

Network Password Recovery Wizard

USER MANUAL

**Copyright (c) 2021 Passcape Software. All rights reserved.
Passcape Software**

1.	Introduction	4
1.1	About the program	5
1.2	Features and benefits	5
1.3	System Requirements	5
2.	Working with the program	7
2.1	Main window	8
2.2	Manual mode for network connections passwords	8
2.3	Recovered network connections passwords	9
2.4	Manual mode for network credentials	11
2.5	Recovered network credentials	12
2.6	Domain cached passwords	12
2.7	Manual mode for wireless network keys	15
2.8	Recovered wireless keys and passwords	17
2.9	Manual mode for remote desktop passwords	20
2.10	Recovered RDP passwords	22
2.11	Decrypting Windows CardSpace (formerly InfoCards)	23
2.11.1	Selecting data source	25
2.11.2	Reading system credentials	26
2.11.3	Decrypting system's Master Key	27
2.11.4	Decrypting user's Master Key	28
2.11.5	Decrypting InfoCard public data	28
2.11.6	Decrypting InfoCard PIN	29
2.11.6.1	Choosing recovery method	31
2.11.6.2	Setting recovery options	32
2.11.6.2.1	Preliminary attack	33
2.11.6.2.2	Artificial Intelligence attack	34
2.11.6.2.3	Dictionary attack options	36
2.11.6.2.4	Brute-force attack options	37
2.11.6.2.5	Mask attack options	38
2.11.6.2.6	Base-word attack options	39
2.11.6.2.7	Combined dictionary attack options	41
2.11.6.2.8	Phrase attack options	43
2.11.6.3	Launching the selected attack	45
2.11.7	Decrypted private data	45
2.12	Asterisks password revealer	47
2.13	Server emulators (POP3, IMAP, SMTP, FTP, NNTP)	49
2.14	Recovering passwords from hashes	52

2.15	Loading online dictionaries	53
2.16	Setting a Program Access Password	54
2.17	Program Interface Language	55
3.	License and registration	57
3.1	License Agreement	58
3.2	Registration	59
3.3	Limitation of unregistered version	60
4.	Technical support	61
4.1	Reporting problems	62
4.2	Suggesting features	62
4.3	Contacts	62
Index		63

Introduction

1 Introduction

1.1 About the program

Network Password Recovery Wizard is a Windows network password recovery program. The range of passwords recoverable by the program is quite wide. NPRW can recover the following types of passwords:

- Network connections passwords, which include Dialup (RAS), VPN, Direct PC, and other passwords.
- Local area network and Internet connection passwords. This category covers stored passwords for accessing other computers within your LAN, Internet Explorer passwords for protected Web sites, other passwords stored by Windows Credential Manager. For example, Exchange server's e-mail passwords, .NET Passport accounts in MSN Messenger, etc.
- Domain cached passwords
- Passwords and keys for accessing wireless networks. NPRW literally "picks out" wireless network passwords from all available places: configuration data stored on USB disk, configuration data saved by Windows Wireless Network Setup Wizard, and from connections data stored in Windows registry.
- Remote Desktop passwords.
- Asterisks (****) passwords
- Mail/FTP/News passwords of any programs (by emulating POP3, IMAP, SMTP, NNTP or FTP server)
- CardSpace (InfoCard) public, private data and PINs.

The program's interface is simple. NPRW can operate automatically, not requiring any special knowledge from you, and under your control (great for advanced users), allowing you managing the recovery process on your own. This approach would be great for recovering passwords from your old accounts data.

1.2 Features and benefits

With this program you can:

- Recover the most of Windows network passwords
- Choose between two (automatic and manual) recovery modes
- Export passwords to text html or excel files
- Prevent an unauthorized program execution

1.3 System Requirements

Requirements

Windows® NT+, less than 6Mb on your hard drive.

You need administrator privileges in order to run the program in automatic mode.

Restrictions

- It is required Windows XP or higher to recover passwords stored by Windows Credential Manager.

- To use Remote Desktop, you need a computer running Windows XP Professional with a connection to a LAN or the Internet.
- To recover wireless keys/passwords it is required Windows XP Service Pack 2 and Wireless Zero Configuration service running.
- WPA-PSK passwords (as well as InfoCard PINs), except simple ones, cannot be decrypted instantly.
- Virtual servers support some extended authentication types (NTLMv1, CRAM-MD5, DIGEST-MD5, etc.). However some rarely used stuff (eg. MicroSoft's SPA) are not supported yet and probably never will.
- Some auto-mode features are required Administrator privileges and may not work if running from a remote drive.
- Asterisks revealer cannot uncover some kinds of programmatically protected **** fields. Some applications are not supported as well (eg. Opera, Firefox).

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

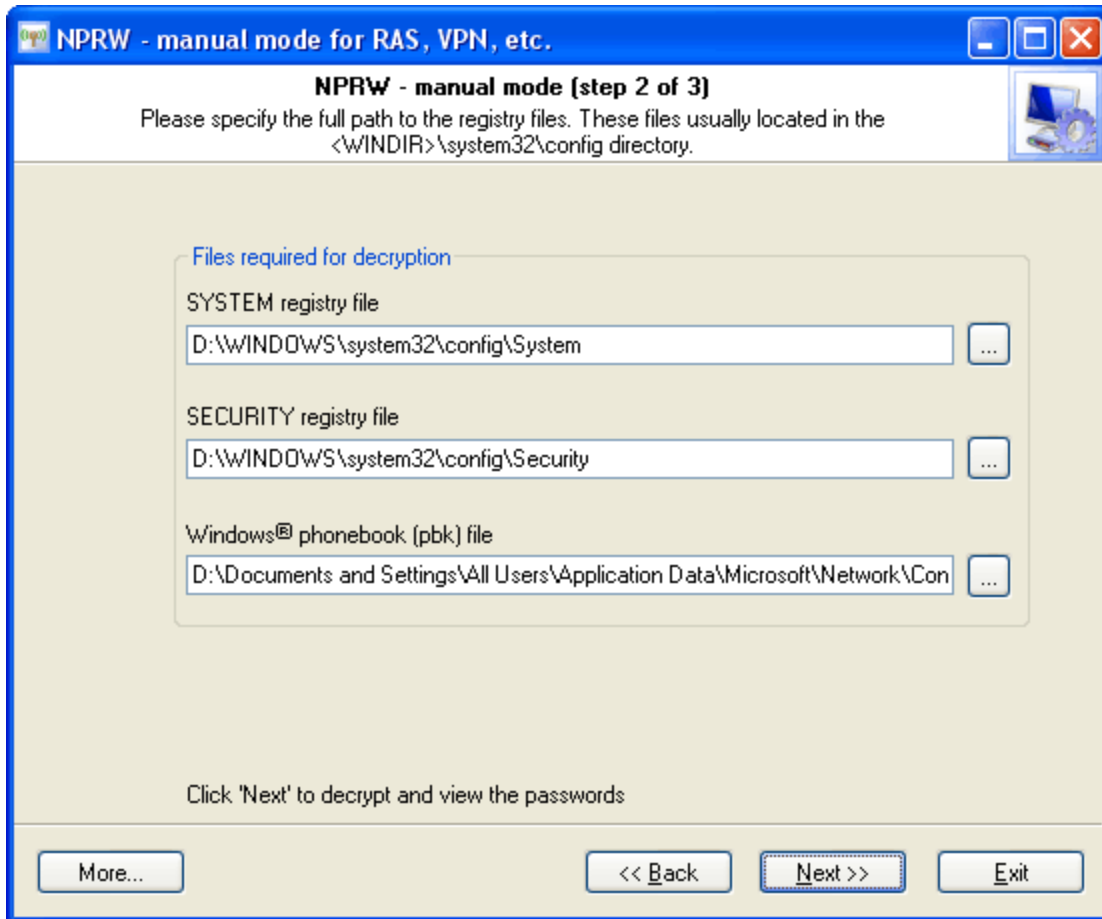
In the program's main dialog, select the wizard operation mode (automatic or manual) and the type of passwords to be recovered. Currently, the program supports 4 types of passwords:

- [Network connections passwords](#)
- [Local and global network credentials](#)
- [Domain cached passwords](#)
- [Wireless network keys](#)
- [Remote desktop passwords](#)
- [Windows Vista CardSpace \(InfoCards\)](#)
- [Asterisks password revealer](#)
- [Server emulators](#)

Advanced options are also available; you can find them at the bottom of the screen. One of those options allows enabling or disabling the logging. Logging is helpful to resolve sudden errors occurred in the program. The second additional option allows [choosing the interface language](#). Additional language modules can be downloaded from Passcape Software's server.

2.2 Manual mode for network connections passwords

To recover network connections passwords manually, you will need to have at least two Windows registry files: SYSTEM and SECURITY. They are stored in the folder C:\Windows\system32\config. The C:\Windows folder can be different on your computer.

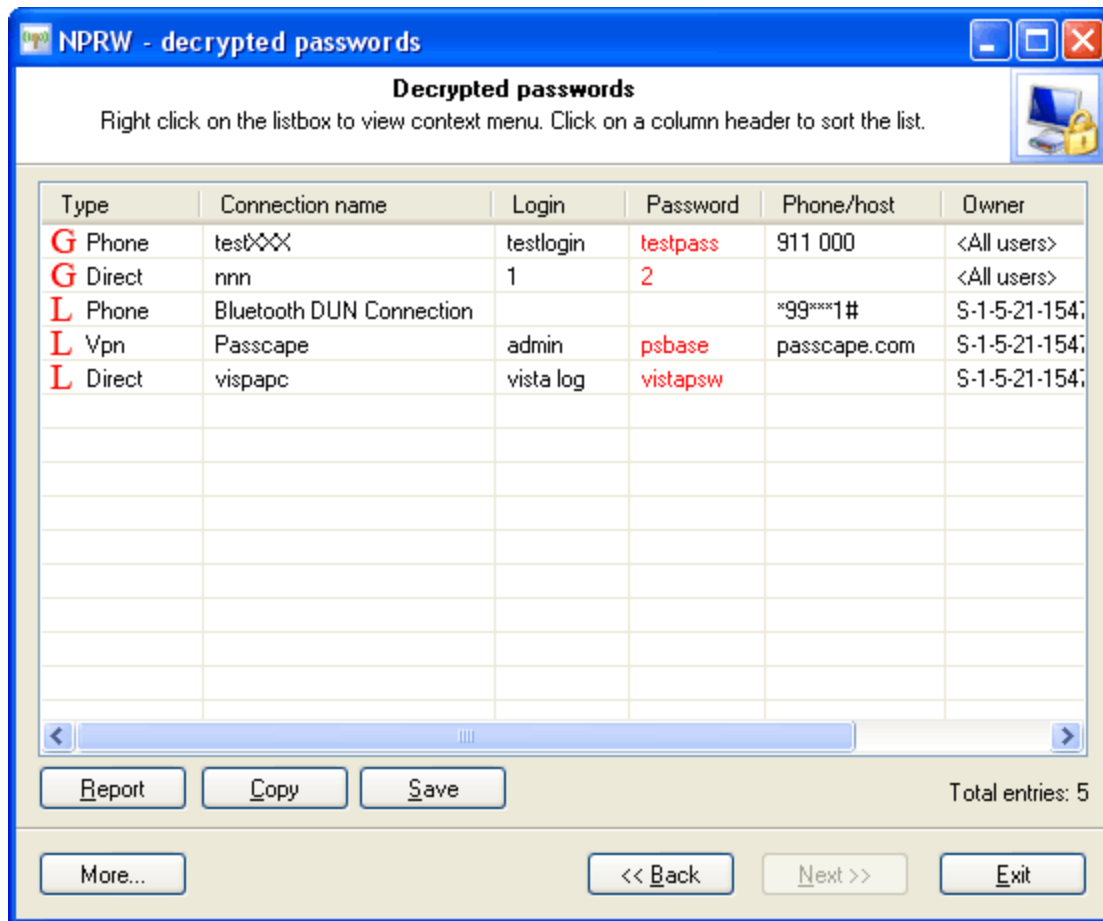


To recover the data in full, you will also need the Phonebook file. This file is normally stored in the folder C:\Documents and Settings\All Users\Application Data\Microsoft\Network\Connections\Pbk\rasphone.pbk. Where C:\Documents and Settings is the path to user profiles folder. Recovering passwords without the phonebook file is also possible. In this case, only logins and passwords will be recovered, missing the connection names, phone numbers, etc.

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 Recovered network connections passwords

This is what recovered passwords look like:



NPRW supports recovering passwords for the following types of connections:

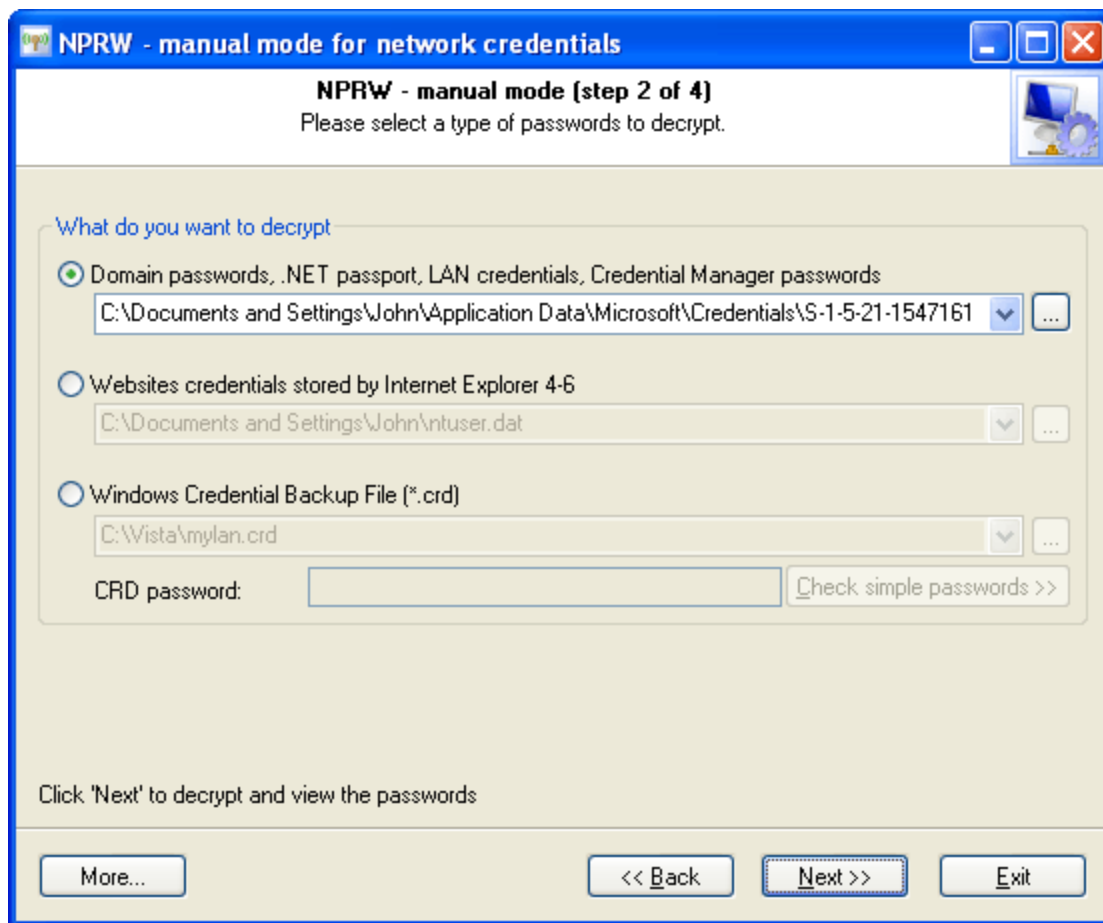
- **Phone** - Phone line, for example, modem, ISDN, X.25
- **Vpn** - Virtual Private Network.
- **Direct** - Direct serial or parallel connection
- **Internet** - Connection Manager connection.
- **Broadband** - Broadband connections, e.g. DSL.

The **L**(ocal) letter standing before a connection type means that the connection settings are only available to the account created the connection.

The **G**(lobal) letter means that the connection is available to all users of this computer.

The **S**(ystem) letter indicates a system account

2.4 Manual mode for network credentials



The manual recovery of local and global network passwords, in its turn, divides into two parts:

1. The recovery of passwords stored in Windows Credentials Manager. Those include passwords for accessing other computers within your LAN, Exchange server's e-mail passwords, .NET Passport accounts in MSN Messenger, etc. Physically all of these passwords are stored in the file `C:\Documents and Settings%\USER%\Application Data\Microsoft\Credentials%\SID%\Credentials`. Where %USER% - is your account name, and %SID% is your account's sid string. Please note that your computer may have a different user profiles folder (`C:\Documents and Settings`). Once the Credentials file is selected, on the next step the program's wizard will ask you to enter three additional parameters that are necessary for the further recovery:
 - user's logon password
 - user's Master Key. It is generally stored in the folder: `C:\Documents and Settings%\USER%\Application Data\Microsoft\Protect%\SID%\xxx`. Where `xxx` stands for a unique key name.
 - user's SID.
 Normally, **NPRW** fills the last two parameters automatically.
2. Passwords to Web resources used, for instance, by Internet Explorer. Passwords of this type are stored in the Protected Storage within user's registry. You will need to select or enter path to it manually. User's registry file is stored in its profile root; the file name is `ntuser.dat`; e.g., `C:\Documents and Settings\John\ntuser.dat`. This file is all you would need to have to recover passwords of this type.

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.

2.5 Recovered network credentials

Type	User name	Password	Domain	Last written
G MS Passport	info@passcape.com	Something	Passport.Net*	05.10.2006 09:06:1
G Domain password	local\testacc	!testpass!	passcape.com	05.10.2006 08:47:5
G MS Passport	username\usr		taggetname	11.08.2006 17:48:4
L MS Passport	info@passcape.com	Something	Passport.Net*	05.10.2006 09:06:1
L Domain password	local\testacc	!testpass!	passcape.com	05.10.2006 08:47:5
L MS Passport	username\usr		taggetname	11.08.2006 17:48:4
W Web resources		admin	192.168.1.1:80/80...	
W Web resources	ASP	pwd	members.asp-shar...	
W Web resources	cocker	bocker	www.passcape.co...	

Password types within this category are marked by the corresponding characters.

W(eb) - for Web resources

L(ocal) and **G**(lobal) - for passwords recovered from Credentials Manager.

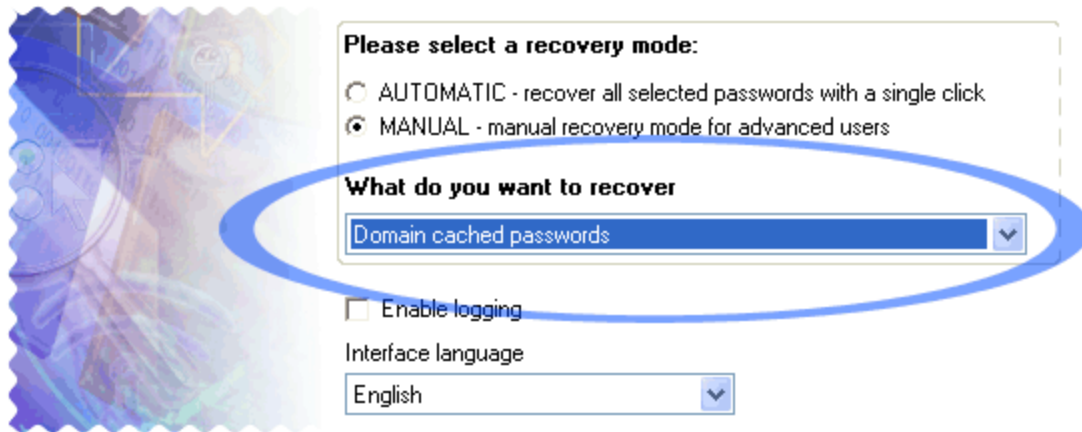
2.6 Domain cached passwords

Let's split the entire recovery process into three pieces:

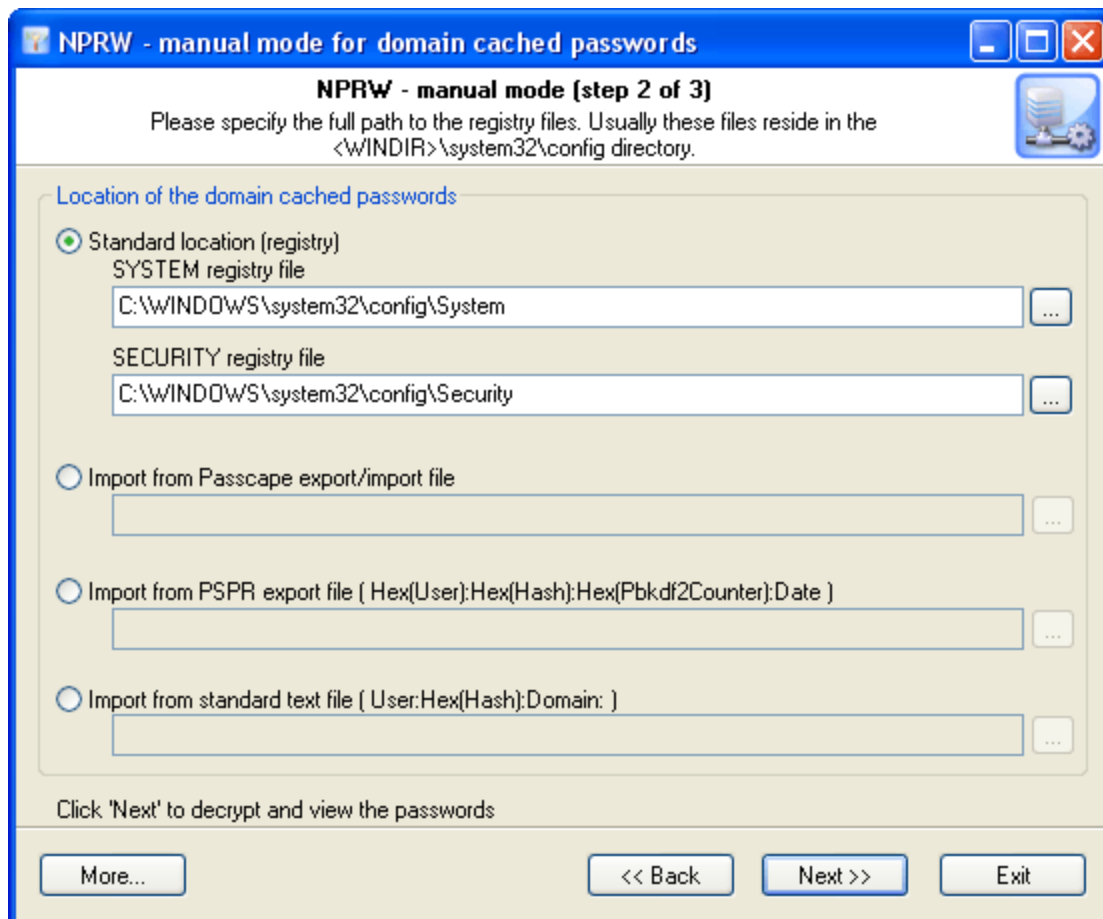
1. Decryption of cached domain entries
2. Analysis of obtained data
3. Decryption of password for selected entry

1. Decryption of cached domain entries

Launch the application and from the drop-down menu select what we want to recover: Domain Cached Passwords. If the cached records are on the local computer, with confidence fire up the automatic mode and move ahead.



The manual operating mode is more flexible and allows user to manually select data source, whether that's the standard location (registry files), Passcape's native import/export file or imported from a file used in other programs.

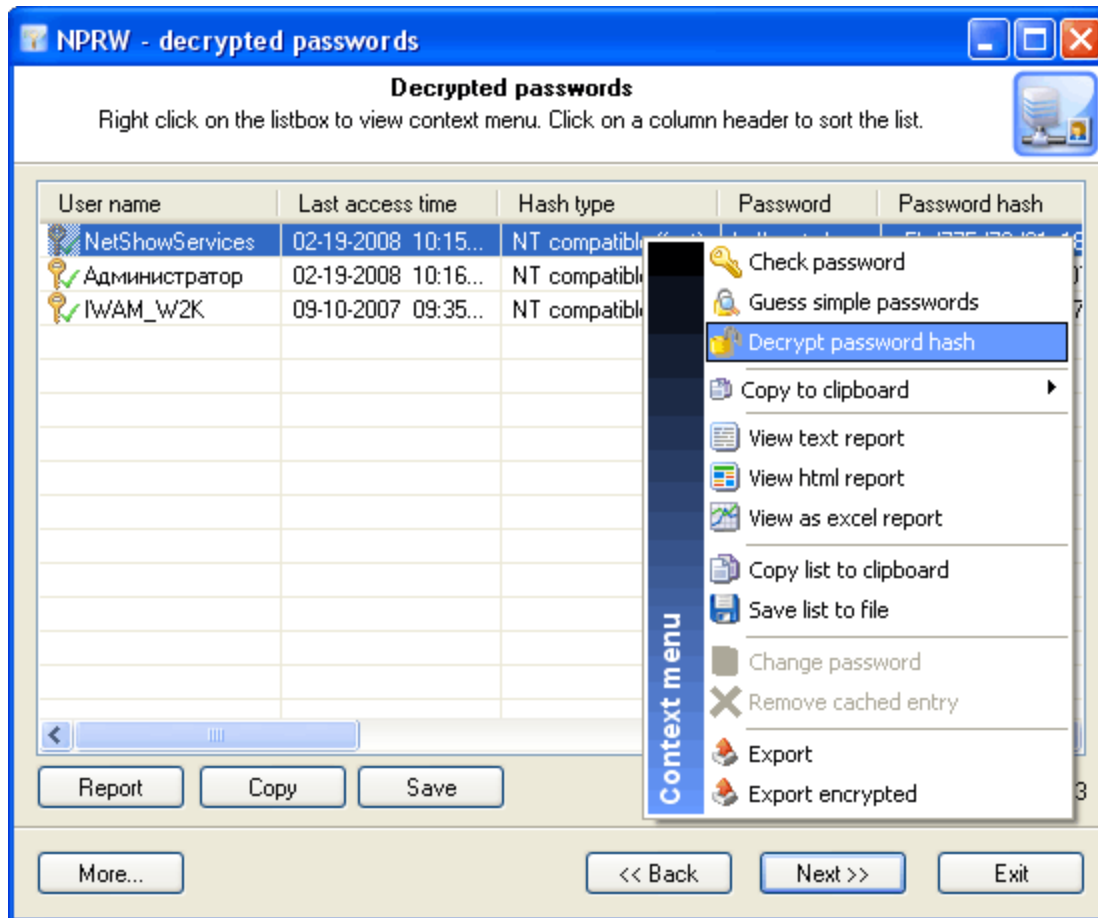


Click 'Next' and wait for the calculation results.

2. Analysis of obtained data

Upon a successful decryption or import of the data, the user will be offered a list of decrypted records. Each record has several fields; for instance, user name, server, membership in groups, etc.

Opening up the context menu by right-clicking allows engaging the program's extended capabilities. For the entire list: copy, save, view report or export entire list. For an individual record: change password, delete record, validate password, recover password by searching the simplest, frequently occurring combinations, or launch a full-scale attack.



Before launching the attack on password of the selected record, take a note of these two fields: 'Password' and 'Hash type'. Sometimes a cached password can be recovered without appealing to the full attack. In such case, if the program has found the password of the record, it will be kept in the 'Password' field, and the record will be marked with the corresponding icon.

The 'Hash type' field contains password hash type, which can be 'NT compatible instant' - instant recovery, 'Win2K compatible fast' - quick recovery at the speed of several millions of passwords per second or 'Vista, slow' - the recovery speed is only several hundreds of passwords per second on a modern computer.

3. Decryption of password for selected entry

So, to begin the recovery of the password for a selected record, right-click on it and then select 'Decrypt password hash' on the context menu. This will open up the decryption method selection dialog, common

to all Passcape Software programs. There is no sense in describing all types of attacks; the detailed information on that can be found on the pages related to the recovery of Opera passwords or Firefox Master Password.

Unsophisticated user might ask a completely reasonable and coherent question: "There is no 100% guarantee of the recovery, although there are many methods; 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:

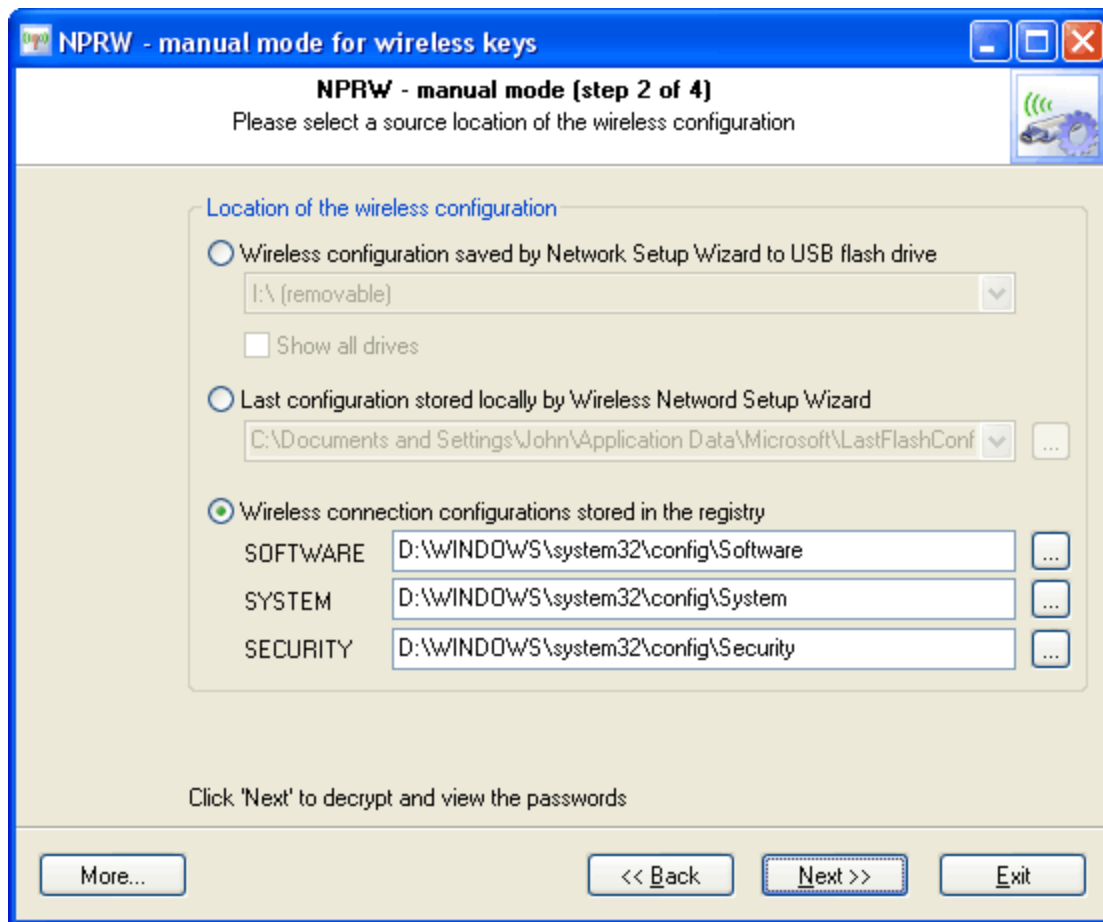
- First, enable the preliminary attack option, if it is available. It will help to recover simple and frequently used combinations.
- Second, if you are aware of any specifics of the password you are looking for, it's better to try mask attack or base-word attack first. Specifically, if you know a part 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.

2.7 Manual mode for wireless network keys

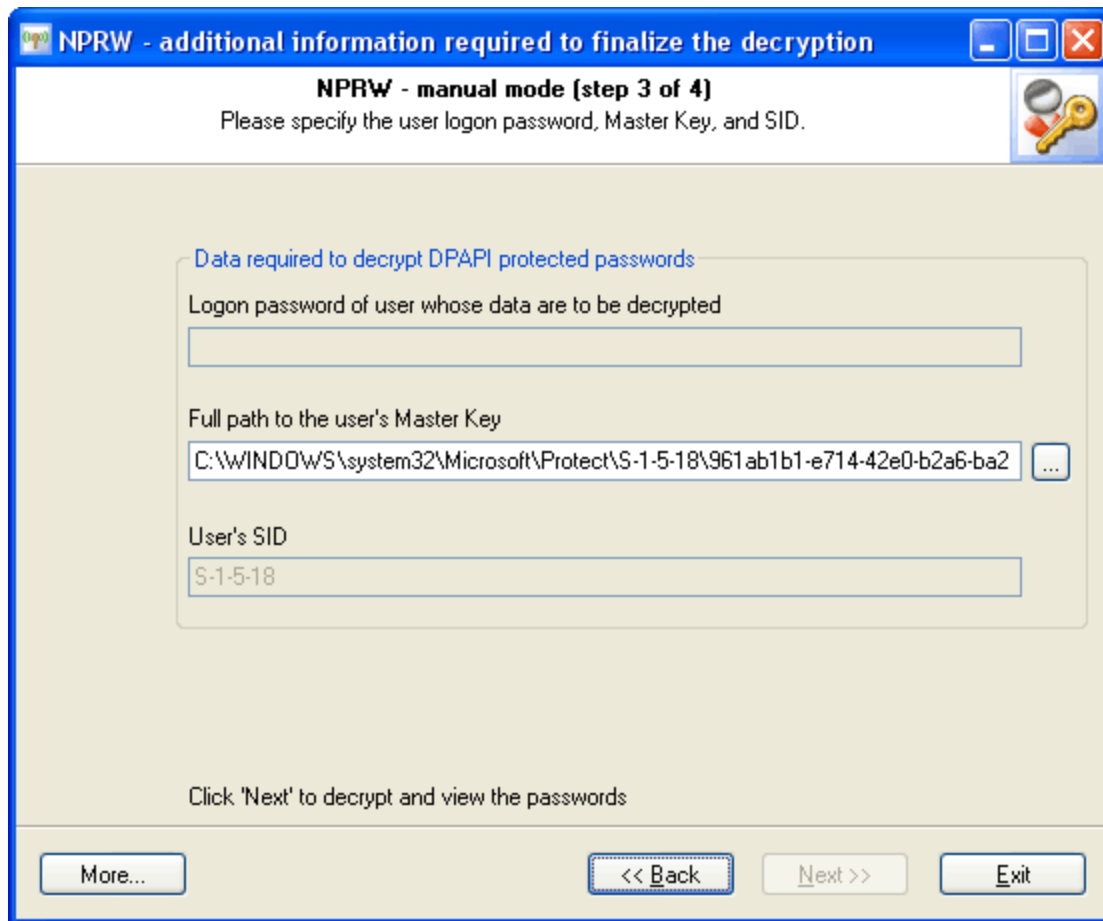
Wireless networking is a way to connect computers or other devices, either in your home or across long distances, using infrared light or radio frequency signals. Sometimes when you connect to a wireless network, you are prompted to enter a network key (also called a **W**ired **E**quivalency **P**rivacy key). This key is like a password that you need to gain access to the network. When you enable WEP, you can specify that a network key be used for encryption. A network key might be provided for you automatically, or you can specify the key by typing it yourself. If you specify the key, you can also specify the key length (40 bits or 104 bits), key format (ASCII characters or hexadecimal digits), and key index. The wireless network adapter in your computer might support the **W**i-Fi **P**rotected **A**ccess security protocol. WPA provides stronger encryption than WEP.

To recover wireless network passwords, you will need to specify their location within your system:

1. **Removable drive.** Wireless network settings can be stored on a USB flash or other removable drive. If you have chosen this option, you will be asked to select a drive with the data on the pull-down list. If the 'Next >>' button remains unavailable after you have selected the disk, it means that the program could not find the data required for this operation. No additional data is necessary for recovering passwords from this configuration.
2. **Wireless Flash Configuration** – the last configuration, which is prudently stored by Windows' wireless network setup wizard. That data is normally saved in a file named LastFlashConfig.WFC, which is stored in the folder C:\Documents and Settings\%USER%\Application Data\Microsoft. **NPRW** will automatically search for the necessary data in all local user profiles on your computer.
3. **Windows registry.** Passwords to wireless connections are stored in Windows registry. If you have selected this location, the further recovery will be possible only when these three Windows registry files are available: SOFTWARE, SYSTEM, and SECURITY. SYSTEM will be used for recovering SYSKEY. SYSKEY and SECURITY will be used for recovering Windows system account password. And the encrypted data actually stored in the SOFTWARE registry hive.



Other than that, once you have selected the registry files, on the third step of the program's wizard you will need to enter path to your system account's master key. Normally, that's a file of C:\WINDOWS\system32\Microsoft\Protect\S-1-5-18\xxx. Where xxx stands for the key name. Nothing bad will happen if you enter a wrong name within this folder; **NPRW** will attempt to locate the correct key automatically (usually, there are a few of them.)



Please note that **NPRW** recovers passwords `_stored_` in Windows, you don't have to be connected to a wireless network.

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.

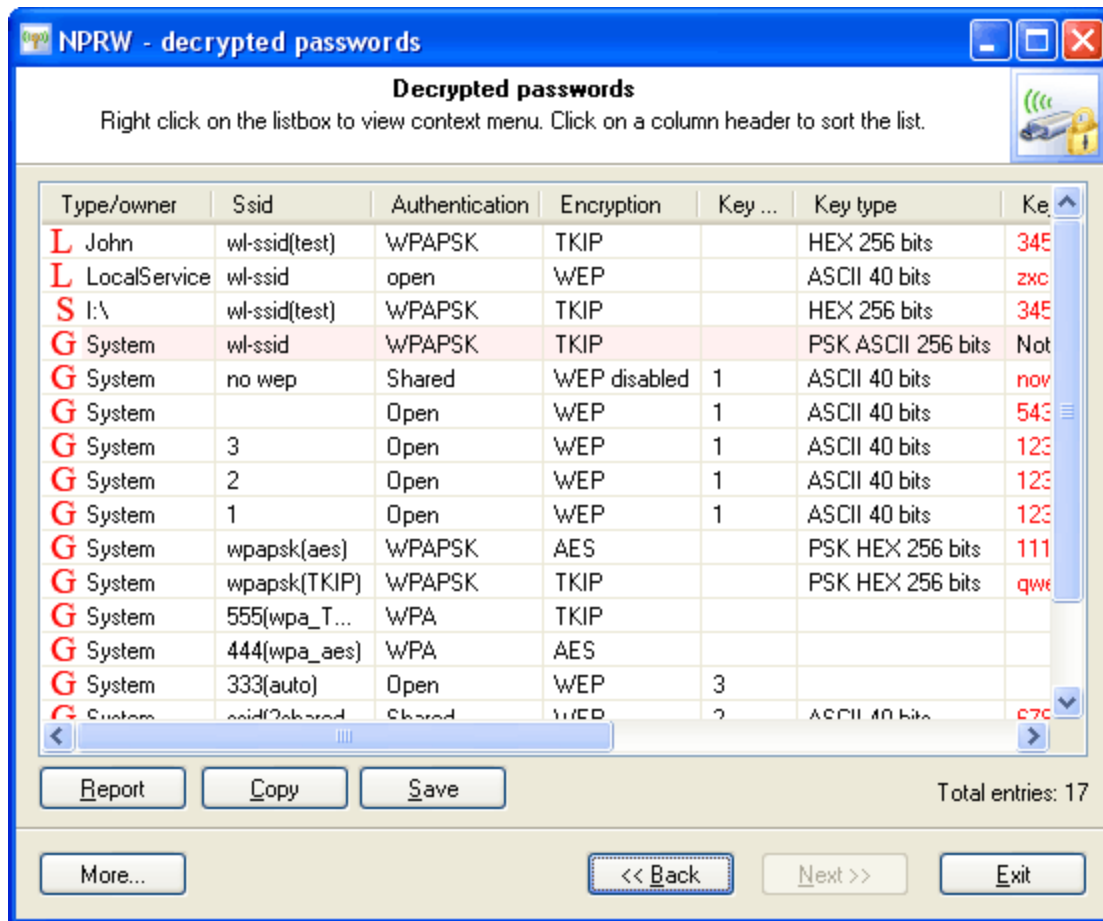
2.8 Recovered wireless keys and passwords

Recovered network connection passwords/keys, as it was said above, are divided into three types and are marked with the corresponding characters:

S(ystem) - system configurations stored on a removable drive

L(ocal) - last configuration stored locally by wireless network setup wizard

G(lobal) - wireless connections passwords/keys



WEP Passwords (or keys, depending on the wireless configuration) are recovered at once. Please note that the recovered WEP connections passwords can be in the plain-text (ASCII) or hexadecimal (HEX) format, depending on the wireless connection settings.

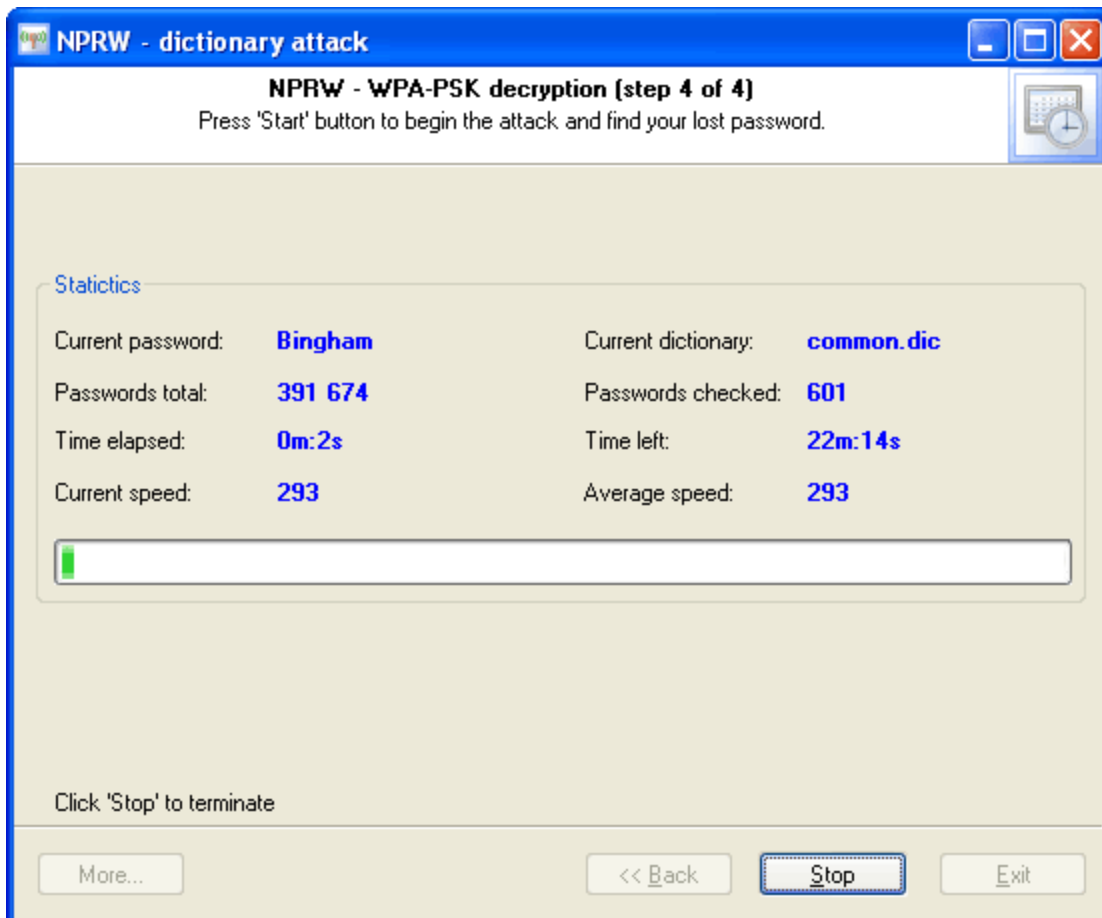
WPA-PSK passwords **cannot** be decrypted instantly. If you are recovering a WPA-PSK password, you should be aware that Windows does not store the actual password. Instead, it calculates its hash using a strong OWF and then stores it in the encrypted format. It is very, very hard to pick a password to such hash in the real life. **NPRW** will try all available combinations for picking a simple WPA-PSK password; therefore, the recovery time increases as the number of WPA-PSK keys found by the program grows. In the final dialog, the failed WPA passwords will be highlighted in red.

In theory, it is not a mandatory to have a WPA-PSK password to create a new wireless connection. You can enjoy the recovered WPA-PSK key. To try using it, copy the WPA-PSK key (its length must be 64 characters) from **NPRW**. Open 'Control Panel' and then run 'Wireless Network Setup Wizard'. Select the 'Setup a new wireless network' option and then 'Manually assign a network key'. Now paste the key you have copied to clipboard into the appropriate edit box (actually there are two fields: one for the key and another one just for confirmation).

As a last resort you can use the context menu to check/recover a forgotten WPA-PSK password manually.



Starting from version 3.0, the program can perform a full attack on WPA-PSK passwords. However the recovery speed is very slow - approximately 500-600 passwords/sec on a modern computer. So there's no point for example to run a brute-force attack on PSK.



P.S. Wireless password recovery works only if your system has Wireless Zero Configuration service installed. To determine if the Wireless Zero Configuration service is installed and running, follow the steps below:

- Click **Start, All Programs, Accessories**, and then click **Command Prompt**.

- Type **sc query wzcsvc** , and press **ENTER**.
- If the Windows Zero Configuration service is active, the words "**STATE : # RUNNING**" will appear.

2.9 Manual mode for remote desktop passwords

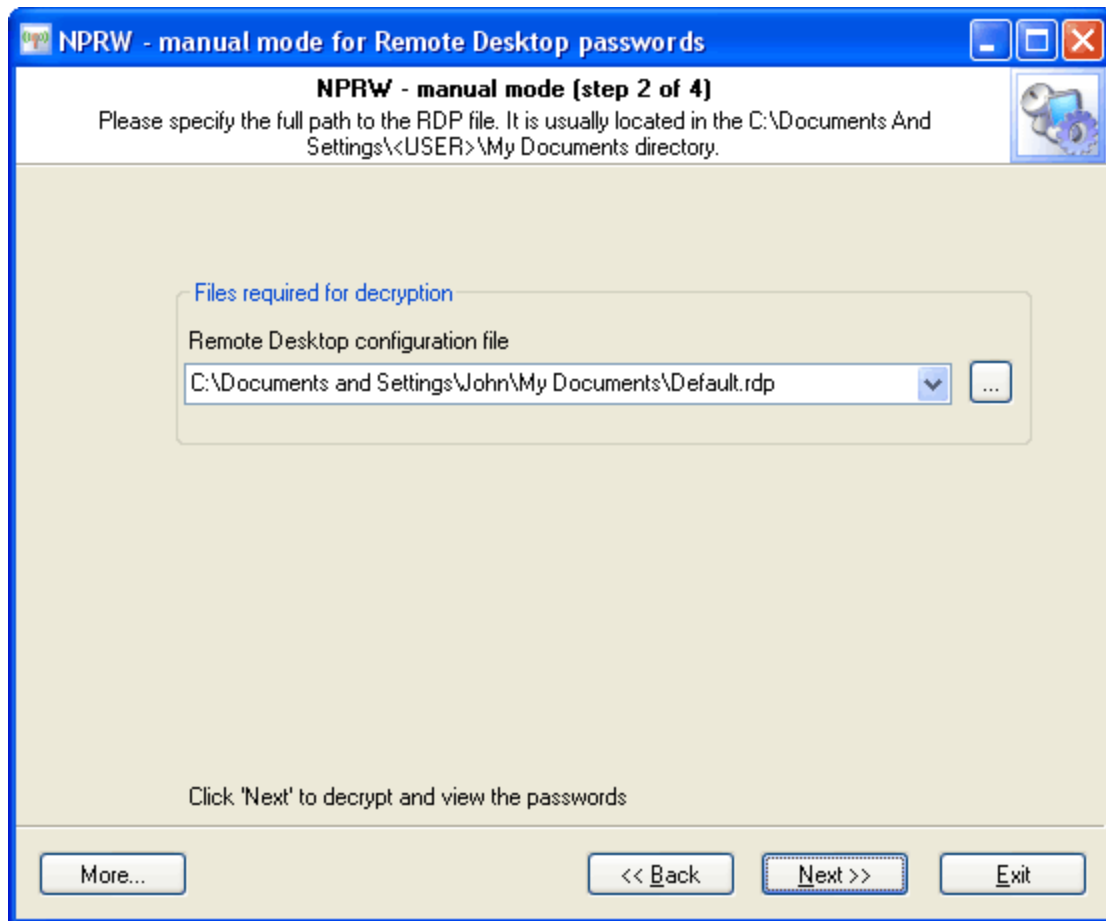
With Remote Desktop, you can have access to a Windows session that is running on your computer when you are at another computer. This means, for example, that you can connect to your work computer from home and have access to all of your applications, files, and network resources as though you were in front of your computer at work.

To use Remote Desktop, you need the following:

- A computer running Windows XP Professional with a connection to a LAN or the Internet.
- A second computer with access to the LAN via network connection, modem, or VPN connection. This computer must have Remote Desktop Connection, formerly called the Terminal Services client, installed.
- Appropriate user accounts and permissions.

Remote Desktop Connections passwords are stored in *.rdp files, which are normally located in current user's 'My Documents' folder. When you select the manual mode, **NPRW** will automatically scan your disk searching for these files. If the program was unable to find a *.rdp file automatically, you can try locating it manually and entering path to it by hand.

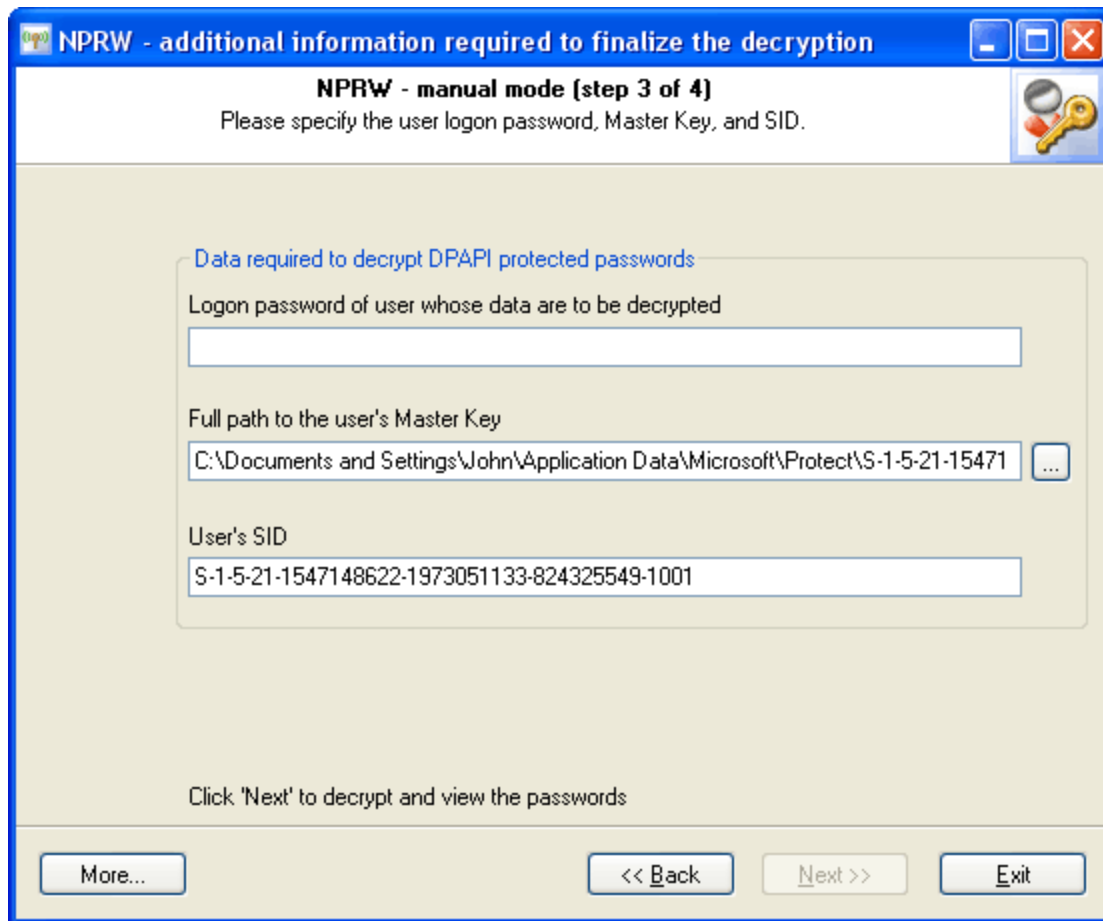
Please note that *.rdp files have hidden attribute, thus may be invisible from Windows Explorer, Windows Search, or from 'Open As' dialog. To let the system show hidden and system files, open 'Control Panel', then click on 'Folder Options', and then select the 'View' tab. On this tab, find the option 'Show hidden files and folders' and select it. Clear the option 'Hide protected operating system files'. When the necessary passwords are recovered, it's better to reset these options to the way they were set before.



You can view the list of available remote desktop configuration through the menu: Start -> All Programs -> Accessories -> Communications -> Remote Desktop Connections.

Once all necessary information is selected, you can move on to the next step in the program's wizard - setting additional recovery parameters. Since the remote desktop password is encrypted using the system's DPAPI mechanism, **NPRW** will need to know three other things:

1. Data owner's logon password (to the rdp file, in our case)
2. User's master key
3. User's SID

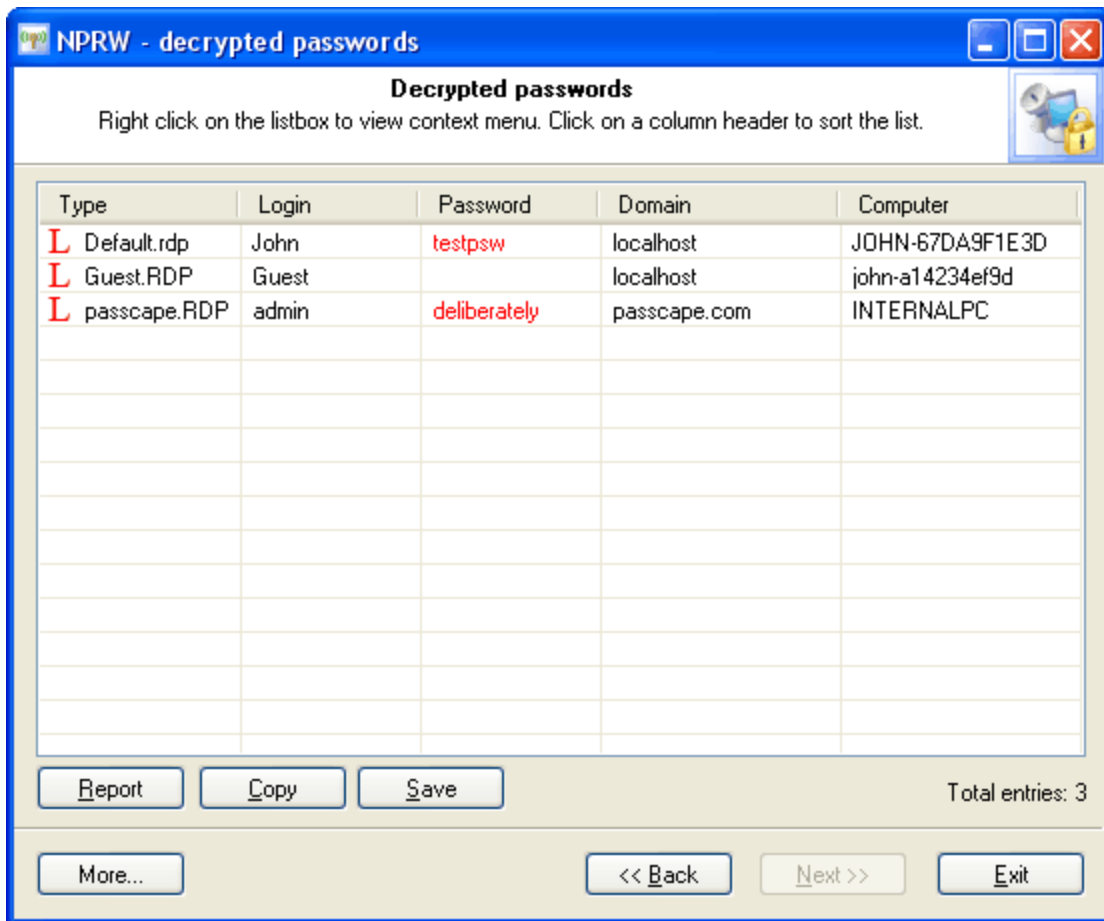


Usually, if we deal with a local account, the last two parameters will be filled by the program automatically. Otherwise, you will need to take care of it.

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.

2.10 Recovered RDP passwords

This is what recovered Remote Desktop passwords look like:



2.11 Decrypting Windows CardSpace (formerly InfoCards)

What is Windows CardSpace

Windows CardSpace is an industry-standard solution for managing user's identity in the Internet. In other words, Windows CardSpace is a simple and secure way to identify users, not requiring them to enter their user names and passwords again and again, while they travel between Web resources. The identification meta-system, adopted by major software vendors, may become a crucial step forward. Taking into account the actuality of security concerns, Microsoft makes significant efforts to propagate its popularity. Unlike the earlier unified identification technologies (e.g., **Microsoft Passport**) Windows CardSpace manages directly the users and applications that are to be contacted. In other words, diverse schemes and levels of difficulty can be used for the access identification; e.g., when registering with Web forums or for online banking.

Windows CardSpace support is implemented in **.Net Framework 3.0**. Microsoft employees have also set out their plans in regards to the development of their identification technologies. After the release of their Longhorn Server, which is scheduled for the end of 2007, the corporation is planning to release the **Security Token Service** technology, intended for the integration to **Active Directory**. Security Token Service is a little resource consuming gateway, running under the WS-Trust specification for servers and clients, which functions as a mediator when exchanging security markers like Kerberos, SAML, etc. According to Microsoft, the foundations for their identification platform - Identity Metasystem - are Active

Directory and **Microsoft Identity Integration Server** (the latter one is to be built into Windows). With time, in these two products the corporation is going to implement the support of strong credential data (such as smartcards), access management, single point of entry, unified identification, protection of information rights, process audit and automation.

On the application level, Windows CardSpace is a pane of identification cards that can be used for authenticating user on diverse online resources. The selector points at the type of credentials necessary for accessing to each of the resources.

Windows CardSpace gives user the access to creating and managing his **Information Cards (InfoCards)**. Just like one's personal information certified, for example, by the person's driver's license, passport or credit card, InfoCards is a data set certified by the publisher's digital signature.

Personal Information Card

Personal Information Card is a type of InfoCard, which user creates on his own and where he records his personal data. That's why Personal Information Card is often called a "**Self-issued Card**". Unlike a **Managed Card**, a Personal Information Card, along with its data, is stored locally, in a special encrypted storage. Personal Information Card contains a permanent set of personal data, which cannot be expanded. Along with the set of private data, Personal Information Card includes general information (version of InfoCard, date issued and updated, current state and status, etc.), uniform identifier and **Master Key** for encrypting private data and generating cryptographic keys. Please note that user can set additional protection with a **PIN** - the InfoCard password.

Personal Information Card data encryption and storage methods deserve a closer look, mainly due to the great number of tricks used for protecting the data.

To begin, InfoCard storage is a locked folder inside user's profile, the access to which is denied for everyone, (including the Administrator), except for the system itself. Path to Vista CardSpace normally looks like this: `C:\Users\%USERNAME%\AppData\Roaming\Microsoft\CardSpace`. This folder contains two files:

CardSpace.db - primary storage for all user's cards.

CardSpace.db.shadow - reserve storage used during card addition, removal operations, etc.

Windows CardSpace encryption

Windows CardSpace encryption is carried out according to the Master Key principle. In other words, to decrypt Windows CardSpace, one will have to decrypt its (Master) key first, which will be used as the primary material for decrypting the cards later on. Windows CardSpace Master Key's intriguing feature is that decrypting it takes two steps: using current **user's DPAPI** first, then using the **system's DPAPI**. Thus, Windows CardSpace is bound not only to current user but also to the operating system.

Windows CardSpace Master Key, in its turn, participates in the decryption of all cards. Each card stored inside Windows CardSpace consists of three objects:

1. **InfoCard public data**, which stores the card's system data; e.g., card version, its name and creation/installation/modification date, uniform identifier, logo, etc.
2. **InfoCard private data**. This object, just like a phone book, stores most frequently used claims. In Personal InfoCard, this set is also permanent. It doesn't contain passwords, account information or credit card numbers, thus minimizing the risk of disclosing user's confidential data.
3. **InfoCard Master Key**. InfoCard Master Key (set of random data) used for generating public/private key-pair used for signing and for encrypting InfoCard private data, if the card is pin-locked.

So, here is the overview of the decryption of InfoCard public data.

InfoCard private data encrypted with user password (infoCard PIN). But what happens if the PIN is lost or forgotten? Fortunately, there is a solution for recovering InfoCard PIN. The bad news is it's extremely hard, if at all possible, to recover it in the most difficult cases (long or tricky PIN). Nevertheless, let's take a look at this process in the **Network Password Recovery Wizard**.

The linear scheme of decrypting InfoCard private data with an unknown PIN can be split into 7 major stages of the Wizard:

1. [Select data source - CardSpace vs CardSpace Backup.](#)
2. [Read and decrypt system credentials. Oh yeah, they also exist.](#)
3. [Decrypt system's Master Key.](#)
4. [Decrypt user's \(data owner\) Master Key.](#)
5. [Decrypt InfoCard public data. Select the card.](#)
6. [Decrypt InfoCard PIN.](#)
 - 6.1. [Select recovery \(attack\) method.](#)
 - 6.2. [Set attack options](#)
 - 6.3. [Launch selected attack.](#)
7. [Decrypt InfoCard private data if the previous step was a success.](#)

* Steps 2-4 of the application's Wizard are not available in the automatic mode.

2.11.1 Selecting data source

Selecting data source - CardSpace vs CardSpace Backup

NPRW - manual mode for CardSpace (InfoCard)

NPRW - manual mode [step 2 of 10]

Please select a CardSpace folder from the drop down list or browse for new CardSpace directory.

Please select a CardSpace (InfoCard) folder

CardSpace (InfoCard) folder
C:\Users\John\AppData\Local\Microsoft\CardSpace

Decrypt from CardSpace Backup File

Windows CardSpace Backup

CardSpace Backup File C:\Users\John\Documents\2.crd

Password
 Hide characters as I type

To continue, click 'Next'

More... << Back Next >> Exit

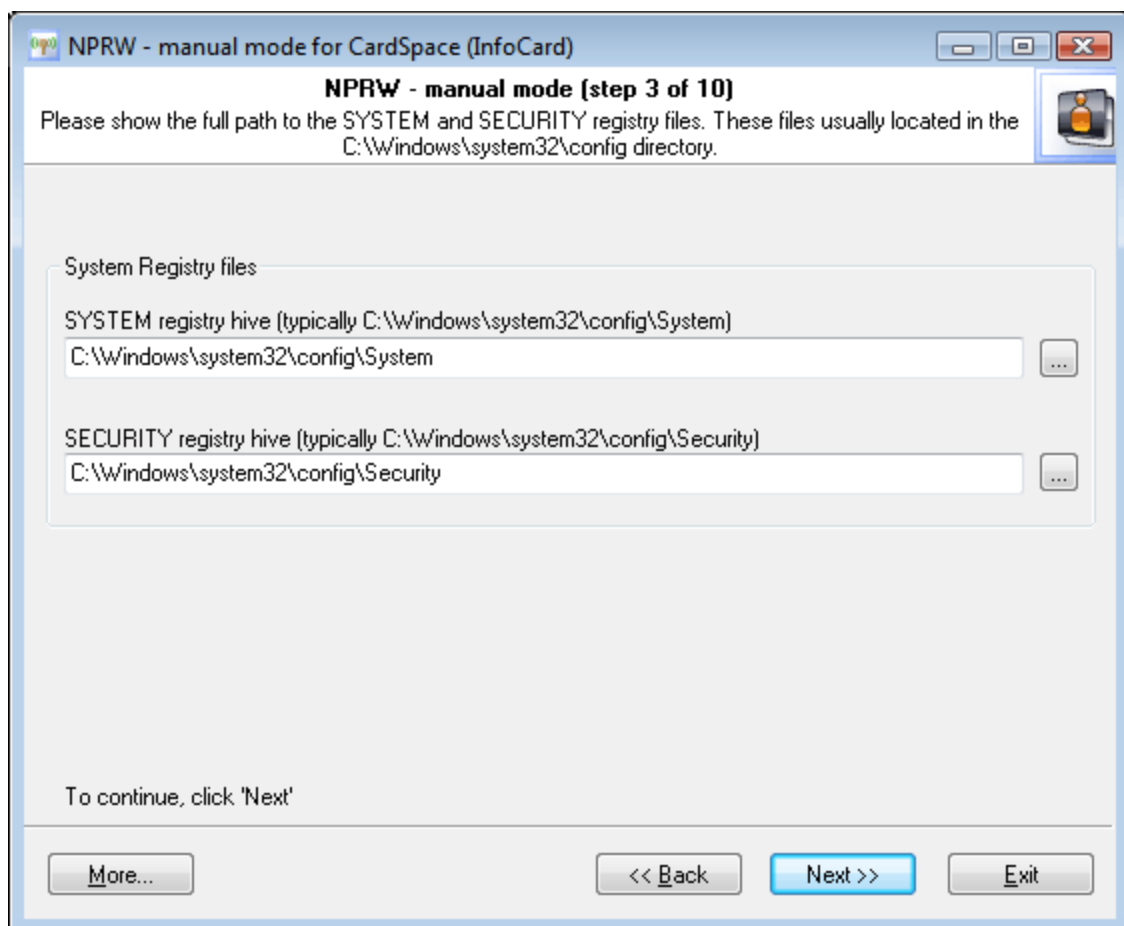
In the beginning, the application's Wizard scans the system and prompts you to select one of the available CardSpace storages. The default choice is current user's CardSpace. If the sought CardSpace storage is not found on the drop-down list, you can set path to its folder manually (by clicking on the **Add New CardSpace** button). Please note that all operations with CardSpace assume you are having the Administrator rights.

Another, alternate source of InfoCards is **CardSpace Backup File**. Normally that's a file with the **.CRDS** extension (if user hasn't set different). Please note that in order to decrypt CardSpace Backup File, you will have to know its password. Windows Vista sets the minimum password length for CRDS as 8 characters.

Once the data source is selected, we can move on to the next step in the Wizard - decrypting system passwords.

2.11.2 Reading system credentials

Reading and decrypting system credentials

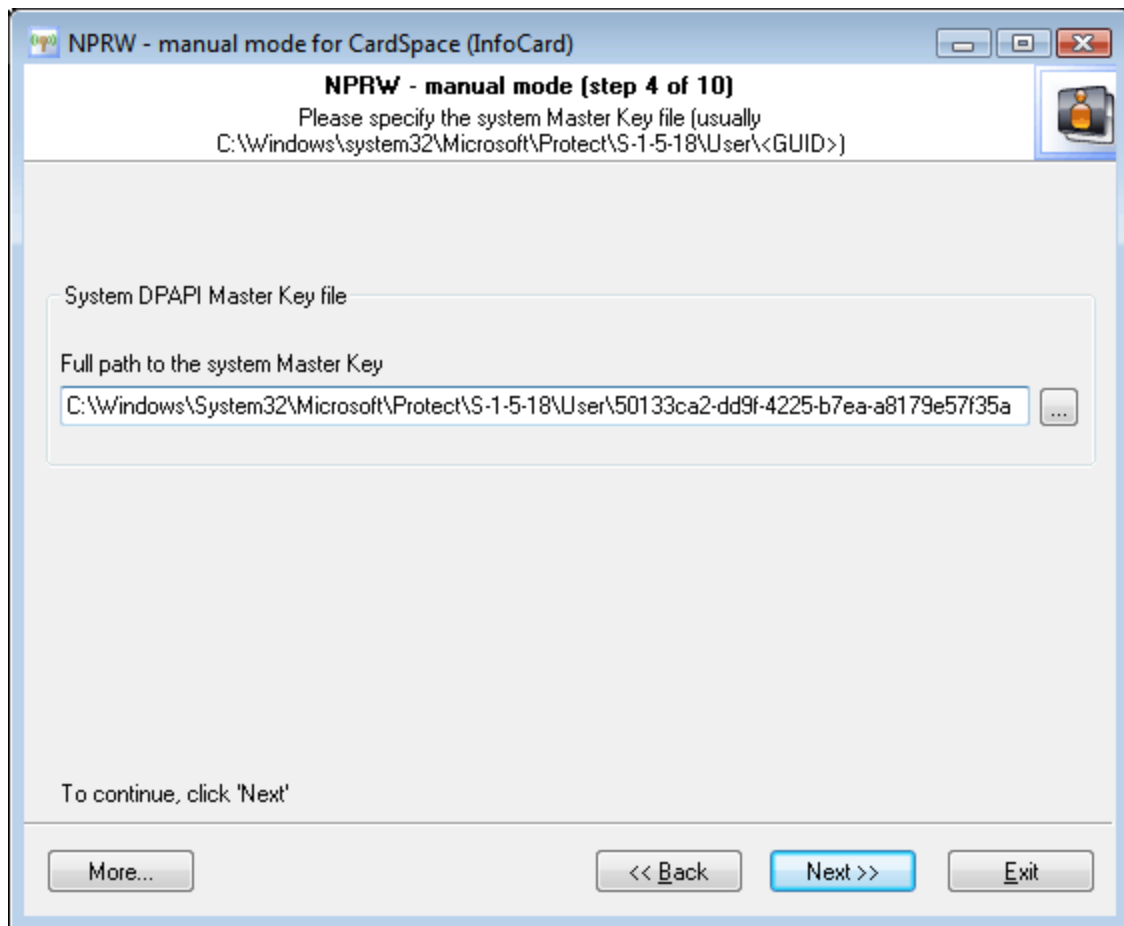


Any account in Windows, whether that's a user or the system, has the right to exist only when the corresponding passwords are set, even if those passwords are blank. System's accounts hide their passwords in **Windows Secrets** - a special storage for private information, inherited from the good old Windows NT.

In the automatic mode, the application reads that data automatically, without user's participation. In our case, we are to set the path to two registry files: SECURITY, which stores secrets (we are interested in just one secret that stores the password to the system account), and SYSTEM with the system data necessary for decrypting those. By default, registry files reside in the Windows folder; to be precise, in `%WINDIR%\system32\config`.

2.11.3 Decrypting system's Master Key

Decrypting system's Master Key

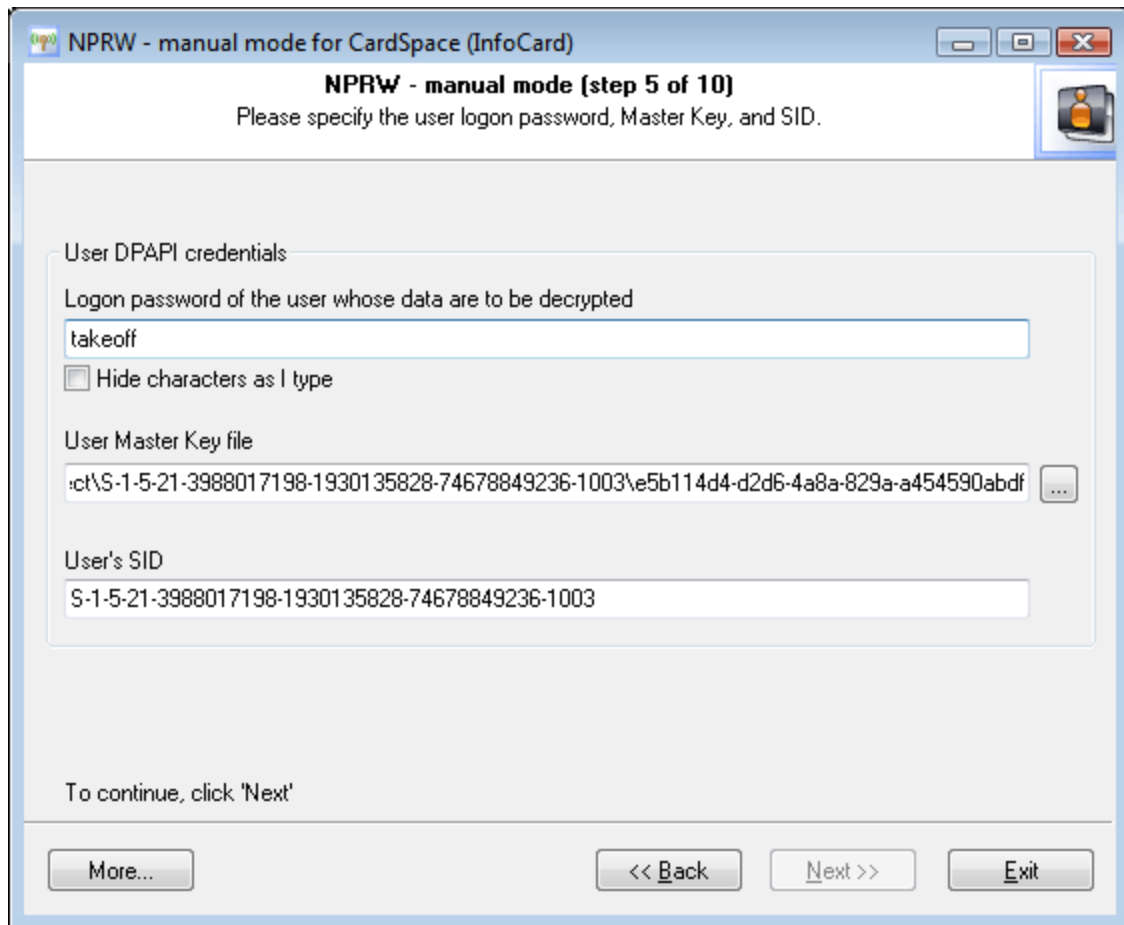


So, we've gotten the system passwords. It gets worse and worse as it goes on. What are we to do next? Right, we'll need to decrypt the **System's Master Key**. If you remember that, system's Master Key along with **User's Master Key** are involved in the decryption of **CardSpace Master Key**. Hmm: Sounds quite funny. If it keeps going that way, soon enough Windows developers will have to invent a Super-Mega-Extra-Master Key.

Skipping unnecessary details and speaking the human language, on this step we will need to set path to the file, which normally resides in the following folder: `%WINDIR%\system32\Microsoft\Protect\S-1-5-18\User`. The application will figure out the file name automatically, using the data obtained on the previous steps. The only thing you will have to do is to set the path to that folder. Going on.

2.11.4 Decrypting user's Master Key

Decrypting user's (data owner) Master Key



NPRW - manual mode for CardSpace (InfoCard)

NPRW - manual mode (step 5 of 10)
Please specify the user logon password, Master Key, and SID.

User DPAPI credentials

Logon password of the user whose data are to be decrypted

takeoff

Hide characters as I type

User Master Key file

c:\S-1-5-21-3988017198-1930135828-74678849236-1003\... ..

User's SID

S-1-5-21-3988017198-1930135828-74678849236-1003

To continue, click 'Next'

More... << Back Next >> Exit

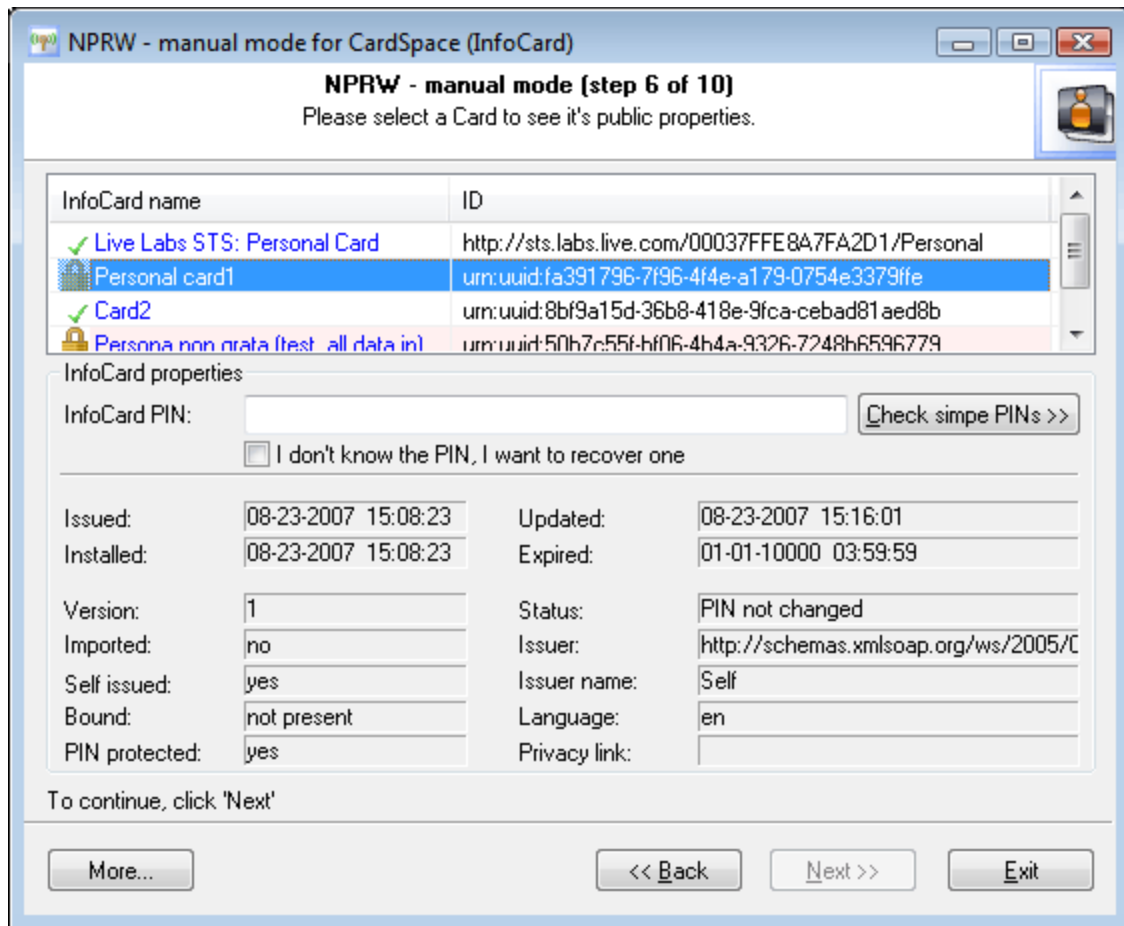
The last preparatory step before the actual decryption of CardSpace (bet you've thought it would never end :) is necessary to obtain user's Master Key. In Windows Vista, **User's Master Key** is located by default in the folder: *C:\Users \%USER%\AppData\Roaming\Microsoft\Protect\%SID%*.

Master Key name will be set by the application automatically. CardSpace owner's account password and its SID, which normally matches with the name of the %SID% folder, are involved in the decryption of the user's Master Key.

Once we are done with user's Master Key and with all the necessary data in our hand, we can finally get on the decryption of CardSpace.

2.11.5 Decrypting InfoCard public data

Decrypting InfoCard public data



If the previous steps of the Wizard have been completed successfully, you should be looking at the picture like this one (see the figure). At the top of the picture, you should see the list of decrypted InfoCard with the names and uniform identifiers. A bit below that are the selected card's properties (to view a card's properties, select the card on the list). A list against the card's name may have icons that indicate whether the card is protected with a password. The meanings of the icons are:

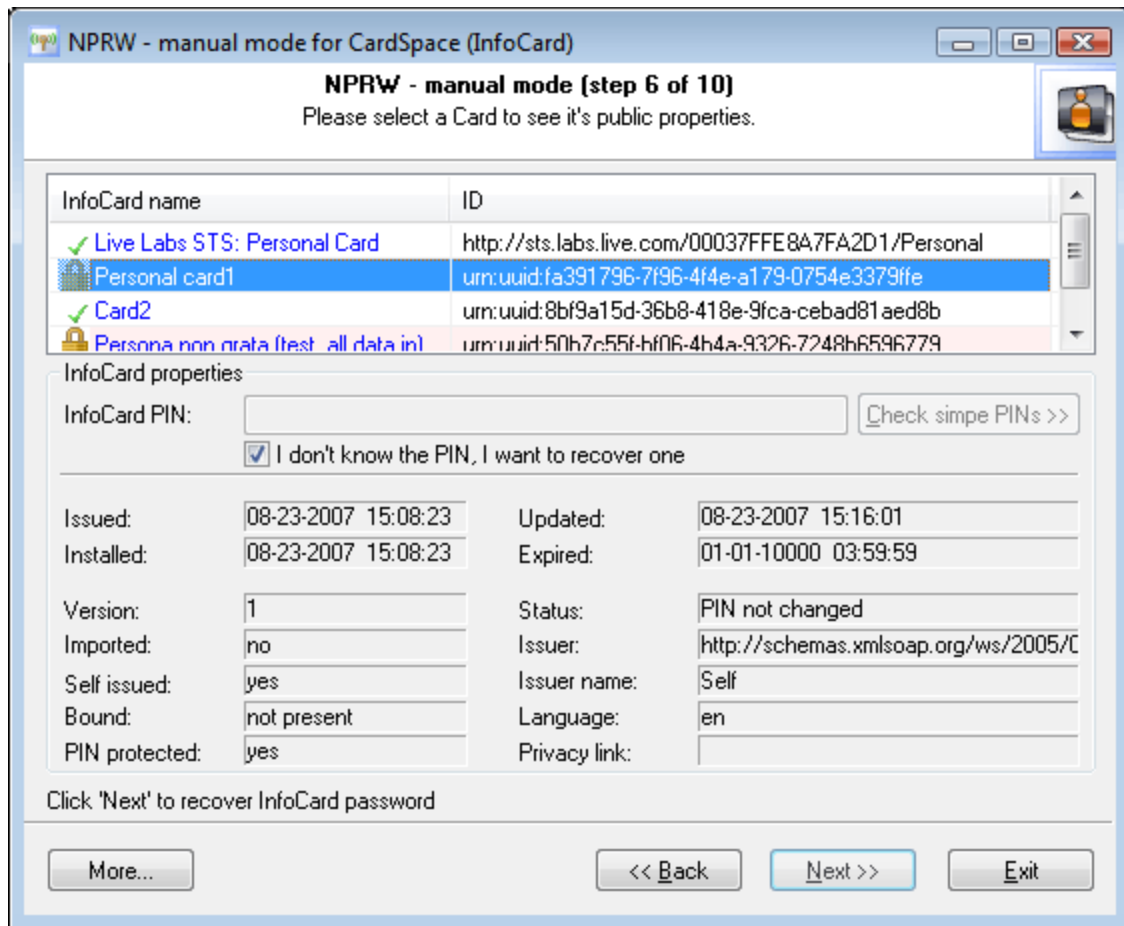
✓ Card not protected with PIN. Private data, i.e. claims, can be decrypted. The **Next>>** button will be enabled.

🔑 Card locked with PIN, but it has been found. Therefore, like in the first case, firmly move on to the Wizard's final step - the decryption of claims.

🔒 Card locked with PIN. The **Next>>** button becomes disabled. The recovery of the private data is impossible; however, you can try to recover the PIN.

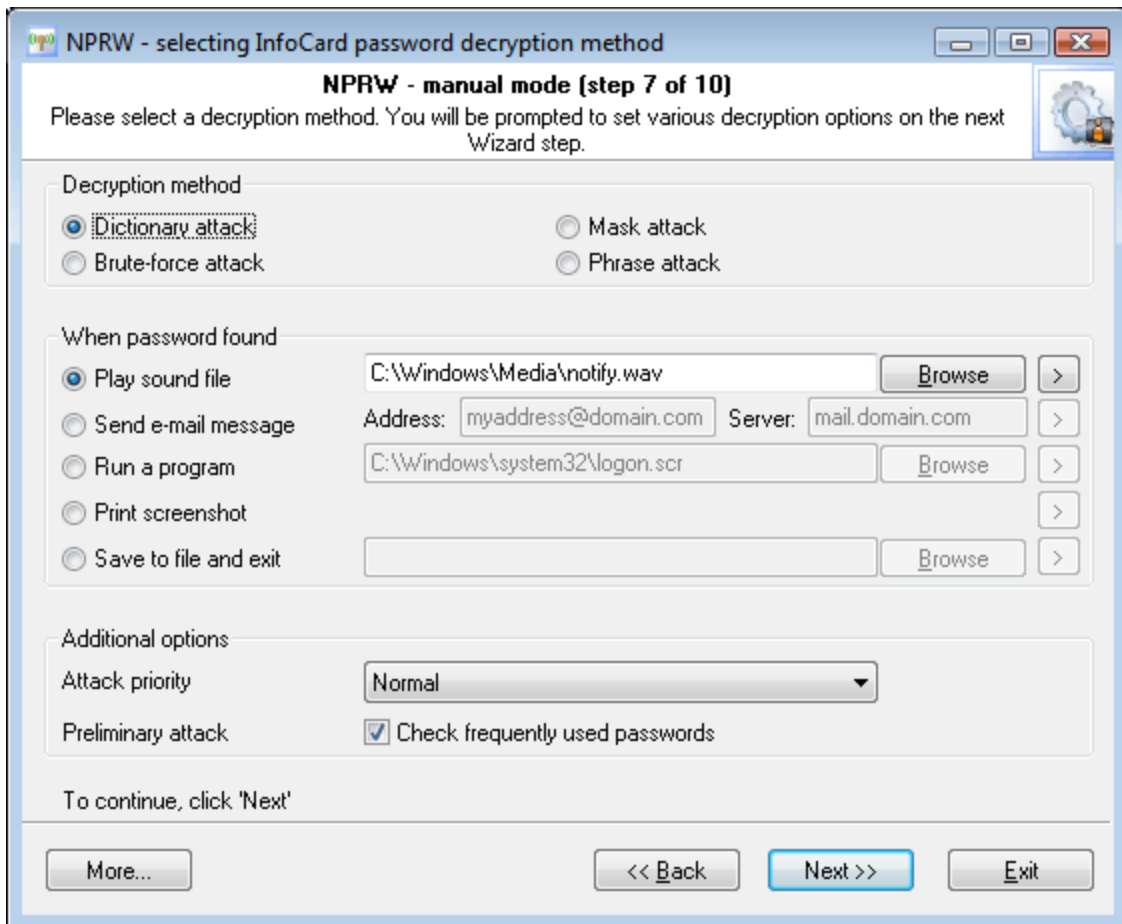
2.11.6 Decrypting InfoCard PIN

Decrypting InfoCard PIN



It's not a bad idea to first check the number against simple combinations (use the **Check Simple PINs>>** button). In one of the latest versions, the software has adopted the **Passcape Password Permutation** mechanism, which is involved in this check. The idea of the trick is that the more the more passwords have been found before the moment (no matter which ones), the more effectively it will recover the rest of the passwords. The search will take less than a minute on a moderate computer. Suppose, we haven't recover the PIN; what can we do next? Next, the only way to recover the PIN is through the search or attack. What does that mean? Select the option **"I don't know the PIN, but want to recover one"** and then click **Next>>** and move on to the recovery of the PIN. At the same time, you will see what the attack is.

2.11.6.1 Choosing recovery 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 found 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.

The most productive password recovery method (or PIN recovery like in our case) - is **dictionary attack**, where the software takes one word at a time from a dictionary and checks whether it works out or not. Optionally, you can enable mutation for each word. When it's enabled, depending on the depth of the mutation, the original word will undergo different modifications. For example, those can be adding numbers to the end of each word, removing vowels from it, etc.

If you know a part of the PIN, you should take a closer look at the last two attacks and maybe even start the recovery with them.

Brute-force attack is normally the worst choice, since to recover, for instance, an 8-character password of Latin characters a-z and numbers 0-9 (totally 2 901 713 047 668 combinations) on a modern computer it will take more than a week, even if the theory of probability is involved in the process. If the **Murphy laws** are involved, the recovery will take about half a month :)

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 proceeding to the next step. 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 several parts and allows to 'catch' short and frequently used passwords like 'qwerty' or '1234'.

2.11.6.2 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.

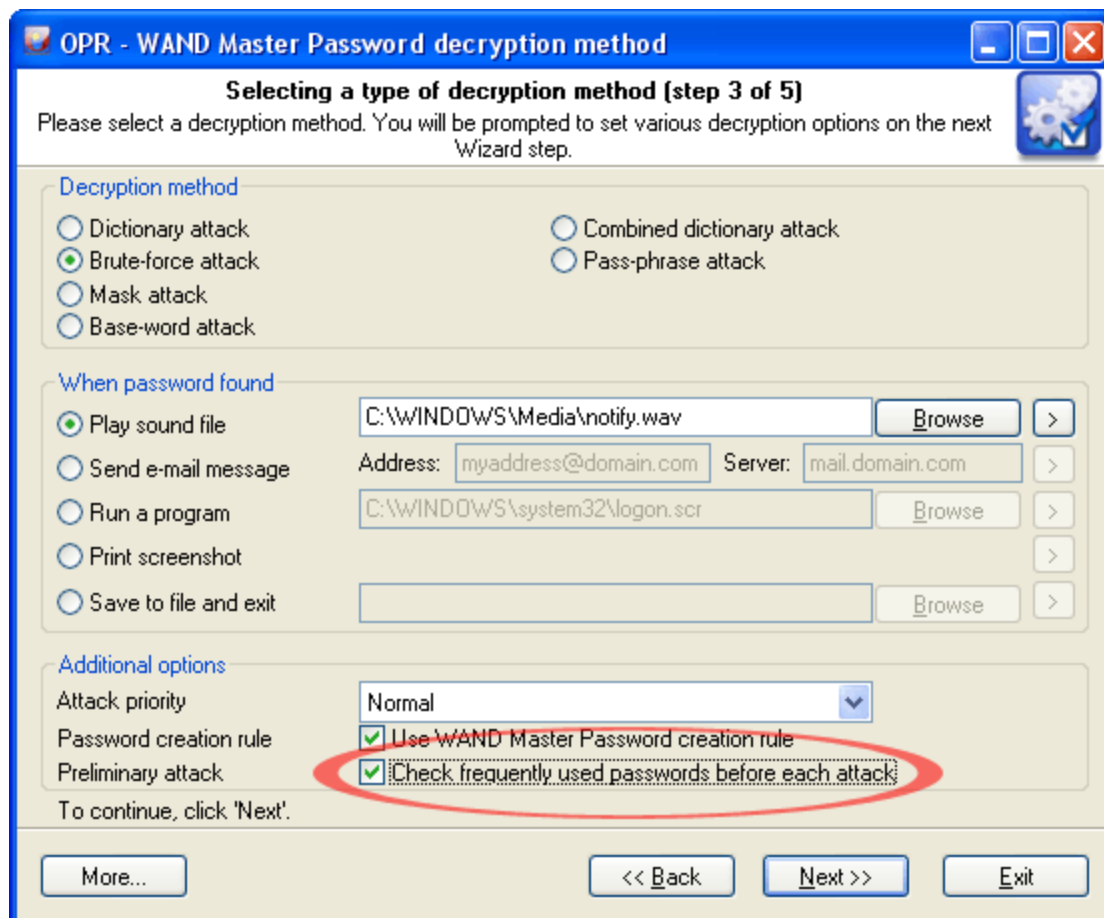
4. Mask attack is very helpful if there's any information about the password.
5. Base-word attack. Useful if a part (or source word) of the password is known.
6. Combined dictionary attack uses to guess complex/compound passwords.
7. Phrase attack uses primary to search complex password by looking through a dictionary with frequently used phrases.

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

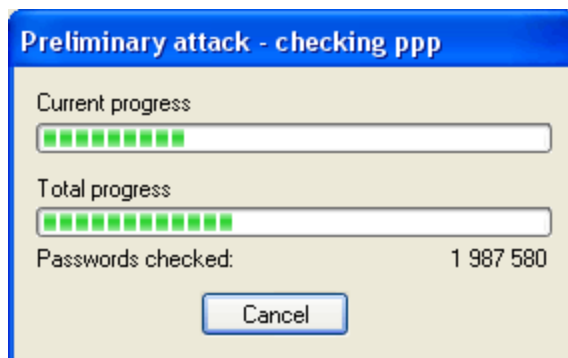
- [Preliminary attack](#)
- [Artificial Intelligence attack](#)
- [Dictionary attack options](#)
- [Brute-force attack options](#)
- [Mask attack options](#)
- [Base-word attack options](#)
- [Combined dictionary attack options](#)
- [Phrase attack options](#)

2.11.6.2.1 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.

2.11.6.2.2 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.

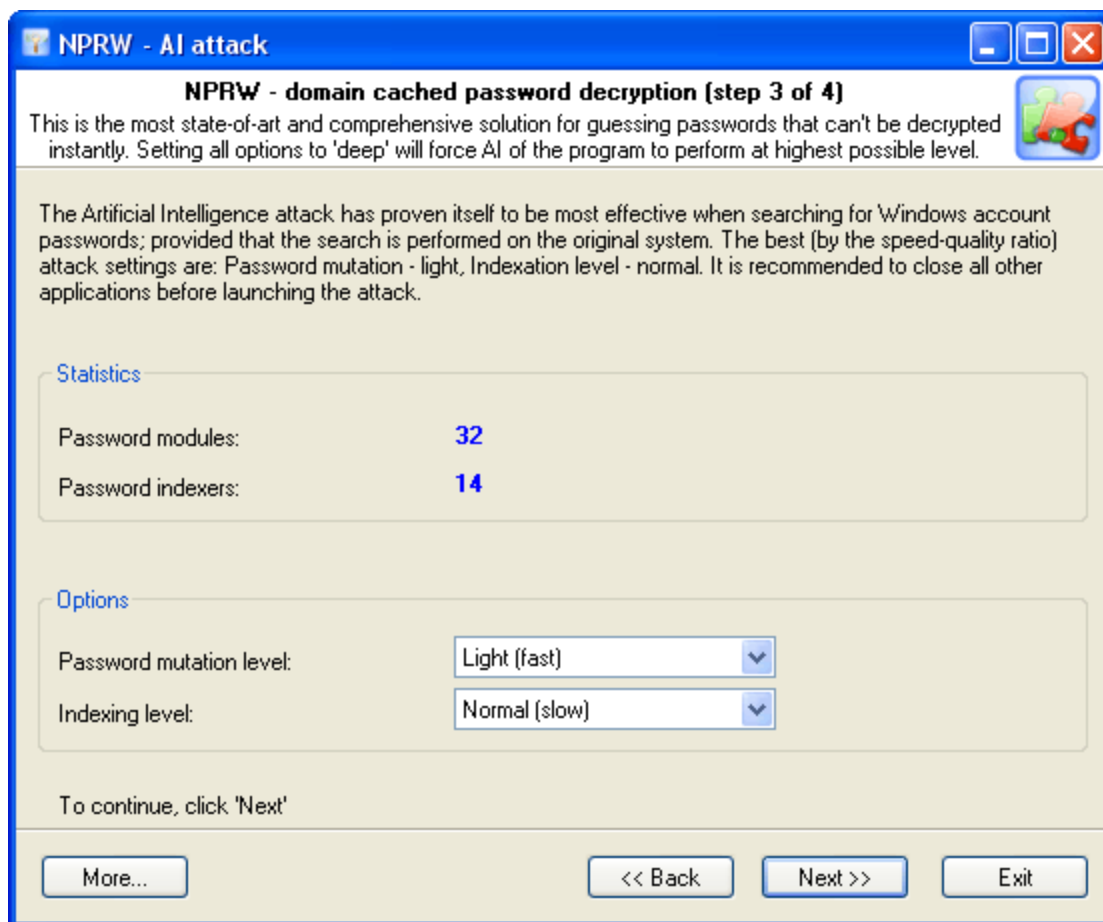
Although this sounds somewhat abstractive, in the reality the attack clearly splits into four successive steps.

- 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.

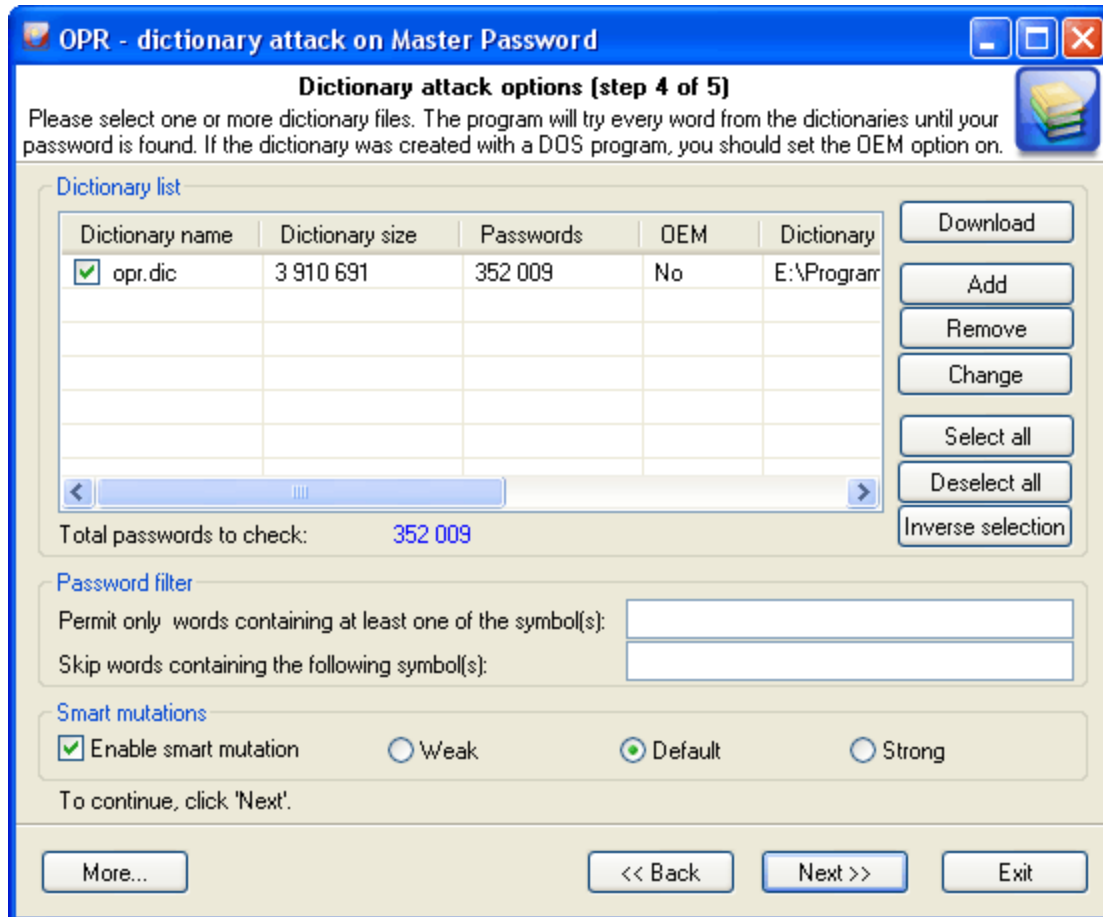
In the beginning of the attack, the program will search the system for all passwords it knows of. For that purpose, there are currently 32 mini modules for decrypting system, mail, browser, messenger, archive and other passwords. Then there goes the file and data indexation, along the course of which 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.



2.11.6.2.3 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 PIN 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 than 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.

2.11.6.2.4 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 InfoCard PIN. There are 3 group of options here.

OPR - brute-force attack on Master Password

Brute-force attack options [step 4 of 5]

Guess the password by trying every single combination of characters from given charset range. You can also split this range and share it between multiple computers.

Brute-force charset

Lowercase Latin (a...z) Uppercase Latin (A...Z) Digits (0...9)

Special symbols (!@#...) All printable (ASCII 32...127) All (ASCII 1...255)

Custom charset Load Save

Charset (ASCII format):

Charset (HEX format):

Charset string: `abcdefghijklmnopqrstuvwxyz`

Password length and position

Minimal length: Starting password:

Maximal length: Total passwords to check: `217 180 147 158`

Distributed attack

Number of computers to participate:

Password range for computer:

To continue, click 'Next'.

More... << Back Next >> Exit

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.

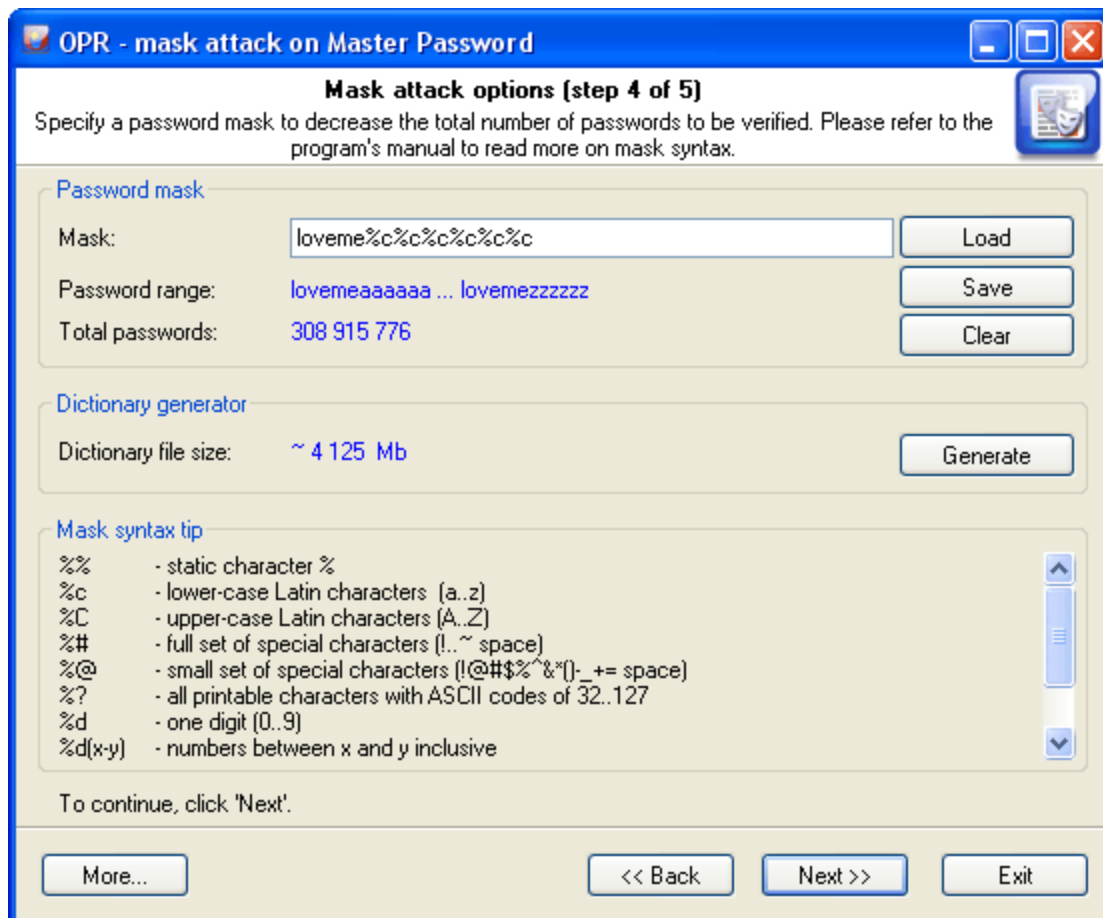
Password length and position

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 PIN 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 attacks.

2.11.6.2.5 Mask attack options



The entry field is used for setting the mask (rule), by which the program will try to recover the PIN. 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.

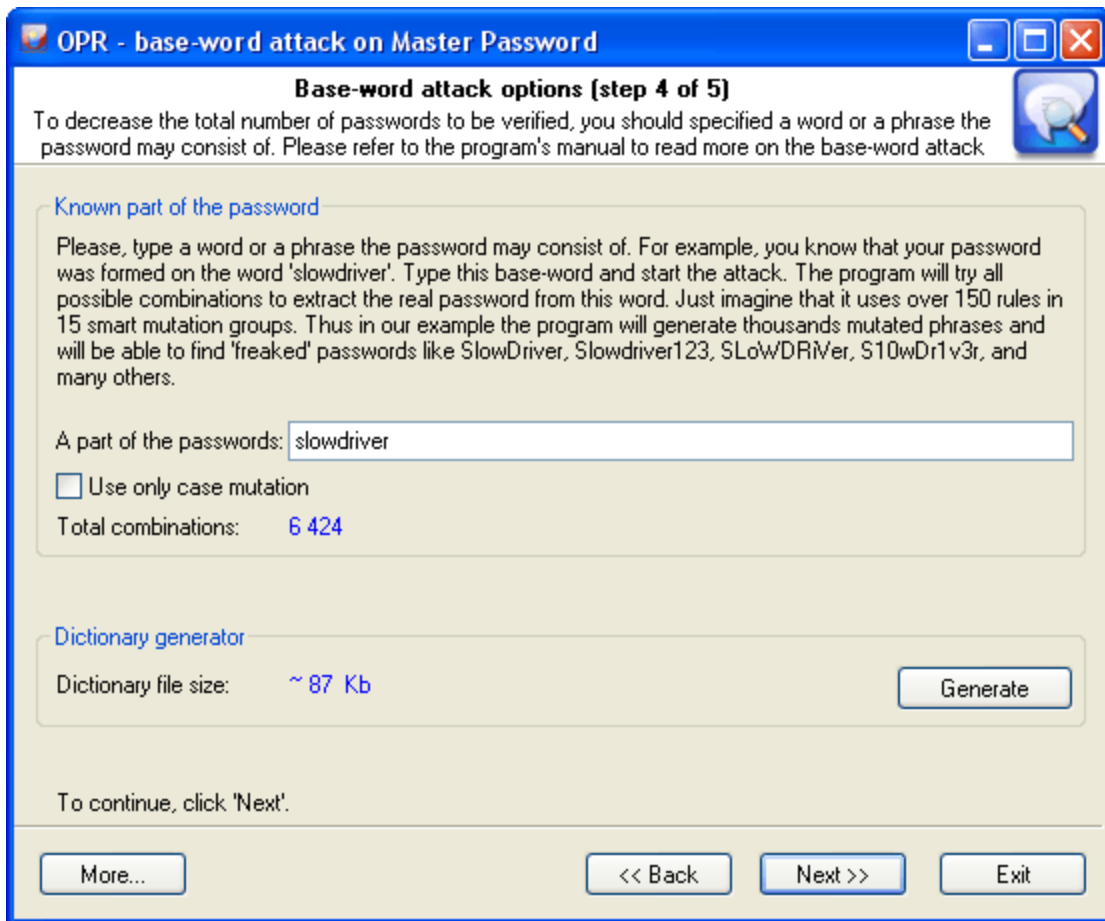
Examples:

- test%d** - will generate password range test0..test9, 10 passwords total
- test%d(1980-2007)** - test 1980..test2007, 28 passwords
- test%r(48-57,97-122)** - test0..testz, 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%d(2)%c%l(2)%c** - 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.

2.11.6.2.6 Base-word attack options

Base-word attack is an irreplaceable recovery tool when you know a portion of the PIN 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 PIN 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.

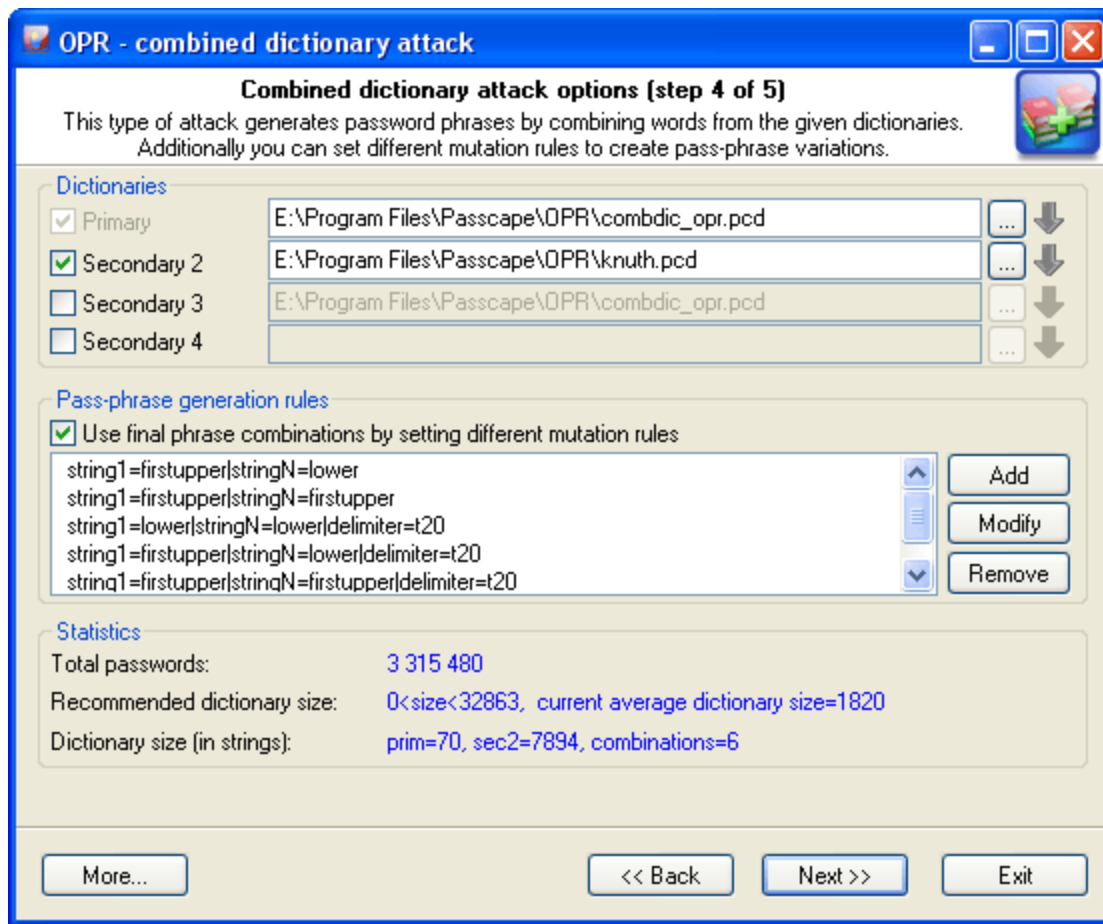
With this tool, the program will attempt to recover the original PIN, trying all possible combinations founded upon 15 groups of rules (total over 140 rules.) If you enter '**slowdriver**' in the field, you will see that the program has generated several thousands of different combinations upon this phrase, and one of those combinations will match our password.

Enter the word or pass-phrase prototypical to your InfoCard PIN.

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.

2.11.6.2.7 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'.

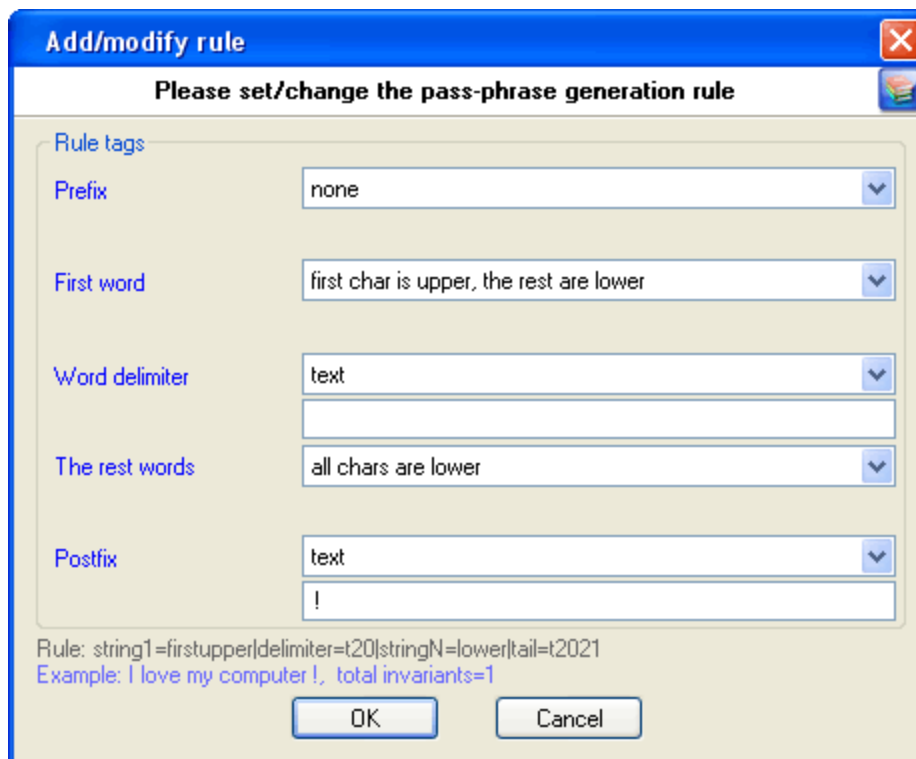
The example is plain but demonstrative. The idea is that for multiple sources you can successfully use both a single dictionary and multiple ones. It all depends on your imagination. The last example shows that a special attention should be paid to the order of the dictionaries if they are different. 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', 'aaacc', 'aaadd', 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.

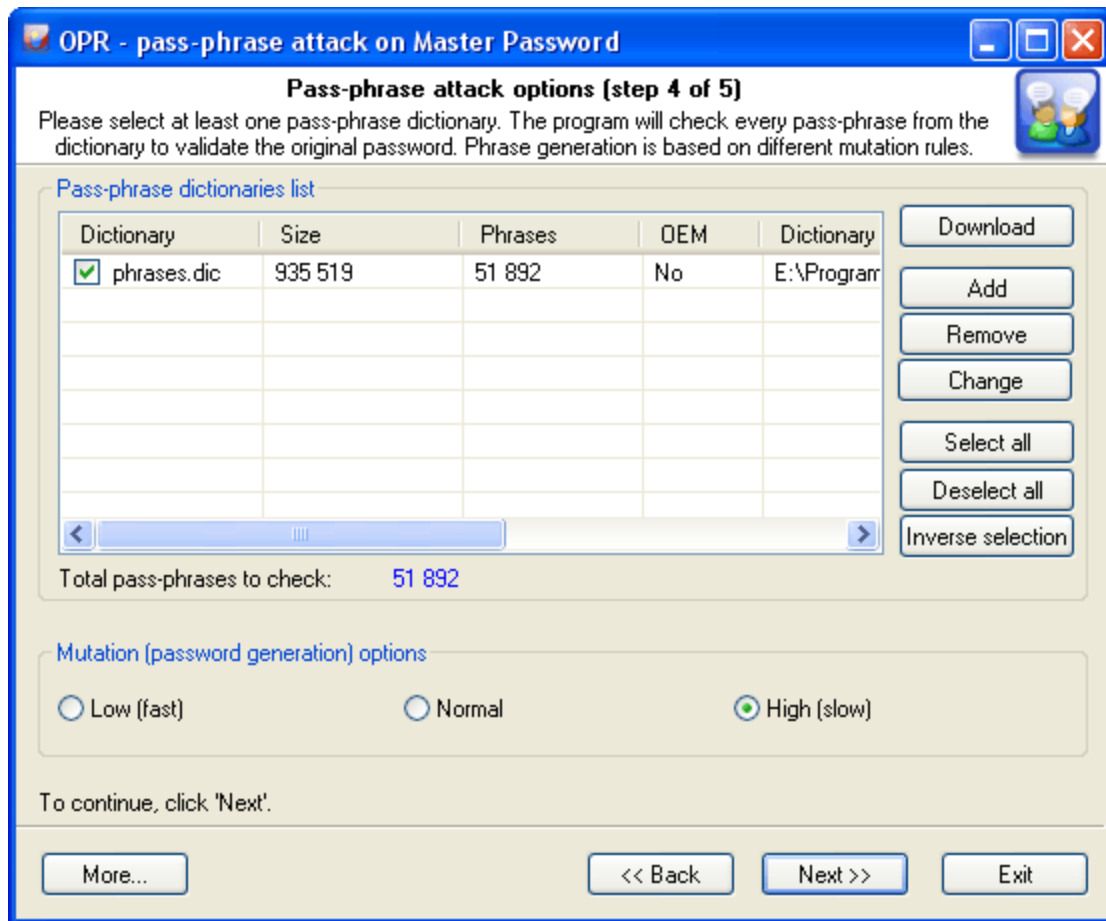
The 'Statistics' group shows the average and recommended average size of a dictionary, number of words in source dictionaries, total number of passwords being generated and other helpful information.

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.

2.11.6.2.8 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.

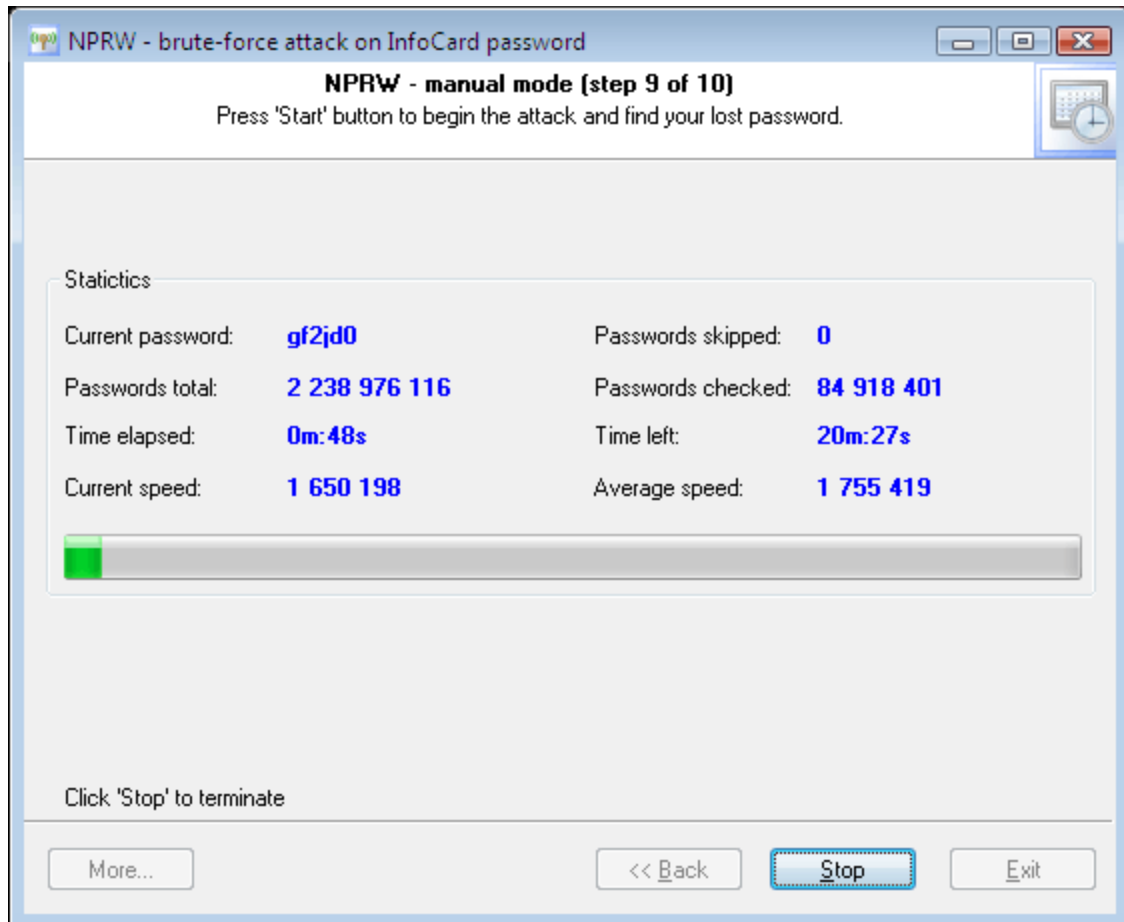
The password-phrase attack options almost completely repeat the simple dictionary attack options: here, you also are to select one or several dictionaries for the phrase source, it also allows loading additional dictionaries from the Passcape website, and it has the same way for setting phrase mutation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

2.11.6.3 Launching the selected attack

This step of the 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.

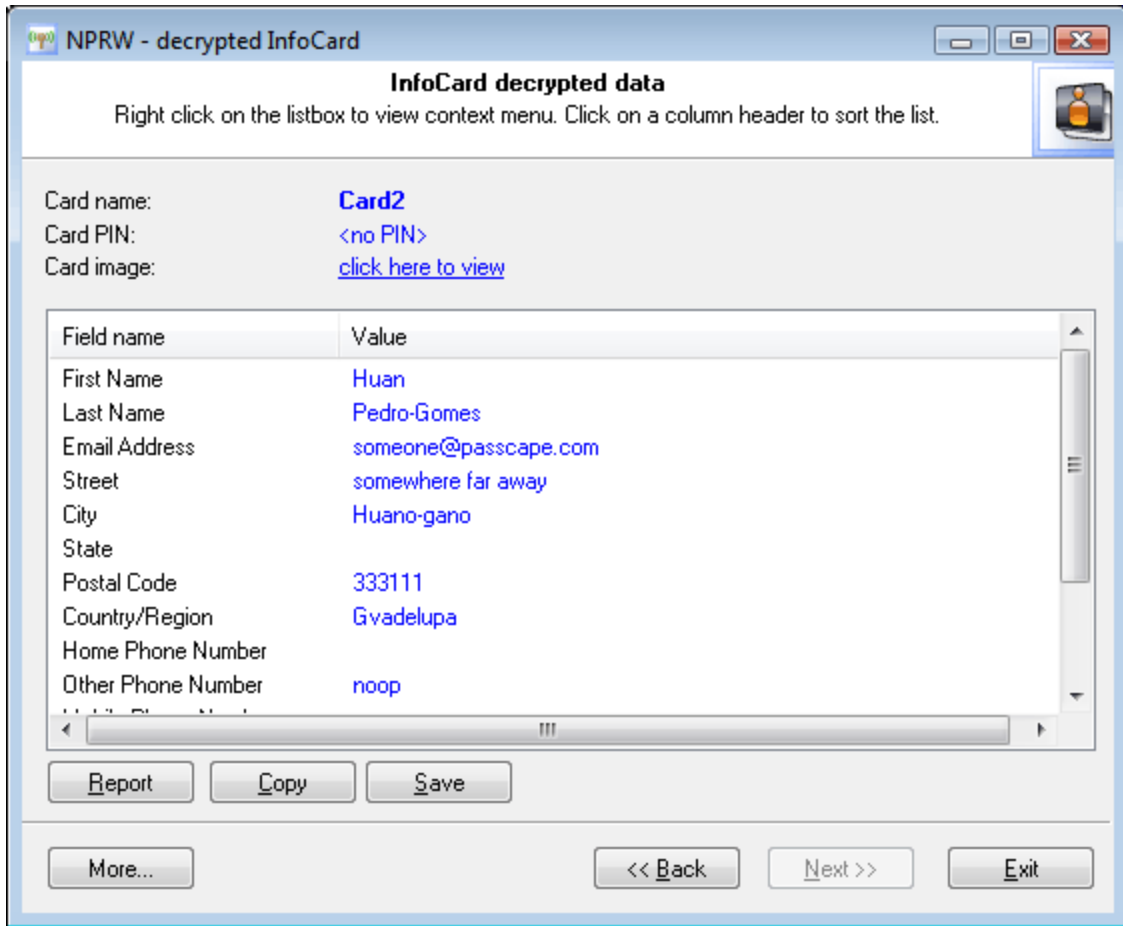
Later, if the PIN you were looking for is found, the program will notify you of that with the alert you have specified and copy the password to clipboard.

At this moment, the speed of the brute-force attack is ~5 mln. passwords/sec on a modern computer.

2.11.7 Decrypted private data

Decrypted private data

So, if the luck has shined, and the PIN has been recovered, you can move on to the recovery of private data in the selected InfoCard. The application Wizard's final dialog with decrypted claims looks like the figure below.



Personal Informion Card, as it has been stated above, contains a permanent set of personal data. Below is the list of all claims available in Personal Information Card along with their **Uniform Resource Identifiers**.

Claim	Uniform Resource Identifier	Description
First Name	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname	This attribute is used to hold the part of a person's name which is not their surname nor middle name.
Last Name	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname	This is the X.500 surname attribute which contains the family name of a person.
Email Address	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress	This attribute type specifies an electronic mailbox attribute following the syntax specified in RFC 822.
Street Address	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/streetaddress	The physical address of the object to which the entry corresponds, such as an address for package delivery.
Locality Name or City	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/locality	This attribute contains the name of a locality, such as a city, county or other geographic region.
State or Province	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/stateorprovince	The full name of a state or province. The values should be coordinated on a national level and if well-known shortcuts exist - like the two-letter state abbreviations in the US - these abbreviations are preferred over longer full names.

Postal Code	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/postalcode	The postal code attribute type specifies the postal code of the named object. If this attribute value is present, it will be part of the object's postal address - zip code in USA, postal code for other countries.
Country	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/country	Contains a two-letter ISO 3166 country code.
Primary or Home Telephone Number	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/homephone	Specifies a home telephone number associated with a person.
Secondary or Work Telephone Number	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/otherphone	This attribute type specifies an office/campus telephone number associated with a person.
Mobile Telephone Number	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/mobilephone	Specifies a mobile telephone number associated with a person.
Date of Birth	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/dateofbirth	The date of birth of a subject in a form allowed by the date data type.
Gender	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/gender	Gender of a subject that can have any of these exact string values: 0 - meaning unspecified, 1 - meaning Male or 2 - meaning Female. Using these values allows them to be language neutral.
Private Personal Identifier	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/privatepersonalidentifier	A private personal identifier (PPID) that identifies the subject to a relying party. The word "private" is used in the sense that the subject identifier is specific to a given relying party and hence private to that relying party. A subject's PPID at one relying party cannot be correlated with the subject's PPID at another relying party. Typically, the PPID should be generated by an identity provider as a pair-wise pseudonym for a subject for a given relying party. For a self-issued information card, the self-issued identity provider in an identity selector system should generate a PPID for each relying party as a function of the card identifier and the relying party's identity.
Web Page	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/webpage	The Web page of a subject expressed as a URL.

2.12 Asterisks password revealer

What is asterisks password revealer

This tool allows to recover passwords hidden behind asterisks. It is often helpful when you need to quickly recall a **** password and don't have the necessary recovery tools handy.

This tool also operates in two modes:

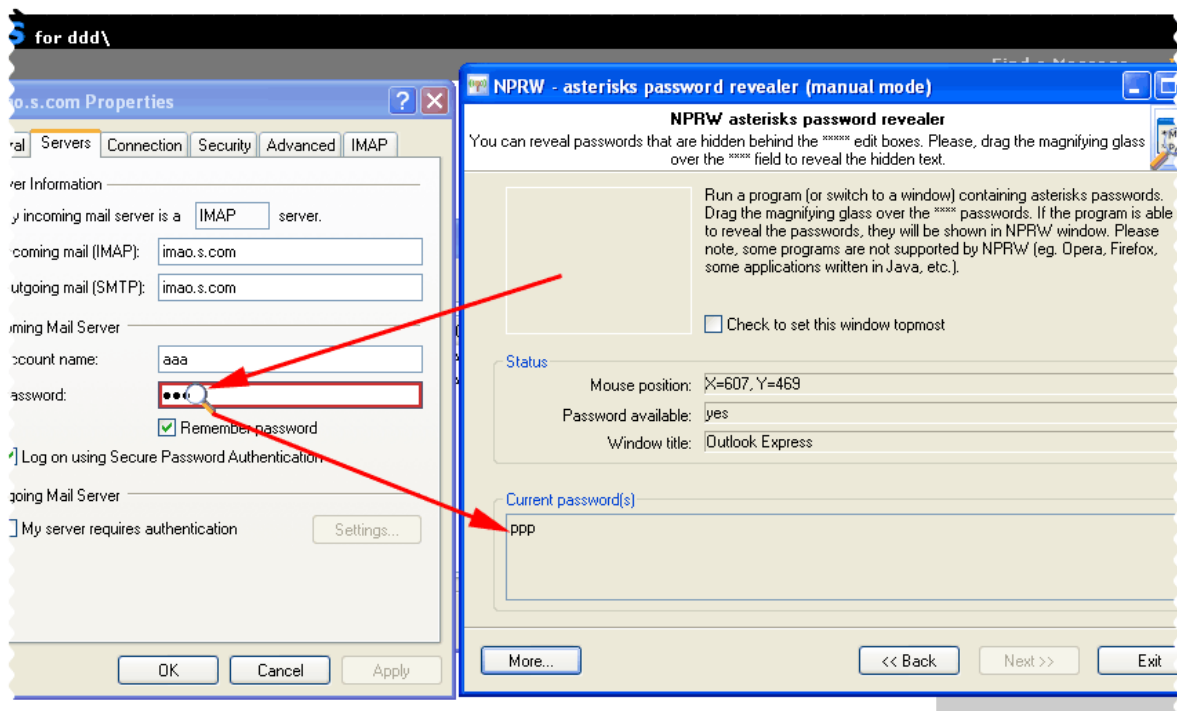
- Manual, where you would have to drag the magic magnifier from the NPRW window to the field with asterisks.
- Automatic, where the recovery application will automatically search for all the **** fields in all open windows on your desktop.

Both cases assume a number of restrictions. Well, is there anything good out there that does not have any restrictions?

- Some applications have their own GUI, and therefore Asterisks Revealer may be unable to interact with such applications. Those include Opera, Mozilla, Firefox, etc.
- Some websites have a built-in protection, which hides either the garbage or the actual asterisks behind the asterisk characters * (asterisks hidden behind asterisks!).
- In some Windows system dialogs asterisks also hide the * character and not the real password. But that happens mainly because Windows stores the majority of its passwords as hash rather than as plain text. Hence, there is just nothing to hide there.
- To ensure the proper operation of this tool, you are to have the administrator privileges. In Windows Vista, make sure that the option 'Run this program as an administrator' on the application shortcut's context menu is enabled.

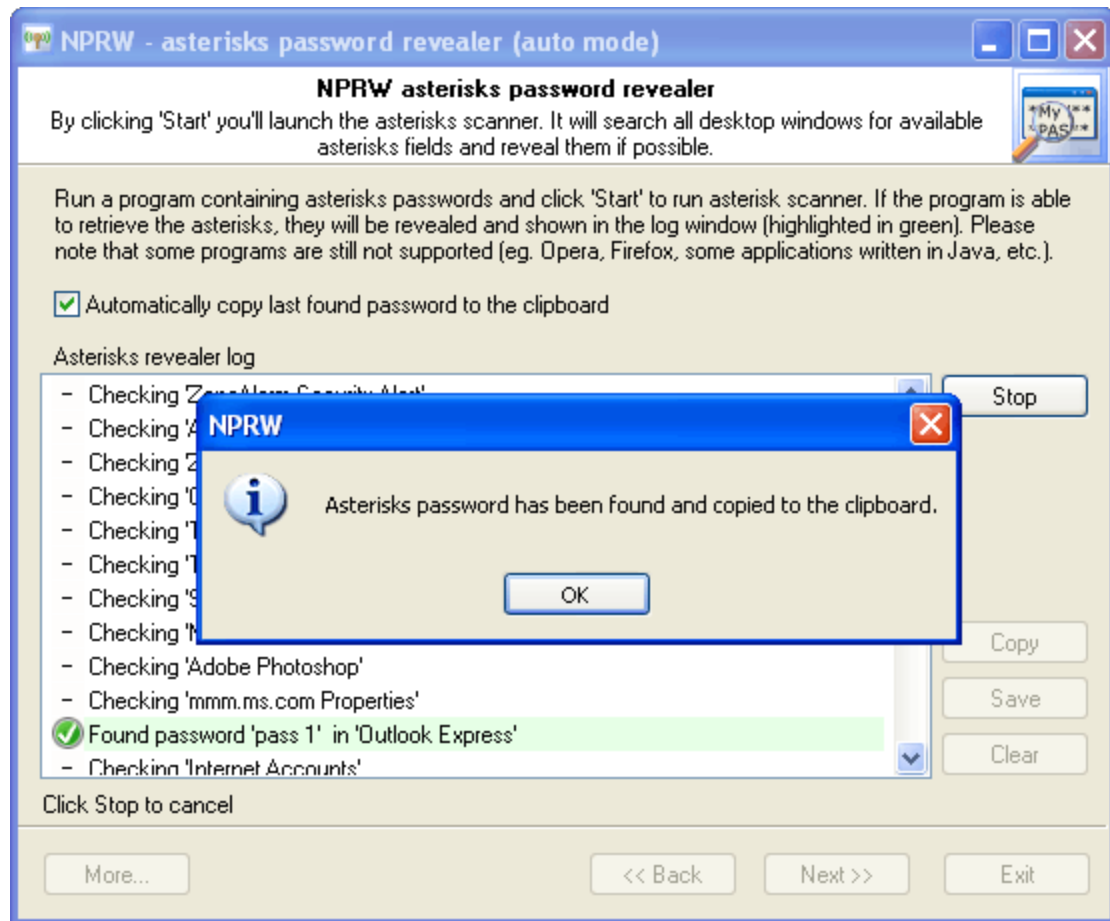
Manual recovery mode

Just drop the magnifying glass to the **** field.



Automatic mode

Or let the program do it.



2.13 Server emulators (POP3, IMAP, SMTP, FTP, NNTP)

What is virtual server

When switching an e-mail client to another, buying a new computer or reinstalling the operating system, chances to lose or forget the password to your e-mail account are great. **Virtual e-mail server** is a universal tool for recovering lost e-mail account passwords when the standard recovery tools are difficult or cannot be used for one reason or the other.

Virtual e-mail server emulates the mail server and intercepts all calls made by the e-mail client to it. When you send or receive your e-mail, your e-mail client connects to the mail server and submits your e-mail account's credentials (normally that's a login and password). Thus, the virtual server can capture and display that information to you. The software supports ALL e-mail clients that use the protocols **POP3**, **IMAP** and **SMTP**, such as MS Outlook Express, MS Outlook, Firefox, Thunderbird, Opera Mail, TheBat!, IncrediMail, Eudora, etc. Please note that the virtual server can recover only logins or passwords that are stored locally on your computer, in your e-mail application.

Virtual **FTP** and **NNTP** (news reader) servers are pretty much similar to the virtual e-mail server; therefore, the majority of what has been said about the virtual e-mail server applies to FTP/NNTP.

Emulator restrictions

A virtual e-mail server has a number of restrictions:

- It is unable to recover passwords to web-based email accounts or to e-mail accounts operating over HTTP.
- Despite the great number of authentication methods supported by the virtual server (e.g., CRAM-MD5 or NTLMv1), in some cases the instant recovery is impossible because the e-mail client does not submit the password itself; instead, it submits the password hash.
- Some authentication types are not supported by **Network Password Recovery Wizard**. Those, for example, include SPA, widely used in Microsoft products. However, in the majority of cases that restriction can be overridden (we will cover this issue a bit later).
- Some e-mail applications do not strictly follow the standard protocols IMAP, POP3 and SMTP. Those, for instance, include Outlook Express 4-6. Unfortunately, each new version of this popular application adopts new features that demand different workarounds.
- Some e-mail clients, despite the strict RFC regulations, use their own authentication mechanisms, not supported by NPRW.
- Each e-mail client acts by its own communication scenario when opening a connection session. Some applications demand the highest security level right off, regardless to the account settings. Others, the other way around, ignore the authentication type and parameters, failing to provide the required security level, transmitting personal information as plain text. There are even applications that do not support some of the declared authentication types at all.

Implementation

Virtual server has two ways of implementation:

1. Manual operating mode
2. Automatic mode

If the **manual mode** is selected, user is to configure:

First, the e-mail account in the e-mail client application. For that purpose, open the account properties, take a note of the server's address, replace it with **127.0.0.1** or **localhost** and then save the account. Once the password is (or is not) recovered, the noted server address is to be returned to its original, lawful place.

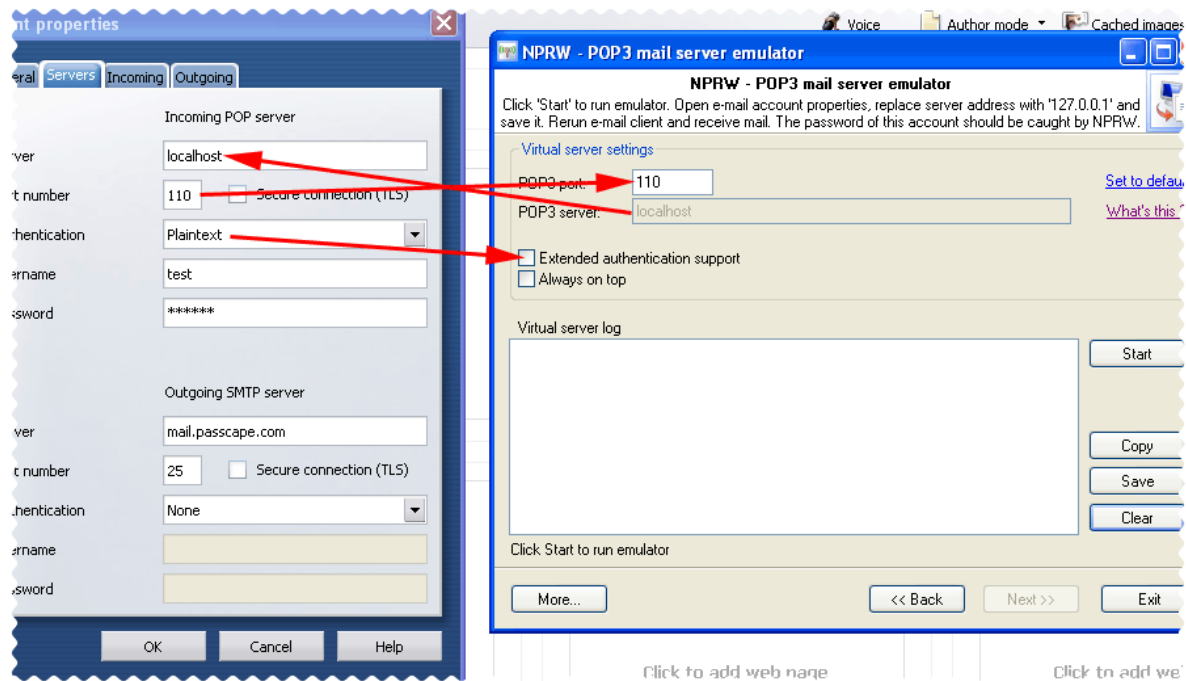
Second, in virtual server properties in NPRW, set the necessary protocol port (the application will automatically set the value used by default in the majority of cases) and the extended authentication support if necessary.

Before launching the virtual server, you are recommended to close all other applications' windows. Here is the algorithm of your actions when using the manual operating mode of the virtual server:

1. Launch your e-mail application.
2. Open properties for the account which password you want to restore.
3. Take a note of the incoming (if you need to recover a POP3 or IMAP account password) or outgoing (for SMTP passwords) server address and then replace it with **localhost**. Take a note of the protocol being used: POP3, IMAP or SMTP.
4. Save the new account settings. In some cases, you may also need to restart your e-mail application.
5. Open the NPRW virtual server and then enter the noted protocol address to it (from the account properties).
6. Launch the virtual server by clicking on the '*Start*' button.
7. Switch to your e-mail application and check your e-mail. If you need to recover an SMTP password, try to send an e-mail message instead. The message text and recipient address don't matter.
8. If all these steps have been completed properly, NPRW should 'catch' your login and password for this account.
9. If you have the additional authentication setting enabled in your account, you can try playing with the '*Extended authentication support*' option in NPRW. Or temporarily disable the additional

authentication in the account's settings. However, you should aware that some applications, including Outlook Express, can easily reset the password itself along with this option's setting.

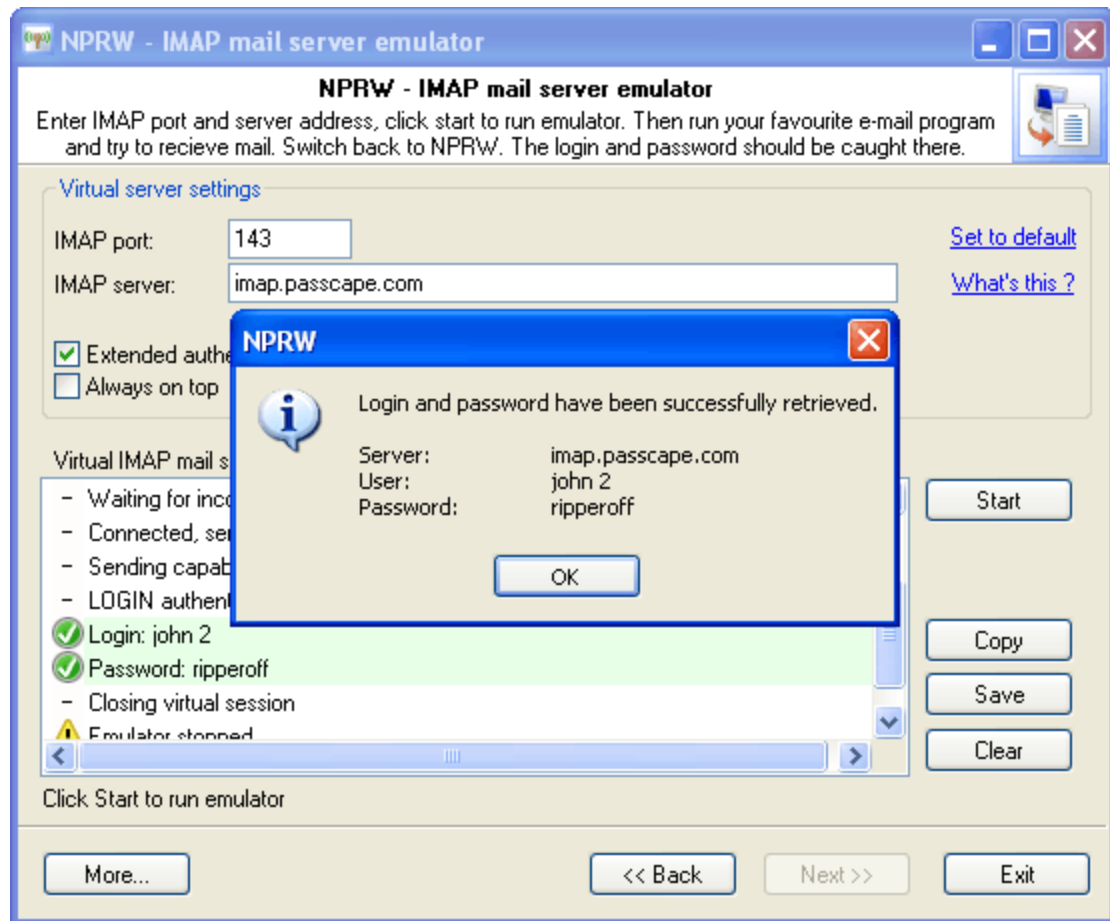
10. Repeat steps 1-9 if necessary.



The virtual server's **automatic mode** is a bit simpler in the operation and does not require any changes in the original e-mail account. However, you will need to know the mail server address (POP3, IMAP or SMTP, depending on the type of the virtual server you are running). It must be exactly the same as in the account settings. Oftentimes, the server address is identical to the e-mail address minus user name. For example, for the e-mail address user@mydomain.com, the server address is likely to be mydomain.com, mail.mydomain.com, pop.mydomain.com, pop3.mydomain.com, imap.mydomain.com, smtp.mydomain.com, etc. You can also enter the server's IP instead; e.g., 212.178.125.13.

Briefly, here is the algorithm of your actions when using the automatic mode:

1. Open the virtual server window and enter the original server address and port number. By default, the POP3 protocol uses port 110, IMAP - 143, and SMTP - 25.
2. Click 'Start' to launch the emulator. If you have any anti-virus or anti-spyware software running, on this step you may get a system configuration change and/or protocol anchor attempt warning. Don't worry; when we are done, NPRW will restore the original configuration. Allow (maybe temporarily) the anchoring to the protocol and the change of the original configuration and continue to the next step.
3. If the e-mail application is already running, please close it and then restart it all over. Then try to check your e-mail (or send a blank message in the case of SMTP). If everything has been completed properly, the NPRW virtual server's log must contain the original account's login and password (it will be highlighted with the green color). Please note that in the case of an IMAP server you may have to read your IMAP folders all over. In Outlook Express that's the 'IMAP Folders' button or the 'Tools -> IMAP Folders' menu.
4. If you have the additional authentication setting enabled in your account, you can try to disable the 'Extended authentication support' option in NPRW. In some cases, it may be helpful to temporarily disable the additional authentication in the account's settings. However, you should remember that some applications can reset the password itself along with this option's setting.
5. Repeat steps 1-5 if necessary.



Using the virtual NNTP or FTP server is completely identical to using the e-mail server. You just need to enter the nntp or ftp server address and attempt to connect to it from your news reader or ftp client.

2.14 Recovering passwords from hashes

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

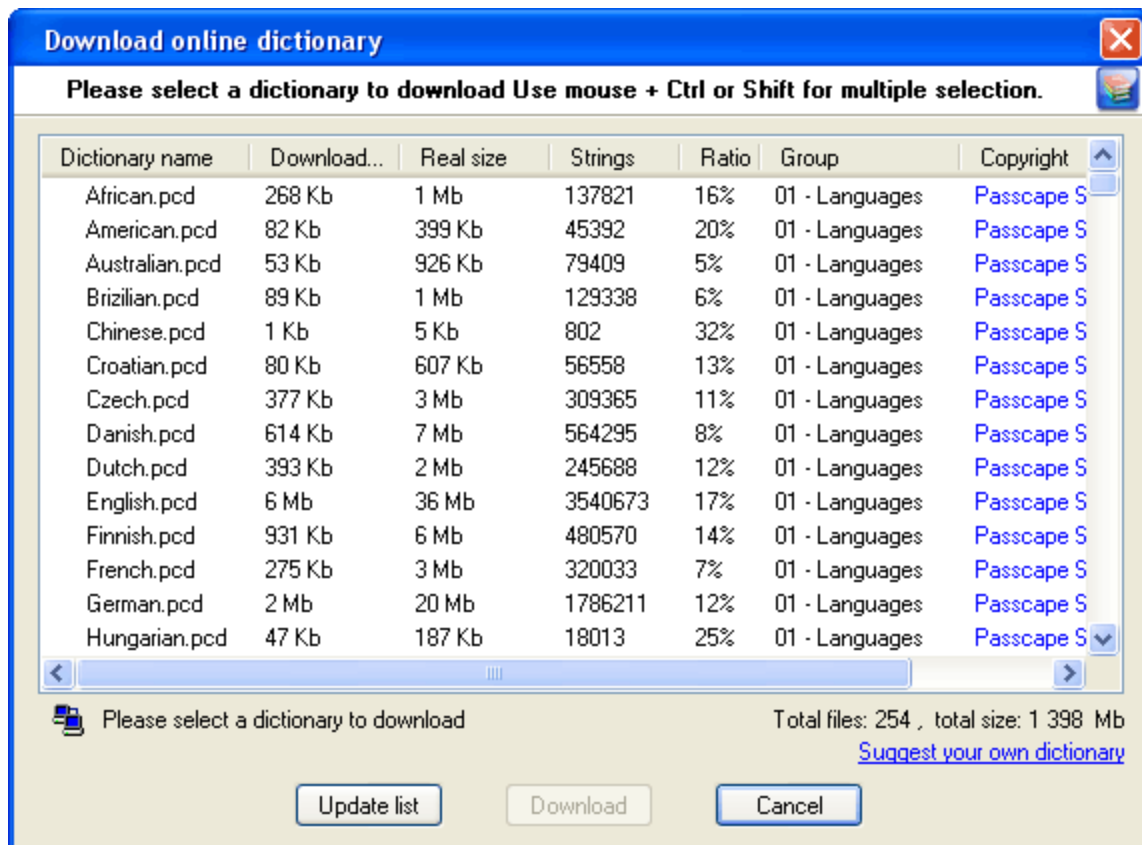
For choosing the type and the sequence of the attacks, we advise to follow this algorithm, which is applicable in the majority of cases to all types of passwords to be recovered:

- 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.

2.15 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.

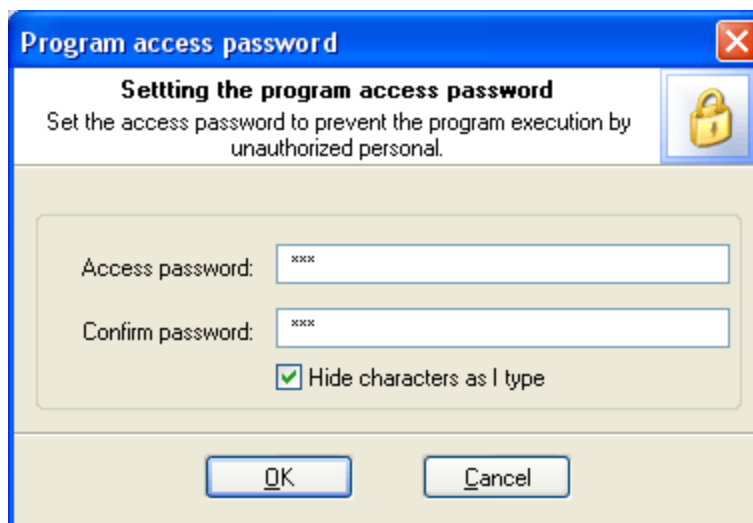
Select the dictionary you need and then click on the 'Download' button to retrieve it and use in the program.

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.

2.16 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 **NPRW** 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.

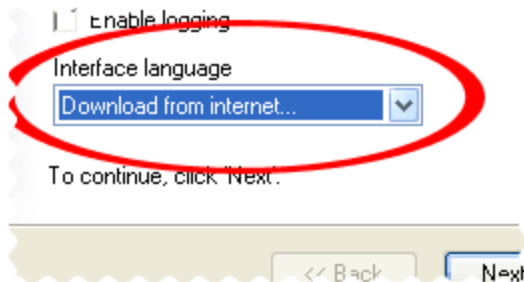
Next time you run the program, you will be asked for the password as shown below:



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

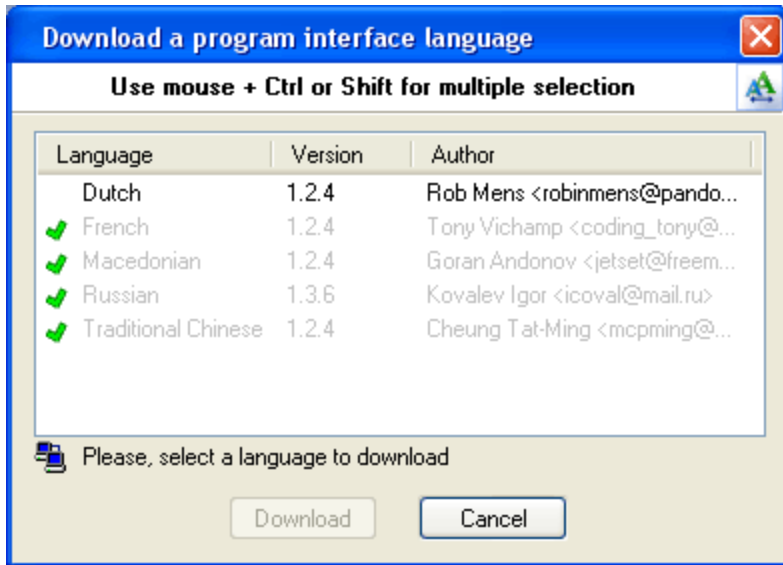
2.17 Program Interface Language

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 "Network Password Recovery Wizard" 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 long an implied warranty may last, do the above limitations or exclusions may not apply to you.

The program that is licensed to you is absolutely legal and you can use it provided that you are the legal owner of all files or data you are going to recover through the use of our SOFTWARE or have permission from the legitimate owner to perform these acts. Any illegal use of our SOFTWARE will be solely your responsibility. Accordingly, you affirm that you have the legal right to access all data, information and files that have been hidden.

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

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

3.2 Registration

You can order fully registered version of **NPRW** at a cost of \$32 for non-commercial personal usage, \$64 for business or \$410 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 **NPRW**.

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.



Registration

Please enter your registration code...

Registration information

Your name (optional): John

Registration code:

Enter the registration code exactly as given to you in the registration e-mail. If you experience any problems during registration process, please refer to program help.

Register

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 the **Network Password Recovery Wizard** shows only first 3 characters of 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 **Nprw.log** files located in the **Network Password Recovery Wizard** 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>.

- B -

Base-word attack options 32