Mozilla Password Recovery

USER MANUAL

Passcape Software

Introduction

1 Introduction

1.1 About the program

If the list of your Web passwords is larger than ten entries, than Password Manager is the right tool for you. You won't have to desperately try to recall the right password, or look it up in your notebook. Mozilla, Firefox, and Thunderbird have comfortable password managers, though if you compare them to the Protected Storage of Internet Explorer or WAND of Opera, the latter ones are more powerful and functional. However, human memory is not without flaws, programs can freeze or get dysfunctional, and the operation system can refuse to boot up. In this case, you will need help to recover your lost or forgotten passwords.
Mozilla Password Recovery is a small utility that reveals the Autofill passwords for Firefox and Mozilla/SeaMonkey, as well as the account passwords of the Thunderbird mail client. The program traditionally offers you two recovery modes: automatic and manual. With this utility you can also recover passwords protected with User Master Password, thus being one step ahead of its competitors.

1.2 Features and benefits

With this program you can:

- Recover all Mozilla, SeaMonkey, Firefox, Thunderbird, K-Meleon, SongBird, Beonex, Flock and Netscape autocomplete data as well as e-mail account passwords
- View Firefox, SeaMonkey, Mozilla cookies, autocomplete data and URL history
- Choose between two (automatic and manual) recovery modes
- Export passwords to text html or excel files
- Prevent an unauthorized program execution
- Decrypt passwords protected with User Master Password
- Master Password recovery

1.3 System Requirements

Requirements
Windows N+, less than 5Mb on your hard drive.

Compatibility
All version of Mozilla-based applications (Firefox, SeaMonkey, Thunderbird, etc.) are supported. Namely

Known issues or bugs
The program although contains no harmful code, may be detected by some anti-virus/anti-spyware software as potentially dangerous or "potentially unwanted program". This is also known as "False Alert", and it's quite a common problem for all password recovery software.

Working with the program

2 Working with the program

2.1 Main window

Main window of the program allows you to choose a recovery mode:

- **AUTOMATIC FIREFOX** - select this mode to recover all found Mozilla Firefox autocomplete passwords
- **AUTOMATIC THUNDERBIRD** - automatically recover Mozilla Thunderbird e-mail account passwords
- **AUTOMATIC MOZILLA** - automatically recover Mozilla/SeaMonkey browser passwords
- **MANUAL FIREFOX** - decrypt Mozilla Firefox autocomplete passwords manually
- **MANUAL THUNDERBIRD** - recover Mozilla Thunderbird e-mail account passwords manually
- **MANUAL MOZILLA** - manual recovery mode for Mozilla/SeaMonkey browser

Extended modes:

- **Master Password Recovery** - recover Firefox, Thunderbird, Mozilla or SeaMonkey Master Password
- **Cookie Explorer** - parse and explore your browser cookies
- **History Viewer** - view and manage your browser URL history

2.2 Manual recovery mode

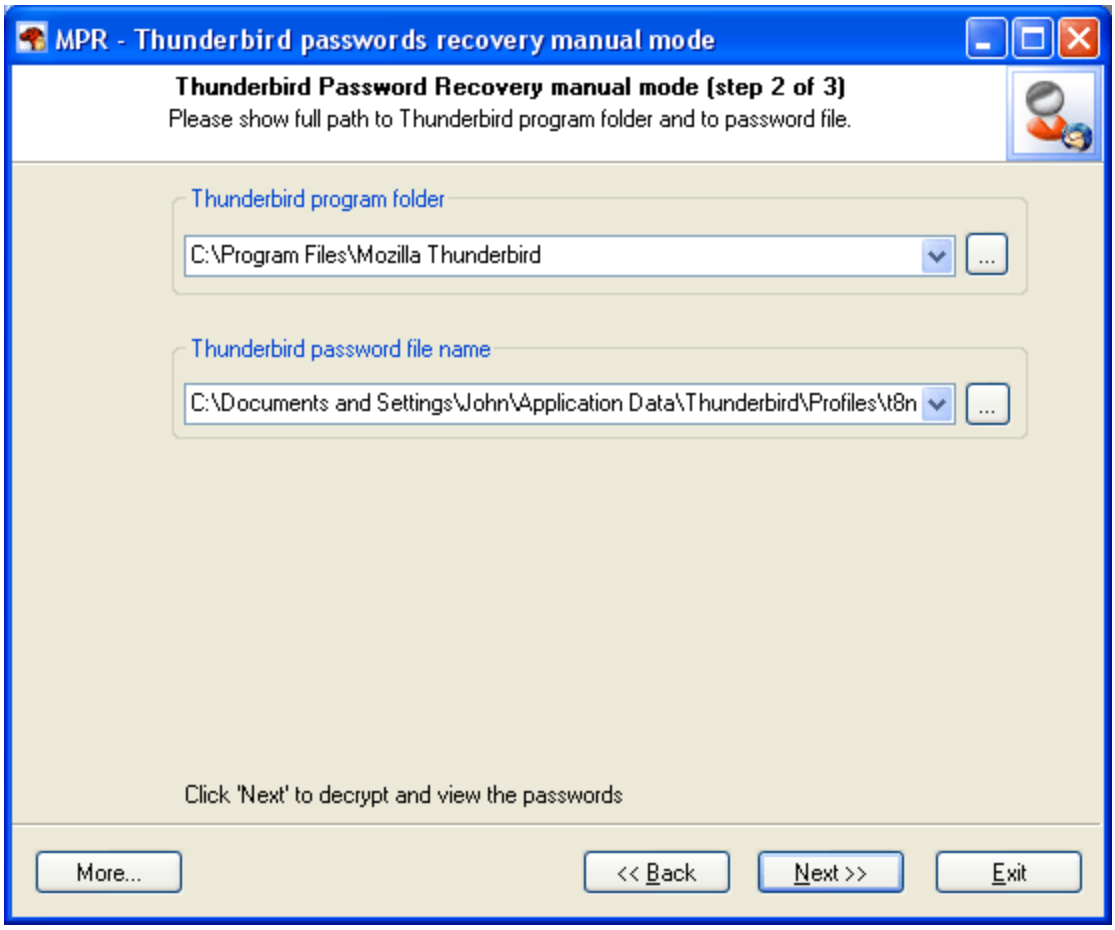
MPR manual modes allow you to set the program recovery options manually. You have to know at least two things for successful recovery.

1) The program installation directory. The directories are typically as follows:
   - *%PROGRAMFILES%\Mozilla Firefox* - for Mozilla Firefox
   - *%PROGRAMFILES%\Mozilla Thunderbird* - for Mozilla Thunderbird
   - *%PROGRAMFILES%\mozilla.org\Mozilla* - for Mozilla/SeaMonkey browser

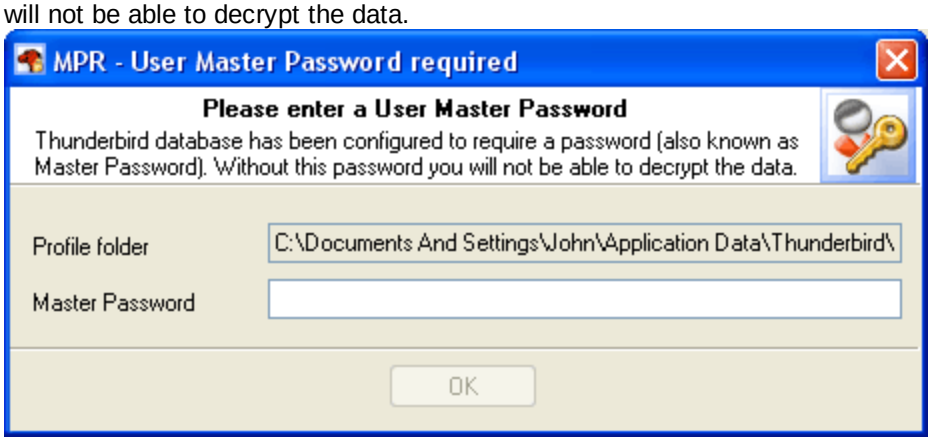
Where *%PROGRAMFILES%* is your Program Files folder.

2) Storage (password) file location. Here are the default locations:
   - *%USERPROFILE%\Application Data\Mozilla\Firefox\Profiles\%PROFILEFOLDER%\signons.txt* - for Firefox
   - *%USERPROFILE%\Application Data\Thunderbird\Profiles\%PROFILEFOLDER%\%pfid%.s* - for Thunderbird
   - *%USERPROFILE%\Application Data\Mozilla\Profiles\default\%PROFILEFOLDER%\%pfid%.s* - for Mozilla/SeaMonkey browser

Where *%USERPROFILE%* is a user profile directory (usually C:\Documents And Settings\xxx), *%PROFILEFOLDER%* is a profile folder name (may look like 6sn16oa4.slt or like t8nosfci.default), *%pfid%* is a program password file id (the whole password filename may look like 44038172.s).



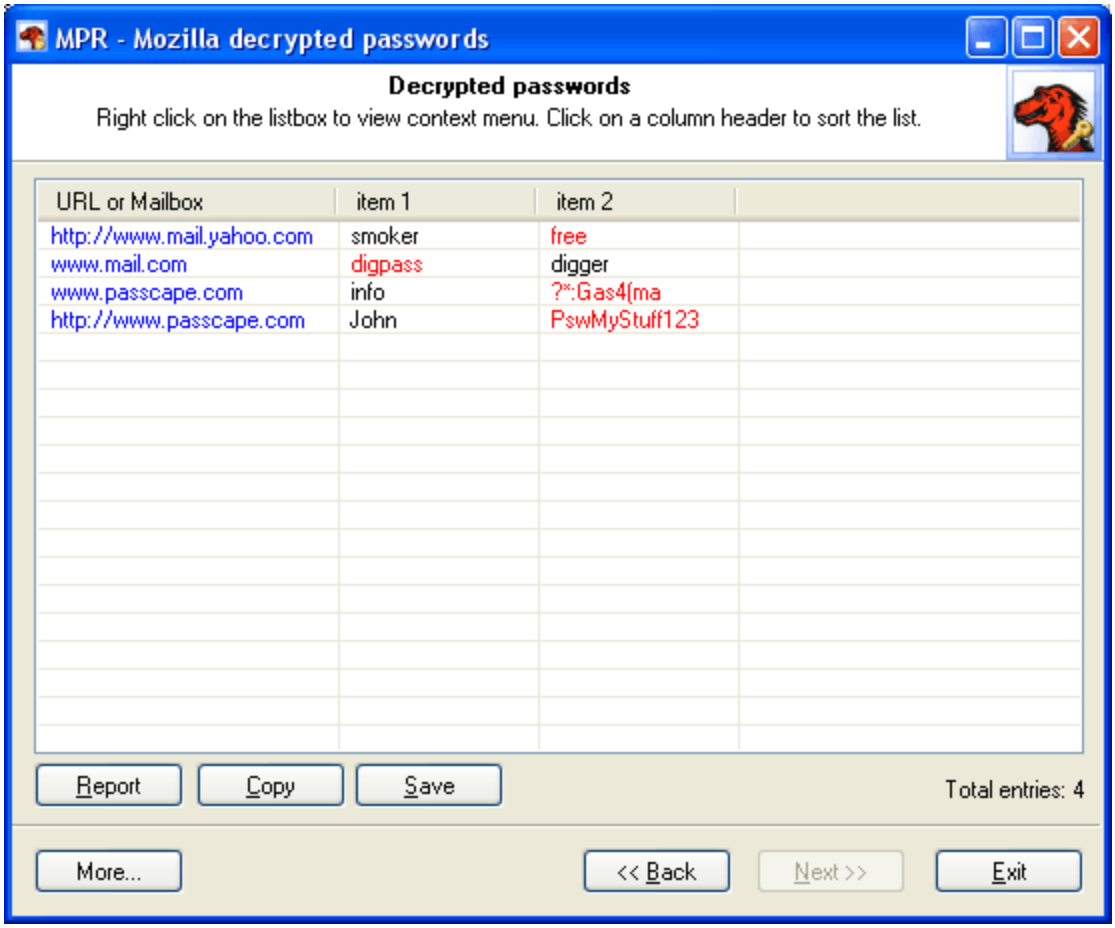
Usually, knowing the program folder and the password file location is enough to recover the passwords. But sometimes it is also required to know the User Master Password. Without the Master Password you will not be able to decrypt the data.



Important! Using the program 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.

2.3 Passwords window

The password window contains found and decrypted passwords.



Password items are marked with red color.

Right click on the passwords list to view context menu.

2.4 Master Password Recovery

The entire process of Master Password recovery for Mozilla/SeaMonkey/Firefox/Thunderbird can be divided into 4 program's steps. These steps are described below.

1) Selecting Master Password location
2) Choosing decryption method
3) Setting recovery options

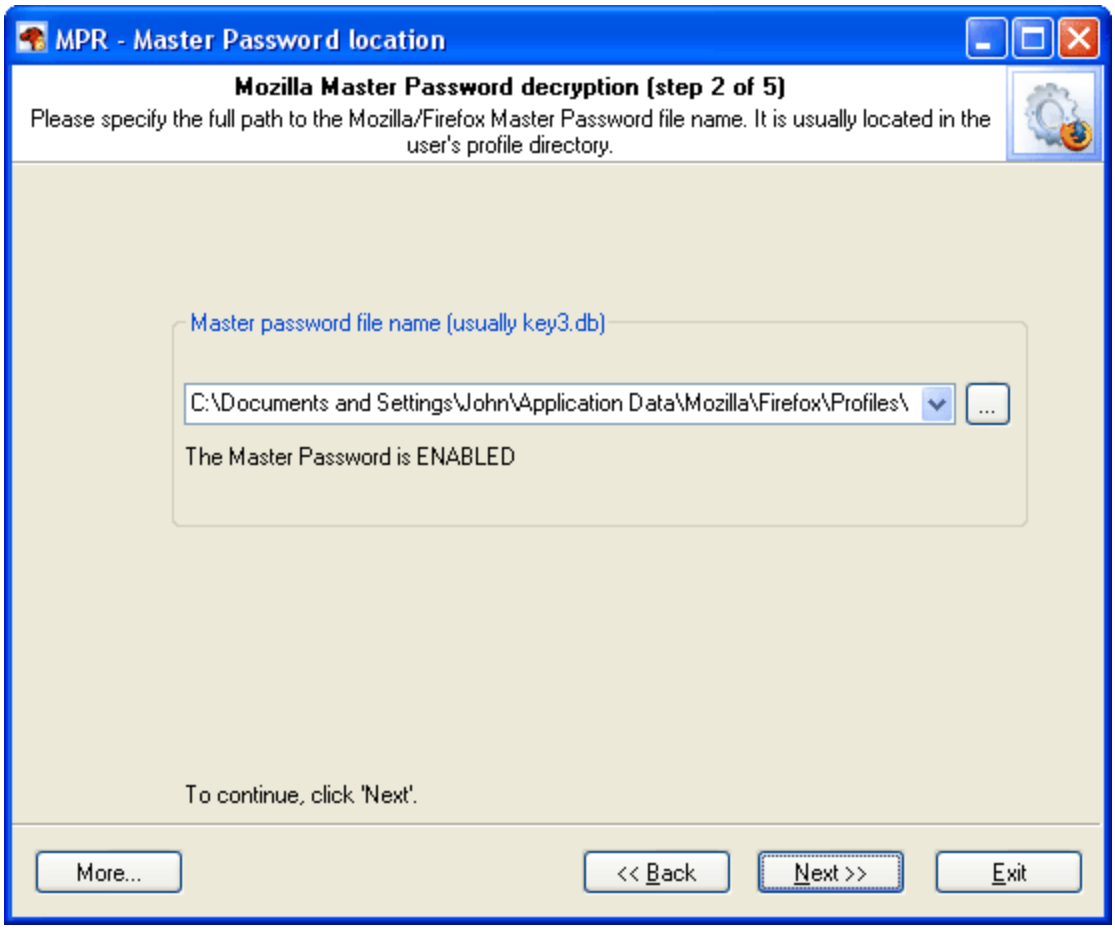
- Artificial Intelligence attack options
- Dictionary attack options
- Brute-force attack options
- Mask attack options

- Base-word attack options
- Combined dictionary attack options
- Phrase attack options

4) Launching the selected attack

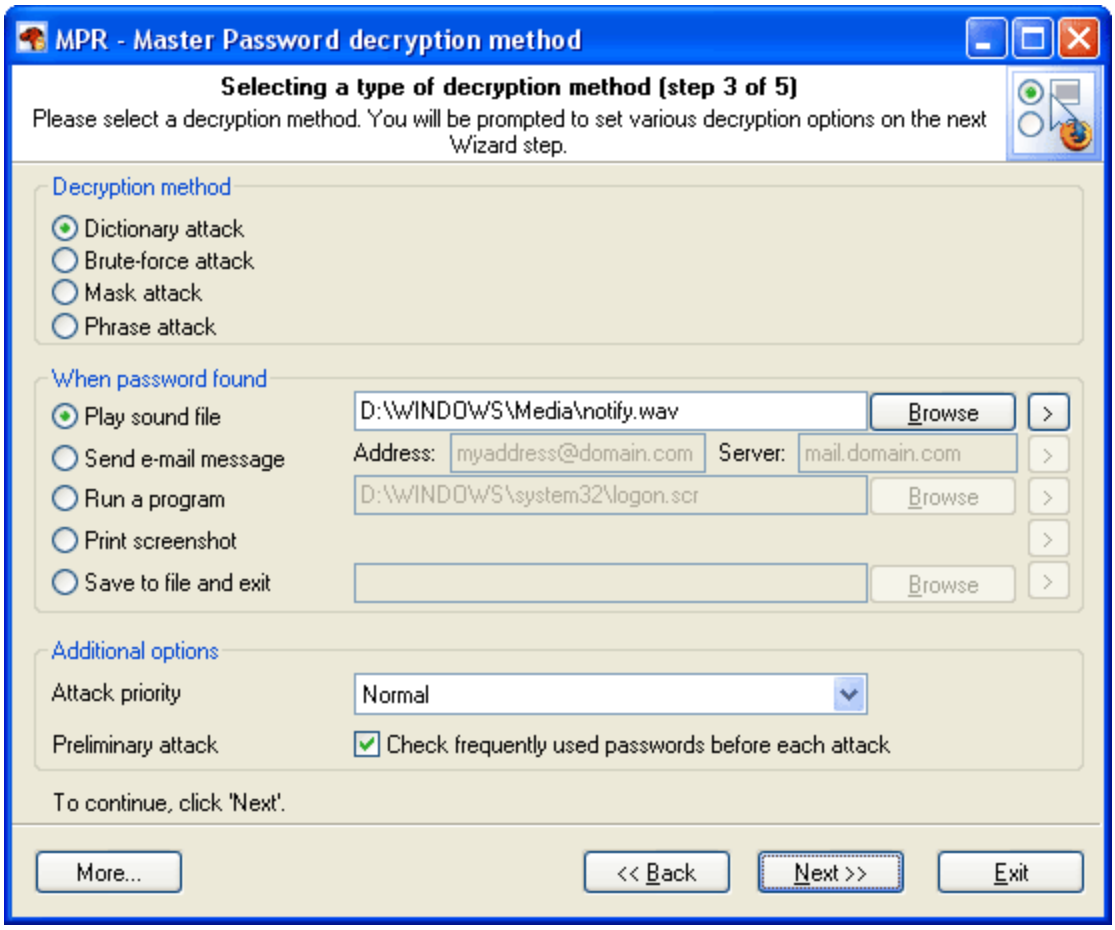
2.4.1 Selecting Master Password location

Select the folder where the program (Mozilla, SeaMonkey, Firefox, or Thunderbird) stores its Master Password. Normally, **MPR** does that automatically and allows you to select the folder manually if you have two or more programs installed on your computer. You can also do that by hand by entering path to the **key3.db** file. It is stored in the program's profile. For example: C:\Documents and Settings\John\Application Data\Mozilla\Firefox\Profiles\3un7ntgo.default\key3.db.



2.4.2 Choosing decryption method

During this step, the program's wizard will ask you to choose the decryption method, set the event (notification) to be performed when the password is found, and set a number of additional decryption options.



Decryption method

Decryption method

Currently the software can guess the password by launching several types of attacks:

- **Artificial Intelligence Attack** is a new type of attack developed in our company. It is based upon a social engineering method and allows, without resort to time-consuming and costly computations, to almost instantly recover certain passwords.
- **Dictionary attack** - is the most efficient recovery method, when the program tries each word from the dictionary (or dictionaries if there are several dictionaries) you specify until it finds the original password or until the wordlist is out of words. This method is efficient since many people use regular words or phrases for password. Other than that, this type of recovery is performed quite fast compared to brute-force attack, for instance. Additional dictionaries can be fond on our website.
- **Brute-force attack**. If the dictionary attack has failed, you may need to take a closer look to brute-force attack, when the program uses all possible combinations from the specified range of characters. For example, for a three-character range of lower-case Latin characters, it will check all possible combinations, starting with 'aaa', 'aab', 'aac', and all the way through 'zzz'. This is the slowest attack, so it is really great for short passwords.
- **Mask attack**. This type of attacks is useful if you have at least some information about the password. For example, you may know that the first four characters in the passwords are Latin letters; they are followed by a three-digit number. The mask attack is a variation of the brute-force attack, except that some characters for finding the password remain unchanged, and only a portion of the password may change. The special syntax is used for setting a mask or rule for finding a password. It will be described in detail in the corresponding chapter below.
- **Base-word attack**. At the first glance, this type of attack reminds the one we just described. It is just as efficient if a portion of the password to be recovered is known to us. However, unlike in the previous

attack, here you do not have to set a mask - just provide a basic word (or phrase). The program will take care of the rest. The phrase attack is based upon the experience of the social engineering and uses over 140 rules for possible modifications of the original phrase to generate a great number of possible password combinations.

- **Combined dictionary attack** uses primary to guess compound passwords. It is very similar to the dictionary attack, except that instead of using a single word for password verification it uses a combination of words created from several dictionaries.
- The idea of the **phrase attack** is to find the right password by searching through predefined and frequently used expressions, sayings, phrases and word combinations.

When password found

This group allows setting an action to be performed automatically when the password is found. This option is convenient, for instance, to system administrators when passwords are being recovered on several computers at once. The program offers five possible notifications: play sound, send e-mail, run application, print screen or store results to file and close the program.

Important! If you choose the send e-mail notification type, make sure you have checked your firewall settings and have allowed the program to send e-mail to the Internet.

Additional options

In the Additional options group you can specify:

Attack priority. If you are planning on using your computer actively during attack, you are recommended to set the priority value to 'Below normal' or even 'Low'.

Preliminary attack. The program will check the most frequently used passwords before each attack. Literally, by selecting this option, you activate the fifth type of attack, the preliminary attack. It may take up to 1 minute on slower computers. Preliminary attack consists of four parts and allows to 'catch' short and frequently used passwords like '*qwerty*'.

2.4.3 Setting recovery options

Currently, as it was mentioned above, there are 7 decryption methods available:

1. Preliminary attack usually runs before each attack.
2. Dictionary attack. Try every word from a dictionary until the password is found. This attack is the most effective.
3. Brute-force attack guesses the password trying all possible password variants by given character set.
4. Mask attack is very helpful if there's any information about the password.
5. Base-word attack. Useful if a part (or source word) of the password is known.
6. Combined dictionary attack uses to guess complex/compound passwords.
7. Phrase attack uses primary to search complex password by looking through a dictionary with frequently used phrases.

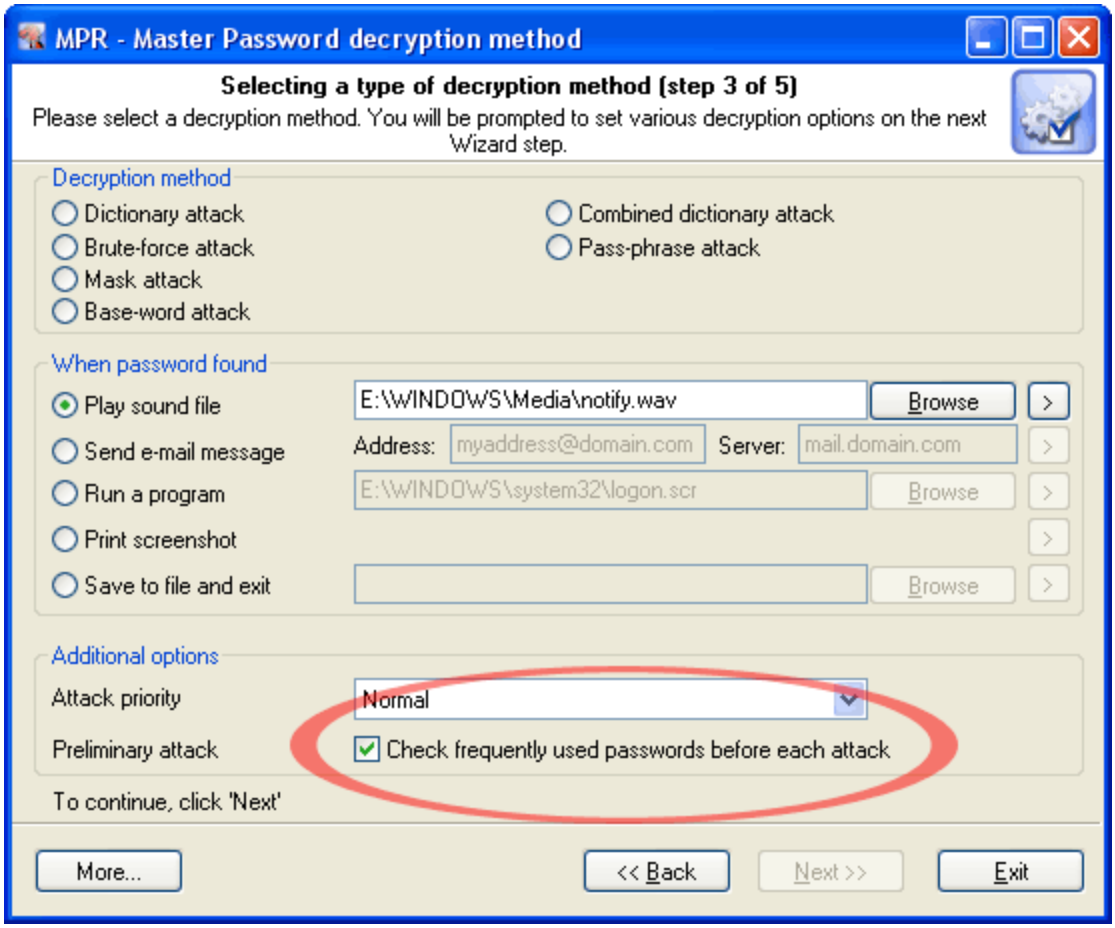
Once selected a recovery type, you will be prompted for different options on the next Wizard page.

- **Preliminary attack**
- Artificial Intelligence attack
- **Dictionary attack options**
- **Brute-force attack options**
- **Mask attack options**
- **Base-word attack options**

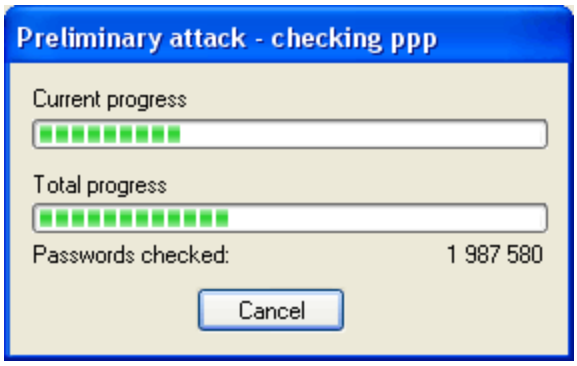
- Combined dictionary attack options
- Phrase attack options

2.4.3.1 Preliminary attack

Preliminary attack is a time-limited simple set of several mini sub-attacks. It is often run when a password cannot be recovered instantly, but there's no need to launch a full (eg. brute-force or dictionary) attack. The preliminary attack activated by setting '*Check frequently used password before each attack*' check box on in common options dialog (see the screenshot below.)



Usually a preliminary attack executes in less than a minute. When it is running the following dialog is displayed:



Preliminary attack consists of at least the following sub-attacks:

- **Common brute-force attack**. Performs several simple brute-force attacks based on predefined character sets.
- **Simple dictionary attack**. Fast check the password by verifying all words from a given dictionary.
- **Extended dictionary attack**. It's almost the same as above but with some smart mutation options set on.
- **Attack on repeatables**. Checking passwords as a repeatable sequence of a character. Eg. '1111111' or 'xxxxxxx'.
- **Attack on simple patterns**, like '123456' or 'qwerty'.
- **Attack on complex patterns**. The same as above, for compound patterns.
- **Keyboard attack** checks for keyboard passwords and all possible combinations. Eg. 'qwer', 'qazwsx', 'asdzxc', etc.
- **National keyboard attack**. The same as above, but checks passwords typed in national keyboard layout.
- **Complex keyboard attack** is the same as previous 2 attacks, for compound keyboard patterns.
- **Passcape Password Prediction attack** is the most complicated and state-of-art password prediction tool.

2.4.3.2 Artificial Intelligence attack

Artificial Intelligence Attack is a new type of attack developed in our company. It is based upon a social engineering method and has never been implemented in password recovery applications.

This attack allows, without resort to time-consuming and costly computations, to almost instantly recover certain passwords encrypted with hash functions. The basic idea behind the AI attack is that an average user very often chooses similar words and word combinations or follows the same password generation rule when creating one's passwords. With that in mind, we could attempt to figure that rule out and pick the original password.

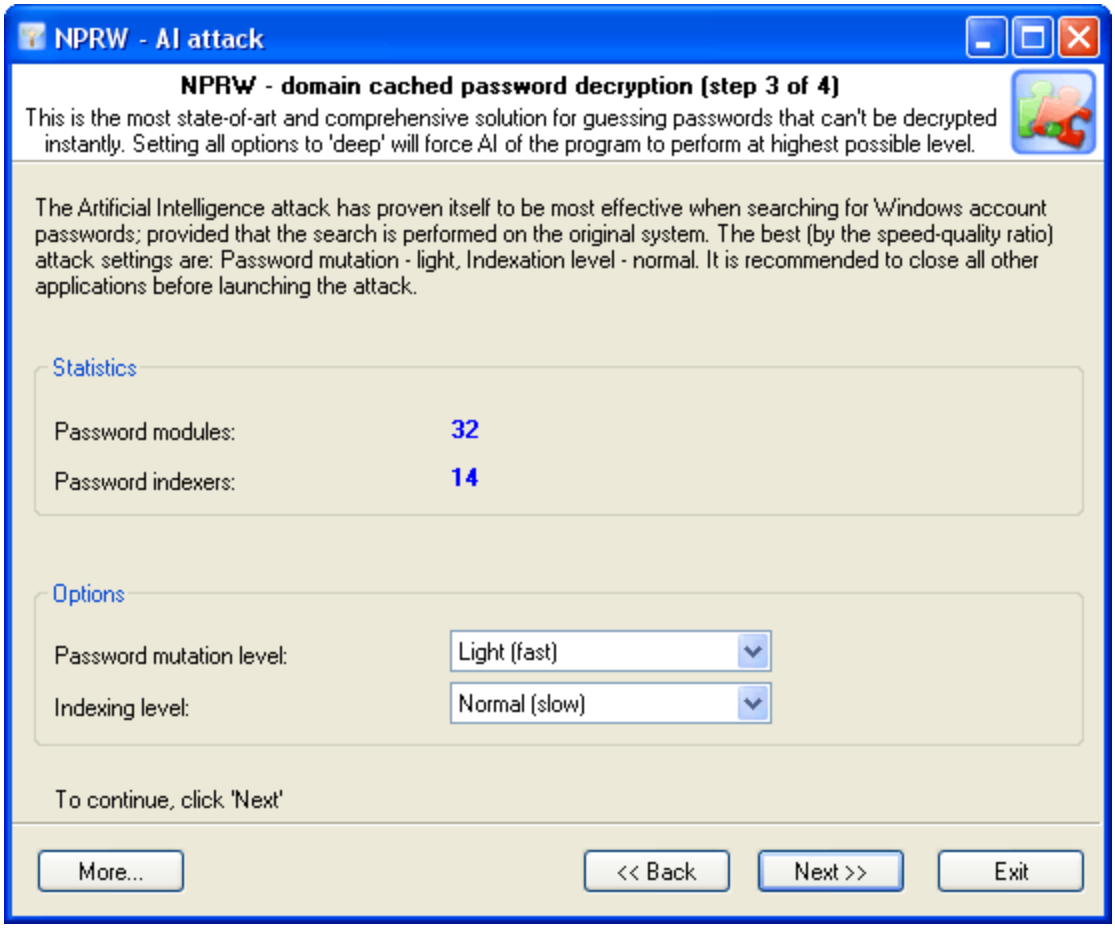
Although this sounds somewhat abstractive, in the reality the attack clearly splits into four successive steps.

- Step 1. Initiating the collection of private data. Here comes into action the password retrieval and indexation module, which looks for all available and hidden in the system passwords entered by user at any moment of time. Those include network access passwords, ICQ, email, FTP, Windows account passwords, server passwords, etc.
- Step 2. Launches the data collection and indexation module. During the execution of this step, we analyze the activity of the user (or all users, if the indexation module selected is different than Light) in the system. Next, basing upon that, we generate the list of words – potential passwords selected from the text files, archives, internet browsers' history, email correspondence, etc.

- Step 3. Includes the semantic analysis module for the database of found passwords and the list of potential passwords.
- Step 4. On the final stage, the data analysis module will perform the mutation of the words and attempt to pick the passwords.

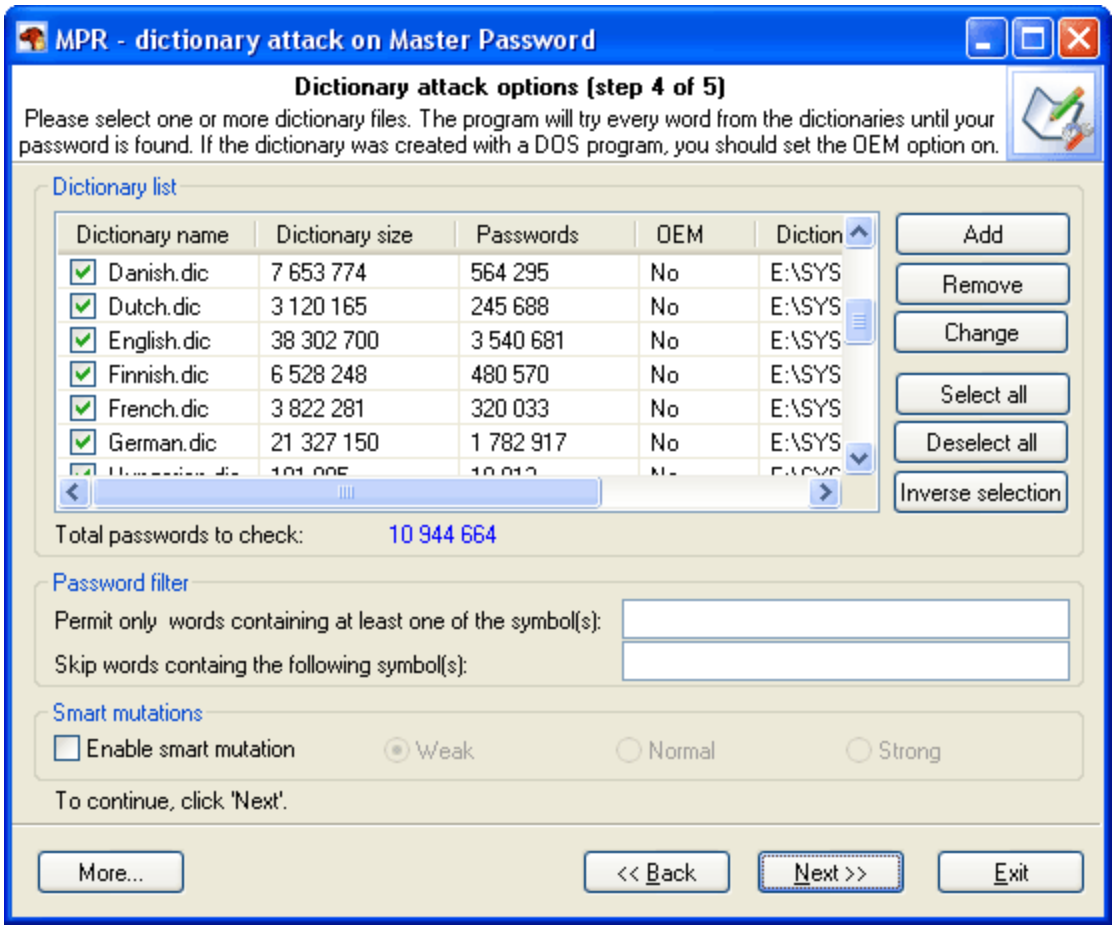
In the beginning of the attack, the program will search the system for all passwords it knows of. For that purpose, there are currently 32 mini modules for decrypting system, mail, browser, messenger, archive and other passwords. Then there goes the file and data indexation, along the course of which the program generates a potential attack dictionary. The third module breaks the passwords and words into pieces, out of which in the last module it will assemble new combinations for picking and guessing the original password.

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



2.4.3.3 Dictionary attack options

All options are conditionally split into three groups: **dictionary list**, **password filter**, and **password mutations**.



Dictionary list
In the first group of options, you must set at least one dictionary for the attack. If the dictionary was created with a DOS program, the option '*Dictionary file in DOS encoding*' must be selected when adding this dictionary to the list. After that, the new file will be added to the active dictionaries list. Please note: although a dictionary can appear on the list, it may remain inactive, i.e. not participate in the attack. To activate a dictionary, select the checkbox by its name. The program comes with a short English wordlist.

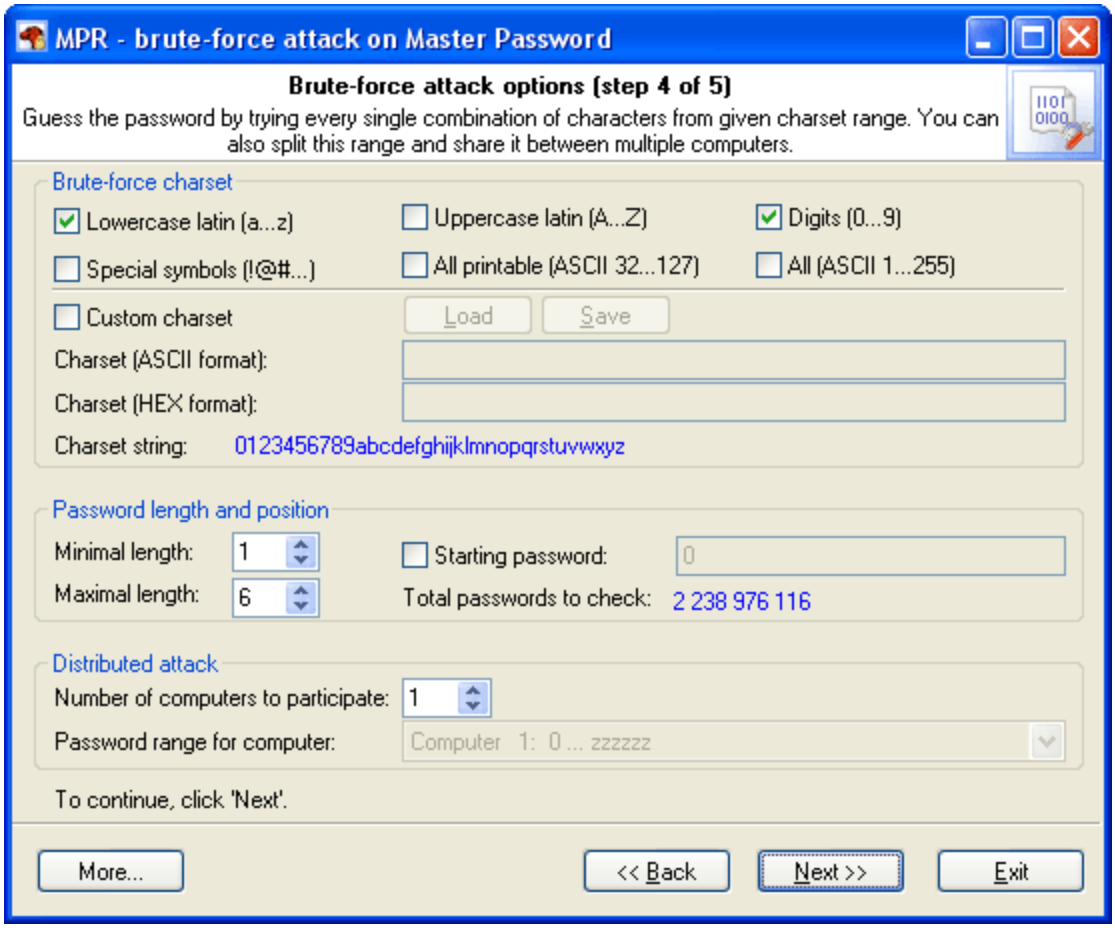
Password filter
To crop unnecessary passwords, you can use two simple filters. If you have set at least one character in the first '*Include*' filter, all passwords that do not contain that character will be ignored (skipped) by the program. The second '*Exclude*' filter is totally opposite. If you have set one or several characters in that filter, the program will skip passwords that contain at least one character specified in the filter.

Password mutations
The last group of options manages mutations for each password to be verified. You can set up to three mutation rules: *Weak* - less number of mutations and, in its turn, greater verification speed; *Strong* - for greater number of mutations, to the prejudice of the speed, and the happy medium, *Normal* option. Dictionary attack speed with smart mutations switched on is much slower then the normal mode (without mutations).
For *Weak* mutations - approximately 15 times slower.
For *Normal* mutations - ~ 50 times slower.

And for *Strong* mutations - ~130 times slower.

2.4.3.4 Brute-force attack options

As it was said above, this type of attack is the slowest. It must be used only if other attacks have failed to recover your password. There are 3 group of options here.

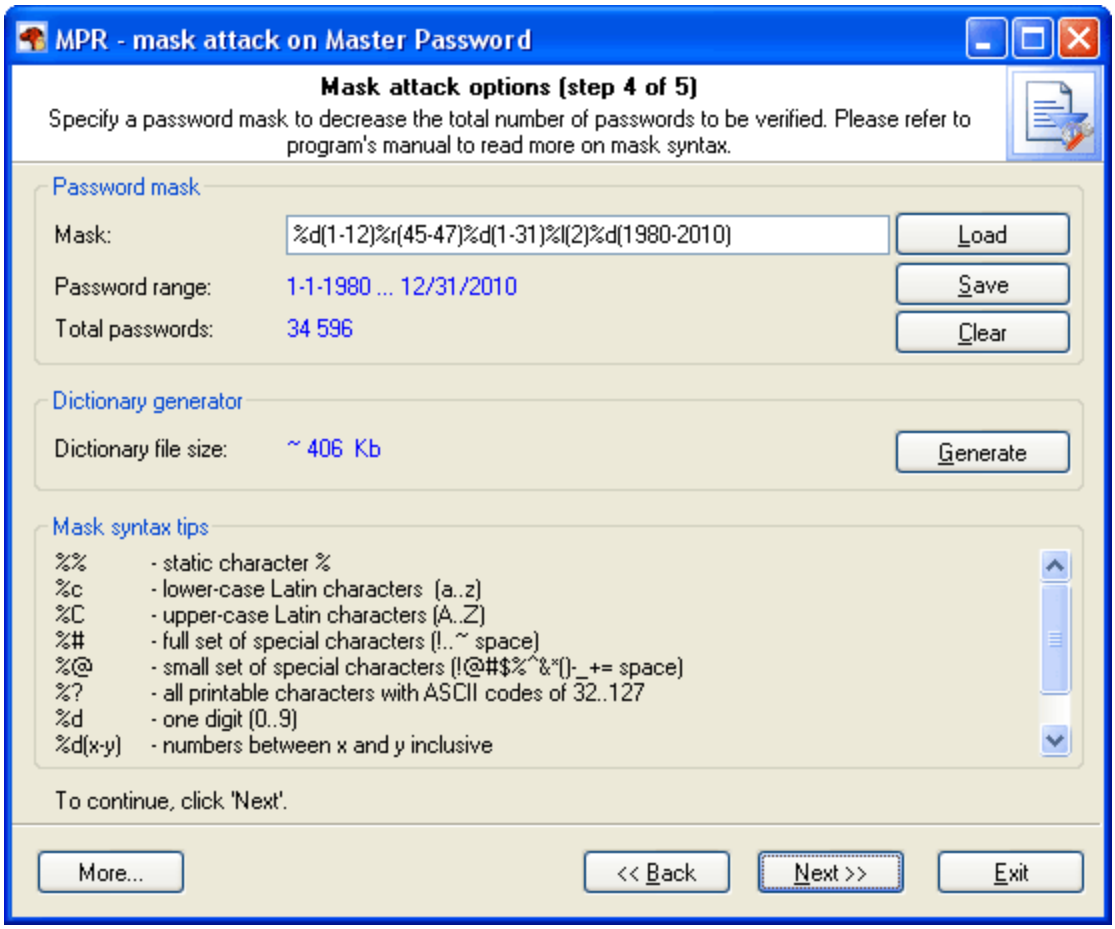


Brute-force charset
Brute-force attack assumes using all possible variations from the specified character range, which is set in the first group of options. You can select and combine predefined character sets (e.g., Latin characters, numbers or special characters) or define your own ones. To define your own character set, select the option '*Custom charset*'. This will enable two fields for defining a custom character set: the first one - for entering ASCII or OEM characters, second one - for entering non-printable characters. You can save your custom character set on disk. The program comes with several examples of user-defined character sets.

Password length and position
The second group of options allows setting the minimum and maximum lengths of the password to be generated. If the last brute-force attack was interrupted or stopped, you can resume it from the last position saved by the program (see '*Starting password*' option.)

Distributed attack
This group of options can be useful when you have access to several computers. In this case, the entire set of characters to be verified, if it is too large, can be split into portions and attack the password by portions on several computers at the same time. To implement that, you will need to select the number of computers participating in the distributed attack (option '*Number of computers to participate*'), select the same settings on all computers, and assign each computer its serial number (in the combo box '*Password range for computer*'.) When all that is done, you can launch the attack(s).

2.4.3.5 Mask attack options



The entry field is used for setting the mask (rule), by which the program will try to recover the password. If the mask is set correctly, below you will see the range of characters generated by the mask. User-defined masks can be saved on disk. The program also allows generating dictionary by mask; however, this option is only available in the registered version of the program.

The password mask consists of static (not changing) characters and special sets - dynamically changing letters, numbers or symbols.
For example, in the mask '**secret%d(1-100)**', the characters '**s**' '**e**' '**c**' '**r**' '**e**' '**t**' are static, and '**%d(1-100)**' is the dynamical set. A dynamical set is marked (start) with **%** character.
The program supports the following dynamical sets:
%c - lower-case Latin characters (a..z), total 26 symbols

%C - upper-case Latin characters (A..Z), total 26 symbols
%# - full set of special characters (!..~ space), total 33 symbols
%@ - small set of special characters (!@#$%^&*()-_+= space), total 15 symbols
%? - all printable characters with ASCII codes of 32..127
%d - one digit (0..9)
%d(x-y) - numbers between x and y inclusive
%r(x-y) - user-defined characters with serial ASCII codes between x and y
%r(x1-y1,x2-y2...xn-yn) - set of several non-overlapping sequences of ASCII characters. Useful for defining custom character sets; e.g., of OEM characters.
%l(n) - link to another set from mask (1 based)
%% - standalone static character %

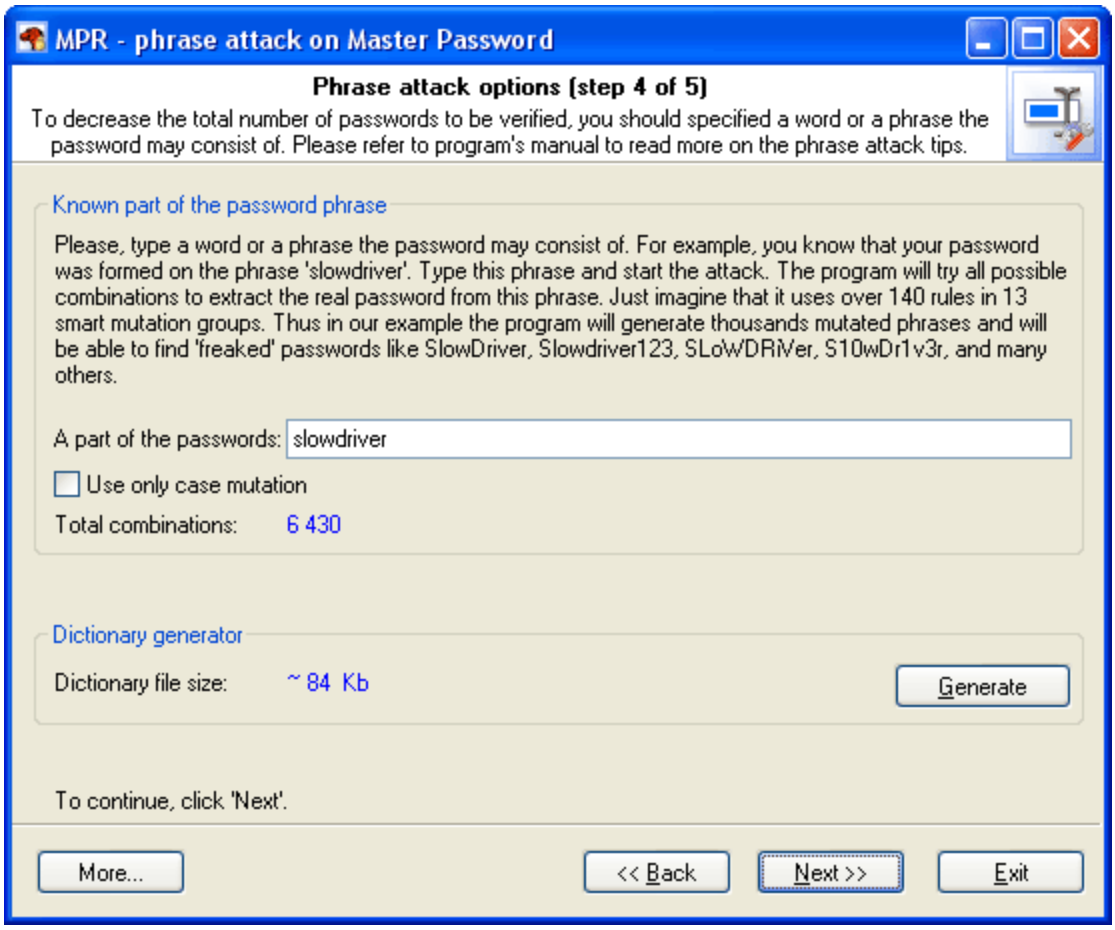
%r allows setting character sets for national languages. For instance, the mask **%r(160-175,241-241,224-239)%r(160-175,241-241,224-239)** will generate the password row of Russian characters, total 33*33=1089 passwords.

Examples:
test%d - will generate password range test*0*..test*9*, 10 passwords total
test%d(1980-2007) - test*1980*..test*2007*, 28 passwords
test%r(48-57,97-122) - test*0*..test*z*, 36 passwords
%#test%# - _test_..~test~, 1089 passwords
%d(1-12)%r(45-47)%d(1-31)%l(2)%d(1980-2010) - *1-1-1980..12/31/2010*, 34596 passwords
%c%r(32-63)%c%l(2)%c%l(2)%c - *a_a_a_a..z?z?z* - 14623232 passwords

Important! When setting %r, keep in mind that the range of defined OEM characters (with character code greater than 127) is generated using the DOS encoding.

2.4.3.6 Base-word attack options

Base-word attack is an irreplaceable recovery tool when you know a portion of the password or its basic component.



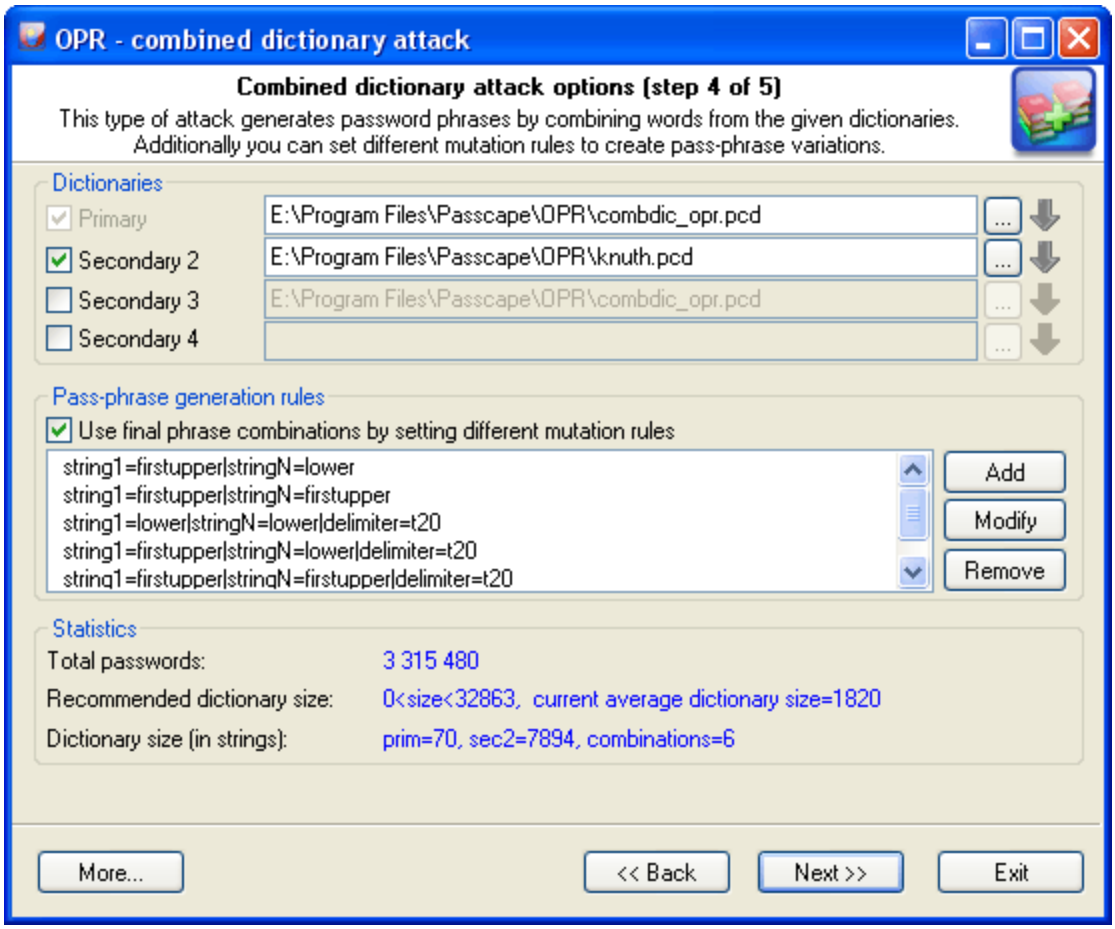
Normally, such cases dispose to using mask attack; however, it does not always allow coping with the task set forth. Suppose our password was '**S10wDr1v3r**'.
Trying to recover such a complicated password using brute-force attack would be an ungrateful job, even if you are quite sure that it is based upon the '**slowdriver**' phrase. These are the cases when the base-word attack will rescue you.

With this tool, the program will attempt to recover the original password, trying all possible combinations founded upon 15 groups of rules (total over 150 rules.)
If you enter '**slowdriver**' in the field, you will see that the program has generated several thousands of different combinations upon this phrase , and one of those combinations will match our password.

Enter the word or pass-phrase prototypal to your password.
Important! If the length of the phrase exceeds 8-10 characters, the mutation may take significant time.
If you remember the original password precisely and simply have forgotten the sequence of the upper-case and lower-case characters in it, you can select the option '*Use only case mutations*'. With this option selected, the program will generate passwords with all possible combinations of upper-case and lower-case characters, total 2^n passwords, where n - is password length. For example, for the password '*slowdriver*' the program will generate 2^10=1024 different combinations.

2.4.3.7 Combined dictionary attack options

This type of attack on difficult and compound passwords is very similar to the simple dictionary attack, except that instead of using a single word for password verification here we use a combination of words or a phrase created by combining words from specified dictionaries.



The purpose of the first group of option is to set and choose the source material for our attack. For a start, we are to specify at least 2 dictionaries. To understand how the combined attack works, let's take a look at a couple of password generation examples that involve, in the first case, the same dictionary and in the second case – two different ones.

1. Suppose we've got a single dictionary with three words: aaa, bbb, and ccc. We will set this dictionary as two original sources: primary dictionary & secondary dictionary2 (see the figure). After these dictionaries have been processed, at the output we have the following phrases (they will be used when checking the password sought):
'aaa aaa', 'aaa bbb', 'aaa ccc'
'bbb aaa', 'bbb bbb', 'bbb ccc'
'ccc aaa', 'ccc bbb', 'ccc ccc'.
9 phrases total.

2. In the second case, we have got two different dictionaries. For example, the first dictionary consists of three words: aaa, bbb, and ccc. The second one also has three words: ddd, eee, fff. In this case, we are going to have the following phrases:
'aaa ddd', 'aaa eee', 'aaa fff'

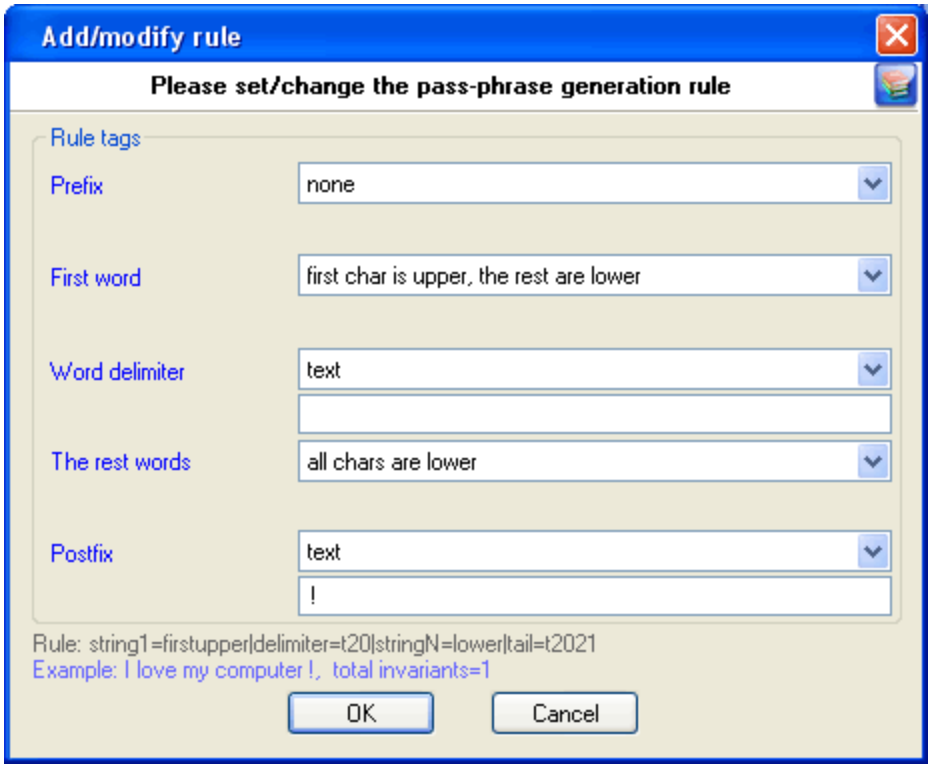
'bbb ddd', 'bbb eee', 'bbb fff'
'ccc ddd', 'ccc eee', 'ccc fff'.

The example is plain but demonstrative. The idea is that for multiple sources you can successfully use both a single dictionary and multiple ones. It all depends on your imagination. The last example shows that a special attention should be paid to the order of the dictionaries if they are different. The order of the words in the phrases to be created depends directly on the order of the source dictionaries. In our second example, if we swap the primary and the secondary dictionaries, at the output we will obtain a completely different set of phrases:
'ddd aaa, 'ddd bbb', 'ddd ccc',
'eee aaa, 'eee bbb', 'eee ccc',
'fff aaa, 'fff bbb', 'fff ccc'.

Combined attack sets a certain limit to the number of dictionaries that can be used; that's not more than 4. Thus, the general limitation of this attack is that only password phrases of not more than 4 words can be recovered using this attack.

Another essential drawback is the wide range of phrases generated. And, as the consequence, the proportional increase of the time spent on the validation of a password. Therefore, you should be careful when selecting the size of source dictionaries, especially for 3 and 4-word combinations.

The next group of options is in charge of creating all possible combinations of phrases. By default, if no password generation parameter based upon mutation rules is set, the program will create passwords by simply concatenating words from the source dictionaries, WITHOUT separating them with spaces. However, you can set your rules as well. For example, have it create phrases with spaces, begin words with caps, append numbers, etc. There are special rules available for this purpose; you don't have to know the syntax of them, for the mutation rule creation dialog is simple and intuitive.



Each mutation rule consists of five elements:

1. **Prefix** – text that will appear before each phrase. This element can be a character, plain text string, one digit between 0 and 9 or a number. For instance, if you set a one-digit prefix, the phrases created with this rules will look as follows: '0 aaa bbb', '1 aaa bbb' … '9 aaa bbb'.
2. **First word** – the action to be performed over the first word of each phrase. There are only four options. Namely: leave intact as is in dictionary, convert all characters to lowercase, convert all characters to uppercase or capitalize only the first letter of the word.
3. **Word separator**. It may be absent. Then all the words will be concatenated. Example: 'aaabbb', 'aaaccc','aaaddd', etc. You can otherwise set a custom separator; e.g. the '-' character: 'aaa-bbb', 'aaa-ccc','aaa-ddd'.
4. **Other words**. With this attribute, similarly to 2., you can set rules for the other words of a phrase.
5. **Postfix** – text that will finalize each phrase. For example, if you set Postfix to the '?' or ' ?', all phrases created with this rule will have the question mark at the end.

Naturally, the more mutation rules you set, the wider is the range of phrases you generate, and the more chances you get for the successful recovery of the original password. On the other hand, if the range is large enough, when searching through the entire range may take half an hour or more, the program will highlight the statistics text with red color. There's no reason to be afraid of that. Simply select one of the source dictionaries of a smaller size or decline from some mutation rules or, leave everything the way it is.

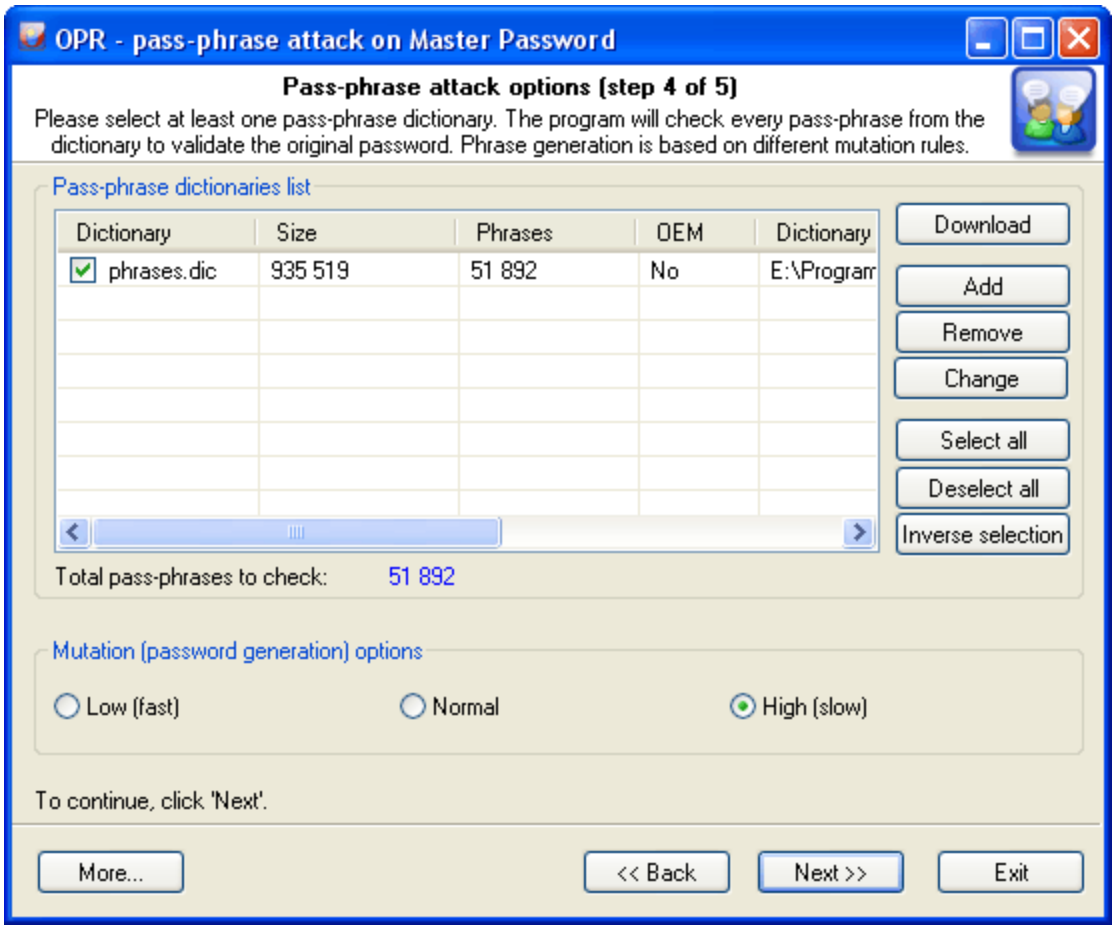
The 'Statistics' group shows the average and recommended average size of a dictionary, number of words in source dictionaries, total number of passwords being generated and other helpful information.

Let's take a look at a specific task. Suppose, we are to find a password of three words, the first one of which is 'nothing' with some punctuation mark at the end. Here is our plan:

You can also download additional dictionary modules from the Passcape Software Web site.

2.4.3.8 Phrase attack options

Pass-phrase attack is an essential password recovery tool, which can hardly be overestimated. The idea of the attack is to guess the right password by searching through predefined frequently used expressions, phrases and word combinations. Similar to the simple dictionary attack, from the source dictionary we sequentially take a phrase and attempt to match with the original password.



More and more users choose to make up their pass phrases of entire phrases, passages from poems, movie aphorisms, Latin aphorisms, etc. Attempting to recover such passwords using the traditional techniques is unthinkable, even with the reference to the advancement of the computing power of modern computers. Therefore, the recovery help comes with the predefined and known phrase attack.

It wouldn't be an overestimation to say that 99 percent of the success in the recovery of a password with a dictionary attack depends on the quality of the dictionaries. Most likely, that is the reason why this type of attacks doesn't appear in just about any password cracker. Passcape Software allows utilizing a whole set of online and offline dictionaries (totally over 500 MB) compiled specially for this type of attack.

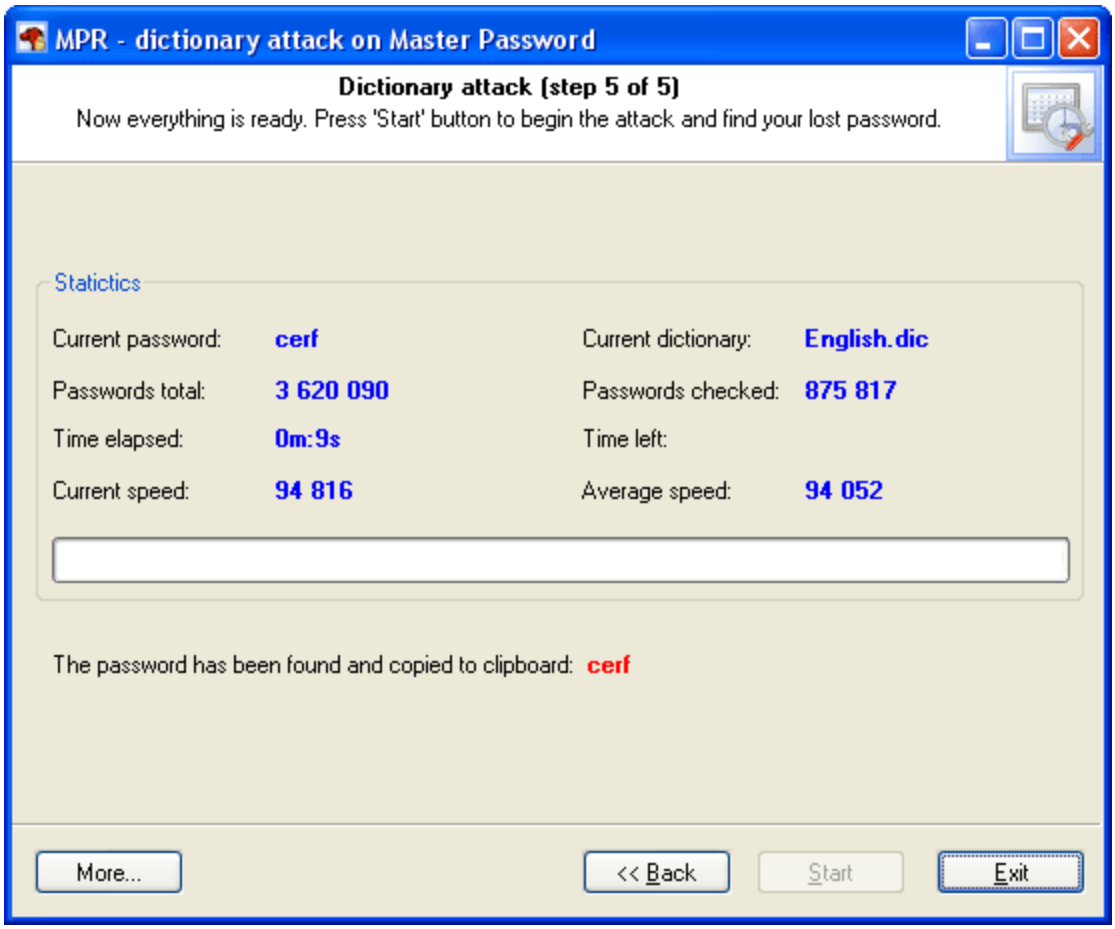
The password-phrase attack options almost completely repeat the simple dictionary attack options: here, you also are to select one or several dictionaries for the phrase source, it also allows loading additional dictionaries from the Passcape website, and it has the same way for setting phrase mutation rules (creating alternative options).

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

The program comes with a short dictionary of phrases and aphorisms.

2.4.4 Launching the selected attack

The last step of the password recovery wizard launches the attack you have selected and gathers and displays its statistics. Click '*Start*' to launch the attack.



Please keep in mind that if you have selected a pretty long phrase (in the phrase attack), the preparation to the attack may take some time. Other than that, if the option '*Check frequently used passwords before each attack*' is selected, the program will attempt to find the password among the most frequently used words and phrases. That normally takes less than a minute.

Later, if the password you were looking for is found, the program will notify you of that with the alert you have specified and copy the password to clipboard.
At this moment, the speed of the search of Mozilla's/SeaMonkey's/Firefox's/Thunderbird's Master Password is really insignificant - just about 150 000 passwords/sec on a modern computer. Probably we will improve the decryption speed in the nearest future.

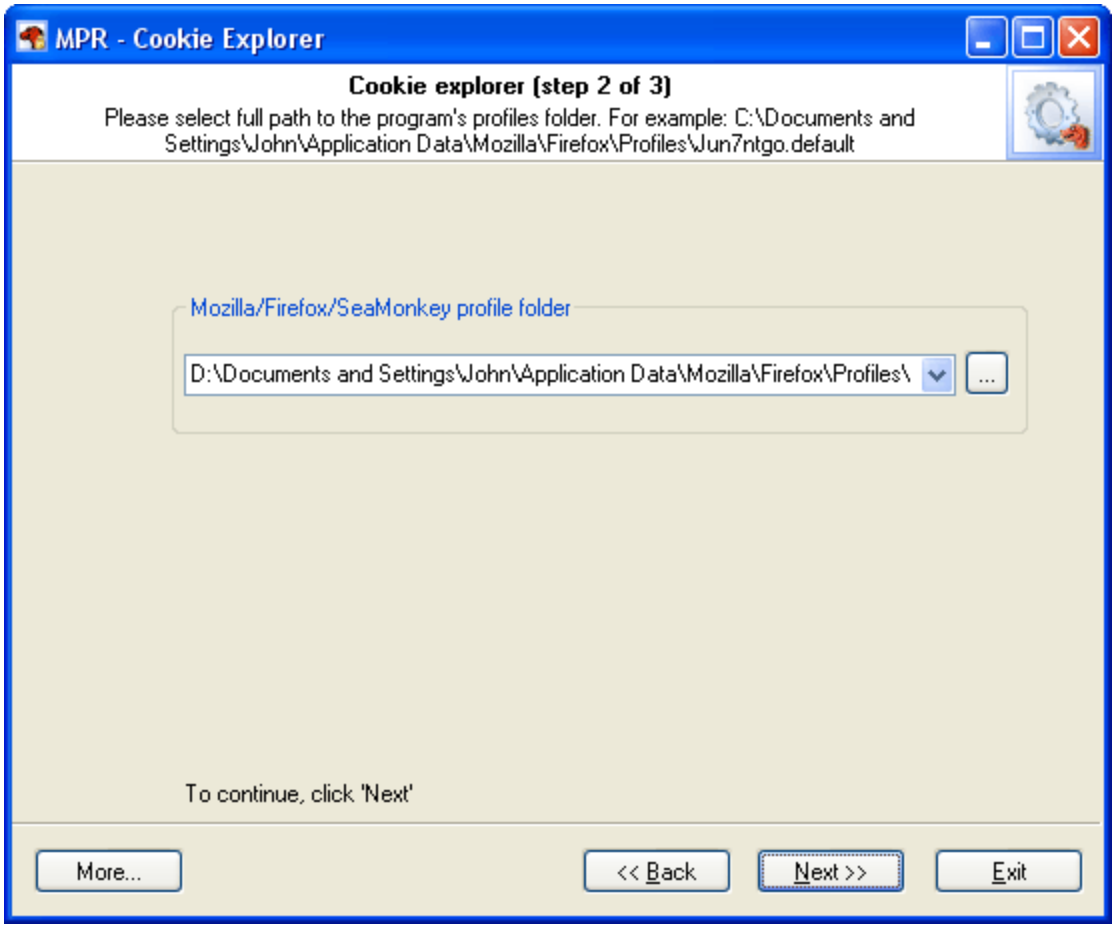
2.5 Cookie Explorer

A cookie is a text file stored on your computer by a web server. This value of a variable that a website sets. If the lifetime of this value is set to be longer than the time you spend at that site, then this string is saved to file for future reference. Cookies were developed to help users to navigate visited sites. But often cookies criticized for weak security and inaccurate user identification. You can read more information about cookies from Microsoft Web site or from Wikipedia.

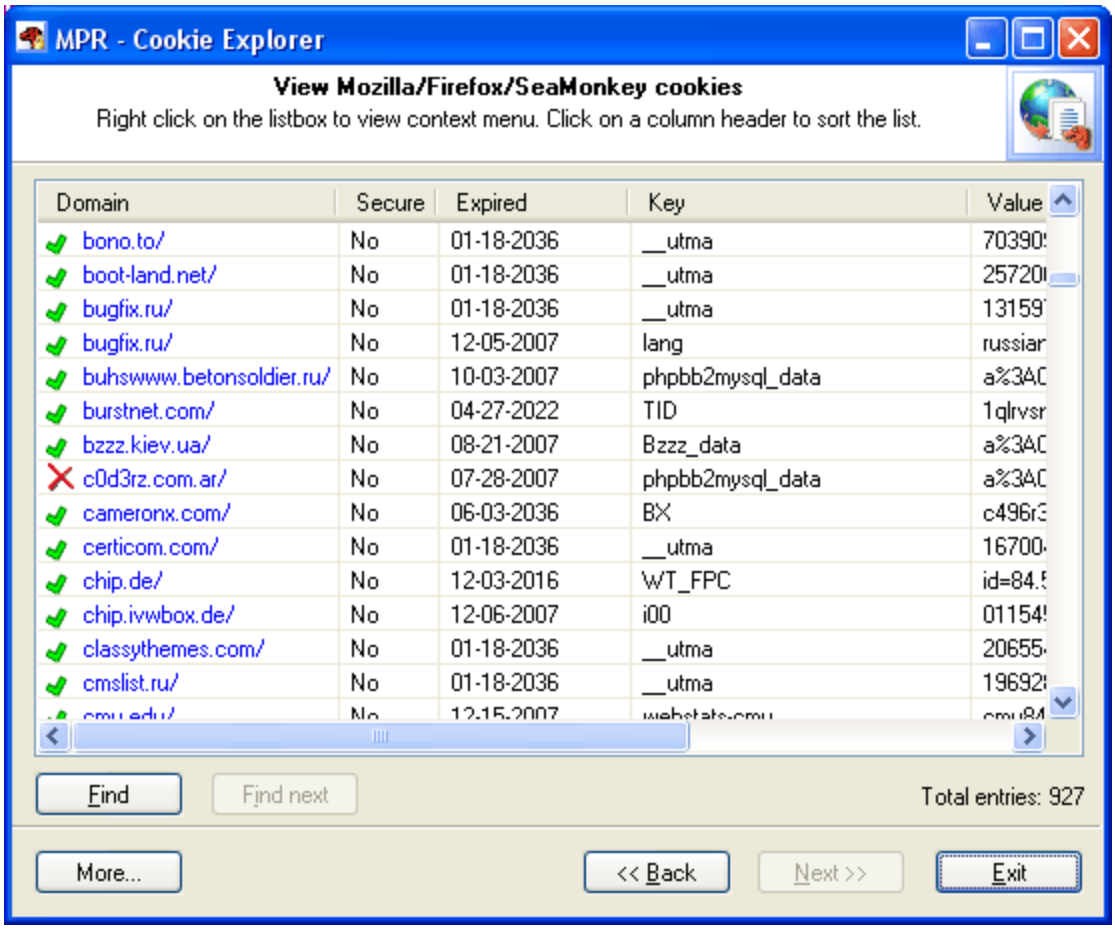
Cookie Explorer is a new feature that was added to **MPR** v2.4 to help you to navigate through the Mozilla/Firefox/SeaMonkey stored cookies. To start browsing cookies, you'll have to show a full path to your Mozilla/Firefox/SeaMonkey profile folder (a folder with the **cookie.txt** file in it). Typically this path should look like this:

- Mozilla and SeaMonkey browsers: C:\Documents And Settings*%USERPROFILE%*\ApplicationData\Mozilla\default*%PROFILEFOLDER%*
- Firefox: C:\Documents And Settings*%USERPROFILE%*\ApplicationData\Mozilla\Firefox\profiles*%PROFILEFOLDER%*

Some examples:
C:\Documents And Settings\John\ApplicationData\Mozilla\Firefox\profiles\js786alk.default
C:\Documents And Settings\kate\ApplicationData\Mozilla\default\6sn16oa4.slt



Select a profile folder from the drop down list and click *Next* to view locally stored cookies.

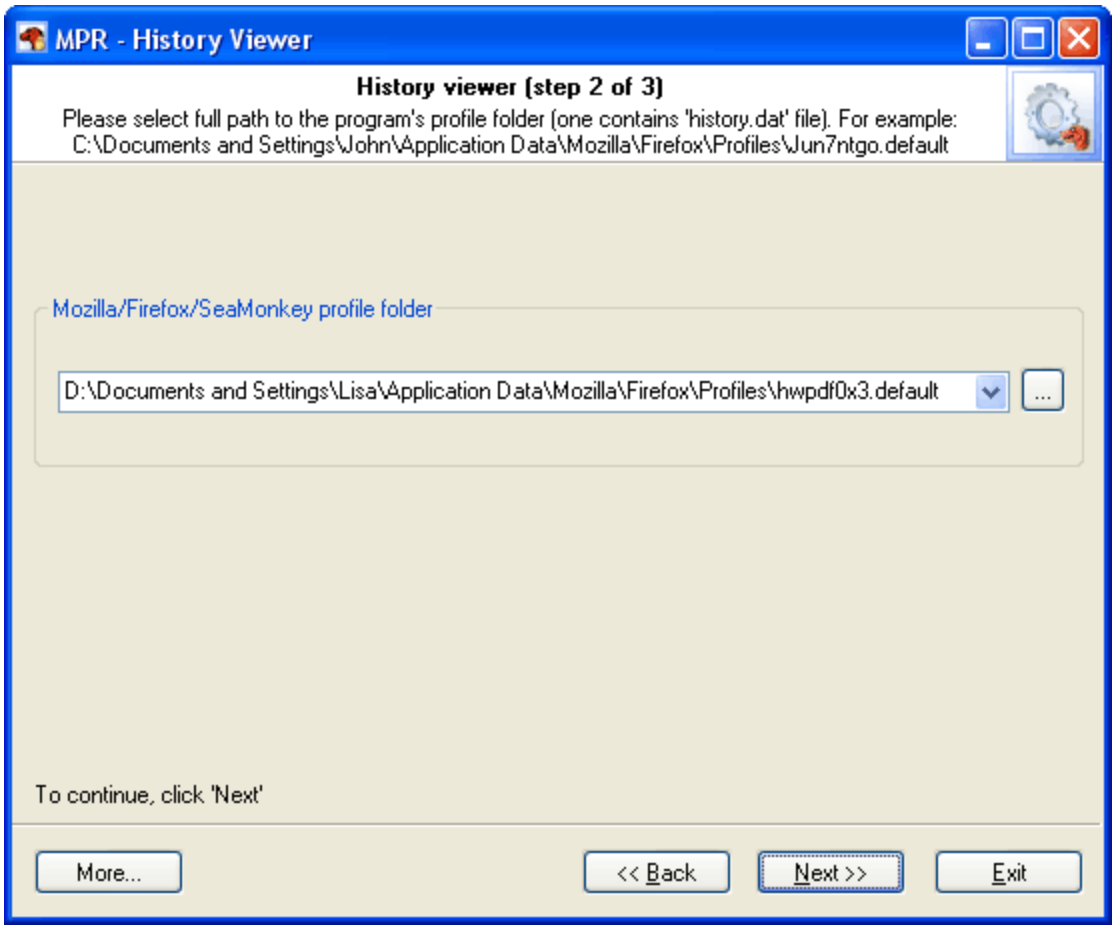


Tip. Click the listbox header to sort the cookies list.

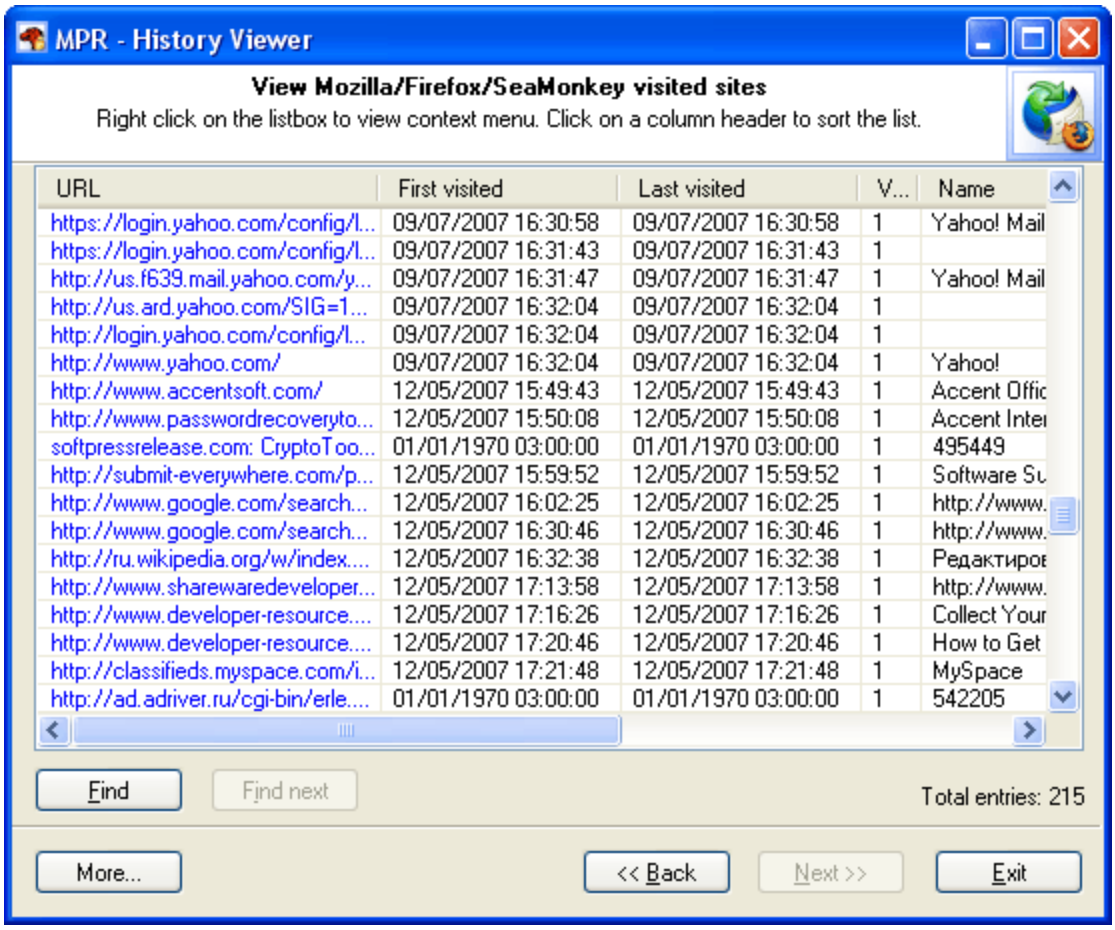
2.6 History Viewer

All browsers save Web pages, visited or simply typed URLs to your hard drive. Thus anyone who gain access to your PC can easily tell where you have been browsing over the network or what you have been searching for. The **History Viewer** shows typed and visited sites and Web pages, sorts them in various orders, and allows to remove them completely from your local computer. This feature was added to MPR v3.0

To view the Firefox/SeaMonkey/Mozilla URL history, you'll have to specify the full path to your browser profile folder (one with the **history.dat** file in it) first. Like this:
For Mozilla or SeaMonkey: C:\Documents And Settings\%USERPROFILE%\ApplicationData\Mozilla\default\%PROFILEFOLDER%
For Firefox browser: C:\Documents And Settings\%USERPROFILE%\ApplicationData\Mozilla\Firefox\profiles\%PROFILEFOLDER%
Some examples:
C:\Documents And Settings\John\ApplicationData\Mozilla\Firefox\profiles\jb7t6a4n.default
C:\Documents And Settings\Ann\ApplicationData\Mozilla\default\d23pd4a1.slt



After selecting/setting a profile folder, click *Next* to parse and view your browser history.



Tip. To sort the history list, click the listbox column header.

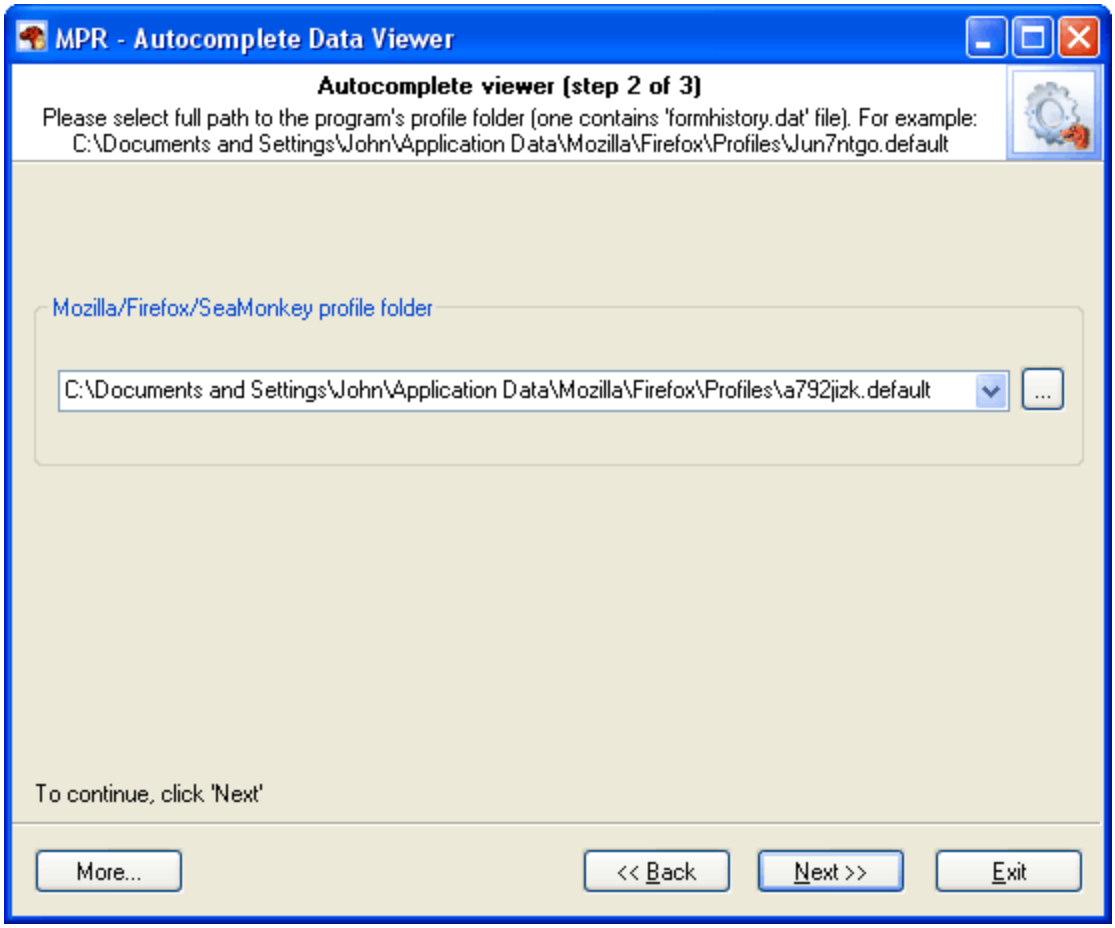
2.7 Autocomplete Data Viewer

Mozilla's Autocomplete feature remembers and saves previous entries you've made for Web addresses, forms, and passwords. Then, when your type information in one of these fields, Mozilla/Firefox/SeaMonkey suggests possible matches for this field. These matches can include your typed in data, stock quotes, search queries, or any other personal information you have ever filled in on a Web page, even your credit card numbers.

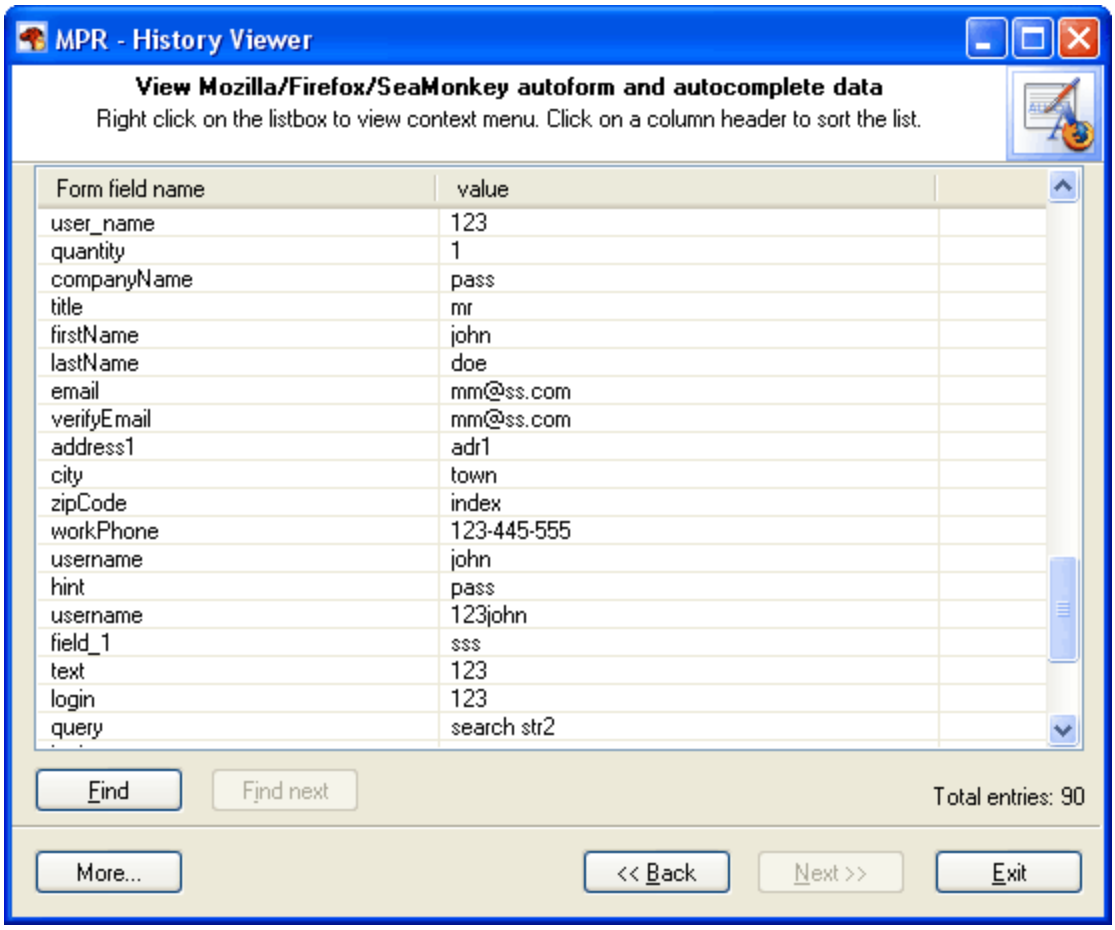
Autocomplete data viewer is a feature to decrypt and view the autocomplete data for Web pages and forms you've ever saved in your Firefox/Mozilla/SeaMonkey browser. With this feature you can as well remove your personal information if it is not needed anymore, to prevent yourself from being a victim of a potential hacker.

First, you'll have to set up your browser's profile folder (one with the **formshistory.dat** file in it), or select one from the drop-down menu. The profiles folder may looke like this:
Firefox: C:\Documents And Settings\%USERPROFILE%\ApplicationData\Mozilla\Firefox\profiles\%PROFILEFOLDER%
Mozilla or SeaMonkey: C:\Documents And Settings\%USERPROFILE%\ApplicationData\Mozilla\default\%PROFILEFOLDER%
Some examples:

C:\Documents And Settings\John\ApplicationData\Mozilla\Firefox\profiles\jb7t6a4n.default
C:\Documents And Settings\Ann\ApplicationData\Mozilla\default\d23pd4a1.slt

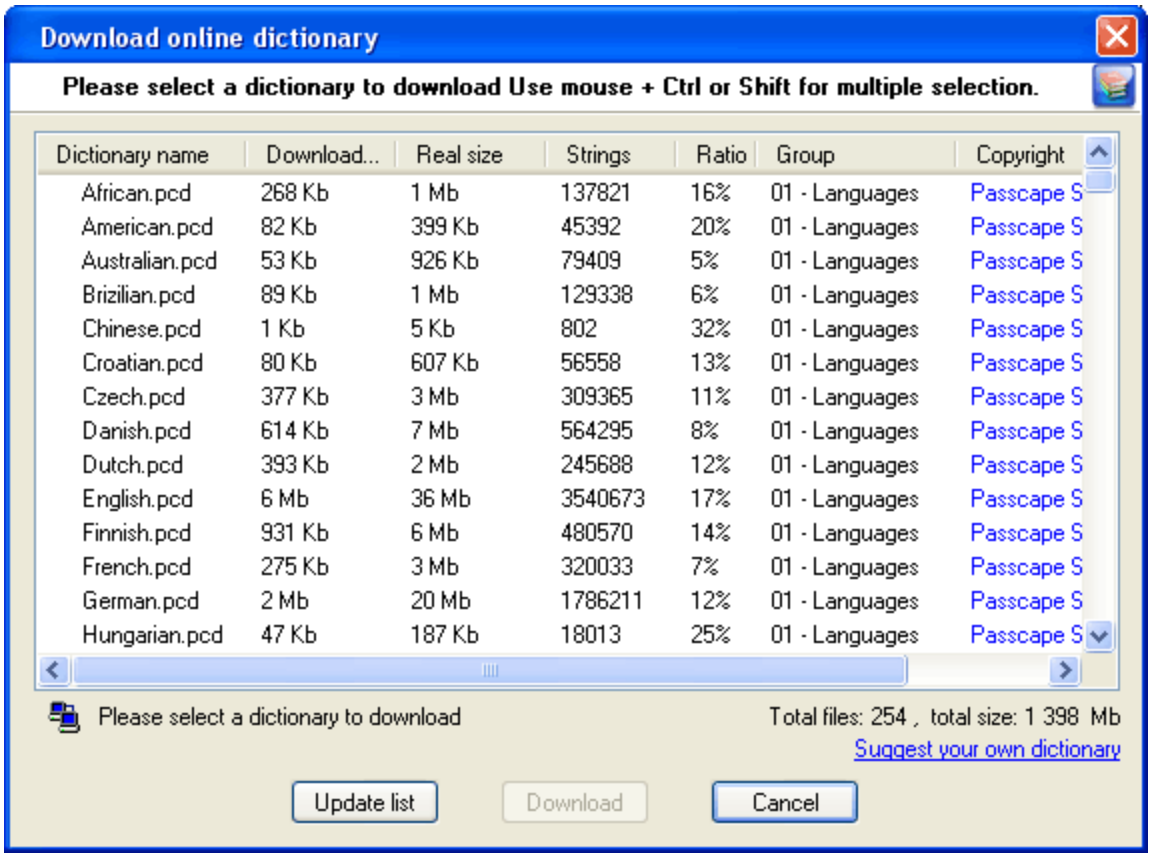


After setting up a profile folder, click *Next* to decrypt and view your browser autocomplete data.



2.8 Loading online dictionaries

The online dictionary selection dialog is extremely simple. When it opens up, the program attempts to establish a connection with the Passcape Software server and then retrieves and displays the list of dictionaries available for downloading.



For more convenience, you can order the list by name, size of source or compressed file, group it belongs to, etc.

Select the dictionary you need and then click on the 'Download' button to retrieve it and use in the program.

Some of the dictionaries are large. For instance, the size of 'music_songs.pcd' is more than 59 MB in the compressed format. Naturally, retrieving such a large amount of data may take some time, which depends upon file size, bandwidth of your Internet connection and net load.

All online (and some additional) dictionaries can be ordered on CD. The total size of all the dictionaries is over 1GB. You can also share your own dictionary with us by e-mailing us the dictionary or the link where it can be downloaded.

2.9 Recovering Master Password

When recovering certain types of passwords - for instance, Firefox Master Password - the major question is: How to organize the recovery process - which attack should I start with to raise the probability of its successful completion?

For choosing the type and the sequence of the attacks, we advise to follow this algorithm, which is applicable in the majority of cases to all types of passwords to be recovered:

- First, enable the preliminary attack option, if it is available. It will help to recover simple and frequently used combinations.

- Second, if you are aware of any specifics of the password you are looking for, it's better to try mask attack or base-word attack first. Specifically, if you know a part of the password - using mask attack would be more effective. If you know the basic component of the password or, for example, know the password but don't remember the sequence of caps and lowercase characters in it, base-word attack would do the job better.
- Third, if you have no information on the password you are looking for, which occurs most frequently, be guided by the following sequence of steps:
  1. Run AI attack with mutation and indexing options set to light.
  2. If it fails to find the password, just try again and set mutation option to 'normal' and indexing to 'deep' levels.
  3. Launch dictionary attack with the mutation option disabled.
  4. Launch dictionary attack with the mutation option enabled; the depth of mutation depends on the amount of available time and the attack speed. When searching for passwords typed in the national keyboard layout, the depth of mutation should be set to strong.
  5. Select and download online dictionaries and repeat steps 3 - 4.
  6. Launch pass-phrase attack with the mutation option disabled.
  7. Launch pass-phrase attack with the mutation option enabled and set to the maximum productivity. This will allow finding passwords typed in the national keyboard layout.
  8. Select and download online pass-phrase dictionaries and repeat steps 6 - 7.
  9. Launch combined dictionary attack with defined phrase generation rules.
  10. Select and download online dictionaries for combined attack and repeat step 9.
  11. Select a charset for brute-force attack, launch the attack.
  12. If necessary, select a new or complete the old character set and repeat the brute-force attack; i.e. step 11.

2.10 Setting a Program Access Password

Setting an access password can help to avoid the program execution by unauthorized persons. To open the "Set Access Password" dialog box, click '**more...**' (in the **MPR** main window) and select '**Set/change access password**' from the popup menu.

To set an access password, you have to enter a new password and confirm it by retyping it in the confirmation field.
Remember! The access password is case-sensitive.

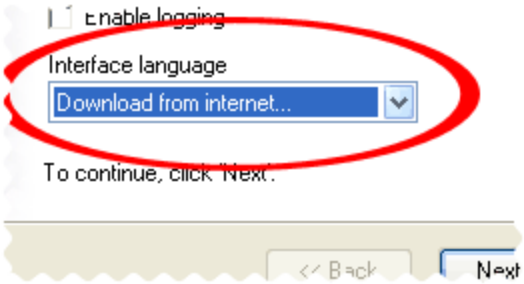
To remove the current password, leave the password fields blank.

Next time you run the program, you will be asked for the password as shown below:

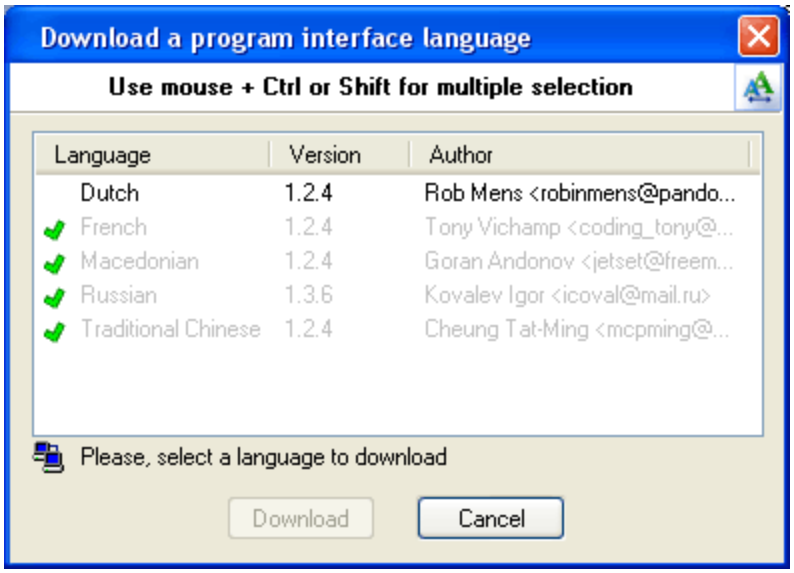
Type in your current password and click **OK** to run the program.

2.11 Program Interface Language

You can change the program interface language and download your native language from our web server. Just select **Download from Internet...** from the **Interface Language** drop-down list as shown below.



After that the program will try to establish a connection to the Passcape server and download the list of language files available for the program. We guarantee that nothing will be sent to Passcape (or to anybody else) from your computer.
So you'll see the language selection dialog box where you can select an interface language and download it.



Already downloaded and installed languages are marked with ✔ sign.

If you can translate the interface of the program into some other language, your help will be really appreciated. Translate the program into your native language and get the program registration for free! Contact us for more information.

License and registration

3 License and registration

3.1 License Agreement

==========
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 "Mozilla 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 within a single site. A multi site license authorizes you to install and use the SOFTWARE to any number of computers belonging to your organization - no matter where they are located.

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

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

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

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

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

3.2 Registration

You can order fully registered version of **MPR** at a cost of $27 for non-commercial personal usage, $54 for business or $370 for multi site license.

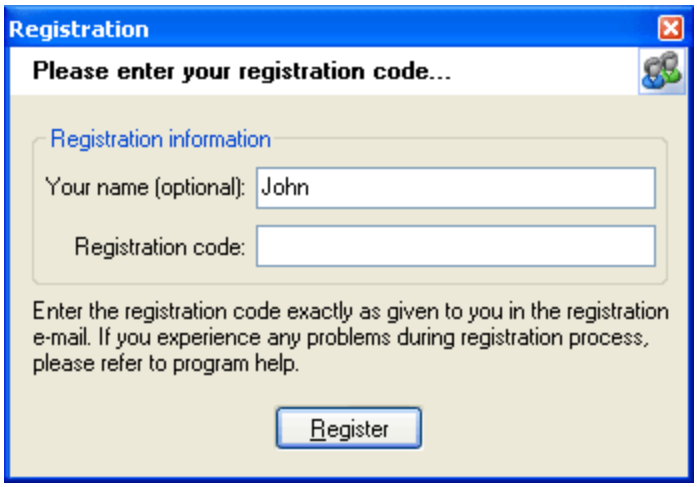
Detailed instructions for all kinds of orders are available online at Passcape ordering page. Online orders are fulfilled in just a few minutes 24 hours a day 7 days a week.

On payment approval (for online orders, usually within a few minutes), we'll send you the registration code which will remove all limitations of the unregistered version. Your registration will be valid for all future versions of **MPR**.

The ordering pages are on a secure server, ensuring that your confidential information remains confidential. As soon as your order is processed (usually in one business day for on-line payments), you will be provided with the registration code for your copy of the program. If you've made a payment, but haven't received a confirmation letter with your registration code within a reasonable amount of time (two business days for credit card payments or two weeks for other payments), please notify us!

Important: when completing the order form, please double-check that your e-mail address is correct. If it will not, we'll be unable to send you the registration code.

To complete the registration process
- Run the program
- Click **more...** button
- Select **Registration** from the popup menu
- Enter your registration code and name (optional) into the related fields and click the **Register** button.



It is recommended to use the Copy and Paste commands instead of typing the code by hand. To do that, select the license key text in the registration message you have received with the mouse or using the text selection keyboard shortcuts (**Shift + arrow keys**). Then press the **Ctrl + Ins** shortcut on the keyboard to copy the selected block to Windows' Clipboard. Then open the registration window in the program, place the cursor in the registration key field and then press the **Shift + Ins** shortcut on the keyboard to paste the text from clipboard to that field. Next, place the cursor in the user name field, enter your name and then click on the **Register** button. If you have done everything right, the program will display the confirmation message.

3.3 Limitation of unregistered version

An unregistered version of **Mozilla Password Recovery** shows only first 3 characters of the decrypted passwords and has some functional limitations.

Technical support

4 Technical support

4.1 Reporting problems

If you have a problem, please contact us at support@passcape.com. Please inform us about the following:

- Windows version including service packs and other fixes installed
- Program full version (see **About** dialog)
- Program registration information if any
- Detailed description of your problem (as much information as possible)

If you're reporting about program error, please attach **Crash.log** and **Mpr.log** files located in the **Mozilla Password Recovery** installation directory.

4.2 Suggesting features

If you have any questions, comments or suggestions about the program or would like more information, email us at: info@passcape.com. Please don't forget to mention the program name and version. Also make sure you have the latest program version installed. Your feedback helps us to improve our products and work more effective.

4.3 Contacts

Please don't hesitate to send your questions regarding our products to e-mail support@passcape.com. You will get reply during one or two days. Note, that registered users have priority in technical support.

If you experience any problems during registration process, please send a letter to sales@passcape.com
We will be happy to assist you with the registration.

Please write in English!

You can find other password recovery utilities at https://www.passcape.com.