

Elcomsoft Phone Breaker Manual

© 2010-2015 ElcomSoft Co.Ltd.



Table of Contents

Part I Introduction	4
Part II Program information	6
1 System requirements.....	6
2 Program interface.....	7
3 EPB settings.....	8
4 [Windows] Hardware acceleration.....	13
5 Updating EPB.....	14
Part III Working with Apple devices	15
1 Useful links.....	15
2 Browsing iTunes and iCloud backups.....	15
3 Keychain explorer.....	17
4 Working with iTunes backup.....	22
About iTunes backups	22
Working with non-encrypted backup	23
Working with encrypted iTunes backup	26
Decryption details report	29
5 Working with iCloud data.....	30
Working with iCloud backups	30
About iCloud backups.....	30
Downloading iCloud backup.....	31
Downloading specific data types.....	34
Exporting backup list.....	38
Possible problems with downloading data from iCloud.....	38
iCloud backup structure (iOS 8.0 and lower).....	39
Supported models.....	40
Working with files in iCloud	46
Downloading files from iCloud.....	46
Exporting iCloud files list.....	49
6 Extracting authentication token for iCloud.....	50
About Authentication token	50
Extracting token on Windows OS	51
Extracting token on live Windows OS.....	51
Extracting token on non-live Windows OS.....	53
Extracting token on OS X	56
Extracting token on live OS X.....	56
Extracting token on non-live OS X.....	58
Part IV Working with BlackBerry data	60
1 Working with BlackBerry Backups.....	60
About BlackBerry backups	60

About BlackBerry Password Keeper and Wallet	60
Decrypt BlackBerry backup	61
Decrypt BlackBerry Link backup	63
Decrypt BlackBerry 10 Password Keeper	66
2 Working with SD card.....	67
About BlackBerry device password	67
Decrypt BlackBerry SD card	68
SD Card Decryption report	71
Part V Working with Windows Phone data	73
1 About Windows Phone data	73
2 Downloading Windows Phone data.....	73
Part VI [Windows] Working with 1Password containers	76
Part VII [Windows] Recovering passwords	77
1 Recovering passwords to storages.....	77
2 Password recovery attacks.....	81
3 Dictionary attack options.....	82
4 Brute-Force attack options.....	87
5 Templates.....	89
Saving templates	89
Viewing templates	90
Loading templates	91
Using templates for attacks	92
Part VIII Technical support	94
1 Contacting us.....	94
2 Where to get the latest version.....	94
Part IX License and registration	95
1 Copyright and license.....	95
2 Registration.....	102
3 EPB Editions.....	104
4 Legal notices.....	106
Part X Troubleshooting	109

1 Introduction

Elcomsoft Phone Breaker (EPB) enables forensic access to iTunes, iCloud and BlackBerry backups, and to backed up data from Windows Phone devices. Featuring the company's patent-pending GPU acceleration technology, Elcomsoft Phone Breaker is the first and only iPhone/iPad/iPod and BlackBerry password recovery tool on the market. The program recovers the original plain-text password that protects encrypted backups containing address books, call logs, SMS archives, calendars, camera snapshots, voice mail and email account settings, applications, Web browsing history and cache.

EPB allows you to:

- Decrypt backups to iPhone (up to iPhone 6S), iPad (all generations), iPad Mini and iPod Touch devices assuming that the password is known.
- Download and decrypt iPhone backups from iCloud (assuming that Apple ID and password are known, or using the iCloud Authentication token), including passing two-step verification for Apple ID.
- Download files synchronized with iCloud including passing two-step verification for Apple ID.
- Decrypt keychains (saved passwords to mail accounts, web sites, and 3rd party applications) from password-protected iTunes backups, from iCloud backups and non-encrypted iTunes backups. For the latter two the Security Key is required.
- Decrypt BlackBerry backups and BlackBerry SD Cards (assuming that the passwords are known).
- Decrypt backups for BlackBerry 10 devices (up to BBOS 10.3.1.1581) created with BlackBerry Link (the BlackBerry ID password must be known).
- Download sensitive data, such as SMS, contacts, notes from Windows Phone cloud backup, assuming that credentials to Microsoft account are known.

In addition to that, the Windows version of EPB allows you to:

- Access password-protected backups to iPhone (up to iPhone 6S), iPad (all generations), iPad Mini and iPod Touch devices.
- Access password-protected BlackBerry backups, including passwords set by BlackBerry Password Keeper and Wallet applications.
- Recover BlackBerry device password.
- Recover master passwords protecting 1Password containers retrieved from Dropbox, iTunes, or iCloud backups.

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 subsequent 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.

2 Program information

2.1 System requirements

Elcomsoft Phone Breaker requires the following system parameters:

Windows

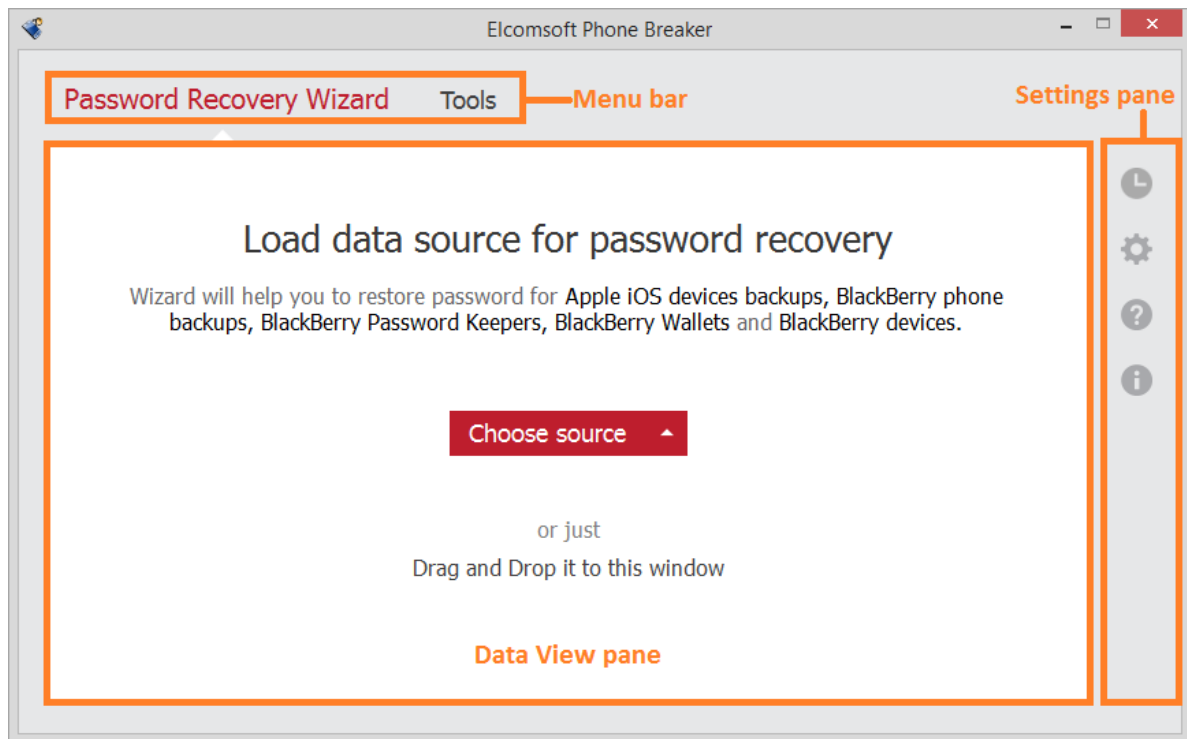
- Windows 10, Windows 8.1, Windows 8, Windows 7, Windows Vista, Windows XP; Windows Server 2012, Windows Server 2008, Windows Server 2003.
- Modern CPU with SSE2 instruction set support (AES-NI recommended).
- About 8 megabytes of free space on hard disk.
- One or more supported NVIDIA or AMD cards, or Tableau TACC1441 (recommended for [hardware acceleration](#)).
- iCloud panel (version 4 or higher) must be installed for downloading files from accounts that use iCloud Drive, and also to view the iOS 9.x.x backups in iCloud.

NOTE: To use GPU acceleration with NVIDIA or AMD card(s), you should have the latest drivers installed.

OS X

- OS X 10.7 - 10.11.
- About 15 megabytes of free space on hard disk
- Modern CPU with SSE2 instruction set support (AES-NI recommended)

2.2 Program interface



Elcomsoft Phone Breaker interface consists of the following elements:


- **Menu bar:** Provides access to main functionality of EPB. Menu bar consists of several tabs:
 - **Password Recovery Wizard:** Allows recovering passwords to iPhone and Blackberry backups, and 1Password containers.
NOTE: This option is available only for EPB running on Windows OS.
 - **Tools:** Allows decrypting backups for [iPhone](#) and [BlackBerry](#) devices. For Apple data, it also provides access to downloading data from [iCloud](#), exploring [Keychain](#), and extracting [authentication token](#). For [Windows Phone](#) data, it allows downloading SMS, Notes, and Contacts from Microsoft account. For BlackBerry devices, it also provides the ability to decrypt the [Password Keeper](#).
- **Data View pane:** Allows managing data in EPB, depending on which tab on the Menu bar is selected.
- **Settings pane:** Allows opening the following tabs:
 - **Journal:** Contains records of all actions performed with data in EPB.
 - **Settings:** Allows configuring Hardware, Network, iCloud, and Templates [settings](#) in EPB.
 - **Help:** Allows reading EPB help file, checking for program updates, sending the feedback to program developers, purchasing a program, or entering a registration code in case you have

already purchased a program online.

- o **About:** Allows viewing the EPB version number and checking if the program is registered or not.

2.3 EPB settings

Elcomsoft Phone Breaker has a number of various settings that allow you to customize working with EPB.

To change **EPB Settings**, select  in the **Settings** pane.

• General

Define the general options for working with EPB:

- **Replace system "Open File" dialog by customized if Apple iTunes or BlackBerry Desktop Software is installed:** When selected, the "Open File" window will be displayed in the same way as in Apple iTunes or Blackberry Desktop Software. This option will take effect only if Apple iTunes or Blackberry Desktop Software is installed on the current computer.
- **Clear log on startup:** Removes the records about EPB functioning from the log file after EPB is restarted. This way, only the records about the current session of work are stored in the EPB log file. The log file is stored in the following locations by default:
 - o **Windows:** *%AppData%\Elcomsoft\Elcomsoft Phone Password Breaker\EPB_<version and revision number>.log*
 - o **OS X:** *~/Users/<username>/Library/Application Support/Elcomsoft Phone Password Breaker/EPB_<version and revision number>.log*. Please note that this directory is hidden by default.

You can select the level of logging in the **Logging level** list. It defines the amount of information that is written to the log: the higher the level, the more detailed information is written to the log file, but at the same time the higher the load on the system at logging. By default, a medium level of logging is set.

You can select one of the following levels of logging:

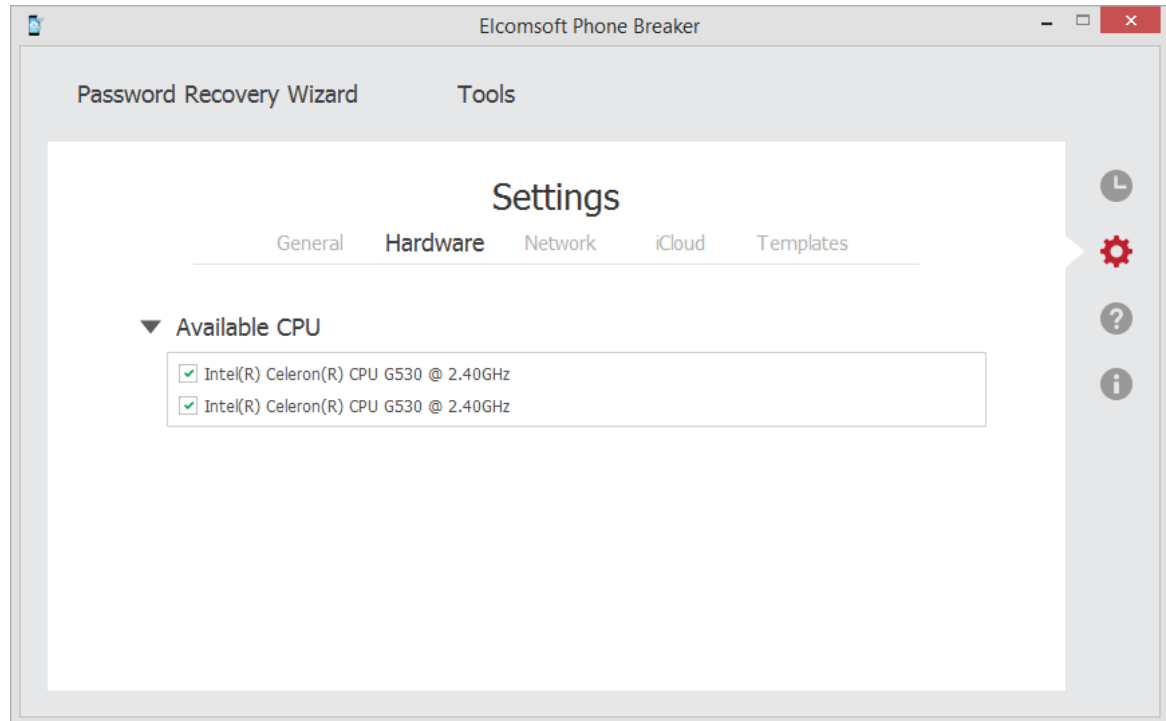
Level	Description
None	No logging is performed.
Fatal	The information about fatal errors only is written in the log.
Error	The information about general program errors is written in the log.
Warning	The information about the program malfunctioning at the warning level is logged.
Info	The program system messages at the information level are logged.
Debug	The level of logging that is necessary for debugging.
Trace	The detailed log about informational events.
Maximum level	All information about the program work is logged. This level is the most informative, so please set logging to this level when reproducing the problem with EPB application.

• Hardware [available in EPB for Windows only]

On the Hardware page, define the processor cores (CPU, GPU) that will be used for processing

information in EPB.

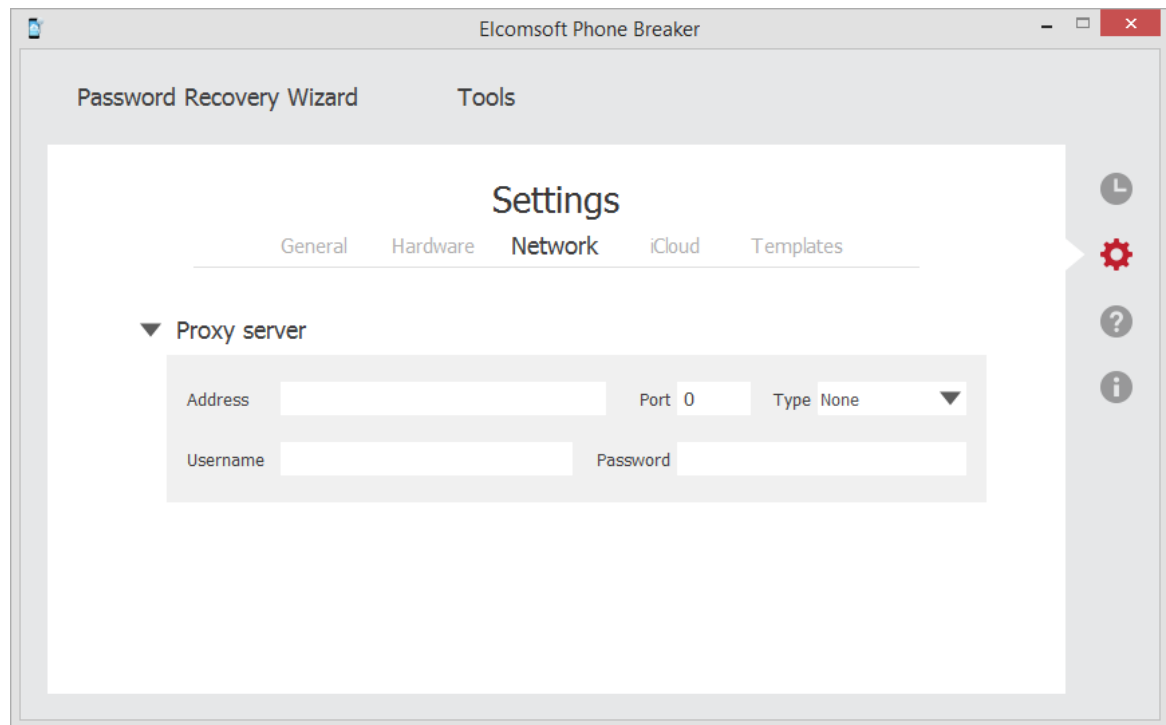
NOTE: Changing the number of CPUs and GPUs is applied at the password recovery attack start. If you change the CPU and GPU settings, the changes will not affect already running attacks.



- **Network**

Define the Proxy server that will be used when downloading [iCloud backups](#) and data from Windows Phone backups. Network connection is also required when decrypting backups for [BlackBerry 10](#) devices (created with BlackBerry Link).

NOTE: Only transparent Proxy servers are supported. Working with data over the network is not available via Proxies with changed certificates.



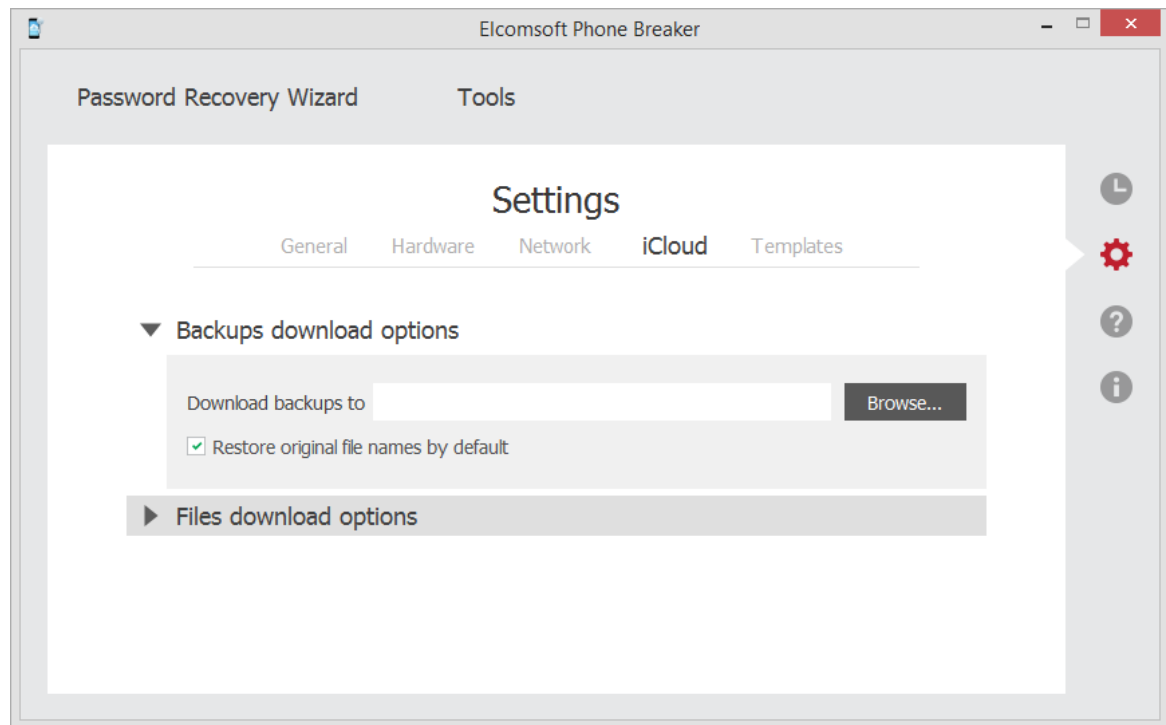
- **iCloud**

Define the default options for downloading backups and files from iCloud.

The following backup downloading options are available:

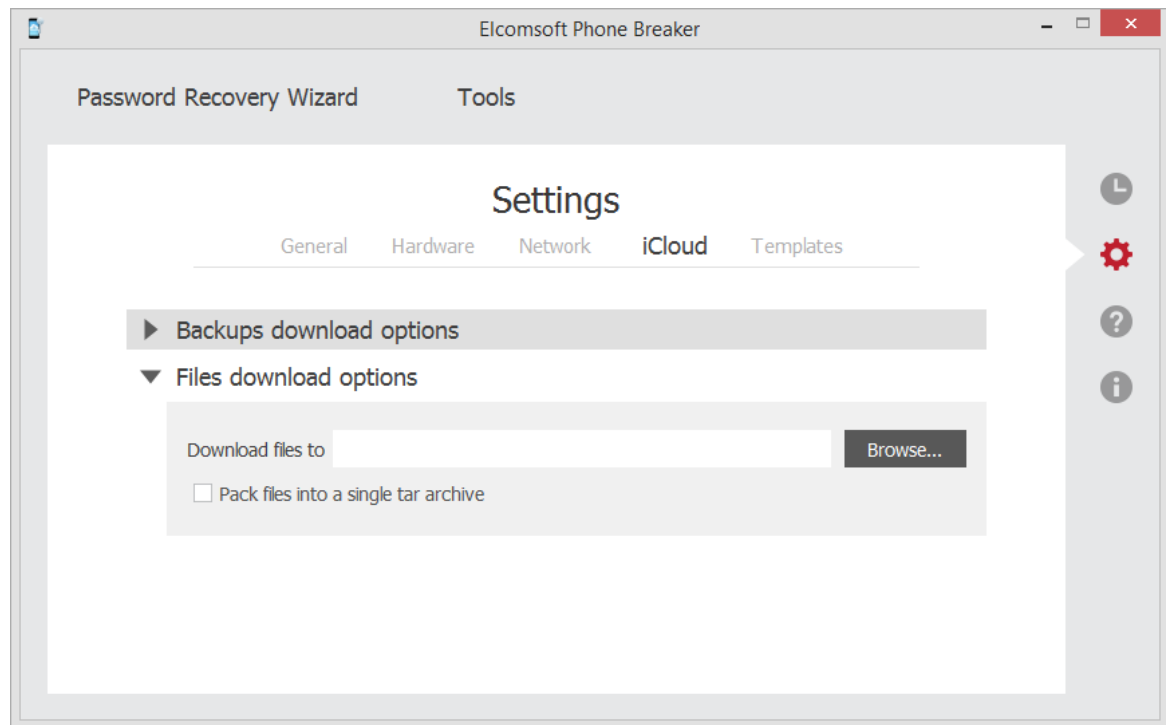
- **Download backups to:** Select the default folder where the backup will be saved.
- **Restore original file names by default:** Allows viewing the folder and file names in the restored backup as they were on the device. If you uncheck this option, the files will still be available after decryption, however, their names will be crypted.

NOTE: You can restore the original file names in the backups any time after decrypting (for iTunes backup) or downloading (for iCloud backup) in Tools -> Apple -> Decrypt backup and selecting the Restore original file names option.



The following files downloading options are available:

- **Download files to:** Select the default folder where the files will be saved.
- **Pack files into a single tar archive:** Allows packing the downloaded files into an archive.





- **Templates [available in EPB for Windows only]**

The **Templates** tab allows viewing and managing [templates](#) for password recovery. Template is a saved combination of settings used for recovering the password in EPB.

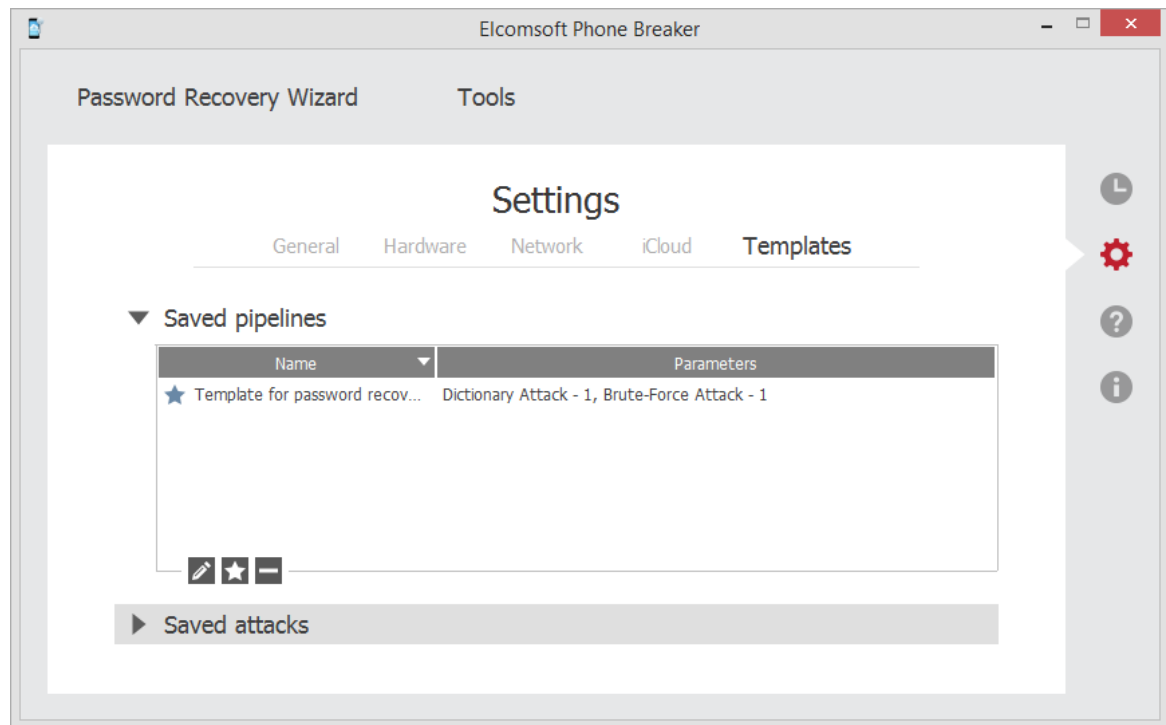
The process of recovering the password is made up of attacks. A combination of attacks is called a pipeline. See [Password recovery attacks](#) section for more details.

The information about templates of pipelines can be viewed in the **Saved pipelines** section. The information about individual attacks is displayed in the **Saved attacks** section.

To edit the template name, select a template and click the **Edit**  button.

To set the template as default, click the  button. Default template will be displayed first every time the **Password recovery** option is used.

To delete a template, select a template, and click the **Delete**  button.



2.4 [Windows] Hardware acceleration

For recovery of passwords for Apple devices (iPhone, iPod and iPad), BlackBerry backups created with new versions of BlackBerry Desktop Software (6.0 for Windows or 2.0 for OS X), and 1Password backups, **EPB** provides hardware acceleration (i.e., runs much faster) on most modern [NVIDIA](#) and [AMD](#) video cards, and on [Tableau](#) TACC1441 hardware accelerators.

Hardware acceleration is available only when running EPB on Windows OS.

NOTE: Only NVIDIA cards with Compute Capability from 1.3 to 5.2 are supported. To find out the Compute Capability of your card, please see <https://developer.nvidia.com/cuda-gpus>

You can use the following NVIDIA GeForce cards:

Desktop products:

- GeForce GTX 400-, 500-, 600-, 700-, 900-, TITAN, TITAN Black, TITAN Z TITAN X
- GeForce GT 400-, 500-, 600-, 700-

Notebook products:

- GeForce GTX 400-, 500-, 600-, 700-, 800- 900-
- GeForce GT 400-, 500-, 600-, 700-
- GeForce 400-, 700- 800-

Quadro and Tesla cards are supported as well, please check <https://developer.nvidia.com/cuda-gpus> to see if your card is supported.

Full list of supported devices can be found [here](#), the list of older products and their GPUs can be found [here](#). If you have multiple cards, you need to disable [SLI](#) (either in driver or by physically disconnecting the cards).

EPB also supports [ATI Stream\(tm\) Technology](#), in particular [Radeon R9 Series](#), [Radeon R7 Series](#), [Radeon 7000 Series](#), [Radeon 6000 Series](#) and [Radeon 5000 Series](#).

Alternatively, you can use [Tableau TACC1441](#) accelerators.

Whether you have NVIDIA or AMD card to use with **EPB**, you should also have the latest drivers installed (supported operating systems: Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008, Windows 7 and 8; 32-bit and 64-bit).

The maximum supported number of GPU devices is 8 (4x PCI-Express slots on motherboard, each with double-GPU device such as [NVIDIA GeForce GTX 690](#) or [AMD Radeon HD 7990](#)).

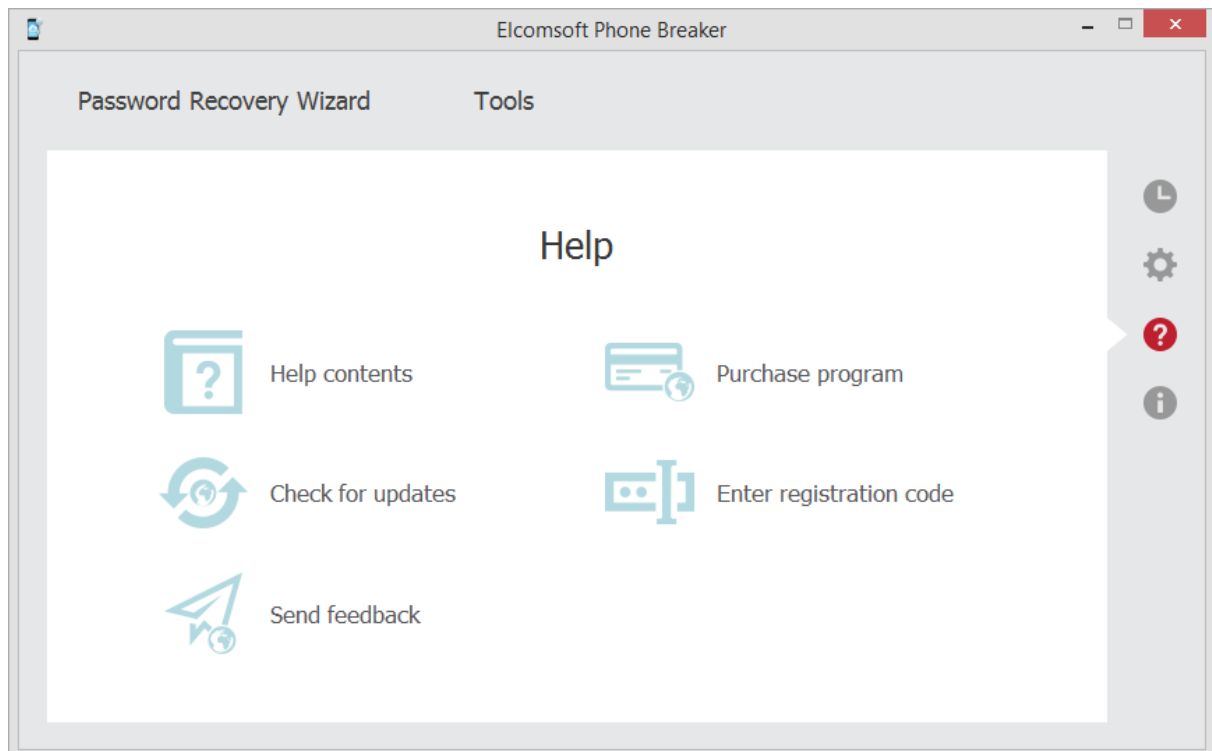
NOTE: CUDA hardware acceleration isn't available when accessing EPB via remote desktop (RDP connection).

2.5 Updating EPB

You can check for available updates of Elcomsoft Phone Breaker and install them yourself.

To update the program, do the following:

1. Click the **Help** icon in the **Settings** pane, to open the **Help** tab.
2. On the **Help** tab, select the **Check for updates** option.
3. If there is a new version available, you will be offered to download it. If there are no new versions available, you will get the corresponding message.



3 Working with Apple devices

3.1 Useful links

You may find the following links useful when working with Apple devices:

iCloud: Back up your iOS device to iCloud

<http://support.apple.com/kb/PH12520>

iCloud: Restore your iOS device from iCloud

<https://support.apple.com/kb/ph12521>

iCloud: Troubleshooting restoring an iCloud backup

<http://support.apple.com/kb/TS4036>

iCloud: iCloud storage and backup overview

<http://support.apple.com/kb/PH12519>

iOS: Unable to restore from backup of a newer device

<http://support.apple.com/kb/TS3682>

iOS: Back up and restore your iOS device with iCloud or iTunes

<http://support.apple.com/kb/HT1766>

iTunes: About iOS backups

<http://support.apple.com/kb/HT4946>

iTunes: About encrypted backups in iTunes

<https://support.apple.com/en-us/HT205220>

Choosing an iOS backup method (Should I use iTunes or iCloud to back up my iOS device?)

<http://support.apple.com/kb/HT5262>

Recovering iCloud contacts, calendars, and bookmarks from an iTunes backup of an iOS device

<http://support.apple.com/kb/TS4108>

iOS: If you can't back up or restore from a backup in iTunes

<http://support.apple.com/kb/TS2529>

iCloud: iCloud security and privacy overview

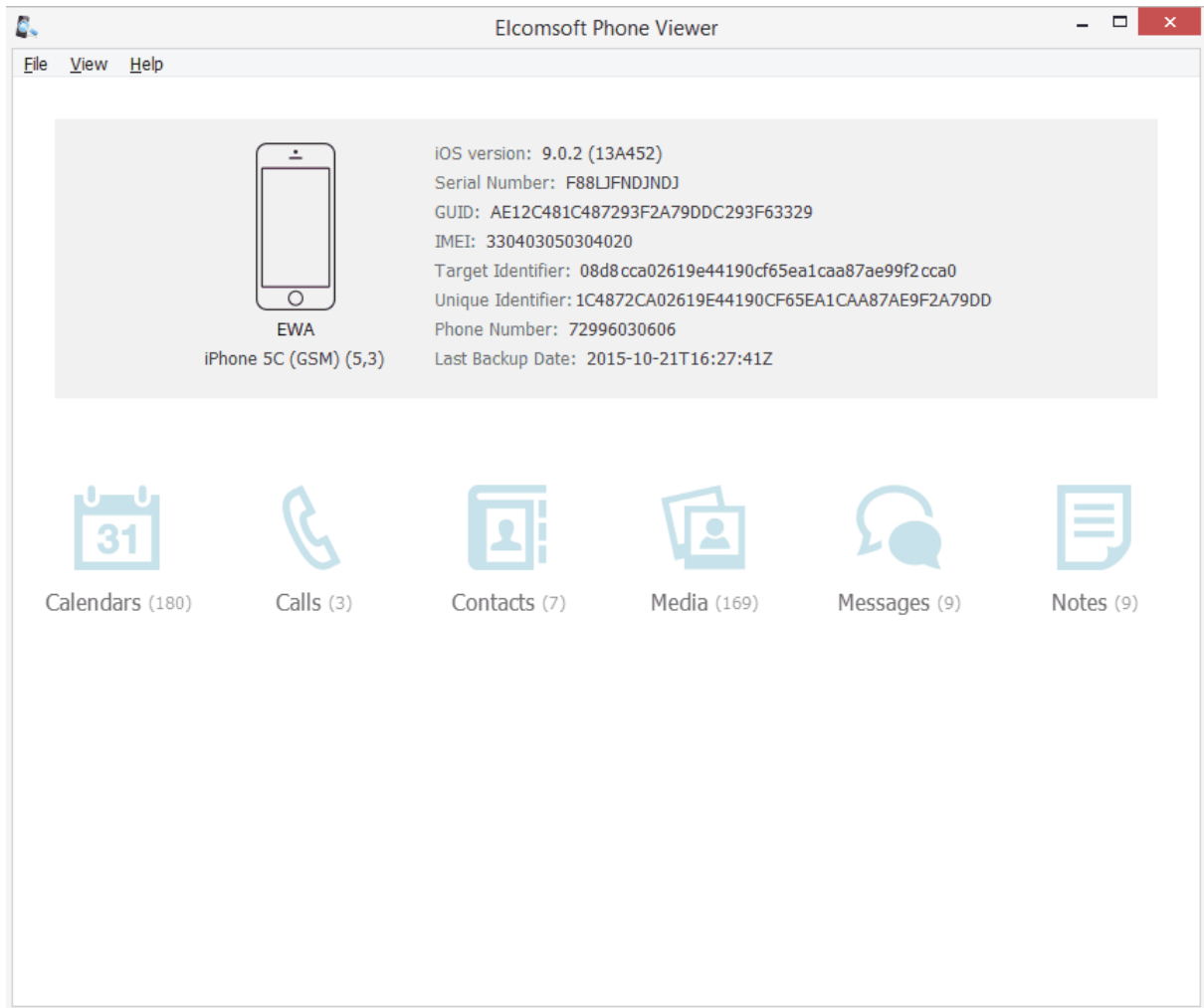
<http://support.apple.com/kb/ht4865>

3.2 Browsing iTunes and iCloud backups

After you have [downloaded](#) an iTunes or iCloud backup or [decrypted](#) a local one using **EPB**, you can explore its content with [Elcomsoft Phone Viewer](#) - a tool for viewing the content of backups produced by iOS and other mobile operating systems. This is the first and only viewer that works both with iOS device backups in original iTunes format and with restored file names. Elcomsoft Phone Viewer provides a convenient way to view the content of the backup, including:

- Information about the device, such as:

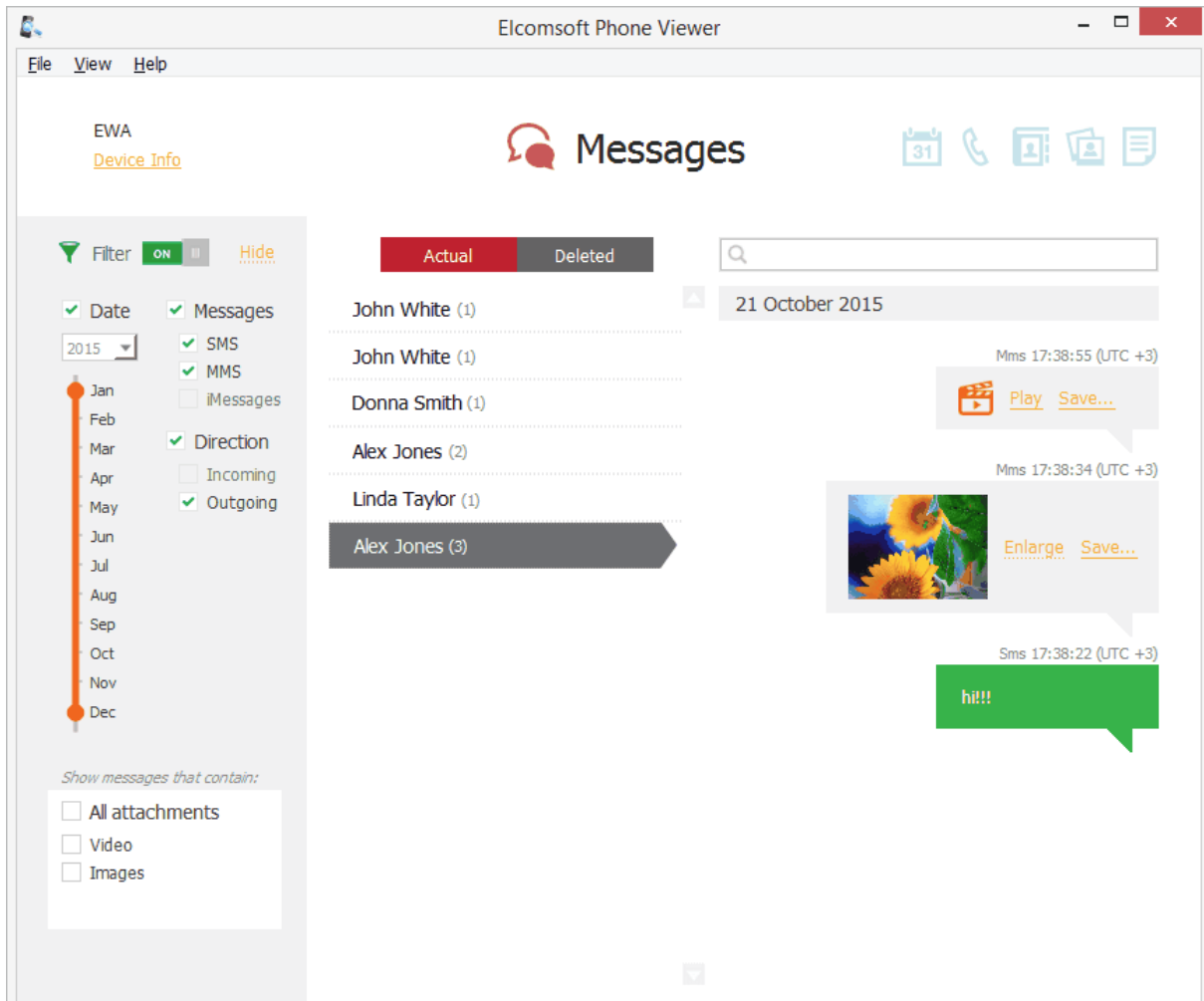
- Model name
- Serial number
- Phone number
- Data stored in the backup, such as:
 - Contacts
 - Messages
 - Call logs
 - Notes
 - Multimedia files
 - Calendar data
- Deleted SMS and iMessages stored in iOS backups



Other features that make Elcomsoft Phone Viewer a highly convenient viewing tool include:

- Support of media files export to a native format
- Displaying location data automatically mapped via Google Maps
- Automatic categorization by the source (Camera Roll, Message Attachments, and Other media)

Besides, Elcomsoft Phone Viewer allows flexible data filtering, providing different sets of search parameters for different types of information. You can search and filter out data by date range, data type, status, and more.



In addition to that, Elcomsoft Phone Viewer allows viewing backups produced by Blackberry 10 and Windows Phone 8/8.1 devices, which makes it an ideal companion for Elcomsoft Phone Breaker.

3.3 Keychain explorer

Some of the most valuable information stored in iPhone, iPod Touch and iPad backups is keychains. This includes email account passwords, Wi-Fi passwords, and passwords you enter into websites and some other applications.

EPB is able to decrypt keychain data from password-protected backups (iOS4 or later), if backup password is known (or [recovered](#) using EPB for Windows). For non-encrypted backups and iCloud backups, you must know the Security Key to the Apple device.

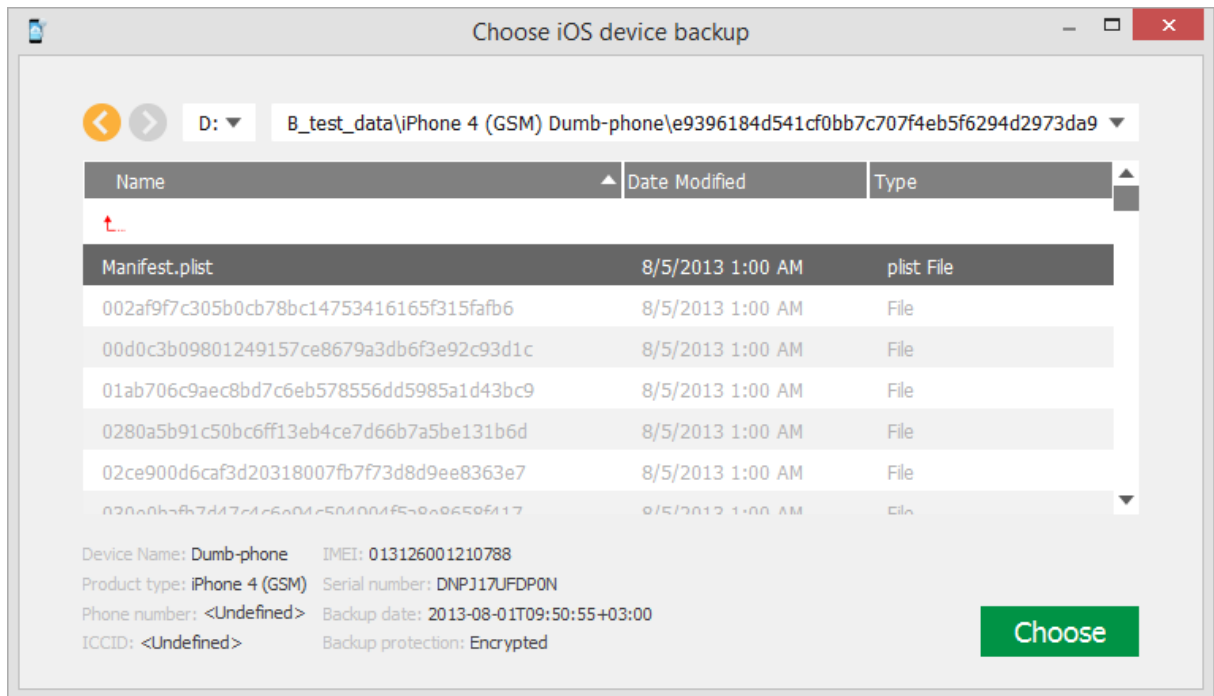
NOTE: Only the backups decrypted with EPB 3.0 or higher are supported. Decrypted backups must have the same file names as in iTunes backup, so don't use the Restore original file names option when decrypting the backup.

You will need the following password/key to decrypt the keychain:

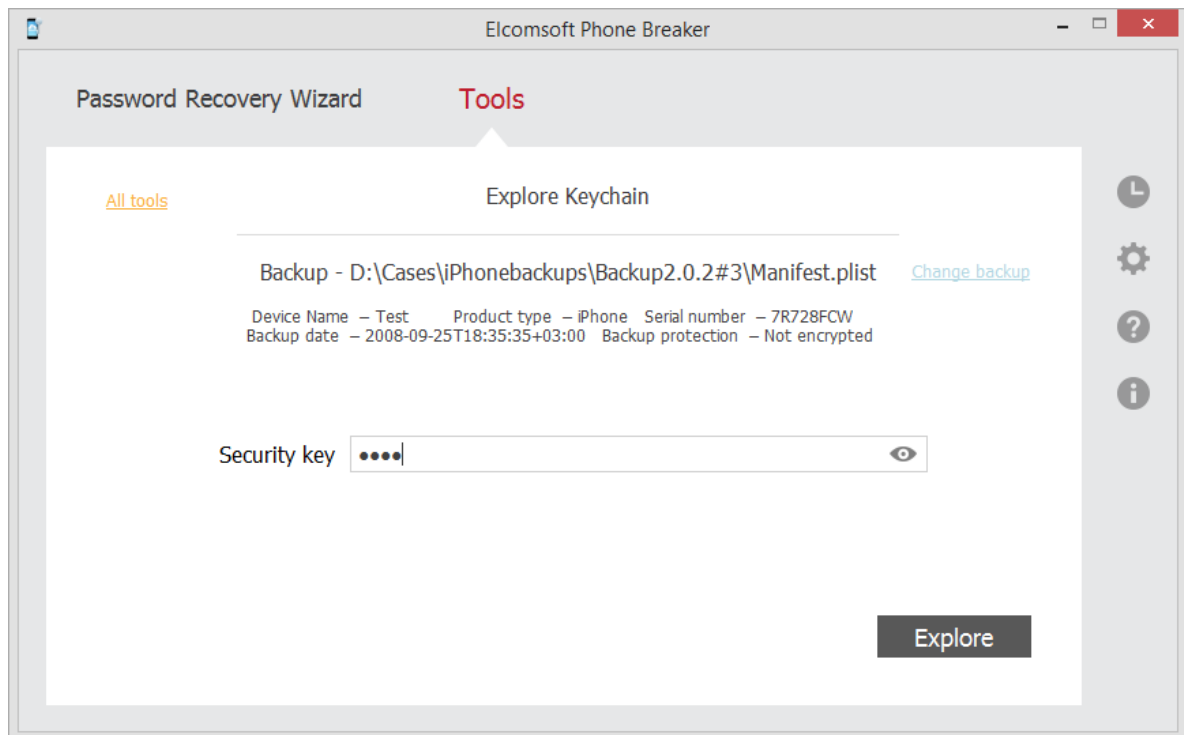
Backup Type	Required
iCloud backup	Security Key
iTunes (not encrypted)	Security Key
iTunes (decrypted by means of EPB)	Backup password
iTunes (encrypted)	Backup password


To decrypt the keychain, do the following:

1. In the **Tools** menu, select the **Apple** tab, and click **Explore keychain**.
2. Select the *Manifest.plist* file either by drag-and-dropping it to the **Explore keychain** page, or click **Choose backup**.
3. In the opened window navigate to the backup file by entering the file path in the path box. Select the *Manifest.plist* file and click **Choose**.
You will see the properties of the selected backup below the grid.
4. Select the file and click **Choose**.

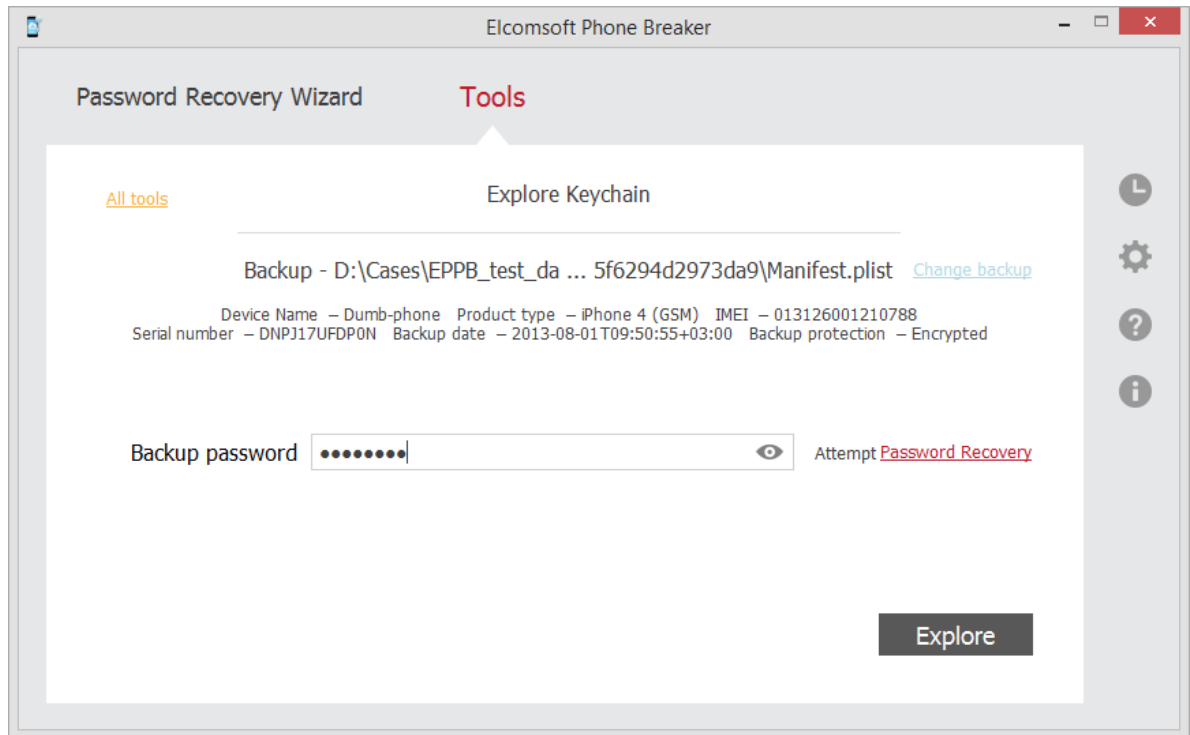


5. Depending on whether the backup is encrypted or not, the following options are available:
 - **For non-encrypted backups and iCloud backups**, enter the Security key:



- **For encrypted backups**, enter the password to the backup if you have already recovered it. Toggle the View  button to display the password as characters or in asterisks (*).

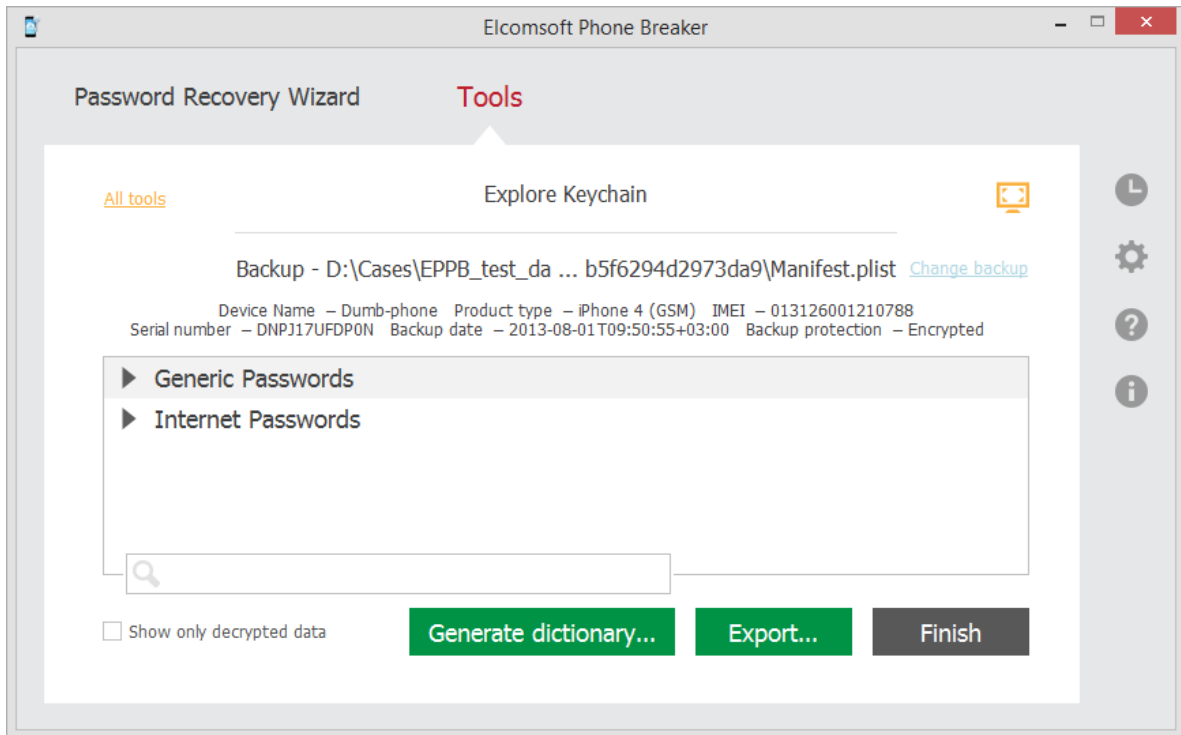
If you are using EPB on Windows OS, click **Restore password** to [recover the password](#) to the backup.



6. Click **Explore** to view the Keychain.

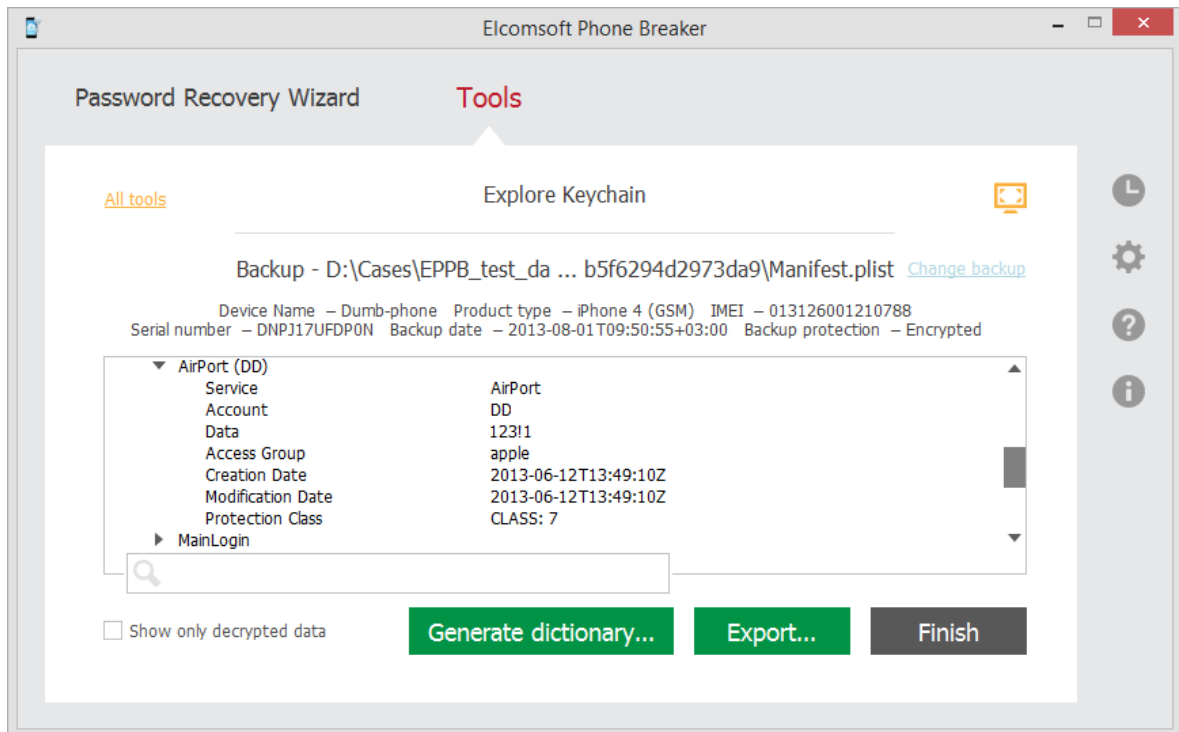
7. The passwords are stored in two major categories in Keychain Explorer:

- **Generic passwords:** passwords to iPhone applications, tokens and passwords to Wi-Fi points.
- **Internet passwords:** passwords entered in Safari browser.



You can hide the not-decrypted data by selecting **Show only decrypted data**. This allows to leave only useful decrypted information while exploring encrypted backups.

You can view the passwords to wireless access points (stored under **Generic Passwords / AirPort**). VPN passwords are also there (with "PPP Password" description).



You can also view the passwords to Mail (POP3, SMTP, IMAP) and Web sites.

To expand the window and view the information full-screen, click **Expand**  .

You can search for the keywords to be found in Keychain data by entering them in the search field and pressing **Enter**.

Click **Generate dictionary** to create a text file that can later be used as a dictionary for [password recovery](#).

Click **Export** to save all keychain data to an XML file.

3.4 Working with iTunes backup

3.4.1 About iTunes backups

[iTunes](#) can create backups of settings and other information on iPhone, iPad and iPod Touch, such as:

- Photos (photos, screenshots, images saved, and videos taken) and Saved Photos (in devices without a camera).
- Contacts and Contact Favorites. (You should regularly sync your contacts to a computer or cloud service, such as iCloud.)
- Health (only if you have an encrypted backup).
- Calendar accounts, events, and subscribed calendars.
- Safari bookmarks, cookies, history, offline data, and currently open pages.
- Autofill for webpages.
- Offline web app cache/database.
- Notes.
- Mail accounts. (Mail messages aren't backed up.)
- Microsoft Exchange account configurations.
- Call history.
- Messages (iMessage and carrier SMS or MMS pictures and videos).
- Voicemail token. (This isn't the voicemail password, but it is used for validation when connecting. This is only restored to a phone with the same phone number on the SIM card.)
- Voice memos.
- Network settings (saved Wi-Fi hotspots, VPN settings, and network preferences).
- Keychain. (Includes email account passwords, Wi-Fi passwords, and passwords you enter into websites and some apps.)
- App Store app data. (Minus the app itself, its tmp, and Caches folder.)
- App settings, preferences, and data, including documents. (PDFs downloaded directly to iBooks on an iOS device are not included in the backup).
- In-app purchases.
- Game Center account.
- Wallpapers.
- Location service preferences for apps and websites you've allowed to use your location.
- Home screen arrangement.
- Installed profiles.
- Map bookmarks, recent searches, and the current location displayed in Maps.
- Nike + iPod saved workouts and settings.
- Paired Bluetooth devices (which you can only use if restored to the same phone that did the backup).
- Keyboard shortcuts and saved suggestion corrections.
- Trusted hosts that have certificates that can't be verified.
- Web clips.

For more information, see <https://support.apple.com/en-gb/HT204269>.

You can use a backup to restore this information back to your device after a software restore or update, or to transfer information to a different device. For more information about creating a backup and restoring from it, please read:

<http://support.apple.com/kb/HT1414>

<http://support.apple.com/kb/HT1766>

By default, backups are stored in the following folders:

- **OS X:** ~/Library/Application Support/MobileSync/Backup/
- **Windows XP:** \Documents and Settings\(\username)\Application Data\Apple Computer\MobileSync\Backup\
- **Windows Vista, Windows 7, and Windows 8, 8.1, Windows 10:** \Users\(\username)\AppData\Roaming\Apple Computer\MobileSync\Backup\

If you are running **EPB** on the computer where iTunes is installed, it will allow you to browse through all backups stored there.

If you want to encrypt the information stored on your computer when iTunes makes a backup, select **Encrypt iPhone backup** in the **iTunes Summary** screen. Encrypted backups are indicated by a padlock icon, and a password is required to restore the information to iPhone. If you forget the password you can continue to do backups and use the device, however you will not be able to restore the encrypted backup to any device without the password. You do not need to enter the password for your backup each time you back up or sync.

Every backup contains many files, but the only one needed for password recovery is **Manifest.plist**. However, if you want to recover passwords and other data saved in Keychain, you need to have the complete device backup.

3.4.2 Working with non-encrypted backup

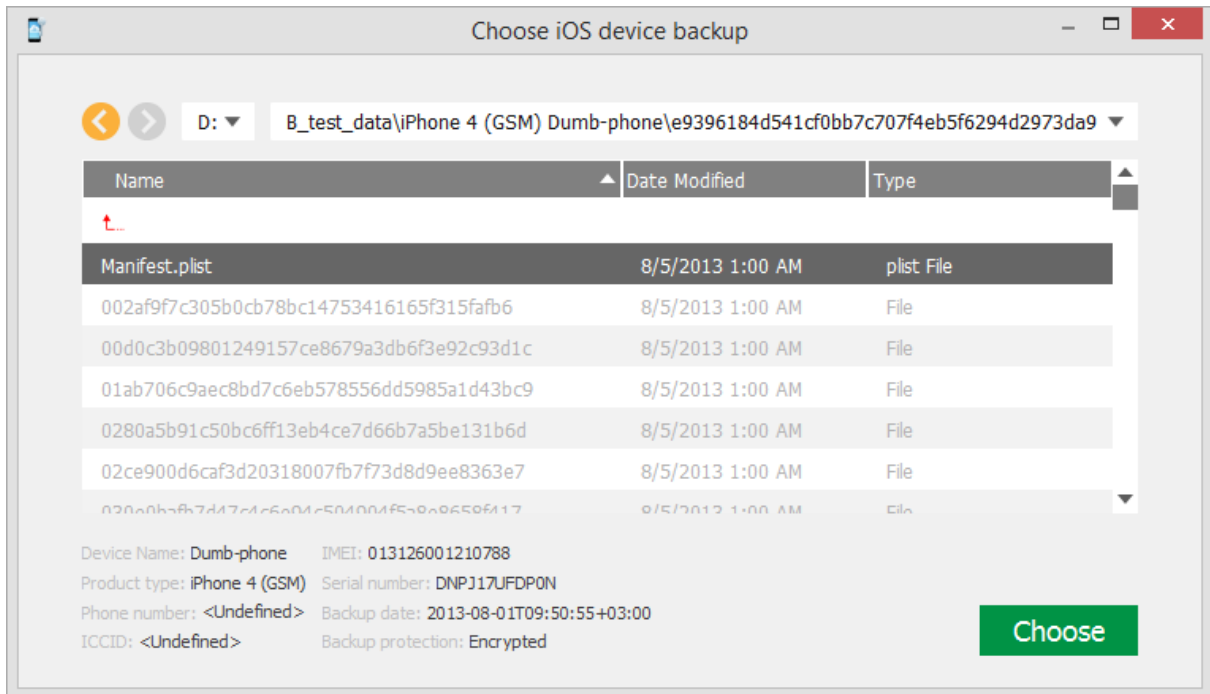
When you work with iTunes backups, the encrypted backups need to be [decrypted](#) in order to work with them. However, non-encrypted backups can be difficult to work with as well, because all file names are displayed as an SHA-1 hash of file name, together with its path and domain.

EPB allows you to restore original file names of non-encrypted backups so that file names in backup are displayed as in OS X. You can [explore the backup content](#) with either restored or not restored file names in Elcomsoft Phone Viewer.

To restore original file names of a non-encrypted backup, do the following:

1. In the **Tools** menu, select the **Apple** tab.
2. Select **Decrypt backup**.
3. Select the *Manifest.plist* file either by drag-and-dropping it to the **Decrypt backup** window, or click **Choose backup**.
4. In the opened window navigate to the backup file by entering the file path in the path box. Select the *Manifest.plist* file and click **Choose**.

The properties of the selected file are displayed below the grid.

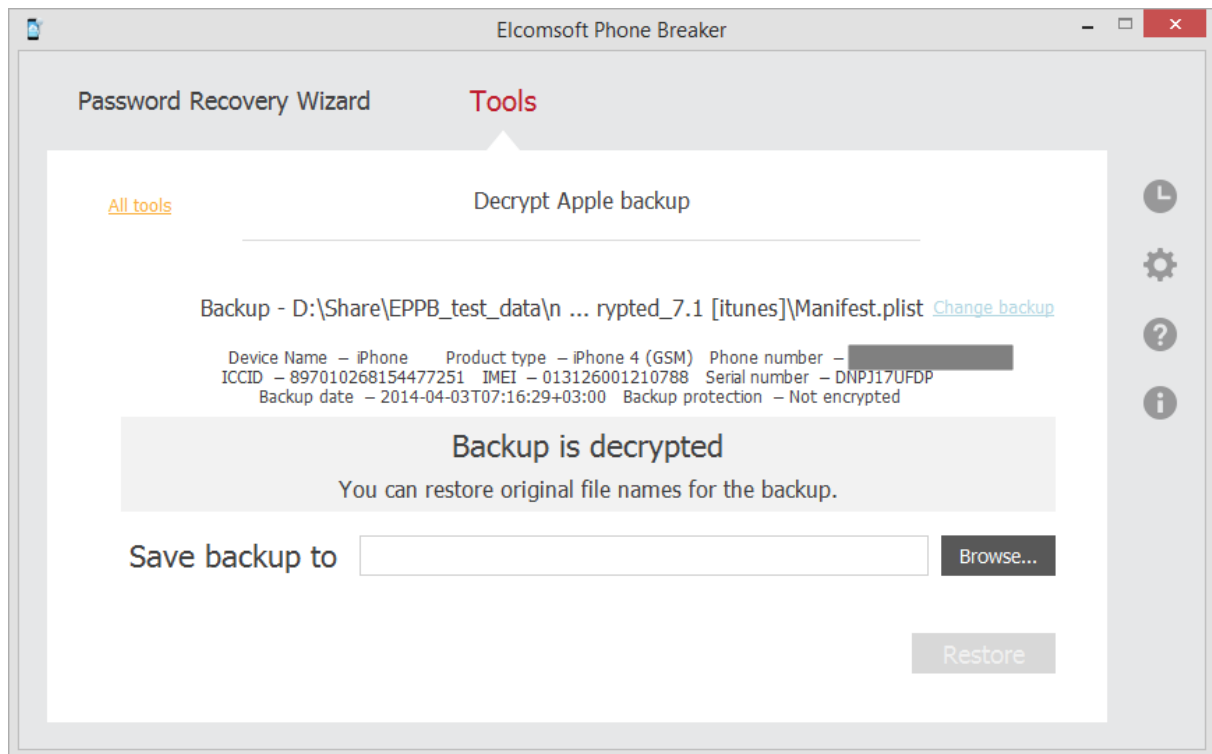


5. When the backup is loaded, you can view the following information about backup:

- **Serial number**
- **Backup date**
- **Product type**

Depending on the backup there may be other information available (i.e., IMEI, ICCID, phone number, etc.)

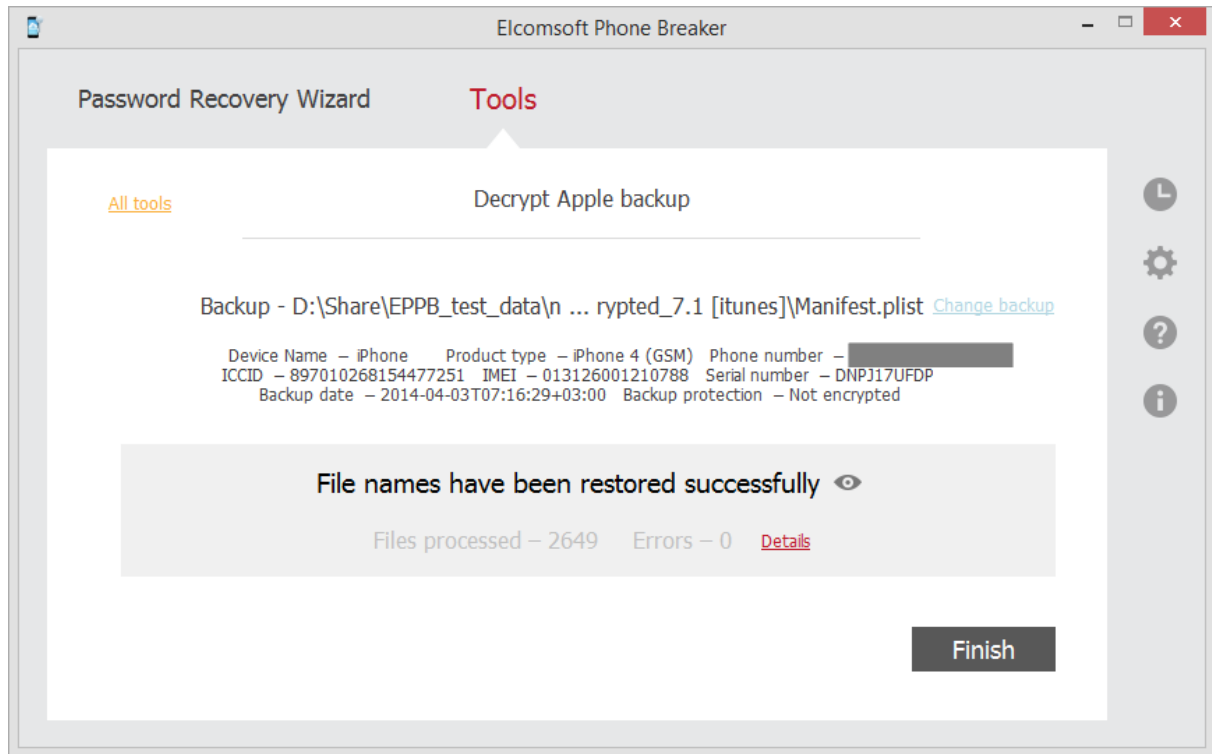
You can select a different backup by clicking **Change backup** next to the backup name.




6. Define the location for saving the backup and click **Restore**. The file names in the restored backup will be displayed as in OS X.

NOTE: The destination location must be empty.

7. The decryption process starts. You can view the number of processed files and the number of errors received during decryption.



8. When decryption is finished, you can click  to view the processed backup on the local computer.
9. To view a detailed [report](#) about decrypted files and errors that occurred during decryption, click **Details**.
10. Click **Finish** to close the **Decrypt Apple backup** window.

3.4.3 Working with encrypted iTunes backup

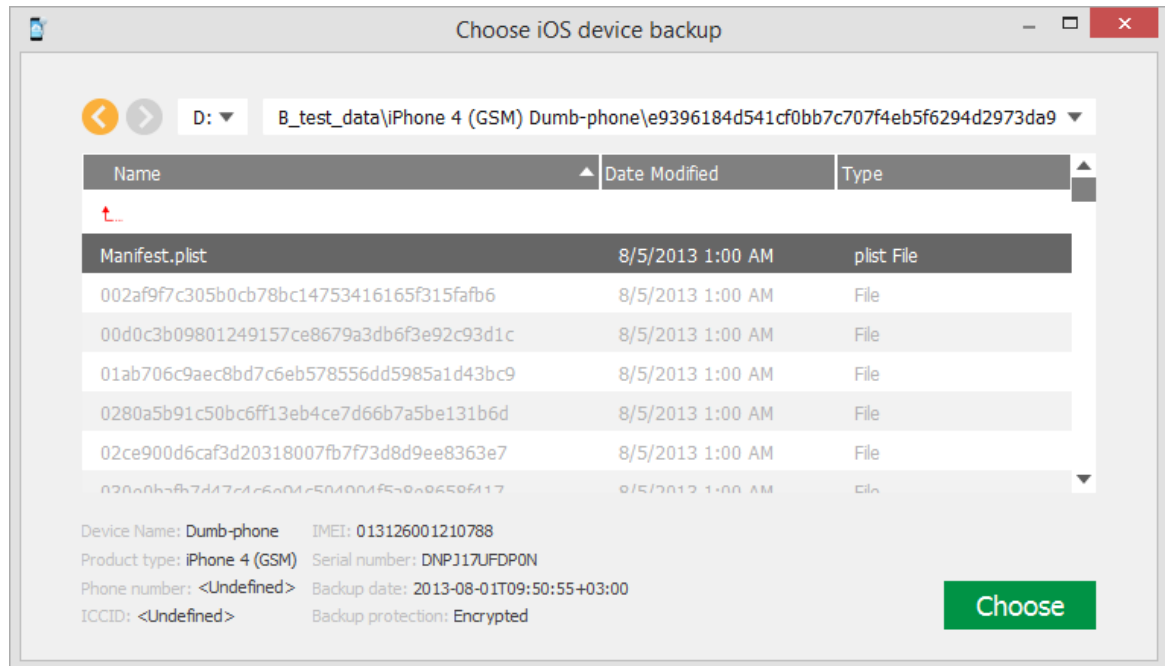
EPB allows you to decrypt an encrypted backup that is stored on a computer where EPB is installed. After decryption is completed successfully, you can [explore the backup content](#) in Elcomsoft Phone Viewer.

Decryption of the backup is available only if you know the password to a backup, so you may first need to [recover the password](#) using EPB for Windows.

To decrypt a backup stored on a currently investigated computer, do the following:

1. In the **Tools** menu, select the **Apple** tab.
2. Select **Decrypt backup**.
3. Select the *Manifest.plist* file by either drag-and-dropping it to the **Decrypt backup** window, or click **Choose backup**.
4. In the opened window navigate to the backup file by entering the file path in the path box. Select the *Manifest.plist* file and click **Choose**.

The properties of the selected file are displayed below the grid.

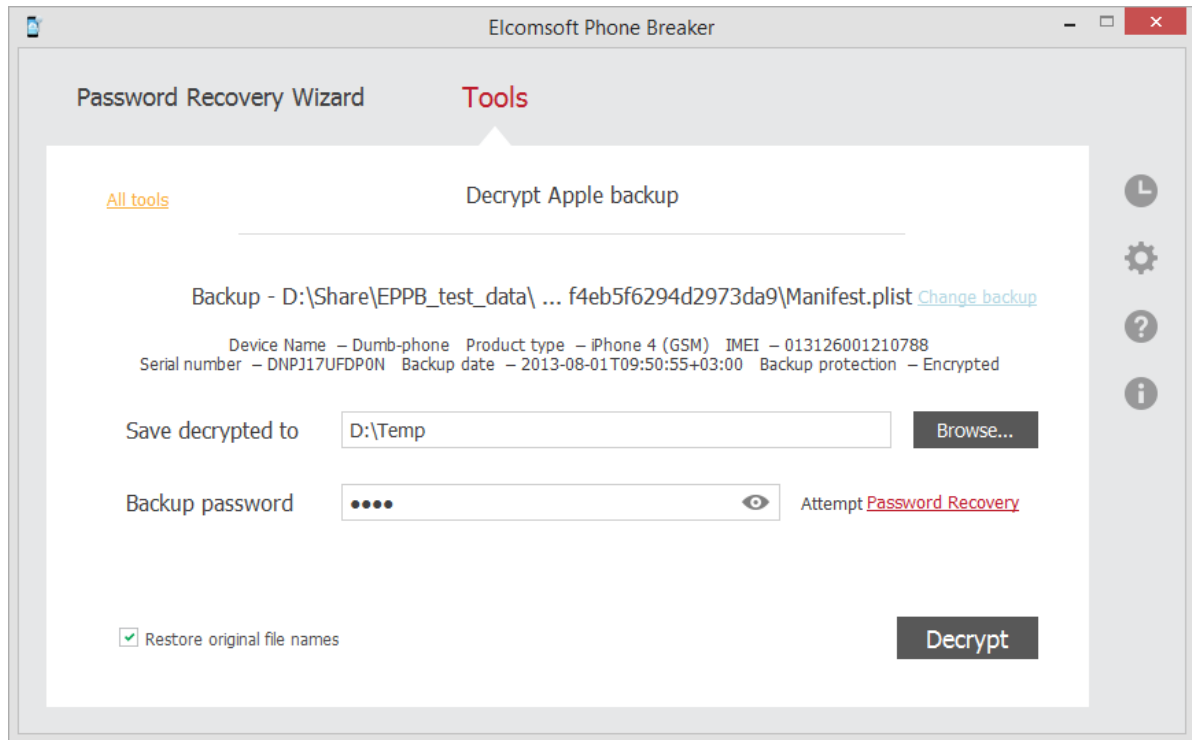


5. When the backup is loaded, you can view the following information about backup:


- **Serial number**
- **Backup date**
- **Product type**

Depending on the backup there may be other information available (i.e., IMEI, ICCID, phone number, etc.)

6. You can select a different backup by clicking **Change backup** next to the backup name.



7. Define the options for backup decryption.


- **Save decrypted to:** Select location for saving decrypted backup. Please note that the destination location must be empty.
- **Backup password:** Enter the password for the backup. Toggle the View  button to display the password as characters or in asterisks (*).

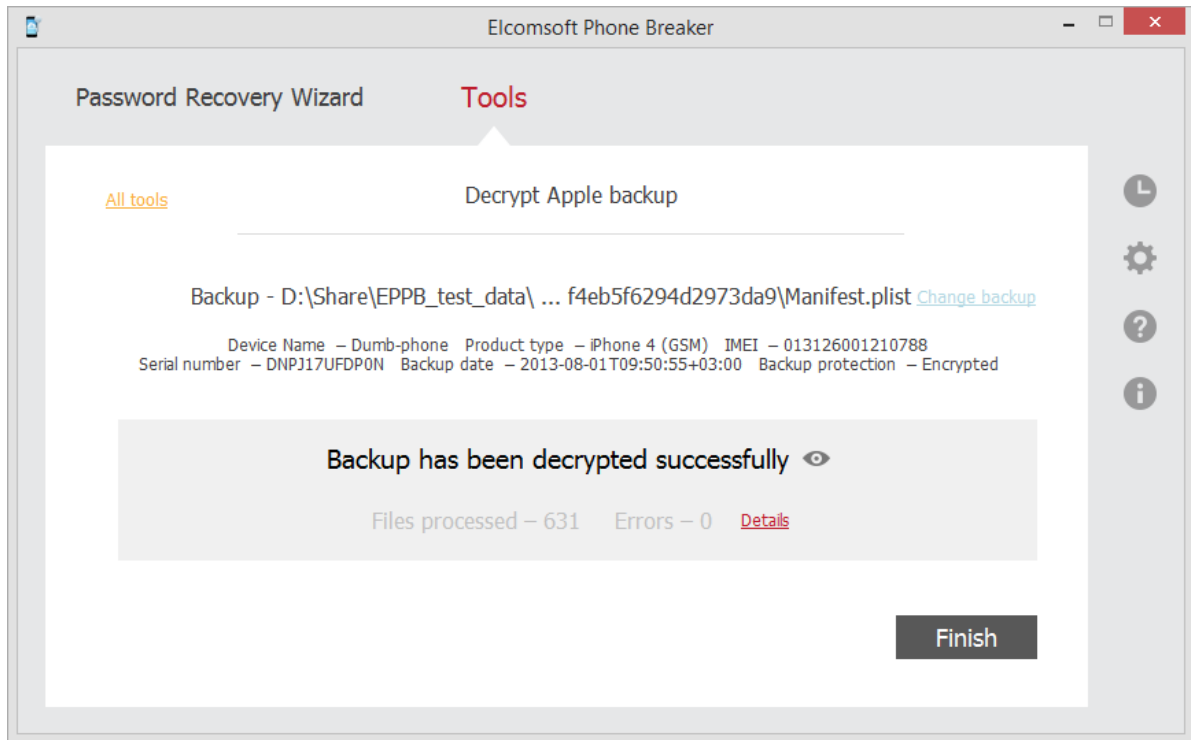
If you are using EPB on Windows OS, click **Restore password** to [recover the password](#) to the backup.

- **Restore original file names:** Allows viewing the folder and file names in the restored backup as they were on the device. If you uncheck this option, the files will still be available after decryption, however, their names will be crypted.

8. Click **Decrypt**.

9. The decryption process starts. You can view the number of processed files and the number of errors received during decryption.

10. When decryption is finished, you can view the backup in the location on the local computer to which it was saved by clicking the View  button.



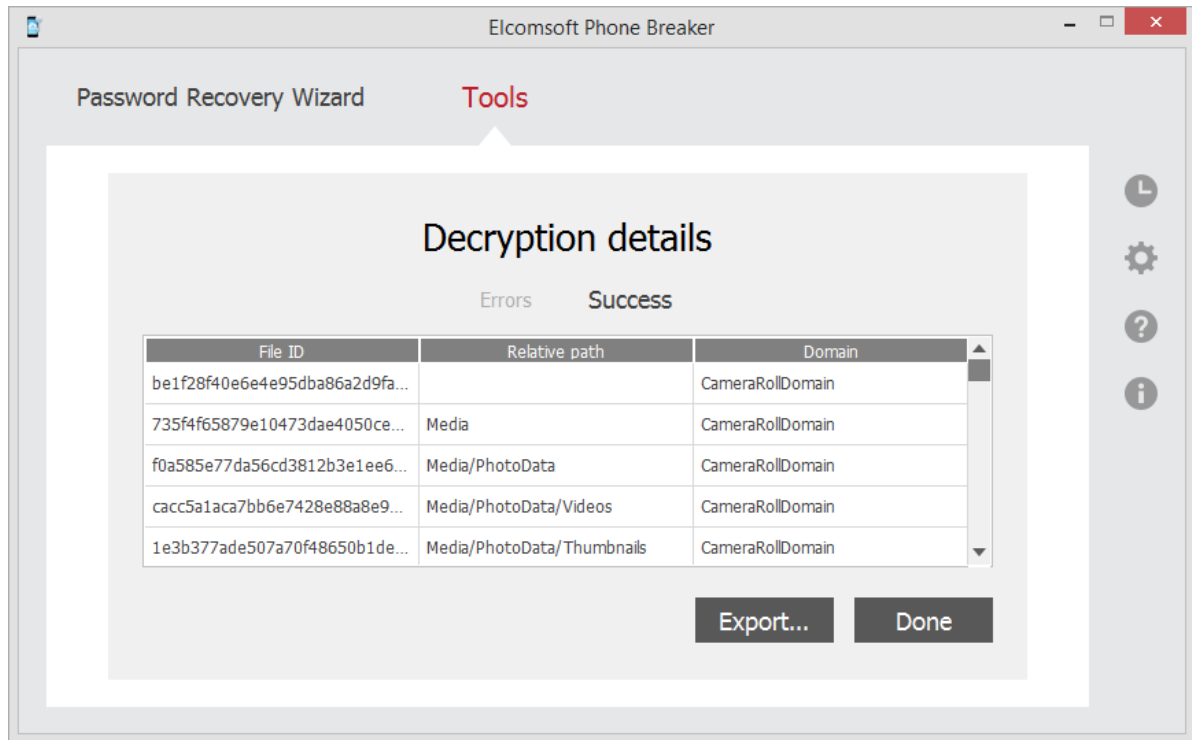
11. To view detailed [report](#) about decrypted files and errors that occurred during decryption, click **Details**.
12. Click **Finish** to close the **Decrypt backup** window.

3.4.4 Decryption details report

Decryption details report allows you to view detailed information about decrypted files and errors that occurred during decryption.

To open the Decryption details report, do the following:

1. After [backup decryption](#) is finished, click **Details**.
2. The **Decryption details** report opens.



Decryption details include:

- **File ID:** The file name made up from a SHA-1 hash of file name, together with its path and domain.
- **Relative path:** The path to the file in a specified domain.
- **Domain:** The name of domain where the file is stored.

To export the **Decryption details** report to a text file or an XML document, click **Export**.

To exit the **Decryption details** report, click **Done**.

3.5 Working with iCloud data

3.5.1 Working with iCloud backups

3.5.1.1 About iCloud backups

It is possible to back up iOS devices data not only locally, but also to iCloud. For more information, please read:

[iCloud - Store and back up your content in iCloud](#)
[Creating an iCloud account: Frequently Asked Questions](#)
[iCloud: Backup and restore overview](#)

Once you have enabled Backup on your device (**Settings | iCloud | Backup & Storage**), it will run on a daily basis as long as the device is connected to Internet over Wi-Fi, connected to a power source, and has the screen locked.

If you know the Apple ID and password (or [authentication token](#) of iCloud user), **EPB** can [extract backup from the iCloud](#), decrypt it, and convert to the same format as used by iTunes. After decryption is completed successfully, you can [explore the backup content](#) using Elcomsoft Phone Viewer.

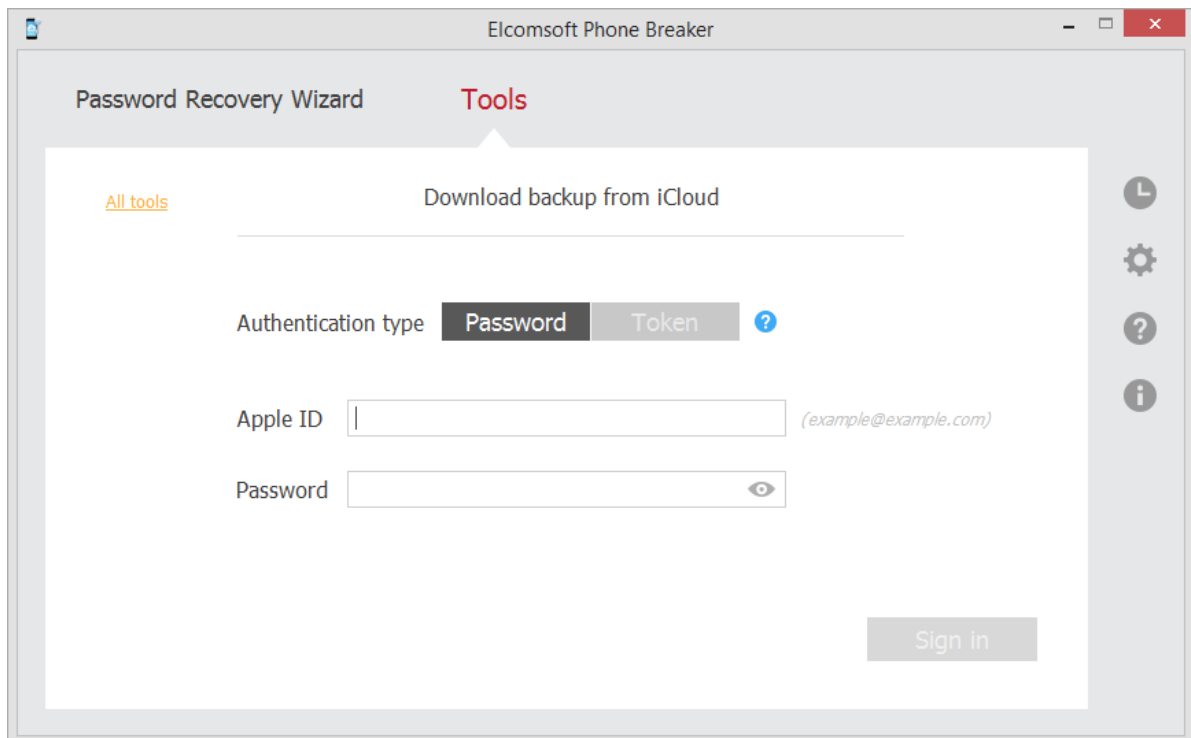
3.5.1.2 Downloading iCloud backup

If you know the Apple ID and the password for entering iCloud, **EPB** can extract backup from the iCloud, decrypt it, and convert to the same format as used by iTunes. After converting iCloud backup to iTunes format, you can [view the backup content](#) in Elcomsoft Phone Viewer for further analysis. It is NOT recommended to restore the device from this copy.

NOTE: To view and download iOS 9.x.x backups from iCloud on Windows PC, it is necessary to have [iCloud Panel](#) ver. 4.0 or higher installed.

To download iCloud backup, do the following:

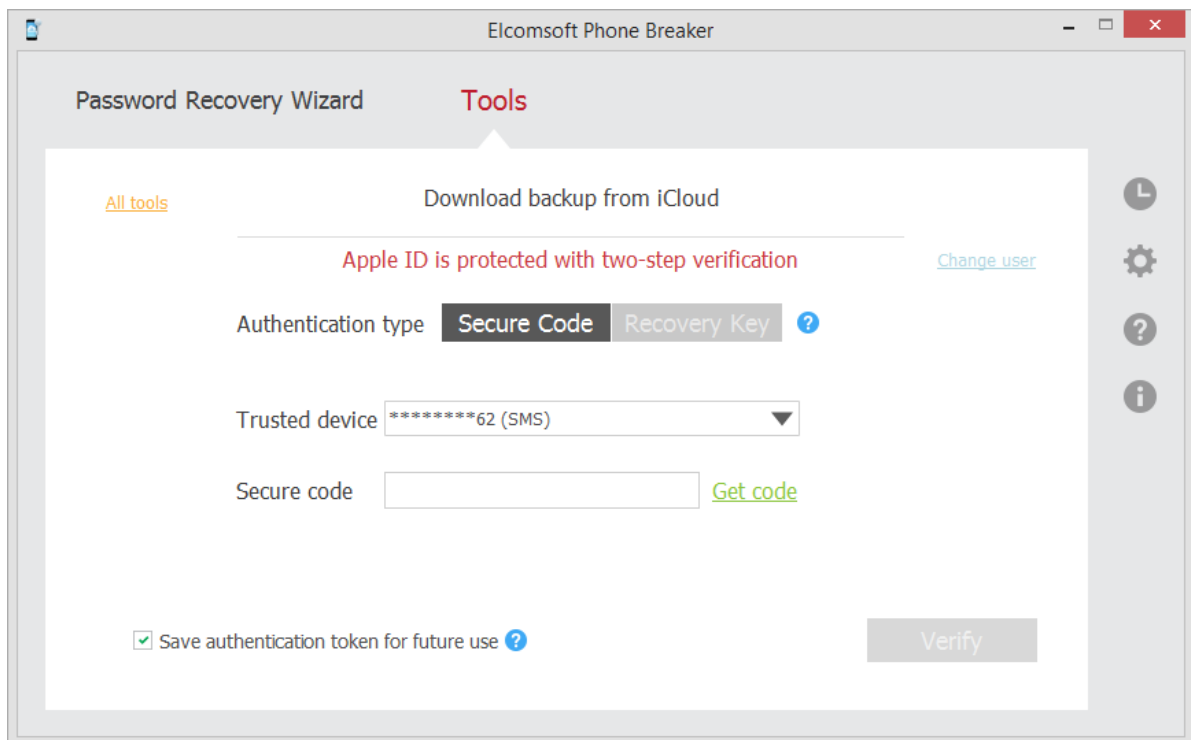
1. In the **Tools** menu, select the **Apple** tab.
2. Select **Download backup from iCloud**.
3. On the **Download backup from iCloud** page, define the authentication type:
 - **Password:** To use your Apple credentials (Apple ID and password)
 - **Token:** To use the Authentication token extracted from iCloud using Elcomsoft Apple Token Extractor. For more information about extracting the token, see the [Extracting Authentication token](#) topic.



The screenshot shows the 'Elcomsoft Phone Breaker' application window. The 'Tools' menu is active, and the 'Download backup from iCloud' page is displayed. The page has two tabs: 'Password' (selected) and 'Token'. Below the tabs are input fields for 'Apple ID' (with a placeholder '(example@example.com)') and 'Password' (with a toggle eye icon). A 'Sign in' button is at the bottom right.

4. Click **Sign in**.

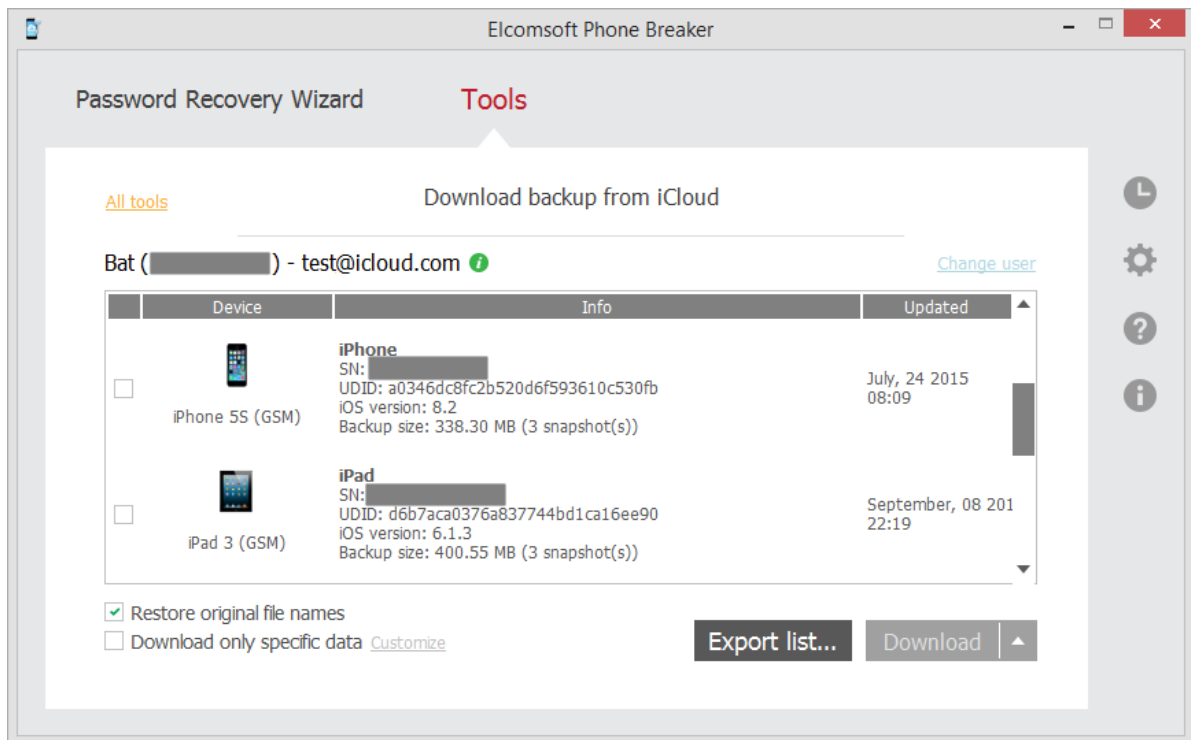
5. If the Apple ID is protected with two-step verification, verify your account by selecting one of the following authentication types:
 - **Secure Code:** in the **Trusted device** field, select a phone number or a trusted device to which the code will be sent, click **Get code**, and then enter the received 4-digit code in the **Secure code** field.
 - **Recovery Key:** enter a 14-character key generated defined in the Apple account settings.
6. Select the **Save authentication token for future use** option, so you don't need to pass two-step verification when you log in with this Apple ID again.
7. Click **Verify**.



8. The iCloud storage of backups opens.

You can view the user name, user ID, and Apple ID of the iCloud user, and the list of backups belonging to this user. By default, 3 latest backups are displayed. Hover mouse over the green *i* icon to view the storage capacity and used size.


To select backups made by a different iCloud user, click **Change user**.



For every device, the following information is displayed:

- Device name
- Model
- Serial number
- Unique device ID
- Date when the latest backup was made
- Size of backup.

9. Select the device(s) whose backups you would like to download by selecting check boxes on the left.

10. Define the options for downloading backups. Click  to view hints for each option.

- **Restore original file names:** If selected, allows saving all backup files with the same file names as in the iOS operating system, including the full path: e.g. messages (SMS and iMessage) are saved as \HomeDomain\Library\SMS\sms.db (SQLite format). If it is not selected, backup will be saved in the same format as iTunes creates when you make the local backup. In that case, you will be able to analyze downloaded backups using any 3rd party software such as [iBackupBot](#) or [Elcomsoft Phone Viewer](#) (if you are holding a license on **EPB**, you can get a discount on iBackupBot; [contact us](#) for more details). Note that this option will be enabled automatically, if you select the next one (Download only specific data).
- **Download only specific data:** Allows selecting [certain types of data](#) to be downloaded.


11. Click **Download** or **Download to** in order to save the backup to the local computer.

12. Define the location for storing the backup and click **Select Folder**.

13. Downloading of iCloud backup begins.

NOTE: The backups that have not been completely created yet will not be downloaded.

14. When downloading is finished, there will be a check mark next to the downloaded backup.

15. In the **Download Status** column, click the **View**  button to view the backup on the local computer.

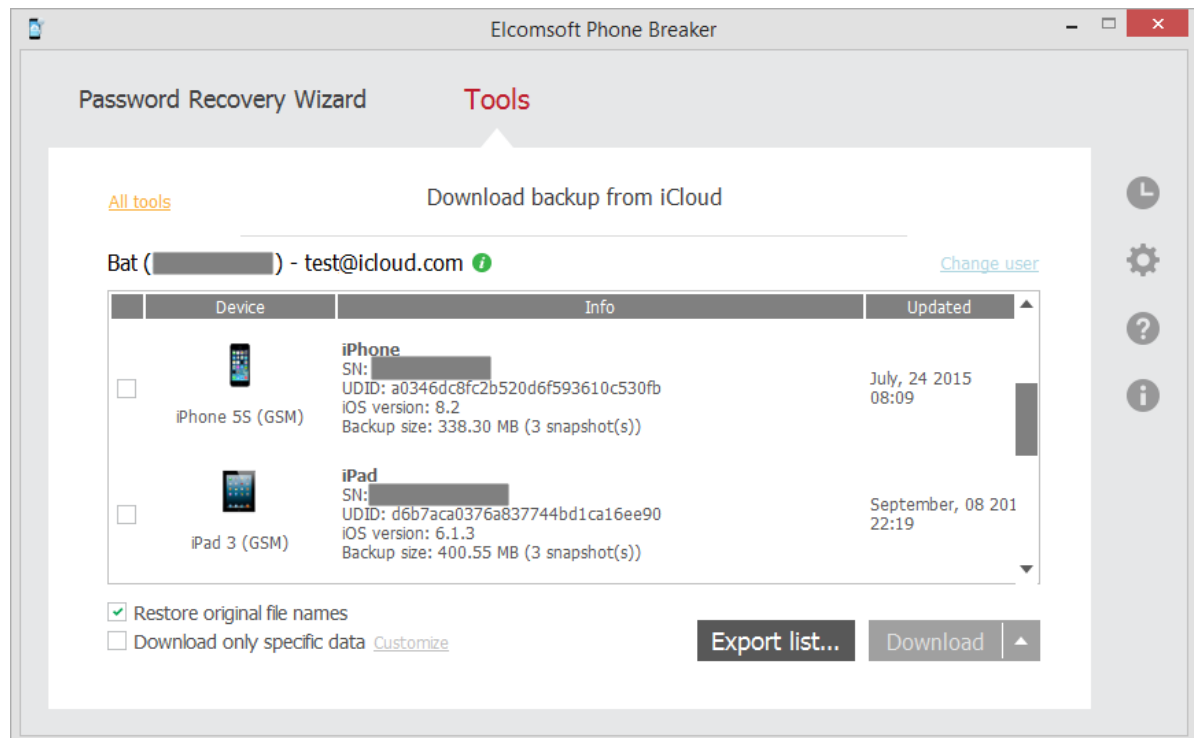
16. Click **Finish** to exit the downloading wizard.

Please note, iOS 9.x.x backups have a different structure than iOS 8.0 and lower backups. That is why if there are several backups of different versions for the same device UDID, they will be saved to a local computer in the folder with UDID name. However, the snapshots belonging to different iOS versions will be stored in different subfolders:

- For iOS 8.0 and lower: in the folder with the name in the form [01][20150507_171956Z][R]
- For iOS 9.x.x: in the folder with the name in the form [A30FD565-3776-4B8E-95AB-B4F06FD930BC][20151007_165923Z]

3.5.1.3 Downloading specific data types

When [downloading iCloud backup](#), you can select the **Download only specific data** option, which allows you to download data from particular categories only.



Click **Customize** to select data to be downloaded. After selecting specific data, the **Customize** link will change its name to **Customized** and its color from **green** to **red**.

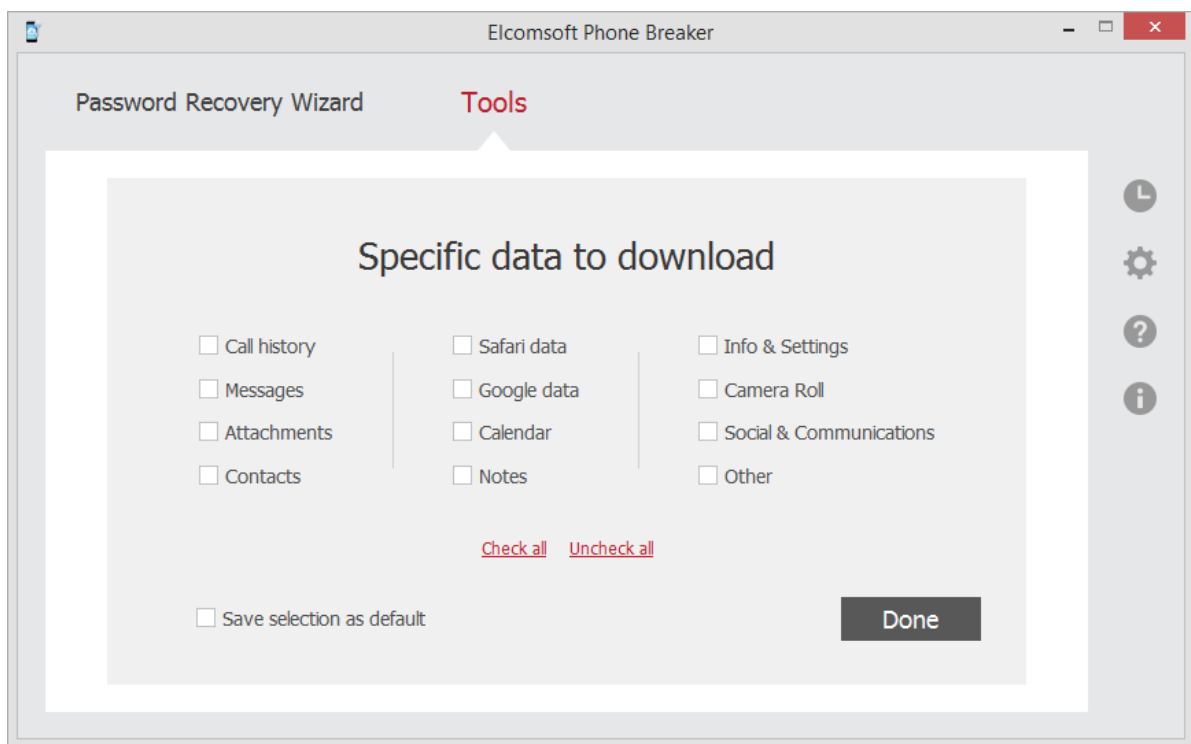
In the **Specific data to download** window, select the categories to be downloaded.

If no category is selected, only the main backup files will be downloaded. These files are used to recover the backup structure. The main files include:

- Info.plist
- Manifest.mbdb
- Manifest.plist
- Status.plist

Select **Check All** or **Uncheck All** to select all categories to be downloaded, or to remove selection from all categories.

Select **Save selections as default** to use current selections as default at the next downloading of a backup.



The following categories are available:

- **Call History** - Allows decrypting the history of incoming, outgoing calls, etc.
The following data will be downloaded:
 \WirelessDomain\Library\CallHistory* (for iOS 7.x and lower)
 \HomeDomain\Library\CallHistoryDB* (for iOS 8.x and higher)
- **Messages** - Allows decrypting SMS, iMessages, and MMS (pictures and video) messages.
The following data will be downloaded:
 \HomeDomain\Library\SMS\sms.db
 \HomeDomain\Library\SMS\Drafts*
- **Attachments** - Includes attachments to SMS messages.
 \MediaDomain\Library\SMS\Attachments*

- **Google data** - Data of Google applications: Google Earth, Chrome, Maps, YouTube, etc.

The following data will be downloaded:

- AppDomain-com.google.b612*
- AppDomain-com.google.GoogleDigitalEditions*
- AppDomain-com.google.GoogleMobile*
- AppDomain-com.google.Blogger*
- AppDomain-com.google.chrome.ios*
- AppDomain-com.google.coordinate*
- AppDomain-com.google.Drive*
- AppDomain-com.google.Gmail*
- AppDomain-com.google.GoogleBooks*
- AppDomain-com.google.GooglePlus*
- AppDomain-com.google.GVDialer*
- AppDomain-com.google.ios.youtube*
- AppDomain-com.google.Maps*
- AppDomain-com.google.offers*
- AppDomain-com.google.Orkut *
- AppDomain-com.google.Translate*
- AppDomain-com.google.hangouts*
- AppDomain-com.google.Authenticator*

See [Google Apps for iOS](#) for details on Google applications.

- **Safari data** - Includes Safari history, cache, cookies, search history.

The following data will be downloaded:

- \HomeDomain\Library\Safari*
- \HomeDomain\Library\Caches*
- \HomeDomain\Library\Cookies*
- \AppDomain-com.apple.mobilesafari*

- **Contacts** - Includes the phone numbers and associated names, email addresses, and other information stored in the Contacts list.

The following data will be downloaded:

- \HomeDomain\Library\AddressBook\AddressBook.sqlitedb
- \HomeDomain\Library\AddressBook\AddressBookImages.sqlitedb

- **Notes** - Allows decrypting notes created by the user.

The following data will be downloaded:

- \HomeDomain\Library\Notes\notes.idx
- \HomeDomain\Library\Notes\notes.sqlite

- **Info & Settings** - Includes the device settings and configuration data.

The following data will be downloaded:

- \HomeDomain\Library\Accounts*.*
- \HomeDomain\Library\ConfigurationProfiles*.*
- \HomeDomain\Library\Preferences*.*
- \RootDomain\Library\Preferences*.*
- \SystemPreferencesDomain*.*
- \WirelessDomain\Library\Preferences*.*

- **Calendar** - Includes calendar events created by the user.

The following data will be downloaded:

- \HomeDomain\Library\Calendar\Calendar.sqlitedb

- **Camera roll** - Includes photos and videos stored in the backup.
 \CameraRollDomain*

- **Social & Communications** - Includes data from instant messengers, such as Skype, WhatsApp, Viber, etc., and social networks.
 The following data will be downloaded:
 - AppDomain-net.whatsapp.WhatsApp*
 - AppDomainGroup-group.net.whatsapp.WhatsApp.shared*
 - AppDomain-com.burbn.instagram*
 - AppDomain-com.facebook.Facebook*
 - AppDomain-com.facebook.Messenger*
 - AppDomain-com.skype.skype*
 - AppDomain-com.atebits.Tweetie2*
 - AppDomain-com.linkedin.Linkedin*
 - AppDomain-com.naveenium.foursquare*
 - AppDomain-com.viber*
 - AppDomain-com.tencent.mQQi*
 - AppDomain-com.tencent.mqq*
 - AppDomain-com.blackberry.bbm1*
 - AppDomain-com.kik.chat*
 - AppDomain-com.aol.aim*
 - AppDomain-com.p.pmsn2free*
 - AppDomain-com.shapeservices.implus*
 - AppDomain-com.ebuddy.xms*
 - AppDomain-com.beejive.WLM*
 - AppDomain-com.beejive.GTalk*
 - AppDomain-com.beejive.YIM*
 - AppDomain-com.beejive.AIM*
 - AppDomain-com.beejive.FacebookIM*
 - AppDomain-com.ceruleanstudios.trillian.iphone*
 - AppDomain-com.yahoo.messenger*

- **Other** - Includes user's dictionaries, voicemail data, Apple maps, Passbook data, and cached mail.
 The following data will be downloaded:
 - \HomeDomain\Library\Keyboard*
 - \HomeDomain\Library\Passes*
 - \HomeDomain\Library\Voicemail*
 - \HomeDomain\Library\Maps*
 - \HomeDomain\Library\SpringBoard*
 - \HomeDomain\Library\Mail*
 - \HomeDomain\Library\WebKit\Databases*
 - \HomeDomain\Library\DataAccess*
 - \RootDomain\Library\Caches\locationd*
 - \KeyboardDomain\Library\Keyboard*

You can [explore the downloaded data](#) in Elcomsoft Phone Viewer.

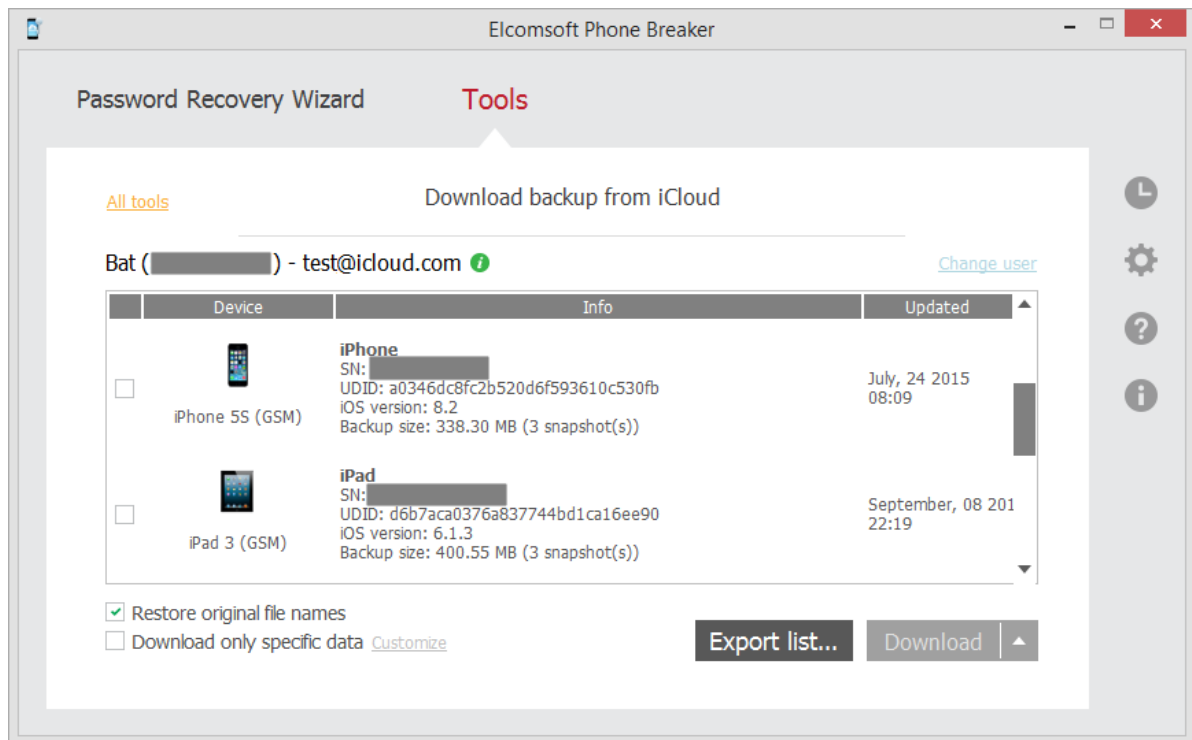
3.5.1.4 Exporting backup list

After [opening iCloud backup](#), you can export the list of backups in it into XML 1.1 format.

NOTE: To view and download iOS 9.x.x backups from iCloud on Windows PC, it is necessary to have [iCloud Panel ver. 4.0 or higher installed](#).

To export the list of iOS device backups in the iCloud, do the following:

1. Click **Export List**.



2. Define the location of the exported XML file.

3. The list is exported. Information about each iOS device contains device name, serial number, UDID, type, model, iOS version, information on the last snapshot, user name, user id, and whether two-step authentication is enabled or not.

3.5.1.5 Possible problems with downloading data from iCloud

Problem	Solution
When downloading the backup from iCloud, the following message is displayed: "The requested backup could not be found" .	The backup you are trying to download has been updated. Log out, then log in to iCloud and try again.
The necessary backup is not available in the list of items for downloading.	The backup is being created at the moment. It will be available as soon as it is created completely.
When downloading the data from iCloud, the message is displayed: "The iCloud Terms of Service have changed. Please log into iCloud panel and accept new terms to continue working with	The Terms of Service for iCloud have changed and the user needs to acknowledge them before using iCloud. Log into the iCloud panel and accept the new Terms of Service.

iCloud services."	After that, you will be able to work with data from iCloud via EPB.
-------------------	---

3.5.1.6 iCloud backup structure (iOS 8.0 and lower)

Once iCloud backup is downloaded and processed, the following folders are created in the destination folder:

```
.chunks
  00
  01
  ...
  ff
<device id>
  .keys
  [01]
  [N]
  [N+1]
  [01 date/timeZ]
  [N date/timeZ]
  [N+1 date/timeZ]
```

The `.chunks` folder is actually the 'cache' of the (raw) data downloaded, to save the time when/if you download backups for the same device again.

The first three folders (with numbers as names) are also the raw data as it is stored in the iCloud, partially converted (and already decrypted). Please note that iCloud backups are cumulative, so in most cases, the first folder is the largest (and its total size is compared to the size of the device itself), the second is much smaller, and the third one is the smallest.

Finally, the folders with the date/time in the names are 'complete' backups converted to Apple iTunes format, and each of them has about the same size as the backup itself (as far as backups are usually being done on a daily basis, the differences are rather small). If you used the *Restore original file names* (or [Download only specific data](#)) option, the folders with date/time will also have the [R] suffix at the end (and the size of each folder may be less than backup size, because not all the data is downloaded).

So the total size needed to store all backup(s) is usually five times more than the size of the single backup as shown on the device itself, or by the program.

Whether or not you are using *Restore original file names* option, it is recommended to download backups always to the same folder, and *do not* delete the `.chunks` folder – downloading will be much faster.

Example

Without *Restore original file names* option:

```
.keys
1
19
20
[01][20131124_132403Z]
[19][20131126_130112Z]
[20][20131128_132645Z]
```

or with *Restore original file names* option:

```
.keys
1
19
20
[01][20131124_132403Z][R]
[19][20131126_130112Z][R]
[20][20131128_132645Z][R]
```

Here you get three backups: created at 24/11/1013, 26/11/2013 and 28/11/2013. The latest backups are in [20][20131128_132645Z] and [20][20131128_132645Z][R] folders respectively.

Full backup (in [20][20131128_132645Z]) contains a lot of files with names like 0ea4ce4cc6e4ce70e34584423b6cfd6fe87fa, plus just four files with readable names:

```
Info.plist
Manifest.mbdb
Manifest.plist
Status.plist
```

This is a complete backup in iTunes format, and there is little you can do with it without additional software like [iBackupBot](#) or [Oxygen Forensic Suite](#).

Converted backups look better, preserving the complete folder structure, as well as the file names as they are stored in iOS file system. Most data is stored is SQLite databases (.db and .sqlite) and .plist files; you also get the pictures in PNG and JPEG, etc.

For more information on backup analysis, please read the following article:

[I've Got the iTunes Backup from the iCloud. What Shall I Do Now?](#)

3.5.1.7 Supported models

EPB 5.10 supports iCloud backups of the Apple devices listed in the table. Maximum iOS version is actual for EPB 5.10 release date.

If you have noticed any inaccuracies, please [contact us](#).

Model	Friendly name	Model No.	Internal name	Identifier	Storage	Original iOS version	Maximum iOS version
iPhone (Original/EDGE)	iPhone	A1203	m68ap	iPhone1,1	4/8/16	1.0	3.1.3
iPhone 3G	iPhone 3G	A1241	n82ap	iPhone1,2	8/16	2.0	4.2.1
iPhone 3G (China/No Wi-Fi)	iPhone 3G (China)	A1324	n82ap	iPhone1,2	8/16	3.0	4.2.1

iPhone 3GS	iPhone 3GS	A1303	n88ap	iPhone2,1	8/16/32	3.0	6.1.6
iPhone 3GS (China/No Wi-Fi)	iPhone 3GS (China)	A1325	n88ap	iPhone2,1	8/16/32	3.0	6.1.6
iPhone 4 (GSM)	iPhone 4 (GSM)	A1332	n90ap	iPhone3,1	8/16/32	4.0	7.1.2
iPhone 4	iPhone 4 (GSM)	A1332	n90ap	iPhone3,2	8	6.0	7.1.2
iPhone 4 (CDMA/Verizon/Sprint)	iPhone 4 (CDMA)	A1349	n92ap	iPhone3,3	8/16/32	4.2.6	7.1.2
iPhone 4S	iPhone 4S	A1387	n94ap	iPhone4,1	16/32/64	5.0	9.1
iPhone 4S (GSM China/WAPI)	iPhone 4S (China)	A1431	n94ap	iPhone4,1	16/32/64	5.1	9.1
iPhone 5 (GSM/LTE 4, 17/North America)	iPhone 5 (GSM)	A1428	n41ap	iPhone5,1	16/32/64	6.0	9.1
iPhone 5 (CDMA/LTE, Sprint/Verizon/KDDI)	iPhone 5 (GSM +CDMA)	A1429	n42ap	iPhone5,2	16/32/64	6.0	9.1
iPhone 5 (CDMA China/UIM/WAPI)	iPhone 5 (China)	A1442	n42ap	iPhone5,2	16/32/64	6.0	9.1
iPhone 5C	iPhone 5C (GSM)	A1456	n48ap	iPhone5,3	16/32	7.0	9.1
iPhone 5C	iPhone 5C (GSM)	A1532	n48ap	iPhone5,3	16/32	7.0	9.1
iPhone 5C	iPhone 5C (GSM +CDMA)	A1507	n49ap	iPhone5,4	16/32	7.0	9.1
iPhone 5C	iPhone 5C (GSM +CDMA)	A1516	n49ap	iPhone5,4	16/32	7.0	9.1
iPhone 5C	iPhone 5C (China)	A1526	n49ap	iPhone5,4	16/32	7.0	9.1

iPhone 5C	iPhone 5C (GSM +CDMA)	A1529	n49ap	iPhone5,4	16/32	7.0	9.1
iPhone 5S	iPhone 5S (GSM)	A1433	n51ap	iPhone6,1	16/32/64	7.0	9.1
iPhone 5S	iPhone 5S (GSM)	A1533	n51ap	iPhone6,1	16/32/64	7.0	9.1
iPhone 5S	iPhone 5S (GSM +CDMA)	A1457	n53ap	iPhone6,2	16/32/64	7.0	9.1
iPhone 5S	iPhone 5S (GSM +CDMA)	A1518	n53ap	iPhone6,2	16/32/64	7.0	9.1
iPhone 5S	iPhone 5S (China)	A1528	n53ap	iPhone6,2	16/32/64	7.0	9.1
iPhone 5S	iPhone 5S (GSM +CDMA)	A1530	n53ap	iPhone6,2	16/32/64	7.0	9.1
iPhone 6 (GSM/ North America)	iPhone 6 (GSM)	A1549	n56ap	iPhone7,2	16/64/128	8.0	9.1
iPhone 6 (CDMA/ Verizon)	iPhone 6 (CDMA)	A1549	n56ap	iPhone7,2	16/64/128	8.0	9.1
iPhone 6 (Global/ Sprint)	iPhone 6 (GSM +CDMA)	A1586	n56ap	iPhone7,2	16/64/128	8.0	9.1
iPhone 6 (China Mobile)	iPhone 6 (China)	A1589	n56ap	iPhone7,2	16/64/128	8.0	9.1
iPhone 6 Plus (GSM/ North America)	iPhone 6 Plus (GSM)	A1522	n56ap	iPhone7,1	16/64/128	8.0	9.1
iPhone 6 Plus (CDMA/ Verizon)	iPhone 6 Plus (CDMA)	A1522	n56ap	iPhone7,1	16/64/128	8.0	9.1
iPhone 6 Plus (Global/ Sprint)	iPhone 6 Plus (GSM +CDMA)	A1524	n56ap	iPhone7,1	16/64/128	8.0	9.1
iPhone 6	iPhone 6	A1593	n56ap	iPhone7,1	16/64/128	8.0	9.1

Plus (China Mobile)	Plus (China)						
iPhone 6s (AT&T/SIM Free/ A1633)	iPhone 6s (SIM Free)	A1633	N71AP N71mAP	iPhone8,1	16/64/128	9.0	9.1
iPhone 6s (Global/ A1688)	iPhone 6s (Global)	A1688	N71AP N71mAP	iPhone8,1	16/64/128	9.0	9.1
iPhone 6s (Mainland China/ A1700)	iPhone 6S (China)	A1700	N71AP N71mAP	iPhone8,1	16/64/128	9.0	9.1
iPhone 6s Plus (AT&T/SIM Free/ A1634)	iPhone 6s Plus (SIM Free)	A1634	N66AP N66mAP	iPhone8,2	16/64/128	9.0	9.1
iPhone 6s Plus (Global/ A1687)	iPhone 6s Plus (Global)	A1687	N66AP N66mAP	iPhone8,2	16/64/128	9.0	9.1
iPhone 6s Plus (Mainland China/ A1699)	iPhone 6S Plus (China)	A1699	N66AP N66mAP	iPhone8,2	16/64/128	9.0	9.1
iPod touch (Original)	iPod Touch	A1213	n45ap	iPod1,1	8/16	1.1	3.1.3
iPod touch (2nd Gen)	iPod Touch 2	A1288	n72ap	iPod2,1	8/16/32	2.1	4.2.1
iPod touch (3rd Gen)	iPod Touch 3	A1318	n18ap	iPod3,1	32/64	3.1.1	5.1.1
iPod touch (4th Gen)	iPod Touch 4	A1367	n81ap	iPod4,1	8/16/32/64	4,1	6.1.6
iPod touch (5th Gen)	iPod Touch 5	A1421	n78ap	iPod5,1	32/64	6.0	9.1
iPod touch (5th Gen, No iSight, 2013)	iPod Touch 5	A1509	n78aap	iPod5,1	16	6.0	9.1
iPod touch (6th)	iPod Touch 6	A1574	n102ap	iPod7,1	16/32/64/1 28	8.4	9.1

generation)							
iPad Wi-Fi (Original)	iPad	A1219	k48ap	iPad1,1	16/32/64	3.2	5.1.1
iPad Wi-Fi/3G/GPS (Original)	iPad (GSM)	A1337	k48ap	iPad1,1	16/32/64	3.2	5.1.1
iPad 2 (Wi-Fi Only)	iPad 2	A1395	k93ap	iPad2,1	16/32/64	4.3	9.1
iPad 2 (Wi-Fi/GSM/GPS)	iPad 2 (GSM)	A1396	k94ap	iPad2,2	16/32/64	4.3	9.1
iPad 2 (Wi-Fi/CDMA/GPS)	iPad 2 (CDMA)	A1397	k95ap	iPad2,3	16/32/64	4.3	9.1
iPad 2 (Wi-Fi Only, China)	iPad 2	A1395	k93aap	iPad2,4	16	4.3	9.1
iPad 3rd Gen (Wi-Fi Only)	iPad 3	A1416	j1ap	iPad3,1	16/32/64	5.1	9.1
iPad 3rd Gen (Wi-Fi/Cellular Verizon/GPS)	iPad 3 (GSM +CDMA)	A1403	j2ap	iPad3,2	16/32/64	5.1	9.1
iPad 3rd Gen (Wi-Fi/Cellular AT&T/GPS)	iPad 3 (GSM)	A1430	j2aap	iPad3,3	16/32/64	5.1	9.1
iPad 4th Gen (Wi-Fi Only)	iPad 4	A1458	p101ap	iPad3,4	16/32/64/128	6.0	9.1
iPad 4th Gen (Wi-Fi/AT&T/GPS)	iPad 4 (GSM)	A1459	p102ap	iPad3,5	16/32/64/128	6.0	9.1
iPad 4th Gen (Wi-Fi/Verizon & Sprint/GPS)	iPad 4 (GSM +CDMA)	A1460	p103ap	iPad3,6	16/32/64/128	6.0	9.1
iPad Air (Wi-Fi)	iPad Air	A1474	j71ap	iPad4,1	16/32/64/128	7.0	9.1

Only)							
iPad Air (Cellular)	iPad Air (Cellular)	A1475	j72ap	iPad4,2	16/32/64/128	7.0	9.1
iPad Air (TD-SCDMA, China)	iPad Air (China)	A1476	j73ap	iPad4,3	16/32/64/128	7.1	9.1
iPad Air 2 (Wi-Fi Only)	iPad Air 2 (Wi-Fi)	A1566	j74ap	iPad5,3	16/64/128	8.1	9.1
iPad Air 2 (Wi-Fi/Cellular)	iPad Air 2 (Wi-Fi +Cellular)	A1567	j75ap	iPad5,4	16/64/128	8.1	9.1
iPad mini (Wi-Fi Only)	iPad Mini	A1432	p105ap	iPad2,5	16/32/64	6.0	9.1
iPad mini (Wi-Fi/AT&T/GPS)	iPad Mini (GSM)	A1454	p106ap	iPad2,6	16/32/64	6.0	9.1
iPad mini (Wi-Fi/Verizon & Sprint/GPS)	iPad Mini (GSM +CDMA)	A1455	p107ap	iPad2,7	16/32/64	6.0	9.1
iPad Mini (Wi-Fi Only)	iPad Mini w/Retina	A1489	j85ap	iPad4,4	16/32/64/128	7.0	9.1
iPad Mini (Cellular)	iPad Mini w/Retina (Cellular)	A1490	j86ap	iPad4,5	16/32/64/128	7.0	9.1
iPad Mini (TD-SCDMA, China)	iPad Mini w/Retina (China)	A1491	j87ap	iPad4,6	16/32/64/128	7.1	9.1
iPad Mini 2 (Retina/2nd Gen, Wi-Fi Only)	iPad Mini 2 w/Retina (Wi-Fi)	A1489	j88ap	iPad4,4	16/32/64/128	7.0	9.1
iPad Mini 2 (Retina/2nd Gen, Wi-Fi/Cellular)	iPad Mini 2 w/Retina (Wi-Fi + Cellular)	A1490	j89ap	iPad4,5	16/32/64/128	7.0.3	9.1

iPad Mini 2 (Retina/2nd Gen, China)	iPad Mini 2 w/Retina (Wi-Fi + Cellular, China)	A1491	j90ap	iPad4,6	16/32/64/128	7.0.3	9.1
iPad mini 3 (Wi-Fi Only)	iPad mini 3 (Wi-Fi)	A1599	J85map	iPad4,7	16/64/128	8.1	9.1
iPad mini 3 (Wi-Fi/ Cellular)	iPad mini 3 (Wi-Fi + Cellular)	A1600	J86map	iPad4,8	16/64/128	8.1	9.1
iPad mini 3 (Wi-Fi/ Cellular, China)	iPad mini 3 (Wi-Fi + Cellular, China)	A1601	J87map	iPad4,9	16/64/128	8.1	9.1
iPad mini 4 (Wi-Fi Only)	iPad mini 4 (Wi-Fi)	A1538	J96ap	iPad5,1	16/64/128	9.0	9.1
iPad mini 4 (Wi-Fi/ Cellular)	iPad mini 4 (Wi-Fi + Cellular)	A1550	J97ap	iPad5,2	16/64/128	9.0	9.1

3.5.2 Working with files in iCloud

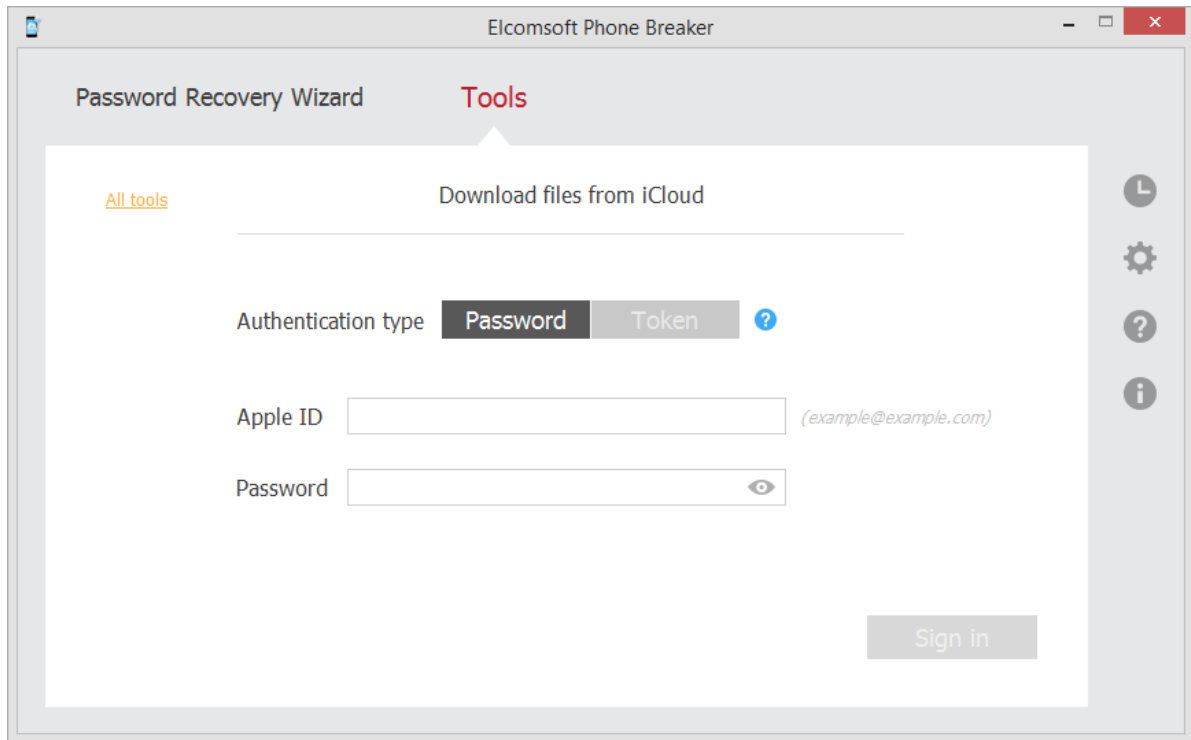
3.5.2.1 Downloading files from iCloud

iCloud stores files used by different iOS device applications together with other data synchronized with iCloud. **EPB** allows downloading and viewing these files.

NOTE: When running EPB on OS X, downloading files from iCloud for Apple IDs that have already been updated to iCloud Drive is only available when running the program on OS X 10.10 and higher. There are no limitations when using the Windows version of EPB.

To download files from iCloud, do the following:

1. In the **Tools** menu, select the **Apple** tab.
2. Select **Download files from iCloud**.
3. On the **Download files from iCloud** page, define the authentication type:
 - **Password:** To use your Apple credentials (Apple ID and password)
 - **Token:** To use the Authentication token extracted from iCloud using Elcomsoft Apple Token Extractor. For more information about extracting the token, see the [Extracting Authentication token](#) topic.



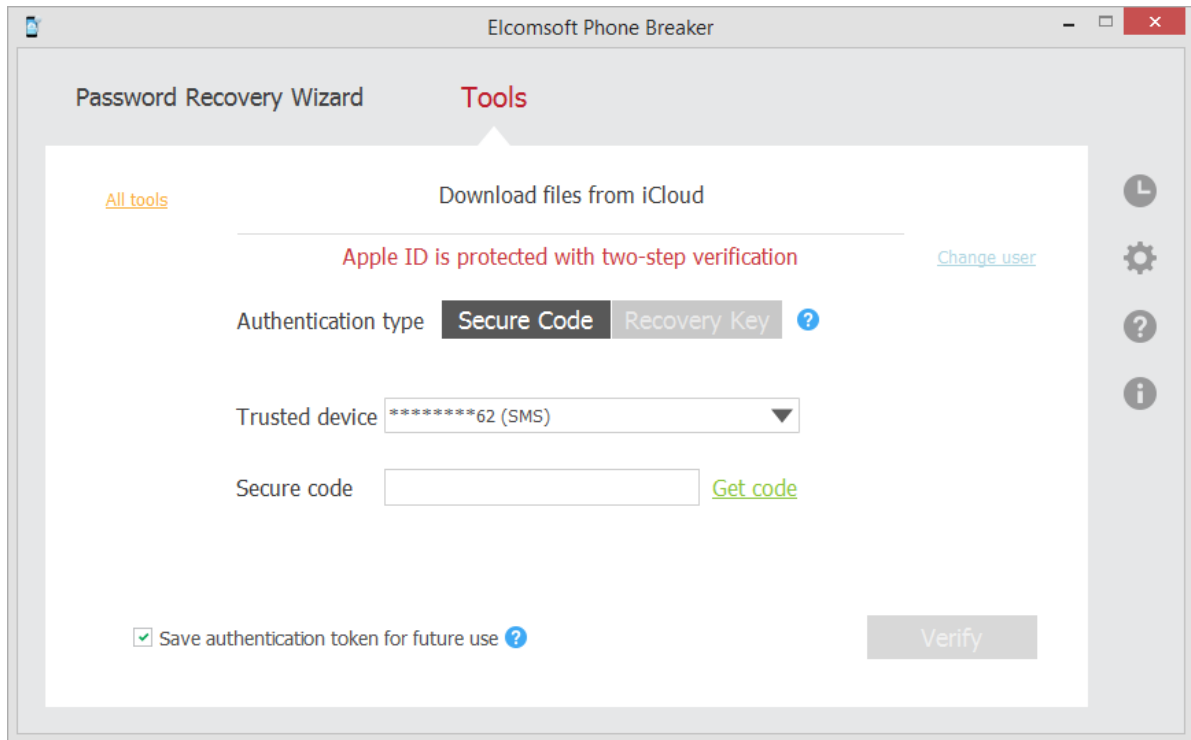
4. Click **Sign in**.

5. If the Apple ID is protected with two-step verification, verify your account by selecting one of the following authentication types:

- **Secure Code:** in the **Trusted device** field, select a phone number or a trusted device to which the code will be sent, click **Get code**, and then enter the received 4-digit code in the **Secure code** field.
- **Recovery Key:** enter a 14-character key generated defined in the Apple account settings.

6. Select the **Save authentication token for future use** option, so you don't need to pass two-step verification when you log in with this Apple ID again.

7. Click **Verify**.

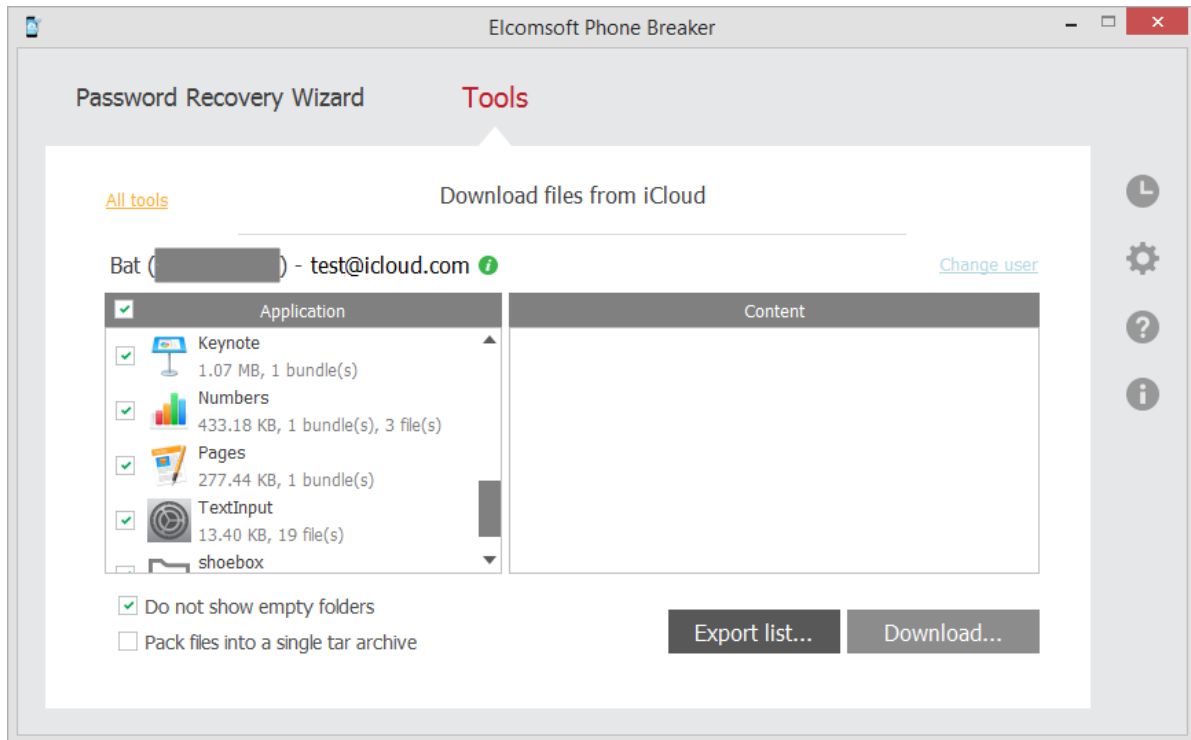


8. The iCloud opens.

You can view files and folders in the **Application** column. The folder's content is displayed in the **Content** column upon clicking the folder name.

Hover mouse over the green *i* icon to view the storage capacity and used size.

To select files made by a different iCloud user, click **Change user**.



The following types of files are supported:

- Regular files
- iWorks bundles
- Other bundles

9. Select the folders and files, which you would like to download by selecting check boxes on the left. The files will be saved in their native format.

10. Select the **Pack files into a single tar archive** option, if you want to download the data in an archive.

11. Click **Download**.

12. Define the location for storing downloaded data.

13. The downloading of iCloud files begins.

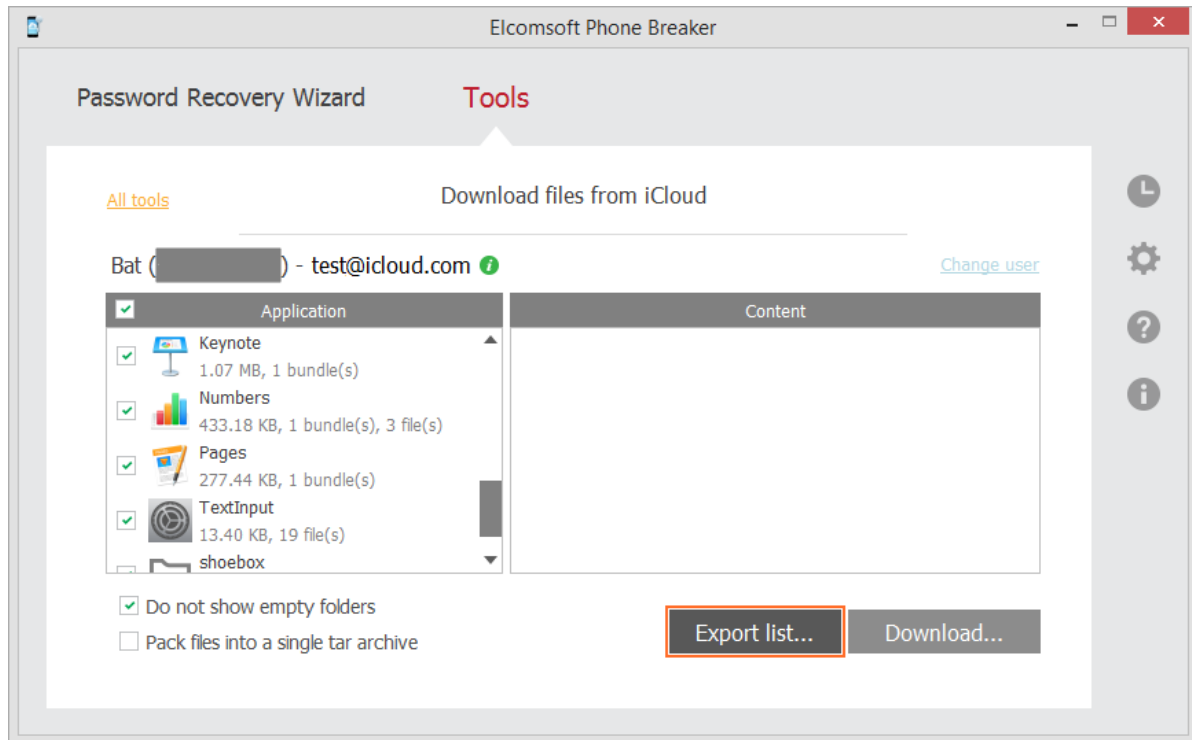
14. When it is finished, click **Finish** to exit the downloading wizard.

3.5.2.2 Exporting iCloud files list

EPB allows exporting the list of files in the iCloud into XML format.

To export the list of files in the iCloud, do the following:

1. Click **Export List**.



2. Define the location of the exported XML file.

3. The list is exported. Information about each file contains file name, path to the file, size of the file in bytes, and time stamp, which indicates the date and time of the last file modification.

3.6 Extracting authentication token for iCloud

3.6.1 About Authentication token

iCloud allows the users to store various information from their iOS devices in the cloud. OS X users can access iCloud without any additional software, as it is built into the operating system (iCloud requires OS X v.10.7.2 or later).

iOS users can get access to their data on Windows OS as well. In this case, exchanging data between iOS devices and the computer is done via the iCloud Control Panel (available for Windows 7 or later). This software allows the user to work with data from iOS on a computer with Windows OS.

EPB allows you to extract authentication token representing the user's iCloud account credentials. You can use this token to sign in to the user's iCloud account in order to download the backups or files stored there. Extracting authentication token is available both from iCloud on OS X and from iCloud Control Panel on Windows OS. It is also possible to get authentication token without logging in to an actual OS where the token was used (e.g., by mounting a disk image to the current system).

The following ways of extracting the token are available:

Operating system	System type	Ways of extraction
Windows	Live system (current system)	Using command-line utility (atex.exe).

	Non-live system (e.g., from the mounted disk image)	Via EPB interface
OS X	Live system (current system)	Using command-line utility (atex.dmg)
	Non-live system (e.g., from the mounted disk image)	Via EPB interface

3.6.2 Extracting token on Windows OS

3.6.2.1 Extracting token on live Windows OS

You can sign in to iCloud account to download the backups and files stored there using the iCloud authentication token.

To extract the token from the current system, you will need an Elcomsoft Apple Token Extractor for Windows OS. This tool is shipped together with EPB (**atex.exe** file). You can find it in EPB installation folder. It is not recommended to start atex.exe from EPB installation folder as there may be not enough permissions for performing token extraction. Copy a file to a folder where you would like the file with authentication token to be created.

EPB allows you to extract authentication tokens for:

- Current iCloud Control Panel user
- Other Windows user who uses iCloud Control Panel on the current computer
- [User of a non-live operating system](#) (e.g., by using disk image mounted to the current computer)

User permissions required for getting authentication token:

Authentication Token For	Permissions Required
iCloud account of the currently logged Windows user	User's permissions are enough
iCloud account of a different Windows user	Run atex.exe as administrator (if UAC is turned on)

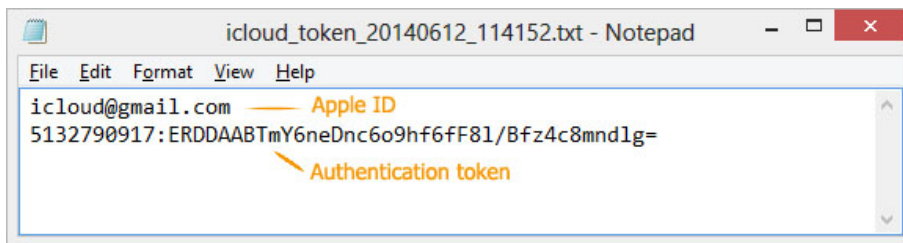
NOTE: When you run atex.exe from a system folder or from the folder you don't have enough permissions to modify, the Windows User Account Control message requesting permission for running this program might appear.

To extract the authentication token for the current iCloud Control Panel user, do the following:

1. Launch **atex.exe**. The file "**icloud_token_<timestamp>.txt**" will be created in the directory from which **atex.exe** was launched (or in the C:\Users\\AppData\Local\Temp folder, if you don't have enough permissions for writing files to the folder where **atex.exe** was launched from).

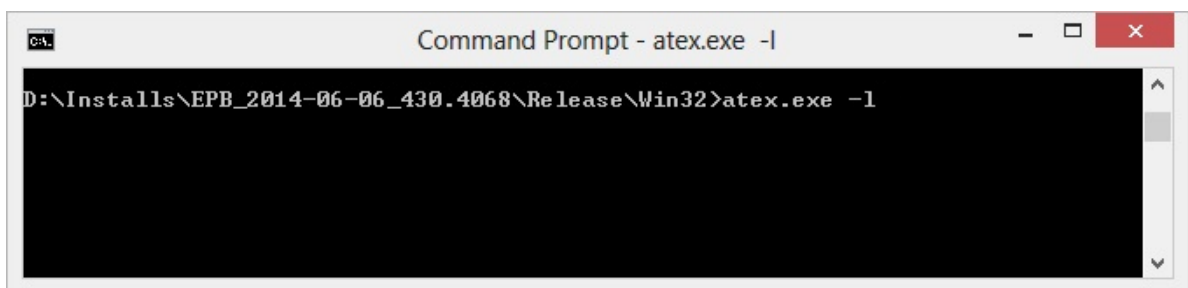
You will see the full path to the file in the opened console window. Please note that Unicode symbols in the file path are not supported.

2. The created .txt file contains the Apple ID of the current iCloud Control Panel user and its Authentication token.



To extract the Authentication token for a certain Windows user, do the following:

1. Open the Command Prompt.
2. Go to the folder where atex.exe is stored.
3. Enter the command **atex.exe -l**



4. The list of all local iCloud users will be displayed.

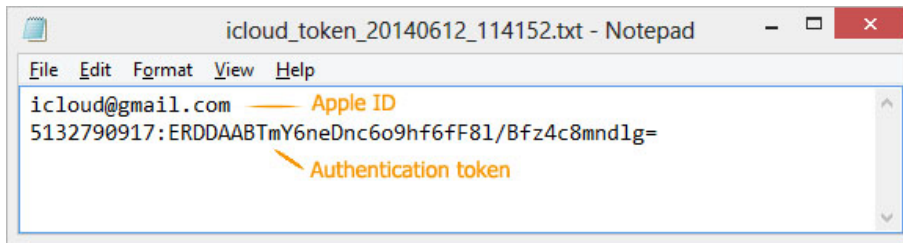


5. Launch atex.exe with getTokenOnline parameter and enter username of a specific local Windows user and the password to this Windows user account in the following form: **atex.exe --getTokenOnline -n <username> -p <password>**

For example: **atex.exe --getTokenOnline -n user1 -p 1234**

6. The "icloud_token_<timestamp>.txt" will be created in the directory from which **atex.exe** was launched.

The created .txt file contains the Apple ID of the current iCloud Control Panel user and its Authentication token.



Parameters for running atex.exe in the command prompt:

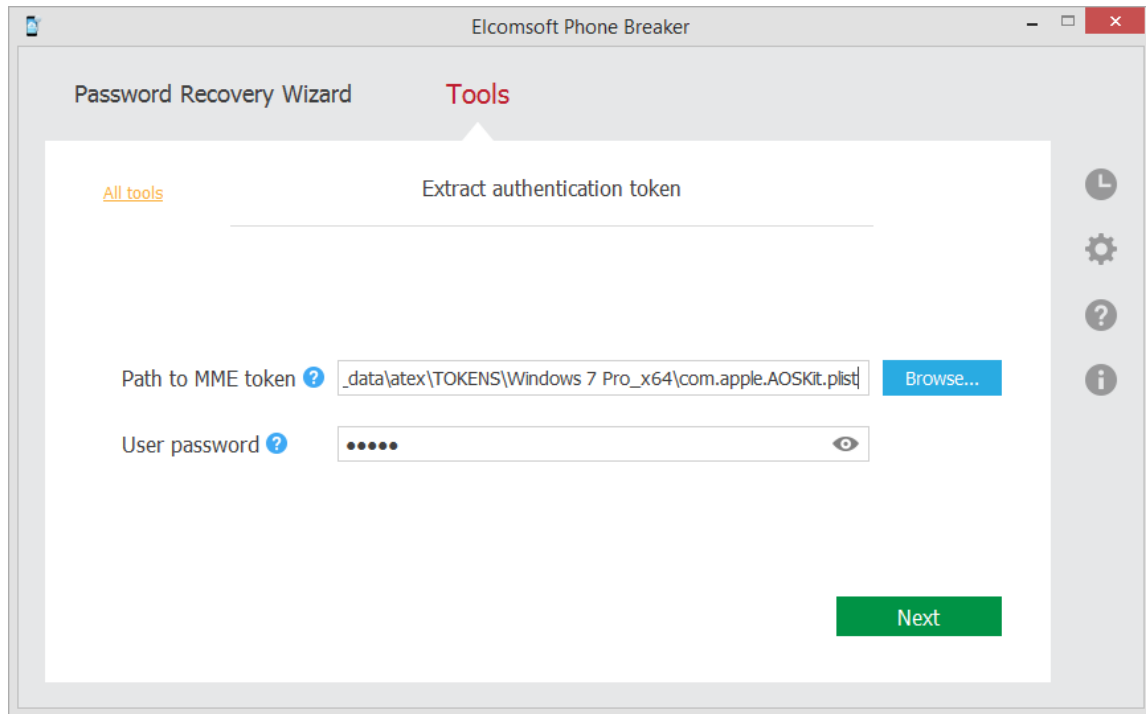
Parameter	Meaning
-h	Displays help message
-l	Displays usernames of iCloud users
--getTokenOnline -n <username> -p <password>	Gets the authentication token for a specified user. Username and password should be entered without brackets.

3.6.2.2 Extracting token on non-live Windows OS

EPB allows you to extract an authentication token to iCloud Panel from a non-live Windows OS, e.g., by mounting the disk image of the operating system in which the token is stored.

To extract the authentication token to iCloud panel, do the following:

1. Mount the image of the disk containing the authentication token.
2. Run Elcomsoft Phone Breaker.
3. In the **Tools** menu, select the **Apple** tab.
4. Click **Extract authentication token**.
5. Define the path and password to the file containing the authentication token:
 - **Path to MME token:** Enter the path to com.apple.AOSKit.plist file. It is usually located in: %appdata%\Apple Computer\Preferences\ on Windows OS.
 - **Password:** Enter the password of the Windows user whose token you are extracting.



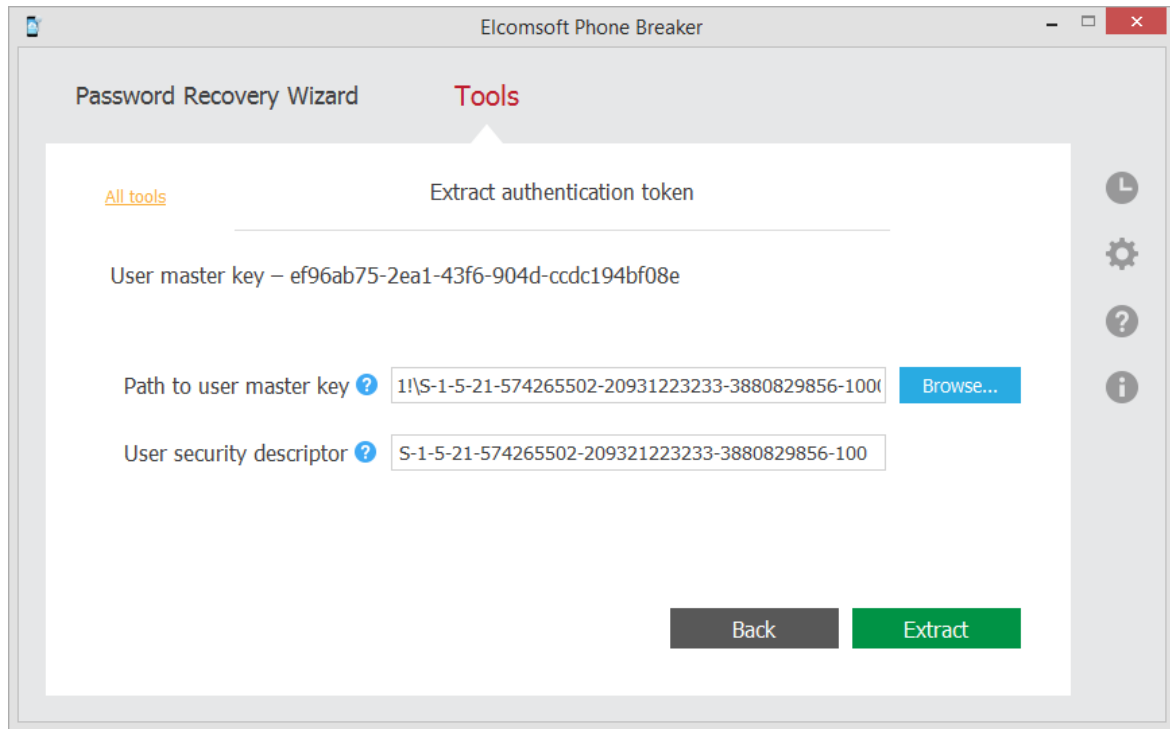
6. Click **Next**.

7. On the following page, define the path to user master key file and its SID. The user master key itself is displayed on top. This key is used to decrypt the authentication token.

- **Path to user master key:** Enter the path to the folder with user master key file. By default the master key is stored in %APPDATA%\Roaming\Microsoft\Protect\\ folder.

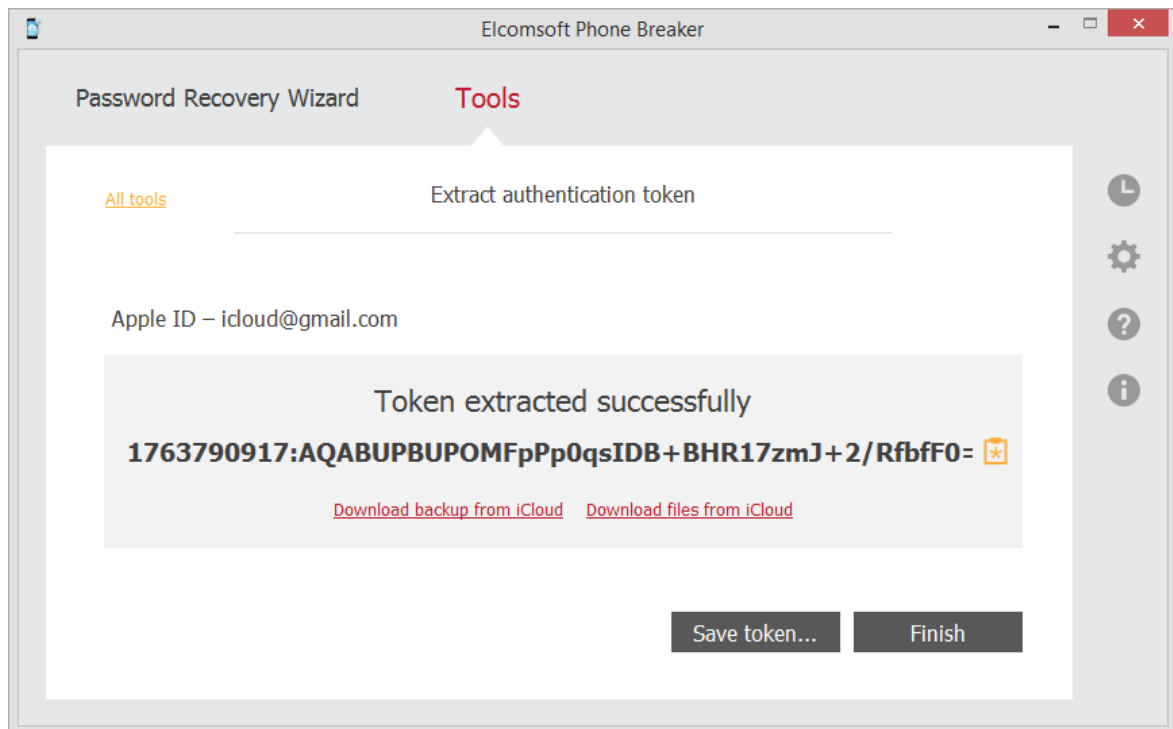
Please note that this folder is usually hidden, so you need to uncheck the **Hide protected operating system files (Recommended)** check box in the Windows Control Panel -> Folder Options -> View.

- **User security descriptor:** The user security descriptor is usually the name of the folder containing the user master key, and it is pre-filled by default.



8. Click **Extract**.

9. The authentication token is extracted.



Click **Save token** to save the extracted string to a text file.

You can now use this token to log into iCloud and download [backup from iCloud](#) or download [files from iCloud](#).

3.6.3 Extracting token on OS X

3.6.3.1 Extracting token on live OS X

You can sign in to iCloud account to download data stored there using the iCloud Authentication token.

To get an Authentication token to iCloud, you will need an Elcomsoft Apple Token Extractor for OS X. This tool is shipped together with EPB (**atex.dmg** file). You can find it in EPB installation folder.

Elcomsoft Apple Token Extractor supports OS X versions up to 10.10.

EPB allows you to extract authentication tokens for:

- Current iCloud user
- Other iCloud user
- [User of a non-live operating system](#) (e.g., by using disk image mounted to the current computer)

User permissions required for getting authentication token:

Authentication Token For	Permissions Required
iCloud account of the currently logged OS X user	User's permissions are enough
iCloud account of a different OS X user	root permissions are required

To extract the Authentication token for the current iCloud user, do the following:

1. Run the atex.dmg file.
2. Copy the **atex** file from the mounted image to the folder where you want the file with authentication token to be saved.
3. Go to the directory where you saved the **atex** file.
4. Launch the **atex** file. The file "**icloud_token_<timestamp>.plist**" will be created in the **Users/ <current user name>** directory.

You will see the full path to the created file in the opened Terminal window.

5. The created "**icloud_token_<timestamp>.plist**" file contains the Authentication token of the current iCloud user.

To extract the Authentication token for a different iCloud user, do the following:

1. Run the atex.dmg file.
2. Copy the **atex** file from the mounted image to the folder where you want the file with authentication token to be saved.
3. Open the command-line Terminal.
4. Go to the directory where you saved the **atex** file.
5. To list all iCloud users, use the command **sudo atex -l** or **sudo atex --iCloudUserList**

sudo command is used to get root privileges for running the program.

6. Enter the password of the root user when prompted.
7. The list of all iCloud users will be displayed.
8. To get authentication token, run the command **sudo atex --getTokenOnline -u <username>**
For example: **sudo atex --getTokenOnline -u mary**
9. Enter the password for the selected user when prompted.



10. Click **Allow** when asked to provide access to the confidential information in keychain.



11. The file "**icloud_token_<timestamp>.plist**" will be created in the directory from which **atex** was launched.

You will see the full path to the created file in the opened Terminal window.

12. The created "**icloud_token_<timestamp>.plist**" file contains the Authentication token of the selected iCloud user.



Parameters for running atex in the Terminal:

Parameter	Meaning
-----------	---------

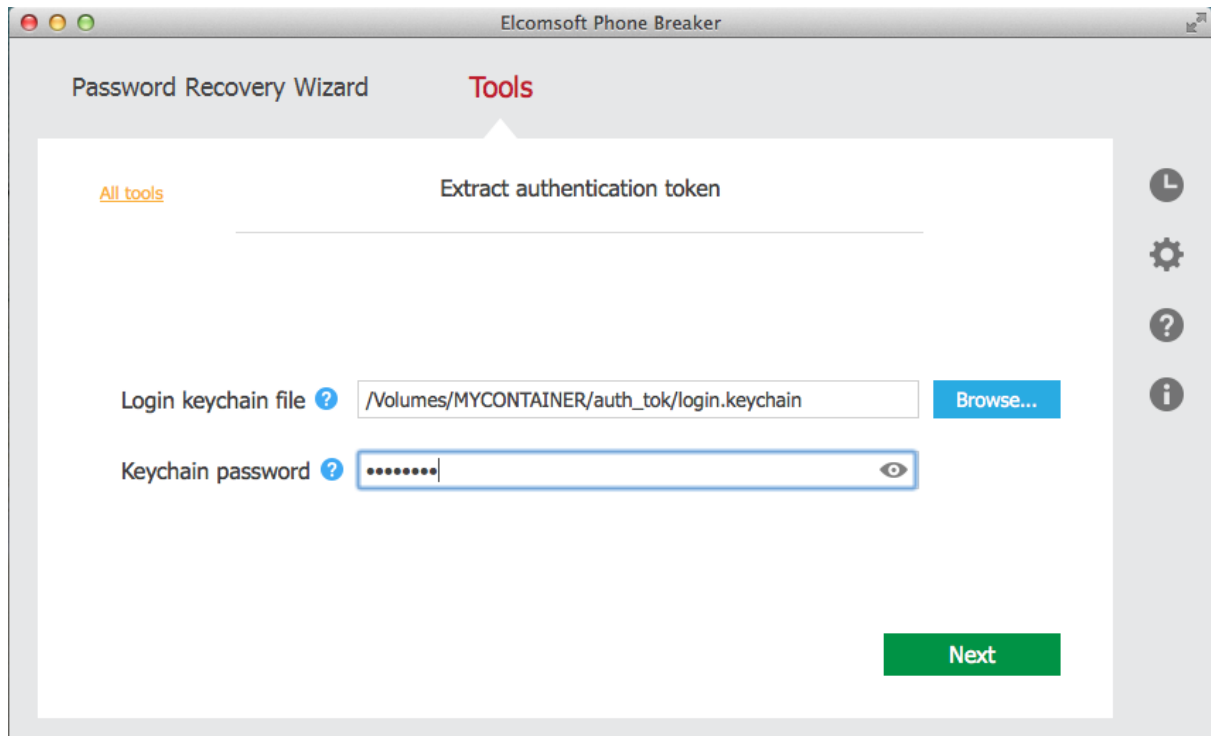
-h or [-help]	Displays help message
-l or [-iCloudUserList]	Displays usernames of iCloud users
--getTokenOnline	Gets authentication token for the user specified in -u parameter.
-u [username]	Indicates a specified user. Username should be entered without brackets.

3.6.3.2 Extracting token on non-live OS X

EPB allows you to extract an authentication token to iCloud from a non-live OS X, e.g., by mounting the disk image of the operating system in which the token is stored.

To extract the authentication token to iCloud, do the following:

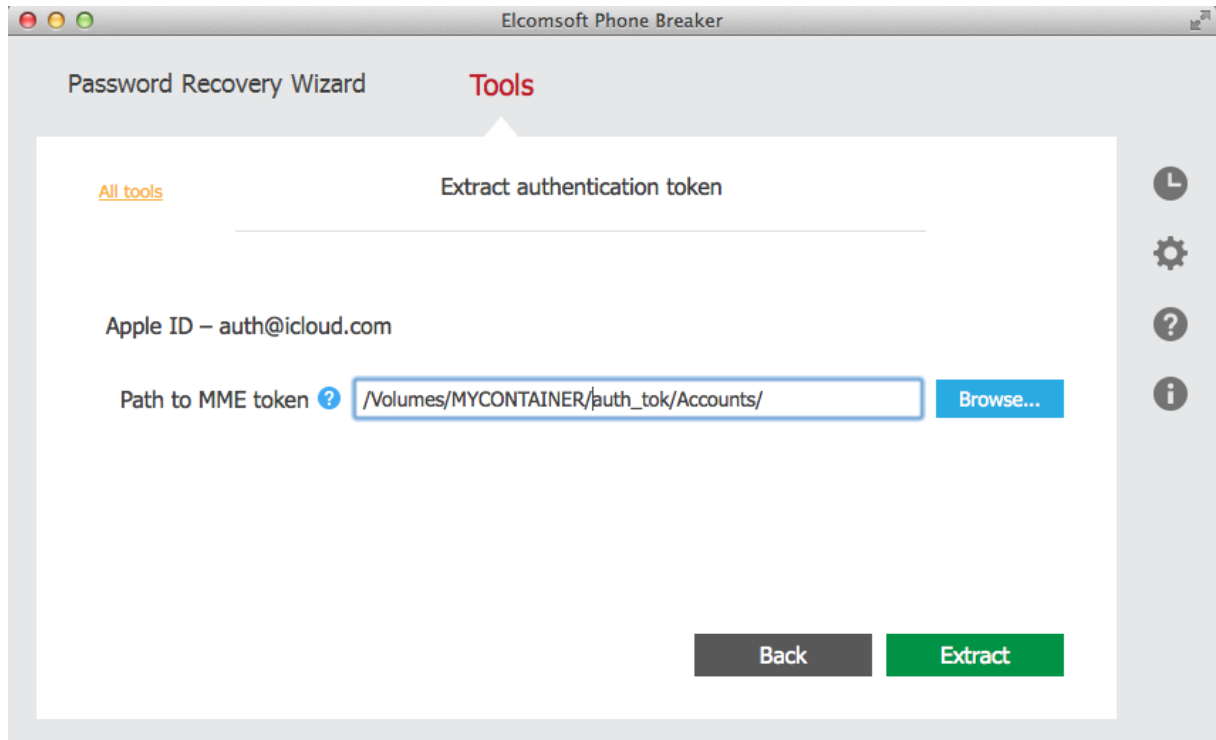
1. Mount the image of the disk containing the authentication token.
2. Run Elcomsoft Phone Breaker.
3. In the **Tools** menu, select the **Apple** tab.
4. Click **Extract authentication token**.
5. Define the path and password to the file containing the authentication token:
 - **Login keychain file:** Enter the path to the login.keychain file that belongs to the user whose token you are decrypting. It is stored in `/Users/<user name>/Library/Keychains/login.keychain` by default.
 - **Keychain password:** The password to a selected login.keychain.



6. Click **Next**.

7. On the following page, define the path to the file containing the authentication token. By default this file is stored on OS X at: */Users/<user name>/Library/Application Support/iCloud/Accounts/*. This file's name is a numerical representation of user's Apple ID in the form of 6-10 digits.

The user's Apple ID is displayed on top.



8. Click **Extract**.

9. The authentication token is extracted.

Click **Save token** to save the extracted string to a *.plist file.

You can now use this token to log into iCloud and download [backup from iCloud](#) or download [files from iCloud](#).

4 Working with BlackBerry data

4.1 Working with BlackBerry Backups

4.1.1 About BlackBerry backups

EPB allows you to decrypt BlackBerry backups created by the [BlackBerry Desktop Software](#)

Backups created by BlackBerry Link (for BlackBerry 10 devices including BBOS 10.3.1.1581) are supported as well, but you need to know the BlackBerry ID password of the user who created the backup.

By default, BlackBerry backups are stored in the following folders:

- **Windows:** My Documents\BlackBerry\Backup.
- **OS X:** /Users/<name>/Documents/BlackBerry Backups.

NOTE: You can change the default location for the backup folder on OS X in the following settings file: `~/Library/Preferences/com.rim.blackberrylink.plist`.

When running EPB on Windows OS, you can [recover the password](#) to the backup before decrypting it.

4.1.2 About BlackBerry Password Keeper and Wallet

BlackBerry users have an option to securely store and quickly access all their passwords and their financial information such as credit card numbers, billing addresses, loyalty points numbers etc. This information is held in [BlackBerry Password Keeper](#) and [Wallet](#) apps, and is securely protected by additional master passwords. Password Keeper and Wallet use separate master passwords. In order to access information stored in these apps, BlackBerry users have to enter the correct master password first. After 10 unsuccessful attempts to guess the master password, all data stored in BlackBerry Password Keeper or Wallet can be permanently erased from the device if a corresponding setting is selected by the user (which is normally the case).

BlackBerry Password Keeper

BlackBerry Password Keeper protects users' passwords with a single master password, offering its users the convenience of having to deal with only one password instead of keeping in mind login credentials to dozens of Web sites, applications and services. BlackBerry users are encouraged to use Password Keeper to generate extremely secure random passwords containing a fairly long sequence of letters, numbers and symbols. All users' passwords are stored securely encrypted, and can be only decrypted with a Password Keeper master password.

Information stored in Password Keeper gets into off-line backups when such backups are produced. However, even when the backup gets decrypted, the users' passwords remain securely protected with an extra password: the Password Keeper master password.

The latest versions of BlackBerry Password Keeper now employ a secure escrow key to protect the password container – and Elcomsoft Phone Breaker can [extract that key](#) and use it to decrypt the protected container instantly and without lengthy attacks.

For older versions of BlackBerry OS (before 10), EPB for Windows can [recover master passwords](#) to the Password Keeper, providing full access to stored information in plain-text by brute-forcing the password.

BlackBerry Wallet

Similar to Password Keeper, BlackBerry Wallet stores users' personal and financial information such as credit card information, billing and shipping addresses, loyalty rewards and membership card numbers. The tool is designed to speed up mobile checkout, significantly simplifying the online purchasing process by filling in the required fields automatically with stored information.

Information stored in BlackBerry Wallet is also encrypted and securely protected with Wallet master password. This password should be, and usually is different from BlackBerry backup password, adding an extra layer of protection to highly sensitive information kept in the Wallet.

EPB for Windows can [recover master passwords](#) to BlackBerry Wallet, providing full access to stored information in plain-text. EPB can try hundreds of thousands passwords per second, making dictionary and brute-force attacks feasible and the recovery time reasonable.

4.1.3 Decrypt BlackBerry backup

If you already know (or have previously [recovered](#)) the password to BlackBerry backup, EPB can decrypt it, so you will be able to open decrypted backup file in other software (we recommend to use Elcomsoft Blackberry Backup Explorer).

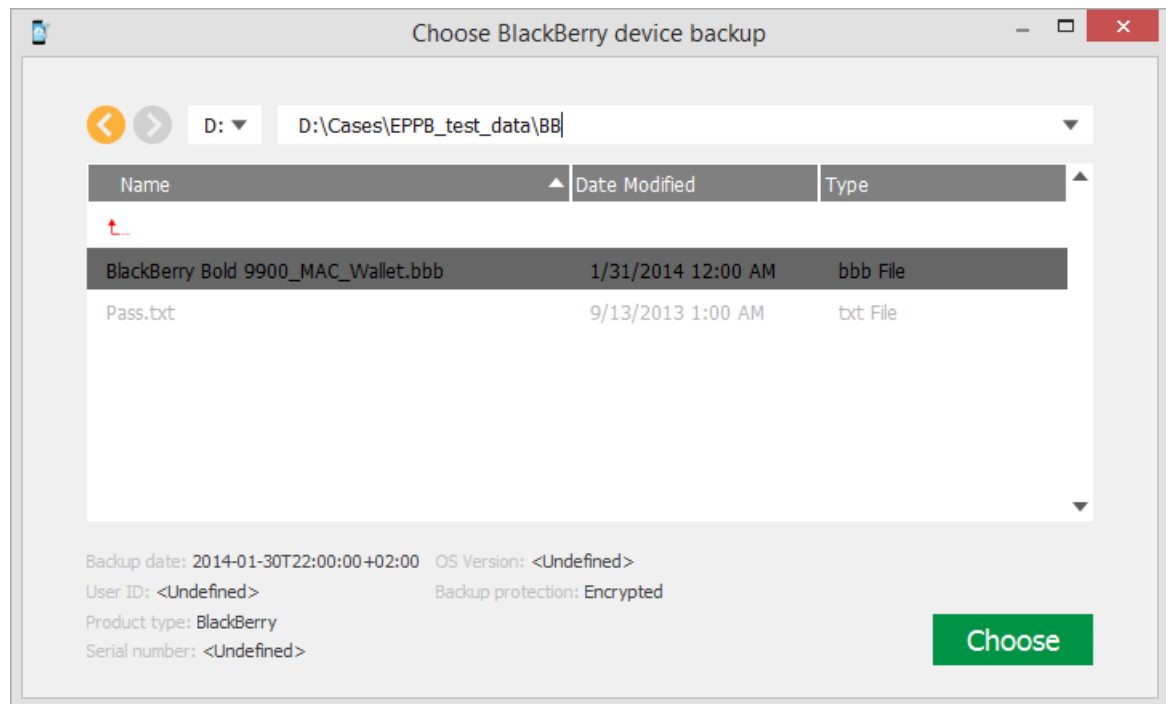
You need a BlackBerry database*.ipd file or backup *.bbb file to decrypt the backup.

Only BlackBerry smartphone backups can be decrypted; backups made from PlayBook devices have different format and are not supported yet, so EPB can only recover the passwords for such files, but cannot decrypt them.

To decrypt a BlackBerry backup, do the following:

1. In the **Tools** menu, select the **BlackBerry** tab.
2. Select **Decrypt backup**.
3. Select either the BlackBerry database file (*.ipd) or BlackBerry backup file (*.bbb) by drag-and-dropping it to the **Decrypt backup** window, or click **Choose backup**.
4. In the opened window navigate to the backup file by entering the file path in the path box. Select the backup file and click **Choose**.

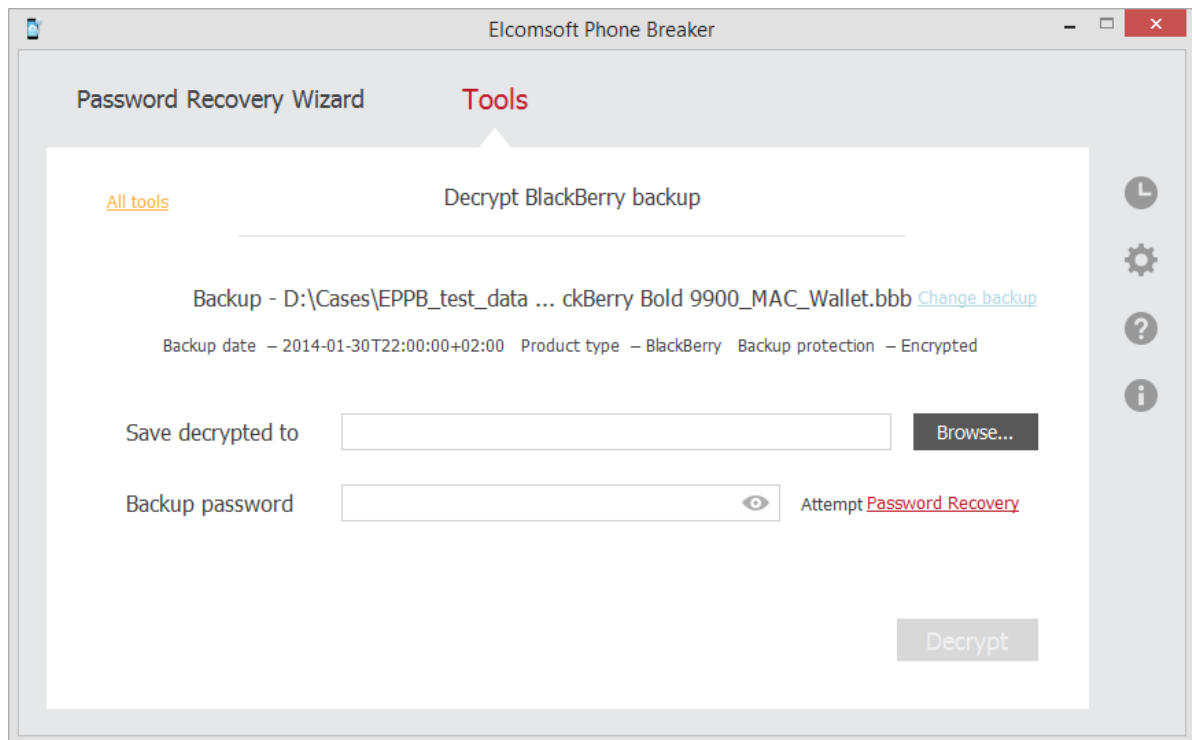
The properties of the backup are displayed below the grid.




5. When the backup is loaded, you can view the following information about backup:

- **Backup date**
- **Product type**

You can select a different backup by clicking **Change backup** next to the backup name.




6. Define the options for backup decryption.

- **Save decrypted to:** Select location for saving decrypted backup.
- **Backup password:** Enter the password for the backup. Toggle the View  button to display the password as characters or in asterisks (*).

If you are using EPB on Windows OS, click **Password Recovery** to [recover the password](#) to the backup.

7. Click **Decrypt**.

8. The decryption process starts.

9. When decryption is finished, you can view the backup in the location on the local computer to which it was saved by clicking the View  button.

10. Click **Finish** to close the **Decrypt backup** page.

4.1.4 Decrypt BlackBerry Link backup

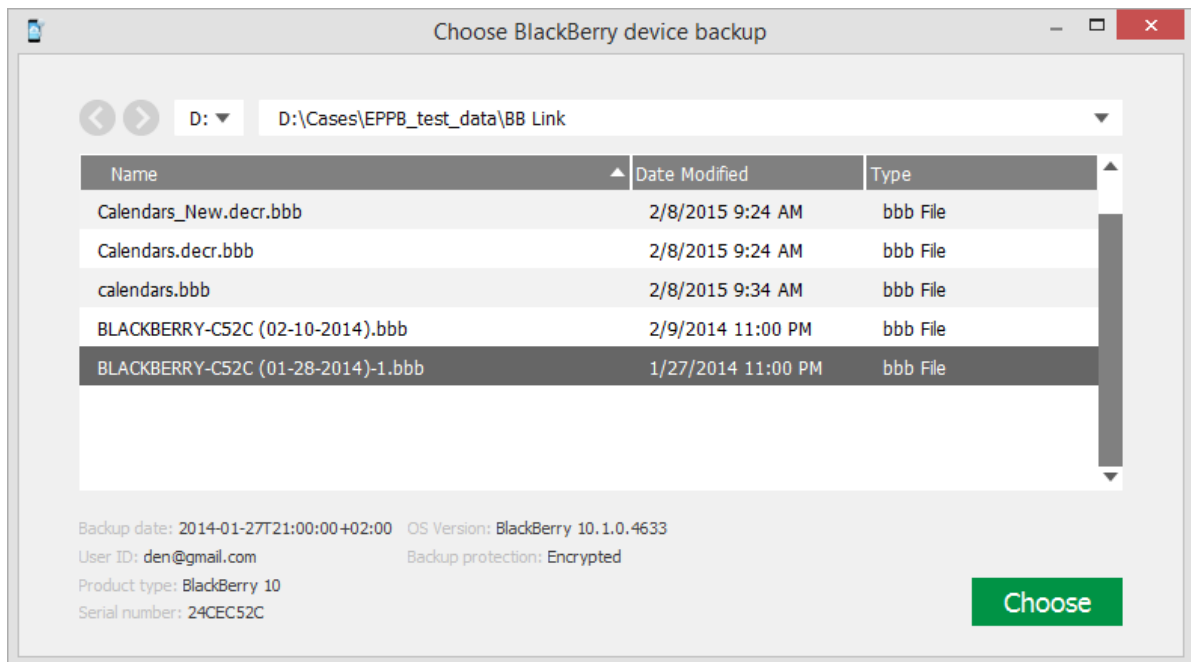
EPB allows you to decrypt the backups for BlackBerry 10 (up to BBOS 10.3.1.1581) devices created by BlackBerry Link.

You need a BlackBerry backup *.bbb file to decrypt the BlackBerry Link backup. You will also need a password to the BlackBerry ID of the user who created the backup.

To decrypt a BlackBerry Link backup, do the following:

1. In the **Tools** menu, select the BlackBerry tab.
2. Select **Decrypt backup**.
3. Select the BlackBerry backup file (*.bbb) by drag-and-dropping it to the **Decrypt backup** window, or click **Choose backup**.
4. In the opened window navigate to the backup file by entering the file path in the path box. Select the *Manifest.plist* file and click **Choose**.

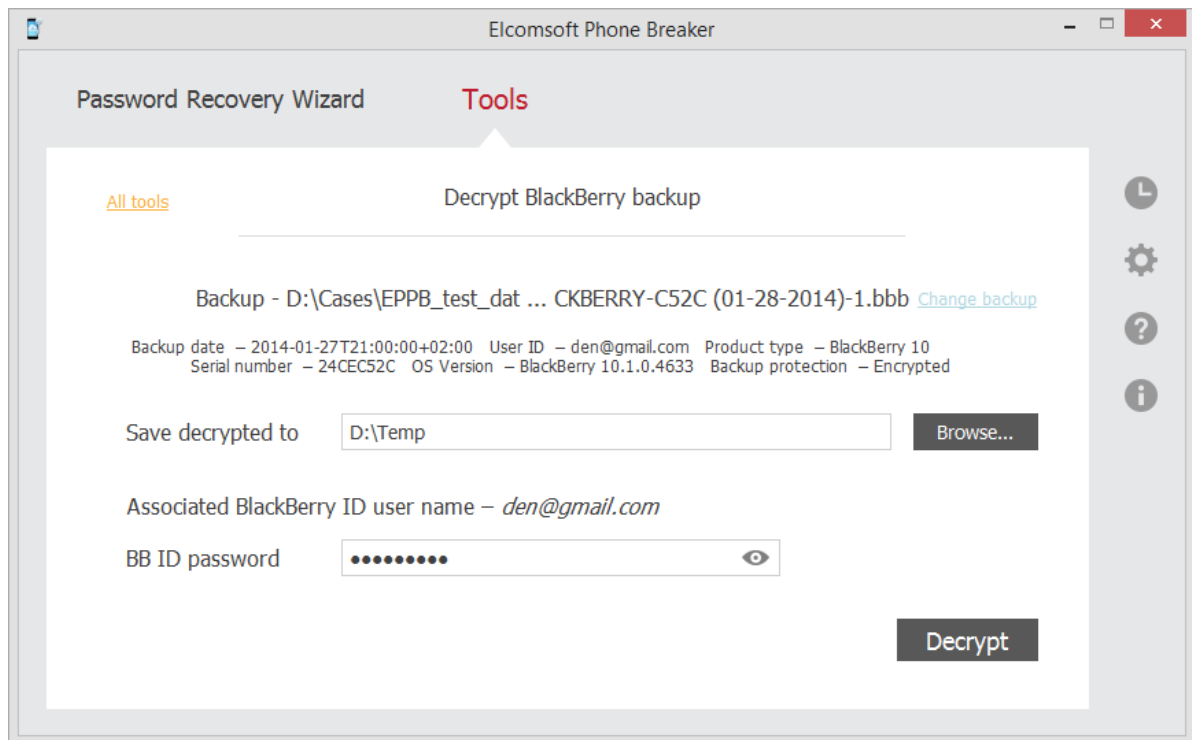
The properties of the backup are displayed below the grid.



5. When the backup is loaded, you can view the following information about backup:


- **Backup date:** The date when the backup was created.
- **Product type:** The type of BlackBerry device that was backed up.
- **PIN:** The ID of the BlackBerry device.

You can select a different backup by clicking **Change backup** next to the backup name.




6. Define the options for backup decryption.

NOTE: The Associated BlackBerry ID user name (the BlackBerry ID (email) of the user who created a backup) is defined automatically.

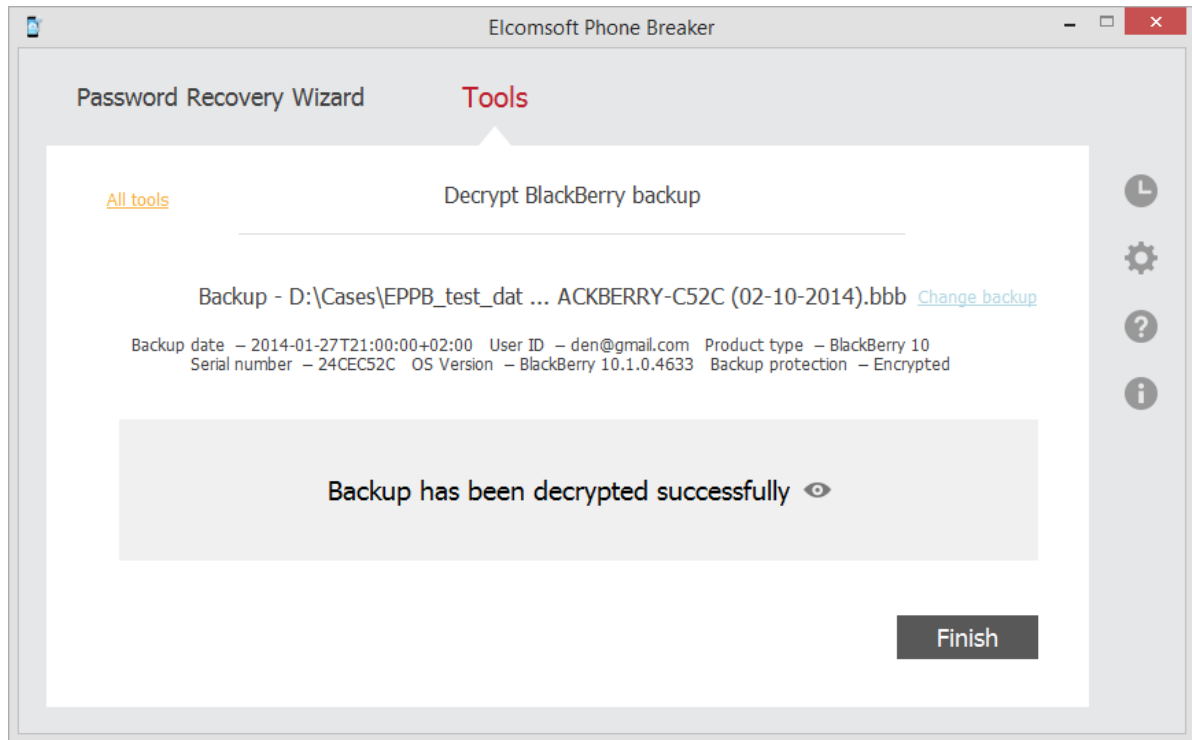
- **Save decrypted to:** Select location for saving decrypted backup.
- **BB ID password:** Enter the password to the BlackBerry ID displayed in italics in **Associated BlackBerry ID user name**. Toggle the View  button to display the password as characters or in asterisks (*).

7. Click **Decrypt**.

8. The decryption process starts.

9. When decryption is finished, you can view the backup in the location on the local computer to which it was saved by clicking the View  button.

NOTE: Decrypting Tar archives stored in BlackBerry backups is not supported in the current version of the program.



10. Click **Finish** to close the **Decrypt backup** window.

4.1.5 Decrypt BlackBerry 10 Password Keeper

EPB can instantly unlock access to passwords stored in BlackBerry Password Keeper for BlackBerry 10. The ability to decrypt the content of this password manager application enables forensic access to some of the most sensitive information stored on BlackBerry device.

Note: BlackBerry 10 backups themselves are also protected and must be decrypted with Elcomsoft Phone Breaker prior to targeting BlackBerry Password Keeper.

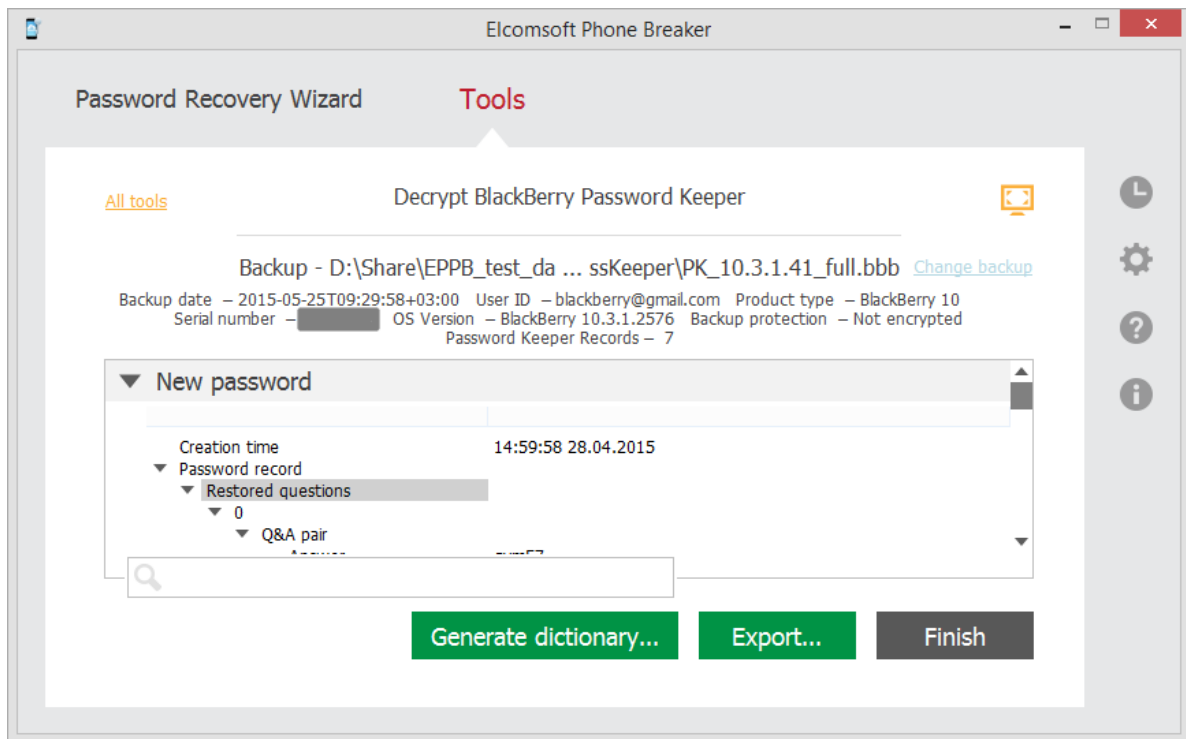
For older versions of BlackBerry OS, [recover the master password](#) to BlackBerry Password Keeper container using EPB for Windows.

To decrypt the BlackBerry 10 Password Keeper, do the following:

1. In the **Tools** menu, select the BlackBerry tab.
2. Select **Decrypt Password Keeper**.
3. Select BlackBerry backup file (*.bbb) by drag-and-dropping it to the window, or click **Choose decrypted backup**.
4. You can view the following information about backup on the **Decrypt BlackBerry Password Keeper** page:
 - Backup date
 - User ID
 - Product type

- Serial number
- OS version
- Backup protection
- Password Keeper Records

The list of records stored in Password Keeper is displayed.



To expand the window and view the information full-screen, click **Expand** .

You can search for the keywords to be found in the Password Keeper data by entering them in the search field and pressing **Enter**.

Click **Generate dictionary** to save the decrypted passwords to a text file for further using as a dictionary for password recovery.

Click **Export** to save all records to an XML file.

4.2 Working with SD card

4.2.1 About BlackBerry device password

Information stored in BlackBerry devices is securely protected with an individual security password (device password). This password is requested every time the device is turned on, or every time after a certain timeout if *Security Timeout* option is selected. If a password is typed incorrectly ten times in a row, all information on the BlackBerry smartphone is wiped clear, leaving no chance of subsequent recovery. This is a security feature, and one of the hallmarks of BlackBerry security model.

BlackBerry smartphones have an option to encrypt the contents of a removable media card, making any information stored on it only accessible to an authorized user. To the contrary of this feature's intent, those opting for extra security may be actually opening a way to recover the device password. A BlackBerry device is not required to perform the recovery. A single file from the removable media card is all that's needed; the password recovery rate is millions passwords per second.

If a user-selectable option to encrypt the contents of a removable media card is selected, **EPB** can analyze information stored on the media card and derive the original device password without the need to use the BlackBerry device itself. Please note that Media Card encryption should be set to either *Security Password* or *Device Password* mode (but not to *Device Key* or *Device Password & Device Key*).

NOTE: Even if *Device Password* or *Device Password & Device Key* option is set on the BlackBerry device, you can still recover device password via EPB (Windows version). But decrypting SD card is only possible when *Device Password* only used for encryption.

For more information on media card encryption, please read [How to encrypt files on an installed media card in the BlackBerry smartphone](#) and [Expectations when encryption is enabled for a media card in a BlackBerry smartphone](#).

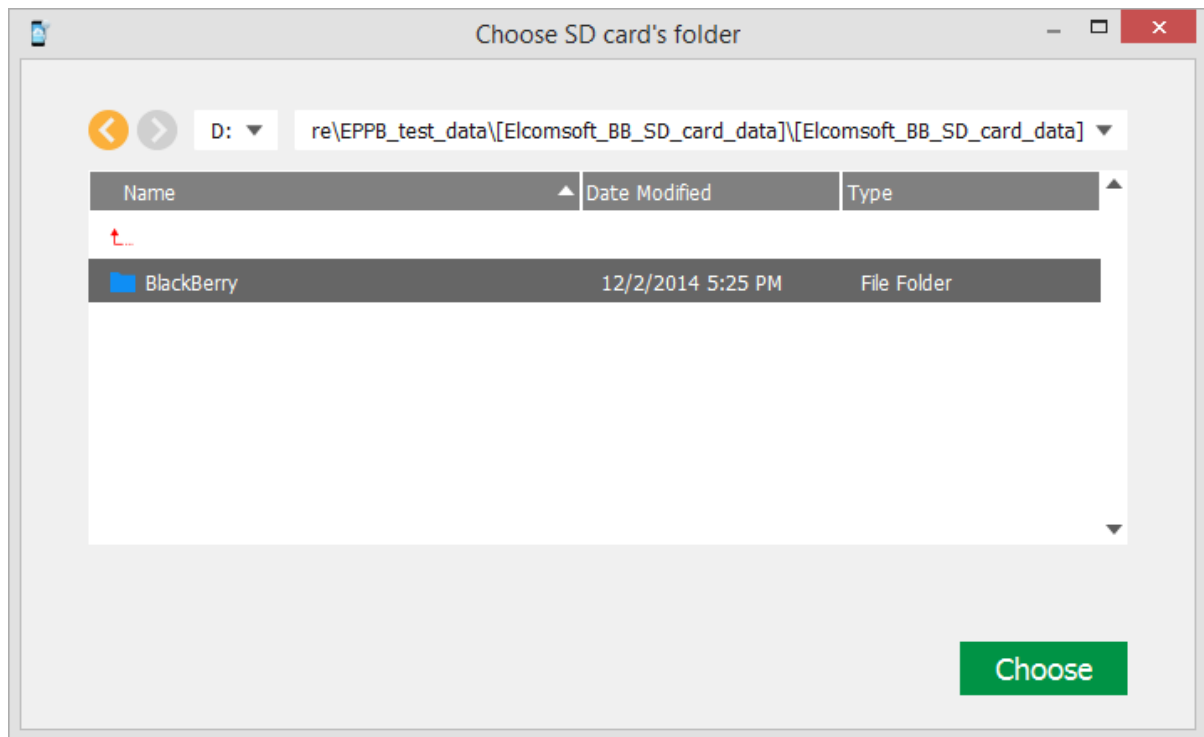
4.2.2 Decrypt BlackBerry SD card


EPB allows you to analyze information stored on the SD (Secure Digital) card for your BlackBerry device and [recover the original device password](#) even if you don't have the device at hand. You will need the *info.mkf* file from SD card for decryption. The *info.mkf* file is usually located in **BlackBerry/system** directory on the media card, and is marked as hidden.

NOTE: Media Card encryption should be set to either **Security Password** or **Device Password** mode (but not to **Device Key** or **Device Password & Device Key**) in the phone settings.

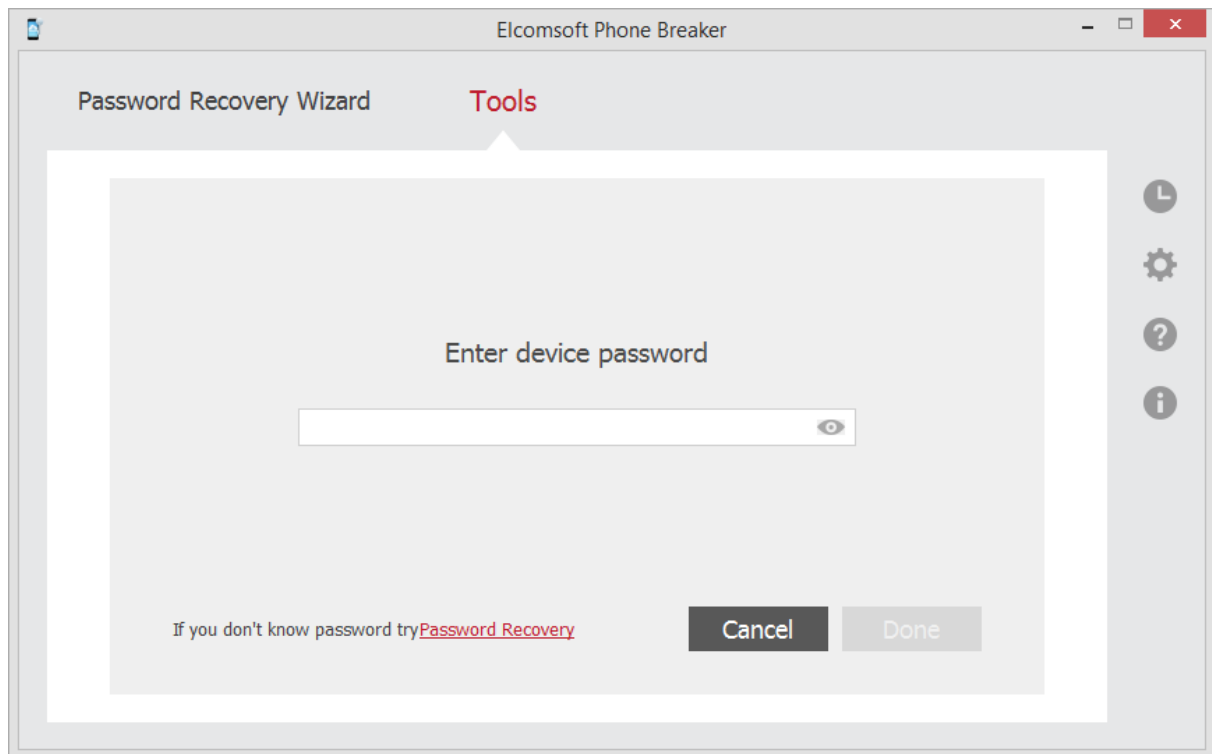
To decrypt the encrypted SD card, do the following:

1. In the **Tools** menu, select the **BlackBerry** tab.
2. Select **Decrypt SD** card.
3. Drag-and-drop the SD card folder to **Decrypt SD Card** page or click **Choose SD card's folder** to navigate to the folder manually. Please select the whole SD card folder, EPB will detect the *info.mkf* file automatically.
4. Click **Choose** to select the file.



5. Enter the password to your BlackBerry device. Toggle the View  button to display the password as characters or in asterisks (*).

If you are using EPB on Windows OS, click **Password Recovery** to [recover the password](#) to the device.



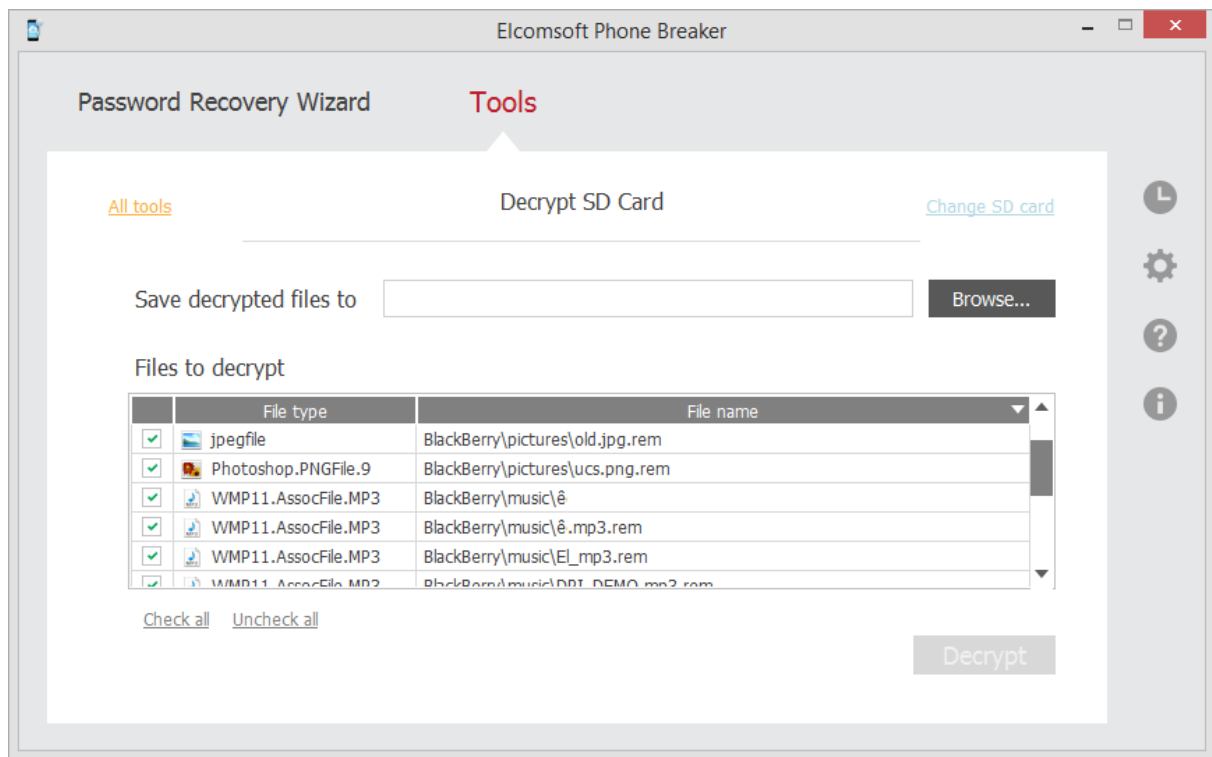
Click **Done** when you have entered the password.

6. The Decrypt SD Card page opens.

Define the location where decrypted files will be saved and select the files that you want to decrypt.


Click **Change SD card** to select a different SD card for decryption.

Use **Check all** and **Uncheck all** options to select or deselect all items in the list.



7. Click **Decrypt**.

NOTE: The folder where the decrypted files will be saved must be empty.

8. When decryption is finished, you can view the general information about processed files and errors on the final page. You can view the decrypted data from SD card in the location on the local computer to which it was saved by clicking the **View**  button.

9. To view detailed [report](#) about decrypted files and errors that occurred during decryption, click **Details**.

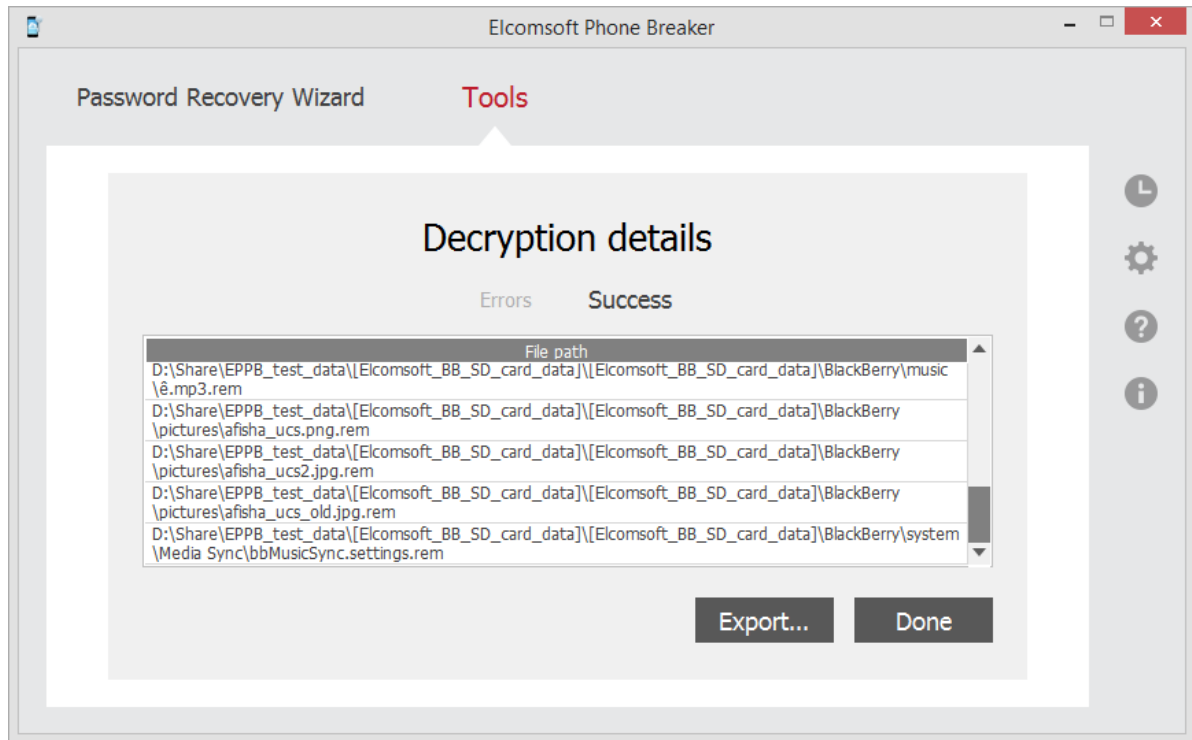
10. Click **Finish** to close the **Decrypt SD Card** page.

4.2.3 SD Card Decryption report

Decryption details report allows you to view detailed information about decrypted files and errors that occurred during decryption of BlackBerry SD card.

To open Decryption details report, do the following:

1. After SD card decryption is finished, click **Details**.
2. The **Decryption details** report opens.



You can view the full path to the saved decrypted files in **Success** tab.

The information about the errors received during decryption is displayed in the **Errors** tab.

To export the **Decryption details** report to a text file or an XML document, click **Export**.

To exit the **Decryption details** report, click **Done**.

5 Working with Windows Phone data

5.1 About Windows Phone data

You can back up the data in your Windows Phone to the cloud when you sign in with your Microsoft account on Windows Phone. For detailed information about creating Windows Phone backups, please see <http://www.windowsphone.com/en-us/how-to/wp8/basics/back-up-my-stuff>

EPB allows you to download Windows Phone data provided you know credentials to Microsoft account that was used for backing data up.

EPB can access the following data for Windows Phone:

- **Contacts**
- **Notes**
- **SMS Messages**


Downloaded data is saved in an archive containing databases with backed up information and a *Manifest.xml* file containing information about every device from account and file name for every database file.

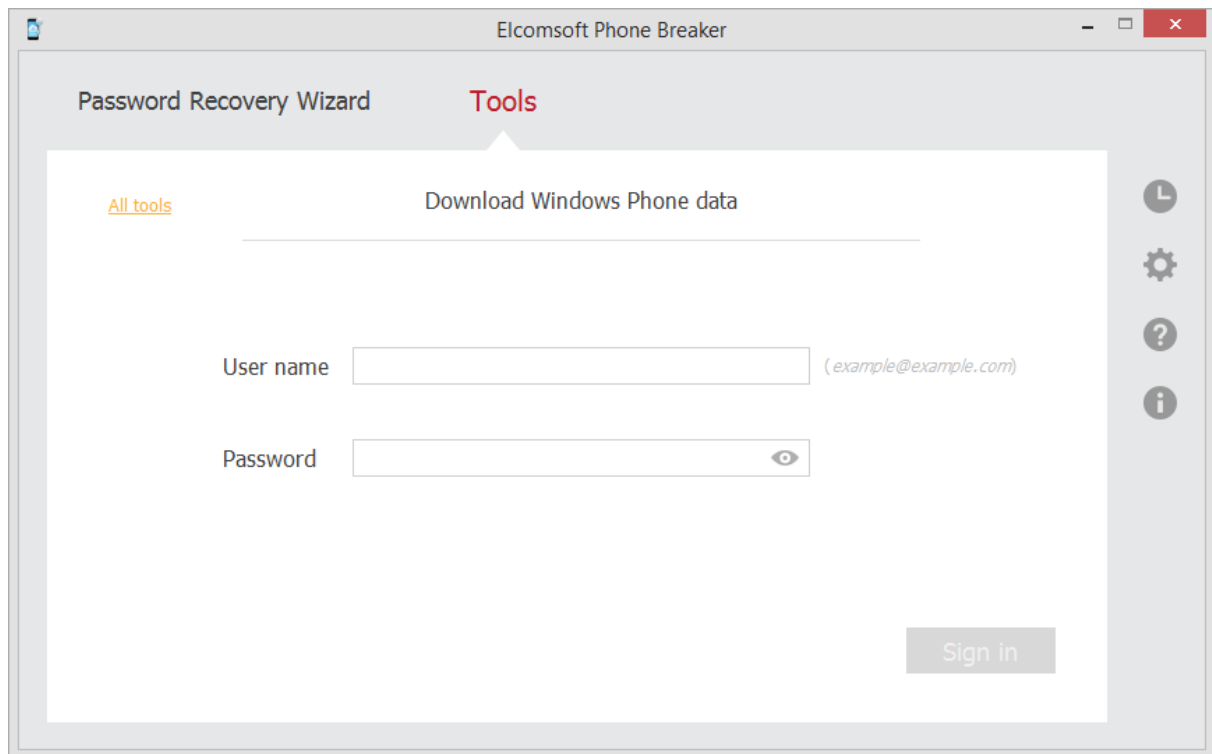
5.2 Downloading Windows Phone data

EPB allows you to download Windows Phone data backed up in the cloud under user's Microsoft account.

To download Windows Phone data, do the following:

1. In the **Tools** menu, select the **Microsoft** tab, and click **Download Windows Phone data**.
2. Define the user name and password to Microsoft account that was used for backing data up.

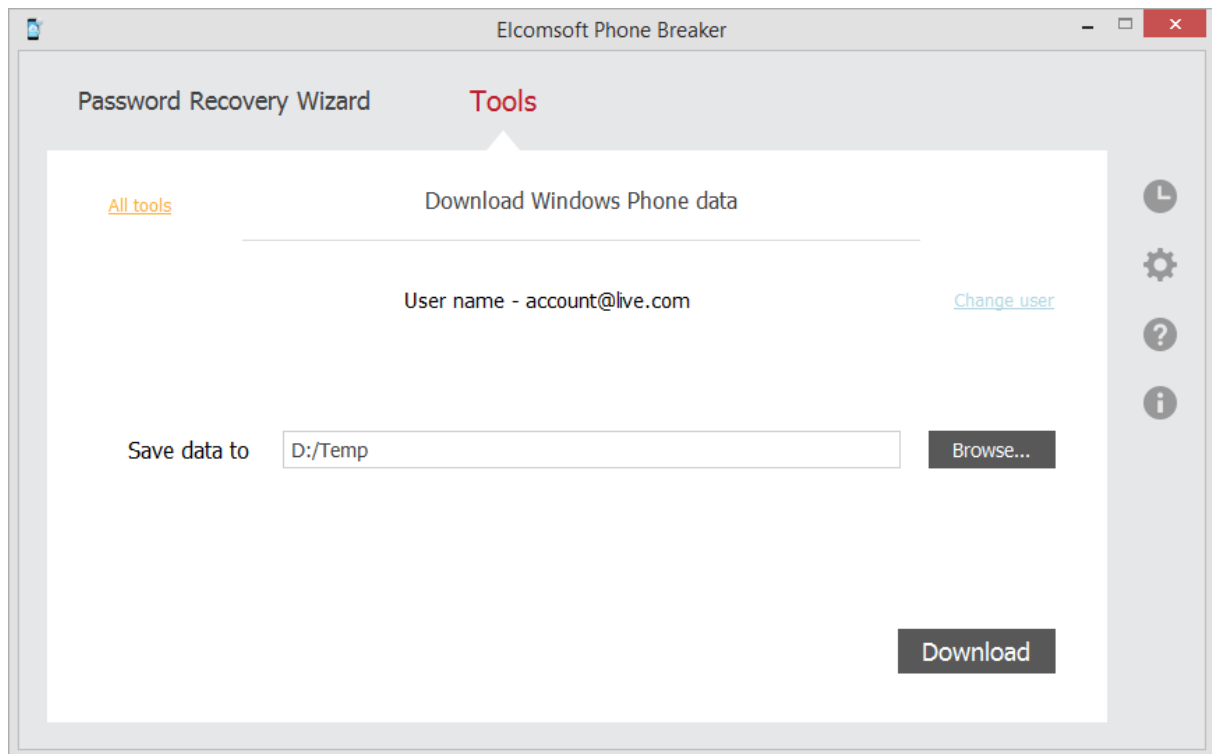
Click the **View**  button to display the password as characters or in asterisks (*).




3. Select location for saving data downloaded from Microsoft account.

You can change the Microsoft user whose backed up data you want to download by clicking **Change user**.

Click **Download** to start downloading backed up data.



4. Data downloading begins. You can view the number of processed files and the number of errors received during decryption.

5. When downloading is finished, you can view the downloaded data in the location on the local computer to which it was saved by clicking the **View**  button.

To view detailed information about decrypted files and errors that occurred during decryption, click **Details**.

6. Click **Finish** to close the **Download Windows Phone data** page.

6 [Windows] Working with 1Password containers

1Password is a popular cross-platform service to keep and synchronize passwords to various accounts between multiple computers and mobile devices. Available for OS X, Windows, Android and iOS, 1Password employs users' Dropbox or iCloudDrive accounts to keep and sync passwords. In iOS, 1Password password databases are also backed up to offline (iTunes) or iCloud backups.

1Password containers are protected with a user-defined master password. Elcomsoft Phone Breaker for Windows OS can [attack master passwords](#) protecting 1Password containers retrieved from the following storages:

- Unencrypted iTunes backups
- iTunes backups decrypted with the help of EPB
- iCloud backups
- encryptionKeys.js files. They are stored inside the *.agilekeychain bundle that can be found in the following locations:
 - If you use Dropbox to synchronize 1Password data, the *.agilekeychain bundle is located in your Dropbox folder. By default it's *C:\Users\\Documents\Dropbox\...\1Password.agilekeychain*.
 - If you don't use Dropbox with 1Password, the keychain is created in *C:\Users\\Documents\1Password\1Password.agilekeychain* by default.

7 [Windows] Recovering passwords

7.1 Recovering passwords to storages

EPB running on Windows OS allows you to recover the passwords to various storages, such as:

- [iTunes backup](#)
- [BlackBerry backup](#)
- [BlackBerry device](#)
- [1Password containers](#)

The following files are necessary for decrypting different types of storages:

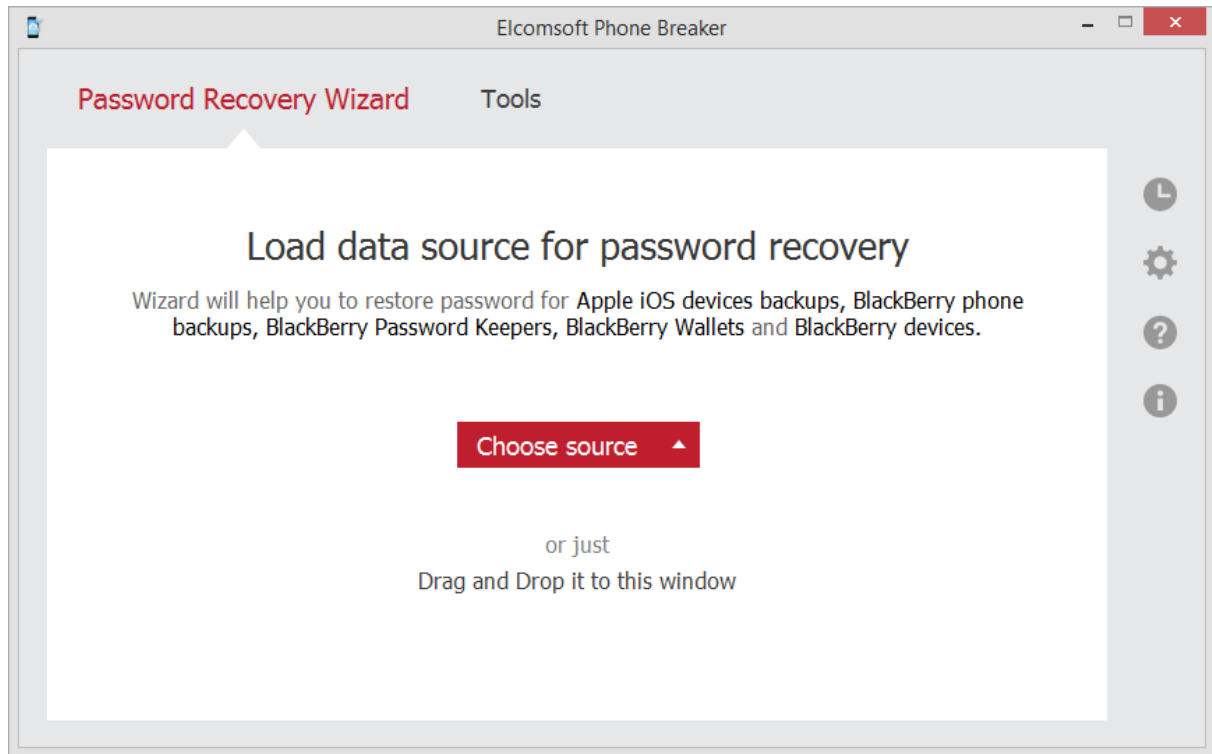
Storage type	Necessary files
iTunes backup	Manifest.plist
BlackBerry device backup	*.ipd or *.bbb backup file
BlackBerry Password Keeper backup	*.ipd or *.bbb backup file
BlackBerry Wallet backup	*.ipd or *.bbb backup file
BlackBerry device password	info.mkf file from the encrypted media card
1Password	Manifest.plist file (iOS backup) or encryptionKeys.js file.

NOTE: You can recover BlackBerry device password even if *Device Password* or *Device Password & Device Key* option is set on the device.

EPB allows you to recover the password by "attacking" the backup or container, so the attack is actually a task that is intended to find the correct password. A combination of attacks makes up a recovery pipeline.

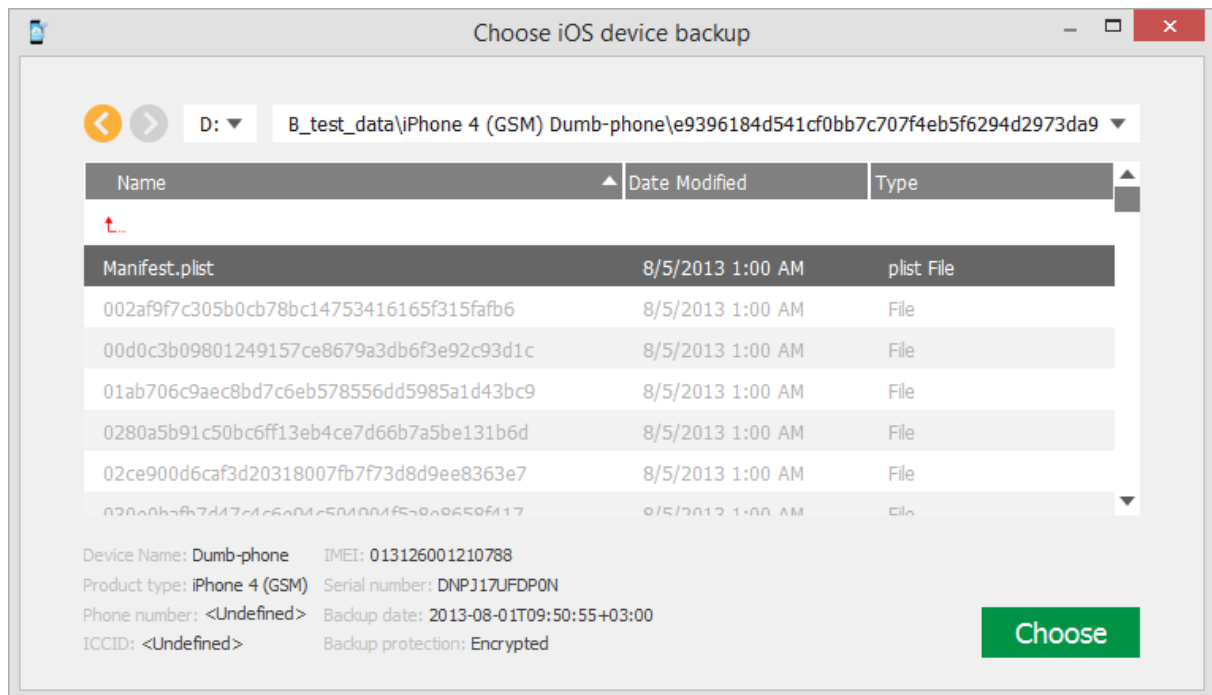
To recover the password, do the following:

1. Run EPB on Windows OS.
2. Open the **Password Recovery Wizard** page.



3. To add the backup or container file, drag and drop it into the Password Recovery Wizard window, or click **Choose source** and select the necessary storage type.
4. In the opened window navigate to the storage file by entering the file path in the path box. Select the necessary file and click **Choose**.

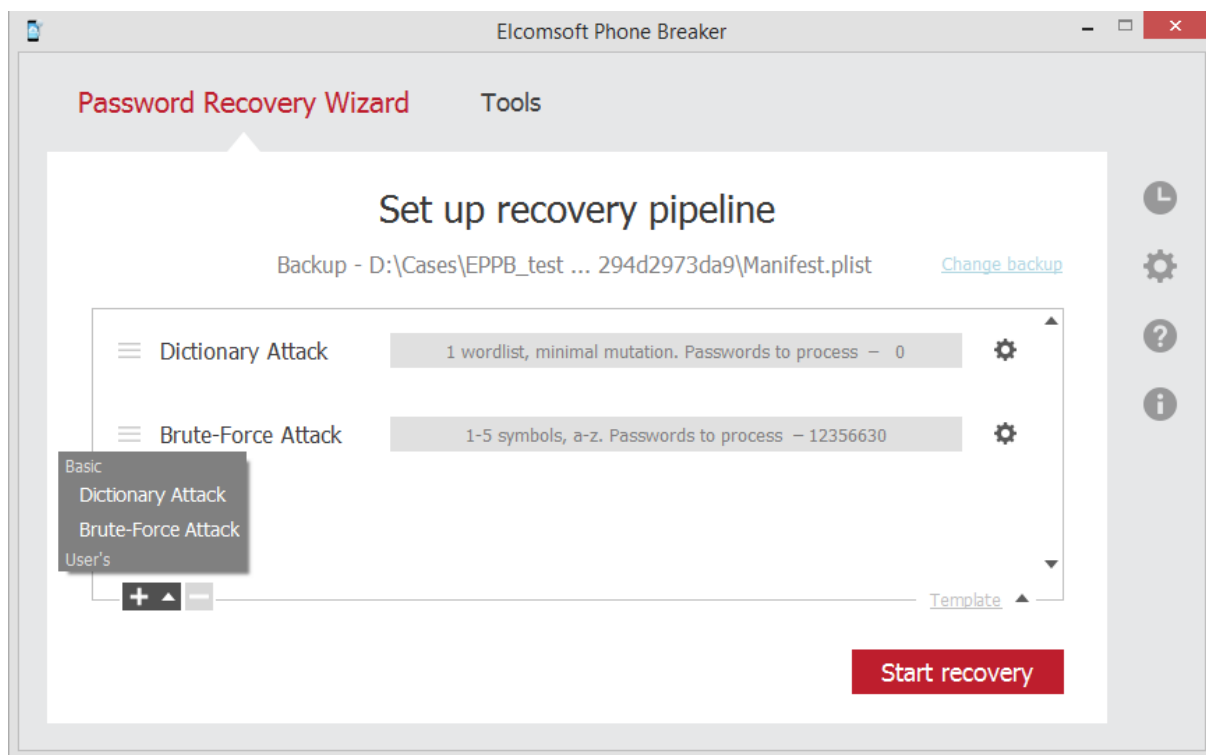
NOTE: The properties of the selected storage are displayed below the grid.



5. When the storage is added, define the attacks that will be used to break the password.

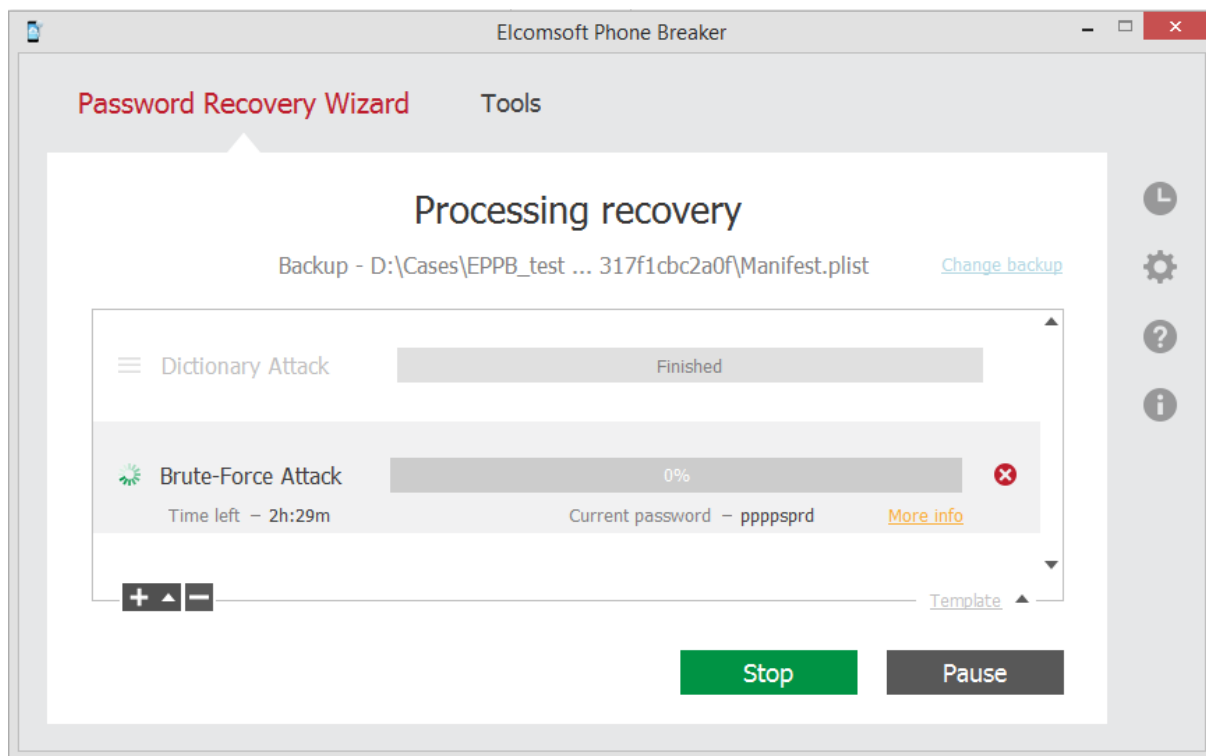
Click the plus “+” sign to add various attacks for breaking the password. By default, Dictionary and Brute-Force attacks are already added. For more information about attacks and their settings, see the [Password recovery attacks](#) topic.

Click **Change backup** to select a different backup for recovery.



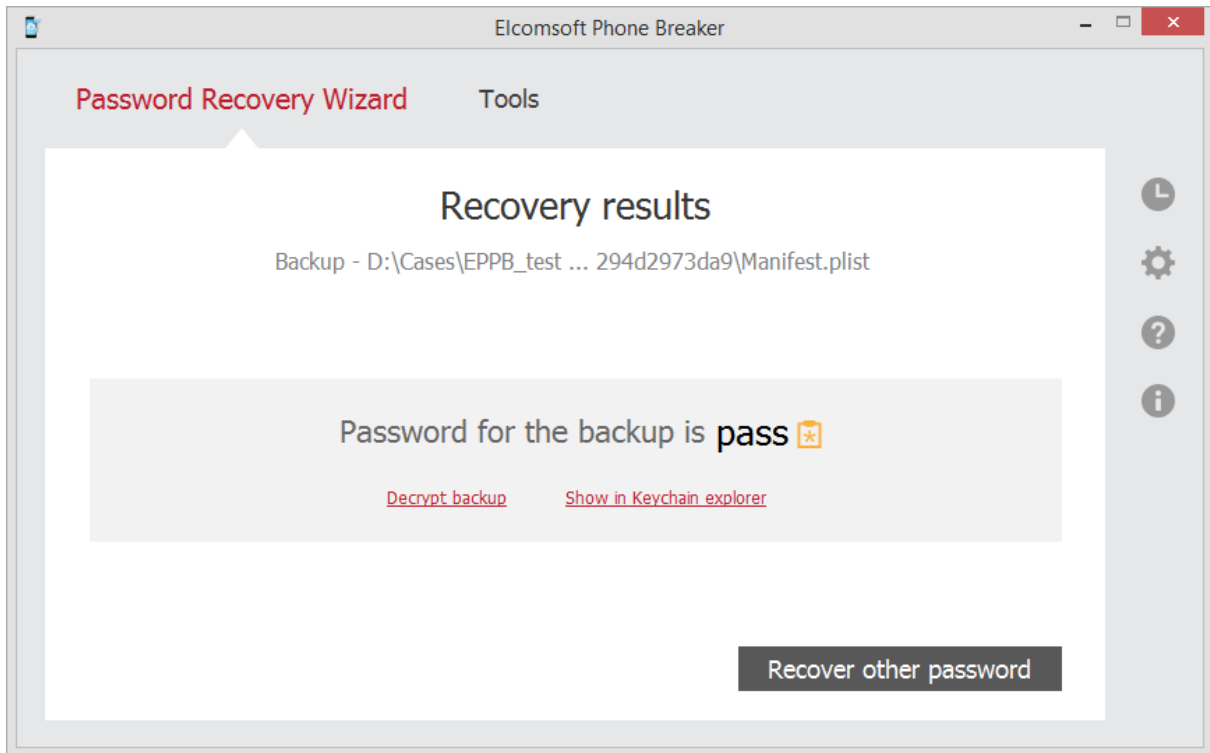
6. Click **Start recovery**.

7. The password recovery starts. You can view the estimated time left and the currently processed word.



Click **More Info** next to the attack to view the average speed of password processing and the number of already processed words.

- When the recovery process is finished, you can view the found password in the **Recovery results** window.



To [decrypt the backup](#) whose password has been restored, click **Decrypt backup**.

To view the information in the Keychain explorer for iTunes backups, click **Show in Keychain explorer**.

To proceed to recover passwords from a different backup, click **Recover other password**.

7.2 Password recovery attacks

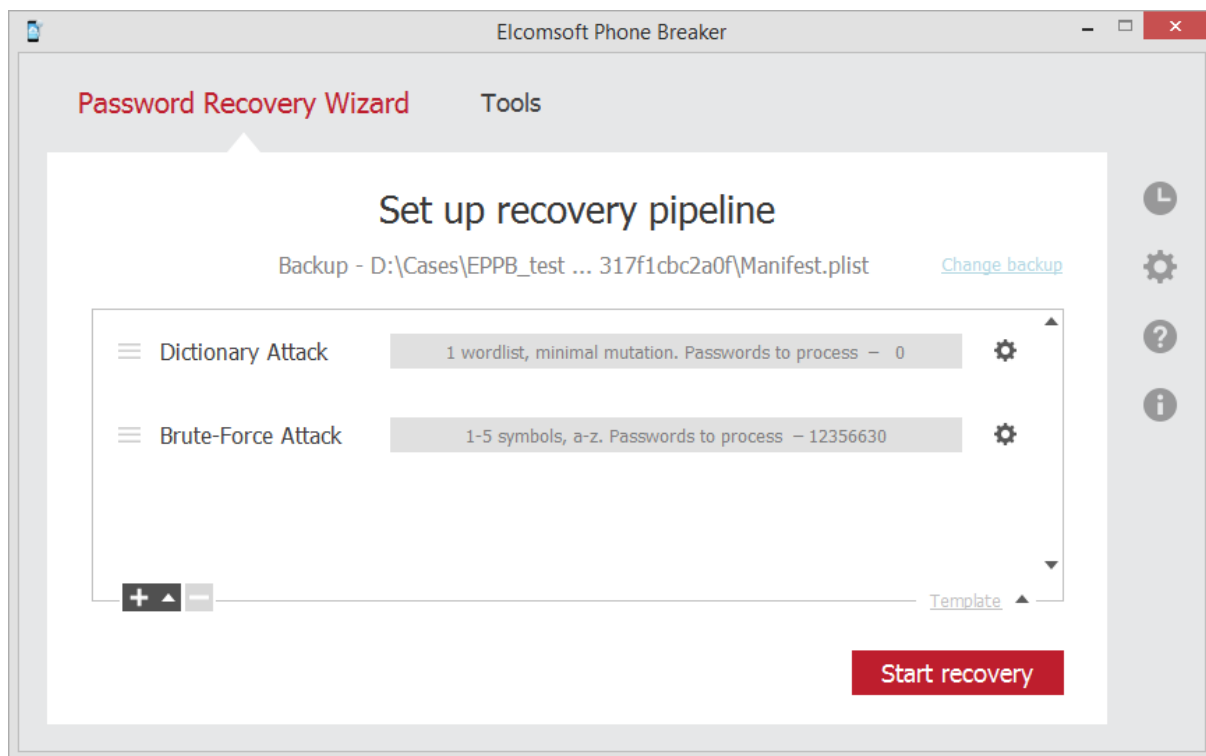
EPB recovers the password to backups and password containers by checking various passwords to see which one matches the backup password. This can be compared to "attacking" the password, so attack is actually a task that is intended to find the correct password. A combination of attacks makes up a recovery pipeline.


NOTE: Recovering passwords is available only when using EPB for Windows OS.

There are two types of attacks available:

- **Dictionary:** The task is based on searching the password in particular dictionaries (the dictionary is a text file, one word per line). You can use third-party password dictionaries, create your own dictionaries, or use the standard one provided by Elcomsoft.

- **Brute-Force:** This type of attack allows checking all passwords in a given range by applying different combinations of symbols to see if they match the necessary password.



You can see the settings of the attack highlighted in grey, including the number of words to be processed during this attack. To change the settings of the attack, click  next to the selected [Dictionary](#) or [Brute-Force](#) attack.

The tasks are checked in the order they are listed, so you can create several tasks with increasing level of difficulty. For example, you can check simple combinations first, then the medium ones, and only after that difficult combinations, to save time if there is high likelihood that a simple password was used.

Additionally, you can use [templates](#) to save selected attacks or to load already existing attacks from a template.

7.3 Dictionary attack options


EPB allows you to set specific options for [recovering the password](#) to backups and password containers.

NOTE: Recovering passwords is available only when using EPB for Windows OS.

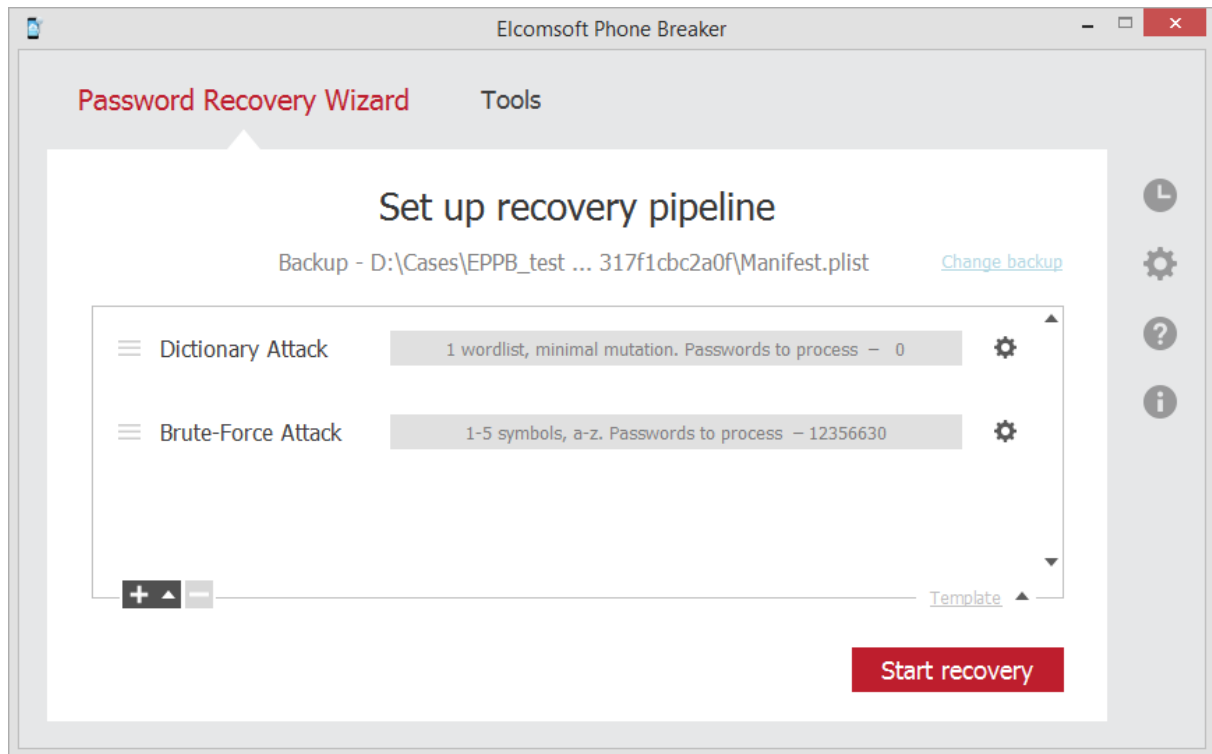
Dictionary attack allows you to check the words in a dictionary to see if they match the required password. The words can be optionally checked with mutations with various levels of difficulty. Mutation means changing the word by certain rules (e.g. using all lowercase or all uppercase letters, changing the order of characters, etc.)

Dictionary is a text file with listing of one word per line. Elcomsoft provides a dictionary for breaking the passwords, but you can create your own dictionary or use a third-party one if necessary.

1. Attack selection

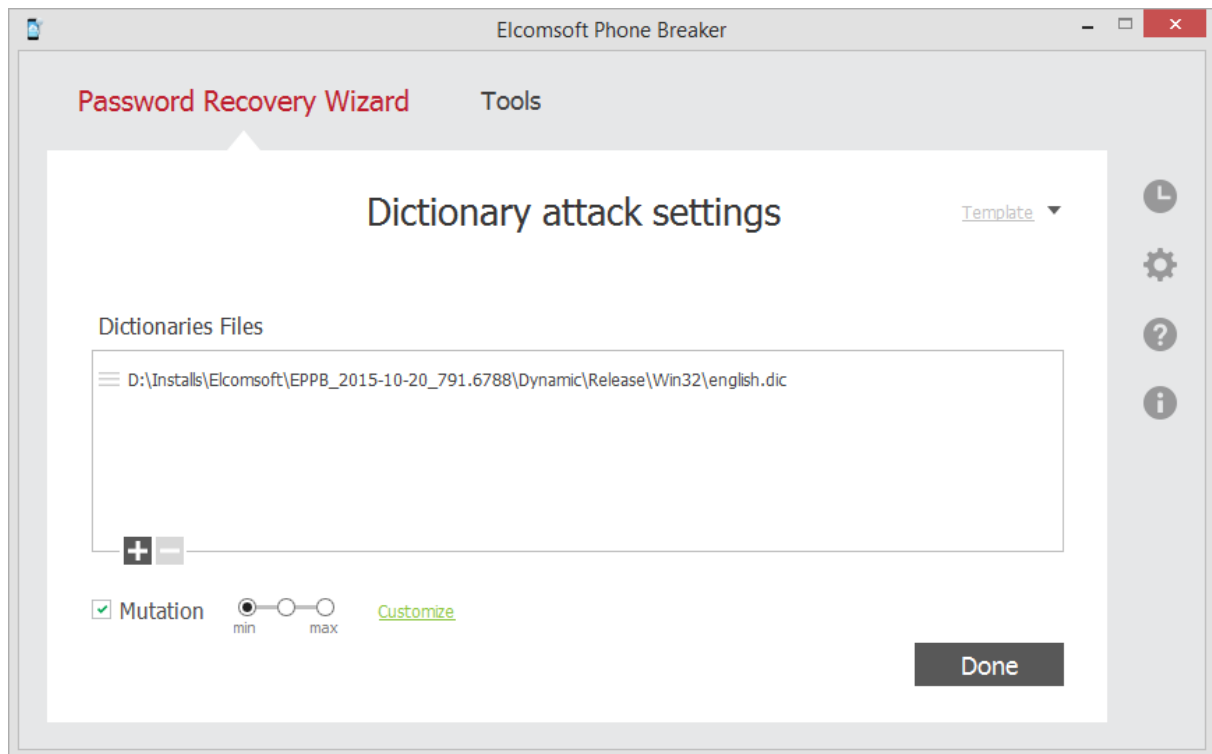
To manage the Dictionary attack settings, [select the backup](#) to be unlocked, double-click the Dictionary attack, or click  next to it.

You can see the settings of the attack highlighted in **grey**, it includes the number of words to be processed during this attack (the number of words is calculated only by the number of dictionaries included in the attack without taking into consideration the levels of included mutations).



2. Defining attack settings

The **Dictionary attack settings** page is displayed:



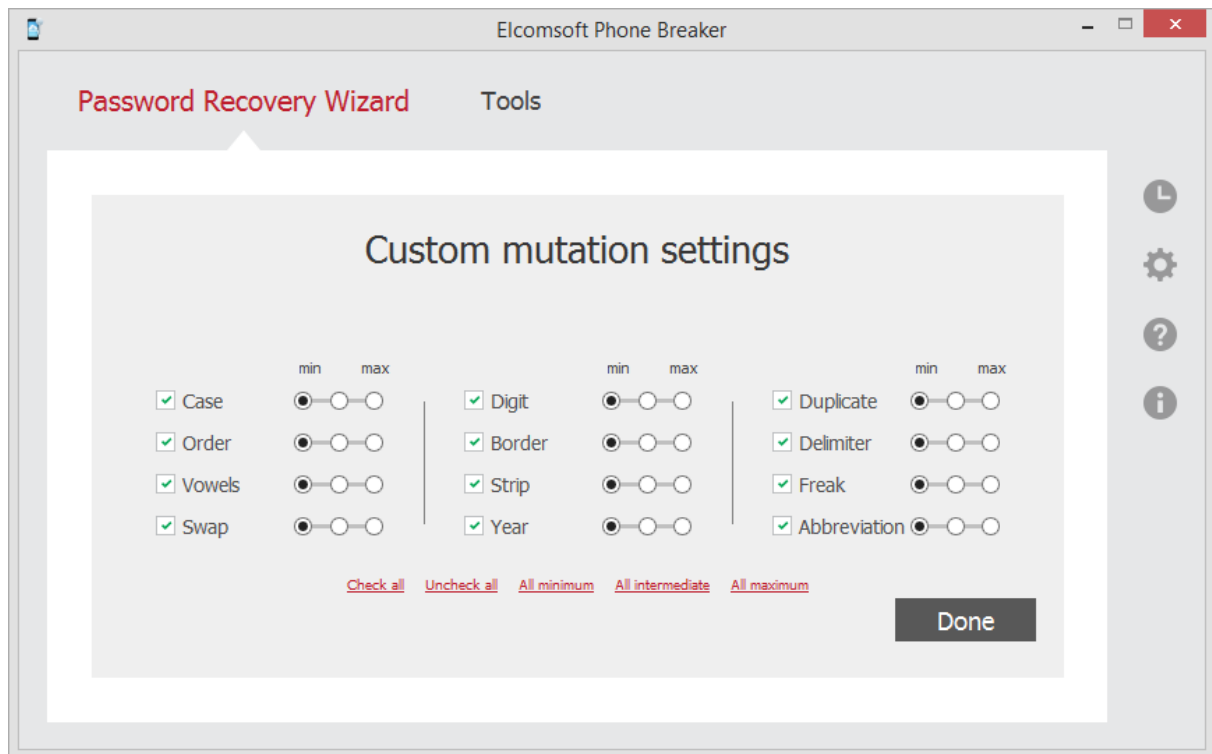
The following options are available:

- **Selection of dictionary.** Click the plus "+" sign to navigate to the dictionary (a text file containing the words in a list) that will be used for breaking the password to the backup. Click the minus "-" sign to remove the dictionary from the list.
- **Mutation.** Selecting this option allows modifying the word in the dictionary list by a set of rules to see if the modified word matches the password. The following general levels of mutation are available:
 - **Minimal:** Program checks only lowercase passwords, and performs basic mutations only: e.g. Border mutation uses not all special characters, but only digits, and only at the end of the password.
 - **Intermediate:** All mutations from the Minimal level together with mutations with the first capital letter.
 - **Maximal:** All mutations from Minimal and Intermediate levels, and checking mutations written in uppercase.

When you define a mutation level, it becomes selected for all mutations. Additionally, you can specify levels of difficulty for each set of mutations by clicking **Customize** next to the mutation check box.

After changing any mutation settings, the **Customize** link will change its name to **Customized** and its color from **green** to **red**.

3. Defining custom mutation settings



All mutations of the words in the dictionary are divided into several 'sets'. You can select the mutation "level" for every set, which allows to select between the speed and efficiency.

You can see examples of the words that will be checked as a result of selected mutation by pointing to a certain level of difficulty.

The following sets of mutations are available:

Mutation Name	Description	Levels	Examples
Case	Allows checking words with lowercase and uppercase letters.	<ul style="list-style-type: none"> Minimal level checks the words in the dictionary written in lowercase, uppercase, and with the first letter written in lowercase and others in uppercase. Intermediate level checks all the combinations from the minimal level and also the first and the last letter of the word written in uppercase. Maximal level checks 	<p><i>password, PASSWORD, pASSWORD.</i></p> <hr/> <p><i>password, PASSWORD, PassworD.</i></p>

Mutation Name	Description	Levels	Examples
		combinations from the previous levels and also combinations with every second letter written in uppercase.	<i>password, PASSWORD, PaSsWoRd.</i>
Order	Reversing the order of letters in the word, repeating the word, adding the reversed word to the original word.	The same as general levels.	<i>password - drowssap passwordpassword, passworddrowssap</i>
Vowels	Removing vowels, or using them in lowercase or uppercase.	The same as general levels.	<i>psswrđ, PaSSWoRD, pAsswOrd</i>
Swap	Changing the order of neighboring characters in the word.	The same as general levels.	<i>apssword, psasword, paswsord</i>
Digit	Adding several digits to the work (from the dictionary) as prefix and suffix.	<ul style="list-style-type: none"> • Minimal level allows adding numbers (0-9) at the end of the word, checking lowercase words, and the words starting from the capital letter. • Intermediate level allows checking words written in uppercase and words with digits in the beginning. • Maximal level allows checking combinations in the range 00 - 99. 	<i>password1, Password1.</i>
			<i>1password, 1PASSWORD.</i>
			<i>11password, PASSWORD99</i>
Border	Similar to the Digit mutation, but adding not only digits, but also most commonly used symbols (e.g., 123, \$\$\$, 666, qwerty, 007,) as prefix and suffix.	The same as general levels.	<i>#password#, \$password\$</i>
Strip	Removing one character from the dictionary word.	The same as general levels.	<i>assword, pssword, password</i>
Year	Adding the year (1900-2050) at the end of the word	The same as general levels.	<i>password1973, password2002</i>
Duplicate	Duplicating the characters in the password.	The same as general levels.	<i>ppassword, paassword, passsword, passsword</i>

Mutation Name	Description	Levels	Examples
Delimiter	Adding delimiters such as . +*-\/#=# between characters.	The same as general levels.	<i>p.a.s.s.w.o.r.d, p+a+s+s+w+o+r+d, p-a-s-s-w-o-r-d</i>
Freak	Replacing some characters in the password with symbols.	The same as general levels.	<i>p@ssword, p@\$s\$word and p@\$s\$w0rd</i>
Abbreviation	Checking some commonly-used abbreviations.	The same as general levels.	<i>ihateyou - ih8you, loveyou - loveu, foryou - 4u.</i>

You can use [templates](#) to save selected attack settings, or to load the attack settings from a template.

Click **Done** when you have finished defining the options.


7.4 Brute-Force attack options

EPB allows you to set specific options for [recovering the password](#) to backups and password containers.

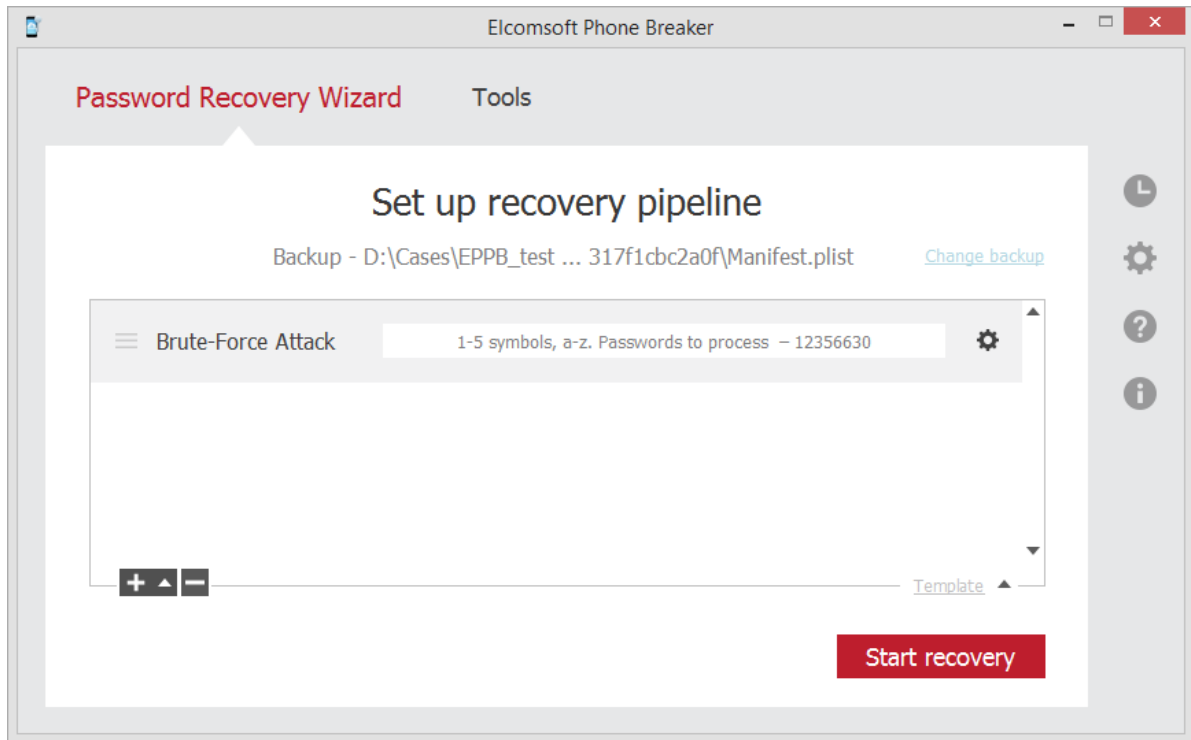
NOTE: Recovering passwords is available only when using EPB for Windows OS.

Brute-force attacks allow checking all combinations of characters within defined limits to see if any of them matches the password.

1. Attack selection

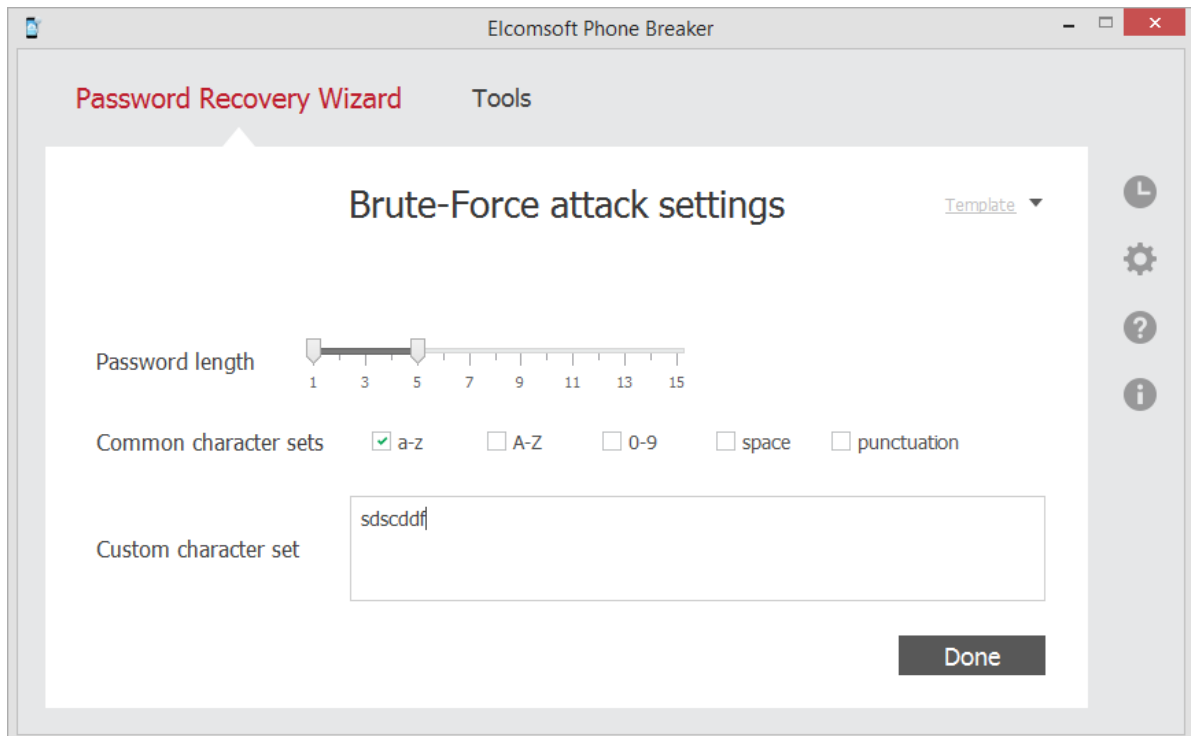
To manage the Brute-Force attack settings, [select the backup](#) to be unlocked, double-click the Brute-Force attack, or click  next to it.

You can see the settings of the attack highlighted in grey, it includes the number of words to be processed during this attack and the characters to be used.



2. Defining attack settings

The **Brute-Force attack settings** page is displayed:



The following options are available:

- **Password length:** You can define the length of the password to be checked, from 1 character to 15. Please note, the longer the password, the longer the check will be performed.
- **Common character sets:** Define the characters that will be checked. The following combinations are available:
 - a-z: Allows checking combinations with lowercase letters.
 - A-Z: Allows checking combinations with uppercase letters.
 - 0-9: Allows checking combinations with numbers from 0 to 9.
 - space: Allows adding a space between characters in the checked password.
 - punctuation: Allows using punctuation marks between characters in the password.
- **Custom character set:** Define a custom set of characters that will be combined when checking the password.

You can use [templates](#) to save selected attack settings, or to load the attack settings from a template.

Click **Done** when you have finished defining the options.

7.5 Templates

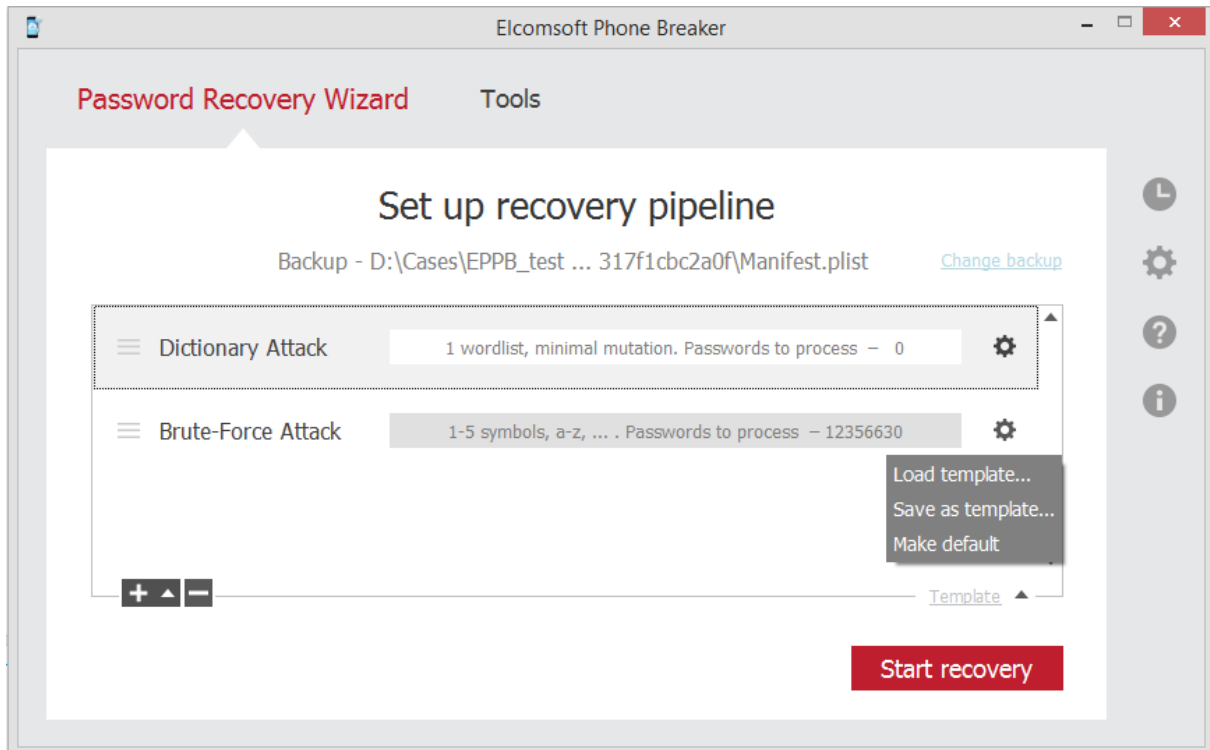
7.5.1 Saving templates

Template is a combination of settings for a pipeline or a separate attack saved in EPB. Templates are created to simplify re-using of certain settings when recovering passwords to several backups.

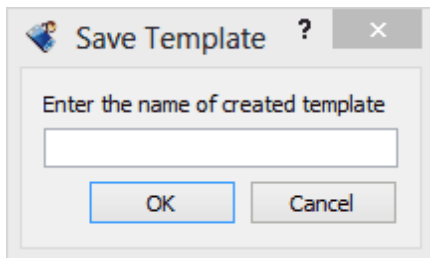
NOTE: Recovering passwords is available only when using EPB for Windows OS.

To save the settings of recovery pipeline to a template, do the following:

1. Start the [password recovery](#).
2. Select **Template - Save as template** on the **Set up recovery pipeline** page. To create a default template that will be displayed first every time the **Password recovery** option is used, select **Make default**.



3. In the **Save Template** window, define the name of the template, and click OK.



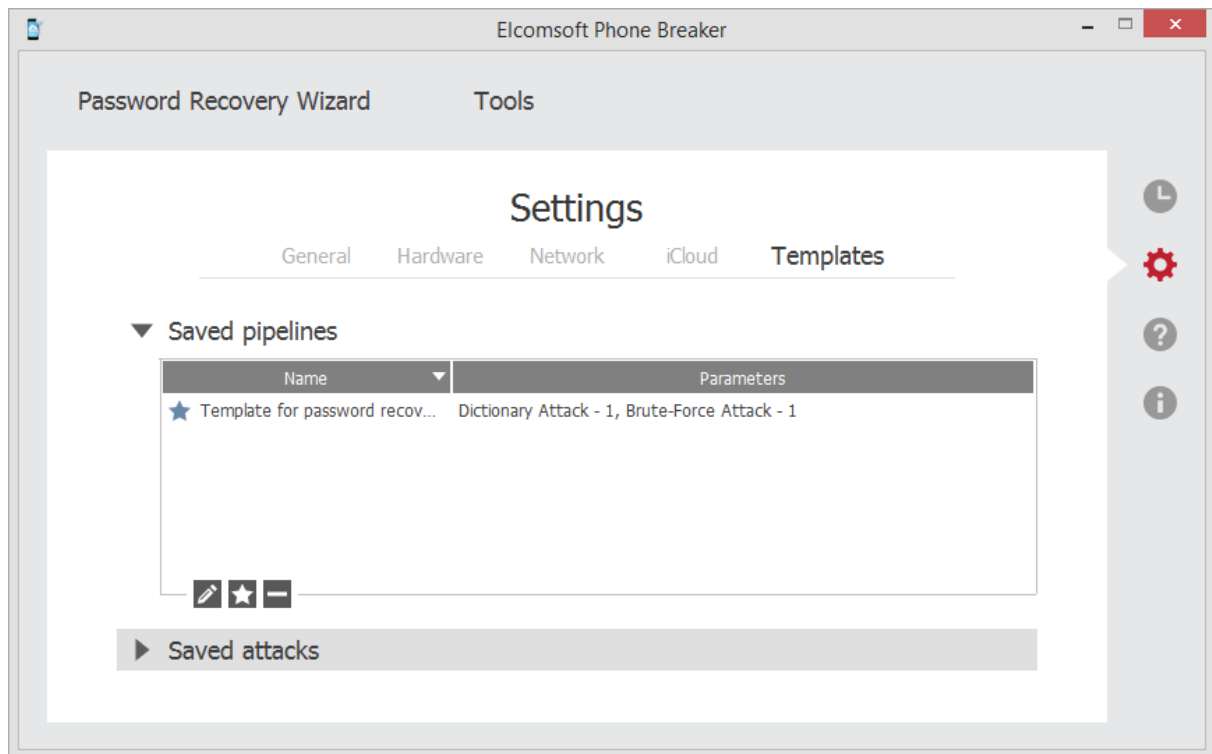
4. The template is saved. Now you can load the template from the template database when you recover a different password.

To [view the saved template](#), go to **Settings -> Templates**.


Additionally, you can save the settings of a [separate attack](#) to a template.


7.5.2 Viewing templates

To view and manage already [saved templates](#), go to **Settings -> Templates**.



The information about templates of pipelines (a combination of attacks) can be viewed in the **Saved pipelines** section. The information about individual attacks is displayed in the **Saved attacks** section.

To edit the template name, select a template and click the **Edit**  button.

To set the template as default, click the  button. Default template will be displayed first when selecting the template for loading.

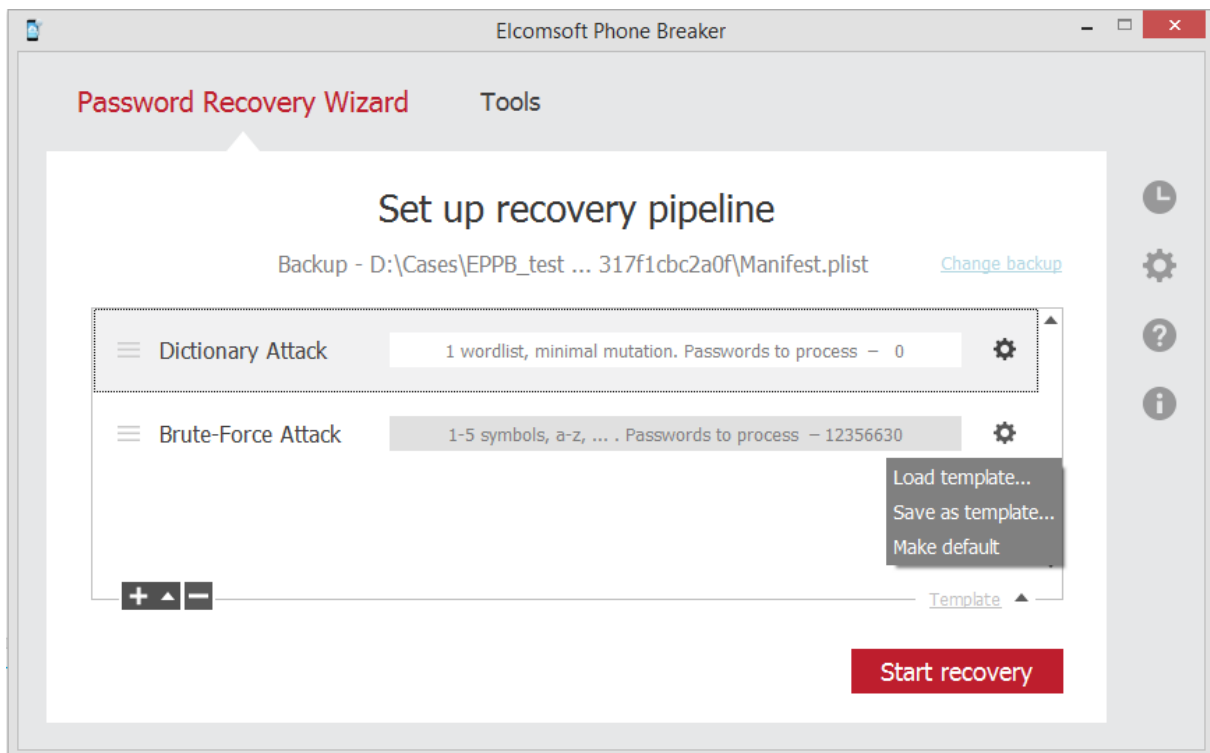
To delete a template, select a template, and click the **Delete**  button.

7.5.3 Loading templates

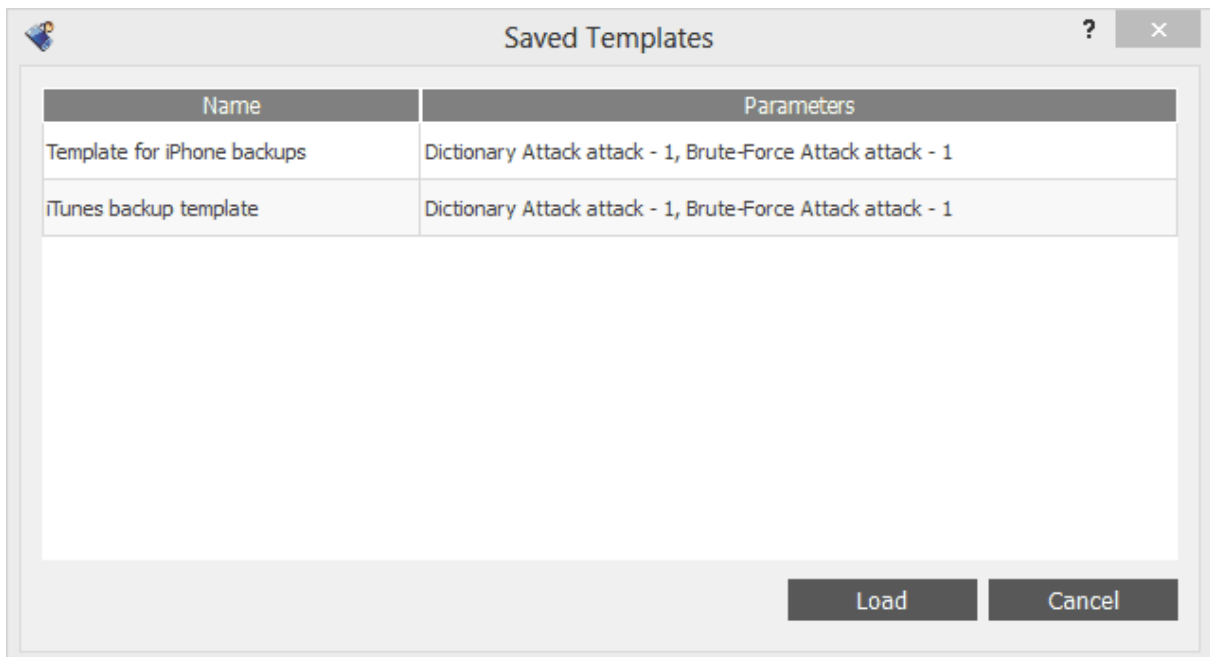
Template is a combination of attack settings saved in EPB. Templates are created to simplify re-using of certain settings when recovering passwords to several backups.

To load the settings of recovery pipeline from a template, do the following:

1. Start the [password recovery](#).
2. Select **Template - Load template** on the **Set up recovery pipeline** page.



3. Select the template you need and click **Load**.




4. The template is loaded in the **Set up recovery pipeline** window.

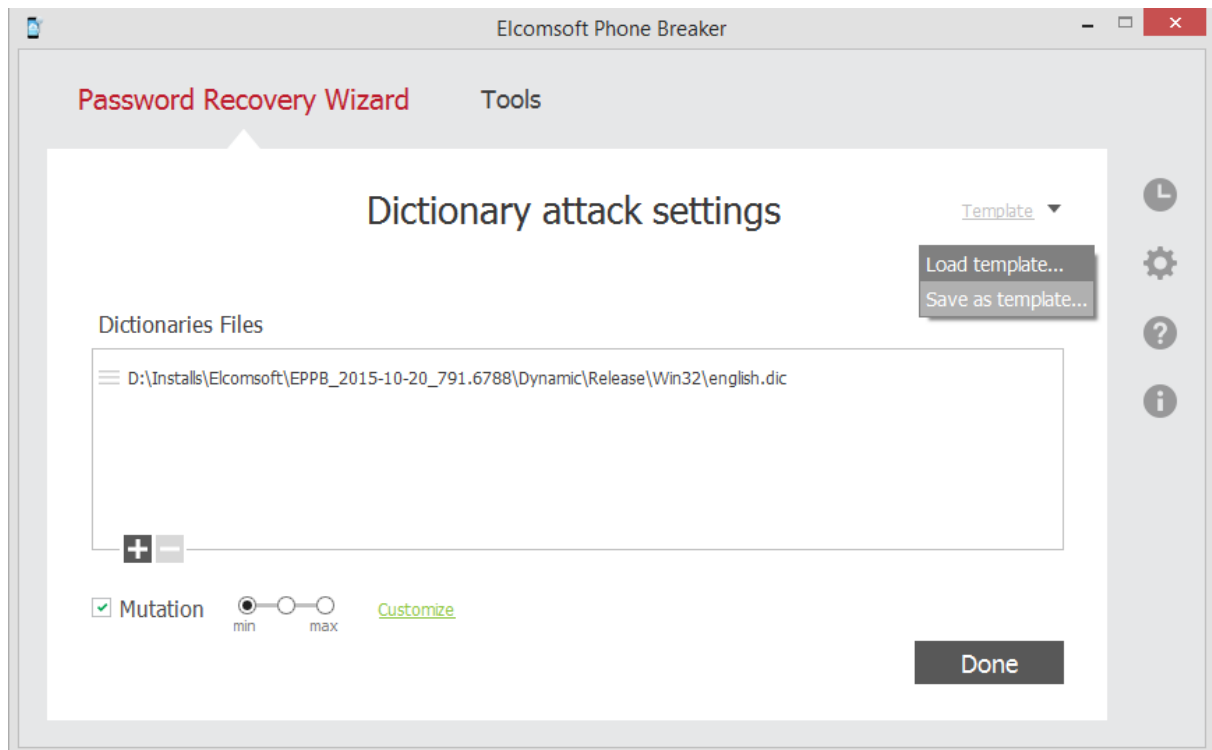
7.5.4 Using templates for attacks

Apart from saving the whole [recovery pipeline](#) to a template, you can save the settings of an individual attack.

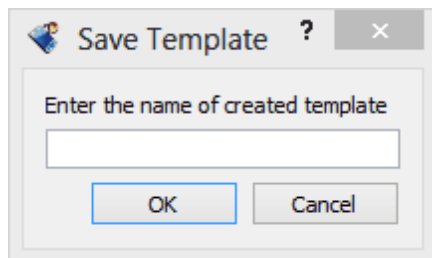
NOTE: Recovering passwords is available only when using EPB for Windows OS.

To save the attack to a template, do the following:

1. Start the [password recovery](#).
2. Add the attacks to be performed in the pipeline.
3. Double-click a certain attack or click  next to it.
4. Select **Template** -> **Save as template** on the **Attack settings** page.



5. In the **Save Template** window, define the name of the template, and click OK.



6. The template is saved. Now you can load the template from the template database when you recover a different password.

To [view the saved template](#), go to **Settings** -> **Templates**.

8 Technical support

8.1 Contacting us

For technical support, please contact us through the web form located at:

<http://www.elcomsoft.com/support.html>

For all other requests (general questions, sales, legal), please use another form:

<http://www.elcomsoft.com/company.html>

Our fax numbers:

+1 866 448-2703 (US and Canada, toll-free)

+44 870 831-2983 (UK)

+49 18054820050734 (Germany)

Please write in English language only.

8.2 Where to get the latest version

The latest version of EPB is always available at:

<http://www.elcomsoft.com/epb.html>

Other password recovery products (for ZIP and RAR archives, all versions of Microsoft Office, Microsoft Outlook and Outlook Express, Microsoft Money, Microsoft Project, VBA; Lotus WordPro, 1-2-3, Approach and Organizer; Adobe Acrobat PDF; Corel Paradox, WordPerfect and QuattroPro; Intuit Quicken and QuickBooks; Microsoft SQL; Sage ACT! and accounting software; email clients such as TheBat!, Eudora, Pegasus etc; instant messengers; Windows 2000/XP/2003/Vista/2008/Windows 7 Encrypting File System on NTFS; Windows logon passwords; Windows PWL/RAS/dial-up/VPN/shares/asterisked passwords; WPA passwords and more) are available from our web site at:

<http://www.elcomsoft.com/products.html>

9 License and registration

9.1 Copyright and license

NOTICE TO USER:

THIS IS AN AGREEMENT GOVERNING YOUR USE OF ELCOMSOFT SOFTWARE, FURTHER DEFINED HEREIN AS "PRODUCT," AND THE LICENSOR OF THE PRODUCT IS WILLING TO PROVIDE YOU WITH ACCESS TO THE PRODUCT ONLY ON THE CONDITION THAT YOU ACCEPT ALL OF THE TERMS AND CONDITIONS CONTAINED IN THIS AGREEMENT. BELOW, YOU ARE ASKED TO ACCEPT THIS AGREEMENT AND CONTINUE TO INSTALL OR, IF YOU DO NOT WISH TO ACCEPT THIS AGREEMENT, TO DECLINE THIS AGREEMENT, IN WHICH CASE YOU WILL NOT BE ABLE TO INSTALL OR OPERATE THE PRODUCT. BY INSTALLING THIS PRODUCT YOU ACCEPT ALL THE TERMS AND CONDITIONS OF THIS AGREEMENT.

This Electronic End User License Agreement (the "Agreement") is a legal agreement between you (either an individual or an entity), the licensee, and ElcomSoft Co. Ltd. and its affiliates (collectively, the "Licensor"), regarding the Licensor's software, as applicable pursuant to a valid license, you are about to download and/or other related services, including without limitation a) all of the contents of the files, disk(s), CD-ROM(s) or other media with which this Agreement is provided and including all forms of code, such as source code and object code, (the "Software"), b) all successor upgrades, modified versions, modified modules, revisions, patches, enhancements, fixes, modifications, copies, additions or maintenance releases of the Software, if any, licensed to you by the Licensor (collectively, the "Updates"), and c) related user documentation and explanatory materials or files provided in written, "online" or electronic form (the "Documentation" and together with the Software and Updates, the "Product"). You are subject to the terms and conditions of this End User License Agreement whether you access or obtain the Product directly from the Licensor, or through any other source. For purposes hereof, "you" means the individual person installing or using the Product on his or her own behalf; or, if the Product is being downloaded or installed on behalf of an organization, such as an employer, "you" means the organization for which the Product is downloaded or installed, then the person accepting this agreement represents hereby that such organization has authorized such person to accept this agreement on the organization's behalf. For purposes hereof the term "organization," without limitation, includes any partnership, limited liability company, corporation, association, joint stock company, trust, joint venture, labor organization, unincorporated organization, or governmental authority.

By accessing, storing, loading, installing, executing, displaying, copying the Product into the memory of a Client Device, as defined below, or otherwise benefiting from using the functionality of the Product ("Operating"), you agree to be bound by the terms and conditions of this Agreement. If you do not agree to the terms and conditions of this Agreement, the Licensor is unwilling to license the Product to you. In such event, you may not Operate or use the Product in any way.

BEFORE YOU PRESS THE "I AGREE" BUTTON, PLEASE CAREFULLY READ THE TERMS AND CONDITIONS OF THIS AGREEMENT, AS SUCH ACTIONS ARE A SYMBOL OF YOUR SIGNATURE AND BY CLICKING ON THE "I AGREE", YOU ARE CONSENTING TO BE BOUND BY AND ARE BECOMING A PARTY TO THIS AGREEMENT AND AGREE THAT THIS AGREEMENT IS ENFORCEABLE LIKE ANY WRITTEN NEGOTIATED AGREEMENT SIGNED BY YOU. IF YOU DO NOT AGREE TO ALL OF THE TERMS OF THIS AGREEMENT, CLICK THE "CANCEL" BUTTON AND THE PRODUCT WILL NOT BE INSTALLED ON YOUR CLIENT DEVICE, AS SUCH TERM IS DEFINED BELOW. For your reference, you may refer to the copy of this Agreement that can be found in the Help for the Software. You may also receive a copy of this Agreement by contacting Licensor at: info@elcomsoft.com.

1. Proprietary Rights and Non-Disclosure.
 - 1.1. Ownership Rights. You agree that the Product and the authorship, systems, ideas, methods of operation, documentation and other information contained in the Product, are proprietary intellectual properties and or the valuable trade secrets of the Licensor and are protected by civil and criminal law, and by the law of copyright, trade secret, trademark and patent of the Russian federation, other countries and international treaties. You may use trademarks only insofar as to identify printed output produced by the Product in accordance with accepted trademark practice, including identification of trademark owner's name. Such use of any trademark does not give you any rights of ownership in that trademark. The Licensor and its suppliers own and retain all right, title, and interest in and to the Product, including without limitations any error corrections, enhancements, Updates or other modifications to the Software, whether made by Licensor or any third party, and all copyrights, patents, trade secret rights, trademarks, and other intellectual property rights therein. Your possession, installation or use of the Product does not transfer to you any title to the intellectual property in the Product, and you will not acquire any rights to the Product except as expressly set forth in this Agreement. All copies of the Product made hereunder must contain the same proprietary notices that appear on and in the Product. Except as stated herein, this Agreement does not grant you any intellectual property rights in the Product and you acknowledge that the license granted under this Agreement only provides you with a right of limited use under the terms and conditions of this Agreement.
 - 1.2. Source Code and Modifications. You acknowledge that the source code for the Product is proprietary to the Licensor and constitutes trade secrets of the Licensor. You agree not to modify, or create derivative works based upon the Product in whole or in part nor reverse engineer, decompile, disassemble the source code of the Product in any way.
 - 1.3. Registration Code File and Confidential Information. You agree that, unless otherwise specifically provided herein or agreed by the Licensor in writing, the Product, including the specific design and structure of individual programs and the Product, including without limitation the Registration Code File provided to you by the Licensor and/or its authorized resellers or distributors, constitute confidential proprietary information of the Licensor. For purposes hereof, "Registration Code" shall mean a unique key identification file or a combination of unique electronic characters provided to you by the Licensor confirming the purchase of the license from the Licensor, which may carry the information about the license and the number of permitted users, and enabling the full functionality of the Product in accordance with the license granted under this Agreement. You agree not to transfer, copy, disclose, provide or otherwise make available such confidential information in any form to any third party without the prior written consent of the Licensor. You agree to implement reasonable security measures to protect such confidential information, but without limitation to the foregoing, shall use best efforts to maintain the security of the Registration Code provided to you by the Licensor and/or its authorized resellers or distributors.
2. Grant of License.
 - 2.1. License. The Licensor grants you the following rights ("License") and you hereby agree and accept such License:
 - a). Trial Version. If you have received, downloaded and/or installed a trial version of the Product and are hereby granted an evaluation license for the Software and you may Operate the Product only for evaluation purposes and only during the single applicable evaluation period of thirty (30) days, unless otherwise indicated, from the date of the initial installation. Following this test period of thirty (30) days or less, if you wish to continue to use the Product, you must register. To register you have to pay for the fully functional version. Upon payment we provide the Registration Code to you. Any use of the Product for other purposes or beyond the applicable evaluation period is strictly prohibited, provided however that, subject to the restrictions contained herein, you may copy and distribute a trial version of the Software without any modifications whatsoever to any third party subject to this Agreement and further provided that you have no technical support rights during the trial period. The 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 Product without written permission from the copyright holder.
 - b). Grant of License. Unless otherwise specifically indicated under a valid license (e.g. volume license) granted by the Licensor, once registered you are granted a non-exclusive and non-transferable

license to install one (1) copy of the Product and during the term of your license, subject to the payment of the applicable fees and your compliance with the terms hereof, this Agreement permits you or any of your employees to Operate one copy of the specified version of the Product, for internal purposes only, on one computer, workstation, or other electronic device of which the software was designed (each a "Client Device"). If you have purchased multiple licenses for the Product, then the number of multiple licenses shall determine the number of copies of the Product you may have and the number of Client Devices on which you may Operate the Product. If the Product is licensed as a suite or bundle with more than one specified software product, this license applies to all such specified software products, subject to any restrictions or usage terms specified on the applicable price list or product packaging that apply to any of such software products individually. Additionally, Licensor reserves the right to provide for specific terms and conditions in the purchased licenses and such terms may be embedded in Registration Code specifying other terms, conditions and restrictions of Operating of the Product. The Licensor reserves all rights not expressly granted herein.

- c). **Limitations on Personal License.** With the purchase of a personal License, the Licensee may operate the Product as set forth in the Agreement for non-commercial purposes in a non-business or non-commercial environment. Use of the Product in a corporate, governmental or business environment requires the purchase of a business license.
- d). **Site License.** With the acquisition of a Site License, the Licensee may install and use the Product on an unlimited amount of CPUs within one office in one geographic location. Within these limitations, the Licensee may install the Product as a "Network" Product and run the software from any networked computer on your LAN, provided those computers are located exclusively within one office at one geographic location.
- e). **Volume Use.** If the Product is licensed with volume license terms specified in the applicable product invoicing or packaging for the Product, you may make use and install as many additional copies of the Product on the number of Client Devices as the volume license terms specify. You must have a reasonable mechanism in place to ensure that the number of Client Devices on which the Product has been installed does not exceed the number of licenses you have obtained.
- f). **Multiple Environment Product; Multiple Language Product; Dual Media Product; Multiple Copies; Bundles.** If the Product supports multiple platforms or languages, if you receive the Product on multiple media, if you otherwise receive multiple copies of the Product, or if you received the Product bundled with other software, the total number of your Client Devices on which all versions of the Product are installed may not exceed the number of licenses you have obtained from the Licensor. You may not rent, lease, sublicense, lend or transfer any versions or copies of the Product you do not use.
- 2.2. **Back-up Copies.** You can make one (1) copy the Product for backup and archival purposes, provided, however, that the original and each copy is kept in your possession or control, and that your installation and use of the Product does not exceed that which is allowed in this Section 2.
- 2.3. **Prohibitions.** You may not use, copy, emulate, clone, rent, lease, sell, modify, decompile, disassemble, otherwise reverse engineer, or transfer the licensed program, or any subset of the licensed program, except as provided for in this Agreement. Any such unauthorized use shall result in immediate and automatic termination of this license and may result in criminal and/or civil prosecution. Neither ElcomSoft binary code nor source may be used or reverse engineered to re-create the program algorithm, which is proprietary, without written permission of Licensor. All rights not expressly granted here are reserved by ElcomSoft Co. Ltd.
- 2.4. **Special Provisions Applicable to Password Recovery Programs.** The Licensor has a strict return policy due to the nature of our products. If the software is unable to recover (or remove, or change) a password, a copy of the unrecovered file must be sent to the Licensor for evaluation. If the password is recovered, you will be either able to keep the software and receive the password to the file (or unprotected copy of the file), or refund can be made and the end user will need to pay for the in-house recovery in order to receive the password. If the Licensor is unable to recover the password, a full refund will be made. This subsection is applicable only to situations when password recovery or removal is guaranteed without brute-force or dictionary attacks.
- 2.5. **Registration Code.** Registration Code provided by the Licensor constitutes the confidential proprietary information of the Licensor. ElcomSoft Registration Code file may not be distributed, except

as stated herein, outside of the area of legal control of the person or persons who purchased the original license, without written permission of the copyright holder. You may not give away, sell or otherwise transfer your Registration Code to a third party. Doing so will result in an infringement of copyright. ElcomSoft Co. Ltd retains the right of claims for compensation in respect of damage which occurred by your giving away the registration code. This claim shall also extend to all costs which ElcomSoft Co. Ltd incurs in defending itself.

2.6. Transfers. Under no circumstances shall Licensee sell, rent, lease, license, sublicense, publish, display, distribute, or otherwise transfer to a third party the Software, any copy thereof, in whole or in part, without Licensor's prior written consent, unless otherwise provided for in this Agreement.

2.7. Acceptance of Licensing Terms. Installing and using the Product signifies acceptance of these terms and conditions of the License. If you do not agree with the terms of the license you must remove all Product files from your storage devices, including any back-up or archival copy, and cease to use the Product.

2.8. Material Terms and Conditions. Licensee specifically agrees that each of the terms and conditions of this Section 2 are material and that failure of Licensee to comply with these terms and conditions shall constitute sufficient cause for Licensor to immediately terminate this Agreement and the License granted under this Agreement. The presence of this Section 2.7 shall not be relevant in determining the materiality of any other provision or breach of this Agreement by either party.

2.9. Term and Termination. The term of this Agreement ("Term") shall begin when you download, access or install the Product or pay the applicable license fees (whichever is earlier) and shall continue for the term specified in your order. Without prejudice to any other rights, this Agreement will terminate automatically if you fail to comply with any of the limitations or other requirements described herein. Upon any termination or expiration of this Agreement, you must immediately cease use of the Product and destroy all copies of the Product.

2.10. No Rights Upon Termination. Upon termination of this Agreement you will no longer be authorized to Operate or use the Product in any way.

3. Support and Updates.

3.1. Terms of Support. During the one-year period you are entitled to technical services and support for the Product which is provided to you by Licensor during the regular business hours (GMT+ 03:00), except for locally-observed holidays, and includes the support provided through a special technical support section of the Licensor's site (the "Site") and email support@elcomsoft.com. During such period of one year e-mail support is unlimited and includes technical and support questions and patch fixes.

3.2. Updates. During the one-year period, you may download Updates to the Product when and as the Licensor publishes them on the Site, or through other online services. If the Product is an Update to a previous version of the Product, you must possess a valid license to such previous version in order to use the Update. You may continue to use the previous version of the Product on your Client Device after you receive the Update to assist you in the transition to the Update, provided that: (i) the Update and the previous version are installed on the same Client Device; (ii) the previous version or copies thereof are not transferred to another party or Client Device unless all copies of the Update are also transferred to such party or Client Device; (iii) you acknowledge that any modification that you made to the Product may be lost, altered, distorted or destroyed rendering such modifications, Product or the part thereof inoperable or non-usable; and (iv) you acknowledge that any obligation the Licensor may have to support the previous version of the Product may be ended upon availability of the Update. Except for the rights to free Updates during the one-year period, as further defined herein, nothing in this Agreement shall be construed as to grant you any rights or licenses with regard to the new releases of the Product or to entitle you to any new release. This Agreement does not obligate the Company to provide any Updates. Notwithstanding the foregoing, any Updates that you may receive become part of the Product and the terms of this Agreement apply to them (unless this Agreement is superseded by a succeeding agreement accompanying such Update or modified version of the Product).

4. Restrictions.

4.1. No Transfer of Rights. You may not transfer any rights pursuant to this Agreement nor rent, sublicense, lease, loan or resell the Product. You may not permit third parties to benefit from the use or functionality of the Product via a timesharing, service bureau or other arrangement, except to the extent

such use is specified in the application price list, purchase order or product packaging for the Product. Except as otherwise provided in Section 1.2 hereof, you may not, without the Licensor's prior written consent, reverse engineer, decompile, disassemble or otherwise reduce any part of the Product to human readable form nor permit any third party to do so, except to the extent the foregoing restriction is expressly prohibited by applicable law. Notwithstanding the foregoing sentence, decompiling the Software is permitted to the extent the laws of your jurisdiction give you the right to do so to obtain information necessary to render the Software interoperable with other software; provided, however, that you must first request such information from the Licensor and the Licensor may, in its discretion, either provide such information to you (subject to confidentiality terms) or impose reasonable conditions, including a reasonable fee, on such use of the Software to ensure that the Licensor's and its affiliates' proprietary rights in the Software are protected. Except for the modification permitted under Section 1.2, you may not modify, or create derivative works based upon the Product in whole or in part.

4.2. Proprietary Notices and Copies. You may not remove any proprietary notices or labels on the Product. You may not copy the Product except as expressly permitted in Section 2 above.

4.3. Compliance with Law. You agree that in Operating the Product and in using any report or information derived as a result of Operating this Product, you will comply with all applicable international, national, state, regional and local laws and regulations, including, without limitation, privacy, trademark, patent, copyright, export control and obscenity law and you shall not use the Product for unethical or illegal business practices or in violation of any obligation to a third party in using, operating, accessing or running any of the Product and shall not knowingly assist any other person or entity to so violate any obligation to a third party.

4.4. Additional Protection Measures. Solely for the purpose of preventing unlicensed use of the Product, the Software may install on your Client Device technological measures that are designed to prevent unlicensed use, and the Licensor may use this technology to confirm that you have a licensed copy of the Product. The update of these technological measures may occur through the installation of the Updates. The Updates will not install on unlicensed copies of the Product. If you are not using a licensed copy of the Product, you are not allowed to install the Updates. The Licensor will not collect any personally identifiable information from your Client Device during this process.

5. WARRANTIES AND DISCLAIMERS.

5.1. Limited Warranty. The Licensor warrants that for 90 days (the "Warranty Period") from the date the Registration Code is provided to you by Licensor, the media on which Product has been provided will be free from defects in materials and workmanship and that the Software will perform substantially in accordance with the Documentation or generally conform to the Product's specifications published by the Licensor. Non-substantial variations of performance from the Documentation do not establish a warranty right. THIS LIMITED WARRANTY DOES NOT APPLY TO UPDATES AS APPLIED TO ANY MODIFIED PRODUCT, WHETHER OR NOT SUCH MODIFICATION IS PERMISSIBLE HEREUNDER, TRIAL AND EVALUATION VERSIONS, UPDATES, PRE-RELEASE, TRYOUT, PRODUCT SAMPLER, OR NOT FOR RESALE (NFR) COPIES OF PRODUCT. This limited warranty is void and your support right terminate if the defect has resulted from accident, abuse, or misapplication or any modification, whether or not such modification is permitted hereunder. No warranty is made as to the integrity, protection or safekeeping of any modification to the Products made by you upon installation of any of the Updates. To make a warranty claim, you must return the Product to the location where you obtained it along with proof of purchase within such sixty (60) day period of the license fee you paid for the Product. THE LIMITED WARRANTY SET FORTH IN THIS SECTION GIVES YOU SPECIFIC LEGAL RIGHTS. YOU MAY HAVE ADDITIONAL RIGHTS WHICH VARY FROM JURISDICTION TO JURISDICTION.

5.2. Customer Remedies. The Licensor and its suppliers' entire liability and your exclusive remedy for any breach of the foregoing warranty shall be at the Licensor's option: (i) return of the purchase price paid for the license, if any, (ii) replacement of the defective media in which the Product is contained, or (iii) correction of the defects, "bugs" or errors within reasonable period of time. You must return the defective media to the Licensor at your expense with a copy of your receipt. Any replacement media will be warranted for the remainder of the original warranty period.

5.3. NO OTHER WARRANTIES. EXCEPT FOR THE FOREGOING LIMITED WARRANTY, AND FOR ANY WARRANTY, CONDITION, REPRESENTATION OR TERM TO THE EXTENT TO WHICH THE

SAME CANNOT OR MAY NOT BE EXCLUDED OR LIMITED BY LAW APPLICABLE TO YOU IN YOUR JURISDICTION, THE PRODUCT IS PROVIDED "AS-IS" WITHOUT ANY WARRANTY WHATSOEVER AND THE LICENSOR MAKES NO PROMISES, REPRESENTATIONS OR WARRANTIES, WHETHER EXPRESSED OR IMPLIED, WHETHER BY STATUTE, COMMON LAW, CUSTOM, USAGE OR OTHERWISE, REGARDING OR RELATING TO THE PRODUCT OR CONTENT THEREIN OR TO ANY OTHER MATERIAL FURNISHED OR PROVIDED TO YOU PURSUANT TO THIS AGREEMENT OR OTHERWISE. YOU ASSUME ALL RISKS AND RESPONSIBILITIES FOR SELECTION OF THE PRODUCT TO ACHIEVE YOUR INTENDED RESULTS, AND FOR THE INSTALLATION OF, USE OF, AND RESULTS OBTAINED FROM THE PRODUCT. THE LICENSOR MAKES NO WARRANTY THAT THE PRODUCT WILL BE ERROR FREE OR FREE FROM INTERRUPTION OR FAILURE, OR THAT IT IS COMPATIBLE WITH ANY PARTICULAR HARDWARE OR SOFTWARE. TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, LICENSOR DISCLAIMS ALL WARRANTIES, EITHER EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT OF THIRD PARTY RIGHTS, INTEGRATION, SATISFACTORY QUALITY OR FITNESS FOR ANY PARTICULAR PURPOSE WITH RESPECT TO THE PRODUCT AND THE ACCOMPANYING WRITTEN MATERIALS OR THE USE THEREOF. SOME JURISDICTIONS DO NOT ALLOW LIMITATIONS ON IMPLIED WARRANTIES, SO THE ABOVE LIMITATION MAY NOT APPLY TO YOU. YOU HEREBY ACKNOWLEDGE THAT THE PRODUCT MAY NOT BE OR BECOME AVAILABLE DUE TO ANY NUMBER OF FACTORS INCLUDING WITHOUT LIMITATION PERIODIC SYSTEM MAINTENANCE, SCHEDULED OR UNSCHEDULED, ACTS OF GOD, TECHNICAL FAILURE OF THE SOFTWARE, TELECOMMUNICATIONS INFRASTRUCTURE, OR DELAY OR DISRUPTION ATTRIBUTABLE TO VIRUSES, DENIAL OF SERVICE ATTACKS, INCREASED OR FLUCTUATING DEMAND, AND ACTIONS AND OMISSIONS OF THIRD PARTIES. THEREFORE, THE LICENSOR EXPRESSLY DISCLAIMS ANY EXPRESS OR IMPLIED WARRANTY REGARDING SYSTEM AND/OR SOFTWARE AVAILABILITY, ACCESSIBILITY, OR PERFORMANCE. THE LICENSOR DISCLAIMS ANY AND ALL LIABILITY FOR THE LOSS OF DATA DURING ANY COMMUNICATIONS AND ANY LIABILITY ARISING FROM OR RELATED TO ANY FAILURE BY THE LICENSOR TO TRANSMIT ACCURATE OR COMPLETE INFORMATION TO YOU.

5.4. LIMITED LIABILITY; NO LIABILITY FOR CONSEQUENTIAL DAMAGES. YOU ASSUME THE ENTIRE COST OF ANY DAMAGE RESULTING FROM YOUR USE OF THE PRODUCT AND THE INFORMATION CONTAINED IN OR COMPILED BY THE PRODUCT, AND THE INTERACTION (OR FAILURE TO INTERACT PROPERLY) WITH ANY OTHER HARDWARE OR SOFTWARE WHETHER PROVIDED BY THE LICENSOR OR A THIRD PARTY. TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, IN NO EVENT WILL THE LICENSOR OR ITS SUPPLIERS OR LICENSORS BE LIABLE FOR ANY DAMAGES WHATSOEVER (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF BUSINESS PROFITS, BUSINESS INTERRUPTION, LOSS OF BUSINESS INFORMATION, LOSS OF DATA, LOSS OF GOODWILL, WORK STOPPAGE, HARDWARE OR SOFTWARE DISRUPTION IMPAIRMENT OR FAILURE, REPAIR COSTS, TIME VALUE OR OTHER PECUNIARY LOSS) ARISING OUT OF THE USE OR INABILITY TO USE THE PRODUCT, OR THE INCOMPATIBILITY OF THE PRODUCT WITH ANY HARDWARE SOFTWARE OR USAGE, EVEN IF SUCH PARTIES HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. IN NO EVENT WILL LICENSOR'S TOTAL LIABILITY TO YOU FOR ALL DAMAGES IN ANY ONE OR MORE CAUSE OF ACTION, WHETHER IN CONTRACT, TORT OR OTHERWISE EXCEED THE AMOUNT PAID BY YOU FOR THE PRODUCT. THIS LIMITATION OF LIABILITY SHALL NOT APPLY TO LIABILITY FOR DEATH OR PERSONAL INJURY TO THE EXTENT THAT APPLICABLE LAW PROHIBITS SUCH LIMITATION. FURTHERMORE, BECAUSE SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OR LIMITATION OF LIABILITY FOR CONSEQUENTIAL OR INCIDENTAL DAMAGES, THE ABOVE LIMITATION MAY NOT APPLY TO YOU.

6. Indemnification

6.1. Indemnification for Violations. Your Operating of the Product, your accessing your account with Licensor and your entering into this Agreement constitutes your consent and agreement to defend, indemnify and hold harmless Licensor and its affiliated companies, employees, contractors, officers and directors from any claim or demand, including reasonable attorney's fees arising out of your use of the

Product in violation of this Agreement.

SPECIAL PROVISION APPLICABLE TO U.S. PERSONS AND ENTITIES.

7. U.S. Government-Restricted Rights.

7.1. Notice to U.S. Government End Users. The Product and accompanying Documentation are deemed to be "Commercial Items," as that term is defined at 48 C.F.R. §2.101, consisting of "Commercial Computer Software" and "Commercial Computer Software Documentation," respectively, as such terms are used in 48 C.F.R. §12.212 or 48 C.F.R. §227.7202, as applicable. Consistent with 48 C.F.R. §12.212 or 48 C.F.R. §§227.7202-1 through 227.7202-4, as applicable, the Commercial Computer Software and Commercial Computer Software Documentation are being licensed to U.S. Government end users (a) only as Commercial Items and (b) with only those rights, including any use, modification, reproduction, release, performance, display or disclosure of the Product and accompanying Documentation, as are granted to all other end users pursuant to the terms and conditions herein. Unpublished-rights reserved under the copyright laws of the United States.

7.2. Export Restrictions. You acknowledge and agree that the Product may be subject to restrictions and controls imposed by the Export Administration Act and the Export Administration Regulations of the United States (the "Acts"). You agree and certify that neither the Product nor any direct product thereof is being or will be used for any purpose prohibited by the Acts. You may not Operate, download, export, or re-export the Product (a) into, or to a national or resident of, any country to which the United States has embargoed goods, or (b) to anyone on the United States Treasury Department's list of Specially Designated Nationals or the U.S. Commerce Department's Table of Deny Orders. By downloading or using the Product, you are representing and warranting that you are not located in, under the control of, or a national or resident of any such country or on any such list. You acknowledge that it is your sole responsibility to comply with any and all government export and other applicable laws and that the Licensor has no further responsibility for such after the initial license to you. You warrant and represent that neither the U.S. Commerce Department, Bureau of Export Administration nor any other U.S. federal agency has suspended, revoked or denied your export privileges.

8. Your Information and the Licensor's Privacy Policy

8.1. Privacy Policy. You acknowledge receipt of and agree to the Licensor's privacy statement which is made available to you in connection with installation and is set forth in full at <http://www.elcomsoft.com/privacy.html>. You hereby expressly consent to the Licensor's processing of your personal data (which may be collected by the Licensor or its distributors) according to the Licensor's current privacy policy as of the date of the effectiveness hereof which is incorporated into this Agreement by reference. By entering into this Agreement, you agree that the Licensor may collect and retain information about you, including your name and email address. The Licensor employs other companies and individuals to perform certain functions on its behalf. Examples include fulfilling orders, delivering packages, sending postal mail and e-mail, removing repetitive information from customer lists, analyzing data, providing marketing assistance, processing credit card payments, and providing customer service. They have access only to personal information needed to perform their functions, but may not use it for other purposes. The Licensor publishes a privacy policy on its web site and may amend such policy from time to time in its sole discretion. You should refer to the Licensor's privacy policy prior to agreeing to this Agreement for a more detailed explanation of how your information will be stored and used by the Licensor. If "you" are an organization, you will ensure that each member of your organization (including employees and contractors) about whom personal data may be provided to the Licensor has given his or her express consent to the Licensor's processing of such personal data. Personal data will be processed by the Licensor or its distributors in the country where it was collected.

8.2. Public Announcements. The Licensor may identify you to the public as a customer of the Licensor and describe in a customer case study the services and solutions delivered by the Licensor to you. The Licensor may also issue one or more press releases, containing an announcement of the execution and delivery of this Agreement and/or the implementation of the Product by you. Nothing contained in this Section shall be construed as an obligation by you to disclose any of your proprietary or confidential information to any third party. In addition, you may opt-out from this Section by writing an opt-out request to the Licensor at info@elcomsoft.com.

9. Miscellaneous.

9.1. Governing Law; Jurisdiction and Venue. This Agreement shall be governed by and construed and enforced in accordance with the laws of the Russian Federation without reference to conflicts of law rules and principles. To the extent permitted by law, the provisions of this Agreement shall supersede any provisions of the Uniform Commercial Code as adopted or made applicable to the Products in any competent jurisdiction. This Agreement shall not be governed by the United Nations Convention on Contracts for the International Sale of Goods, the application of which is expressly disclaimed and excluded. The courts within the Russian Federation shall have exclusive jurisdiction to adjudicate any dispute arising out of this Agreement. You agree that this Agreement is to be performed in the Russian Federation and that any action, dispute, controversy, or claim that may be instituted based on this Agreement, or arising out of or related to this Agreement or any alleged breach thereof, shall be prosecuted exclusively in the courts in of the Russian Federation and you, to the extent permitted by applicable law, hereby waive the right to change venue to any other state, county, district or jurisdiction; provided, however, that the Licensor as claimant shall be entitled to initiate proceedings in any court of competent jurisdiction.

9.2. Period for Bringing Actions. No action, regardless of form, arising out of the transactions under this Agreement, may be brought by either party hereto more than one (1) year after the cause of action has occurred, or was discovered to have occurred, except that an action for infringement of intellectual property rights may be brought within the maximum applicable statutory period.

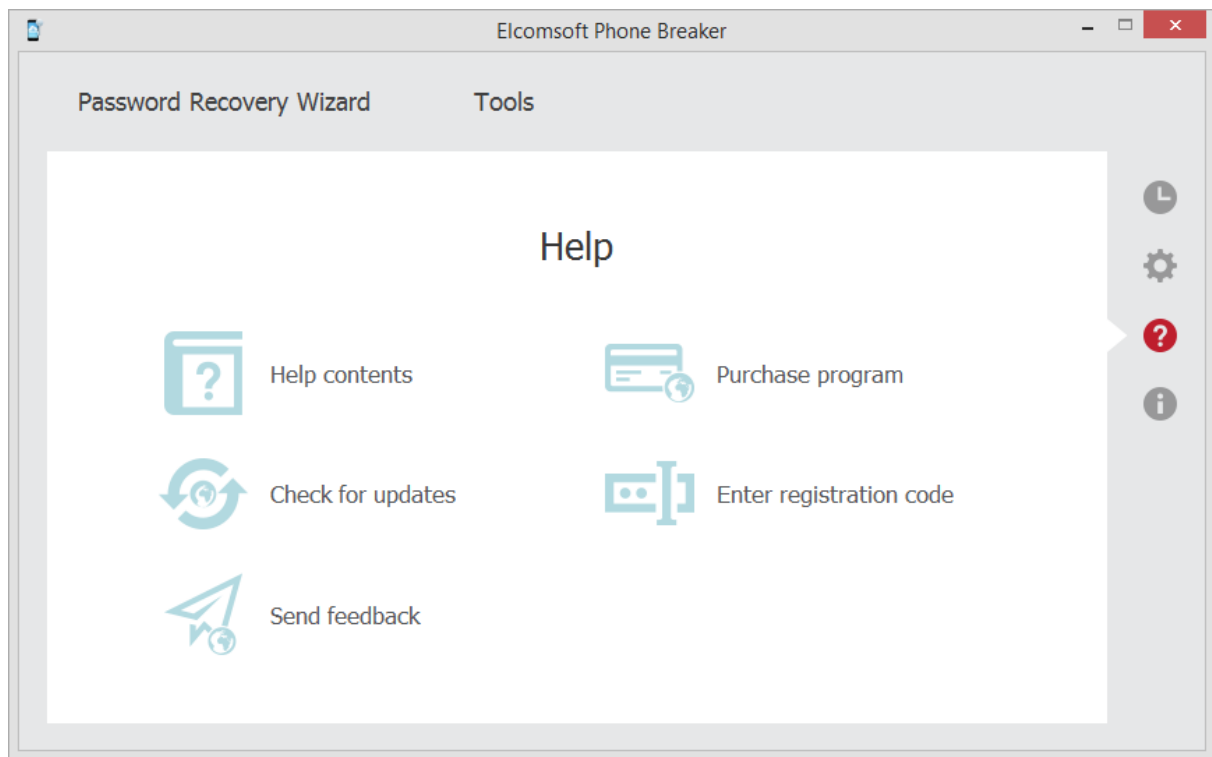
9.3. Entire Agreement; Severability; No Waiver. This Agreement is the entire agreement between you and Licensor and supersedes any other prior agreements, proposals, communications or advertising, oral or written, with respect to the Product or to subject matter of this Agreement. You acknowledge that you have read this Agreement, understand it and agree to be bound by its terms. If any provision of this Agreement is found by a court of competent jurisdiction to be invalid, void, or unenforceable for any reason, in whole or in part, such provision will be more narrowly construed so that it becomes legal and enforceable, and the entire Agreement will not fail on account thereof and the balance of the Agreement will continue in full force and effect to the maximum extent permitted by law or equity while preserving, to the fullest extent possible, its original intent. No waiver of any provision or condition herein shall be valid unless in writing and signed by you and an authorized representative of Licensor provided that no waiver of any breach of any provisions of this Agreement will constitute a waiver of any prior, concurrent or subsequent breach. Licensor's failure to insist upon or enforce strict performance of any provision of this Agreement or any right shall not be construed as a waiver of any such provision or right.

9.4. Contact Information. Should you have any questions concerning this Agreement contact us at legal@elcomsoft.com.

© 1998-2015 ElcomSoft Co. Ltd. All rights reserved. The Product, including the Software and any accompanying Documentation, are copyrighted and protected by copyright laws and international copyright treaties, as well as other intellectual property laws and treaties.

9.2 Registration

There are three editions of EPB: Home, Professional, and Forensic (for more information, see [EPB Editions](#)). To place an order online, go to **Help - Purchase program**:



Alternatively, you can purchase EPB by using the following order form:

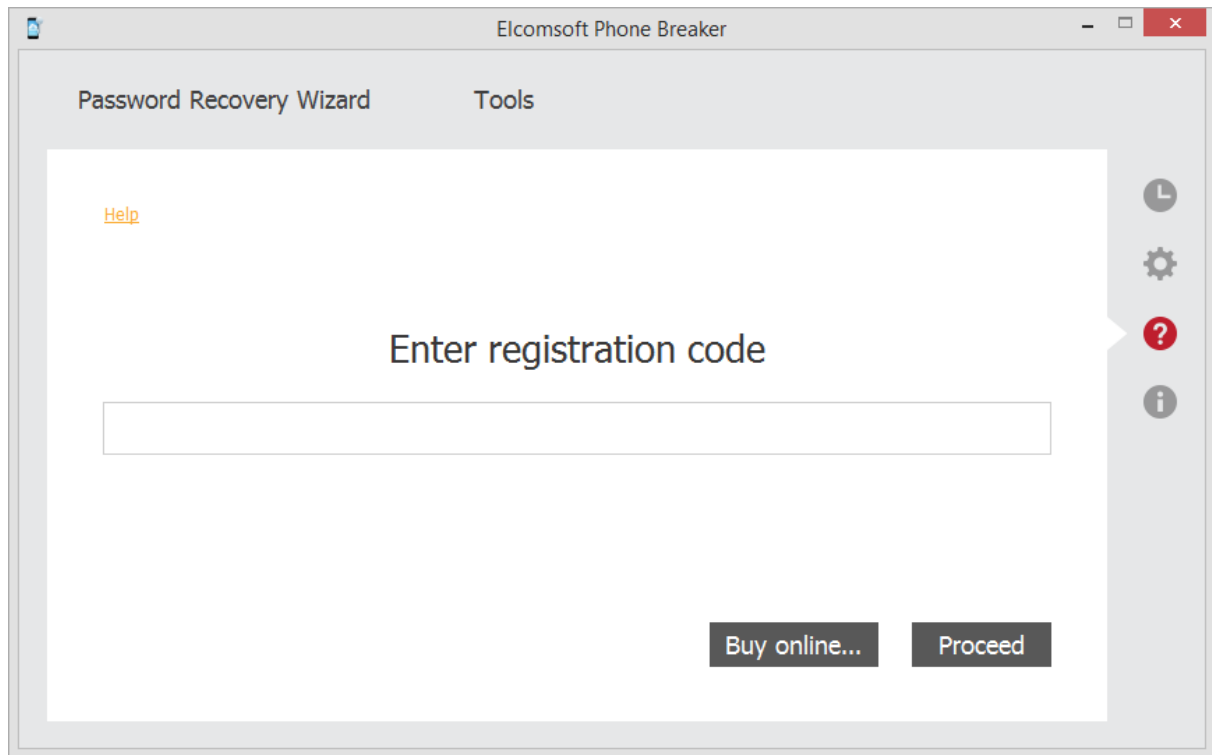
Windows version: <http://www.elcomsoft.com/purchase/buy.php?product=epb>

OS X version: https://www.elcomsoft.com/purchase/purchase.php?product=epbm&additional=ELCOM_PROG_PAGE.XXXXXXXX

Please note that there are some small processing charges for orders placed by fax, by check/money order or with back/wire transfer. European customers are also charged VAT. More information about all payment options is available at ordering page on ElcomSoft web site:

<http://www.elcomsoft.com/order.html?product=epb>

On payment approval (for online orders, usually within a few minutes), we'll send you the registration key which will remove all limitations of the unregistered version. To enter the registration key, go to **Help - Enter registration code**. Enter the key you received in the **Enter registration code** field, and click **Proceed**:



9.3 EPB Editions

There are three editions of EPB: Home, Professional, and Forensic.

Functionality	EPB Trial	EPB Home	EPB Professional	EPB Forensic
Support for iOS from 3.x to 9.x	✓	✓	✓	✓
Support for iPhone 3G/3GS/4/4S/5/5C/5S/6/6S	✓	✓	✓	✓
Support for iPod Touch and iPad	✓	✓	✓	✓
Support for all BlackBerry devices (except PlayBook)	✓	✓	✓	✓
Extract authentication token	✓	✓	✓	✓
Number of CPUs supported	32	2	32	32
Number of GPUs supported	8	1	8	8
Hardware acceleration on Tableau TACC1441 (available only for EPB running on Windows OS)	—	—	✓	✓
Extract and decrypt keychain data (Apple)	—	—	✓	✓

devices with iOS 4/5/6/7/8/9)				
Decrypt iPhone/iPad/iPod backup (with known password)	-	-	✓	✓
Decrypt BlackBerry backup (with known password)	-	-	✓	✓
Decrypt BlackBerry Password Keeper	-	-	✓	✓
Decrypt BlackBerry 10 backup (with known BlackBerry ID password of the user who created the backup)	-	-	-	✓
Recover BlackBerry backup passwords (available on Windows OS only)	⚠ Limited, only 2 characters of found password are shown	✓	✓	✓
Recover iPhone backup passwords (available on Windows OS only)	⚠ Limited, only 2 characters of found password are shown	✓	✓	✓
Recover BlackBerry Password Keeper passwords (available on Windows OS only)	⚠ Limited, only 2 characters of found password are shown	⚠ Limited, only 2 characters of found password are shown	✓	✓
Recover BlackBerry Wallet passwords (available on Windows OS only)	⚠ Limited, only 2 characters of found password are shown	⚠ Limited, only 2 characters of found password are shown	✓	✓
Recover BlackBerry Device Password (available on Windows OS only)	⚠ Limited, only 2 characters of found password are shown	⚠ Limited, only 2 characters of found password are shown	✓	✓
Recover 1Password password (available on Windows OS only)	⚠ Limited, only 2 characters of found password are shown	⚠ Limited, only 2 characters of found password are shown	✓	✓
Decrypt BlackBerry SD card	-	-	✓	✓
Explore keychain	Passwords are not displayed	Passwords are not displayed	✓	✓
Download backup from iCloud using Apple ID and password	⚠ Limited, only the following categories are available: • Info & settings	⚠ Limited, only the following categories are available: • Info & settings	✓	✓

	<ul style="list-style-type: none"> • Address book • Calendar • Call history • Notes 	<ul style="list-style-type: none"> • Address book • Calendar • Call history • Notes 		
Download backup from iCloud with authentication token.	<p>⚠ Limited, only the following categories are available:</p> <ul style="list-style-type: none"> • Info & settings • Address book • Calendar • Call history • Notes 	<p>⚠ Limited, only the following categories are available:</p> <ul style="list-style-type: none"> • Info & settings • Address book • Calendar • Call history • Notes 	<p>⚠ Limited, only the following categories are available:</p> <ul style="list-style-type: none"> • Info & settings • Address book • Calendar • Call history • Notes 	✓
Apple accounts with two-step authentication	—	—	—	✓
Download files from iCloud Drive	—	—	—	✓
Extract Windows Phone data from the cloud (with known credentials to Microsoft account that was used for backing data up)	—	—	✓	✓

9.4 Legal notices

Copyright (c) 1998-2011 The OpenSSL Project. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgment: "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (<http://www.openssl.org/>)"
4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.
5. Products derived from this software may not be called "OpenSSL" nor may "OpenSSL" appear in their names without prior written permission of the OpenSSL Project.
6. Redistributions of any form whatsoever must retain the following acknowledgment: "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (<http://www.openssl.org/>)"

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT "AS IS" AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

=====
This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

Copyright (C) 1995-2004 Jean-loup Gailly and Mark Adler

This software is provided 'as-is', without any express or implied warranty. In no event will the authors be held liable for any damages arising from the use of this software.

Permission is granted to anyone to use this software for any purpose, including commercial applications, and to alter it and redistribute it freely, subject to the following restrictions:

1. The origin of this software must not be misrepresented; you must not claim that you wrote the original software. If you use this software in a product, an acknowledgment in the product documentation would be appreciated but is not required.
2. Altered source versions must be plainly marked as such, and must not be misrepresented as being the original software.
3. This notice may not be removed or altered from any source distribution.

Jean-loup Gailly jloup@gzip.org
Mark Adler madler@alumni.caltech.edu

Copyright (c) 1996 - 2012, Daniel Stenberg, <daniel@haxx.se>.

All rights reserved.

Permission to use, copy, modify, and distribute this software for any purpose with or without fee is hereby granted, provided that the above copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OF THIRD PARTY RIGHTS. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Except as contained in this notice, the name of a copyright holder shall not be used in advertising or otherwise to promote the sale, use or other dealings in this Software without prior written authorization of the copyright holder.

Copyright 2008, Google Inc.

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- * Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- * Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
- * Neither the name of Google Inc. nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Code generated by the Protocol Buffer compiler is owned by the owner of the input file used when generating it. This code is not standalone and requires a support library to be linked with it. This support library is itself covered by the above license.

10 Troubleshooting

The system information about Elcomsoft Phone Breaker work is logged in the EPB log file.

The log is placed in the following locations by default:

- o **Windows:** %AppData%\Elcomsoft\Elcomsoft Phone Password Breaker\EPB_<version and revision number>.log
- o **OS X:** ~/Users/<username>/Library/Application Support/Elcomsoft Phone Password Breaker/EPB_<version and revision number>.log

NOTE: The folder with a log file is a hidden on OS X, so press Shift + Command + G (or Shift + Win + G) and enter the path to the folder to open it.

If you are experiencing any problems with Elcomsoft Phone Breaker, please send us the log file at <http://support.elcomsoft.com/>

Depending on selections in [EPB Settings](#) (General settings), the log from the previous session of work can be saved to the EPB_<version and revision number>.bak file after the application is restarted. In this case, please attach both the log and the *.bak file when reporting an issue with program work.

The amount of information that is written to the log is defined by the level of logging set in the [EPB Settings](#) on the **General** page.