

# Elcomsoft Mobile Forensic Bundle

© 2010-2020 ElcomSoft Co.Ltd.



# Table of Contents

<b>Part I Introduction</b>	<b>7</b>
<b>Part II System requirements</b>	<b>9</b>
<b>Part III Elcomsoft Phone Breaker</b>	<b>10</b>
<b>1 EPB Program information.....</b>	<b>10</b>
Program interface .....	10
EPB settings .....	11
[Windows] Hardware acceleration .....	17
<b>2 Working with Apple devices.....</b>	<b>18</b>
Useful links .....	18
Browsing iTunes and iCloud backups .....	18
Keychain explorer .....	20
<b>Working with iTunes backup .....</b>	<b>28</b>
About iTunes backups.....	28
Working with non-encrypted backup.....	29
Working with encrypted iTunes backup.....	32
Decryption details report.....	35
<b>Working with iCloud data .....</b>	<b>36</b>
Working with iCloud backups.....	36
About iCloud backups.....	36
Downloading iCloud backups.....	37
Downloading specific data types.....	43
Exporting backup list.....	47
Possible problems with downloading data from iCloud.....	48
iCloud backup structure.....	48
Working with files in iCloud.....	50
Downloading files from iCloud.....	50
Exporting iCloud files list.....	56
Downloading synced data from iCloud.....	57
<b>Extracting authentication token for iCloud .....</b>	<b>70</b>
About Authentication token.....	70
Extracting token on Windows OS.....	71
Extracting token on live Windows OS.....	71
Extracting token on non-live Windows OS.....	73
Extracting token on macOS.....	76
Extracting token on live macOS.....	76
Extracting token on non-live macOS.....	79
<b>3 Working with BlackBerry data.....</b>	<b>81</b>
<b>Working with BlackBerry Backups .....</b>	<b>81</b>
About BlackBerry backups .....	81
About BlackBerry Password Keeper and Wallet.....	82
Decrypt BlackBerry backup.....	82
Decrypt BlackBerry Link backup.....	84
Decrypt BlackBerry 10 Password Keeper.....	87
<b>Working with SD card .....</b>	<b>88</b>

About BlackBerry device password.....	88
Decrypt BlackBerry SD card.....	89
SD Card Decryption report.....	92
<b>4 Working with Microsoft account data.....</b>	<b>93</b>
About Microsoft account data .....	93
Downloading Microsoft account data .....	94
<b>5 [Windows] Recovering passwords.....</b>	<b>98</b>
Recovering passwords to storages .....	98
Password recovery attacks .....	103
Saving password recovery attack sessions .....	104
Dictionary attack options .....	108
Brute-Force attack options .....	113
Templates .....	115
Saving templates.....	115
Viewing templates.....	116
Loading templates.....	117
Using templates for attacks.....	118
<b>Part IV Elcomsoft Phone Viewer</b>	<b>120</b>
<b>1 EPV Program information.....</b>	<b>120</b>
EPV Settings .....	120
Supported Apple device backups .....	122
Supported BlackBerry device backups .....	122
Microsoft account data .....	123
<b>2 Working with Apple device data.....</b>	<b>123</b>
About iTunes backups .....	123
About iCloud backups .....	125
About iOS device images .....	126
Working with iOS backups .....	126
Working with iOS device images .....	132
Working with iCloud synced data .....	138
<b>3 Working with Microsoft and BlackBerry data.....</b>	<b>142</b>
Working with backups of BlackBerry devices .....	142
Working with Microsoft account data .....	145
<b>4 Plugins.....</b>	<b>148</b>
Account info .....	148
Apple Pay .....	151
Apple Maps .....	153
Applications .....	157
Calendars .....	159
Calls .....	160
Contacts .....	162
Health .....	163
iBooks .....	167
Keychain .....	168
Locations (iOS) .....	174
Locations (Microsoft) .....	176
Media .....	178
Messages .....	181
Notes .....	185
Photos .....	191
Notifications .....	195

Signal .....	197
Skype .....	201
Screen Time .....	205
Telegram .....	212
Voice Memos .....	219
Wallet .....	221
Web .....	223
Wi-Fi .....	231

## Part V Elcomsoft Cloud Explorer 234

<b>1 ECX Program information.....</b>	<b>234</b>
ECX Program interface .....	234
ECX settings .....	235
Changing path to backup storage .....	236
<b>2 Working with Google account vackups.....</b>	<b>237</b>
Signing in .....	237
Google account snapshots .....	240
Reports .....	243
Exporting data .....	246
Two-step verification .....	251
Exceptional verification cases .....	254
<b>3 Working with Google Drive backups.....</b>	<b>255</b>
Signing in .....	255
Google Drive snapshots .....	257
Exporting data .....	259
Exporting Backup List .....	260
Two-step verification .....	261
Exceptional verification cases .....	264
<b>4 Extracting Google authentication tokens.....</b>	<b>265</b>
About Google Token Extractor .....	265
Extracting token on Windows OS .....	265
Extracting token on Mac OS X .....	268
<b>5 Plugins.....</b>	<b>270</b>
Contacts .....	270
Calendars .....	272
Calls .....	273
Chrome .....	275
Mail .....	277
Media .....	281
Messages .....	283
Google Keep .....	285
History .....	286
Wi-Fi .....	287
Chats .....	289
User Info .....	290
Google Fit .....	291
Google Drive .....	300
Locations .....	301
Places .....	302
Routes .....	304
Your Places.....	307
Maps.....	308

<b>Dashboard .....</b>	<b>309</b>
YouTube.....	309
Tasks.....	310
Search Console.....	310
Search.....	311
Photos).....	312
Payments.....	313
Package Tracking.....	314
News.....	315
Maps.....	316
Location History.....	317
Keep.....	318
Groups.....	319
Google Play Music.....	320
Google Play.....	321
Gmail.....	322
FeedBurner.....	323
Drive.....	324
Device Activity .....	325
Contacts.....	326
Connected Apps .....	327
Chrome.....	328
Calendars.....	329
Brand Accounts.....	330
Books.....	331
Blogger.....	332
Android.....	333
Analytics.....	334
Alerts.....	335
AdSense.....	336
Account.....	337

**Part VI Elcomsoft eXplorer for WhatsApp 339**

<b>1 EXWA Program information.....</b>	<b>339</b>
EXWA settings .....	339
Supported devices .....	339
Moving backup storage .....	340
<b>2 Working with backups of Apple devices.....</b>	<b>340</b>
About backups of Apple devices .....	340
Creating WhatsApp data backups.....	340
About authentication token.....	341
Adding backups to EXWA .....	341
Working with WhatsApp data in local iOS backups.....	341
Working with WhatsApp data in iCloud backups .....	343
Working with WhatsApp data in iCloud Drive files.....	346
<b>3 Working with data from Android devices.....</b>	<b>349</b>
About WhatsApp data from Android devices .....	349
Loading WhatsApp data from Android devices .....	350
About Google authentication token .....	350
Working with data loaded from Android device .....	351
Working with Android data from local storage .....	359
Working with data from Google Drive .....	362

<b>4</b>	<b>Plugins.....</b>	<b>368</b>
	Account info .....	368
	Contacts .....	369
	Calls .....	371
	Media .....	372
	Messages .....	374
<b>Part VII Support &amp; updates</b>		<b>377</b>
<b>1</b>	<b>Contacting us.....</b>	<b>377</b>
<b>2</b>	<b>Updating.....</b>	<b>377</b>
<b>3</b>	<b>Registration.....</b>	<b>378</b>
<b>4</b>	<b>Copyright and license.....</b>	<b>379</b>
<b>5</b>	<b>Legal notices.....</b>	<b>386</b>
<b>6</b>	<b>Troubleshooting.....</b>	<b>389</b>

# 1 Introduction

## Elcomsoft Phone Breaker

**Elcomsoft Phone Breaker (EPB)** enables forensic access to iTunes, iCloud and BlackBerry backups and synchronized Microsoft Account data. The Windows edition features the patented GPU acceleration technology to deliver the fastest password recovery speeds on a single PC. The tool can attack 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.

### **Use cases:**

- Decrypt iOS backups (with known password).
- Download and decrypt iOS backups from iCloud (with valid authentication credentials).
- Download iCloud synchronized data (with valid authentication credentials).
- Decrypt and display Keychain data extracted with Elcomsoft iOS Forensic Toolkit or stored in password-protected iTunes backups (password must be known)
- Download iCloud Keychain and other point-to-point encrypted data from Apple accounts (authentication credentials and password/passcode of a trusted device required).
- Decrypt classic BlackBerry backups (known password).
- Decrypt BlackBerry 10 backups (up to BBOS 10.3.2.2876) created with BlackBerry Link (BlackBerry ID password must be known).
- Download data from Microsoft accounts including text messages, call logs, contacts, notes, locations, browsing history, search history etc.

## Elcomsoft Phone Viewer

Elcomsoft Phone Viewer is a lightweight tool for analyzing information contained in mobile backups, synchronized data and file system images obtained with Elcomsoft's other tools. Analyze information stored in offline and cloud backups and synchronized data extracted with Elcomsoft Phone Breaker and Elcomsoft iOS Forensic Toolkit. Explore the iOS file system images extracted with Elcomsoft iOS Forensic Toolkit and select third-party tools in both .tar and .zip formats. **Elcomsoft Phone Viewer (EPV)** enables access to contacts, messages, call logs, notes, media, and calendar data located in mobile backups and file system images, and displays essential information about the device such as model name, serial number, date of last backup etc.

In addition to iOS, Elcomsoft Phone Viewer allows viewing BlackBerry 10 backups produced with BlackBerry Link, as well as Microsoft Account data downloaded with [Elcomsoft Phone Breaker](#).

Elcomsoft Phone Viewer supports encrypted and unencrypted iOS backups. A valid password is required for accessing encrypted backups.

## Elcomsoft Cloud eXplorer

**Elcomsoft Cloud eXplorer (ECX)** is an all-in-one tool for downloading, viewing and analyzing information stored in the user's Google Account. The tool pulls information from the many available

sources scattered throughout the Google Account, automatically parses the data and displays information in human-readable form.

Google collects massive amounts of information from registered customers. Contacts and Hangouts messages, Google Keep notes, search history with click-through data, synced Google Chrome data including passwords and forms, bookmarks, page transitions and browsing history, location history, calendars and images are just a few pieces of data to mention. The different types of data are scattered around different Google servers and stored in diverse formats. Elcomsoft Cloud Explorer not only downloads more data than provided by Google itself but also offers the ability to view and analyze information without leaving the tool.

With valid authentication credentials, ECX becomes the perfect tool for investigating users' online activities. The integrated viewer displays downloaded data in human-readable form, making it easy to analyze users' communication circles, search and browsing activities. The viewer includes instant filtering and quick search functionality. Finding a certain contact, message or Web site authentication credentials is easy: you just need to type part of the word you are looking for into the search box.

### **Elcomsoft eXplorer for WhatsApp**

**Elcomsoft eXplorer for WhatsApp (EXWA)** provides the ability to obtain and explore WhatsApp data stored in iTunes and iCloud backups, Android WhatsApp and WhatsApp Business data.

#### **Use cases:**

- Download and decrypt WhatsApp for iOS data from iCloud backups.
- Download WhatsApp files synchronized with iCloud.
- Access WhatsApp contacts, messages, call history, and media located in iTunes backups.
- Download and decrypt WhatsApp data from Google Drive.
- Access WhatsApp and WhatsApp Business contacts, messages, call history, and media located in Android backups.
- Load WhatsApp and WhatsApp Business contacts, messages, call history, and media from an Android device.

## 2 System requirements

### Windows

- Windows 10, Windows 8.1, Windows 8, Windows 7; Windows Server 2016, Windows Server 2012
- CPU with SSE2 instruction set (AES-NI recommended)
- At least 300 MB of free disk space
- Recommended: one or more supported NVIDIA or AMD cards or Tableau TACC1441 (recommended for [hardware acceleration](#))

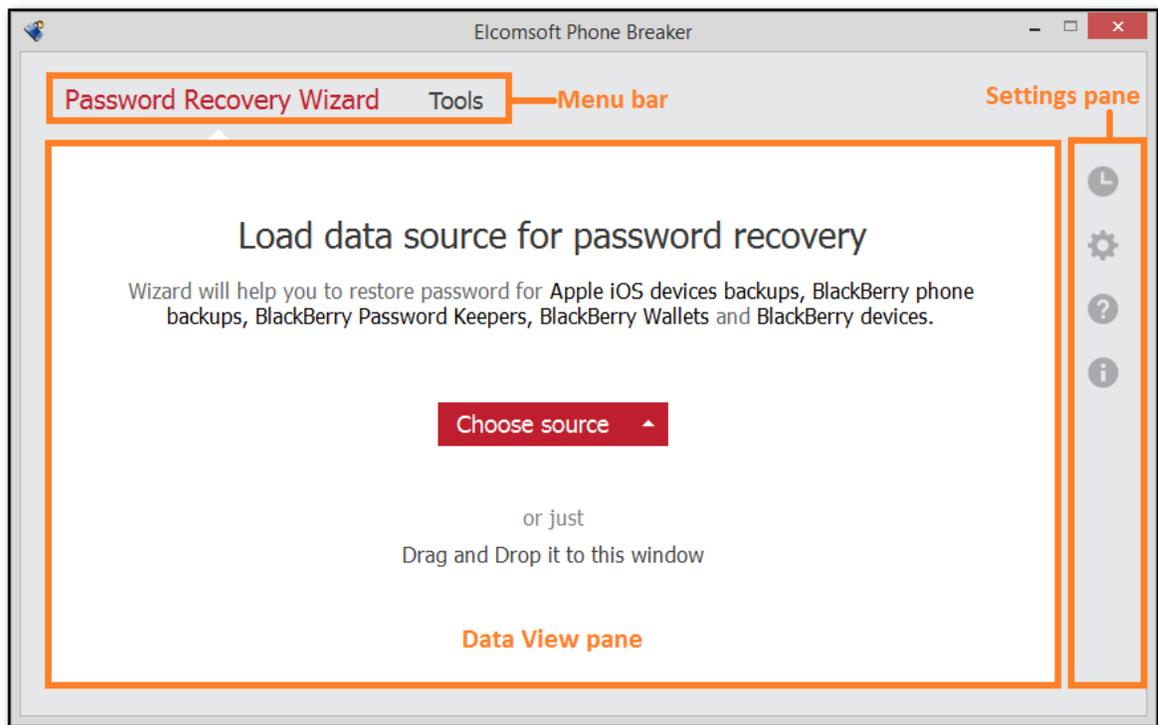
### macOS

- macOS 10.12 - macOS 10.15
- At least 300 megabytes of free disk space disk

## 3 Elcomsoft Phone Breaker

### 3.1 EPB Program information

#### 3.1.1 Program interface



The Elcomsoft Phone Breaker user interface consists of the following elements:

- **Menu bar:** Provides access to the main functionality. The menu bar consists of several tabs:
  - **Password Recovery Wizard:** Allows launching an attack on passwords protecting iOS and Blackberry backups.  
**NOTE: This option is only available in the Windows edition.**
  - **Tools:** Allows decrypting backups for [iPhone](#) and [BlackBerry](#) devices.  
iOS: [iCloud](#) downloads, FileVault decryption, [Keychain](#) explorer, and [authentication token](#) extraction.  
Microsoft Accounts: downloads text messages, Calls, Contacts, Notes, Locations, Web Browsing History and Web Search History.  
BlackBerry: [Password Keeper](#) decryption.
- **Data View pane:** Allows managing data in EPB, depending on which tab on the Menu bar is selected.
- **Settings pane:** Access to the following tabs:
  - **Journal:** Access logged events.

- **Settings:** Configure Hardware, Network, iCloud, and Templates [settings](#).
- **Help:** Access Help, check for updates (macOS), send feedback, purchase or enter registration code.
- **About:** version number and registration information.

### 3.1.2 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:

- **Interface language:** Allows switching between English- and Russian-language interfaces. The changes are applied after restarting the application.
- **Replace system "Open File" dialog by customized if Apple iTunes or BlackBerry Desktop Software is installed:** When selected, the "Open File" window will be 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:
  - **Windows:** *%AppData%\Elcomsoft\Elcomsoft Phone Password Breaker\EPB\_<version and revision number>.log*
  - **macOS:** *~/Users/<username>/Library/Application Support/Elcomsoft Phone Password Breaker/EPB\_<version and revision number>.log*. Please note that this directory is hidden by default.

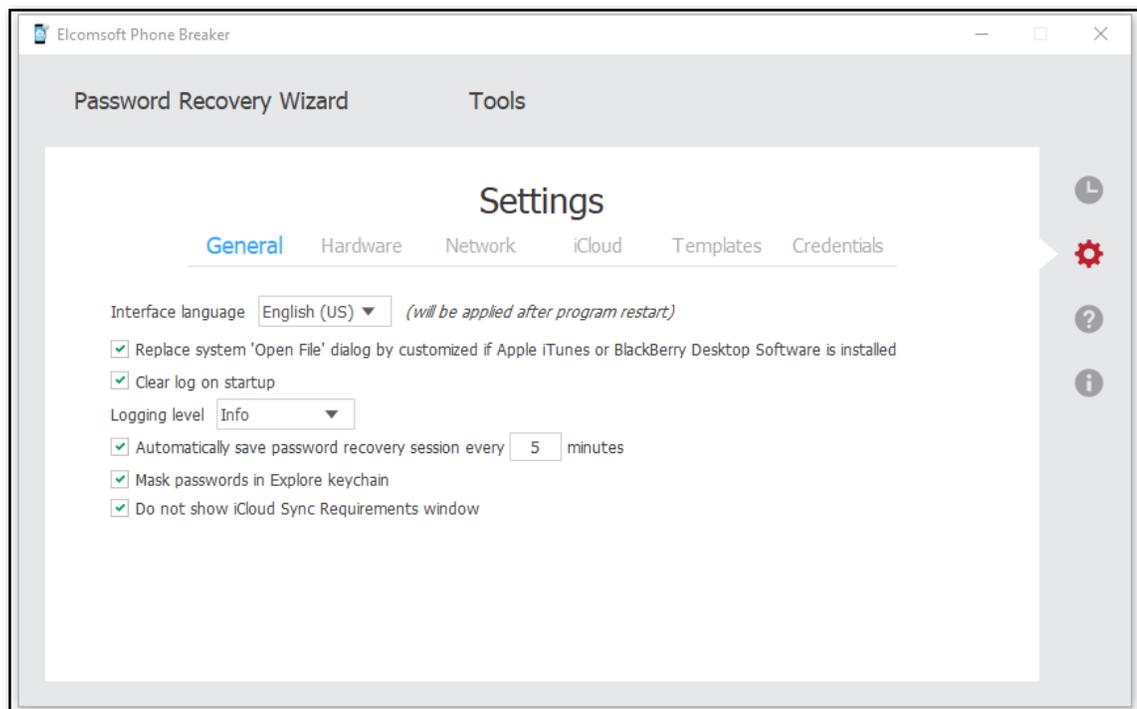
You can select the level of logging in the **Logging level** list. It defines the amount of information that is written to the log: the higher the level, the more detailed information is written to the log file, but at the same time the higher the load on the system at logging. By default, a medium level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

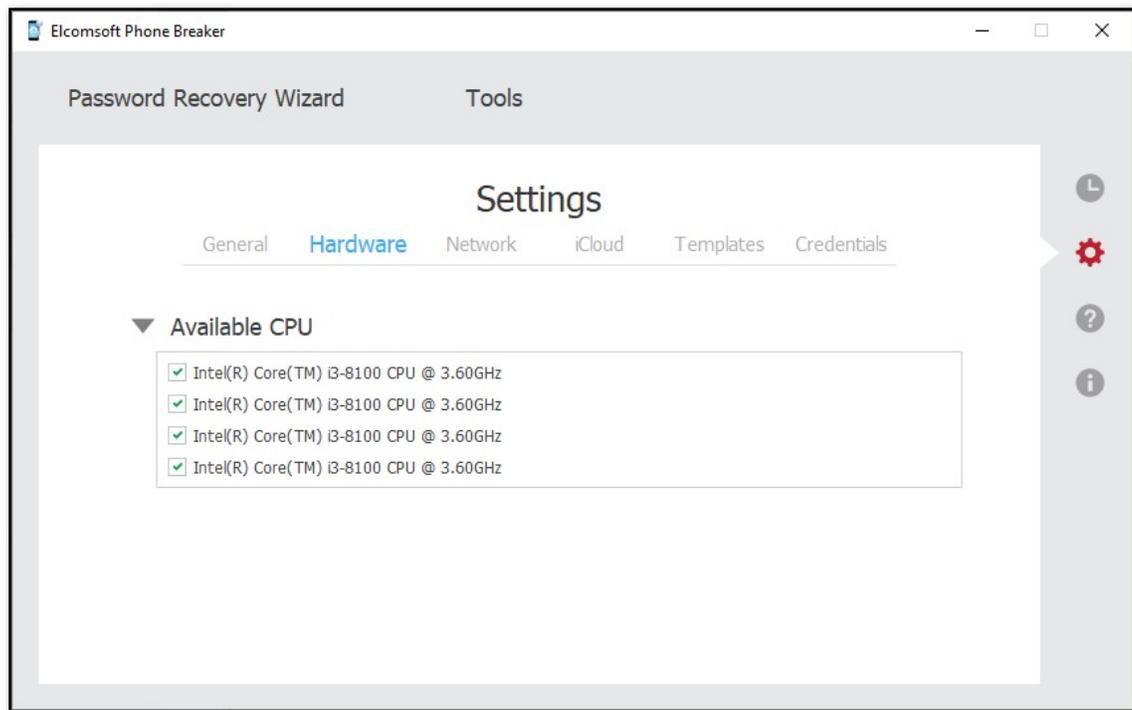
with EPB application.

- **Automatically save password recovery session every <> minutes:** Allows defining how often you want password recovery sessions to be autosaved. By default, set to every 5 minutes.
- **Mask passwords in Explore keychain:** Allows masking passwords with asterisks when exploring keychain data.
- **Do not show iCloud Sync Requirements window:** Allows skipping the iCloud Sync Requirements when downloading synced data from iCloud.



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

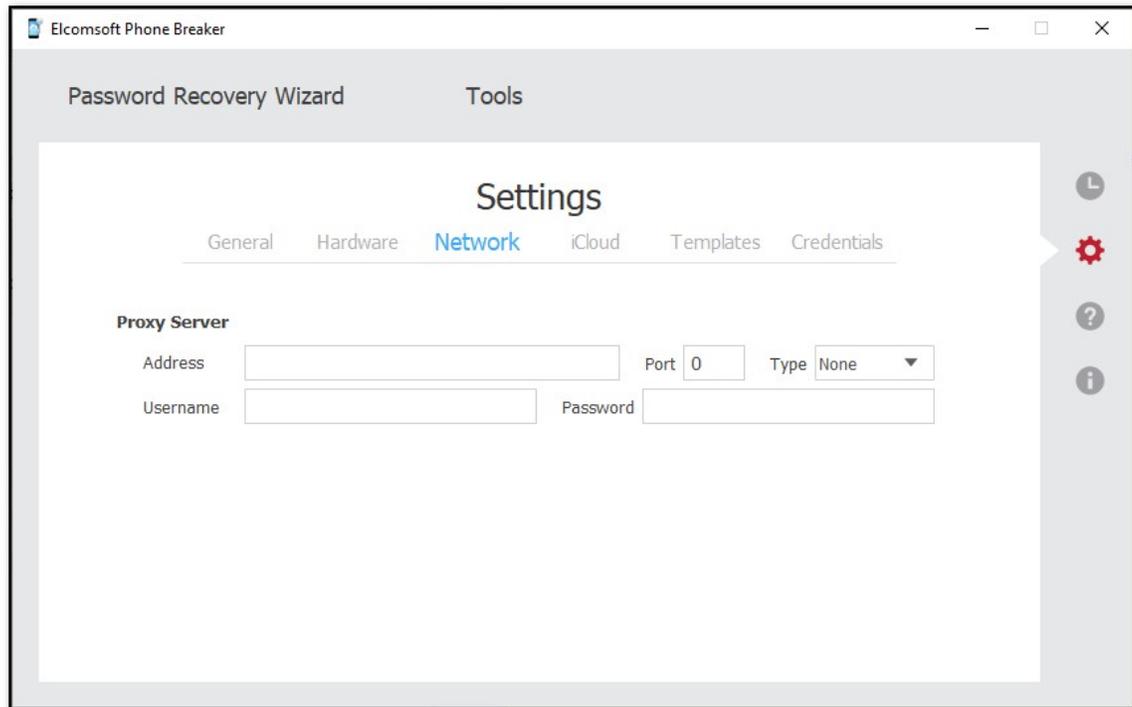
On the Hardware page, define the processor cores (CPU, GPU) that will be used for processing information in EPB.



- **Network**

Define the Proxy server that will be used when downloading [iCloud backups](#) and Microsoft account data. 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:

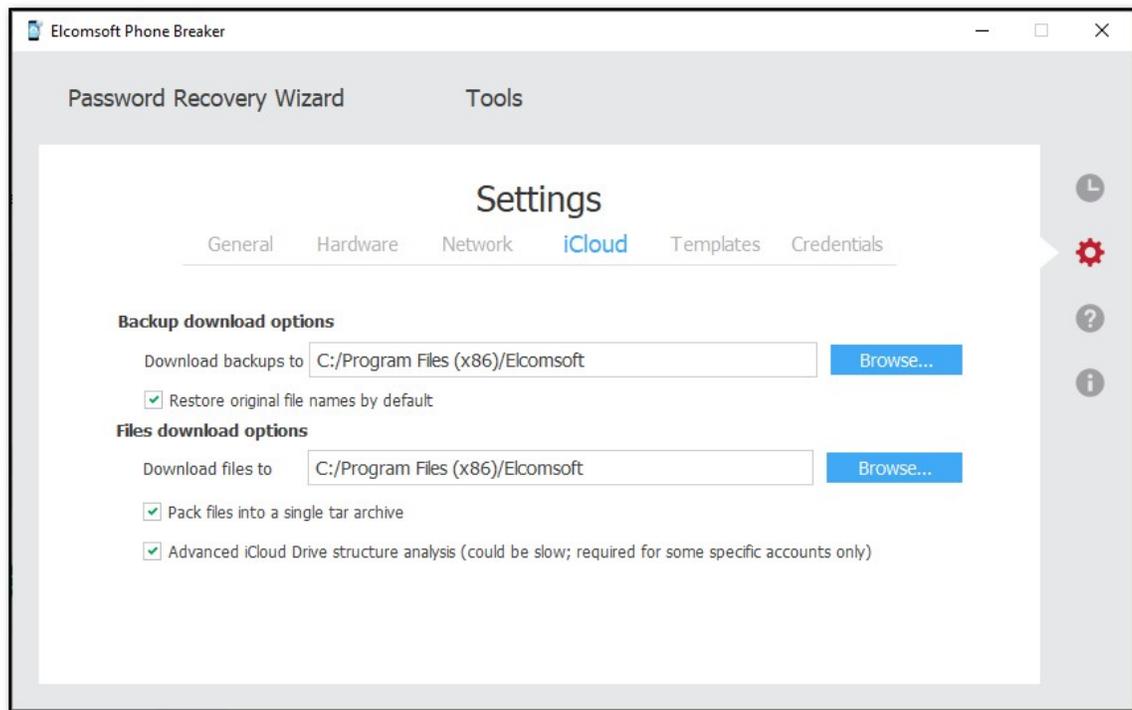
- **Download backups to:** Select the default folder where the backup will be saved.
- **Restore original file names by default:** Allows viewing the folder and file names in the restored backup as they were on the device. If you uncheck this option, the files will still be available after decryption, 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.
- **Advanced iCloud Drive structure analysis:** Allows obtaining an additional information for downloading data from iCloud Drive and iCloud synced data.

**NOTE:** If this option is selected, the downloading process can take a long time. It is required for some specific accounts only.



- **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.

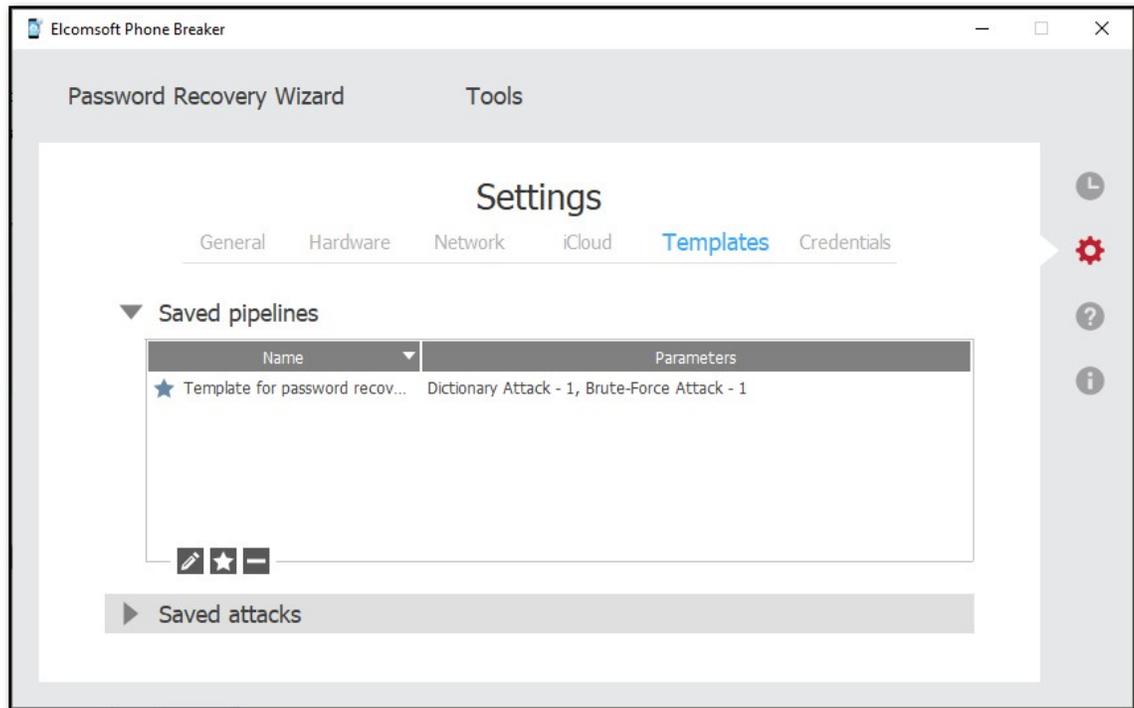
The process of recovering the password is made up of attacks. A combination of attacks is called a pipeline. See [Password recovery attacks](#) section for more details.

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.

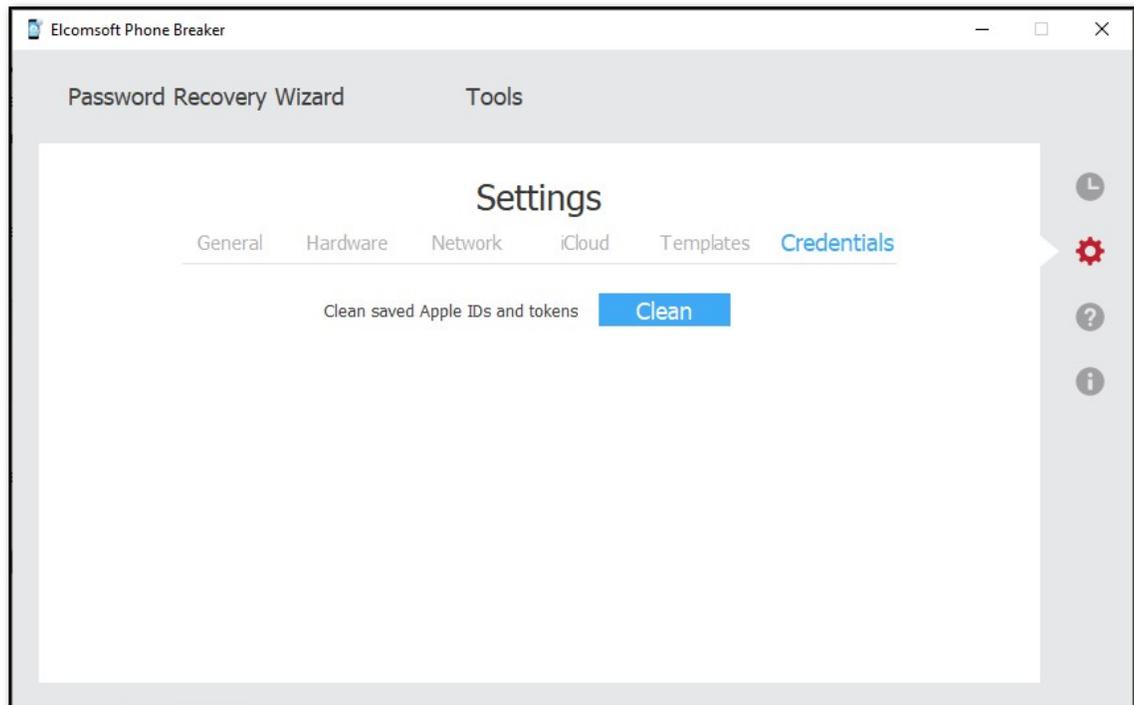
To set the template as default, click the  button. Default template will be displayed first every time the **Password recovery** option is used.

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



- **Credentials**

Click the **Clean** button to clean saved credentials or tokens.



### 3.1.3 [Windows] Hardware acceleration

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

For Apple devices running iOS 10 and higher, password recovery speed is increased only on CPU.

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

**NOTE: Only NVIDIA cards with Compute Capability from 3.0 to 7.0 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 600-, 700-, 900-, 1080-, TITAN, TITAN Black, TITAN Z, and TITAN X
- GeForce GT 600-, 700-

Laptop products:

- GeForce GTX 600-, 700-, 800-, and 900-
- GeForce GT 600-, 700-
- GeForce 700-, and 800-

The following cards are not supported: GeForce GT 610, GeForce 610M, GeForce GT 620, GeForce GT 620M, GeForce GT 625M, GeForce GT 630, GeForce GT 630M, GeForce GT 635M, GeForce GT 640 (GDDR3), GeForce GTX 670M, GeForce GTX 675M, GeForce 710M, GeForce GT 720M, GeForce 820M

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 the 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 an NVIDIA or AMD card to use with **EPB**, you should also have the latest drivers installed (supported operating systems: Windows 10, Windows 8.1, Windows 8, Windows 7, Windows Server 2016, Windows Server 2012, Windows Server 2008 R2; 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).**

## 3.2 Working with Apple devices

### 3.2.1 Useful links

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

[iCloud: Back up your iOS device to iCloud](#)

[iCloud: Restore your iOS device from iCloud](#)

[iCloud: Troubleshooting restoring an iCloud backup](#)

[iCloud: iCloud storage and backup overview](#)

[iOS: Unable to restore from backup of a newer device](#)

[iOS: Back up and restore your iOS device with iCloud or iTunes](#)

[iTunes: About iOS backups](#)

[iTunes: About encrypted backups in iTunes](#)

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

[Recovering iCloud contacts, calendars, and bookmarks from an iTunes backup of an iOS device](#)

[iOS: If you can't back up or restore from a backup in iTunes](#)

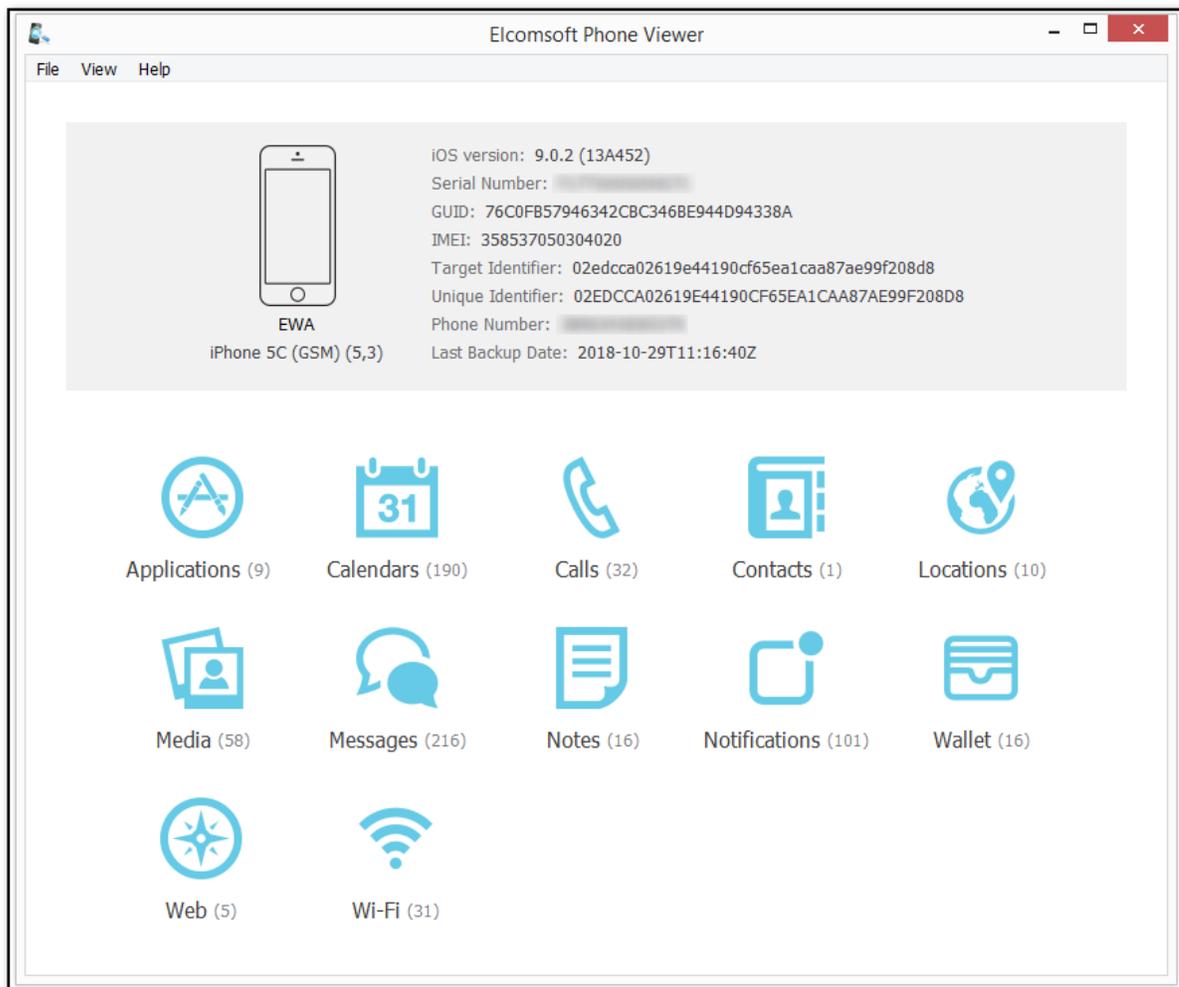
[iCloud: iCloud security and privacy overview](#)

[Get a verification code and sign in with two-factor authentication](#)

### 3.2.2 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:

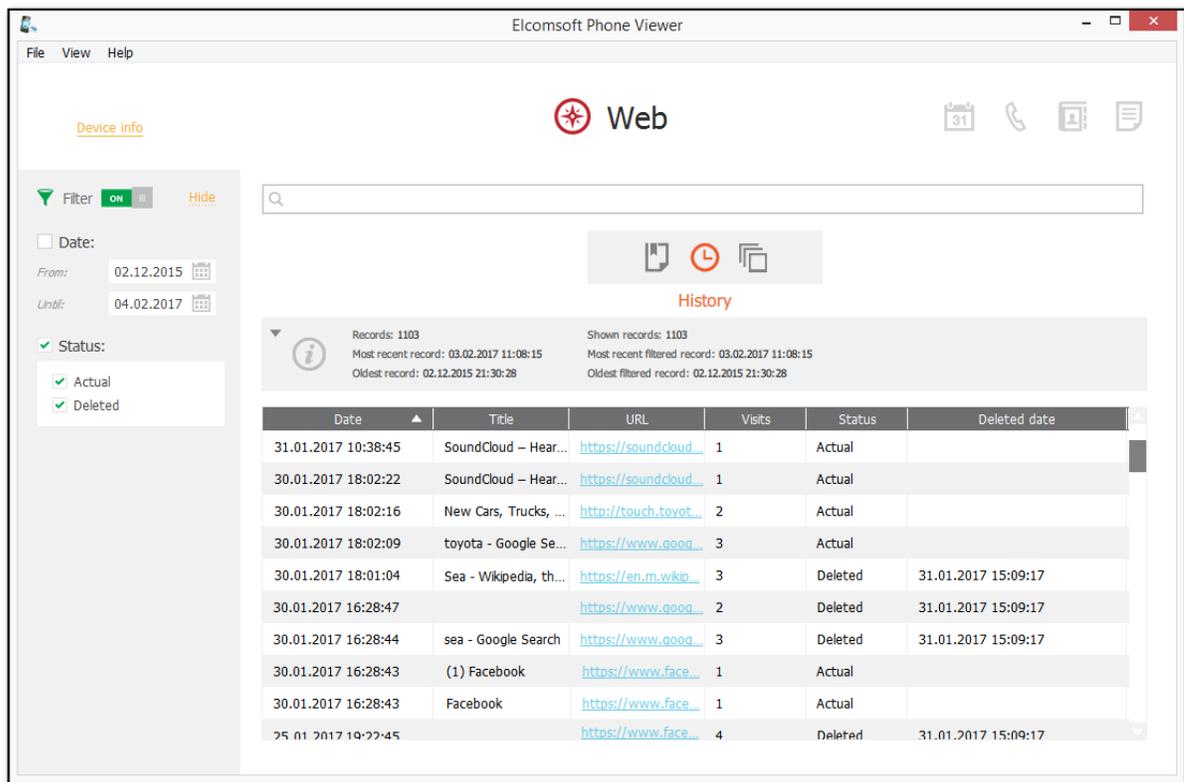
- Information about the device, such as:
  - Model name
  - Serial number
  - Phone number
- Data stored in the backup, such as:
  - Applications
  - Calendar data
  - Contacts
  - Call logs
  - Locations
  - Messages
  - Notes
  - Notifications
  - Multimedia files
  - Wallet data
  - Web browsing data
  - Wi-Fi connections
- 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 synced Microsoft account data, which makes it an ideal companion for Elcomsoft Phone Breaker.

### 3.2.3 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 on the websites and in some other applications.

EPB is able to decrypt keychain data from password-protected backups (iOS 4 and later) if the backup password is known (or has been [recovered](#) using EPB for Windows). For iTunes backups that do not have the password set, as well as for iCloud backups, keychain can be decrypted only if the "security key" is known. That key is unique for every device and is not available in the backup. It can be obtained from 32-bit devices (up to iPhone 5/5C) using the physical acquisition method, e.g. with [Elcomsoft iOS Forensic Toolkit](#).

**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, which is why it is recommended to not 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

**EPB** also allows you to explore keychain data downloaded from iCloud Keychain (*iCloud\_Keychain.xml* file) or [iCloud synced data](#) (*icloud\_synced.xml* file).

With **EPB**, you can also explore the keychain dump downloaded via [Elcomsoft iOS Forensic Toolkit](#). The downloaded file name is *keychaindump.xml* by default.

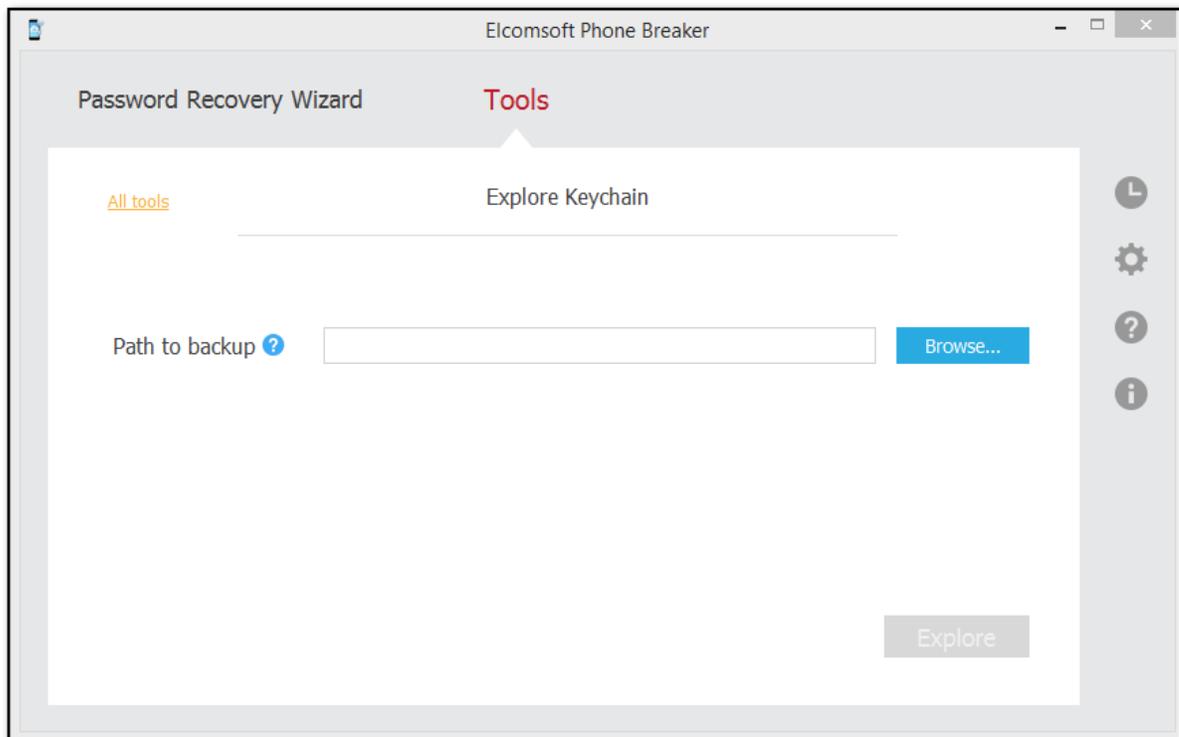
**To explore the keychain**, do the following:

1. In the **Tools** menu, select the **Apple** tab, and click **Explore keychain**.
2. Click **Browse** to navigate to the necessary file:

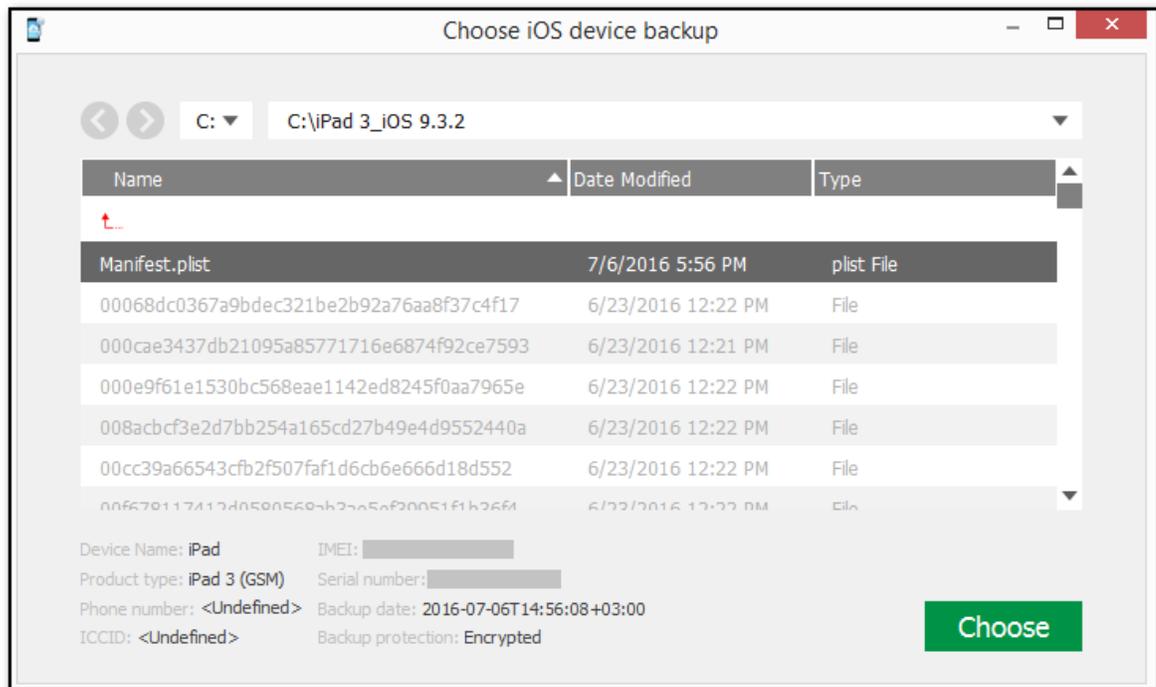
Source	File
iTunes/iCloud backup	<i>Manifest.plist</i>
Keychain data downloaded from iCloud Keychain (EPB 9.50 and lower)	<i>iCloud_Keychain.xml</i>
Keychain data downloaded from <a href="#">iCloud synced data</a> (EPB 9.60 and later)	<i>icloud_synced.xml</i>
Keychain dump downloaded via <a href="#">Elcomsoft iOS Forensic Toolkit</a>	<i>keychaindump.xml</i>

**NOTE:** You can also drag-and-drop the *Manifest.plist* file to the Explore Keychain page.

**NOTE:** On macOS 10.14 and higher, you need to grant the Full Disk Access permission to EPB to have access to the default iTunes backups folder. For details, see [Troubleshooting](#).

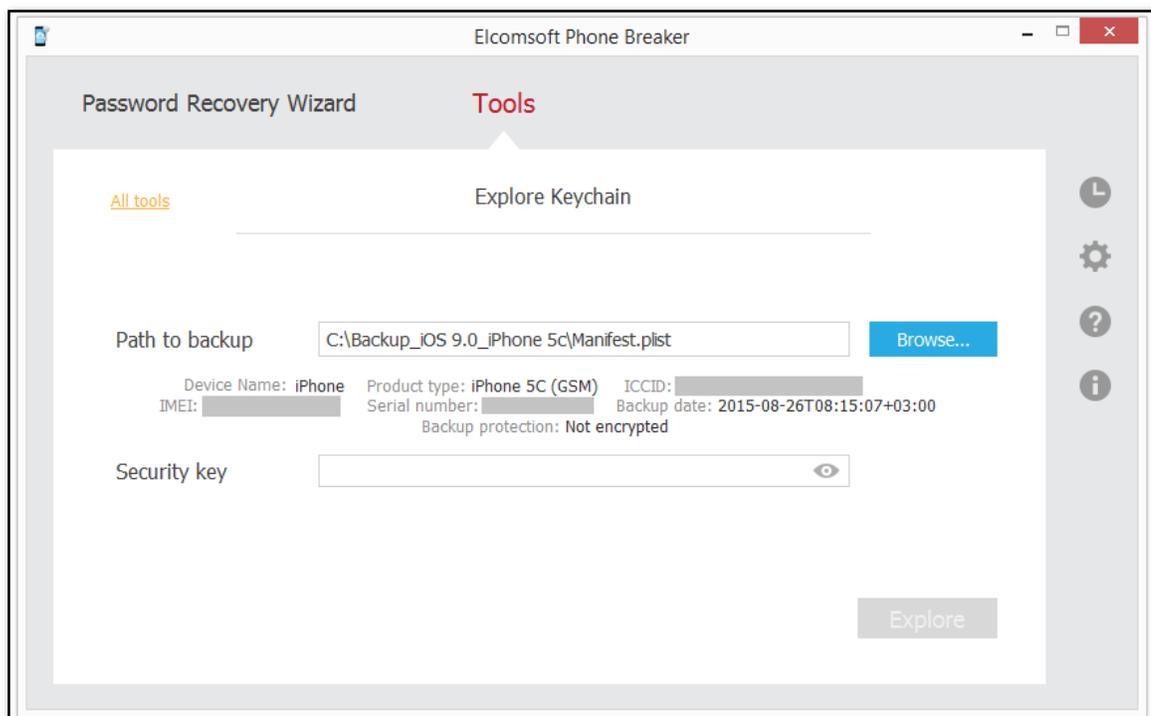


3. Select the file, and then click **Continue**.



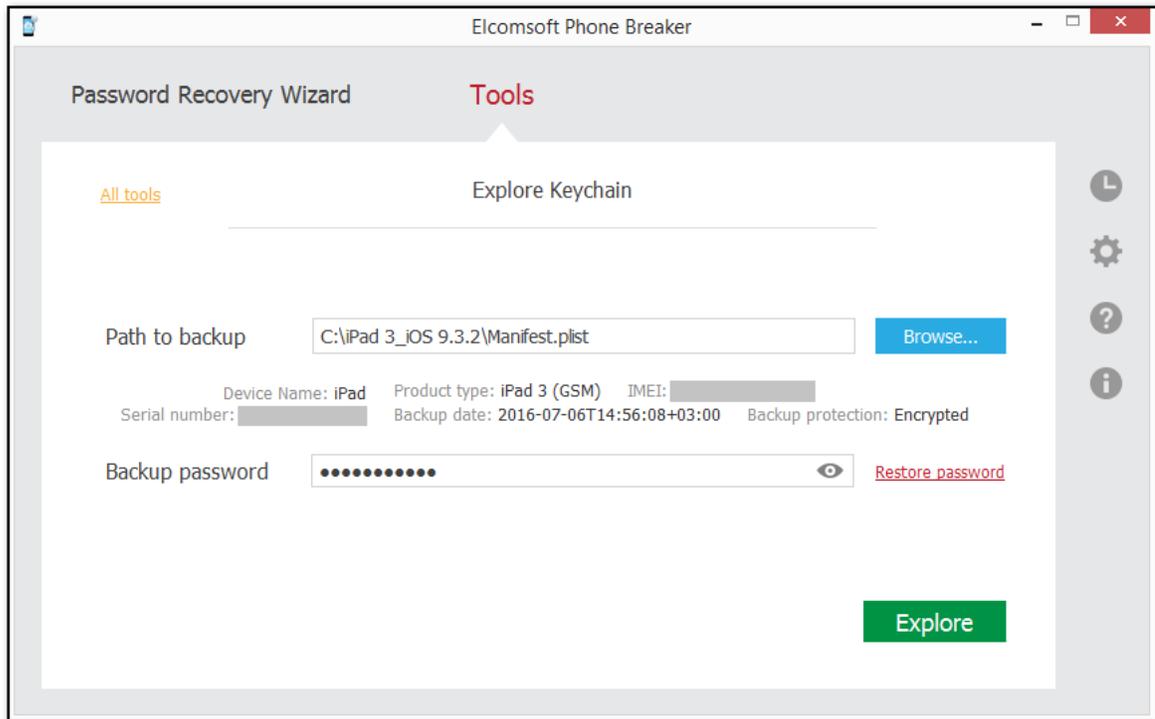
4. Depending on whether the backup is encrypted or not, do one of the following:

- **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. Click the **View**  button to display the password.

If you have not recovered it yet and you are using EPB on Windows OS, click **Restore password** to [recover the password](#) to the backup.



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

5. The passwords are stored in categories in the Keychain Explorer. Each category contains the following information:

Category	General Information for all categories	Category-Specific Information
Apple IDs	<ul style="list-style-type: none"> <li>○ Name: the source for which the data is saved in the keychain.</li> <li>○ Creation date</li> <li>○ Modification date</li> </ul>	<ul style="list-style-type: none"> <li>○ Apple ID (Account)</li> <li>○ Password</li> </ul>
Wi-Fi accounts		<ul style="list-style-type: none"> <li>○ SSID (Account)</li> <li>○ Password</li> </ul>
Mail accounts		<ul style="list-style-type: none"> <li>○ Protocol</li> <li>○ Account</li> <li>○ Password</li> </ul>
Browser passwords		<ul style="list-style-type: none"> <li>○ Address</li> </ul>

		<ul style="list-style-type: none"> <li>○ Account</li> <li>○ Password</li> </ul>
Credit cards		<ul style="list-style-type: none"> <li>○ Card name</li> <li>○ Cardholder name</li> <li>○ Card number</li> <li>○ Expiration date</li> </ul>
DSIDs & Tokens		<ul style="list-style-type: none"> <li>○ Token</li> <li>○ DSID</li> </ul>
Other		All available records that did not fit into any of the categories mentioned above.

6. The information about passwords is displayed in the three views:

- **Tree view:** This view is displayed by default and can be selected by clicking the  icon. This view displays all keychain records (including not-encrypted records).

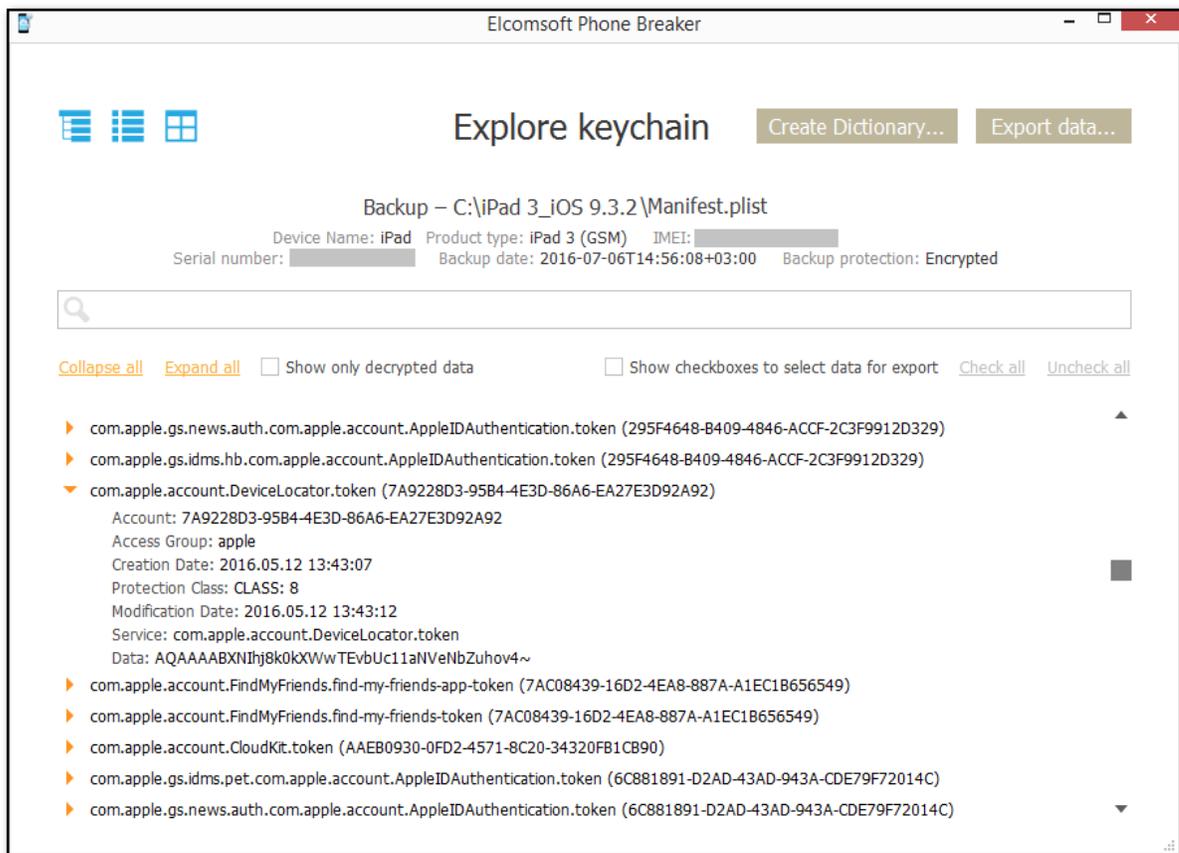
To hide non-decrypted data, select the **Show only decrypted data** check box. This option will leave you with only useful decrypted information while exploring encrypted backups.

To expand the required record, click the orange arrow next to it. Thus, you you will be able to view all information associated with it.

To expand all records, click **Expand all**.

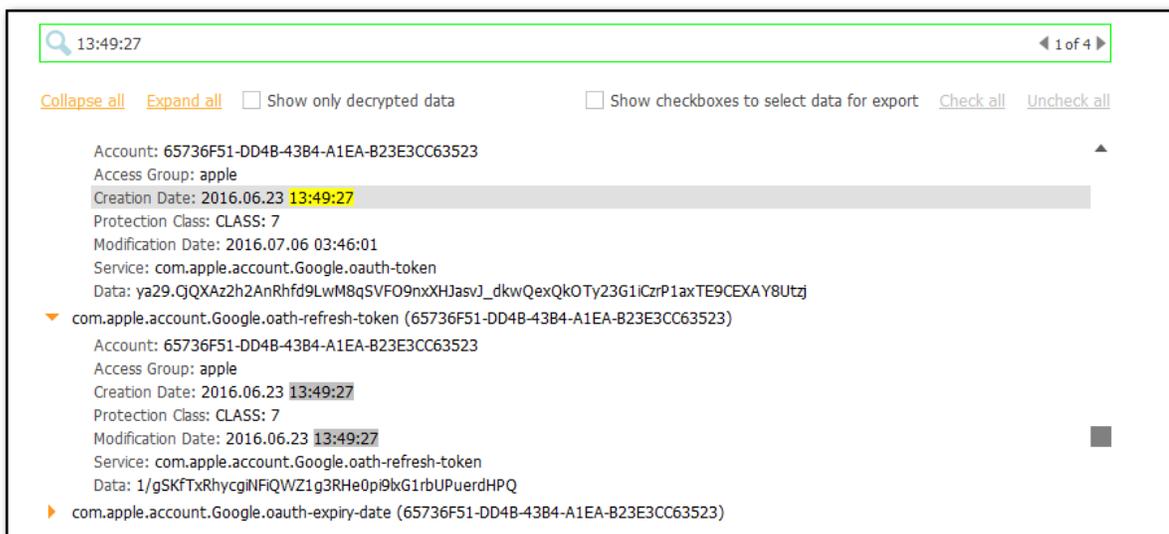
To collapse all records, click **Collapse all**.

To mask passwords with asterisks, go to [EPB Settings](#) and select the **Mask passwords in Explore keychain** check box.

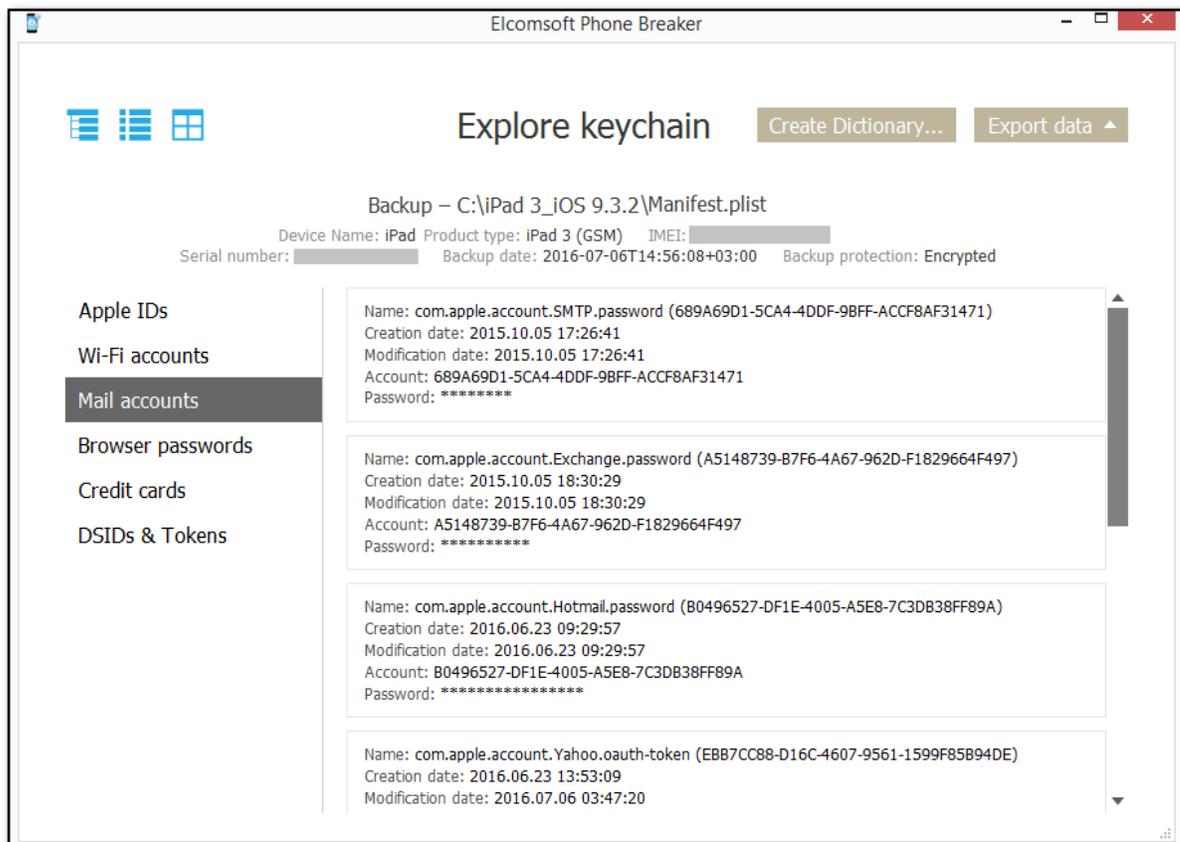


You can perform searches in the Keychain data by entering required expressions in the **Search** field and pressing **Enter**. The search results will be highlighted in yellow.

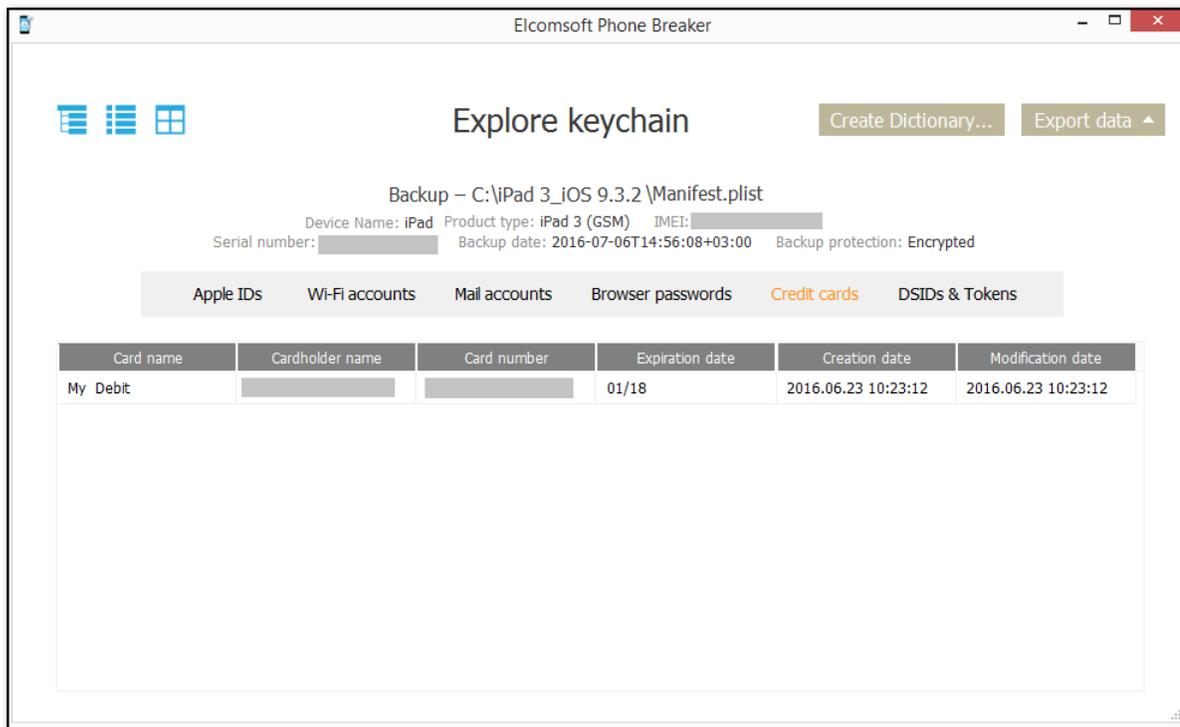
If there are several search results matching the entered expression, you can navigate between them by clicking the arrows in the **Search** field.



- **Category view:** This view is selected by clicking the  icon. It displays the keychain records sorted by category.



- **Grid view:** This view can be selected by clicking the  icon. To sort data in the grid, click the necessary column header.



## Exporting data

You can export all keychain data or keychain data from a selected category.

**To export the data displayed in a Tree view**, do the following:

1. Select the **Show checkboxes to select data for export** option.
2. Select the check boxes next to the records you wish to export or click the **Check All** option to select all records.
3. Click **Export Data** in the upper right corner of the program window and then select one of the following options: **All** or **Selected**.
4. In the opened window, select the location to which the file must be saved.
5. Click **Save**.
6. The default name for the exported file is **keychain\_export.xml**.

**To export the data displayed in the Categories or the Grid view**, do the following:

1. Click **Export Data** in the upper right corner of the program window and then select one of the following options: **All** or **Selected Category**.
2. In the opened window, select the location to which the file must be saved and the format of the exported file in the **Save as type** drop-down list.

3. Click **Save**.

4. The default name for the file with all exported keychain data is **keychain\_export.xml**.

The default name for the file with partially exported keychain data is **keychain\_export\_<category\_name>.xml** or **keychain\_export\_<category\_name>.csv**.

### Creating dictionary

You can generate a dictionary from all passwords in the keychain, despite the selected category and view. The dictionary is a file in TXT format that can later be used as a dictionary for [password recovery](#).

To create a dictionary, click **Create dictionary** in the upper right corner of the program window, select the location to which the file must be saved in the opened window, and then click **Save**.

The default name for the dictionary file is **keychain\_passwords.txt**.

## 3.2.4 Working with iTunes backup

### 3.2.4.1 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:

- **macOS:** /Users/(username)/Library/Application Support/MobileSync/Backup/
- **Windows 7, Windows 8, Windows 8.1, and 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** (for iOS 10 and higher, the Manifest.db file located in the same folder is also needed). However, if you want to recover passwords and other data saved in Keychain, you need to have the complete device backup.

#### 3.2.4.2 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 macOS. You can [explore the backup content](#) with either restored or not restored file names in Elcomsoft Phone Viewer.

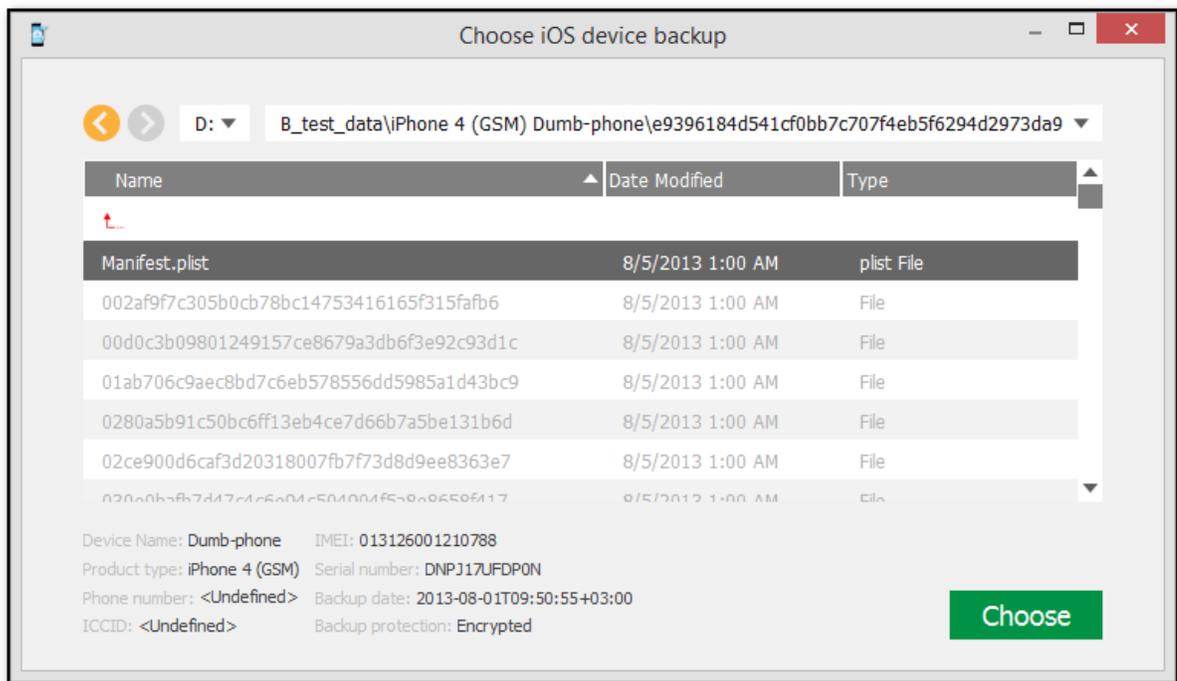
**To restore original file names of a non-encrypted backup**, do the following:

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**.

**NOTE: On macOS 10.14 and higher, you need to grant the Full Disk Access permission to EPB to have access to the default iTunes backups folder. For details, see [Troubleshooting](#).**

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.

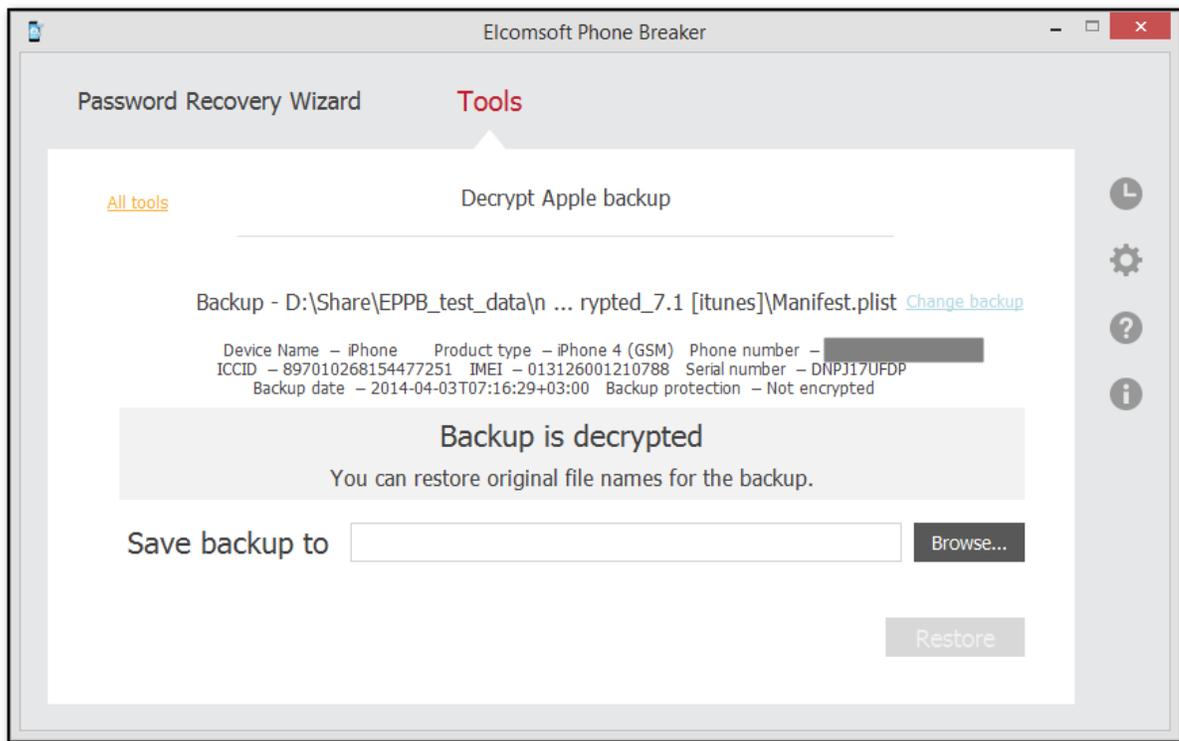


5. When the backup is loaded, you can view the following information about backup:

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

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

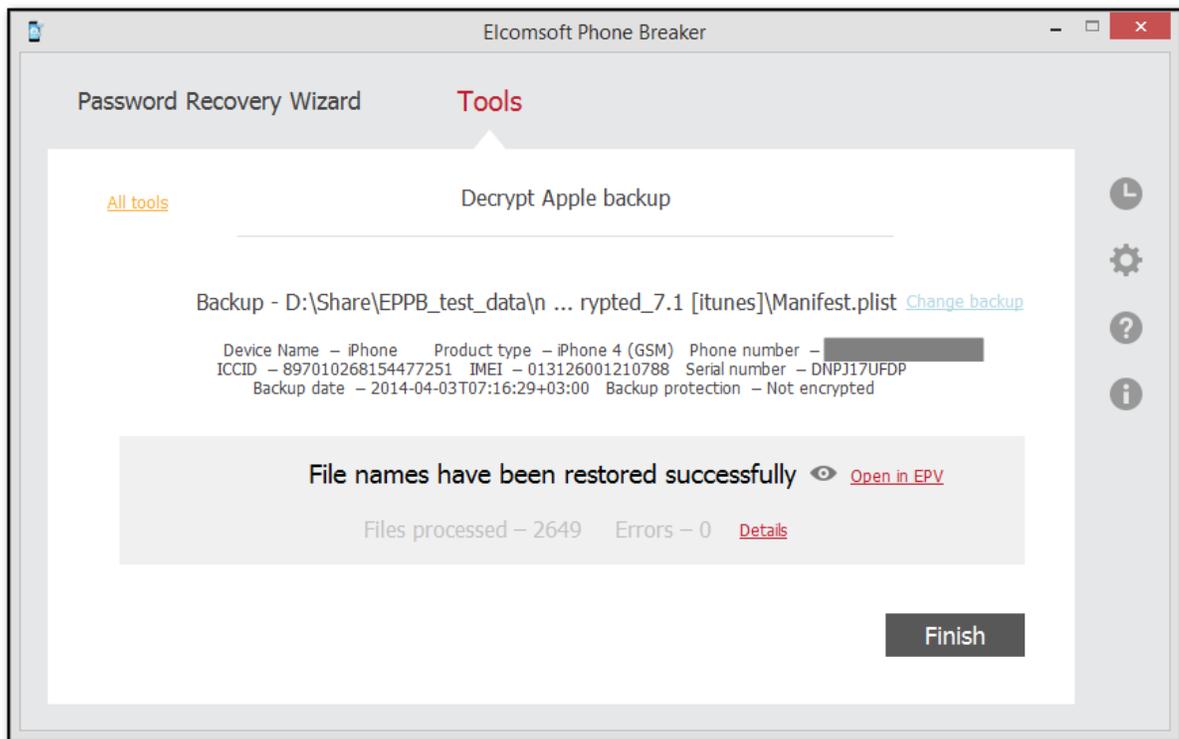
You can select a different backup by clicking **Change backup** next to the backup name.



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

**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.

If you have Elcomsoft Phone Viewer installed on your computer, you can explore the backup content by clicking the **Open in EPV** link.

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.

### 3.2.4.3 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.

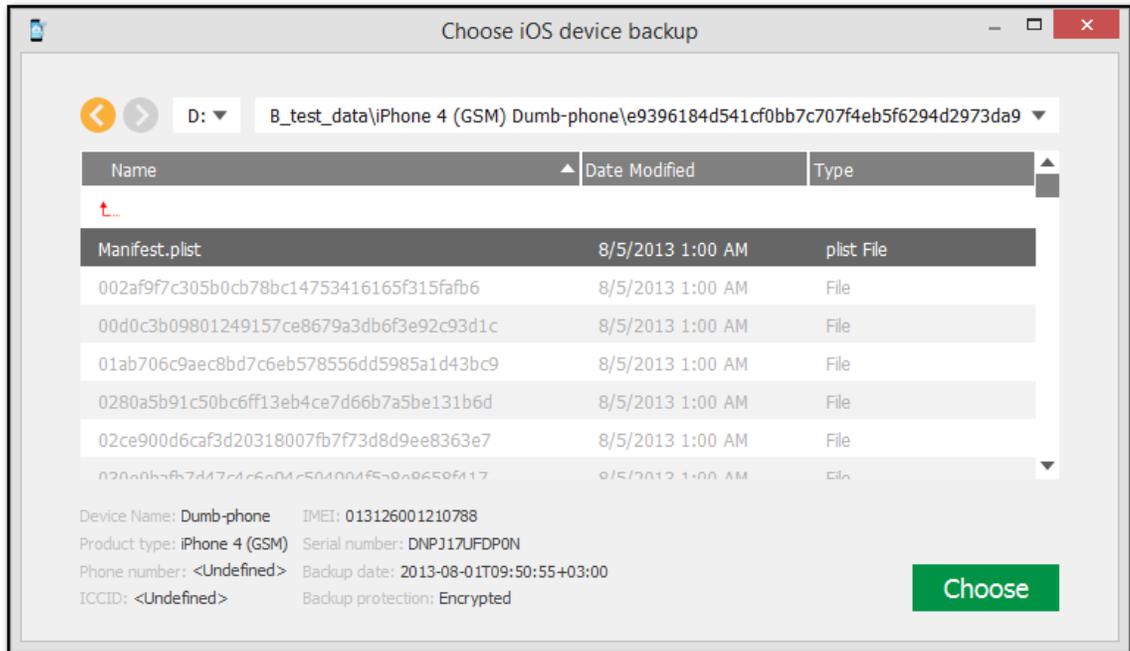
**To decrypt a backup stored on a currently investigated computer**, do the following:

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**.

**NOTE: On macOS 10.14 and higher, you need to grant the Full Disk Access permission to EPB to have access to the default iTunes backups folder. For details, see [Troubleshooting](#).**

- 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.

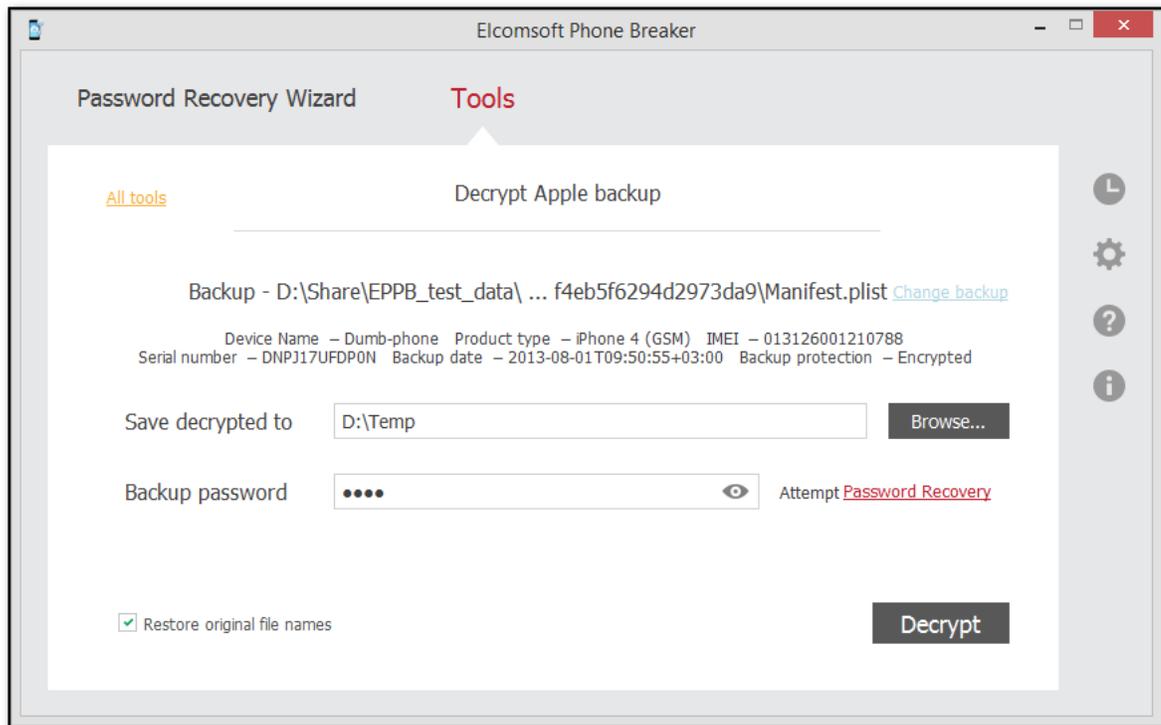


- When the backup is loaded, you can view the following information about backup:

- **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.



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.

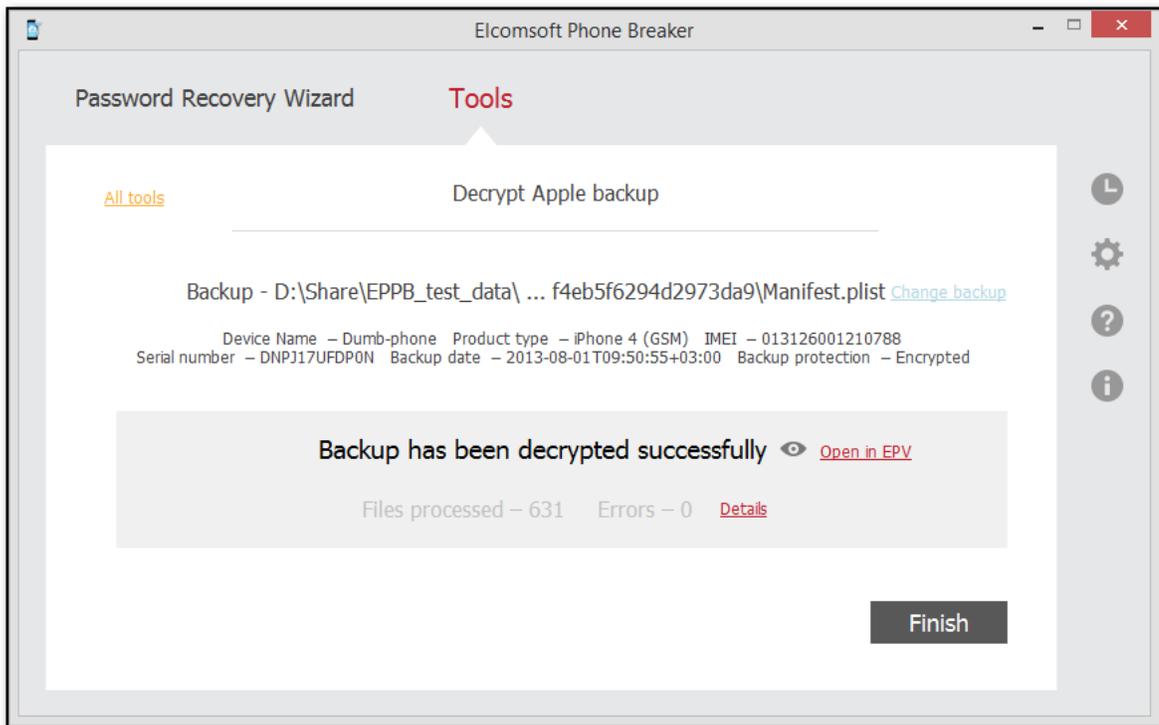
- **Restore original file names:** Allows viewing the folder and file names in the restored backup as they were on the device. If you uncheck this option, the files will still be available after decryption, however, their names will be crypted.

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.

If you have Elcomsoft Phone Viewer installed on your computer, you can explore the backup content by clicking the **Open in EPV** link.

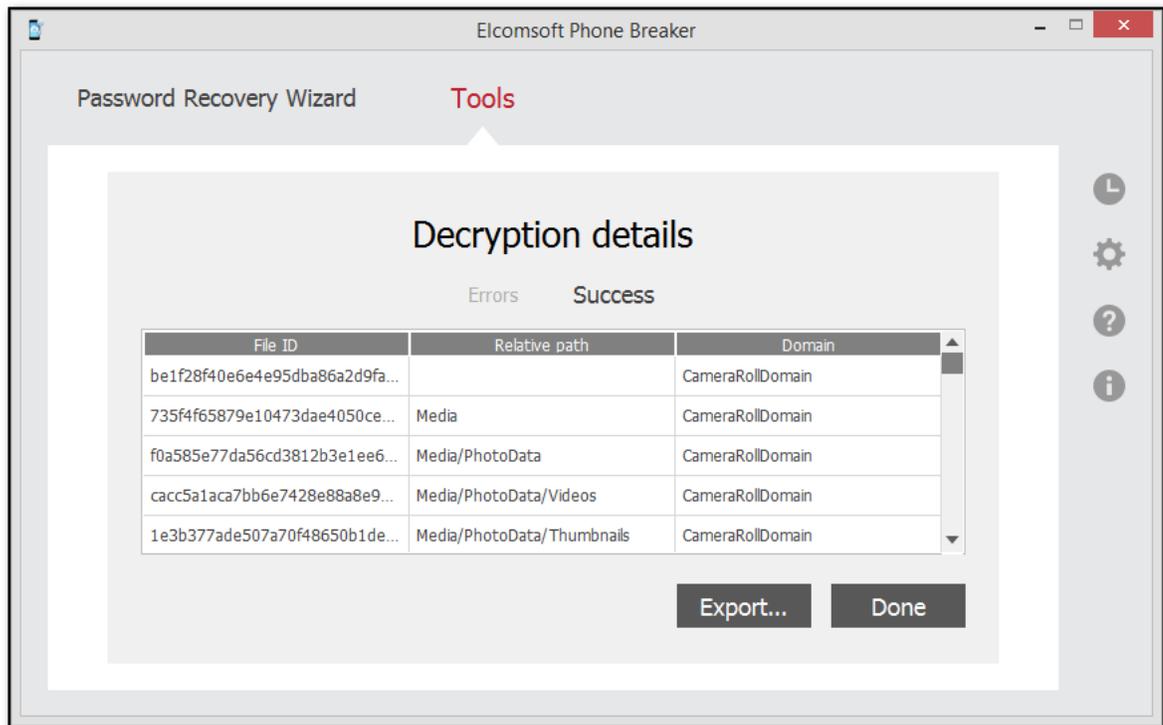


11. To view detailed [report](#) about decrypted files and errors that occurred during decryption, click **Details**.
12. Click **Finish** to close the **Decrypt backup** window.

#### 3.2.4.4 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**.

## 3.2.5 Working with iCloud data

### 3.2.5.1 Working with iCloud backups

#### 3.2.5.1.1 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.

### 3.2.5.1.2 Downloading iCloud backups

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.

EPB allows you to download iCloud backups created on iOS up to 14 (incl.).

**To download an 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.

**NOTE: Only backups created on iOS versions lower 11.2 can be downloaded using the tokens. In this case the Authentication token without limitations for the account with two-factor authentication or Authentication token for the account without two-factor authentication should be used.**

The screenshot shows the 'Tools' menu in Elcomsoft Phone Breaker. The 'Download backup from iCloud' page is active, featuring a 'Password' tab selected over a 'Token' tab. The form includes fields for 'Apple ID' and 'Password', a 'Save credentials for future use' checkbox, and a 'Sign in' button.

4. Click **Sign in**.

**NOTE: If you have entered the Apple ID in a wrong format, a message about the account being locked will be displayed. Close the message and try again. Please make sure to enter your apple ID in the standard format (i.e., [example@example.com](mailto:example@example.com)).**

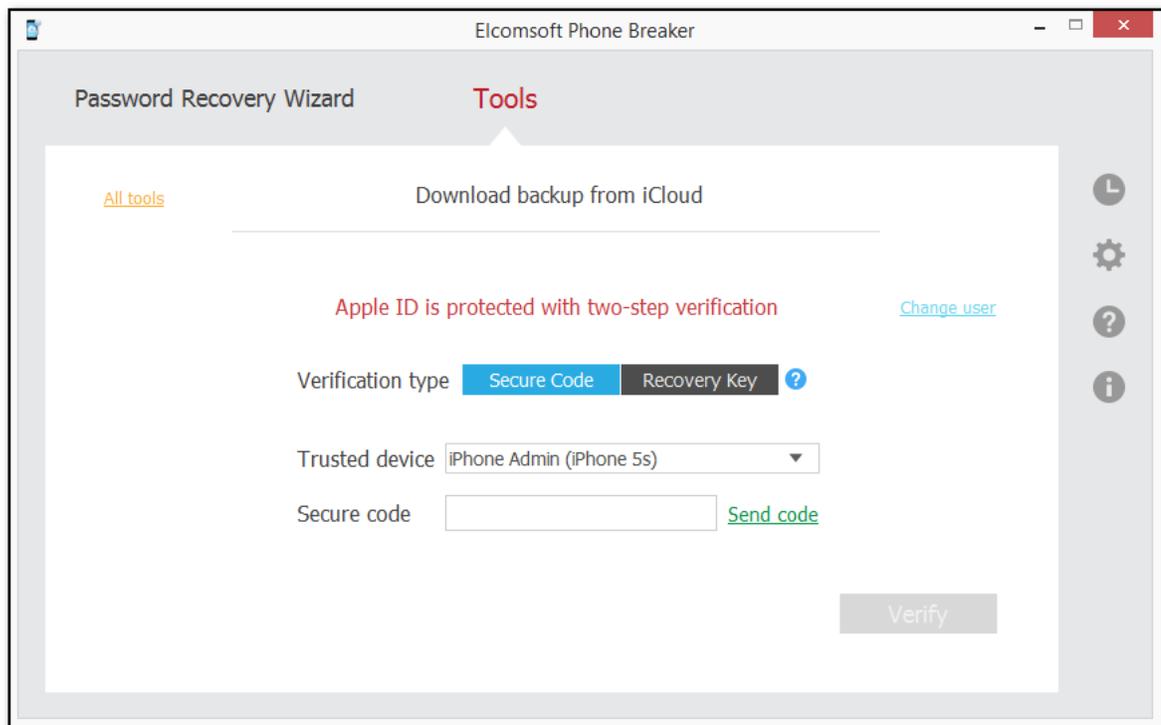
**NOTE: If the Apple ID is protected with two-factor authentication, you need to confirm sending the verification code to all of your trusted devices or to your phone.**

You can select the **Save credentials for future use** option when logging in so that you don't need to enter them when you log in with this Apple ID again.

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. Click **Verify**.



7. If the Apple ID is protected with two-factor authentication, perform authentication in one of the following ways:

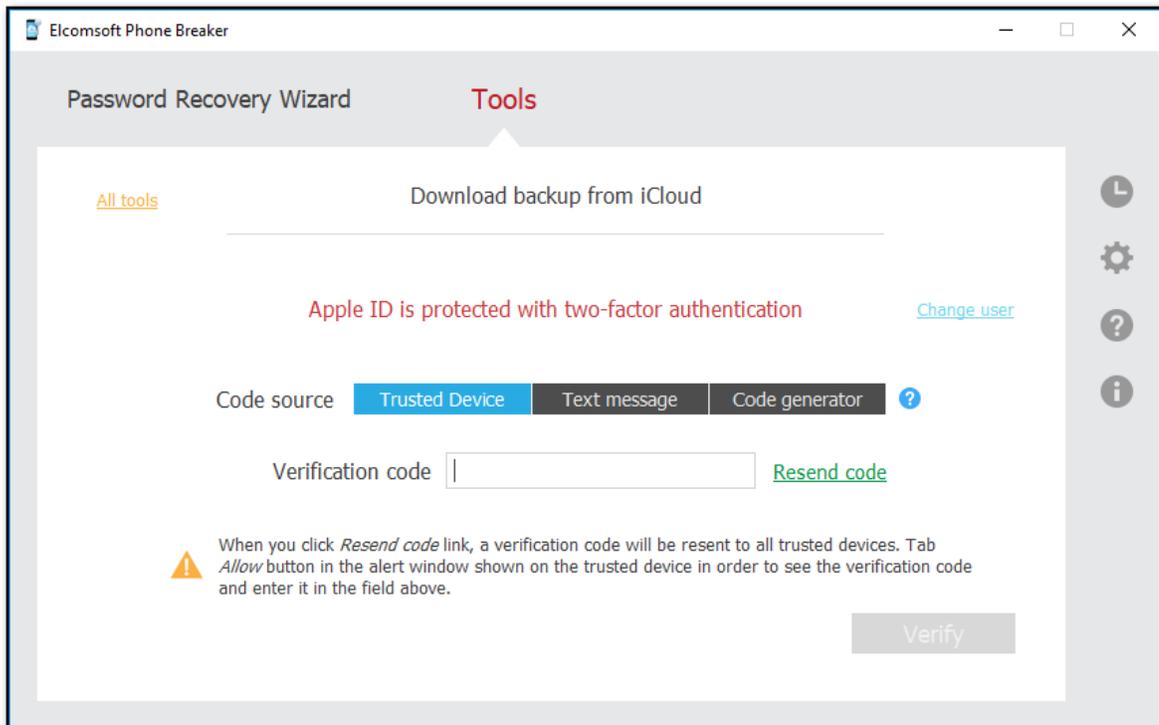
- Select **Trusted Device** and enter the 6-digit code in the **Verification code** field. Click **Resend code** for the verification code to be sent to all trusted devices.

- Select **Text message** and enter the 6-digit code in the **Verification code** field. Click **Send code** for the verification code to be sent as a text message to the selected trusted phone number. Click **Resend code** for it to be sent again.

**NOTE: macOS 10.12 or higher is required for sending text messages.**

**NOTE: Authentication via the Text message is available for the Forensic edition only.**

- Select **Code generator** and enter the 6-digit code in the **Verification code** field. The code is generated on the trusted device or via Cloud Panel.

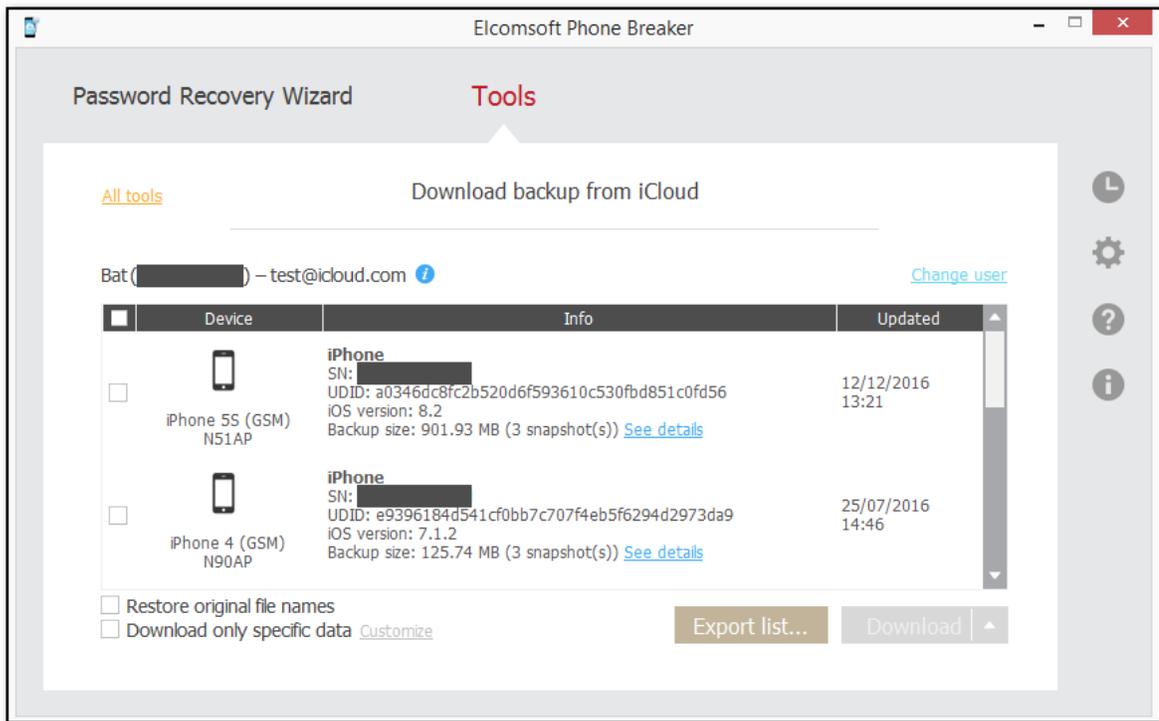


8. Click **Verify**.

9. 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 blue *i* icon to view the storage capacity and used size.

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

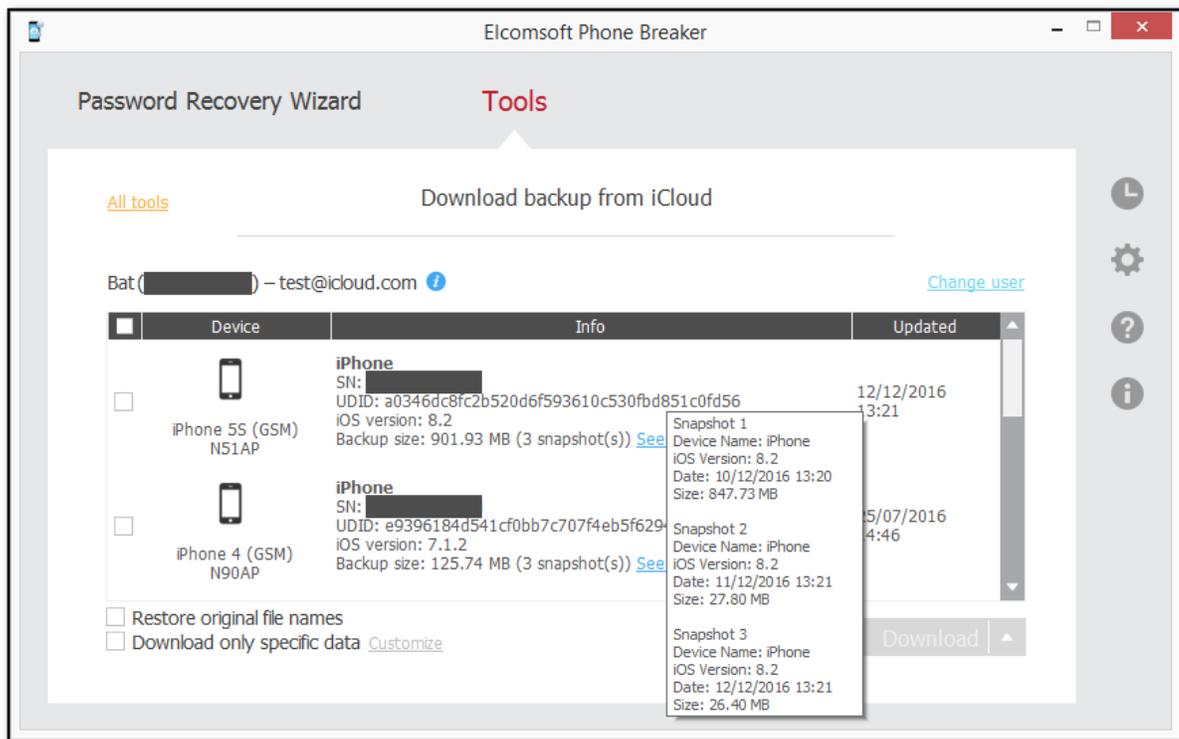


For every device, the following information is displayed:

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

**NOTE: The time is stated as it is (was) set on the device.**

To view snapshot details for a device, click **See details**.



For every snapshot, the following information is displayed:

- Device Name
- iOS version
- Date when the snapshot was made
- Size of the snapshot

**NOTE: For the snapshots other than the first one, the displayed size is the size of the data added by the time the snapshot was saved, not the snapshot itself.**

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

11. Define the options for downloading backups. Hover over check boxes 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, the 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 the downloaded backups with [Elcomsoft Phone Viewer](#) (if you are holding a license on **EPB**, you can get a discount on iBackupBot; [contact us](#) for more details) or any 3rd party software that supports iTunes backup format. 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.

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

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

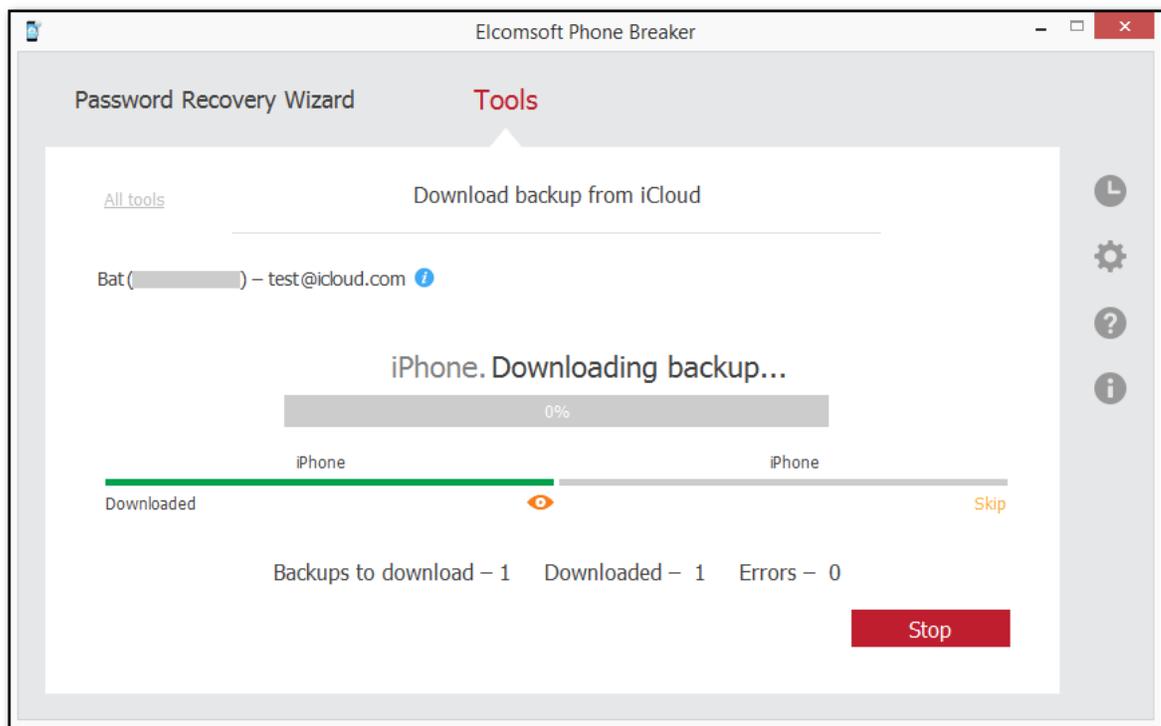
14. Downloading of the iCloud backup begins.

**NOTE: If by this moment the token has expired, you will not be able to use it to download backups. However, using the expired token you can still download iCloud Files, and synced data.**

**You will have the following options:**

- **Log in again to generate a new token for further downloading of backups**
- **Proceed with the expired token to download iCloud Files, and synced data.**

15. If you have selected several backups, you can click **Skip** to skip downloading either of them.

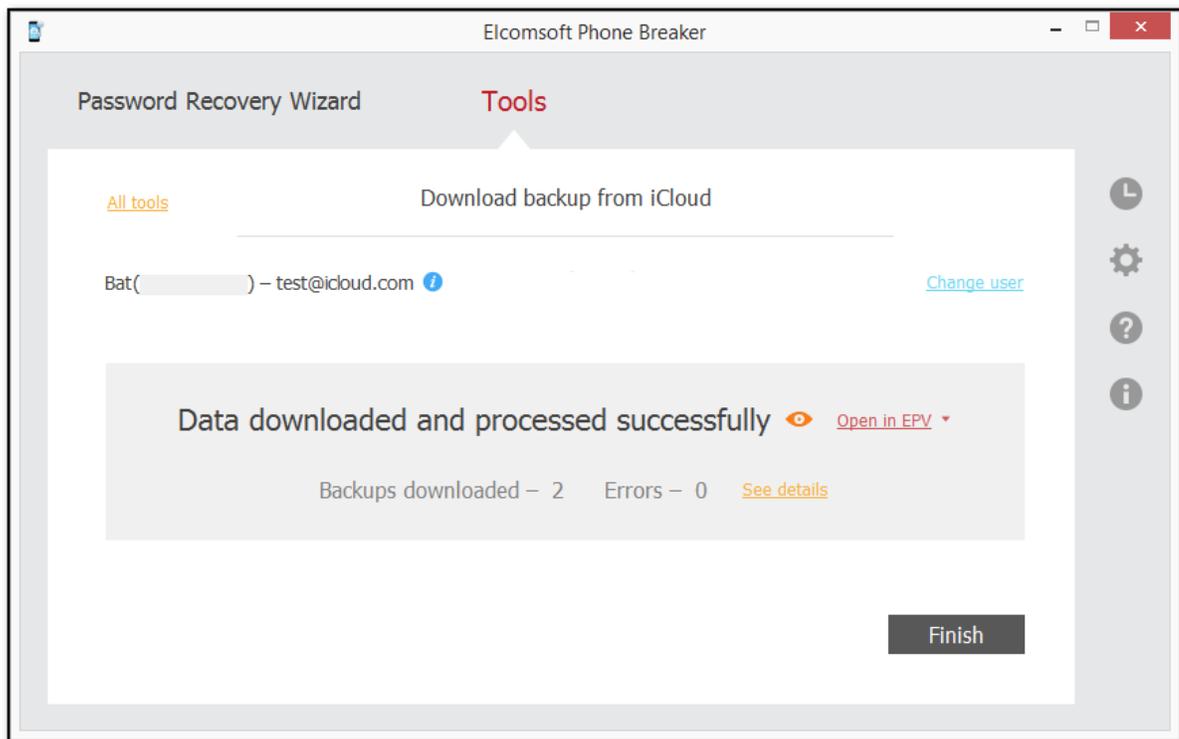


**NOTE: The backups that have not been completely created yet will not be downloaded.**

16. When downloading is finished, click the **View**  button to view the backup on the local computer.

If you have Elcomsoft Phone Viewer installed on your computer, you can explore the backup content by clicking the **Open in EPV** link.

If you have an older version of Elcomsoft Phone Viewer installed, update it to explore downloaded data.



17. Click **See details** to view the detailed information about the download process.

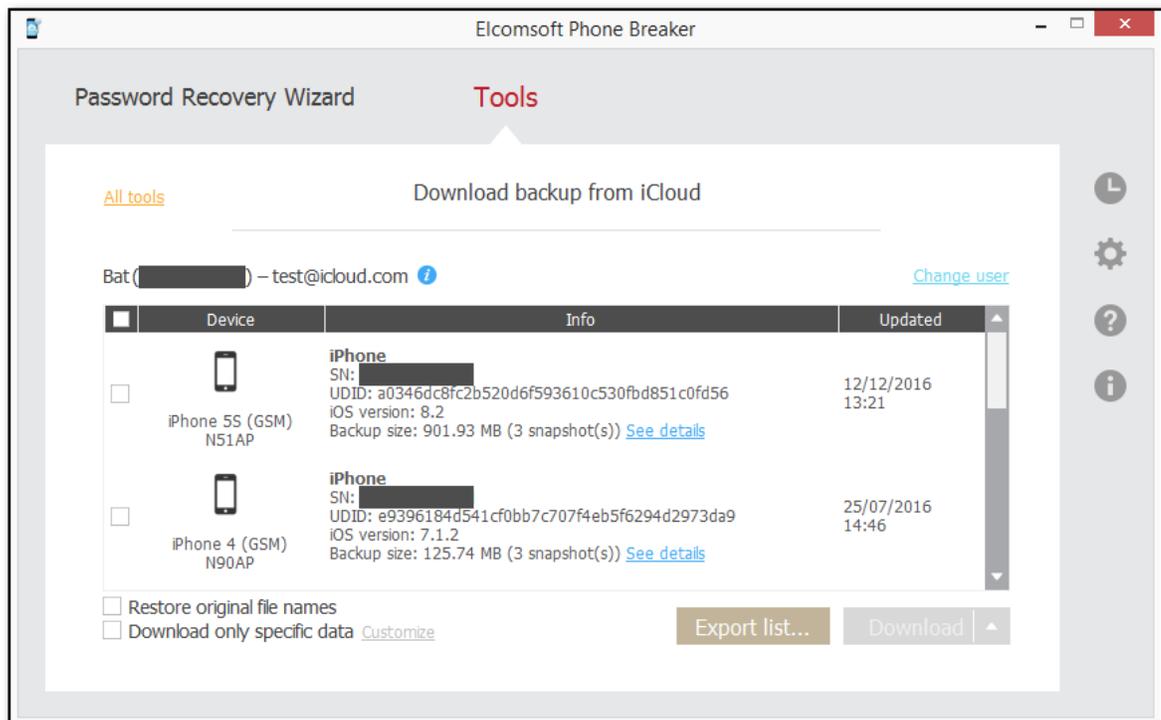
18. Click **Finish** to exit the downloading wizard.

Please note, backups starting with iOS 9.x.x and higher have a different structure from 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] [YYYYMMDD\_HHMMSSZ][R], where [YYYYMMDD\_HHMMSSZ] is the backup date and time stamp.
- For iOS 9.x.x and higher: in the folder with the name in the form [A30FD565-3776-4B8E-95AB-B4F06FD930BC][YYYYMMDD\_HHMMSSZ], where [YYYYMMDD\_HHMMSSZ] is the backup date and time stamp.

#### 3.2.5.1.3 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**.

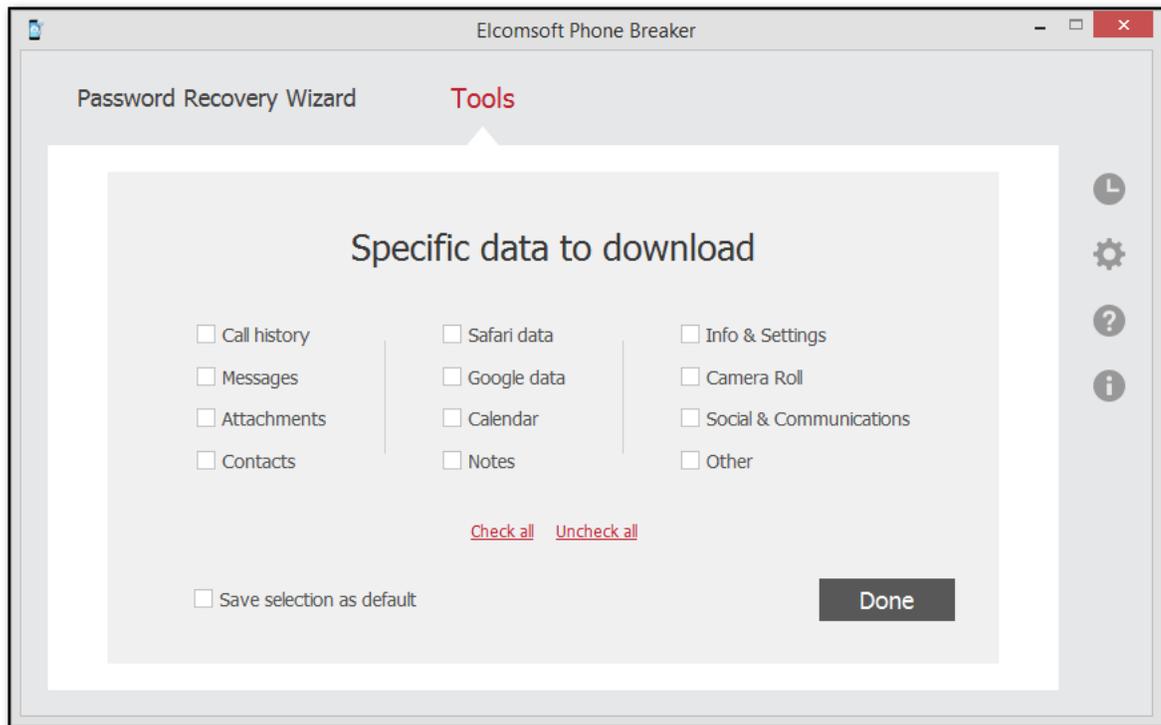
In the **Specific data to download** window, select the categories to be downloaded. If no category is selected, only the main backup files will be downloaded. These files are used to recover the backup structure. The main files include:

- Info.plist
- Manifest.mbdb / Manifest.db
- Manifest.plist
- Status.plist

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

**NOTE: The timezone data is always downloaded.**

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.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.mqq\  
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\location\  
\KeyboardDomain\Library\Keyboard

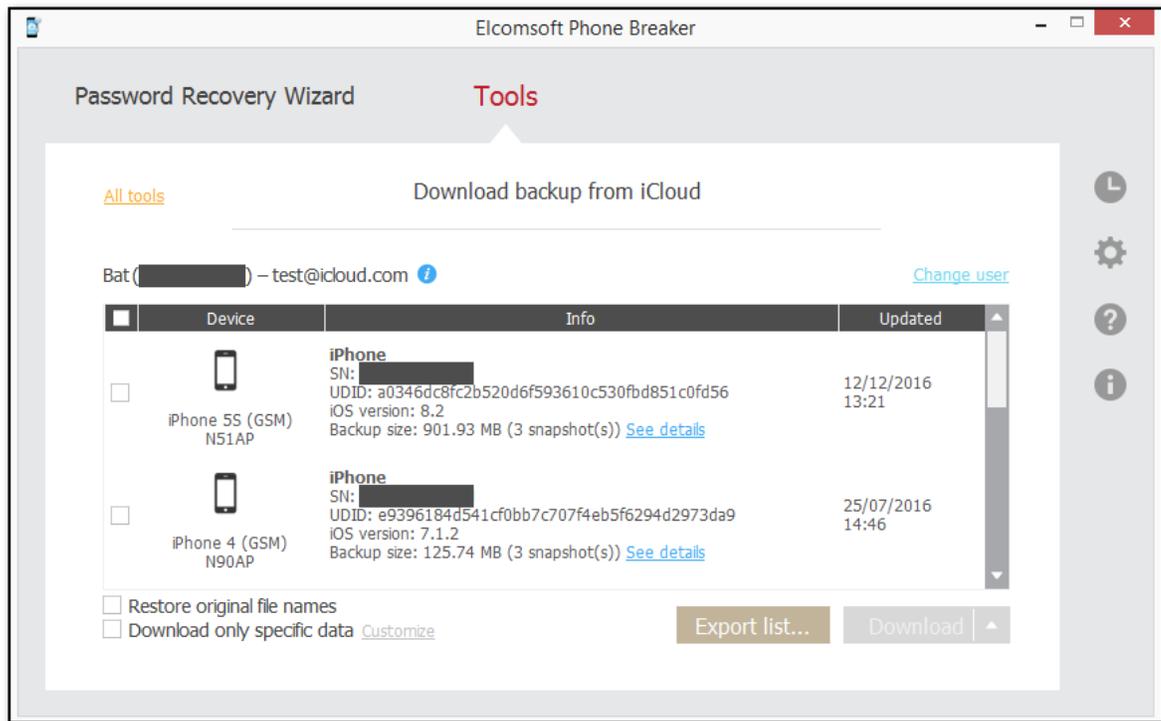
You can [explore the downloaded data](#) in Elcomsoft Phone Viewer.

#### 3.2.5.1.4 Exporting backup list

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

**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.

#### 3.2.5.1.5 Possible problems with downloading data from iCloud

Problem	Solution
When downloading the backup from iCloud, the following message is displayed: " <b>The requested backup could not be found</b> ".	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 iCloud services."	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. After that, you will be able to work with data from iCloud via EPB.

#### 3.2.5.1.6 iCloud backup structure

Once iCloud backups are downloaded and processed, the following folders are created in the destination folder (iOS 9.x and higher):

```
.chunks
<device ID>
  [backup ID][YYYYMMDD_HHMMSSZ]
```

```
...
[backup ID][YYYYMMDD_HHMMSSZ]
<device ID>
...
```

where the <device ID> is the unique ID of the device, and <backup ID> is the unique ID of a particular backup (usually as many as three latest backups are stored in the iCloud). [YYYYMMDD\_HHMMSSZ] is the date and time when the backup was created.

The .chunks folder is actually the 'cache' of the (raw) data downloaded that allows saving time when/if you download backups for the same device again.

Please note that in backups for iOS 10 and higher, each file with an unrestored name is stored in a subfolder whose name is the first two letters of the file name. E.g., a full path to the file named "fd4056e1b33b" will be the following:  
<backup\_root>/fd/fd4056e1b33b

For iOS 8 and older versions, downloaded data has a different structure:

```
.chunks
<device id>
.keys
[01]
...
[N]
[N+1]
[01][YYYYMMDD_HHMMSSZ]
...
[N][YYYYMMDD_HHMMSSZ]
[N+1][YYYYMMDD_HHMMSSZ]
```

The first three folders (with numbers used 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. In most cases, the first folder is the largest (and its total size is compared to the size of the device itself), the second one is much smaller, and the third one is the smallest.

The folders with the date/time in the names are 'complete' backups converted to the Apple iTunes format. Each of them has about the same size as the backup itself (as far as backups are usually created 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 the backup size because not all the data is downloaded).

**So the total size required for storing all backup(s) is usually five times more than the size of a single backup as shown on the device itself or by the program.**

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

**Example:**

Without the *Restore original file names* option:

```
.keys
```

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

or with the *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 on 24/11/1013, 26/11/2013 and 28/11/2013. The latest backups are in the [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. To view the content, we recommend using [Elcomsoft Phone Viewer](#).

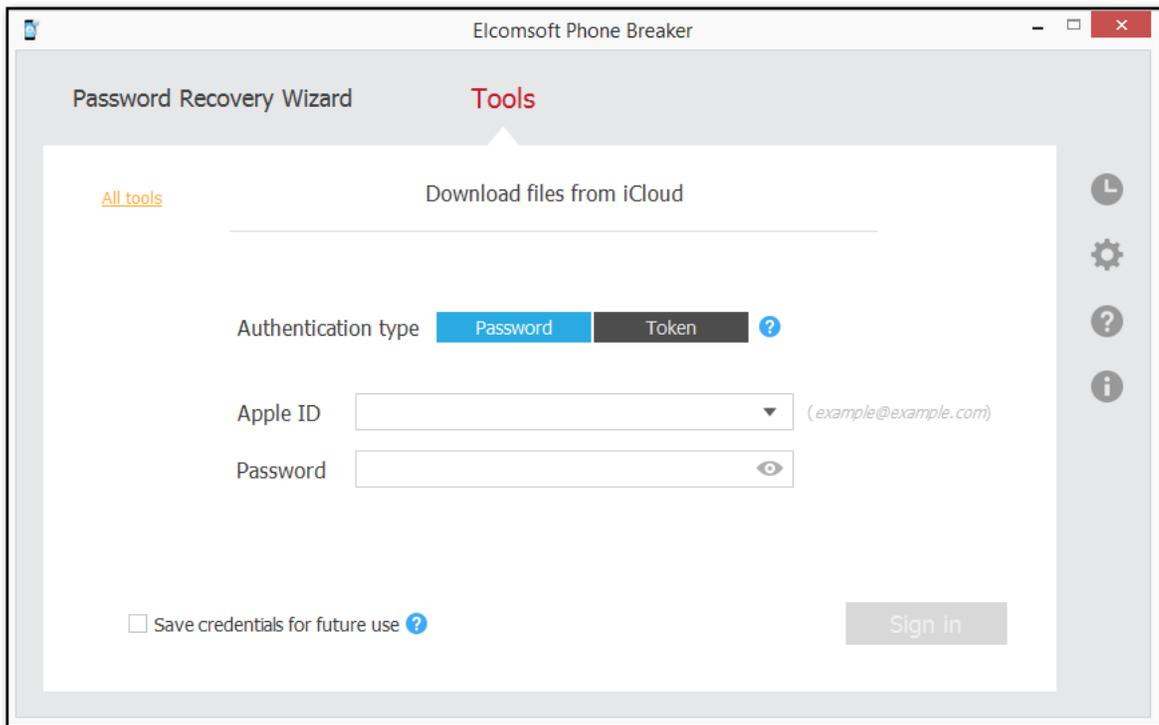
Converted backups look better, preserving the complete folder structure, as well as the file names as stored in the iOS file system. Most data is stored in SQLite databases (.db and .sqlite) and .plist files; you also get pictures in PNG and JPEG, etc.

### 3.2.5.2 Working with files in iCloud

#### 3.2.5.2.1 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. 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**.

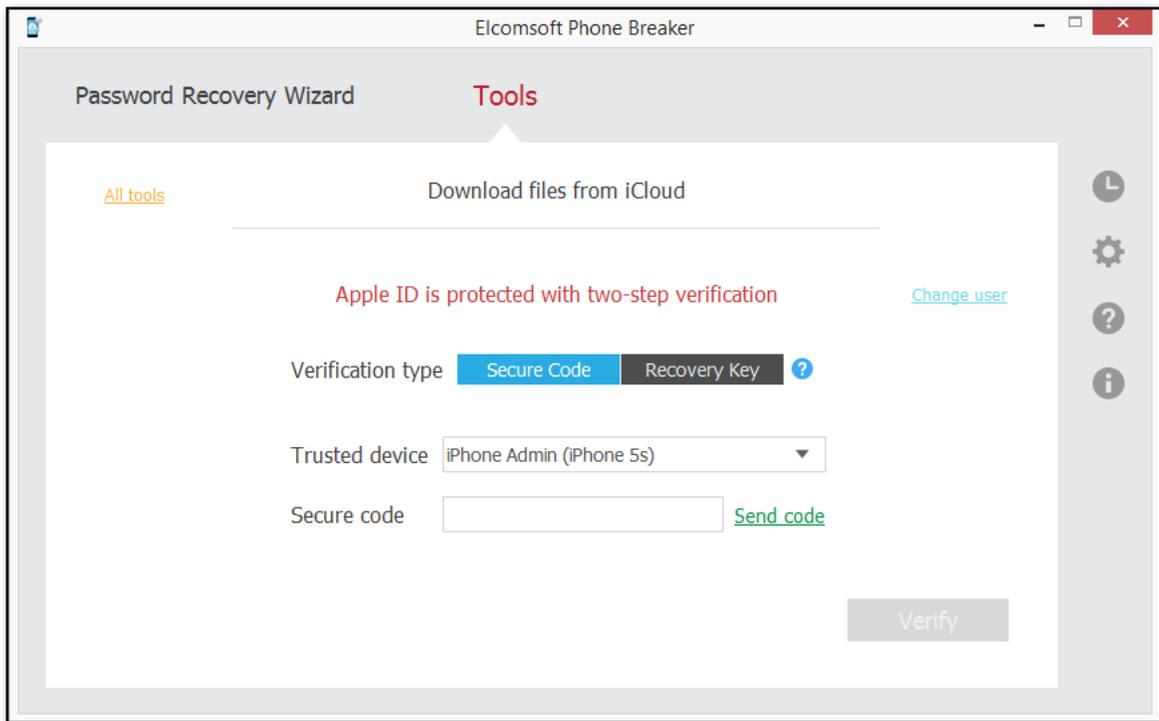
**NOTE:** If you have entered the Apple ID in a wrong format, the message about the account being locked will be displayed. Close the message and try again. Please make sure to enter your apple ID in the standard format (i.e., [example@example.com](mailto:example@example.com)). If the Apple ID is protected with two-factor authentication, you need to confirm sending the verification code to all of your trusted devices or to your phone.

You can select the **Save credentials for future use** option when logging in so that you don't need to enter them when you log in with this Apple ID again.

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. Click **Verify**.

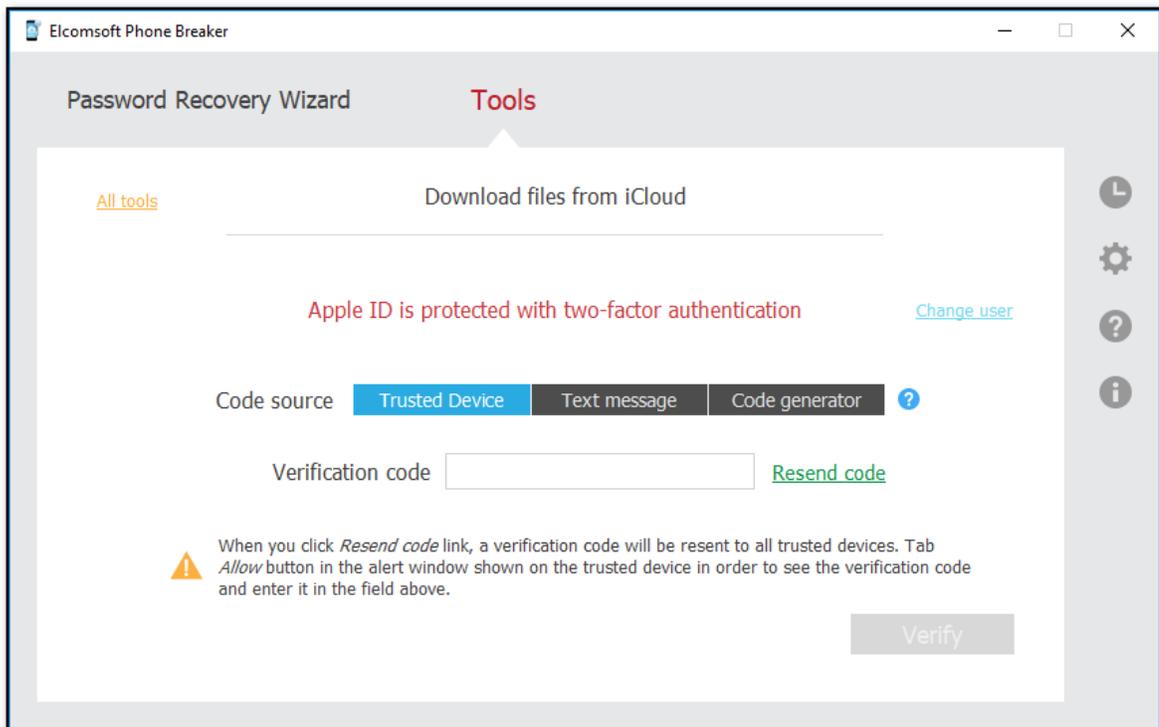


7. If the Apple ID is protected with two-factor authentication, perform authentication in one of the following ways:

- Select **Trusted Device** and enter the 6-digit code in the **Verification code** field. Click **Resend code** for the verification code to be sent to all trusted devices.
- Select **Text message** and enter the 6-digit code in the **Verification code** field. Click **Send code** for the verification code to be sent as text message to the selected trusted phone number. If you have not received the code, you can resend it by clicking **Resend code**.

**NOTE: macOS 10.12 or higher is required for sending text messages. Authentication via the Text message is available for the Forensic edition only.**

- Select **Code generator** and enter the 6-digit code in the **Verification code** field. The code is generated on the trusted device or via Cloud Panel.



8. Click **Verify**.

9. The iCloud opens.

You can view files and folders in the **Application** column.

The **Creation time** column displays the date and time the file/folder was created.

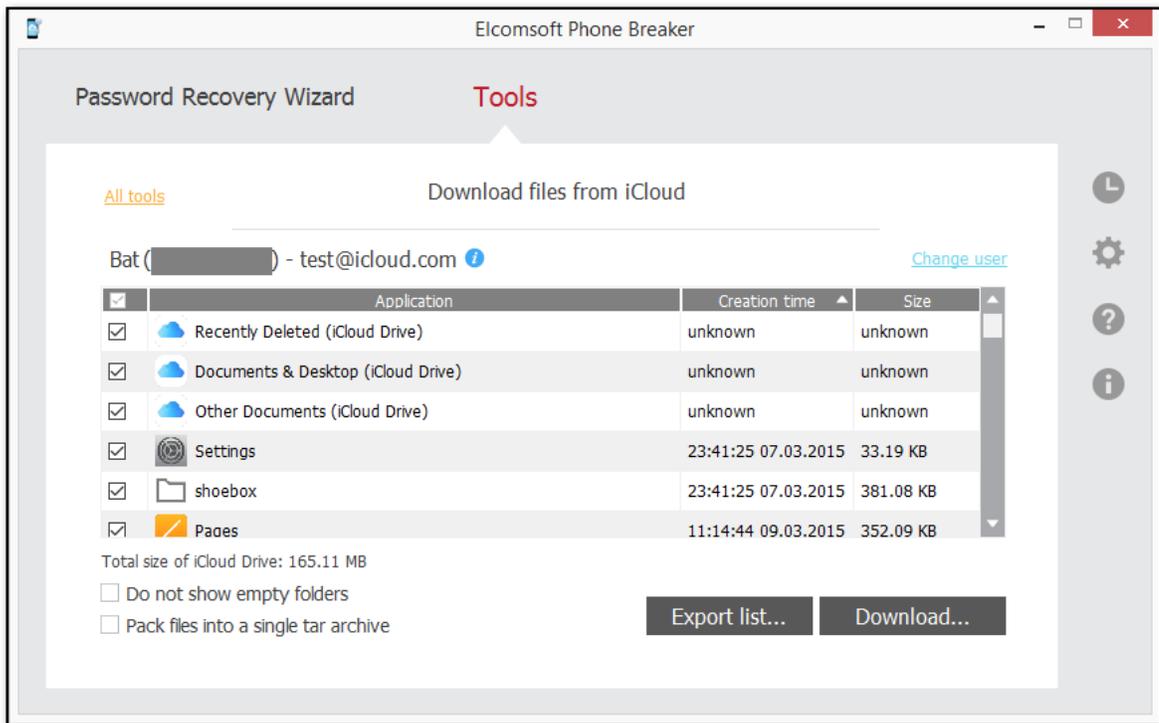
The **Size** column displays the size of a file/folder. The total size of the following folders is displayed under the grid:

- Recently Deleted (iCloud Drive): Contains recently deleted files that have been synced with iCloud.
- Documents & Desktop (iCloud Drive): Contains files and folders from the Desktop and Documents folders in iCloud Drive.
- Other Documents (iCloud Drive): Contains other files and folders from iCloud Drive.

**NOTE: Files and folders that are not available for downloading in the current version of EPB, are disabled and cannot be selected.**

Hover mouse over the  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

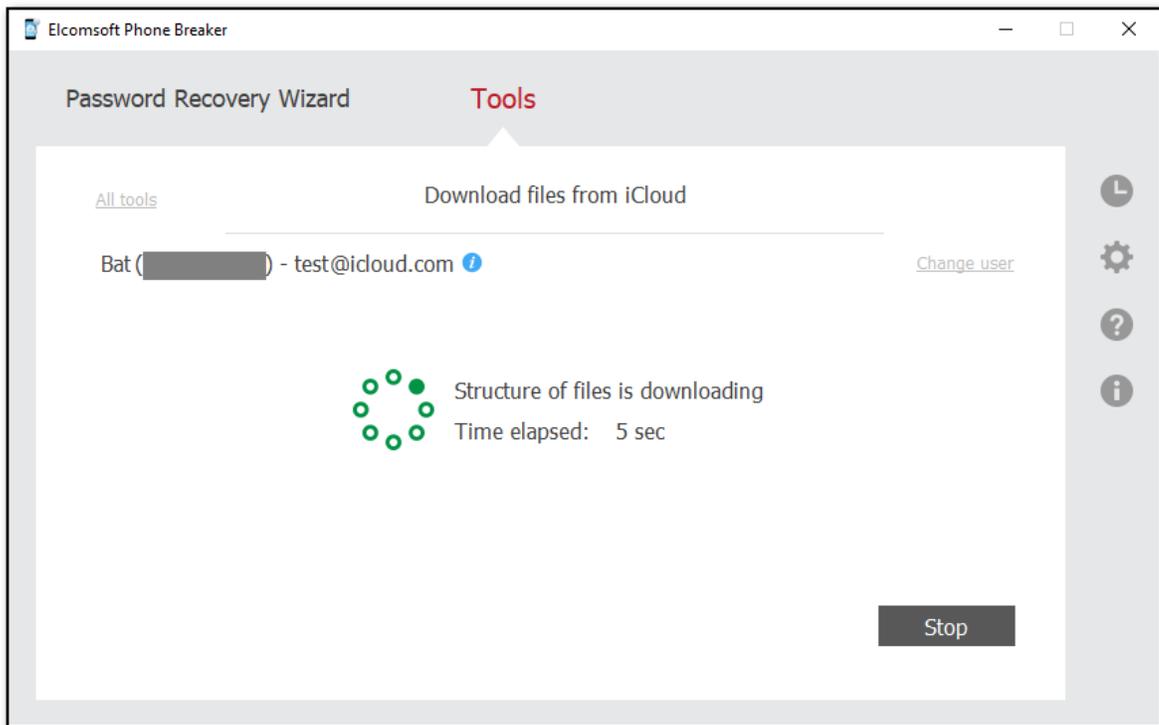
10. Select the folders and files you would like to download by selecting check boxes on the left. The files will be saved in their native format.

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

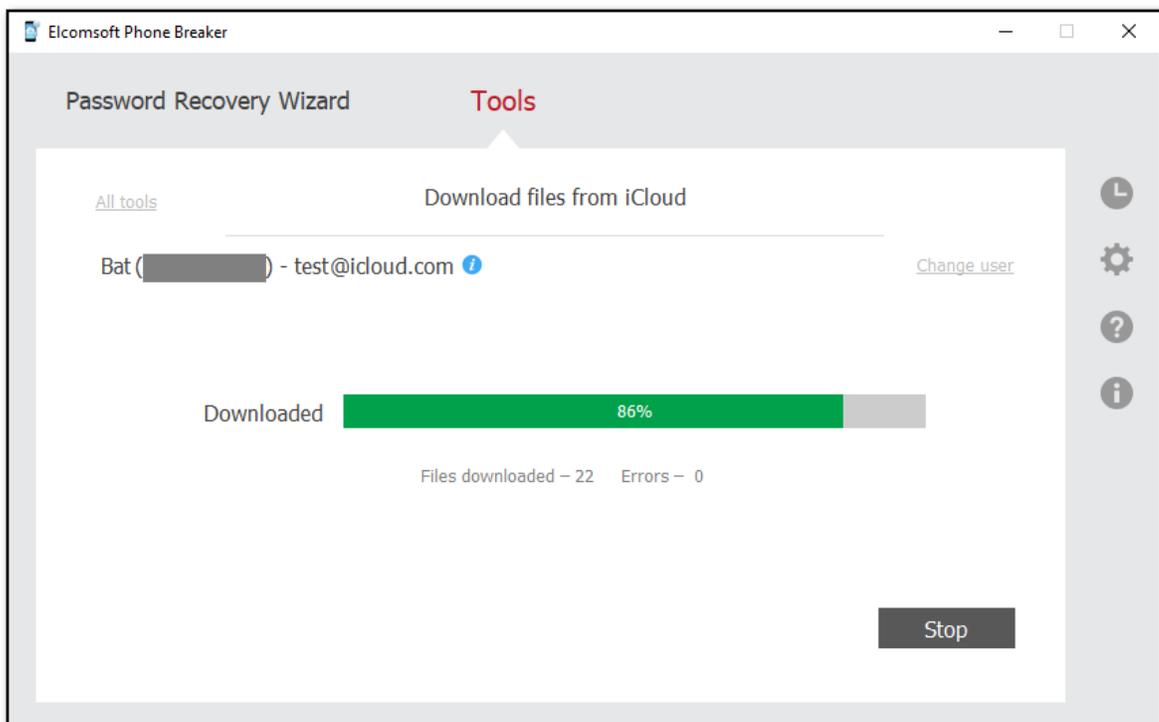
12. Click **Download**.

13. Define the location for storing downloaded data.

14. The downloading of files structure starts. It will take time to download the structure of files.



15. Once the structure of files is downloaded, the process of downloading files from iCloud begins.



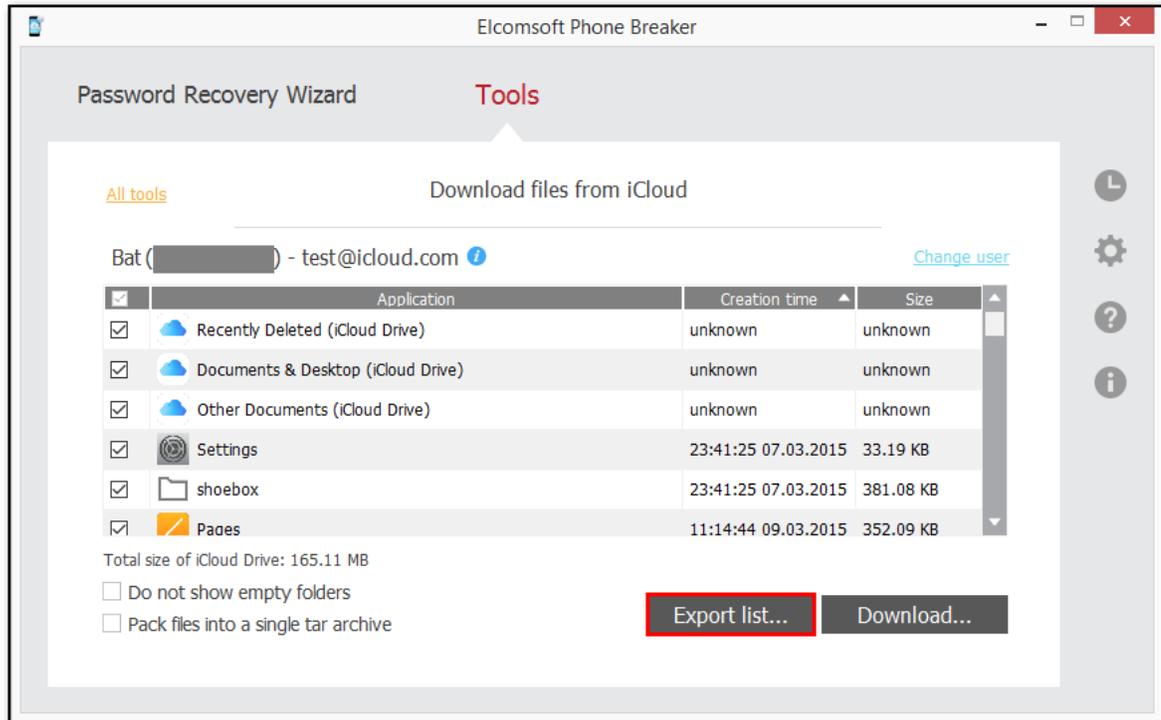
16. When it is finished, click **Finish** to exit the downloading wizard.

## 3.2.5.2.2 Exporting iCloud files list

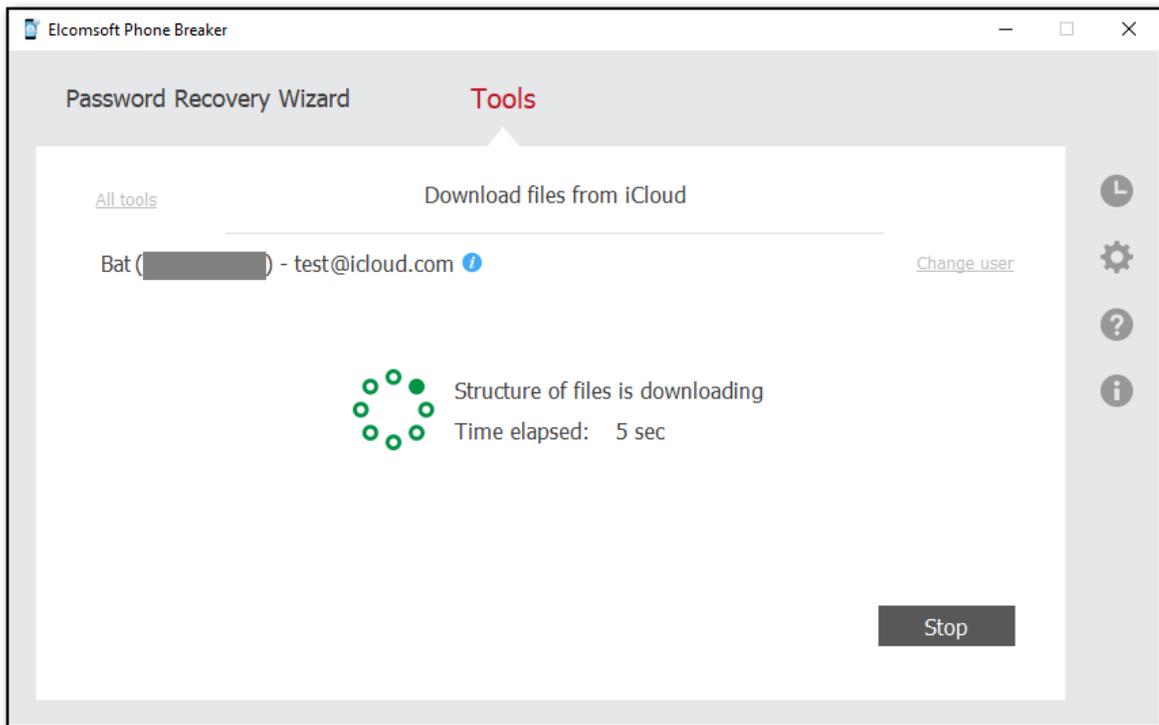
**EPB** allows exporting the list of files in the iCloud into XML format.

**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 structure of files starts downloading.



4. Once the structure of files is downloaded, click **Finish**.

5. 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.

### 3.2.5.3 Downloading synced data from iCloud

**EPB** allows downloading device data synchronized with an iCloud account. This data can then be viewed on your computer or in **Elcomsoft Phone Viewer**.

The following categories of the synced data are available:

- Account Info
- Apple Maps
- Calendar
- Calls
- Contacts
- FileVault2 token
- Health
- iBooks
- Keychain
- Messages
- Notes
- Photos
- Safari
- Screen Time
- Voice Memos
- Wallet
- Wi-Fi

### System requirements

1. For downloading **iCloud Keychain**, your computer has to meet the following requirements:

For **macOS**, you need macOS 10.12 or higher.

2. For downloading **iCloud Photos**, install iCloud for Windows version 4.0 or later from Apple's website (<https://support.apple.com/en-us/HT204283>):

## Download iCloud for Windows

With iCloud for Windows, you'll have your photos, videos, mail, calendar, files, and other important information on the go and on your Windows PC.



[Download iCloud for Windows from the Microsoft Store](#)

### Here's what you need

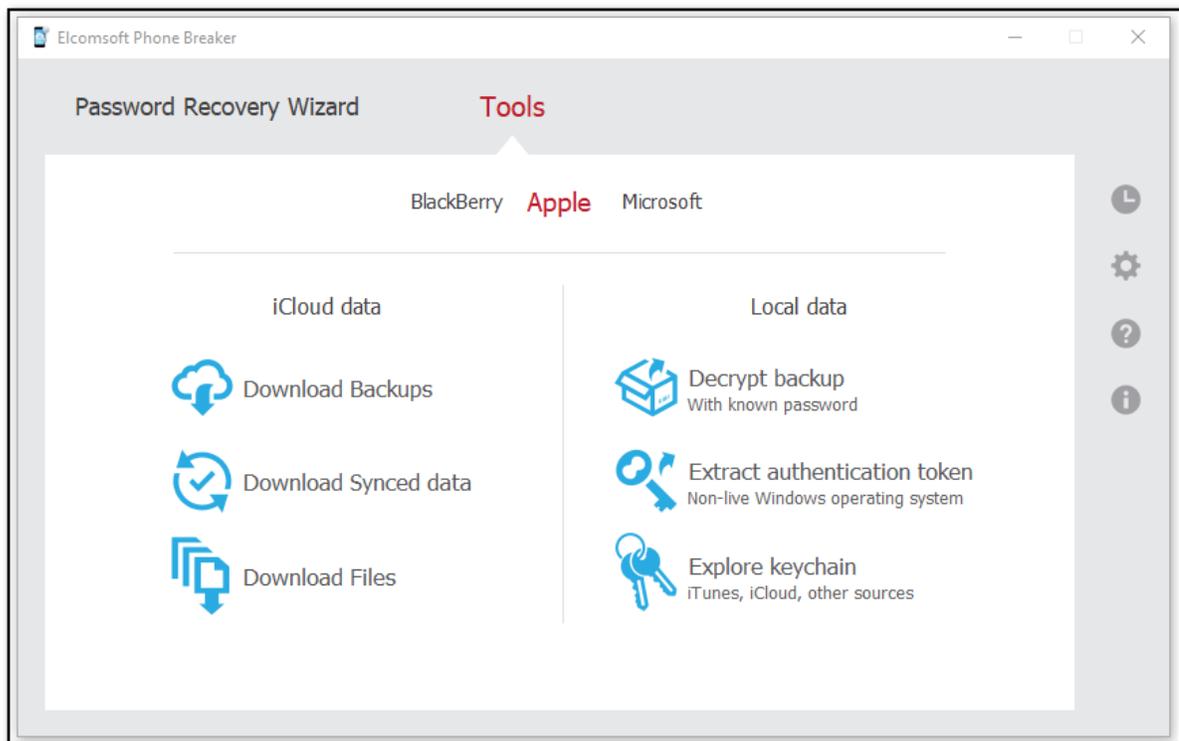
- Make sure that your PC or Microsoft Surface is updated to the latest version of Windows 10.\*
- [Have your Apple ID and password ready](#). If you don't have an Apple ID, [you can create one](#).

\* On Windows 7 and Windows 8, you can [download iCloud for Windows on Apple's website](#).

**NOTE: iCloud for Windows from the Microsoft Store is not supported.**

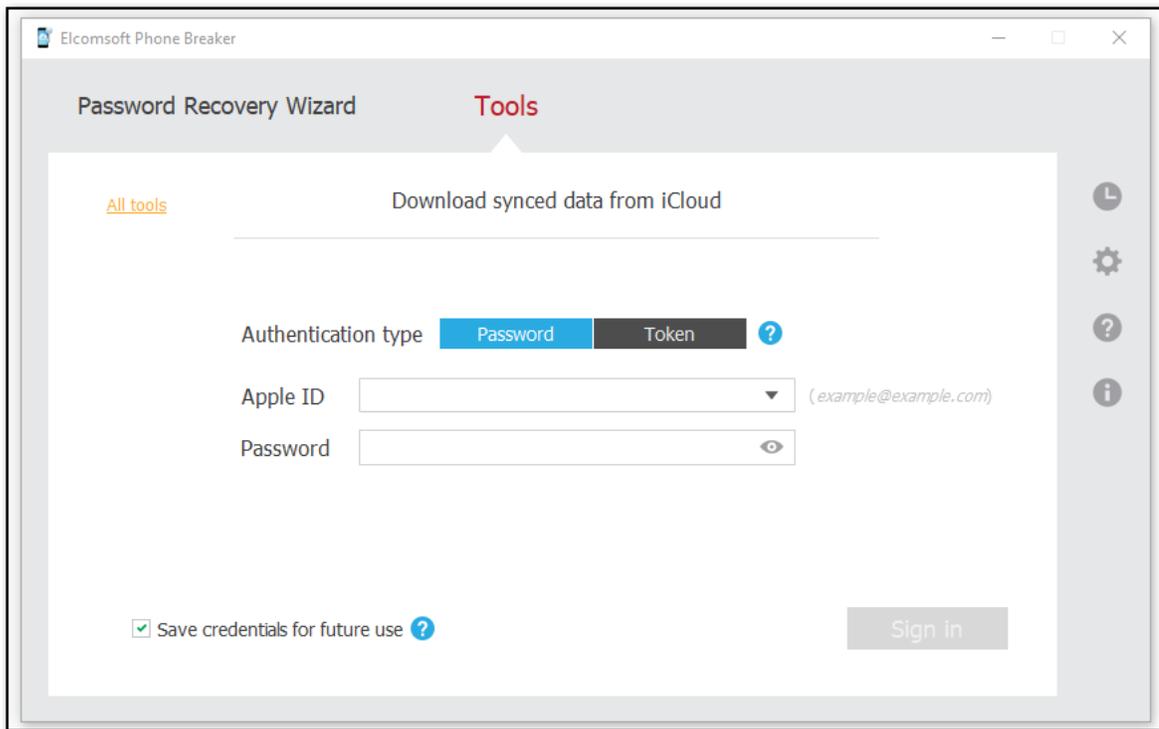
**To download iCloud synced data**, do the following:

1. In the **Tools** menu, select the **Apple** tab.
2. Select **Download Synced data**.



3. On the **Download synced data from iCloud** page, define the authentication type:

- **Password:** Select this option to use your Apple credentials (Apple ID and password)
- **Token:** Select this option 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**.

**NOTE: If you have entered the Apple ID in a wrong format, the message about the account being locked will be displayed. Close the message and try again. Please make sure to enter your apple ID in the standard format (i.e., [example@example.com](#)).**

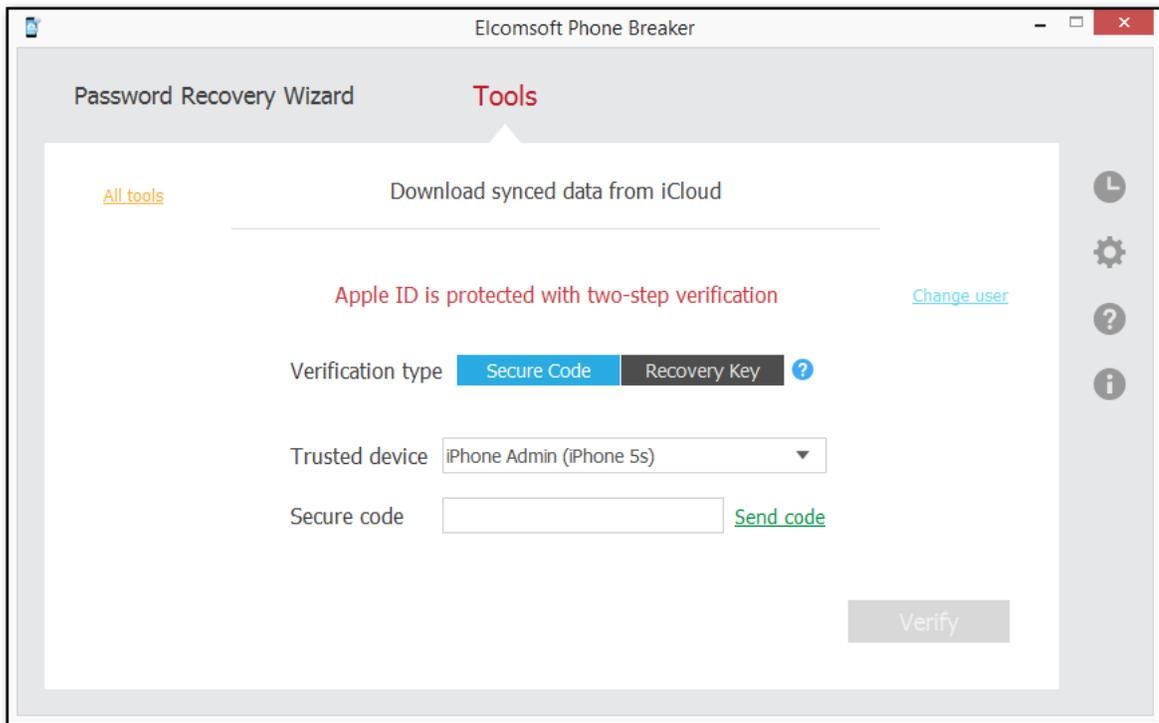
**NOTE: If the Apple ID is protected with two-factor authentication, you need to confirm sending the verification code to all of your trusted devices or to your phone.**

You can select the **Save credentials for future use** option when logging in so that you don't need to enter them when you log in with this Apple ID again.

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 **Send code**, and then enter the received 4-digit code in the **Secure code** field. Click **Resend code** for it to be sent again.
- **Recovery Key:** enter a 14-character key generated defined in the Apple account settings.

6. Click **Verify**.



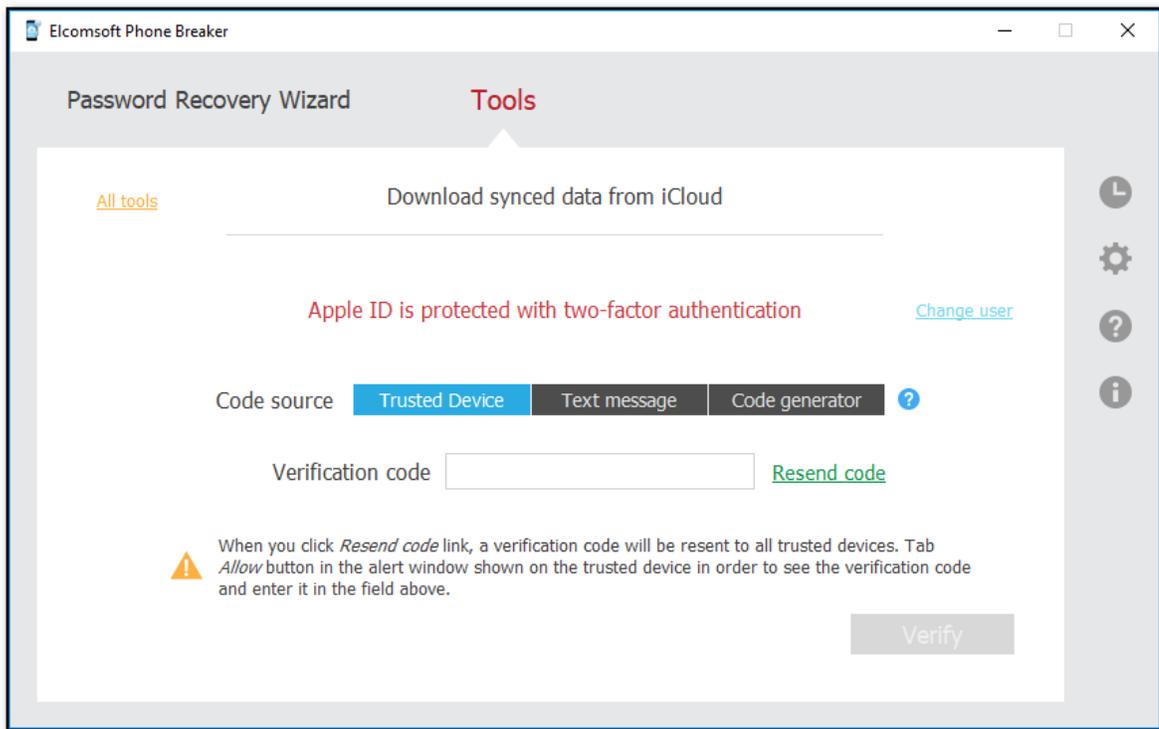
7. If the Apple ID is protected with two-factor authentication, perform authentication in one of the following ways:

- Select **Trusted Device** and enter the 6-digit code in the **Verification code** field. Click **Resend code** for the verification code to be sent to all trusted devices.
- Select **Text message** and enter the 6-digit code in the **Verification code** field. Click **Send code** for the verification code to be sent as a text message to the selected trusted phone number. Click **Resend code** for it to be sent again.

**NOTE: macOS 10.12 or higher is required for sending text messages.**

**NOTE: Authentication via the Text message is available for the Forensic edition only.**

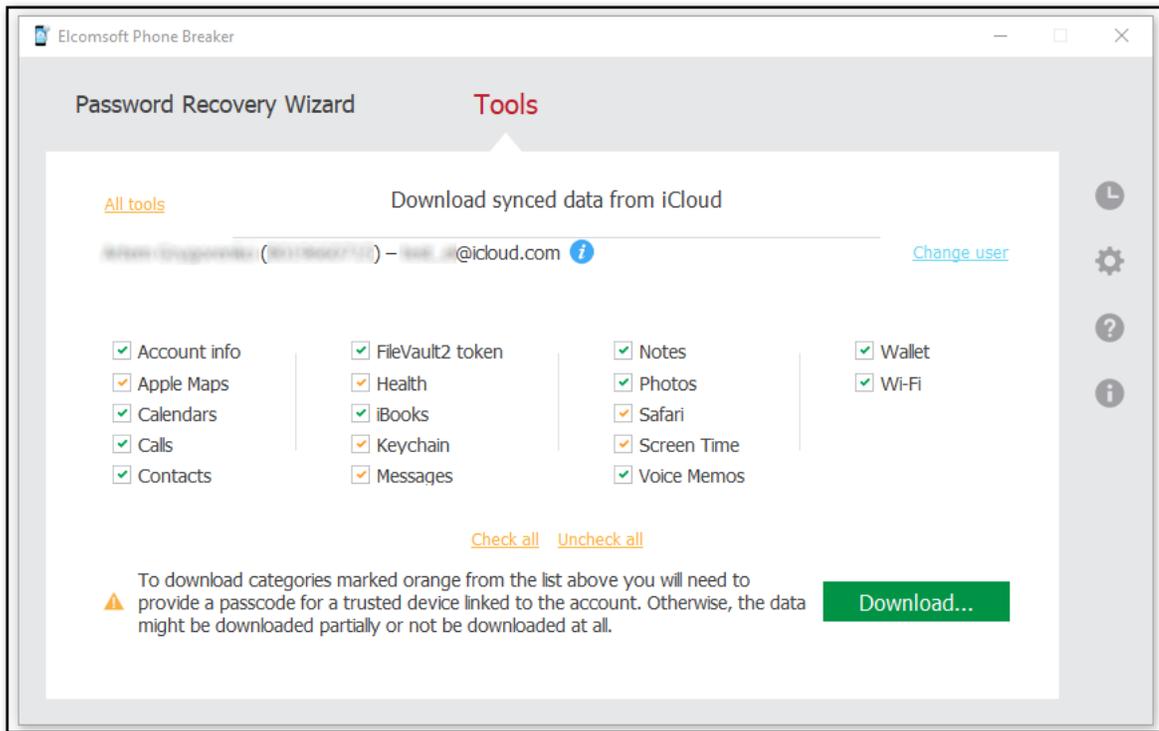
- Select **Code generator** and enter the 6-digit code in the **Verification code** field. The code is generated on the trusted device or via Cloud Panel.



8. Click **Verify**.

9. The following information is displayed after signing in: user name, DSID, Apple ID.

**NOTE:** To download synced data for a different user, click **Change user**.



10. Select the data categories to download and click **Download**.

When downloading the **Account info**, **Messages**, **Health**, **Screen Time**, **Voice Memos**, **Safari** and **Apple Maps** data categories, consider the following limitations:

Category	Accounts with two-factor authentication	Accounts without two-factor authentication	Download data using authentication token
<b>Account info</b>	✓	✓	—
<b>Messages</b>	✓	—	—
<b>Health</b>	✓	✓	Partially (without secured containers)
<b>Screen Time</b>	✓	—	—
<b>Voice Memos</b>	✓	—	—
<b>Apple Maps</b>	✓	✓	Partially (without secured containers)
<b>Safari</b>	✓	✓	Partially (without secured containers)

**NOTE:** The **Apple Maps** (from devices running iOS 13 and later), **Account info**, **Messages**, **Health**, **Screen Time**, **Safari** secured data, and **Voice Memos** data are available for downloading in the **Forensic edition only**.

**NOTE:** The **Apple Maps** data from devices running iOS 13 and later can be downloaded only from **iCloud accounts with two-factor authentication after entering the passcode**.

The **Messages** category contains messages synced from devices with the following operating systems:

- iOS 11.4 and higher

- macOS 10.13.15 and higher

**NOTE: When downloading data for categories marked orange, the decryption keys might become invalid or might not be generated on the environment that supports these data categories in iCloud and the data might not be downloaded. Make sure that you sign in to the Apple ID on the device with the latest iOS or macOS. Try to log out and log in to iCloud on your device, and then turn off and turn back on iCloud Keychain. Then try downloading messages again. You can also try using another trusted device.**

Starting with EPB 6.40, the downloaded **Safari** history data includes the link status (Actual or Deleted) and the deletion date for the deleted records, which can be explored in EPV after the download.

**Safari** history data for the latest two weeks is available for download.

For the **Calls** category, only calls for the last month are available for download.

The **Screen Time** category contains information synced from devices with the iOS 12 and higher.

The **Voice Memos** category contains voice memos synced from devices with the following operating systems:

- iOS 12.x.x and higher
- macOS 10.14

11. The **Select path to download synchronized data** window opens.

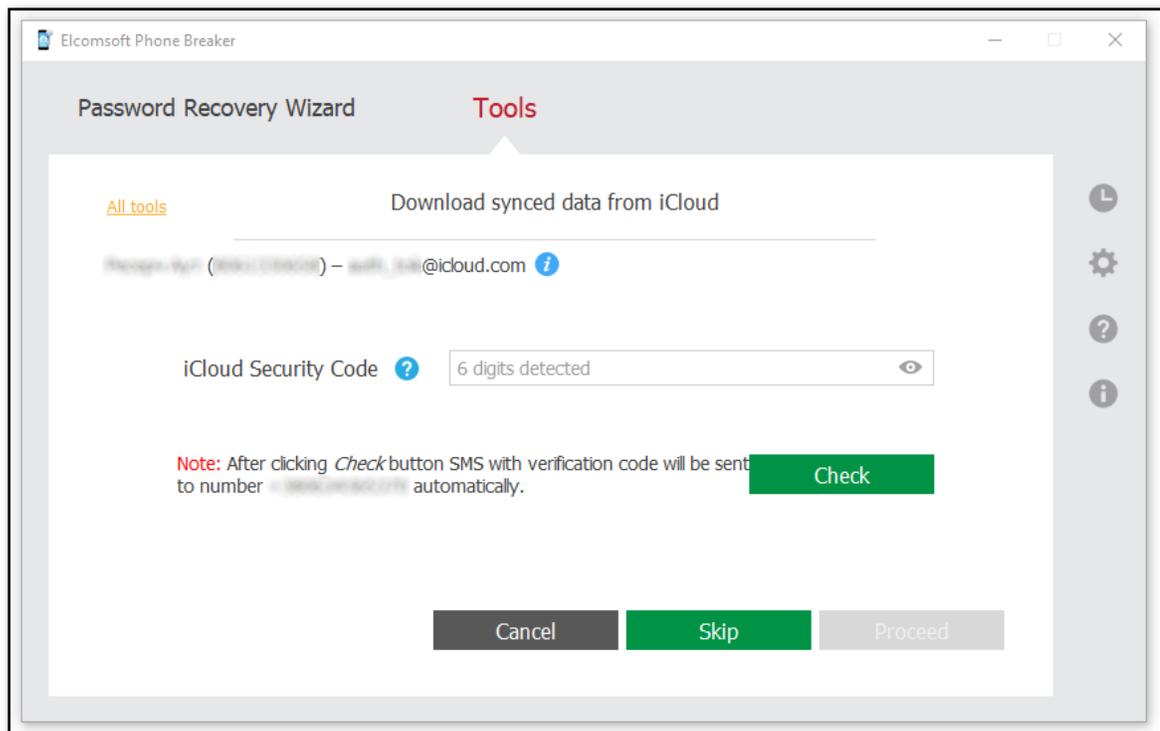
12. In the **Select path to download synchronized data** window, define the location for storing downloaded data and click **Select Folder**.

13. If your account is not protected with two-factor authentication, you need to enter the iCloud Security Code to download the **Keychain** category data.

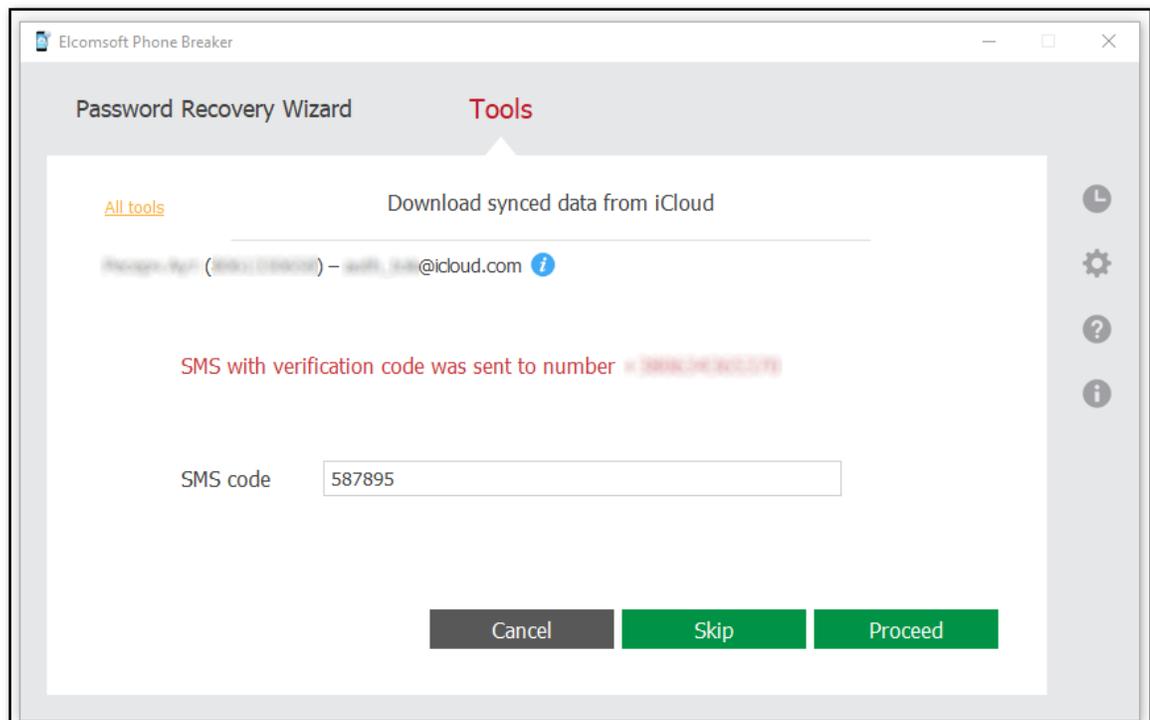
**NOTE: iCloud Security Code is a code entered when iCloud Keychain was first synchronized with this device. The code is associated with a specific phone number.**

14. Enter the iCloud Security Code and click **Check**. An SMS with a verification code will be sent to the phone number iCloud Keychain is associated with.

**NOTE: If you enter the wrong iCloud Security Code too many times, your access to iCloud Keychain will be temporarily blocked. To unblock it, you can turn to Apple support. Once you get your access to iCloud Keychain unblocked, be very cautious entering the right iCloud Security Code. If you enter it wrong again after your access to iCloud Keychain was unblocked, the iCloud Keychain data will be deleted.**



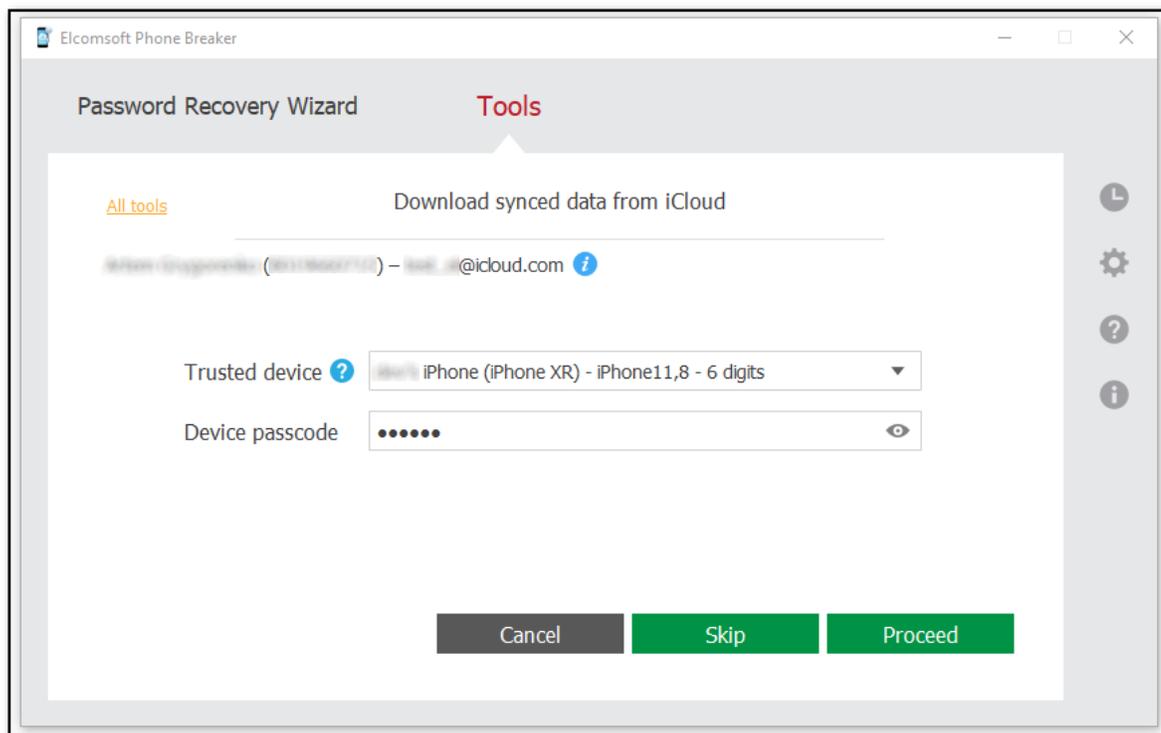
15. Enter the verification code you received in the SMS and click **Proceed**.



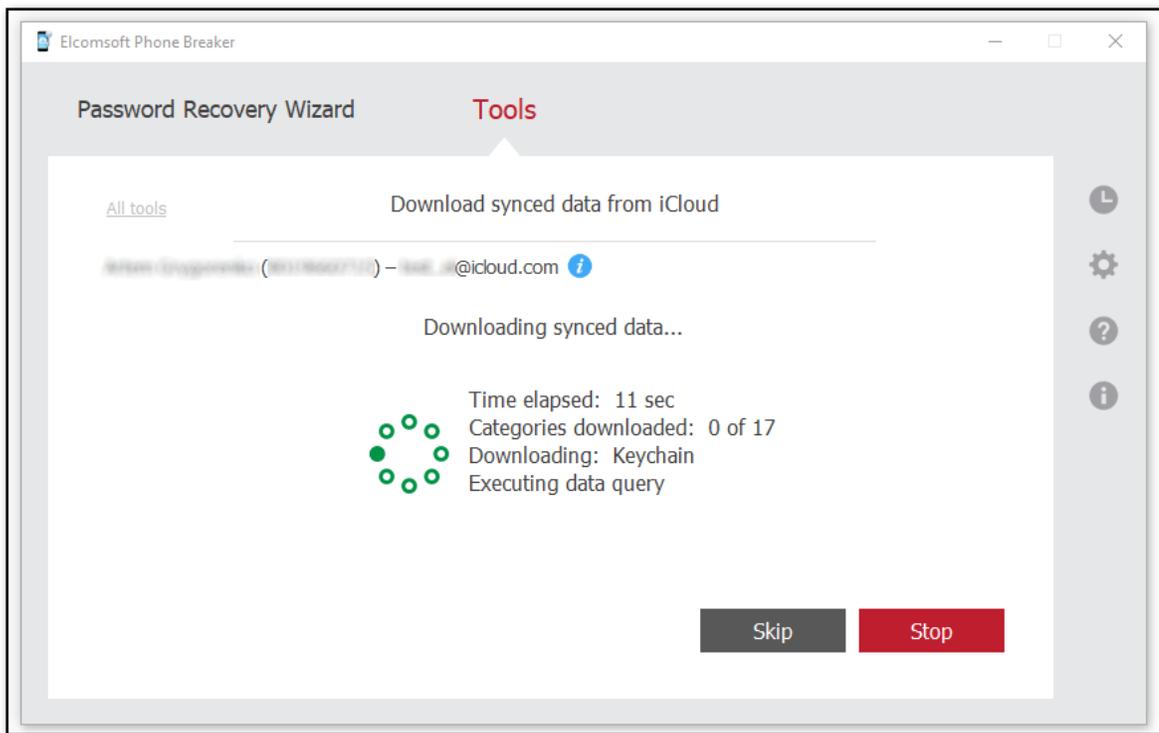
16. If you select the categories marked orange for an account with activated two-factor authentication, select a trusted device and enter the passcode (for iOS) or the password to the user account in the operating system (for macOS).

**NOTE: If you do not provide the passcode, data might be downloaded partially or not be downloaded at all.**

**NOTE: If you enter the wrong device passcode 10 times, the device will be blocked in EPB. This will not affect the device itself but you will not be able to use it for downloading data in EPB. To unblock the device, you need to change its passcode, confirm it, and synchronize iCloud Keychain with this device again. You can also download data using another trusted device and its passcode.**



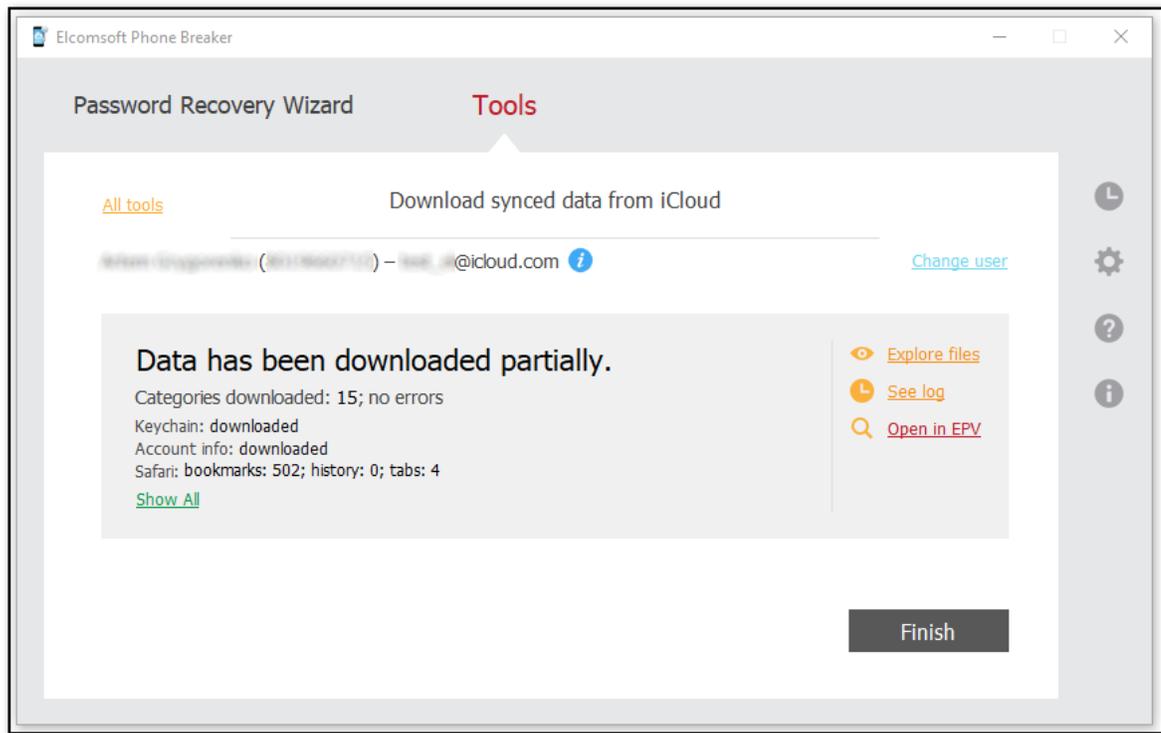
17. Click **Proceed**. The process of downloading synced data from iCloud begins. The progress is displayed in the program window. To skip downloading the current category, click **Skip**. To stop the downloading process, click **Stop**. (If some files have been downloaded before you stopped the process, you will be able to explore them.)



18. When downloading is finished, you can see the following information:

- **Categories downloaded:** The count of downloaded categories and the downloading status (no errors or with errors).
- **Count of records** for the downloaded categories.
- For the **Calendars, Calls, Apple Maps, Wi-Fi, Messages, Health, Screen Time** and **Notes** categories, you can also see the **date range** (from the earliest to the latest record).

**NOTE:** The Trial version of Elcomsoft Phone Breaker allows downloading only 10 most recent calls, notes, Wi-Fi hotspots, Apple Maps favorites and history searches, and Safari history records.



You can do the following:

- Click **Explore files** to open the folder with synced iCloud data.
- Click **See log** to open the journal and view the start time and end time of downloading and the errors that occurred during downloading.
- Click **Open in EPV** to view the synced iCloud data in Elcomsoft Phone Viewer.

**NOTE: This option is available only if you have Elcomsoft Phone Viewer 3.10 or a higher version installed.**

- Click **Change user** to download iCloud synced data for a different Apple ID.
- Click **All tools** to return to the list of tools for working with Apple backups.
- Click **Finish** to exit the downloading wizard.

### Viewing downloaded iCloud synced data

You can explore downloaded iCloud synced data using Elcomsoft Phone Viewer.

**To view downloaded iCloud synced data in Elcomsoft Phone Viewer**, click the **Open in EPV** link after the downloading process is complete. The **Elcomsoft Phone Viewer** will open and you will be able to investigate the iCloud synced data.

You can also view the content of the iCloud synced data folder on your computer.

To view the content of the iCloud synced data folder on your computer, open the folder on your computer to which the data was downloaded.

The name of the folder with iCloud synced data is **iCloud\_sync\_<apple\_id>\_<time stamp>**.

**NOTE: The time stamp in the name of the folder with iCloud synced corresponds to the time zone of the local computer.**

In the **iCloud\_sync\_<apple\_id>\_<time stamp>** folder, the following items are displayed:

- **Account Info** folder containing files with the account data.
- **AppleMaps** folder containing the **AppleMaps.db** file (a database in which the Apple Maps record attributes are stored).
- **Calendars** folder containing the **Calendars.db** file (a database in which the calendar record attributes are stored).
- **Calls** folder containing the **calls.db** file (a database in which the call record attributes are stored).
- **Contacts** folder with the following contents:
  - **Contacts.db** file (a database in which the contact record attributes are stored).
  - **Vcards** subfolder containing contact cards.

**NOTE: vCards of groups are included into the count of downloaded contacts in EPB. Therefore, the number of contacts displayed in EPB might be greater than the one displayed in EPV.**

- **FileVault** folder with the **filevault2\_token.xml** file containing a recovery token to decrypt the macOS disk image in [Elcomsoft Forensic Disk Decryptor](#).
- **Health** folder containing the **healthdb.db**, **healthdb\_secure.db**, **locations.db** files, etc.
- **iBooks** folder containing a list of downloaded books.
- **Keychain** folder containing **keychain.data** file.
- **Messages** folder containing **Messages.db** file (a database in which the message record attributes are stored) and **Attachments** folder.
- **Notes** folder containing **Notes.db** file (a database in which the note record attributes are stored) and note files.
- **Photos** folder with the following contents:
  - **All Photos folder**: a folder to which the media files from all albums were downloaded.
  - **Photos.db**: a database in which the attributes of media files are stored.

**NOTE: The names of photos in the folder correspond to their IDs in iCloud.**

- **Safari** folder containing **Safari.db** file (a database in which the Safari record attributes are stored).
- **ScreenTime** folder containing **ScreenTime.db** file (a database in which the Screen Time record attributes are stored).

- **VoiceMemos** folder containing a list of audio recordings and **VoiceMemos.db** file (a database in which the Voice Memos record attributes are stored)
- **Wallet** folder containing multiple files associated with the user's wallet.
- **Wifi** folder containing **Wifi.db** file (a database in which the Wi-Fi record attributes are stored).
- **CardPhoto.jpg** file containing the user account photo.
- **icloud\_synced.xml** file containing the information about the Apple ID, start and end time of downloading, and the status of downloading (success, canceled, finished with errors).

### Viewing downloaded iCloud Keychain data

You can explore the downloaded iCloud Keychain data using [Keychain explorer](#). Navigate to the synced data folder with the keychain data and open the **icloud\_synced.xml** file in the root of this folder.

**NOTE: If you use EPB 9.50 or lower version, navigate to the folder with iCloud Keychain data (named in the following format: iCloud\_keychain\_account@icloud.com\_YYYY.MM.DD\_HH-MM-SS) and open the icloud\_keychain.xml file in the root of this folder.**

## 3.2.6 Extracting authentication token for iCloud

### 3.2.6.1 About Authentication token

iCloud allows the users to store various information from their iOS devices in the cloud. macOS users can access iCloud without any additional software, as it is built into the operating system (iCloud requires macOS 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 for Windows (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 macOS and from iCloud for Windows. 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 OS	Live system (current system)	<a href="#">Using command-line utility (atex.exe)</a> .
	Non-live system (e.g., from the mounted disk image)	<a href="#">Via EPB interface</a>
macOS	Live system (current system)	<a href="#">Using command-line utility (atex.dmg)</a> .
	Non-live system (e.g., from the mounted disk image)	<a href="#">Via EPB interface</a>

**Types of the authentication tokens extracted by EPB on Windows OS and macOS:**

	iCloud for Windows lower v. 7.0	iCloud for Windows v. 7.0 and later	macOS lower 10.13	macOS 10.13 and later
Account with two-factor authentication	Authentication token without limitations	Authentication token with limitations	Authentication token without limitations	Authentication token with limitations
Account without two-factor authentication	Authentication token for the account without two-factor authentication	Authentication token for the account without two-factor authentication	Authentication token for the account without two-factor authentication	Authentication token for the account without two-factor authentication

#### Authentication tokens supported on Windows OS and macOS for downloading data via EPB:

	Authentication token without limitations for the account with two-factor authentication	Authentication token with limitations for the account with two-factor authentication	Authentication token for the account without two-factor authentication
Windows OS	Supported	NOT supported	Supported
macOS	Supported	Supported	Supported

**NOTE: Authentication token with limitations for the account with two-factor authentication is valid only if it was extracted on the same computer and under the same user.**

### 3.2.6.2 Extracting token on Windows OS

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

**NOTE: For tokens extracted using iCloud for Windows 7.3 or higher, for accounts with two-factor authentication, there are the following limitations:**

- **The token cannot be used to download iCloud backups.**

- The token is valid only if it was extracted on the current computer and the user did not log out of iCloud.

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 for Windows 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\<user name>\AppData\Local\Temp` folder, if you don't have enough permissions for writing files to the folder where `atex.exe` was launched from).

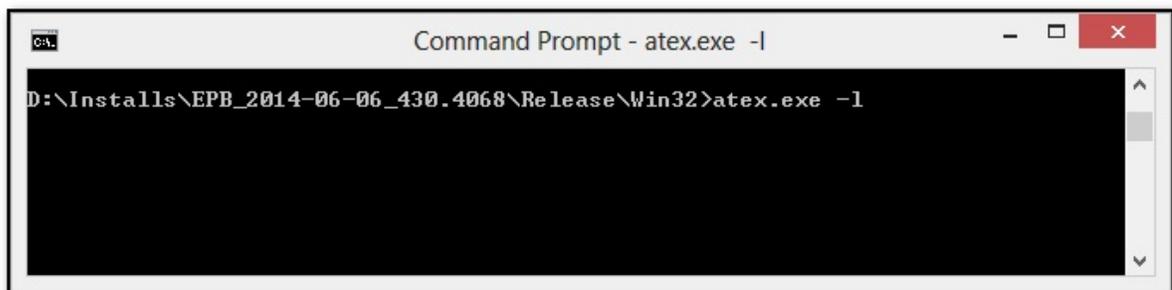
You will see the full path to the file in the opened console window. Please note that Unicode symbols in the file path are not supported.

2. The created `.txt` file contains the Apple ID of the current iCloud for Windows 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.



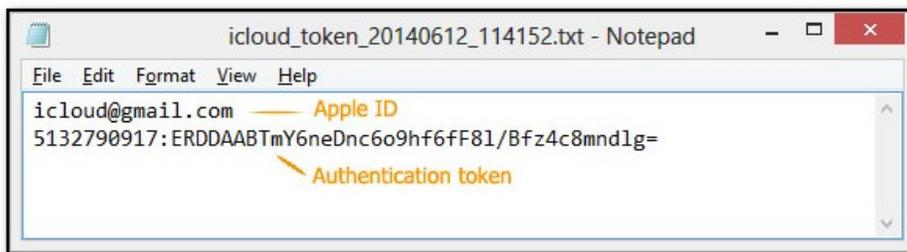
```
D:\Installs\EPPB_2014-06-06_430.4068\Release\Win32\atex.exe
iCloud users:
kon@DEU
Press any key to exit...
```

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

For example: **atex.exe --getToken -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 for Windows user and its Authentication token.



```
icloud@gmail.com — Apple ID
5132790917:ERDDAABTmY6neDnc6o9hf6fF81/Bfz4c8mndlg=
                Authentication token
```

#### Parameters for running atex.exe in the command prompt:

Parameter	Meaning
<b>-h</b> or <b>[--help]</b>	Displays help message
<b>-l</b> or <b>[--iCloudUserList]</b>	Displays usernames of iCloud users
<b>--getToken -n &lt;username&gt; -p &lt;password&gt;</b>	Gets the authentication token for a specified user. Username and password should be entered without brackets.
<b>-n</b> or <b>[--username]</b>	Indicates a specified user. Username should be entered without brackets.
<b>-p</b> or <b>[--password]</b>	Indicates a password for a specified user. Password should be entered without brackets.

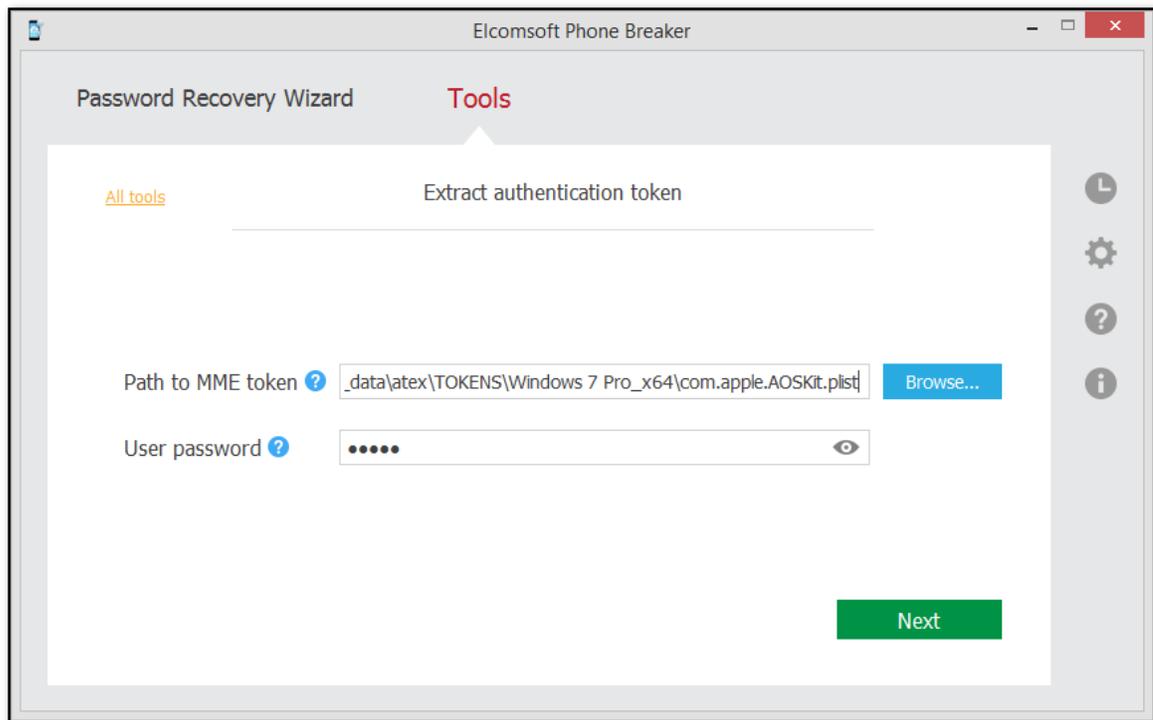
#### 3.2.6.2.2 Extracting token on non-live Windows OS

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:

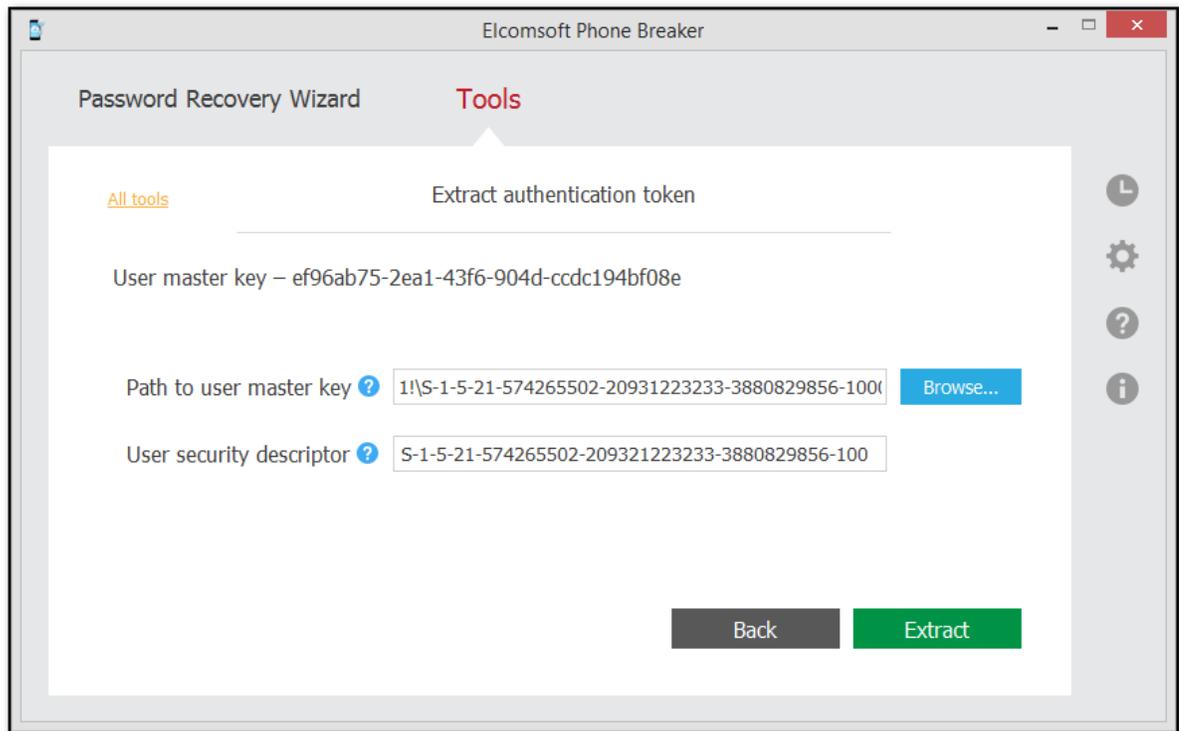
1. Mount the image of the disk containing the authentication token.

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.

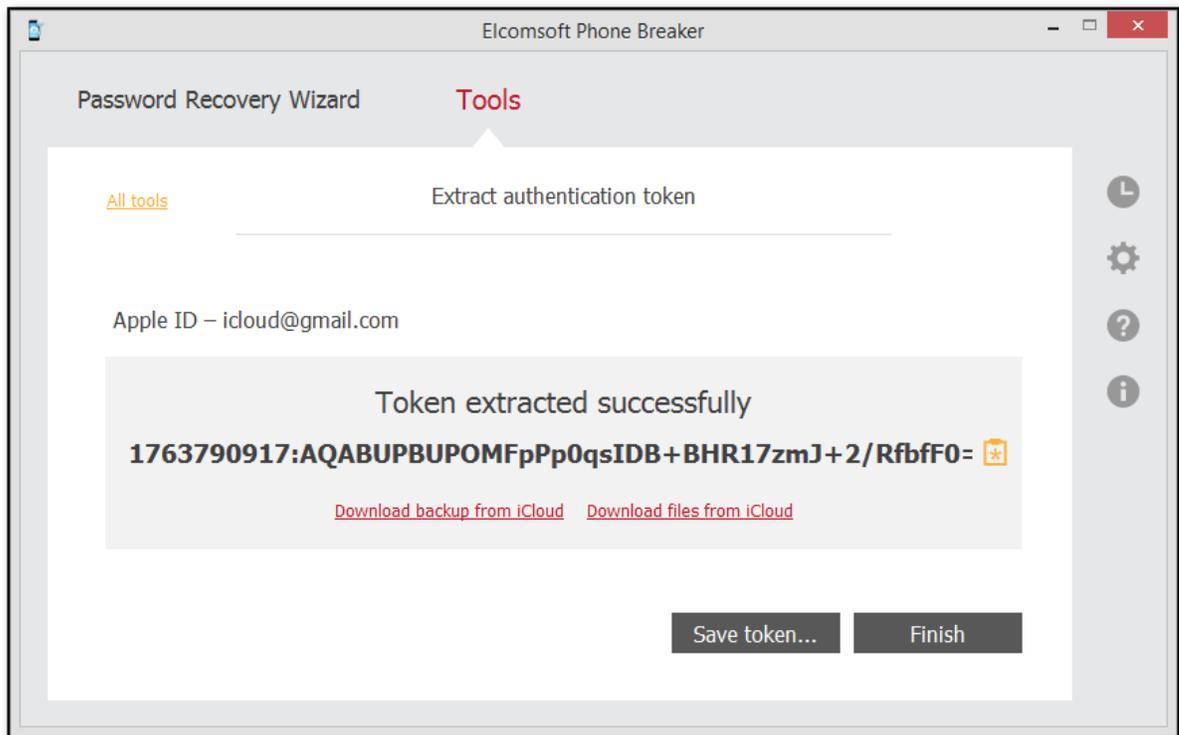


6. Click **Next**.
7. On the following page, define the path to user master key file and its SID. The user master key itself is displayed on top. This key is used to decrypt the authentication token.
  - **Path to user master key:** Enter the path to the folder with user master key file. By default the master key is stored in %APPDATA%\Roaming\Microsoft\Protect\<SID>\ 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](#).

### 3.2.6.3 Extracting token on macOS

#### 3.2.6.3.1 Extracting token on live macOS

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 macOS. This tool is shipped together with EPB (**atex.dmg** file). You can find it in EPB installation folder.

Elcomsoft Apple Token Extractor supports macOS versions up to 10.15.

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 macOS user	User's permissions are enough
iCloud account of a different macOS user	<b>root</b> permissions are required

**Types of authentication tokens extracted by EPB:**

	macOS lower 10.3	macOS 10.3 and higher
Account with two-factor authentication	Authentication token without limitations	Authentication token with limitations
Account without by two-factor authentication	Authentication token for account without two-factor authentication	Authentication token for account without two-factor authentication

The "**icloud\_token\_<timestamp>.plist**" file, which is created as the result of the token extraction, might contain the following types of tokens:

Token Type	Description
<b>auth_token</b>	<b>Authentication token.</b> Has no limitations.
<b>auth_token_with_limitations</b>	<b>Authentication token with limitations.</b> Has the following limitations: <ul style="list-style-type: none"> <li>The token cannot be used to download iCloud backups.</li> <li>The token is valid only if it was extracted on the current computer and the user did not log out of iCloud.</li> </ul>
<b>ctoken</b>	<b>Continuation token.</b> Cannot be used in EPB yet.

Key	Type	Value
▼ Root	Dictionary	(6 items)
apple_id	String	test@gmail.com
atex_version	String	1.4
auth_token	String	11179869442:IAAAAAAABLwIAAAAAFvqx/ORDmdzLmljbG91ZC5hdX
auth_token_with_limitations	String	11179869442:EAAEAAAABLwIAAAAAFvhjEoRDmdzLmljbG91ZC5hdX
ctoken	String	MDAwNDk3LTA4LWFkNGl0YWwLTUwYzltNDQ2ZC1iOWFiLTJkYTMyZ
date	String	2018-11-13 12:47:59 +0000

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

1. Run the atex.dmg file.

*NOTE: If Elcomsoft Apple Token Extractor cannot be opened, see the detailed information in the [Troubleshooting](#) topic.*

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 "**icloud\_token\_<timestamp>.plist**" file 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.

**NOTE: Make sure that there is Internet connection on the computer where the token is extracted. Otherwise, only the token with limitations will be extracted.**

5. The created "**icloud\_token\_<timestamp>.plist**" file contains the Authentication token of the current iCloud user.

The "**icloud\_token\_<timestamp>.plist**" file created for the current iCloud user contains the following information:

macOS Version	Contents
macOS up to 10.12.5	<ul style="list-style-type: none"> <li>Apple ID (apple_id)</li> </ul>

	<ul style="list-style-type: none"> <li>▪ Authentication token (auth_token)</li> <li>▪ Continuation token (ctoken)</li> <li>▪ Password to Apple ID - in some cases</li> </ul>
macOS 10.3 and higher	<ul style="list-style-type: none"> <li>▪ Apple ID (apple_id)</li> <li>▪ Authentication token (auth_token)</li> <li>▪ Authentication token with limitations (auth_token_with_limitations)</li> <li>▪ Continuation token (ctoken)</li> <li>▪ Password to Apple ID - in some cases</li> </ul>

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

1. Run the atex.dmg file.

*NOTE: If Elcomsoft Apple Token Extractor cannot be opened, see the detailed information in the [Troubleshooting](#) topic.*

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 --getToken -u <username> -p <password>**

For example: **sudo atex --getToken -u mary -p 1234**

**NOTE: Make sure that there is Internet connection on the computer where the token is extracted. Otherwise, only the token with limitations will be extracted.**

9. 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.

10. The created "**icloud\_token\_<timestamp>.plist**" file contains the Authentication token of the selected iCloud user.

The "**icloud\_token\_<timestamp>.plist**" file created for a different iCloud user contains the following information:

macOS Version	Contents
macOS up to 10.12.5	<ul style="list-style-type: none"> <li>▪ Apple ID (apple_id)</li> <li>▪ Authentication token (auth_token)</li> <li>▪ Continuation token (ctoken)</li> <li>▪ Password to Apple ID - in some cases</li> </ul>
macOS 10.3 and higher	<ul style="list-style-type: none"> <li>▪ Apple ID (apple_id)</li> <li>▪ Authentication token with limitations (auth_token_with_limitations)</li> <li>▪ Continuation token (ctoken)</li> <li>▪ Password to Apple ID - in some cases</li> </ul>

Parameters for running atex in the Terminal:

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

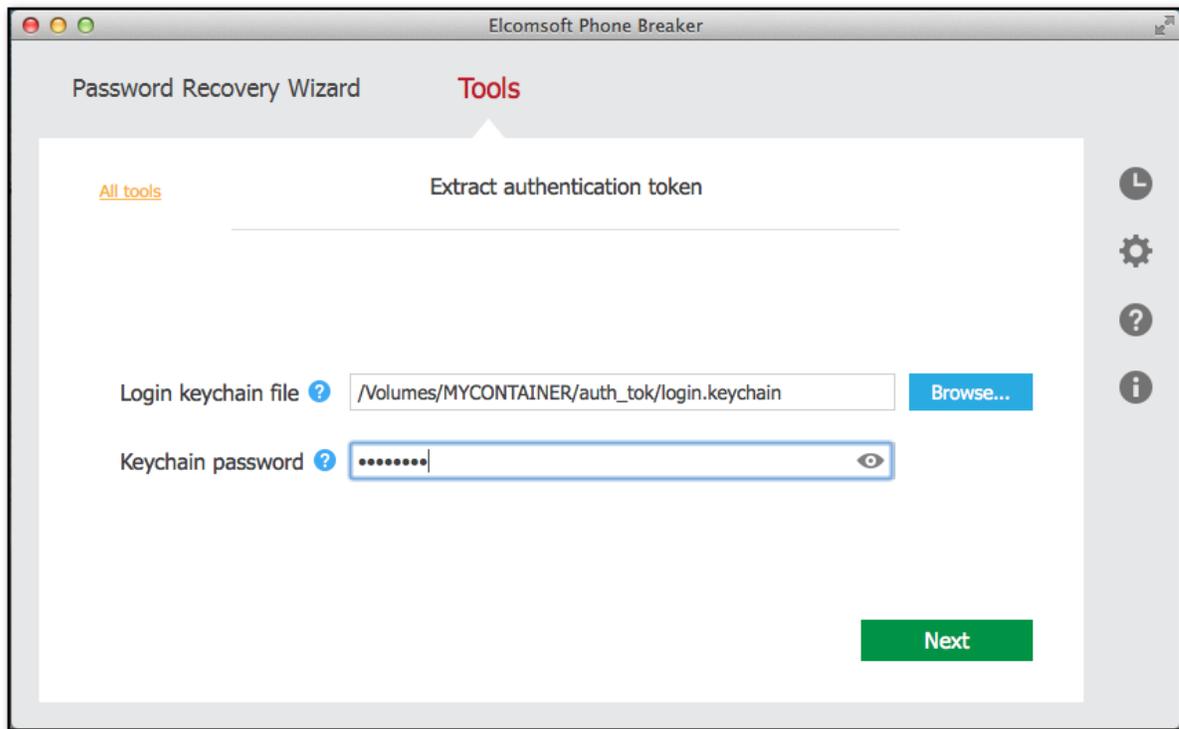
<b>-h</b> or <b>[--help]</b>	Displays help message
<b>-l</b> or <b>[--iCloudUserList]</b>	Displays usernames of iCloud users
<b>--getToken -u &lt;username&gt; -p &lt;password&gt;</b>	Gets the authentication token for a specified user. Username and password should be entered without brackets.
<b>-u</b> or <b>[--username]</b>	Indicates a specified user. Username should be entered without brackets.
<b>-p</b> or <b>[--password]</b>	Indicates a password for a specified user. Password should be entered without brackets.

#### 3.2.6.3.2 Extracting token on non-live macOS

EPB allows you to extract an authentication token to iCloud from a non-live macOS, 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:

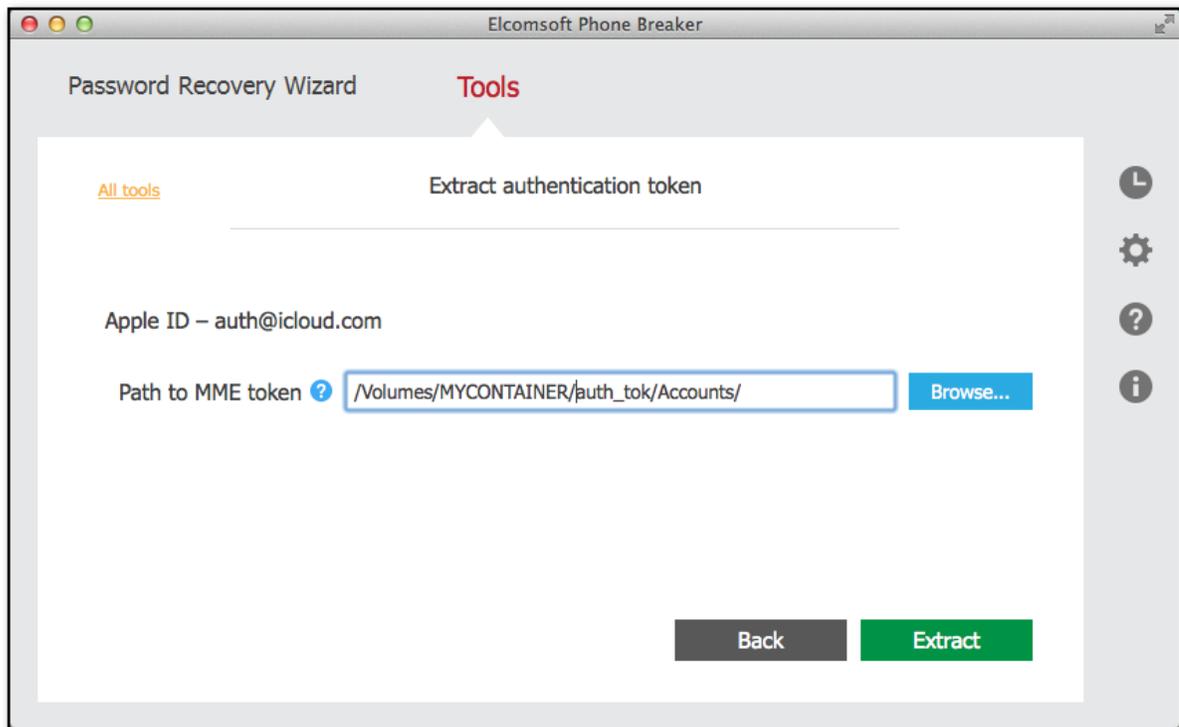
1. Mount the image of the disk containing the authentication token.
2. Run Elcomsoft Phone Breaker.
3. In the **Tools** menu, select the **Apple** tab.
4. Click **Extract authentication token**.
5. Define the path and password to the file containing the authentication token:
  - **Login keychain file:** 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 macOS 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](#).

## 3.3 Working with BlackBerry data

### 3.3.1 Working with BlackBerry Backups

#### 3.3.1.1 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 10.3.2.2876) 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.
- **macOS:** /Users/<name>/Documents/BlackBerry Backups.  
**NOTE:** You can change the default location for the backup folder on macOS 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.

### 3.3.1.2 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.

### 3.3.1.3 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).

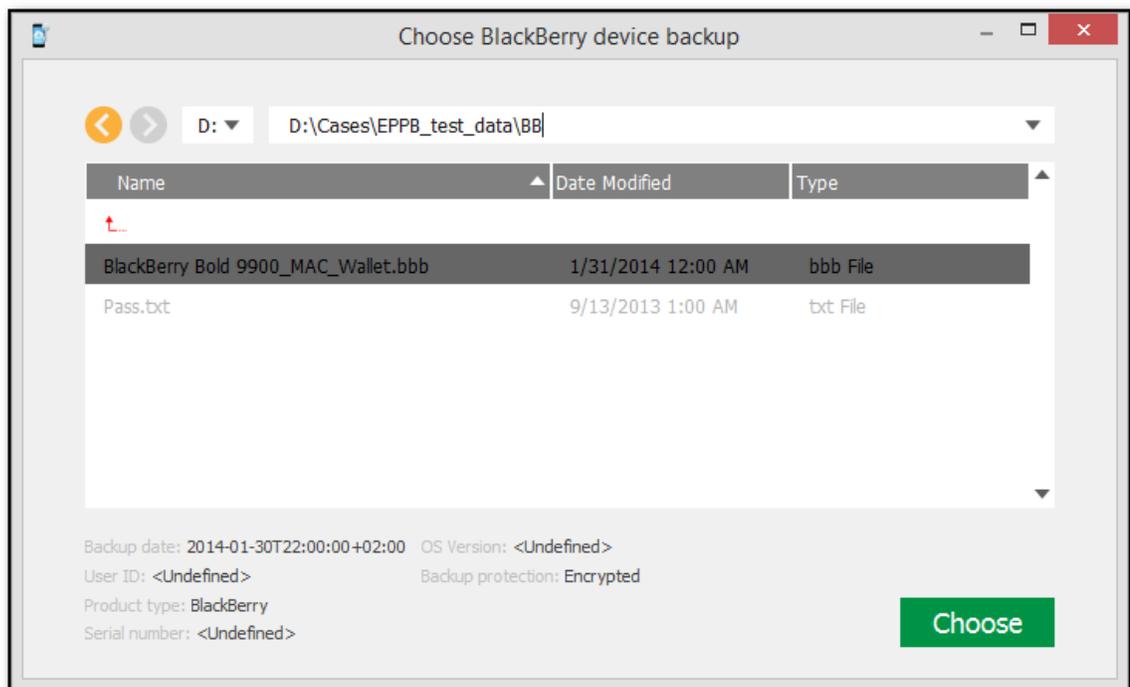
You need a BlackBerry database\*.ipd file or backup \*.bbb file to decrypt the backup.

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**.

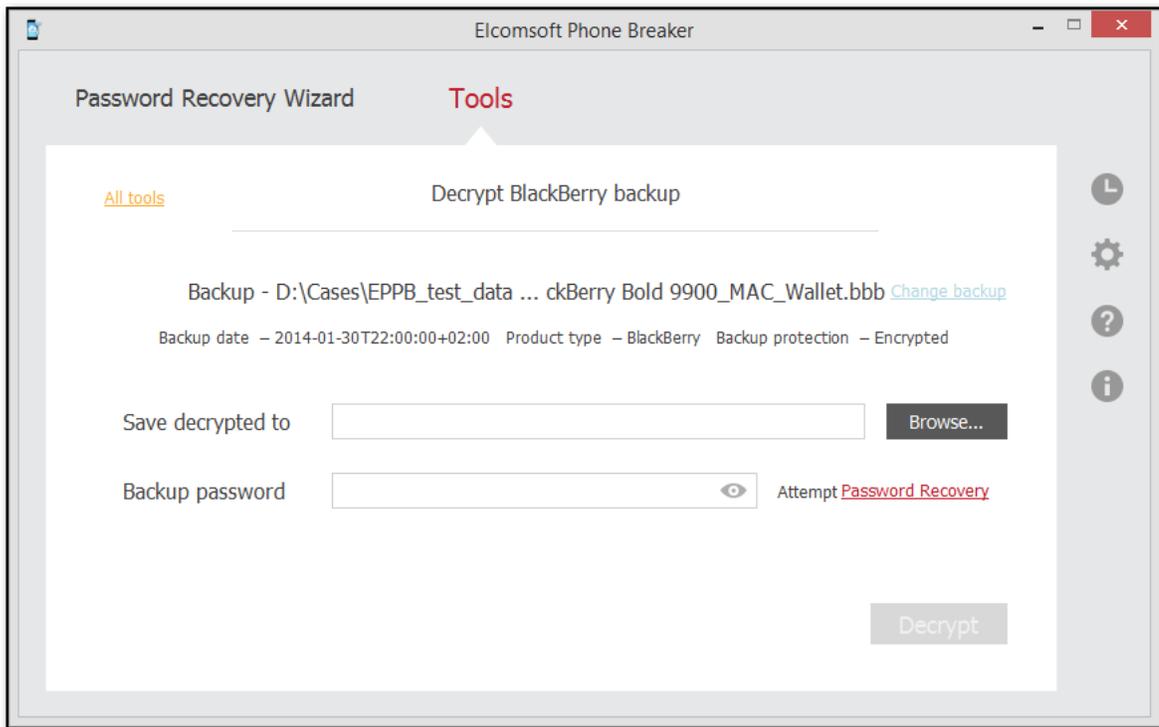
The properties of the backup are displayed below the grid.



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.

#### 3.3.1.4 Decrypt BlackBerry Link backup

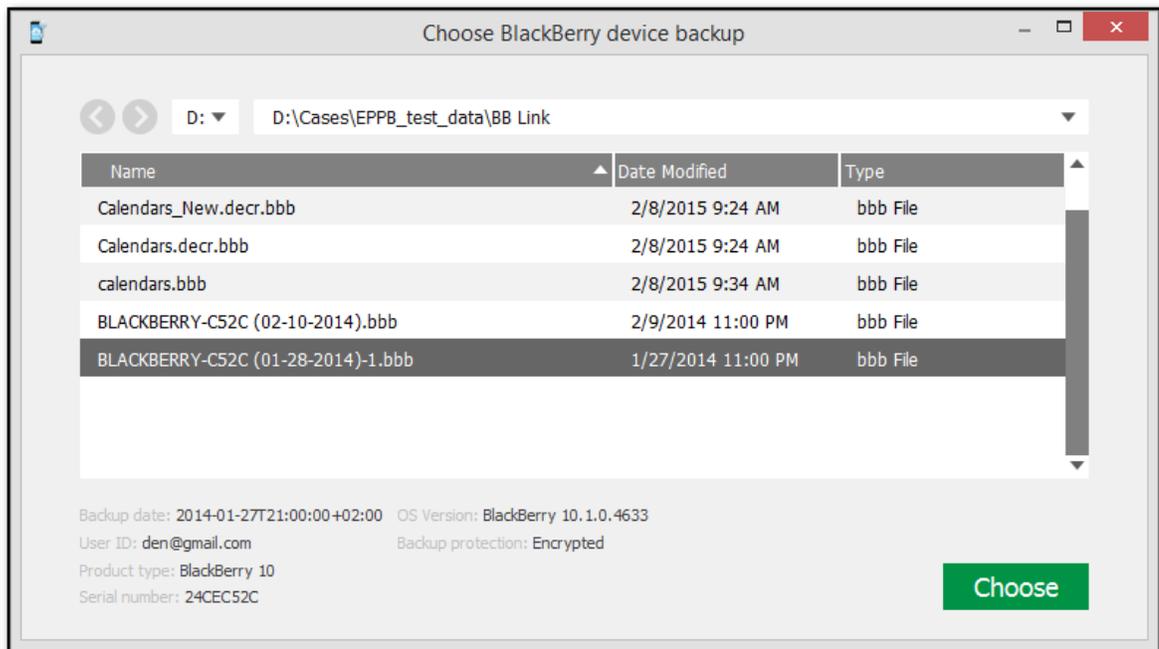
EPB allows you to decrypt the backups for BlackBerry 10 (up to BBOS 10.3.2.2876) devices created by BlackBerry Link.

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:

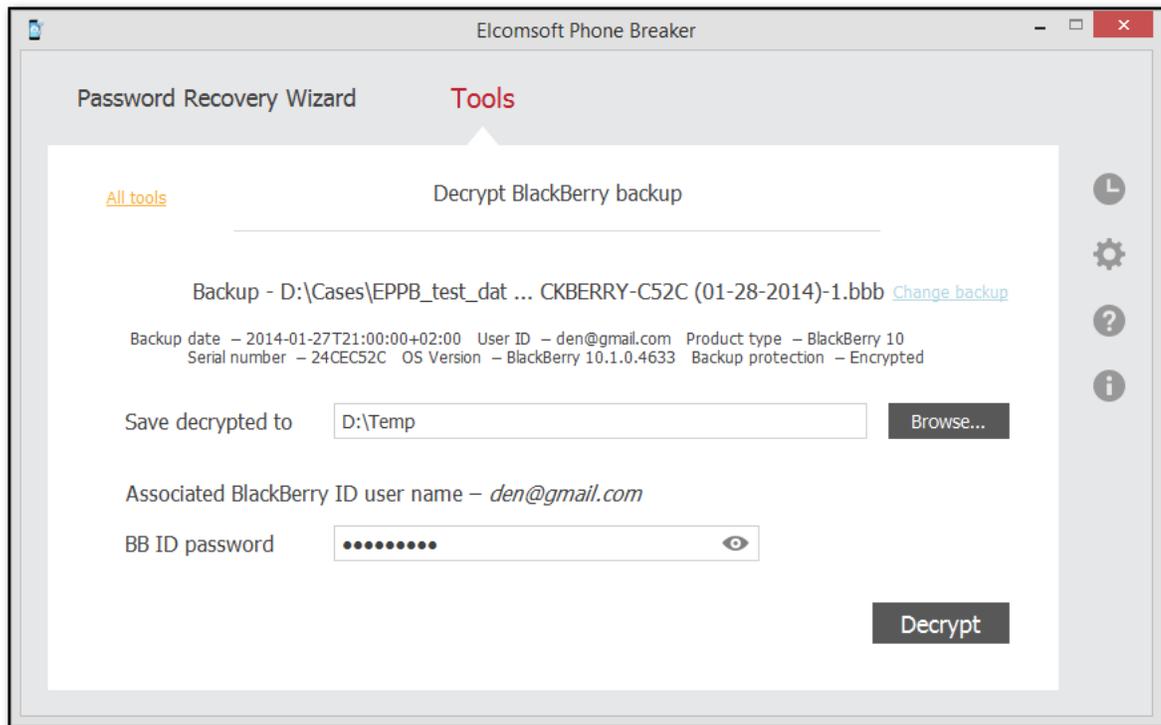
1. In the **Tools** menu, select the BlackBerry tab.
2. Select **Decrypt backup**.
3. Select the BlackBerry backup file (\*.bbb) by drag-and-dropping it to the **Decrypt backup** window, or click **Choose backup**.
4. In the opened window navigate to the backup file by entering the file path in the path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

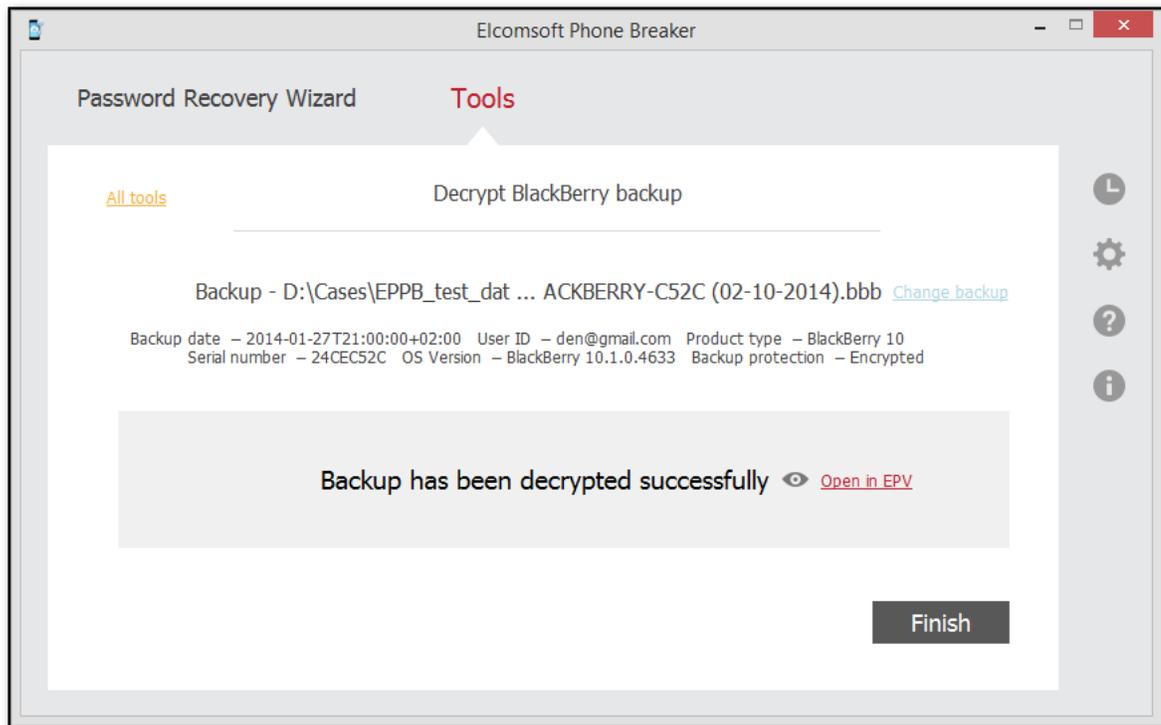
7. Click **Decrypt**.

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.

If you have Elcomsoft Phone Viewer installed on your computer, you can explore the backup content by clicking the **Open in EPV** link.

**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.

### 3.3.1.5 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.**

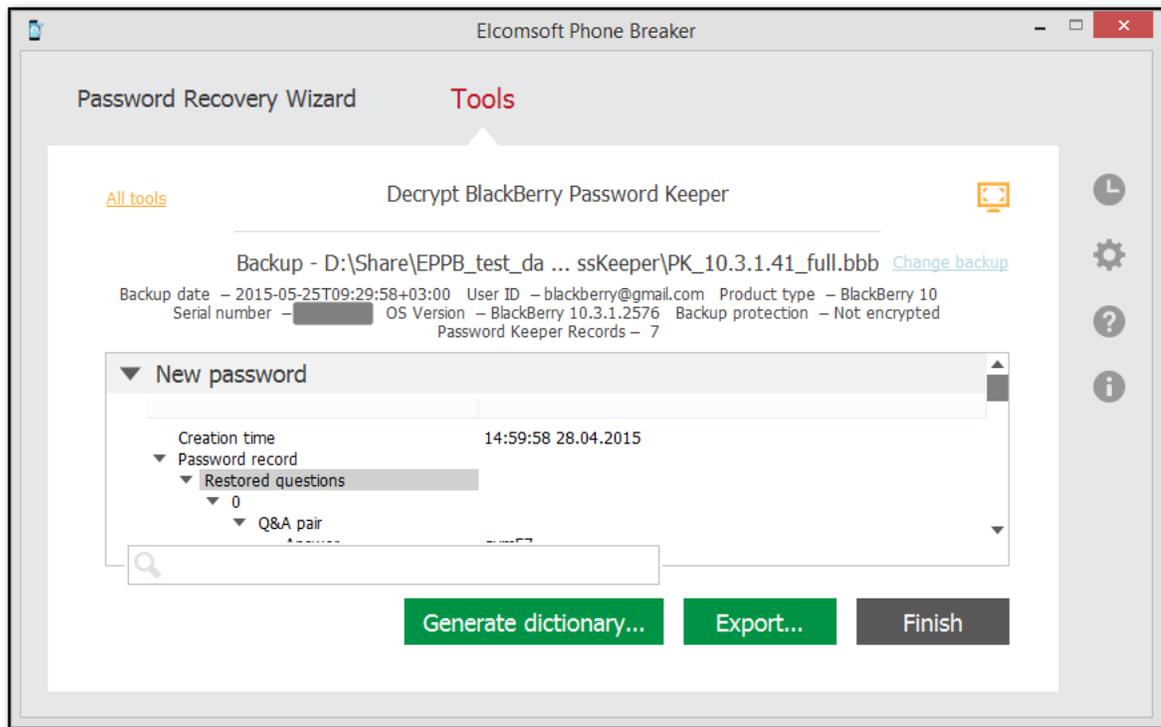
For older versions of BlackBerry OS, [recover the master password](#) to BlackBerry Password Keeper container using EPB for Windows.

**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.

### 3.3.2 Working with SD card

#### 3.3.2.1 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](#).

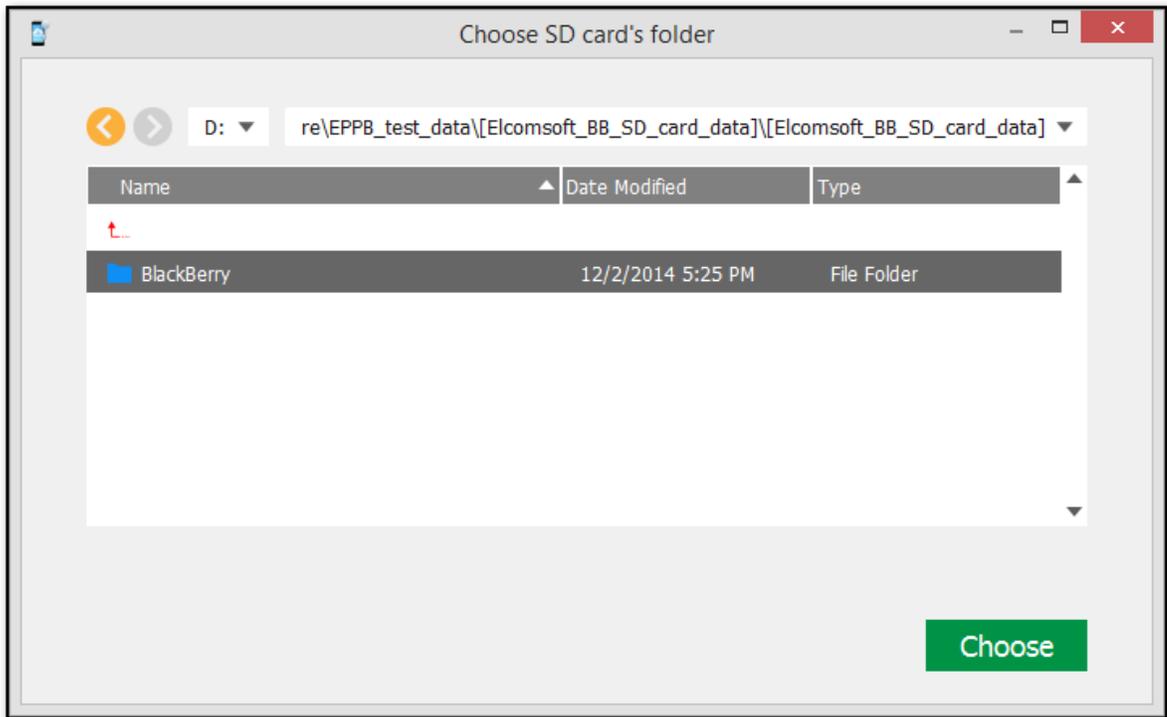
### 3.3.2.2 Decrypt BlackBerry SD card

**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.**

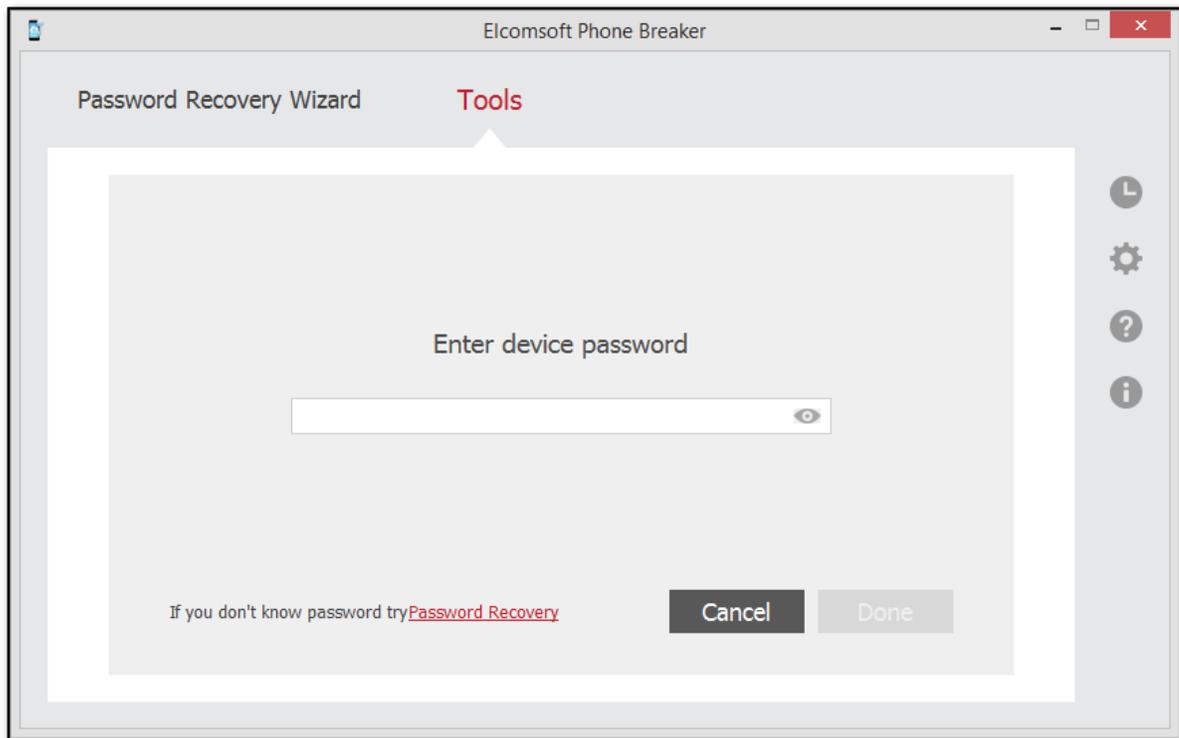
To decrypt the encrypted SD card, do the following:

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.



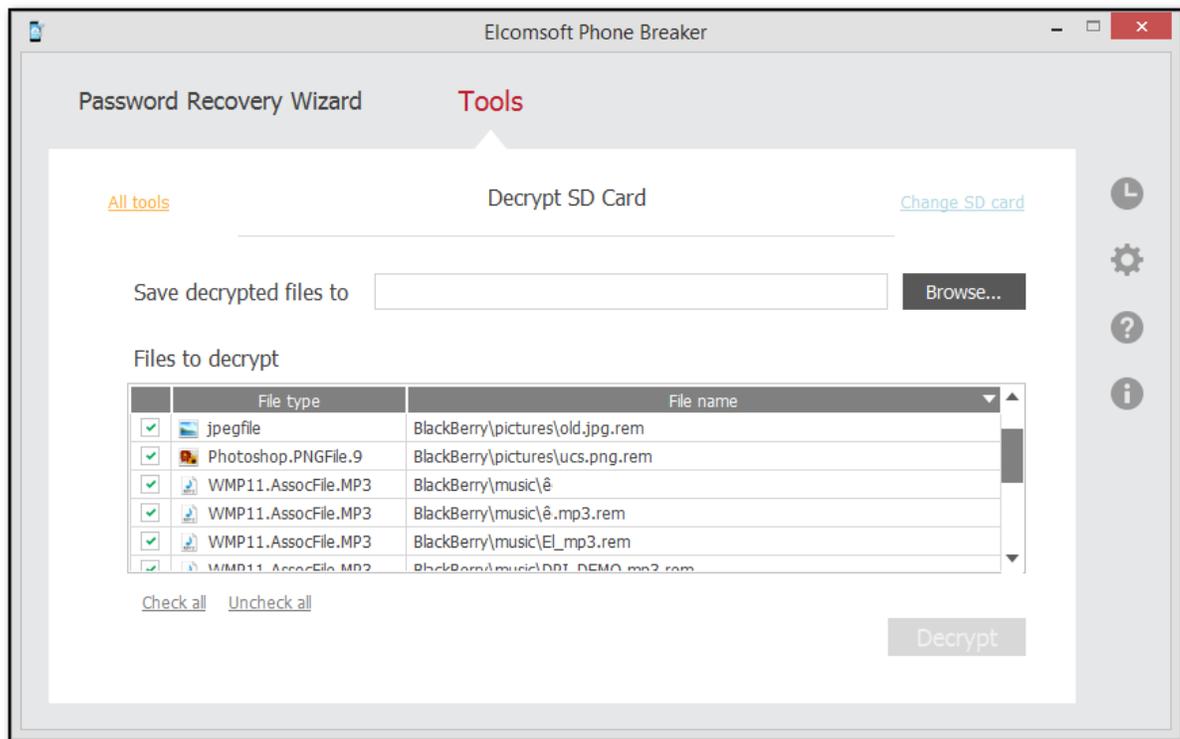
Click **Done** when you have entered the password.

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**.

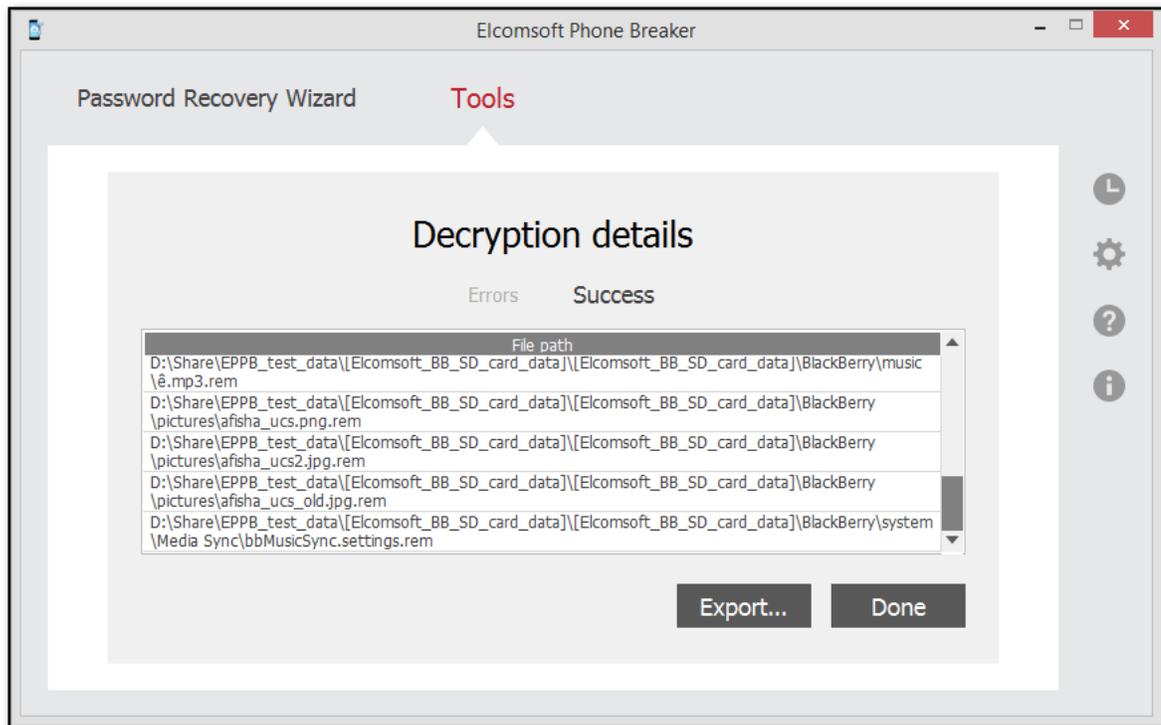
10. Click **Finish** to close the **Decrypt SD Card** page.

### 3.3.2.3 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**.

## 3.4 Working with Microsoft account data

### 3.4.1 About Microsoft account data

You can download Microsoft account data synced from devices or Windows PCs where the user signed into this account. EPB downloads this data from the cloud in the form of a backup.

EPB allows you to download Microsoft account data provided you know the credentials to this Microsoft account. The following data can be downloaded:

- **Contacts**
- **SMS Messages**
- **Notes** (downloaded from OneNote)
- **Calls**
- **Search History**
- **Browsing History**
- **Locations History**

- Skype

**NOTE:** If Skype attachments (except Pictures) are sent more than 30 days ago, they will be deleted from MS server and will not be available for downloading via EPB. In this case only attachments metadata will be available for downloading. More detailed information about terms of data storage can be found here <https://support.skype.com/en/fac/FA34893/how-long-are-files-and-data-available-in-skype>

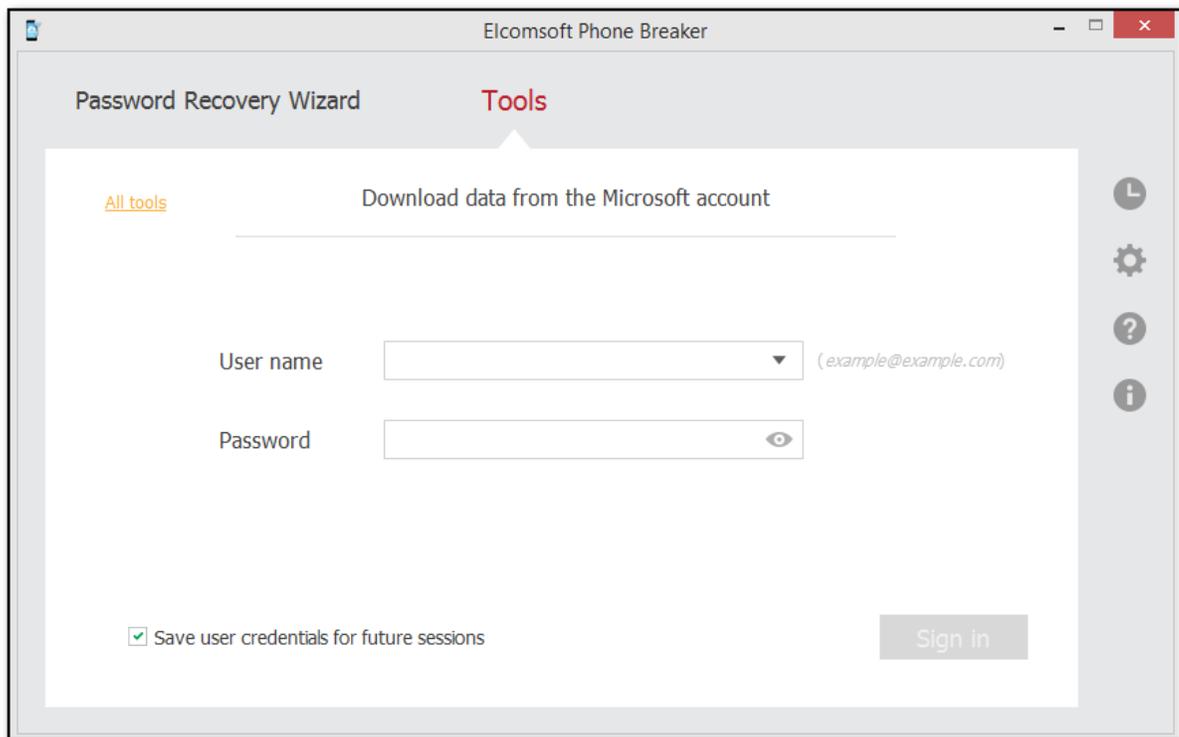
Downloaded data is saved in an archive containing databases with downloaded information and a *Manifest.xml* file containing information on every device associated with the account and file name for every database file.

### 3.4.2 Downloading Microsoft account data

To download synced Microsoft account data, do the following:

1. In the **Tools** menu, select the **Microsoft** tab, and click **Download data from the Microsoft Account**.
2. Enter the user name and password for the Microsoft account.

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

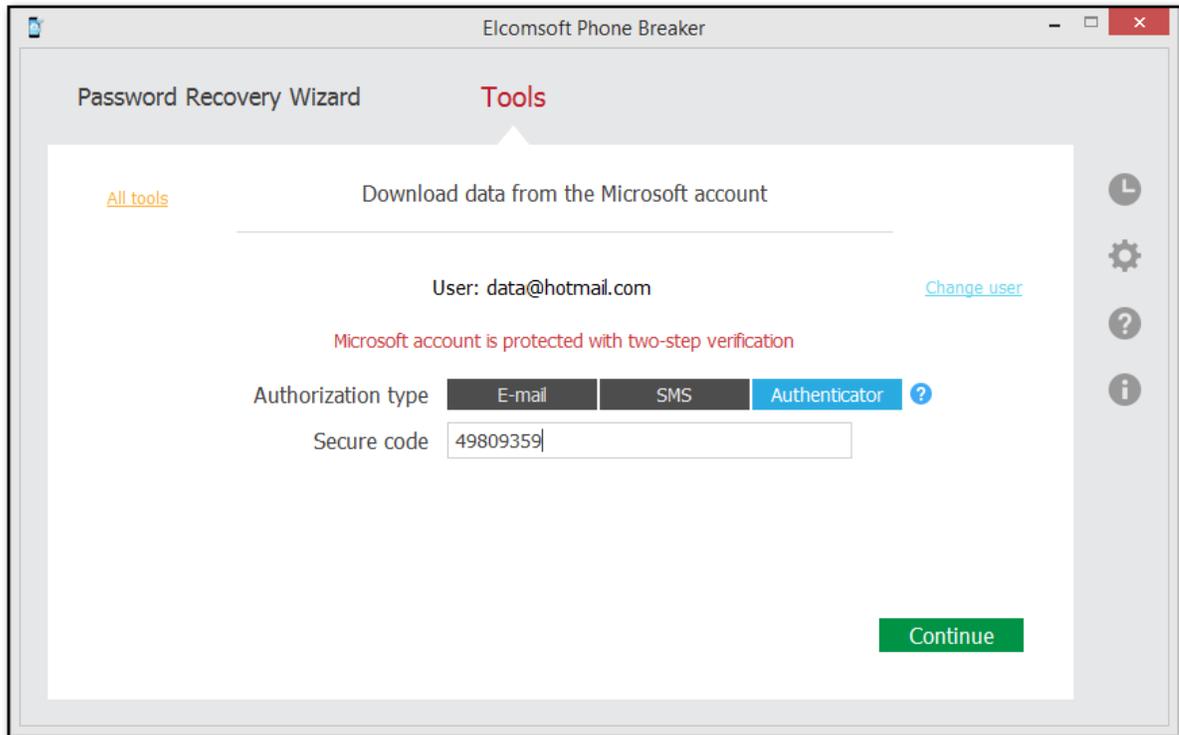


3. If your account is protected with two-factor authentication, you need to enter the secure code. The following authorization types are supported:

- E-mail
- SMS

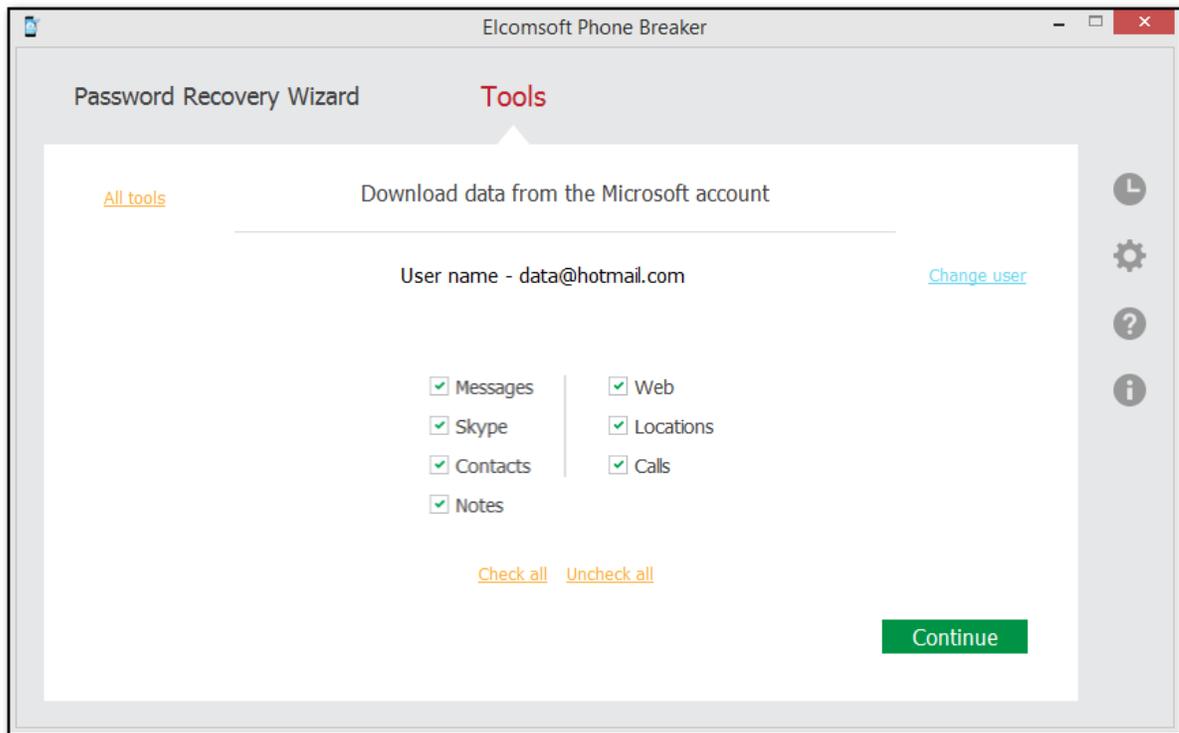
- Authenticator: EPB supports 8-character codes generated in the standard Microsoft authenticator and 6-character codes generated in third-party apps.

Choose the Authorization type, enter the secure code, and click **Continue**.

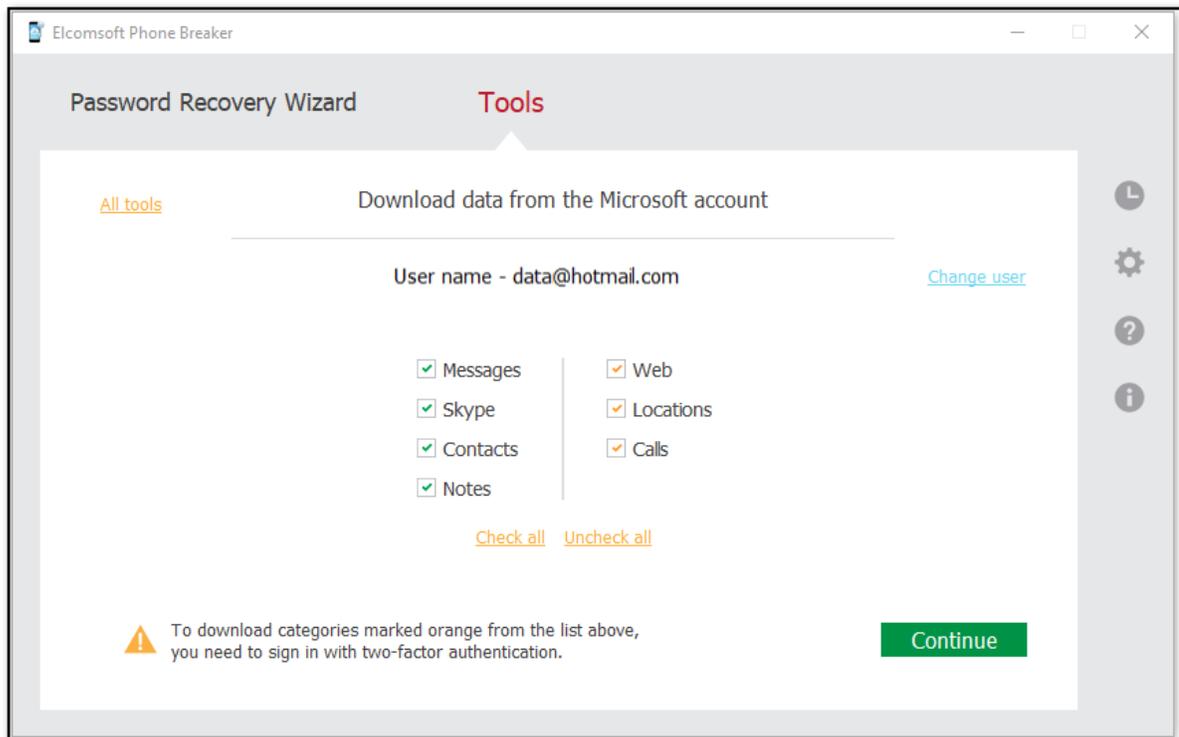


4. Select the data categories you want to download and click **Continue**.

If your account is protected with two-factor authentication, your download starts immediately.



If your account is not protected with two-factor authentication, you can see the categories which you can download only after you sign in with two-factor authentication. Such categories are marked orange. In the current version of EPB, there are three such categories, **Calls**, **Web**, and **Locations**.



If your account is not protected with two-factor authentication and you want to download the **Calls**, **Web**, or **Locations** category, choose how you want to receive your secure code:

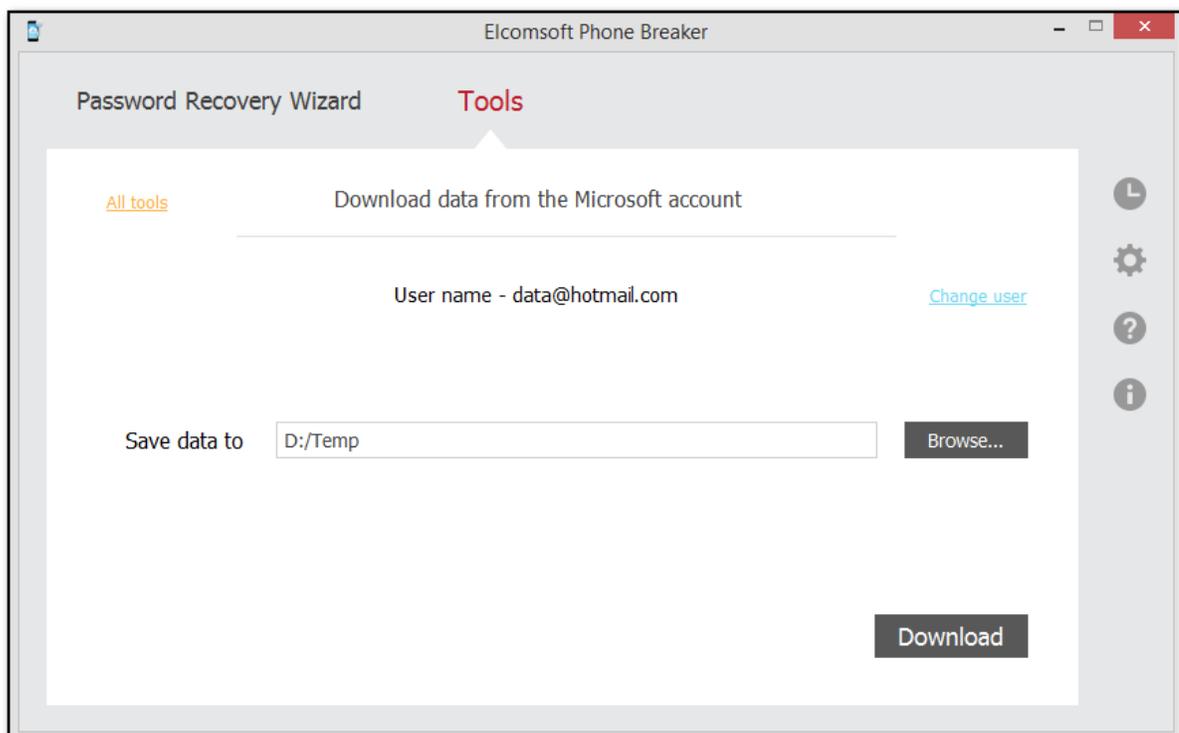
- Trusted e-mail address
- SMS

Complete the trusted e-mail or trusted phone number information and click **Send code**. You will receive a secure code to this email address or phone number. Enter the received secure code in the **Secure code** field and click **Continue**.

5. Select location for saving data downloaded from the Microsoft account.

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

Click **Download** to start downloading synced Microsoft account data.

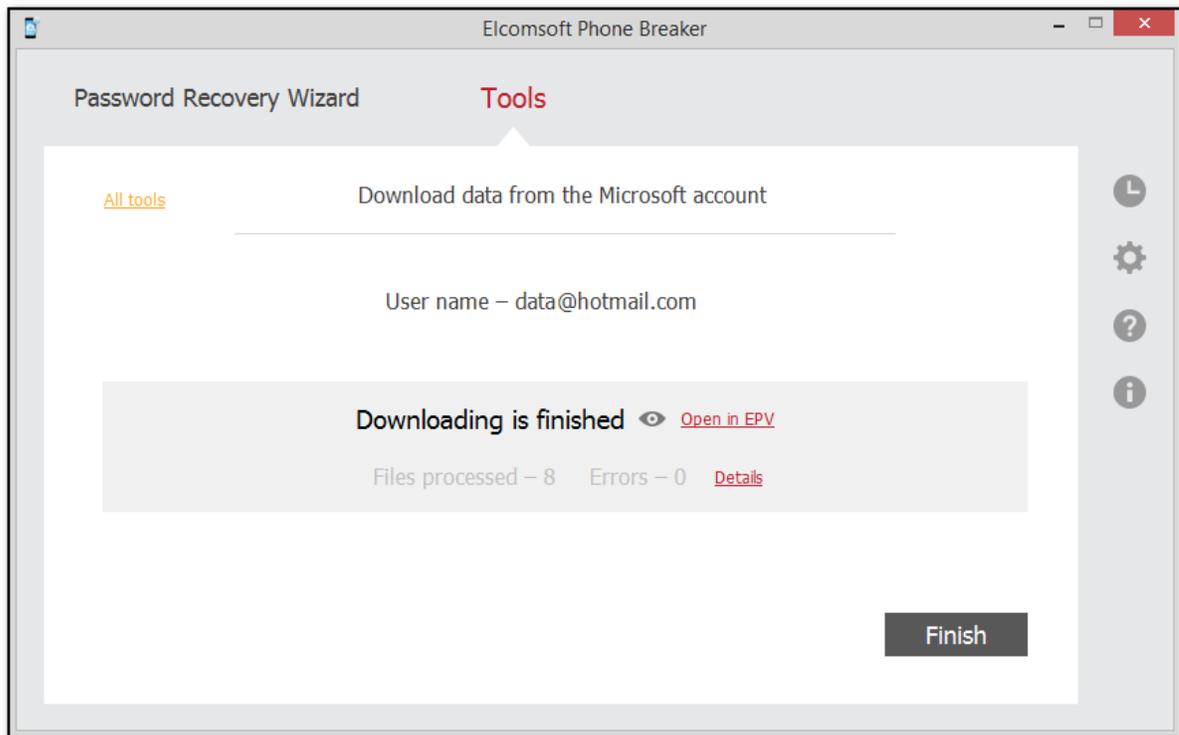


6. Data downloading begins. You can view the number of processed files and the number of errors received during the download.

7. 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.

If you have [Elcomsoft Phone Viewer](#) installed on your computer, you can explore the backup content by clicking the **Open in EPV** link.

To view detailed information about downloaded files and errors that occurred during the download, click **Details**.



8. Click **Finish** to close the **Download data from the Microsoft account** page.

## 3.5 [Windows] Recovering passwords

### 3.5.1 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](#)

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

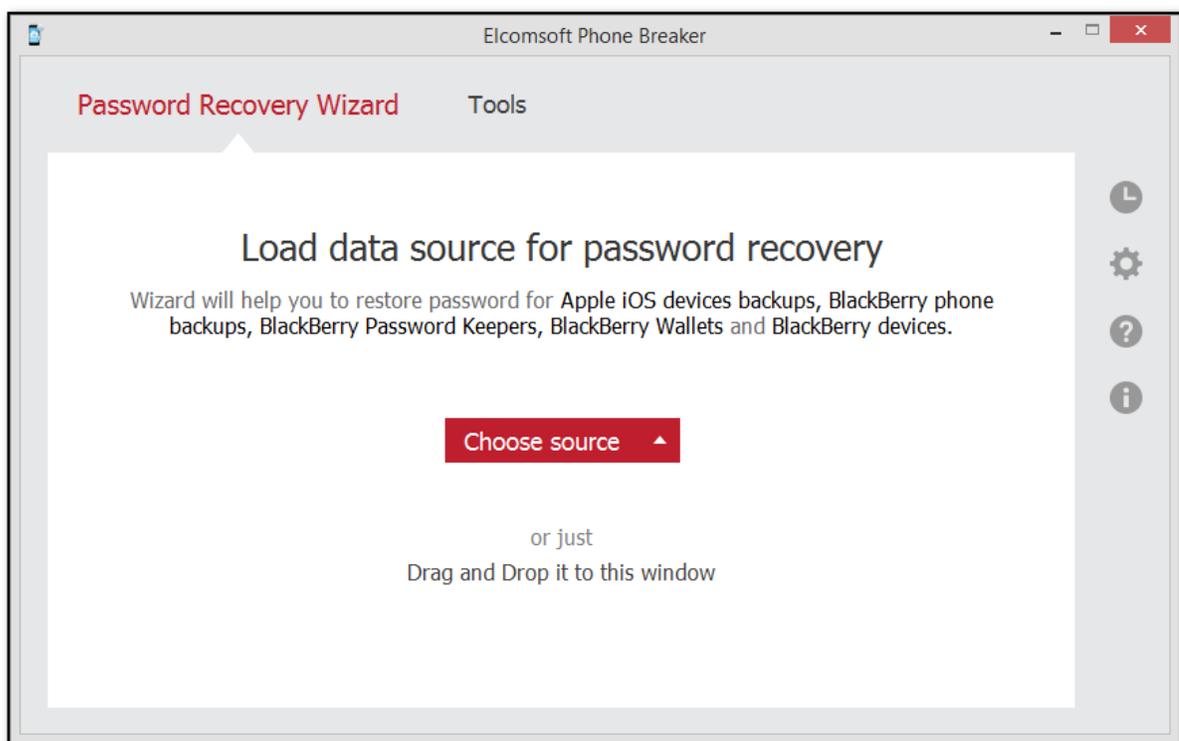
Storage type	Necessary files
iTunes backup	Manifest.plist (for iOS 10 or later, the Manifest.db file must be present in the same folder)
BlackBerry device backup	*.ipd or *.bbb backup file
BlackBerry Password Keeper backup	*.ipd or *.bbb backup file
BlackBerry Wallet backup	*.ipd or *.bbb backup file
BlackBerry device password	info.mkf file from the encrypted media card

**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.

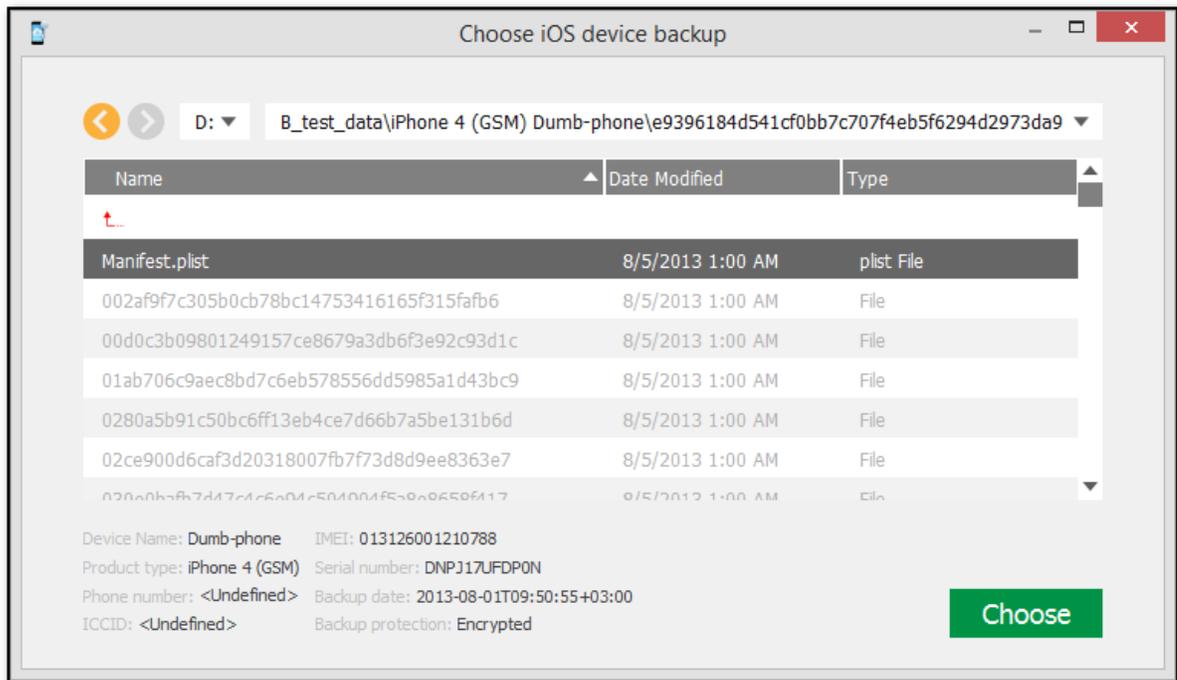
To recover the password, do the following:

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**.

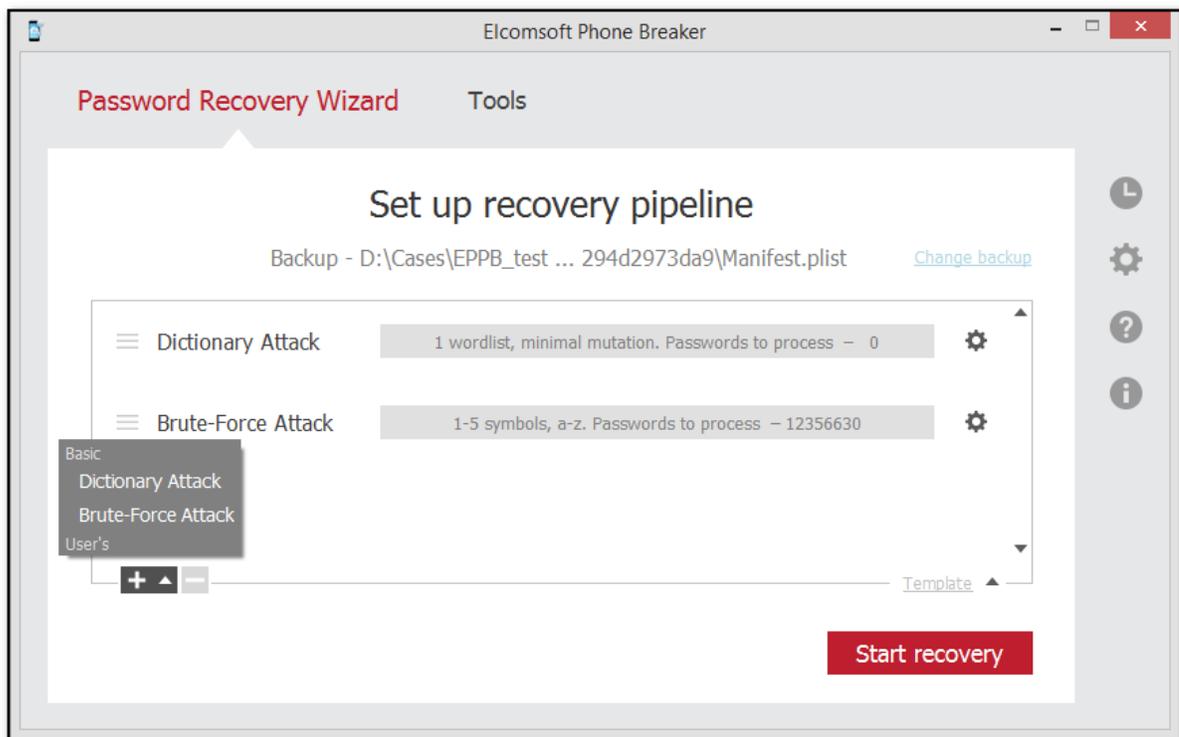
**NOTE: The properties of the selected storage are displayed below the grid.**



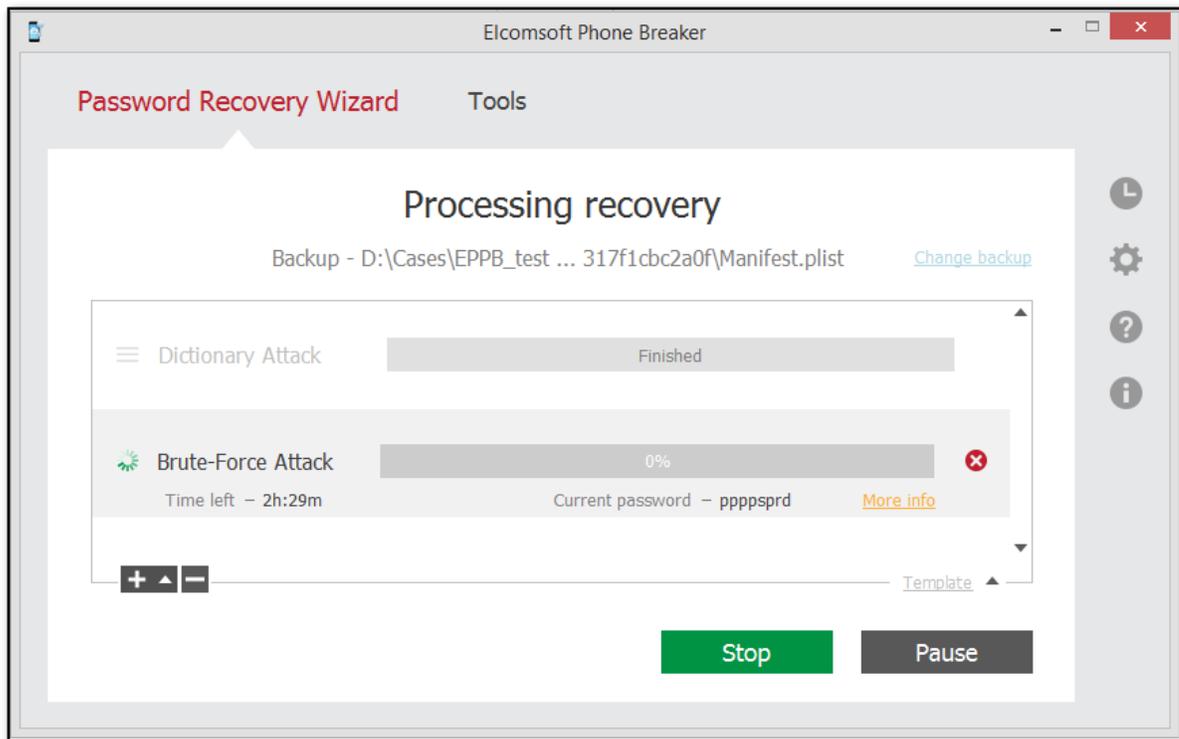
5. When the storage is added, define the attacks that will be used to break the password.

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.



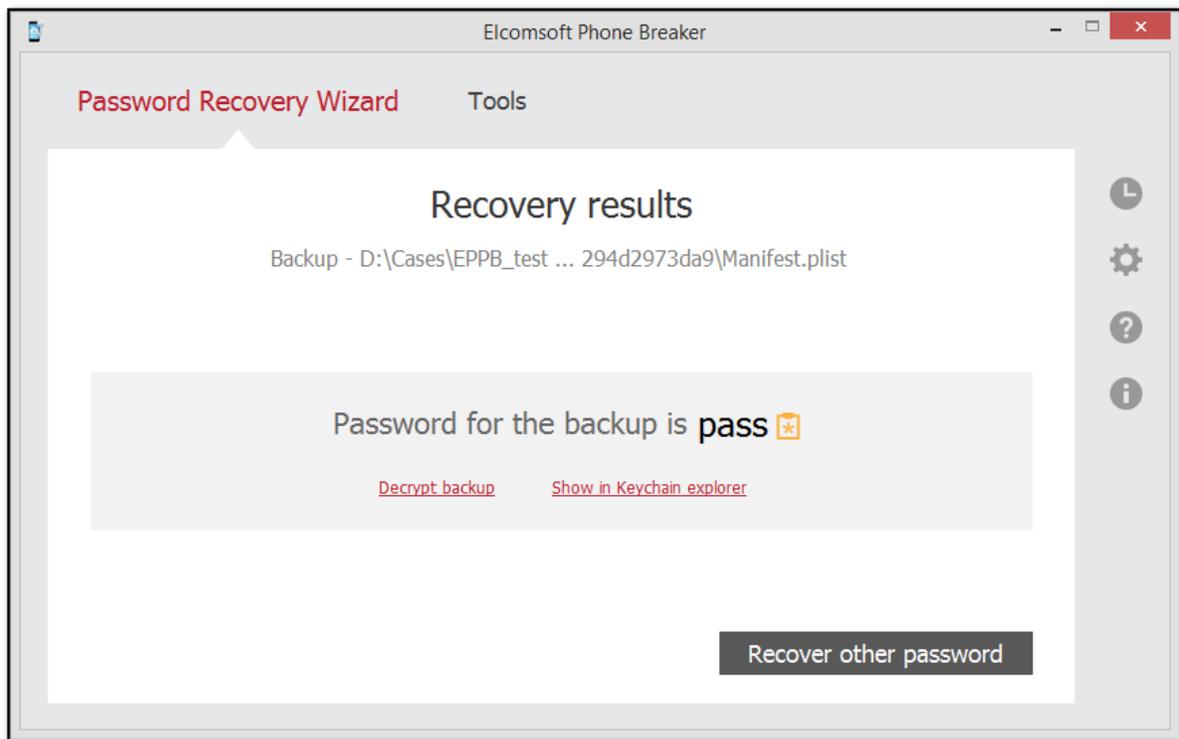
6. Click **Start recovery**.
7. The password recovery starts. You can view the estimated time left and the currently processed word.



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

8. You can pause or stop the recovery process by clicking the **Pause** and **Stop** buttons.

9. 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**. Please note, all the backup files must be located in the same folder as the Manifest.plist file.

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

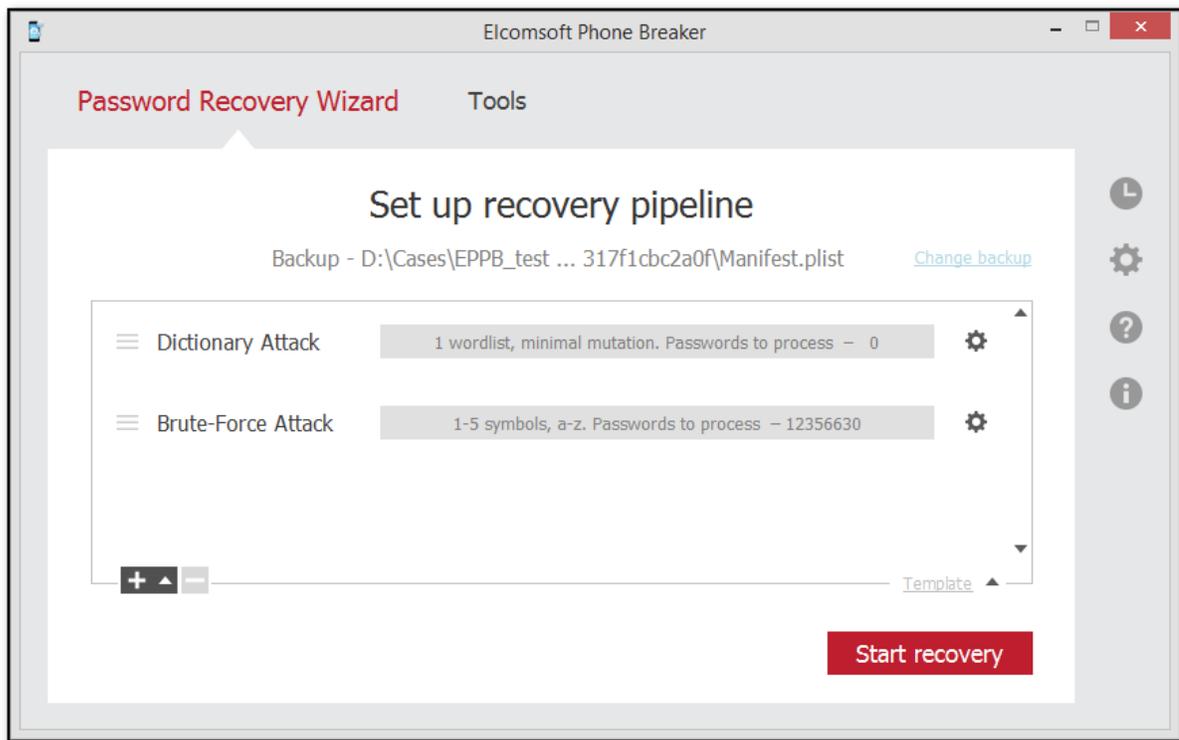
### 3.5.2 Password recovery attacks

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.

### 3.5.3 Saving password recovery attack sessions

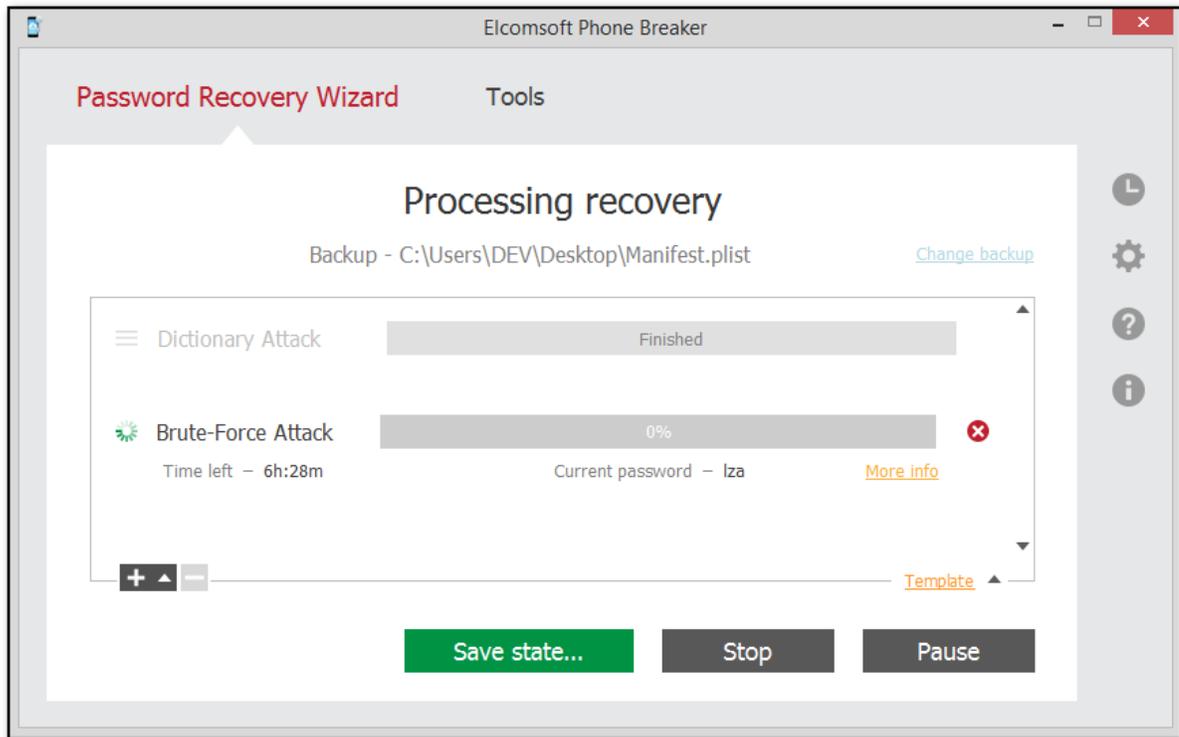
You can save and resume the pipeline and the intermediate state of password recovery attack sessions. Saving can be performed manually or automatically.

#### Saving and resuming attack sessions manually

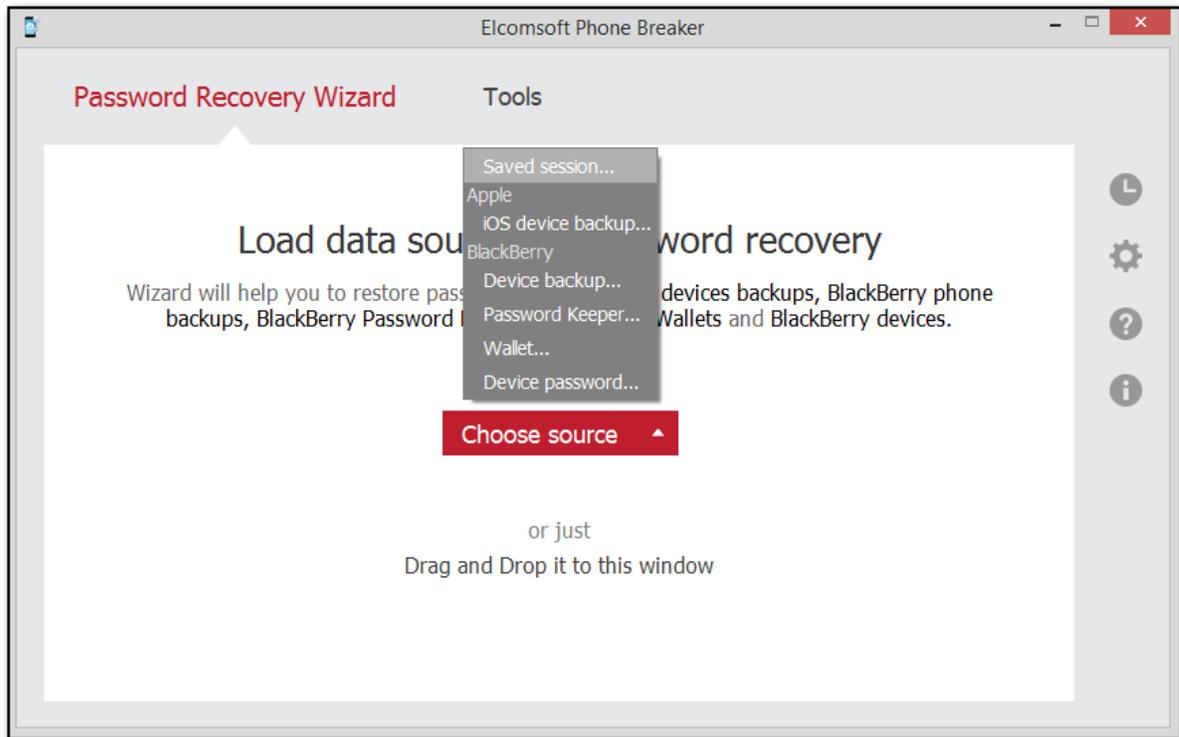
To save the state of a password recovery attack session manually, do one of the following:

- click **Pause**, and then click **Save State** and navigate to the destination path.
- click **Save State**, and then navigate to the destination path. In this case, the attack is paused and resumed automatically once the session is saved.

By default, the first-time destination path is %USERPROFILE%\Documents. On next saves, the latest destination path is displayed by default.



To resume a manually saved attack session, select **Saved session** in the main menu in Password Recovery Wizard, and then navigate to the session file. The attack session will continue from the moment it was stopped.



### Autosaving sessions

If the application was terminated before the attack was completed, attack sessions are saved automatically. By default, autosaved sessions are stored in %AppData%\Elcomsoft\Elcomsoft Phone Password Breaker\Sessions\~autosave.epb).

You can also configure EPB to save attack sessions automatically at a desired frequency. To do this, go to [EPB settings > General](#) and:

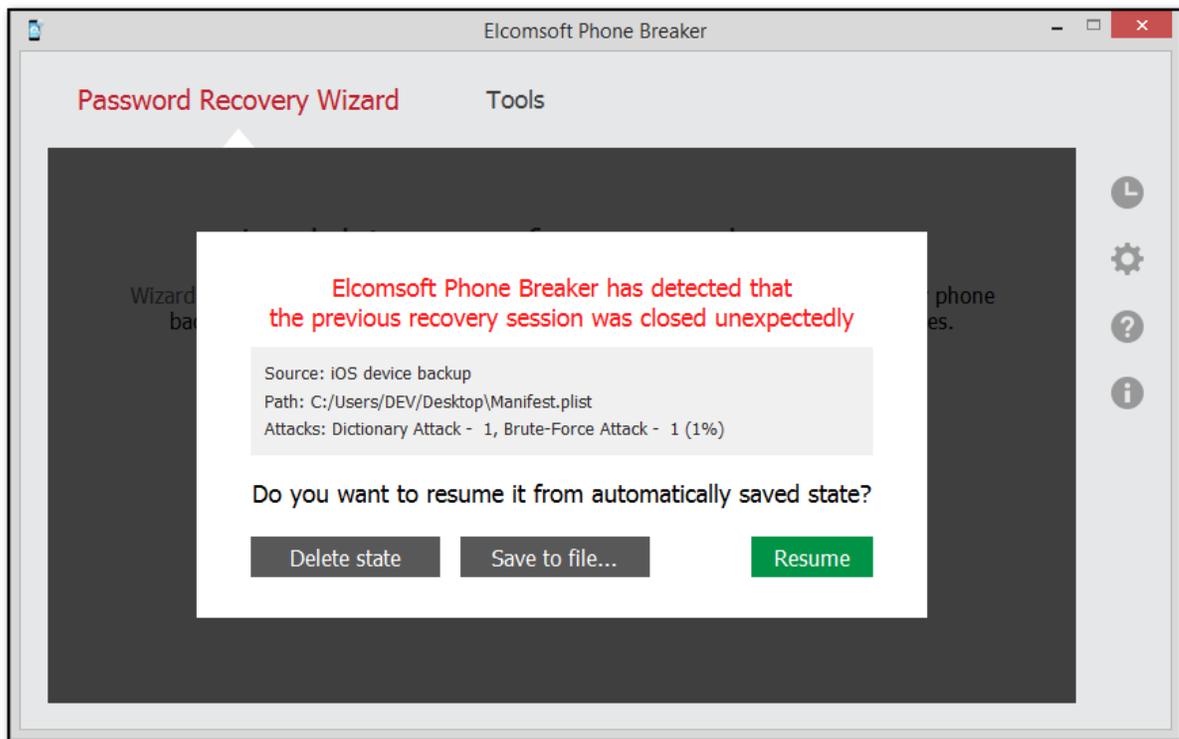
- make sure the **Automatically save password recovery session every <> minutes** option is selected (by default, it is selected).
- set the desired autosave frequency to any time interval between 1 and 180 minutes (the default frequency is every 5 minutes).

If an attack is completed successfully, or if you press **Stop** during an attack session, the autosaved session file is deleted automatically.

### Resuming autosaved sessions

If the application was terminated, you will be offered to resume an autosaved attack session when you restart EPB and select Password Recovery Wizard. You can see the following information on the autosaved attack:

- **Source:** the backup type.
- **Path:** the destination path to the backup file.
- **Attacks:** attacks and their status (**Finished** for completed attacks and completion percentage for interrupted attacks).

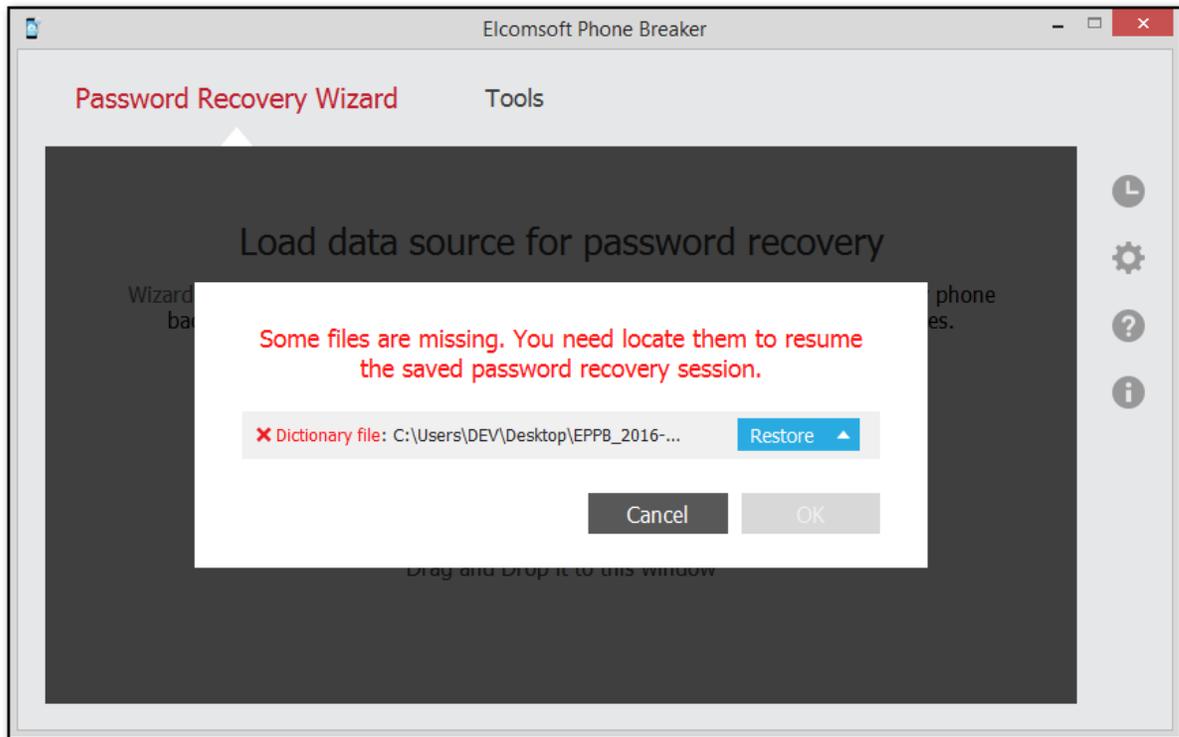


Press **Resume** to resume the autosaved attack session from the moment it was interrupted.  
Press **Save to file** to save the autosaved attack session manually.  
Press **Delete state** to delete the autosaved attack session.

### Resuming attack sessions with missing files

If, after restarting EPB, the backup file or an attack dictionary is missing in the specified destination folder, click **Restore** and select one of the following:

- **Browse**: to navigate to the files you need.
- **Skip**: to resume the attack session without the missing files.



### Resuming attack sessions in a different environment

You can resume an attack session in a different environment (on a Windows-powered computer with different CPU and GPU). Also, if you pause an attack and change CPU and/or GPU [settings](#) on your computer, EPB will resume the attack with the new settings applied.

### 3.5.4 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.**

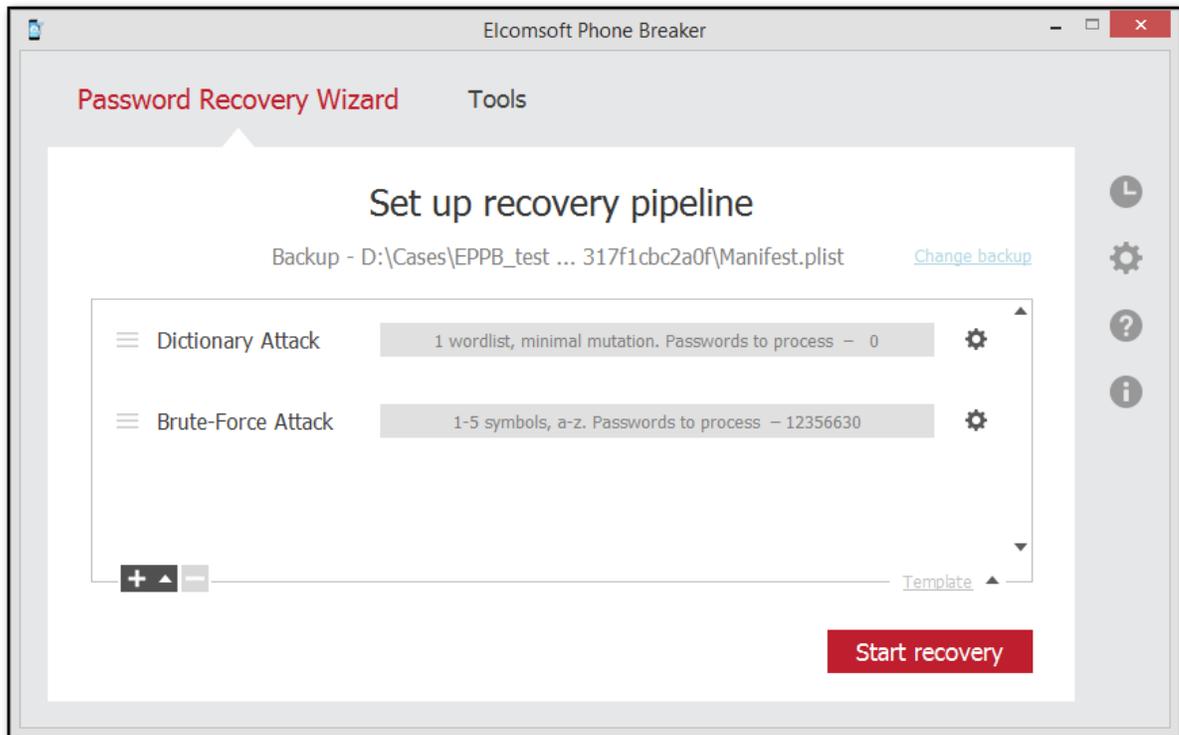
Dictionary attack allows you to check the words in a dictionary to see if they match the required password. The words can be optionally checked with mutations with various levels of difficulty. Mutation means changing the word by certain rules (e.g. using all lowercase or all uppercase letters, changing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

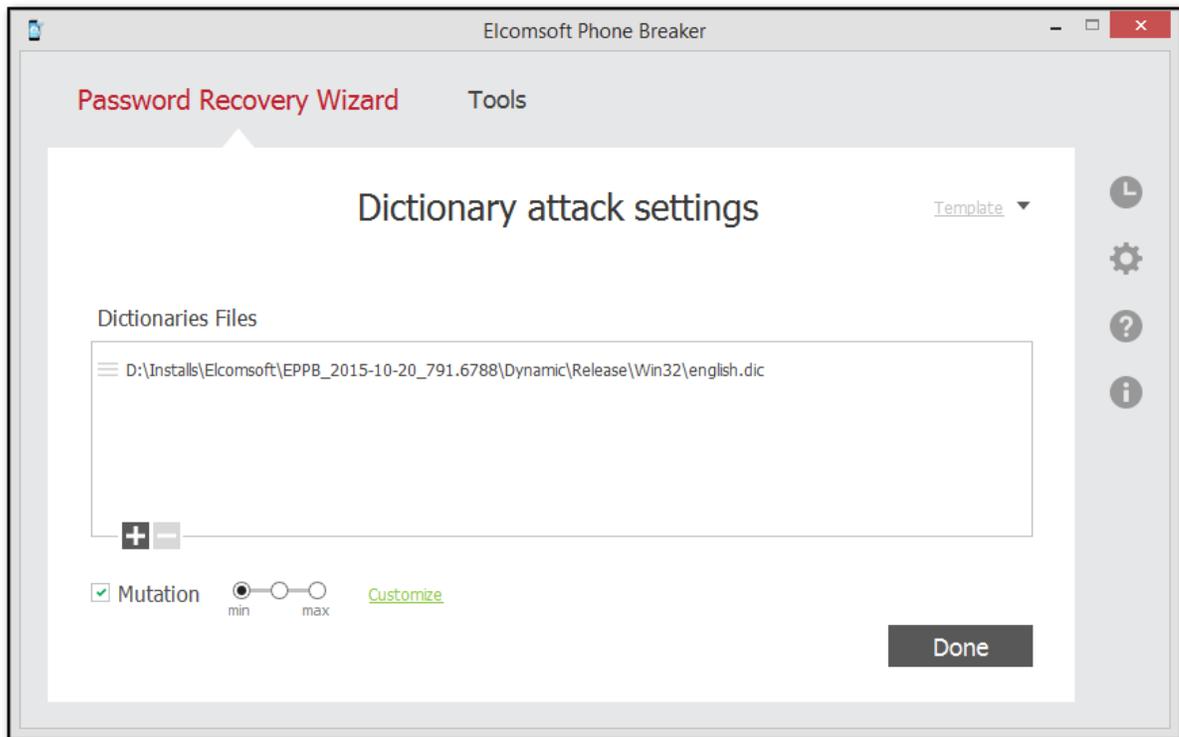
To manage the Dictionary attack settings, [select the backup](#) to be unlocked, double-click the Dictionary attack, or click  next to it.

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:



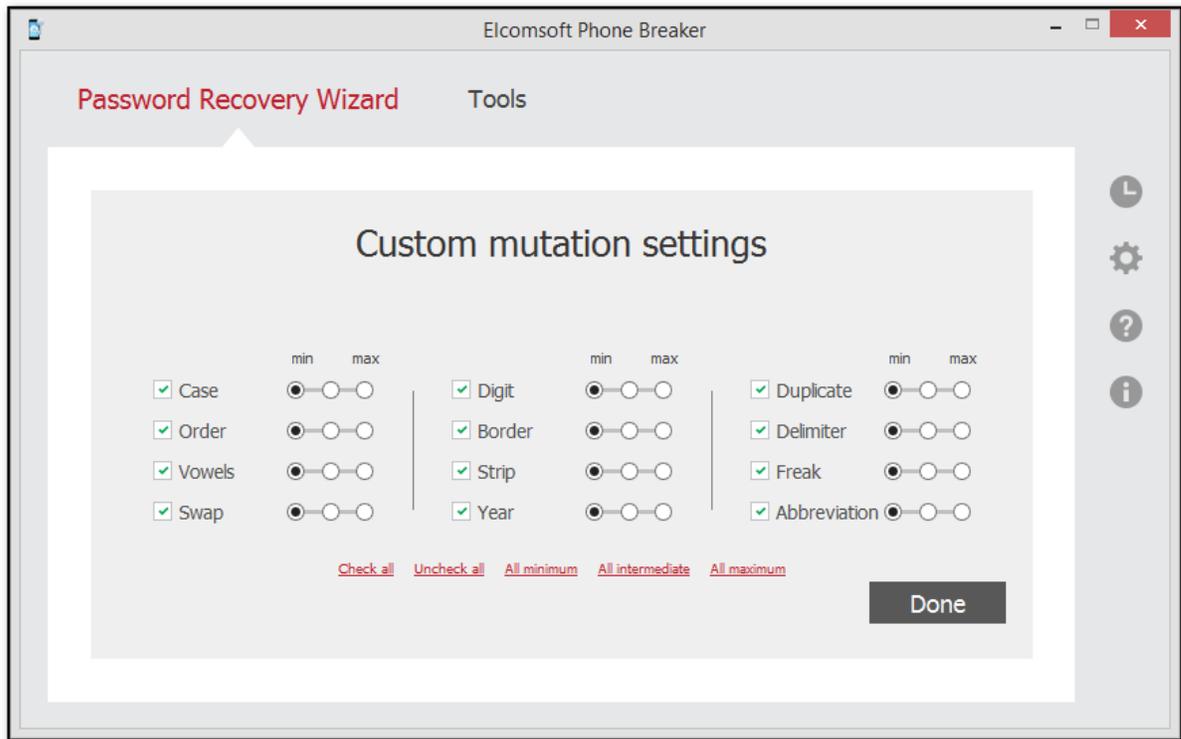
The following options are available:

- **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"> <li><b>Minimal</b> level checks the words in the dictionary written in lowercase, uppercase, and with the first letter written in lowercase and others in uppercase.</li> <li><b>Intermediate</b> level checks all the combinations from the minimal level and also the first and the last letter of the word written in uppercase.</li> </ul>	<p><i>password, PASSWORD, pASSWORD.</i></p> <hr/> <p><i>password, PASSWORD, Password.</i></p>

Mutation Name	Description	Levels	Examples
		<ul style="list-style-type: none"> <li>• <b>Maximal</b> level checks combinations from the previous levels and also combinations with every second letter written in uppercase.</li> </ul>	<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"> <li>• <b>Minimal</b> level allows adding numbers (0-9) at the end of the word, checking lowercase words, and the words starting from the capital letter.</li> <li>• <b>Intermediate</b> level allows checking words written in uppercase and words with digits in the beginning.</li> <li>• <b>Maximal</b> level allows checking combinations in the range 00 - 99.</li> </ul>	<i>password1, Password1. 3password, 3PASSWORD. 33password, 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>

Mutation Name	Description	Levels	Examples
Duplicate	Duplicating the characters in the password.	The same as general levels.	<i>ppassword, paassword, passsword, passwword</i>
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@\$\$word and p@\$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.

### 3.5.5 Brute-Force attack options

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

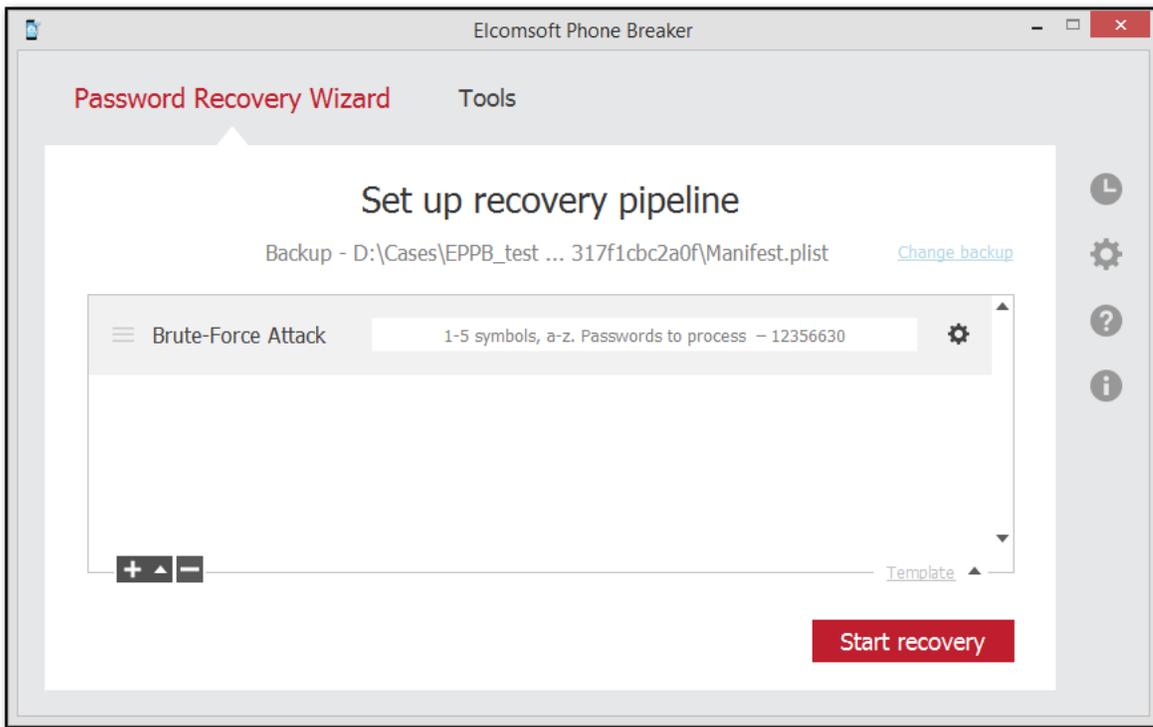
**NOTE: Recovering passwords is available only when using EPB for Windows OS.**

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

#### 1. Attack selection

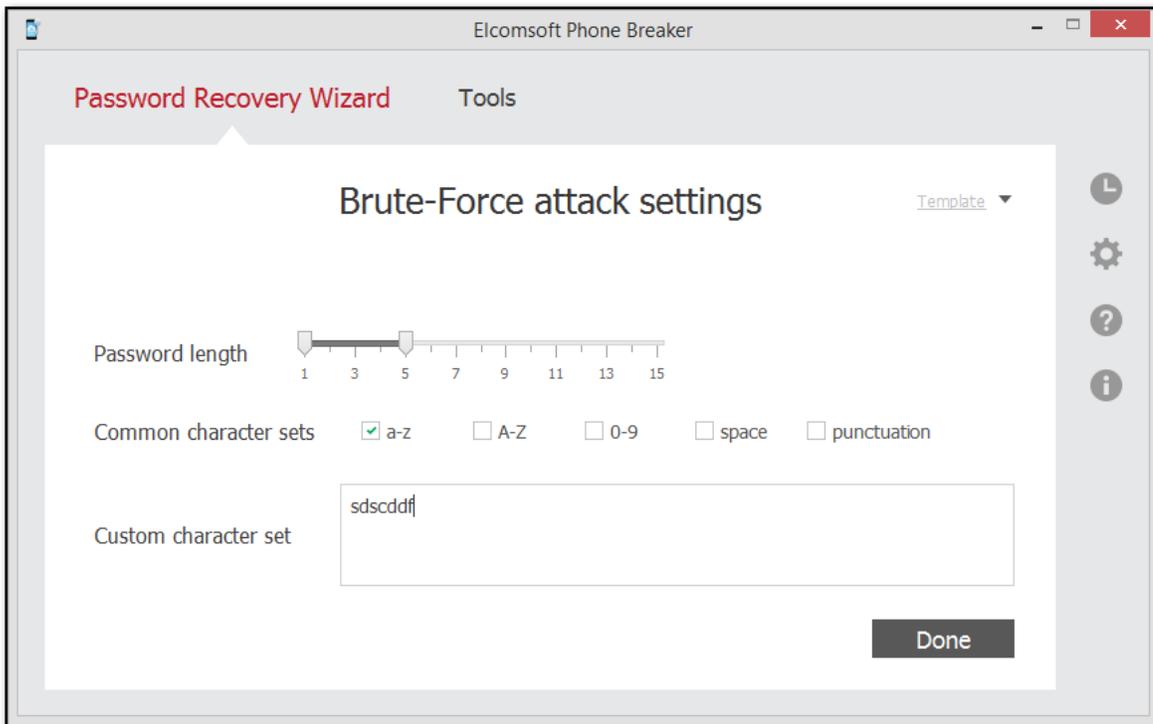
To manage the Brute-Force attack settings, [select the backup](#) to be unlocked, double-click the Brute-Force attack, or click  next to it.

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.

## 3.5.6 Templates

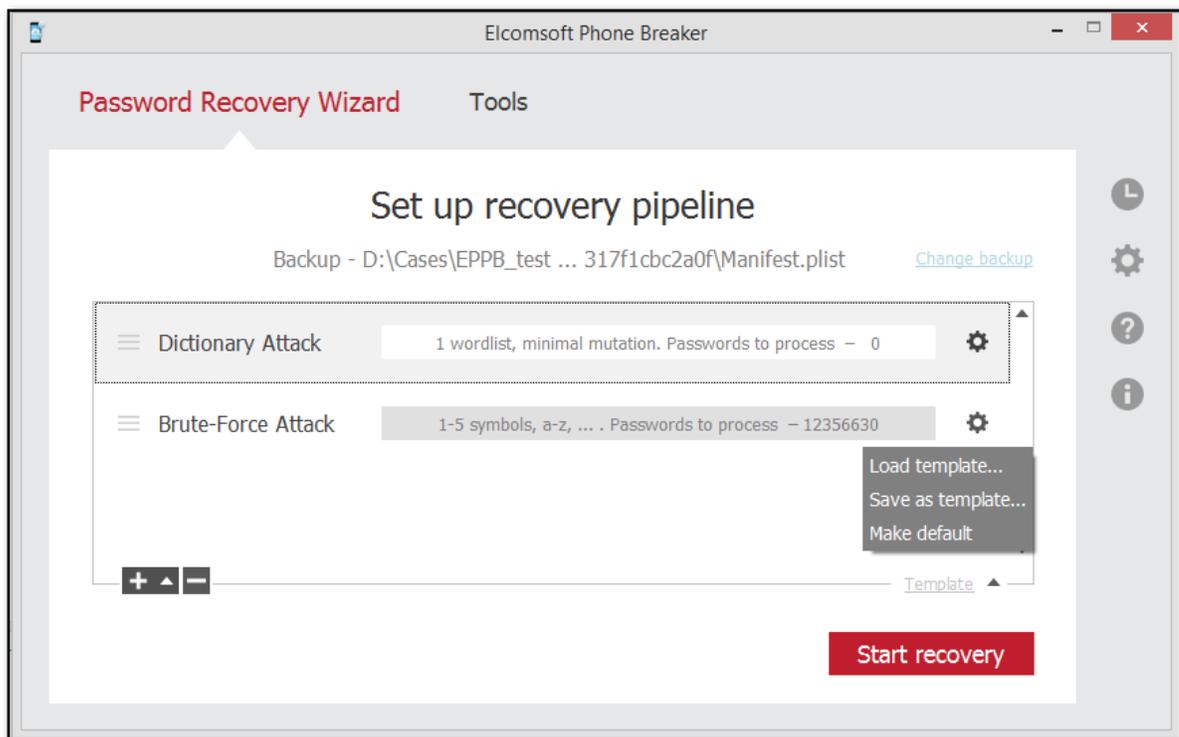
### 3.5.6.1 Saving templates

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.

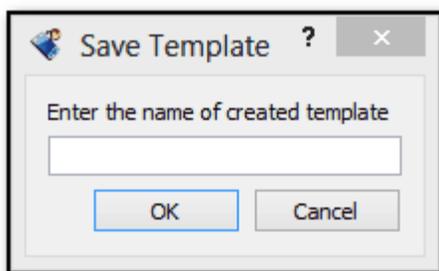
**NOTE: Recovering passwords is available only when using EPB for Windows OS.**

**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.



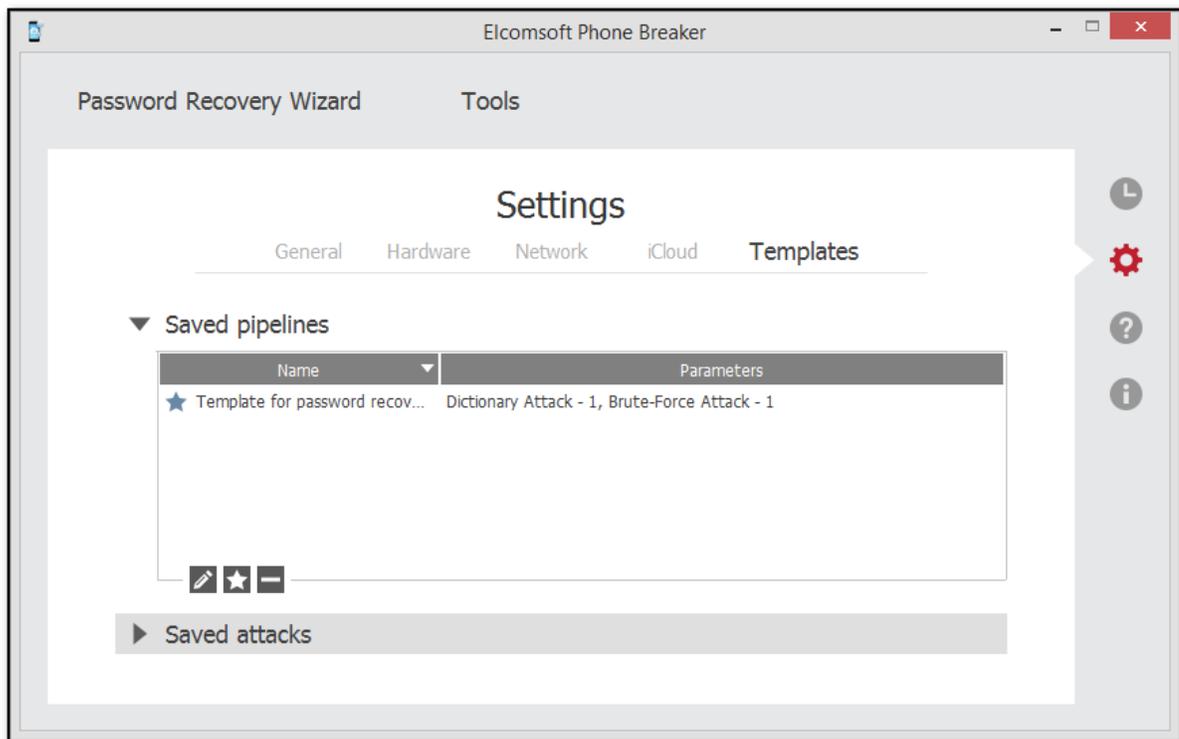
4. The template is saved. Now you can load the template from the template database when you recover a different password.

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

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

### 3.5.6.2 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.

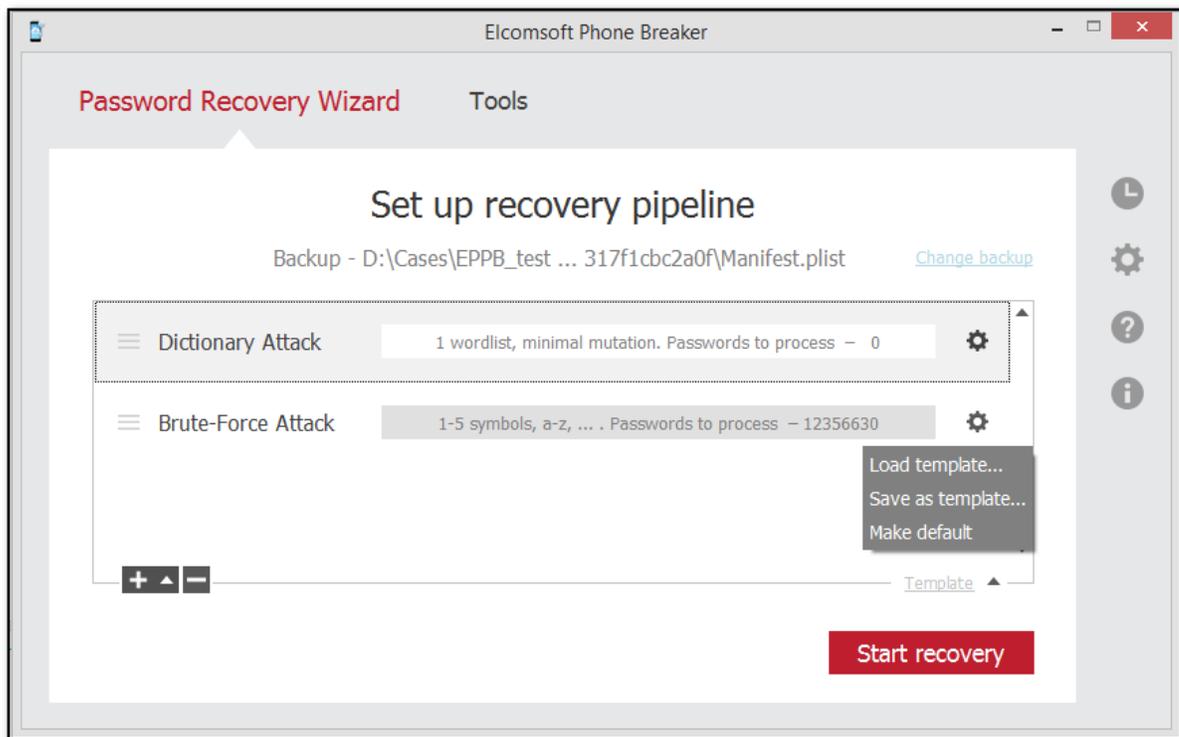
To delete a template, select a template, and click the **Delete**  button.

### 3.5.6.3 Loading templates

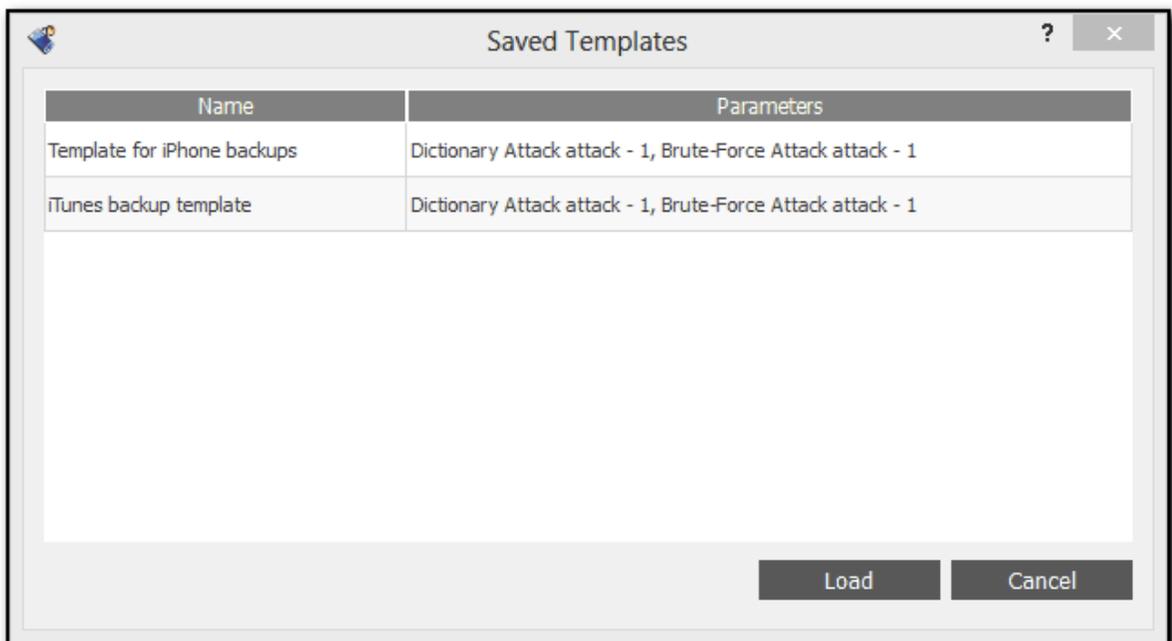
Template is a combination of attack settings saved in EPB. Templates are created to simplify re-using of certain settings when recovering passwords to several backups.

**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.

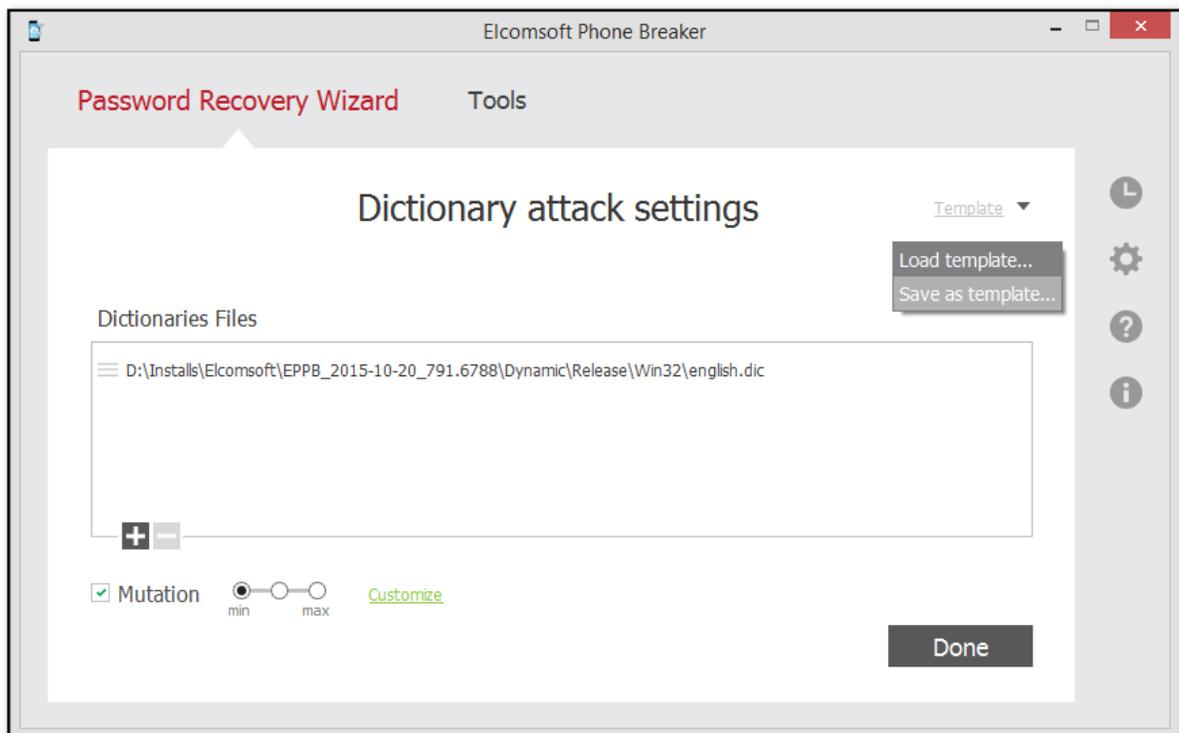
#### 3.5.6.4 Using templates for attacks

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

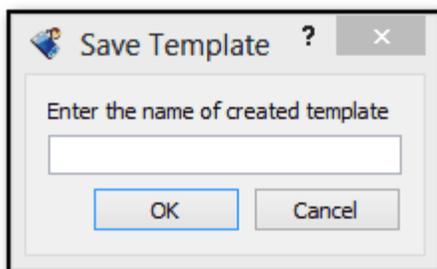
**NOTE: Recovering passwords is available only when using EPB for Windows OS.**

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**.

## 4 Elcomsoft Phone Viewer

### 4.1 EPV Program information

#### 4.1.1 EPV Settings

You can switch between English- and Russian-language interface of Elcomsoft Phone Viewer. The changes are applied after restarting the application.

When decrypting a backup, a number of files containing temporary data are created. The total size of temporary files equals to the size of the backup.

You can define the location on your computer to which the temporary data will be extracted during backup decryption.

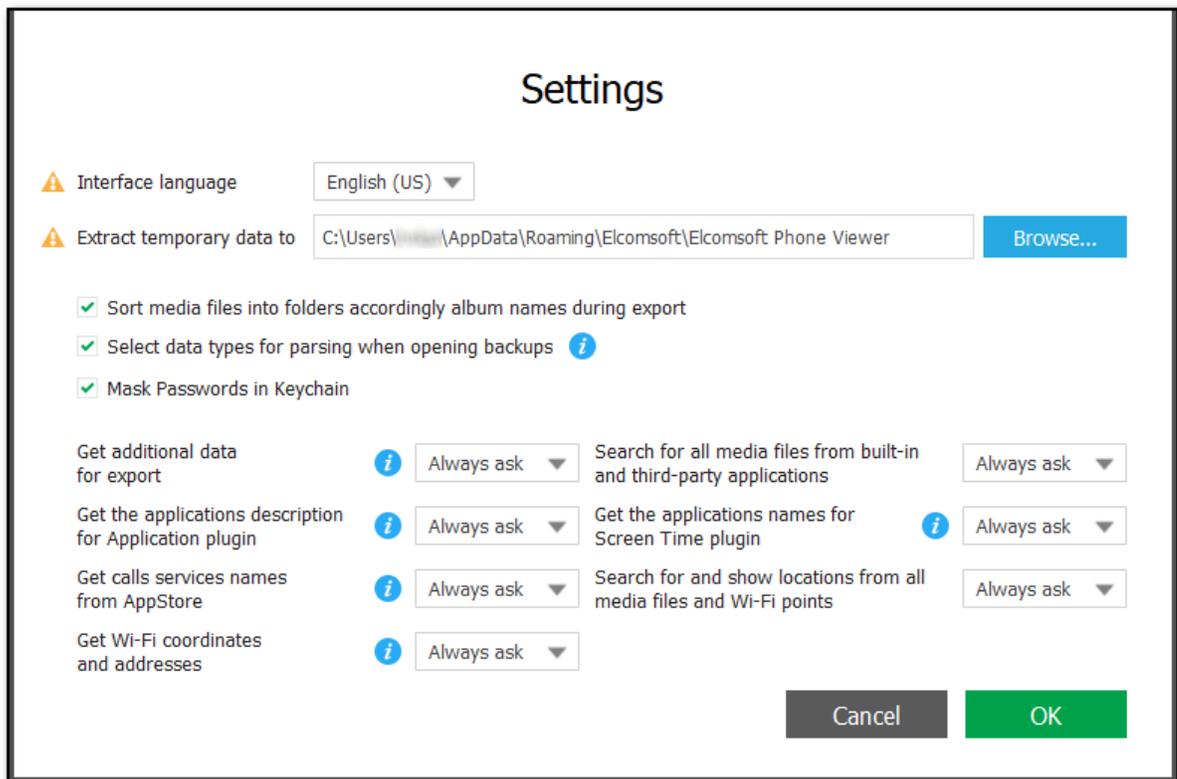
**To define the folder for temporary data extraction**, do the following:

1. In the **View** menu, click **Settings**.
2. In the **Extract temporary data to** field, enter the path to the folder on your computer or click **Browse**, select the necessary folder, and click **Select Folder**.
3. Click **OK**.

The default path to the folder where temporary data is extracted to is:

- **Windows:** *C:\Users\Username\AppData\Roaming\Elcomsoft\Elcomsoft Phone Viewer*
- **macOS:** *~/Users/<username>/Library/Application Support/Elcomsoft/Elcomsoft Phone Viewer*

*Please note that after defining a new path to the folder instead of the default path, the changes will come into effect as soon as the program is restarted.*



Select the **Sort media files into folders accordingly album names during export** check box in order to have convenient access to exported media galleries with large numbers of files.

If this option is selected, images and videos will be categorized into albums similar to those in the device.

If you want to **select data types for parsing when opening backups**, select the check box with the corresponding name.

*NOTE: This option is available for iTunes backups, iCloud backups retrieved with Elcomsoft Phone Breaker, iCloud synced data, iOS device images, BlackBerry backups, and Microsoft account data.*

If you want to **mask passwords in Keychain**, select the check box with the corresponding name.

If you want to **get additional data for export** using Internet, select **Yes** for this option. You can select **Always ask** to make decision every time.

If you select **No**, Internet will not be used, but less data will be obtained.

If you want to **get the applications description for Application plugin** when working with backups containing applications, select **Yes** for this option. You can select **Always ask** in order to decide for every backup.

If you want to **get calls services names from AppStore** when working with backups containing calls, select **Yes** for this option. You can select **Always ask** in order to decide for every backup.

If you want to **get Wi-Fi coordinates and addresses** when working with backups containing Wi-Fi connections data, select **Yes** for this option. You can select **Always ask** in order to decide for every backup.

If you want to **search for all media files from built-in and third-party applications** when working with backups containing media files, select **Yes** for this option. You can select **Always ask** in order to decide for every backup.

If you select **No**, only Camera roll and attached media files will be searched for. This would make working with encrypted backups quicker as only these media sources will be decrypted.

If you want to **get the applications names for Screen Time plugin** when working with Screen Time data, select **Yes** for this option. You can select **Always ask** to make decision every time.

If you want to **search for and show locations from all media files and Wi-Fi points** when working with backups containing locations, select **Yes** for this option. You can select **Always ask** in order to decide for every backup.

If you select **No**, only locations from Camera roll media files will be searched for.

#### 4.1.2 Supported Apple device backups

All devices (iPhone, iPad and iPod Touch) running iOS versions from 6 to 13 (except for encrypted notes) are supported. There are different types of backups, though:

Backup type	Supported by EPV	Comments
iTunes backup (not encrypted)	Yes	
iTunes backup (not encrypted) with restored file names	Yes	
iTunes backup (encrypted)	Yes	
iCloud backup	Yes	
Partial iCloud backup	Yes	
iCloud Photos	Yes	At least some of supported categories should be selected when downloading You can view photos downloaded from iCloud using the <b>Elcomsoft Phone Breaker</b> program.
iCloud synced data	Yes	You can view iCloud synced data downloaded from iCloud using the <b>Elcomsoft Phone Breaker</b> program.
iOS device image	Yes	You can view data of iOS device images acquired via <b>Elcomsoft iOS Forensic Toolkit</b> .

More information on iOS backups:

[About iTunes backups](#)

[About iCloud backups](#)

#### 4.1.3 Supported BlackBerry device backups

EPV works with backups of devices running BlackBerry 10 - 10.3 OS, created using [BlackBerry Link](#) software (for Windows or macOS). More information:

[Backing up and restoring device data](#)

BlackBerry backups contain all information from the device, including:

- Contacts
- Files (pictures, music, documents)
- Calendar items

- Tasks and Memos
- BBM contacts
- Browser bookmarks and folders
- Alarm/clock settings
- Text/SMS/MMS messages
- Phone Call Logs
- WLAN Profiles (for non-enterprise networks)
- Password Keeper entries

All BB backups are encrypted using the encryption keys that are stored inside the device and are unique for every [BlackBerry ID](#). In order to be able to work with such backups in EPV, they must be decrypted using [Elcomsoft Phone Breaker](#) first; decryption requires the password from BlackBerry ID.

Please note that EPV does NOT support backups of older BlackBerry models (running BlackBerry OS 6 or 7) created with [BlackBerry Desktop Software](#).

#### 4.1.4 Microsoft account data

EPV allows you to explore the Microsoft account user data downloaded by [Elcomsoft Phone Breaker](#) from the cloud. This data includes user contacts, notes, web browsing and search history, etc.

Newest [Elcomsoft Phone Breaker](#) version downloads the Microsoft user data synced with the device and/or collected from the web browser.

Older [Elcomsoft Phone Breaker](#) versions download the Microsoft user data as Windows Phone backups. Windows Phone 8 (and 8.1) allows creating a kind of backup of the device in the cloud (no local backups are available), saving installed applications and their settings, text messages (SMS and MMS), photos/videos etc. (More information is available here: <http://www.windowsphone.com/en-us/how-to/wp8/settings-and-personalization/back-up-my-stuff>)

Unfortunately, there is no way to download the complete backup of the device. At this time, the following data can be extracted from Microsoft accounts:

- Contacts (aggregated)
- Notes (in Microsoft OneNote format)
- Messages (SMS)
- Calls
- Web browsing history
- Web search history
- Location history
- Skype

Extraction of Microsoft account data can be done using [Elcomsoft Phone Breaker](#) -- with valid Microsoft Live! credentials (login/email and password, it downloads the information listed above (as well as info on all Windows Phone devices connected to the account) and creates backup in its own format.

Note: Windows Live accounts from *microsoft.com* domain are NOT supported.

## 4.2 Working with Apple device data

### 4.2.1 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.
- 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.
- 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:

[Use iTunes to restore your iOS device to factory settings](#)

[Back up and restore your iPhone, iPad, or iPod touch using iCloud or iTunes](#)

- **macOS:** ~/Library/Application Support/MobileSync/Backup/
- **Windows 7, Windows 8, Windows 8.1, and Windows 10:** \Users\\AppData\Roaming\Apple Computer\MobileSync\Backup\

If you run EPV 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.

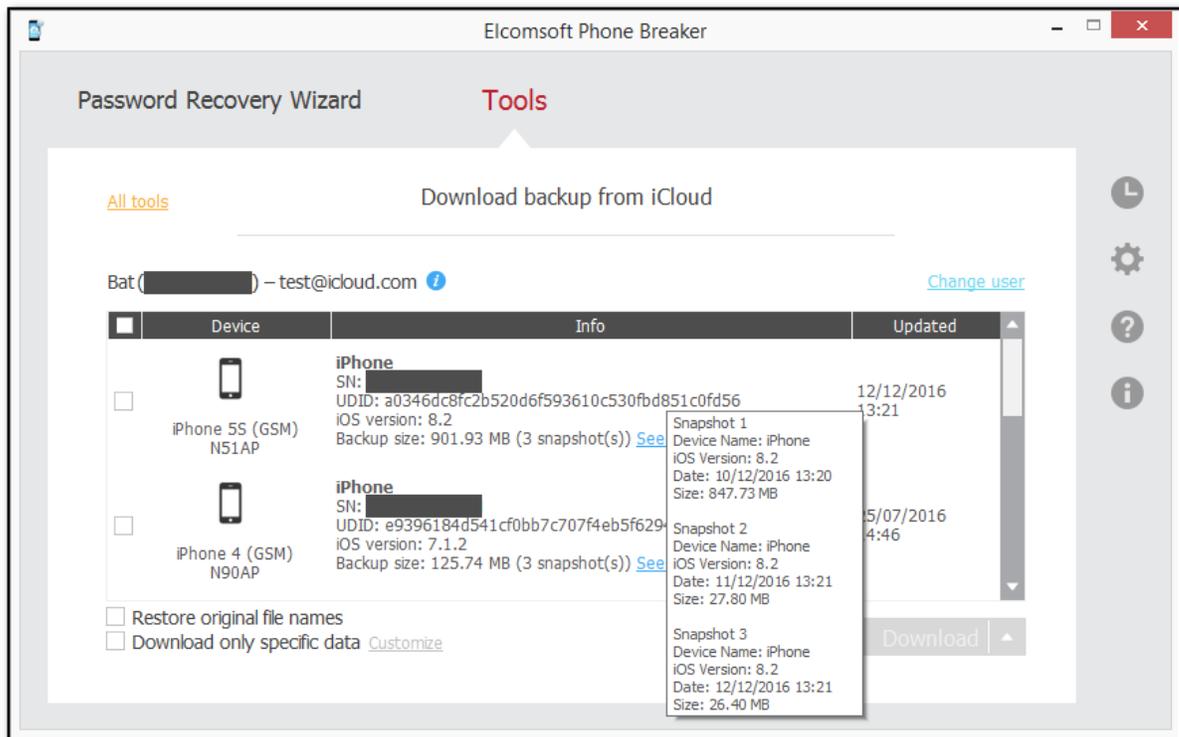
## 4.2.2 About iCloud backups

It is possible to back up iOS devices not only locally, but also to [iCloud](#). For more information, please read:

[Creating an iCloud account: Frequently Asked Questions](#)  
[Cloud: iCloud storage and backup overview](#)  
[Manage your iCloud storage](#)

Once you have enabled iCloud backup on your device (**Settings | iCloud | Backup | iCloud Backup**), 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.

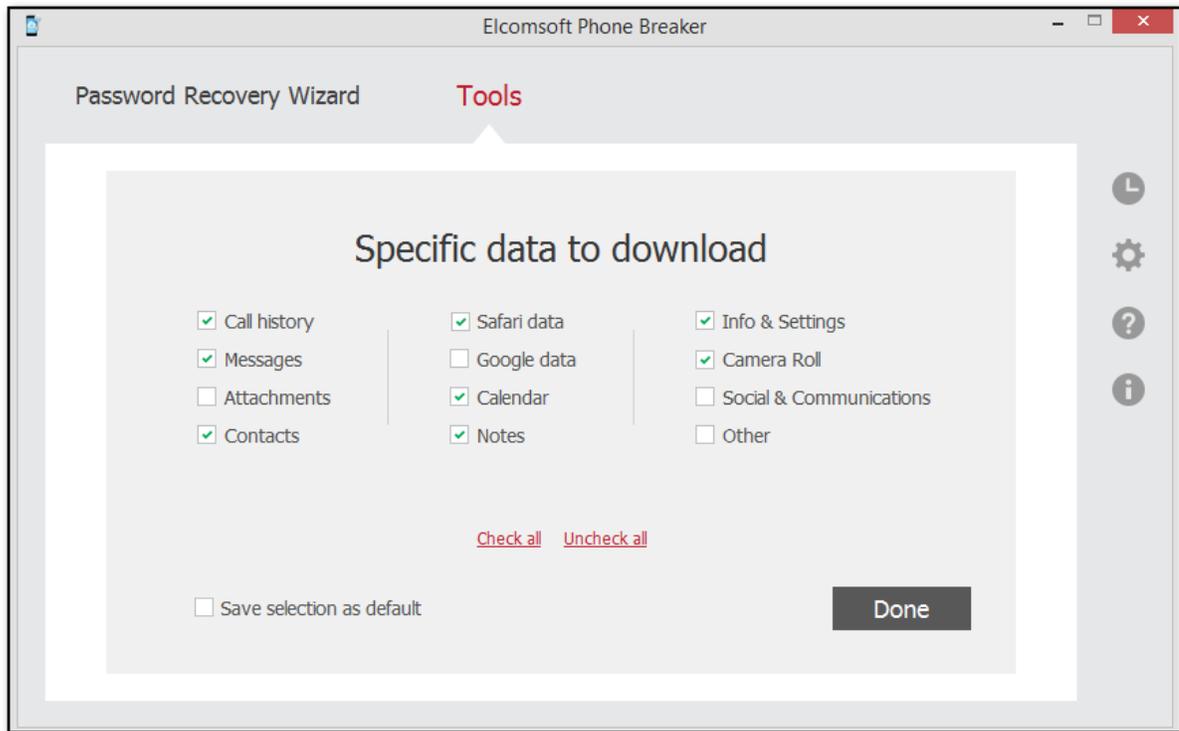
If you have the Apple ID and password, use the [Elcomsoft Password Breaker](#) to download backup from the iCloud. You can enable *Restore original file names* option if you wish (EPV supports both formats -- original iTunes one and with file names restored), and you can also enable *Download only specific data*.



Just make sure that you enabled *Info & Settings* category and at least one of the following:

- Call history
- Messages
- Contacts

- Calendar
- Notes
- Safari data
- Camera Roll



### 4.2.3 About iOS device images

EPV allows you to view iOS device images acquired via [Elcomsoft iOS Forensic Toolkit](#).

**Elcomsoft iOS Forensic Toolkit (EIFT)** is a set of tools aimed at acquiring iOS devices. EIFT allows you to do the following:

- Obtain information about the device, even if it is locked.
- Obtain the snapshot of user partitions, capturing the entire file system.
- Perform logical acquisition by producing the iTunes-style backup (can use lockdown file to unlock).
- 32-bit devices: Obtain the physical (dd-style) dump of the root (system) and user (data) partitions.
- 32-bit devices: Extract all keys required to decrypt user (data) filesystem as well as keychain items.
- 32-bit devices: Run the passcode recovery attack.

*NOTE: Jailbreak and OpenSSH installation are required to acquire iPhone 4s and newer devices.*

EIFT iOS device images have the .tar extension. Currently, EPV supports only physical iOS device images acquired via EIFT.

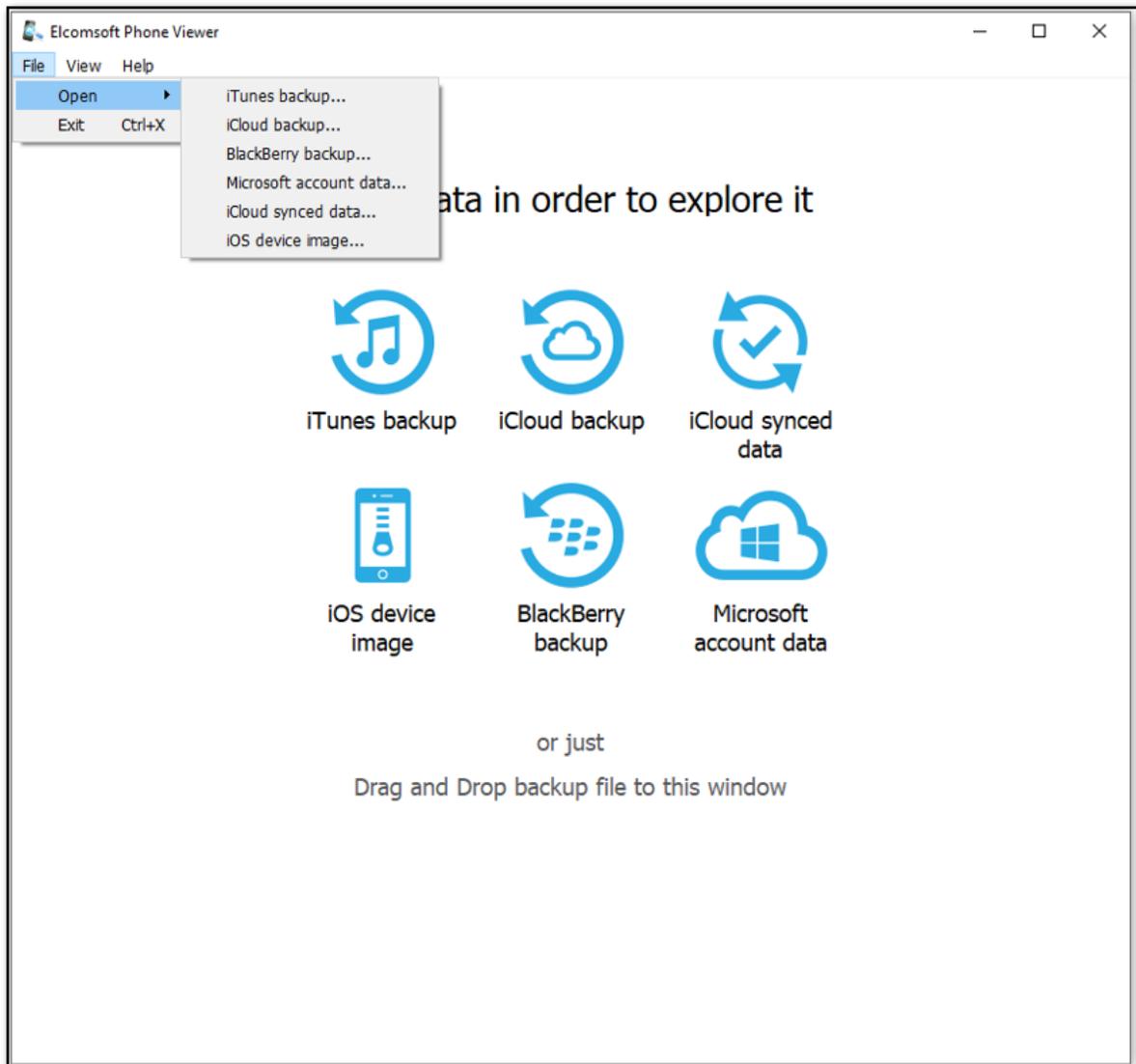
### 4.2.4 Working with iOS backups

To add the iOS backup to EPV, do the following:

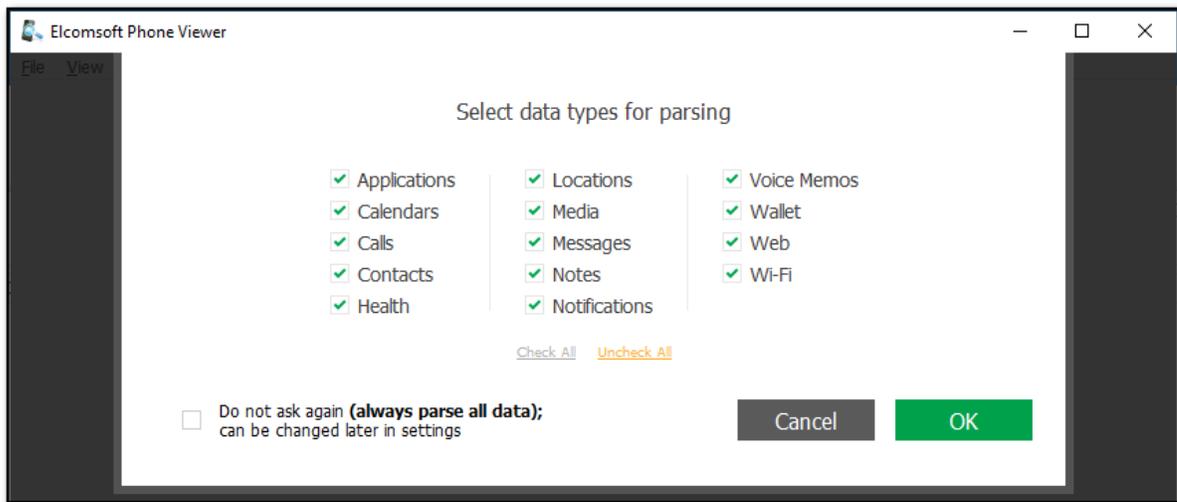
1. On the main screen, click **iTunes backup** or **iCloud backup**, select the necessary backup in the **File > Open** menu, or drag and drop the backup file to the program window.

2. Browse for the Manifest.plist file in the folder where your iOS device backup is located (see [Supported Apple device backups](#), [About iTunes backups](#) and [About iCloud backups](#) for more info).

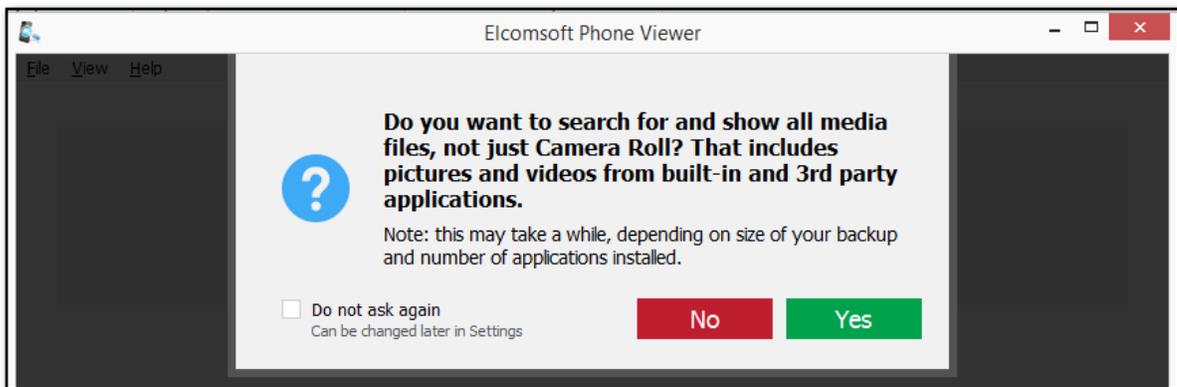
*NOTE: On macOS 10.14 and higher, you need to grant the Full Disk Access permission to EPB to have access to the default iTunes backups folder. For details, see [Troubleshooting](#).*



3. Select data types for parsing when opening the backup file (you can change this later in Settings).



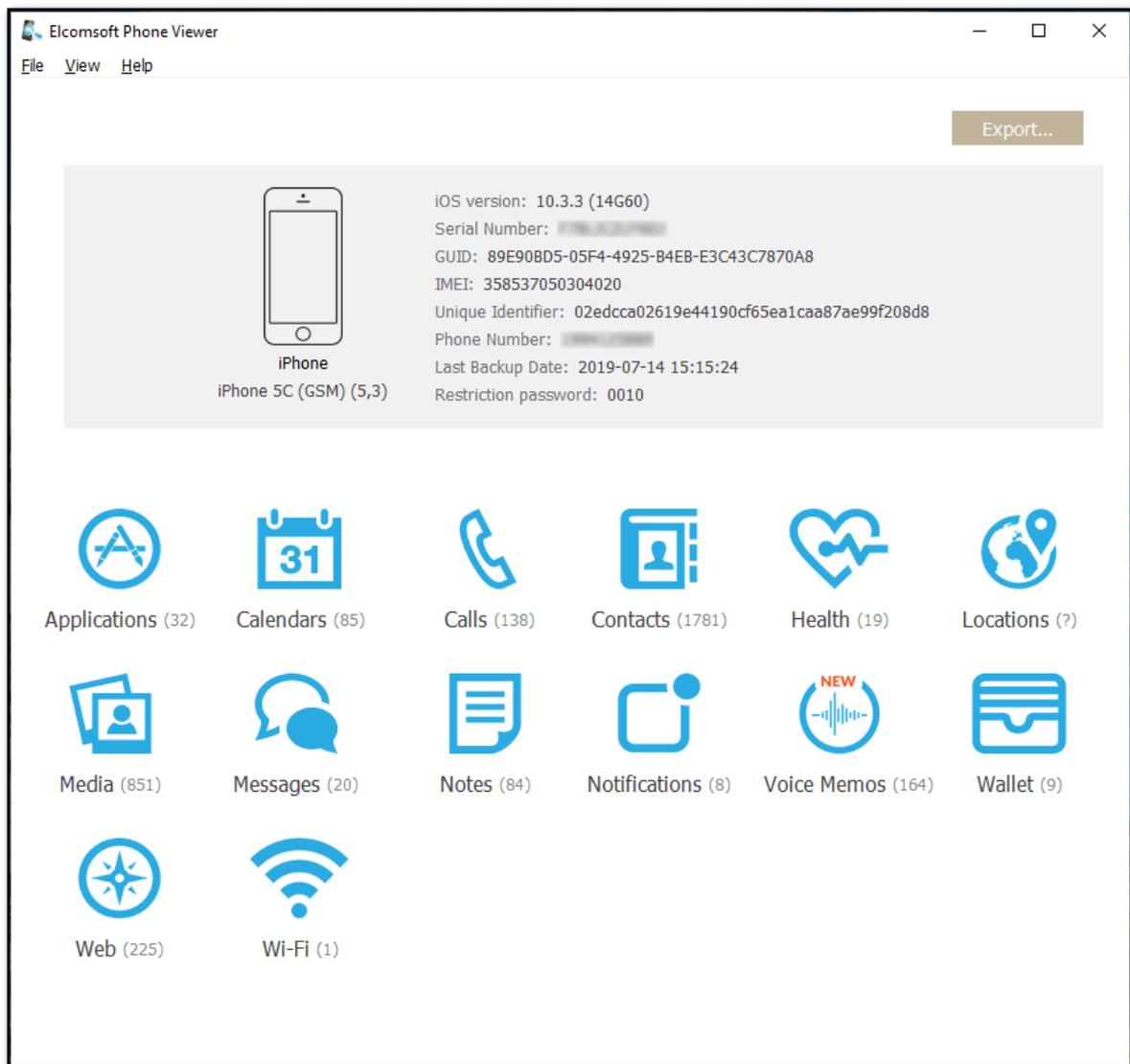
4. Select if you want EPV to search for and display Camera Roll media only or all media files (you can change this later in Settings).



Once the backup is loaded, its name and device type is shown under a generic image, as well as the following information (some of it may not be available for iCloud backups, so only for local iTunes backups this information is complete):

- iOS version
- Serial Number
- GUID
- IMEI
- Target Identifier
- Unique Identifier (usually the same as above)
- Phone number
- Last backup date
- Restriction or Screen Time password

*NOTE: Restriction password is available for encrypted, not encrypted, and decrypted iOS 11 and lower backups. Screen Time password is available for encrypted and decrypted iOS 12 backups.*



The lower part of the window shows all plugins available (some of them might be disabled if there is no appropriate information in the backup):

- [Applications](#)
- [Calendars](#)
- [Calls](#)
- [Contacts](#)
- [Health](#)
- [Locations](#)
- [Media](#)
- [Messages](#)
- [Notes](#)
- [Notifications](#)
- [Voice Memos](#)
- [Wallet](#)
- [Web](#)

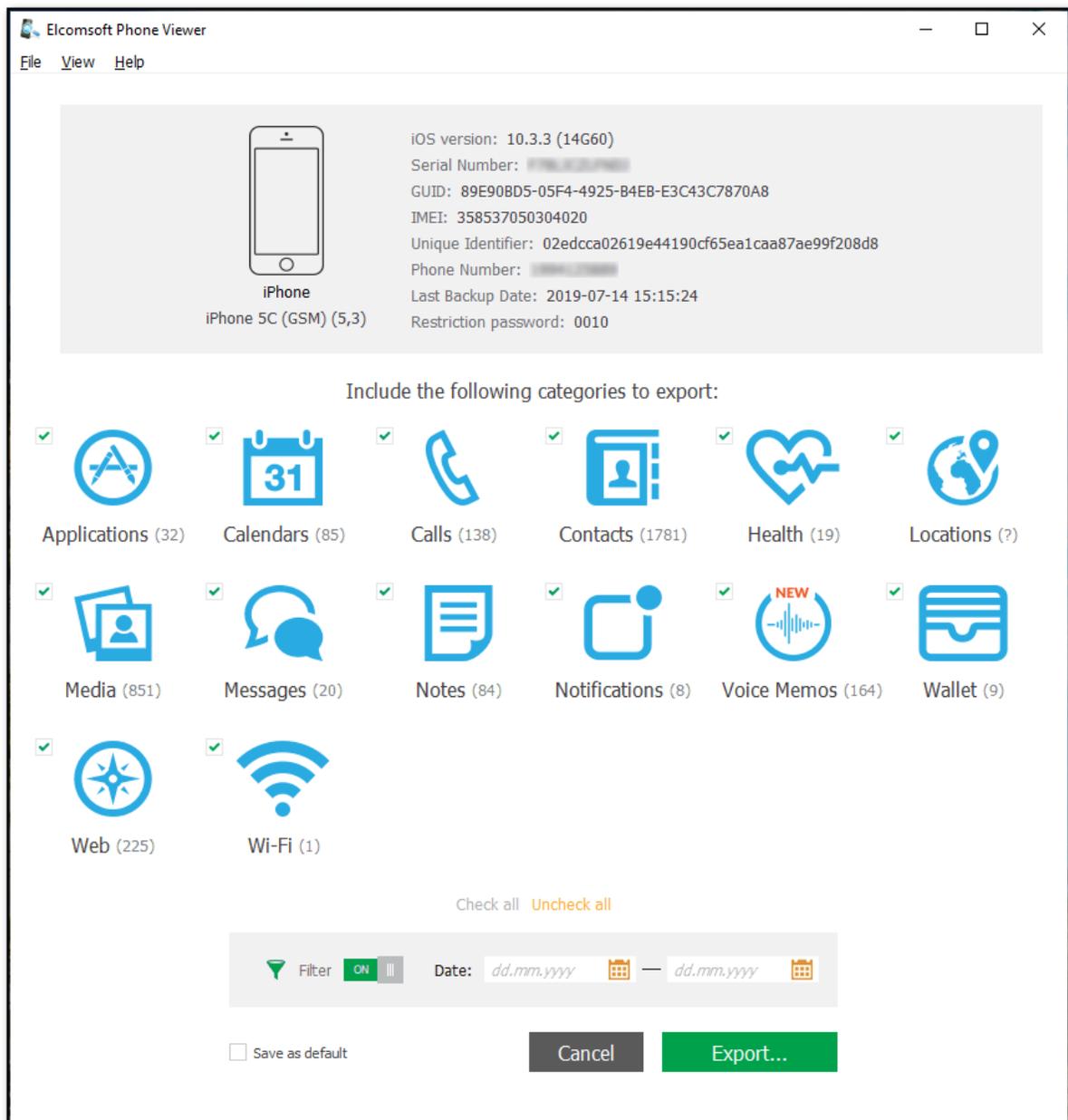
- [Wi-Fi](#)

Click the plugin icon to view the contents.

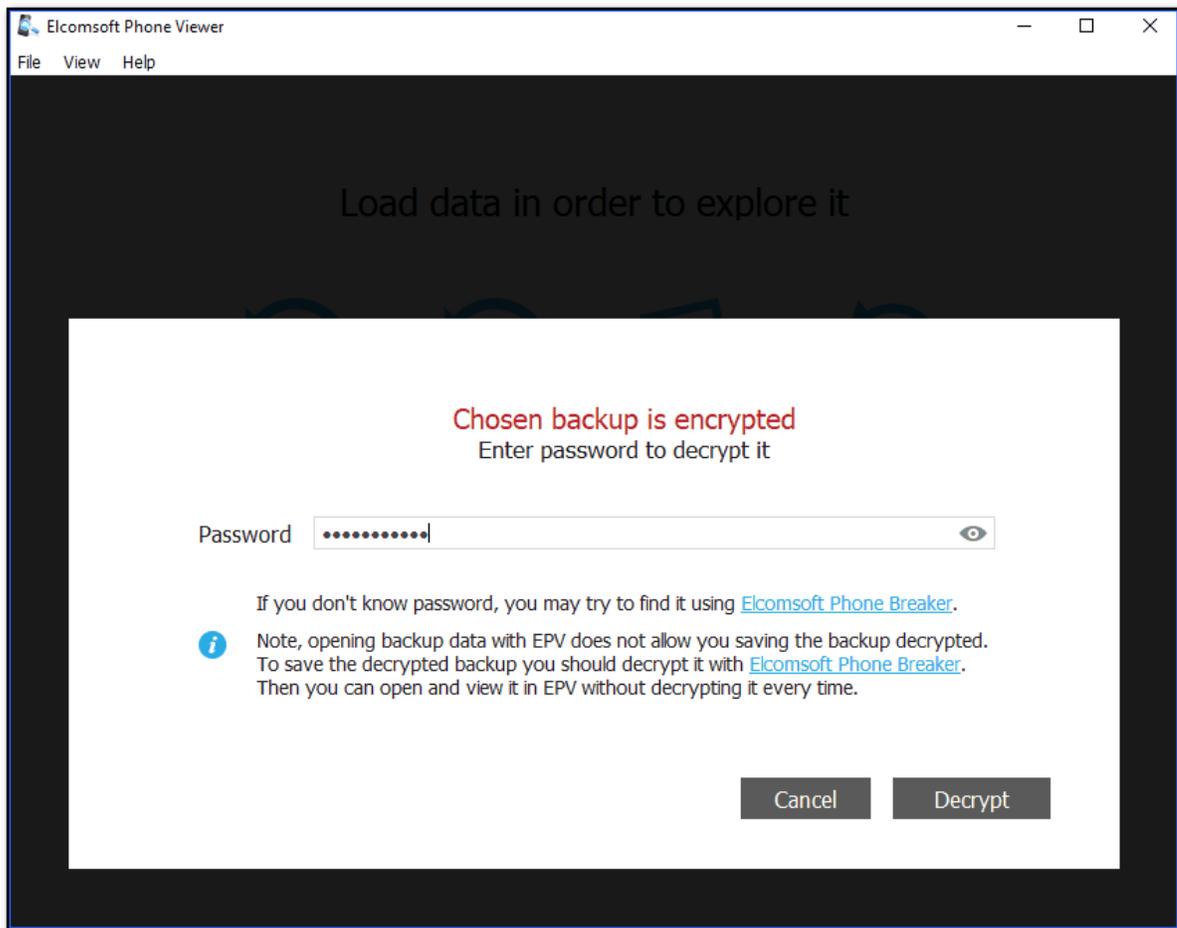
*NOTE: If the databases of some apps changed during an iOS update, no data might be displayed when you are trying to view the contents of some plugins.*

#### **Exporting Data from Plugins**

1. Click **Export**.
2. Select the plugins data from which you want to export or click **Check all**.
3. Optionally, enable filtering to export data for a certain time period. To do so, switch the **On/Off** toggle, and then select the dates in the calendar fields.
4. Click **Export**.
5. In the opened window, select the location in which the file with exported data will be saved and enter the file name.
6. Click **Save**.
7. The **<file name>.xlsx** file is saved in the selected location.



EPV allows you to decrypt password-protected iTunes backup assuming that the password is known.



Also, you can decrypt an encrypted iTunes backup with [Elcomsoft Password Breaker](#) (with or without an option *Restore original file names* option) in order to be able to view its contents in EPV.

#### 4.2.5 Working with iOS device images

EPV allows you to view iOS device images acquired via [Elcomsoft iOS Forensic Toolkit](#) (EIFT). Currently, the following categories are available for iOS device images:

- Apple Pay
- Applications
- Calendars
- Calls
- Contacts
- Health
- Locations
- Media
- Messages
- Notes
- Notifications
- Signal
- Telegram

- Voice Memos
- Wallet
- Web
- Wi-Fi

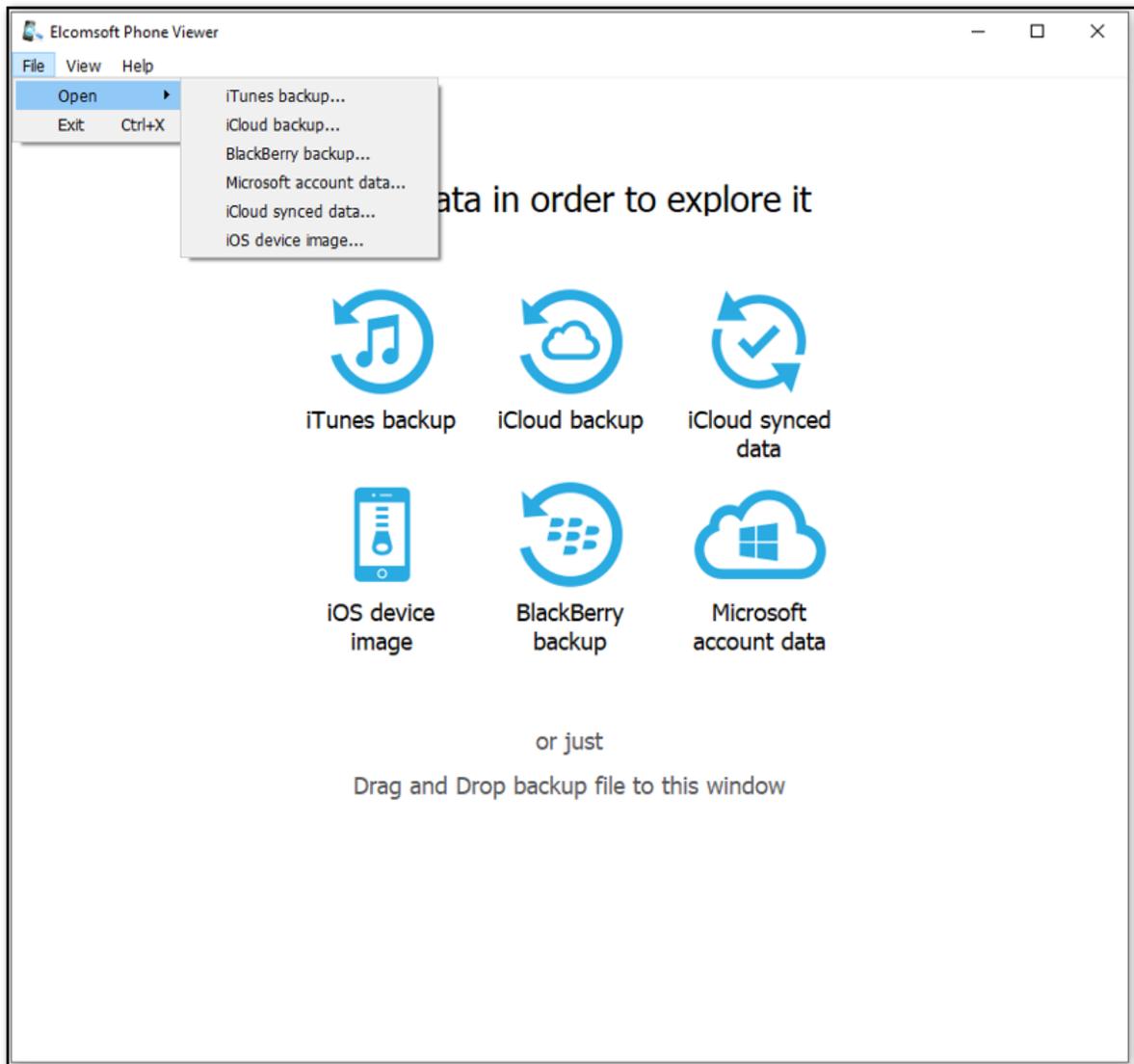
To reduce the time it takes to add the iOS device image, disable the Windows Defender protection first:

1. Open the Windows **Start** menu.
2. Click **Windows Defender Security Center** in the app list.
3. Click **Virus & threat protection**.
4. Click **Virus & threat protection settings**.
5. Turn off **Real-time protection**.

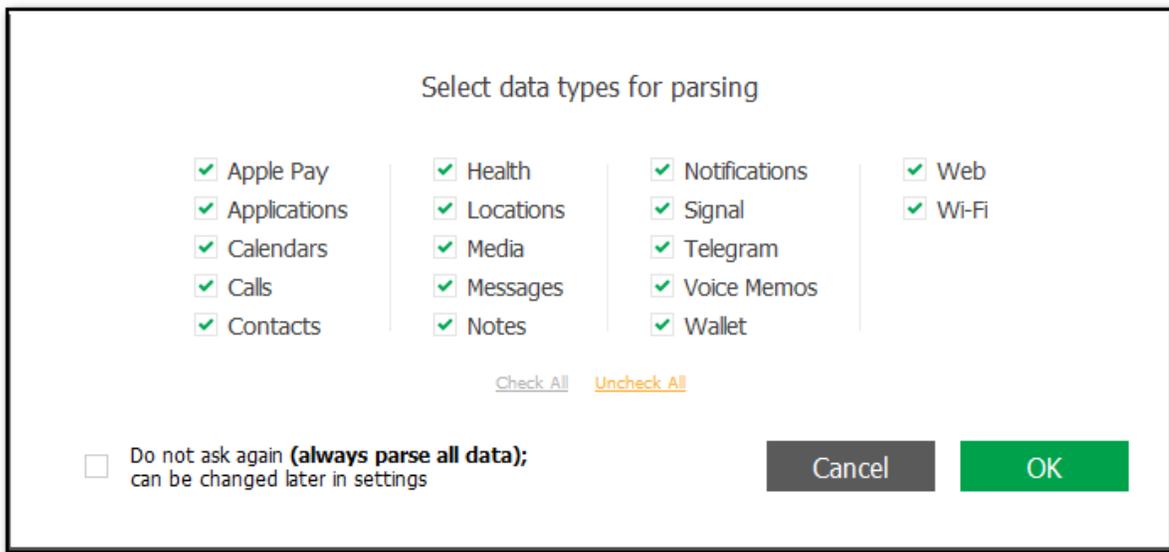
Once the steps are completed, Windows Defender will temporarily disable the real-time protection. The next time you restart your computer, the Windows Defender protection will be re-enabled automatically. Once the iOS device image is added, it is recommended to enable the Windows Defender protection.

To add the iOS device image to EPV, do the following:

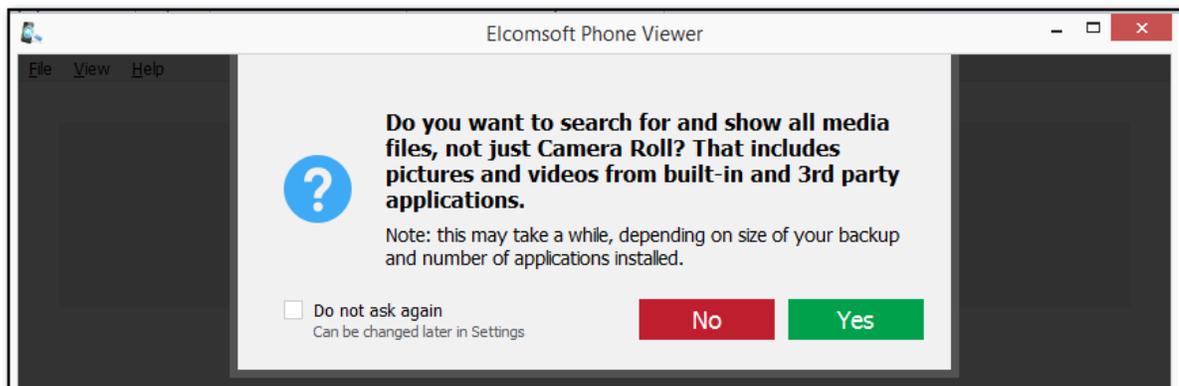
1. On the main screen, click **iOS device image**, select **iOS device image** in the **File > Open** menu, or drag and drop the image file (.tar archive) to the program window.
2. Browse for the .tar file with the iOS device image acquired via EIFT (see [Supported Apple device backups](#) and [About iOS device images](#) for more info).



3. Select data types for parsing when opening the image file (you can change this later in Settings).



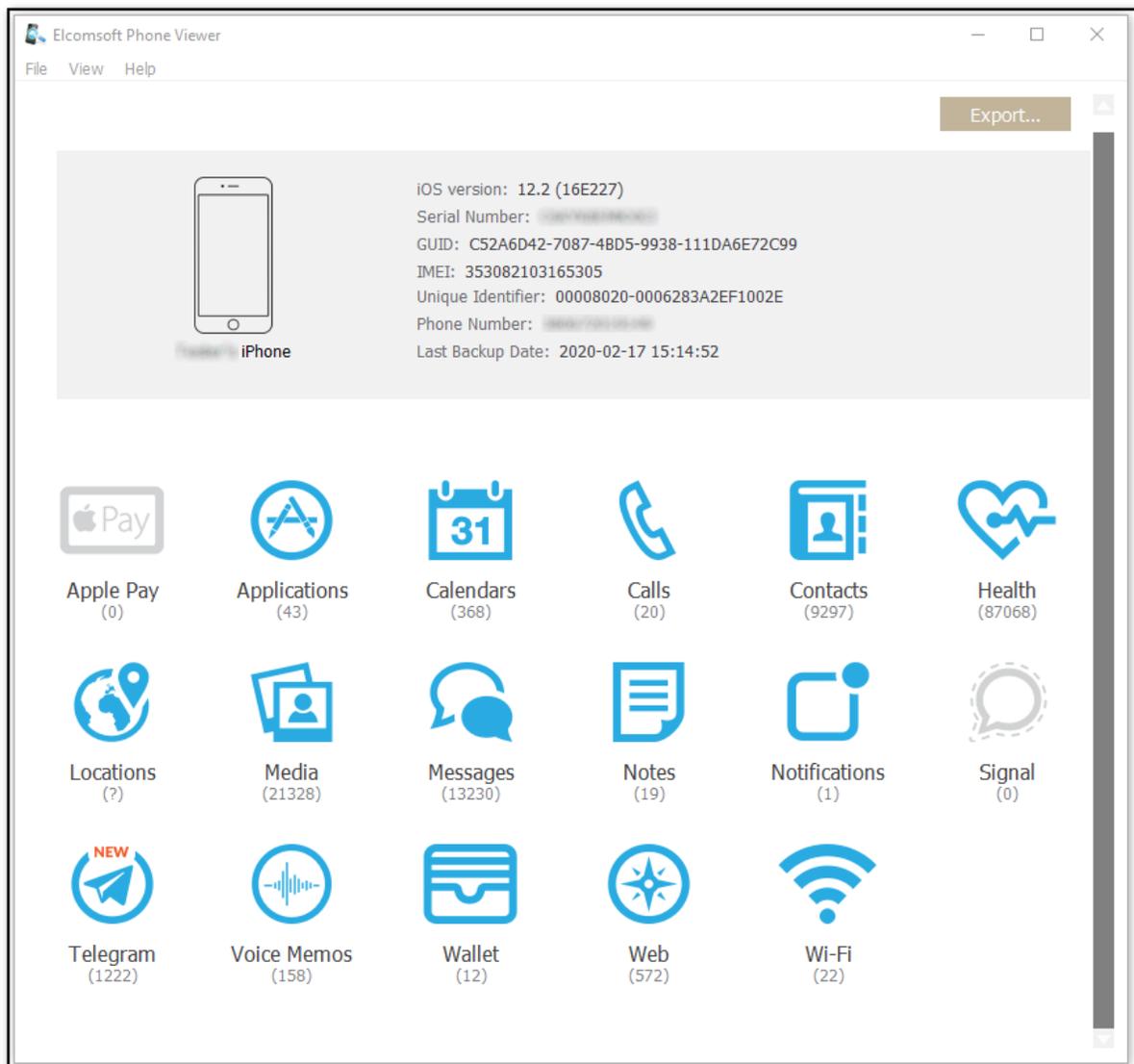
4. Select if you want EPV to search for and display Camera Roll media only or all media files (you can change this later in Settings).



Once the iOS device image is loaded, its name and device type is shown under a generic image, as well as the following information:

- iOS version
- Serial Number
- GUID
- IMEI
- Unique Identifier
- Phone number
- Restriction password

*NOTE: Restriction password is available for encrypted, not encrypted, and decrypted iOS 11 and lower backups.*



The lower part of the window shows all plugins available (some of them might be disabled if there is no appropriate information in the device image):

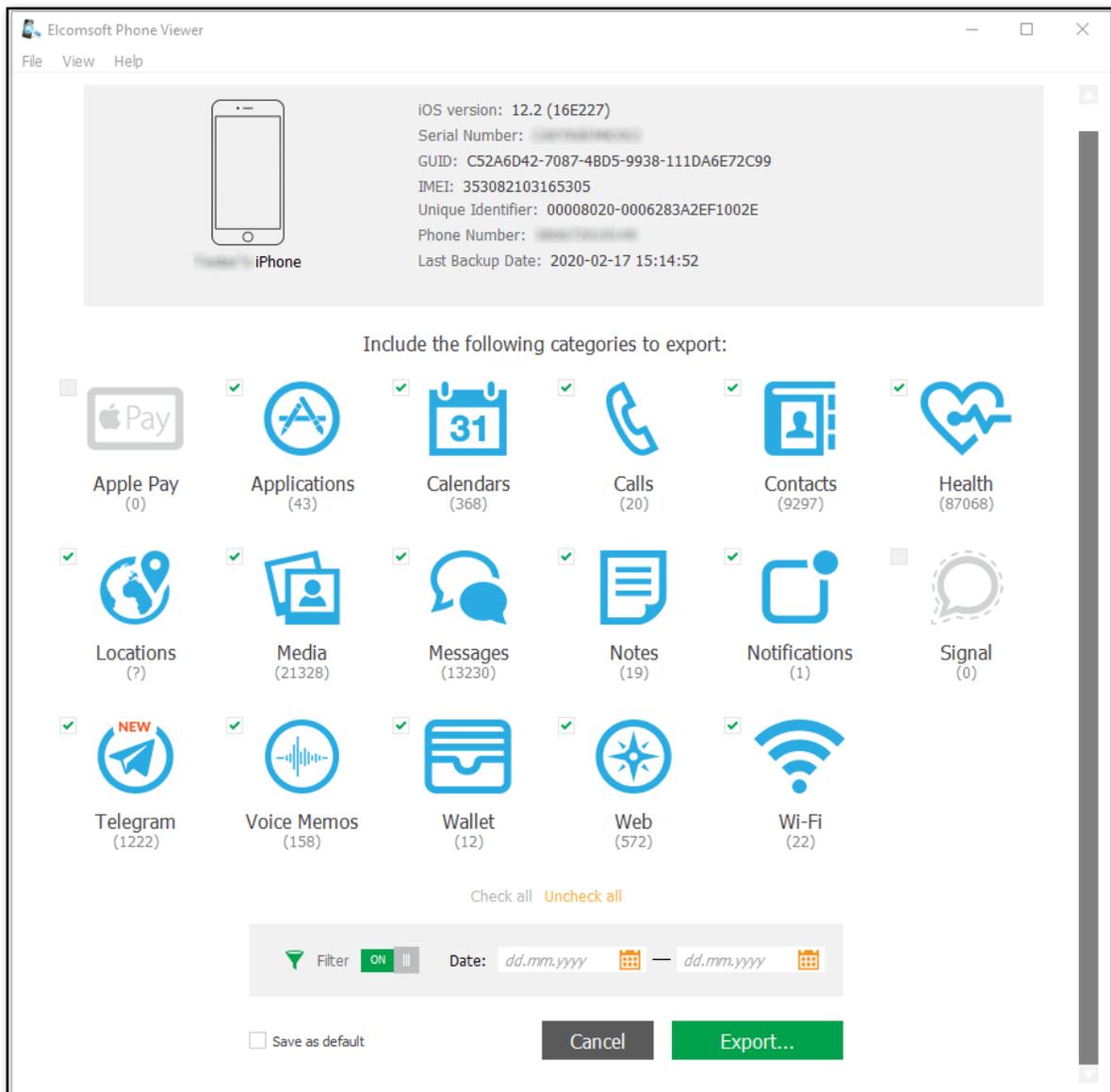
- [Apple Pay](#)
- [Applications](#)
- [Calendars](#)
- [Calls](#)
- [Contacts](#)
- [Health](#)
- [Locations](#)
- [Media](#)
- [Messages](#)
- [Notes](#)
- [Notifications](#)
- [Signal](#)
- [Telegram](#)

- [Voice Memos](#)
- [Wallet](#)
- [Web](#)
- [Wi-Fi](#)

Click the plugin icon to view the contents.

### Exporting Data from Plugins

1. Click **Export**.
2. Select the plugins data from which you want to export or click **Check all**.
3. Optionally, enable filtering to export data for a certain time period. To do so, switch the **On/Off** toggle, and then select the dates in the calendar fields.
4. Click **Export**.
5. In the opened window, select the location in which the file with exported data will be saved and enter the file name.
6. Click **Save**.
7. The **<file name>.xlsx** file is saved in the selected location.



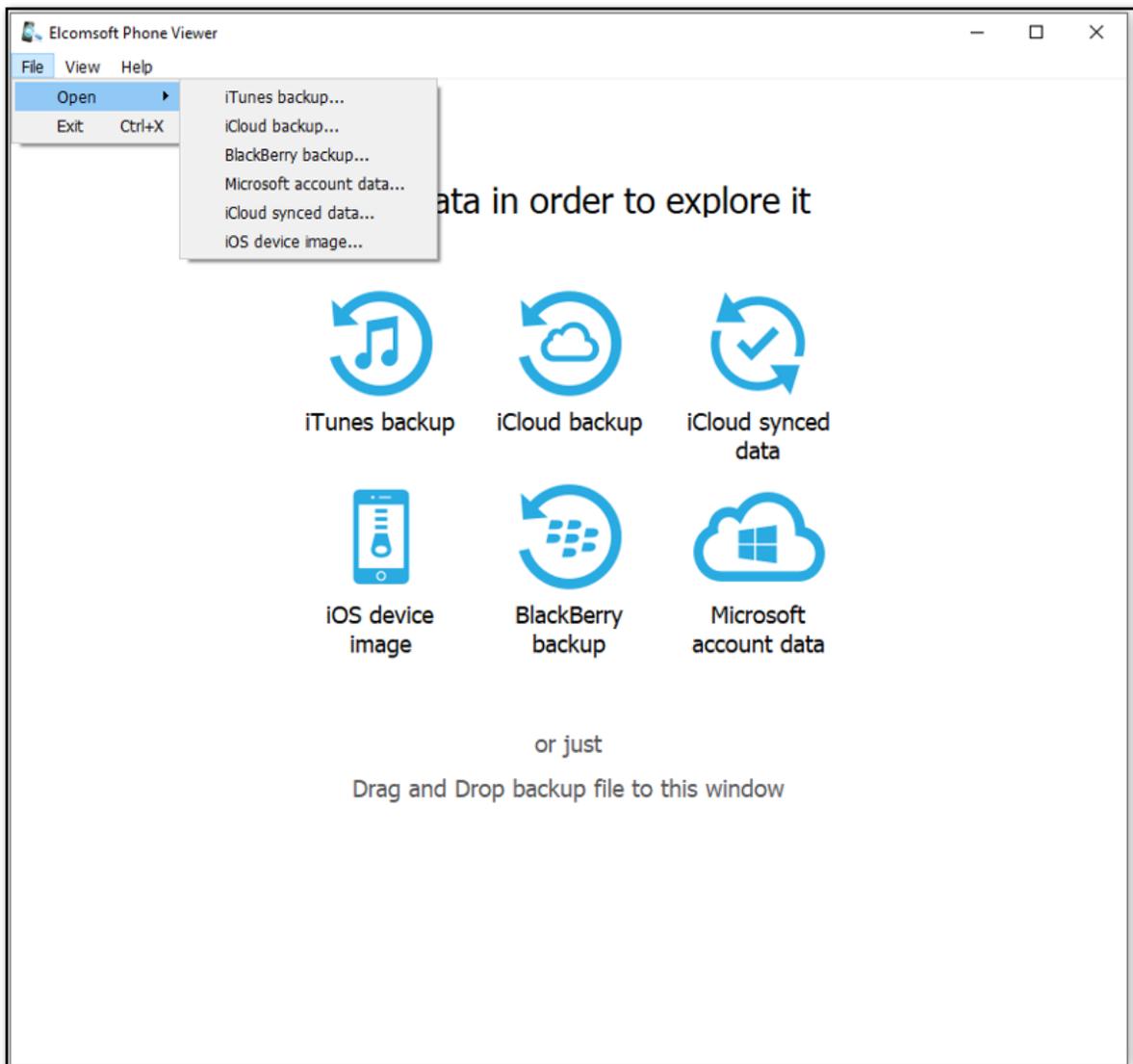
#### 4.2.6 Working with iCloud synced data

EPV allows you to view device data synced with iCloud and downloaded using [Elcomsoft Password Breaker](#). Currently, the following categories of synced data are available:

- Account info
- Apple Maps
- Calendars
- Calls
- Contacts
- Health
- iBooks
- Keychain
- Messages
- Notes

- Photos
- Screen Time
- Voice Memos
- Wallet
- Web
- Wi-Fi

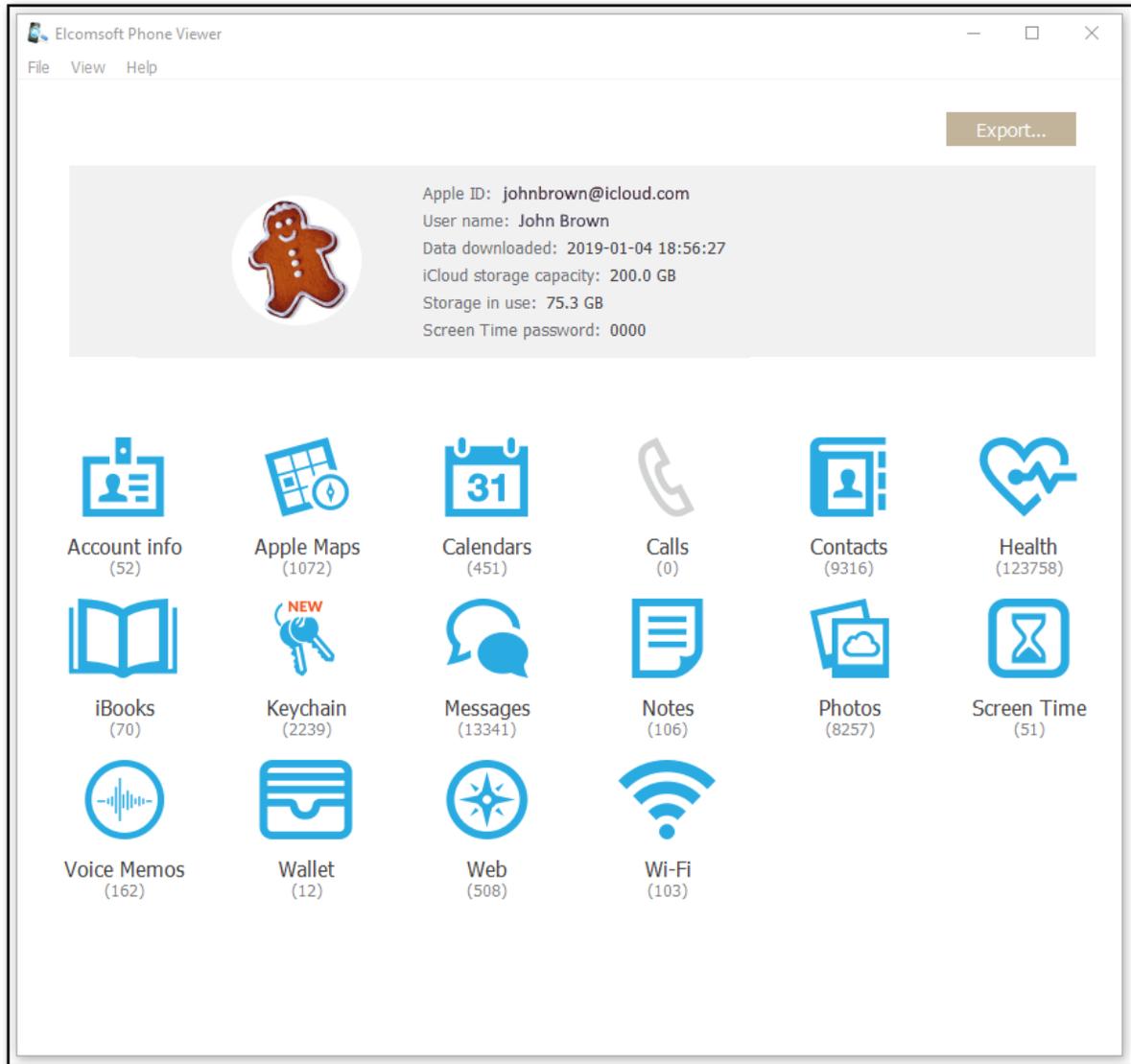
To open iCloud synced data in EPV, on the main program screen, click **iCloud synced data**, select **iCloud synced data** in the **File > Open** menu, or drag and drop the **icloud\_synced.xml** file to the main program screen.



Once the synced data is loaded, you can see the following backup information:

- Apple ID
- User name
- Data downloaded (the date and time the backup was downloaded)

- iCloud storage capacity
- Storage in use
- Screen Time password



The lower part of the window shows all available plugins:

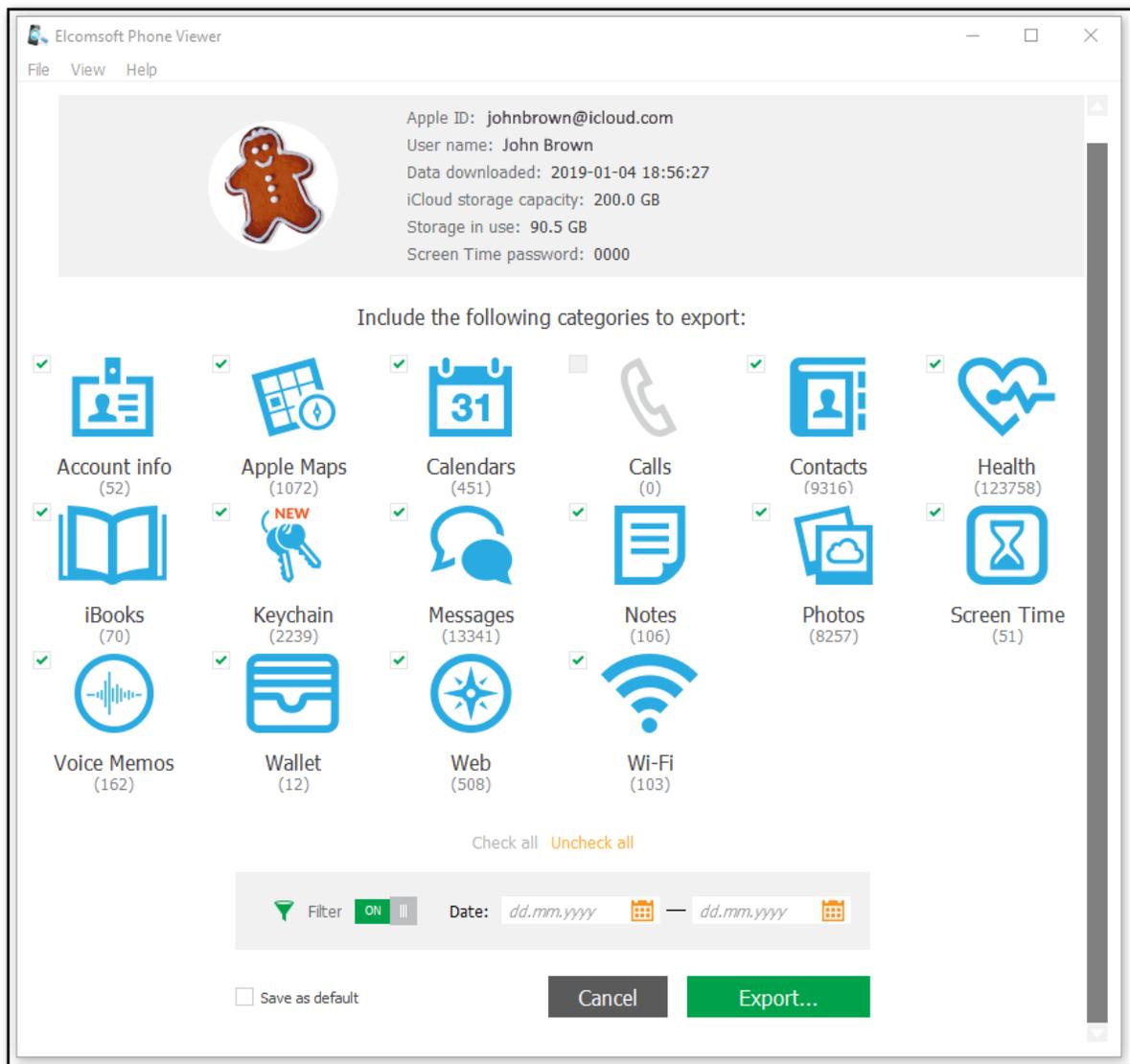
- [Account info](#)
- [Apple Maps](#)
- [Calendars](#)
- [Calls](#)
- [Contacts](#)
- [Health](#)
- [iBooks](#)
- [Keychain](#)
- [Messages](#)

- [Notes](#)
- [Photos](#)
- [Screen Time](#)
- [Voice Memos](#)
- [Wallet](#)
- [Web](#)
- [Wi-Fi](#)

Click the plugin icon to view the contents.

### Exporting Data from Plugins

1. Click **Export**.
2. Select the plugins data from which you want to export or click **Check all**.
3. Optionally, enable filtering to export data for a certain time period. To do so, switch the **On/Off** toggle, and then select the dates in the calendar fields.
4. Click **Export**.
5. In the opened window, select the location in which the file with exported data will be saved and enter the file name.
6. Click **Save**.
7. The **<file name>.xlsx** file is saved in the selected location.

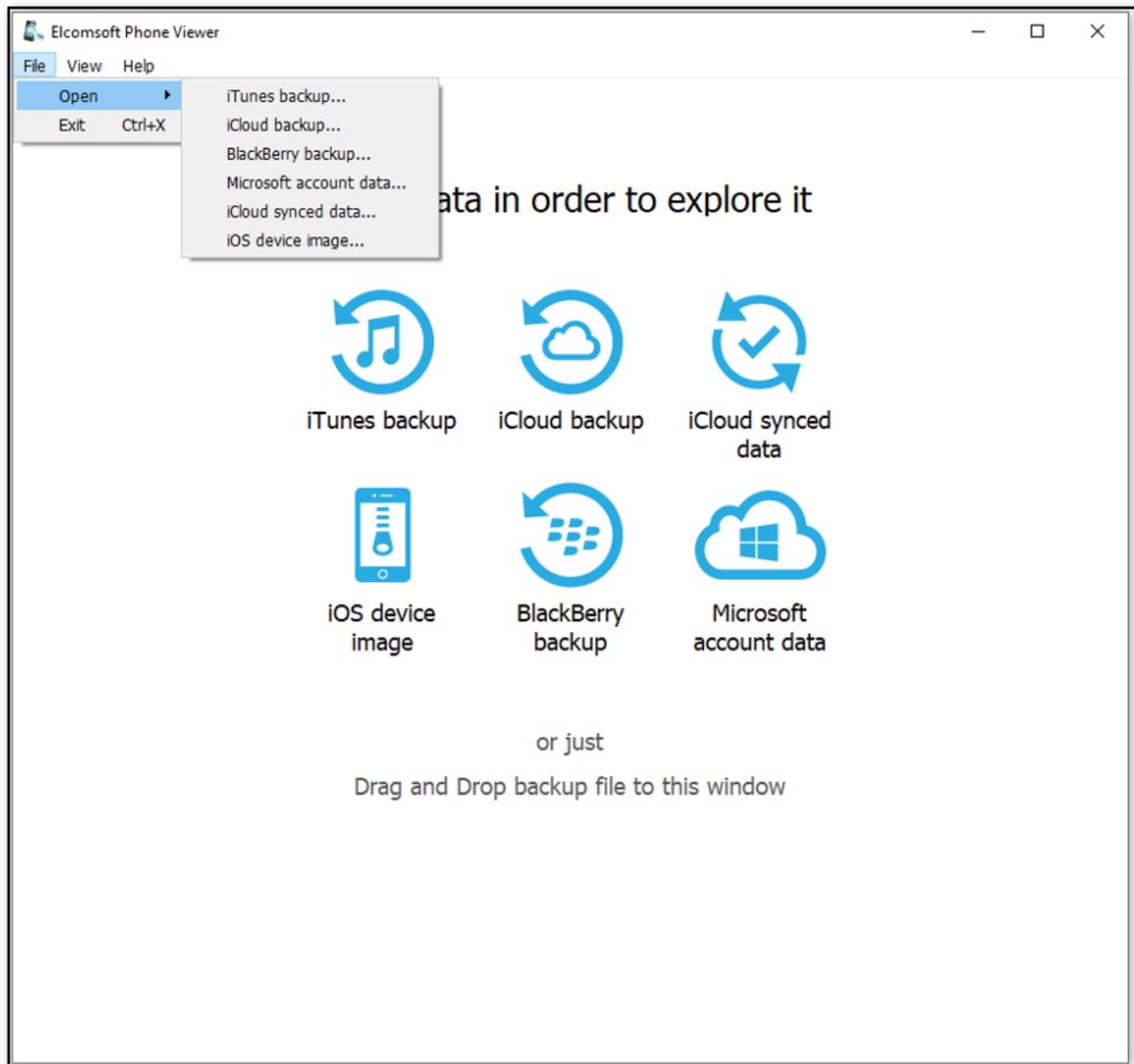


## 4.3 Working with Microsoft and BlackBerry data

### 4.3.1 Working with backups of BlackBerry devices

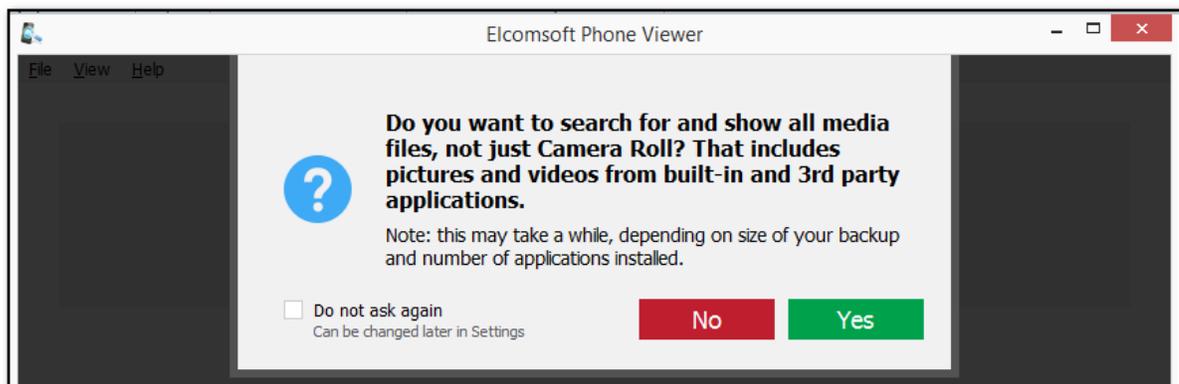
To add the BlackBerry backup to EPV, do the following:

1. On the main program screen, click **BlackBerry backup**, select **BlackBerry backup** in the **File > Open** menu, or drag and drop the backup file to the program window..
2. Browse for BlackBerry backup (\*.bbb; backup should be decrypted, see [Supported BlackBerry device backups](#) for details).



3. Select data types for parsing when opening the backup file.

4. Select if you want EPV to search for and display Camera Roll media only or all media files (you can change this later in Settings).



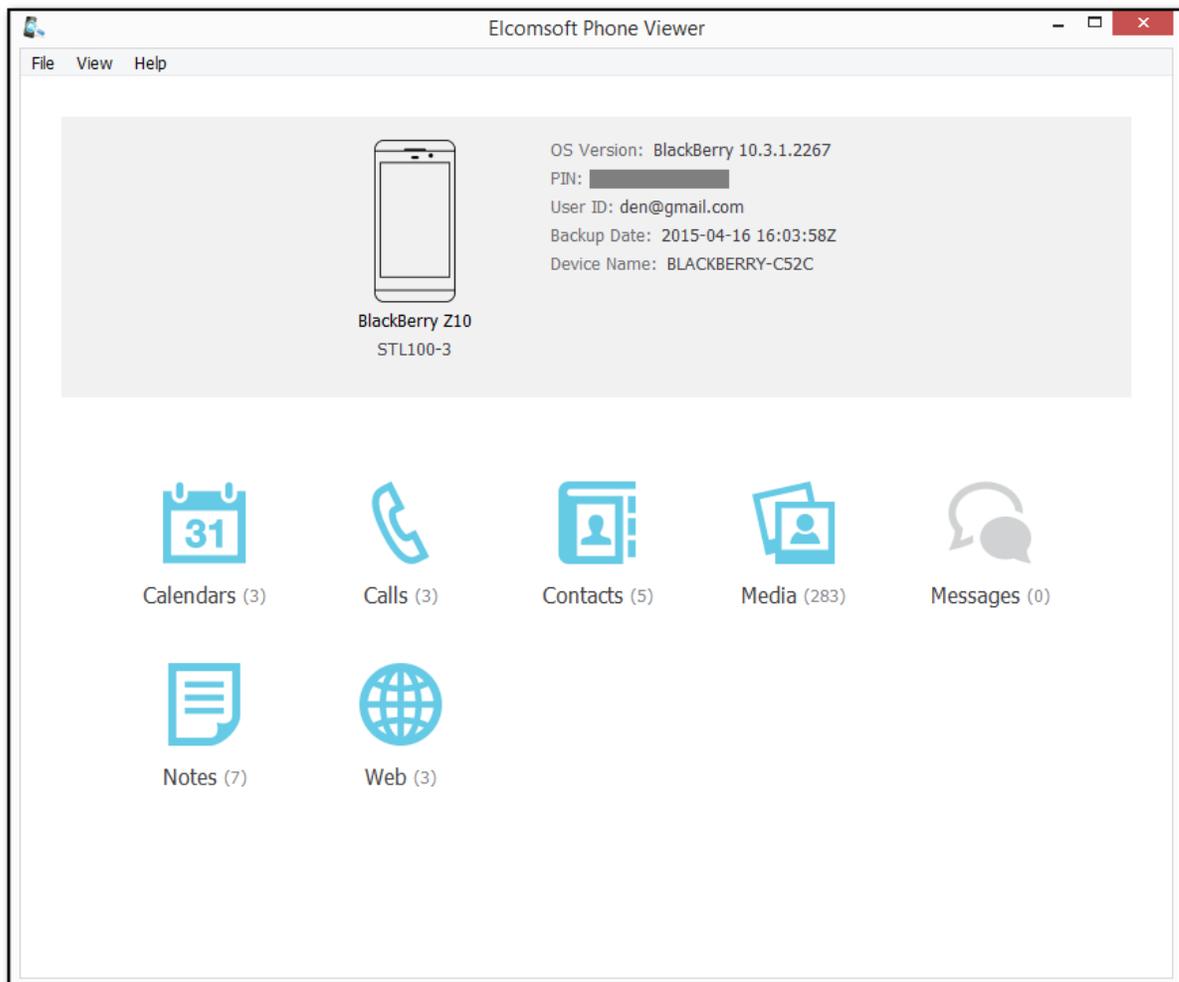
Once all the data in the backup is parsed, the program shows the following information:

- Device image (not the actual one, but generic)
- Device model
- Device "sub-model"
- BB OS version
- Device PIN
- User ID
- Backup date
- Device name
- Country code
- Phone number

The lower part of the window shows all plugins available (some of them might be disabled if there is no appropriate information in the backup):

- [Calendars](#)
- [Calls](#)
- [Contacts](#)
- [Media](#)
- [Messages](#)
- [Notes](#)
- [Web](#)

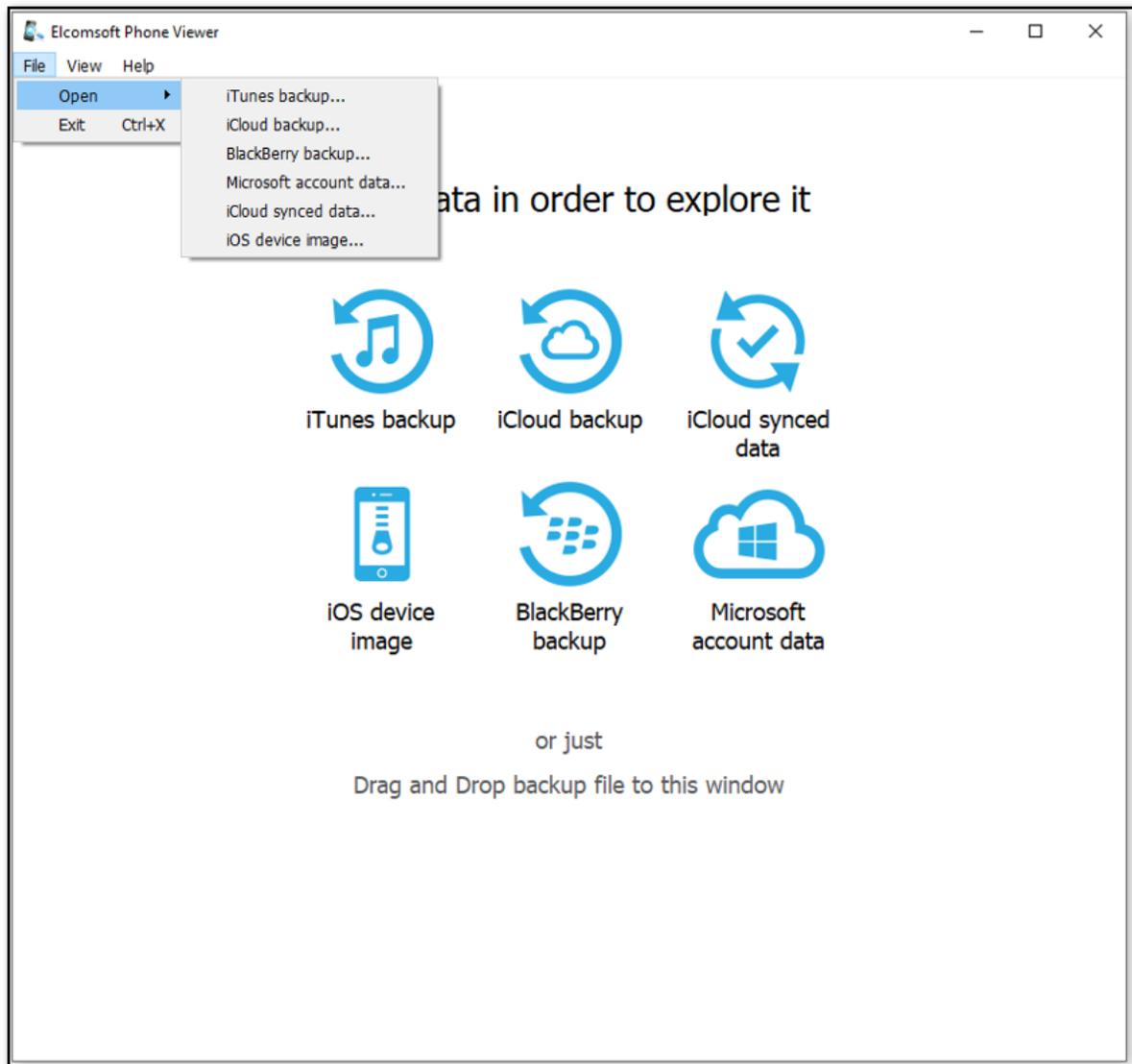
Click the plugin icon to view the contents.



### 4.3.2 Working with Microsoft account data

To add the Microsoft account data to EPV, do the following:

1. On the main program screen, click **Microsoft account data**, select **Microsoft account data** in the **File > Open** menu, or drag and drop the backup file to the program window.
2. Browse for \*.zip file containing the Microsoft account data (see [Microsoft account data](#)).



Once all the data in the backup is parsed, the program shows the following information:

- Device image (generic one)
- Device model
- Device ID
- Phone Number (if available)
- Backup date (which is actually the date when backup has been created/acquired with *Elcomsoft Phone Breaker*)

*Please note that for Windows Phone, the time is the same as on the local PC (the actual time zone of the device is not available).*

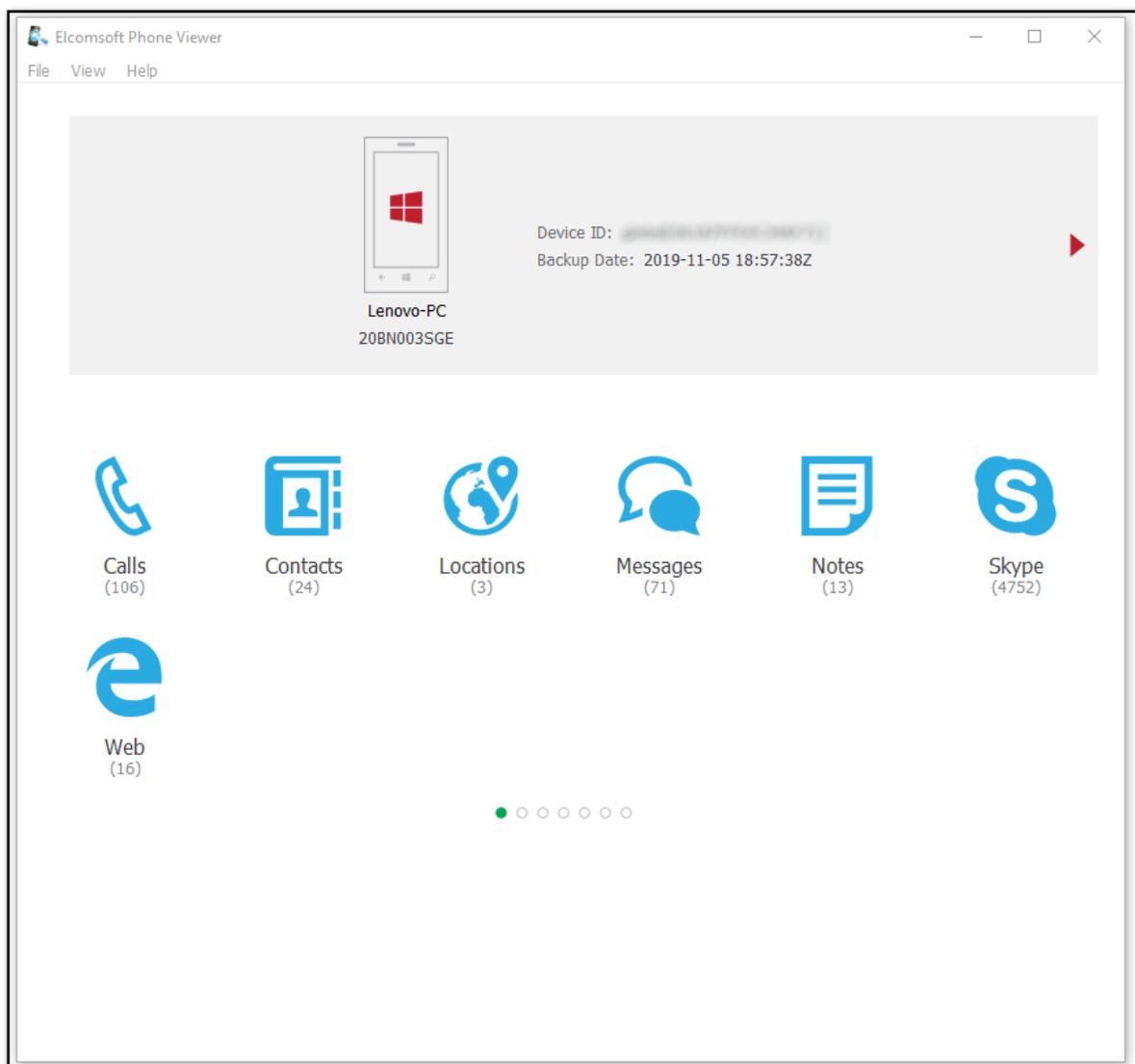
*NOTE: The backup may contain information on several devices connected to the Windows Live! account (used for backup acquisition). If that's the case, you can switch between devices using the arrow signs (at the left and/or right), or with the green dot at the bottom of the screen.*

The lower part of the window shows all plugins available (some of them might be disabled if there is no appropriate information in the backup):

- [Calls](#)
- [Contacts](#)
- [Locations](#)
- [Messages](#)
- [Notes](#)
- [Skype](#)
- [Web](#)

Click the plugin icon to view the contents.

*Please note that information listed above (even SMS) is synced across all the devices on the account, and so does not depend on the particular device you select.*



## 4.4 Plugins

### 4.4.1 Account info

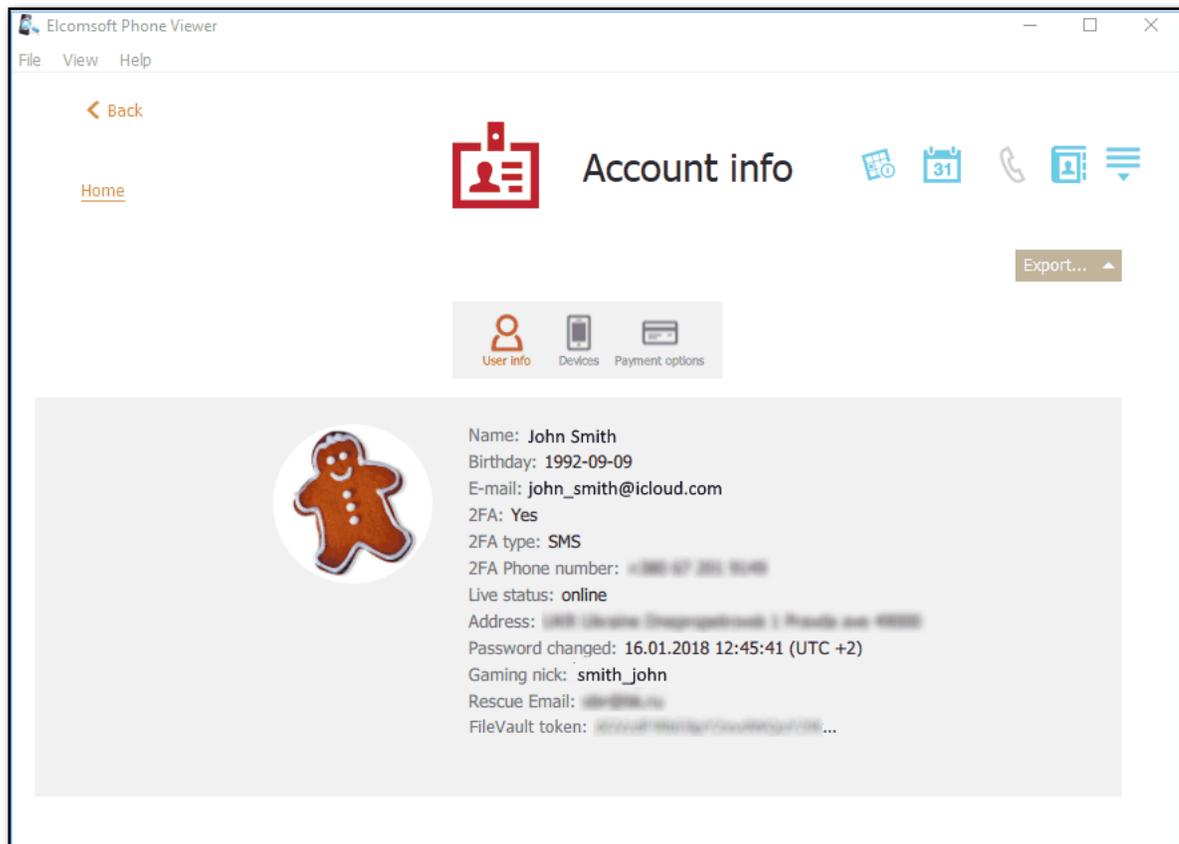
The **Account info** plugin allows you to explore the data related the user's account, such as user personal info, devices information, and payment information.

*NOTE: This plugin is only available for iCloud synced data.*

#### Viewing User info

For **User info**, the following information is displayed:

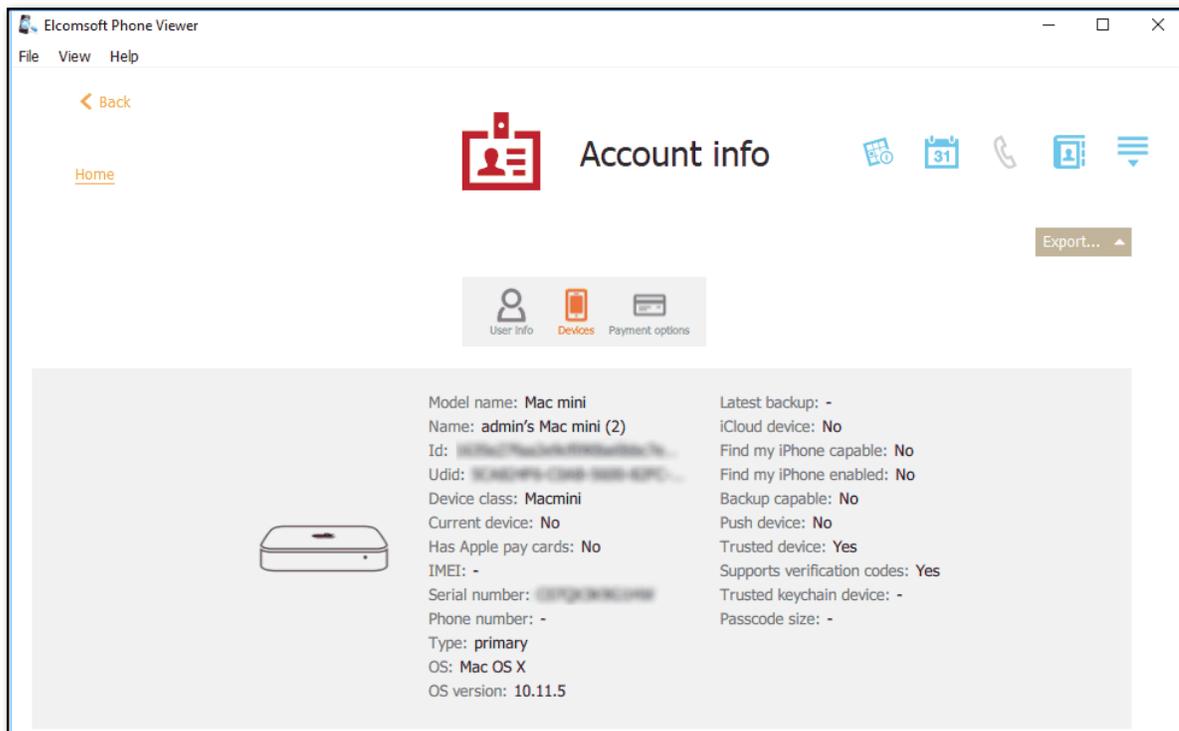
- Name
- Birthday
- E-mail
- 2FA (Yes/No)
- 2FA type
- 2FA Phone number
- Live status (online/offline)
- Address
- Password changed (date of the latest password changing)
- Gaming nick
- Rescue Email (email address for security notifications)
- FileVault token (a recovery token used to decrypt the macOS disk image in **Elcomsoft Forensic Disk Decryptor**)



## Viewing Devices

For **Devices**, the following information is displayed:

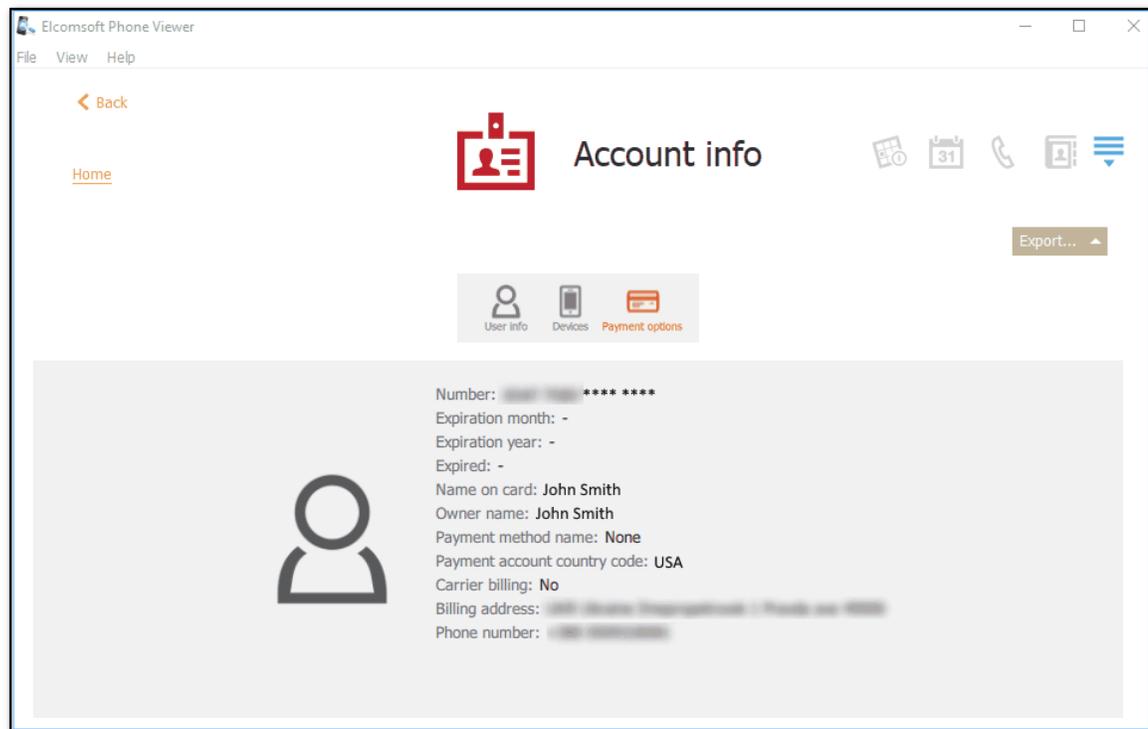
- Model name
- Name
- Id
- Udid (unique device ID)
- Device class
- Current device
- Has Apple pay cards
- IMEI
- Serial number (only for accounts with 2FA)
- Phone number
- Type
- OS
- OS version
- Latest backup (date of the latest backup)
- iCloud device
- Find my iPhone capable (only for accounts with 2FA)
- Find my iPhone enabled (only for accounts with 2FA)
- Backup capable (only for accounts with 2FA)
- Push device
- Trusted device (only for accounts with 2FA)
- Supports verification codes
- Trusted keychain device
- Passcode size



### Viewing Payment options

For **Payment options**, the following information is displayed:

- Number
- Expiration month
- Expiration year
- Expired
- Name on card
- Owner name
- Payment method name
- Payment account country code
- Carrier billing
- Billing address
- Phone number



### Exporting Account Info

To export account info, do the following:

1. Click **Export**.
2. Select **All**.
3. The **Select destination file** window will open.
4. In the opened window, select the location in which the file with exported account info will be saved, enter the file name and select the file extension (.xml or .xlsx).
5. Click **Save**.
6. The file is saved in the selected location.

## 4.4.2 Apple Pay

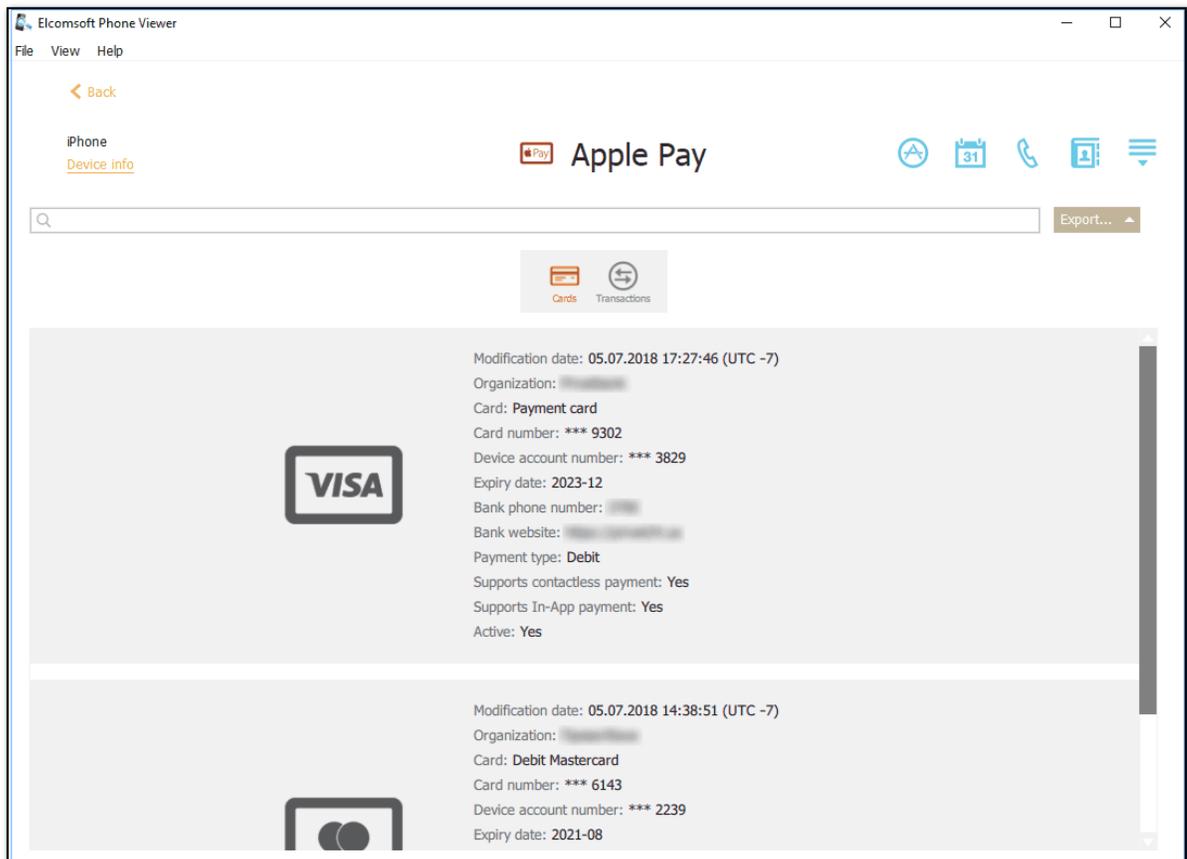
The **Apple Pay** plugin allows you to explore the Apple Pay app data such as information about cards and transactions.

*NOTE: This plugin is only available for images (.tar) of iOS devices with a set passcode.*

### Viewing Cards

Click the **Cards** tab to see the following information on each card:

- Modification date: The date and time the card was added/edited
- Organization
- Card: The type of the card
- Card number
- Device account number
- Expiry date
- Bank phone number
- Bank website
- Payment type
- Supports contactless payment (Yes/No)
- Supports In-App payment (Yes/No)
- Active (Yes/No)



## Viewing Transactions

Click the **Transactions** tab to see the following information about transactions in a grid:

- Date: The date and time the transaction was made
- Merchant
- Category
- Amount
- Status (Approved/Denied)
- Card Number (only the last four digits are displayed)
- Device Account Number
- Location
- Address
- Merchant Location
- Merchant Address
- Merchant Phone Number
- Merchant URL: The merchant website

The general information about transactions is displayed above the grid:

- **Records:** total number of transactions
- **Most recent:** date and time the most recent transaction was made
- **Oldest:** date and time the oldest transaction was made

If the filtering is on, you can also view the statistic information on the filtered transactions:

- **Shown records:** number of transactions that match the filtering criteria
- **Most recent filtered record:** date and time the most recent transaction (among the filtered records) was made
- **Oldest filtered record:** date and time the oldest transaction (among the filtered records) was made

To sort the transactions in the grid, click the necessary column header.

The screenshot shows the Elcomsoft Phone Viewer interface for an iPhone. The main view is titled "Apple Pay" and displays a list of transactions. A sidebar on the left contains a filter menu with options for "Date Created" (From: 05.07.2018, Until: 08.07.2018) and "Card number" (6143 (2), 9302 (4)). The main area shows a summary of 6 records, with the most recent record on 08.07.2018 at 17:32:46 and the oldest on 05.07.2018 at 18:08:40. Below the summary is a table of transactions.

Category	Amount	Status	Card Number	Device Account Number
SUPERMARKETS	268.70 USD	Approved	*** 9302	*** 3829
SUPERMARKETS	68.40 USD	Approved	*** 9302	*** 3829
RETAIL	68.40 USD	Denied	*** 6143	*** 2239
SUPERMARKETS	79.55 USD	Approved	*** 9302	*** 3829
DINING	45.00 USD	Approved	*** 9302	*** 3829
RETAIL	45.00 USD	Denied	*** 6143	*** 2239

## Searching and Filtering

To perform searches in the **Apple Pay data**, enter the search request in the search field and press **Enter**. The search results will be highlighted in yellow. The number of search results will be displayed in the search field.

Search can be performed by the following parameters:

- **Cards:**
  - Organization
  - Card
  - Card number
  - Device account number
  - Expiry date
  - Bank phone number
  - Bank website
  - Payment type
- **Transactions:**
  - Merchant
  - Category
  - Amount
  - Card Number
  - Device Account Number
  - Location
  - Address
  - Merchant Location
  - Merchant Address
  - Merchant Phone Number
  - Merchant URL

To filter the **Apple Pay data**, open the **Filter** pane by clicking the  icon on the left. Only **Transactions** can be filtered.

Enable filtering by switching the **On/Off** toggle, and define the filtering options:

- **Date:** filters transactions by date. Define the **From** and **Until** dates.
- **Card number:** filters transactions by card numbers.

## Exporting Apple Pay Data

To export data, do the following:

1. Click **Export**.
2. Select one of the following values from the drop-down list: **Filtered** (available only for **Transactions**) or **All**.
3. The **Select destination file** window opens.
4. In the opened window, select the location in which the file with exported data will be saved and enter the file name.
5. Click **Save**.
6. The **<file name>.xlsx** file is saved in the selected location.

### 4.4.3 Apple Maps

The **Apple Maps** plugin allows you to explore such information as detailed search history, information about created bookmarks, explored places, and directions searches.

*NOTE: This plugin is only available for iCloud sync backups with Apple Maps support.*

All records are displayed in a grid. The most recently added records are displayed on top. The general information about records is displayed above the grid:

- **Records:** total number of records
- **Most recent:** date and time when the most recent records were added
- **Oldest:** date and time when the oldest records were added

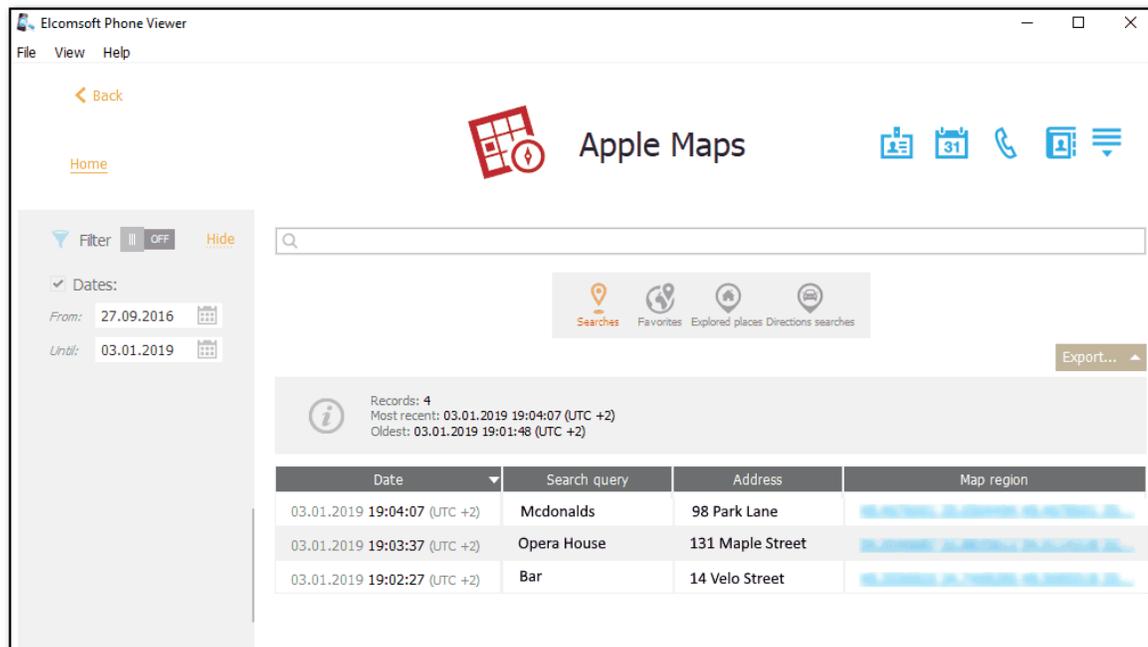
If the filtering is on, you can also view the statistic information on the filtered records:

- **Shown records:** number of records that match the filtering criteria
- **Most recent filtered:** date and time of when the most recent records (among the filtered records) were added
- **Oldest filtered:** date and time when the oldest records (among the filtered records) were added

### Viewing Searches

For **Searches**, the following information is displayed:

- Date (date and time of the search)
- Search query (search phrase)
- Address (found location)
- Map region (latitude and longitude of the location)

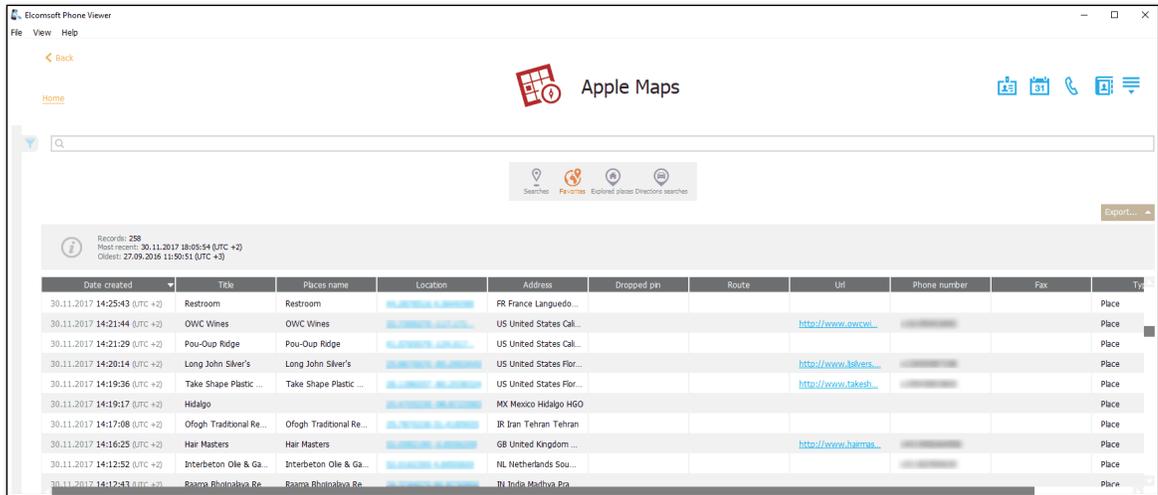


### Viewing Favorites

For **Favorites**, the following information is displayed:

- Date created
- Title
- Place name

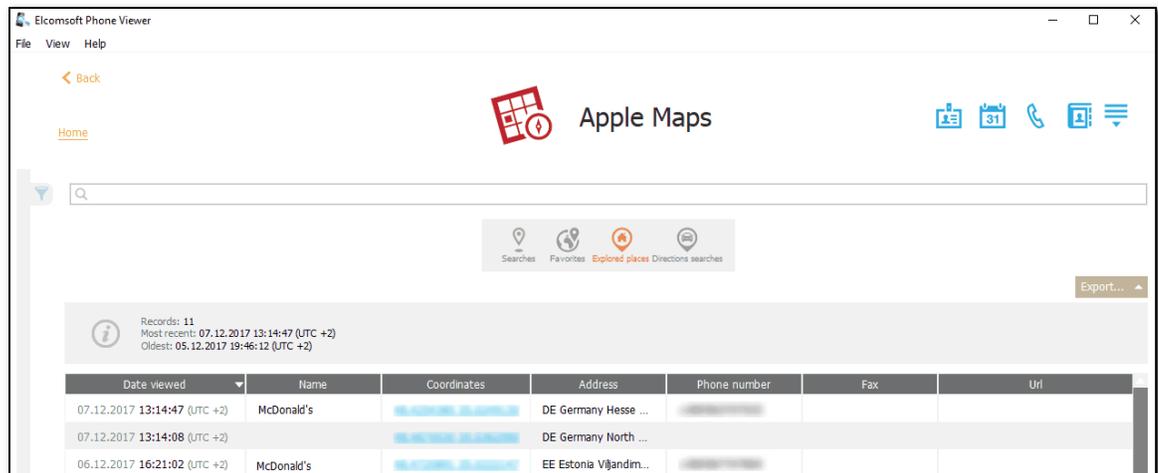
- Location
- Address
- Dropped pin (coordinates of a pinned location)
- Route
- Url
- Phone number
- Fax
- Type



### Viewing Explored places

For **Explored places**, the following information is displayed:

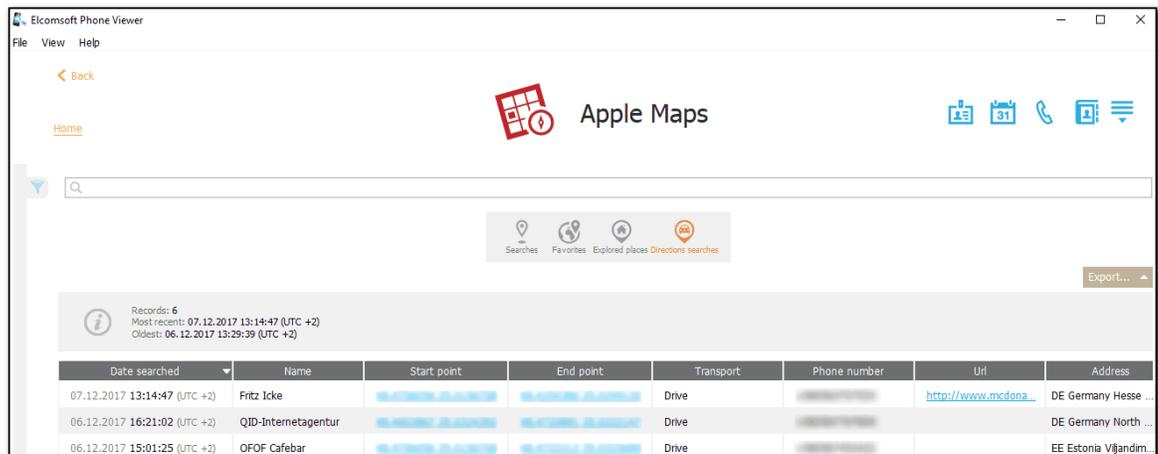
- Date viewed
- Name
- Coordinates
- Address
- Phone number
- Fax
- Url



## Viewing Directions

For **Directions**, the following information is displayed:

- Date searched
- Name
- Start point
- End point
- Transport
- Phone number
- Url
- Address



## Searching and Filtering

You can search for **Apple Maps data** by all parameters except for date values.

**To perform searches in Apple Maps**, enter the necessary value in the search field and press **Enter**. The search results will be highlighted in yellow. The number of search results will be displayed in the search field.

**To filter the Apple Maps data**, open the **Filter** pane by clicking the  icon on the left.

Enable filtering by switching the **On/Off** toggle, select the **Date** check box, and then select the **From** and **Until** dates in the calendar fields.

## Exporting Apple Maps Data

**To export data**, do the following:

1. Click **Export**.
2. Select one of the following values from the drop-down list: **Filtered** or **All**.
3. The **Select destination file** window will open.
4. In the opened window, select the location in which the file with exported data will be saved, enter the file name and select the file extension (.kml or .xlsx).
5. Click **Save**.
6. The file is saved in the selected location.

#### 4.4.4 Applications

The **Applications** plugin allows you to explore the information on applications installed on the device.

*NOTE: This plugin is only available for iOS 7.x.x and higher backups.*

When opening the plugin, you have an option to download the additional information about the applications from the internet. Please note that the internet connection is required in order to get the additional information.

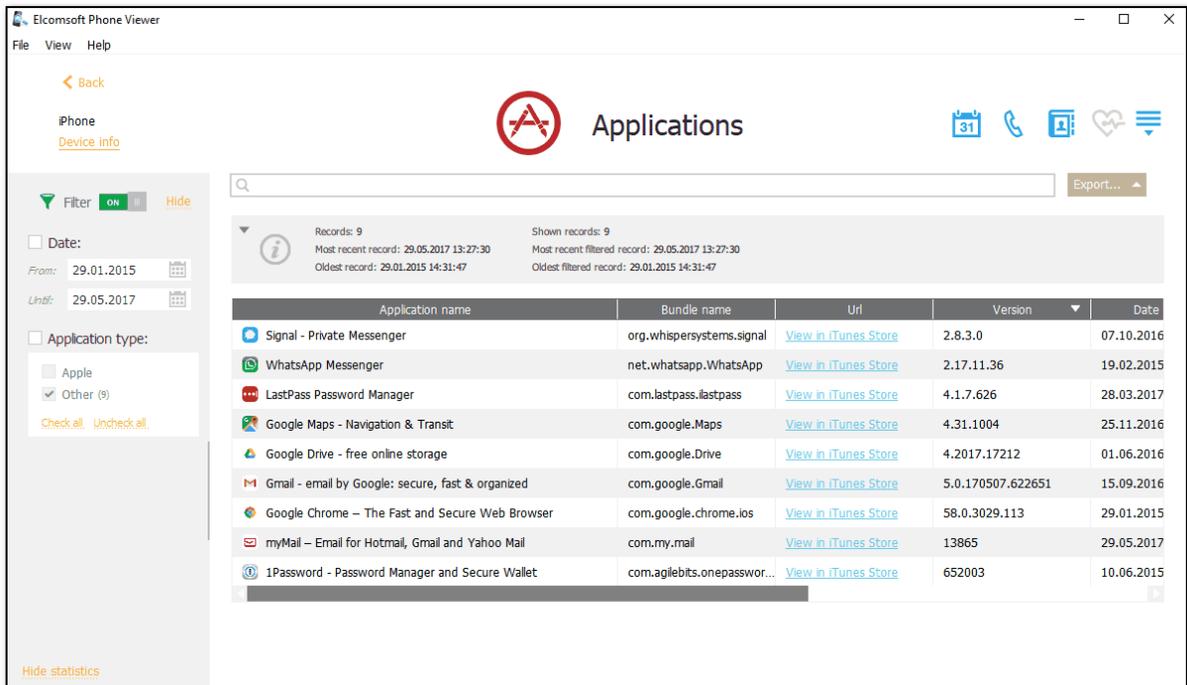
**For local backups**, the following information is available:

- General information:
  - Application icon
  - Application name
  - Bundle name (for example: Com.google.Maps)
  - URL to the application in iTunes
  - Bundle version
  - Date purchased
  - Date installed (for iOS device images only)
  - Date uninstalled (for iOS device images only)
  - AppleID
  - Copyright
  - Vendor
  - Category
  - Rated
  - Date updated
- Additional information that is displayed only if the option to download the detailed information was selected when opening the plugin:
  - Compatibility: supported devices
  - Languages
  - Required iOS
  - Description: description of the application
  - What's New: release notes
  - Price
  - Currency

**For iCloud backups**, the following information is available:

- General information:
  - Bundle name (for example: Com.google.Maps)
- Additional information that is displayed only if the option to download the detailed information was selected when opening the plugin:
  - Application name
  - Bundle name (for example: Com.google.Maps)
  - Category
  - Rated
  - Compatibility: supported devices
  - Languages
  - Required iOS
  - Description: description of the application
  - What's New: release notes
  - Price
  - Currency
  - Date updated

Please note that the additional information downloaded from the Internet corresponds to the most recent version of the application that can be different than the version installed on the device.



All applications are displayed in a grid. The most recently installed application is displayed on top. The general information about applications is displayed above the grid:

- **Records:** total number of applications
- **Most recent record:** date and time when the most recent application was installed
- **Oldest record:** date and time when the oldest application was installed

If the filtering is on, you can also view the statistic information on the filtered applications:

- **Shown records:** number of applications that match the filtering criteria.
- **Most recent filtered record:** date and time of when the most recent application (among the filtered records) was installed
- **Oldest filtered record:** date and time when the oldest application (among the filtered records) was installed

To sort the applications in the grid, click the necessary column header.

### Searching and Filtering

You can search for applications by all parameters except for date values.

**To perform searches in Applications**, enter the necessary value in the search field and press **Enter**. The search results will be highlighted in yellow. The number of search results will be displayed in the search field.

**To filter the applications**, open the **Filter** pane by clicking the  icon on the left. Enable filtering by switching the **On/Off** toggle, and define the filtering options:

- **Date:** filters the applications by installation date. Select the **Date** check box and then select the **From** and **Until** dates in the calendar fields.
- **Application type:** filters the applications by application type (category). Select the **Application type** check box and then select the check boxes for the necessary application types.

If you clear any check box for an application type, a negative number will be displayed next to the **Application type** filter. This number indicates the number of records that are currently not displayed.

### Exporting Applications

To export applications, do the following:

1. Click **Export**.
2. Select one of the following values from the drop-down list: **Filtered** or **All**.
3. The **Select destination file** window will open.
4. In the opened window, select the location in which the file with exported applications will be saved, enter the file name and select the file extension (.xml or .xlsx).
5. Click **Save**.
6. The file is saved in the selected location.

### 4.4.5 Calendars

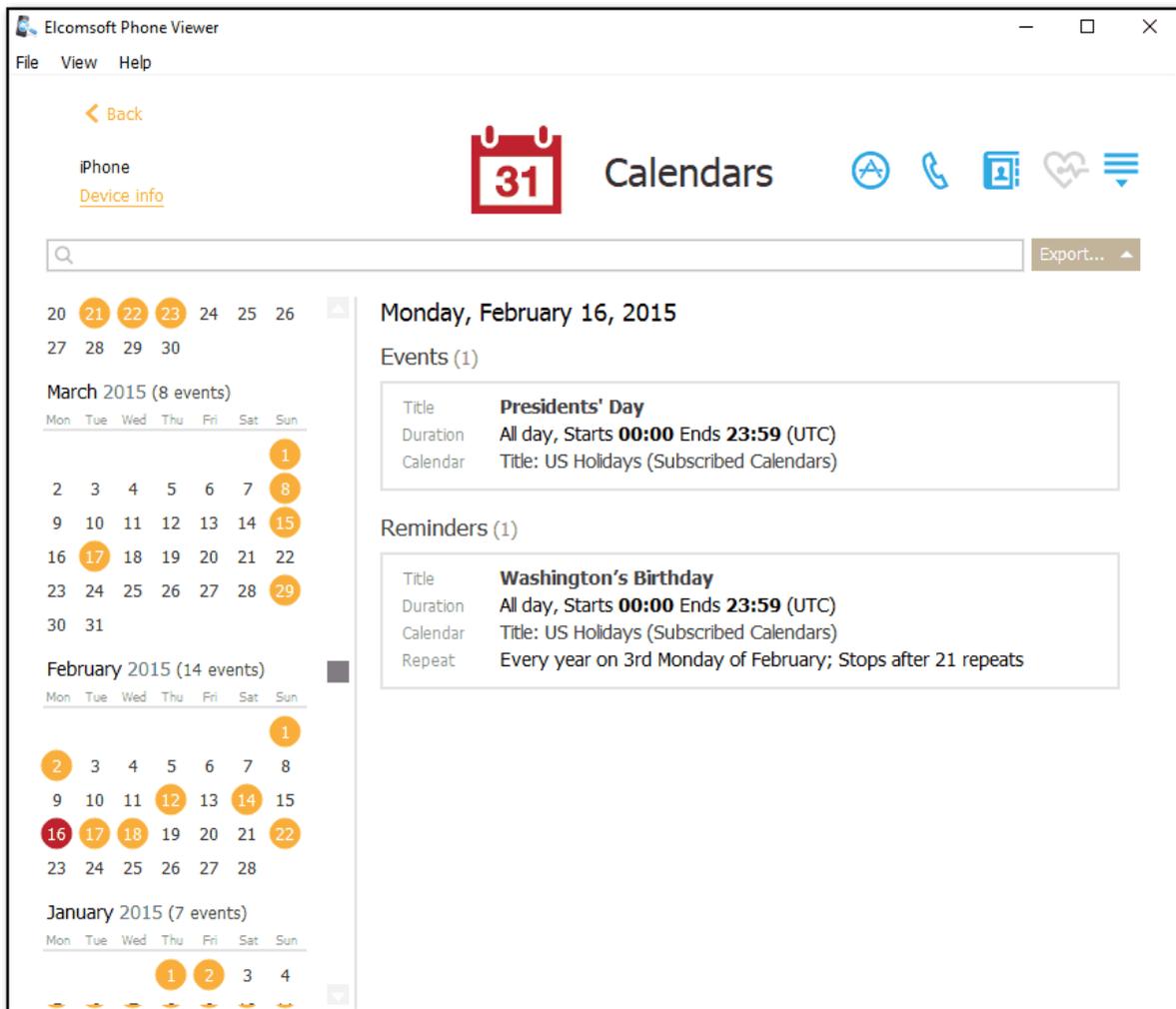
You can explore the events planned in all calendars (regardless of the account) used by device user: one time and regular events, birthdays, holidays and so on. Please note that for recurrent events/appointments, only the first day of the event is shown.

*Note: There are no calendars in Windows Phone backups, so this plugin is active for BlackBerry and iOS backups only.*

Scroll down to month/year you want to view the events for, and select the proper day -- all events for the selected day will be shown on the right, including the following information:

- Title
- Location
- Duration (including the time zone)
- Calendar (there could be a few accounts in the system)
- Organizer (the person who organizes the event)
- Participants
- Alert, if set
- Repeat (if available)
- Notes (if available)

To perform searches in **Calendars**, enter the necessary keyword in the search field and press **Enter**. The search results will be highlighted in yellow.



## Exporting

To export calendars data, do the following:

1. Click **Export**.
2. Select **All**.
3. The **Select destination file** window will open.
4. In the opened window, select the location in which the file with exported data will be saved and enter the file name.
5. Click **Save**.
6. The **<file name>.xlsx** file is saved in the selected location.

### 4.4.6 Calls

EPV allows you to explore the call history of the device under investigation. You can analyze the full history of outgoing/incoming/missed/not answered calls. You can also see whether a call was a regular phone one or made via third-party services (Skype, WhatsApp, Viber or FaceTime).

The following call properties are displayed:

- Type (incoming, outgoing, missed, dialed; voice or video)
- Date and time (including the time zone)

*NOTE: If the timezone of the device is not detected, the time of the call will be displayed in UTC time and the corresponding warning will be displayed in the Journal of the View menu.*

- Phone number and information about a contact from the [Contacts](#)
- Status/Duration: for answered incoming and outgoing calls the duration is displayed while missed and unanswered calls are marked *Missed* or *Not Answered*, respectively.
- Service: The service that the call was made through (Cellular, Skype, WhatsApp, Viber, or FaceTime).

*NOTE: Calls made via third-party services (Skype, WhatsApp, Viber, FaceTime) are supported for Apple device backups only. The Service column is not displayed for Blackberry backups and Microsoft account data.*

## Exporting

To export calls, do the following:

1. Click **Export**.
2. Select one of the following values from the drop-down list: **Filtered** or **All**.
3. The **Select destination file** window will open.
4. In the opened window, select the location in which the file with exported data will be saved and enter the file name.
5. Click **Save**.
6. The **<file name>.xlsx** file is saved in the selected location.

## Searching and Filtering

To perform searches in **Calls**, enter the search request in the search field and press **Enter**. The search results will be highlighted in yellow.

To filter the calls, open the **Filter** pane by clicking the  icon on the left.

Enable filtering by switching the On/Off toggle, and define the filtering options:

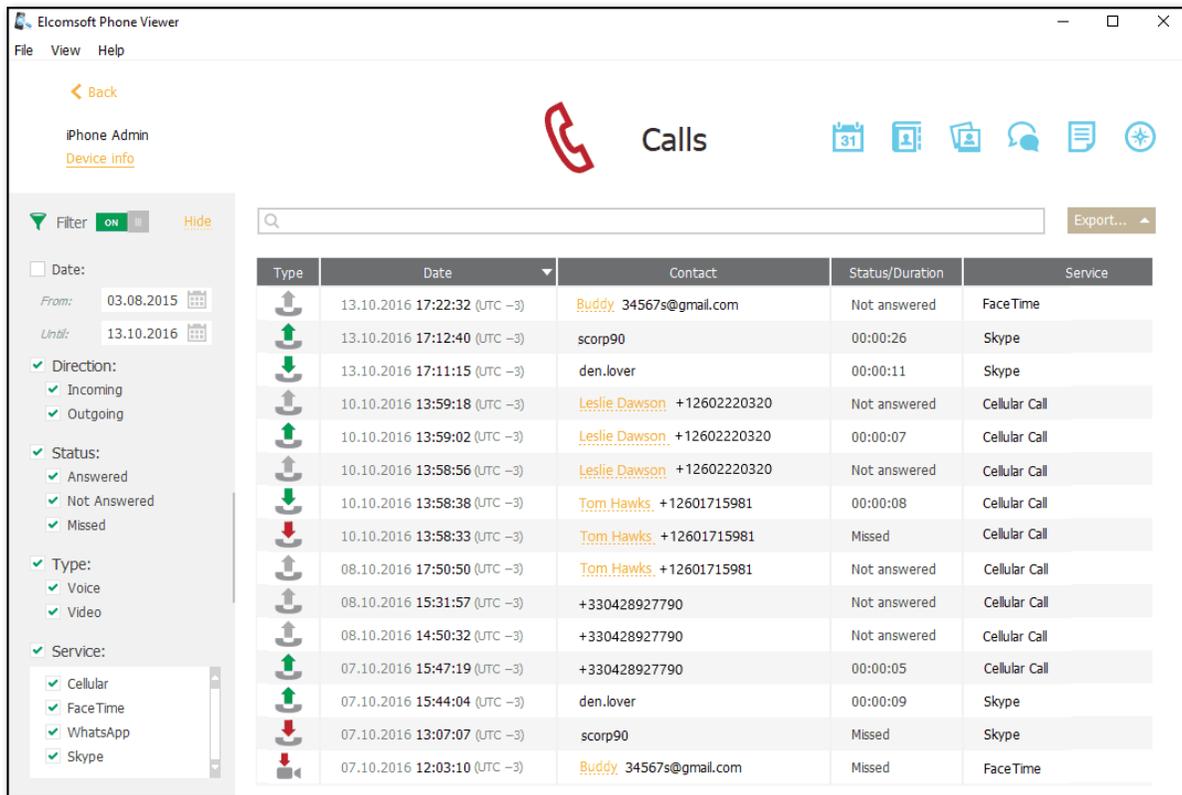
- **Date:** filters the calls by date. Select the year in the drop-down list below and define the time interval by moving the slider on the scale with names of months.
- **Direction:** filters the calls by direction (incoming or outgoing).
- **Status:** filters the calls by the status (answered, not answered, or missed).
- **Type:** filters the calls by their type (voice or video).  
*NOTE: Calls made via third-party services (Skype, WhatsApp, Viber, FaceTime) are not supported for BlackBerry backups. Filtering by type is not available for Blackberry backups.*
- **Service:** filters the calls by the service they were made through (cellular, Skype, WhatsApp, Viber, FaceTime).

*NOTE: Calls made via third-party services (Skype, WhatsApp, Viber, FaceTime) are supported for Apple backups only. Filtering by service is not available for Blackberry backups and Microsoft account data.*

- **Devices:** filters the calls by the device.

*NOTE: This filter is available only for Microsoft account data.*

*NOTE: When using filter options, you will be able to view only the records allowed by your license type.*



#### 4.4.7 Contacts

This plugin shows all the contacts included into the backup (which may include not just the local device address, but also the contacts from the accounts: Exchange/Outlook, iCloud, Google etc, if synced with the device). Select the contact on the left, and all the information that is available for it will be shown on the right.

The general information about the contact is usually the following:

- Contact photo/image/avatar
- Created/modified date and time (including the time zone)

*Please note that for BlackBerry and iOS devices the time is stated as it is (was) set on the device; for Windows Phone, the time is the same as on the local PC (the actual time zone of the device is not available).*

*If the timezone of the device is not detected for BlackBerry and iOS devices, the time will be displayed in UTC time and the corresponding warning will be displayed in the Journal of the View menu.*

*Note that the timezone is shown correctly for full iCloud backups but might be also shown always in UTC if only selected categories have been downloaded.*

- First and last name
- Company name
- Phone numbers
- Groups
- Other info (email, web site, links to social media profiles, etc)

Note that the list of contact properties may vary from device to device and account type.

## Exporting

To export contacts, do the following:

1. Click **Export**.
2. Select **All**.
3. The **Select destination file** window will open.
4. In the opened window, select the location in which the file with exported data will be saved and enter the file name.
5. Click **Save**.
6. The **<file name>.xlsx** file is saved in the selected location.

## Searching and Filtering

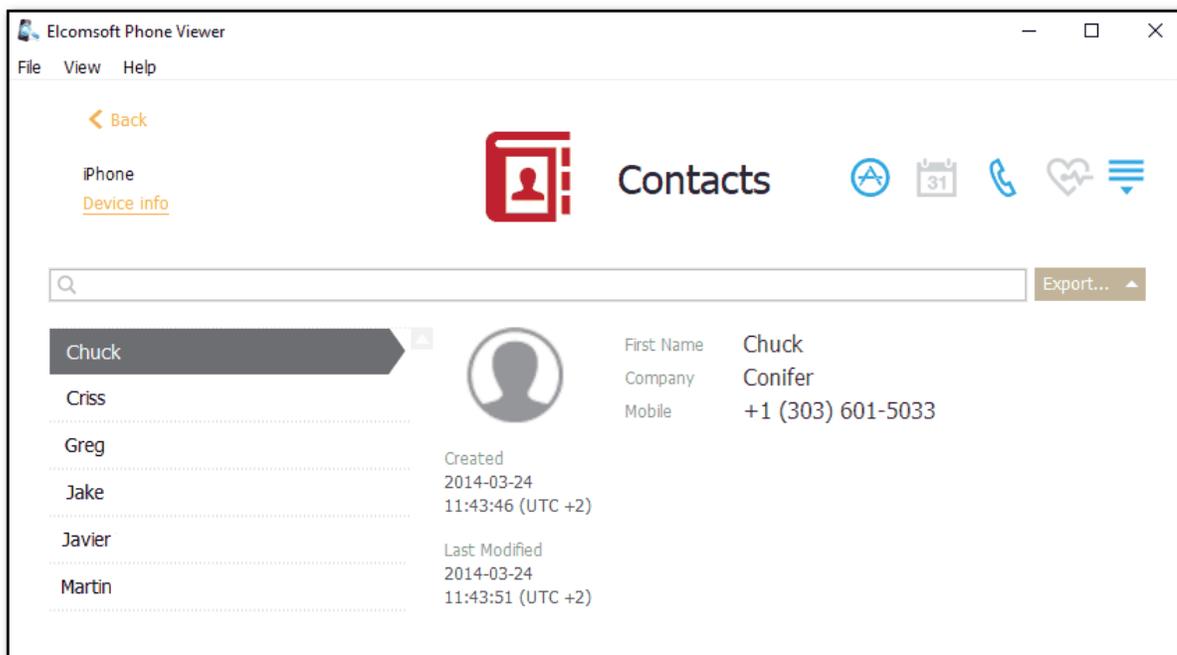
To perform searches in **Contacts**, enter the search request in the search field and press **Enter**. The search results will be highlighted in yellow.

To filter out the contacts by accounts and groups, open the **Filter** pane by clicking the  icon on the left.

Enable filtering by switching the On/Off toggle, and define the filtering options:

- Select the **Show only favorites** check box to find the contacts marked as favorite. Please note that this option is available only for iOS and Windows Phone backups.
- Filter by groups or accounts the contacts belong to.

*NOTE: When using filter options, you will be able to view only the records allowed by your license type.*



### 4.4.8 Health

The **Health** plugin allows you to explore the Apple Health app data such as information about user's fitness activities, sleep cycles, nutrition, etc.

*NOTE: This plugin is available for backups of the following types: iCloud synced data, images of iOS device, and iTunes (only encrypted backups).*

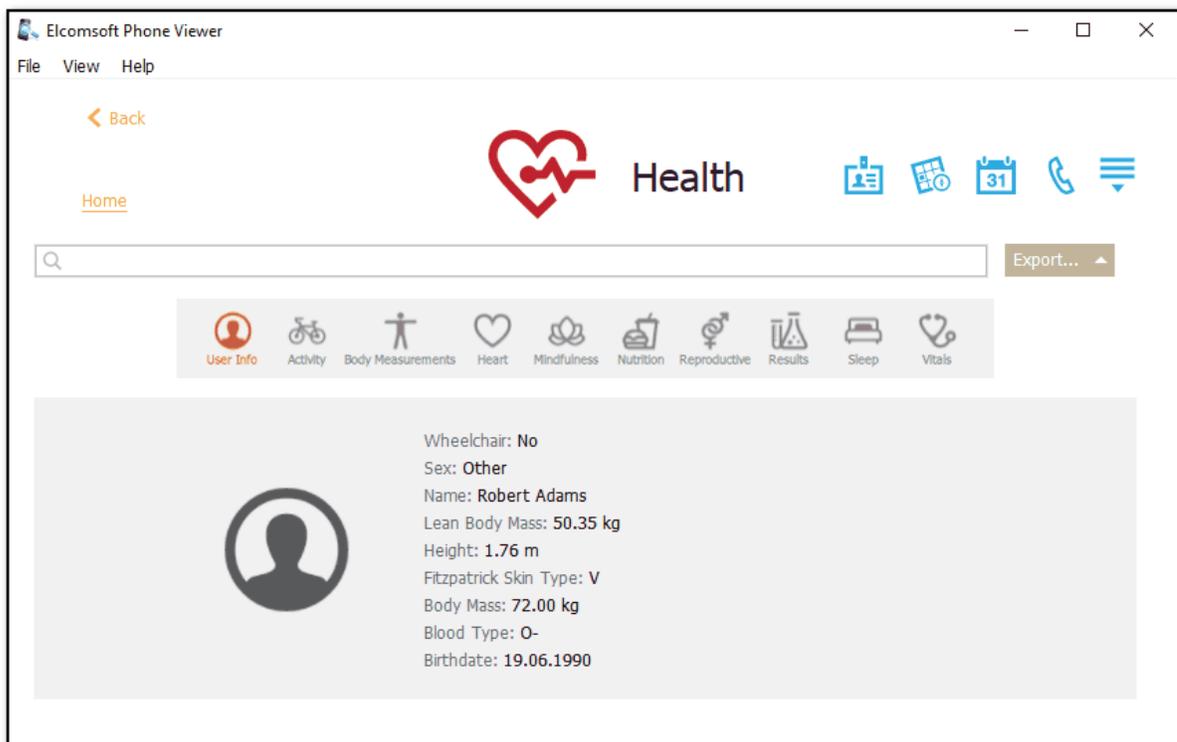
The data in the plugin is divided into the following health & fitness data categories:

- User Info
- Activity
- Body Measurements
- Heart
- Mindfulness
- Nutrition
- Reproductive
- Results
- Sleep
- Vitals

Some categories might be disabled if there is no corresponding data.

For **User Info**, the following information is displayed:

- Wheelchair (Yes/No)
- Sex
- Name
- Lean Body Mass
- Height
- Fitzpatrick Skin Type
- Body Mass
- Blood Type
- Birthdate



For all health & fitness data categories except **User Info**, all records are displayed in a grid. The most recently added records are displayed on top.

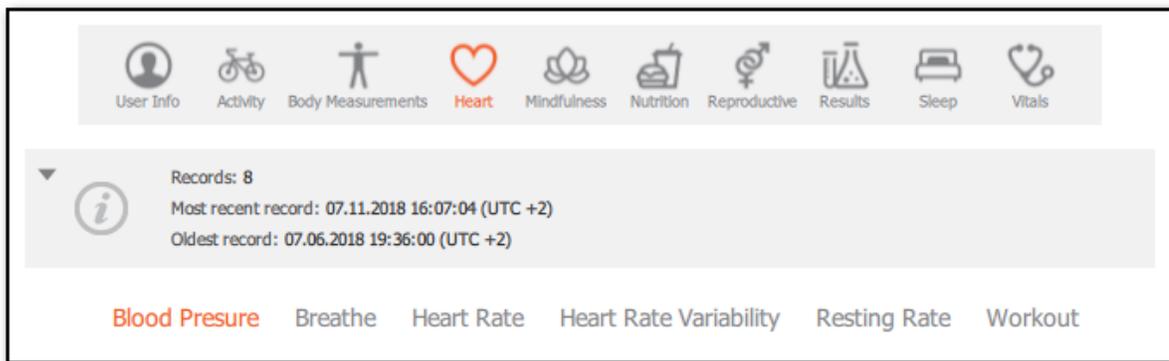
The general information about records is displayed above the grid:

- **Records:** total number of records
- **Most recent record:** date and time when the most recent record was added
- **Oldest record:** date and time when the oldest record was added

If the filtering is on, you can also view the statistic information on the filtered records:

- **Shown records:** number of records that match the filtering criteria
- **Most recent filtered record:** date and time when the most recent record (among the filtered records) was added
- **Oldest filtered record:** date and time when the oldest record (among the filtered records) was added

For the **Activity**, **Body Measurements**, **Heart**, **Nutrition**, **Reproductive**, **Results**, and **Vitals** health & fitness data categories, the information is divided into subcategories. Each subcategory is displayed only if there is corresponding data in the backup.

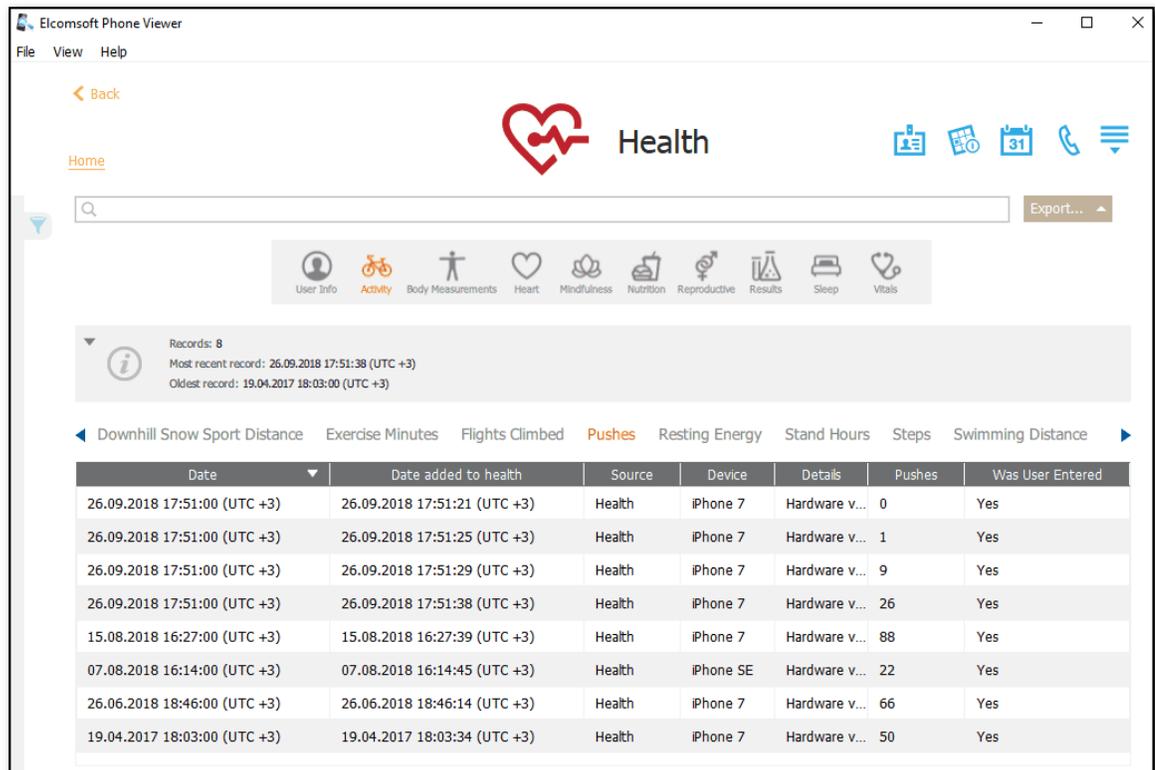


For the **Activity**, **Body Measurements**, **Heart**, **Mindfulness**, **Nutrition**, **Reproductive**, **Results**, **Sleep**, and **Vitals** health & fitness data categories, the following information is displayed:

- Date (or Start Date, End Date)
- Date added to health: Date and time the record was added to the Health app
- Source: Source of health & fitness data (for example, Health app or another third-party fitness app, Apple Watch, fitness band, etc.)
- Device: The device from which the health & fitness data was synced with iCloud
- Details: Information on the hardware version and source version
- Was User Entered (Yes/No)
- Information specific to each category/subcategory (for example, in the Activity data category, in the Pushes subcategory, specific information pushes is displayed in the Pushes column)

Deleted records for some categories might be displayed. Unfortunately, not all deleted records can be recovered. Date/time information is not available in many cases, and records might look corrupted.

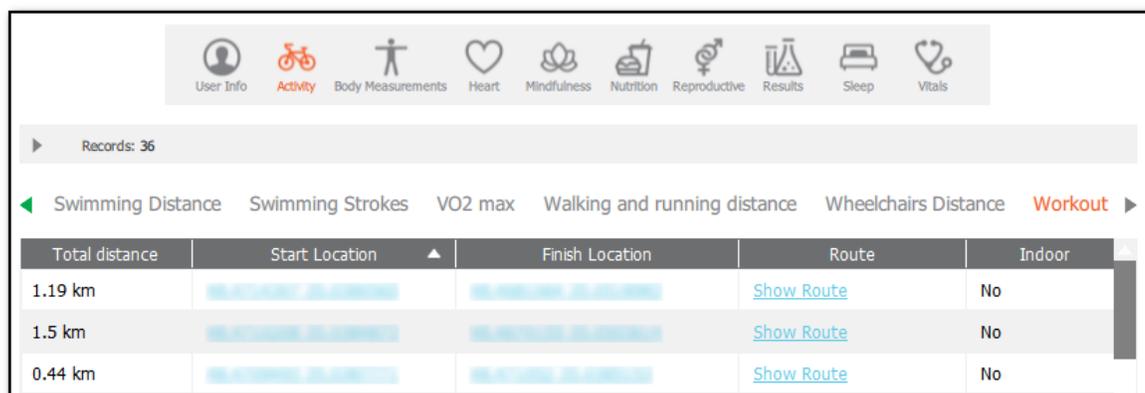
You can filter out the deleted records by selecting the corresponding filtering option (**Type: Deleted**)



In the **Activity** data category, in the **Workout** subcategory, you can view the information on locations in the following columns:

- Start Location: Latitude and longitude of the location where the workout started
- Finish Location: Latitude and longitude of the location where the workout finished
- Route: Contains a Show Route link allowing you to view the route on a map

*NOTE: Latitude and longitude are available only for iCloud synced data.*



### Exporting Health Data

To export data, do the following:

1. Click **Export**.
2. Select one of the following values from the drop-down list: **Filtered** or **All**.
3. The **Select destination file** window opens.

4. In the opened window, select the location in which the file with exported data will be saved and enter the file name.
5. Click **Save**.
6. The **<file name>.xlsx** file is saved in the selected location.

### Searching and Filtering

**To perform searches in the Health app data**, enter the necessary value in the search field and press **Enter**. The search results will be highlighted in yellow. The number of search results will be displayed in the search field.

To filter out data, open the **Filter** pane by clicking the  icon on the left.

Enable filtering by switching the **On/Off** toggle and define the filtering options:

- **Date**: filters data by date. Define the **From** and **Until** dates.
- **Source**: filters data by sources.
- **Device**: filters data by devices at which the data was synced with iCloud.
- **Type**: filters data by actual records and deleted ones.

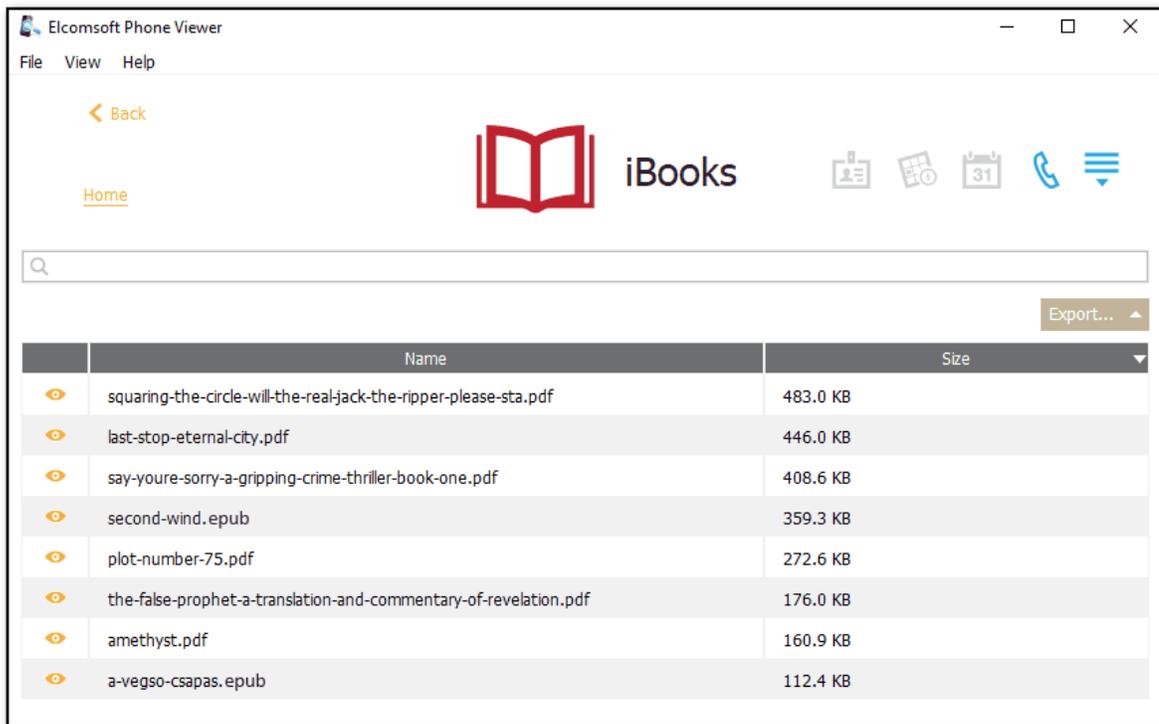
#### 4.4.9 iBooks

The **iBooks** plugin allows you to explore files from the iBooks application. It displays list of pdf and epub files downloaded by user manually.

*NOTE: This plugin is only available for iCloud synced data.*

In the grid, the following information is available:

- Name
- Size



### File viewing

To view a certain file, click **Show file** icon . The file opens in the default viewer (depends on the file format) on your machine.

### Searching

You can perform searches for files by name of a book and size.

To perform searches in iBooks, enter the necessary value in the search field and press **Enter**. The search results will be highlighted in yellow. The number of search results will be displayed in the search field.

### Exporting

To export iBooks data, do the following:

1. Click **Export**.
2. Select **All**.
3. The **Select destination file** window will open.
4. In the opened window, select the location in which the file with exported data will be saved and enter the file name.
5. Click **Save**.
6. The **<file name>.xlsx** file is saved in the selected location.

## 4.4.10 Keychain

This plugin allows you to explore the **Keychain** data such as Apple ID passwords, Wi-Fi passwords, mail account passwords, credit card information, etc.

*NOTE: This plugin is only available for iCloud synced data downloaded by EPB.*

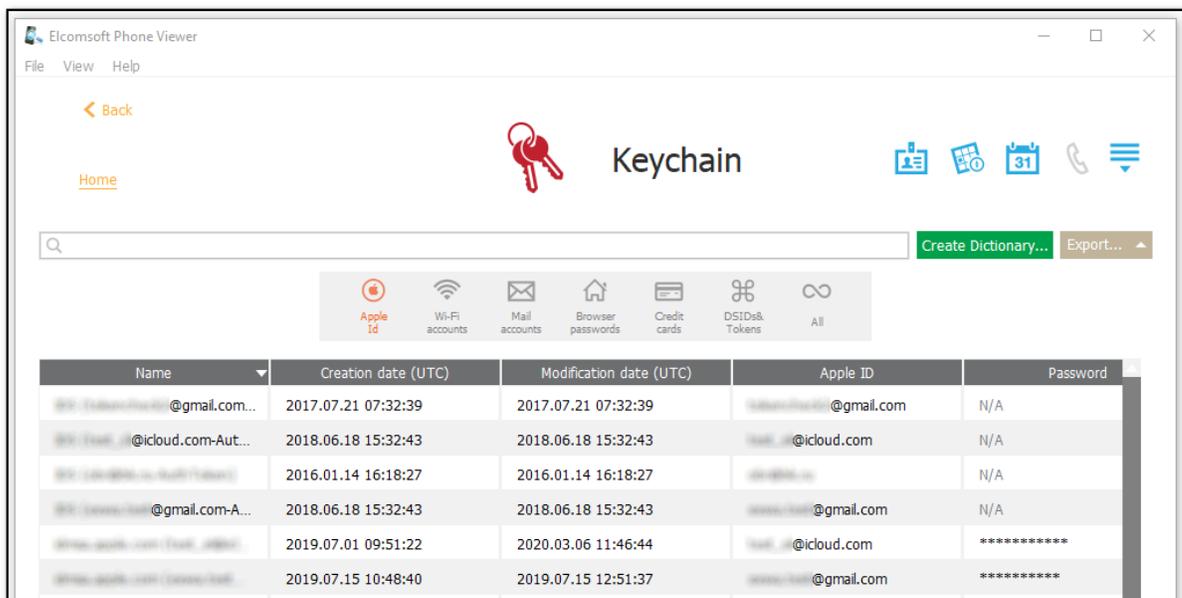
**NOTE:** To unmask passwords, card numbers, tokens and hash values, clear the **Mask Passwords in Keychain** option in the **Settings**.

The data in the **Keychain** plugin is divided into the following categories:

- **Apple Id:** information about Apple Ids
- **Wi-Fi accounts:** information about Wi-Fi accounts
- **Mail accounts:** information about the mail accounts
- **Browser passwords:** information about the web forms passwords
- **Credit cards:** information about the credit cards
- **DSIDs & Tokens:** information about destination signaling identifiers and tokens
- **All:** detailed information about all keychain data

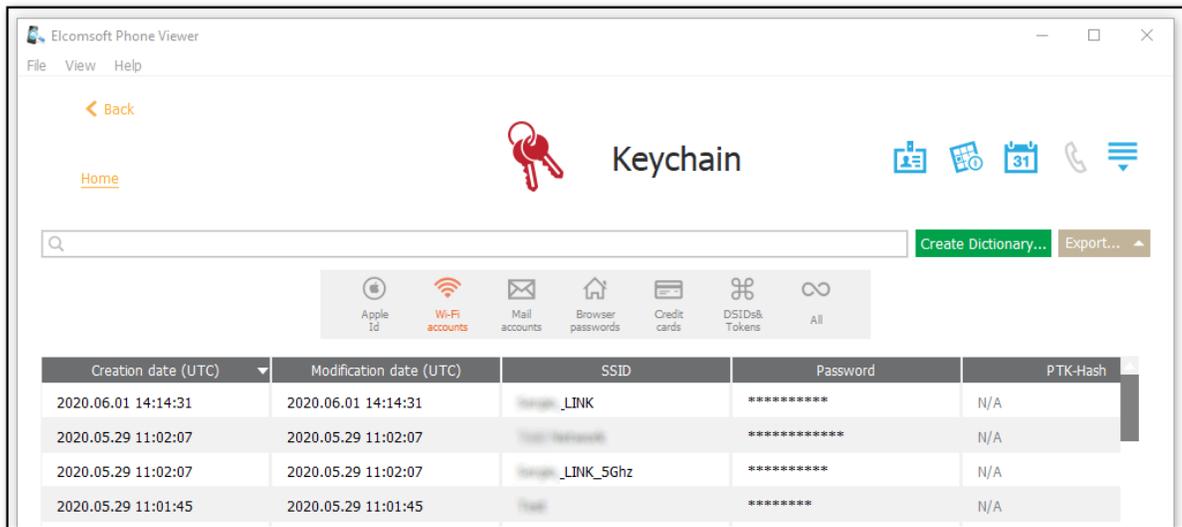
For **Apple Id**, the following is displayed:

- **Name**
- **Creation date (UTC):** date and time
- **Modification date (UTC):** date and time
- **Apple ID**
- **Password**



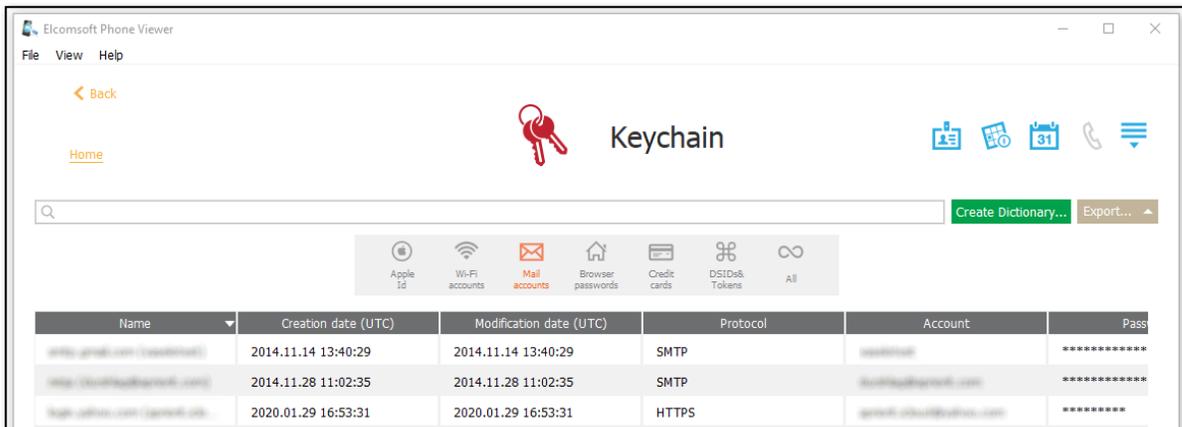
For **Wi-Fi accounts**, the following is displayed:

- **Creation date (UTC):** date and time
- **Modification date (UTC):** date and time
- **SSID**
- **Password**
- **PTK-Hash:** hash values



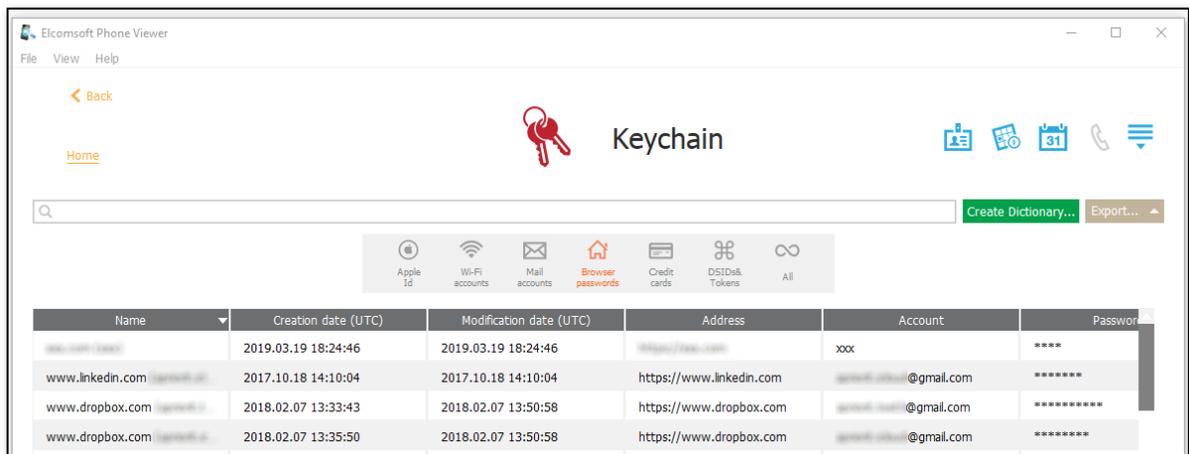
For **Mail accounts**, the following is displayed:

- **Name**
- **Creation date (UTC):** date and time
- **Modification date (UTC):** date and time
- **Protocol**
- **Account:** mail account name
- **Password**



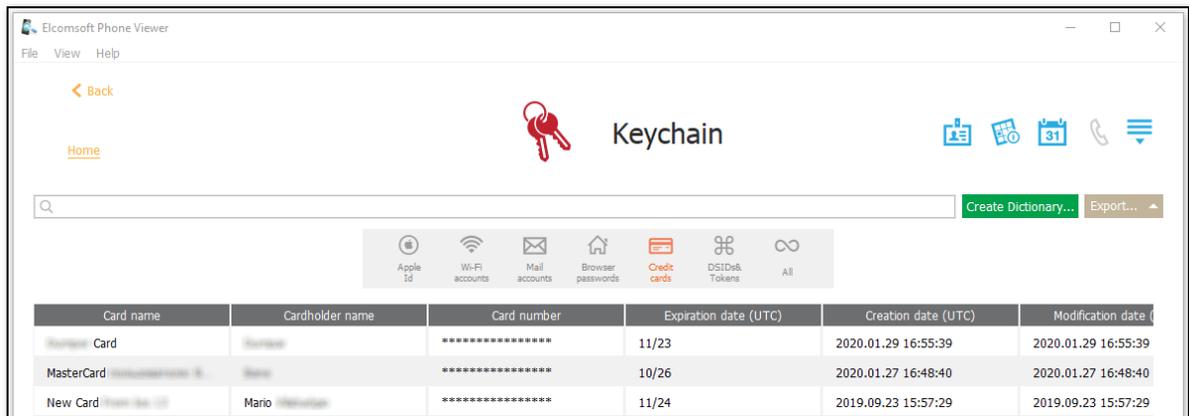
For **Browser passwords**, the following is displayed:

- **Name**
- **Creation date (UTC):** date and time
- **Modification date (UTC):** date and time
- **Address:** web address
- **Account**
- **Password**



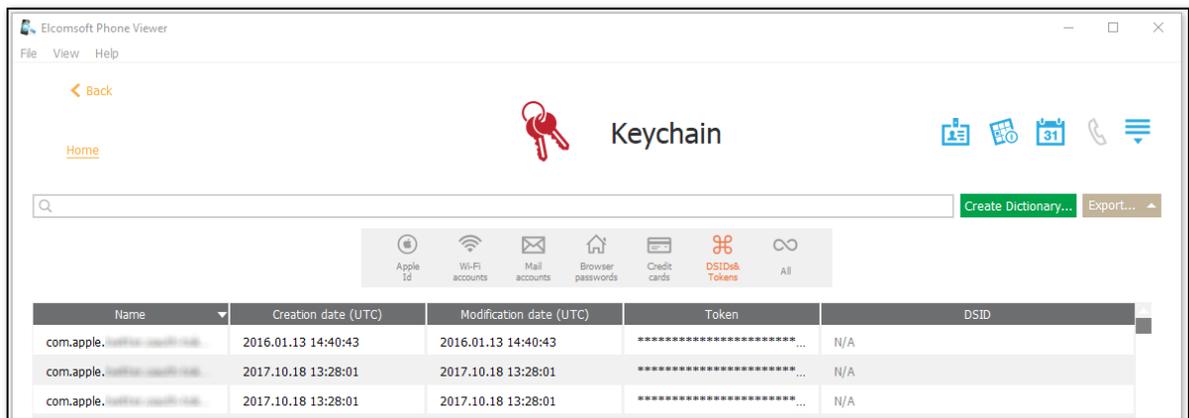
For **Credit cards**, the following is displayed:

- **Card name**
- **Cardholder name**
- **Card number**
- **Expiration date (UTC):** date
- **Creation date (UTC):** date and time
- **Modification date (UTC):** date and time



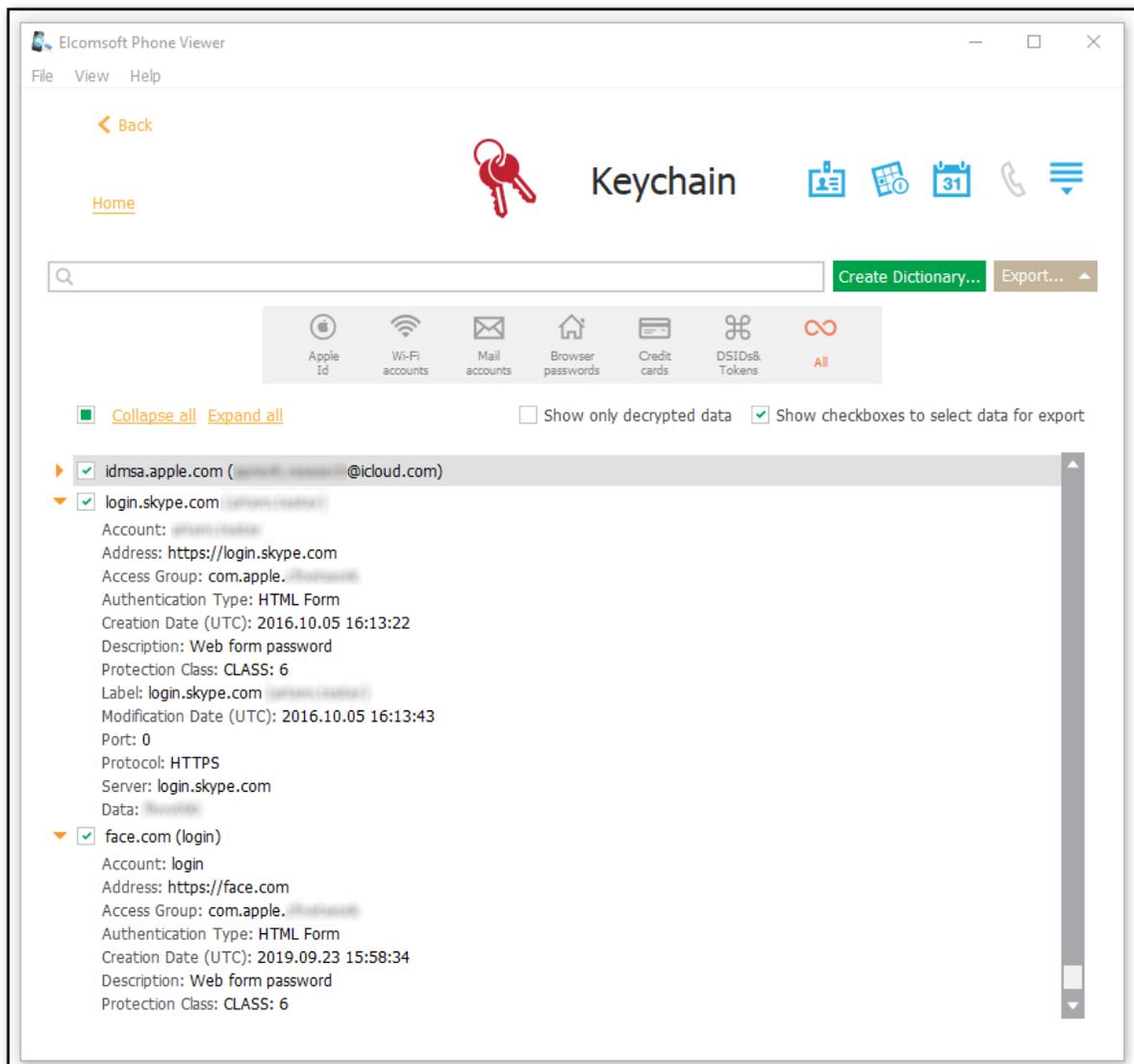
For **DSIDs & Tokens**, the following is displayed:

- **Name**
- **Creation date (UTC):** date and time
- **Modification date (UTC):** date and time
- **Token**
- **DSID**



The **All** category contains a list of all keychain data. For every list item (depending on its type), you can find the following information including, but not limited to:

- **Account**
- **Address**
- **Access Group**
- **Authentication Type**
- **Key Size in Bits**
- **Decryption**
- **Derivation**
- **Encryption**
- **Application label**
- **Label**
- **Permanence**
- **Digital Sign**
- **Unwrapping**
- **Wrapping**
- **Creation Date (UTC)**
- **Description**
- **Invisible**
- **Protection Class**
- **Modification Date (UTC)**
- **Path**
- **Port**
- **Protocol**
- **Server**
- **Data:** password



The following options are available in the **All** category:

- **Collapse all** allows collapsing the detailed information about all items in the list
- **Expand all** allows expanding the detailed information about all items in the list
- Click  to expand or collapse the detailed information about the certain item in the list
- **Show only decrypted data** option allows viewing the decrypted data only
- **Show checkboxes to select data for export** allows selecting the data for export.

### Creating Dictionary

**EPV** allows you to create a dictionary of the passwords found in the keychain.

To create a dictionary, do the following:

1. Click **Create Dictionary**.
2. The **Select destination file** window opens.
3. In the opened window, select the location to which the file with the passwords will be saved and enter the file name.
4. Click **Save**.
5. The **<file name>.txt** file is saved to the selected location.

### Exporting Keychain Data

To export data, do the following:

1. Click **Export**.
2. Select one of the following values from the drop-down list: **Selected** or **All**.
3. The **Select destination file** window opens.
4. In the opened window, select the location to which the file with exported data will be saved and enter the file name.
5. Click **Save**.
6. The **<file name>.xml** file is saved to the selected location.

### Searching

To perform searches in **Keychain**, enter the search request in the search field and press **Enter**. The search results will be highlighted in yellow. The number of search results will be displayed in the search field. Use the navigation arrows to navigate between the search results.

## 4.4.11 Locations (iOS)

This plugin displays the location data from iOS backups and iOS device images acquired via Elcomsoft iOS Forensic Toolkit.

When opening the Locations plugin, you might be asked to confirm whether you want to search for and display the Wi-Fi location data and locations for other media except for camera roll. Please note that the Internet connection is required to get the Wi-Fi location data for the first time.

After the Wi-Fi location data is downloaded, it is saved to local cache. You will not be able to open other plugins until the process is finished.

Click **Refresh** or reopen the plugin to update the information in the plugin. Defined filter settings will be cleared.

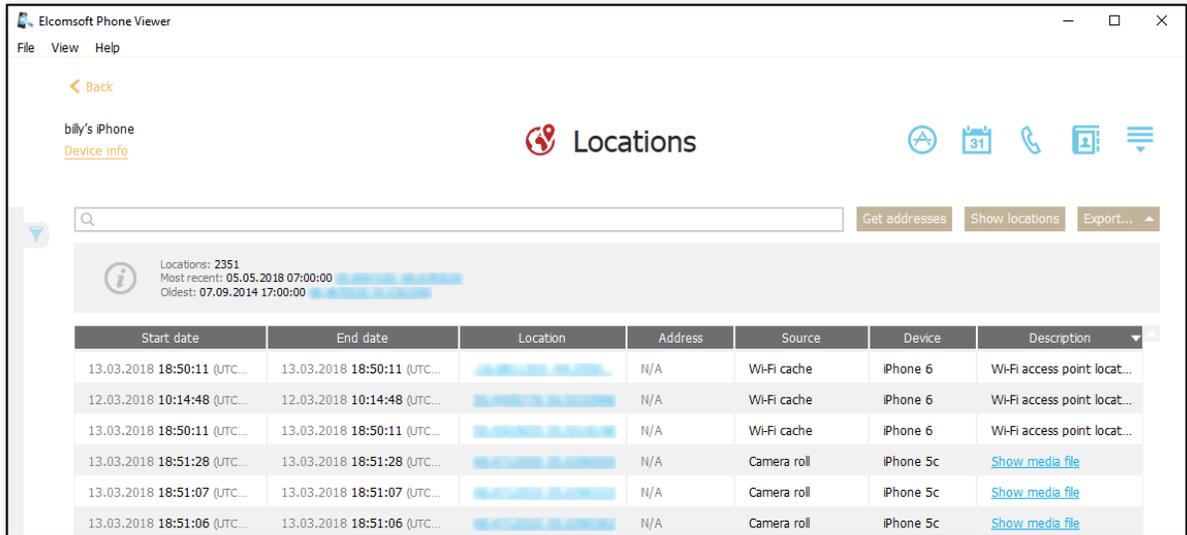
In the grid, you can see the following information:

- Start Date: Date and time the user entered the location
- End Date: Date and time the user left the location
- Location: Latitude and longitude of the location
- Address: Address of the location
- Source: Source of the location data
- Device
- Description: Additional information about the location (for example, a link to a media file or a calendar event)

*NOTE: For Other media and Camera roll locations, it is sometimes impossible to get the timezone. In such a case, the 'UTC unknown' value will be displayed in the Start date and the End date columns.*

The general information about locations is displayed above the grid:

- **Locations:** total number of locations
- **Most recent:** date and time the most recent location was created
- **Oldest:** date and time the oldest location was created



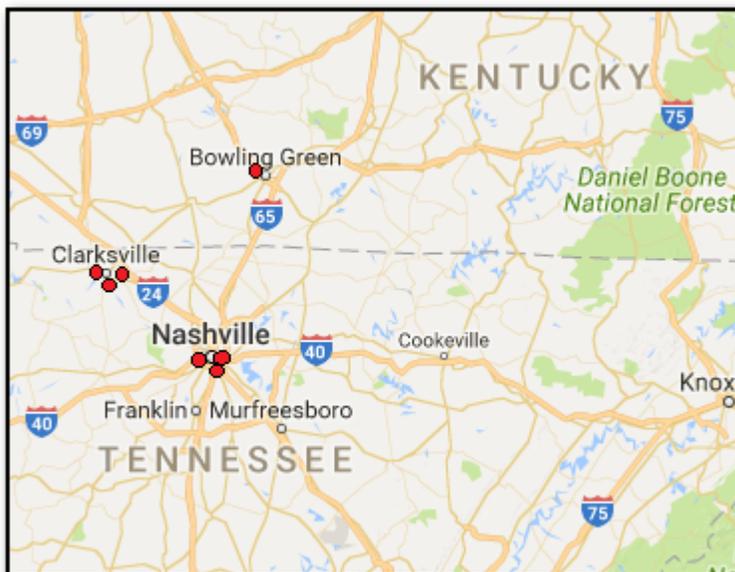
Start date	End date	Location	Address	Source	Device	Description
13.03.2018 18:50:11 (UTC...)	13.03.2018 18:50:11 (UTC...)	[REDACTED]	N/A	Wi-Fi cache	iPhone 6	Wi-Fi access point locat...
12.03.2018 10:14:48 (UTC...)	12.03.2018 10:14:48 (UTC...)	[REDACTED]	N/A	Wi-Fi cache	iPhone 6	Wi-Fi access point locat...
13.03.2018 18:50:11 (UTC...)	13.03.2018 18:50:11 (UTC...)	[REDACTED]	N/A	Wi-Fi cache	iPhone 6	Wi-Fi access point locat...
13.03.2018 18:51:28 (UTC...)	13.03.2018 18:51:28 (UTC...)	[REDACTED]	N/A	Camera roll	iPhone 5c	<a href="#">Show media file</a>
13.03.2018 18:51:07 (UTC...)	13.03.2018 18:51:07 (UTC...)	[REDACTED]	N/A	Camera roll	iPhone 5c	<a href="#">Show media file</a>
13.03.2018 18:51:06 (UTC...)	13.03.2018 18:51:06 (UTC...)	[REDACTED]	N/A	Camera roll	iPhone 5c	<a href="#">Show media file</a>

To view the addresses of the locations, do the following:

1. Click the **Get addresses** button.
2. If the confirmation message appears, click **Yes**.
3. Once the addresses for the locations are found, they are displayed in the **Address** column.

*NOTE: Internet connection is required to get the addresses.*

You can view the locations on a Google map by clicking the **Show locations** button. A Google map will open in your browser, displaying the locations marked with red points. Click a point to view its longitude, latitude, altitude, and time.



## Exporting

To export location data, do the following:

1. Click **Export**.
2. Select one of the following values from the drop-down list: **Filtered** or **All**.
3. The **Select destination file** window will open.
4. In the opened window, select the location in which the file with exported data will be saved, enter the file name and select the file extension (.kml or .xlsx).
5. Click **Save**.
6. The file is saved to the selected location.

## Searching and Filtering

To perform searches in **Locations**, enter the necessary value in the search field and press **Enter**. The search results will be highlighted in yellow.

To filter out locations, open the **Filter** pane by clicking the  icon on the left. Enable filtering by switching the **On/Off** toggle and define the filtering options:

- **Date:** Enter the desired dates into the **From** and **Until** fields.
- **Devices:** Select which device(s) you want to get location data from.
- **Sources:** Select the sources you want to get location data from. The following sources might be available:
  - For iOS backups and iOS device images:
    - Google Maps
    - Apple Maps
    - Camera roll
    - Other media
    - Calendar
    - Wi-Fi
    - Uber
  - For iOS device images only:
    - Base Station (GSM)
    - Base Station (LTE)
    - Base Station (CDMA)
    - Base Station (SCDMA)
    - Graph Service
    - Locations cache
    - Wi-Fi cache
    - Cache
    - Significant Location
    - Frequent Location

If you click **Show locations** after you filtered locations, only the filtered locations will be displayed on the Google map.

### 4.4.12 Locations (Microsoft)

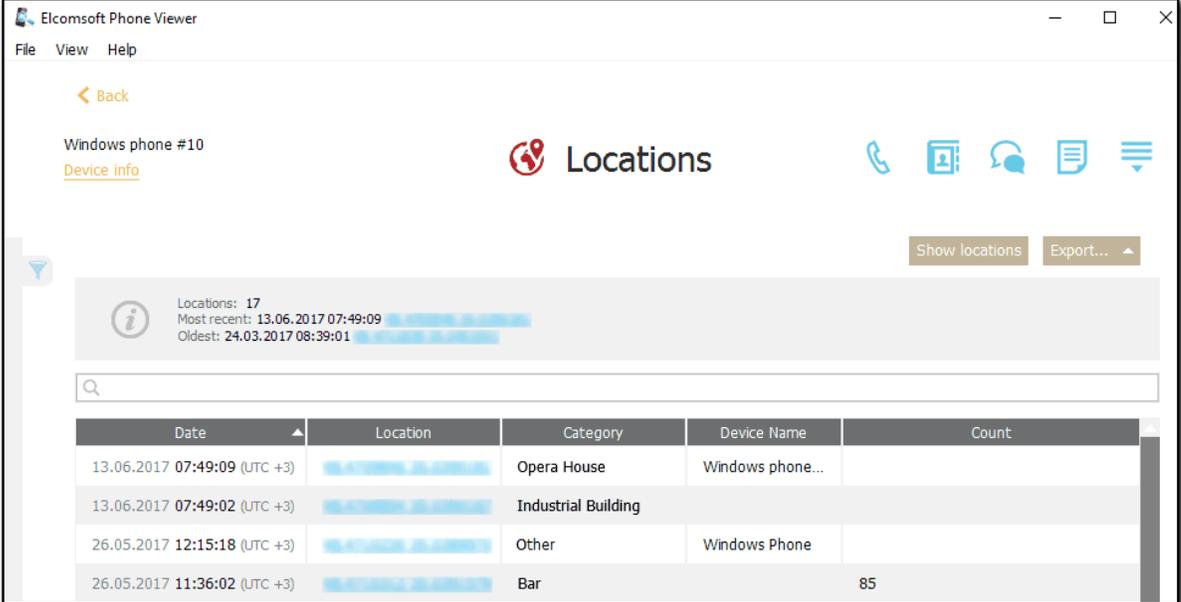
EPV allows you to view the Microsoft account user's location history downloaded from One Drive using Elcomsoft Phone Breaker.

You can find the following information:

- Date
- Location: Latitude and longitude of the location
- Category: Location category (e.g., bank, gym, etc.)
- Device Name
- Count: How many times the location was registered by the device

You can see information on the number of locations as well as on the most recent and the oldest locations.

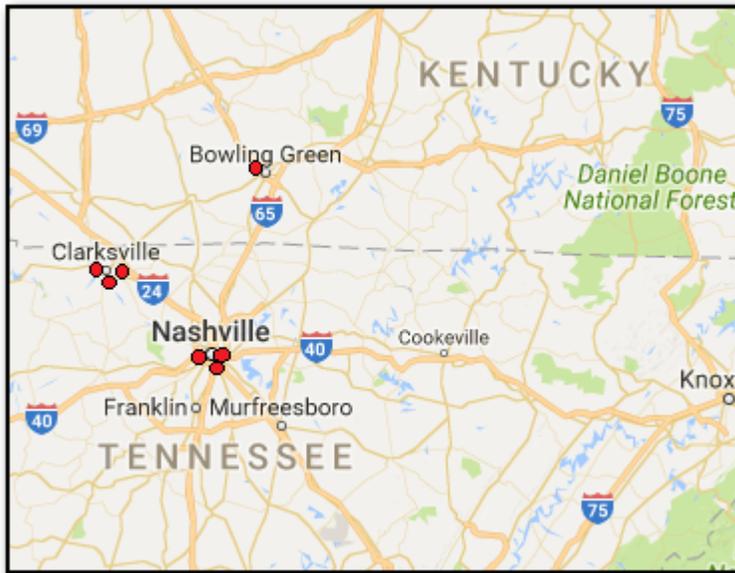
All locations are sorted by date, with the most recent one on top.



The screenshot shows the 'Locations' section of the Elcomsoft Phone Viewer application. The interface includes a 'Back' button, the device name 'Windows phone #10', and a 'Device info' link. A summary box displays 'Locations: 17', 'Most recent: 13.06.2017 07:49:09', and 'Oldest: 24.03.2017 08:39:01'. Below this is a search bar and a table of location records. The table has columns for Date, Location, Category, Device Name, and Count. The records are sorted by date in descending order.

Date	Location	Category	Device Name	Count
13.06.2017 07:49:09 (UTC +3)		Opera House	Windows phone...	
13.06.2017 07:49:02 (UTC +3)		Industrial Building		
26.05.2017 12:15:18 (UTC +3)		Other	Windows Phone	
26.05.2017 11:36:02 (UTC +3)		Bar		85

You can view the user's location history on a Google map by clicking the **Show locations** button. A Google map will open in your browser, displaying the user's locations marked with red points. Click a point to view its longitude, latitude, altitude, and time.



You can export information on locations to your computer by clicking the **Export** button. You can choose to export either all or all filtered locations. Please note that location data export for Windows Phone is only available in the registered version of the program.

### Searching and Filtering

To perform searches in **Locations**, enter the necessary value in the search field and press **Enter**. The search results will be highlighted in yellow.

To filter out locations, open the **Filter** pane by clicking the  icon on the right. Enable filtering by switching the **On/Off** toggle and define the filtering options:

- **Date:** Enter the desired dates into the **From** and **Until** fields.
- **Devices:** Select which device(s) you want to get location history from.

If you click **Show locations** after you filtered locations using either or both of the filters, only the filtered locations will be displayed on the Google map.

### 4.4.13 Media

This plugin displays all multimedia data from iOS and BlackBerry backups. You can also view the media sent by a certain contact in the [Messages](#) plugin.

*NOTE: When you open BlackBerry 10 backups, data will be extracted to the following folder: %appdata%\Elcomsoft Phone Viewer\Temp\Backup (if you didn't specify a different location in [Settings](#)). Please make sure you have enough space on disk C to store this data.*

General information about media files includes:

- Total number of files in the backup and the number of files displayed.
- The number of video, image, and audio files in backup and currently displayed. You can also view the size of all files in each category.

To export media objects, check them and click **Export**. It is possible to export checked media files, filtered files or all files.

The creation time of exported media files will be set to the current one, while the modification time is the same as on the device.

*Please note that if the timezone of the device is not detected, the time for all web data will be displayed in UTC time and the corresponding warning will be displayed in the Journal of the View menu.*

*NOTE: Exporting the media files and copying file properties are not allowed in the Trial version of EPV.*

### Viewing Media Files

To view a certain media file, click it in the grid. The file opens in the viewer where you can also view its properties:

- **Name:** The name of the file.
- **Type:** File type.
- **Dimensions:** The image size in pixels.
- **Size:** The size of the file in KB.
- **Modified:** Date and time the file was last modified.

*NOTE: For the WhatsApp data synced from another device, modified date can be displayed incorrectly.*

- **Folder:** The folder in the backup where the file is located.

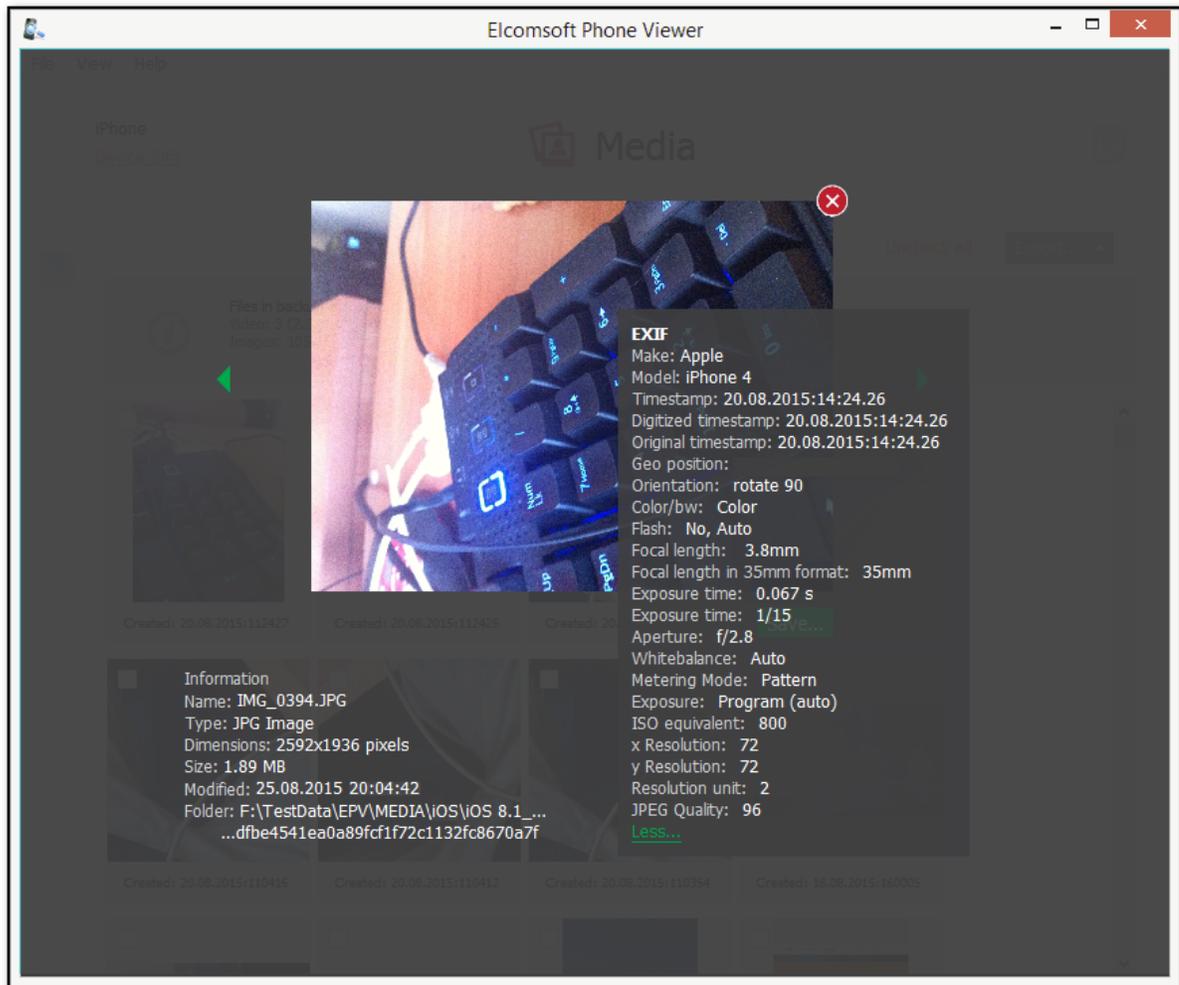
If the image has EXIF properties, they will be displayed in the EXIF properties section. It contains additional properties of the image made by digital camera or scanner.

*NOTE: In backups made for iPhone 7 and higher running iOS 11 and higher, there can be HEVC (video) and HEIF (image) files.*

*Files of such formats are created if the user turns on the High Efficiency setting in Settings > Camera > Formats.*

*HEIF image files can be viewed via means of EPV. HEVC video files can be viewed in EPV on Windows (if special codecs are installed) and on macOS 10.13 and higher.*

To save the file, click **Save** and select the destination location.



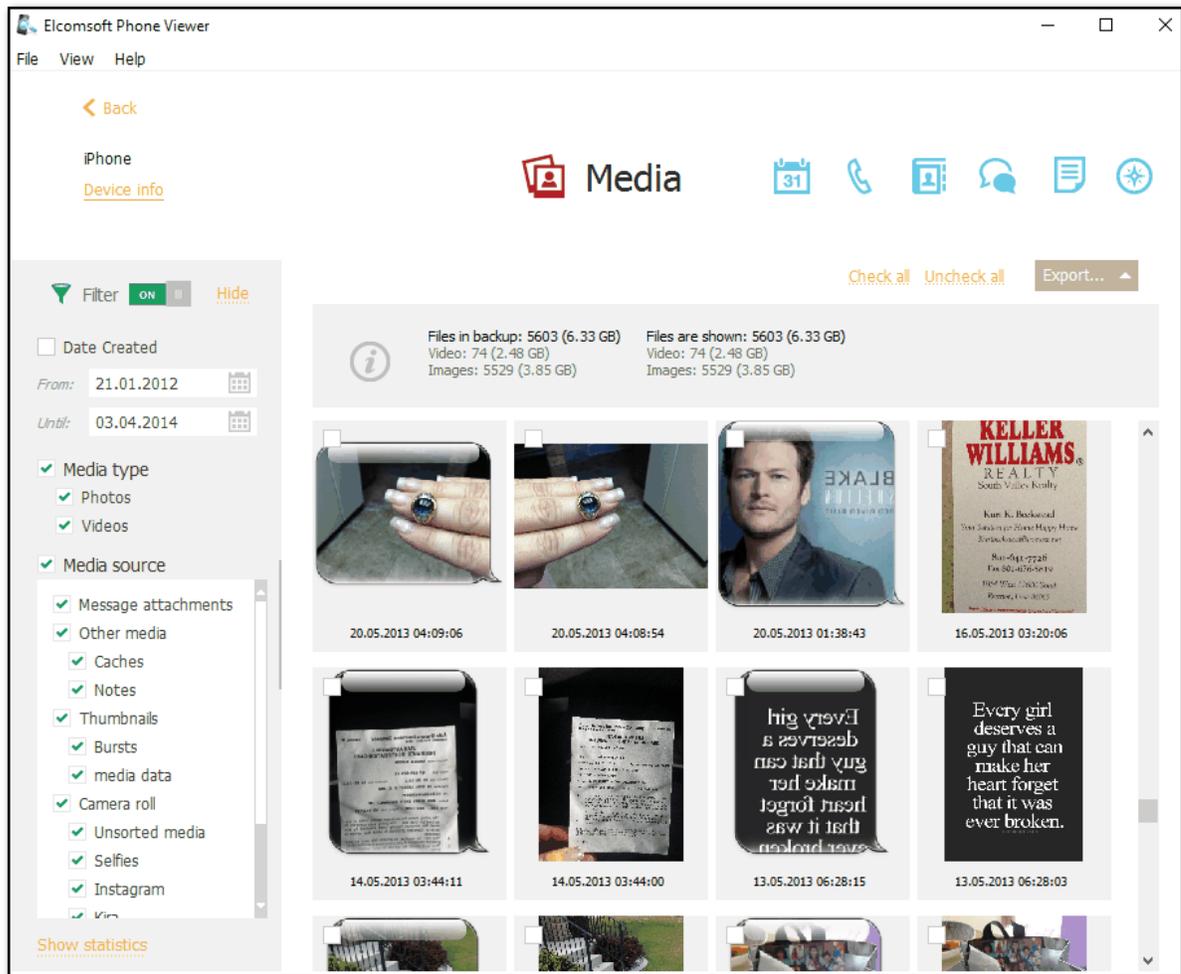
## Filtering

To filter out the media, open the **Filter** pane by clicking the  icon on the left.

*NOTE: Once you enable filtering, all previously checked files become unchecked.*

Enable filtering by switching the On/Off toggle and define the filtering options:

- **Date Created:** filters the media created within a specific time period. Select the **From** and **Until** dates in the corresponding drop-down lists.
- **Media Type:** filters the media by a media type (photo, video, and audio).
- **Media Source:** media contained in Camera roll, in message attachments, thumbnails and other sources. If you have selected to search for and display Camera roll media only on adding the backup, **Other media** will be disabled.
- **Albums:** filters media by albums stored on the device. The names of albums are displayed below the **Camera roll**, **Thumbnails**, and **Other media** filters.



If you clear any check box for Media Type, Media Source, or Albums, a negative number will be displayed next to the filter category. This number indicates the number of files that are currently not displayed.



#### 4.4.14 Messages

This plugin allows you to explore the user's message history.

Left pane of the window shows the contacts (phone number, name, or email -- depends on the conversation type) any conversation has ever been made with.

You can view the following types of messages for each contact:

Message Type	iOS Backups/Dev	iCloud Synced	BlackBerry Device	Microsoft Account	Comments
--------------	-----------------	---------------	-------------------	-------------------	----------

	ice Images	Data	Backups	Data	
SMS	Yes	Yes	Yes	Yes	
MMS	Yes	Yes	Yes	-	
iMessages	Yes	Yes	-	-	
Handwriting	Yes	-	-	-	Only for iOS 10 and higher devices.
Digital Touch	Yes	-	-	-	Only for iOS 10 and higher devices.
Reactions	Yes	-	-	-	Only for iOS 10 and higher devices.
Effects	Yes	-	-	-	Only for iOS 10 and higher devices.
Stickers	Yes	Yes	-	-	Only for iOS 10 and higher devices.

Incoming messages are shown on the left and outgoing messages are shown on the right. The number of messages for every contact is shown (in brackets). You can also view the group chats.

The emoji are displayed in both message texts and contacts (they are supported for other plugins as well).

For iOS devices, SMS are shown in green color, MMS are shown in gray, and iMessages are shown in blue.

### Viewing Attachments

For iOS and BlackBerry backups, as well as iCloud synced data, you can also view the message attachments of the following types:

- iOS backups and iCloud synced data: pictures, audio, videos, and Google Maps locations, files, and contacts.
- BlackBerry backups: pictures, audio, videos, Google Maps locations, appointments, files, and contacts.

*NOTE: In backups made for iPhone 7 and higher running iOS 11 and higher, there can be HEVC (video) and HEIF (image) files.*

*Files of such formats are created if the user turns on the High Efficiency setting in Settings > Camera > Formats.*

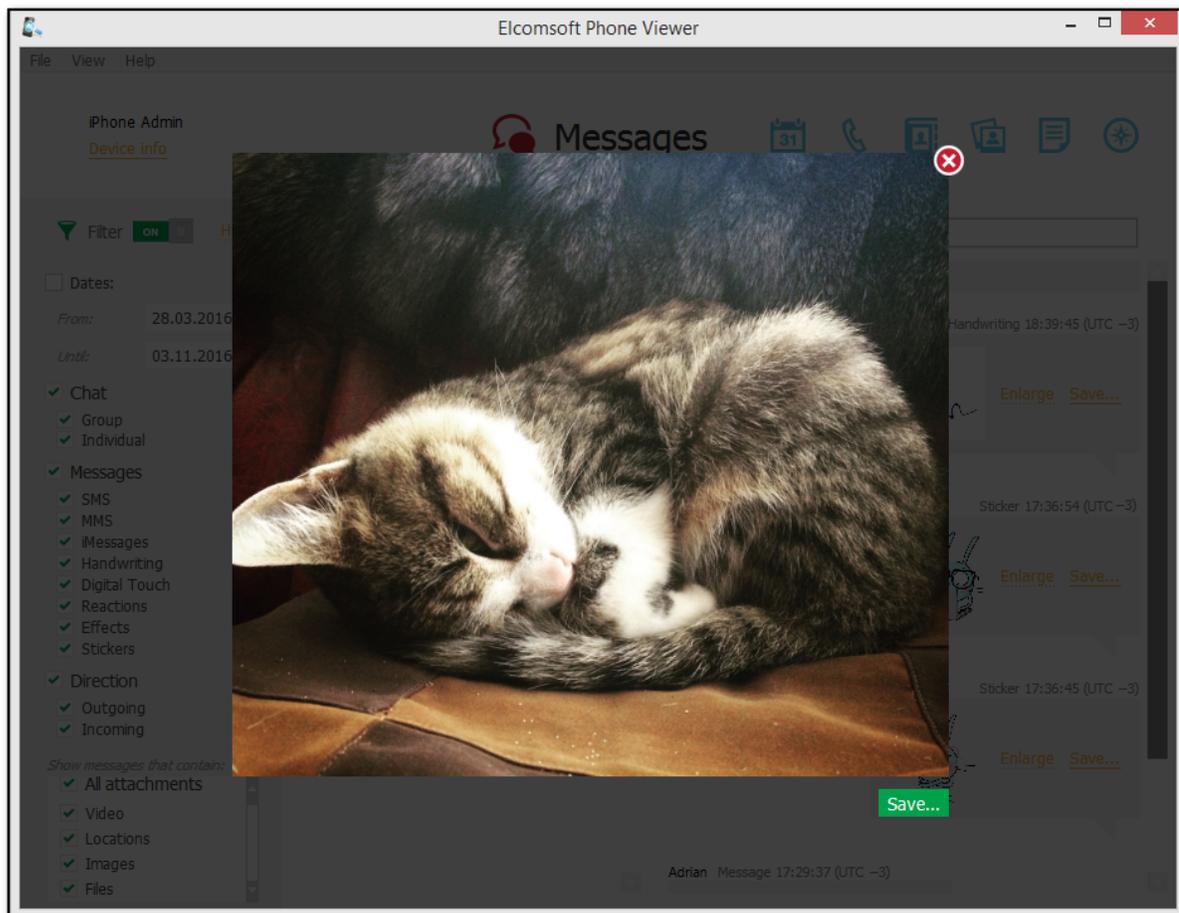
*HEIF image files can be viewed via means of EPV. HEVC video files can be viewed in EPV on Windows (if special codecs are installed) and on macOS 10.13 and higher.*

To save the attachments to your computer, click **Save** next to the selected attachment, define the destination folder in the opened window, and then click **Save**.

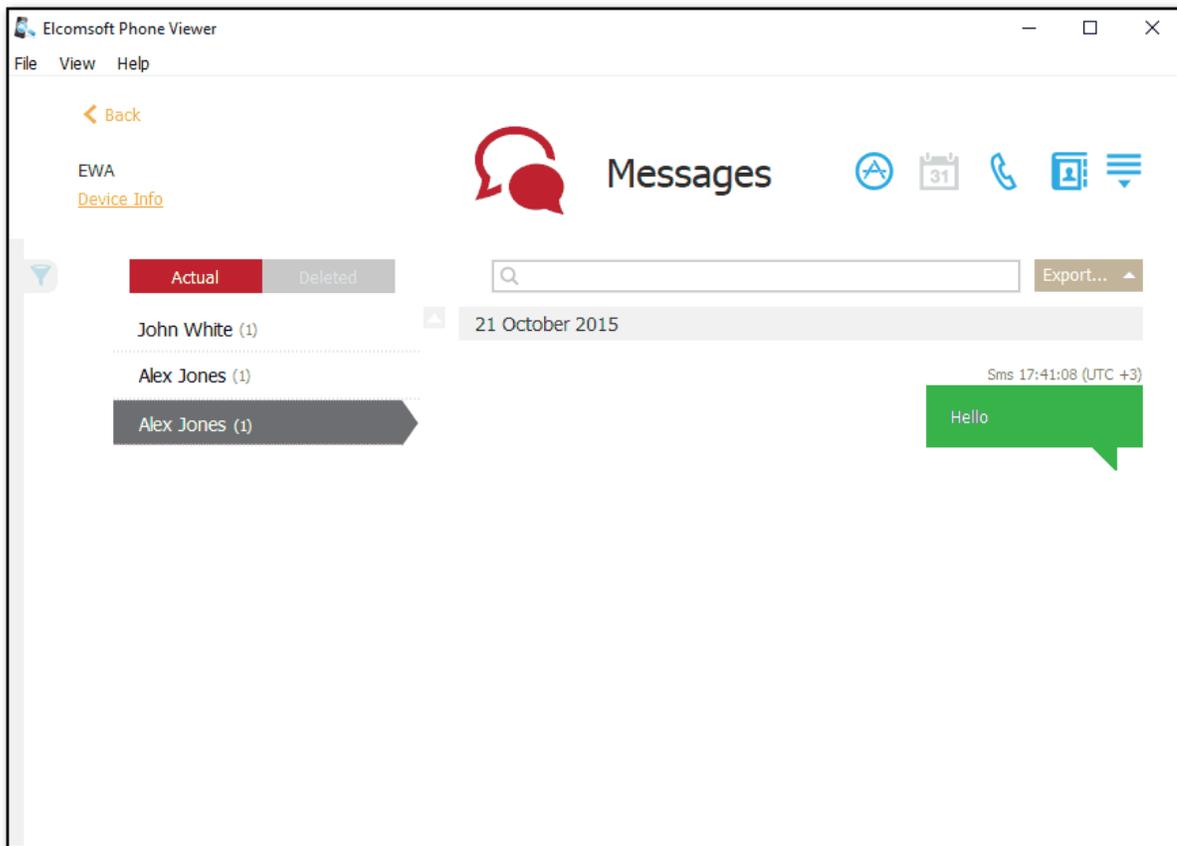
*Please note that for BlackBerry and iOS devices the time is stated as it is (was) set on the device; for Windows Phone – the time is the same as on the local PC (the actual time zone of the device is not available).*

*If the timezone of the device is not detected for BlackBerry and iOS devices, the time will be displayed in UTC time and the corresponding warning will be displayed in the Journal of the View menu.*

*Note that the timezone is shown correctly for full iCloud backups but might be also shown always in UTC if only selected categories have been downloaded.*



For iOS backups and iOS device images, you can also switch between *Actual* and *Deleted* messages. Recovery of deleted messages may take some time (the first time when you select *Deleted*). Unfortunately, not all deleted messages can be recovered. In addition, not all contacts for messages can be recovered. Such messages are placed in the *Unknown* chat. Date/time is also not available in many cases, and message contents may look corrupted.



## Exporting

To export messages, do the following:

1. Click **Export**.
2. Select one of the following values from the drop-down list: **Filtered** or **All**.
3. The **Select destination file** window will open.
4. In the opened window, select the location in which the file with exported messages will be saved and enter the file name.
5. Click **Save**.
6. The **<file name>.xlsx** file is saved in the selected location.

## Searching and Filtering

To perform searches in **Messages**, enter the search request in the search field and press **Enter**. The search results will be highlighted in yellow.

To filter out the messages, open the **Filter** pane by clicking the  icon on the left.

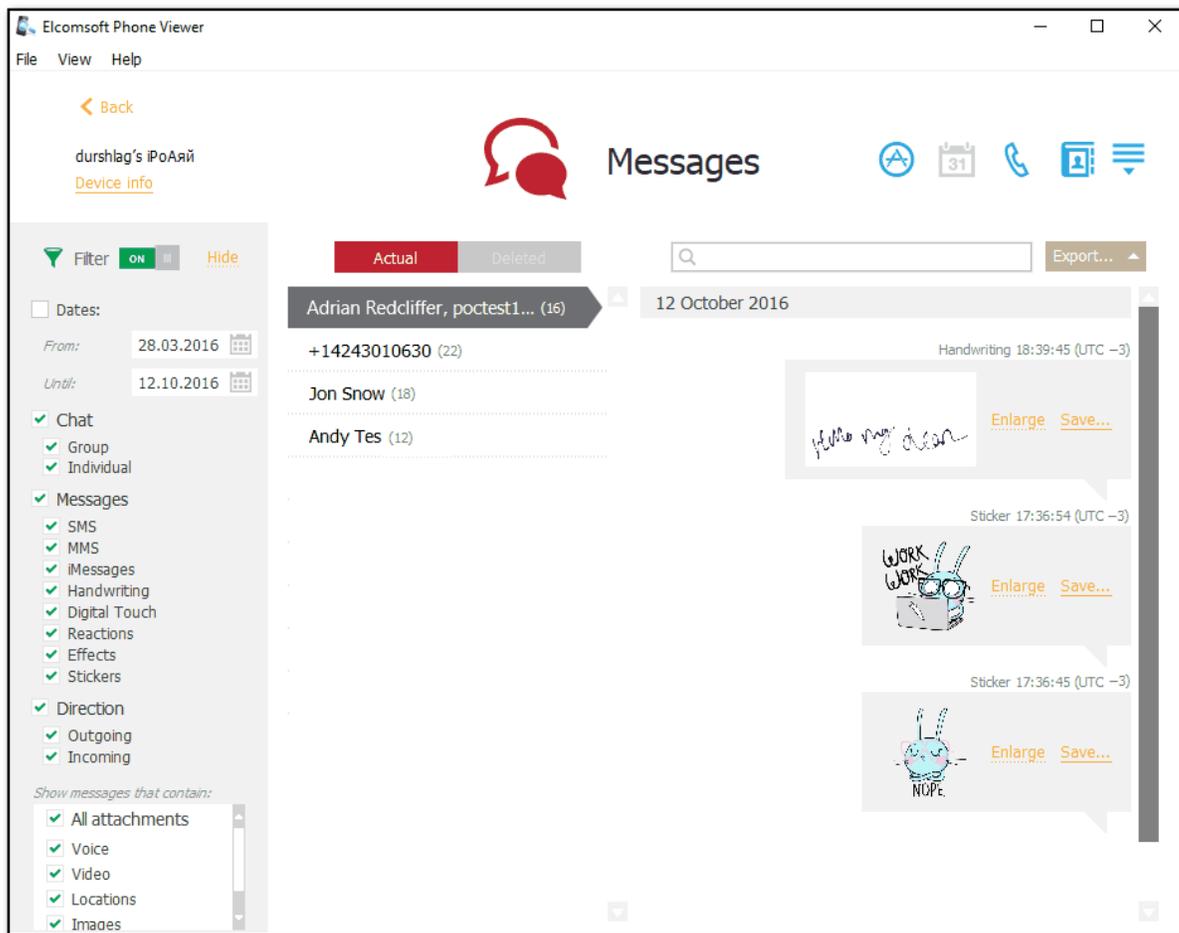
Enable filtering by switching the On/Off toggle, and define the filtering options:

- **Date:** filters messages by date. Define the **From** and **Until** dates.
- **Chat:** filters messages by chat.
- Select the **SMS**, **MMS**, **iMessages**, **Handwriting**, **Digital Touch**, **Reactions**, **Effects**, or **Stickers** check boxes to filter messages by their types.

- Define whether you need the **Incoming** or **Outgoing** messages.
- **All Attachments/Voice/Audio/Video/Locations/Contacts/Images/Files/Appointments**: filters messages by the attachment type.

*NOTE: When using filter options, you will be able to view only the records allowed by your license type.*

To copy the whole message, right-click on it and select **Copy message**. To copy a part of the message, click the area where the text is to be copied from, highlight the text, right-click and select **Copy** or **Select All**.



#### 4.4.15 Notes

For all notes extracted from backup, the program shows the date/time the note was created and last updated, the folder it is stored in, and the first two lines of the message text. Notes are sorted by the date they were last modified.

*Please note that for BlackBerry and iOS devices the time is stated as it is (was) set on the device; for Windows Phone, the time is the same as on the local PC (the actual time zone of the device is not available).*

*If the timezone of the device is not detected for BlackBerry and iOS devices, the time will be displayed in UTC time and the corresponding warning will be displayed in the Journal of the View menu.*

*Note that the timezone is shown correctly for full iCloud backups but might be also shown always in UTC if only selected categories have been downloaded.*

EPV also allows viewing deleted notes in iCloud Synced data downloaded using Elcomsoft Phone Breaker. Deleted notes are marked with a red trash can icon and can belong to the following folders:

- **Recently Deleted:** A system folder that contains notes deleted by the user.
- **Recovered:** A folder that contains notes deleted from the Recently Deleted folder on the device and recovered by EPV.

Each note has an info bar that shows the following information:

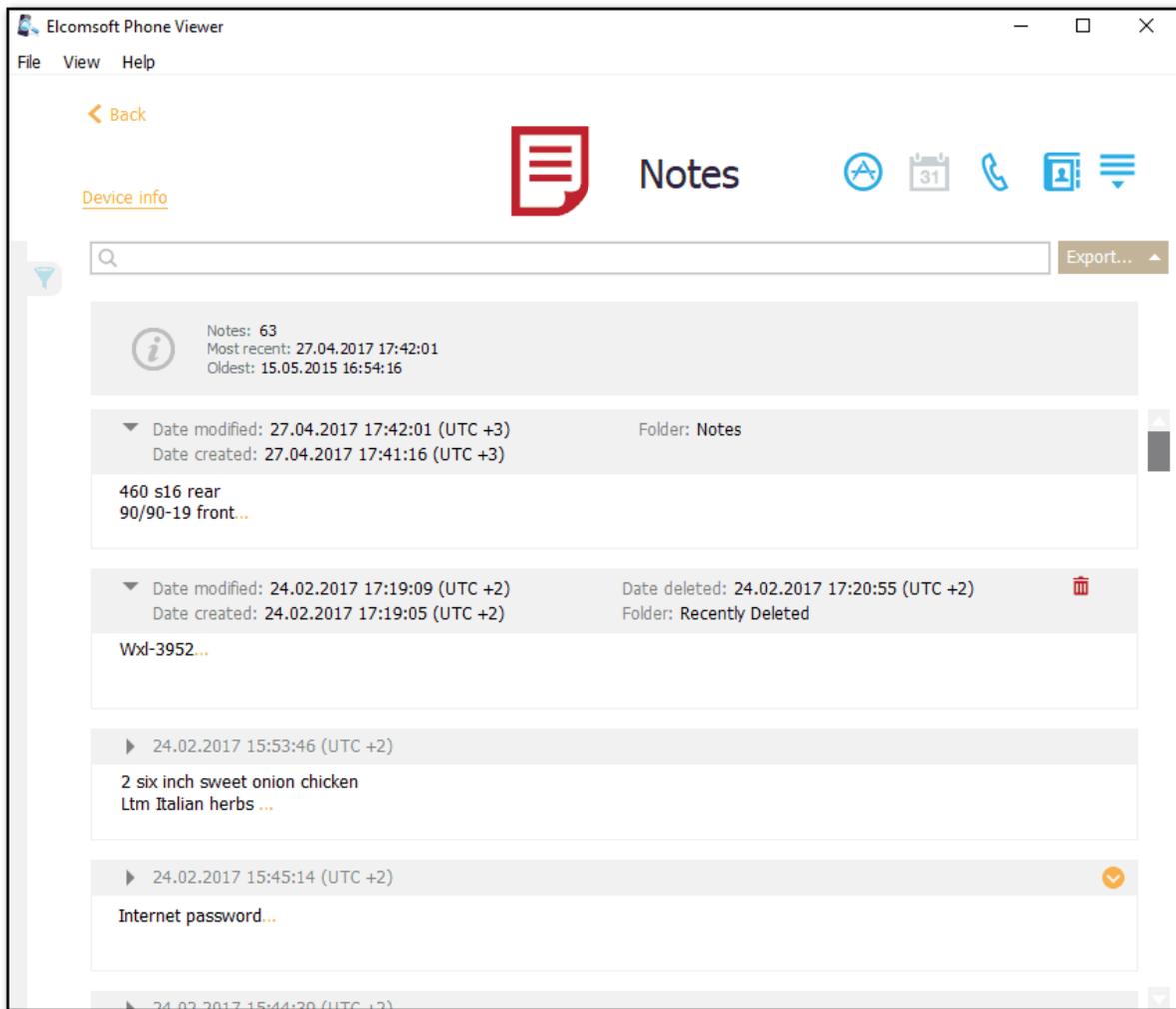
- **Date modified**
- **Date created**
- **Folder:** System or user folder a note belongs to.
- **Date deleted:** Date when a note was moved to the Recently Deleted folder or removed from this folder.
- **Attachment:** Notes with attachments are marked with the  icon. (For more information, please find **Viewing Attachments** below.)
- **Number of attached images:** Number of attached images. (For more information, please find **Viewing Attachments** below.)

*NOTE: If the user deleted a note via the website, the **Date deleted** value might not be correct. However, it is always correct for notes deleted via the phone.*

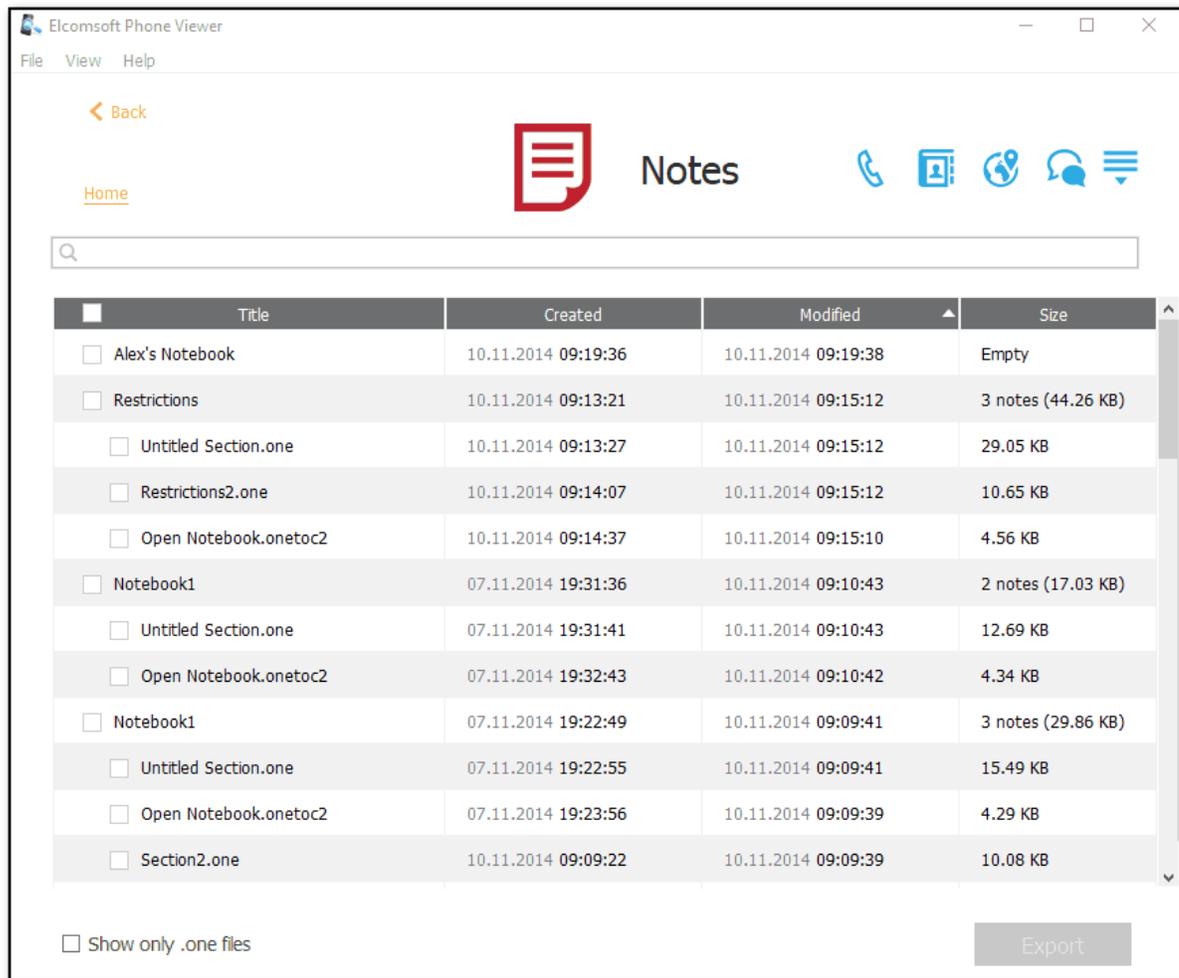
Click the gray arrow icon at the top-left corner of the note to view the info bar.

Click the orange arrow icon at the top-right corner of the note to expand the full note text.

*NOTE: Text formatting and tables are not supported in the current version of EPV. The note content is displayed as plain text.*



For notes extracted from Windows Phone backups, the actual notes content is not shown, but just the *notebook* name, with the file names (usually there are at least two files for every note: table of contents and the note itself). You can select the notes and/or the whole notebooks and press Export to save them as [Microsoft OneNote](#) files for further review.



## Viewing Attachments

EPV allows you to view images and other types of files embedded in notes. The following types of attachments are supported:

- **For notes in all types of backups:** Images
- **For notes in iCloud Synced data downloaded using Elcomsoft Phone Breaker:** Images, documents, video, audio, and other types of files.
- **For notes in iOS backups:** Images, documents, video, audio, and other types of files that were added to the note (but not created within the note).

*NOTE 1: Scanned documents, drawings, and taken photos are not supported in the current version of EPV.*

*NOTE 2: In backups made for iPhone 7 and higher running iOS 11 and higher, there can be HEVC (video) and HEIF (image) files.*

*Files of such formats are created if the user turns on the High Efficiency setting in Settings > Camera > Formats.*

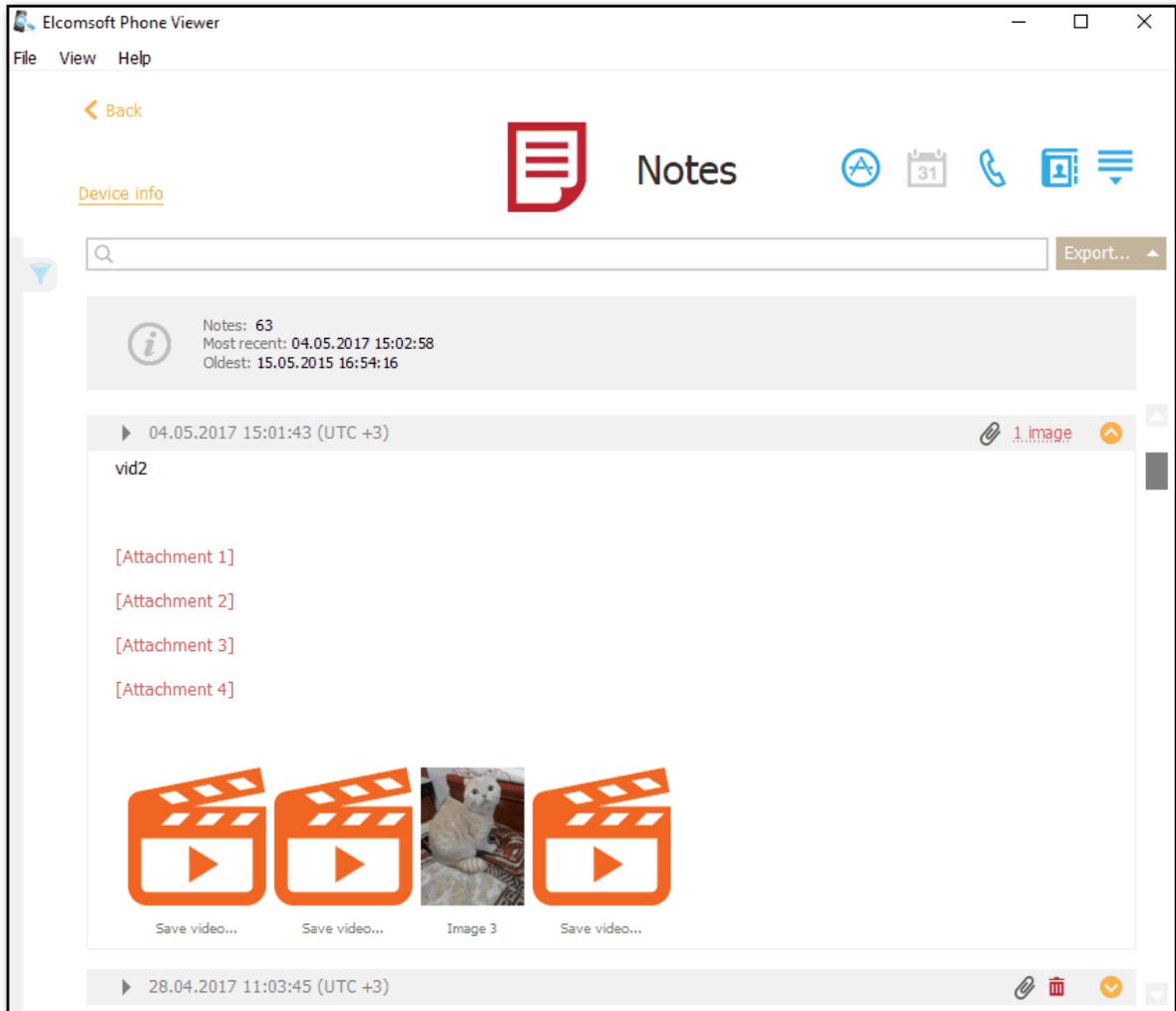
*HEIF image files can be viewed via means of EPV. HEVC video files can be viewed in EPV on Windows (if special codecs are installed) and on macOS 10.13 and higher.*

Notes with attachments are marked with the [Attachment] link in the note body and the  icon on the info bar. For notes with graphic attachments, the info bar also shows the number of attached images. To see thumbnails of attached images, expand the note body by clicking the orange arrow icon on the info bar.

To see a full-sized attached image, click its thumbnail or the Image link on the info bar.

To save an image to your computer, click **Save** in the image preview mode.

You can also save any types of attached files to your computer by clicking the [Attachment] link or the attached file icon in the note body.



## Exporting

To export notes, do the following:

1. Click **Export**.
2. Select one of the following values from the drop-down list: **Filtered** or **All**.
3. The **Select destination file** window will open.
4. In the opened window, select the location in which the file with exported notes will be saved and enter the file name.
5. Click **Save**.

6. The <file name>.xlsx file is saved in the selected location.

### Searching and Filtering

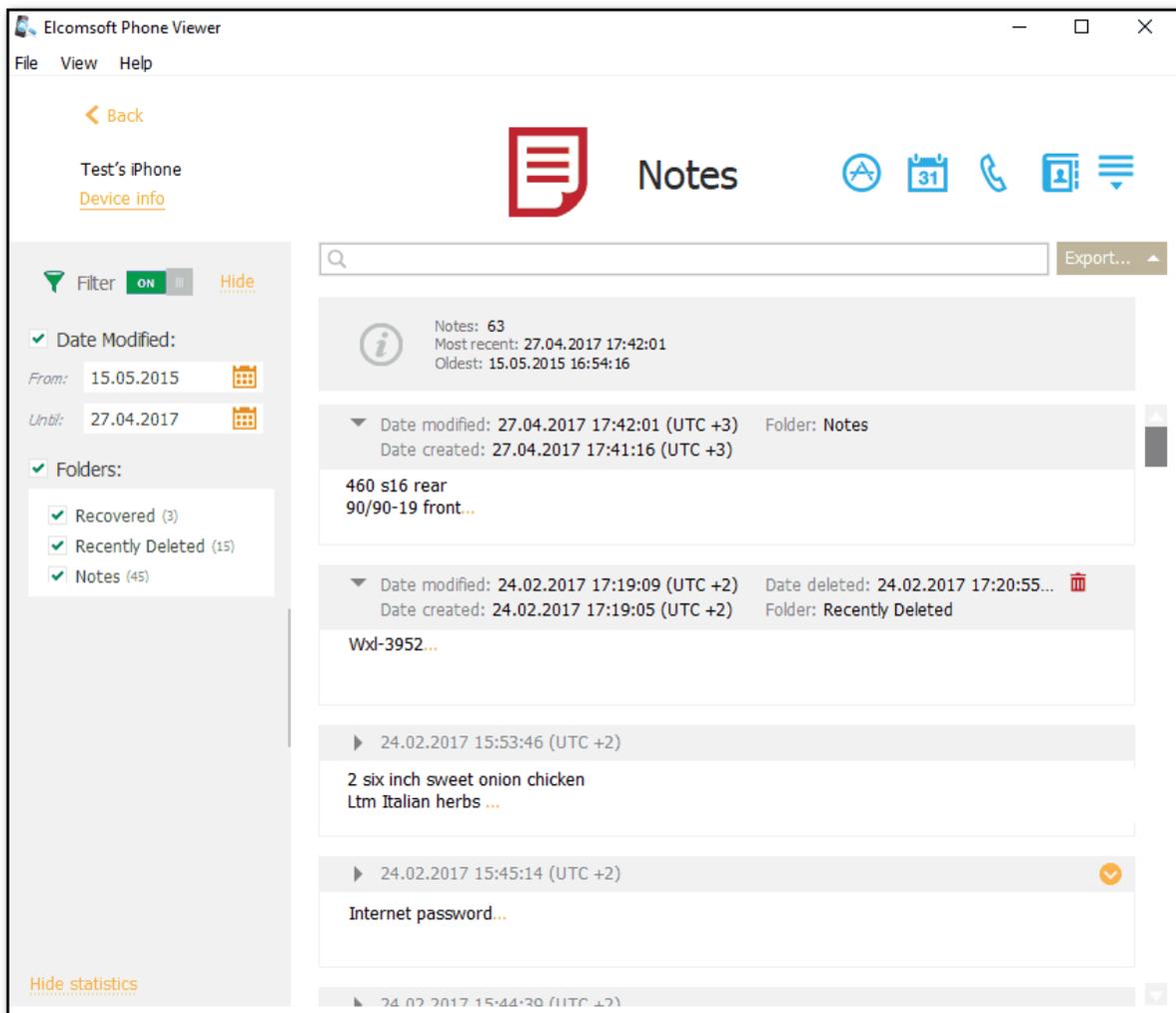
To perform searches in the **Notes**, enter the search request in the search field and press **Enter**. The search results will be highlighted in yellow.

To filter out notes, open the **Filter** pane by clicking the  icon on the left.

Enable filtering by switching the On/Off toggle, and define the filtering options:

- **Date:** filters messages by date. Define the **From** and **Until** dates.
- **Folder:** filters messages by folder. This filter is available only for notes in iCloud Synced data.

*NOTE: When using filter options, you will be able to view only the records allowed by your license type.*



#### 4.4.16 Photos

This plugin allows you to view media files downloaded from iCloud using the **Elcomsoft Phone Breaker** program.

*NOTE: This plugin is only available for iCloud synced data.*

The following general information about the media files is available:

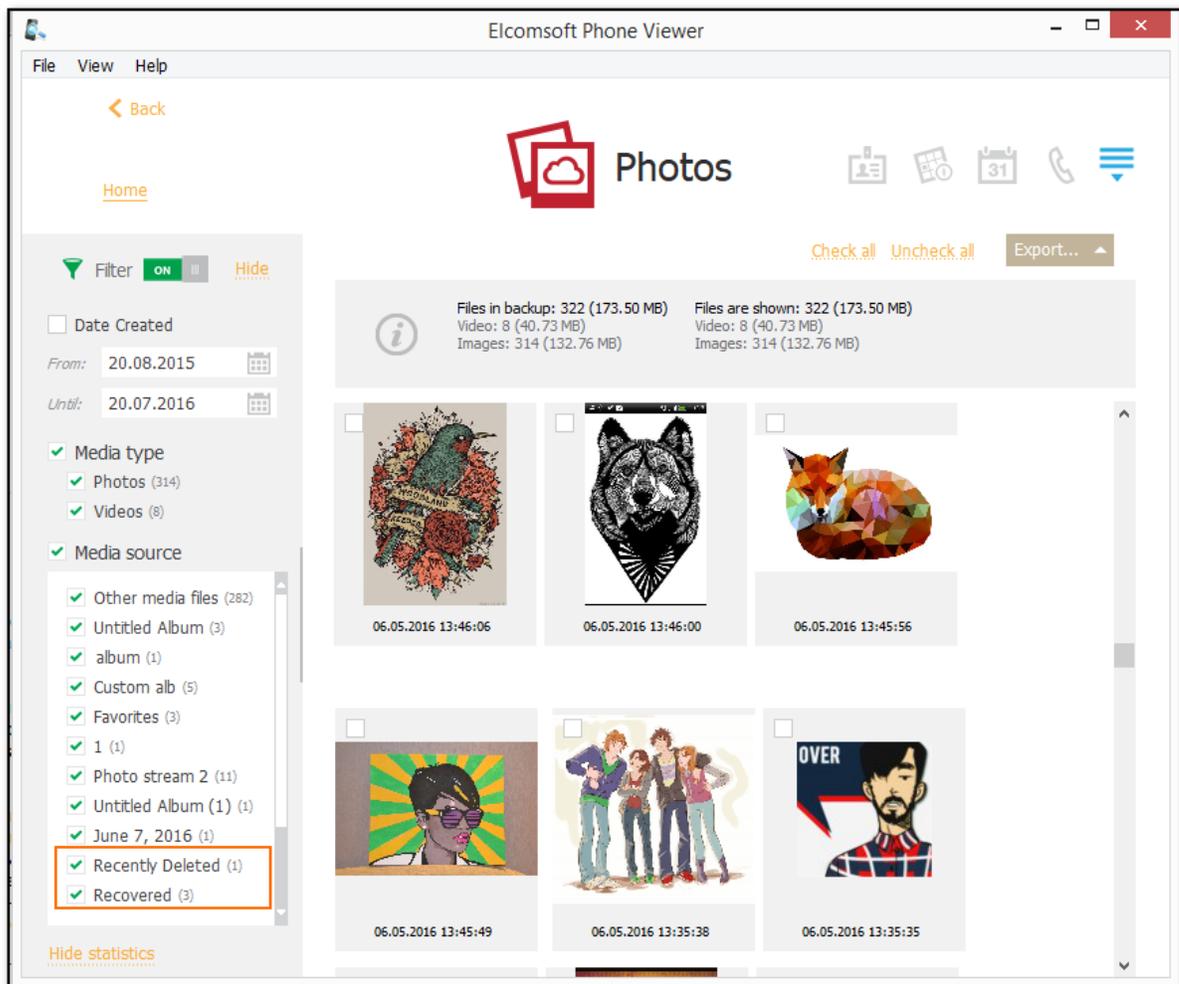
- Total number of files in the backup and the number of files shown
- The number of video and image files in the backup and currently shown. You can also view the size of all files in each category.

The most recent files are displayed on top of the grid. The date and time of each file corresponds to the date and time of the last file modification in iCloud.

To export media files, check them and click **Export**. It is possible to export checked media files, filtered files or all files.

**EPV** also allows you a unique capability to view all deleted files, which are loaded with the use of **two different Media source** filters:

- **Recently Deleted.** It filters the files which have been deleted from the device but can still be viewed in iCloud and in the corresponding folder on the device.
- **Recovered.** It filters the files which have been deleted from the device but can no longer be viewed on the device nor in iCloud, only in EPV.



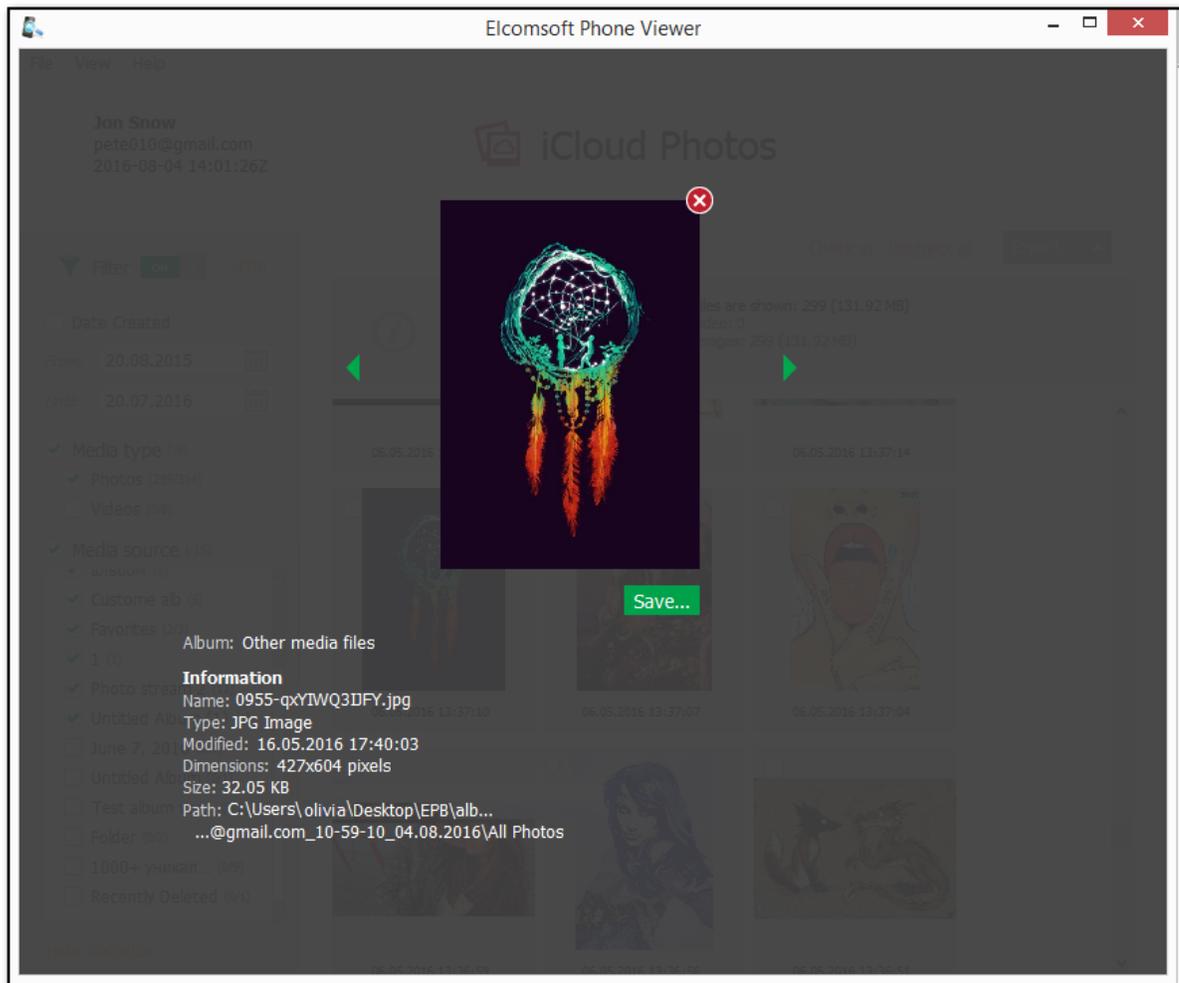
### Viewing Media Files

To view a certain media file, click it in the grid. The file opens in the viewer where you can also view its properties:

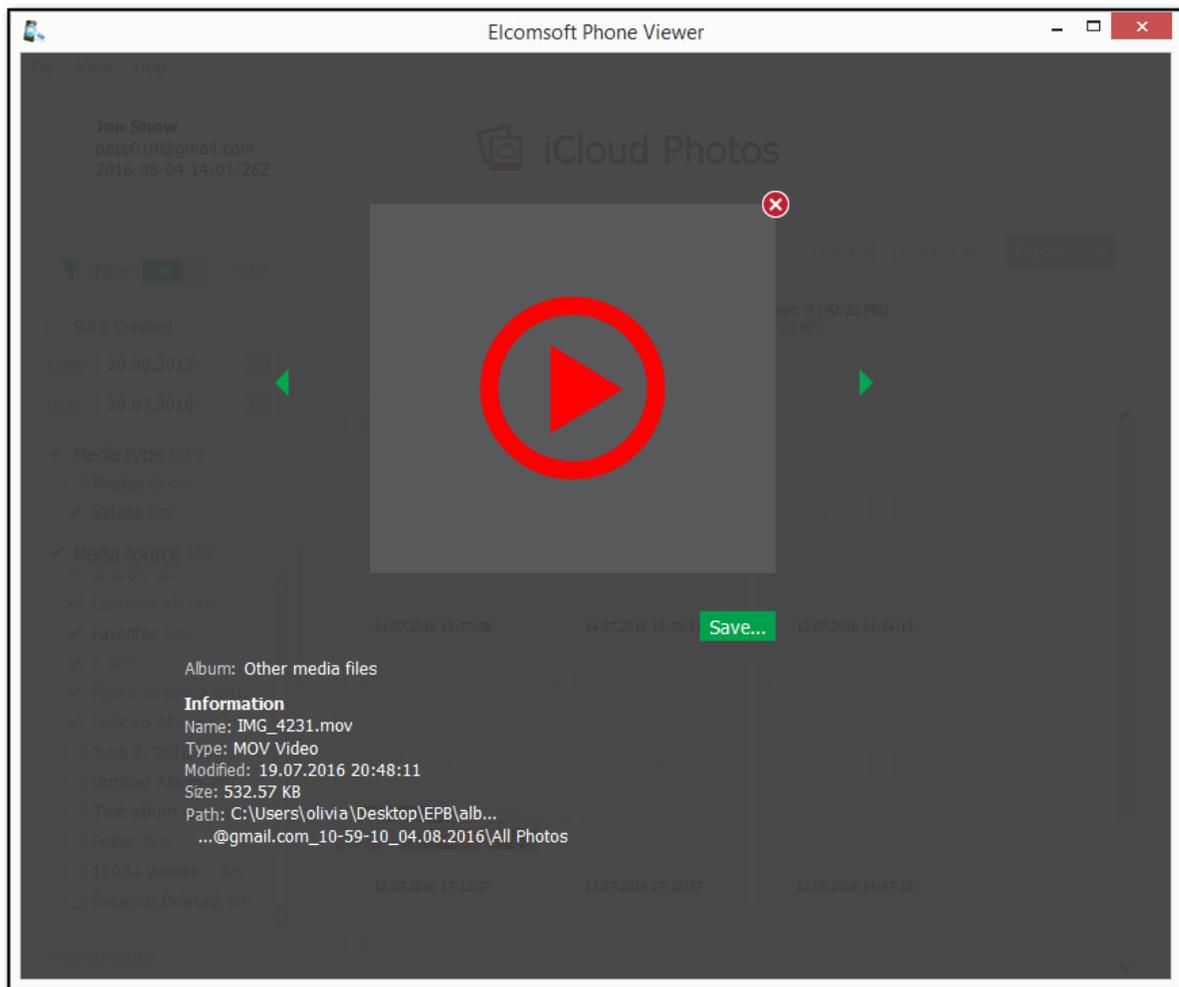
- **Album:** The album in which the file is stored in iCloud.
- **Name:** The original name of the file in iCloud.
- **Type:** File type.
- **Created:** The date and time the file was created in iCloud.
- **Modified:** The date and time the file was last modified in iCloud.
- **Deleted:** The date and time the file was deleted from iCloud.
- **Dimensions:** The image size in pixels.
- **Size:** The size of the file in KB.
- **Path:** The full path to the file in the filesystem.
- **Description:** Description of the file (if any).
- **Keyword:** Keyword of the file (if any).

If the image has EXIF properties, they will be displayed in the EXIF properties section. It contains additional properties of the image made by digital camera or scanner.

To save the file, click **Save** and select the destination location.



To view a video file, click it in the grid, and then click the **Play** icon. The video file will open in the player installed on your computer.



## Filtering

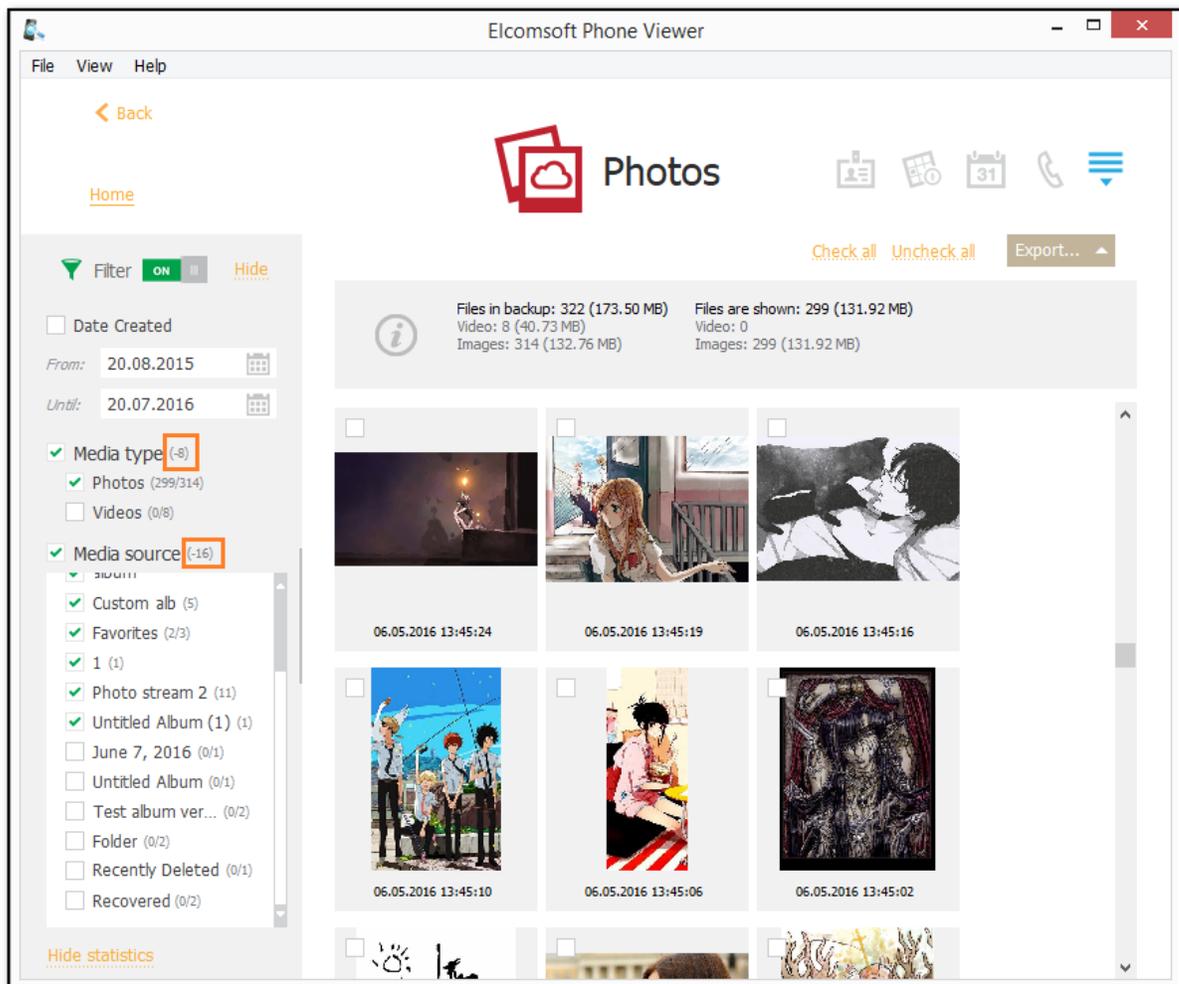
To filter out the media, open the **Filter** pane by clicking the  icon on the left.

*NOTE: Once you enable filtering, all previously checked files become unchecked.*

Enable filtering by switching the **On/Off** toggle and define the filtering options:

- **Date Created:** filters the media created within a specific time period. Select the **From** and **Until** dates in the corresponding drop-down lists.
- **Media type:** filters the media by a media type (photo and video).
- **Media source:** filters the media by albums in iCloud. Select the **Recovered** folder to view the deleted files, which are no longer displayed in the **Recently Deleted** folder.

If you clear any check box for Media Type or Album, a negative number will be displayed next to the filter category. This number indicates the number of files that are currently not displayed.



#### 4.4.17 Notifications

This plugin allows you to explore the user's **push notifications** that are used for applications to inform about different types of updates.

*NOTE: This plugin is only available for iOS 7.x.x - 10.x.x backups of the following types: iCloud and iTunes (encrypted, not encrypted, and backups with restored file names).*

You can view the following information received in notifications:

- **Date and time (including the time zone)** when the notification was received
- **Application** from which the notification was sent
- **Description** which contains the notification text

*NOTE: If the notification text is long and does not fit the screen, it ends with "...". To view the full notification text, hover the mouse over the notification and full text will be displayed as a prompt.*

All notifications are displayed in a grid. The most recent notifications are displayed on top. The general information about notifications is displayed above the grid:

- **Records:** total number of notifications
- **Most recent record:** date and time when the most recent notification was received
- **Oldest record:** date and time when the oldest notification was received

If the filtering is on, you can also view the statistic information on the filtered notifications:

- **Shown records:** number of notifications that match the filtering criteria.
- **Most recent filtered record:** date and time of when the most recent notification (among the filtered records) was received
- **Oldest filtered record:** date and time when the oldest notification (among the filtered records) was received

To sort the notifications in the grid, click the necessary column header.

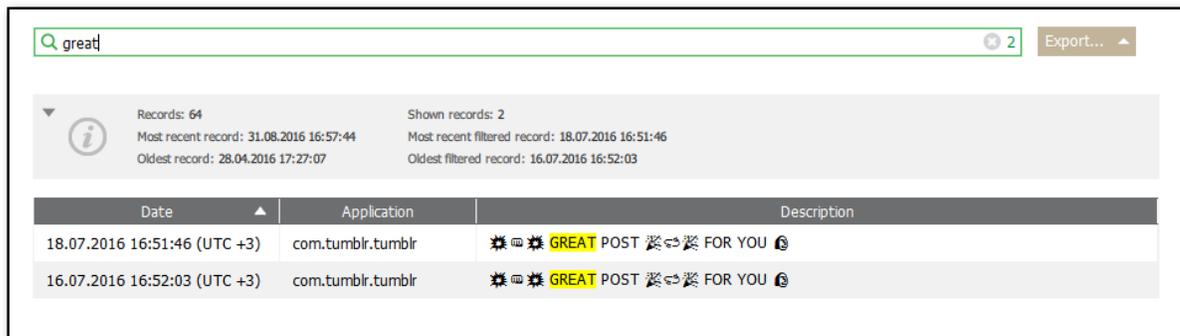
The screenshot displays the 'Notifications' section in Elcomsoft Phone Viewer. The interface includes a search bar, a filter sidebar, and a table of notifications. The filter sidebar shows 'Filter ON' and 'Hide' options. The table has columns for Date, Application, and Description. The notifications are sorted by date, with the most recent at the top.

Date	Application	Description
04.07.2016 16:51:57 (UTC +3)	com.tumblr.tumblr	You'll want to be sitting down for this post
03.07.2016 16:51:52 (UTC +3)	com.tumblr.tumblr	unsounded is a genius
02.07.2016 16:51:42 (UTC +3)	com.tumblr.tumblr	unsounded posted this when you weren't looking
01.07.2016 16:51:47 (UTC +3)	com.tumblr.tumblr	They've got a crush on unsounded's post
30.06.2016 16:51:48 (UTC +3)	com.tumblr.tumblr	We've got a crush on this photo
29.06.2016 16:51:41 (UTC +3)	com.tumblr.tumblr	unsounded is a genius
28.06.2016 16:51:46 (UTC +3)	com.tumblr.tumblr	We've got a crush on this post
27.06.2016 16:51:48 (UTC +3)	com.tumblr.tumblr	You'll want to be sitting down for this post
26.06.2016 16:51:45 (UTC +3)	com.tumblr.tumblr	unsounded's video is trending with 674,035 notes.
25.06.2016 16:51:57 (UTC +3)	com.tumblr.tumblr	unsounded is a genius.
24.06.2016 17:03:34 (UTC +3)	com.tumblr.tumblr	We've got a crush on this post
22.06.2016 16:51:54 (UTC +3)	com.tumblr.tumblr	unsounded posted this when you weren't looking

## Searching and Filtering

You can search for notifications by the application name and description.

To perform searches in Notifications, enter the search request in the search field and press **Enter**. The search results will be highlighted in yellow. The number of search results will be displayed in the search field.



You can filter notifications by dates and applications.

**To filter the notifications**, open the **Filter** pane by clicking the  icon on the left.

Enable filtering by switching the **On/Off** toggle, and define the filtering options:

- **Date:** filters the notifications by date. Select the **Date** check box and then select the **From** and **Until** dates in the calendar fields.
- **Application:** filters the notifications by applications. Select the **Application** check box and then select the check boxes for the necessary application names.

If you clear any check box for an application name, a negative number will be displayed next to the **Application** filter. This number indicates the number of records that are currently not displayed.

### Exporting Notifications

**To export notifications**, do the following:

1. Click **Export**.
2. Select one of the following values from the drop-down list: **Filtered** or **All**.
3. The **Select destination file** window will open.
4. In the opened window, select the location in which the file with exported notifications will be saved, enter the file name and select the file extension (.txt or .xlsx).
5. Click **Save**.
6. The file is saved in the selected location.

When the file has **.txt** extension, it is exported in **.csv** format. **To open the file in Excel**, right-click it and then select **Excel** from the **Open with** menu.

## 4.4.18 Signal

This plugin allows you to explore the Signal app data such as user's profile, calls, messages, and attachments.

*NOTE: This plugin is only available for iOS device images.*

The data in the **Signal** plugin is divided into the following categories:

- Profile
- Calls
- Messages
- Attachments

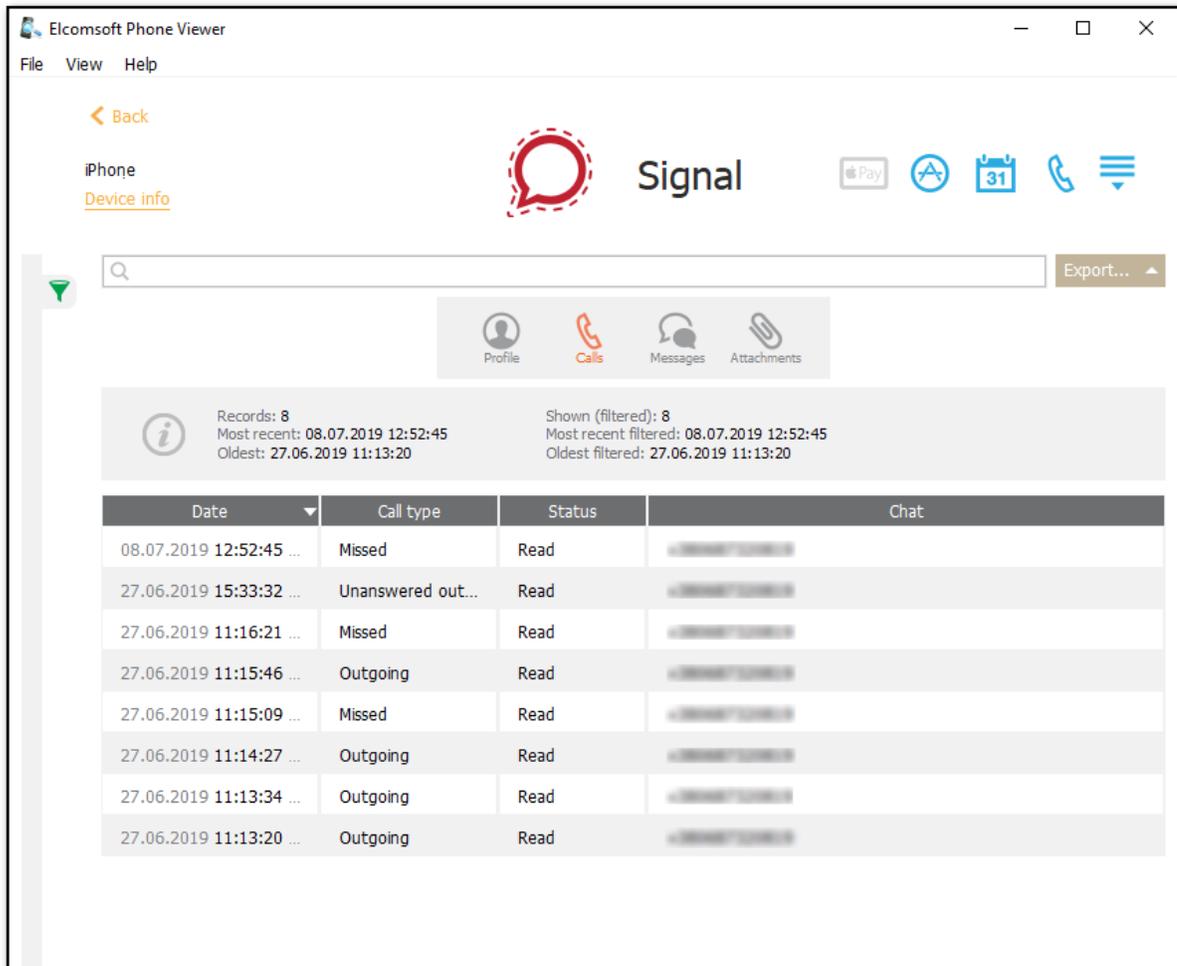
For **Profile**, the following information is displayed:

- Avatar (you can click the  icon to view the avatar)
- Name
- Phone Number

- Linked Devices

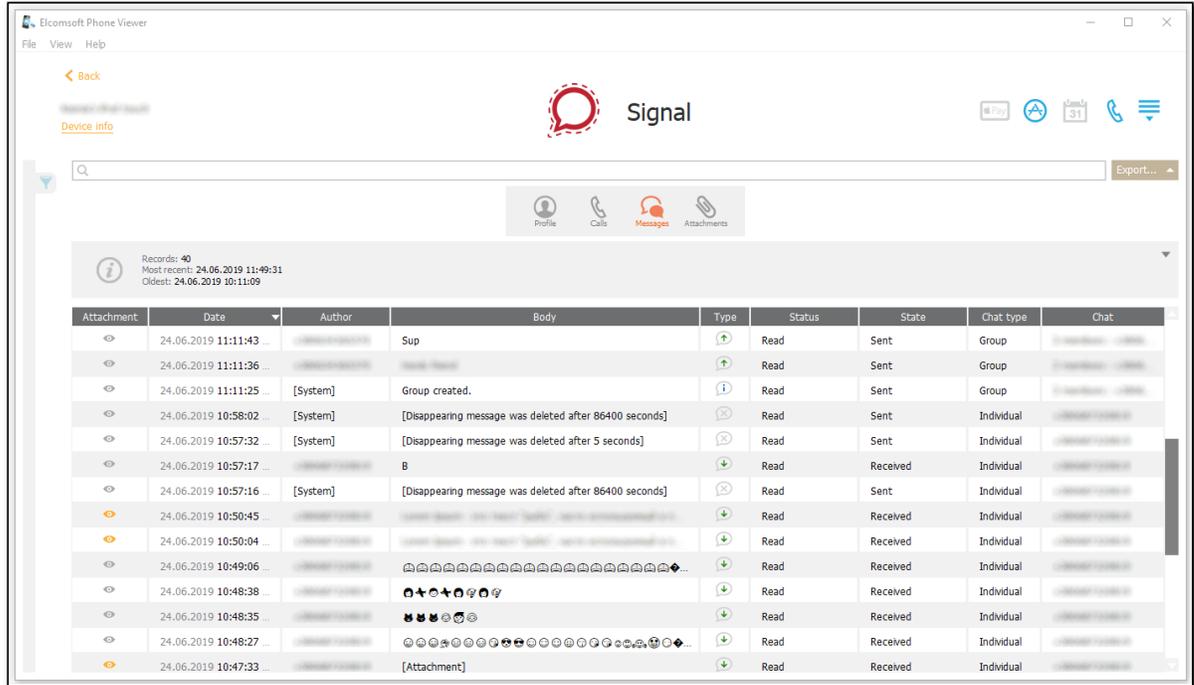
For **Calls**, the following information is displayed:

- Date
- Call type
- Status
- Chat



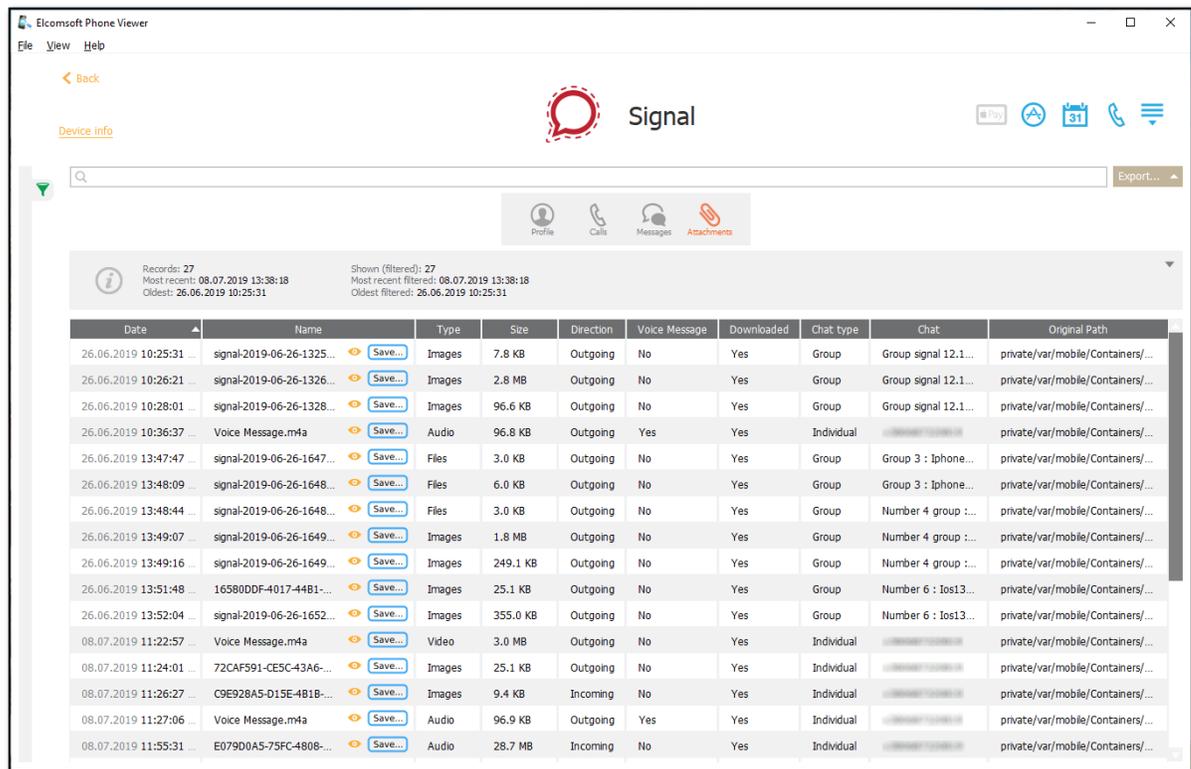
For **Messages**, the following information is displayed:

- Attachment (you can click the  icon next to view the file)
- Date
- Author
- Body
- Type (  - **outgoing** message;  - **incoming** message;  - **system** message (information message);  - **system** message (information about disappearing message))
- Status
- State
- Chat type
- Chat



For **Attachments**, the following information is displayed:

- Date
- Name (To view the attachment, click the  icon. To save the attachment, click the  icon)
- Type
- Size
- Direction
- Voice Message
- Downloaded
- Chat type
- Chat
- Original Path



## Exporting Signal Data

To export data, do the following:

1. Click **Export**.
2. Select one of the following values from the drop-down list: **Filtered** or **All**.
3. The **Select destination file** window opens.
4. In the opened window, select the location in which the file with exported data will be saved and enter the file name.
5. Click **Save**.
6. The **<file name>.xlsx** file is saved in the selected location.
7. The attachments are saved in the selected location in the **<file name>\_Signal** folder name.

## Searching and Filtering

To perform searches in **Signal**, enter the search request in the search field and press **Enter**. The search results will be highlighted in yellow. The number of search results will be displayed in the search field.

To filter out the messages, open the **Filter** pane by clicking the  icon on the left. Enable filtering by switching the On/Off toggle, and define the filtering options:

- **Status:** filters calls and messages by status (**Read** or **Unread**).
- **Call type:** filters calls by type (**Missed**, **Outgoing**, or **Unanswered outgoing**).
- **Chat type:** filters chats by type (**Group** or **Individual**).
- **State:** filters message by state (**Draft**, **Received**, or **Sent**).
- **Voice Message:** filters if the attachment is a voice message or not.

- **Downloaded:** filters if the attachment was downloaded or not.
- **Has attachments:** filters if the messages has attachments or not.
- **Directions:** filters attachments by direction (**Incoming** or **Outgoing**)
- **Type:** filters messages (**Incoming**, **Info**, or **Outgoing**) or attachments (**Audio**, **Files**, **Images**, or **Video**) by type.

The screenshot shows the Elcomsoft Phone Viewer interface. On the left, there is a filter sidebar with sections for Dates, Chat type, Voice Message, Direction, and Type. The main area displays a table of messages with columns for Date, Name, Type, Size, Direction, Voice Message, Downloaded, Chat type, Chat, and Original Path. The table contains 27 records, with the most recent filtered record being from 08.07.2019 13:38:18 and the oldest being from 26.06.2019 10:25:31.

Date	Name	Type	Size	Direction	Voice Message	Downloaded	Chat type	Chat	Original Path
26.06.2019 10:25:31	signal-2019-06-26-1325...	Images	7.8 KB	Outgoing	No	Yes	Group	Group signal 12.1...	private/var/mobile/Container...
26.06.2019 10:26:21	signal-2019-06-26-1326...	Images	2.8 MB	Outgoing	No	Yes	Group	Group signal 12.1...	private/var/mobile/Container...
26.06.2019 10:28:01	signal-2019-06-26-1328...	Images	96.6 KB	Outgoing	No	Yes	Group	Group signal 12.1...	private/var/mobile/Container...
26.06.2019 10:36:37	Voice Message.m4a	Audio	96.8 KB	Outgoing	Yes	Yes	Individual		private/var/mobile/Container...
26.06.2019 13:47:47	signal-2019-06-26-1647...	Files	3.0 KB	Outgoing	No	Yes	Group	Group 3 : Iphone...	private/var/mobile/Container...
26.06.2019 13:48:09	signal-2019-06-26-1648...	Files	6.0 KB	Outgoing	No	Yes	Group	Group 3 : Iphone...	private/var/mobile/Container...
26.06.2019 13:48:44	signal-2019-06-26-1648...	Files	3.0 KB	Outgoing	No	Yes	Group	Number 4 group :...	private/var/mobile/Container...
26.06.2019 13:49:07	signal-2019-06-26-1649...	Images	1.8 MB	Outgoing	No	Yes	Group	Number 4 group :...	private/var/mobile/Container...
26.06.2019 13:49:16	signal-2019-06-26-1649...	Images	249.1 KB	Outgoing	No	Yes	Group	Number 4 group :...	private/var/mobile/Container...
26.06.2019 13:51:48	16580DDF-4017-44B1-...	Images	25.1 KB	Outgoing	No	Yes	Group	Number 6 : Ios13...	private/var/mobile/Container...
26.06.2019 13:52:04	signal-2019-06-26-1652...	Images	355.0 KB	Outgoing	No	Yes	Group	Number 6 : Ios13...	private/var/mobile/Container...
08.07.2019 11:22:57	Voice Message.m4a	Video	3.0 MB	Outgoing	No	Yes	Individual		private/var/mobile/Container...
08.07.2019 11:24:01	72CAF591-CE5C-43A6-...	Images	25.1 KB	Outgoing	No	Yes	Individual		private/var/mobile/Container...
08.07.2019 11:26:27	C9E928A5-D15E-481B-...	Images	9.4 KB	Incoming	No	Yes	Individual		private/var/mobile/Container...
08.07.2019 11:27:06	Voice Message.m4a	Audio	96.9 KB	Outgoing	Yes	Yes	Individual		private/var/mobile/Container...
08.07.2019 11:55:31	E079D0A5-75FC-4808-...	Audio	28.7 MB	Incoming	No	Yes	Individual		private/var/mobile/Container...

#### 4.4.19 Skype

This plugin allows you to explore the **Skype** data such as account info, contacts, calls, etc.

*NOTE: This plugin is only available for Microsoft backups.*

The data in the **Skype** plugin is divided into the following categories:

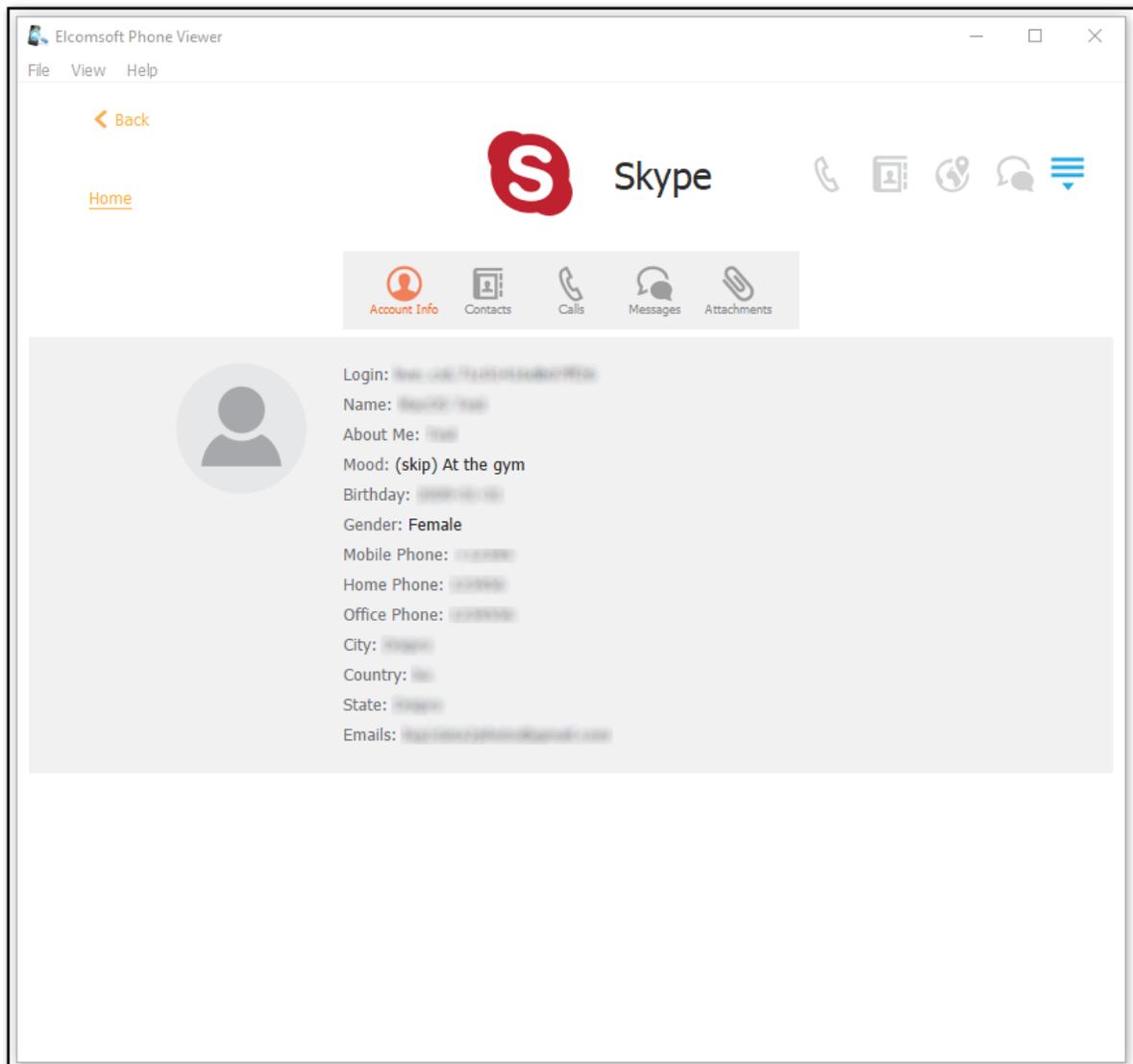
- **Account Info:** information about the user's Skype account
- **Contacts:** information about the user's contacts
- **Calls:** information about the user's calls
- **Messages:** information about the user's messages
- **Attachments:** information about attachments

*NOTE: If attachments (except Pictures) are sent more than 30 days ago, they will be deleted from MS server and will not be available for viewing in EPV. All other data types will be available regardless of the terms of their storage. More detailed information about terms of data storage can be found here <https://support.skype.com/en/faq/FA34893/how-long-are-files-and-data-available-in-skype>*

For **Account Info**, the following information is displayed:

- **Login**
- **Name**
- **About Me**

- Mood
- Birthday
- Gender
- Mobile Phone
- Home Phone
- Office Phone
- City
- Country
- State
- Emails



For **Contacts**, the following information is displayed:

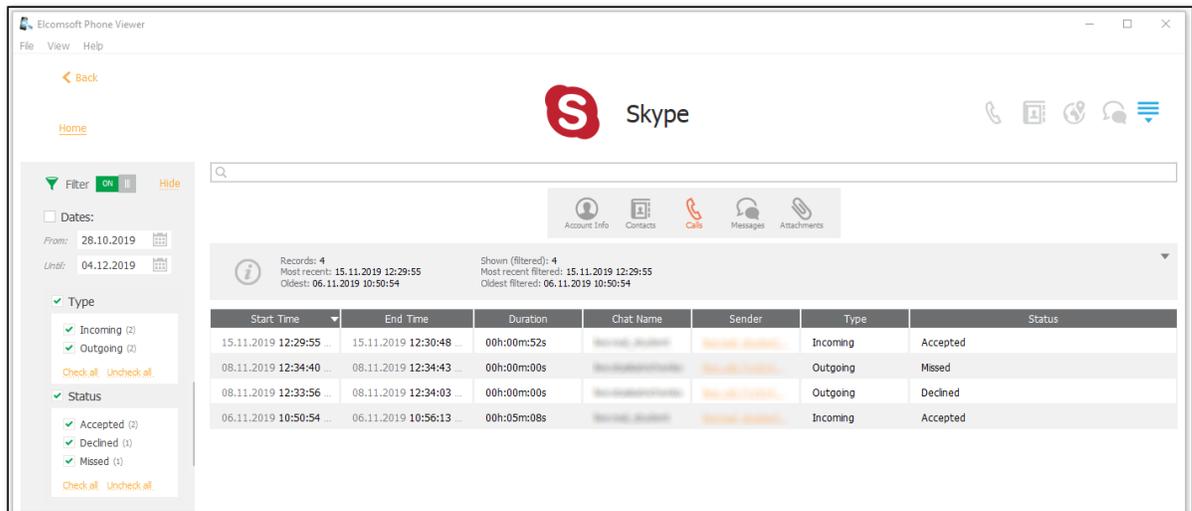
- **Avatar** (To view the avatar, click the  icon. To save the avatar, click the  icon)
- **Login**
- **Display name**

- Name
- About me
- Mood
- Company
- Birthday
- Creation time
- Gender
- Job title
- Mobile phone
- Office phone
- Home phone
- City
- Country
- State
- Is blocked
- Is favorite

Avatar	Login	Display name	Name	About me	Mood	Company	Birthday	Creation time
skypeAttachments/Avatars/...	...	...	...				14.02.1989	29.10.2019 16:42:2
skypeAttachments/Avatars/...	...	...	...				18.06.1993	29.10.2019 16:42:2
skypeAttachments/Avatars/...	...	...	...				23.07.1986	29.10.2019 16:42:2
skypeAttachments/Avatars/...	...	...	...				No date is found	29.10.2019 16:42:2
skypeAttachments/Avatars/...	...	...	...				02.10.1994	29.10.2019 16:42:2

For **Calls**, the following information is displayed:

- Start Time
- End Time
- Duration
- Chat Name
- Sender
- Type
- Status



For **Messages**, the following information is displayed:

- **Date**
- **Attachment** (To view the attachment, click the  icon. To save the attachment, click the )
- **Sender**
- **Content**
- **Message Type**
- **Chat Name**
- **Bookmarked**
- **Edit Time**
- **Removal Time**

For **Attachments**, the following information is displayed:

- **Date**
- **File name** (To view the file, click the  icon. To save the file, click the )
- **Type**
- **Size**
- **Sender**
- **Chat Name**
- **Attachment path**

**NOTE: If attachments (except Pictures) are sent more than 30 days ago, they will be deleted from MS server and will not be available for viewing in EPV. In this case only attachments metadata, such as date, size, file name, sender, and chat name will be available for viewing.**

### Searching and Filtering

To perform searches in **Skype**, enter the search request in the search field and press **Enter**. The search results will be highlighted in yellow. The number of search results will be displayed in the search field.

To filter out the **Skype** data, open the **Filter** pane by clicking the  icon on the left.

Enable filtering by switching the **On/Off** toggle, and define the filtering options:

- **Dates:** filters contacts, calls, messages, and attachments by the date range
- **Call type:** filters calls by type (**Incoming** or **Outgoing**)
- **Message type:** filters messages by type (**Attachment, Call, Call Recording, Card, Contact, Flik Message, Location, Poll, Scheduled Call, or Text**)
- **Attachment type:** filters attachments by type (**Audio, File, Mojis, Picture, SWIFT, Sticker, or Video**)
- **Call status:** filters calls by status (**Accepted, Declined, or Missed**)
- **Show only favorite contacts**
- **Show only blocked contacts**
- **Show only edited messages**
- **Show only deleted messages**
- **Show only bookmarked messages**

#### 4.4.20 Screen Time

This plugin allows you to explore the Screen Time information such as device restrictions, time spent using applications, websites, etc.

*NOTE: This plugin is only available for iCloud synced data 5.x.x and higher.*

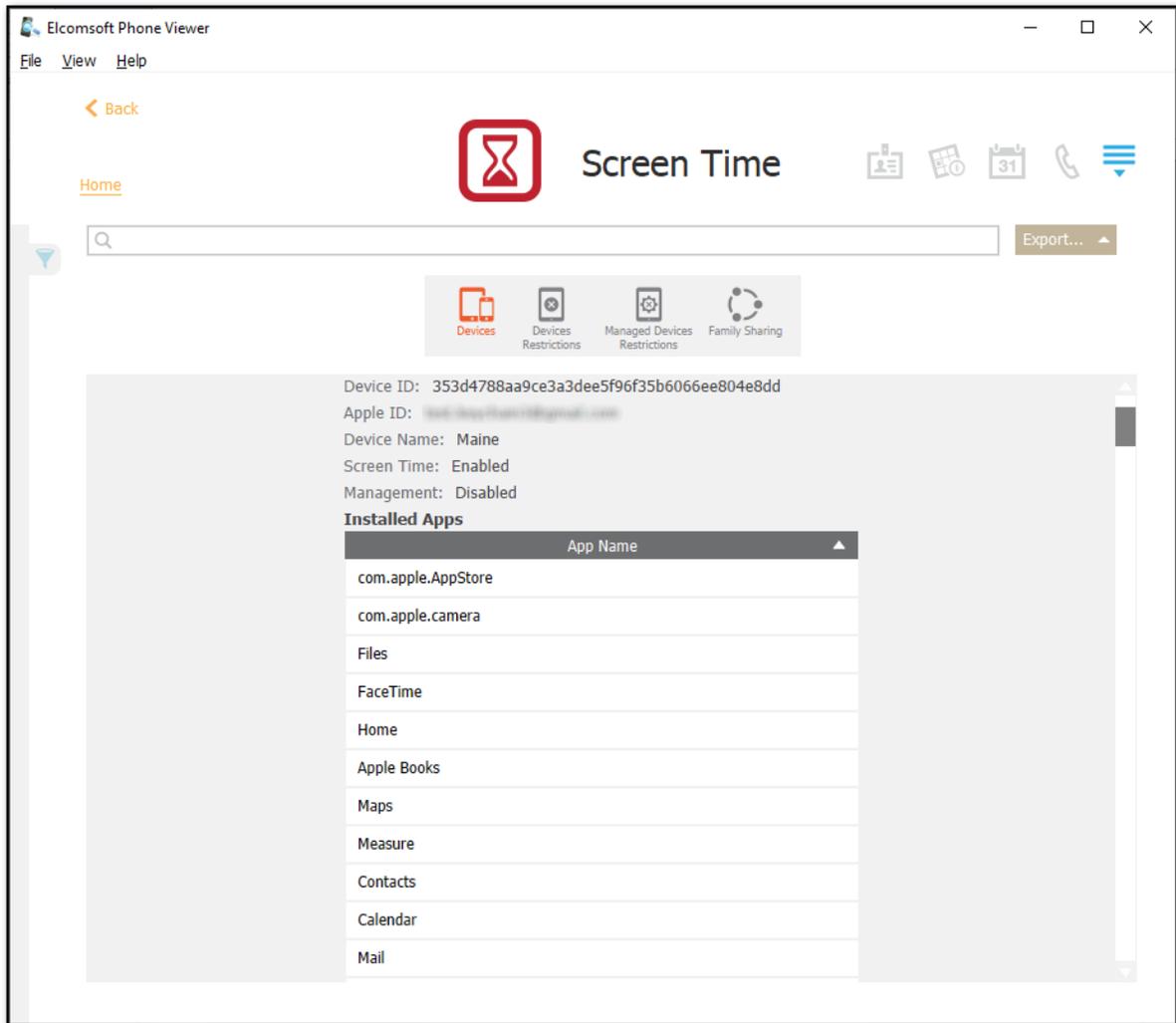
The data in the **Screen Time** plugin is divided into the following categories:

- **Devices:** information about the synced devices and installed apps on them
- **Devices Restriction:** information about the set restrictions on the user's device
- **Managed Devices Restrictions:** information about the set restrictions on the user's child's device
- **Family Sharing:** information about the Family Sharing feature

*NOTE: The Screen Time restrictions that are not enabled are not displayed in the Devices Restrictions and Managed Devices Restrictions tabs.*

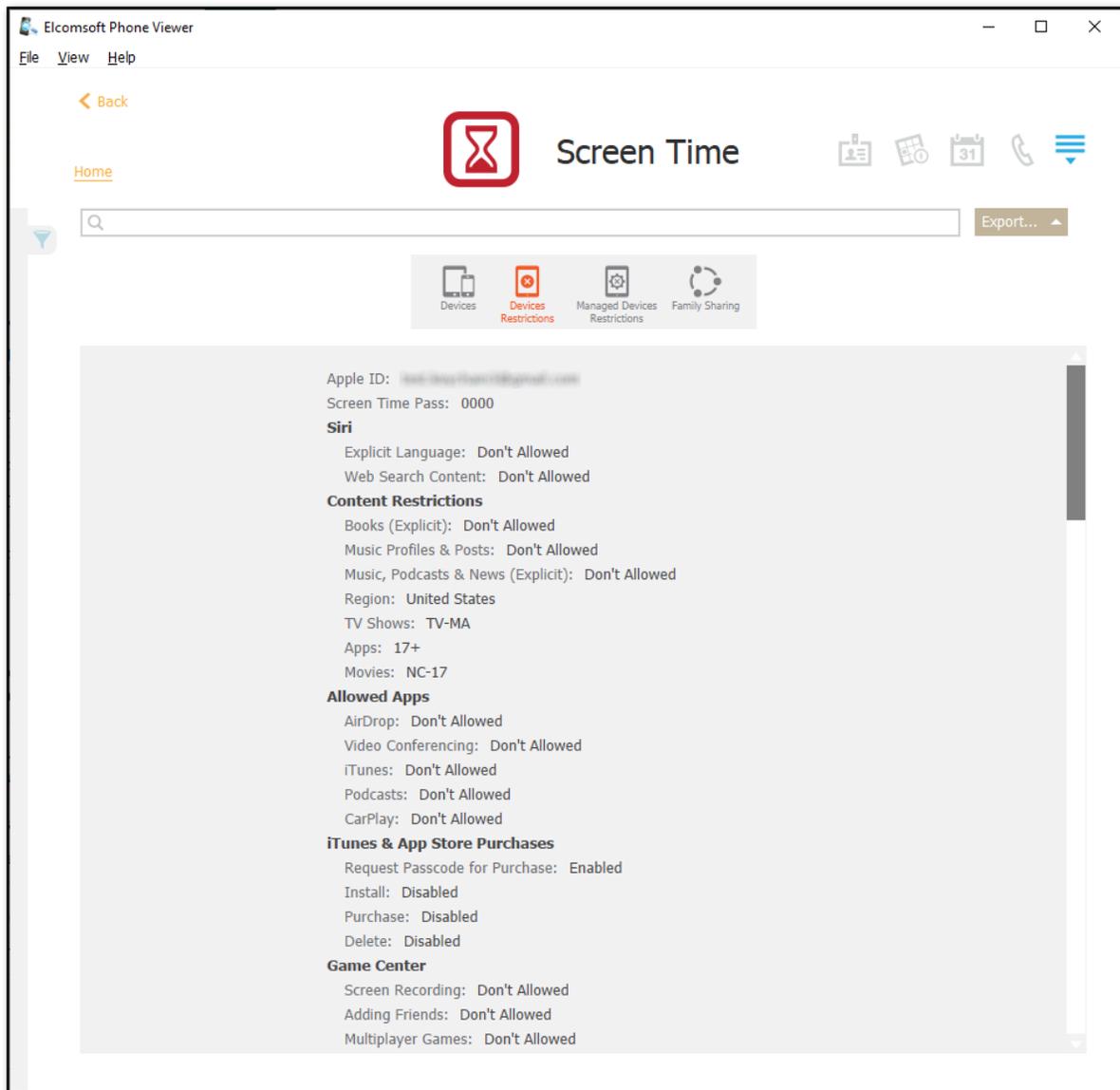
For **Devices**, the following information is displayed:

- **Device ID**
- **Apple ID**
- **Device Name**
- **Screen Time**
- **Management**
- **Installed Apps**



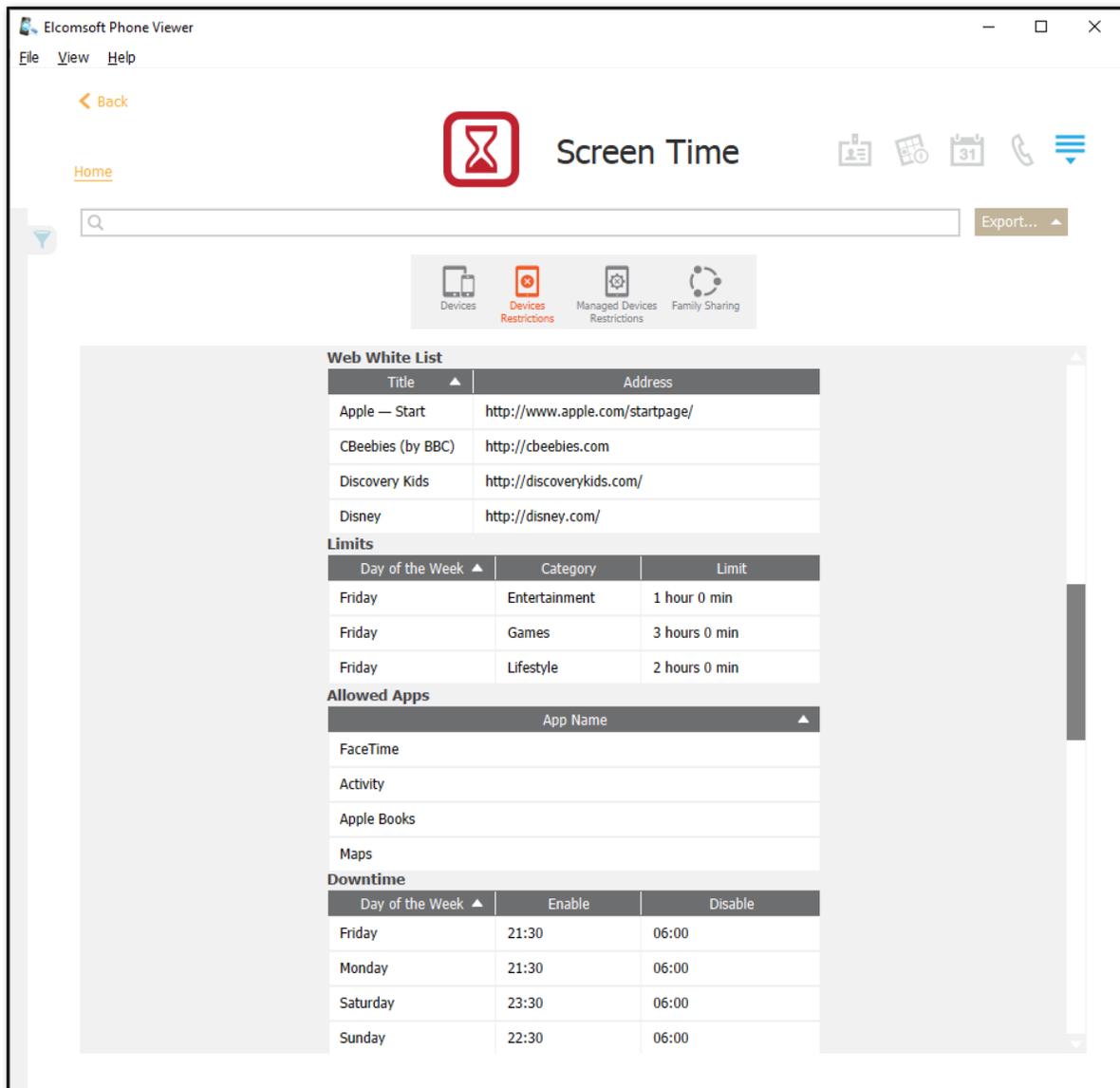
For **Devices Restrictions**, the following information is displayed:

- **Apple ID**
- **Screen Time Pass**
- **Siri** (Explicit Language; Web Search Content)
- **Content Restrictions** (Books (Explicit); Music Profiles & Posts; Music, Podcasts & News (Explicit); Region; TV Shows; Apps; Movies)
- **Allowed Apps** (AirDrop; Video Conferencing; iTunes; Podcasts; CarPlay)
- **iTunes & App Store Purchases** (Request Passcode for Purchase; Install; Purchase; Delete)
- **Game Center** (Screen Recording; Adding Friends; Multiplayer Games)
- **Web Content** (Web Restriction; Web Content Filter)
- **Allow Changes** (Account Changes; TV Provider; Passcode Changes; Background App Activities; Do Not Disturb While Driving; Find My Friends Modification; Cellular Plan Changes; App Cellular Data Changes)



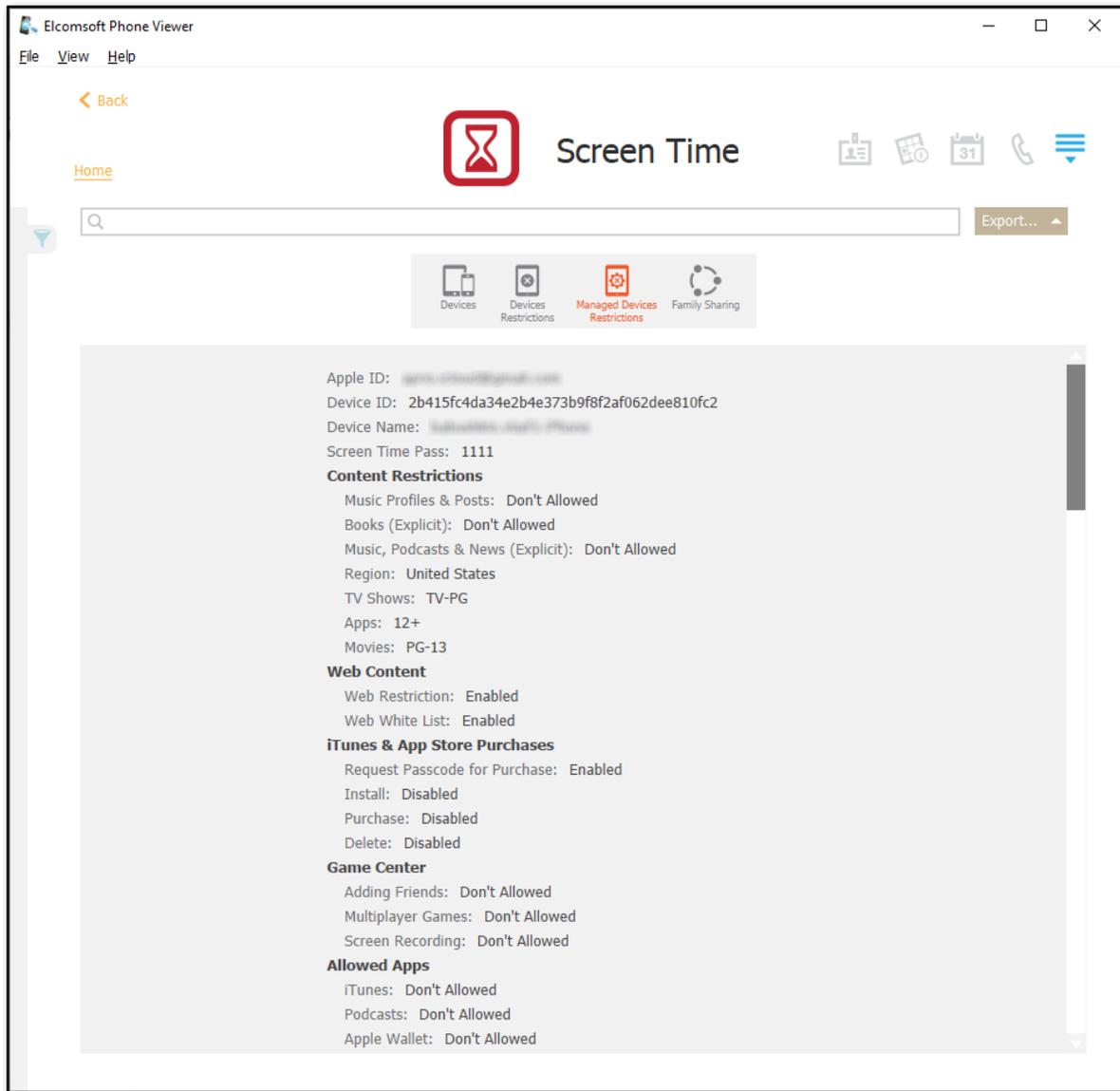
In the grids of **Devices Restrictions**, the following information is displayed:

- **Web White List** (Title; Address)
- **Limits** (Day of the Week; Category; Limit)
- **Allowed Apps** (App Name)
- **Downtime** (Day of the Week; Enable; Disable)



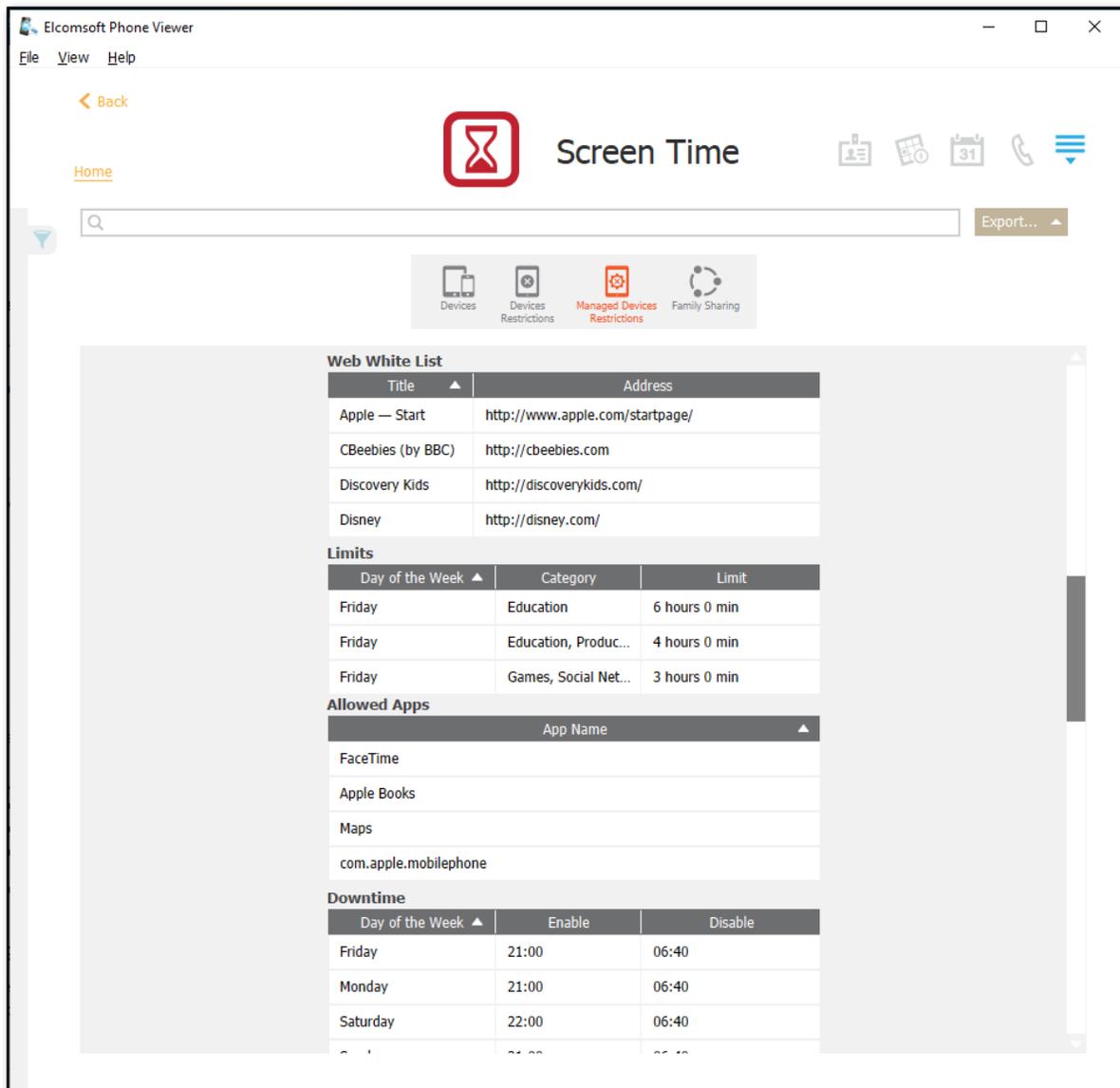
For **Managed Devices Restrictions**, the following information is displayed:

- **Apple ID**
- **Device ID**
- **Device Name**
- **Screen Time Pass**
- **Content Restrictions** (Music Profiles & Posts; Books (Explicit); Music, Podcasts & News (Explicit); Region; TV Shows; Apps; Movies)
- **Web Content** (Web Restriction; Web White List; Web Content Filter)
- **iTunes & App Store Purchased** (Request Passcode for Purchase; Install; Purchase; Delete)
- **Game Center** (Adding Friends; Multiplayer Games; Screen Recording)
- **Allowed Apps** (iTunes; Podcasts; Apple Wallet; CarPlay)
- **Siri** (Explicit Language; Web Search Content)
- **Allow Changes** (Find My Friends Modification; Cellular Plan Changes; App Cellular Data Changes; Account Changes; Background App Activities; TV Provider; Do Not Disturb While Driving; Passcode Changes)



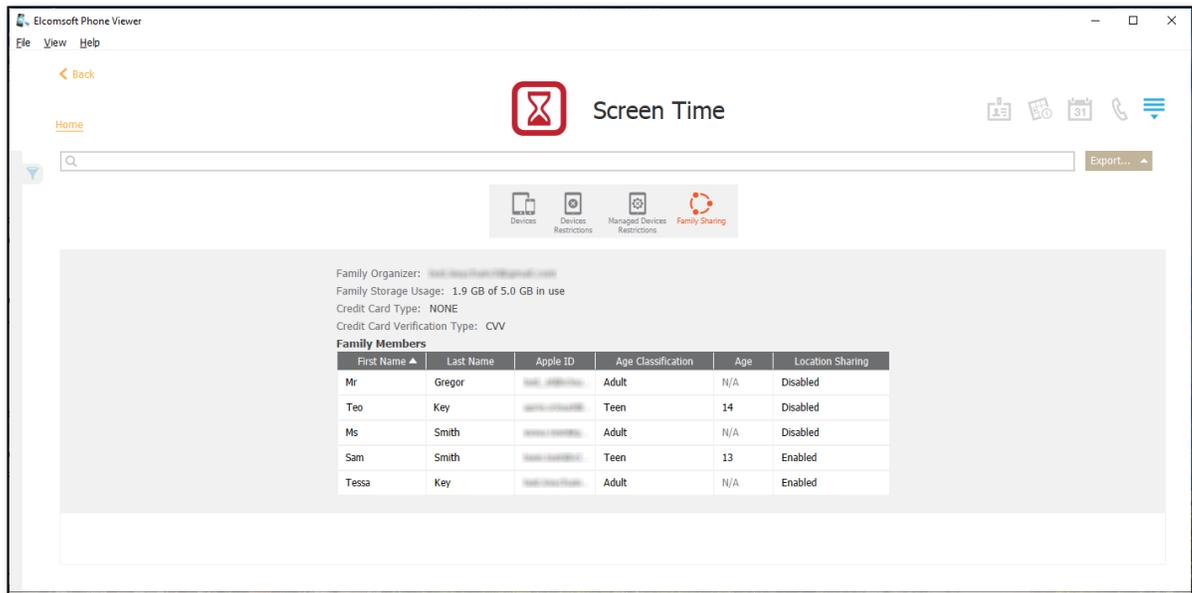
In the grids of **Managed Devices Restrictions**, the following information is displayed:

- **Web White List** (Title; Address)
- **Limits** (Day of the Week; Category; Limit)
- **Allowed Apps** (App Name)
- **Downtime** (Day of the Week; Enable; Disable)



For **Family Sharing**, the following information is displayed:

- **Family Organizer**
- **Family Storage Usage**
- **Credit Card Type**
- **Credit Card Verification Type**
- **Family Members** (First Name; Last Name; Apple ID; Age Classification; Age; Location Sharing)



## Exporting Screen Time Data

To export data, do the following:

1. Click **Export**.
2. Select one of the following values from the drop-down list: **Filtered** or **All**.
3. The **Select destination file** window opens.
4. In the opened window, select the location in which the file with exported data will be saved and enter the file name.
5. Click **Save**.
6. The **<file name>.xlsx** file is saved in the selected location.

## Searching and Filtering

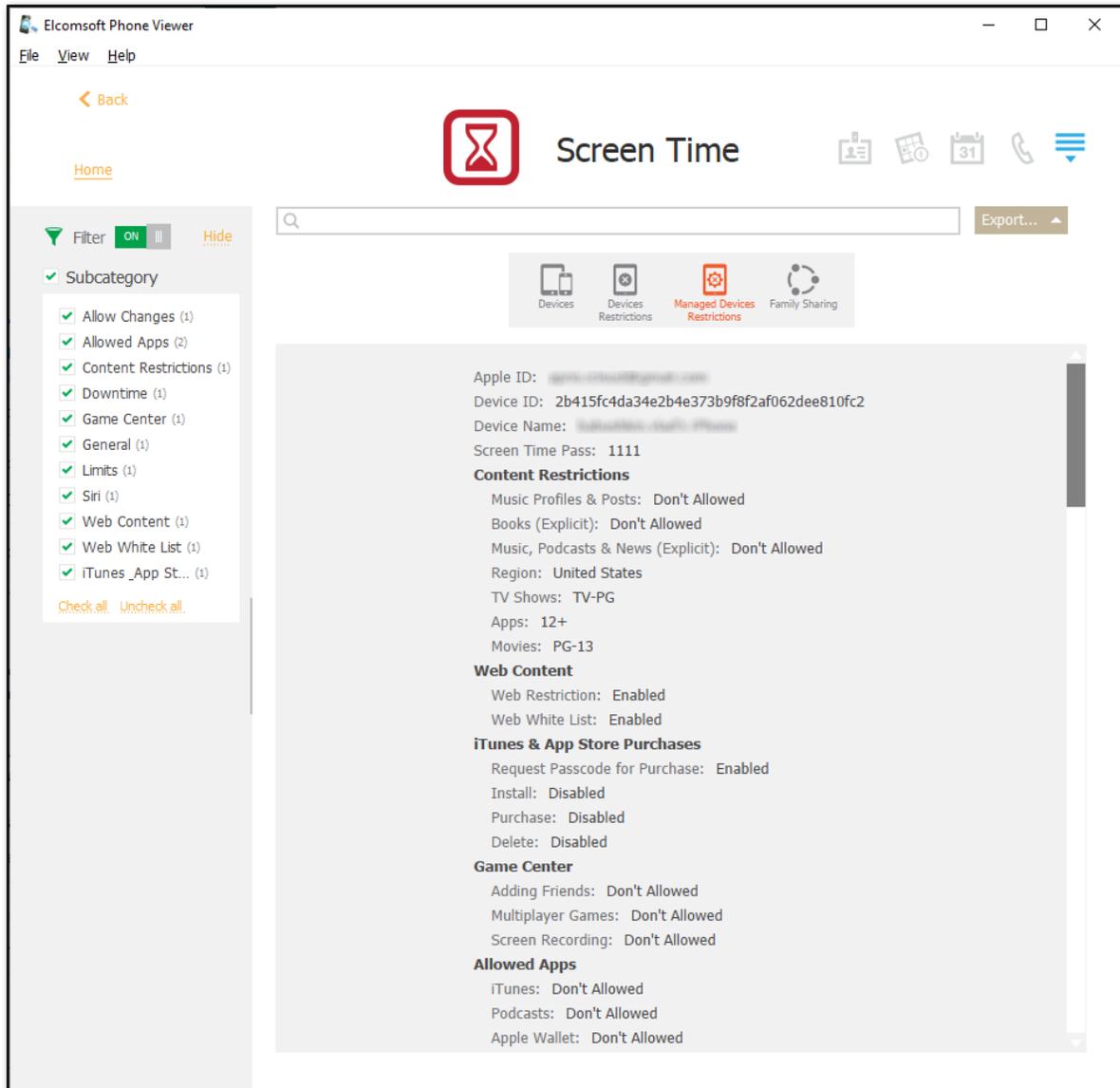
To perform searches in **Screen Time**, enter the search request in the search field and press **Enter**. The search results will be highlighted in yellow. The number of search results will be displayed in the search field.

To filter out the restrictions, open the **Filter** pane by clicking the  icon on the left. Enable filtering by switching the **On/Off** toggle, and define the filtering options:

- General (not included in any subcategory data)
- Allow Changes
- Allowed Apps
- Installed Apps
- Content Restrictions
- Downtime
- Game Center
- Limits
- Siri
- Web Content

- Web White List
- iTunes App Store Purchases
- Family Members

*NOTE: The number of the filtering options depend on the number of the set Screen Time restrictions.*



#### 4.4.21 Telegram

This plugin allows you to explore the **Telegram** data such as account info, contacts, calls, chat information, etc.

*NOTE: This plugin is only available for iOS device images.*

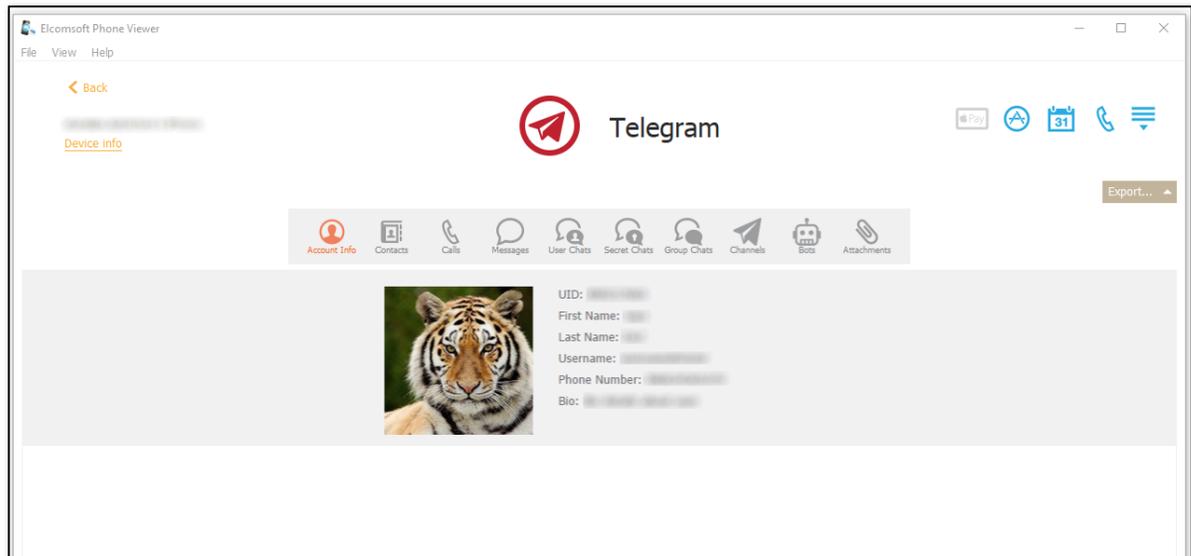
The data in the **Telegram** plugin is divided into the following categories:

- **Account Info:** information about the user's account
- **Contacts:** information about the user's contacts

- **Calls:** information about the user's calls
- **Messages:** information about the user's messages
- **User Chats:** information about the individual chats
- **Secret Chats:** information about the individual secret chats
- **Group Chats:** information about the group chats
- **Channels:** information about the channels
- **Bots:** information about the bots
- **Attachments:** information about the attachments

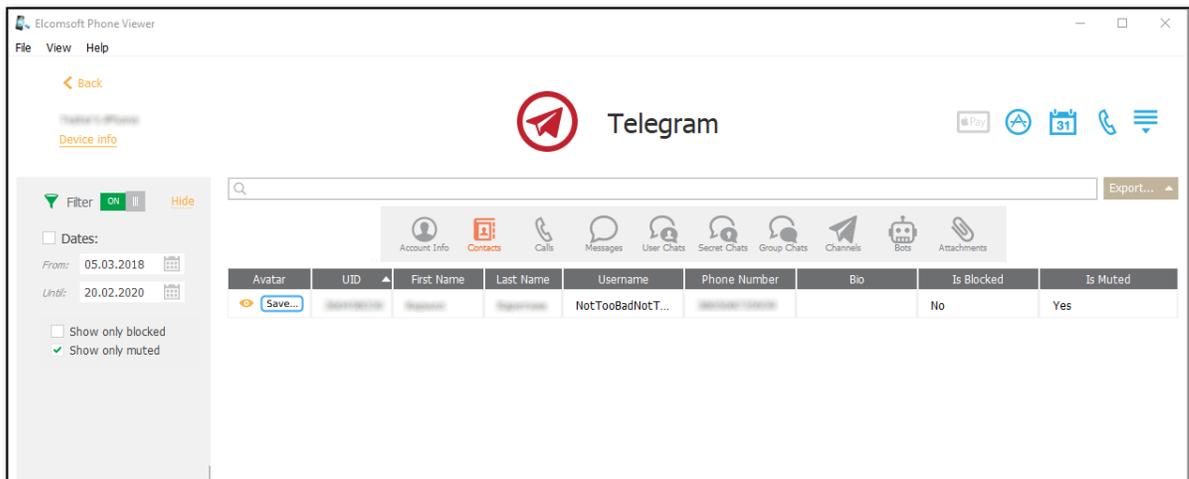
For **Account Info**, the following is displayed:

- **Avatar**
- **UID**
- **First Name**
- **Last Name**
- **Username**
- **Phone Number**
- **Bio**



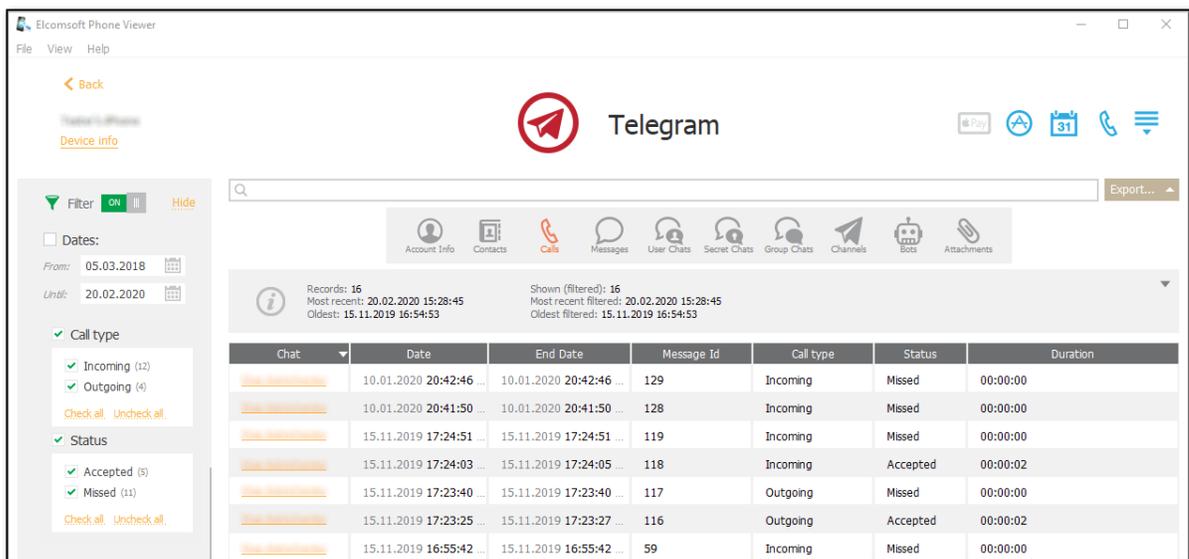
For **Contacts**, the following information is displayed:

- **Avatar** (To view the avatar, click the  icon. To save the avatar, click the  icon)
- **UID**
- **First Name**
- **Last Name**
- **Username**
- **Phone Number**
- **Bio**
- **Is Blocked**
- **Is Muted**



For **Calls**, the following information is displayed:

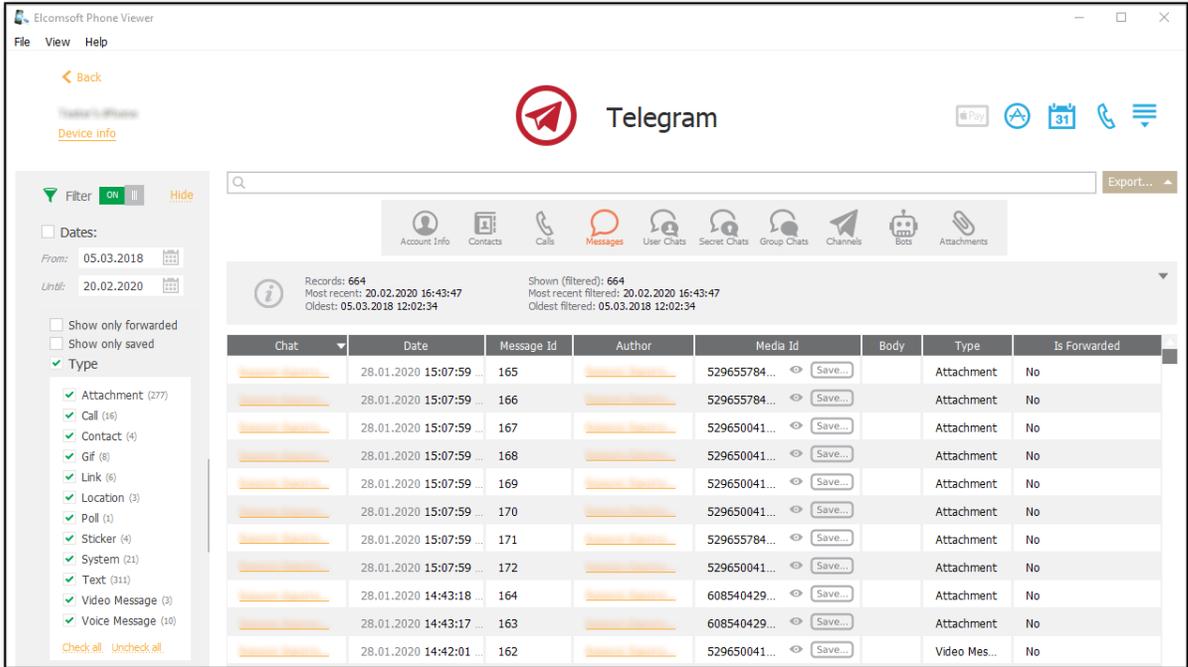
- **Chat** (It contains data about persons the user chatted with, namely, **avatar, type, UID, first name, last name, username, phone number, bio, is blocked, is muted, is pinned, and is archived**. To view such data, click the link in the **Chat** column)
- **Date**
- **End Date**
- **Message Id**
- **Call type**
- **Status**
- **Duration**



For **Messages**, the following information is displayed:

- **Chat** (It contains data about persons the user chatted with, namely, **avatar, type, UID, first name, last name, username, phone number, bio, is blocked, is muted, is pinned, and is archived**. To view such data, click the link in the **Chat** column)
- **Date**
- **Message Id**

- **Author** (It contains data about the message author, namely, **avatar**, **type**, **UID**, **first name**, **last name**, **username**, **phone number**, **bio**, **is blocked**, **is muted**, **is pinned**, and **is archived**. To view such data, click the link in the **Author** column)
- **Media Id** (To view the message attachment, click the  icon. To save the message attachment, click the  icon)
- **Body**
- **Type**
- **Is Forwarded**



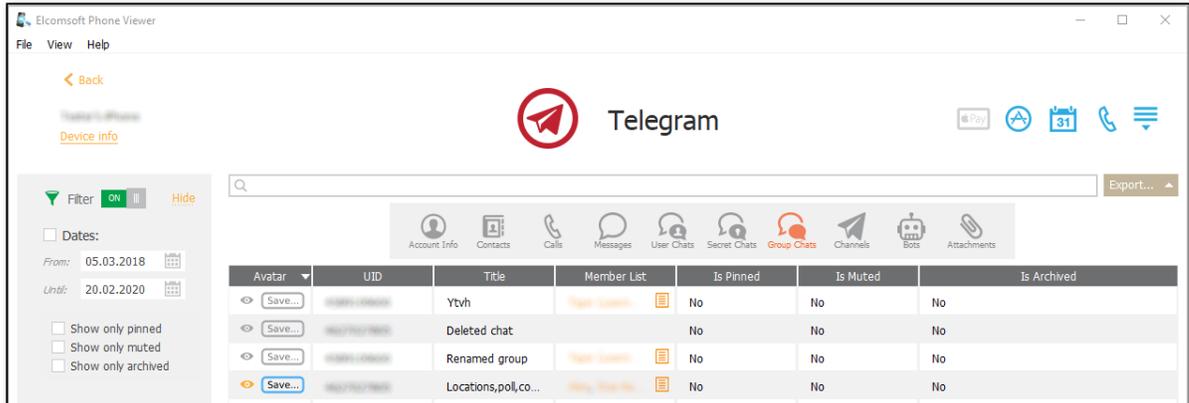
The screenshot displays the Elcomsoft Phone Viewer interface for a Telegram chat. The top navigation bar includes 'Back', 'Telegram', and various utility icons. A search bar and 'Export...' button are visible. Below the navigation is a toolbar with icons for Account Info, Contacts, Calls, Messages, User Chats, Secret Chats, Group Chats, Channels, Bots, and Attachments. The main area shows a table of messages with columns for Chat, Date, Message Id, Author, Media Id, Body, Type, and Is Forwarded. The table contains 12 rows of message data.

Chat	Date	Message Id	Author	Media Id	Body	Type	Is Forwarded
	28.01.2020 15:07:59 ...	165		529655784... 		Attachment	No
	28.01.2020 15:07:59 ...	166		529655784... 		Attachment	No
	28.01.2020 15:07:59 ...	167		529650041... 		Attachment	No
	28.01.2020 15:07:59 ...	168		529650041... 		Attachment	No
	28.01.2020 15:07:59 ...	169		529650041... 		Attachment	No
	28.01.2020 15:07:59 ...	170		529650041... 		Attachment	No
	28.01.2020 15:07:59 ...	171		529655784... 		Attachment	No
	28.01.2020 15:07:59 ...	172		529650041... 		Attachment	No
	28.01.2020 14:43:18 ...	164		608540429... 		Attachment	No
	28.01.2020 14:43:17 ...	163		608540429... 		Attachment	No
	28.01.2020 14:42:01 ...	162		529650041... 		Video Mes...	No

For **User Chats**, the following information is displayed:

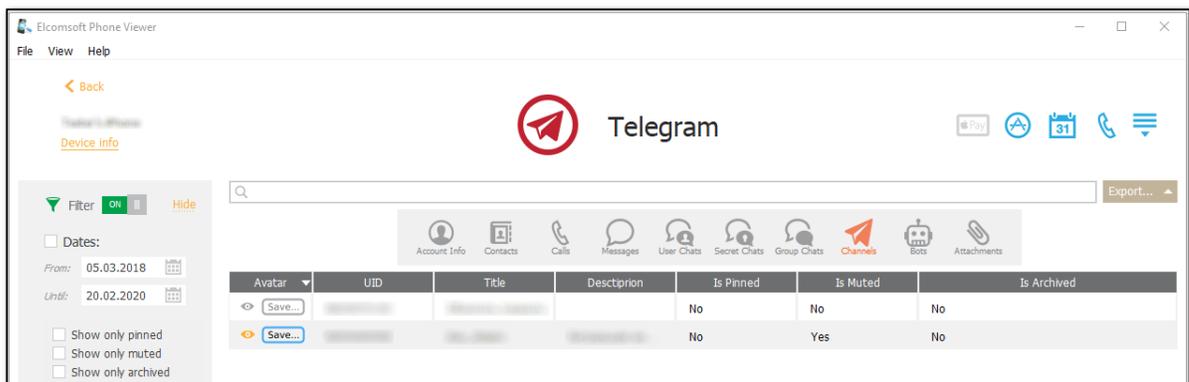
- **Avatar** (To view the avatar, click the  icon. To save the avatar, click the  icon)
- **UID**
- **First Name**
- **Last Name**
- **Username**
- **Phone Number**
- **Bio**
- **Is Blocked**
- **Is Muted**
- **Is Pinned**
- **Is Archived**





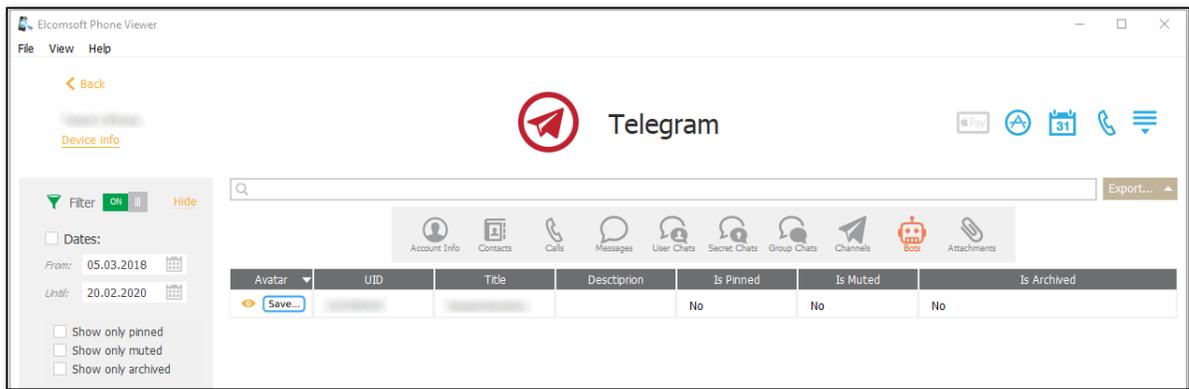
For **Channels**, the following information is displayed:

- **Avatar** (To view the avatar, click the icon. To save the avatar, click the Save... icon)
- **UID**
- **Title**
- **Description**
- **Is Pinned**
- **Is Muted**
- **Is Archived**



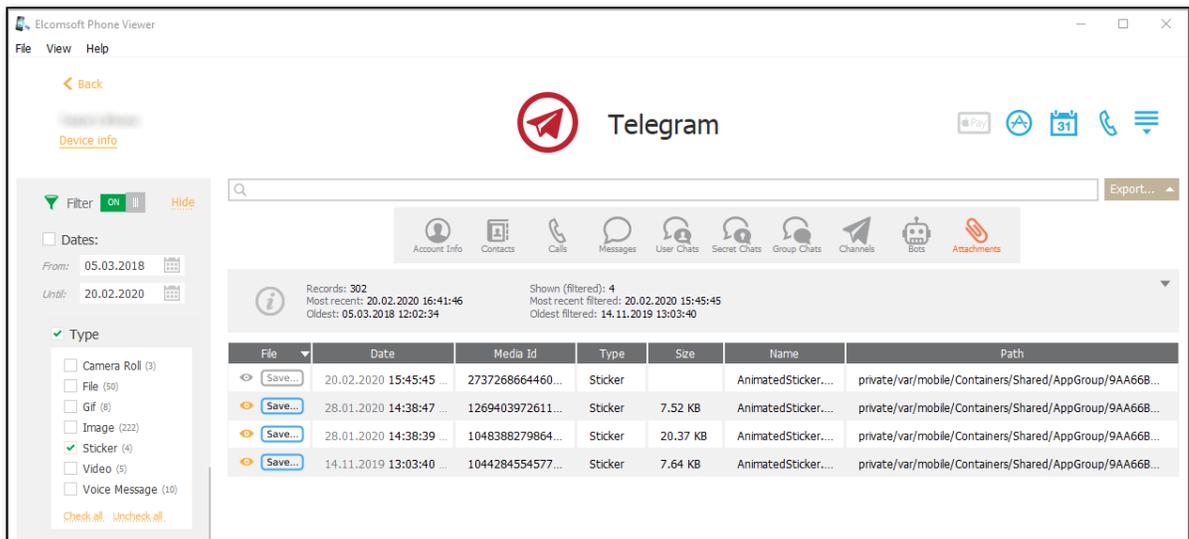
For **Bots**, the following information is displayed:

- **Avatar** (To view the avatar, click the icon. To save the avatar, click the Save... icon)
- **UID**
- **Title**
- **Description**
- **Is Pinned**
- **Is Muted**
- **Is Archived**



For **Attachments**, the following information is displayed:

- **File** (To view the file, click the  icon. To save the file, click the **Save...** icon)
- **Date**
- **Media Id**
- **Type**
- **Size**
- **Name**
- **Path**



## Exporting Telegram Data

To export data, do the following:

1. Click **Export**.
2. Select one of the following values from the drop-down list: **Selected**, **Filtered** or **All**.
3. The **Select destination file** window opens.
4. In the opened window, select the location to which the file with exported data will be saved and enter the file name.
5. Click **Save**.
6. The **<file name>.xlsx** file is saved to the selected location.

## Searching and Filtering

To perform searches in **Telegram**, enter the search request in the search field and press **Enter**. The search results will be highlighted in yellow. The number of search results will be displayed in the search field.

To filter out the **Telegram** data, open the **Filter** pane by clicking the  icon on the left.

Enable filtering by switching the **On/Off** toggle, and define the filtering options:

- **Dates:** filters contacts, calls, messages, user chats, secret chats, group chats, channels, bots and attachments by the date range
- **Call type:** filters calls by type (**Incoming** or **Outgoing**)
- **Call status:** filters calls by status (**Accepted** or **Missed**)
- **Message type:** filters messages by type (**Attachment**, **Call**, **Contact**, **Gif**, **Link**, **Location**, **Poll**, **Sticker**, **System**, **Text**, **Video Message**, or **Voice Message**)
- **Attachment type:** filters attachments by type (**Camera Roll**, **File**, **Gif**, **Image**, **Sticker**, **Video**, or **Voice Message**)
- **Show only blocked contacts**
- **Show only muted contacts**
- **Show only forwarded messages**
- **Show only saved messages**
- **Show only blocked user chats, secret chats**
- **Show only muted user chats, secret chats, group chats, channels, bots**
- **Show only pinned group chats, channels, bots**
- **Show only archived group chats, channels, bots**

#### 4.4.22 Voice Memos

This plugin allows you to explore the Voice Memos app data such as records and information about them.

*NOTE: This plugin is available for iOS 3.1.3 - 12 and higher iCloud and iTunes backups, iOS device images, and iCloud synced data (iOS 12 and higher, MacOS 10.14 and higher, watchOS 6, and iPadOS 13).*

In the grid, you can view the following information:

- **Date and time (including the time zone)** when the voice memo was recorded
- **Unique ID** of the voice memo
- **Custom label** which contains the recording date
- **Duration** of the voice memo

To listen to the required voice memo, click  near the recording date in the **Custom label** column.

All voice memos are displayed in a grid. The most recent voice memos are displayed on top. The general information about voice memos is displayed above the grid:

- **Records:** total number of voice memos
- **Most recent:** date and time when the most recent voice memo was recorded
- **Oldest:** date and time when the oldest voice memo was recorded

If the filtering is on, you can also view the statistic information on the filtered voice memos:

- **Shown (filtered):** number of voice memos that match the filtering criteria.
- **Most recent filtered:** date and time of when the most recent voice memo (among the filtered records) was recorded
- **Oldest filtered:** date and time when the oldest voice memo (among the filtered records) was recorded

To sort the voice memos in the grid, click the necessary column header.

The screenshot shows the Elcomsoft Phone Viewer application window. The title bar reads "Elcomsoft Phone Viewer" and the menu bar includes "File", "View", and "Help". The main window has a "Voice Memos" header with a red waveform icon. Below the header is a search bar and an "Export..." button. A summary box shows "Records: 164", "Most recent: 18.07.2019 16:35:47", and "Oldest: 25.03.2019 17:16:18". A table lists the voice memos with the following columns: Date, Unique ID, Custom label, and Duration. Each row includes a "Play" button. The table is sorted by Date in descending order.

Date	Unique ID	Custom label	Duration
04.04.2019 15:16:32 ...	D142891F-5292-4982-8786-1...	04.04.2019, 15:16	00:10:27
04.04.2019 13:25:26 ...	3CB80D59-E9CC-4CB5-9851-E...	04.04.2019, 13:25	00:02:00
04.04.2019 13:25:26 ...	A96E9AE5-087E-4A69-AB27-...	04.04.2019, 13:25	00:02:00
26.03.2019 17:59:53 ...	38311158-3360-446E-8511-E...	26.03.2019, 17:59	00:00:04
26.03.2019 17:59:53 ...	5BDD2745-B611-4D0B-9A86-...	26.03.2019, 17...	00:00:04
26.03.2019 17:59:46 ...	467F5889-6018-4999-87EE-0...	26.03.2019, 17:59	00:00:05
26.03.2019 17:59:46 ...	61129057-15A4-4C05-A550-4...	26.03.2019, 17...	00:00:05
26.03.2019 17:59:38 ...	31B02C14-3CDD-4B66-8531-E...	26.03.2019, 17:59	00:00:05
26.03.2019 17:59:38 ...	A79F3A97-D295-4F03-A665-D...	26.03.2019, 17:59	00:00:05
25.03.2019 19:29:28 ...	08452CA2-089F-4598-846F-B...	25.03.2019, 19:29	00:00:10
25.03.2019 19:29:28 ...	79D1E388-7A74-43EA-811D-...	25.03.2019, 19...	00:00:10
25.03.2019 19:29:21 ...	83ADD647-EDAB-4201-96FF-...	25.03.2019, 19...	00:00:05
25.03.2019 19:29:21 ...	EA473286-4C83-48BA-B952-D...	25.03.2019, 19:29	00:00:05
25.03.2019 19:29:10 ...	71217620-3849-4E02-8883-C...	25.03.2019, 19:29	00:00:05
25.03.2019 19:29:10 ...	FB0906A0-23B0-441C-B487-A...	25.03.2019, 19:29	00:00:05
25.03.2019 17:16:30 ...	B83352C2-F79E-4EE5-B9FC-4...	25.03.2019, 17...	00:00:05

### Exporting Voice Memos Data

To export data, do the following:

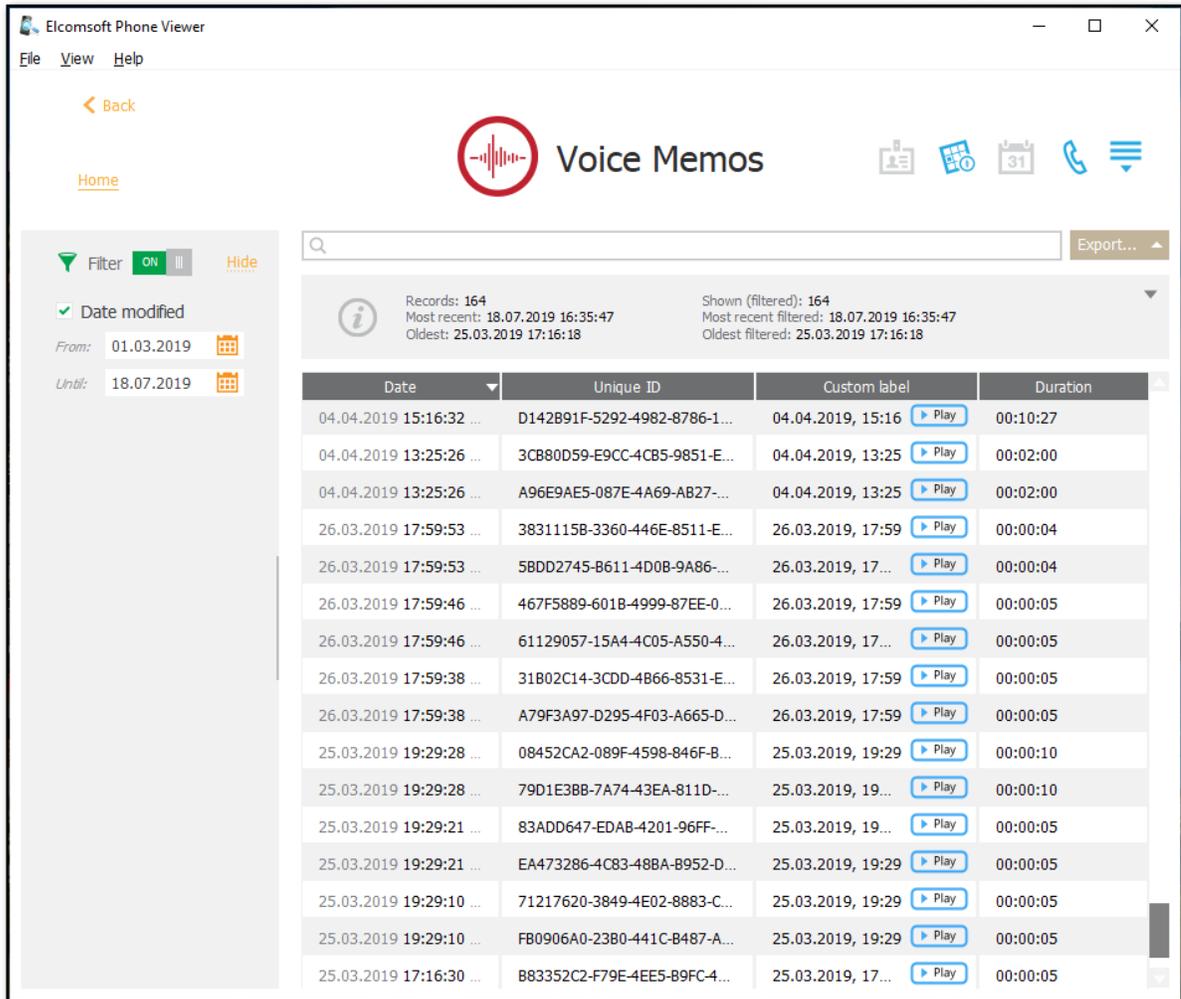
1. Click **Export**.
2. Select one of the following values from the drop-down list: **Filtered** or **All**.
3. The **Select destination file** window opens.
4. In the opened window, select the location in which the file with exported data will be saved and enter the file name.
5. Click **Save**.
6. The **<file name>.xlsx** file is saved in the selected location.

### Searching and Filtering

To perform searches in **Voice Memos**, enter the search request in the search field and press **Enter**. The search results will be highlighted in yellow. The number of search results will be displayed in the search field.

To filter out the voice memos, open the **Filter** pane by clicking the  icon on the left.

Enable filtering by switching the **On/Off** toggle, select the **Date modified** check box, and then select the **From** and **Until** dates in the calendar fields.



The screenshot displays the 'Voice Memos' section of the Elcomsoft Phone Viewer application. The interface includes a search bar at the top, a filter pane on the left, and a list of voice memos. The filter pane shows 'Filter ON' and 'Date modified' checked, with 'From' and 'Until' date pickers set to 01.03.2019 and 18.07.2019 respectively. The list of memos is as follows:

Date	Unique ID	Custom label	Duration
04.04.2019 15:16:32 ...	D142B91F-5292-4982-8786-1...	04.04.2019, 15:16	00:10:27
04.04.2019 13:25:26 ...	3CB80D59-E9CC-4CB5-9851-E...	04.04.2019, 13:25	00:02:00
04.04.2019 13:25:26 ...	A96E9AE5-087E-4A69-AB27-...	04.04.2019, 13:25	00:02:00
26.03.2019 17:59:53 ...	3831115B-3360-446E-8511-E...	26.03.2019, 17:59	00:00:04
26.03.2019 17:59:53 ...	5BDD2745-B611-4D0B-9A86-...	26.03.2019, 17:...	00:00:04
26.03.2019 17:59:46 ...	467F5889-6018-4999-87EE-0...	26.03.2019, 17:59	00:00:05
26.03.2019 17:59:46 ...	61129057-15A4-4C05-A550-4...	26.03.2019, 17:...	00:00:05
26.03.2019 17:59:38 ...	31B02C14-3CDD-4B66-8531-E...	26.03.2019, 17:59	00:00:05
26.03.2019 17:59:38 ...	A79F3A97-D295-4F03-A665-D...	26.03.2019, 17:59	00:00:05
25.03.2019 19:29:28 ...	08452CA2-089F-4598-846F-B...	25.03.2019, 19:29	00:00:10
25.03.2019 19:29:28 ...	79D1E38B-7A74-43EA-811D-...	25.03.2019, 19:...	00:00:10
25.03.2019 19:29:21 ...	83ADD647-EDAB-4201-96FF-...	25.03.2019, 19:...	00:00:05
25.03.2019 19:29:21 ...	EA473286-4C83-48BA-B952-D...	25.03.2019, 19:29	00:00:05
25.03.2019 19:29:10 ...	71217620-3849-4E02-8883-C...	25.03.2019, 19:29	00:00:05
25.03.2019 19:29:10 ...	FB0906A0-23B0-441C-B487-A...	25.03.2019, 19:29	00:00:05
25.03.2019 17:16:30 ...	B83352C2-F79E-4EE5-B9FC-4...	25.03.2019, 17:...	00:00:05

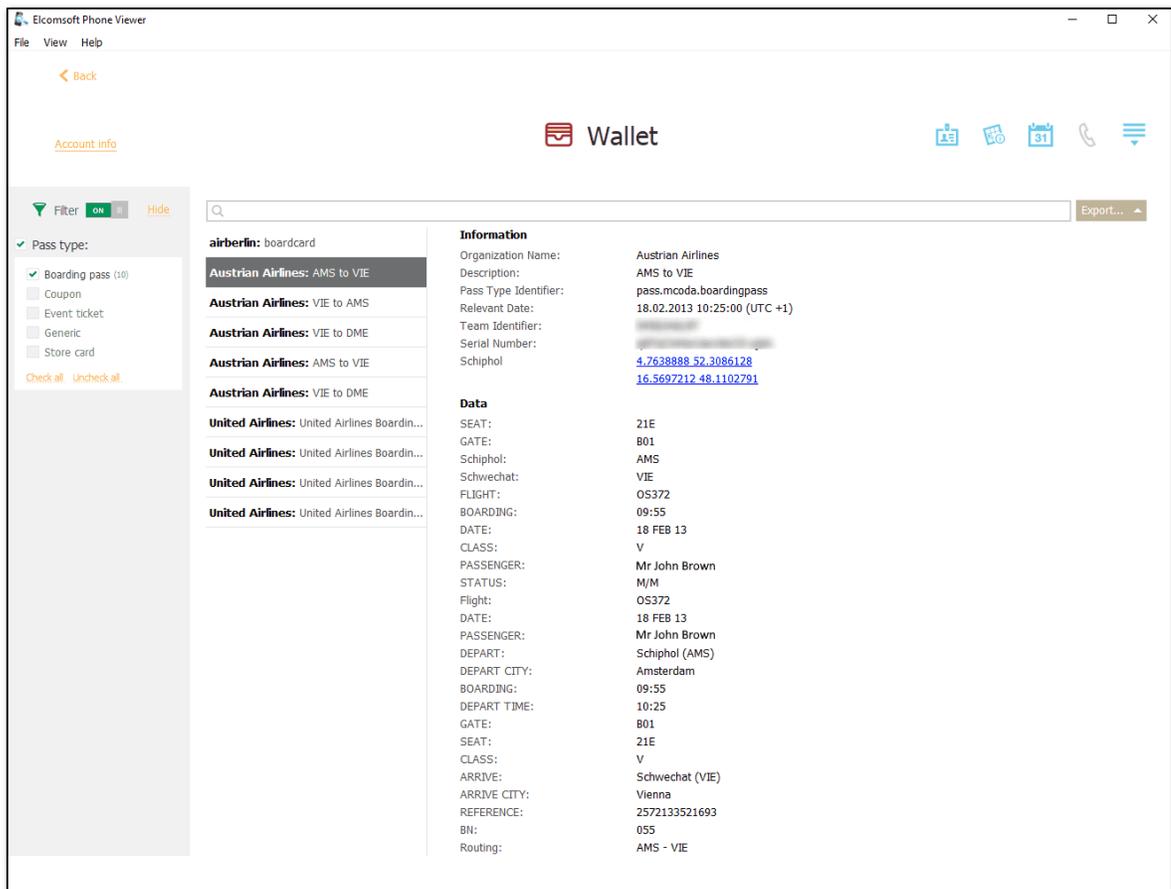
#### 4.4.23 Wallet

The **Wallet** plugin allows you to explore information about the user's passes from the Apple Wallet application.

*NOTE: This plugin is available for iOS device images, iOS backups, and iCloud synced data.*

In the **Information** section, you can view the generic information about the selected user's pass.

In the **Data** section, you can view detailed information about the selected pass. Depending on the type of the selected pass, different data are available.



## Searching and Filtering

To perform searches in **Wallet**, enter the search request in the search field and press **Enter**. The search results will be highlighted in yellow.

To filter out the passes, open the **Filter** pane by clicking the  icon on the left.

Enable filtering by switching the On/Off toggle and select **Pass type**, and then select the pass types:

- Boarding pass
- Coupon
- Event ticket
- Generic
- Store card
- Payment card (for iOS backup images only)

## Exporting

To export information on passes, do the following:

1. Click **Export**.
2. Select one of the following values from the drop-down list: **Filtered** or **All**.

3. The **Select destination file** window will open.
4. In the opened window, select the location in which the file with exported information on passes will be saved, enter the file name and select the file extension (.xml or .xlsx).
5. Click **Save**.
6. The file is saved in the selected location.

#### 4.4.24 Web

EPV allows you to explore the user's Internet activity.

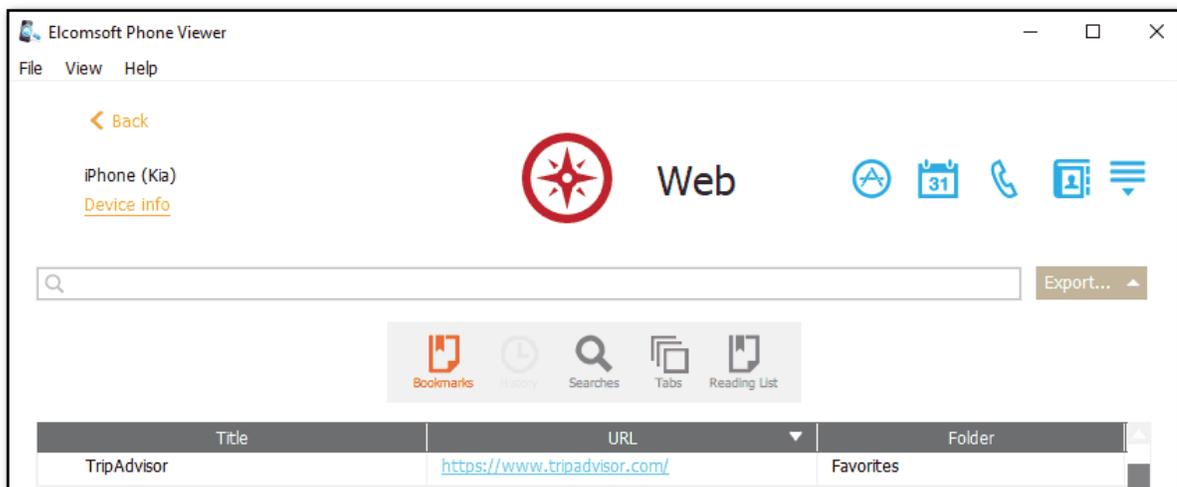
- **For iOS backups**, the data is taken from the Safari browser and includes bookmarks, browsing history, twenty most recent search queries, and tabs of the visited pages.
- **For BlackBerry backups**, the data is taken from the standard Internet browser and includes bookmarks, browsing history, and autofills.
- **For Microsoft account data**, the data is taken from the Edge browser and includes browsing and search history.

*Please note that if the timezone of the device is not detected, the time for all web data will be displayed in UTC time and the corresponding warning will be displayed in the Journal of the View menu.*

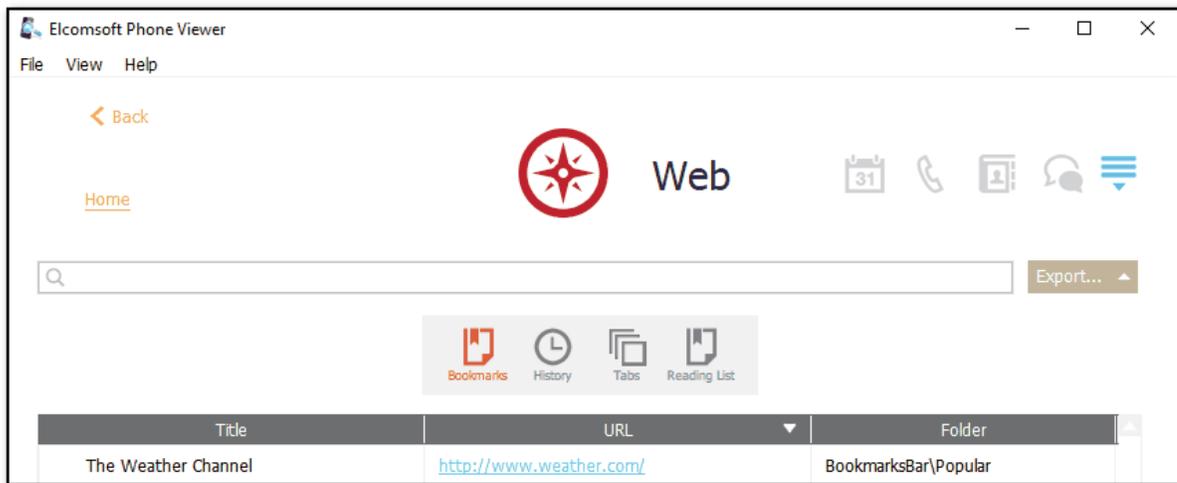
#### Viewing Bookmarks

For bookmarks, the following information is displayed:

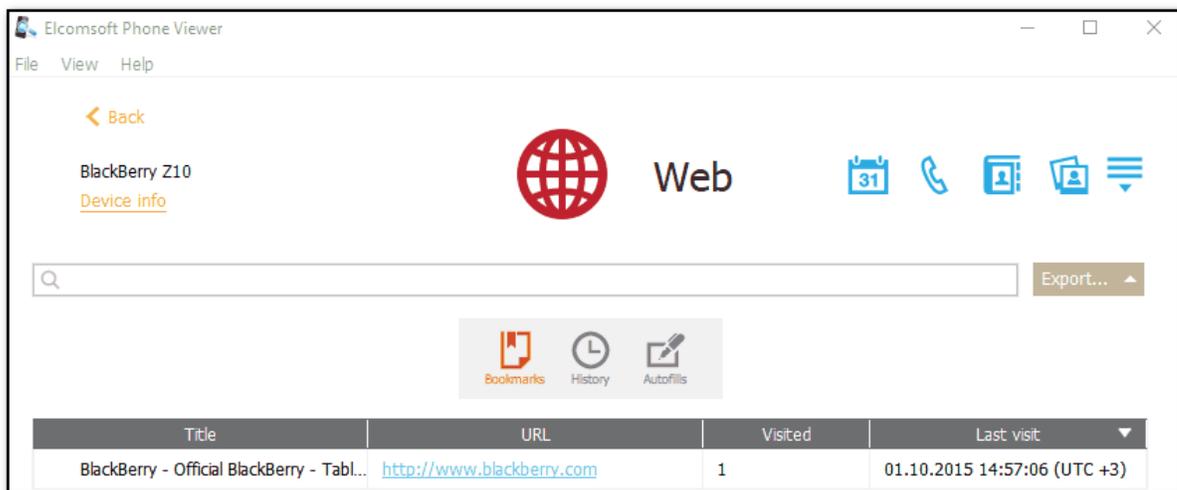
- **iOS backups:** Title, URL, Folder, Status (Actual or Deleted)



- **iCloud synced data:** Title, URL, Folder.



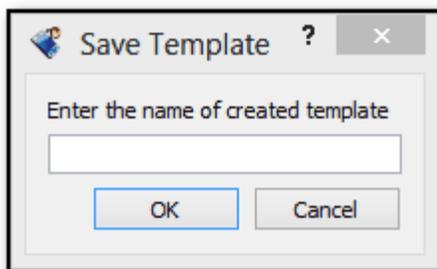
- **BlackBerry backups:** Title, URL, Visited, Last visit (including the time zone).



### Viewing History

For browsing history, the following information is displayed:

- **iOS backups:** Date (including the time zone), Title, URL, Visits, Status (Actual or Deleted).



- **iCloud synced data:** Date, Title, URL, Visits, Status (Actual or Deleted), Deleted date

Please note that the **Deleted** status marks the records actually deleted from Safari History by the user. The date and time the record was deleted is displayed in the Deleted date column. The **Actual** status marks the actual records and the older records which are not synched with the data on the device.

The screenshot displays the Elcomsoft Phone Viewer application window. The main interface shows a web browser with a search bar and navigation buttons. A sidebar on the left contains filters for Date and Status. The Status filter is checked for both 'Actual' and 'Deleted'. The main area displays a table of browsing history records.

Date	Title	URL	Visits	Status	Deleted date
31.01.2017 10:38:45	SoundCloud – Hear...	<a href="https://soundcloud...">https://soundcloud...</a>	1	Actual	
30.01.2017 18:02:22	SoundCloud – Hear...	<a href="https://soundcloud...">https://soundcloud...</a>	1	Actual	
30.01.2017 18:02:16	New Cars, Trucks, ...	<a href="http://touch.toyot...">http://touch.toyot...</a>	2	Actual	
30.01.2017 18:02:09	toyota - Google Se...	<a href="https://www.goog...">https://www.goog...</a>	3	Actual	
30.01.2017 18:01:04	Sea - Wikipedia, th...	<a href="https://en.m.wikip...">https://en.m.wikip...</a>	3	Deleted	31.01.2017 15:09:17
30.01.2017 16:28:47		<a href="https://www.goog...">https://www.goog...</a>	2	Deleted	31.01.2017 15:09:17
30.01.2017 16:28:44	sea - Google Search	<a href="https://www.goog...">https://www.goog...</a>	3	Deleted	31.01.2017 15:09:17
30.01.2017 16:28:43	(1) Facebook	<a href="https://www.face...">https://www.face...</a>	1	Actual	
30.01.2017 16:28:43	Facebook	<a href="https://www.face...">https://www.face...</a>	1	Actual	
25.01.2017 19:22:45		<a href="https://www.face...">https://www.face...</a>	4	Deleted	31.01.2017 15:09:17

- **BlackBerry backups:** Last visited (including the time zone), Title, URL, Visited.

Elcomsoft Phone Viewer

File View Help

BlackBerry Z10  
Device info

Web

Filter ON Hide

Date:

From: 01.10.2015

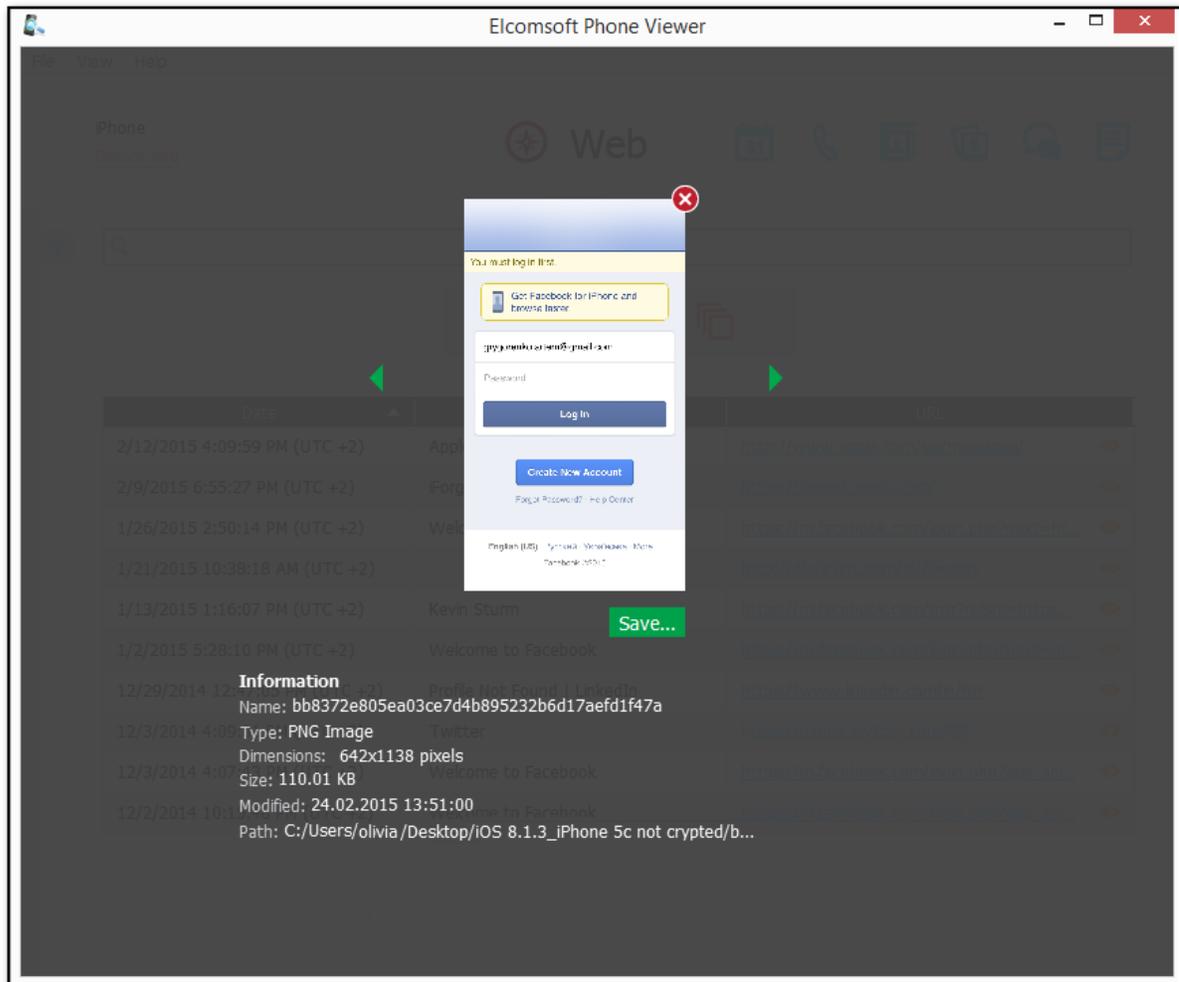
Until: 30.12.2015

Records: 90  
Most recent record: 30.12.2015 20:15:03 (UTC +2)  
Oldest record: 02.12.2015 12:00:27 (UTC +2)

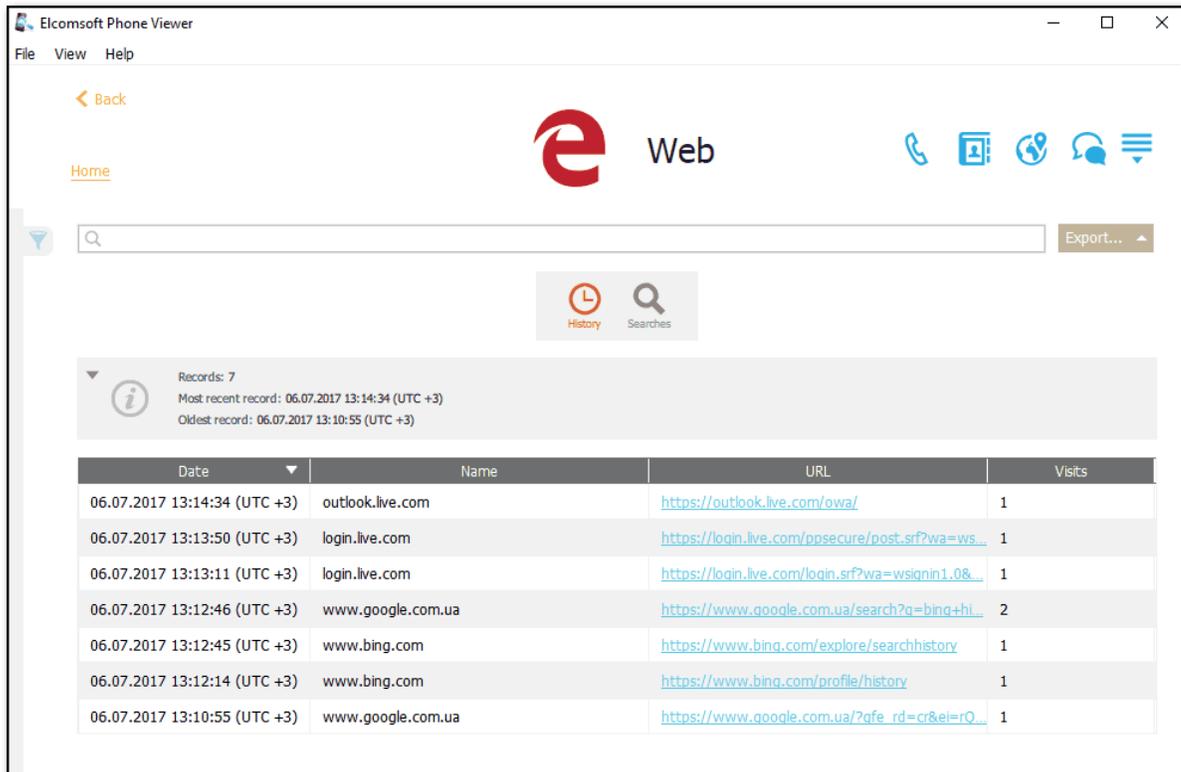
Shown records: 9  
Most recent filtered record: 30.12.2015 18:15:03 (UTC +2)  
Oldest filtered record: 02.12.2015 10:00:27 (UTC +2)

Last visited	Title	URL	Visited
30.12.2015 17:07:23 (UTC +2)	Google+	<a href="https://plus.google.com/app/...">https://plus.google.com/app/...</a>	1
18.12.2015 12:16:01 (UTC +2)	Google+	<a href="https://plus.google.com/app/...">https://plus.google.com/app/...</a>	1
18.12.2015 12:16:00 (UTC +2)	Google+	<a href="https://plus.google.com/app/...">https://plus.google.com/app/...</a>	1
18.12.2015 10:20:20 (UTC +2)	Google+	<a href="https://plus.google.com/app/...">https://plus.google.com/app/...</a>	1
18.12.2015 10:20:17 (UTC +2)	Google+	<a href="https://plus.google.com/app/...">https://plus.google.com/app/...</a>	1
18.12.2015 10:20:09 (UTC +2)	Google+	<a href="https://accounts.google.com...">https://accounts.google.com...</a>	1
18.12.2015 10:19:58 (UTC +2)	Google+	<a href="https://accounts.google.com...">https://accounts.google.com...</a>	1
18.12.2015 10:19:57 (UTC +2)	Google+	<a href="https://accounts.google.com...">https://accounts.google.com...</a>	3
02.12.2015 10:02:23 (UTC +2)	Google+	<a href="https://accounts.google.com...">https://accounts.google.com...</a>	3

You can also view the thumbnails of the visited pages when working with BlackBerry backups. To view the thumbnail, click the **Show thumbnail** icon  next to the URL. The thumbnail opens in the viewer where you can also view its properties: Name, Type, Dimensions, Size, Modified, Path. To save the thumbnail to your computer, click **Save**, define the destination folder in the opened window, and then click **Save**.



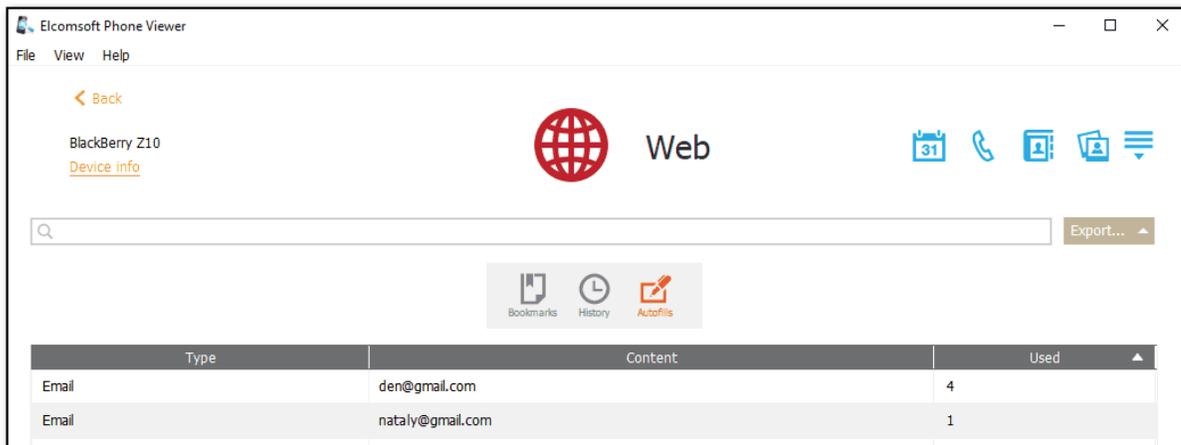
- **Microsoft account data:** Date (including the time zone), Name, URL, Visits.



### Viewing Autofills

When working with BlackBerry backups, you can view the following information about the autofill data:

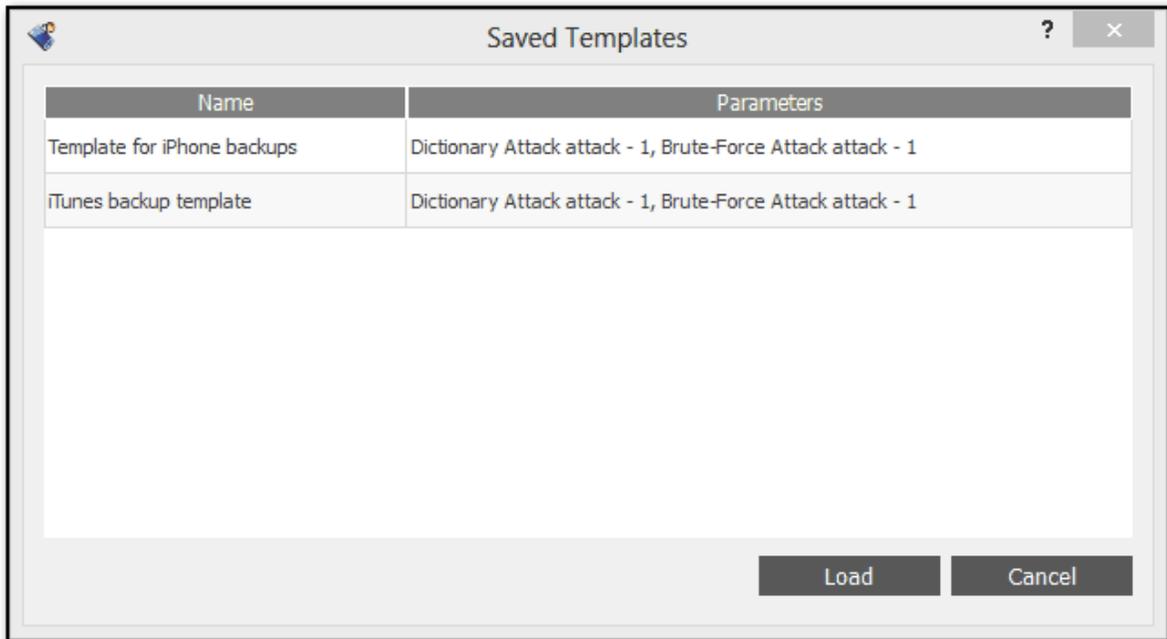
- Type
- Content
- Used



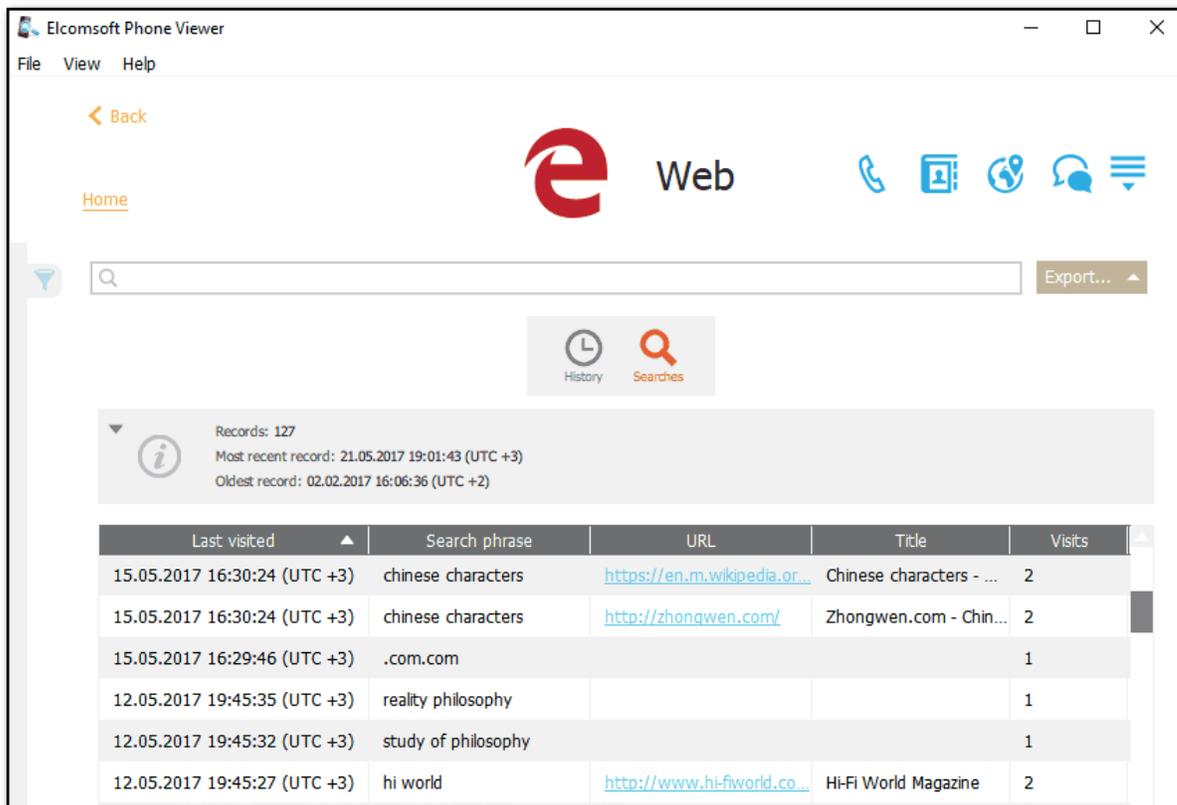
### Viewing Search History

For search history, the following information is displayed:

- **iOS backups:** Last visited (date and time including the time zone) and search phrases.



- **For Microsoft account data:** Last visited (date and time including the time zone), Search phrase, URL, Title, Visits.



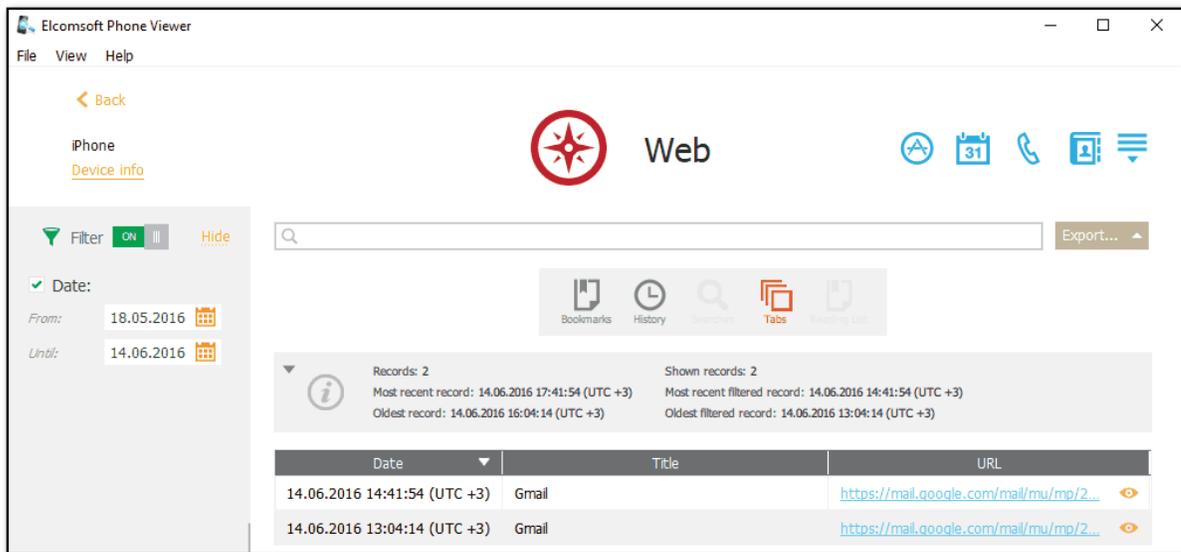
## Viewing Tabs

For viewed tabs, you can see the following information:

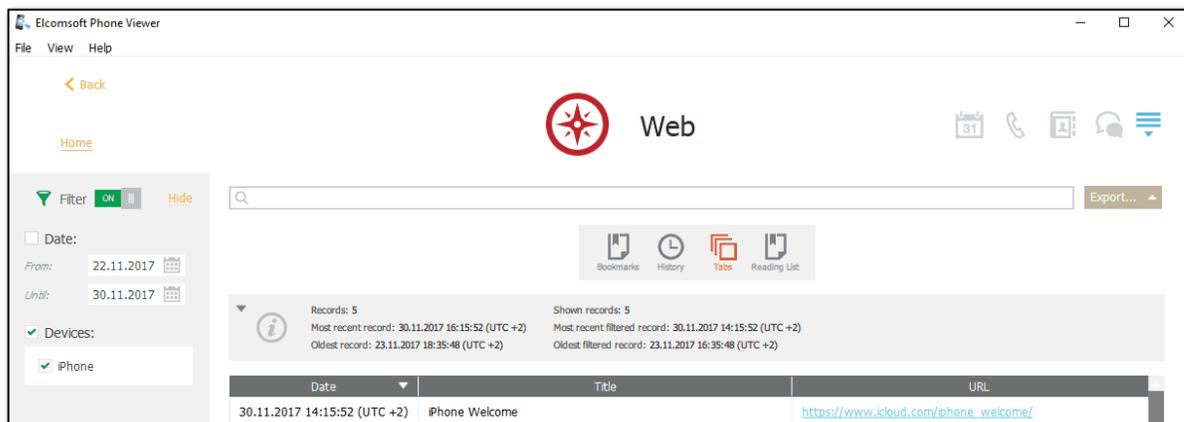
- **iOS backups:** Date, Title, URL, Status (Actual or Deleted)

To view the thumbnail, click the **Show thumbnail** icon  on the right. The thumbnail opens in the viewer where you can also view its properties: Name, Type, Dimensions, Size, Modified, Path.

To save the thumbnail to your computer, click **Save**, define the destination folder in the opened window, and then click **Save**.



- **iCloud synced data:** Date, Title, URL, Device.



## Viewing Deleted Web Data

EPV allows you to view the following deleted web data from the different iOS backups:

- Bookmarks
- History

- Tabs
- Reading List

The deleted web data is available in the backups from the devices with the following iOS versions:

	Bookmarks	History	Tabs	Reading List
iTunes backup	iOS 7–12	iOS 8–11	iOS 10–11	iOS 7–12
iCloud backup	iOS 7–12	iOS 8–11	iOS 10–11	iOS 7–12
iOS device image	iOS 7–12	iOS 8–11	iOS 10–11	iOS 7–12

**Note:** The deleted web data is marked as **Deleted** in the **Status** column of the corresponding category table.

### Exporting Web Data

To export data, do the following:

1. Click **Export**.
2. Select one of the following values from the drop-down list: **Filtered** or **All**.
3. The **Select destination file** window opens.
4. In the opened window, select the location in which the file with exported data will be saved and enter the file name.
5. Click **Save**.
6. The **<file name>.xlsx** file is saved in the selected location.

### Searching and Filtering

To perform searches in **Web**, enter the search request in the search field and press **Enter**. The search results will be highlighted in yellow.

To filter out the web data, open the **Filter** pane by clicking the  icon on the left.

Enable filtering by switching the On/Off toggle and select the **From** and **Until** dates in the corresponding calendar fields.

For iCloud synced Safari History, as well as for Safari Bookmarks, History, Tabs, and Reading List from iOS backups, you can also filter out **Actual** or **Deleted** records.

#### 4.4.25 Wi-Fi

The **Wi-Fi** plugin allows you to explore the information on detected and saved Wi-Fi connections.

*NOTE: This plugin is only available for iOS 7.x.x - 13 backups of the following types: iCloud, iCloud sync, and iTunes (encrypted, not encrypted, and backups with restored and not restored file names).*

When opening the plugin, you have an option to download the locations and addresses of the Wi-Fi connections. Please note that the Internet connection is required to get the locations and addresses for the first time. After the Wi-Fi location data is downloaded, it is saved to local cache.

The following information is available on each connection:

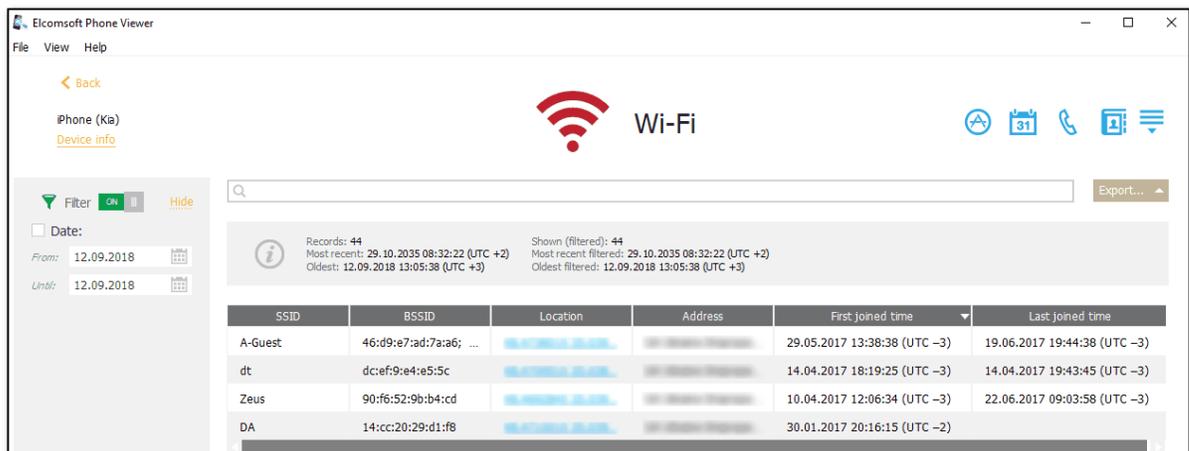
- SSID: name of connection
- BSSID: MAC address
- Location: location coordinates of the Wi-Fi point
- Address: address of the Wi-Fi point

- Synced by (for iCloud synced data): name of the device associated with the connection
- Encryption (for iTunes backups): encryption type (e.g., WPA2 Personal)
- First joined time (for iTunes backups): date and time of first connection to Wi-Fi. The time corresponds to the time zone of the backup
- Last joined time (for iTunes backups): date and time of the most recent connection to Wi-Fi. The time corresponds to the time zone of the backup
- Wi-Fi Password: password of the Wi-Fi network (you can click the  icon next to the password to view the characters)

*NOTE: This column is displayed only for encrypted backups.*

Please note that for iOS 7 backups only the information about the most recent connection is available.

All connections are displayed in a grid. The record with the most recent Last joined time is displayed on top.



## Exporting

To export information on Wi-Fi connections, do the following:

1. Click **Export**.
2. Select one of the following values from the drop-down list: **Filtered** or **All**.
3. The **Select destination file** window will open.
4. In the opened window, select the location in which the file with exported information on Wi-Fi connections will be saved and enter the file name.
5. Click **Save**.
6. The **<file name>.xlsx** file is saved in the selected location.

## Searching and Filtering

You can perform searches for connections by name of connection (SSID) and MAC address (BSSID). **To perform searches in Wi-Fi**, enter the necessary value in the search field and press **Enter**. The search results will be highlighted in yellow. The number of search results will be displayed in the search field.

You can filter the connections by last joined time.

**To filter the records**, open the **Filter** pane by clicking the  icon on the right.

---

Enable filtering by switching the **On/Off** toggle, select the **Date** check box, and then select the **From** and **Until** dates in the calendar fields.

For iCloud synced connections, you can filter the data by device's name. Select the **Device** check box, and then select the devices names.

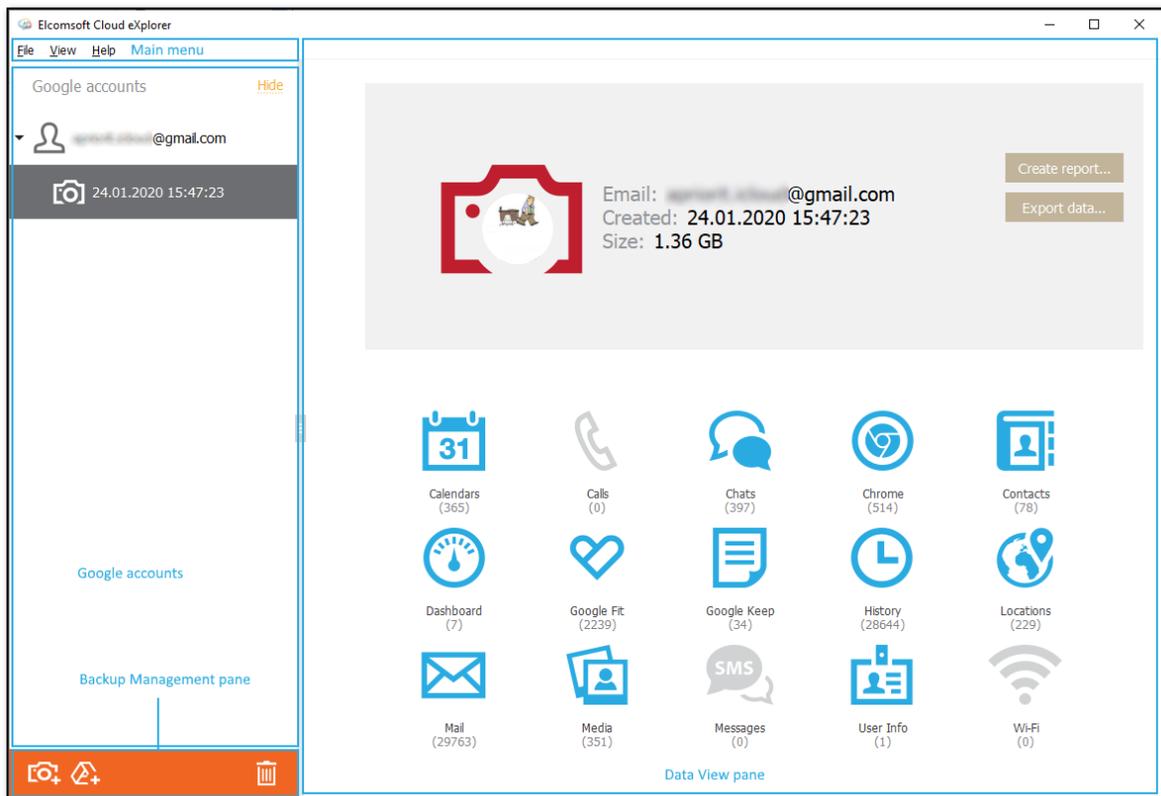
## 5 Elcomsoft Cloud Explorer

### 5.1 ECX Program information

#### 5.1.1 ECX Program interface

The Elcomsoft Cloud eXplorer interface consists of the following elements:

- **Main menu:** Provides access to the main functionality of ECX:
  - **File:** Allows downloading Google backups and removing them from the backup list.
  - **View:** Allows viewing records of all actions performed with data in ECX in the form of a Journal, defining ECX settings, and viewing the device info once the Google account data is loaded. It also provides access to all available plugins.
    - **Help:** Allows viewing the ECX version number, checking if the program is registered or not, reading ECX 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.
- **Data View pane:** Allows managing data.
- **Google Accounts pane:** Allows viewing Google backups account and Google Drive backups added to ECX.
- **Backup Management pane:** Allows downloading Google account and Google Drive backups and removing them from the backup list.



## 5.1.2 ECX settings

Elcomsoft Cloud eXplorer allows you to customize working with ECX.

To define ECX Settings, navigate to **View - Settings**.

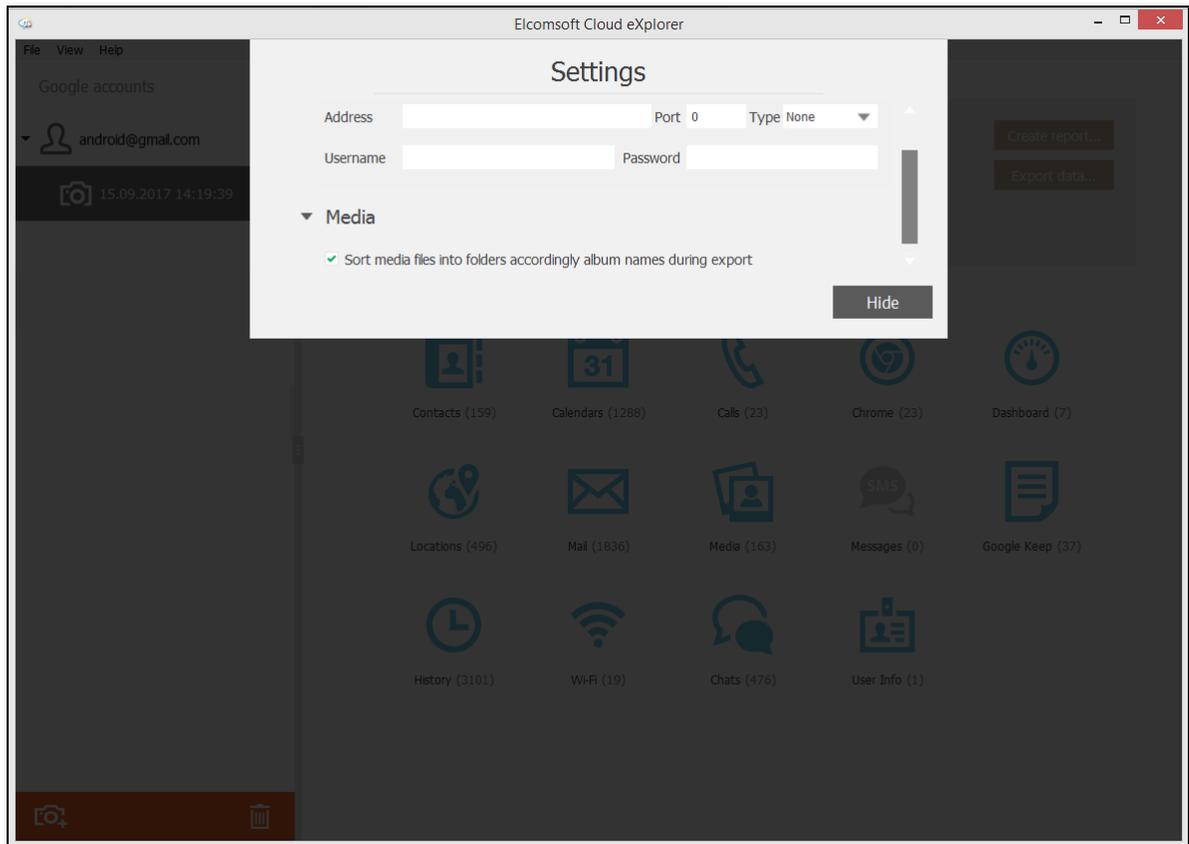
- **Proxy server**

Define the Proxy server that will be used when downloading Google backups.

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

- **Media**

Define whether you want to have media files sorted into folders according to album names during export.



### 5.1.3 Changing path to backup storage

By default, backups generated by ECX are stored in:

- **Windows:** *C:\Users\Username\AppData\Elcomsoft\Elcomsoft Cloud eXplorer\Backups* (insert your system user name instead of *Username*).
- **macOS:** *~/Library/Application Support/Elcomsoft/Elcomsoft Cloud eXplorer/Backups*

To change the backup storage location, do the following:

1. Go to the ECX directory via the following path:

- **Windows:** *C:\Users\Username\AppData\Roaming\Elcomsoft\Elcomsoft Cloud eXplorer* (insert your system user name instead of *Username*).
- **macOS:** *~/Library/Application Support/Elcomsoft/Elcomsoft Cloud eXplorer*

**NOTE:** The AppData folder is hidden by default. Please make sure the hidden folders are displayed in your system.

2. Open the *settings.ini* file in the Elcomsoft Cloud eXplorer folder.

3. In the **Backups** section, after *Path=*, replace the existing path with the desired one. Make sure the path you define does not contain any non-Latin characters.

4. Save the file.
5. Close the file and restart ECX to apply the changes.

Once you have changed the path, all the information stored in the previous location is moved to the new one.

## 5.2 Working with Google account vackups

### 5.2.1 Signing in

To download a Google account backup using ECX, you are required to sign in first. The authentication process may vary depending on the Google account security settings.

**To sign in**, on the **Download snapshot** page, define the authentication type:

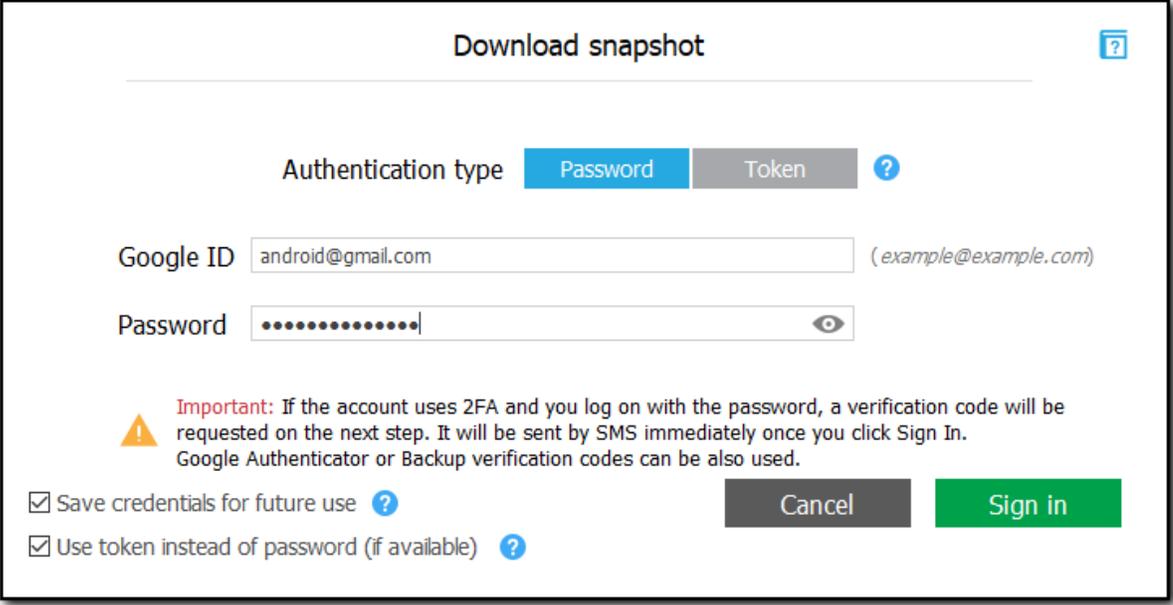
- **Password**: Select this option to use the Google account credentials.
- **Token**: Select this option to use the Authentication token extracted from the Google Chrome browser using Google Token Extractor (GTEX). For more information about extracting the token, see the [Extracting authentication token](#) topic.

#### Signing In Using Credentials

If you sign in using the **Password** option, enter the Google account ID (in the [account@gmail.com](#) format) and the password.

When you sign in with the **Save credentials for future use** option selected, ECX stores an authentication token. To use the token on next sign-in to this account, enter the login and make sure the **Use token instead of password (if available)** option is selected. When signing in with a token, you do not have to use the password or pass two-steps verification (use USB-token, Google Prompt, or enter a secure code).

**NOTE:** ECX doesn't support Google accounts with CAPTCHA protection. You can wait for a while until CAPTCHA protection is turned off and then try to log in again.



The screenshot shows a dialog box titled "Download snapshot" with a help icon in the top right corner. Below the title bar, there are two tabs for "Authentication type": "Password" (selected) and "Token". A question mark icon is next to the "Token" tab. Below the tabs, there are two input fields: "Google ID" with the value "android@gmail.com" and a placeholder "(example@example.com)", and "Password" with a masked field of dots and an eye icon to toggle visibility. Below the input fields, there is an important warning icon and text: "Important: If the account uses 2FA and you log on with the password, a verification code will be requested on the next step. It will be sent by SMS immediately once you click Sign In. Google Authenticator or Backup verification codes can be also used." At the bottom, there are two checkboxes: "Save credentials for future use" (checked) and "Use token instead of password (if available)" (checked). To the right of the checkboxes are two buttons: "Cancel" and "Sign in".

### Signing In Using Authentication Token

If you sign in using the **Token** option, select the previously saved token from the list or specify the path to a new token .xml file extracted from the Google Chrome browser via Google Token Extractor (GTEX). By default, the token file is saved to the folder where the Google Token Extractor is located. For more information about extracting the token, see the [Extracting authentication token](#) topic.

When you sign in with the **Save credentials for future use** option selected, ECX saves the token and you can select it from the list on the next sign in.

**NOTE:** If you sign in using the **Token** option, the following categories will not be available for downloading: **Users Info, Contacts, Locations, Media, Mail, Messages.**

**NOTE:** To download a Google account backup, you can use only tokens extracted from the **Google Chrome browser.**

Download snapshot

Authentication type Password Token ?

Token C:/Program Files (x86)/Elcomsoft Password Recovery/Elcomsoft Cloud eXp...

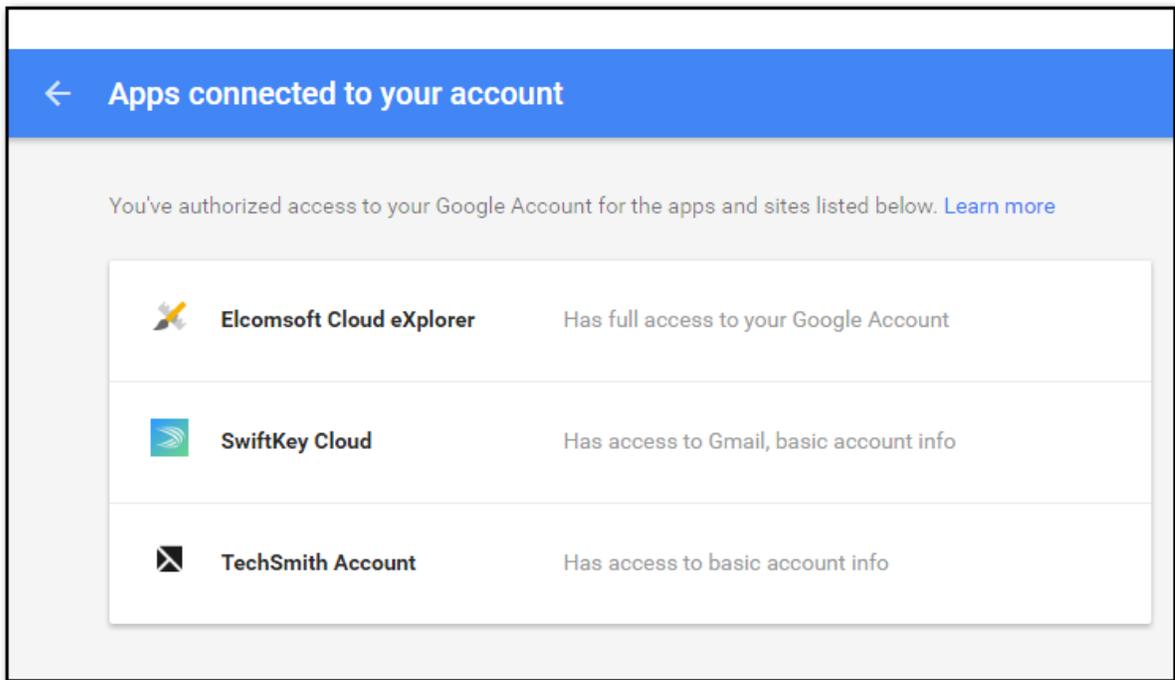
*i* You can only use Google Chrome tokens to download a snapshot.

Save credentials for future use ?

Cancel Sign in

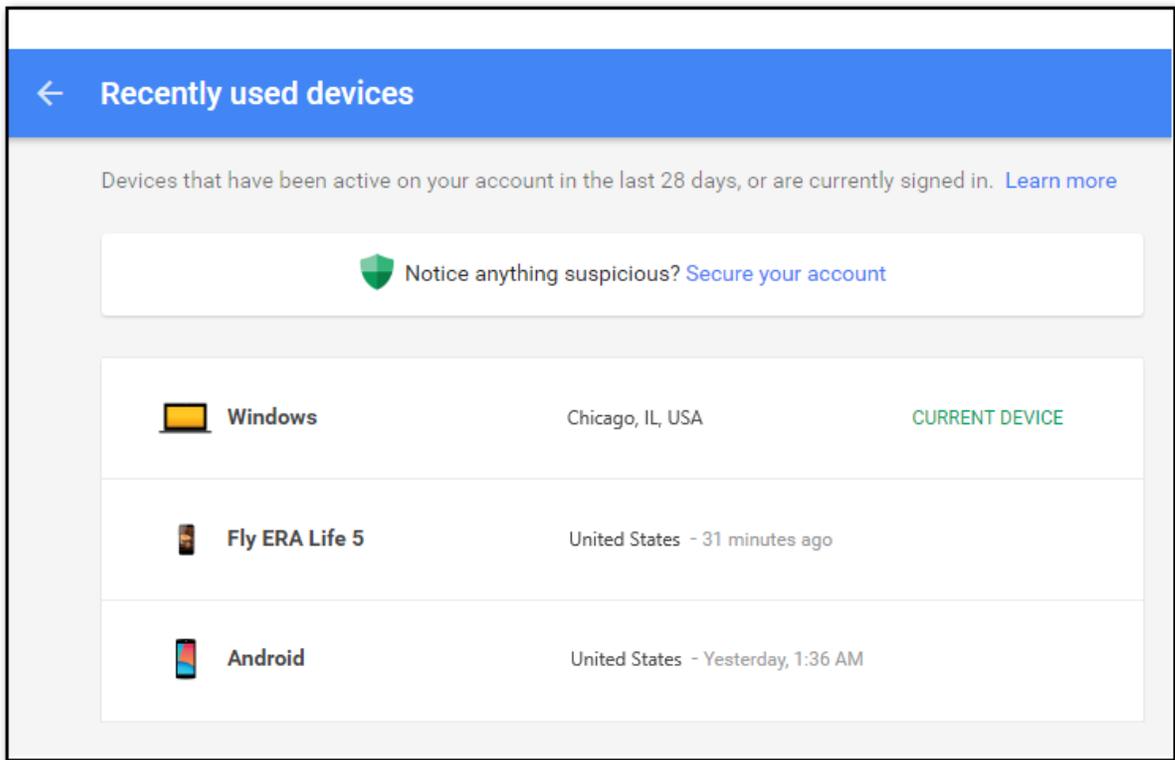
### Security Notifications

When you sign in via ECX, the information on this sign-in is displayed in your Google account (My Account > Sign-in & security > Connected apps & sites > Apps connected to your account). You will see Elcomsoft Cloud eXplorer on the list of apps and sites with authorized access to your account.



If you sign in via ECX using the login and password, you will get email notifications in the Google account you signed into. You will also see an additional notification in your Google account (My Account > Sign-in & security > Device activity & notifications > Recently used devices). You will not see any mentions of the ECX applications, but there will be a Windows or Unknown OS device on the list of devices currently or recently signed in to your account.

If you download data for the Calls and Wi-Fi categories, there will be an Android device on the list of devices currently or recently signed in to your account (My Account > Sign-in & security > Device activity & notifications > Recently used devices).



Also, if you sign in via ECX from an IP address which you haven't previously signed in from, an email notification will be sent to your Gmail account with information on a new sign-in.

## 5.2.2 Google account snapshots

With ECX, you can download information from the account, store it as a backup, and then explore the backup content.

The following data categories are available:

- **User Info:** The Google account user data, including name, account type (person or company), birth date, the URLs to social network profiles, and more.
- **Chats:** Google Hangouts chat history.
- **Contacts:** The Google account user contacts and all available information on them.
- **Google Keep:** The user's notes downloaded from Google Keep.
- **Chrome:** Google Chrome data, including passwords, bookmarks, autofills, and pages transitions.
- **Calendars:** Events planned in Google Calendar, including one time and regular events, birthdays, holidays, etc.
- **Dashboard:** The Google Dashboard content, including, but not limited to:
  - devices associated with the Google account.
  - the Google account.
  - the user's Google search history.
  - the user's activity on YouTube.
  - the user's connected apps.
  - the user's location history and saved places.
  - the user's photos.
  - the user's calendar events and so on.
- **Locations:** The user's location history tracked in the [Google Timeline](#) service.

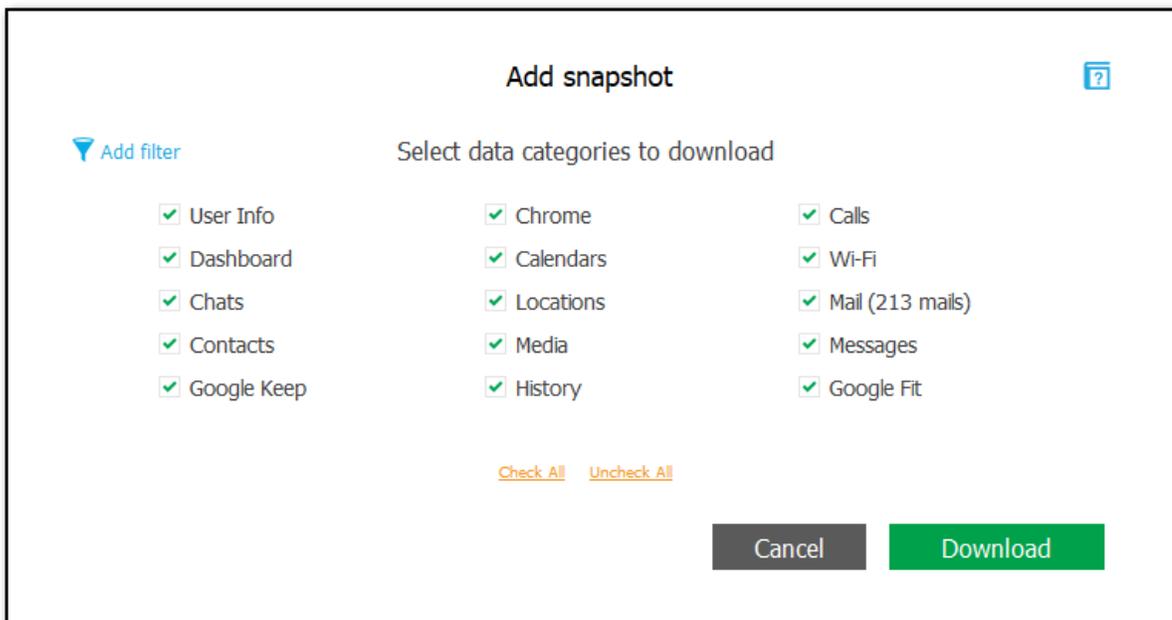
- **Media:** The user's photos stored in Google Photos.
- **History:** The user's Google History information, including search history, search history, YouTube search and watch history, visited web-sites history, and device history.
- **Mail:** The user's email data from Gmail.
- **Wi-Fi:** Information on Wi-Fi connections stored in the user's Google account.
- **Calls:** The information on user's call history stored in the user's Google account.
- **Messages:** The user's text messages stored in the user's Google account.
- **Google Fit:** The user's activity data downloaded from Google Fit.

**NOTE:** The **Wi-Fi**, **Calls**, and **Messages** information will not be downloaded, if Android device (v. 9.0 and higher) is protected by the cryptographic key or passcode.

To download information from the Google account, do the following:

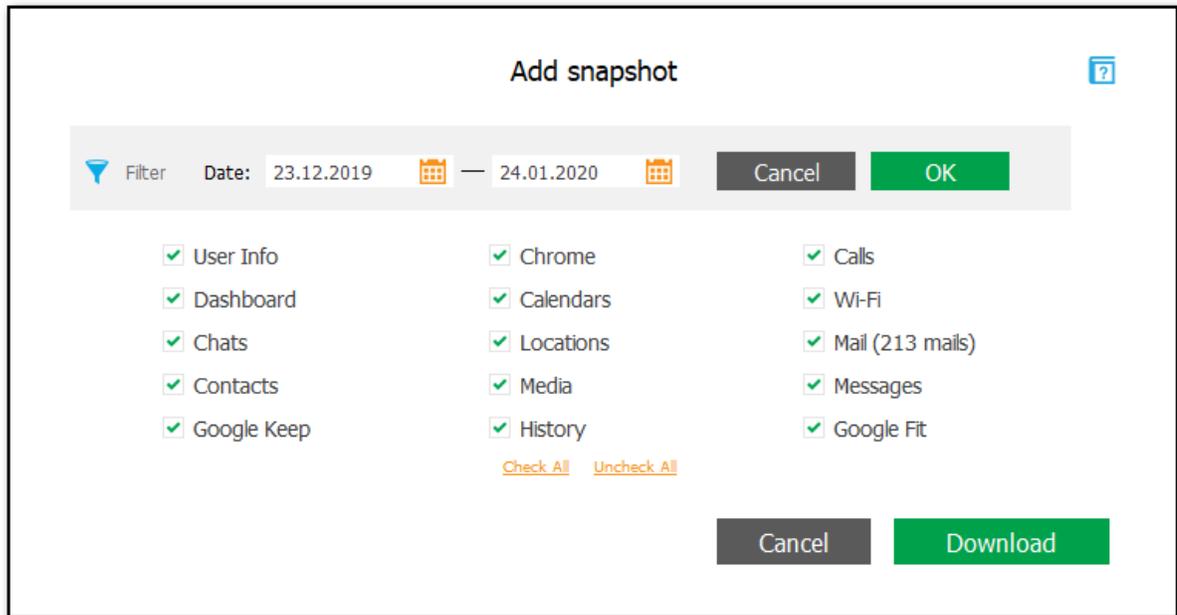
1. In the main menu, click **File**, and then click **Add Google Snapshot**; or click the  button in the bottom-left corner of the ECX screen.
2. On the **Download snapshot** page, define the authentication type:
  - **Password:** Select this option to use the Google account credentials (Google ID (in the [account@google.com](#) format) and password).
  - **Token:** Select this option to use the authentication token extracted from **the Google Chrome browser** using Google Token Extractor (GTEX). For more information about extracting the token, see the [Extracting authentication token](#) topic.
3. Click **Sign in**.
 

**NOTE:** If you have any issues with signing in, please see [Signing in](#).
4. Select the data categories you wish to download.



For the **Mail** and **Media** categories, you can click **Add filter** and then define the time interval for which the data must be downloaded.

To define the time interval, click the  icon in each **Date** field, select the dates from the calendar, and then click **OK**.

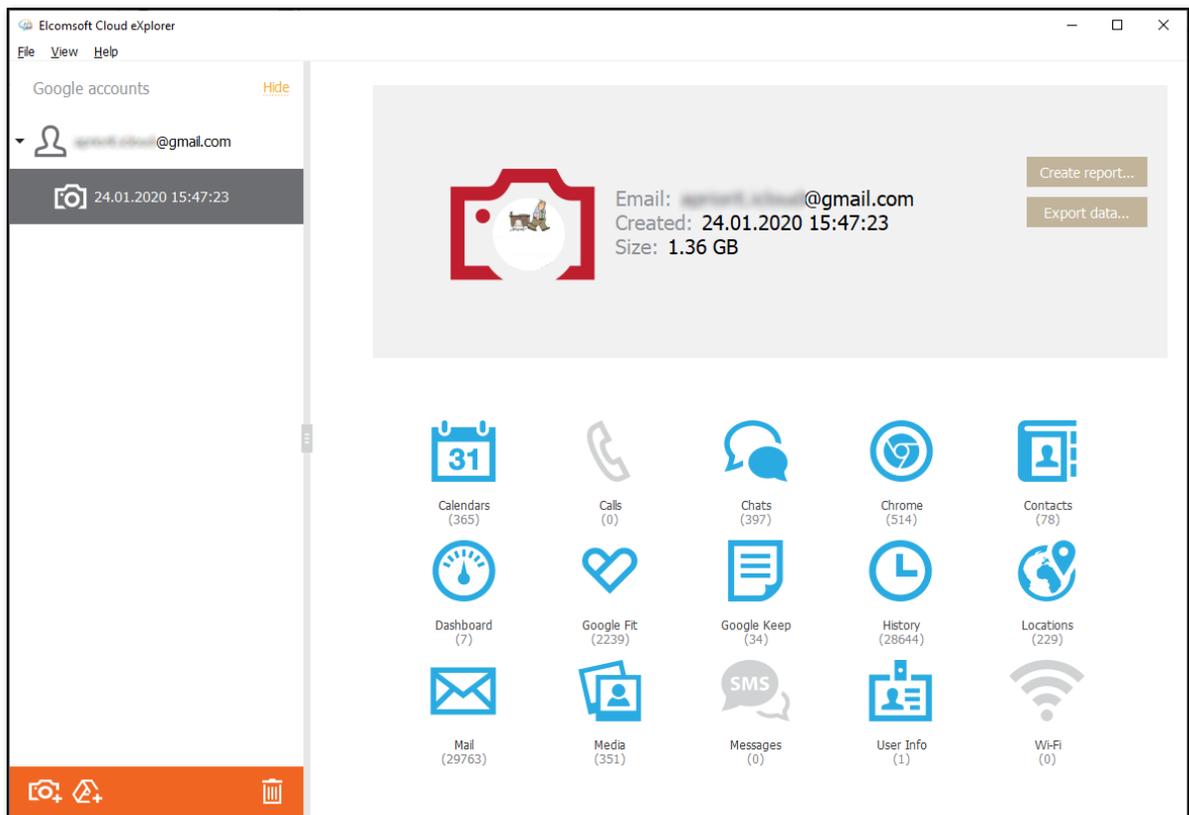


5. Click **Download**.

**NOTE:** Some Chrome data may be encrypted with a passphrase (for more information, please see <https://support.google.com/chrome/answer/1181035?hl=en>). If you select to download the **Chrome** data category, and Chrome information in your Google account is encrypted with a passphrase, ECX requires you to enter this passphrase. If you enter the passphrase, all the Chrome data is downloaded. If you don't enter the passphrase, the encrypted data is not downloaded.

Once the download is completed, you can see the Google account profile and its backup in the **Google Accounts** pane on the left. The backup title consists of its creation date and time. If the Google account has several backups, they are all listed under this Google account.

In the main window, you can see what data categories have been downloaded in each backup, as well as how many records each backup contains. Data categories that were not selected to be downloaded and categories that have no data are displayed in gray.



To explore the backup content, just click the desired backup record.

To remove a Google account profile or a backup, select the desired record and click the  icon in the bottom-right corner of the **Google Accounts** pane, or, in the main menu, select **File**, and then click **Remove Backup**.

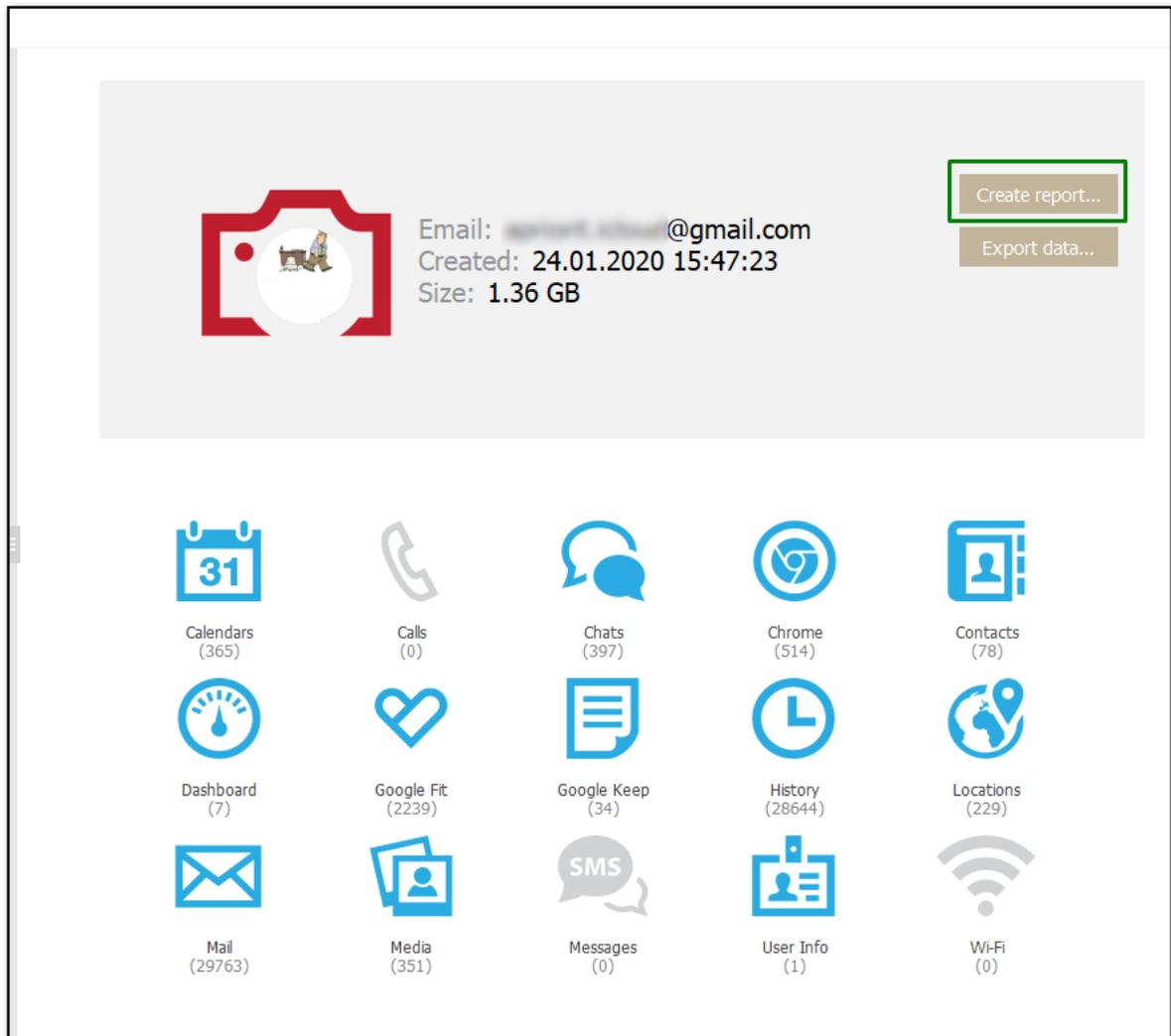
### 5.2.3 Reports

With ECX, you can generate a report on Google account data. The report is generated in **html** format. Along with the report, a folder containing all attachments is created.

Please note that reports are only available in the registered version of the program.

To generate a report, do the following:

1. In the backup information section, click **Create report**.

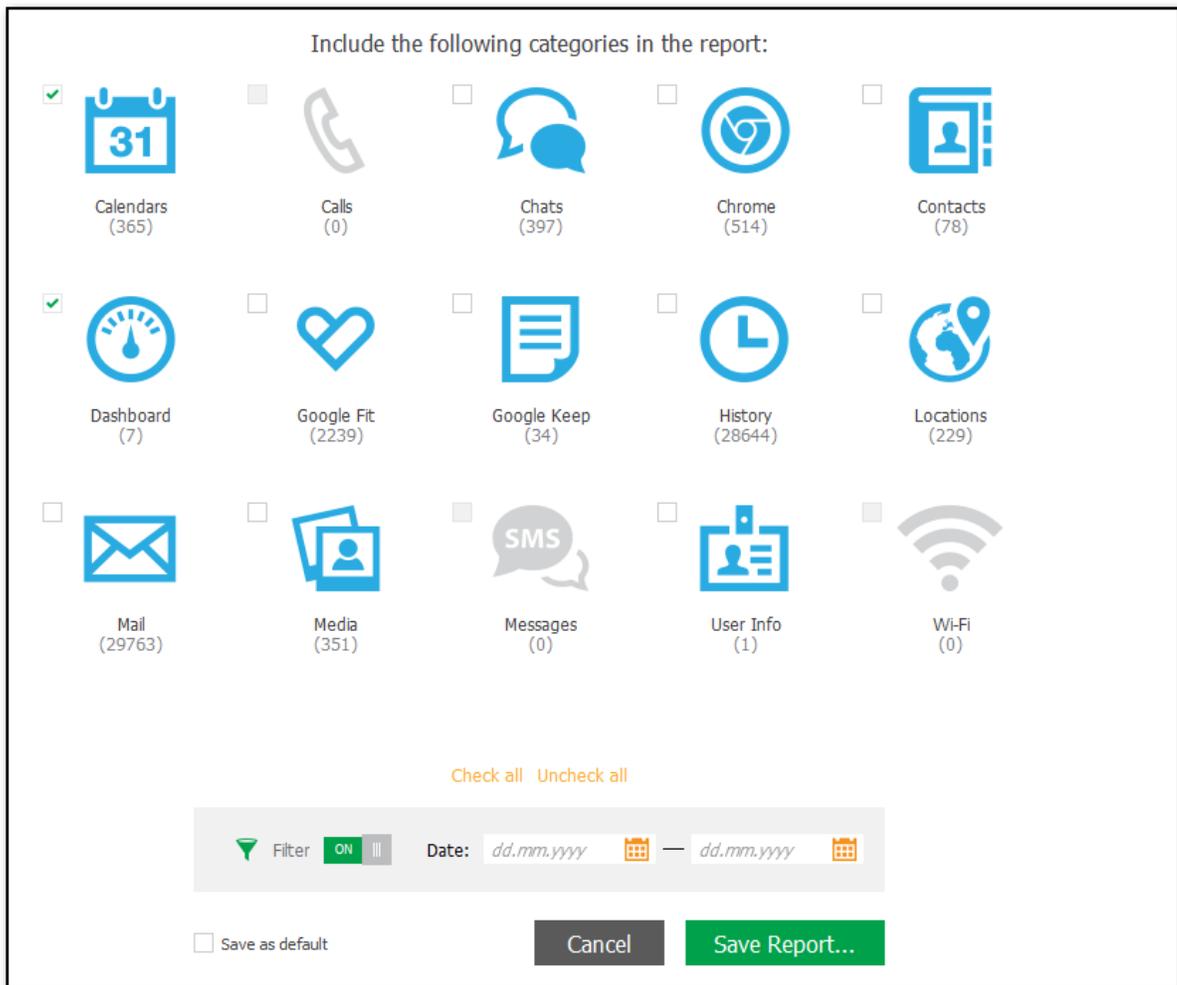


2. Select the data categories to be included.

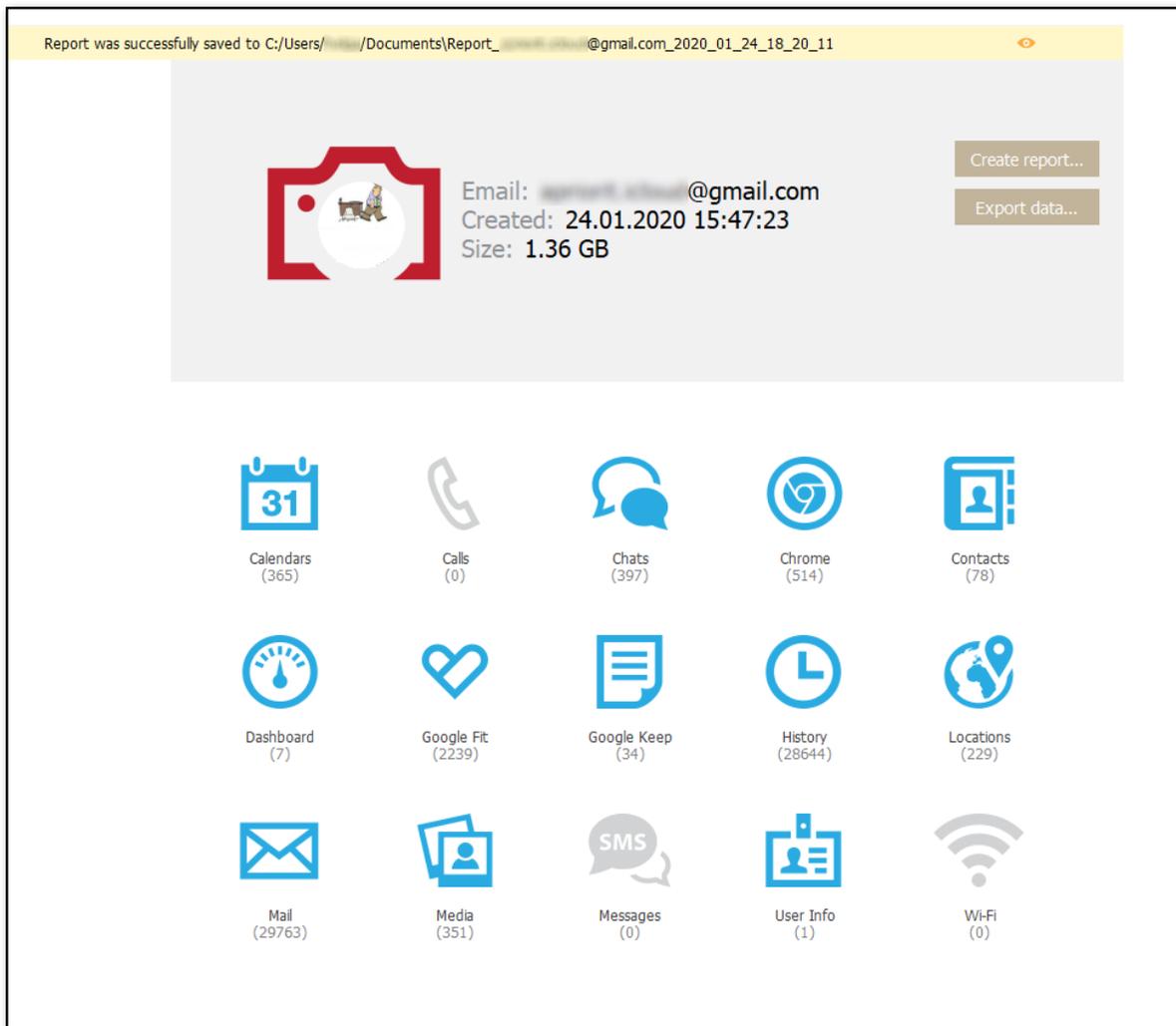
**NOTE:** The **Mail** and **Google Fit** categories are not supported in the current version of the program.

3. Define the time interval for which the report must be generated as follows: enable filters by switching the On/Off toggle and then select the dates in the **From** and **Until** fields.

4. Click **Save Report**.



4. The window will open in which you can select the location for the report.
5. Once you select the location, click **Save**.
6. The report generation will start.
7. To open the generated report, click the  icon next to **Report was successfully saved** message highlighted in yellow or double-click the report file in the location to which it was saved.



8. The report will be opened in the browser set as default by the user.

9. The report contains the following data:

- **Report Information** such as: date and time of report creation, time interval the report includes, data categories that are included and not included to the report.
- **Backup Information** such as: account name, date when the backup was downloaded, backup size, and number of records in each data category.
- **Information about records from each data category added to the report.**

#### 5.2.4 Exporting data

ECX allows you to export Google account data to your PC. Data is exported to an XLSX file, and all attachments/files are saved to a folder in the same location as the XLSX file.

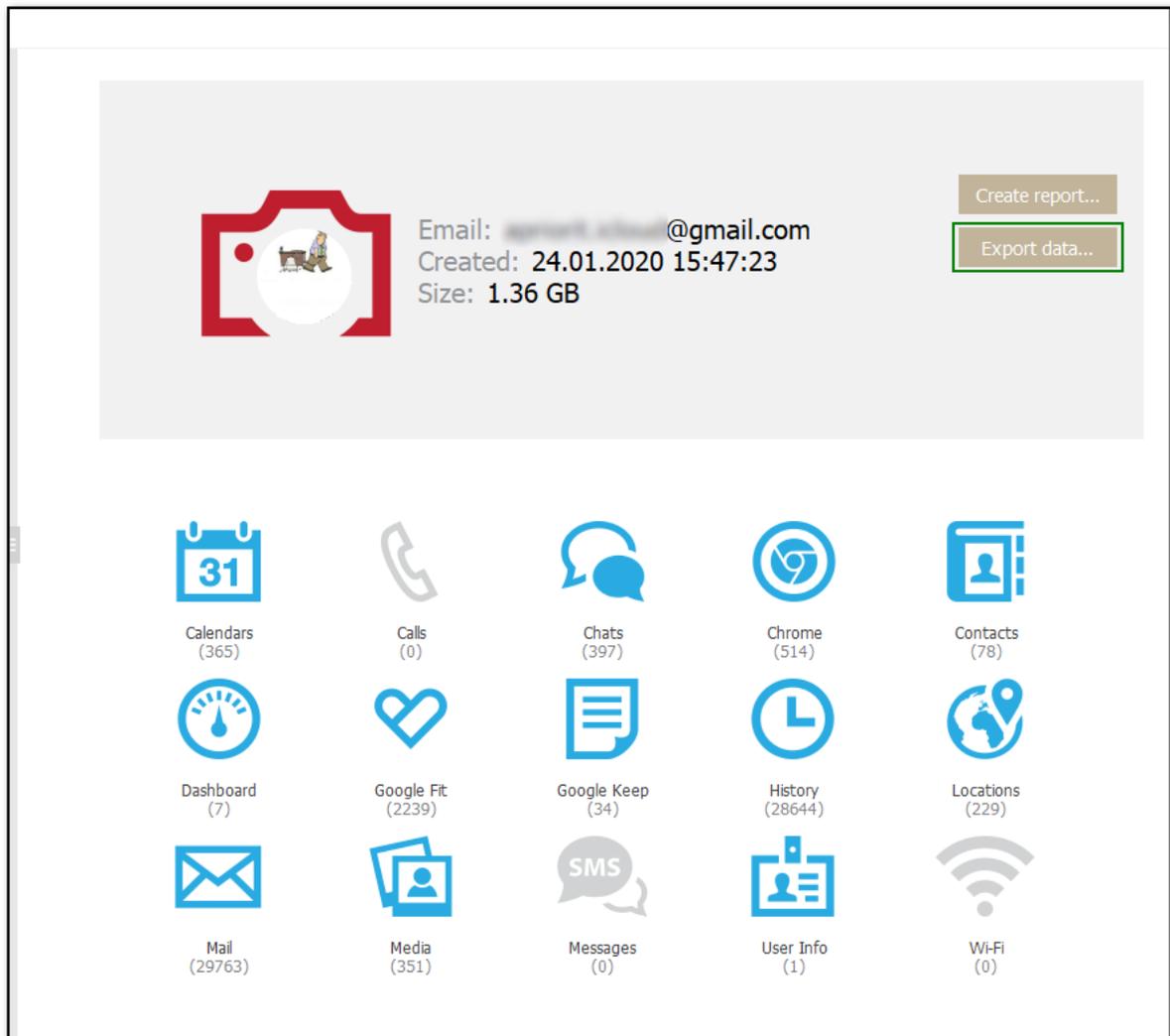
**NOTE:** Export of the Dashboard category data is not supported in the current version of ECX.

You can export **Google account** data from the main Google backup information window, where you can select what data categories to export. You can also export data directly from the plugin window.

Please note that data export is only available in the registered version of the program.

To export Google account data from the main window, do the following:

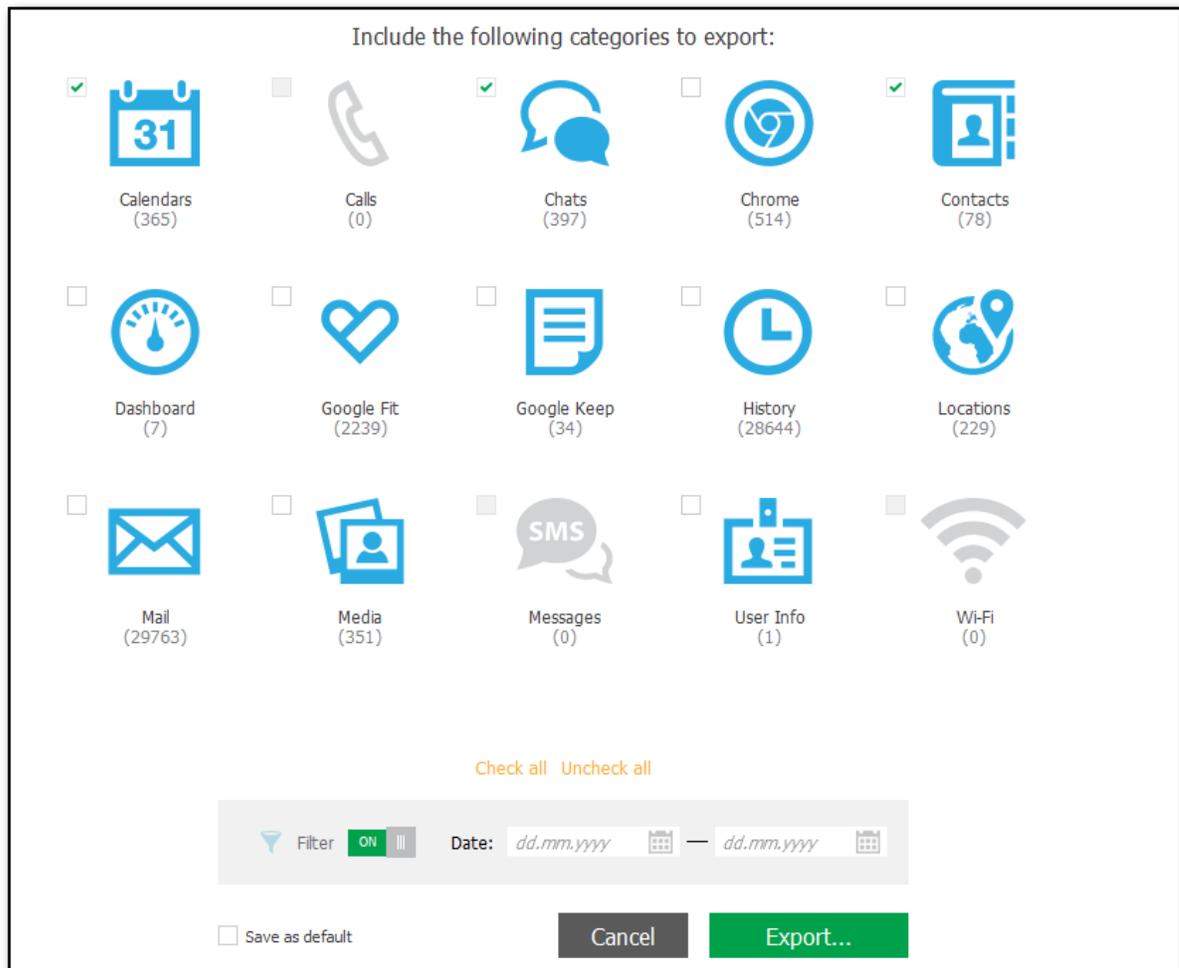
1. In the backup information section, click **Export data**.



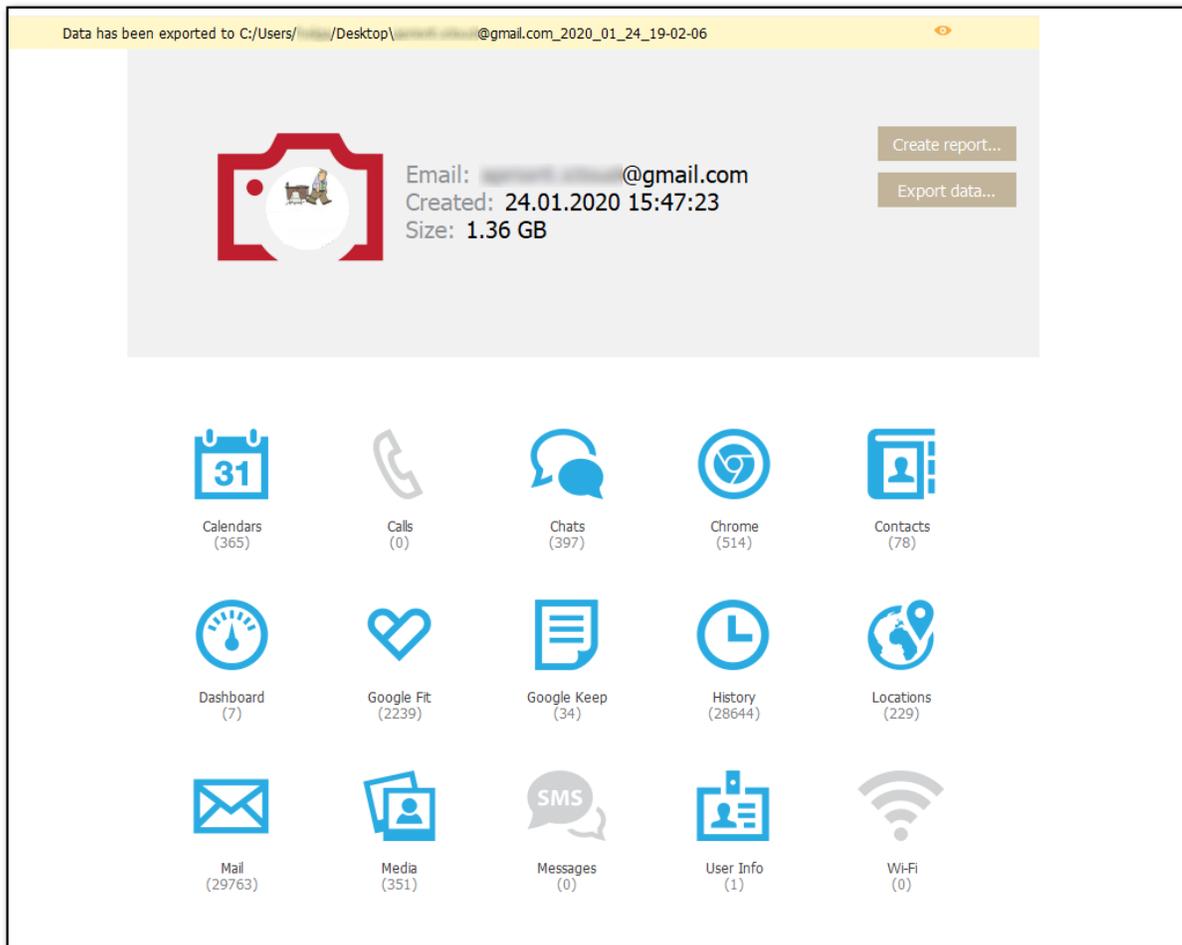
2. Select the data categories to export.

**NOTE:** The **Dashboard** category is not available for export.

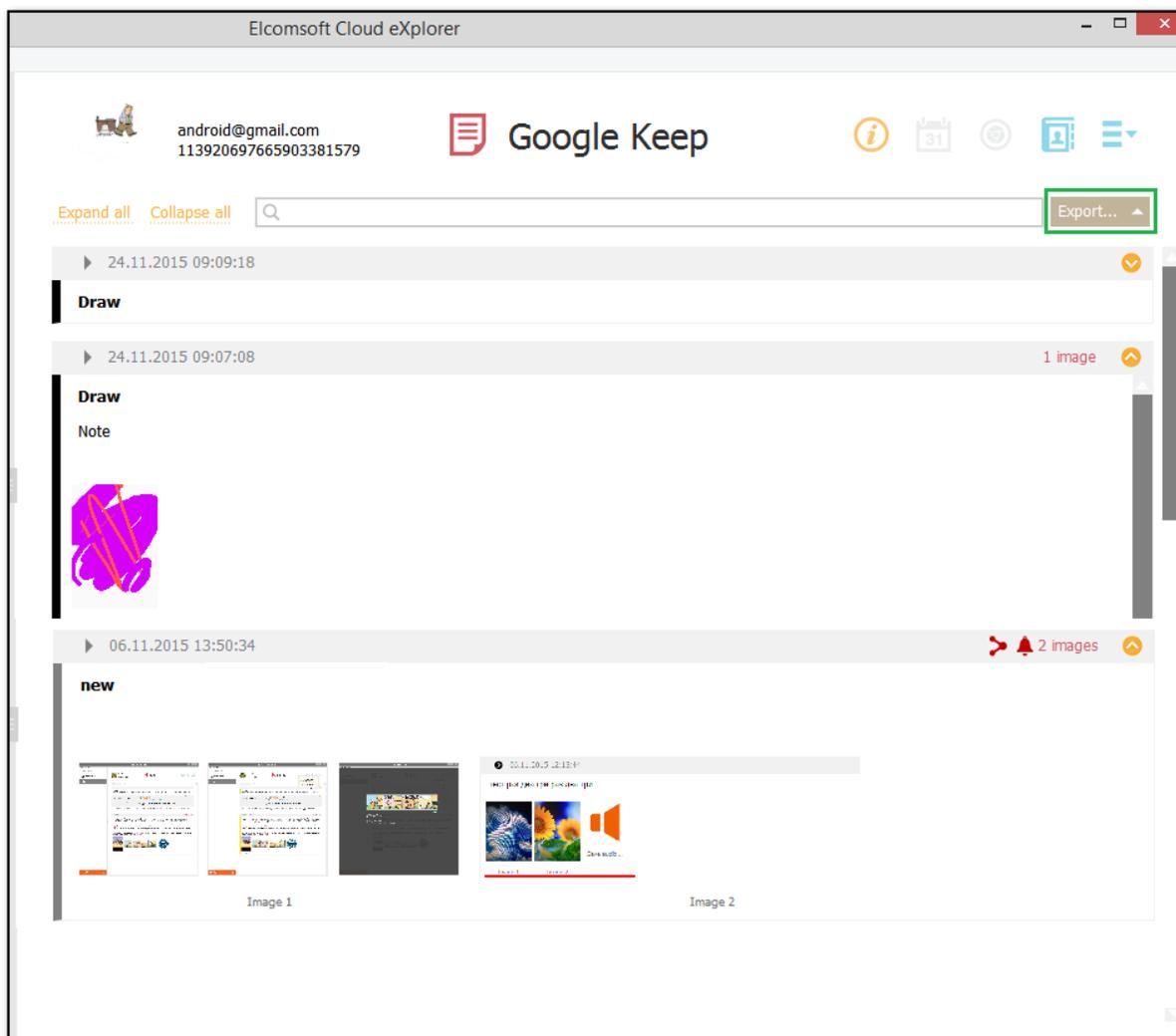
3. Define the time interval for which you want to export data as follows: enable filters by switching the On/Off toggle and then select the dates in the **From** and **Until** fields.
4. Click **Export**.



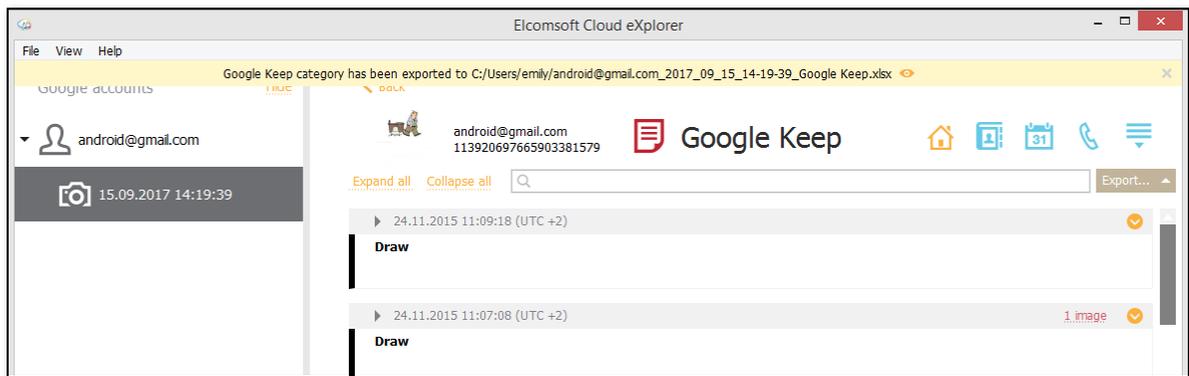
5. The window will open in which you can select the location for exported data.
6. Once you select the location, click **Save**.
7. Data export will start.
8. To open exported data, click the  icon next to **Data has been exported** message highlighted in yellow or open it from the location to which it was saved.



**To export Google account data from the plugin window, do the following:**  
1. Open the desired plugin. Click **Export** next to the search field.



2. Select whether you want to export all or filtered data. (Please note that you can also export selected data for the **Media** category.)
3. The window will open in which you can select the location for exported data.
4. Once you select the location, click **Save**.
5. Data export will start.
6. To open exported data, click the  icon next to **Data has been exported** message highlighted in yellow or open it from the location to which it was saved.



## 5.2.5 Two-step verification

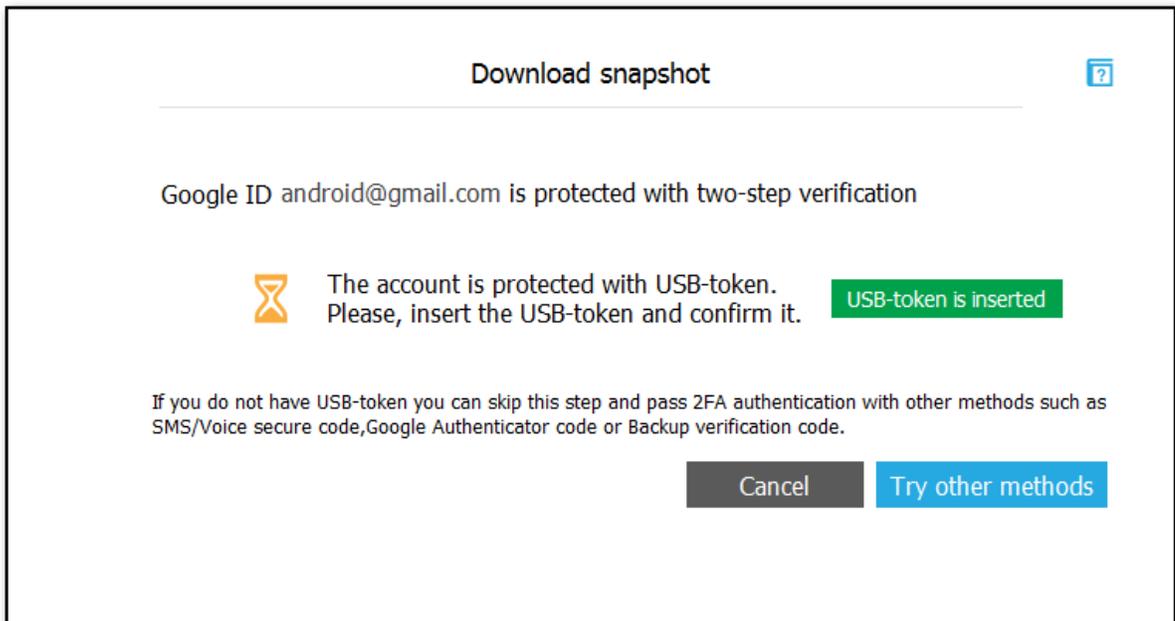
Some Google accounts require two-step verification, which means they are protected with the password and one of the following additional methods (depending on the method defined as default in the Google account security settings):

- USB-token.
- Google Prompt notification sent to the trusted device.
- A code sent to the trusted phone number in SMS text message (if the account is configured for this).
- A code generated in the [Google Authenticator](#) application.
- One of backup verification codes available on the Google Accounts Overview page (for more information, please see <https://support.google.com/accounts/answer/1187538?hl=en>).

If your Google account is protected with USB-token or Google Prompt, use the secure key or the application to pass verification.

### Singing in with USB-token

If your Google account is protected with USB-token, insert the USB-token and click **USB-token is inserted**.



If you don't have the USB-token, click **Try other methods** to pass two-step verification with other methods, such as SMS secure code, Google Authenticator code, or backup verification code. Select the preferred **verification type** by clicking one of the following tabs:

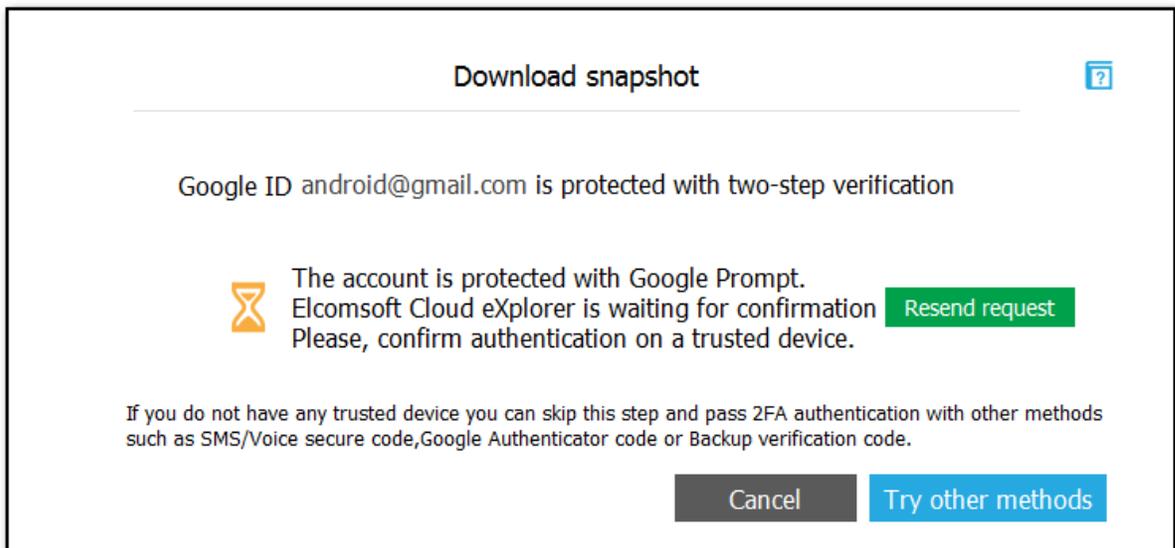
- SMS
- Authenticator
- Backup code

Enter the code in the field below and click **Verify**.

### Signing in with Google Prompt

If your Google account is protected with Google Prompt, the Google application on your device will send you a notification to confirm that you are trying to sign in.

If you haven't received the notification, click the **Resend request** link to get a new one.



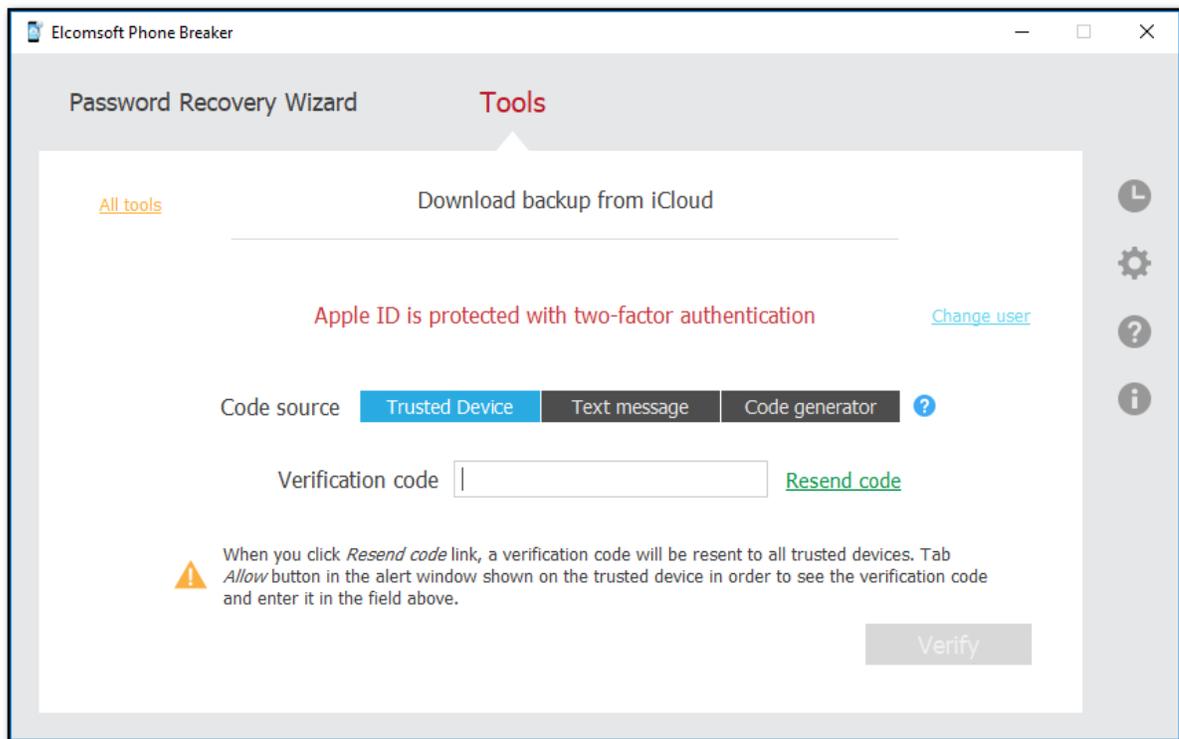
If you don't have any trusted devices with the Google application, click **Try other methods** to pass two-step verification with other methods such as SMS secure code, Google Authenticator code, or backup verification code.

Select the preferred **verification type** by clicking one of the following tabs:

- SMS
- Authenticator
- Backup code

Enter the code in the field below and click **Verify**.

If your Google account is protected with other methods, you will be required to enter the secure code or the backup code after you click **Sign in**.



### Signing in with a secure code sent in SMS text message

If your Google account is configured for sending codes in SMS text message, a code will be sent to the trusted phone number right after you click **Sign in**.

Select the preferred **verification type** by clicking one of the following tabs:

- SMS
- Authenticator
- Backup code

Enter the code in the field below and click **Verify**.

If you haven't received the code to the phone number, click the **request a new one** link to get a new one.

### Signing in with a secure code generated in Google Authenticator

If you use Google Authenticator, you can use a secure code generated in this application.

Select the preferred **verification type** by clicking one of the following tabs:

- SMS
- Authenticator
- Backup code

Enter the code in the field below and click **Verify**.

Please note that Google Authenticator generates a new code every 24 seconds. If you fail to sign in, it means the code may have expired. Try signing in with a new generated code.

### Signing in with backup verification codes

You can use one of the backup verification codes available on the Accounts overview page.

Select the preferred **verification type** by clicking one of the following tabs:

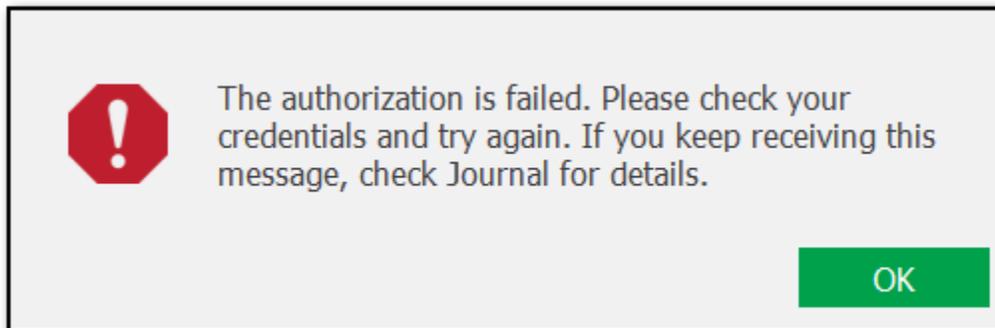
- SMS
- Authenticator
- Backup code

Enter the code in the field below and click **Verify**.

Please note that you can use each backup verification code only once. If you fail to sign in, it means the code is probably used. Try signing in with another backup verification code. If all of the available backup verification codes are invalid, generate new codes on your Google account settings page.

## 5.2.6 Exceptional verification cases

In the course of signing in to Google, there might be some exceptional cases when the authorization is failed. In this case, you will receive the following message:



The authorization fails in the following cases:

1. If you try to log in using ECX from a random IP which you haven't previously used to sign in to Chrome, while being logged into the same Google account.
2. If you are logged into the Google account in one region (city or country), and then try to log in via ECX from another region (city or country).

If you fail to authorize in any other situation except the two ones described above, contact our support team (please see [Contacting us](#) for more details).

If the authorization is failed, open your Google account in Google Chrome. You will see a notification:

## Verify it's you

Something seems a bit different about the way you're trying to sign in. Complete the step below to let us know it's you and not someone pretending to be you. [Learn more.](#)

The steps you need to perform for verification vary:

- If both a recovery email and a phone number are defined for this account, you can choose one of them to receive the verification code.
- If only a recovery email account is defined for this account, you are asked to enter a recovery email account to which the verification code will be sent.
- If only a recovery phone number is defined for this account, you are asked to choose how you would like to receive the verification code (by SMS or phone call).
- If no recovery phone number and email are defined for this account, you are asked to specify the last city in which you logged into the account.

Once you have verified your identity, try logging into the Google account using ECX again.

## 5.3 Working with Google Drive backups

### 5.3.1 Signing in

To download files from Google Drive using ECX, you are required to sign in first. The authentication process may vary depending on the Google account security settings.

**To sign in**, on the **Download files from Google Drive** page, define the authentication type:

- **Password**: Select this option to use the Google account credentials.
- **Token**: Select this option to use the Authentication token extracted from the Google Chrome browser or the Google Drive (Backup and Sync) application using Google Token Extractor (GTEX). For more information about extracting the token, see the [Extracting Authentication token](#) topic.

#### Signing In Using Credentials

If you sign in using the **Password** option, enter the Google account ID (in the [account@gmail.com](#) format) and the password.

When you sign in with the **Save credentials for future use** option selected, ECX stores an authentication token. To use the token on next sign-in to this account, enter the login and make sure the **Use token instead of password (if available)** option is selected. When signing in with a token, you do not have to use the password or pass two-steps verification (use USB-token, Google Prompt, or enter a secure code).

**NOTE:** ECX doesn't support Google accounts with CAPTCHA protection. You can wait for a while until CAPTCHA protection is turned off and then try to log in again.

### Download files from Google Drive

Authentication type **Password** Token ?

Google ID  (example@example.com)

Password

**Important:** If the account uses 2FA and you log on with the password, a verification code will be requested on the next step. It will be sent by SMS immediately once you click Sign In. Google Authenticator or Backup verification codes can be also used.

Save credentials for future use ?

Use token instead of password (if available) ?

Cancel Sign in

#### Signing In Using Authentication Token

If you sign in using the **Token** option, select the previously saved token from the list or specify the path to a new token .xml file extracted from the Google Chrome browser via Google Token Extractor (GTEX). By default, the token file is saved to the folder where the Google Token Extractor is located. For more information about extracting the token, see the [Extracting authentication token](#) topic.

When you sign in with the **Save credentials for future use** option selected, ECX saves the token and you can select it from the list on the next sign in.

**NOTE:** To download files from Google Drive, you can use tokens extracted from either the **Google Chrome browser** or **Google Drive (Backup and Sync)** application.

### Download files from Google Drive

Authentication type Password **Token** ?

Token

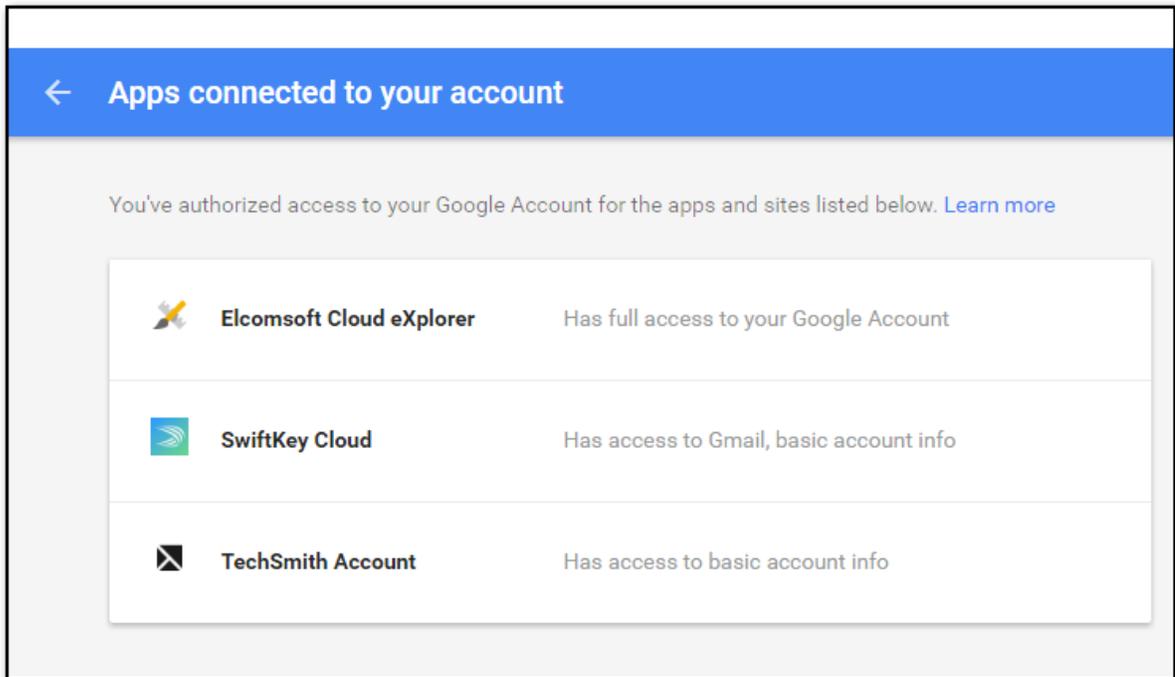
**i** You can use either Google Chrome or Google Drive tokens to download files.

Save credentials for future use ?

Cancel Sign in

## Security Notifications

When you sign in via ECX, the information on this sign-in is displayed in your Google account (My Account > Sign-in & security > Connected apps & sites > Apps connected to your account). You will see Elcomsoft Cloud eXplorer on the list of apps and sites with authorized access to your account.



If you sign in via ECX using the login and password, you will get email notifications in the Google account you signed into. You will also see an additional notification in your Google account (My Account > Sign-in & security > Device activity & notifications > Recently used devices). You will not see any mentions of the ECX applications, but there will be a Windows or Unknown OS device on the list of devices currently or recently signed in to your account.

Also, if you sign in via ECX from an IP address which you haven't previously signed in from, an email notification will be sent to your Gmail account with information on a new sign-in.

### 5.3.2 Google Drive snapshots

With ECX, you can download files from Google Drive, store them as a backup, and then explore the backup content.

The following data categories are available:

- **Google Drive:** Files uploaded by the user to Google Drive.
- **Computers:** Files synchronized with the user's PC.
- **Deleted:** Files located in the Trash folder of user's Google Drive.
- **Shared with me:** Files shared with the user.

**To download files from Google Drive,** do the following:

1. In the main menu, click **File**, and then click **Download files from Google Drive**; or click the  button in the bottom-left corner of the ECX screen.

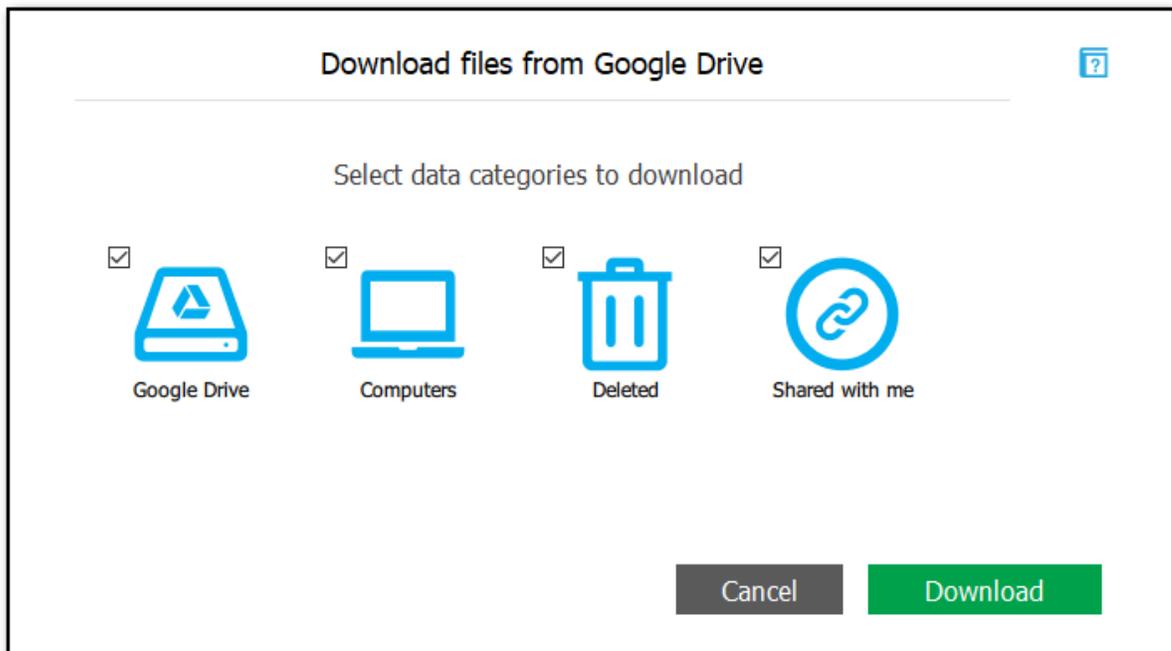
2. In the **Download files from Google Drive** window, define the authentication type:

- **Password:** Select this option to use the Google account credentials (Google ID (in the [account@google.com](#) format) and password).
- **Token:** Select this option to use the authentication token extracted from the Google Chrome browser or Google Drive (Backup and Sync) application using Google Token Extractor (GTEX). For more information about extracting the token, see the [Extracting authentication token](#) topic.

3. Click **Sign in**.

**NOTE:** If you have any issues with signing in, please see [Signing in](#).

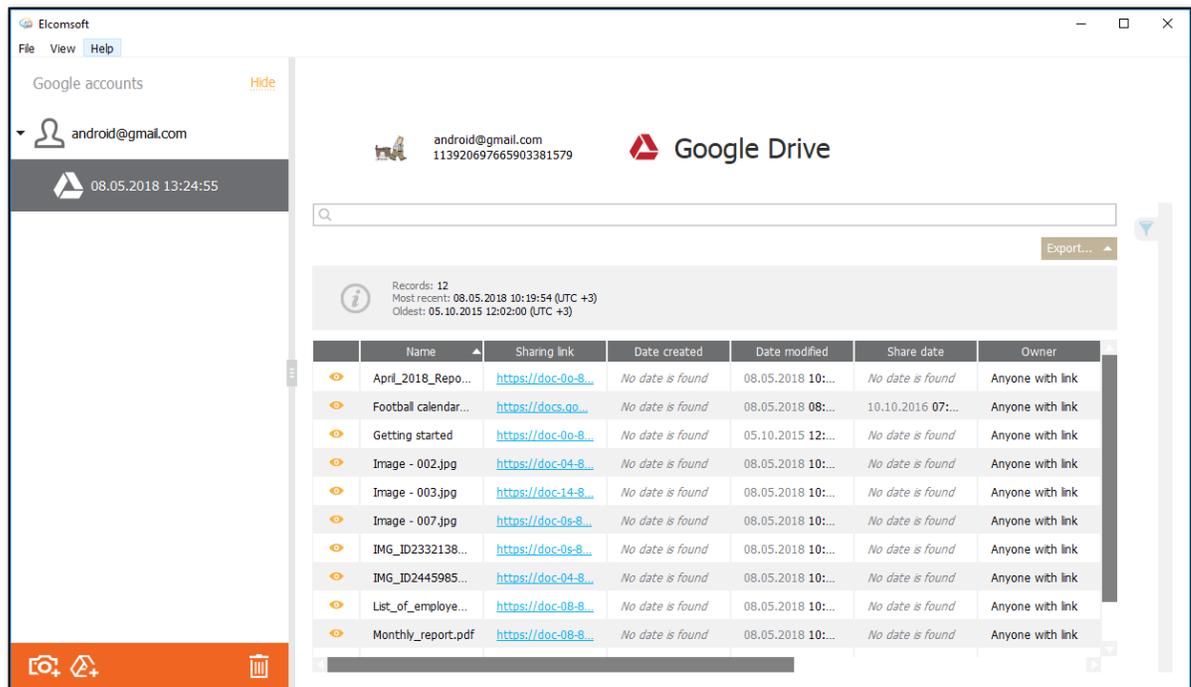
4. Select the data categories you wish to download.



5. Click **Download** and select the folder to which the Google Drive files will be downloaded.

Once the download is completed, you can see the Google account profile and its Google Drive backup in the **Google Accounts** pane on the left. The backup title consists of its creation date and time. If the Google account has several backups, they are all listed under this Google account.

In the main window, you can see the files that have been downloaded in each Google Drive backup. For more information, see the [Google Drive plugin](#) topic.



To explore the Google Drive backup content, just click on it.

To remove a Google account profile or a backup, select the desired record and click the  icon in the bottom-right corner of the Google Accounts pane, or, in the main menu, select **File**, and then click **Remove Backup**.

### 5.3.3 Exporting data

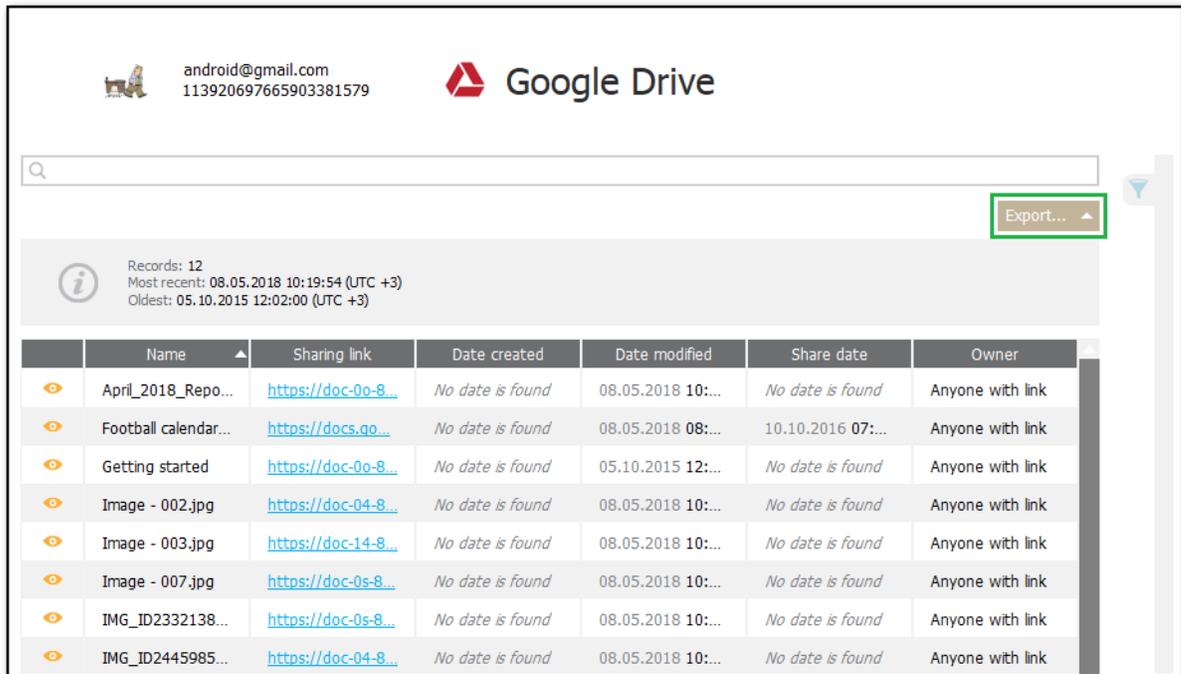
ECX allows you to export information about downloaded Google Drive files to an XLSX file.

You can export information from the Google Drive plugin window.

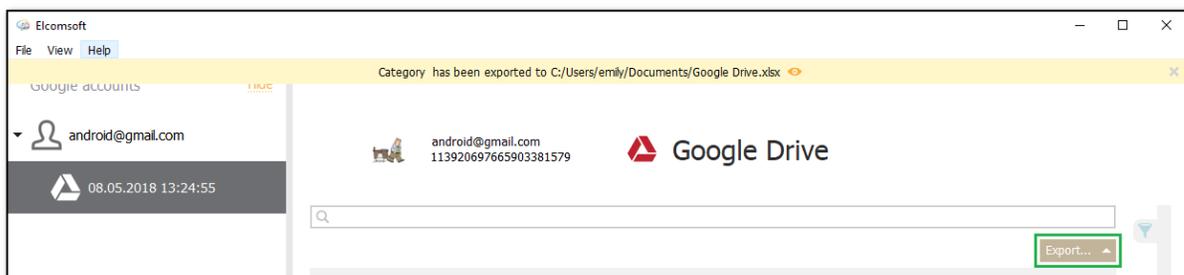
Please note that export is only available in the registered version of the program.

To export information about downloaded Google Drive files, do the following:

1. Open the Google Drive backup. Click **Export** next to the search field.



2. Select whether you want to export all or filtered data.
3. The window will open in which you can select the location for exported data.
4. Once you select the location, click **Save**.
5. Data export will start.
6. To open the exported data, click the  icon next to the **Data has been exported** message highlighted in yellow or open it from the location to which it was saved.

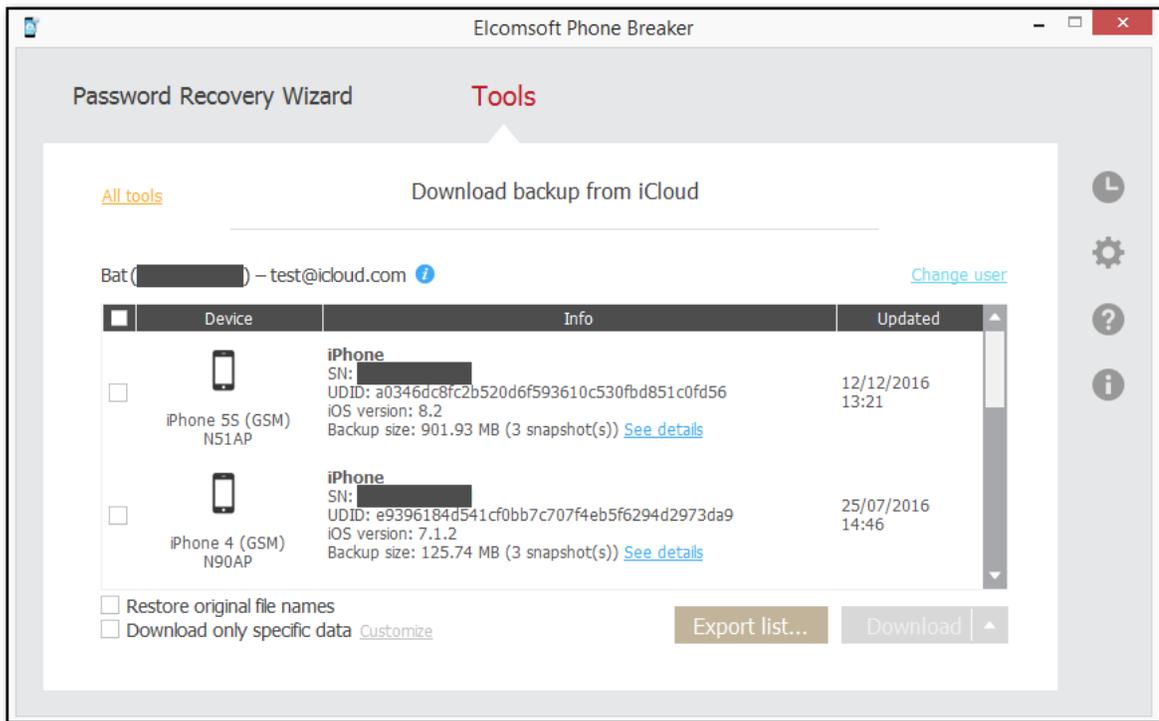


### 5.3.4 Exporting Backup List

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

**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.

### 5.3.5 Two-step verification

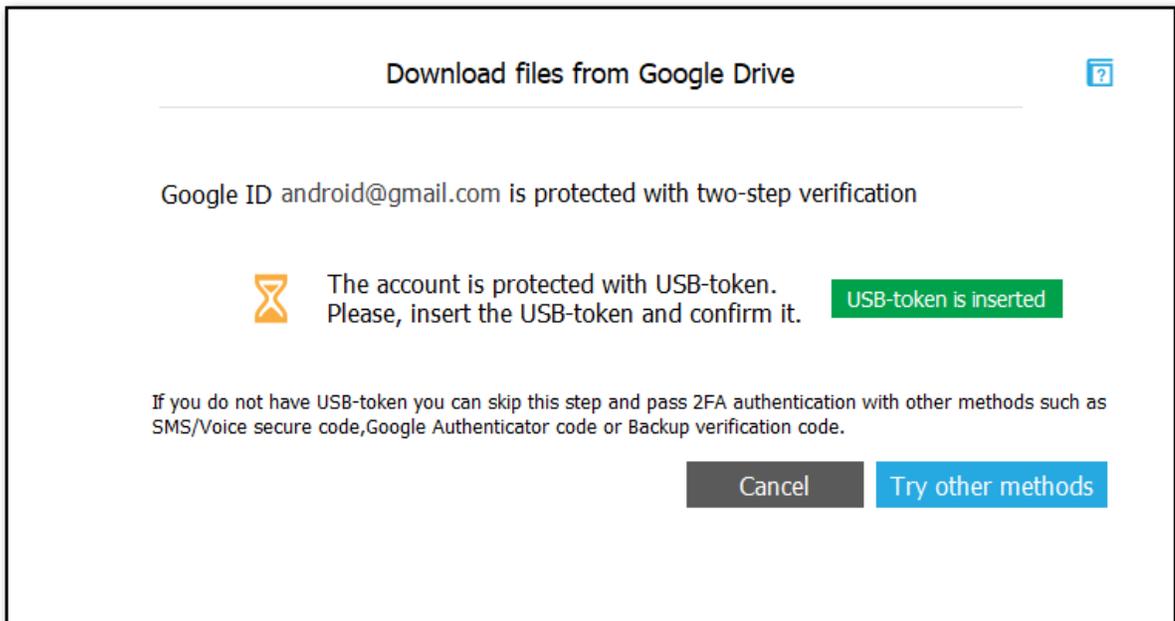
Some Google accounts require two-step verification, which means they are protected with the password and one of the following additional methods (depending on the method defined as default in the Google account security settings):

- USB-token.
- Google Prompt notification sent to the trusted device.
- A code sent to the trusted phone number in SMS text message (if the account is configured for this).
- A code generated in the [Google Authenticator](#) application.
- One of backup verification codes available on the Google Accounts Overview page (for more information, please see <https://support.google.com/accounts/answer/1187538?hl=en>).

If your Google account is protected with USB-token or Google Prompt, use the secure key or the application to pass verification.

#### Singing in with USB-token

If your Google account is protected with USB-token, insert the USB-token and click **USB-token is inserted**.



If you don't have the USB-token, click **Try other methods** to pass two-step verification with other methods, such as SMS secure code, Google Authenticator code, or backup verification code. Select the preferred **verification type** by clicking one of the following tabs:

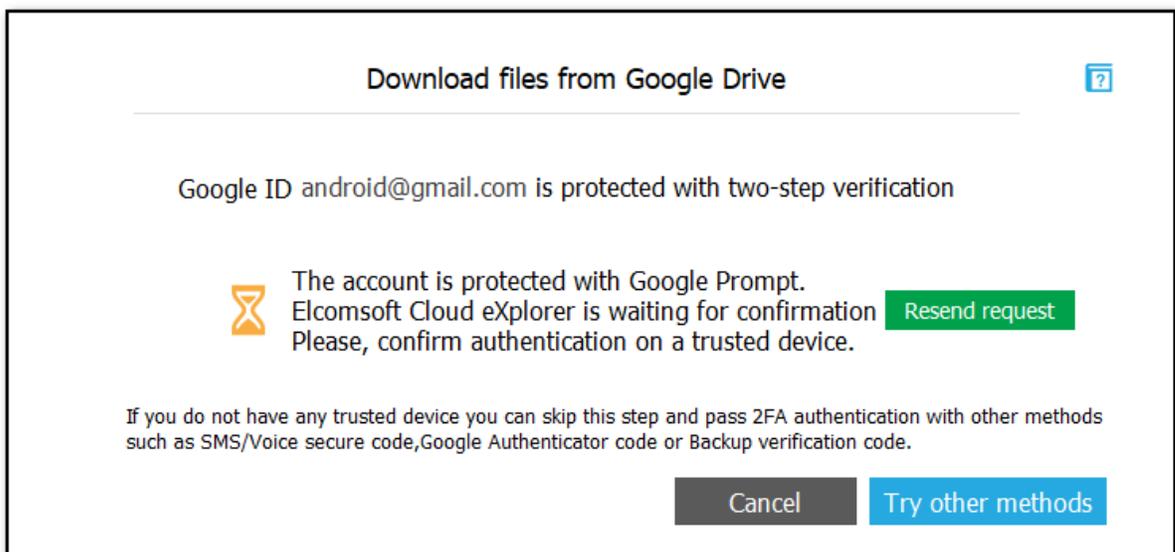
- SMS
- Authenticator
- Backup code

Enter the code in the field below and click **Verify**.

#### Signing in with Google Prompt

If your Google account is protected with Google Prompt, the Google application on your device will send you a notification to confirm that you are trying to sign in.

If you haven't received the notification, click the **Resend request** link to get a new one.



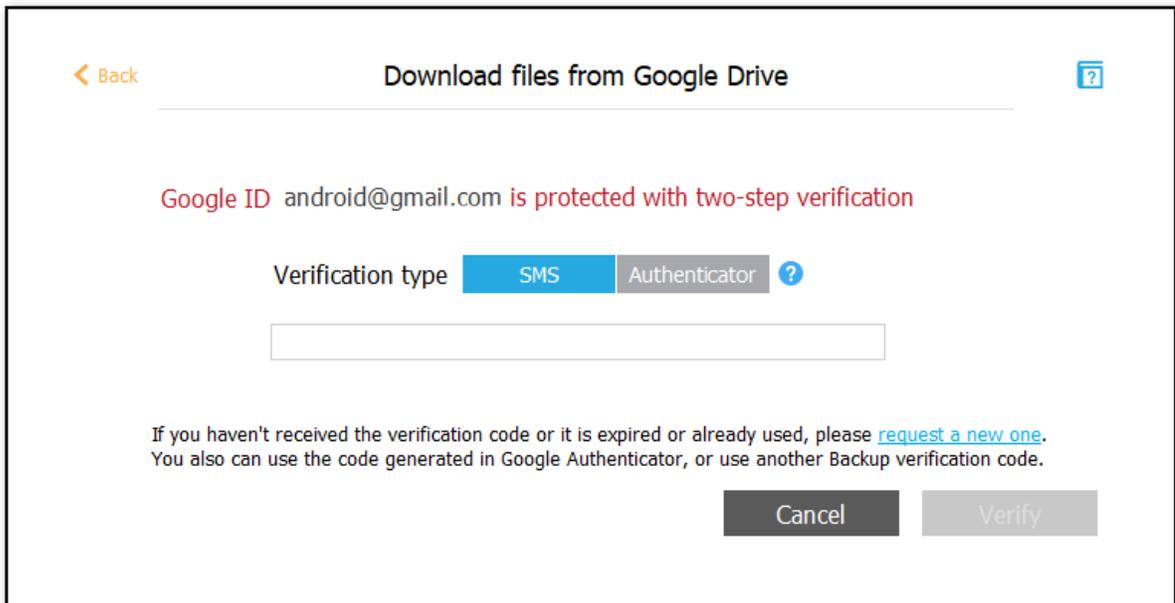
If you don't have any trusted devices with the Google application, click **Try other methods** to pass two-step verification with other methods such as SMS secure code, Google Authenticator code, or backup verification code.

Select the preferred **verification type** by clicking one of the following tabs:

- SMS
- Authenticator
- Backup code

Enter the code in the field below and click **Verify**.

If your Google account is protected with other methods, you will be required to enter the secure code or the backup code after you click **Sign in**.



#### Signing in with a secure code sent in SMS text message

If your Google account is configured for sending codes in SMS text message, a code will be sent to the trusted phone number right after you click **Sign in**.

Select the preferred **verification type** by clicking one of the following tabs:

- SMS
- Authenticator
- Backup code

Enter the code in the field below and click **Verify**.

If you haven't received the code to the phone number, click the **request a new one** link to get a new one.

#### Signing in with a secure code generated in Google Authenticator

If you use Google Authenticator, you can use a secure code generated in this application.

Select the preferred **verification type** by clicking one of the following tabs:

- SMS
- Authenticator
- Backup code

Enter the code in the field below and click **Verify**.

Please note that Google Authenticator generates a new code every 24 seconds. If you fail to sign in, it means the code may have expired. Try signing in with a new generated code.

#### Signing in with backup verification codes

You can use one of the backup verification codes available on the Accounts overview page.

Select the preferred **verification type** by clicking one of the following tabs:

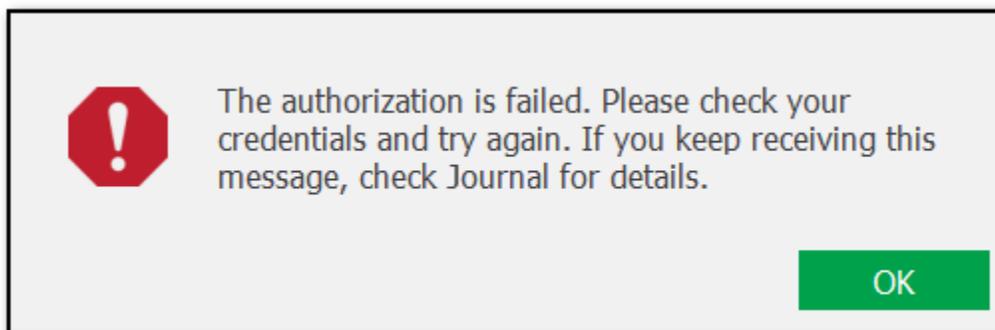
- SMS
- Authenticator
- Backup code

Enter the code in the field below and click **Verify**.

Please note that you can use each backup verification code only once. If you fail to sign in, it means the code is probably used. Try signing in with another backup verification code. If all of the available backup verification codes are invalid, generate new codes on your Google account settings page.

### 5.3.6 Exceptional verification cases

In the course of signing in to Google, there might be some exceptional cases when the authorization is failed. In this case, you will receive the following message:



The authorization fails in the following cases:

1. If you try to log in using ECX from a random IP which you haven't previously used to sign in to Chrome, while being logged into the same Google account.
2. If you are logged into the Google account in one region (city or country), and then try to log in via ECX from another region (city or country).

If you fail to authorize in any other situation except the two ones described above, contact our support team (please see [Contacting us](#) for more details).

If the authorization is failed, open your Google account in Google Chrome. You will see a notification:



The steps you need to perform for verification vary:

- If both a recovery email and a phone number are defined for this account, you can choose one of them to receive the verification code.
- If only a recovery email account is defined for this account, you are asked to enter a recovery email account to which the verification code will be sent.
- If only a recovery phone number is defined for this account, you are asked to choose how you would like to receive the verification code (by SMS or phone call).

- If no recovery phone number and email are defined for this account, you are asked to specify the last city in which you logged into the account.

Once you have verified your identity, try logging into the Google account using ECX again.

## 5.4 Extracting Google authentication tokens

### 5.4.1 About Google Token Extractor

**Google Token Extractor (GTEX)** is console utility for extracting tokens to Google accounts from live (current) Windows OS and macOS.

GTEX can extract tokens from the Google Chrome browser and the Google Drive ([Backup and Sync](#)) application.

You can use tokens extracted by GTEX to sign in to the user's Google account in order to download Google account and Google Drive backups.

GTEX is supported by the following operating systems:

- Windows 7, Windows 8, Windows 8.1, Windows 10
- macOS 10.8 - 10.14

GTEX supports extracting tokens from the following applications:

- Google Chrome v. 26 to v. 64
- Backup and Sync v. 1.32

The extracted token expires if:

- The user revokes the access in the Google account permission settings.
- The token was not used for 6 months.
- The user changed the password.
- The user enabled two-step verification after the token was extracted.

### 5.4.2 Extracting token on Windows OS

You can sign in to a Google account to download Google account and Google Drive backups using the Google authentication token.

To extract the token, you will need a Google Token Extractor. This tool is shipped together with ECX (**GoogleTokenExtractor.exe** file). You can find it in the ECX installation folder.

Google Token Extractor is portable, so you can copy the GoogleTokenExtractor.exe file to a folder where you would like the file with the authentication token to be created.

GTEX can extract tokens from the Google Chrome browser and Google Drive ([Backup and Sync](#)) application.

GTEX allows you to extract authentication tokens for:

- The currently logged in Windows user
- Other Windows users on the current computer

### Preconditions

Prior to extracting the authentication token, make sure that at least one the following conditions is met:

- Google Chrome browser (v.26 - v.64) is installed and at least one user is logged in to the Google Chrome account. The Google Chrome application must be closed during the token extraction process (make sure that there is no Chrome.exe process in the Task Manager)
- Backup and Sync application (v. 1.32) is installed and at least one user is logged in. Application can be run during the token extraction process.

Prior to using GTEX for extracting the token, make sure that Internet connection is established.

### User permissions required for getting the authentication token:

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

**NOTE: If you run GoogleTokenExtractor.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 tokens for the current Windows user**, do the following:

1. Launch **GoogleTokenExtractor.exe**. The file "**<Windows user>\_<Google ID>\_<token type>\_<timestamp>\_<time zone>.xml**" will be created in the directory from which **GoogleTokenExtractor.exe** was launched.

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

2. The created .xml file contains the following information:
  - GTEX Version
  - Platform
  - Google ID
  - Token
  - Token Type (Google Chrome or Google Drive)
  - Client ID
  - Client Secret
  - Date and time of extraction

**To extract the authentication tokens for a certain Windows user**, do the following:

1. Open the Command Prompt with administrator privileges.
2. Go to the folder where **GoogleTokenExtractor.exe** is stored.
3. Enter the command **GoogleTokenExtractor.exe --get-users-list**
4. The list of all local users with Google Chrome and Google Drive (Backup and Sync) applications installed will be displayed.

5. Launch GoogleTokenExtractor.exe with the get-token chrome (for Google Chrome browser) or get-token drive (for Backup and Sync application) parameter and enter username of a specific local Windows user and the password to this Windows user account in the following form:

**GoogleTokenExtractor.exe --get-token chrome --username <username> --password <password>**

**GoogleTokenExtractor.exe --get-token drive --username <username> --password <password>**

**For example: GoogleTokenExtractor.exe --get-token chrome --username user1 --password 1234**

For users with the blank password, type "" as the value to the password parameter.

**For example: GoogleTokenExtractor.exe --get-token chrome --username user1 --password ""**

6. The "<Windows user>\_<Google ID>\_<token type>\_<timestamp>\_<time zone>.xml" file will be created in the directory from which **GoogleTokenExtractor.exe** was launched.

The created .xml file contains the following information:

- GTEX Version
- Platform
- Google ID
- Token
- Token Type (Google Chrome or Google Drive)
- Client ID
- Client Secret
- Date and time of extraction

#### Parameters for running GoogleTokenExtractor.exe in the Command Prompt:

Parameter	Meaning
--help	Displays a list of all possible command-line parameters and their descriptions
--get-users-list	Displays a list of users with installed Google Chrome/Backup and Sync applications.
--get-token chrome	Gets the authentication token from the Google Chrome browser for the current user.
--get-token drive	Gets the authentication token from the Backup and Sync application for the current user.
--get-token chrome --username <username> --password <password>	Gets the authentication token from the Google Chrome browser for the specific user. Username and password should be entered without brackets.
--get-token drive --username <username> --password <password>	Gets the authentication token from the Backup and Sync application for the specific user. Username and password should be entered without brackets.
For users with the blank password, type "" as the value to the password parameter.	

### 5.4.3 Extracting token on Mac OS X

You can sign in to a Google account to download Google account and Google Drive backups using the Google authentication token.

To extract the token, you will need a Google Token Extractor. This tool is shipped together with ECX (**GoogleTokenExtractor** file).

GTEX can extract tokens from the Google Chrome browser and Google Drive ([Backup and Sync](#)) application.

GTEX allows you to extract authentication tokens for:

- The currently logged in Mac OS user
- Other Mac OS users on the current computer

#### Preconditions

Prior to extracting the authentication token, make sure that at least one the following conditions is met:

- Google Chrome browser (v.26 - v.64) is installed and at least one user is logged in to the Google Chrome account. The Google Chrome application must be closed during the token extraction process.
- Backup and Sync application (v. 1.32) is installed and at least one user is logged in. Application can be run during the token extraction process.

Prior to using GTEX for extracting the token, make sure that Internet connection is established.

#### User permissions required for getting the authentication token:

Authentication Token For	Permissions Required
Google account of the currently logged in Mac OS user	User's permissions are enough
Google account of a different Mac OS user	<b>root</b> permissions are required

**To extract the authentication tokens for the current Mac OS user**, do the following:

1. Launch the **GoogleTokenExtractor** file. The file "**<Mac OS user>\_<Google ID>\_<token type>\_<timestamp>\_<time zone>.xml**" will be created in the `/Users/<username>/Documents/` directory.

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

2. The created .xml file contains the following information:
  - GTEX Version
  - Platform
  - Google ID
  - Token
  - Token Type (Google Chrome or Google Drive)
  - Client ID
  - Client Secret
  - Date and time of extraction

To extract the authentication tokens for a certain Mac OS user, do the following:

1. Copy the **GoogleTokenExtractor** file to the folder where you want the file with authentication token to be saved.
2. Open the command-line Terminal.
3. Go to the directory where you saved the **GoogleTokenExtractor** file.
4. To list all users with installed Google Chrome/Backup and Sync applications, use the command **sudo ./GoogleTokenExtractor --get-users-list**  
**sudo** command is used to get root privileges for running the program.
5. Enter the password of the root user when prompted.
6. The list of all users with installed Google Chrome and Google Drive (Backup and Sync) applications will be displayed.
7. To get the authentication token, launch GoogleTokenExtractor with the get-token chrome (for Google Chrome browser) or get-token drive (for Backup and Sync application) parameter and enter username of a specific local Mac OS user and the password to this Mac OS user account in the following form:

```
sudo ./GoogleTokenExtractor --get-token chrome --username <username> --password <password>
```

```
sudo ./GoogleTokenExtractor --get-token drive --username <username> --password <password>
```

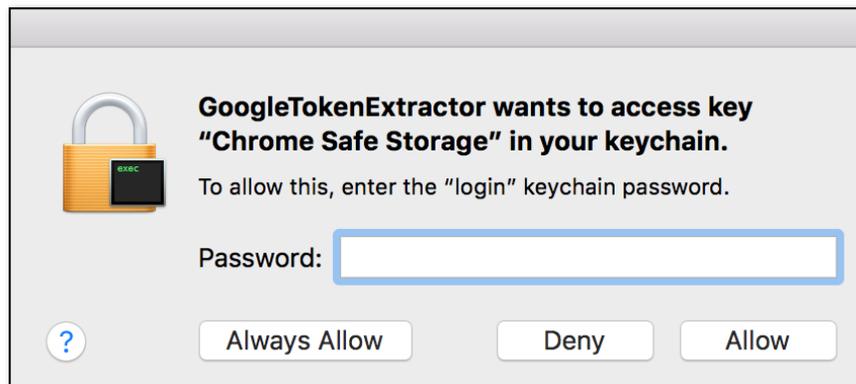
For example: **sudo GoogleTokenExtractor --get-token chrome --username user1 --password 1234**

For users with the blank password, type "" as the value to the password parameter.

For example: **sudo GoogleTokenExtractor --get-token chrome --username user1 --password ""**

**NOTE: Do not launch GoogleTokenExtractor using the sudo command with no parameters.**

8. Enter the password for the selected user when prompted.
9. Click **Allow** when asked to provide access to the confidential information in keychain.



10. The "<Mac OS user>\_<Google ID>\_<token type>\_<timestamp>\_<time zone>.xml" file will be created in the directory from which **GoogleTokenExtractor** was launched.

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

11. The created .xml file contains the following information:

- GTEX Version
- Platform
- Google ID
- Token
- Token Type (Google Chrome or Google Drive)
- Client ID
- Client Secret
- Date and time of extraction

#### Parameters for running GoogleTokenExtractor in the Terminal:

Parameter	Meaning
--help	Displays a list of all possible command-line parameters and their descriptions
--get-users-list	Displays a list of users with installed Google Chrome/Backup and Sync applications.
--get-token chrome	Gets the authentication token from the Google Chrome browser for the current user.
--get-token drive	Gets the authentication token from the Backup and Sync application for the current user.
--get-token chrome --username <username> --password <password>	Gets the authentication token from the Google Chrome browser for the specific user. Username and password should be entered without brackets.
--get-token drive --username <username> --password <password>	Gets the authentication token from the Backup and Sync application for the specific user. Username and password should be entered without brackets.
	For users with the blank password, type "" as the value to the password parameter.

## 5.5 Plugins

### 5.5.1 Contacts

With ECX, you can view the Google account user's contacts. In the left pane of the main window, you can see the list of contacts sorted by their name in the alphabetical order. The contacts with no name specified are displayed at the end of the list with the No Name tag. The contacts which belong to the Favorite group are marked with a star.

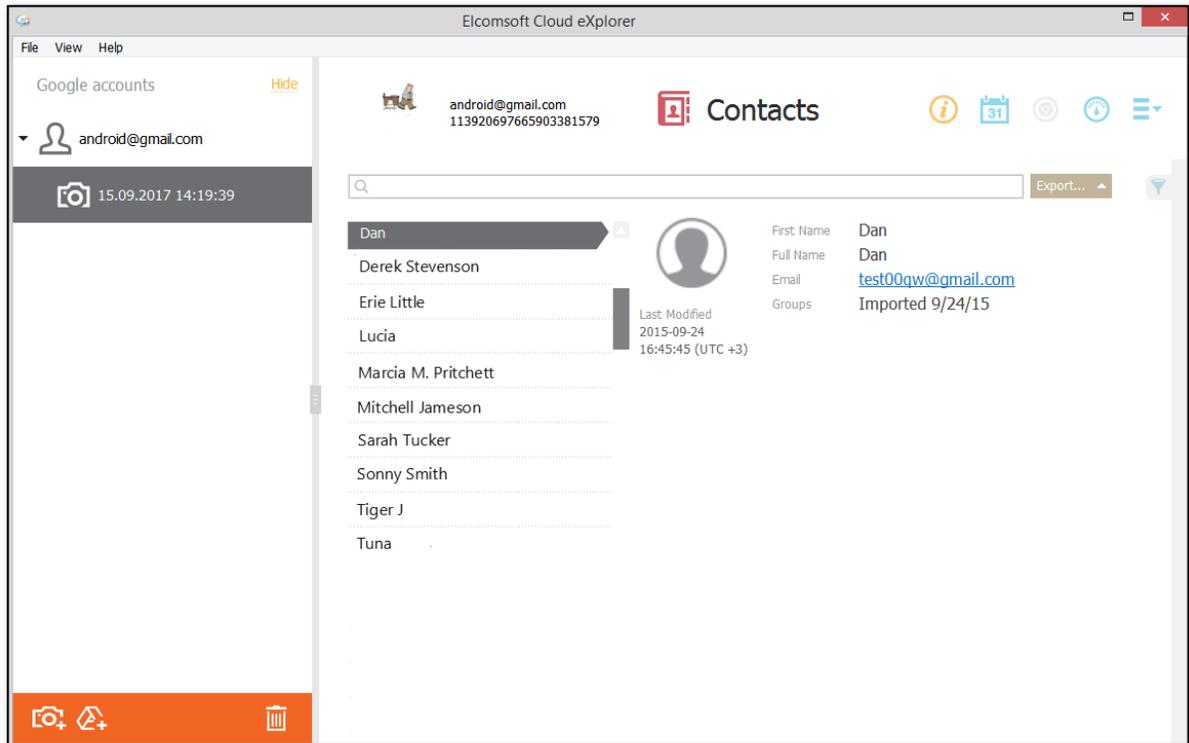
Select the contact from the contact list on the left, and all the information that is available for it will be shown on the right.

General information on the contact is usually (but not limited to) the following:

- First name
- Last name
- Photo
- Last modified (the date the contact was last modified)
- Groups (the groups the contact belongs to)
- Nickname
- Company
- Job title
- Phone number
- Address
- Birthday
- Website (a URL you can click to open the page in your browser)
- IM
- Notes
- Language

Please note that the list of contact properties may vary depending on what information is available on the contact.

You can export contacts to your computer by clicking the **Export** button.



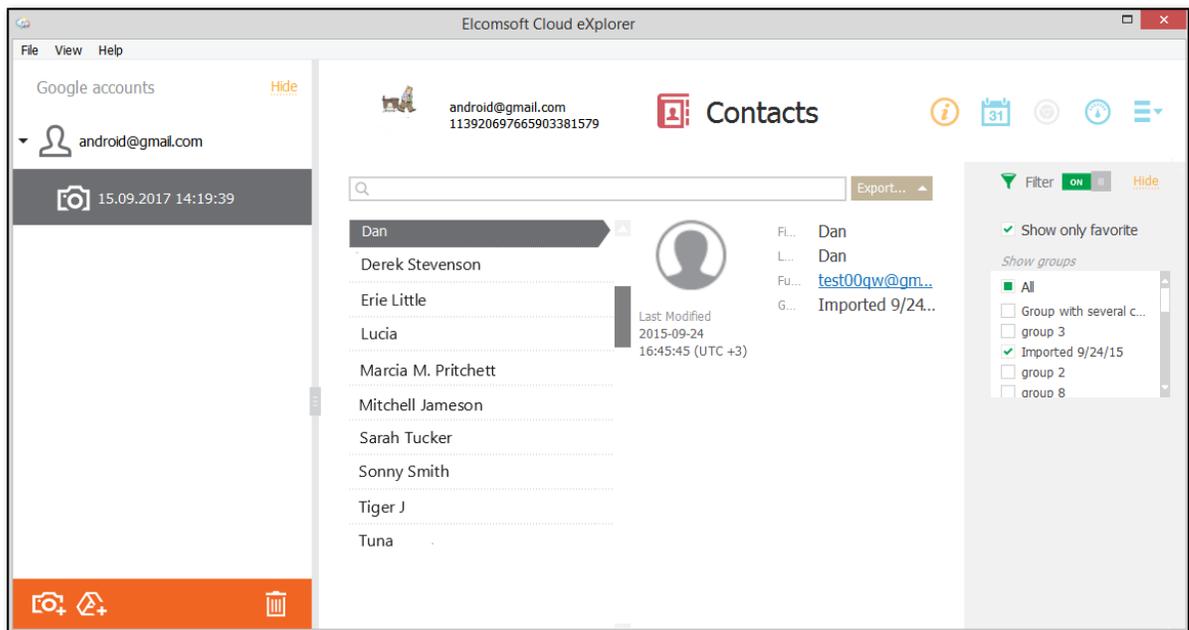
## Searching and Filtering

To perform searches in **Contacts**, fill the search field and press **Enter**. The search results will be highlighted in yellow.

To filter out the contacts by groups, open the **Filter** pane by clicking the  icon on the right. Enable filtering by switching the On/Off toggle and define the filtering options:

- Select the **Show only favorites** check box to find the contacts marked as favorite.
- Filter by the groups the contacts belong to.

You can export the contacts you have filtered. Click **Export** and select the **Filtered** option.



## 5.5.2 Calendars

You can explore events planned in Google Calendar including one time and regular events, birthdays, holidays, etc. Please note that for recurrent events/appointments, only the first day of the event is shown.

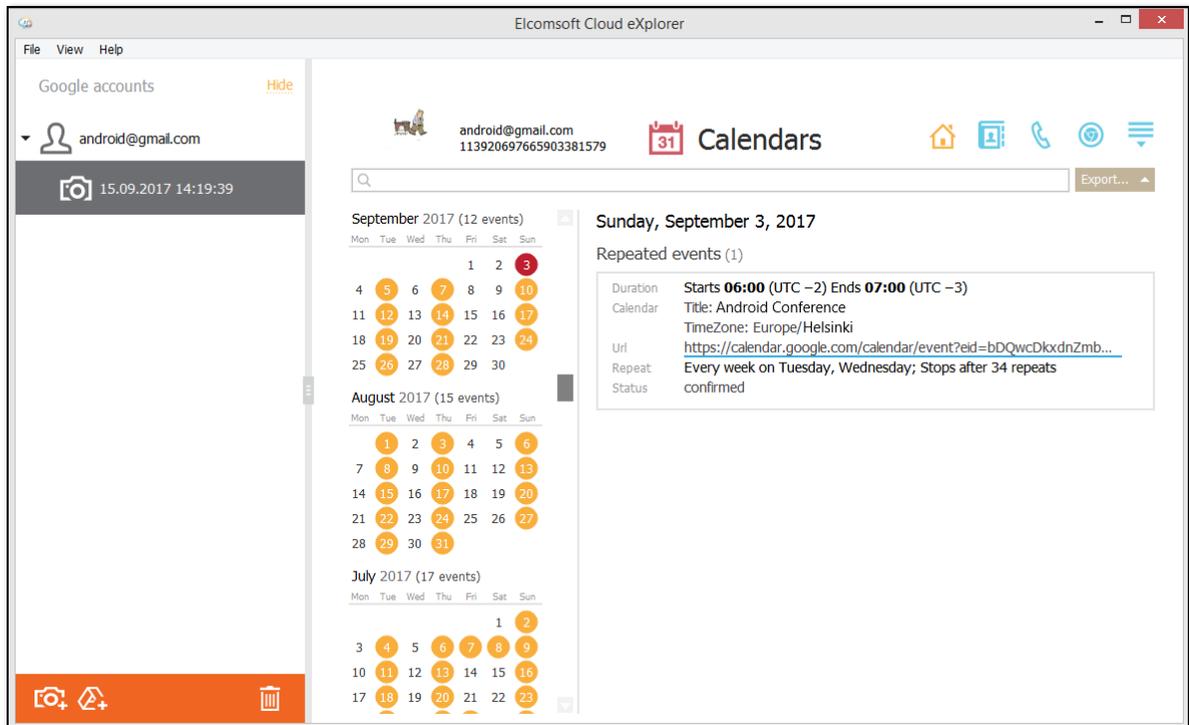
The calendar is displayed in the left pane of the main window. You can see the total number of events for each month next to its name. Days with no events are inactive. Days that have at least one event are colored yellow. Click a day to see all the events associated with it in the right pane of the main window. The following information can be available:

- Title
- Location
- Location link (the link to the event location on Google Maps)
- Duration (the start/end time of the event)
- Calendar Title (which of the user's calendars the event belongs to)
- Calendar Timezone
- URL (the link which you can click to view the event in Google Calendar)
- Accounts (the users the event is shared with)
- Attendees
- Repeat (when and how many times the event repeats)
- Reminder (the type and frequency of the event reminders)
- Status
- Notes
- Description
- Attachment (a link which you can click to view the attached file in your browser)
- Organizer

You can export calendar events to your computer by clicking the **Export** button.

To perform searches in **Calendars**, fill the search field and press **Enter**. The search results will be highlighted in yellow.

You can export the calendar events that were filtered out as search results. Click **Export** and select the **Filtered** option.



### 5.5.3 Calls

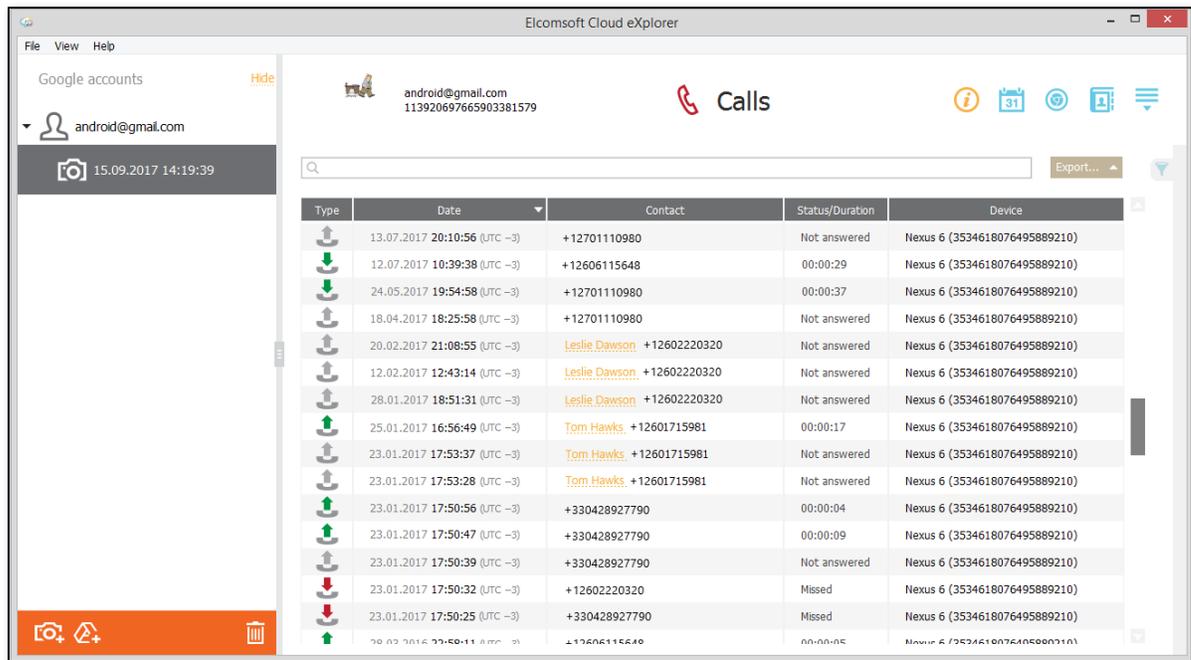
The **Calls** plugin allows you to explore the information on call history stored in the user's Google account. This information is available if the Google account user chose to back up his/her device and store the information in the Google account.

The following information can be available:

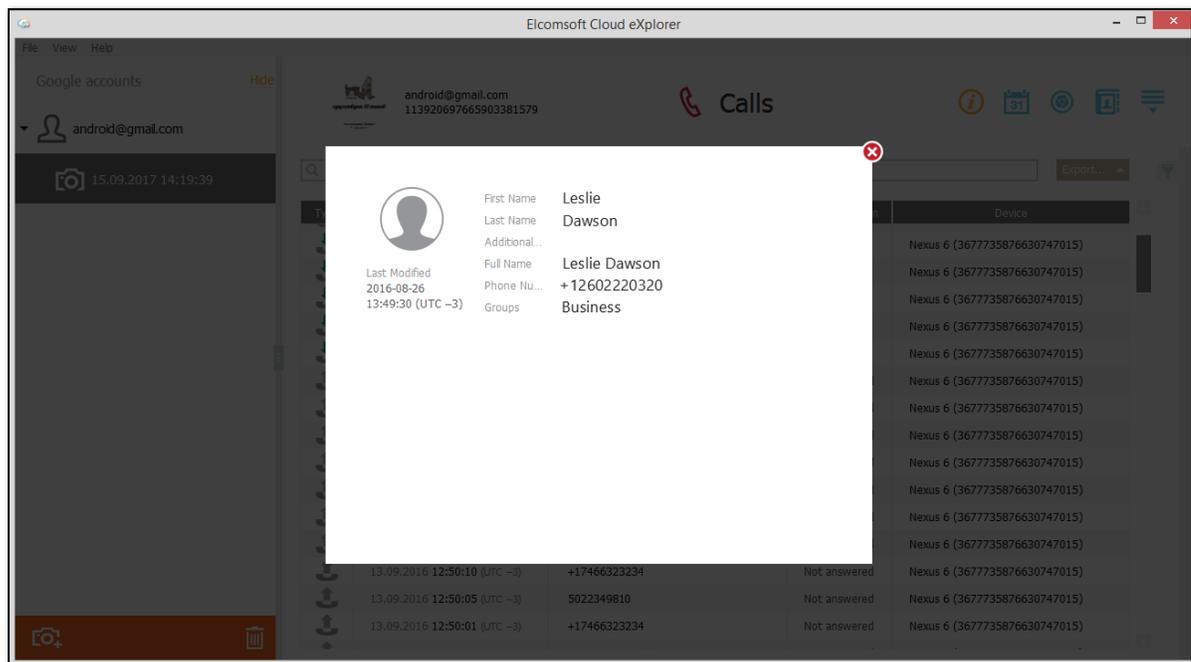
- Type (outgoing answered, outgoing unanswered, incoming received, incoming missed)
- Date (the date and time the call was made as well as the timezone)
- Contact (if the contact is the user contact list, the contact name is displayed next to the phone number)
- Status/Duration:
  - Not answered (for outgoing unanswered calls)
  - Missed (for incoming missed calls)
  - Call duration (for outgoing answered and incoming received calls)
- Device (device model and IMEI)

**NOTE:** The **Calls** information will not be downloaded, if Android device (v. 9.0 and higher) is protected by the cryptographic key or passcode.

You can export call history to your computer by clicking the **Export** button.



You can click the contact name to see the detailed contact information:



## Searching and Filtering

To perform searches in **Calls**, fill the search field and press **Enter**. The search results will be highlighted in yellow.

To filter out the call records by groups, open the **Filter** pane by clicking the  icon on the right. Enable filtering by switching the On/Off toggle and define the filtering options:

- **Dates:** filters calls by time interval. Select the year and the months you want to view the call history for.
- **Direction:** filters calls by their type. Define whether you need the **Incoming** or **Outgoing** calls.
- **Status:** filters calls by their status. Define whether you need **Answered**, **Not Answered**, or **Missed** calls.
- **Devices:** filters calls by devices they were made from. Select the desired devices.

You can export the call history records you have filtered. Click **Export** and select the **Filtered** option.

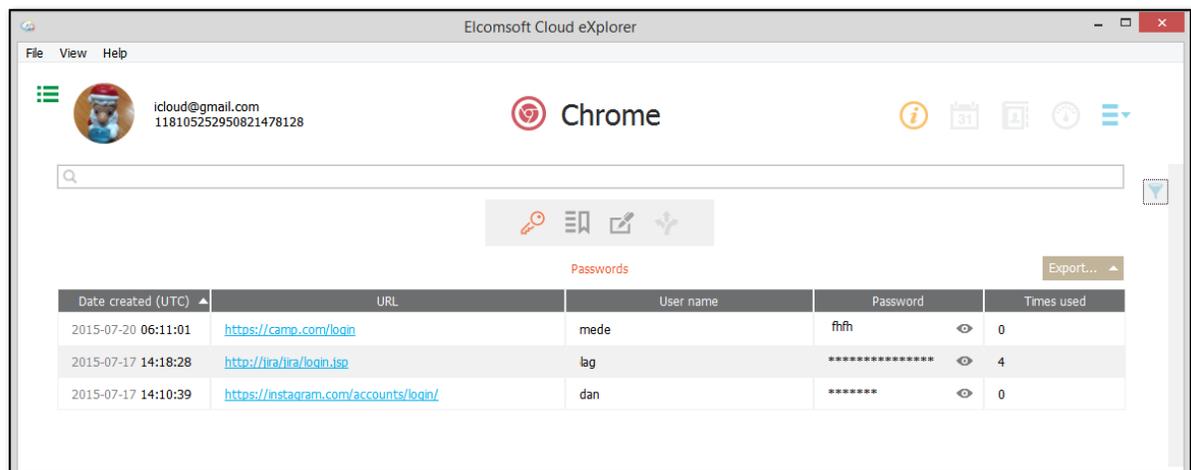
## 5.5.4 Chrome

ECX allows you to explore Google Chrome data using the **Chrome** plugin.

**NOTE:** Some Chrome data may be encrypted with a passphrase (for more information, please see <https://support.google.com/chrome/answer/1181035?hl=en>). If you select to download the Chrome data category, and Chrome information in your Google account is encrypted with a passphrase, ECX requires you to enter this passphrase. If you enter the passphrase, all the Chrome data is downloaded. If you don't enter the passphrase, the encrypted data is not downloaded.

The **Chrome** plugin includes the following sections:

- Passwords
- Bookmarks
- Autofills
- Pages Transitions



**To move to the desired section**, click the corresponding icon in the gray rectangle area over the grid.

In the **Passwords** section of the **Chrome** plugin, you can view the user's saved passwords to different websites. You can find the following information:

- Date created
- URL (which you can click to open the page in your browser)
- User name
- Password (you can click the  icon next to the password to view the characters)
- Times used

In the **Bookmarks** section, you can view information on the user's bookmarked web pages, such as:

- Date created
- Title
- URL (which you can click to open the page in your browser)
- Folder (the folder where the bookmark is stored)

In the **Autofills** section, you can view information on the user's autofill forms on different websites. You can find the following information:

- Full name
- First name
- Middle name
- Last name
- Organization
- Street address
- City
- Postal code
- Country
- Phone
- Email

In the **Pages Transitions** section, you can view information on the websites which the user opened by entering their URLs into the address bar.

- Date created
- URL (which you can click to open the page in your browser)
- Hidden

You can export Chrome data to your computer by clicking the **Export** button.

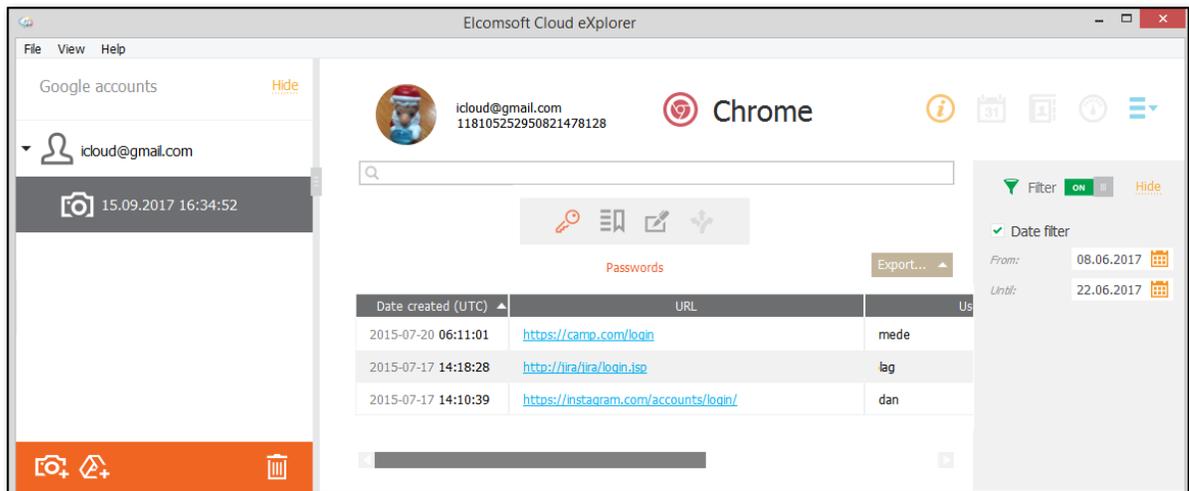
### Searching and Filtering

To perform searches in any section of the **Chrome** plugin, fill the search field and press **Enter**. The search results will be highlighted in yellow.

To filter out records in any section of the **Chrome** plugin, open the **Filter** pane by clicking the  icon on the right.

Enable filtering by switching the On/Off toggle, select the **Date** filter, and define the time interval in the **From** and **Until** fields.

You can export the Chrome data you have filtered. Click **Export** and select the **Filtered** option.

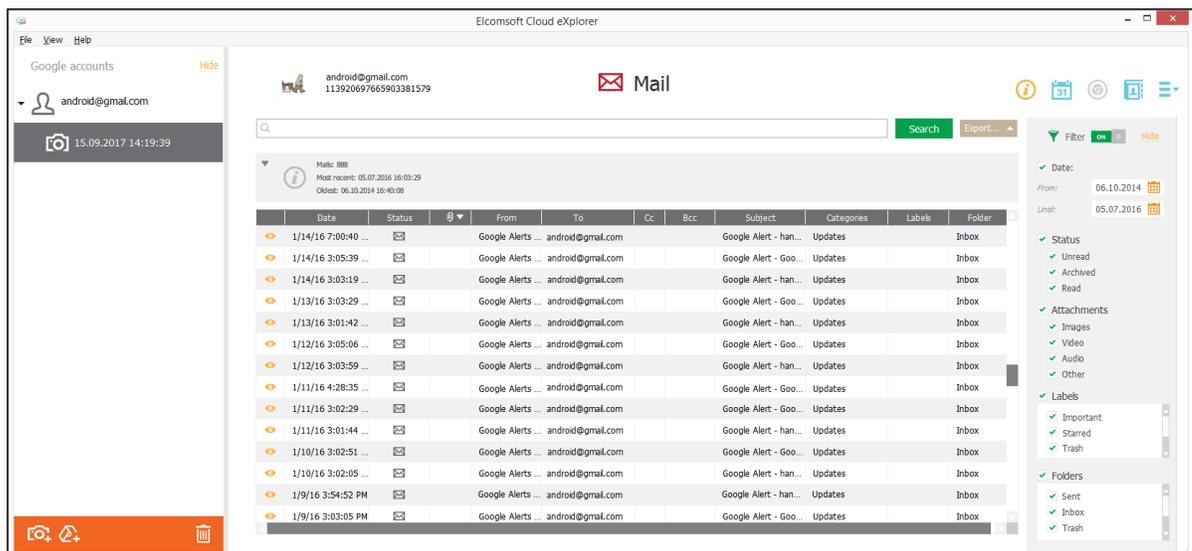


## 5.5.5 Mail

The **Mail** plugin allows you to view the data for Gmail accounts which includes the following:

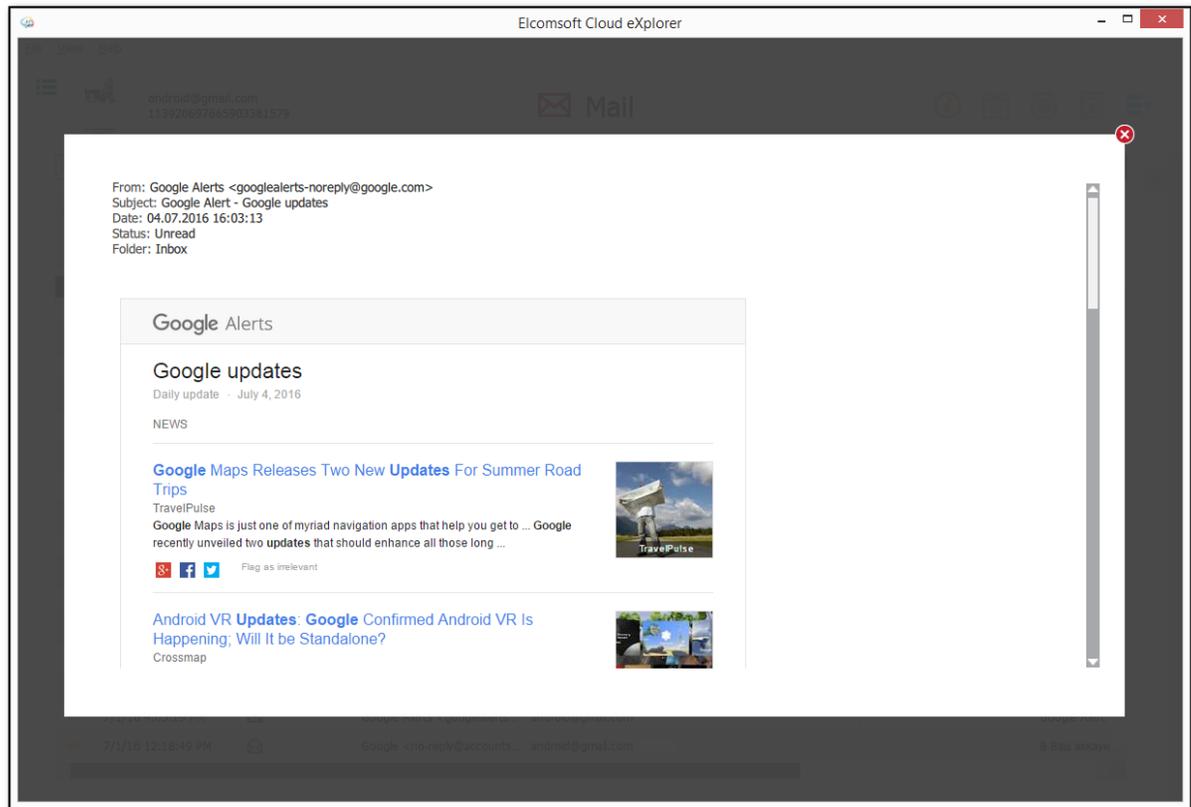
- **Date:** The date and time the email was received.
- **Status:** Read, unread, or archived.
- **Attachment:** Files attached to an email.
- **From:** The address from which an email was sent.
- **To:** The address to which an email was sent.
- **Cc:** Email addresses of users to which an email copy is sent.
- **Bcc:** Hidden email addresses of users to which an email copy is sent.
- **Subject:** The subject of an email.
- **Categories:** The category of an email.
- **Labels:** The label of an email.
- **Folder:** The folder of an email.

You can export mail data to your computer by clicking the **Export** button. Data is exported to an XLSX file, and all attached files are saved to a folder in the same location as the XLSX file.



## Viewing Messages

To view an email message, click the  icon for the selected record. The window containing a message will open and there you can view an email body and the other information such as: subject, date, status, etc.

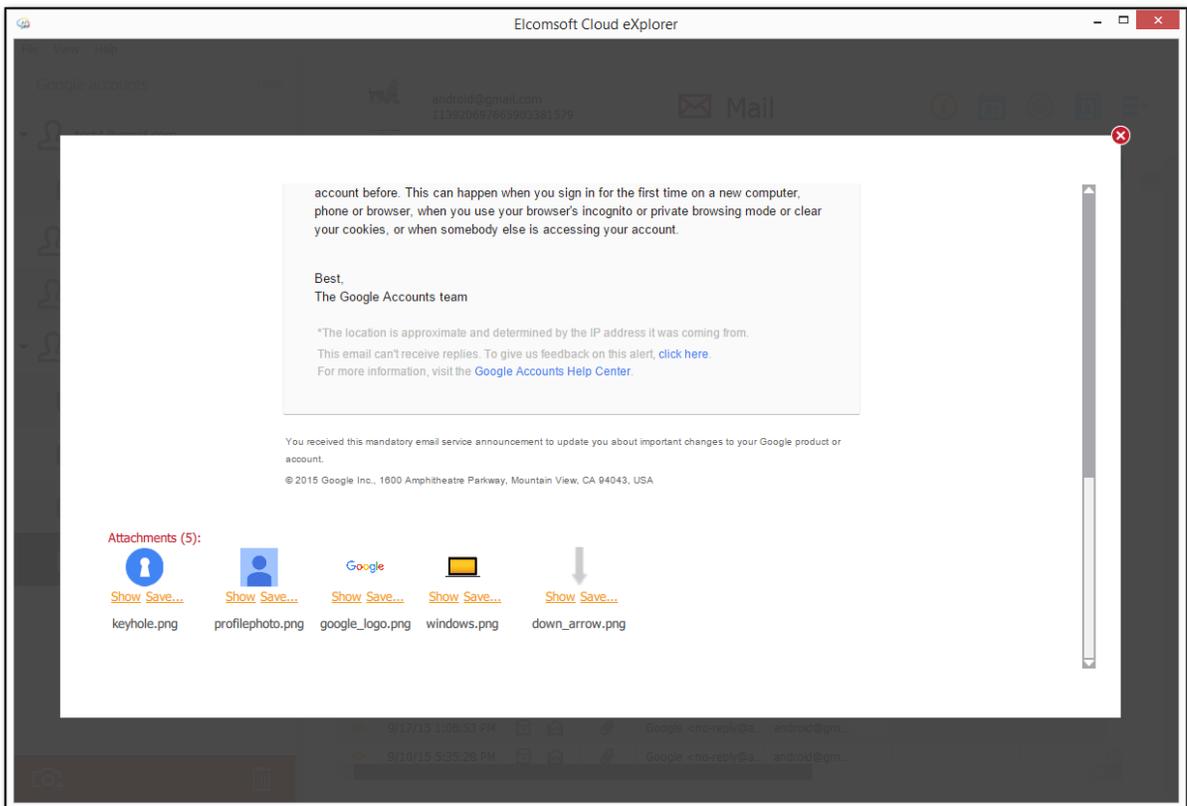


If there is an email thread, you can view all of its messages. The number of messages in the thread is displayed next to **Conversation** below the body of the opened email message. To view the content of other messages, click **Unfold**.

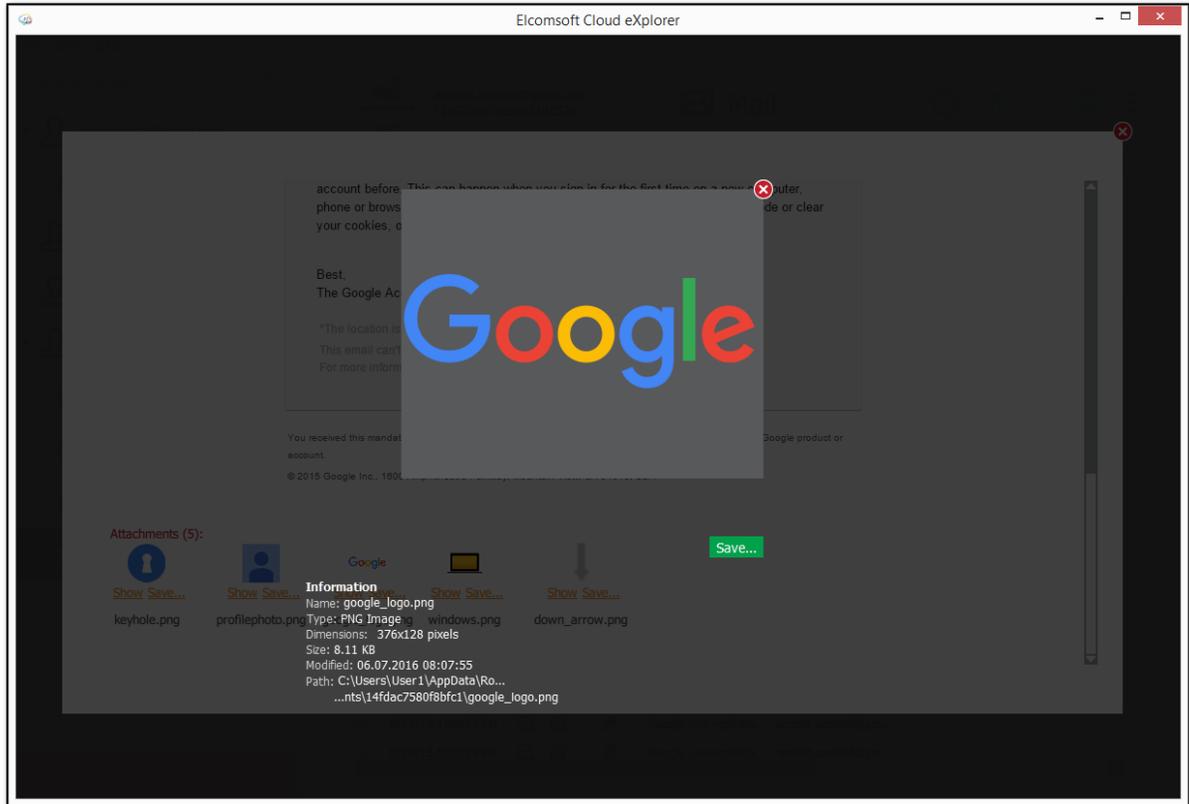


## Viewing Attachments

Email attachments are displayed below the email body.



To view an attachment, click **Show** for the selected file. The attachment will open in a window in which you can view the information about the attached file such as size, type, name, etc. For attached images you can also view the EXIF data (if any).



To save an attachment to your computer, do the following:

1. Click **Save** in the window with the opened attachment or click **Save** for the selected attachment in the window with the opened email message.
2. The **Save File** window opens.
3. In the opened window, define the location on your computer to which the file must be saved.
4. Click the **Save** button in the window.

### Searching and Filtering

To perform searches in the **Mail** plugin, fill the search field and press **Search**. The search results will be highlighted in yellow. If the search results are found in the email body, the  icon is highlighted.

To filter out records of the **Mail** plugin, open the **Filter** pane by clicking the  icon on the right. Enable filtering by switching the On/Off toggle and define the filtering options:

- **Date:** filters messages by date. Define the time interval in the **From** and **Until** fields.
- **Status:** filters messages by the status of an email. Select one or more of the following options: **Read, Unread, Archived**.
- **Attachments:** filters messages by attachment types. Select one or more of the following options: **Images, Video, Audio, Other (documents, archives, etc.)**.
- **Labels:** filters messages by labels. Select one or more options in the **Labels** list. The number of options depends upon the number of labels created by the user in Gmail.

- **Folders:** filters messages by folders. Select one or more options in the **Folders** list. The number of options depends upon the number of folders created by the user in Gmail.

You can export the mail data you have filtered. Click **Export** and select the **Filtered** option.

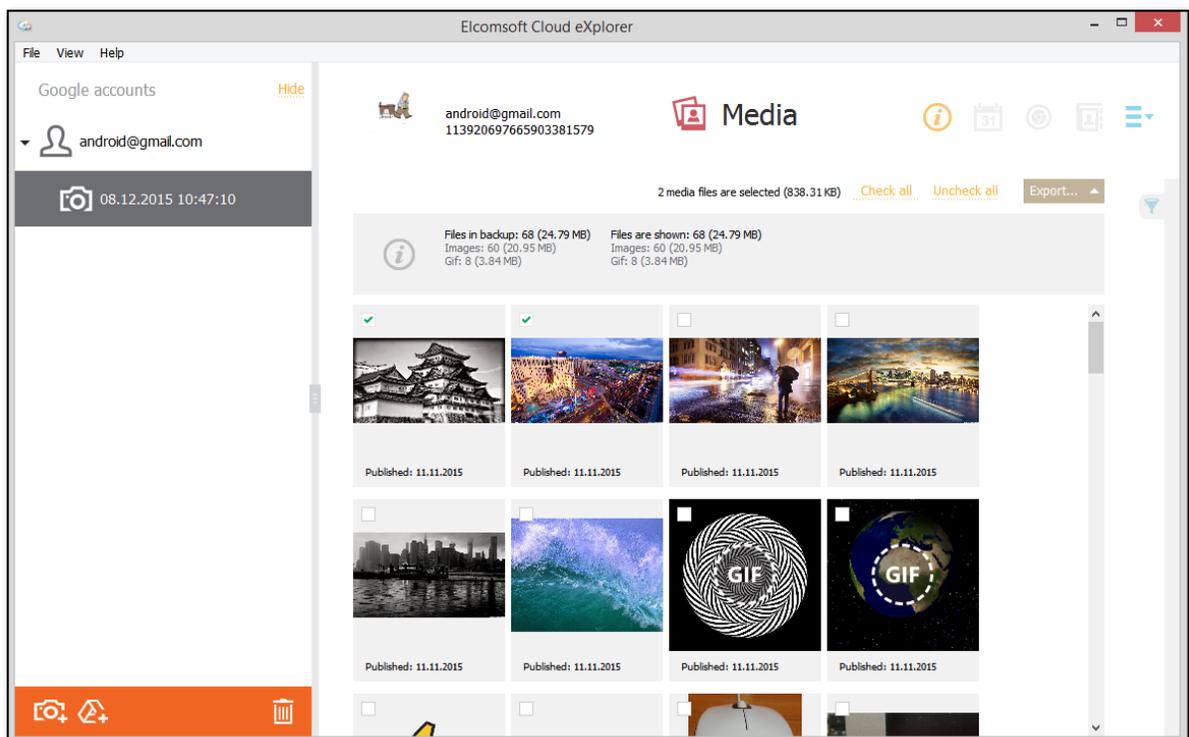
## 5.5.6 Media

With the **Media** plugin, you can view the user's photos stored in Google Photos.

When you open the **Media** plugin, you can see:

- Total number of files in backup and the number of files displayed.
- A grid with the thumbnails of all the user's photos sorted by creation date (starting with the most recent ones).

You can export media files to your computer by clicking the **Export** button. You can export either selected files or all files.



### Viewing Media Files

To view a certain photo, click it in the grid. The photo opens in the viewer where you can navigate between photos as well as view the following properties for each one:

- **General information:**
  - Id
  - Path: the path to the location where the file is stored on your computer.
  - Content URL: a URL to the file, which you can click to open the file in your browser.
  - Type
  - Dimensions: the image size in pixels.
  - Size
  - Published: date and time the file was published.

- **Account information:**

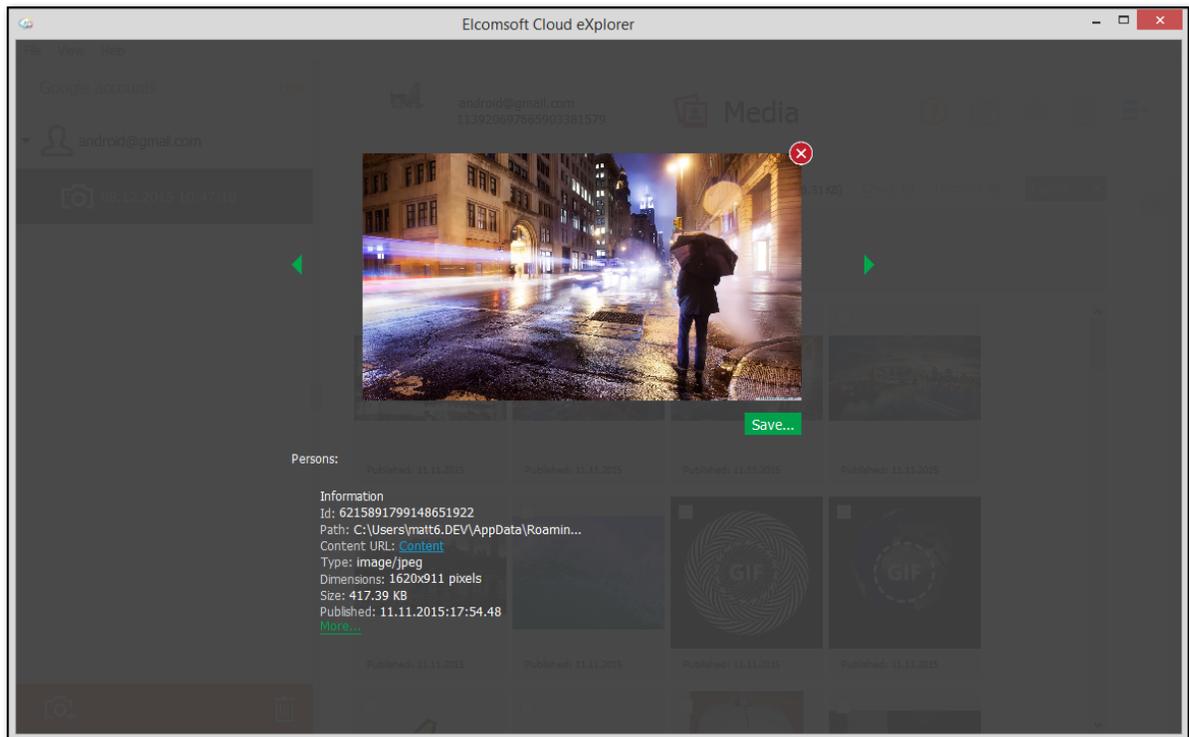
- Id
- Name
- Email
- Nickname
- URL: a URL to the account, which you can click to view it in your browser.
- Interactions rank

- **Album information:**

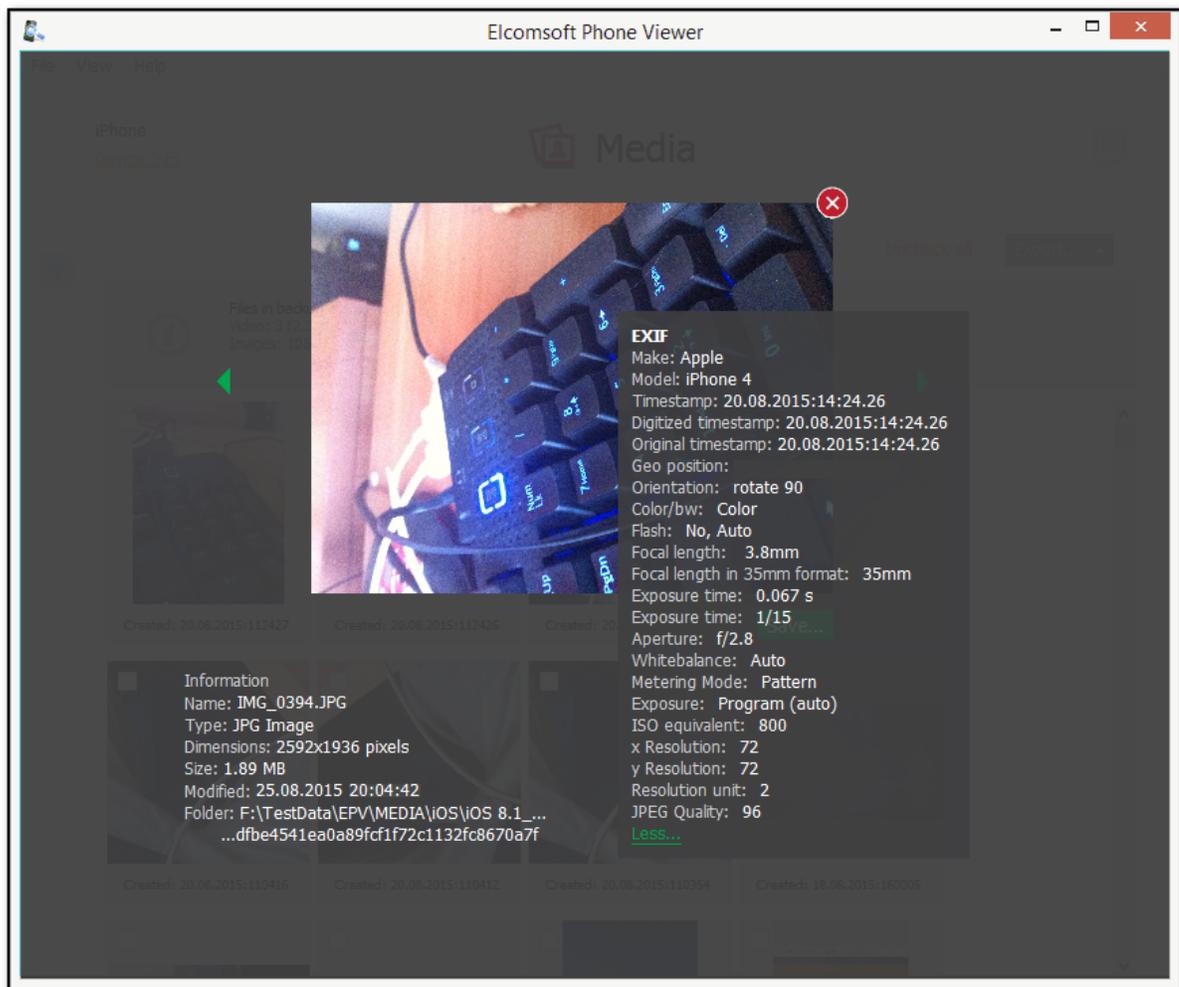
- Id
- Name
- Title
- Subtitle
- Icon URL: a URL to the album icon, which you can click to view it in your browser.

The property fields that have no data are not displayed.

You can save the photo to your computer by clicking the **Save** button in the viewer and selecting the desired destination.



If the image has EXIF properties, they will be displayed in the EXIF properties section. It contains additional properties of the image made by digital camera or scanner.



Below the photo, you can also see information on the users tagged in the photo (if any).

## Filtering

To filter out the photos, open the **Filter** pane by clicking the  icon on the right.

Enable filtering by switching the On/Off toggle and define the filtering options:

- **Date created:** filters the media created within a specific time period. Select the **From** and **Until** dates in the respective drop-down lists.
- **Photos:** filters photo images
- **Gifs:** filters .gif files
- **Google Albums:** filters the photos from specific albums

You can export the media files you have filtered. Click **Export** and select the **All filtered** option.

## 5.5.7 Messages

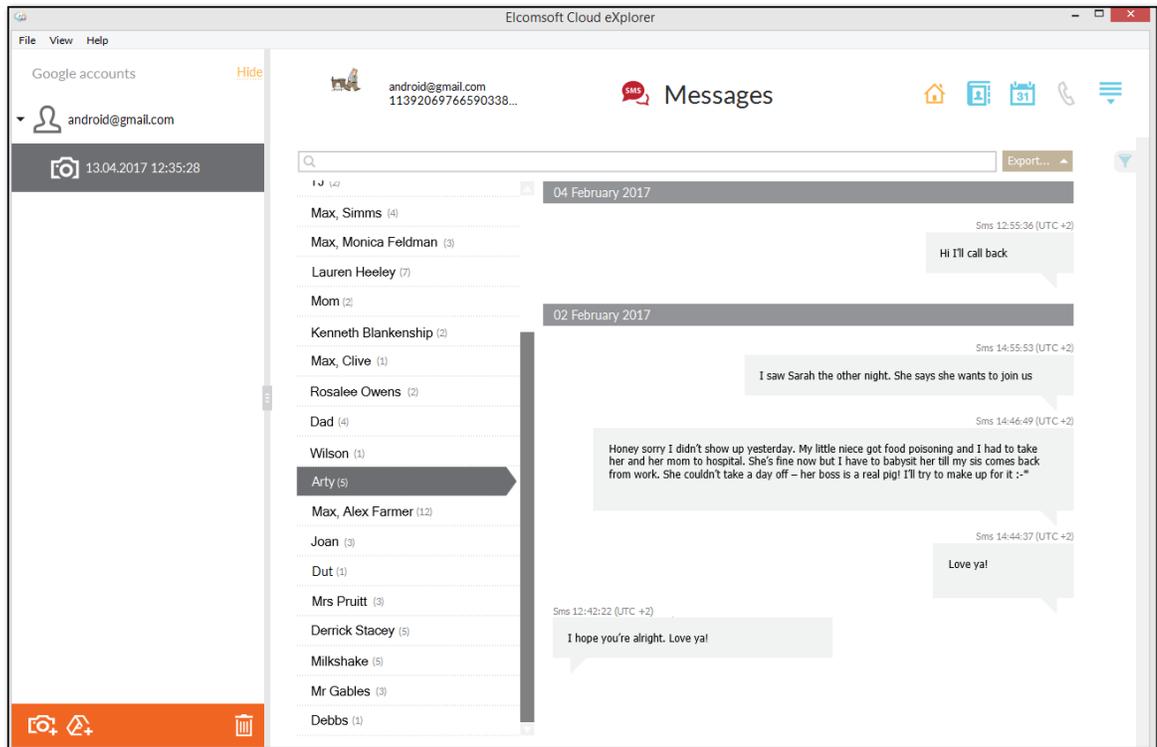
The **Messages** plugin allows viewing text messages that were backed up from devices to the Google drive. You can view SMS and the text content of MMS messages (the MMS attachments are not extracted).

**NOTE:** The **Messages** information will not be downloaded, if Android device (v. 9.0 and higher) is protected by the cryptographic key or passcode.

The left pane of the window shows the contacts who the user sent and/or received SMS from. Messages with the most recent messages are displayed on top. In the right pane, you can see the message history for a selected user, with the most recent messages on top. Incoming messages are shown on the left and outgoing messages are shown on the right. The number of messages for every contact is shown in brackets. You can also view group chats and see which user sent each of the messages.

Text messages are displayed as plain text. The emoji are displayed in both message texts and contacts (they are supported for other plugins as well).

You can export message history to your computer by clicking the **Export** button.



### Searching and Filtering

To perform searches in **Messages**, fill the search field and press **Enter**. The search results will be highlighted in yellow.

To filter out messages, open the **Filter** pane by clicking the  icon on the right.

Enable filtering by switching the On/Off toggle and define the filtering options:

- **Dates:** filters messages by date. Define the time interval in the **From** and **Until** fields.
- **Chats:** filters messages by chat type. Define whether you need **Group** or **Individual** chats.
- **Direction:** filters messages by their type. Define whether you need **Incoming**, **Outgoing**, or **Not Sent** messages.

- **Devices:** filters messages by devices they were sent from/received on (i.e., by specific backups stored on the Google drive).
- **Personal numbers:** filters messages by phone numbers they were sent from/received on.

You can export the messages you have filtered. Click **Export** and select the **Filtered** option.

To copy the whole message, right-click on it and select **Copy message**. To copy a part of the message, click the area where the text is to be copied from, highlight the text, right-click and select **Copy** or **Select All**.

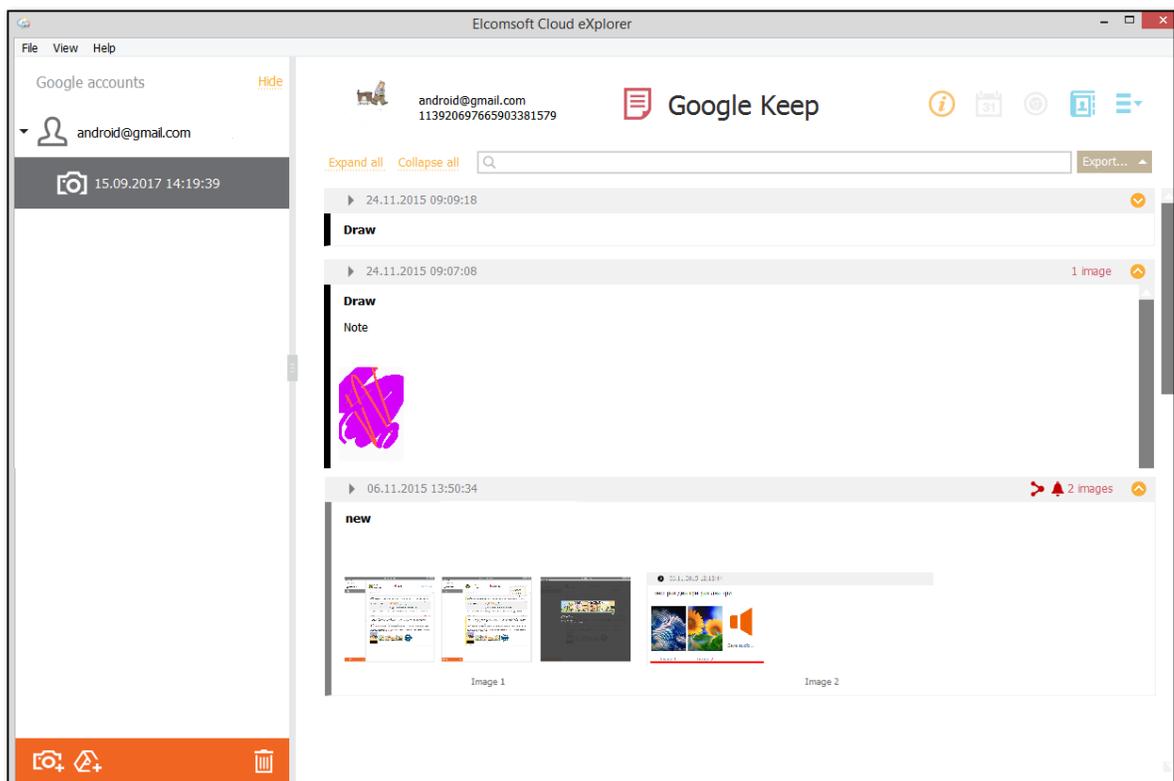
### 5.5.8 Google Keep

The **Google Keep** plugin allows viewing the user's notes downloaded from Google Keep.

You can view the list of the user's notes, with the most recent ones on top. You can view the following types of notes:

- **Note:** a text reminder
- **List:** a checkbox list and a text.

You can export Google Keep data to your computer by clicking the **Export** button. Data is exported to an XLSX file, and all attached files are saved to a folder in the same location as the XLSX file.



Click the  icon at the top-right corner of the note to expand the note body. Click the  icon at the top-left corner of the note to view the note data, such as:

- Date modified

- Date created
- Owner
- Last modifier
- Shared (the list of users who the note is shared with)
- Share date
- Label
- Reminder (reminder details. A reminder can have one of the following types: **Remind me on location** and **Remind me on day**)

The notes shared with other users have the  icon at the top-right corner. You can move your mouse pointer to the icon to see a tooltip with the names of the users the note is shared with.

The notes that have a reminder are marked with the  icon at the top-right corner. You can move your mouse pointer to the icon to see a tooltip with the reminder details.

The notes that have a label are marked with the  icon at the top-right corner. You can move your mouse pointer to the icon to see a tooltip with the label details.

You can view images embedded in the notes. Click the image thumbnail to preview the image. To save the image to your computer, click **Save** in the image preview mode and specify the desired destination.

You can also view the following information in the image preview mode:

- Time created
- Time last updated
- MIME Type
- File name
- Dimensions
- Size

To perform searches in the **Google Keep** plugin, fill the search field and press **Enter**. The search results will be highlighted in yellow.

You can export the Google Keep data you have filtered out with your search. Click **Export** and select the **Filtered** option.

You can expand or collapse all the notes by clicking **Expand all** or **Collapse all** next to the search field.

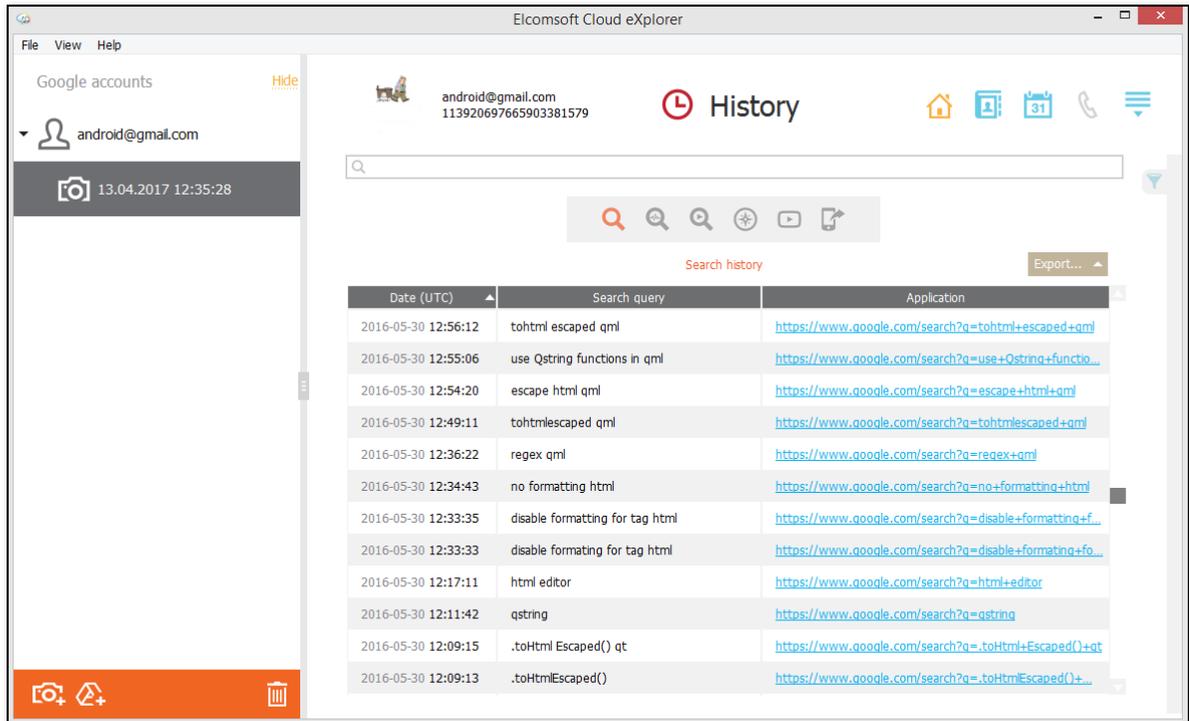
### 5.5.9 History

The **History** plugin allows viewing the user's Google History information. The **History** plugin has the following sections:

- **Search History**: a grid with data on Google search queries, the date and time, and the URLs, which you can click to open the pages in your browser.
- **Voice search history**: a grid with data on voice search queries, the date and time, the URLs, which you can click to open the pages in your browser, and the links to .mp3 audio files. You can click the links to hear the voice search recordings in the audio player installed in your system.
- **Youtube search history**: a grid with data on YouTube search queries, the date and time, and the URLs, which you can click to open the pages in your browser.
- **Visited tree history**: a grid with data on the web-pages visited by the user, the date and time of the visits, the status (viewed, visited or general), and the source.
- **Youtube watch history**: a grid with the titles of watched videos, the date and time, duration, views, and source. It also contains the URLs, which you can click to open the pages in your browser, and the links to thumbnails. You can click these links to view the videos in your browser.

- **Device history:** a grid with data on the devices from which the user logged into his/her Google account, the devices activity, and the date and time of the activity.

You can export History data to your computer by clicking the **Export** button. Data is exported to an XLSX file, and voice search history records are saved to a folder in the same location as the XLSX file.



## Searching and Filtering

To perform searches in any section of the **History** plugin, fill the search field and press **Enter**. The search results will be highlighted in yellow.

To filter out records in any section of the **History** plugin, open the **Filter** pane by clicking the  icon on the right.

Enable filtering by switching the On/Off toggle, select the **Date** filter, and define the time interval in the **From** and **Until** fields.

You can export the History data you have filtered. Click **Export** and select the **Filtered** option.

### 5.5.10 Wi-Fi

The **Wi-Fi** plugin allows you to explore the information on Wi-Fi connections stored in the user's Google account. This information is available if the Google account user chose to back up his/her device and store the information in the Google account.

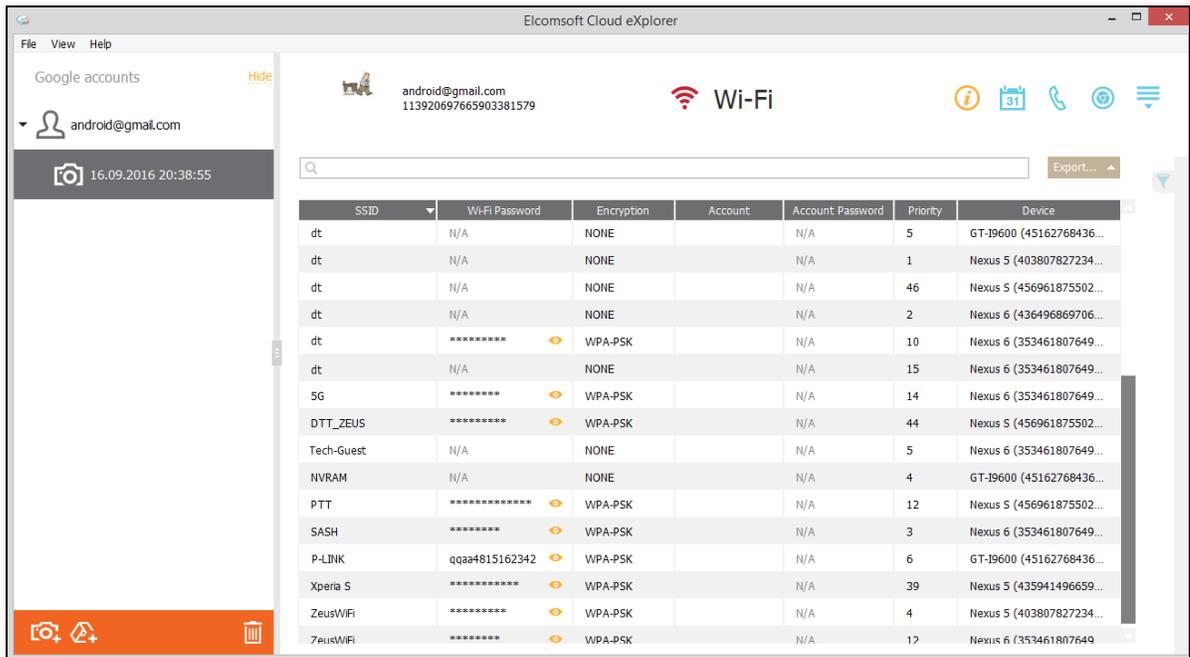
You can view the total number of Wi-Fi connections. The following information can be available on each connection:

- SSID

- Wi-Fi Password (you can click the  icon next to the password to view the characters)
- Encryption
- Account (the account under which the user connected to WiFi)
- Account Password
- Priority (the WiFi connection priority)
- Device (device model and IMEI)

**NOTE:** The **Wi-Fi** information will not be downloaded, if Android device (v. 9.0 and higher) is protected by the cryptographic key or passcode.

You can export Wi-Fi data to your computer by clicking the **Export** button.



SSID	Wi-Fi Password	Encryption	Account	Account Password	Priority	Device
dt	N/A	NONE		N/A	5	GT-I9600 (45162768436...
dt	N/A	NONE		N/A	1	Nexus 5 (403807827234...
dt	N/A	NONE		N/A	46	Nexus 5 (456961875502...
dt	N/A	NONE		N/A	2	Nexus 6 (436496869706...
dt	***** 	WPA-PSK		N/A	10	Nexus 6 (353461807649...
dt	N/A	NONE		N/A	15	Nexus 6 (353461807649...
5G	***** 	WPA-PSK		N/A	14	Nexus 6 (353461807649...
DTT_ZEUS	***** 	WPA-PSK		N/A	44	Nexus 5 (456961875502...
Tech-Guest	N/A	NONE		N/A	5	Nexus 6 (353461807649...
NVRAM	N/A	NONE		N/A	4	GT-I9600 (45162768436...
PTT	***** 	WPA-PSK		N/A	12	Nexus 5 (456961875502...
SASH	***** 	WPA-PSK		N/A	3	Nexus 6 (353461807649...
P-LINK	qqaa4815162342	WPA-PSK		N/A	6	GT-I9600 (45162768436...
Xperia S	***** 	WPA-PSK		N/A	39	Nexus 5 (435941496659...
ZeusWiFi	***** 	WPA-PSK		N/A	4	Nexus 5 (403807827234...
7eUsWiFi	***** 	WPA-PSK		N/A	12	Nexus 6 (353461807649...

## Searching and Filtering

To perform searches in **Wi-Fi**, fill the search field and press **Enter**. The search results will be highlighted in yellow.

To filter out the call records by groups, open the **Filter** pane by clicking the  icon on the right. Enable filtering by switching the On/Off toggle and define the filtering options:

- **Encryption:** filters Wi-Fi connections by encryption. Select the encryption type
- **Devices:** filters Wi-Fi connections by devices they are associated with. Select the desired devices.

You can export the Wi-Fi data you have filtered. Click **Export** and select the **Filtered** option.

## 5.5.11 Chats

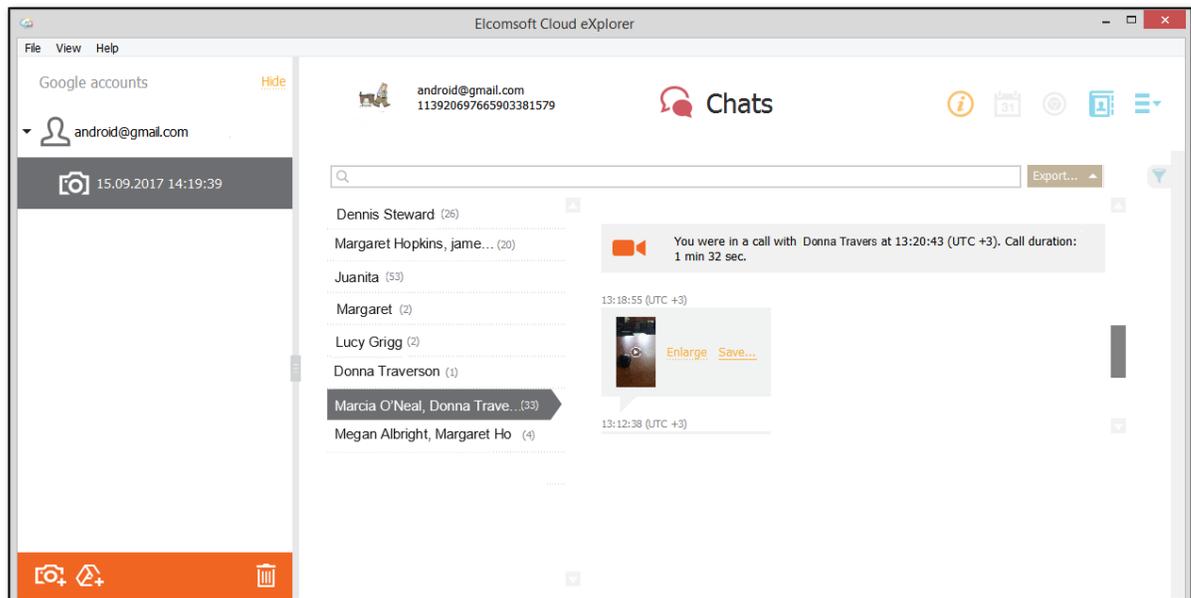
ECX allows viewing Google Hangouts chats.

The left pane of the window shows the contacts who the user has had chats with. Chats with the most recent messages are displayed on top. In the right pane, you can see the chat history for a selected user, with the most recent messages on top. Incoming messages are shown on the left and outgoing messages are shown on the right. The number of messages for every contact is shown in brackets. You can also view group chats and see which user sent each of the messages. The emoji are displayed in both message texts and contacts (they are supported for other plugins as well).

You can view the following type of messages:

- Text message
- Message with attached images
- Message with attached videos
- Video chat
- Geographic location

You can export chat history to your computer by clicking the **Export** button. Data is exported to an XLSX file, and all attached files are saved to a folder in the same location as the XLSX file.



### Viewing text messages

Text messages are displayed as plain text. If a message contains a URL, you can click it, and the page will open in your browser.

### Viewing attached images

If a conversation contains an image, its thumbnail is displayed in the conversation. Click **Enlarge** to open a full-size image in the viewer and view its properties:

- **From** (the sender)
- **Received** (date and time)
- **Type** (the file format)
- **Dimensions** (the image size in pixels)
- **Size** (the image size in KB)

- **Link** (the URL to the image, which you can click to view it in your browser)
- **Path** (the path to the location on your computer where the file is stored)

To save an image, click **Save** next to the thumbnail or the image in the viewer and specify the desired destination.

#### Viewing attached videos

If a conversation contains a video attachment, you can see its preview. Click **Enlarge** to open a full-size preview image and view its properties.

To save a video preview, click **Save** next to the video preview or the image in the viewer and specify the desired destination.

#### Viewing video chats

The following information is displayed for this type of message:

- The names of the video chat participants
- Video chat start time
- The number of video chat participants
- Duration
- The number of users who did not participate in the video chat

#### Viewing geographic location

If a message contains a geographic location (the location name or the coordinates), you can click it. A Google map will open in your browser.

#### Searching and Filtering

To perform searches in **Chats**, fill the search field and press **Enter**. The search results will be highlighted in yellow.

To filter out messages, open the **Filter** pane by clicking the  icon on the right.

Enable filtering by switching the On/Off toggle and define the filtering options:

- **Dates:** filters messages by date. Define the time interval in the **From** and **Until** fields.
- **Direction:** filters messages by their type. Define whether you need the **Incoming** or **Outgoing** messages
- **Show messages that contain:** filters messages by the attachment type. Define whether you need the messages that contain all attachments, locations or images.

You can export the chat history you have filtered. Click **Export** and select the **Filtered** option.

To copy the whole message, right-click on it and select **Copy message**. To copy a part of the message, click the area where the text is to be copied from, highlight the text, right-click and select **Copy** or **Select All**.

### 5.5.12 User Info

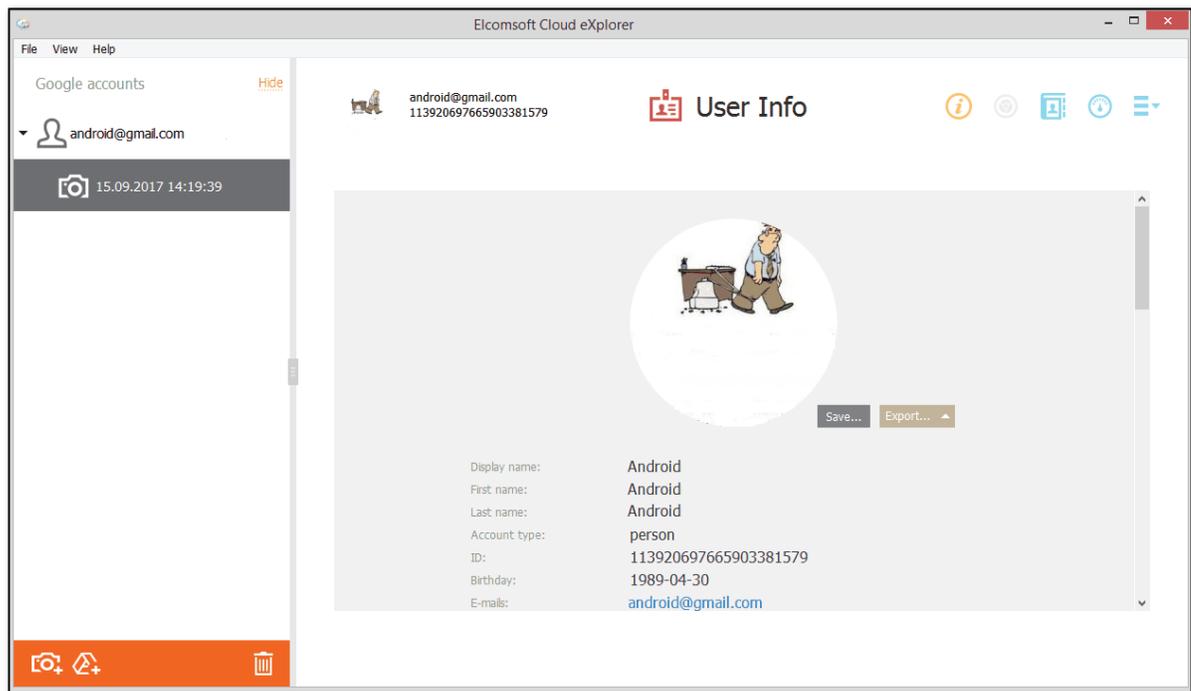
ECX allows viewing the Google account user data. The information that can be available includes the following:

- **Basic information:**
  - User picture
  - Display name
  - First name
  - Last name
  - Birthdate

- ID
- Account type (person or company)
- Primary email
- URLs to social network profiles (you can click the links to open the pages in your browser)
- **Additional information:**
  - URL
  - Nickname
  - Marital status
  - User domain
  - Organization
  - Job Title
  - Location
  - Skills

You can save the user's picture by clicking the **Save** button.

You can export the user info data to your computer by clicking the **Export** button. Data is exported to an XLSX file, and the user's profile picture is saved to a folder in the same location as the XLSX file.



### 5.5.13 Google Fit

The **Activity** category of the **Google Fit** plugin allows you to view the information about the user's activity and includes the following subcategories:

- **Active Minutes:** The information about the user's activity periods.
- **Heart points:** The information about the heart points assigned to the user during the activity periods.
- **Activity Segment:** The information about the types of activity performed by the user.
- **Walking and running:** The information about speed and distance during the walking and running activities.
- **Steps:** The information about steps taken by the user.
- **Locations:** The information about the user's locations during the activity sessions.

- **Sessions:** The information about the user's activity sessions.

You can export the **Google Fit** information to an XLSX file by clicking the **Export** button.

In the **Active Minutes** subcategory, you can view the following data:

- **Start date:** The date, time and timezone the activity started
- **End date:** The date, time and timezone the activity ended
- **Modification date:** The date, time and timezone of any changes made to the activity data
- **Activity Source:** The name of the data source
- **Package name:** The name of the used Google service
- **Device:** The name of the device used for recording the activity data
- **Value (min):** The duration of the activity period in minutes.

The screenshot displays the Elcomsoft Cloud eXplorer interface for Google Fit data. The main content area shows a table of activity records under the 'Active Minutes' subcategory. The table has the following columns: Start date, End date, Modification date, Activity Source, Package name, Device, and Value (min). The records show activity periods with a value of 1 minute each, occurring between 09:39:00 and 12:43:00 on 20.01.2020. The Activity Source is 'com.google.active\_...' and the Package name is 'com.google.android...'. The Device is listed as 'N/A'.

Start date	End date	Modification date	Activity Source	Package name	Device	Value (min)
20.01.2020 12:42:00...	20.01.2020 12:43:00...	20.01.2020 14:02:26 ...	com.google.active_...	com.google.android...	N/A	1
20.01.2020 12:41:00...	20.01.2020 12:42:00...	20.01.2020 14:02:26 ...	com.google.active_...	com.google.android...	N/A	1
20.01.2020 11:08:00...	20.01.2020 11:09:00...	20.01.2020 12:38:56 ...	com.google.active_...	com.google.android...	N/A	1
20.01.2020 11:07:00...	20.01.2020 11:08:00...	20.01.2020 12:38:56 ...	com.google.active_...	com.google.android...	N/A	1
20.01.2020 10:57:00...	20.01.2020 10:58:00...	20.01.2020 11:01:31 ...	com.google.active_...	com.google.android...	N/A	1
20.01.2020 10:53:00...	20.01.2020 10:54:00...	20.01.2020 11:01:31 ...	com.google.active_...	com.google.android...	N/A	1
20.01.2020 10:52:00...	20.01.2020 10:53:00...	20.01.2020 12:38:57 ...	com.google.active_...	com.google.android...	N/A	1
20.01.2020 10:51:00...	20.01.2020 10:52:00...	20.01.2020 12:38:57 ...	com.google.active_...	com.google.android...	N/A	1
20.01.2020 09:40:00...	20.01.2020 09:41:00...	20.01.2020 11:01:31 ...	com.google.active_...	com.google.android...	N/A	1
20.01.2020 09:39:00...	20.01.2020 09:40:00...	20.01.2020 11:01:31 ...	com.google.active_...	com.google.android...	N/A	1

In the **Heart points** subcategory, you can view the following data:

- **Start date:** The date, time and timezone the activity started
- **End date:** The date, time and timezone the activity ended
- **Modification date:** The date, time and timezone of any changes made to the activity data
- **Activity Source:** The name of the data source
- **Package name:** The name of the used Google service
- **Device:** The name of the device used for recording the activity data
- **Points:** The number of heart points assigned.

The screenshot shows the Elcomsoft Cloud Explorer application window. At the top, there is a menu bar with 'File', 'View', and 'Help'. Below the menu, there is a navigation bar with a 'Back' button and a user profile section showing an email address and a phone number. The main header features the Google Fit logo and a search bar. A filter panel on the right side is open, showing filters for 'Date' (From: 01.10.2019, Until: 23.01.2020), 'Activity Source' (com.google.heart\_mi...), and 'Device' (Other, apple iphone(com.app...)).

The main content area displays a table of activity records. The table has the following columns: Start date, End date, Modification date, Activity Source, Package name, Device, and Points. The records are sorted by Start date in descending order.

Start date	End date	Modification date	Activity Source	Package name	Device	Points
20.01.2020 09:39:00...	20.01.2020 09:40:00...	20.01.2020 11:01:31 ...	com.google.heart_minutes	com.google.fitkit	apple iphone...	1
20.01.2020 09:38:00...	20.01.2020 09:39:00...	20.01.2020 11:01:31 ...	com.google.heart_minutes	com.google.fitkit	apple iphone...	1
20.01.2020 09:37:00...	20.01.2020 09:38:00...	20.01.2020 11:01:31 ...	com.google.heart_minutes	com.google.fitkit	apple iphone...	1
17.01.2020 20:25:00...	17.01.2020 20:26:00...	19.01.2020 21:40:20 ...	com.google.heart_minutes	com.google.fitkit	apple iphone...	1
17.01.2020 20:24:00...	17.01.2020 20:25:00...	19.01.2020 21:40:20 ...	com.google.heart_minutes	com.google.fitkit	apple iphone...	1
17.01.2020 20:23:00...	17.01.2020 20:24:00...	19.01.2020 21:40:20 ...	com.google.heart_minutes	com.google.fitkit	apple iphone...	1
23.10.2019 12:36:00...	23.10.2019 12:37:00...	23.10.2019 12:57:09 ...	com.google.heart_minutes	com.google.androi...	N/A	2
23.10.2019 12:35:00...	23.10.2019 12:36:00...	23.10.2019 12:57:09 ...	com.google.heart_minutes	com.google.androi...	N/A	2
23.10.2019 12:34:00...	23.10.2019 12:35:00...	23.10.2019 12:57:09 ...	com.google.heart_minutes	com.google.androi...	N/A	2
23.10.2019 12:33:00...	23.10.2019 12:34:00...	23.10.2019 12:57:09 ...	com.google.heart_minutes	com.google.androi...	N/A	2

In the **Activity Segment** subcategory, you can view the following data:

- **Start date:** The date, time and timezone the activity started
- **End date:** The date, time and timezone the activity ended
- **Modification date:** The date, time and timezone of any changes made to the activity data
- **Activity Source:** The name of the data source
- **Package name:** The name of the used Google service
- **Device:** The name of the device used for recording the activity data
- **Activity type:** The name of the activity performed.

The screenshot displays the Elcomsoft Cloud eXplorer interface for Google Fit data. The main window shows a list of activity records with columns for Start date, End date, Modification date, Activity Source, Package name, Device, and Activity type. The records are filtered to show walking and running activities on a Google Pixel device.

Start date	End date	Modification date	Activity Source	Package name	Device	Activity type
23.01.2020 17:12:07 ...	23.01.2020 21:28:35 ...	24.01.2020 01:23:02...	com.google.activity...	com.google.androi...	Google Pixel...	Still (not moving)
22.01.2020 17:12:07 ...	23.01.2020 17:12:07 ...	23.01.2020 19:38:26...	com.google.activity...	com.google.androi...	Google Pixel...	Still (not moving)
21.01.2020 17:12:07 ...	22.01.2020 17:12:07 ...	22.01.2020 20:40:01...	com.google.activity...	com.google.androi...	Google Pixel...	Still (not moving)
21.01.2020 12:42:11 ...	21.01.2020 17:11:02 ...	21.01.2020 19:15:42...	com.google.activity...	com.google.androi...	Google Pixel...	Still (not moving)
20.01.2020 12:43:02 ...	21.01.2020 12:42:11 ...	21.01.2020 17:11:12...	com.google.activity...	com.google.androi...	Google Pixel...	Still (not moving)
20.01.2020 12:42:11 ...	20.01.2020 12:43:02 ...	20.01.2020 14:02:22...	com.google.activity...	com.google.androi...	Google Pixel...	Walking
20.01.2020 12:42:03 ...	20.01.2020 12:42:11 ...	20.01.2020 14:02:22...	com.google.activity...	com.google.androi...	Google Pixel...	Walking
20.01.2020 12:41:19 ...	20.01.2020 12:42:03 ...	20.01.2020 14:02:22...	com.google.activity...	com.google.androi...	Google Pixel...	Walking
20.01.2020 12:40:45 ...	20.01.2020 12:41:19 ...	20.01.2020 14:02:22...	com.google.activity...	com.google.androi...	Google Pixel...	Walking
20.01.2020 12:38:58 ...	20.01.2020 12:40:45 ...	20.01.2020 14:02:22...	com.google.activity...	com.google.androi...	Google Pixel...	Still (not moving)

In the **Walking and running** subcategory, you can view the following data:

- **Start date:** The date, time and timezone the activity started
- **End date:** The date, time and timezone the activity ended
- **Modification date:** The date, time and timezone of any changes made to the activity data
- **Activity Source:** The name of the data source
- **Package name:** The name of the used Google service
- **Device:** The name of the device used for recording the activity data
- **Average speed (km/h):** The average walking or running speed in km per hour
- **Distance (km):** The walking or running distance in km.

The screenshot displays the Elcomsoft Cloud Explorer interface for Google Fit. The user's email is @gmail.com and their ID is 118105252950821478128. The interface shows a search bar, an 'Export...' button, and a summary of 85 records. The 'Walking and running' subcategory is selected, showing a table of activity records with columns for Start date, End date, Modification date, Activity Source, Package name, Device, Average speed (km/h), and Distance (km).

Start date	End date	Modification date	Activity Source	Package name	Device	Average speed (km/h)	Distance (km)
21.01.2020 10:50:08...	21.01.2020 11:02:29 ...	21.01.2020 11:58:13...	com.google.distanc...	com.google.androi...	N/A	0.034	0.007
20.01.2020 12:41:02...	20.01.2020 12:43:02 ...	20.01.2020 14:02:24...	com.google.distanc...	com.google.androi...	Google Pixe...	2.467	0.082
20.01.2020 10:50:39...	20.01.2020 10:52:05 ...	20.01.2020 12:38:56...	com.google.distanc...	com.google.androi...	Google Pixe...	1.157	0.028
20.01.2020 10:52:05...	20.01.2020 10:53:05 ...	20.01.2020 12:38:56...	com.google.distanc...	com.google.androi...	Google Pixe...	1.234	0.021
20.01.2020 11:06:56...	20.01.2020 11:09:04 ...	20.01.2020 12:38:55...	com.google.distanc...	com.google.androi...	Google Pixe...	1.157	0.041
20.01.2020 11:06:23...	20.01.2020 11:08:24 ...	20.01.2020 12:38:52...	com.google.distanc...	com.google.androi...	N/A	0.519	0.017
20.01.2020 11:08:24...	20.01.2020 11:12:28 ...	20.01.2020 12:38:52...	com.google.distanc...	com.google.androi...	N/A	0.006	0
20.01.2020 09:38:28...	20.01.2020 09:38:59 ...	20.01.2020 11:01:31...	com.google.distanc...	com.google.androi...	Google Pixe...	4.628	0.04
20.01.2020 09:38:59...	20.01.2020 09:39:29 ...	20.01.2020 11:01:31...	com.google.distanc...	com.google.androi...	Google Pixe...	5.909	0.049
20.01.2020 09:39:29...	20.01.2020 09:39:59 ...	20.01.2020 11:01:31...	com.google.distanc...	com.google.androi...	Google Pixe...	5.035	0.042

In the **Steps** subcategory, you can view the following data:

- **Start date:** The date, time and timezone the activity started
- **End date:** The date, time and timezone the activity ended
- **Modification date:** The date, time and timezone of any changes made to the activity data
- **Activity Source:** The name of the data source
- **Package name:** The name of the used Google service
- **Device:** The name of the device used for recording the activity data
- **Steps:** The step count.

The screenshot displays the Elcomsoft Cloud eXplorer interface for Google Fit activity data. The main window shows a list of activity records with the following columns: Start date, End date, Modification date, Activity Source, Package name, Device, and Steps. The records are sorted by modification date in descending order.

Start date	End date	Modification date	Activity Source	Package name	Device	Steps
23.01.2020 12:38:21...	23.01.2020 12:38:52 ...	23.01.2020 12:39:04 ...	com.google.step_c...	com.google.androi...	N/A	0
22.01.2020 14:06:30...	22.01.2020 14:07:30 ...	22.01.2020 14:17:36 ...	com.google.step_c...	com.google.androi...	Google Pixe...	21
20.01.2020 12:42:11...	20.01.2020 12:43:02 ...	20.01.2020 14:02:27 ...	com.google.step_c...	com.google.androi...	Google Pixe...	54
20.01.2020 12:42:03...	20.01.2020 12:42:11 ...	20.01.2020 14:02:27 ...	com.google.step_c...	com.google.androi...	Google Pixe...	8
20.01.2020 12:41:19...	20.01.2020 12:42:03 ...	20.01.2020 14:02:27 ...	com.google.step_c...	com.google.androi...	Google Pixe...	48
20.01.2020 12:41:02...	20.01.2020 12:43:02 ...	20.01.2020 14:02:19 ...	com.google.step_c...	com.google.androi...	Google Pixe...	128
20.01.2020 12:40:45...	20.01.2020 12:41:02 ...	20.01.2020 14:02:27 ...	com.google.step_c...	com.google.androi...	Google Pixe...	6
20.01.2020 12:40:02...	20.01.2020 12:41:02 ...	20.01.2020 14:02:19 ...	com.google.step_c...	com.google.androi...	Google Pixe...	20
20.01.2020 11:08:24...	20.01.2020 11:09:04 ...	20.01.2020 12:38:56 ...	com.google.step_c...	com.google.androi...	Google Pixe...	20
20.01.2020 11:08:24...	20.01.2020 11:08:24 ...	20.01.2020 12:38:56 ...	com.google.step_c...	com.google.androi...	Google Pixe...	0

In the **Locations** subcategory, you can view the following data:

- **Start date:** The date, time and timezone the activity started
- **End date:** The date, time and timezone the activity ended
- **Modification date:** The date, time and timezone of any changes made to the activity data
- **Activity Source:** The name of the data source
- **Package name:** The name of the used Google service
- **Device:** The name of the device used for recording the activity data
- **Location:** The latitude and longitude displayed as a link to the Google Maps (after clicking the link, the Google Maps with the exact location will open automatically)
- **Altitude (m):** The altitude in meters above sea level
- **Accuracy (m):** The accuracy level in meters.

The screenshot shows the Elcomsoft Cloud Explorer application window. At the top, there's a navigation bar with 'File', 'View', and 'Help' menus. Below that, a user profile is displayed with an email address and a phone number. The main content area features the Google Fit logo and a search bar. A summary bar indicates 307 records, with the most recent and oldest records listed. Below this, there are tabs for 'Active Minutes', 'Heart points', 'Activity Segment', 'Walking and running', 'Steps', 'Locations', and 'Sessions'. The 'Locations' tab is selected, showing a table of activity records.

Start date	End date	Modification date	Activity Source	Package name	Device	Location	Altitude (m)	Accuracy (m)
23.01.2020 13:15:...	23.01.2020 13:15:...	23.01.2020 13:33:35...	com.google.location...	com.google.fitkit	apple iphon...	<a href="#">23.711288, 59.931288</a>	16	89.4
23.01.2020 12:41:...	23.01.2020 12:41:...	23.01.2020 13:33:35...	com.google.location...	com.google.fitkit	apple iphon...	<a href="#">23.711288, 59.931288</a>	23.7	89.1
22.01.2020 11:57:...	22.01.2020 11:57:...	22.01.2020 12:17:30...	com.google.location...	com.google.fitkit	apple iphon...	<a href="#">23.711288, 59.931288</a>	16	89.4
21.01.2020 18:24:...	21.01.2020 18:24:...	21.01.2020 19:15:35...	com.google.location...	com.google.fitkit	apple iphon...	<a href="#">23.711288, 59.931288</a>	16.5	89.4
21.01.2020 11:02:...	21.01.2020 11:02:...	21.01.2020 11:58:11...	com.google.location...	com.google.fitkit	apple iphon...	<a href="#">23.711288, 59.931288</a>	23.6	89.1
21.01.2020 10:50:...	21.01.2020 10:50:...	21.01.2020 11:02:20...	com.google.location...	com.google.fitkit	apple iphon...	<a href="#">23.711288, 59.931288</a>	26.7	89.4
20.01.2020 13:27:...	20.01.2020 13:27:...	20.01.2020 14:02:17...	com.google.location...	com.google.fitkit	apple iphon...	<a href="#">23.711288, 59.931288</a>	18	89.1
20.01.2020 13:27:...	20.01.2020 13:27:...	20.01.2020 14:02:17...	com.google.location...	com.google.fitkit	apple iphon...	<a href="#">23.711288, 59.931288</a>	1300	0
20.01.2020 11:12:...	20.01.2020 11:12:...	20.01.2020 12:38:51...	com.google.location...	com.google.fitkit	apple iphon...	<a href="#">23.711288, 59.931288</a>	17.2	96.3
20.01.2020 11:08:...	20.01.2020 11:08:...	20.01.2020 12:38:51...	com.google.location...	com.google.fitkit	apple iphon...	<a href="#">23.711288, 59.931288</a>	17	96.3

In the **Sessions** subcategory, you can view the following data:

- **Start date:** The date, time and timezone the activity session started
- **End date:** The date, time and timezone the activity session ended
- **Modification date:** The date, time and timezone of any changes made to the activity session data
- **Duration:** The duration of the activity session
- **Package name:** The name of the used Google service
- **Activity type:** The type of the activity session
- **Name:** The name of the activity session
- **Description:** The description of the activity session
- **Is deleted:** Displays if the activity session is deleted or not
- **Start location:** The latitude and longitude displayed as a link to the Google Maps (after clicking the link, the Google Maps with the exact start location of the session will open automatically)
- **Finish location:** The latitude and longitude displayed as a link to the Google Maps (after clicking the link, the Google Maps with the exact finish location of the session will open automatically)
- **Total calories (kcal):** The caloric output during the activity session (in kcal)
- **Route:** The activity session route displayed as a link to the Google Maps (after clicking the link, the Google Maps with the route of the session will open automatically).

Elcomsoft Cloud eXplorer

File View Help

Back

@gmail.com  
118105252950821478128

Google Fit

Export...

Activity

Records: 17  
Most recent record: 02.10.2019 11:01:00  
Oldest record: 01.10.2019 12:01:00

Shown records: 17  
Most recent filtered record: 02.10.2019 11:01:00  
Oldest filtered record: 01.10.2019 12:01:00

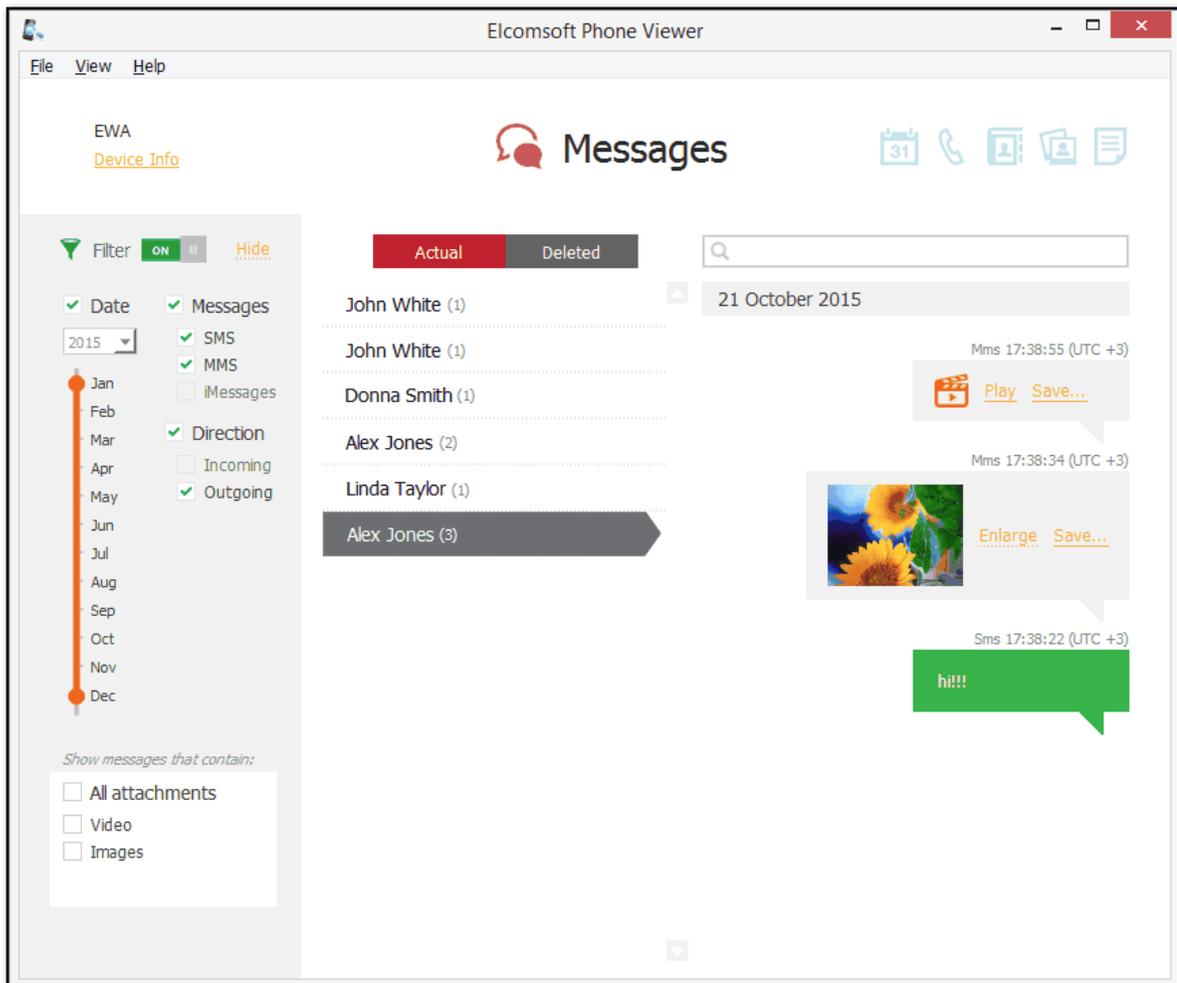
Active Minutes Heart points Activity Segment Walking and running Steps Locations Sessions

Start date	End date	Modification date	Duration	Package name	Activity type	Name	Description	Is deleted	Start lo
23.10.2019 11...	23.10.2019 1...	23.10.2019 11:48:52...	00h:00m:07s	com.google.androi...	Rowing	Rowing		No	
23.10.2019 11...	23.10.2019 1...	23.10.2019 12:57:11...	01h:00m:00s	com.google.androi...	Rowing	Rowing		No	
23.10.2019 10...	23.10.2019 1...	23.10.2019 11:48:52...	01h:00m:00s	com.google.androi...	Rowing machine	Rowing machine		No	N/A
16.10.2019 17...	16.10.2019 1...	16.10.2019 18:09:43...	01h:00m:00s	com.apple.health	Jogging	Running	N/A	No	N/A
16.10.2019 11...	16.10.2019 1...	16.10.2019 12:06:06...	00h:10m:24s	com.google.androi...	Running on sand	Running on sand		No	
16.10.2019 11...	16.10.2019 1...	16.10.2019 12:06:06...	00h:00m:06s	com.google.androi...	Baseball	every day I dre...		No	N/A
16.10.2019 10...	16.10.2019 1...	16.10.2019 12:06:06...	01h:00m:00s	com.google.androi...	Baseball			No	N/A
16.10.2019 00...	16.10.2019 0...	16.10.2019 14:01:11...	07h:38m:00s	com.google.androi...	Sleeping	N/A	N/A	No	N/A
15.10.2019 12...	15.10.2019 1...	15.10.2019 13:55:16...	00h:00m:04s	com.google.androi...	Badminton			No	N/A
15.10.2019 12...	15.10.2019 1...	15.10.2019 12:50:39...	00h:00m:11s	com.google.androi...	Hockey			No	N/A

## Searching and Filtering

To perform searches in the **Google Fit** plugin, fill the search field and press the **Enter** key. The search results will be highlighted in yellow.

To filter out records of the **Google Fit** plugin, open the **Filter** pane by clicking the



icon on the right.

Enable filtering by switching the On/Off toggle and define the filtering options:

- **Date:** filters the activity records by dates. Define the time interval in the **From** and **Until** fields.
- **Activity Source:** filters the activity records by the activity sources available for the certain subcategory. Select the activity source from the list (The **Other** option is available for the records with no activity source specified).
- **Device:** filters activity records by the device name available for the certain subcategory. Select the device name from the list (The **Other** option is available for the records with no device specified).
- **Package name:** filters **Sessions** records by the package name available for the **Sessions** subcategory. Select the the package name from the list.
- **Activity type:** filters **Sessions** records by the activity type available for the **Sessions** subcategory. Select the the activity type from the list.

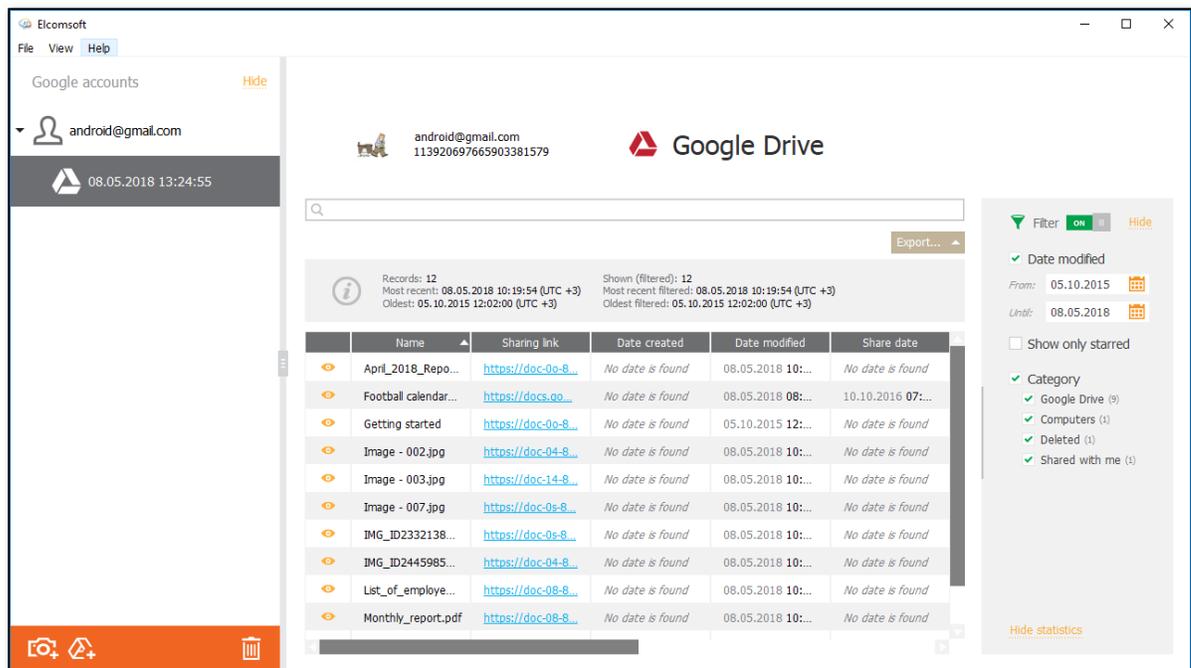
You can export the data you have filtered. Click **Export** and select the **Filtered** option.

### 5.5.14 Google Drive

The **Google Drive** plugin allows you to view the information about Google Drive files which includes the following:

- **Name:** The name of the file.
- **Sharing link:** The link via which the file can be shared (You can download files shared via a link by clicking the link in the table).
- **Date created:** The date and time the file was created.
- **Date modified:** The date and time the file was last modified.
- **Share date:** The date and time the file was shared.
- **Owner:** The owner of the file.
- **Last edited by:** The last user who edited the file.
- **Starred:** Defines whether the file is starred in Google Drive. (Yes/No)
- **Deleted:** Defines whether the file is deleted. (Yes/No)
- **Category:** The category the file belongs to (Google Drive/Computers/Shared with me/Deleted).

You can export information about downloaded Google Drive files to an XLSX file by clicking the **Export** button.



You can open files by clicking the  icon for the selected record. The file will open in the default application assigned to the type of file that you open.

#### Searching and Filtering

To perform searches in the **Google Drive** plugin, fill the search field and press the **Enter** key. The search results will be highlighted in yellow.

To filter out records of the **Google Drive** plugin, open the **Filter** pane by clicking the  icon on the right.

Enable filtering by switching the On/Off toggle and define the filtering options:

- **Date modified:** filters files by the date they were modified. Define the time interval in the **From** and **Until** fields.
- **Show only starred:** Select this option to show only files marked as starred in Google Drive.
- **Category:** filters files by the category they belong to. Select one or more of the following options: **Google Drive**, **Computers**, **Deleted**, **Shared with me**.

You can export the data you have filtered. Click **Export** and select the **Filtered** option.

### 5.5.15 Locations

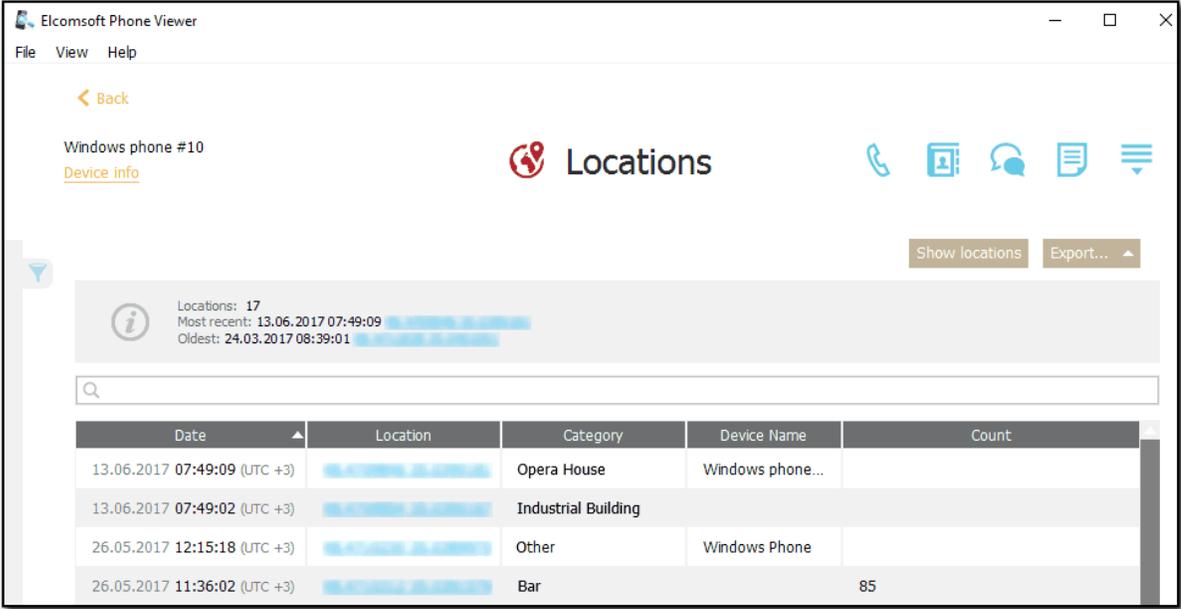
EPV allows you to view the Microsoft account user's location history downloaded from One Drive using Elcomsoft Phone Breaker.

You can find the following information:

- Date
- Location: Latitude and longitude of the location
- Category: Location category (e.g., bank, gym, etc.)
- Device Name
- Count: How many times the location was registered by the device

You can see information on the number of locations as well as on the most recent and the oldest locations.

All locations are sorted by date, with the most recent one on top.



Elcomsoft Phone Viewer

File View Help

< Back

Windows phone #10  
[Device info](#)

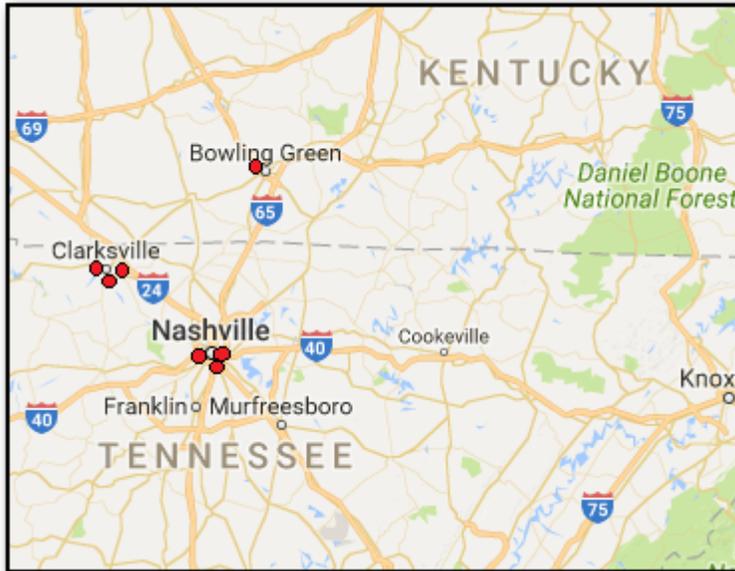
Locations

Show locations Export...

Locations: 17  
Most recent: 13.06.2017 07:49:09  
Oldest: 24.03.2017 08:39:01

Date	Location	Category	Device Name	Count
13.06.2017 07:49:09 (UTC +3)		Opera House	Windows phone...	
13.06.2017 07:49:02 (UTC +3)		Industrial Building		
26.05.2017 12:15:18 (UTC +3)		Other	Windows Phone	
26.05.2017 11:36:02 (UTC +3)		Bar		85

You can view the user's location history on a Google map by clicking the **Show locations** button. A Google map will open in your browser, displaying the user's locations marked with red points. Click a point to view its longitude, latitude, altitude, and time.



You can export information on locations to your computer by clicking the **Export** button. You can choose to export either all or all filtered locations. Please note that location data export for Windows Phone is only available in the registered version of the program.

### Searching and Filtering

To perform searches in **Locations**, enter the necessary value in the search field and press **Enter**. The search results will be highlighted in yellow.

To filter out locations, open the **Filter** pane by clicking the  icon on the right. Enable filtering by switching the **On/Off** toggle and define the filtering options:

- **Date:** Enter the desired dates into the **From** and **Until** fields.
- **Devices:** Select which device(s) you want to get location history from.

If you click **Show locations** after you filtered locations using either or both of the filters, only the filtered locations will be displayed on the Google map.

#### 5.5.15.1 Places

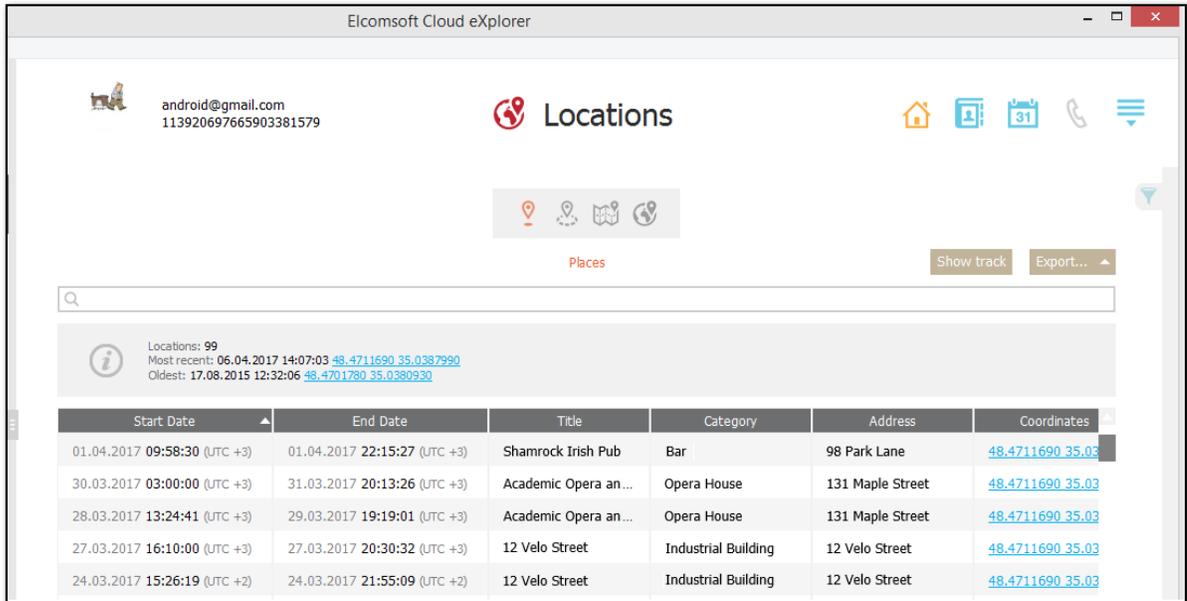
In the **Places** section of the **Locations** plugin, you can view the user's location history. You can find the following information:

- Start Date
- End Date
- Title
- Category: Location category (e.g., bank, gym, etc.)
- Address
- Coordinates

You can see information on the number of locations as well as on the most recent and the oldest locations.

All locations are sorted by date, with the most recent one on top.

You can export Places data to your computer by clicking the **Export** button.



The screenshot shows the Elcomsoft Cloud eXplorer application window. The title bar reads "Elcomsoft Cloud eXplorer". The main interface includes a user profile section with the email "android@gmail.com" and ID "113920697665903381579". The central heading is "Locations". Below this, there are navigation icons for home, user, calendar (showing "31"), phone, and a menu. A search bar is present. A summary box indicates "Locations: 99", with the most recent location at "06.04.2017 14:07:03" (coordinates 48.4711690, 35.0387990) and the oldest at "17.08.2015 12:32:06" (coordinates 48.4701780, 35.0380930). Below this is a table of location records.

Start Date	End Date	Title	Category	Address	Coordinates
01.04.2017 09:58:30 (UTC +3)	01.04.2017 22:15:27 (UTC +3)	Shamrock Irish Pub	Bar	98 Park Lane	<a href="#">48.4711690 35.0387990</a>
30.03.2017 03:00:00 (UTC +3)	31.03.2017 20:13:26 (UTC +3)	Academic Opera an...	Opera House	131 Maple Street	<a href="#">48.4711690 35.0387990</a>
28.03.2017 13:24:41 (UTC +3)	29.03.2017 19:19:01 (UTC +3)	Academic Opera an...	Opera House	131 Maple Street	<a href="#">48.4711690 35.0387990</a>
27.03.2017 16:10:00 (UTC +3)	27.03.2017 20:30:32 (UTC +3)	12 Velo Street	Industrial Building	12 Velo Street	<a href="#">48.4711690 35.0387990</a>
24.03.2017 15:26:19 (UTC +2)	24.03.2017 21:55:09 (UTC +2)	12 Velo Street	Industrial Building	12 Velo Street	<a href="#">48.4711690 35.0387990</a>

You can view the user's location history on a Google map by clicking the **Show track** button. A Google map will open in your browser, displaying the user's locations marked with red points. The most recent location is connected to the second most recent one, and so on. Click a point to view its address, category, coordinates, and start/end date and time data.



You can export information on locations to your computer by clicking the **Export** button. You can choose to export either all or all filtered locations.

### Searching and Filtering

To perform searches in **Places**, fill the search field and press **Enter**. The search results will be highlighted in yellow.

To filter out locations, open the **Filter** pane by clicking the  icon on the right.

Enable filtering by switching the **On/Off** toggle and define the filtering options:

- **Date:** Enter the desired dates into the **From** and **Until** fields.
- **Category:** Select the location category.

If you click **Show Track** after you filtered locations using either or both of the filters, only the filtered locations will be displayed on the Google map.

You can export the user's location history you have filtered. Click **Export** and select the **Filtered** option.

#### 5.5.15.2 Routes

In the **Routes** section of the **Locations** plugin, you can view the user's detailed location history including all parts of the route. You can find the following information on each part of the route:

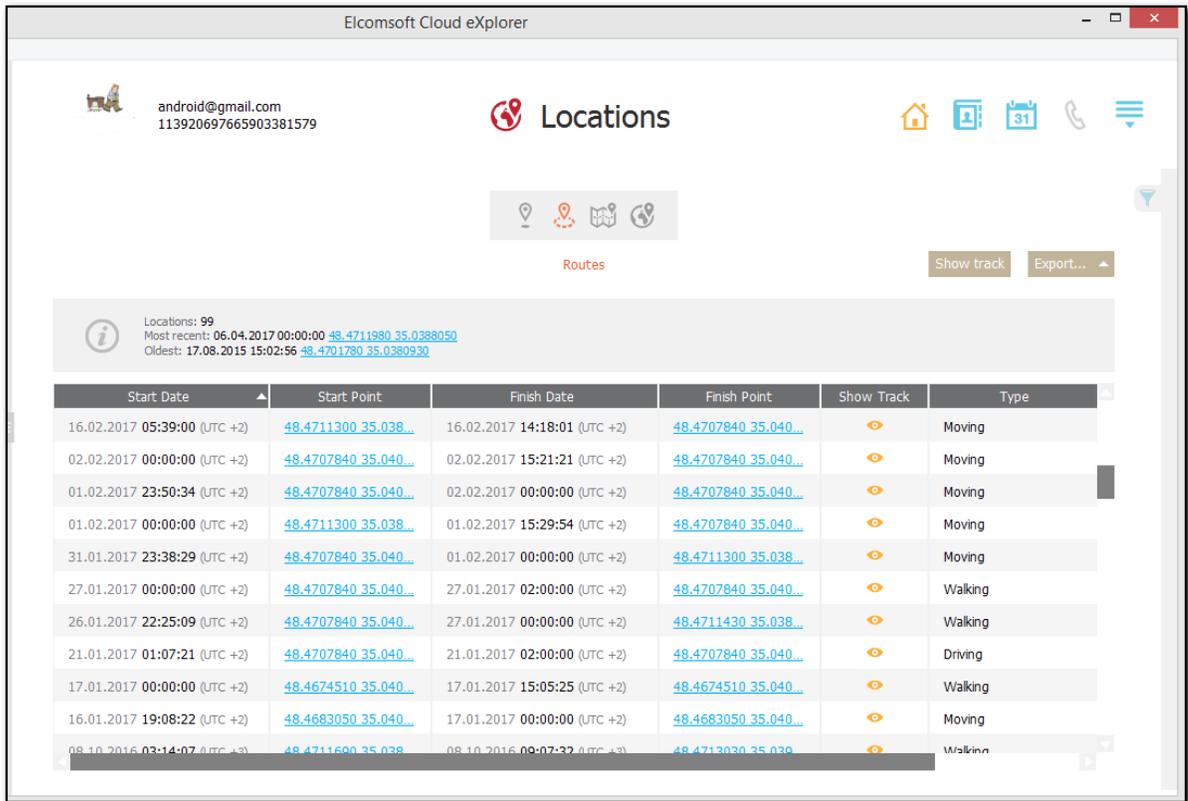
- Start Date
- Start Point

- Finish Date
- Finish Point
- Type: Type of movement (walking, driving, riding on a bus, etc.)
- Distance, km

You can see information on the number of stored locations as well as on the most recent and the oldest locations.

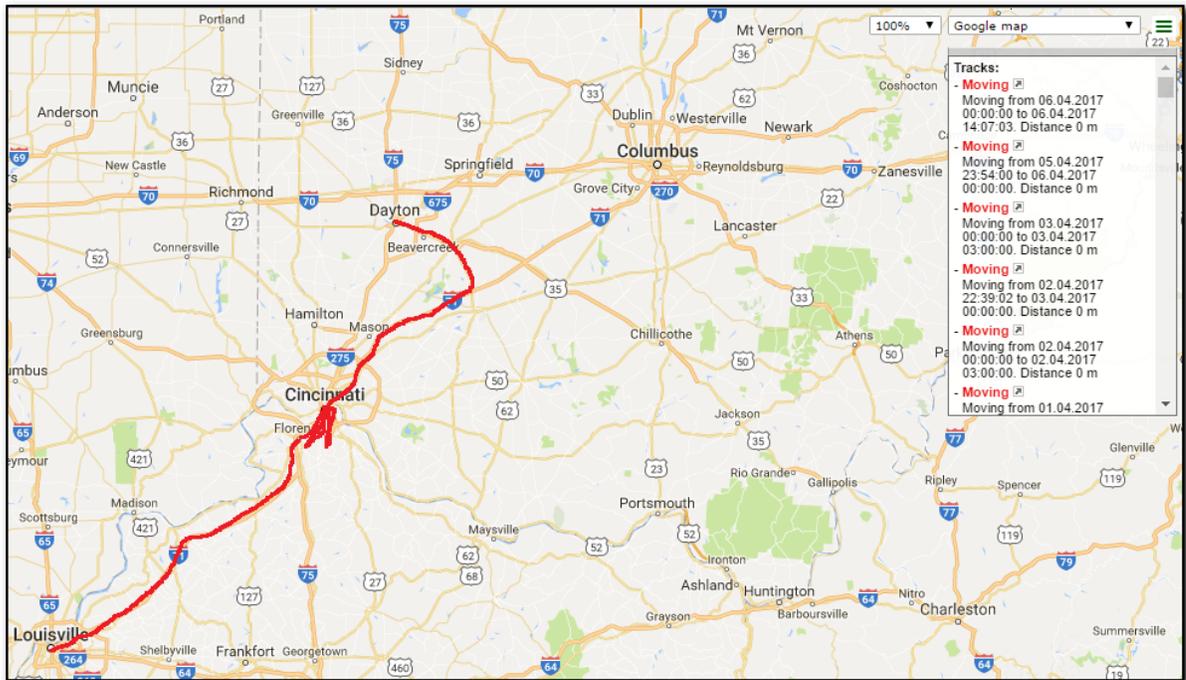
All locations are sorted by date, with the most recent one on top.

You can export Routes data to your computer by clicking the **Export** button.

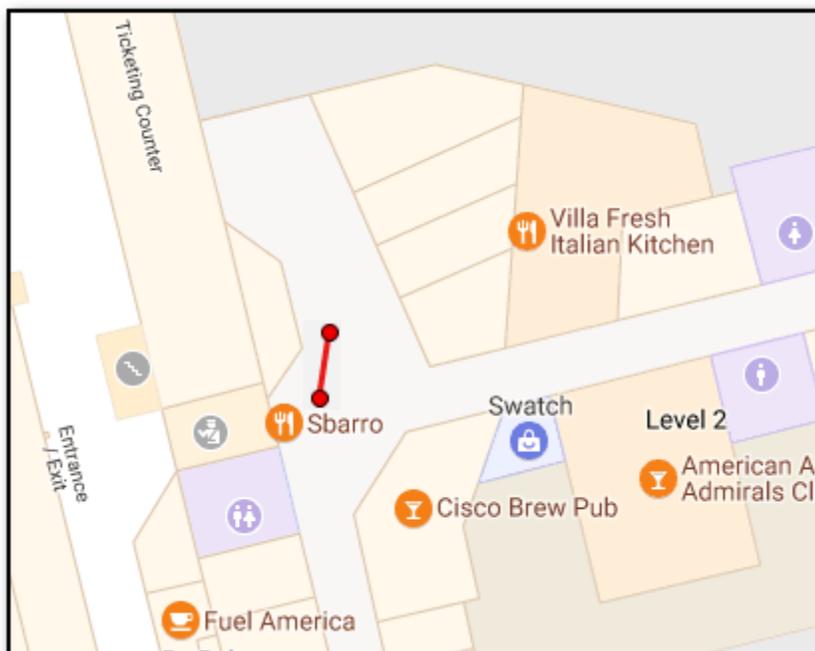


Start Date	Start Point	Finish Date	Finish Point	Show Track	Type
16.02.2017 05:39:00 (UTC +2)	<a href="#">48.4711300 35.038...</a>	16.02.2017 14:18:01 (UTC +2)	<a href="#">48.4707840 35.040...</a>		Moving
02.02.2017 00:00:00 (UTC +2)	<a href="#">48.4707840 35.040...</a>	02.02.2017 15:21:21 (UTC +2)	<a href="#">48.4707840 35.040...</a>		Moving
01.02.2017 23:50:34 (UTC +2)	<a href="#">48.4707840 35.040...</a>	02.02.2017 00:00:00 (UTC +2)	<a href="#">48.4707840 35.040...</a>		Moving
01.02.2017 00:00:00 (UTC +2)	<a href="#">48.4711300 35.038...</a>	01.02.2017 15:29:54 (UTC +2)	<a href="#">48.4707840 35.040...</a>		Moving
31.01.2017 23:38:29 (UTC +2)	<a href="#">48.4707840 35.040...</a>	01.02.2017 00:00:00 (UTC +2)	<a href="#">48.4711300 35.038...</a>		Moving
27.01.2017 00:00:00 (UTC +2)	<a href="#">48.4707840 35.040...</a>	27.01.2017 02:00:00 (UTC +2)	<a href="#">48.4707840 35.040...</a>		Walking
26.01.2017 22:25:09 (UTC +2)	<a href="#">48.4707840 35.040...</a>	27.01.2017 00:00:00 (UTC +2)	<a href="#">48.4711430 35.038...</a>		Walking
21.01.2017 01:07:21 (UTC +2)	<a href="#">48.4707840 35.040...</a>	21.01.2017 02:00:00 (UTC +2)	<a href="#">48.4707840 35.040...</a>		Driving
17.01.2017 00:00:00 (UTC +2)	<a href="#">48.4674510 35.040...</a>	17.01.2017 15:05:25 (UTC +2)	<a href="#">48.4674510 35.040...</a>		Walking
16.01.2017 19:08:22 (UTC +2)	<a href="#">48.4683050 35.040...</a>	17.01.2017 00:00:00 (UTC +2)	<a href="#">48.4683050 35.040...</a>		Moving
08.10.2016 03:14:07 (UTC +3)	<a href="#">48.4711600 35.038...</a>	08.10.2016 09:07:37 (UTC +3)	<a href="#">48.4713030 35.038...</a>		Walking

You can view the user's location history on a Google map by clicking the **Show track** button. A Google map will open in your browser, displaying the user's locations connected to each other with red lines. The most recent location is connected to the second most recent one, and so on. Hover your mouse over a point on the track to view the type of movement, distance and start/end date and time data for it.



You can also view the track for each part of the route by clicking the  icon. A Google map will open in your browser, displaying the start and end points of this part of the route. Hover your mouse over a point to view the type of movement, distance and start/end date and time data for it.



You can export information on locations to your computer by clicking the **Export** button. You can choose to export either all or all filtered locations.

## Filtering

To filter out locations, open the **Filter** pane by clicking the  icon on the right. Enable filtering by switching the **On/Off** toggle and define the filtering options:

- **Date:** Enter the desired dates into the **From** and **Until** fields.
- **Type:** Select the type of movement.

If you click **Show Track** after you filtered locations using either or both of the filters, only the filtered locations will be displayed on the Google map.

You can export the Routes data you have filtered. Click **Export** and select the **Filtered** option.

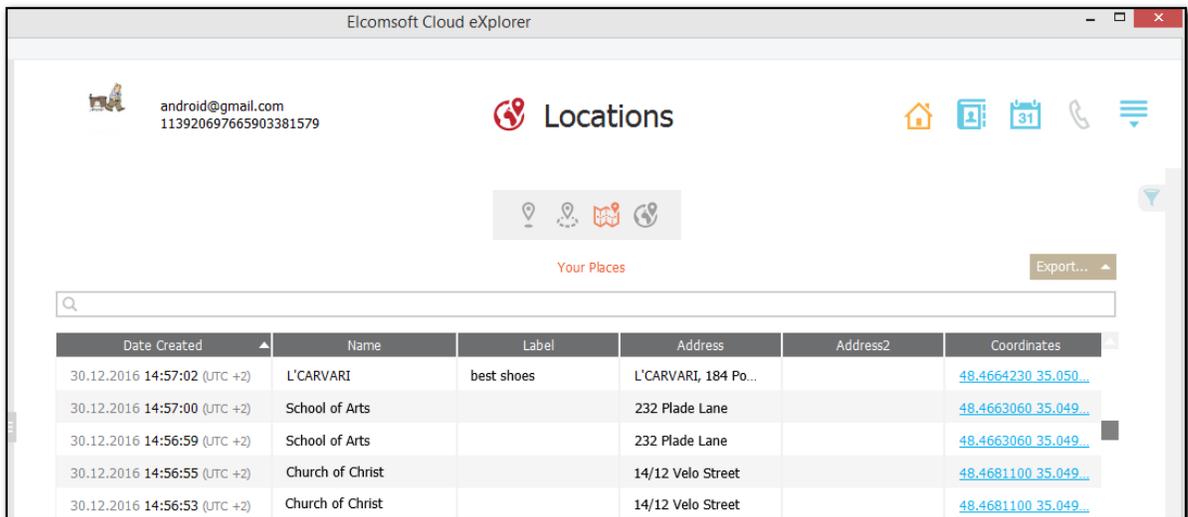
### 5.5.15.3 Your Places

In the **Your Places** section of the **Locations** plugin, you can view locations that the user attended and/or manually labeled on Google maps. You can find the following information:

- Date Created
- Name
- Label
- Address
- Address 2
- Coordinates
- Type: Location type (visited, labeled, saved, etc.)
- URL: Link to this place on the Google map
- Time Zone
- Category: Location category (e.g., bank, gym, etc.)
- Date Started
- Date Ended
- Event Name

All locations are sorted by date, with the most recent one on top.

You can export Your Places data to your computer by clicking the **Export** button.



The screenshot shows the 'Locations' plugin interface in Elcomsoft Cloud eXplorer. The user is logged in as 'android@gmail.com' with ID '113920697665903381579'. The 'Your Places' section is active, displaying a table of location data. The table has columns for Date Created, Name, Label, Address, Address2, and Coordinates. The data is sorted by date, with the most recent entries at the top.

Date Created	Name	Label	Address	Address2	Coordinates
30.12.2016 14:57:02 (UTC +2)	L'CARVARI	best shoes	L'CARVARI, 184 Po...		<a href="#">48.4664230 35.050...</a>
30.12.2016 14:57:00 (UTC +2)	School of Arts		232 Plade Lane		<a href="#">48.4663060 35.049...</a>
30.12.2016 14:56:59 (UTC +2)	School of Arts		232 Plade Lane		<a href="#">48.4663060 35.049...</a>
30.12.2016 14:56:55 (UTC +2)	Church of Christ		14/12 Velo Street		<a href="#">48.4681100 35.049...</a>
30.12.2016 14:56:53 (UTC +2)	Church of Christ		14/12 Velo Street		<a href="#">48.4681100 35.049...</a>

## Searching and Filtering

To perform searches in **Your Places**, fill the search field and press **Enter**. The search results will be highlighted in yellow.

To filter out locations, open the **Filter** pane by clicking the  icon on the right. Enable filtering by switching the **On/Off** toggle and define the filtering options:

- **Date**: Enter the desired dates into the **From** and **Until** fields.
- **Type**: Select the location type.
- **Category**: Select the location category.

You can export the Your Places data you have filtered. Click **Export** and select the **Filtered** option.

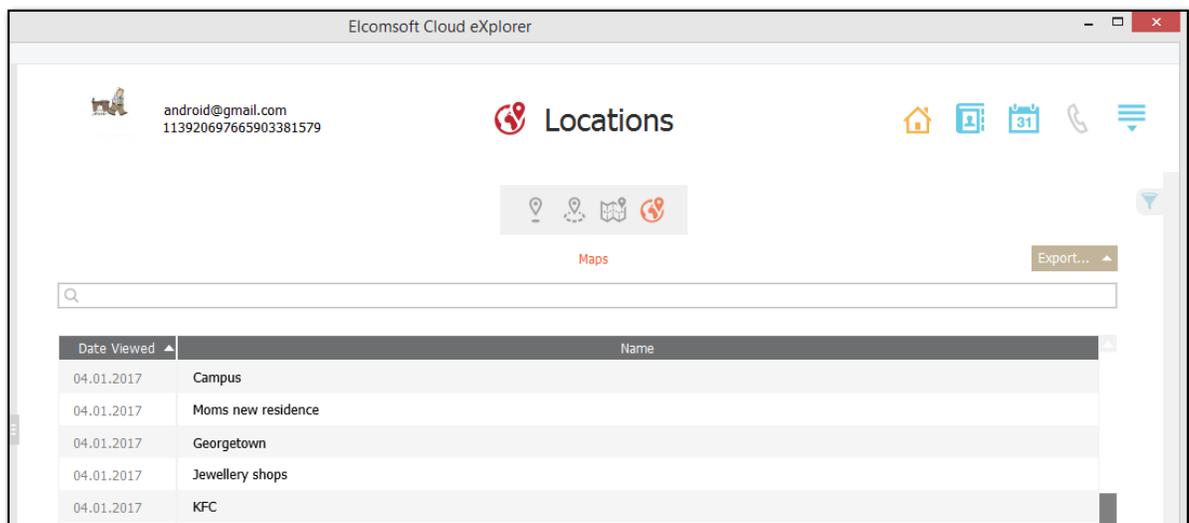
### 5.5.15.4 Maps

In the **Maps** section of the **Locations** plugin, you can view the user's saved Google maps. You can find the following information on each map:

- Date Viewed
- Name

All maps are sorted by date, with the most recent one on top.

You can export Maps data to your computer by clicking the **Export** button.



## Searching and Filtering

To perform searches in **Maps**, fill the search field and press **Enter**. The search results will be highlighted in yellow.

To filter out maps, open the **Filter** pane by clicking the  icon on the right. Enable filtering by switching the **On/Off** toggle and define the filtering options:

- **Date:** Enter the desired dates into the **From** and **Until** fields.

You can export the Maps data you have filtered. Click **Export** and select the **Filtered** option.

## 5.5.16 Dashboard

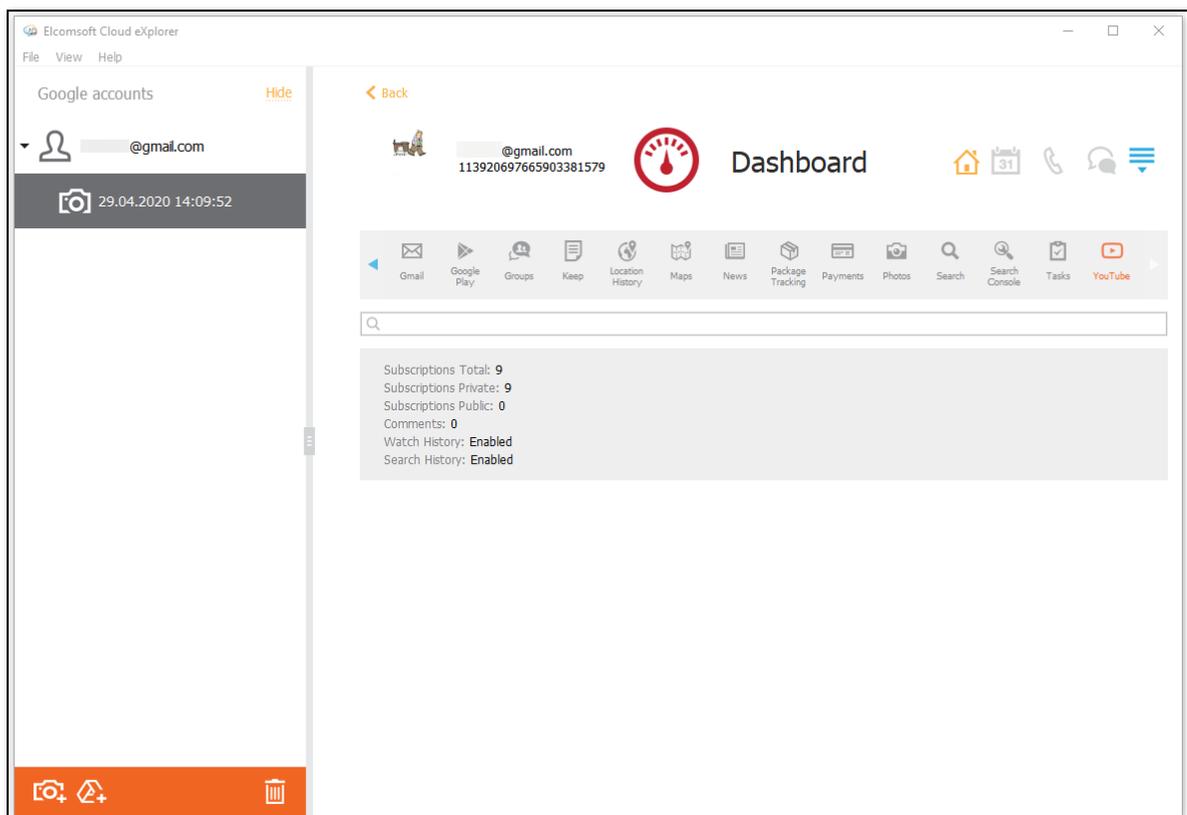
Enter topic text here.

### 5.5.16.1 YouTube

In the **YouTube** section of the **Dashboard** plugin, you can view the information on the user's activity on YouTube, such as:

- **Subscriptions Total:** number of subscriptions
- **Subscriptions Private:** number of subscriptions
- **Subscriptions Public:** number of subscriptions
- **Comments:** number of comments
- **Watch History:** Enabled/Disabled
- **Search History:** Enabled/Disabled

To perform searches in the **YouTube** section, fill the search field and press **Enter**. The search results will be highlighted in yellow.

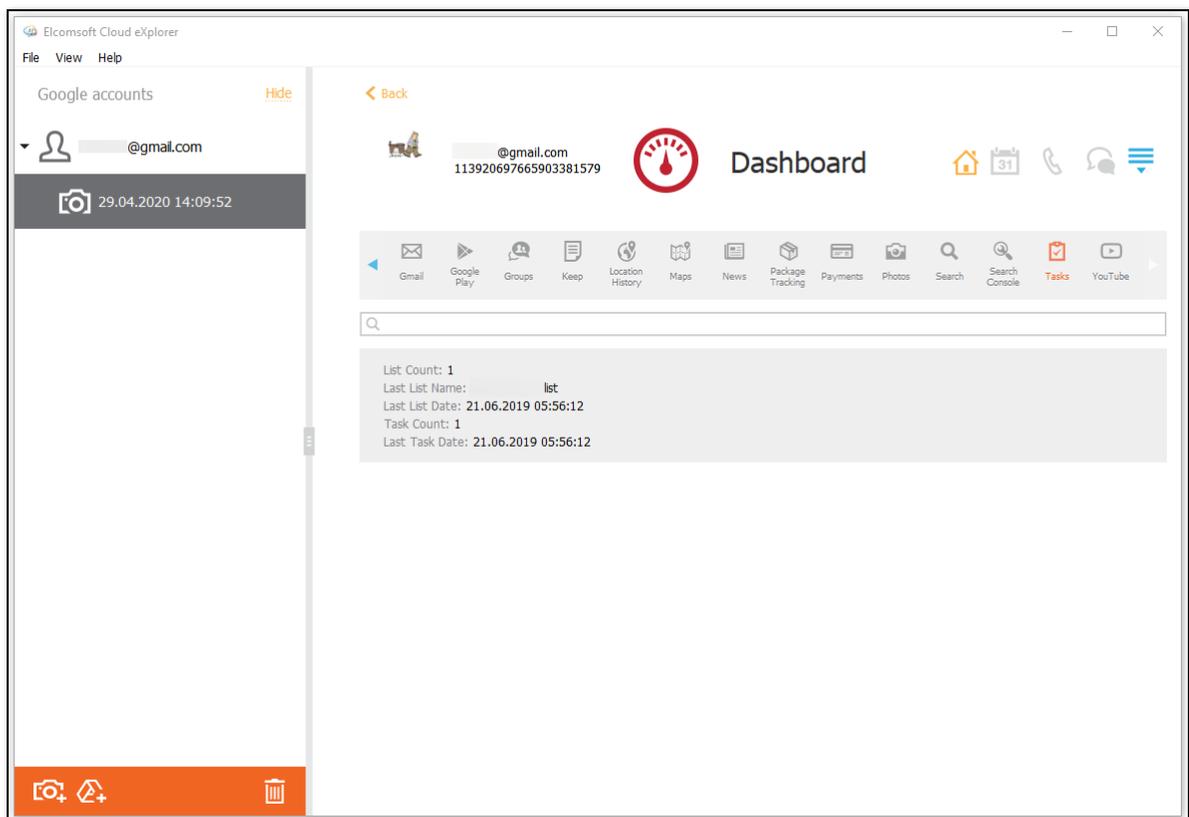


### 5.5.16.2 Tasks

In the **Tasks** section of the **Dashboard** plugin, you can view information from the Google Tasks, such as:

- **List Count:** number of lists
- **Last List Name**
- **Last List Date:** date, time, and timezone
- **Task Count:** number of tasks
- **Last Task Date:** date, time, and timezone

To perform searches in the **Tasks** section, fill the search field and press **Enter**. The search results will be highlighted in yellow.

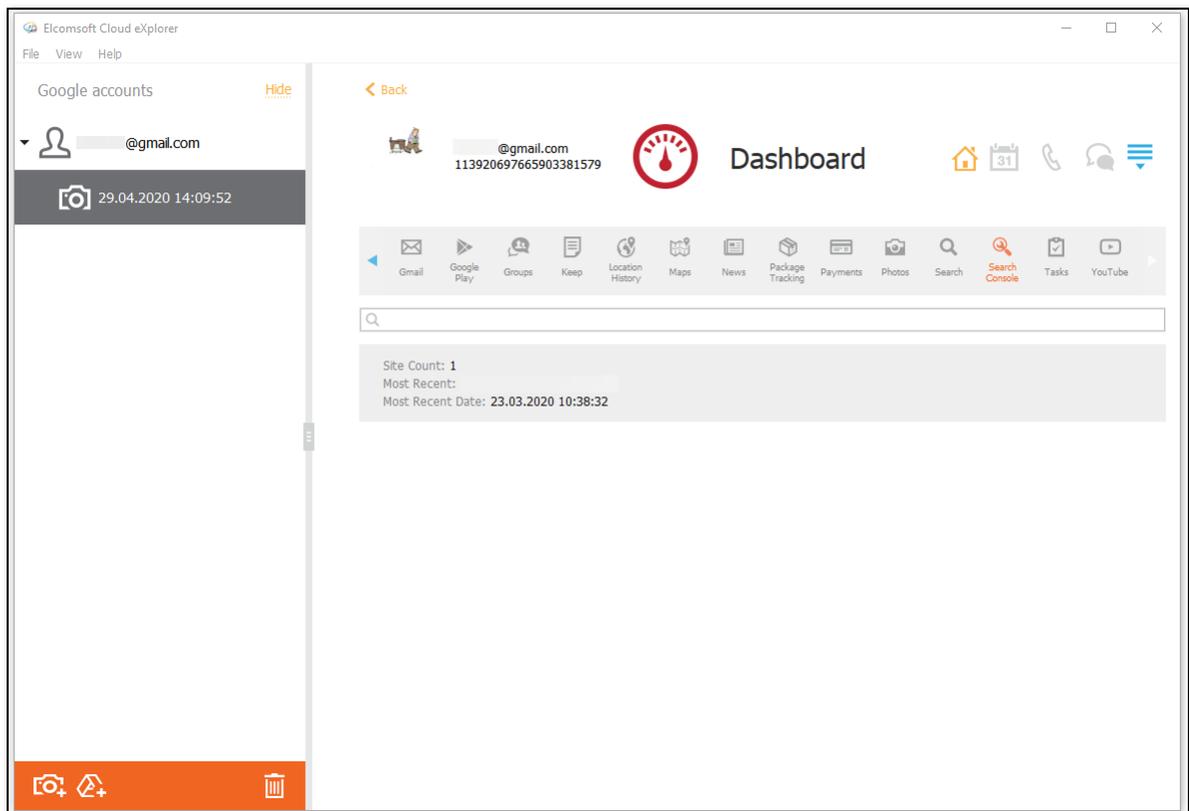


### 5.5.16.3 Search Console

In the **Search Console** section of the **Dashboard** plugin, you can view the information from the Google Search Console service, such as:

- **Site Count:** number of sites
- **Most Recent:** the most recent site
- **Most Recent Date:** date, time, and timezone

To perform searches in the **Search Console** section, fill the search field and press **Enter**. The search results will be highlighted in yellow.

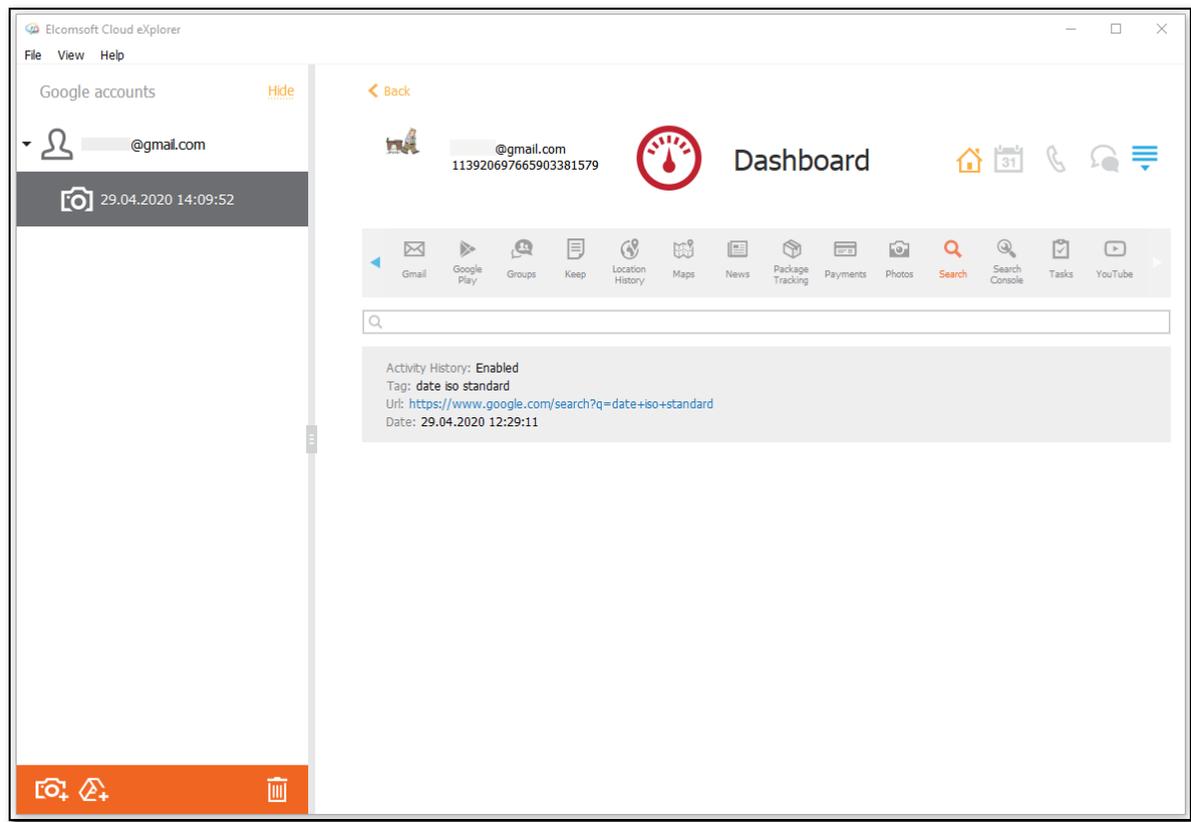


#### 5.5.16.4 Search

In the **Search** section of the **Dashboard** plugin, you can view the information on the user's Google search history, such as:

- **Activity History:** Enabled/Disabled
- **Tag:** search request
- **Url:** the link to the search request results on Google
- **Date:** date, time, and timezone of the search request

To perform searches in the **Search** section, fill the search field and press **Enter**. The search results will be highlighted in yellow.

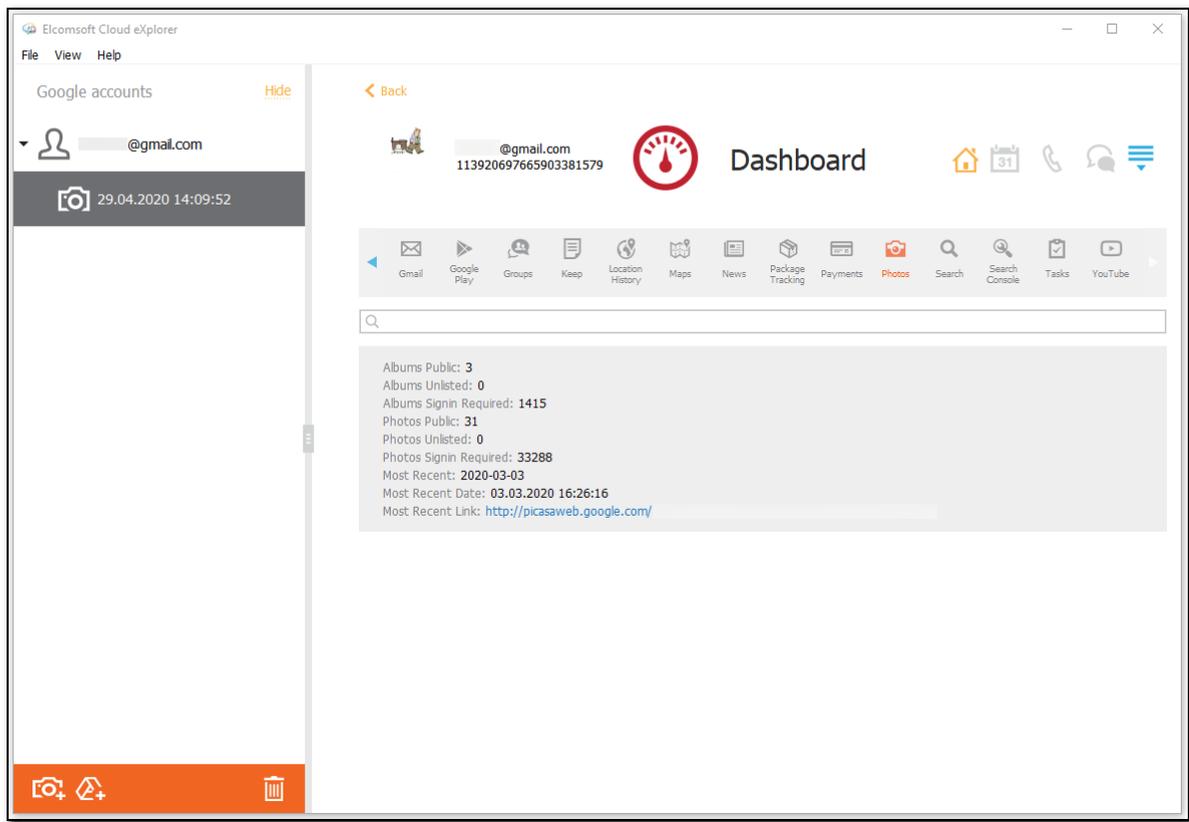


### 5.5.16.5 Photos)

In the **Photos** section of the **Dashboard** plugin, you can view the information from the Google Photos service, such as:

- **Albums Public:** number of the albums
- **Albums Unlisted:** number of the albums
- **Albums Signin Required:** number of the albums
- **Photos Public:** number of the photos
- **Photos Unlisted:** number of the photos
- **Photos Signin Required:** number of the photos
- **Most Recent:** date of the most recent photo
- **Most Recent Date:** date, time, and timezone of the most recent photo
- **Most Recent Link:** the link to the most recent photo

To perform searches in the **Photos** section, fill the search field and press **Enter**. The search results will be highlighted in yellow.

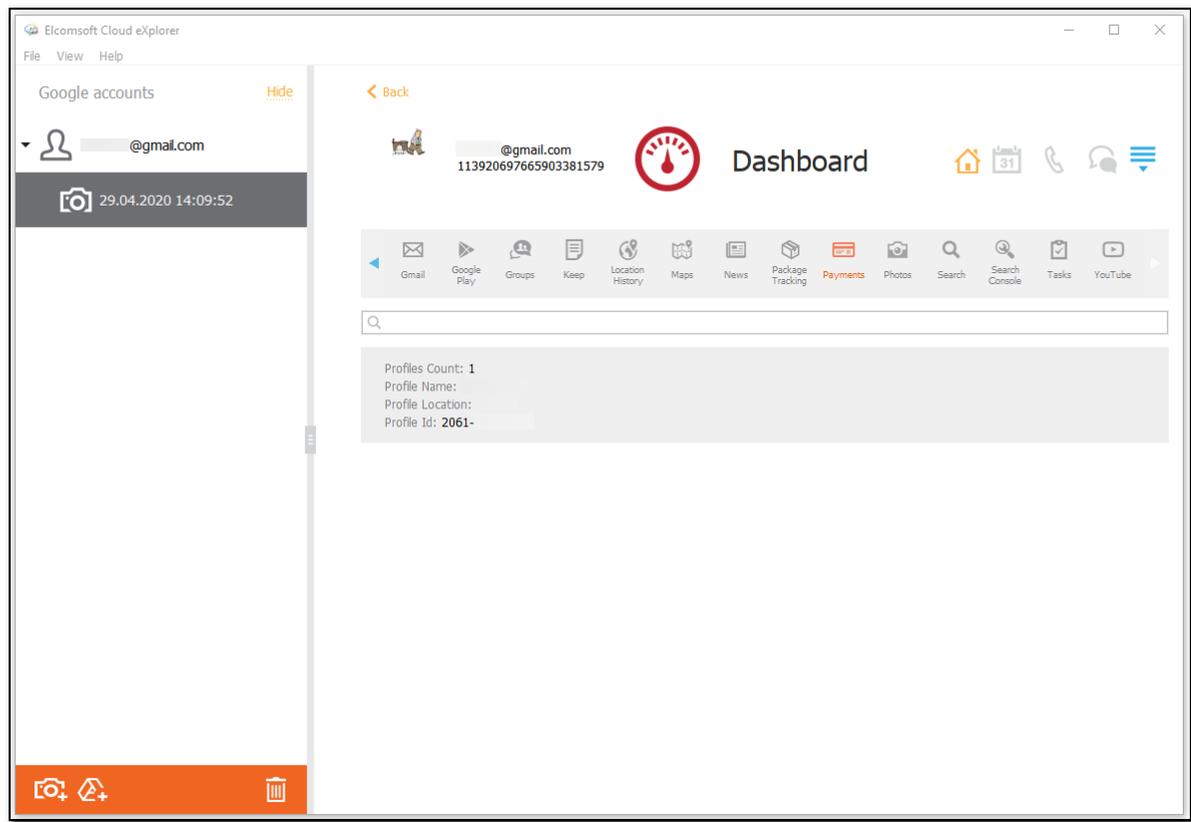


### 5.5.16.6 Payments

In the **Payments** section of the **Dashboard** plugin, you can view the information on the Google payments, such as:

- **Profiles Count:** number of profiles
- **Profile Name**
- **Profile Location**
- **Profile Id**

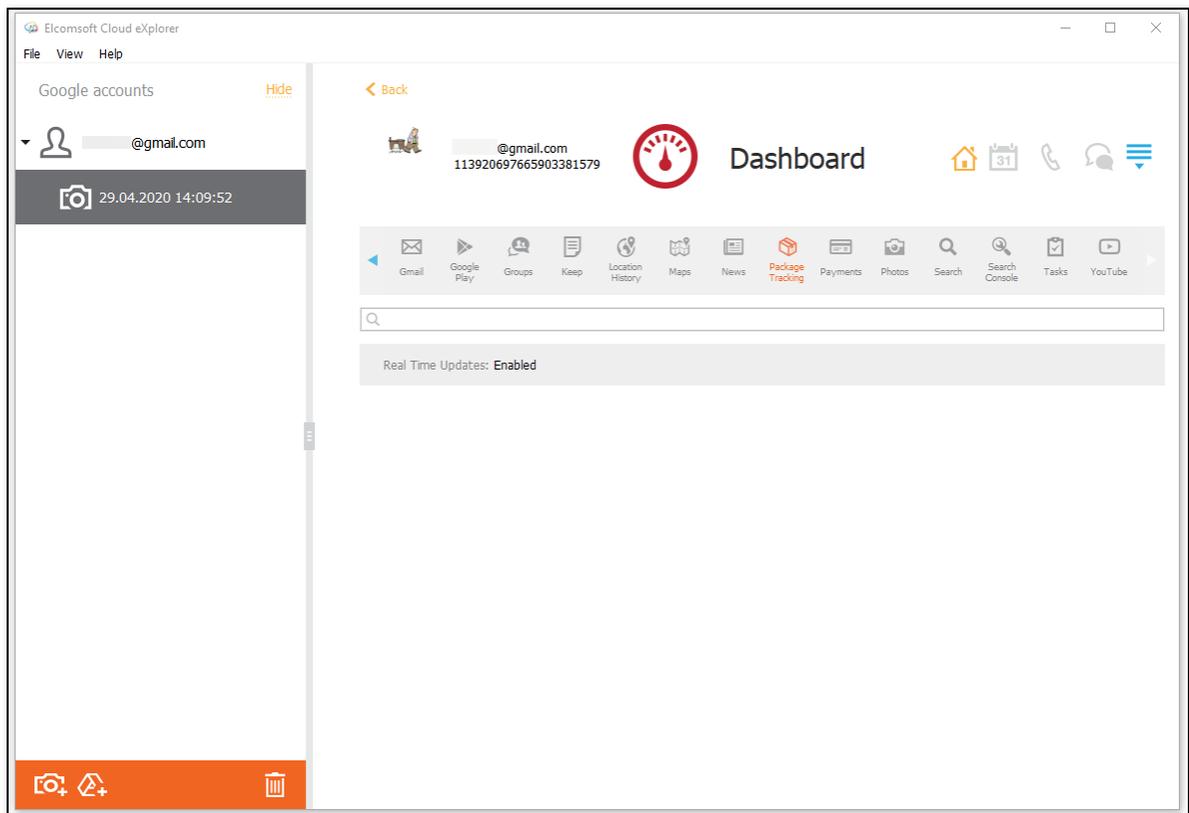
To perform searches in the **Payments** section, fill the search field and press **Enter**. The search results will be highlighted in yellow.



### 5.5.16.7 Package Tracking

In the **Package Tracking** section of the **Dashboard** plugin, you can view whether the updates on the package tracking are enabled or disabled.

To perform searches in the **Package Tracking** section, fill the search field and press **Enter**. The search results will be highlighted in yellow.

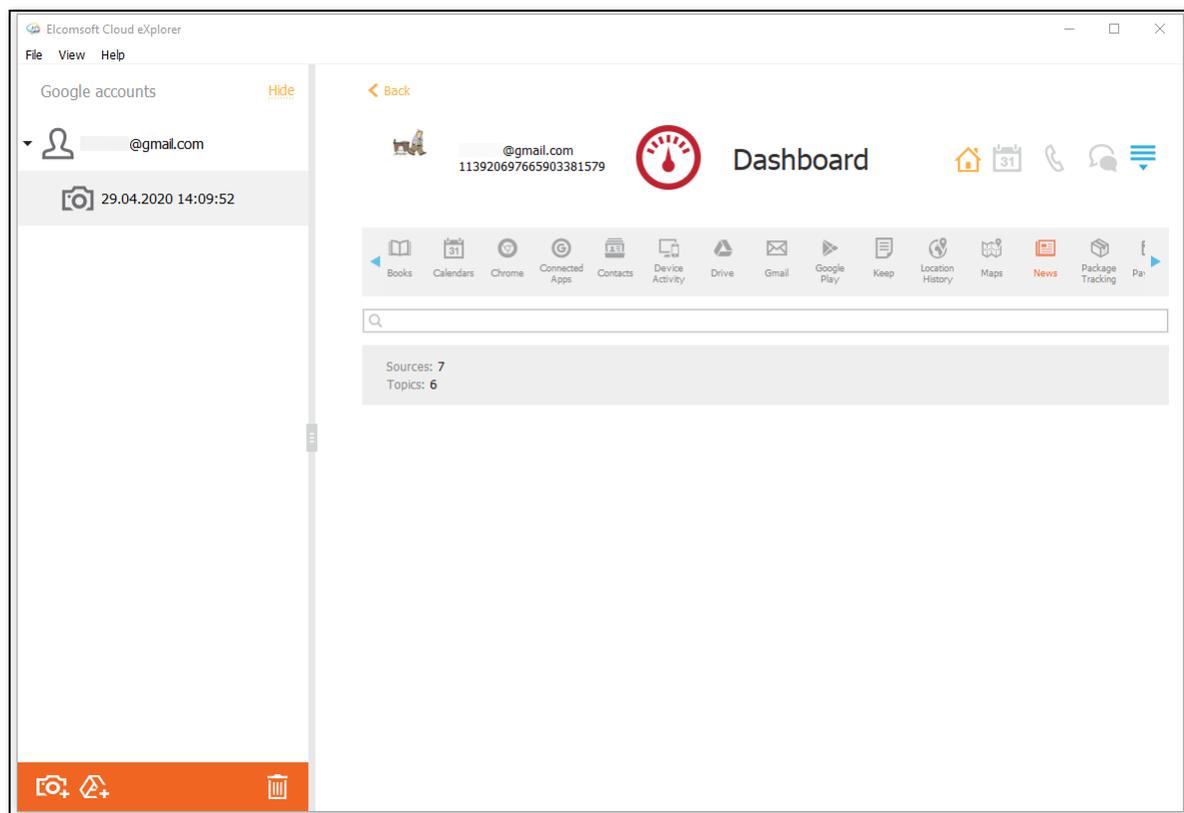


### 5.5.16.8 News

In the **News** section of the **Dashboard** plugin, you can view the information from the Google News aggregator, such as:

- **Sources:** number of sources
- **Topics:** number of topics

To perform searches in the **News** section, fill the search field and press **Enter**. The search results will be highlighted in yellow.

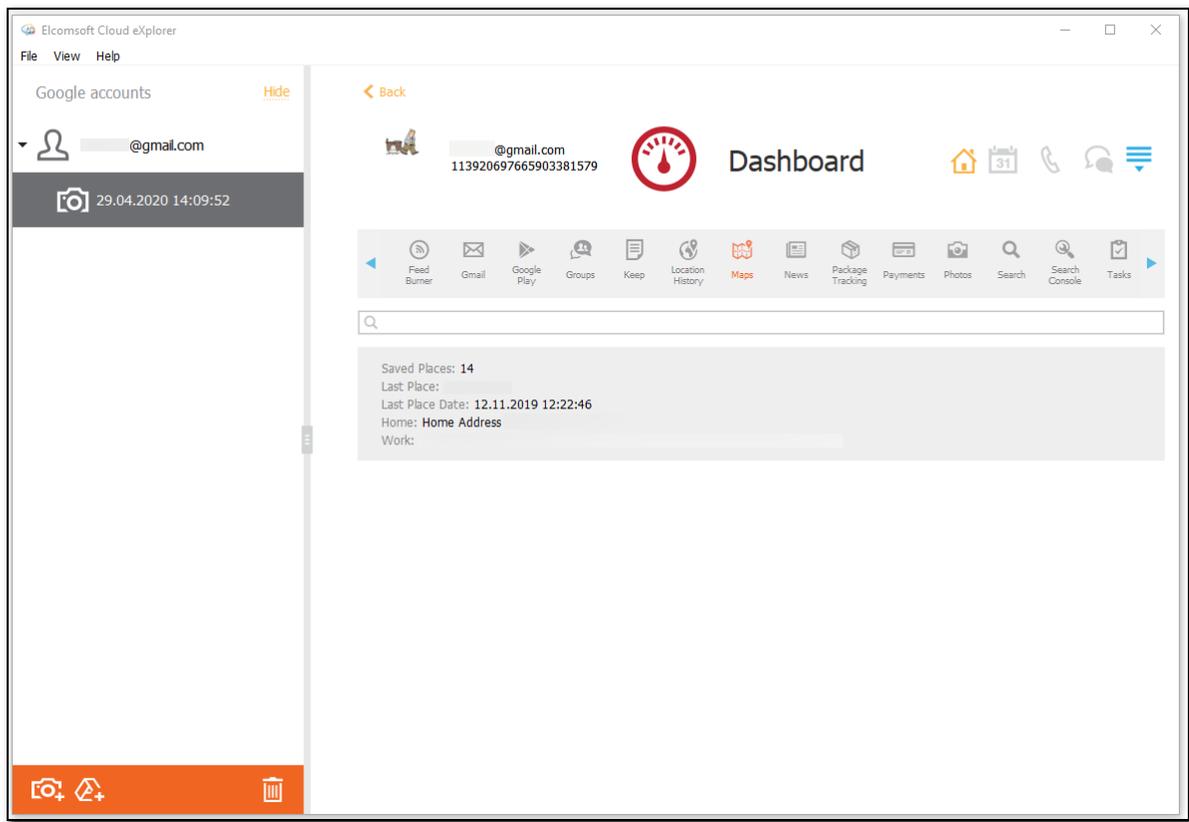


### 5.5.16.9 Maps

In the **Maps** section of the **Dashboard** plugin, you can view the information from the Google Maps, such as:

- **Saved Places:** number of the saved places
- **Last Place:** the link to the last place (to view the place on the Google Maps, click the link)
- **Last Place Date:** date, time, and timezone
- **Home:** home address
- **Work:** work address

To perform searches in the **Maps** section, fill the search field and press **Enter**. The search results will be highlighted in yellow.

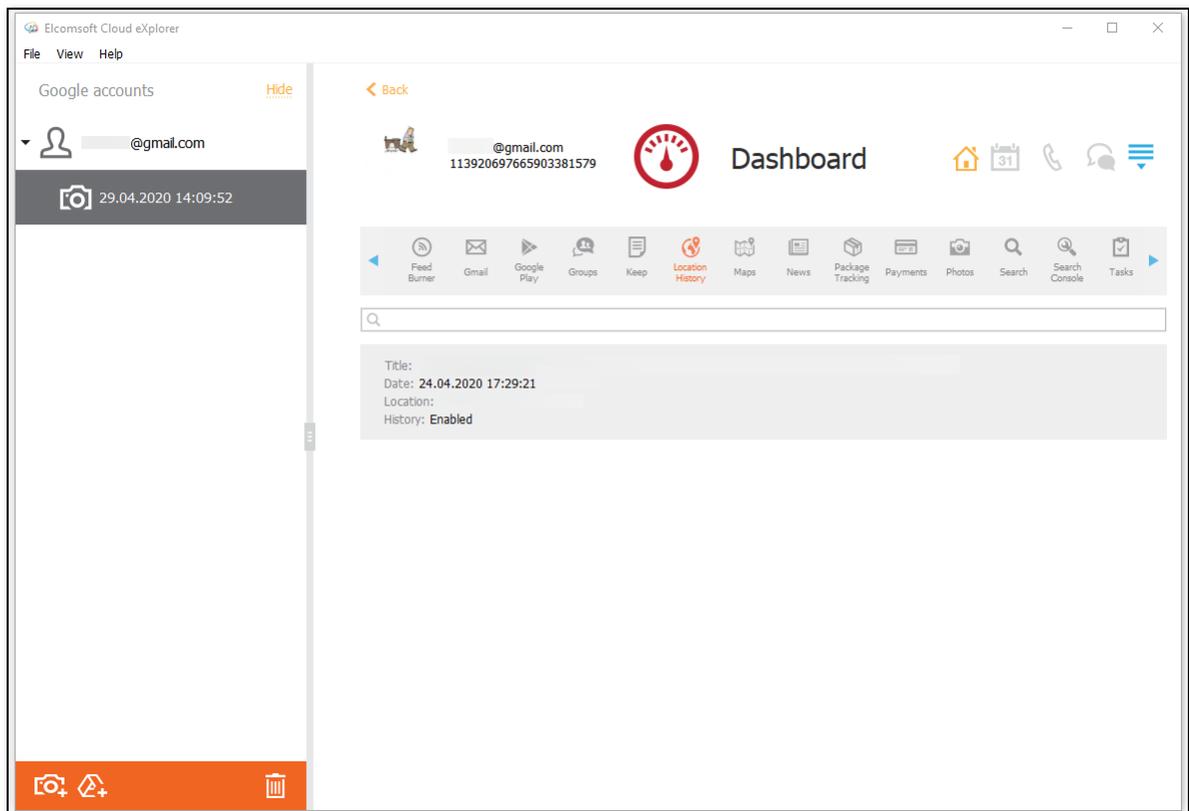


#### 5.5.16.10 Location History

In the **Location History** section of the **Dashboard** plugin, you can view the user's location history, such as:

- **Title:** the location address
- **Date:** date, time, and timezone
- **Location:** latitude and longitude link (to view the location on the Google Maps, click the link)
- **History:** Enabled/Disabled

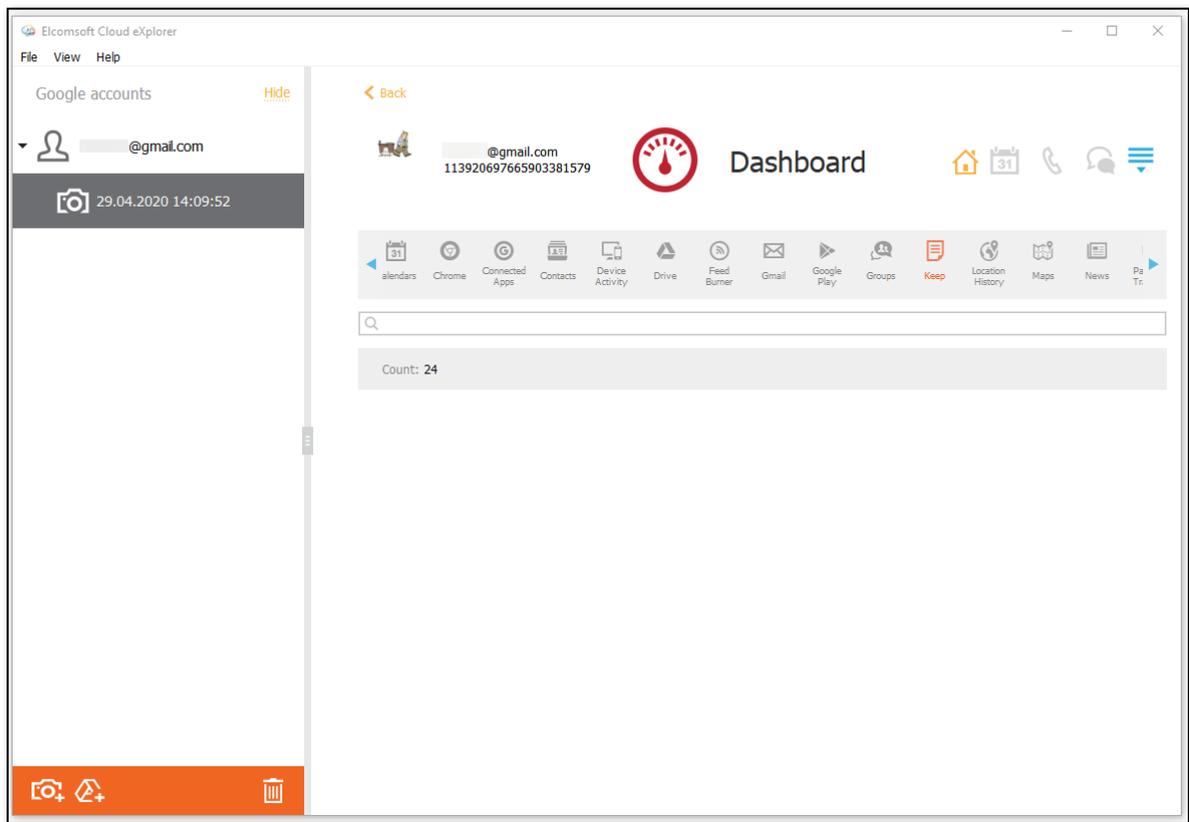
To perform searches in the **Location History** section, fill the search field and press **Enter**. The search results will be highlighted in yellow.



### 5.5.16.11 Keep

In the **Keep** section of the **Dashboard** plugin, you can view the number of the notes made via Google Keep service.

To perform searches in the **Keep** section, fill the search field and press **Enter**. The search results will be highlighted in yellow.

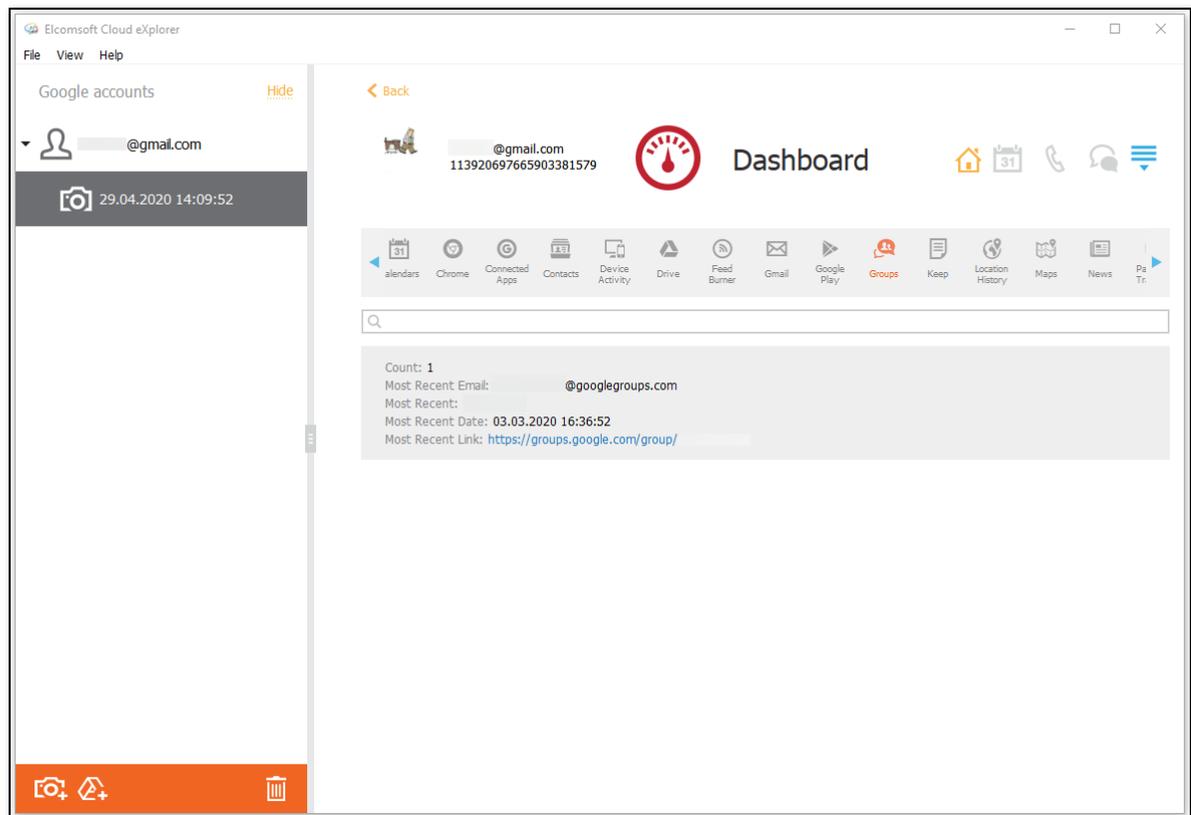


### 5.5.16.12 Groups

In the **Groups** section of the **Dashboard** plugin, you can view the information from the Google Groups service, such as:

- **Count:** number of groups
- **Most Recent Email**
- **Most Recent:** name of the most recent group
- **Most Recent Date:** date, time, and timezone
- **Most Recent Link:** the link to the most recent group

To perform searches in the **Groups** section, fill the search field and press **Enter**. The search results will be highlighted in yellow.

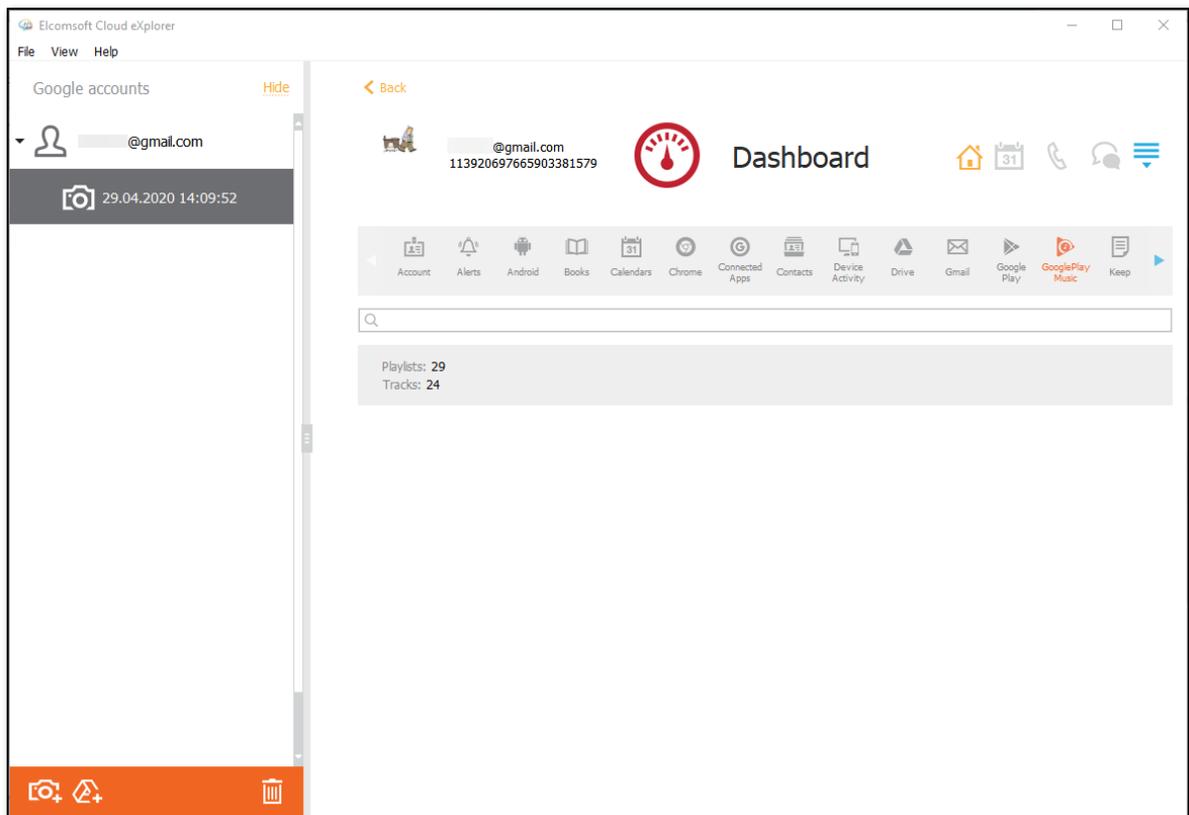


### 5.5.16.13 Google Play Music

In the **Google Play Music** section of the **Dashboard** plugin, you can view the information from the Google Play Music service, such as:

- **Playlists:** number of playlists
- **Tracks:** number of tracks

To perform searches in the **Google Play Music** section, fill the search field and press **Enter**. The search results will be highlighted in yellow.

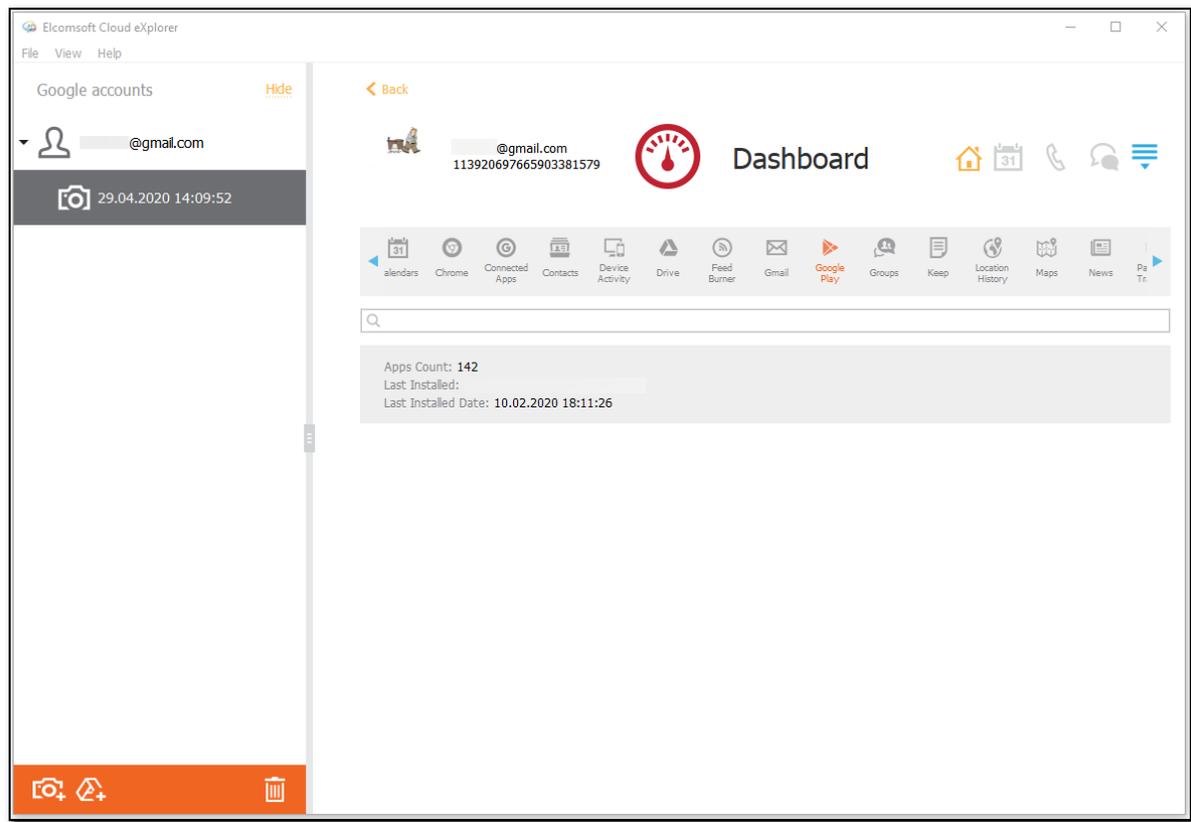


#### 5.5.16.14 Google Play

In the **Google Play** section of the **Dashboard** plugin, you can view the information on the applications installed from the Google Play, such as:

- **Apps Count:** number of the installed applications
- **Last Installed:** name of the application
- **Last Installed Date:** date, time, and timezone

To perform searches in the **Google Play** section, fill the search field and press **Enter**. The search results will be highlighted in yellow.

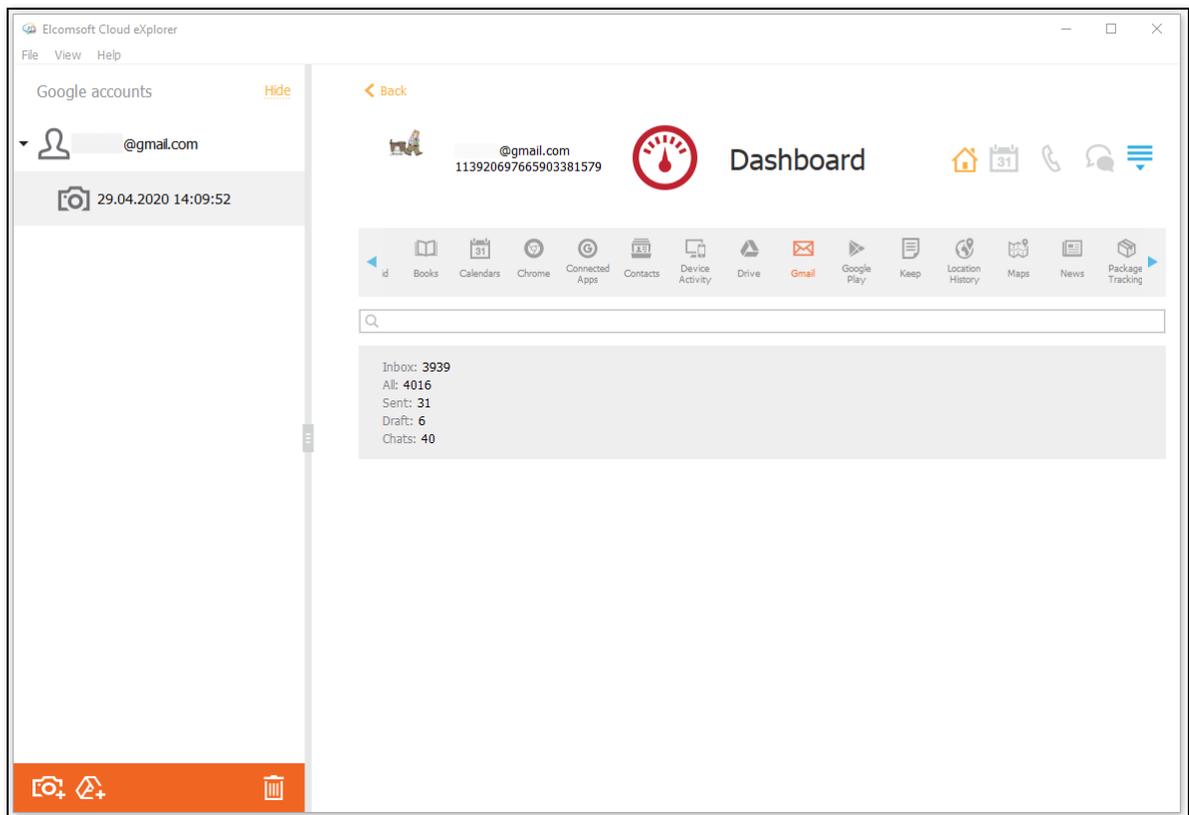


### 5.5.16.15 Gmail

In the **Gmail** section of the **Dashboard** plugin, you can view the information from the Google Mail, such as:

- **Inbox:** number of Inbox mails
- **All:** total number of mails
- **Sent:** number of sent mails
- **Draft:** number of drafts
- **Chats:** number of chats

To perform searches in the **Gmail** section, fill the search field and press **Enter**. The search results will be highlighted in yellow.

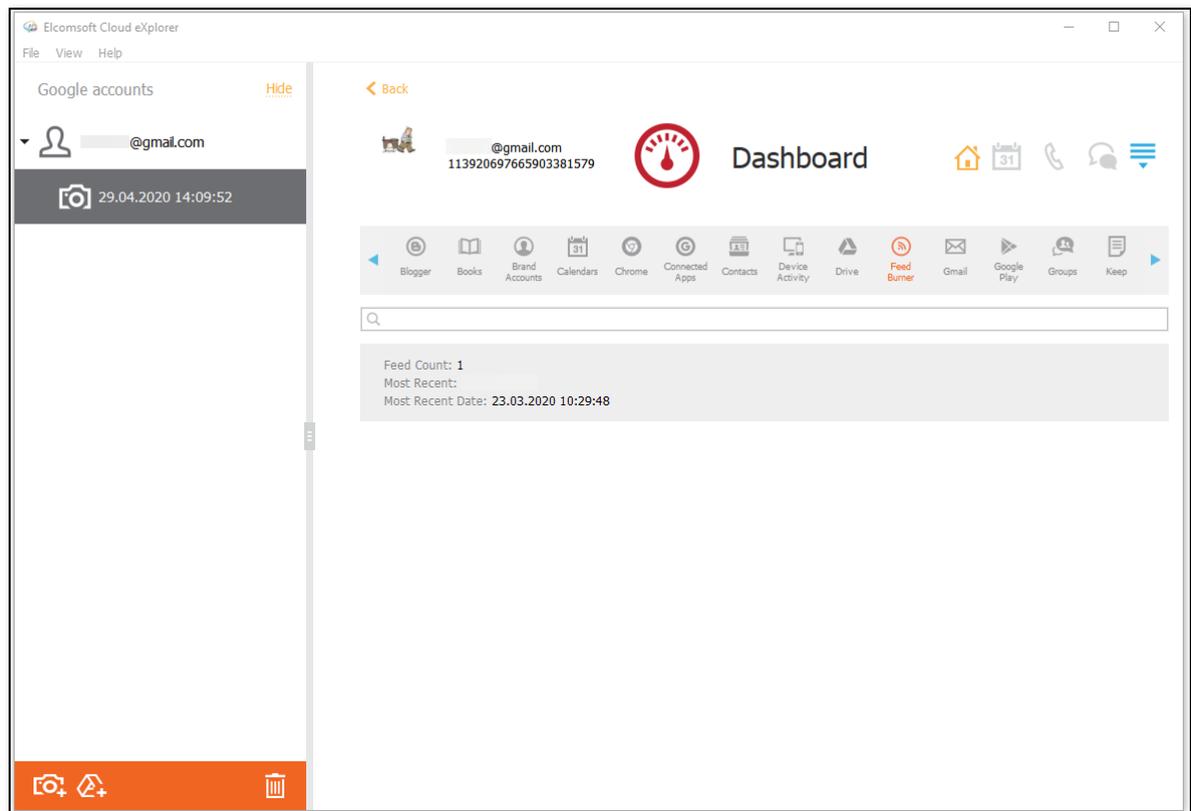


#### 5.5.16.16 FeedBurner

In the **FeedBurner** section of the **Dashboard** plugin, you can view the information from the Google FeedBurner service, such as:

- **Feed Count:** number of feeds
- **Most Recent:** name of the most recent feed
- **Most Recent Date:** date, time, and timezone

To perform searches in the **FeedBurner** section, fill the search field and press **Enter**. The search results will be highlighted in yellow.

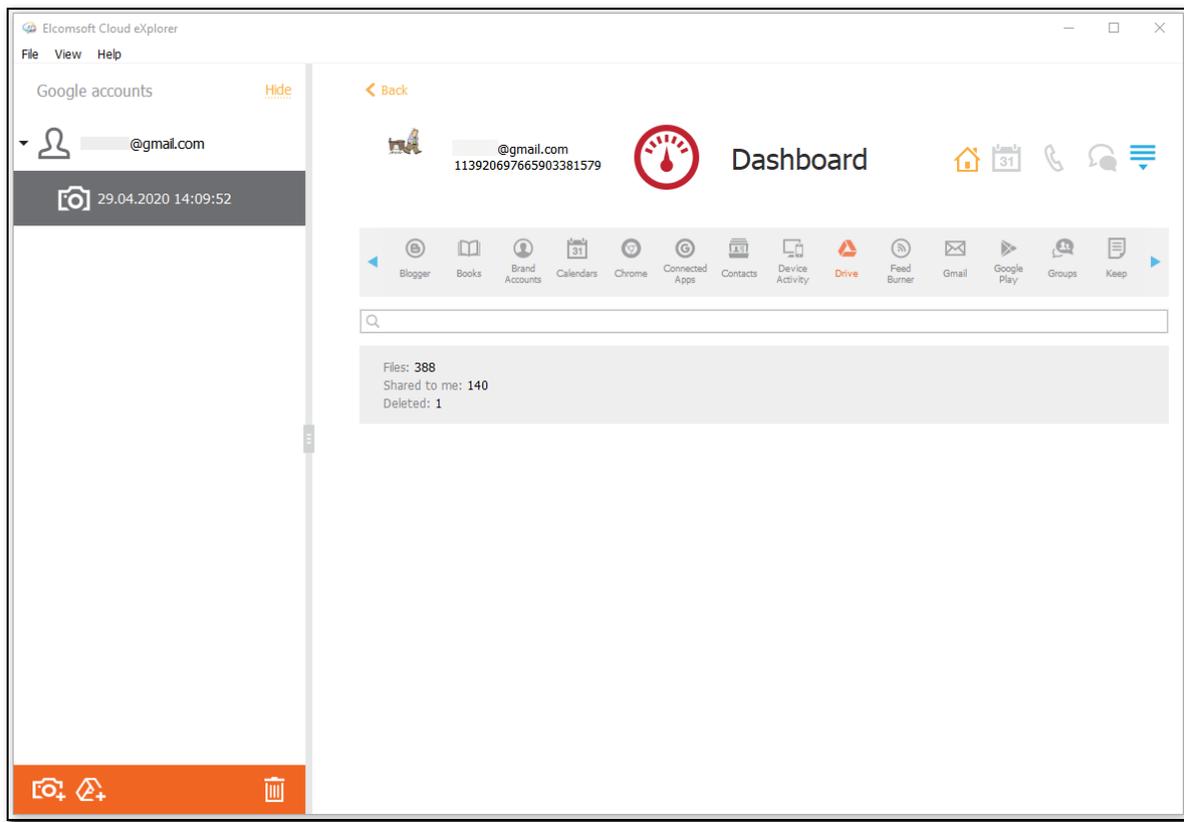


### 5.5.16.17 Drive

In the **Drive** section of the **Dashboard** plugin, you can view the information from the Google Drive, such as:

- **Files:** number of files
- **Shared to me:** number of shared files
- **Deleted:** number of files

To perform searches in the **Drive** section, fill the search field and press **Enter**. The search results will be highlighted in yellow.

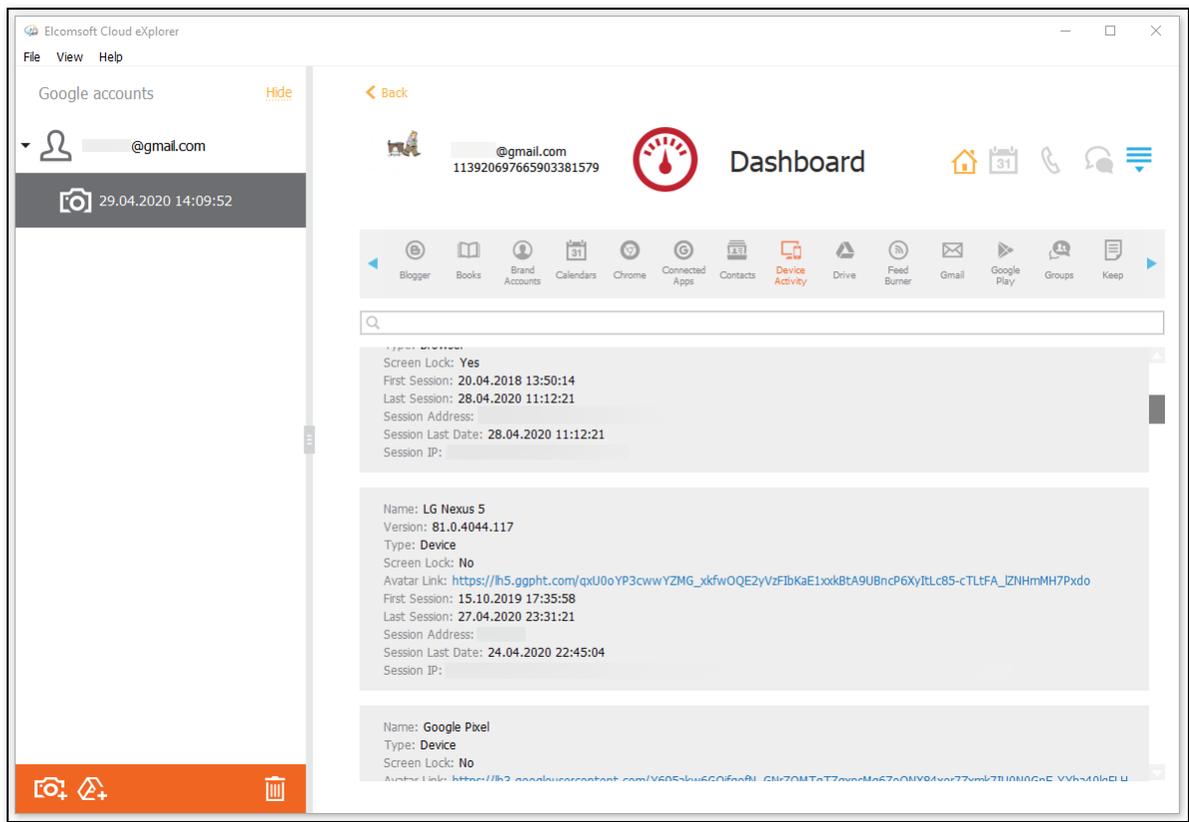


### 5.5.16.18 Device Activity

In the **Device Activity** section of the **Dashboard** plugin, you can view the information on activity of the devices associated with the Google account, such as:

- **Name:** the device name
- **Version:** the device version
- **Is Current Device:** Yes/No
- **Type**
- **Screen Lock:** Yes/No
- **Avatar Link:** the link to the device avatar
- **First Session:** date, time, and timezone
- **Last Session:** date, time, and timezone
- **Session Address**
- **Session Last Date:** date, time, and timezone
- **Session IP**

To perform searches in the **Device Activity** section, fill the search field and press **Enter**. The search results will be highlighted in yellow.

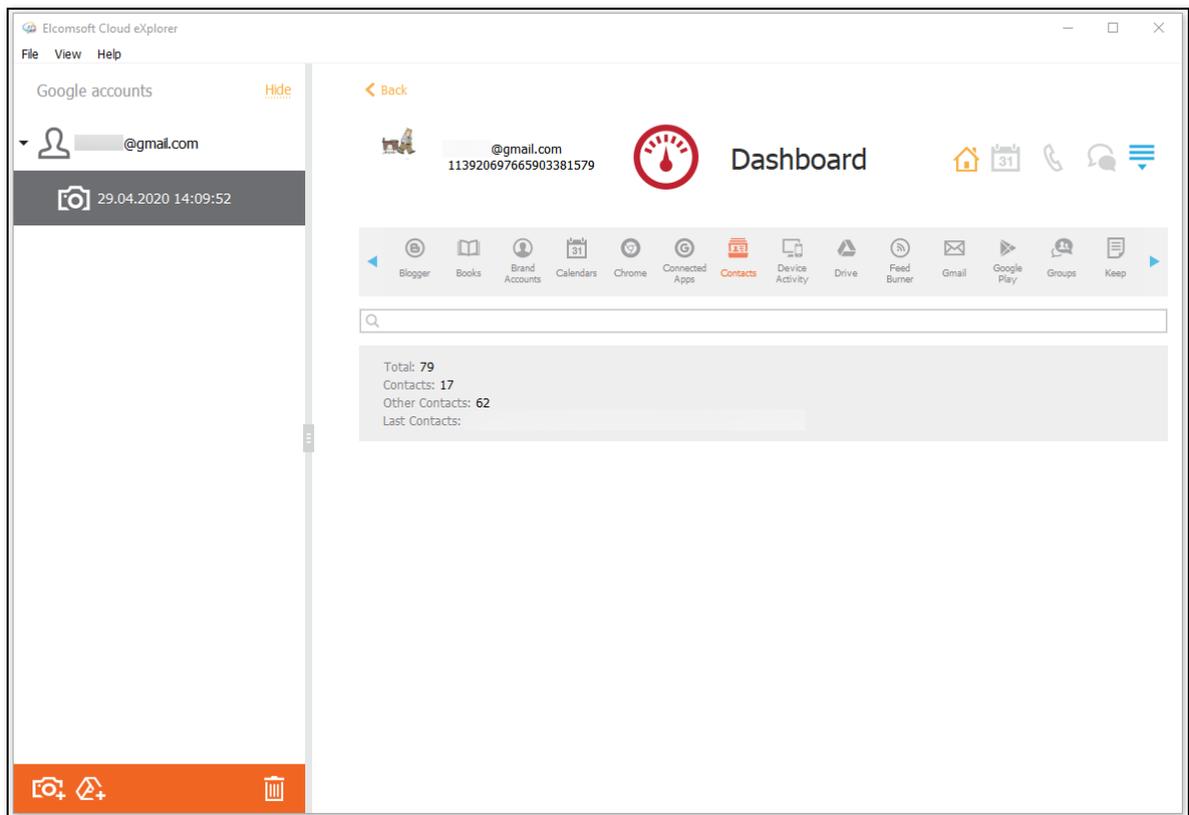


### 5.5.16.19 Contacts

In the **Contacts** section of the **Dashboard** plugin, you can view the information on the user's contacts, such as:

- **Total:** number of contacts
- **Contacts:** number of contacts
- **Other Contacts:** number of contacts
- **Last Contacts:** a list of contacts

To perform searches in the **Contacts** section, fill the search field and press **Enter**. The search results will be highlighted in yellow.

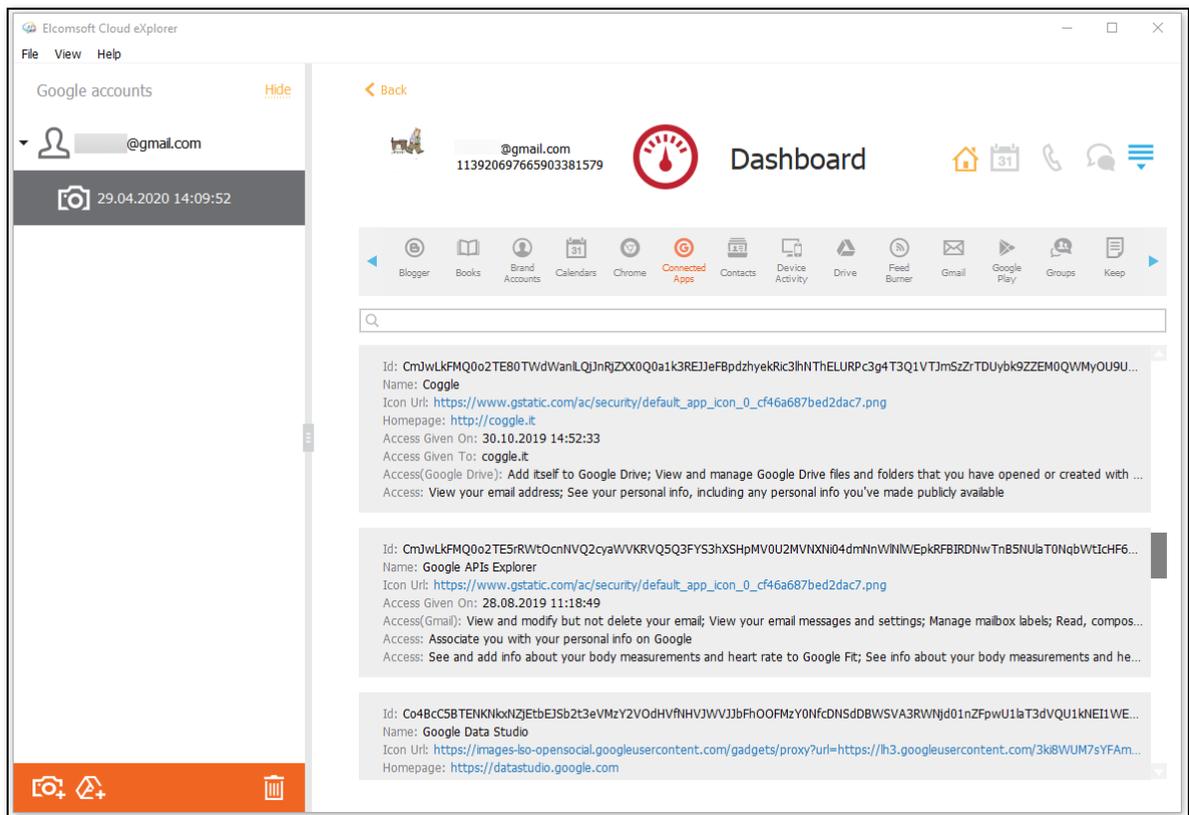


### 5.5.16.20 Connected Apps

In the **Connected Apps** section of the **Dashboard** plugin, you can view the information on the applications connected to the account, such as:

- **Id**
- **Name**
- **Icon Url**: the link to the application icon
- **Homepage**: the link to the application homepage
- **Access Given On**: date, time, and timezone
- **Access Given To**
- **Access**: the access type

To perform searches in the **Connected Apps** section, fill the search field and press **Enter**. The search results will be highlighted in yellow.

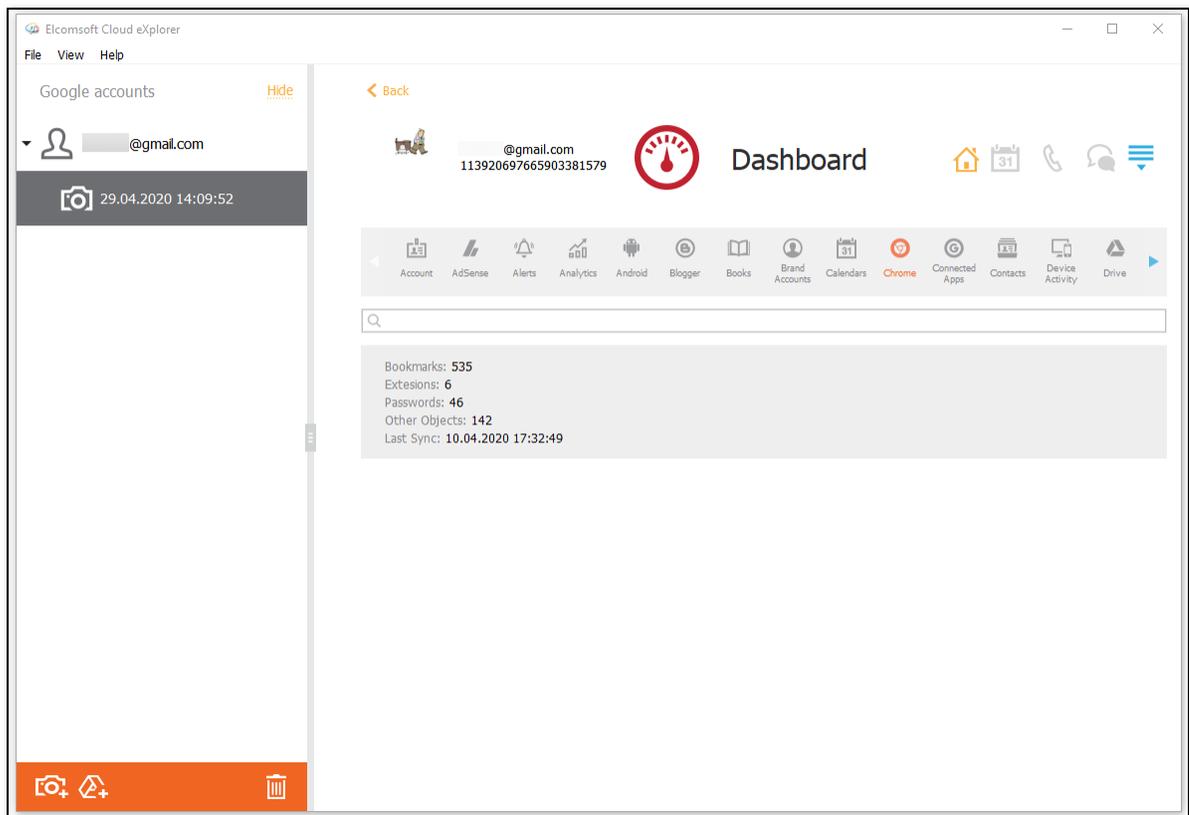


### 5.5.16.21 Chrome

In the **Chrome** section of the **Dashboard** plugin, you can view the information from the Google Chrome, such as:

- **Bookmarks:** number of bookmarks
- **Extensions:** number of extensions
- **Passwords:** number of passwords
- **Other Objects:** number of other objects
- **Last Sync:** date, time, and timezone of the last synchronization

To perform searches in the **Chrome** section, fill the search field and press **Enter**. The search results will be highlighted in yellow.

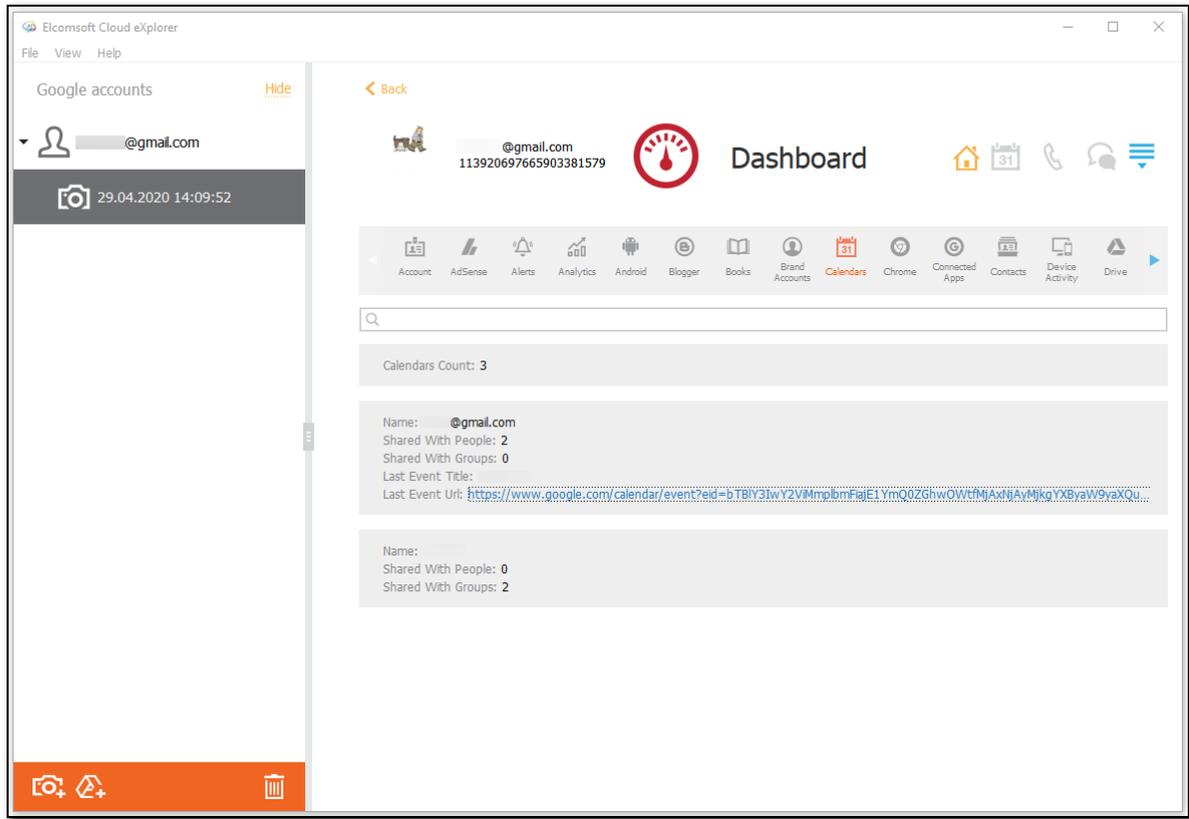


### 5.5.16.22 Calendars

In the **Calendars** section of the **Dashboard** plugin, you can view the information on the Google Calendars, such as:

- **Calendars Count**
- **Name**
- **Shared with People:** number of persons
- **Shared with Groups:** number of groups
- **Last Event Title**
- **Last Event Url:** the link to the event in the calendar

To perform searches in the **Calendars** section, fill the search field and press **Enter**. The search results will be highlighted in yellow.

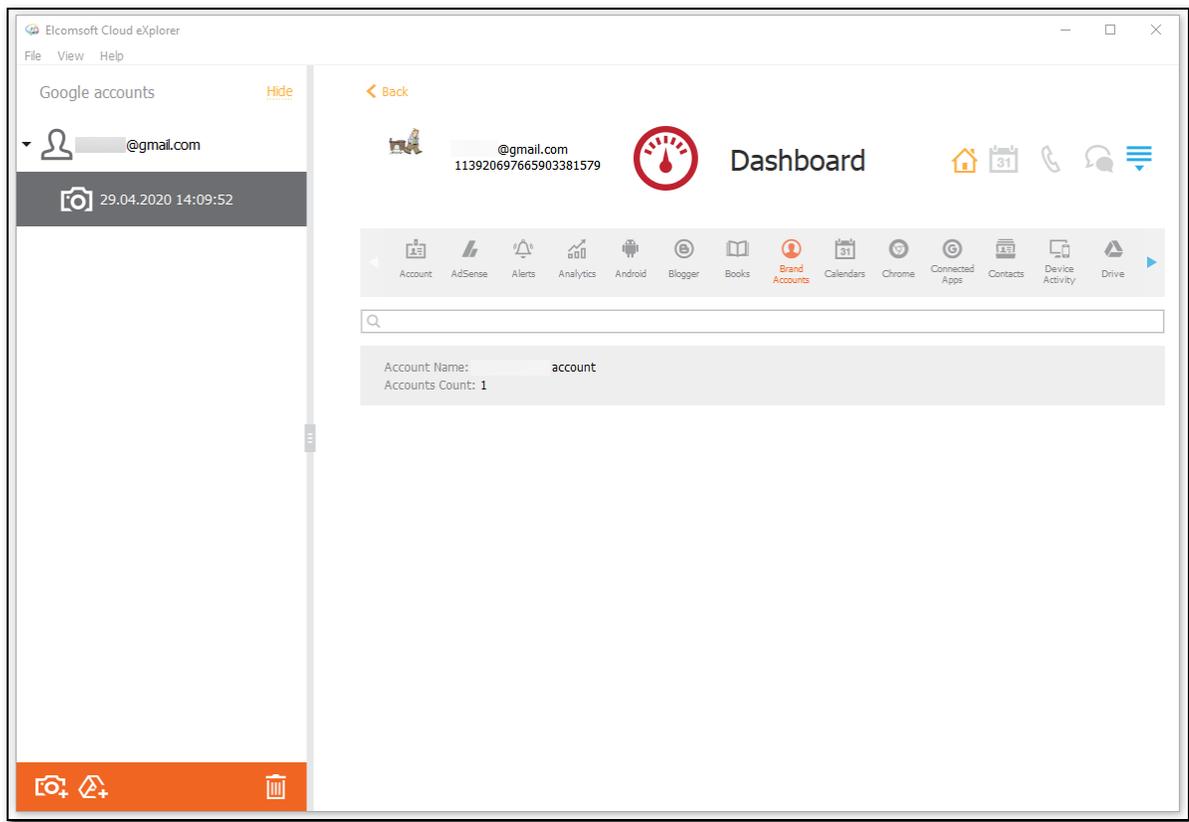


### 5.5.16.23 Brand Accounts

In the **Brand Accounts** section of the **Dashboard** plugin, you can view the information on the user's Brand Accounts, such as:

- **Account Name**
- **Accounts Count**

To perform searches in the **Brand Accounts** section, fill the search field and press **Enter**. The search results will be highlighted in yellow.

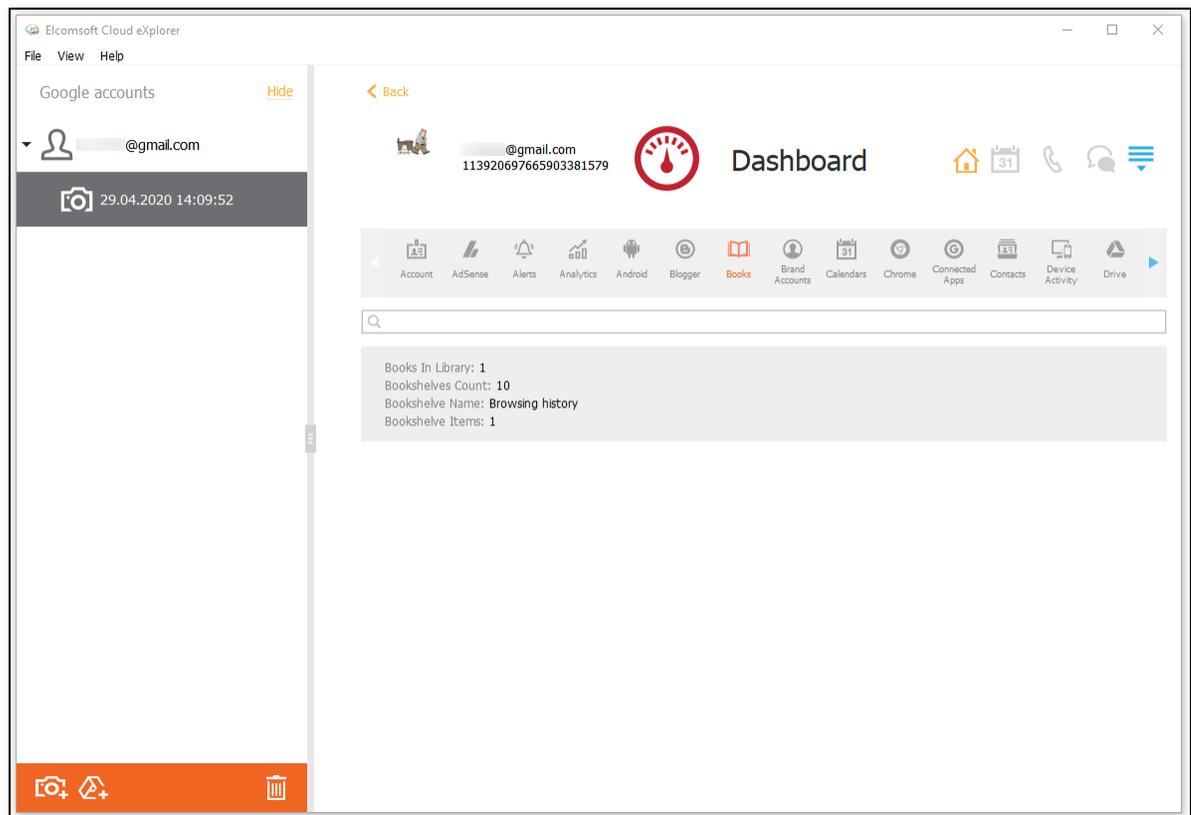


#### 5.5.16.24 Books

In the **Books** section of the **Dashboard** plugin, you can view the information from the Google Books service, such as:

- **Books In Library**
- **Bookshelves Count**
- **Bookshelf Name**
- **Bookshelf Items:** number of items

To perform searches in the **Books** section, fill the search field and press **Enter**. The search results will be highlighted in yellow.

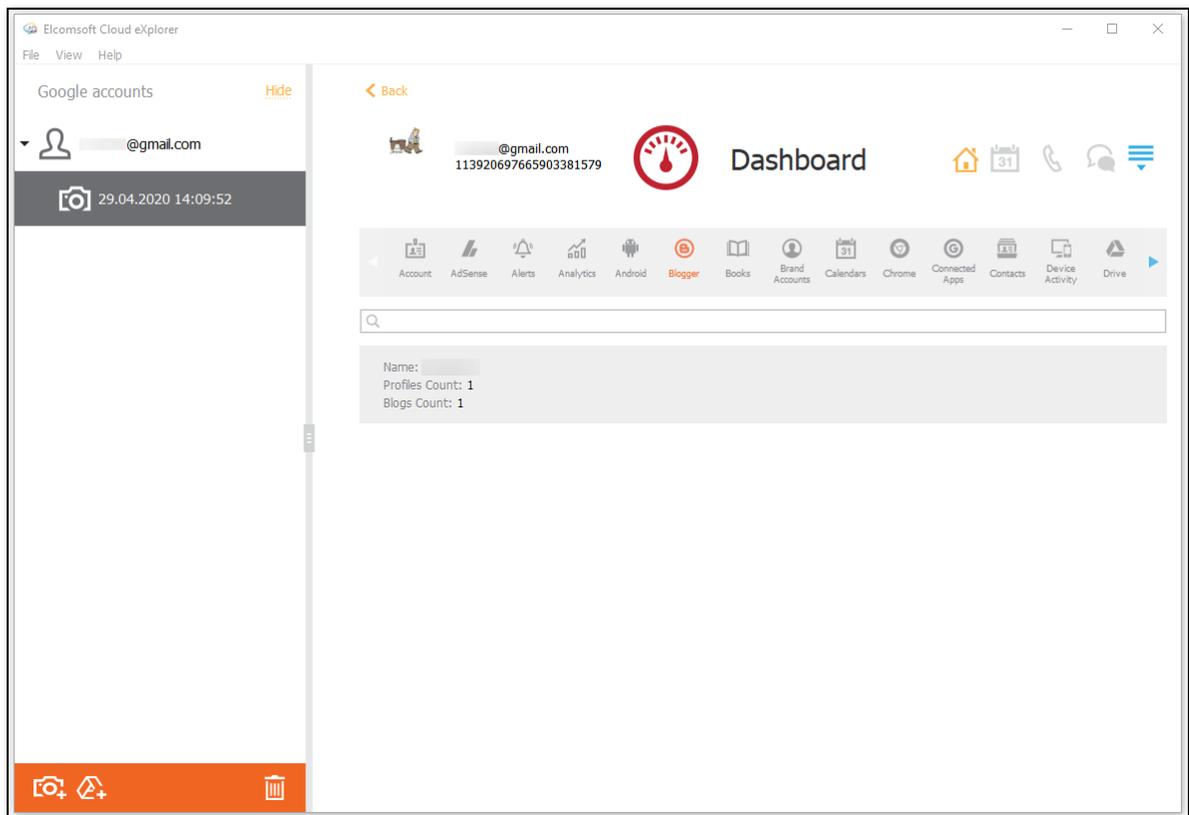


### 5.5.16.25 Blogger

In the **Blogger** section of the **Dashboard** plugin, you can view the information from the Google Blogger service, such as:

- **Name**
- **Profiles Count**
- **Blogs Count**

To perform searches in the **Blogger** section, fill the search field and press **Enter**. The search results will be highlighted in yellow.



### 5.5.16.26 Android

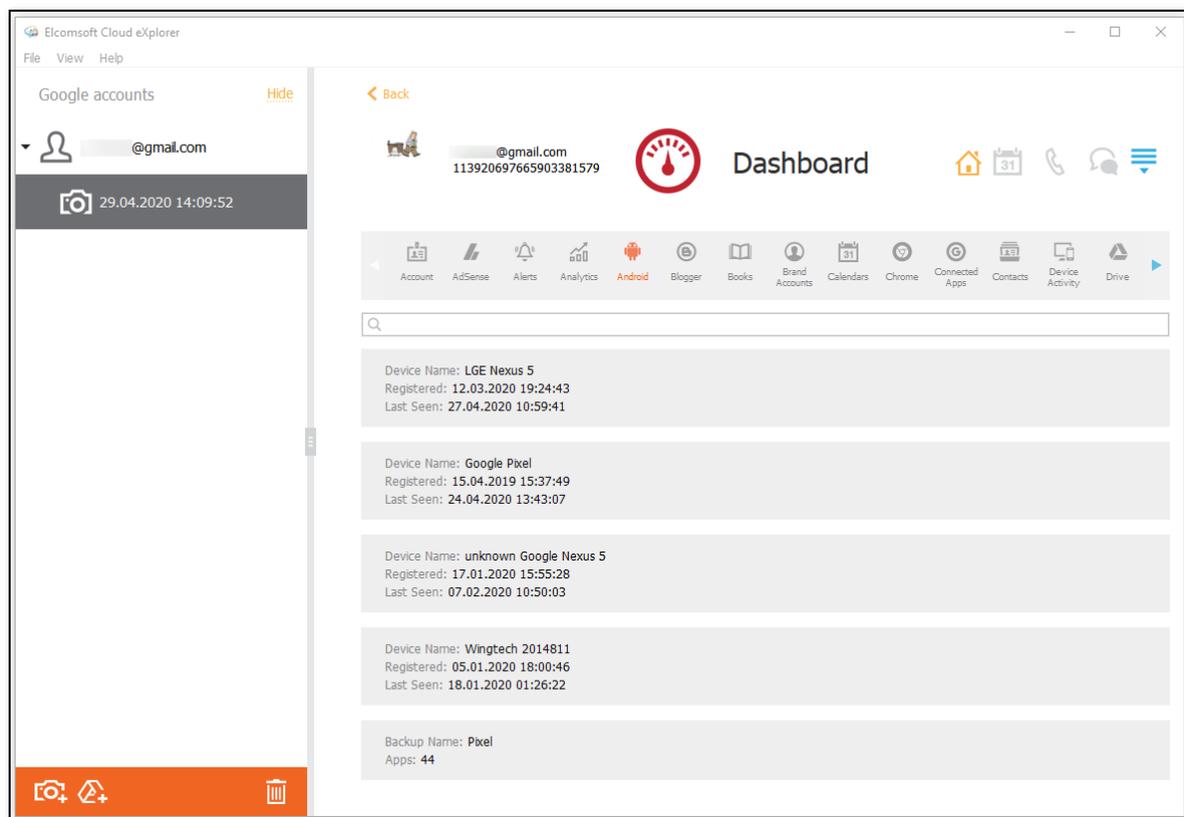
In the **Android** section of the **Dashboard** plugin, you can view the general information on each device associated with the Google account, such as:

- **Device Name**
- **Registered:** date, time, and timezone
- **Last Seen:** date, time, and timezone

The **Android** section also displays the following information on the backups:

- **Backup Name**
- **Apps:** number of the backed up applications

To perform searches in the **Android** section, fill the search field and press **Enter**. The search results will be highlighted in yellow.

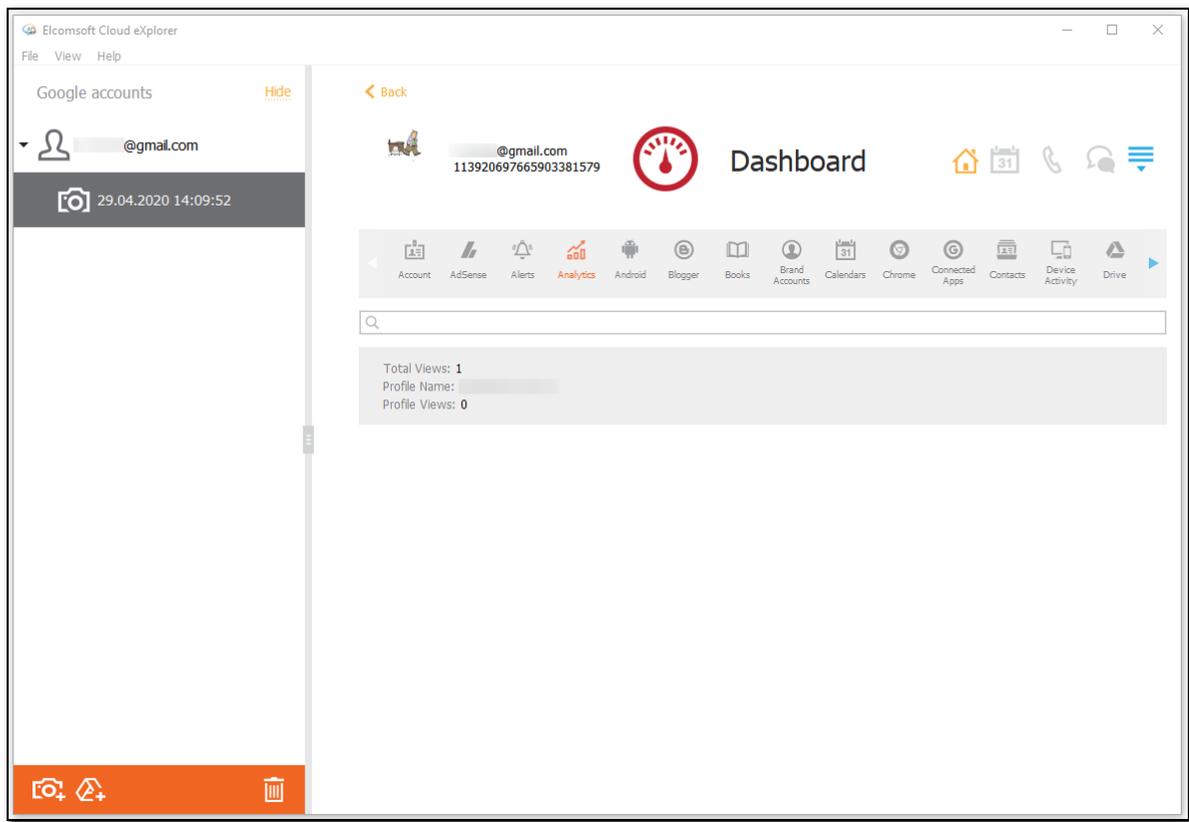


### 5.5.16.27 Analytics

In the **Analytics** section of the **Dashboard** plugin, you can view the information from the Google Analytics service, such as:

- **Total Views**
- **Profile Name**
- **Profile Views**

To perform searches in the **Analytics** section, fill the search field and press **Enter**. The search results will be highlighted in yellow.

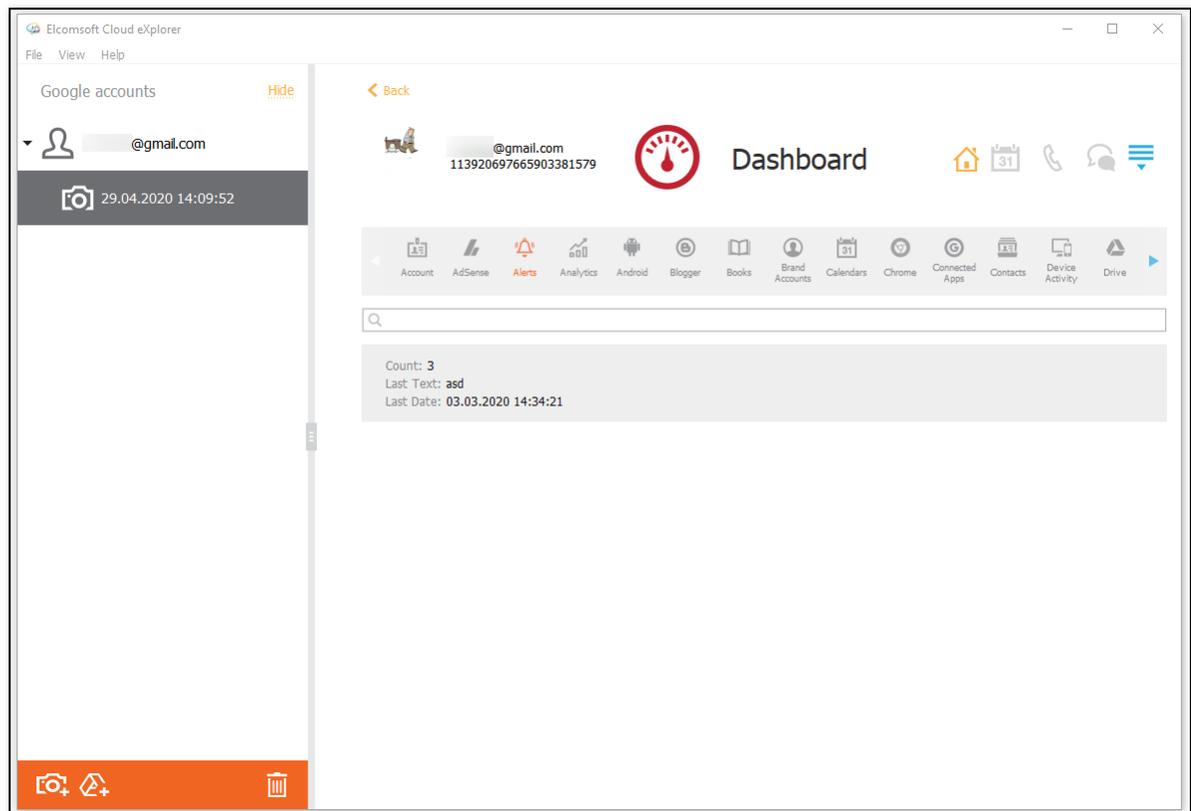


### 5.5.16.28 Alerts

In the **Alerts** section of the **Dashboard** plugin, you can find the information from the Google Alerts notification service, such as:

- **Count:** number of alerts
- **Last Text**
- **Last Date:** date, time, and timezone

To perform searches in the **Alerts** section, fill the search field and press **Enter**. The search results will be highlighted in yellow.

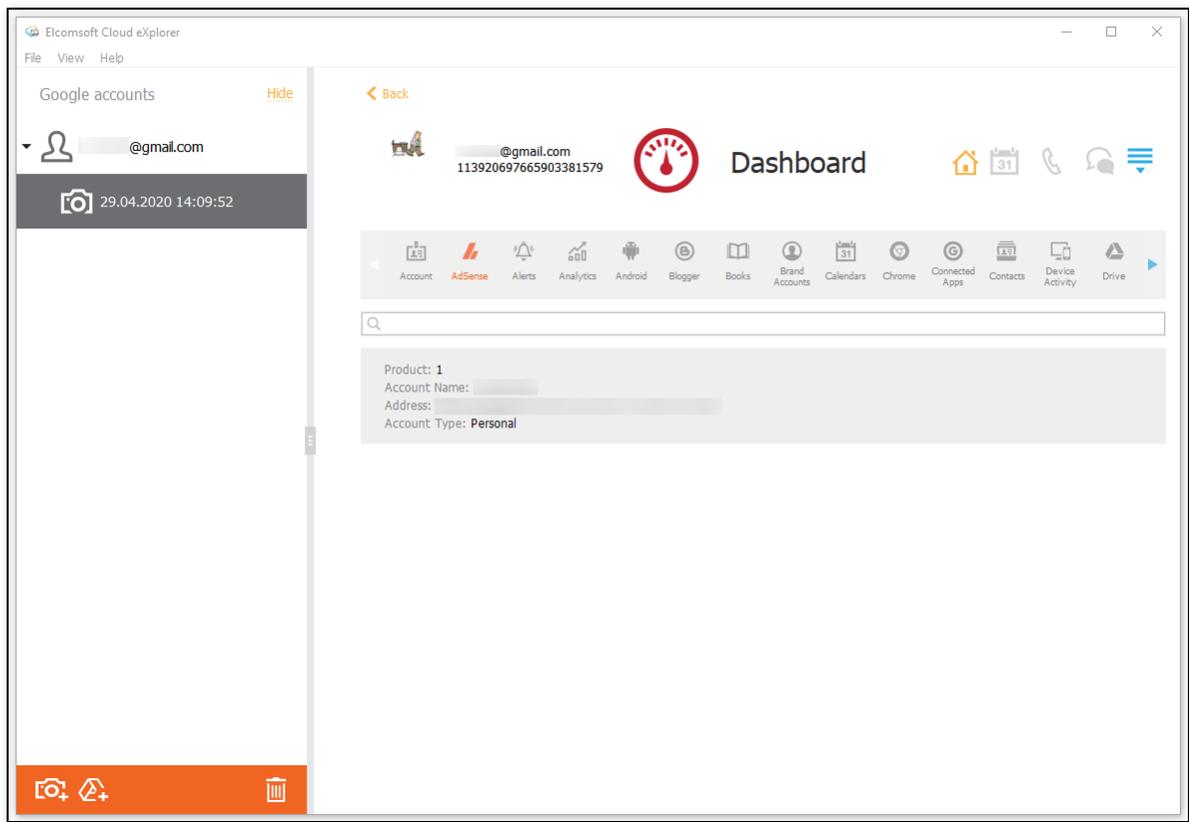


### 5.5.16.29 AdSense

In the **AdSense** section of the **Dashboard** plugin, you can view the information from the Google AdSense service, such as:

- **Product**
- **Account Name**
- **Address**
- **Account Type**

To perform searches in the **AdSense** section, fill the search field and press **Enter**. The search results will be highlighted in yellow.

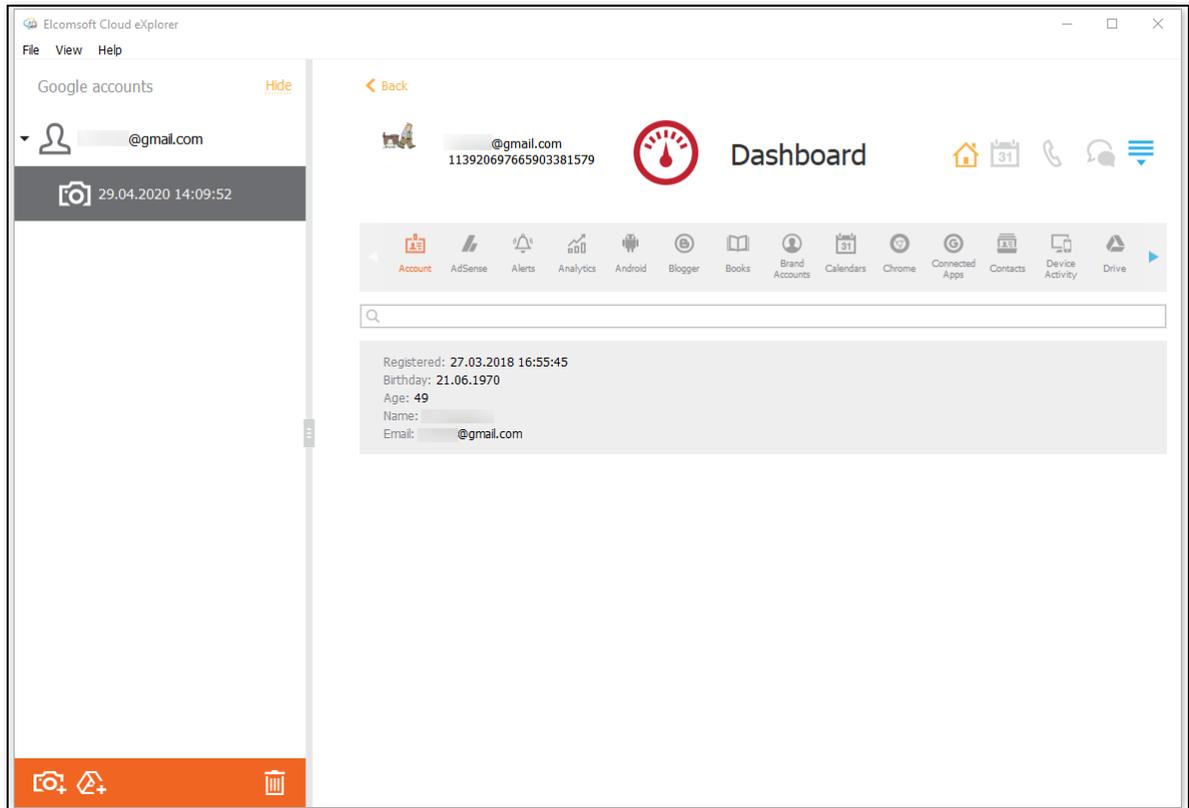


### 5.5.16.30 Account

In the **Account** section of the **Dashboard** plugin, you can view the general information on the Google account, such as:

- **Registered:** date, time, and timezone
- **Birthday**
- **Age**
- **Name**
- **Email**

To perform searches in the **Account** section, fill the search field and press **Enter**. The search results will be highlighted in yellow.



## 6 Elcomsoft eXplorer for WhatsApp

### 6.1 EXWA Program information

#### 6.1.1 EXWA settings

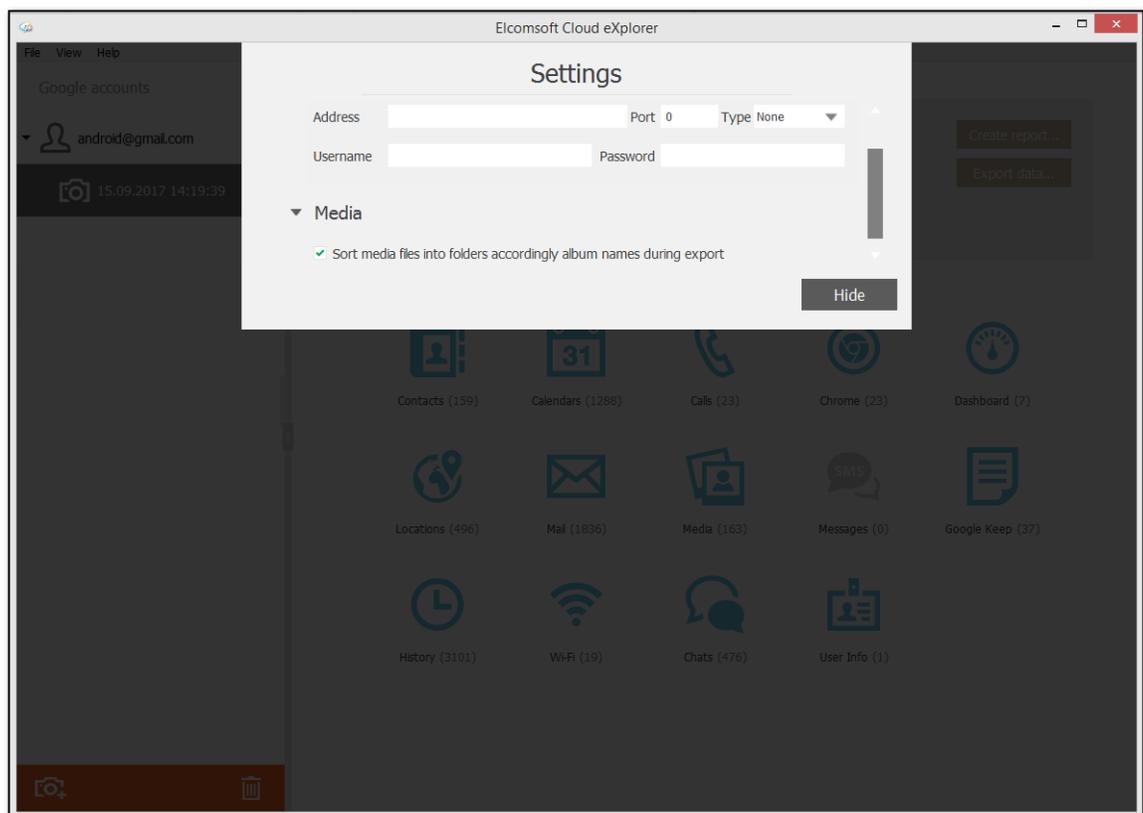
Elcomsoft eXplorer for WhatsApp allows you to customize working with EXWA.

To define EXWA Settings, navigate to **View - Settings**.

- **Proxy server**

Define the Proxy server that will be used when downloading [iCloud backups](#).

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



#### 6.1.2 Supported devices

All devices (iPhone, iPad and iPod Touch) running iOS versions from 6 to 14.0 are supported for all WhatsApp versions.

For all WhatsApp an Android, all devices running Android from 4.0 to 6.0.1 (unrooted) and 9.0 (rooted only) are supported.

### 6.1.3 Moving backup storage

You can move the backup storage to another location on your computer.

**To move the storage**, make sure that EXWA is not running and then do the following:

1. Open the **Settings.ini** file. The file is located here: \AppData\Roaming\Elcomsoft\Elcomsoft eXplorer for WhatsApp\Setting.ini.
2. Enter the new path for the storage using double back slashes (\\) and only Latin characters (e.g., **C:\Users\jane.smith\AppData\Roaming\Elcomsoft**). The new location must not be a shared folder and must contain enough free space.
3. Save the **Settings.ini** file.
4. Copy the current **Backups** folder to the new location specified in the **Settings.ini** file.
5. The new settings will be applied as soon as EXWA is started for the first time after editing the **Settings.ini** file.

Please note that the **Temp** folder and the log files with settings cannot be replaced from the **AppData** folder.

## 6.2 Working with backups of Apple devices

### 6.2.1 About backups of Apple devices

#### 6.2.1.1 Creating WhatsApp data backups

You can back up your WhatsApp data to iCloud backup or iCloud Drive.

##### Creating iCloud backup

To back up your WhatsApp data to iCloud backup, go to **Settings > iCloud > Storage > Manage Storage > This iPhone**. Make sure WhatsApp is turned on.

##### Creating iCloud Drive backup

To back up your WhatsApp data to iCloud Drive, go to **WhatsApp Settings > Chats and Calls > Chat Backup**, and then tap **Back Up Now**.

You can also schedule automatic backups of your WhatsApp data to iCloud Drive. To do this, go to **WhatsApp Settings > Chats and Calls > Chat Backup**, and then tap **Auto Backup**. Choose the backup frequency you need.

Requirements for creating WhatsApp data backups in iCloud Drive:

- There must be iOS 5.1 or later on your iPhone.
- You must be signed into iCloud (**iPhone Settings > iCloud**).
- You must have enough free space on both your iCloud and your iPhone.
- Make sure the following settings are set to ON:
  - For iOS 7: Documents & Data (iPhone Settings > iCloud > Documents & Data)
  - For iOS 8 and later: iCloud Drive (iPhone Settings > iCloud > iCloud Drive)

For more information on creating iCloud Drive backups, please follow the link:  
<https://www.whatsapp.com/faq/en/iphone/20888066#backup>

### 6.2.1.2 About authentication token

iCloud allows users to store various information from their iOS devices in the cloud.

For Windows OS, exchanging data between iOS devices and the computer is done via the iCloud for Windows (available for Windows 7 or later). This software allows the user to work with data from iOS on a computer with Windows OS. macOS users can access iCloud without any additional software, as it is built into the operating system (iCloud requires macOS 10.7.2 or later).

To extract authentication token representing the user's iCloud account credentials, you are going to need an **Elcomsoft Apple Token Extractor** for Windows OS or macOS which is shipped with the **Elcomsoft Phone Breaker**. You can use this token to sign in to the user's iCloud account in order to download the backups or files stored there. It is also possible to get authentication token without logging in to an actual OS, Windows or macOS, where the token was used (e.g., by mounting a disk image to the current system) via Elcomsoft Phone Breaker.

**Types of the authentication tokens extracted by Elcomsoft Apple Token Extractor on Windows OS and macOS:**

	iCloud for Windows lower v. 7.0	iCloud for Windows v. 7.0 and later	macOS lower 10.13	macOS 10.13 and later
<b>Account with two-factor authentication</b>	Authentication token without limitations	Authentication token with limitations	Authentication token without limitations	Authentication token with limitations
<b>Account without two-factor authentication</b>	Authentication token for the account without two-factor authentication	Authentication token for the account without two-factor authentication	Authentication token for the account without two-factor authentication	Authentication token for the account without two-factor authentication

**Authentication tokens supported on Windows OS for downloading data via EXWA:**

- Authentication token without limitations for the account with two-factor authentication
- Authentication token for the account without two-factor authentication

## 6.2.2 Adding backups to EXWA

### 6.2.2.1 Working with WhatsApp data in local iOS backups

#### Adding local iOS backups

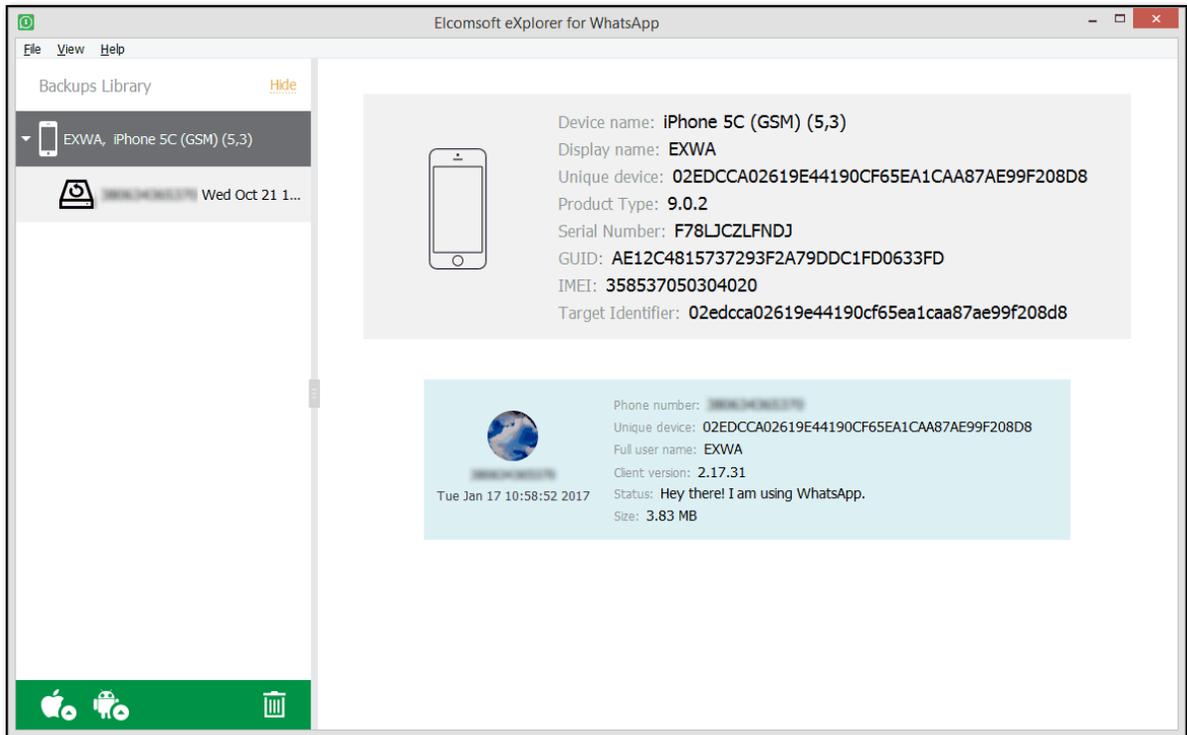
To start working with local backups:

1. In the Backups Library pane, click the **Acquire data for Apple iOS device** icon .
2. In the opened menu, click the **Load iTunes/iCloud backup** icon .
3. Browse for folder where your iOS device backup is located (see [Supported Apple device backups](#), [About iTunes backups](#) and [About iCloud backups](#) for more info) and click **Open**.
4. If the backup is encrypted, enter the password to the backup and click **Done**.

Once backup is loaded, the following device information is displayed (some of it may not be available for iCloud backups, so only for local iTunes backups this information is complete):

- Device name

- Display name
- Apple Id
- Unique device ID
- Product Type
- Serial number
- GUID
- IMEI
- Target identifier (usually the same as Unique device)



The lower part of the window displays the userpic, phone number, and the backup date (according to the time zone and date format defined on the local PC) as well as the following WhatsApp information:

- Phone number
- Unique device ID
- Full user name
- Client version
- Status
- Size

### Viewing data

When you select the target WhatsApp backup in the Backups Library to the left, the lower part of the window shows all plugins available (some of them might be disabled if there is no appropriate information in backup):

- [Calls](#)
- [Contacts](#)
- [Media](#)

- [Messages](#)

Click the plugin icon to view the contents.

### Exporting data

EXWA allows you to export data from a backup to your PC. Data is exported to an XLSX file, and all attachments/files are saved to a folder in the same location as the XLSX file.

Please note that data export is only available in the registered version of the program.

To export data, do the following:

1. In the **Data View** pane, click **Export data**.
2. Select the data categories to export.
3. Define the time interval for which you want to export data as follows: enable filters by switching the On/Off toggle and then select the dates in the From and Until fields.
4. Click **Export**.
5. The window will open in which you can select the location for exported data.
6. Once you select the location, click **Save**.
7. Data export will start.
8. To open exported data, click the icon next to the **Data has been exported** message highlighted in yellow or open it from the location to which it was saved.

### 6.2.2.2 Working with WhatsApp data in iCloud backups

#### Adding iCloud backups

To start working with iCloud backups:

1. In the Backups Library pane, click the **Acquire data for Apple iOS device** icon .
2. In the opened menu, click the **Download iCloud backup** icon .
3. In the opened window, enter your Apple ID and password or [authentication token](#), extracted via EPB. Click **Sign in**.

**NOTE: If the Apple ID is protected with two-factor authentication, you need to confirm sending the verification code to all of your trusted devices or to your phone.**

You can select the **Save user credentials for future sessions** option when logging in. If this option is selected, the entered login and password will be saved to be quickly added into corresponding fields during next login.

Please note that after logging in the authentication token is saved and the **Verification code** is no longer required to be entered for the account in case of [two-step verification](#) or [two-factor authentication](#).

4. 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 in the Apple account settings.

Click **Verify**.

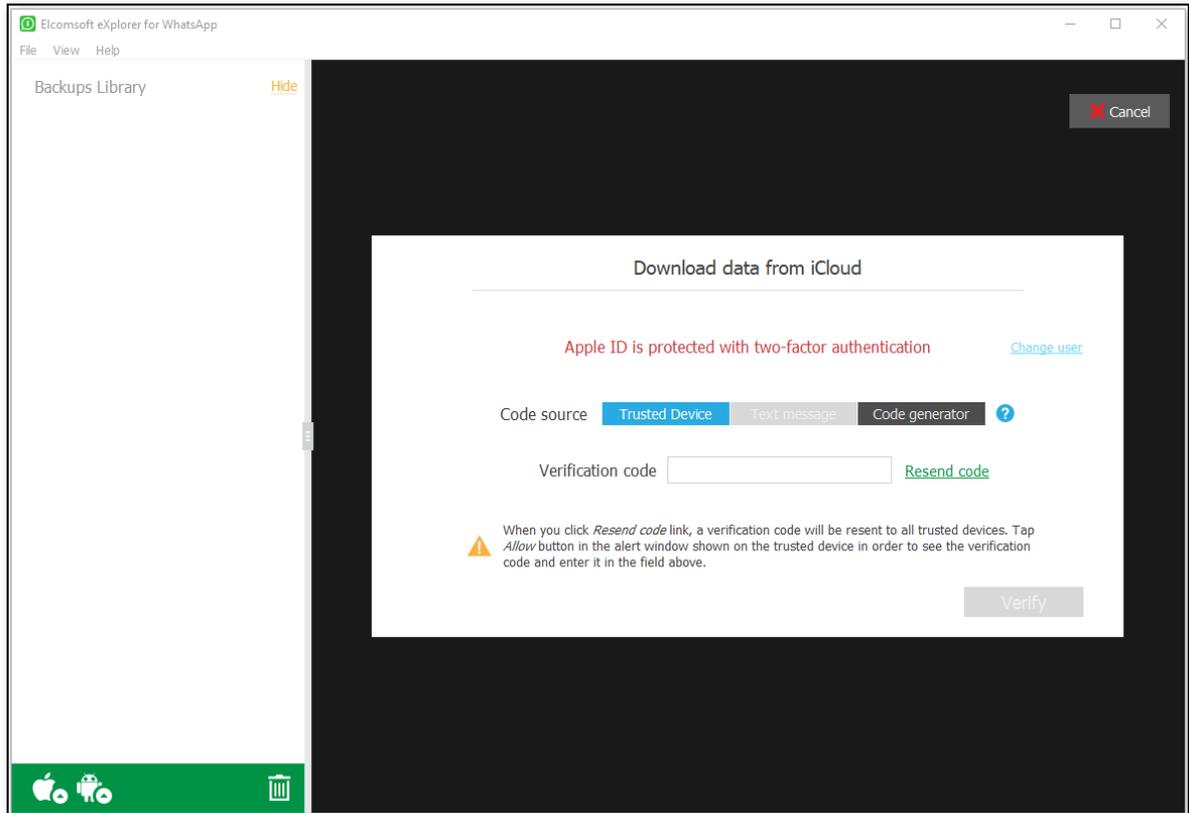
If the Apple ID is protected with [two-factor authentication](#), perform authentication in one of the following ways:

- Select **Trusted Device** and enter the 6-digit code in the **Verification code** field. Click **Resend code** for the verification code to be sent to all trusted devices.

- Select **Code generator** and enter the 6-digit code in the **Verification code** field. The code is generated on the trusted device or via Cloud Panel.

**NOTE: The current version of EXWA does not support authentication via the Text message.**

Click **Verify**.



5. Once the backup is downloaded and iCloud data is processed, the following Apple ID information is displayed:

- Display name
- Apple Id
- Person Id
- Auth Type
- Storage Total Size
- Storage Used Size

The lower part of the window displays the information about backed up devices linked to the target Apple Id, their names and device types, as well as the following information:

- Apple Id
- Unique device
- Product Type
- Serial number
- Backup date (according to the time zone and date format defined on the local PC)
- Backup size

Click the target device in the Backups Library to the left. The following device information is displayed:

- Device name
- Display name
- Apple Id
- Unique device
- Product Type
- Serial number
- Backup date (according to the time zone and date format defined on the local PC)
- Backup size

The lower part of the window shows all WhatsApp backups available for the selected device with the following information:

- Apple Id
- Phone number
- Unique device
- Full user name
- Client version
- Status
- Size

#### Viewing data

When you select the target WhatsApp backup in the Backups Library, the lower part of the window displays all plugins available (some of them might be disabled if there is no appropriate information in backup):

- [Calls](#)
- [Contacts](#)
- [Media](#)
- [Messages](#)

Click the plugin icon to view the contents.

#### Exporting data

EXWA allows you to export data from a backup to your PC. Data is exported to an XLSX file, and all attachments/files are saved to a folder in the same location as the XLSX file.

Please note that data export is only available in the registered version of the program.

To export data, do the following:

1. In the **Data View** pane, click **Export data**.
2. Select the data categories to export.
3. Define the time interval for which you want to export data as follows: enable filters by switching the On/Off toggle and then select the dates in the From and Until fields.
4. Click **Export**.
5. The window will open in which you can select the location for exported data.
6. Once you select the location, click **Save**.
7. Data export will start.
8. To open exported data, click the icon next to the **Data has been exported** message highlighted in yellow or open it from the location to which it was saved.

### 6.2.2.3 Working with WhatsApp data in iCloud Drive files

#### Adding iCloud Drive files

To start working with iCloud Drive files:

1. In the Backups Library pane, click the **Acquire data for Apple iOS device** icon .
2. In the opened menu, click the **Download Files from iCloud Drive** icon .
3. In the opened window, enter your Apple ID and password, or [authentication token](#), extracted via EPB. Click **Sign in**.

**NOTE: If the Apple ID is protected with two-factor authentication, you need to confirm sending the verification code to all of your trusted devices or to your phone.**

You can select the **Save user credentials for future sessions** option when logging in. If this option is selected, the entered login and password will be saved to be quickly added into corresponding fields during next login.

Please note that after logging in the authentication token is saved and the **Verification code** is no longer required to be entered for the account in case of [two-step verification](#) or [two-factor authentication](#).

4. 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 in the Apple account settings.

Click **Verify**.

If the Apple ID is protected with [two-factor authentication](#), perform authentication in one of the following ways:

- Select **Trusted Device** and enter the 6-digit code in the **Verification code** field. Click **Resend code** for the verification code to be sent to all trusted devices.
- Select **Code generator** and enter the 6-digit code in the **Verification code** field. The code is generated on the trusted device or via Cloud Panel.

**NOTE: The current version of EXWA does not support authentication via the Text message.**

Click **Verify**.

4. Once the WhatsApp files are downloaded from iCloud Drive and processed, the following Apple ID information is displayed:

- Display name
- Apple Id
- Person Id
- Auth Type
- Storage Total Size
- Storage Used Size

The lower part of the window shows all WhatsApp backups available for the selected Apple ID with the following information:

- Apple Id

- Phone number
- Photos
- Messages
- Calls Received
- Calls Sent
- Size

### Viewing data

When you select the target WhatsApp backup in the Backups Library, the lower part of the window displays all plugins available (some of them might be disabled if there is no appropriate information in backup):

- [Calls](#)
- [Contacts](#)
- [Media](#)
- [Messages](#)

Click the plugin icon to view the contents.

### Exporting data

EXWA allows you to export data from a backup to your PC. Data is exported to an XLSX file, and all attachments/files are saved to a folder in the same location as the XLSX file.

Please note that data export is only available in the registered version of the program.

To export data, do the following:

1. In the **Data View** pane, click **Export data**.
2. Select the data categories to export.
3. Define the time interval for which you want to export data as follows: enable filters by switching the On/Off toggle and then select the dates in the From and Until fields.
4. Click **Export**.
5. The window will open in which you can select the location for exported data.
6. Once you select the location, click **Save**.
7. Data export will start.
8. To open exported data, click the icon next to the **Data has been exported** message highlighted in yellow or open it from the location to which it was saved.

### Working with encrypted iCloud Drive backups

Encrypted backups are labeled with the  icon in the backup list and a special "lock" element in the backup info panel.

Please note that decrypting iCloud Drive backups is only available in the registered version of the program.

To view an encrypted backup:

1. Select the target encrypted backup. A message will be displayed:



Backup is encrypted. You can decrypt it if you have access to a SIM card tethered to the backup or the keychain file extracted via the Elcomsoft iOS Forensic Toolkit. If not, you can open the backup but only media data will be available.

**Note:** During backup decryption via a SIM card, the user will be signed out of WhatsApp on the device.

Open
Decrypt

2. Make your choice:

- Click **Open** to get an immediate access to the backup (but only **Media** data will be available to view).
- Click **Decrypt** to decrypt the backup for a full access to the backup data.

3. If you select to decrypt the backup, on the **Decrypt backup** page, define the decryption type:

- **SMS:** In the **Phone number** field, enter a phone number associated with the WhatsApp account, click **Send code**, and then enter the received code in the **Verification code** field.

If you did not receive the code or it expired, click **Resend code**. A special timer shows when it will be possible to send a new code.

**NOTE:** Using this decryption type, EXWA cannot decrypt a backup if the WhatsApp account on iOS was protected with two-step verification while the backup was being created.

**NOTE:** Do not click the URL in the message with the verification code. You have to enter the verification code manually, otherwise EXWA will not be authenticated with WhatsApp and you will have to wait for a while until a new code is sent.

### Decrypt backup

---

Decrypt with SMS Keychain dump ?

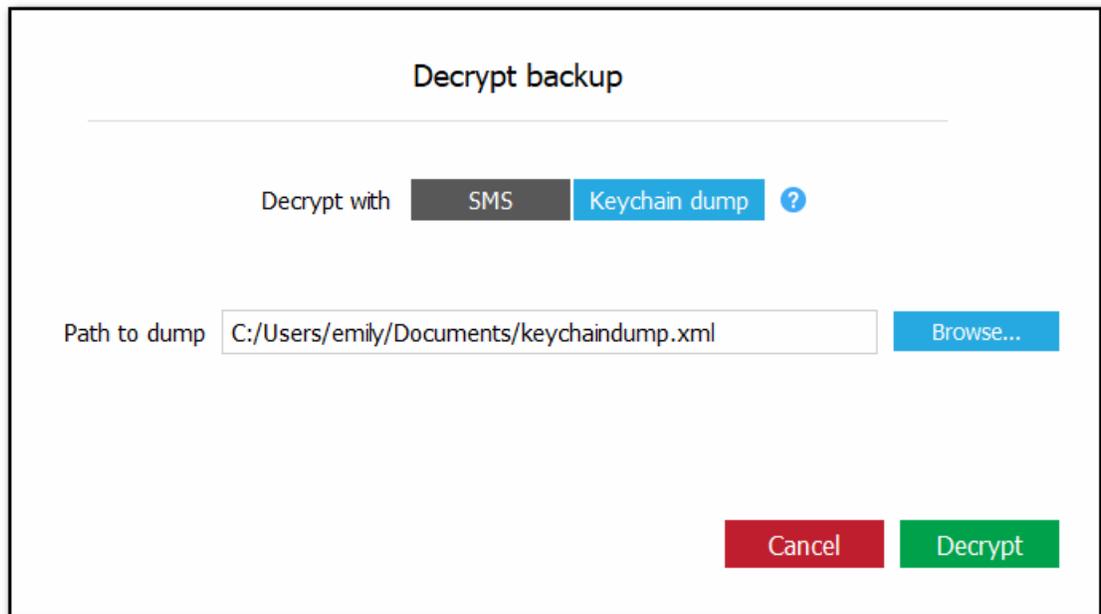
Phone number

Verification code  Resend code 00:01:04

⚠ **Note:** you will be logged out of WhatsApp on your device. To continue using WhatsApp on your device, you will have to sign in again after obtaining the key with the program.

Cancel
Decrypt

- **Keychain dump:** In the **Path to dump** field, enter the full path to the decrypted keychain dump (.xml file) extracted via [Elcomsoft iOS Forensic Toolkit](#) (EIFT) or click **Browse** and navigate to the file. EIFT can extract keychain dumps only from jailbroken iOS devices.



4. Click **Decrypt**.

**NOTE:** During backup decryption via SMS, the user will be signed out of WhatsApp on the device.

5. Once EXWA is authenticated with WhatsApp, the decryption process starts. Please note that after you decrypt a backup associated with a phone number, all other backups for this phone number will be decrypted automatically after the download or on clicking a backup.

Decrypted backups are labeled with the  icon in the backup list.

## 6.3 Working with data from Android devices

### 6.3.1 About WhatsApp data from Android devices

EXWA allows you to analyze the WhatsApp and WhatsApp Business data from your rooted Android devices previously backed up to your computer.

Loading WhatsApp data from Android devices is available for both rooted and unrooted devices. Loading WhatsApp Business data from Android devices is available only for rooted devices.

When saving the WhatsApp data to the local storage:

1. Make sure your device is rooted.
2. Copy the `\data\data\com.whatsapp` folder from the device. Once you have copied it, make sure to preserve the original WhatsApp data structure. Otherwise, EXWA would be unable to analyze it properly.
3. Take note of the path to the `com.whatsapp_preferences.xml` file (i.e., `<folder with the backup on your PC>\com.whatsapp\shared_prefs\`)
4. Copy the `\sdcard\WhatsApp` folder from the device. Once you have copied it, make sure to preserve the original WhatsApp data structure. Otherwise, EXWA would be unable to analyze it properly.

5. Take note of the path to the **Media** folder (i.e., **<folder with the backup on your PC>\WhatsApp\Media**)

When saving the WhatsApp Business data to the local storage:

1. Make sure your device is rooted.
2. Copy the **\data\data\com.whatsapp.w4b** folder from the device. Once you have copied it, make sure to preserve the original WhatsApp Business data structure. Otherwise, EXWA would be unable to analyze it properly.
3. Take note of the path to the **com.whatsapp.w4b\_preferences.xml** file (i.e., **<folder with the backup on your PC>\com.whatsapp.w4b\shared\_prefs\**)
4. Copy the **\sdcard\WhatsApp Business** folder from the device. Once you have copied it, make sure to preserve the original WhatsApp Business data structure. Otherwise, EXWA would be unable to analyze it properly.
5. Take note of the path to the **Media** folder (i.e., **<folder with the backup on your PC>\WhatsApp Business\Media**)

### 6.3.2 Loading WhatsApp data from Android devices

EXWA allows you to analyze the WhatsApp and WhatsApp Business data loaded directly from your Android devices while working with EXWA.

Loading WhatsApp data from Android devices is available for both rooted and unrooted devices. Loading WhatsApp Business data from Android devices is available only for rooted devices.

Before loading the data from it, you need to enable the **USB debugging mode** on the device.

To enable the USB debugging mode on Android **4.0 - 4.1.x**:

1. Go to Settings > Developer Options.
2. Enable **Developer Options**.
3. Tap **USB Debugging**.
4. Tap **OK** in the confirmation message.

To enable the USB debugging mode on Android **4.2.x and higher**:

1. Go to App drawer > Settings.
2. Tap **About phone** or **About tablet**.
3. Tap **Build number** seven times. The "You are now a developer!" confirmation message is displayed.
4. Tap **Back**.
5. Go to Settings > Developer Options > USB Debugging.
6. Tap **USB Debugging**.
7. Tap **OK** in the confirmation message.

### 6.3.3 About Google authentication token

When you sign in via EXWA using the login and password with the **Save credentials for future use** option selected, EXWA stores an authentication token locally.

To use the token on next sign-in to this account, enter the login and make sure the **Use token instead of password (if available)** option is selected. When you sign in with a token, you do not have to use the password or pass two-step verification (use USB-token, Google Prompt, or enter a secure code).

### 6.3.4 Working with data loaded from Android device

#### Adding data from Android device

To start working with data loaded from Android device:

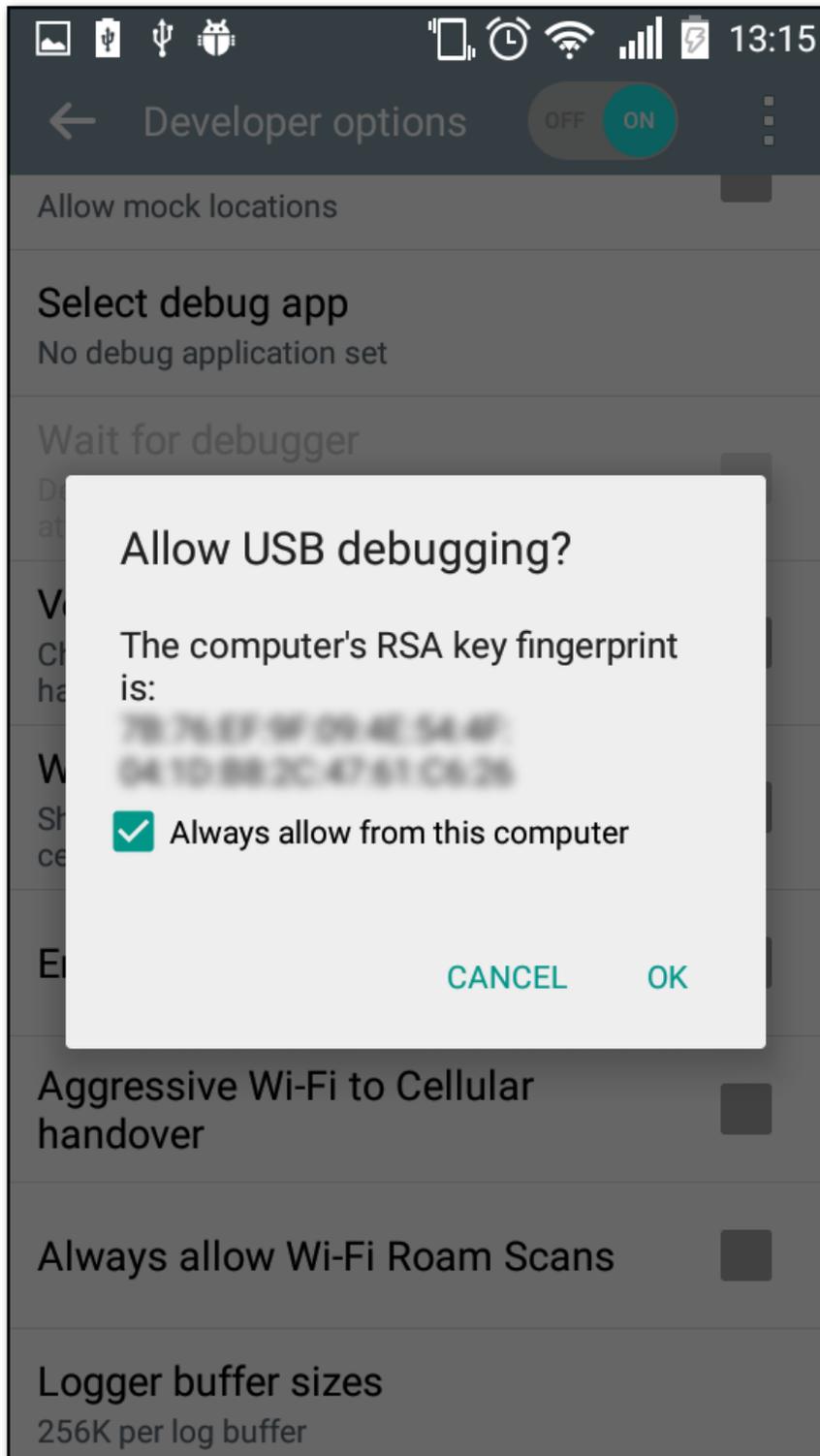
1. Connect the Android device to the machine with EXWA installed.
2. Make sure the USB Debugging Mode is enabled on the device.

3. In the Backups Library pane, click the **Acquire data for Android device** icon .

4. In the opened menu, click the **Load from device** icon .

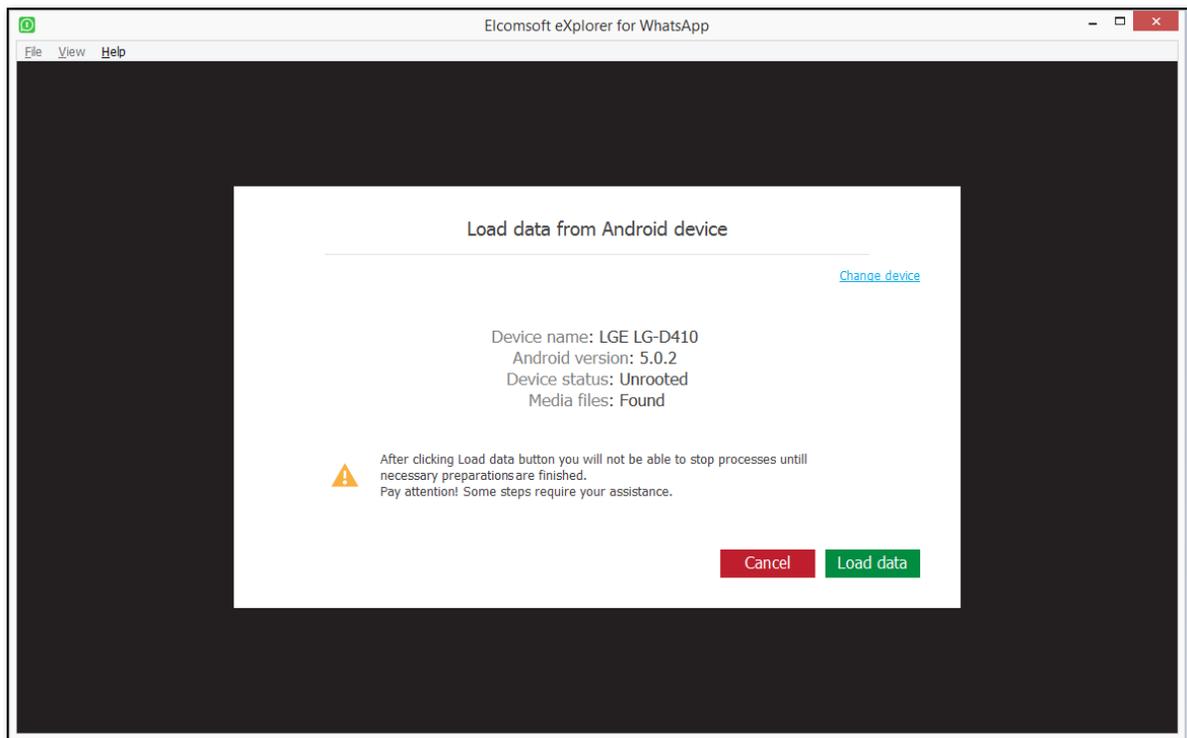
**NOTE: If you do not have the latest version of Java installed, the message with the link to download it will be displayed. Download and install the latest Java version.**

5. Click **Check**.
6. On the unblocked device, tap **Always allow from this computer** and allow the device to communicate to the computer.



7. Once the connection is established, the following information about the device is displayed:
- Device name

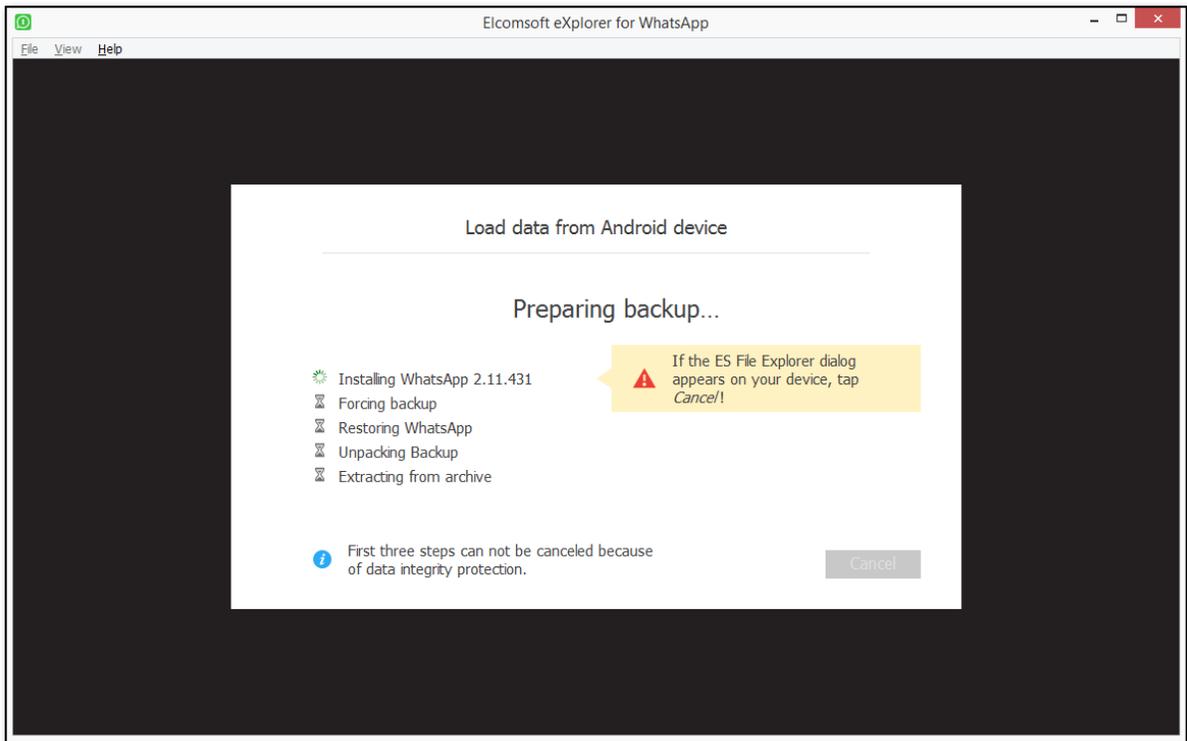
- Android version
- Device status (rooted, unrooted)
- Media files (found, not found)



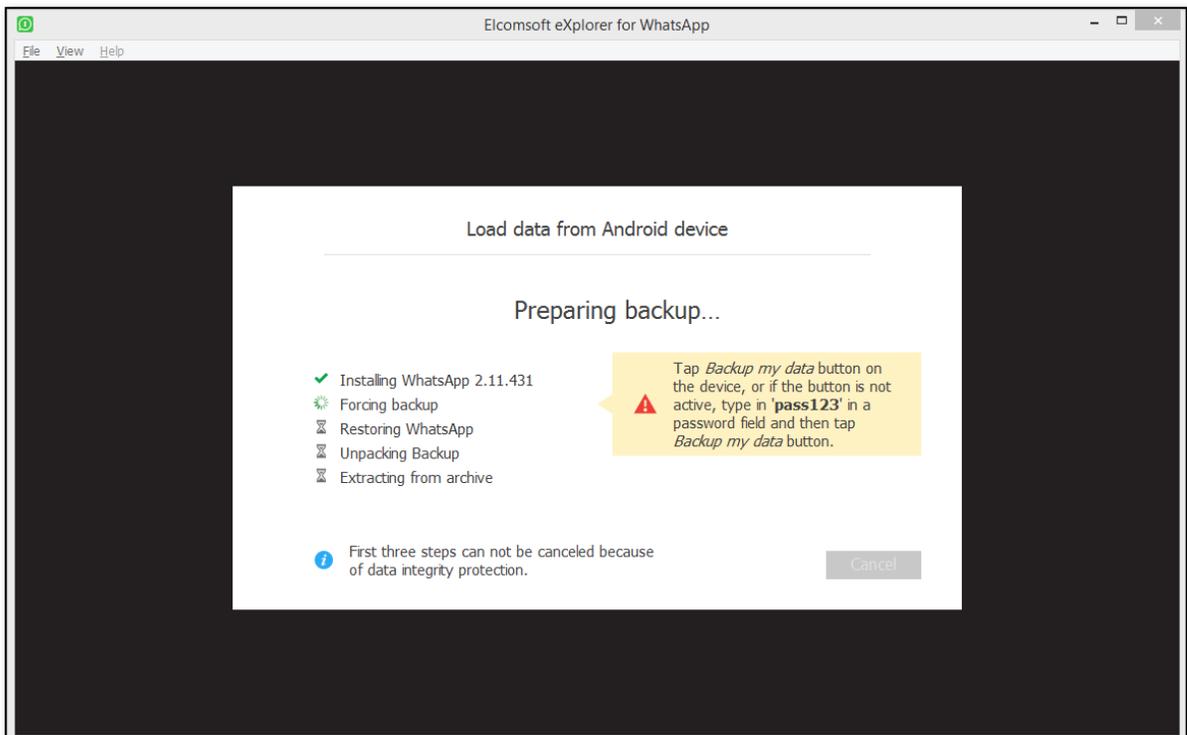
8. If there are both WhatsApp and WhatsApp Business applications installed on the device, click the  icon on the **Load data** button and select what data you want to load. If you select both applications, data will be displayed as a separate snapshot for each of them.
9. Click **Load data**.
10. Backup preparation starts. Some steps may require your assistance:

**NOTE:** The connection between the device and the computer might break during preparation due to the state of the *adb* daemon on the device. If this happens, click **Check** and try to load data again.

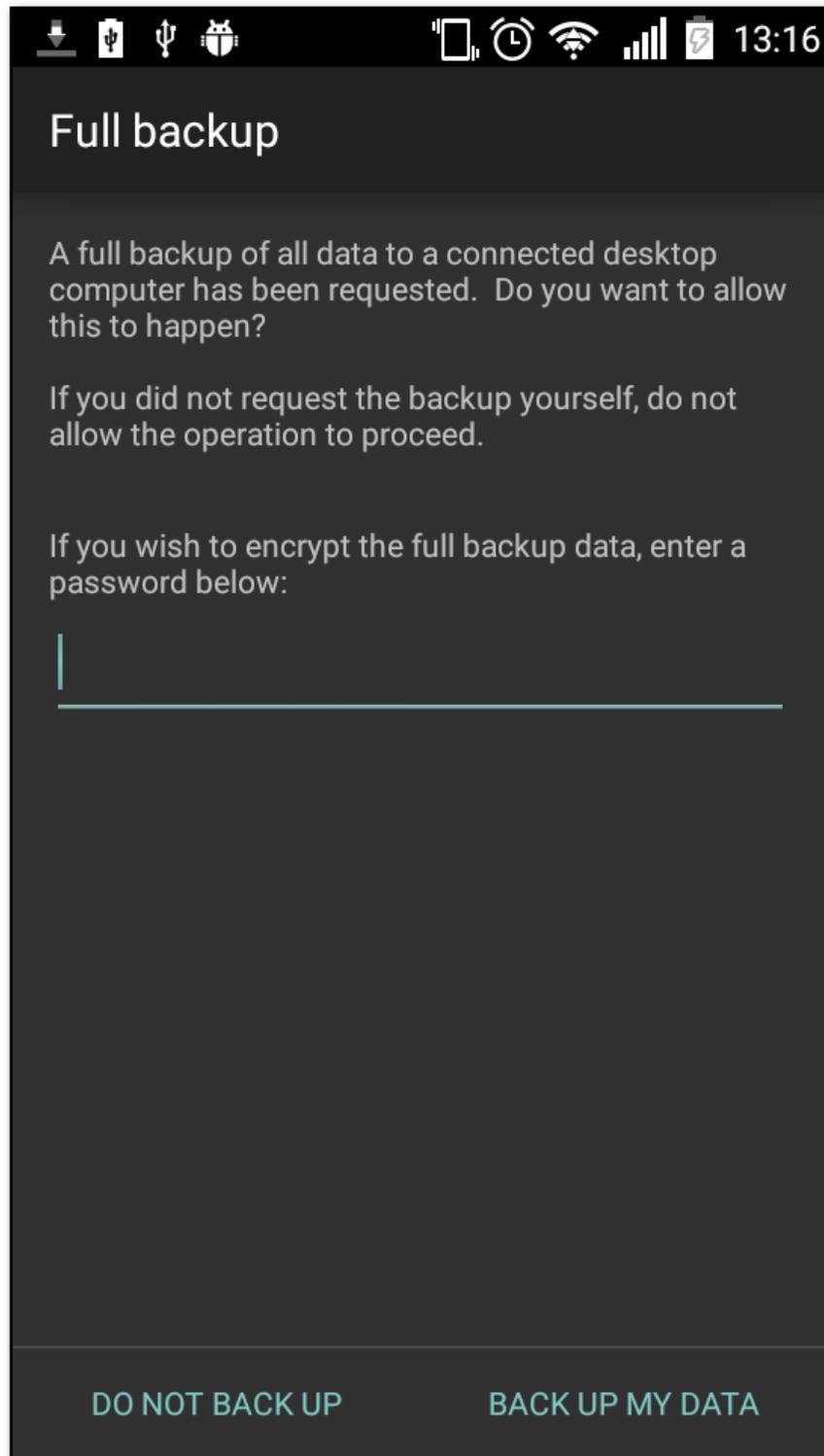
- **Installing WhatsApp.** If the ES File Explorer dialog appears on the device, tap **Cancel**.



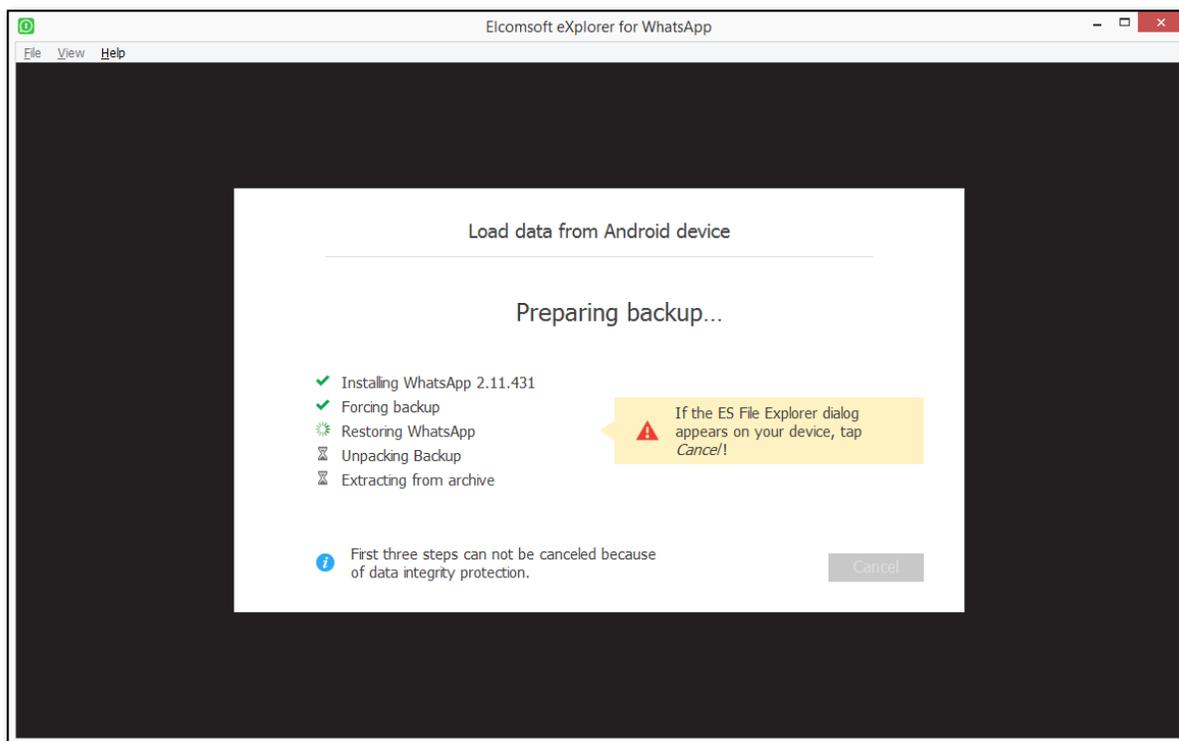
o Forcing backup.



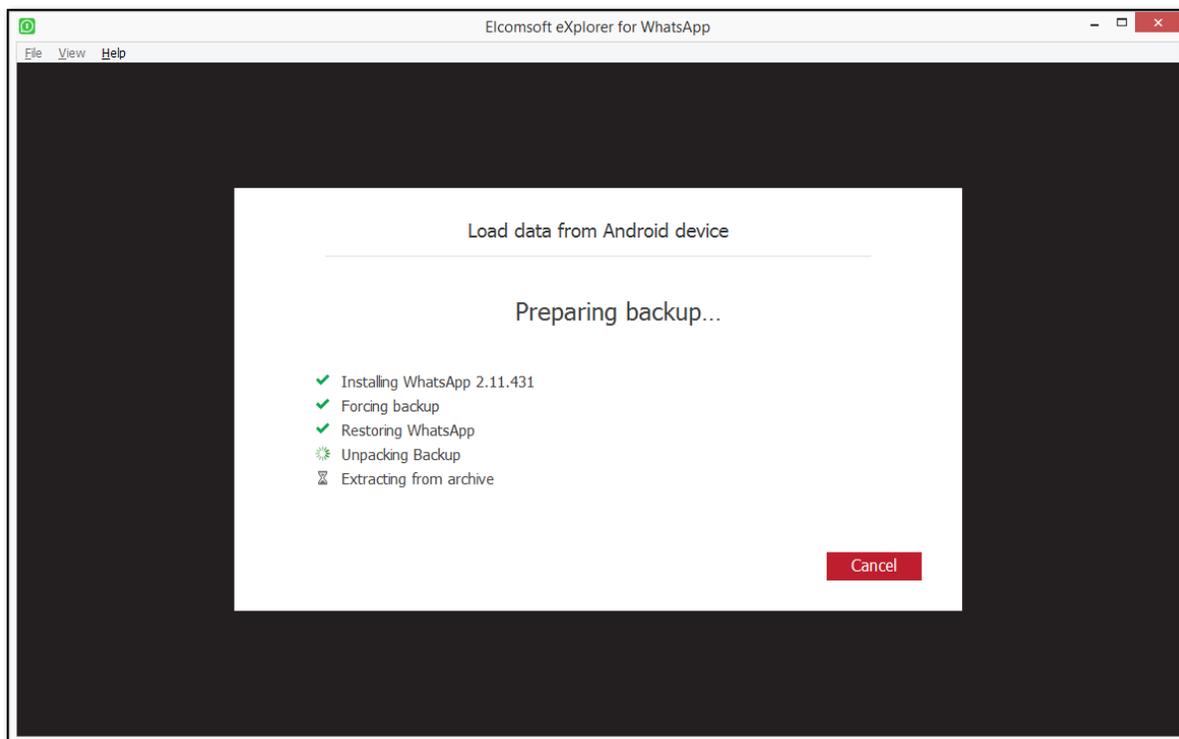
Tap **Backup my data** on the device. If the button is not active, type in 'pass123' in a password field and then tap **Backup my data**.



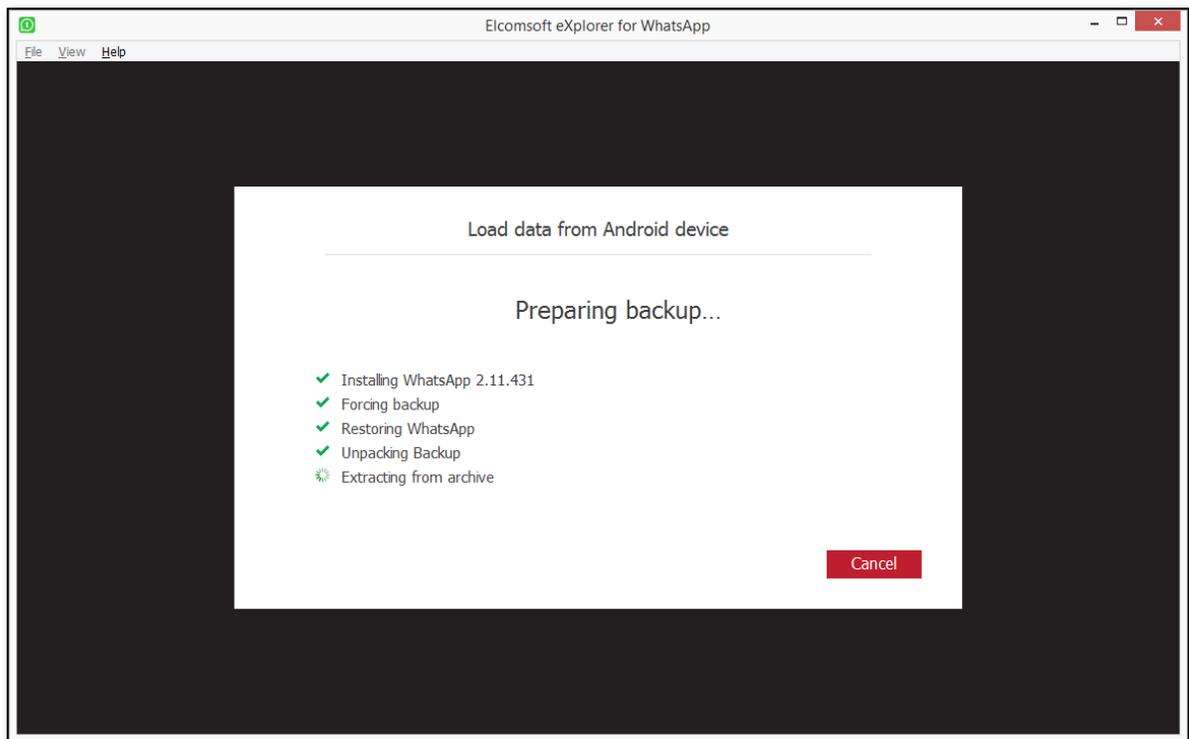
- **Restoring WhatsApp.** If the ES File Explorer dialog appears on the device, tap **Cancel**.



○ **Unpacking Backup.**

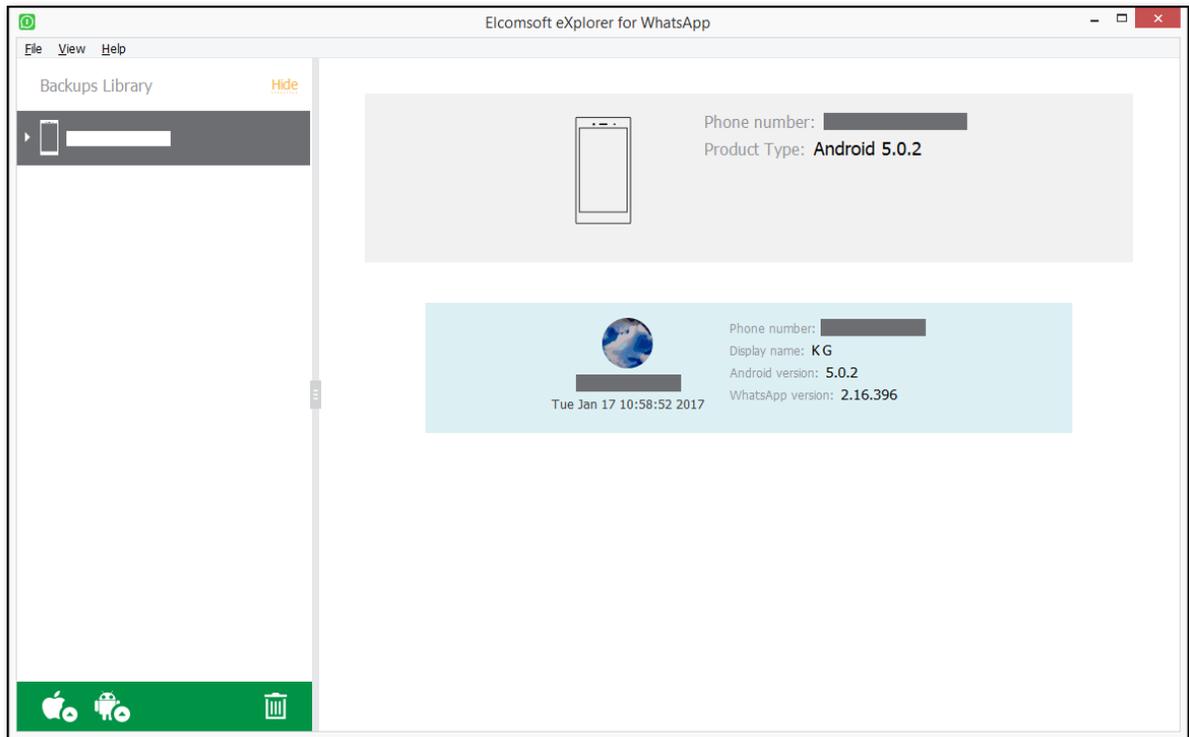


○ **Extracting from archive.**



11. Once the backup is loaded and WhatsApp/WhatsApp Business data is processed, the following information about the device is displayed:

- Phone number
- Product Type (Android version)



The lower part of the window displays the userpic, phone number, and the backup date (according to the time zone and date format defined on the local PC) as well as the following WhatsApp information (some of it may not be available):

- Phone number
- Display name
- Status
- Google account
- Android version
- WhatsApp version

### Viewing data

When you select the target WhatsApp or WhatsApp Business backup in the Backups Library, the lower part of the window displays all plugins available (some of them might be disabled if there is no appropriate information in backup):

- [Calls](#)
- [Contacts](#)
- [Media](#)
- [Messages](#)
- [Account info](#) (WhatsApp Business only)

Click the plugin icon to view the contents.

### Exporting data

EXWA allows you to export data from a backup to your PC. Data is exported to an XLSX file, and all attachments/files are saved to a folder in the same location as the XLSX file.

Please note that data export is only available in the registered version of the program.

To export data, do the following:

1. In the **Data View** pane, click **Export data**.
2. Select the data categories to export.
3. Define the time interval for which you want to export data as follows: enable filters by switching the On/Off toggle and then select the dates in the From and Until fields.
4. Click **Export**.
5. The window will open in which you can select the location for exported data.
6. Once you select the location, click **Save**.
7. Data export will start.
8. To open exported data, click the icon next to the **Data has been exported** message highlighted in yellow or open it from the location to which it was saved.

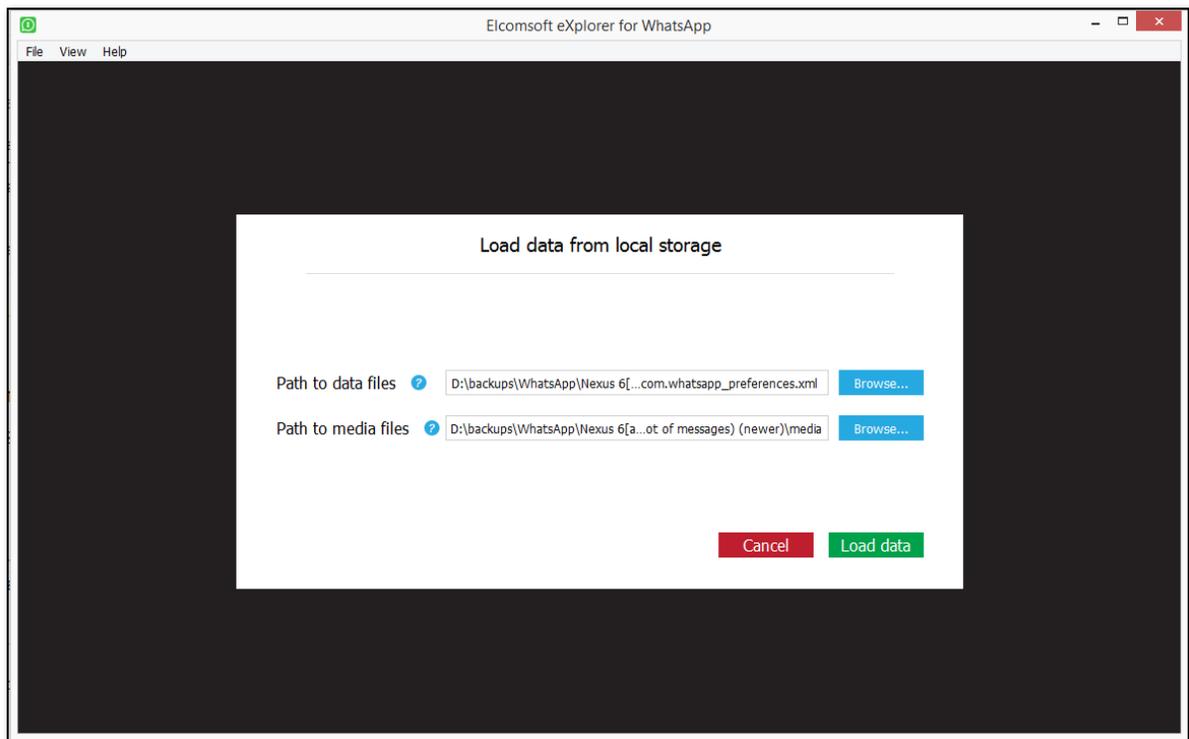
## 6.3.5 Working with Android data from local storage

### Adding Android data from local storage

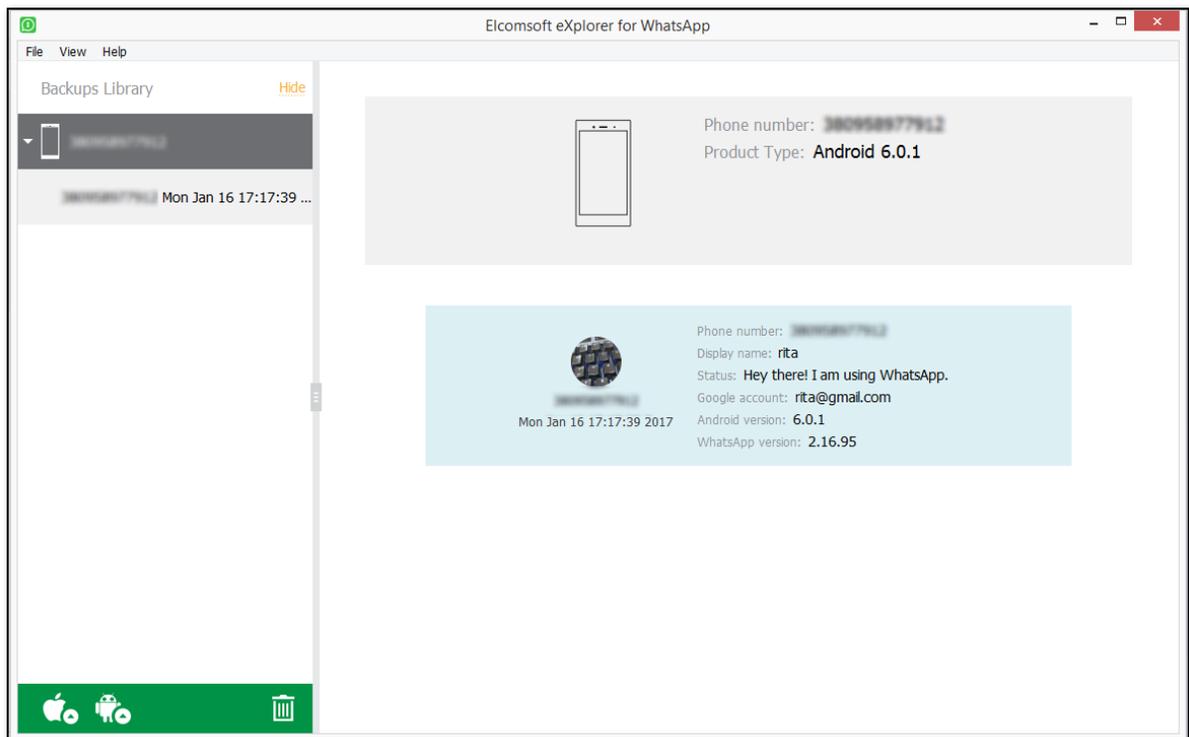
To start working with local Android backups:

1. In the Backups Library pane, click the **Acquire data for Android device** icon .
2. In the opened menu, click the **Load from local storage** icon .
3. In the opened window, specify the path to the **com.whatsapp\_preferences.xml** (for WhatsApp) or **com.whatsapp.w4b\_preferences.xml** (for WhatsApp Business) file in the **Path to data files** field.

Specify the path to the **Media** folder in the **Path to media files** field.



4. Click **Load data**.
5. Once the backup is loaded, the following device information is displayed:
  - Phone number
  - Product type (Android version)



The lower part of the window displays the userpic, phone number, and the backup date (according to the time zone and date format defined on the local PC) as well as the following WhatsApp information (some of it may not be available):

- Phone number
- Display name
- Status
- Google account
- Android version
- WhatsApp version

### Viewing data

When you select the target WhatsApp backup in the Backups Library to the left, the lower part of the window shows all plugins available (some of them might be disabled if there is no appropriate information in backup):

- [Calls](#)
- [Contacts](#)
- [Media](#)
- [Messages](#)
- [Account info](#) (WhatsApp Business only)

Click the plugin icon to view the contents.

### Exporting data

EXWA allows you to export data from a backup to your PC. Data is exported to an XLSX file, and all attachments/files are saved to a folder in the same location as the XLSX file.

Please note that data export is only available in the registered version of the program.

To export data, do the following:

1. In the **Data View** pane, click **Export data**.
2. Select the data categories to export.
3. Define the time interval for which you want to export data as follows: enable filters by switching the On/Off toggle and then select the dates in the From and Until fields.
4. Click **Export**.
5. The window will open in which you can select the location for exported data.
6. Once you select the location, click **Save**.
7. Data export will start.
8. To open exported data, click the icon next to the **Data has been exported** message highlighted in yellow or open it from the location to which it was saved.

## 6.3.6 Working with data from Google Drive

### Adding data from Google Drive

To start working with Google Drive data:

1. In the Backups Library pane, click the **Acquire data for Android device** icon .
2. In the opened menu, click the **Download from Google Drive** icon .
3. In the opened window, enter your Google account ID and password, or use an [authentication token](#). Click **Sign in**.

### Download data from Google Drive

---

Google ID  (example@example.com)

Password  

 **Important:** If the account uses 2FA and you log on with the password, a verification code will be requested on the next step. It will be sent by SMS immediately once you click Sign In. Google Authenticator or Backup verification codes can be also used.

Save credentials for future use 

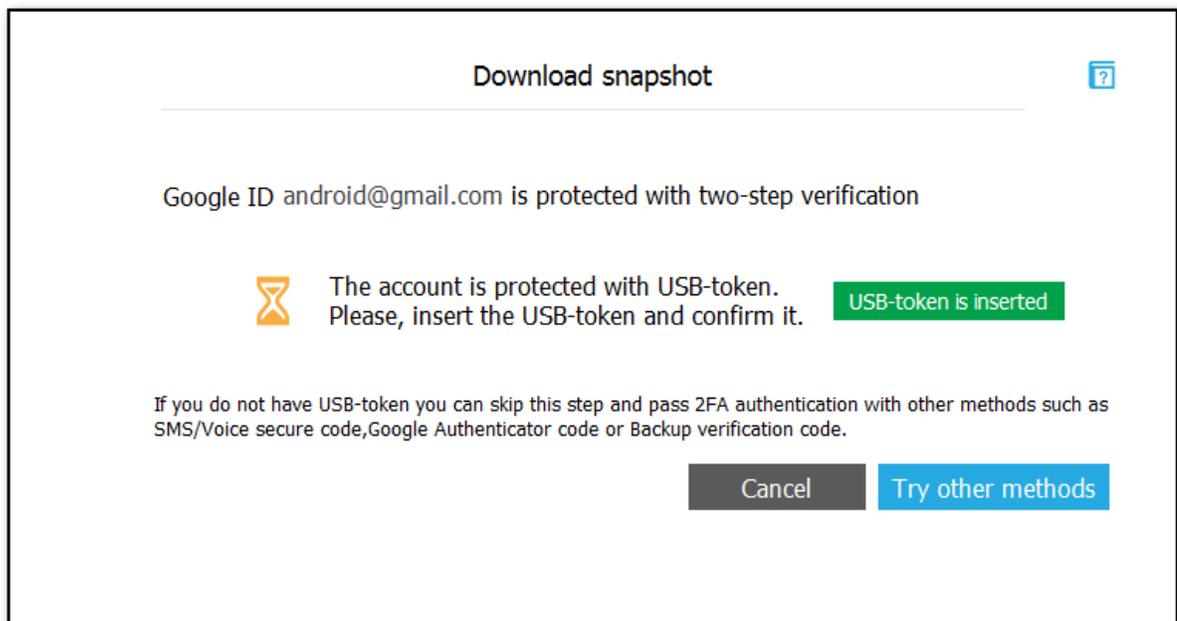
Use token instead of password (if available) 

**NOTE: EXWA doesn't support Google accounts with CAPTCHA protection. You can wait for a while until CAPTCHA protection is turned off and then try to log in again.**

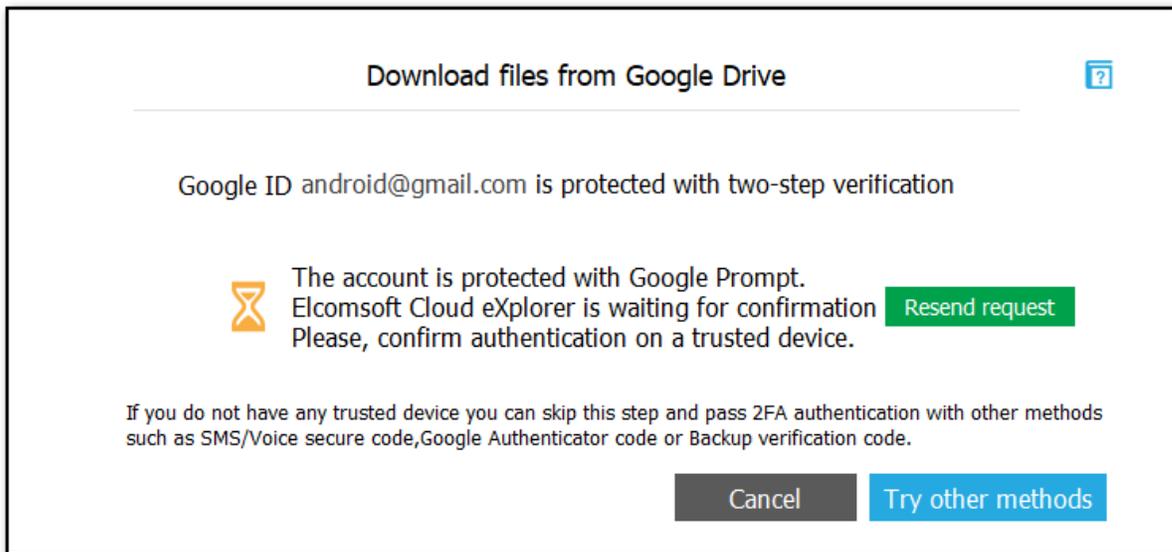
Some Google accounts require two-step verification, which means they are protected with the password and one of the following additional methods (depending on the method defined as default in the Google account security settings):

- USB-token.
- Google Prompt notification sent to the trusted device.
- A code sent to the trusted phone number in SMS text message.
- A code generated in the [Google Authenticator](#) application.
- One of backup verification codes available on the Google Accounts Overview page (for more information, please see <https://support.google.com/accounts/answer/1187538?hl=en>).

4. If your Google account is protected with USB-token, insert the USB-token and click **USB-token is inserted**.

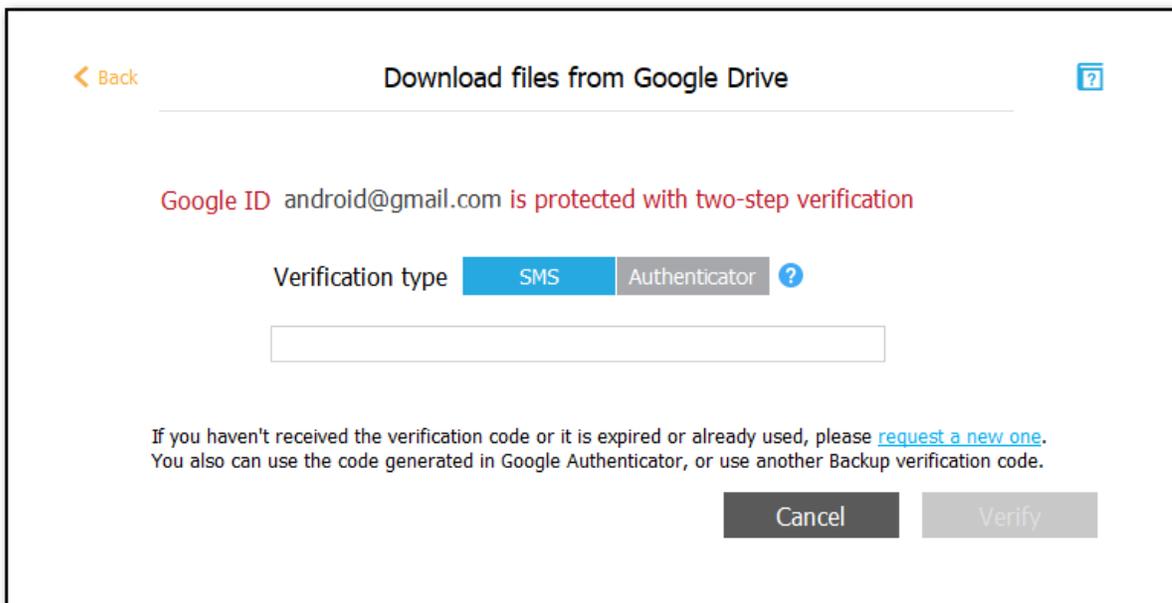


5. If your Google account is protected with Google Prompt, the Google application on your device will send you a notification to confirm that you are trying to sign in. If you haven't received the notification, click the **Resend request** link to get a new one.



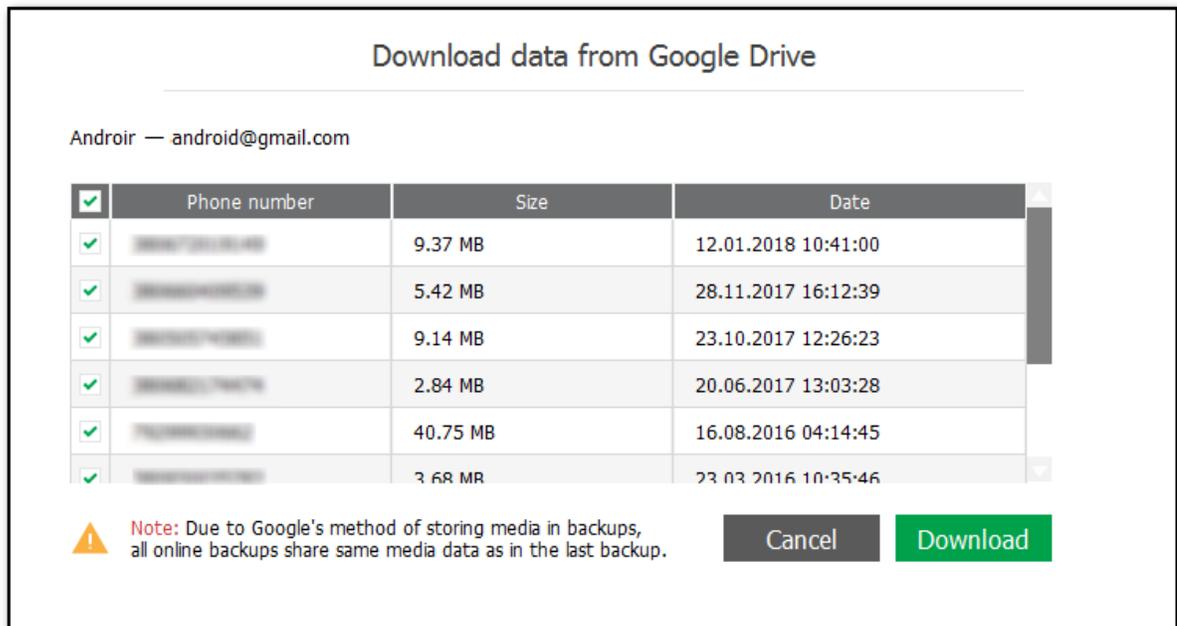
If your Google account is protected with other methods, you will be required to enter the secure code or the backup code after you click **Sign in**.

6. For other authentication types, select the corresponding tab, enter the code, and click **Verify**:



- **SMS:** The code will be sent to the trusted phone number. If you haven't received the code to the phone number, click the **request a new one** link to get a new one.
- **Authenticator:** The secure code generated in Google Authenticator every 24 seconds. If you fail to sign in, it means the code may have expired. Try signing in with a new generated code.
- **Backup verification code:** The backup verification codes available on the Accounts overview page. You can use each code only once. If you fail to sign in, it means the code was probably used. Try signing in with another code. If all of the available codes are invalid, generate new codes on your Google account settings page.

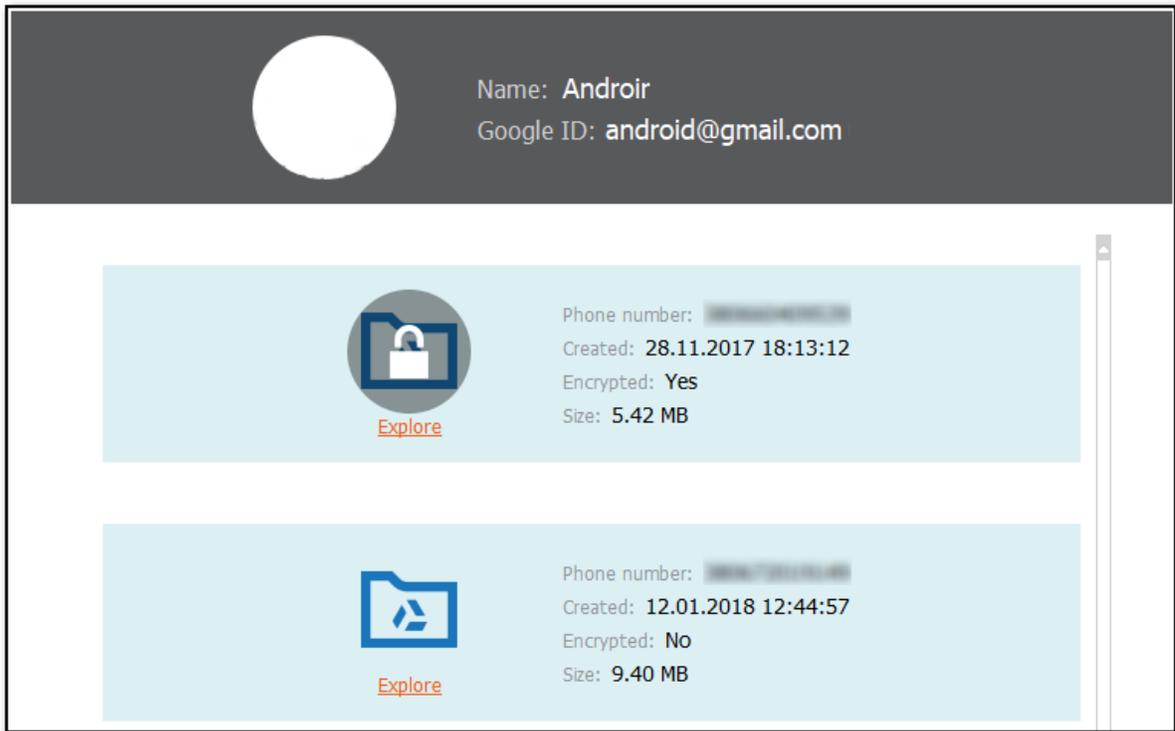
7. In the opened window, select WhatsApp and WhatsApp Business account backups you want to download. Click **Download**.



**NOTE:** When backing up data from WhatsApp and WhatsApp Business accounts sharing the same phone number to Google Drive, only the last backup is saved. If you backup data from WhatsApp and WhatsApp Business accounts that have different phone numbers, there will be two separate backups.

8. Once the backup is loaded, the following account information is displayed:

- Name
- Google ID



The lower part of the window displays the phone number, created date, indicates whether the backup is encrypted or not, and size of the backup.

### Viewing data

To view backup data, click **Explore** or select the target WhatsApp or WhatsApp Business backup in the Backups Library to the left, the lower part of the window shows all plugins available (some of them might be disabled if there is no appropriate information in the backup):

- [Calls](#)
- [Contacts](#)
- [Media](#)
- [Messages](#)
- [Account info](#) (WhatsApp Business only)

Click the plugin icon to view the contents.

### Exporting data

EXWA allows you to export data from a backup to your PC. Data is exported to an XLSX file, and all attachments/files are saved to a folder in the same location as the XLSX file. Please note that data export is only available in the registered version of the program.

To export data, do the following:

1. In the **Data View** pane, click **Export data**.
2. Select the data categories to export.

3. Define the time interval for which you want to export data as follows: enable filters by switching the On/Off toggle and then select the dates in the From and Until fields.
4. Click **Export**.
5. The window will open in which you can select the location for exported data.
6. Once you select the location, click **Save**.
7. Data export will start.
8. To open exported data, click the icon next to the **Data has been exported** message highlighted in yellow or open it from the location to which it was saved.

### Working with encrypted Google Drive backups

Encrypted backups are labeled with a black  icon in the backup list and a special "lock" element in the backup info panel.

Please note that decrypting Google Drive backups is only available in the registered version of the program.

To view an encrypted backup:

1. Select the target encrypted backup or click **Explore**. A message will be displayed:



2. Make your choice:
  - Click **Open** to get an immediate access to the backup (but only **Media** and **Contacts** data will be available to view).
  - Click **Decrypt** to decrypt the backup for a full access to the backup data.
3. If you select to decrypt the backup, the following dialog is displayed:

### Decrypt backup

---

Decrypt with SMS Keychain dump ?

Phone number

Verification code  [Resend code](#) 00:01:04

⚠ **Note:** you will be logged out of WhatsApp on your device. To continue using WhatsApp on your device, you will have to sign in again after obtaining the key with the program.

Cancel Decrypt

Click **Send code** to get a special registration code that will be sent to the device associated with the backup.

If you did not receive the code or it expired, click **Resend code**. A special timer shows when it will be possible to get a new code sent.

Once you receive the code, enter it in the **Verification code** field and click **Decrypt**.

The EXWA application will authenticate itself with WhatsApp and the current user will be logged out of WhatsApp on the device.

**NOTE: Do not click the URL in the message with the secure code. You have to enter the secure code manually, otherwise EXWA will not be authenticated with WhatsApp and you will have to wait for a while until a new code is sent.**

4. Once EXWA is authenticated with WhatsApp, the decryption process starts.

Please note that you have to enter the verification code every time you decrypt the Google Drive backup.

Decrypted backups are labeled with a black  icon in the backup list.

## 6.4 Plugins

### 6.4.1 Account info

This plugin is available only for WhatsApp Business backups.

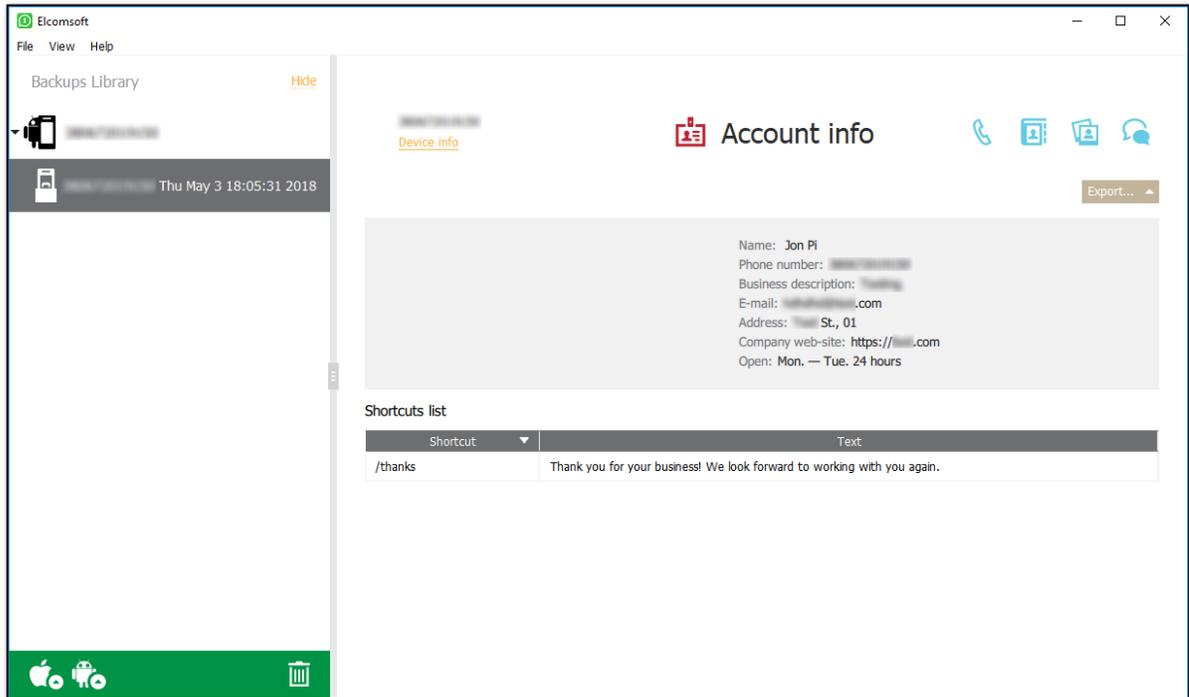
The following account information is displayed:

- Name
- Phone number
- Business description
- Email
- Company web-site
- Address

- Open (business hours)

The Account info plugin also displays the following information:

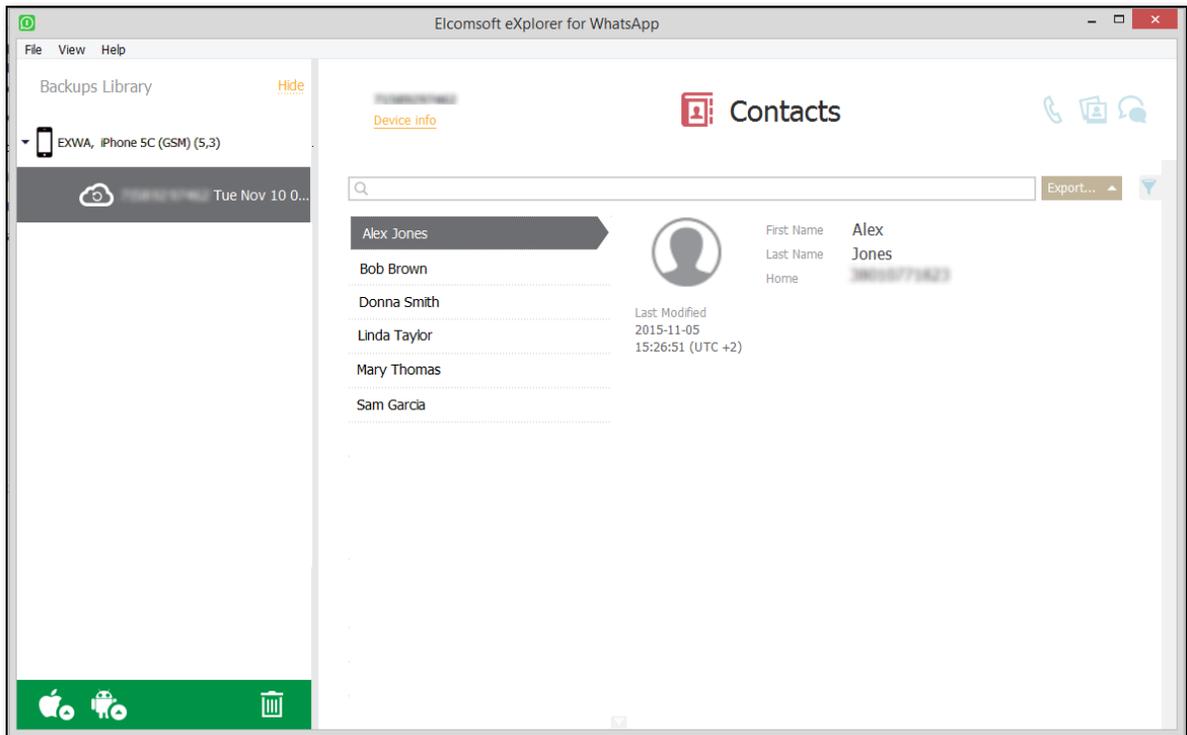
- **Shortcuts list:** A table displaying a list of user's shortcuts (quick reply messages).
- **Automatic replies:** A table displaying a list of automatic reply messages.



To copy the account data in **Account info**, right-click the target value and select **Copy full**.

## 6.4.2 Contacts

This plugin shows all the contacts included into the backup (which may include not just the local device address, but also the contacts from the accounts: Exchange/Outlook, iCloud, Google etc, if synced with the device). Select the contact on the left, and all the information that is available for it will be shown on the right.



The general information about the contact is usually the following:

- Contact photo/image/userpic
- Last modified date and time
- First and last name
- Phone numbers
- Status text

Additional information can be displayed for contacts with business accounts:

- Address
- Business account
- Business description
- Company website
- Email

**NOTE: Additional information about contacts with business accounts is available only for backups loaded from Android rooted devices and local storage.**

### Searching and Filtering

To perform searches in **Contacts**, enter the necessary data in the searching field and press **Enter**. The found results will be highlighted in yellow.

To filter out the contacts by accounts and groups, open the **Filter** pane by clicking the  icon on the left.

Enable filtering by switching the On/Off toggle and select the **Show only favorite** check box to filter the contacts marked as favorite or **Show only business** (for WhatsApp Business backups only) to filter the contacts marked as business.

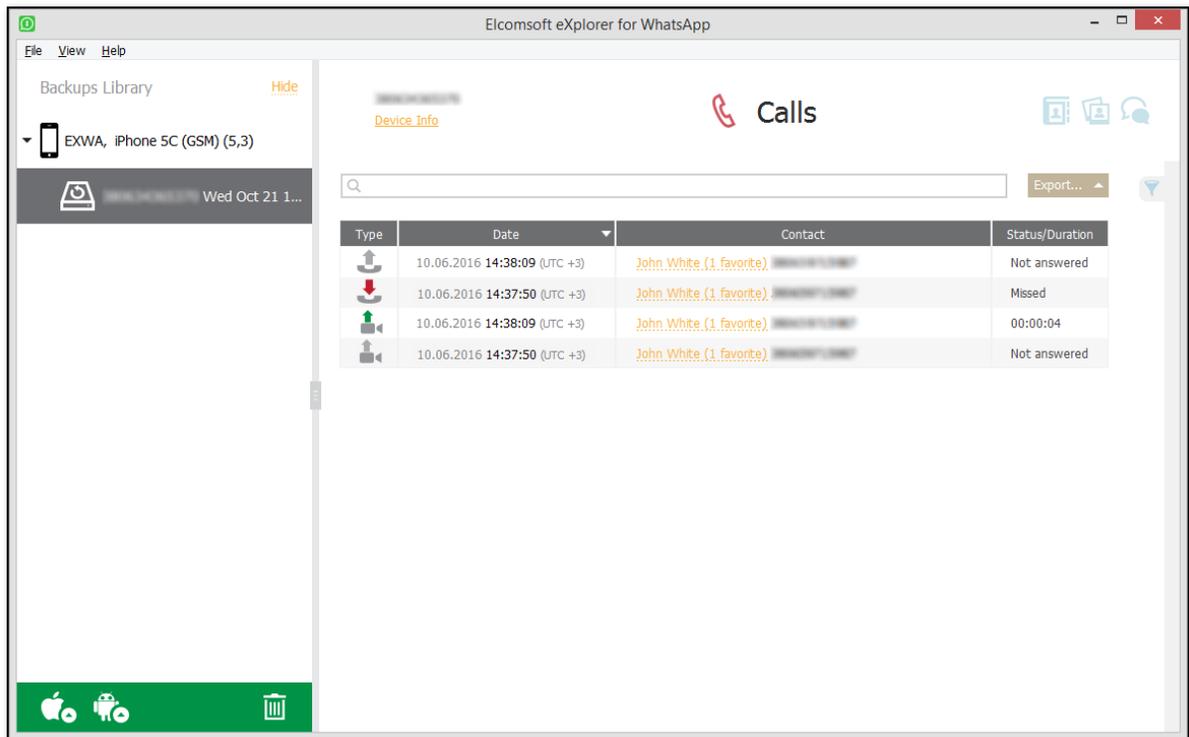
**NOTE: Ability to filter contacts marked as business is available only for backups loaded from Android rooted devices and local storage.**

To copy text, click the area where the text is to be copied from, highlight the text, right-click and select **Copy** or **Select All**.

### 6.4.3 Calls

EXWA allows you to explore the call history of the WhatsApp account under investigation. You can simply analyze the full history of outgoing/incoming/missed/not answered audio and video calls. The following call properties are available:

- Icon (to indicate the call type; both audio and video calls are supported)
- Date and time (according to the time zone and date format defined on the local PC)
- Phone number and information about a contact from the [Contacts](#)
- Status/Duration: for answered incoming and outgoing calls the duration is available for analysis; or just *Missed* or *Not Answered*.



### Searching and Filtering

To perform searches in **Calls**, enter the necessary data in the searching field and press **Enter**. The found results will be highlighted in yellow.

To filter out calls, the data by date, direction, and status, click the icon to the right.

Enable filtering by switching the On/Off toggle, and define the filtering options:

- **Date:** filters the calls by date. Select the year in the drop-down list below and define the time interval by moving the slider on the scale with names of months.

- **Direction:** filters the calls by direction (incoming or outgoing).
- **Status:** filters the calls by the status (answered, not answered, or missed).

To copy the contact data in **Calls**, right-click the target contact and select **Copy**. To copy a part of the contact data, click the area where the text is to be copied from, highlight the text, right-click and select **Copy** or **Select All**.

#### 6.4.4 Media

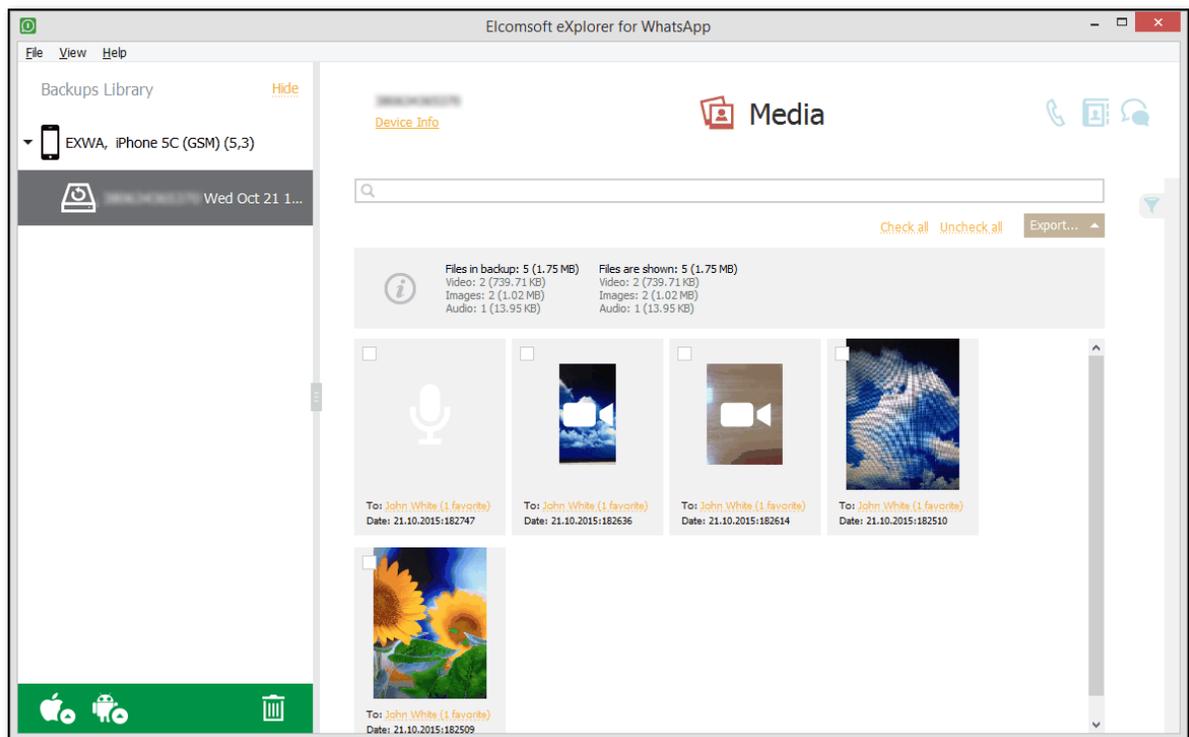
This plugin displays all multimedia data sent in WhatsApp chats, including images, videos (starting with WhatsApp 2.12.7), and audio files. You can also view the media sent by a certain contact in the [Messages](#) plugin.

General information about media files includes:

- Total number of files in backup and the number of files displayed.
- The number of video, image, and audio files in backup and currently displayed. You can also view the size of all files in each category.

All existing media is displayed as thumbnails. The general information about the media file displayed is:

- The number of the receiver.
- Date and time the object was sent (according to the time zone and date format defined on the local PC).



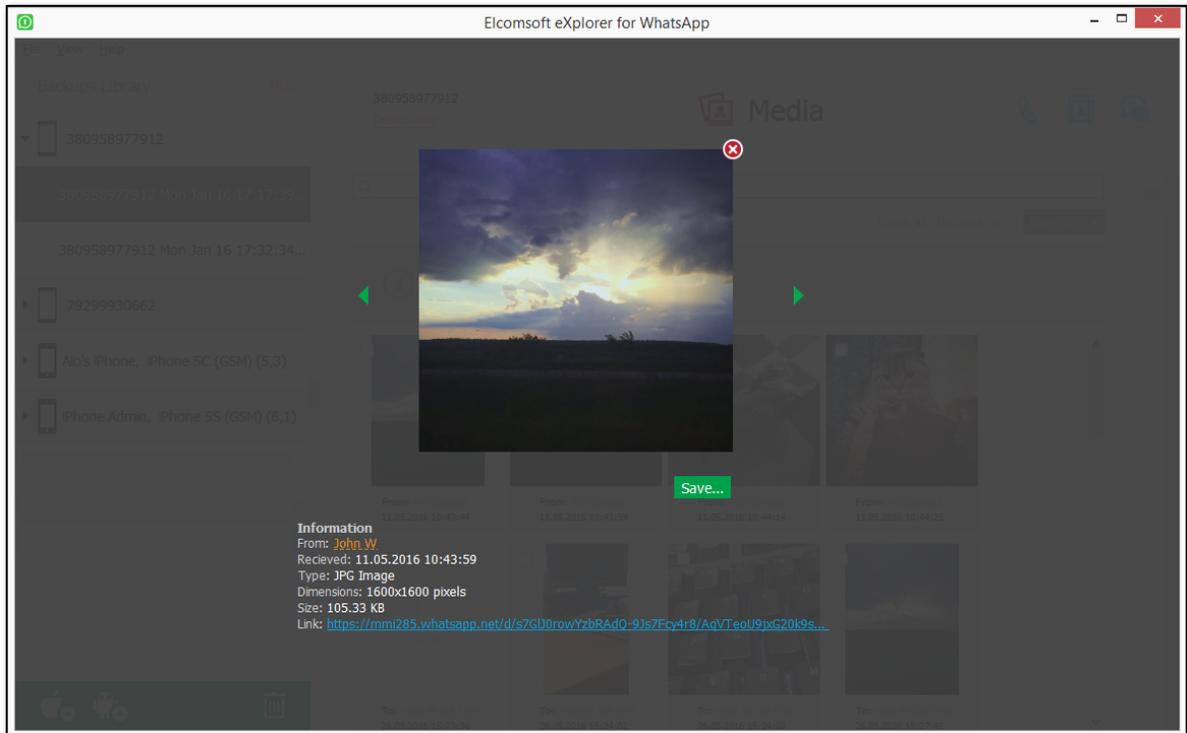
To export media objects, check them and click **Export**. It is possible to export checked media files, filtered files or all files.

#### Viewing Media Files

To view a certain media file, click it in the grid. The file opens in the viewer where you can also view its properties:

- **From:** The contact name or the phone number the media was sent from.
- **Received:** Date and time the file was received (according to the time zone and date format defined on the local PC).
- **Type:** File type.
- **Dimensions:** The image size in pixels.
- **Size:** The size of the file in KB.
- **Link:** The link for downloading the file.

To save the file, click **Save** and select the destination location.



## Searching and Filtering

To perform searches in **Media**, enter the necessary data in the searching field and press **Enter**. The found results will be highlighted in yellow.

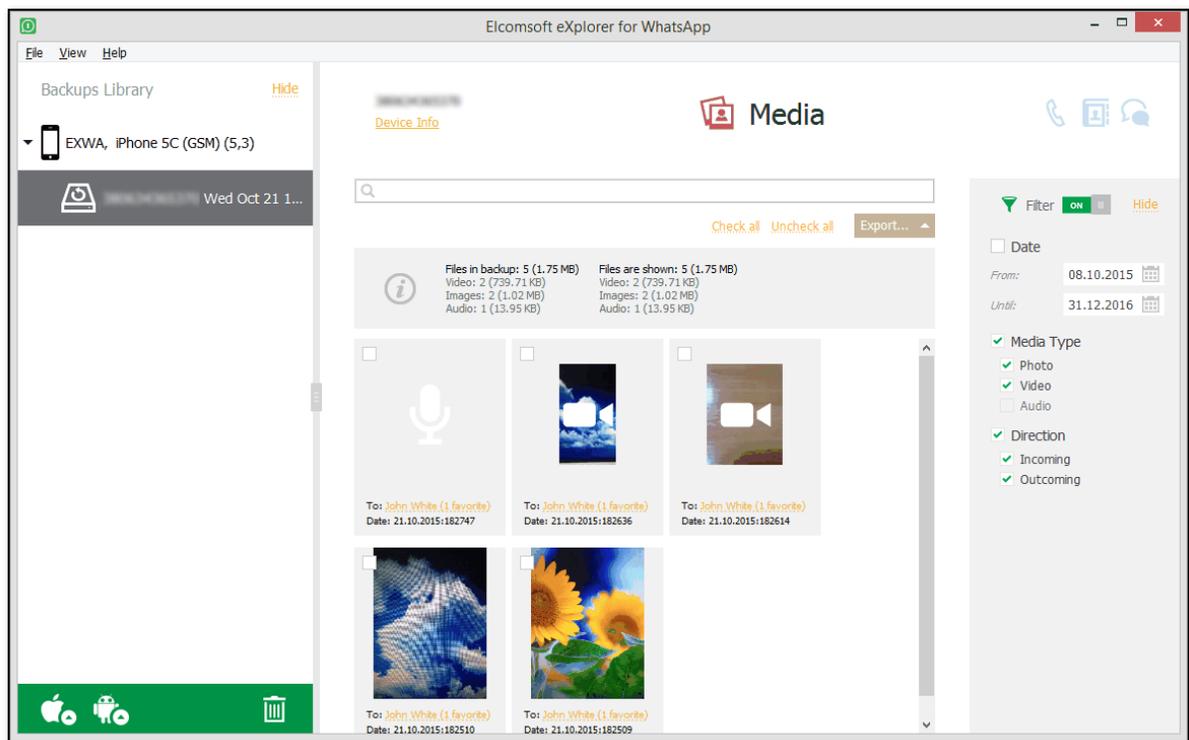
To filter out the media, open the **Filter** pane by clicking the  icon on the left.

**NOTE: Once you enable filtering, all previously checked files become unchecked.**

Enable filtering by switching the On/Off toggle and define the filtering options:

- **Date:** filters the media sent within a specific time period. Select the **From** and **To** dates in the respective drop-down lists.
- **Media Type:** filters the media by a media type (photo, video, and audio).
- **Direction:** filters media by direction (incoming or outgoing).

**Note: When using filter options, you will be able to view only the number of records allowed by your license type.**



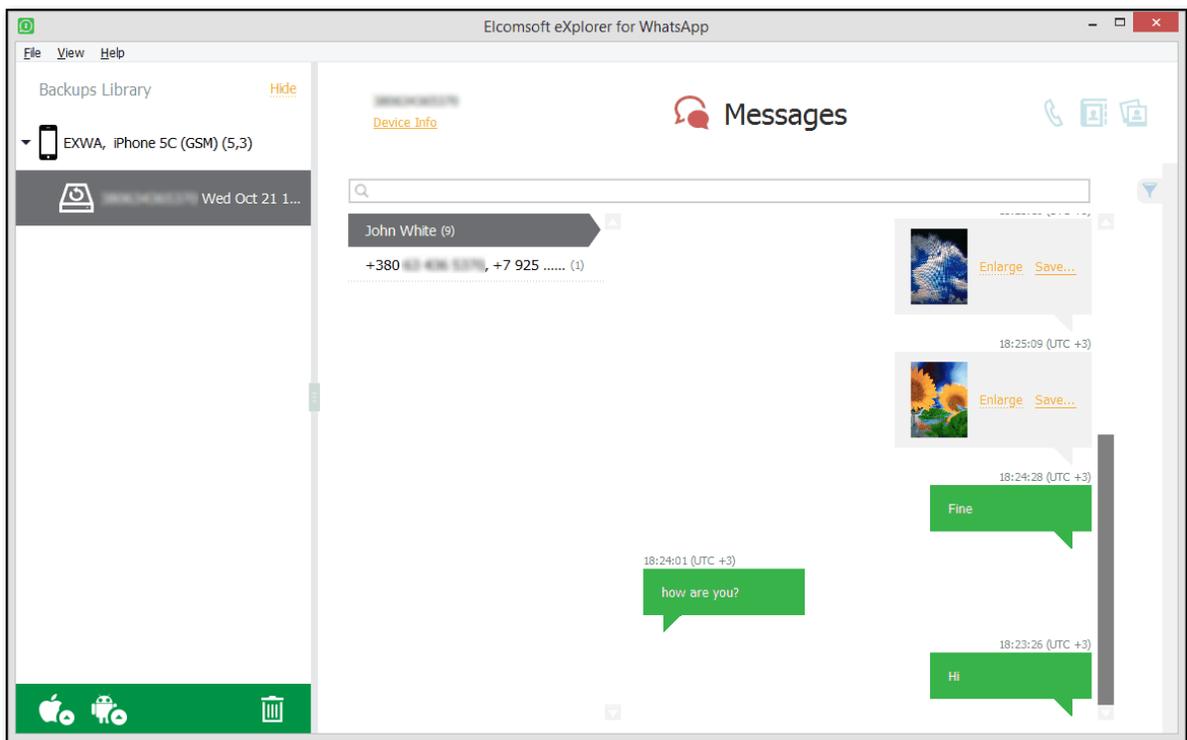
## 6.4.5 Messages

The left pane of the window displays the conversations as a list of contacts (phone number or name).

Incoming messages are shown on the left and outgoing messages are shown on the right. The number of messages for every contact is shown (in brackets). You can also view group and archived chats as well as system messages.

The emoji are displayed in both message texts and contacts.

In WhatsApp Business backups, messages and chats can be marked with label icons 🏷️. These are labels assigned by the user. Point to the label icon to view its name.



## Viewing attachments

You can view the message attachments of the following types: pictures, audio, video (starting with WhatsApp 2.12.7), contacts, and Google Maps locations.

To save the attachments to your computer, click **Save** next to the selected attachment, define the destination folder, and click **Save**.

**NOTE:** The current version of EXWA does not support viewing attached documents that were sent using the Share Document option in WhatsApp. You will be able to see the name of the document only.

## Searching and Filtering

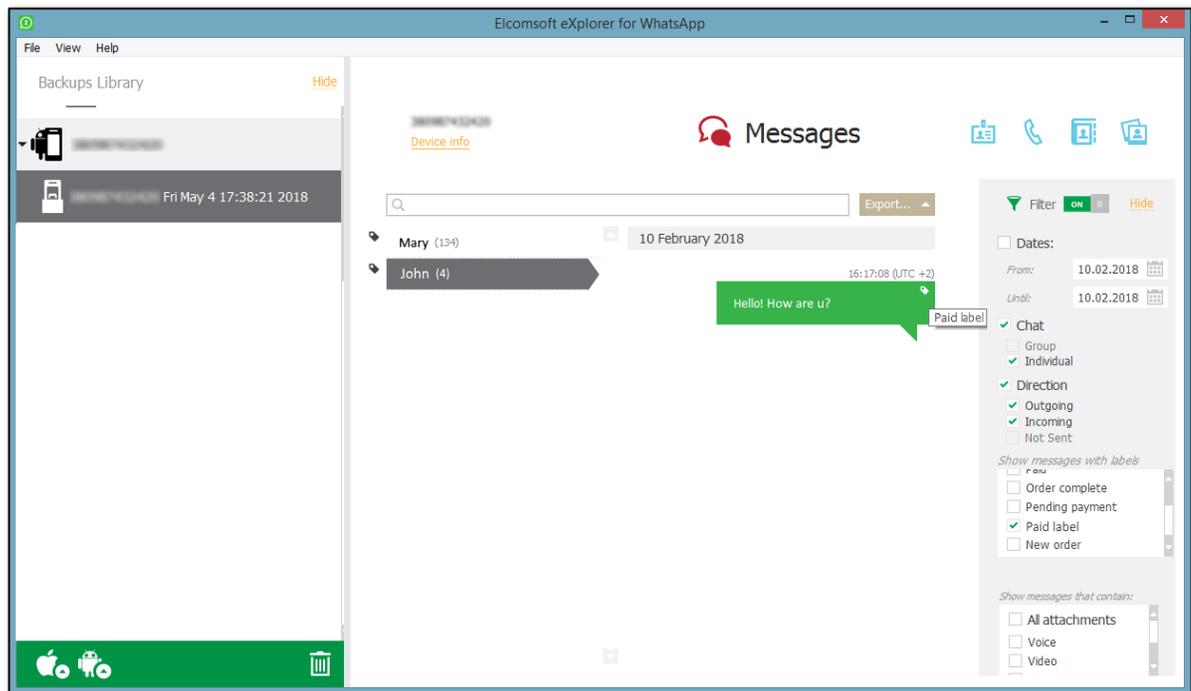
To perform searches in **Messages**, enter the necessary data in the searching field and press **Enter**. The found results will be highlighted in yellow.

To filter out the messages, open the **Filter** pane by clicking the  icon on the left.

Enable filtering by switching the On/Off toggle, and define the filtering options:

- **Date:** filters messages by date, then select the year in the drop-down list below and define the time interval by moving the slider on the scale with names of months.
- **Chat:** filters messages by chat type (individual or group).
- **Direction:** filters messages by direction (incoming or outgoing).
- **Show messages that contain:** filters messages by the attachment type (All Attachments/Audio/Video/Locations/Contacts/Images).
- **Show messages with labels** (available for WhatsApp Business backups only): filters messages by default and custom labels.

**NOTE: When using filter options, you will be able to view only the number of records allowed by your license type.**



To copy the whole message, right-click on it and select **Copy message**. To copy a part of the message, click the area where the text is to be copied from, highlight the text, right-click and select **Copy** or **Select All**.

## 7 Support & updates

### 7.1 Contacting us

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

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

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

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

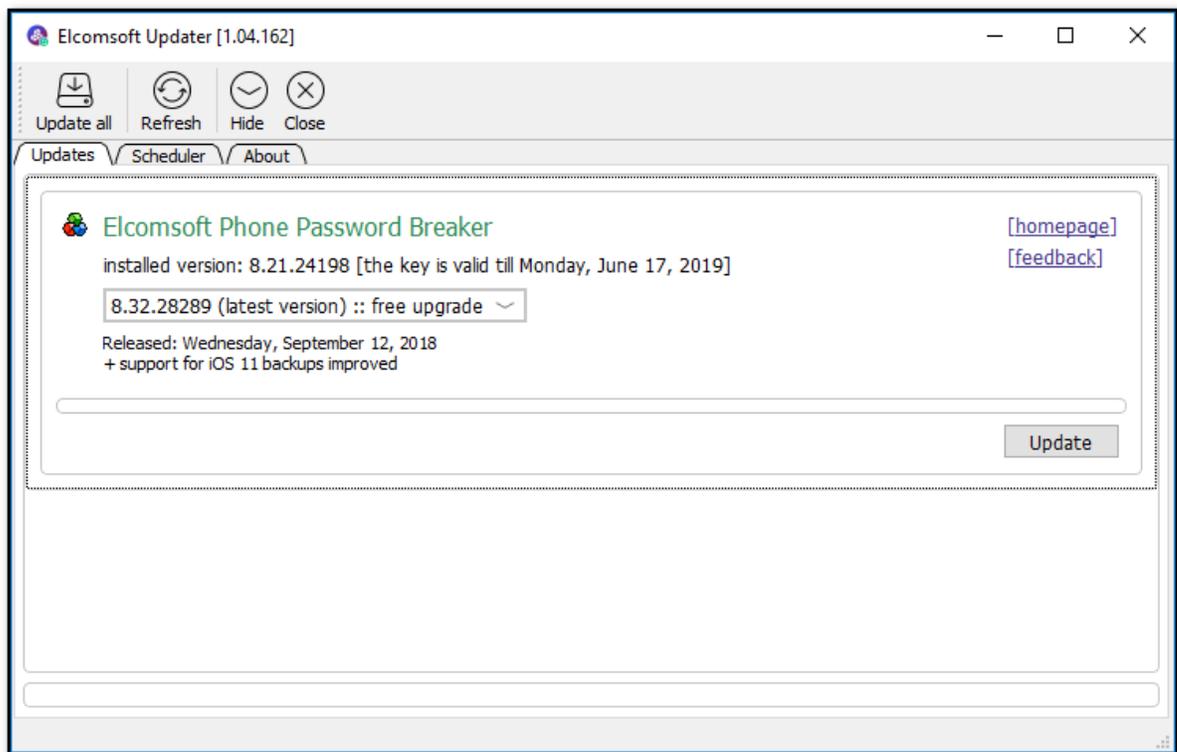
Latest version of all programs included into Mobile forensic Bundle is available at:

<https://www.elcomsoft.com/emfb.html>

### 7.2 Updating

You can check for available updates and install them yourself. Just do the following:

1. Launch **Elcomsoft Updater**.
2. On the **Updates** tab, find the program you have installed (for example, **Elcomsoft Phone Password Breaker**). If there is no such section, a new version is not available yet.
3. Select the program version from the list and click **Update**. The updating process starts.

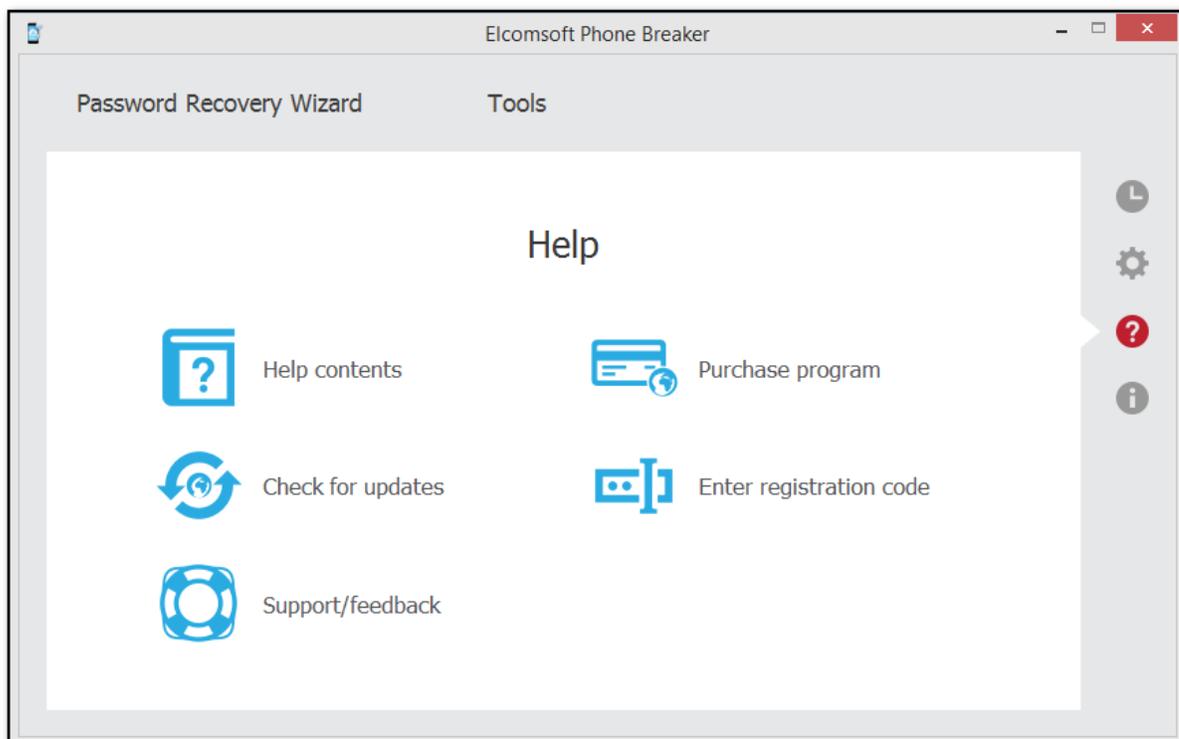


On **macOS**, only manual program update is available for now. For example, for **Elcomsoft Phone Breaker**:

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.

## 7.3 Registration

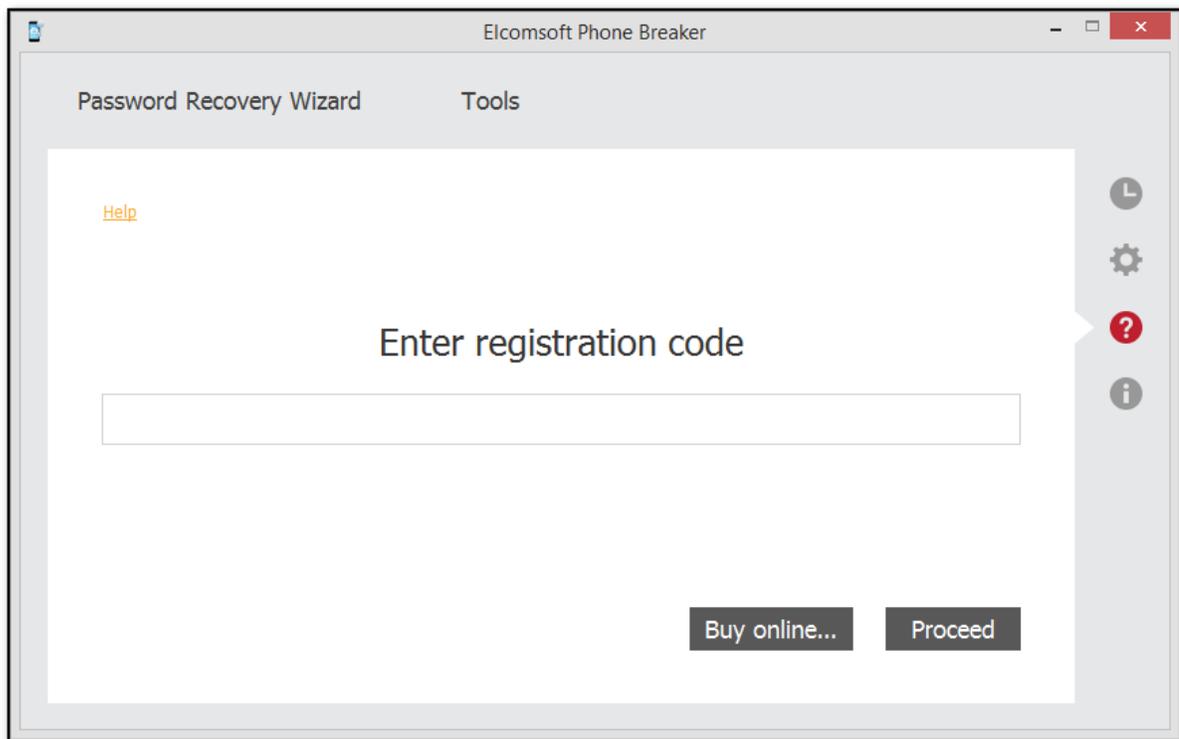
To place an order online, go to **Help - Purchase program.**, for example in Elcomsoft Phone Breaker:



Alternatively, you can purchase any product by clicking **BUY NOW** link on appropriate product page.

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.

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**:



## 7.4 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](mailto: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](mailto: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](mailto:legal@elcomsoft.com).

© 1998-2020 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.

## 7.5 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](mailto: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 ([ey@cryptsoft.com](mailto:ey@cryptsoft.com)). This product includes software written by Tim Hudson ([tjh@cryptsoft.com](mailto: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](mailto:jloup@gzip.org)  
Mark Adler [madler@alumni.caltech.edu](mailto:madler@alumni.caltech.edu)

#### **Copyright (c) 1996 - 2012, Daniel Stenberg, <[daniel@haxx.se](mailto: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.

**Copyright (c) 2015-2016, Apple 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:

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. Neither the name of the copyright holder(s) nor the names of any 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.

## 7.6 Troubleshooting

[Troubleshooting](#)