microsoft\Protect\%SID%**, et la Master Key du compte système est stockée dans le répertoire **%SYSTEMDIR%\Microsoft\Protect**.
Il faut savoir qu'il peut y avoir plusieurs Master Keys, Alors qu'un objet peut être décrypter en utilisant avec une seule clé, le nom étant stocké dans le fichier Policy.vpol.
Lors de la recherche d'une Master Key, le programme peut supprimer par filtrage les noms non nécessaires.

Décryptage de la Master Key

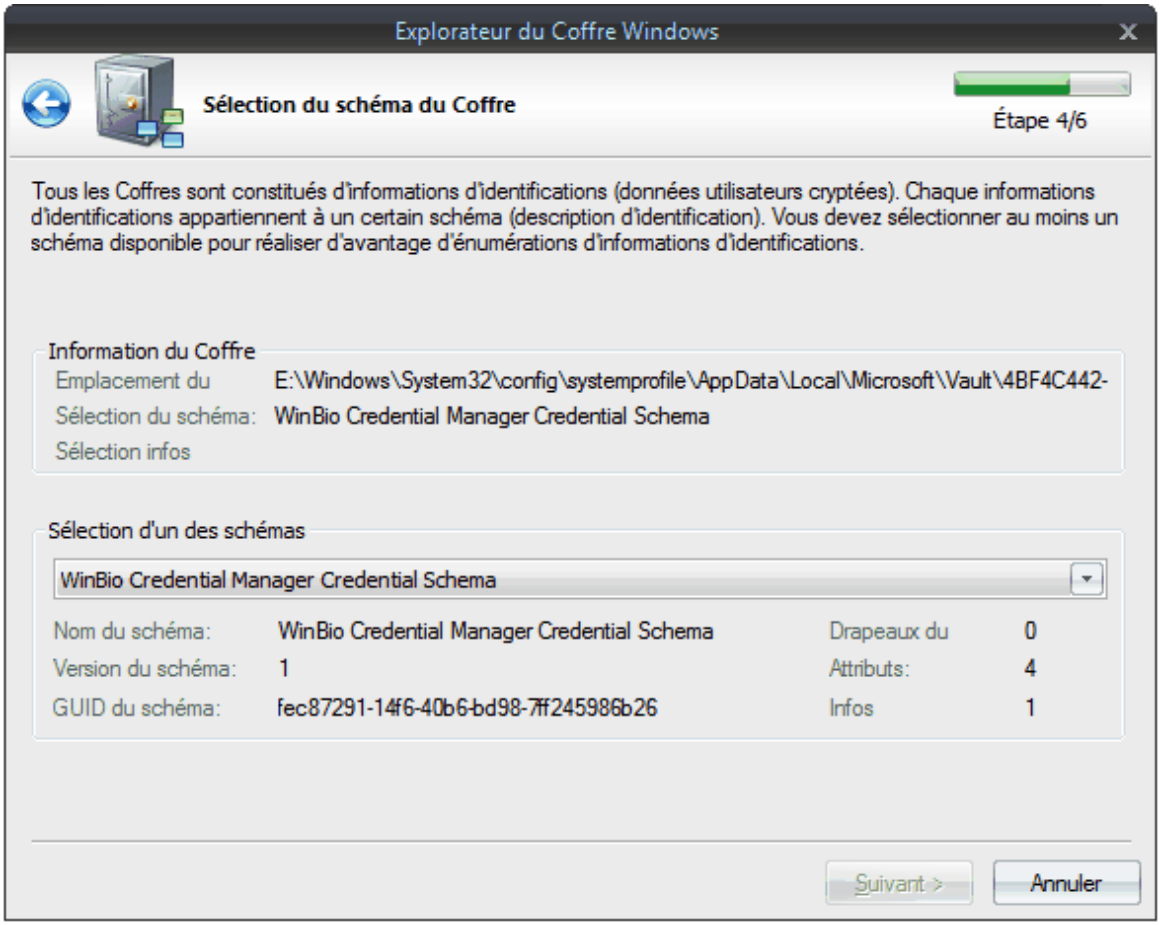


Pour décrypter la Master Key de l'utilisateur, vous devez fournir au moins deux paramètres: le mot de passe de connexion de l'utilisateur et son identifiant de sécurité (SID), lequel est normalement inclus dans le chemin de la Master Key. Sachant que le programme trouve automatiquement le SID de l'utilisateur. Si cela n'a pas été le cas pour quelque raison que ce soit, indiqué le manuellement.
Pour décrypter la Master Key système, vous n'avez pas besoin d'indiquer le mot de de passe; le programme extraira toutes les informations nécessaires à partir des deux fichiers du registre: **SYSTEM** et **SECURITY**.

Dans certains cas, le décryptage de la Master Key nécessite de fournir le chemin du fichier de registre **SAM**. C'est le cas seulement lorsque le compte du propriétaire des données dans Windows 8 est du type d'un **LiveID**.

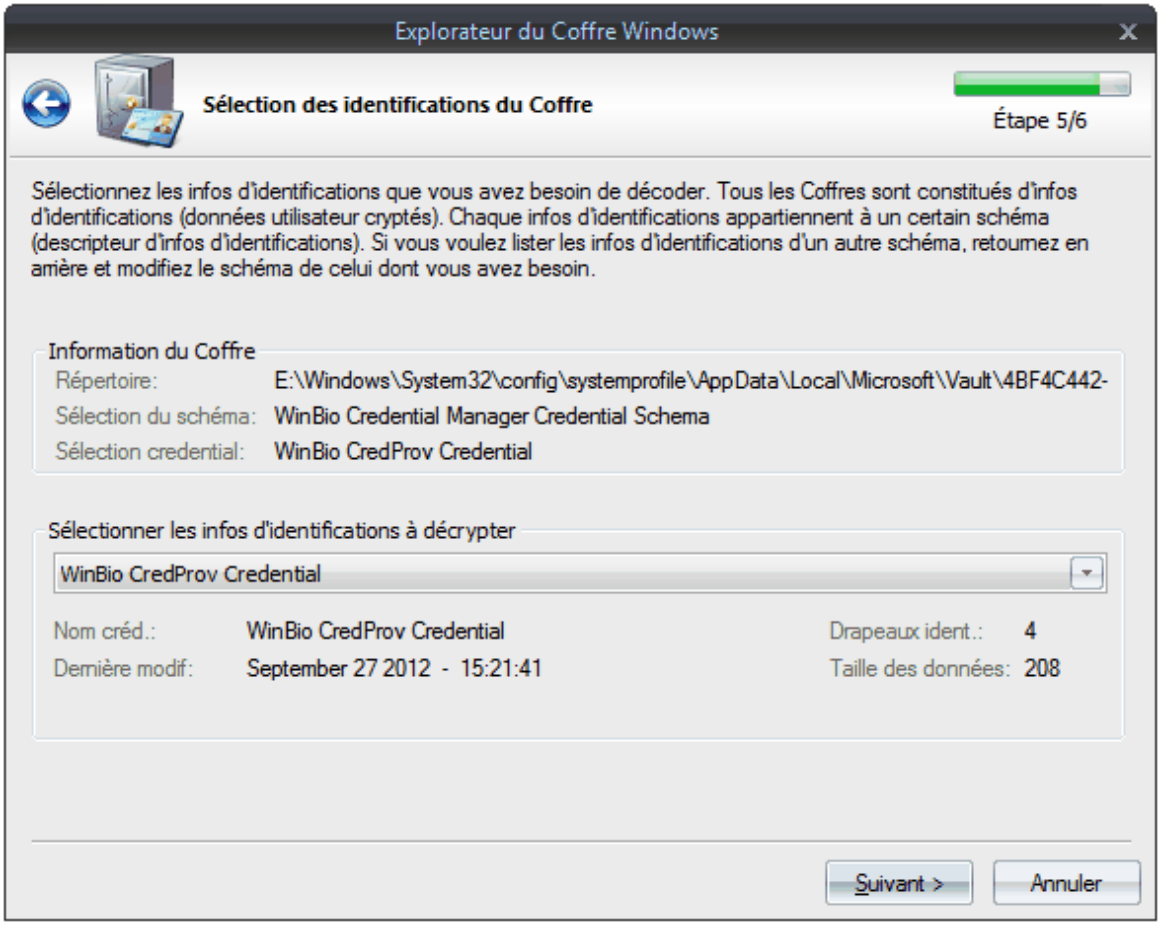
Windows Password Recovery depuis la version 9.7 utilise certaines vulnérabilités dans le cryptage de la Master Key DPAPI. Donc pour décrypter TOUTES
les entrées du Coffre d'un utilisateur de Domaine, le mot de passe de connexion du propriétaire n'est plus nécessaire.

Sélection du schéma de Coffre



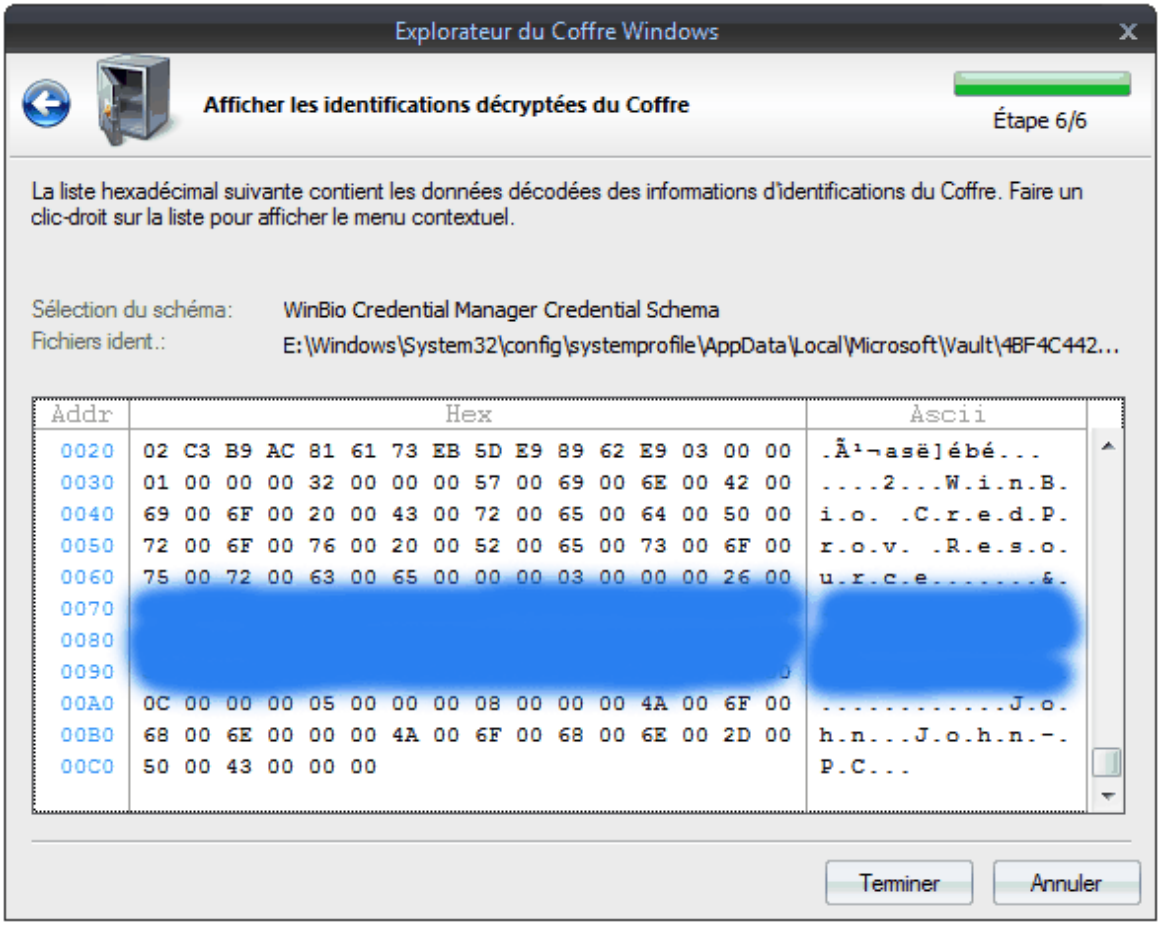
A la 4ème étape, le précédent a été passé avec succès, le programme vous demandera de sélectionner un des schémas de votre Coffre à partir de la liste déroulante. En dessous de la liste, vous pouvez voir les caractéristiques générales du schéma sélectionné: le nom, version, GUID, "flags", nombre d'attributs et infos d'identifications.

Sélection de l'information d'identification du Coffre



Dans le même style, sélectionnez une des infos d'identification qui vous intéresse qui corresponds au schéma que vous avez choisi à l'étape précédente de l'assistant.

Décryptage des informations d'identification du Coffre



Et enfin, pour la dernière étape, vous pouvez voir le décryptage des données, les copier dans le presse-papiers ou le sauvegarder dans un fichier pour de futures analyses. L'image vous montre un mot de passe décrypté au format texte, du compte administrateur configuré pour ouvrir la session en utilisant les informations biométriques (empreintes digitales).

2.7.4.7 Explorateur Windows Hello

Windows Hello est une toute nouvelle technologie biométrique qui permets aux utilisateurs de s'authentifier, sur leurs appareils avec Windows 10, avec juste une empreinte digitale, un scan de l'iris de l'oeil, du visage ou une reconnaissance vocale. Windows Hello est supposé plus confortable et sécurisé que l'usage d'un mot de passe.

Windows Password Recovery possède un jeu d'utilitaires pour analyser la sécurité du système de Windows Hello.
Ce jeu d'utilitaires est constitué de trois fonctionnalités:

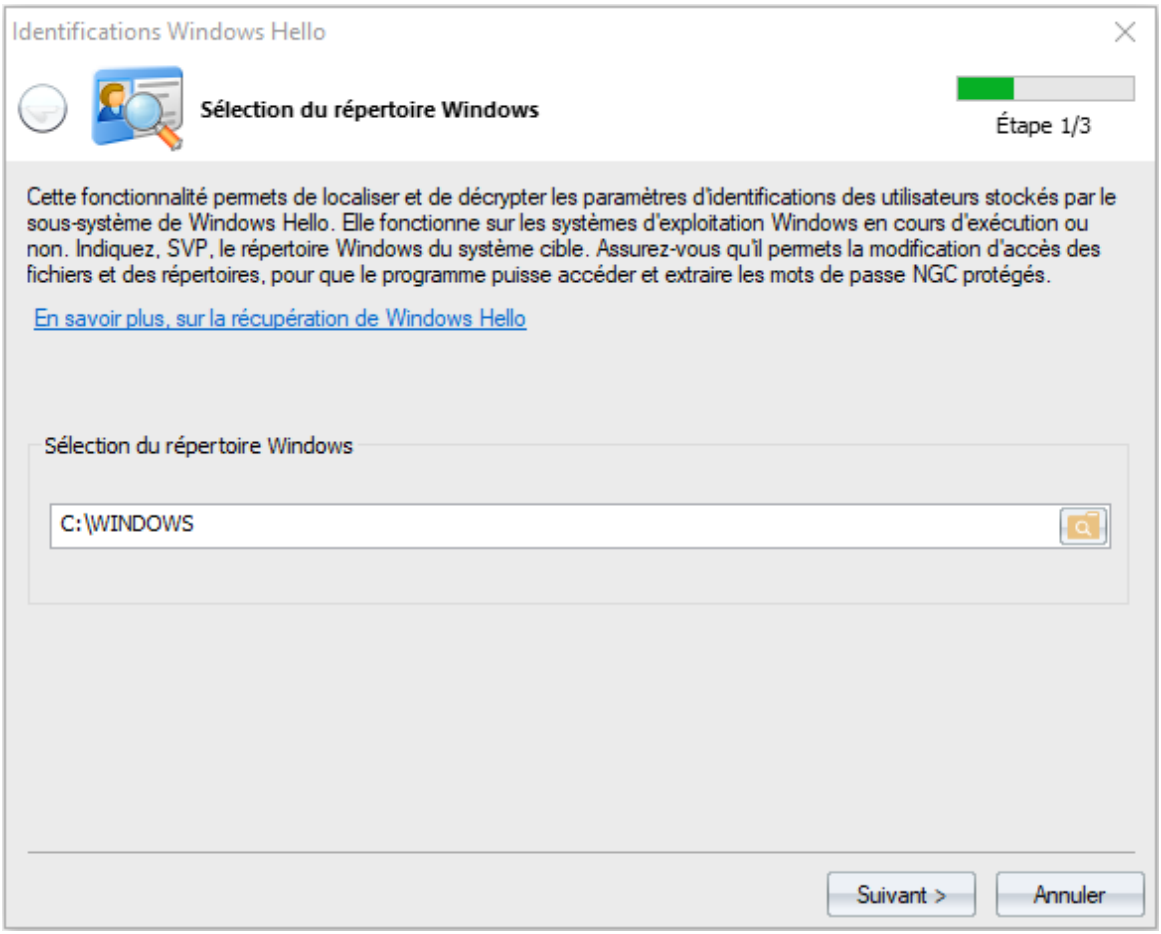
- Extraction des mots de passe enregistrer en clair par le système Windows Hello
- Décryptage des identités digitales (par exemple, les empreintes digitales des utilisateurs) stockés dans les bases de données biométriques
- Outil de récupération du code PIN.

2.7.4.7.1 Mots de passe Windows Hello

Cette fonctionnalité est capable pour localiser et décrypter les identifiants de connexion stockés, en clair, par Windows Hello. Windows hello utilise le système "Next Generation Cryptography" (NGC ou aussi appelé CNG) pour protéger et stocker les données privées et les clés de cryptages des utilisateurs. Même si NGC est un système très élaboré et sophistiqué (précisant qu'il utilise même une astuce non documentée pour protéger les clés de cryptage et les données), Passcape software est le premier, comme dans le cas de DPAPI, qui a réussi à créer un ensemble d'API presque identique mais aussi avec un support pour le mode hors ligne. En effet, cet outil permet de l'utiliser sur un système actif ou sur tous les OS externe.

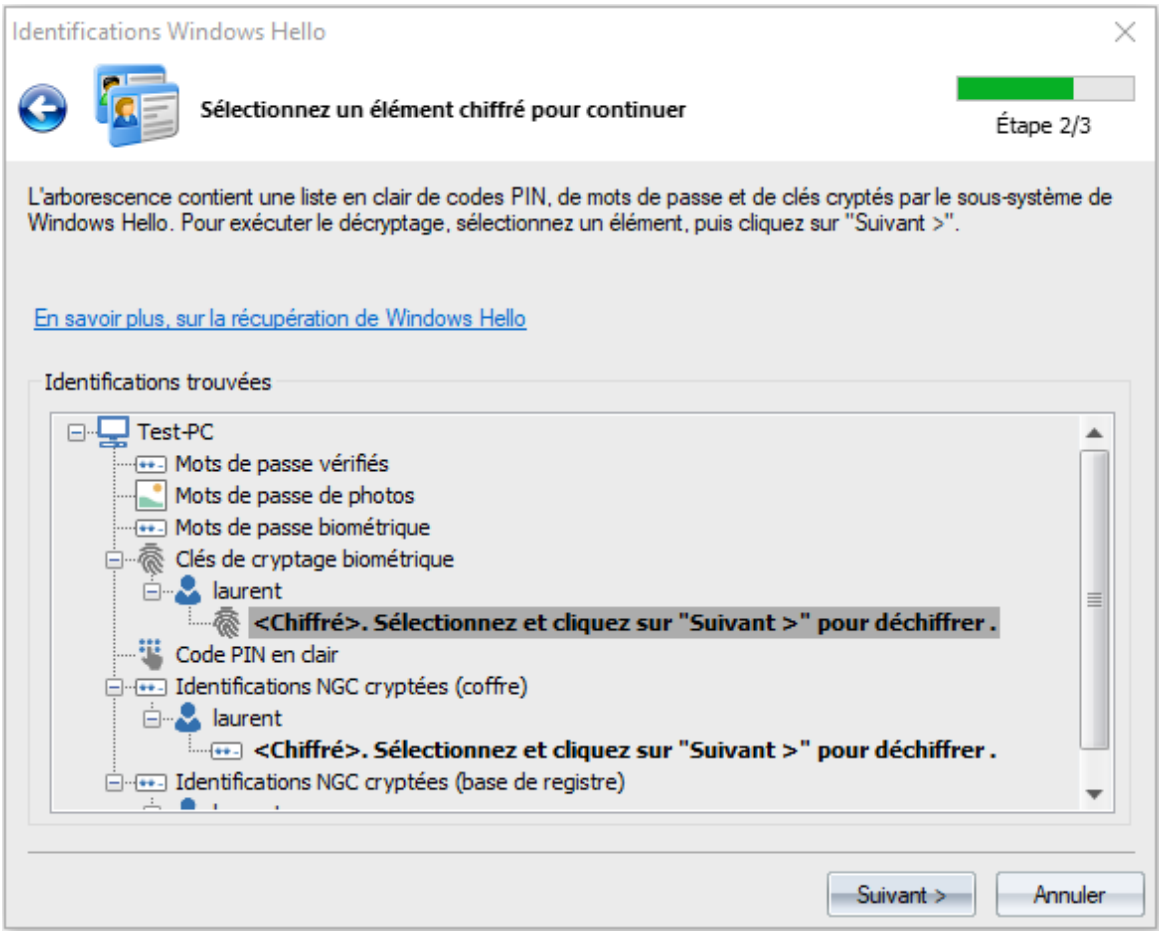
CE qui permets de travailler avec le programme facilement même pour une personne novice, laissant au programme toutes les opérations et routines au programme.

1 Sélection du répertoire Windows



Ce mode détecte automatiquement le répertoire Windows. Ce répertoire contient les fichiers et les clés de cryptage protégées des accès même par les administrateurs. Pour extraire les clés , ce répertoire doit permettre la modifications des droits d'accès pour les opérations de modifications et d'écritures de fichiers. Sinon, le programme ne pourra pas décrypter les mots de passe cryptés par NGC.

2 Sélection des données à décrypter



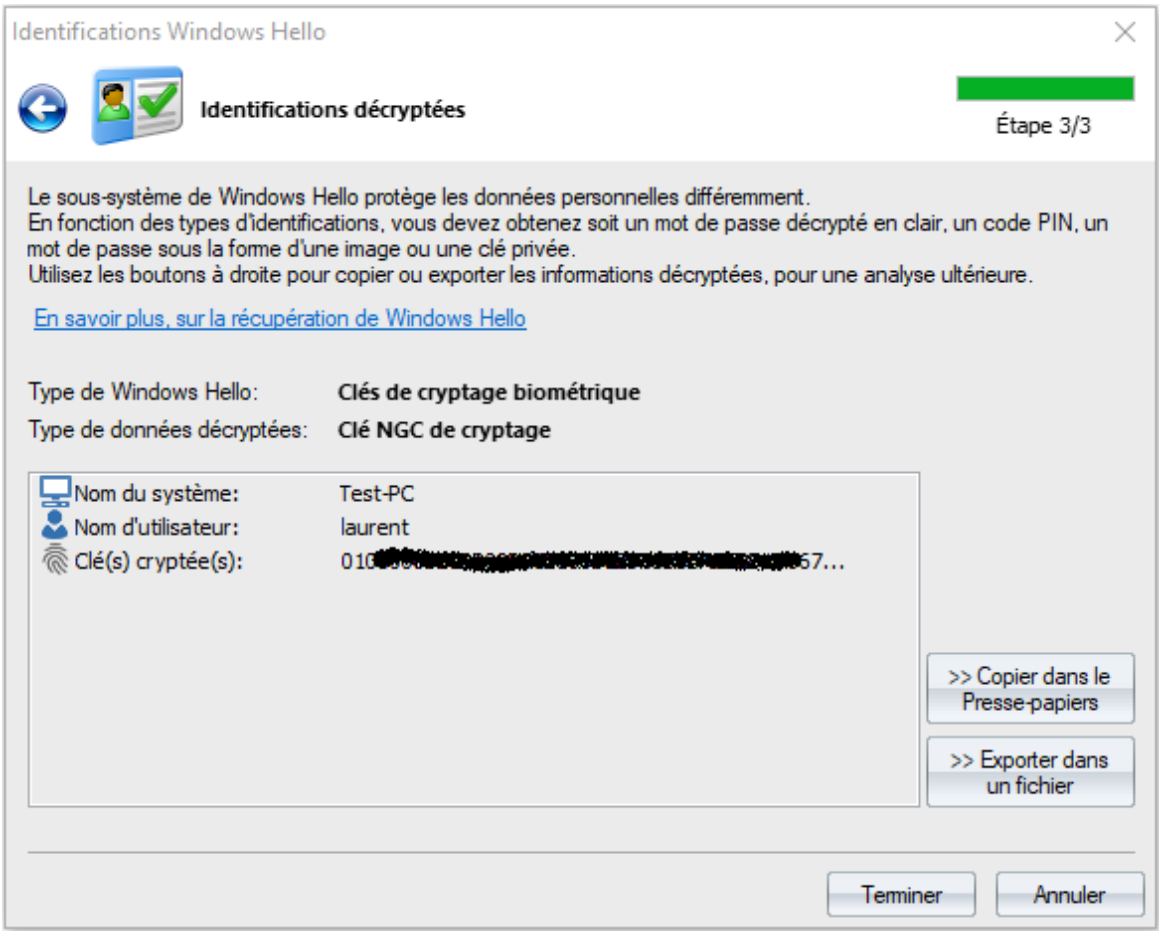
A ce étape, le programme affiche les mots de passe d'identifications de connexion, les clés et les codes PIN, mais non décryptés.
Il est clair, que Windows Hello a été développé par plusieurs équipes de développeurs, car plusieurs sous-systèmes sont utilisés et l'ensemble des données personnelles est disséminé dans tout le système de Windows.
Le programme prends en charge les types de données suivantes:

- Les mots de passe d'images
- Les mots de passe de connexion en clair (non cryptés) protégés avec des mots de passe image
- Les identifications par empreintes digitales
- Les mots de passe de connexion en clair (non cryptés) protégés par des identifications biométriques
- Les clés de cryptages biométriques
- Les codes PIN en clair (non cryptés)
- Les mots de passe en clair (non cryptés),stockés dans le Coffre Windows et protégés par NGC
- Les mots de passe en clair (non cryptés),stockés dans la base de registre Windows et protégés par NGC

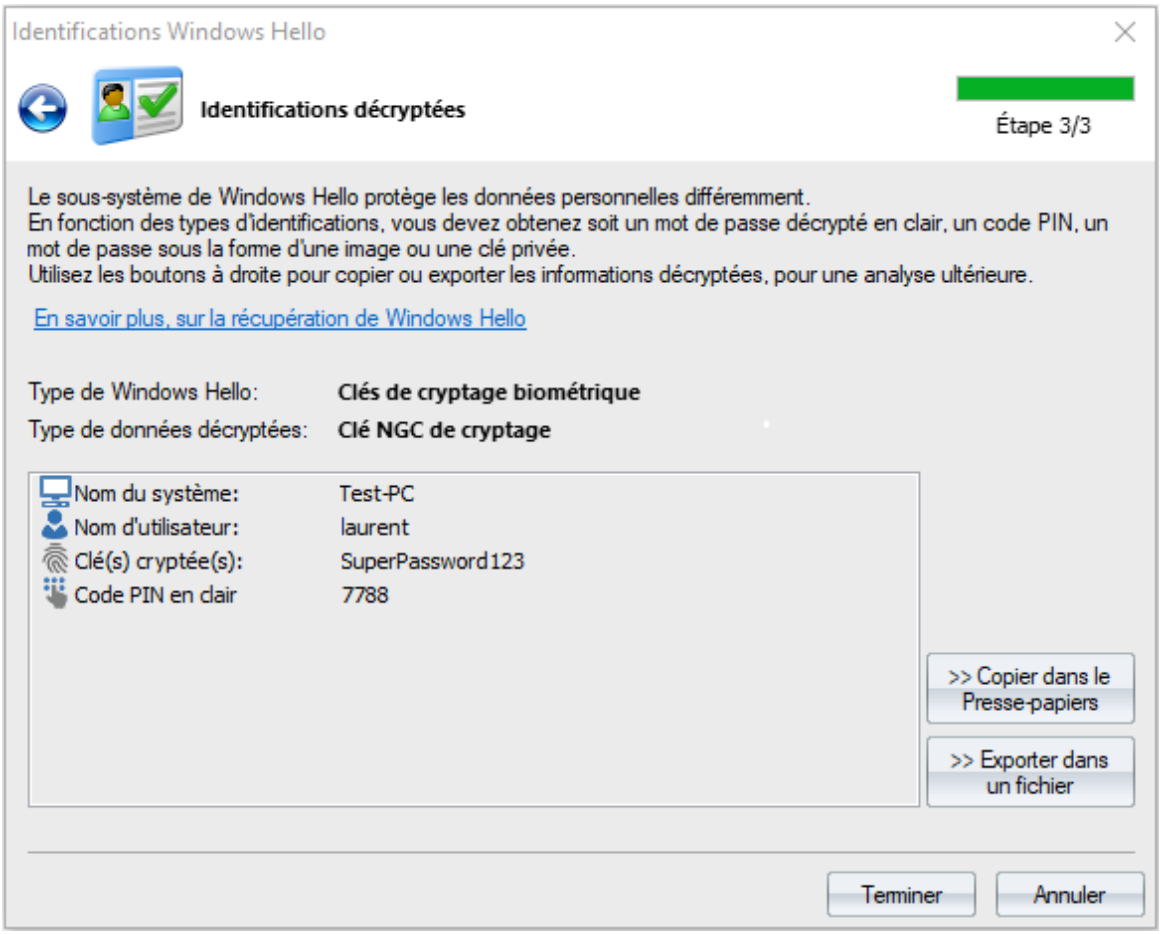
Pour finaliser le décryptage, double-cliquez sur un élément en gras ou cliquez sur suivant après l'avoir sélectionné.

3 Identifications décryptés

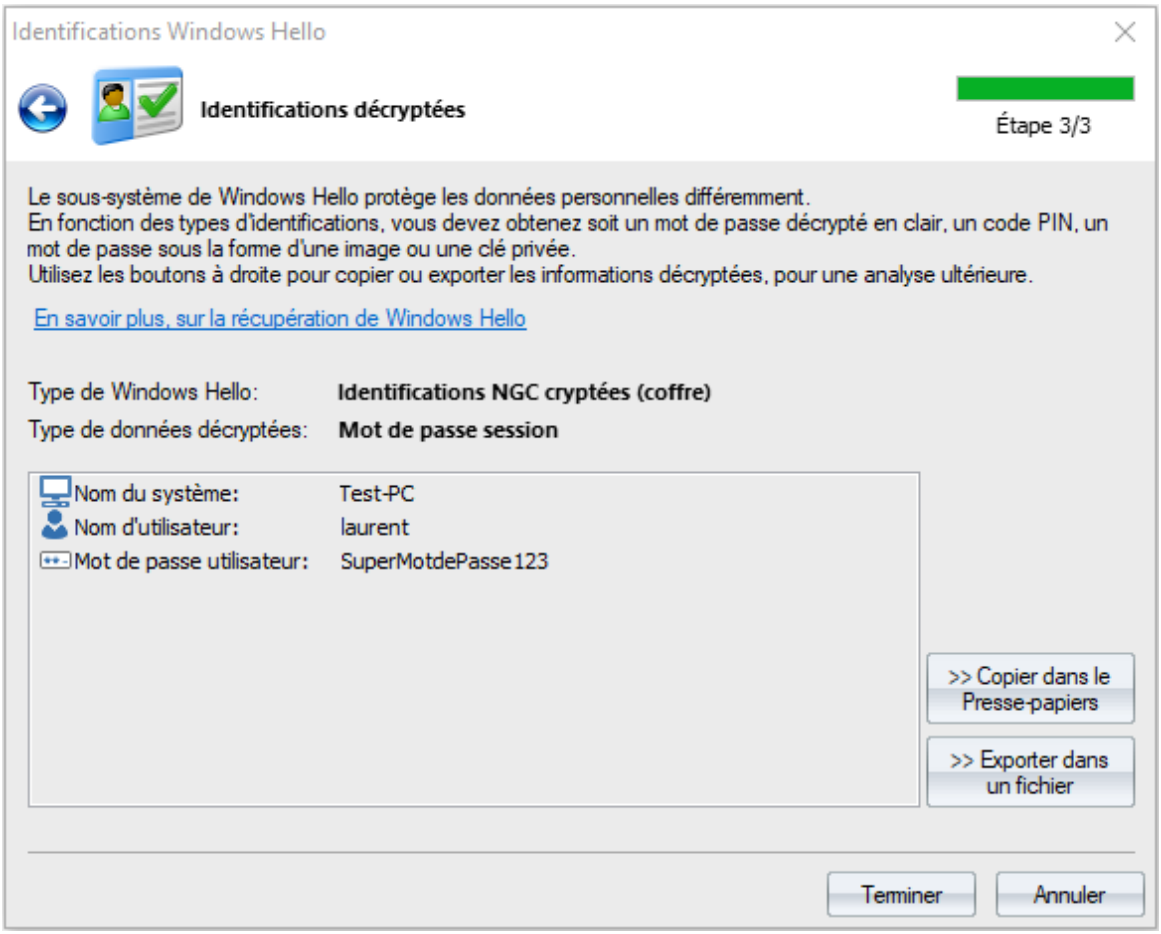
Le système de Windows Hello protège les données personnelles différemment. En fonction, du type d'identification vous allez pouvoir décrypter un mot de passe en clair (non crypté), un code PIN, un mot de passe sous la forme d'une image ou une clé privée.
Utilisez les boutons à droite pour copier ou exporter les informations décodées, pour une analyse ultérieure.



Mot de passe de connexion décrypté (masqué,ici, dans l'exemple).



Mot de passe de connexion et le code PIN décrypté.



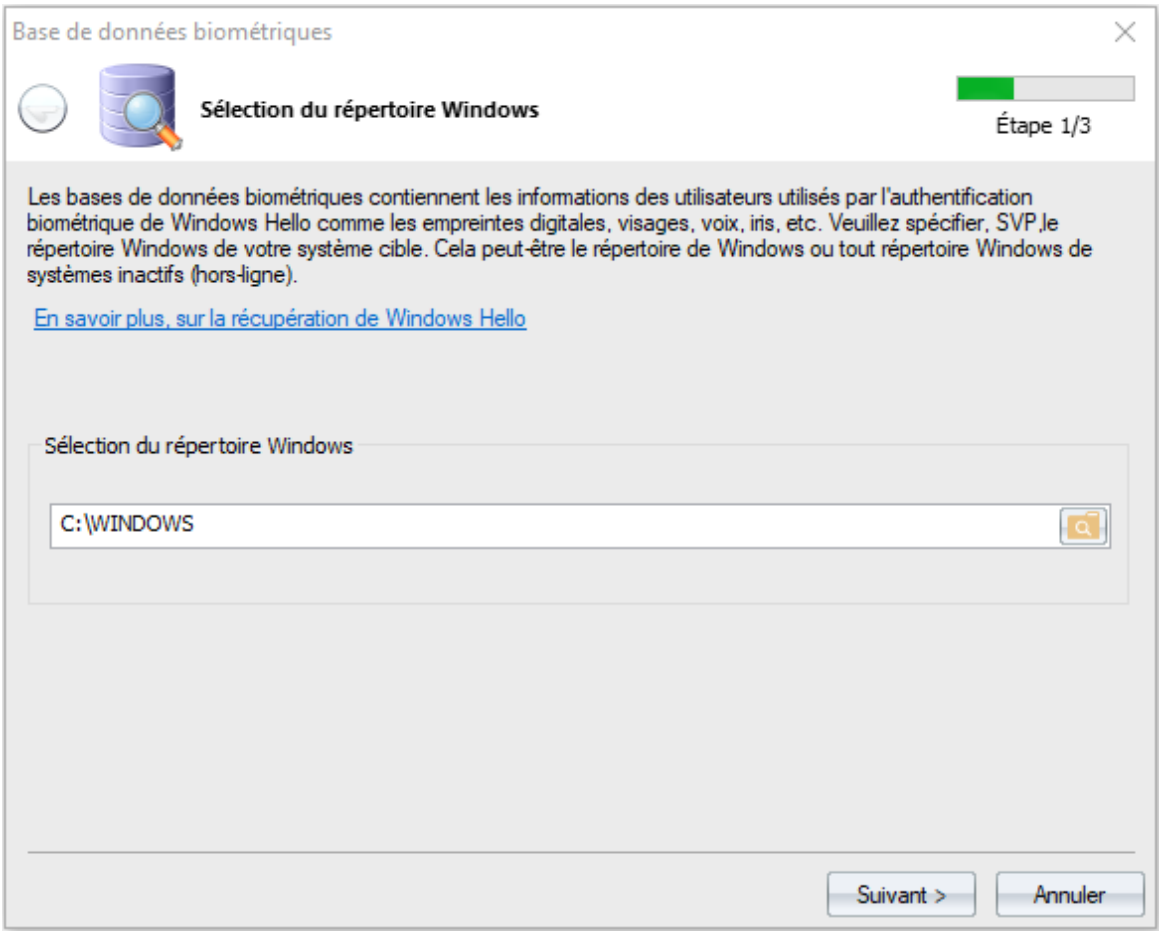
Mot de passe de connexion pour l'utilisateur "Laurent".

Notez que les mots de passe en clair protégés par NGC peuvent être décryptés soit en utilisant une clé biométrique ou un code PIN. Le programme essaye tout d'abord, de localiser et d'utiliser les clés biométriques. Si il n'y parvient pas (par ex: dans le cas où l'identification biométrique n'a pas été configuré), WPR demande le code PIN pour pouvoir décrypter les données.

2.7.4.7.2 Bases de données biométriques

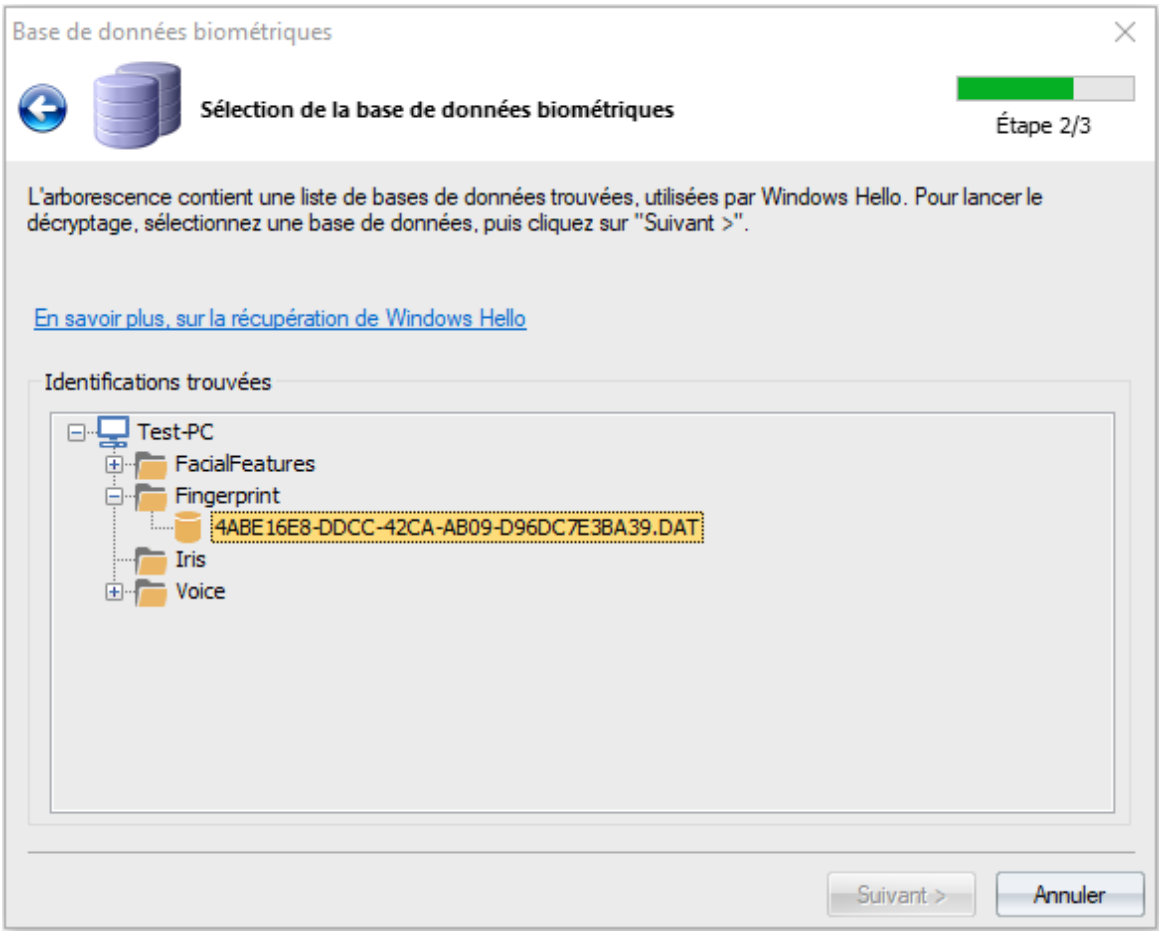
Les base de données biométriques contient les identités numériques utilisées pour authentifier un utilisateur avec le système Windows Hello.
Ces identités peuvent être des empreintes digitales, un visage en 3D, une voix ou l'iris d'un oeil.

1 Sélection du répertoire Windows



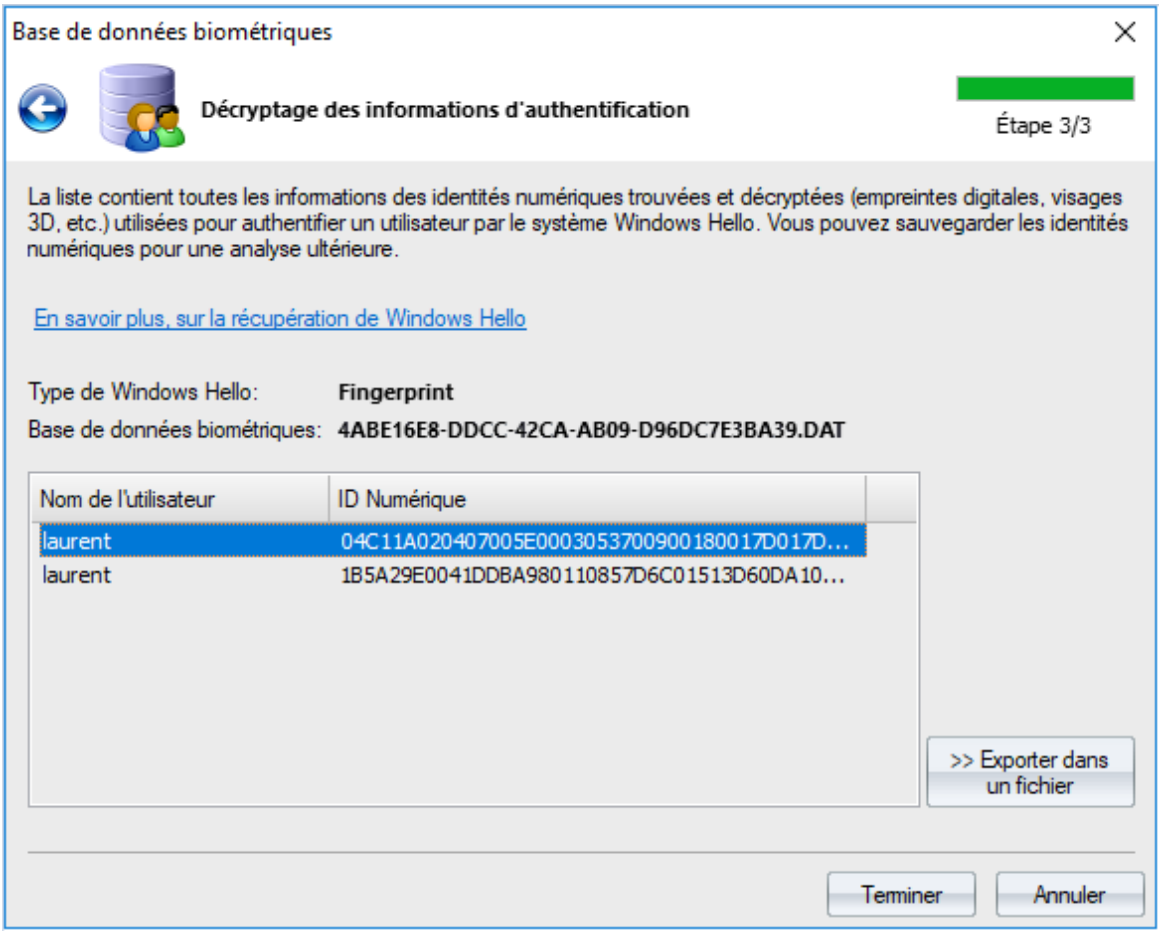
Vous devez, en premier, indiquer le répertoire Windows du système cible. Cela peut être le répertoire Windows de votre système actuel ou bien tout système d'exploitation externe.

2 Sélection de de la base de données biométriques



Pour décrypter une base de données, double-cliquez simplement sur la liste ou cliquez sur "Suivant" après l'avoir sélectionnée.

3 Décryptage des informations d'authenfication



La base de données décryptée contient les identités numériques trouvées et décryptées, comme les empreintes digitales, les visages en 3D, etc. Par exemple, si un utilisateur a enregistré 2 empreintes pour s'authentifier à l'aide du système de Windows Hello, les empreintes seront décryptées et affichées à droite du nom de l'utilisateur. Comme ici dans l'exemple, pour l'utilisateur "laurent", dans l'image ci-dessus.

Vous pouvez enregistrer les ID numériques décryptées dans un fichier, pour une analyse ultérieure.

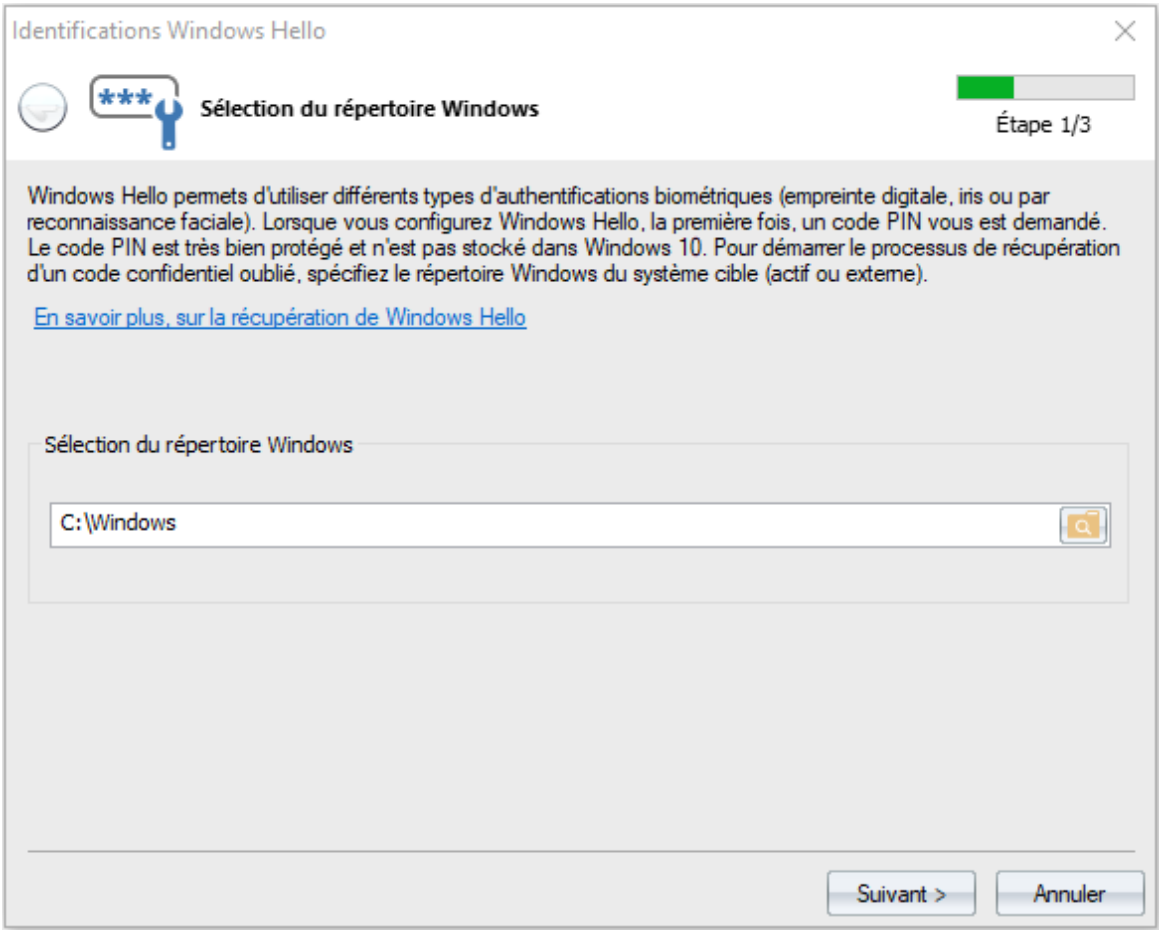
Malgré le fait que Microsoft affirme avoir avec Windows Hello un système très sécurisé, les ID numériques sont très mal protégés contre la possibilité de les substituer (tant qu'elles ne sont pas utilisées avec des périphériques TMP) et peuvent être facilement déplacées ou copiées d'un PC vers un autre.
Par exemple, vous pouvez créer votre propre empreinte digitale, puis la copier dans un autre compte d'un utilisateur d'un PC. Ensuite vous pouvez authentifier dans le compte en utilisant votre propre empreinte digitale.
Du fait de cette très grande vulnérabilité qui comprends la sécurité totale du système, la migration d'ID numérique a été désactivée dans la version de ce programme.

2.7.4.7.3 Attaquer les codes PIN par Force brute

Windows Hello permets différents types d'authentifications biométriques: par empreintes digitales, l'iris de l'œil, le visage ou la reconnaissance vocale.
Lorsque vous configurez Windows Hello, la première étape est la création d'un code PIN. Le code PIN est très bien protégé et n'est pas stocké dans Windows 10. Cependant, il peut être facilement décrypté dans Windows 8.
Pour deviner un code PIN perdu, vous devez indiquer, en premier, le répertoire Windows du système cible. Cela peut être votre répertoire actuel ou tout répertoire Windows externe.

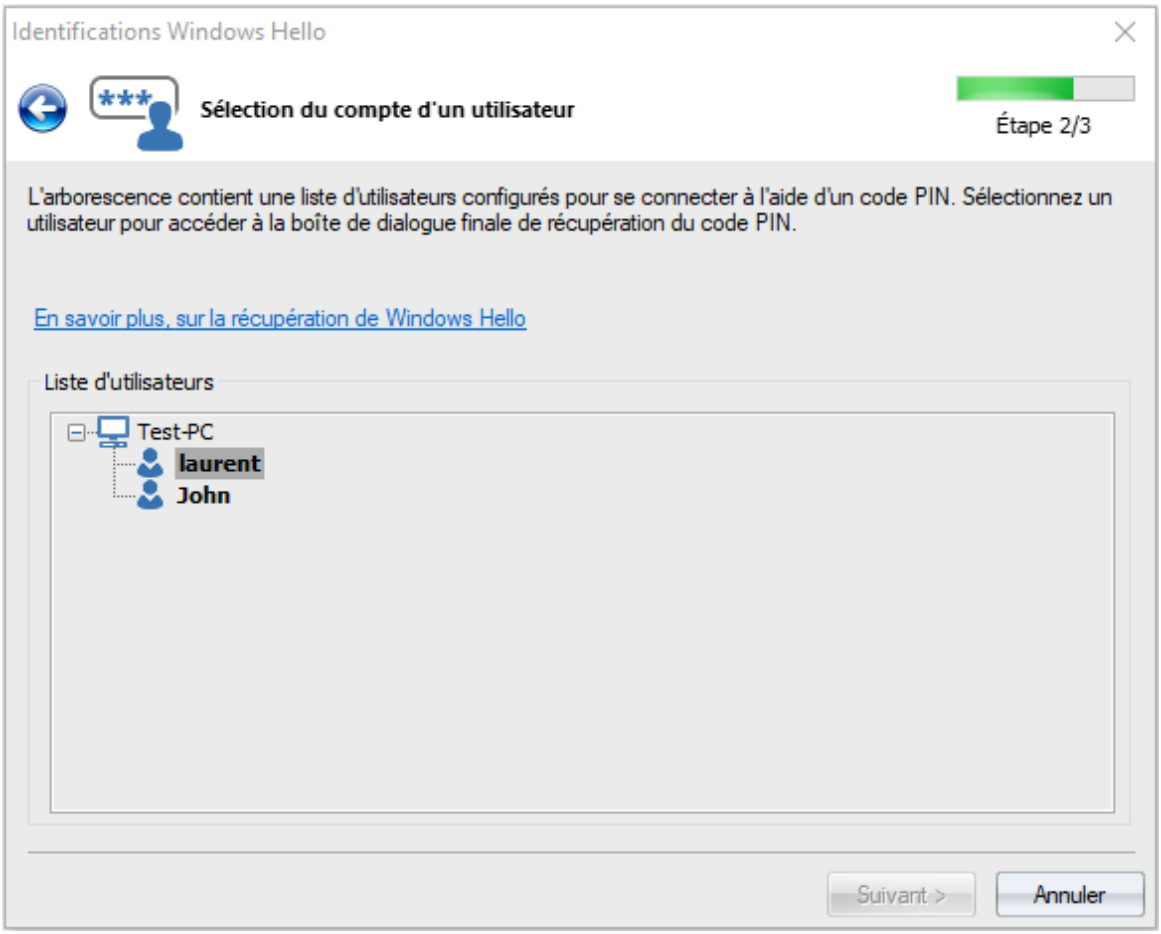
Pour assurer une synchronisation avec tous les périphériques, Microsoft garde une copie de votre code PIN sur ces serveurs (pour les comptes Microsoft uniquement).

1 Sélection du répertoire Windows



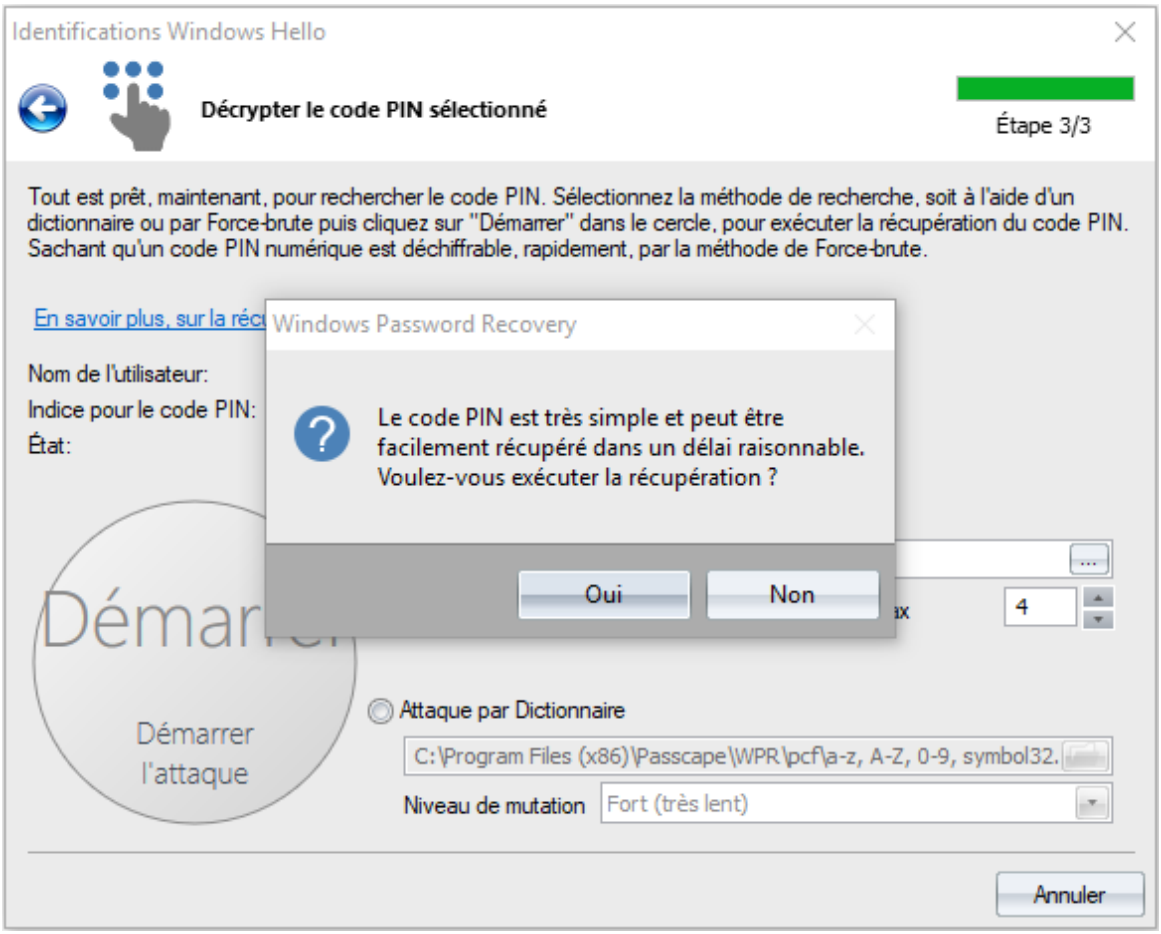
Vous devez indiquez, en premier, le répertoire Windows du système cible.
Pour pouvoir extraire le code PIN, le répertoire Windows doit permettre la modifications des droits de modifications et d'écritures des fichiers. Dans le cas où vous avez indiqué le répertoire Windows de système actuel, l'exécution du programme (WPR) avec les droits administrateurs est suffisant.

2 Sélection du compte d'un utilisateur

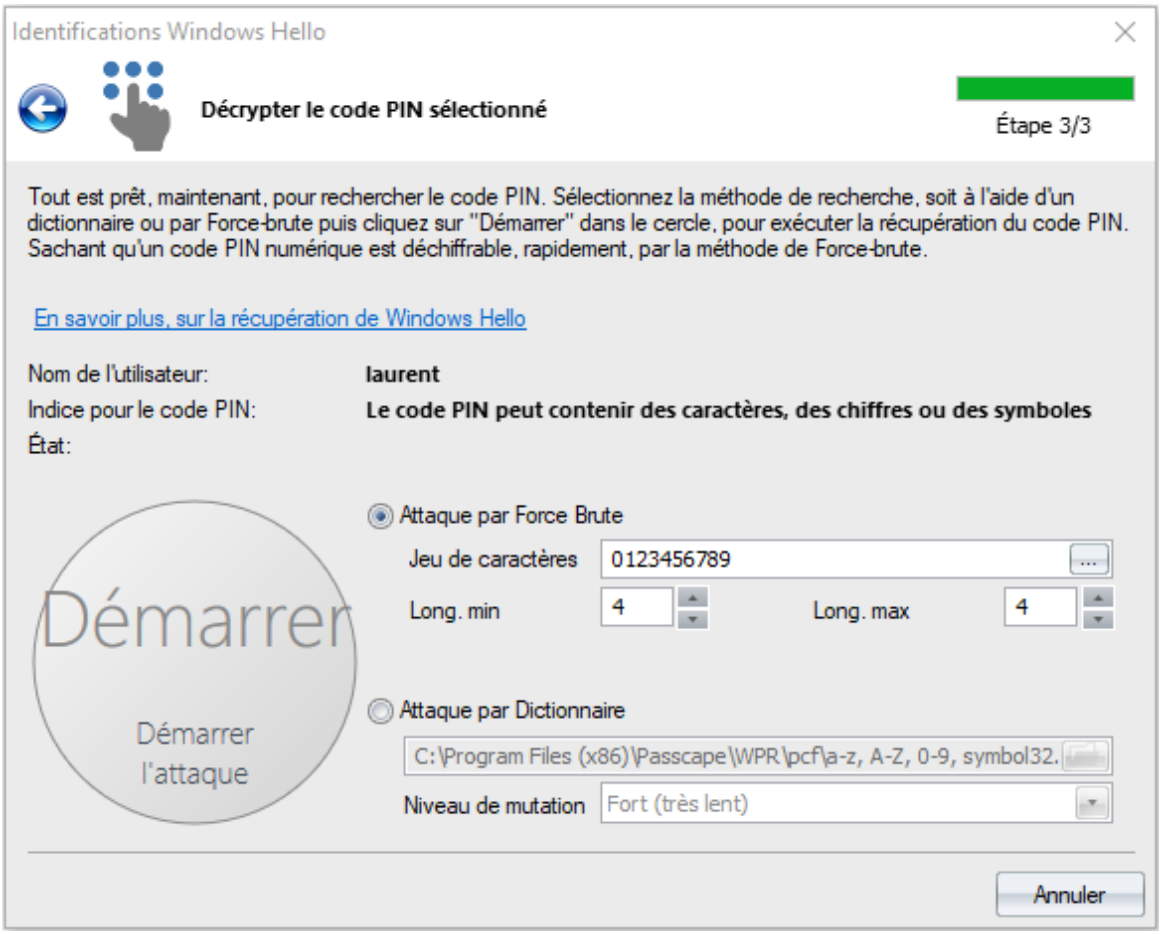


A cette étape, le programme affiche tous les comptes des utilisateurs trouvés qui ont un code PIN configuré pour s'authentifier au système.
Sélectionnez un utilisateur puis cliquez sur "Suivant" pour accéder à la boite de dialogue pour la récupération du code PIN.

3 Décryptage du code PIN d'un utilisateur



Dans le cas où le code PIN est constitué de chiffre et peut être décrypté facilement et rapidement, une boite de dialogue vous propose de lancer la récupération avec des paramètres, par défaut, optimisés. Si vous souhaitez exécuter la récupération avec des paramètres de votre choix, cliquez sur "NON".



Le programme prends en charge deux méthodes de récupération:
- Par Force brute
- Par dictionnaire.

La configuration de chacun est relativement facile.
Dans le cas de l'attaque par Force brute, vous devez définir le jeu de caractères, la longueur minimale et maximale du code PIN.
Dans le cas de l'attaque par dictionnaire, choisissez simplement, une liste de mots et le niveau de mutations dont vous avez besoin.

Pour lancer ou arrêter l'attaque, utilisez le bouton rond à gauche des paramètres "Démarrer l'attaque".

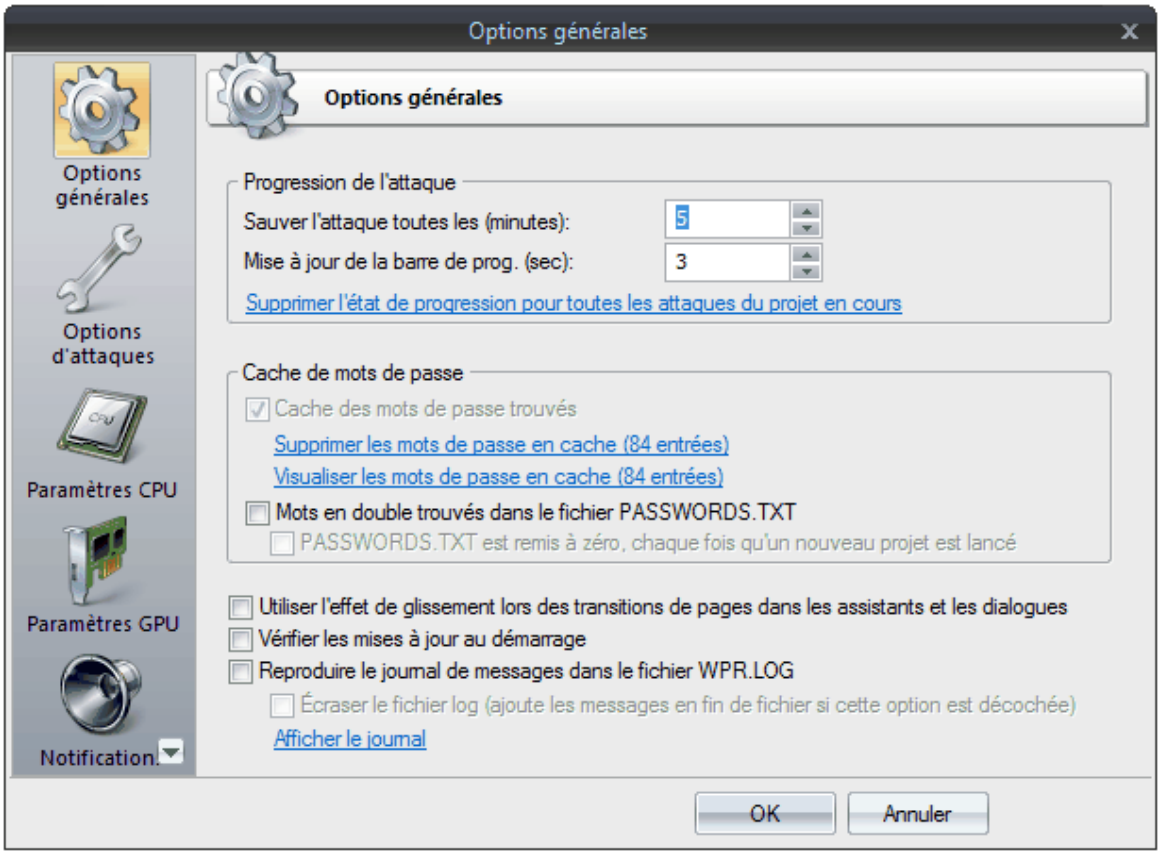
Dans certains cas, le programme peut détecter le jeu de caractères utilisés pour créer le code PIN. Dans ce cas, une astuce vous indique dans le champ corresponds le contenu "Indice pour le code PIN".

2.8 Menu Options

2.8.1 Options générales

Les Options générales sont divisées en 5 éléments.

2.8.1.1 Options générales



Progression de l'attaque
Le premier groupe de paramètres permets de définir les intervalles d'enregistrements et de la barre de progression pour l'état de l'attaque en cours. Par défaut, une attaque enregistre son état toutes les 5 minutes (cela donne la possibilité de reprendre l'attaque au niveau ou vous l'avez enregistré) et rafraîchie l'écran toutes les 3 secondes.

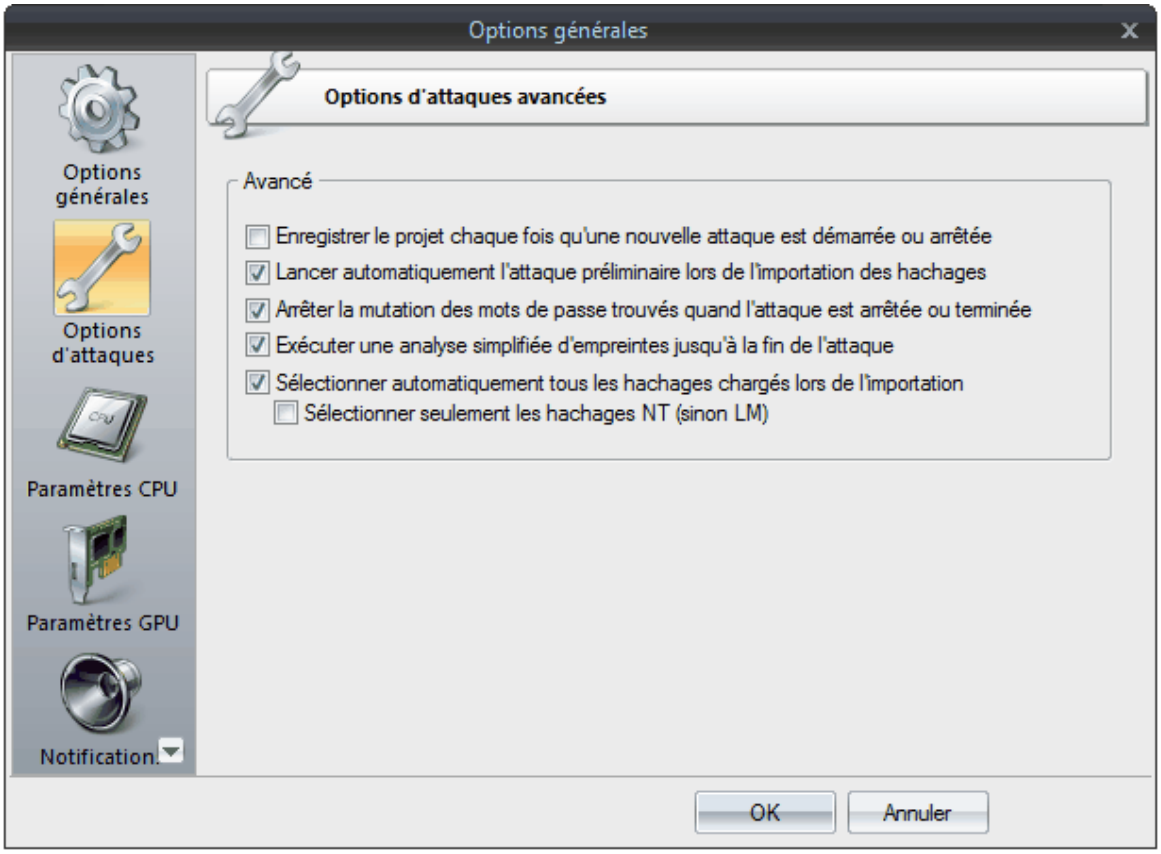
Cache de mots de passe
Tous les mots de passe trouvés par le programme sont mis en cache par défaut. Une aide très précieuse qui est utilisée dans plusieurs sous-programme. Par exemple, lors d'une attaque préliminaire ou intelligente.
L'effacement du cache de mots de passe est recommandé dans les cas d'extrêmes nécessités. Par exemple, lorsque leurs nombres excèdent dix milles. Dans ce cas, la vitesse de recherche pour certaines attaques peut chuter de manière significative.
En complément, vous pouvez copier les mots de passe trouvés dans un fichier texte. Ainsi, si le programme se bloque ou dans le cas d'une panne soudaine d'alimentation, les mots de passe trouvés seront assurés d'être copié dans un fichier.

Vérifier les mises à jour au démarrage - vérifie si une mise à jour est disponible à chaque démarrage du programme. L'option fonctionne uniquement si le PC est connecté à Internet.

Reproduire le journal de messages dans le fichier wpr.log - Lorsque cette option est activée, le programme écrit tous les messages de la fenêtre du journal dans le fichier WPR.LOG. Cette option peut être la source de dégradation des performances avec de grandes listes de hachages, car wpr.log vide son contenu sur le disque chaque fois qu'un nouveau message arrive. Cela peut-être cependant très utile lorsque le programme bloque ou devient instable.
WPR.LOG est situé dans le répertoire d'installation du programme.

Écraser le fichier log - écrase le fichier log à chaque démarrage du programme. Cependant, les nouveaux messages seront ajoutés à la fin du fichier log.

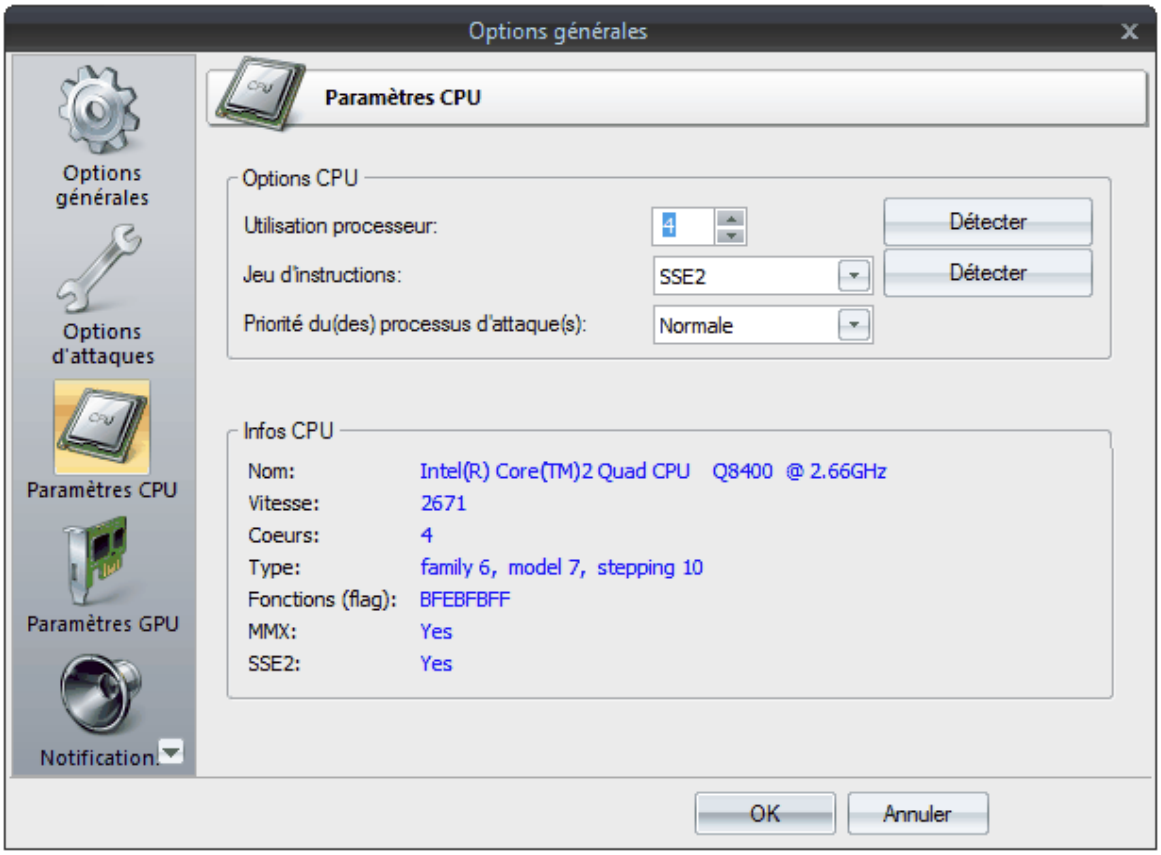
2.8.1.2 Options d'attaques



Avancé

- *'Enregistrer le projet chaque fois ...'* - force le programme à sauvegarder automatiquement le projet chaque fois qu'une nouvelle attaque est démarrée ou arrêtée (incluant aussi les sous-attaques de l'attaque par lots).
- *"Lancer automatiquement l'attaque préliminaire lors de l'importation des hachages"* - lance automatiquement l'attaque préliminaire lors de l'importation des hachages. Cette attaque trouve les mots de passe de très faibles complexités en quelques secondes.
- *"Arrêter la mutation des mots de passe trouvés quand l'attaque est arrêtée ou terminée"* - active l'analyse de mots de passe et le module de mutation pour les mots de passe trouvés après l'attaque. Cette option peut être extrêmement utile; par exemple pour la récupération de mots de passe similaires.
- *"Exécuter une analyse simplifiée d'empreintes jusqu'à la fin de l'attaque"* - active le second module d'analyse. Il est lancé à la fin de l'attaque, et crée un nouveau dictionnaire d'empreinte des mots de passe trouvés, en essayant de retrouver le plus de mots de passe possible. Très utile avec les grandes listes de hachages, d'historique de hachages, etc.
- *"Sélectionner automatiquement tous les hachages chargés lors de l'importation"* - sélectionne automatiquement les entrées à utiliser pour la recherche après l'importation.

2.8.1.3 Paramètres CPU

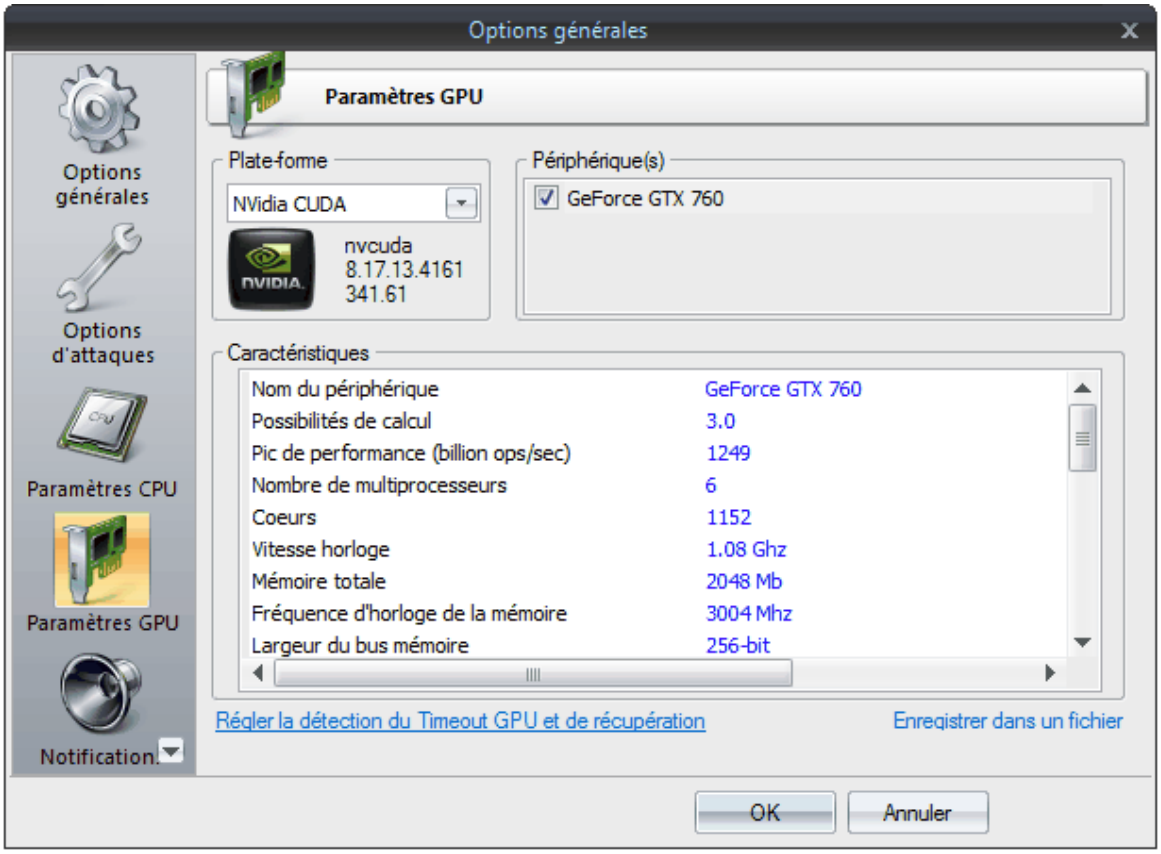


Depuis que la majorité des attaques supportent le multitâche, vous pouvez définir le nombre de processus à lancer simultanément. Dans la majorité des cas, il doit correspondre au nombre de cœurs de votre CPU. Cependant, si le CPU supporte la technologie Hyper-Threading, vous pouvez doubler le nombre de cœurs à lancer simultanément.

Les algorithmes de recherche DES et MD4 dans Windows Password Recovery sont optimisés pour trois types d'architectures: X86, MMX et SSE2. Naturellement, sur les CPUs de nouvelles architectures, la recherche devrait être plus rapide.

Il n'est pas recommandé de choisir la priorité d'attaque au dessus de "normale"; sinon, vous risquez d'avoir une réduction assez importante des performances du système complet.

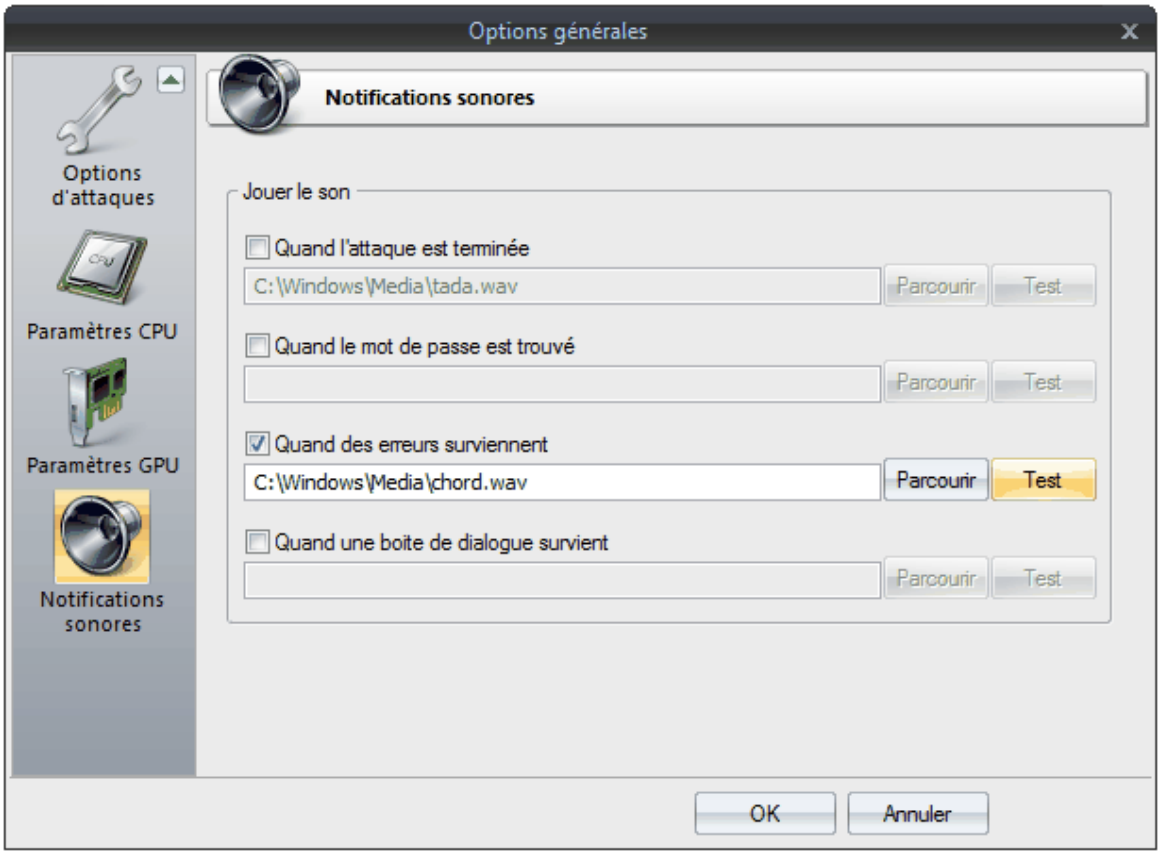
2.8.1.4 Paramètres GPU



Avant de lancer une attaque avec un GPU, il est nécessaire de le sélectionner dans la liste des périphériques, en cochant la case à gauche du nom du GPU.
Toutes les caractéristiques du périphérique sont affichées dans la fenêtre "Caractéristiques".

Le logiciel supporte les GPUs NVidia (à base de plate-forme CUDA) et AMD (à base de plate-forme OpenCL).

2.8.1.5 Notifications sonores

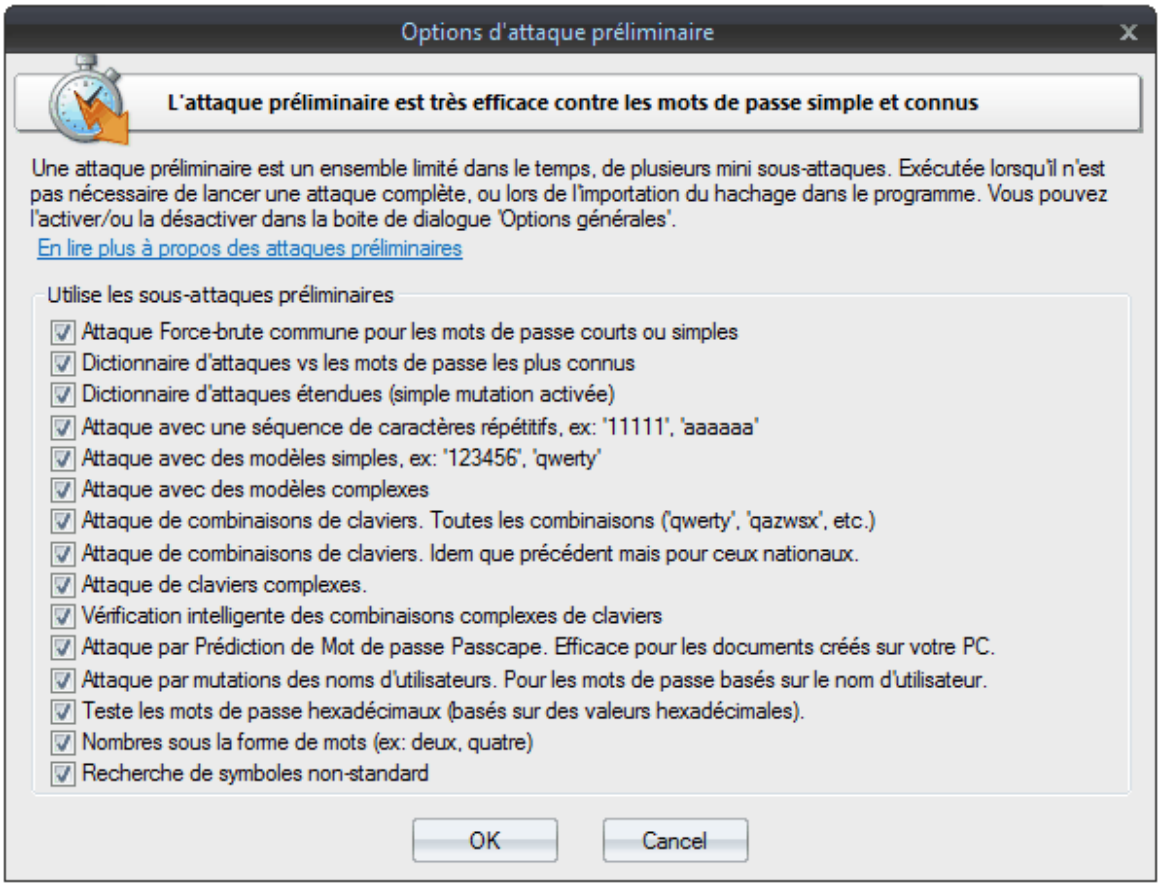


Le logiciel permets de définir des notifications sonores pour certains événements. Par exemple, lorsque l'attaque est terminée ou quand un mot de passe est trouvé.

2.8.2 Options d'attaques

2.8.2.1 Attaque Préliminaire

L'attaque préliminaire (développée chez Passcape) est très efficace contre les mots de passe courts, simples, de dictionnaires, répétitifs, de claviers, etc. et est constitué de plusieurs mini-attaques. Chaque mini-attaque peut être activée/désactivée individuellement.



L'attaque préliminaire s'exécute durant 10 à 20 minutes ou souvent plus rapidement. Elle constituée d'au moins une des sous-attaques suivantes:

- Attaque Force-brute commune. Exécute plusieurs attaques simples de Force-brute basées sur un jeu de caractères prédéfinis.
- Dictionnaire d'attaques contre les mots de passe les plus connus. Test rapidement le mot de passe en vérifiant tous les mots à partir d'un dictionnaire fourni .
- Dictionnaire d'attaques étendues. Elle est globalement identique à la précédente avec quelques petites modifications des options activées.
- Attaque avec une séquence de caractères répétitifs. Teste les mots de passe ayant des séquences de caractères répétitifs. Ex: "1111111" ou "xxxxxx".
- Attaque avec des modèles simples, ex: '123456', 'qwerty'.
- Attaque avec des modèles complexes. La même que la précédente, pour les modèles composés.
- Attaque de combinaisons de claviers. Toutes les combinaisons ('qwerty', 'qazwsx', etc.).
- Attaque de combinaisons de claviers. Idem que précédent mais les mots de passe utilisant les lettres des claviers nationaux.
- Attaque de claviers complexes. Identique à l'attaque deux lignes plus haut, pour les modèles composés.
- Attaque par Prédiction de Mot de passe Passcape. La plus compliquée et la plus évoluée comme outil de prédiction de mots de passe.
- Attaque par mutations des noms d'utilisateurs.
- Teste les mots de passe hexadécimaux (ex: 7A49F3).
- Nombre sous la forme de mots (ex: deux, quatre).
- Recherche les symboles non-standard et les mots de passe courts qui ont été créé en utilisant des symboles UNICODE non-standard.

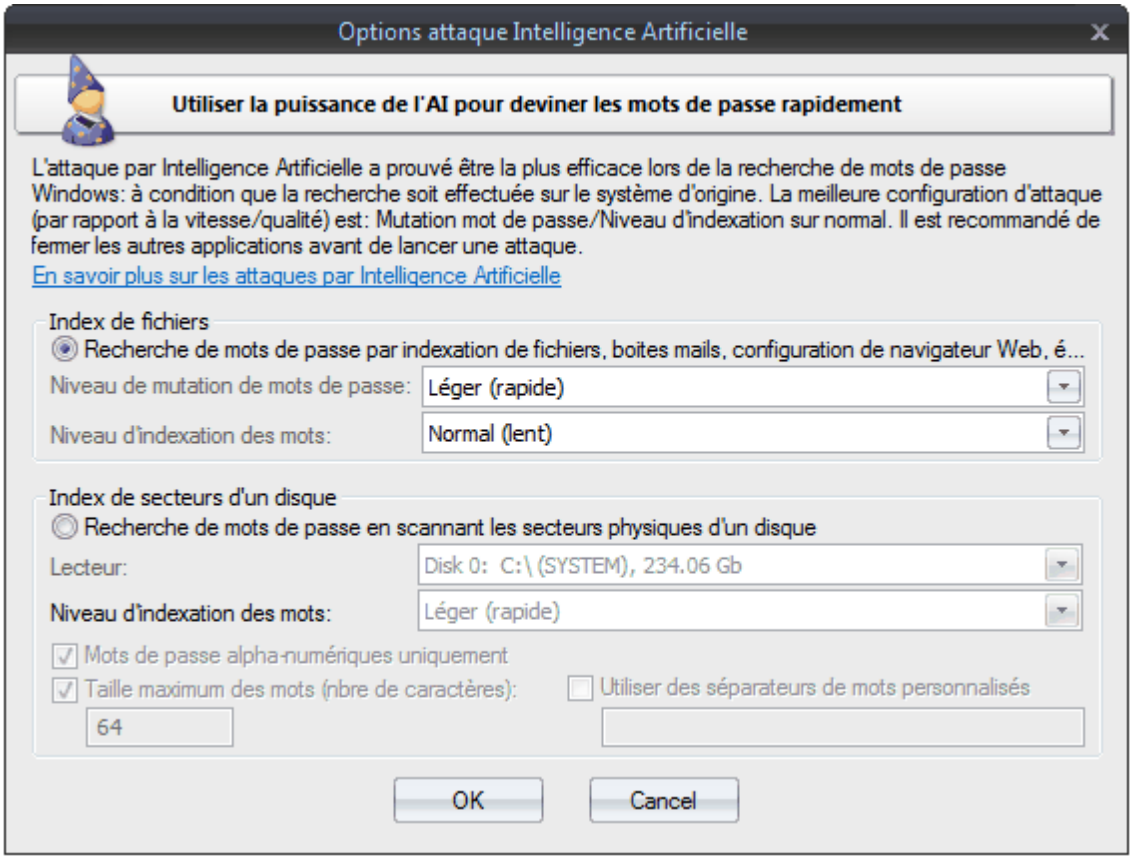
2.8.2.2 Attaque par Intelligence Artificielle

L'attaque par Intelligence Artificielle est un nouveau type d'attaque développée dans notre entreprise. Elle est basée sur une méthode d'ingénierie sociale et n'a jamais encore été mise en œuvre dans des

applications de récupération de mots de passe.

Celle-ci est le plus souvent utilisée lorsque les hachages sont importés depuis un ordinateur local. L'attaque Intellectuelle scanne l'ordinateur local, indexe et crée la liste des mots trouvés et les mots de passe, les analysent, donne les préférences de l'utilisateur en fonction des résultats de l'analyse, effectue la mutation des mots trouvés et, sur la base de tout cela, tente de récupérer les mots de passe .

Cette attaque permet, sans avoir recours à du temps et des calculs coûteux, de récupérer presque instantanément certains mots de passe cryptés avec des fonctions de hachage. L'idée de base derrière l'attaque par Intelligence Artificielle est qu'un utilisateur moyen choisi très souvent des mots similaires et des combinaisons de mots ou suit la même règle de génération de mots de passe lors de la création d'un mots de passe. En gardant cela à l'esprit, nous pouvons tenter de comprendre cette règle et choisir le mot de passe original.



Bien que cela semble un peu abstrait, dans la réalité, l'attaque se divise clairement en quatre étapes successives.
Au début, une collecte de données privées est effectuée. A cet étape, entre en action, le module de récupération de mots de passe et d'indexation, lequel recherche tous les mots de passe disponibles et cachés dans le système saisis par l'utilisateur à n'importe quel moment. Cela inclus les mots de passe d'accès au réseau, ICQ, email, FTP, les mots de passe de comptes Windows, de serveurs, de Secrets LSA, etc.

1. Lancement du module d'indexation et de collecte de données. Pendant l'exécution de cette étape, l'activité de l'utilisateur est analysée (ou de tous les utilisateurs, si le niveau module d'indexation choisi est différent de "**Léger**") dans le système. Ensuite, sur cette base, une liste de mots - de mots de passe possible, est générée à partir de fichiers textes, d'archives, d'historiques de navigateurs Internet, d'emails, etc.
2. Inclus un module d'analyse sémantique pour la base de données des mots de passe trouvés et ceux possible.
3. A la dernière étape, le module d'analyse de données effectuera une mutation des mots et tentera la récupération des mots de passe.

Au début de l'attaque, le programme recherchera pour le système tous les mots de passe qu'il connaît.

Pour cela, il y a 32 mini-modules pour le décryptage des mots de passe système, des mails, des navigateurs Internet, des messageries instantanées, des archives et autres. Puis vient l'indexation des fichiers et des données qui sont produites lors de la création du dictionnaire des attaques potentielles. Le troisième module divise les mots de passe et les mots en morceaux, afin que le dernier module les assemble en de nouvelles combinaisons pour choisir et deviner le mot de passe original.

En moyenne, avec les derniers niveaux d'indexations et de mutations le temps d'attaque peut varier entre 1 minutes et 10-15 minutes, en fonction de l'activité réseau de l'utilisateur.
Sur un ordinateur personnel, le temps de traitement prends normalement pas plus de 2-3 minutes. Habituellement, plus le niveau de mutation et d'indexation sera complexe, plus l'efficacité de la recherche sera élevée. Cependant, atteindre un niveau d'indexation et analyse élevé peut prendre plusieurs heures voir jours, en fonction de la vitesse de l'algorithme de validation du mot de passe et du nombre d'utilisateurs du système.

L'attaque par Intelligence Artificielle a prouvé qu'elle est la plus efficace lorsque la recherche est réalisée sur le système d'origine.
Seulement deux options sont disponible ici: le niveau de mutation des mots de passe et le niveau d'indexation des mots.
Les paramètres conseillées pour une attaque rapide sont: ***Léger:Léger***. Pour une recherche en profondeur (et en même temps lente), choisissez les paramètres ***Normal*** voir ***En profondeur***. La durée de l'attaque par Intelligence Artificielle dépends de la configuration de votre système, votre charge système et d'autres facteurs.

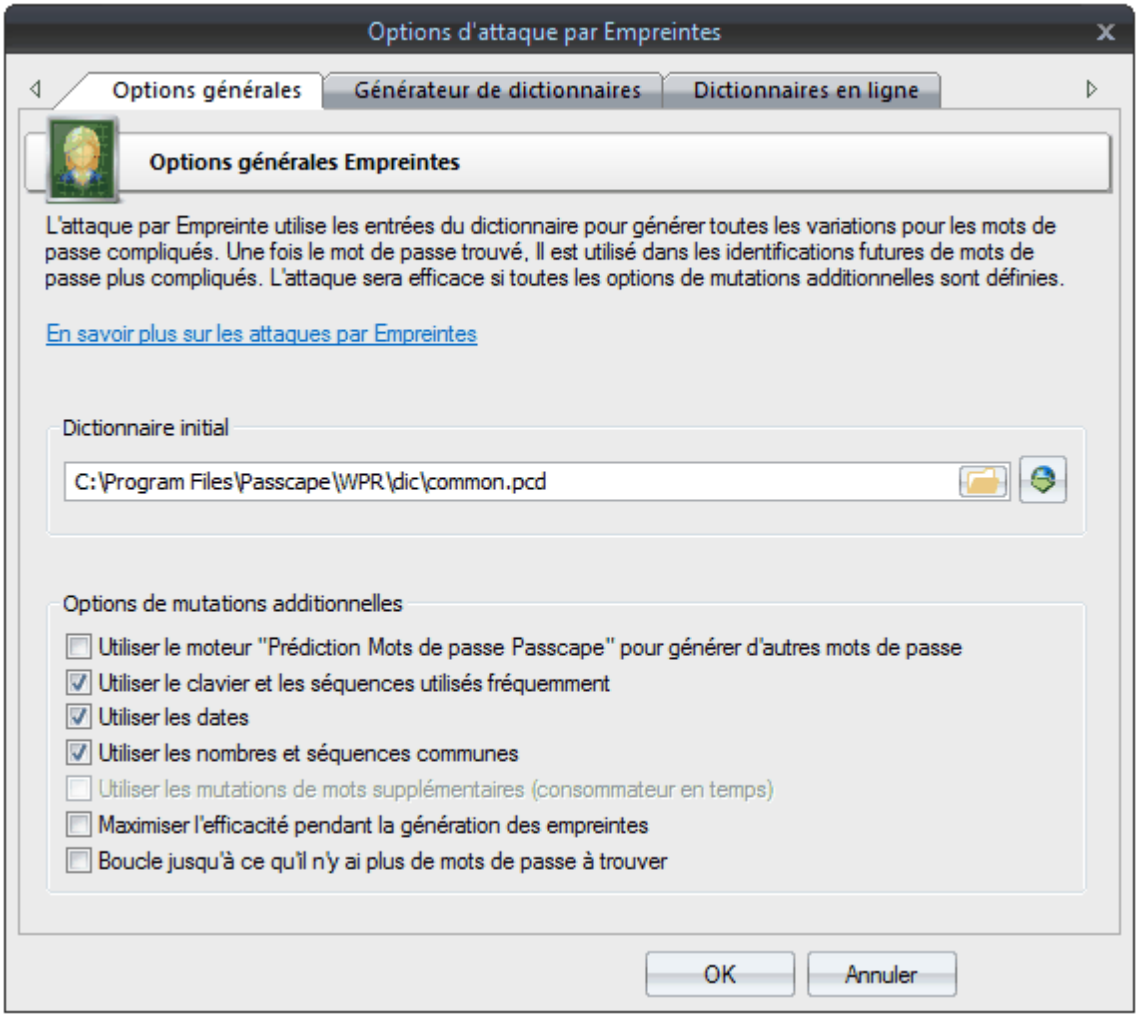
Il est fortement recommandé de fermer tous les autres programmes avant de lancer une attaque. Si votre attaque par Intelligence Artificielle s'exécute très lentement, vous pouvez avoir besoin de supprimer le cache de mots de passe de votre programme (par ex. si le total de mots de passe en cache excède 10000).

La version 9.5 de Windows Password Recovery est fournie maintenant avec une toute nouvelle fonctionnalité qui permets de rechercher les mots de passe en indexant les secteurs des disques sélectionnés. Cette fonctionnalité fonctionne avec les hachages LM et NTLM, l'analyse de mots de passe ASCII et UNICODE.
Vous pouvez modifier également les paramètres avancés ici. Par exemple, le '***Niveau d'ndexation des mots***' définit la mutation complémentaire de tous les mots de passe trouvés.
Attention, le parcours de tous les secteurs du disque dur avec l'option réglée sur '***En profondeur***' peut prendre beaucoup de temps. Notez également, que l'algorithme de scanne des secteurs n'est pas efficace avec les disques qui ont un cryptage comme Bitlocker ou TrueCrypt, par exemple.

2.8.2.3 Attaque par Empreinte

L'attaque par Empreinte est un outil relativement nouveau pour la récupération de mots de passe complexes, lesquels ne peuvent pas être décryptés par d'autres attaques. L'idée de cette attaque est de récupérer un mot de passe, non pas un mot individuel provenant du dictionnaire, comme avec l'attaque par dictionnaires, ni une combinaison de mots, comme avec l'attaque combinée, mais à base d'Empreintes.
Tous les mots sources provenant du dictionnaire sont utilisés pour générer plusieurs empreintes. Si un des mots de passe est trouvé durant cette attaque, il participera à la génération de nouvelles empreintes, et l'attaque reprendra depuis le début.

Avant de lancer l'attaque, il est nécessaire de fournir le dictionnaire source à utiliser pour la création de la banque d'empreintes. Le logiciel est livré avec un dictionnaire, common.pcd, optimisé pour cette attaque. Mais vous pouvez utiliser le votre ou en télécharger un sur Internet (Onglet "Dictionnaires en ligne"). Il n'y a pas de conditions particulières pour le dictionnaire, excepté le fait qu'il ne doit pas avoir une taille trop importante., sinon, l'attaque prendra un beaucoup de temps.
Vous pouvez utilisez les dictionnaires avec des mots de passe nationaux, si vous suspectez que le mot de passe recherché contient des caractères nationaux.



Voici la méthode pour générer des empreintes: en premier, chaque mot provenant du dictionnaire source sera divisé en mots de passe d'un caractère, ensuite en mots de passe de 2 caractères, etc.
Par exemple, le mot **crazy** divisé en empreintes d'un caractère. Vous obtenez:
c
r
a
z
y
Maintenant, en deux caractères:
cr
ra
az
zy
Puis en trois caractères:
cra
raz
azy
Et finalement en quatre caractères:
craz
razy

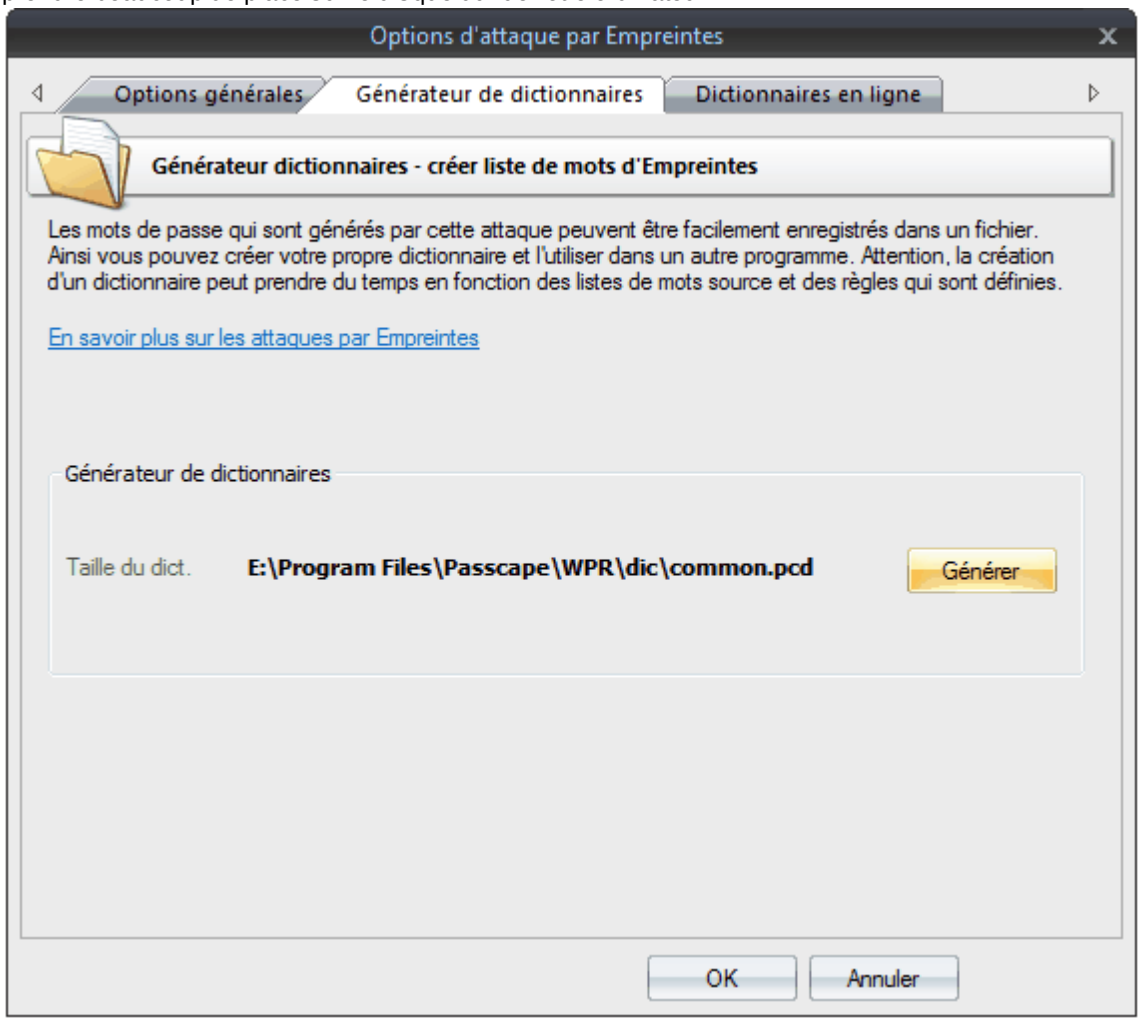
Vous obtenez ainsi 5+4+3+2=14 empreintes, sans compter le mot source.
Répétez cela pour chaque mot du dictionnaire source. Après cela, toutes les empreintes seront dumpées dans une base de données unique, sans doublons. Vous obtenez une base de données d'empreintes qui sera utilisée pour tester les mots de passe en collant toutes les empreintes entre elles, afin de trouver le mot de passe.

Le réel algorithme d'empreintes est un peu plus sophistiqué. Toutefois, il y a une option dans les paramètres d'attaque, **Maximiser l'efficacité pendant la génération des empreintes**, qui utilise un algorithme plus sophistiqué, qui maximise l'efficacité (au détriment de la vitesse) en générant des empreintes additionnelles.

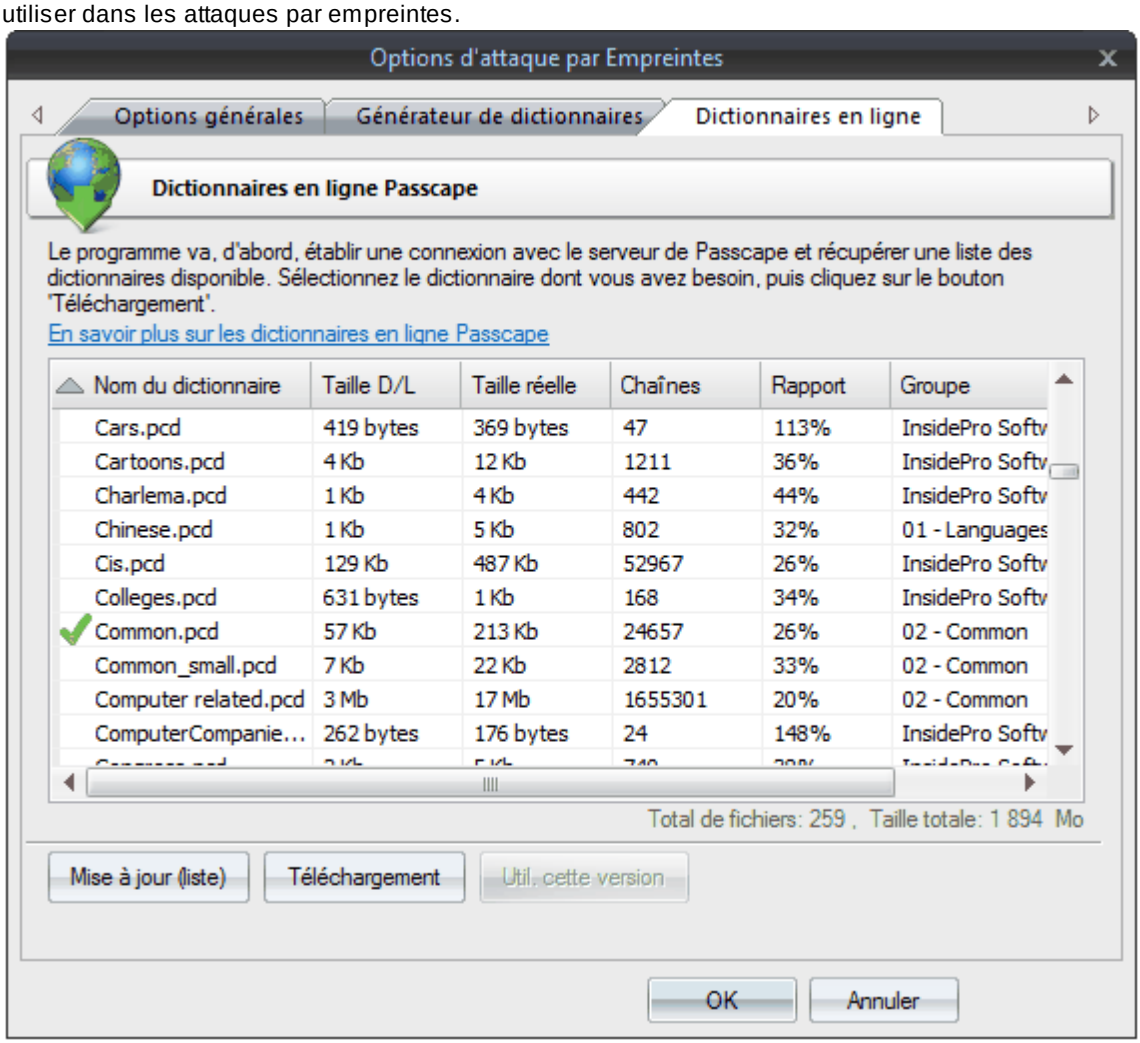
Jetons un coup d'œil aux options restantes:
Utilise le moteur "Prédiction Mots de passe Passcape" pour générer d'autres mots de passe - utilise les mots de passe trouvés dans d'autres attaques lors de la génération des empreintes.
Utiliser le clavier et les séquences utilisés fréquemment - ajoute les combinaisons de claviers et les séquences fréquentes à la banque d'empreintes.
Utiliser les dates - ajoute les dates aux empreintes.
Utiliser les nombres et séquences communes - utilise les chiffres et les combinaisons simple de lettres.

La plus grande attention doit être apportée à l'option "**Boucle jusqu'à ce qu'il n'y ai plus de mots de passe a trouver**". C'est là ou l'attaque par empreintes montre son efficacité.
Voici comment cela fonctionne: si au moins un mot de passe est trouvé pendant l'attaque, quand l'attaque se termine, le mot de passe participe à la création des nouvelles empreintes, et l'attaque redémarre. Cette option fonctionne très bien sur les grandes listes de hachages et sur les hachages d'historique de mot de passe. Cependant, une fois que cette option est activée, vous ne serez plus capable de lancer l'attaque à partir de la dernière position sauvegardée.

Le second onglet comporte des paramètres permettant de créer et d'enregistrer un dictionnaire personnalisé utilisant les options courantes de l'attaque par empreintes. Attention; le dictionnaire peut prendre beaucoup de place sur le disque dur de votre ordinateur.



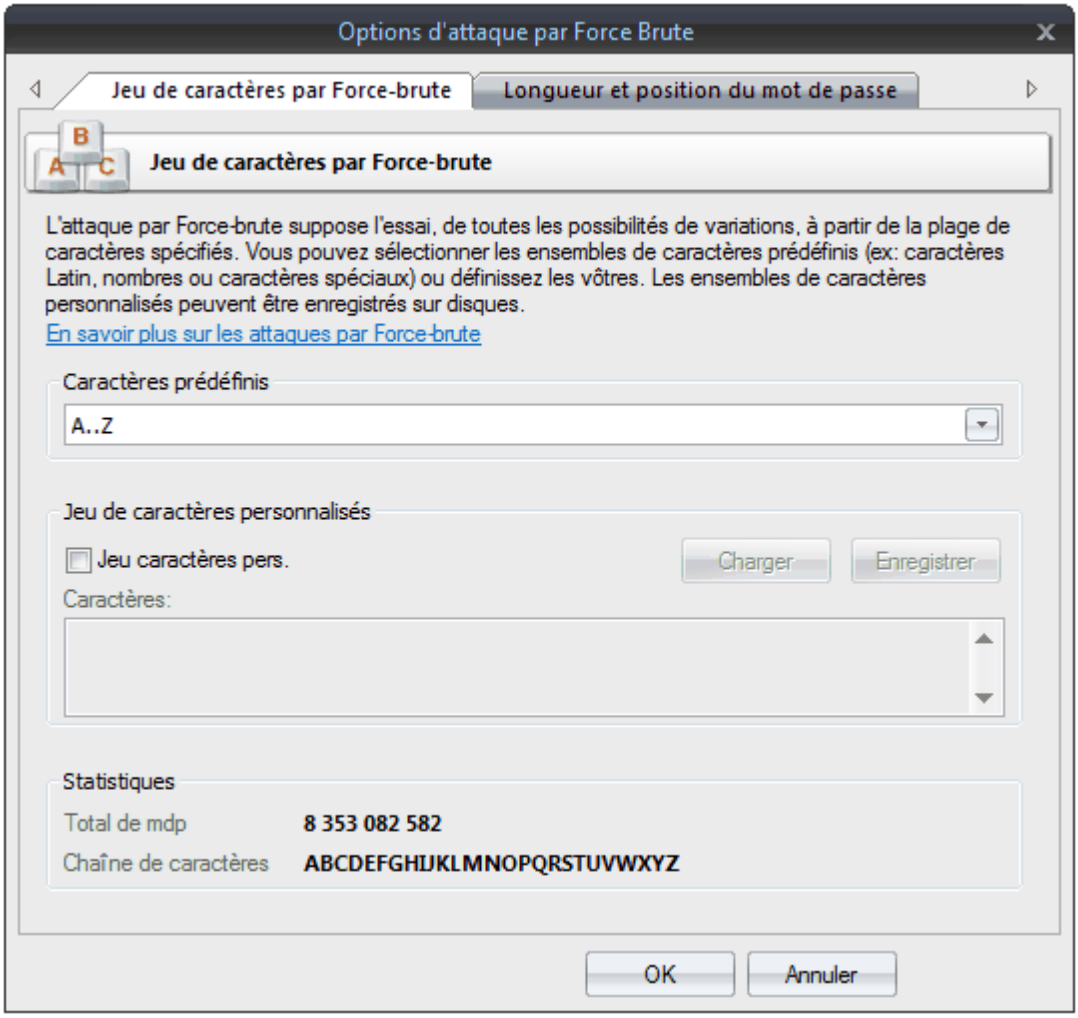
Dans le troisième onglet, vous pouvez télécharger des dictionnaires sources à partir d'Internet pour les utiliser dans les attaques par empreintes.



2.8.2.4 Attaque par Force-brute (recherche exhaustive)

En crypto-analyse, une attaque par Force-brute est une méthode pour venir à bout d'un modèle de cryptographie en essayant un large nombre de possibilités; par exemple, travailler exhaustivement avec toutes les clés possibles pour décrypter un message. Cette définition a été extraite du site de Wikipedia.

En quelques mots, une attaque par Force-brute devine un mot de passe en essayant toutes les variantes possibles à partir d'un jeu de caractères. Par exemple, en testant toutes les combinaisons du jeu de caractères Latin en minuscule, qui est *'abcdefghijklmnopqrstuvwxyz'.* Une attaque par Force-brute est très lente. Par exemple, une fois choisi le jeu de caractères Latin pour votre attaque par Force-brute, vous devez parcourir les 217 180 147 158 variantes pour un mot de passe de 1-8 symboles. Cette méthode doit être utilisée seulement si toutes les autres attaques ont échoué dans la récupération de votre mot de passe.



Les options de l'attaque par Force-brute sont constitués de deux onglets.

Dans le premier onglet, vous pouvez définir la plage de caractères à rechercher. Vous pouvez utiliser les jeux de caractères prédéfinis ou créer les vôtres. Pour définir votre propre jeu de caractères, sélectionnez l'option "*Utiliser un jeu de caractères personnalisé*". Cela activera un champ pour définir le jeu de caractères personnalisé. Les caractères peuvent être ASCII ou non-imprimables. Vous pouvez enregistrer votre jeu de caractères personnalisé sur le disque dur. Le programme est fourni avec plusieurs exemples de jeux de caractères prédéfinis.

Dans le deuxième onglet, vous pouvez définir la longueur minimum et maximum des mots de passe à rechercher. Notez, que pour l'attaque des hachages LM, la longueur maximum des mots de passe ne doit pas excéder 7 caractères. Vous pouvez aussi définir le mot de passe de départ, à partir du quel vous souhaitez démarrer la recherche.

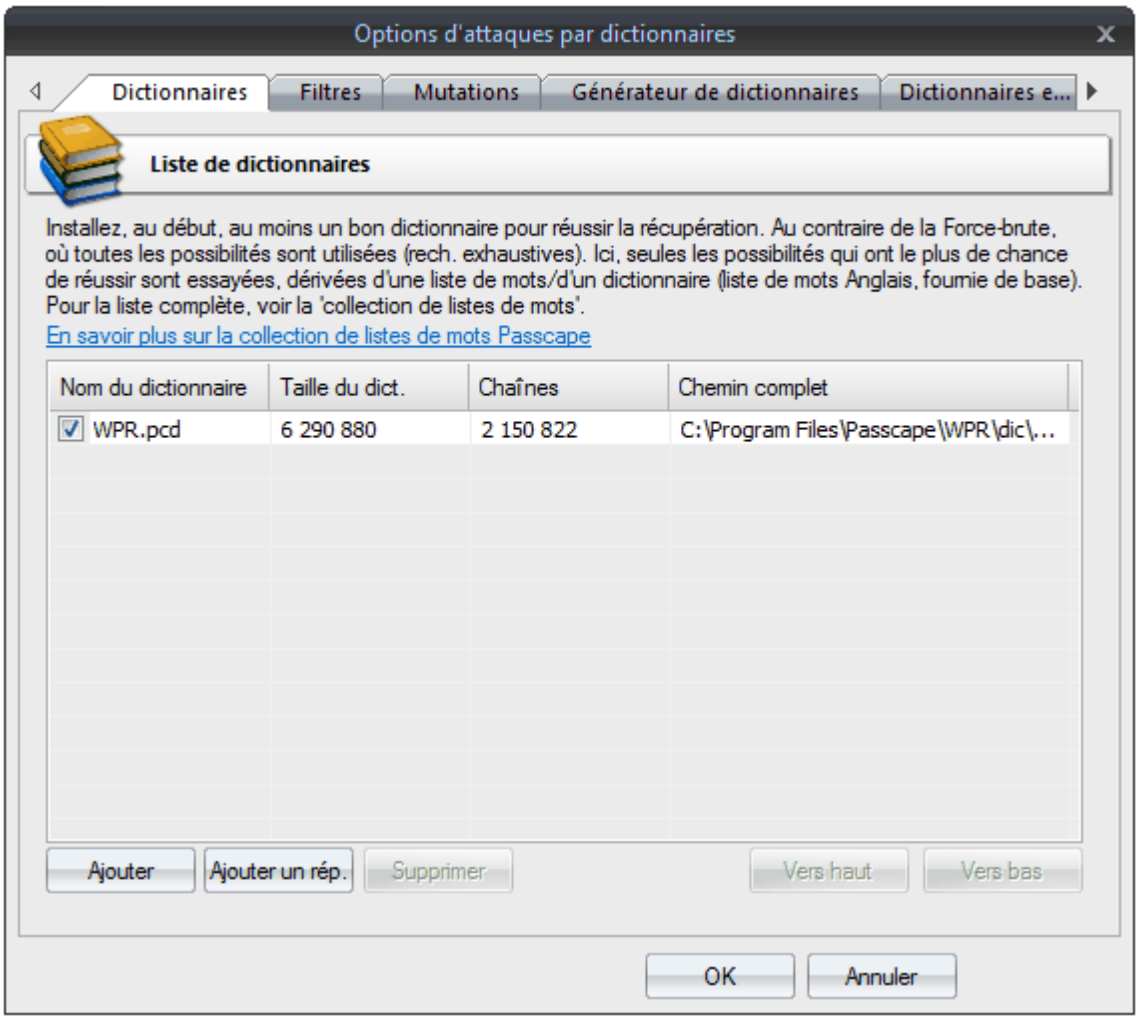
Dans le tableau suivant, vous pouvez voir la 'force' du mot de passe en fonction de sa longueur et de sa complexité. Sachant que la vitesse de récupération est de 100M de mots de passe par seconds.

Jeu de caractères	Longueur du mot de passe	Exemple de mot de passe	Temps pour le 'cracker' (recherche par Brute-force)
A .. Z	5	CRUEL	immédiatement
A .. Z	6	SECRET	3s
A .. Z	7	MONSTER	1m 23s
A .. Z	8	COOLGIRL	36m 11s
A .. Z, 0 .. 9	5	COOL3	immédiatement
A .. Z, 0 .. 9	6	BANG13	22s

A .. Z, 0 .. 9	7	POKER00	13m 26s
A .. Z, 0 .. 9	8	LETMEBE4	8h 3m 37
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	DidIt13	9h 56m 33s
A .. Z, a .. z, 0 .. 9	8	GoAway99	25jours 16h 26m 34s

2.8.2.5 Attaque par Dictionnaire

A la différence de l'attaque par Force-brute, où toutes les possibilités sont essayés exhaustivement, une attaque par Dictionnaire essaye seulement les possibilités qui ont le plus de chance de réussir, typiquement dérivées d'une liste de mots ou d'un dictionnaire. Généralement, les attaques par Dictionnaire réussisse parce que beaucoup de monde à tendance à choisir des mots de passe courts, des mots simples dans un dictionnaire, ou sont de simples variantes facile à prédire.



Dans l'onglet '*Dictionnaires*', choisissez la liste de dictionnaires à utiliser pour l'attaque. Le logiciel supporte les dictionnaires textes aux formats ASCII, UNICODE et UTF8, tout comme ceux cryptés/compressés au format natif PCD, développé par Passcape. Les listes de mots compressées au format ZIP et RAR sont également supportées avec certaines restrictions.
Pour désactiver un dictionnaire, il suffit de décocher la case devant son nom. Le dictionnaire restera dans la liste mais ne sera pas utilisé pendant l'attaque.
Le logiciel est fourni avec un dictionnaire de 360000 mots. Pour la liste complète des dictionnaires, consultez notre collection complète de listes de mots. Ou vous pouvez utiliser, aussi, nos dictionnaires en ligne comme alternative.

L'onglet '*Filtres*' permets de filtrer les mots d'un dictionnaire par inclusions/exclusions. Si le premier filtre d'inclusions, est activé, l'attaque acceptera seulement, les mots qui contiennent au moins un des caractères contenus dans le champ du filtre. Si le second filtre, exclusion, est activé, le programme sautera les mots qui contiennent au moins un des caractères contenus dans le champ du filtre.

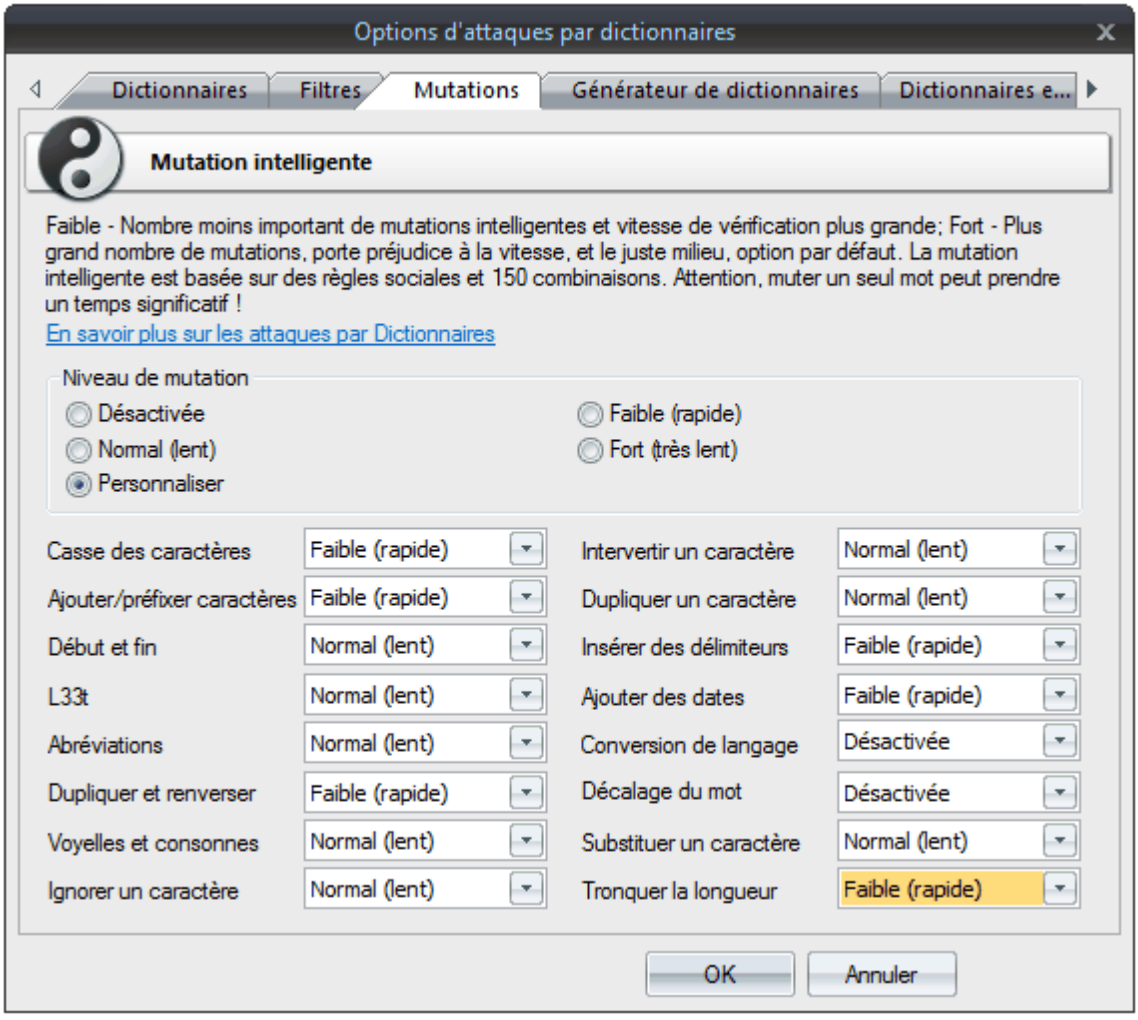
L'onglet '*Mutations'* permets de paramétrer toutes les combinaisons possibles de mots à rechercher. Par exemple, si vous choisissez une forte mutation, le programme créera plusieurs centaines d'analogies pour chaque mot du dictionnaire. Par exemple, secret - Secret - s3cr3t - secret123, et ainsi de suite. Vous pouvez aller jusqu'à trois règles de mutations: '*Faible'* - qui génère très peu de mutations et une grande vitesse de vérification; '*Fort*' - qui génère un grande de mutations, au préjudice de la vitesse, et en intermédiaire, vous disposez d'un réglage médian '*Normal'* par défaut.

Vous pouvez utiliser le '*Générateur de Dictionnaire*' pour créer votre propre liste de mots (dictionnaire) en fonction du réglage effectués dans les trois premiers onglets.

Dictionnaires en ligne. Le programme possède une fonctionnalité qui permets de télécharger et d'utiliser des dictionnaires disponible sur le site Web de Passcape. Nous avons accumulé une large collection de dictionnaire - plus de 250 différents. Cela vous évitera une recherche supplémentaire sur Internet pour trouver ce dont vous avez besoin.

Personnaliser les mutations

A partir de la version 4.0, le programme a la possibilité de personnaliser la mutation intelligente de l'attaque par Dictionnaire. Toutes les mutations sont divisées en 16 groupes principaux. Vous pouvez régler le niveau de mutations sur un des trois niveau ou la désactiver, séparément pour chaque groupe.



Par exemple, vous pouvez désactiver la mutation OEM (et ainsi doubler votre vitesse d'attaque par

Dictionnaire) si vous êtes sûr que le mot de passe que vous recherchez contient seulement des caractères Latin.

La description de la signification de ces groupes est donnée par le tableau suivant:

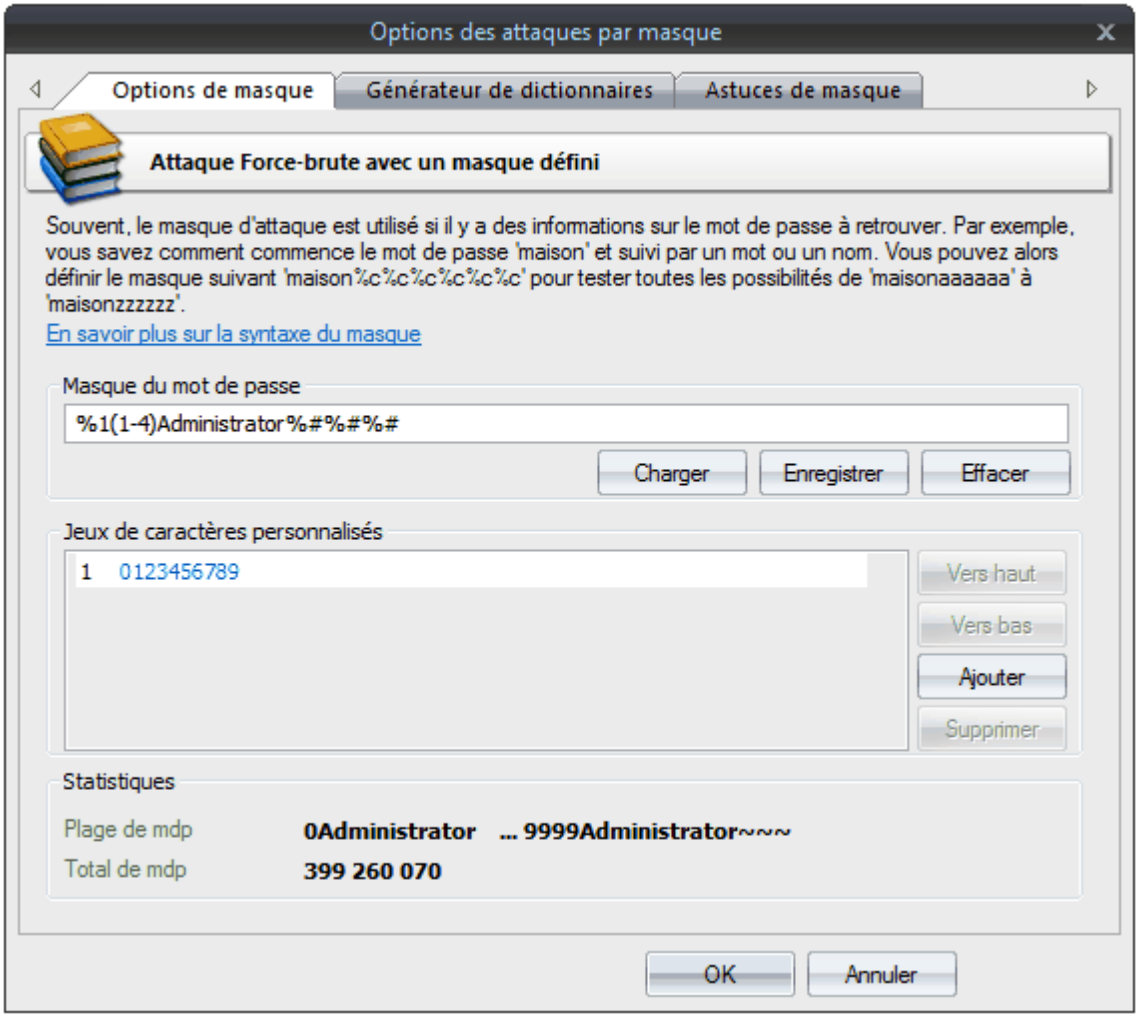
Nom du groupe	Description	Exemples (pour le mot '**password**')	Commentaires
Casse des caractères	Teste les combinaisons de casses pour le mot saisi.	Password, PassworD, PaSsWoRd	Le niveau maximum (Fort) d'un groupe de mutation NE GÉNÈRE pas tous les combinaisons de casses possibles des mots saisis. Pour tester toutes les variantes de cas possibles, pensez à utiliser l'attaque par Dictionnaire Hybride (règle **aN**)
Ajouter/ préfixer des chiffres	Ajoute des chiffres au début ou à la fin du mot.	password99, 2Password, PASSWORD3	Le niveau maximum ajoute 2 chiffres.
Début et fin	Presque le même que le précédent, mais mais ajoute au début ou à la fin des mots, des abréviations, des caractères et des combinaisons de claviers, etc.	#Password#, password12345, 4everPASSWORD, Passwordqwerty	
L33t	Crée différentes combinaisons en utilisant le langage leet.	p@ssword, P@$$w0rd, P@$$W0RD	
Abréviations	Converti plusieurs combinaisons de caractères (si le mot d'origine en contient une) en abréviation.	ihateyou -> ih8you, Ih8u	
Dupliquer et renverser	Renverse, duplique le mot, etc.	drowssap, passwordpassword, PasswordDrowssap	
Voyelles et consonnes	Réalise une mutation des voyelles et des consonnes (caractères Anglais seulement).	Psswrd, PaSSWoRD, pAsswOrd	
Ignorer un caractère	Saute un caractère du mot original.	assword, Passwrd, Pasword	
Intervertir un caractère	Interverti deux caractères adjacents.	apssword, Passowrd	
Dupliquer un caractère	Duplique des caractères.	ppasword, ppaasswwoorrdd, Passwordddd	
Insérer des délimiteurs	Sépare les caractères avec des délimiters comme des points ou des traits d'unions.	p.a.s.s.w.o.r.d, P-a-s-s-w-o-r-d	Niveau maximal est de 10 délimiteurs.
Ajouter des dates	Ajoute des dates à la fin des mots.	Password2010, password1980	Souvent le moteur de mutations peut générer plus de variations compliquées (par exemple, password03171998 ou Password19710830), cette fonction est

Nom du groupe	Description	Exemples (pour le mot '**password**')	Commentaires
			désactivée, ici, dans le niveau maximum de mutations.
Conversion de langage	Converti les mots Anglais en autre langage et vice-versa en utilisant un clavier alternatif (autre clavier, par ex. second langage de l'OS).	Si votre OS possède deux langages installés (comme Anglais et Russe), le programme convertira le mot d'origine '**password'** en Russe '**зфыыцщкв**', et en Russe **пароль** sera converti en '**gfhjkm'**.	Le programme fonctionne correctement pour 2 ou plus de langages. Ainsi si vous avez 5 langages installés localement (incluant l'Anglais), Il y aura 4 différentes combinaisons de mots.
Décalage du mot	Décale stupidement tous les caractères du mot vers la droite ou la gauche.	asswordp, dpasswor	
Substituer un caractère	Remplace un caractère d'un mot.	oassword, passqord	C'est une règle un peu utile si on tient compte du fait que les caractères de substitutions sont pris d'une table spéciale. Par exemple, le caractère 's' sera remplacé avec les suivants: 'a', 'w', 'e', 'd', 'x', 'z'. Vous pouvez noter que tous ces caractères sont situés près du 's' sur un clavier Qwerty.
Tronquer la longueur	Réduit la longueur du mot pour essayer toutes les combinaisons possibles de longueurs.	passwor, passwo, Pass	

2.8.2.6 Attaque par Masque

L'attaque par Masque est un outil irremplaçable lorsque l'on connaît déjà une partie du mot de passe ou des informations sur son contenu. Par exemple, lorsque vous savez que le mot de passe à une longueur de 12 caractères et se termine par *qwerty*, il est évident que lancer une recherche de tous les mots de passe de 12 caractères est impensable. Seul une recherche des 6 premiers caractères est nécessaire pour trouver le mot de passe. Ce type d'attaque par Masque est conçu pour cela.

Dans notre cas, vous pouvez définir le masque suivant: **%c%c%c%c%c%cqwerty**. Ce qui signifie que le programme devra tester en série les combinaisons suivantes: aaaaaaqwerty .. zzzzzzqwerty. Si le mot de passe d'origine est *'secretqwerty'*, il est effectivement dans notre plage de recherche.



Le champ de saisie du masque est utilisé pour définir la règle, qui permettra au programme de tenter de trouver le mot de passe. Si le masque est défini correctement, dans la fenêtre '*Statistiques*' s'affichera la plage de caractères générée par le masque. Les masques créés peuvent être sauvegardés sur le disque de l'ordinateur. Vous pouvez aussi utiliser l'outil de création de masques pour générer un dictionnaire (disponible uniquement dans certaines versions du programme).

La syntaxe du masque est un peu classique et est constituée en jeux ou caractères statiques (non modifiables) et dynamiques (modifiables). Les caractères ou jeux de caractères dynamiques sont toujours constitués d'un caractère principal '%'. Par exemple, si vous définissez le masque secret%d(1-100), le programme générera 100 mots de passe (secret1, secret2: secret100).

Windows Password Recovery supporte les jeux de masques de caractères suivants:

- %c caractères Latin en minuscules (a..z), 26 lettres
- %C caractères Latin en majuscules (A..Z), 26 lettres
- %# jeu complet de caractères spéciaux (!..~ espace), total 33 lettres/ symboles
- %@ petit jeu de caractères spéciaux (!@#$%^&*()-_+= espace), 15 symboles
- %? tous les caractères imprimables avec le code ASCII de 32..127
- %* Tous les caractères ASCII (codes de 1 à 255)
- %d un chiffre (0..9)
- %d(x-y) nombres inclus en x et y
- %r(x-y) caractères choisis par l'utilisateur avec le code UNICODE en série entre x et y
- %r(x1-y1,x2-y2...xn-yn) jeu de plusieurs séquences sans chevauchement de caractères UNICODE.
- %[1..9] un caractère du jeu de caractères personnalisé 1..9

- %[1..9](min-max) plage personnalisé de longueur variable (du min à max). Vous pouvez définir jusqu'à 9 jeux de caractères personnalisés.
- %% caractère statique indépendant %

Exemples:
test%d - générera une plage de mots de passe de test0..test9, un total de 10 mots de passe
test%d(1980-2007) - test1980 .. test2007, 28 mots de passe
test%r(0x0600-0x06ff) - 256 mots de passe avec des caractères Arabe à la fin
%#test%# - _test_ .. ~test~, 1089 mots de passe
admin%1(1-5) - admina .. adminzzzzz, où %1 est un caractère du jeu 1 personnalisé (a..z)
%1%1%1pin%2%2%2 - aaapin000 .. zzzpin999, %1 est un jeu de caractères personnalisé de a..z et %2 est un deuxième jeu de caractères personnalisé contenant les caractères de 0..9

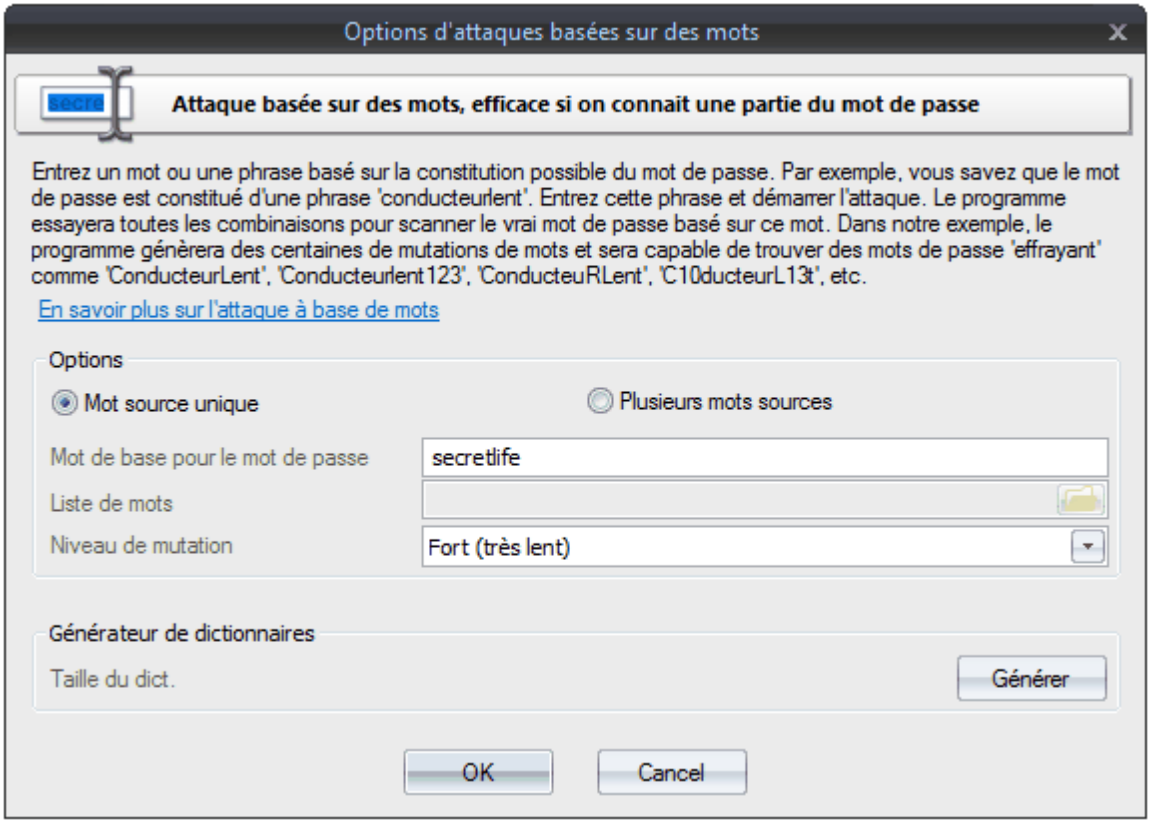
En passant à l'onglet '***Générateur de dictionnaires***', vous pouvez générer votre propre dictionnaire à l'aide d'un masque, et le sauvegarder sur le disque. Cette fonctionnalité est disponible, uniquement, dans la version 'Advanced' du programme.

Le troisième onglet '***Astuces de masque'*** contient une description de la syntaxe des masques et un ensemble d'exemples.

2.8.2.7 Attaque à base de Mots

L'attaque à base de Mots (développée par Passcape) est sous plusieurs aspects similaire à l'attaque par Masque. Cependant, ici, vous n'avez pas besoin de définir la syntaxe; entrez simplement les lettres du mot, qui sont supposées être la base du mot de passe. C'est un outil de récupération irremplaçable lorsque l'on connaît une partie du mot de passe ou de sa composition. Normalement, dans ces cas on utilise l'attaque par Masque; cependant, elle ne permets pas toujours de faire face à cette tache. Supposez que votre mot de passe soit *'S10wDr1v3r'*. Si essayez de trouver un mot de passe compliqué en utilisant de l'attaque par Force-brute, cela n'aboutira pas, même si vous êtes sûr qu'il est basé sur le mot *'slowdriver'*. C'est dans ce cas que l'attaque à base de mots vous sauvera.

Avec cet outil, le programme essayera de trouver le mot de passe original, en essayant toutes les combinaisons possibles basées sur 15 groupes de règles (un total de plus de 150 règles). Si vous saisissez *'slowdriver'* dans le champ 'Mot de base pour le mot de passe', vous verrez que le programme a généré plusieurs milliers de différentes combinaisons de cette phrase, et seulement une combinaison corresponds à votre mot de passe.



Si la longueur de la phrase saisie dépasse les 8-10 caractères, la mutation peut prendre beaucoup de temps. Si vous vous souvenez du mot de passe original et que vous avez tout simplement oublié la séquence des caractères en minuscules/majuscules, vous pouvez sélectionner l'option, pour le niveau de mutation '***Muter uniquement la casse des caractères (majuscules/minuscules)***'.
Avec cette option activée, le programme générera les mots de passe avec toutes les combinaisons de caractères en majuscules et minuscules, pour un total de 2^n mots de passe, où n - est la longueur du mot de passe.
Par exemple, pour le mot de passe *'slowdriver', le programme générera* 2^10=1024 différentes combinaisons pour chaque types de claviers installées sur votre ordinateur. Vous pouvez aussi générer un dictionnaire de ces mutations et le sauvegarder sur votre disque (fonction non disponible dans toutes les versions du logiciel).

Notez, que si la longueur du mot de passe dépasse les 15-16 caractères, cela peut prends du temps pour préparer (muter) le mot de passe pour l'attaque.

Dans la version 9.5 de Windows Password Recovery, la récupération par mots a été divisé en 2 modes: '***Mot source unique*** et '***Plusieurs mots sources***'. Le mode avec plusieurs mots source fonctionne comme avec l'attaque par Dictionnaire avec un maximum de mutations actives, mais cela génère beaucoup plus de mots de passe (comme si le niveau de mutations de l'attaque à base de Mots était réglé à 'Faible'), ce qui peut être utile dans certaines situations.

2.8.2.8 Attaque par Dictionnaires combinés

L'attaque par Dictionnaires combinés (développée par Passcape Software) est idéale pour la récupération de mots de passe qui sont constitués de 2, 3 ou de 4 mots.
Ce type d'attaque pour les mots de passe difficiles et composés est très similaire à une simple attaque par dictionnaire, excepté le fait qu'à la place d'utiliser un simple mot pour tester le mot de passe, ici, nous utilisons une combinaison de mots ou une phrase créée en combinant plusieurs mots à partir de dictionnaires spécifiques.
Pour utiliser cette attaque, il est nécessaire de choisir au moins deux dictionnaires et de définir les règles pour générer les mots de passe. Vous pouvez choisir des dictionnaires classiques utilisés dans l'attaque par Dictionnaire, mais il est recommandé d'utiliser de petits dictionnaires avec le plus de mots communs.

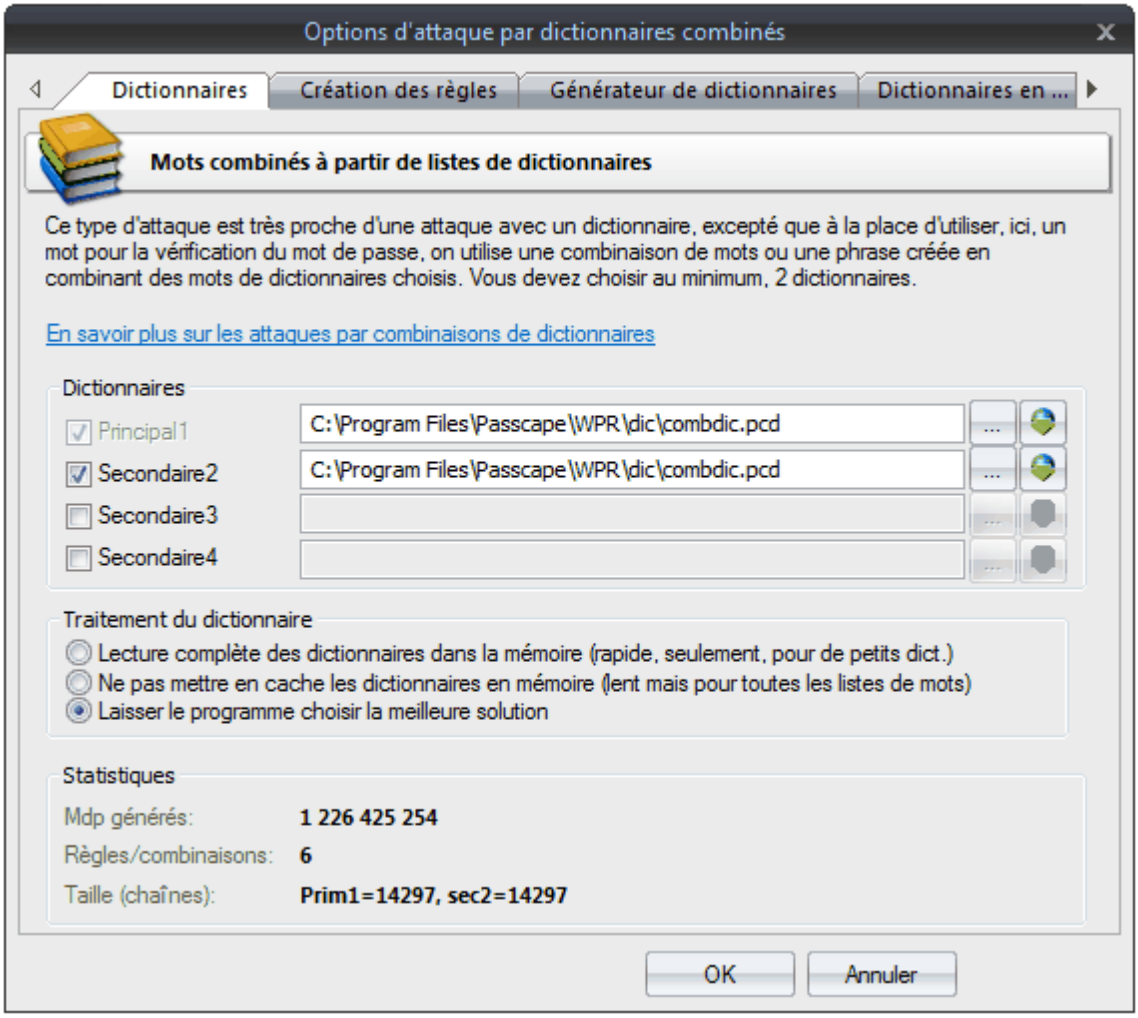
Les dictionnaires parfait pour cela sont ceux qui ont différentes formes pour les même mots; ex. jump, jumper, juped, jumping.

L'attaque combinée possède 'une certaine limite au nombre de dictionnaires qui peuvent être utilisés, avec un maximum possible de 4 dictionnaires. Du coup, la limitation de cette attaque ne permets pas la récupération d'un mot de passe composé d'une phrase de plus de 4 mots.

L'autre inconvénient est la largeur des phrases générées. Et, comme conséquence, l'augmentation proportionnelle du temps prit pour le test d'un mot de passe. Gardez à l'esprit que durant la génération des mots de passe constitués de 3 ou 4 mots, le processus peut prendre un temps beaucoup de temps.

Si trouver le dictionnaire, le plus adapté est difficile, ne vous soyez pas inquiet. Le logiciel est fourni un dictionnaire spécialement adapté pour l'attaque combinée. Vous pouvez aussi vous servir de l'onglet 'Dictionnaires en ligne' ou le bouton (icône vert) pour télécharger des dictionnaires similaires du site Web de Passcape.

Dictionnaires



La manière dont l'attaque combinée fonctionne est relativement simple. Par exemple, si vous avez défini deux dictionnaires, le programme générera les mots de passe de la manière suivante: il prendra le premier mot à partir du premier dictionnaire et le collera au premier mot du second dictionnaire, puis avec le second mot, et ainsi de suite jusqu'à la fin.

Pour comprendre comment l'attaque combinée fonctionne, jetons un coup d'œil sur deux exemples de mots de passe générés utilisant, dans le premier cas, le même dictionnaire et dans le second cas - deux différents.

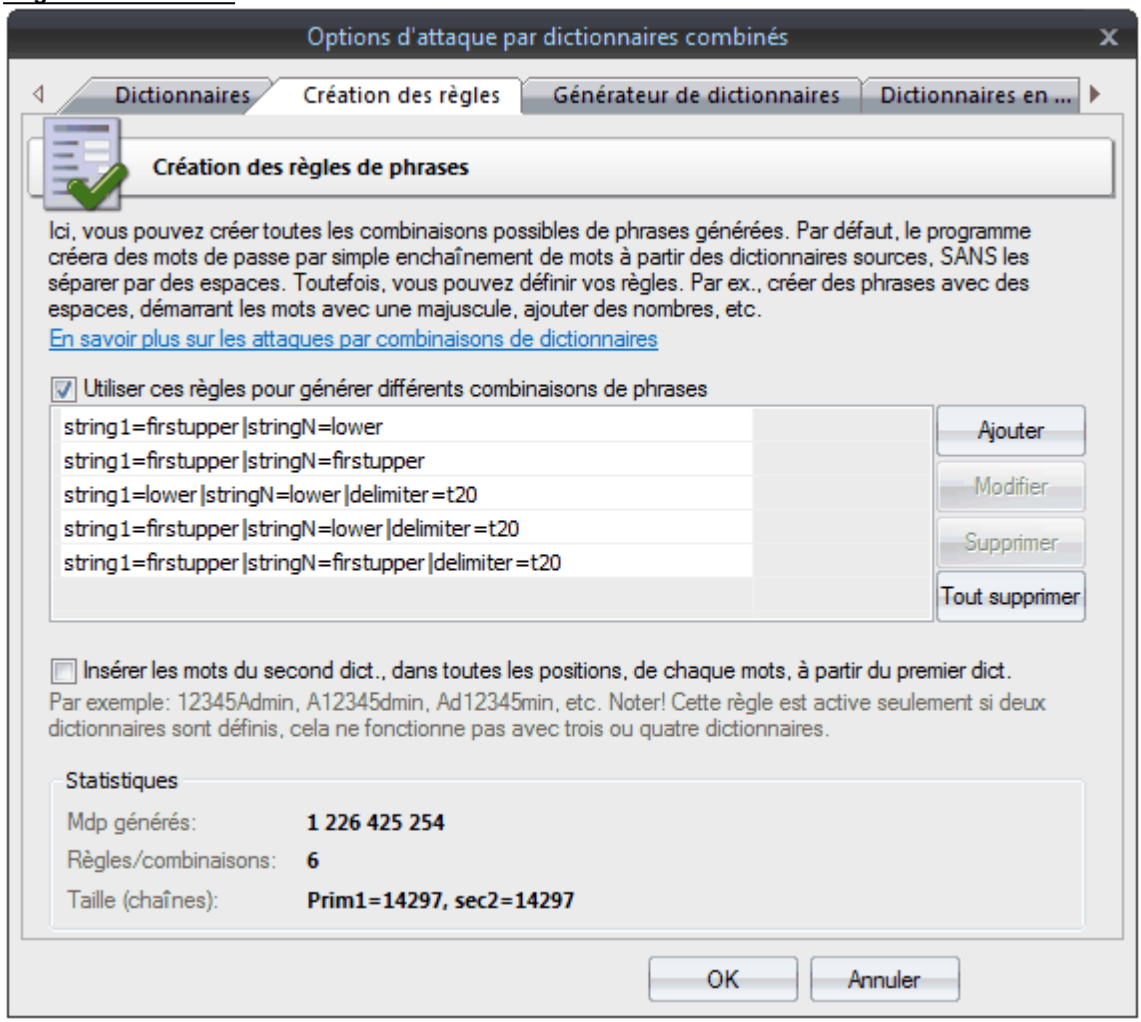
1. Supposons que vous avez un simple dictionnaire avec trois mots: action, bad, et computer. Et que vous l'avez défini comme dictionnaire pour les deux sources : dictionnaire principal1 et secondaire2

(voir l'image ci-dessus). Après l'analyse de ces dictionnaires, vous obtiendrez les phrases suivantes (elles seront utilisées pour tester le mot de passe à trouver):
'actionaction', 'actionbad', 'actioncomputer'
'badaction', 'badbad', 'badcomputer'
'computeractio', 'computerbad', 'computercomputer'.
un total de 9 phrases.

2. Dans le second cas, nous avons deux dictionnaires différents. Par exemple, le premier dictionnaire est constitué de trois mots: action, bad, et computer. Le second est constitué de trois mots: date, eagle, fail. Dans ce cas, nous allons obtenir les phrases suivantes:
'actiondate', 'actioneagle', 'actionfail'
'baddate'', 'badeagle', 'badfail'
'computerdate', 'computereagle', 'computerfail'.

L'exemple est simple mais un bon exemple. L'idée est que pour les sources multiples vous pouvez utiliser à la fois un simple dictionnaire et plusieurs. Tout dépends de votre imagination. Le dernier exemple montre une attention toute particulière à l'ordre des dictionnaires si ils sont différent. L'ordre des mots dans les phrases à créer dépend directement de l'ordre des dictionnaires sources.
Dans notre second exemple, si vous inversez le dictionnaire principal et le secondaire, en sortie, vous obtiendrez un ensemble de phrases complètement différentes.

Règles de mutations

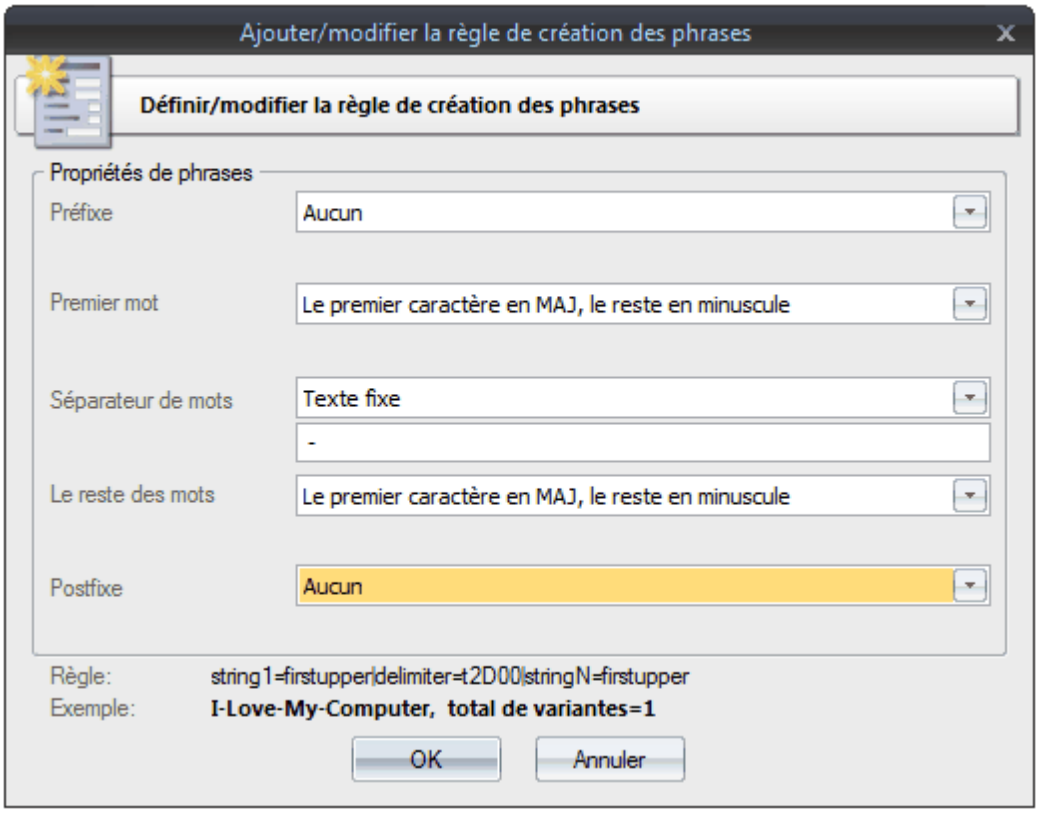


Les mots de passe créés par l'attaque combinée sont générés en fonction des règles spéciales qui ont été définies dans le deuxième onglet '***Création des règles***'. Par défaut, lorsque les règles de création des mots de passe sont désactivées, le programme génère des mots de passe en collant les mots provenant des dictionnaires, sans les séparer par un espace. Par exemple, avec les deux mots 'my' et 'computer',

vous obtenez 'mycomputer'.

Si l'option d'insertion de mots est activée, le programme créera des mots de passe complémentaires en insérant des mots du second dictionnaire dans toutes les positions du mot à partir du dictionnaire 1. Par exemple, si le premier mot du dictionnaire est **Admin**, et le mot du second dictionnaire est **12345**, le programme générera les mots de passe suivants:
12345Admin
A12345dmin
Ad12345min
Adm12345in
Admi12345n
Et ainsi de suite pour tous les mots du second dictionnaire. Puis prends un autre mot du dictionnaire 1, etc. L'option est activée si seulement 2 dictionnaires sont définis.

Les règles sont conçues pour étendre les options de recherches des mots de passe. Par exemple: Mycomputer, MyComputer, MY COMPUTER, my-computer, etc. Il y a des règles spéciales disponibles pour cette fonctionnalité; vous n'avez pas besoin de connaître leurs syntaxes, pour les boites de dialogues de création des règles de mutations, elles sont simples et intuitives.



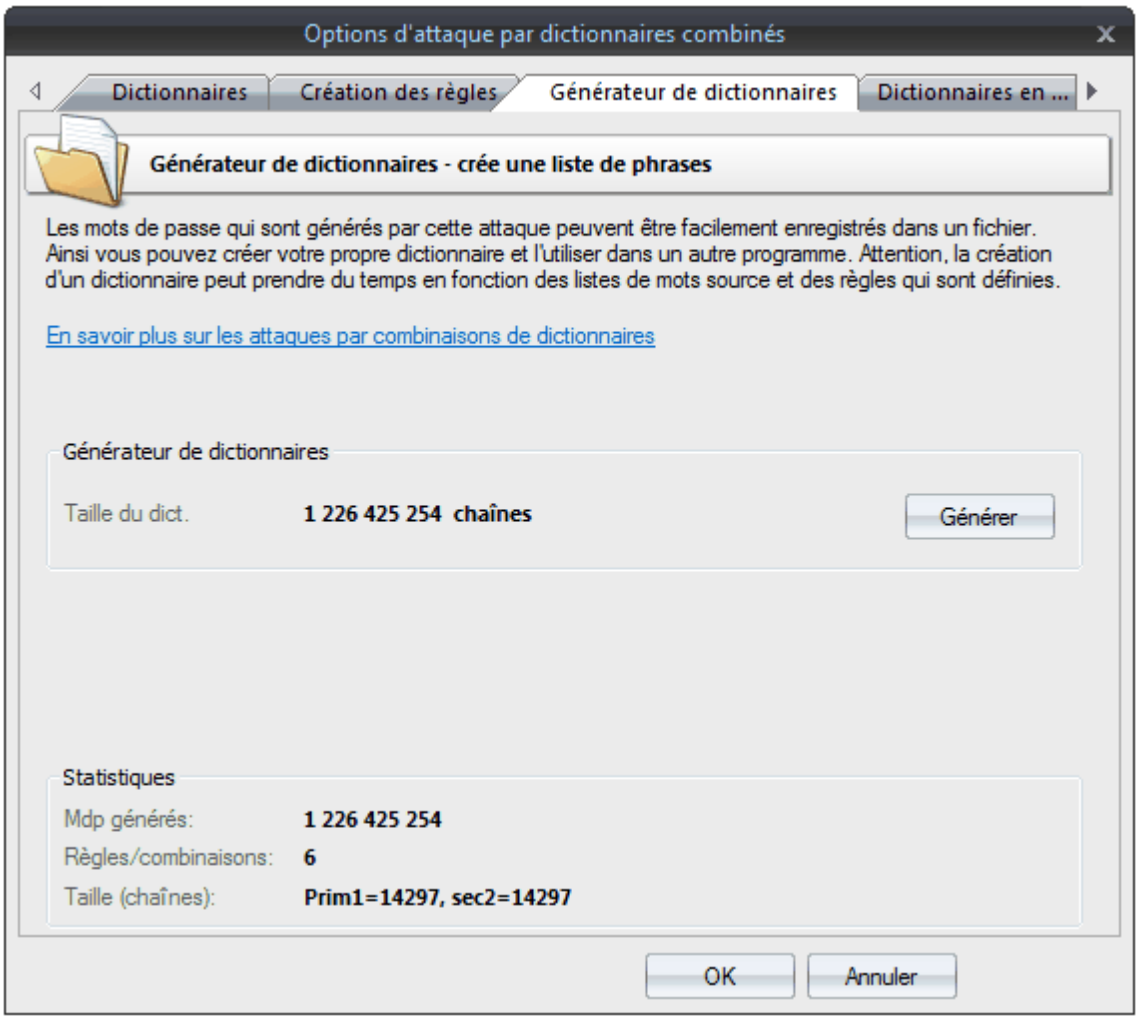
Chaque règles de mutations est constituée de cinq parties:
1. *Préfixe* - partie du texte placé avant chaque phrase. Cet partie peut être un caractère, une chaîne de textes, un chiffre entre 0 et 9 ou un nombre. Par exemple, si vous définissez un chiffre comme préfixe, les phrases créées seront du style: '0 aaa bbb', '1 aaa bbb' : '9 aaa bbb'.
2. *Premier mot* - actions à réaliser sur le premier mot de chaque phrase. Il y a seulement quatre options. le nom: reste identique comme il est dans le dictionnaire, converti tous les caractères en minuscules, converti tous les caractères en majuscules ou mets en majuscule la première lettre du mot.
3. *séparateur de mots*. Il peut être absent. Ensuite tous les mots seront associés. Exemple: 'aaabbb', 'aaaccc','aaaddd', etc. Vous pouvez également définir un séparateur personnalisé; ex: le caractère '-': 'aaa-bbb', 'aaa-ccc','aaa-ddd'. Ou vous pouvez définir une plage de caractères.
4. *Le reste des mots*. Avec cet attribut, similaire au point 2, vous pouvez définir les règles pour les autres mots de la phrase.

5. *Postfixe* - partie du texte qui termine chaque phrase. Par exemple, si vous définissez Postfixe à '?' or ' ?', toutes les phrases créées avec cette règle auront un point d'interrogation à la fin.

Plus vous définissez des règles de génération de mots de passe, plus vous avez de chances d'obtenir le bon mot de passe. Mais, aussi plus vous prendrez du temps sur une attaque.

Le groupe '***Statistiques***' affiche la moyenne et la taille moyenne recommandée pour le dictionnaire, le nombre de mots dans les dictionnaires sources, le nombre total de mots de passe qui ont été générés et d'autres information utiles.

Générateur de dictionnaires



Le troisième onglet des options a pour fonction de créer une attaque combinée à base de dictionnaires (disponible uniquement dans certaines versions du programme).

Vous pouvez aussi télécharger des dictionnaires complémentaires à partir du site Web de Passcape Software.

2.8.2.9 Attaque Pass-phrases (à base de phrases)

De plus en plus d'utilisateurs construisent leurs phrases de mots de passe à partir d'une phrase complète, d'un passage de poèmes, aphorismes de films ou Latin, etc. Essayez de récupérer ce type de mots passe en utilisant les méthodes traditionnelles est impensable, malgré l'avance de la puissance de calcul des ordinateurs modernes. Cependant, la récupération s'aidera de l'attaque prédéfinie et de

phrases connues.

L'attaque Pass-phrase est très similaire à une simple attaque par dictionnaire, excepté que ici, la recherche de mots de passe avance phrase phrase au lieu de mot par mot. L'idée principale de cette attaque est de deviner le bon mot de passe en parcourant les expressions fréquemment utilisées, les phrases et les combinaisons de mots.

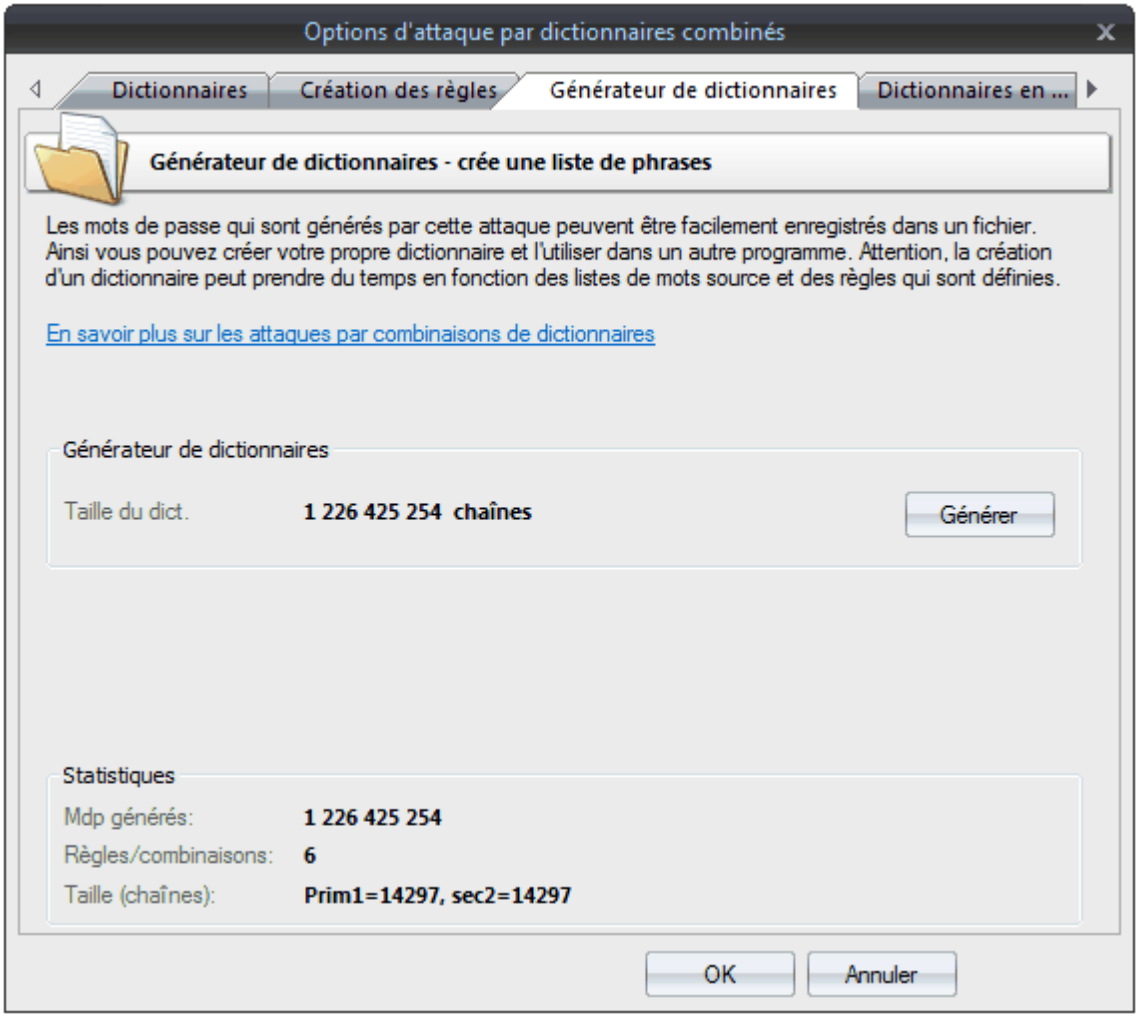
Par exemple, si vous pensez que le mot de passe est en fait des phrases répandues comme 'To be or not to be', il est évident que cette attaque est la seule qui peut faire face à ce type de mot de passe. Pour pouvoir réaliser cela vous devez spécifier un dictionnaire spécial de phrases de mots de passe. Un simple dictionnaire de phrases est fourni avec le logiciel, mais vous pouvez aussi télécharger des dictionnaires en ligne qui sont compilés spécifiquement pour cette attaque.

Ce serait être optimiste de dire que 99% du succès, dans une récupération d'un mot de passe, avec une attaque par dictionnaire dépends de la qualité des dictionnaires. Il est probable que c'est pour cette raison que ce type d'attaque n'est pas présente dans tous les crackers de mots de passe. Passcape Software permets l'utilisation d'un ensemble complet en ligne et hors-ligne de dictionnaires (pour un total de plus de 500 Mo) compilés spécialement pour ce type d'attaque.

Par exemple, beaucoup d'utilisateurs font leurs mots de passe avec des extraits de leurs musiques ou de leurs groupes favoris. C'est pour cette raison que nous avons créé des jeux de phrases clés spéciales, orientés musique (que vous ne trouverez nulle part ailleurs sur le Net !). Il y a aussi des jeux de phrases bibliques de films, de proverbes, etc.

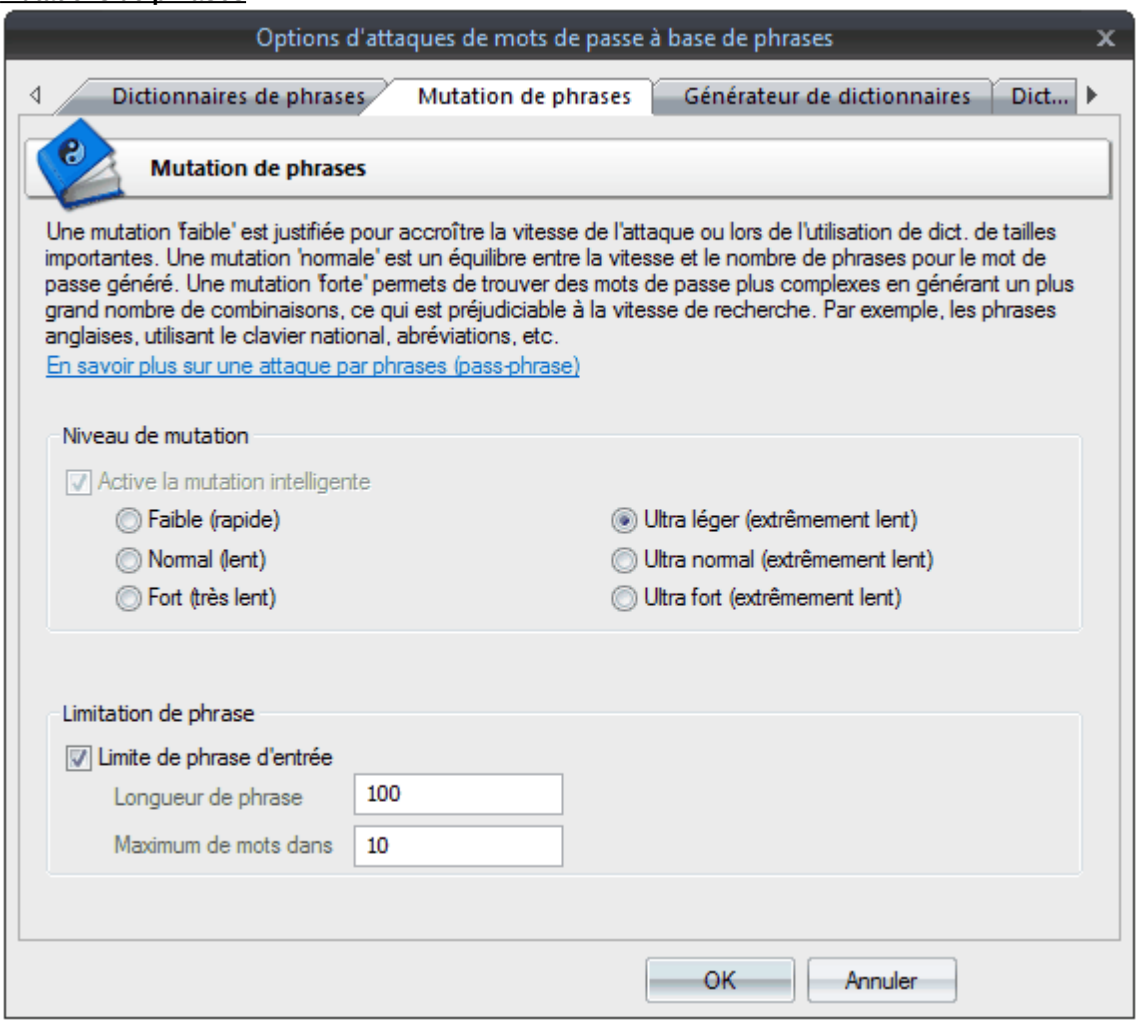
Windows Password Recovery est fourni avec un petit dictionnaire de phrases et d'aphorismes.

Dictionnaires de phrases



Les options d'attaques par phrases de mots de passe reprennent presque complètement les options de l'attaque par simple dictionnaire: ici, vous pouvez aussi sélectionnez un ou plusieurs dictionnaires de phrases sources, il est aussi possible de télécharger des dictionnaires complémentaires à partir du site Web de Passcape, et la création des règles de mutations de phrases suit les même règles (options de créations).

Mutations de phrases



La mutation en elle-même, veut dire plus, puisque depuis que vous connaissez la mutation réglée sur 'forte', qui augmente considérablement les chances de réussite d'une récupération. La mutation 'Faible' est normalement justifiée dans un seul cas: pour augmenter la vitesse d'attaque ou lors de l'utilisation des dictionnaires de grandes tailles. La mutation 'Moyenne' est un équilibre entre la vitesse d'exécution et le nombre de phrases de mots de passe générées. La mutation 'Forte' permet de trouver les mots de passe les plus difficiles en générant le plus large éventail de toutes les combinaisons possibles, au préjudice de la vitesse de recherche. Plus grand sera le niveau de mutations, plus l'attaque couvrira le plus grand nombre de mots de passe. Par exemple, pour les expressions Anglaises saisies à l'aide du clavier national, abréviations, etc.

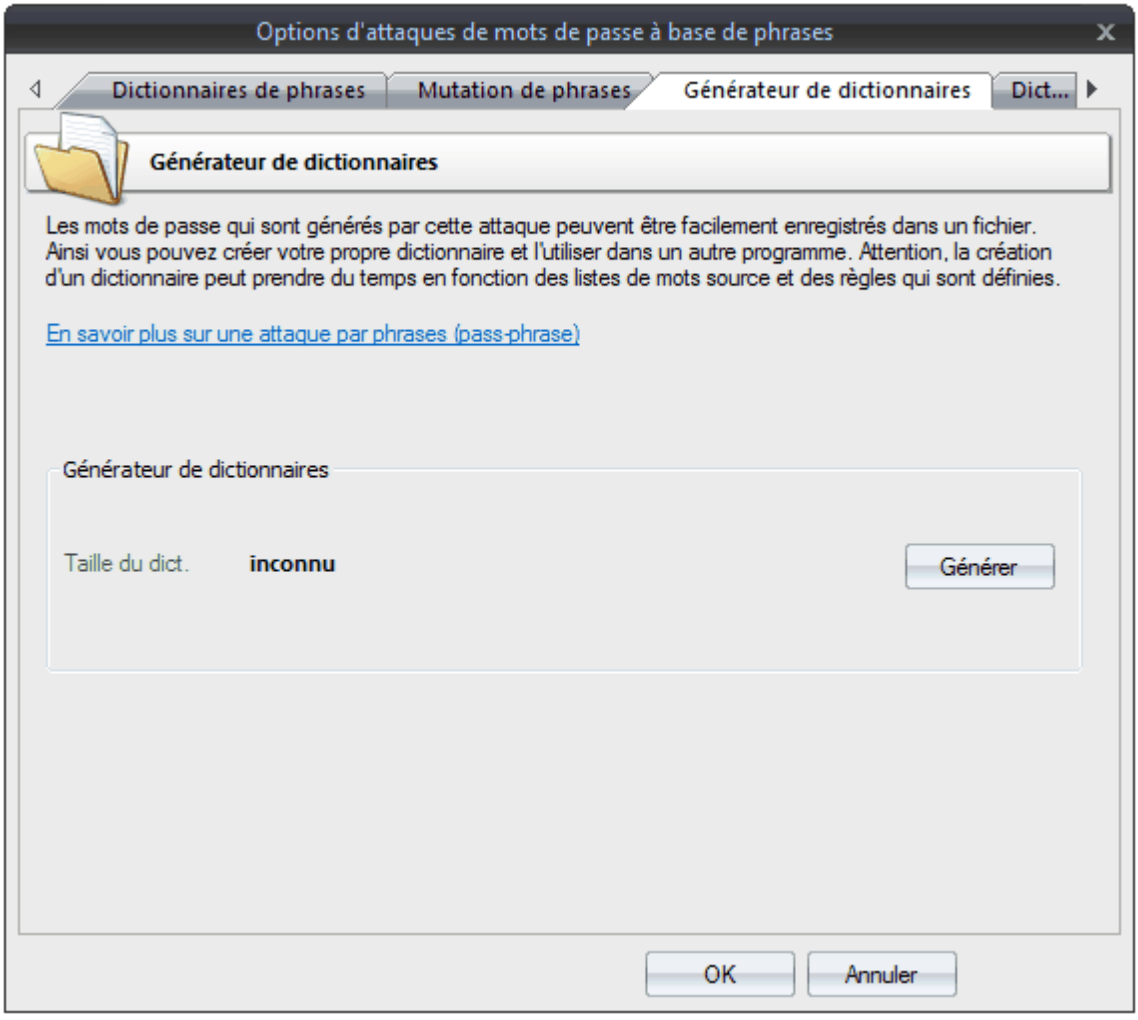
Différences principales des niveaux de mutations:

- Faible - la plus simple donc rapide des mutations.
- Normal - la même que Faible, mais génère des mutations supplémentaires et des combinaisons de casses.
- Fort - La même que Normal, mais avec plus de mutations de mots de passe nationaux (en rapport avec les claviers installés, si ils le sont).
- Ultra léger - c'est la 2ème étape de mutations parce que tous les mots de passe générés en mode Faible passent au second tour de mutations (l'un d'eux est utilisé dans le mode Faible d'une attaque simple par dictionnaire).

- Ultra normal - 2ème étape de mutation. Tous les mots de passe générés dans le mode Normal sont utilisés comme source pour générer des combinaisons supplémentaires en implémentant un niveau Normal complémentaire de mutations.
- Ultra fort - chaque mot de passe généré dans le mode Fort est utilisé comme source pour générer des combinaisons supplémentaires en utilisant un niveau supplémentaire de mutation Forte.

Attention ! Les modes Ultra génèrent un grand nombre de mots de passe, du coup, l'attaque peut s'exécuter extrêmement lentement. Pour augmenter la vitesse d'attaque, pensez à limiter le nombre de phrases sources. Par exemple, vous pouvez limiter le nombre de phrases à 10 mots et 100 caractères.

Générateur de dictionnaires

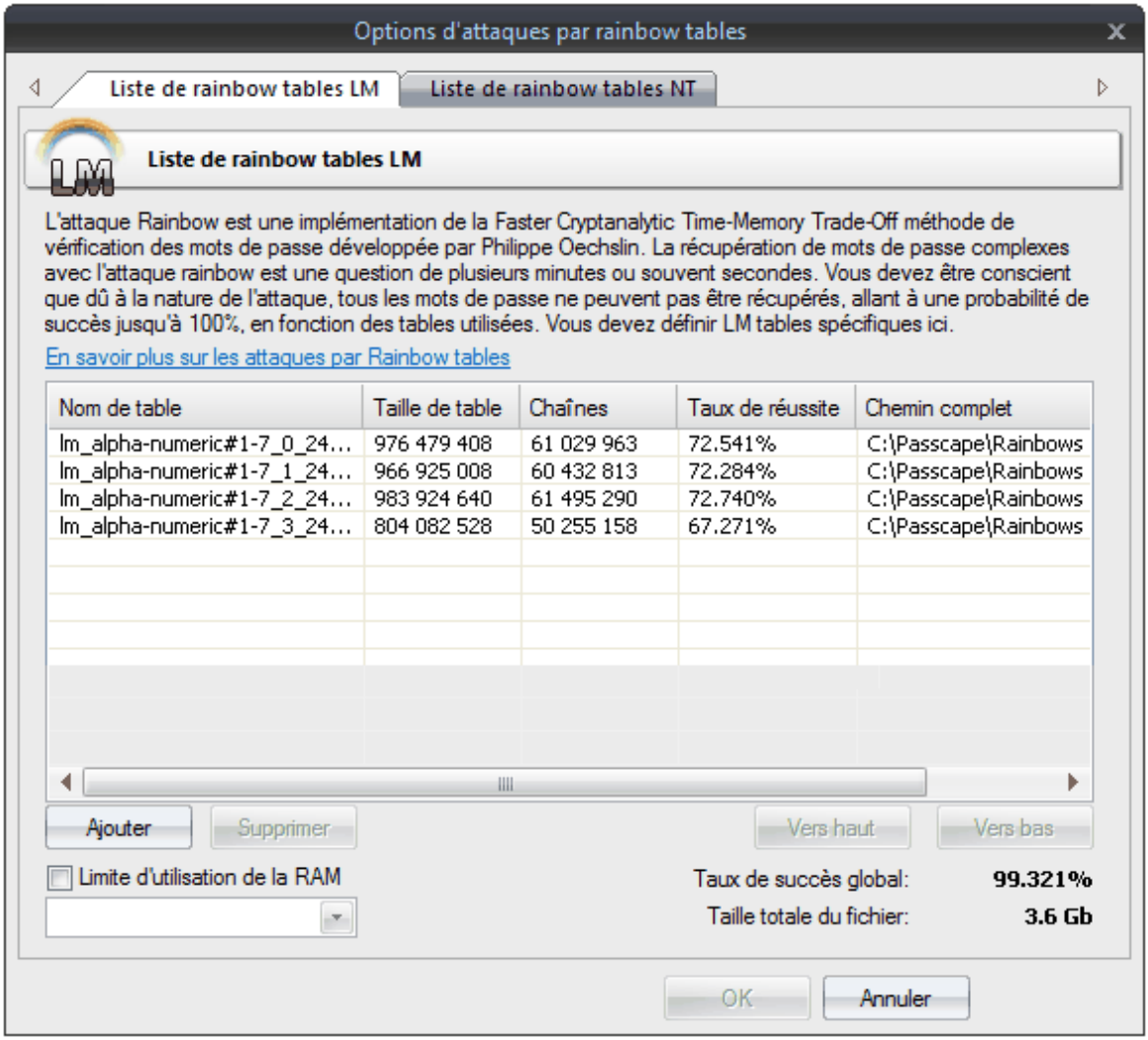


Le troisième onglet '***Générateur de dictionnaires***' est utilisé pour créer les dictionnaires de phrases de mots de passe.

2.8.2.10 Attaque par Rainbow tables

Une rainbow table est une table de recherche offrant un compromis temps-mémoire utilisée dans la récupération d'un mot de passe texte à partir d'un hachage de mot de passe généré par une fonction de hachage, par exemple les mots de passe Windows.

C'est un outil d'audit de mots de passe assez sophistiqué. Cette méthode a été développé par Philippe Oechslin pour la récupération rapide de mots de passe utilisant des tables pré-calculées. Il suffit de dire que le mot de passe recherchée peut être récupéré en quelques minutes, voire en quelques secondes.



Le programme supporte le standard *.rt, indexé *.rti et les tables hybrides. Le multi-tâche est également supporté.

Il faut mentionner que l'attaque rainbow ne garantie pas la récupération de tous les mots de passe, mais la probabilité de récupération est proche de 100%, dépendant des tables que vous possédez.

Une rainbow table spécifique peut être mise en œuvre, ayant été créée pour un hachage. Ex: Les tables LM spécifiques doivent être utilisées pour casser les hachages LM uniquement.

Les options d'attaques permettent un nombre limité de RAM qui peut être utilisé par une attaque lorsque avec des anciens ordinateurs (l'attaque prends de grandes quantités de RAM pour les calculs).

2.8.2.11 Attaque par hybride par Dictionnaires

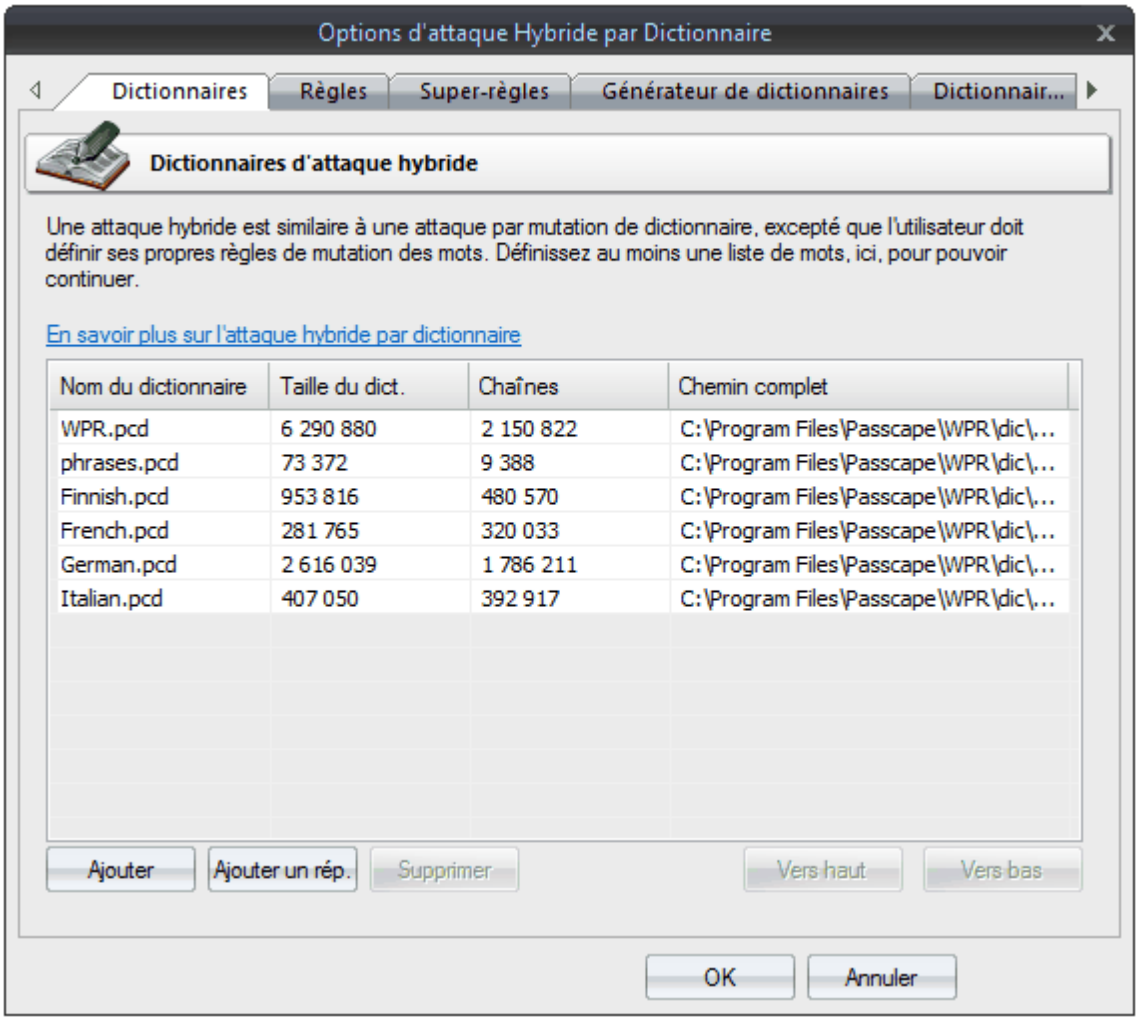
L'attaque par hybride par dictionnaires est une forme d'attaque par simple dictionnaire. Cependant, à la différence de cette dernière, l'attaque hybride permets de définir ses propres règles de mutations de mots (variations) et d'essayer de valider les mots comme mots de passe sources. Par exemple, l'utilisateur peut mettre en majuscule la première lettre d'un mot de passe à tester, lui ajouter '2', remplacer le nombre 8 par la lettre B, O avec un 0 (zéro), etc.

Les actions, réalisées sur les mots sources d'un dictionnaire, sont appelées des règles. Des règles multiples peuvent être appliquées à chaque mot source. La syntaxe de définition des règles est compatible avec les logiciels John the Ripper et PasswordsPro. L'auteur de ce dernier a aimablement fourni un ensemble étendu de règles, légèrement modifiées, qui sont fournies avec le kit distribué pour

Windows Password Recovery.

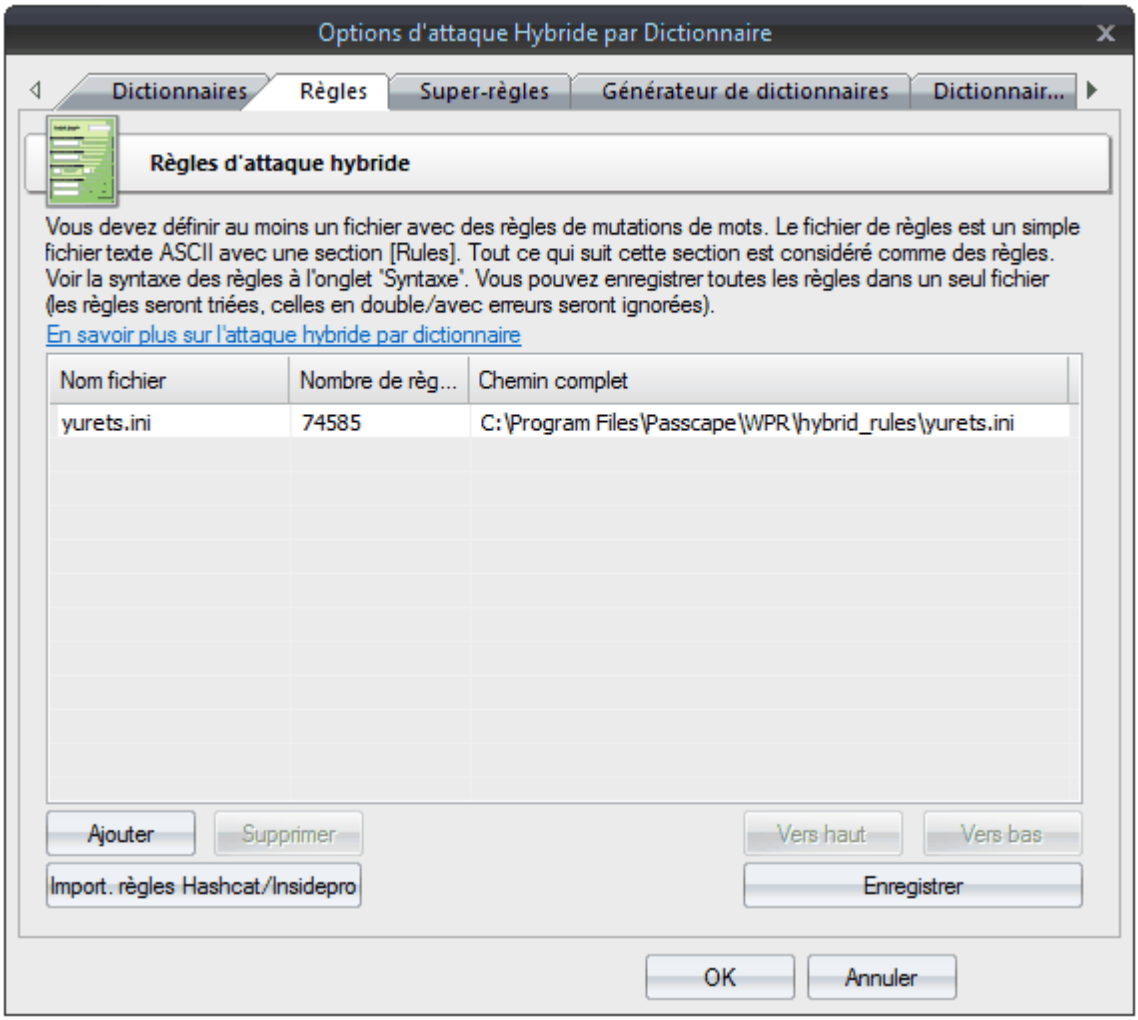
Les paramètres d'attaques hybride par dictionnaires sont réparties en 7 onglets:
1. **Dictionnaires** - pour le paramétrage des dictionnaires sources.
2. **Règles** - fichiers contenant un ensemble de règles.
3. **Super-règles** - règles appliquées avant toutes les règles standards.
4. **Générateur de dictionnaires**, où vous pouvez créer des fichiers de mots obtenus à partir d'un attaque hybride.
5. **Dictionnaires en ligne** - pour télécharger de nouveaux dictionnaires pour le logiciel.
6. **Syntaxe hybride** - description complète de toutes les règles avec des exemples.
7. **Testeur de règles**, emplacement pour tester vos règles.

Les listes de mots qui sont utilisées dans une attaque sont définies dans ce premier onglet. Traditionnellement, le logiciel supporte les listes de mots au format ASCII, UTF8, UNICODE, PCD, RAR et ZIP. La position des fichiers dans la liste peut être modifiée. Par exemple, vous pouvez déplacer les petits dictionnaires au début de la liste ou autrement. Pendant l'attaque, ils seront utilisés les uns après les autres, en fonction de leur position dans la liste.

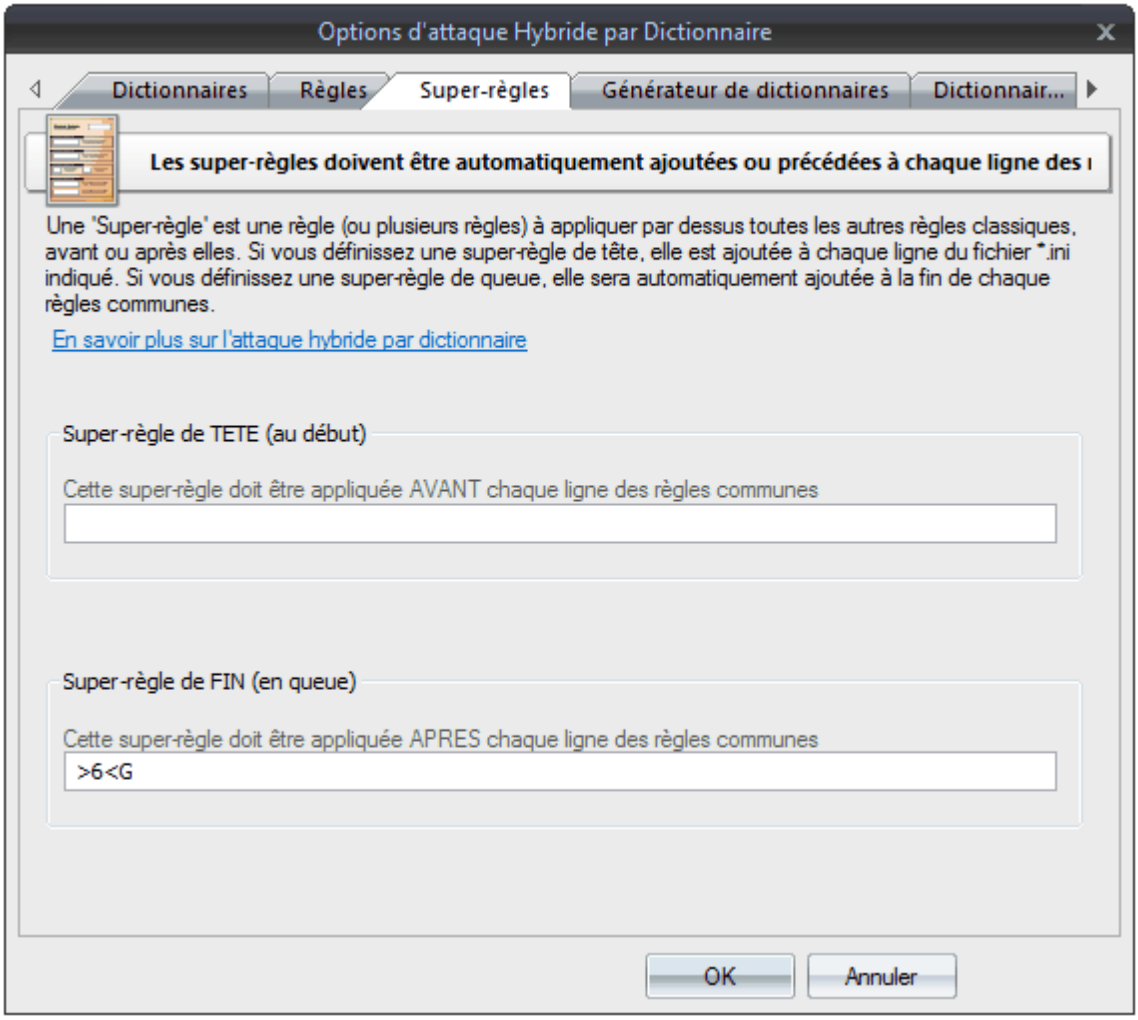


Dans l'onglet '**Règles**', vous devez définir au moins un fichier avec des règles de mutations de mots de passe. Le format du fichier de règles est quelque peu ordinaire; c'est un fichier texte ASCII contenant la chaîne '**[Rules]**'. Tout ce qui sera présent avant cette chaîne entre crochets sera considéré comme des commentaires et ignoré par le programme. Et tous ce qui sera après, donc, sera considéré comme des règles. Chaque chaînes peut contenir plusieurs règles, applicable au mot source.
La règle d'exclusion est **aN**. Cette règle ne doit pas être sur la même ligne que les autres règles. Si une chaîne contient plusieurs règles par mot, ces règles seront parcourues de gauche à droite. Par exemple, si vous appliquez la règle '@pc$a$b$c' au mot source 'password', après l'application de la règle vous

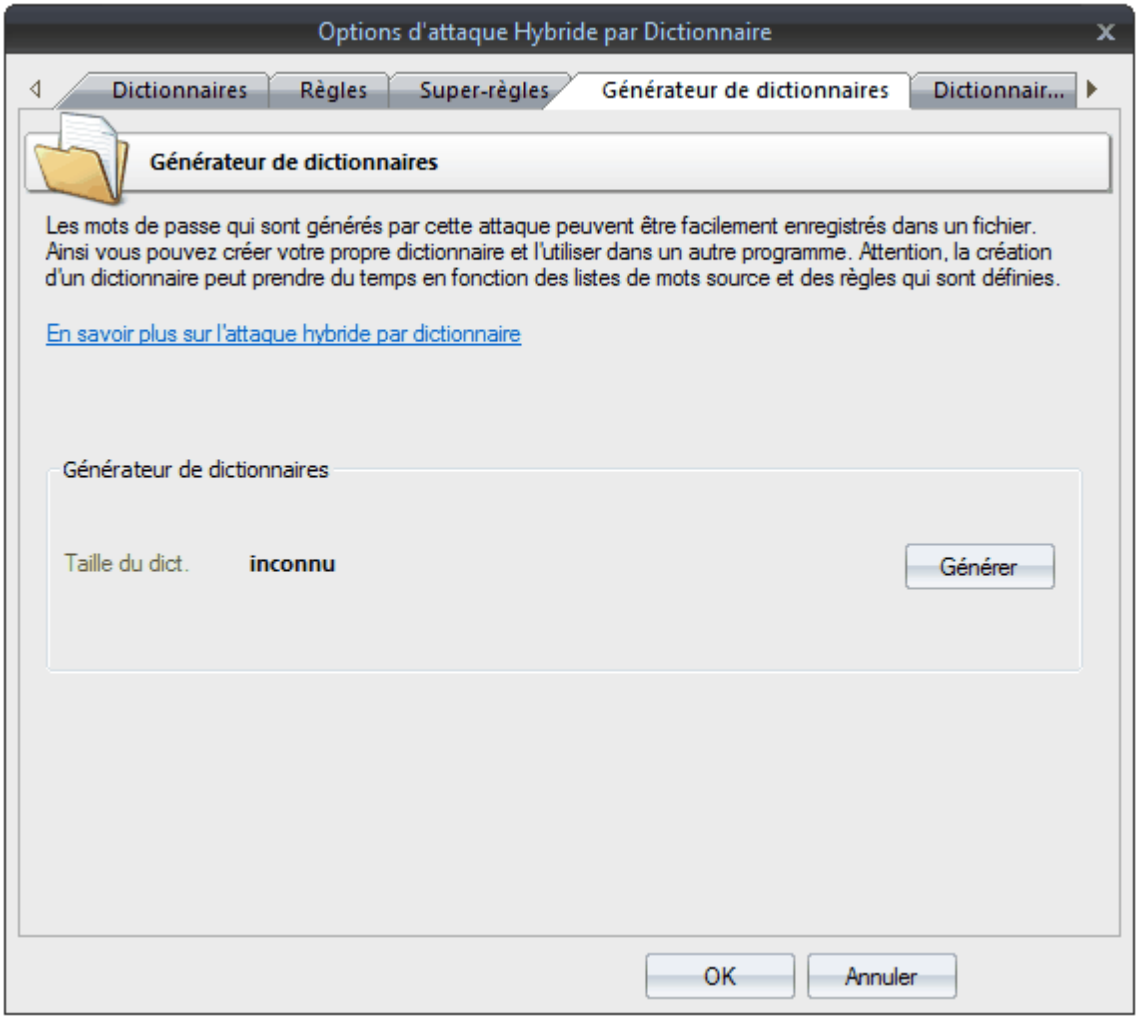
obtiendrez 'Asswordabc'. La longueur maximum du mot en sortie ne peut excéder **256** caractères.



'**Super-règles**' est une règle (ou plusieurs) qui peuvent être appliqués avant ou après les dessus les règles classiques. Par exemple, vous pouvez définir une liste de super-règles 'a8' pour créer toutes les combinaisons possibles après que la mutation standard a été réalisée. Du coup, la règle '/asa4' du fichier l33t.ini deviendra '/asa4a8', '/csc(' deviendra '/csc(a8', etc. Comme cet autre exemple: définissez la règle en tête '>6<G' qui permets de sauter tous les mots de moins de 6 caractères ou plus de 16 caractères, avant de démarrer la mutation commune. Cette fonctionnalité est très utile une fois que l'on a décidé d'ajouter la même règle à toutes les lignes textes des fichiers *.ini sélectionnés. Il est du coup pas nécessaire de tous les modifier. Attention dans ce type d'utilisation, la super-règle 'aN' peut augmenter de manière importante le total de de mots de passe générés.

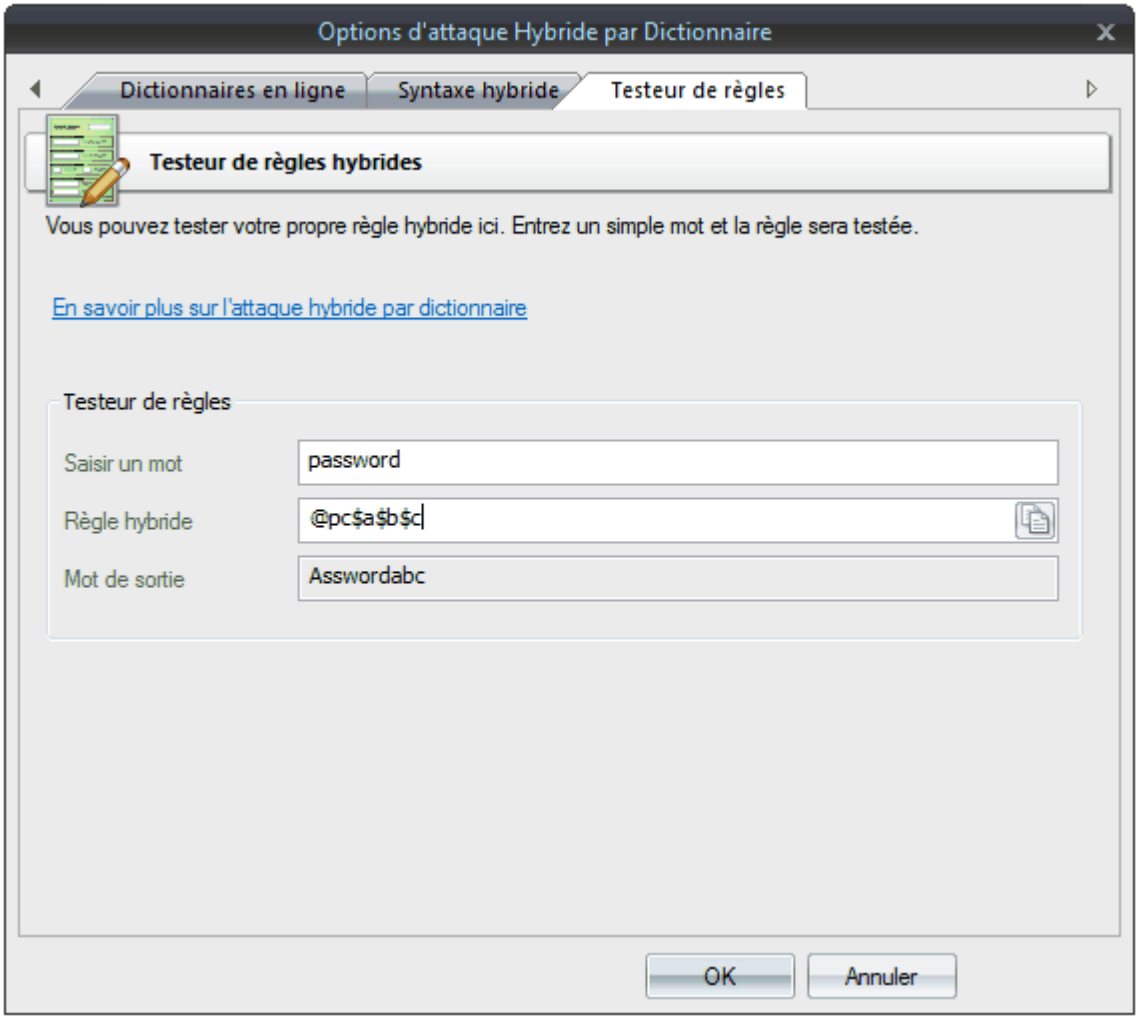


L'onglet '**Générateur de dictionnaires**' est conçu pour générer des dictionnaires obtenus à partir de l'attaque. Ces dictionnaires pourront être utilisés par exemple, dans d'autres applications. Pour générer un dictionnaire, sélectionnez un dictionnaire source et définissez les règles de mutations à lui appliquer. La taille du fichier créée pour le dictionnaire ne peut excéder 2 Go.
Attention, la génération d'un dictionnaire peut prendre beaucoup de temps !



Vous pouvez télécharger des listes de mots complémentaires pour l'attaque en utilisant l'onglet '[Dictionnaires en ligne]'.

Si vous voulez créer vos propres jeux de règles, vous pouvez utiliser les deux derniers onglets comme sources d'aides. Alors que l'onglet '**Syntaxe hybride**' donne plus de détails sur les règles disponibles, dans le dernier onglet vous pouvez les tester en indiquant un source mot spécifique et une règle pour l'attaque hybride. En retour, vous pouvez nous envoyer vos jeux de règles; si nous les trouvons intéressantes/utiles, elles seront incluses par défaut dans le programme WPR.



Description des règles pour l'attaque hybride par dictionnaires

Plusieurs règles peuvent être définies par ligne.
Les règles (si elles sont multiples par ligne) sont exécutées de la gauche vers la droite.
La longueur maximum par ligne est limitée à **256** caractères.
La longueur maximum du mot de sortie est de **256** caractères.
Les espaces sont ignorés tant qu'ils ne sont pas utilisés comme paramètres.
Une ligne démarrant avec le caractère # est considérée comment un commentaire.
Tous les textes avant la ligne '**[Rules]**' sont considérés comme des commentaires.
N et M démarre toujours de 0 (zéro). Pour les valeurs supérieures à 9, utilisez les lettres A..Z (A=10, B=11, etc.).
Ne modifiez pas les noms des fichiers des règles standard (fournies avec le programme). Certains sont utilisés par le programme.
?iN[C], ?i[C], ?oN[C], ?o[C] ?iZ[C], ?oZ[C] Ces règles utilisent les jeux de caractères prédéfinis suivants (vous pouvez définir vos propres jeux de caractères personnalisés):

digits - 0123456789
loweralpha - abcdefghijklmnopqrstuvwxyz
upperalpha - ABCDEFGHIJKLMNOPQRSTUVWXYZ
alpha - abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ
special - !@#$%^&*()-_+=~`[]{}|\:;'"<>,.?/ "
loweralphanumeric - abcdefghijklmnopqrstuvwxyz0123456789
upperalphanumeric - ABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789
alphanumeric - abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789
printable - abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789!@#$%^&*()-_+=~`[]{}|\:;'"<>,.? /

Règles

Règle	Exemple	Source	Sortie	Description
:	:	password	password	Ne modifie pas le mot source
{	{	password	asswordp	Retourner le mot vers la gauche
}	}	password	dpasswor	Retourner le mot vers la droite
[	[	password	assword	Supprimer le premier caractère
]	]	password	passwor	Supprimer le dernier caractère
c	c	password	Password	Mettre le la première lettre en majuscule
C	C	password	pASSWORD	Mettre en majuscule toute les lettres du mot sauf la première (minuscule pour le premier caractère, majuscule pour le reste du mot)
d	d	password	passwordpassword	Dupliquer le mot et l'ajouter à la fin du mot
f	f	password	passworddrowssap	Ajouter à la fin du mot le mot inversé (mot en reflet)
k	k	password пароль	зфыыцщквgfhjkm	Convertir le mot en utilisant un arrangement de clavier alternatif (le premier après celui par défaut). La règle fonctionne dans les deux directions. Par exemple, si un clavier Russe a été installé précédemment dans le système, la règle doit convertir le mot 'password' en Russe 'зфыыцщкв', et le mot Russe 'пароль' en 'gfhjkm'. Cette règle est très utile, lorsque vous recherchez des mots de passe non-Anglais. Si un seul langage est installé dans le système, la règle ne fera rien.
K	K	password	passwodr	Intervertir les deux derniers caractères
l	l	password	password	Convertir tous les caractères en minuscules
q	q	password	ppaasssswwoorrdd	Dupliquer tous les symboles
r	r	password	drowssap	Inverser le mot
t	t	PassWord	pASSwORD	Inverser la casse de tous les caractères
u	u	password	PASSWORD	Convertir tous les caractères en majuscules
U	U	my own password	My Own Password	Mets en majuscule toutes les premières lettres de chaque mots séparés par un espace (mets en majuscule tous les premier caractères après un espace)
V	V	password	PaSSWoRD	Mets en minuscule les voyelles et en majuscule les consonnes
v	v	password	pASSWoRD	Mets en majuscule les voyelles et en minuscule les consonnes
'N	'4	password	pass	Raccourci la longueur du mot de N caractère (s)
+N	+1	password	pbssword	Incrémente le caractère à la position N de 1 valeur ASCII
-N	-0	password	oassword	Décrémente le caractère à la position N de 1 valeur ASCII
.N	.4	password	passoord	Remplace le caractère à la position N avec le caractère de la position N +1
,N	,1	password	ppssword	Remplace le caractère à la position N avec le caractère à la position N-1. Où N > 0
<N				Ignore (saute) le mot si il est plus grand de N caractères de long
>N				Ignore (saute) le mot si il est moins grand que N caractères de long

Règle	Exemple	Source	Sortie	Description
aN				Test toutes les casses de symboles pour le mot. N est la longueur maximum du mot sur laquelle il faut appliquer la règle
DN	D2D2	password	paword	Supprimer le caractère à la position N
pN	p3	key	keykeykey	Copie le mot N fois
TN	T1T5	password	pAsswOrd	Inverse la casse avec le caractère à la position N
yN	y3	password	paspassword	Duplique le(s) N premier caractère(s)
YN	Y3	password	paswordord	Duplique le(s) N dernier caractère(s)
zN	z3	password	ppppassword	Duplique le premier caractère du mot N fois
ZN	Z3	password	passworddd	Duplique le dernier caractère du mot N fois
$X	$0$0$7	password	password007	Ajoute X caractère(s) à la fin du mot
^X	^3^2^1	password	123password	Insère X caractère(s) au début du mot
@X	@s	password	paword	Supprime tous les caractères X du mot
!X				Ignorer (saute) si il contient au moins un caractère X
/X				Ignorer (saute) si il ne contient pas de caractères X
(X				Ignorer (saute) si il le premier caractère n'est pas X
)X				Ignorer (saute) le mot si le premier caractère n'est pas un X
eX	e@	mike@yahoo.com	mike	Extrait une sous-chaîne à la position 0 et se terminant avant le premier caractère X (ne fait rien si X n'est pas trouvé)
EX	E@e.	mike@yahoo.com	yahoo	Extrait une sous-chaîne démarrant à droite après le premier caractère X trouvé et jusqu'à la fin de la chaîne (ne fait rien si X n'est pas trouvé)
%MX				Ignorer (saute) le mot si il ne contient pas au moins M fois le caractère X
***XY**	*15	password	possward	Interverti les caractères à la position X et Y
=NX				Rejette (saute) le mot si le caractère à la position N n'est pas identique à X
iNX	i4ai5bi6c	password	passabcword	Insère le caractère X à la position N
oNX	o4*o5*	password	pass**rd	Écrase le caractère à la position N avec le caractère X
sXY	ss$so0	password	pa$$w0rd	Remplace tous les caractères X avec Y
xNM	x4Z	password	word	Extrait la sous-chaîne jusqu'à une longueur de M caractères, en démarrant d la position N
INX-Y	rl0/-/r	google.com	google.com/	Insère le caractère X à la position N si le caractère précédent à la position N n'est pas Y
INX+Y	rl0.+.r	password.	password..	Insère le caractère X à la position N si le précédent caractère à la position N est Y
ONX-Y	O0-+p	password	-assword	Si le caractère à la position N n'est pas Y, il sera écrasé par le caractère X
ONX+Y	O0P+p	password	Password	Si le caractère à la position N est Y, il sera écrasé par le caractère X
RNM+Y	R01+a	password	assword	Supprime le caractère à la position N si le caractère à la position M est Y
RNM	R40-b	password	passord	Supprime le caractère à la position N si le caractère à la position M n'est

Règle	Exemple	Source	Sortie	Description
-Y		rd		pas Y
?iN [C]	?i0 [digits]	password	0password, 1password ... 9password	Insère un caractère à partir du jeu de caractère [C] à la position N du mot. [C] étant soit un nom de jeu de caractères prédéfini ou un jeu de caractères personnalisés.
?iZ [C]	?iZ [digits]	password	password0, password1 ... password9	Insère un caractère à partir du jeu de caractères [C] à la dernière position du mot. [C] étant soit un nom de jeu de caractères prédéfini ou un jeu de caractères personnalisés.
?i[C]	?i [special]	password	~password, !password ... password_, password+	Insère un caractère à partir du jeu de caractères [C] à toutes les positions du mot. [C] étant soit un nom de jeu de caractères prédéfini ou un jeu de caractères personnalisés.
?oN [C]	?o1 [upperalpha]	password	pAssword, pBssword ... pZssword	Remplace un caractère à la position N par un caractère provenant du jeu de caractères [C]. [C] étant soit un nom de jeu de caractères prédéfini ou un jeu de caractères personnalisés.
?oZ [C]	?oZ [upperalpha]	password	passworA, passworB ... passworZ	Remplace le caractère à la dernière position du mot par un caractère provenant du jeu de caractères [C]. [C] étant soit un nom de jeu de caractères prédéfini ou un jeu de caractères personnalisés.
?o [C]	?o[-=.]	password	-assword, =assword ... passwor.	Remplace le caractère à toutes les positions du mot par un caractère provenant d'un jeu de caractères [C].

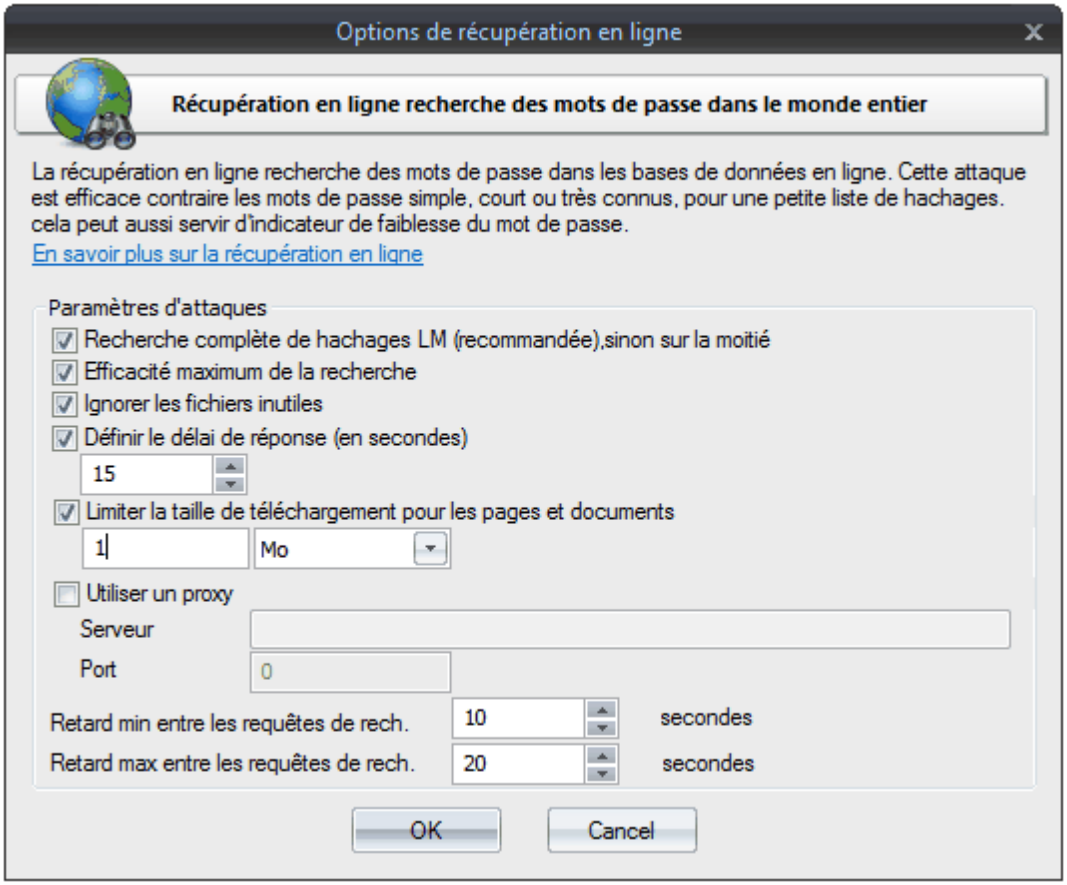
En complément
Le kit de distribution de Windows Password Recovery contient des ensembles étendues de règles de mutations de mots de passe:
hybrid_rules/english_words.ini - fichier contenant les règles basiques pour des mots de passe Anglais.
hybrid_rules/nonenglish_words.ini - contient les règles communes pour les mots de passe non-Anglais.
hybrid_rules/simple_dates.ini - grand nombre de règles avec des dates, mois, et saisons, etc.
hybrid_rules/l33t.ini - règles de mots bizarres (basées sur le dictionnaire Leet). Par exemple, password->p@$$w0rd
...

Vous recherchez une meilleure façon de manipuler les mots de passe ? Téléchargez l'ensemble complet de plus de 180000 règles triées et libre d'être copiées.

2.8.2.12 Récupération en Ligne

La récupération en ligne (développée par Passcape Software) trouve les mots de passe en utilisant les serveurs de moteurs de recherche sur Internet. Elle fonctionne assez bien avec les mots de passe courts et fréquemment utilisés. Mais cette méthode de récupération possède des inconvénients comme sa faible vitesse et sa mauvaise aptitude pour le traitement de larges listes de hachages.

La récupération en ligne a été développé par Passcape Software et est une amélioration dans la recherche de mots de passe en ligne. Pour trouver des mots de passe, le programme soumettra consécutivement une demande de recherche pour chaque hachage au moteur de recherche, puis téléchargera les fichiers de mots de passe trouvés et analysera leurs contenus. La recherche en ligne est relativement lente; cependant, elle est appropriée pour les petites listes de hachages. Il faut savoir que les mots de passe trouvés sont, habituellement, limités à un vocabulaire simple et de courtes combinaisons. D'une façon ou d'une autre, l'attaque peut être assez utile, par exemple, lors d'audits des mots de passe, comme la détection de simples vulnérabilités pour certains systèmes.



Options de récupération en ligne

- **Recherche complète de hachages LM** - utilise la totalité des 16 octets du hachage lors de la recherche de hachages LM. Si cette option n'est pas activée, la recherche sera effectuée sur la moitié (8 octets). Pour s'assurer d'une recherche plus efficace et éviter les trafics parasites, il est recommandé d'activer cette option. Lors de la recherche de hachages NT, cette option peut être ignorée.
- **Efficacité maximum de la recherche** - augmente l'efficacité de la recherche sans affecter la vitesse d'attaque. Il est recommandé, également, de toujours activer cette option.
- **Ignorer les fichiers inutiles** - ne vérifie pas les fichiers qui sont suspectés ne pas contenir de mots de passe.
- **Définir le délai de réponse** - défini le temps de réponse maximum de ressources Web.
- **Limiter la taille de téléchargement pour les pages et les documents** - limite la taille des documents téléchargés. Certaines base de données de hachages ont une taille importante, même en dépit de cela, ils peuvent ne pas contenir de mots de passe. Cependant, pour les connections Internet lentes et pour réduire la perte de débit, il est recommandé de définir la limite de taille des pages téléchargées. Malheureusement, il n'est pas possible de savoir ce que contiennent les données à télécharger; du coup, l'utilisation de cette fonction dépends de vos préférences et vos aptitudes dans le choix.
- **Utiliser un proxy** - utilise un serveur proxy pour la recherche de mots de passe.
- **Retard min/max entre les requêtes de rech.** - retards minimum et maximum entre deux requêtes consécutives au serveur de recherche. Certains serveurs de recherche peuvent rejeter des requêtes si la série, à partir de la même adresse IP est faite dans un intervalle de temps très rapproché (moins de 10 secondes). En dépit de cela, Windows Password Recovery a un générateur interne de requêtes, qui permets de faire chuter ce retard de manière significative (à peu près de 1 à 2 secondes respectivement), les valeurs qui assure qu'une requête soit exécutée par le serveur sont min=15 et max=30 secondes. Évidemment, la vitesse d'attaque dépends de la relation entre ces deux options.

Attention ! La récupération en ligne peut générer beaucoup de trafics Internet !

2.8.2.13 Attaque par Rainbow Tables Passcape

Les Rainbow Tables Passcape sont le prochain développement logique de simples tables pré-calculées. Elles sont les plus appropriés pour la récupération d'un grand nombre de combinaisons et de mots de passe complexes d'une longueur illimitée.

La méthode originale des rainbow tables simples
Le principe de fonctionnement d'une rainbow table simple consiste en une plage de caractères (par exemple, a..z) et d'une longueur maximum du mot de passe, suivi par le calcul de toutes les variantes et la génération de millions de chaînes. Chaque chaînes étant calculée par la formule suivante:

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

où **P** – est le mot de passe, **hash** – la fonction de hachage, **R** – la fonction de réduction. Ainsi, à partir du mot de passe d'origine, la fonction de hachage produit un hachage, puis convertie le mot de passe suivant, et le processus se répète jusqu'à la fin et termine en générant les chaînes. Chaque chaîne stocke uniquement la valeur initiale et finale. Stocker seulement le premier et le dernier hachage est une opération nécessitant des compromis et à sauver de la mémoire au détriment du temps consacré à la cryptanalyse.

Pour récupérer un mot de passe que l'on recherche, il est soumit au hachage et la fonction de réduction et ensuite à une recherche dans la table. Pour cette raison, une clé de chaîne est générée en commençant avec **R(Hn)** jusqu'à la longueur maximum de chaîne. Si **Hn** est obtenu avec le mot de passe utilisé lors de la création de la table, nous obtenons finalement la clé qui correspond à la clé de la chaîne respective. Cette dernière clé est enregistrée dans la table avec la première clé de chaîne. En utilisant la première clé de chaîne, nous pouvons récupérer la chaîne dans son intégralité, en particulier, la valeur juste avant **R (Hn)**. Qui est en fait la clé qui a été utilisé pour générer **Hn**, notre mot de passe recherché.

Principe de fonctionnement des rainbow tables Passcape
La récupération en utilisant les rainbow tables Passcape est à peu près la même que en utilisant de simples rainbow tables. Cependant, à la différence de cette dernière, c'est une sorte d'attaque hybride par Empreinte et de simples tables, où à la place de définir une plage de caractères spécifiques, les mots de passe sont validés dans une plage appelée 'empreinte de mots'. L'idée de l'attaque par Empreinte développée par Passcape revient à prendre le dictionnaire source et créer une banque d'empreintes de mots (empreintes numériques), nécessaires pour valider le mot de passe, en dehors de ce dictionnaire; puis lors de l'attaque, de rechercher toutes les variantes possibles de mots qui se composent de deux de ces empreintes.

Similaire à l'attaque par Empreintes, l'attaque par rainbow tables Passcape crée une banque d'empreintes de mots à partir d'une liste de mots de l'utilisateur. La banque d'empreinte de mots est analogue au jeu de caractères dans de simples rainbow tables. C'est utilisé pour la création de tables Passcape et la validation des mots de passe. Ainsi, une rainbow table Passcape est constitué d'un ou plusieurs fichiers ***.prt** (les tables actuelles) et une banque d'empreintes de mots (***.prti**), lesquels peuvent être utilisés avec les tables qui ont été créé avec elle.

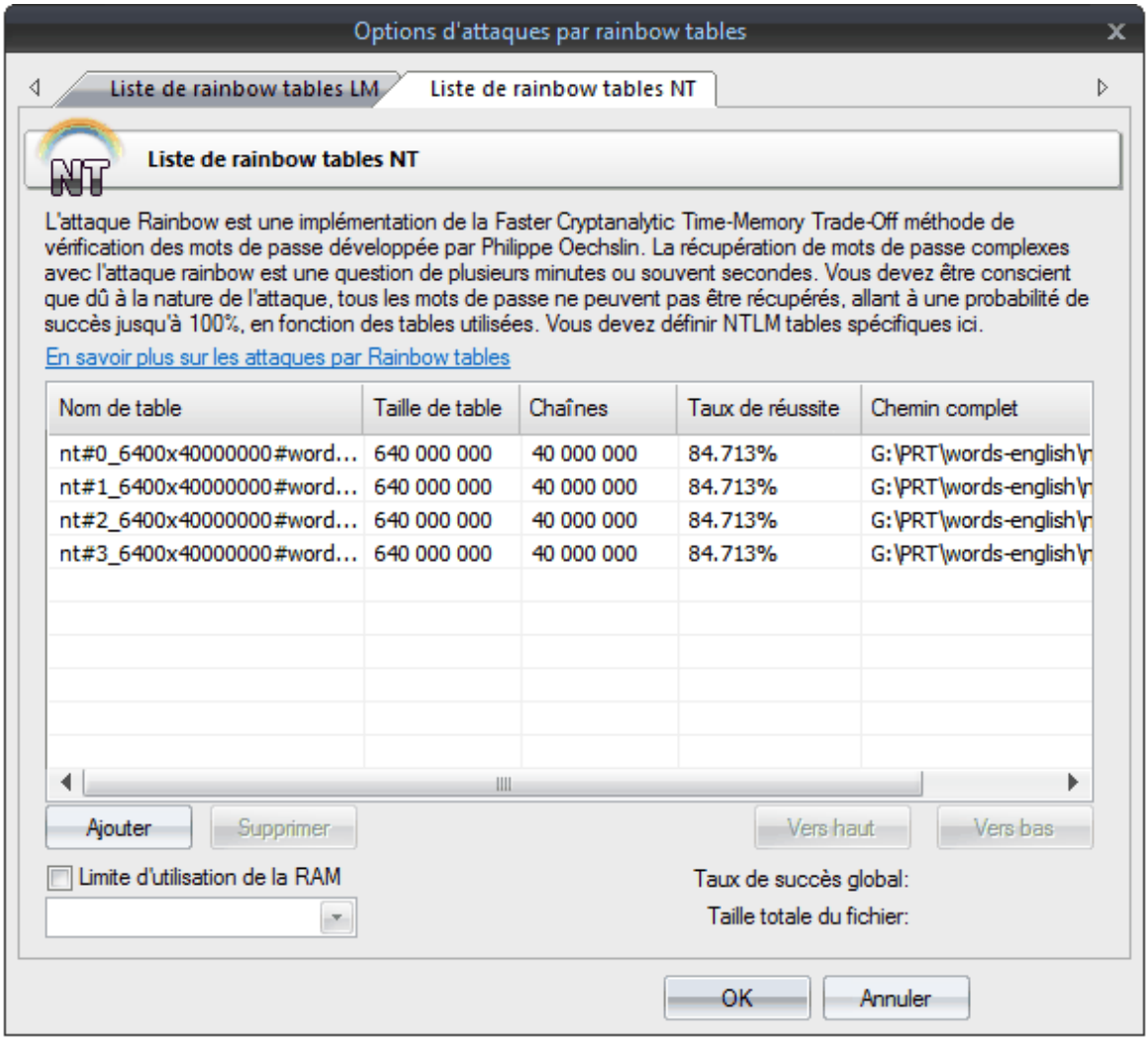
Il y a un grand nombre d'avantages à utiliser des empreintes de mots à la place de jeux de caractères lors de la création de tables:
- La longueur des mots de passe testés avec des tables Passcape est illimitée. A la différence de simples rainbow tables, lesquelles ne peuvent pas être créées pour des mots de passe de plus de 9 caractères. Avec des tables Passcape, on peut récupérer à la fois un mot de passe de 1 caractère ou de 50 caractères avec la même probabilité.
- Un jeu de caractères dans une table ordinaire affecte beaucoup ses paramètres critiques de la table: plus la plage de caractères est grande, plus la longueur de la chaîne est grande, ou le nombre total de chaînes pour stocker le taux de réussite (pourcentage de succès pour trouver un mot de passe). Par contre, dans une table Passcape, un jeu de caractères n'affecte pas les paramètres critiques de la table.
- Les tables simples ont certaines difficultés lors de la génération des tables de validation des mots de passe dans les jeux de caractères nationaux; tous les programmes ne gèrent pas correctement ce type de tableaux, et tous ne peuvent pas les créer. Avec les rainbow tables Passcape, lors de la génération

des tables, par exemple avec des mots de passe russes, on peut simplement spécifier le dictionnaire source Russe.
- Avec les tables Passcape, les mots de passe sont recherchés à l'aide de combinaisons plus significatives; Cependant, cela dépend en grande partie du dictionnaire source.

Les points suivants peuvent être considérés comme des inconvénients des rainbow tables Passcape:
- Tous les dictionnaires source ne sont pas égaux pour les tables. L'utilisation de grands dictionnaires (supérieur à 1 Mo) génère de trop grandes banques d'empreintes; du coup la création des tables peut nécessiter un temps et des ressources considérables.
- Utiliser des dictionnaires avec de longs mots ou phrases est décourageant pour les raisons expliquées précédemment.
- L'attaque Rainbow table utilise un grand nombre de ressources: la banque d'empreintes doit correspondant à la RAM de l'ordinateur.

Paramètres d'attaque par rainbow table Passcape

Les paramètres d'attaque de rainbow table Passcape sont assez simples. Vous devez définir une ou plusieurs tables *.prt, qui doivent se trouver dans le même répertoire que la banque d'empreintes (fichier ***.prti**). Sachant que cette attaque consomme plus de RAM que l'attaque utilisant les simples rainbow tables, il est recommandé de limiter la quantité de RAM qui doit être utilisée en réglant l'option correspondante.



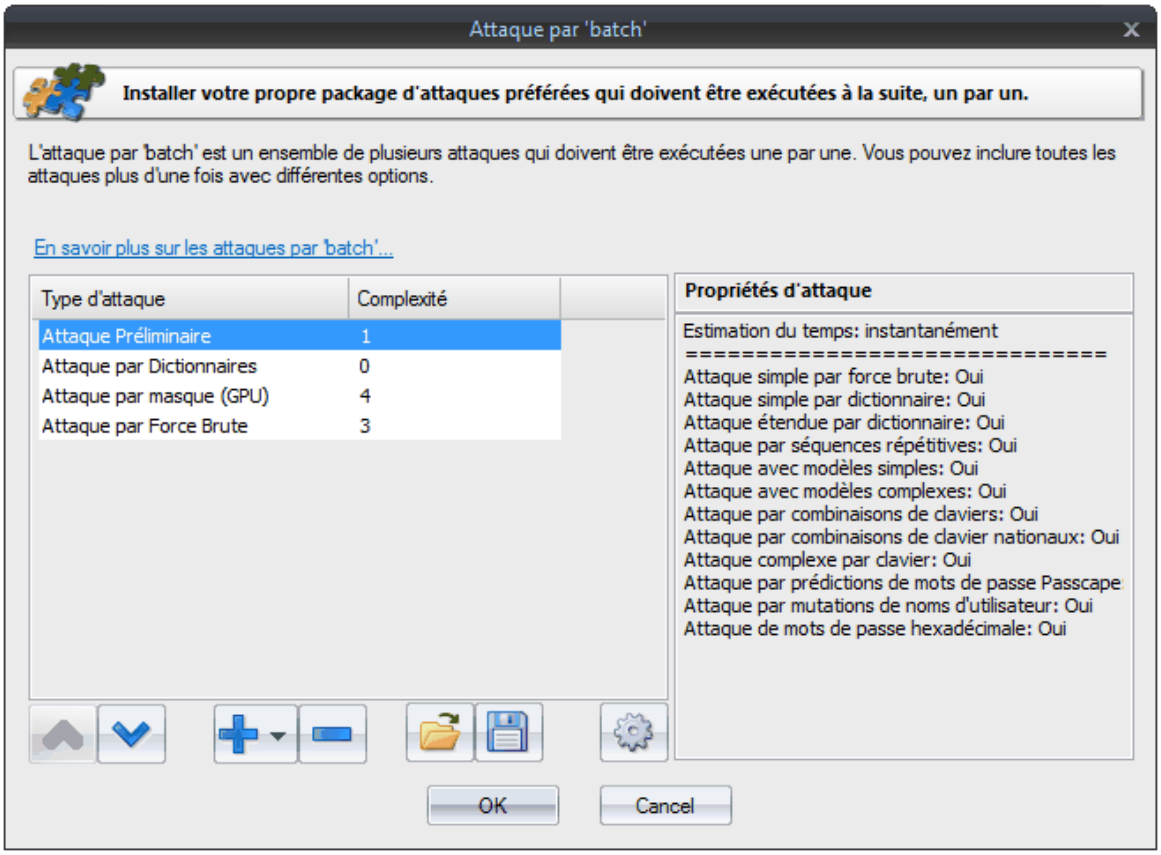
Les tables ne peuvent 'cracker' que les types de hachages pour lesquelles elles sont prévus, ex: Les tables NT ne peuvent 'cracker' que les hachages NT !

Pour créer vos propres tables, vous pouvez utiliser cet outil.

Vous pouvez télécharger un exemple de tables Passcape pour cette attaque à partir de notre site Web.

2.8.2.14 Attaque par Lots

Sachant que chaque attaque couvre sa propre plage de mots de passe, cependant, pour pouvoir récupérer tous les hachages de mots de passe, vous devez exécuter plusieurs attaques les une après les autres. L'idée de base derrière l'attaque par lots (développée par Passcape Software) est de créer une liste/lot d'attaques à exécuter les une après les autres, ainsi vous pouvez lancer ces attaques avec un simple clic de souris et non en configurant chaque d'elles individuellement chaque fois que vous en avez besoin.



Les options de l'attaque par lots sont disponibles sous la forme d'une liste qui peut être étendue ou réduite (boutons [+] et [-]). Chaque attaque peut être déplacée vers le haut ou le bas dans la liste (boutons [^] et [v]), et les paramètres peuvent être édités. Un lot (batch) peut inclure plusieurs attaques du même type, mais les attaques peuvent avoir des paramètres différents. Le panneau de droite, affiche les propriétés de l'attaque sélectionnée; en résumé les spécifications et le temps estimé prit par l'attaque pour aboutir.

2.8.2.15 GPU: Attaque par Force-brute

Une attaque GPU par Force-brute est identique à l'attaque standard par Force-brute, exceptée que tous les mots de passe sont recherchés par l'unité de calcul de la carte graphique de votre PC. Ce n'est pas un secret que les performances des cartes graphiques sont bien plus puissantes que les CPUs; Il est important de comprendre que les calculs en utilisant les cartes graphiques ont de nombreux désavantages. Par exemple, certains algorithmes avec un grand nombre de sauts conditionnels et ou d'autres tests démontrent la très faible performance des GPUs, et dans certains cas il peut être moins performant qu'un CPU standard.

Quoi qu'il en soit, le logiciel supporte la recherche de mots de passe par force-brute en utilisant un GPU. Vous pouvez comparer les indices de performances des calculs GPU versus CPU à l'aide menu

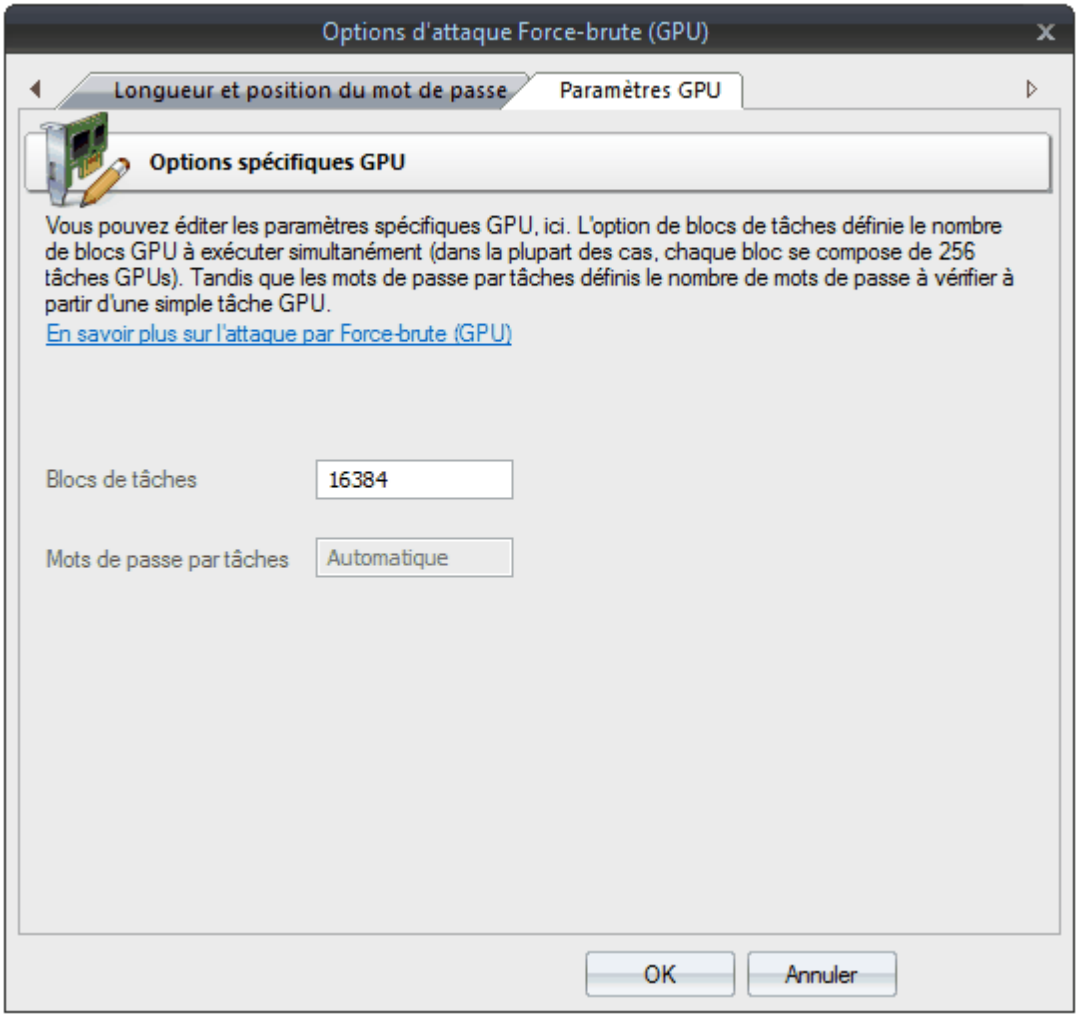
correspondant du logiciel ou visible à partir du menu '**Rapports**'

La configuration de l'attaque GPU par Force-brute est constituée de trois parties:
1. Choisissez un jeu de caractères pour la recherche.
2. Indiquez la longueur du mot de passe.
3. Configurez l'unité graphique de calcul.

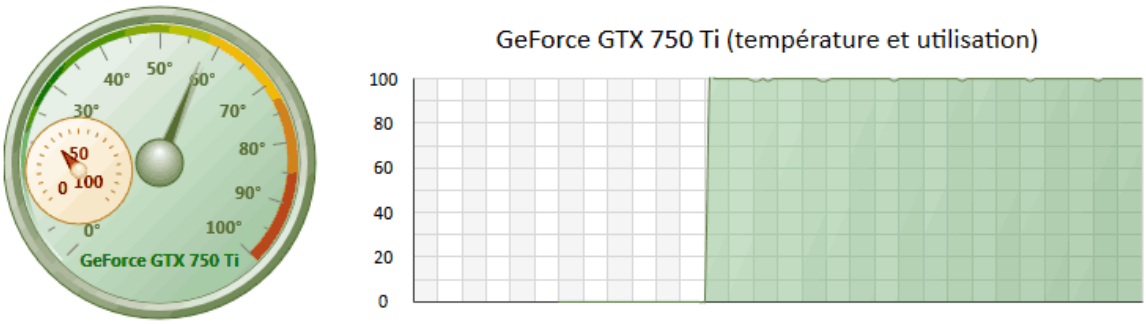
Choix d'un jeu de caractères pour la recherche
Lors du choix d'un jeu de caractères pour l'attaque par Force-brute, vous êtes habituellement guidé par considérations empiriques. Par exemple, si vous supposez que le mot de passe est constitué de caractères Latin en minuscules et de chiffres, il est logique de choisir une plage allant de 'a-z, 0-9'. Plus petit sera le jeu de caractères, plus rapide sera la fin de l'attaque.
En d'autres termes, il y a toujours un risque de faire le mauvais choix du jeu de caractères. Si au moins, un caractère du mot de passe à récupérer n'est pas inclus dans le jeu de caractères choisi, le mot de passe ne sera pas trouvé.
En bas de la boite de dialogue, du paramétrage de l'attaque, vous pouvez voir le nombre total de mots de passe qui corresponds au jeu de caractères choisi et à la longueur du mot de passe.
Il est important de savoir que les mots de passe LM dans Windows sont toujours converti en majuscule; cela réduit considérablement la plage de mots de passe a rechercher !

Paramétrage de la longueur du mot de passe
Dans le deuxième onglet des pages d'options, il faut définir la longueur minimum et maximum des mots de passes à rechercher. Comme alternative à la longueur minimum, vous pouvez définir un mot de passe source, avec lequel la recherche débutera. La longueur maximum des mots de passe LM, dans le système d'exploitation Windows est de 7.

Paramétrage de l'unité graphique de calcul (GPU)
Avant de pouvoir utiliser cette attaque, vous devez en premier choisir la carte graphique dans le menu correspondant.



La configuration du GPU est composée d'un seul paramètre: le nombre de blocs de tâches à exécuter pour le GPU. Chaque bloc est constitué de 256 tâches. Ainsi, si vous définissez le nombre de blocs à 25600, le GPU exécutera 25600 * 256 = 6553600 tâches. Chaque tâches de GPU peut vérifier plusieurs mots de passe. Le nombre total de mots de passe vérifié dépends beaucoup des autres options. Si vous définissez le paramètre '**Blocs de tâches**' inférieur à 10000, sur les cartes graphiques modernes, dans la majorité des cas, cela conduit à une mauvaise performance. Pour éviter une dégradation des performances, après avoir configuré le paramètre et lancé l'attaque, assurez-vous que le taux de charge de GPU est proche de 100% sans pics (voir la capture d'écran ci-dessous).

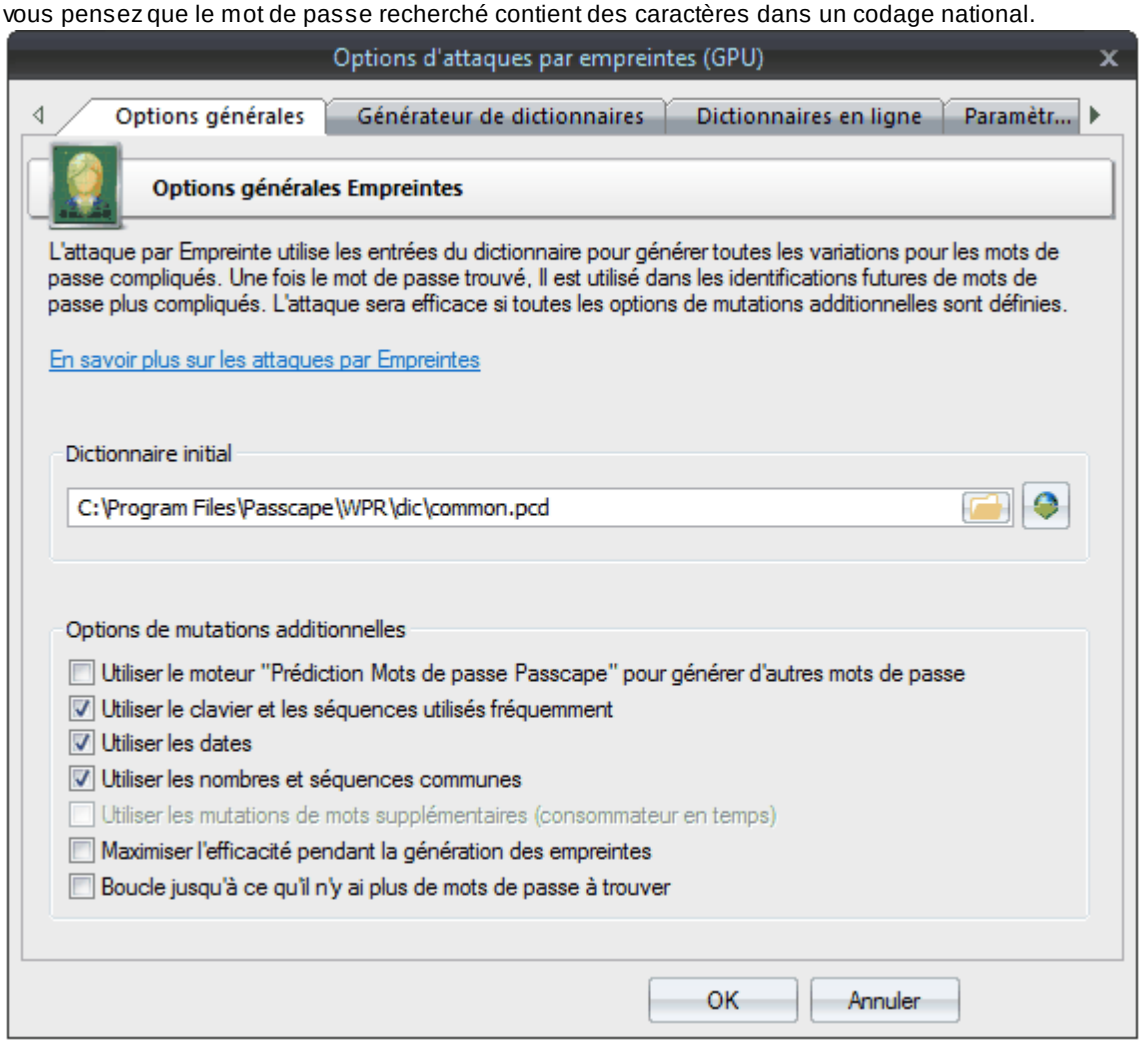


2.8.2.16 GPU: Attaque par Empreintes

L'attaque par empreintes est un outil tout récent pour la récupération des mots de passe complexes, qui ne pourraient pas être décryptés simplement. L'idée de cette attaque est que ici, pour récupérer un mot de passe, nous prenons ni des mots individuels à partir d'un dictionnaire source, comme dans l'attaque par

Dictionnaire, ni même des combinaisons de mots, comme dans l'attaque combinée, mais des "empreintes". Ainsi, chaque mot du dictionnaire source est utilisé pour générer plusieurs empreintes. Si un mot de passe est trouvé lors de l'attaque, il participe à la génération de nouvelles empreintes, et l'attaque recommence à nouveau. La mise en œuvre de la puissance de calcul des GPU permet d'augmenter la vitesse de récupération de façon importante.
Les options d'empreintes sont composées de 4 parties:

Options générales
Avant de lancer l'attaque, définissez le dictionnaire source à utiliser pour créer les empreintes. Le logiciel est livré avec le dictionnaire 'common.pcd', optimisé pour cette attaque, mais vous pouvez utiliser le votre ou en télécharger un sur Internet (Onglet '**Dictionnaires en ligne**'). Il n'y a pas d'exigences particulières concernant la liste de mots sources, sauf une: elle ne doit pas être trop grande; autrement, l'attaque prendra un temps considérable. Vous pouvez utiliser des dictionnaires de mots de passe nationaux, si vous pensez que le mot de passe recherché contient des caractères dans un codage national.



Voici la façon dont les empreintes sont générées: d'abord, un mot du dictionnaire source est divisé en mots de passe de 1 caractère, puis - dans de 2 caractères, etc. Par exemple, le mot source **crazy** est divisé en empreintes d'un seul caractère. Donc, nous obtenons:
c
r
a
z
y

Maintenant, en deux caractères:
cr
ra

az
zy

Ensuite, trois caractères:
cra
raz
azy

Et, finalement en quatre caractères:
craz
razy

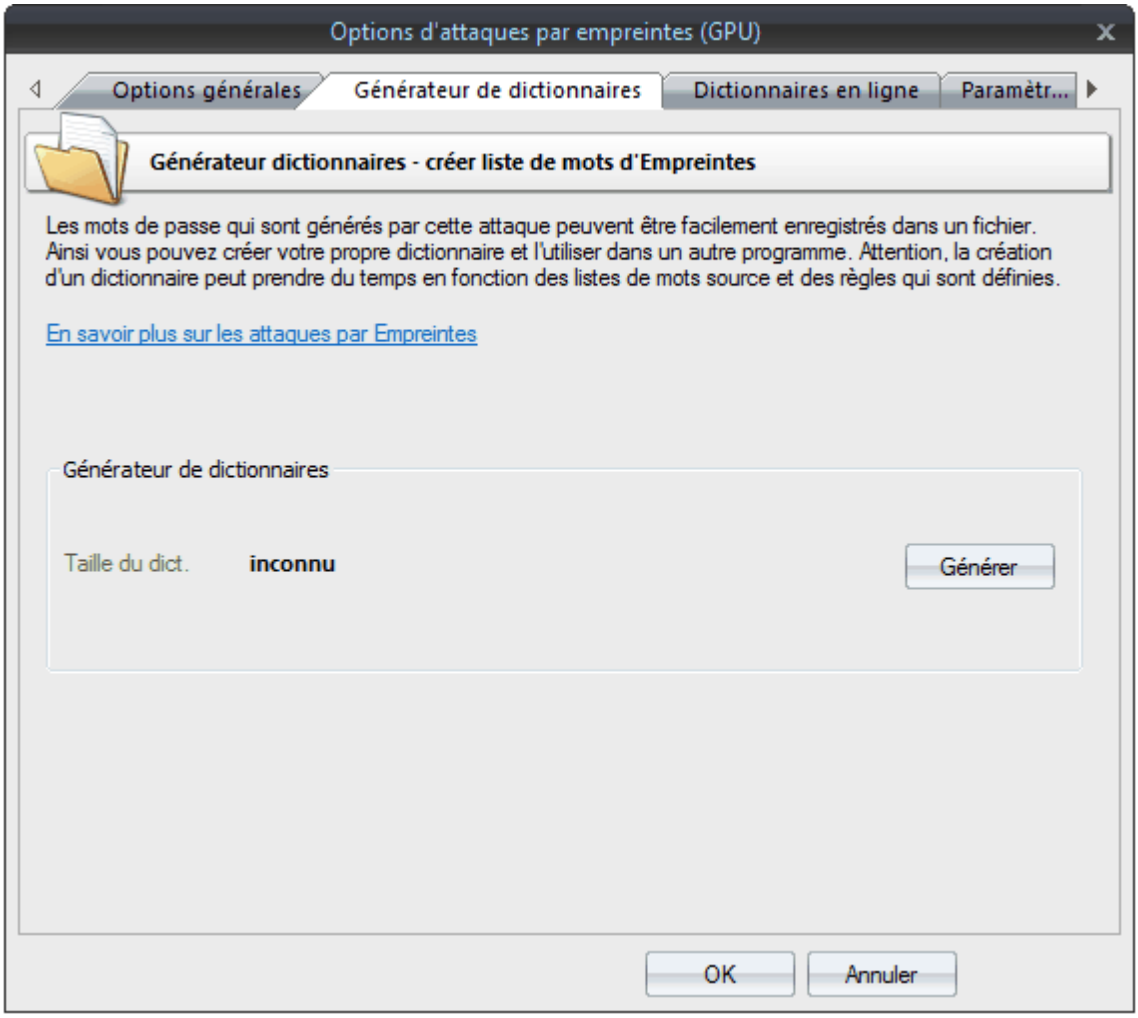
Nous avons 5 + 4 + 3 + 2 = 14 empreintes, sans compter le mot source.
Tous les mots du dictionnaire source sont divisés en empreintes. Après cela, toutes les empreintes sont envoyées dans une seule base de données, naturellement, en rejetant les doublons. Donc nous avons une base de données d'empreintes qui pourrait être utilisée pour la vérification des mots de passe en collant toutes les empreintes les unes avec les autres et jusqu'à trouver une correspondance.

Le vrai algorithme de génération d'empreintes est un peu plus sophistiqué. En outre, il y a une option dans les paramètres d'attaque, '**Maximiser l'efficacité pendant la génération des empreintes'** , qui maximise l'efficacité (au détriment de la vitesse) en générant des empreintes supplémentaires.

Jetons un coup d'œil sur les options restantes:
Utiliser le moteur PPP pour générer d'autres mots de passe - Utilise les mots de passe trouvés dans d'autres attaques lors de la génération des empreintes.
Utiliser le clavier et les séquences utilisés fréquemment - Ajoute des combinaisons de touches et de séquences communes à la banque d'empreintes.
Utiliser des dates - Ajoute des dates aux empreintes.
Utiliser des nombres et des séquences communes - Utilise des chiffres et et de simples combinaisons de lettres.

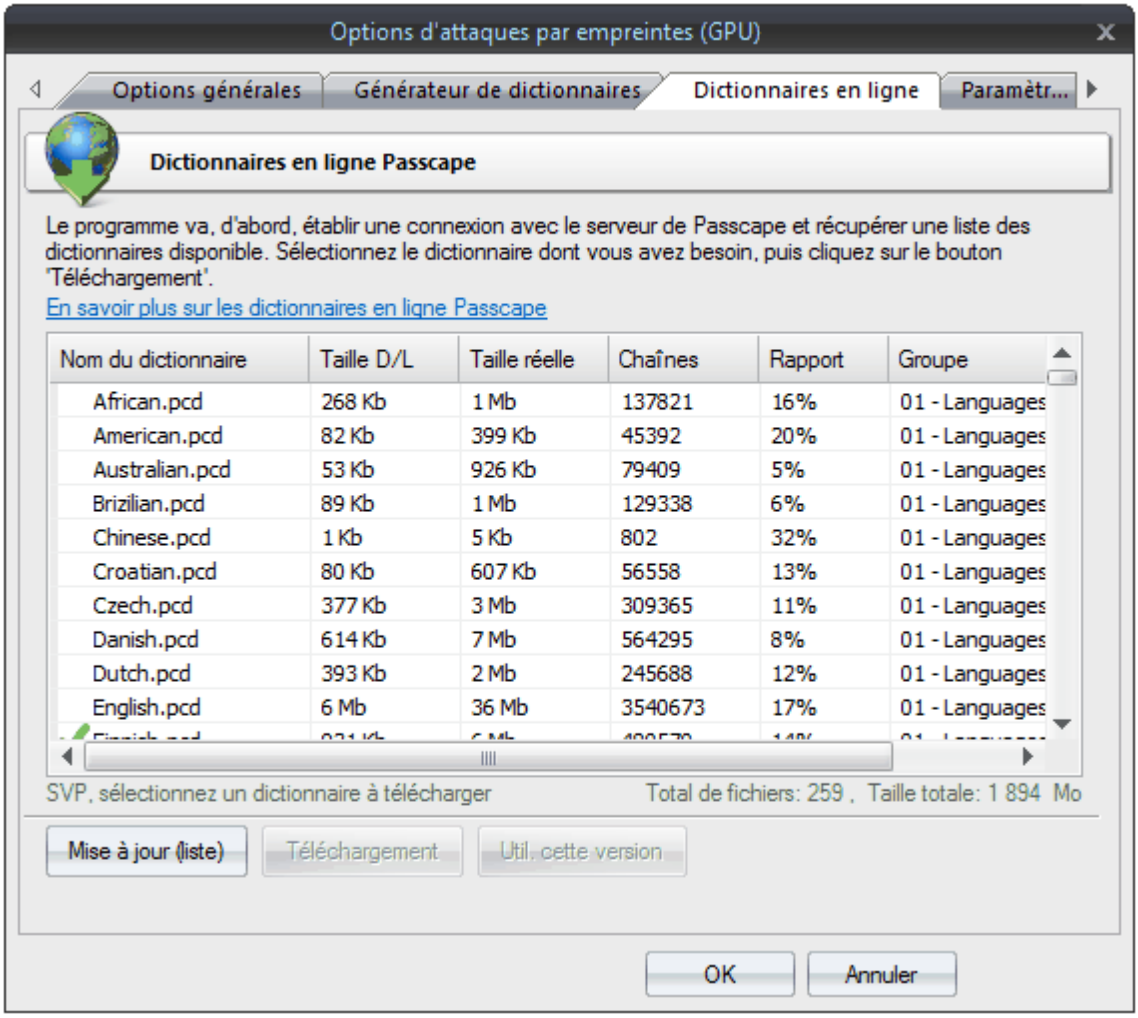
La plus grande attention doit être apportée à l'option '**Boucle jusqu'à ce qu'il n'ai plus de mots de passe à trouver**'. C'est ici où l'attaque par empreintes peut vraiment montrer son efficacité.
Voici comment cela fonctionne:
Si au moins un mot de passe est trouvé lors d'une attaque, lorsque l'attaque est terminée, le mot de passe participe a générer de nouvelles empreintes, et l'attaque redémarre à nouveau. Cette option fonctionne très bien sur de grandes listes de tables de hachage et sur les hachages d'historique de mots de passe. Cependant, une fois l'option activée, vous ne serez plus en mesure d'exécuter l'attaque de la dernière position enregistrée

Générateur de dictionnaires
Le deuxième onglet avec les paramètres, permet de créer et sauvegarder un dictionnaire personnalisé en utilisant les options actuelles de l'attaque par empreintes. Attention; le dictionnaire peut prendre beaucoup d'espace sur le disque dur de votre PC.



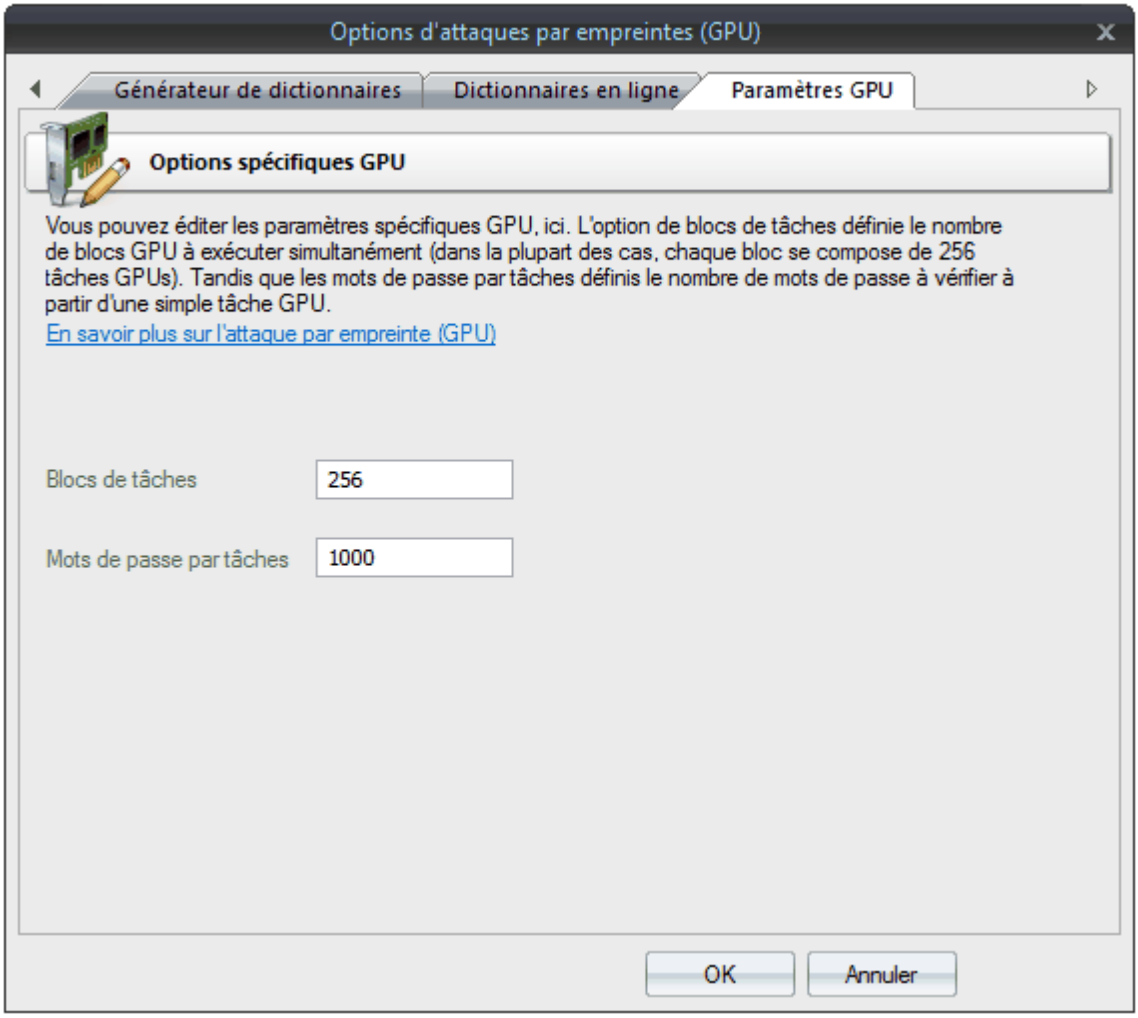
Dictionnaires en ligne

Dans le troisième onglet, vous pouvez télécharger des listes de mots de source pour l'attaque par empreintes à partir d'Internet. Soyez prudent, tous les dictionnaires ne sont pas adaptés à cette attaque.



Paramètres GPU

Avant d'utiliser un GPU dans une attaque, vous devez d'abord sélectionner la carte graphique dans le menu Options Générales.



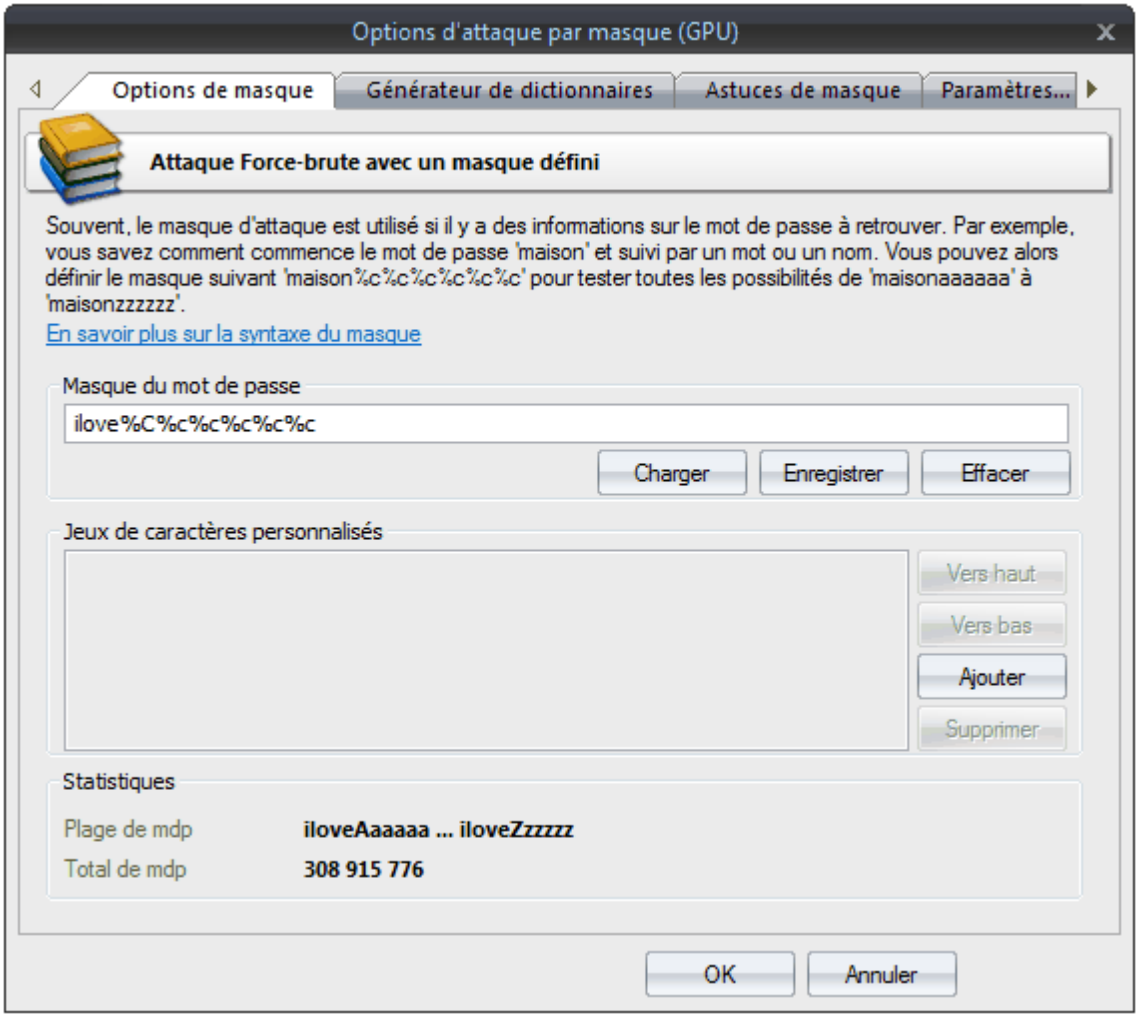
Le paramétrage du GPU est assez simple et se compose de deux parties:

1. Définissez le nombre de blocs parallèles de la carte graphique, où les mots de passe doivent être recherchés. Typiquement, chaque bloc se compose de 256 tâches. Ainsi, si vous définissez le nombre de blocs à 256, le GPU exécutera 256 * 256 = 65536 tâches. Le nombre total de mots de passe testés pour un appel au noyau GPU sera 256*Blocs de tâches*TâchesParMotdePasse. Dans notre cas 256 * 256 * 1000 = 65 536 000 mots de passe. Régler le paramètre '**Blocs par tâches**' plus petit que 256 sur les cartes graphiques modernes, dans la majorité des cas, cela conduit à une dégradation des performances.
2. Définissez le nombre de mots de passe à rechercher pour une simple tâche. Plus grande est la valeur, plus le nombre de tâches sera faible, et du coup la vitesse de recherche importante. Cependant, une trop grande valeur peut bloquer l'ordinateur ou provoquer d'importantes fluctuations de la vitesse de recherche en cours. Ce nombre est affichée sur l'onglet d'état de l'attaque. Ceci est provoqué par le fait que le temps d'achèvement de la tâche sur le GPU est supérieure au temps nécessaire pour l'actualisation de l'état actuel de l'attaque. Définir un trop grand nombre peut causer une défaillance du système (plantage du PC).

2.8.2.17 GPU: Attaque par Masque

Options de masque

L'attaque par masque est un outil irremplaçable quand vous connaissez une partie du mot de passe ou si vous avez des informations spécifiques à son sujet. Par exemple, quand vous savez que le mot de passe est composé de 12 caractères et se termine avec *qwerty*, Il est évident que faire une recherche des mots de passe sur une plage de 12 caractères est déraisonnable (et inutile, car il prend une éternité à terminer). Tout ce qui serait nécessaire dans ce cas est de deviner les 6 premiers caractères du mot de passe recherché. L'attaque par Masque est idéale pour ce genre de situation.

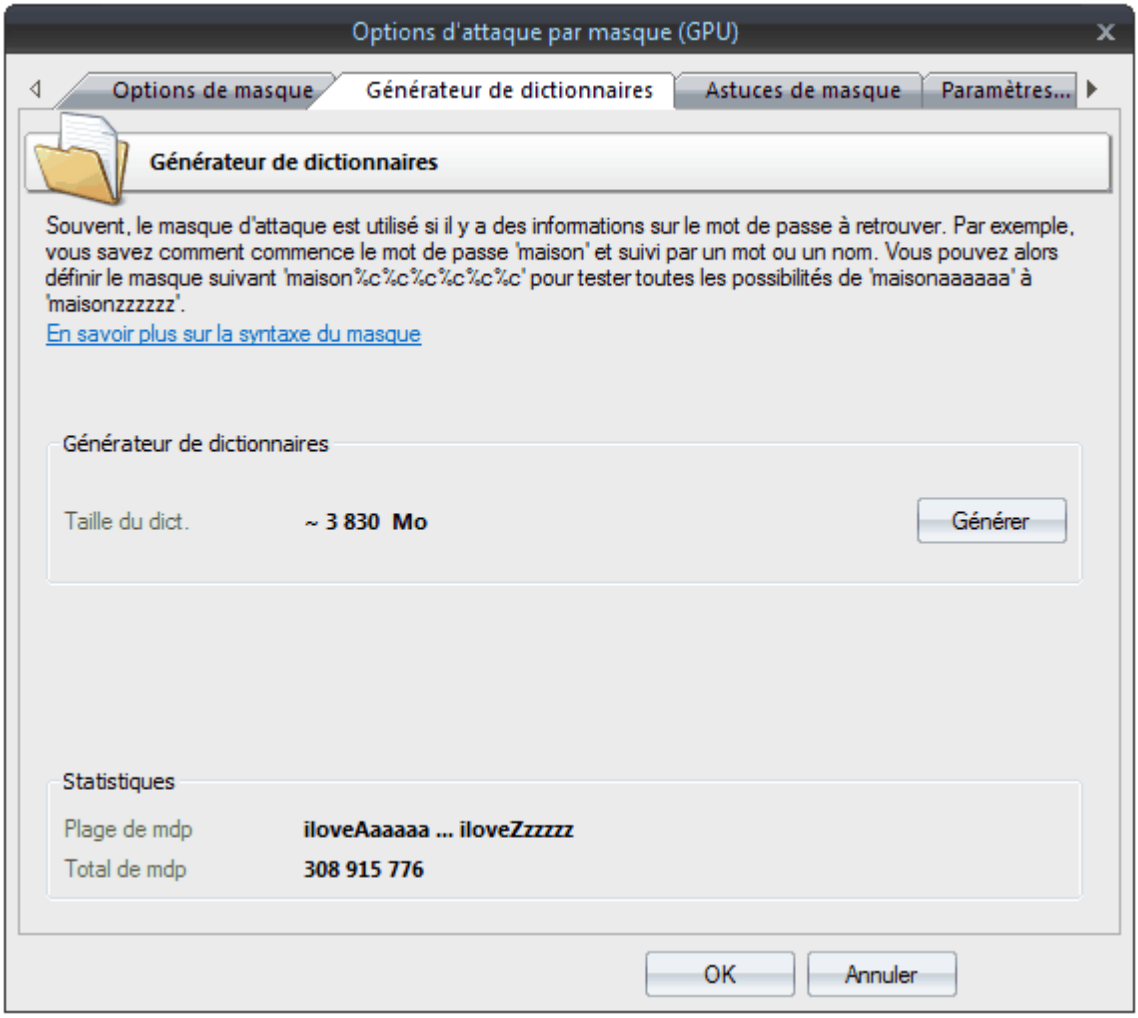


Dans notre cas, nous pouvons définir le masque suivant: **%c%c%c%c%c%cqwerty**. Cela signifie que le programme va vérifier successivement les combinaisons suivantes: aaaaaaqwerty, aaaaabqwerty, aaaaacqwerty .. zzzzzzqwerty. Si le mot de passe d'origine est '*secretqwerty*', Il est parfaitement dans la plage de recherche.

Le champ de saisie du masque est utilisé pour définir la règle, qui est utilisé par le programme pour deviner le mot de passe. Si la syntaxe du masque est correcte, dans le bas de la boite de dialogue s'affichera la plage de caractères générée par le masque. Les masques définis par l'utilisateur peuvent être sauvegardés sur le disque dur de votre ordinateur..

Générateur de dictionnaire

Dans l'onglet '**Générateur de dictionnaires**', vous pouvez générer votre propre dictionnaire avec un masque donné, et l'enregistrer sur le disque. Cette fonctionnalité est disponible dans l'édition 'Advanced' du programme seulement.



Astuces de masque

Le troisième onglet des options de masque contient une brève description de la syntaxe de masque et quelques exemples. La syntaxe de masque est assez simple et se compose de caractères (non modifiable) et dynamiques (modifiables). Les caractères dynamiques ont caractères ' % ' au début. Par exemple, si vous définissez le masque **secrète%d%d%d%d**, Le programme va générer 10000 mots de passe (secret0000, secret0001, secret0002 .. secret9999).

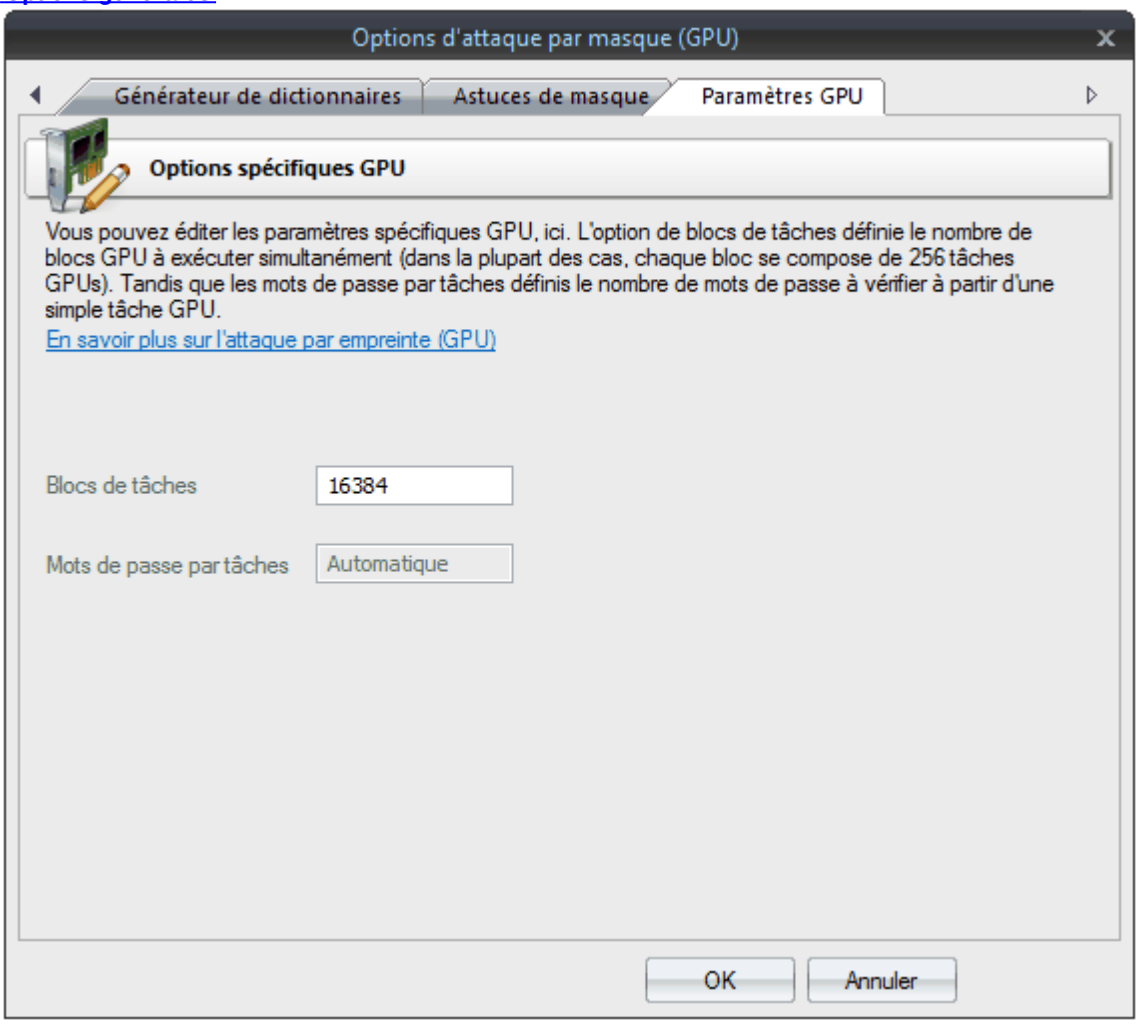
Windows Password Recovery prends en charge les jeux de masques dynamiques suivants:

- **%c** caractères en minuscules Latin (a..z), 26 symboles
- **%C** caractères en majuscules Latin (A..Z), 26 symboles
- **%#** jeu complet des caractères spéciaux (!..~ espace), total 33 symboles
- **%@** petit jeu de caractères spéciaux (!@#$%^&*()-_+= espace), 15 symboles
- **%?** tous les caractères imprimables avec les codes ASCII de 32..127
- **%*** Tous les caractères ASCII (codes 1 à 255)
- **%d** un chiffre (0..9)
- **%r(x-y)** les caractères définis par l'utilisateur avec la série de codes ASCII entre x et y
- **%r(x1-y1,x2-y2...xn-yn)** jeu de plusieurs séquences de caractères ASCII sans chevauchement. Très utile pour définir des jeux de caractères personnalisés; ex., de caractères OEM.
- **%1[2,3..9]** un caractères provenant d'un jeu de caractères personnalisé 1..9
- **%%** caractères statique '%' indépendant

Exemples:
test%d - générera une plage de mot de passe de test0..test9, un total de 10 mots de passe
test%d%d%d%d - test0000..test9999, 10000 mots de passe
test%r(0x0600-0x06ff) - 256 mots de passe avec des caractères Arabe à la fin
%#test%# - _test_..~test~, 1089 mots de passe
%1%1%1pin%2%2%2 - aaapin000.. zzzpin999, где %1 est un jeu de caracteres defini par l'utilisateur 1 (a..z), et %2 - le second jeu de caractères défini par l'utilisateur 0..9
ilove%1%1%1%1%1 - iloveaaaaa .. iloveZZZZZ, %1 est un jeu de caractères (a..z, A..Z)

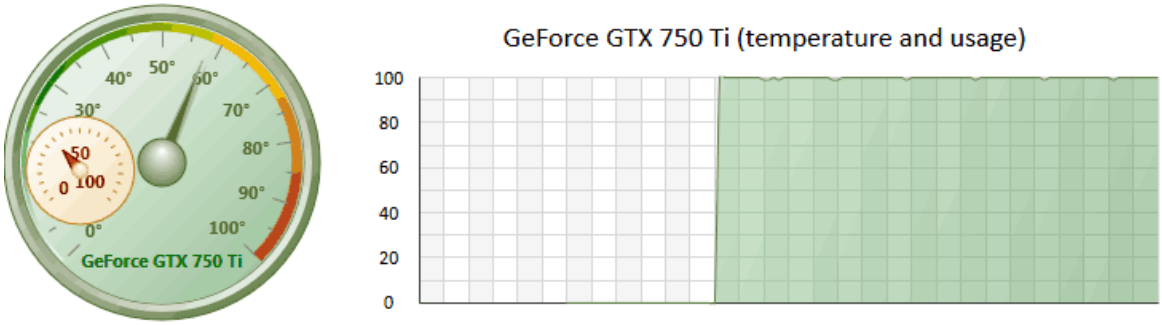
La syntaxe de l'attaque par masque (GPU) diffère légèrement de celle utilisée dans une attaque normale par masque. La principale différence est que dans l'attaque à base de GPU vous **ne pouvez pas** définir des numéros entre x et y et vous ne pouvez pas définir une plage de longueur variable définie par l'utilisateur, par ex. la syntaxe suivante ne fonctionnera pas pour une attaque par masque (GPU):
%d(x-y)
%1[2,3..9](min-max)

Paramètres GPU
Avant de pouvoir utiliser cette attaque, vous devez d'abord sélectionner la carte graphique dans le menu '**Options générales**'.



La configuration GPU pour l'attaque par Masque est composée d'un seul paramètre: le nombre de blocs de tâches à exécuter pour le GPU. Chaque bloc est constitué soit de 128 ou de 256 tâches. Ainsi, si vous définissez le nombre de blocs à 10000, le GPU exécutera 25600 * 256 = 6553600 tâches. Chaque tâche de GPU peut vérifier plusieurs mots de passe. Le nombre total de mots de passe vérifié dépends beaucoup des autres options. Si vous définissez le paramètre '**Blocs de tâches**' inférieur à 10000, sur les

cartes graphiques modernes, dans la majorité des cas, cela conduit à une mauvaise performance. Pour éviter une dégradation des performances, après avoir configuré le paramètre et lancé l'attaque, assurez-vous que le taux de charge de GPU est proche de 100% sans pics (voir la capture d'écran ci-dessous, d'une NVidia GTX 750Ti avec 15000 blocs).



2.8.2.18 GPU: Attaque par Dictionnaire-Force brute

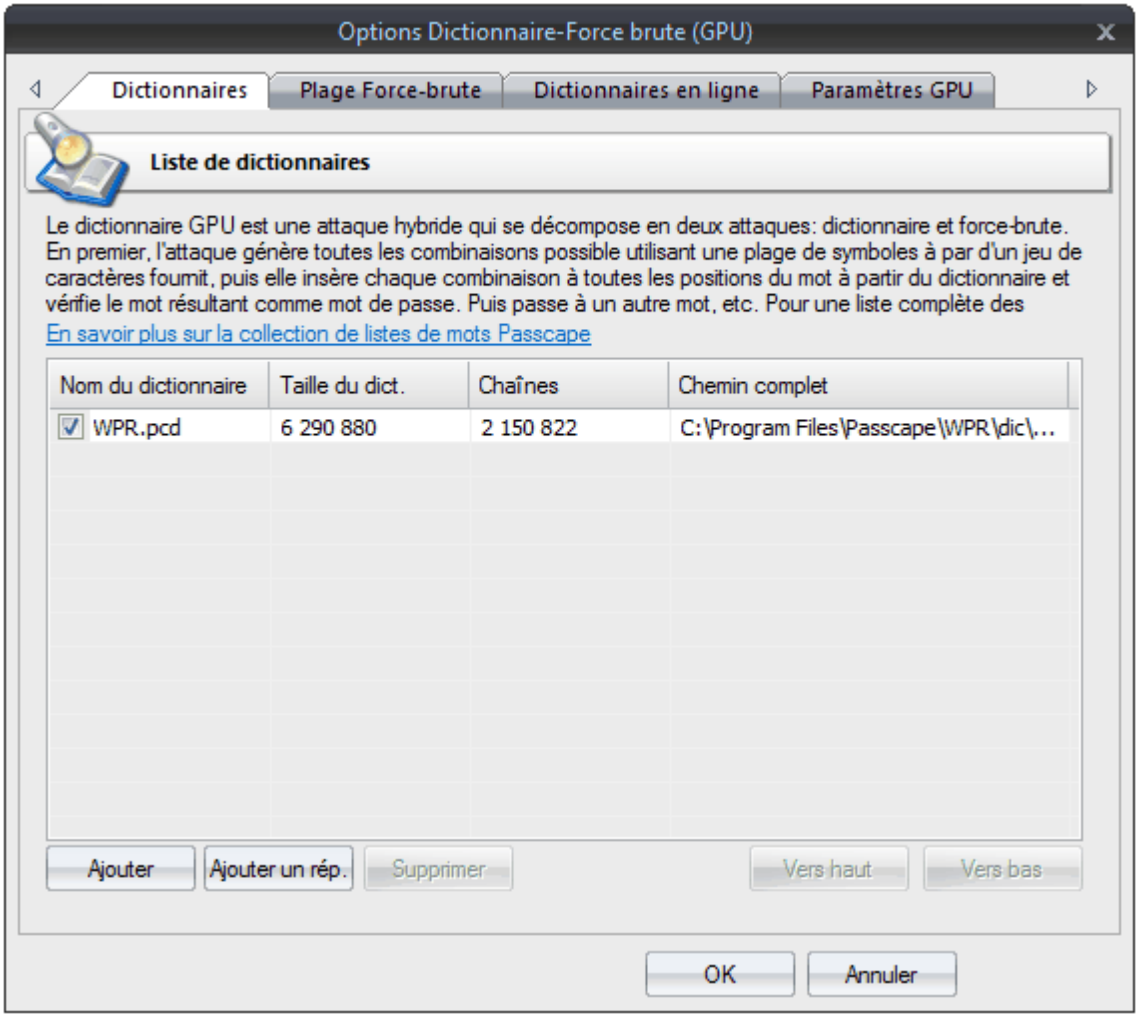
Souvent, lors de la création de mots de passe, les utilisateurs ajoutent certains caractères au début, à la fin ou même milieu du mot. Pour récupérer ce type spécifique de mots de passe, nous en sommes venus à une attaque par dictionnaire force-brute (GPU), qui est entre la simple attaque de dictionnaire et l'attaque par Force-brute.

Cette attaque fonctionne de la manière suivante:
- En premier, la lecture du premier mot du dictionnaire.
- En fonction du jeu de caractères défini et la longueur minimum/maximum de la plage de recherche, génère toutes les variantes possibles.
- Ces variantes (caractères) sont ensuite ajoutées au début, à la fin ou au milieu du mot. La position dans le mot, où les séquences générées doivent être insérées, peuvent être définies selon vos souhaits.
- Ensuite on passe au prochain mot du dictionnaire, etc.

Par exemple, si nous spécifions une plage de caractères pour la recherche entre **0** et **9**, et la plage de longueur entre **1** et **2**, le programme va générer 100 combinaisons: 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11 .. 99. Ensuite, ces séquences seront ajoutés au début, au milieu ou à la fin du mot. Ainsi, pour le mot **test**, si les séquences qui doivent être insérées à toutes les positions listées, le programme vérifiera les mots de passe suivants:
0test, 1test .. 99test
t0est, t1est .. t99est
te0st, te1st .. te99st
tes0t, tes1t .. tes99t
test0, test1 .. test99
Total - 100*5=500 variantes

Jetons un coup d'œil, de plus près, aux paramètres d'attaque.

Dictionnaires
Dans l'onglet '**Dictionnaires**', vous pouvez spécifier la liste des dictionnaires à utiliser dans l'attaque. Le programme supporte des listes de mots texte dans les formats suivants: ASCII, UNICODE, UTF8, RAR, ZIP, ainsi que des dictionnaires chiffrés/compressés dans le format natif de PCD, développés par notre société. Pour désactiver un dictionnaire, décochez simplement la case portant son nom. Ainsi, bien que le dictionnaire reste sur la liste, il sera ignoré lors de l'attaque. Le logiciel est livré avec la valeur par défaut, un dictionnaire de 400000 mots. Vous pouvez commander un jeu complet de dictionnaires, qui représente une taille de plus de 6 Go, sur CDs ou de profiter des dictionnaires disponibles en ligne.

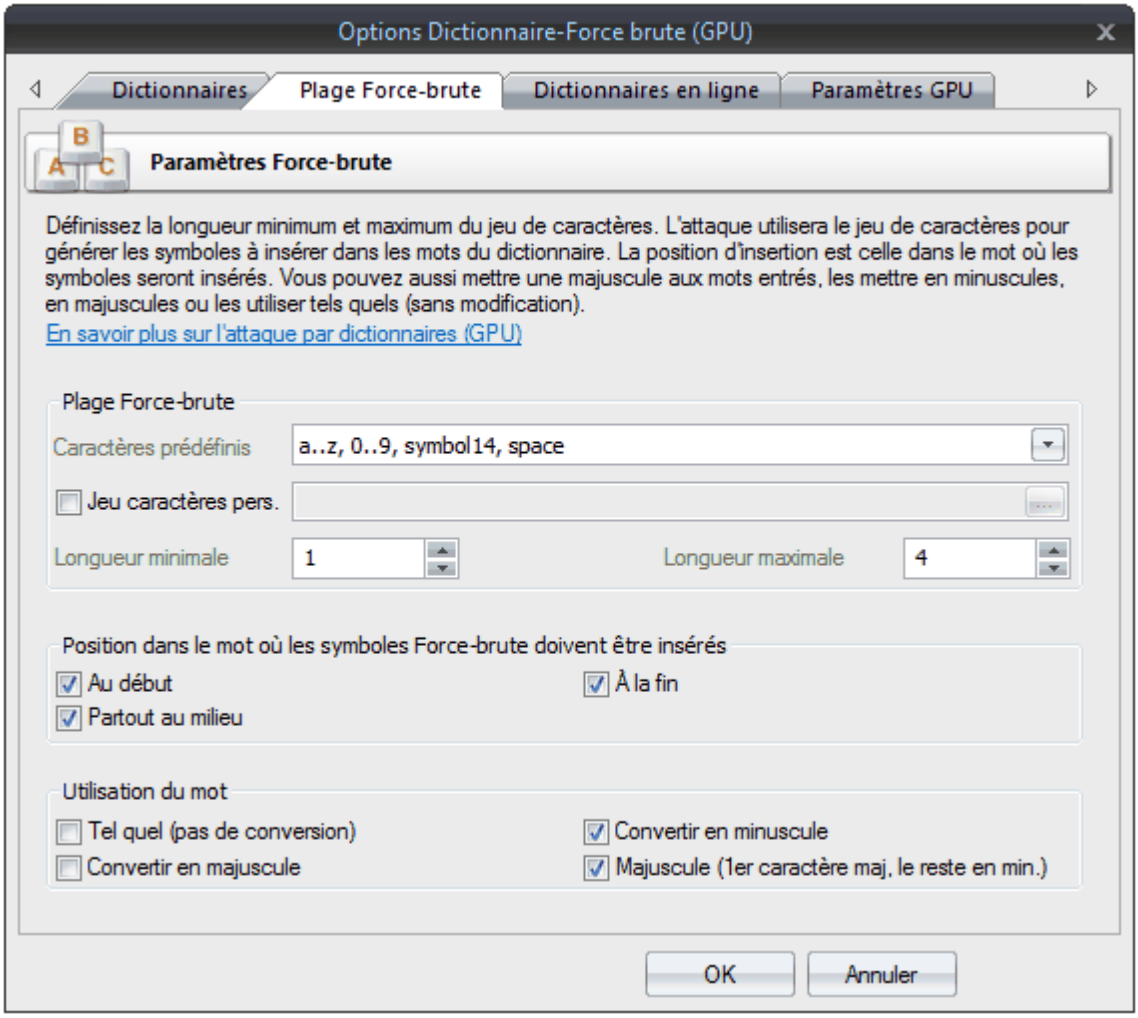


Plage de recherche

Dans cet onglet, vous devez définir la plage de caractères qui doivent être insérée dans les mots de base, sa longueur minimale et maximale. Lors du paramétrage de la plage, vous pouvez utiliser les modèles existants, ou après avoir coché la case correspondante, définir le votre. Lors de la sélection de la longueur maximale de la plage, gardez à l'esprit que le paramétrage d'une valeur trop large ou trop petite est déconseillé. Alors que dans le premier cas, la vitesse de recherche du mot de passe peut descendre à 0, en paramétrant une plage trop étroite de caractères à rechercher cela revient à l'utilisation non rationnelle de la puissance de calcul du GPU.

Dans le second groupe d'options, paramétrez la position dans le mot, où les caractères de la plage de recherche doivent être insérés.

Et, enfin, le troisième groupe de paramètres - ils sont en charge du pré-calcul des mots du dictionnaire source. Si vous cochez l'option '**Tel quel (pas de conversion)**' cela permets au programme d'utiliser le mot source sans le convertir en majuscules ou en minuscules. Le nombre de mots de passe à rechercher croît directement proportion avec le nombre des options spécifiées dans ce groupe. D'autre part, le programme est assez intelligent pour ne pas utiliser des mots en doublons. Par exemple, le mot **12345678**, même si toutes les options de conversion sont activées, ne sera utilisé qu'une seule fois.



Le nombre de mot de passe à rechercher pour un simple mot peut être calculé avec la formule suivante:

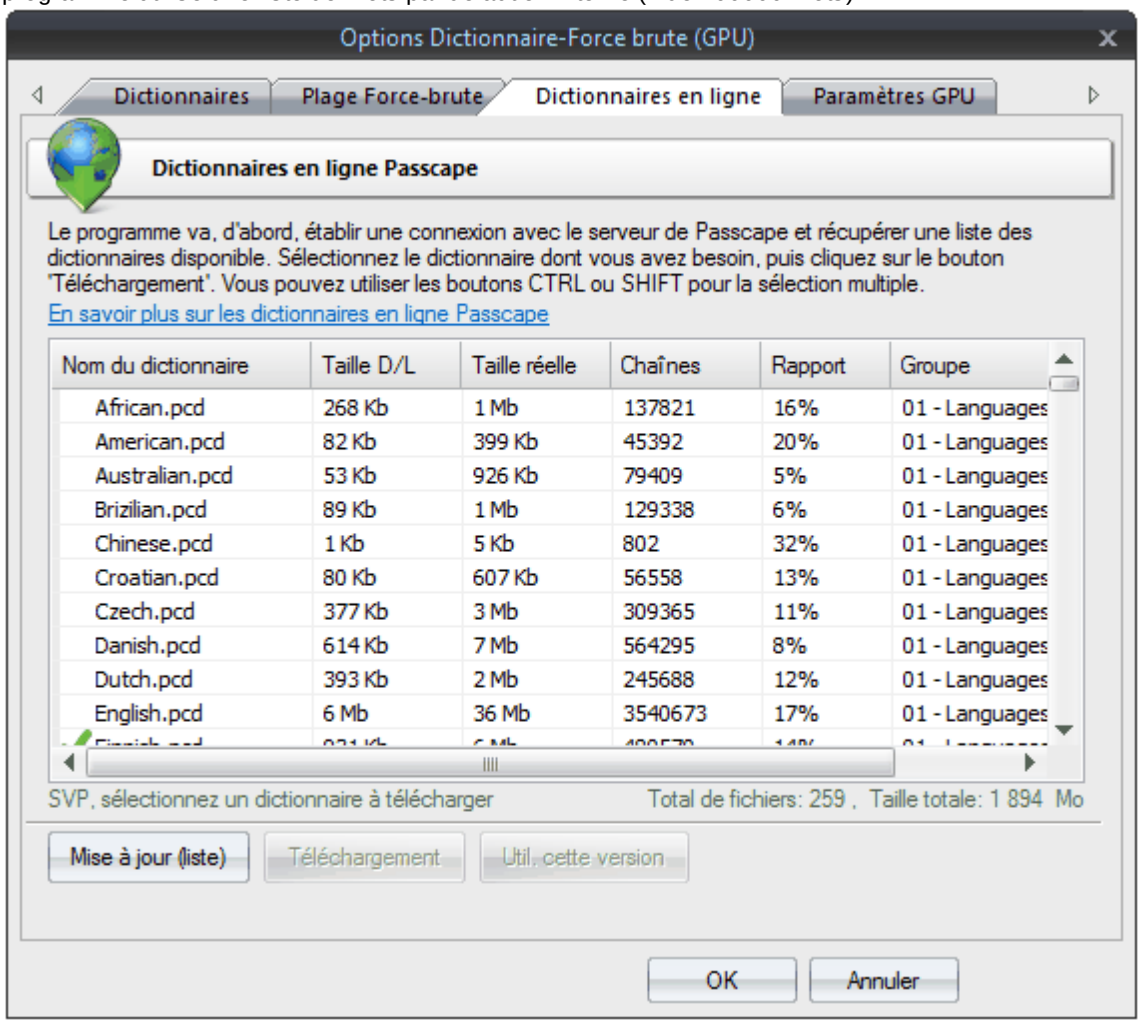
Les mots de passe = R * L * K
où
R - est la plage de caractères, calculée en utilisant la formule: R = longueur du jeu de caractères ^ longueur maximum - longueur du jeu de caractères ^ (longueur minimum-1) +1
L - est la position dans le mot. Calculée de la manière suivante: si l'insertion est faite dans le milieu du mot, L = longueur du mot de passe - 1; ensuite on ajoute +1 si l'insertion est faite au début et à la fin du mot.
K - est le nombre d'options choisies dans le groupe '**Utilisation du mot**'.

Par exemple, si le mot source est **window**, et que les options choisies sont à l'image de celles-ci:
- plage de caractères **a..z,A..Z,0..9,symbol14,espace**
- insertion à toutes les positions
- conversion en minuscule
- capitalisation (première caractère en majuscule, le reste en minuscule)

Calculons maintenant, combien de mots de passe nous allons vérifier pour ce mot:
longueur du jeu de caractères = 26+26+10+14+1 = 77
R = 77^4 - 77^0 + 1 = 35153041
L = (6-1) + 1 + 1 = 7
K = 2
Nombre de mots de passe = 35153041 * 7 * 2 = **492 142 574**

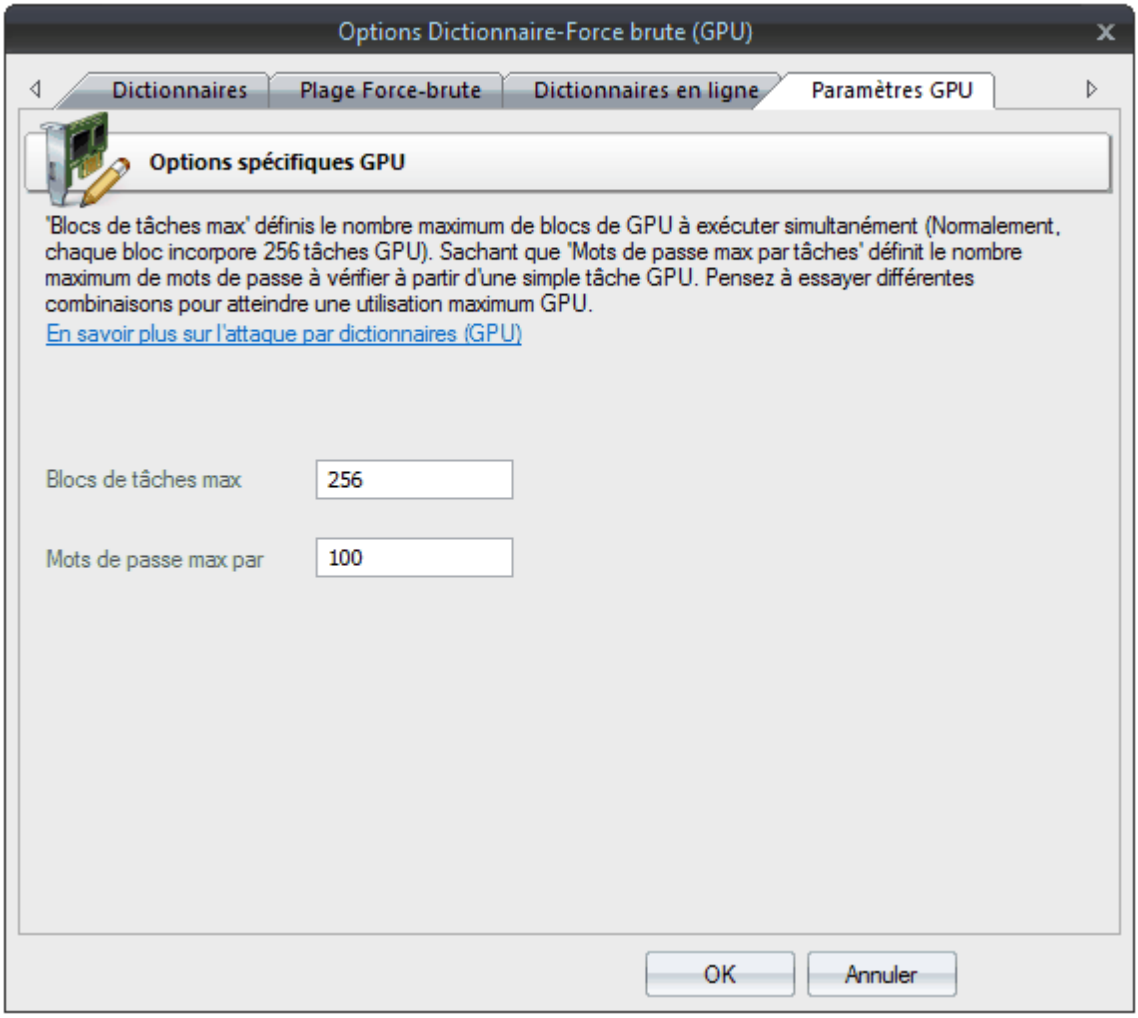
Dictionnaires en ligne

Dans ce troisième onglet, vous pouvez télécharger des listes de mots source pour l'attaque. Le programme utilise une liste de mots par défaut en interne (+ de 400000 mots).



Paramètres GPU

Avant de pouvoir utiliser un GPU pour l'attaque, vous devez d'abord en choisir une dans le menu correspondant du menu principal.



Le paramétrage du GPU est assez simple et se compose de deux parties:

1. Définissez le nombre des blocs parallèle de la carte graphique, où les mots de passe doivent être recherchés. Typiquement, chaque bloc se compose de 256 tâches. Ainsi, si vous définissez le nombre de blocs à 256, le GPU exécutera 256 * 256 = 65536 tâches. Le nombre total de mots de passe et testés pour un appel au noyau GPU sera 256*Blocs de tâches*TâchesParMotdePasse. Dans notre cas 256 * 256 * 1000 = 65 536 000 mots de passe. En réglant le paramètre '**Blocs par tâches**' plus petit que 256 sur les cartes graphiques modernes, dans la majorité des cas, cela conduit à une dégradation des performances.
2. Définissez le nombre de mots de passe à rechercher pour une simple tâche. Plus grande est la valeur, plus le nombre de tâches sera faible, et du coup la vitesse de recherche importante. Cependant, une trop grande valeur peut bloquer l'ordinateur ou provoquer d'importantes fluctuations de la vitesse de recherche en cours. Ce nombre est affichée sur l'onglet d'état de l'attaque. Ceci est provoqué par le fait que le temps d'achèvement de la tâche sur le processeur graphique est supérieur au temps nécessaire pour l'actualisation de l'état actuel de l'attaque. Définir un trop grand nombre peut causer une défaillance du système (plantage du PC).

En fonction des options que vous avez choisi, un choix de paramètres GPU optimal peut considérablement, voir plusieurs fois, accroître la vitesse de recherche des mots de passe. Nous vous recommandons de 'jouer' au maximum, avec les paramètres GPU pour optimiser au maximum son utilisation dans cette attaque.

2.8.2.19 GPU: Attaque hybride par Dictionnaire

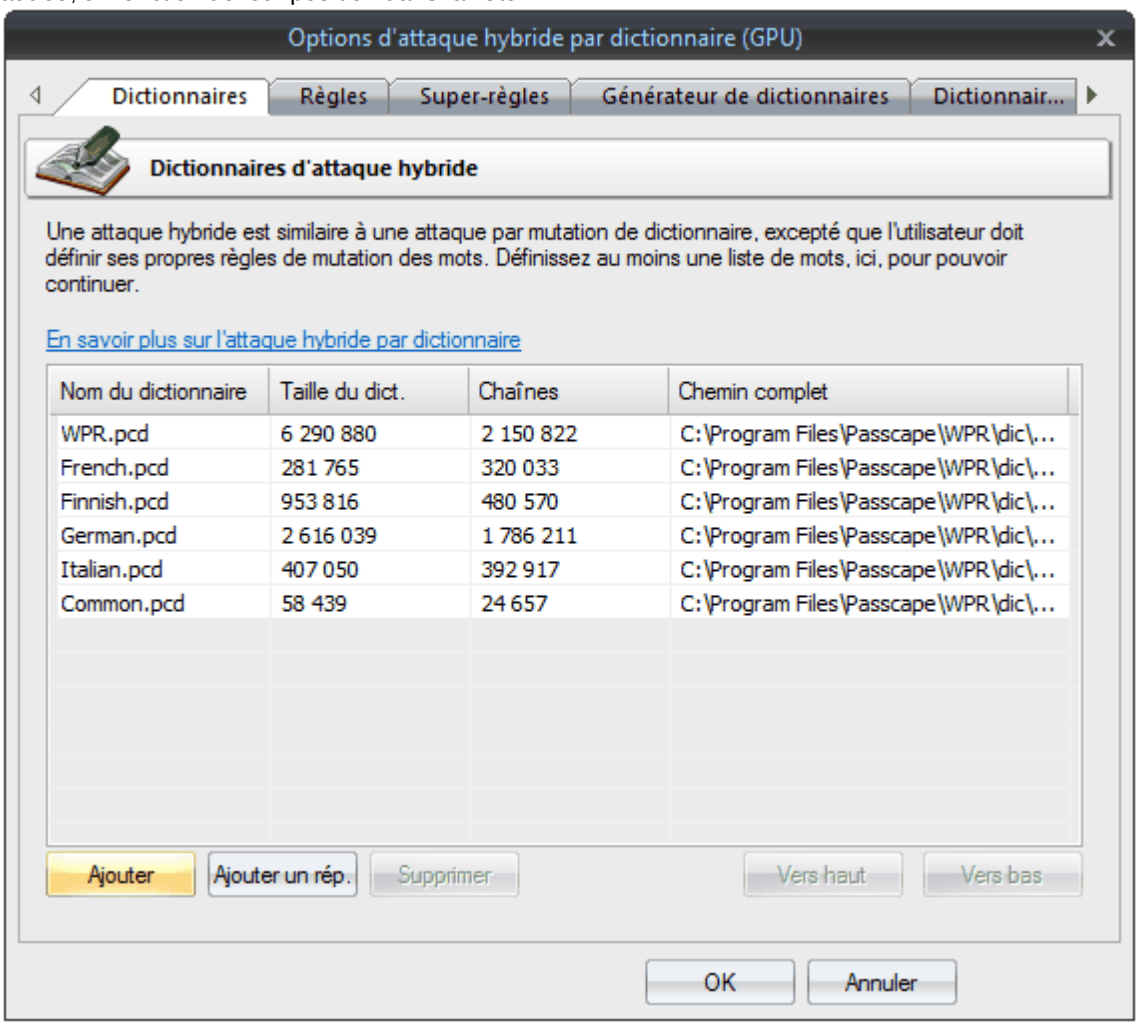
L'attaque hybride par dictionnaires - GPU est à peu près la même que L'attaque hybride par dictionnaire, excepté le fait qu'elle utilise la puissance du GPU à la place du CPU. Ce qui la rends extrêmement rapide. Approximativement 10 fois plus rapide qu'une simple attaque hybride. Le gain en vitesse dépends grandement des options et du matériel qui est utilisé. L'attaque hybride permets à l'utilisateur de définir

ses propres règles de modifications de mots et de vérifier les mots créés.

Les actions, effectuées sur les mots du dictionnaire, sont appelées des règles. Des règles multiples peuvent être appliquées à chaque mot source.

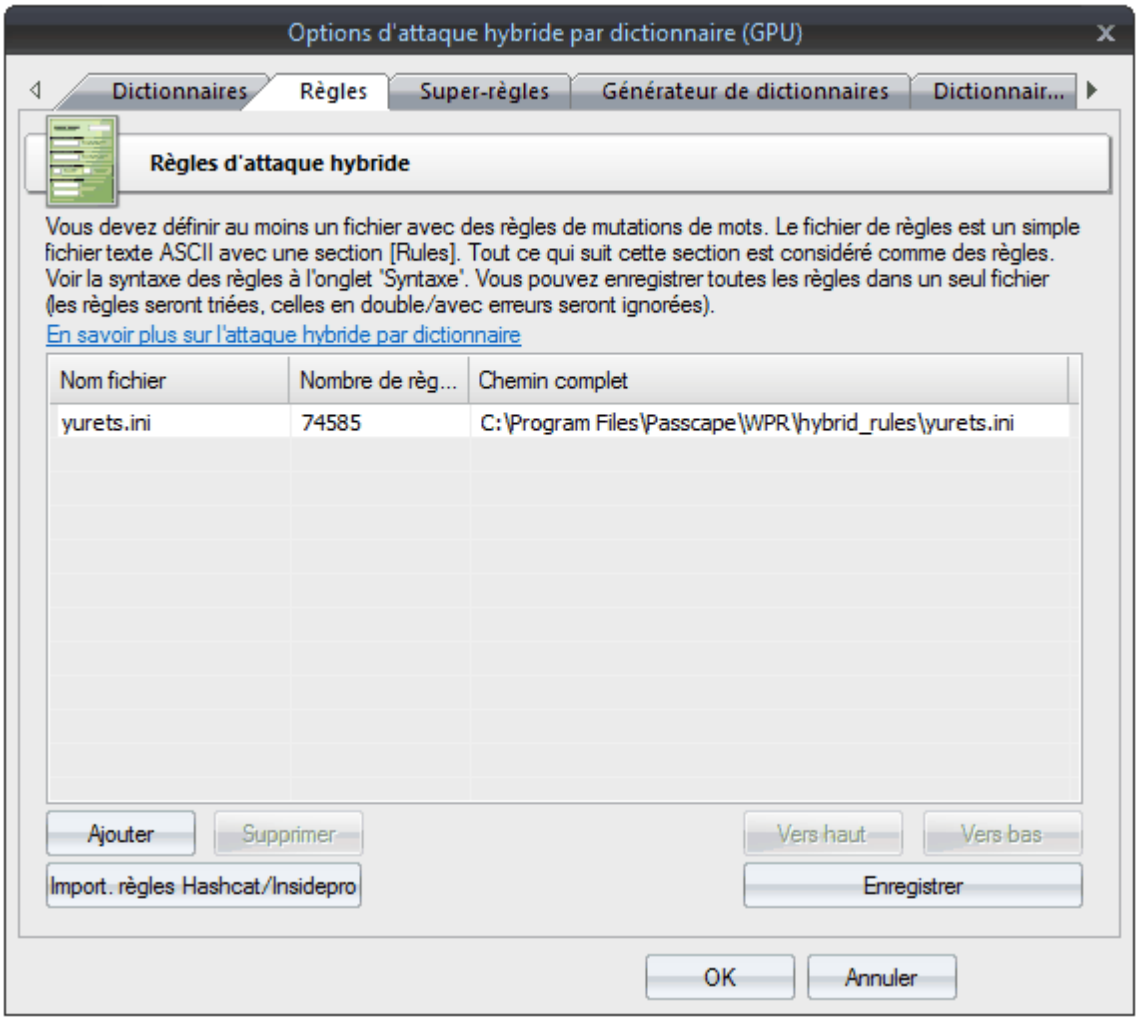
Les paramètres de l'attaque hybride par dictionnaire sont regroupés en 8 onglets:
1. **Dictionnaires** - pour le paramétrage des dictionnaires sources.
2. **Règles** - fichiers contenant les jeux de règles.
3. **Super-règles** - règles à appliquer par dessus les règles standard définies.
4. **Générateur de dictionnaires -** permets la création de fichiers de mots obtenu à partir de l'attaque hybride.
5. **Dictionnaires en ligne** - pour le téléchargement de nouveau dictionnaires pour le logiciel.
6. **Syntaxe hybride** - description complète de toutes les règles avec des exemples.
7. **Testeur de règles -** permets de tester vos règles.
8. **Paramètres GPU** - utilisé pour ajuster vos paramètres GPU.

Les listes de mots qui sont utilisées dans une attaque sont définies dans ce premier onglet. Traditionnellement, le logiciel supporte les listes de mots au format ASCII, UTF8, UNICODE, PCD, RAR et ZIP. La position des fichiers dans la liste peut être modifiée. Par exemple, vous pouvez déplacer les petits dictionnaires au début de la liste ou autrement. Pendant l'attaque, ils seront utilisés les uns après les autres, en fonction de leur position dans la liste.

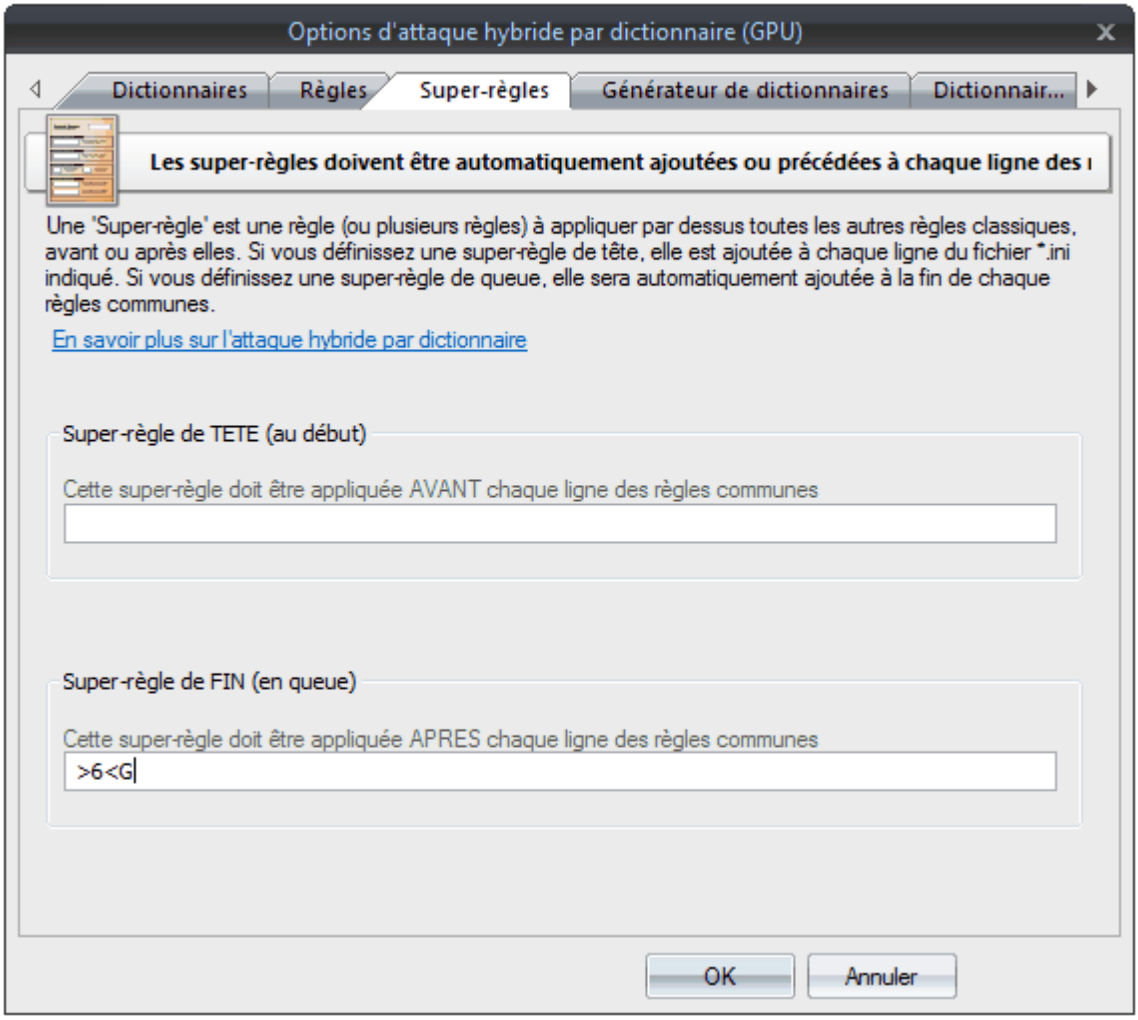


Dans l'onglet '**Règles**', vous devez définir au moins un fichier avec des règles de mutations de mots de passe. Le format du fichier de règles est quelque peu ordinaire; c'est un fichier texte ASCII contenant la chaîne '**[Rules]**'. Tout ce qui sera présent avant cette chaîne entre crochets sera considéré comme des commentaires et ignoré par le programme. Et tous ce qui sera après, donc, sera considéré comme des

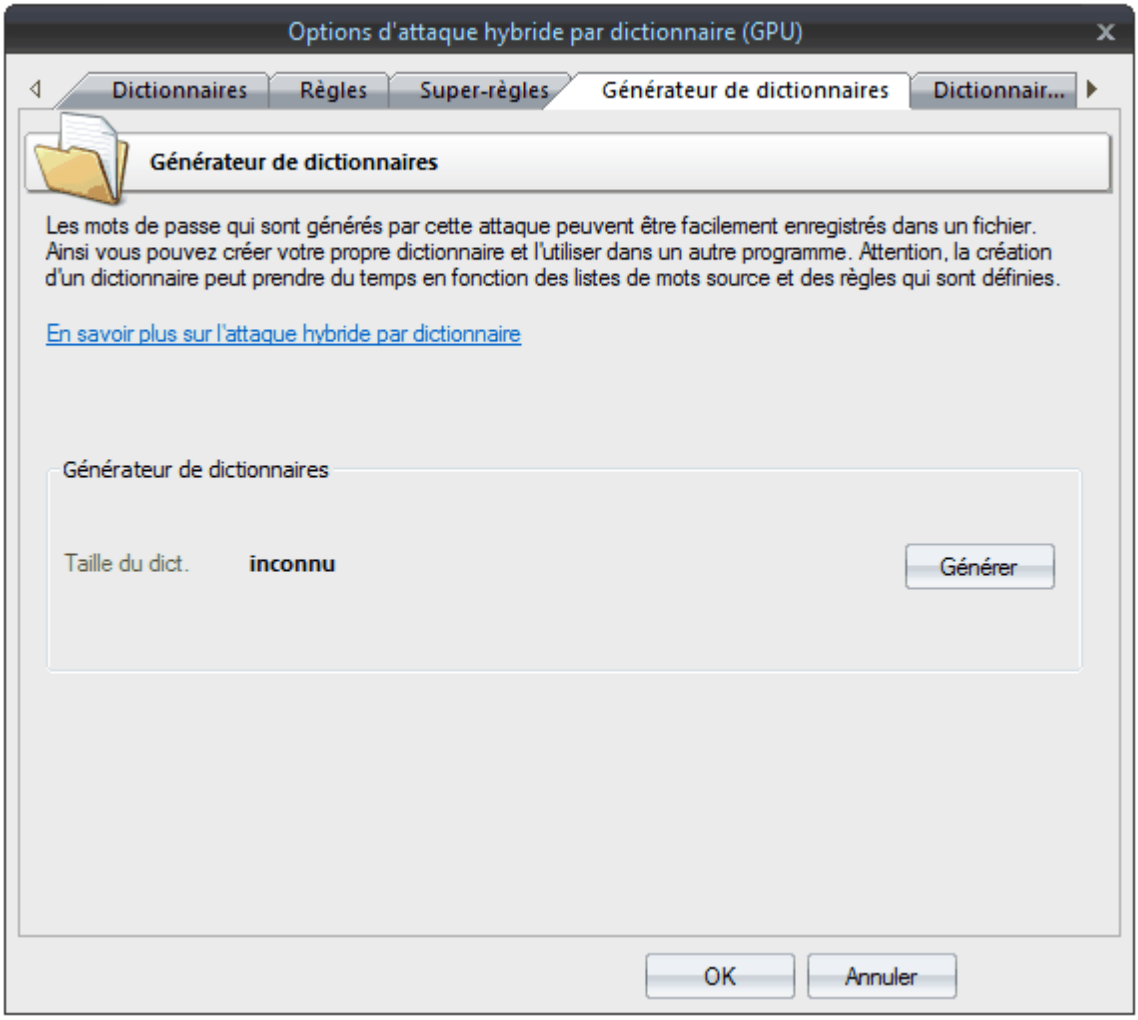
règles. Chaque chaînes peut contenir plusieurs règles, applicable au mot source. Si une chaîne contient plusieurs règles par mot, ces règles seront parcourues de gauche à droite. Par exemple, si vous appliquez la règle '@pc$a$b$c' au mot source 'password', après l'application de la règle vous obtiendrez 'Asswordabc'. La longueur maximum du mot en sortie ne peut excéder **256** caractères.



'**Super-règles**' est une règle (ou plusieurs) qui peuvent être appliqués avant ou après les dessus les règles classiques. Par exemple, vous pouvez définir une liste de super-règles 'a8' pour créer toutes les combinaisons possibles après que la mutation standard a été réalisée. Du coup, la règle '/asa4' du fichier l33t.ini deviendra '/asa4a8', '/csc(' deviendra '/csc(a8', etc. Comme cet autre exemple: définissez la règle en tête '>6<G' qui permets de sauter tous les mots de moins de 6 caractères ou plus de 16 caractères, avant de démarrer la mutation commune. Cette fonctionnalité est très utile une fois que l'on a décidé d'ajouter la même règle à toutes les lignes textes des fichiers *.ini sélectionnés. Il est du coup pas nécessaire de tous les modifier. Attention dans ce type d'utilisation, la super-règle 'aN' peut augmenter de manière importante le total de de mots de passe générés.

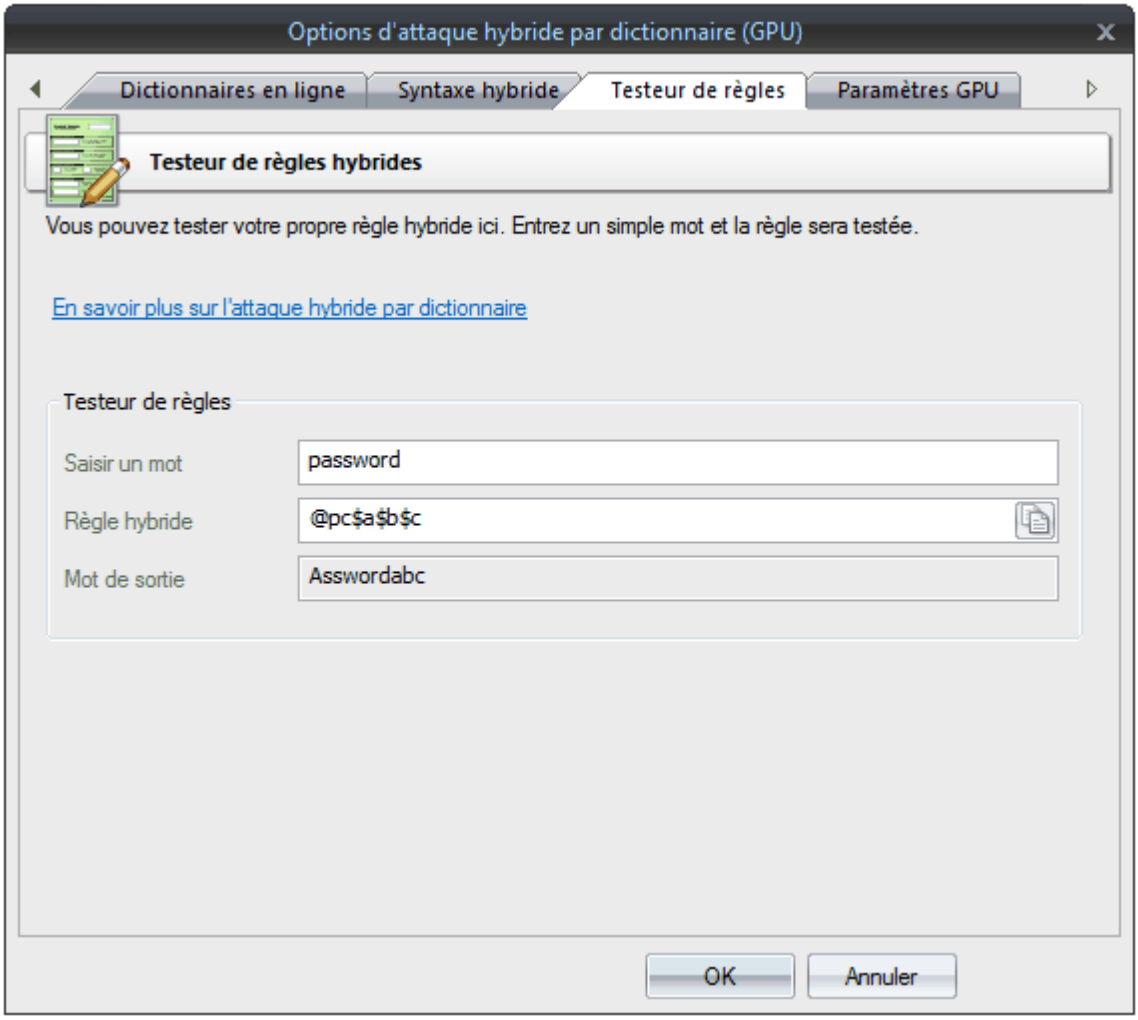


L'onglet '**Générateur de dictionnaires**' est conçu pour générer des dictionnaires obtenus à partir de l'attaque. Ces dictionnaires pourront être utilisés par exemple, dans d'autres applications. Pour générer un dictionnaire, sélectionnez un dictionnaire source et définissez les règles de mutations à lui appliquer. La taille du fichier créée pour le dictionnaire ne peut excéder 2 Go, si il est enregistré sur un disque formaté en NTFS.
Attention, la génération d'un dictionnaire peut prendre beaucoup de temps, et d'espace disque !



Vous pouvez télécharger des listes de mots complémentaires pour l'attaque en utilisant l'onglet '[Dictionnaires en ligne]'.

Si vous voulez créer vos propres jeux de règles, vous pouvez utiliser les deux derniers onglets comme sources d'aides. Alors que l'onglet '**Syntaxe hybride**' donne plus de détails sur les règles disponibles, dans le dernier onglet '**Testeur de règles**', vous pouvez les tester en indiquant un source mot spécifique et une règle. En retour, vous pouvez nous envoyer vos jeux de règles; si nous les trouvons intéressantes/ utiles, elles seront incluses par défaut dans le programme WPR.



Description des règles pour l'attaque hybride par dictionnaires

Plusieurs règles peuvent être définies par ligne.
Les règles (si elles sont multiples par ligne) sont exécutées de la gauche vers la droite.
La longueur maximum par ligne est limitée à **256** caractères.
La longueur maximum du mot de sortie est de **256** caractères.
Les espaces sont ignorés tant qu'ils ne sont pas utilisés comme paramètres.
Une ligne démarrant avec le caractère # est considérée comment un commentaire.
Tous les textes avant la ligne '**[Rules]**' sont considérés comme des commentaires.
N et M démarre toujours de 0 (zéro). Pour les valeurs supérieures à 9, utilisez les lettres A..Z (A=10, B=11, etc.).
Ne modifiez pas les noms des fichiers des règles standard (fournies avec le programme). Certains sont utilisés par le programme.
?iN[C], ?i[C], ?oN[C], ?o[C] ?iZ[C], ?oZ[C] Ces règles utilisent les jeux de caractères prédéfinis suivants (vous pouvez définir vos propres jeux de caractères personnalisés):

digits - 0123456789
loweralpha - abcdefghijklmnopqrstuvwxyz
upperalpha - ABCDEFGHIJKLMNOPQRSTUVWXYZ
alpha - abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ
special - !@#$%^&*()-_+=~`[]{}|\:;'"<>,.?/ "
loweralphanumeric - abcdefghijklmnopqrstuvwxyz0123456789
upperalphanumeric - ABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789
alphanumeric - abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789
printable - abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789!@#$%^&*()-_+=~`[]{}|\:;'"<>,.? /

Règles

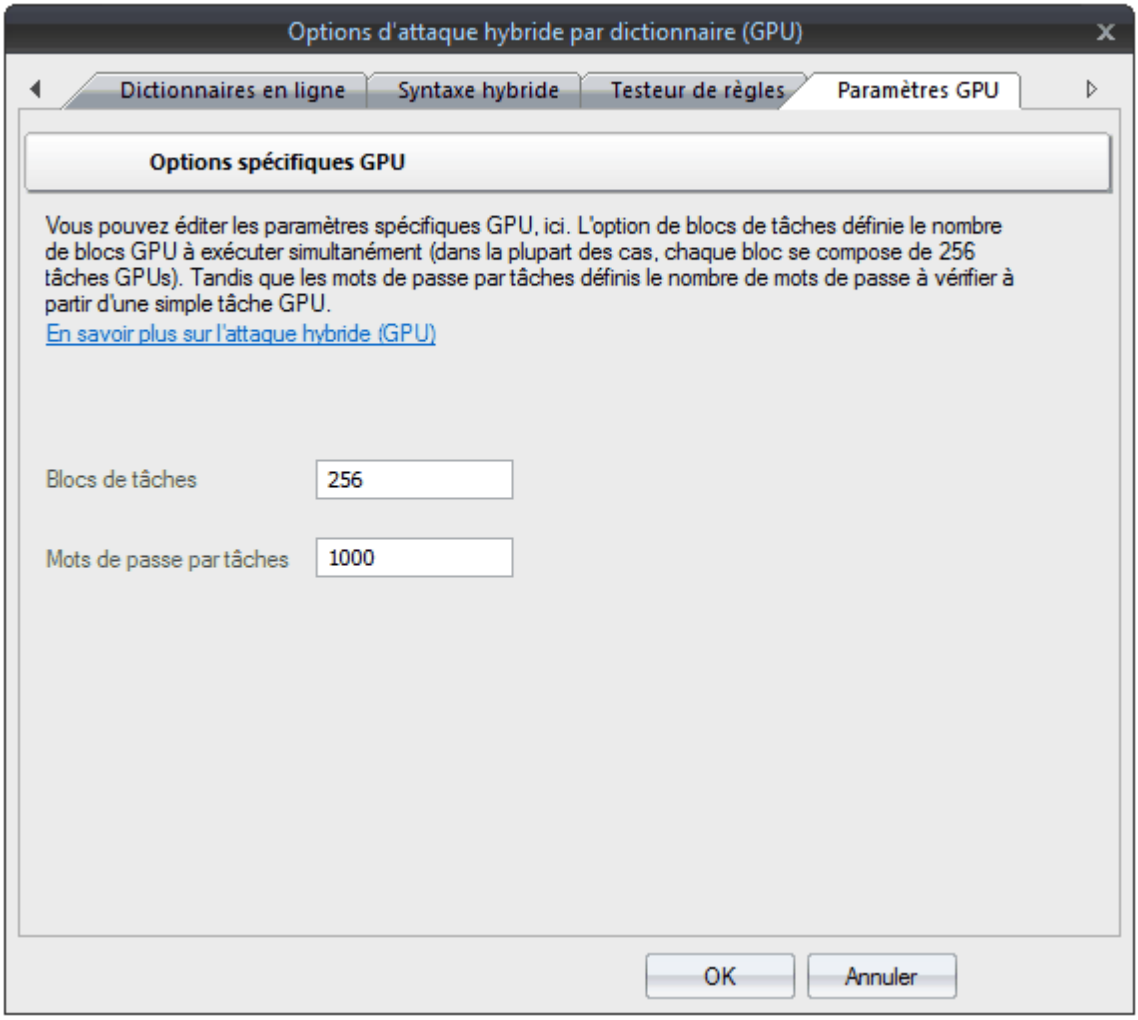
Règle	Exemple	Source	Sortie	Description
:	:	password	password	Ne modifie pas le mot source
{	{	password	asswordp	Retourner le mot vers la gauche
}	}	password	dpasswor	Retourner le mot vers la droite
[	[	password	assword	Supprimer le premier caractère
]	]	password	passwor	Supprimer le dernier caractère
c	c	password	Password	Mettre le la première lettre en majuscule
C	C	password	pASSWORD	Mettre en majuscule toute les lettres du mot sauf la première (minuscule pour le premier caractère, majuscule pour le reste du mot)
d	d	password	passwordpassword	Dupliquer le mot et l'ajouter à la fin du mot
f	f	password	passworddrowssap	Ajouter à la fin du mot le mot inversé (mot en reflet)
k	k	password пароль	зфыыцщквgfhjkm	Convertir le mot en utilisant un arrangement de clavier alternatif (le premier après celui par défaut). La règle fonctionne dans les deux directions. Par exemple, si un clavier Russe a été installé précédemment dans le système, la règle doit convertir le mot 'password' en Russe 'зфыыцщкв', et le mot Russe 'пароль' en 'gfhjkm'. Cette règle est très utile, lorsque vous recherchez des mots de passe non-Anglais. Si un seul langage est installé dans le système, la règle ne fera rien.
K	K	password	passwodr	Intervertir les deux derniers caractères
l	l	password	password	Convertir tous les caractères en minuscules
q	q	password	ppaasssswwoorrdd	Dupliquer tous les symboles
r	r	password	drowssap	Inverser le mot
t	t	PassWord	pASSwORD	Inverser la casse de tous les caractères
u	u	password	PASSWORD	Convertir tous les caractères en majuscules
U	U	my own password	My Own Password	Mets en majuscule toutes les premières lettres de chaque mots séparés par un espace (mets en majuscule tous les premier caractères après un espace)
V	V	password	PaSSWoRD	Mets en minuscule les voyelles et en majuscule les consonnes
v	v	password	pASSWoRD	Mets en majuscule les voyelles et en minuscule les consonnes
'N	'4	password	pass	Raccourci la longueur du mot de N caractère (s)
+N	+1	password	pbssword	Incrémente le caractère à la position N de 1 valeur ASCII
-N	-0	password	oassword	Décrémente le caractère à la position N de 1 valeur ASCII
.N	.4	password	passoord	Remplace le caractère à la position N avec le caractère de la position N +1
,N	,1	password	ppssword	Remplace le caractère à la position N avec le caractère à la position N-1. Où N > 0
<N				Ignore (saute) le mot si il est plus grand de N caractères de long
>N				Ignore (saute) le mot si il est moins grand que N caractères de long

Règle	Exemple	Source	Sortie	Description
aN				Test toutes les casses de symboles pour le mot. N est la longueur maximum du mot sur laquelle il faut appliquer la règle
DN	D2D2	password	paword	Supprimer le caractère à la position N
pN	p3	key	keykeykey	Copie le mot N fois
TN	T1T5	password	pAsswOrd	Inverse la casse avec le caractère à la position N
yN	y3	password	paspassword	Duplique le(s) N premier caractère(s)
YN	Y3	password	paswordord	Duplique le(s) N dernier caractère(s)
zN	z3	password	ppppassword	Duplique le premier caractère du mot N fois
ZN	Z3	password	passworddd	Duplique le dernier caractère du mot N fois
$X	$0$0$7	password	password007	Ajoute X caractère(s) à la fin du mot
^X	^3^2^1	password	123password	Insère X caractère(s) au début du mot
@X	@s	password	paword	Supprime tous les caractères X du mot
!X				Ignore (saute) si il contient au moins un caractère X
/X				Ignore (saute) si il ne contient pas de caractères X
(X				Ignore (saute) si il le premier caractère n'est pas X
)X				Ignore (saute) le mot si le premier caractère n'est pas un X
eX	e@	mike@yahoo.com	mike	Extrait une sous-chaîne à la position 0 et se terminant avant le premier caractère X (ne fait rien si X n'est pas trouvé)
EX	E@e.	mike@yahoo.com	yahoo	Extrait une sous-chaîne démarrant à droite après le premier caractère X trouvé et jusqu'à la fin de la chaîne (ne fait rien si X n'est pas trouvé)
%MX				Ignore (saute) le mot si il ne contient pas au moins M fois le caractère X
***XY**	*15	password	possward	Interverti les caractères à la position X et Y
=NX				Ignore (saute) le mot si le caractère à la position N n'est pas identique à X
iNX	i4ai5bi6c	password	passabcword	Insère le caractère X à la position N
oNX	o4*o5*	password	pass**rd	Écrase le caractère à la position N avec le caractère X
sXY	ss$so0	password	pa$$w0rd	Remplace tous les caractères X avec Y
xNM	x4Z	password	word	Extrait la sous-chaîne jusqu'à une longueur de M caractères, en démarrant d la position N
INX-Y	rl0/-/r	google.com	google.com/	Insère le caractère X à la position N si le caractère précédent à la position N n'est pas Y
INX+Y	rl0.+.r	password.	password..	Insère le caractère X à la position N si le précédent caractère à la position N est Y
ONX-Y	O0-+p	password	-assword	Si le caractère à la position N n'est pas Y, il sera écrasé par le caractère X
ONX+Y	O0P+p	password	Password	Si le caractère à la position N est Y, il sera écrasé par le caractère X
RNM+Y	R01+a	password	assword	Supprime le caractère à la position N si le caractère à la position M est Y
RNM	R40-b	password	passord	Supprime le caractère à la position N si le caractère à la position M n'est

Règle	Exemple	Source	Sortie	Description
-Y		rd		pas Y
?iN [C]	?i0 [digits]	password	0password, 1password ... 9password	Insère un caractère à partir du jeu de caractère [C] à la position N du mot. [C] étant soit un nom de jeu de caractères prédéfini ou un jeu de caractères personnalisés.
?iZ [C]	?iZ [digits]	password	password0, password1 ... password9	Insère un caractère à partir du jeu de caractères [C] à la dernière position du mot. [C] étant soit un nom de jeu de caractères prédéfini ou un jeu de caractères personnalisés.
?i[C]	?i [special]	password	~password, !password ... password_, password+	Insère un caractère à partir du jeu de caractères [C] à toutes les positions du mot. [C] étant soit un nom de jeu de caractères prédéfini ou un jeu de caractères personnalisés.
?oN [C]	?o1 [upper alpha]	password	pAssword, pBssword ... pZssword	Remplace un caractère à la position N par un caractère provenant du jeu de caractères [C]. [C] étant soit un nom de jeu de caractères prédéfini ou un jeu de caractères personnalisés.
?oZ [C]	?oZ [upper alpha]	password	passworA, passworB ... passworZ	Remplace le caractère à la dernière position du mot par un caractère provenant du jeu de caractères [C]. [C] étant soit un nom de jeu de caractères prédéfini ou un jeu de caractères personnalisés.
?o [C]	?o[-=.]	password	-assword, =assword ... passwor.	Remplace le caractère à toutes les positions du mot par un caractère provenant d'un jeu de caractères [C].

Paramètres GPU

Avant de lancer une attaque, assurez-vous de configurer les paramètres GPU correctement.



Le paramétrage du GPU est assez simple et se compose de deux paramètres:

1. Le nombre de blocs GPU à exécuter pour un simple appel au GPU. Chaque bloc est constitué de 256 tâches. Ainsi, si vous définissez le nombre de blocs à 256, le GPU exécutera 256 * 256 = 65536 tâches. Le nombre total de mots de passe testés pour un appel au noyau GPU sera 256*Blocs de tâches*TâchesParMotdePasse. Dans notre cas 256 * 256 * 1000 = 65 536 000 mots de passe.
2. Le nombre de mots de passe a rechercher pour une simple tâches GPU. Plus grande est la valeur, plus le nombre de tâches sera faible, et du coup la vitesse de recherche importante. Cependant, une trop grande valeur peut bloquer l'ordinateur, le GPU ou provoquer d'importantes fluctuations de la vitesse de recherche en cours. Ce nombre est affichée sur l'onglet d'état de l'attaque. Ceci est provoqué par le fait que le temps d'achèvement de la tâche sur le GPU est supérieure au temps nécessaire pour l'actualisation de l'état actuel de l'attaque.

Attention, lors du paramétrage des règles 'lourdes' comme aN, ?iN, ?oN, etc. Ces règles peuvent augmenter plus de 100 fois le nombre de mots de passe générés et bloquer le système ou que votre carte GPU ne réponde plus 'freeze'.

2.9 Menu Afficher

Le menu '***Afficher***' active/désactive les éléments complémentaires de l'interface, change la langue du logiciel, réduit l'application dans la barre de notification de Windows ou exécute le programme en mode invisible.

2.10 Menu Thèmes

Vous pouvez choisir ici les thèmes que vous aimez ou créer le votre.

2.11 Menu d'aide

Dans cette partie du menu, vous pouvez accéder aux articles d'aide sur l'utilisation du logiciel. Visitez également la page Web du programme, pour vérifier la disponible de mises à jour, soumettre un rapport d'erreur (bug), acheter une licence pour Windows Password Recovery, etc.

2.12 Moniteur système (matériel)

Dans ce onglet, vous pouvez visualiser la charge CPU, l'utilisation de la RAM, la température et la charge GPU. Par défaut, l'intervalle de rafraîchissement est de 2 secondes. Attention: la collecte de ces statistiques prends aussi du temps CPU; du coup, lors de l'exécution d'attaque "lourde", comme l'attaque par Force-brute, il est recommandé de désactiver le moniteur système.

Comment utiliser le programme

3 Comment utiliser le programme

3.1 Attaque des hachages Windows

Actuellement, le programme peut décrypter les hachages Windows à l'aide différentes attaques:

Attaque Préliminaire (développée par Passcape Software) basée sur une méthode d'ingénierie sociale et composée de plusieurs sous attaques. L'attaque préliminaire est très rapide et est souvent utilisée pour deviner les mots de passe simples et courts quand il n'y a pas besoin de lancer une attaque entièrement évolutive.

Attaque par Intelligence artificielle - Est un tout nouveau type d'attaque développée par notre entreprise Passcape. Elle est basée sur une méthode d'ingénierie sociale et permet, sans avoir recours à du temps et des calculs coûteux, de presque instantanément et sans difficulté, de récupérer certains des mots de passe.

Attaque par Dictionnaire - C'est la méthode la plus efficace de récupération, lorsque le programme tente chaque mot du dictionnaire (ou dictionnaires si il y en a plusieurs) choisi jusqu'à ce qu'il trouve le mot de passe d'origine ou jusqu'à ce que la liste de mots arrive à la fin. Cette méthode est très efficace car beaucoup de gens utilisent des mots ou des expressions habituelles pour le mot de passe. En outre, ce type de récupération est effectuée assez rapidement par rapport à l'attaque par Force-brute, par exemple. Des dictionnaires supplémentaires et listes de mots peuvent être téléchargés à partir de notre site ou peuvent être commandés sur CDs.

Attaque par Force-brute - Elle teste toutes les combinaisons possibles de la plage de caractères spécifiée. Par exemple, pour une plage de trois caractères Latin en minuscules, le programme va vérifier toutes les combinaisons possibles, en commençant par «AAA», «AAB», «aac», et ainsi de suite jusqu'à «zzz». Cette attaque est la plus lente, et idéale pour les mots de passe courts.

Attaque par Masque - C'est une variante de l'attaque par Force-brute, sauf que certains caractères pour trouver le mot de passe restent inchangés, et seule une partie du mot de passe peut changer. Une syntaxe spéciale est utilisée pour paramétrer le masque ou la règle pour trouver un mot de passe.

Attaque à Base de mots (développée par Passcape) - Au premier coup d'œil, ce type d'attaque rappelle celle que nous venons de décrire. elle est tout aussi efficace si une partie du mot de passe à récupérer est connue. Cependant, contrairement à l'attaque précédente, ici, vous ne devez pas définir un masque - juste fournir juste un mot de base. Le programme se chargera du reste. L'attaque par phrase est basée sur l'expérience en ingénierie sociale pour générer un grand nombre de combinaisons possibles pour le mot de passe.

Attaque par Dictionnaires combinés (développée par Passcape) - Elle est utilisée pour trouver des mots de passe composés. Par exemple, 'nothingtodo' ou 'je renonce'. Elle est très similaire à l'attaque par dictionnaire, sauf qu'au lieu d'utiliser un seul mot pour la vérification de mots de passe, elle utilise une combinaison de mots créés en combinant des mots de plusieurs dictionnaires. Vous pouvez créer vos propres règles de génération de mots de passe.

Attaque par Phrase (développée par Passcape) - Elle est très efficace contre les mots de passe complexes. L'idée est de deviner le bon mot de passe en recherchant des phrases et des combinaisons fréquemment utilisées. Vous pouvez télécharger des listes de mots composées de phrases de mots de passe et des dictionnaires sur notre site Web.

Attaque Rainbow (développée par Philippe Oechslin) - Elle est un compromis temps/mémoire utilisée dans la récupération de mots de passe testés à partir de hachages. Cette attaque est un outil assez rapide et efficace pour la vérification des hachages Windows.

Attaque par Empreintes (développée par Passcape), suivant l'idée originale de Atom - L'attaque analyse la liste de mots pour générer des «empreintes» utilisées pour récupérer le mot de passe. L'attaque est très efficace dans la recherche de mots de passe difficiles pour de grandes listes de hachages ou pour les hachages d'historiques de mots de passe.

Attaque hybride par Dictionnaire - Identique a une attaque simple par dictionnaire, mais permet à l'utilisateur de personnaliser la mutation du mot et de définir ses propres règles de mutations de mots de passe. La syntaxe de définition des règles est compatible avec d'autres logiciels de récupération de mots de passe.

Récupération en Ligne (développée par Passcape Software). Elle permets la recherche de mots de passe dans les bases de données d'Internet. Elle traite assez bien les mots de passe simples et fréquemment utilisés. Son inconvénient est son assez faible vitesse de traitement et sa mauvaise aptitude à la manipulation de grandes listes de hachages.

Attaque Rainbow table Passcape (développée par Passcape Software). Elle est la prochaine génération de tables pré-calculées. L'attaque par tables Passcape est la plus appropriée pour la récupération des mots de passe complexes de longueurs littéralement illimités.

Attaque par Lots (Batch) (développée par Passcape Software). Elle crée une liste/un lot d'attaques à exécuter une par une, de sorte que vous pouvez lancer toutes ces attaques en un seul clic de souris au lieu de configurer chacune d'elle individuellement.

Attaque GPU par Force-brute - Elle est complètement identique à une simple attaque par Force-brute, sauf que pour deviner les mots de passe, elle utilise le GPU de la carte vidéo au lieu du CPU. Pour qu'un périphérique GPU puisse être utilisé pour une attaque, vous devez le sélectionner dans les '**Options générales**'.

Attaque GPU par Empreintes - Elle fonctionne exactement de la même manière que la simple attaque par empreinte mais utilise la puissance du GPU.

Attaque GPU par Masque - Cette méthode de récupération de mots de passe est entièrement identique à l'attaque par masque standard, sauf que le mot de passe à deviner est traitée par une carte graphique de votre PC, donc la vitesse de récupération est beaucoup plus élevée.

Attaque GPU par Dictionnaire/Force-brute. Souvent, lors de la création de mots de passe, les utilisateurs ajoutent certains symboles au début, à la fin ou même au milieu du mot. Pour récupérer les mots de passe de ce type, on utilise l'attaque GPU par Dictionnaire-Brute force.

Attaque GPU hybride par Dictionnaires. Identique à l'attaque hybride par dictionnaire mais beaucoup plus rapide puisqu'elle utilise pour les calculs le GPU.

3.2 Tableau de comparaisons des attaques

Quelle attaque est la meilleure ? Comment choisir le type d'attaque? Les réponses à ces questions peuvent être trouvées dans le tableau de comparaisons d'attaques, ci-dessous:

Attaque	Description	Temps nécessaire	Résultat Garanti	Les plus	Les moins	Limitations
Préliminaire	Un ensemble de mini-attaques légères et rapides pour trouver des combinaisons simples, courtes ou communes.	Quelques minutes	Non	Excellent outil rapide pour une récupération rapide des mots de passe communs, simples, de courtes combinaisons de touches, les séquences répétitives, etc.	Pratiquement inutile pour une analyse sérieuse, lors de la récupération de la majorité des mots de passe complexes.	Adaptée principalement à récupération des mots de passe simples.

				Efficace pour trouver rapidement des mots de passe faibles; ne nécessite pas de réglages supplémentaires.		
Intelligence Artificielle	La façon la plus avancée pour la récupération des mots de passe, sur la base des méthodes d'ingénierie sociale.	Min: 2-3 minutes, Max: plus d'une heure	Non	Le meilleur outil pour trouver des mots de passe complexes, face aux autres méthodes qui ne peuvent pas faire face. Fonctionne très bien pour les mots de passe, des mots et des combinaisons que l'utilisateur a stocké précédemment dans le système à tout moment.	Avec une analyse la plus efficace possible, lorsque toutes les options sont réglées sur les performances maximales, l'attaque prendra un temps considérable. N'est pas capable de trouver tous les mots de passe.	Efficace uniquement lorsque l'attaque est exécutée sur le système d'origine (d'où les mots de passe sont extraits).
Force-brute	Recherche toutes les combinaisons possibles au sein d'un jeu de caractères spécifique.	Dépend des options	Oui	La seule attaque (avec l'attaque par masque) qui est garantie de récupérer un mot de passe totalement inconnu. Adaptée pour les mots de passe courts et d'une longueur moyenne.	La recherche de longs mots de passe prends beaucoup de temps. Il est difficile de deviner la bonne plage de caractères à rechercher.	La recherche peut prendre des siècles pour les longs mots de passe. Elle ne permets pas de trouver les mots de passe lorsque qu'on utilise un mauvais jeu de caractères ou que la longueur du mot de passe dépasse celle spécifiée.
Dictionnaire	Trouve le mot de passe en recherchant des mots venant de dictionnaires	Presque instantanément	Non	Bon outil et rapide pour la récupération de mots de	Nécessite d'avoir de bons dictionnaires, ne prends pas en compte les particularités	Trouve uniquement les mots de passe

	prédéfinis (listes de mots)			passe ordinaires.	de la casse de la langue.	ordinaires.
Dictionnaire avec mutations intelligentes	Identique à l'attaque par dictionnaire, sauf que ici, chaque mot du dictionnaire subit toutes sortes de mutations. Par exemple, l'ajout de chiffres, modification de la casse, déformation (déplacer) des lettres, etc.	Jusqu'à 1000000 fois plus lent qu'une simple attaque par dictionnaire.	Non	Efficace pour toutes les sortes de variations de mots de passe ordinaires.	La mutation maximum (la plus efficace) prends beaucoup de temps.	Échoue lors de la recherche de mots de passe forts, la mutation prends un temps considérable.
Masque	Trouve les mots de passe avec un masque (règle de génération des mots de passe)	Dépend des options	Oui	Garanti de récupérer la partie restante d'un mot de passe. Bonne option lorsque une partie du mot de passe d'origine est connue.	Nécessite d'avoir la partie connue exacte pour le mot de passe et sa longueur. Et d'indiquer le bon jeu de caractère à rechercher.	Le mot de passe ne sera pas trouvée si un mauvais jeu de caractères est choisi. Si la longueur ou une partie connue est incorrecte du mot de passe.
Dictionnaires combinés	Vérifie les mots de passe complexes (composés de deux ou plusieurs mots) en collant les mots de plusieurs dictionnaires.	Dépend des options	Non	La seule attaque qui trouve les mots de passe longs et complexes.	Jeu limité de dictionnaires spécifiques, qui ne prend pas en compte les particularités de mots de passe non-anglais (terminaisons, des suffixes, etc.). Avec un grand dictionnaire source, l'attaque peut prendre un temps considérable.	Nécessite de connaître à l'avance le mot de passe a rechercher composé de deux ou plusieurs mots; relativement lent.
Dictionnaires combinés avec mutations	Identique à l'attaque	Dépend des options	Non	Identique à l'attaque	Identique à l'attaque	Identique à l'attaque

intelligentes	combinée, avec en plus les mutations.			précédente.	précédente. Nécessite de définir des règles de mutations complémentaires pour les mots de passe à générer.	précédente; les mutations nécessite un temps considérable.
A base de mots	Profite d'un mot de base connu, utilisé pour la fabrication du mot de passe.	Quelques secondes si la longueur du mot de base n'est pas supérieure à 16 caractères.	Non	Bon pour les cas où vous connaissiez le mot de passe d'origine, mais vous avez oublié ses variations, par exemple, la casse des lettres ou des suites de nombres.	Mutation de longs mots de passe (supérieurs à 16 caractères); peut prendre un temps considérable.	Ne fonctionne pas toujours.
Phrase	Identique à l'attaque par dictionnaire, sauf qu'au lieu de vérifier avec un mot l'attaque utilise une phrase, une expression populaire, des extraits de chansons, livres, etc.	De plusieurs minutes jusqu'à plusieurs heures.	Non	La seule attaque contre les mots de passe de phrases.	Seul un petit pourcentage d'utilisateurs emploient des mots de passe de phrases comme mots de passe. La mutation de phrases n'est pas parfaite; la mutation et l'analyse prennent un temps considérable. Un nombre insuffisant de dictionnaires pertinents; en particulier, avec des phrases non-anglaises et des expressions.	Ne prend pas en compte les particularités de la langue; choix limité de mutations. Difficulté dans la création de dictionnaires spécialisés.
Rainbow tables	Utilise des tables pré-calculées.	Habituellement plusieurs minutes (voire quelques secondes) pour chaque mot de passe.	Jusqu'à 100% si le mot de passe convient au jeu de caractères et à la longueur mot de passe de la table (s).	Actuellement, l'une des meilleurs attaque pour récupérer la majorité des mots de passe avec un rapport temps/ coefficient d'efficacité.	Nécessite des tables. Le pré-calcul des tables peut prendre beaucoup de place sur un disque dur. Il est impossible de récupérer de longs mots	Ne peut pas récupérer tous les mots de passe simultanément; la génération d'une nouvelle table prend plus de temps que de d'exécuter une

					de passe en utilisant cette attaque..	attaque par Force-brute. Capacités limitées de récupération des mots de passe longs et non-Anglais.
Empreinte	Basée sur les empreintes qui ont été générés en dehors de la liste de mots fournie.	De plusieurs heures à plusieurs jours (dépend du dictionnaire initial).	Non	Trouve les mots de passe complexes qui étaient impossibles à récupérer dans d'autres attaques.	Les grands dictionnaires peuvent générer beaucoup trop d'empreintes. Le succès dépend du dictionnaire d'entrée.	L'attaque prend trop de temps pour terminer lorsque vous définissez une grande liste de mots d'entrée..
Dictionnaire hybride	Elle est très semblable à une simple attaque par dictionnaire, sauf que les règles de mutation de mots de passe sont entièrement personnalisables et doivent être réglées par l'utilisateur.	Dépend de la liste de mots sources et du total de règles. Habituellement jusqu'à plusieurs minutes pour une petite liste de mots.	Non	Bon pour toutes sortes de variations de mots de passe ordinaires.	Ne peut pas récupérer des mots de passe complexes.	Échoue lors de la recherche de mots de passe forts (non-dictionnaire).
Récupération en ligne	Recherche les mots de passe via Internet.	Dépend des options définies et de la vitesse de connexion Internet. Habituellement, moins de 1 minute pour un seul hachage.	Non	Très bel outil alternatif pour trouver les mots de passe simples et fréquemment utilisés.	Traitement des hachages très lent, qui produit beaucoup de trafics Internet.	Échoue lors de la recherche de la plupart des mots de passe forts. Ne fonctionne que lorsqu'une connexion Internet est disponible.
rainbow tables Passcape	Utilise les tables spécialement pré-calculées pour deviner des mots de passe forts et complexes.	Plusieurs minutes (voire quelques secondes) pour chaque mot de passe, en fonction des paramètres de table.	Non	En fait, c'est une très bonne et avancée attaque pour récupérer des mots de passe forts et complexes qui ne peuvent être 'crackés' dans d'autres attaques.	Une bonne table pré-calculée peut prendre beaucoup d'espace disque et de temps. Le taux de succès de récupération de mots de passe dépend grandement d'une liste de mots.	Ne peut pas récupérer tous les mots de passe en même temps; la génération d'une nouvelle table prend plus de temps que d'exécuter une attaque par Force-brute. Toutes les listes de mots initiales ne conviennent pas bien pour

la création de tables Passcape.

3.3 Récupération de mots de passe de hachages

Utilisez ces simples instructions pour la récupération des mots de passe dans les programmes Passcape. Ces instructions sont offertes sous la forme de recommandations et sont destinées principalement pour la récupération des mots de passe cryptés avec OWF; par exemple, à partir de hachages Windows.

Lors de la récupération de certains types de mots de passe la grande question est: Comment organiser le processus de récupération - par quelle attaque je devrais commencer pour augmenter la probabilité de réussite ?

Pour choisir le type et la séquence des attaques, nous vous conseillons de suivre cet algorithme, qui est applicable dans la majorité des cas à tous les types de mots de passe à récupérer:

Tout d'abord, activez l'option d'attaque préliminaire, si elle est disponible. Il vous aidera à récupérer des combinaisons simples et fréquemment utilisés.

Deuxièmement, sélectionnez un ou plusieurs mots de passe que vous devez tout d'abord décrypter et ensuite, exécuter la récupération en ligne pour trouver les mots de passe simples et fréquemment utilisés.

Troisièmement, si vous êtes au courant de toutes les spécificités du mot de passe que vous cherchez, il est préférable d'essayer l'attaque par masque ou à base de mots en premier. Plus précisément, si vous connaissez une partie du mot de passe - utilisez une attaque par masque qui sera plus efficace. Si vous connaissez la partie principale du mot de passe ou, par exemple, vous connaissez le mot de passe mais sans vous souvenir de la séquence des caractères en majuscules et minuscules, l'attaque à base de mots devrait permettre de mieux faire ce travail.

Quatrièmement, si vous n'avez pas d'informations sur le mot de passe que vous cherchez, ce qui se produit le plus souvent, suivez ce guide avec les étapes décrites suivantes:

1. Lancer l'attaque par Intelligence Artificielle avec les options de mutation et d'indexation réglées au niveau '*léger*'.
2. Si le mot de passe n'est pas trouvé, essayer à nouveau l'option de mutation réglée sur le niveau '*normal*' et l'indexation sur '*En profondeur*'.
3. Exécuter une attaque par rainbow table si il n'y a aucune table.
4. Démarrer l'attaque par rainbow table Passcape.
5. Exécuter l'attaque par dictionnaire avec l'option de mutation désactivée.
6. Lancer l'attaque par dictionnaire avec l'option de mutation activée; la profondeur de de la mutation dépend du temps disponible et la vitesse d'attaque. Lors de la recherche de mots de passe saisi avec un clavier avec un arrangement de touches national (layout), la profondeur de la mutation doit être réglé à '*Fort*'.
7. Sélectionner et télécharger les dictionnaires en ligne, puis répéter les étapes 5 - 6.
8. Exécuter l'attaque par dictionnaire hybride.
9. Répéter l'attaque hybride en utilisant les listes de mots alternatives.
10. Lancer l'attaque par phrase de mots de passe avec l'option de mutation désactivée.
11. Lancer l'attaque par phrase de mots de passe avec l'option de mutation activée et réglée sur le maximum de productivité. Cela permettra de trouver même les mots de passe saisis avec des arrangement de clavier nationaux (layout).
12. Sélectionner et télécharger les dictionnaires de phrase de mots de passe en ligne, puis répéter les étapes 10 - 11.
13. Lancer l'attaque par dictionnaire combiné avec les règles de génération de phrases définies.
14. Sélectionner et télécharger les dictionnaires en ligne pour l'attaque combinée, puis répéter l'étape 13.

15.Exécuter l'attaque par empreinte avec le dictionnaire par défaut.
16.Sélectionner et télécharger le nouveau dictionnaire en ligne pour l'attaque par empreinte, ajuster les options, définissez le nouveau dictionnaire et répéter l'étape 15.
17.Sélectionner un jeu de caractères et la longueur du mot de passe pour l'attaque par Force-brute, puis lancer l'attaque.
18.Si nécessaire, sélectionner un nouveau ou compléter l'ancien jeu de caractères, puis répéter l'attaque par force-brute; par exemple l'étape 17.

Sur la base de ces recommandations, il est facile de créer vos propres règles pour l'attaque par lots (batch).

3.4 FAQ - Mots de passe Windows

Q. Qu'est ce qu'une protection par mot de passe?
R. Peut-être que personne ne contestera, que les systèmes d'exploitation basés sur Windows NT, sont aujourd'hui les plus populaires partout dans le monde. Cela fait d'eux des cibles très vulnérables pour divers types de pirates, les intrus et les utilisateurs malhonnêtes. La propagation du réseau mondial ne fait qu'aggraver la situation. Pour s'assurer que les données personnalisées de l'utilisateur ou du système sont stockées et protégées contre les accès non autorisés par des tiers, il a été proposé d'utiliser la technologie de protection par mot de passe. Actuellement, la protection principale dans les systèmes d'exploitation Windows est la protection par mot de passe. L'accès aux données privées dans ce cas est possible uniquement lorsque l'utilisateur connaît le mot de passe original, qui est normalement un mot ou une phrase. Voici à quoi cela ressemble dans la vie réelle: le programme ou le système, sur une tentative d'accès à des données privées, demande à l'utilisateur des mots de passe texte. Ce mot de passe est vérifié avec le mot de passe original, et, si les valeurs correspondent, le système permet l'accès aux données privées; sinon, il refuse l'accès. Le principal inconvénient de la protection par mot de passe est que le programme ou le système doivent stocker le mot de passe original quelque part, afin d'avoir quelque chose à comparer avec la valeur saisie.

Q. Comment les systèmes d'exploitation stockent les mots de passe ?
R. Mais tout n'est pas si mal; Windows NT a été développé d'une manière a ne pas stocker la valeur du texte original du mot de passe. "Comment ça ?" Vous demandez vous ? - Très facile. Il existe des algorithmes de passe cryptographiques spéciaux qui travaillent dans un seul sens. Voilà pourquoi parfois ils sont appelés OWF - fonctions à sens unique. En gros, vous pouvez obtenir le hachage du mot de passe, mais il n'y a aucun moyen d'obtenir le mot de passe d'un hachage. Comment ça marche dans Windows? Lors de la création d'un compte, l'utilisateur entre le mot de passe d'origine, qui, cependant, n'est pas stocké sous forme de texte; à la place, il est haché avec une fonction OWF. Le hachage retourné par la fonction sera stocké dans le système. En outre, lors de la tentative de connexion, le système demandera à l'utilisateur le mot de passe; il hache le mot de passe de nouveau et ensuite compare la valeur de hachage générée par l'original qui est stocké dans le système. Si les deux valeurs correspondent, les mots de passe, naturellement, correspondent aussi. Ainsi, le mot de texte d'origine n'est pas stocké dans le système. En outre, il y a de nouveaux algorithmes qui ne stockent même pas le hachage, et leur nombre de ces algorithmes ne cesse de croître. Un algorithme de ce genre, par exemple, est utilisé pour chiffrer les mots de passe dans Internet Explorer 7-8. Vous pouvez en apprendre plus à ce sujet dans dans notre article.

Q. Comment les mots de passe sont cryptés ?
R. Pour le hachage de mots de passe utilisateur, Windows NT utilise deux algorithmes: LM, que nous avons héritées de réseaux LAN Manager, qui est basé sur une simple conversion DES, et NT, basés sur la fonction de hachage MD4. Les hachages LM, les plus faibles et vulnérables, ne sont pas pris en charge par défaut par la dernière version de Windows Vista et Windows 7; Cependant, vous pouvez toujours l'activer. En outre, il existe une tendance à les éliminer complètement ou de les remplacer. Il est important de savoir que lorsque l'option de hachage LM est activée (elle est activée par défaut dans Windows XP), tous les mots de passe d'utilisateurs sont considérées comme très vulnérables. 'Cracker' la majorité de ces mots de passe prend normalement quelques minutes. Le hachage NT ne possède pas ces inconvénients, communs au hachage LM. Par conséquent, il est beaucoup plus difficile de choisir le bon mot de passe pour un hachage NT connu que pour un hachage LM. Mais la tendance actuelle de l'augmentation de la puissance de calcul des ordinateurs modernes, en

particulier lors de l'utilisation GPU, rendra éventuellement ce standard trop vulnérable pour les attaques potentielles

Q. Où sont les hachages de mots de passe sont stockés ?

R. Donc, nous avons découvert que les mots de passe de l'utilisateur dans les systèmes Windows sont convertis en valeurs spéciales - hachages. Les hachages LM et NT ont tous les deux une taille fixe - 16 octets - et peuvent être stockés dans deux lieux de stockages: SAM - pour les comptes classiques et Active Directory - pour les comptes de domaine.

SAM: Les comptes classiques qui contiennent le nom d'utilisateur, le mot de passe et d'autres informations complémentaires sont stockés dans la base de registre de Windows NT; précisément, dans le fichier SAM (Security Account Manager). Ce fichier se trouve sur le disque dur, dans le répertoire % windows%\system32\config. Le %windows% représente le chemin d'accès de votre dossier Windows. Par exemple, C:\Windows\System32\Config\SAM. Le systeme dispose d'un acces prioritaire au fichier SAM, du coup l'accès au fichier est refusé à toute personne, même les administrateurs, lorsque que le système a une charge importante; Néanmoins, Windows Password Recovery contourne cette restriction avec facilité. De plus, un grand intérêt pour un attaquant potentiel serait la sauvegarde du fichier de SAM.SAV et la copie archivée compressée de SAM dans le répertoire %windows%\Repair. Une autre façon d'accéder au fichier SAM est de lancer un programme spécial à partir d'une disquette de démarrage, puis de copier le fichier. Quoi qu'il en soit, vous avez besoin d'un accès physique à l'ordinateur contenant les mots de passe. Les mots de passe de l'utilisateur ou, pour être précis, les hachages sont en outre cryptés avec l'utilitaire SYSKEY, qui stocke ses données de service dans le fichier de la base de registre SYSTEM. Ainsi, pour extraire les hachages de SAM, vous allez avoir besoin également du fichier SYSTEM, qui est situé dans le même dossier que SAM.

Active Directory: Les comptes de domaine sont stockés dans la base de données de l'Active Directory. Habituellement, la base de données Active Directory se trouve dans le fichier %Windows%\NTDS \NTDS.DIT; elle est au cœur de Active Directory. La manière dont les hachages des utilisateurs sont cryptés, est ici est un peu différente de celle qui est utilisée dans SAM, mais la récupération pourrait également nécessiter le fichier SYSTEM. L'accès à la base de données est également sous le contrôle complet du système; Cependant, à la différence de SAM, la base de données ntds.dit est résistante aux modifications venant de l'extérieur.

Q. Si tout est si facile, pourquoi ne pas tout simplement refuser l'accès à SAM ou à l'Active Directory à tous les utilisateurs ?

R. Voici de la manière dont cela est fait. Par défaut, seul le système a accès à ces fichiers. Cependant, ces restrictions peuvent être facilement remplacées. Par exemple, WPR peut importer des hachages des fichiers actuels SAM et AD (verrouillés par le système). En outre, le système stocke les hachages dans la mémoire de l'ordinateur pour accélérer leurs accès, du coup, le dumping de la mémoire de l'ordinateur est également une option.

Q. Je ne comprends pas très bien; que dois-je copier de l'ordinateur pour récupérer les mots de passe ?

R. Si c'est un ordinateur classique, copiez les fichiers: SAM, SYSTEM (les fichiers SECURITY et SOFTWARE sont également nécessaires). Si c'est un serveur, vous aurez besoin des mêmes fichiers, plus le fichier 'ntds.dit'.

Q. Combien de temps faut-il pour récupérer un mot de passe si le hachage LM est disponible ?

R. Le plus grand inconvénient de l'algorithme de LM est qu'il sépare le mot de passe en deux moitiés de 7 caractères. Si l'utilisateur saisit un mot de passe qui est plus court que 14 caractères, le programme le remplira par des zéros pour obtenir une longue chaîne de 14 caractères. Si le mot de passe de l'utilisateur dépasse les 14 caractères, le hachage LM ressemblera à celui d'un mot de passe vide. Chacune des moitiés de 7 caractères sont cryptées de façon indépendante; facilitant et accélérant considérablement le processus de récupération du mot de passe. Un autre inconvénient majeur du hachage LM est lié au fait que pendant le cryptage, tous les caractères alphabétiques du mot de passe sont convertis en majuscules. En d'autres termes, les valeurs de hachage pour PASSWORD, password, Password ou pAsswOrd seront totalement identiques. En exécutant une attaque par Force-brute contre chaque moitié, les ordinateurs personnels modernes peuvent trouver un hachage LM alphanumérique en quelques minutes (voire quelques secondes, lorsque vous utilisez l'attaque Rainbow).
Faisons un peu de calcul. Pour trouver un mot de passe pour toute les combinaisons

alphanumériques, nous devons diviser le mot de passe en deux parties de 7 caractères de longs et ensuite chercher 36 + 32 ^ 2 + .. 36 ^ 7 = 80 603 140 212 combinaisons. Sachant, tous les hachages seront recherchés simultanément. La vitesse de recherche dans Windows Password Recovery sur un ordinateur Intel Core i7 est de plus de 100 millions de mots de passe par seconde. Arrondissons vers le bas à 100. 80 603 140 212 / 100 000 000 = 806 secondes. Cela signifie, nous sommes assurés d'obtenir le bon mot de passe en un peu plus de 10 minutes en utilisant la Force-brute.

Q. Puis-je voir les sources de cryptage ?
R. Bien sûr. Revoyez, le travail d'un programme de cryptage d'un mot de passe pour l'algorithme LM.

Q. Combien de temps est-il nécessaire pour deviner le mot de passe, si son hachage NT est connu ?
R. Avec les hachages NT c'est un peu plus compliqué. Le hachage NT ne présente pas les inconvénients qui sont communs aux hachages LM. Par conséquent, la probabilité de la récupération du mot de passe dépend entièrement de sa longueur et de la complexité, et roule comme une boule de neige. Même en dépit du fait que l'algorithme de conversion NT est plus rapide. Jetons un coup d'oeil au tableau suivant qui démontre comment le temps de recherche dépend de la longueur et de la complexité du mot de passe. En supposant que la vitesse de récupération Force-brute est de 10 milliards de mots de passe par seconde (le plus puissant GPU en 2014).

Jeu de caractères	Longueur du mot de passe	Exemple de mot de passe	Temps pour le 'cracker'
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

Q. Combien de temps est-il nécessaire pour deviner le mot de passe par NT par son hachage LM ?
R. Presque instantanément.

Q. Pourquoi ne puis-je pas simplement supprimer/définir le hachage, par ex. pour définir un mot de passe vide ?
R. Qui a dit que vous ne pouviez pas? Vous le pouvez, en utilisant, par exemple cet utilitaire. Cette méthode est très bien pour ceux qui ont besoin de retrouver l'accès à leur compte à tout prix (ou quelqu'un d'autre - par exemple, quand on parle des autorités). Cependant, avec l'utilitaire mentionné ci-dessus, vous pouvez faire cela: mémoriser le hachage, puis le réinitialiser, connectez vous sur le compte avec un mot de passe vide, faites les manipulations nécessaires avec lui, et puis restaurer le hachage mémorisé. Mais ce est pas aussi simple qu'il n'y paraît. Même si vous avez réinitialiser le mot et réussi à accéder au compte, vous ne serez toujours pas en mesure de récupérer la majorité des autres mots de passe. Pourquoi ? - Parce que le mot de passe de l'utilisateur participe à la création de la clé principale de l'utilisateur, qui est utilisée dans le cryptage EFS et DPAPI et d'autres sous-systèmes Windows. En d'autres termes, même si vous réinitialisez le mot de passe, vous ne serez pas en mesure de récupérer l'une des données suivantes: les fichiers cryptés EFS, les mots de passe de comptes Outlook, les mots de passe d'Internet Explorer, 7-9, les mots de passe de connexion réseau (RAS, DSL, VPN, etc. .), les mots de passe réseau d'autres ordinateurs, les clés de réseau sans fil, les informations d'identifications MSN Messenger, les mots de passe Google Talk et Google Chrome, Skype, etc.

Q. Donc, pour pouvoir récupérer, par exemple, un mot de passe d'Internet Explorer, je vais avoir besoin d'abord du mot de passe du compte, c'est bien cela ?
R. Exactement.

Q. Y at-il des portes dérobées ?
R. Comme partout. Par exemple, parfois le mot de passe du compte peut être stocké sous forme de texte dans les secrets. Les mots de passe pour de nombreux comptes système peuvent également être récupérés avec facilité.

Q. Est-ce que le fichier de la base registre SECURITY est requis pour l'importation des hachages de l'ordinateur local ?
R. Oui. Le but principal de la sécurité est d'avoir un stockage pour les soi-disant secrets LSA. Ces secrets (mais pas eux seuls) peuvent stocker des mots de passe en texte. L'attaque par Intelligence Artificielle met en œuvre une vérification pour les possibles vulnérabilités dans le système et, comme conséquence, les chances de récupérer une partie des mots de passe.

Q. Puis-je rentrer un hachage existant au lieu du mot de passe, lors de la connexion au système ?
R. Il y a des programmes qui font cela. Voici comment ils fonctionnent. Avant le démarrage du système, ils extraient les hachages du mot de passe de l'utilisateur. Puis, lors du chargement du compte, ils remplient les hachages connus à la place des mots de passe. Cependant, le résultat de ces manipulations est le même que de simplement remettre à zéro le mot de passe. du coup, vous ne serez plus en mesure de récupérer la majorité des autres mots de passe.

Q. Que puis-je faire si le fichier SAM est désespérément corrompu ? Y a t-il un moyen de récupérer le mot de passe d'origine dans ce cas ?
R. Oui c'est possible. Cependant, vous ne pourrez plus avoir accès au système. Vous pouvez, par exemple, choisir le mot de passe en utilisant la clé principale de l'utilisateur. Passcape Software possède des moyens pour le faire. Si l'ordinateur appartient à un domaine, les noms et mots de passe hachés des dix derniers utilisateurs enregistrés sur l'ordinateur sont mis en cache dans sa base de registre locale, dans la section SECURITY\Policy\Secrets. Vous pouvez profiter de Reset Windows Password pour dumper ces hachages (ils sont également appelés MSCACHE), puis les attaquer en utilisant Network Password Recovery Wizard.

Q. Je dois retrouver l'accès à mon compte. Pouvez-vous décrire "pour les nuls" - quelle est la meilleure façon de le faire, et comment je peux le faire ?
R. En bref, il y a deux façons de retrouver l'accès à un compte:
1. Réinitialiser le mot de passe; par exemple, effacer le mot de passe. Il existe des utilitaires spéciaux pour faire cela; le plus puissant est Reset Windows Password. Son principe de fonctionnement est simple. L'exécution d'un programme de création de disque de démarrage et de créer avec un CD de démarrage / DVD ou disque USB Reset Windows Password.
   Ensuite, allumez l'ordinateur avec le compte dont vous avez besoin de retrouver l'accès et modifiez les paramètres du BIOS pour permettre à l'ordinateur de démarrer à partir du CD / DVD / USB. Certains ordinateurs ont cette option activée par défaut. Maintenant, démarrez à partir du disque de démarrage 'Reset Windows Password' et suivez les instructions de l'assistant pour réinitialiser le mot de passe pour le compte. Toutefois, la réinitialisation du mot de passe garantie que l'accès au compte. Si vous avez aussi besoin de retrouver l'accès à des fichiers cryptés EFS ou de récupérer d'autres mots de passe d'autres (par exemple, celles du réseau), cette méthode ne vous sera pas adaptée.
2. Pour récupérer le mot de passe d'origine. Par ailleurs, cela peut être fait avec 'Reset Windows Password', en exécutant l'attaque par Intelligence. Cependant, ses capacités sont limitées pour des mots de passe seulement faibles et vulnérables. Pour restaurer le mot de passe d'origine, il est recommandé d'utiliser 'Windows Password Recovery'. Dans ce programme, une fois que les valeurs de hachages sont importées, sélectionnez et lancez l'une des attaques proposées. Si l'attaque ne réussit pas, vous pouvez modifier les paramètres et exécuter l'attaque en cours ou la remplacer par une autre. Lisez cet article, pour savoir comment choisir la meilleure attaque pour vos hachages.

Q. Où puis-je trouver des listes de mots pour les attaques de dictionnaire ?
R. Il ne faut pas en chercher. Vous pouvez télécharger des dictionnaires à partir de Windows Password Recovery. Nous avons une large collection de sortes de dictionnaires sur notre site Web.

Q. Comment puis-je faire pour mieux sécuriser mon mot de passe ?

R. Il y a plusieurs façons pour vous assurer de sécuriser vos mots de passe contre des attaquants potentiels:

- Ne pas utiliser de mots du dictionnaire (quelque soit la langue), les noms, les numéros, les séquences répétitives de lettres et de chiffres, les abréviations, les combinaisons de touches, des renseignements personnels, etc. Ces mots de passe peuvent être devinés extrêmement rapidement et facilement.
- Augmenter la longueur du mot de passe. Cependant, il y a une limite raisonnable pour tout. Rappelez-vous que la longueur est pas la chose principale (mais pas avec des mots de passe). Enfin, faire un trop long mot de passe sera sans aucun doute oublié après une fête de week-end ou de vacances. Cependant, la mémoire d'un être humain moyen ne peut pas détenir plus de 5-7 mots de passe à la fois. Pourtant, il y a un mot de passe réseau, le mot de passe Web, etc. - qui sont à retenir également.
- Étendre le jeu de caractères utilisé dans le mot de passe. Par exemple, remplacer des caractères les «a» dans le mot de passe avec le «@». Utilisation des caracteres nationaux renforce egalement les mots de passe radicalement. Utilisez des caractères rares; par exemple, '~'. Ne pas utiliser de mots de passe difficile à mémoriser qui se composent d'un ensemble de caractères aléatoires - sauf si vous êtes un génie.
- Ne pas utiliser le même mot de passe pour la connexion à Windows, les sites Web, les services, etc.
- Si vous avez du mal à se souvenir de tous vos mots de passe, les enregistrer dans un fichier protégé par un mot de passe distinct dans un endroit sûr. Une bonne protection par mot de passe est utilisée, par exemple, dans le logiciel WinRAR. Ne gardez pas ce fichier sur l'ordinateur local.
- Ne jamais saisir votre mot de passe sur l'ordinateur de quelqu'un d'autre.
- Ce n'est pas une bonne idée d'écrire vos mots de passe sur des post-it et de les coller sur le moniteur.
- Pensez à une protection supplémentaire. Par exemple, si vous activez l'option du mot de passe de démarrage SYSKEY, les chances sont proches de 100% qu'aucun attaquant ne sera en mesure de briser vos mots de passe sans avoir deviné, en premier,le mot de passe SYSKEY.

3.5 FAQ - Windows Password Recovery

Q. Qu'est-ce que les points d'interrogation dans les mots de passe LM signifient ?
R. Comme vous devez le savoir, un mot de passe LM se compose de deux moitiés. Si un mot de passe LM a 7 principaux points d'interrogation, cela qui signifie que seule la seconde moitié du mot de passe est trouvée. Les points d'interrogation suivant indiquent que la première moitié du mot de passe récupéré.

Q. Quelle est la différence entre les mots de passe LM et NT ? J'ai trouvé deux mots de passe: MASTERGURU et MasterGuru. Lequel des deux est le bon ? Lequel dois-je utiliser ?
R. .Pour vous connecter au système, vous devez utiliser le mot de passe NT.

Q. Quand je 'Force-brute' un mot de passe LM, le programme affiche un message et me dit qu'il tronque le mot de passe à 7 caractères. Est-ce un bug ?
R. Non. Comme vous le savez, un mot de passe LM est divisé en deux moitiés de 7 caractères. Par conséquent, la longueur maximale de Force-brute des mots de passe LM est de 7 caractères.

Q. Je connais mon mot de passe NT, mais le programme ne parvient pas à le trouver, pour quelles raisons ? Pourquoi ?
R. Le mot de passe NT est sensible à la casse. Peut-être, vous avez défini une gamme de recherche incorrecte. Essayez de tester le mot de passe manuellement (Outils-Testeur de mots de passe). Le testeur de mots de passe teste automatiquement toutes les combinaisons possibles de caractères majuscules et minuscules.

Q. J'ai récupéré le mot de passe administrateur, mais lorsque je tente de me connecter avec, le système me dit que le mot de passe est incorrect. Qu'est-ce qui se passe ?
R. Très probablement, vous avez récupéré le mot de passe de l'administrateur local, alors que votre ordinateur appartient à un domaine. Les mots de passe de domaine sont stockées dans l'Active Directory, y compris le mot de passe de l'administrateur de domaine. Essayez de vous connecter au système en mode sans échec.

Q. Lors d'une attaque par dictionnaire, j'ai récupéré un mot de passe qui n'était pas dans le dictionnaire. Comment est-ce arrivé ?
R. Très probablement, vous aviez mis le niveau maximal de mutation, le programme vérifie également les

mots du dictionnaire saisis dans un jeu de caractères non-anglais, national, en fonction de la configuration du clavier. Par exemple, le mot «secret» saisi avec une disposition de clavier en cyrillique produira le mot «ыускуе '. Hormis, l'echange de configurations de clavier, les mutations actives peuvent mutiler les mots au point où ils sont difficiles à reconnaître. La mutation est utilisée dans les attaques préliminaire, par dictionnaire, et combinées, ainsi que dans les mots clés ou les phrases.

Q. Dans une attaque par lots (batch), est-ce qu'il est possible de mettre plusieurs fois la même attaque, mais avec des paramètres différents ?
R. Oui, c'est possible.

Q. J'ai une question concernant les dictionnaires en ligne. J'ai remarqué qu'ils sont très compressés, à un niveau supérieur que ceux qui sont produites par les logiciels de compression/décompression de fichiers. Qu'est ce que le format PCD ?
R. Ce dictionnaire est un format de stockage propriétaire développé dans Passcape, qui utilise des algorithmes d'optimisations et de chiffrements supplémentaires. Certains dictionnaires peuvent être, en effet, compressés plus efficacement qu'avec un logiciel de compression/décompression de fichiers classique. Par exemple, le dictionnaire Australian.pcd, dans le format d'origine, prend 926 Ko d'espace, alors que dans le format compressé il fait seulement 53 Ko.

Q. J'ai choisi de lancer une attaque par dictionnaire et défini le niveau moyen de mutation. Lorsque je lance l'attaque, j'ai été désagréablement surpris par la faible vitesse de l'attaque, seulement quelques milliers de mots de passe par seconde. Pourquoi est-ce si lent ?
R. Le programme montre la vitesse d'attaque sans mutations. Par exemple, si 1000 mots ont été traité dans une seconde, elle montre 1000 mdp/s, alors que le module de mutation aurait généré 1000 mots supplémentaires par chaque mot pendant ce temps. Ainsi, la vitesse de recherche réelle est des centaines ou même des milliers de fois plus grande que ce que vous voyez à l'écran.

Q. Puis-je utiliser les dictionnaires classiques dans une attaque par dictionnaire combiné ?
R. Oui, c'est possible.

Q. Je sais que le mot de passe commence avec "blue". Quelle attaque serait la meilleur à utiliser ?
R. Vous pouvez essayer l'attaque par dictionnaire. Par exemple, le masque blue%c%c%c%c%c%c cherchera la plage de blueaaaaaa jusqu'à bluezzzzzz.
Vous pouvez également essayer de lancer une attaque par dictionnaire combinée. Pour ce faire, ouvrez le bloc-notes, puis saisissez «blue» et enregistrez le fichier sous le nom, par exemple, 1.dic. Ensuite, ouvrez les options de l'attaque combiné et paramétré 1.dic comme dictionnaire principal et n'importe quel autre - comme dictionnaire secondaire. De cette façon, le programme recherchera des mots de double syllabe comme bluepig, blueberry, bluegirl, etc. Si vous ajoutez le troisième dictionnaire, le programme va rechercher à travers une combinaison de trois composantes. Par exemple, bluecoolgirl, blueblackhash, bluebadboy.

Q. L'attaque par Intelligence Artificielle est trop lente. Qu'est-ce qui se passe ?
R. Soit parce que le cache de mots de passe est plein. Dans ce cas, vous devez essayer de le vider. Ou parce que vous avez défini le niveau de mutation trop important, et le programme a trouvé assez de mots «suspects»; par ex. les mots qui sont considérés comme des mots de passe potentiels.

Q. Quand je lance la Force-brute, le programme signale qu'il n'a rien à faire. Pourquoi ?
R. Avant le lancement de la Force-brute, vous devez d'abord sélectionner les valeurs de hachages. Vous pouvez le faire à l'aide du menu 'Éditer --> Menu Sélectionner', puis sélectionner un ou des hachages.

Q. Qu'est ce que les Rainbow tables tables ? Et comment peuvent-elles être utilisées pour récupérer les mots de passe ?
R. Pour lancer une attaque rainbow, dans les options d'attaque vous devez charger les fichier *.RT ou *.RTI qui contiennent des Rainbow tables. Le type de tables doit correspondre au type des hachages sélectionnés pour l'attaque. Par conséquent, les noms des fichiers avec les tables doivent commencer en conséquence: "lm_*.rt" pour hachages LM, "ntlm_*.rt" pour les hachages NT. Vous pouvez obtenir des informations supplémentaires et télécharger des rainbow tables sur le site http://project-rainbowcrack.com.

3.6 FAQ - GPU

Q. Quelles sont les exigences système pour le programme ?
R. Actuellement, le programme prends en charge:
- Les cartes vidéo NVIDIA CUDA ayant une capacité de calcul 2.0 et les modèles supérieures.
- Les GPU AMD Radeon, à partir de la gamme 7xxx et les modèles supérieurs
- Les processeurs graphiques Intel HD Graphics, à partir de la gamme 4xxx et les modèles supérieurs.

La liste complète des périphériques pris en charge CUDA peuvent être trouvés à l'adresse http://developer.nvidia.com/cuda-gpus. Les cartes AMD Radeon compatibles sont listées ici: http://en.wikipedia.org/wiki/Comparison_of_AMD_graphics_processing_units.
Vous devez avoir installé le pilote graphique le plus récent.

Q. Quelles versions de Windows sont prises en charge par le programme ?
R. L'accélération GPU est supportée à partir de Windows XP (GPUs NVIDIA) et Windows Vista (AMD GPUs) sur les systèmes 32-bits et 64-bits.

Q. Comment puis-je savoir quelle architecture supporte ma carte vidéo ?
R. Pour les périphériques NVidia:
Lancez le programme, ouvrez le menu 'Options - Général", Sélectionnez l'onglet 'Paramètres GPU', sélectionnez 'Nvidia CUDA' dans plate-forme et choisissez votre carte vidéo. Le champ 'possibilités de calcul' dans la section 'caractéristiques' doit afficher votre architecture GPU.
Pour les appareils AMD:
Lancez le programme, ouvrez le menu 'Options - Options générales", Sélectionnez l'onglet 'Paramètres GPU', sélectionnez 'AMD OpenCL' dans 'plate-forme' et choisissez votre carte vidéo. Le champ 'CL_DEVICE_VERSION' et 'CL_DEVICE_OPEN_C_VERSION » devrainet afficher votre architecture GPU prise en charge.

Q. Où puis-je obtenir les derniers pilotes vidéo ?
R. Vous pouvez télécharger les derniers pilotes à partir des sites Web de NVidia (http://www.nvidia.ru/drivers) et de AMD (http://support.amd.com/us/gpudownload/Pages/index.aspx).

Q. Où je peux en savoir plus sur CUDA?
R. Le site Wikipedia est un bon point de départ.

Q. Où je peux en savoir plus à propos des cartes AMD Radeon?
R. http://en.wikipedia.org/wiki/Comparison_of_AMD_graphics_processing_units

Q: Où je peux en savoir plus à propos des cartes graphiques Intel ?
A: https://en.wikipedia.org/wiki/Intel_HD_and_Iris_Graphics

Q. Après avoir lancé une attaque à base de GPU, mon ordinateur se bloque ou se bloque dans BSOD. Quel est le problème ?
R. Le problème peut être provoqué par les raisons suivantes:
- Votre carte vidéo a été overclockée, et le mauvais fonctionnement est créé par la charge élevée. Si tel est le cas, restaurer les fréquences de mémoire vidéo/cœurs à ses valeurs par défaut.
- Un refroidissement insuffisant ou inefficace de votre carte. Lorsque vous lancez une attaque à base de GPU, le programme utilise le maximum de la puissance du GPU, et la température du GPU a atteint un niveau critique. Assurez-vous que votre carte vidéo est bien refroidie, que les aérations du GPU et l'unité centrale sont exempts de saletés et de poussières. Une utilisation imprudente de certains paramètres vidéo peuvent avoir un impact négatif sur la température de la carte vidéo et sa stabilité dans des conditions de charge élevée. Par exemple, certaines applications réduise la vitesse du ventilateur afin de minimiser le bruit, réduisant le bruit, mais augmentant également la température du noyau.
- Un problème d'alimentation. Votre carte GPU peut consommer beaucoup d'énergie à pleine charge, et l'alimentation peut être incapable de gérer une telle demande élevée de puissance. Si la carte vidéo possède des connecteurs d'alimentation 6 broches ou 8 broches supplémentaires, assurez-vous qu'ils sont correctement connectés.

Q. Quand je lance une attaque GPU, mon ordinateur ralentit beaucoup. Comment puis-je résoudre ce problème ?
R. Par défaut, l'application est paramétrée pour l'utilisation de cartes vidéo de performance moyenne.

Habituellement de 256 tâches par bloc, 256 blocs et 1000 mots de passe par tâches. Pour les cartes vidéo plus anciennes, une telle configuration est inadaptée et peut provoquer un ralentissement. Envisager, donc, de réduire la valeur de "Mots de passe par tâches" à 100 ou même moins.

Q. Quelle est la meilleure façon de trouver les valeurs optimales de "Blocs de tâches" et "Mots de passe par tâches" dans les paramètres d'attaque GPU ?
R. Vous pouvez le faire soit de façon empirique ou en faisant des maths. Par exemple, si les valeurs sont 100 et 100, et la vitesse moyenne d'attaque est de 1 milliard de mots de passe par seconde, vous pouvez calculer que le noyau GPU est appelé environ 390 fois par seconde (le nombre de mots de passe calculés chaque fois est généralement 256 * ThreadBlocks * PasswordsPerThread *). Normalement, moins il y a d'appels, moins la charge est importante, et plus grande est la vitesse d'attaque. En d'autres termes, vous devez appeler le programme GPU au moins deux fois par seconde. Il faut donc utiliser une calculatrice, et ajuster les paramètres. Vous pouvez également les ajuster en utilisant une règle de base, qui est, d'augmenter les valeurs jusqu'à ce que la vitesse d'attaque s'arrête de monter et que l'ordinateur ralentit. Si vous avez un moniteur de GPU installé dans votre système, il devrait indiquer une charge d'au moins 98-99 pour cent. En outre, il est important de connaître éléments. Tout d'abord, ne pas régler ces paramètres a des valeurs trop élevées. Sinon, votre système peut ne pas fonctionner correctement ou se geler (freeze). Deuxièmement, il est préférable de ne pas définir la valeur de "Mots de passe par tâches" à une valeur inférieure à 100, car cela nuira à la vitesse d'attaque indépendamment du type de carte vidéo utilisée.

Q. Est-ce que le bus PCI-Express peut avoir un impact sur les performances ?
R. En fait, cet impact est négligeable. Il est généralement masqué par d'autres facteurs. En fait, la génération de votre bus PCI-Express et ses performances ne comptent pas beaucoup.

Q. Est-ce que la quantité de mémoire vidéo est utile ?
R. Non, pas vraiment. Cependant, dans la plupart des cas, votre GPU doit avoir au moins 256 Mo de mémoire vidéo.

Q. Une attaque à base de GPU ralentit mon PC, du coup je peux à peine utiliser. Comment puis-je résoudre ce problème ?
R. Il y a deux façons de le régler ce problème: temporairement ou définitivement. Comme solution temporaire au problème, aller dans les paramètres d'attaque et essayer de réduire le nombre de blocs de GPU utilisés ou le nombre de mots de passe testés par tâches de GPU. Comme une solution permanente, installez une seconde carte vidéo, à condition que vous avez un deuxième emplacement sur votre carte mère et que votre bloc d'alimentation peut gérer la charge supplémentaire. Par exemple, vous pouvez utiliser certaines cartes peu onéreuse comme carte vidéo principale (pour afficher des informations sur votre moniteur), et une seconde plus puissante, pour les attaques par Force-brute des mots de passe.

Q. Je possède plus d'une carte vidéo dans mon ordinateur. Puis-je les utiliser pour les attaques par Force-brute ?
R. Oui. Vous pouvez les utiliser toutes ou une partie d'entre elles. Il suffit d'ouvrir les paramètres généraux et de spécifier le périphérique(s) GPU qui doit être utilisé par le programme.

Q. Quel est le nombre maximal de périphériques GPU supporte votre programme ?
R. Il dépend de votre matériel. Même si le programme prends en charge jusqu'à 255 périphériques, généralement, jusqu'à 8 périphériques peuvent être installés dans un emplacement PCI-E carte mère 4 (4 cartes double GPU).

Q. Est-ce que je peux lancer une attaque Force-brute avec des périphériques GPU de performances différentes ?
R. Oui vous le pouvez.

Q. Le programme ne peut pas détecter ma carte vidéo. Que puis-je faire ?
R. Mettez à jour vos pilotes vidéo. Si cela ne vous aide pas, essayez de prolonger le bureau à toutes les cartes (si vous avez plus d'un appareil). Re-brancher votre carte vidéo à un autre emplacement PCI-Express.

Q. Votre application ne peut pas utiliser tous mes GPUs.
R. Vous devrez désactiver SLI afin d'être en mesure d'utiliser tous les dispositifs.

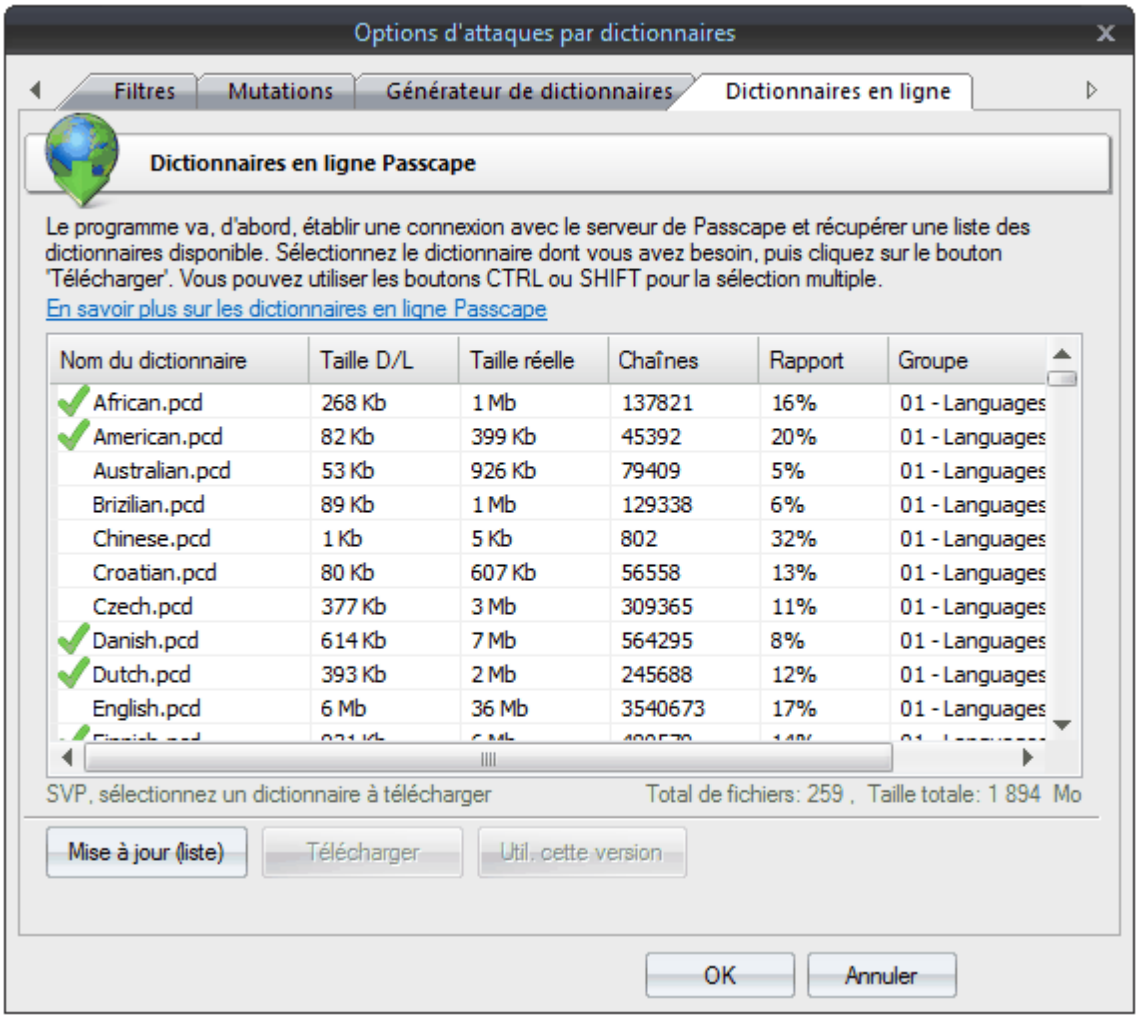
Q. Puis-je utiliser les trois cartes graphiques NVIDIA, AMD et INTEL simultanément ?
R. Oui, vous pouvez utiliser des périphériques NVIDIA, AMD et Intel simultanément.

Q. Comment puis-je vérifier mon utilisation GPU ?
R. Ouvrir l'onglet "Moniteur matériel". Dans "Choix d'affichage" choisir l'appareil dont vous avez besoin et sélectionnez "Afficher" pour l'afficher. Vous pouvez alors cliquer sur les boutons 'Démarrer' 'Arrêter' ou pour gérer la surveillance du matériel. Le moniteur de GPU montre la charge du périphérique (d'utilisation), la température et la vitesse du ventilateur.

Q. Mon GPU NVidia est absent dans le moniteur système.
R. Vous devez installer/réinstaller la bibliothèque NVAPI. Vous pouvez télécharger la bibliothèque à l'adresse: https://developer.nvidia.com/nvapi

Q. Mon GPU AMD affiche des zéros dans moniteur système.
R. Installer/réinstaller les derniers pilotes AMD ou composants ADL. Assurez-vous que votre périphérique AMD est activé (connecté à votre moniteur). Les périphériques inactifs ne sont pas gérés correctement par AMD Display Library (ADL), à cause d'un bug dans les pilotes graphiques de AMD.

3.7 Dictionnaires en ligne



La boite de dialogue pour la sélection de dictionnaire en ligne est extrêmement simple. Quand elle s'ouvre, le programme tente d'établir une connexion avec le serveur Passcape, puis il récupère et affiche la liste des dictionnaires disponibles pour le téléchargement

Sélectionnez le dictionnaire, puis cliquez sur le bouton '**Télécharger**' pour le récupérer et pouvoir l'utiliser dans le programme.

Certains dictionnaires ont une taille importante. Par exemple, la taille de ***'music_songs.pcd'*** est de plus de 59 Mo au format compressé. Naturellement, récupérer un si gros volume de données peut prendre du temps, qui dépends de la taille du fichier, de la bande passante de votre connexion Internet et de la charge du réseau.

Tous les dictionnaires (et d'autres en options) peuvent être commandés sur CD. La taille totale de tous les dictionnaires est supérieur à 7.5 Go. Vous pouvez aussi partager votre propre dictionnaire avec nous, en l'envoyant par email ou en nous fournissant le lien où il peut être téléchargé.

Les listes de mots peuvent être utilisées dans l'attaque par simple dictionnaire, dictionnaires combinés et phrases de mots de passe.

Licence et enregistrement

4 Licence et enregistrement

4.1 Contrat de licence

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

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

All copyrights to SOFTWARE are exclusively owned by Passcape Software.

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

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

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

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

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

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

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

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

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

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

The program that is licensed to you is absolutely legal and you can use it provided that you are the legal owner of all files or data you are going to recover through the use of our SOFTWARE or have

permission from the legitimate owner to perform these acts. Any illegal use of our SOFTWARE will be solely your responsibility. Accordingly, you affirm that you have the legal right to access all data, information and files that have been hidden.

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

4.2 Enregistrement du logiciel

Le logiciel est disponible en trois éditions: 'Light', 'Standard' et 'Advanced'. Le détail des fonctionnalités est consultable dans à cette page de l'aide.

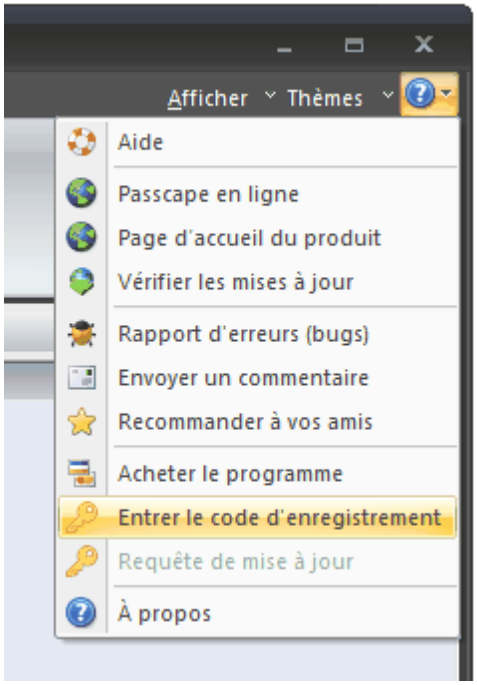
Vous pouvez commander une licence pour la version complète de Windows Password Recovery, au tarif suivant en fonction de l'édition choisie:

- 'Light' pour un prix de 65$ (licence et usage personnel)
- 'Standard' pour un prix de 345$ (licence et usage personnel)
- 'Advanced' pour un prix de 895$ (licence et usage professionnelle).

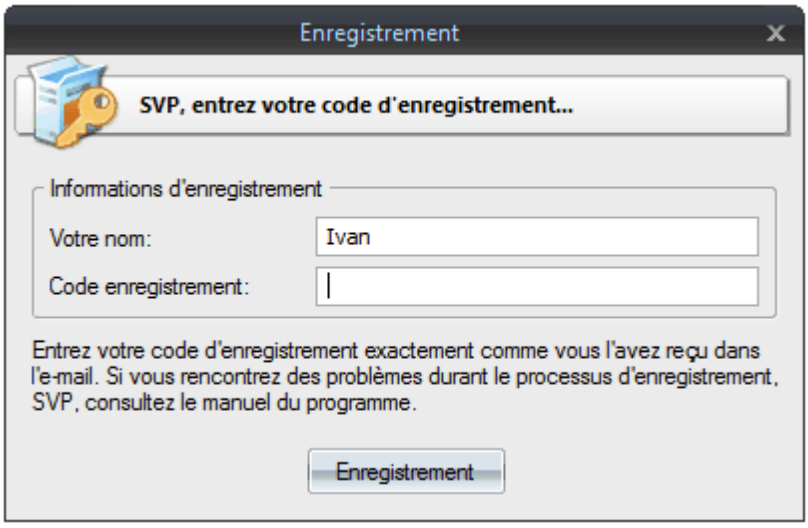
Les informations détaillées pour la commande du logiciel, et les différents moyens de paiement sont disponible en ligne sur la page de commande de WPR. Les commandes en ligne sont traitées en quelques minutes, 24h/24 et 7jours/7. Si vous achetez nos logiciels en ligne, vous recevrez un message par e-mail généré automatiquement avec les détails de votre enregistrement en quelques minutes (si votre paiement est accepté par le système de détection de fraudes). Cependant, certaines commandes doivent être vérifiées manuellement ou vues comme 'suspicieuse'. Dans ces cas, le temps de traitement de votre commande peut prendre plusieurs heures.

Important: lors de la rédaction du formulaire de commande, s'il vous plaît, vérifiez deux fois que votre adresse e-mail est correcte. Si cela n'était pas le cas, nous serions incapable de vous envoyer votre code d'enregistrement.

Pour terminer l'enregistrement:



- Ouvrez le message d'enregistrement reçu de Passcape (e-mail) et copiez le code d'enregistrement dans le presse-papiers de Windows.
- Lancez le programme, sélectionnez dans la barre de menu '**Aide - Entrer le code d'enregistrement**'.
- Saisissez votre nom et coller le code dans la case réservée au code.
- Cliquez sur le bouton '**Enregistrement**' pour confirmer.



4.3 Limitations de la version non enregistrée (démo)

La version de démo (non enregistrée) de **Windows Password Recovery** affiche seulement les 3 premiers caractères des mots de passe récupérés et possède certaines limitations de fonctionnalités.
La version enregistrée du programme supprime toutes les restrictions. Consultez cette page, s'il vous plaît, pour voir les restrictions de certaines versions du programme.

4.4 Versions du logiciel

Windows Password Recovery existe en trois éditions: Light, Standard et Advanced. Le tableau, ci-dessous, affiche la liste détaillée des fonctionnalités et de compatibilités:

FONCTIONNALITES	Light	Standard	Advanced
Support de stations de travail sous Windows 2000/XP/Vista/7/8/10	+	+	+
Support Windows serveur 2000/2003/2008/2012	+	+	+
Support de Windows 64-bits	+	+	+
Support de Windows Non-US	+	+	+
Support des mots de passe internationaux	+	+	+
Récupération multi-tâches	+	+	+
Support de thèmes pour l'interface graphique	+	+	+
Chargement de hachages à partir de l'ordinateur local	+	+	+
Chargement de hachages à partir de l'ordinateur distant (remote)	-	+	+
Dump des hachages classiques	+	+	+
Dump des hachages d'historiques de mots de passe	+	+	+
Recherche de mots de passe textes	+	+	+
Chargement de hachages à partir de SAM	+	+	+
Chargement de hachages de l'Active Directory	+	+	+
Importation de hachages à partir d'autres logiciels	+	+	+
Chargement de hachages à partir de répertoires de restaurations système	+	+	+
Exportation de hachages vers un fichier PWDUMP	+	+	+
Attaques communes	+	+	+
Attaques avancées	+	+	+
Attaques Intelligentes	+	+	+
Attaques à base de GPU	+	+	+
Support de plusieurs cartes graphiques GPU	-	+	+
Attaque par lots (batch)	-	-	+
Visionneuse du cache de mots de passe AI	-	-	+
Mutation intelligente de mots de passe	+	+	+
Dictionnaires disponibles en ligne	+	+	+
Support du décryptage de SYSKEY	+	+	+
Support du décryptage du mot de passe de démarrage SYSKEY	+	+	+
Support du décryptage de la disquette SYSKEY	+	+	+
Outil pour générer les listes de mots personnalisés dans l'attaque par Dictionnaire	-	-	+
Générateur de dictionnaires par masques	-	-	+
Générateur de dictionnaire à base de mots	-	-	+
Générateur de dictionnaires combinés	-	-	+
Générateur de dictionnaires Pass-phrase	-	-	+
Générateur de dictionnaires d'empreintes	-	-	+
Création de listes de mots basés sur l'attaque par dictionnaire hybride	-	-	+
Support de tables indexées pour les tables Arc-en-ciel hybride et indexées (*.rti)	+	+	+
Possibilité de restreindre l'accès au programme	+	+	+
Mesure de la force du mot de passe	+	+	+
Testeur de hachages	+	+	+
Générateur aléatoire de hachages	+	+	+
Générateur de hachages multiples	-	+	+
Outil de génération de tables Arc-en-ciel	+	+	+
Outil de génération de tables Arc-en-ciel Passcape	+	+	+

FONCTIONNALITES	Light	Standard	Advanced
Générateur de hachages à base de dictionnaires	-	+	+
Sauvegarde des fichiers de la base de registre	-	+	+
Sauvegarde de la base de données de l'Active Directory	-	-	+
Outil de visualisation des mots de passe sous les Asterisk (****)	+	+	+
Outil hors-ligne de suppression de mots de passe	-	-	+
Dumper de secrets LSA	+	+	+
Explorateur d'infos d'identifications de Domaine en cache	-	+	+
Explorateur SAM	-	+	+
Explorateur d'Active Directory	-	-	+
Explorateur de Coffre Windows	-	-	+
Outils de listes de mots: création d'une liste de mots en indexant des fichiers	-	+	+
Outils de listes de mots: fusionner des listes de mots	+	+	+
Outils de listes de mots: statistiques de liste de mots	+	+	+
Outils de listes de mots: tri	+	+	+
Outils de listes de mots: conversion/compression	+	+	+
Outils de listes de mots: comparaison de listes de mots	+	+	+
Outils de listes de mots: opérations complémentaires	+	+	+
Outils de listes de mots: indexations de mots/de mots de passe de surfaces de disque sensibles	-	-	+
Outils de listes de mots: extracteur de liens HTML	+	+	+
DPAPI: récupérateur hors-ligne de blobs DPAPI	*	*	+
DPAPI: analyseur de blobs DPAPI	+	+	+
DPAPI: recherche de blobs DPAPI	+	+	+
DPAPI: analyseur de Master Key	*	*	+
DPAPI: dump des hachages de l'historiques des mots de passe	-	-	+
DPAPI: analyseur de l'historique de mots de passe	*	*	+
Windows Hello: Récupération des identifiants des utilisateurs	-	+	+
Windows Hello: Décryptage des bases de données biométriques	-	+	+
Windows Hello: Attaque de codes PIN par Force-brute			
Moniteur matériel	+	+	+
Rapports de mots de passe	-	+	+
Exécution en mode caché	+	+	+
Nombre maximum de comptes utilisateurs chargés en même temps	500	5000	illimité
Garantie d'un remboursement de paiement en 14 jours	+	+	+
Type de licence	usage personnel	usage personnel	professionnelle
Prix du logiciel	$65	$345	$895

* - certaines fonctionnalités sont restreintes

Support technique

5 Support technique

5.1 Signaler des problèmes

Si vous avez un problème, s'il vous plaît, contactez-nous à l'adresse e-mail support@passcape.com.
Sans oublier de nous communiquer les informations suivantes:

- Nom complet et version du programme
- Version de Windows incluant le service pack, OEM et information du langage, etc.
- Information sur votre enregistrement, si vous l'êtes.
- Description détaillé de votre problème, si l'erreur est constante ou intermittente.
- Si vous signalez une erreur critique, n'oubliez pas de joindre votre fichier 'crash.log' qui a été sauvegardé pendant la session d'exception non gérée.

5.2 Suggestions de fonctionnalités

Si vous avez des questions, des commentaires ou suggestions à propos du programme ou si vous souhaitez avoir plus d'informations, envoyez-nous un e-mail à l'adresse: info@passcape.com

S'il vous plaît, n'oubliez pas de mentionner le nom du programme et la version. Assurez vous, aussi, que vous avez installé la dernière version du programme.

Votre retour d'informations nous aidera à améliorer nos logiciels et à travailler plus efficacement.

5.3 Contacts

S'il vous plaît, n'hésitez pas à envoyer vos questions concernant nos logiciels, à l'email suivant: support@passcape.com.
Nous vous répondrons sous un à deux jours. Notez, que les utilisateurs enregistrés ont priorité pour le support technique.

Si vous avez rencontré des problèmes durant le processus d'enregistrement, s'il vous plaît, envoyez une lettre à l'adresse sales@passcape.com

Nous serons heureux de vous assister dans votre enregistrement.

S'il vous plaît, écrivez-nous en Anglais !

Vous pouvez trouver d'autres utilitaires de récupération sur notre site Web à l'adresse: https://www.passcape.com

Aide de WPR traduit par Laurent DEBARD - 07/06/2018