

Passcape Internet Explorer Password Recovery

USER MANUAL

**Copyright (c) 2022 Passcape Software. All rights reserved.
Passcape Software**

1. Introduction	3
1.1 About PIEPR	4
1.2 Features and benefits	4
1.3 System Requirements	4
2. Working with the program	5
2.1 Main window	6
2.2 Manual recovery mode	6
2.3 Recovering Internet Explorer 7 passwords	8
2.3.1 Defining data source	9
2.3.2 Recovering user's Master Key. Statistics on recovered passwords.	10
2.3.3 Looking for encryption keys	11
2.3.4 Recovering data	16
2.4 Passwords window	16
2.5 Content Advisor	18
2.6 Asterisks password revealer	19
2.7 IE Cookie Explorer	19
2.8 IE URL History Cache Explorer	20
2.9 IE File Cache Explorer	20
2.10 IE Favorites Explorer	20
2.11 IE Typed URLs	20
2.12 Setting a Program Access Password	21
2.13 Program Interface Language	22
3. License and registration	23
3.1 License Agreement	24
3.2 Registration	25
3.3 Limitation of unregistered version	26
4. Technical support	27
4.1 Reporting problems	28
4.2 Suggesting features	28
4.3 Contacts	28

Introduction

1 Introduction

1.1 About PIEPR

Passcape Internet Explorer Password Recovery is a program for recovering ALL types of Internet Explorer and Microsoft Edge passwords:

- IE cached credentials
- FTP saved passwords
- IE autofill and autocomplete fields
- IE autocomplete passwords
- IE synchronization passwords
- Identity passwords
- Content Advisor password

PIEPR is the first program that can decrypt Internet Explorer passwords not only for the current user but also for any user of your system (or even of another machine). See [MANUAL recovery mode](#) for details.

1.2 Features and benefits

With this program you can:

- Recover ALL types of Internet Explorer saved passwords
- Choose between two (automatic and manual) recovery modes
- Export passwords to text html or excel files
- Turn on/off IE password caching
- Remove or add new IE password resources
- Manage Content Advisor password
- Decrypt passwords directly from Windows registry files. If your system is unbootable, just copy NTUSER.DAT registry file to floppy or flash drive and then feed it to **PIEPR**
- Reveal passwords hidden behind asterisks
- View and organize IE cookies, cached entries, favorites, typed URLs.

1.3 System Requirements

Requirements

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

Compatibility

Internet Explorer versions 3 - 11, Microsoft Edge

Known issues or bugs

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

Working with the program

2 Working with the program

2.1 Main window

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

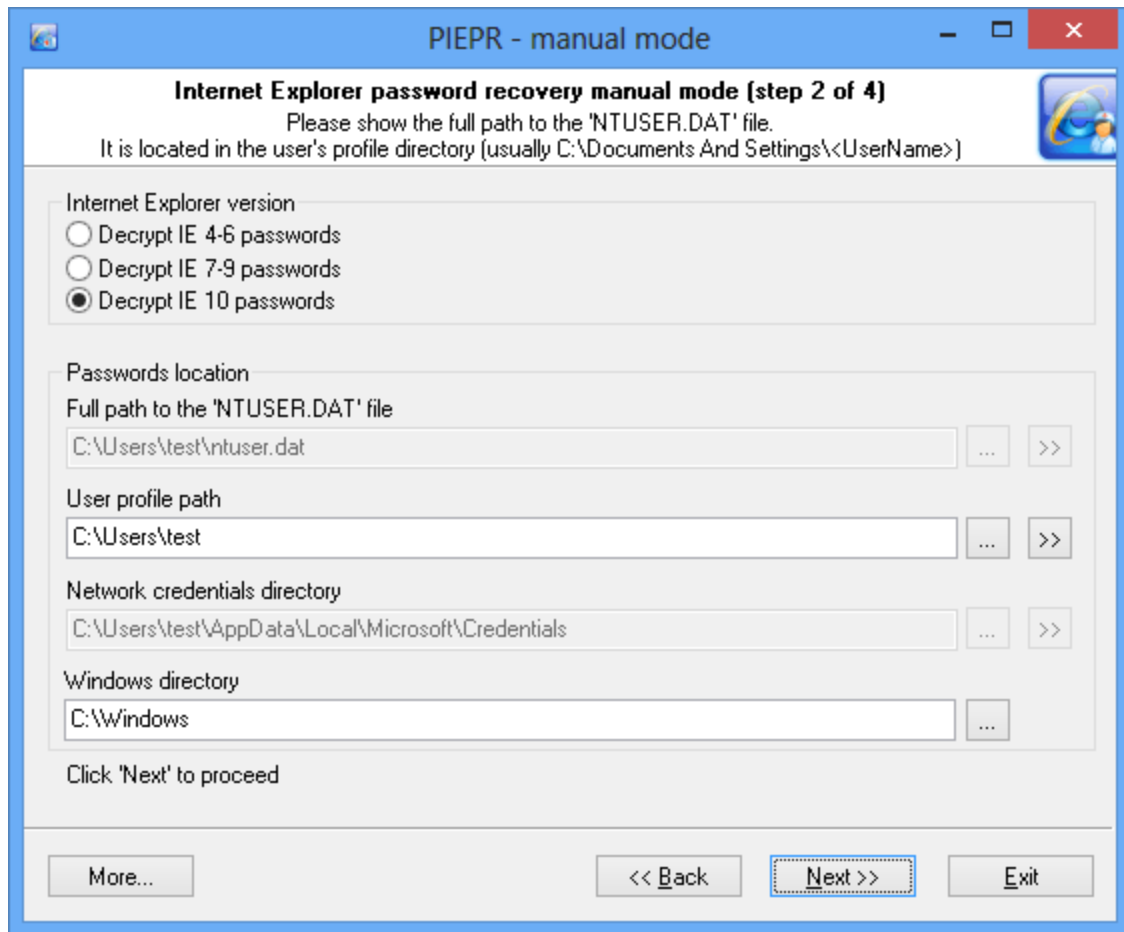
- **AUTOMATIC** - select this mode to recover IE stored passwords of the current user account;
- [MANUAL](#) - recover IE passwords for any user (you must supply a user registry file);
- [CONTENT ADVISOR](#) - manage IE Content Advisor password.
- [ASTERISKS PASSWORDS](#) - reveal text hidden behind ****

- [IE Cookie Explorer](#) - cookie viewer
- [IE URL History Cache Explorer](#) - view and organize IE cache
- [IE File Cache Explorer](#) - cached files viewer
- [IE Favorites Explorer](#) - list IE favorites entries and some usefull options
- [IE Typed URLs](#) - a list of all previously typed URLs

2.2 Manual recovery mode

To recover IE passwords manually you should provide NTUSER.DAT registry file. It is located in the user profile directory (typically C:\Documents And Settings\<USERNAME>, where <USERNAME> is the name of the user account).

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.



If you fail to boot up your system, please follow the steps below:

- 1) Create any bootable CD or USB flash drive to boot from. Use WinPE or BartPE for example.
- 2) Start the dead system from this drive.
- 3) Find and copy the file NTUSER.DAT from the user profile directory (usually C:\Documents And Settings\<AccountName>) to an USB or Floppy drive.
- 4) Find and copy the user MasterKey file from the MK directory (usually C:\Documents And Settings\<AccountName>\Application Data\Microsoft\Protect\<UserSid>) to your backup drive. If you doubt about the file name you may save all files from this directory. PIEPR will choose the correct MK file later.
- 5) Run PIEPR in the manual recovery mode and enter the full path to the registry file.
- 6) You will be asked for additional information as shown below.



Enter the user logon password and the MasterKey path, then click 'OK' to move on to the FTP password decryption.

Note. Steps 4 and 6 are not required if you don't have FTP passwords or FTP passwords are not encrypted.

2.3 Recovering Internet Explorer 7 passwords

Unlike its older brotherhood, the new version of Internet Explorer 7 - 9 utilizes absolutely different concepts of encrypting private data, without saving encryption keys. That makes it extremely difficult to recover such data, especially in the automatic mode. Therefore, to ensure the complete recovery of the password, we have added the manual operating mode to the application's Wizard as an alternative to the automatic recovery mode. More flexible and advanced, it uses some specially invented algorithms and allows extracting keys that are unavailable in the automatic mode.

The manual mode can be theoretically split into 5 parts or 5 steps of the application's Wizard. To be more accurate, there are just 4 steps, and during the first step you are to choose the operating mode itself.

[Step 1: Select the manual operating mode.](#)

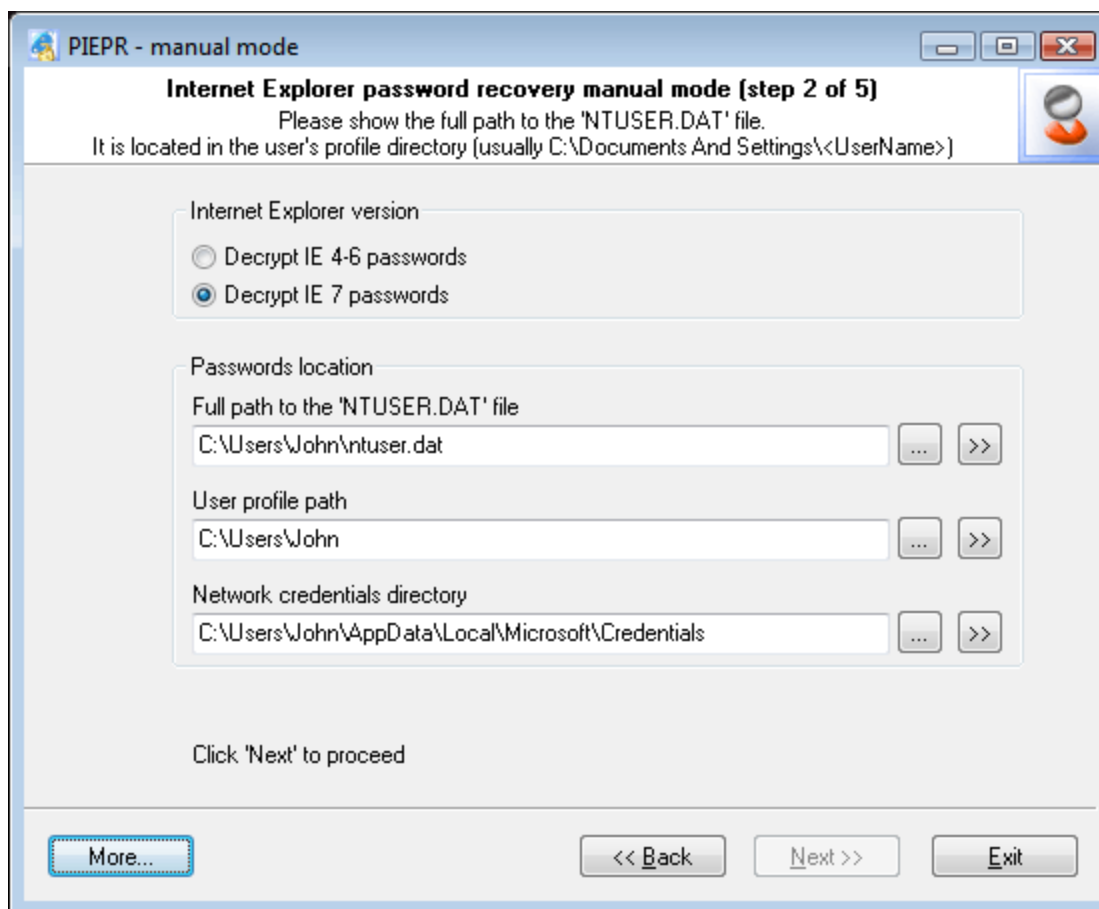
[Step 2: Defining the data source. Select the data source.](#)

[Step 3: Recovering user's Master Key. Statistics on recovered passwords.](#)

[Step 4: Gathering encryption keys.](#)

[Step 5: Recovering data.](#)

2.3.1 Defining data source



On this, second, step of the manual recovery, you will be prompted to enter the three parameters that are necessary to start the recovery process. Actually, the software will try to acquire all the necessary data automatically; however, if it fails to succeed, it will ask you to enter the necessary data by hand.

1. **Path to user's registry file** (ntuser.dat), which is located in the user's profile. User's registry is the main container that stores three types of encrypted IE7-9 passwords (there are totally 4 of those). In Windows XP-2003, path to this file normally looks like this: *C:\Documents And Settings\%USER%\ntuser.dat*, where *%USER%* stands for your account name. For Vista/7/8, the default path may look a bit different: *C:\Users\%USER%\ntuser.dat*. This parameter is mandatory, and the further recovery is impossible unless this parameter is supplied.
2. **Path to user's profile** (optional parameter). The software normally detects it automatically by user's registry located in it (see above). User's profile folder is the starting point for the automatic detection of some other options that appear on the next step. If this parameter is not set, the recovery wizard will be unable to find out the path to user's **Master Key** on the third step, and the further recovery is only possible when that parameter is properly supplied.
3. **Network credentials directory** (optional). **Windows Credentials Manager** creates and controls this folder, storing many applications' private data in it. Those may include domain and LAN passwords, .Net Passport accounts, Exchange server passwords, etc. All of that data is encrypted and stored in network credentials directory. In our case, we are particularly interested in IE7's Web passwords to protected websites, which are also known as **Wininet Credentials**. For more information on Wininet Credentials, please take a look at our article on Internet Explorer passwords. In Windows XP-2003, Wininet Credentials can be stored in two different folders: *C:\Documents And Settings\%USER%\Application Data\Microsoft\Credentials\%SID%* or *C:\Documents And Settings*

%USER%\Local Settings\Application Data\Microsoft\Credentials\%SID%. Please note that %USER% stands for your Windows account name, and %SID% is the SID of the user whose passwords are to be recovered. In Vista/7/8, SID is not used in the network credentials directory name, so the path to the encrypted Wininet Credentials data looks a bit different: C:\Users\%USER%\AppData\Local\Microsoft\Credentials and C:\Users\%USER%\AppData\Roaming\Microsoft\Credentials.

Here is a couple of examples with real paths to NCD:

- C:\Users\John\AppData\Local\Microsoft\Credentials
- D:\Documents and Settings\Kate\Application Data\Microsoft\Credentials\S-1-5-21-1927147842-1992852531-225342917-1003.

It is very convenient to use the >> button to find out a local user's network credentials directory. When you click on that button, you will be prompted to choose the required local user's profile, and the software will automatically choose the network credentials directory corresponding to that. If the data that were required for the recovery were taken from another computer, you will have to enter the path to network credentials directory manually (by clicking on the ... button).

2.3.2 Recovering user's Master Key. Statistics on recovered passwords.

PIEPR - manual mode (IE7)

Internet Explorer password recovery manual mode (step 3 of 5)

Please setup correctly the user logon password, the MasterKey file and the SID of the passwords' owner.
Without this data you will not be able to decrypt IE7 passwords.

Passwords statistics

Autoform fields found:	1
Autocomplete passwords found:	2
FTP passwords:	0
Wininet credentials:	?

User logon information

Owner logon password

☐ Hide characters as I type

Owner MasterKey file
C:\Users\John\AppData\Roaming\Microsoft\Protect\S-1-5-21-39778491498-...

Owner SID
S-1-5-21-3977849149-3191733863-3911273036-1003

Click 'Next' to proceed

More... << Back Next >> Exit

On the third step, the recovery wizard that you have supplied with the necessary information will attempt to find out whether any IE 7-9 passwords are available and how many of them are there. The *Password Statistics* section will display information on the found (but not yet recovered) passwords. The software can find out the number of available Wininet Credentials only after you have:

- Entered a correct Network Credentials directory parameter on the previous step of the recovery wizard.
- Filled all options in the User logon information section, including user's password.

Usually, the software automatically finds the *Owner MasterKey* file and *Owner SID* the parameters for a local user. However, you can specify those manually. By default, user's *Master Key* file is stored in the following folders:

XP-2003: C:\Documents and Settings\%USER%\Application Data\Microsoft\Protect\%SID%

Vista: C:\Users\%USER%\AppData\Roaming\Microsoft\Protect\%SID%

The text parameter *Owner SID* is normally the same as the %SID% folder name.

Once you have entered a correct password in the User logon information field, the software will count the number of Wininet credentials, and the **Next >>** button will be enabled, so you can go on to the next step of the wizard – gathering the encryption keys.

2.3.3 Looking for encryption keys

Gathering encryption keys is the most important and crucial moment in the entire recovery process. As it was mentioned before, the encryption mechanism in Internet Explorer 7-9 was purposely made up such way that whenever it is possible, the application would not store its encryption keys on the local computer. So, before you get started with searching and picking the keys, you will have to understand the IE's concept of operation used when encrypting passwords and form data. For now, you can forget about *FTP* and *Wininet* passwords, since on this, fourth step of the recovery wizard, the software has sufficient information to recover them completely.

So, the encryption algorithm for autocomplete passwords in IE 7-9 looks as follows:

1. During the first visit to the Web page, once user has entered the password, IE 7 saves the current page's **URL** and calculates a hash from that address **hash=SHA(URL)**.
2. The **URL** saved on the previous step (a Unicode-based text string) is used as the encryption key. This key is used for encrypting the password with strong encryption algorithms (DPAPI).
EncryptedPassword=DPAPI(URL,password).
3. The **EncryptedPassword** is linked to the **hash**, and both of those values are stored in the user's registry.
4. The URL is purged as it is no longer necessary.

The only conclusion that comes from the above is that unless one knows the original URL, he will be unable to recover the password, for the reverse recovery of the URL from the hash is literally impossible. On the other hand, it is not at all necessary to store the encryption key (URL) on the local computer.

But then how does IE recover its own passwords? – Well, very simply...

When the website is visited again, Internet Explorer again calculates a hash from the URL. Then it verifies the obtained hash against all values (**hash + EncryptedPassword**) that are stored in the registry. If one of the hash values stored in the registry has matched, the encrypted password linked to that hash is recovered with the **URL** supplied as the corresponding key.

The encryption of autofill data is implemented a bit different way. For example, if the authentication page has fields for entering login and password, the login is encrypted and stored different way than the password. The basic difference is that instead of the URL the software uses the field name in the HTML form for the encryption key. Let's take a look at an excerpt of an html file that contains a form for entering login and password.

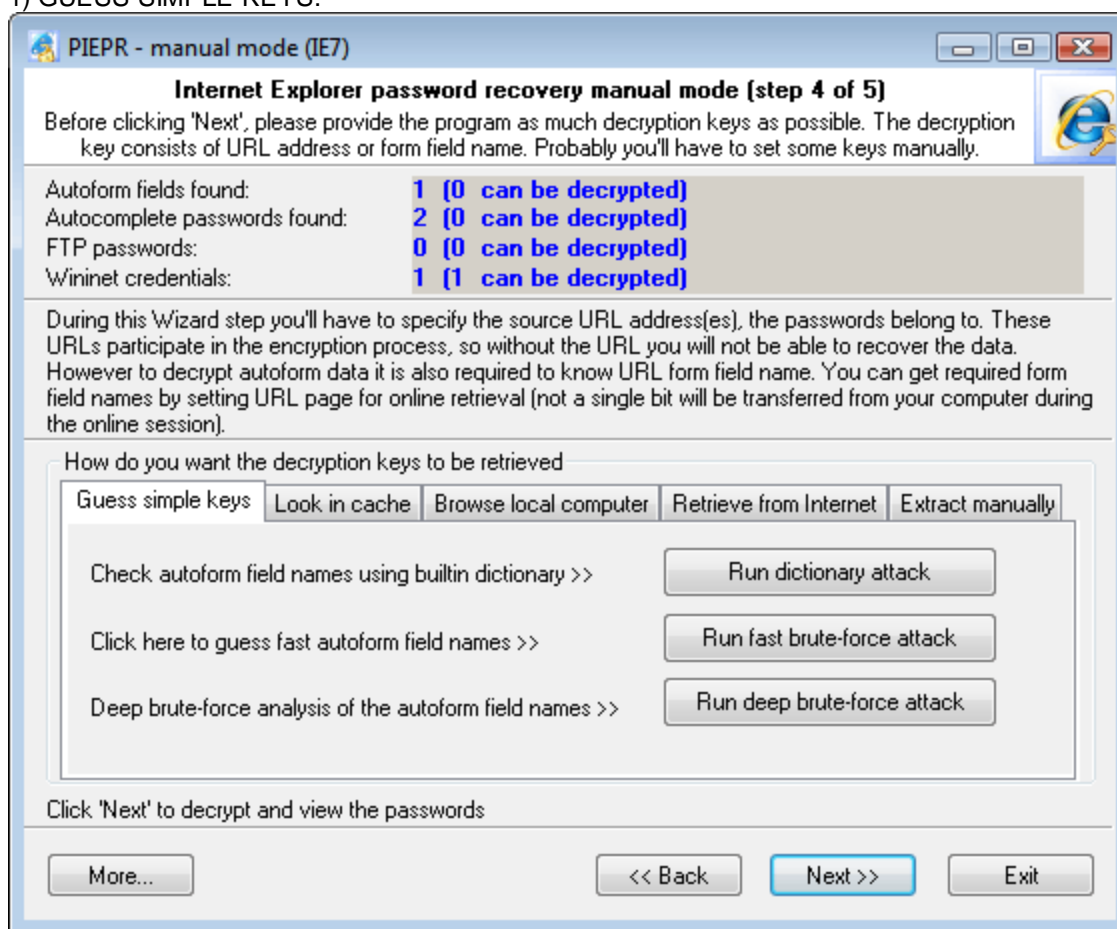
```
<table><tr>
<td><input type="text" name="loginname" value=""><br></td>
<td><input type="password" name="pwd" value=""><br></td>
```

</tr></table>

In our case, the form field name and the encryption key will be the text value **loginname**. Other than that, the encryption mechanism for autoform data is completely the same as the mechanism for encrypting password.

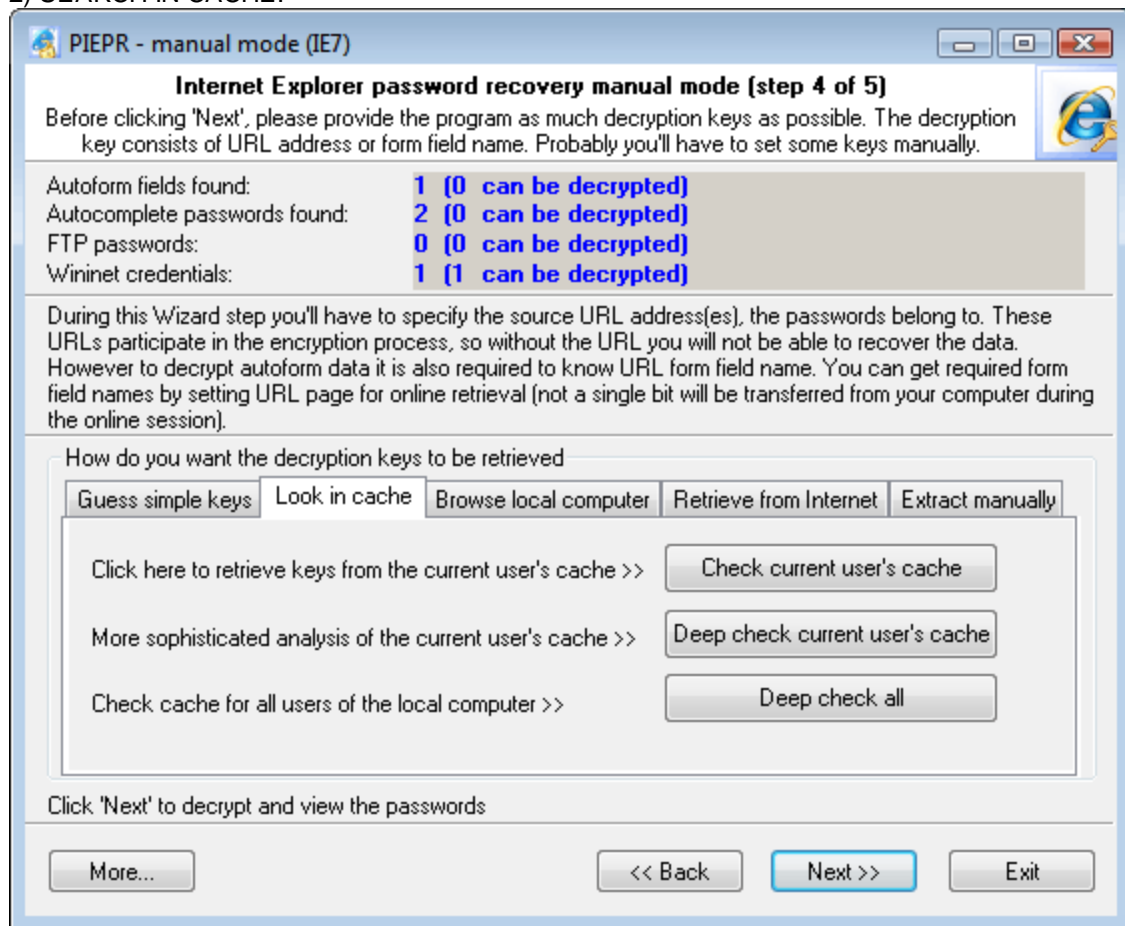
Therefore, for the complete recovery of autoform fields and autocomplete passwords in IE 7 we have created such a tricky and not so clear at first user interface. The five tabs that you see on the screenshot are just the five methods that you can utilize to recover encryption keys (let us know if you know more). Those keys, in their turn, are required to recover the found passwords. The number of recovered passwords depends directly upon the efficiency of your actions on that step. So, here is a brief description of each method.

1) GUESS SIMPLE KEYS.



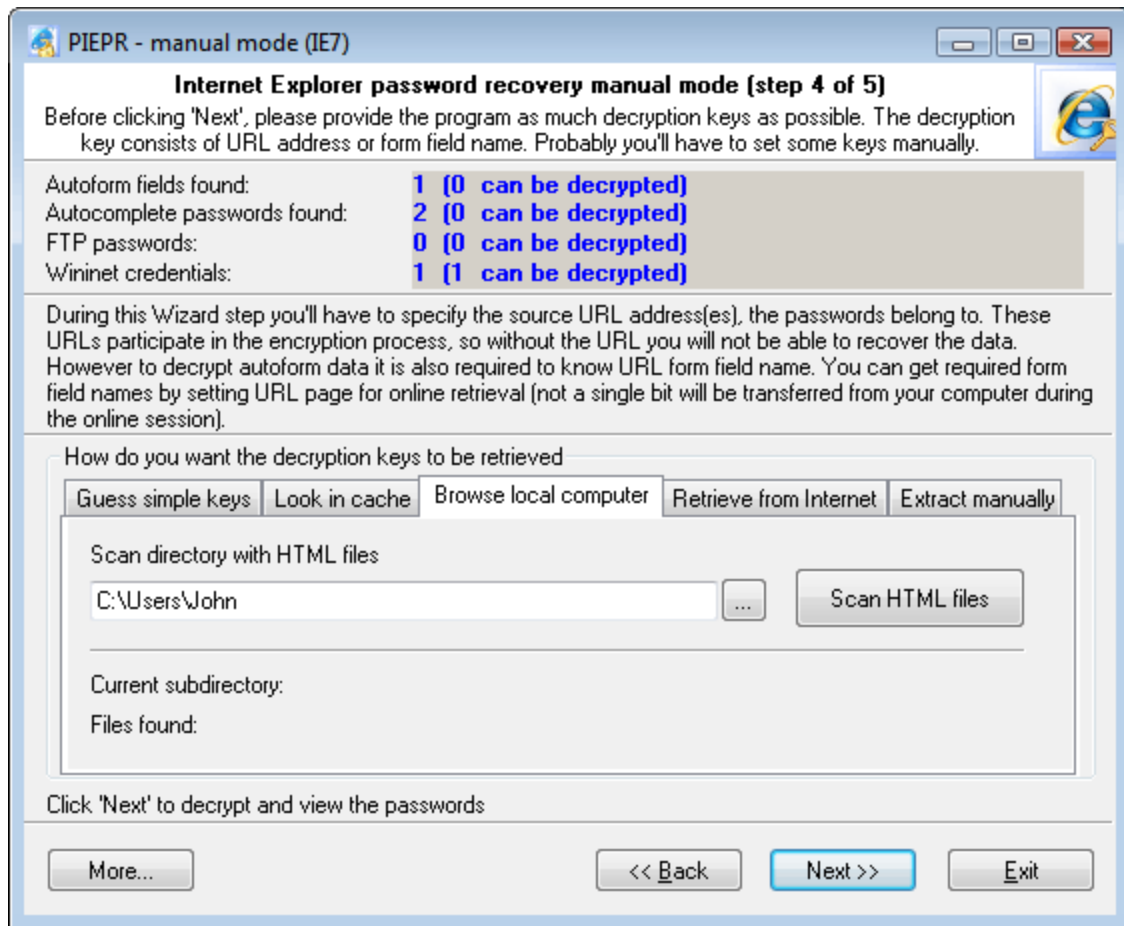
This method allows finding autoform encryption keys using dictionary or brute-force attack. When you click on the **Run Dictionary Attack** button, the software will search for the keys using the built-in dictionary, which comes along with the application. If you want to use your own dictionary, just name it *custom.dic* and copy it to the program's installation directory. You can also attempt the brute-force attack, where the software will check the password against all possible combinations of letters and numbers. However, the major drawback of this method is that it can be efficiently used only for short (up to 6 characters) keys. In the next version of the software, we are planning to introduce a new type of attack using smart mutations.

2) SEARCH IN CACHE.



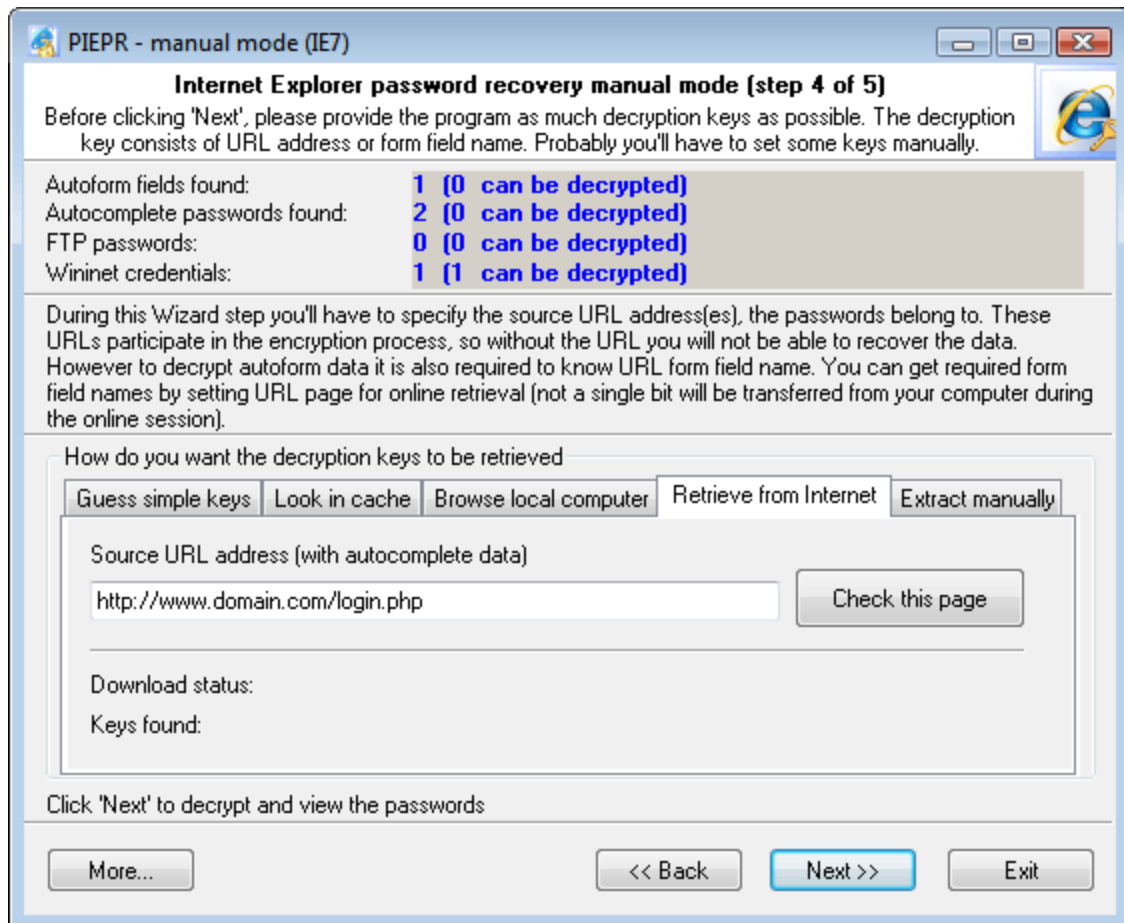
On this tab, you can attempt to find your lost Internet Explorer 7-9 encryption keys (for both passwords and forms) in your local computer's cache. When you click on the **Check Current User's Cache** button, the application will launch the quick key search in the current user's cache. To launch the deep search, you will need to click on the **Deep Check Current User's Cache** button. Despite that it is slightly slower than the previous one its major advantage is that the search is performed independently of Windows API functions. However, the slowest but sometimes most efficient method for finding autoform keys is the third search type (**Deep Check All**), where the search is performed in all users' cache on the local computer.

3) BROWSE LOCAL COMPUTER.



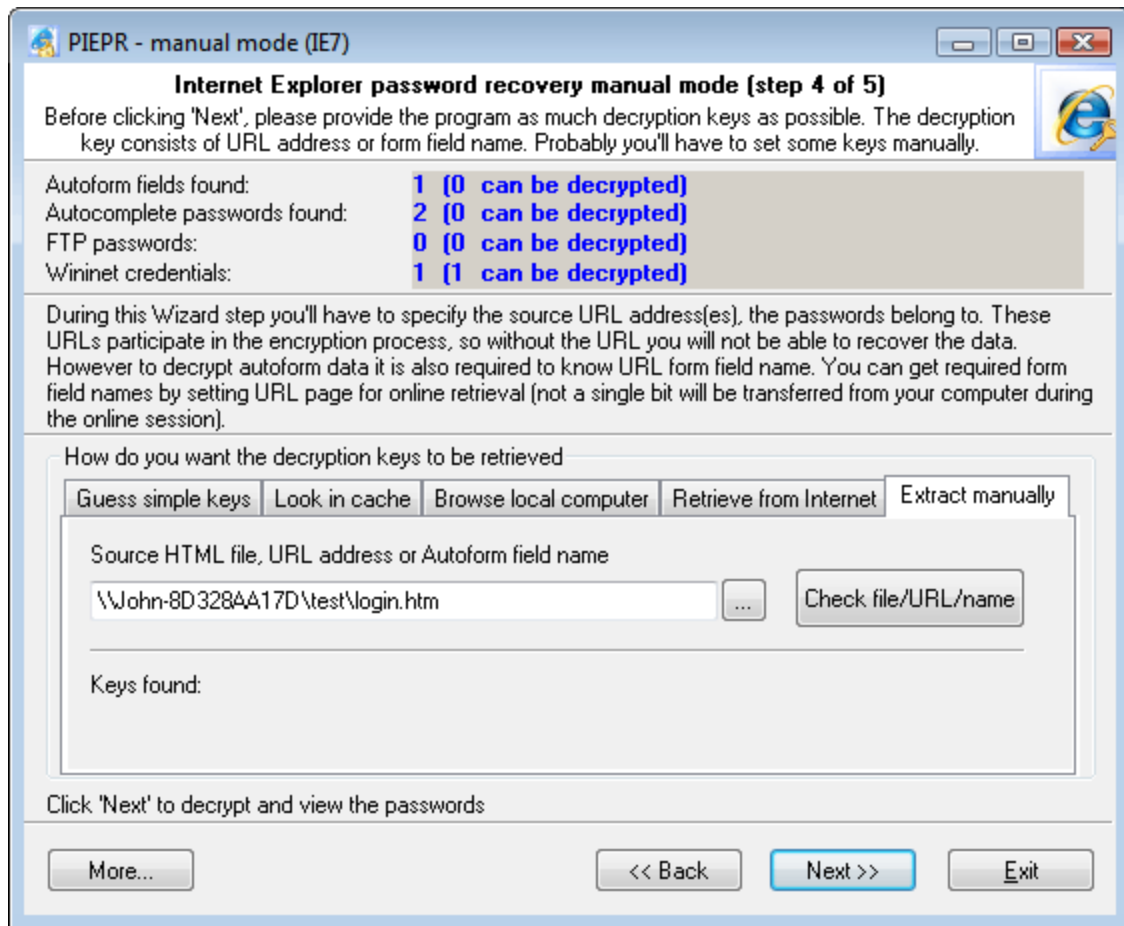
This tab only allows finding encryption keys for autoforms. To go on with this method, you will need to specify the path to the folder with html files. It doesn't matter what kind of files those are; the idea is to get as many files as possible. Such folder, alternate to Internet Explorer cache, for example, could be a folder with html files from another browser. For example, *Opera* stores (caches) all visited pages to a special location (normally C:\Documents and Settings\%USER%\Application Data\Opera\Opera\profile\cache4). Once such folder has been specified, you can get started with scanning the HTML files and verifying all the found form field names. These names very often match those that you are to find.

4) RETRIEVE FROM INTERNET.



If you've got any passwords still not recovered (the statistics appears at the top of the dialog window), this tab will be your last source of hope. Enter the URL of the page (you can copy it from your browser's Address line), which you are to recover the passwords for, and then click Check this page. The software will attempt to perform two things. First, it will check whether the URL is good as the key for the remaining autocomplete passwords. Then it will attempt to download the specified page off the Internet to check it for the autofill keys. In the next versions, the software will possibly support URL lists.

5) MANUAL RECOVERY.



Finally, the last tab for a despaired paranoiac.

You don't have to be connected to the Internet to get started with it. However, you can specify:

- HTML file – for searching autoform encryption keys
- URL address – for verifying autocomplete passwords
- Name of a specific field on the html form – to verify autoform encryption keys.

The tabs follow one another according to their efficiency. The most efficient method for finding keys is dictionary attack on the **Guess simple keys** tab. It is followed by the **search in IE cache, processing html files, retrieving from the Internet**, and, finally, **manual recovery**. If you've got at least one still not recovered password, try all these recovery methods before clicking **Next>>**.

2.3.4 Recovering data

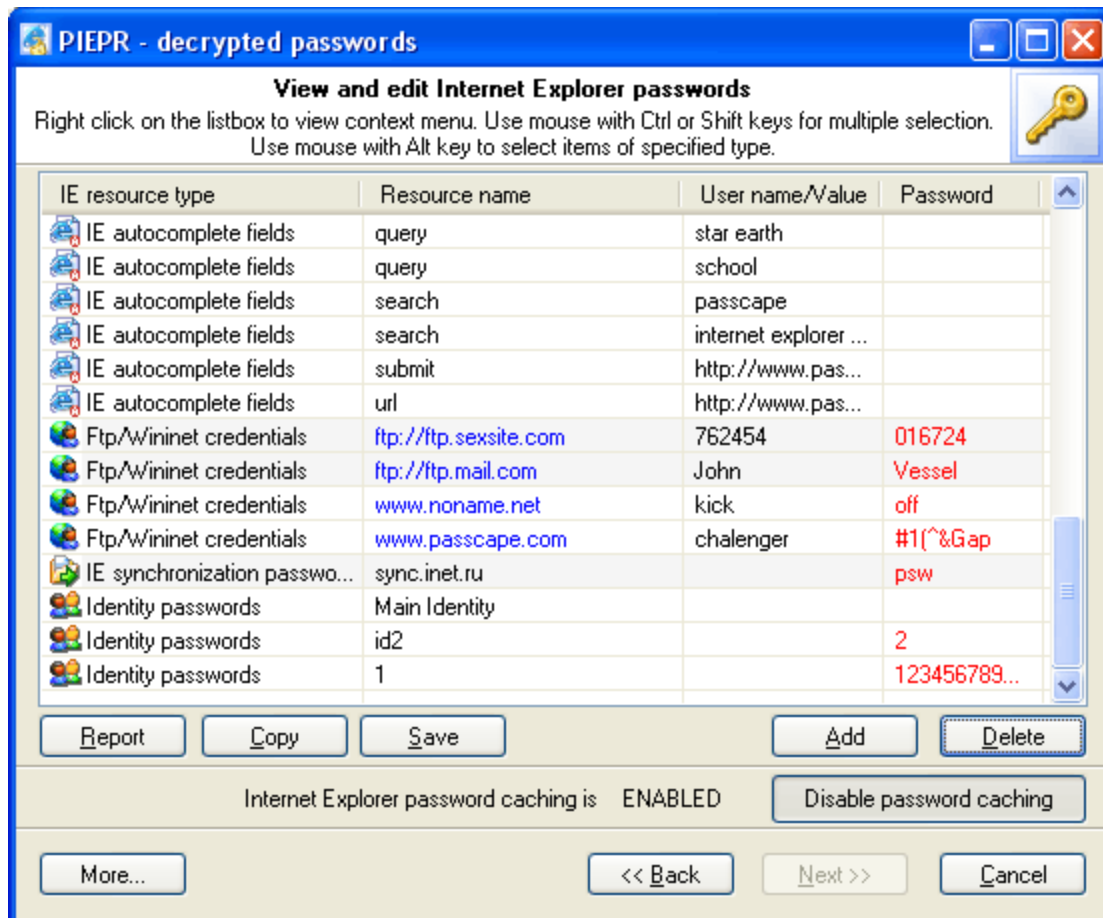
On the final step, the recovery wizard will analyze all the obtained keys and recover the original encrypted data.

2.4 Passwords window

The password window contains IE decrypted passwords of the following types:

- IE cached credentials
- FTP saved passwords

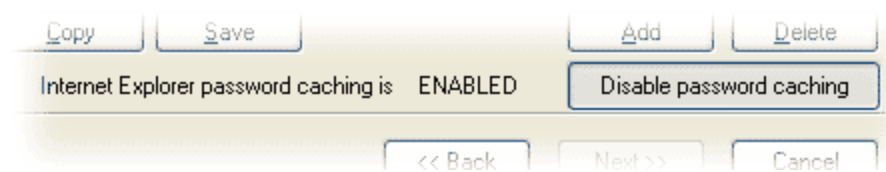
- IE autofill and autocomplete fields
- IE autofill passwords
- Synchronization passwords
- Identity passwords



Right click on the passwords list to view context menu.

When you run IE and attempt to view a password-protected site, you are prompted to type your security credentials in the Enter Network Password dialog box. If you click the Save this password in your password list check box in this dialog box, your computer saves your password so you do not have to type the password again when you attempt to use the same document. This is known as password caching.

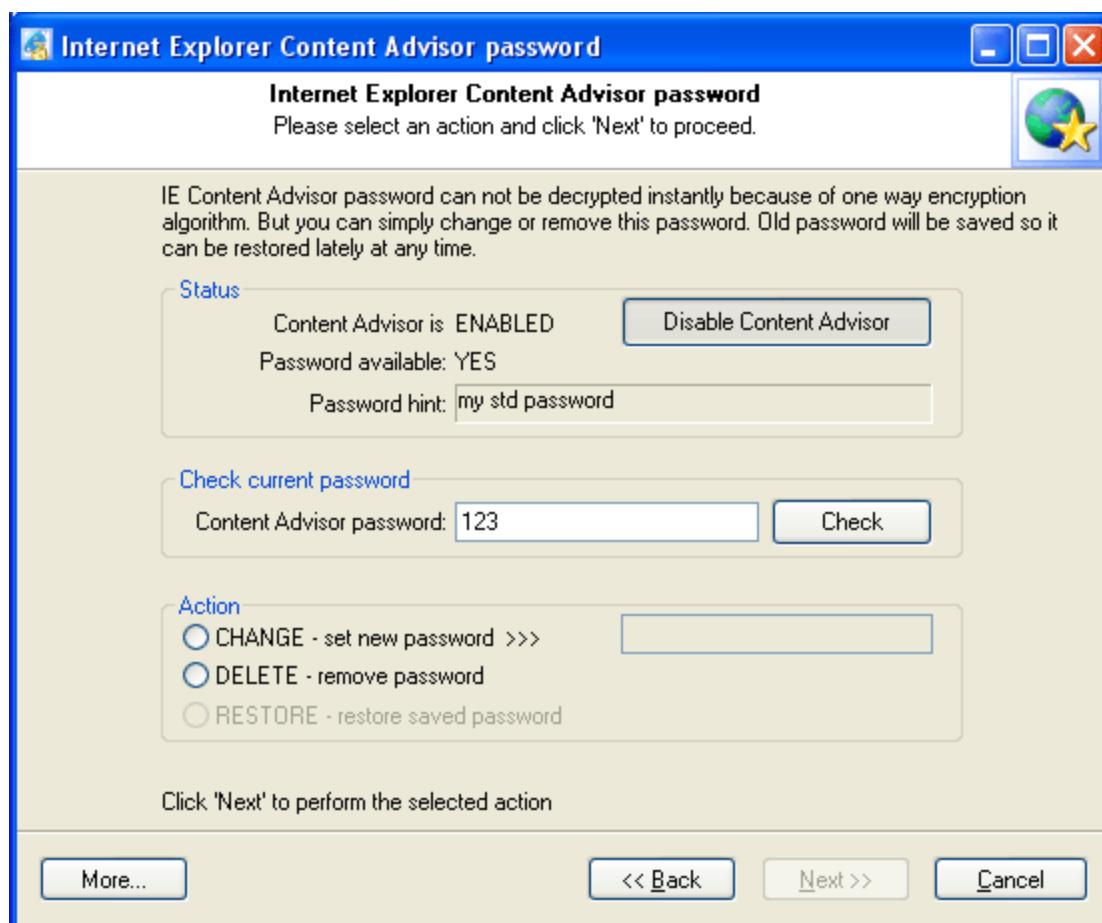
PIEPR v1.1 allows you to enable/disable Internet Explorer password caching (for **AUTOMATIC** recovery mode only).



Just click 'Disable password caching' button to disable it. The password caching will be disabled and button text will be changed to "Enable password caching" state. Click again to enable password caching.

2.5 Content Advisor

Another feature of this program is the ability to remove, change and recover password to IE Content Advisor. If you lost or forgot a password to your Content Advisor, you'll be unable to use Internet Explorer. **PIEPR** solves this problem by temporary removing a password to Content Advisor or letting you to turn it off. Select **CONTENT ADVISOR** option in the main wizard window and press **Next** button to view IE Content Advisor password dialog.



Status groupbox shows current Content Advisor information:

- Content Advisor status (**ENABLED** or **DISABLED**)
- Password availability (whether the password was set or not)
- Password hint (may be empty)

Check current password groupbox allows you to check current password (if one was set)

Action groupbox allows you to manage IE Content Advisor password. You can change the password to your own or just delete it.

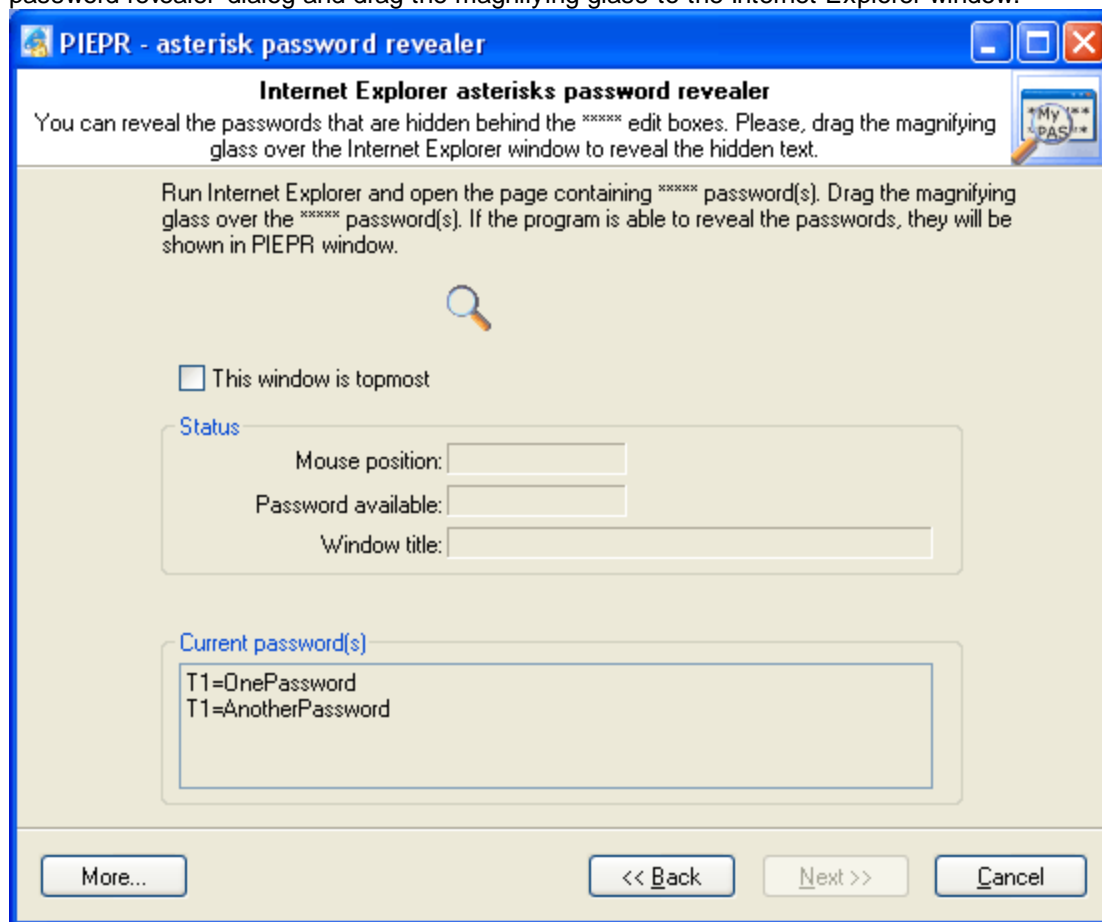
- to *change* current password check **CHANGE** option, enter a new password in edit box at the right side and press **Next** button. Old password will be remembered (saved) so you can restore it later if needed.
- to *remove* current password check **DELETE** option and press **Next** button. Old password will be remembered as well.

- to *restore* last changed/deleted password check **RESTORE** option and press **Next**.

Please don't forget to close Internet Explorer before run the program. Otherwise the changes will take no effect.

2.6 Asterisks password revealer

Sometimes it is required to reveal the password that is hidden behind the ***** edit boxes. PIEPR can solve this problem and recover Internet Explorer text that is under the asterisks. Just open 'Asterisks password revealer' dialog and drag the magnifying glass to the Internet Explorer window.



Also note, that you can reveal ***** passwords for all programs that use IE frames (including Outlook, Outlook Express, Windows Explorer, some IE based browser etc.).

2.7 IE Cookie Explorer

A cookie is a text file stored on your computer by a web server. Cookies were developed to help users to navigate visited sites. But often cookies criticized for weak security and inaccurate user identification. You can read more information about cookies from [here](#).

IE Cookie Explorer is a new feature that was added to PIEPR v1.3 to help you to navigate through the Internet Explorer stored cookies. Just click a cookie entry to view it. Also you may remove suspicious cookies from your local computer.

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

2.8 IE URL History Cache Explorer

Internet Explorer traces and remembers sites you've ever visited and files you've ever opened. It is also known as URL history caching and helps to boost your internet speed.

The URL History dialog allows you to view and remove the cached entries and files, as well as to manipulate some IE cache options.

2.9 IE File Cache Explorer

Almost the same as URL History Cache Explorer, but shows only cached files instead of visited sites.

You can click entry with  icon to view an image.

2.10 IE Favorites Explorer

View IE Favorites (a list of web pages you've created as your favorites).

Probably you may find useful two options here:

- 1) Disable "Favorites" menu. Check it to hide completely your Favorites from IE.
- 2) Hide rarely visited sites. Rather useful option if your Favorites list is very large.

2.11 IE Typed URLs

Sometimes it is urgently required to remember the site or web page you've entered some time ago. All IE typed URLs are stored in Windows registry thus can be recovered.

IE Typed URLs dialog allows you to view all previously typed URLs or to remove them if needed.

You can also turn on/off IE URL AutoComplete here.

2.12 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 **PIEPR** main window) and select the '**Set/change access password**' from the popup menu.



To set an access password, please 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.

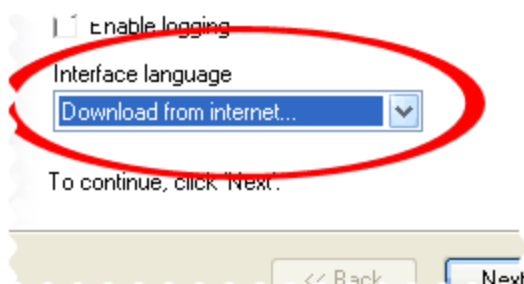
Next time you run the program, you will be asked for the password as shown below.



Just type your current password in the password box and click **OK** button to start the program.

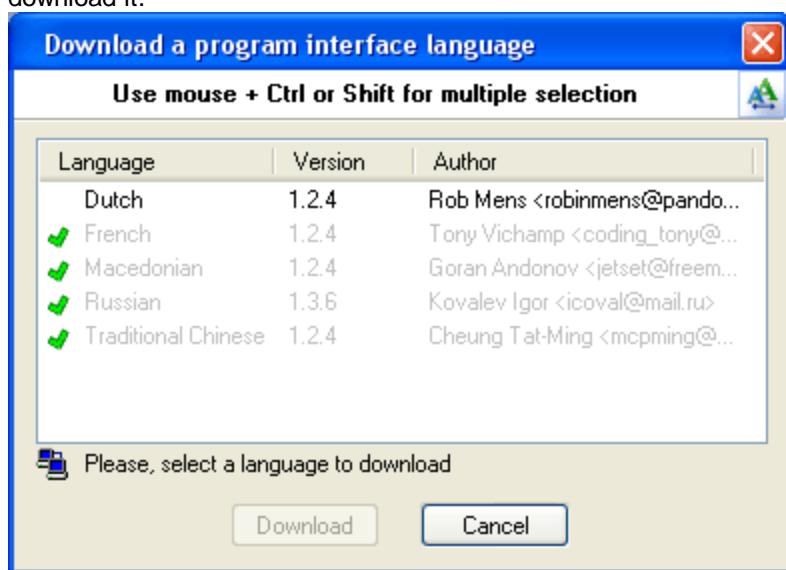
2.13 Program Interface Language


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 "Passcape Internet Explorer Password Recovery" software product ("SOFTWARE").

All copyrights to SOFTWARE are exclusively owned by Passcape Software.

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

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

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

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

With the personal license, you can use the SOFTWARE as set forth in this Agreement for non-commercial purposes in non-business, non-commercial environment. To use the SOFTWARE in a corporate, government or business environment, you should purchase a business license. With the business license you can run the SOFTWARE on multiple computers within a single site. A multi site license authorizes you to install and use the SOFTWARE to any number of computers belonging to your organization - no matter where they are located.

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

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

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

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

Passcape Software does not warrant that the software is fit for any particular purpose. Passcape Software disclaims all other warranties with respect to the SOFTWARE, either express or implied. Some

jurisdictions do not allow the exclusion of implied warranties or limitations on how 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 subsequential 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

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.

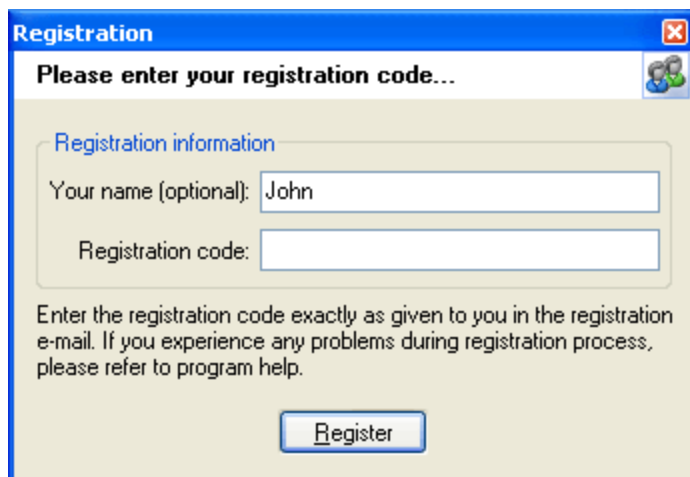
On payment approval (for online orders, usually within a few minutes), we'll send you the registration code which will remove all limitations of the unregistered version. Your registration will be valid for all future versions of **PIEPR**.

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 lines and click the **Register** button.

A screenshot of a Windows-style registration dialog box titled "Registration". The dialog has a blue title bar with a close button. Below the title bar, it says "Please enter your registration code...". There is a "Registration information" section with two text input fields: "Your name (optional):" containing the text "John" and "Registration code:" which is empty. Below these fields, there is a paragraph of text: "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." At the bottom of the dialog is a button labeled "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 **Passcape Internet Explorer Password Recovery** shows passwords that are not longer than 3 characters 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 **Piepr.log** files located in the **Passcape Internet Explorer Password Recovery** 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.

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>.