702 San Conrado Terrace, Unit 1
Sunnyvale CA 94085
USA and Canada: +1 650 272 0384
Web: https://belkasoft.com
Email: support@belkasoft.com

Belkasoft Evidence Center X User Reference

Table of Contents

About

What is this document about?

This document describes **Belkasoft Evidence Center X** (**Belkasoft X** a digital forensic software product developed by Belkasoft. The document describes Belkasoft X from a user's perspective; basic digital forensics principles as well as technical details of the product implementation are out of scope of this document.

If you would like to receive a better understanding of the product and digital forensics in general, please consider **Belkasoft official training** at https://belkasoft.com/training. An option to become a certified user is also available.
Note: screenshots of the product may vary from version to version, so your actual copy of Belkasoft X may look a bit different.

Other resources

You can find more information on Belkasoft X on our site at https://belkasoft.com:

- General info and technical specification: https://belkasoft.com/ec
- Video tutorials: https://belkasoft.com/tutorials
- What's new in the latest version: https://belkasoft.com/new
- Belkasoft customers: https://belkasoft.com/customers
- Customer testimonials: https://belkasoft.com/testimonials
- Sign up for a free webinar: https://belkasoft.com/webinar
- Request a quote: https://belkasoft.com/quote or contact sales@belkasoft.com
- Belkasoft articles on digital forensics: https://belkasoft.com/articles
- Learn more on Belkasoft training and certification programs: https://belkasoft.com/training
- Find a reseller in your region: https://belkasoft.com/partners or contact sales@belkasoft.com

You can always download a free trial version at https://belkasoft.com/trial (30-days limited version of **Belkasoft X**).

Legal notes and disclaimers

Introduction

What is Belkasoft Evidence Center (Belkasoft X) and who are its users?

Belkasoft Evidence Center X (further abbreviated as Belkasoft X) is Belkasoft's flagship digital forensic suite. The product makes it easy for an investigator to perform all steps of modern digital investigation including:

- Data acquisition from various devices and clouds
- Artifact extraction and recovery
- Analysis of extracted data
- Reporting
- Sharing evidence

The product supports the following types of digital forensics in a single user interface:

- Mobile forensics
- Computer forensics
- Memory (RAM) forensics
- Cloud forensics

Both high-level and low-level analysis can be done with Belkasoft X.
On a low-level, the product allows you to view raw data in files and databases using low-level viewers such as **File System**, **Hex Viewer**, **SQLite Viewer**, **Registry Viewer** and **Plist viewer**.
On a high-level, the product can automatically extract a so-called "Low hanging digital forensic fruit", meaning the hundreds of forensically important artifacts such as emails, documents, chats, and so on.

The product can also be used for Incident Response and has a specialized window for incident investigations.

Belkasoft X is used to conduct digital investigations, often in connection with an online or offline crime, data recovery, intelligence and counterintelligence. Typical Belkasoft X customers are:

- Police
- Federal investigative organizations
- RCFLs (Regional Computer Forensics Laboratories)
- CAC (Crimes Against Children) and ICAC (Internet Crimes Against Children) departments
- Government drug enforcement organizations
- Customs
- State post
- Military

Various private companies use the product for incident response. Private investigators employ Belkasoft X to assist in their investigations.

Types of tasks Belkasoft X is used for

Belkasoft X is a comprehensive product used for various types of investigation tasks. One can utilize it for:

- Conducting digital investigations in a criminal or civil case
- Incident response
- Low-level analysis for various types of files such as SQLite databases, Registries and so on
- Search for illicit pictures and videos
- Data recovery
- Surveillance
- and many other tasks where a digital device is involved, and it is needed to recover and analyze its contents

Typical Belkasoft X workflow

The standard product workflow is as follows:

- **Case creation**
- **Acquisition**
    - Acquiring a mobile device or a computer drive
    - Downloading cloud data
    - Creating RAM dump
- **Adding data source to the case**
    - Adding one or multiple dumps acquired by Belkasoft X
    - Adding image or dump created with tools
    - While conducting live forensics one can add a physical or network drive, including the drives inside write-blocker devices
- **Artifact extraction and review**
    - Out of the box recovery and artifact extraction for 1000 + various applications and formats
    - Search for files matching the specified hashset database
    - Carving of deleted data from allocated or unallocated space, RAM, slack space and so on, including carving by custom signatures
    - Bookmarking data of interest
- **Analysis**
    - Search for faces, guns, pornography, skin, texts on pictures
    - Link analysis and Communities detection inside Connection graph
    - Low-level analysis of databases and other files in **Hex Viewer**, **SQLite Viewer** and other low-level viewers
    - Locating data of interest inside indexed texts using keyword or GREP search
- **Reporting**
    - Creating report in multiple available formats such as HTML, PDF, Word, Excel and others
    - Exporting entire case or its contents to a portable case using **Evidence Reader** feature

Belkasoft X workflow in detail is described in the following chapters.

Forensically sound software

Belkasoft X sticks to all the guidelines and regulations that define forensically sound software.

- Belkasoft X never tries to write on a medium under investigation. Belkasoft X is fully compatible with write-blocking devices and image files
- Belkasoft X works under an investigator account on the investigator's machine. Belkasoft X does not require client applications—especially those used by an individual under investigation—to be installed. For example, to retrieve an Outlook mailbox, Belkasoft X does not require you to have Outlook installed on your computer
- Belkasoft X remains completely operational on offline computers—with a few exceptions, described below (see 'When Belkasoft X uses the internet')
    - Dongle-based licenses do not require an Internet connection for the activation
    - Electronic (fixed) licenses can be activated offline through another machine connected to the Internet

Note: The rules (above) apply to dead-box analysis.

When Belkasoft X uses the Internet

Belkasoft X is able to function without an Internet connection. When Belkasoft X does operate offline, some functions are unavailable. These are the defined and well-known cases when or for which Belkasoft X requires an Internet connection:

- When Belkasoft X starts, Windows automatically checks its code-sign certificate and initiates a standard OCSP call to find out whether the X.509 certificate is revoked. Windows is responsible for this process. The task is performed because Belkasoft X is signed with a known publisher certificate. When you block this connection, nothing bad happens
- To check memory processes and files with **VirusTotal**, Belkasoft X needs the Internet to access virustotal.com
- To view geolocations on **Open Street Maps**, Belkasoft X needs the Internet to connect to Open Street website involved
- To acquire cloud data, Belkasoft X needs the Internet to connect to the cloud server involved
- Analysis of **S3** buckets (for public cloud)
- Belkasoft X uses the Internet to check for updates—if you choose to check for updates automatically
- Belkasoft X uses the Internet for the one-time activation—when you first run the trial version or buy a product with a fixed license. The dongle license does not require the Internet for the activation
- When you click on a tutorial on the **Home** window, Belkasoft X sends the link to your web browser, which then loads the video on YouTube using your Internet connection

In general, at any time, you can configure your firewall to block connections for Belkasoft X or allow all or some of them. Alternatively, you can set up a disconnected virtual machine and run Belkasoft X inside it.

Why Belkasoft X?

There are a number of benefits using **Belkasoft X**, which make it the product of choice with customers in more than 100 countries worldwide. These benefits include:

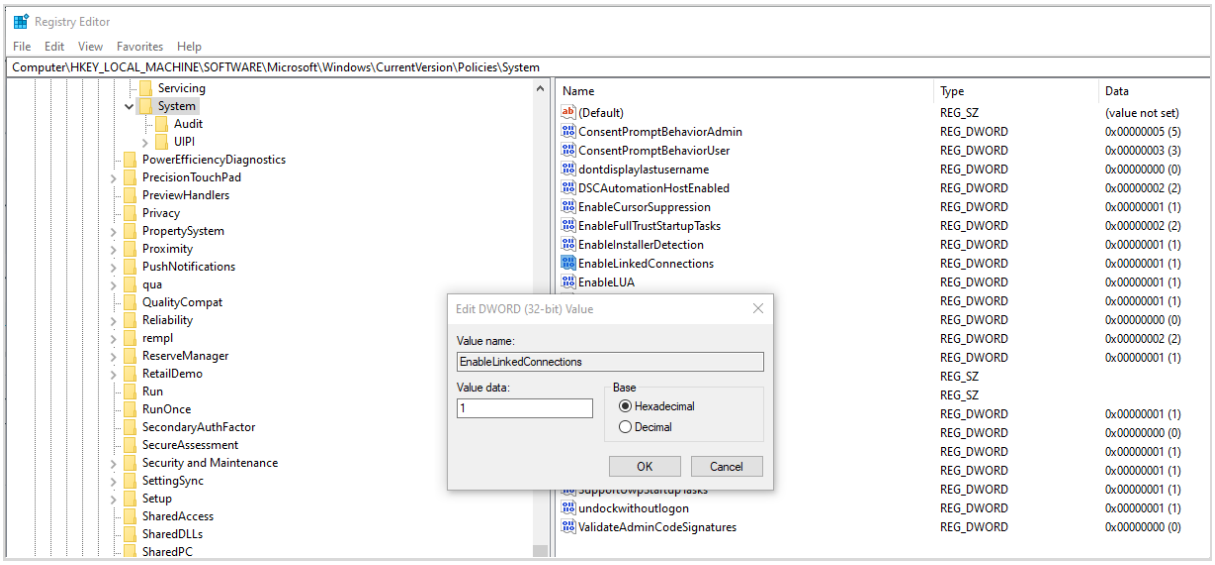
- **Belkasoft X supports both mobile and computer forensics** as well as remote forensics, RAM and cloud forensics
- **Belkasoft X recovers all available data.** Does not matter if data is still kept in files or deleted, hidden in unallocated or slack space, the product can easily reveal it by searching inside existing files, carving using file or record signatures, analyzing Volume Shadow Copy and many other forensically important areas (such as, for example, SQLite freelists)
- **Belkasoft X supports all stages of your investigation.** Starting from the acquisition phase, where the product helps you to copy a hard drive, create a smart mobile device dump, capture RAM memory and even download Google Drive or iCloud, through analysis, to the creation of reports in various formats. The product **simplifies** all routine operations of your investigation
- **Belkasoft X can extract 1000+ artifact types right out of the box.** Automatic application data extraction, which we call "Low hanging digital forensic fruit", can be enough to solve the vast majority of cases, where you are investigating internet communications, documents or photos. The product knows all popular (and even less known) apps, such as WhatsApp, WeChat, Wickr Me, Skype, Signal, major browsers and mail apps such as Outlook, office formats such as MS Word or Open Office Spreadsheet, so you do not have to know data formats, file locations, signatures for carving files or individual records, encryption schema, and so on. Moreover, the product will find data in all potential places, that is, not only in existing files, but also in Live RAM memory, pagefile or hibernation files, virtual machines, VCS snapshots, unallocated or slack space and so on
- **Belkasoft X is easy to use.** Getting first results using "low hanging fruit analysis" is easy as 1-2-3. There are only few things you need to do. These are:
    - Add device or dump to your case (or acquire it using built-in acquisition feature)
    - Select types of artifacts to look for
    - Enjoy reviewing found results!

  After the software finishes searching, all data will be conveniently presented in different perspectives: by file system location, by application profile and by type of data. Timeline will show you all events inside the device sorted by timestamp; bookmarks are used to mark important items; index-based search will find keywords, including GREP search and predefined search (e.g. credit cards, SSN numbers, MAC or IP addresses and so on). The product interface is so simple and intuitive that you can start using it right after the installation, without weeks of paid training that some other products require in order to operate effectively. Though training is always recommended
- **Advanced low-level analysis is available in Belkasoft X.** While in most cases automated extraction will be enough, investigations that are more complex may require manual analysis of devices in question. For such types of investigations, Belkasoft X provides the powerful File System Explorer, which shows all volumes and partitions inside the device, existing and deleted folders, VCS snapshots, existing and deleted files. Each partition or file can be reviewed in Hex Viewer, the window assisting you to investigate individual bytes, make automatic type conversions, create bookmarks, run custom carving and apply various encodings
- **Belkasoft X is much more cost-effective and overall a much better value.** The product offers more features for a lower price than most other products on the market. Not only does it save

you money at the moment of purchase, it also helps you save every year after that with its cost-effective priced renewals. Moreover, our free Evidence Reader allows you to share your work with your colleagues at absolutely no cost, thus saving you even more! Finally, Belkasoft X customers have a wide variety of discounts towards the purchase from our partners' digital forensic products.

Work with mapped drives

Belkasoft X is launched with elevated privileges under administrator's account. Mapped drives, therefore, are hidden when Windows Explorer is called from the product, even when current user's settings allow to show them. In order to work with mapped drives in such dialogs as 'Open folder', 'Open', 'Select a folder', 'Select the image target path' and similar, one can manually add a Windows registry entry. Do do this, open the **Registry editor** and go to:
HKEY_LOCAL_MACHINE/SOFTWARE/Microsoft/Windows/CurrentVersion/Policies/System.
Here create DWORD EnableLinkedConnections with value 1:



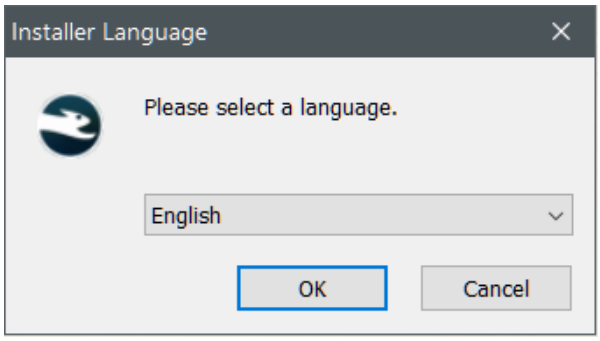
Quick Start

Installing Belkasoft X

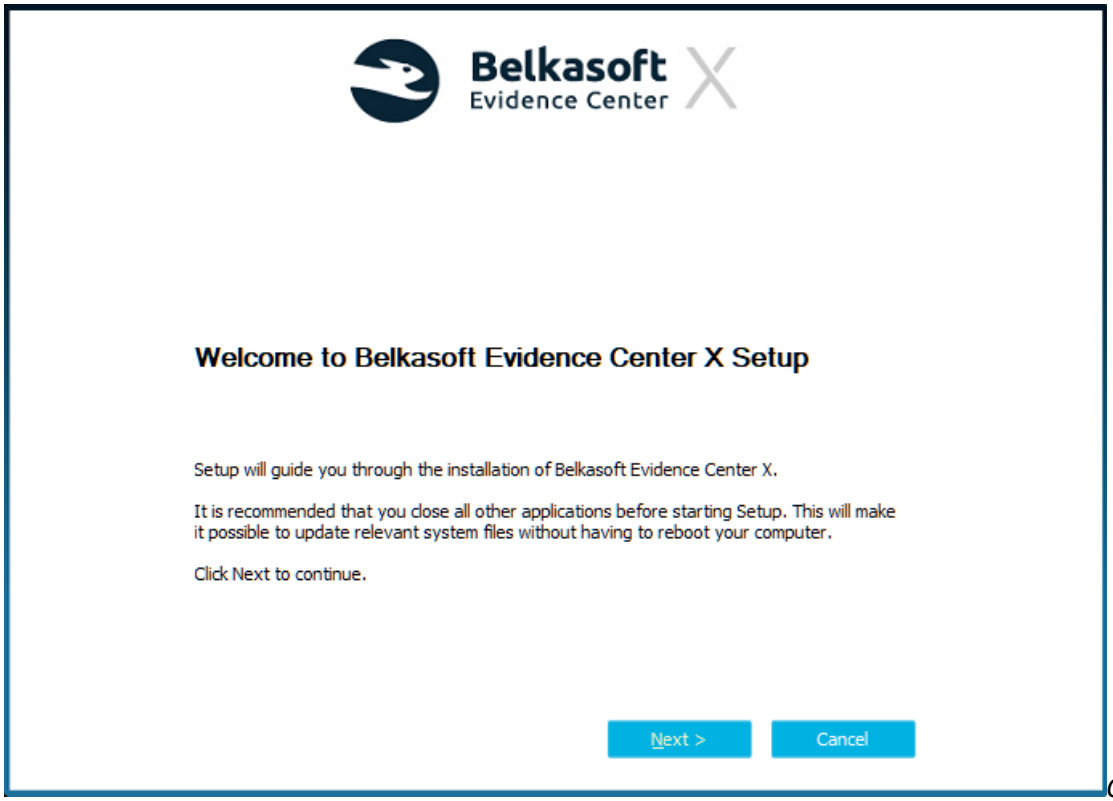
To install **Belkasoft Evidence Center X**, unpack the archive you downloaded from **Belkasoft site**.

Please don't install new version of Belkasoft X over the older version. We are recommended always install it in a new empty folder.

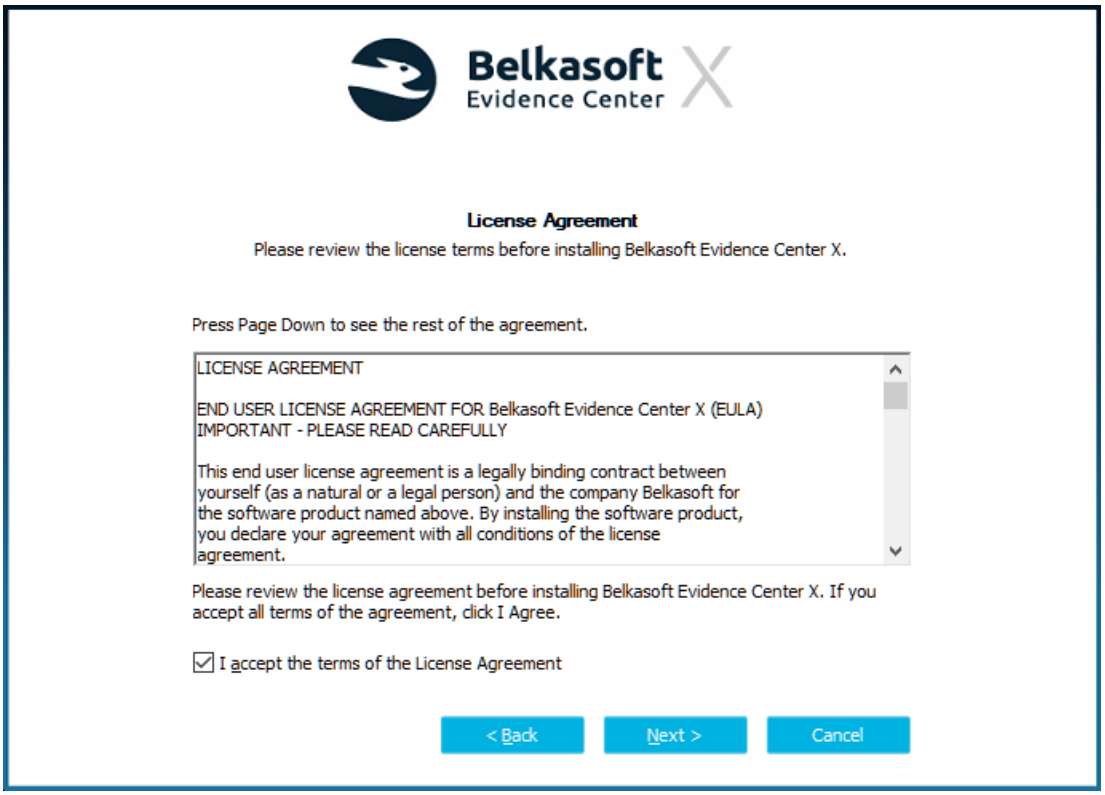
Run the executable file. The installation wizard will guide you through the installation procedure.



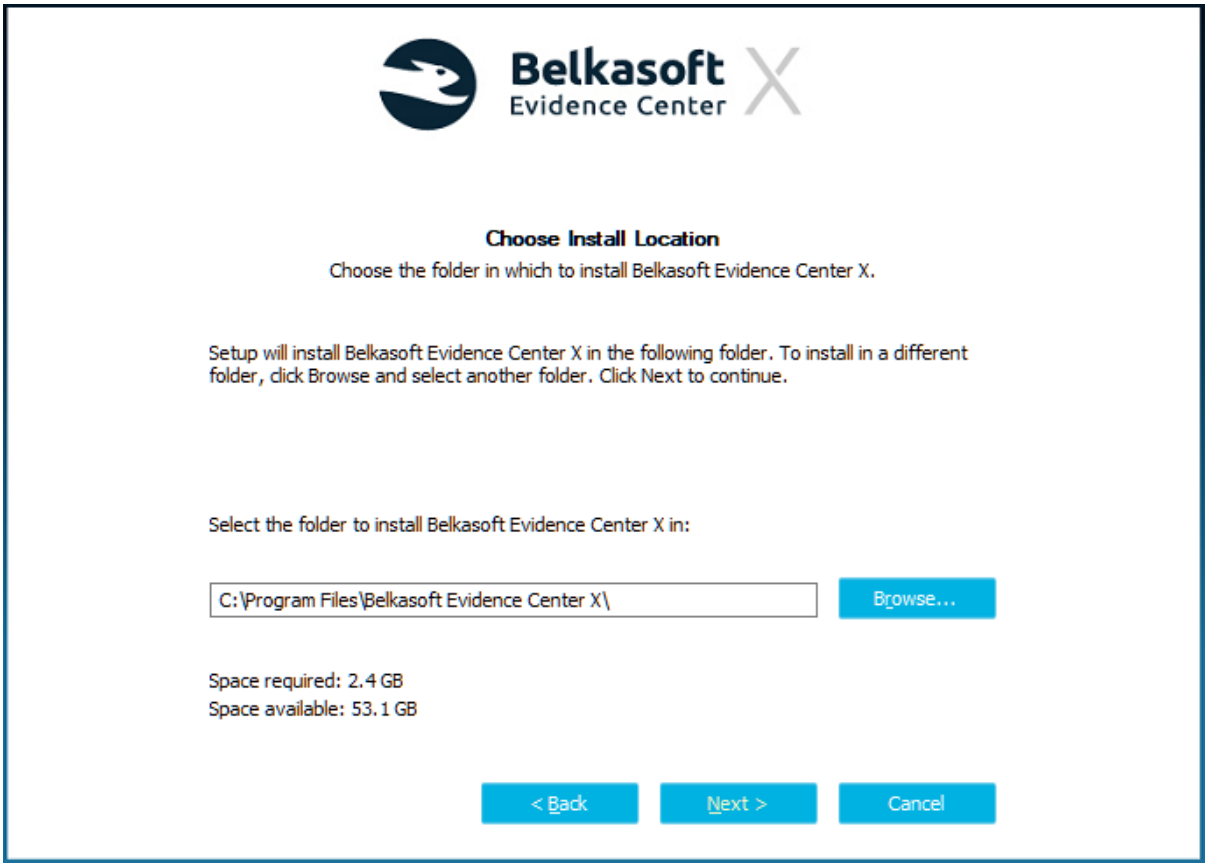
First, select your preferred language.



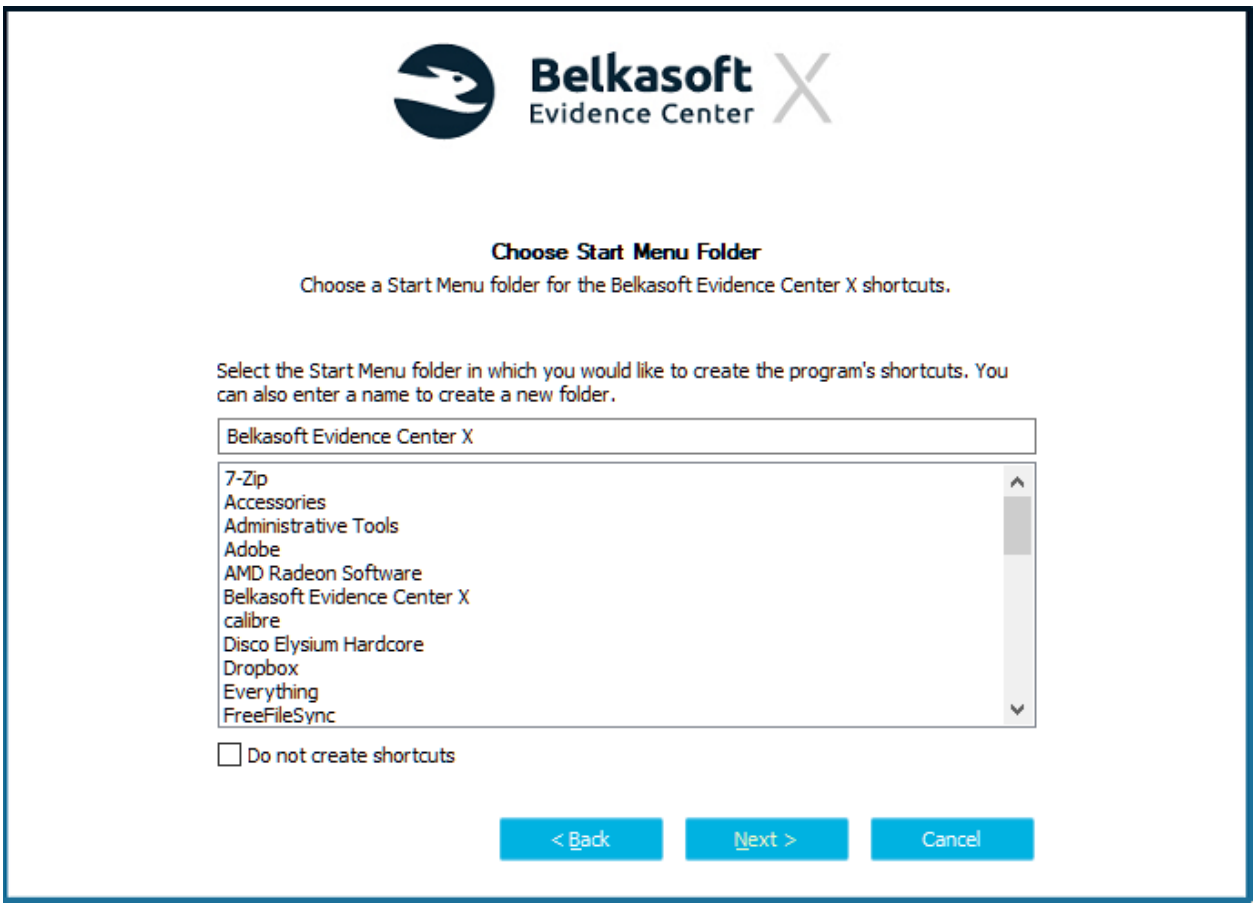
Click on ***Next*** *on the first installer screen*



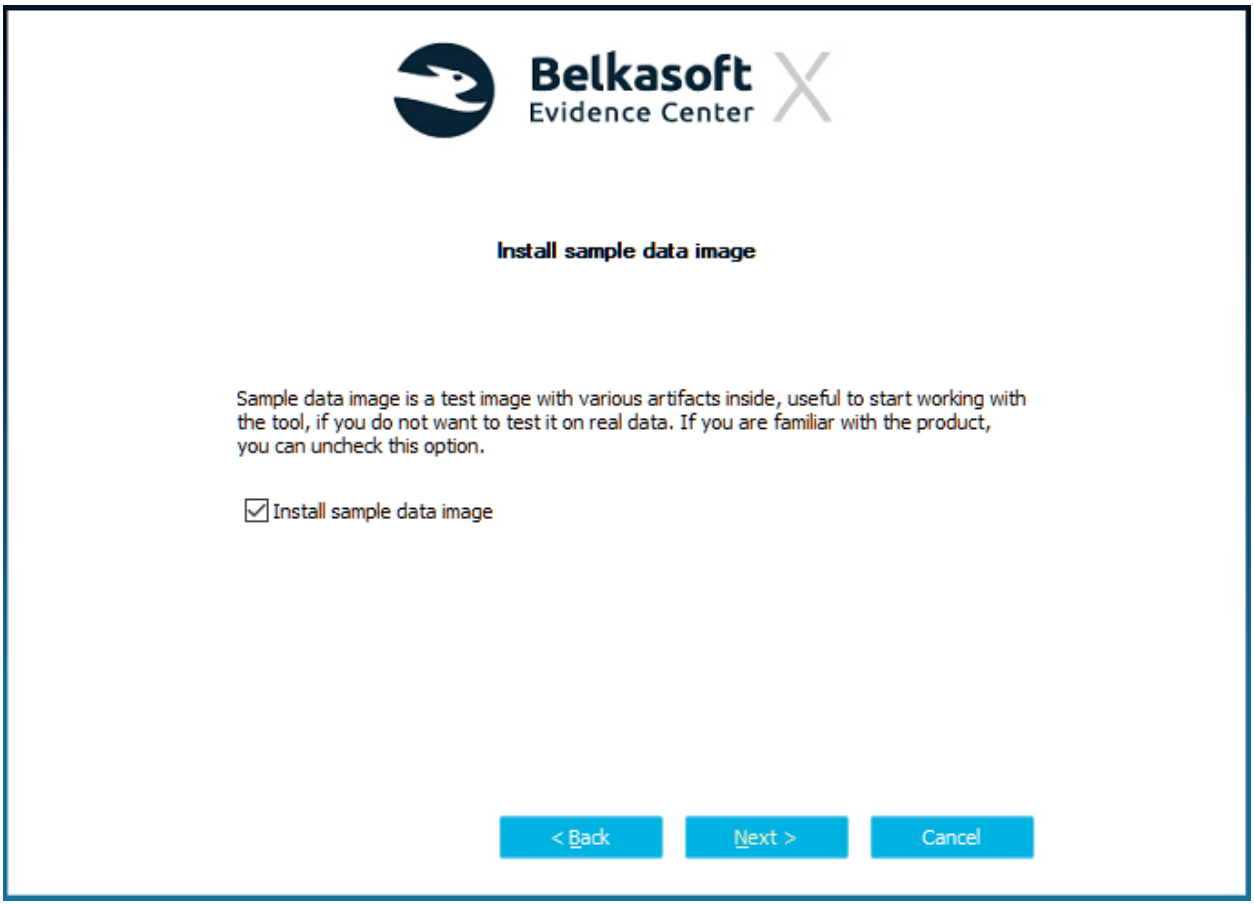
Read and accept the end-user license agreement



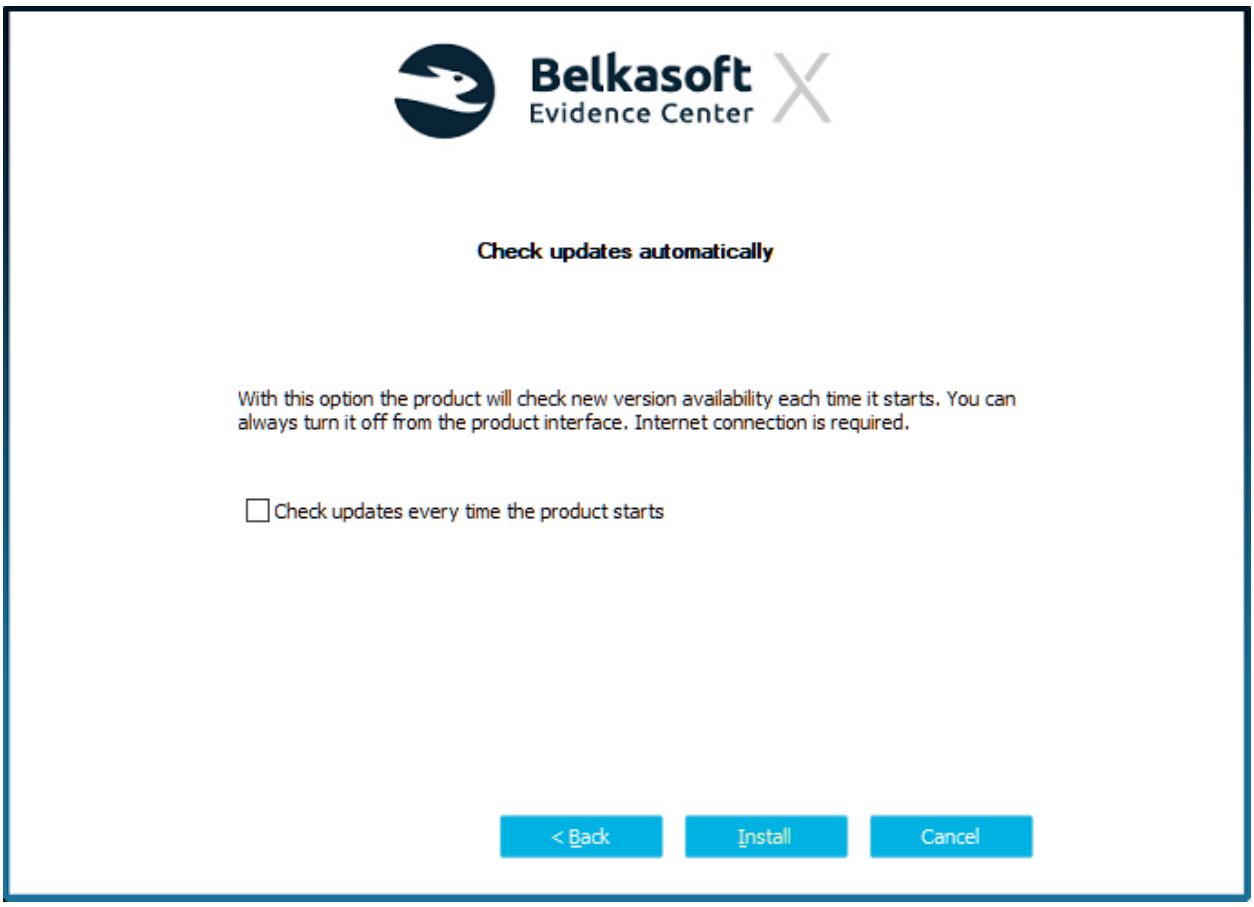
Select the target folder for Belkasoft X installation



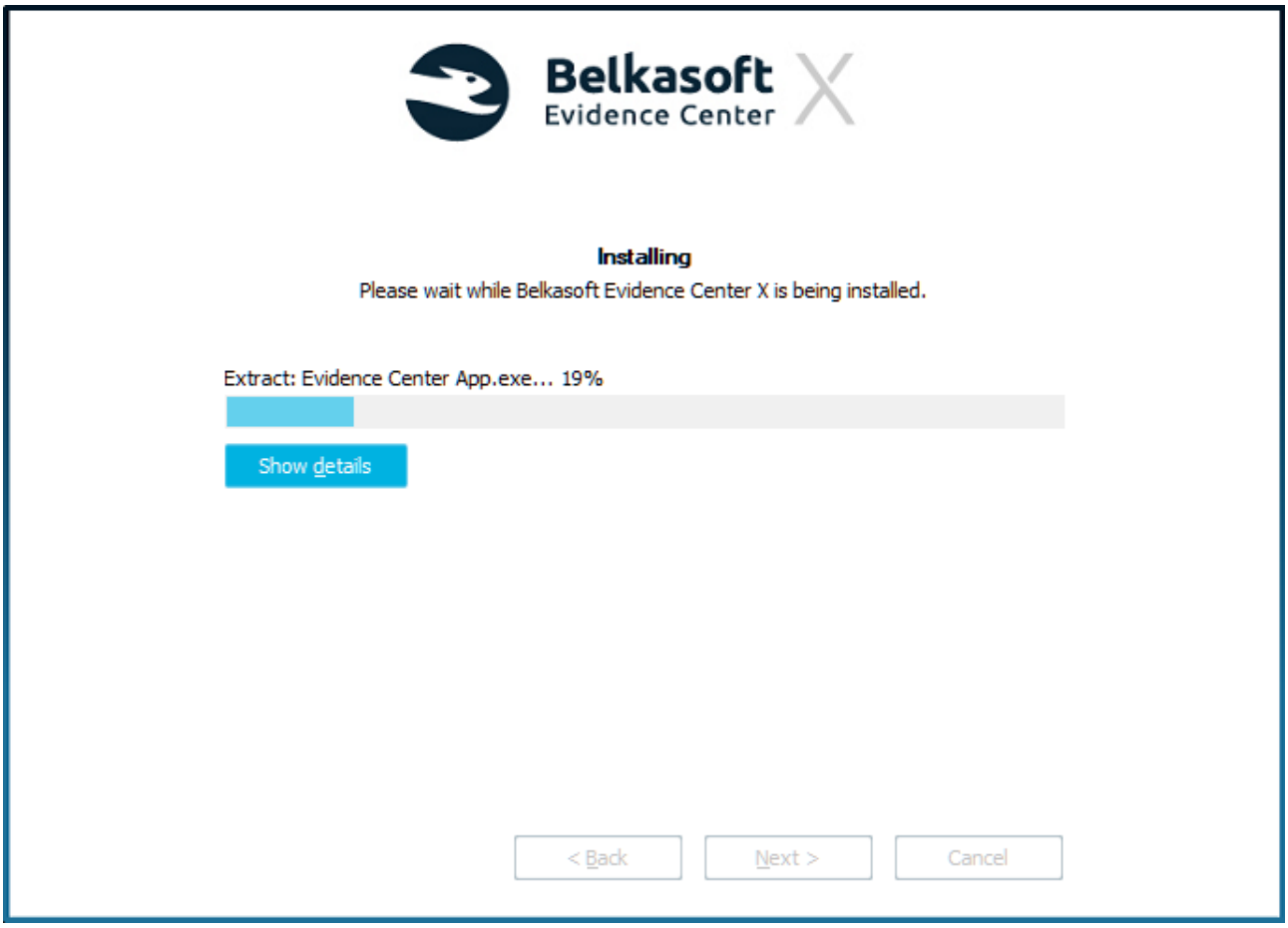
Select the Windows Start Menu folder location for Belkasoft X (or check Do not create shortcuts)



Decide whether you would like to install sample data

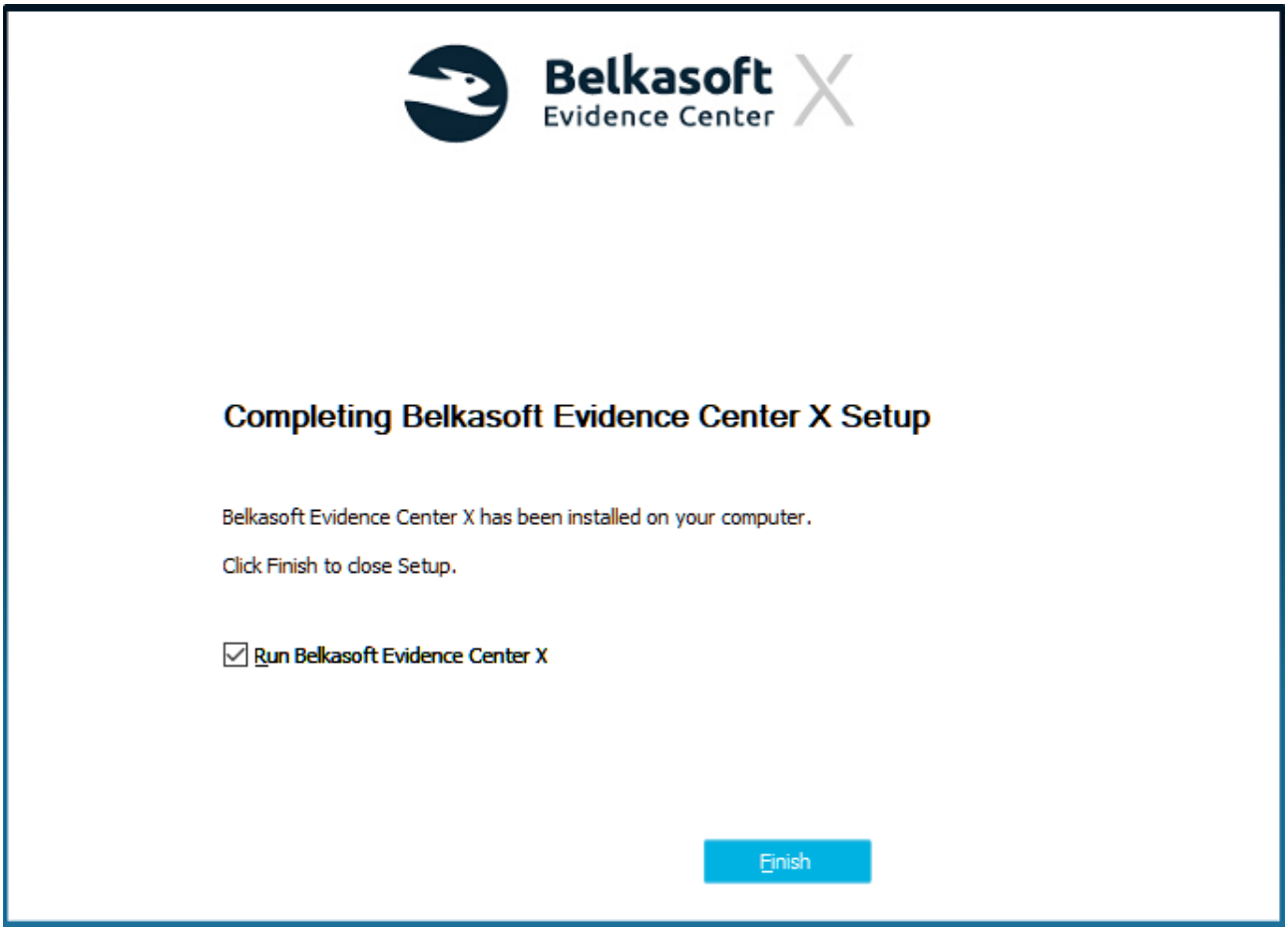


Choose if you would like to check for updates automatically every time the product starts. Please note: an Internet connection is required for this to work



On this screen, wait until all the product files get copied.

If you get an error stating that some files cannot be written, verify that Belkasoft X processes (especially Evidence Center.exe and ApplicationClient.exe) are not running



*Click **Finish** to close Belkasoft X installer. If you want to start using the tool right away, check the "Run Belkasoft Evidence Center X" checkbox*

The product should be marked as successfully installed now.

Belkasoft X Trial version limitations

Most of acquisition and analytical features in trial work the same way they do in the licensed/registered mode. However, in the trial mode, there are a few limitations you should know about:

1. The product works for 30 days only. If a previous Belkasoft X version was installed on your computer, the application might refuse to initiate a new trial period—this depends on the policy for a new individual release; in some scenarios, a new trial may be allowed. Once the trial ends, the product stops opening your cases
2. Reports contain 50% randomly selected artifacts
3. Export to Evidence Reader is not provided
4. Decryption functionality is not provided
5. The trial version does not work on virtual machines. It also requires online activation.
6. Trial cannot be launched from a command line
7. The following acquisition types are not included into the trial version:
    - Full logical backup of jailbroken iOS devices.

- Agent-based acquisition of iOS devices.
- Checkm8-based acquisition of iOS devices.
- Android filesystem copy.
- EDL acquisition for Android devices with Qualcomm processors.
- Agent-based MTK acquisition of Android devices.

Activating Belkasoft X license

To activate your license, you will need a license file. *This file is required; even if, you are working with a dongle-based license.*

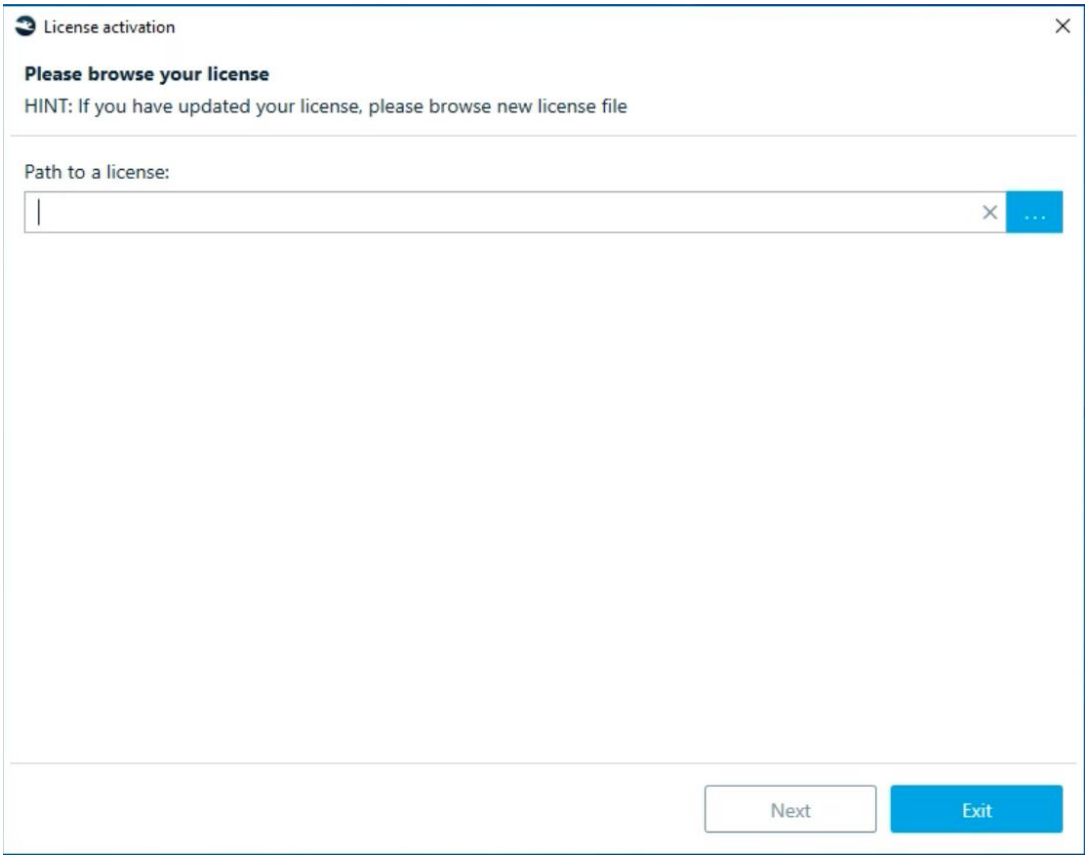
When you purchase Belkasoft X, Belkasoft sends you the license file. You can also download the license file from your Customer Portal, which is created upon your purchase. The file appears as **license.xml** or, in a packed form—**license.xml.zip**. This file contains information about your license, such its expiration date and the available features on your license.

Warning: Do not try to edit the license file because it may end up being corrupted. Belkasoft uses cryptographic signature to protect the file and secure its integrity.

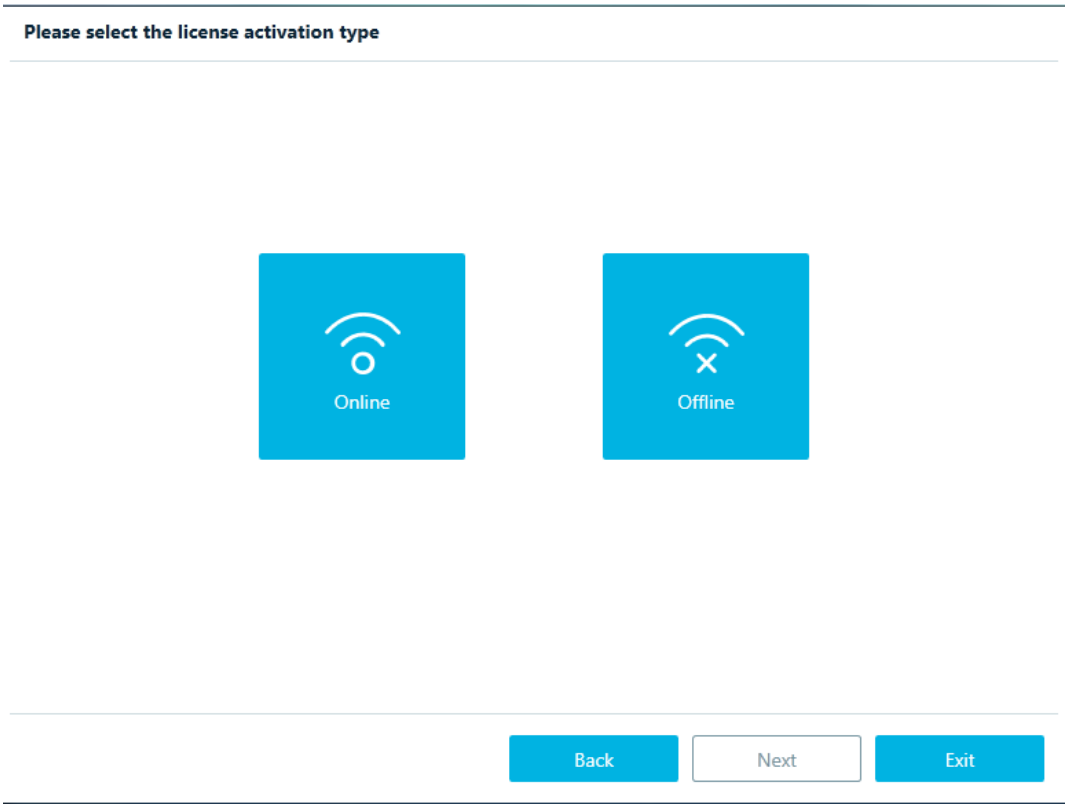
You can place the license file (even in its unpacked form) in the product folder, or you can browse to it through the **License activation** window shown at start for an unregistered product.

Electronic License Activation

After the first launch following the installation, Belkasoft X will ask you to browse to the license file.

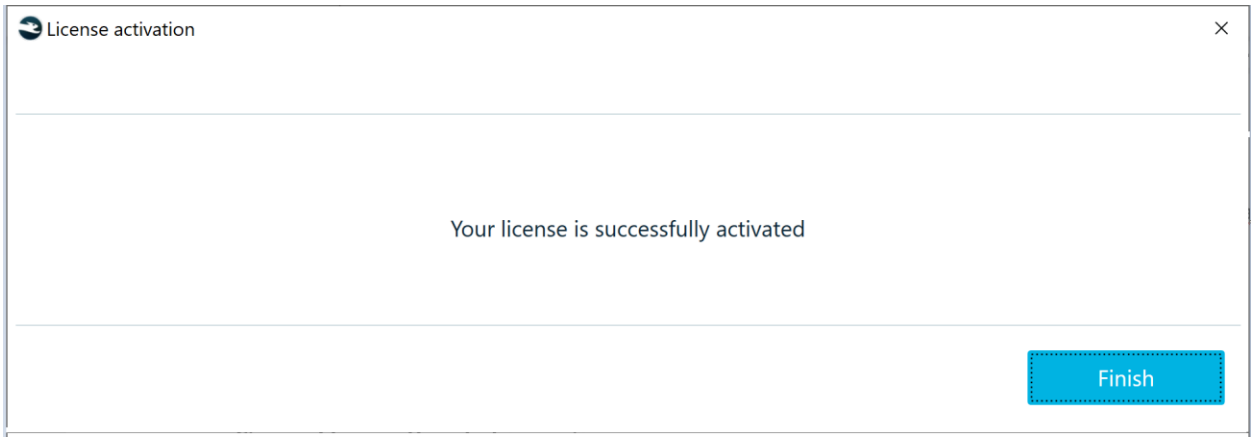


After selecting a license file, Belkasoft X prompts you to activate the product. You can activate an electronic license either online or offline.



Online activation

Online activation should be used when you have internet access on the computer on which Belkasoft X is installed. Click **Online** button. The license is now activated online.



Offline activation

Offline activation may be useful if the computer on which Belkasoft X is installed.

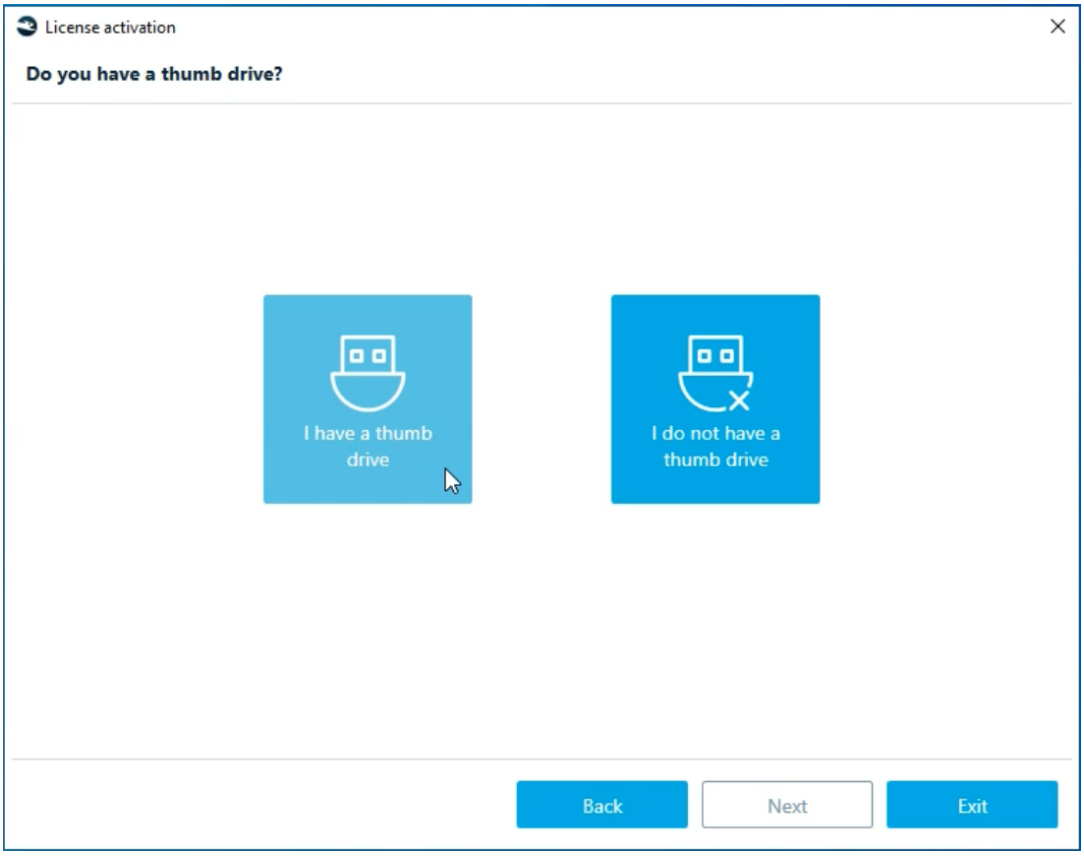
- Lacks Internet access
- Uses a firewall, which limits the available web resources
- Suffers from restrictions that make online activation of a license impossible.

Two options are available: with a thumb drive and without a thumb drive.

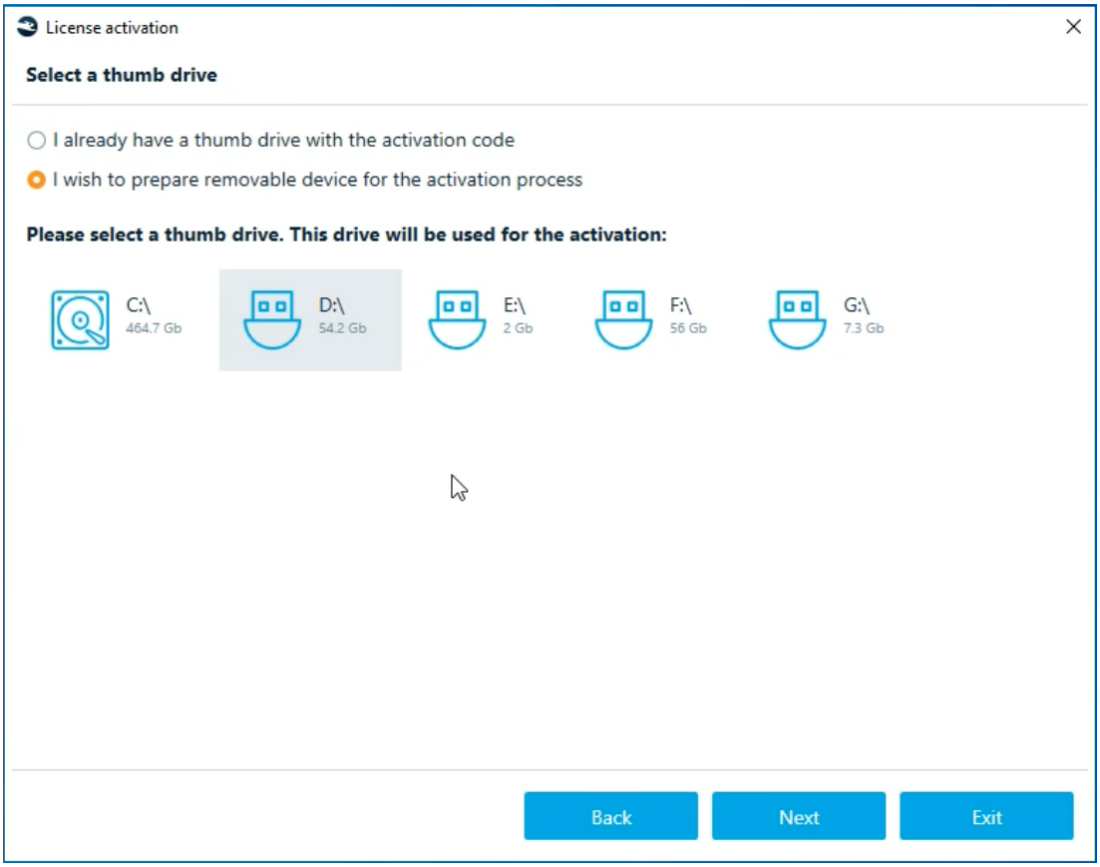
Click on the **Offline** button.

With a thumb drive

Choose **I have a thumb drive** option.

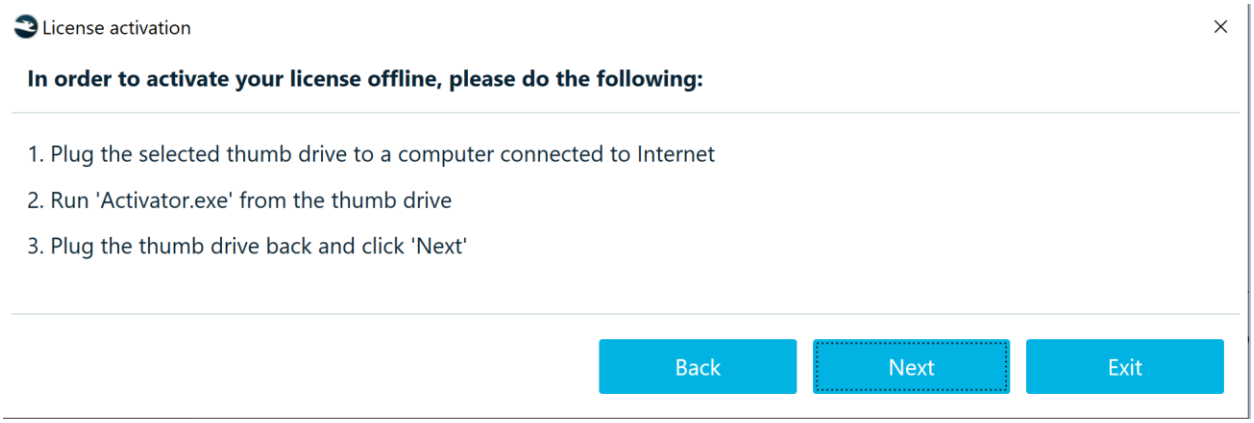


Insert the thumb drive you intend to use into your computer. Select your drive from the list.

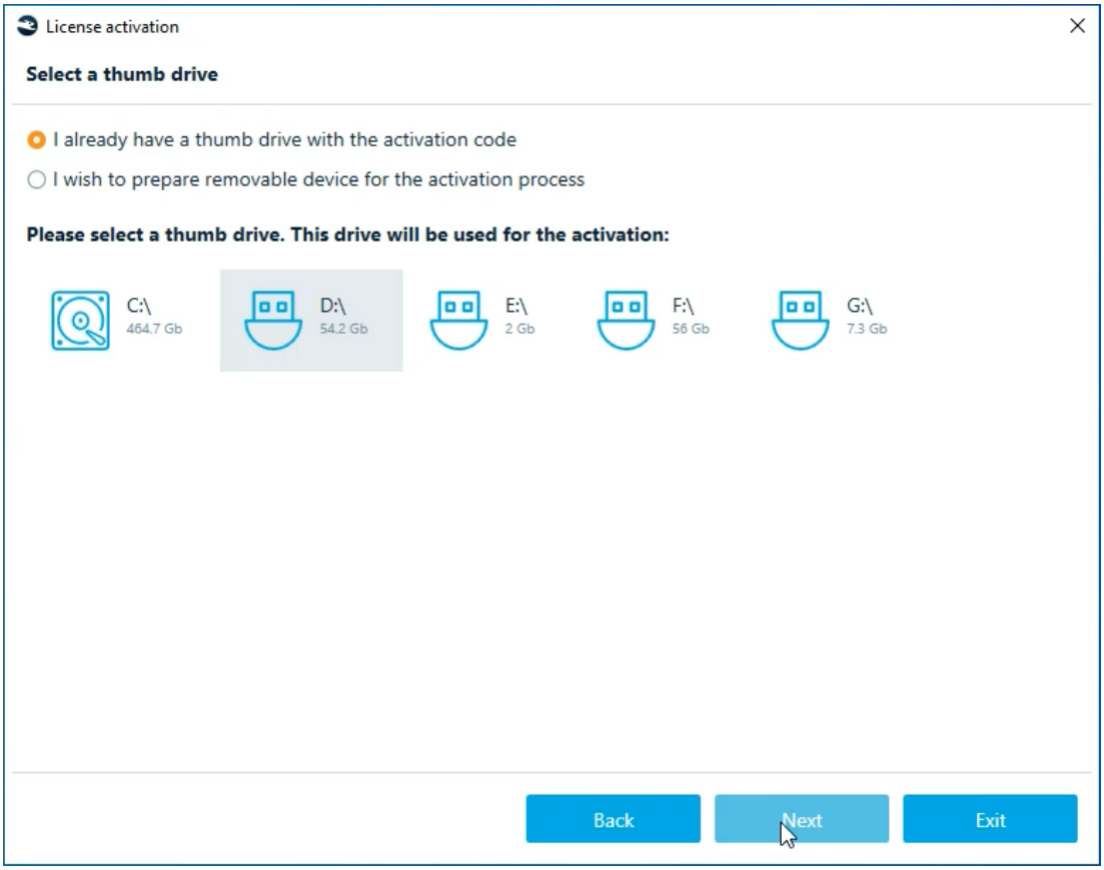


The folder with **info.toserver** file will be copied onto your drive.

After that, follow the instruction on the screen:



Now select the **I already have a thumb drive with the activation code** option. Click **Next**.

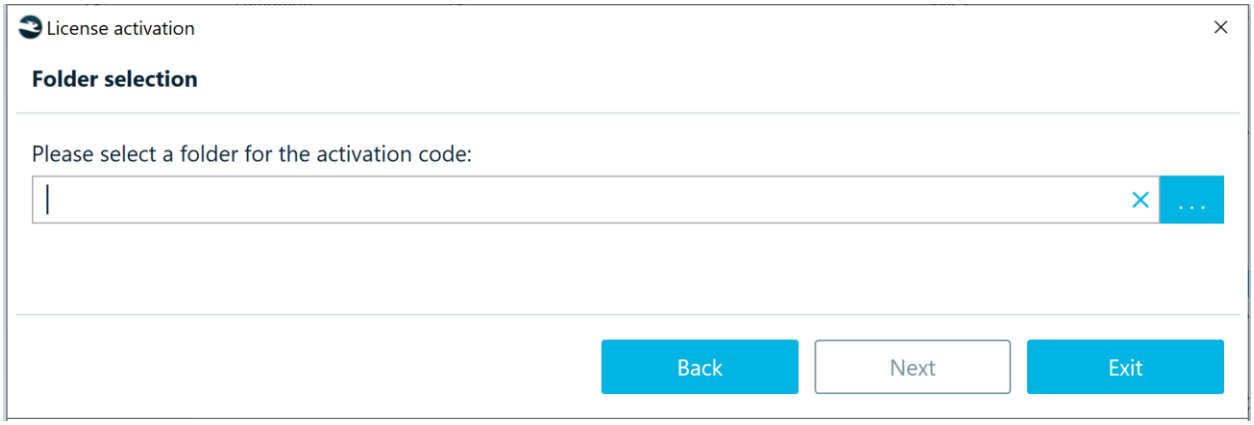


The license is now activated.

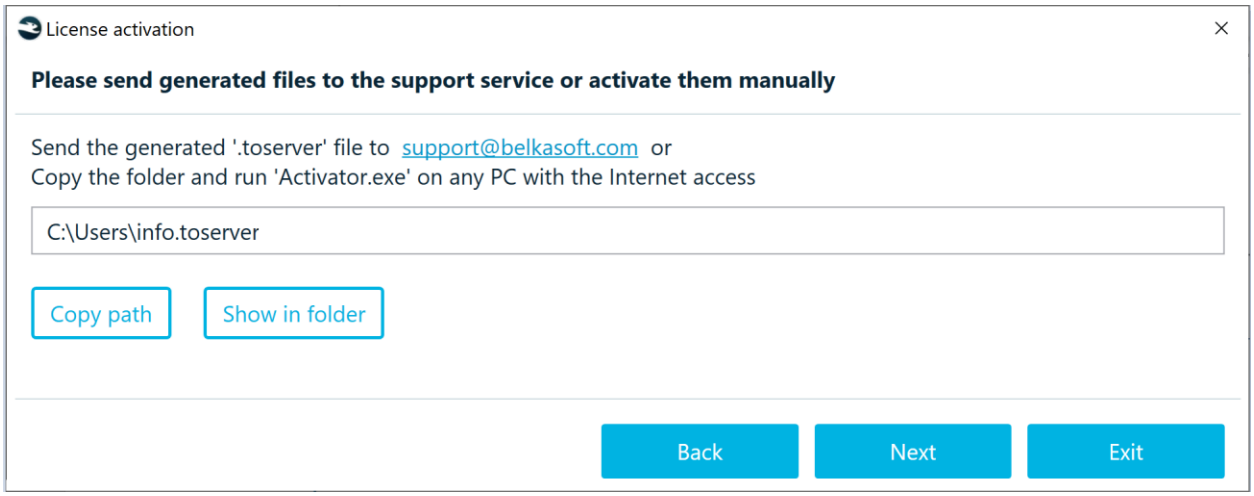
Without a thumb drive

If you do not have a thumb drive, click on **I do not have a thumb drive** button and continue from there.

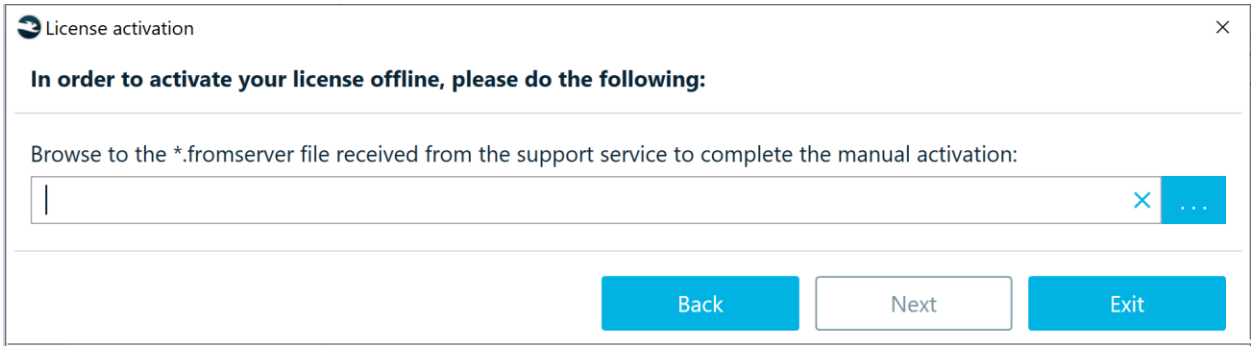
You should see this window:



Select the folder where **info.toserver** file will be saved. After that, either send file to support@belkasoft.com for activation or activate it by running Acrivator.exe on the computer with the Internet access.



In any case, you will get the **response.fromserver** file, which you need for the third step of activation process.



Browse the **response.fromserver** file and click on **Next**.

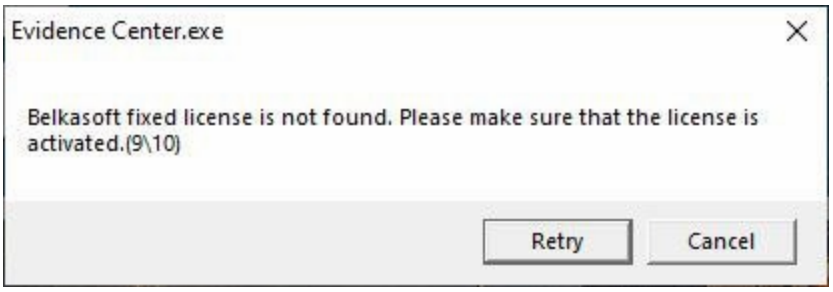
Belkasoft X is now activated. No need to restart the program.

Trial Version Activation

The procedure is similar to the electronic license activation procedure described above. Here, however, you do not need a license file.

Select **Online** or **Offline** activation and follow the steps described in the corresponding sections for Electronic License Activation.

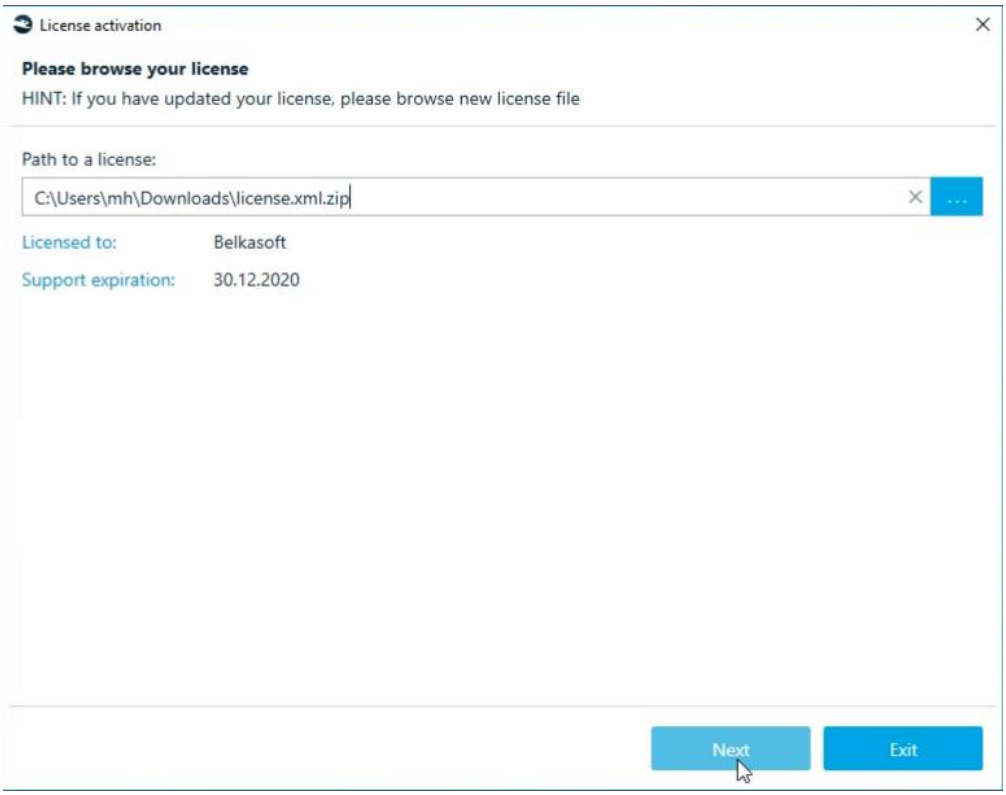
If you see the message: 'Belkasoft fixed license is not found':



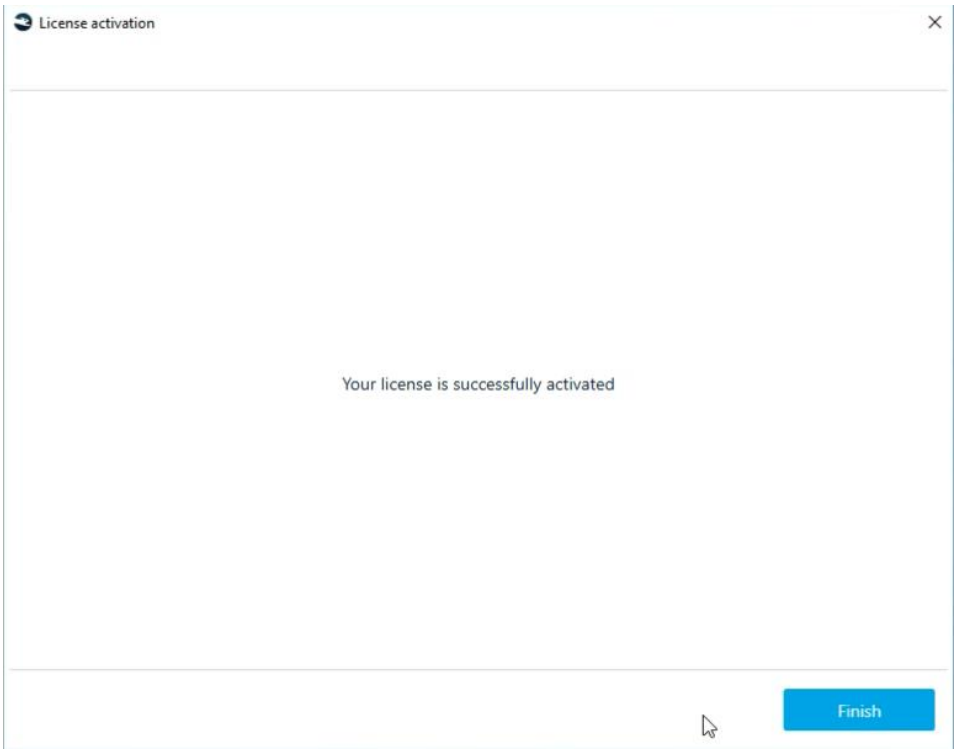
This means that the trial version has not been activated, send info.toserver file to the support team support@belkasoft.com and make sure that the computer does not have Guardant drivers.

Floating (Dongle) License Activation

To activate a dongle license, you need to insert the dongle and browse the license file.



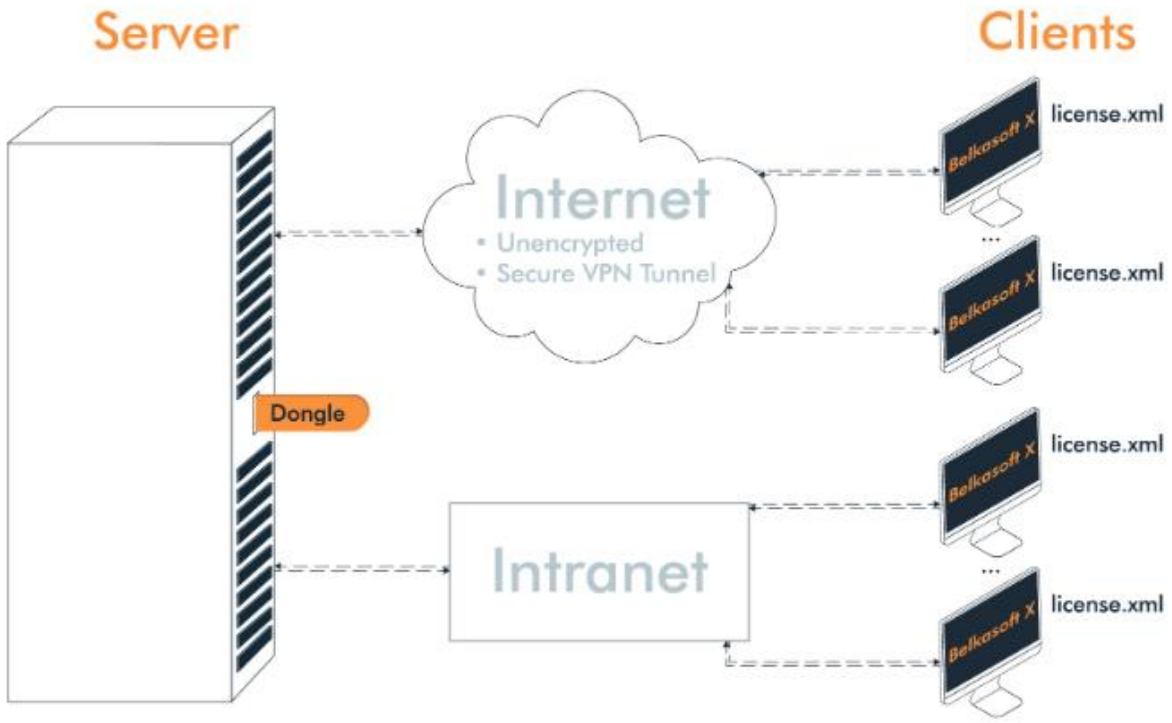
Click **Next**. The license will be activated automatically.



The dongle license is now activated.

You must repeat the described process on every machine where you work and use same dongle for Belkasoft X.

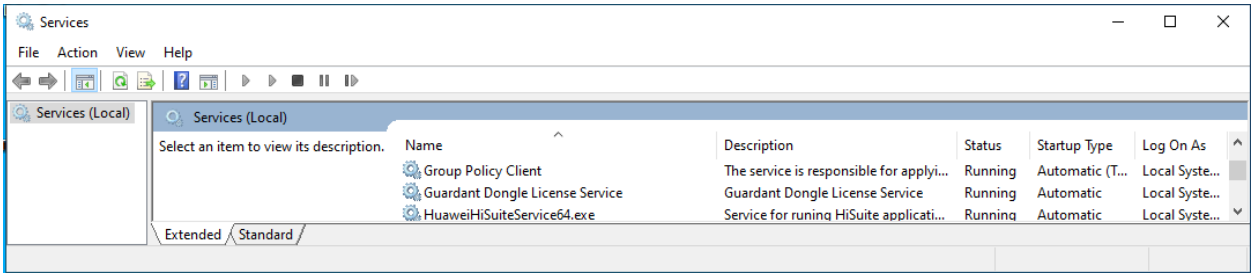
Network licenses (how to configure server and client)



Please note: *Guardant License Server and Belkasoft X (Clients) cannot be installed on the same machine, use different computers in your network.*

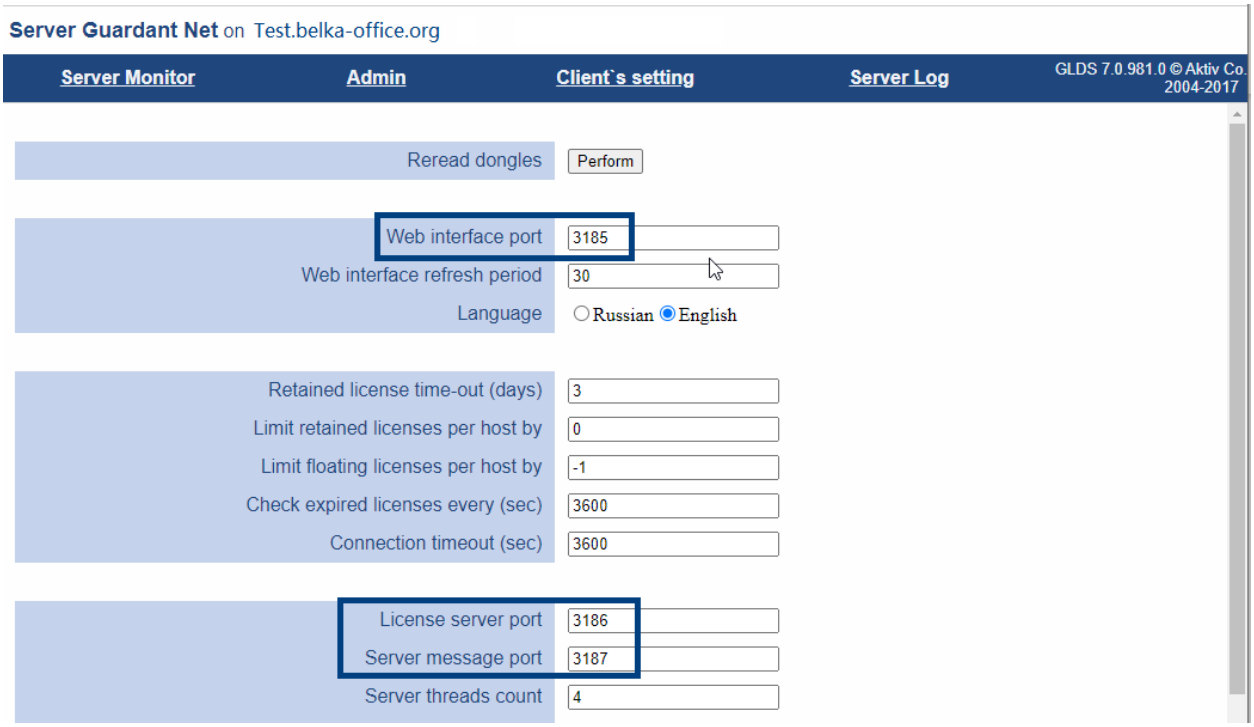
Server

Before you can use your network license, you need to install **Guardant License Server 7**.
Guardant License Server is installed on a dedicated computer and provides communication between the protected network application and Guardant Net dongle in LANs. One server is capable of servicing queries addressed to several Guardant Net dongles.
Guardant License Server is compatible with Windows 10/8/7/2008/Vista/2003/XP and Linux (Debian).
Please use this link for downloading Guardant License Server from Guardant official website: https://www.guardant.com/support/download/server/.
Connect Guardant Net dongle to the computer on which the server will be configured and run GLDS.exe. After starting GLDS.exe, Guardant Dongle Licensing Service appears in the list of Windows system services.



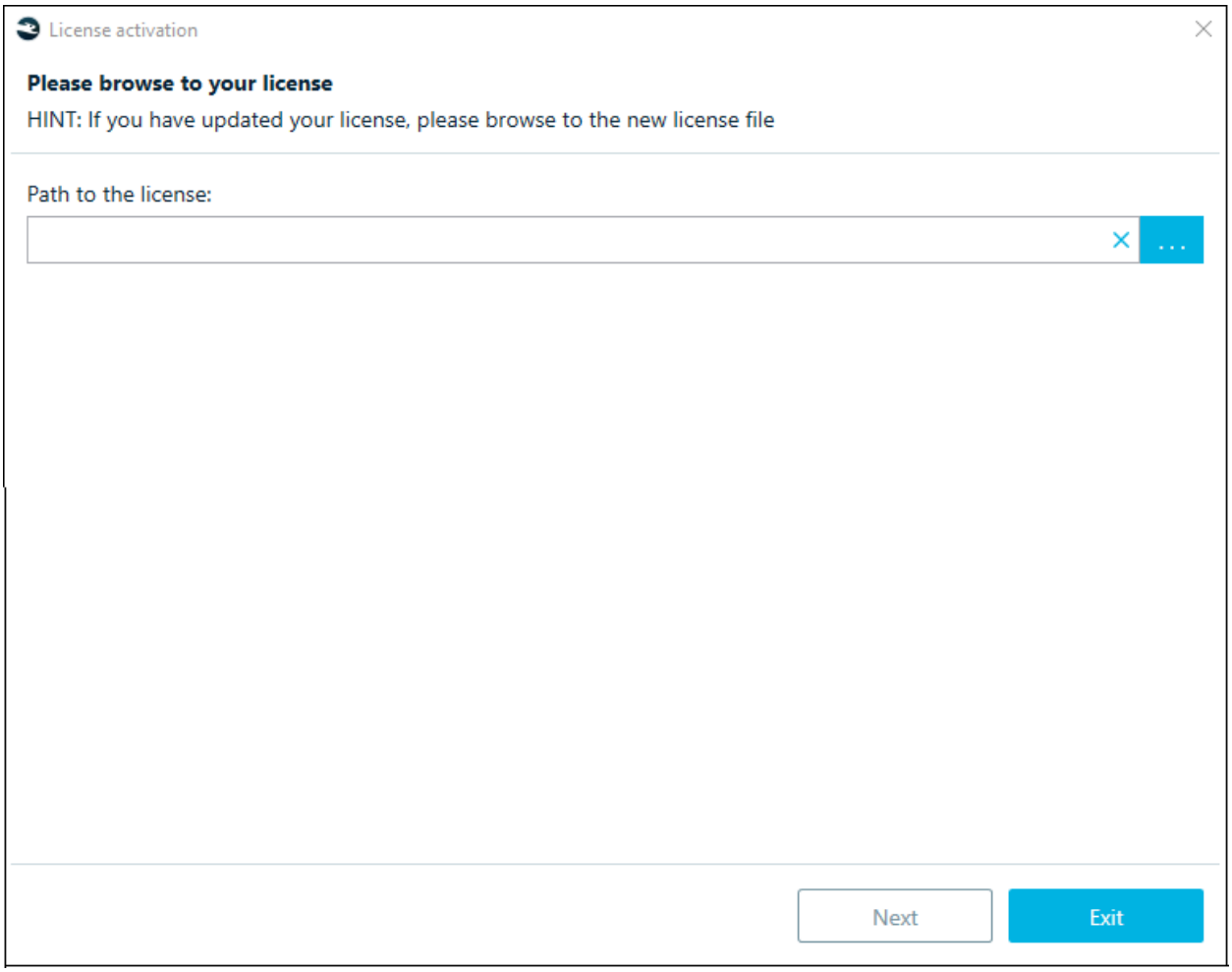
For up-to-date information about the state of Guardant License Server and Guardant Net dongle and for

their customization, the web interface is used (Server Guardant Net). After installing the server, check the availability of the web interface *http://<[IP / computer name]: port>* (for example, http://192.168.0.1:3185).
Check that the system ports are open in the firewall configuration (at the time of this writing, these are 3185, 3186, 3187). The ports are listed on the Admin tab in Server Guardant Net (the default password for access is *admin*).

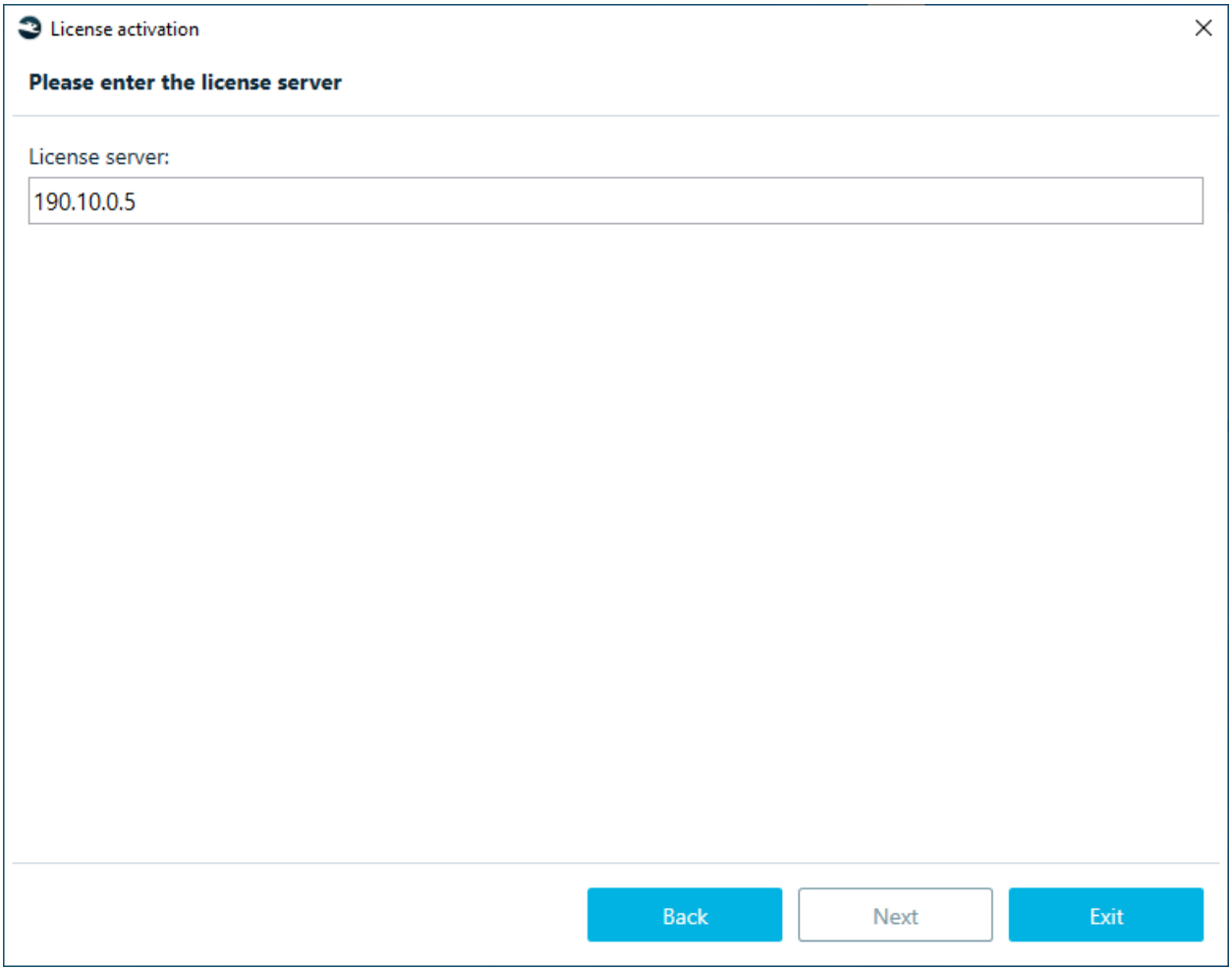


Client

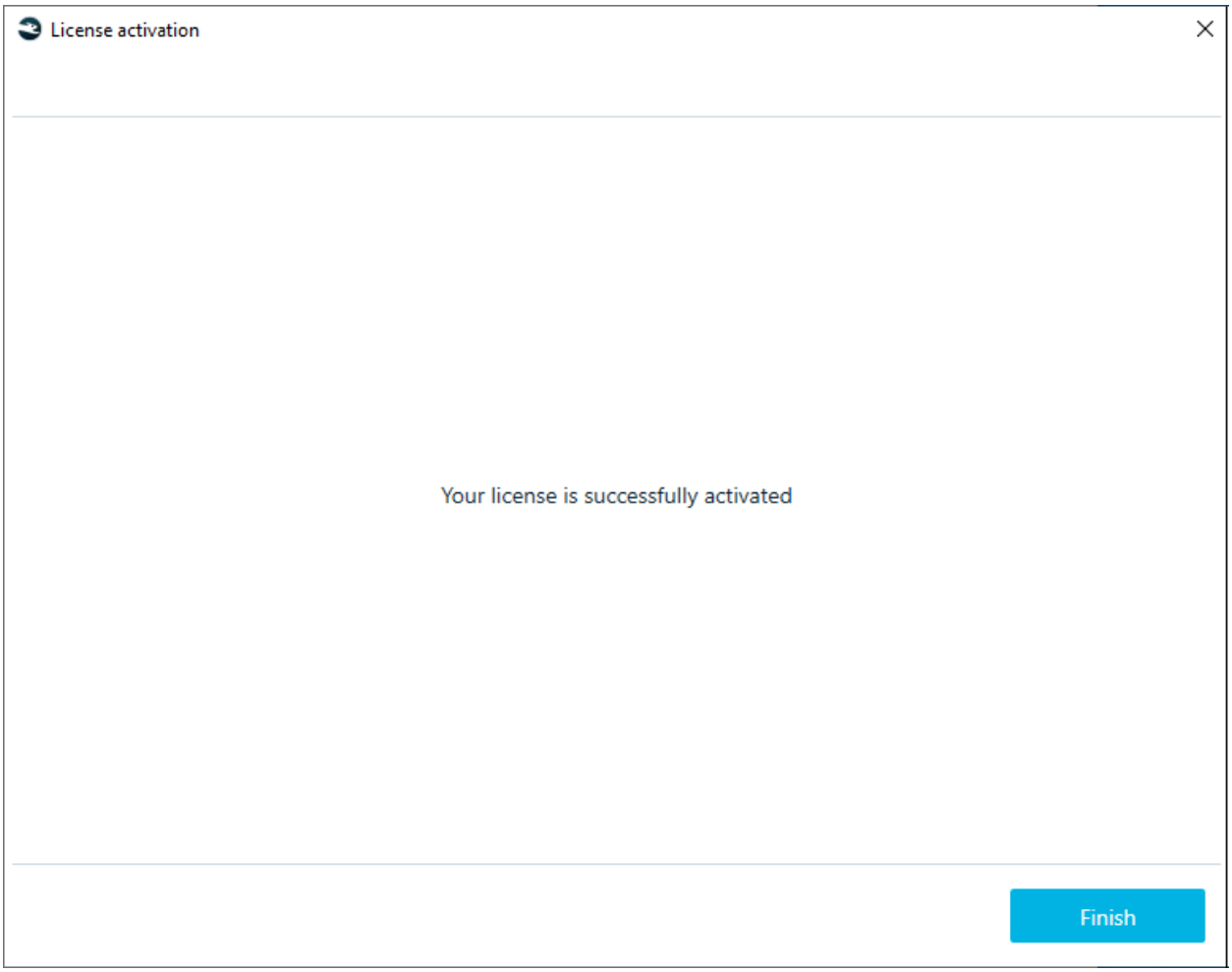
1. Before starting work, check that Server Guardant Net is available.
2. Run the Belkasoft X installation.
3. First time you launch Belkasoft X you will be asked to activate your license.
4. Browse to the saved license file:



The license file is usually sent to you by Belkasoft once you complete your purchase. It could also be downloaded at the Customer Portal.
The file is called **license.xml** or, in packed form, **license.xml.zip**. Please do not try to edit the license file. This may damage the license as its integrity is protected by a cryptographic signature.
Then specify the license server (server name or IP address):



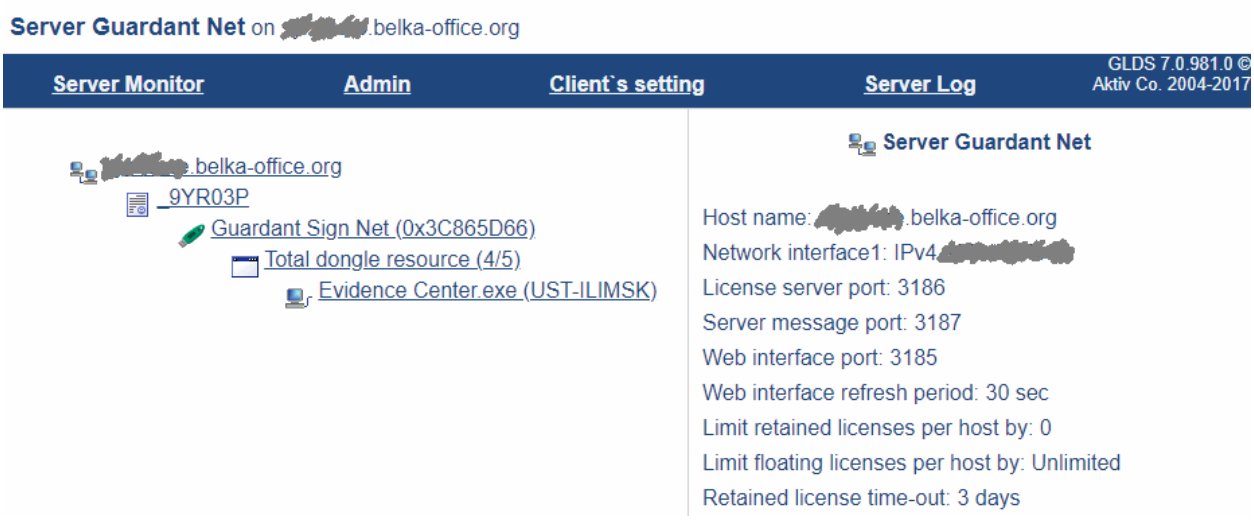
Upon successful activation, a window will appear:



If the dongle is not found:

- Check that the number in the license file (Network Hardware ID) matches the number on the dongle
- The client configuration file gnclient.ini contains the correct IP address (or network name) of the server and the network port.

If everything is done correctly, connection information will appear in the web interface (Server Guardant Net):



If you have any issues, please contact support@belkasoft.com and we will help you within a business day.

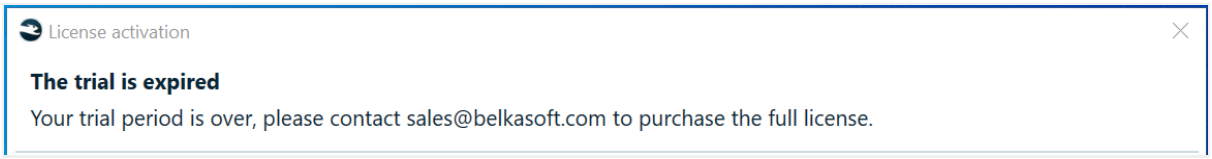
License troubleshooting

General advice

Please find the first steps to resolve issues with licensing below:

- Make sure you have the file called license.xml or license.xml.zip in your product folder (this doesn't refer to trial versions)
- Add the product to the list of antivirus exceptions
- Do not use a USB hub for Belkasoft dongles
- Change USB port from 3.0 to 2.0 and vice versa (we recommend USB 3.0)

Message: The trial is expired

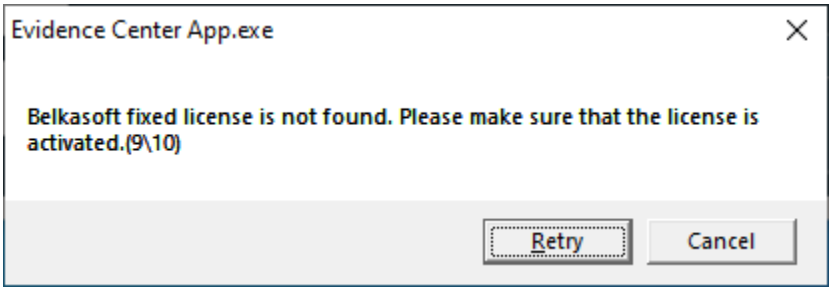


Prerequisites: the trial version directly after the installation or when the product is launched

Reason: The trial can be activated only once on each machine. Even if the user is not aware of the fact, this message means that the trial version was previously installed and activated on this computer

Solution: Either use another computer for the evaluation or contact sales@belkasoft.com

Message: Belkasoft fixed license is not found. Please make sure that the license is activated



Prerequisites: Trial and fixed versions, when the product is launched

Reasons:

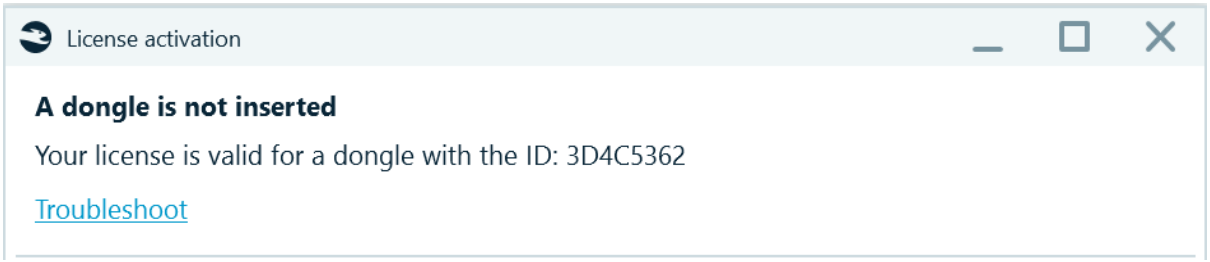
1. Guardant drivers are installed.

   Solution: Delete Guardant drivers (you could do that using “Add or remove programs”). If activation is not prompted upon the next start, reinstall the product to another folder.

2. Info.toserver was chosen instead of the response.fromserver in the License activation wizard

   Solution: Launch Belkasoft X and select the Offline activation option once again. Make sure that the response.fromserver file was successfully created and chosen in the ‘Browse to the *.fromserver file received from the support service to complete the manual installation’ field.

Message: A dongle is not inserted. Your license is valid for a dongle with the ID:



Prerequisites: dongle-based version

Reasons:

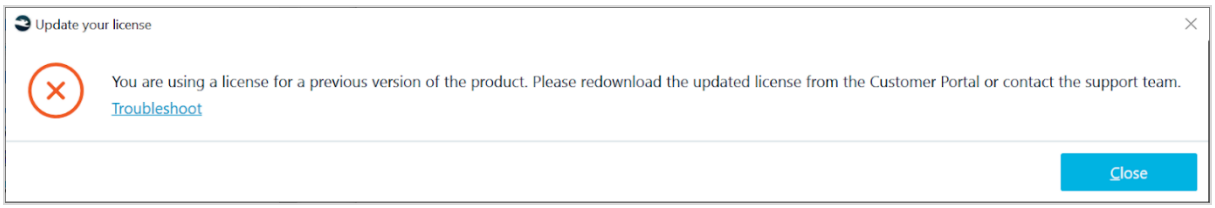
1. A dongle is not inserted

   Solution: Insert a dongle

2. A wrong dongle is inserted

   Solution: Compare the dongle’s ID, it is printed on the side of the dongle. If the ID doesn’t match, please contact sales@belkasoft.com

Message: You are using a license for a previous version of the product. Please redownload the updated version

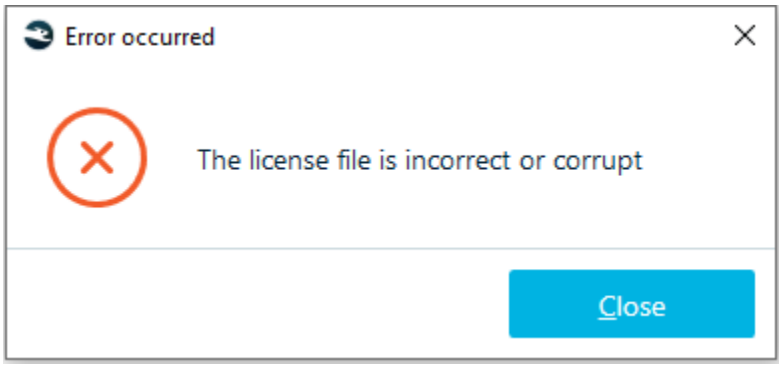


Prerequisites: fixed and floating Belkasoft X versions upon the product's launch

Reason: A license.xml file of the old Evidence Center version (prior to Belkasoft X) is used

Solution: Delete old license.xml and license.xml.zip from the product folder, log in to the customer portal and download a corresponding Belkasoft X license file. Contact sales@belkasoft.com in case of any questions.

Message: The license file is incorrect or corrupt

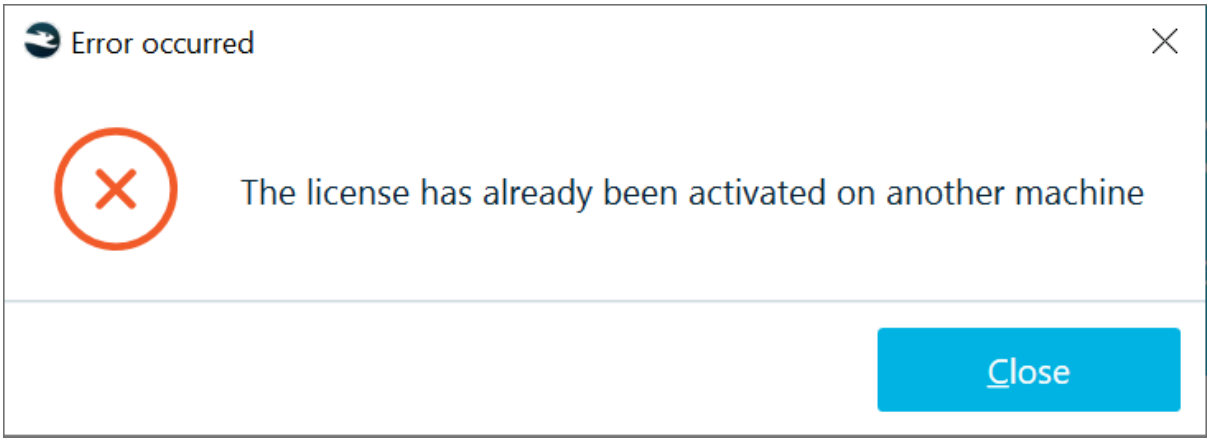


Prerequisites: fixed and trial versions, **Offline** license activation option

Reason: response.fromserver file is corrupt or the user has chosen not a response.fromserver file in the License activation wizard

Solution: Make sure that the user selects response.fromserver file in the 'Browse to the *.fromserver file received from the support service to complete the manual installation' field. If yes, contact support@belkasoft.com and attach the info.toserver file, you will be sent a valid response.fromserver file.

Message: The license has already been activated on another machine

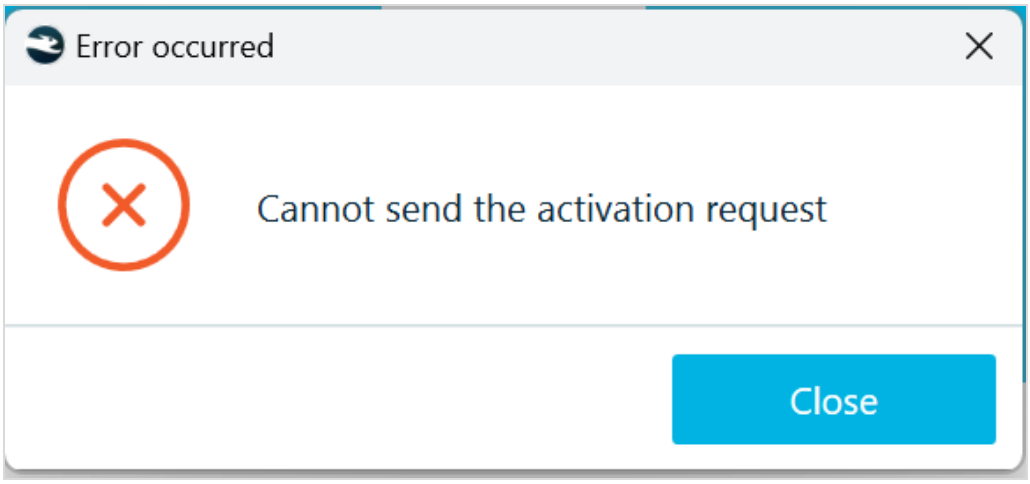


Prerequisites: fixed version after an attempt to activate license.xml

Reason: This license.xml was activated on some other computer, e.g. by mistake or somebody else's license.xml is used

Solution: Make sure that a correct electronic license is used, log in to the customer portal and download the corresponding license file. If this does not help, please contact sales@belkasoft.com.

Message: Cannot send the activation request

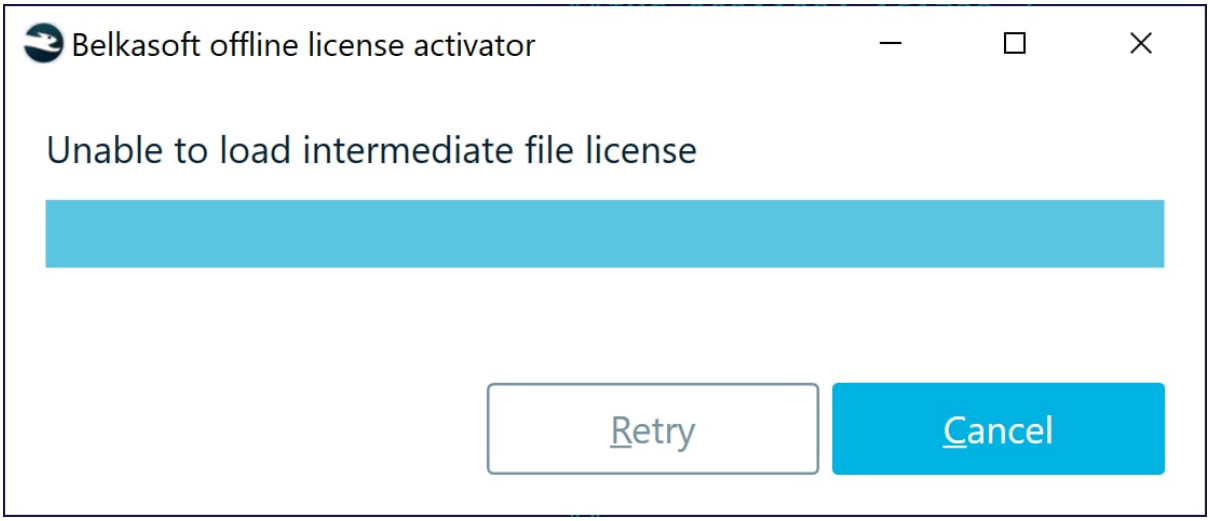


Prerequisites: Trial and fixed licenses, 'Online' and 'Offline' license activation options

Reason: Network restrictions. Outbound connections are forbidden by firewall settings.

Solution: Ask your network administrator to open outbound connections (standard HTTPS protocol ports are used: 443 and 8443). Or activate offline with Belkasoft support (send info.toserver to support@belkasoft.com).

Message: Unable to load intermediate file license

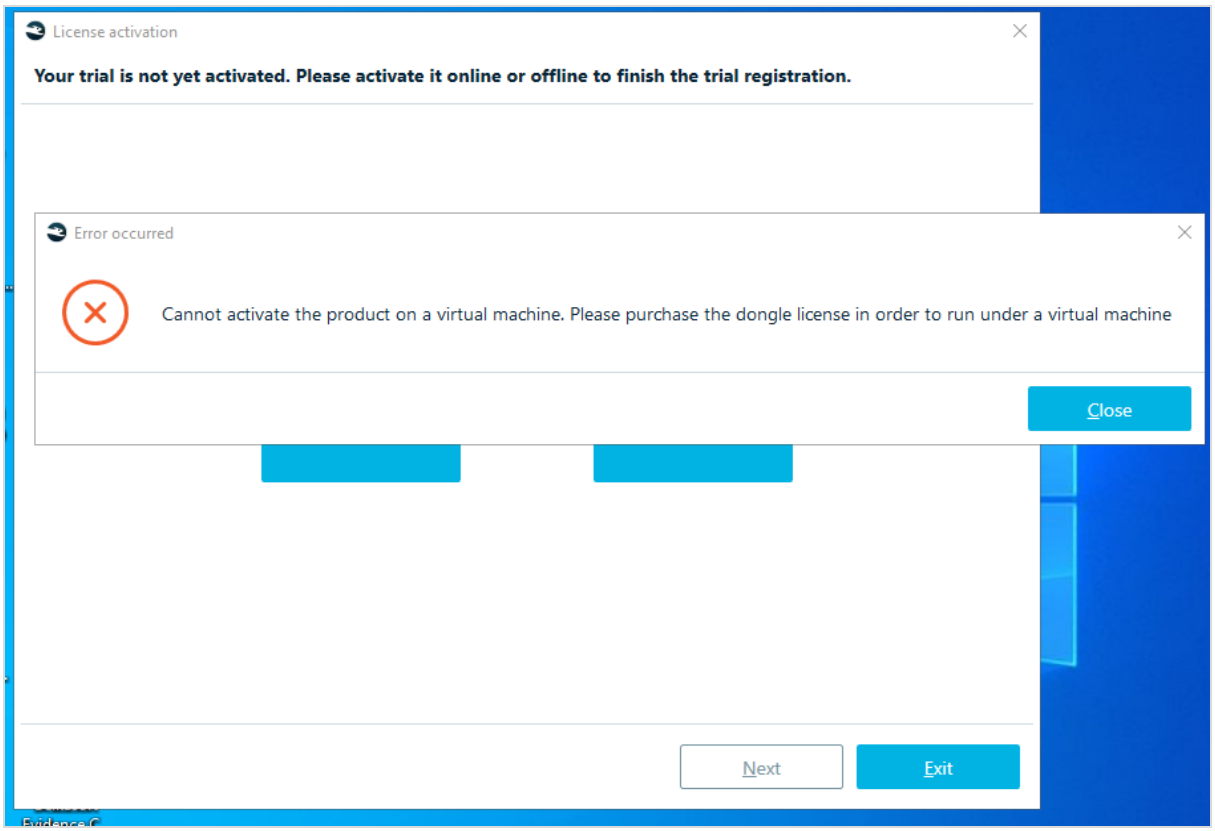


Prerequisites: Trial and fixed license. The message is issued by Activator.exe

Reasons: info.toserver is missing in the Activator.exe folder

Solution: Choose the 'Offline' activation option, follow the instructions and make sure that info.toserver is created. Launch Activator.exe from the same folder where info.toserver is saved.

Message: Cannot activate the product on a virtual machine. Please purchase the dongle license in order to run under a virtual machine



Prerequisites: Trial or fixed license

Reason:

1. The product is being activated on a virtual machine

   Solution: Activate a product on a host machine or purchase a dongle-based version, which can be used on virtual machines

2. The product is being activated on a host machine, which is for some reason considered to be virtual by Guardant

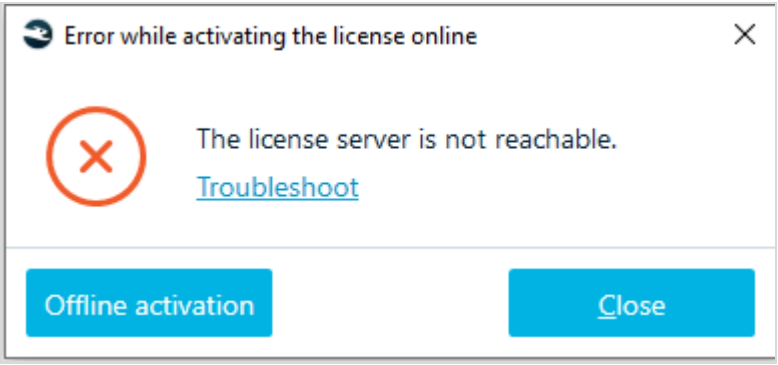
   Solution: Try another host machine

Message: An error occurred while copying the license file to the product folder. Please close the product, copy the license to 'C:\...\Belkasoft Evidence Center X"

Prerequisites: Any build, when browsing to the license file in the 'License activation' window (immediately after the installation or in the 'Home' tab → 'License information')

Solution: Copy the license.xml file manually to the product folder and restart Belkasoft X.

Message: The license server is not reachable



Prerequisites: network licences, both regular and academic

Reasons: Belkasoft X cannot reach the Guardant Net server due to something from the following list:

1. Wrong server's name or IP address in gnclient.ini

   Solution: Correct the server's name or IP address in gnclient.ini, or delete gnclient.ini from the product folder, launch Evidence Center.exe and enter a correct IP address in the 'License activation' wizard.

2. Guardant Net Server is not installed

   Solution: Install the Guardant Net Server.

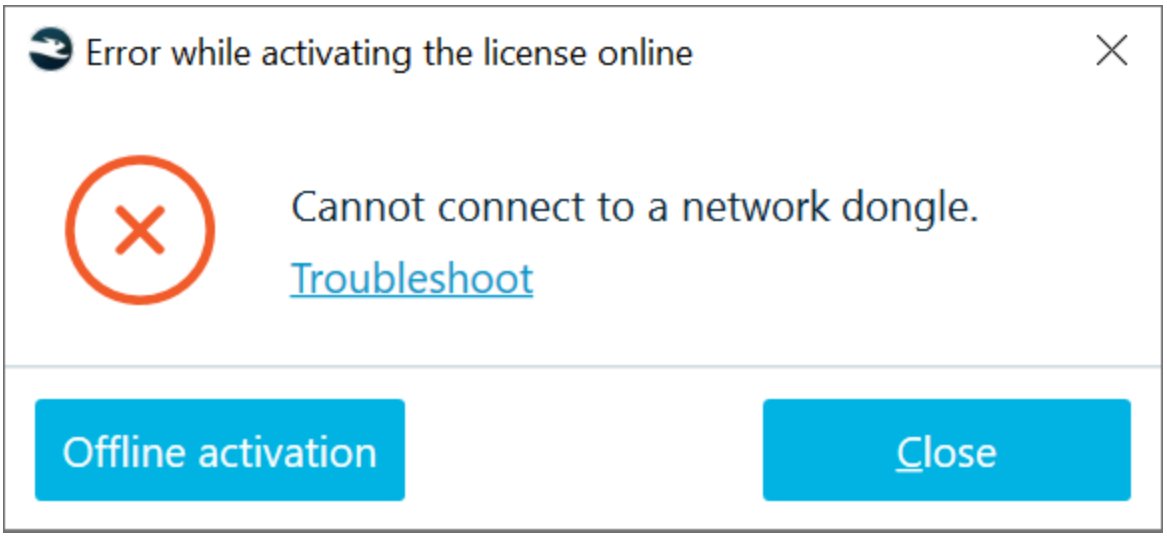
3. Guardant Net Server is not launched

   Solution: Launch the Guardant Net Server service in Services.

4. Guardant Net Server ports 3185, 3186 and 3187 are closed for incoming connections

   Solution: Forward all necessary ports through the Windows Firewall or any other firewalls.

Message: Cannot connect to a network dongle



Prerequisites: Network dongle-based versions of Belkasoft X, both regular and academic

Reason:

1. Dongle is not detected by the Guardant network server

   Solution: Make sure that the dongle is inserted to the server machine and is visible in the Web-interface of the Guardant Net Server (<server IPv4>:3185 by default).

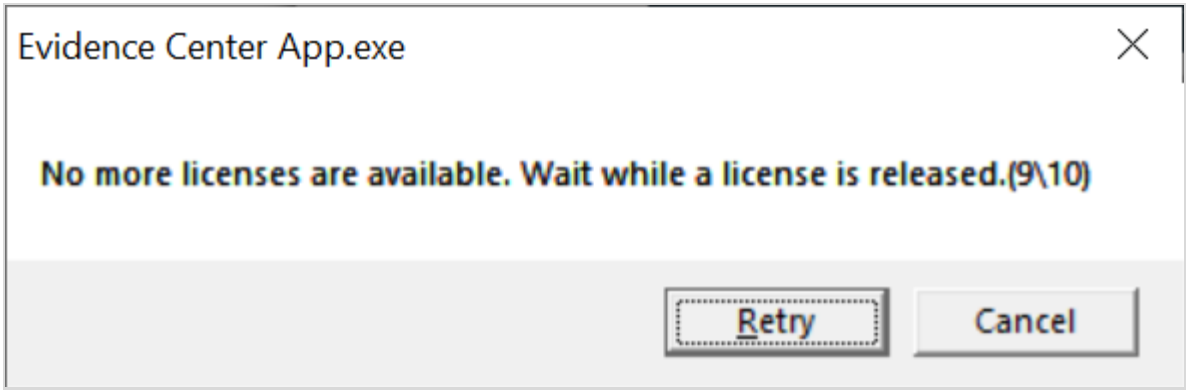
2. Hardware ID is missing in the license.xml on a client machine

   Solution: Contact support@belkasoft.com, provide the dongle number and attach your license.xml file, the license file requires correction.

3. Hardware ID in license.xml on a client machine does not match the actual dongle ID on a server machine

   Solution: Check if there is another dongle with matching ID and insert it to the computer with an installed Guardant Network Server. Contact support@belkasoft.com, provide the dongle number and attach your license.xml file, you will be either shipped with another dongle or receive another license.xml file.

Message: No more licences are available. Wait while a licence is released



Prerequisites: network dongle-based licence, both standard and academic

Reason: the number of available client connections is exceeded

Solution: Contact sales@belkasoft.com and purchase additional user connections or disconnect one of the previously connected clients.

Message: This version of Evidence Center X can be used with the fixed license only. Please download corresponding installation from your Customer Portal

Or

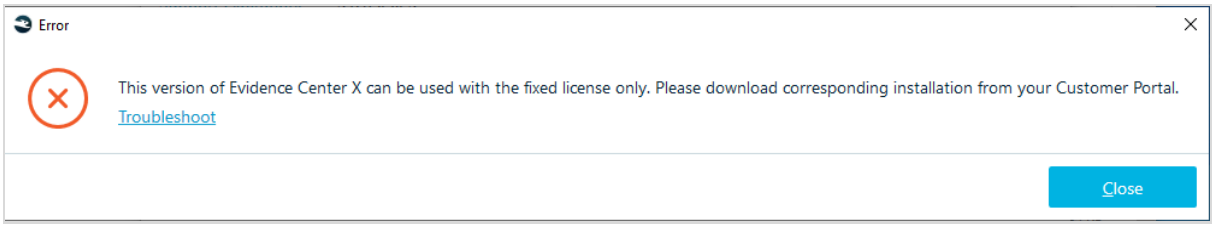
This version of {0} can be used with the floating license only. Please download the corresponding installation from your Customer Portal.

Or

This license can be used with the academic version of {0} only. Please download the corresponding installation from your Customer Portal.

Or

This version of {0} can be used with the academic license only. Please download the corresponding installation from your Customer Portal.



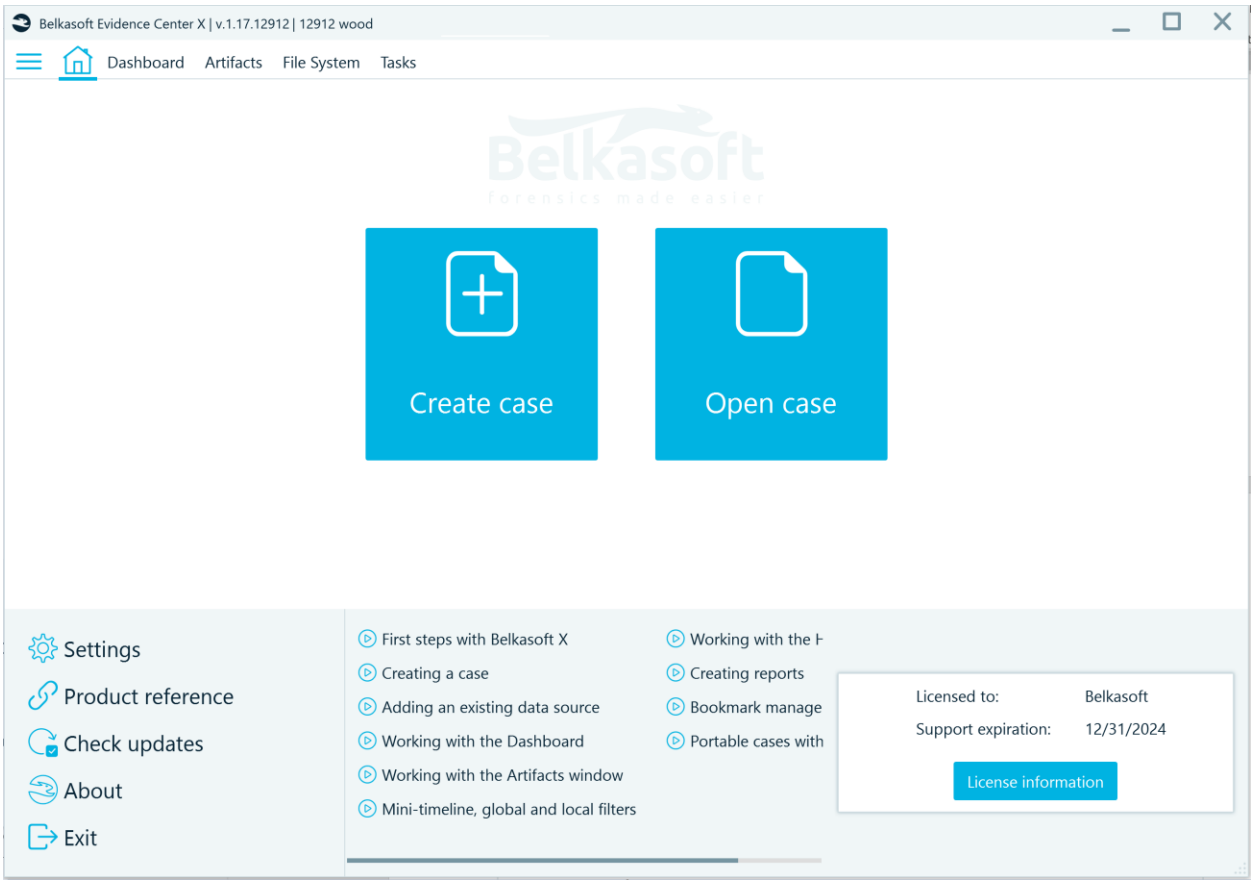
Prerequisites: Fixed, floating, academic builds when license.xml is chosen during the license activation procedure or upon the application's launch

Reason: The license and the build do not match, e.g. a floating license.xml is being applied to a fixed build

Solution: Log into the customer portal and download an installation package with a corresponding license.

Home screen

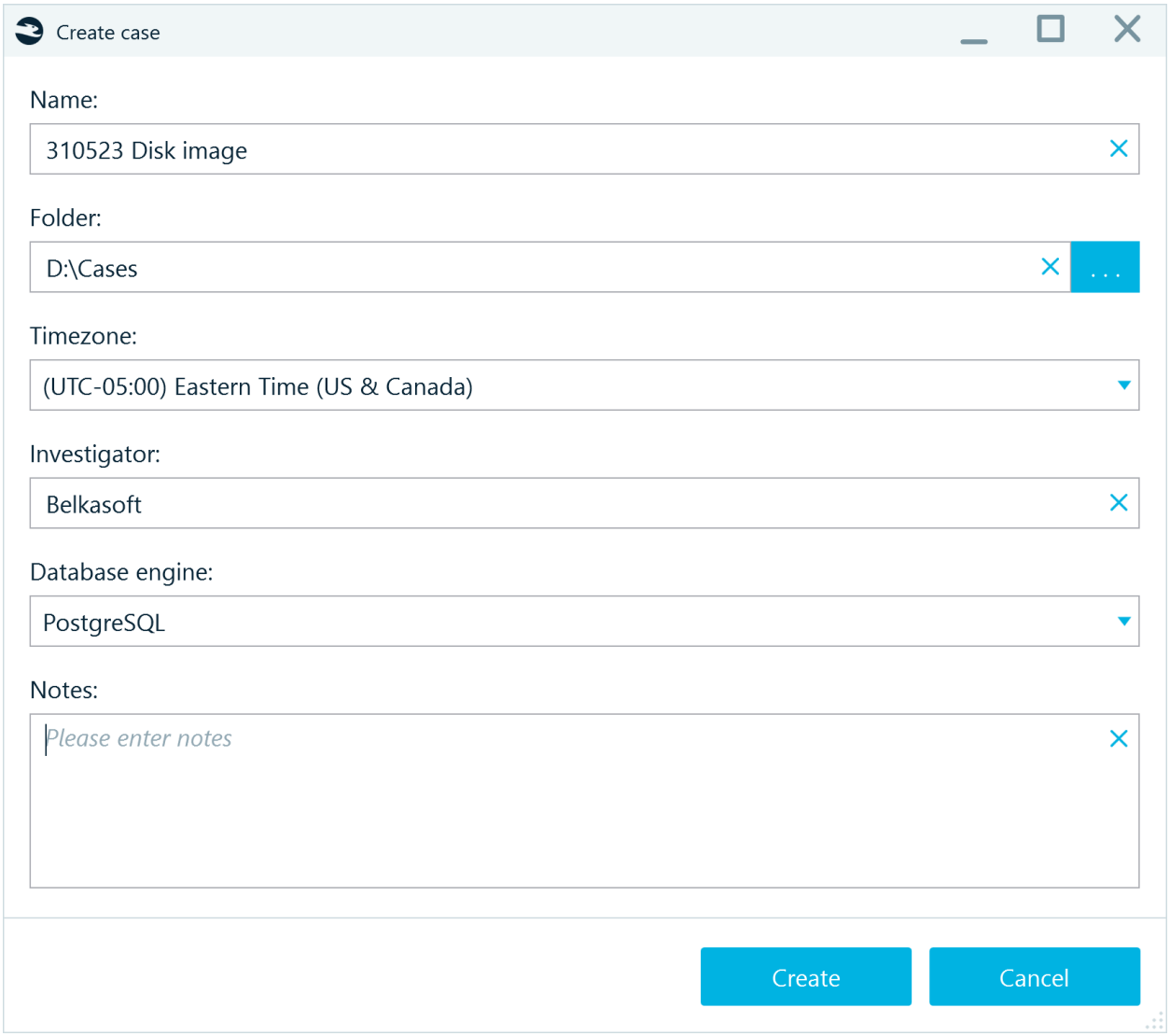
After opening **Belkasoft X**, you will first see the **Home** screen. To proceed, you need to create a new case or open an existing case.



Note: Belkasoft X can be run without administrative rights, although it is recommended to use admin rights if possible. Additionally, before launching Belkasoft X, you need to disable hibernation mode on Windows. If Windows goes into hibernation while Belkasoft X is running, the program may need to be restarted afterward.

Creating a case

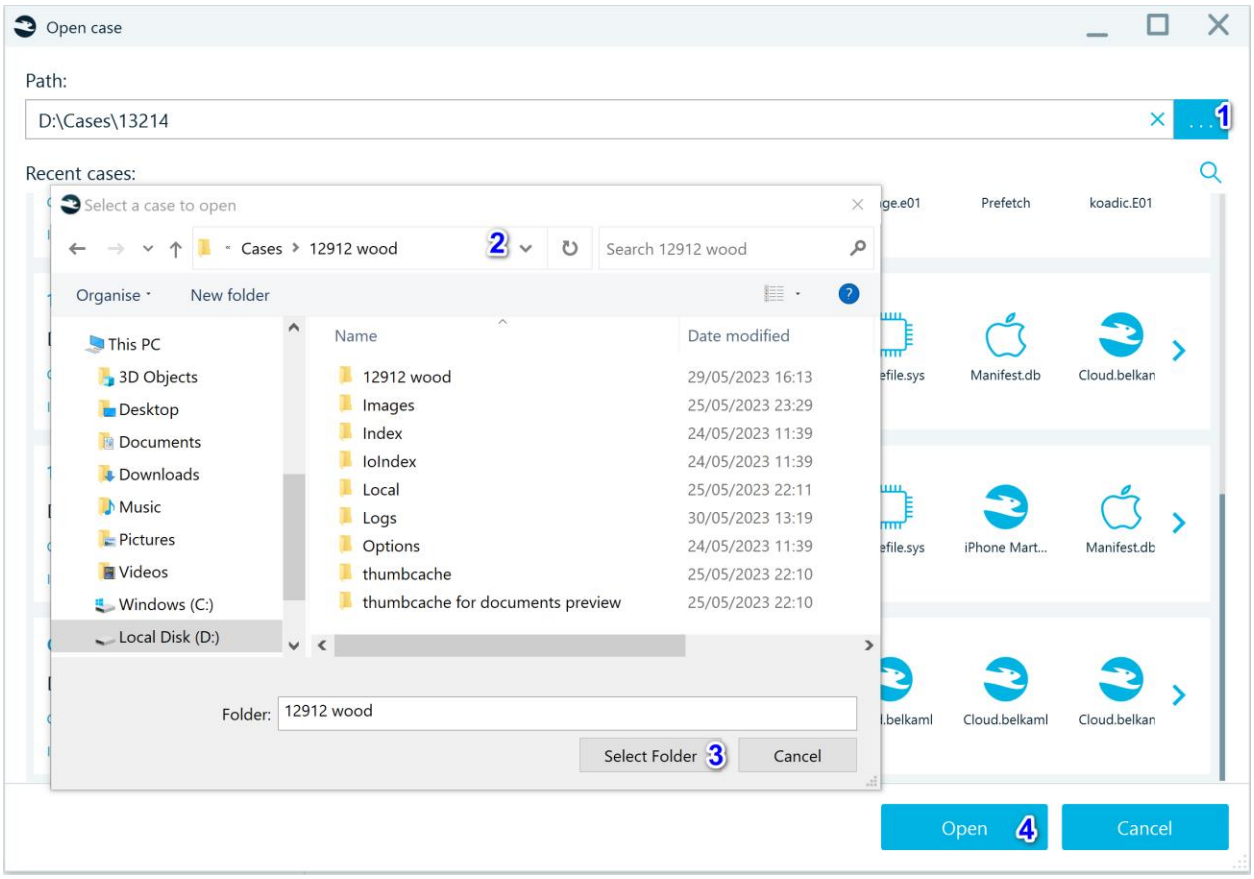
To create a new case, click on **Create case**. On the **Create Case** window, fill in basic details for the case. Click on **Create**.



Database Engine option allows to select a database: SQLite or PostgreSQL, depending on the complexity of the new case.

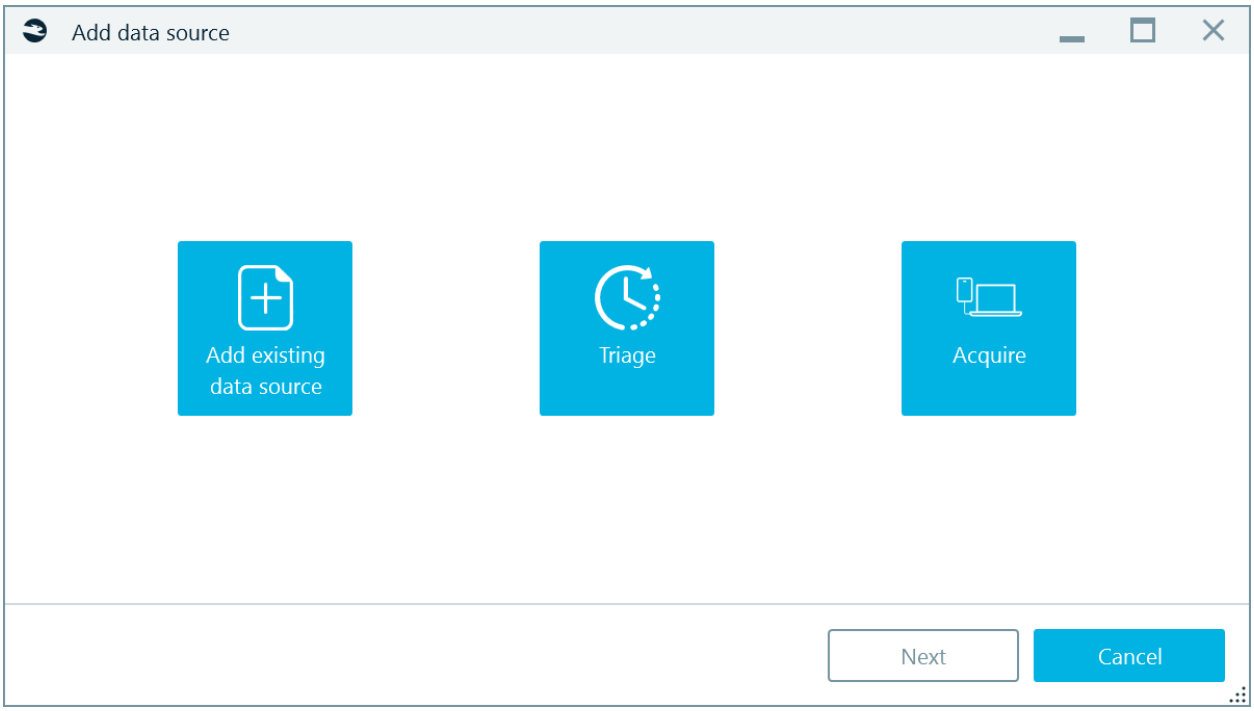
Opening an existing case

To open an existing case, click on **Open case**. Specify the path to the case folder and click on **Open**.



Adding a data source to a case

When you create a case or open an existing case, Belkasoft X prompts you to add a data source to it. A data source can be an image, dump, folder, or even a live drive.

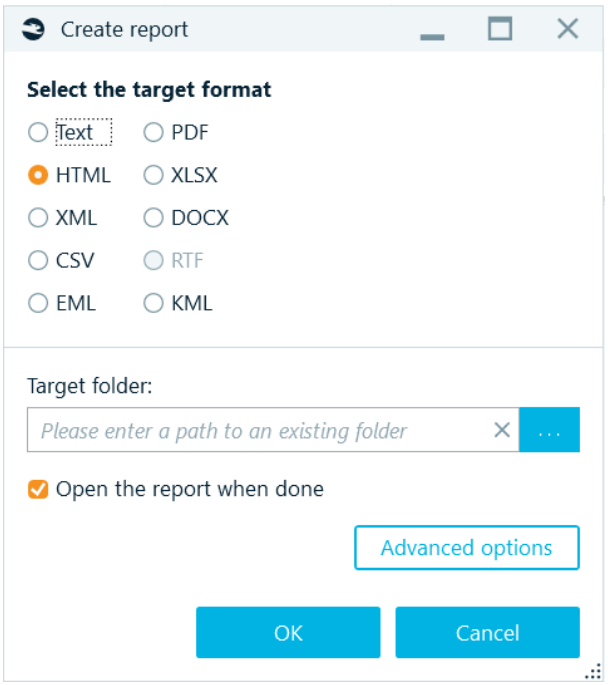


Creating a report

A report is the standard result of an investigation. Belkasoft X allows you to create reports in multiple formats for different data sets. You can create a report for a case, profile(s), selected artifacts, or a bookmark.

To create a report for a case, do this: Go to the **Dashboard** tab. Under **Actions**, click on **Create report**.

To create a report for an artifact, folder, or detail, do this: Click the item for which you want to create a report. Right-click on the item. Select **Create report**.



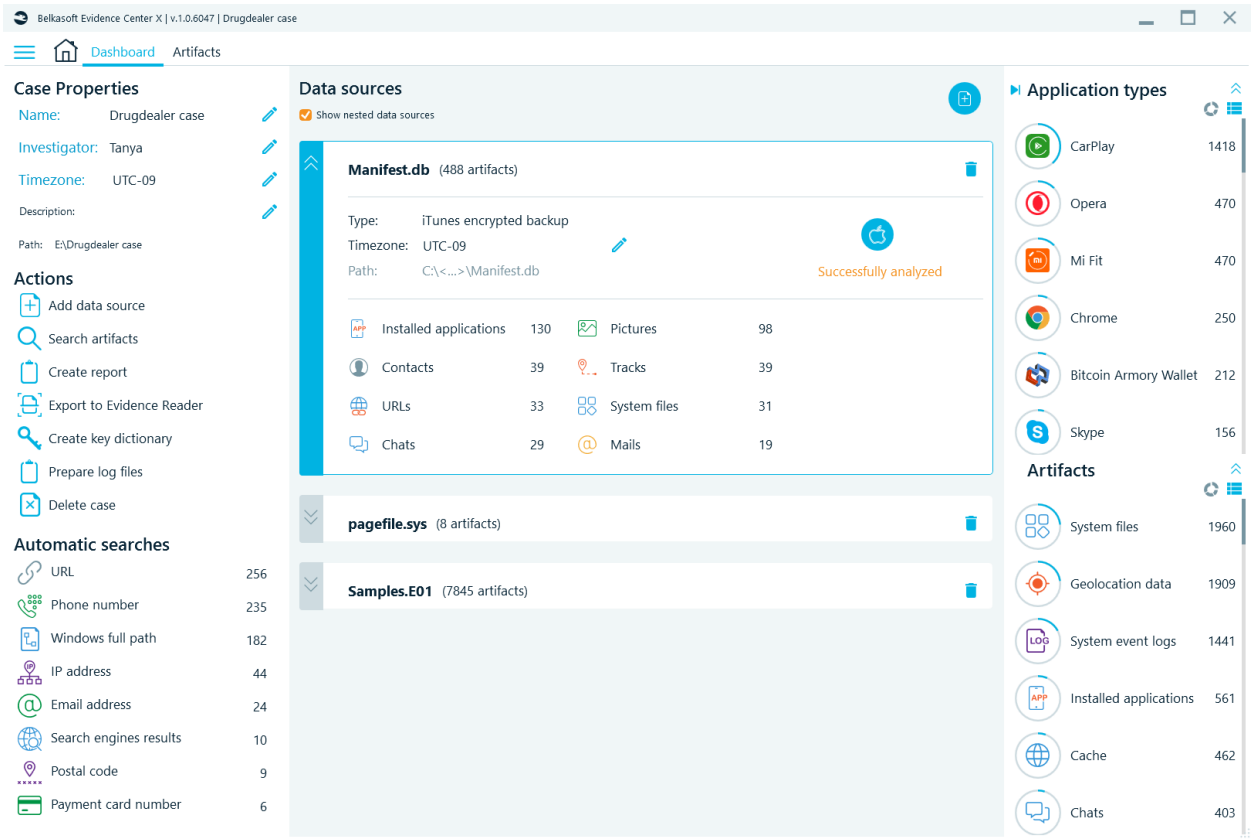
Choose your preferred target format. Specify the Target folder.

- If you want to view the report quickly after Belkasoft X creates it, tick the **Open report when done** checkbox.
- If you want to customize the report—in terms of formatting, style, and other attributes—click on **Advanced Options**. Continue on the screen presented.

On the **Create report** screen, click on the **OK** button.

Dashboard

When you open a case in Belkasoft X, **Dashboard** tab appears automatically. You can review the basic details for an open case, add data sources to a case, view automatic search results, and perform other tasks.

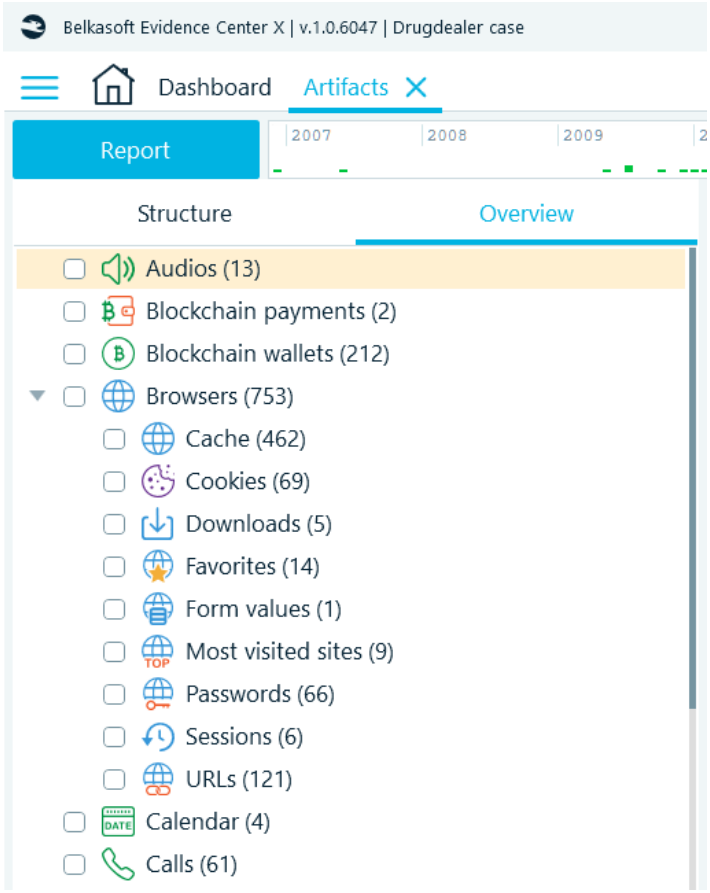


Artifacts

This tab displays items extracted out the box, such as documents, pictures, links, chats, and others. On the **Artifacts** tab, on the left pane, you should see **Structure** and **Overview.**

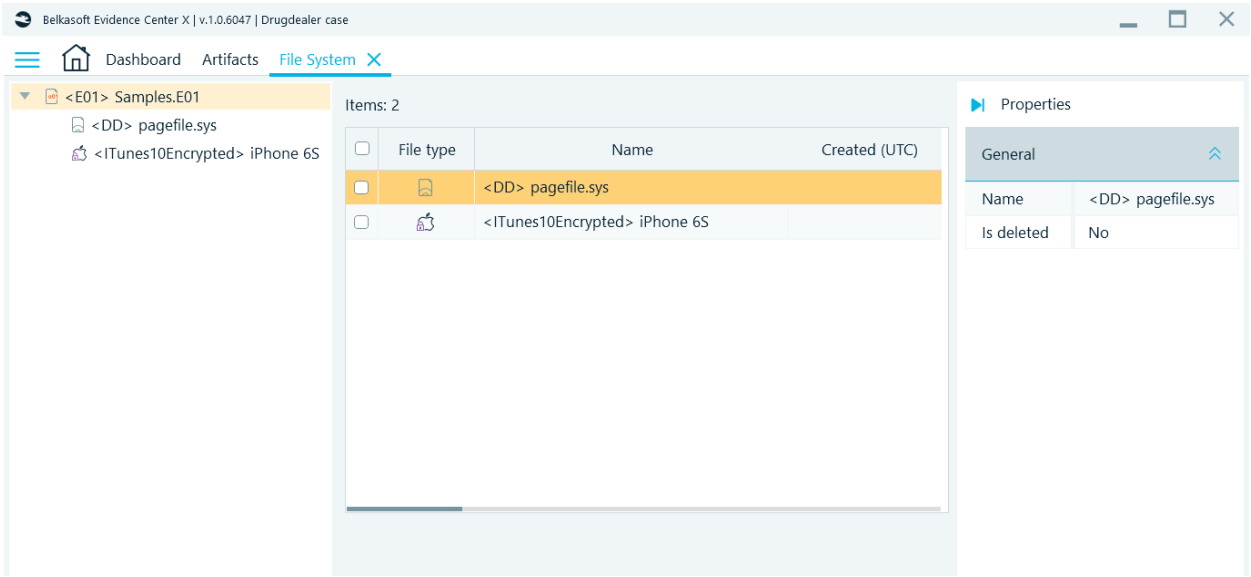
Under **Structure**, items are grouped based on their sources or locations. For example, if you add two different dumps or data sources containing chats for a case, Belkasoft X displays the chats under two different **Instant Messenger** nodes on **Structure**.

Under **Overview**, items are grouped based on their similarities. For example, if you add two different dumps or data sources containing chats, Belkasoft X displays all the messages for case—regardless of where they come from—under a single **Chat** node on **Overview**.

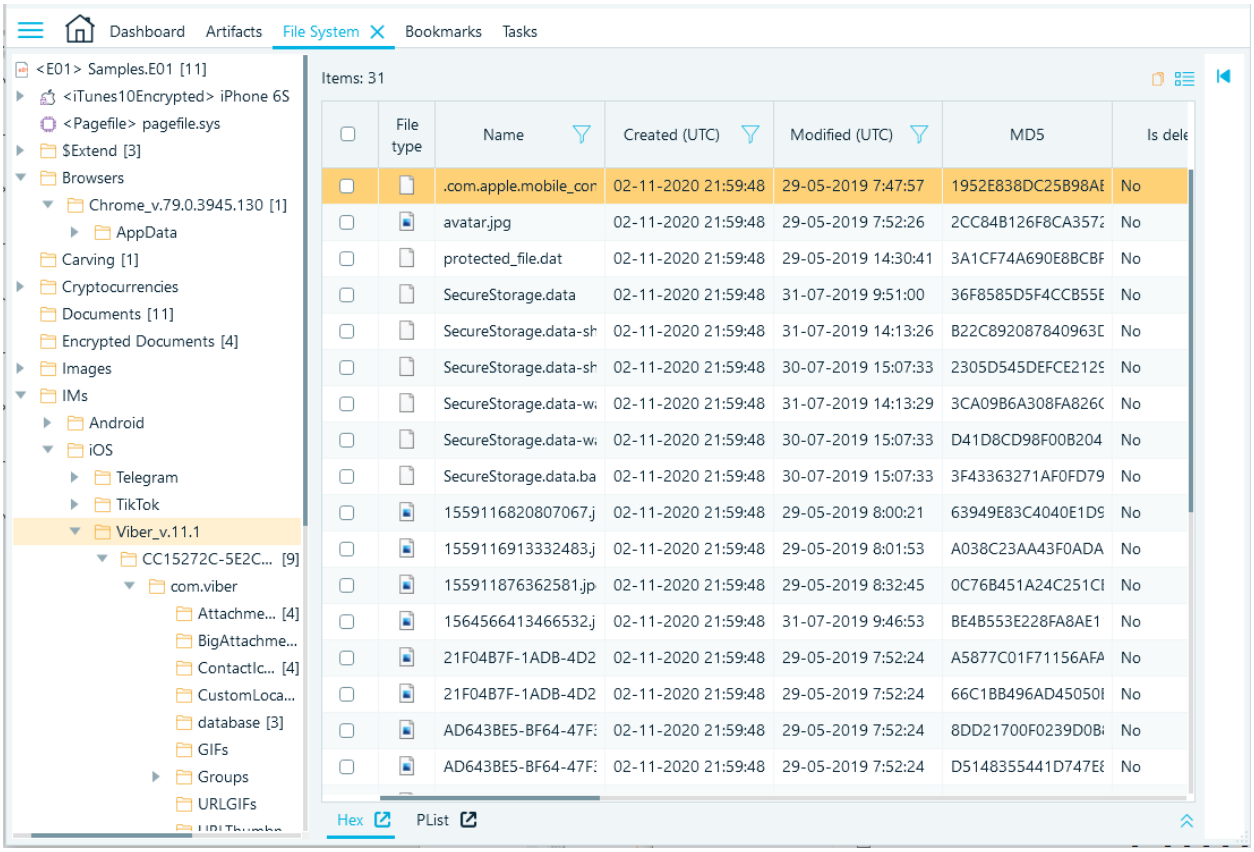


File System

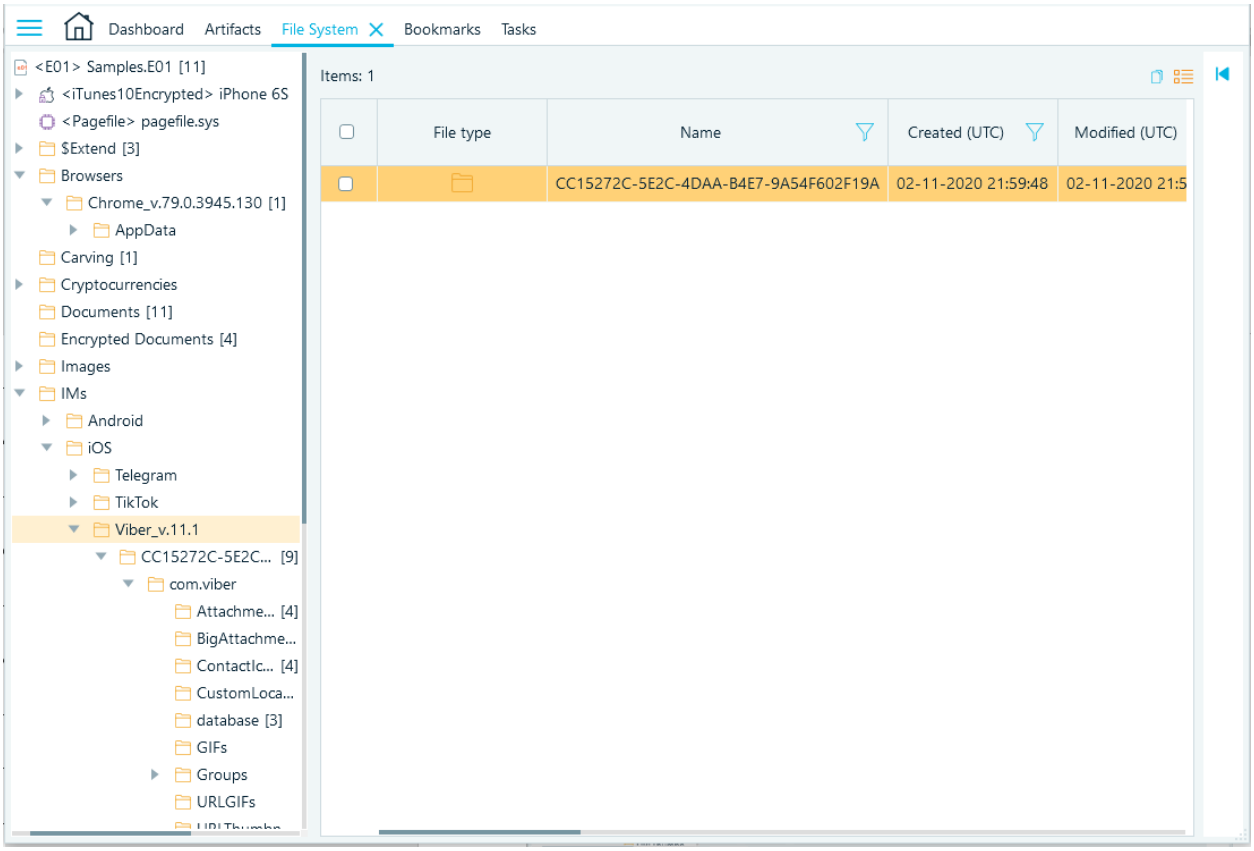
On the **File System** tab, Belkasoft X shows the structure of data sources added to a case. There, you can view partitions and volumes, folders and files, and Volume Shadow Copy snapshots. Belkasoft X also displays the memory processes for RAM dumps, options to detect malware and run hashset analysis.



Recursive view



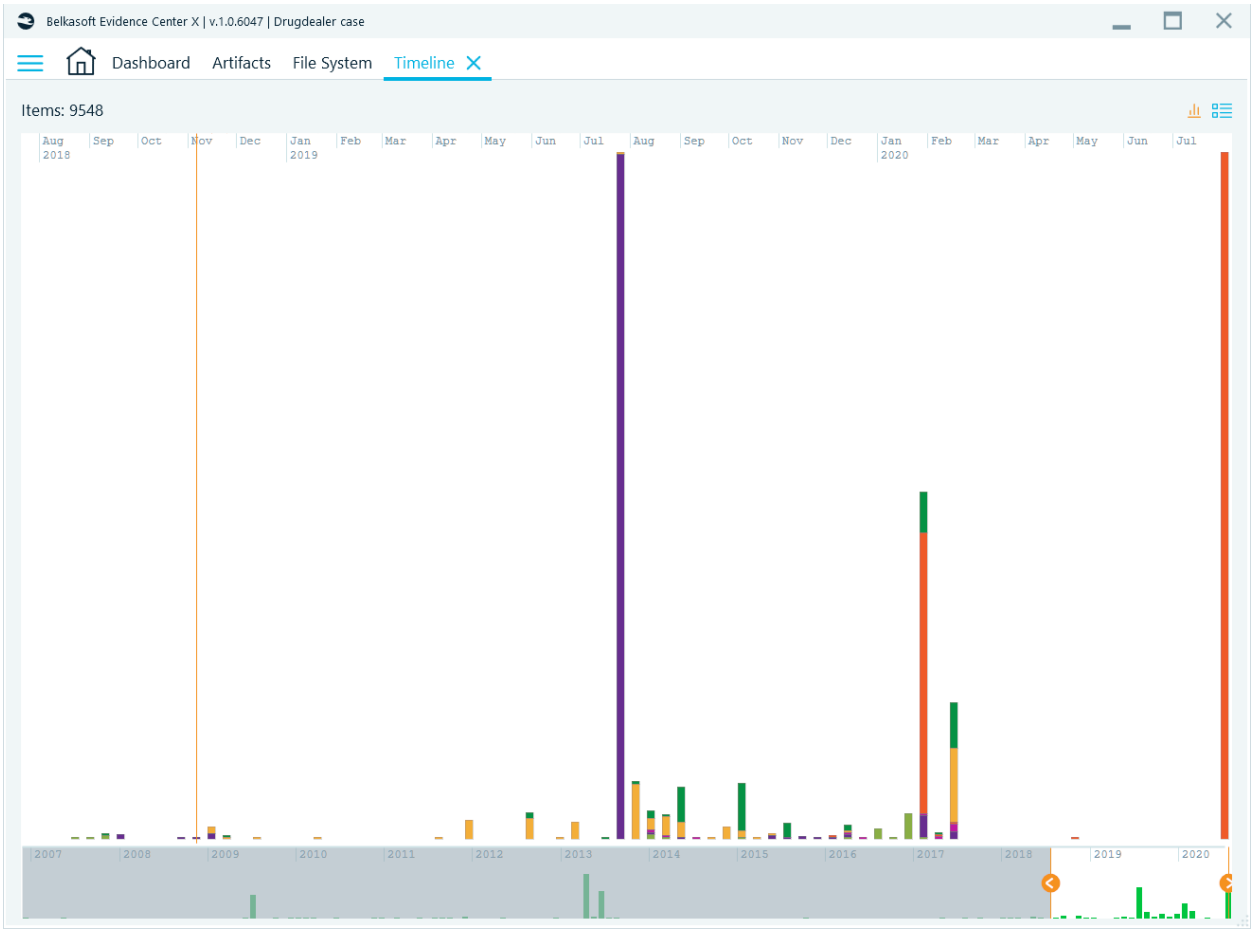
Grid view



Timeline

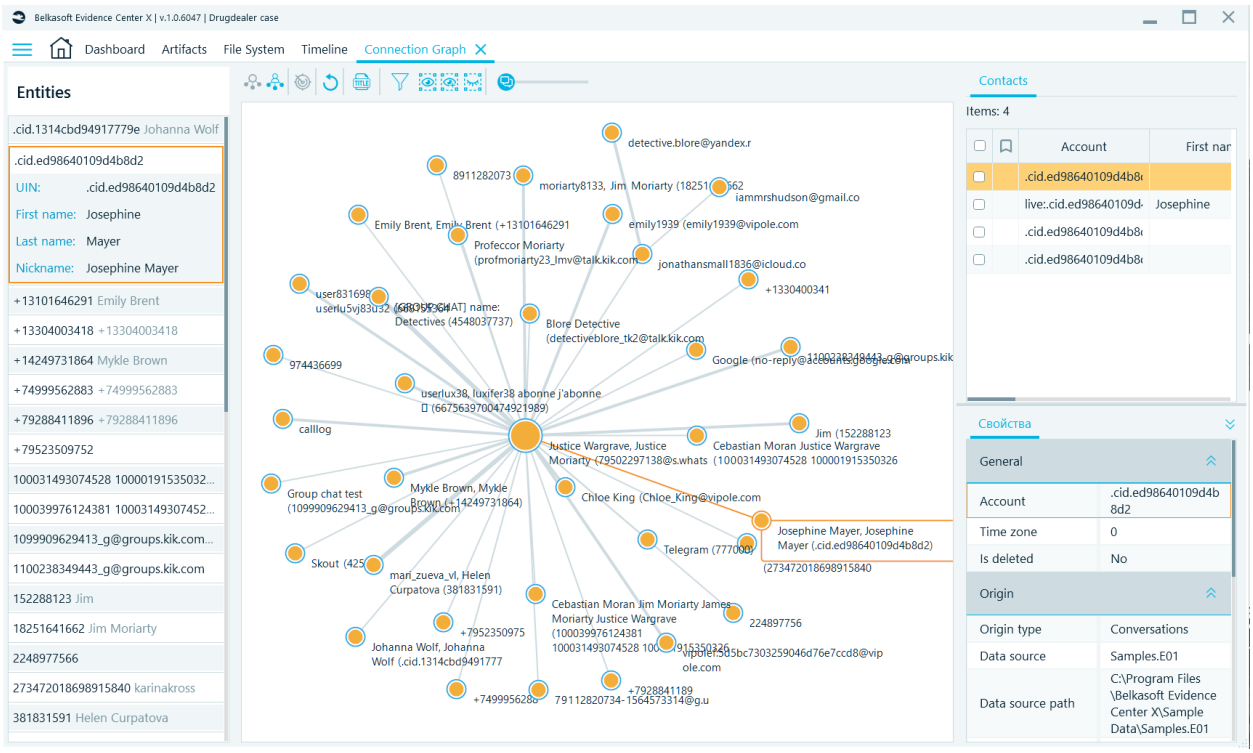
On the **Timeline** tab, Belkasoft X combines all the artifacts with date/time stamps—such as chats, emails, documents, and pictures—from a case and presents them together. Here, you can examine all events, which were happening at a given date or time on a device.

Some artifacts may appear twice on the **Timeline** tab—for example, a file-based artifact, such as a document, from different operating system times and with different Created or Last Access timestamps. Similarly, artifacts with metadata, such as a picture, may have several events recorded in it—for example, GPS time for shot or Date/time digitized. The described artifacts will appear with separate lines on the **Timeline**.



Connection Graph

On the **Connection Graph** tab, Belkasoft X displays a high-level visualization of interactions between people involved in a case. You may see individuals represented as dots (or avatars), which are linked together by lines—and this means the individuals interacted with each other (communicated) through calls, SMS, instant messenger chats, file transfer sessions, emails, and other means.

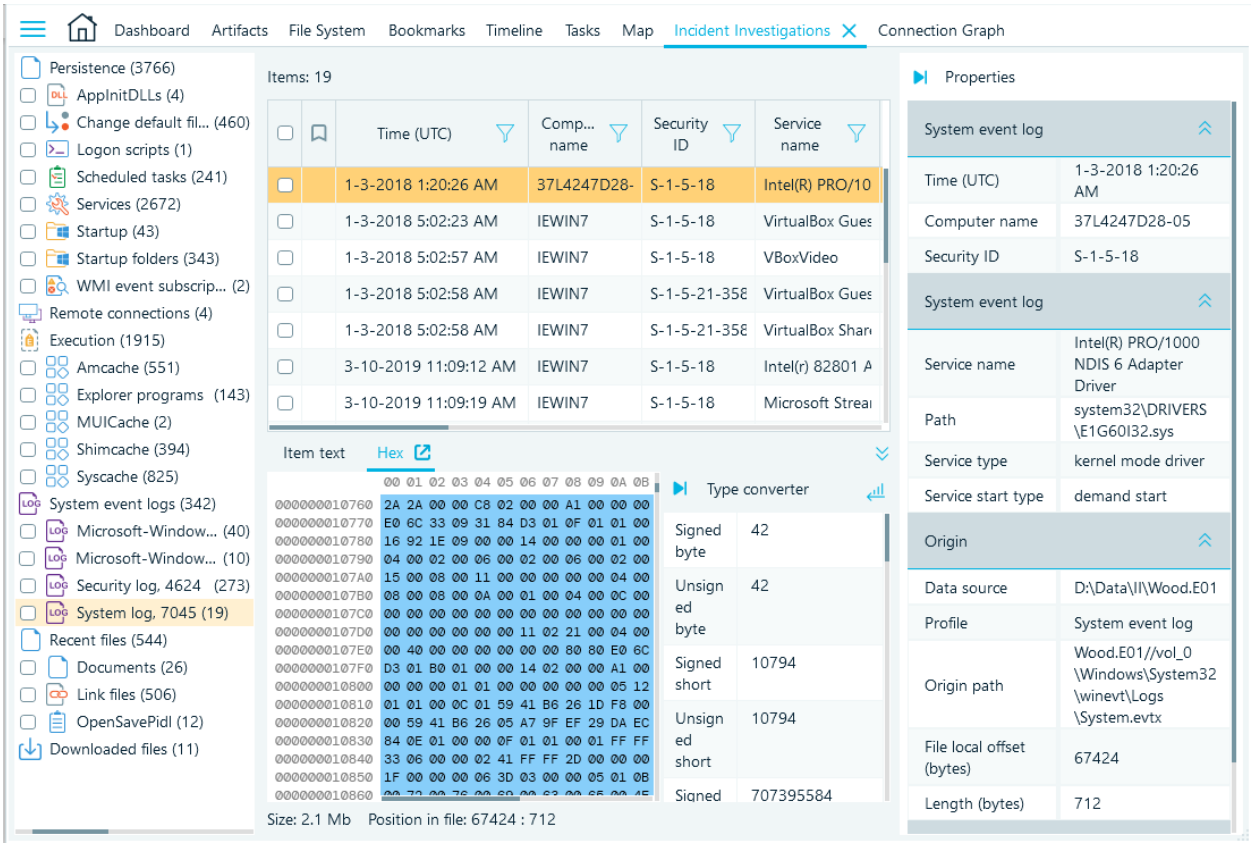


Incident Investigations

Information in **Incident Investigation** window is aimed to help users investigate hacking attempts of Windows-based computers. By analyzing numerous sources such as registry, event logs and memory dumps, it can find traces, which are typical to various tricks used by hackers to penetrate company's infrastructure.

Belkasoft X looks at various artifacts located inside Amcache, Shimcache, Syscache, BAM/DAM, AppInit DLLs, Change of default file association, scheduled tasks, remote connections (RDP, Remote Connection, TeamViewer and others), startup tasks, browser extensions and so on; it detects suspicious connections and scripts.

The results of analysis are then presented inside separate **Incident investigation** window, making it easy to separate suspicious activities from regular forensic artifacts.



Command Line Configurator

Command Line Configurator (CLi Configurator) is a powerful tool for conveniently creating a JSON file that is designed to be used through the command line. It helps automate analysis or acquisition quickly in Belkasoft X.

CLi Configurator allows user to:

- add data sources to an existing case or create a new one
- acquire an image of the logical and physical disks in E01, RAW formats
- acquire a Tableau image in Ex01, Lx01 formats
- analyze physical, logical drives, disk images, mobile images, folders, RAM
- build a report in one or several selected formats

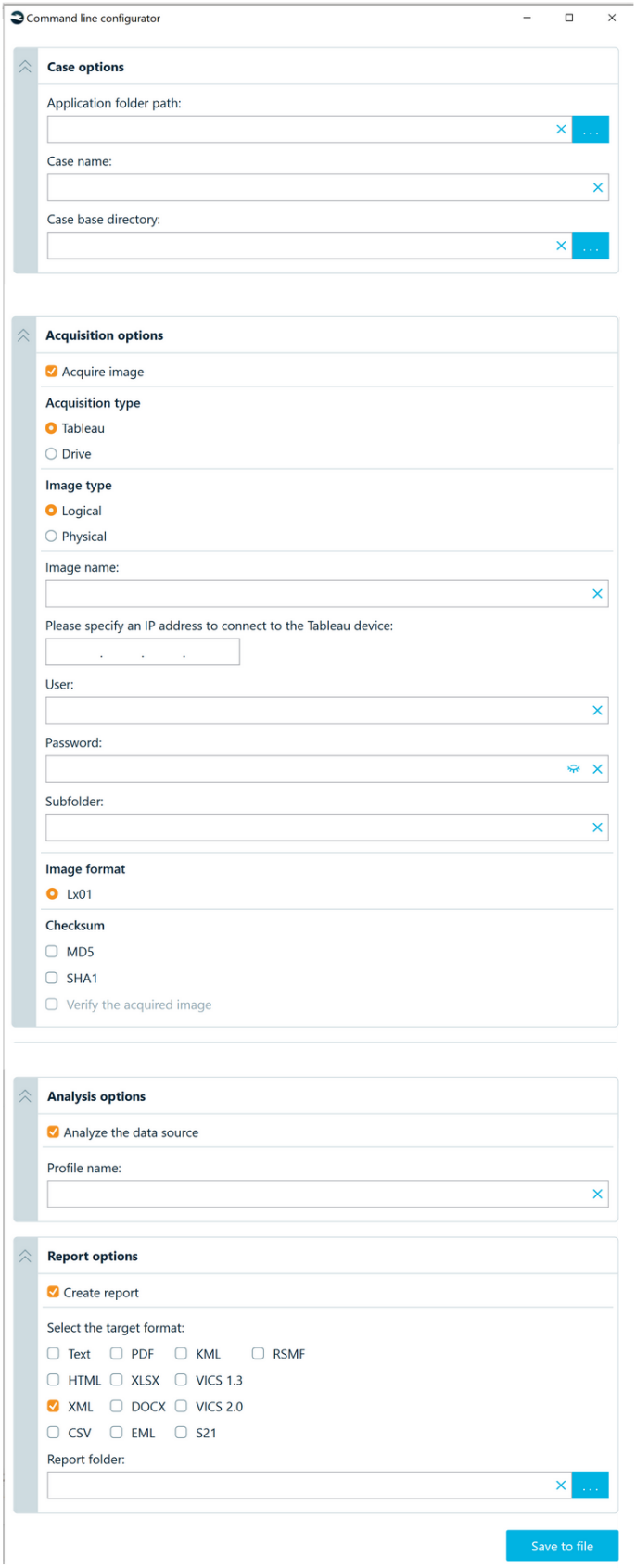
Belkasoft X can be launched from a **command line** with a variety of arguments, therefore, image acquisition and data analysis processes can be automated using scripts.

The command line should be executed with administrative privilege, otherwise a manual confirmation of the rights elevation is required.

To start, use the **Belkasoft.Cli.bat** executable file in the installation folder. All parameters which are necessary for the launch should be written in the JSON file.
Ways to set parameters:

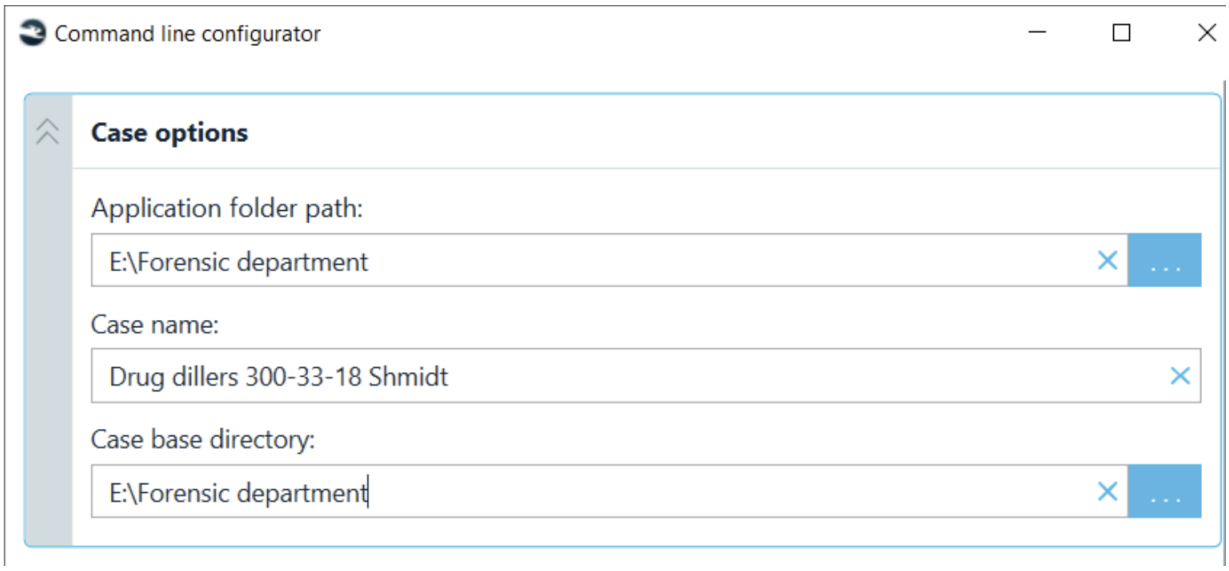
1. By running **Belkasoft.Cli.Configurator.exe** which located in the ..**[Installation folder]\App folder**
   Command line configurator has 4 sections (for all necessary parameters):

- Case options
- Acquisition options
- Analysis options
- Report options


Command line configurator
Case options
Application folder path:
Case name:
Case base directory:
Acquisition options
Acquire image
Acquisition type
Tableau
Drive
Image type
Logical
Physical
Image name:
Please specify an IP address to connect to the Tableau device:
User:
Password:
Subfolder:
Image format
Lx01
Checksum
MD5
SHA1
Verify the acquired image
Analysis options
Analyze the data source
Profile name:
Report options
Create report
Select the target format:
Text
PDF
KML
RSMF
HTML
XLSX
VICS 1.3
XML
DOCX
VICS 2.0
CSV
EML
S21
Report folder:
Save to file

Case options

Create a new case or add data sources to an existing case:

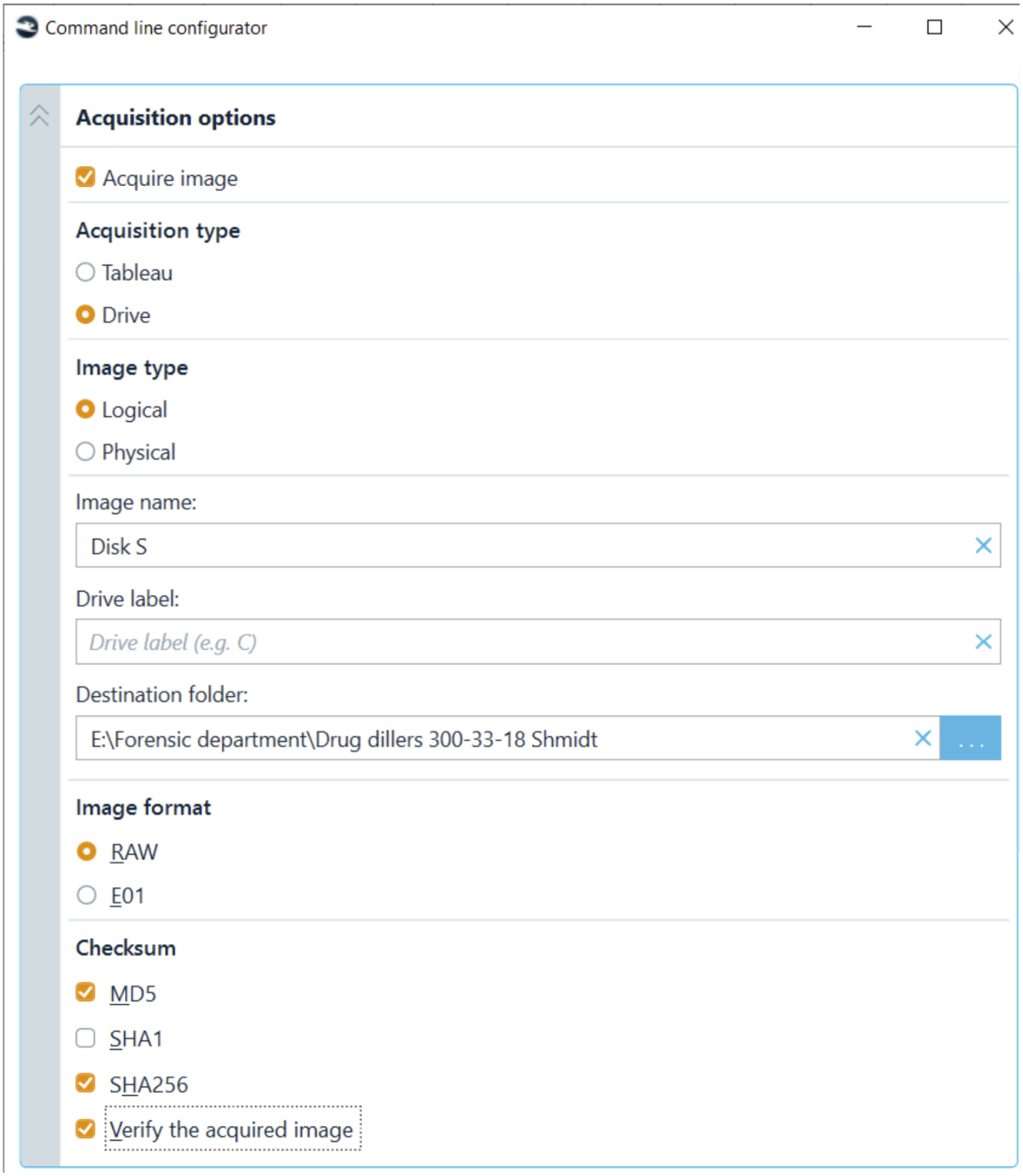


Acquisition options

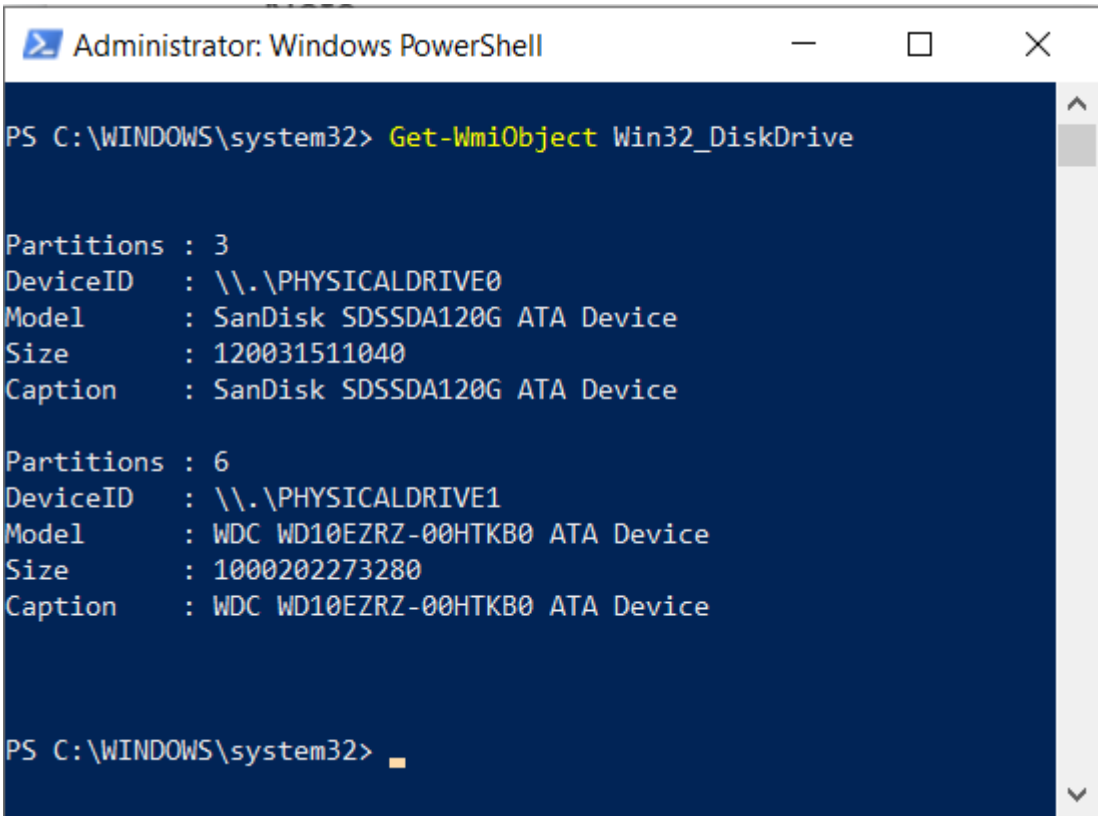
Acquire the image from the connected Tableau TX1 or the selected disk.

Select required options:

- **Type** logical or physical
- **Format** EX01, LX01 for Tableau; E01, RAW for disk image
- **Calculate hashes**: MD5, Sha1, Sha256



Note: In the case of choosing physical disk image acquisition (or analysis), it is necessary to specify the **DeviceID** of the physical disk. The list of physical disks can be obtained by using the **'Get-Wmiobject Win32_DiskDrive**' command in PowerShell (run in administrative mode).

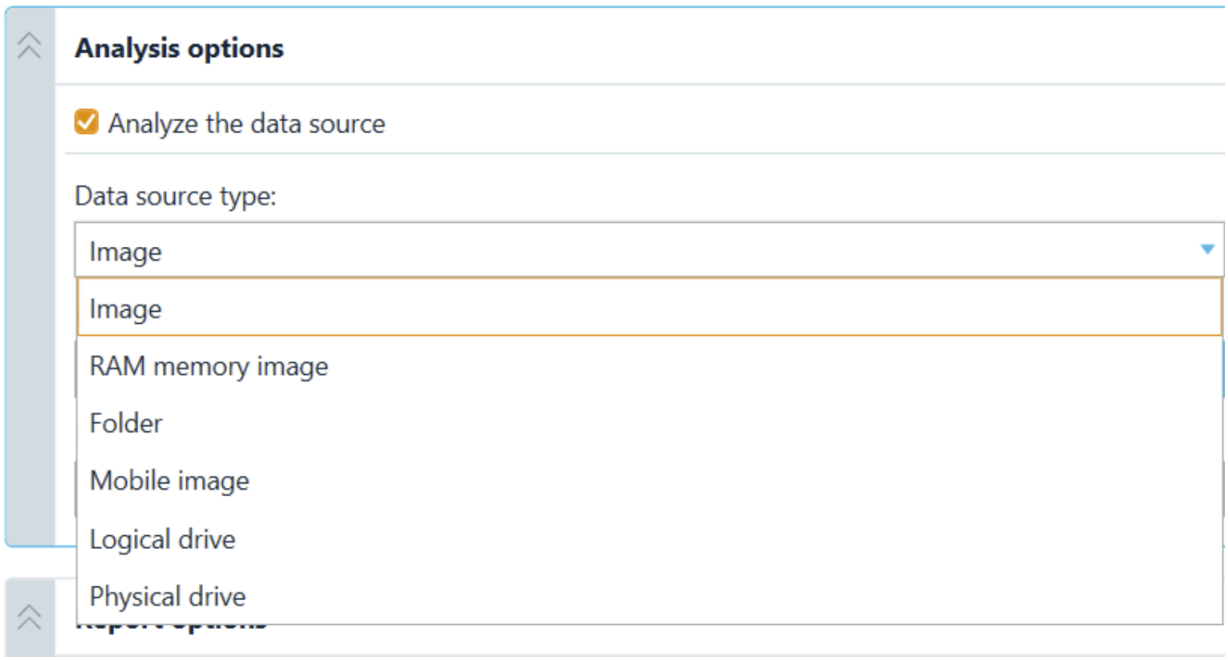


Analysis options

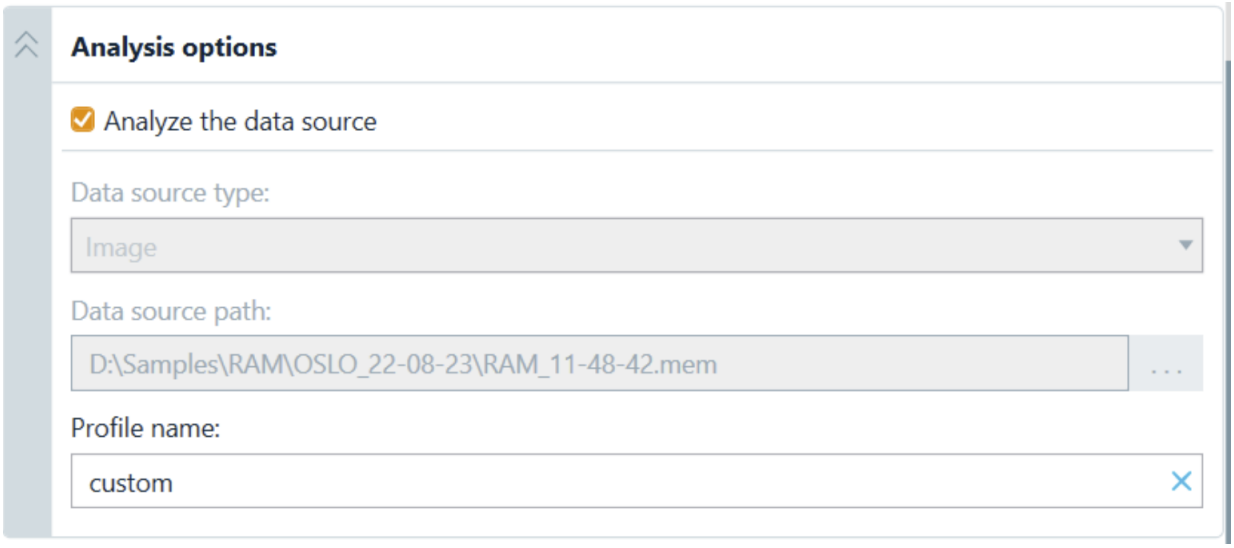
The CLi Configurator allows to analyze a data sources:

- Image
- RAM memory image
- Folder
- Mobile image
- Logical drive
- Physical drive

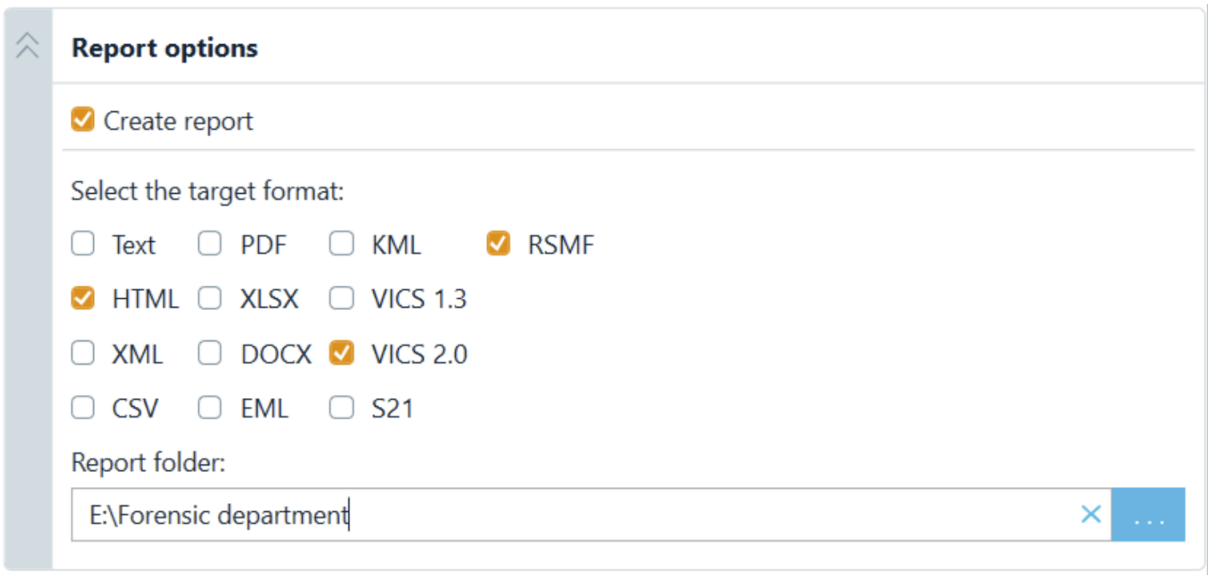
If no analysis is required, clear the **Analyze the data source** checkbox.



Set the name of the analysis profile.
Note: If the profile name is misspelled, the default profile named **Custom** will be used, which includes analysis of all source profiles.

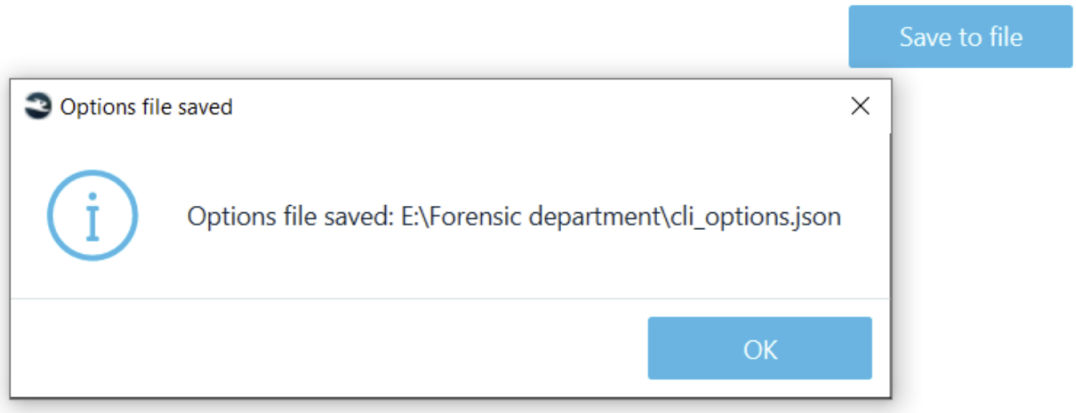


Report options



Save to file

Pressing **Save to file** saves the set options to JSON.



Example:

```
{
  "caseName": "Drug dillers 300-33-18 Shmidt",
  "caseFolder": "E:\\Forensic department",
  "appFolder": "E:\\Forensic department",
  "steps": {
    "analysis": {
      "sourceType": "image",
      "profile": "Custom",
      "sourcePath": "D:\\Samples\\DiskImages\\Washer 17.E01"
    },
    "report": {
      "format": "html, rsmf, vics20",
      "folder": "E:\\Forensic department"
    }
  }
}
```

2. Set parameters manually
   - Run Command promt as Administrator.
   - Navigate to the Belkasoft X installation folder
   - Run the following command: **Belkasoft.Cli.bat -optionsPath="[path to options JSON file]"**
     Example:**Belkasoft.Cli.bat -optionsPath="C:\Users\Path\To\options.json"**

The generated reports will open automatically upon completion of the tasks. Created cases can be opened in Belkasoft X.

Tableau Acquisition JSON file example:

```
{
    "caseName": "TestCase", //The case name
    "caseFolder": "D:\\Documents\\BelkasoftX\\Cases", //Application folder
    "steps": {
        "acquisition": {
            "acquisitionType": "Tableau",//Only Tableau acquisition is available now
            "tableauOptions": {
                "imageType": "Logical", //Logical or Duplicate
                "hostAddress": "192.168.0.21",
                "user": "user", //The real user credentials
                "password": "password",
                "destinationSubfolder": "Images\\tableau_test\\test",
                "imageName": "new_image"
            }
        },
        "analysis": {
            "sourceType": "image",
            "profile": "Custom" //Existing analysis profile
        },
        "report": { // Export options
            "format": "pdf", //Appropriate report format valid in Belkasoft X
            "folder":"D:\\Documents\\BelkasoftReports"  //Path to the report folder
        }
    }
```

```
}
```

Folder acquisition example:

```
{
    "caseName": "TestCase",
    "caseFolder": "D:\\Documents\\BelkasoftX\\Cases",
    "steps": {
        "analysis": {
            "sourceType": "folder",
            "sourcePath": "D:\\Documents\\BelkasoftX\\Pictures\\Face Detection",
            "profile": "Images"
        },
        "report": {
            "format": "pdf",
            "folder": "D:\\Documents\\BelkasoftReports"
        }
    }
}
```

The list of the command line arguments:

- ***createCase***
  Creates a new case in the indicated directory
- ***caseName***
  Sets a case name, should be unique
- ***caseFolder***
  Path to the Application folder for cases, use a directory with enough free space in it. If this folder does not exist, it will be created automatically. Use “\\” characters to indicate a path
- ***caseBaseDir***
  Indicates a directory, where a new case will be created. If this folder does not exist, it will be created automatically. If the path contains spaces, use double quotes “”
- **dataSourcePath**
  A path to a data source. If the path contains spaces, use double quotes “”
- **analysisType**
  Specifies a type of the analyzed data source
  The list of the analysis type arguments:
  - ***image*** a data source is an image
  - ***mobile*** a data source is a mobile image
  - ***ram*** a data source is a memory dump
  - ***folder*** a data source is a folder
- **profile**
  Specifies an analysis profile, the profile should be existing
- ***acquisitionType***
  Disk, Mobile, Cloud, Tableau
- ***sourceType***
  Specifies a type of the analyzed data source
- **imageType**
  Logical, Duplicate (for Tableau)
- **hostAddresses**
  Host where Tableau is plugged in

- **user, password**
  User credentials
- **destinationSubfolder**
  Parameter specifies a path from the shared folder (Tableau destination) to the file itself. For example, when the Destination "\\shared\drive\X" is selected on a Tableau device, a path to an image will look like this: \\shared\drive\X\<destinationSubfolder>\<imageName>.Lx01
  where destinationSubfolder and imageName are taken from the options.
- **imageName**
  The name of the created image
- **profile**
  Use an existing analysis profile
- **format**
  Select an appropriate report format valid in Belkasoft X: pdf, html, txt, rsmf, csv, xml, docx, xlsx, eml, kml, vics, s21
- **folder**
  Destination report folder

Note: When running the analysis from the command line, decryption tasks will be skipped (for such tasks use launch from GUI).

Belkasoft also offers an API to automate data analysis. Please contact support@belkasoft.com for more information.

How to report a problem

If you wish to report a problem with Belkasoft X, you can send logs to our support service.

By default, all logs are stored together with other case data in this location:
C:\Users\[YourAccount]\AppData\Roaming\Belkasoft\Evidence Center X\[Case Name]\Logs.

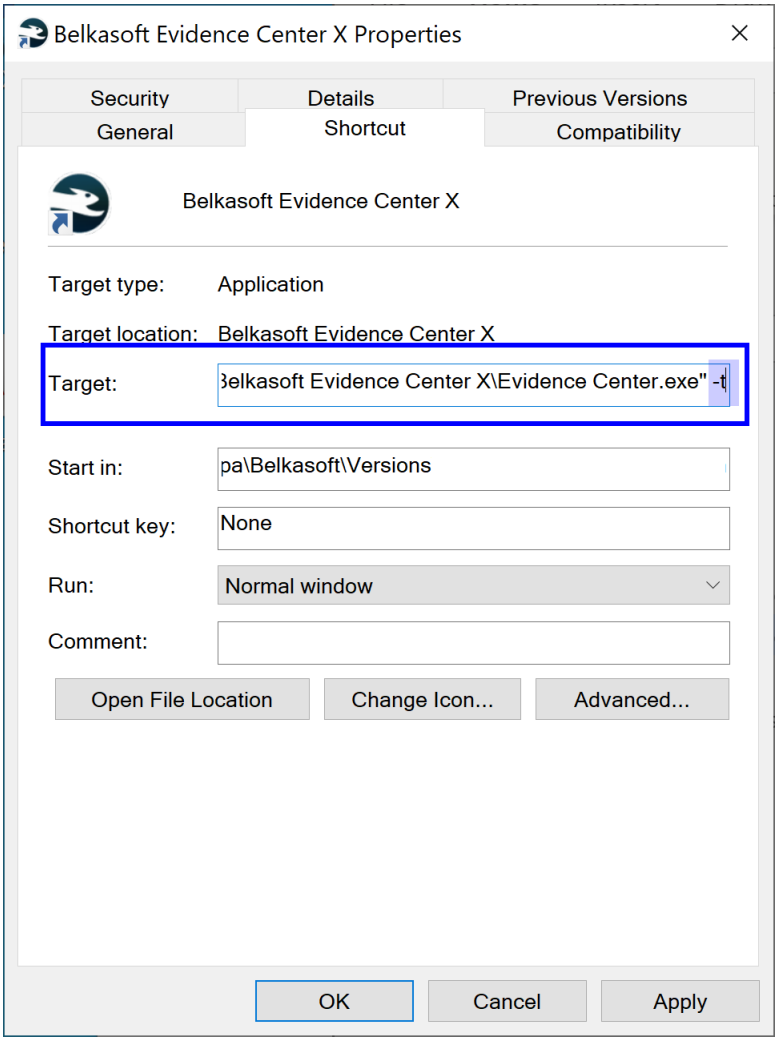
If Belkasoft X fails to start, find a file with name "[date]_[time].AppLog", located in C:\Users\[YourAccount]\AppData\Roaming\Belkasoft\Evidence Center X\Logs, and send it to support@belkasoft.com.

Extended logs

Usually extended logs contain more useful information. How to get it?
There are two ways to launch Belkasoft X in the extended logs mode - via shortcut properties or via the command line.

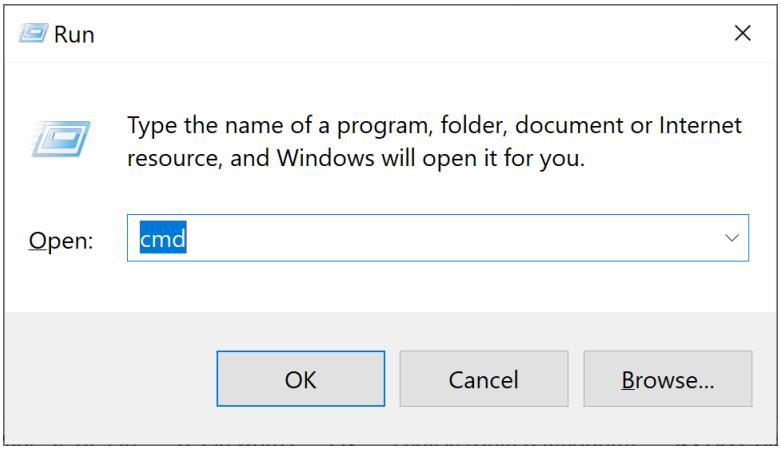
Extended logs mode via shortcut properties

Right-click on the Belkasoft Evidence Center X shortcut and choose **Properties** from a dropdown menu. On a **Shortcut** tab go to the **Target** field and after the closing quotes type argument **-t** separated by a space. Apply the changes and launch Belkasoft X using the altered shortcut.
Note: You will need to provide administrator permission to change these settings.

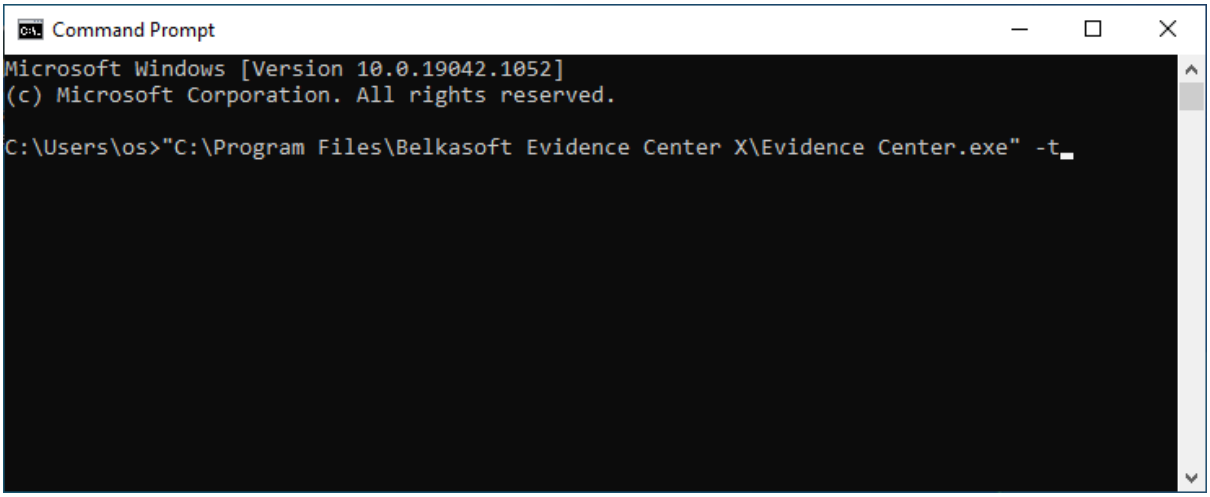


Extended logs mode from a command line

Open the **Run** box (press buttons Windows + R). Type “cmd” into the box and then press Ctrl+Shift+Enter to run the command as an administrator.



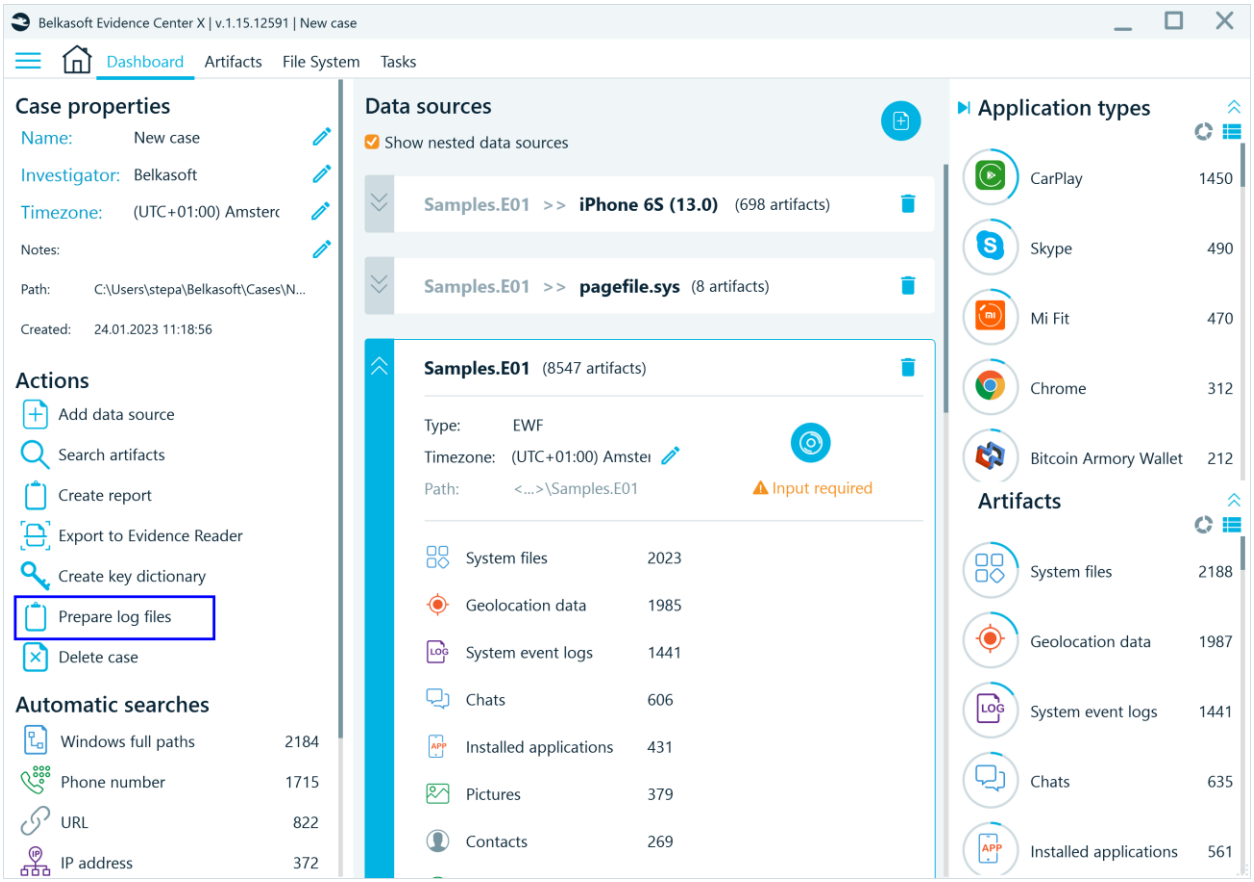
Then start the product from the command line with the argument -t:

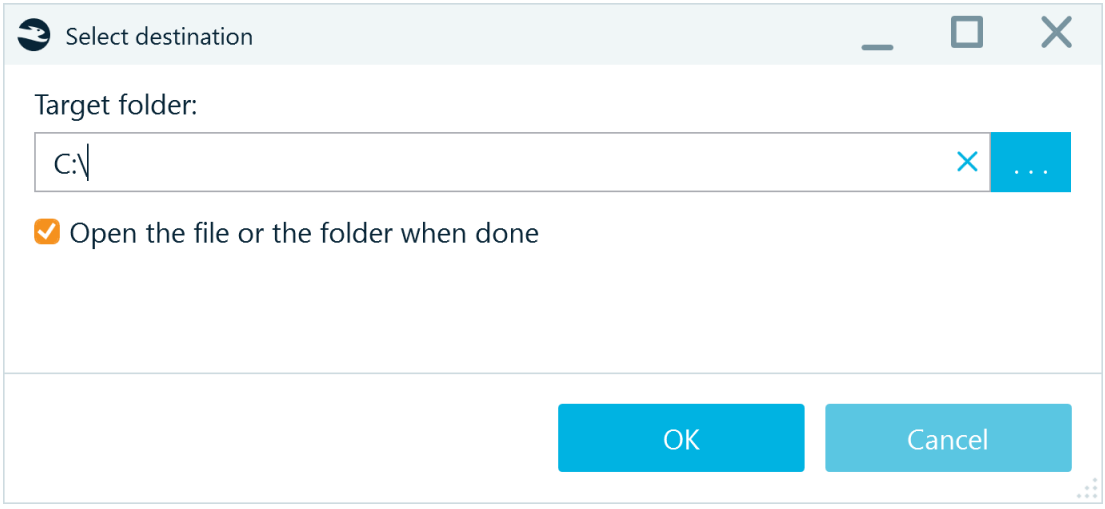


Preparing a file with multiple logs

Logs can be exported from Tasks or Dashboard windows of Belkasoft X.

More often it's required to send all logs. To do so, switch to Dashboard window of Belkasoft X and in **Actions** section click on the button **Prepare log files**. In the opened dialog select the folder, where your logs should be saved.
Send the resulting archive to support@belkasoft.com.



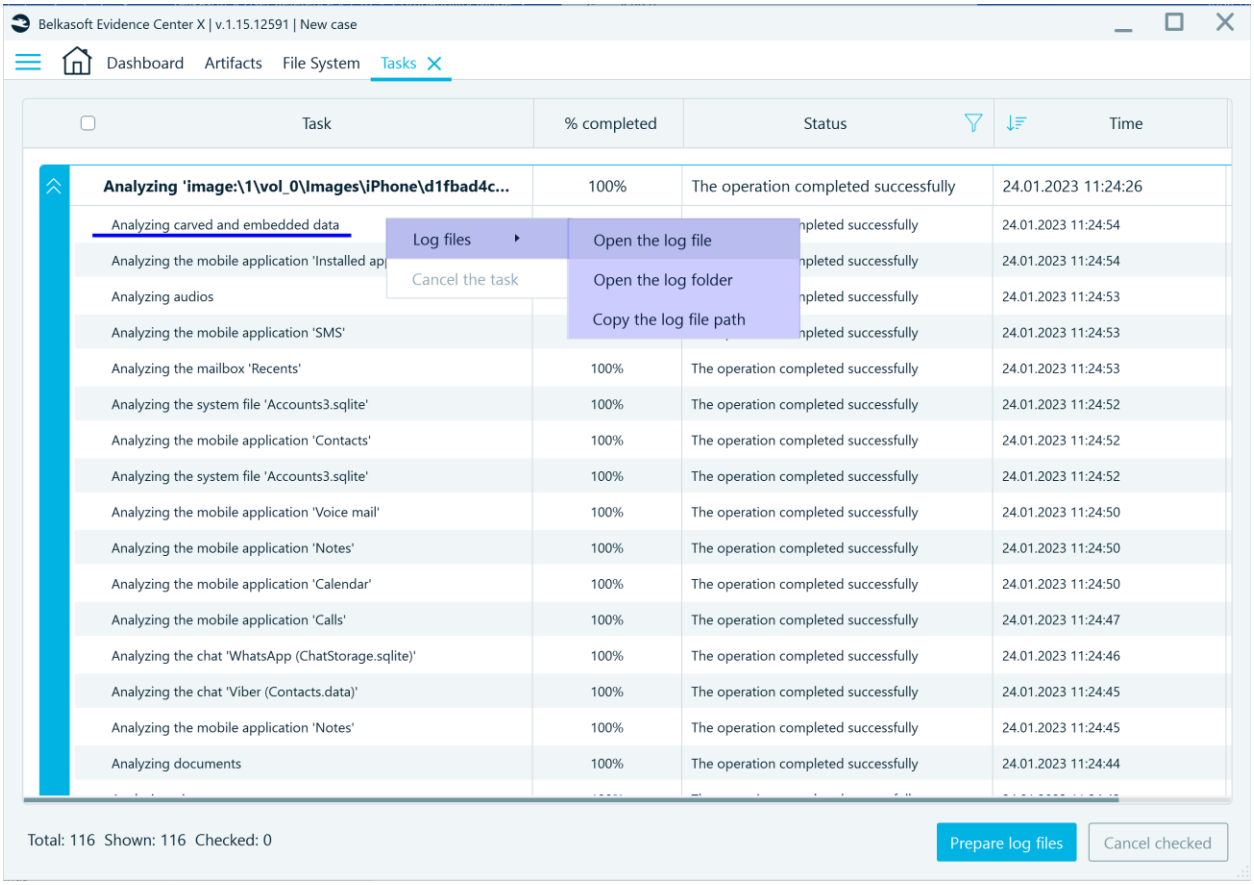


Preparing a file with a single log

If there was only one task that the product failed to complete, in Belkasoft X's Tasks window simply double-click on the operation and the log for this process will appear. Or open drop-down menu and select action:

- Open the log file
- Open the log folder
- Copy the log file path

Send log file to support@belkasoft.com with a description of what data source you are working with, what actions preceded the error, any screenshots you have to visualize the issue.



Belkasoft Evidence Center X Editions

Belkasoft X is offered in several editions.

X Computer

X Computer edition is a cost-effective solution developed specifically for investigators in local police departments, experts in small to medium consulting companies providing digital forensic and incident response services, and individual customers such as private investigators or digital forensic consultants. Customers who typically deal with only a few computer-related cases per year and/or have a limited budget will enjoy the very affordable price of X Computer edition.

Key features of X Computer edition:

- Extracts data from hard drives, mount and analyze hard drives, disk images, virtual machines, and RAM.
- Mounts third-party tools images (EnCase, FTK, X-Ways, etc.), L01/Lx01, DD, DAR images, archive files (such as .tar, .zip, and others).
- Examines and analyzes hundreds of artifacts: chats, browsers, mailboxes, documents, pictures and videos, and system files.
- Uses analytical features, such as **Connection Graph**, **Timeline**, advanced picture analysis.

- Performs in-depth examinations into the contents of files and folders on the device with **File System Explorer**. Find even more evidence with **Registry** and **SQLite Viewers**.
- Powerful file and data Carving features help to locate evidence that was deleted or hidden.

Belkasoft X Computer supports these data types:

- Audio
    - Belkasoft X supports dozens of formats, including ape, flac, m4a, mp3, ogg, wav, and others.
- Browsers
    - Belkasoft X supports all major web browsers—Chrome, Firefox, Internet Explorer, Edge, Opera, Safari, Baidu, Dolphin, Maxthon, Mercury, QQ Browser, 360 Browser, and others.
- Cloud applications
    - Belkasoft X supports popular cloud apps—Dropbox (with decryption), Google Drive, One Drive, Yandex.Disk, Flickr. Regards apps that lack installable clients, Belkasoft X analyzes RAM artifacts for their contents.
- Cryptocurrencies
    - Belkasoft X supports analysis tasks for Bitcoin, Bitcoin Core, and Ethereum (and the Jaxx app).
- Email
    - Belkasoft X supports all major email clients—Outlook, Outlook Express, Gmail offline, Mozilla Thunderbird, Windows Live Mail, The Bat, Apple Mail, and others.
- Encrypted files and volumes
    - Belkasoft X supports over 300 encryption types
      Encrypted File Systems such as Bitlocker (used in Windows), APFS, FileVault, McAfee, PGP, TrueCrypt, VeraCrypt;
      Encrypted chats: WhatsApp (Android) crypt 7, crypt 12, crypt 13, crypt 14, Signal (Android), Signal (iOS), WeChat (Android), WeChat (iOS), Telegram (Windows), Wickr (iOS), Wickr (Windows);
      Dropbox profile, Google sync data, Microsoft Office documents, archives (7z, RAR, and others), encrypted iTunes backups, and others.
- OLE containers and yEnc files.
- Instant messengers
    - Belkasoft X supports all popular instant messenger apps and services, such as WhatsApp, Telegram, Facebook Messenger, Skype, WeChat, SnapChat, and more.
- Geolocation data
    - Belkasoft X can extract geolocation information from images (with GPS tags in their EXIF metadata), Google Maps browser queries, geolocation details shared in chats, fitness trackers location data, and others.
- MMORPG
    - Belkasoft X can extract data for MMORPG games—Karos, Lineage, World of Warcraft, — from RAM dumps.
- Peer-to-peer (P2P) clients
    - Belkasoft X can analyze popular Windows P2P clients, such as Ares Galaxy, Emule, Frostwire, Gigatribe, Limewite, Shareaza, SHAREit, and Torrent.
- Payment systems
    - Qiwi wallets can be analyzed (also see above for Crypto currencies support).
- Pictures

    - Belkasoft X scans pictures and videos for EXIF data, pornography, skin, faces, scanned text, and guns.
    - Grouping similar faces found in pictures.
    - Belkasoft X supports more than 90 image formats, ranging from RAW camera formats to JPG, PNG, TIFF, HEIC and other widely used formats.
- Social network communications
    - From RAM dumps, Belkasoft X analyzes Bebo, Facebook, Facebook Messenger, OK (Odnoklassniki), OrKut, Twitter, and Vkontakte (VK).
    - Mobile apps support.
    - Extraction from browser cache.
- System files Belkasoft X supports:
    - Windows: Windows Event Log, thumbnails and thumb cache, registry files, jump lists, TOAST notifications, LNK files, Prefetch, Windows 10 timeline, and others.
    - macOS: System configuration, installed applications, Bluetooth configuration, WiFi connections, and others.
    - Native support for Windows registry files—Belkasoft X recovers badly damaged and partially overwritten registries.
    - Built-in **Registry Viewer** for viewing Windows registries (without third party applications).
    - Built-in **Plist Viewer** for viewing macOS system files (without the use of third party applications).
- Thumbnails
    - Belkasoft X can analyze thumbnail files for Android, iOS.
- Videos
    - Belkasoft X can find videos in over 30 formats, such as AVI, MOV, MTS, WMV, and others.
    - Belkasoft X supports keyframe extraction for supported video files. An appropriate codec must be installed on the machine.
- Webmail
    - Belkasoft X can detect webmail traces—for Gmail, Yahoo mail, and others— through Live RAM analysis.

Note: As additional artifacts become supported in new Belkasoft X releases, the contents of the list above may change depending on the Belkasoft X version.

Supported acquisition types

Belkasoft X supports several local acquisition methods for devices.

- Active Windows machine RAM (volatile memory)—through the Live RAM Capturer tool bundled with Belkasoft X installation package.
- Hard and removable drive acquisition to raw or E01 format.
- Cloud acquisition for many cloud, social networking, and webmail services
    - Belkasoft X currently supports these services: Google Drive, Google Timeline, Gmail, Instagram, and over 30 webmail providers (Yahoo, Hotmail, QQ, and others).

Note: To learn more about the different acquisition types—especially their pros and cons, when they are suitable for use, and other variables—you can sign up for a course at Belkasoft forensic training.

Supported extraction types

Belkasoft X extracts and recovers artifacts using different techniques:

- Analyzing existing files.
- Carving (signature-based analysis) deleted or hidden data—unallocated or slack space or free space—on a hard drive or an image.
- Carving RAM dump; Analyzing live memory to extract social network remnants (Facebook, Twitter, and others), web-based mails (Gmail, Hotmail, and others), cloud application data (Dropbox, Flickr, and others). Belkasoft X supports Volatility functions, you can read more about installation in the special section.
- Extract processes.
- Carving using custom signatures.
- Analyzing Volume Shadow Copy snapshots.
- Analyzing virtual machine files (without switching on the virtual machine).

Supported analysis types

Full-text search through all forms of evidence collected

- **Timeline -** to filter and present all user activities and system events at given dates on a single screen.
- Pictures analysis - to detect skin, guns, pornography, scanned texts, and faces.
- Geolocation data presentation on the **Open Street View** window or Google Earth third-party app.
- **Connection Graph** and its features—communication visualization and community detection—to show links between individuals and detect tightly connected groups.

Other functions

These functions are also included in Belkasoft X Computer configuration:

- Report creation in numerous formats, such as text (file), HTML, XML, CSV, PDF, RTF, Excel, Word, EML, KML, and JSON.
- Project Vic support.
- Sharing of findings—through Belkasoft Evidence Reader—with colleagues and people, who may not have Belkasoft Evidence Center X installed on their computers.

SQLite support:

- Native support for SQL databases for recovery of critically damaged and partially overwritten databases.
- Proprietary SQLite Viewer for viewing SQLite databases without the need for third-party applications. With Belkasoft X, you can inspect database schema, view existing and deleted data, run time, and string column conversations.
- Belkasoft X SQLite Viewer for opening damaged SQLite files, which standard SQLite Viewer struggle to deal with perfectly.
- SQLite freelist, WAL, journal file, SQL unallocated analysis functions for extracting destroyed evidence and viewing deleted information, such as iPhone SMS messages and Skype chats that were deleted.

Office documents support:

- Microsoft Office: DOC, DOCX, XLS, XLSX, PPT, PPTX
- OpenOffice: ODT, ODS, ODP
- PDF
- RTF
- Text files (TXT and LOG files)
- macOS: KEY, KEYNOTE, NUMBERS and PAGES
- For the supported file types files plain text as well as metadata is extracted and indexed
- Embedded files can be extracted and shown
- Document preview is shown for PDF files

File System support:

- APFS (including encrypted)
- F2FS
- FAT
- exFAT
- NTFS
- HFS
- HFS+
- ext2
- ext3
- ext4
- YAFFS
- YAFFS2

File System Explorer allows you to perform a thorough low-level forensics analysis. You are able to view and navigate through all folders and file from a data source (added to case) and examine hidden, deleted, and special system files and folders, such as $OrphanFiles or $Extends.

Belkasoft X extracts memory processes from RAM dumps.

You can browse through mobile or computer file systems and memory dumps acquired through Belkasoft or any third-party app.

On the **Hex Viewer** window, you can view the contents of a selected file or process binary conveniently. You can use the hashset analysis function. A NSRL hashset database or folder with previously known files is also available for use.

File System Explorer also allows you to check memory processes and files for malware through different techniques—for example, detection of fake system processes using VirusTotal.

X Mobile

X Mobile edition is a cost-effective solution developed specifically for investigators in local police departments, experts in small to medium consulting companies who provide digital forensic and incident response services, as well as individual customers (i.e. private investigators or digital forensic consultants). Customers who typically deal with just few cases per year involving unlocked mobile devices, and usually have limited budgets will enjoy the affordable price of X Mobile edition.

Key features of X Mobile edition:

- Acquires images of iOS and Android devices using standard backup as well as jailbreak-related methods, lockdown files, MTP/PTP, MTK and ODIN.
- Extracts full file system copy and keychain from iOS devices with the help of Belkasoft agent without doing a jailbreak.
- Mounts mobile backups and third-party tool smartphone images (UFED, OFB, GrayKey iOS images), chip-off dumps, TWRP images, JTAG dumps, etc.
- Examines and analyzes mobile artifacts—calls and messages, mailboxes, messenger apps data (WhatsApp, Signal, Telegram, Snapchat, WeChat, etc.), social media apps (Facebook, Twitter, Tinder, etc.), browsers, cryptocurrencies, and many more.
- Uses analytical features, such as **Connection Graph**, **Timeline**, and advanced picture analysis.
- Performs in-depth examinations into the contents of files and folders on a device with **File System Explorer**. Finds even more evidence with **PList** and **SQLite Viewers**.

When the Mobile Device Analysis module is installed, you can mount these data sources:

- iTunes backups of iPhones/iPads
- Full file system copy of jailbroken iOS devices acquired by Belkasoft X
- GrayKey images
- Android ADB backups
- Android Agent backups
- Android physical dumps
- Android MTP/PTP dumps
- Android MTK and Agent MTK backups
- OFB images
- UFED images of Androids and iPhones/iPads (excluding encrypted UFED images)
  .DAR
- Chip-off dumps
- JTAG dumps
- Blackberry IPD and BBB backups.

Belkasoft X can extract hundreds of artifacts from these iOS and Android apps:

- Browsers
- Chat apps
- Email clients
- Cloud services
- Social network apps
- Online map apps
- Fitness tracker apps, such as Fitbit or Mi Fit apps
- System data—Wi-Fi connections, connected/paired Bluetooth devices, and IP connections
- Webmail mobile apps, such as the Gmail app, Yandex Mail app, and others
- Popular apps, such as Uber, Tinder, Evernote, GetTaxi, Pininterest, Pokemon Go, Swarm, and others.

In general, on supported mobile platforms, Belkasoft X extracts known data based on these sources/apps: calendar, calls, voice mails, contacts, installed apps, SMS, tasks, and others.

X Forensic

X Forensic edition is the complete solution for conducting in-depth investigations on all types of digital media devices and data sources, including computers, mobile devices, and the cloud. Combining the functionality of X Computer and X Mobile editions with advanced features such as cloud data extraction, checkm8-based acquisition, and WDE decryption. It is an irreplaceable analytical tool for digital forensic laboratories of federal law enforcement agencies and state-level police departments.

Key features of X Forensic edition:

- All features of X Computer and X Mobile.
- Acquires and analyzes data from cloud sources.
- Uses forensically sound checkm8-based acquisition to extract data from the range of iPhone devices (from iPhone 5s through iPhone X) and even from locked iPhones without a jailbreak.
- Access devices encrypted with whole device encryption, such as APFS, Bitlocker, TrueCrypt and others.

Belkasoft X user interface

Belkasoft X uses different tabs to provide various views and functions to help you manage your cases, review artifacts, analyze devices and dumps, and perform low-level analysis tasks on raw data.

When you click on the menu icon at the top-left corner, you see the list containing these tabs (only if a case is loaded, otherwise, 'exit' only):

Dashboard. This is the main screen for managing an open case. Here, you get to edit a case's properties, perform actions on the case, review its statistics, find automatic searches, and so on.

Artifacts. This is the main screen for reviewing artifacts extracted in your case. Here you can go through artifacts, based on categories or groups, view their properties, perform filtering and search, create reports and so on.

Bookmarks. This is the main screen for viewing the bookmarks you created for artifacts. Here, you able to examine bookmarks (in depth), edit them, and also delete them.

Connection Graph. This is the main screen for reviewing connections. Here, Belkasoft X provides a high-level communication diagram that shows the connections between individuals in your case.

File System. This is the main screen for examining data source locations and their attributes on a low level. Here, you can view partitions and volumes, volume shadow copy snapshots (if available), folders and files, and memory processes for RAM dumps.

Hex Viewer. You can use this tab to review a file, processes, or a data source (in its entirety) on a byte level. You can also perform type conversions, run search tasks, bookmark pieces of bytes, and so on.

Incident Investigations. This screen combines various artifacts from various data sources such as registry, Event log and others, which can help in a course of an incident response case.

Map. This screen allows you to review artifacts having geolocation on Open Street Maps (with an Internet connection) or Google Earth (if its installed locally).

Plist Viewer. You can use this tool to view Mac property lists including binary format.

Registry Viewer. You can use this tab to review registry entries and files.

Search results. This is the main screen for reviewing searches.

SQLite Viewer. You can this tab to examine the contents of SQLite databases. This viewer unveils database schema and table row data; it supports journal, WAL, freelist and SQLite unallocated space reviewing.

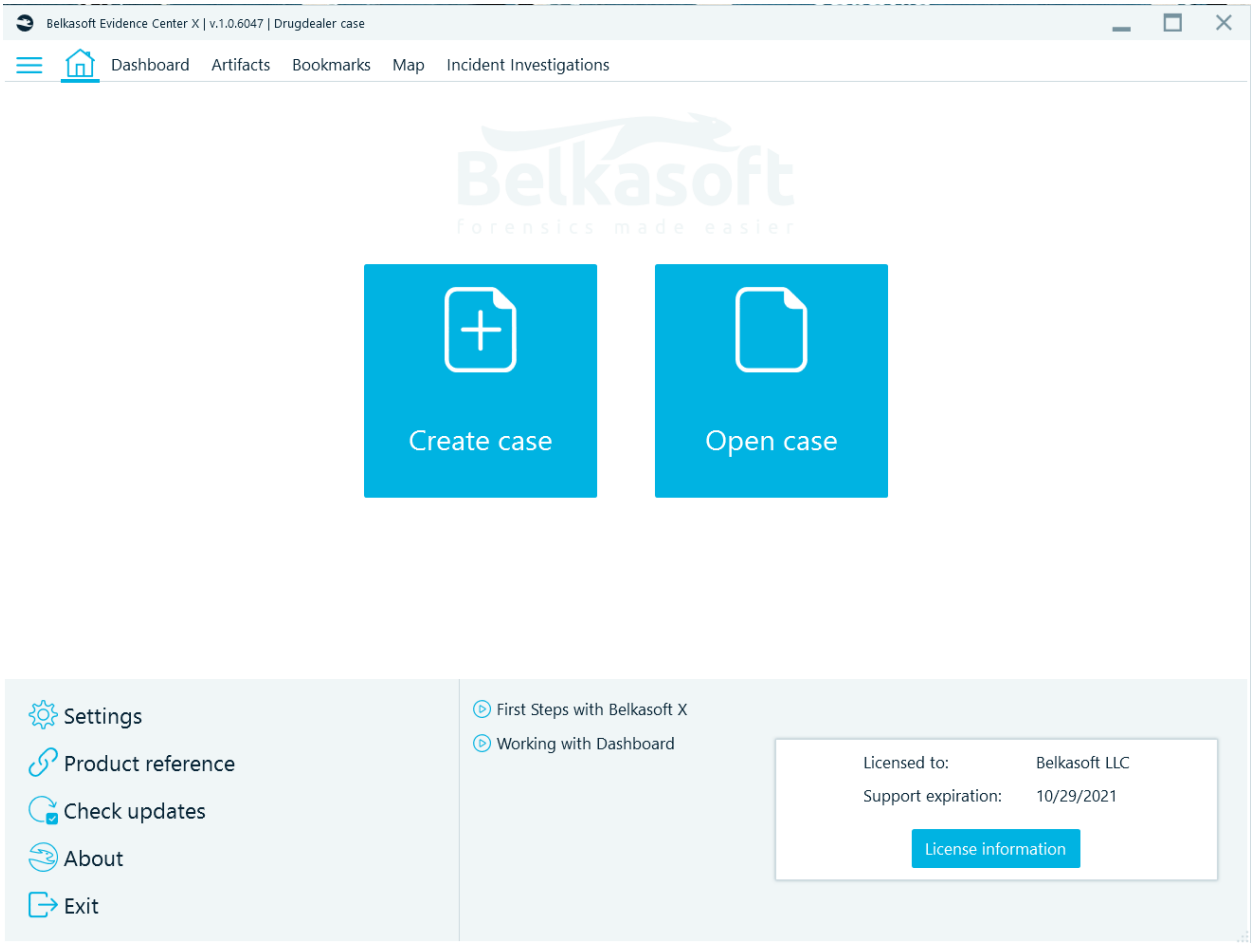
Timeline. This is the main screen for reviewing events or activities based on time. Here, Belkasoft X combines all the artifacts involved in a case.

Tasks. This screen helps managing tasks in Belkasoft X. It provides information on task statuses and useful logs. Here, you can stop tasks.

Home screen

On the Home screen, you find the primary functions for creating and opening a case and controls for Belkasoft X itself. Regardless of what you have ongoing with in Belkasoft X, you can always return to the Home screen.

The contents of the Home screen do not change, so you can use the functions there at any point in time.



Creating a case

To create a new case, click on Create case.

On the **Create case** window, fill in the **Name** box, specify the **Folder** to which Belkasoft X stores the case, choose your preferred **Time zone**, fill in the **Investigator** box, and fill in the **Description** box.

We recommend you select a root folder (inside a big drive) as the location to which Belkasoft X saves cases. The cases may be huge, so you should try to make preparations free up as much space as possible.

If your machine has a small-sized SSD, then you you can still use it. Ideally, you should get a big HDD drive and store your cases there. You cannot change the Case folder (for a case) later, so you must make the correct decision before you create your case.

Belkasoft X determines the path automatically based on the root folder and case name.

Time zone setting for a case—and its importance

The **Time zone** is an important setting in digital forensics. Artifacts are stored in UTC time or local time—this setting allows Belkasoft X to assign different times to points on a specific timeline. Belkasoft X sets the time zone automatically to the default (in use) on your computer.

When you work with devices or sources from a time zone that differs from yours, you may want to change your time zone setting.

Note: When your case contains multiple devices or sources from different time zones, you can—and we recommend that you do—set the time zone for each device separately. For more information, see *Supported analysis types*.

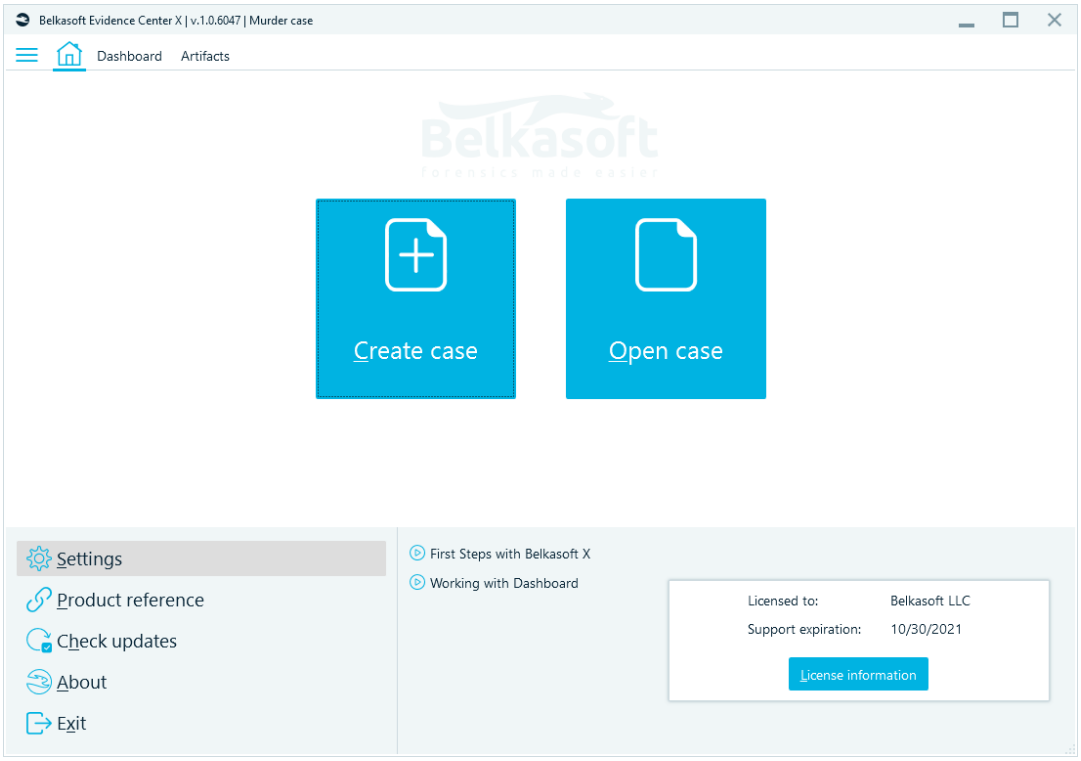
Opening a case

To open a case, you previously created in Belkasoft X, click on Open case.

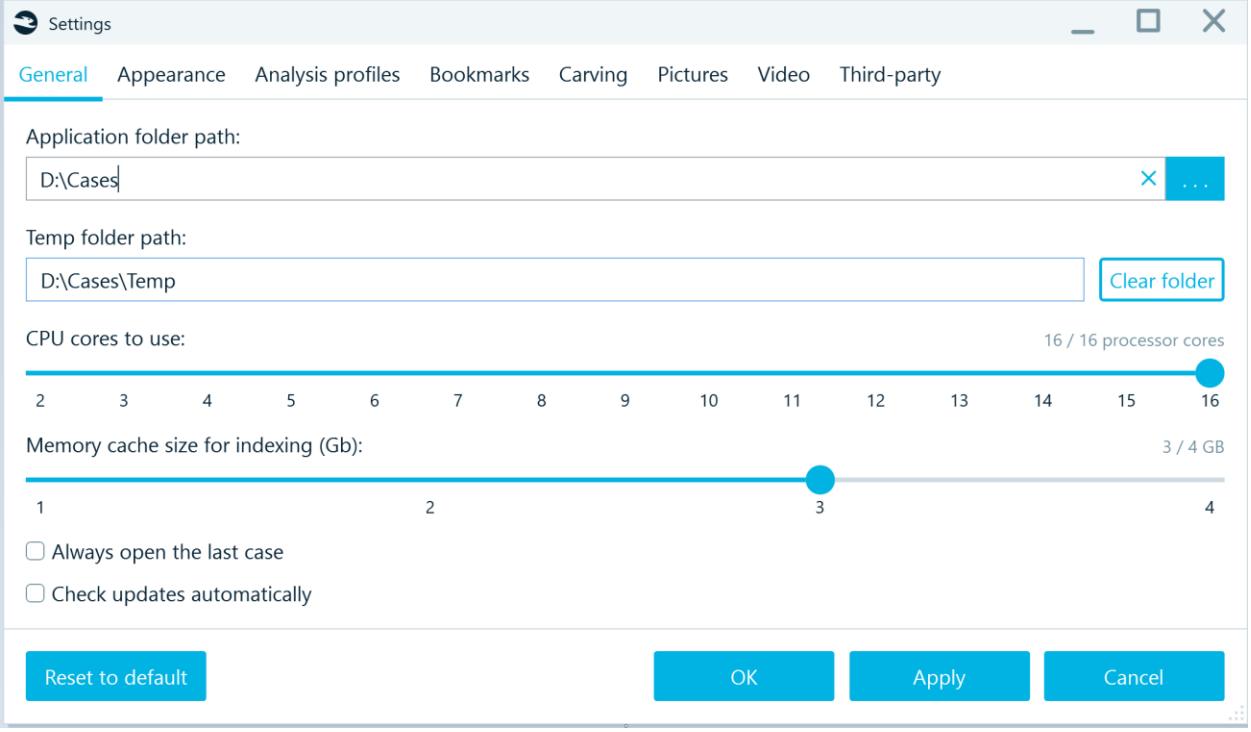
On the Open case window, click on the case you want Belkasoft X to open.

Settings

You can fine-tune the product with the help of various available settings. To do so, go to **Home screen** and double click on **Settings** at the bottom left corner.



The following window will be shown:



Product settings are divided up into several categories:

- General
- Appearance
- Analysis profiles
- Bookmarks
- Carving
- Pictures
- Video
- VirusTotal
- Volatility

General settings

The following general settings are available:

- **Application folder path**. This path is used by Belkasoft X to store its settings. In most cases you can just leave this option to its default setting, but if you are going to store cases and options onto a thumb drive and move this drive along different machines, you will find this option very helpful.

- **Temp folder path**. During the analysis, Belkasoft X processes a lot of information, and unpacks and extracts various files. Temporary folder is used to store these files. If your system drive is a small SSD drive, we highly recommend you redirect Temp folder to a larger HDD.

- **CPU cores to use**. This option helps you to specify how aggressively Belkasoft X should use your computer's resources. Available options are two to N, where N equals the amount of your processor cores. You cannot specify to use only core, since Belkasoft X reserves one core for its user interface. By default, Belkasoft X uses two cores: one is for case processing and one core is for the interface. If you have a powerful machine with dozens of processors, the bottleneck will probably be your hard drive, not the CPU, so advisable to decrease the amount of cores used (**such as**, only use 16 cores out of 32). It is not possible to give specific advice for all available configurations, testing with your unique set up by you may be needed.

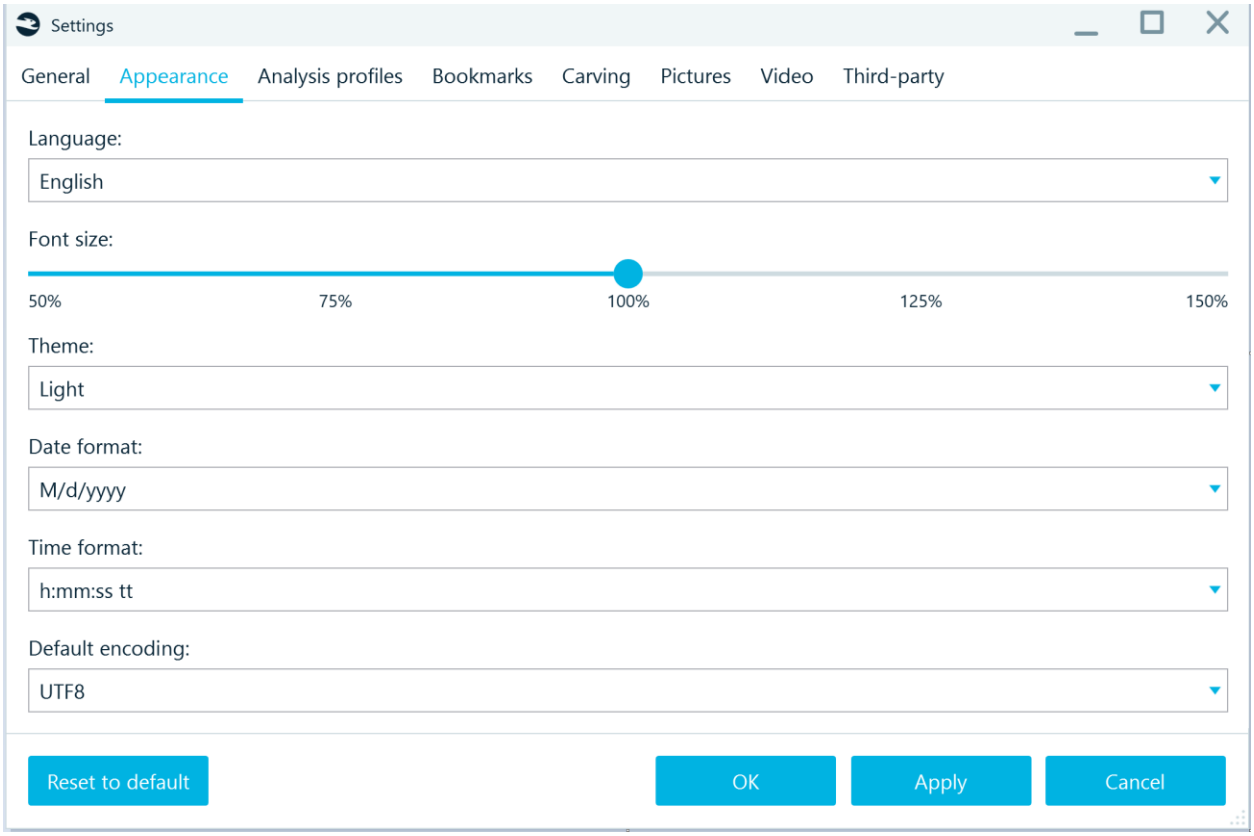
- **Memory cache size for indexing (Gb)**. The product uses ElasticSearch engine which requires a significant amount of memory. If you are limited in memory and see memory errors reported by the product during analysis, consider decreasing the amount of memory allocated to the indexing.
  Note: The memory cache size cannot exceed 30% of the total RAM. This setting will not be saved by Belkasoft X, as it slows down all other processes.

- **Always open the last case**. If this option is set, Belkasoft X, when started, will try to re-open the last case that was open before your license was previously closed. Otherwise, no case is opened by default, and you will have to specify which case to open.

- **Check updates automatically**. If this option is set, Belkasoft X will try to check for available software updates on each start (needs an Internet connection).

Appearance settings

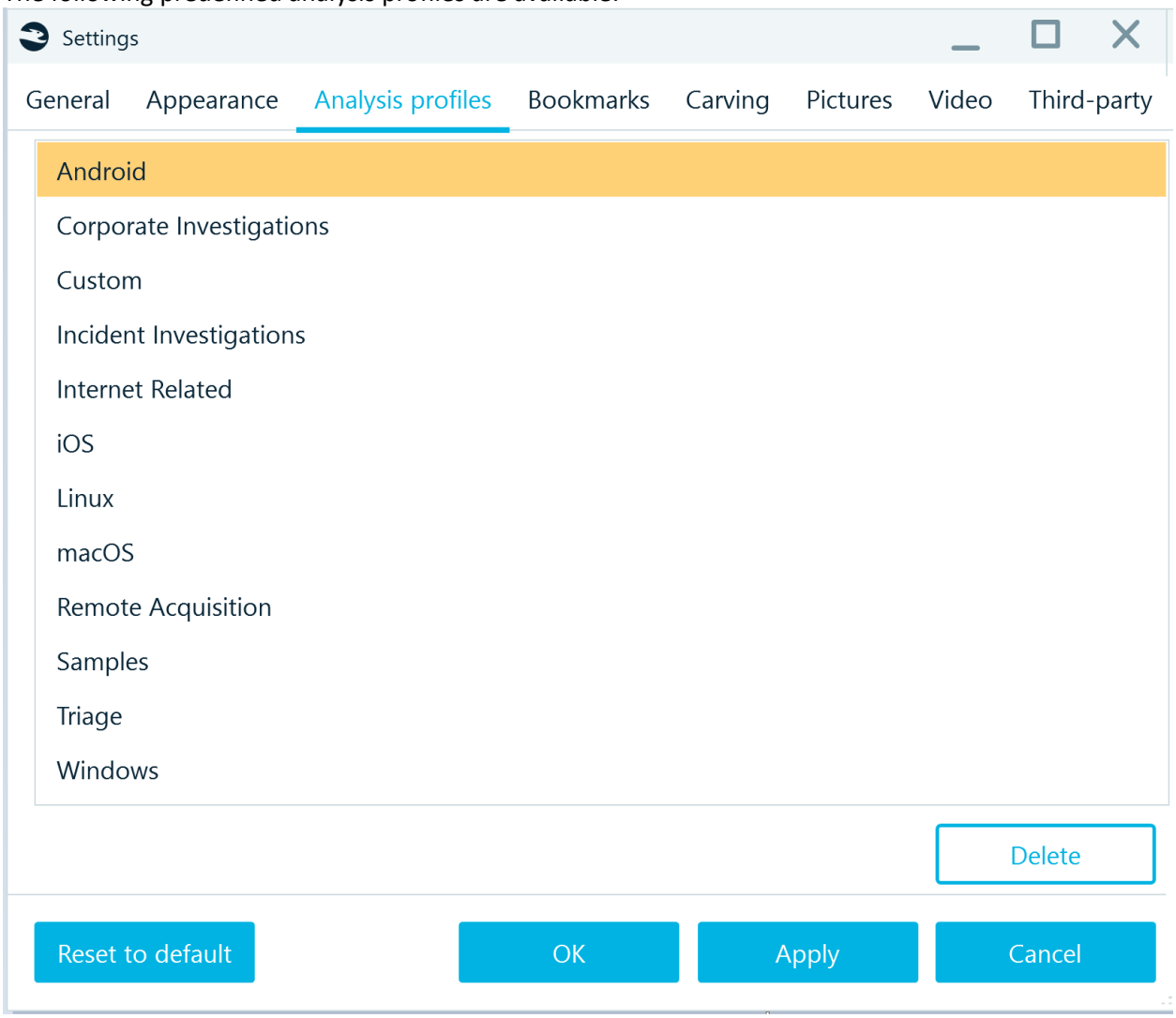
The following appearance settings are available:



- **Language**. There are a number of languages supported. If you found your language, excellent, choose it and press OK. If you did not find your language and wish to volunteer to help us translate the product, let us know.
  Note: the user interface language also affects language of generated reports
- **Font size**. The ability to customize the font size in the interface. You can set your own font scale from 50% to 150% depending on your screen settings and the size of the system fonts. This is the second feature of the product (along with the dark theme) that reduces the strain on your eyes. Belkasoft takes care of your health!
- **Theme**. You can choose between Light or Dark themes. The changes will be applied after restarting the product. Take a minute to try the Dark one, you might like it!
- **Date format** and **Time format**. These fields help to specify date and time formats to be used in the product user interface and reports. Date formats vary from country to country. Some put month before date, some put the day before the month, and still others put the year in front. Also, countries differ in time format. Some use the am/pm, others use 24-hour time format and so on. You can select any one of many predefined formats from a list.
- **Default encoding**. Some applications used only in one country or a region store their data in local encodings, such as, Shift-JIS, rather than Unicode or UTF8. Though you can always specify encodings for them using Encoding context menu for the application profile node. It is more convenient to specify the default encoding once in settings.

Analysis profiles

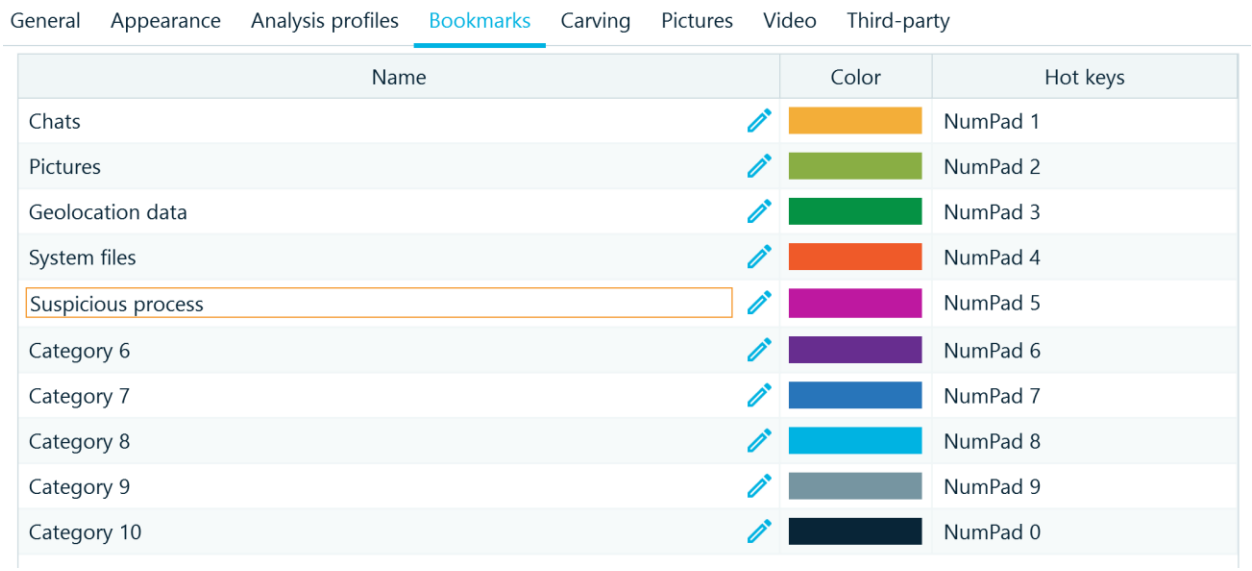
The following predefined analysis profiles are available:



A profile combines these sets of analysis options: what applications to analyze, whether to extract data, how to analyze hash sets and media files. When you add a data source, the selected profile will be used by default; however, you will be able to edit a predefined profile and save it as a new custom profile.

Bookmark settings

You can see and manage bookmark categories within the **Bookmarks** tab:

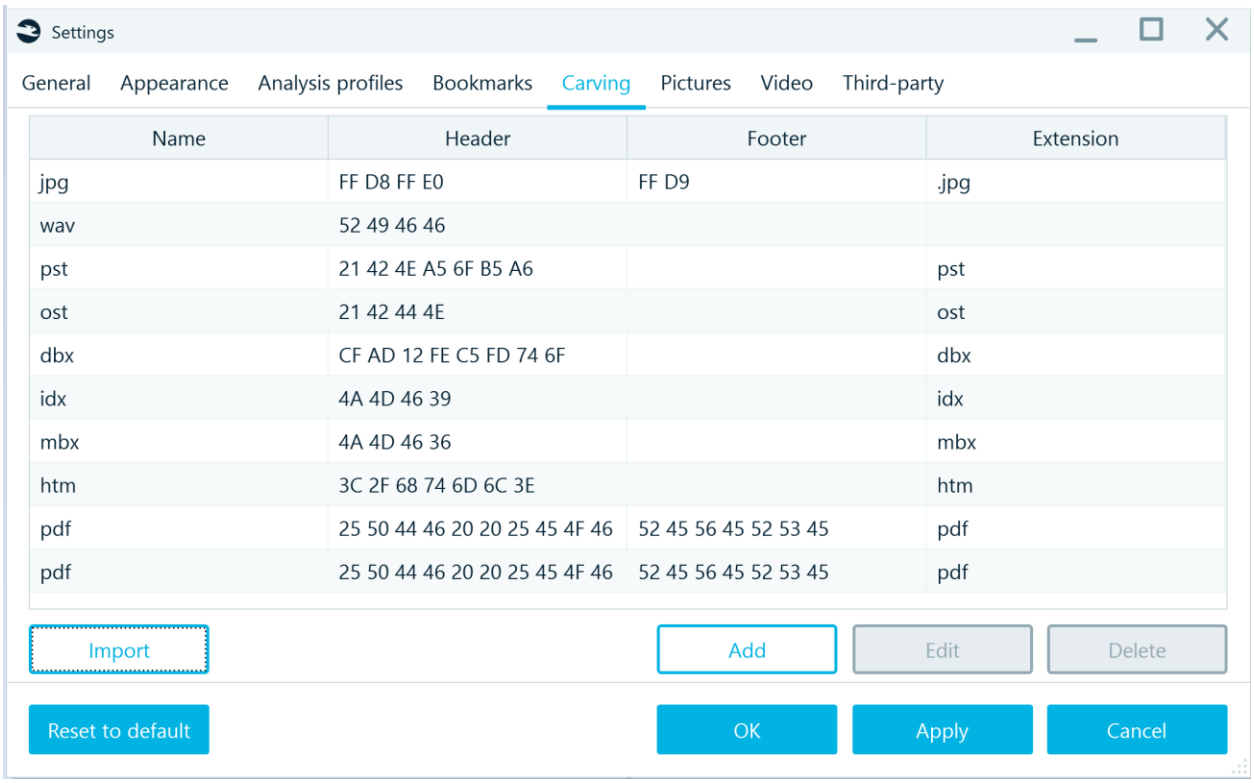


By default, there are 10 available categories, and the following properties are displayed:

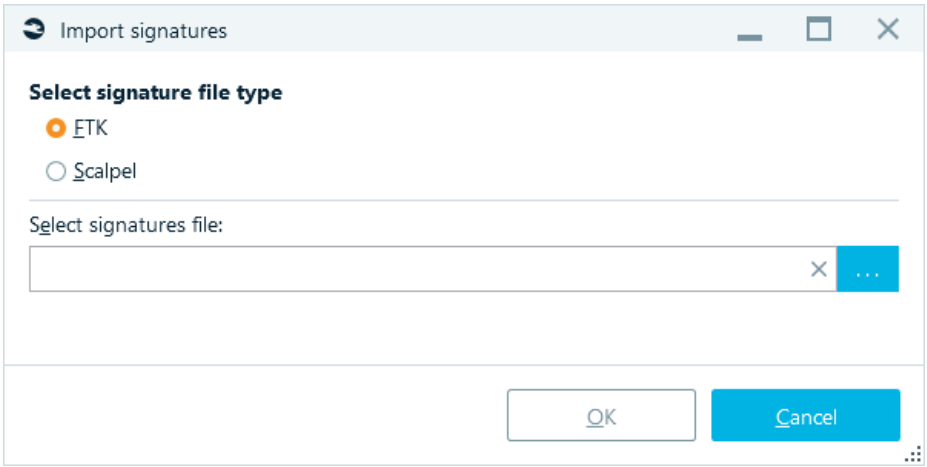
- **Name**. The category name is displayed when you create a new bookmark. You can rename some of the categories (or all of them) on the **Bookmarks** settings tab.
- **Color**. All bookmarked artifacts are marked with a colored bookmark flag in **Artifacts** and other item lists. The flag color is defined by the category the bookmark belongs to.
- **Hot keys**. You could use the category hot key in order to bookmark selected artifacts. If there are no bookmarks in this category yet, a bookmark will be created. If the selected artifacts belong to a category already, they will be removed from the corresponding bookmark.

Carving settings

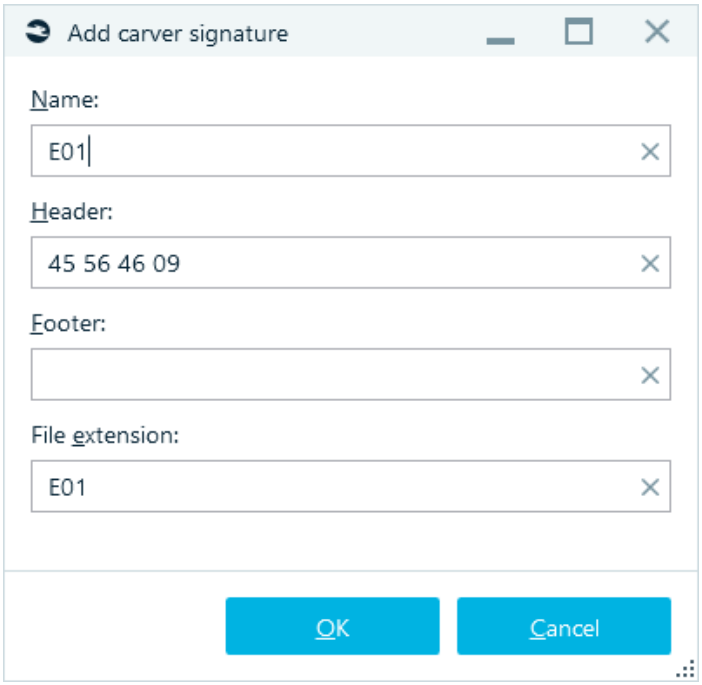
Belkasoft X allows the user to specify custom signatures to carve. You can **Import**, **Add**, **Edit** and **Delete** signatures from this window:



- **Import**. Using this button, you can import FTK or Scalpel signature sets. Specify the path to an FTK or Scalpel signature file and select FTK or Scalpel.



- **Add**. You can add your own signatures individually by clicking on **Add** button. The following screen will be shown:



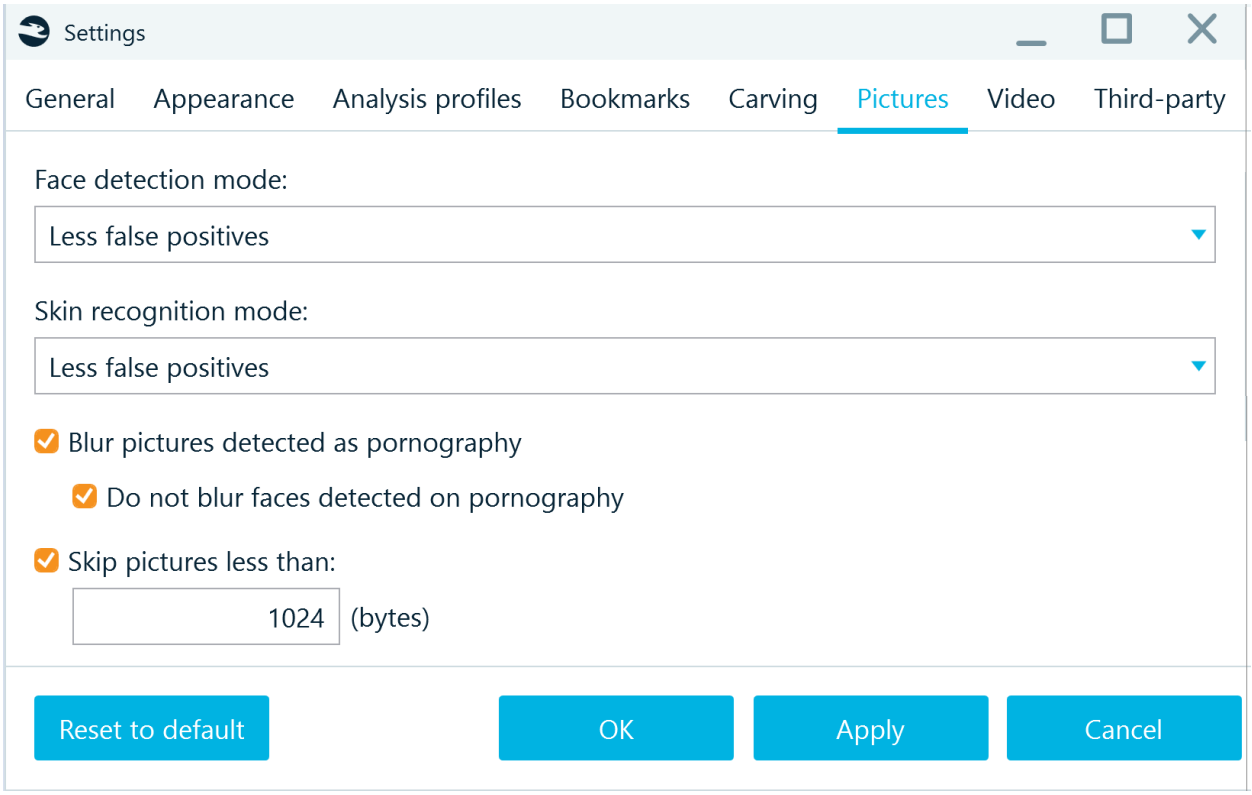
Name is the name for your new signature; **Header** is hexadecimal bytes for the beginning of data, **Footer** is hexadecimal bytes for the end of data (optional), **File extension** is a hint for the Belkasoft X of what extension to save a carved file under; **Artifact type** is a hint for Belkasoft X of where to show carved result (on the screenshot above it is instructed to show carved data under Pictures node).

- **Edit**. This button opens the same window in which you edit existing signature.
- **Delete**. Deletes selected signatures.

Be careful, when adding custom carving signatures and make sure they are unique. Adding signatures like "00 01" will result in a huge amount of carving results and slow down the entire analysis significantly. An example of a suitably unique signature is "SQLite Format 3".

Picture settings

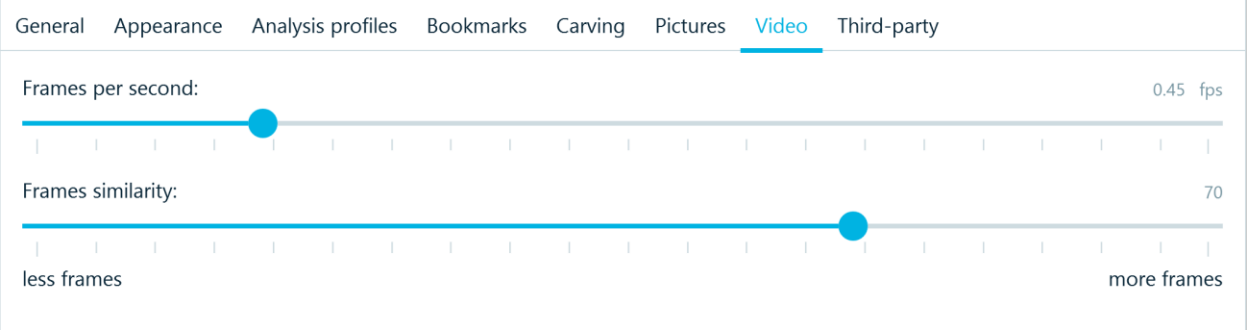
The following picture-related settings are available:



- **Face detection mode** and **Skin recognition mode**. These two settings help to specify modes for face and skin detection in pictures. These two detections may discover more true pictures with faces or skin, but in this case, they may also find false positives (pictures, which do not contain face or skin). You can specify to find less false positives (in this case you may receive more false negatives, that is, pictures which contain face or skin that are not detected).
- Pornography detection
    - **Blur pictures detected as pornography**. If a picture of pornography is detected, it will be blurred, if this option is set. Note: before you run pornography or skin detection, the product is unable to distinguish such pictures and will not blur them.
    - **Do not blur faces detected as pornography**. If both the first option and this one is set, faces in pictures detected as pornography will not be blurred.
- **Skip pictures less then.** A standard computer hard drive contains thousands of tiny pictures like 1x1 pictures for HTML layout or 10x10 background pictures. In most cases, they will not contain any meaningful information for forensic or incident response purposes and are safe to skip. If you decided to do so, you can specify the minimum picture size in bytes. Pictures smaller than the size you choose will be ignored by Belkasoft X. By default, all pictures smaller than 1Kb (1024 bytes) are ignored.

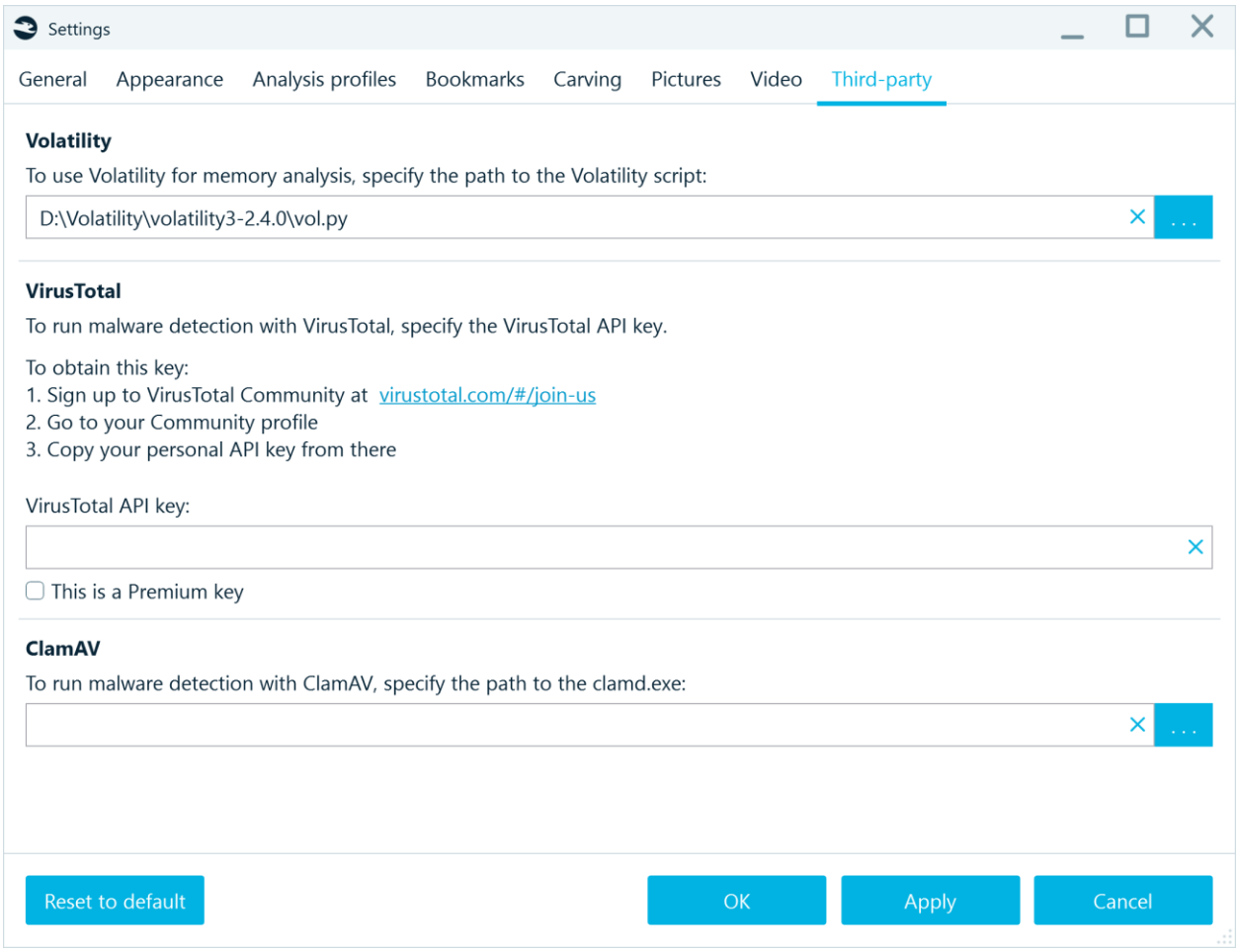
Video settings

The following video-related settings are available:



- **Frames per second**. This option is used for video keyframe extractions. You can specify how many frames per second to process. The more to the right this indicator is, the more keyframes will be extracted. If you specify 1 fps, it will mean that Belkasoft X will take the next frame one second after the previous keyframe and compare. If they are similar enough, the current frame is not set as keyframe and Belkasoft X will take the next candidate frame one second later. If this option is set to 2 fps, frame candidates will be taken half second from each other.
- **Frames similarity**. This option specifies how different should be two frames be to determine that both of them are keyframes. The more at the right this value is, the more keyframes will be extracted. Typical value here is 70, but it is good to test against your typical video to discover, what similarity value suits your needs best.

Third-party



Volatility

Volatility is an open-source cross-platform tool for analyzing RAM images.

Installation

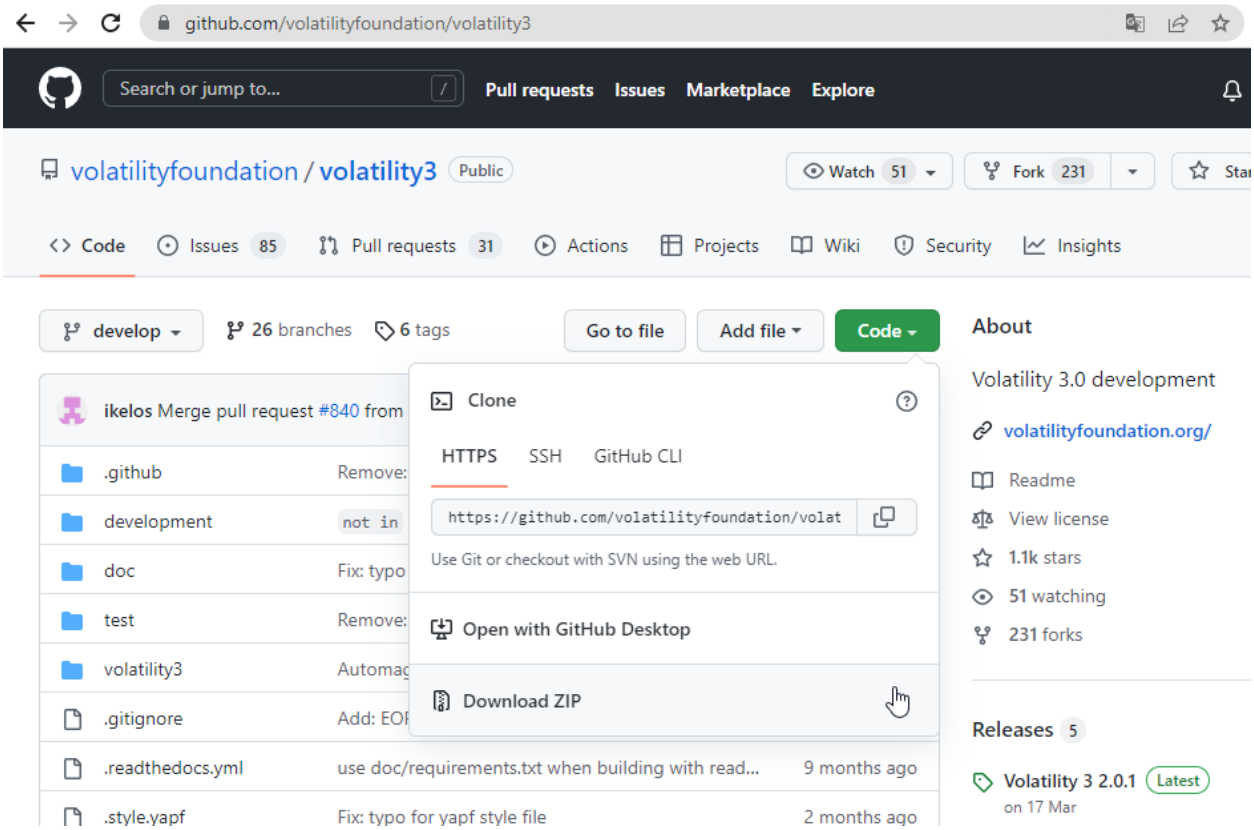
1. Download and install Git https://gitforwindows.org/.

Use default settings during the installation.

2. Install **Volatility 3** from GitHub: https://github.com/volatilityfoundation/volatility3.

On the Volatility 3 tab click Code. The Volatility setup files can be downloaded or cloned.

The download option. Click ‘Code’ – Download.zip. Unpack the downloaded archive to the Volatility3 folder on your computer.



Clone:

Create a folder to which the Volatility should be cloned. Copy the link in the HTTPS section on the Github.
Launch Git CMD or Command Prompt or Windows PowerShell.

cd [Volatility folder path]

Press Enter and type:

git clone [path from git]

If you get the following error: 'git' is not recognized as an internal or external command, …
Modifying PATH on Windows 10:

- In the Start Menu or taskbar search, search for "environment variable".
- Select "Edit the system environment variables".
- Click the "Environment Variables" button at the bottom.
- Double-click the "Path" entry under "System variables".
- With the "New" button in the PATH editor, add C:\Program Files\Git\bin\ and C:\Program Files\Git\cmd\ to the end of the list.
- Close and re-open your console.

3. Download symbols from
https://downloads.volatilityfoundation.org/volatility3/symbols/windows.zip

Open the **symbols** folder: **…volatility3\symbols** and unpack **windows.zip** here.

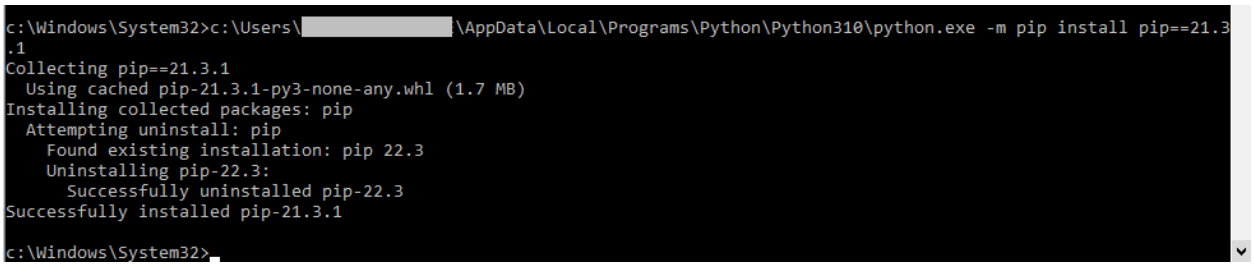
4. Download Python (**version 3.8**) from https://www.python.org/downloads/release/python-3810/

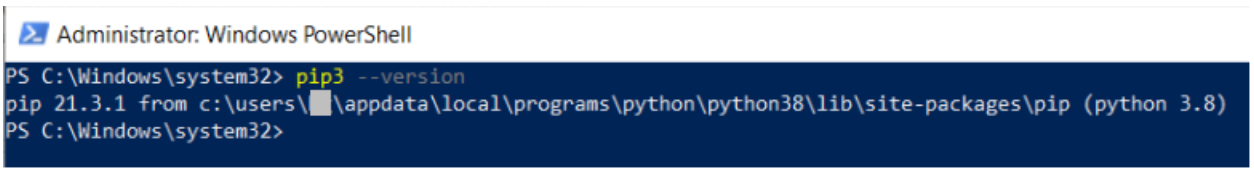
5. Install Python with a check **"Add Python 3.8 to PATH"**, agree to **"Disable the path length limit"**

6. Check the pip3 version.
   Launch Git CMD / Command Prompt / Windows PowerShell and type:
   pip3 --version

If the version is different from 21.3.1, install the correct version: Type in Git CMD / Command Prompt / Windows PowerShell:

pip install pip==21.3.1



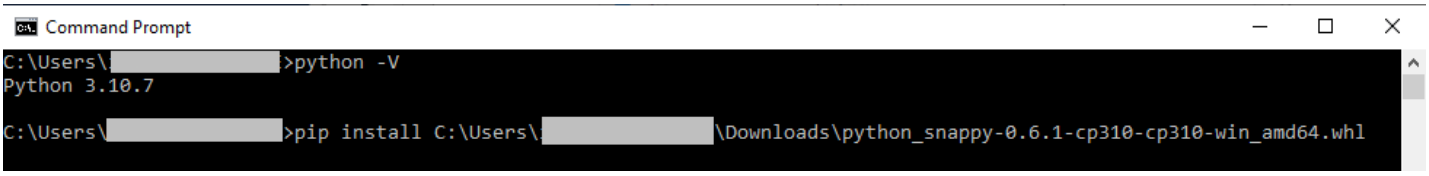


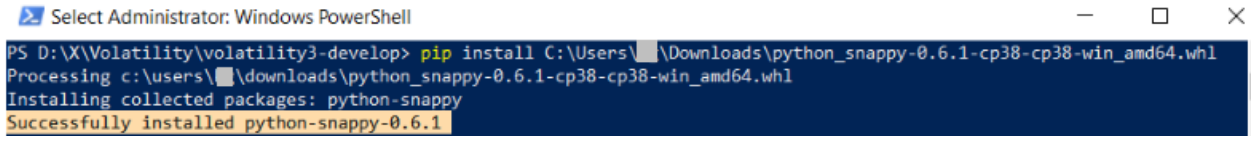
7. Download Python Snappy.

Select the one, that is suitable for your system from
https://www.lfd.uci.edu/~gohlke/pythonlibs/#python-snappy.

For Windows 10 with python 3.8 select **python_snappy-0.6.1-cp38-cp38-win_amd64.whl.**

Install the Python Snappy: type in the Git CMD / Command Prompt / Windows PowerShell command:
pip install [full path to snappy file location]





8. Install requirements.

Requirements.txt is located in the Volatility3 installation folder.

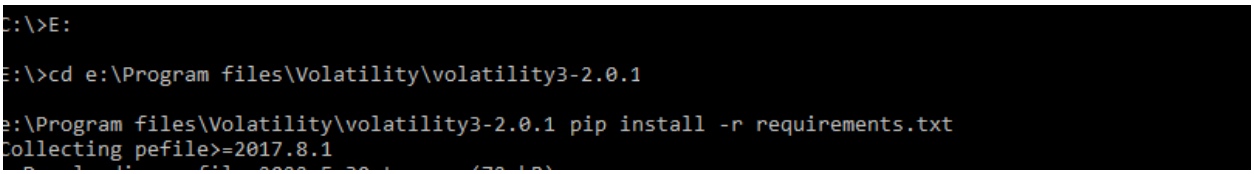
Run Command Prompt as Administrator and switch to the directory with the file requirements.txt.

Type:

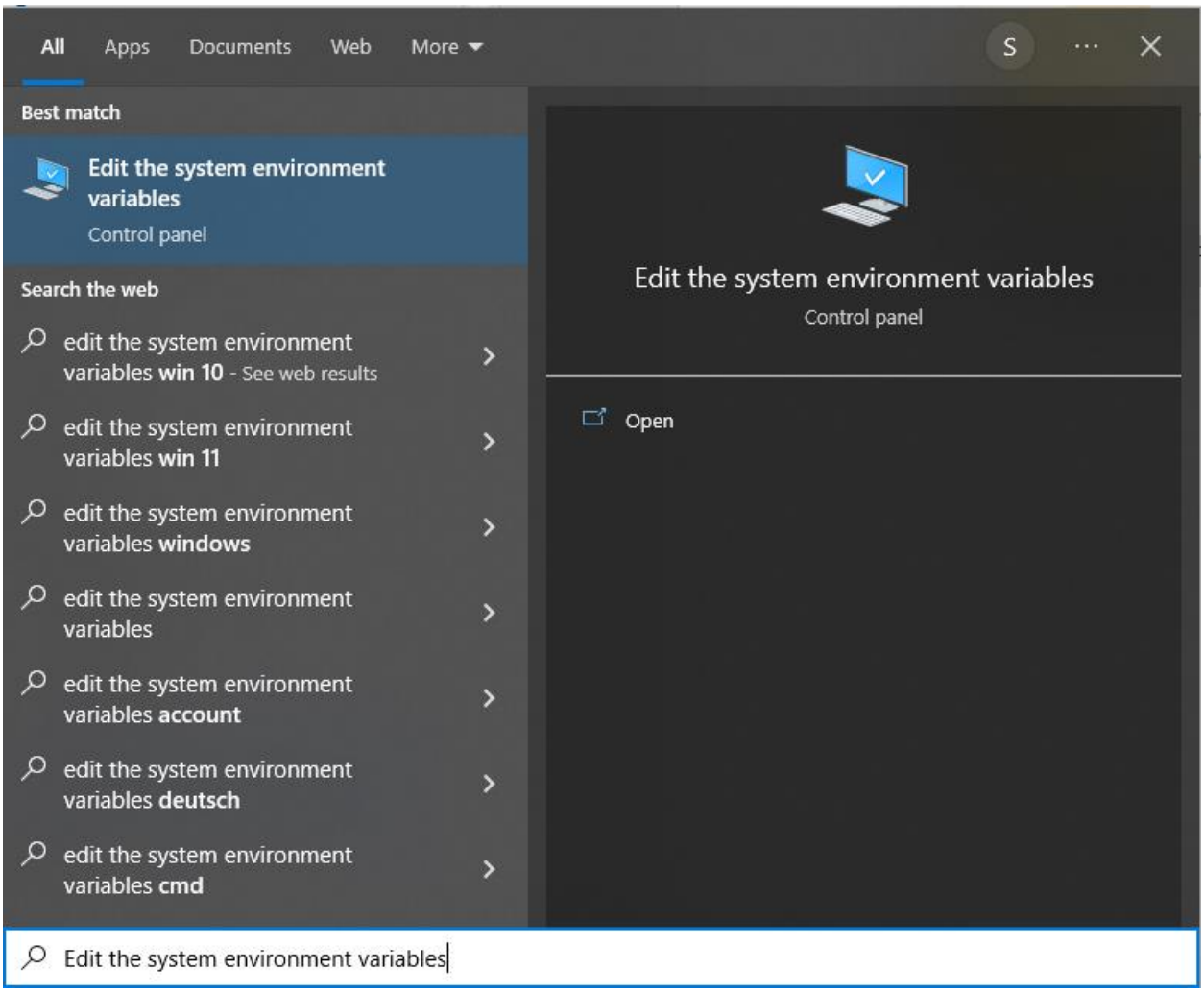
cd [full path to requirements.txt]

Press Enter and type command:

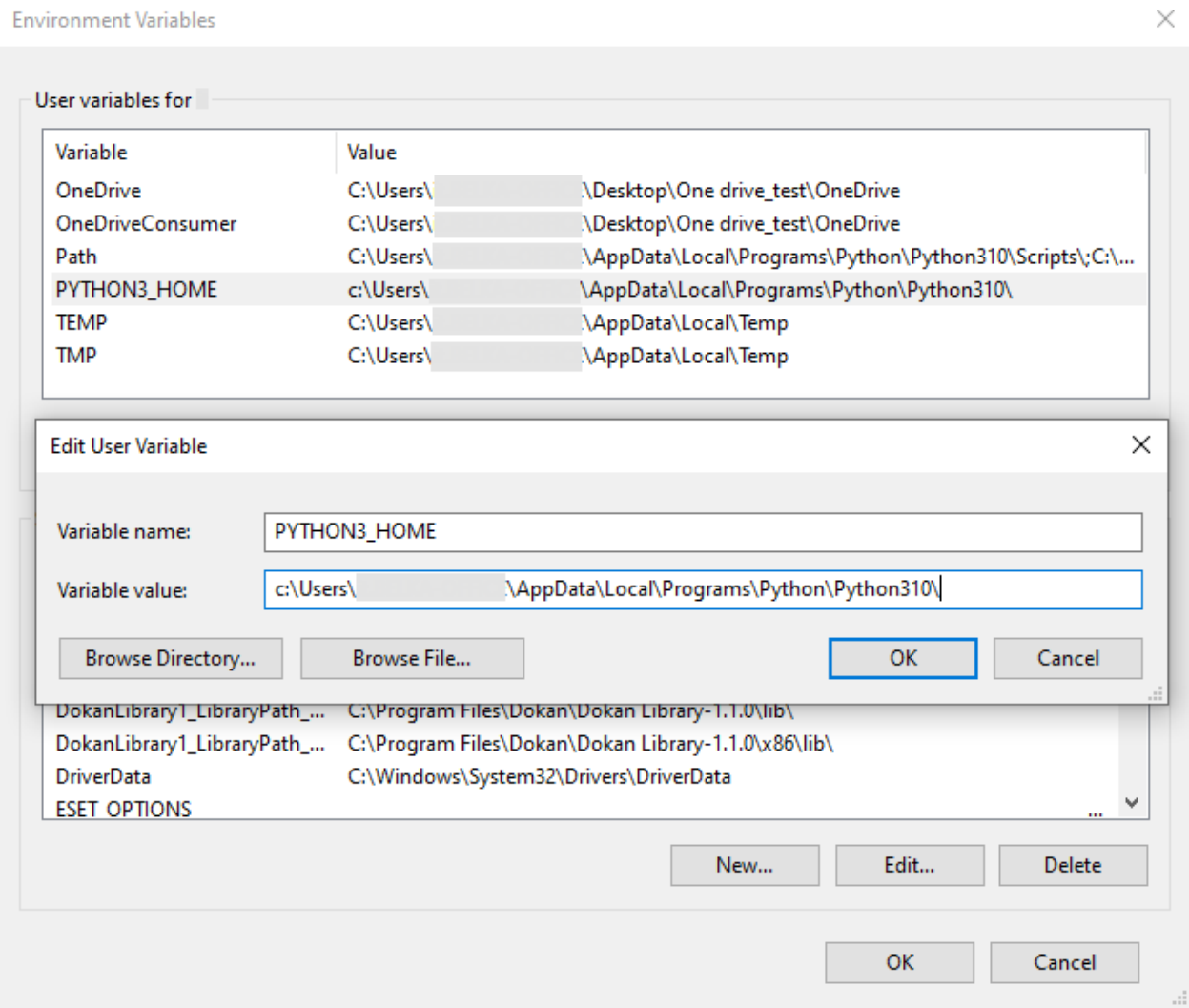
pip install -r requirements.txt:



9. Open the Windows Control panel – System – Advanced system settings and edit the system environment variables.

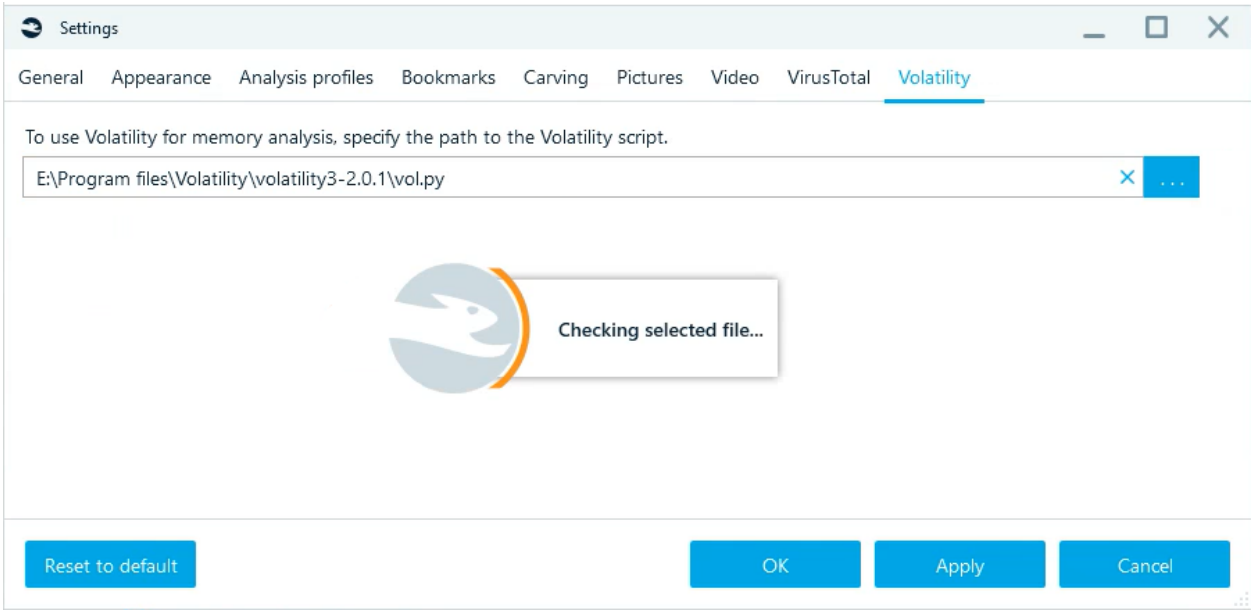


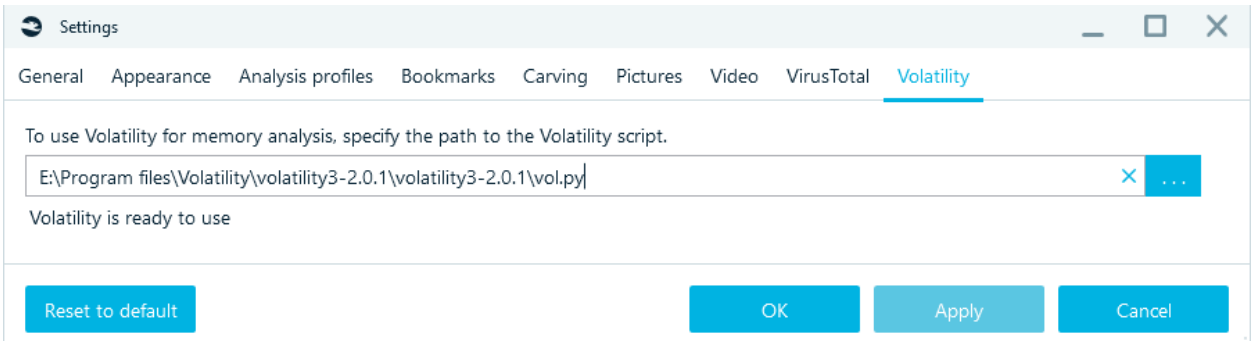
Click the **Environment Variables…** button, then click ‘New’ in the ‘User variables for Administrator’ section and add a new **User variable::**
Name: PYTHON3_HOME
Value: Full path to the folder with python.exe



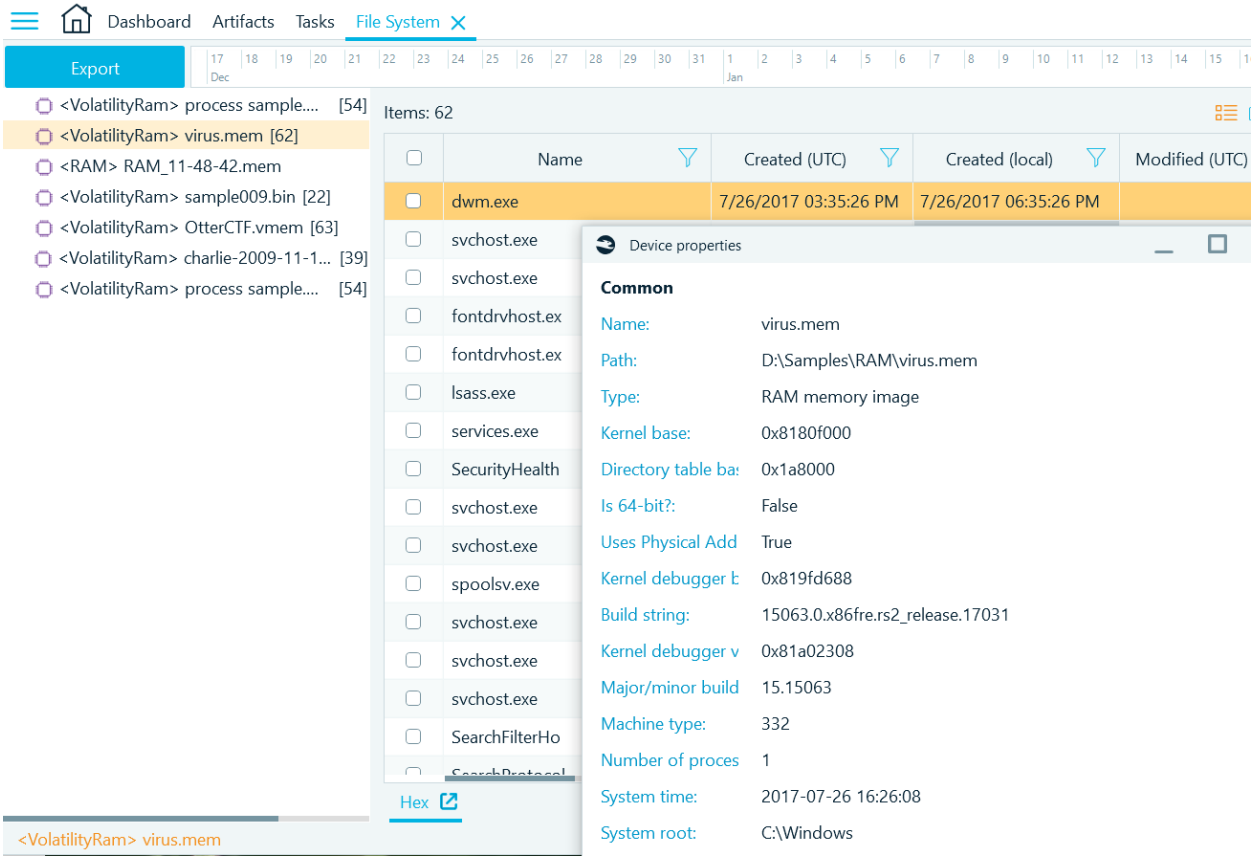
Save the variable and exit the editor.

10. Open **Belkasoft X** or restart it if the application was already launched.
Go to **Home screen** and click on **Settings**, **Volatility** tab:
Set full path to file **vol.py.** This file is located in Volatility3 installation folder. Wait for the **"Volatility is ready to use"** status to appear:



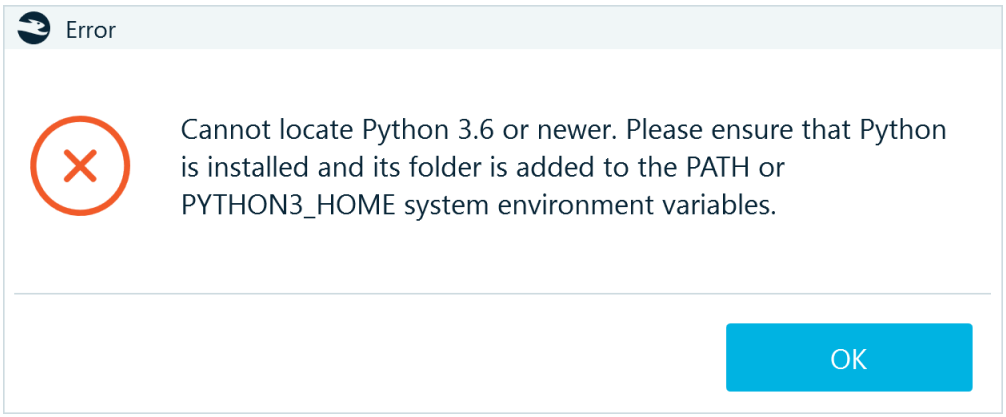


11. Run your RAM images for analysis from **Dashboard.** Check the results on the **File System** tab:



Troubleshooting

- “Cannot locate Python 3.6 or newer”



Download Python from https://www.python.org/downloads/release/python-3810/ and check that all the steps of the instruction have been completed.

- If memory parsing fails with the **missing symbols error**, do the following:

1. Launch Git CMD / Command Prompt / Windows PowerShell as Administrator
2. Navigate to the directory where the **vol.ry** file is located. Type:

cd [Volatility folder path]

3. Run command**:**

python vol.py -v -f [memory dump full path] windows.info

4. Restart the memory dump analysis in Belkasoft X

VirusTotal

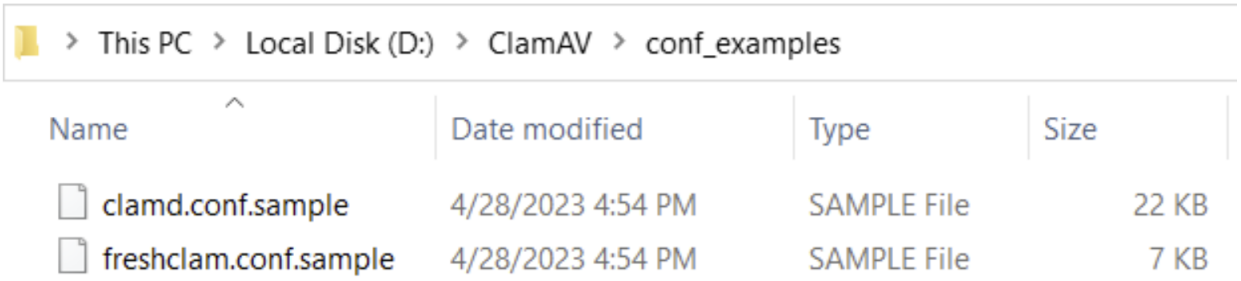
To analyze suspicious files in VirusTotal, the memory of processes (for RAM) and the hash sum (for files) are sent.

ClamAV

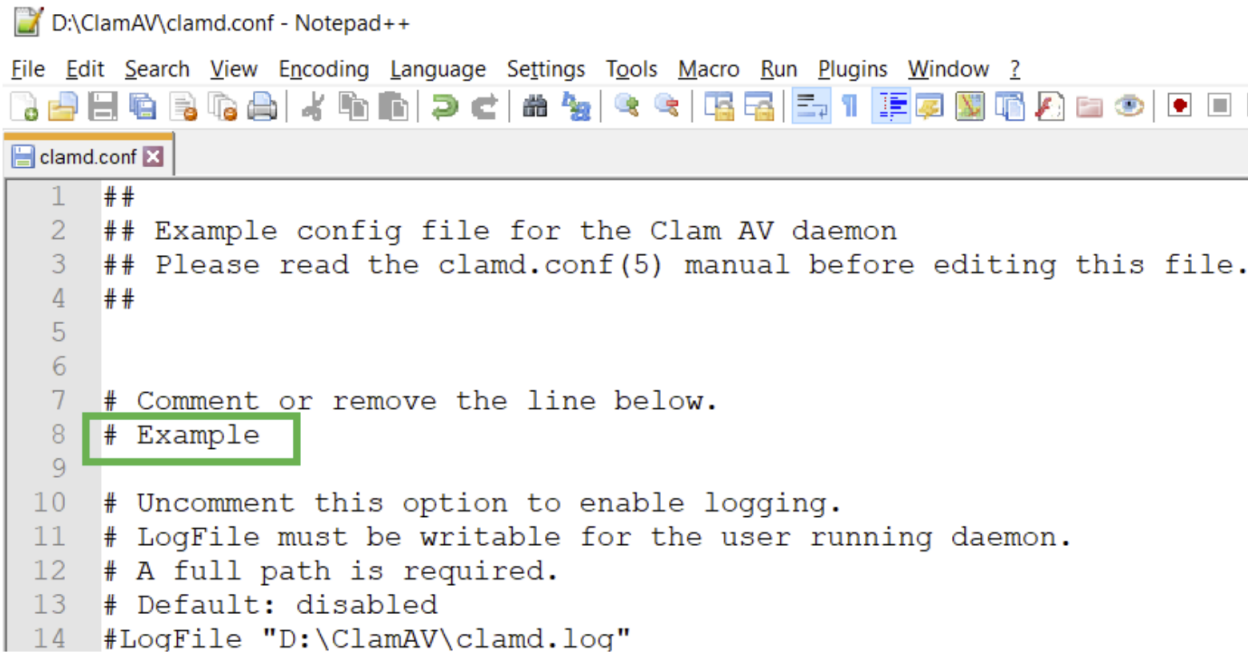
ClamAV is a popular open-source antivirus software that can detect various types of malware, including viruses, trojans, and worms. The software is lightweight and easy to use, and it is compatible with most operating systems, including Windows, Linux, and macOS.

Installation

1. Download the latest version of ClamAV https://www.clamav.net/downloads
2. Complete the installation process
3. Navigate to **conf_examples** folder



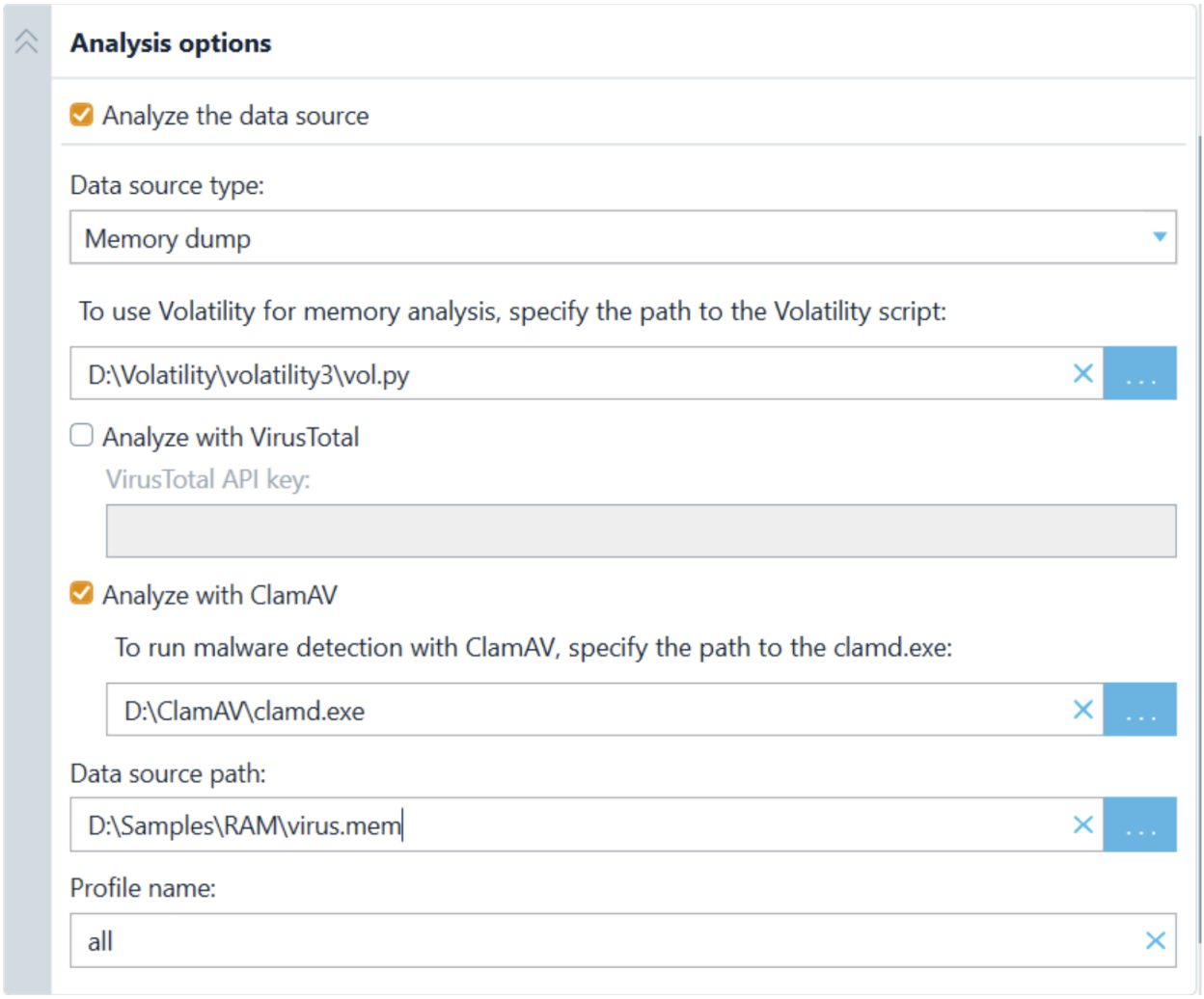
4. Open the file **clamd.conf.sample**, comment **Examples** line and save the file under the name clamd.conf in the upper folder (where clamd.exe is located).
   Do the same with **freshclam.conf** file.



5. Run cmd as Administrator and execute **freshclam.exe**. This will download the latest virus databases. If updating the database was not successful, please follow the link above and manually download the database. Then, transfer the downloaded databases to the database folder.
6. Run **clamd.exe**, and if the check is completed without errors, **ClamAV** is ready for use.

You can initiate the analysis using **ClamAV** either through Belkasoft X or the Command line Configurator.

Command line setup



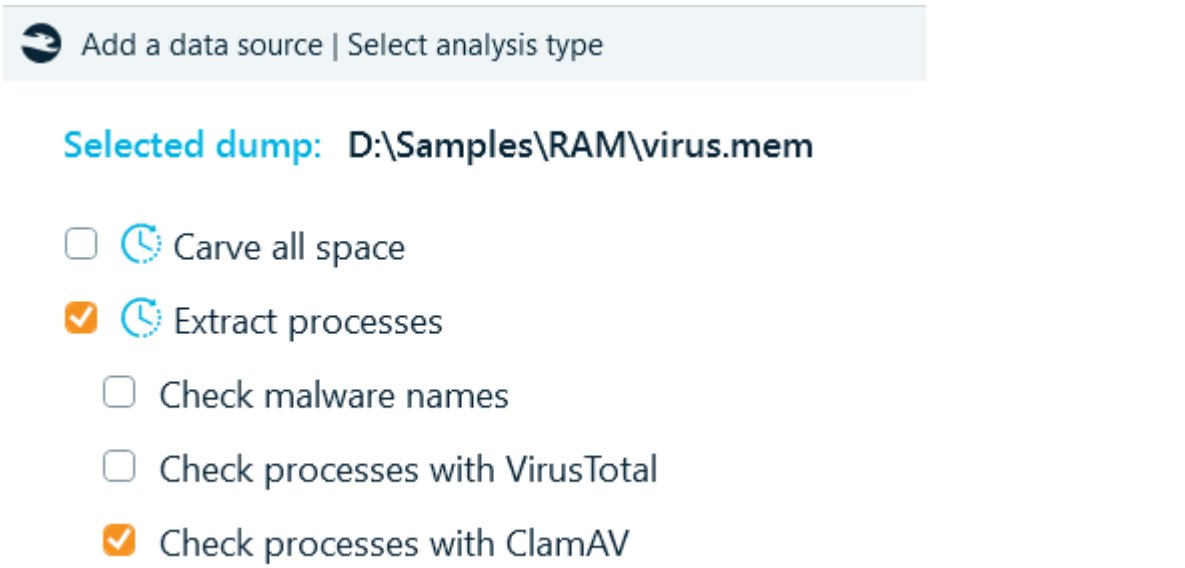
Add the link in the corresponding field to **clamd.exe** file.

Belkasoft X setup

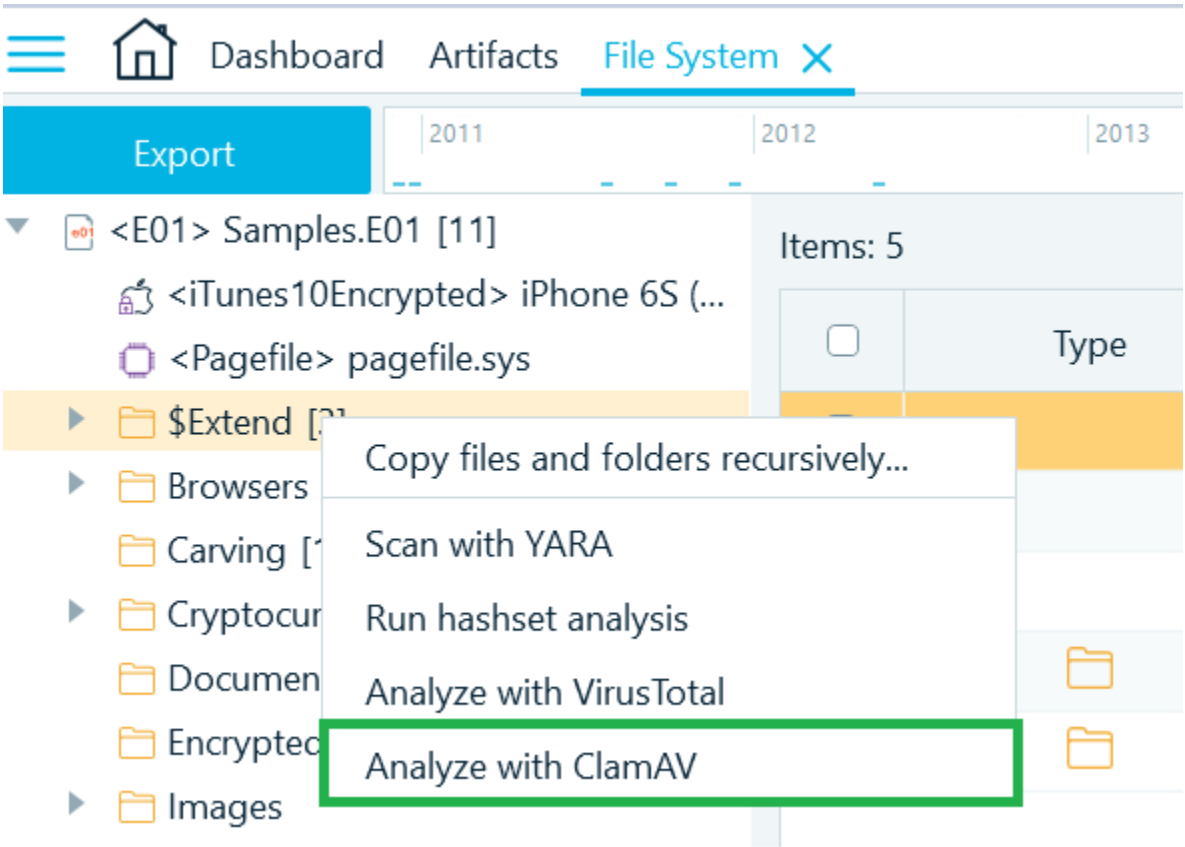
1. Open Belkasoft X, Home tab.
2. Open Settings, Third-party tab
3. Add the path to **clamd.exe** in the corresponding field
4. Apply the new settings

ClamAV analysis

Run **RAM analysis** from **Dashboard** tab and choose **ClamAV** analysis type option

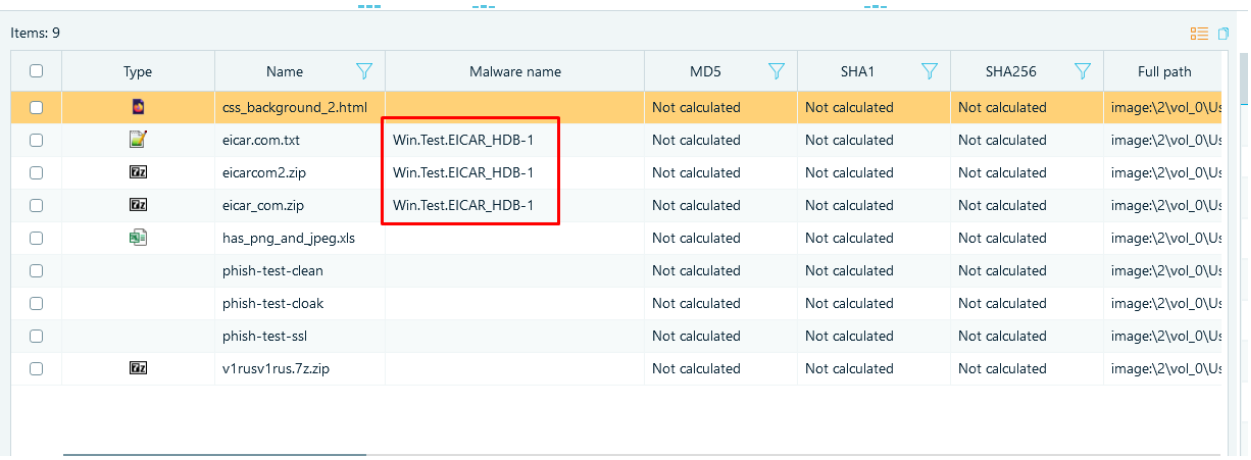


ClamAV analysis can be run from context menu in **File System** tab:

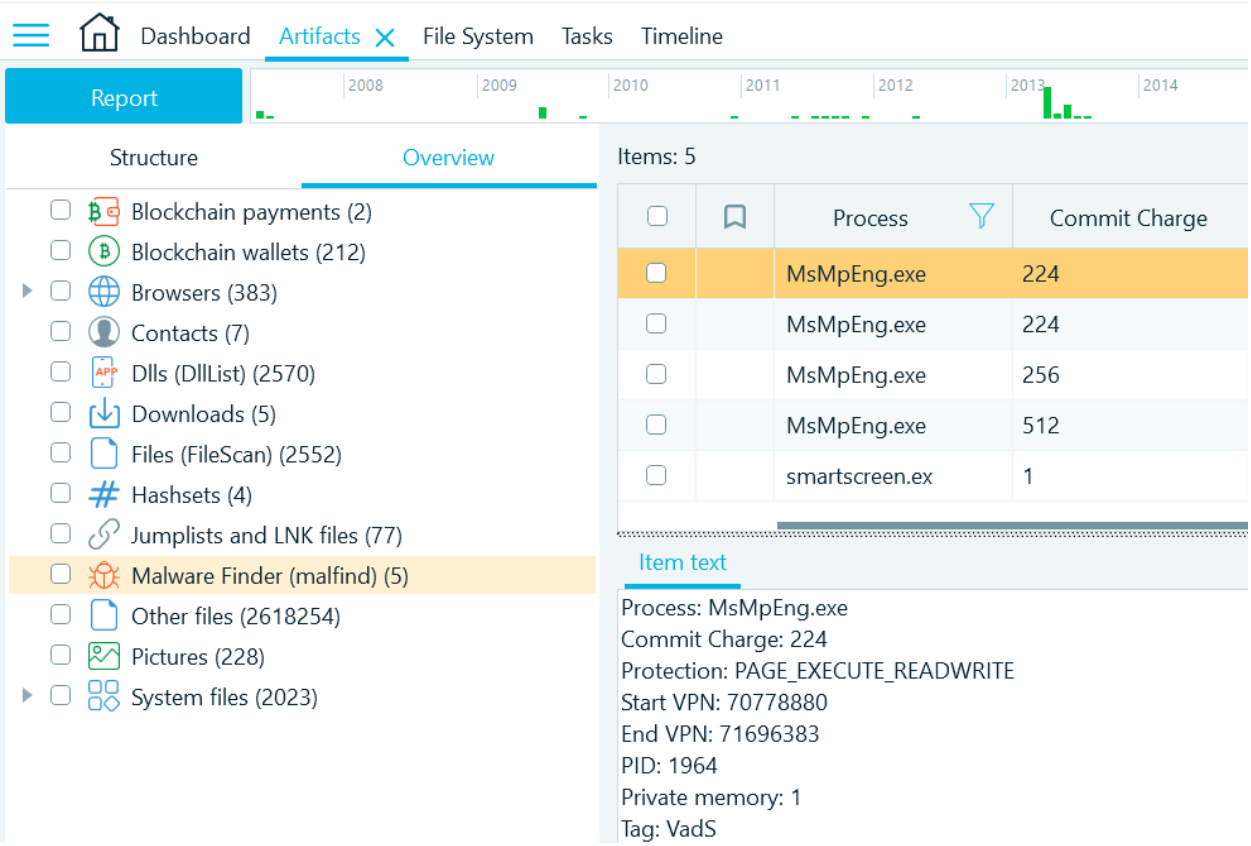


ClamAV results

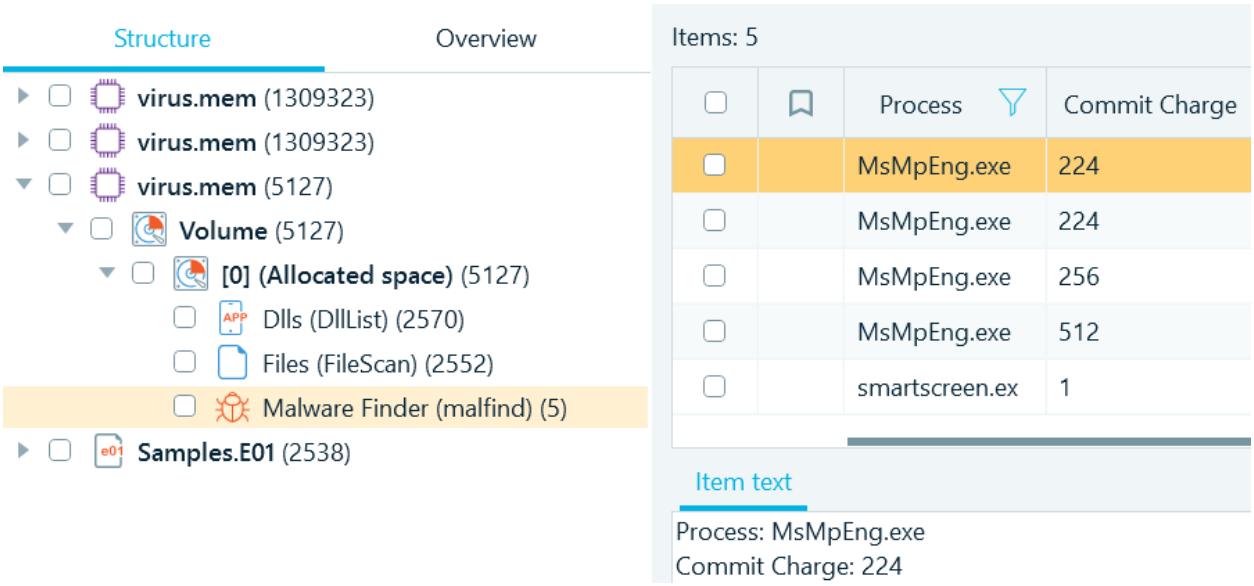
File system tab:



Artifacts tab Overview view:

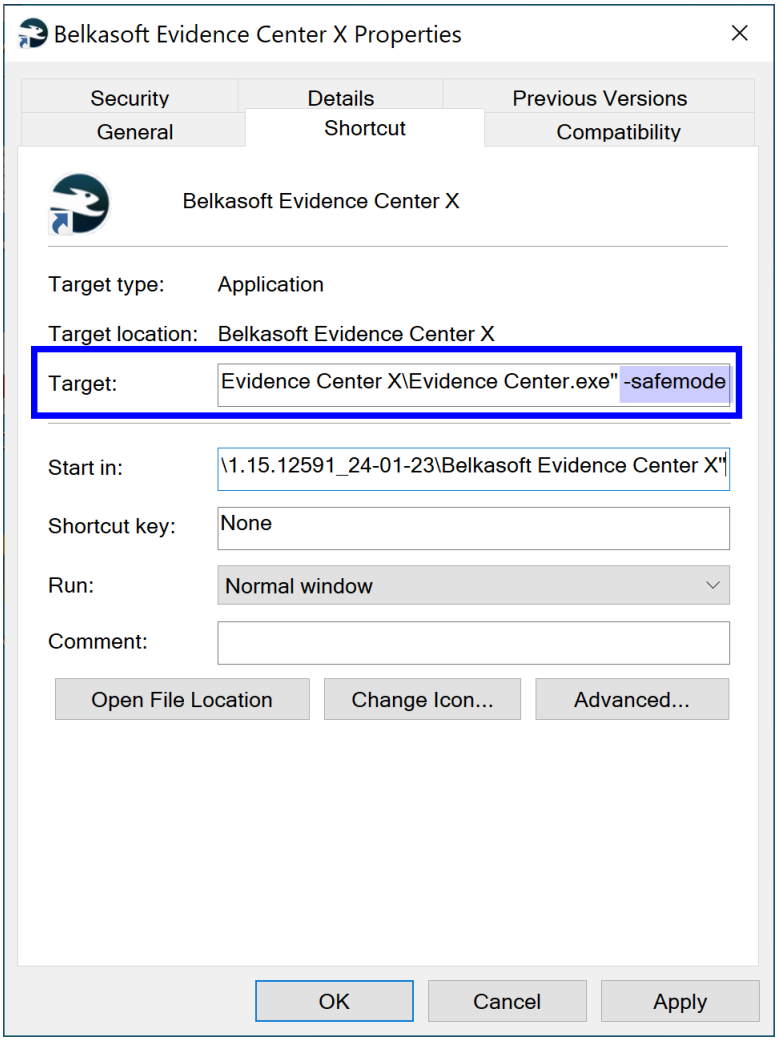


Artifacts tab Structure view:

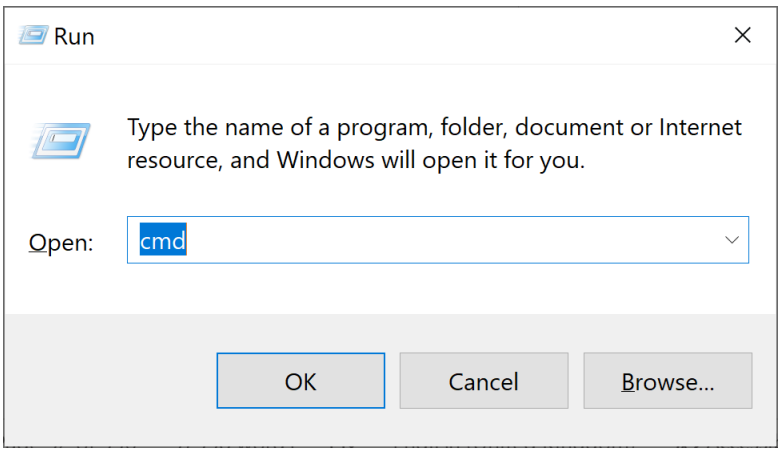


Start with default settings (safemode)

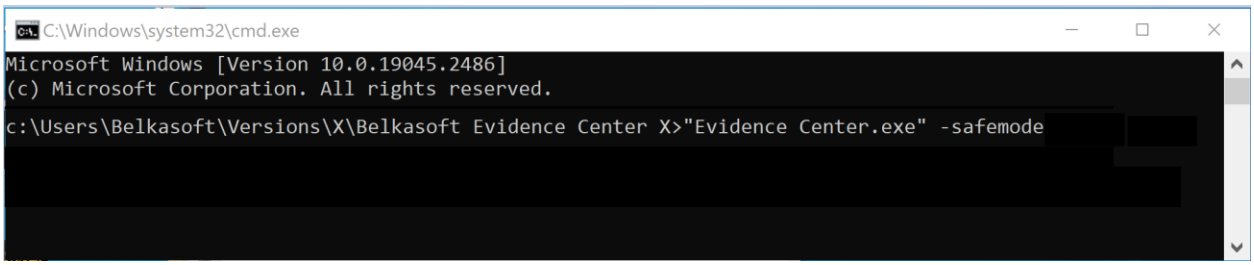
Right-click on the Belkasoft Evidence Center X shortcut - choose **Properties**. On a **Shortcut** tab go to the **Target** field and after the closing quotes type argument **-safemode** separated by a space. Apply the changes and launch Belkasoft X using the altered shortcut.
Note: You will need to provide administrator permission to change these settings.



Or you can use a command line:
Open the **Run** box (press buttons Windows + R). Type “cmd” into the box and then press Ctrl+Shift+Enter to run the command as an administrator.



Then start the product from the command line with the argument **-safemode**:



Other options and functions on Home screen

Opening Belkasoft X help

To open Belkasoft X help, click on **Product Reference**.

Checking for updates

To receive updates for Belkasoft X, click on **Check for updates**. Belkasoft X searches for current updates.

Viewing Belkasoft X info

To view information about Belkasoft X installed on your computer—available modules, support expiration and other details—click on **About**.

Closing Belkasoft X

To close Belkasoft X, click on **Exit**.

Belkasoft X tutorials

To watch a tutorial on a topic, click on the topic.

Note: Belkasoft X forwards the link to your browser and opens the tutorial video on YouTube. An internet connection is required to watch tutorial videos.

Accessing license info

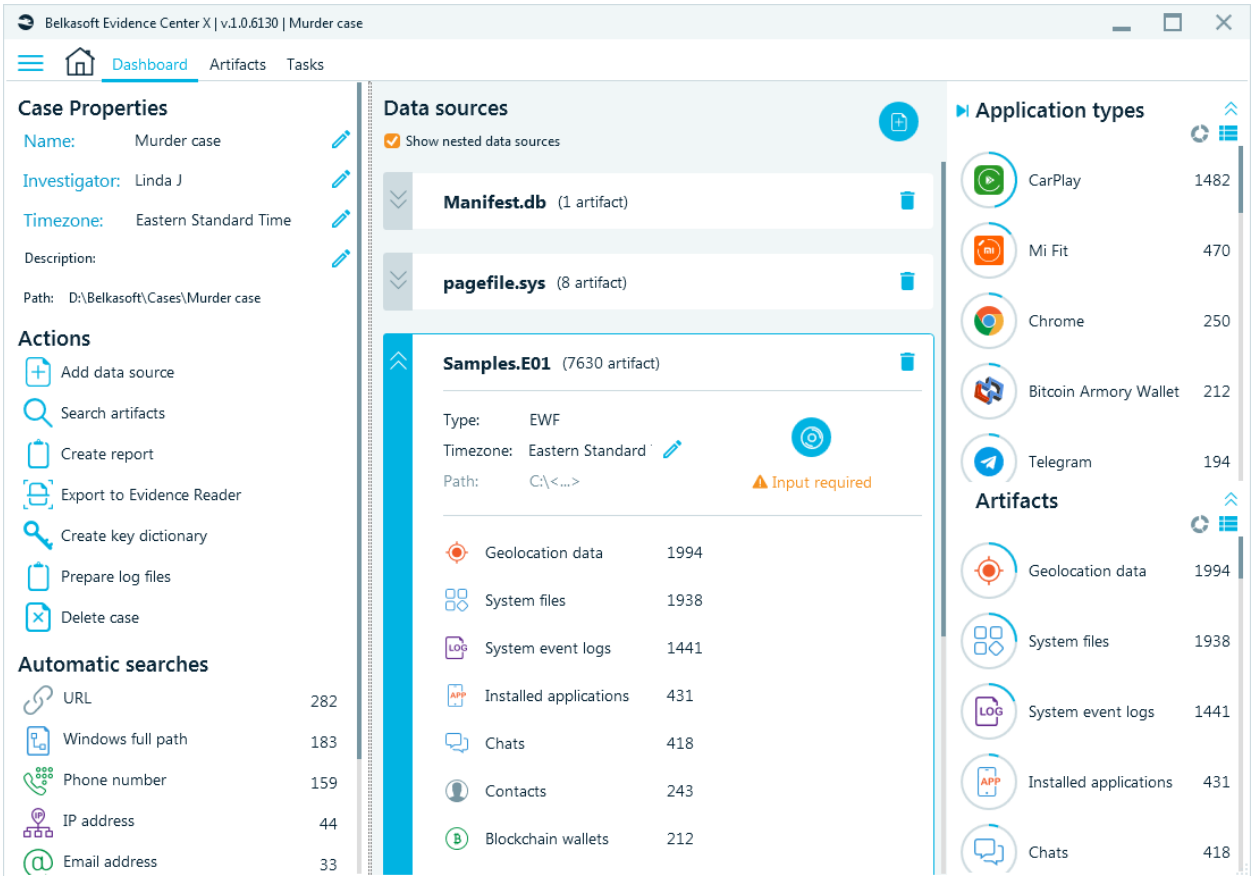
To view your license, click on License information. Belkasoft X presents your license details—to whom Belkasoft X is licensed, license expiry date, and installed modules—on the License activation window.

- **Extending your license**
  To extend your license, click on **Renew your support**. Belkasoft X now directs you to the customer portal on your browser window. Fill in your credentials to log into your account.
- **Activating and using another license**
  To activate or use a different license, click on Browse another license. Browse through your computer and select the license file.

To dismiss the License information window, click on **Close**.

Dashboard

Dashboard is the main product window. It is opened when you open or create a case. It has various actions about case and information on it.



The window is divided into three panes: left, middle and right.

From the left pane, you can access:

- Case Properties
- Actions
- Automatic Searches

Case Properties

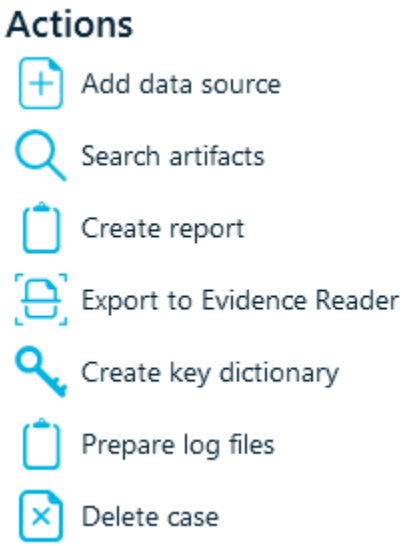
The following case properties are displayed:

- Name
- Investigator
- Time zone
- Description
- Path

Note: You can edit these properties with the help of a pencil icon. Path cannot be changed; however, you can click on it to copy.

Actions

Actions allow you to do various actions with the case.

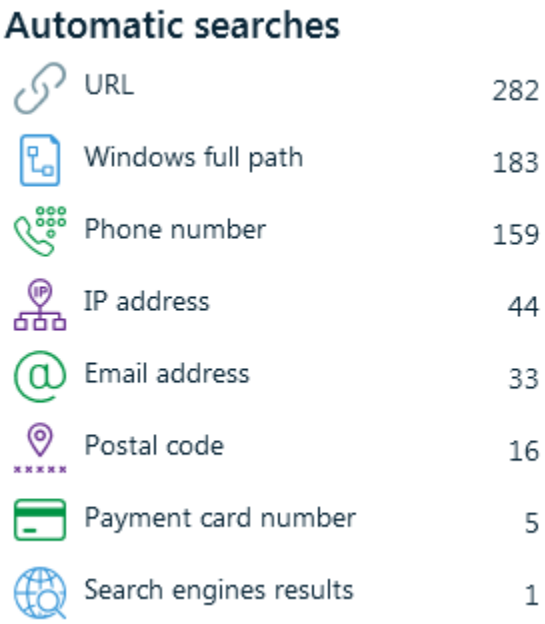


The following actions are available:

- **Add data source**, which you use to add any number of devices and images.
- **Search artifacts.** Using this action, you may locate any artifact already extracted by the product. Is important to mention that this kind of search does not search inside the entire drive or image. It also, does not look for files. It only searches for various artifacts like links, chats, documents, emails and so on, which you can then see on the **Artifacts** window.
- **Create Report.** Using this action, you able create a report for the entire case. Should you like to generate a report for just a selected portion of data, please go to **Artifacts** and other windows.

- **Export to Evidence Reader.** This function allows you to share all your findings with anyone, even if they do not have a paid Belkasoft X license. Evidence Reader is a free product, which helps a user to review cases or their parts exported from Belkasoft X.
- **Create key dictionary.** With the help of Create key dictionary action, you can generate a file with all languages used in all the artifacts in your case. Such a dictionary can be a huge benefit when you are decrypting something encrypted by a user. Note that it makes sense to use a created key dictionary only for files encrypted by the same user to maximize your chances for success**.**
- **Prepare log files.** Prepare log files option helps you when you have any difficulties working with the product. In such a case, run this action and send us the resulting archive, which will assist us in our efforts to provide you solutions for your issue.
- **Delete case.** You can delete a case, which you no longer need.

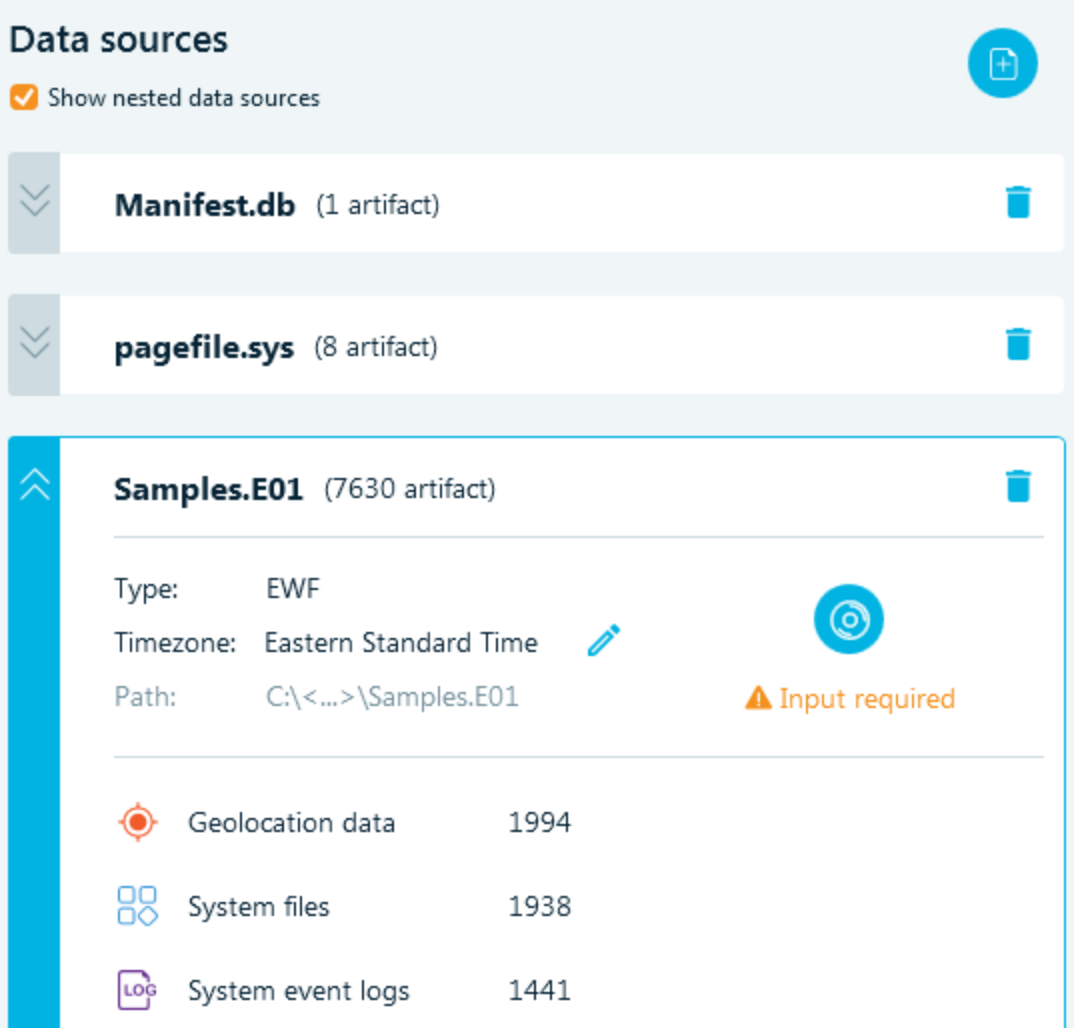
Automatic searches



These are searches of various interesting artifacts, which the product automatically performs as it analyzes data sources. You will find here things like phone and credit card numbers, IP and Mac addresses, links like video hosting URLs, and so on. You can double click on any result to navigate to the **Search Results** window for this particular type of automatic search.

Data sources

The middle part of **Dashboard** is devoted to data sources.



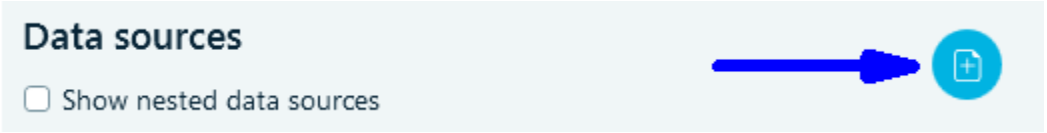
Note: The checkbox **Show nested data sources** helps you to filter out data sources automatically added by the product, which are stored inside data sources you added explicitly.
Every box in the middle part represents a data source. Each data source has a name, type, time zone, and path. You can click to the path to copy it and you can change data source time zone if it comes from a time zone other than case time zone. In this case, the time zone set for the data source will be considered primary and will override the case setting. As a reminder, time zone is particularly important when doing UTC from and to local time zone calculations.
For each data source, the total amount of artifacts is shown and, below, breakdown by most common artifact types, for instance, pictures, chats, or documents. For data sources, which were not analyzed, the amount of artifacts will be shown as 0.

You will also notice a status on the analysis, for example:

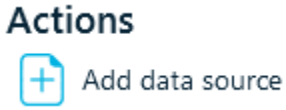
Double click to see the detailed information in **Tasks** window.

Adding a new data source

You can add a new data source from this pane:



Or select **Add data source** under **Actions**.

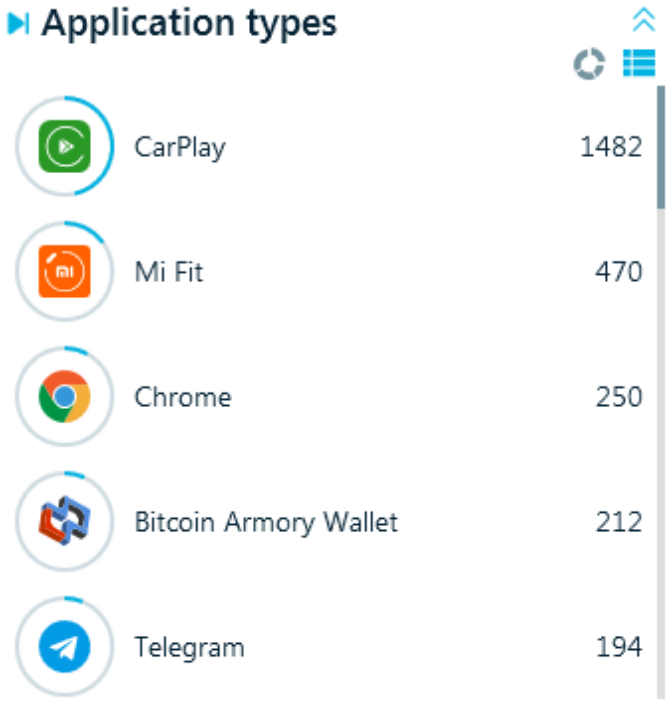


Case statistics

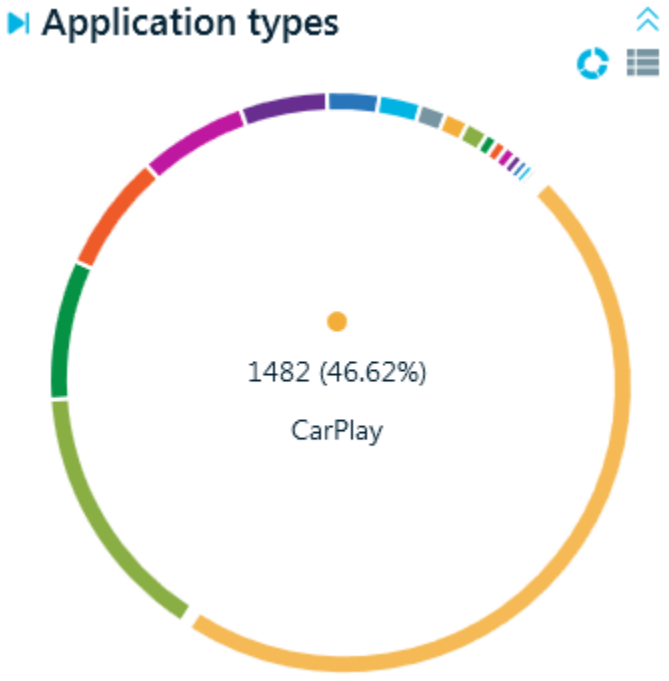
At the right, there are two graphs: most important applications sorted by number of artifacts extracted for each application, and most important artifacts. You can change the view for both graphs, from list to the pie chart. You can also collapse one or both, and you can collapse the entire panel to make more space for the data source part of the **Dashboard**. As with artifacts, you can double click on any item under each graph to navigate to the corresponding node in the Artifacts window.

Application types

- Under **Application types**, you will see a diagram of artifacts breakdown by application type. On the picture below, the case has most of artifacts extracted from CarPlay, then from Mi Fit. The most accessed chat app in the case was Telegram.



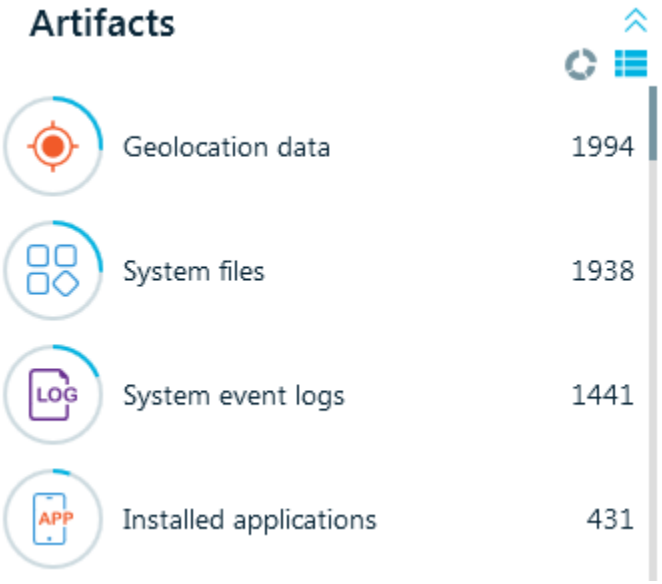
If you switch to the chart view using icon, you will see a pie chart. You could hover over any colored part of the chart to see the detailed information:



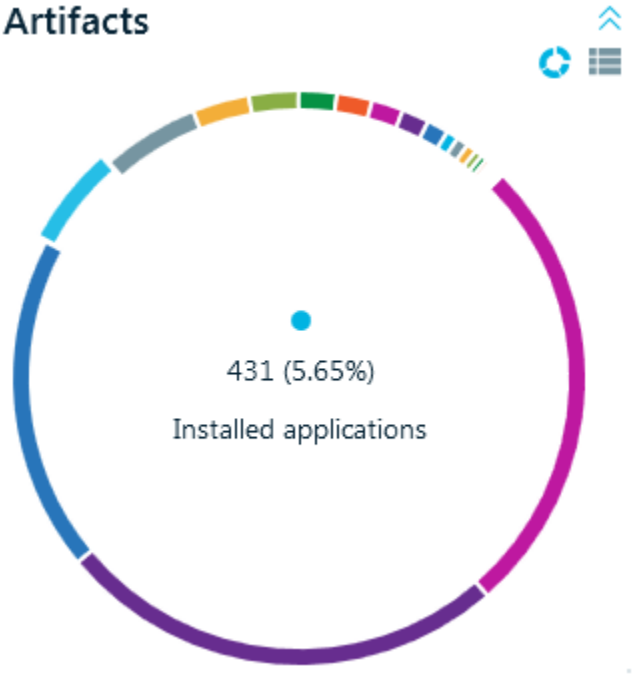
Artifacts

- Under **Artifacts** title, there is another chart showing you breakdown by type of artifact, such as mails, chats or browsers. Note the difference with the first chart by **Application types**, which

shows breakdown by application (e.g. Chrome or Safari) vs. breakdown by all browsers, all chats, all mail types shown here:



If you switch to the chart view, you will see a pie chart:

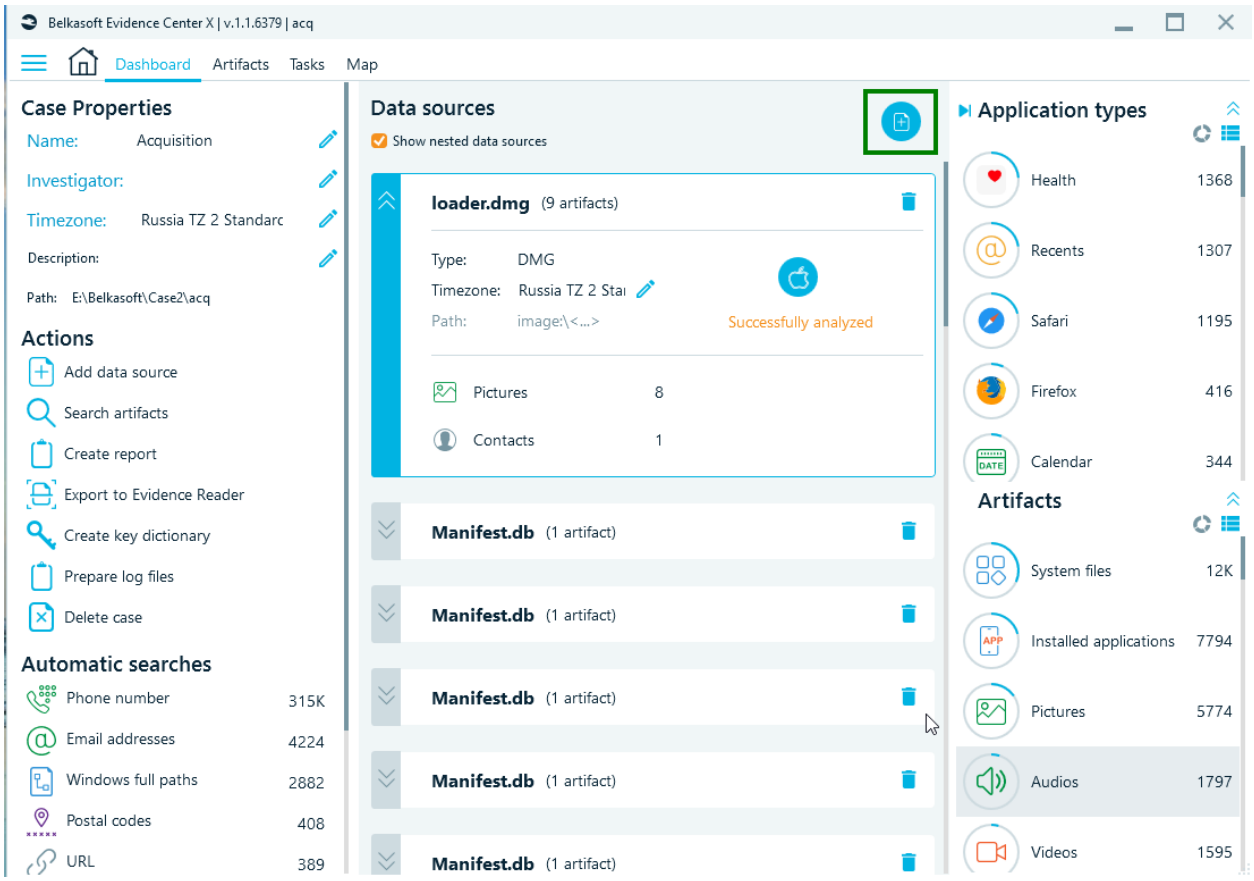


You could collapse one or both graphs using the arrows and .

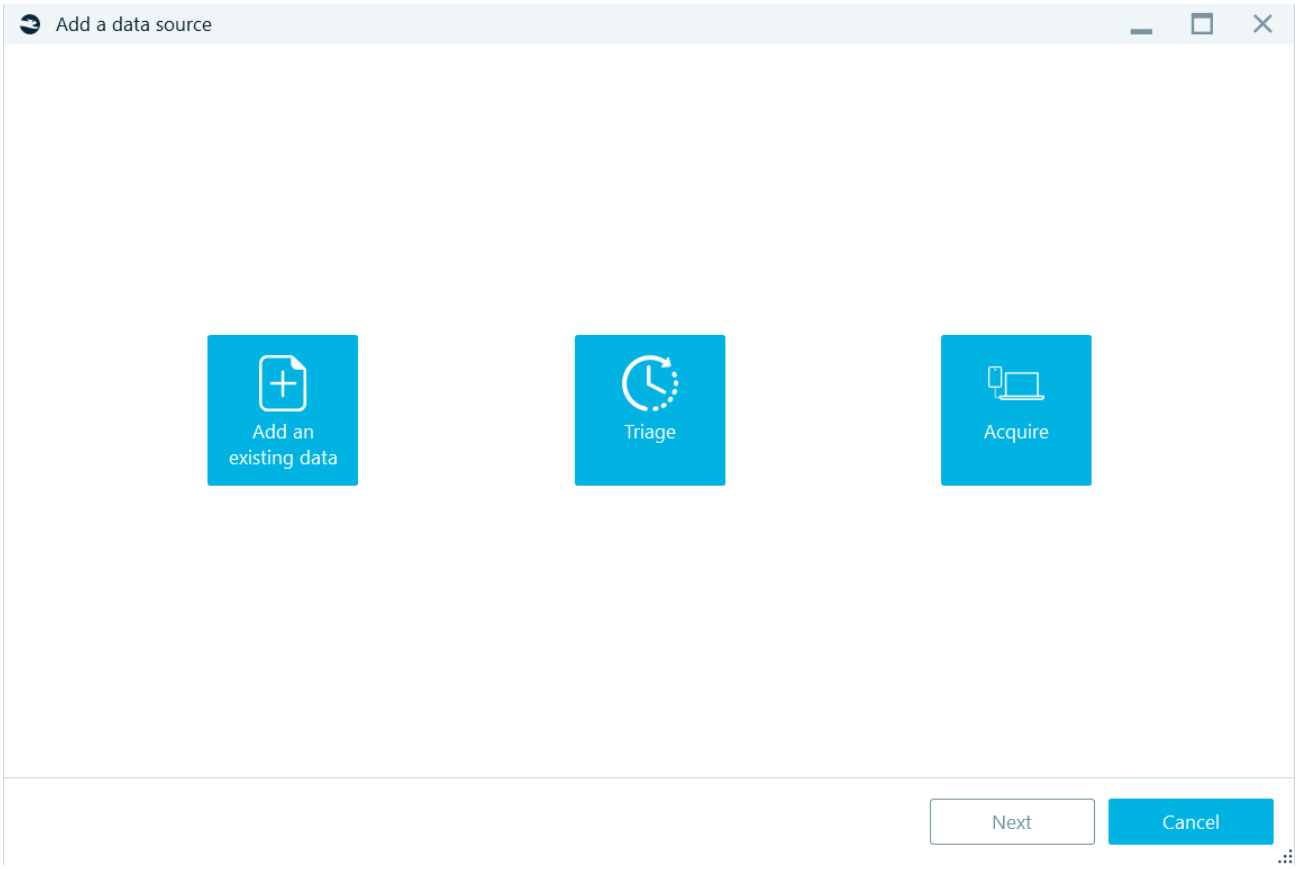
Adding data source to a case

Once you have created a case, you may start adding data sources to it. There are a few ways to add a data source:

- Using the button on the second page of a new case creation.
- Using the **Add data source** menu from the Actions menu of the **Dashboard** window.
- Using the round **+** button at the right top corner of the middle part of the **Dashboard** window.



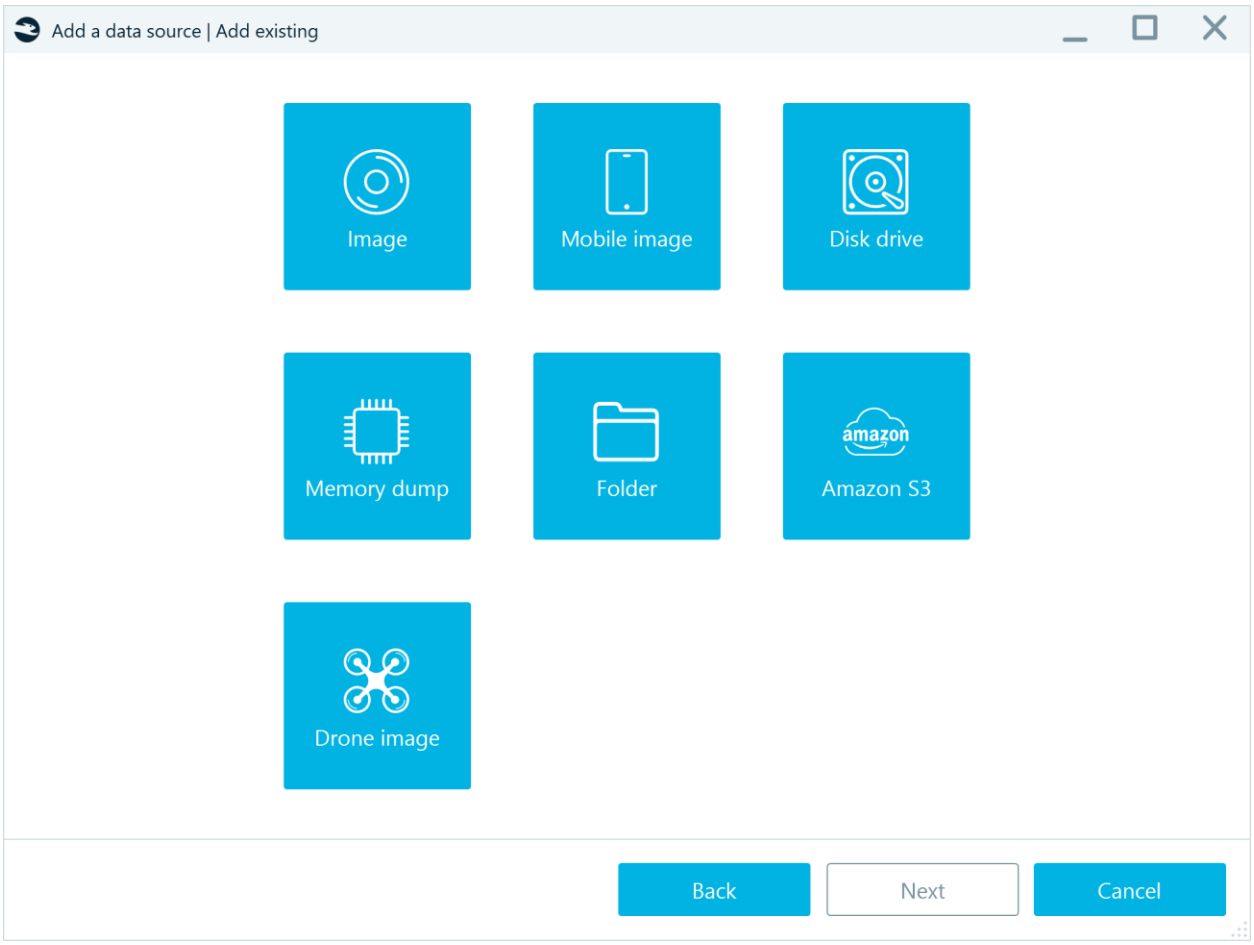
Whichever way you use, the following screen will be shown:



To add an existing data source, select the corresponding button at the left.
There are various types of data sources the product supports, including:

- Images of a computer or a mobile device, created by various third-party tools as well as by Belkasoft X.
- Disk and removable drives, including ones inside a hardware write blocker device.
- Memory dumps for various operating systems.
- Folders
- Drone image

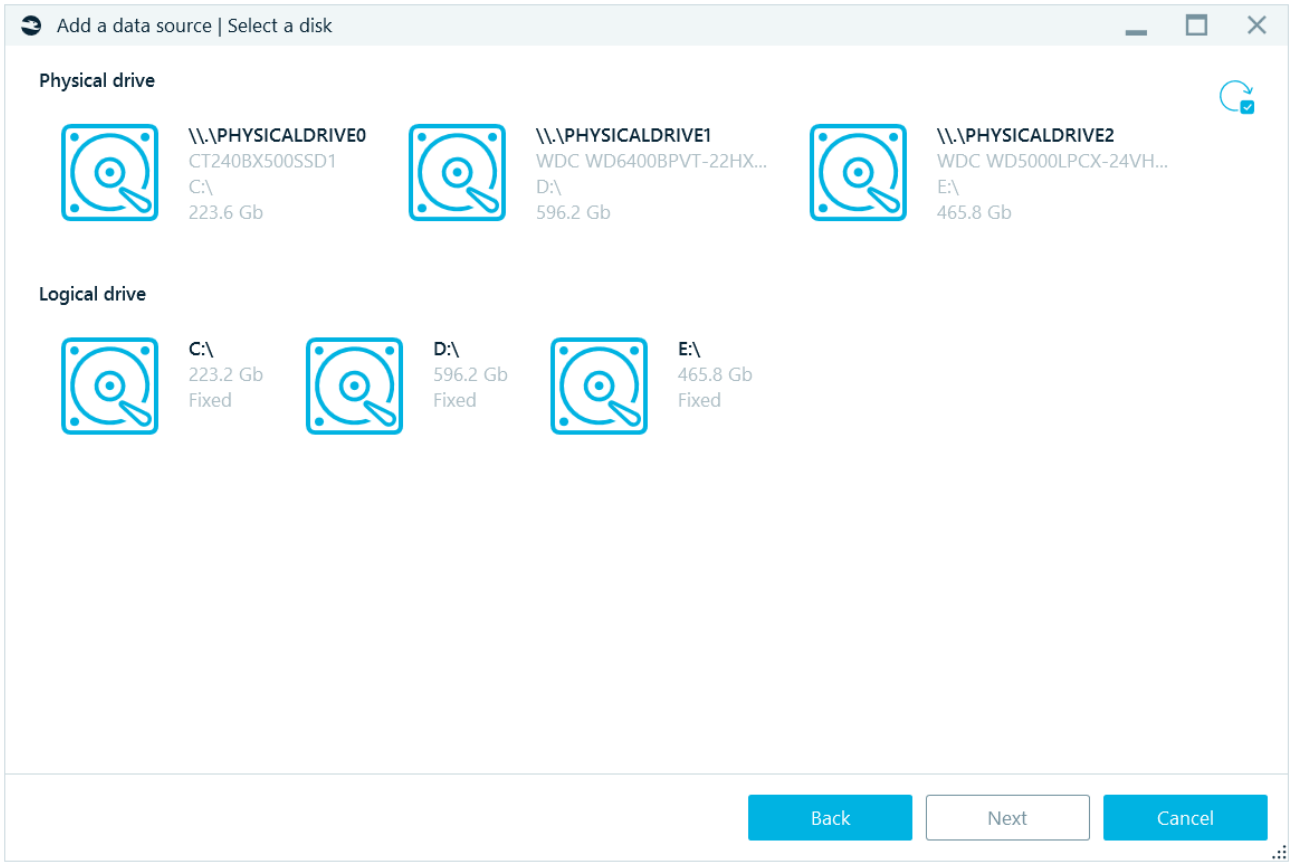
Select any of them on the **Add existing** window of **Add data source** sequence:



You will be prompted to browse for the image (for options **Image**, **Mobile image, Memory dump and Drone image**), a folder (for **Folder** option), cloud data stored in the **Amazon S3** cloud, and **Disk drive**.

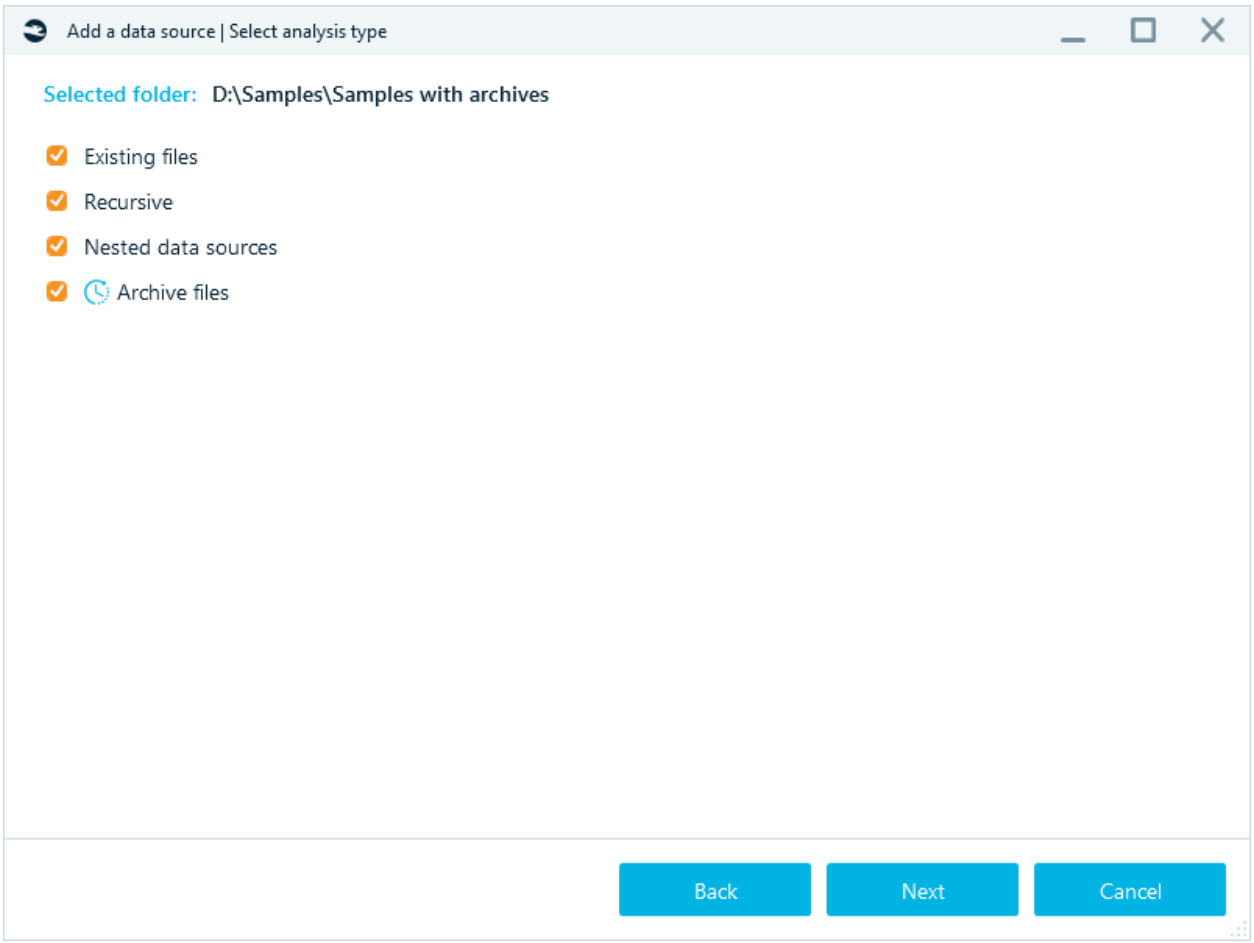
Disk drive

After clicking on **Disk drive**, you will be presented with the list of all physical and logical drives existing in your system:

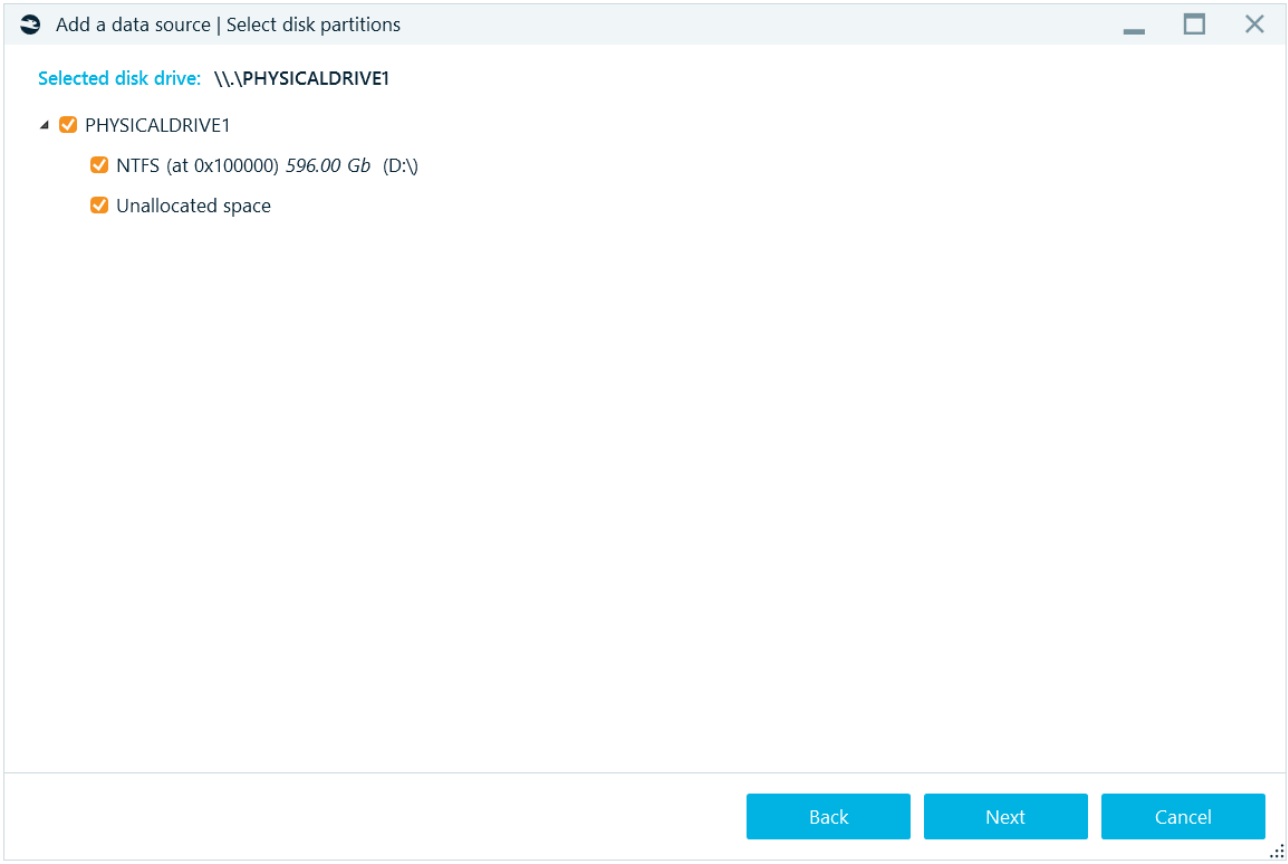


Select any physical or logical drive. If you just connected a device (for example, a removable logical drive), and do not see it in this list, click on the **Refresh** button at the top right corner.
Once you have selected a data source, you will be asked further questions, depending on the type of the data source. For example, for a folder there are the following options:

- **Existing files** option: analyze existing files found inside the folder.
- **Recursive** option: whether to analyze the selected folder along with subfolders, or analyze the selected folder only.
- **Nested data sources** option: whether to add a 'nested' (or 'internal') data source, such as a virtual machine file, page file, hibernation file, smartphone backup, DMG file, etc., found inside the folder, to the case.
- **Archive files** option: analysis of archives existing in the data source.

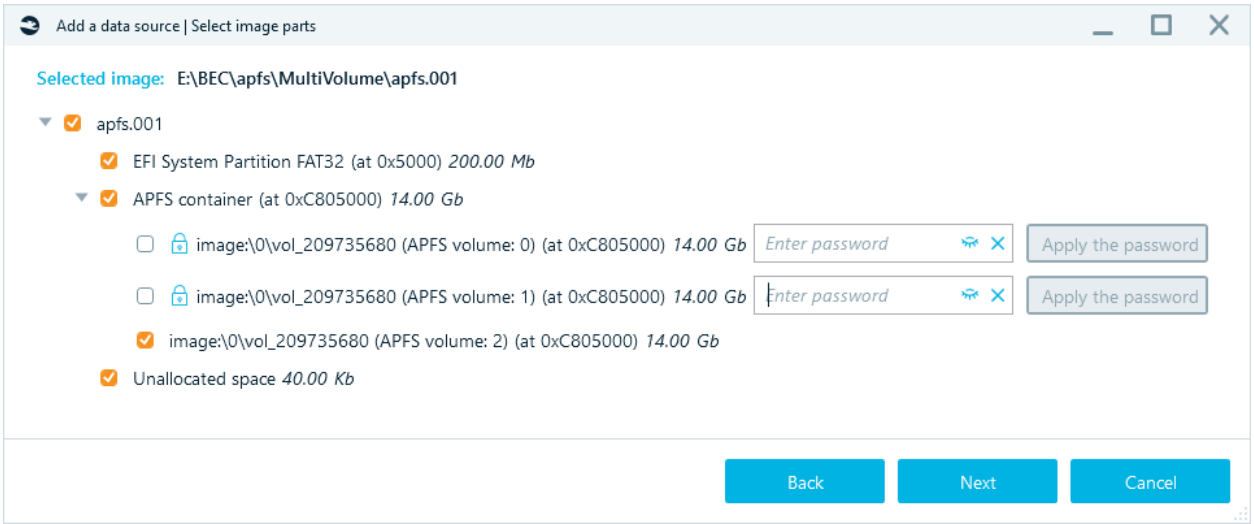


For a physical image of a disk, such as a computer or a mobile physical image and real hard or removable drive, the **Select disk partitions** window will be shown:

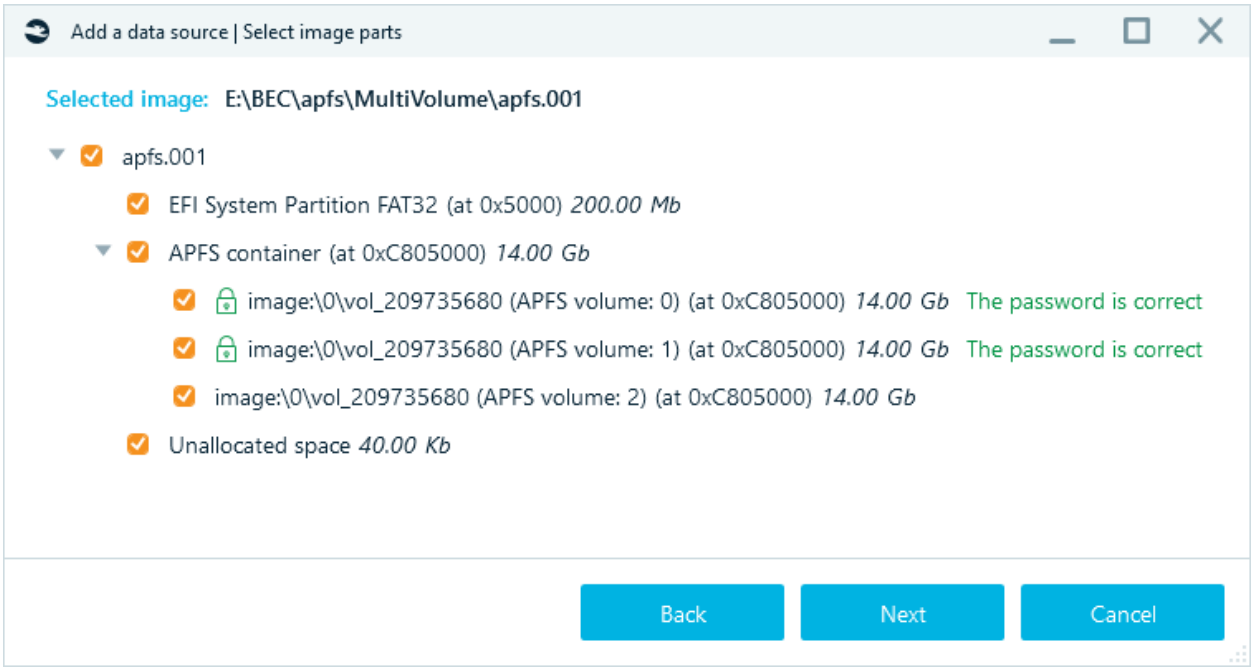


On this window you can select, which parts of an image to add to your case. This way, you can exclude parts of the data source, you do not need (for example, system or reserved areas).

If any of partitions are encrypted, the product will show you the **Enter password box** next to the partition name and the lock icon at the left of it:



Once you have specified a password, click on the **Apply the password** button. If the password is correct, the product will show you decrypted volume structure. The lock icon will turn green and the corresponding label will be shown for the partition (or, as on the screenshot, for an iTunes backup):



Otherwise, the product reports that the password is not correct, and you will get another chance to try another password.

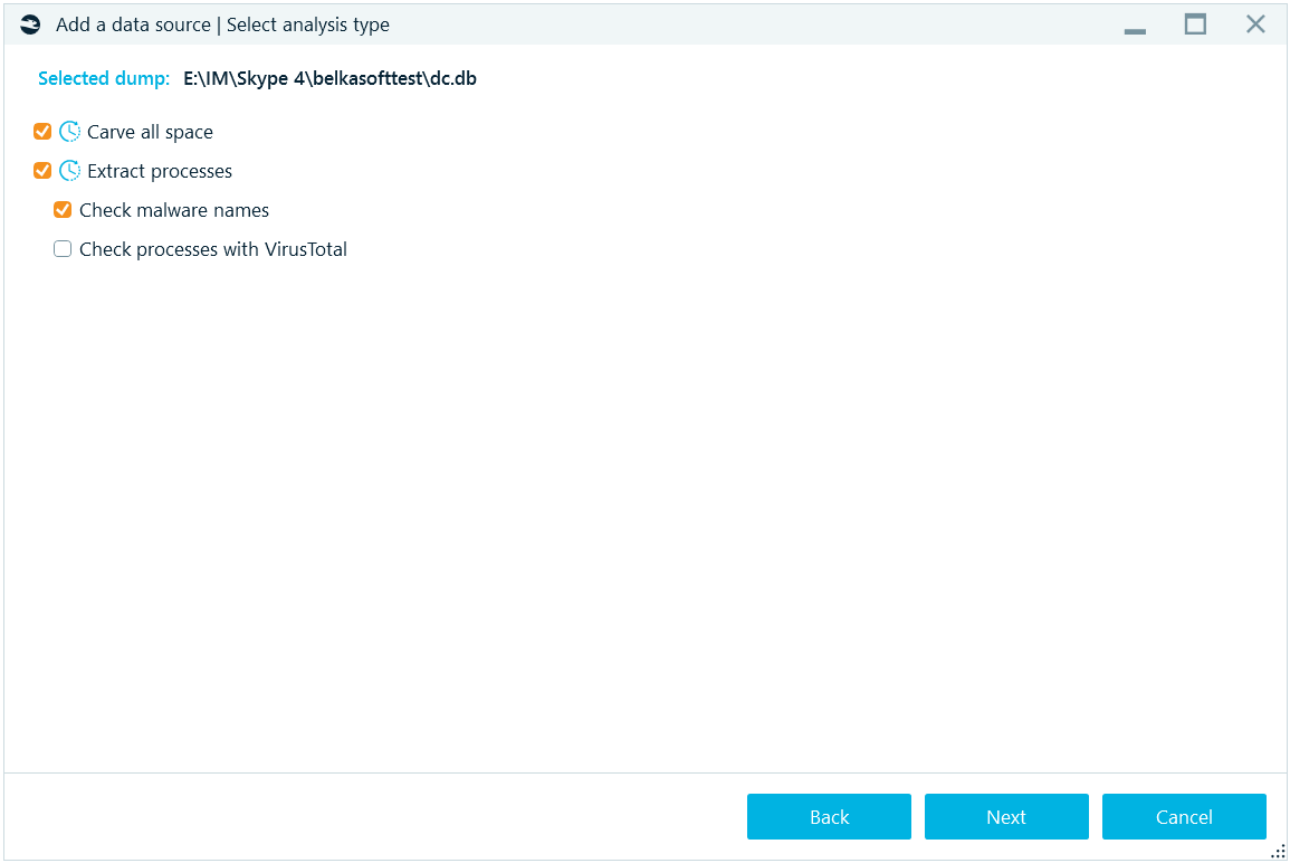
By default, your input is hidden inside the **Enter password** box, however, you can unhide it by using the eye icon.

Memory dump

After selecting dump options will be available:

- **Carve all space**: whether to carve the dump for artifacts, basing on signatures for different supported artifacts.
- **Extract processes**: whether to extract a list of processes which were running at the moment of the dump creation.
- **Check malware names**: this option is only available if you have opted to extract processes. For extracted processes, this will check if their names are suspicious (that is, mimicing a known system process name by slightly changing the name, say, s**cv**host.exe instead of s**vc**host.exe).
- **Check processes with VirusTotal**: the option is only available if you have opted to extract processes. For extracted processes, this will upload the entire process memory to VirusTotal and get the result of whether the process is classified as a malware or a virus. You will need an Internet connection for this analysis to work properly. Also note, that the entire process memory is uploaded (not a hash value, as for files) because the process is different every time it is run and uploading its hash value will give you no meaningful results.

Note: the clock icon , which designates a 'long operation'. It is shown for every option, which will presumably take a lot of time. Consider unchecking such options if you do not really need to view them.



Options **Check Malware name** and **Check proceeded with VirusTotal** can also be run in the **File system** tab.

Amazon S3

Belkasoft X supports the analysis of cloud data stored in the Amazon S3 cloud https://aws.amazon.com/s3/.

Amazon S3 or **Amazon Simple Storage Service** is a service offered by Amazon Web Services (AWS) that provides object storage through a web service interface. Amazon S3 can store any type of object, including data images, mobile images and memory dumps.

The registration is needed in order to use the Amazon S3 cloud storage. To connect with the Amazon S3 service from Belkasoft X GUI, one will need these Amazon credentials:

- **Access key ID** (20 symbols)
- **Access key** (40 symbols)

How to get Amazon credentials

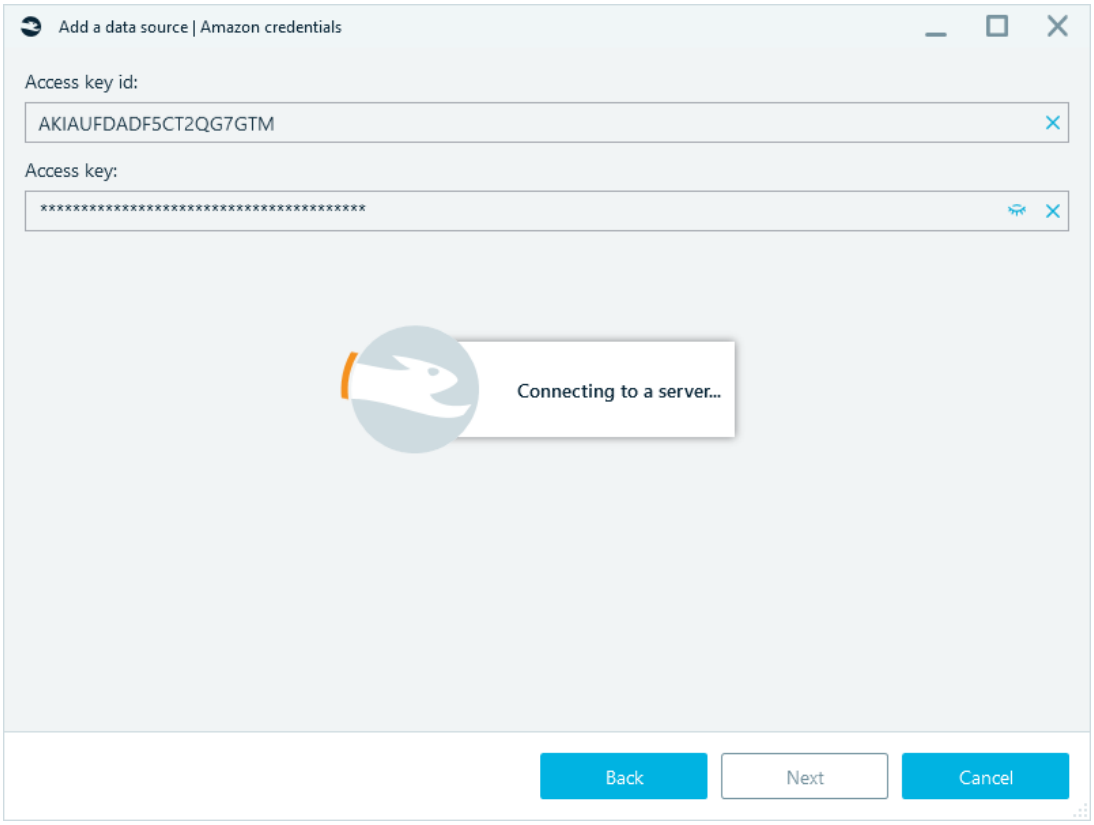
Once you are registered at Amazon S3, set up a user with programmatic access at the IAM console

https://console.aws.amazon.com/iamv2.
Keep in mind security recommendations https://docs.aws.amazon.com/IAM/latest/UserGuide/best-practices.html#create-iam-users.

1. In the navigation panel, choose **Users**, and then choose **Add user**.
2. Provide a user name, select **Programmatic access** checkbox, navigate to the next page.
3. Choose **Attach existing policies directly permission**. In Search, enter **AmazonS3FullAccess** and select the filtered policy option.
4. Finish creating the user, the following pages can be left untouched.

Amazon S3 data source analysis

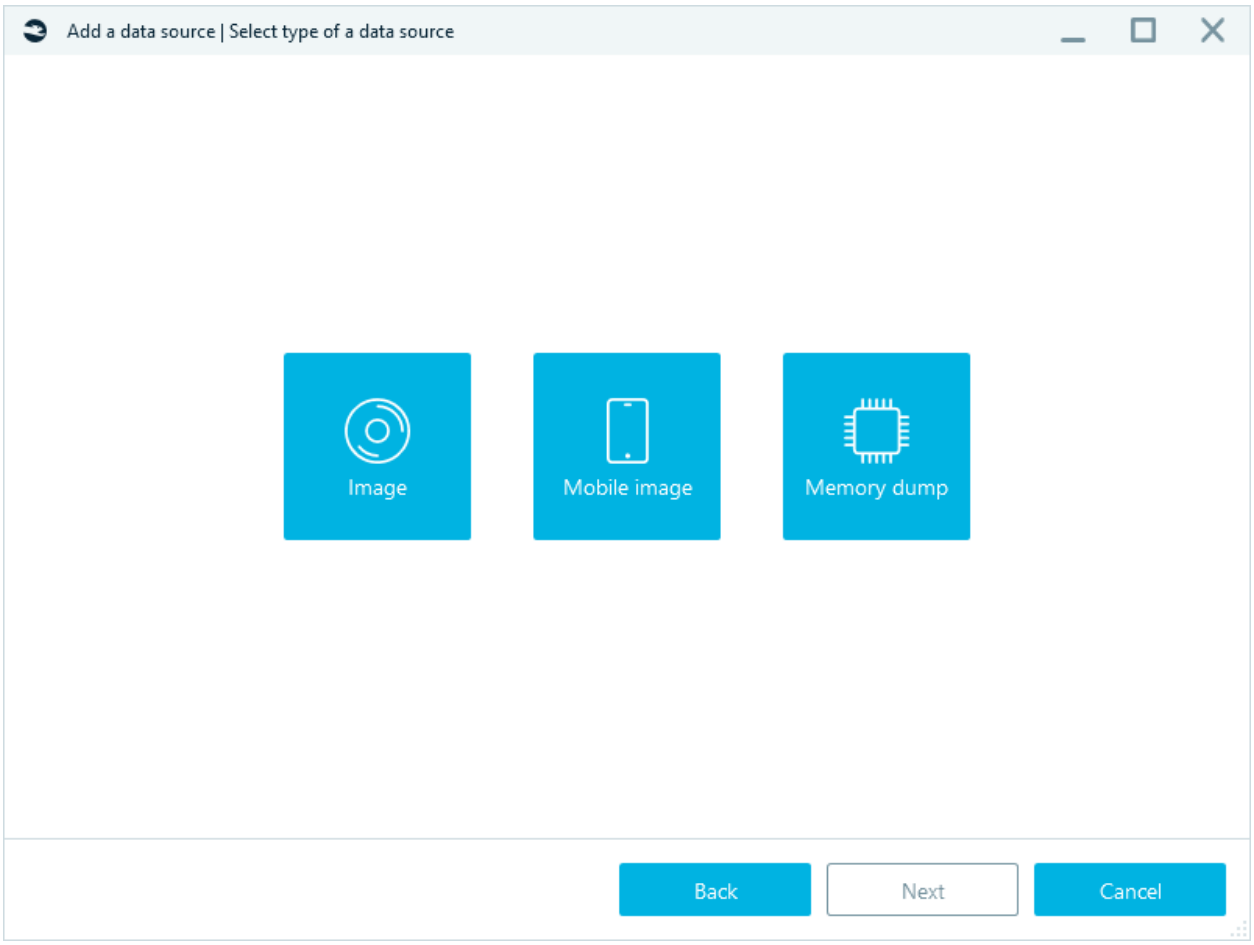
After clicking on **Amazon S3** enter your Amazon credentials and click Next:



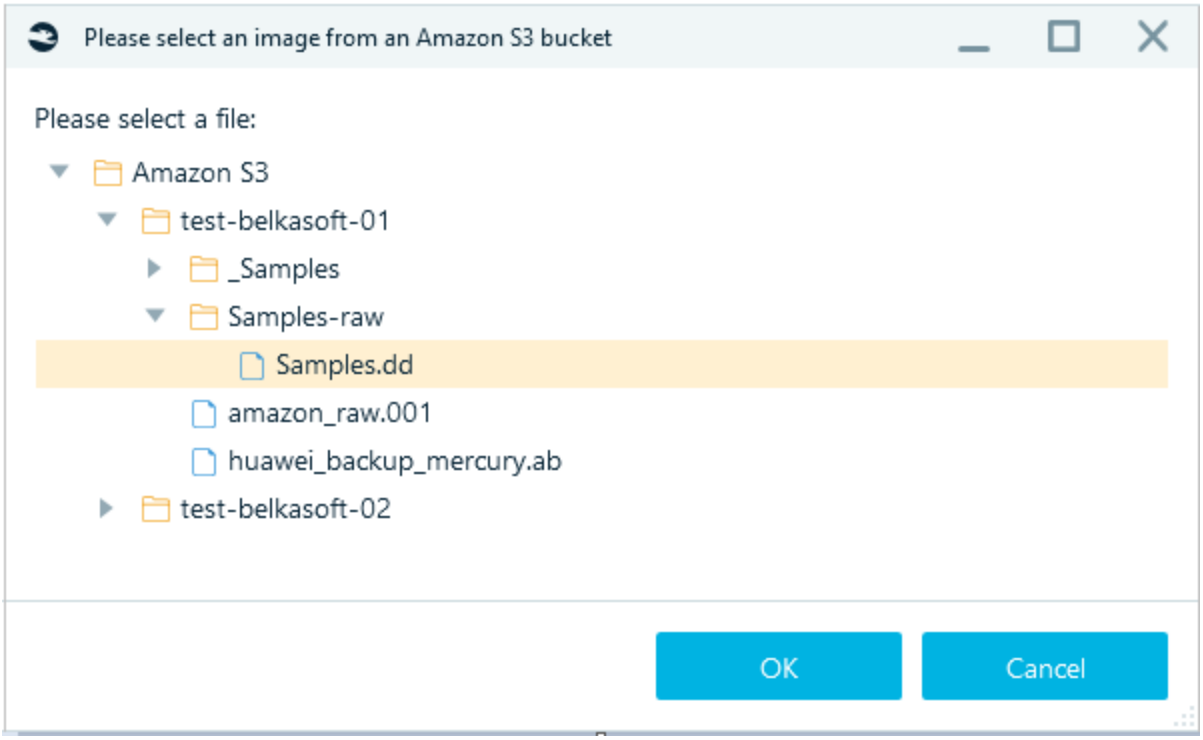
Select the type of the acquired data source. Three options are available:

- Image
- Mobile image
- Memory dump

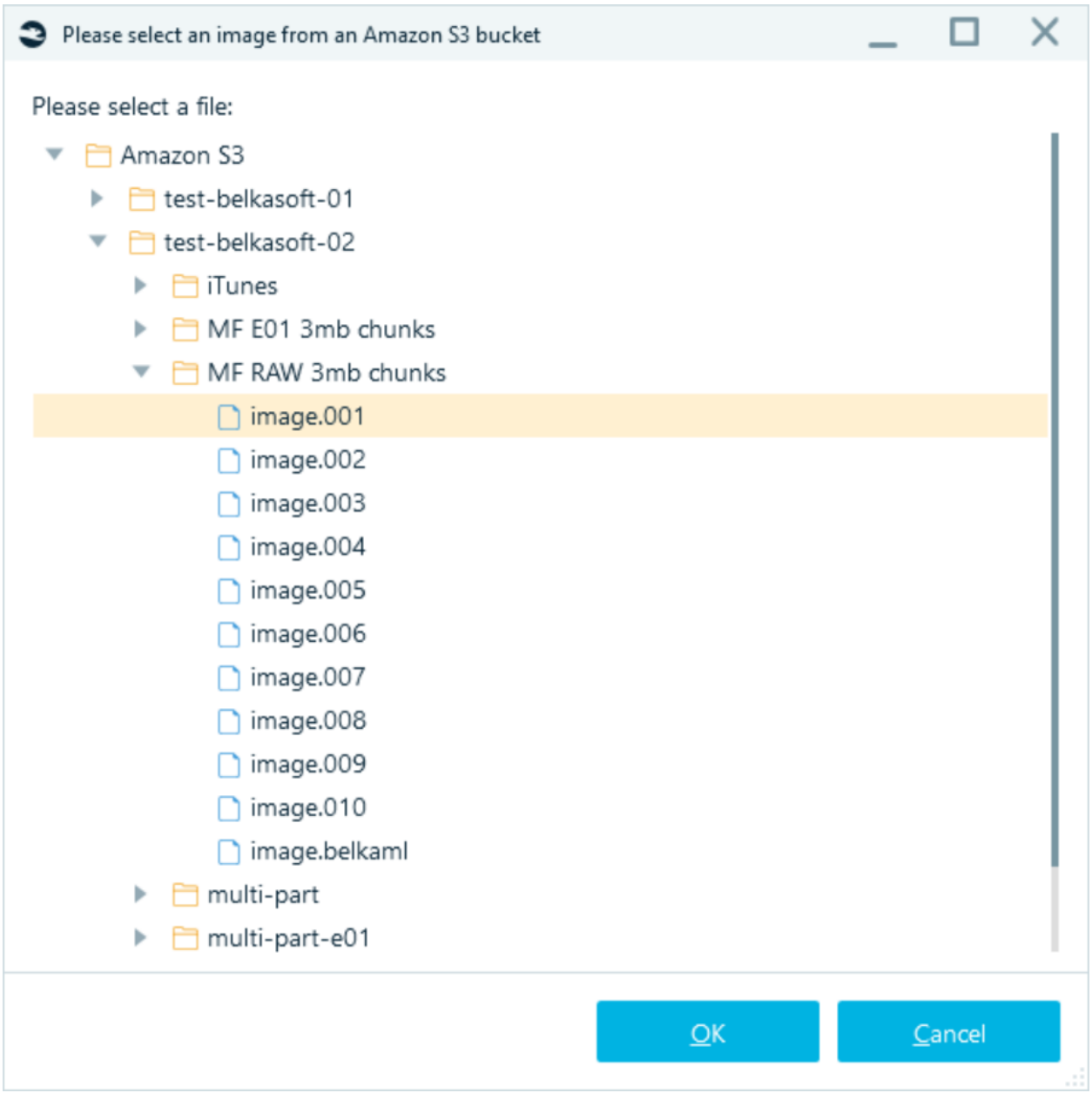
The Image analysis supports both multi file and single file images in RAW and E01 formats.
Please note - if a multi file image was acquired via Belkasoft X and uploaded together with its .belkaml file, for the analysis one needs to select the first chunk of the image rather than the corresponding .belkaml.



Then choose the data source of interest in the built-in file browser, click OK.



Single file image



Multi file image

A standard Add data source wizard will be opened; analyze your cloud data source exactly the same way as local data.

Note: only the **Carve all space** option is available for memory dumps stored in Amazon S3. For more options (processes extraction, malware names checking, VirusTotal checking) analyze the memory dump locally.

Drone image

Belkasoft X allows ingesting, parsing, and analyzing of the following drone models:

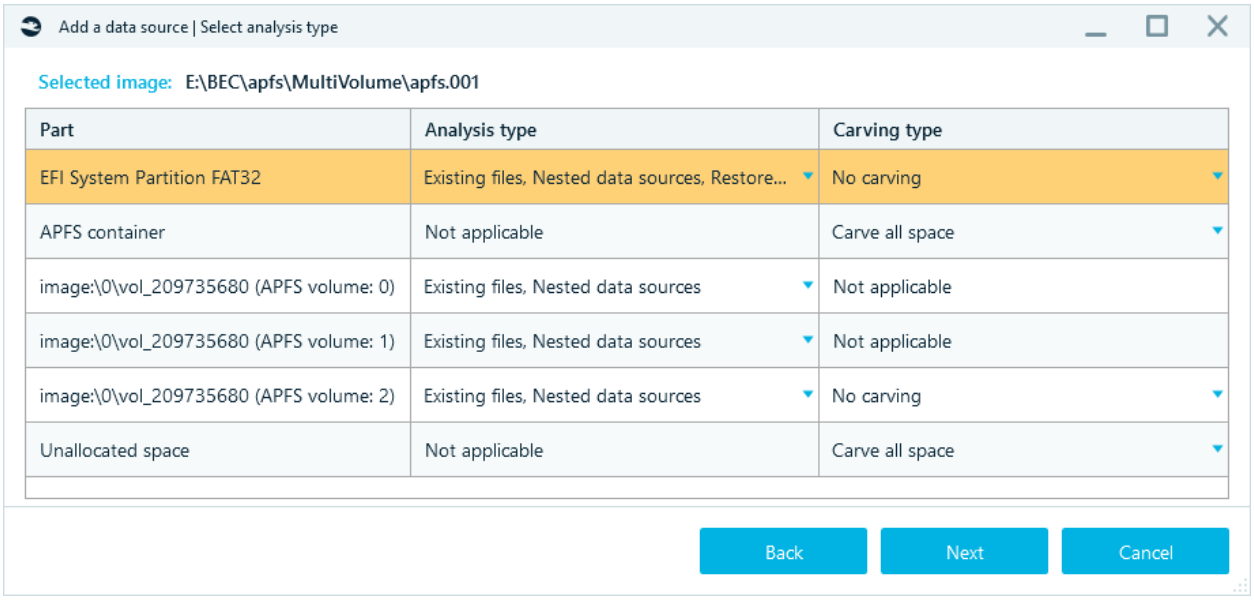
- ArduPilot DIY Drone
- DJI Agras MF-1S

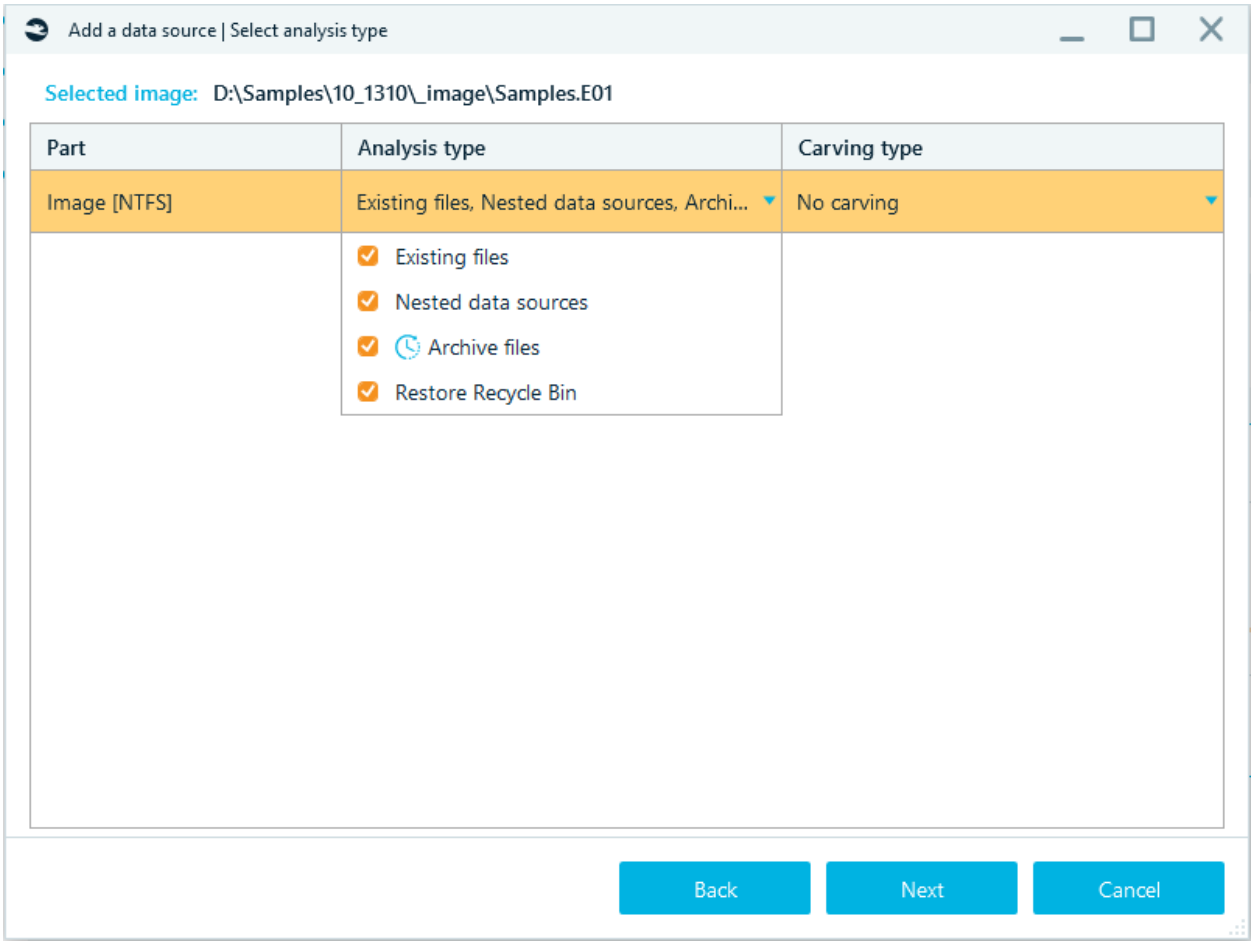
- DJI Matrice
- DJI Mavic
- DJI Phantom 3
- DJI Phantom 4
- DJI Spark
- Parrot Anafi
- Yuneec Typhoon Q500

You can also analyze compatible drone models.
The most important types of data supported include geolocation and tracks, pictures and videos, operator logs, and tracks.

Analysis type

On S**elect analysis type** window, you can fine tune what kinds of analysis to perform on each separate part of the selected image or disk:





There are two columns on this window for fine tuning the processing of the data source: **Analysis type** and **Carving type**.

Analysis type combines all options, which are based on the file system information, such as:

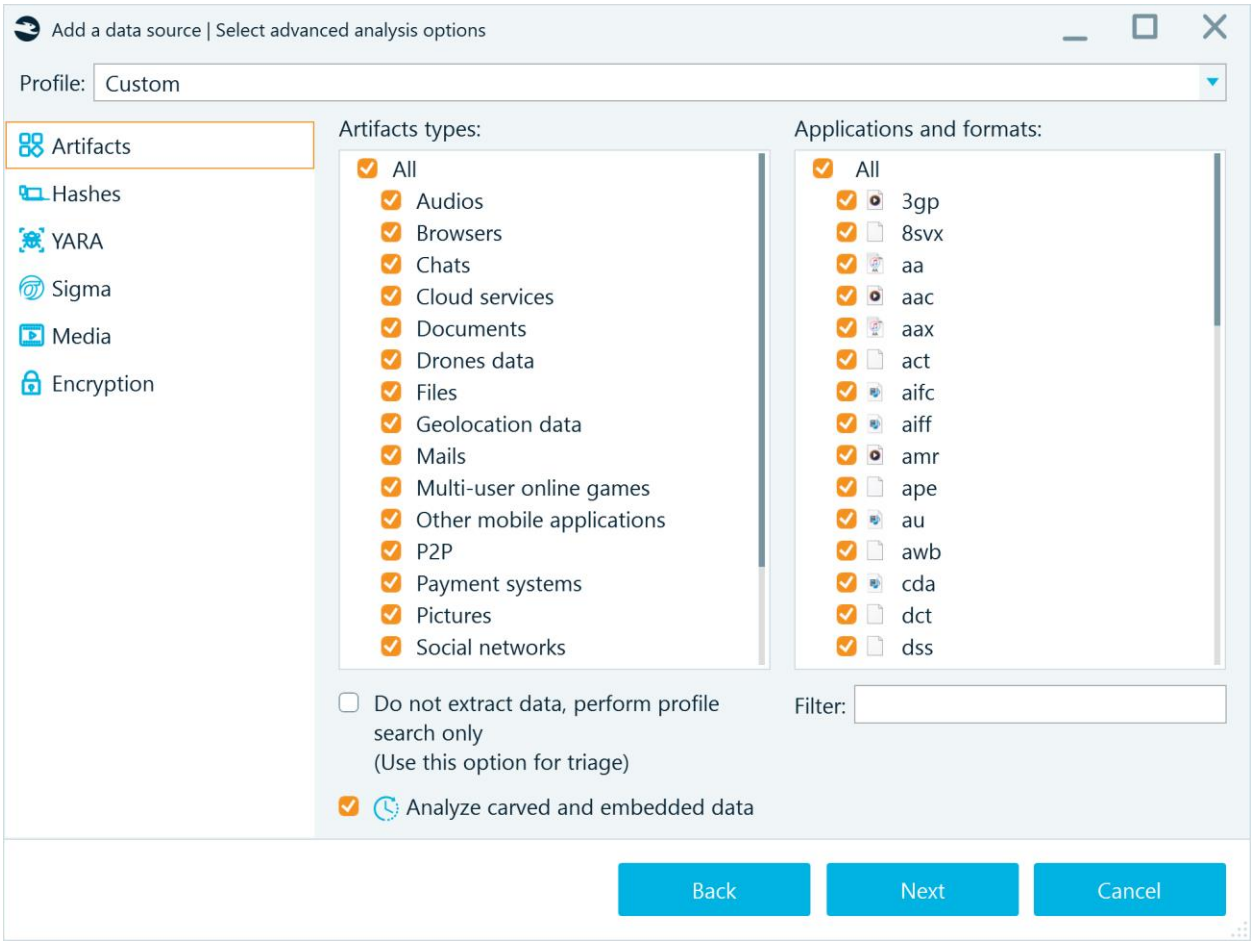
- **Existing files**: searching for artifacts inside existing files.
- **Nested data sources**: adding nested data sources to the case or not.
- **Archive files**.
- **Restore recycle bin**: NTFS-only option which instructs the product to analyze information about file names of files deleted to the recycle bin.

Carving type combines all options, which are based on the search for signature, such as:

- **No carving**: do not run search for known signatures.
- **Carve all space**: carve all available binary data inside the data source and try to recover artifacts based on known signatures.
- **Carve free space**: NTFS-only option which instructs the product to carve only space which is allocated but not occupied with data. This option allows saving time by not carving unallocated space and occupied allocated space.

Advanced analysis options

After this selection is completed, the product shows you **Select advanced analysis options** window:



Here, you can select a profile (see 'Profiles' section of this reference) to quick start with predefined options.

Artifacts

On **Artifacts** tab you can specify artifacts you would like the product to extract and carve. Note, that once you select an **Artifact type** in the middle part of this tab, corresponding **Application types and formats** are shown. You can select all or some or none of artifacts to look for.
Selecting **Artifact type – Files** allows you to extract by signatures (for the case when carving options are selected). Including signatures specified in Carving setting.

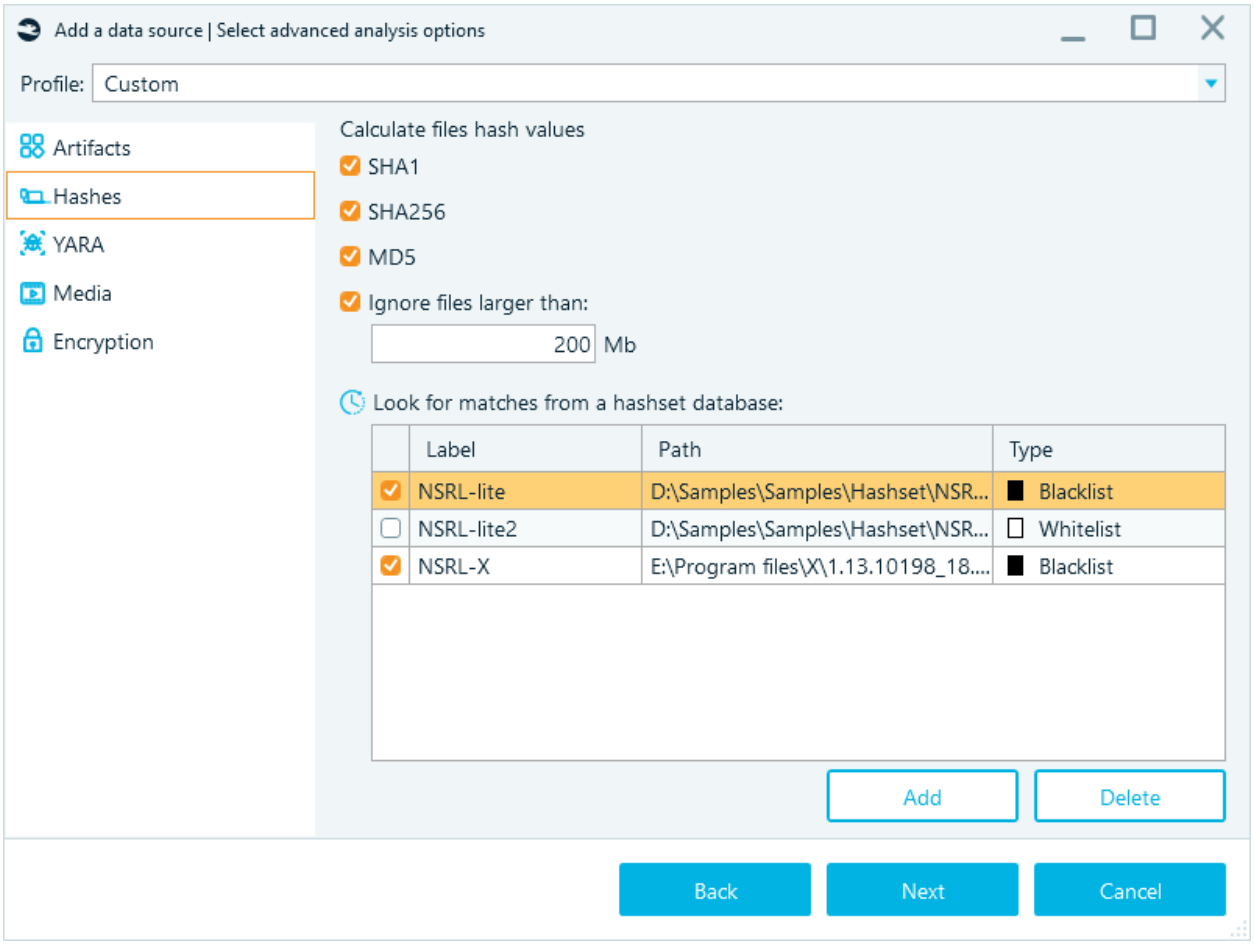
Below, there is the box called **Do not extract data, perform profile search only**. This box allows you to not extract data for application profiles (which may take a while) but to show corresponding profiles only. As an example, instead of extracting mails from an Outlook mailbox, with this option checked the product will only show you that the mailbox exists. This option can be useful to create your own Triage profiles. Alternatively, you can use **Belkasoft Triage**.

Analyze carved and embedded data - allows you to extract metadata from embedded pictures and documents obtained during file analysis. In addition, it launches metadata extraction for files and documents restored during carving.

In addition, using the Filter box, you can filter out only applications and formats, which have specified substrings in their names (for example, for 'an' they will be 'T**an**go', 'H**an**gouts', 'Trilli**an**' and others).

Hashes

On the next tab, **Hashes**, you can specify hashing algorithms to use and other options:



The algorithms available are:

- **SHA1**
- **SHA256**
- **MD5**

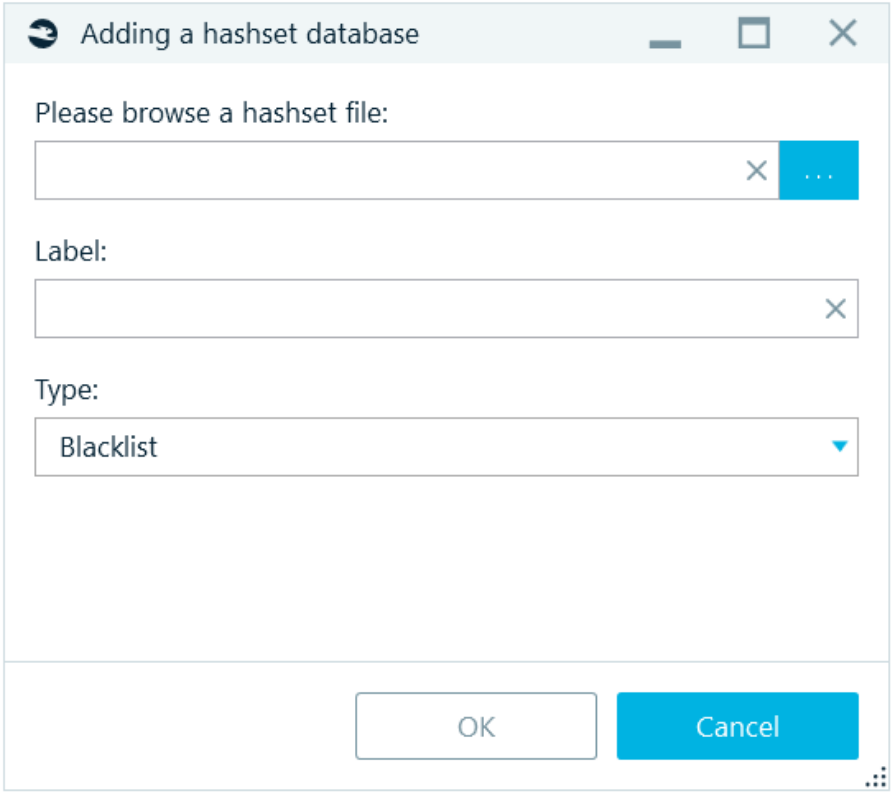
Note: MD5 is notoriously known to have collisions. It is recommended to use SHA256 or the pair of SHA1 plus MD5. More on hashing can be found at Belkasoft trainings (https://belkasoft.com/training).
Since large files may take a while for their hash calculation, you may decide to exclude such files. With the default settings, files larger than 200 megabytes will not have hash values.

Look for matches from a hashset database

You can add one or multiple hashset databases against which you can look for matches. The following types of hash databases are supported:

- **NSRL**
- **RDSv3**
- **ProjectVic** versions 1.3 and 2.0
- **Plain files** in text and CSV formats. This option is most handy if you would like to provide the product with your own hashset. You may create a simple text file with one hash value per line. You do not have to specify the hash algorithm in this case, the product will understand it automatically. For a CSV file, you may provide the column name such as **MD5**, **SHA1**, **SHA256**.

Once you have a hashset file or a database, click on **Add** button to browse for it:



The **Label** on this window can be any text you like. The **Type** can be one of the following:

- **Blacklist**: which means that any match with any hash in this database must be reported to the product's Overview tab under **Hashsets** node
- **Whitelist**: this means that such files are harmless and can be ignored (for example, system dll files). The product will not show such files in its File System window

In order to run search for matches, you have to select at least one of the hash algorithms on top of the window and check at least one hashset database under **Look for matches from a hashset database**.
Note: adding a hashset database is not enough, it must be also checked in the list.
At any time, you can delete one or multiple hashset databases with the help of **Delete** button.

YARA

YARA is a tool that helps software researchers identify and classify malware or files they are interested in. The target can be an image, a file, a folder, or a process.
YARA's docs can be found here: https://yara.readthedocs.io/en/stable/gettingstarted.html#.

Rules setup

YARA performs signature analysis based on formal YARA descriptions - rules. They contain indicators of compromise for different types of malware.

Rule template:

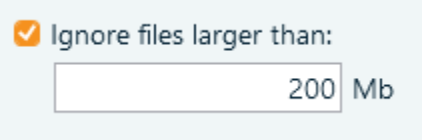
```
rule Sample {
    meta:
       author="Belkasoft"
       date = "01.01.2023"
       version="0.1"

   strings:
       $my_Sample_string = … //comments

            condition:
                    $my_Sample_string
}
```

Strings
Definitions sections - contains constants, hashes, HEX fragments, links, strings characteristic of malware;
Condition
Condition section — contains the conditions by which decisions are made regarding the analyzed file.

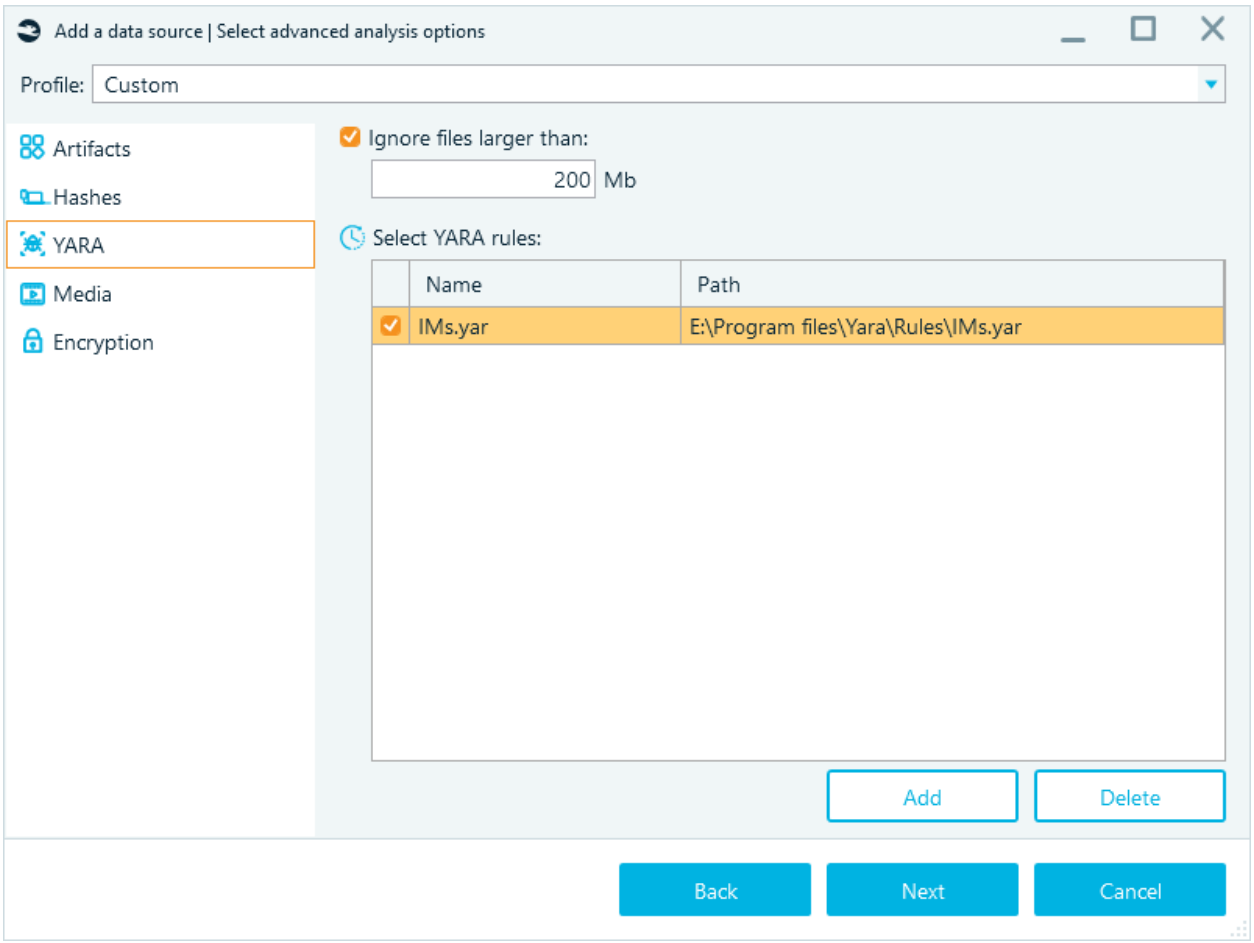
Save rule as XXXX**.yar**.
Rules can be combined into one .yar file, but rules must have unique names.

YARA tab

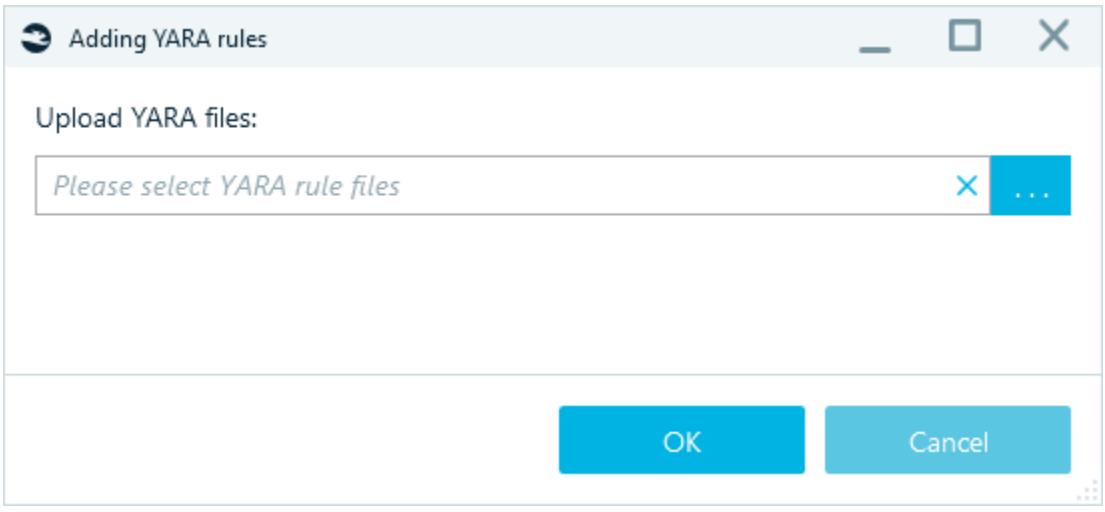
On YARA tab you can determine the files to be skipped depending on their size:



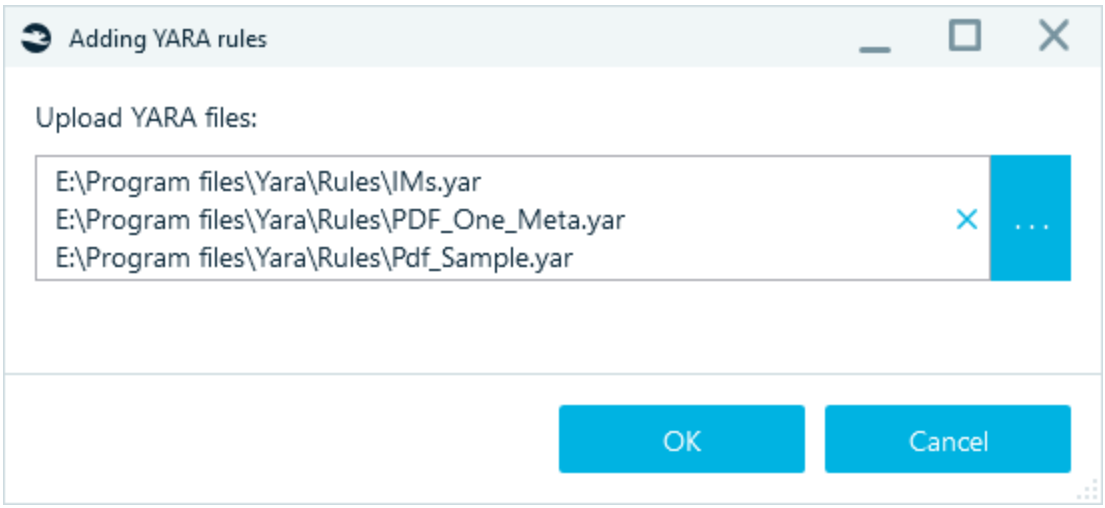
Specify YARA rules and select them.



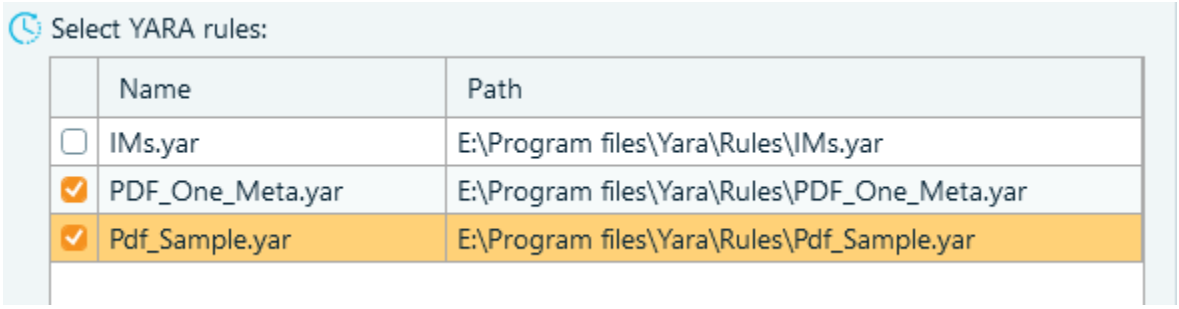
Click on Add button to add rules:



Multiple selection available:



After clicking on OK button, the rules are added and available for selection:



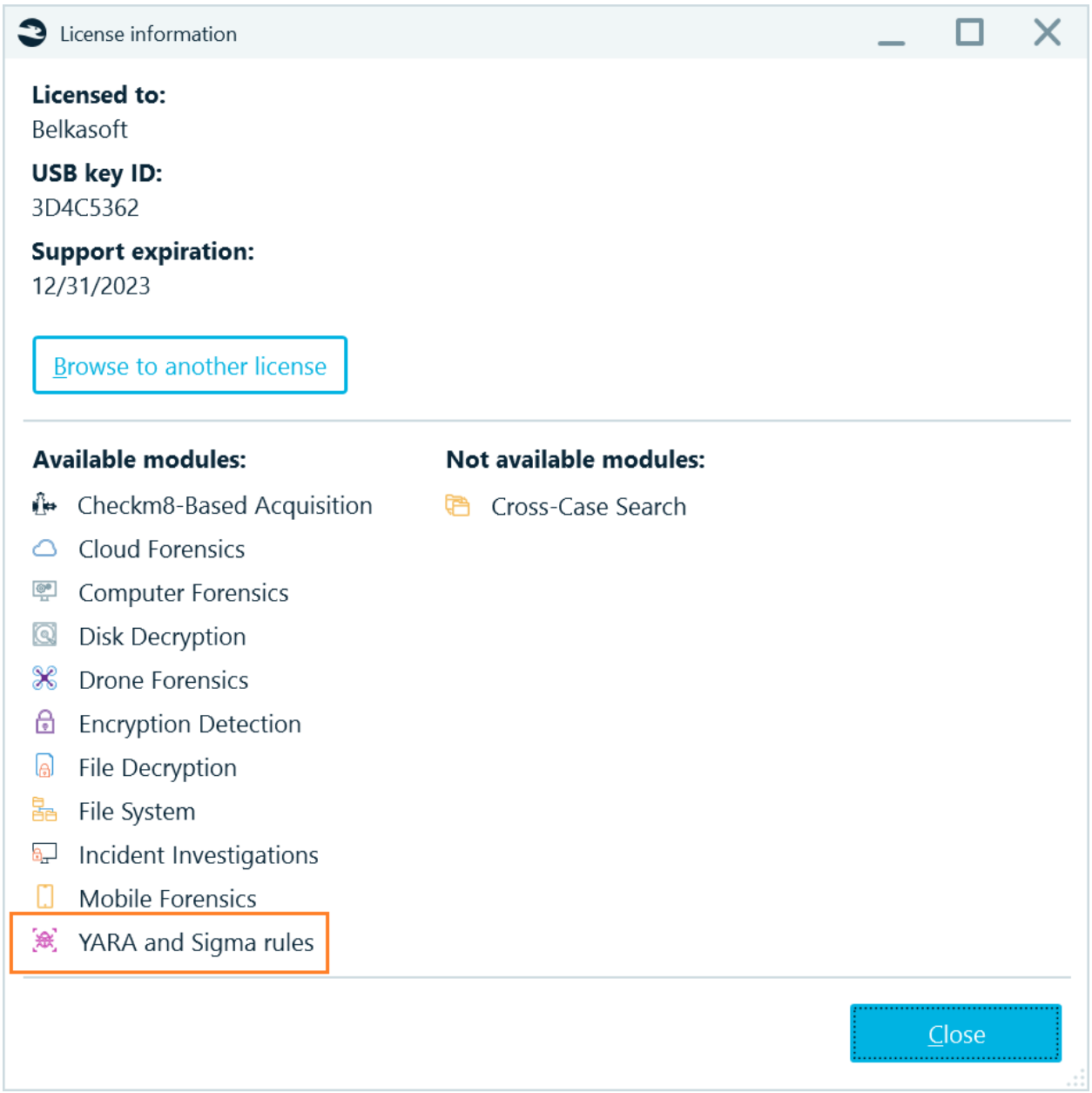
After starting the analysis, the selected rules will be applied to the selected data source.

Sigma

Sigma is a popular open-source format for describing detection rules for security information and event management (SIEM) systems. Sigma rules are used to identify specific patterns of behavior, events, or indicators of compromise (IOCs) in log files, network traffic, and other digital artifacts. By importing Sigma rules into Belkasoft X, examiners can leverage these rules to automatically identify suspicious or malicious activity in their investigations.

Sigma rule is a YAML-based signature format that enables a security operations team to describe relevant log events in a flexible and standardized format. In Belkasoft X Sigma rules are supported in two formats: **.yml** and **.yaml**.

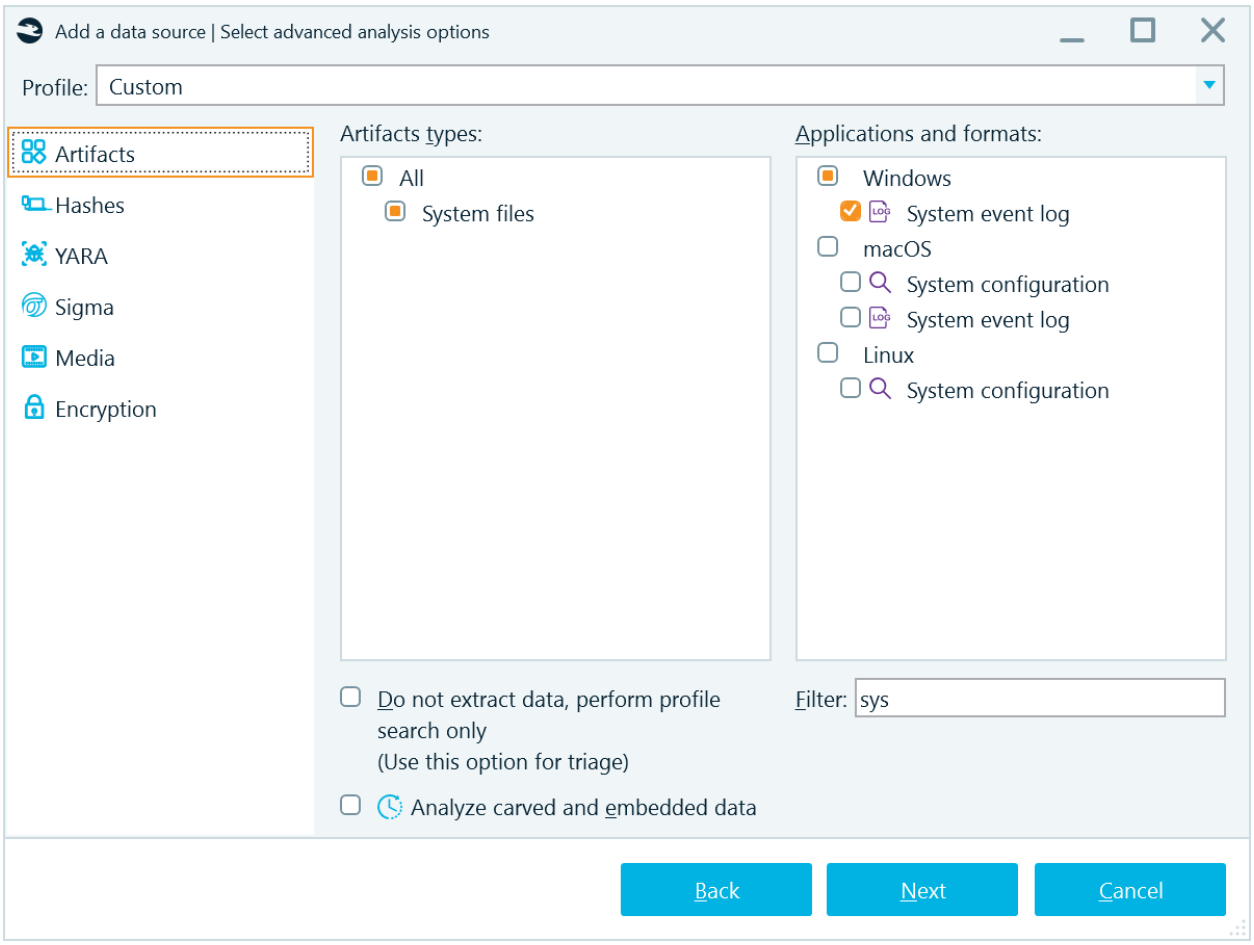
Sigma feature requires the 'YARA and Sigma rules' license module.



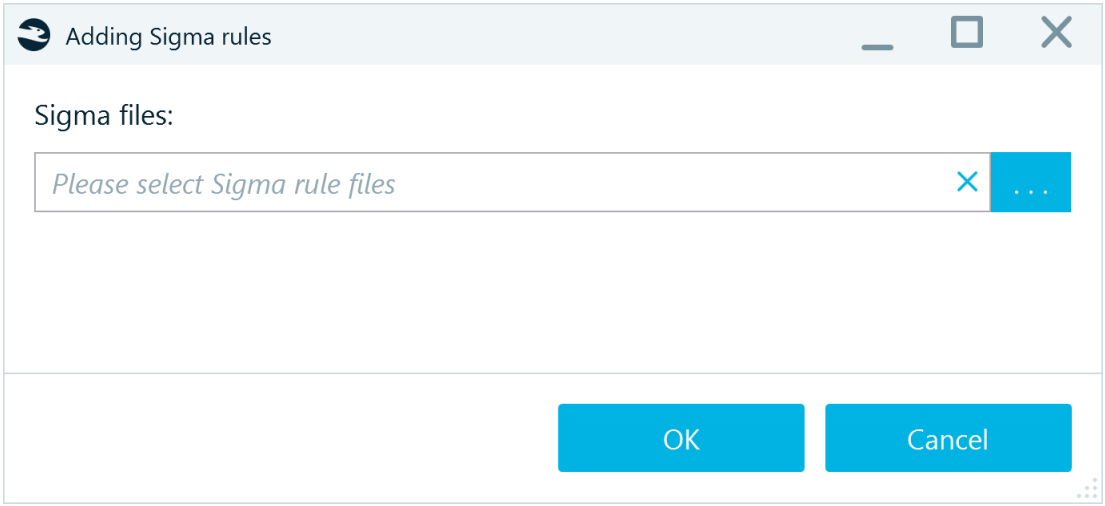
Sigma rules implementation

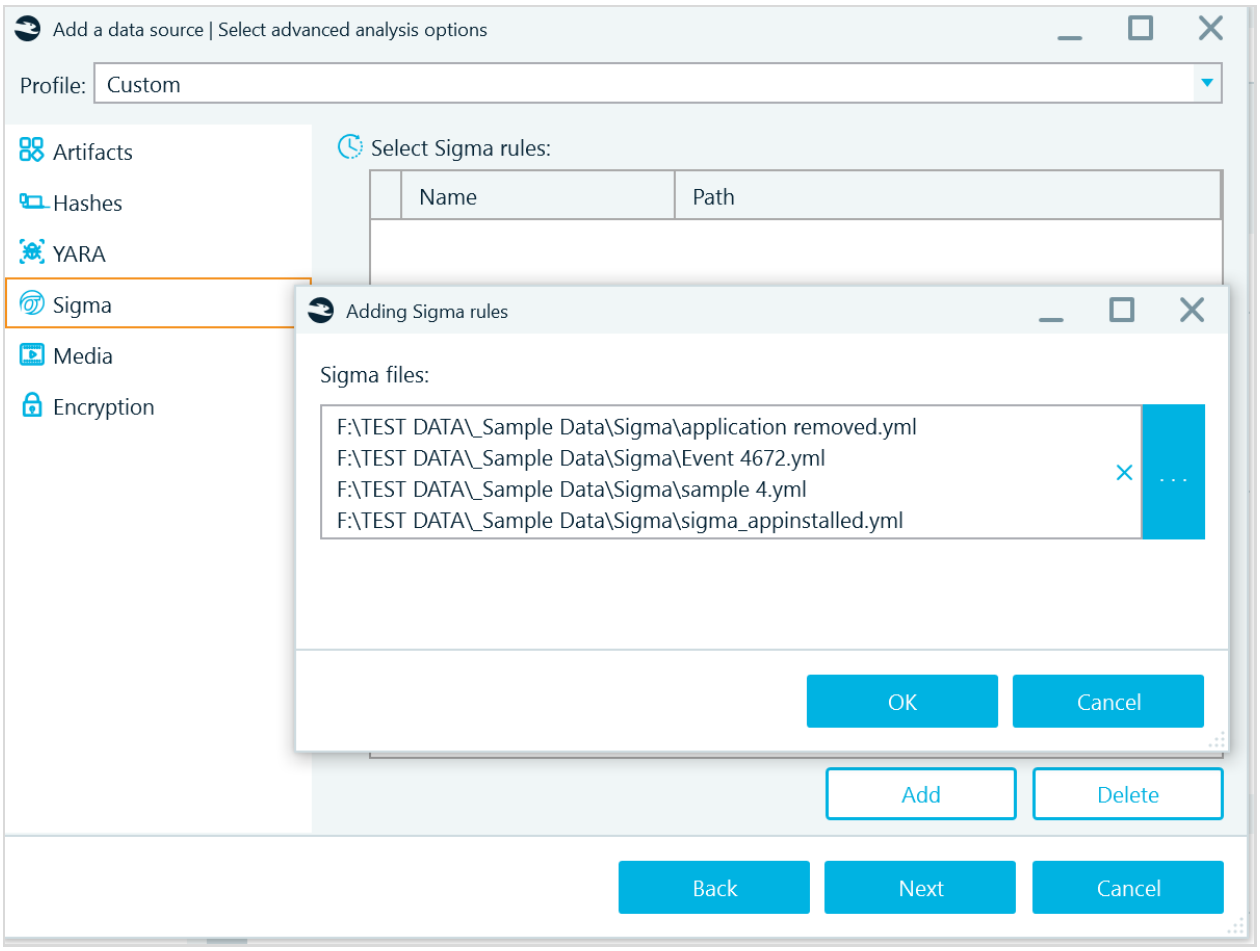
Add a data source and proceed to the Advanced analysis options. Make sure to select the System files analysis profile in the **Artifacts** section.

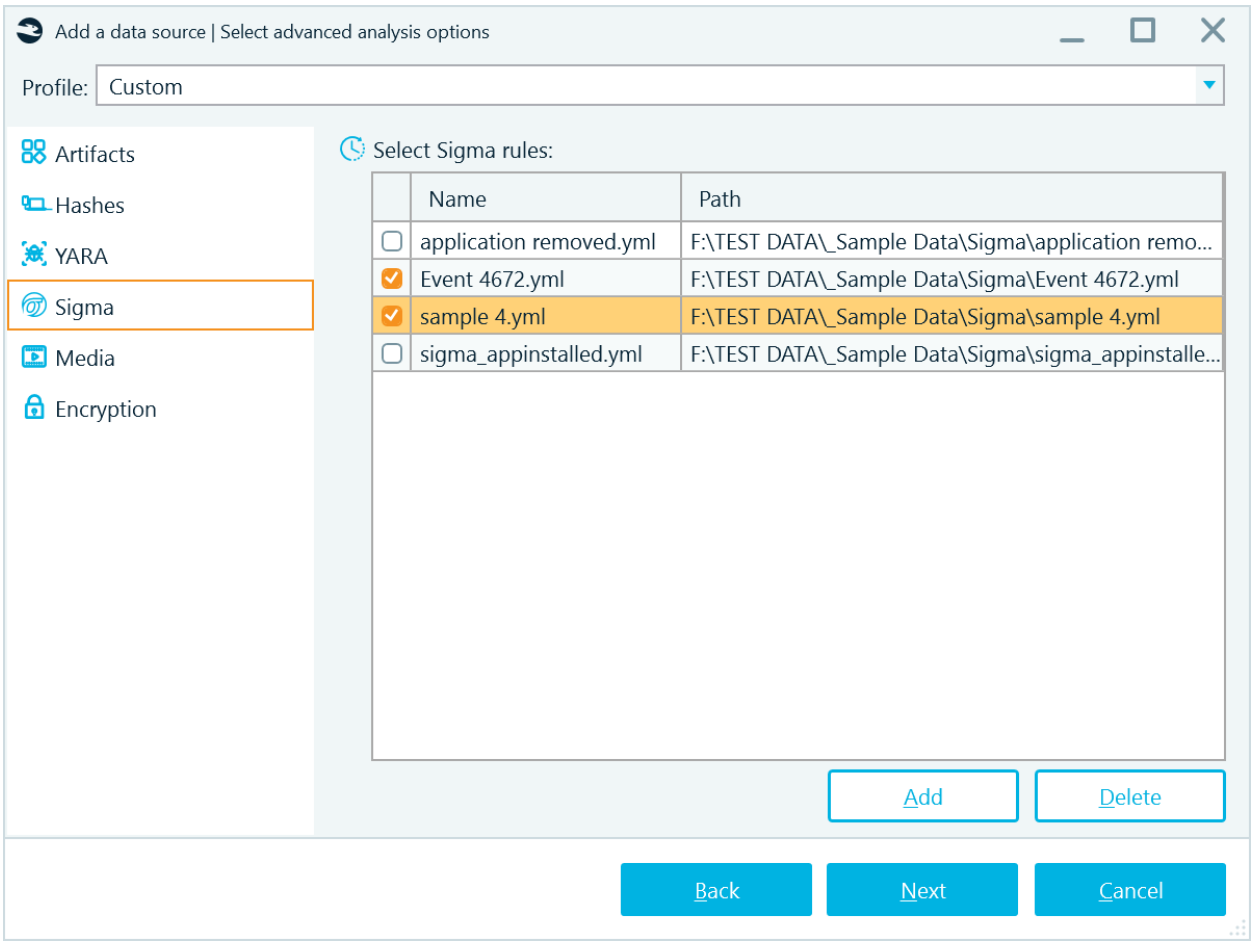
Note: This operation is time consuming.
Note: Sigma rules will be applied only if System files are selected for the analysis.



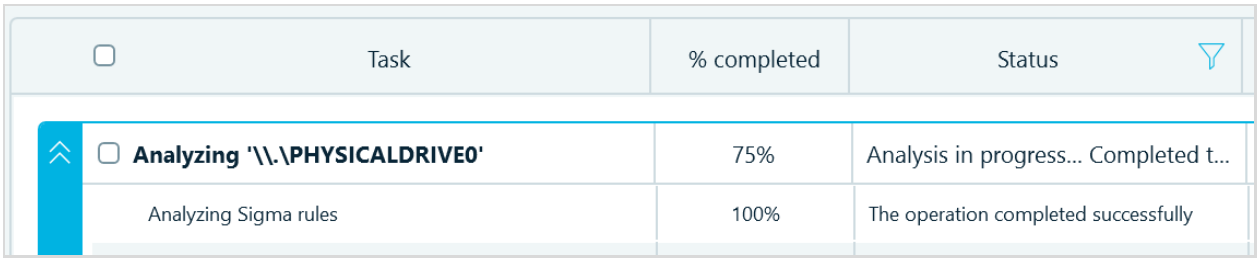
Then, in the **Sigma** section, add one or multiple Sigma rules in .yaml or .yml format.
Click **Add**, then browse for Sigma rules file and click **OK**.



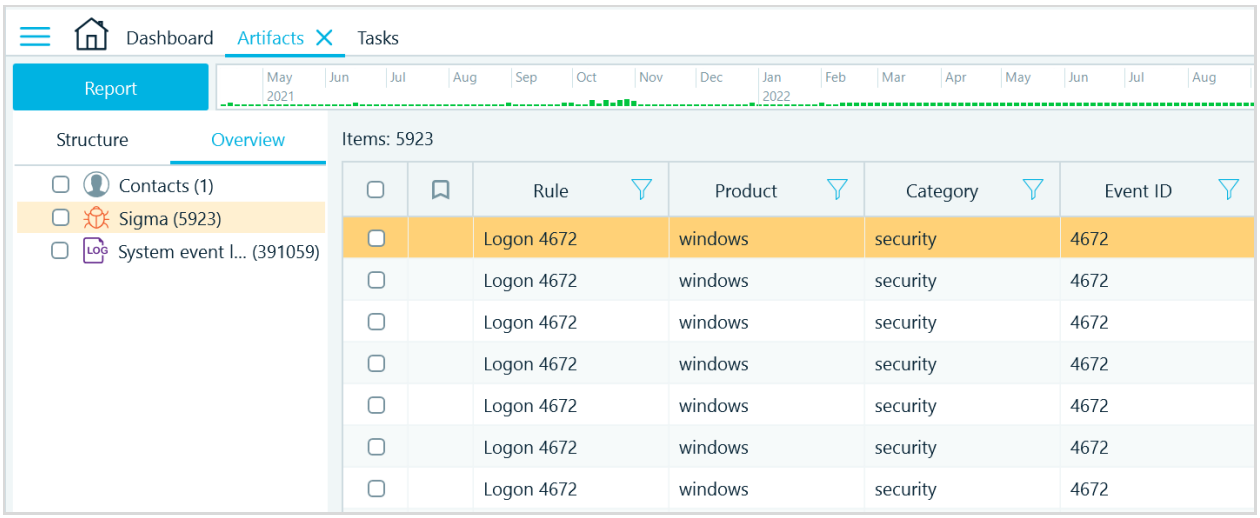

Add a data source | Select advanced analysis options
Profile:
Custom
Artifacts
Hashes
YARA
Sigma
Media
Encryption
Select Sigma rules:
Name
Path
Adding Sigma rules
Sigma files:
F:\TEST DATA_Sample Data\Sigma\application removed.yml
F:\TEST DATA_Sample Data\Sigma\Event 4672.yml
F:\TEST DATA_Sample Data\Sigma\sample 4.yml
F:\TEST DATA_Sample Data\Sigma\sigma_appinstalled.yml
OK
Cancel
Add
Delete
Back
Next
Cancel



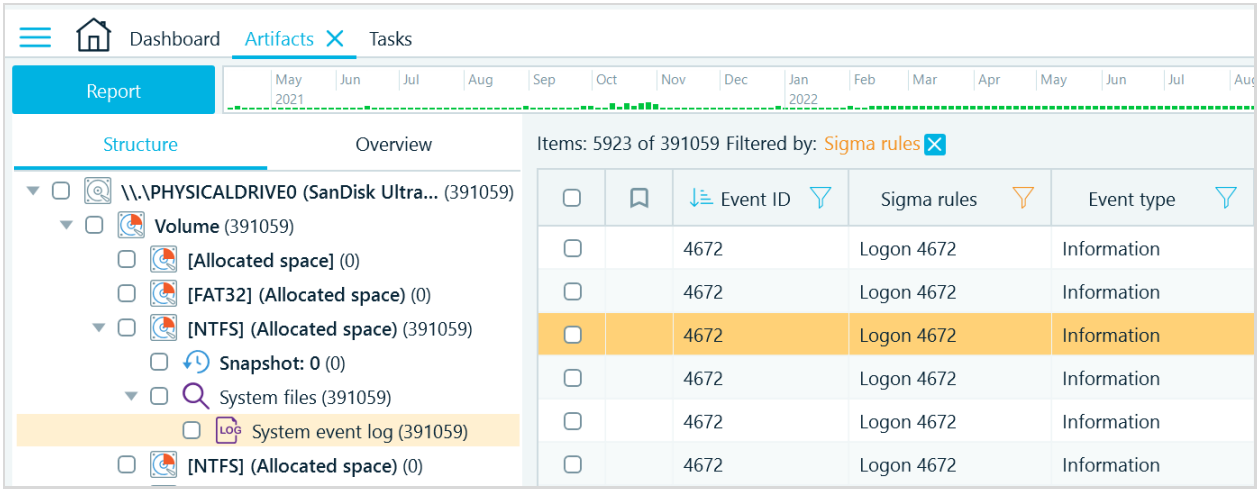
Check the analysis progress in the Tasks window.



The results of the Sigma rules application are shown in the **Overview** tab of the Artifacts window, in the Sigma node.



In the Structure tab of the Artifacts window, analysis results are displayed in the **Sigma rules** column of the **System event log** node. This column can be sorted and filtered.



Sigma rule creation

An official guide on Sigma rules creation can be found here https://github.com/SigmaHQ/sigma/wiki/Rule-Creation-Guide.

You can find a variety of Sigma rules on the Internet, or you can create your own.

To create a Sigma rule, you will need to start by creating a file with a .yml or .yaml extension and opening it in a text editor. We recommend using VS Code as it has extensions for working with yml files, including formatters.

Sigma rules have some obligatory and optional parameters, formatting, such as nesting levels, is important.

Here is an example of the rule, which simply selects all the events with the code 4672 from the System event log, obligatory lines are highlighted yellow:

```
title: Logon 4672
description: Logon with privileges
author: Belkasoft
tags: event
logsource:
    category: security
    product: windows
detection:
    selection:
        EventID: 4672
    condition: selection
```

Naturally, Sigma rules can get a lot more complicated.

Each log has its own set of properties. Different logs may have different properties, but there are some properties that are common for most of the logs.

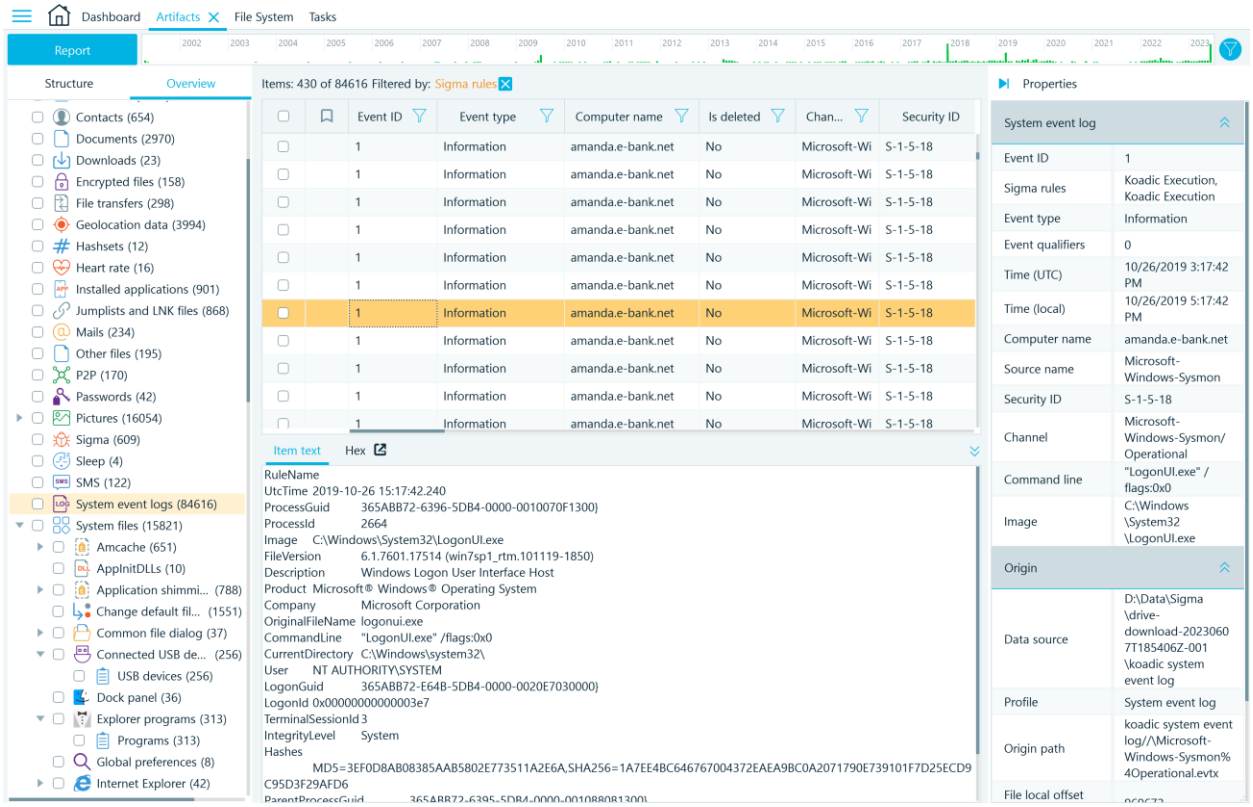
Note: Belkasoft X analyzes extracted and parsed event logs, which means that certain event properties may have different names in the product and not all the properties are extracted. Keep this in mind while creating a Sigma rule.

Belkasoft X extracts the following properties:

System event log property	Belkasoft X column's name	Supported Sigma rule names	Type of variable	Example
EventID	Event ID	EventID Event_ID Event ID	int	
Level	Event type	Level EventLevel EventType Event type	string	Success Critical Error Warning Information Verbose SuccessAudit FailureAudit Unknown
Category	Event category	Category EventCategory Event category	int	process_creation
Qualifiers	Event qualifiers	Qualifiers EventQualifiers Event qualifiers	int	0
System time	Time (UTC) Time (local)	System time TimeUtc Time Time utc	int	2013-04-25 2019-10-26 15:19:18.157

		UtcTime WrittenTimeUtc CreationTimeUtc		
Security_UserID UserSid	Security ID	Security_UserID SubjectUserSid Security ID	string	S-1-5-18
Computer	Computer name	Computer ComputerName Computer name	string	Computer MSI
Provider_Name	Source name	Provider_Name Provider Name ProviderName	string	Microsoft-Windows-Sysmon
Channel	Channel	Channel	string	Setup Application Microsoft-Windows-Sysmon/Operational
ProcessName	Process name	Process_Name Process Name ProcessName	string	C:\Windows\servicing\TrustedInstaller.exe
Task	Task	Task	string	
Task_Name	Task Name	Task_Name Task Name TaskName	string	\Microsoft\Windows\Wininet\CacheTask”
Task_Content	Task Content	Task_Content Task Content TaskContent	string	
Logon_Type	Logon Type	Logon_Type Logon Type LogonType	int	11
Logon_Process_Name	Logon Process Name	Logon_Process_Name Logon Process Name LogonProcessName	string	User32
Service_Name	Service Name	Service_Name Service Name ServiceName	string	upnphost termservice
Service_File_Name	Service File Name	Service_File_Name Service File Name ServiceFileName	string	
Command_Line	CommandLine	Command_Line Command Line CommandLine	string	net user support 123qwe123 /ADD /DOMAIN
Image	Image	Image	string	C:\Windows\System32\regsvr32.exe
Image_Path	Image Path	Image_Path	string	

		Image Path ImagePath		
Ip_Address	Ip Address	Ip_Address Ip Address IpAddress	string	192.168.1.79 ::1
Ip_Port	Ip Port	Ip_Port Ip Port IpPort	string	55326
Object_Name	Object name	Object_Name Object Name ObjectName	string	net.exe
ObjectType	Object Type	Object_Type Object Type ObjectType	string	File
Subject_User_Name	Subject user name	Subject_User_Name Subject User Name SubjectUserName	string	Belkasoft AUTHORITY\SYSTEM BANK\Administrator
Target_User_Name	Target User Name	Target_User_Name Target User Name TargetUserName	string	taylor sshd_server
Target_Name	Target Name	Target_Name Target Name TargetName	string	
Application	Application	Application	string	
Workstation_Name	Workstation Name	Workstation_Name Workstation Name WorkstationName	string	WIN-U06LF6G9RNQ IEWIN7
All other properties	Description		string	

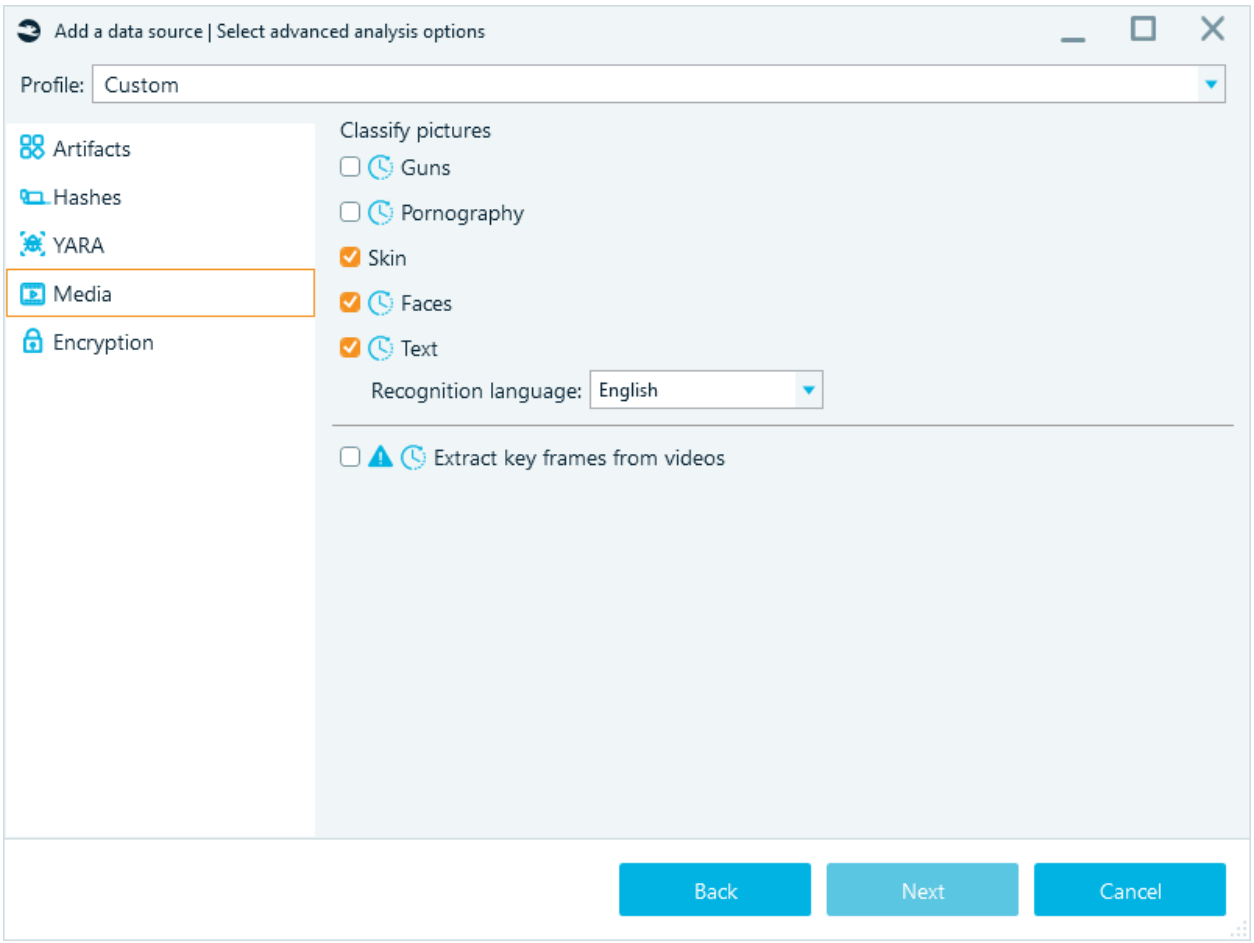


Note: Search by **System time**

- Date (without time)
- Date format should be: YYYY-MM-DD
- Example:
  title: System time aka Time (UTC)
  description: this rule finds the DATE in the Date/Time property "2022-11-10 15:15:37.802"
  logsource:
  product: windows
  detection:
  selection:
  System time|contains: 2022-11-10
  condition: selection

Media

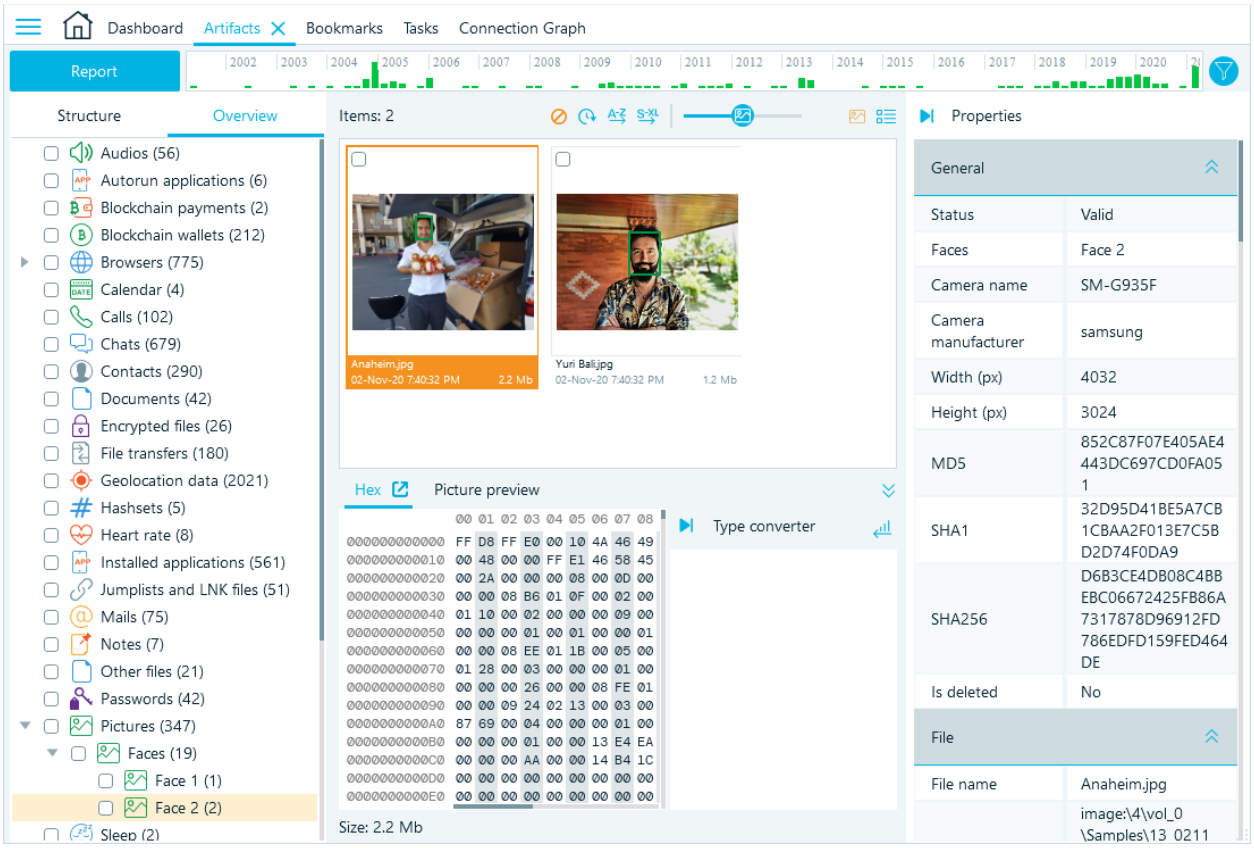
The **Media** tab of the **Select advanced analysis options** window allows you to classify pictures, recognize faces and extract key frames from videos:



The following picture classes can be detected:

- **Faces**
- **Guns**
- **Pornography**
- **Skin**
- **Text**

Face Grouping. If you opt to detect **Faces** in still images and video keyframes, the product will group found faces if they look similar to each other (and likely belong to the same person). The results are shown under the Faces subnode of the Overview's Picture node inside the Artifacts window:



A face detection algorithm was integrated and is now based on the most modern ANN (Artificial Neural Network), which made the new face detection quicker and more robust.
There is a filter by size: 60 by 60 pixels: faces less than 60 to 60 are not detected.

For text detection, an OCR (optical character recognition) is available. You may specify one of 50 different alphabets available under **Recognition language** combo box. You may need to download some language files from the Belkasoft website.

At the bottom of this tab, there is an option to **Extract key frames from videos**. Note the 'extremely long' operation time warning. If your data source contains multiple huge video files such as high-quality movies, you may opt to extract key frames individually from selected videos only.
The key frame extraction operation will produce a set of still pictures for each video. The key frame is a frame from a video, which significantly differs from a previous key frame. Thus, by reviewing key frames only, it is possible to get an idea of the entire video. Belkasoft deliberately does not extract extract frames every few seconds, because it will result in too many unnecessary frames.

Encryption

The last tab of the **Select advanced analysis options** window is **Encryption**. Using the single check box here, you can instruct the product to **Search for encrypted files and volumes**. The product supports detection of several hundred types of file encryption and about a dozen of various disk encryption including WDE (whole disk encryption) and FVE (full volume encryption).

Once you set all options on this page and click **Next**, the **Review a data source** window is shown. Here, you have the last chance to varify the options you specified for the analysis of the data source you have added. Note the green **Complete** button. Whenever a long process is expected to be run, the product shows you green button instead of a blue one. This way, you have full understanding that the process is about to start with the click on this button, and have the change to change your analysis preferences, using the **Back** button or even **Cancel** button, which will close the sequence without doing anything.

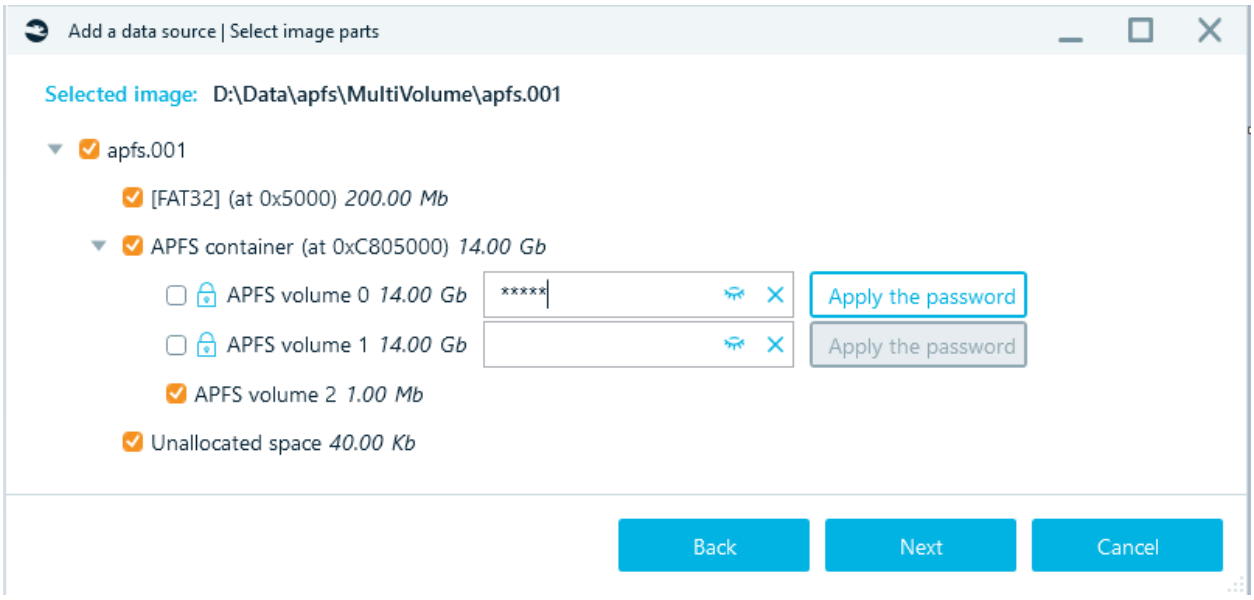
WDE

Supported encryption types:

- APFS
- Bitlocker
- FileVault / FileVault2
- McAfee
- PGP
- VeraCrypt
- TrueCrypt

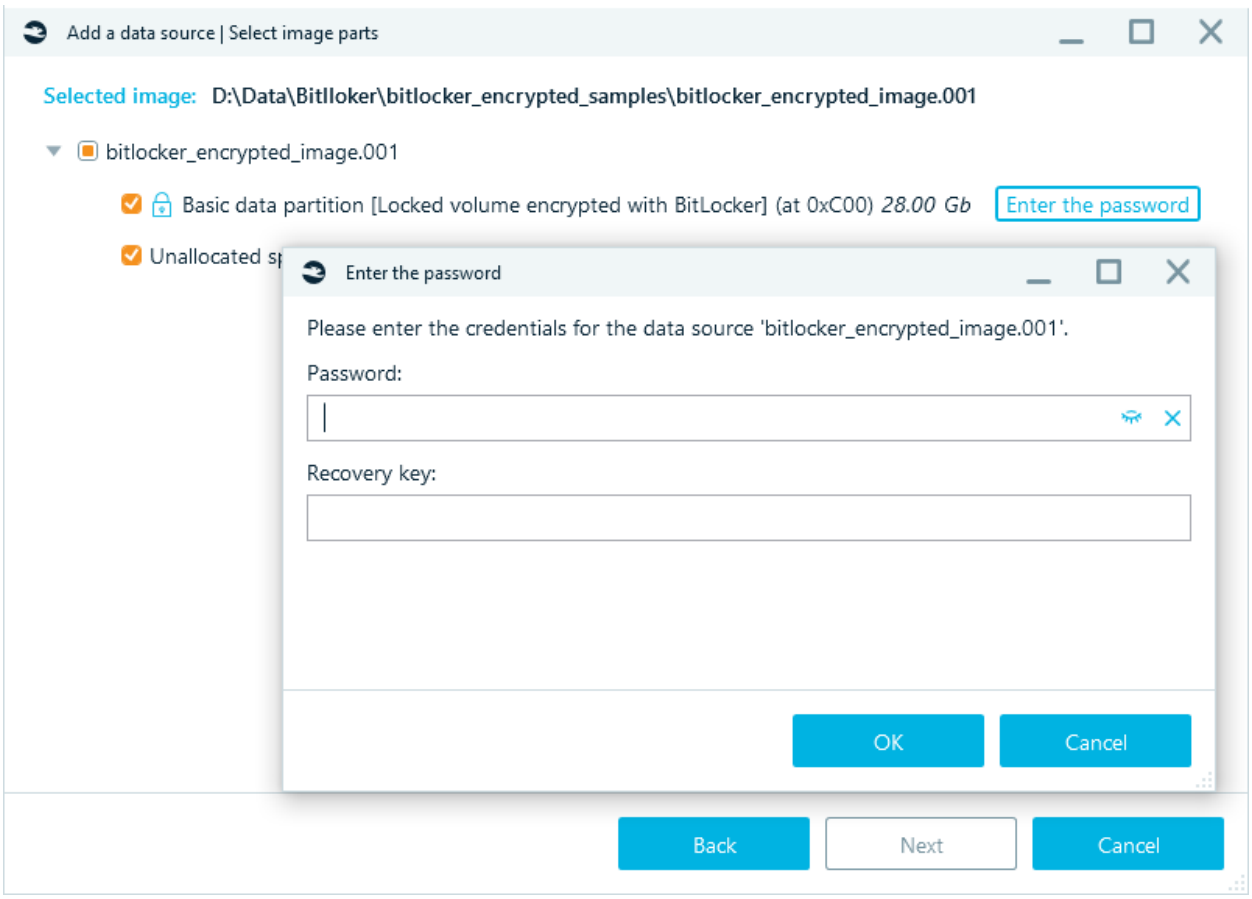
APFS

You will need a password for the encrypted partition.



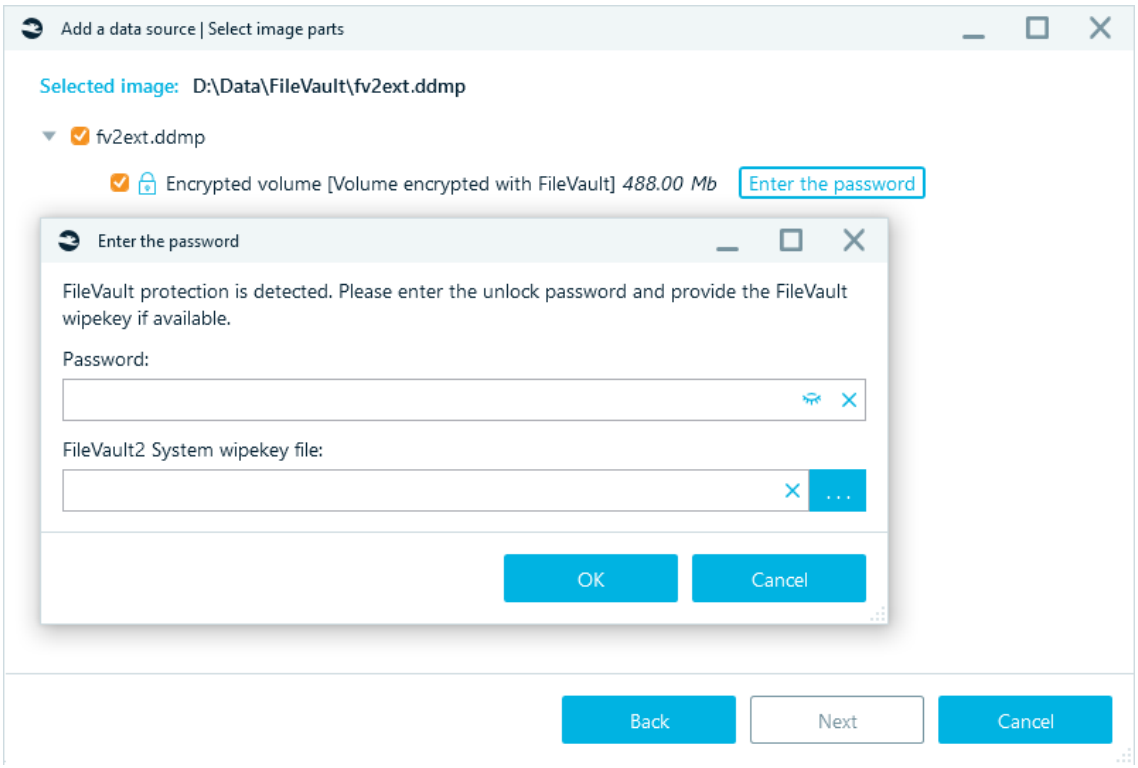
Bitlocker

You will need a password OR recovery key for the encrypted partition.



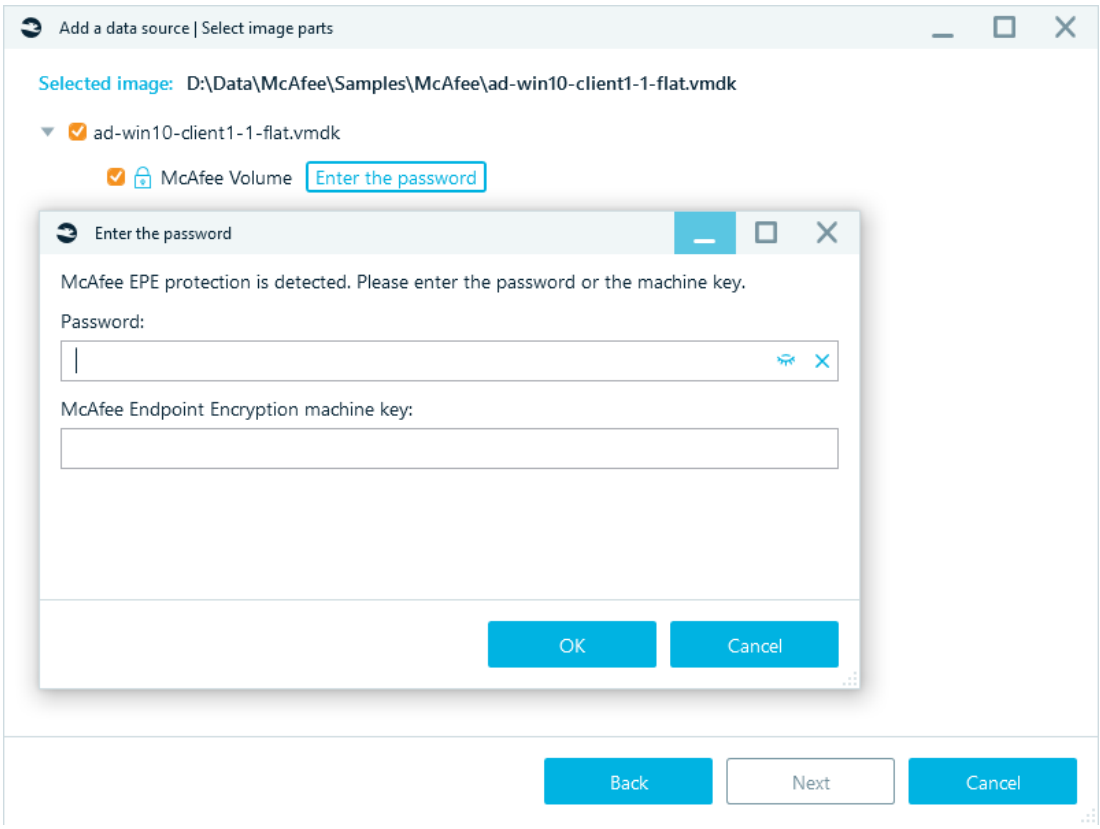
FileVault

You will need a password OR Wipekey file for the encrypted partition.
The EncryptedRoot.plist.wipekey is stored in the Mac OS Recovery folder.



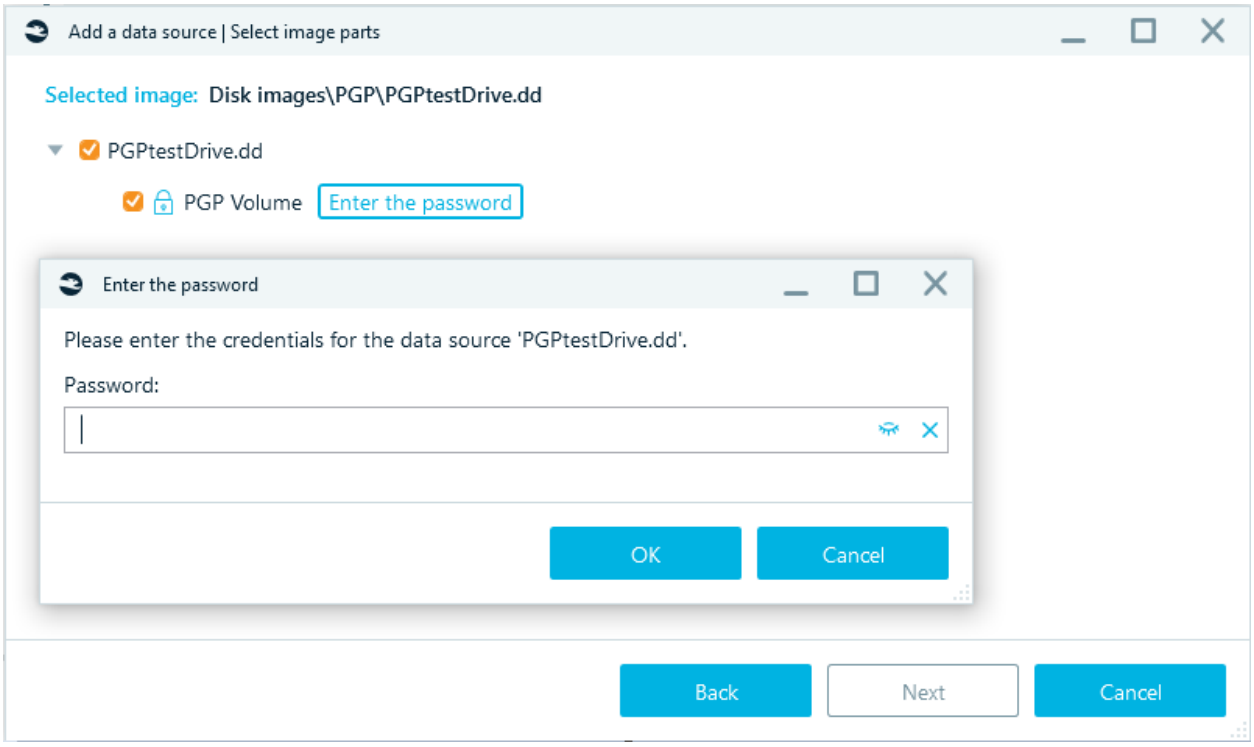
McAfee

You will need a password OR McAfee Endpoint Machine Key file for the encrypted partition. Each system has its own unique McAfee Endpoint Machine Key, key length - 44 characters. The Machine Key is stored in the McAfee ePO database.



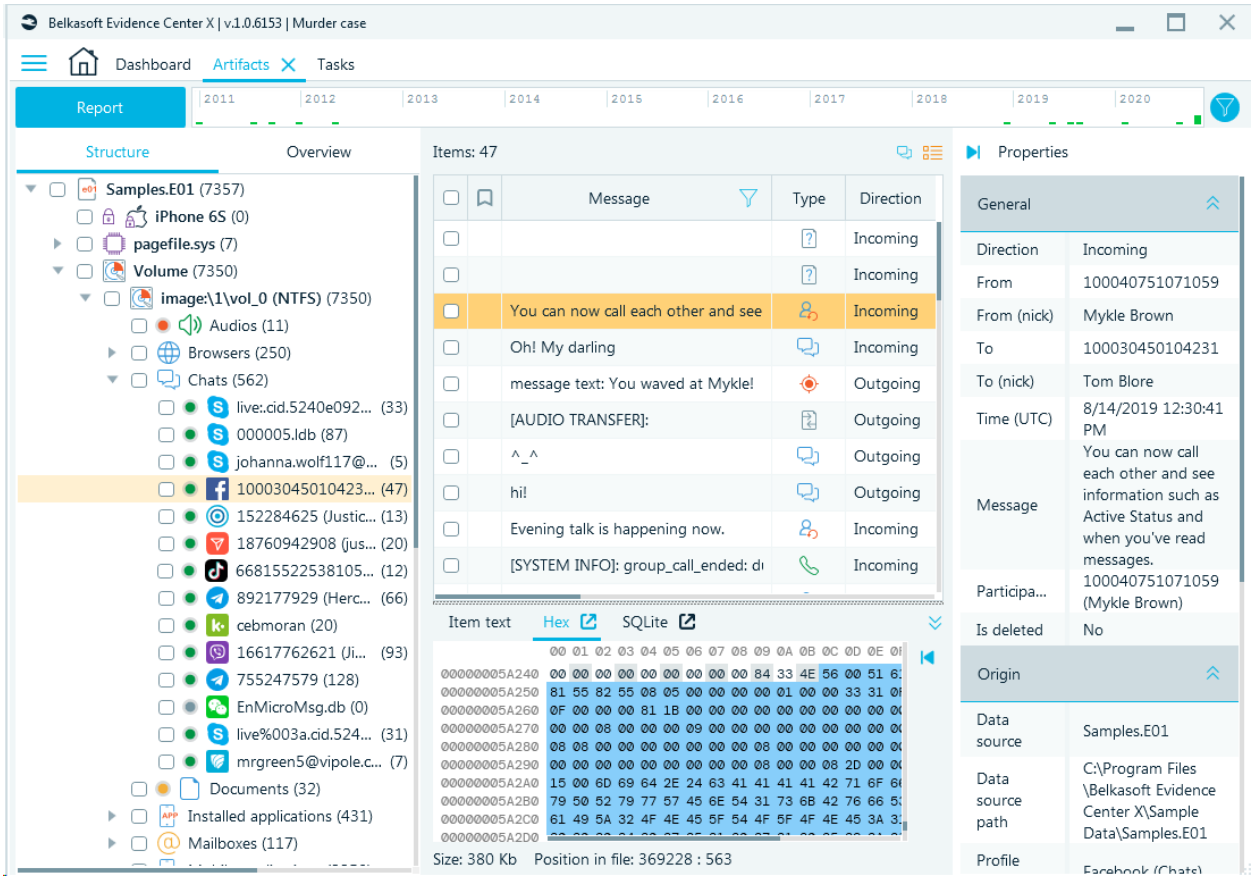
PGP

You will need a password for the encrypted partition.



Artifacts

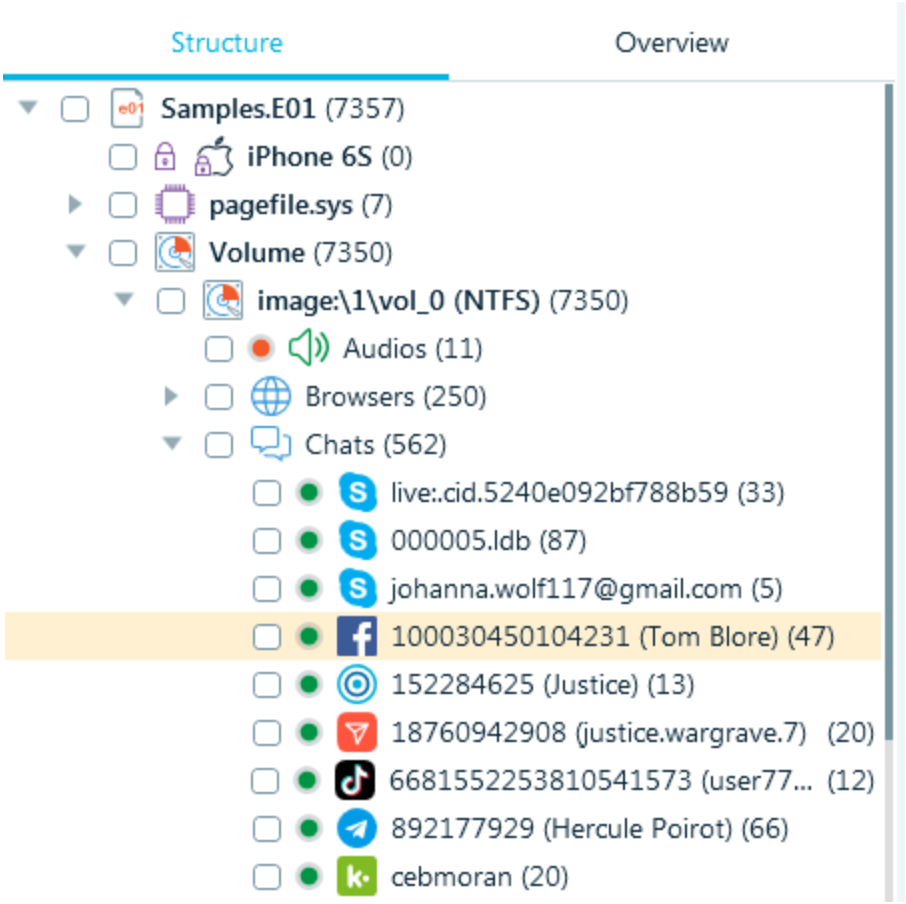
Artifacts window helps you to work with various pieces of forensically important data, automatically extracted by Belkasoft from data sources which you added to your case. Examples of an artifact are a chat, a document, an email, a picture, a registry key, a video and so forth.



The window is divided into several parts. At the left you can see **Structure** and **Overview** tabs.

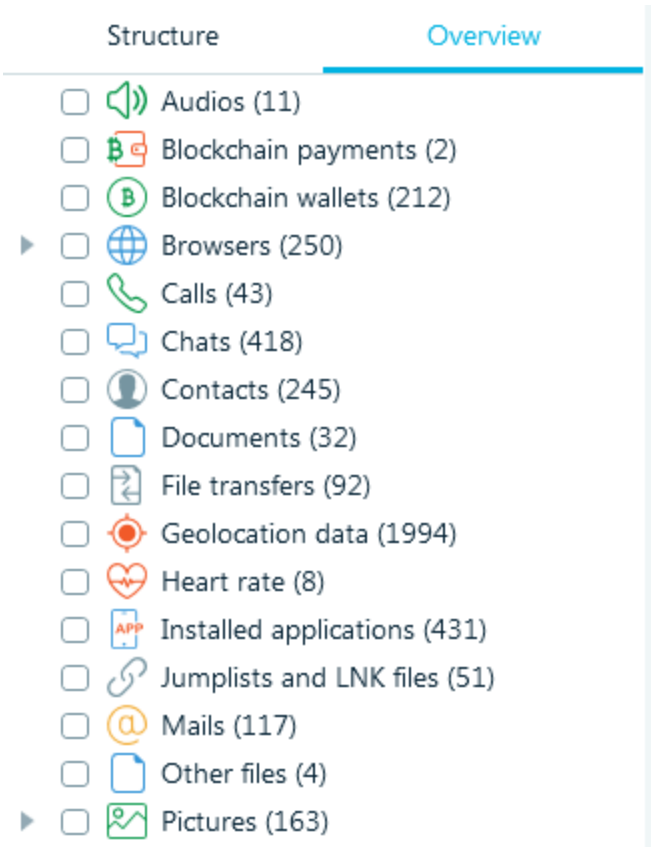
Structure

On the **Structure** tab you can see where exactly your artifacts are stored: at the top level there is a data source, which may have different artifact type nodes like Audios, Chats, Documents, and so on. Under each subnode you will see the profile name, for example, Telegram profile.



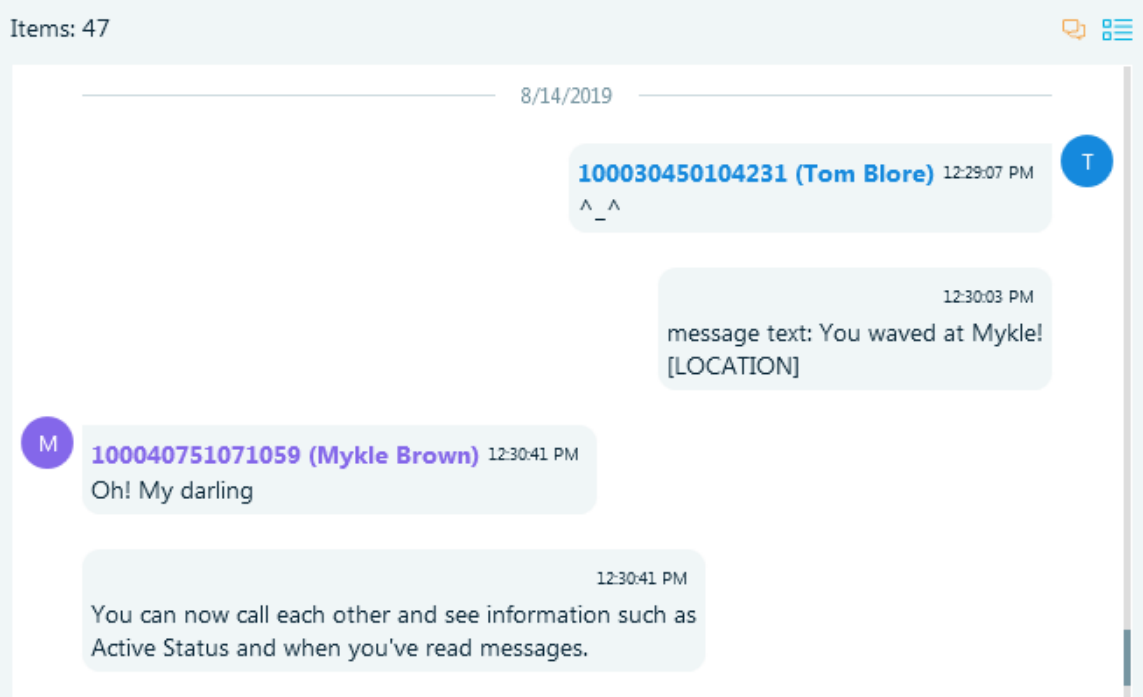
Overview

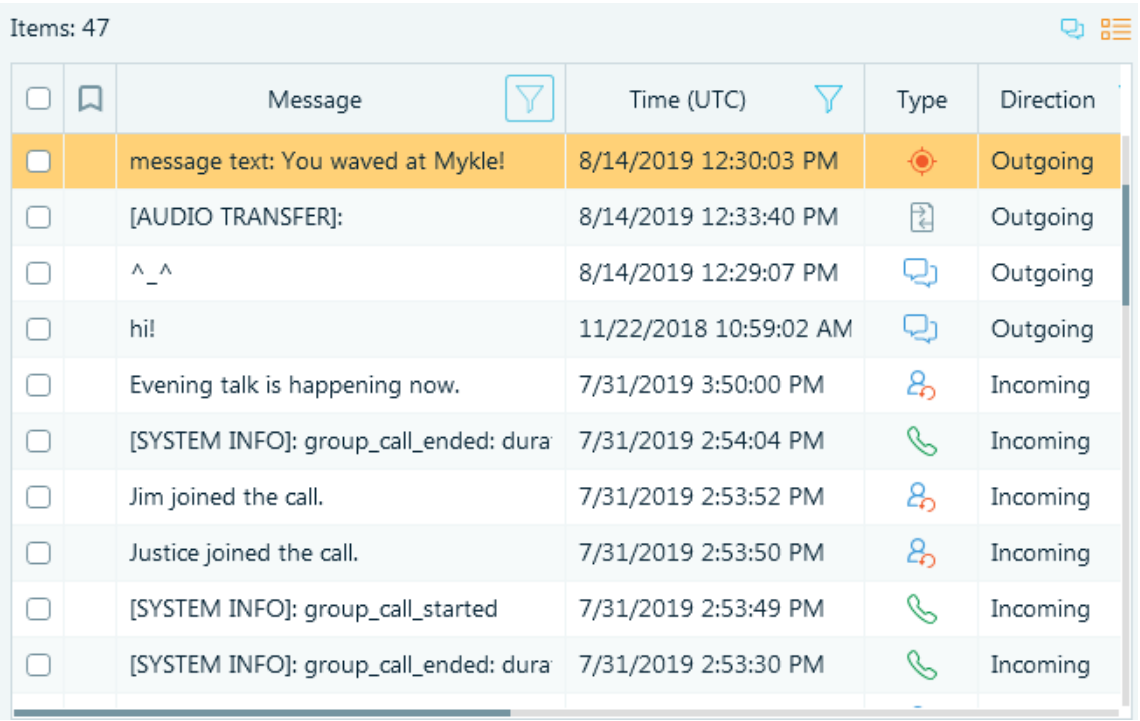
Unlike **Structure**, the **Overview** tab contains all artifacts of the same type under the same node. For example, if you have several data sources and each has several chat applications such as WhatsApp, Skype and Telegram, all these chats will be shown under the Chats node in the **Overview** while in **Structure** they all will have different nodes. To summarize, **Overview** is more lightweight and gives you an easier overview, while **Structure** gives you more details about artifact origins.



Artifact list

The middle part of the window shows you a list of artifacts, which you selected in either the **Structure** or **Overview** tab. There are various types of views available depending on the selected artifact type. For example, if you have selected a chat, there is a bubble view and a table view. Bubble view mimics whats viewed on the device and is easier to share with non-technical people, while table view allows you to fit more information on screen and to select columns you need.





In the table view you can sort the list by any column. To do so just click on the column header. You can also filter by any column having the funnel icon. Find more information in **Filtering** chapter.

Drop-down menu

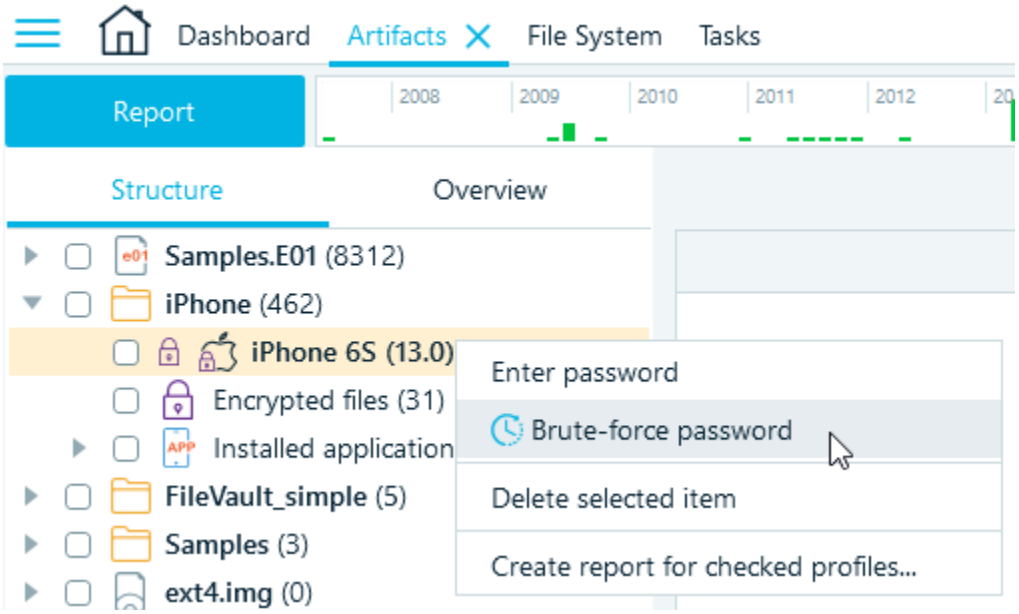
Right-clicking on a node in the tree or on the list of artifacts opens a drop-down menu. The set of operations in the menu changes depending on the node/artifact on which it is opened. Let's take a look

at some of them.

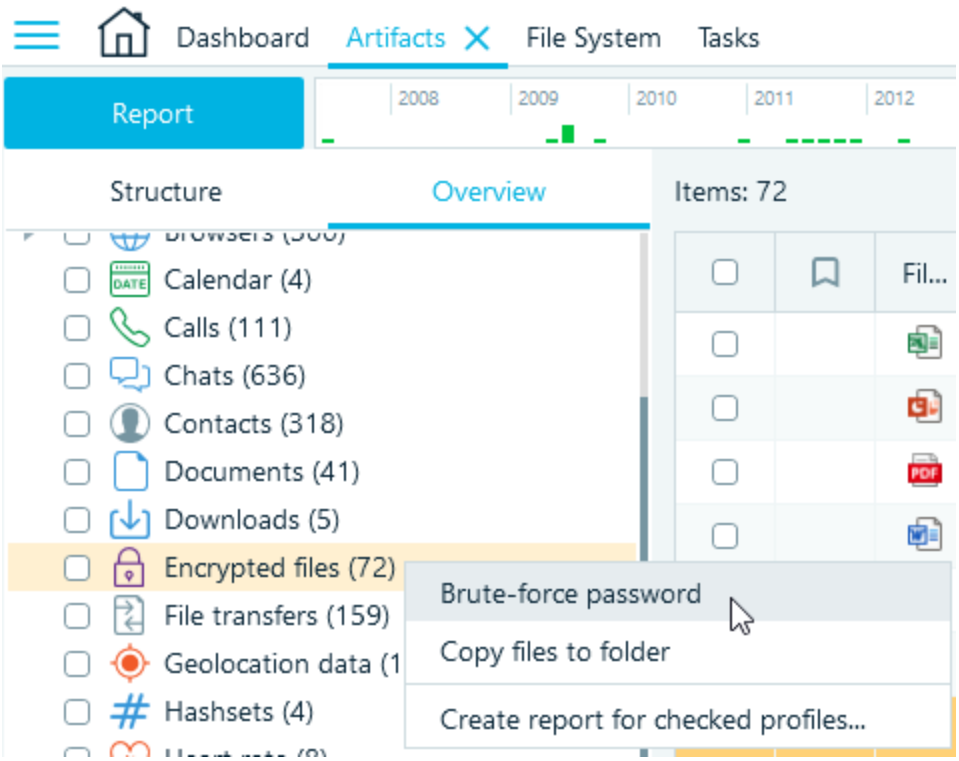
Brute-force password

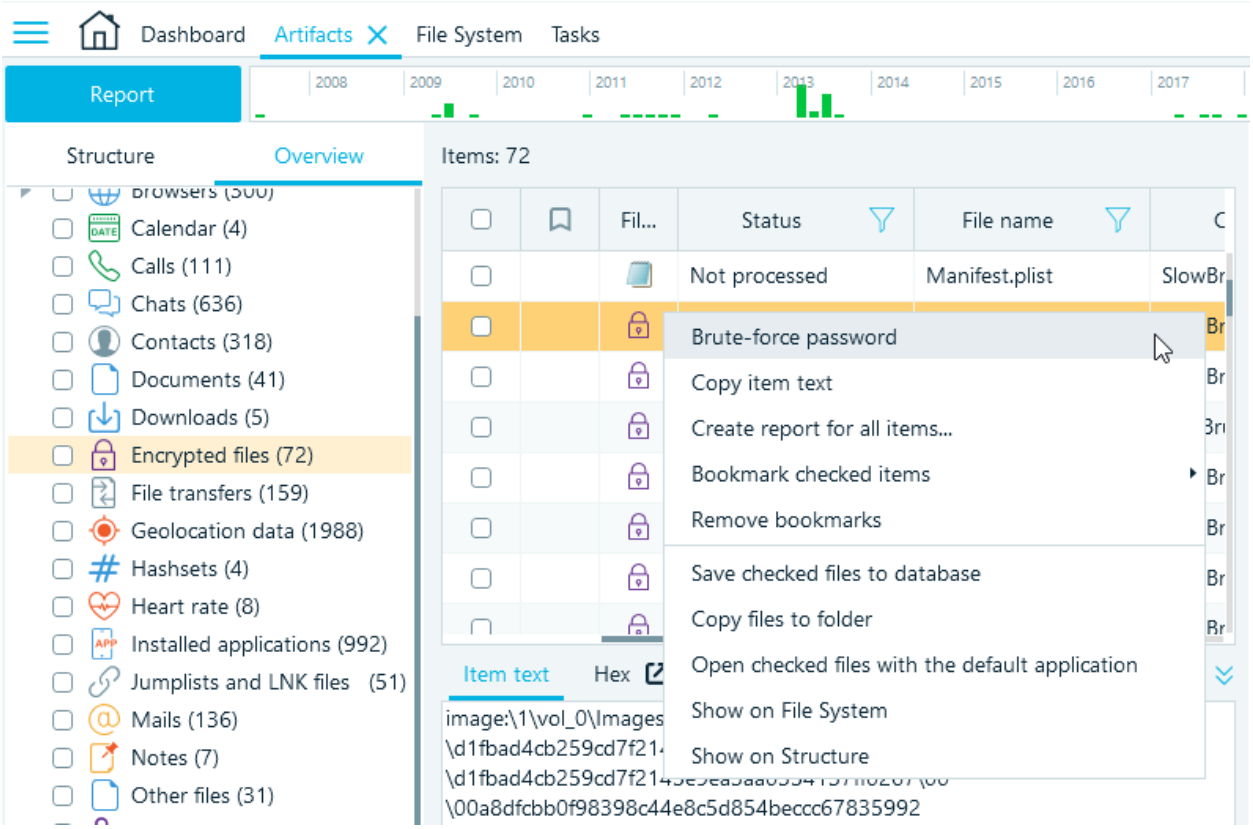
This feature allows cracking passwords for encrypted files and iTunes backups. It is available for customers, who purchased **File decryption license** and have Passware Kit Forensic.

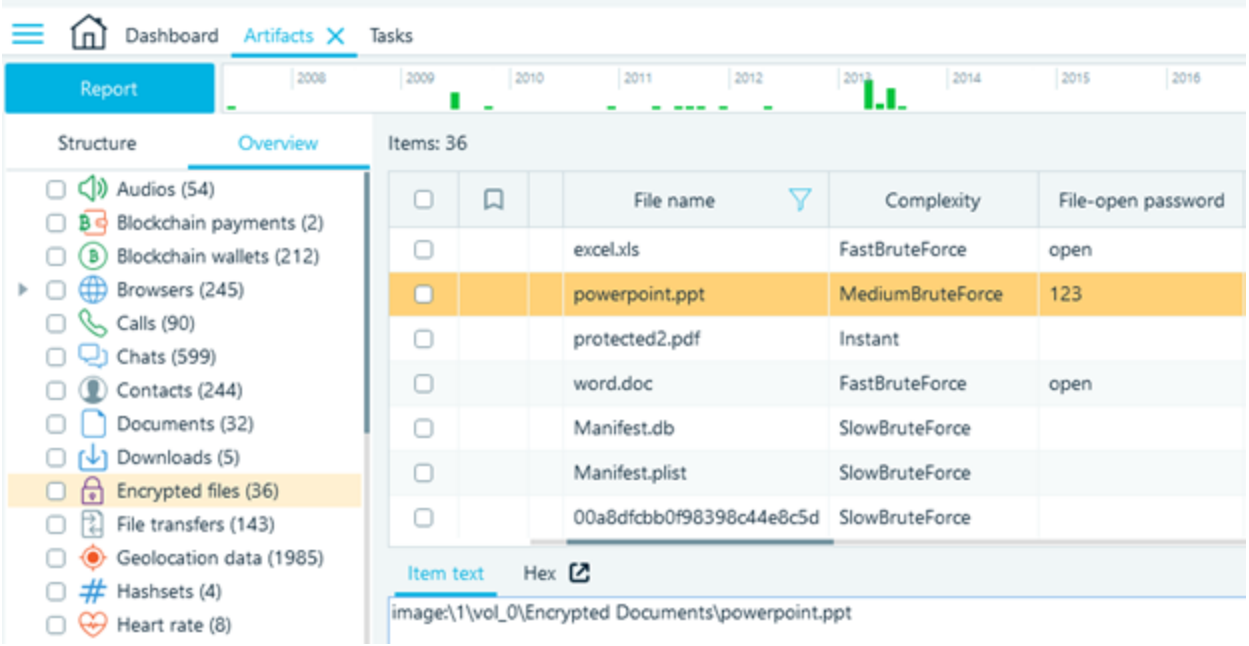
Brute-force password window is available in the context menu both from **Structure** and **Overview** tabs of the **Artifacts** window.



Detected encrypted files are placed in a separate node in **Overview**. They can be brute forced both from the Tree and from the Grid view; either all together or selectively. Once the file is successfully decrypted, its password is shown in the **File-open password** column in the grid view of the **Encrypted files** node.

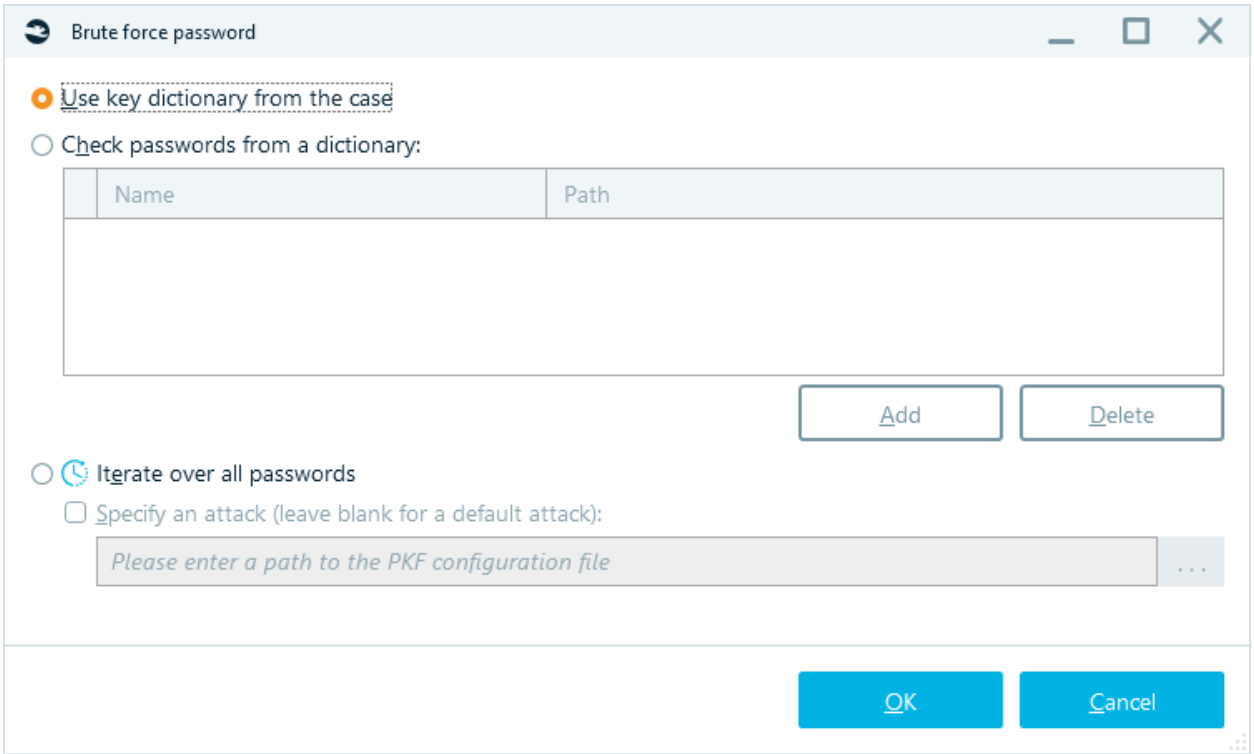

Dashboard
Artifacts
File System
Tasks
Report
2008
2009
2010
2011
2012
Structure
Overview
Items: 72
Fil...
Calendar (4)
Calls (111)
Chats (636)
Contacts (318)
Documents (41)
Downloads (5)
Encrypted files (72)
File transfers (159)
Geolocation data (1
Hashsets (4)
Brute-force password
Copy files to folder
Create report for checked profiles...


Dashboard
Artifacts
File System
Tasks
Report
2008
2009
2010
2011
2012
2013
2014
2015
2016
2017
Structure
Overview
Items: 72
Calendar (4)
Calls (111)
Chats (636)
Contacts (318)
Documents (41)
Downloads (5)
Encrypted files (72)
File transfers (159)
Geolocation data (1988)
Hashsets (4)
Heart rate (8)
Installed applications (992)
Jumplists and LNK files (51)
Mails (136)
Notes (7)
Other files (31)
Fil...
Status
File name
Not processed
Manifest.plist
SlowBr
Brute-force password
Copy item text
Create report for all items...
Bookmark checked items
Remove bookmarks
Save checked files to database
Copy files to folder
Open checked files with the default application
Show on File System
Show on Structure
Item text
Hex
image:\1\vol_0\Images
\d1fbad4cb259cd7f21
\00a8dfcbb0f98398c44e8c5d854beccc67835992

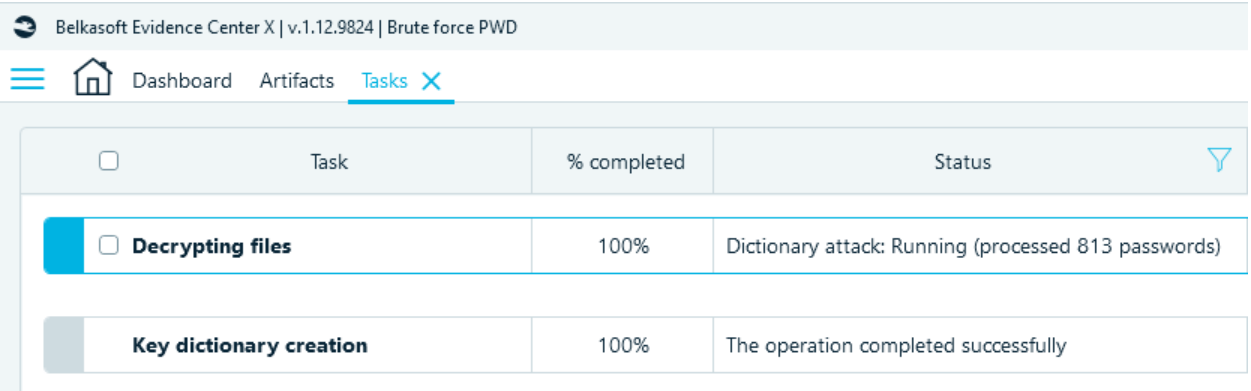


A click on the **Brute-force password** menu item opens a **Brute-force password** window, where one will find 3 possible choices:

- Use key dictionary from the case
- Check passwords from a dictionary
- Iterate over all passwords (with an option to *Specify an attack*)

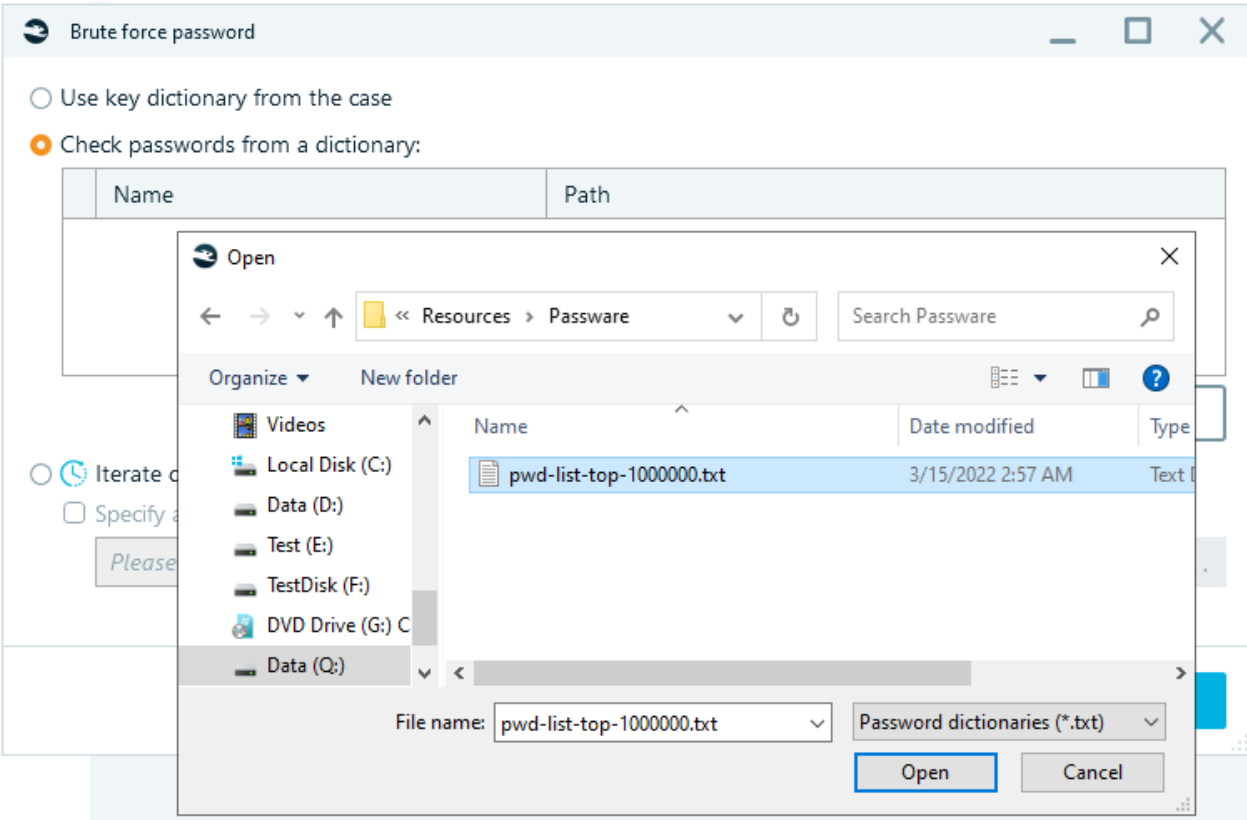


Use key dictionary from the case. When this option is chosen, Belkasoft X creates a Key dictionary, which contains all text artifacts indexed in the data source (read more on Key dictionary here) and then launches *Decrypting files* operation based on a dictionary attack.



Check passwords from a dictionary. This option allows using a password dictionary. It can be created by the user himself or one can utilize any list of popular passwords. Belkasoft Evidence Center X\Resources\Passware folder contains one of such dictionaries - *pwd-list-top-1000000.txt*

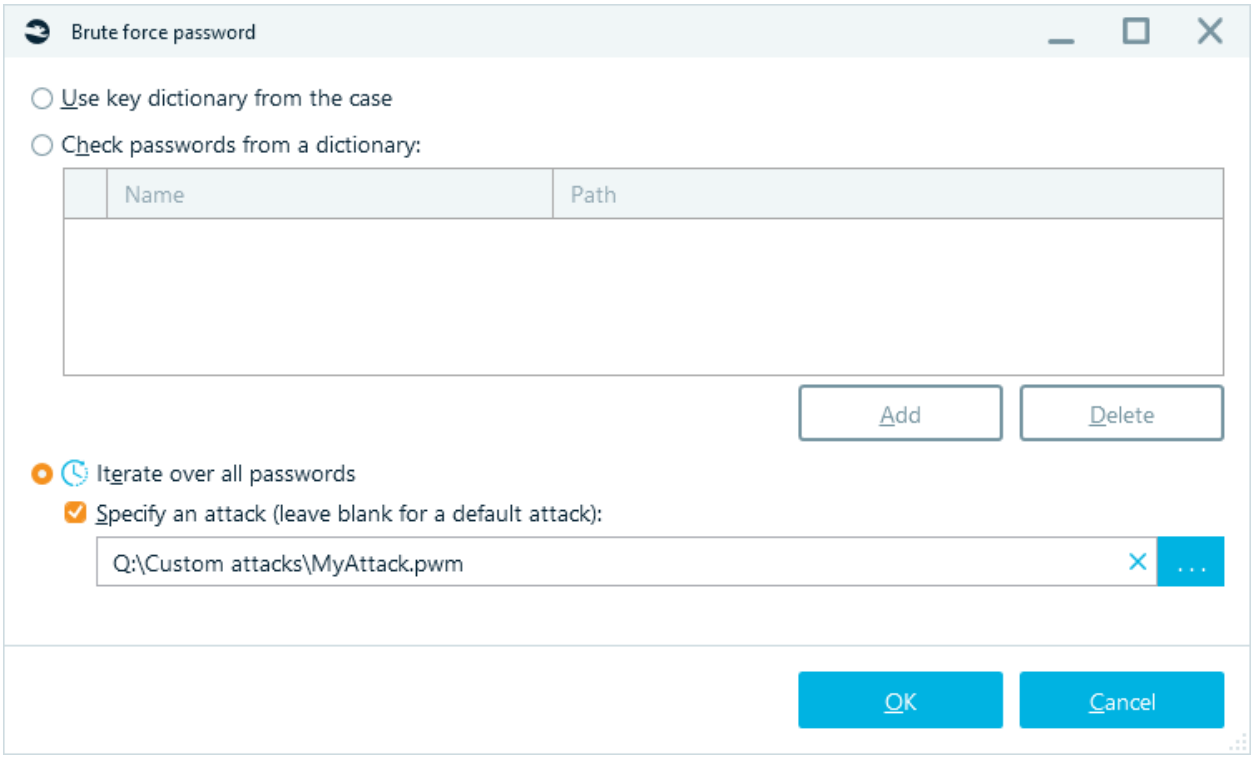
Select **Check password from a dictionary** in the **Brute force password** window:



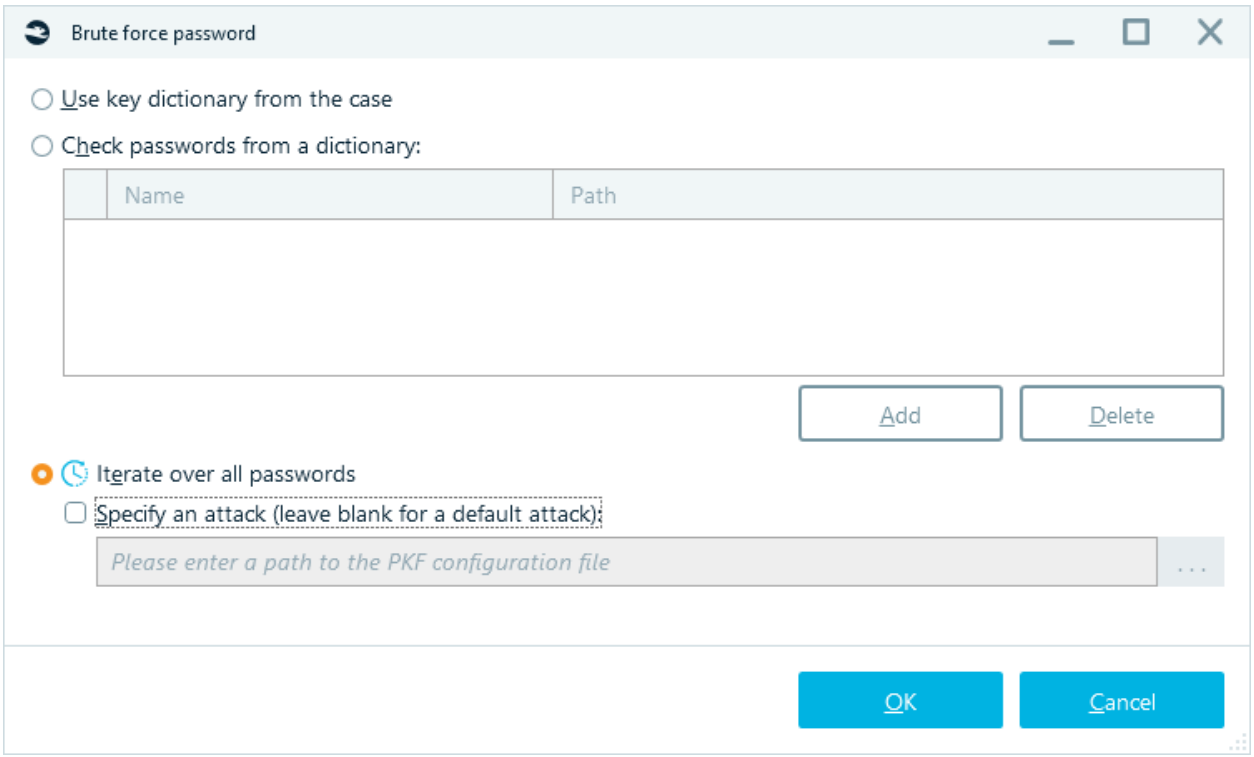
It is possible to add several dictionaries, the search will be conducted on all of them. Click **OK** and decryption begins. You can observe the progress in the **Tasks** window. To delete a dictionary, select it in

the **Brute force password** window and click on the **Delete** button.

Iterate over all passwords. This option is used when two others did not bring results. It initiates a full-scale password brute-force process. One can use a default attack or choose a customized one by ticking the **Specify an attack (leave blank for a default attack)** checkbox. Attacks should be in .pwm format.



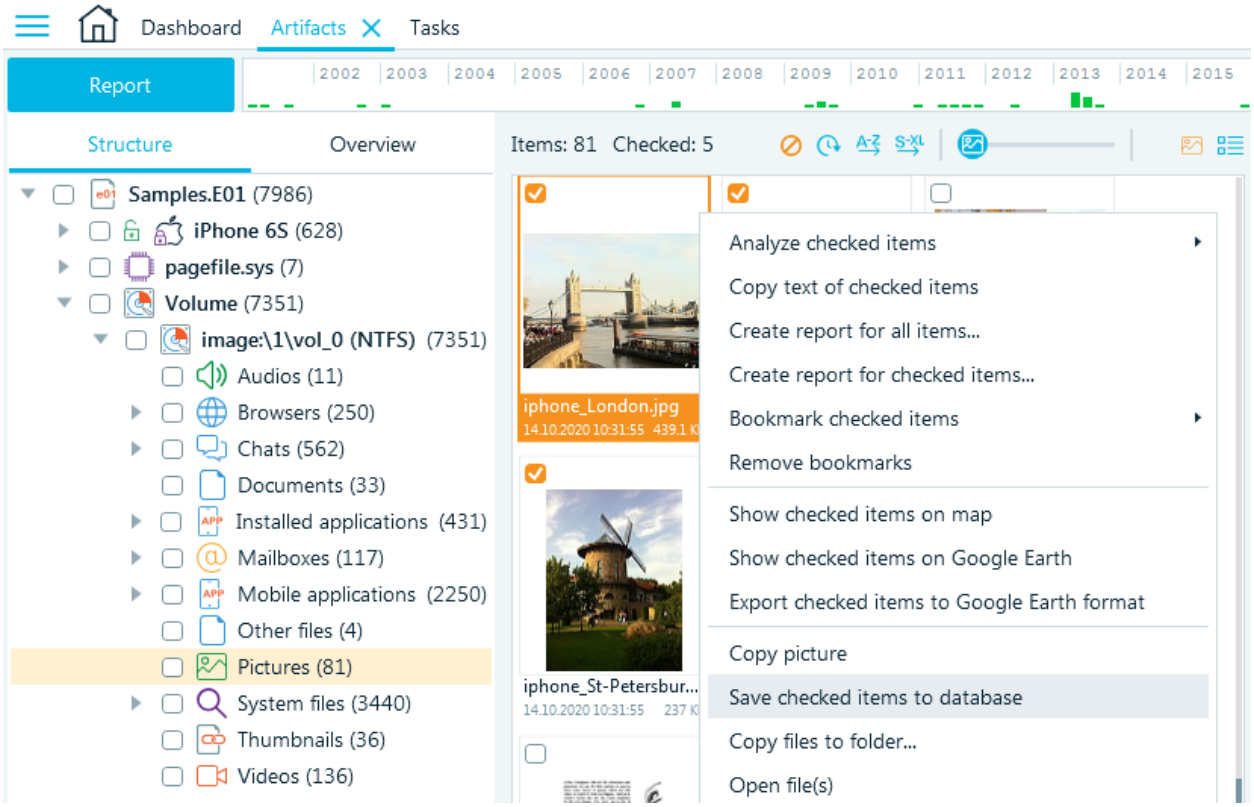
If you do not have a customized attack, leave the checkbox unchecked and click **OK**. Brute-force starts. **Please note** that this is a highly time-consuming process, as indicated by the corresponding icon.



Save checked items to database

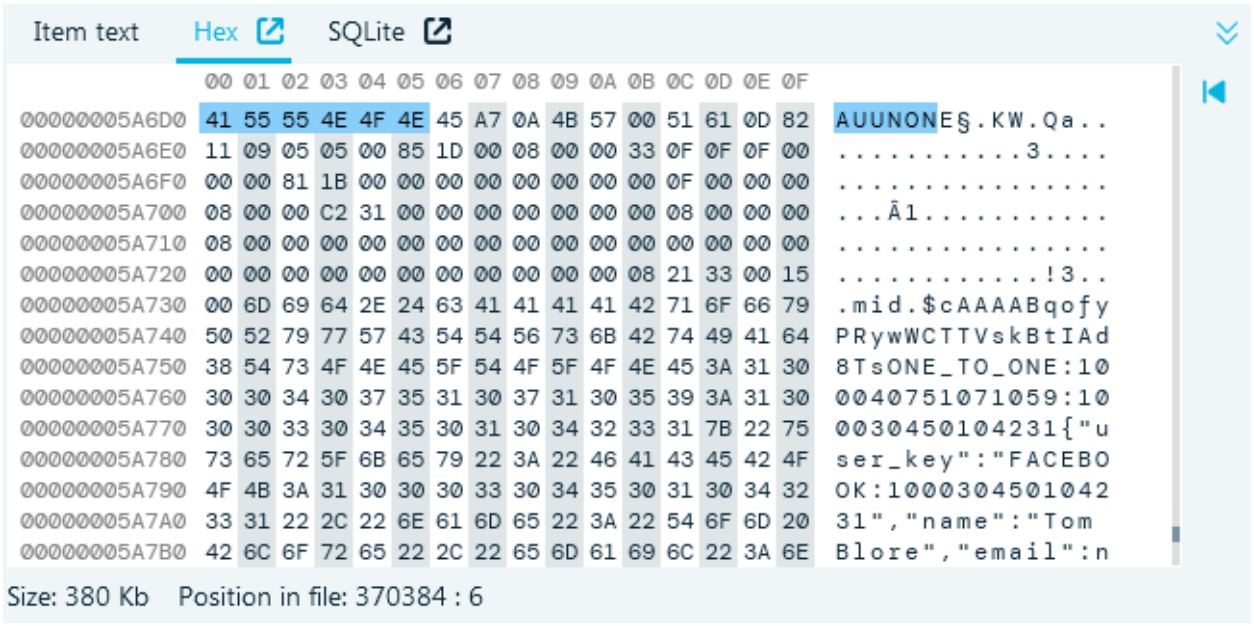
Larger size files are not stored in a case database. Types of files which are not saved, include pictures, videos, documents, SQLite databases, and so on. If you export a case with these types of artifacts to Evidence Reader, you will not be able to open or preview them. Only textual information will be available, such as metadata or plain texts (for documents).

If you would like to be able to review pictures, preview documents and so on, you should save needed artifacts to database before exporting them to Evidence Reader. To do so, select artifacts you need in a corresponding artifact list and choose **Save checked items to database** context menu item:



Tools

At the bottom of the middle part you will find **Tools**.



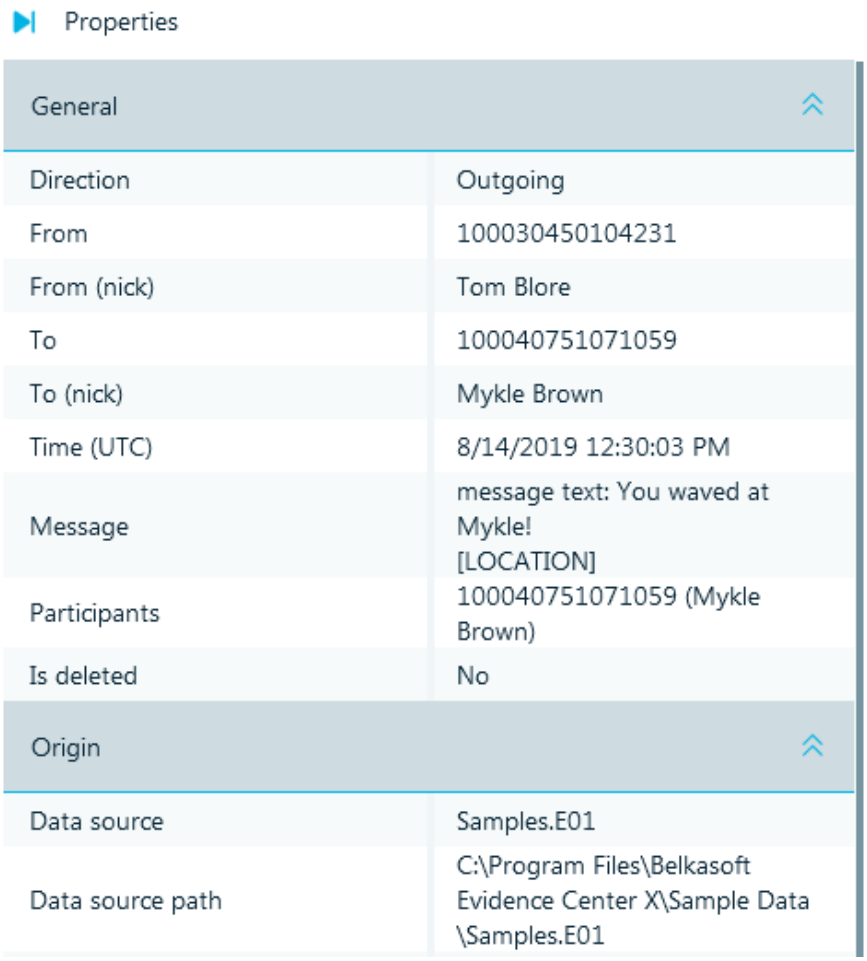
Tools contain Item text, **Hex Viewer** and other viewers depending on how the original item is stored. If it was stored in an SQLite database, there will be a **SQLite viewer**. If it was a registry or Plist item, a corresponding viewer will be shown.

To open a viewer full screen, click on the corresponding  icon at the right of the viewer name.

You can hide the **Tools** pane using  icon.

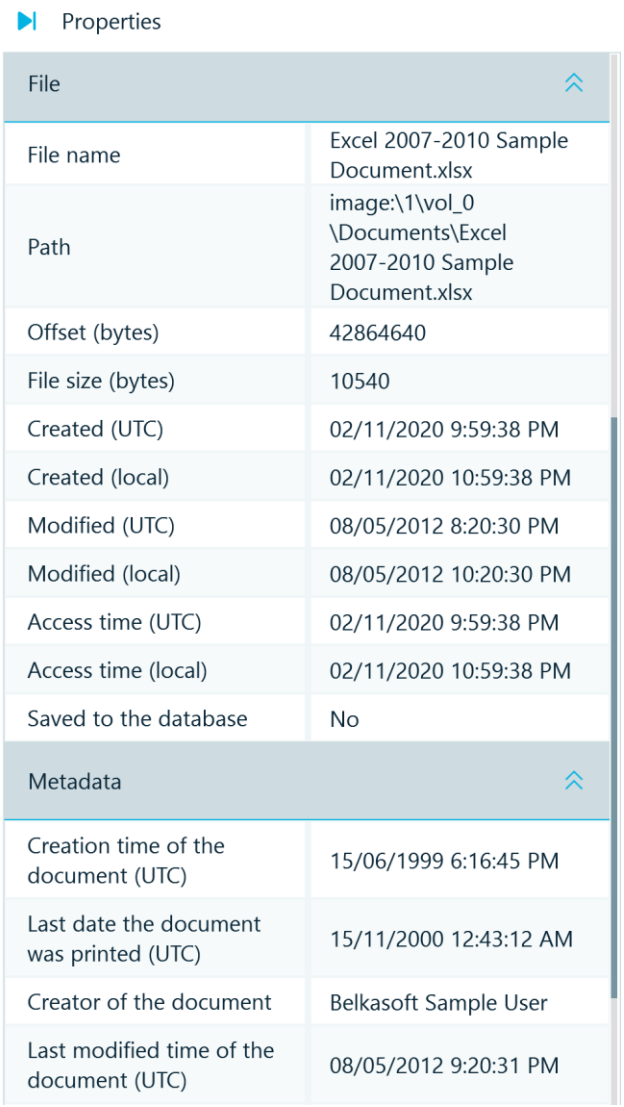
Properties

At the right side of the **Artifacts** window, there is **Properties** pane. Here you can review the properties of an item currently selected in the item list. You can also copy any property or its part.



Difference between **File** properties and **Metadata** properties:

File results - file properties in the corresponding OS file system (for example: *Creation time in Windows* is the creation time at the current location. It changes with any copy within the system.).
Metadata results - metadata stored by a document of a certain format (in this case, Excel).



In this case:

The original document was created on 15/06/1999 (from the Created metadata) and was printed 15/11/2000 then the user opened and modified the file on 08/05/2012 at 09:20:31 PM (the Modified metadata in the document). Then document was copied to a new location on 02/11/2020 (Created from the file system).

Top part

At the top there is the Report button, the mini-timeline, and the global filter button.

Report button creates a report for all items checked in the currently shown tab at the left, either **Structure** or **Overview**. If you need to create a report for items checked in the item list, right click there.

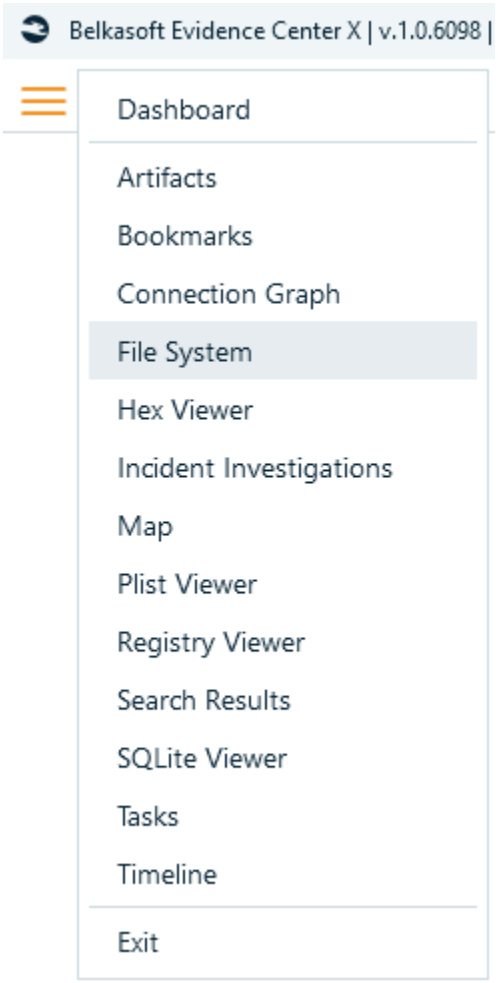
Mini-timeline shows you how artifacts spread over time. You can click inside and select a date range. The product will filter all items and show only those which fall under the selected range. You can adjust the range by dragging its left and right border. Clear the selection by single clicking anywhere on the timeline.

At the right of the mini-timeline, there is a **global filter** icon. Click on it to apply, edit or reset global filters. When a filter is applied, this icon turns orange. Find more information in the **Filtering** chapter.

File System

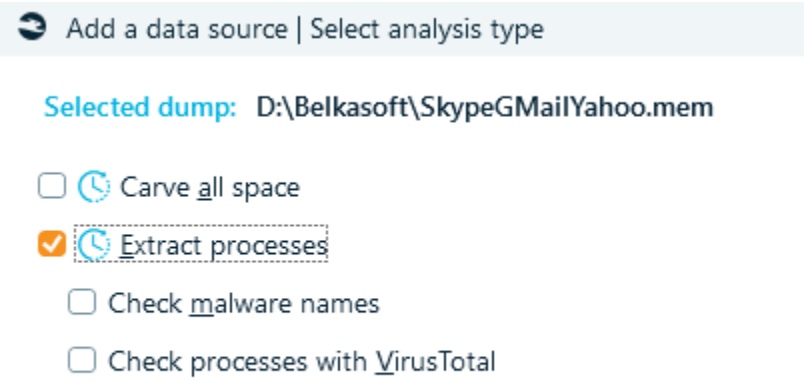
File System window allows you to examine the file system of data sources, added to your case, including special and hidden files and folders. It can also visualize memory dumps, particularly showing you memory processes for a given RAM dump.

If you do not see **File System** window, you can show it by clicking on **File System** main menu item.



For data sources, which have file system inside, the product shows the file system contents even if you did not opt to analyze artifacts at the **Add data source** window. However, to see RAM processes, you will

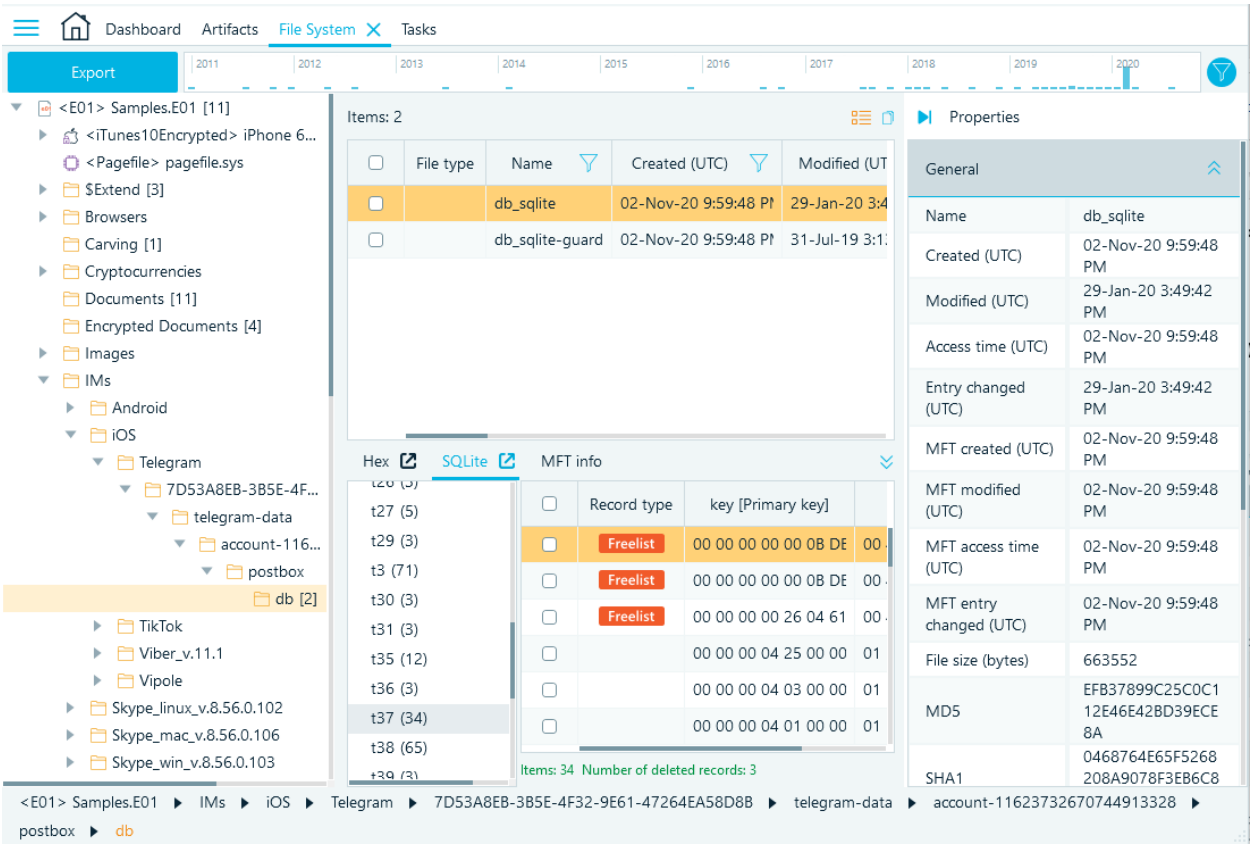
need to analyze the memory dump of interest and specify **Extract processes** option while adding a data source:



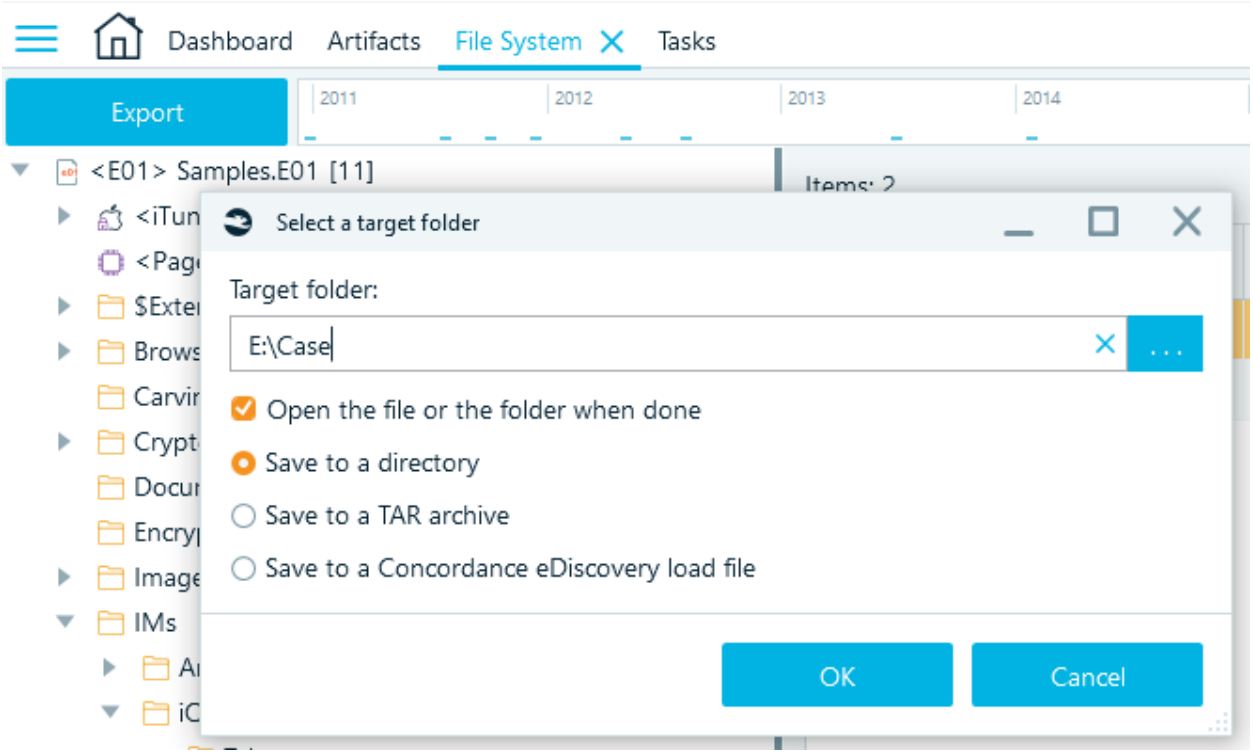
Note: This option slows down RAM dump analysis so do not select it if you only need to carve the dump for artifacts and are not interested in the process list.

File System window is divided into six parts:

- Timeline (top panel)
- Data source structure (pane at the left)
- File or process list (pane at the top center)
- Selected file in Hex, SQLite or MFT info Viewers, if applicable (pane at the bottom center)
- Selected file details (pane at the right)
- The path (navigation) to the currently highlighted node (at the bottom)



You can save a copy of the file system using the button **Export**.



Data source structure

Data source structure pane is organized as a form of a tree view with the following nodes:

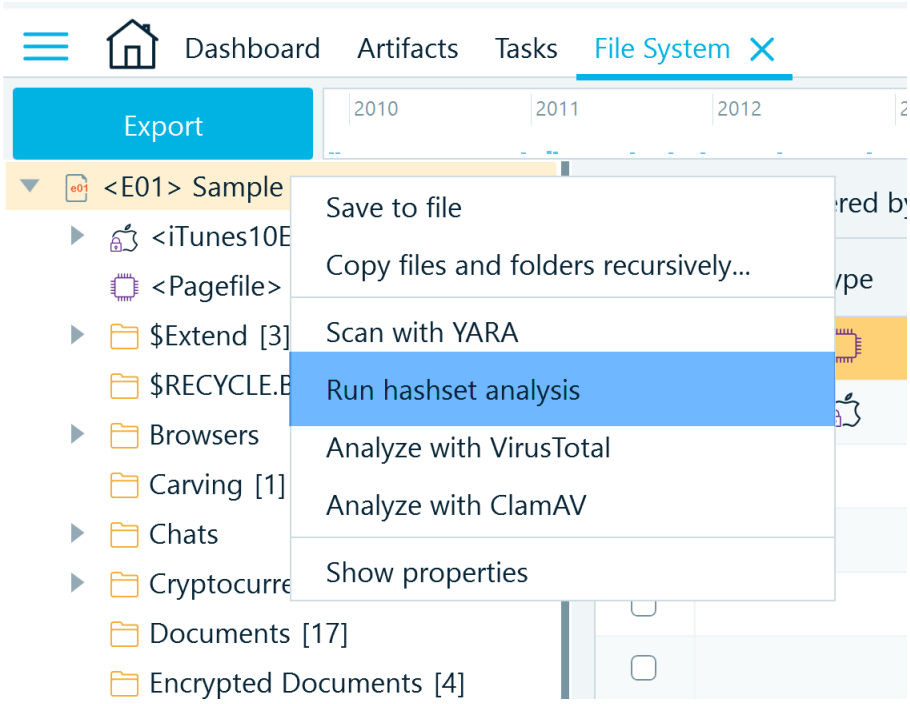
- Top level nodes are data sources added to your case using **Add Data Source** window. You can see type of data source in angle brackets preceding data source name. On the picture above you can see that "Samples" is of type "E01" and "iPhone 6S" is of type "iTunes10Encrypted" (encrypted iTunes backup). An icon at the left of data source name can also helps to quickly classify the data source
- Lower levels can be:
    - Nested data sources (e.g. iTunes backup on the picture above)
    - Volumes and partitions
    - Folders
    - Volume shadow copy snapshots

The number inside square brackets indicates the number of files located in this folder (no brackets mean no files, as, for example, for "Thumbnails" folder on the picture above). It does not include files in subfolders. For RAM dump, this number indicates the amount of processes recovered in this dump (shown only if you analyzed the dump with **Extract processes** advanced carving option switched on). When you select any folder, snapshot or RAM dump in data source structure pane, the corresponding item contents will be shown in the list at the right, such as subfolders, files or memory processes.

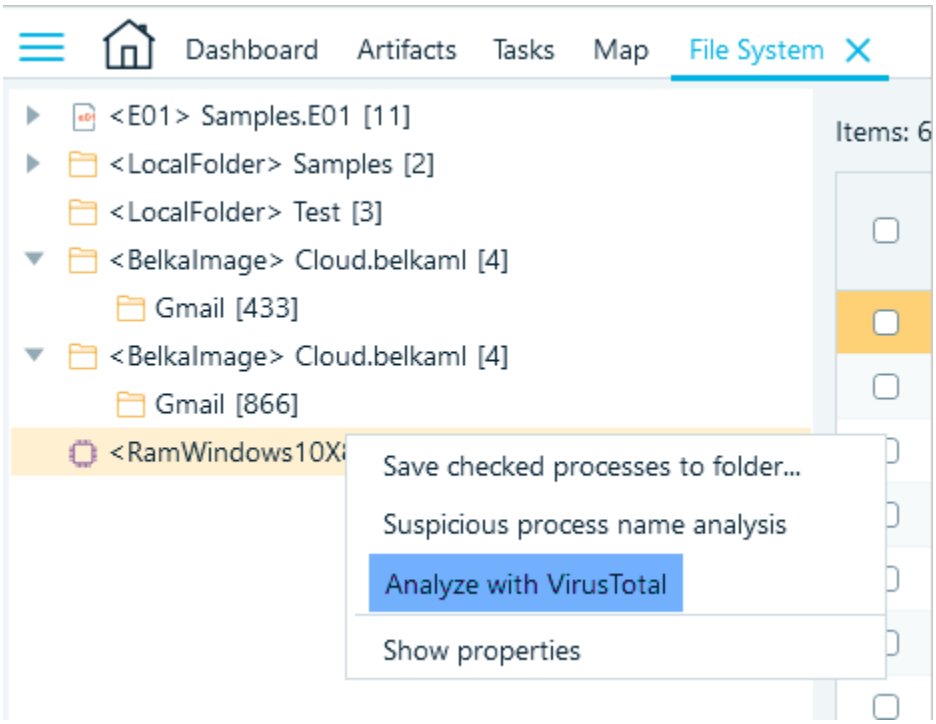
Data source structure context menu

When you right click on a node in the data source structure pane, a corresponding context menu will appear, which may contain some of the commands below:

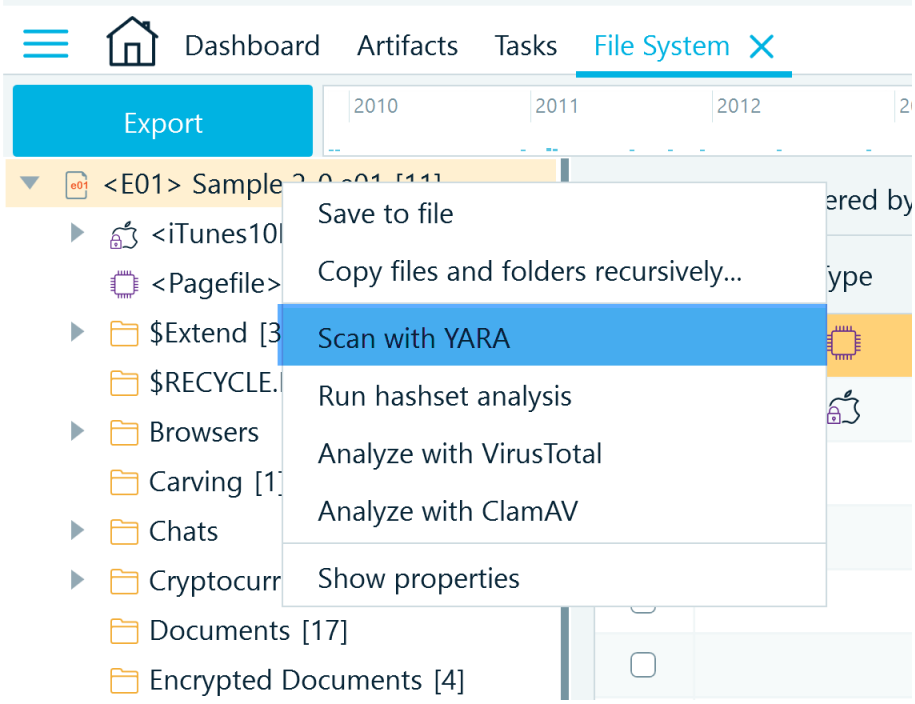
- **Run hashset analysis.** Allows to initiate the calculation of hashes for the data source.



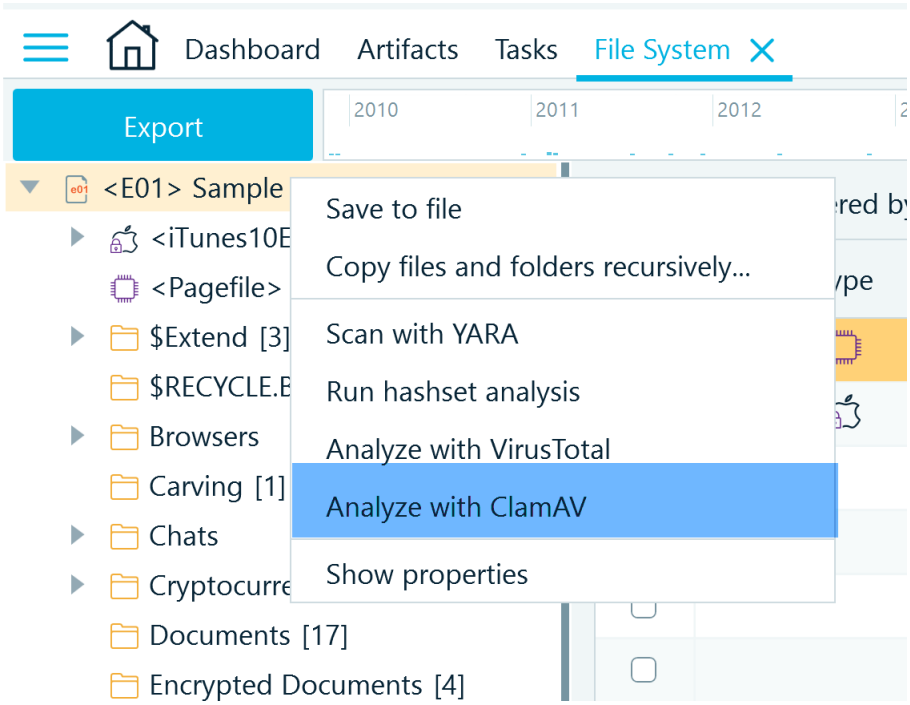
- **Analyze with VirusTotal**. This menu item is available for memory dumps with processes extracted by Belkasoft X. It will upload the entire memory contents for each process to VirusTotal and retrieve analysis result from there.
  Note: This function needs an Internet connection.
  Note: Unlike for files, the entire process memory is uploaded since hash analysis is not applicable for memory. Analysis results will be then shown in the process list and process details panes.



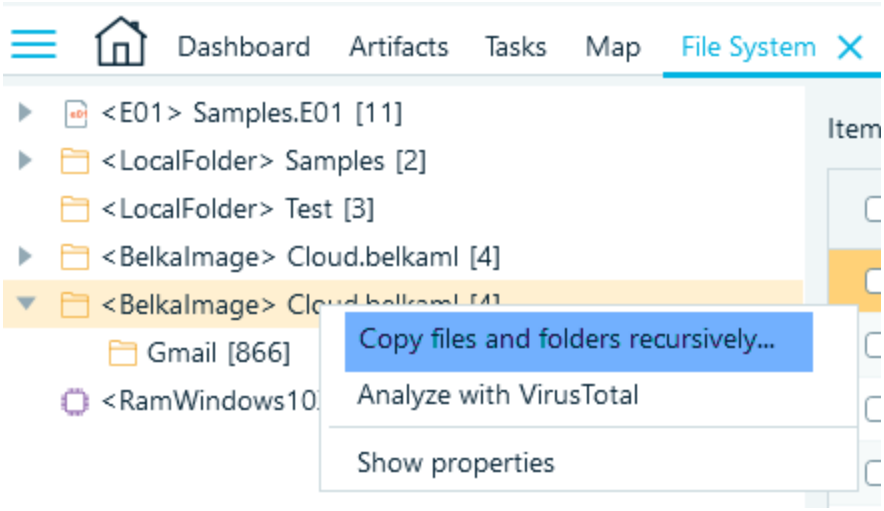
- **Scan with YARA.** Allow run signature analysis based on YARA rules.

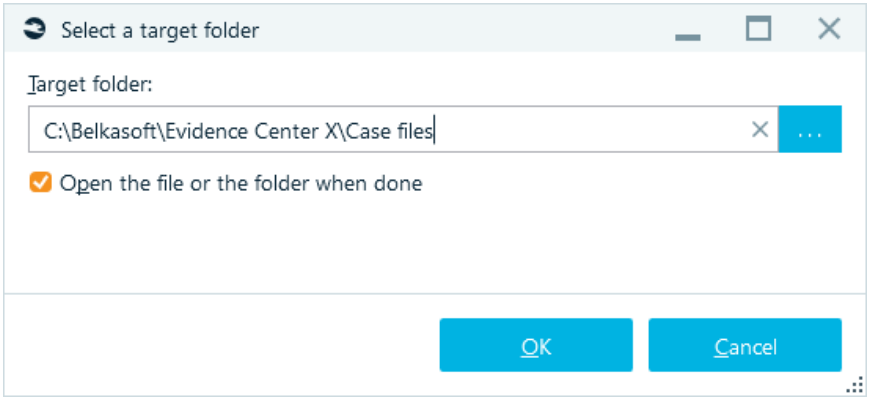


- **Analyze with ClamAV.** Run files analysis with open-source antivirus software ClamAV.

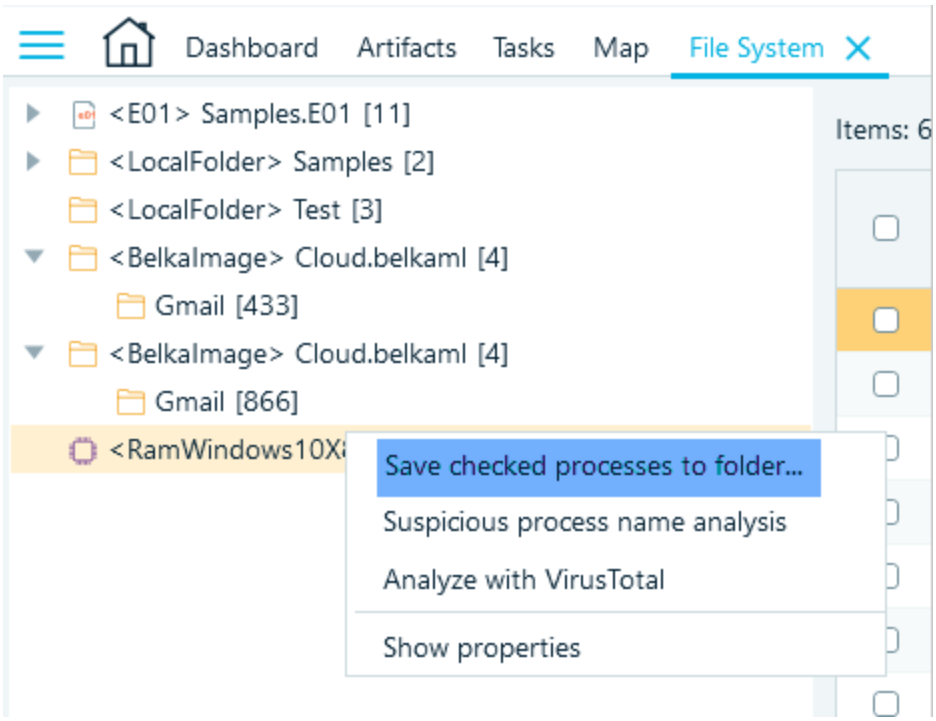


- **Copy files and folders recursively...** This menu item will copy files from a selected folder and its subfolders to your host machine folder.

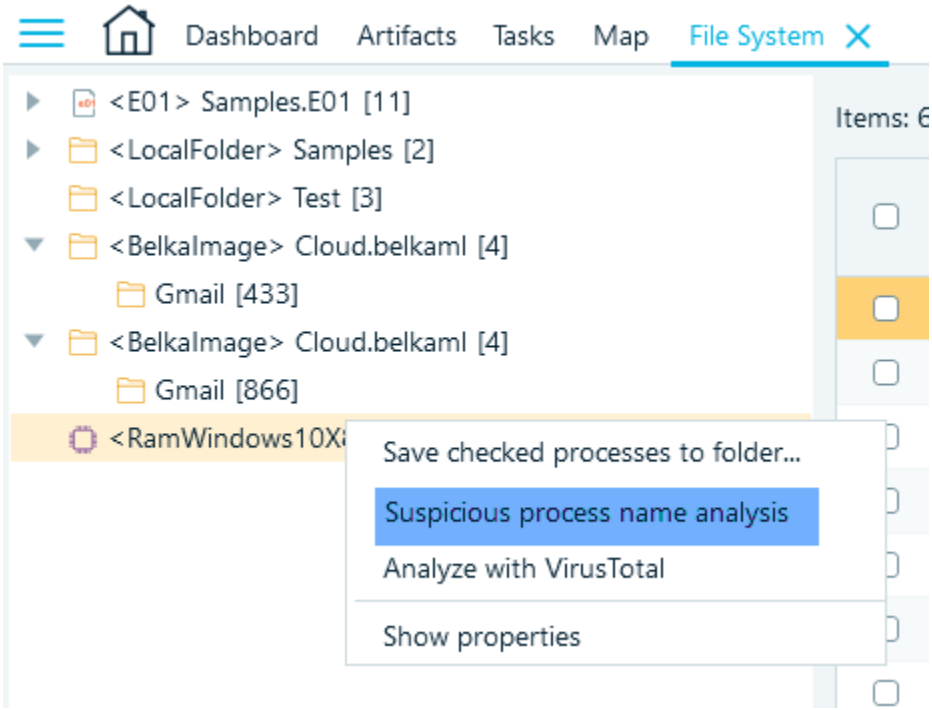




- **Save checked processes to folder…** This menu item is available for memory dumps with processes extracted by Belkasoft X. It works similarly to **Copy files and folders recursively** menu with the only difference that it copies processes, not files.

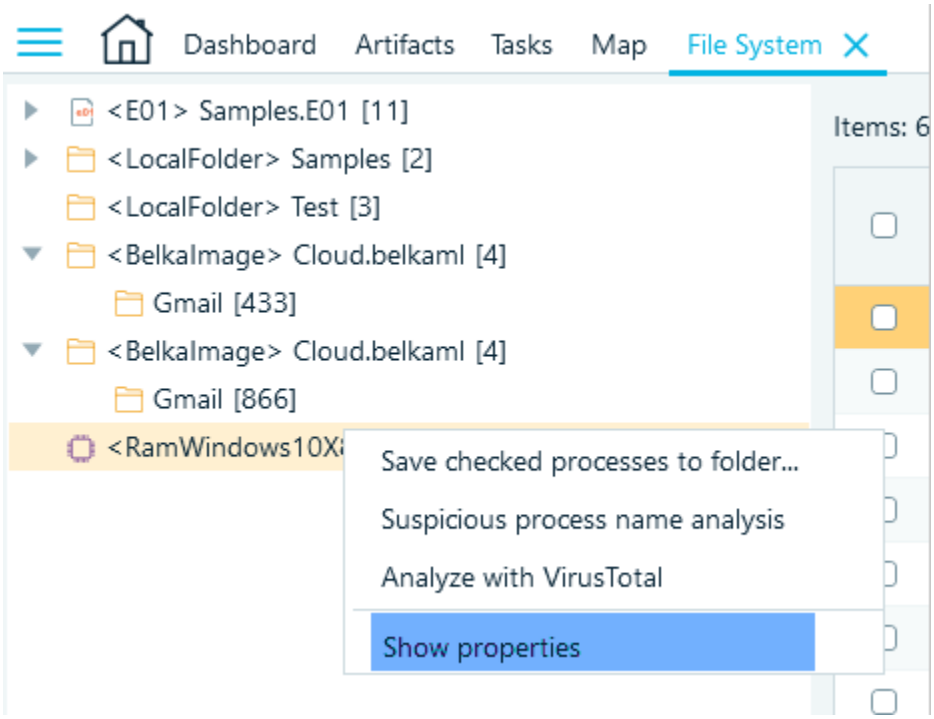


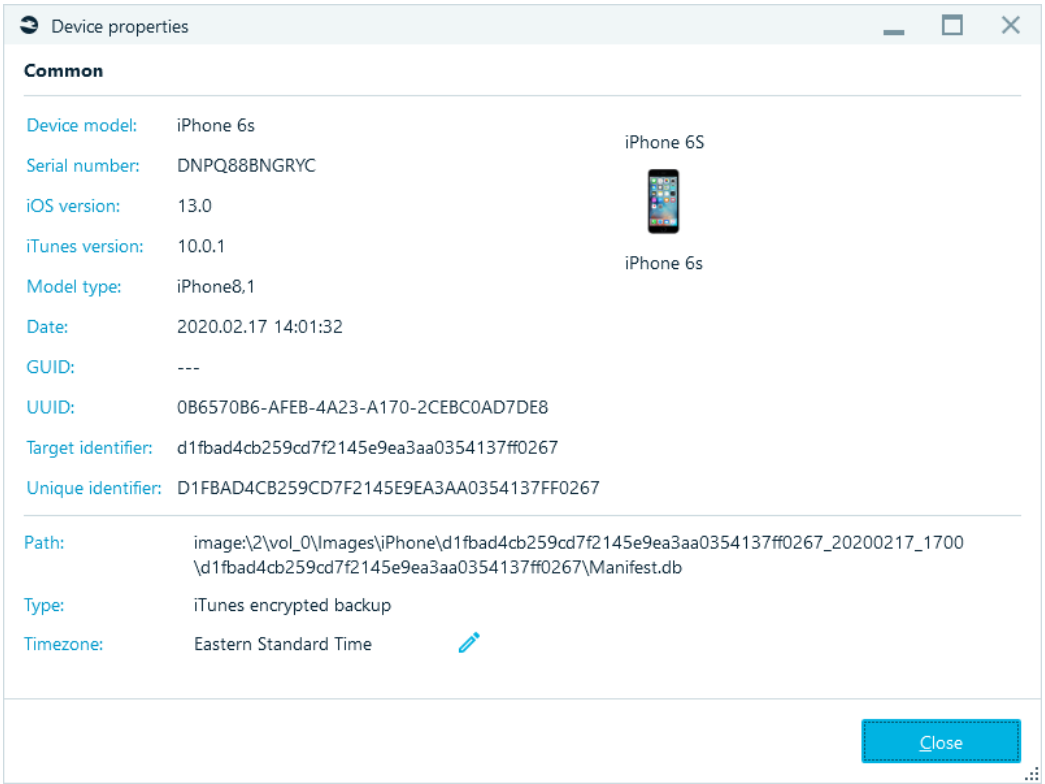
- **Suspicious process name analysis**. This menu item is available for memory dumps with processes extracted by Belkasoft X. It checks names of extracted processes against a list of suspicious names, for example, s**cv**host.exe instead s**vc**host.exe. The latter is a valid system process name while the former is a fake and, quite probably be malware.



- **Show properties**. This menu item is available for data sources and it opens Properties window. The set of properties displayed depends on the data source type. The window below shows

properties of an iTunes backup, which include such information as **Device model**, **Serial number**, **iOS version,** etc.

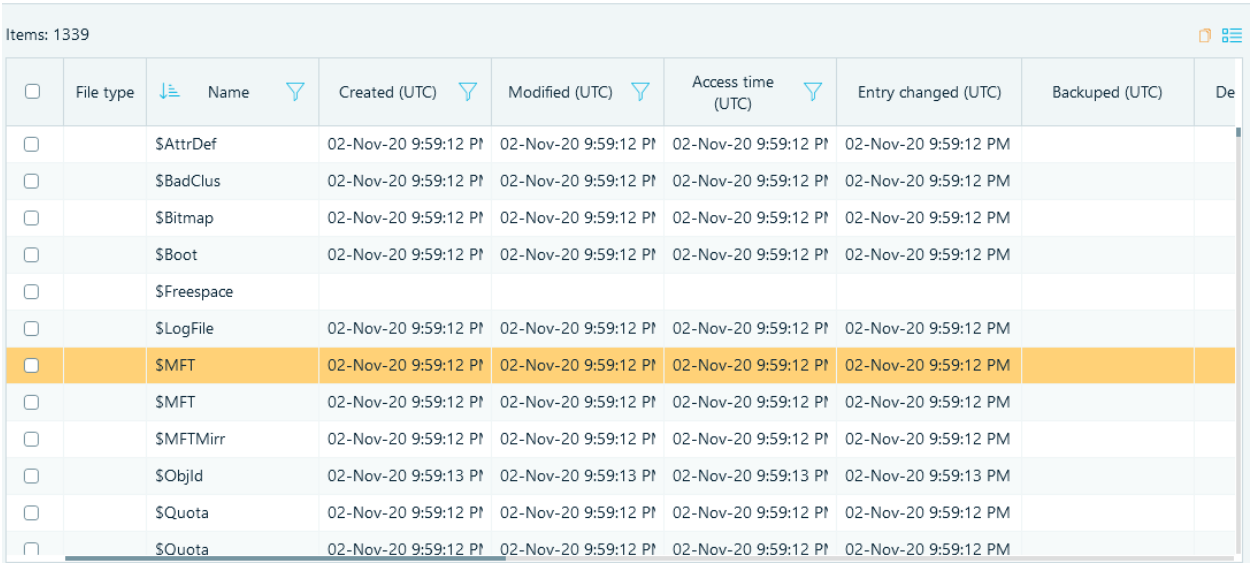




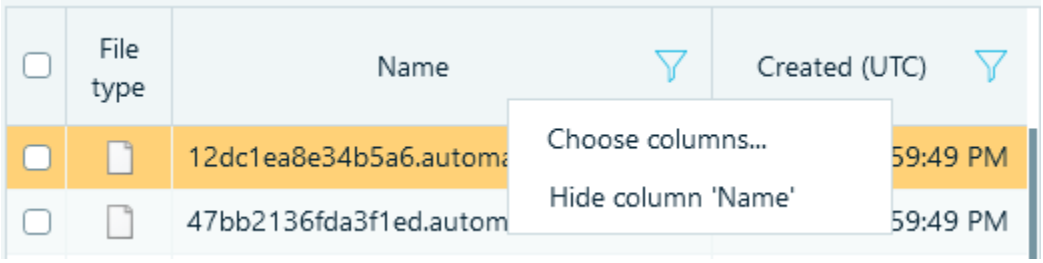
File or process list

The pane at the middle of **File System** window is a list of items corresponding to the selection in the data source structure pane. These items can be subfolders and files (if a folder selected in the data source structure pane) or processes (if a RAM dump is selected and this dump was analyzed with **Extract processes** option).

There is a recursive view and a grid view. Using recursive view, you can instruct the product to show all files within currently selected folder (or a partition, if you selected it) and all its subfolders. A number of useful filters such as filter by file name and various file times are also available.



Each list contains a checkbox for multi-item operations. There are various columns, including file or process name, times (such as Created, Modified or Last Accessed) and other properties of a file or a process. As in other lists, you can click on any column header to sort by this column value, and second click will reverse the sort order. Right click on any column header will allow you to choose columns to display, change column order or hide the selected column:



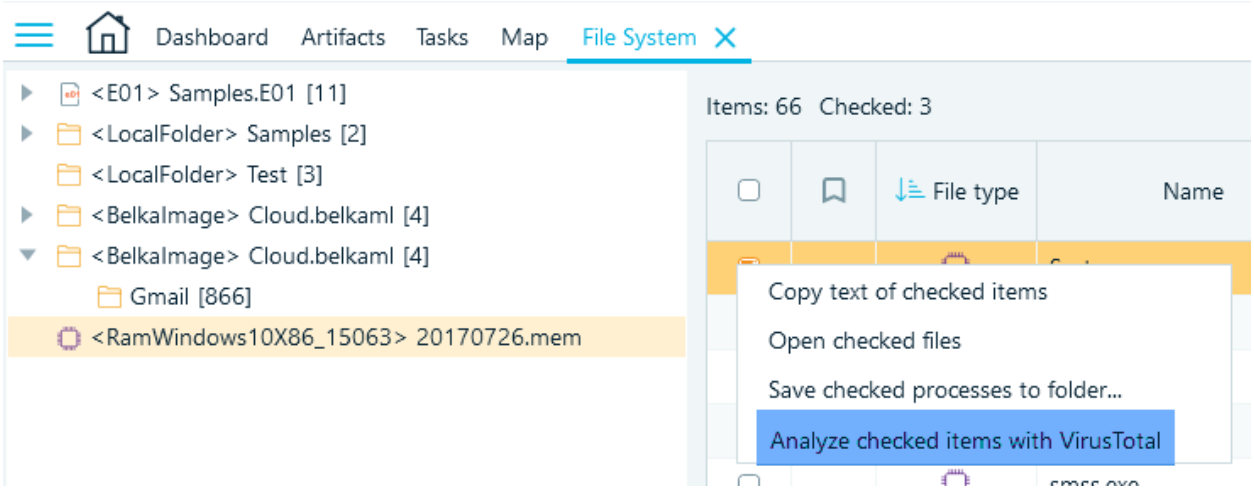
*Right click on any column header and select **Choose columns...** context menu item to specify set of columns to show or change their display order*

File or process list context menu

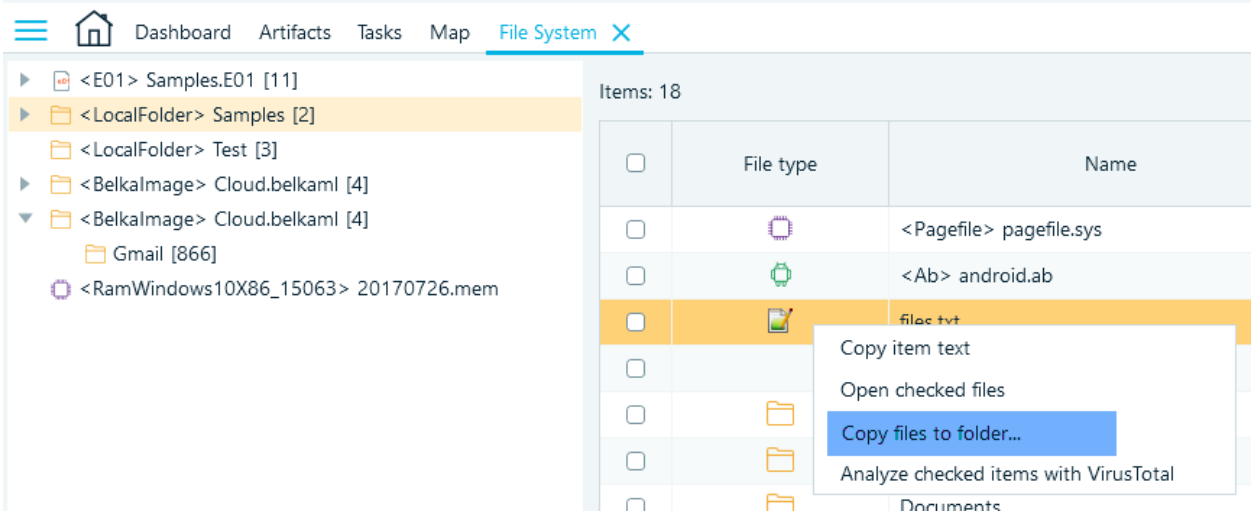
When you right click on an item in the file list pane or process list pane, corresponding context menu will

appear, which may contain any of the commands below:

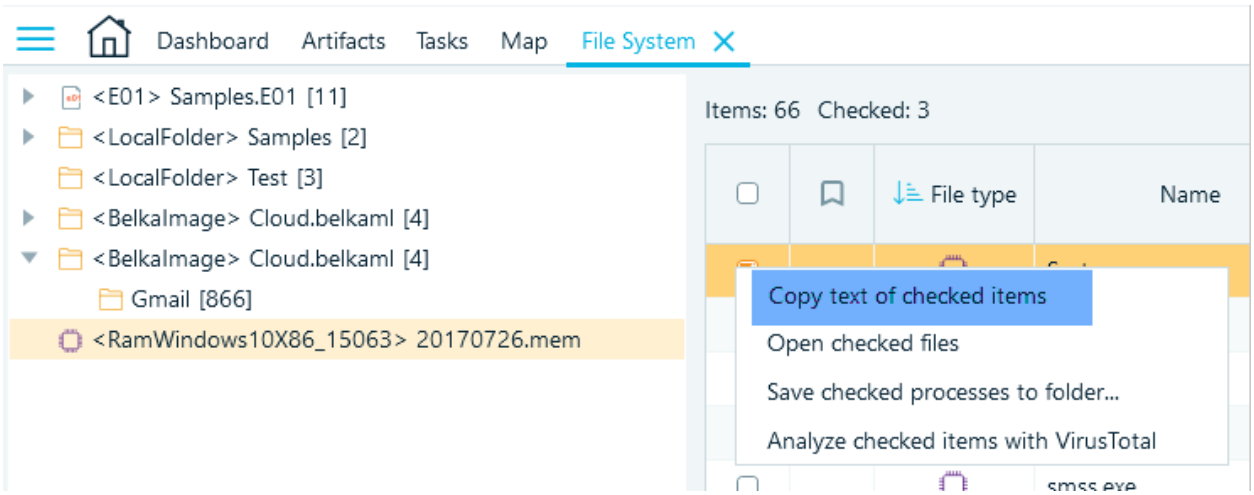
- **Analyze checked items with VirusTotal**. This menu will upload the entire memory contents (if a process is selected) or a file hash (if a file is selected) for checked item to VirusTotal and retrieve analysis result from there.
  Note: This function needs an Internet connection.
  Note: Unlike for files, the entire process memory is uploaded since hash analysis is not applicable for memory. Analysis results will be then shown in the file or process list columns and details pane.



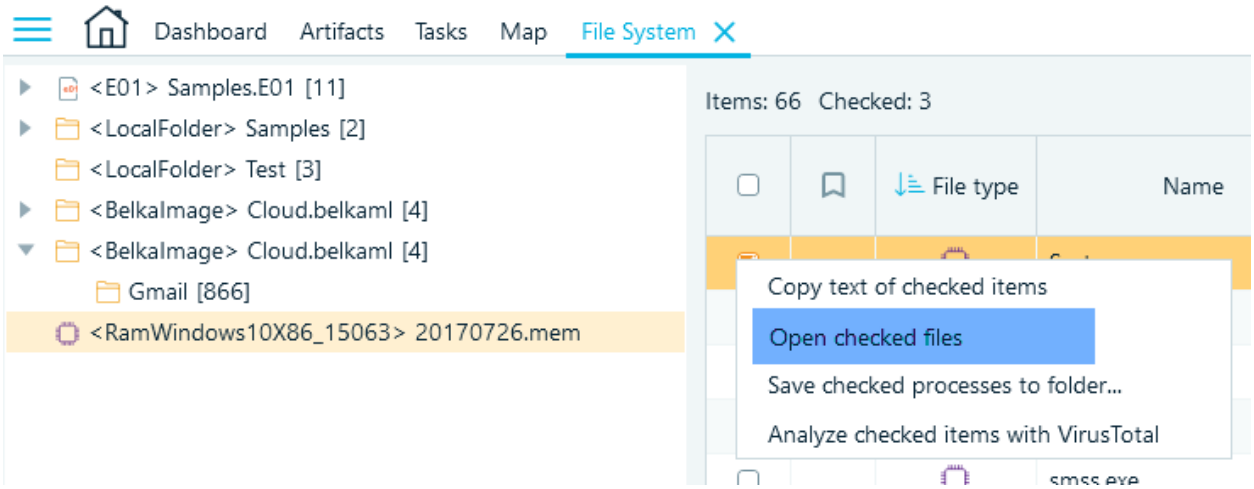
- **Copy files to folder…** This menu item will copy checked files from the file list to your host machine folder.



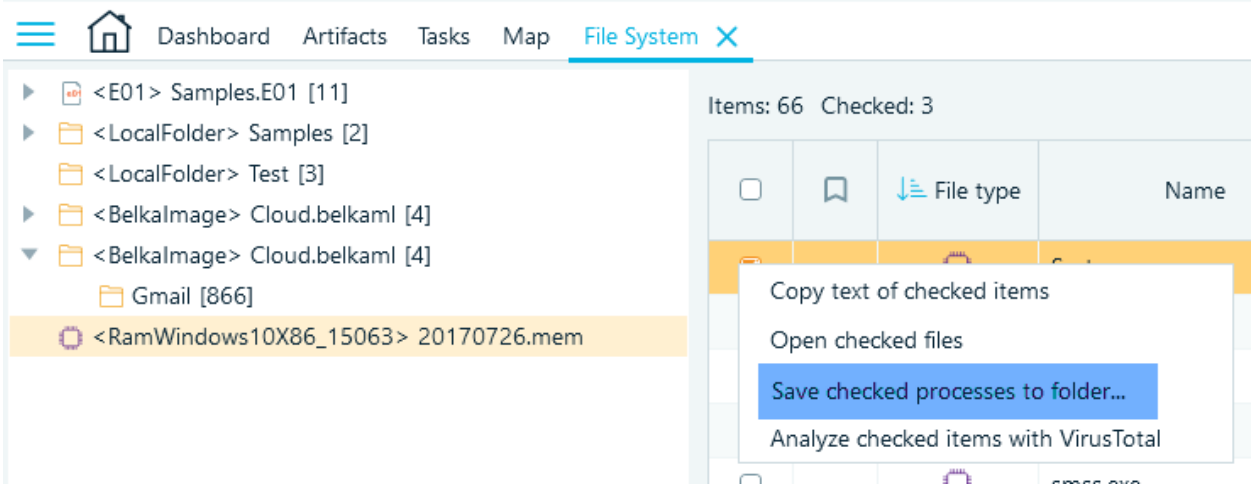
- **Copy item text / Copy text of checked items** will copy all checked items along with visible properties, delimited by semicolon.



- **Open file(s) / Open checked files** menu will open checked files in default viewers such as a text or a document editor.



- **Save checked processes to folder…** This menu item is available for the process list. It copies checked processes' memory to a selected folder on your host machine.

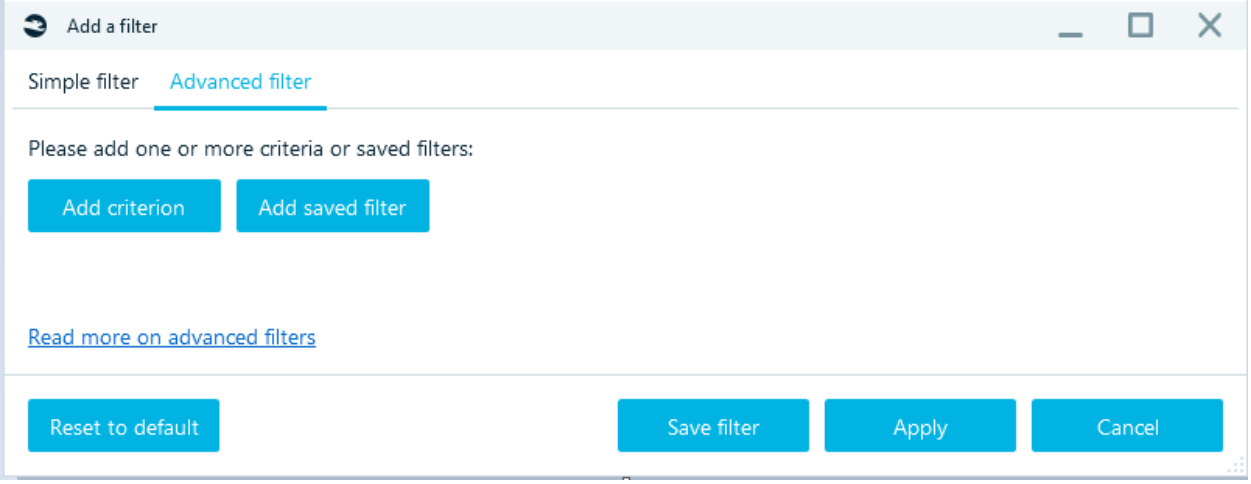


Selected file or process details

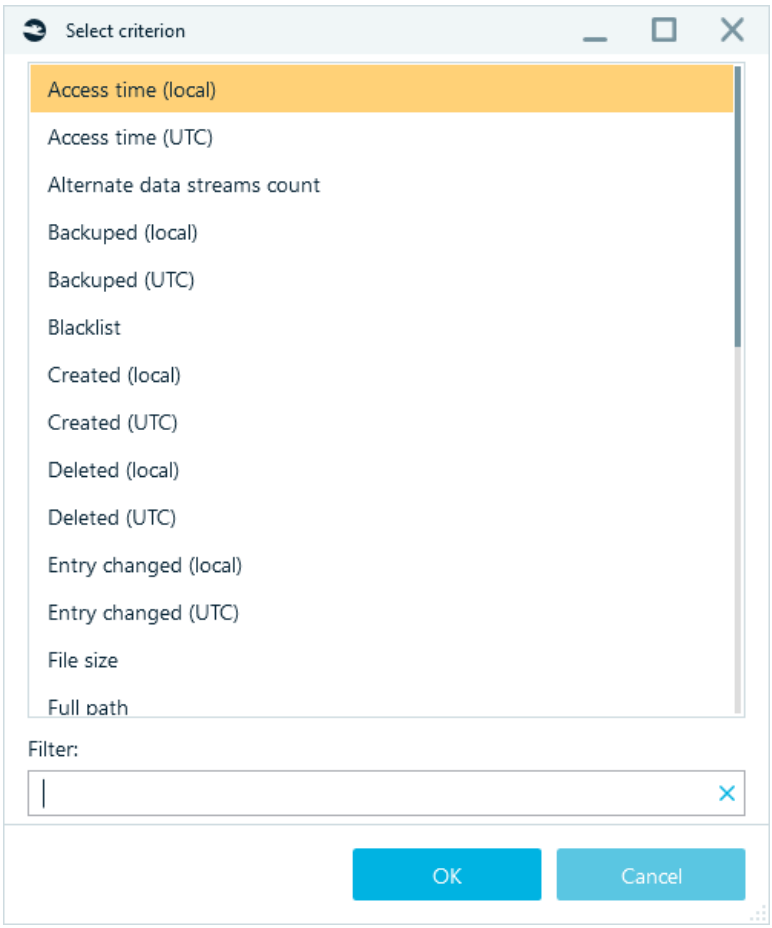
Once you selected a file or a process in the file list or the process list, its details will be shown at the right. You can see the file or process properties in this pane, such as name, timestamps, file size.
Under the file or process list you could review the file or process contents inside **Hex Viewer** and other viewers depending on your selection.
The work with details pane is the same as in other artifact lists.

Advanced filter

On **File System** tab, in addition to **Simple filters**, **Advanced filter** is also available.

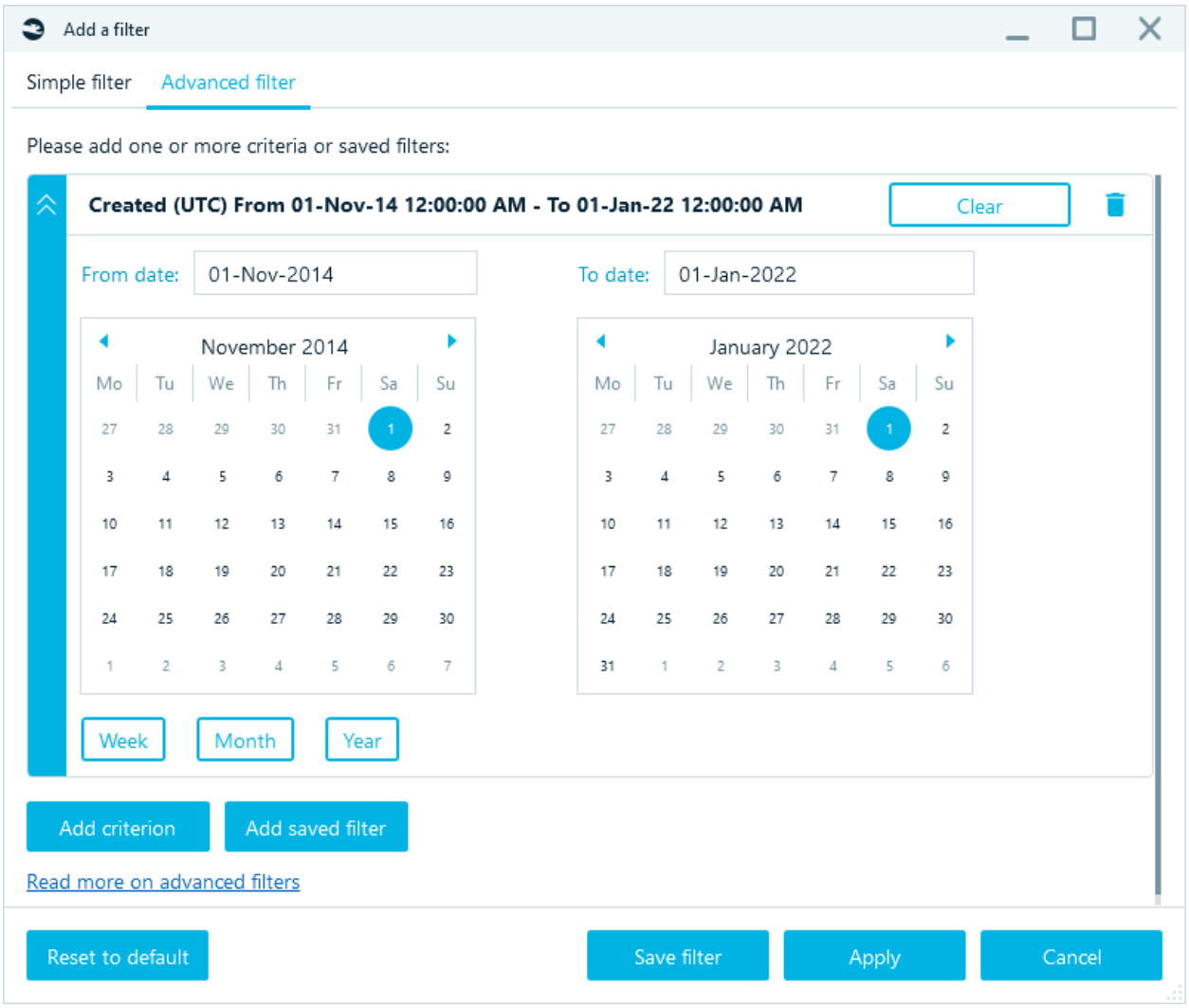


When you select **Add criterion**, a window with a list of criteria available for filtering appears:



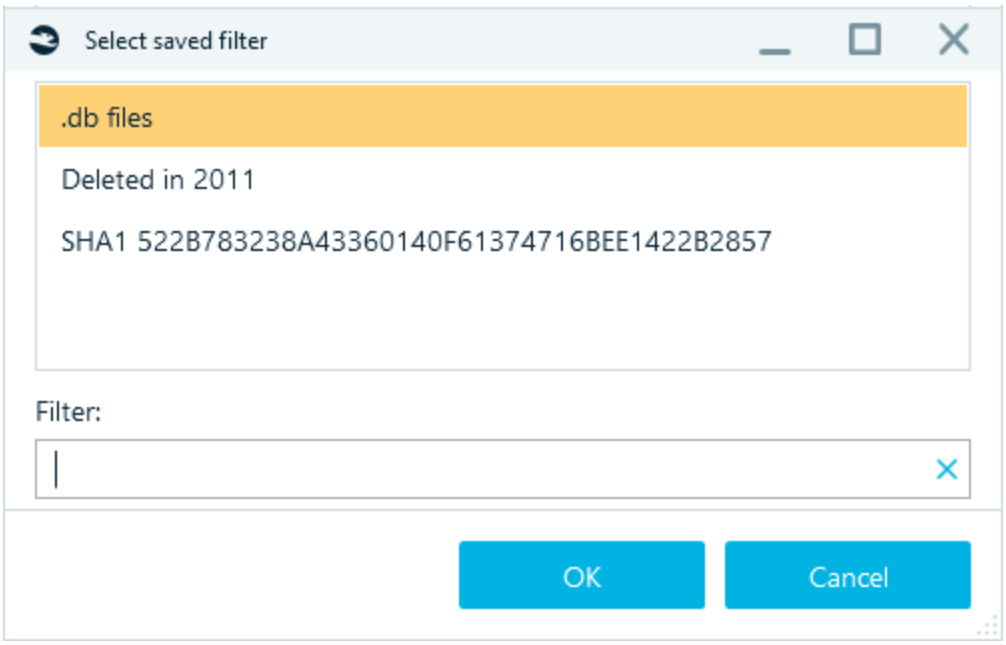
The names of the criteria are arranged in alphabetical order, you can also quickly find the criteria you need by typing in the name in the **Filter** field. After selecting the required criteria, click **OK**.

Set the parameters of the selected criterion.



Add the required criteria by clicking on **Add criterion**.

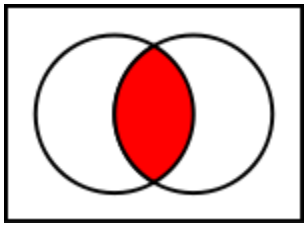
As a criterion for an **Advanced filter**, you can select a saved filter. For this click on **Add saved filter**.



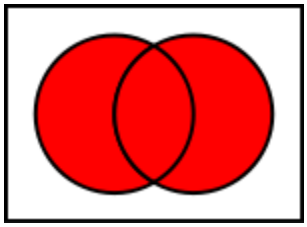
The names of the saved filters are also arranged in alphabetical order, use the **Filter** field for a quick search.

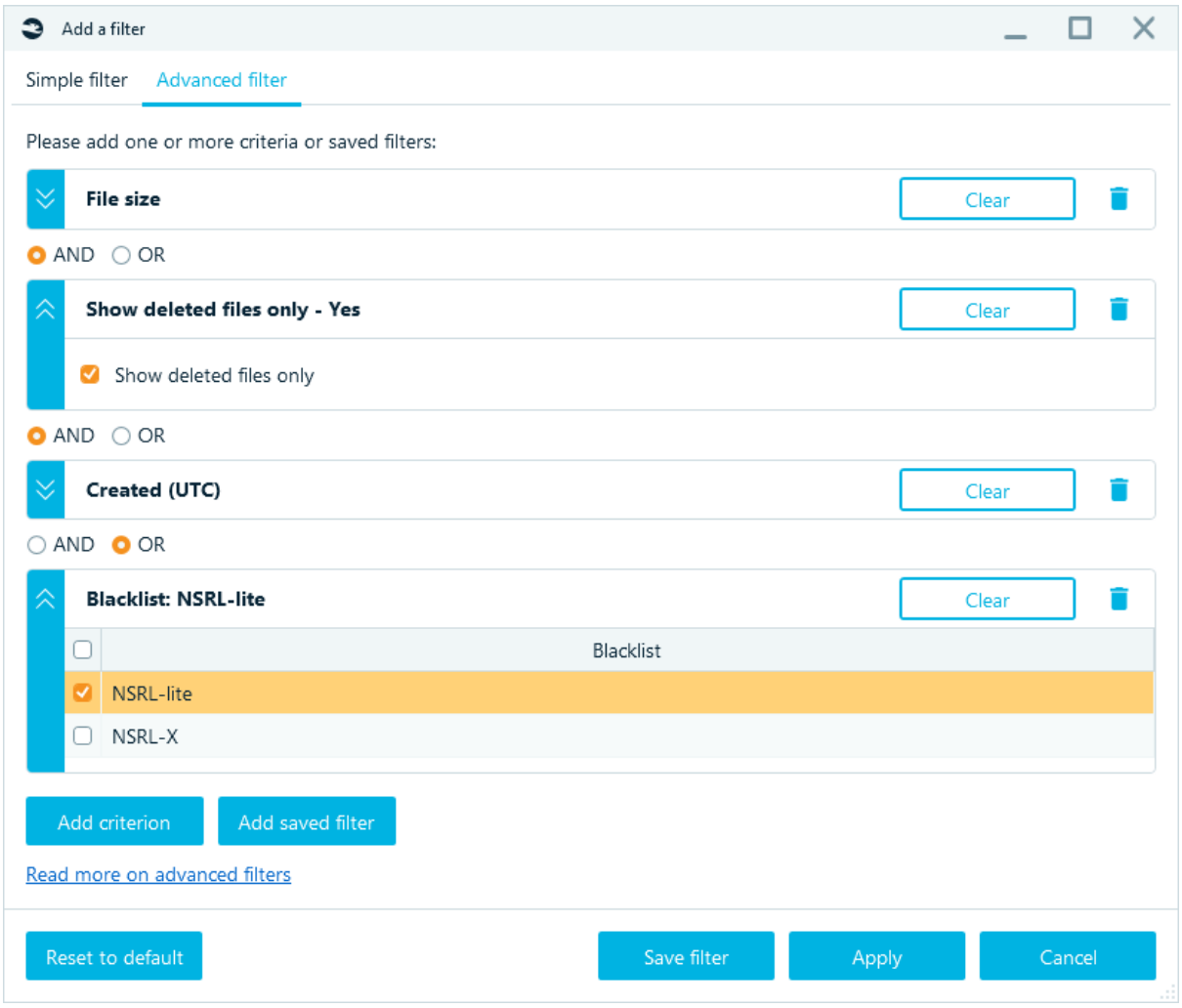
There are two conjunctions available:

- **AND**. This conjunction means that both criteria must be met. It also can be treated as an intersection of its logical parts



- **OR**. This conjunction means that any criteria can be met. It also can be treated as a union of its logical parts





If you need to delete a criterion - click on the icon . To clear the criterion value (without deleting the selected filter condition) – click on the **Clear** button Clear .

The **Save Filter** button allows you to specify a filter name and save the filter.

The **Apply** button closes the **Add a filter** window and filters the data on the selected filter criteria.

The **Cancel** button closes the **Add a filter** window without applying the selected conditions.

The **Reset to default** button removes all selected criteria without closing the **Add a filter** window.

To edit the conditions of the applied filter, click on the filter name above the grid:

Timeline

With Timeline, Belkasoft X combines all artifacts with timestamps—chats, emails, documents, pictures, and others—in your case and presents them in a defined order. Timeline allows you to review all activities or events that occurred around specific periods on one or more devices.
If you do not see **Timeline** window, you can open it by clicking on **Timeline** main menu item.

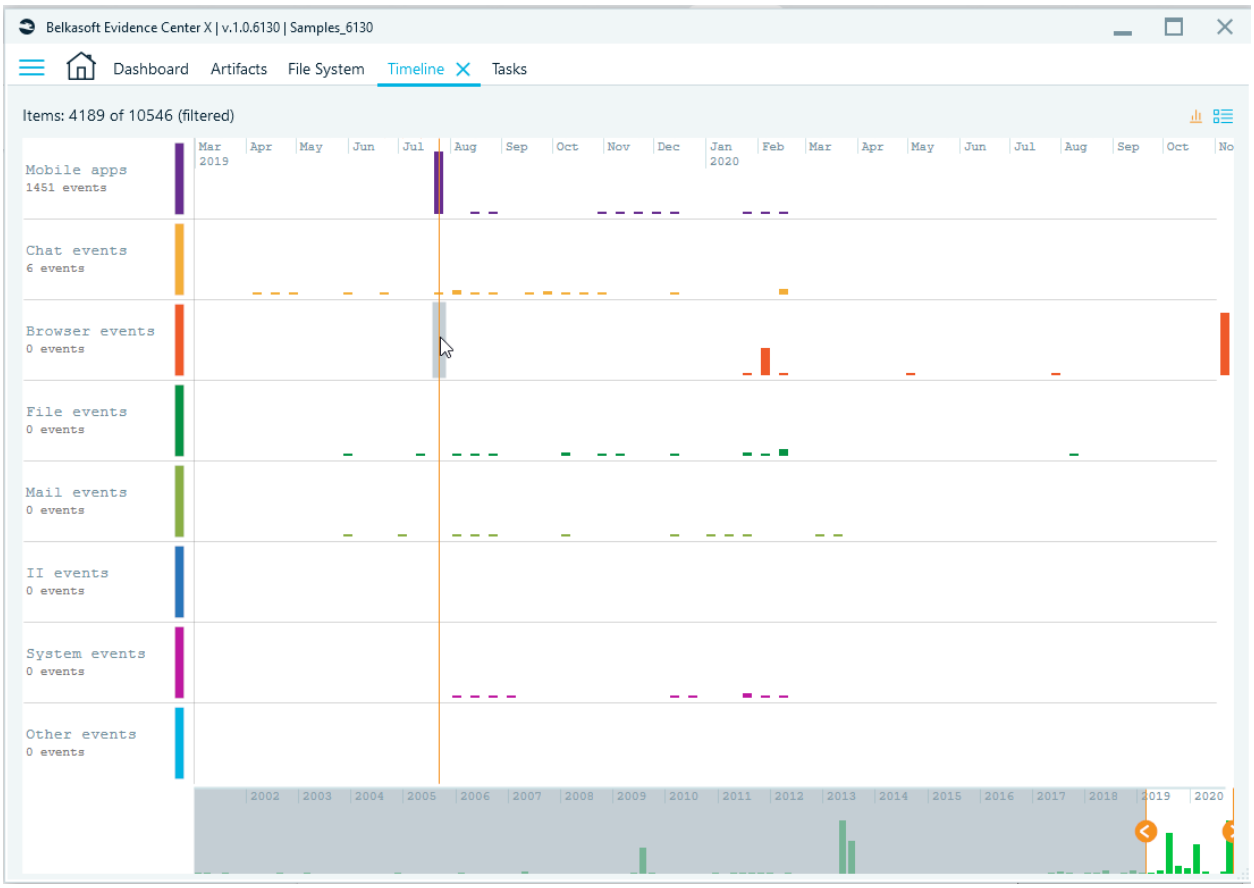
To update the Timeline contents (anytime), click on the refresh icon.

Timeline's view

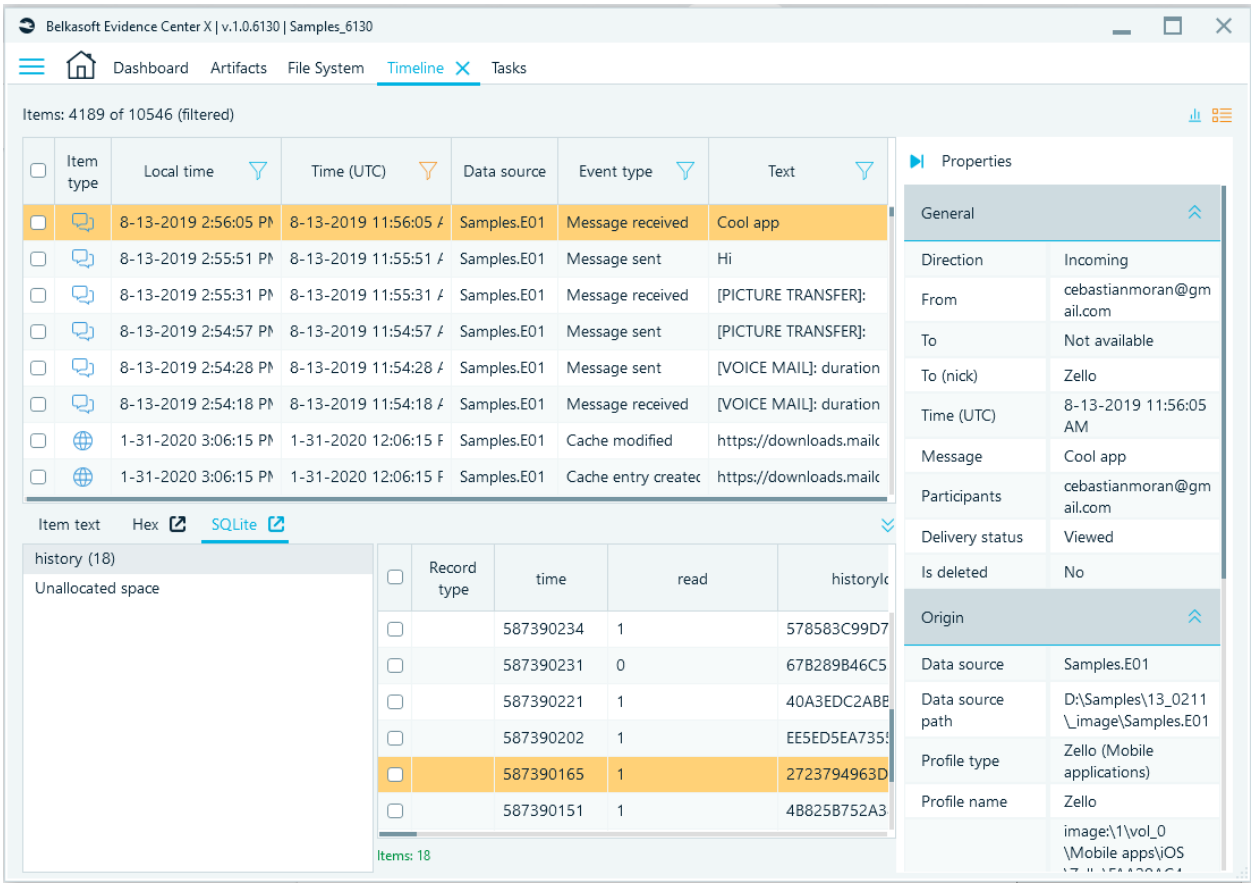
To select a view—Timeline or List —click on the option at the top-right corner. **Timeline (graph) view** has 3 display modes: with categories, colored bars, solid bars. To switch between modes, use the keyboard shortcuts ctrl + q / w / e. The default mode is with colored bars (ctrl + w).
You can also select a theme: light / dark using the keyboard shortcut ctrl + t.

Within the context menu are shown the first 20 events that fall into the selected time point. After you select an event from the drop-down list, you can navigate to this item on the **Structure** or **Overview** tabs.

The time interval can be changed by selecting the required area in the values area (top of the window) or in the overview area (bottom of the window). A double click removes the filter.



List view. When the list view is selected, you can go through artifacts arranged based on time. When you click on an artifact, Belkasoft X presents its attributes under the Properties pane on the right.



As other lists, **Timeline** item list has a checkbox column for operations with multiple checked items (such as a report creation), allows for sorting by clicking on a column header, filtering, customizing column set and so on.

Context menu of **Timeline** item list has the same items as other lists, but there is also one command, which is not yet described: **Go to original item**. This command navigates you to the item, which originated the selected **Timeline** item. Say for a "message sent" event, it will open **Artifacts Structure,** select corresponding chats profile and corresponding message in the list.

Note that some artifacts may be listed multiple times inside this window. For example, each file-based artifact (such as a document) has various operating system times, e.g. Created or Last access time. Besides, artifacts having metadata (such as a picture) may have various events recorded inside, e.g. "GPS time for shot" or "Date/time digitized". Each such time will result in a separate entry in **Timeline** (Grid view), which is why total amount of artifacts shown in **Artifacts Structure** typically does not match with the number of items in **Timeline** item list.

Usually **Timeline** contains a huge number of elements, so you may want to filter it by time span or types of events to show, for instance, only emails sent or received, or only computer boot times. For more information on this, see "Filtering data lists".

Difference between Local Time and Time (UTC)

Belkasoft X displays time values for artifacts under both **Local Time** and **Time (UTC)**.

When an artifact is stored used local time, Belkasoft X uses the value to calculate UTC time (based on the time zone settings you defined). When a data source uses a time zone that differs from that in the case, Belkasoft X uses the data source time zone.

Connection Graph

Connection Graph is a window, which on a high-level visualizes communications between people involved in the case. This window shows persons as dots (or avatars) and connects them with lines in case these persons had one or more occurrences of various types of communications, such as

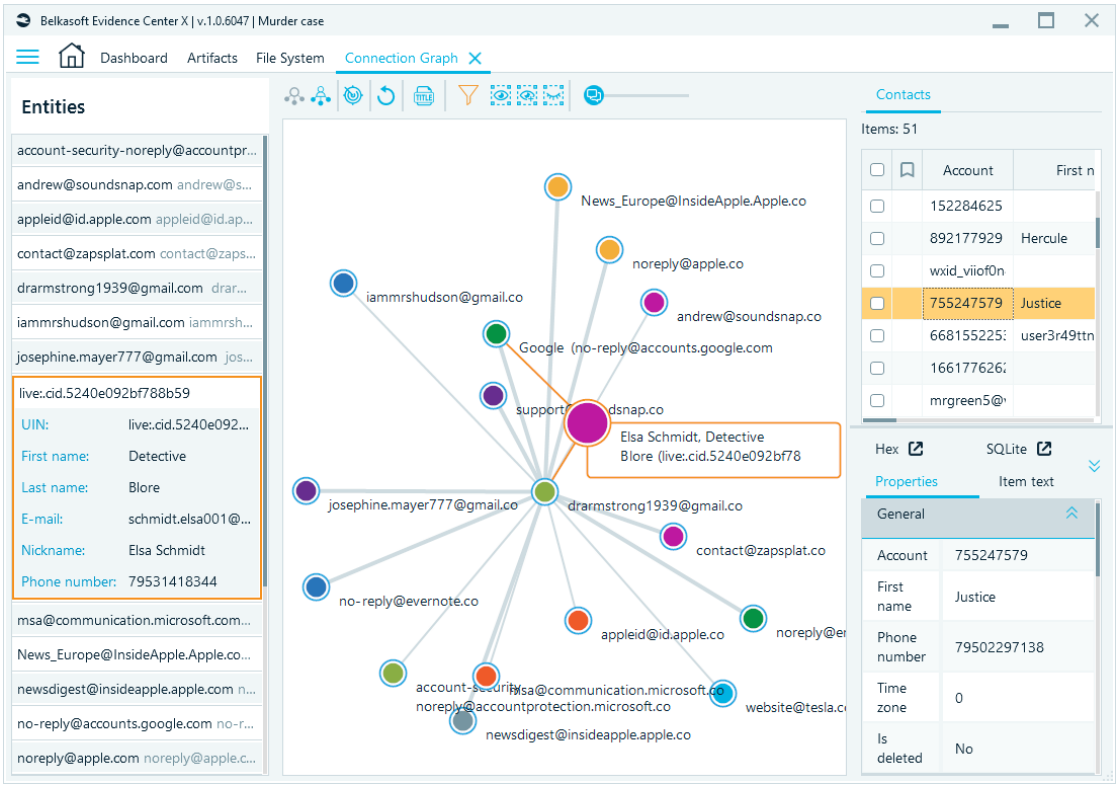
- Call
- SMS
- Instant messenger chat, file transfer or voice mail
- Email
- and so on

If you do not see **Connection Graph** window, you can open it by clicking on **Connection Graph** main menu item.

Connection Graph window consists of the following parts:

- Entities pane at the left

- Graph pane in the middle
- Contact or connection properties pane at the right



When you click on an entity on Graph pane, Belkasoft X displays the entity on the left pane and the contact list on the right pane. When you click on a connecting line on Graph pane, Belkasoft X displays both connected entities on the left pane and the communication between them on the right pane.

Contacts and entities

It is important to explain notions of contacts and entities. **"Contact"** is one account in email, or one chat profile or one phone number, while **"entity"** is something what unites various contacts. For example, if someone owns a smartphone, they may have multiple contacts: email, profile in Snapchat, another profile in Skype or WhatsApp, a few phone numbers. Belkasoft X tries to combine all contacts like that into a single entity so that you can see communication on a higher level.

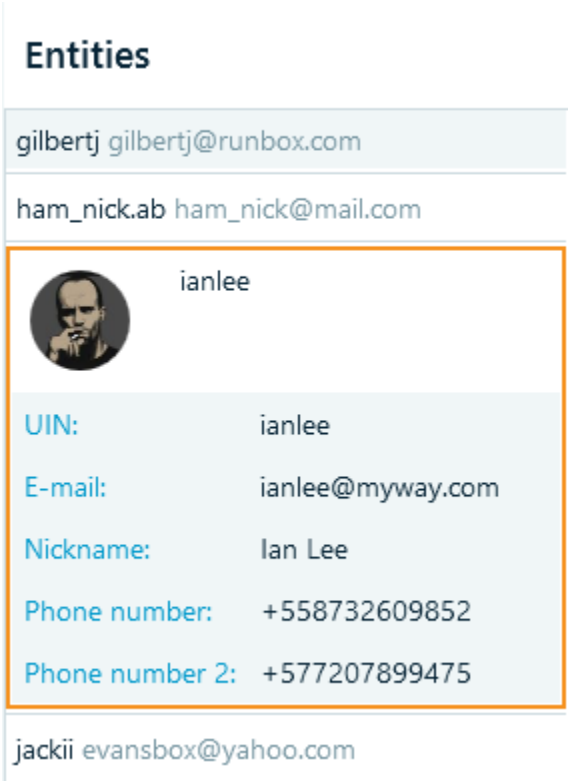
There are some assumptions on how Belkasoft X unites contacts into entities. It is supposed that there is only one owner of a smartphone and a computer. For other contacts, Belkasoft X tries to unite contacts by some properties, which are already found in the case. Say for instance, if someones WhatsApp account is bound to the same phone number that Telegram account, Belkasoft X supposes that there is just one person behind these two, so it creates an entity, which contains both WhatsApp and Telegram profiles. The same applies to various other types of contacts, which overlap in some properties, such as email, first and last names and so on.

Entities pane

In the entities pane you can see all entities extracted by Belkasoft X from all data sources and all

communication profiles in the case (e.g. instant messenger contacts, phone book records, email recipients and so on). Each data source also has an artificial contact of its owner.
You can select single entity in the entities pane by just clicking on it, multiple entities by clicking on entities of interest and holding Ctrl button and a range of entities by clicking with Shift button being pressed. Corresponding entities will be highlighted in the graph pane. On the picture above you can see one of the entities highlighted with the yellow circle, meaning that it is currently selected.
When you click on an entity in the entities pane, you will see available contact details under the selected entity.
The following information will be shown:

- Avatar (if any)
- Nickname or first and last name, if available
- UIN, if any
- Phone and email, if any



Graph pane

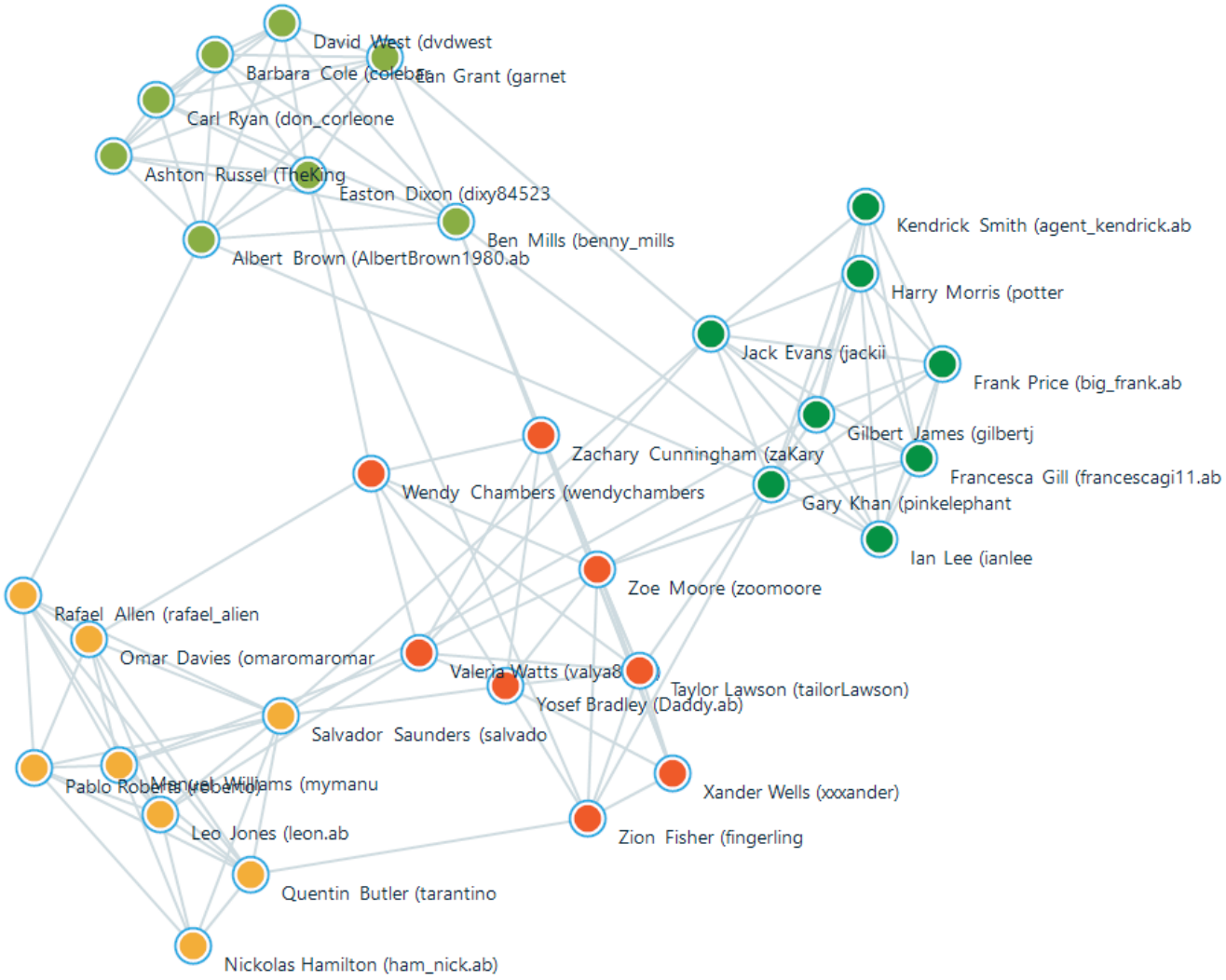
The main pane contains a graphical visualization on how people in your case were communicating. Lines in this graph mean communication occurred in a form of a chat, a call, an SMS, a voicemail or an email, so you can easily see who was talking with whom.
At the top of this window, you can see a separate toolbar, which helps you to configure **Connection Graph** appearance:

There are following items available:

- **Icons** . This button switches the vertex view mode from dots to icons. In icon mode, all contacts or entities are shown using application icon. For example, if communication was performed using Outlook, the Outlook icon will be shown. If multiple apps were used, a blue person icon will be shown (as on the picture below). Besides, since many communication apps are using avatars for a profile owner, Belkasoft X can extract and show these avatars in **Icons** mode.
- **Dots** . This button switches the vertex view mode from icons to dots. Icon view can take a lot of space, especially when avatars are shown; while **Dots** view mode helps to use screen space more efficiently

Note that in both **Icons** and **Dots** modes bigger icon and dot mean more significant person: having more communications and connections than others. You may want to start your investigation with these entities .

- **Detect communities** . This button starts a procedure of detecting groups of tightly connected people, which are called a "communities" in Belkasoft X. A community in this reference consists of people, who probably know each other very well. They also may not know people of another community (or know them not as well as people of the community to which they belong). An example of community could be a group of friends, co-workers sitting in the same room, or a criminal group. Belkasoft X employs a proprietary scientific algorithm of community detection, which is based on how people were communicating with each other. Some forms of communications are valued over others to improve correctness of detection. Once community detection is complete, a colored graph with various colors, as on the picture below will be displayed:

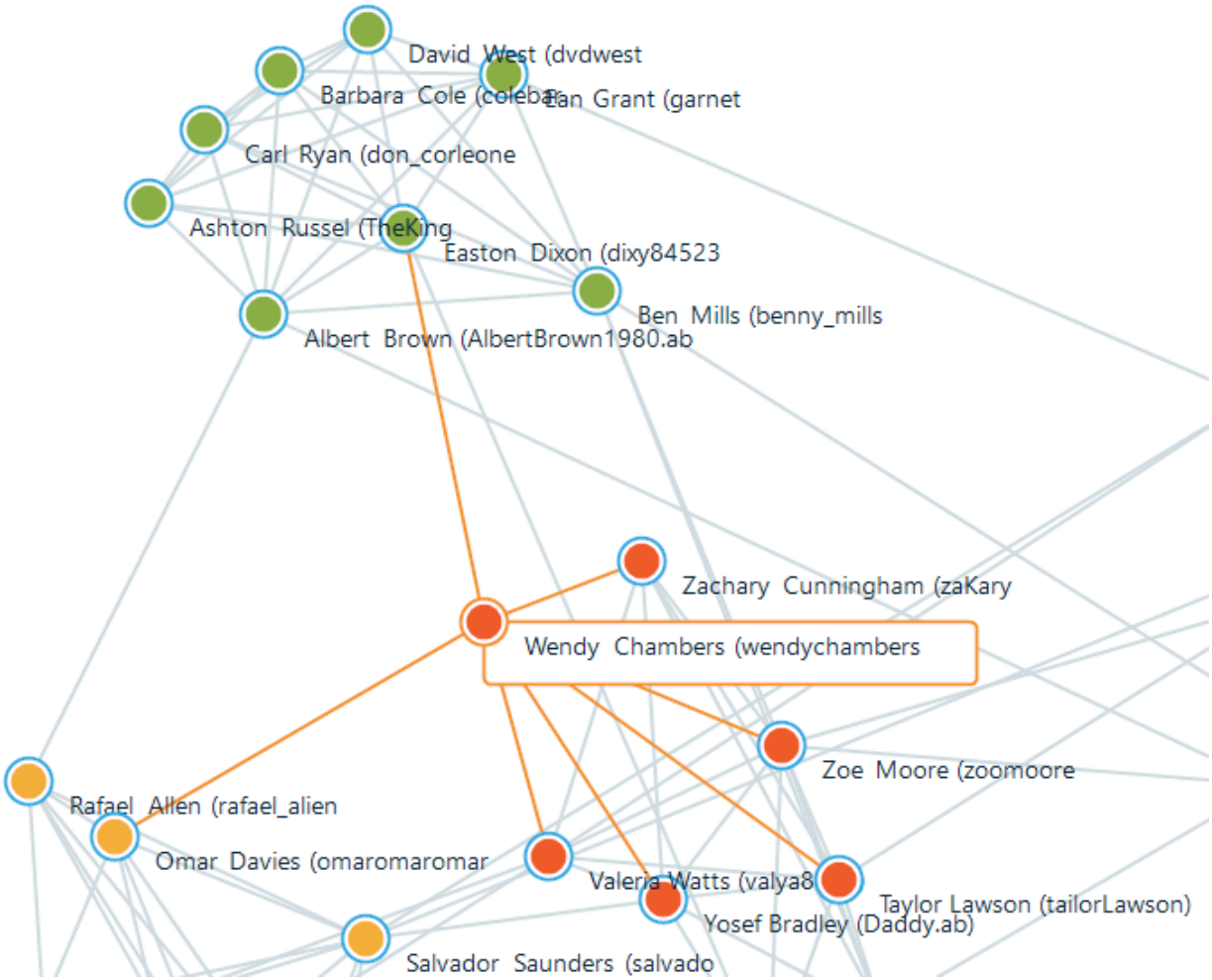


Here you can see four communities

- **Rebuild layout** . If for some reason you do not like the way the graph is currently presented, you can use this button to rearrange it automatically. If communities are detected, Belkasoft X will try to keep community vertices together. You can also drag graph vertices using mouse
- **Show/Hide titles** . This button shows or hides vertices title (corresponding contact or entity name)
- **Add a filter** . Filter the graph by different criteria, such as contacts shown, data source, type of communications, and so on. For more on this, see "Filtering data lists"
- **Filter selected nodes** . This button hides all vertices of the graph except for selected ones, when you wish to focus on just one part of the picture
- **Filter selected nodes and neighbors** . This button hides all vertices except for ones you have previously selected and ones connected to them with an arc (that is, persons, which were in contact with selected ones)

- **Hide selected nodes and neighbors**  . This button hides selected vertices from the graph
- **Entities with less than X communications will be hidden**  **.** This control defines communication threshold, the minimum number of communications an entity needs to have in order to be shown on the Graph pane. By default, it is 0 and all the entities are displayed.

After you filtered (hidden or shown) some vertices of the graph, you can revert to the original picture by resetting corresponding filters. For more this subject, see "Filtering data lists".
Once you have configured the way you would like to see the graph, you can start investigating connections between persons. You can click on any contact or entity in the graph to review its properties. The selected item is highlighted with yellow circle and its properties are shown on the right pane (contact properties pane). When a contact or entity is selected, all its communications are highlighted so you can easily distinguish with whom this entity was communicating:



You can see selected entity (surrounded by the yellow circle) and its connections (lines colored in orange).
If you select a connection, at the right pane you will see both participants and all communications

between them.

Contact or connection properties pane

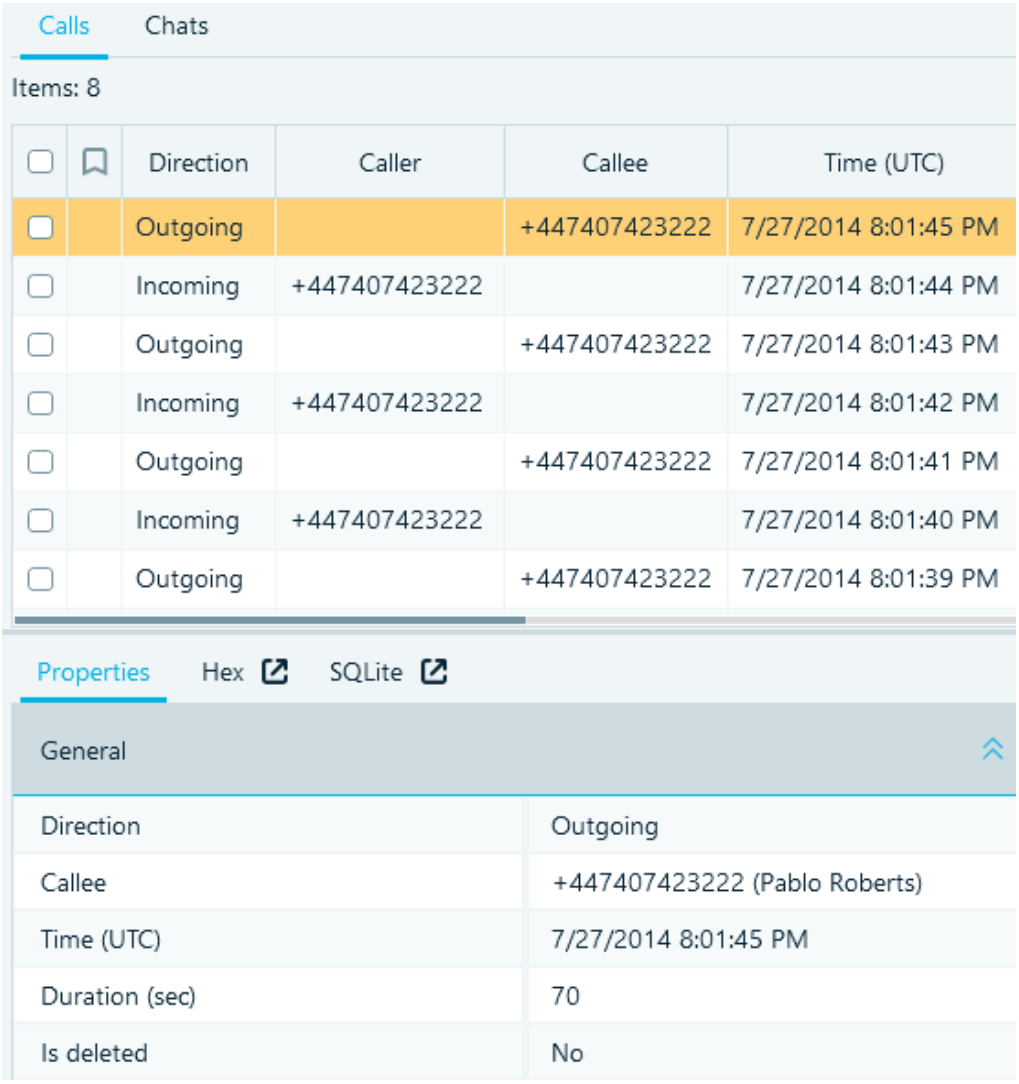
In this pane, situated at the right of the **Connection Graph** window you can see properties of an item selected in the graph pane: entity or connection.

When an entity is selected, this pane will be divided into the following parts:

- Contact list: contacts, with whom this entity is connected
- Contact properties, which shows information about a contact selected in the contact list

If a connection is selected, this pane is divided into the following parts:

- Communication list: a list, which contains actual messages, calls, SMS and other communications between involved parties. Each type of communication has its own tab:

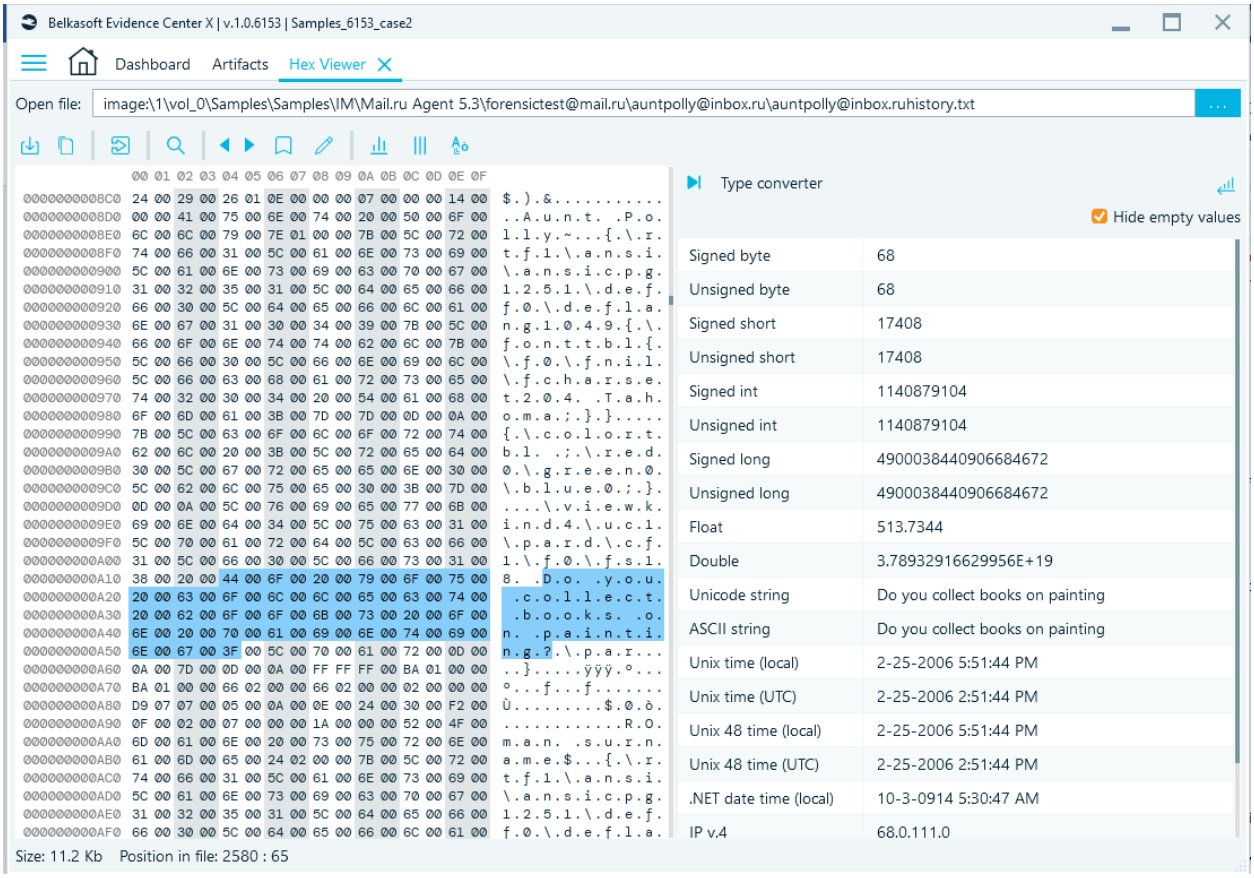


- The pane at the bottom shows selected communication properties as if it were selected in **Artifacts** item list. You will also notice **Hex**, **SQLite** or other relevant viewers here

Hex Viewer

Hex Viewer is used to view or examine the raw constituents of an item—file, process, data source, or even a partition—from a case or standalone file.

Hex Viewer consists of 2 panes: Raw data and Type converter. The Type converter pane may be hidden—click on its toggle to hide/unhide it.



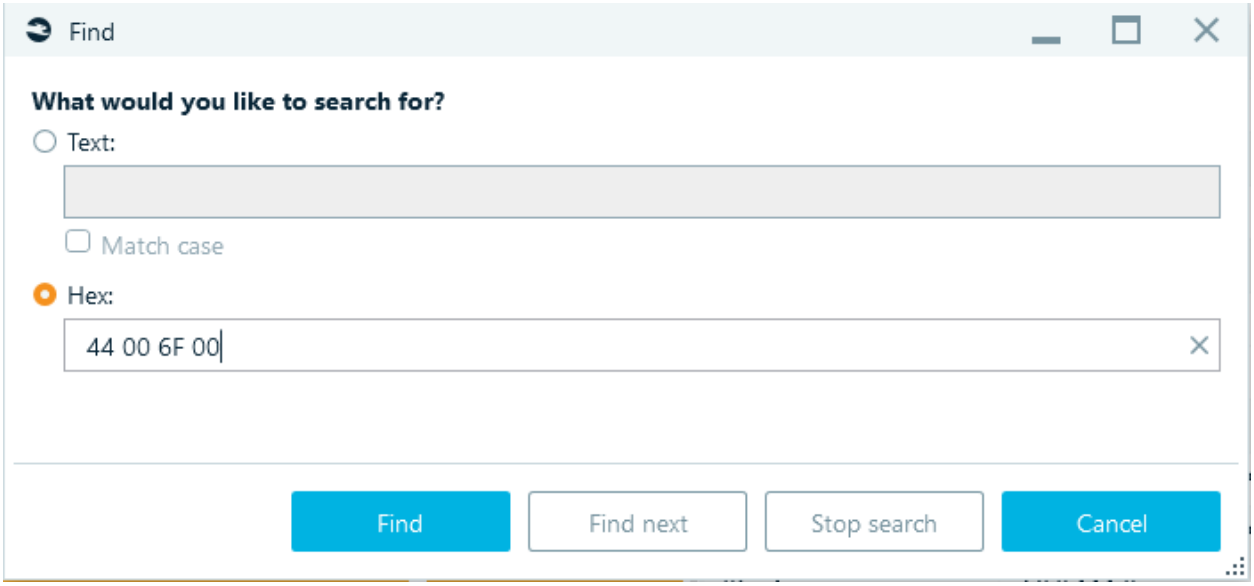
To open a file in **Hex Viewer**, click on the menu bar at the top. Specify the path to the file.

Hex Viewer Toolbar

When a file is open in **Hex Viewer**, Belkasoft X provides these toolbar functions for your use:

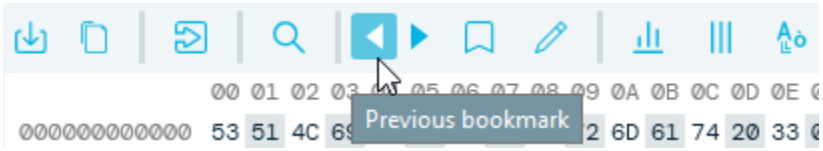
- **Save selection:** Belkasoft X saves the section highlighted on the raw data pane. On the Save as window, give the file a name and choose its format. Click on Save.
- **Copy as hex**: Belkasoft X sends your selection (in hex) to your clipboard. For example, if you highlight ‘Types’ or ‘54 79 70 65 73’ and then use the copy as hex function, Belkasoft X sends ‘54 79 70 65 73’ to your clipboard.
- **Copy as text:** Belkasoft X sends your selection (in text) to your clipboard. For example, if you highlight ‘Types’ or ‘54 79 70 65 73’ and then use the copy as text function, Belkasoft X sends ‘Types’ to your clipboard.

- **Go to:** Belkasoft X navigates to a specific offset in the presented data. On the Go to window, type in the figure, specify the numeral system, specify the offset position, click on OK.
- **Search:** Belkasoft X searches for a keyword. On the **Find** window, type in the keyword, tick the Match case checkbox—if you want the search to be case sensitive. Or you can search for hex.

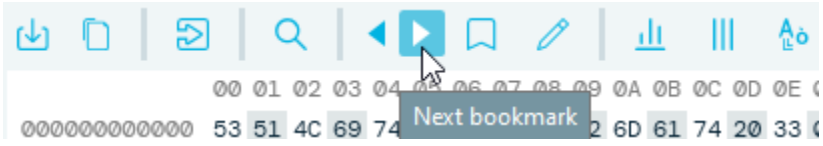


When you click on **Find**, Belkasoft X presents the first match for the keyword or hex.
Note: The search operation may take some time to complete.
When you click on **Find next**, Belkasoft X presents the second match, and so on (in that order).
To terminate the search operation, click on **Stop search.**

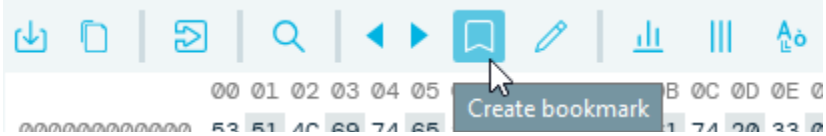
- **Previous bookmark:** Belkasoft X navigates to the previous bookmark.



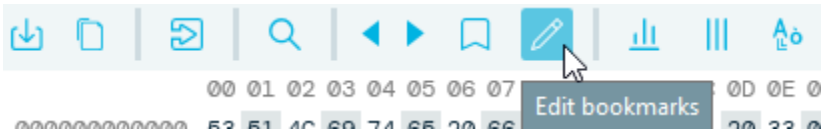
- **Next bookmark**: Belkasoft X navigates to the next bookmark.



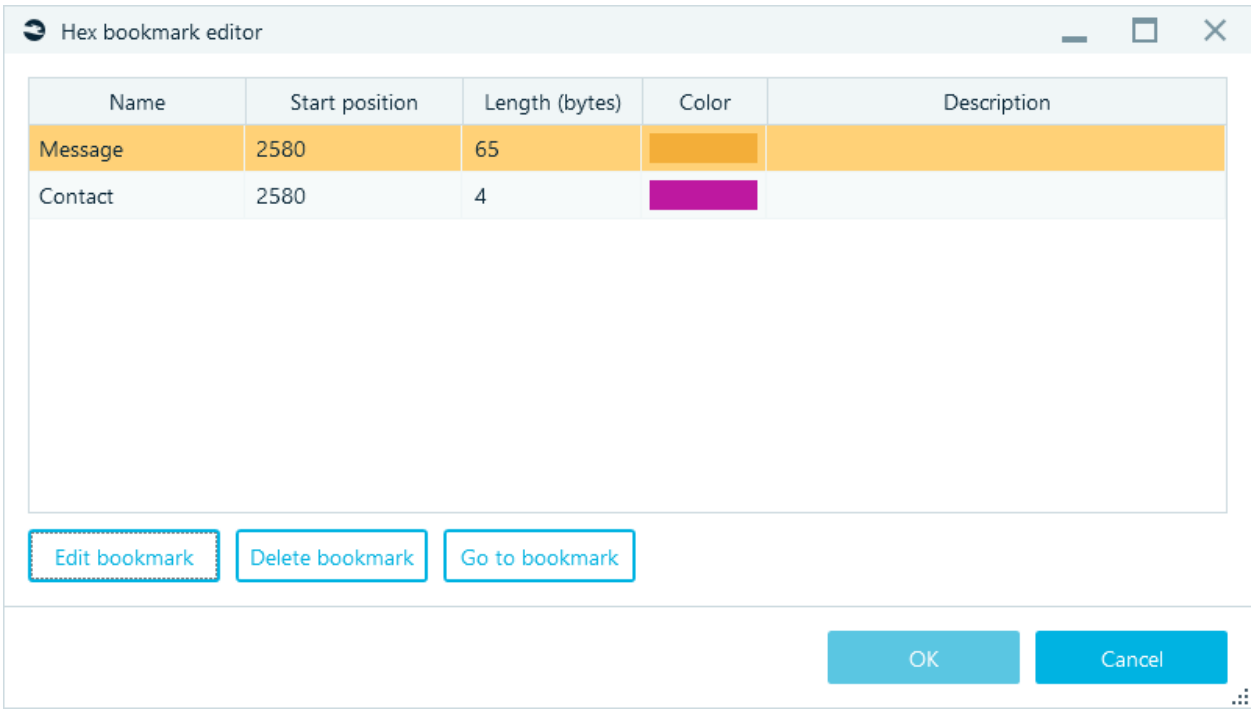
- **Create bookmark:** Belkasoft X lets you to highlight a bookmarked item.



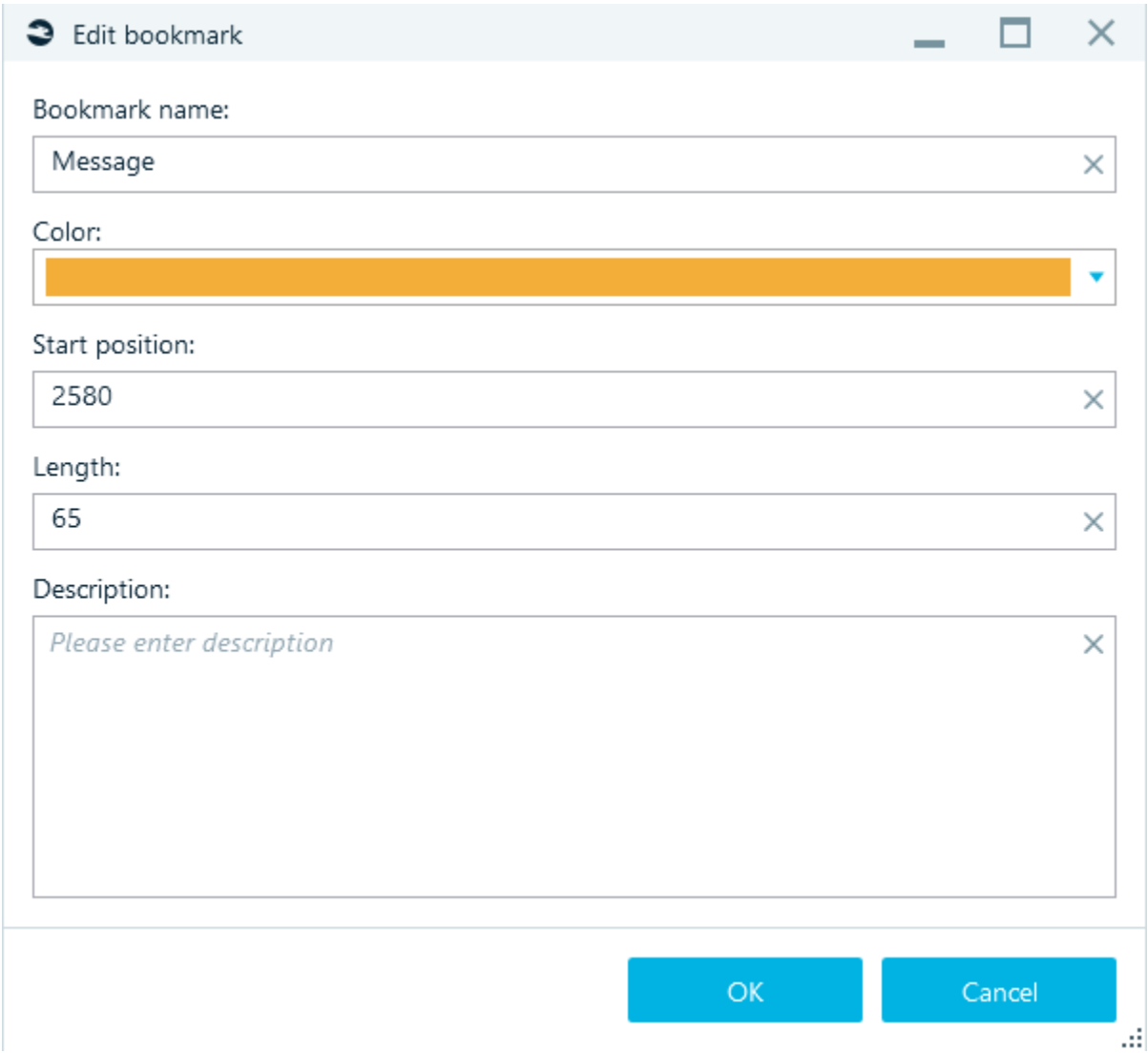
- **Edit bookmark**: Belkasoft X displays **Hex Bookmark Editor**.



Hex Bookmark Editor. Here you can edit, delete, and navigate to bookmarks on this window. Simply click on a bookmark and then click on an action (Edit bookmark, Delete bookmark, or Go to bookmark).



  - ***Edit bookmark*.** You can give the bookmark a name, change its color, modify its start position and length, and provide a description. These details may help you better identify or locate the bookmark.



  - ***Delete bookmark.*** Belkasoft X removes the color on the selection.
  - ***Go to bookmark*.** Belkasoft X takes you to the bookmark's position.
- **Bytes per row:** Specify the number of bytes you want Belkasoft X to show on a row.
- **Bytes per group:** Specify the number of bytes you want Belkasoft X to show in a group.
- **Change encoding:** Specify your preferred encoding. Click on **Additional encodings** to see more encoding options.

Raw data

When you click on a byte, Belkasoft X states the position of the byte in the file at the bottom of the raw data pane. When you highlight a section, Belkasoft X states the position of the first byte (in the selection) and the number of highlighted bytes.

When you highlight a section on the raw data pane, Belkasoft X displays the corresponding details for the highlighted section on the type converter pane.

The Raw data pane contain the Size and Position in the file.

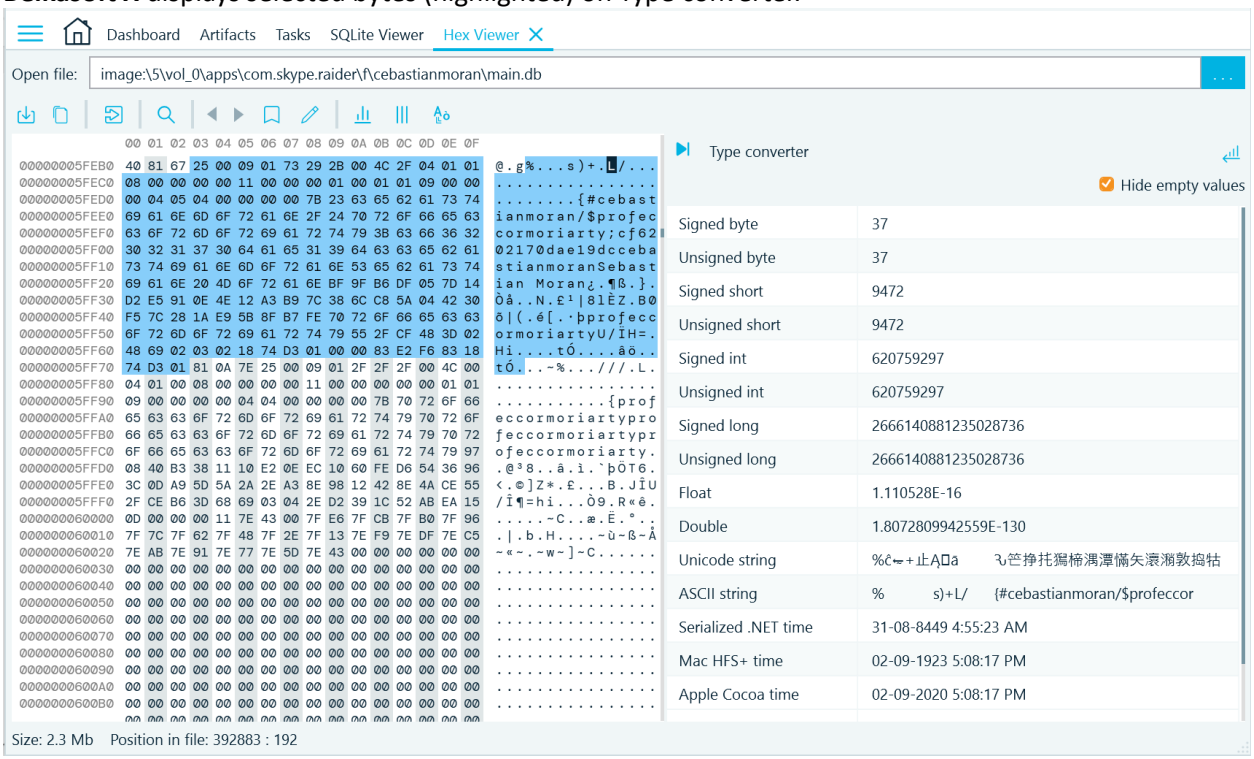
Raw data context menu

When you right-click on an object or select on the raw data pane

- **Copy as text**
- **Copy as hex**
- **Selection**: Belkasoft X provides these actions for selections:
    - **Select all**: Belkasoft X highlights everything
    - **Deselect:** Belkasoft X deselects the highlighted section
    - **Go to selection start:** Belkasoft X takes you to the start of the selection
    - **Go to selection end:** Belkasoft X takes you to the end of the selection
    - **Save selection**: Belkasoft X saves the selection. On the Save as window, type in a name, specify the file format, click on OK.

Type converter

Belkasoft X displays selected bytes (highlighted) on Type converter.

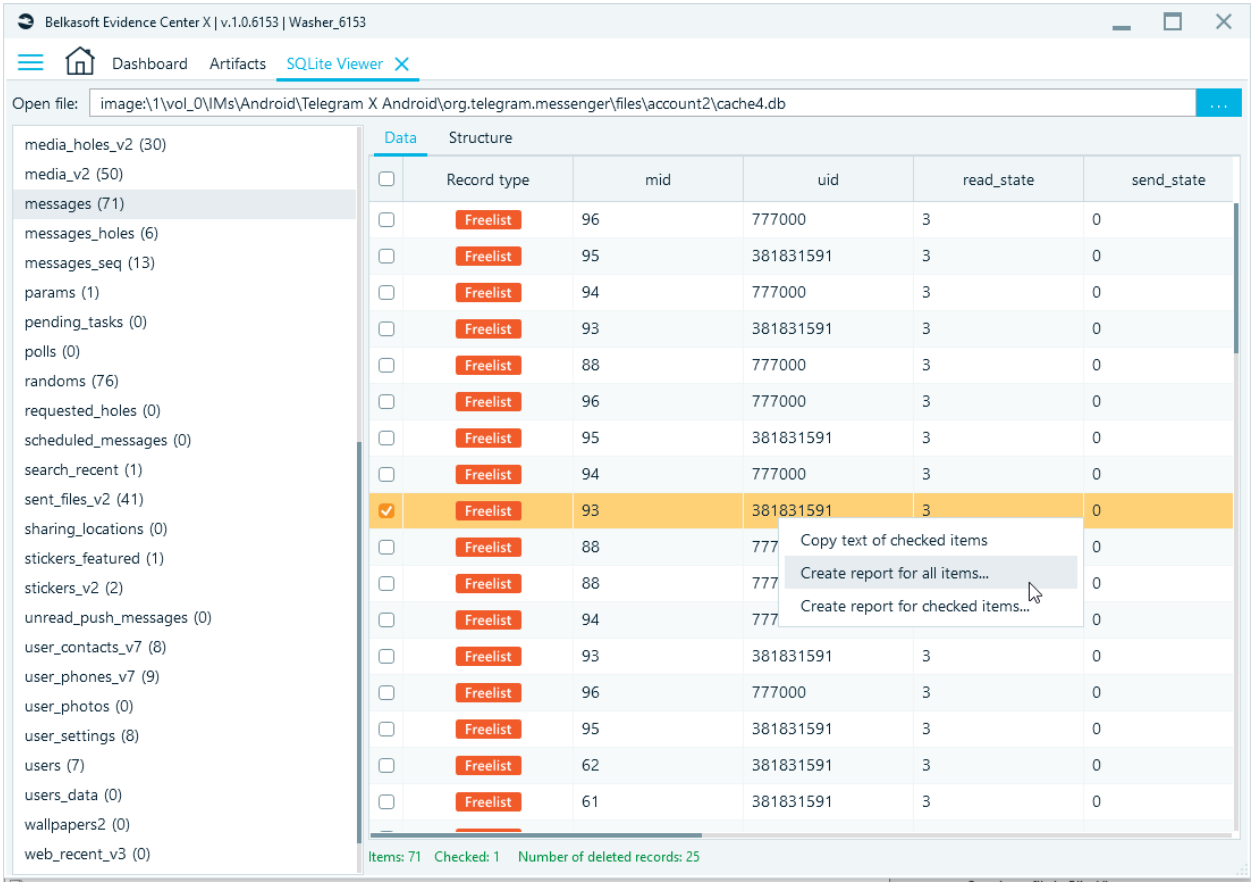


You get to see interpretations of the bytes and figure out what the selected parts of a file mean. For example, when examining a file with an unknown structure, you may infer that an IP address exists inside the file. In that case, you can find the address through the raw data and type converter pane. Depending on your selection, the Type converter displays these fields and their values: Signed byte, Unsigned byte, Signed short, Unsigned short, Float, Double, Unicode, string, ASCII string, IPv4, IPv6, and many others.

- **Hide empty values**: Belkasoft X shows only the types that matches the selected bytes. If you do not want to see fields with empty values, tick the Hide empty values checkbox.
- **Little and big endian:** Belkasoft X switches to another sequence. To switch between little endian and big endian, click on the toggle at the top-right corner.

SQLite Viewer

SQLite Viewer is used to examine SQLite databases from a case or standalone file.



To open a file in **SQLite Viewer**, click on the menu button at the top of the window, specify the path to the SQLite database file, and then click on **Open**.

SQLite Viewer has 2 panes: Table list (left pane) and Table data (right pane).

When you click on an item (usually a table) under Table list, Belkasoft X displays the constituents of the table under Table data.

Table list

Under Table list, Belkasoft X displays all the tables inside the SQLite file. Belkasoft X sorts the tables alphabetically. The figure in parenthesis is the number of rows in the table.

The last row of the table—an artificial row at the bottom—is termed ‘Unallocated space’. Hence, it contains 0 records. If you click on this pseudo-table, Belkasoft X shows the SQLite unallocated space records, including carved data.

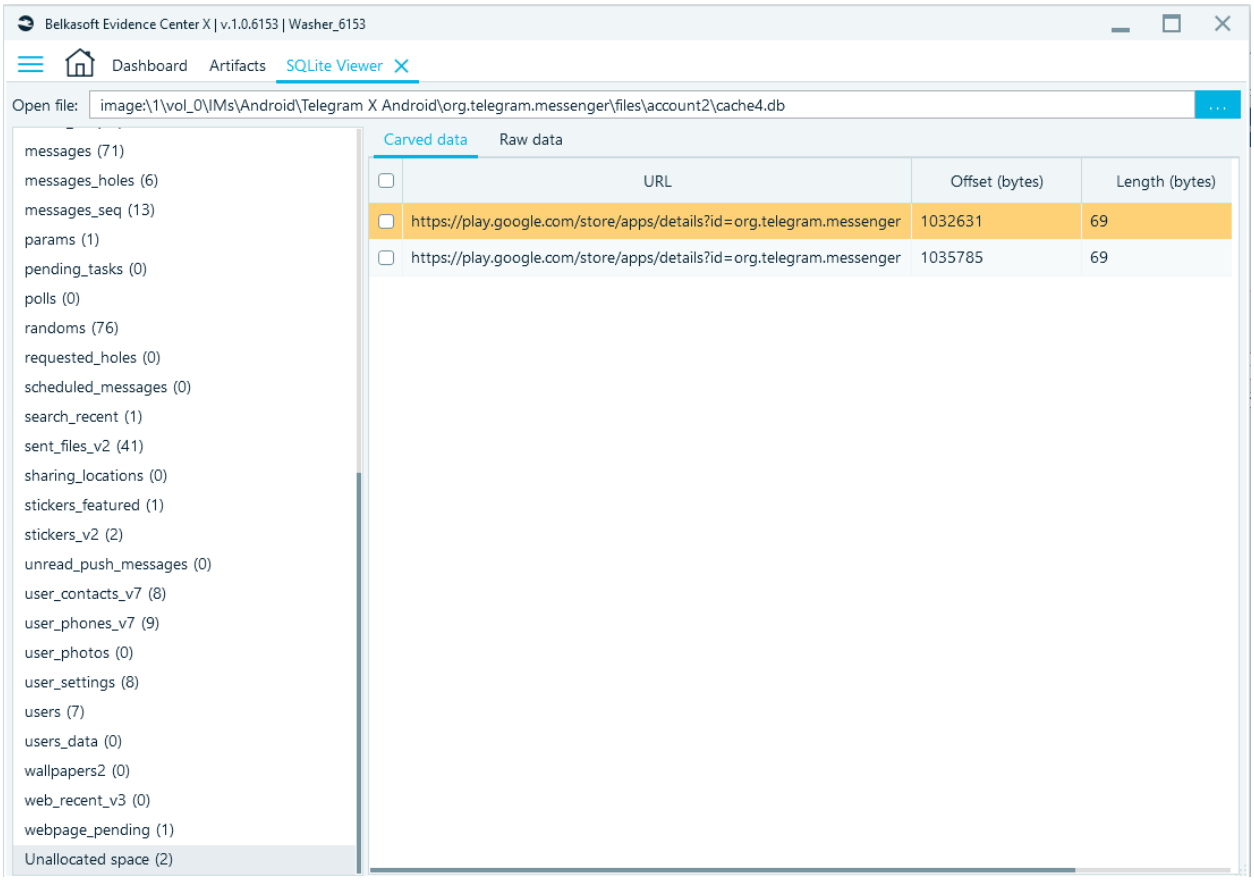


Table data

Table data has 2 tabs: **Data** and **Structure**. Under **Data** Belkasoft X displays the records inside the selected database table. Under **Structure**, Belkasoft X displays the columns and the types of columns in the selected table. You should see these fields and their values: ID, Column name, Type, Default value, Not null, and others.

Data context menu

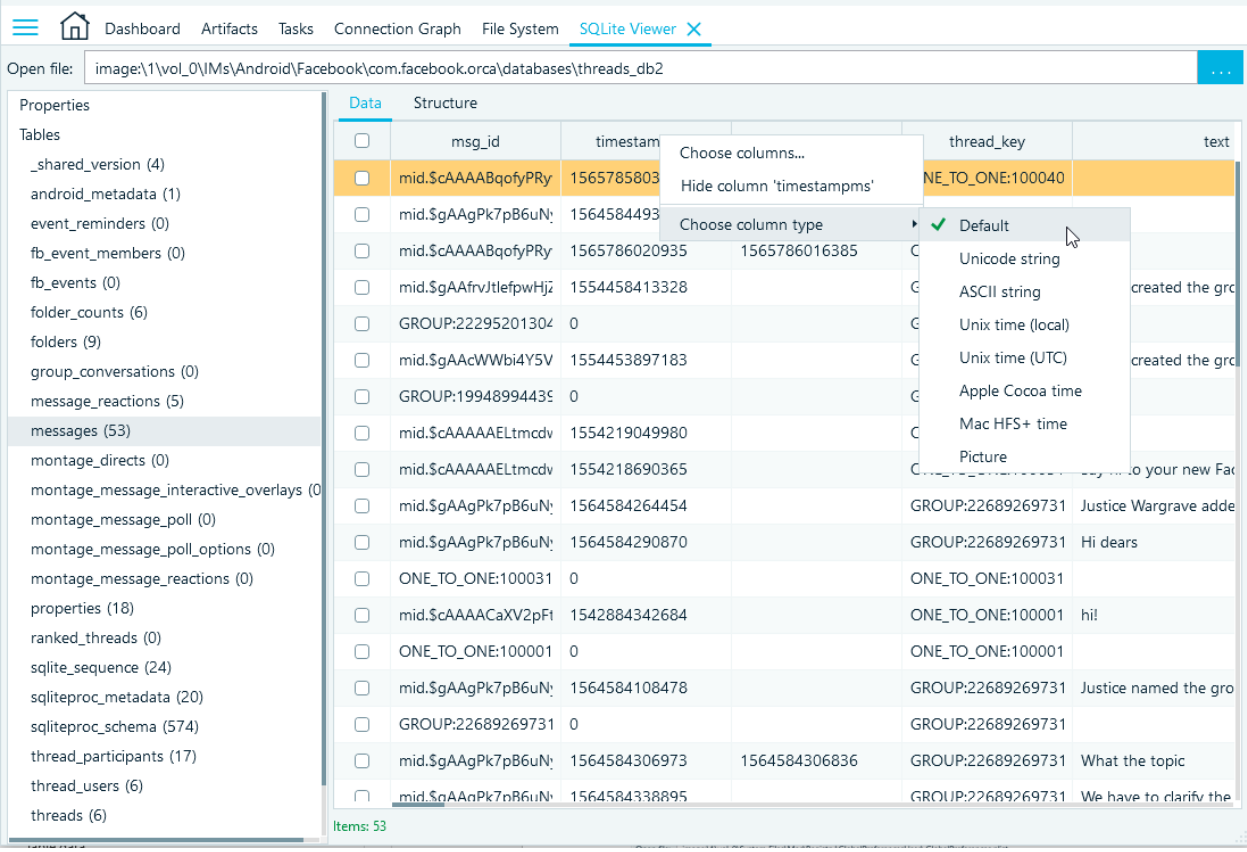
- **Copy text of checked item**
- **Create report for all items**
- **Create report for checked items**
- **Choose columns (for table header).** By default, Belkasoft X displays all table columns.

If you want Belkasoft X to display only certain columns, right-click on any spot under **Data**, and then select **Choose columns**. On the **Choose columns** window, use the navigation buttons to move columns between the **Available columns** and **Selected columns** boxes. Under **Available columns**, Belkasoft X lists all the columns existing inside the database table. Under **Selected columns**, Belkasoft X lists the columns it is set to display.

Table context menu

- **Choose columns**
- **Hide column**

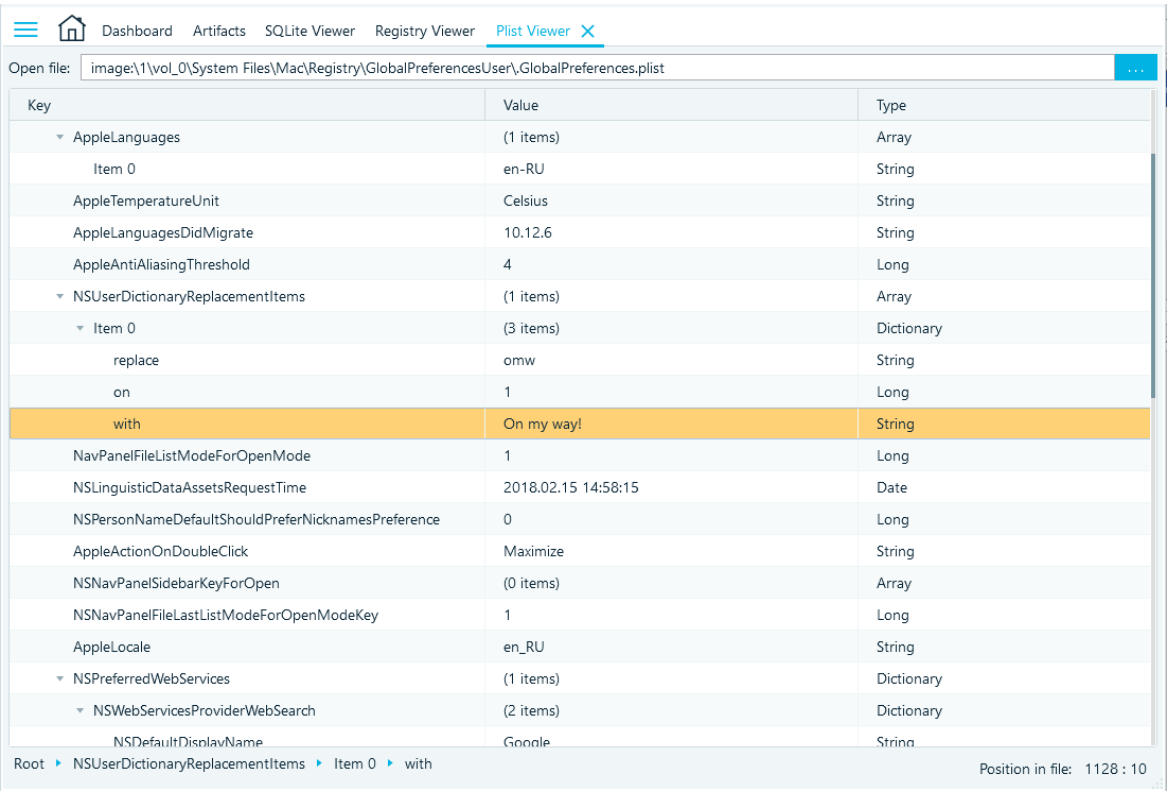
- **Choose column type**
  - Default
  - Unicode string
  - ASCII string
  - Unix time (local)
  - Unix time (UTC)
  - Apple Cocoa time
  - Mac HFS+ time
  - Picture



For example, if by default the values are presented in a **UNIX timestamp**, then all values in the table can be immediately converted to a human date (local/UTC). This menu item is shown for all columns but applies to time or blob values.

Plist Viewer

On the **Plist Viewer tab**, you can examine PLIST (Property List) files. PLIST files are used mostly in Apple's ecosystem (macOS and iOS).



To open a file in **Plist Viewer**, click on the menu at the top of the window, specify the path to the Plist file, and then click on **Open**.
Plist Viewer provides 3 columns: Key, Value, and Type.

- **Key -** the name of a node
- **Value**
- **Type -** the type of the node (if it is for a leaf) or Array/Dictionary (if it is for a parent node)

At the bottom of the **Plist Viewer** window:

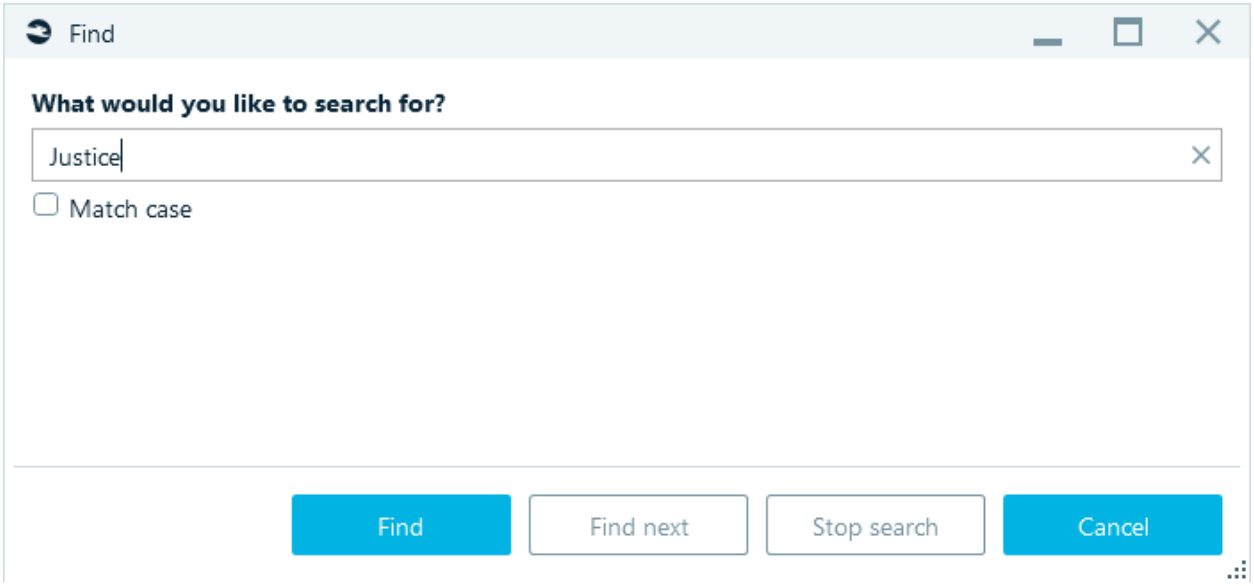
- Belkasoft X specifies the path (navigation) to the currently highlighted node. The path is the direction from the root folder to the selected node
- Belkasoft X specifies the selected object position in the Plist file

Belkasoft X denotes delimitation for nodes with the symbol. You can expand a node by clicking on that symbol. You can also click on a node name to navigate to the corresponding node.

Plist Viewer context menu

- **Copy key:** Belkasoft X copies the key's name to your clipboard.
- **Copy value:** Belkasoft X copies the key's value to your clipboard.
- **Copy row:** Belkasoft X copies the key's name, value, and array to your clipboard.
- **Copy as Plist:** Belkasoft X copies the selected node and its children as a Plist to your clipboard.
- **Save as XML:** Belkasoft X brings up the Save as window. Input a name for the file, specify the format (Plist, XML, or All files) in which you want Belkasoft X to save the file, and then click on OK.
- **Expand Children:** Belkasoft X expands the selected node to show its contents.

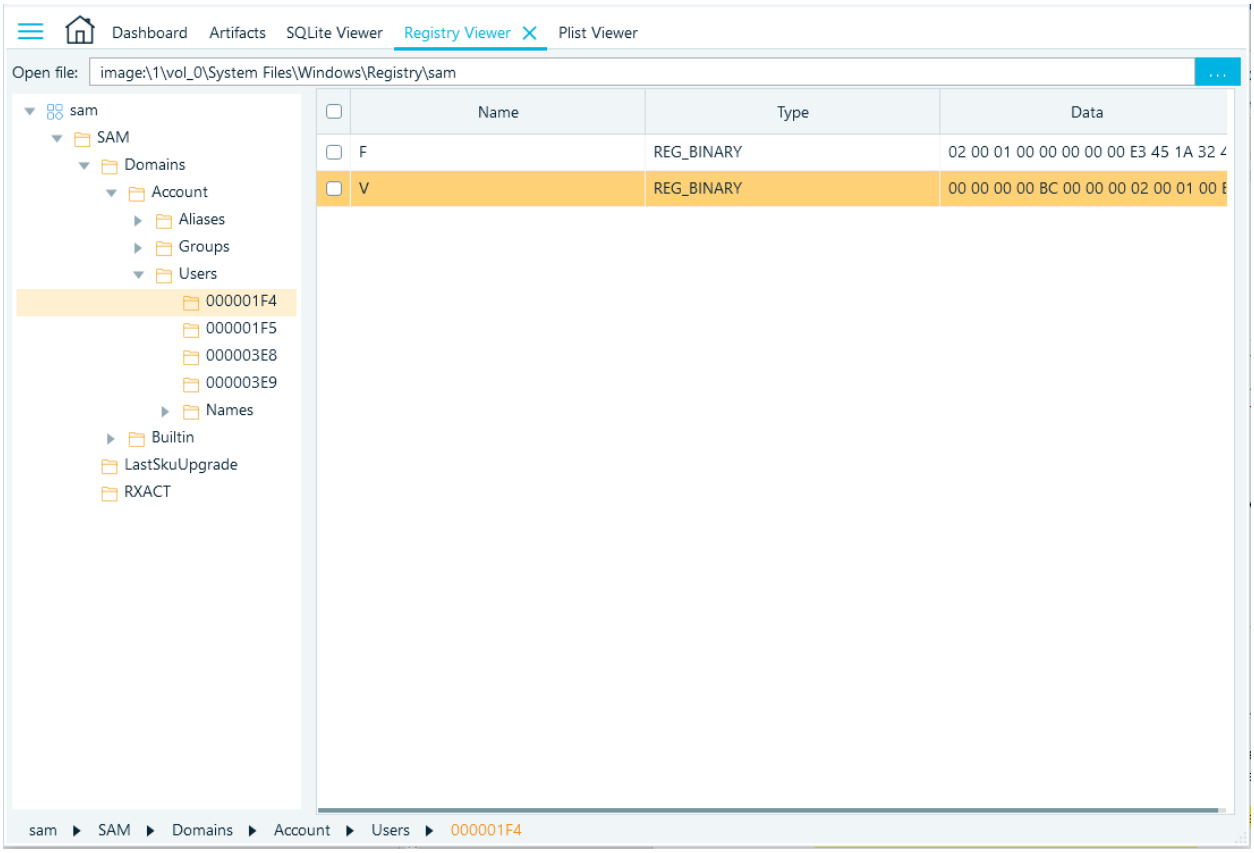
- **Collapse Children:** Belkasoft X collapses the selected node to hide its contents.
- **Find** (ctrl+F): Belkasoft X brings up the **Find** window. Input a keyword and tick the **Match case** checkbox if you want to run a case sensitive search.



- **Find Next:** In a search operation, Belkasoft X navigates to the next search result.

Registry Viewer

On the **Registry Viewer** tab, you can examine Windows registry files such as NTUSER.DAT files, SAM, software, system, and others from your case, or a standalone registry file on your host machine.



To open a file in **Registry Viewer**, click on the menu icon at the top of the window, specify the path to the registry file, and then click on OK.

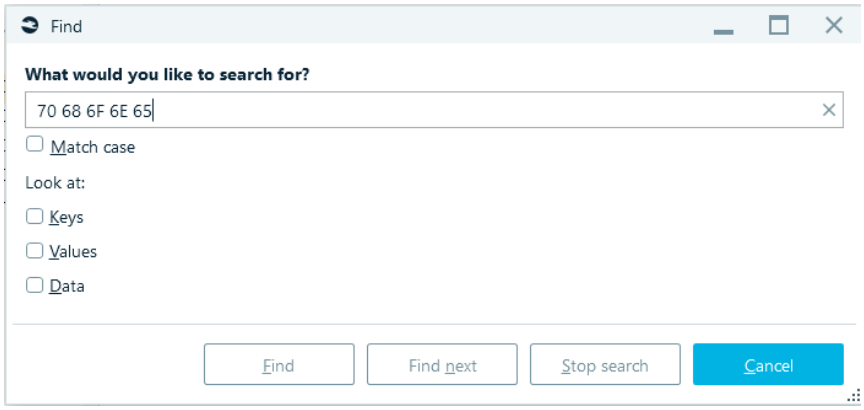
- On left pane, Belkasoft X displays the registry structure.
- On the right pane, Belkasoft X displays the contents of the selected registry key (if it contains values) under the **Name**, **Type**, and **Data** fields.
- On the bottom, Belkasoft X displays the path (navigation) to the currently selected object.

To expand a key, click on the expansion icon.

Registry Viewer context menu

- **Copy name:** Belkasoft X copies the value's name to your clipboard.
- **Copy data:** Belkasoft X copies the value's data to your clipboard.
- **Copy type:** Belkasoft X copies the value's type to your clipboard.
- **Copy item text:** Belkasoft X copies the value's name, type, and data to your clipboard.
- **Create report:** Belkasoft X brings up the Create Report window to allow you create a report for the chosen item. Specify the necessary parameters to create the report. For more on this subject, see the Report topic.

- **Create report for selected items:** Belkasoft X brings up the **Create Report** window to allow you create a report for the chosen items. Specify the necessary parameters to create the report. For more on this subject, see the Report topic.
- **Find** (ctrl+F)**:** Belkasoft X brings up the **Find** window to allow you search for something. Input the keyword. Tick the checkbox for Match case—if you want to run a case sensitive search. Tick the checkbox for Keys, Values, and Data—if you want Belkasoft X to run a search for specific objects or files.



- **Choose columns (for table header)**: Belkasoft X brings up the **Choose column** window to allow you specify the columns you want to see. Use the navigation buttons to move items between the Available columns and Selected Columns box.

Bookmarks

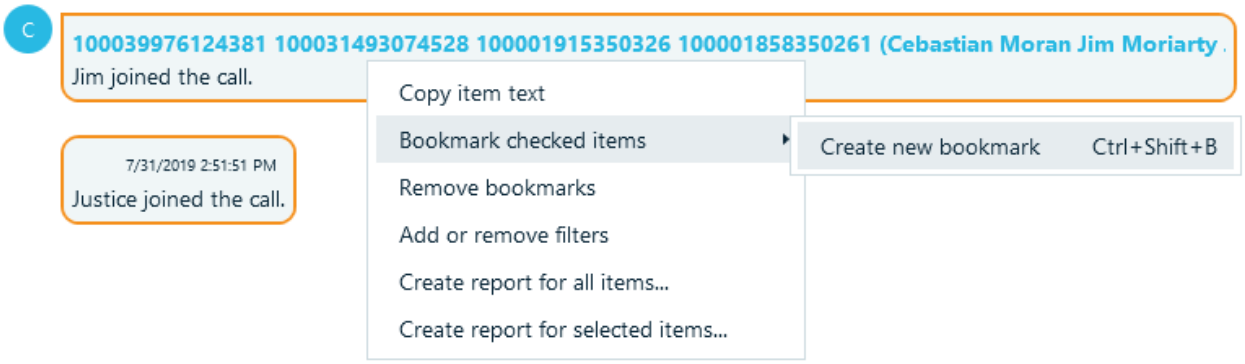
Belkasoft X allows you to create bookmarks for almost all artifacts or objects—such as an email, chat, contact, geolocation, or even a registry setting—presented after analysis under the **Artifacts** tab. For example, Belkasoft X highlights bookmarked artifacts with colors to help you to find and recognize them easily.

However, you cannot create bookmarks for these items: a file under the **File System** tab, an SQLite record under **SQLite Viewer**, a registry setting under **Registry Viewer**, and similar objects in those locations.

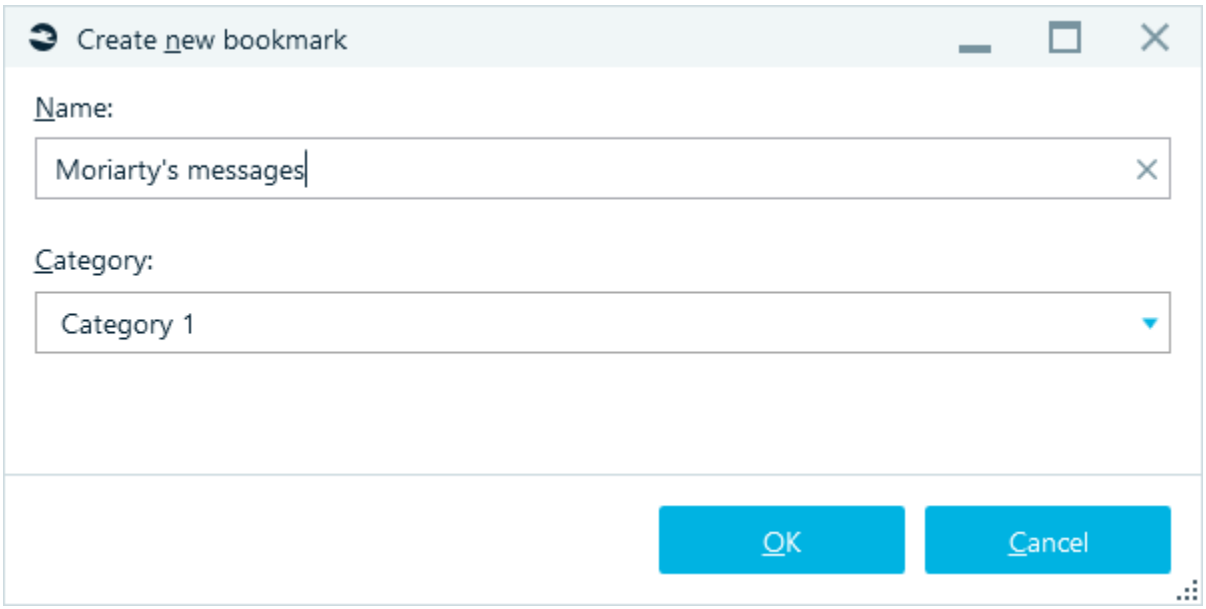
Creating a new bookmark

In order to create a new bookmark, check one or multiple artifacts in any artifact list, for example, list inside **Artifacts**, **Connection Graph**, **Search Results**, or other windows, which show a list of artifacts. When you have all artifacts selected, you can:

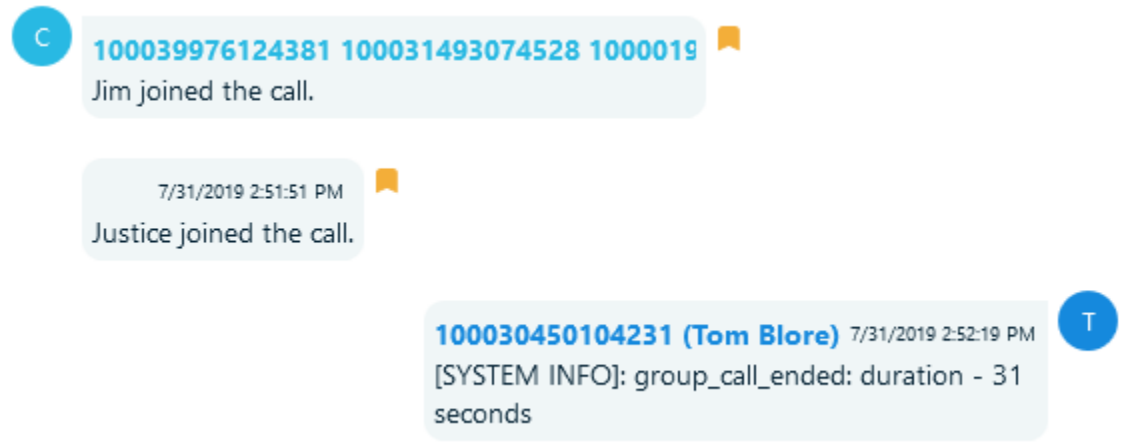
- Press **Ctrl-Shift-B** key combination or
- Right click, select **Bookmark checked items** context menu item and then **Create new bookmark** submenu:



On the **Create new bookmark** window, input a name and specify the category for the bookmark. Click on the **OK** button.



Bookmarked items are marked with a colored bookmark flag. The flag color depends on the bookmark category.

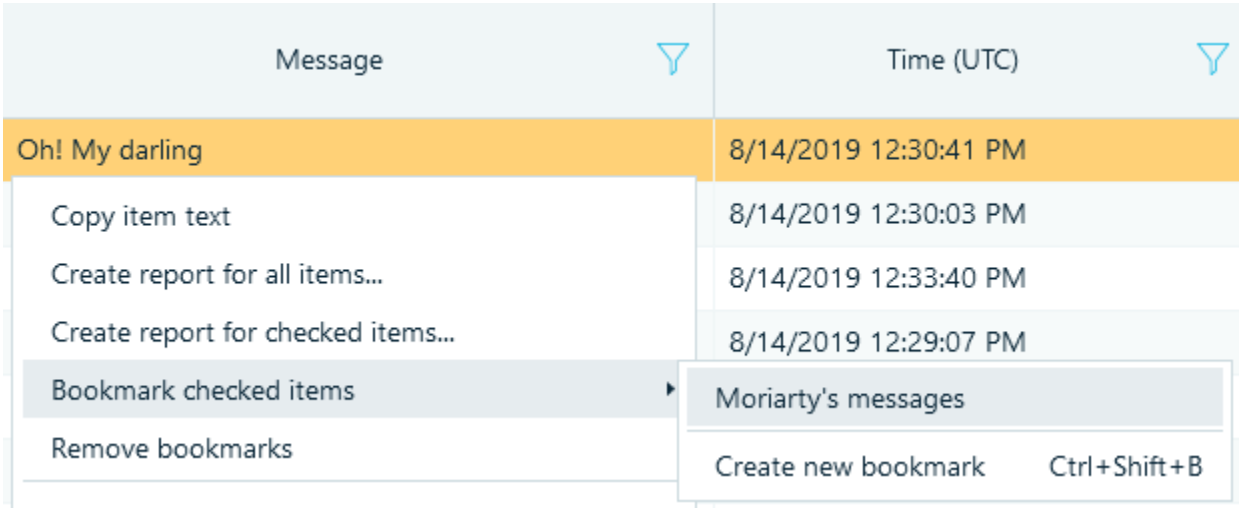


You could also use hot keys to bookmark selected artifacts by categories (see **Settings** -> Bookmarks).

Adding an artifact to an existing bookmark

Once you have created one or multiple bookmarks, you can add more items to any existing bookmark. To do so,

- Press **Ctrl-B** key combination. This will add checked artifacts to the last bookmark you created.
- Right click, select **Bookmark checked items** context menu item and then any existing bookmark from the list (see "Suspicious chats" bookmark on the screenshot below):



Note: Do not confuse artifact bookmarks with those in **Hex Viewer.** Hex viewer has its own bookmarks for a group of bytes. See "Hex Viewer" chapter for more.

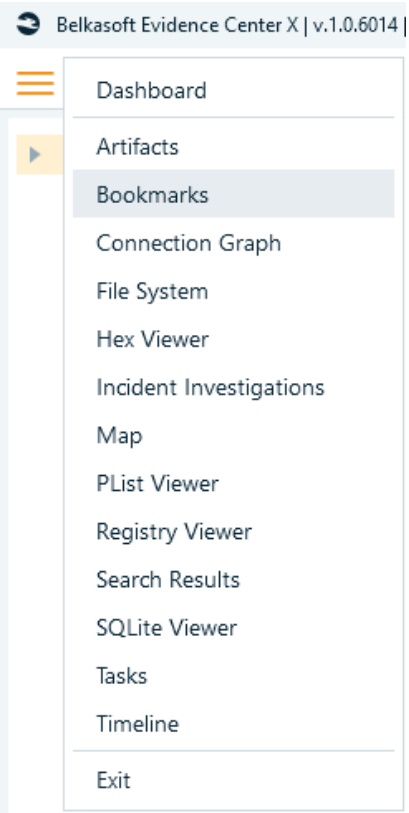
Complex items bookmarking

When you bookmark an item, which was originated from another item, for example, a picture from email attachment, both these items are bookmarked, child and parent. This is useful, when you first look for some specific content (for instance, pictures with guns) and then need to investigate where these items came from (chats, emails, documents and so on).

Bookmarks window

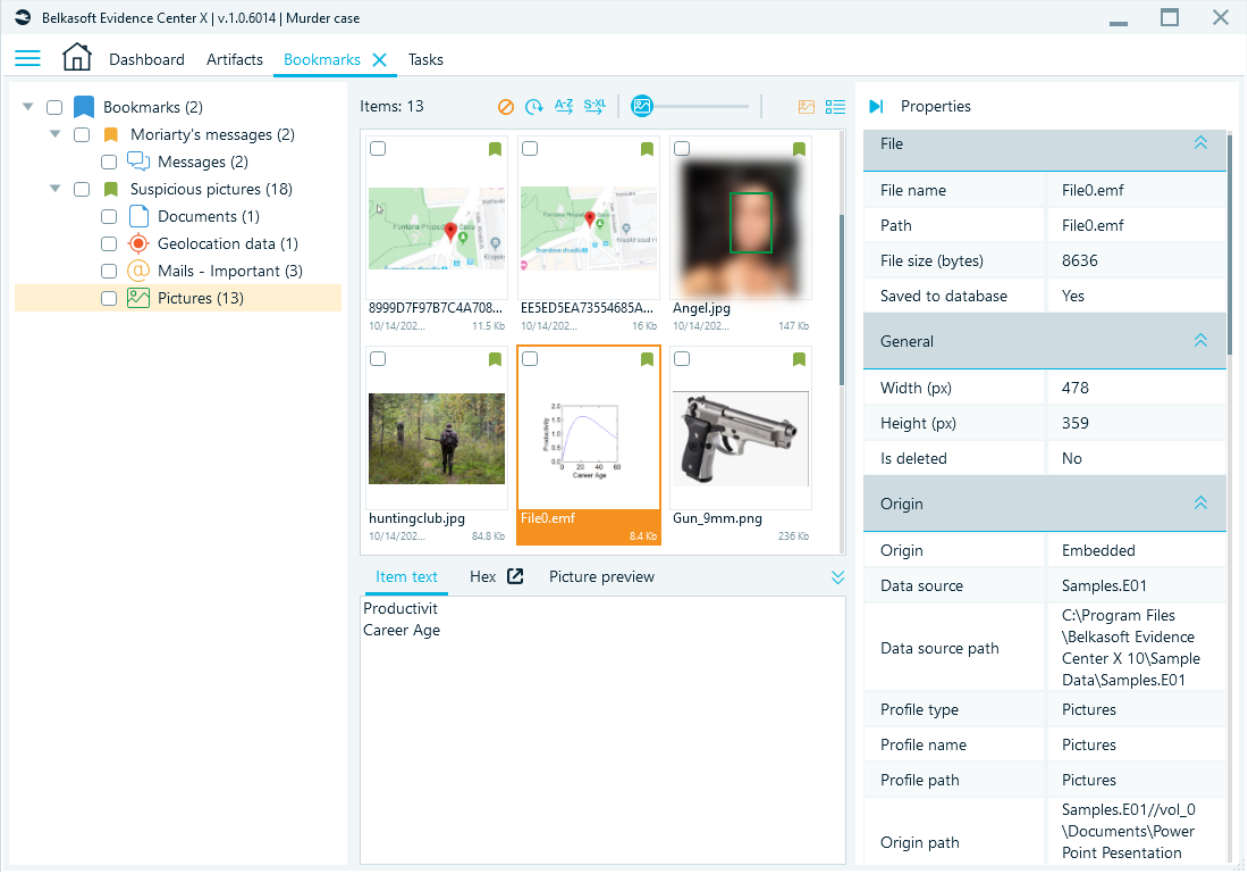
On the **Bookmarks** tab, Belkasoft X displays the bookmarks you created for artifacts at regular locations (for example, under the **Artifacts** tab). On **Bookmarks**, you can examine bookmarks (in depth), edit them, and also delete them.

You can open **Bookmarks** window by using **Bookmarks** main menu item.



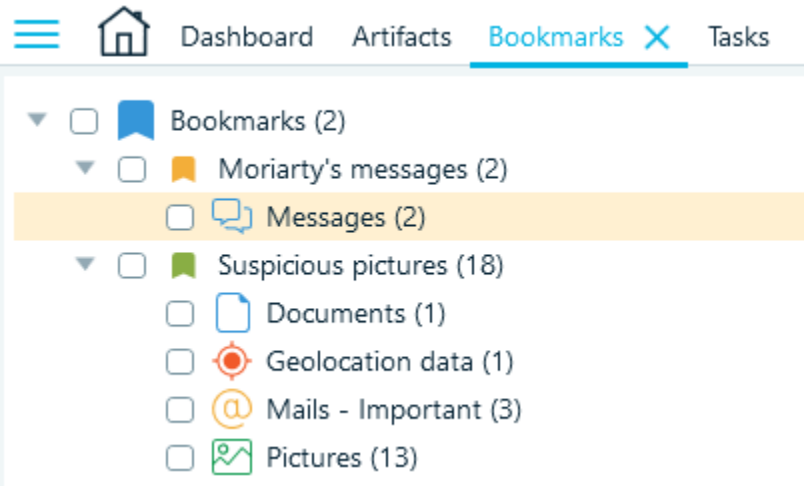
Bookmarks window consists of following parts:

- Bookmarks pane (at the left).
- Bookmarked artifacts list (at the top right).
- Selected artifact details (at the bottom right), to include full text, raw data and SQLite data, if applicable.
- Selected artifact properties (at the right).



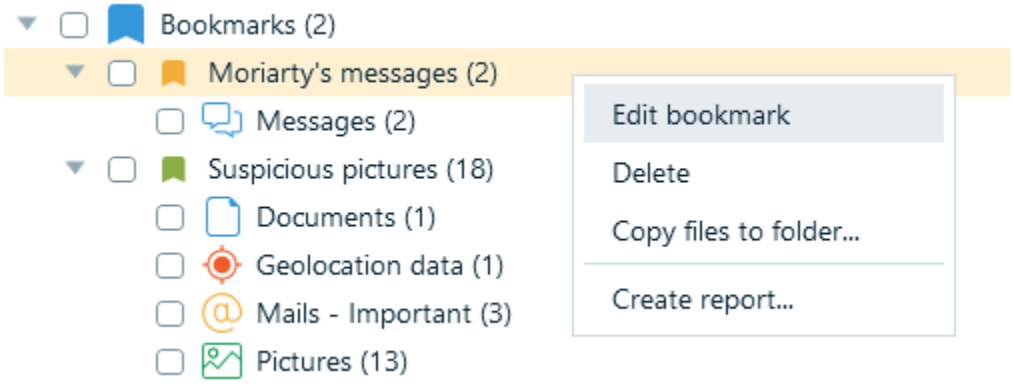
Bookmarks pane

At the top of this pane, you can see **Bookmarks** node followed by the number of bookmarks in parenthesis. Child nodes of this parent node are bookmarks, each are followed by the number of bookmarked artifacts in parenthesis. Also, under any bookmark node there are artifact types, such as Instant Messengers, Mailboxes, Pictures, and so forth. Note that a bookmark can contain multiple items and can contain items of different types:

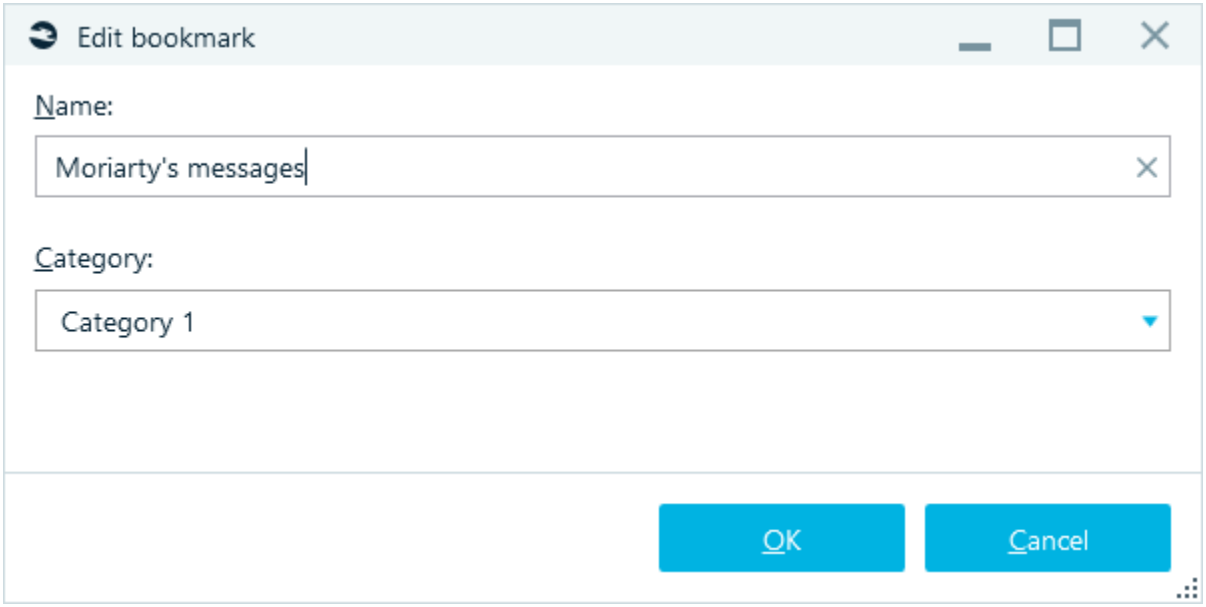


If you right click on a bookmark, a context menu will be opened with the following items:

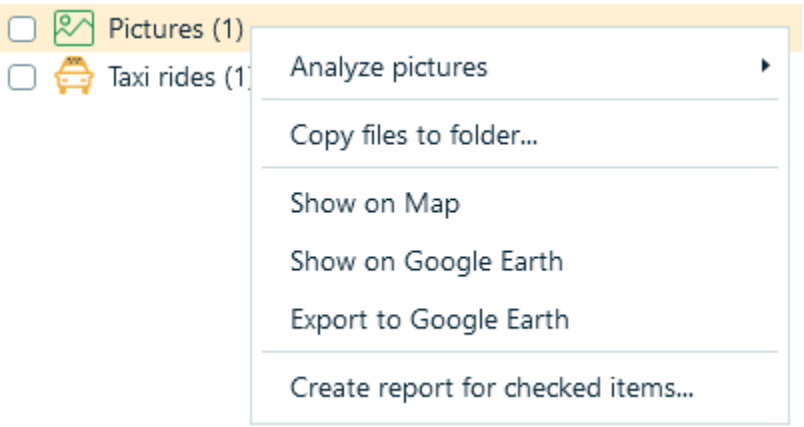
- **Edit bookmark.** Belkasoft X brings up the Edit bookmark window to allow you make changes to the selected bookmark.
- **Copy files to folder…** This menu item will copy all bookmarked files (if any) to a selected folder on your host machine. This is useful when you are bookmarking documents, pictures or other file-based artifacts.
- **Create report…** This menu will create a report for a selected bookmark (or all bookmarks being chosen for the top-level node). Note that since a bookmark can contain artifacts of different types, several report files may be created.
- **Delete**. This menu will delete a chosen bookmark, effectively un-bookmarking all previously bookmarked artifacts.



The **Edit bookmark** allows you to change the bookmark name and/or to change the category for the bookmark.



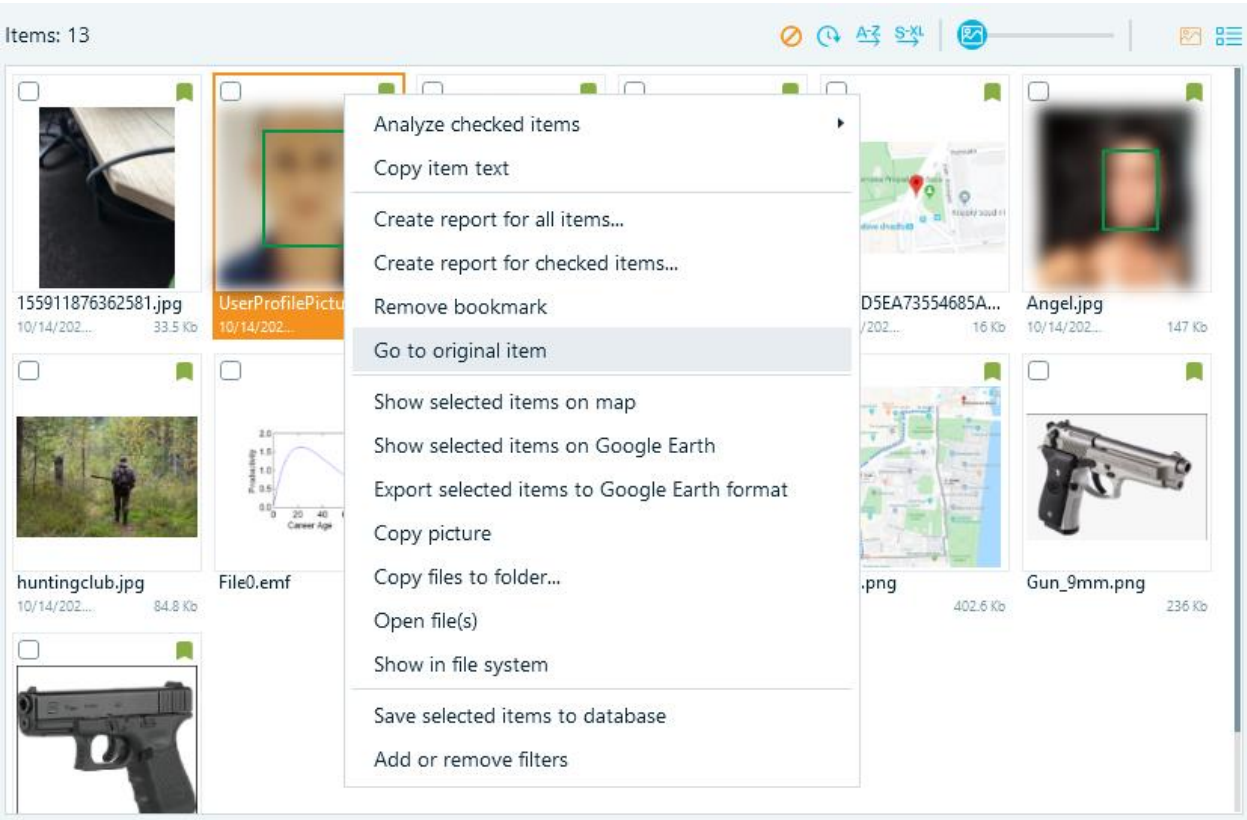
If you right click on an artifact type, a specific context menu will be opened. Its content will depend on the selected artifact type and might contain such menu items as **Analyze pictures**, **Show on Map**, etc.



Bookmarked artifacts list

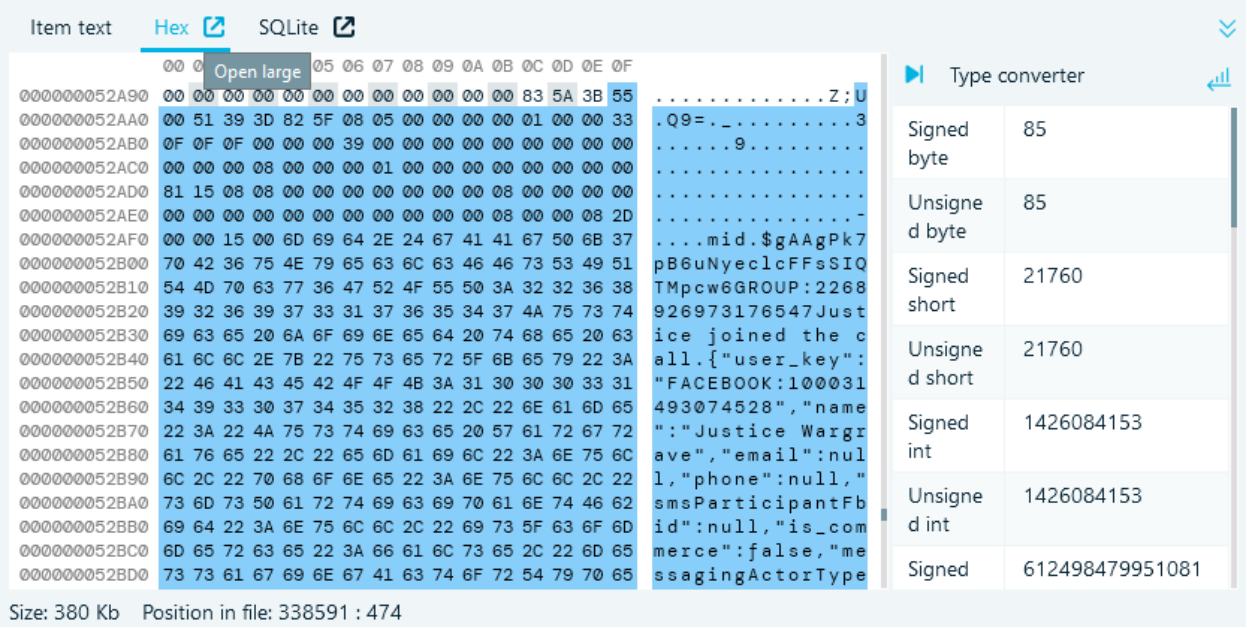
This list shows all artifacts, which belong to a bookmark, selected in the bookmarks pane. This list works the same as an artifact list in **Artifacts** and has the same context menu items but there are also two specific context menu items:

- **Remove bookmark**. This menu item will remove checked artifacts from a bookmark. Note that you can also remove an artifact from all bookmarks using **Remove bookmarks** context menu item inside **Artifacts.**
- **Go to original item**. This menu helps you to find an original artifact. Once selected, it will navigate you to the corresponding profile in **Artifacts**, bookmarked artifact will be selected.



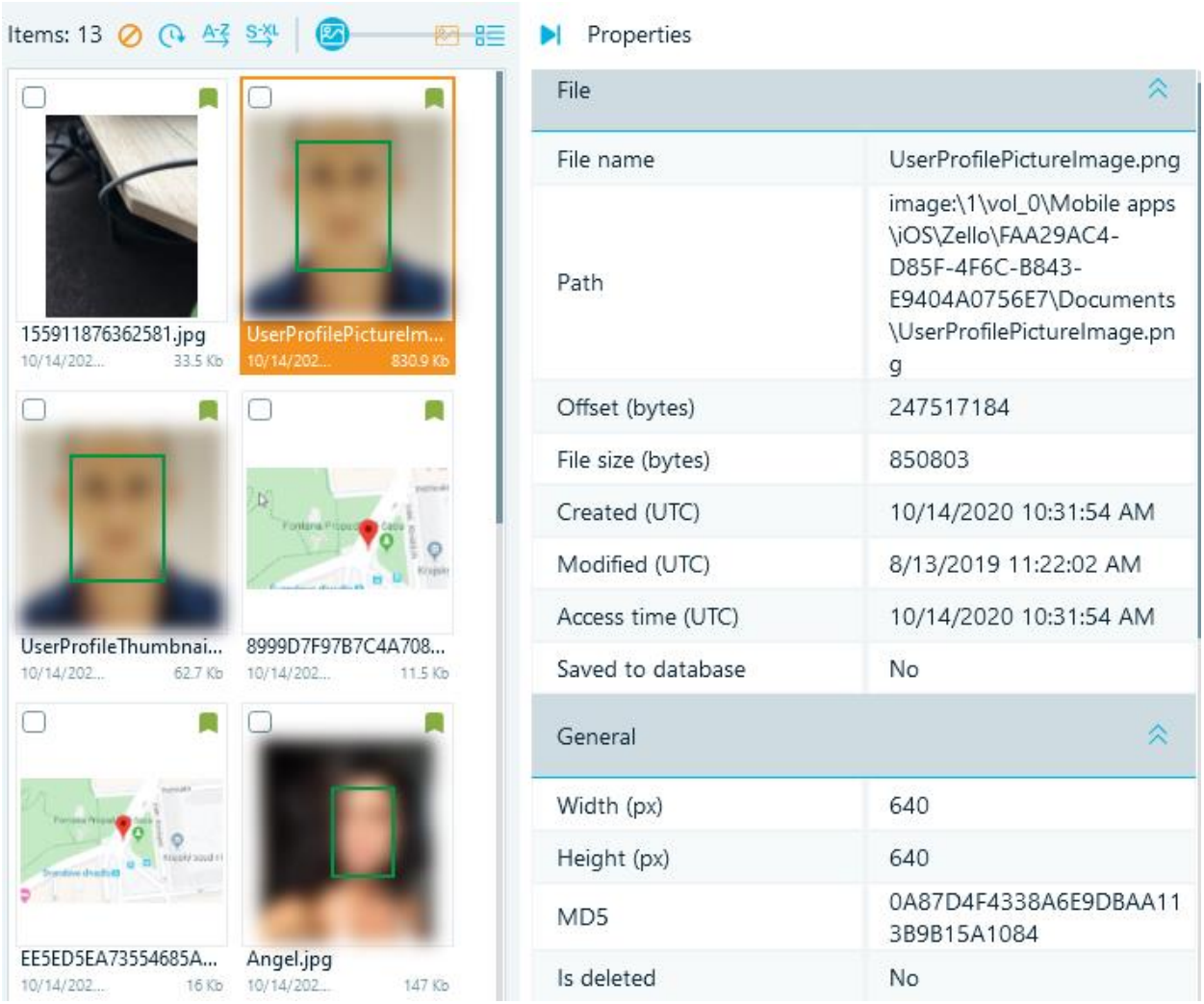
Depending on the artifact you bookmarked, when you click on an item, Belkasoft X may display **Item text** and lightweight versions of the **Hex Viewer** and/or **SQLite Viewer** at the button of the window.

For Hex Viewer and SQLite Viewer, you can then click on the expansion icon (Open large) to make Belkasoft X open the file on the full Hex Viewer or SQLite Viewer tab.



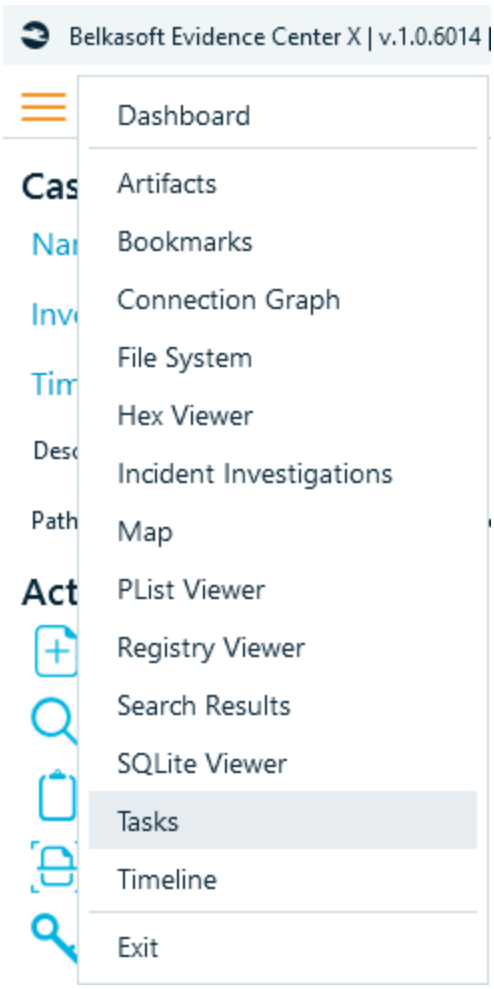
Selected artifact properties

This pane works similarly to artifact property panes inside other windows such as **Artifacts**. It shows selected bookmarked artifact properties.

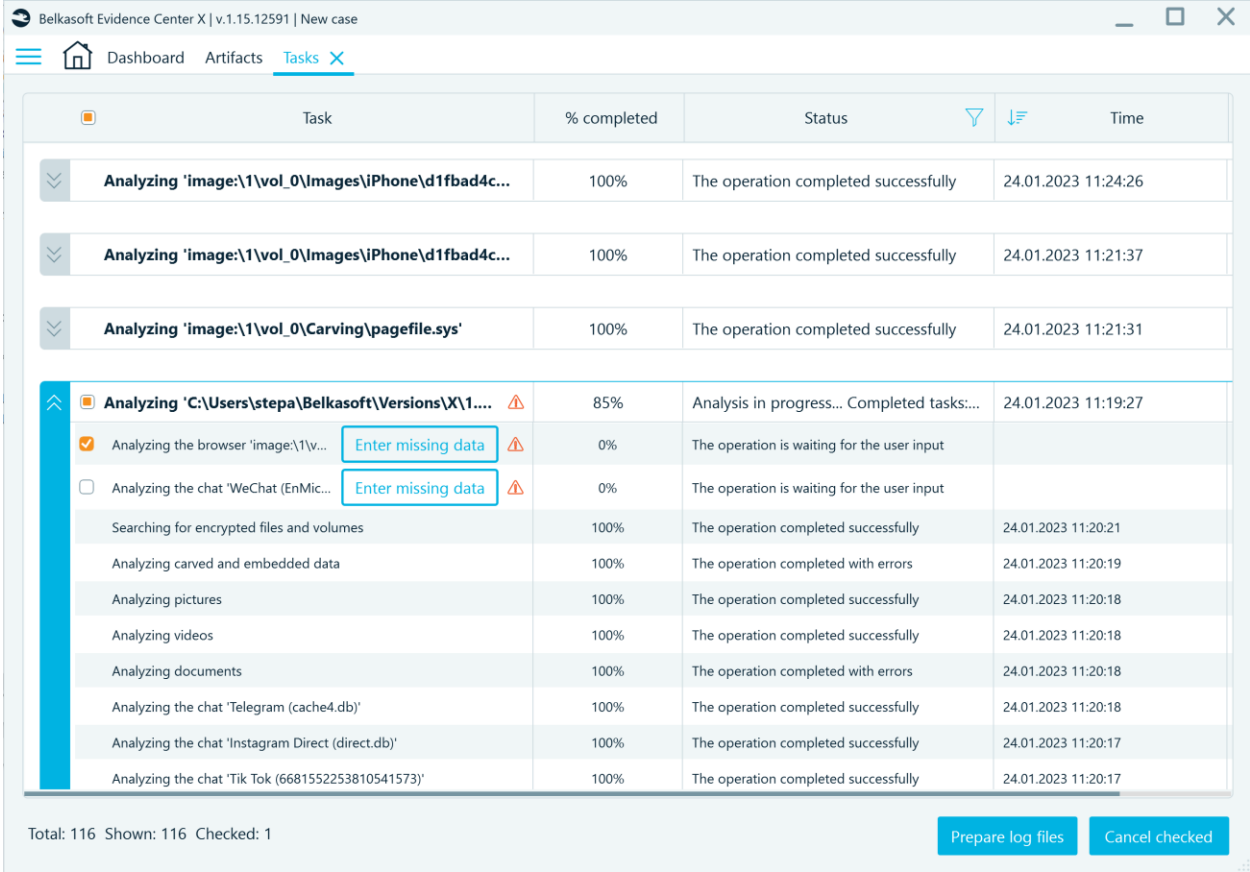


Tasks

Tasks window allows you to inspect all tasks Belkasoft X performs. You can open this window by using **Tasks** main menu item.



By default, **Tasks** window displays **top-level tasks**, which are run by user, such as acquiring a device, analysis of a data source, creating report or searching for an artifact. It may also show other bigger tasks, which are run automatically, for example, if a nested data source is found, a task for its analysis is also shown in this pane.



Each task which contains **subtasks**, can be expanded and you can see any particular task's progress.

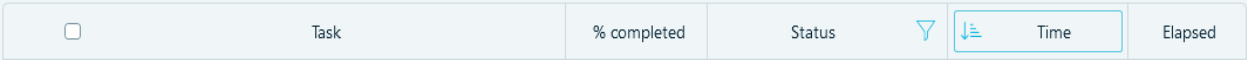
Subtasks are smaller tasks, which are run by Belkasoft X as a part of bigger tasks like as analyzing a data source. An example of an individual task would be an analysis of a particular application profile (for example, a particular Outlook mailbox, a particular Skype account, or a particular registry file). A data source can contain hundreds and thousands of profiles, so the list of subtasks can be huge.

Tasks pane contains a table with the following columns:

- **Task**—here you can see a task name.
- **% completed** shows a progress of a particular task.
- **Status** shows whether a task is in progress, scheduled, or completed. For completed tasks, you can see if they were completed successfully, completed with errors, or failed.
- **Time** here represents the startup time of a task. This column is empty for scheduled tasks.
- **Elapsed** column shows how long the task is (or was) running.

Sorting tasks

This table allows for sorting tasks by clicking on a column header.

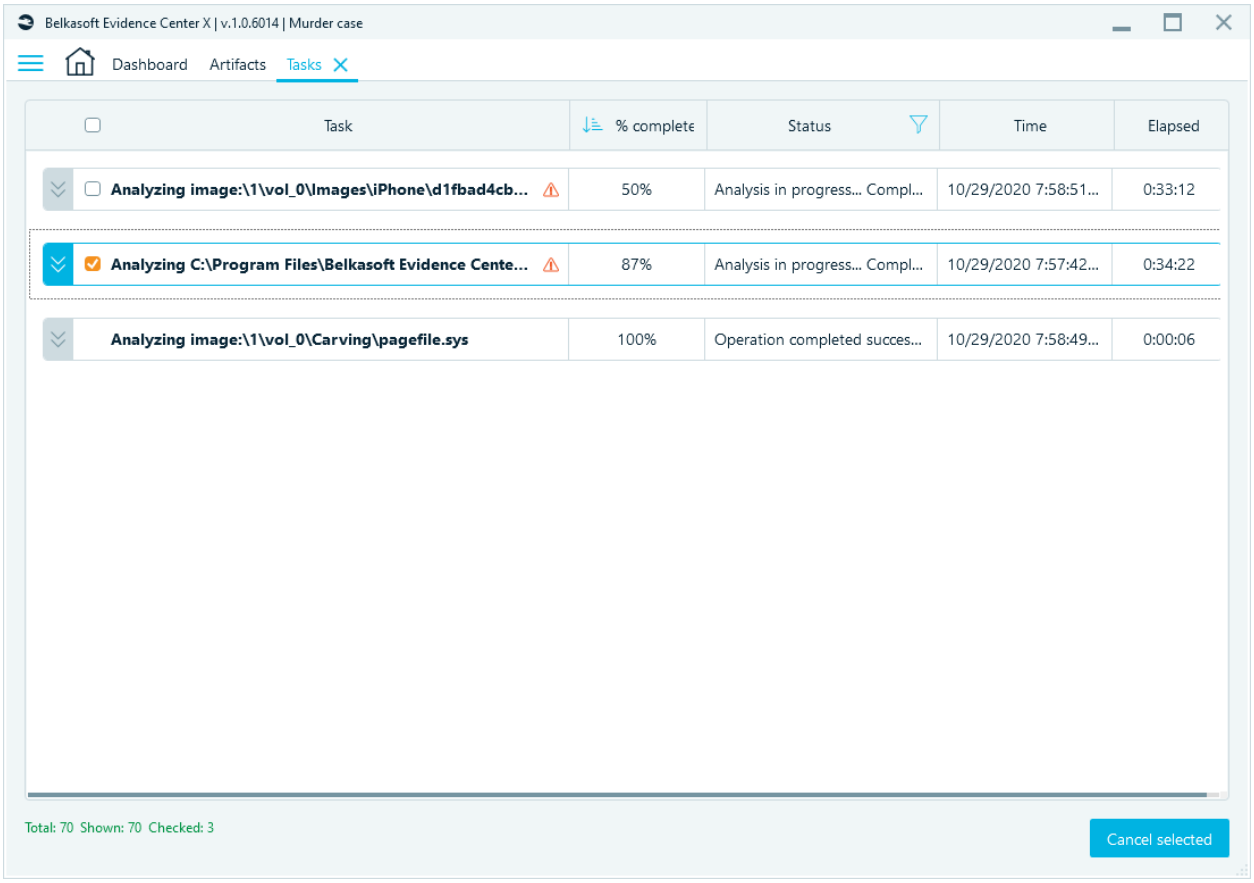


Viewing a task log

A double click on any task will open its log, which can be useful for troubleshooting.

Cancelling a task

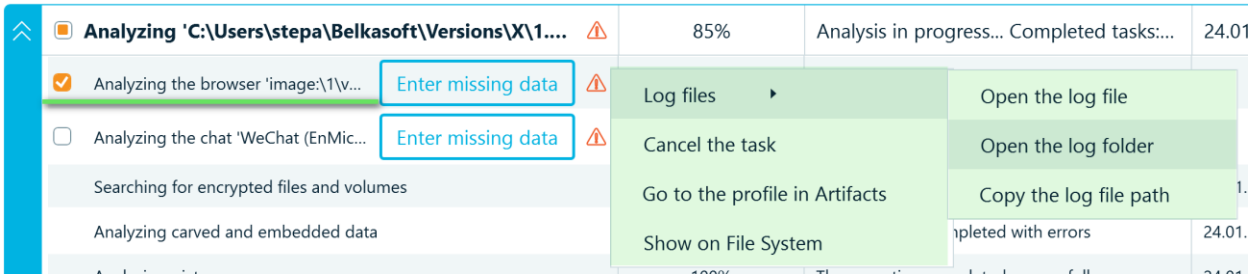
To cancel a task, click on the task's checkbox, and then click on the **Cancel selected** button (at the bottom-right corner). You might need to wait a while for Belkasoft X to cancel the task.



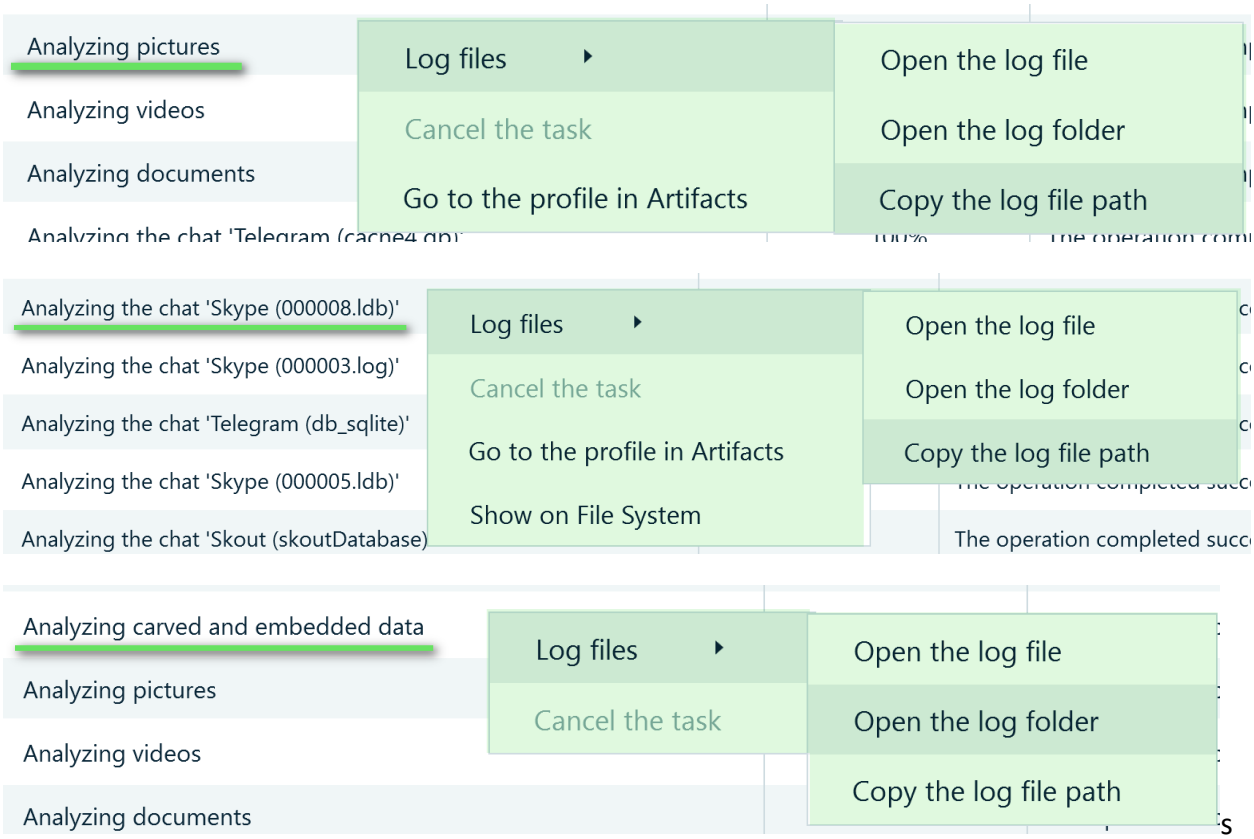
You can also cancel a task by calling the appropriate command from the dropdown menu.
Note: You can only cancel active and pending tasks. You cannot cancel tasks that have already reached completion.

Drop-down menu

The dropdown menu for different tasks is slightly different.
Task in progress:



Finished task:



Task Statuses

In Belkasoft X Belkasoft X, tasks may have different statuses depending on the activity or success or the operation. These values appear under the Status column:

- **Operation completed successfully:** the task completed without problems. When this status appears for an extraction task, for example, it means Belkasoft X extracted all the supported information.

- **Operation completed with errors:** Belkasoft X encountered some problems while processing the tasks. When this status appears for an extraction task, it means Belkasoft X completed the task and found some information, but some details might be missing.

- **Operation failed to complete:** Belkasoft X failed to perform the task. Unlike the 'Operation completed with errors' status, when Belkasoft X uses the 'Operation failed' status for a task, it means that Belkasoft X did not find information, did not generate a report, or did not find the search term. The failure—or its effects—is dependent on the type of task Belkasoft X worked on in the first place.

- **Operation canceled**: User-canceled tasks (including ones, which were canceled due to the closing of the software) are marked with this status. The information may be incomplete if you cancel a task before it finishes analysis, extraction or report creation.

- **Operation scheduled:** This status means that the task is scheduled but is not yet running. Belkasoft X tries to use as much processing power as your machine has, but if there are too many tasks, running them simultaneously will lead to slowing down the entire process, so some tasks are postponed until there is a free processor core.

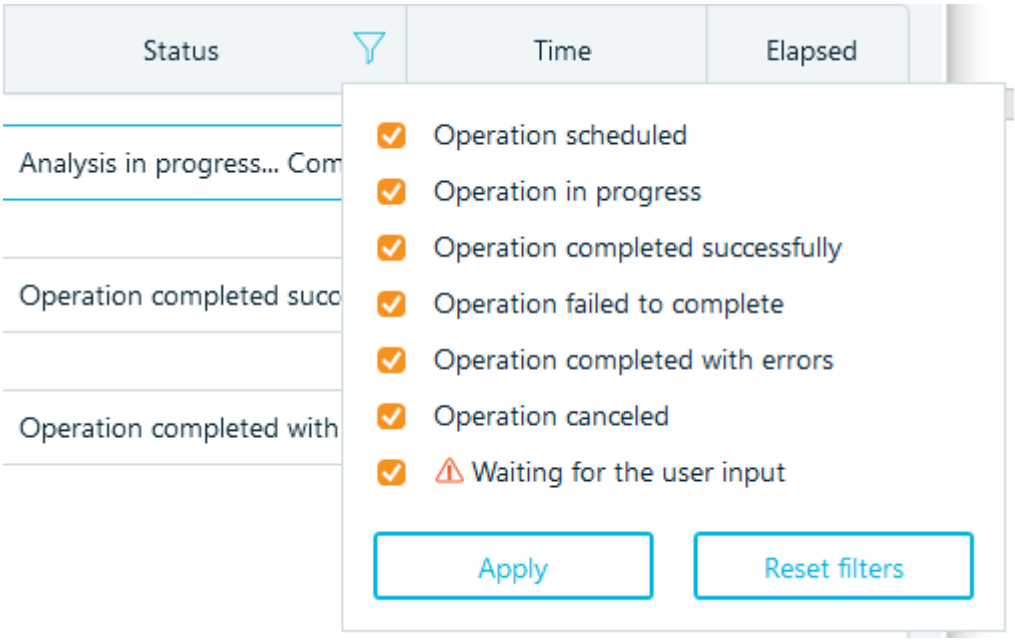
- **Operation is waiting for user input:** Belkasoft X is waiting for you provide some input before it starts or continues performing the task. For example, if Belkasoft X requires you to input the password for an encrypted file, Belkasoft X gives the analysis task for that file the status here. In such a scenario, after you click on Enter missing data, Belkasoft X prompts you to provide the password—and then (after you input the correct password) Belkasoft X continues with the task.

- **Analysis in progress:** Belkasoft X is actively performing the task. Depending on the task involved and some variables—the process, the data source (if it exists), selected analysis types and settings, your machine's CPU speed, amount of RAM available, speed of the source and/or target hard drive, and so on - Belkasoft X may display this status for a fraction or a second or a few days. If you are analyzing a simple or small data source using basic settings, for example, Belkasoft X is likely to perform the task quite fast.

Filtering tasks

In Belkasoft X, there might be hundreds or even thousands of tasks. If you want to see only certain tasks—for example, tasks that require some input from you—you can use the filter function to make Belkasoft X show only tasks that fall under the category you have in mind.

To filter tasks, click on the filter icon beside Status. Tick the checkboxes for the task statuses (categories) that you want to see.

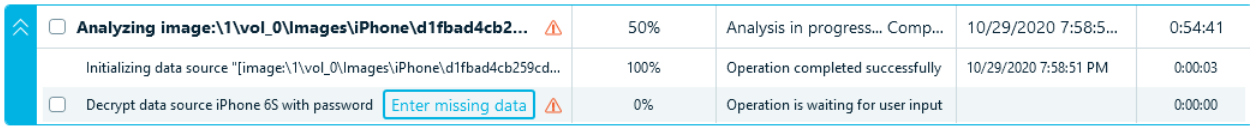


For example, if you want to see only tasks that require input from you, tick the **Waiting for user input** checkbox and untick all other checkboxes, and then click on the **Apply** button.

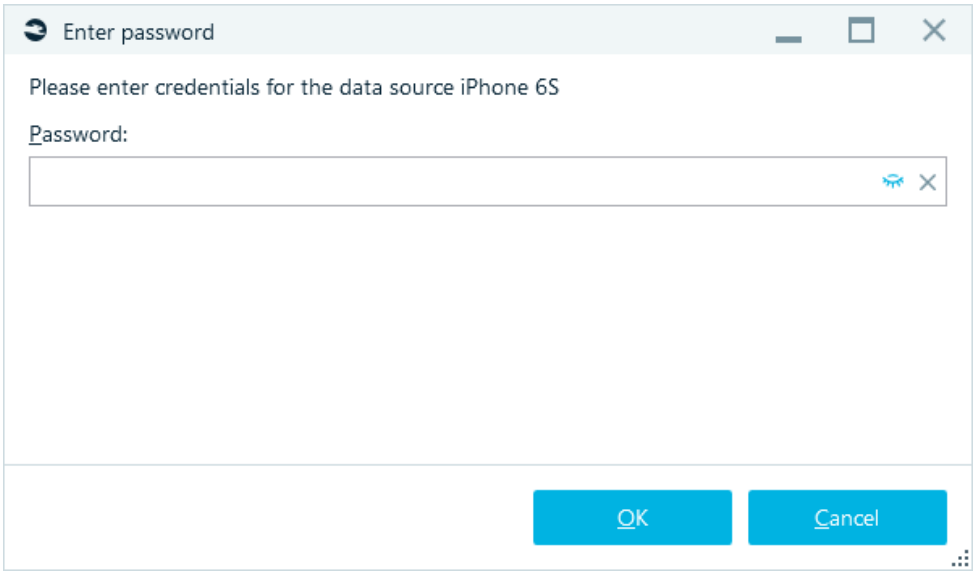
By checking and unchecking these check boxes, you can combine tasks of various statuses. Note that both top-level and individual tasks will be filtered (say if, you selected **Operation completed successfully** check box only and there is at least one individual task with this status, both individual task and corresponding top-level task will be shown; otherwise top-level task will be hidden).

Entering missing data

If you see an exclamation mark next to the top-level task name, it means you need to expand it and check the subtask statuses.



After you clicked on **Enter missing data**, a window will appear and ask for additional parameters. For example, the following is iPhone **Enter password** screen:

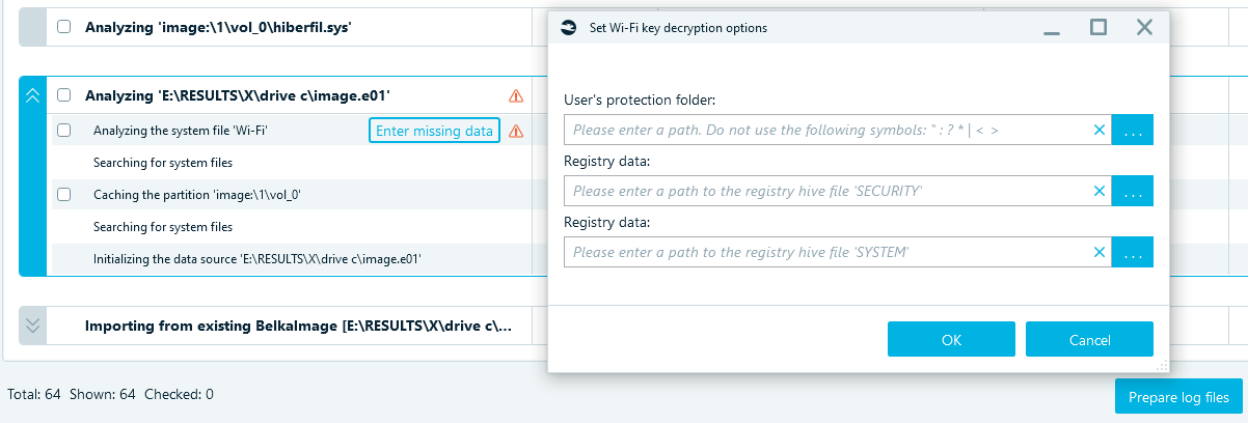


After you provide the needed information and click on OK, Belkasoft X will reinitiate the task and change its status to **Extracting data**.
If the entered data is incorrect, the decryption task will be displayed again.

Decryption tips

Windows Wi-Fi passwords extraction

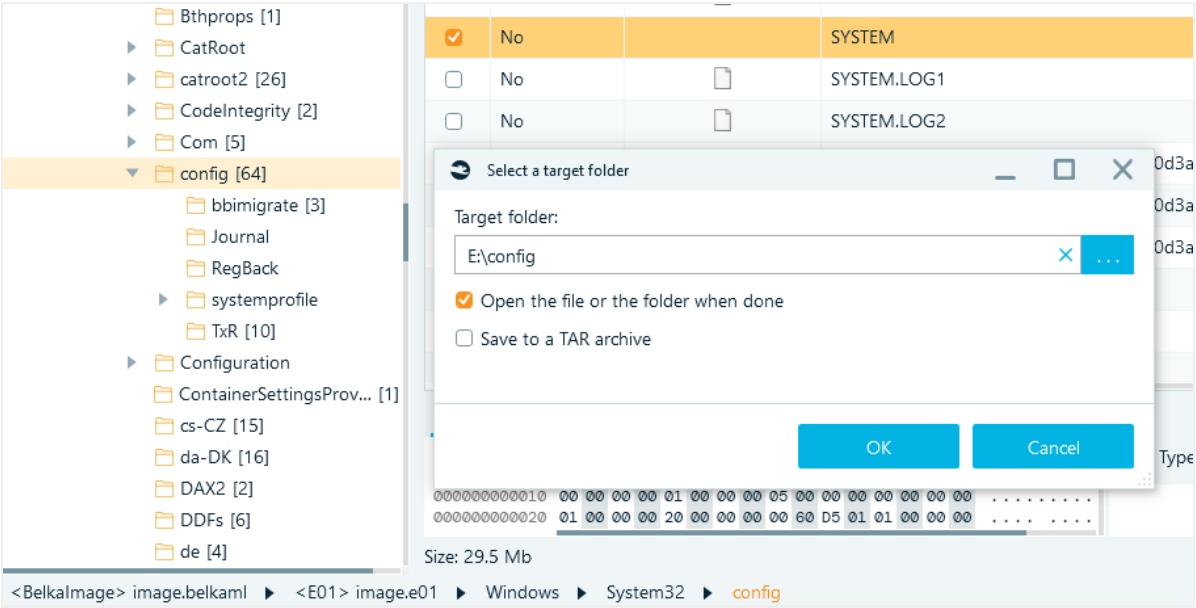
In order to extract Wi-Fi passwords, the user's input is required. Needed security data should be provided in the **Enter missing data** dialog for the operation 'Analyzing the system file 'Wi-Fi' in the Tasks window.



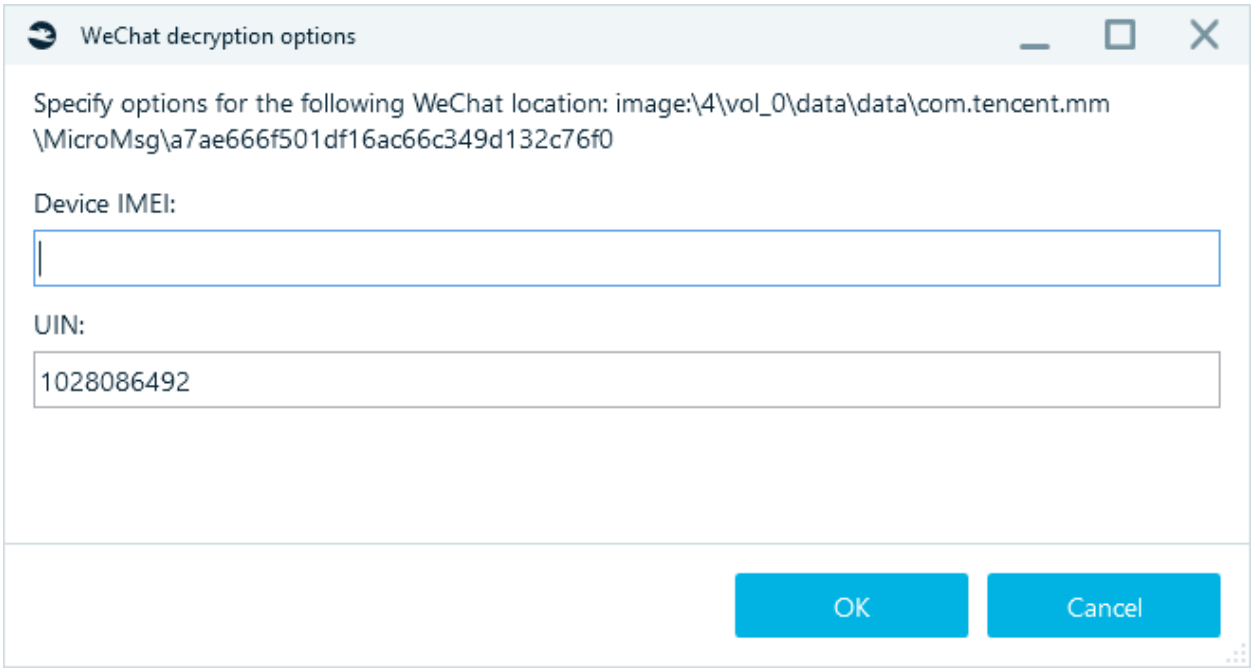
- **User's protection folder** path in Windows 10 is C:\Windows\System32\Microsoft\Protect
- **Registry data** path in Windows 10 is C:\Windows\System32\config (SECURITY and SYSTEM)

Note that registry files are in use, and therefore when the operating system drive is being acquired, those should be copied beforehand to another directory in order to grant Belkasoft X an administrative access to them.

The easiest way to obtain the needed protection folder and registry keys is to copy them from the **File system** tab of Belkasoft X.



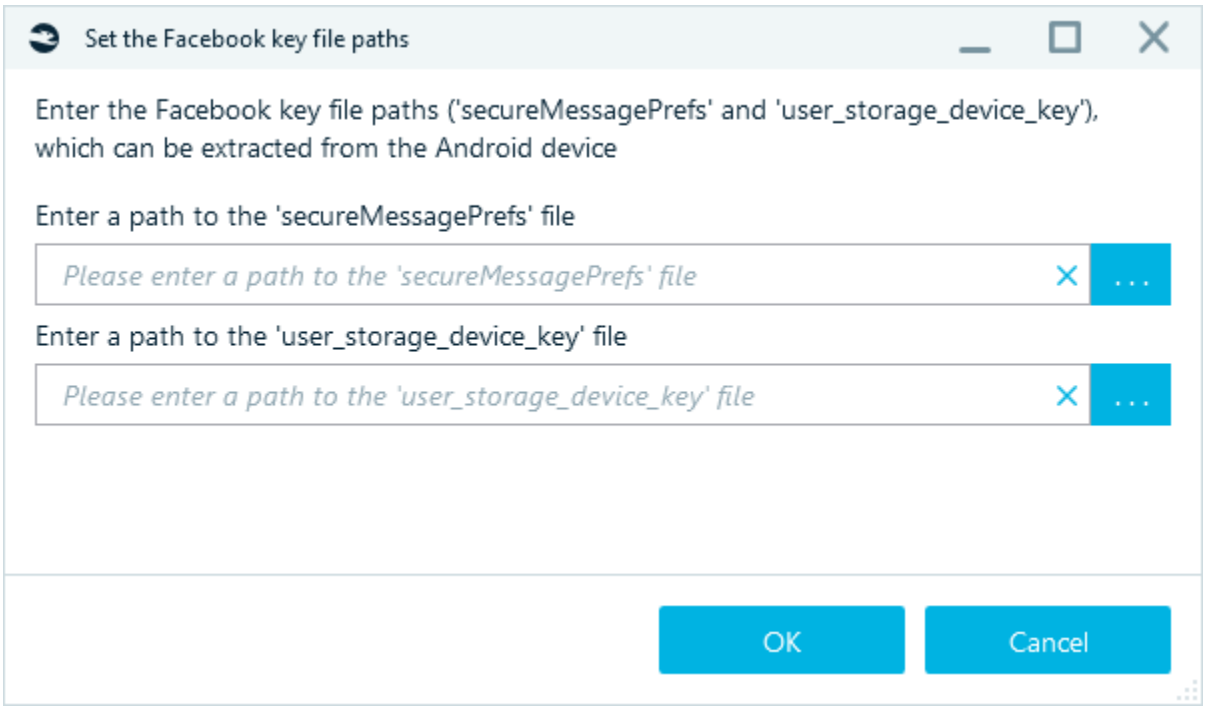
WeChat (Android)



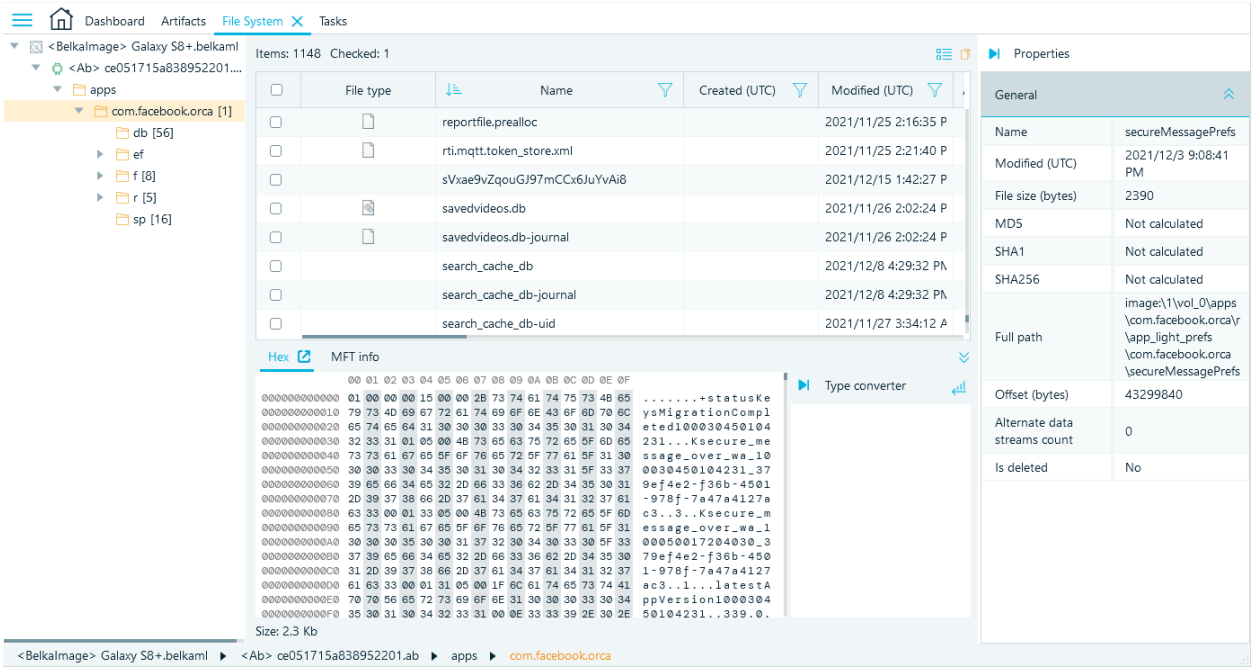
UIN can be found in file system files **system_config_prefs.xml** and **app_brand_global_sp.xml**
IMEI:

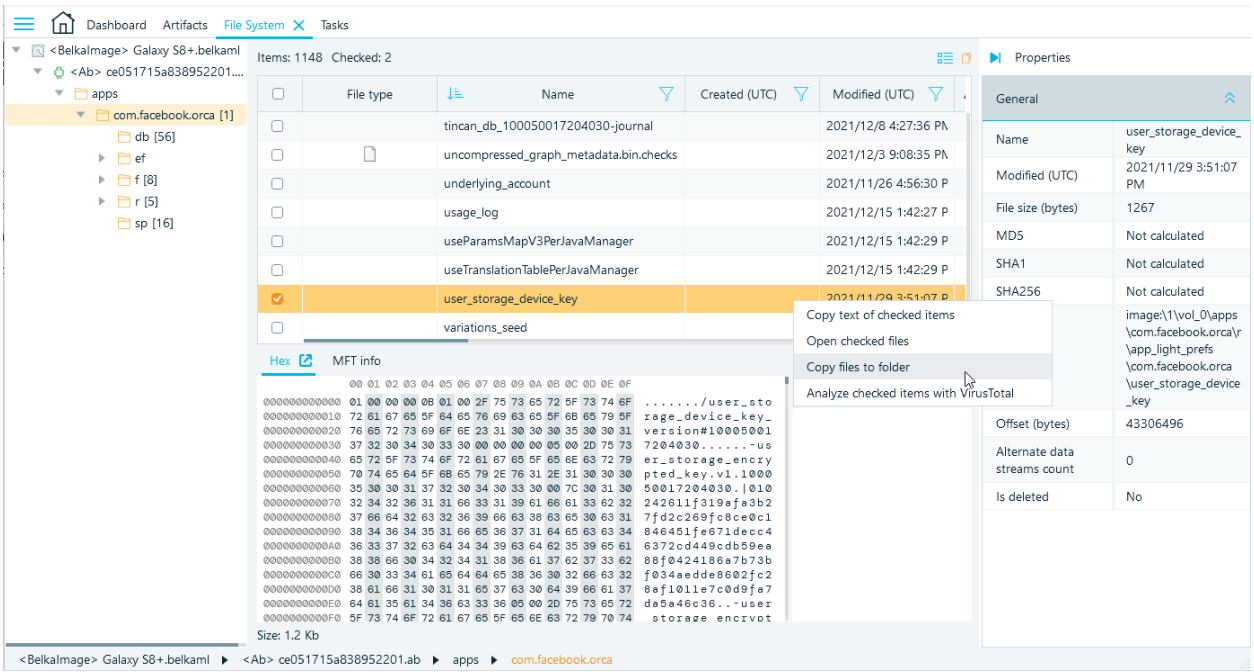
- USSD Request ***#06#**
- Find IMEI in phone settings

eFacebook messenger (Android)

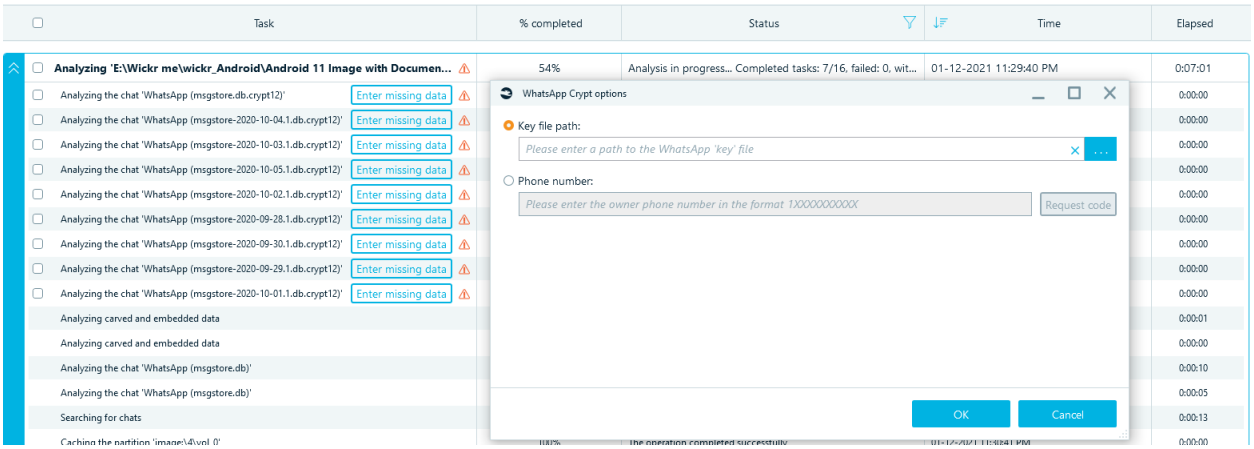


Acquire Facebook messenger by method APK Downgrade and find files in File system tab:

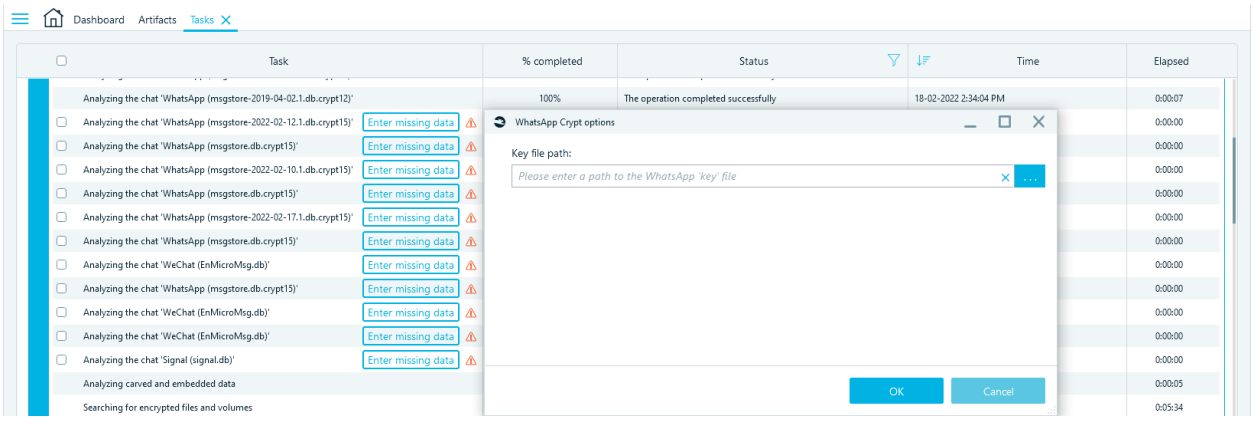




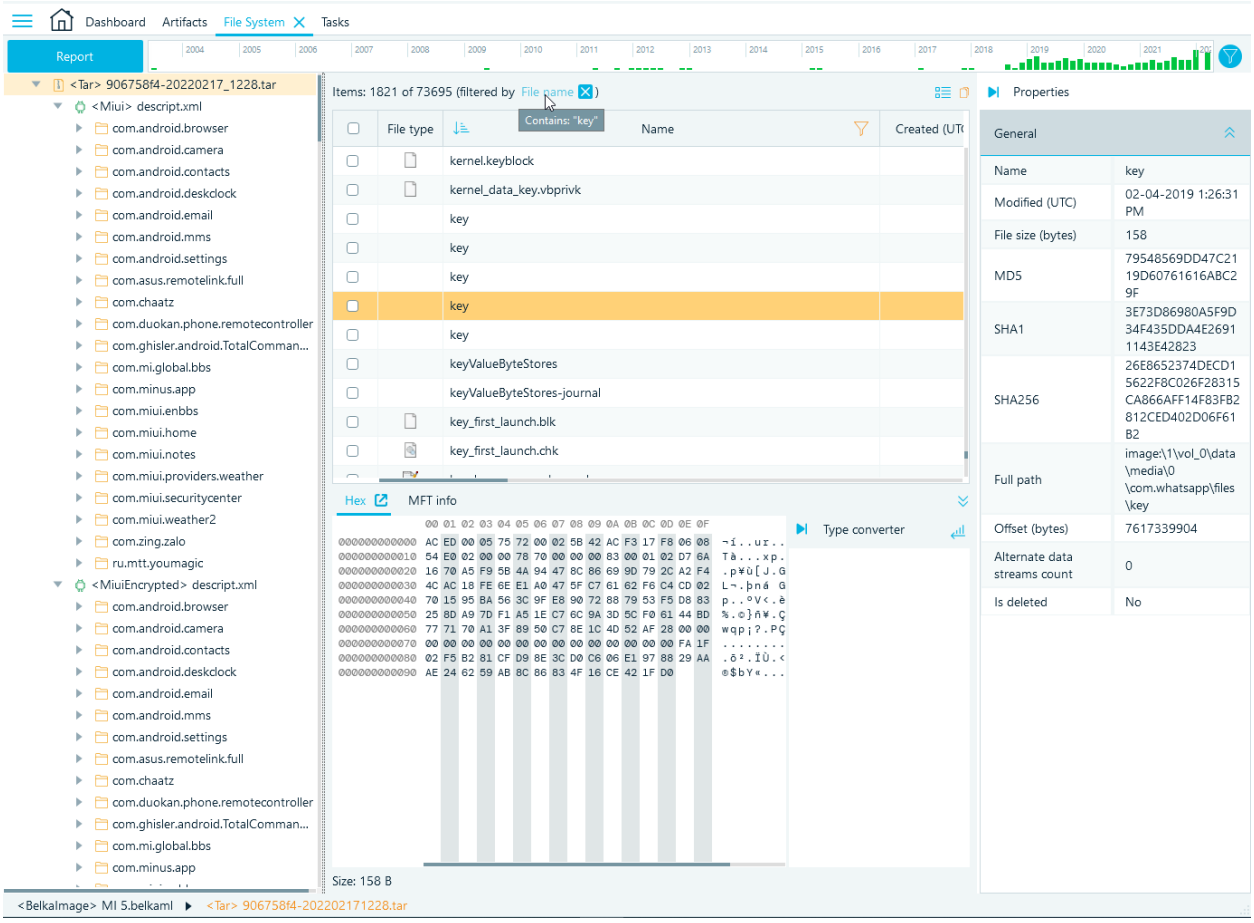
WhatsApp (Android)



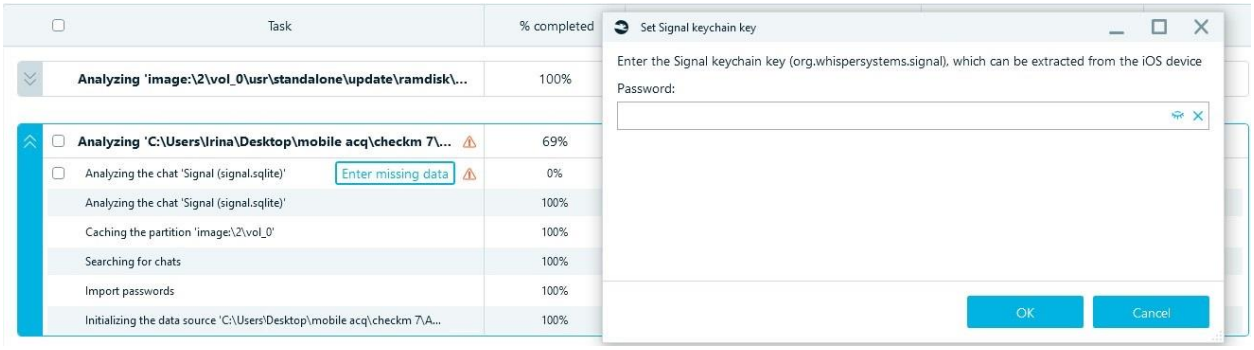
For crypt15:



The **key** file: contains a cryptographic key. Located along the path: '/data/data/com.whatsapp/files/'. Used to decrypt encrypted WhatsApp backups.
To access such file, you need a full file system copy (acquisition method ‘Android file system copy’). ***Root*** rights required.



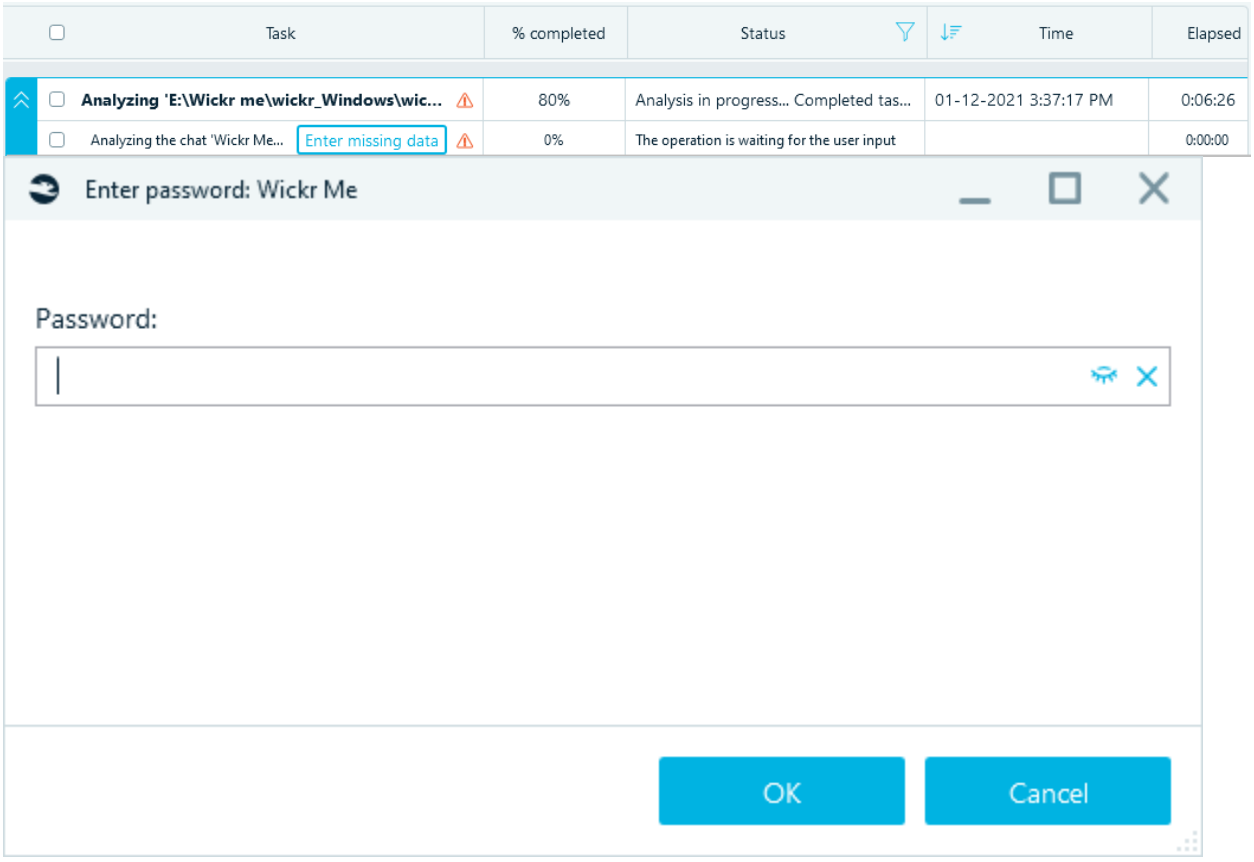
Signal (iOS)



Open keychain file and find '**org.whispersystems.signal**'.
Find value for **PasswordDataOrigin**:

```
<dict>
    <key>Accessible</key>
    <string>kSecAttrAccessibleAfterFirstUnlockThisDeviceOnly</string>
    <key>Account</key>
    <string>GRDBDatabaseCipherKeySpec</string>
    <key>CreationDate</key>
    <date>2020-12-01T18:28:11Z</date>
    <key>EntitlementGroup</key>
    <string>U68MSDN6DR.org.whispersystems.signal</string>
    <key>HaveStringValue</key>
    <false/>
    <key>ModificationDate</key>
    <date>2020-12-01T18:28:11Z</date>
    <key>PasswordDataOrigin</key>
    <string>S4fNoyzcASh2fBzu7a9eUxXAVf5qrHyo7XcWevbErwvvOPwi5Ap2HzpBk3fjMlLv</string>
    <key>Service</key>
    <string>GRDBKeyChainService</string>
    <key>Synchronizable</key>
    <integer>0</integer>
</dict>
```

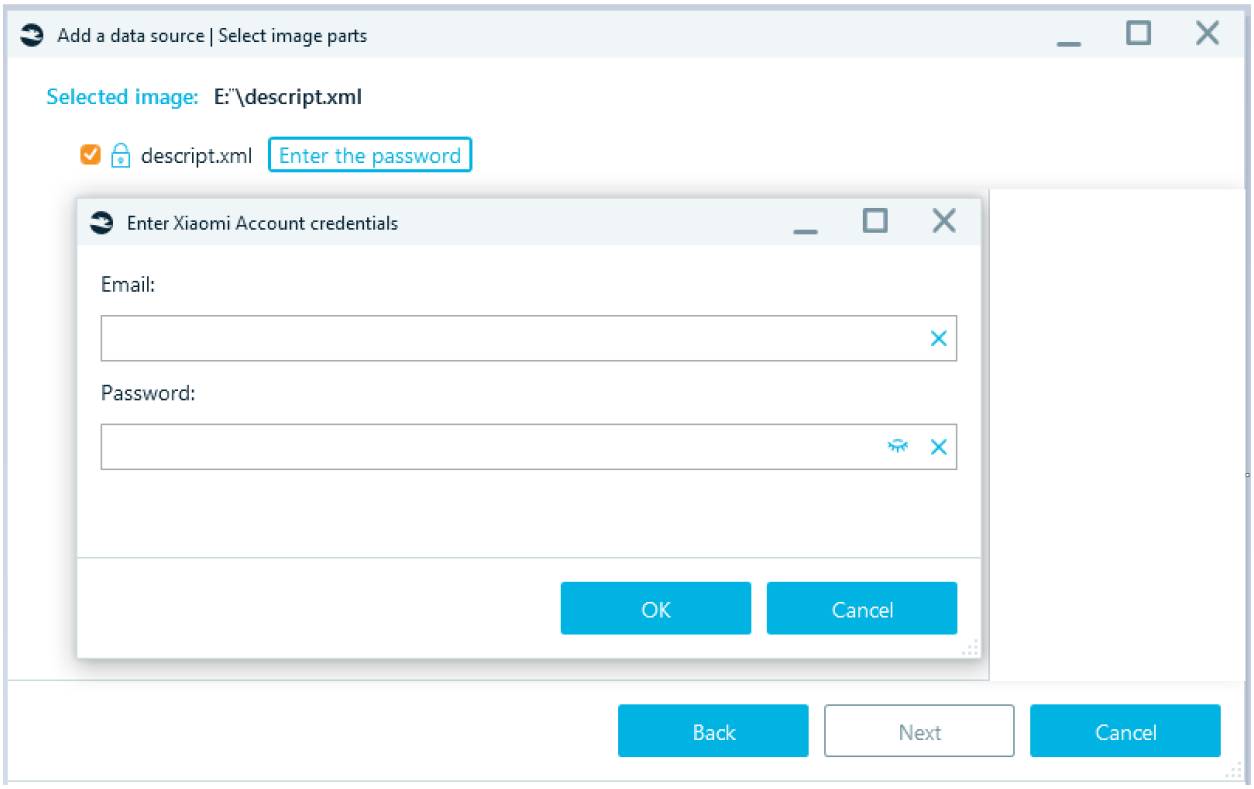
WickrMe / Wickr Pro (Windows, Linux, Android)



Enter WickrMe / Wickr Pro account password.

MIUI backup decryption

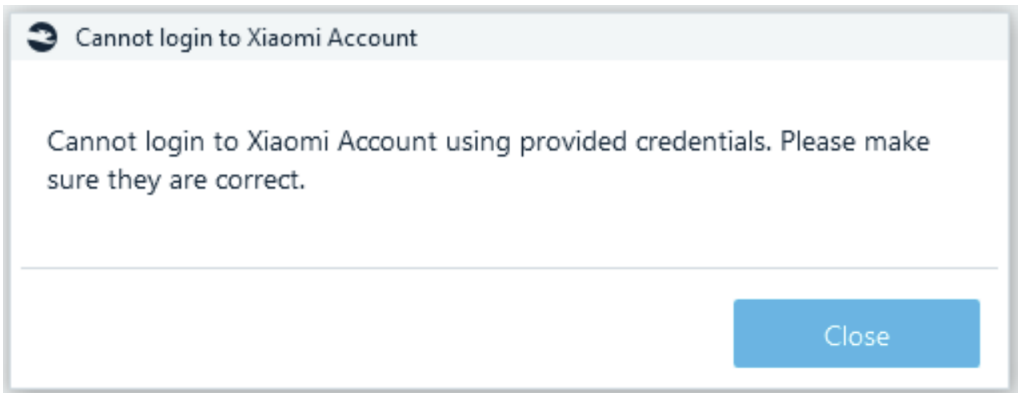
To decrypt the MIUI backup created on the Xiaomi device, you need to get the decryption password from the Xiaomi server. To get the password you need to login to Xiaomi Account and submit the special key from the manifest file.



There are several cases that may occur and prevent from receiving the decryption password.

- Cannot login to Xiaomi Account.

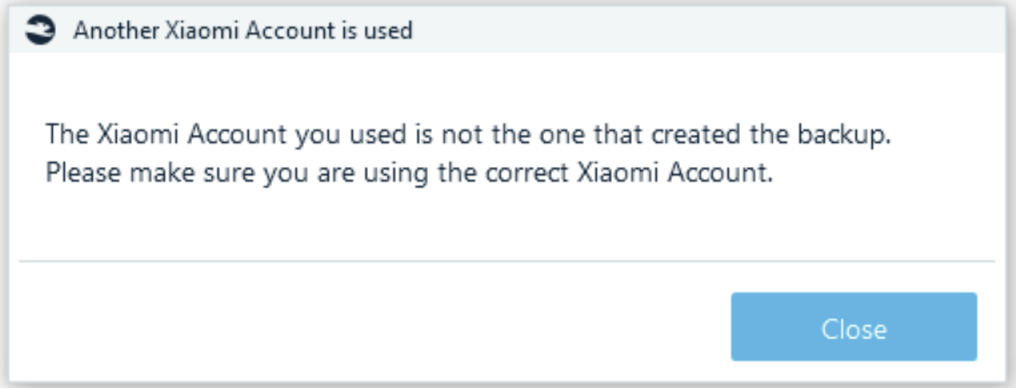
The message is displayed when there is no registered Xiaomi Account with the provided Credentials.



- Another Xiaomi Account is used.

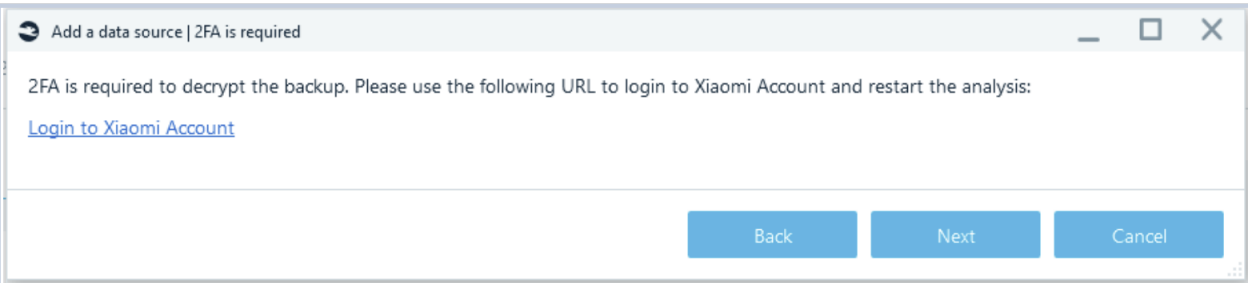
The message is displayed when the other Xiaomi Account credentials were provided. To decrypt the MIUI backup you need to enter the Xiaomi Account that was used to create the backup. Another account

credentials won't fit in this case.



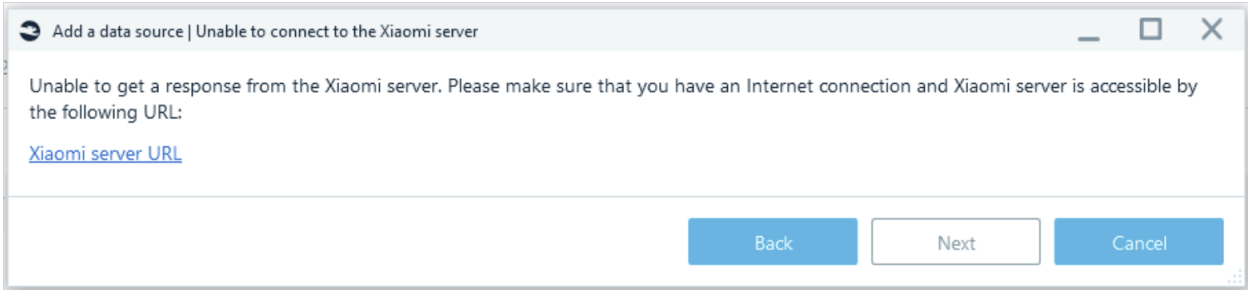
- 2FA is required.

The window is displayed when a Xiaomi Account requires 2FA. Some Xiaomi Accounts require 2FA to get the decryption password. To verify the 2FA you need to login to Xiaomi Account using the generated URL. You can follow the 2FA link by clicking the «Login to Xiaomi Account» text element. Once the 2FA is verified, you can click the «Next» button to proceed with decrypting the MIUI backup.



- Unable to connect to the Xiaomi server.

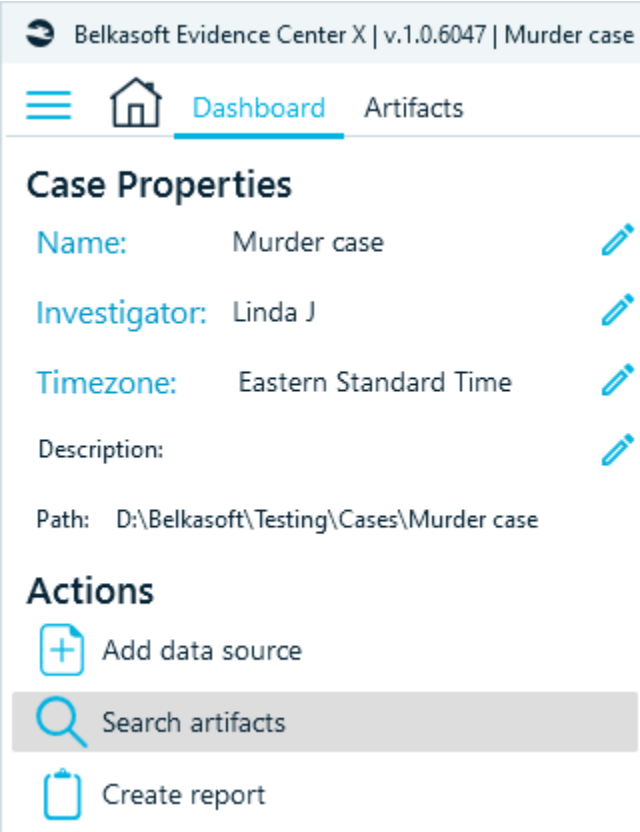
The window is displayed when it is unable to connect to the Xiaomi server. To check the Xiaomi server availability, you can click the «Xiaomi server URL» text element.



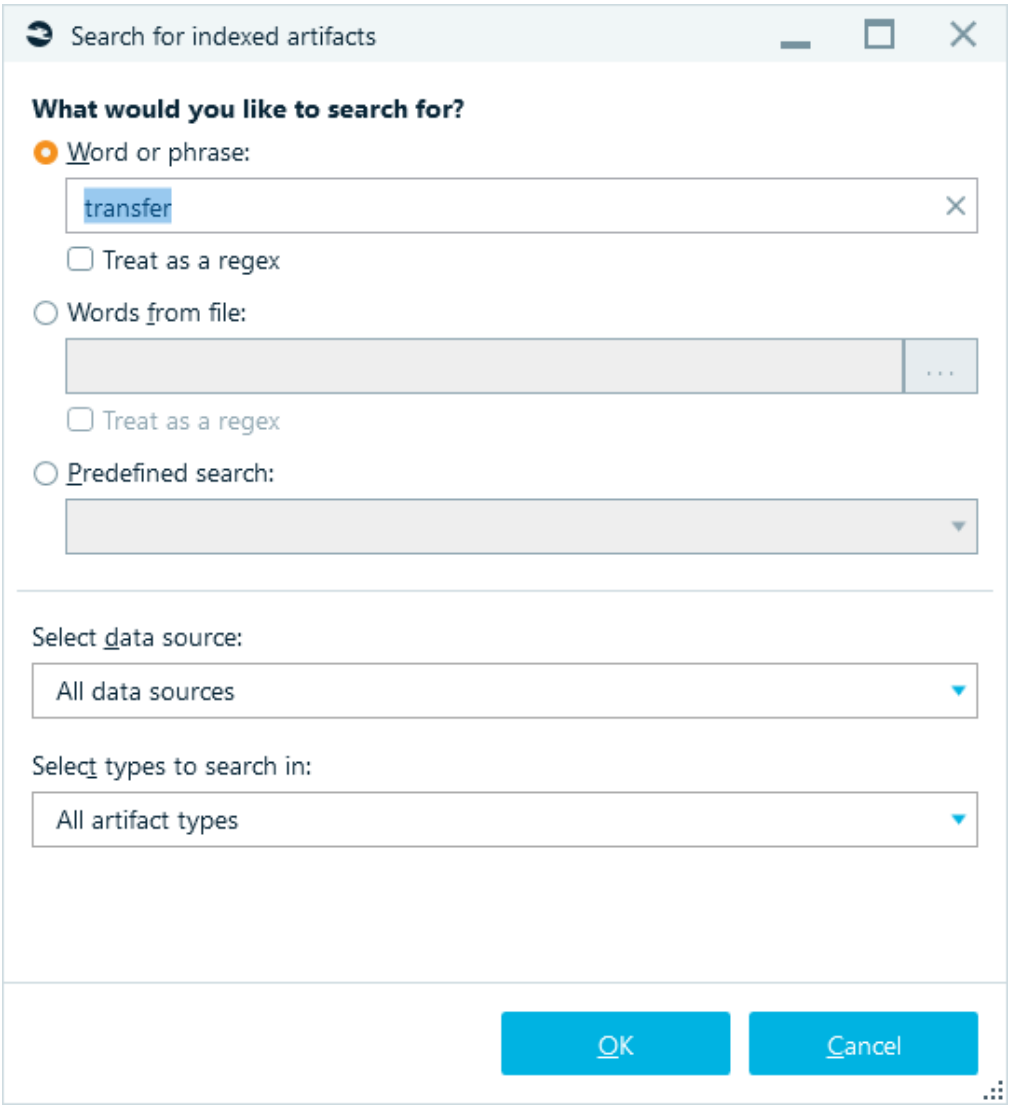
Searching artifacts

Once you have artifacts extracted, you may want to do a search using different criteria. Along with filtering, search allows you to narrow number of items to review. Belkasoft X automatically indexes all text-based properties of artifacts, such as their texts, dates and times, metadata, and so forth. So, running a search query against extracted artifacts data is a quick process.

Note: Do not confuse the search of profiles and the search inside artifact texts. Search for application profiles is performed during analysis of a data source and the main goal is to find all artifacts for a specific application. For instance, Belkasoft X will find an Outlook mailbox (and will extract all emails) and 1000 documents (and will extract texts and metadata for every one of those items). Once that mailbox and the documents within are analyzed, you can search for particular texts extracted from them.
To run search in artifacts, you can either press **Ctrl-F** key combination or go to the **Dashboard** and choose **Search artifacts** item of the **Actions** list.



Search data window will be shown:



The following search options are available:

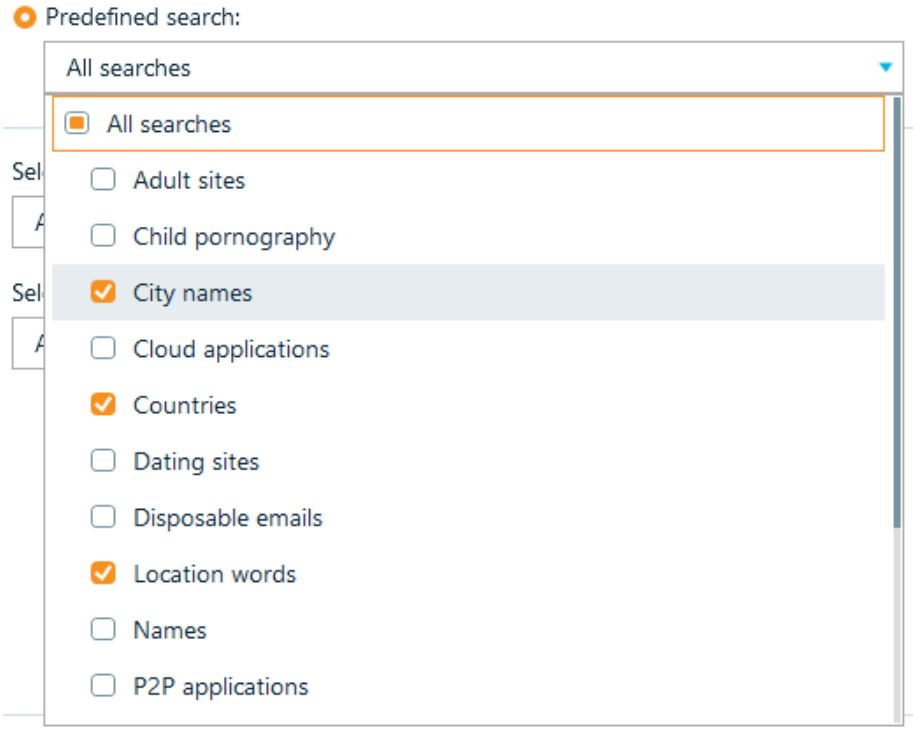
- **Word or phrase**. Choose this option to find all data containing a certain word or phrase.
    - This search is **not** case sensitive.
    - This search is carried out by exact match of the whole word. If you need to find artifacts by part of a word, use the * symbol.

    Check the **Treat as a regex** checkbox if you would like to use a regular expression. Regular expression is a powerful mechanism to perform complicated searches. You can choose this option when you do not know exactly what you are looking for, for example, while searching for emails or credit cards when you do not yet know the exact email address or card number. More details about the syntax of writing regular expressions will be discussed below.

- **Words from file**. Choose this option when you have a keyword file containing all words of interest. Having such a file saves a lot of time if you have numerous words in which you need to search—all the keywords can be searched for in a single search operation.

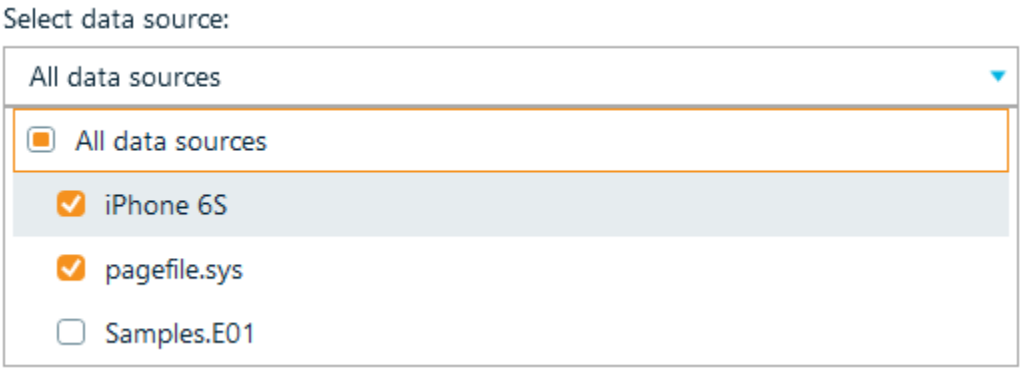
  Check **Treat as a regex** checkbox if you would like to use a file containing a list of regular expressions.

- **Predefined search**. Belkasoft X offers you a set of predefined searches based on vocabulary, for example, adult sites, city names, disposable (one time) email addresses, steganography app names, and so on. Note that these searches are customizable: you can find them under the product folder (e.g. C:\Program Files\Belkasoft Evidence Center X\Resources\Search\Names\AmericanNames.txt") and edit them as you need.

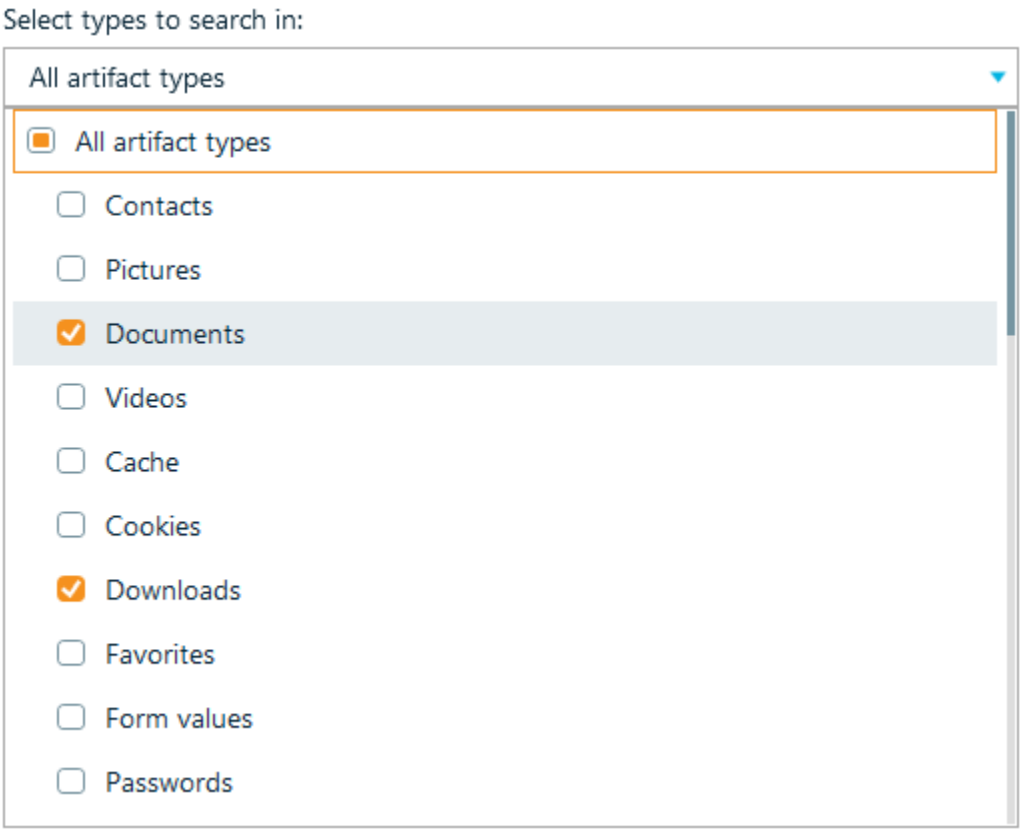


At the bottom of this window, you can see two drop downs:

- **Select data source**. Here you can specify which data sources to search in



- **Select types to search in**. Here you can specify which artifact types to look for, for example, to perform search in Documents and Downloads only



Both panes have root checkboxes helping you to do mass selection operations.
Typically, one performs a search inside all data sources and profiles, because it is better to find all the results and only then to filter those using filters inside **Search Results** window.
When you click on **OK** button, the search task will start and be shown in Belkasoft X's **Tasks** window.

If it is not entirely clear what to look for, use special search operators.

1. Wildcard operator, type an asterisk (*) in place of the world you're not sure about. It replaces zero or more characters.

Example:
win* Matching: win, wine, wineglass, etc.

Example:
in Matching: win, wine, skin, instagram, etc.

2. Wildcard ? operator will replace any single character

Example:
?hat Matching: what, that, etc.
Example:
h?t Matching: hat, hot, etc.

3. Fuzzy ~ operator. Find all terms with a maximum of two changes, where a change is the insertion, deletion or substitution of a single character, or transposition of two adjacent characters.

Example:
what~ Matching: what, that, hat, wat, etc.

To speed up the search, all found artifacts (words, dates, documents content, passwords, etc.) are indexed. Due to this, the search even on huge amounts of data is fast. A list of all indexed artifacts placed in the Key dictionary. It can be created from Dashboard actions.

Almost all non-alphanumeric characters are delimiters. The exceptions are @, underscore _, and dots. If the artifact contains a delimiter, after indexing, it will be split into two indexed words before and after the delimiter.
List of delimiters: ; : $ # ₽ _ & ? ( ) { } [ ] | \ / " ' ! < > % + ~ & *

Example:
Drugs+Guns Matching in key dictionary: drugs, guns

- search by Drugs+Guns return 0 matches
- search by drugs or guns reveals this example

Example	Matching in key dictionary
"SD500"	"**SD**", "**500"**
"//hello---there, dude"	"**hello**", "**there**", "**dude**"
"O'Neil's"	"**O**", "**Neil**"

Regular expression syntax

Below is the table of the most commonly used characters, with their meanings and examples.

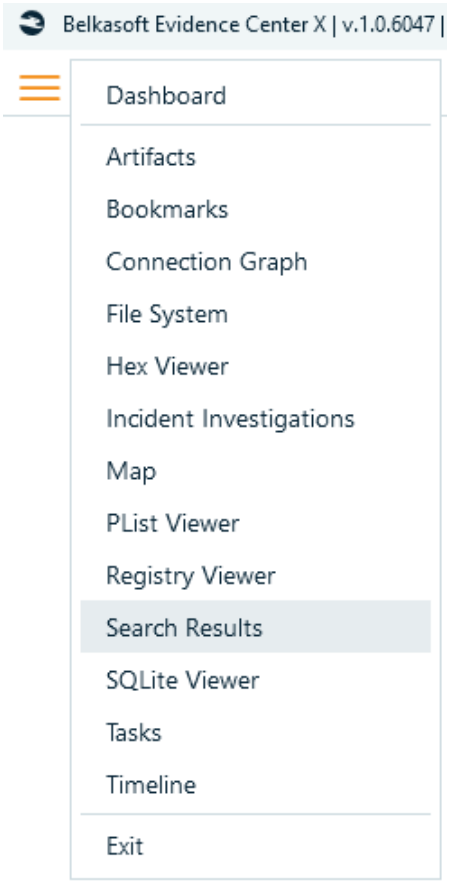
Regular expression	Explanation	Example	Matching
.	Any single character excluding a newline.	**.ar**	The **car par**ked in the **gar**age

[ ]	Searches for any of the characters in parentheses.	**[Tt]he**	**The** car parked in **the** garage
[a-z]	A **dash** means a range of characters	**[e-g]**	The s**ell**e**r** sold 2 **g**uns and 7 pistols.
[0-9]	Finds any digit between 0 and 9	**[3-8]**	The seller sold 2 guns and **7** pistols.
[^]	Matches any character that is not contained between the square brackets	**[^c]ar**	The car **par**ked in the **gar**age.
\.	A **dot** matches almost any character, use **** symbol to find a regular dot	**ar\.**	A garage is a good place to park a c**ar.**
|	The pipe symbol "**|**" acts as an OR operator.	**gr[e|a]y**	**grey, gray**
{m}	Repeat exactly **m** times	**colou{3}r**	**colouuur**
{m,n}	Repeat from **m** to **n** times	**colou{2,4}r**	**colouur, colouuur, colouuuur**
{m,}	Repeat at least **m** times	**colou{2,}r**	**colouur, colouuur, colouuuur, etc**
{,n}	Repeat not less **n** times	**colou{,3}r**	**color, colour, colouur, colouuur**
?	Makes the preceding character optional. Matches zero or one times: corresponding {0,1}	**colou?r**	**color, colour**
*****	**repeat zero-or-more times: corresponding {0,}**	**colou*r**	**color, colour, colouur, etc**
+	repeat **once or more** times: corresponding {1,}	**colou+r**	**colour, colouur, etc (but not color)**
^	Finds the beginning of the entered string	**^a**	**aaa aaa**
x$	A line ending with the **x**	**a$**	**aaa aaa**
(xyz)	Finds a group of characters in a strictly specified order.	**(at)**	F**at** c**at** is going to St**at**en Island
****	Cancel the special meaning of the metacharacter that follows it. Allows searching for service characters [] () {}. * +? ^ $ \ |	**(f|c|m)at\.?**	The **fat cat** sat on the **mat.**
\s	Space	**\s*cat\s***	The fat **cat** sat on the con**cat**enation.
/^Yes/	A line starting with **Yes**	**/^Yes/**	**Yes** ... **Yes**terday ...
/th/	Occurrence of the string th anywhere in a word	**/th/**	**th**e, **th**ere, pa**th**, ba**th**ing, etc

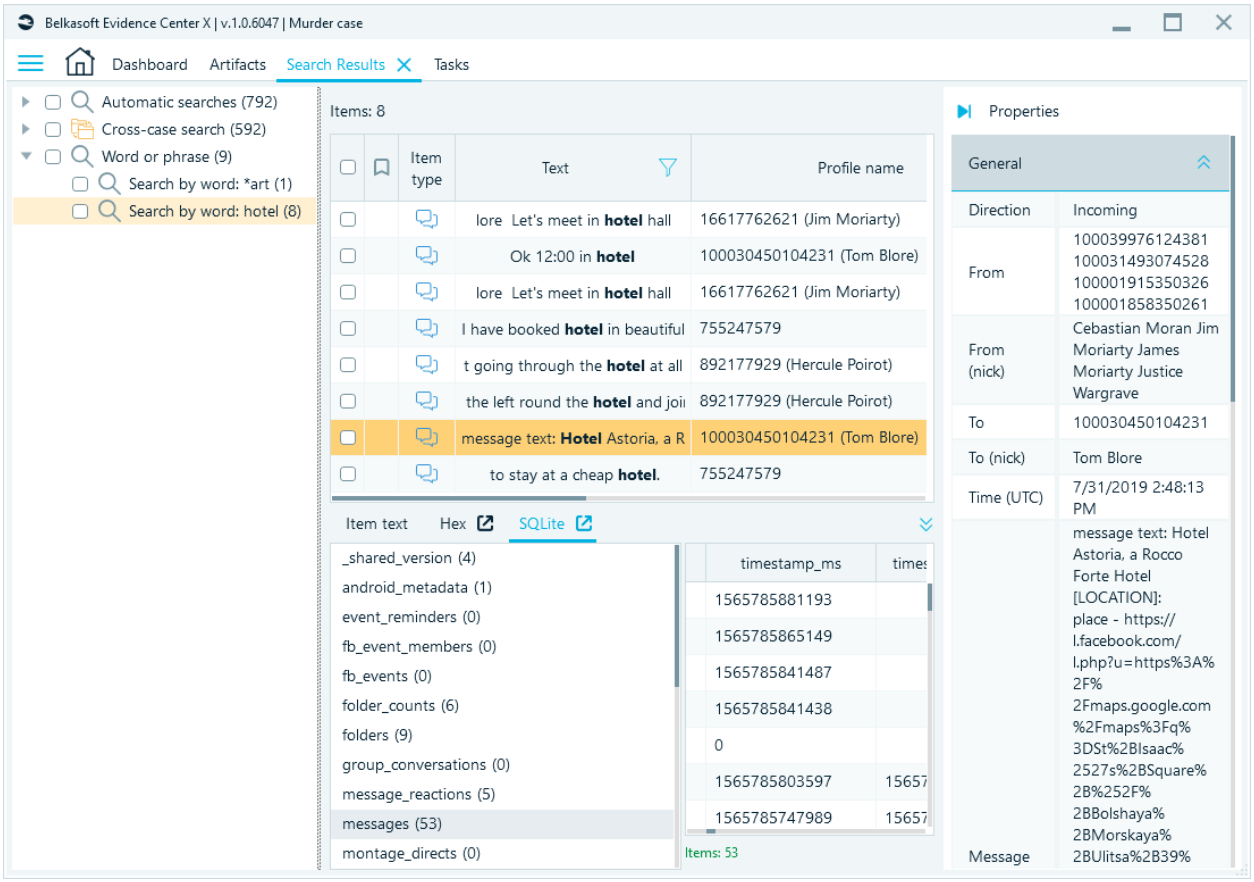
Example: how to find artifacts like 123-1234 with any number? Use this regular expression: [0-9]{3}-[0-9]{4}.

Search Results window

Search Results is a top-level window, which shows the results of automatically performed predefined searches and cross-case searches, as well as user created searches.
If you do not see **Search Results** window, you can show it by clicking on **Search Results** main menu item.



Also **Search Results** window is shown when a search is completed:



Search Results window consists of three panes:

- Search history pane at the left
- Search results list in the middle
- Search result item properties at the right

Search history pane

The search history pane may have up to five nodes:

- **Automatic searches**. This node contains all predefined search results, whether run automatically (regular expression-based searches, which are performed whilst data source analysis) or by a user (using **Predefined search** option described above).
- **Cross-case search**. This node contains all matches between the current case and older cases during analysis. The following types of data can be searched: email addresses, phone numbers, application UINs, and profile names.
- **Regular expression**. This node contains all searches by regular expression. The search term is noted for each search performed.
- **Word or phrase**. This node contains all searches by a word or a phrase. The search term is noted for each search performed.
- **Words from file**. This node contains all searches by words from a file. The file name is noted for each search performed.

All nodes in this pane have a number in parentheses following the node name. This number indicates the amount of results of corresponding type.
You can create a report for any search session by right clicking on a node and selecting **Create report for checked items...**.

Search results list

The search results list shows you all found artifacts for a search session, currently selected in the search history pane. This list has the following columns:

- **Checkbox column**. It works similarly to other lists and can be used to include multiple items to a report or do mass operations.
- **Text**. Displays the particular text where a search term was found. The term is highlighted with a bold font so you can see why the specific item is a search hit.
- **Field name**. This column makes it easy to understand inside which property of an artifact a search term was found; meaning, there could be multiple fields to search in. For example, a document can have text info in its body or metadata, a picture can have various EXIF tags with texts, an email can have email text and headers.
- **Profile name**. Displays the name of a profile where the artifact was originally extracted.
- **Profile type**. Indicates the type of a profile where the artifact was originally extracted.
- **Source**. Is a name of a data source where the artifact was originally extracted.
- **Time (UTC)** and **Time (Local)**. Data timestamp of an artifact (if any). Typically, only one of these columns contain value.

This list works similarly to other artifact lists such as **Artifacts**: it has sorting, filtering, and reporting; however, it has one extra item in its context menu, namely **Go to original item**. This menu will navigate you to the corresponding profile and artifact inside **Artifacts** so that you can see the origin of the search result.
Depending on the artifact type, when you click on an item, Belkasoft X may display **Item text** and lightweight versions of the **Hex Viewer** and/or **SQLite Viewer** at the button of the window.

Search result item properties

The search result item properties work similarly to all other artifact property panes in the product, e.g. inside **Artifacts** window.

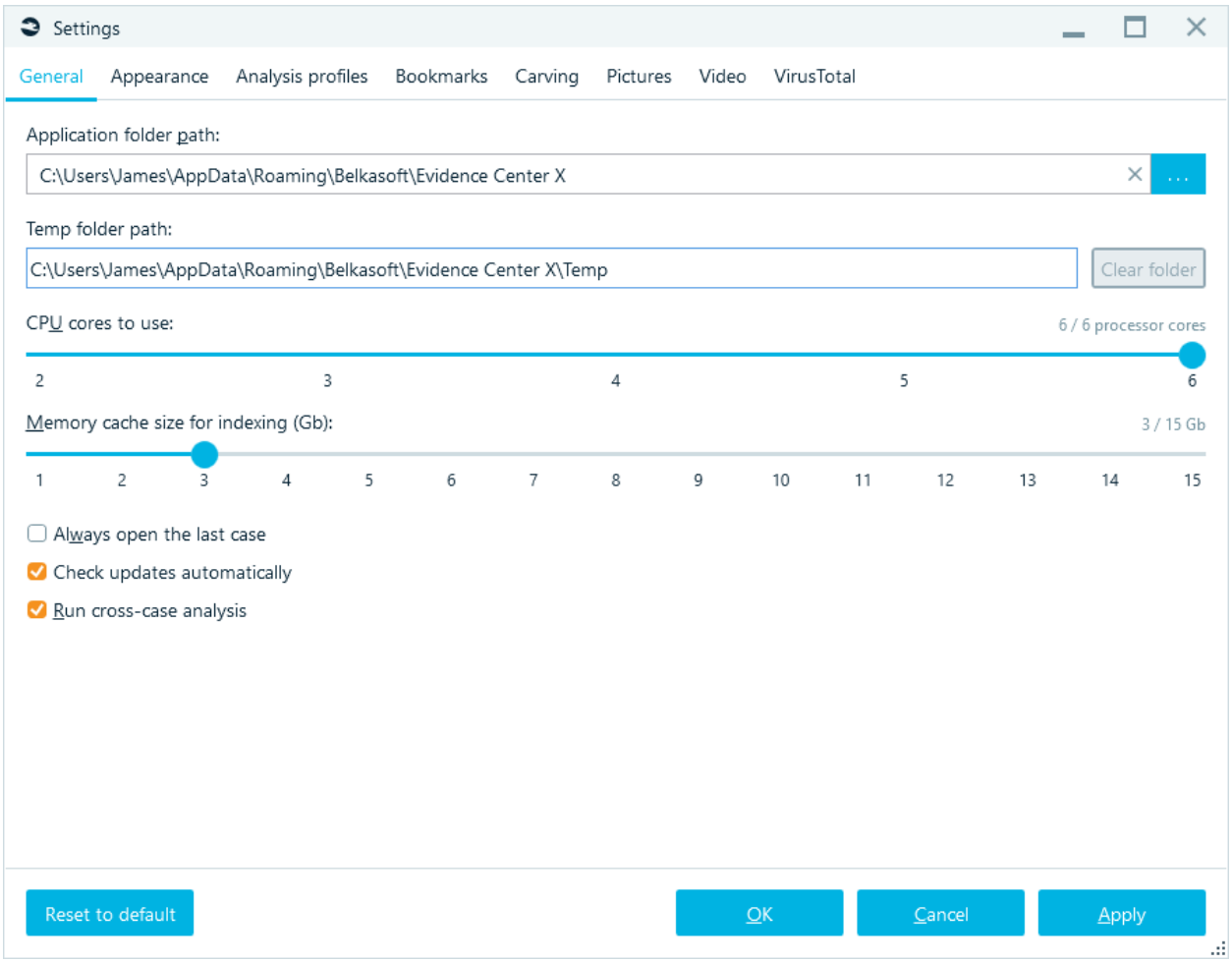
Cross-case search

Belkasoft X allows you to search for matches between the current case and older cases. The following types of data can be searched:

- Email addresses
- Phone numbers
- Application UINs and profile names

Run cross-case search

To enable cross-case search, switch on **Run cross-case analysis** option at the first **General** tab of **Settings** window:



Reviewing geolocation data

Belkasoft X allows you to work with various artifacts having geolocation data inside.

Which artifacts might have geolocation properties?

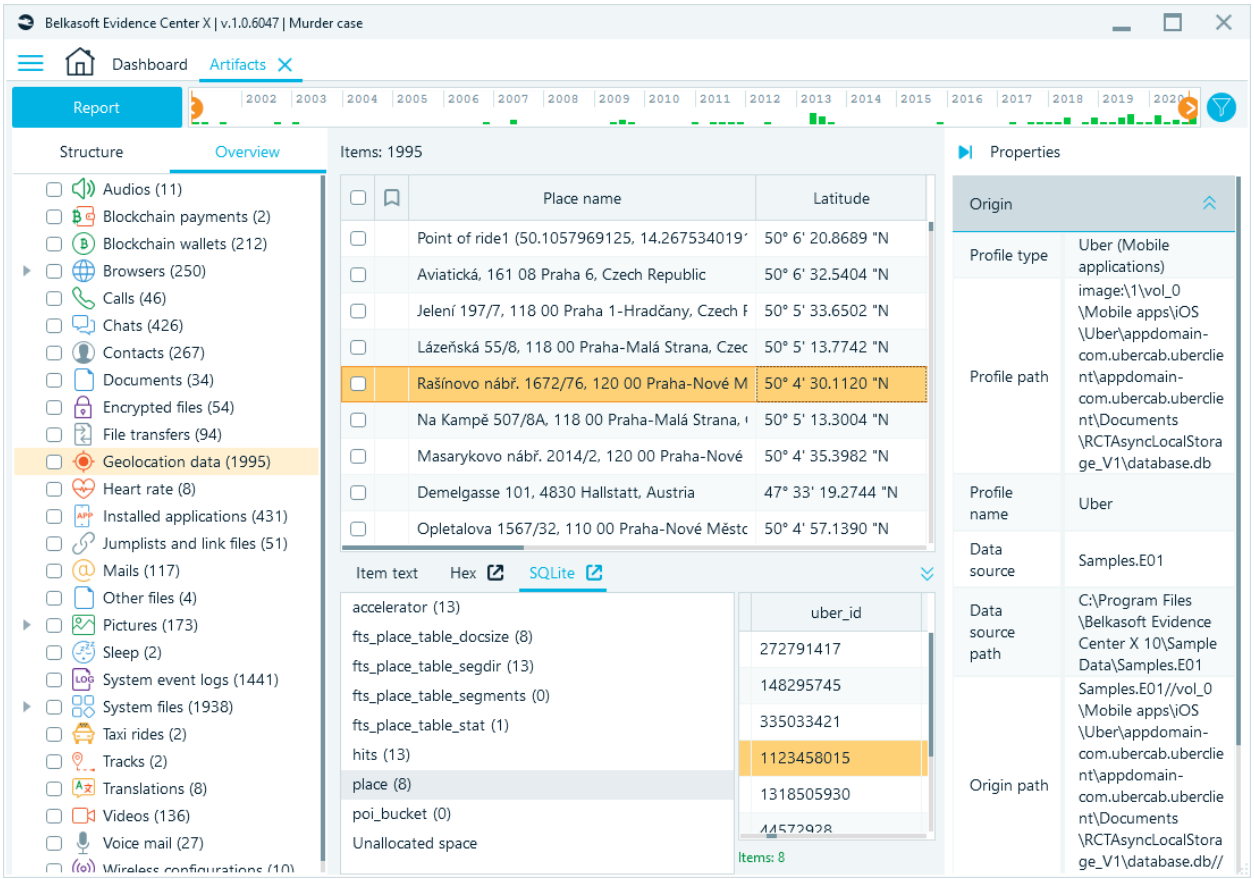
The following artifacts supported by Belkasoft X may have geolocation data:

- **Pictures**. If a picture is shot using a modern smartphone with GPS module, its EXIF properties will contain geolocation data, which will be extracted by the Belkasoft X.
- **Online map search results**. If Google Maps or a similar services were used in a browser, search result links will contain geolocation data. Such links will be processed during browser analysis, and the geodata will be extracted.
- **Mobile map apps**. Such apps (including mobile Google Maps) may store the users recent searches, favorites and routes, which will be extracted by Belkasoft X.

- **Taxi apps**. Taxi apps such as Uber or Gett may store your ride history, including start and finish points, user searches and favorites.
- **Chat apps**. Some chat apps allow to share user location with their peers and this info can be extracted.
- **Fitness tracker apps**. Some trackers may store tracks of user activities such as jogging.
- and many other artifacts.

Geolocation data node

To review all geolocation artifacts found by Belkasoft X, you should open **Artifacts** window, select **Overview** tab, and find **Geolocation data** node. Geolocation data is not shown on **Structure** tab.



The artifact list for **Geolocation data** nodes contains the following columns:

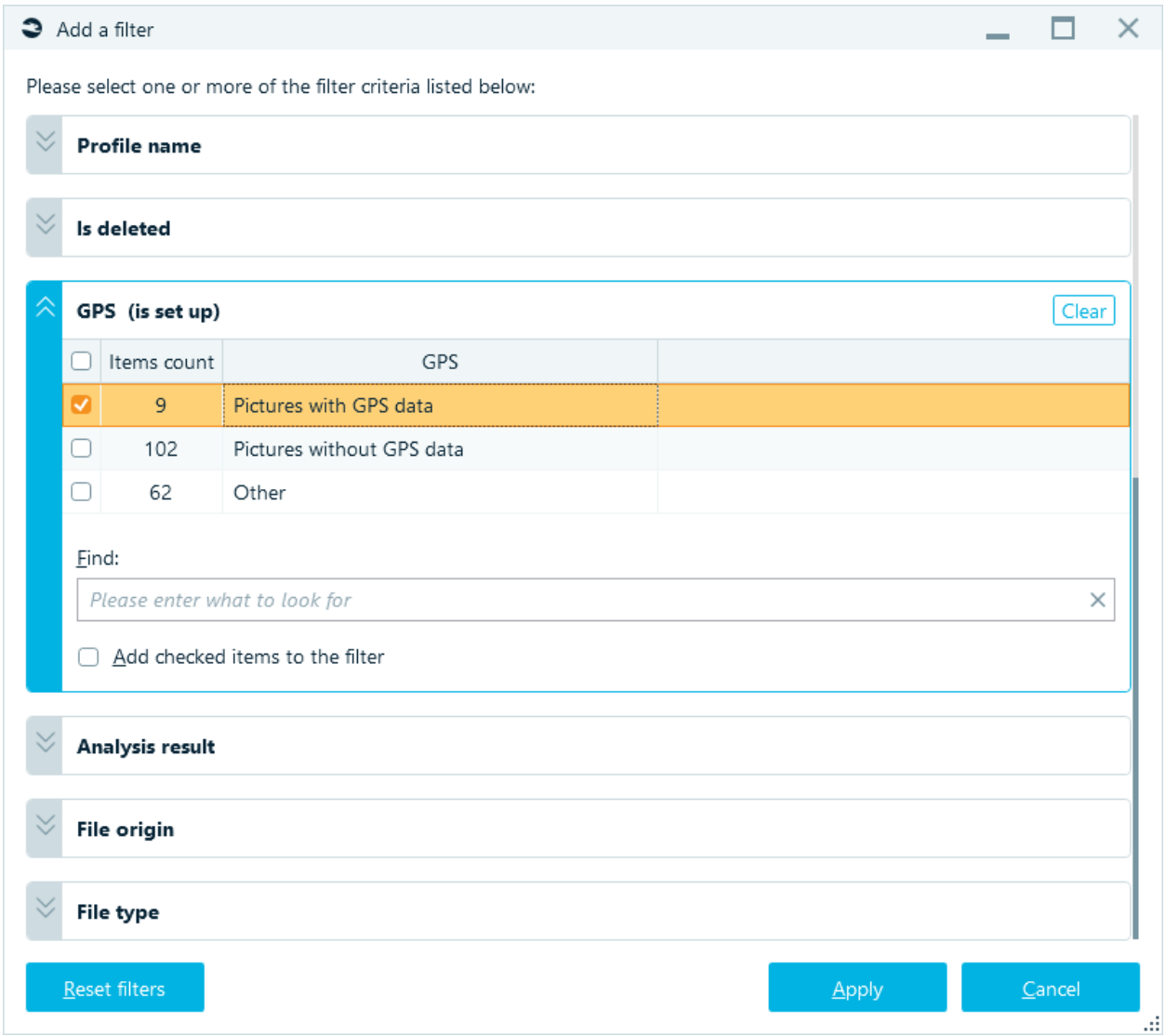
- **Place name**. Can be a name (if this is a favorite in some app) or a link (if this is Google Maps search or similar).
- **Latitude** and **Longitude**. These are coordinates of a corresponding point.
- **Latitude2** and **Longitude2**. These are second coordinates for stored offline maps. Some apps allow a user to store map for offline browsing, two coordinates of saved map corners are stored.
- **Origin type**. This column displays where corresponding location came from: a browser URL, a picture, an app bookmark or favorite and so on.

Other columns are not geolocation-specific (e.g. data source, profile and origin path).

Pictures with GPS

Pictures with GPS are of a particular interest. Since pictures may have both geolocation and time, it is possible to track a person's route using these properties. You can find all pictures with GPS coordinates by the following steps:

- Navigate to **Overview** tab of **Artifacts** window.
- Select **Pictures** node at the left.
- Add a filter **Pictures with GPS data**:



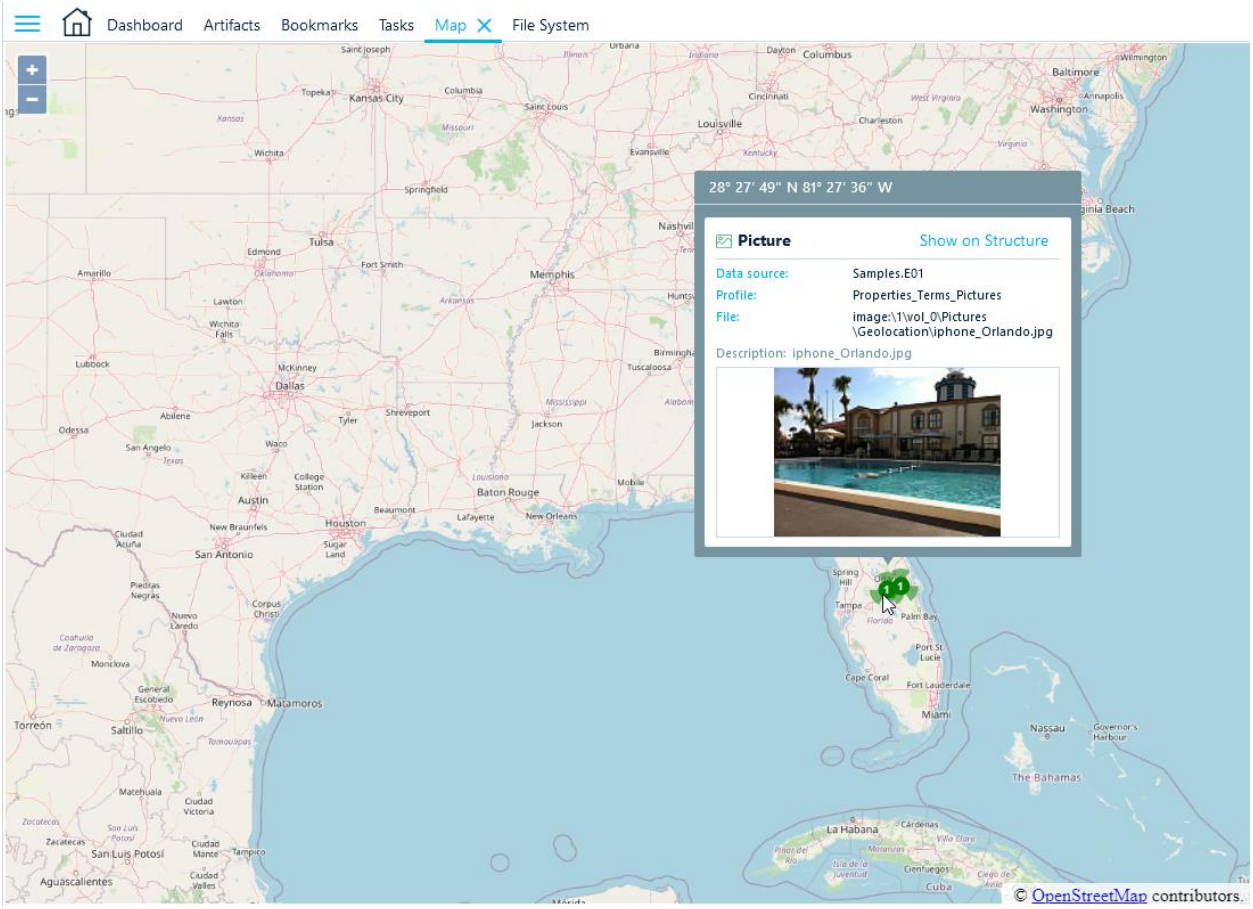
Showing geolocation artifacts on Open Street Maps or Google Earth

Belkasoft X allows you to review artifacts having geolocation on Open Street Maps (if you have an Internet connection) or Google Earth (if you have it installed locally). To do so, you can

- right click corresponding node on **Overview** tab (such as **Geolocation data**, Browser **URLs**, or **Pictures**) and select **Show on Map** or **Show on Google Earth** menus.

- check particular artifacts in the corresponding artifact list, right click and select **Show on Map** or **Show on Google Earth** context menu item.

If you selected Open Street Maps and you have Internet connection, the product will show you all chosen artifacts on a map:



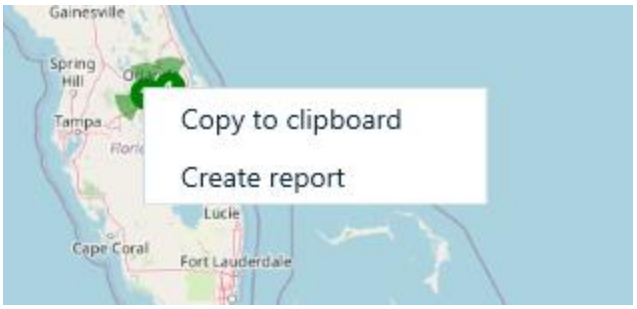
On this picture, you can see two locations, clustered into two green points. You can zoom in and see these locations separately.

The map inside **Open Street Maps** window has the same controls as Open Street Maps in a browser. You can zoom in or out by using mouse wheel or +/– buttons, Map or Satellite views are also available, as well as other features.

If you click on any particular location or a cluster, you will see a tooltip or several tooltips, showing properties of each location. **Show on Structure** navigates you to the item in Structure tab.

You can create a report of a selected map view by right clicking on the map and selecting **Create report** context menu item. Along with artifact location properties, a current view will be included into the report.

You can also copy the current view as a picture by using **Copy to clipboard** context menu item. You may then paste it to any graphical editor, document or even a chat.



Exporting geolocation artifacts to KML format

If you have neither Internet connection nor Google Earth installed, you can still review geolocation artifacts on a map. To do so, you can export locations to KML format. Select corresponding node in **Artifacts** or check needed items in a corresponding artifact list, choose **Export checked items to Google Earth format** in its context menu.
Another option is to choose **Create report** menu item and opt for KML format in the list of target formats.
As a result, the following XML file in KML format is generated:

```
<?xml version="1.0" encoding="utf-8"?>
<kml xmlns="http://www.opengis.net/kml/2.2">
  <Document>
    <Placemark>
      <name>https://www.google.com/maps/@51.5039926,-
0.1022688,16z?hl=en</name>
      <description />
      <Point>
        <coordinates>-0.1022688,51.5039926</coordinates>
      </Point>
    </Placemark>
    <Placemark>
      <name>https://www.google.com/maps/place/Tower Bridge/@51.5039526,-
0.0889865,16z/data=!4m2!3m1!1s0x0000000000000000:0x9e78421a085a6f2d?hl=en</na
me>
      <description />
      <Point>
        <coordinates>-0.0889865,51.5039526</coordinates>
      </Point>
    </Placemark>
  </Document>
</kml>
```

Such a file contains the place coordinates and their names (URLs or bookmark name used in an app) and does not contain any specific data about the device, its user or your case. It is safe to expose such file to the Internet so you can review its contents in any online KML file viewer.

Filtering data

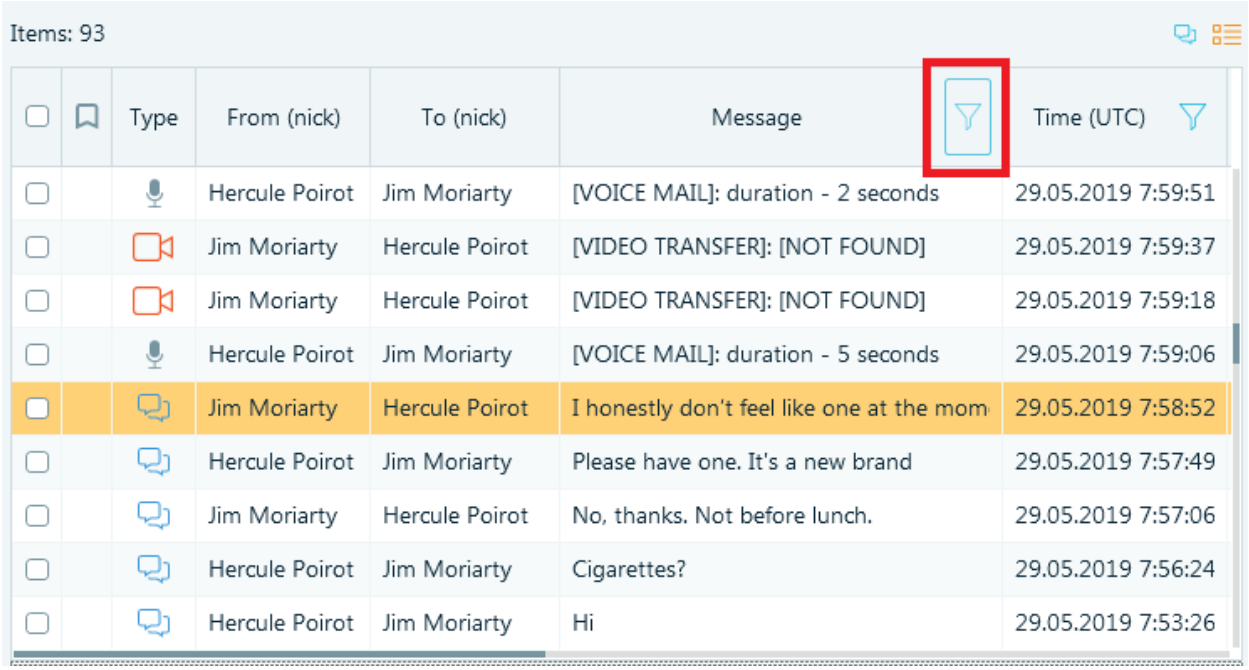
Once you have various artifacts extracted, you will most likely need to find the needle in a haystack. A typical case nowadays can contain hundreds of thousands and even millions of items, and to limit the

number of artifacts to review, you will need use Belkasoft X filtering functionality.
You can filter almost any artifact list in Belkasoft X, such as artifact lists in **Artifacts**, **Connection Graph**, and maybe the most importantly (since it typically has the largest number of items) **Timeline**.
Note: **Tasks** window has its own mechanism of filtering. For more on that, see "Tasks" chapter.
Examples of useful filters you can create with Belkasoft X are:

- Filter visited URLs to see only social network links.
- Filter visited URLs to see only search engines links and used search terms.
- Filter pictures having geolocation properties.
- Filter pictures found inside documents (exclude pictures found as separate files or using carving).
- In **Artifacts Overview**, filter chats originated from Skype accounts only.
- Filter pictures having faces, skin or scanned text inside.
- Filter emails having attachments or documents having embedded files.
- and many more other useful filters.

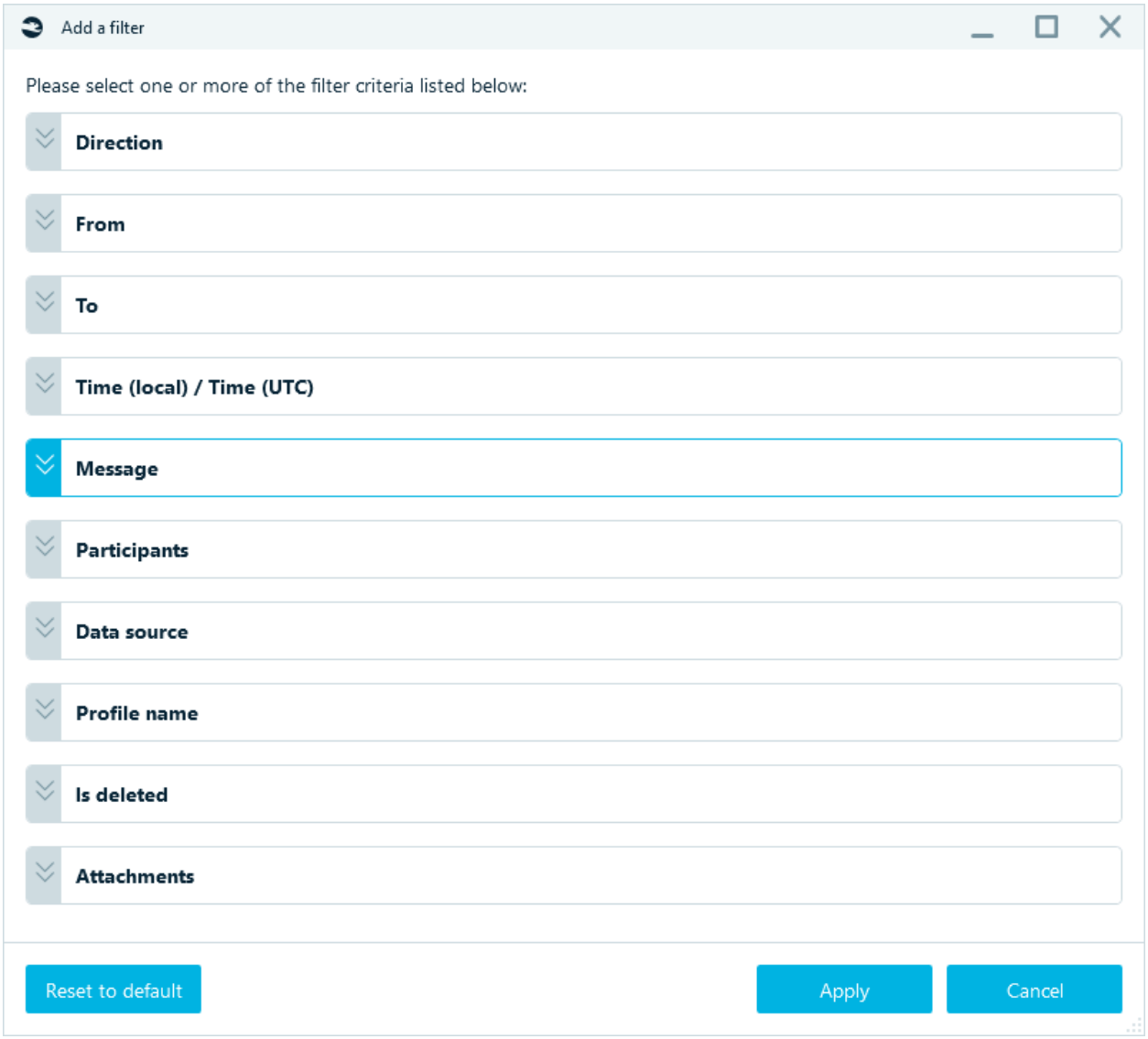
Creating a filter

There are two ways to create a filter. You could create a global filter (navigate to **Creating a global filter** to learn more) or filter a particular artifact list.
If you would like to create a local filter, click a funnel icon inside a column header to create a filter:

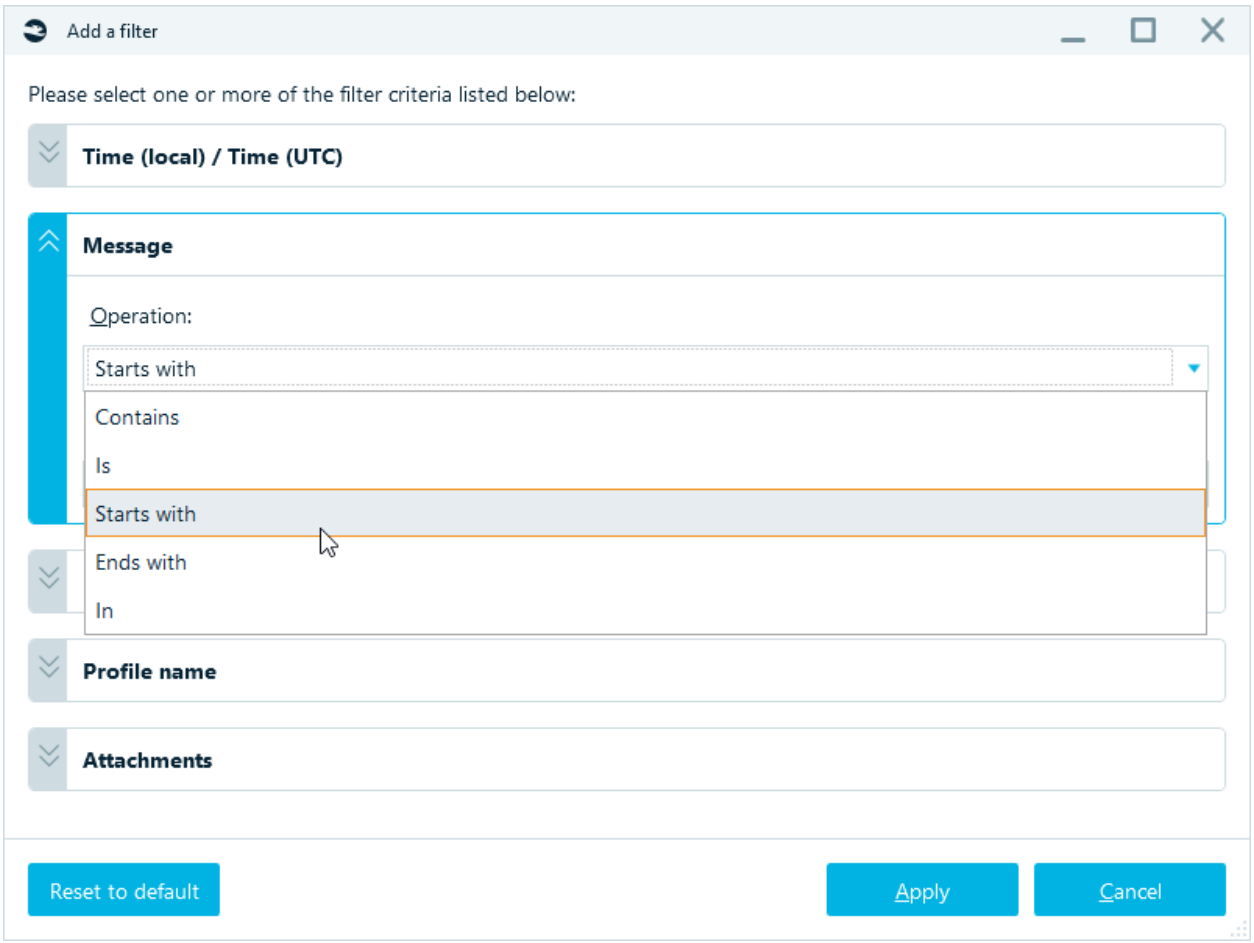


*If you click on the selected funnel icon, a filter by **Message** column will be created*

That will open **Add a filter** window:

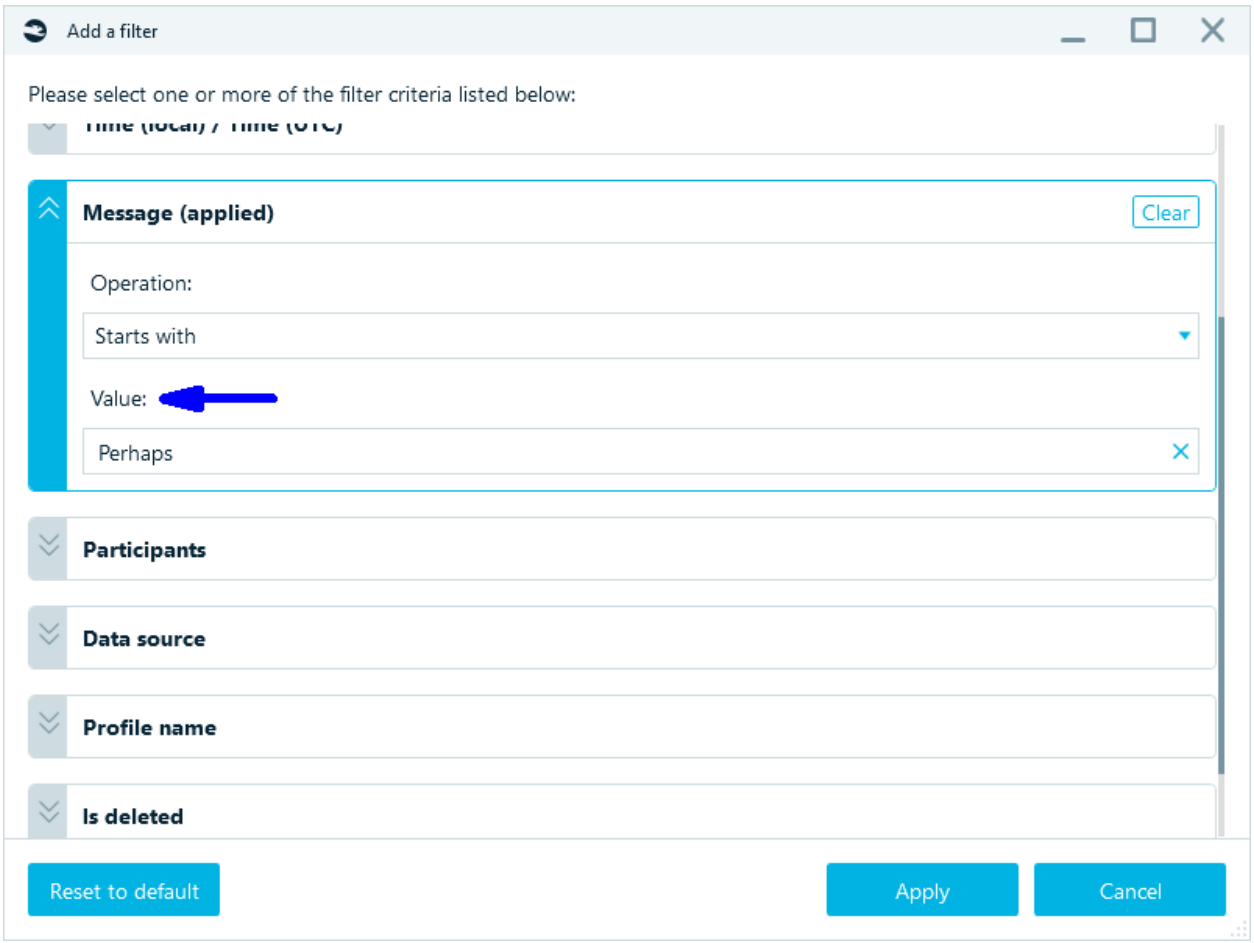


On this window, you can see various criteria: **Direction**, **From, To**, **Time (UTC) / Time (Local)**, **Message**, **Participants**, **Data source**, **Profile name, Is deleted, Attachments**. The set of available criteria depends on type of artifacts you decided to filter.
Click on any filter bar to configure corresponding criterion.
On the screenshot, you can type a part of message you are looking for:



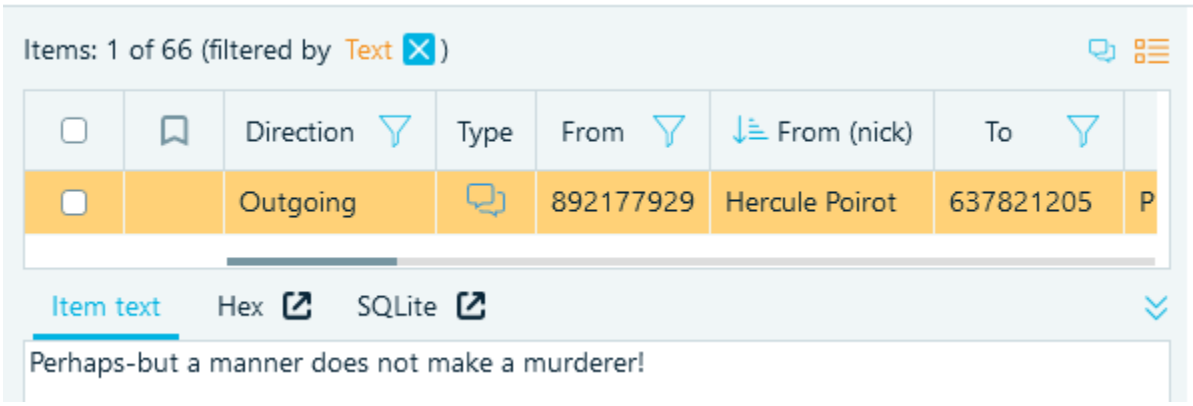
Select **Operation**:

- **Contains** - search value can be anywhere in the word
- **Is** - search word exact match
- **Starts with** - search word starts with
- **Ends with** - search word ends with
- **In** - set several conditions at once line by line

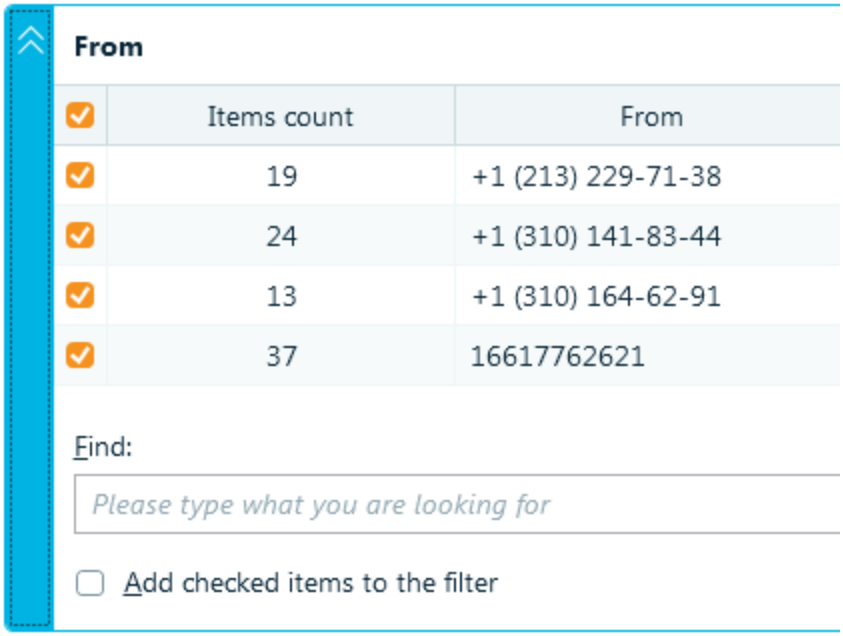


And set **Value**.

When you done with configuring criteria, click **Apply** button. The list will be filtered, and the applied filter will be highlighted:



If you select the **From** filter, you can select the senders to show messages from:



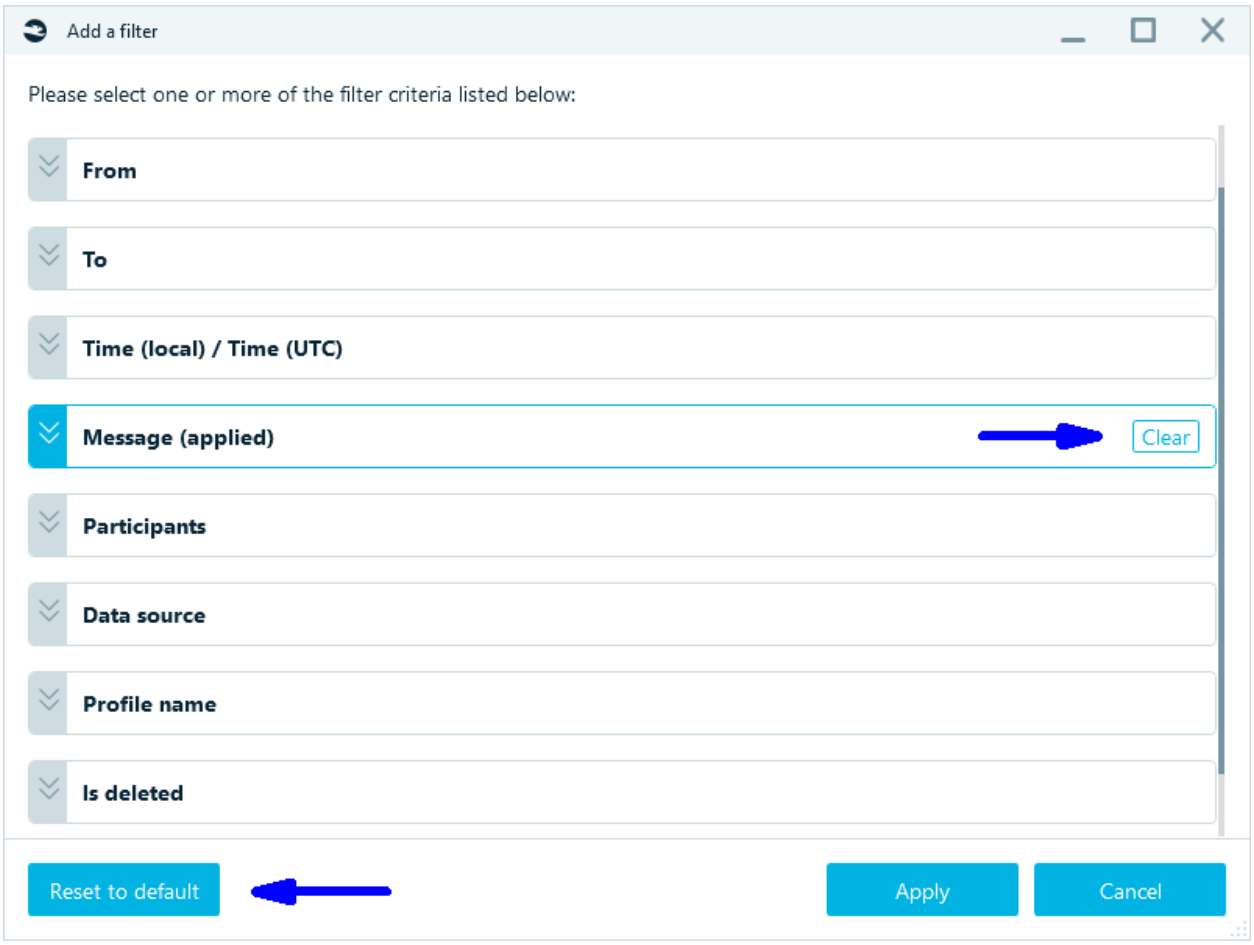
You can select all, none, or some of message senders using the leftmost checkbox column. In the **Items count** column you can see a total amount of messages from this sender. Finally, the **From** column shows the sender information.

Editing existing filter

You can edit existing filter by clicking the funnel  icon again. This will open the same **Add a filter** window with the corresponding filter options. You can change values set for corresponding criterion or even add more criteria.

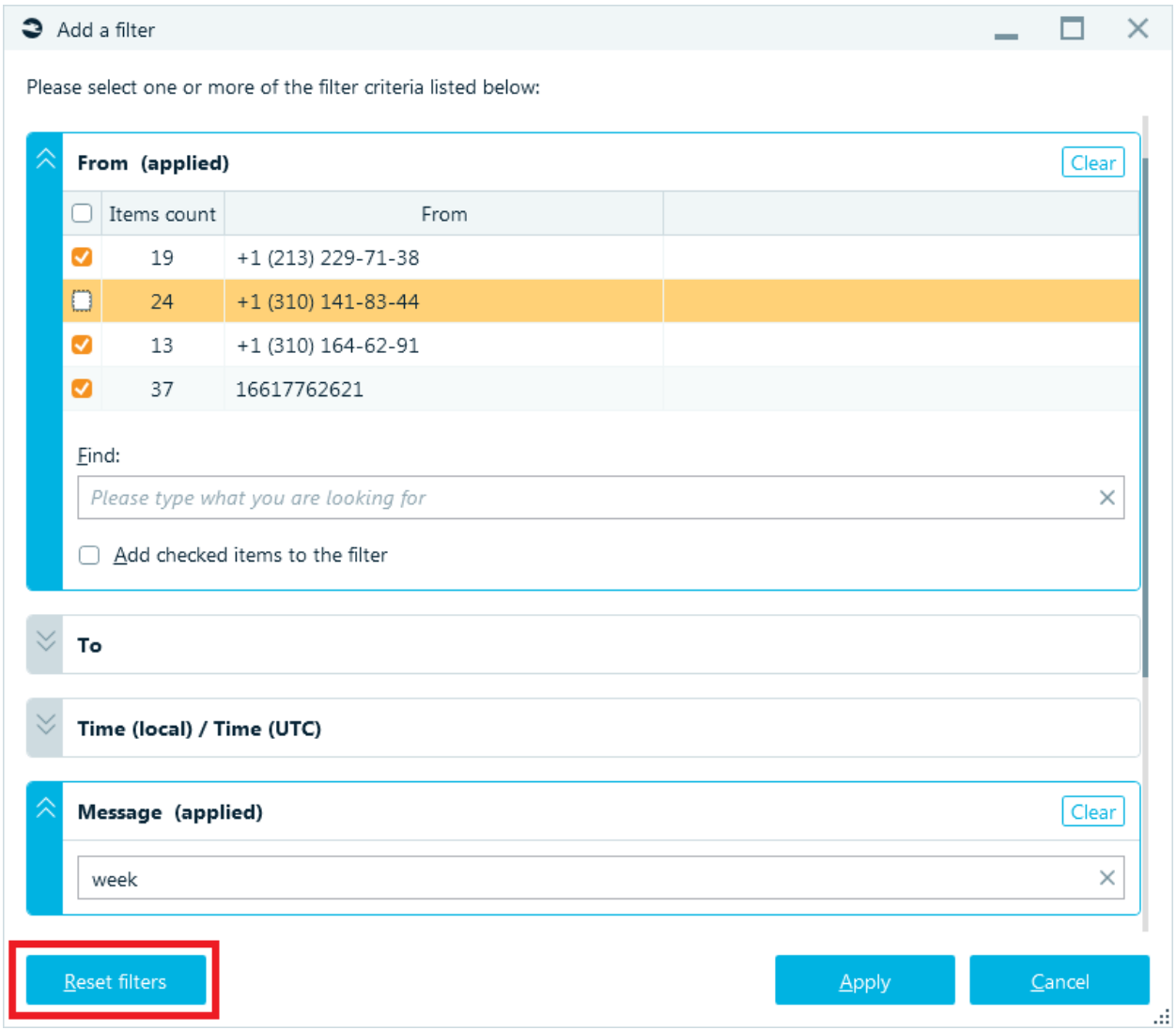
Deleting filter

You can remove filters using **Clear** (for particular filters) or **Reset to default** (for all filters) buttons in **Add a filter** window.



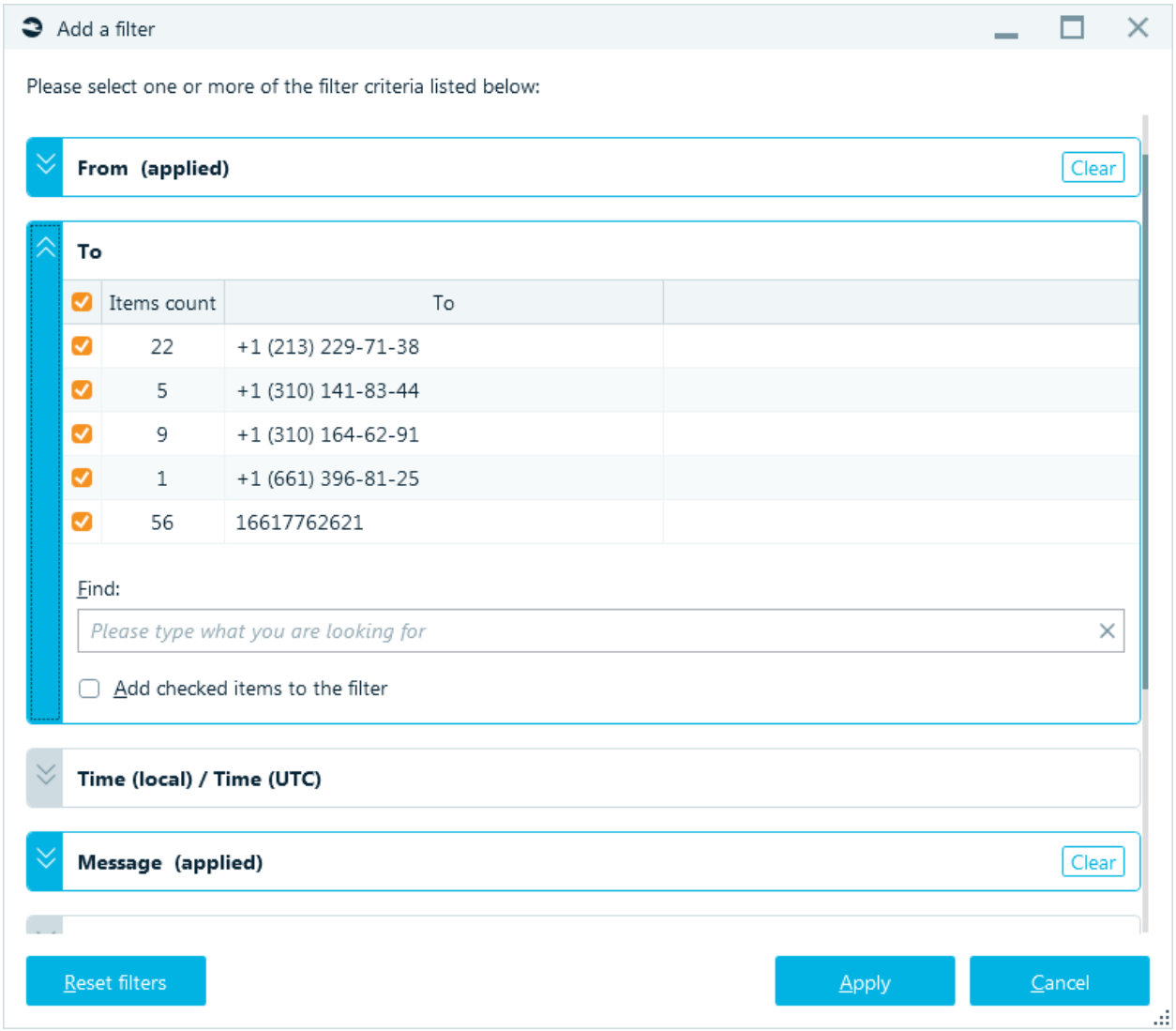
Resetting all filters

You can reset all filters by using **Reset filters** button in **Add a filter** window.



Adding multiple criteria

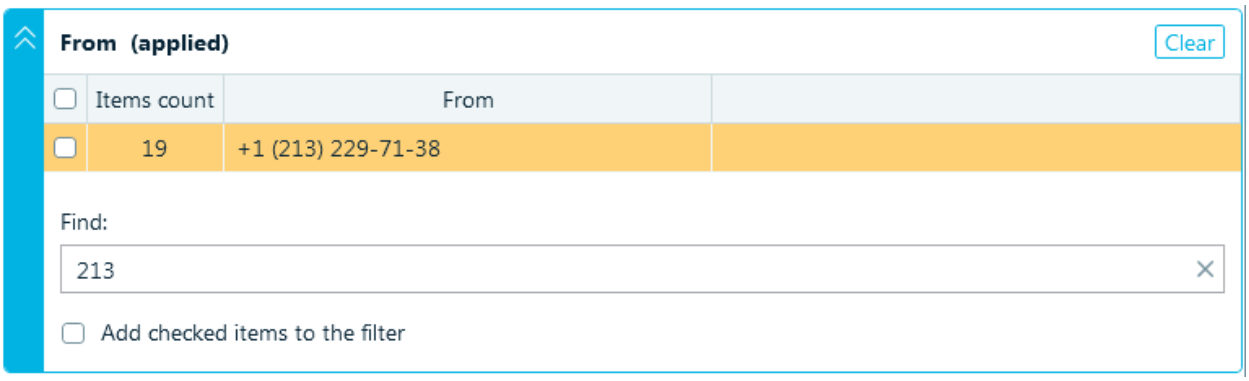
Using **Add a filter** window, you can specify multiple criteria. Once you configured a first criterion, you can click on another one and tune it. All configured criteria will be highlighted with blue color and marked as 'applied'; this helps you to see which ones are edited and which ones are not:



*On the screenshot **From** and **Message** criteria are configured and thus highlighted with blue color and marked as applied*

Finding and adding multiple values to a criterion

Criteria based on a selection from a list allow you to filter that value list. This is important when a list of possible values is potentially immense, such as a list of all contacts or all profiles. Lists of these types can contain hundreds and thousands of items, so you need a filter just to find a needed value. For this purpose, all lists inside **Add a filter** window contain **Find** text box. Once you put something inside this text box, the corresponding list of values is filtered by your input:



*On this screenshot, a list of senders is filtered by "213" substring entered into **Find** text box, so only one sender is shown, matching this input*

Now, what if you need to add all senders with telephone numbers containing ‘213’ and ‘310’? Perform the following steps:

- Find "213" using **Find** text box.
- Check all found entries using corresponding check boxes (if they are already checked, do nothing).
- Check **Add checked items to filter** check box.
- Now, do another search by "310" using **Find** text box.
- Check all found entries using corresponding check boxes (if they are already checked, do nothing).
- Click **OK** button.

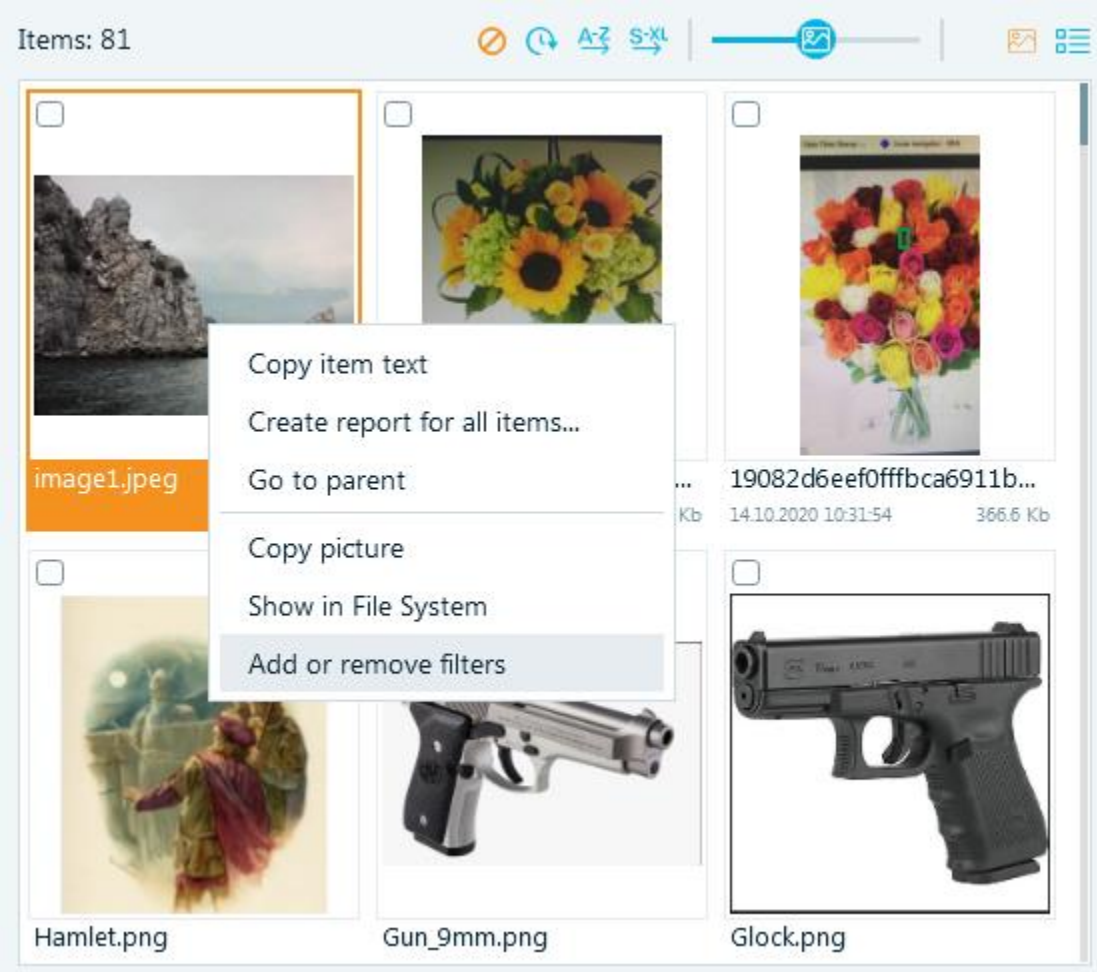
Generated filter criteria

Some criteria appear only after specific kind of analysis performed by Belkasoft X. For example, after you analyze pictures for pornography, skin, guns, faces or texts one additional criterion will appear, namely **Content classification**. Using this filter, you can instruct Belkasoft X to show only pictures with, say, faces found. This criterion is not available without picture analysis performed prior to the filter creation. There are other types of criteria which appear only after corresponding type of analysis.

Managing filters from Gallery view

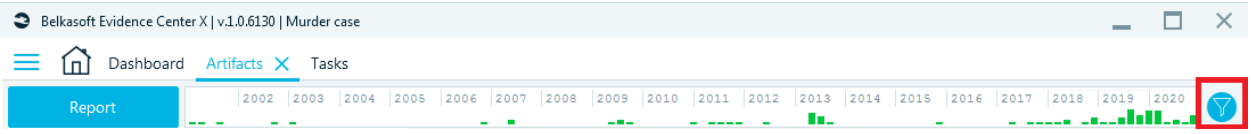
If you are using **Gallery view**, for example, exploring pictures, you could add, remove or modify filters

using a context menu.

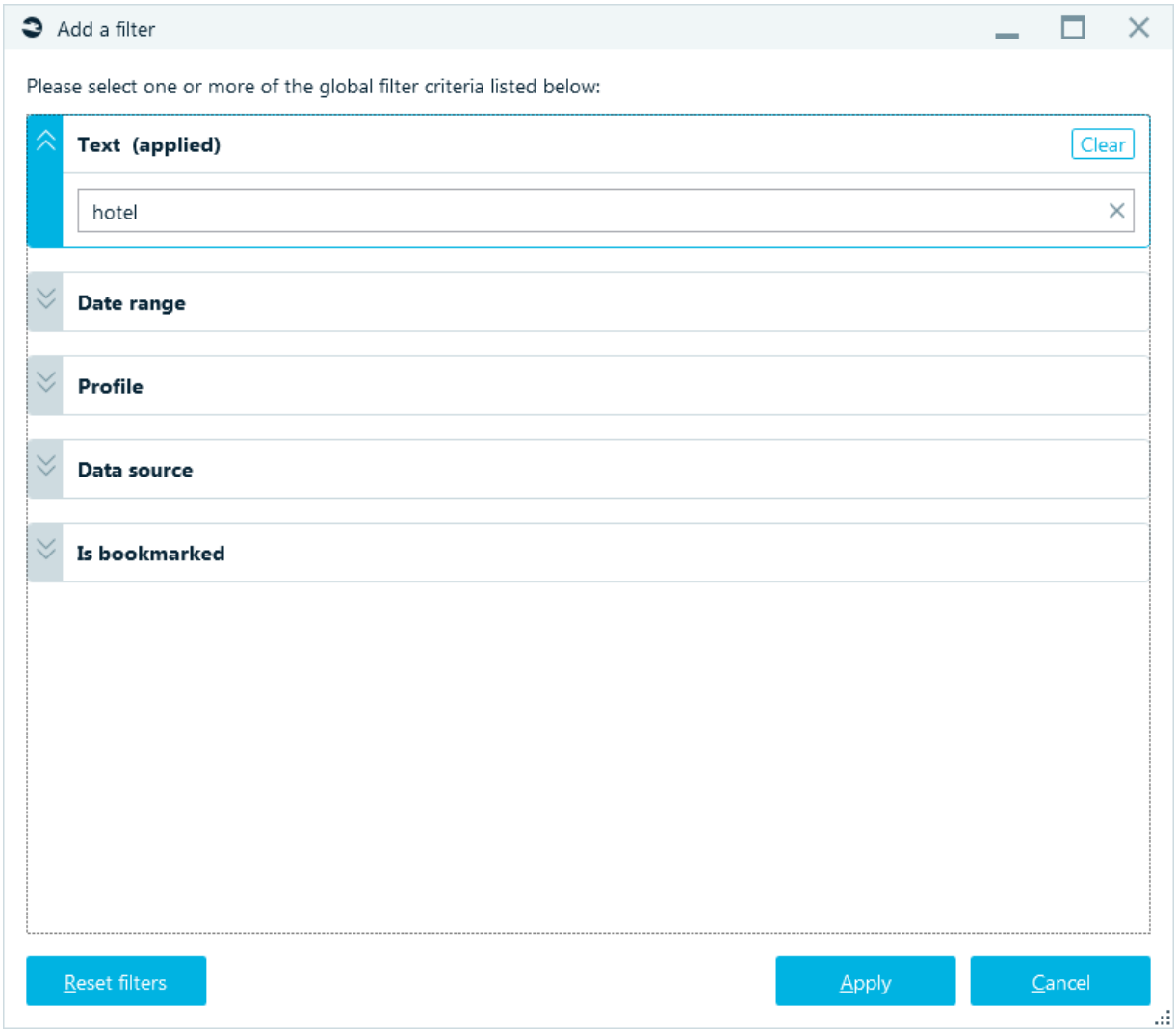


Creating a global filter

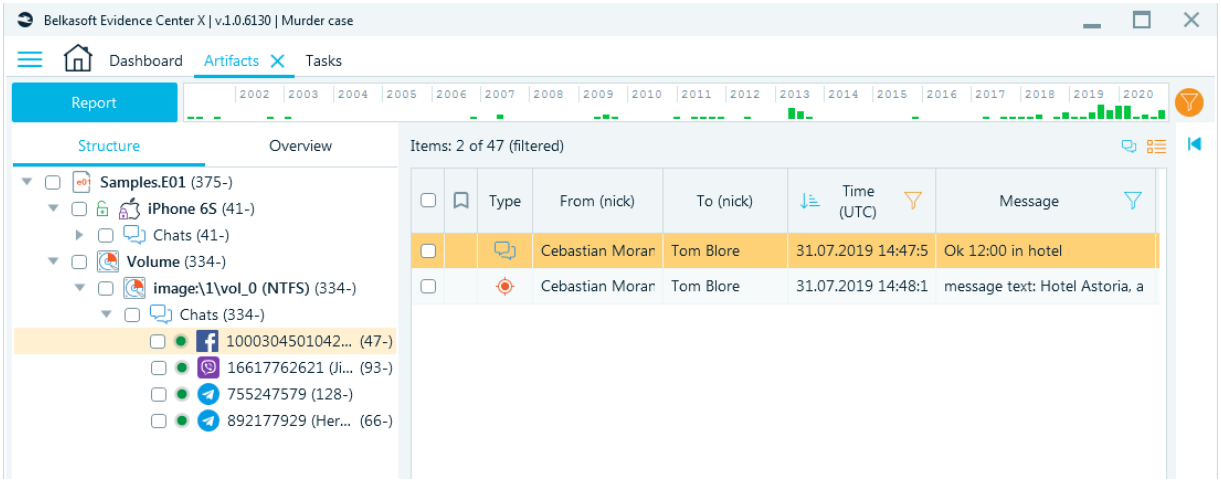
If you would like to create a global filter, use the blue funnel button in the upper right corner.



On this window, you can see the following criteria: **Text, Date range, Profile**, **Data source**, **Is bookmarked**.



After applying a filter, you will see filtered information on **Artifacts** window. Only lists containing relevant artifacts will be shown:

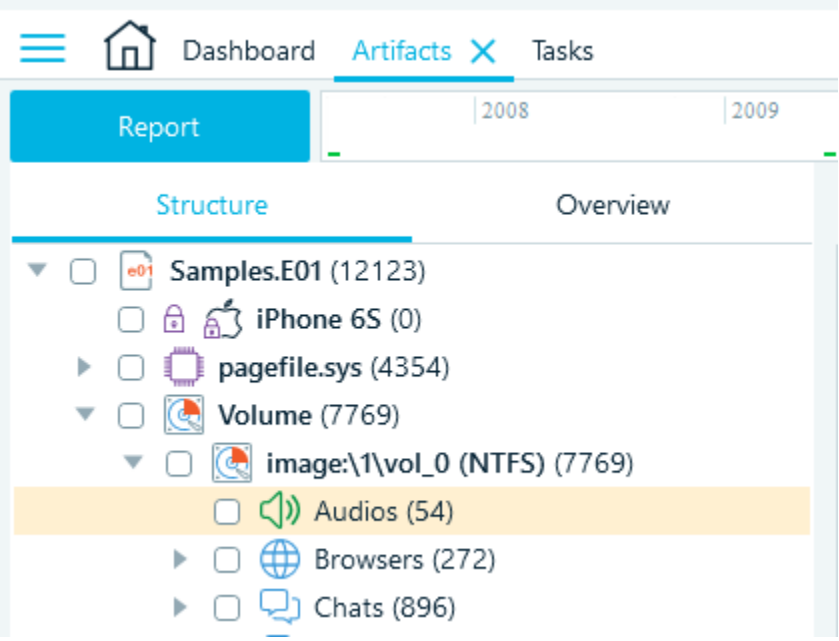


The global filter icon is now highlighted in yellow, indicating that the global filter has been applied. Note that numbers in brackets remain unchanged and indicate how many artifacts were found. The '-' sign means that not all of them are shown at the moment.

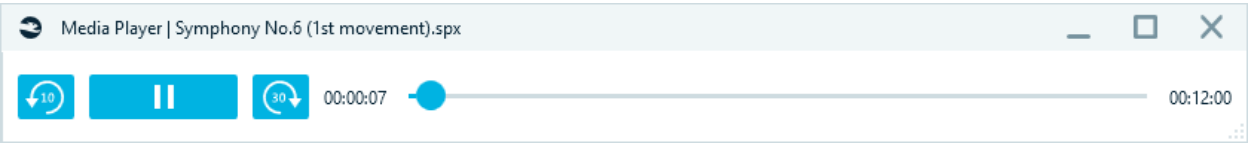
Built-in Media Players

Audio Player

All audio artifacts found in the case are located in the **Artifacts** tab, Audios node.

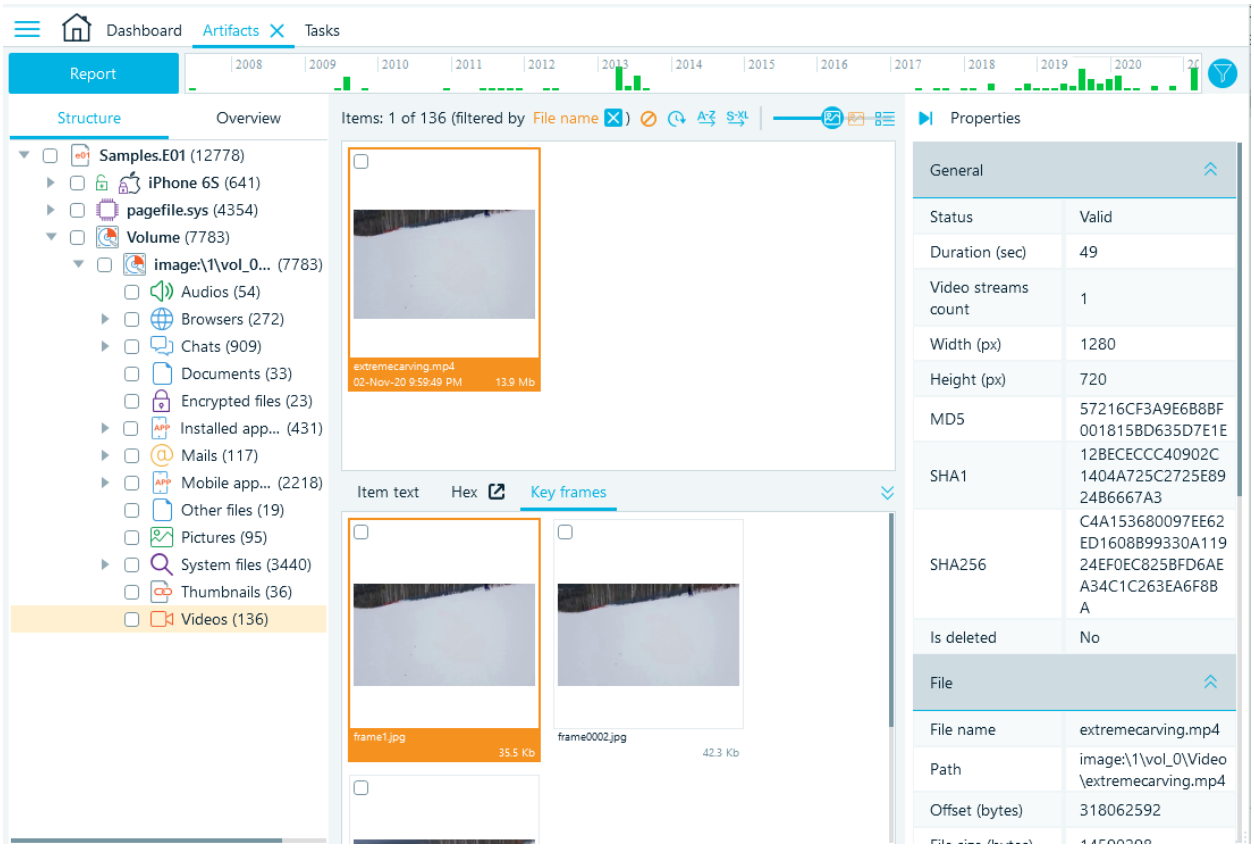


Double-clicking on any audio file opens the **built-in Audio player** for listening.

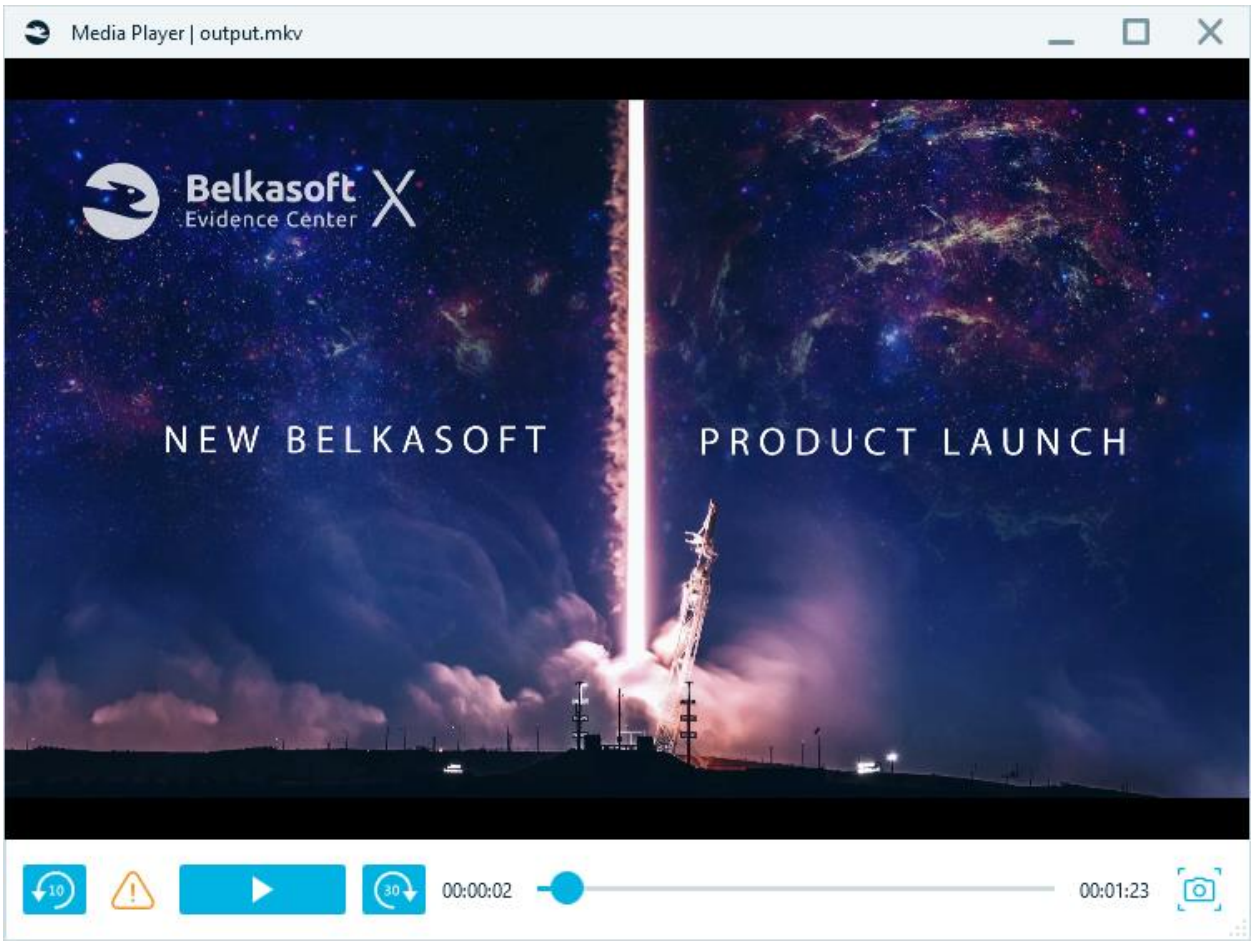


Video Player

All collected video case artifacts are available in the **Artifacts** tab, Videos node.

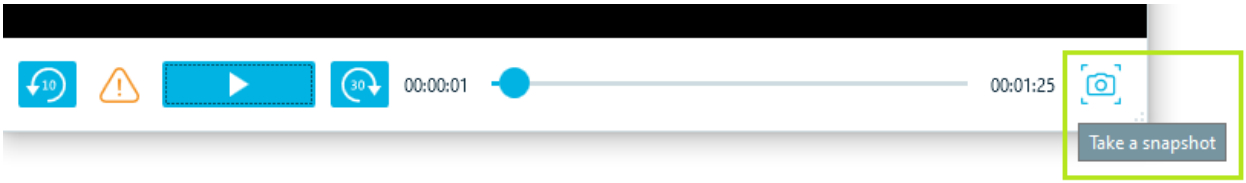


Double-clicking on any video file opens the **built-in Video player**.



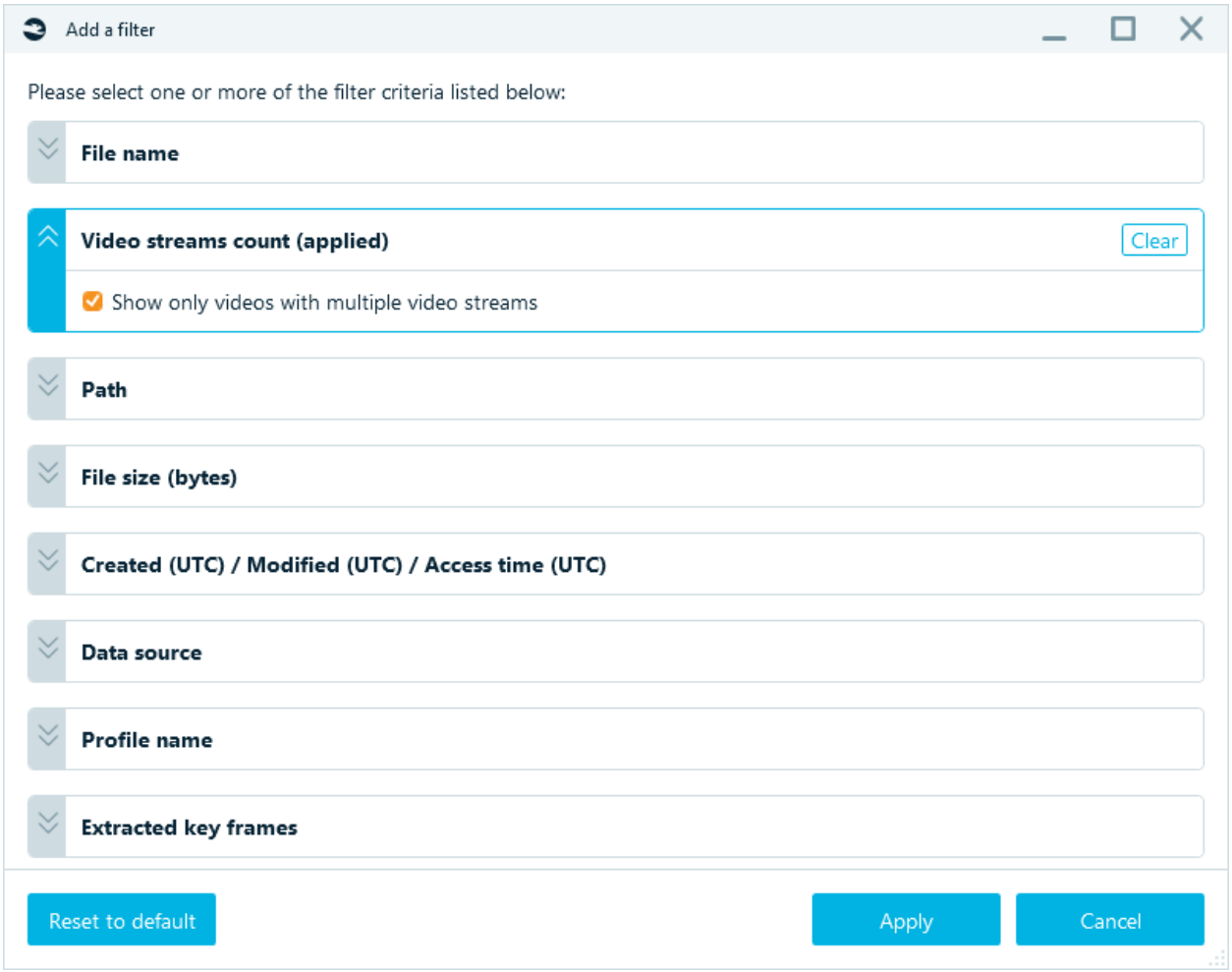
The built-in video player allows to play, pause video, skip forward and backward like a standard video player. However, the most valuable for forensics, it allows to take snapshots and view various video streams if more than one is detected.

To **Take a snapshot** from anywhere in the video, click the camera icon and select the desired location on the disk.



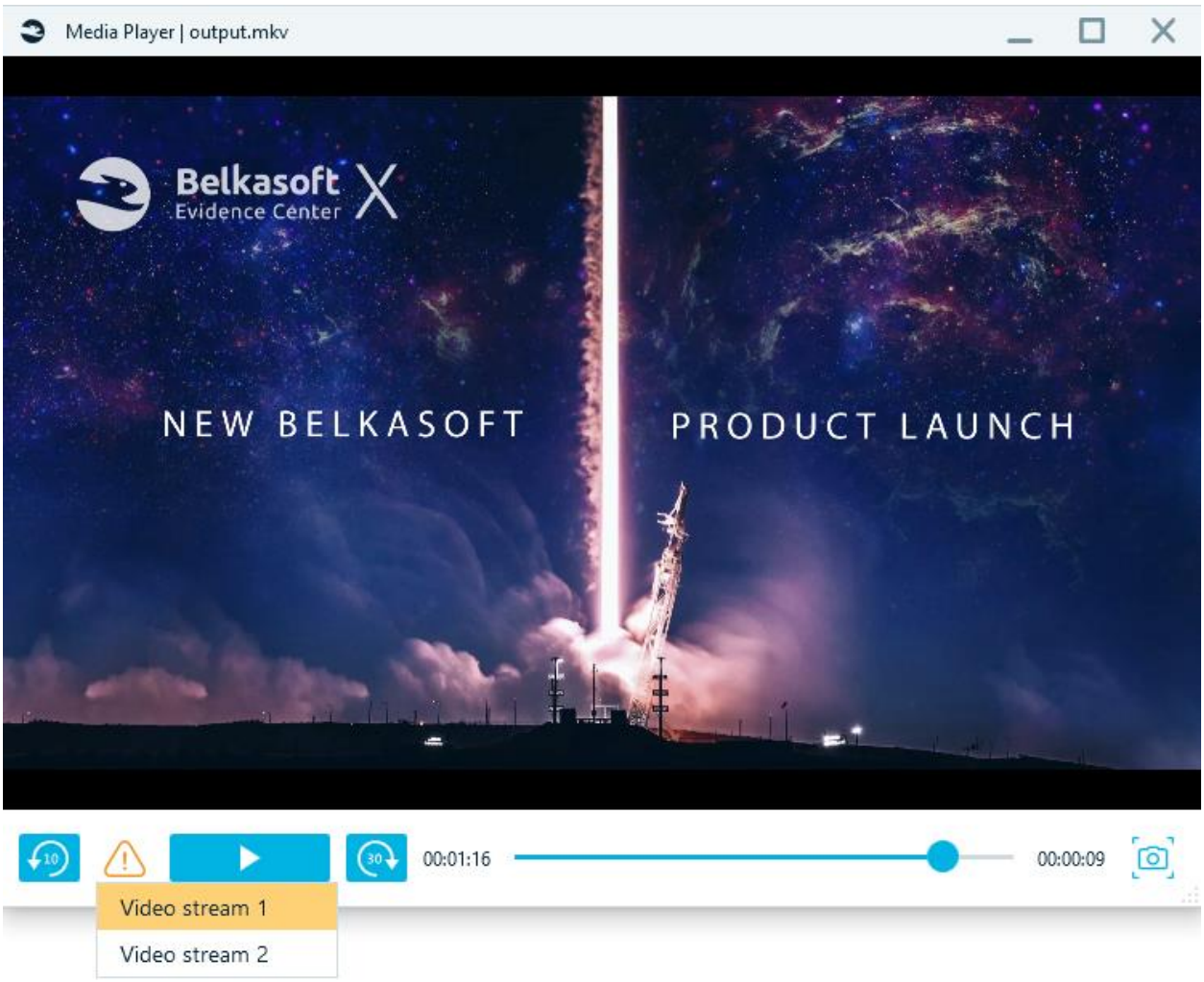
In a digital forensic case, **Multiple Video streams** in the same video file may mean a situation when a CSAM content is hidden. **Belkasoft X video analysis** detects all video streams and allows to quickly switch between them.

In order to see all videos with more than one stream, use the grid filter.

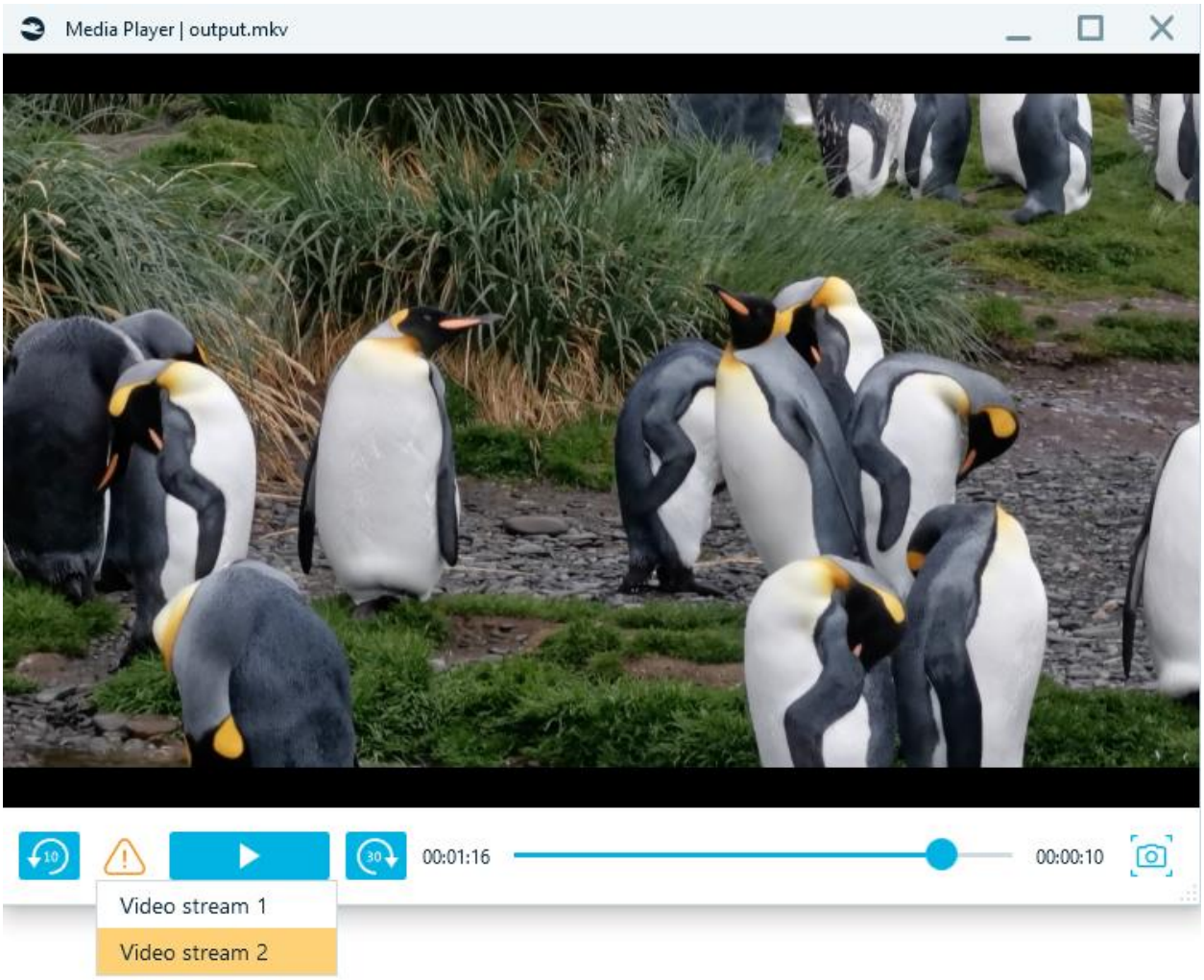


To view different video streams, click the **yellow warning triangle** in the video button bar and view the different streams for data analysis.

Pay attention to the results:
Video stream 1:



Video stream 2:



Hint, if you need to watch the video in another editor, open it from the context menu.

Reports

Creating reports

Belkasoft X allows you to create various types of reports from almost anywhere within the product. There are also many options and customizations available.

How to schedule a report

You can run a report from various places in the tool, for example:

- Any node in **Artifacts** left pane (artifact type list, case list).
- Any single item in any **artifact list.**
- **SQLite Viewer** table list or table data.
- **Connection Graph** window.
- **Open Street Maps** window.
- **Search Results** window.
- **Bookmarks** window or bookmarked artifact list.
- **Tasks** window.

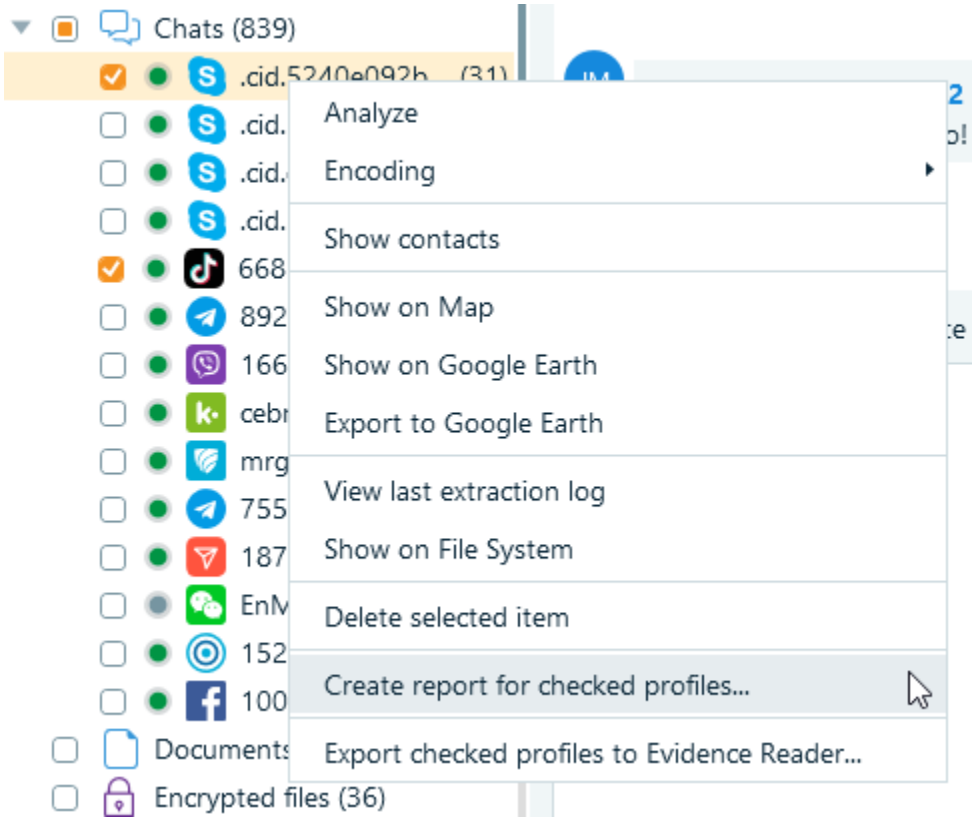
- **Timeline** window.
- **Registry** window branch values.

There are however, some places where you cannot create report from:

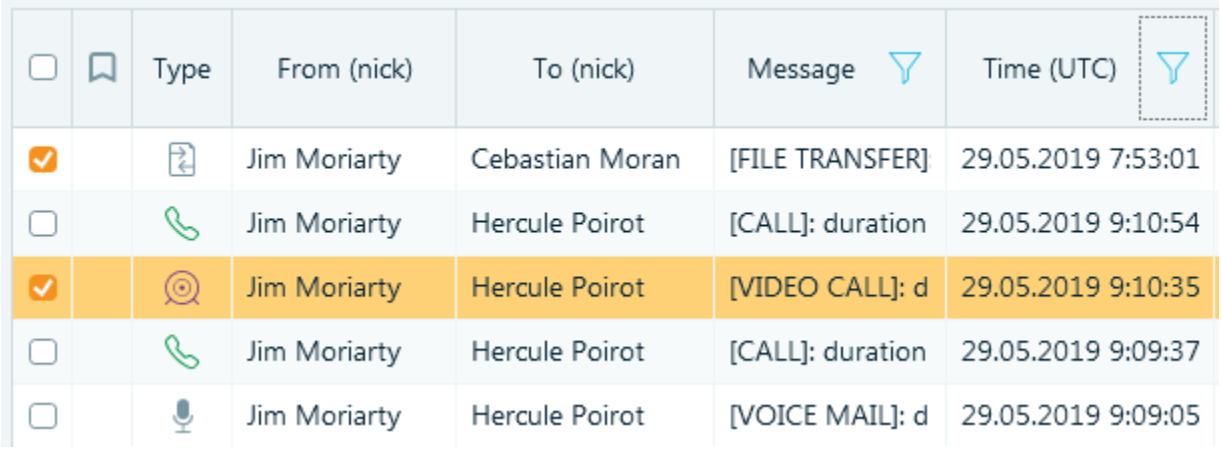
- **Dashboard**
- **File System**
- **Hex Viewer**
- **Plist Viewer**

To schedule a report, do the following:

- Select nodes or items from the item list:
    - If you are creating a report for entire contents of any single node, select it (for example, to create a report for all chats, select **Chats** node in **Artifacts** window)
    - If you are creating a report for several profiles, check them in the tree. You can select profiles of different artifact types, e.g. **Audios** and several chat profiles



    - If you are creating a report for specific artifacts, check them in the corresponding list using leftmost checkbox column:



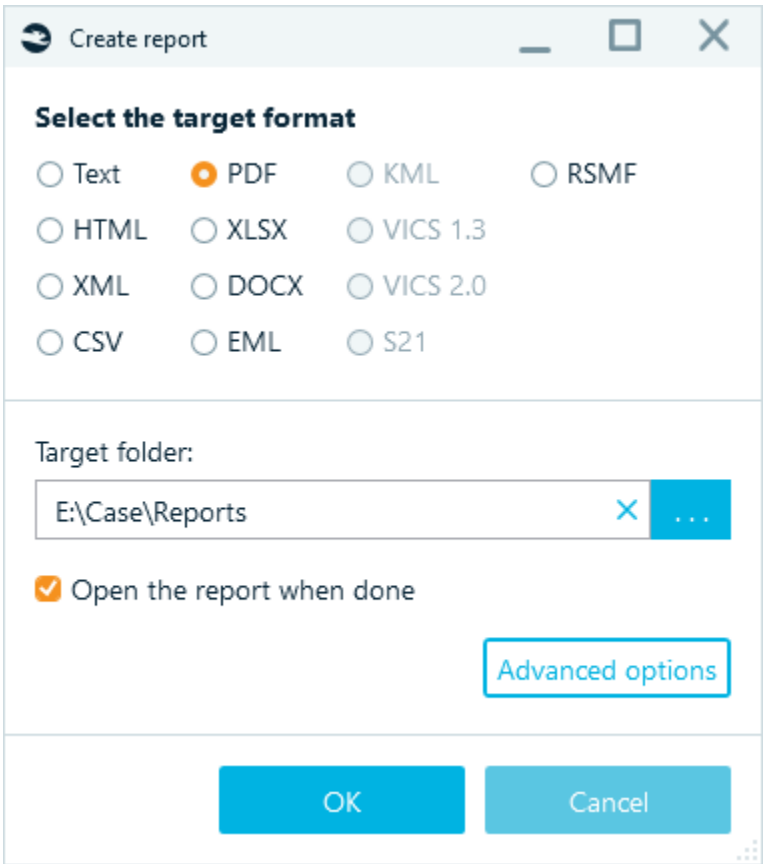
Type	From (nick)	To (nick)	Message	Time (UTC)
	Jim Moriarty	Cebastian Moran	[FILE TRANSFER]	29.05.2019 7:53:01
	Jim Moriarty	Hercule Poirot	[CALL]: duration	29.05.2019 9:10:54
	Jim Moriarty	Hercule Poirot	[VIDEO CALL]: d	29.05.2019 9:10:35
	Jim Moriarty	Hercule Poirot	[CALL]: duration	29.05.2019 9:09:37
	Jim Moriarty	Hercule Poirot	[VOICE MAIL]: d	29.05.2019 9:09:05

On this screenshot two chats are checked for a report

Once you have selected items for the report, select **Create report** item in the context menu (right click on a node or artifact list to show the menu).

Report options

Report options window shown when you selected to create a report, allows you to set basic report options:



Here you can select a target format, such as text, HTML, PDF and others. Some options may be greyed out, like on the screenshot above. This means that for selected artifacts these formats cannot be applied. Such formats as EML are used to export email messages, while KML works for geolocation data. Bubble view for chats can be exported to HTML only.

RSMF or Relativity Short Message Format - allows to export chats and mails in a specific structured format that can be read in Relativity products. The created **.RSMF** file has an encrypted BASE64 part containing a .json file with all data and mails/chats attachments if they exist.

You can also specify a **Target folder**. You choose leave it blank and Belkasoft X will automatically save your report to the default path inside your AppData folder.
Advanced options button provides more options for you to further fine tune your report. These options are listed in the **Advanced report options** section below.
Open the report when done checkbox instructs the product to open reports once they are completed. A default system viewer will be used to open resulting files, so if a report is not open after the task is reported success, check if you have an application bound to the corresponding file extension.

Advanced report options

Advanced report options window allows you to customize your report. It has a number of tabs (depending on which report you are creating), among which are:

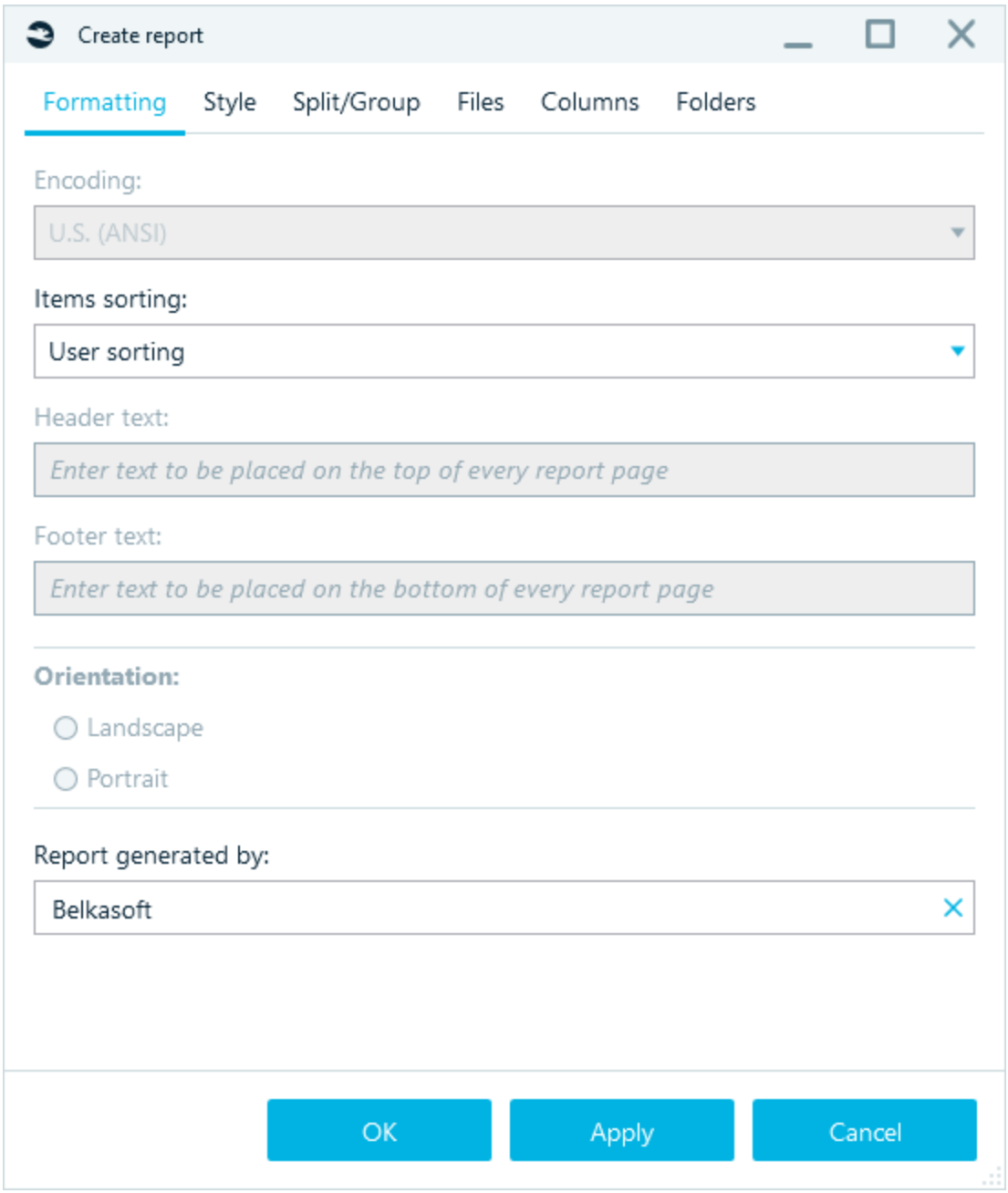
- **Formatting**. provides various formatting options for you to choose, such as sorting or a date format.
- **Style**. Used to specify a logo and fonts.
- **Split / Group**. Helps to split information over multiple files and group artifacts in one document.
- **Files**. Helps to tune file-related options.
- **Columns**. Allows to select which columns to include to a report.
- **Folders**. You can specify the structure of folders for generated report files.

Note: In previous versions of Belkasoft X more tabs were available such as Contacts and Dates. In our latest edition , we found it advantageous to use filters instead. For more info on this topic, see "Filtering data lists".

Formatting

On the **Formatting** tab of **Advanced report options** window, you can specify the following options:

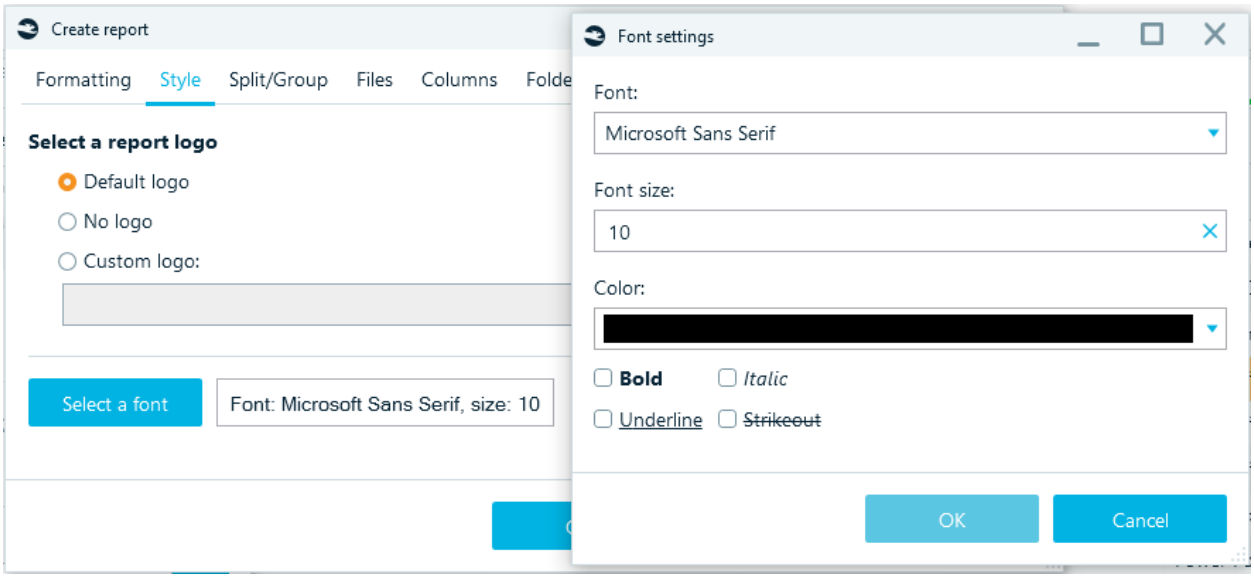
- **Encoding**. If you are creating a report in a text format such as plain text or CSV, you can specify which text encoding to use. Other formats will use UTF8 or Unicode by default.
- **Items sorting**. You can specify to arrange items in the report by time ascending or descending.
- **Header text** and **Footer text** can be only specified for PDF report formats. You can place a text like the investigator’s signature, or any other information required by the rules and regulations of which you follow.
- **Orientation**. You can specify **Landscape** or **Portrait** orientation for formats such as PDF, DOC and RTF.
- **Report generated by**. Use this field to specify a name of a person who generates a report. By default, the same name as specified as the case creator will be used, but you can override this setting.



Style

On the **Style** tab of **Advanced report options** window, you can specify the following options:

- **Default logo**. By default, Belkasoft logo is included into all reports.
- **Custom logo**. Using this option, you can specify your own file to use as a logo on the report.
- **No logo**. You can switch off adding a logo to report files using this option.
- **Select a font**. Set your own font settings (pick a new font, font size, font style and color)

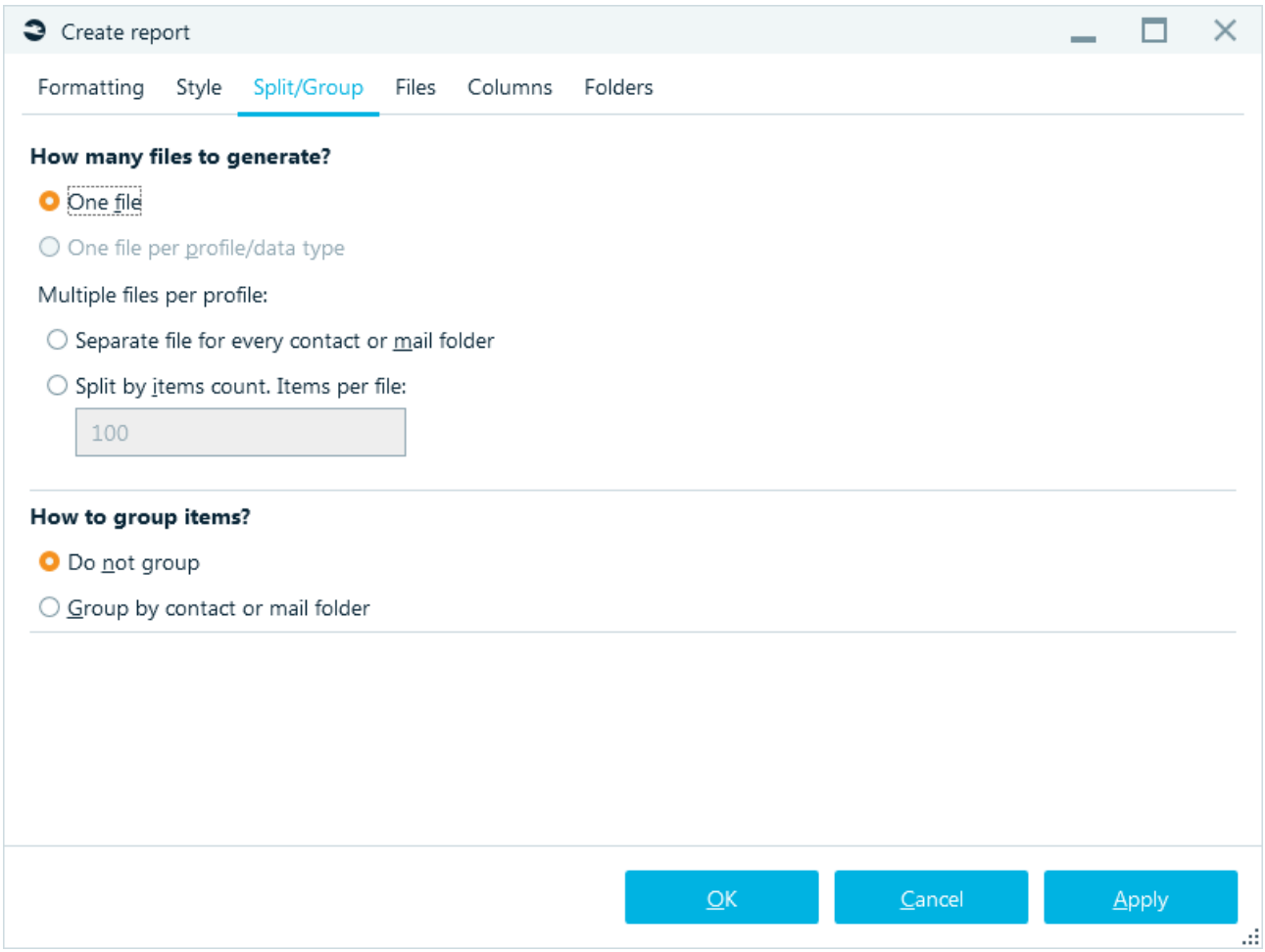


Split / Group

On the **Split/Group** tab of **Advanced report options** window you can specify the following options:

- **How many files to generate?** This setting has the following options:
  - **One file**. A single file will be generated for all selected artifacts. This option would be useful, for example, if you want to have all your case data in a single report file, even if there are artifacts of different types. Note that not every format allows for this option, such as, a report in XML format cannot be created with **One file** option if your case contains heterogeneous data.
  - **One file per profile/data type**. One file will be generated for each profile (for data types having profiles, such as chat apps or browsers) and for each data type (for data types which do not have profiles, such as pictures or documents).
  - **Separate file for every contact or mail folder**. Applies only to chat apps and mailboxes. A separate file will be generated for each participant in chat history and for each separate email folder inside mailbox.
  - **Split by items count. Items per file:…** You can split report into files of a predefined size, not exceeding specified number, say for instance, no more than 500 items in each standalone report file.

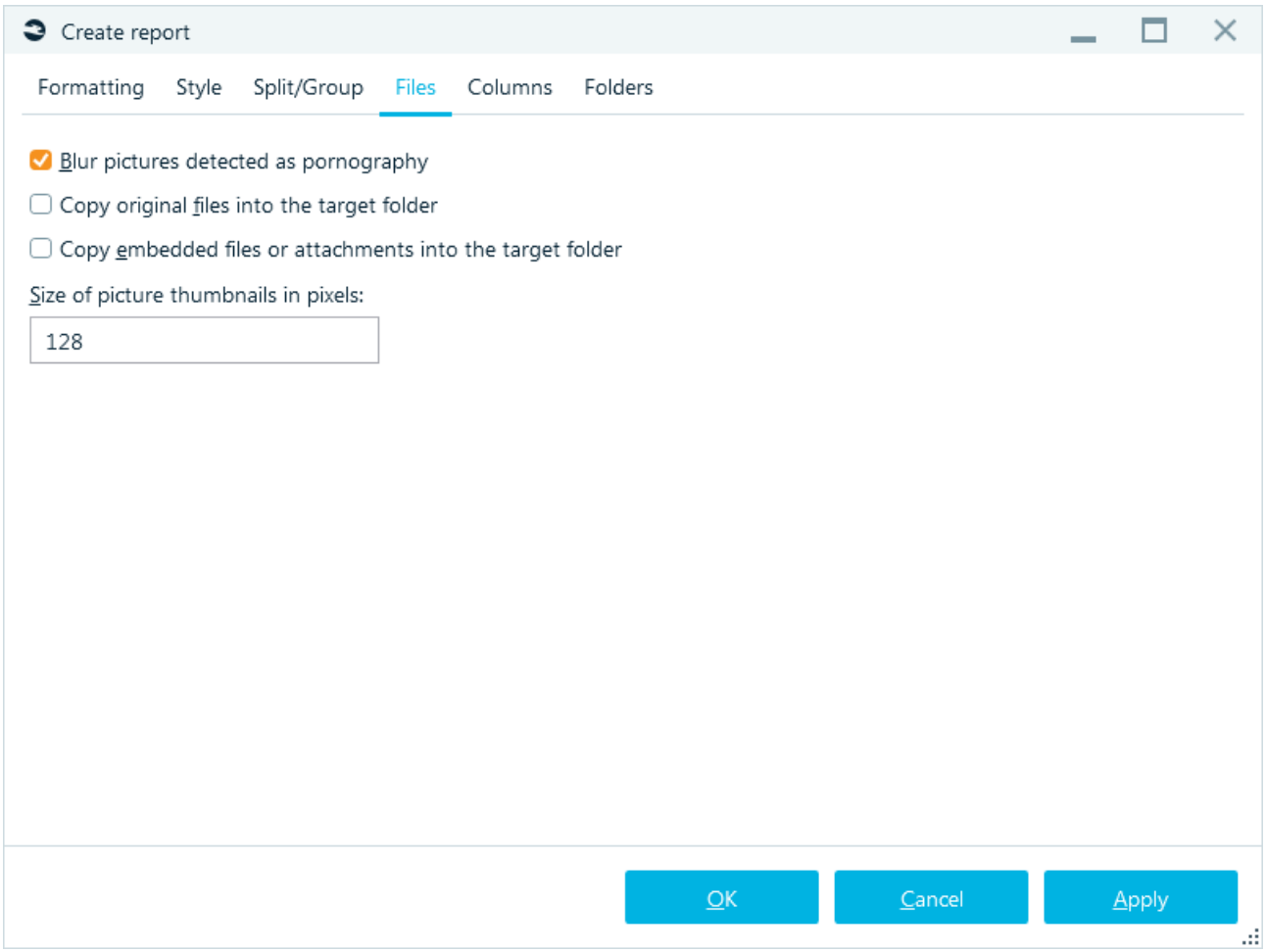
- **How to group items?** This setting applies to chats and email profiles and has the following options:
  - **Do not group**. No grouping used.
  - **Group by contact or mail folder**. Group chat history or email communication by person (for chats) or an email folder (for emails). If you set this option, you can see the entire chat with each single contact of a profile owner. Otherwise, you will see all chats within that profile would be mixed, with chats originating from different persons, put together and sorted by time.



Files

On the **Files** tab of **Advanced report options** window, you can specify various file-related options. Below are the avialble options:

- **Blur picture detected as porn**. If you have this option checked, pictures with pornography detected within them, will be included into a report; however the picture will be blurred on the report.
  Note: this only works if you run pornography detection before creating a report.
- **Copy original files into the target folder**. This option instructs the product to copy original pictures and documents to the target report folder (otherwise only document or picture properties and raw document contents will be included into a report). If the target format selected is PDF or HTML, hyperlinks to copied files will be also available in the report.
- **Copy embedded files or attachments into the target folder.**
- **Size of picture thumbnails in pixels**. If you opted to include picture preview into a report, this option helps to specify its size in pixels so that the report layout looks good.

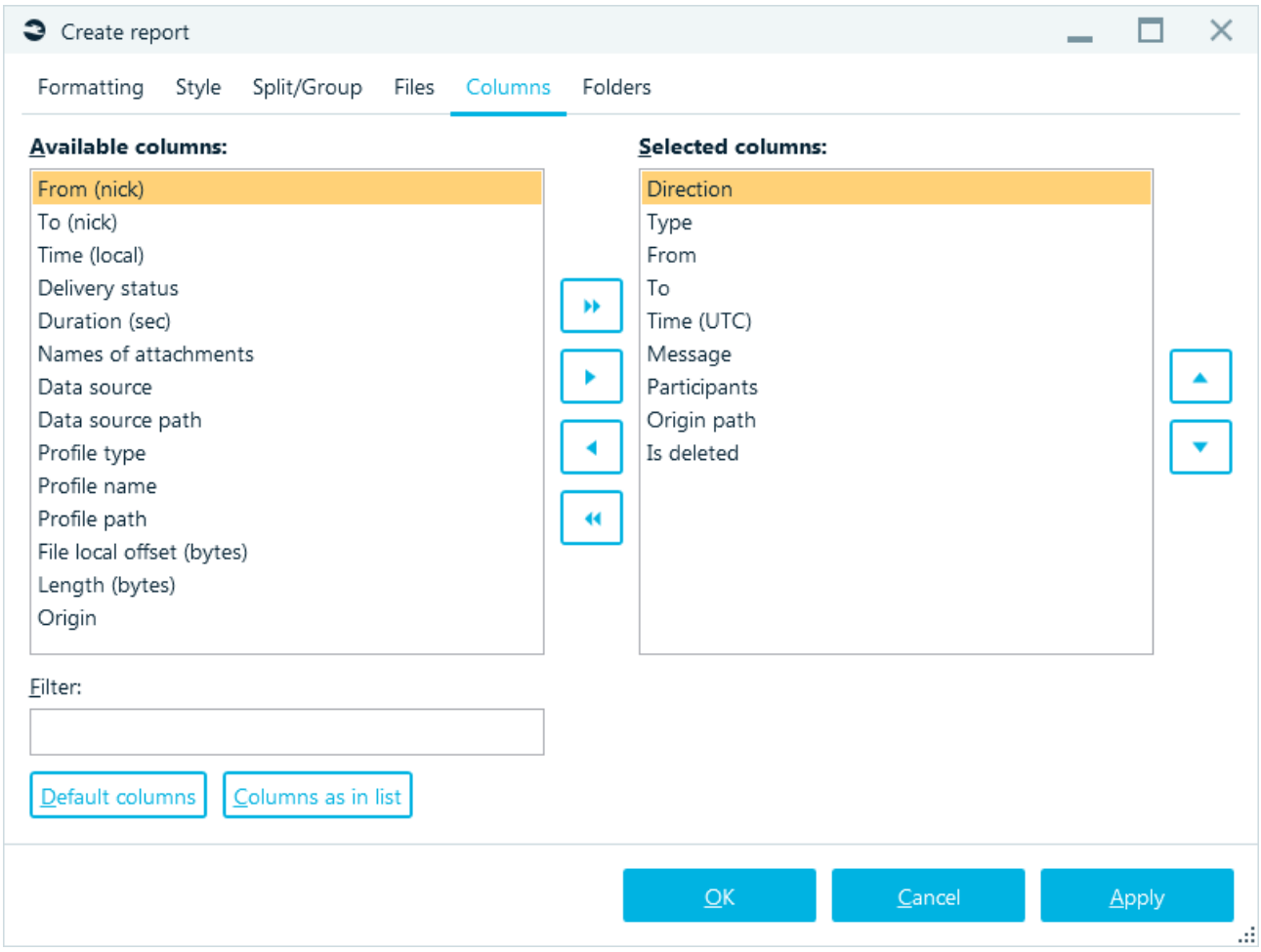


Columns

On the **Columns** tab of **Advanced report options** window, you can specify columns to include into your report. This tab consists of the following parts:

- **Artifact types**. Select the artifact type for column selection. If you are generating a report just for one artifact type, this list will not be shown: however, when you select a data source or the entire case (like the screenshot below), there will be numerous artifact types each with its own available columns set
- **Available columns**. Once you select a report type, this list will be populated with all columns (that is, properties) of items of the selected type. You can select one or multiple available columns to include into a report with the help of the corresponding buttons (see **Buttons** below)
- **Selected columns**. This list contains columns, which will be used for a report generation. If you exclude any columns from this list, they will not be included into your report. Note that if the order in this list is important, the order of the columns can be customized using corresponding buttons (see **Buttons** below)
- **Filter**. This field is useful for reports containing artifacts with many properties, such as pictures having a lot of EXIF fields. Type the first letters of a column to see all matching fields inside **Available columns** list
- **Buttons >>, >, <, <<,** 

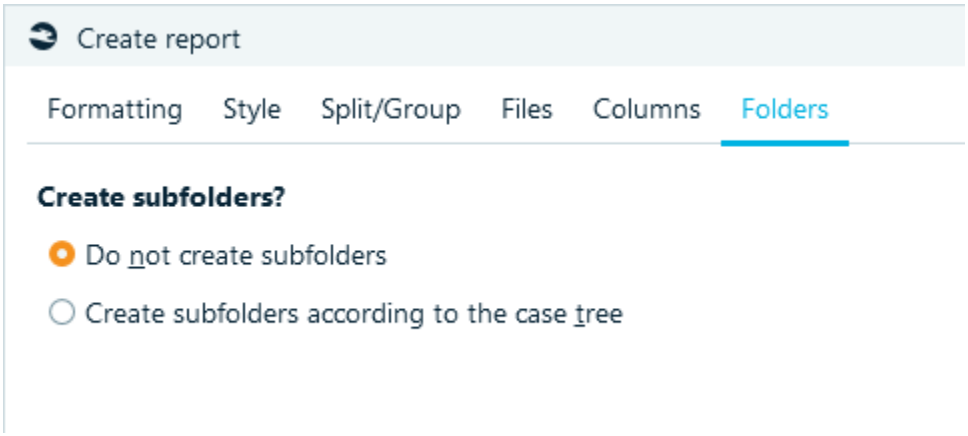
- **>>** button moves all columns to **Selected columns**. Note that if there are many columns in the report, the final document can be messy, unless you are using formats like CSV or XLSX. A report in DOCX or PDF format can typically have 7-10 columns at max (depending on whether you selected landscape or portrait orientation)
- **>** button moves currently selected column from **Available columns** to **Selected columns**
- **<** button moves currently selected column from **Selected columns** to **Available columns**
- **<<** button moves all columns to **Available columns**. This selection has a special meaning. This clears the list of all columns, thereby making it easier for you create the column list from scratch.
  Note: if you do not, in turn, add any columns back into the report, Belkasoft X will by default add all columns back on to the report.
-  buttons change the order of columns inside **Selected columns**, the specified order is preserved in a report



Folders

On the **Folders** tab of **Advanced report options** window, you can specify where to put the files of your report. This option should be used when you specify to generate one report per profile. There two choices In this window:

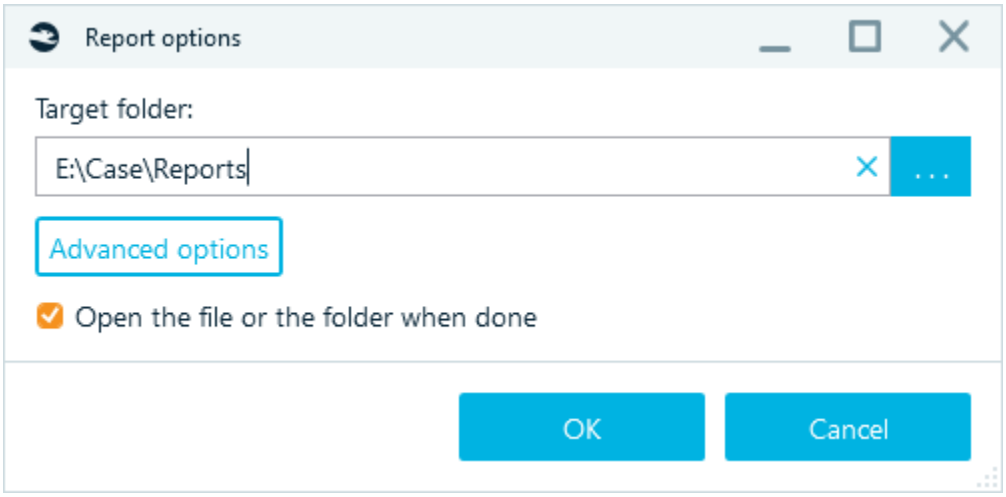
- **Do not create subfolders**. If you select that option, report folder will be used, and no subfolders will be created.
- **Create subfolders according to the case tree**. If you opted to create subfolders, this option will create subfolders inside target report folder and repeat the same structure as in Belkasoft X's **Artifacts** case tree. For example, if some profile was shown under My Case → Samples → Instant Messengers, and your target report folder is E:\Cases\Reports, then the full path to a report for this profile will be E:\Cases\Reports\My Case\Samples\Instant Messengers.



Including a map to a report

You can generate a report for geolocation artifacts shown on **Open Street Maps** window of Belkasoft X, and it will automatically include current map into the report. To do so, tune the map using your mouse: move the map by holding left mouse button and moving your mouse, zoom in or out using (+) or (-) buttons located at the bottom right corner or by using the mouse wheel. When you are satisfied with the view, right click on the map and select **Create report…** context menu item.

The product will show you a simplified version of report options, since this kind of report is available only in PDF format:

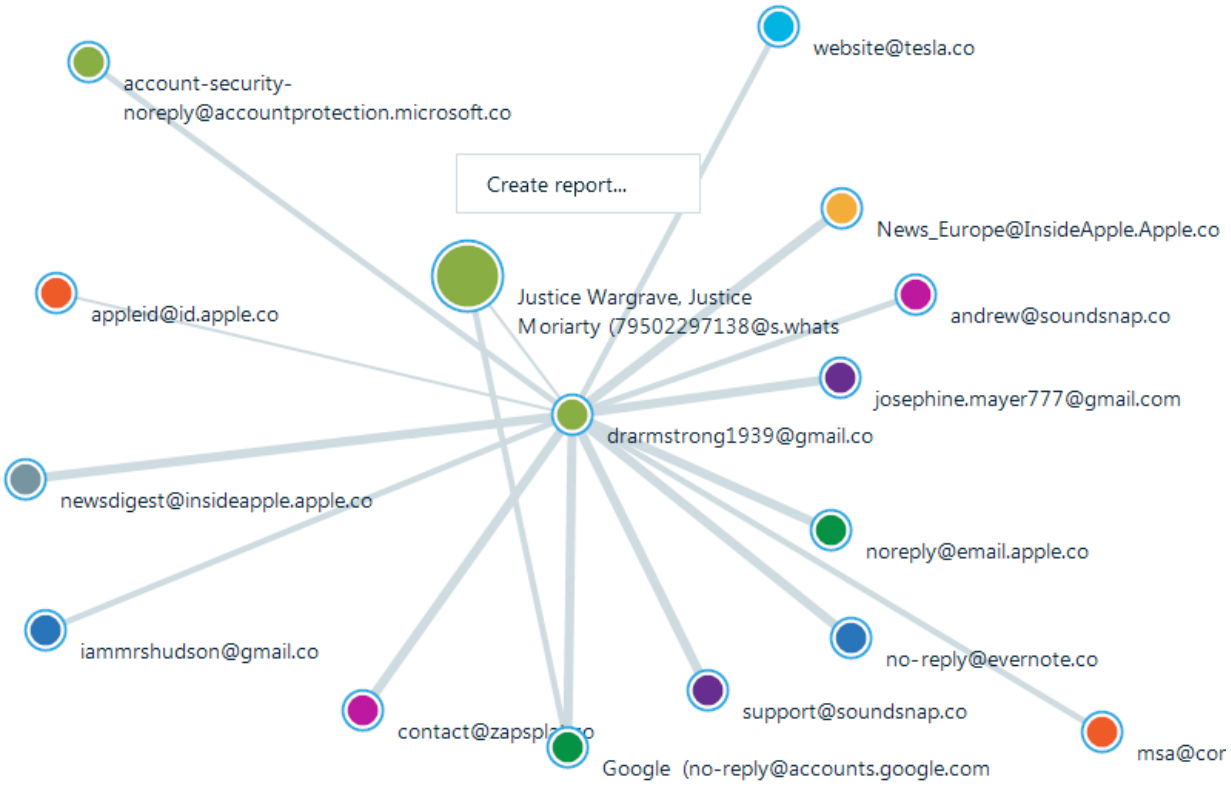


Some advanced options, e.g. **Formatting** and **Style** options are available to you.

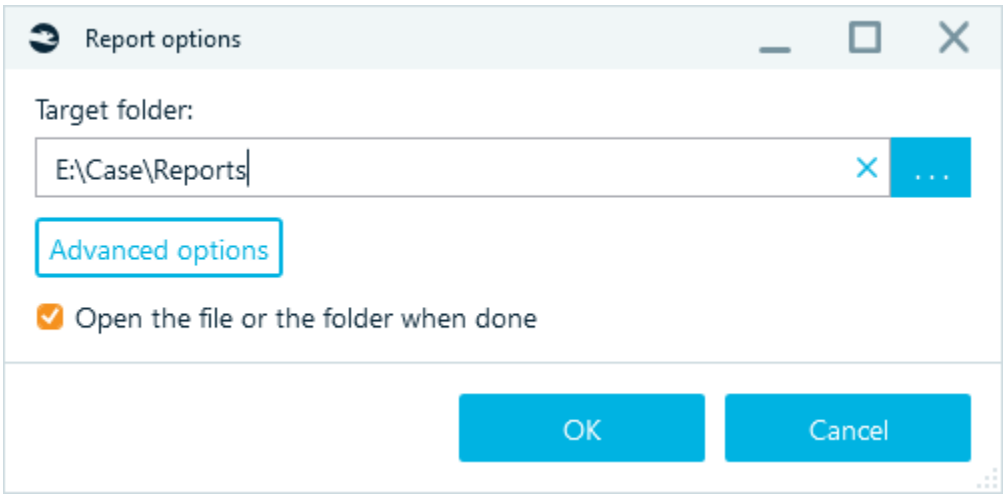
Including a connection graph to a report

You can generate a report for **Connection Graph** window of Belkasoft X, that will automatically include a current graph view into the report. Before doing that, you could filter out all the nodes you do not need in the report and adjust the overall graph appearance.

When you are satisfied with the current view, right click on the connection graph, and select **Create report…** context menu item.



The product will show you a simplified version of report options, since this kind of report is available only in PDF format:

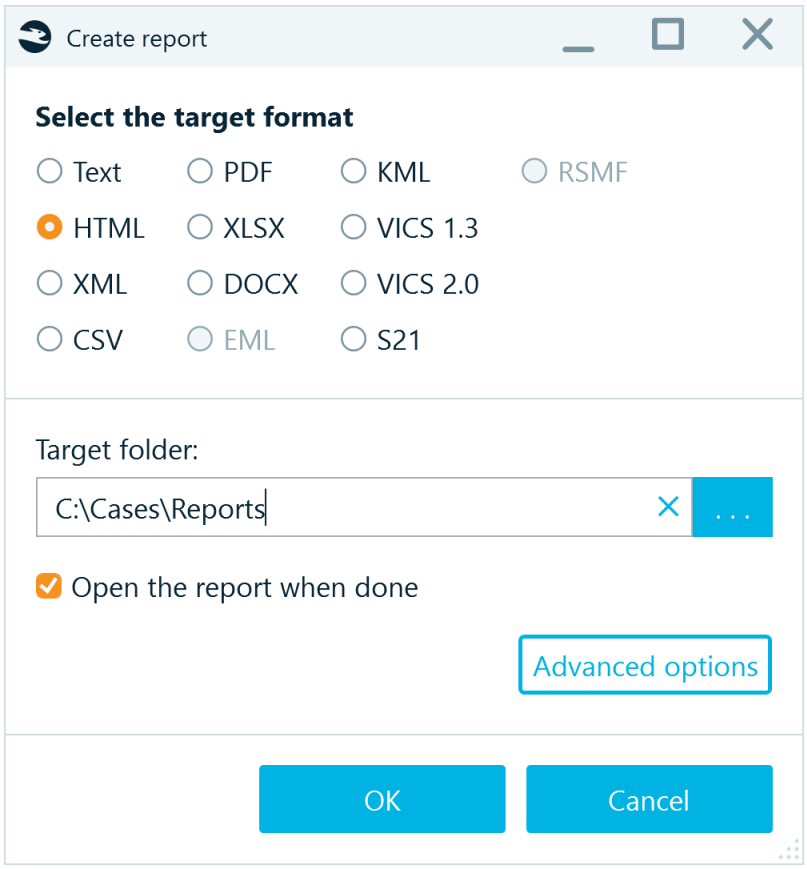


As with Map reports, advanced options are available to you.

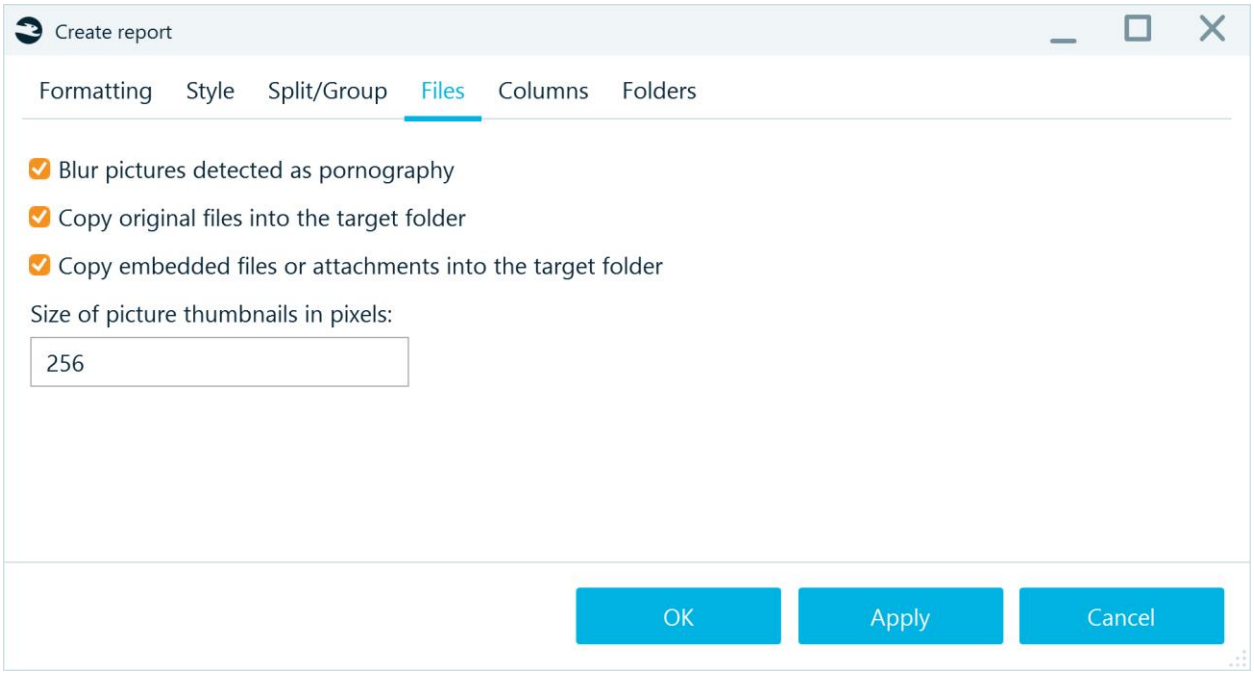
Hyperlinks in reports

To create a report with hyperlinks to files mentioned in the report, follow these steps:

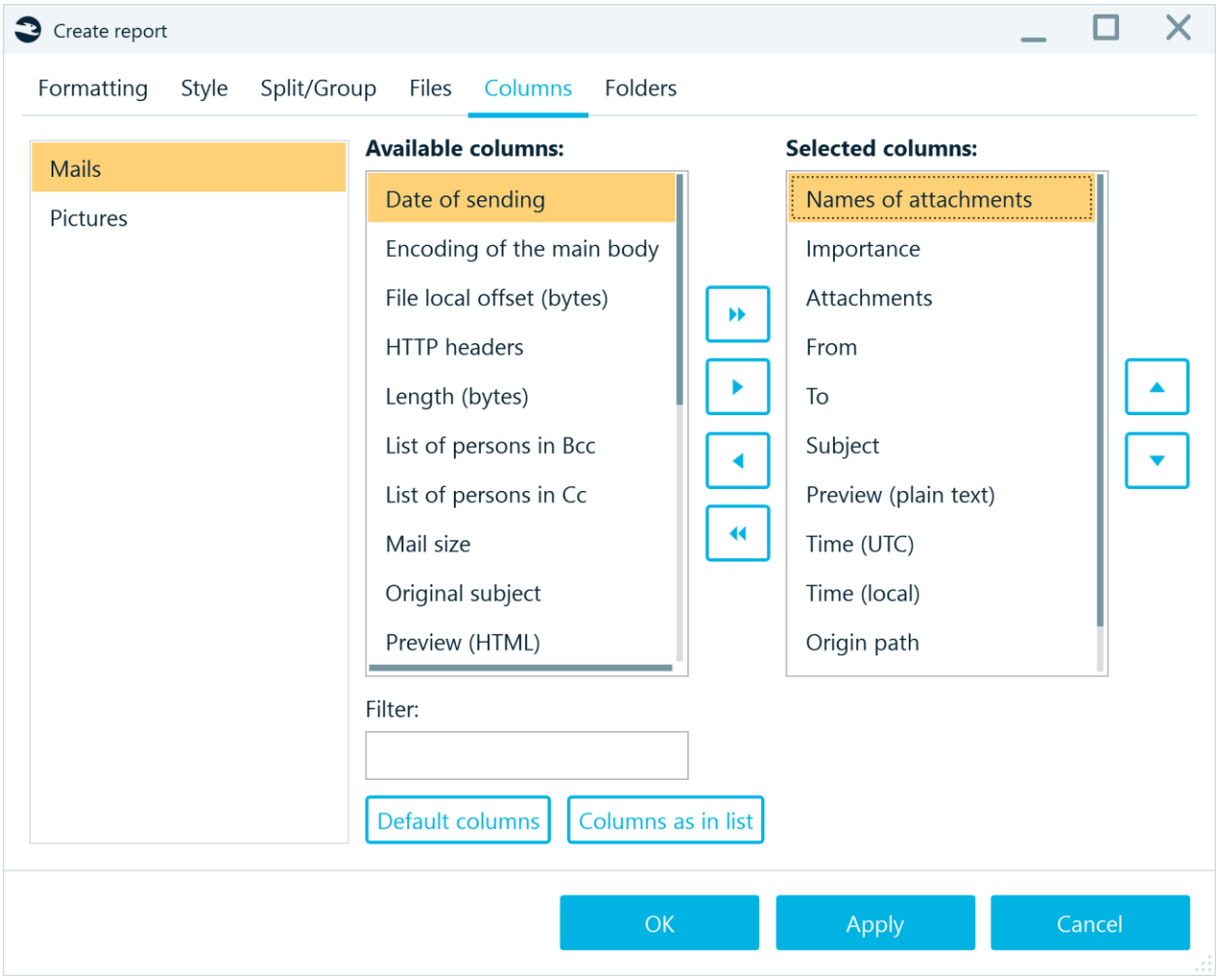
- Select HTML or PDF format



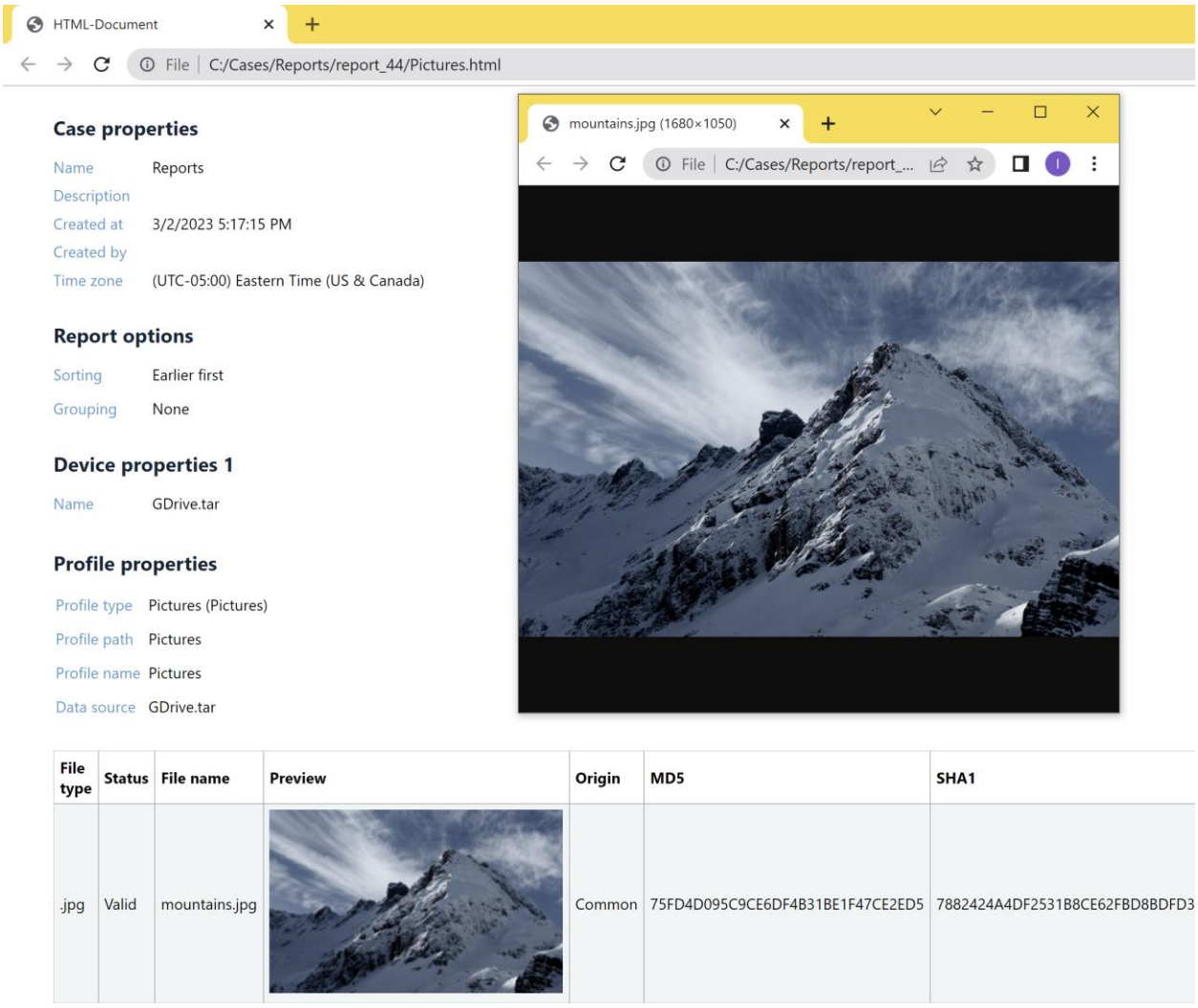
- Open **Advanced options** for the report
- Check **Copy original files into the target folder** in **Files** tab



If you would like to get a hyperlink to a file that is an attachment, then you need to select column **Names of attachments** of in setting tab **Columns**.



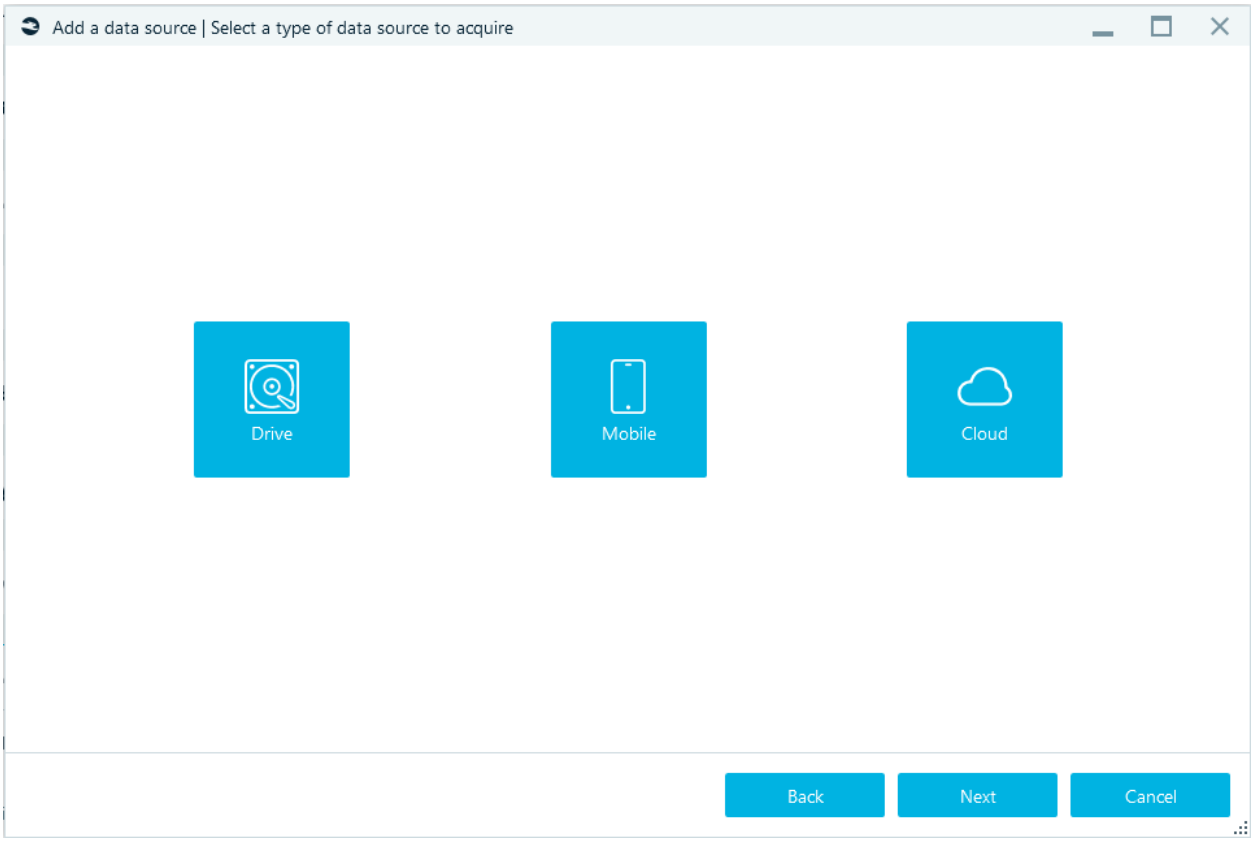
After making the necessary settings, click on **Appy** and then **OK** buttons.



Acquiring data source

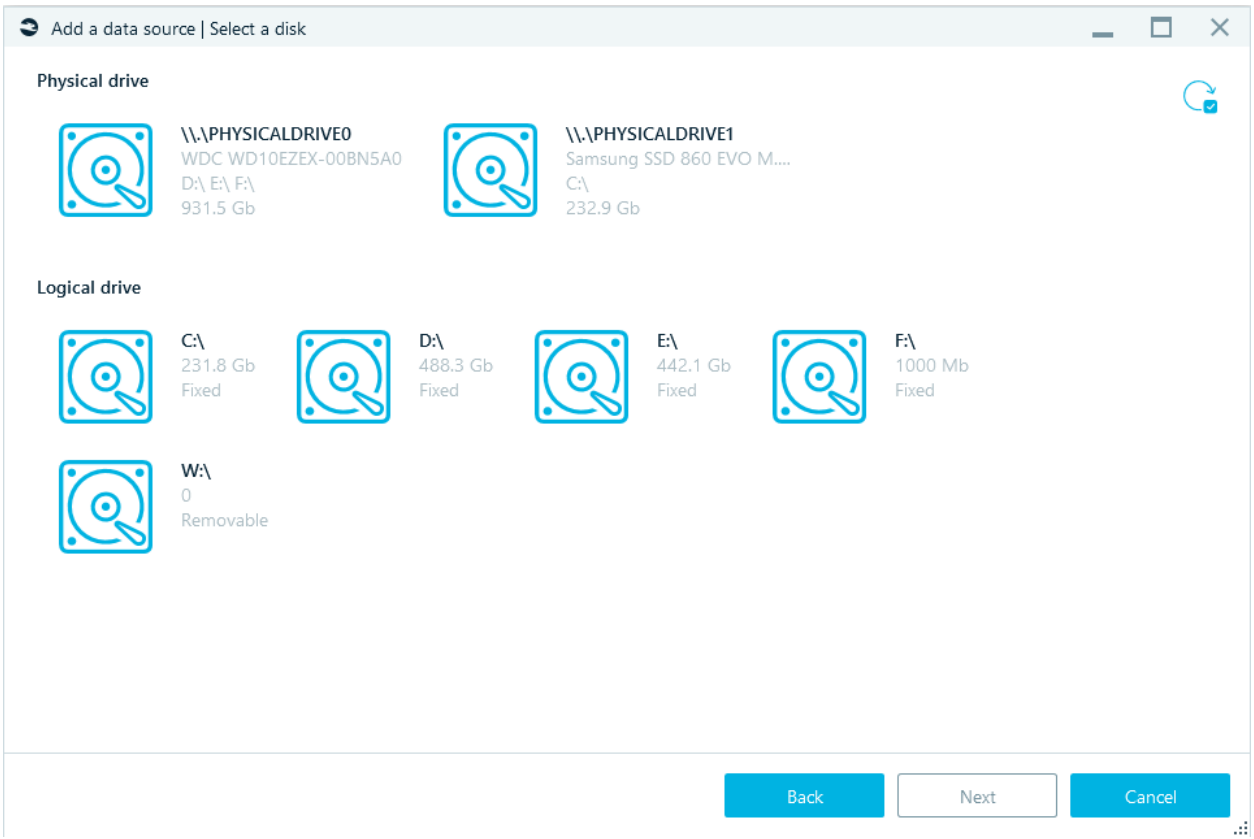
There are following acquisition options available:

- Acquire a disk drive
- Acquire a smart device
- Acquire a cloud
- For RAM acquisition, please use a standalone Belkasoft tool called **Live RAM Capturer**
- For remote acquisition, please use a standalone Belkasoft tool called Belkasoft R

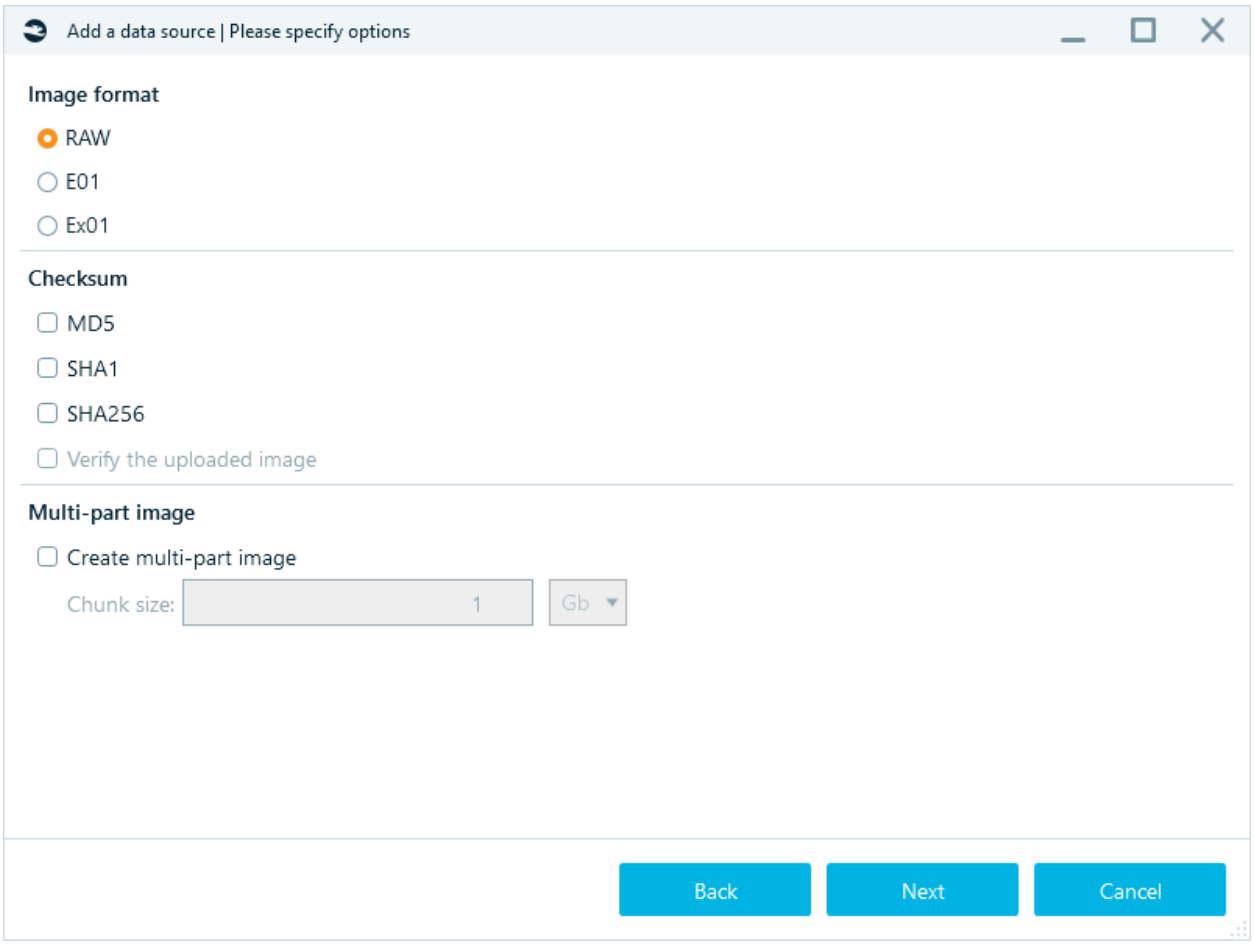


Acquiring disk drive

Using this option, you can acquire a disk drive connected to your machine. The disk must be "seen" by the operating system.



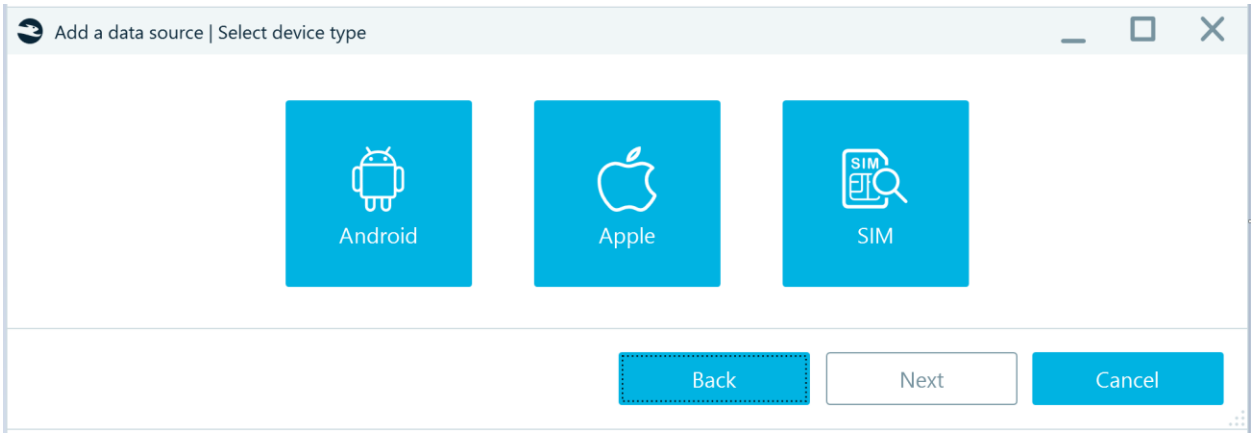
On the picture above you can see a window shown after **Add a data source** → **Acquire** → **Drive** button clicked. There is a **Source drive** list, which shows physical and logical drives, seen by the operating system. Some basic info is shown for each, such as its identification in the system, serial number, capacity and, for physical drives, all logical drives inside that physical drive.



In the next window you can specify options: **Image format** such as RAW, E01 or Ex01, then you can ask Belkasoft X to calculate a **Checksum** in **SHA-1, SHA-256** or **MD5** forms and **Verify output** upon acquisition completion. Finally, you can split output image file by chunks of a given size.

Acquiring mobile

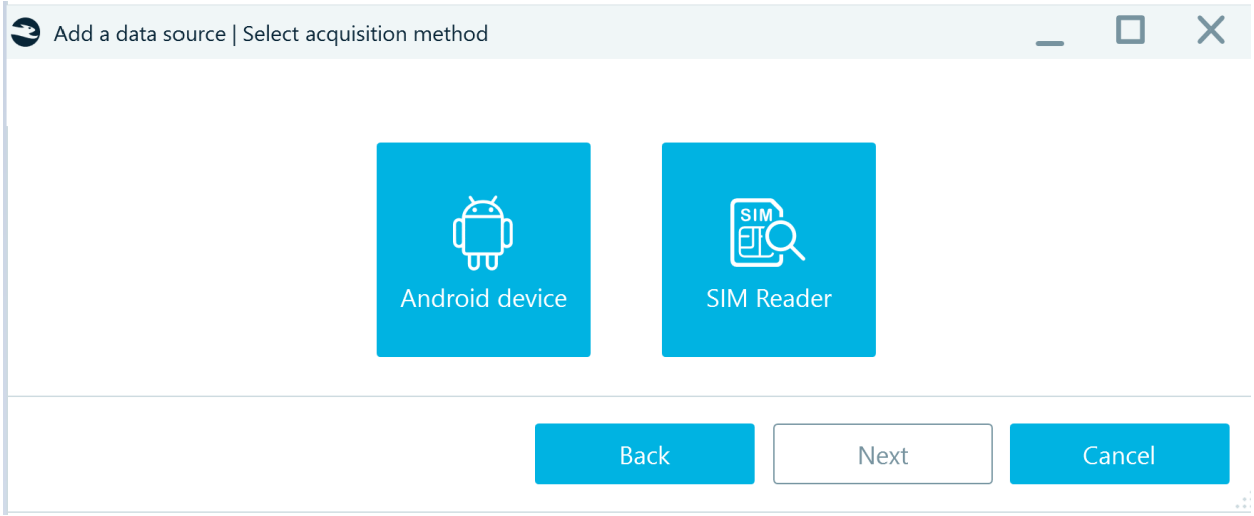
Using this option, you can acquire a smart device connected to your machine.



SIM

Belkasoft Evidence Center X has two options for Sim card analysis:

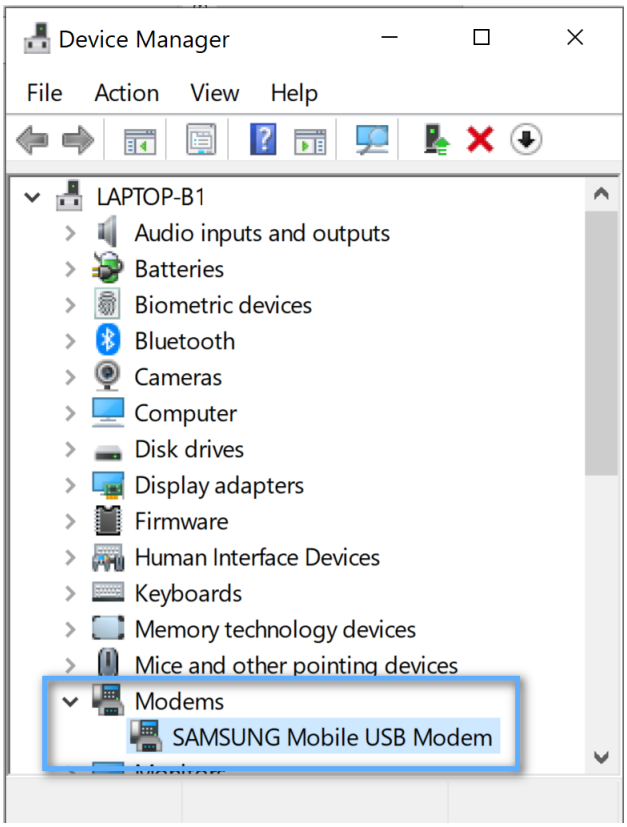
- **Android device**
  Android device acquisition allows to collect information about the SIM card and device via AT commands, without having to remove the SIM card from the phone.
- **SIM reader**
  The SIM reader method extracts the entire file system of the SIM card, using AT commands including only sms, contacts and device information as a result.



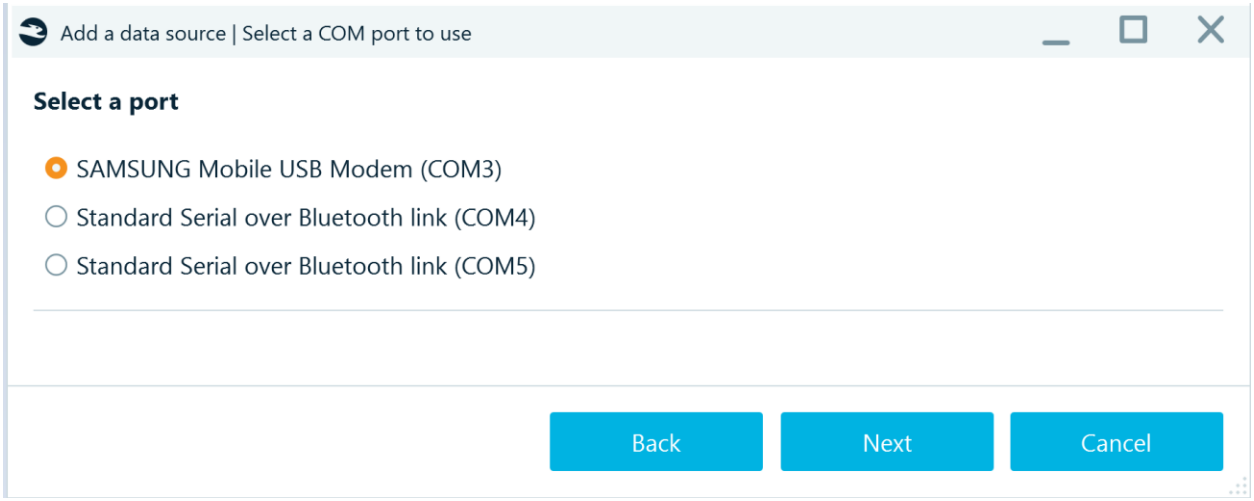
Android device acquisition

Before the acquisition make sure that:

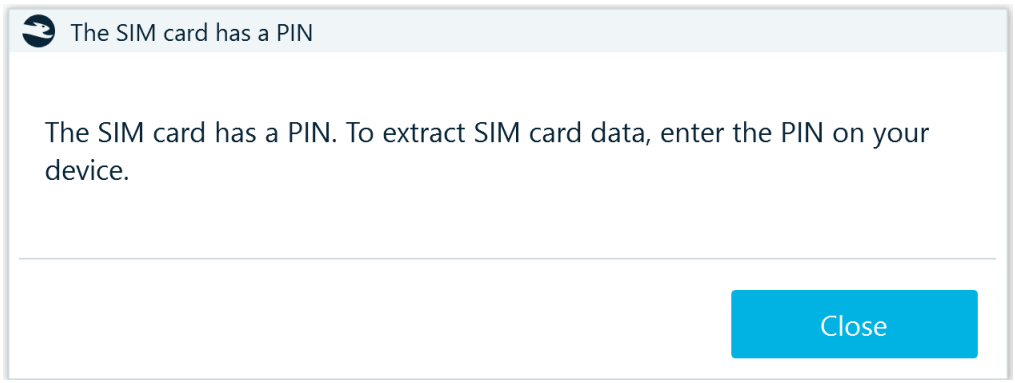
1. The SIM card is inserted in the first slot, the second slot is not supported yet (for phones with two SIM cards)
2. The connected device is displayed in the Device Manager under the Modems node. If not, please use suitable USB drivers for connecting required devices to the computer.



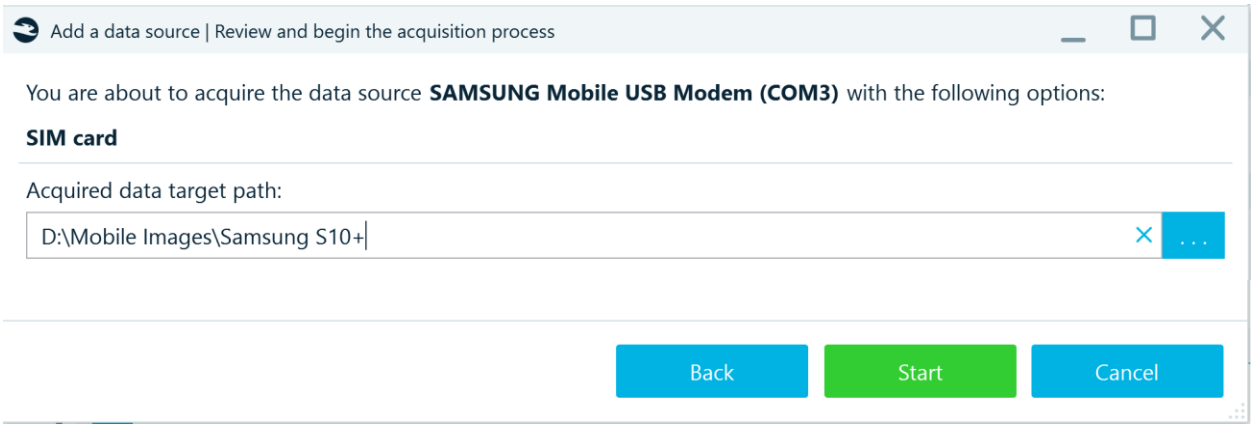
Run the Android Device acquisition in Belkasoft X. Select a required port with a connected device and press **Next**.

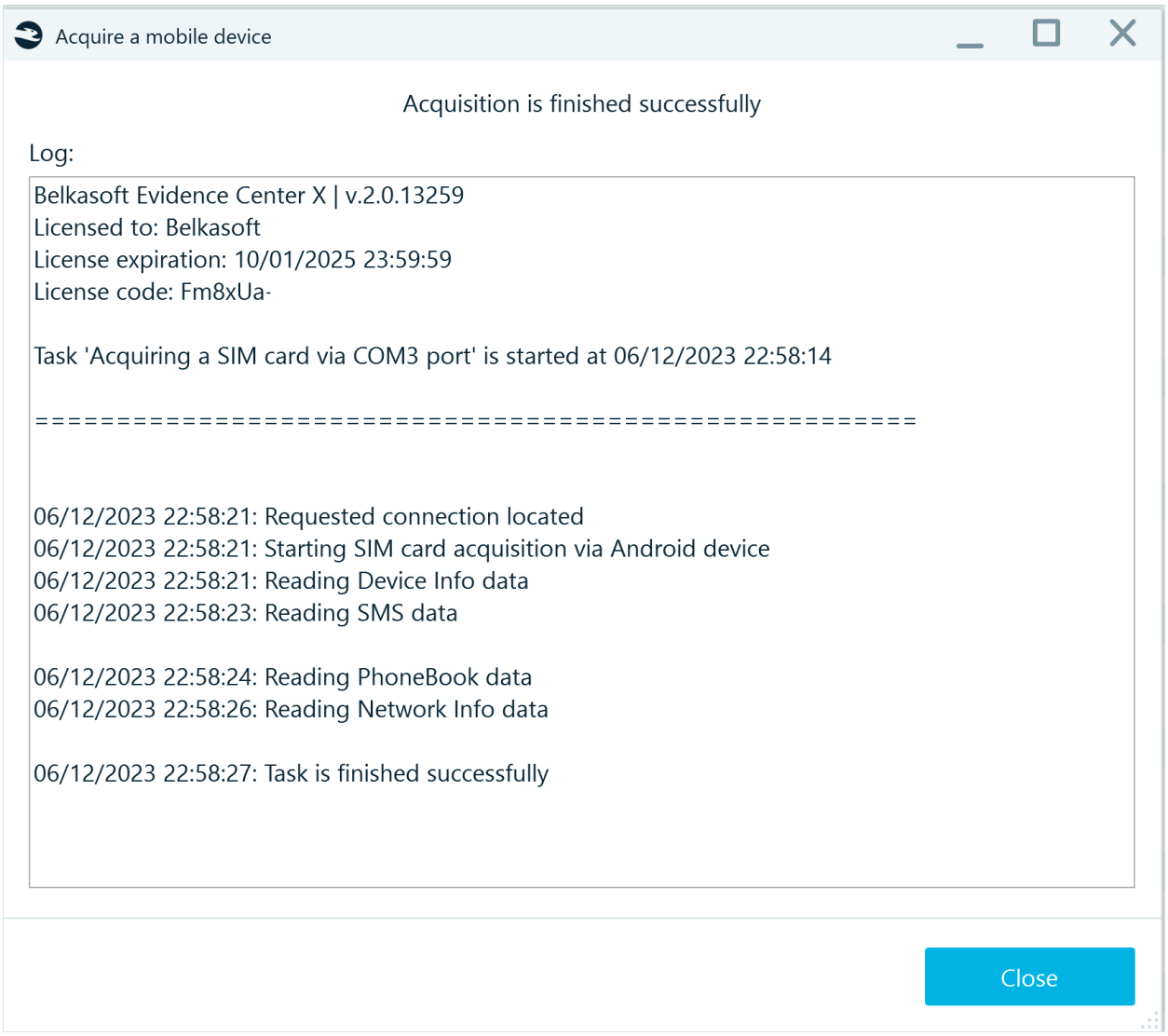


If a password is set on the SIM card, a message will appear:

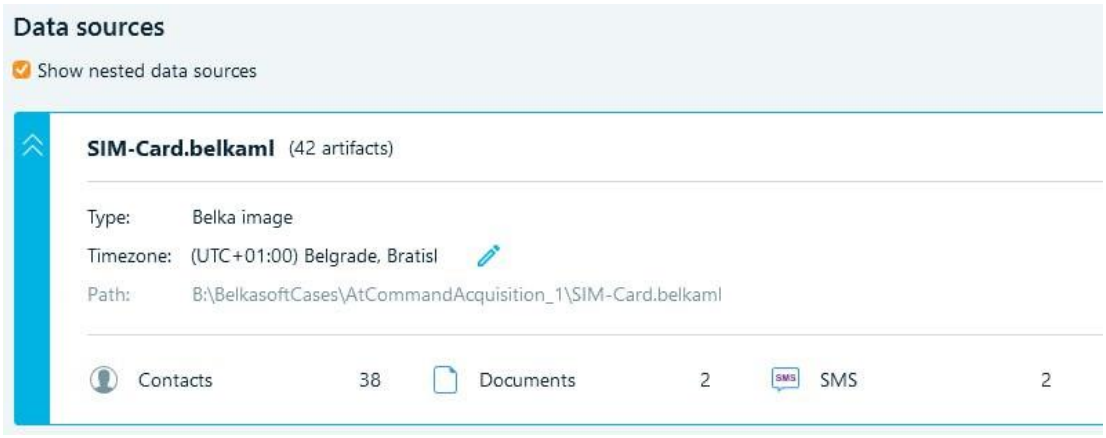


Specify the target path and click **Start**:





Wait for the end of the acquisition process, the acquired image will be automatically offered by Belkasoft X for analysis.
Review the acquired information:



SIM Reader

SIM card acquisition allows users to get:

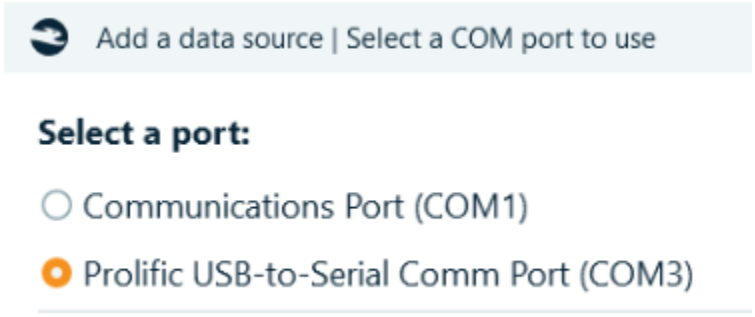
- The name of the card
- IMSI number
- Abbreviated Dialing Numbers (ADN)
- Contacts
- SMS messages

Before you start acquisition: Download and install necessary drivers (USB-COM port emulator).

Insert the SIM card into the SIM reader. Connect the SIM reader to the computer's USB port.

After selecting **SIM Reader** (in the window 'Add a data source| Select device type') you will see all ports available for the analysis.

The sim reader port's name usually contains words such as "USB", "Serial" (the name set by a driver). By default, the port containing these words is selected.

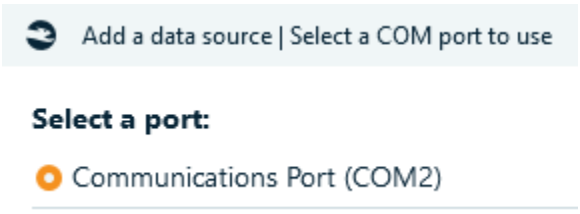


After the acquisition two archive files will be created:

- **SimReader.tar** contains four binary files: SIM-Name.bin, SIM-IMSI.bin, SIM-SMS.bin, SIM-ADN.bin.
- **SimReaderParser.tar** contains four text files: SIM-Parsed-Name.txt, SIM-Parsed-IMSI.txt, SIM-Parsed-SMS.txt, SIMParsed-AND.txt.

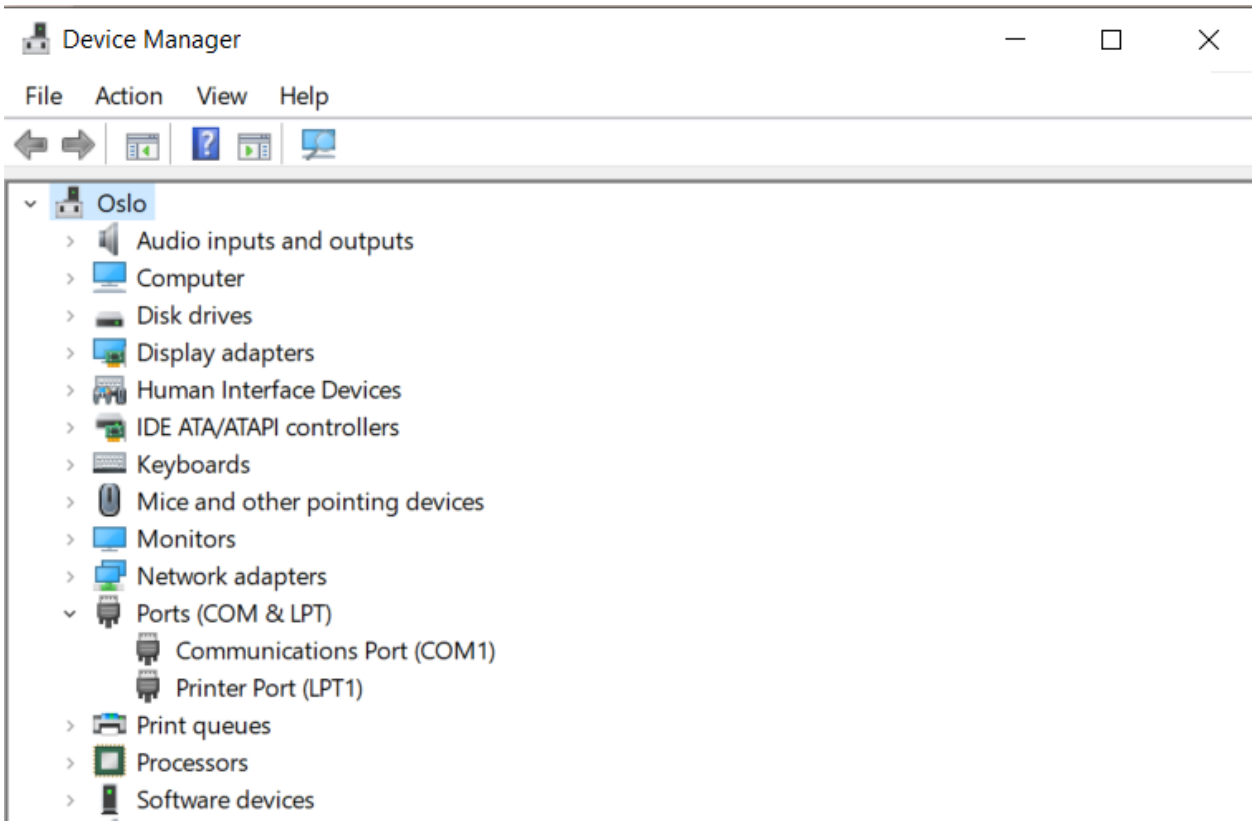
Troubleshooting

If the SIM reader port is not on the list (see the picture below) there might be a problem with a driver.



To verify that the SIM card reader driver is installed correctly, follow these steps:

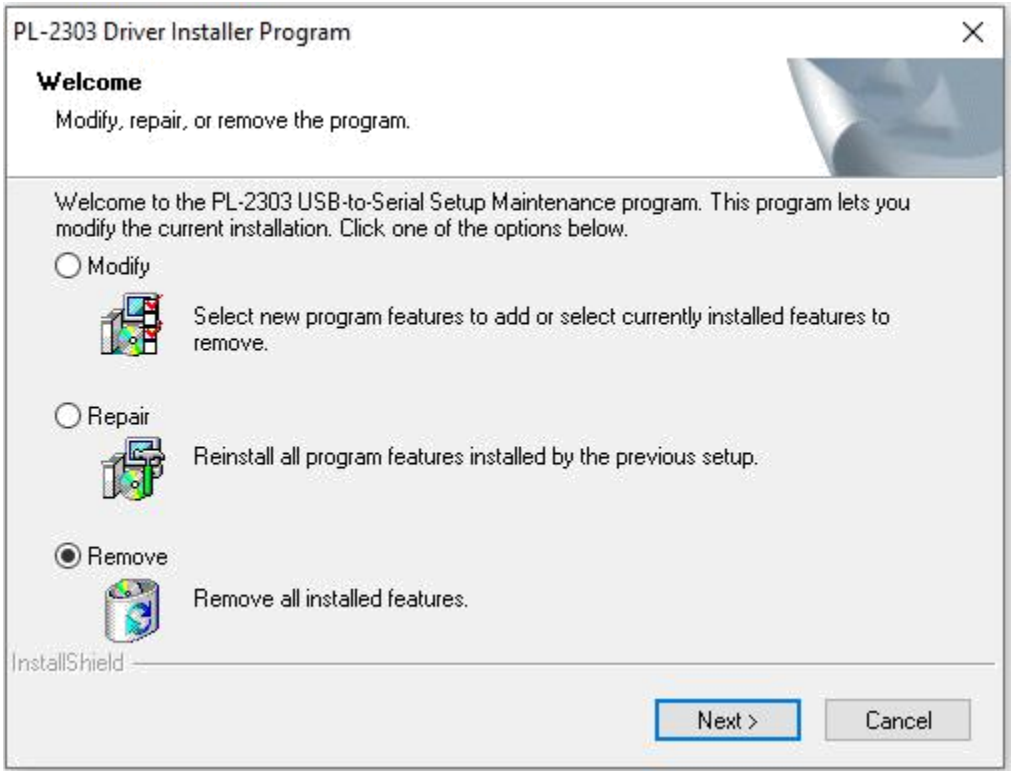
- Open the **Device Manager**.



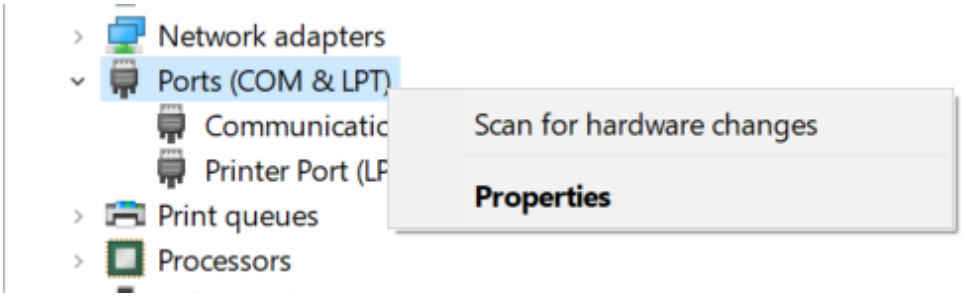
- The connected sim reader should be displayed under the Ports (COM & LPT) node.
  If the drivers are incorrect, a device with a name like the one in the screenshot or an unknown device is shown.

- Right click on the device and select **Uninstall device**.
  Check **Delete the driver software for this device**.

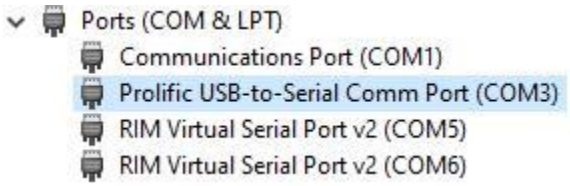
- Select **Remove** and click **Next**.



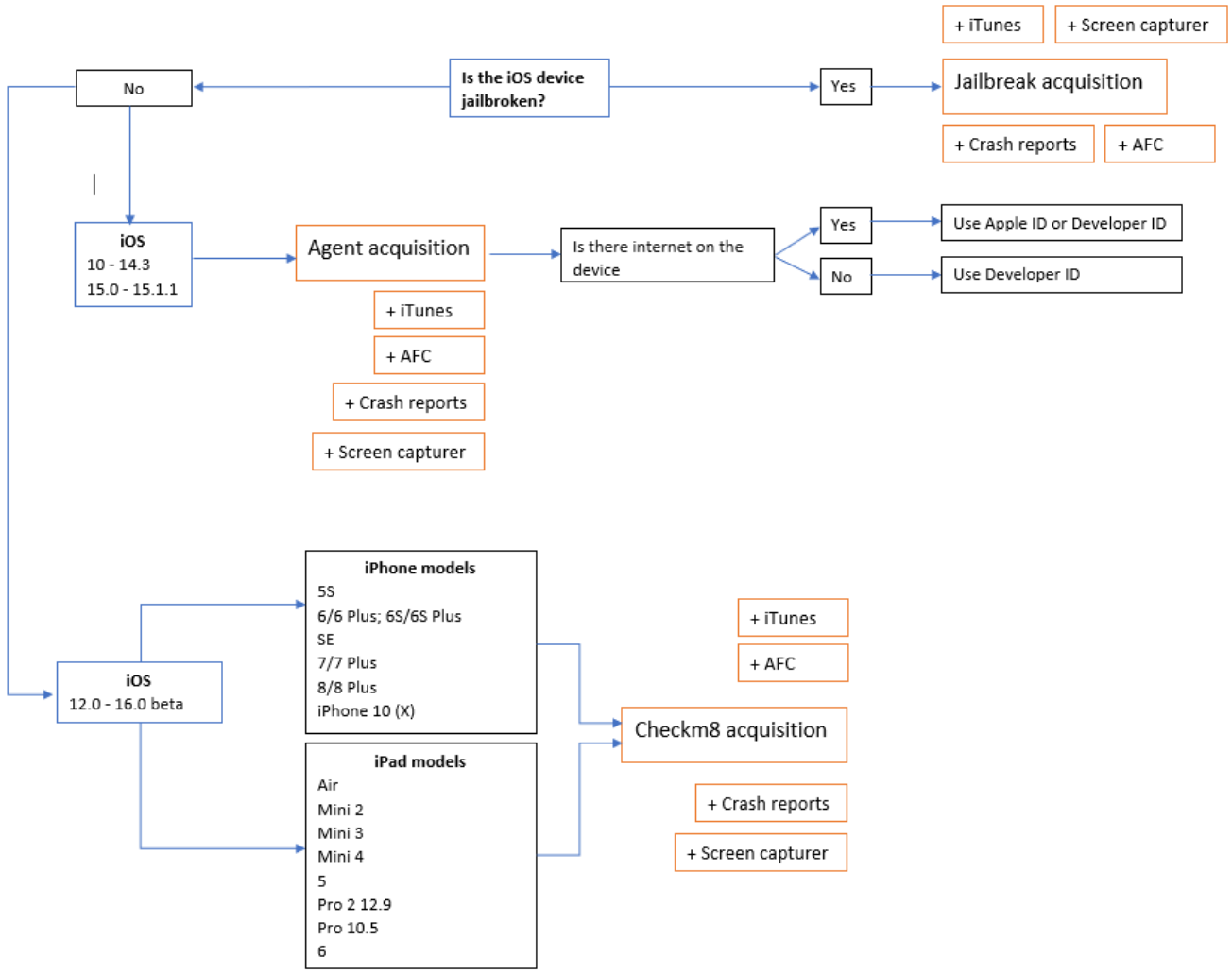
- Reboot the computer if necessary and re-install the driver
- Select **Scan for hardware changes** in the **Device Manager** to check if the drivers were successfully installed.



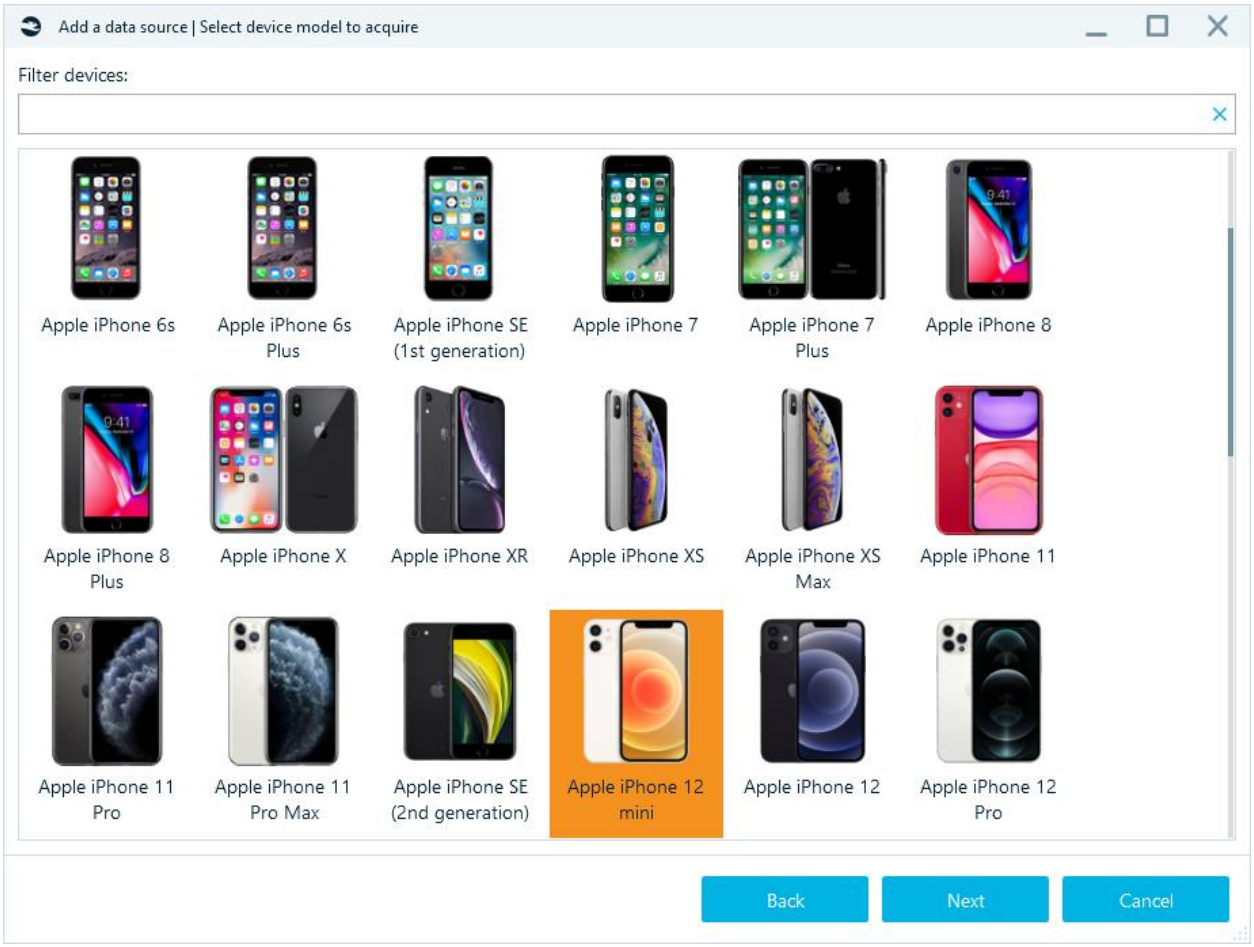
- After the correct installation, you will see a new COM-port device with a similar name:



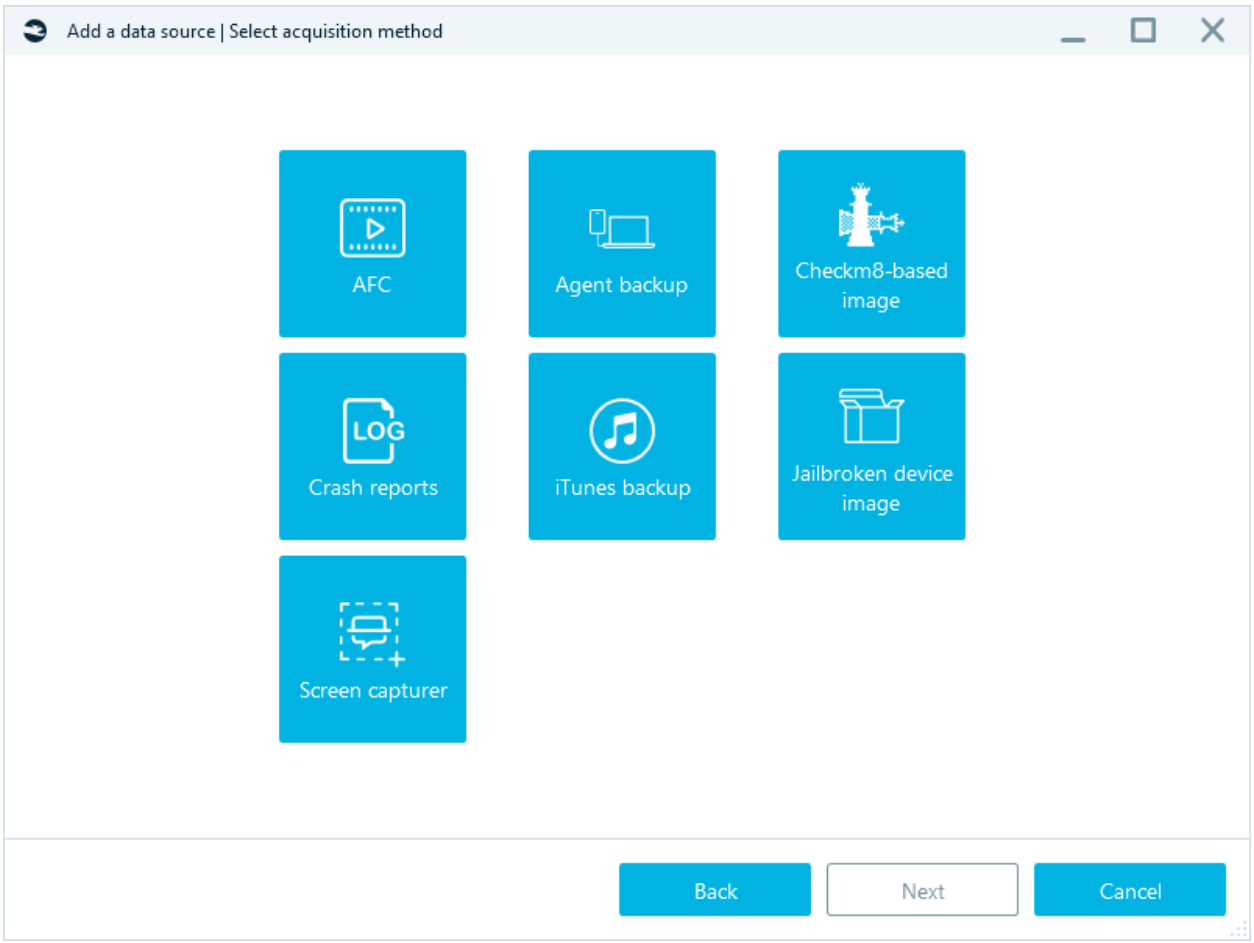
Apple



After clicking on **Apple**, a list of devices will be displayed:



Select the device you want to work with (the filter will help you in your search) and click **Next**. You will see the list of acquisition types, available for the selected model.



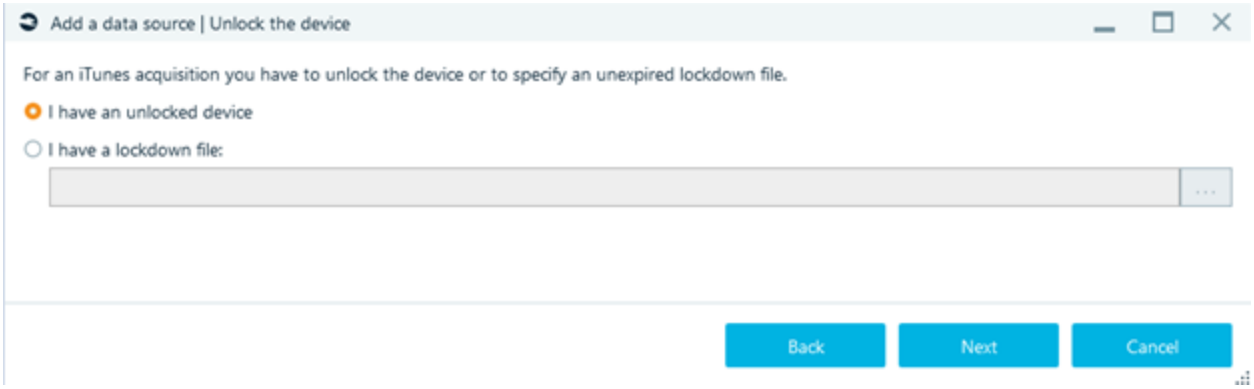
iTunes backup

This is the standard way to backup iOS device data. It requires iTunes to be installed on the machine where Belkasoft X is running.

Note: Encrypted backup contains more data. Belkasoft X automatically turns on encryption if no password is set in iTunes. The specified password is visible in the log and in the belkaml files.

```
1  Belkasoft Evidence Center X | v.1.15.10915
2  Licensed to: Belkasoft
3  License expiration: 2023.06.01
4  License code: 32595C
5
6  Task 'Creating the iTunes backup for 'iPhone Martha Louise Hudson'' is started at 9/1/2022 5:36:08 PM
7
8  ======================================================
9
10 9/1/2022 5:36:25 PM: Requested connection located
11 9/1/2022 5:36:26 PM: Try set backup encryption by password 12345
12 9/1/2022 5:36:29 PM: Handling notification message: com.apple.mobile.backup.domain_changed
13 9/1/2022 5:36:29 PM: The backup is going to be encrypted using the password '12345'.
14 9/1/2022 5:36:31 PM: Received DLMessage:
15 ...
16 9/1/2022 5:38:05 PM: Task is finished successfully
17 9/1/2022 5:38:07 PM: Backup password is found in data source metadata: 12345
```

To start an acquisition, you need to unlock smartphone or determine the path to the lockdown file.



Specify the **Target path** (for the folder where the smartphone image will be stored) and click **Start** - acquisition will begin.

Agent-based acquisition of iOS devices

This method copies the contents of the file system through the installation of a special agent application. The amount of extracted data will be the same as with Full logical backup of jailbroken iOS devices acquisition or Checkm8-based acquisition of iOS devices (including data from keychain).

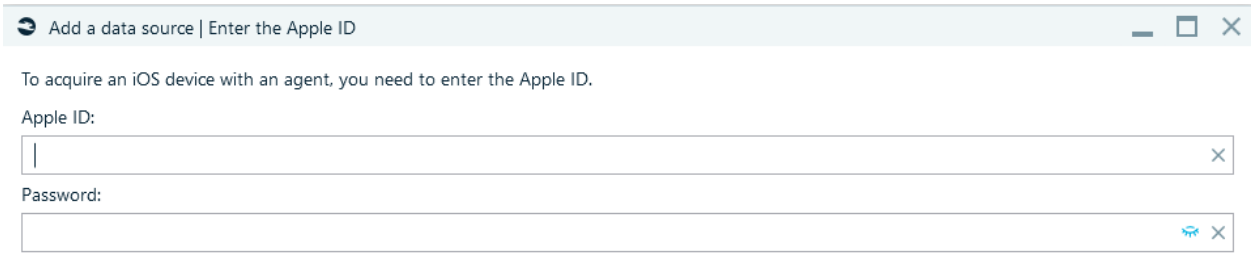
Supported iPhone models: all types.
The functionality is also supported on iPads.
Supported iOS versions: from iOS 10.0 down to 14.3, from 15.0 to 15.7.1 and 16.0-16.1.2.

Before you start acquisition with the agent backup, check and confirm that:

- Computer has internet access if you are using an **Apple Developer ID**
- Smartphone has internet access if you are using an **Apple ID** (free)
- Antivirus is stopped or paused.

Select an Apple device.

You will see the window below after selecting **Agent backup** in the window **Add data source| Please select the acquisition type**:

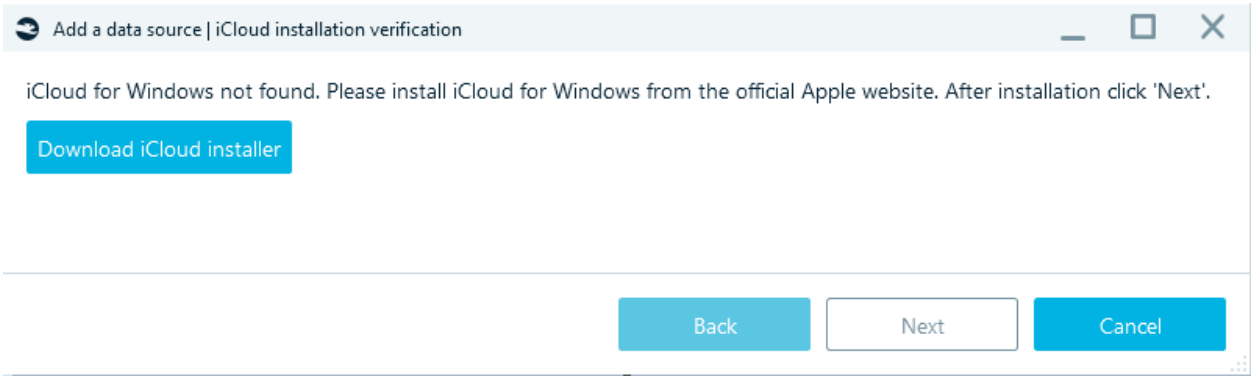


If you are using an **Apple Developer ID** (an Apple ID that participates in the Apple Developer Program) enter it and the App-specific password. Or use **Free Apple ID** and Password.

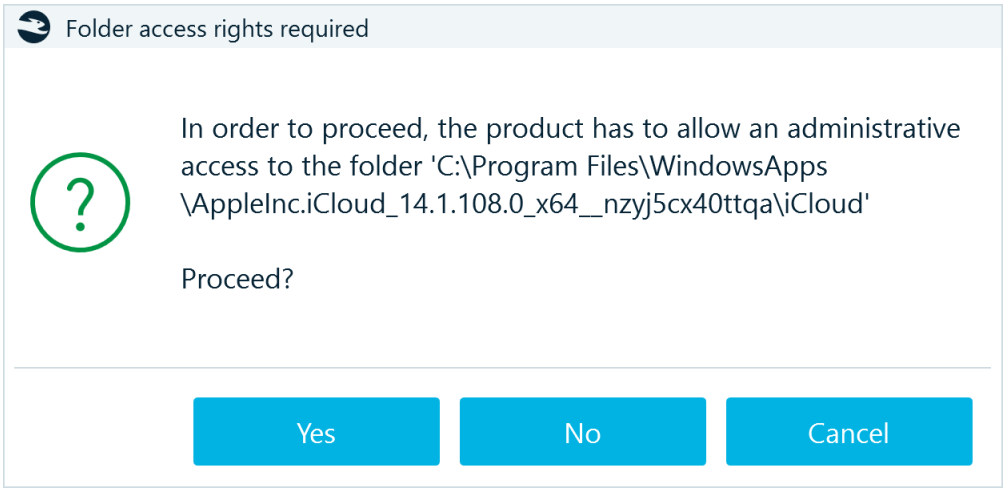
Note:

- When using **Apple Developer ID**, the device does not need the Internet.
- **Apple Developer ID** can be used on 100 devices.
  - When using **Free Apple ID**, the device requires the Internet.
  - **Free Apple ID** can only be used on three devices.

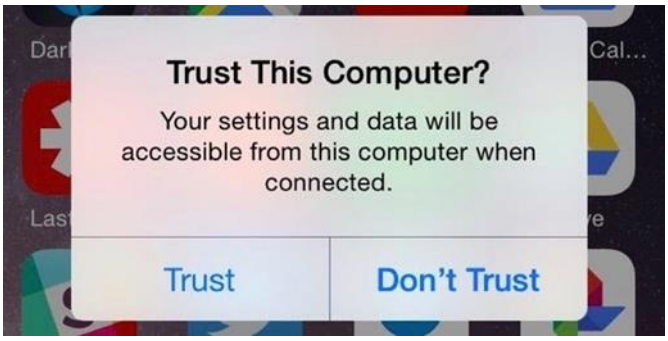
Install iCloud if necessary (requires computer restart).



Allow administrative access to the iCloud folder (administrative access is added by pressing Yes):



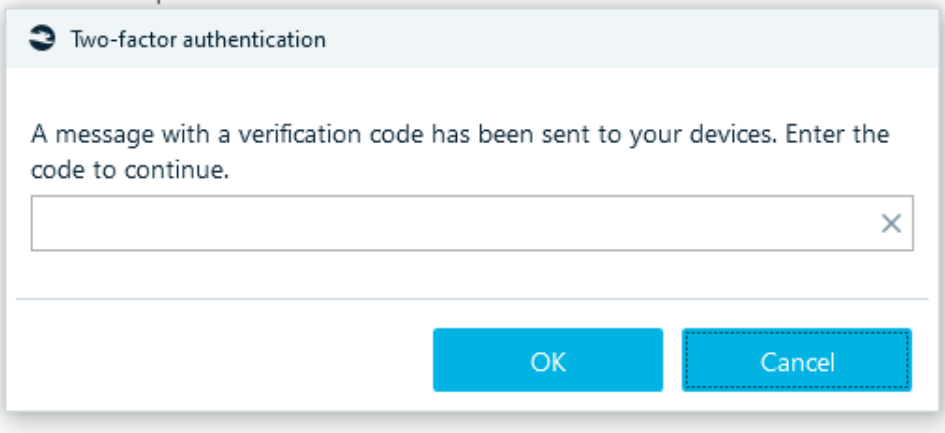
Unlock an Apple device using its passcode and connect the device to PC using a USB cable (**port 3.0 is preferred**). When you see the **Trust this computer** message on the iPhone, click **Trust**.



Specify the **Target path** and click **Start** - acquisition will begin.

If an Apple ID has two-factor authentication, enter the verification code in the **Two-factor authentication** window:

6/2021 10:03:10 PM: Requested connection located



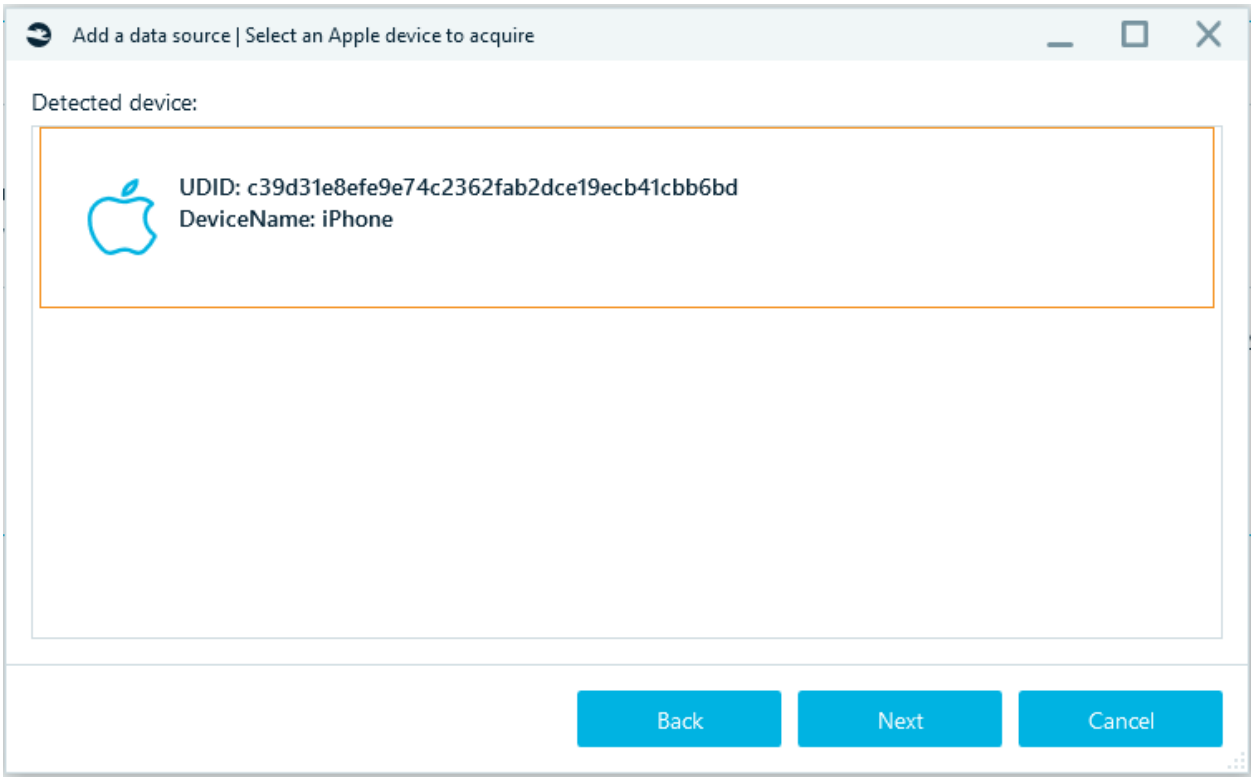
Follow the instructions in window **Acquire a mobile device**:
In order for the application to work, the certificate must be confirmed in the device settings:

1. In the iOS Settings scroll down and tap 'General'
2. Scroll down and tap 'Profiles, Profiles & Device Management' or 'Device Management', depending on the iOS version.
3. Select a profile with Apple ID.
4. Tap 'Trust [Apple ID]' and confirm your choice.
5. Waiting for the profile to be trusted.

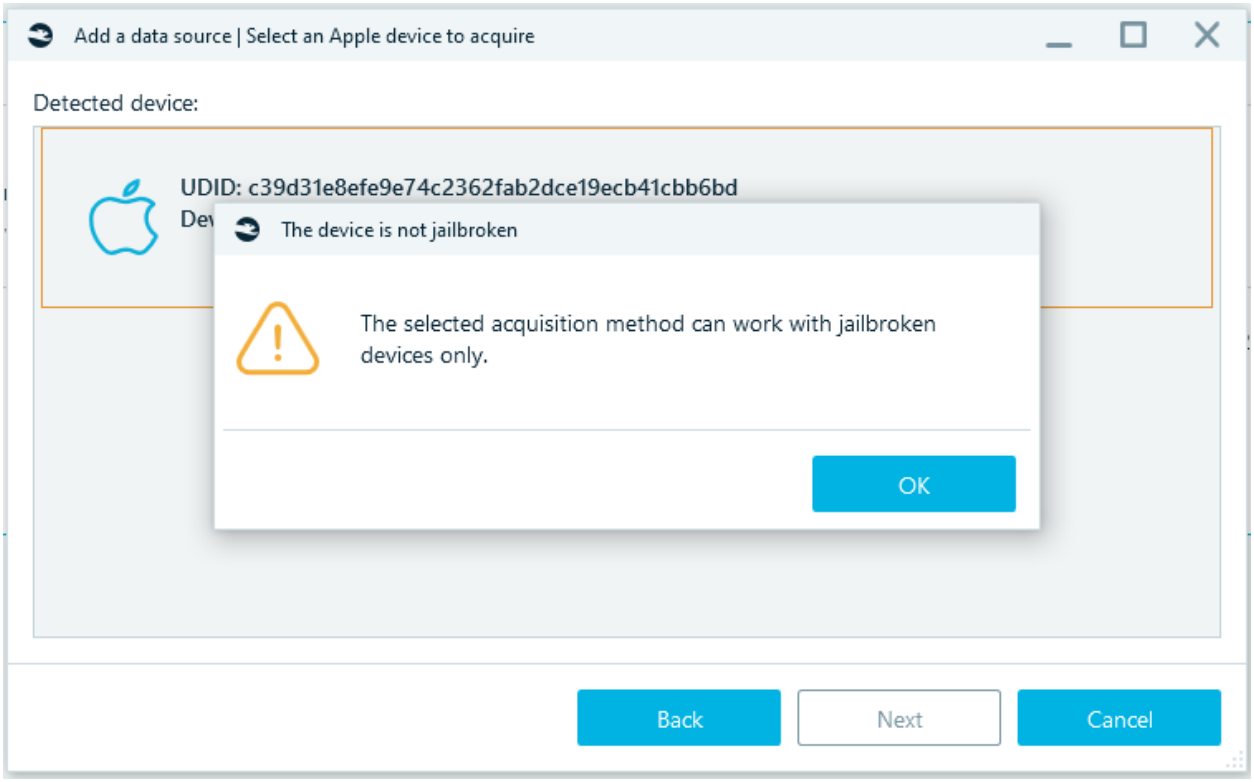
After the Agent is downloaded to the smartphone, enter the smartphone password.

Jailbroken device image

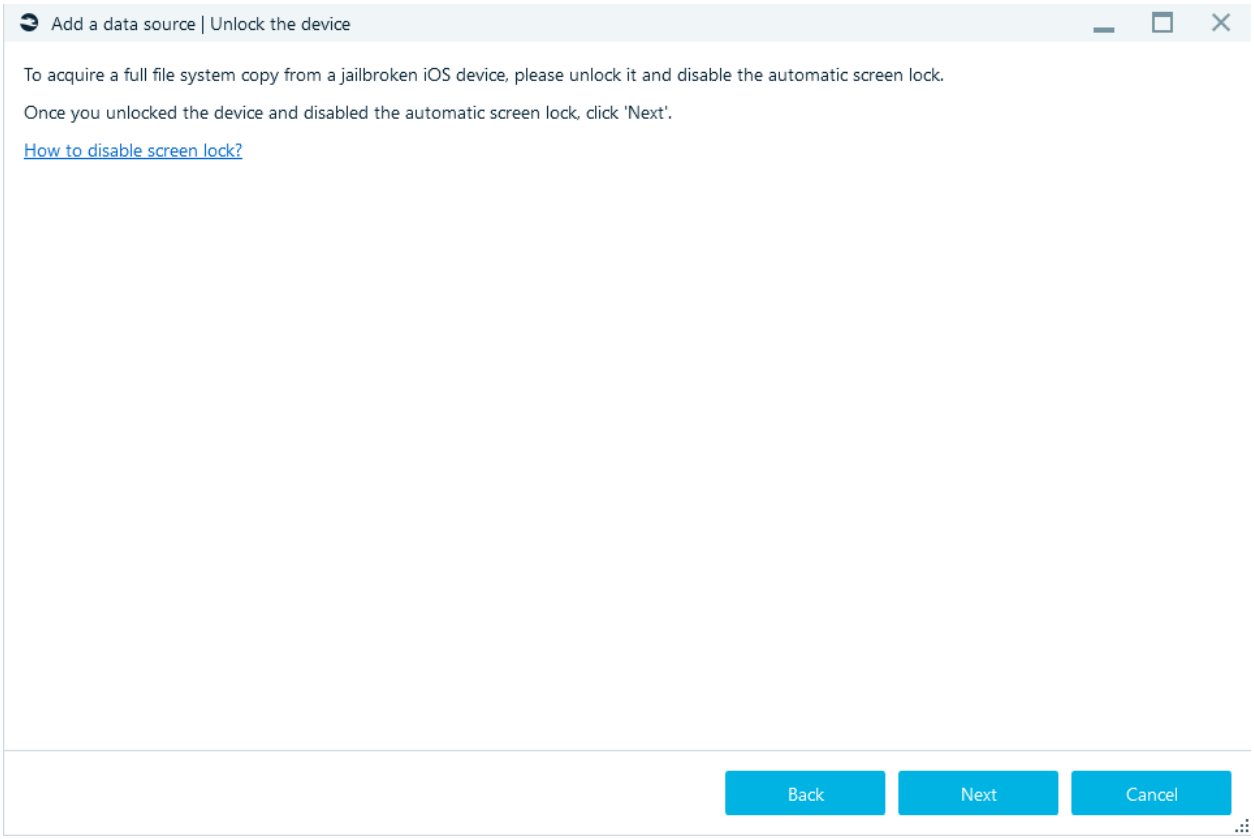
This acquisition method is only available for jailbroken iOS devices; however, it allows extracting much more data than by using standard iTunes backup.
This requires iTunes to be installed on the machine running Belkasoft X.
After choosing **Jailbroken device image** and connecting smartphone, you will see the window below:



After clicking on the **Next** button, the jailbreak status of the phone will be checked. If Jailbreak has not been completed on the device, a message will appear:



If Jailbreak has been completed on the device you will see:



Then select Target folder, click Start, and the acquisition process begins. Once the process reaches completion, you will see the iPhone or iPad image, which comes out as a TAR archive housing all the acquired data (including keychain).

Checkm8-based acquisition of iOS devices

The Apple Checkm8 function provides direct access to the file system of iPhones/iPads and allows for forensically sound extraction of data from the devices.
Compatible devices include the range of iPhone devices powered by Apple's A7 through A11 SoC.
Supported **iPhone models:**

- 5S
- 6/6 Plus; 6S/6S Plus
- SE
- 7/7 Plus
- 8/8 Plus
- iPhone 10 (X)

Supported **iPad models**:

- Air
- Mini 2
- Mini 3
- Mini 4

- 5
- Pro 2 12.9
- Pro 10.5
- 6
- 7

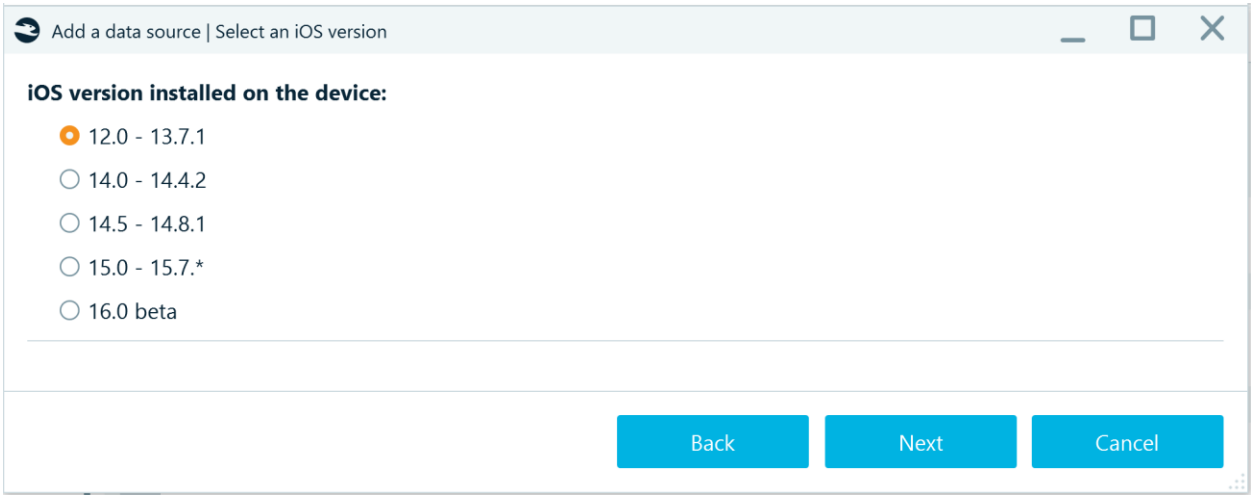
Supported iOS versions:

- iOS builds starting from iOS 12.0 till iOS 16.0 beta.

Note: To run **Belkasoft X** and perform the task here, you need a Windows 10 PC with the latest iTunes version installed on it.
After selecting **Apple Checkm8**, connect the device to your PC using a USB cable.

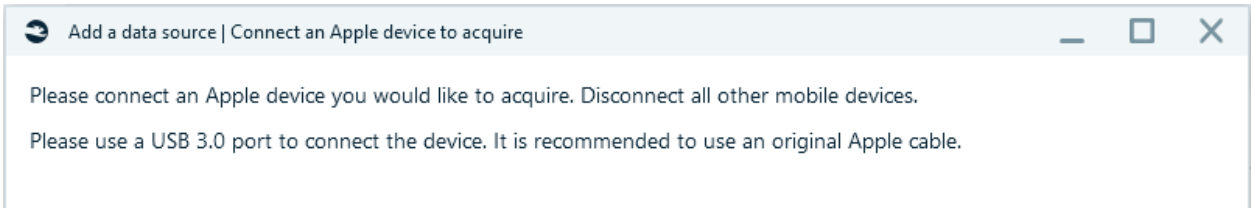
- The cable must be original
- Use a USB 3.0 port (or 3.1/3.2)
- It is better if the phone is password-protected - in this case, more data will be extracted (of course, if the password is known).
- Confirm the correct settings are set on the phone: **Settings - Display & Brightness - Auto-Lock** should be **Never**.

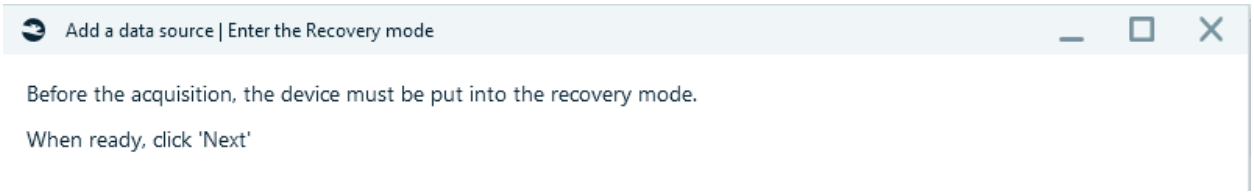
Choose the device iOS and model:



and follow the instructions on the screen:

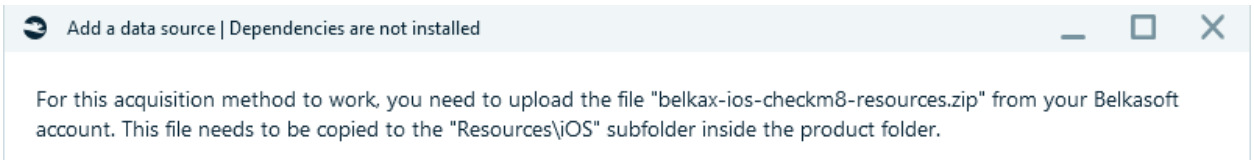
iOS version 12.0-13.7.1, 14.0-14.4.2:

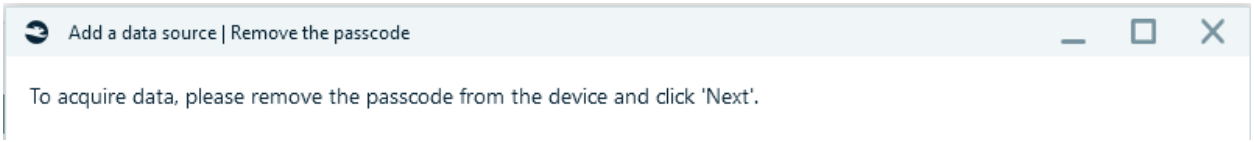


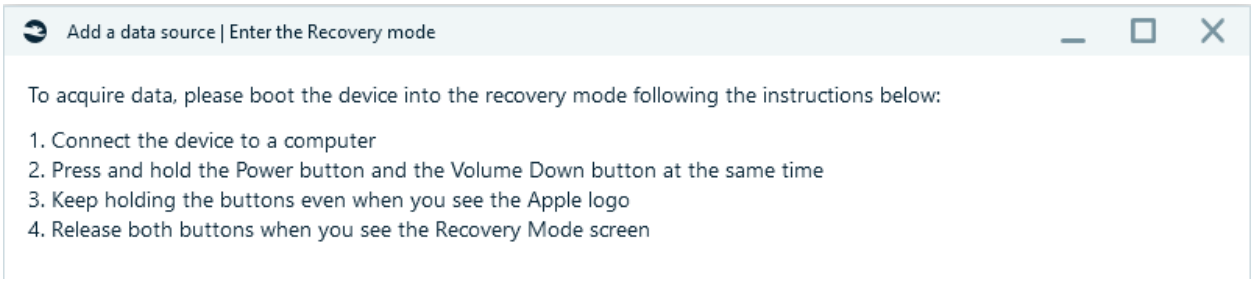


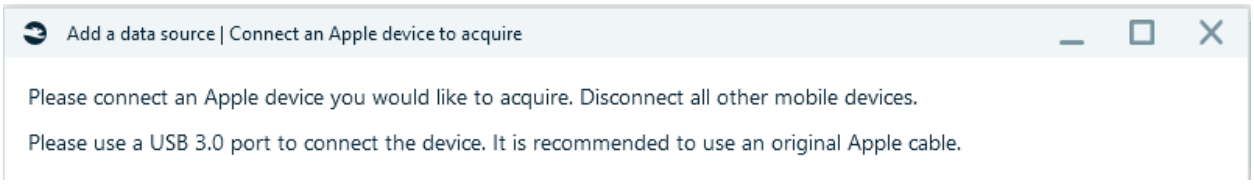
Put your iPhone into Recovery and then into DFU mode.

iOS version 15.0-15.6:

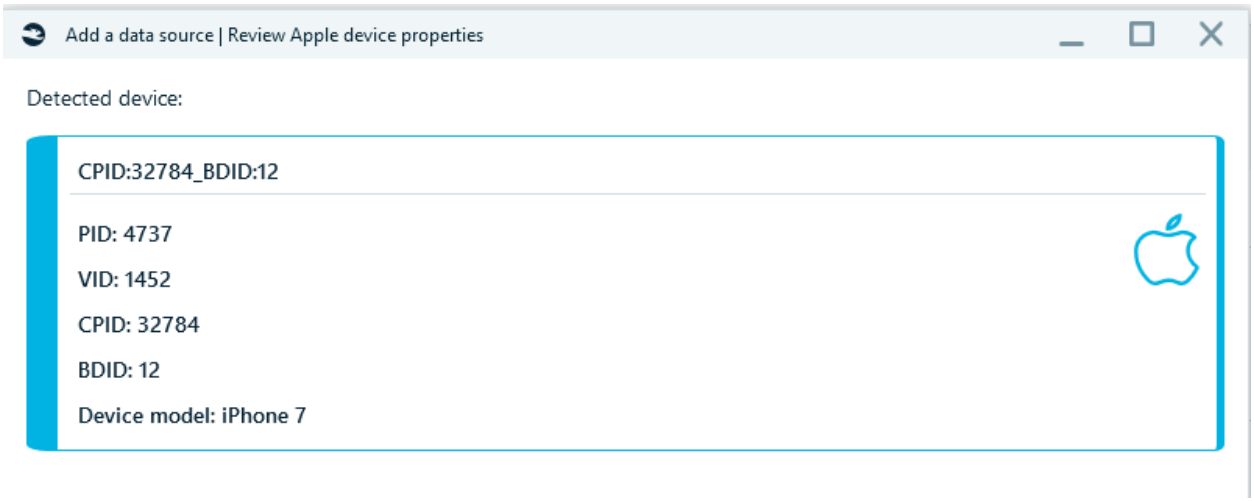


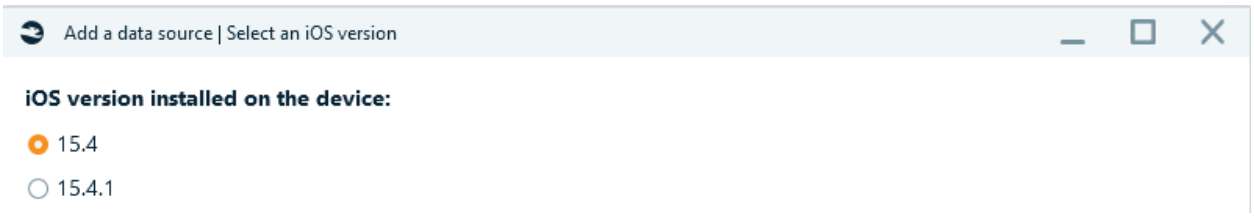




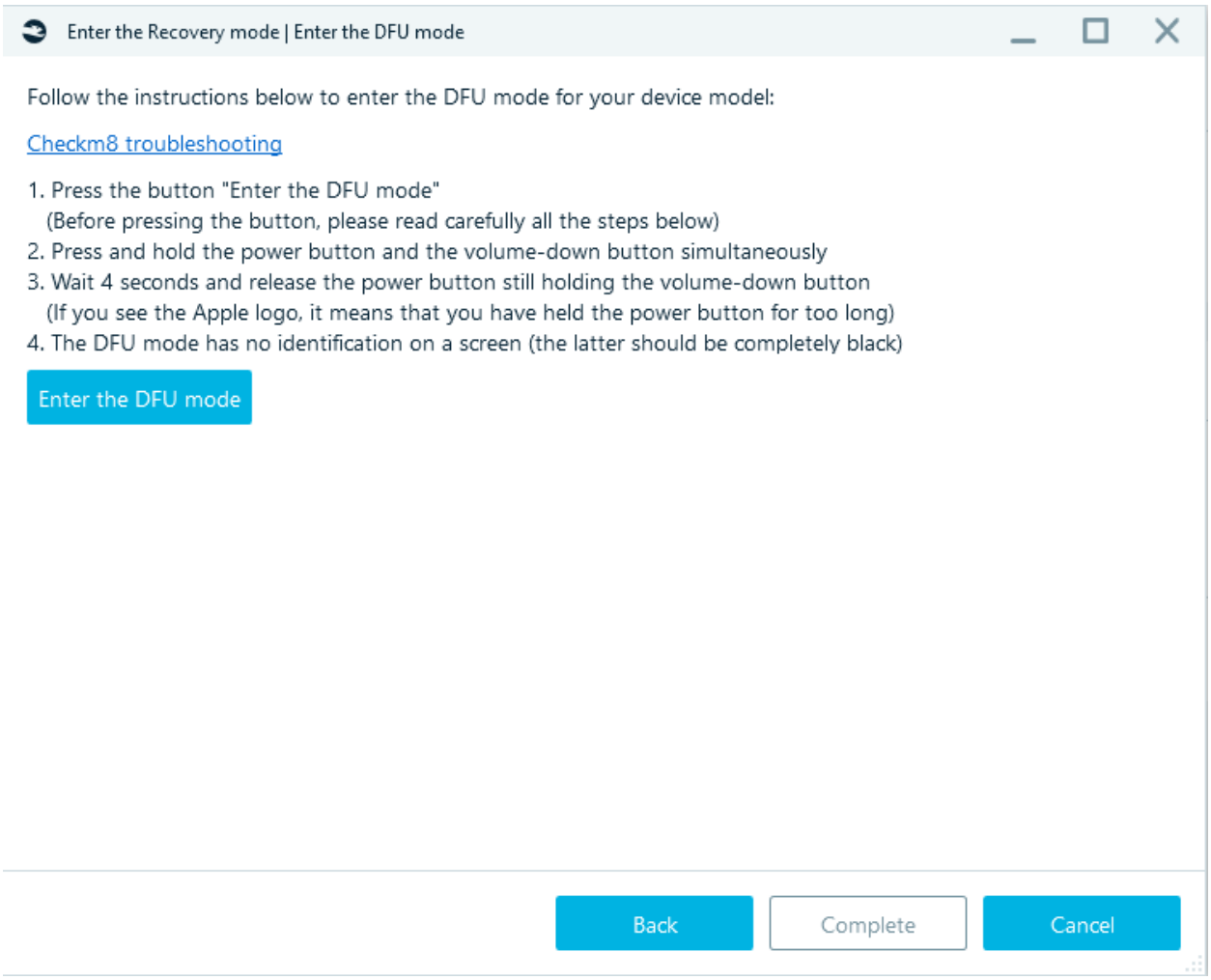


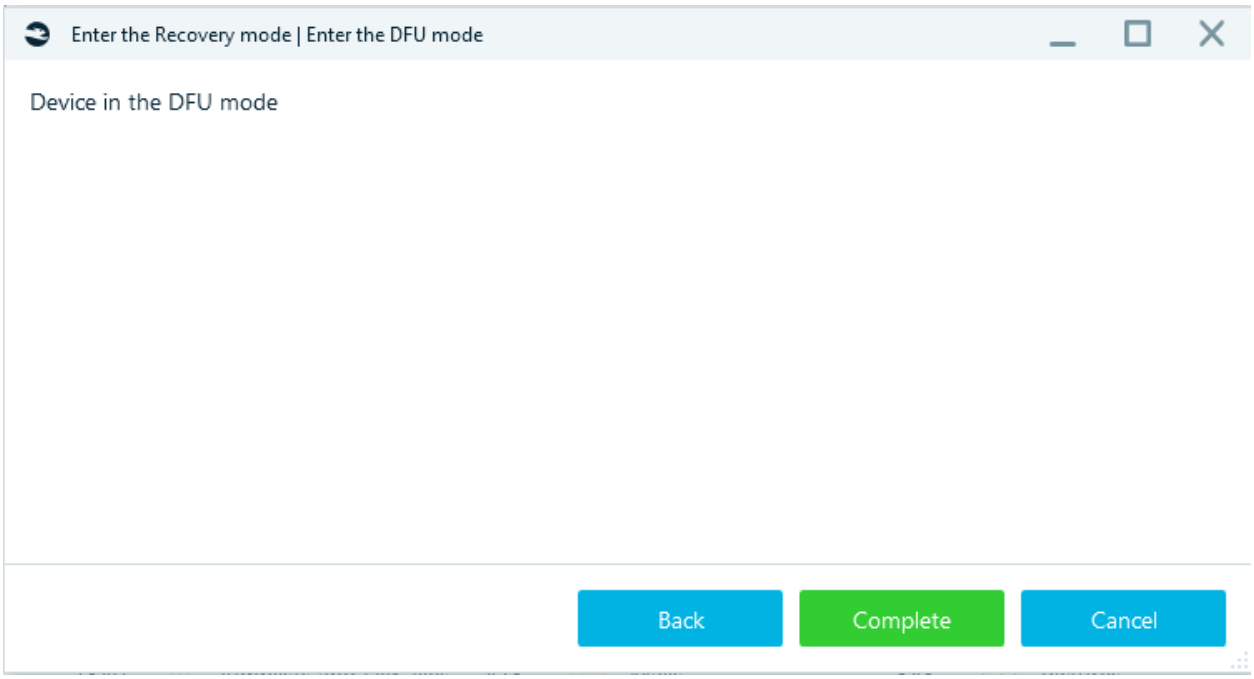
Then information about the connected device is displayed.





Put your iPhone into DFU mode.


Enter the Recovery mode | Enter the DFU mode
Follow the instructions below to enter the DFU mode for your device model:
Checkm8 troubleshooting
1. Press the button "Enter the DFU mode"
(Before pressing the button, please read carefully all the steps below)
2. Press and hold the power button and the volume-down button simultaneously
3. Wait 4 seconds and release the power button still holding the volume-down button
(If you see the Apple logo, it means that you have held the power button for too long)
4. The DFU mode has no identification on a screen (the latter should be completely black)
Enter the DFU mode
Back
Complete
Cancel

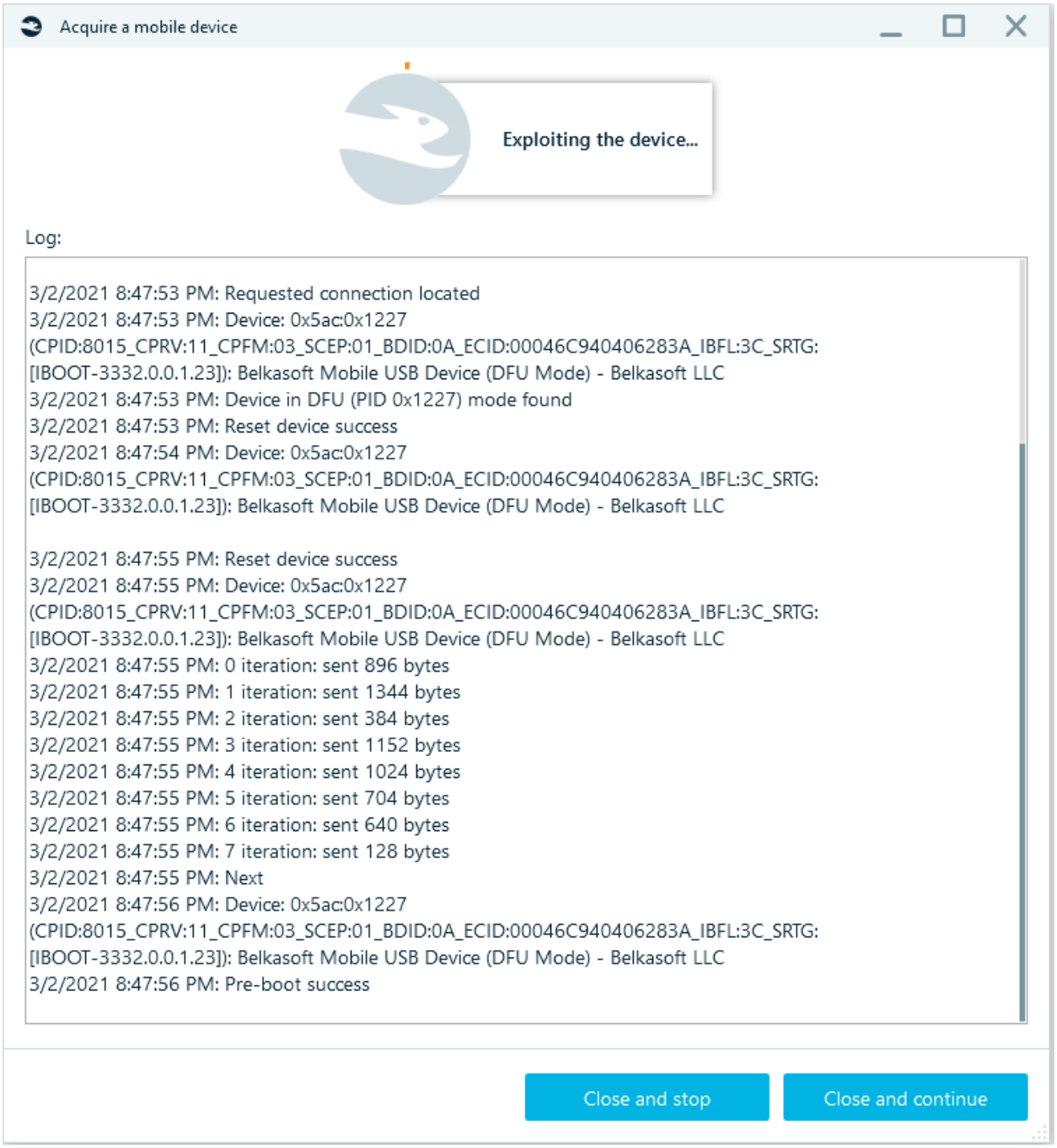

Enter the Recovery mode | Enter the DFU mode
Device in the DFU mode
Back
Complete
Cancel

Click on the **Complete/Next** button.

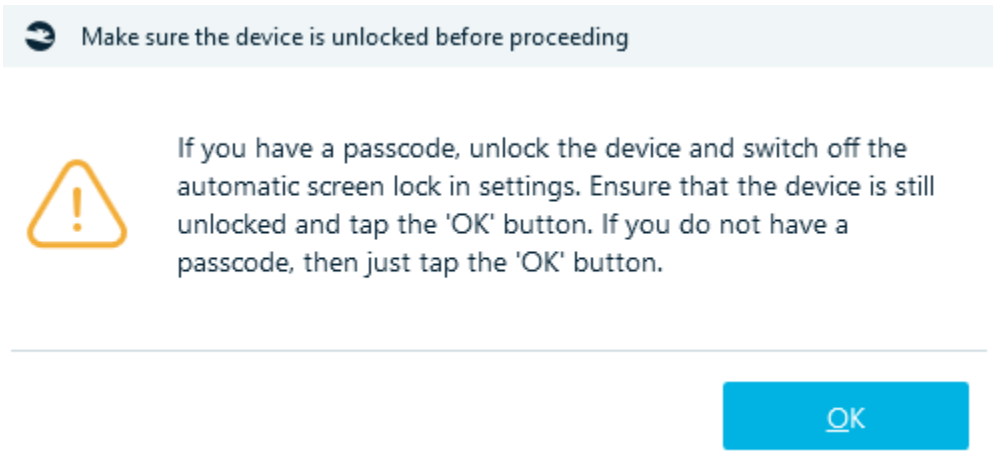
Specify the **Target path**, click **Start**, Belkasoft X will communicate with the device and run the exploit.

Belkasoft logo will appear on the phone screen:

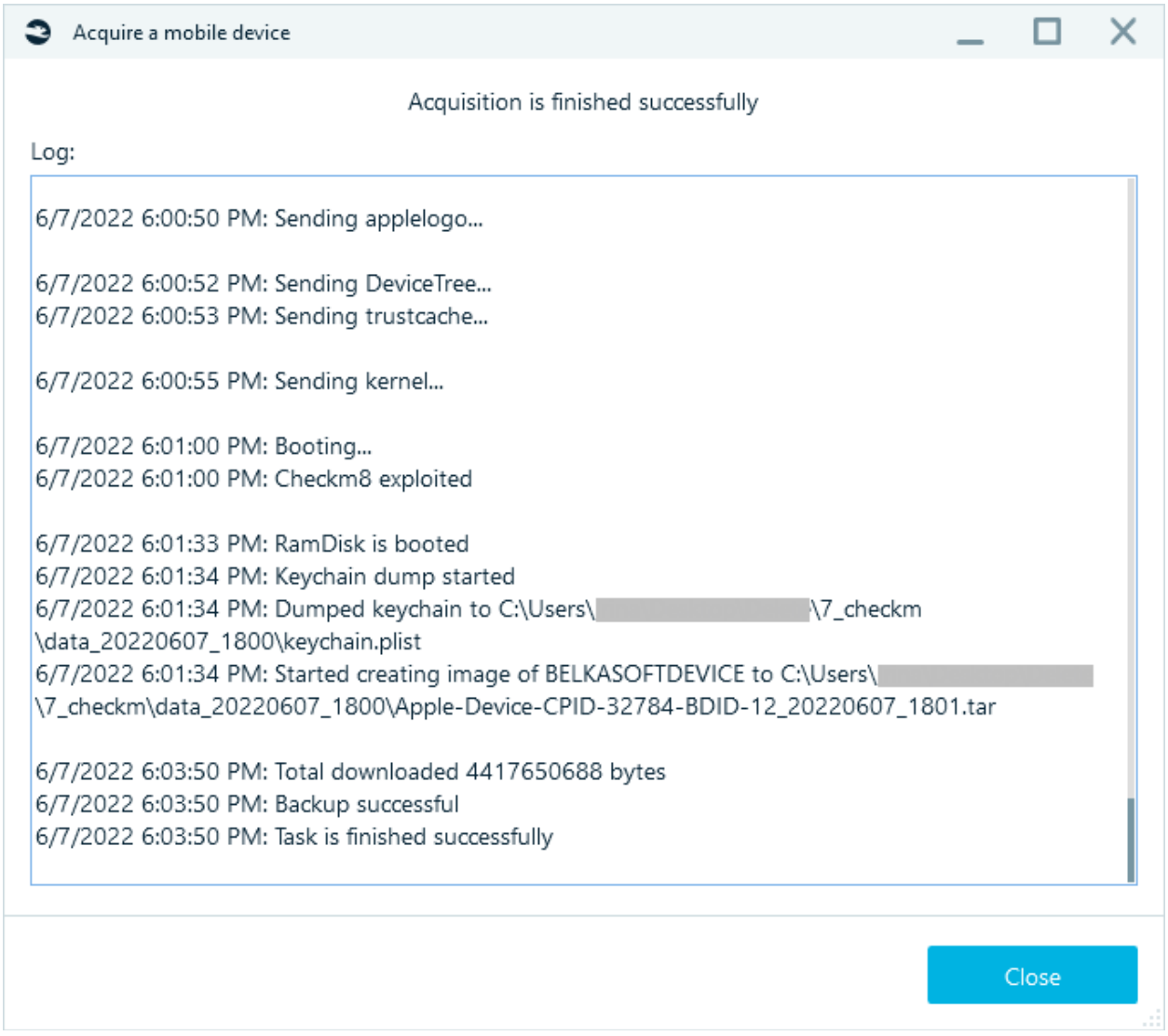
The events log will be displayed:



You should pay attention to them. Belkasoft X might prompt you to enter the passcode for the iPhone. If the password is known, use it to unlock the device now. Otherwise, if the passcode is unavailable, click on the **OK** button to dismiss the prompt. In any case, Belkasoft X will start copying data from the iPhone.



At the end of it all, you will see **Operation completely successfully** message.



AFC

This type of acquisition uploads data through **Apple File Conduit** (AFC) protocol**.** Available files: Photos, Videos, and some apps.
It requires iTunes to be installed on the machine where Belkasoft X is running.

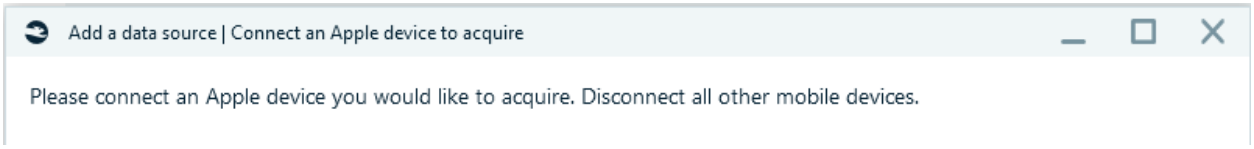
Crash reports

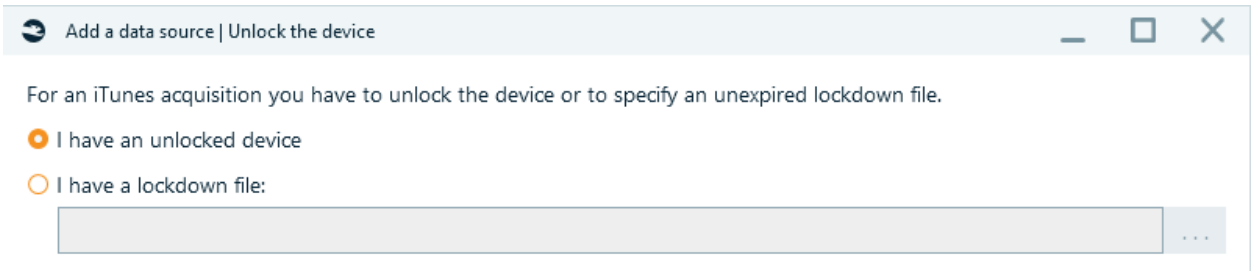
Extracting application and system crash logs on iOS.
To use this functionality, you do not need to jailbreak your device, it is sufficient to have a passcode or a lockdown file of the device.

Screen capturer

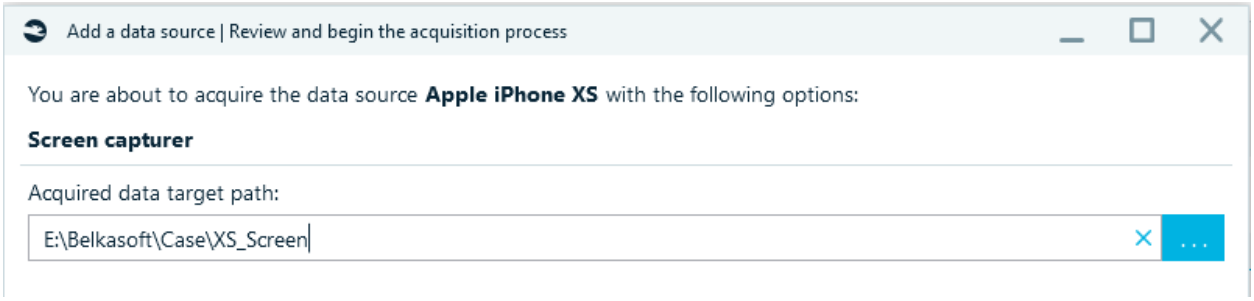
This method allows you to take screenshots from the screen of a mobile device.
iOS version supported for screen capturer: from 10 to 16.5.

Follow the instructions on the screen:

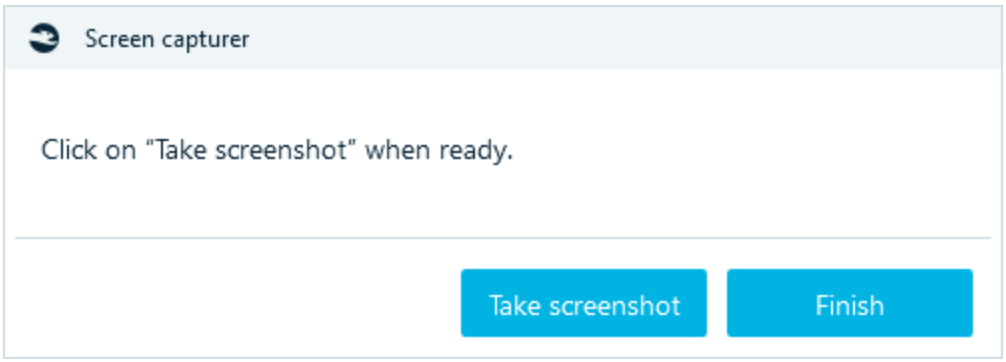




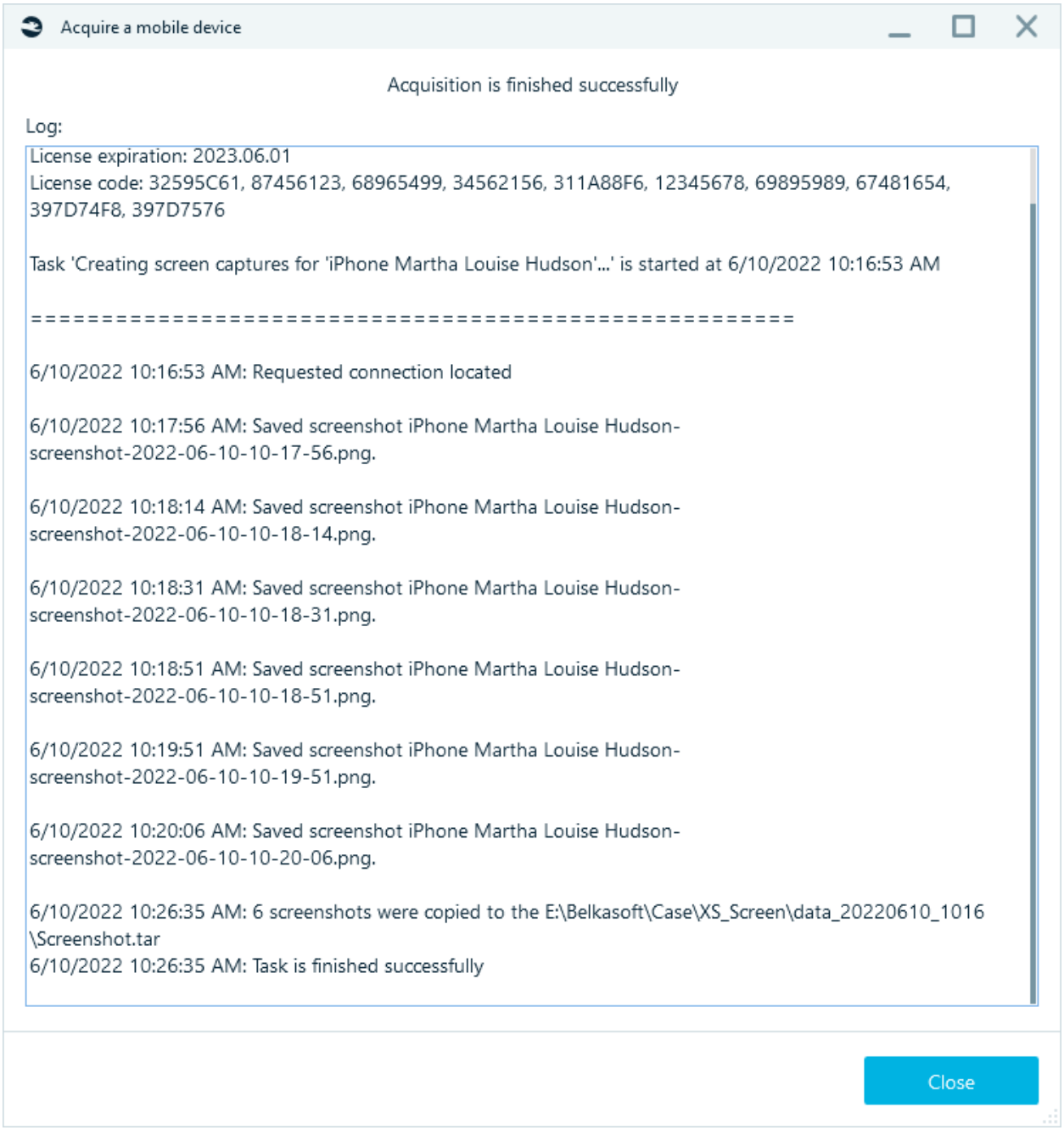
Specify target path and click Start.



By pressing **Take screenshot** to take the necessary screenshots and then pressing **Finish**.



All actions will be included in the task log:



FAQ

- Sometimes checkm8 works from second or third attempt only. Between attempts, please reboot the device twice.
- Some 3.0 ports do not work for checkm8-based acquisition. In this case, use 3.1/3.2 USB ports.
- If the phone was previously jailbroken with other jailbreaks (or many times with checkra1n), it is common that it does not work with checkm8.

- Phones having MDM tools installed, have issues with checkm8 and checkra1n. The proper acquisition is not guaranteed, it is recommended to unregister them from the corresponding MDM.

- Other forensic tools, which support checkm8-based acquisition on Windows, may interfere Belkasoft work. It is recommended to separate these tools.

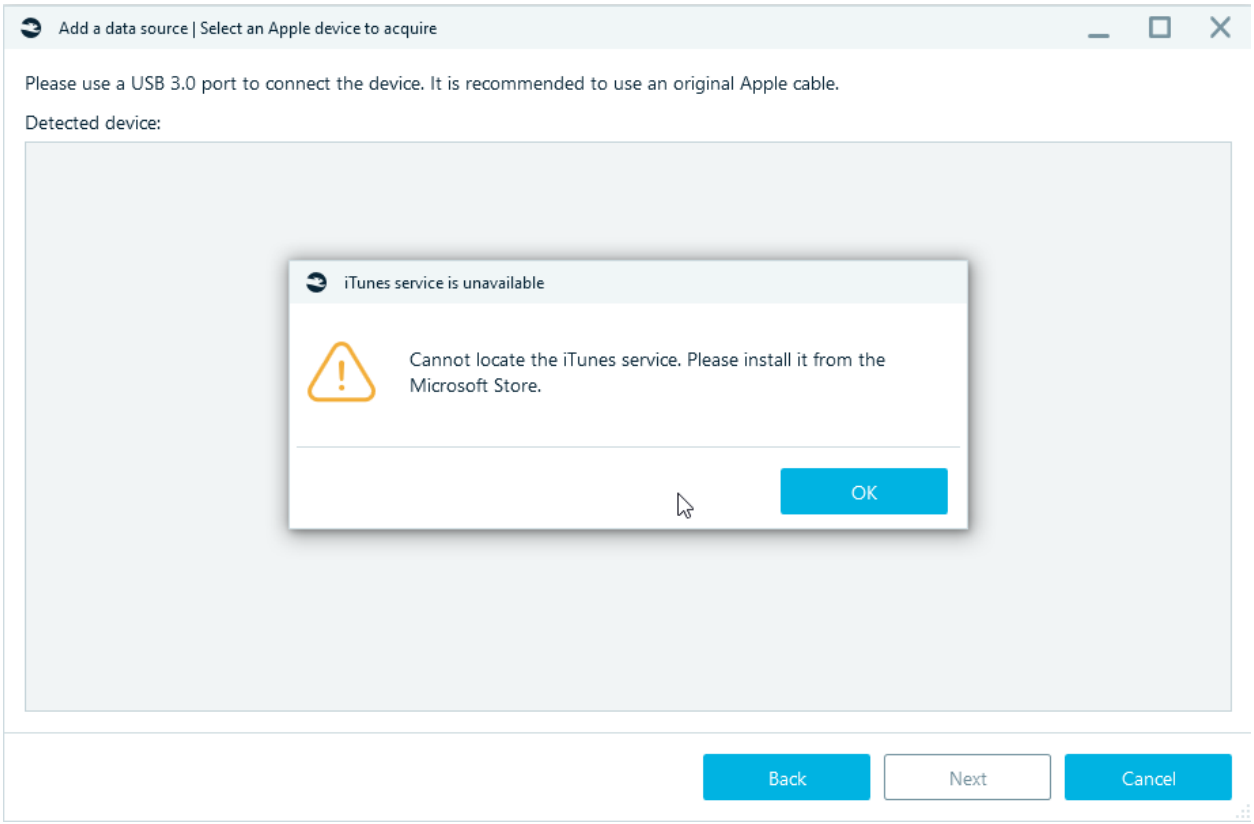
- If the **USB Restricted Mode is enabled** on the device and you do not have the passcode to an iPhone, you will be able to acquire data in BFU (BFU is an acronym for Before First Unlock). Belkasoft X disables USB Restricted Mode automatically during the checkm8-based acquisition process. You do not even need to perform manual or complicated maneuvers.

  BFU acquisition can still provide you a lot of data. Here, you can see the results from one of our experiments—Belkasoft checkm8-based acquisition from the same iPhone with and without the passcode:

	Locked (without the passcode)	Unlocked (with the passcode)
Audios	2367	2370
Autorun applications	393	393
Browsers	-	1109
Calendar	-	109
Calls	-	330
Chats	-	134
Cloud files	-	2
Contacts	14	232
Documents	918	959
Encrypted files	160	205
File transfers	-	32
Geolocation data	-	3
Installed applications	182	8189
Mails	-	1600
Notes	-	9
Notifications	1	9
P2P	-	10
Passwords	-	638
Pictures	10981	11972
SMS	-	30
System files	5476	13721
Tracks	1	725
Videos	1299	1332
Voice mail	-	4
Wi-Fi connections	5	5

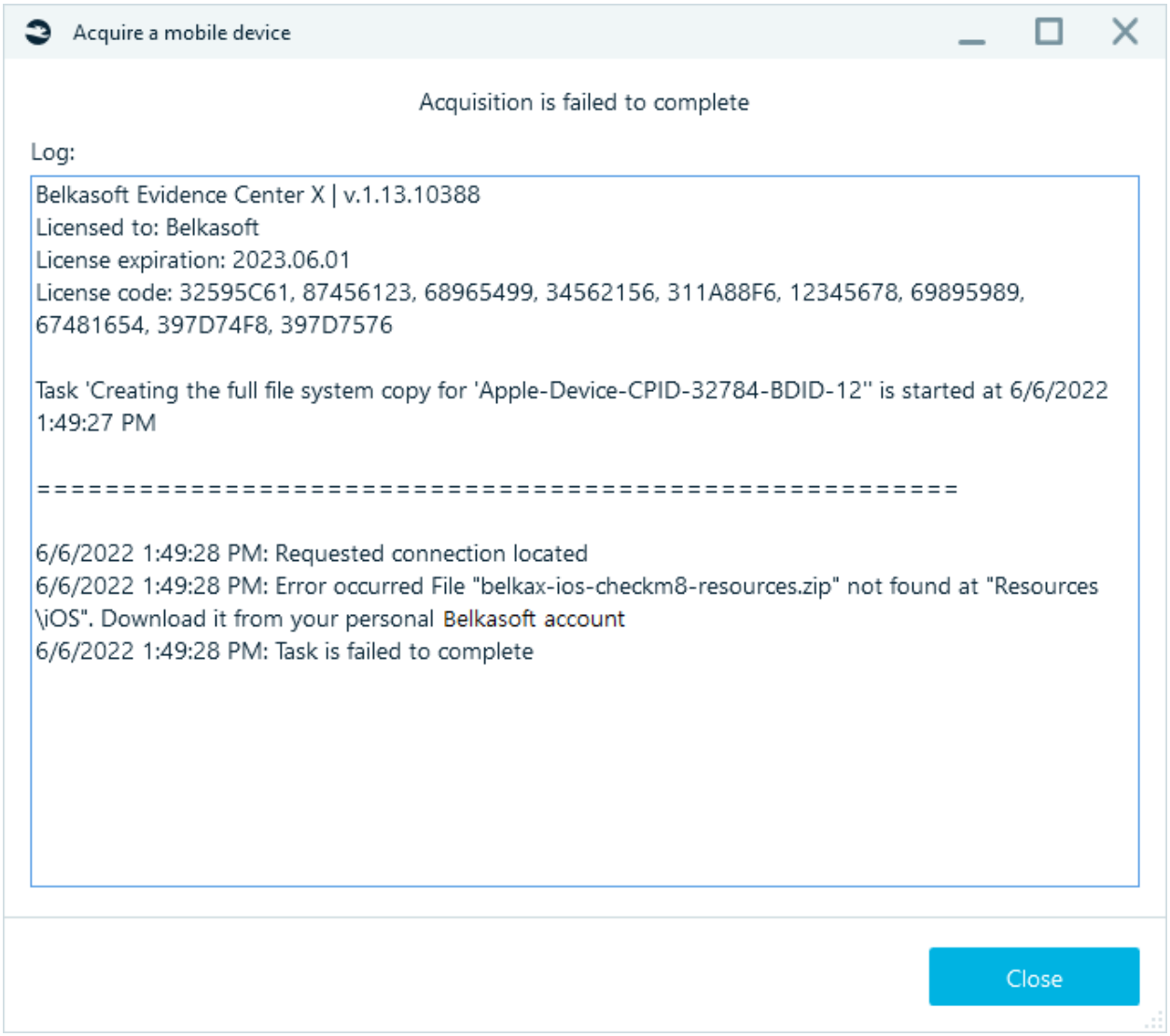
Wireless configurations	8	8

- If in the process of preparation for acquisition message ‘Cannot locate the iTunes service. Please install it from the Microsoft Store appears:



Try opening iTunes or reinstalling. The list of services should contain: **AppleMobileDeviceService.exe (AppleMobileDeviceProcess.exe)**, **ApplicationFrameHost.exe**.

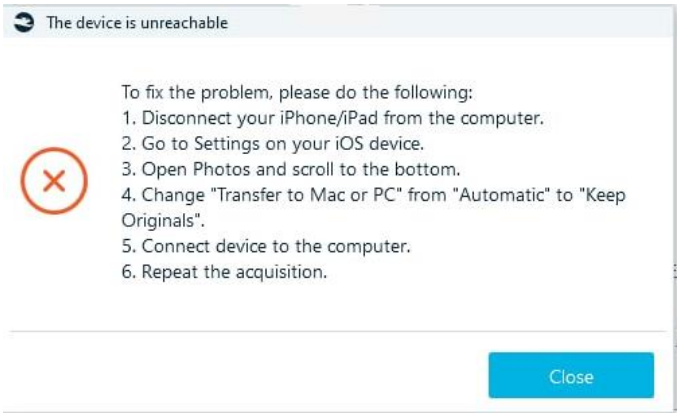
- If you suspect that the issue is with the Belkasoft product, try manual checkra1n. If it does not work either, most possibly, you will not be able to acquire the device with software-based methods.
- Error occurred File "belkax-ios-checkm8-resources.zip" not found at "Resources\iOS". Download it from your personal Belkasoft account.



Download "belkax-ios-checkm8-resources.zip" from the personal account of **Belkasoft.com** in the **Downloads** tab:

Put "belkax-ios-checkm8-resources.zip" in the folder …\Belkasoft Evidence Center X\Resources\iOS. **Do not unpack.**

- AFC acquisition
  System.Runtime.InteropServices.COMException (0x80070141) in log.
  It happens because, by default, iOS devices convert media files to a PC-compatible format. To avoid this error, you need to disable automatic file conversion.



- Comparison table for methods iTunes and Jailbreak/Checkm8/Agent-based acquisition

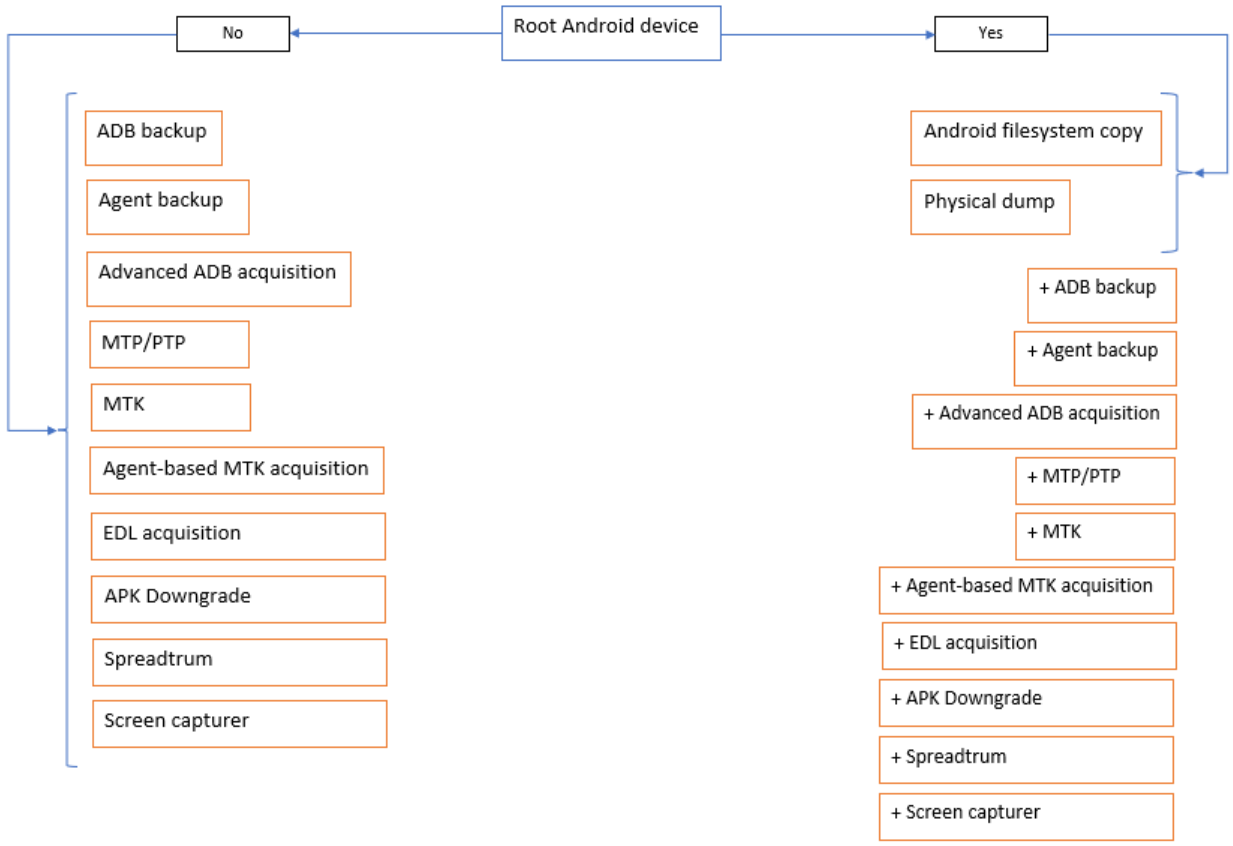
iPhone 7	FFS	iTunes
Files found (total)	**271851**	**1469**
Artifacts found (total)	**43237**	**8829**
Audios	1123	21
Browsers	3090	31
Chats	83	8
WhatsApp	*8*	*8*
Telegram	*52*	-
Skype	*23*	-
Documents	795	33
Installed applications	1267	157
Instagram	*364*	-
Driver	*910*	-
SMS	*226*	*224*
Health	*5149*	*5149*
Wi-Fi	*6*	*6*
Calls/Contacts	*101*	*18*
Calendar	*26*	*4*
Contacts by apps	*146*	-
Mails	952	183
Apple mail	*21*	-
Recents	*931*	*183*
Mobile applications	6928	5403
Other files	6	-
Passwords	1269	941
Pictures	8900	256
System files	18547	1781
Thumbnails	101	-

Videos	176	15

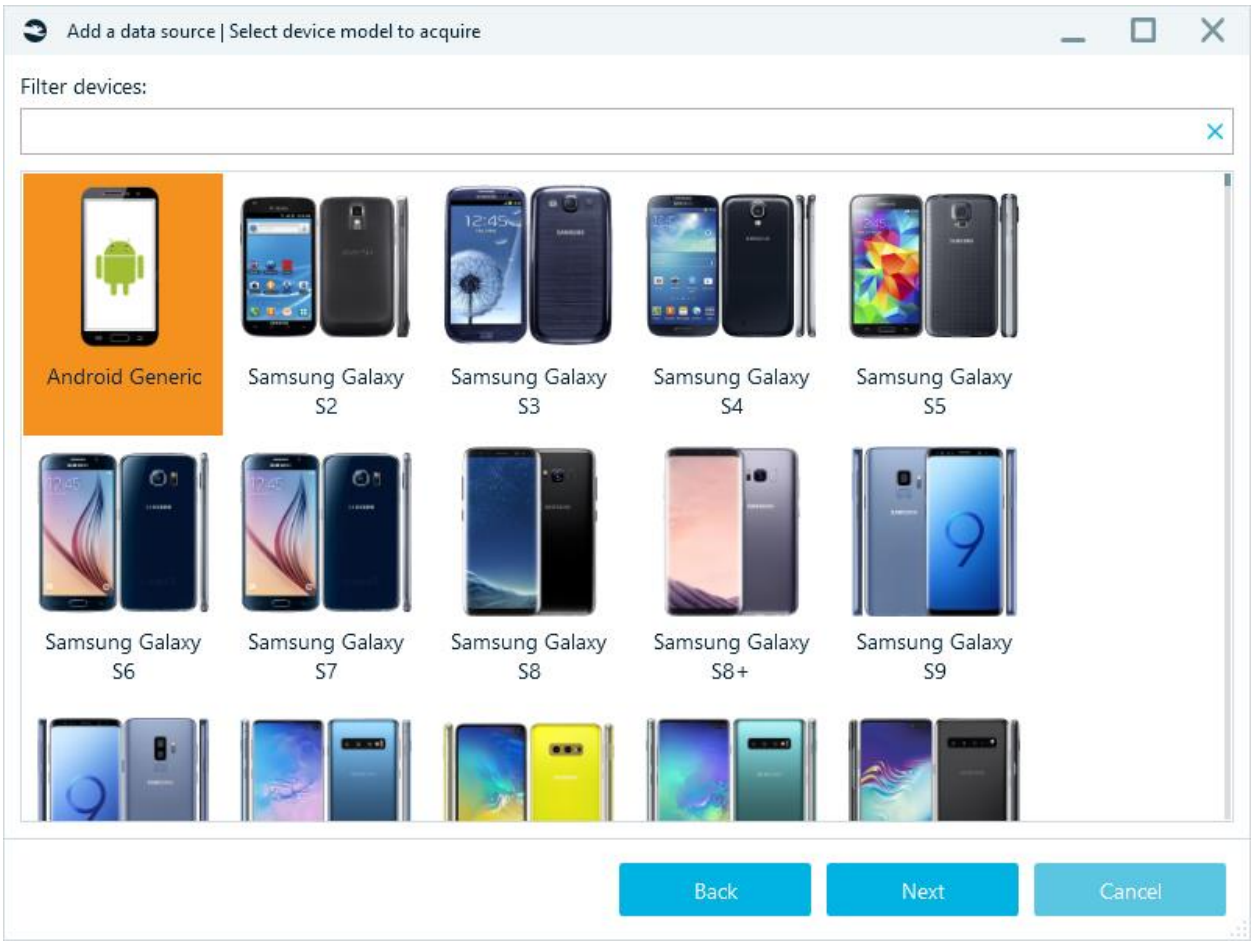
Keychain extraction

Keychain is the password management system developed by Apple. Without the keychain, it is impossible decrypt the various encrypted data extracted with the full file system acquisition. Checkm8-enabled version of Belkasoft X can extract keychain not only via checkm8-based acquisition but also from any jailbroken iPhone, no matter which jailbreak was used. Based on the extracted information, various decryption tasks become possible. For instance, Belkasoft X can decrypt iOS Signal and Wickr messengers out of the box.

Android

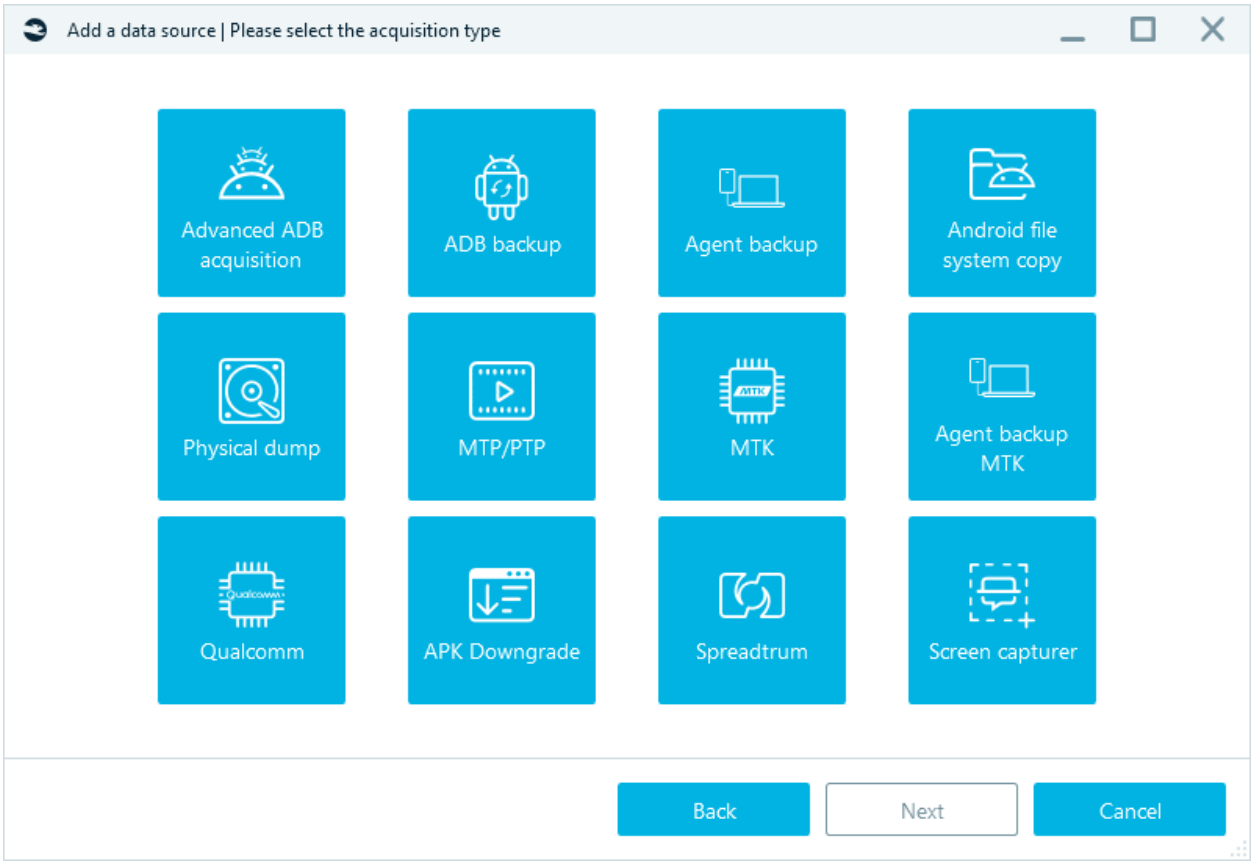


After clicking on **Android,** a list of devices will be displayed:



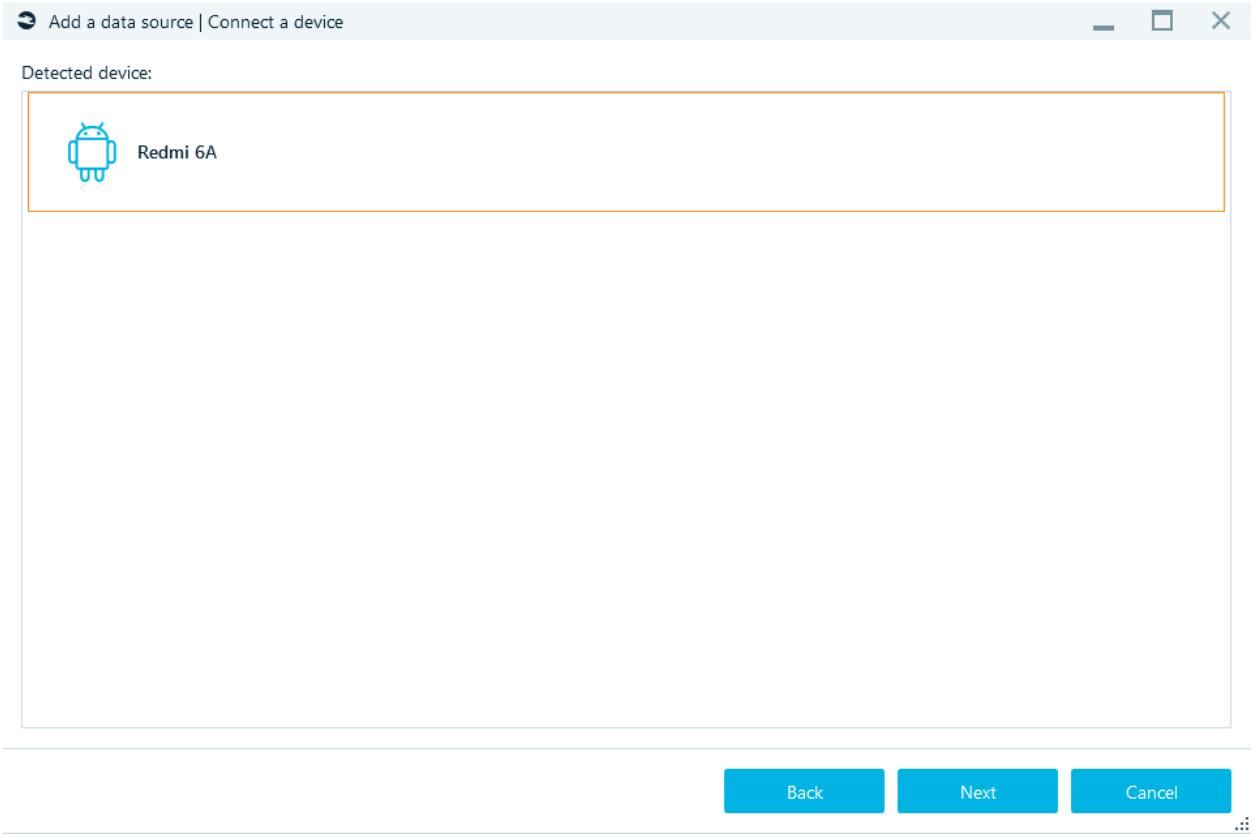
Use the filter to select the device model, if the device model is not shown in the list, select **Android Generic**.

In the next step, in the window **Add data source| Please select the acquisition type**, you will see screen with list of acquisition types, available for the selected model.



ADB backup

This is a standard **ADB backup** available built-in the **Android** operating system and available on any **Android** device.
After choosing **ADB backup** and connecting smartphone, you will see the window below:



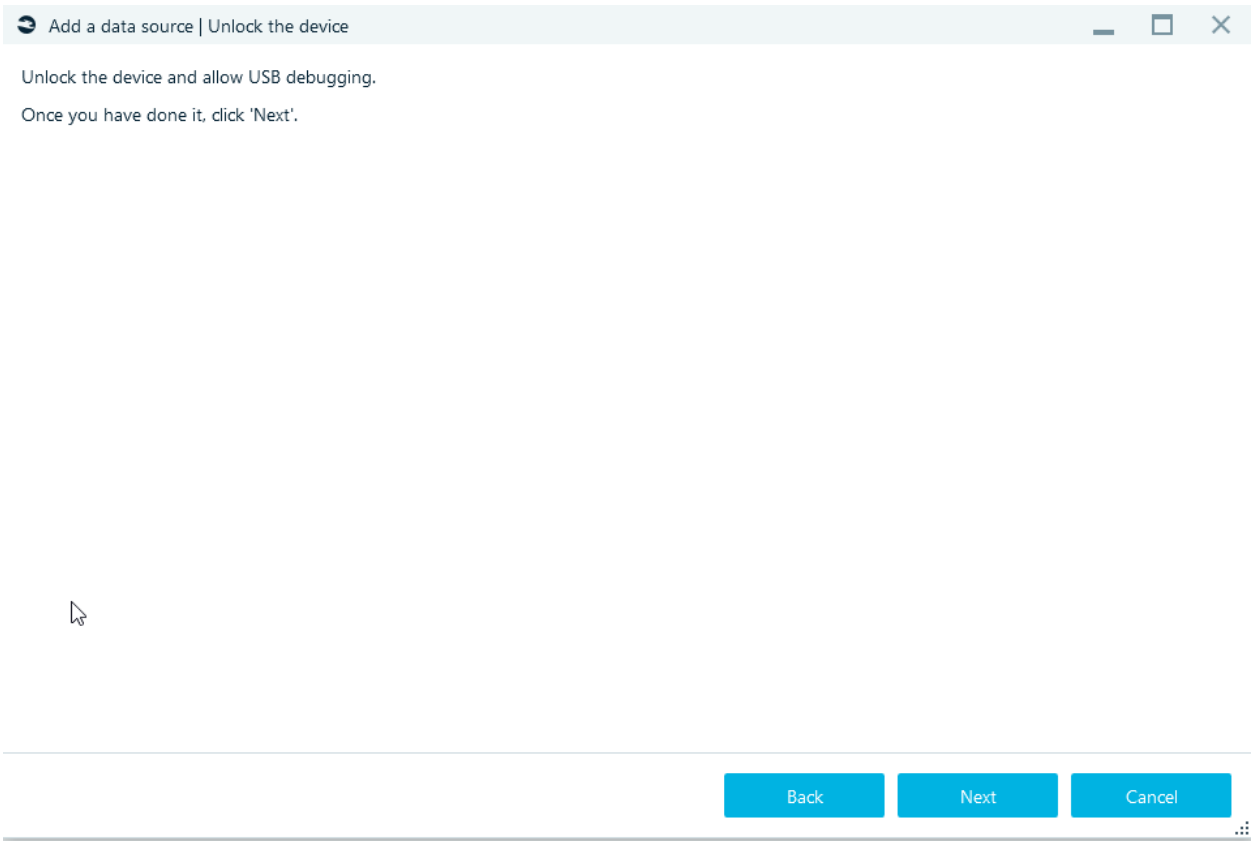
Unlock the device and allow USB debugging.
In **Full backup** window that appears **on the smartphone screen**, automatically will start creating a backup (with a password). If creating a backup does not start automatically, press **Back up my data** (without password).

Advanced ADB acquisition

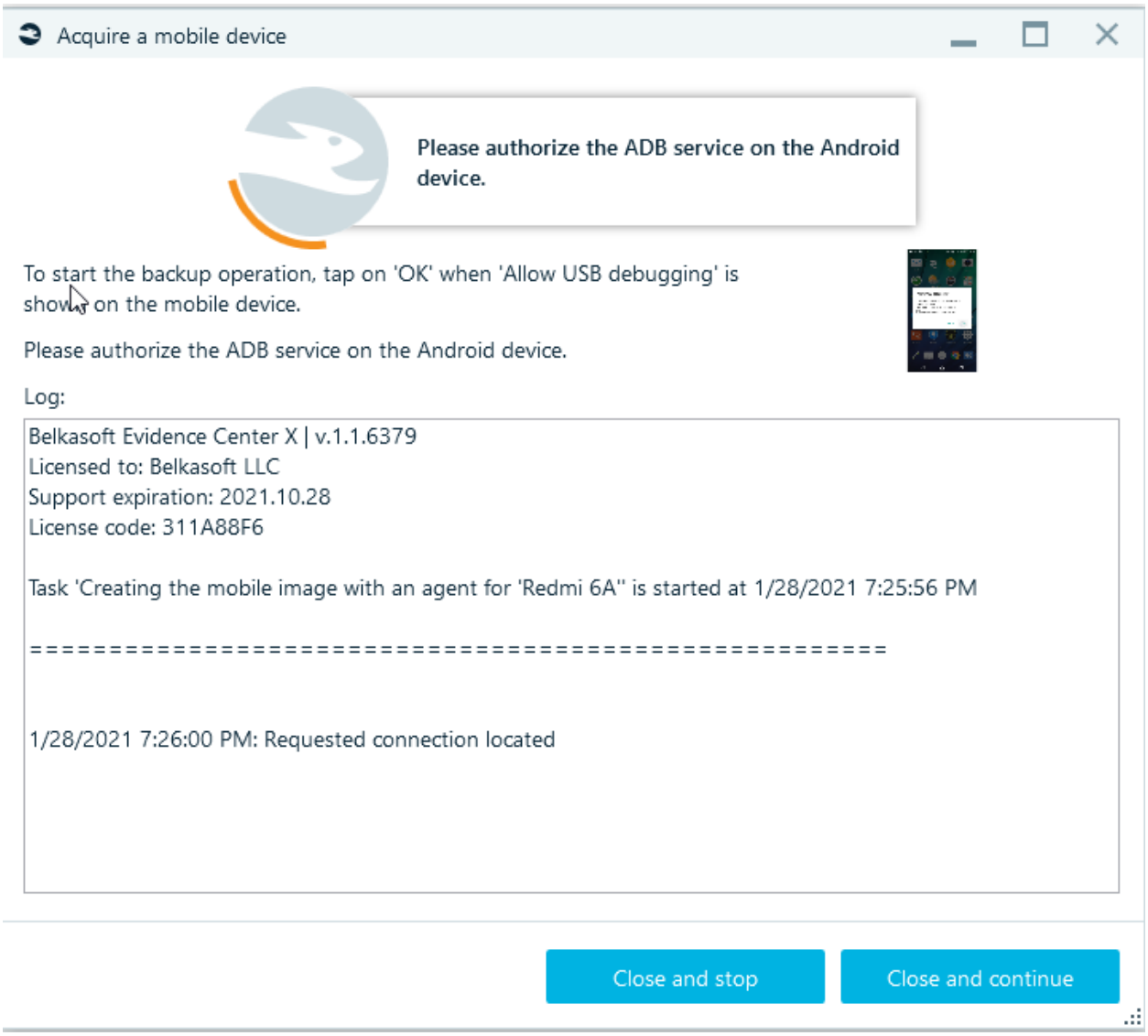
ADB backup with AT commands and Agent backup (more details about this features are described in the corresponding section). Combines the advantages of three methods.

Agent backup

This type of acquisition uploads and installs a special application ("agent"), which transfers data from the device to Belkasoft X. Upon the acquisition the agent is uninstalled.



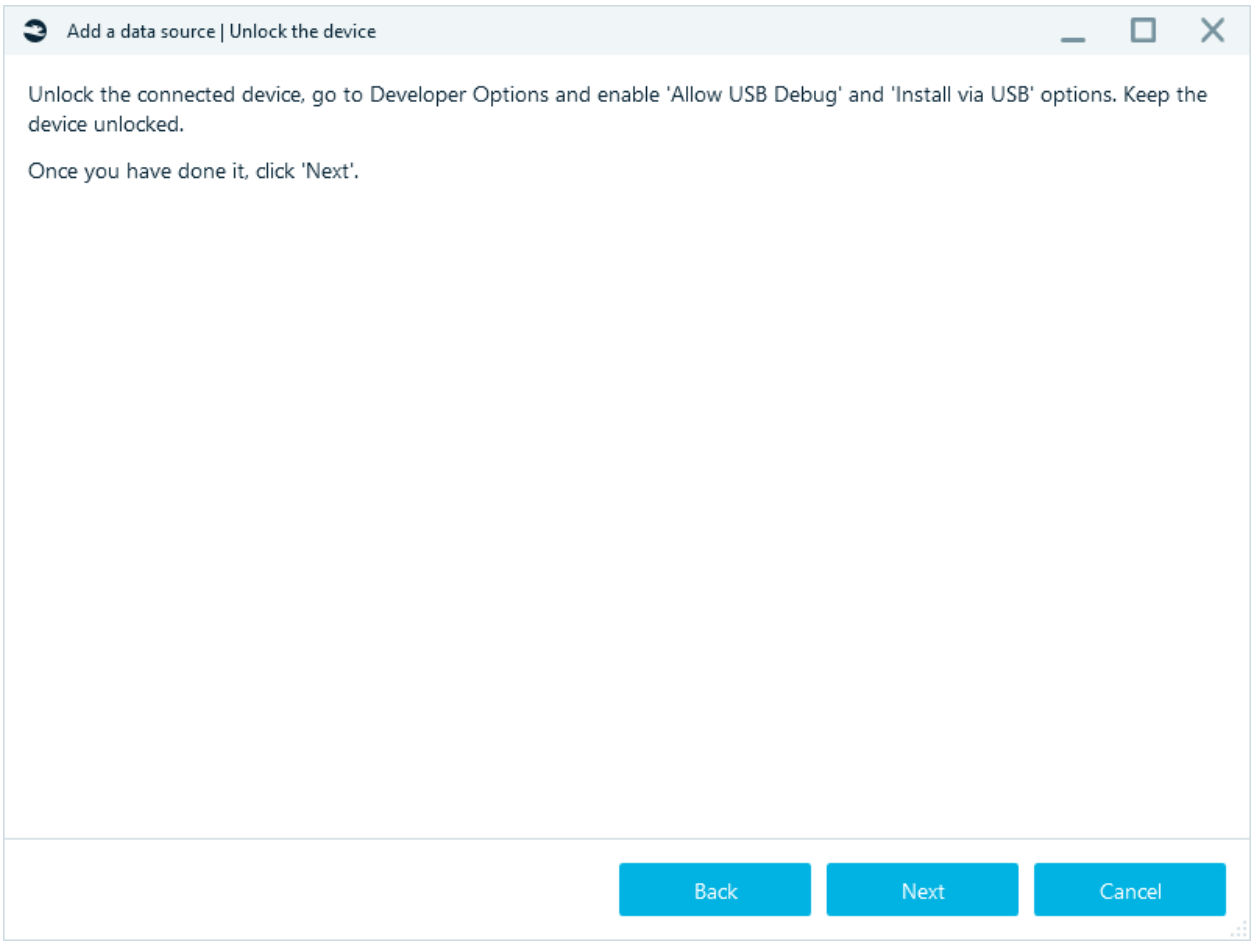
Unlock the device and allow USB debugging.
Acquisition will start after pressing the **Start** button.

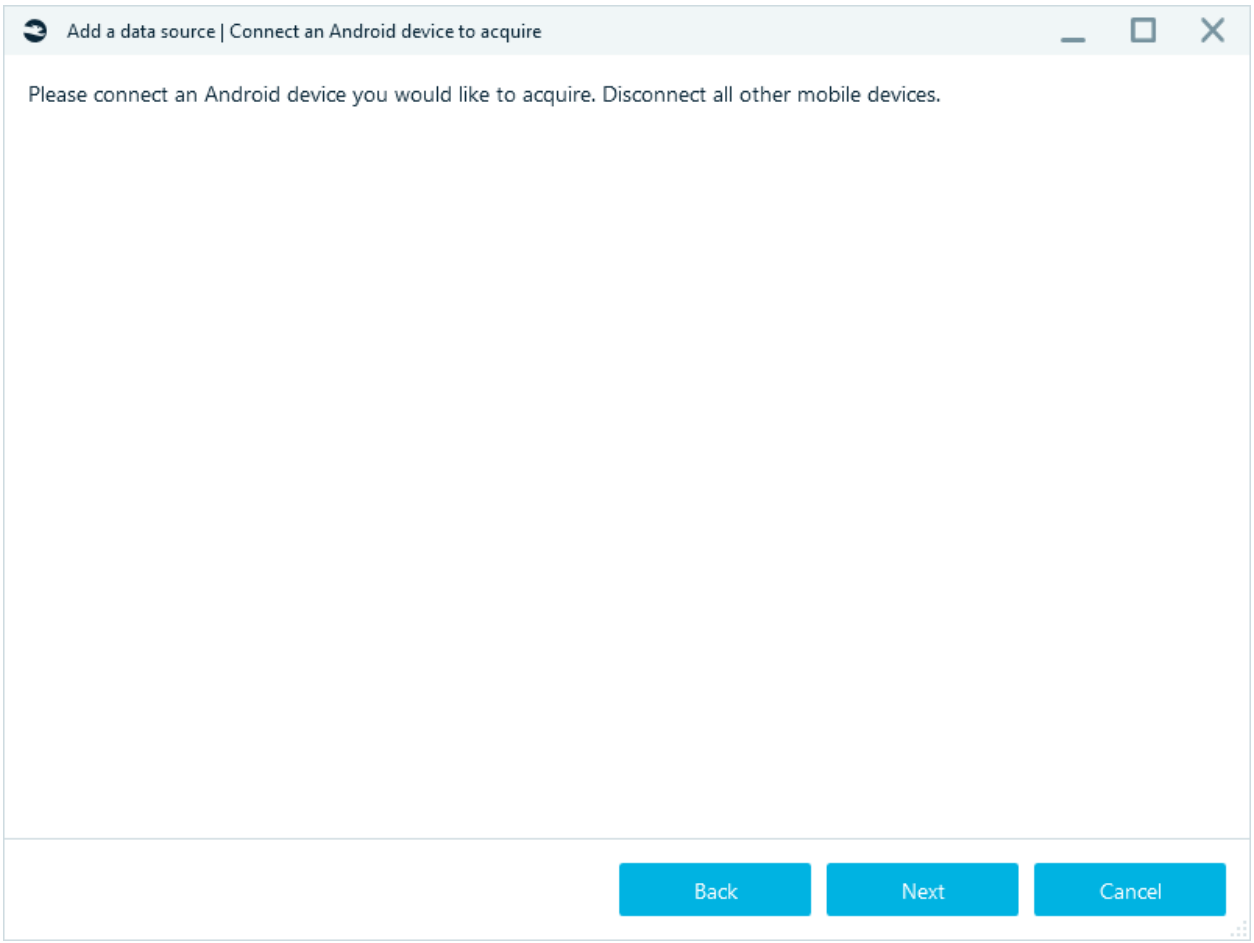


Android filesystem copy

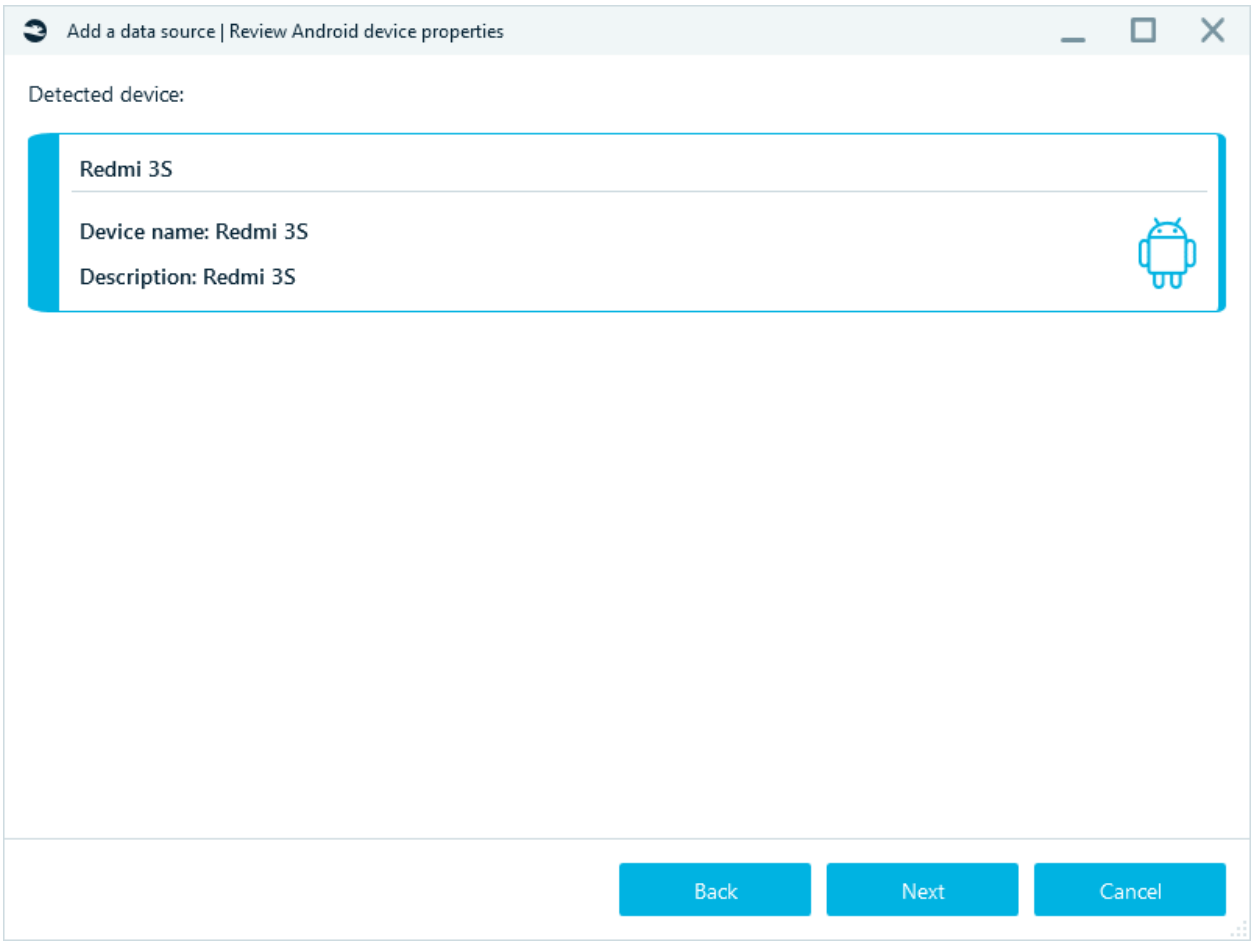
This method is available only for **rooted Android devices**.
Before starting acquisition:

- Unlock the device
- Enable **Allow USB Debug**
- Enable **Install via USB**
- Disconnect all other mobile devices

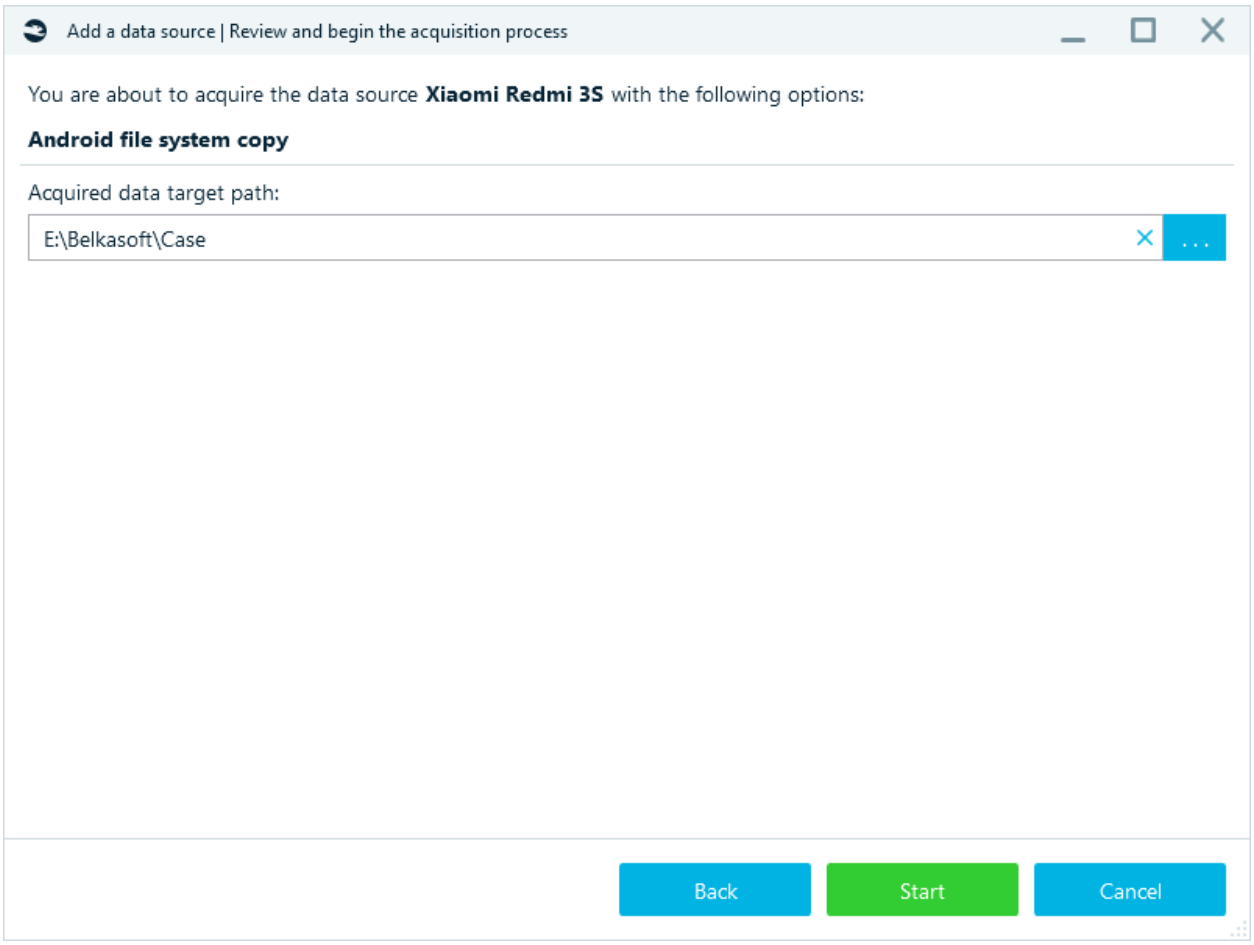

Add a data source | Unlock the device
Unlock the connected device, go to Developer Options and enable 'Allow USB Debug' and 'Install via USB' options. Keep the device unlocked.
Once you have done it, click 'Next'.
Back
Next
Cancel



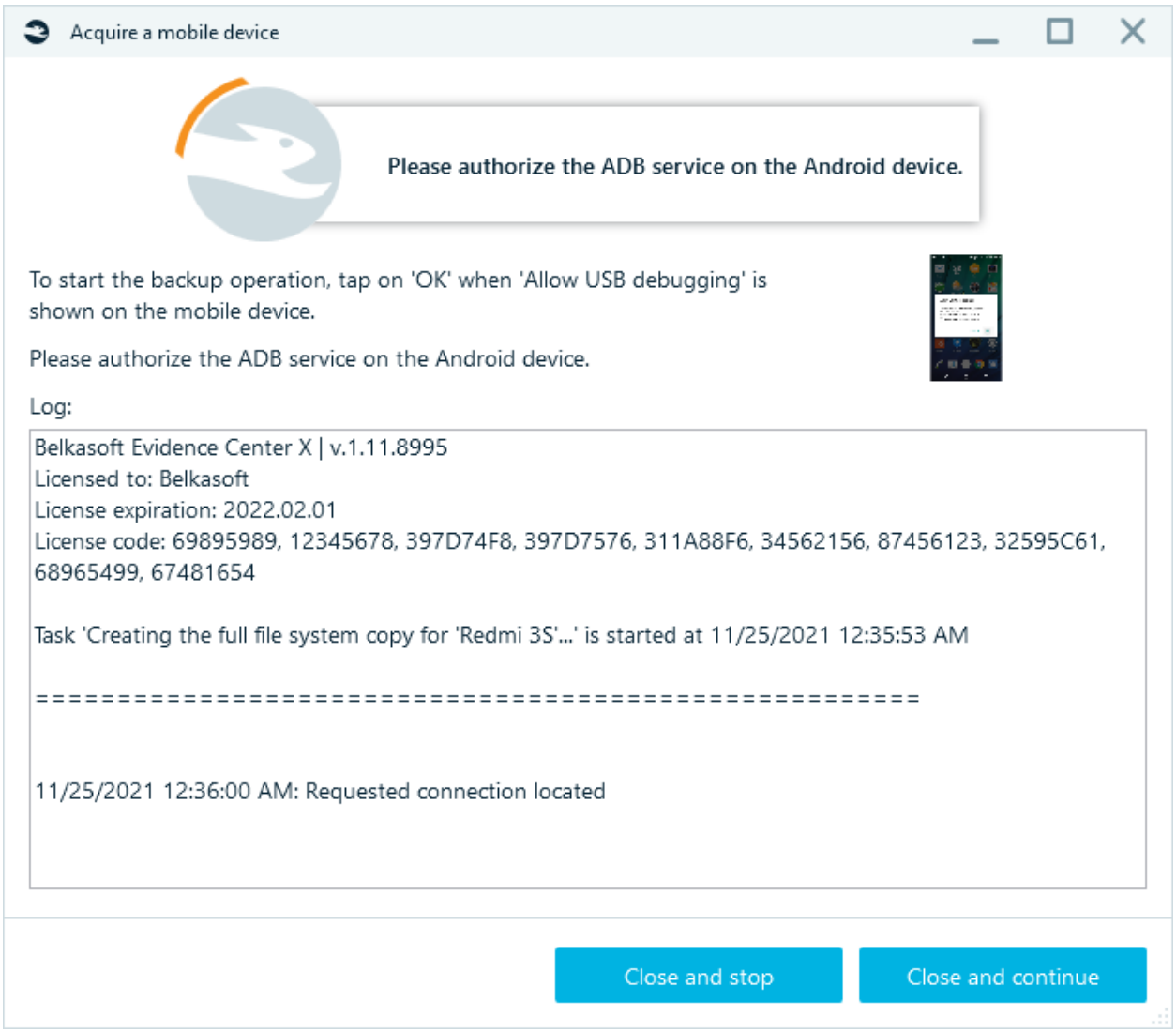
Check that the correct device is detected:



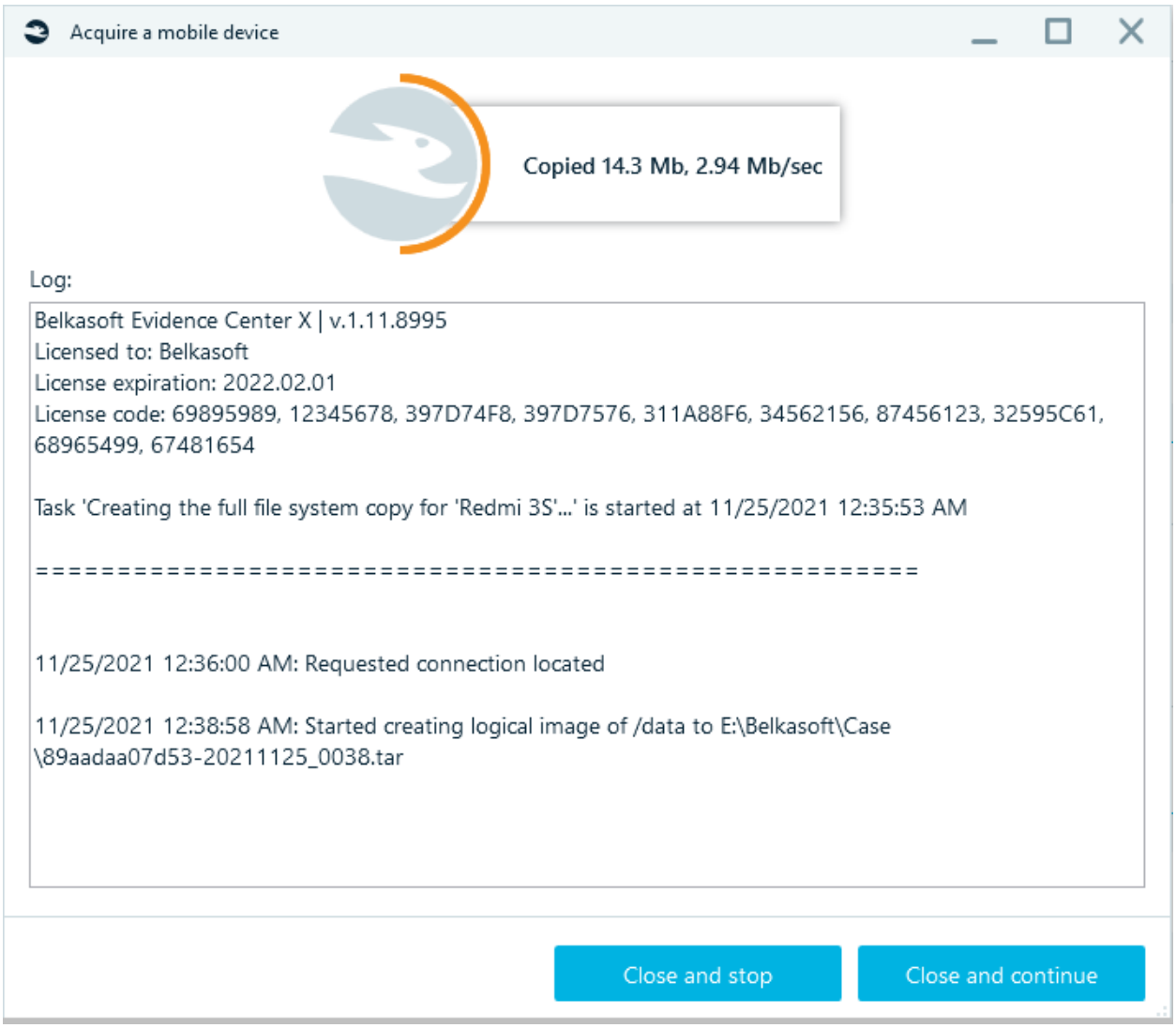
Specify target path:



Click **Start** - acquisition will begin.
Follow the instructions on the screen: authorize the **ADB service** on the Android device. Tap on '**OK**' when '**Allow USB debugging?'** appears.

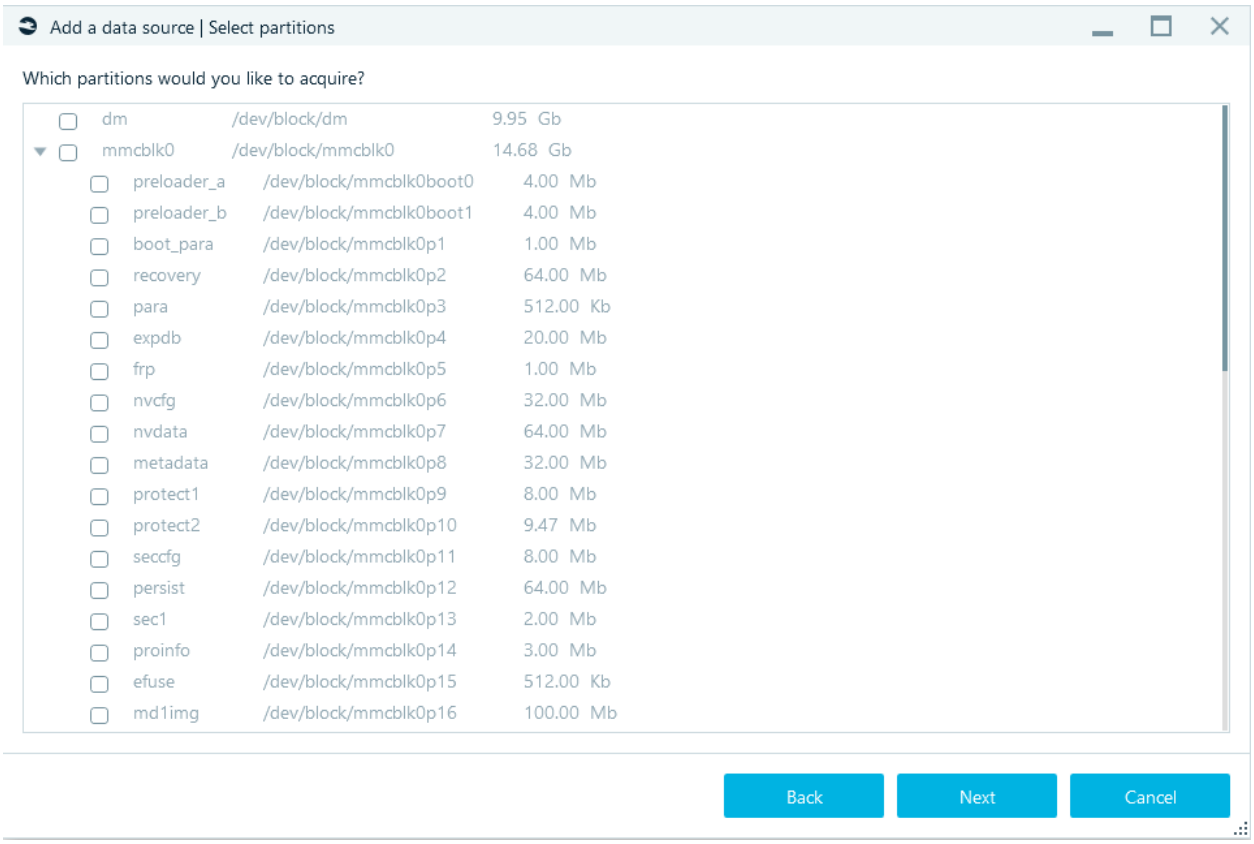


Creating the full file system copy will start:



Physical dump

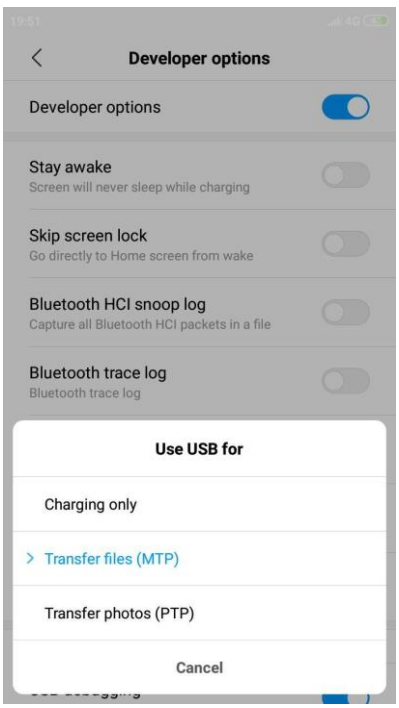
This method is available only for **rooted Android devices** and creates a physical backup of the selected device.
Connecting smartphone, unlock and turn off lock screen.
Select partitions and click **Next**.

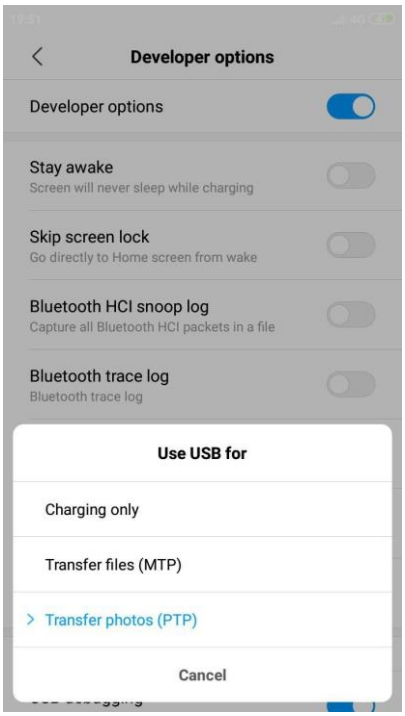


Specify the **Target path** (for the folder where the smartphone image will be stored).
Click **Start** - acquisition will begin.

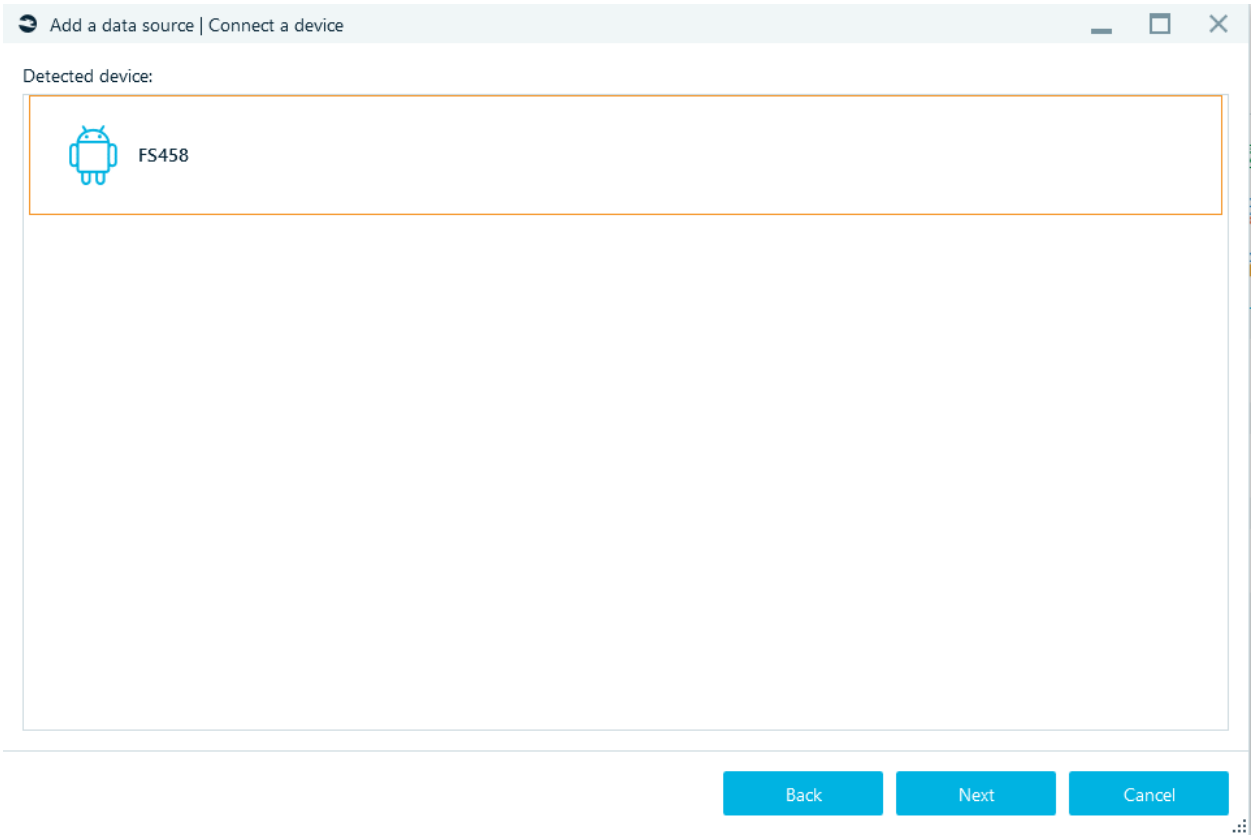
MTP/PTP

This type of acquisition uploads data through **Media Transfer protocol** / **Picture Transfer Protocol.** Before you start acquisition, connect device to the computer and select the appropriate mode in the settings:

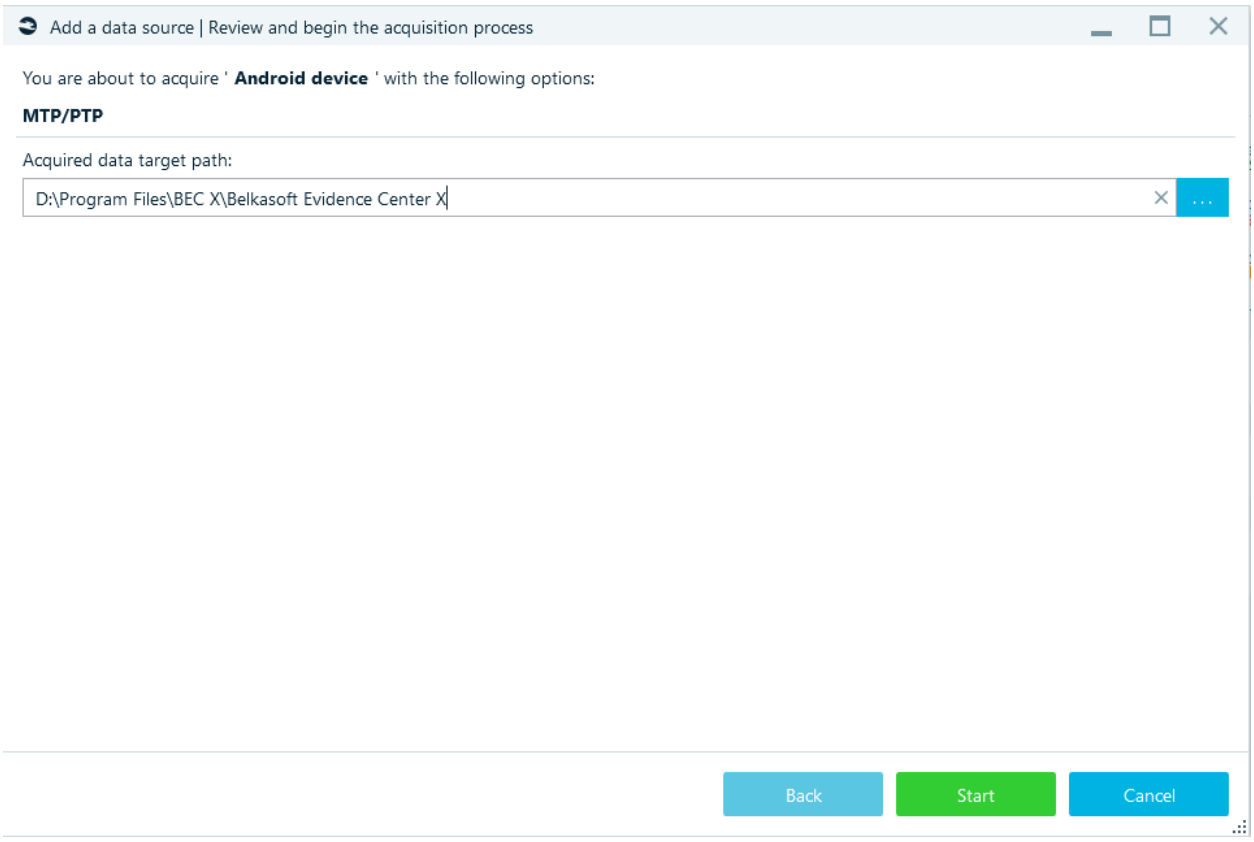




After selecting **MTP/PTP** (in the window ‘Add data source| Please select the acquisition type’) you will see the window below:



Select device and click **Next**.



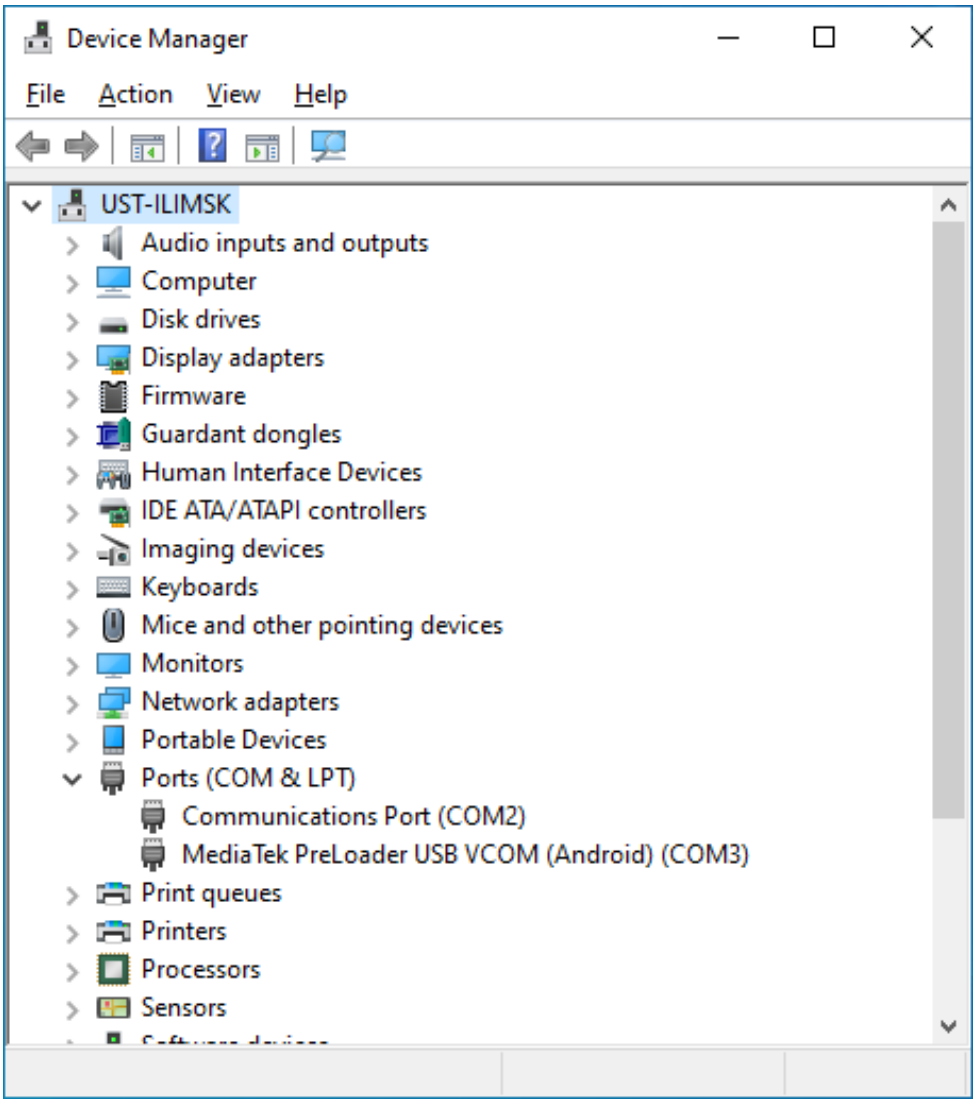
Click **Next** and specify the **Target path** (for the folder where the smartphone image will be stored).
Click **Start** - acquisition will begin.

MTK

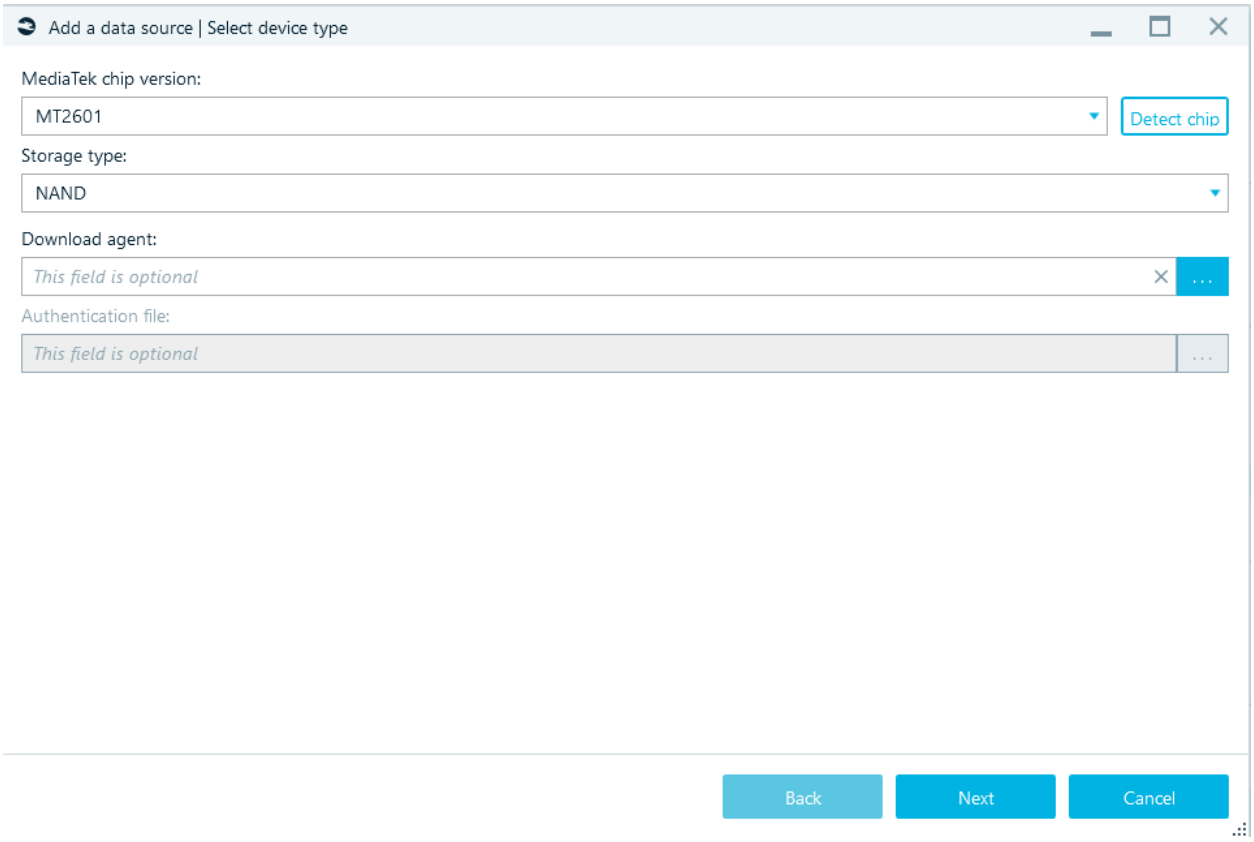
Creating the image from devices based on **chipsets MediaTek**.
The **MediaTek function** allows you to create an image from a smartphone with a **MediaTek processor**.
Such smartphones typically have the PreLoader module, which is part of their preinstalled software.

To access the PreLoader module on a MediaTek smartphone**, you do not** even **have to turn on the device**. Therefore, it is possible to create images from such smartphones even when the smartphone lacks a screen, battery, or even its case.
Technically, the smartphone board and a USB cable (to connect the device to a PC) are the only essential hardware items need to create an image.
You can confirm the presence of the PreLoader module on a MediaTek smartphone this way:

1. Open the **Device Manager** app on a PC.
2. Expand the **Universal Serial Bus controllers** or **Ports** category to view the devices there.
3. Connect the MediaTek smartphone to the PC using a USB cable.



Confirmation: Watch out for changes on the **Device Manager** window. After you connect the smartphone to the PC, the **MediaTek PreLoader USB** driver will appear for a short period of time and then disappear.
For this reason, you must avoid connecting the MediaTek smartphone to a PC before the main process starts. You must connect the smartphone to a PC only at the right moment (when the flash memory wizard is expecting the connection).
After selecting **MTK** (in the window 'Add data source| Please select the acquisition type') you will see the window below:



Select the **MediaTek chip version** from the drop-down menu or click **Detect chip**. Select the **Storage type** technology. If necessary, you can determine options:

- Download agent. The DowloadAgent (an executable) is loaded into the smartphone memory.
- Use an authentication file.

Click **Next** and specify the **Target path** (for the folder where the smartphone image will be stored).
Click **Start**. Turn off mobile device, remove the battery and plug the device in with a USB cable.

List of supported chipsets

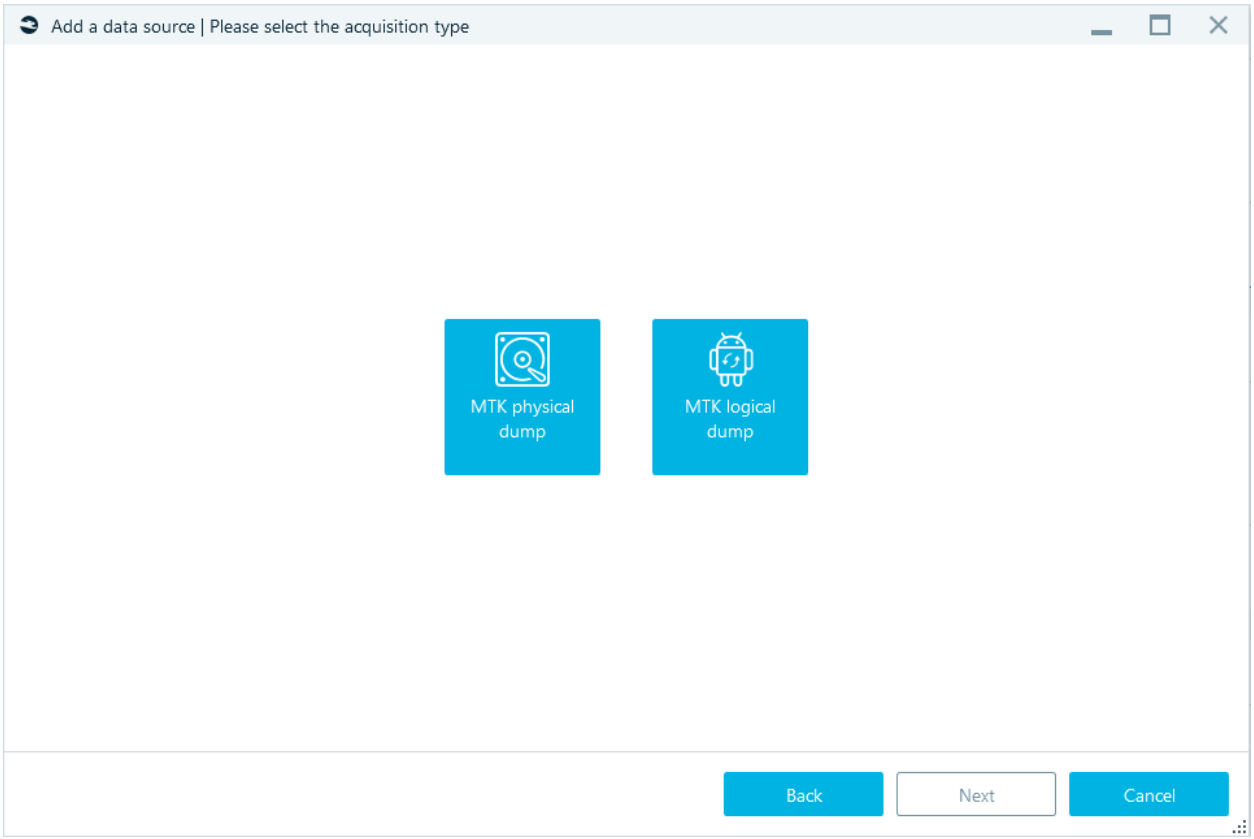
MT2601
MT2701
MT6205
MT6205B
MT6217
MT6218
MT6218B
MT6219
MT6223
MT6223P
MT6225
MT6226
MT6226D

MT6226M
MT6227
MT6227D
MT6228
MT6229
MT6230
MT6235
MT6235B
MT6236
MT6238
MT6239
MT6251
MT6251T
MT6253
MT6253D
MT6253T
MT6255
MT6268A
MT6268B
MT6268T
MT6270A
MT6276
MT6516_AP
MT6516_MD
MT6570
MT6571
MT6572
MT6573
MT6574
MT6575
MT6577
MT6580
MT6582
MT6589
MT6592
MT6595
MT6735
MT6735M
MT6737M
MT6737T
MT6739

MT6750
MT6752
MT6753
MT6755
MT6757
MT6757D
MT6758
MT6759
MT6763
MT6795
MT6797
MT6799
MT7623
MT7683
MT7863
MT8127
MT8135
MT8163
MT8167
MT8173
MT8521
MT8531
MT8590
MT8591
MT8592
MT8695

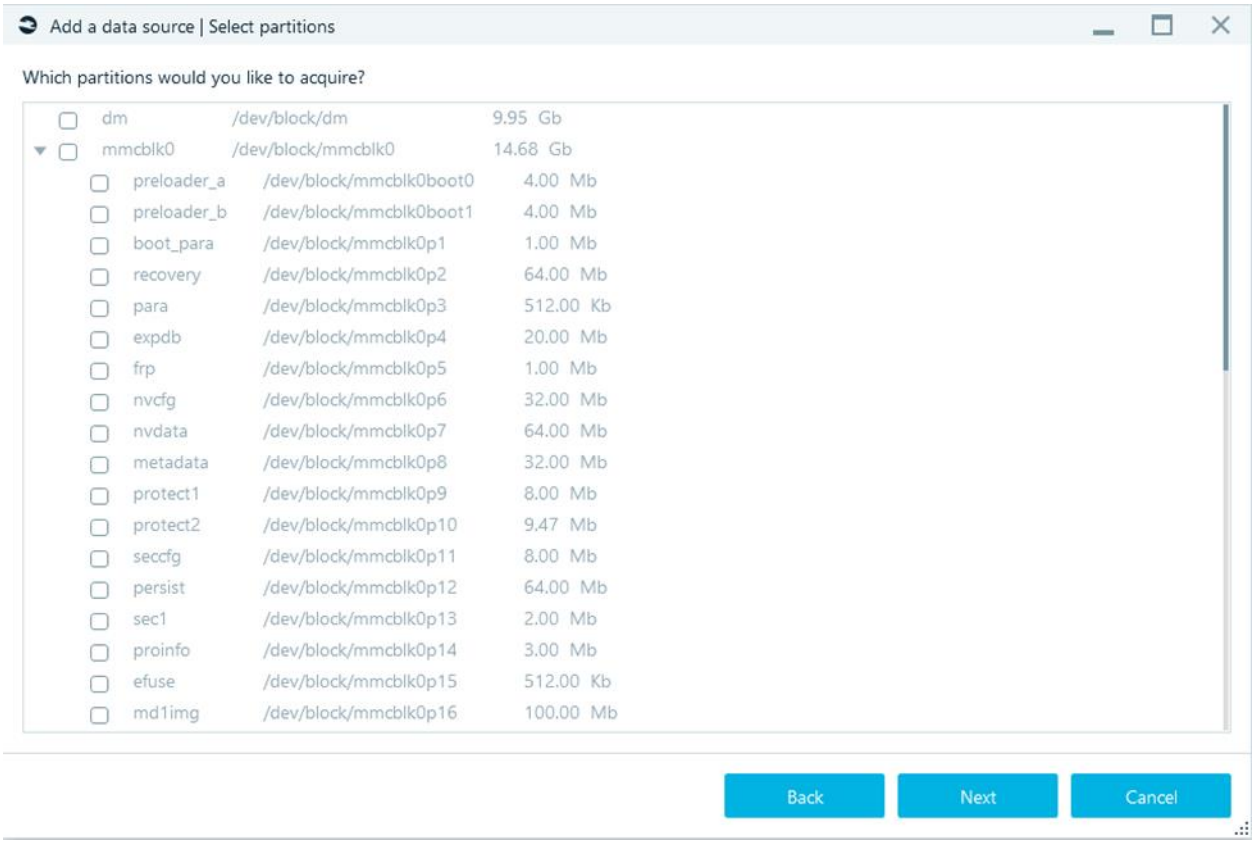
Agent-based MTK acquisition

Before start acquisition: **Stop or pause antivirus**.
You can choose one of 2 options: **MTK physical dump** or **MTK logical dump**:



MTK physical dump

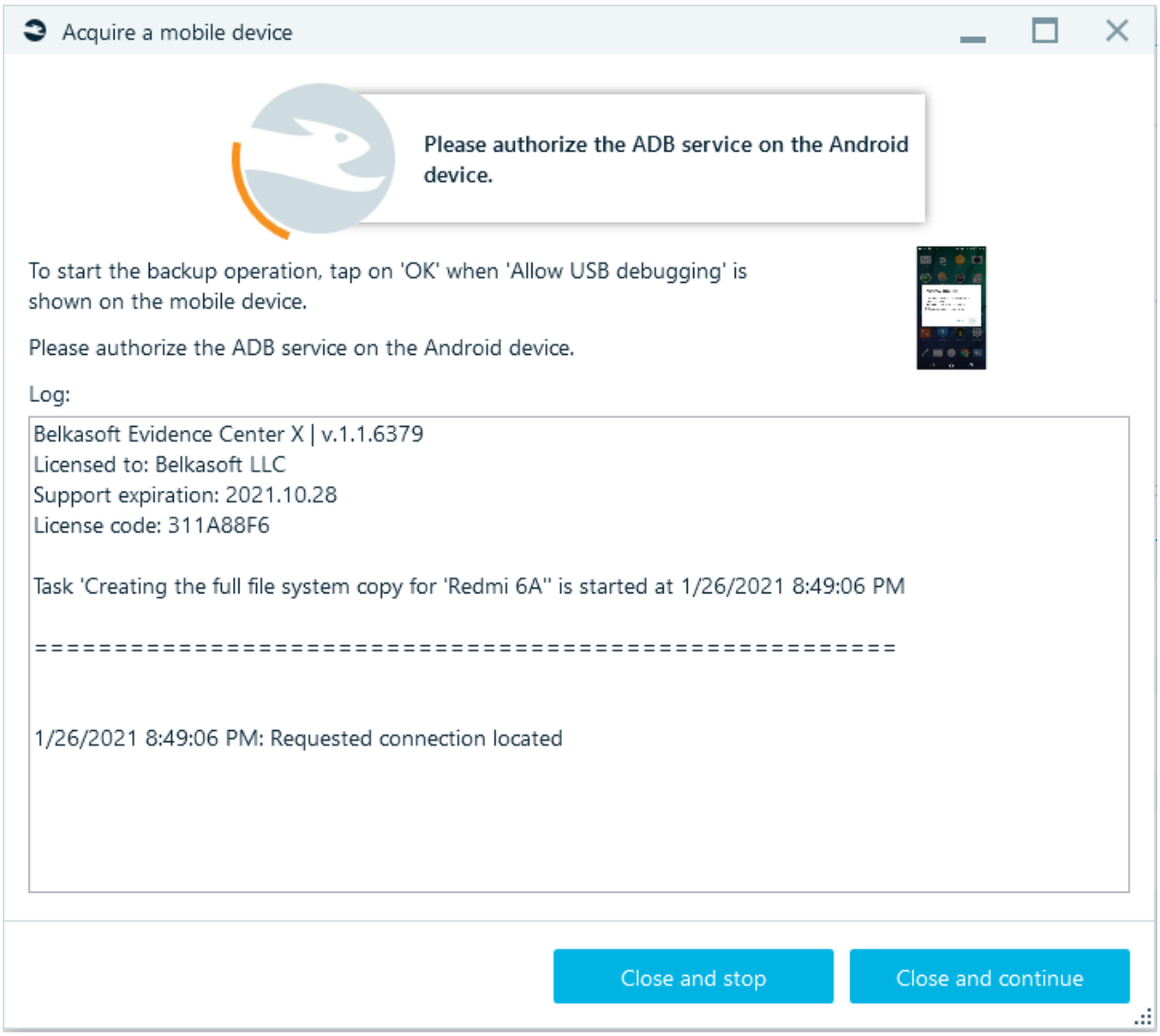
Connecting smartphone, unlock and turn off lock screen.
When ‘Allow USB debugging’ is shown on the smartphone tap on ‘OK’.
Select partitions and click **Next**.



Specify the **Target path** (for the folder where the smartphone image will be stored).
Click **Start** - acquisition will begin.

MTK logical dump

Connecting smartphone, unlock and turn off lock screen.
Click **Next** and specify the **Target path** (for the folder where the smartphone image will be stored).
Click **Start**.



Supported phone models

Acer Iconia One 10 B3-A30/B3-A40/B3-A50 series
Acer Iconia One 8 B1-860 series
Acer Iconia Talk S
Alba tablet series
Alcatel 1 5033 series
Alcatel 1C
Alcatel 3L (2018) 5034 series
Alcatel 3T 8
Alcatel A30 5049 series
Alcatel A5 LED 5085 series
Alcatel Idol 5

Alcatel Tetra 5041C
Alcatel U5 / Orange Rise 52
Alcatel/TCL A1 A501DL
Alcatel/TCL LX A502DL
Alldocube iPlay10 Pro
Alldocube iPlay8
Amazon Fire 7 2019 -- up to Fire OS 6.3.1.2 build 0002517050244 only
Amazon Fire HD 10 2017 -- up to Fire OS 5.6.4.0 build 636558520 only
Amazon Fire HD 10 2019 -- up to Fire OS 7.3.1.0 only
Amazon Fire HD 8 2016 -- up to Fire OS 5.3.6.4 build 626533320
Amazon Fire HD 8 2017 -- up to Fire OS 5.6.4.0 build 636558520 only
Amazon Fire HD 8 2018 -- up to Fire OS 6.3.0.1 only
Amazon Fire TV 2 -- up to Fire OS 5.2.6.9 only
ANRY S20
ASUS ZenFone 3 Max ZC520TL
ASUS ZenFone Max Plus X018D
ASUS ZenPad 3s 10 Z500M
ASUS ZenPad Z3xxM(F) MT8163-based series
Barnes & Noble NOOK Tablet 10.1" BNTV650
Barnes & Noble NOOK Tablet 7" BNTV450 & BNTV460
Blackview A8 Max
Blackview BV9600 Pro (Helio P60)
BLU Life Max
BLU Life One X
BLU R1 series
BLU R2 LTE
BLU S1
BLU Tank Xtreme Pro
BLU Vivo 8L
BLU Vivo XI
BLU Vivo XL4
Bluboo S8
BQ Aquaris M4.5
BQ Aquaris M8
CAT S41
Coolpad Cool Play 8 Lite
Coolpad Legacy S(R)
Cubot Power
Doogee X70

Dragon Touch K10
Echo Feeling
Evercoss Genpro X Pro S50
Gionee F103 Pro
Gionee M7
Gionee S9
HiSense Infinity H12 Lite
HomTom HT20
HTC Desire 12
Huawei GR3 series
Huawei Y5II
Huawei Y6II MT6735 series
ION Gravity
Lava Iris 88S
Lenovo A5
Lenovo C2 series
Lenovo Tab E7
Lenovo Tab E8
Lenovo Tab2 A10-70F
Lenovo Tab3 10
Lenovo Vibe K5 Note
LG K10 (2017)
LG K10--K430 series
LG K50
LG K8+ (2018) X210ULMA (MTK)
LG Q7 (MTK)
LG Stylo 4 (MTK) -- up to Q710AL11k
LG Tribute Dynasty
LG X power 2/M320 series (MTK)
LG Xpression Plus 2/Harmony 3/K40 LMX420 series
Lumigon T3
Meizu M5c
Meizu M6
Meizu Pro 7 Plus
Motorola Moto C series
Motorola Moto E3 series (MTK)
Motorola Moto E4 series (MTK)
Mtk агент
Nokia 1

Nokia 1 Plus
Nokia 3
Nokia 3.1
Nokia 3.1 Plus
Nokia 5.1
Nokia 5.1 Plus/X5
Odys PACE 10 (MT8163)
Onn 7" Android tablet
Onn 8" & 10" tablet series (MT8163) -- up to 10/2019 FW only
Oppo A59 series
Oppo A5s -- up to A.30 only
Oppo A7x -- up to Android 8.x
Oppo F5 series/A73 -- up to A.39
Oppo F7 series -- Android 8.x only
Oppo F9 series -- Android 8.x only
Oppo R9xm series
Oukitel K12
Oukitel K6
Oukitel K9
Oukitel U18
Philips E518
Protruly D7
RCA Voyager III - RCT6973W43MDN
Realme 1
Realme 3
Snopow M10 series
Sony Xperia C4
Sony Xperia C5 series
Sony Xperia L1
Sony Xperia L3
Sony Xperia M5 series
Sony Xperia XA series
Sony Xperia XA1 series
Southern Telecom Smartab ST1009X (MT8167)
Teclast M30
TECNO Spark 3 series
Umidigi F1 series
Umidigi Power
Verizon Ellipsis 10 HD QTAXIA1

Vernee Mix 2
Wiko Ride
Wiko Sunny
Wiko View3
Xiaomi Redmi 6/6A series
ZTE Blade 10 Prime
ZTE Blade A530
ZTE Blade A7 Prime
ZTE Blade D6/V6
ZTE Blade V8 Lite
ZTE Quest 5 Z3351S
ZTE Voyage 4S/Blade A611/Blade A610

Qualcomm (EDL acquisition for Android devices with Qualcomm processors)

Creating the physical image from devices on **Qualcomm Snapdragon SoC** using **EDL mode**.

Install EDL driver or if you see message: “The COM-port is not open. The EDL driver may not be installed or don't have digital signature. Please, try reboot the system with driver signature verification disabled” disable Driver Signature Verification on Windows.

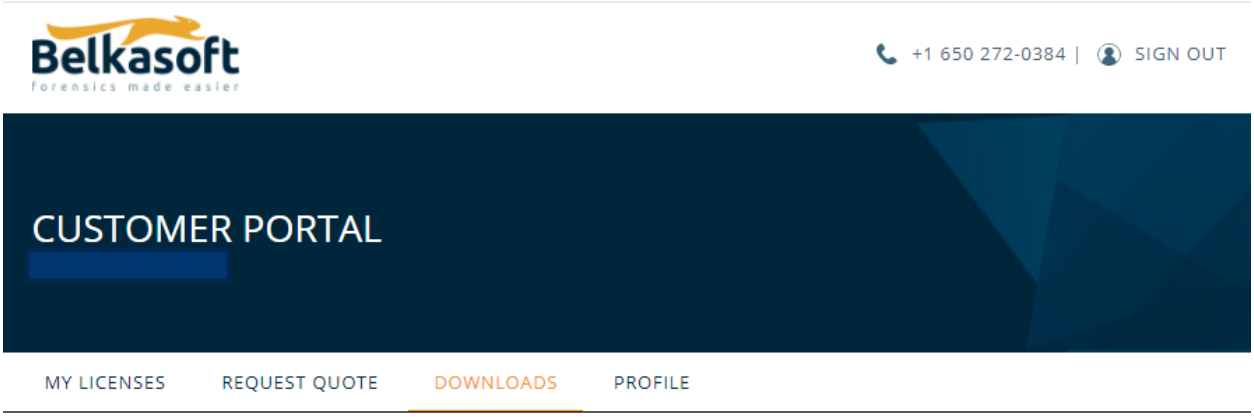
Start your computer and then keep pressing the F8 key before Windows starts. You will see the Advanced Options screen.
Choose Troubleshoot > Advanced options > Startup Settings and click the Restart button.
When your computer restarts you will see a list of options. Press F7 on your keyboard to select Disable driver signature enforcement.

Your computer will now restart, and you will be able to install unsigned drivers. Install EDL driver.

Fully charge your smartphone.
Switch the phone to EDL mode:

- Take apart the phone and short the test pins.
- Via ADB console:
  adb reboot bootloader
  fastboot oem edl

The second method may not work depending on the smartphone model and condition (the bootloader may be locked). Xiaomi smartphones almost everything is locked by default.
Select **Firehose programmer**.
Download Firehose programmers from the personal account of **Belkasoft.com** in the **Downloads**.



Put them in folder …\Belkasoft Evidence Center X\Resources\Android\Edl. **Do not unpack.**

Supported phone models

Asus

Asus Zenfone 4 Pro (Z01GD)	Asus ZenFone 3 (5.2")(ZE520KL)
Asus ZenFone 4 ZE554KL	Asus ZenFone 3 (5.5")(ZE552KL)
Asus Zenfone 5 ZE620KL	Asus ZenFone 3 Deluxe (5.5")(ZS550KL)
Asus Zenfone Max Pro M1	Asus ZenFone 3 Zoom/ZenFone Zoom S (ZE553KL)
Asus Zenfone Max Pro M2	Asus Zenfone 4 Selfie Pro (ZD552KL)
Asus ZenFone 5Z	Asus ZenFone 3 Laser
Asus ROG Phone (2.96Ghz)	Asus ZenFone 3 Max ZC553KL
Asus ZenFone 3 Deluxe (5.7" 64GB) (ZS570KL)	Asus Zenfone 2 Laser ZE500KL
Asus ZenFone 3 Deluxe (5.7" 256GB) (ZS570KL)	Asus Zenfone Max ZC550KL
Asus Zenfone AR	Asus ZenFone 5 Lite
Asus Zenfone Ares (2018)	

Lenovo

Lenovo K9 Note	Lenovo P2
Lenovo K5 Pro	Lenovo S5
Lenovo S5 Pro	Lenovo K6

Lenovo Z5	Lenovo K6 Note
Lenovo S5 Pro GT	Lenovo K6 Power
Lenovo Z5s	Lenovo A805e
Lenovo Z5 Pro	Lenovo Sisley S90
Lenovo Z6 SE/Z6 Lite/Youth	Lenovo Vibe Z2
Lenovo Phab 2 Pro	Lenovo A6000
Lenovo K9 Plus	Lenovo Vibe X3

LG

LG G4
LG V10
LG X mach/X fast

Meizu

Meizu E3
Meizu 15
Meizu 16X
Meizu X8
Meizu 16
Meizu 16 Plus
Meizu Zero
Meizu 15 Lite/Meizu M15
Meizu M6 Note
Meizu Note 8

Motorola

Motorola Moto Z3	Motorola Moto Z2 Play
Motorola Moto X4	Motorola One
Motorola Moto G6 Plus	Motorola Moto G4
Motorola Moto G7 Plus	Motorola Moto G4 Plus
Motorola Moto Z3 Play	Motorola Moto G5
Motorola One Power/P30 Note	Motorola Moto G6 Play
Motorola P30	Motorola Moto E5 Plus (India and China)
Motorola Moto Z	Motorola Moto E5 Plus
Motorola Moto Z Force	Motorola Moto E4 (USA)
Motorola Moto G5 Plus	Motorola Moto E5 Play
Motorola Moto G5S Plus	Motorola Moto G6 Play
Motorola Moto Z Play	Motorola Moto Z2 Force

Nokia

Nokia 8	Nokia 9 Pureview
Nokia 8 Sirocco	Nokia 5
Nokia 6.1	Nokia 6
Nokia 7	Nokia 2.1
Nokia 6.1 Plus/X6	Nokia 8110 4G
Nokia 7.1	Nokia 2720 Flip
Nokia 6.2	Nokia 800 tough

Nokia X71	Nokia 2
Nokia 7 Plus	Nokia X2
Nokia 7.2	Nokia X7/8.1/7.1 Plus

OnePlus

OnePlus 5
OnePlus 5T
OnePlus 6
OnePlus 6T
OnePlus 6T McLaren Edition

Oppo

OPPO R11	OPPO R17 Neo/RX17 Neo
OPPO R11 Plus	OPPO F3 Plus
OPPO R11s	OPPO R9 Plus
OPPO R11s Plus	OPPO R9s Plus
OPPO R15 Pro	OPPO R9s
OPPO R15 Dream Mirror	OPPO A57
OPPO K1 (64GB only, 128GB model is called R15x)	

Samsung

Samsung Galaxy S8 (USA/Canada/China/Hong-Kong/Japan)	Samsung Galaxy S7 Edge (SM-G9350/A/P/T/U/V)
Samsung Galaxy S8+ (USA/Canada/China/Hong-Kong/Japan)	Samsung galaxy S7 Active (SM-G891A)
Samsung Galaxy S8 Active (AT&T USA)	Samsung Galaxy Note 7 (SM-N9300)
Samsung Galaxy Note 8 (USA/Canada/China/Hong-Kong/Japan)	Samsung Galaxy Tab S3
Samsung Galaxy Tab S4	Samsung W2017
Samsung W2018	Samsung Galaxy Note FE (SM-N9350)
Samsung Galaxy S7 (SM-G9300/A/P/T/U/V)	

Sharp

Sharp Aquos C10	Sharp Aquos Sense Plus
Sharp Aquos D10	Sharp Aquos S2 128GB
Sharp Aquos S2 64GB	Sharp Aquos S3 128GB
Sharp Aquos S3	Sharp Aquos R Compact
Sharp Aquos S3 Mini	

Vivo

Vivo Z1i	Vivo Xplay 6
Vivo V9 6GB (Indonesia)	Vivo V3 Max
Vivo V11 Pro	Vivo X6s
Vivo X20	Vivo X6s Plus
Vivo X20 Plus	Vivo X7

Vivo X20 Plus UD	Vivo X7 Plus
Vivo X21	Vivo X9 Plus
Vivo X21 UD	Vivo X9s
Vivo X21s	Vivo X9s Plus
Vivo Z1	Vivo Xplay5
Vivo X23 Symphony	Vivo V5 Plus
Vivo Nex A	Vivo V9
Vivo Nex A UD	Vivo X9
Vivo X27 (256GB)	Vivo Y79
Vivo X27 Pro	Vivo Y53
Vivo Z3 (6GB RAM)	Vivo Y66
Vivo Z5x	Vivo Y93
Vivo Nex S	Vivo Y95
Vivo iQOO Neo	Vivo U1
Vivo Xplay 5 Elite	Vivo Y3

Xiaomi

Xiaomi Mi 6	Xiaomi Mi MIX
Xiaomi Mi MIX 2	Xiaomi Mi 5 64GB/128GB
Xiaomi Redmi Note 5/Redmi Note 5 Pro	Xiaomi Mi 5s
Xiaomi Redmi Note 5 AI Dual Camera	Xiaomi Mi Note Pro
Xiaomi Redmi Note 6 Pro	Xiaomi Mi 4c
Xiaomi Mi Max 3	Xiaomi Mi 4s
Xiaomi Mi Note 3	Xiaomi Mi Max (16GB/32GB)
Xiaomi Mi 8 Lite/Mi 8 Youth	Xiaomi Mi Max (64GB/128GB)
Xiaomi Mi A2/Mi 6X	Xiaomi Mi 5X/Mi A1
Xiaomi Mi Pad 4	Xiaomi Mi A2 Lite/Redmi 6 Pro
Xiaomi Mi Pad 4 Plus	Xiaomi Mi Max 2
Xiaomi Redmi Note 7 India	Xiaomi Redmi 4 Prime
Xiaomi Redmi Note 7 International/7S	Xiaomi Redmi 5 Plus/Redmi Note 5
Xiaomi Mi CC9 (Mi 9 Lite)	Xiaomi Redmi Note 4
Xiaomi Mi CC9 Meitu Edition	Xiaomi Redmi Note 4X(32GB)
Xiaomi Mi 8 SE	Xiaomi Redmi S2/Redmi Y2
Xiaomi Mi MIX 2S	Xiaomi Redmi 4 (India)
Xiaomi Mi MIX 3	Xiaomi Redmi Y1 (India)
Xiaomi Pocophone F1	Xiaomi Redmi 4X
Xiaomi Mi 8	Xiaomi Redmi Note 5A Pro
Xiaomi Mi 8 Explorer Edition	Xiaomi Redmi 3S
Xiaomi Mi 8 Pro/Mi 8 Screen Fingerprint Edition	Xiaomi Redmi 4 (China)
Xiaomi Black Shark	Xiaomi Redmi 4A
Xiaomi Black Shark Helo	Xiaomi Redmi 5A
Xiaomi Mi 5 32GB	Xiaomi Redmi Note 5A
Xiaomi Mi 5s Plus	Xiaomi Redmi Y1 Lite
Xiaomi Mi Note 2	Xiaomi Redmi Go

ZTE

ZTE Nubia Z17	ZTE Nubia Z11 Max
ZTE Nubia Z17S	ZTE Nubia Z17 mini
ZTE Nubia Red Magi	ZTE Axon 7 MAX
ZTE Axon 7s	ZTE Axon Max 2
ZTE Axon M	ZTE Blade Max 3
ZTE Axon 7	ZTE Blade V8 Pro
ZTE Nubia Z11	ZTE Nubia M2
ZTE Axon & Axon Pro & Axon Lux & Axon Elite	ZTE Nubia N3
ZTE Nubia Z9 Max & Max Elite	ZTE Nubia V18
ZTE Nubia Z9	ZTE Nubia Z11s mini
ZTE Nubia Z9 Elite	ZTE Zmax Pro
ZTE Nubia Z9 Exclusive	

APK Downgrade

Android APK downgrade method allows a user to downgrade applications on an Android device, meaning that an older version of an app is temporarily copied onto the device. This simple trick provides extraction of data from applications that have removed the possibility of backing up their data. Examples of such applications include Facebook Messenger, WhatsApp, Signal, Telegram, and others.
After completing the data extraction process, it is important to restore the original version of the app on the device.

However, it's crucial to note that the APK downgrade method carries certain risks, including:

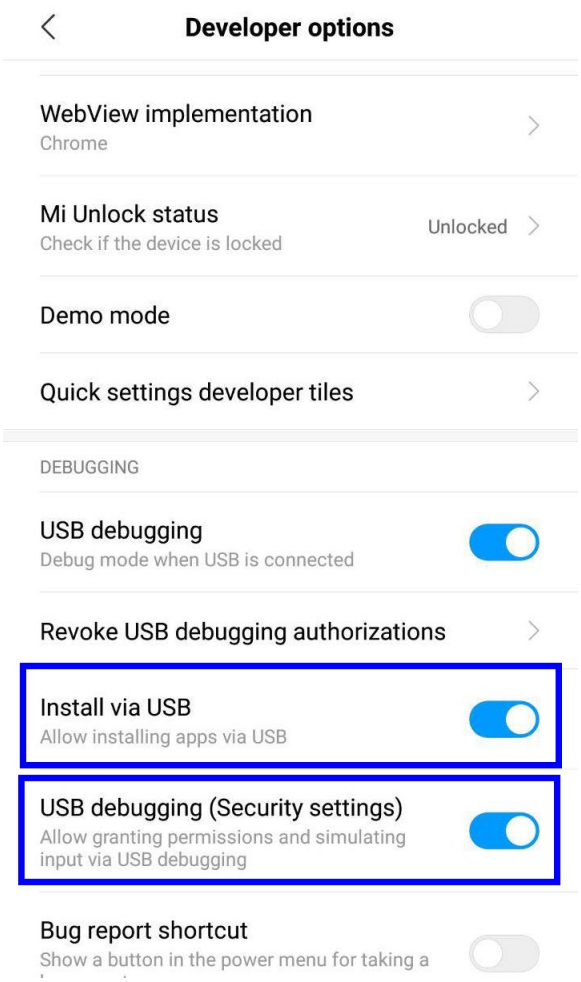
- Inability to restore the application.
- Logging out from the restored application.
- Data loss

Please use the APK downgrade method responsibly and only as a last resort.

The requirements for using this method are the same as for a standard ADB backup:

- The device must be powered on
- The device must be unlocked
- Enable in Developer options on smartphone:
  - ✓ USB debugging (Security settings)
  - ✓ Install via USB

Rooting device is not required.



Supported Apps List

- Badoo
- Dolphin
- Dropbox
- Evernote
- Facebook
- Facebook Messenger
- Firefox browser
- Hangouts
- Instagram
- ICQ
- Kakao Talk
- Kate Mobile
- Kate Mobile Lite
- Likee
- Line
- Linkedin
- Maxthon browser
- Odnoklassniki

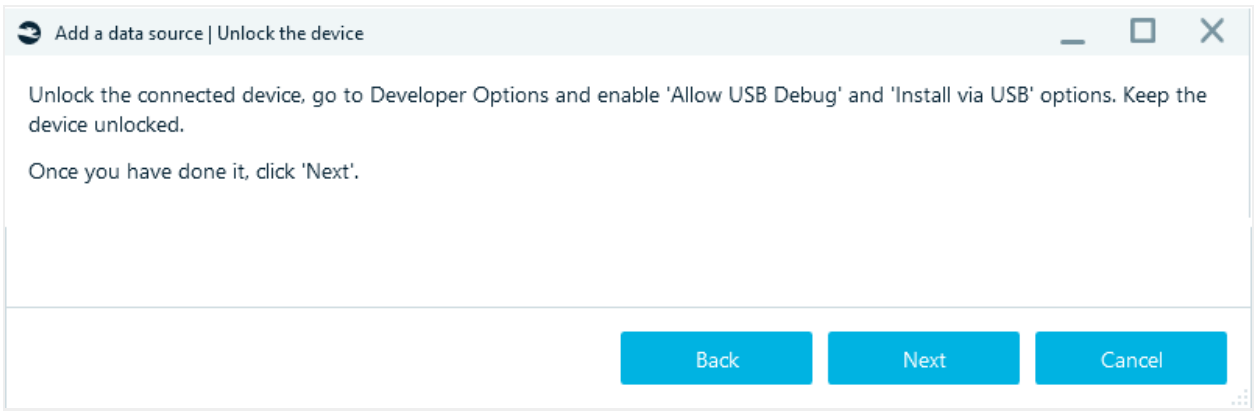
- OneDrive
- Opera
- Opera beta
- Pinterest
- Puffin browser
- QQ
- Sango
- Signal
- SHAREit
- Sinaweibo
- Skype
- StarChat
- TamTam
- Telegram
- Tik Tok
- Tumblr
- Twitter
- Via browser
- Viber
- VKontakte
- Voxer
- WeChat
- WhatsApp
- Wickr Me
- Yalla
- Yandex Browser
- YandexGo
- Yandex Mail
- Zangi
- Zello
- Zoom

Only apps installed on a particular device and supported by this method are shown.

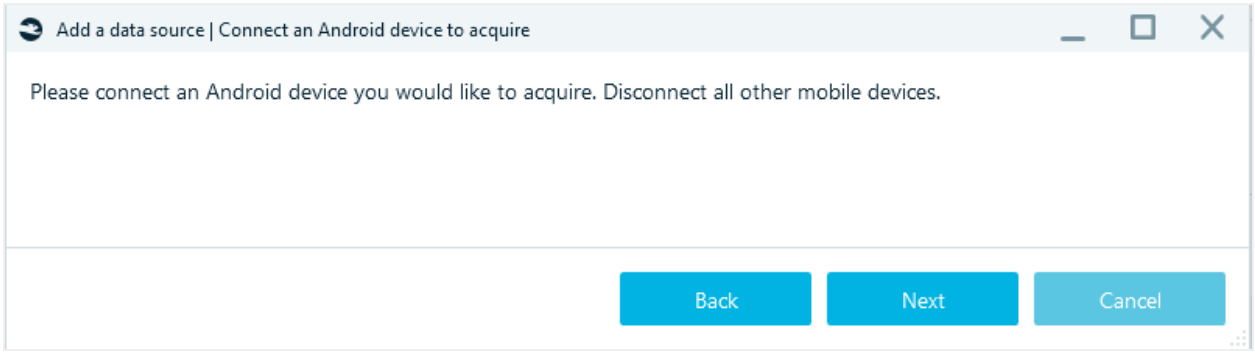
To perform an APK downgrade, follow these steps:

Click **Add data source** on the Dashboard.
Select **Acquire** - **Mobile** - **Android**.
Choose the device's model or use the 'Android generic' option.
Click **APK Downgrade**.

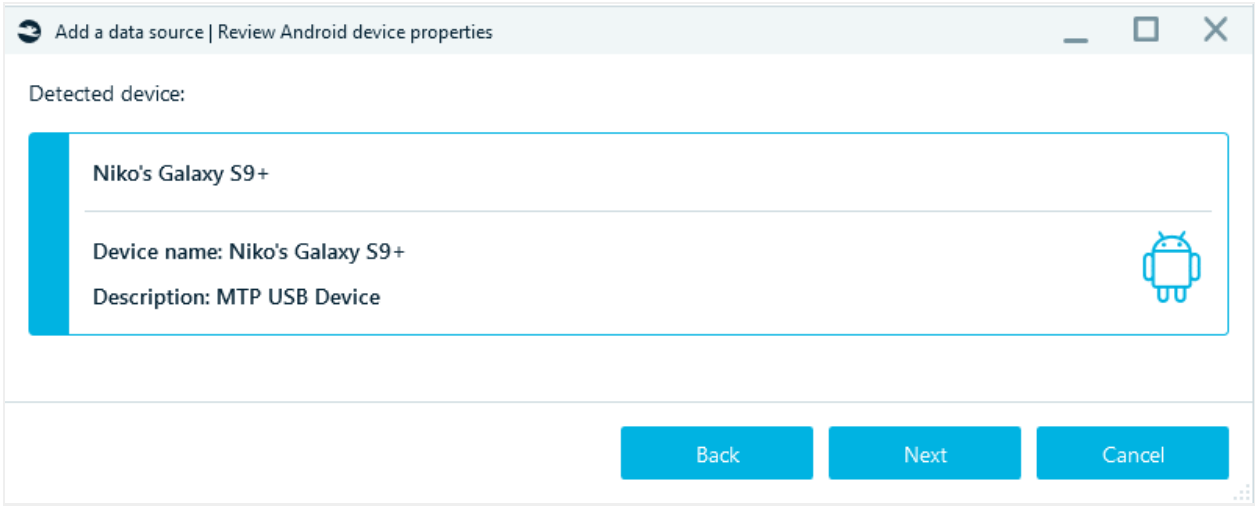
You will be prompted to unlock the device and enable 'Allow USB Debug' and 'Install via USB' options.



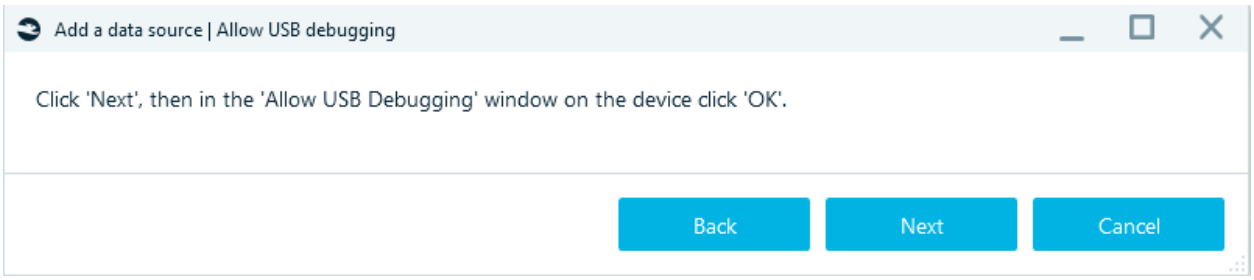
Switch these options on and click **Next**. Ensure that only one Android device is connected, disconnecting all other mobile devices if necessary.



Click **Next**. If everything is done correctly, your device will be detected in the 'Review Android device properties' window.'

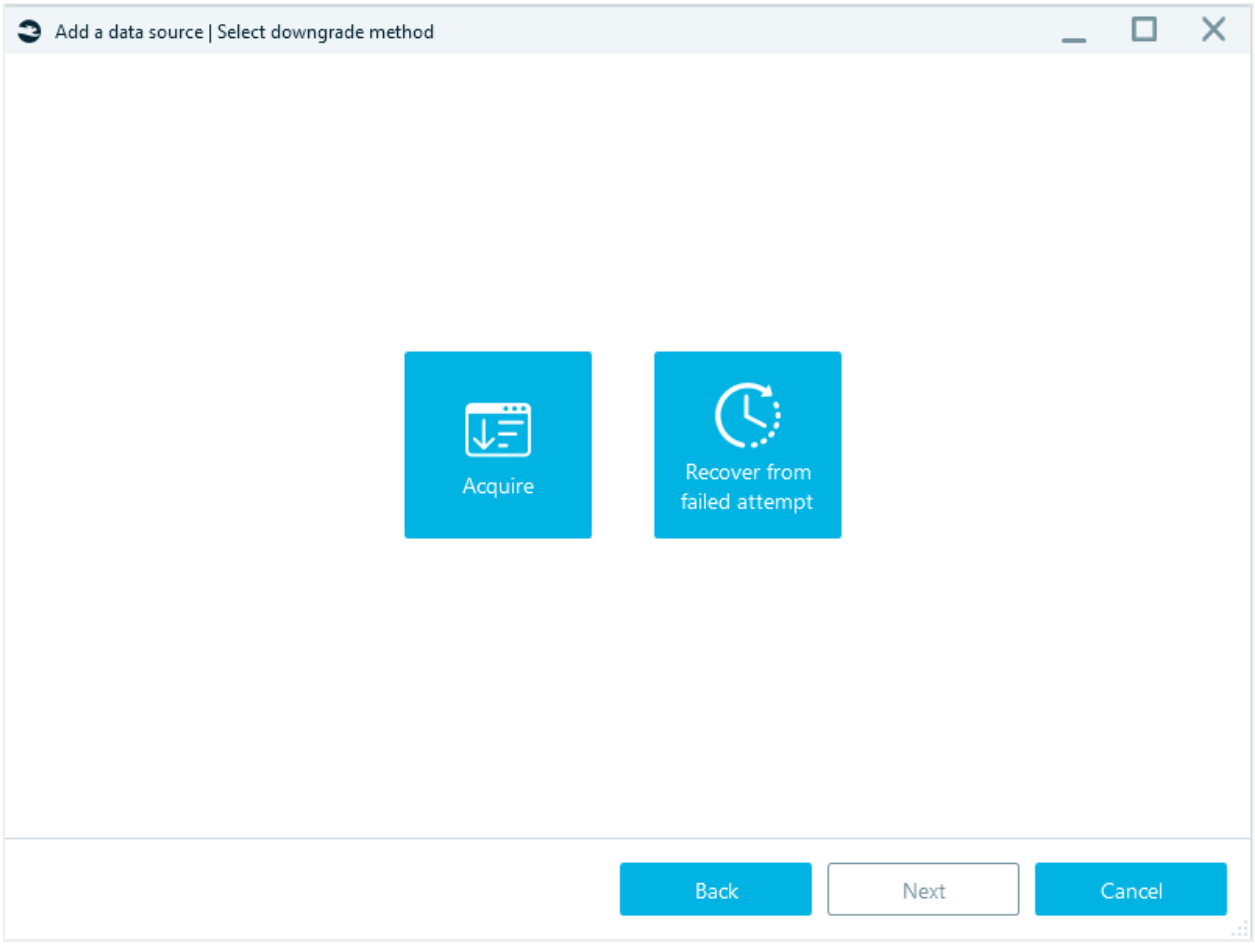


Click **Next**. At the next step you will be prompted to allow USB debugging on the device.



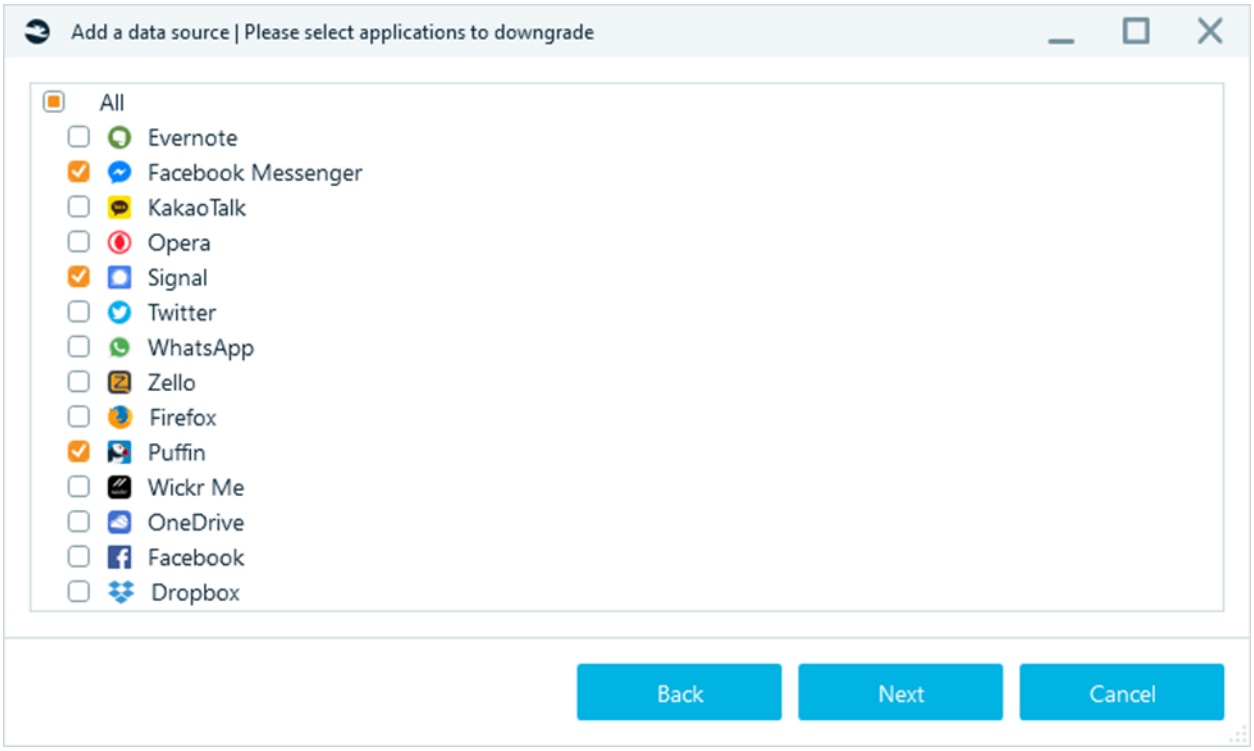
Click **OK** on the corresponding message on the acquired device, then click **Next** in the acquisition wizard.

In the ‘Select downgrade method’ window, choose whether you would like to acquire an application or recover it after a failed attempt. Click **Acquire**.

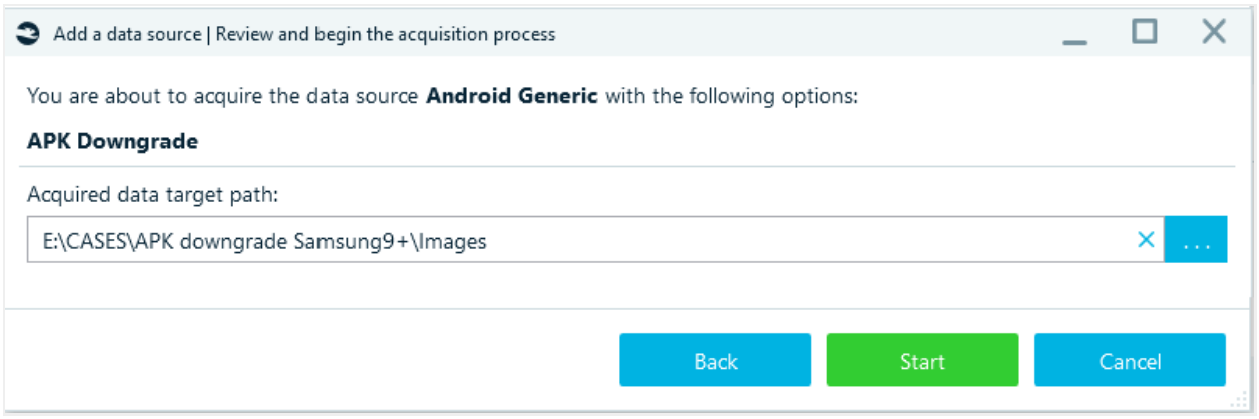


Only apps installed on your device and supported by the APK downgrade method will be shown.

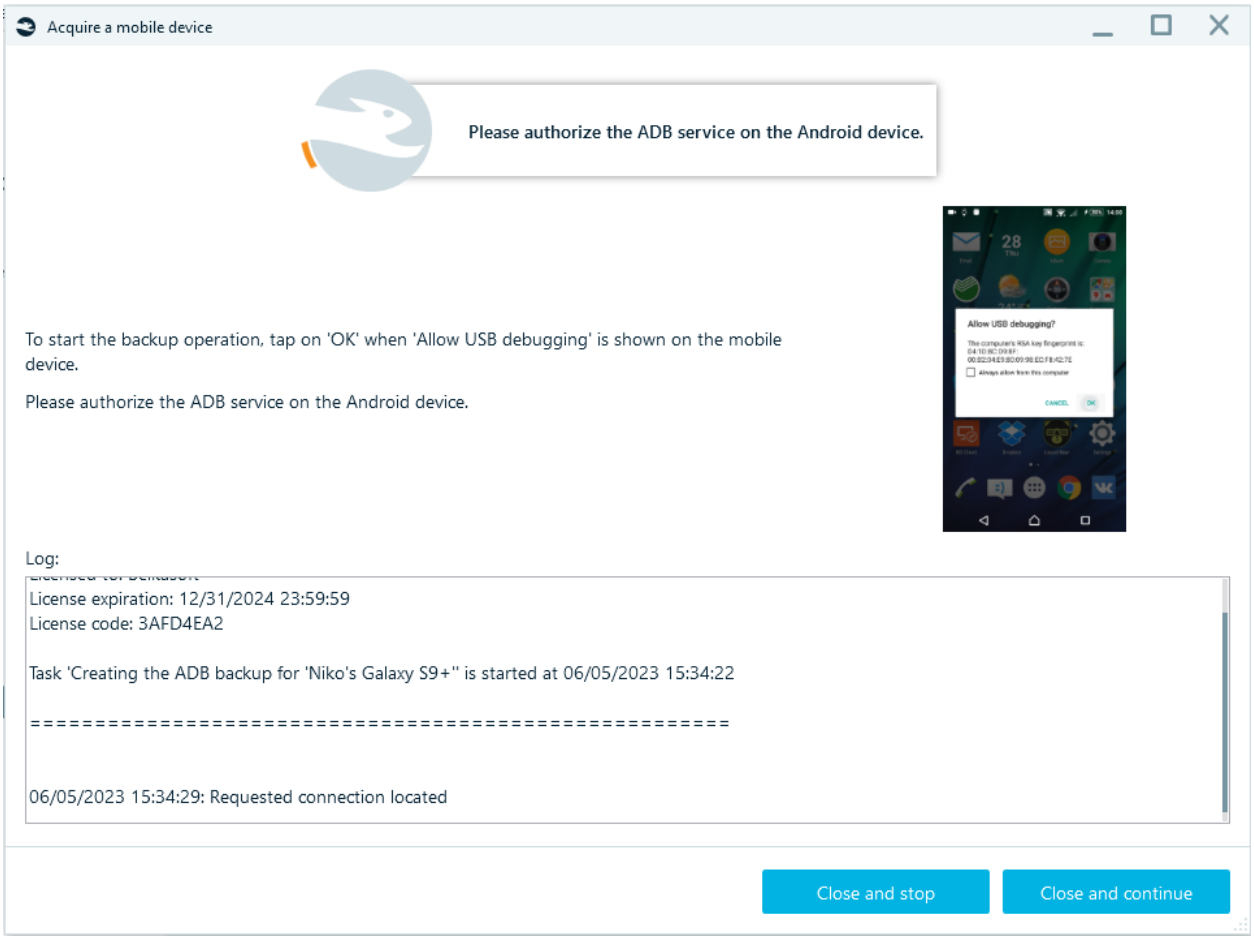
Select one or more applications to acquire using the checkboxes:



Click **Next**. Specify a target path for the acquired data and click **Start.**



Again, you will be asked to authorize the ADB service. Click ‘Allow’ or ‘OK’ on your mobile device.



Once you start the acquisition process, Belkasoft X will perform the following actions:

- Back up the current versions of the applications on the local drive. The original versions will be stored in the …\<application folder>\Options\<deviceID> folder. You can check the application folder path in Settings - General.
- Install the old versions of the applications .
- Reboot the device if required .
- Create an ADB backup.
- Restore the original application versions.

If anything goes wrong during the process, it will be possible to restore applications by using the APK downgrade method again and choosing the 'Recover from failed attempt' option.

Troubleshooting checklist

Preconditions:

- You run the APK Downgrade acquisition or the Advanced ADB method to extract data from an Android device, using Belkasoft X software
- The acquisition session finished unsuccessfully
- The original versions of the downgraded applications were not restored automatically

Please follow the steps below:

1. Reboot your device

2. Connect the device to the computer using original manufacturer cable
3. Use the USB 3.0 port on the rear side of the computer (preferably directly connected to the motherboard)
4. Run the APK Downgrade again and choose the 'Recover from failed attempt' option
5. If Belkasoft X fails to restore the original version of the application, you can do it manually. You will find an original APK file in the **…\<appfolder>\Options\<deviceID>** folder on the computer
6. In case of repetitive unsuccessful acquisitions, try different cables and different USB 3.0 ports

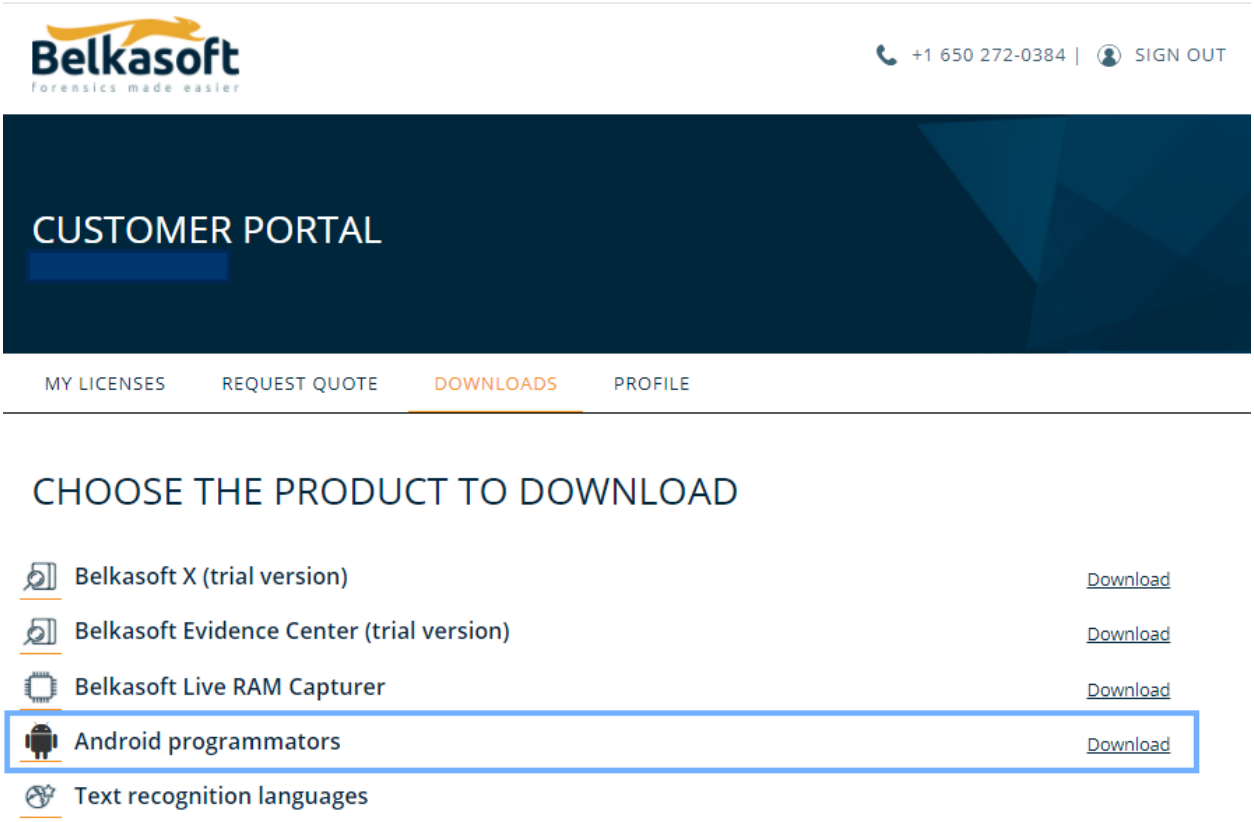
If you are working with Android version 12, please make sure you are using Belkasoft X version 1.14 or later. This release addresses a number of issues specific to Android 12.

As your last resort, if nothing else works, you can restore the applications manually from corresponding manufacturers' sites or web archives.

Spreadtrum

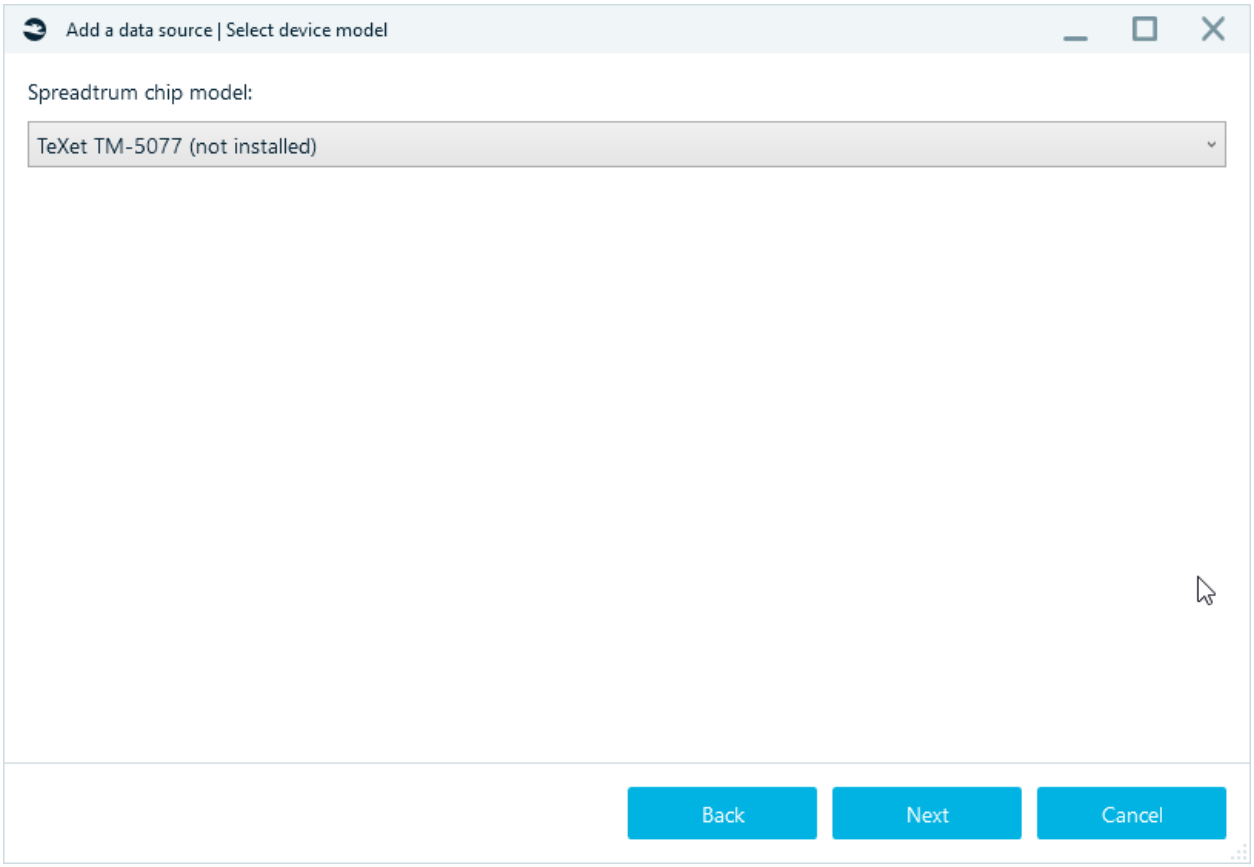
Creating the image from devices on **Spreadtrum chipsets**.
The procedure for creating the image:

1. Install Spreadtrum drivers.
2. Download programmers from the personal account of **Belkasoft.com** in the **Downloads** tab:

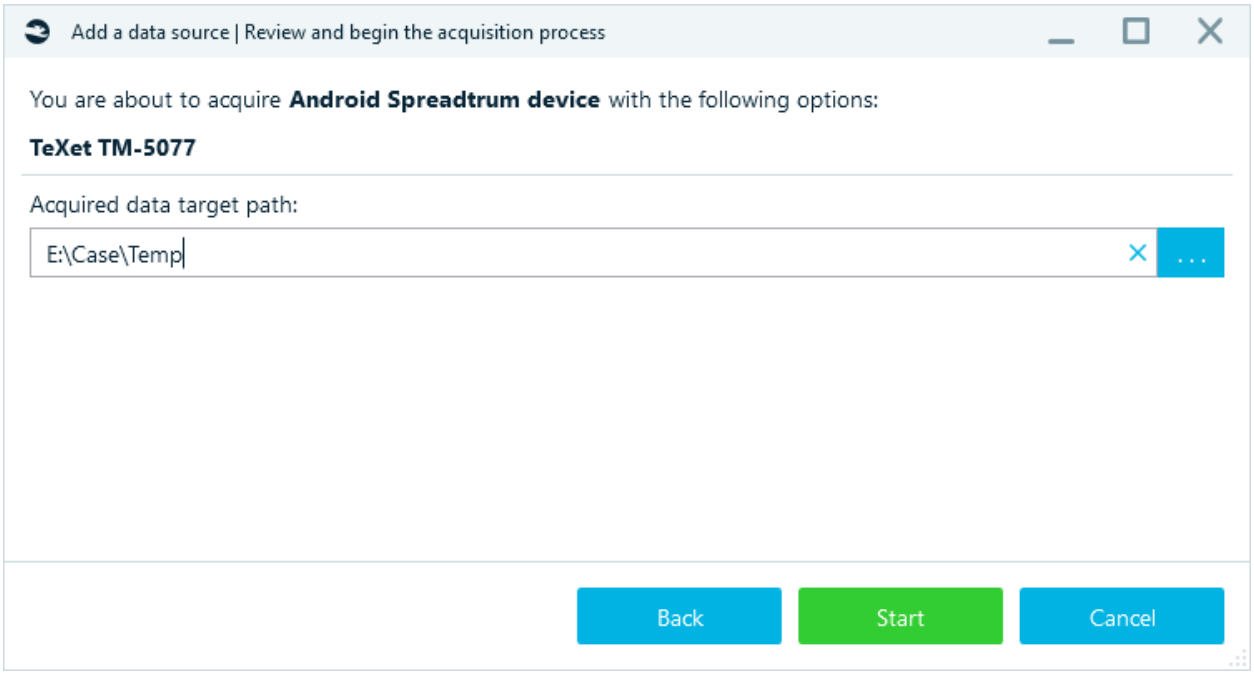


Put programmators in the folder …\Belkasoft Evidence Center X\Resources\Android. **Do not unpack.**

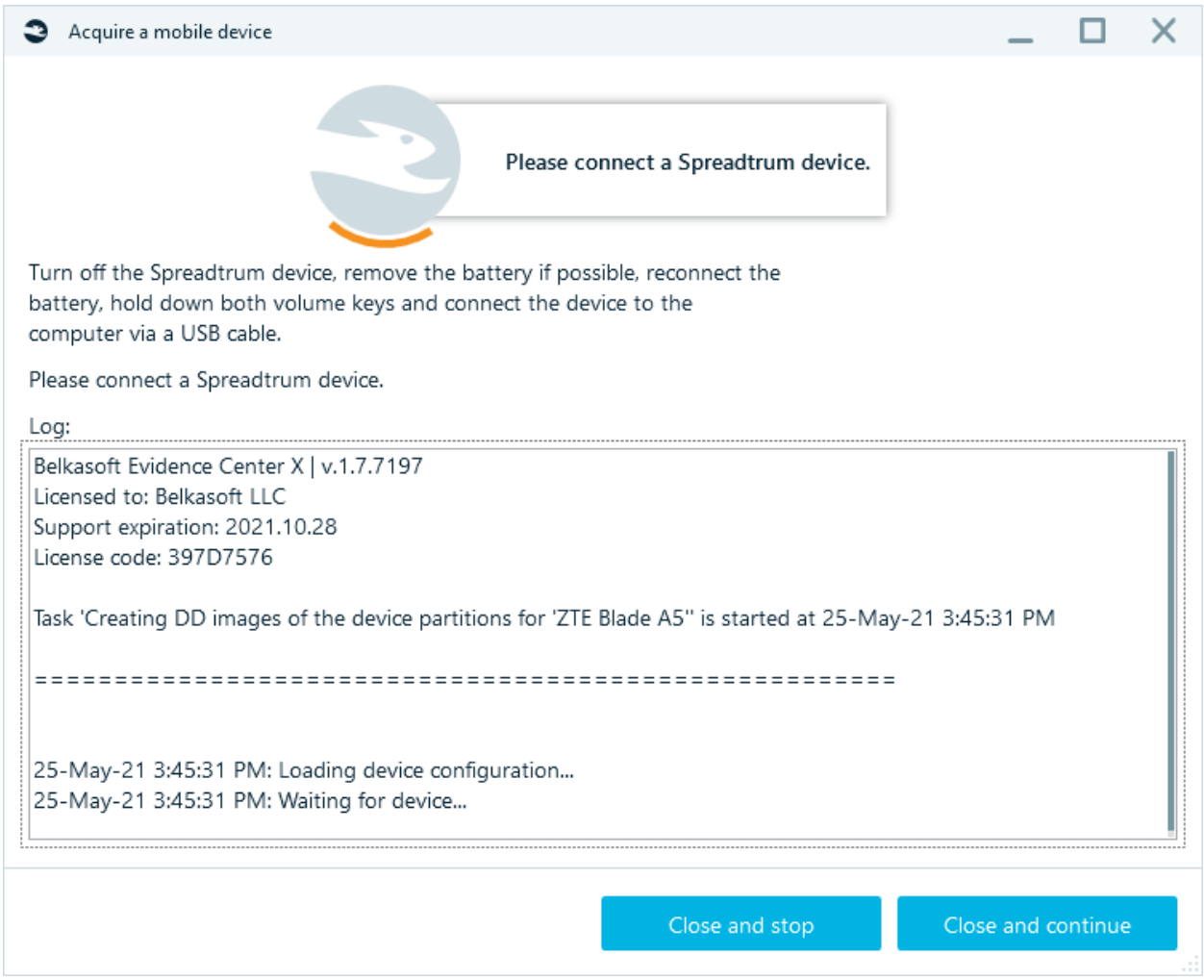
3. Open Belkasoft X. Proceed to Add data source – Acquire – Android – Spreadtrum.
   Select **Spreadtrum chip model**:



4. Specify the **Target path** for acquired data:



5. Click **Start**:



6. Do not connect the device, turn off
7. Remove the battery from the device
8. Insert the battery into the device
9. Hold down a combination of buttons (depending on the phone, usually vol + and vol-)
10. Connect the device via USB cable

The acquisition will begin.

Supported phone models

Alcatel 1C 5003D
Alcatel 1S 5024D
Archos 40D Titanium
Archos 55 Platinum
ARK Benefit Note 1
ARK Benefit S402
ARK Benefit S453
Assistant AS-5411

BLU G5
BLU G60
BQ 5528L Strike Forward
BQ 5731L Magic S
BQ 6040L Magic
BQ 6042L Magic E
Coolpad Mega 5A
DEXP Ixion E140 Strike
DEXP Ixion E150 Soul
DEXP Ixion E250 Soul
DEXP Ixion E345 Jet
DEXP Ixion E350 Soul 3
DEXP Ursus TS370
Digma Citi Z520
Digma Hit Q400
Digma Linx A400
Digma Linx A401
Digma Linx A420
Digma Linx A450
Digma LINX Rage 4G
Digma LINX Trix 4G
Digma Plane 7574s
Digma Vox A10
Digma VOX E502 4G
Digma Vox G450
Digma Vox S507
FinePower C2
FinePower C5
Fly FS528 Memory Plus
Fly FS551 Nimbus4
Fly IQ436i Era Nano 9
Fly IQ4490i Era Nano 10
Gigaset GS80
Ginzzu S4020
Gionee Max
GoClever Max
HTC Desire 326G DualSim
INOI 7
Intex 7

Intex Elyt Dual
Intex Indie 6
Intex Staari 11
Irbis SP05
Irbis SP06
Itel P36 Pro
Itel Vision 1
Itel Vision 1 Plus
Jinga A400
Leagoo Z5c
Lenovo A1000
Lenovo A2800D
Lenovo A398T+
Micromax Q301
Micromax Q326
Micromax Q346
Micromax Q346 Lite
Micromax Q379
Micromax Q385
Micromax Q465
Nobby X800
Philips S260
Philips S307
Prestigio Muze V3 LTE
Prestigio Wize NV3 3537Duo
TeXet TM-4003
TeXet TM-5073
TeXet TM-5075
TeXet TM-5076
TeXet TM-5077
TeXet X-line TM-5006
TeXet X-quad TM-4503
Vertex Impress Wolf
Wiko Sunny 2
Wiko Sunny 3
Wiko Sunny 4
ZTE Blade A3 2019
ZTE Blade A3 2020
ZTE Blade A5

ZTE Blade AF3
ZTE Blade GF3

Screen capturer

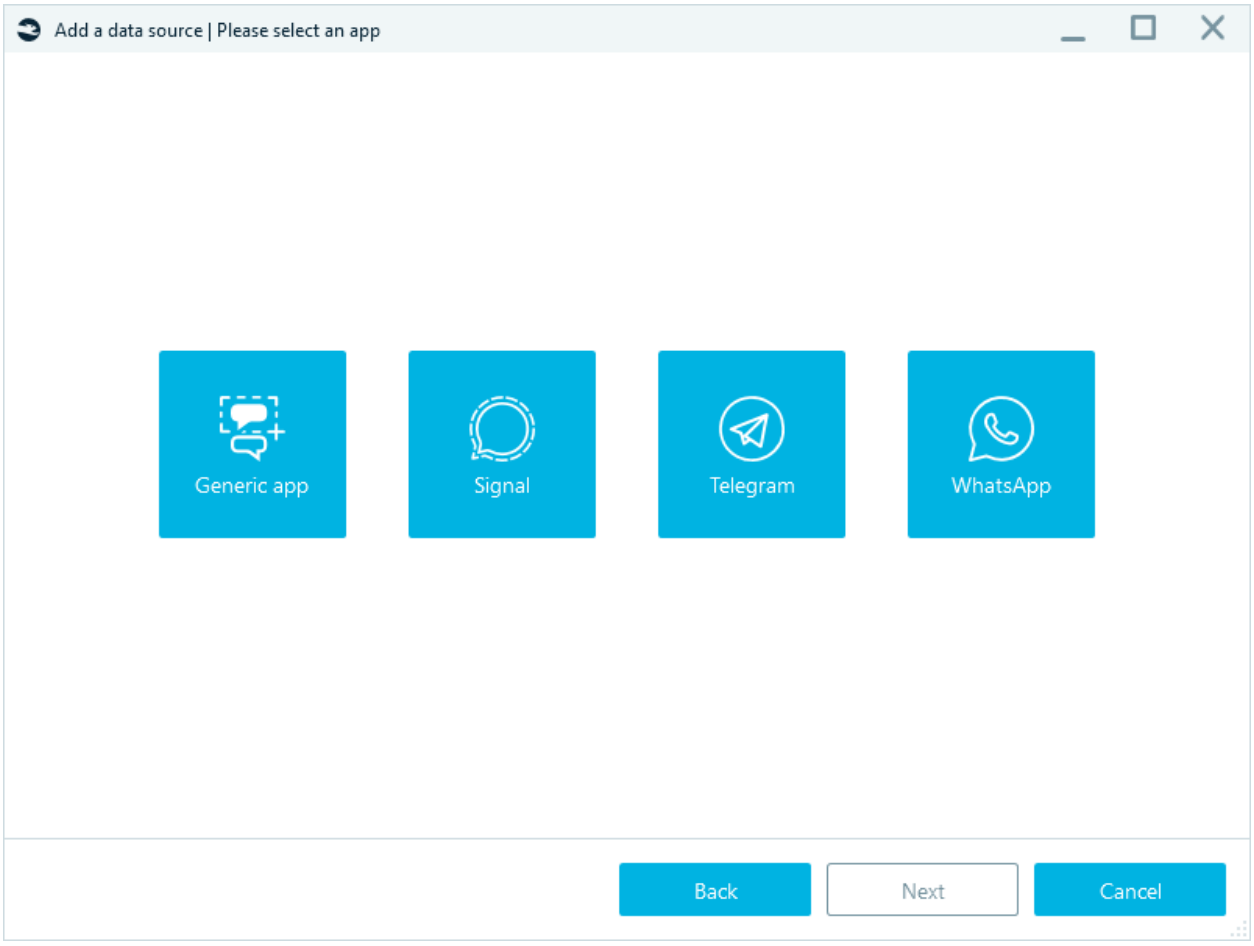
This is an acquisition method for Android devices, which allows you to take all or a certain number of screenshots from applications installed on the phone.

Supported applications:

- Signal
- Telegram
- Whatsapp
- Generic app

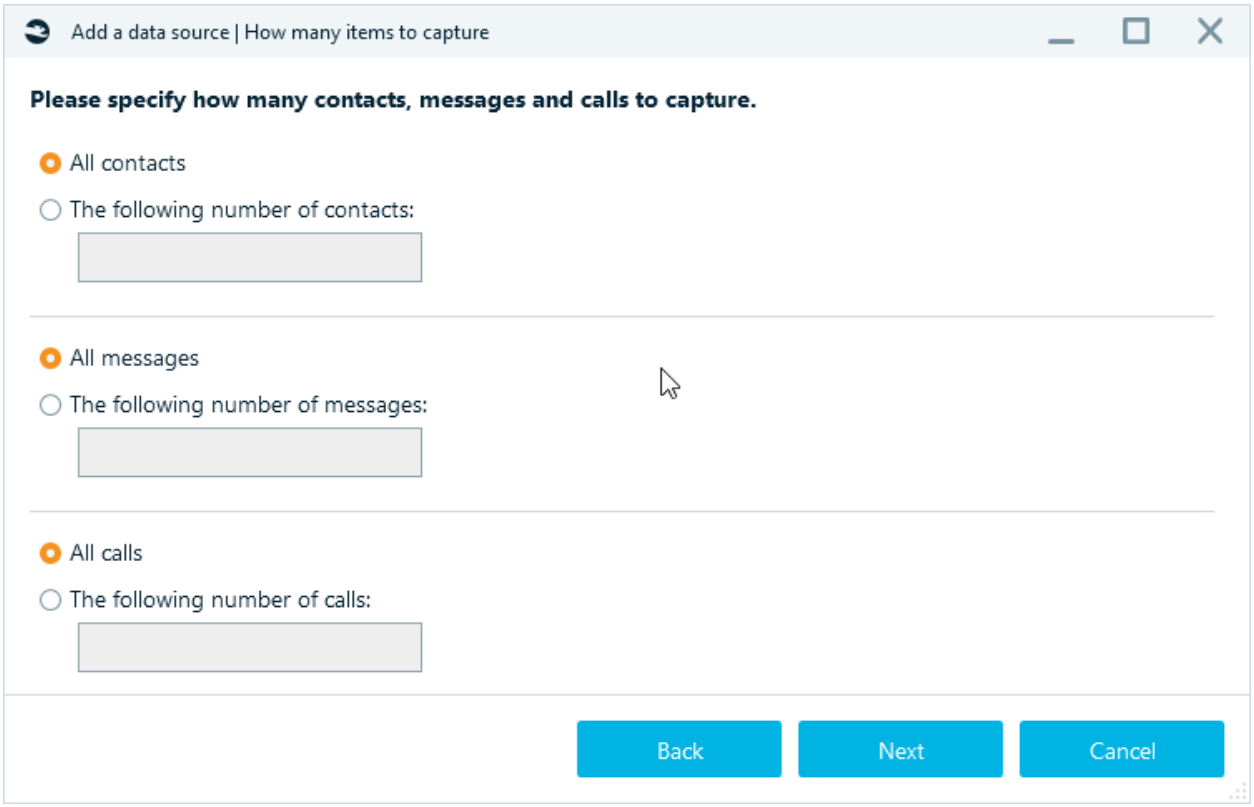
Before you start acquisition: allow **USB debugging mode** in **Developer options**, turn on **Flight mode** on the device and connect the device to the computer.

After selecting **Screen capturer** (in the window 'Add data source| Please select the acquisition type') you will see the window below:

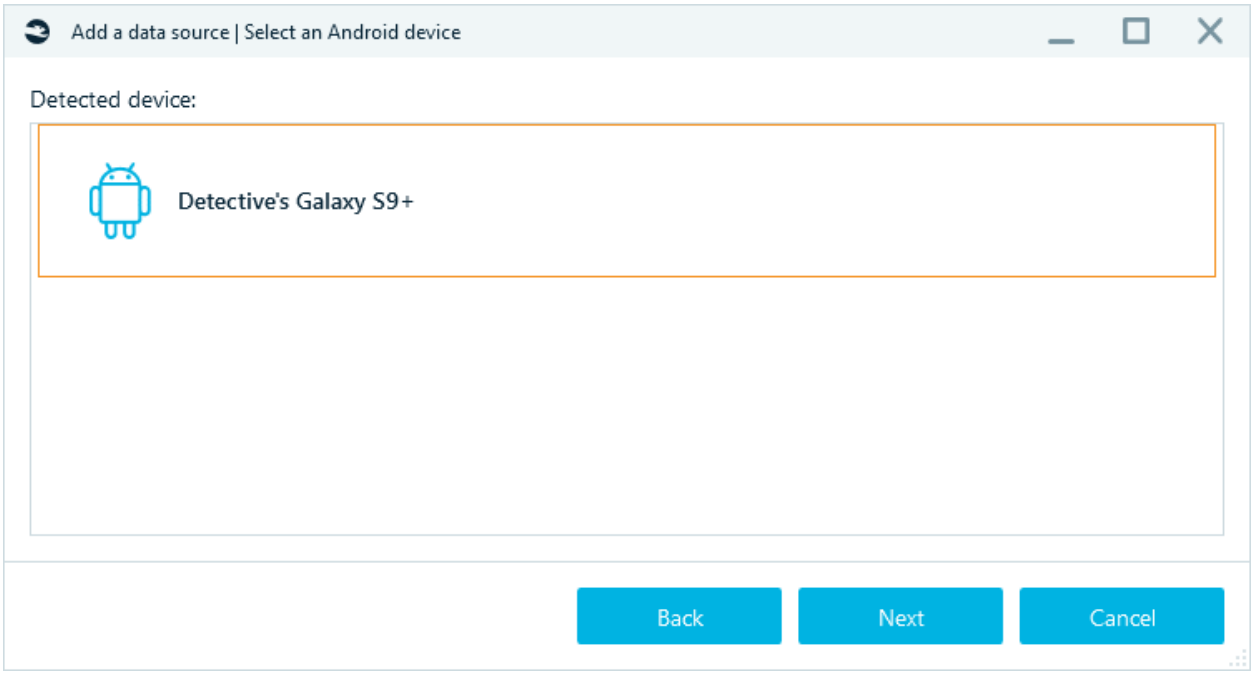


Choose application that you want to capture.

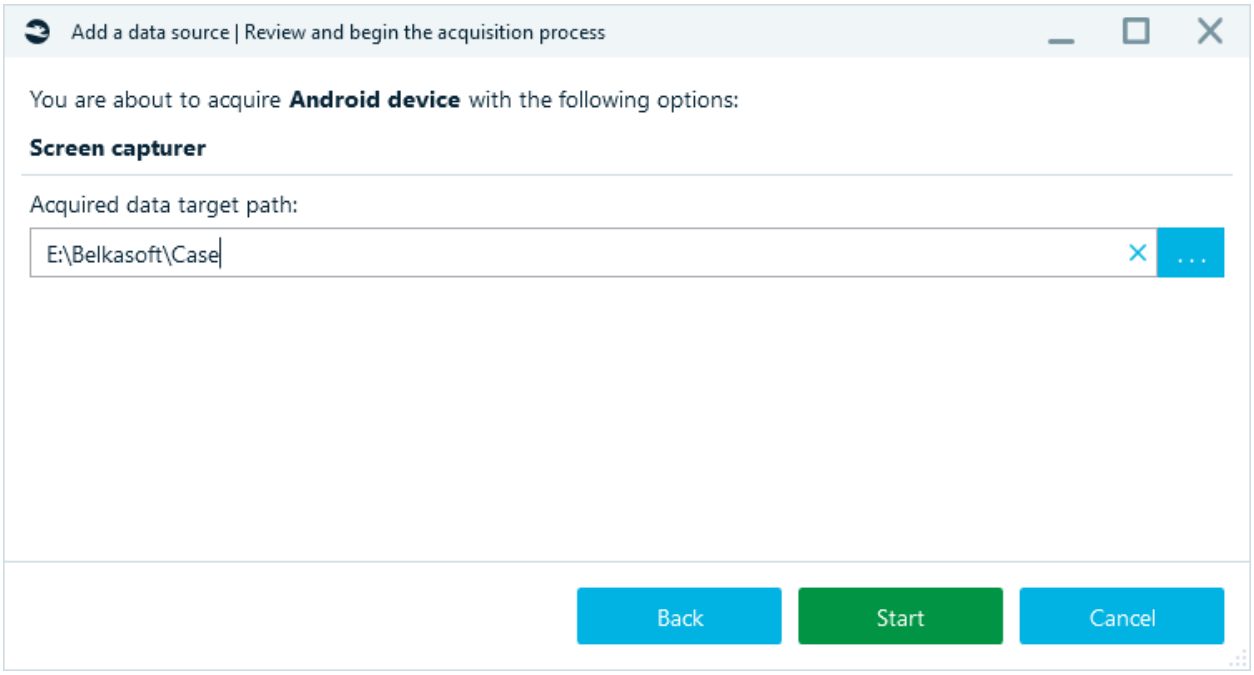
Then specify acquisition settings (settings change depending on the selected application):



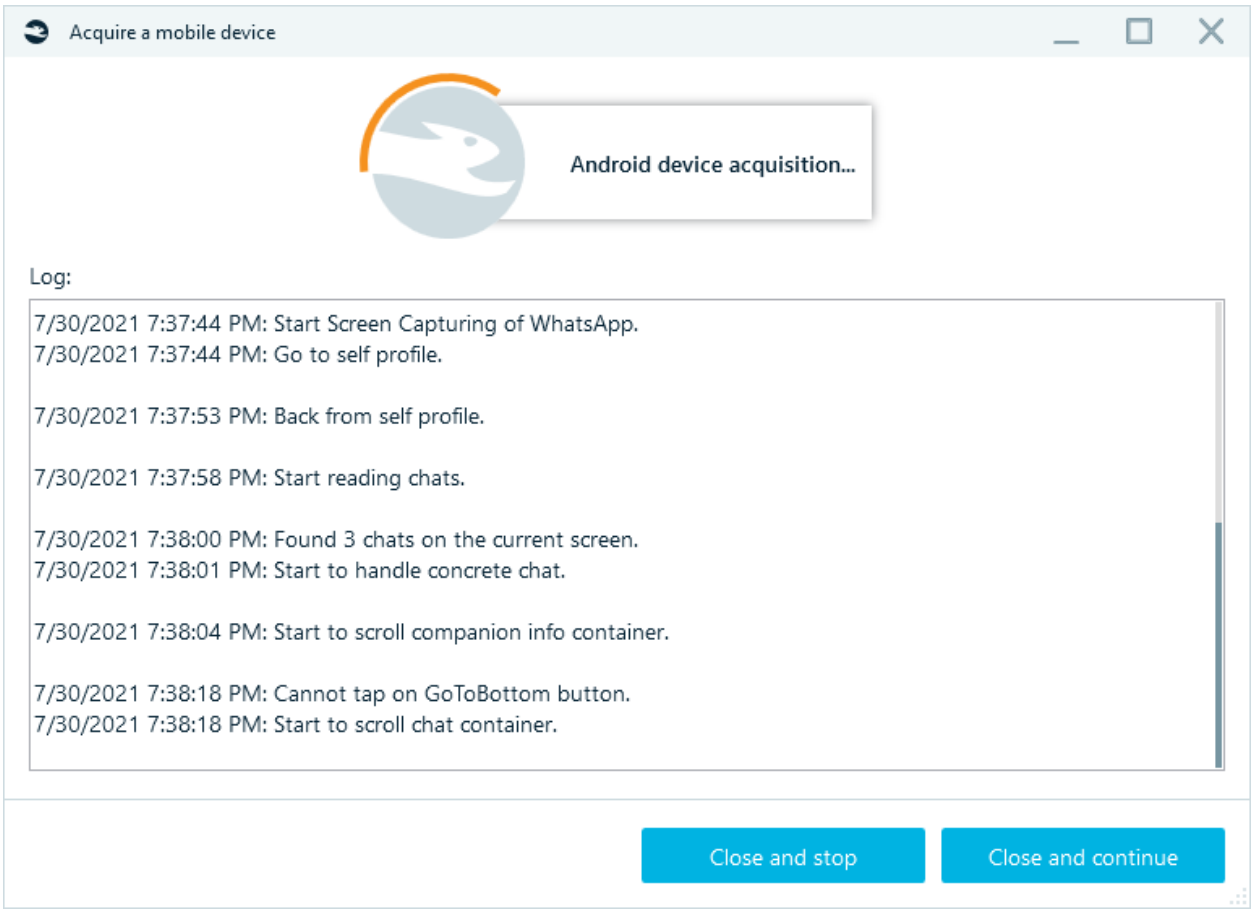
Select device:



And specify the **Target path** (for the folder where the smartphone image will be stored):



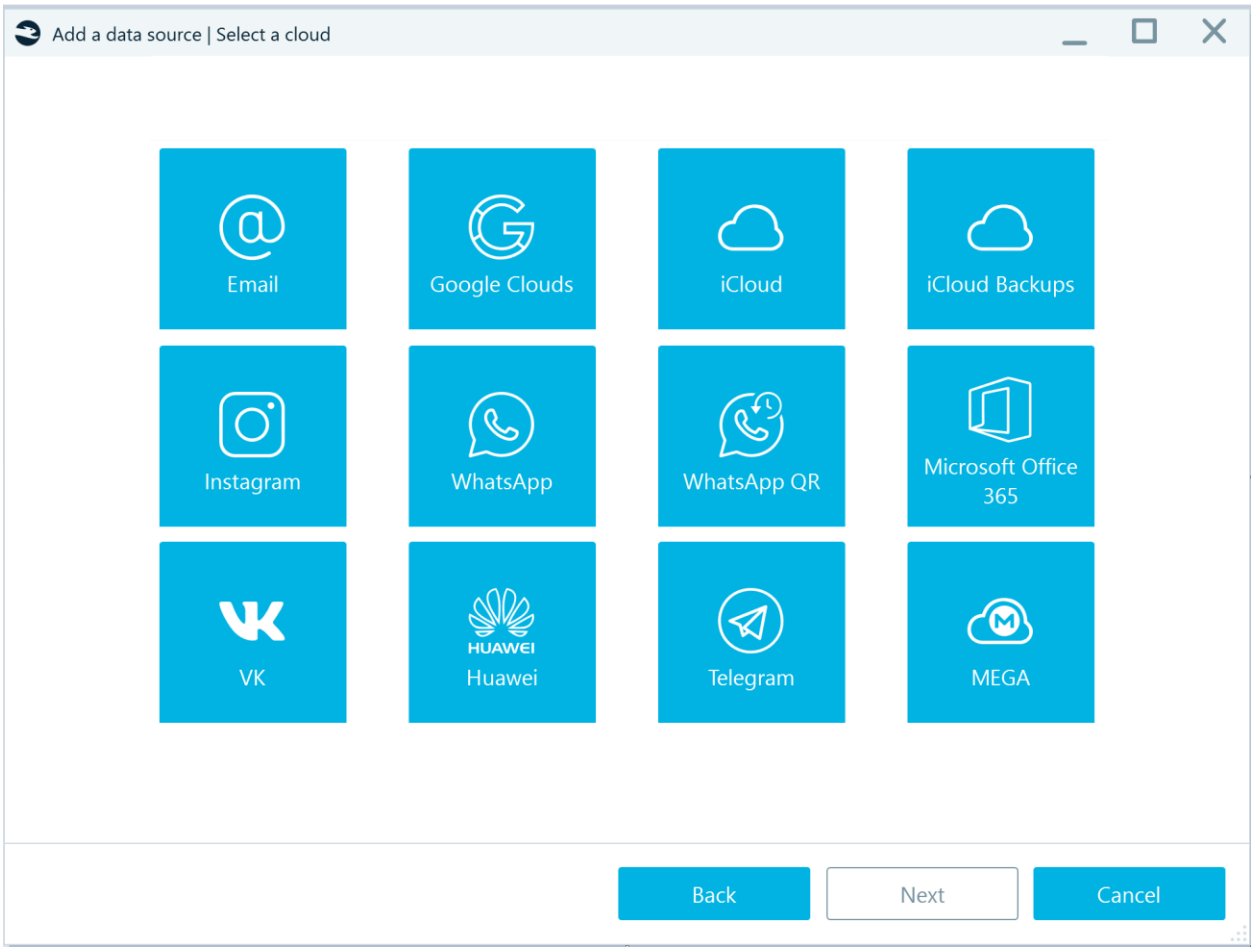
Click **Start** - acquisition will begin.
Click **Allow USB Debugging** when displayed on the device screen.
DO NOT TOUCH the device during whole acquisition process. Throughout the entire process, the log reflects information about what is happening at the moment.



Wait for the acquisition has been completed and observe the results.

Acquiring cloud

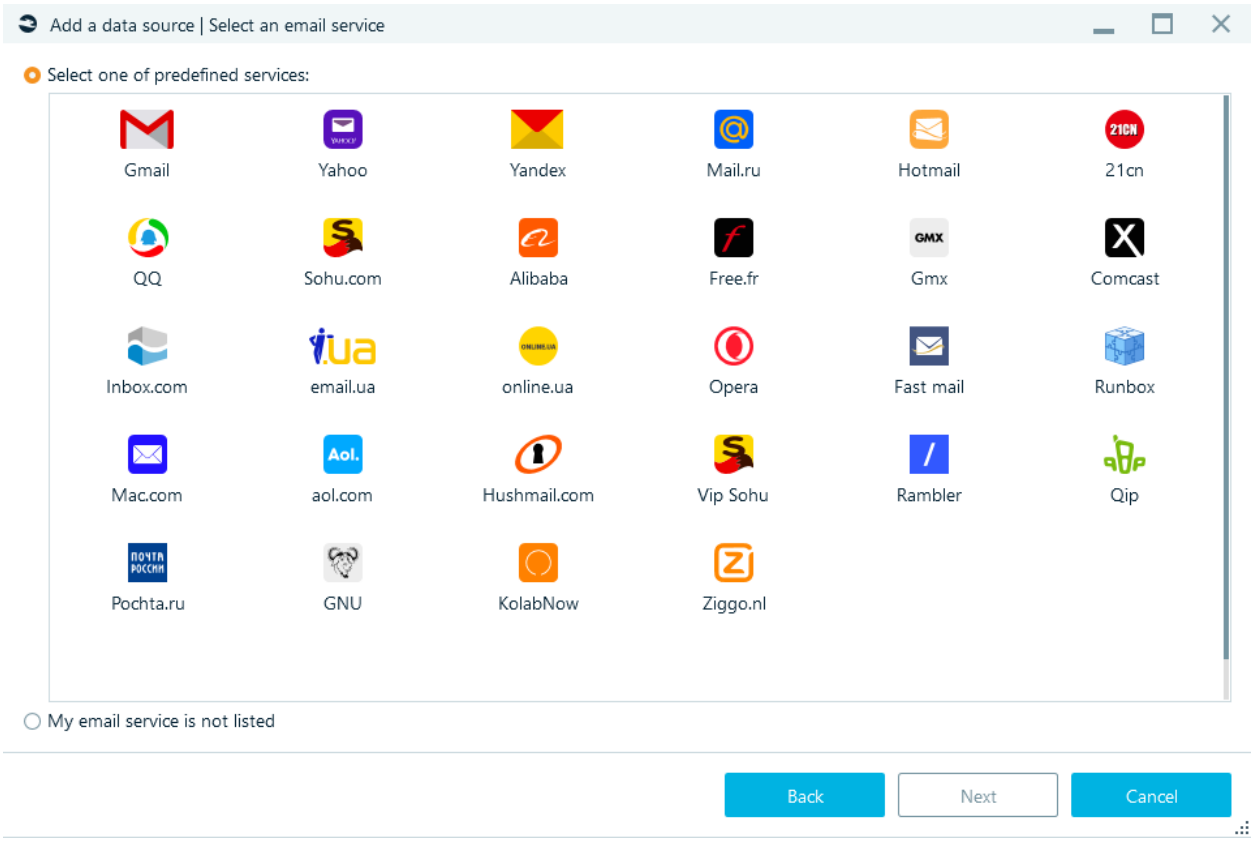
Using this option, you can acquire remote data stored on one of supported cloud services.
After clicking on **Cloud** (in the window **Add a data source | Select a type of data source to acquire**), you will see screen with list of supported cloud services:



Upon click on one of those, you will see further settings.

Email

For **Email** cloud services, the following screen is shown:

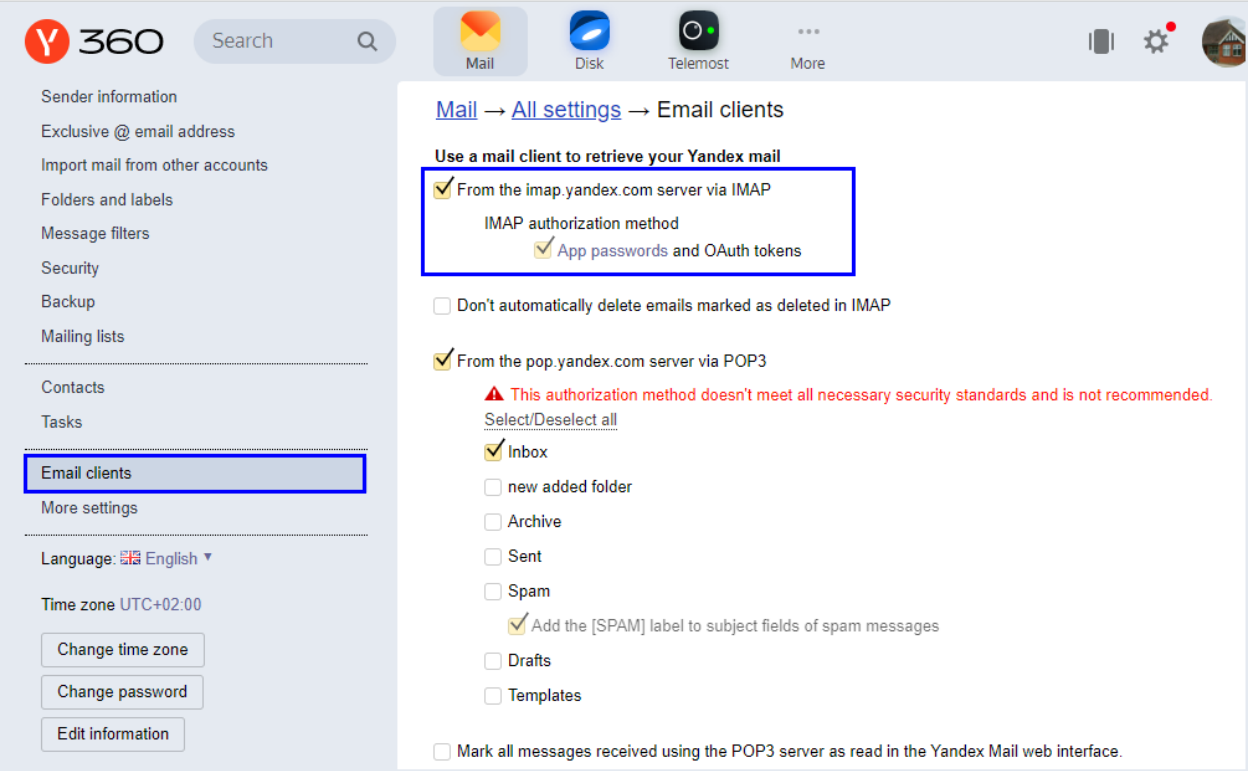


You can select any service Belkasoft X supports or select **My email service is not listed**.

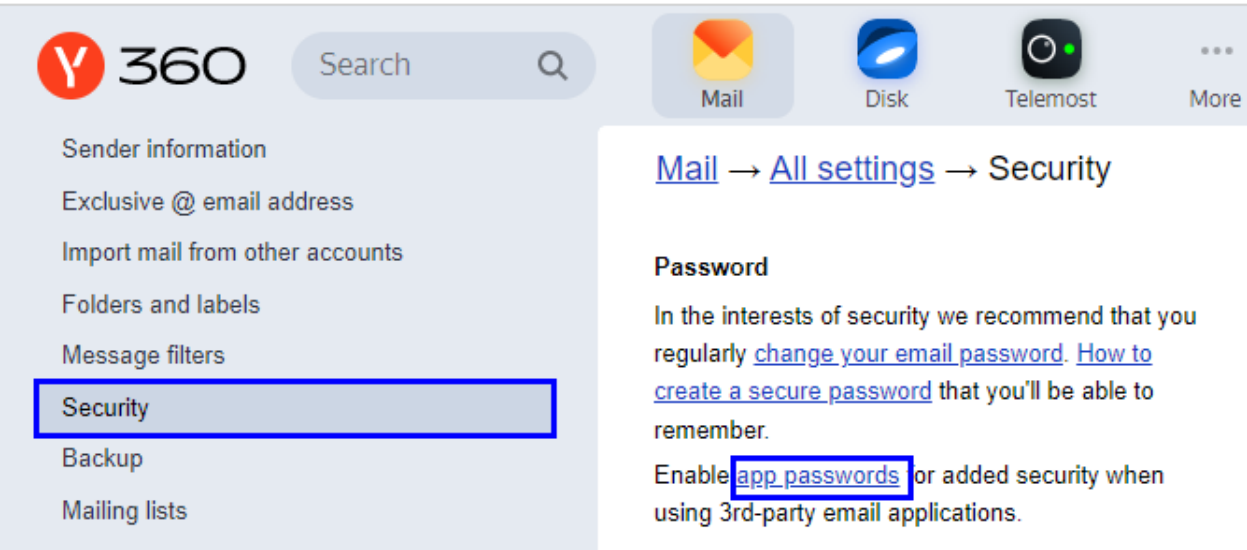
Emails are downloaded via IMAP or POP3.

Yandex mail

For download by IMAP:
Go to Settings, select Email clients.
For *Use a mail client to retrieve your Yandex mail* check *From the imap.yandex.com server via IMAP* and *App passwords and OAuth tokens*:

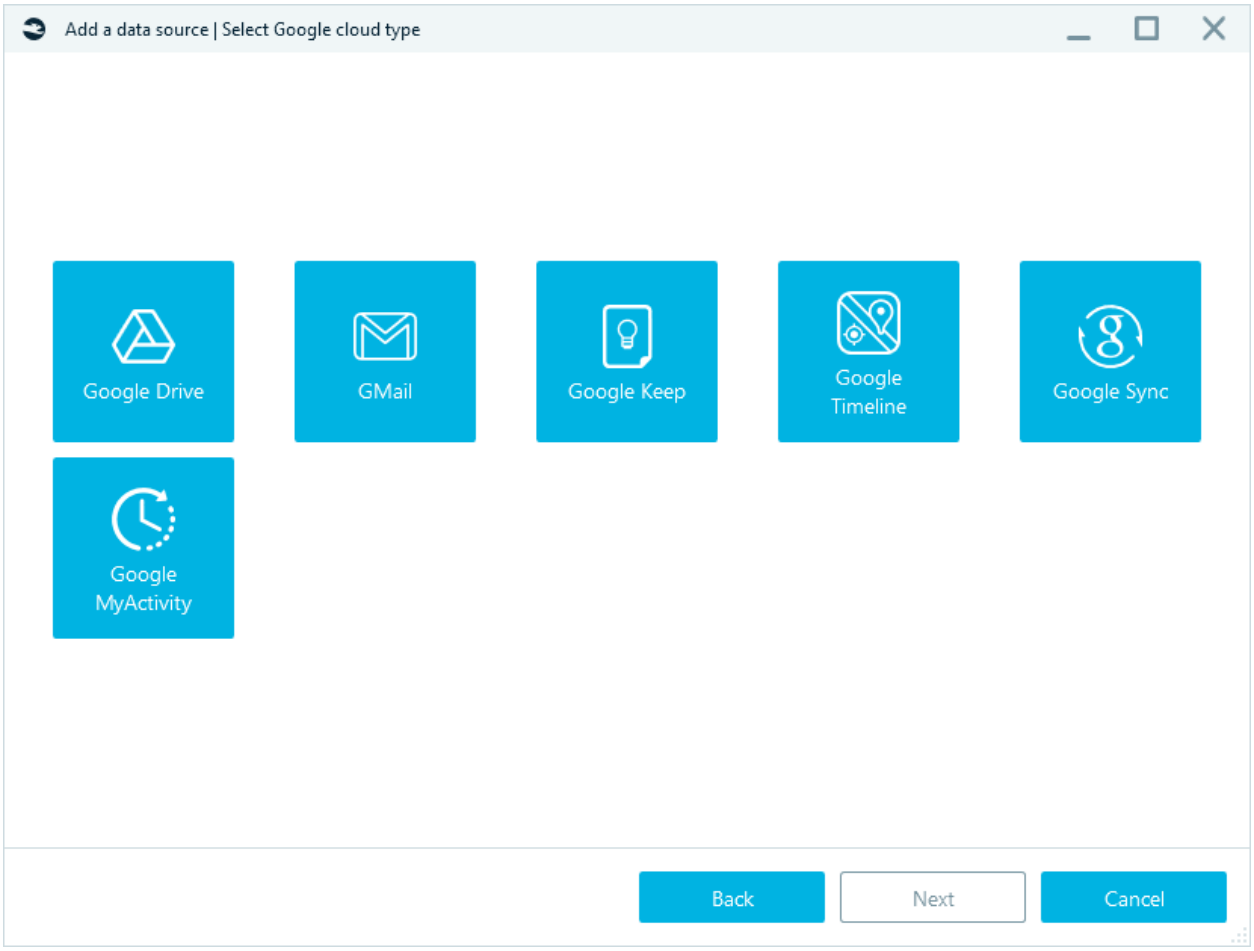


Create an Application password (Settings - Security - App passwords):



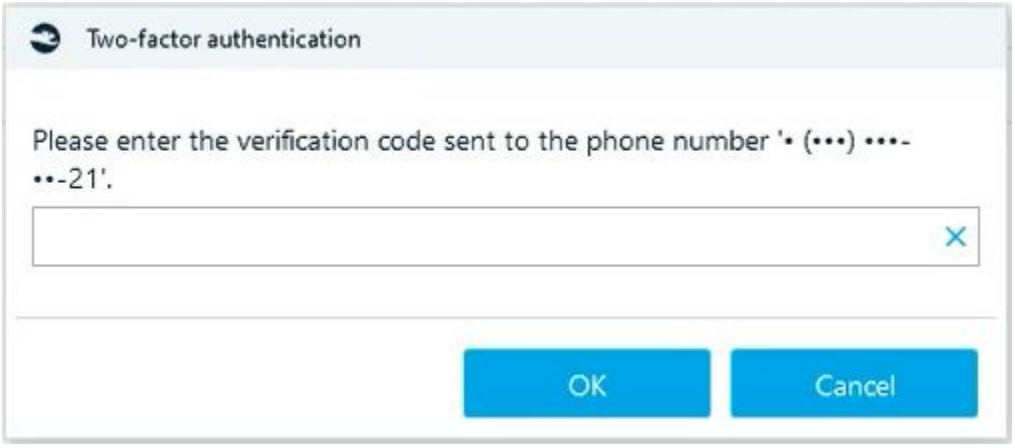
In Belkasoft X when downloading use the generated password.

Google clouds



Once you specified a service, you will see authentication screen:

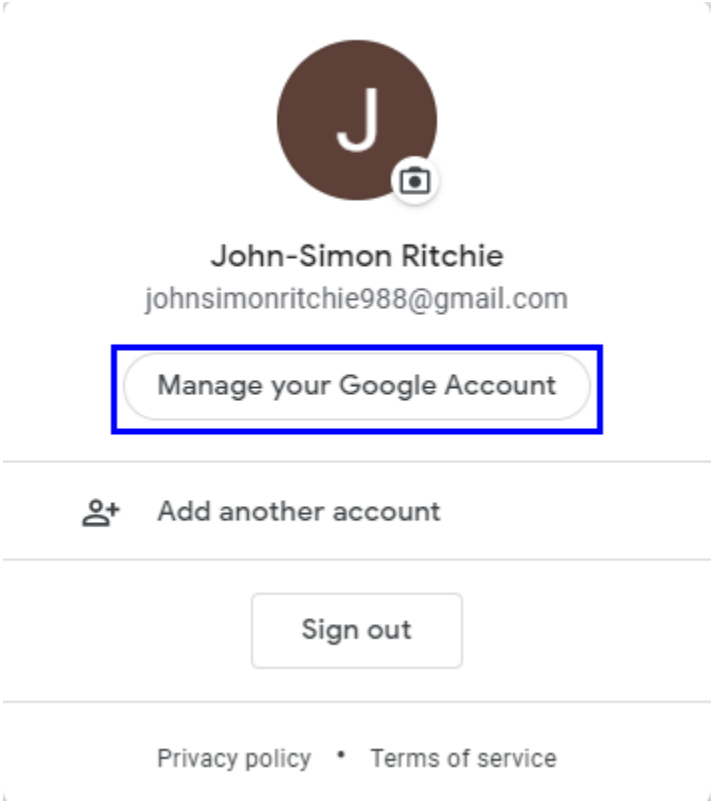
Also supports two-factor authentication for extracting Google Cloud data.
If the two-factor authentication function is enabled, a window for entering the passcode will appear:



Gmail

If task 'Downloading cloud data' (for Gmail) fails, set up IMAP and try to use an App Password. An App Password is a 16-digit passcode that gives a less secure app or device permission to access your Google Account. App Passwords can only be used with accounts that have 2-Step Verification turned on.
How to create App Password?

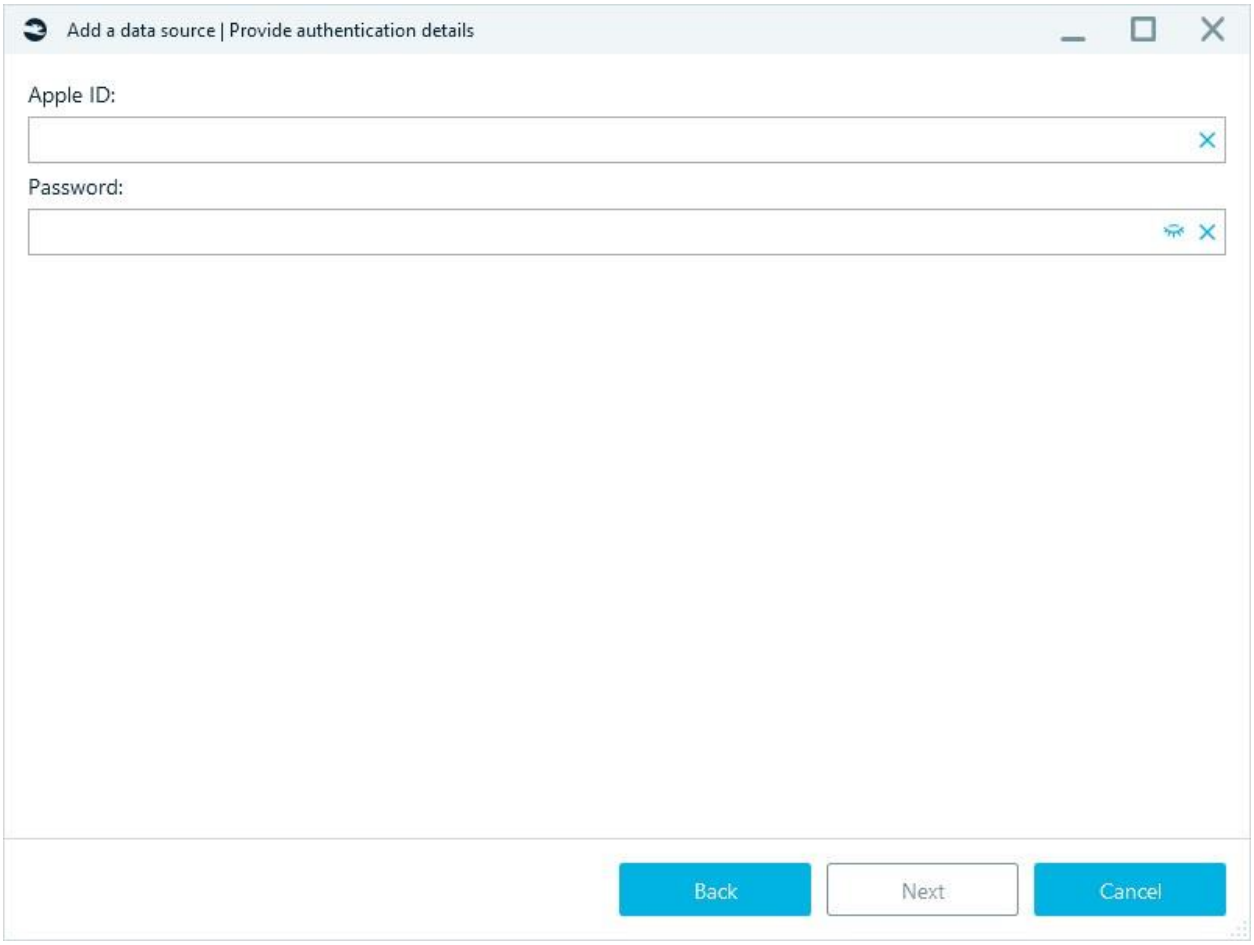
1. Go to Google Account (click on Manage your Google account).



2. Select Security. Under "Signing in to Google," select App Passwords. You may need to sign in.
3. At the bottom, choose Select app and choose the app you using and then Select device and choose the device you're using and then Generate.
4. Follow the instructions to enter the App Password. The App Password is the 16-character code in the yellow bar on your device.

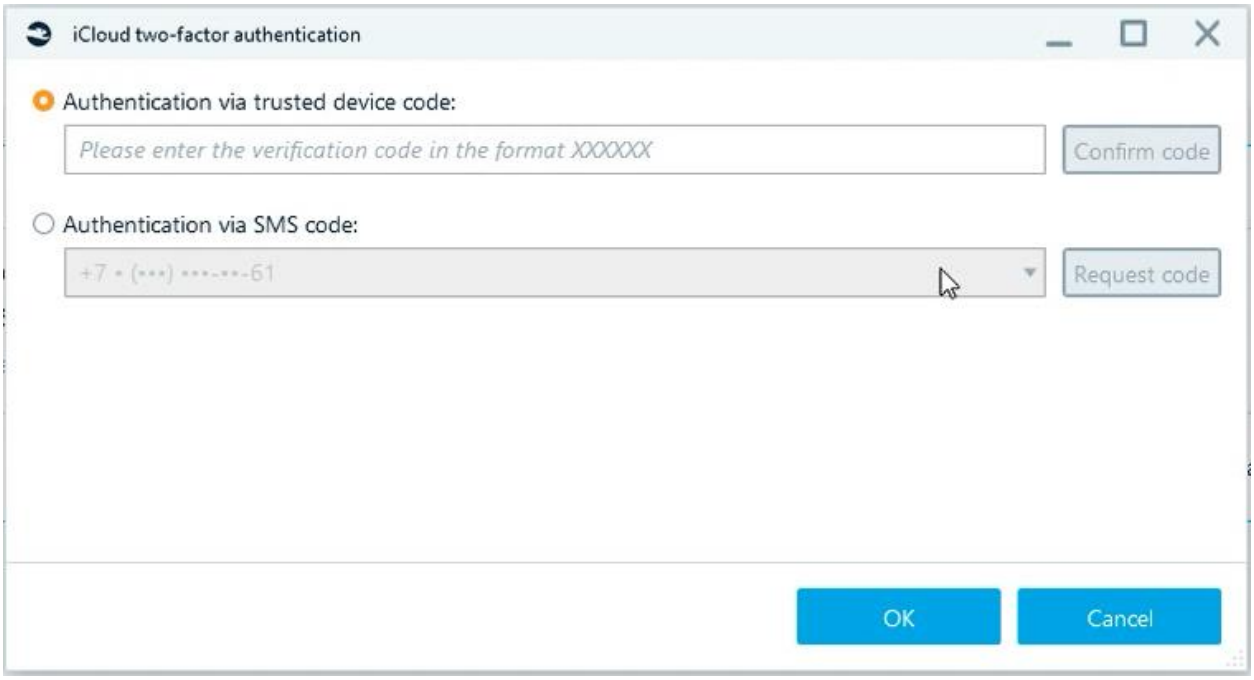
iCloud

Enter Apple ID and password:

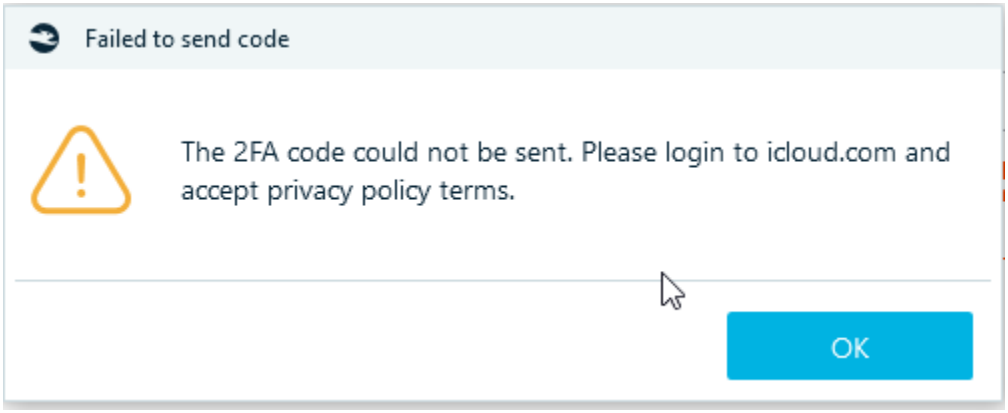


Specify the **Target path** for acquired data, click **Start.**

Authenticate with a code from a trusted device or an SMS code:



When authenticating via SMS, Privacy policy terms confirmation may be required:

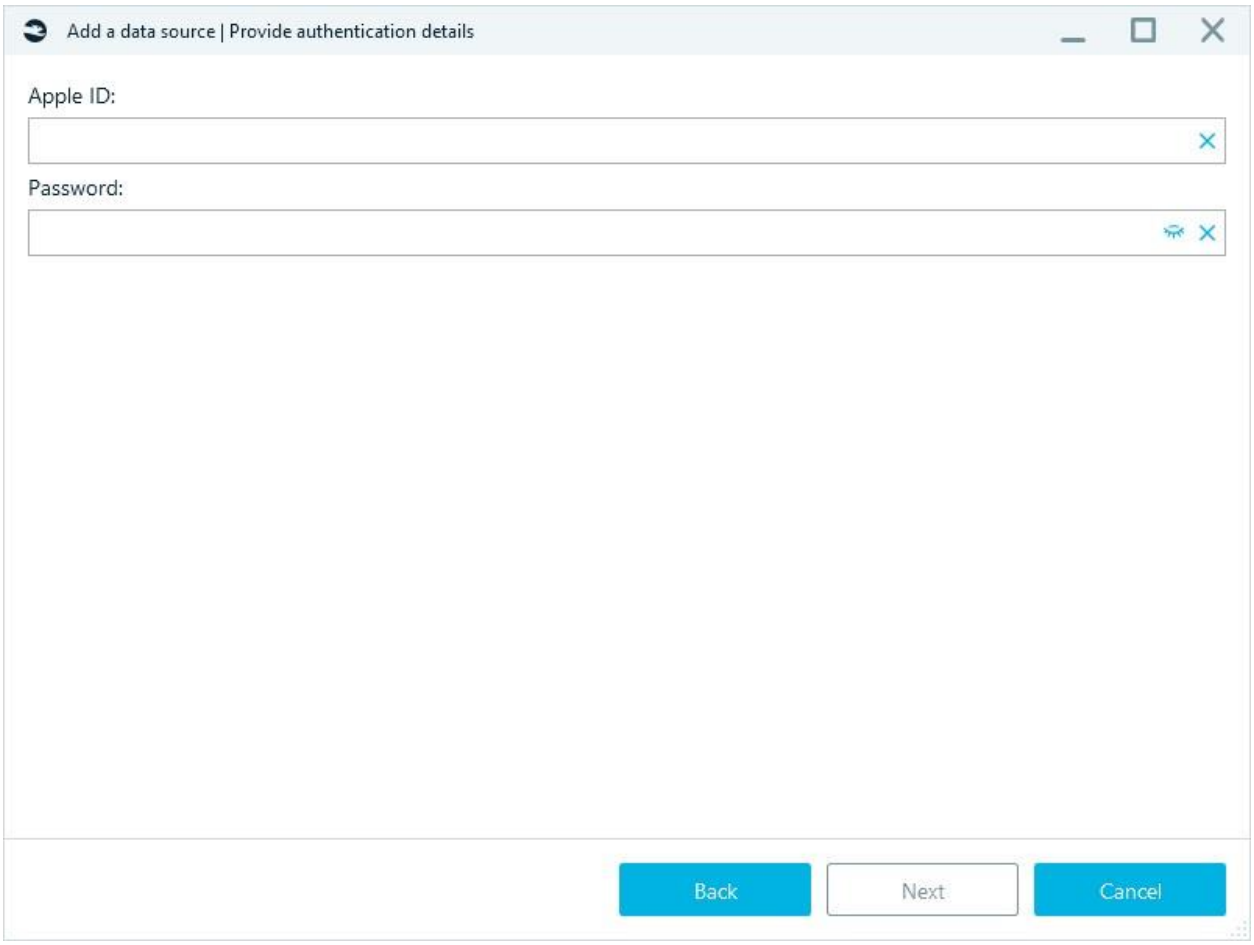


After successful authentication, data download will start.

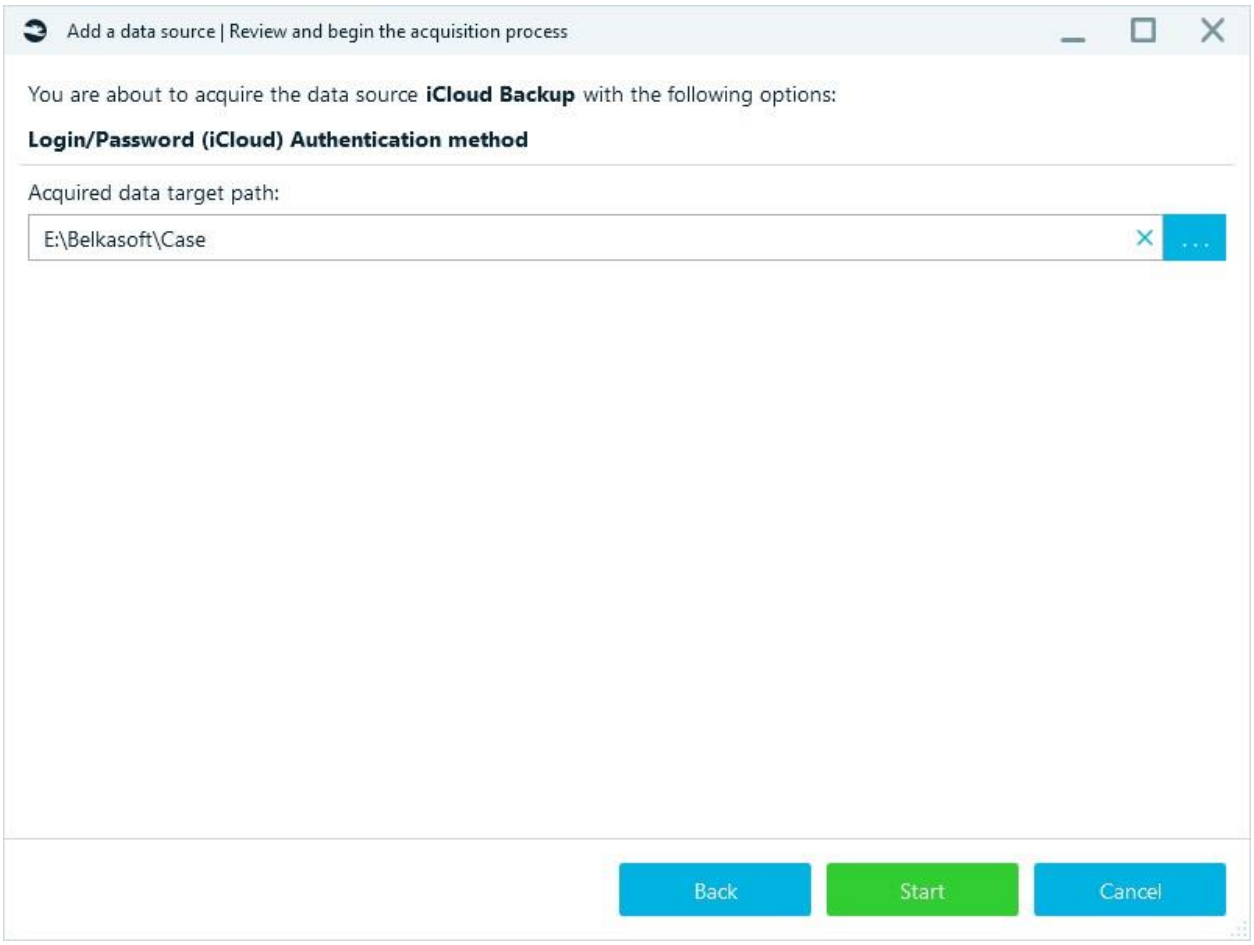
iCloud Backups

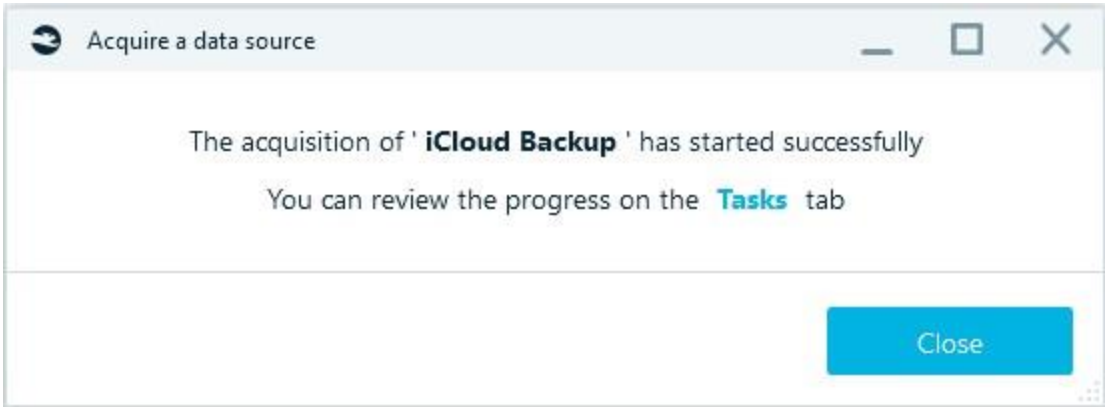
Before the start of the acquisition, launch iTunes and iCloud (log in with an account different from the one that will be used for the acquisition)**.**

Enter Apple ID and password:



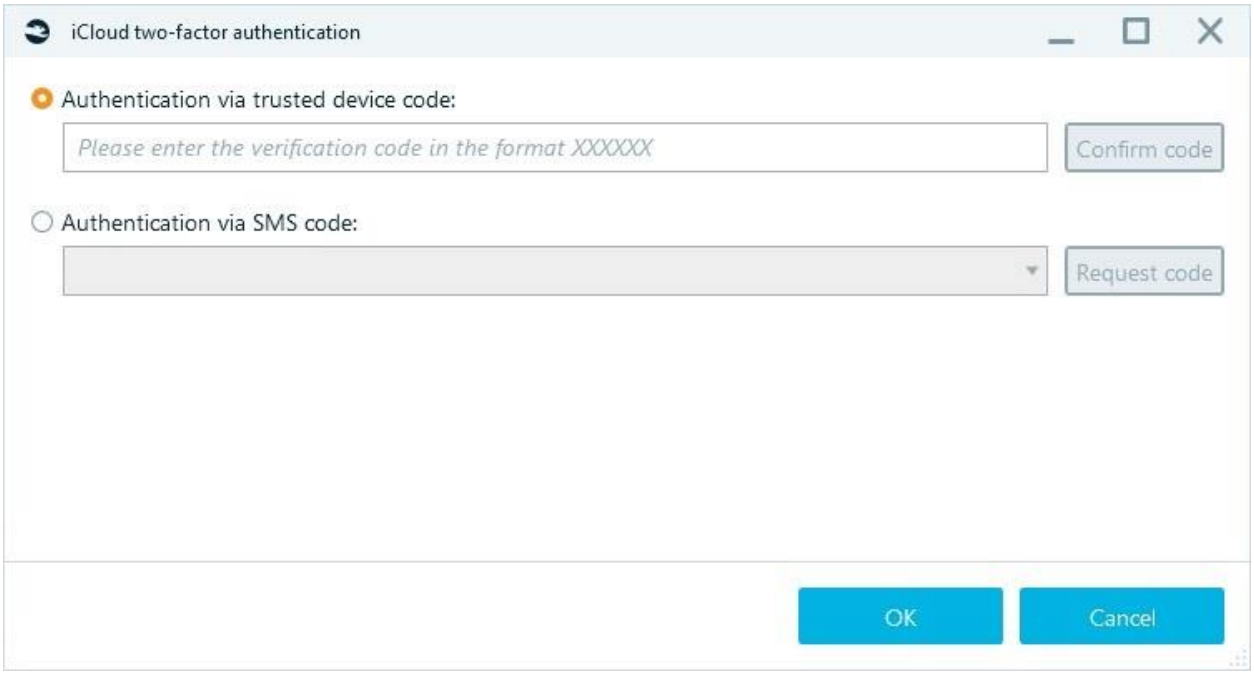
Specify the **Target path** for acquired data, click **Start.**



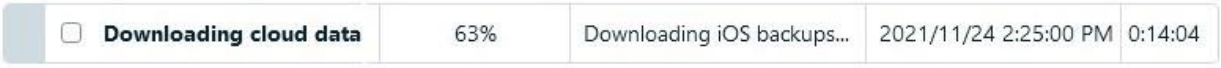


Downloading cloud data task will start:

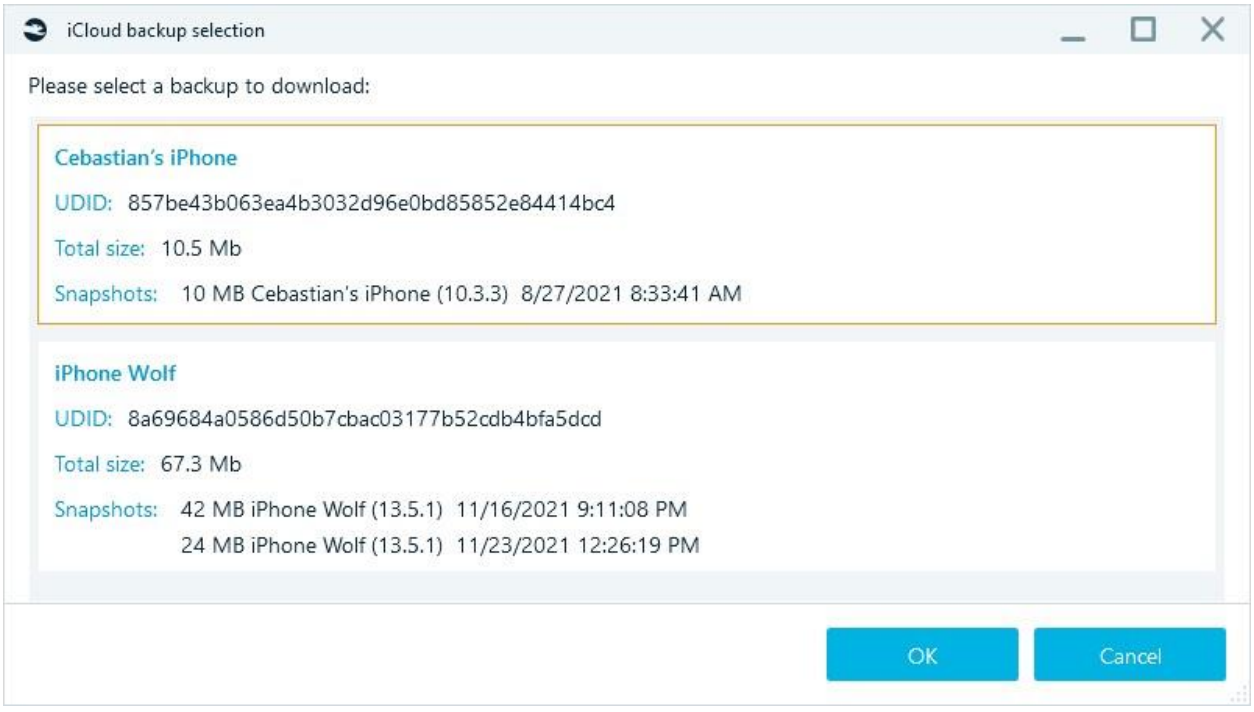
Then you will be prompted to authenticate using a code on a trusted device or an SMS code:



After successful authentication, data download will start:

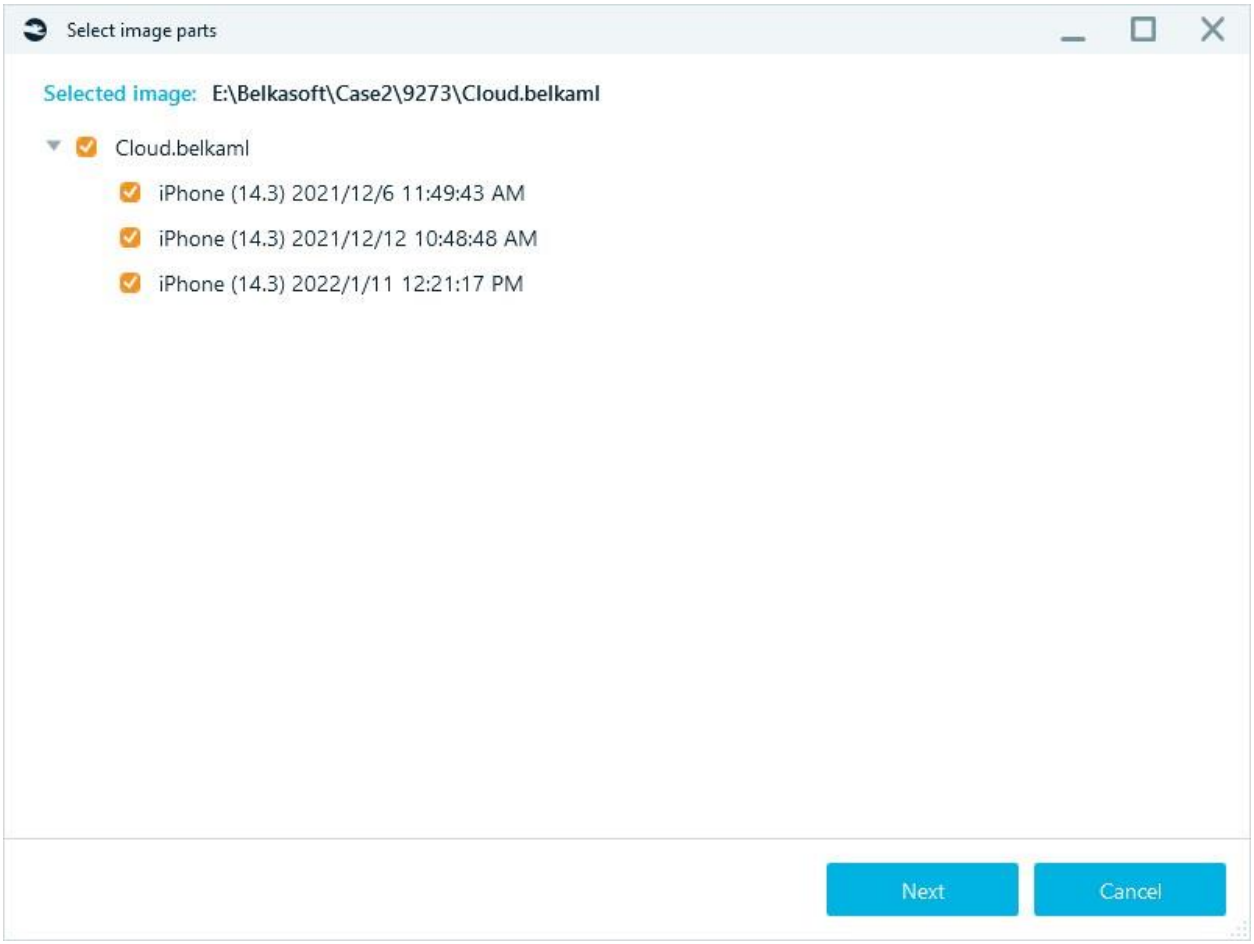


In the **iCloud backup selection** window, select the backup you are interested in. For multiple selection, hold down Ctrl.

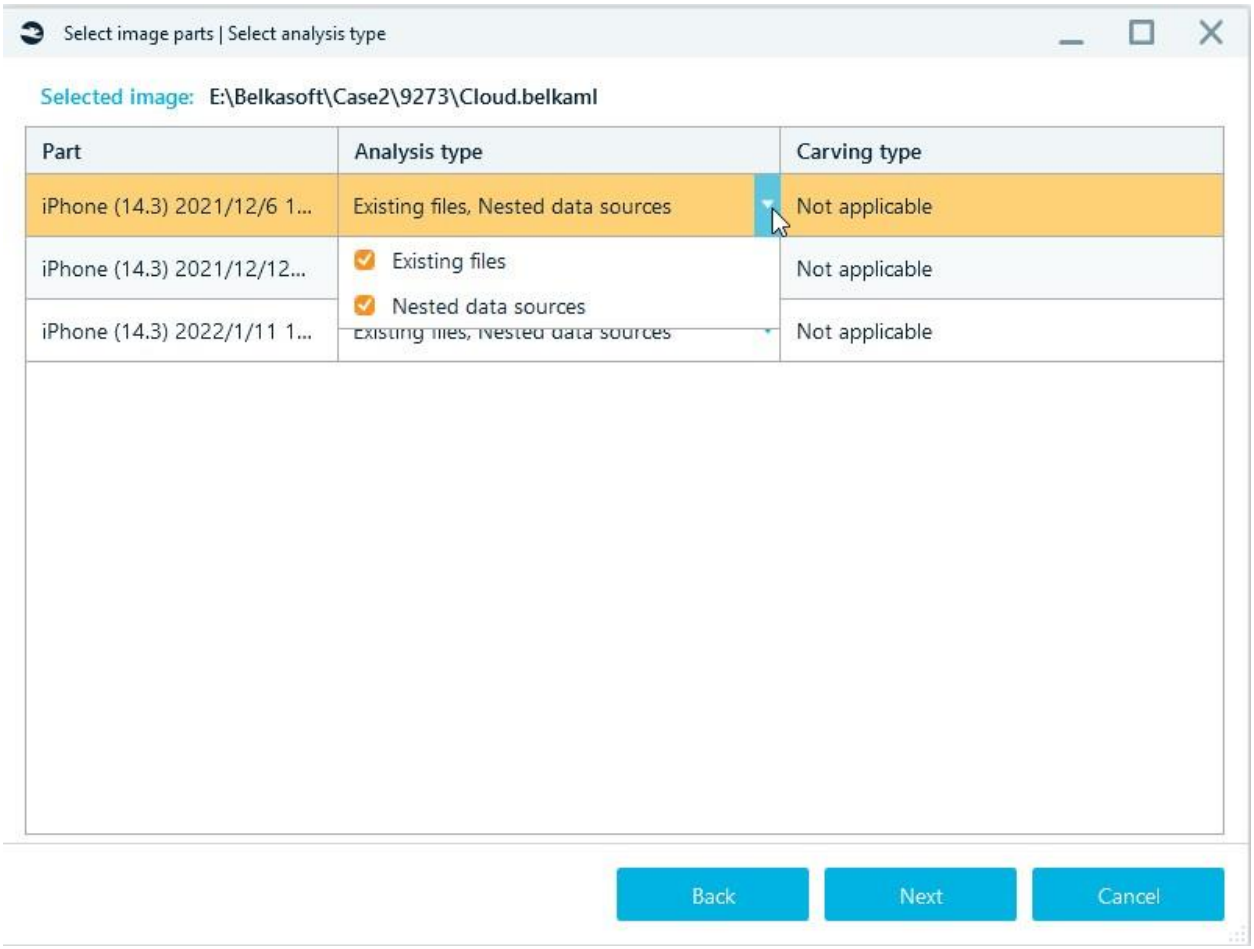


After acquisition is finished, you will be prompted to start the analysis.

Select image parts:



And other analysis settings:



Note: If iTunes and iCloud are running, but the 'Downloading cloud data' task is failed to complete, restart Belkasoft X.

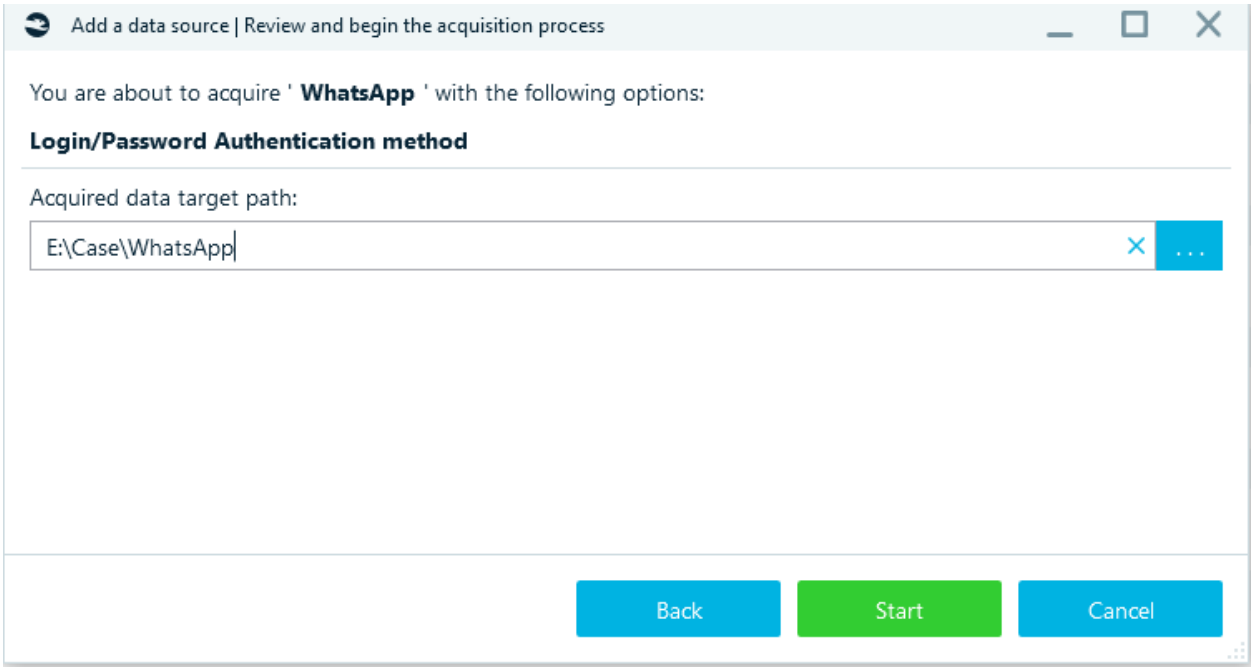
WhatsApp

For Android devices that have backed up chats.

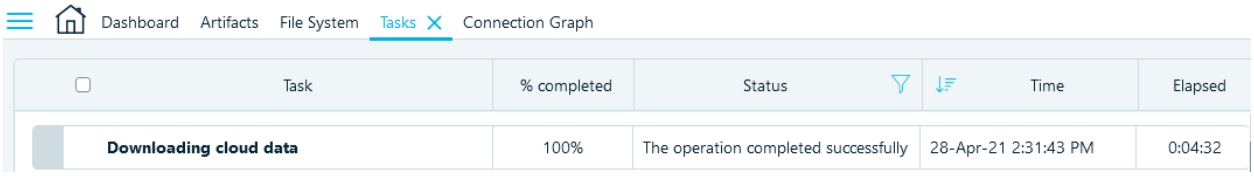
After choosing WhatsApp, you will see authentication screen:

Enter Email and Password (Google account) and press Next.

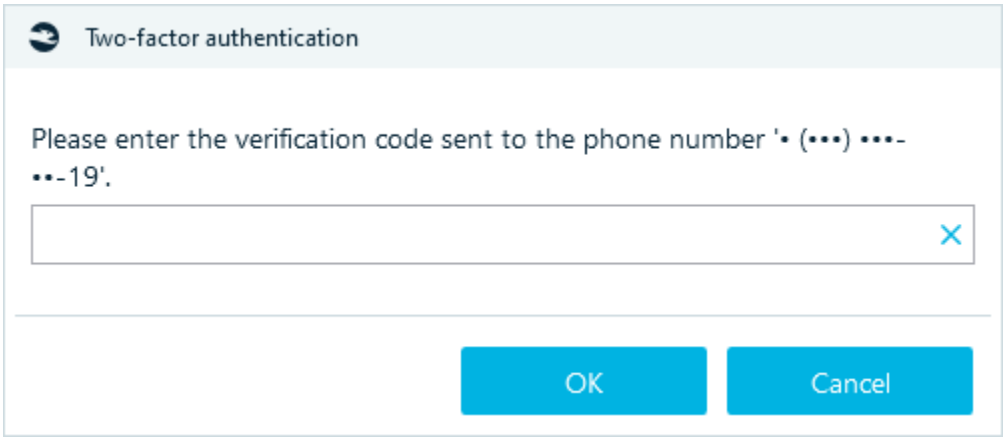
Check your selection and press Start:



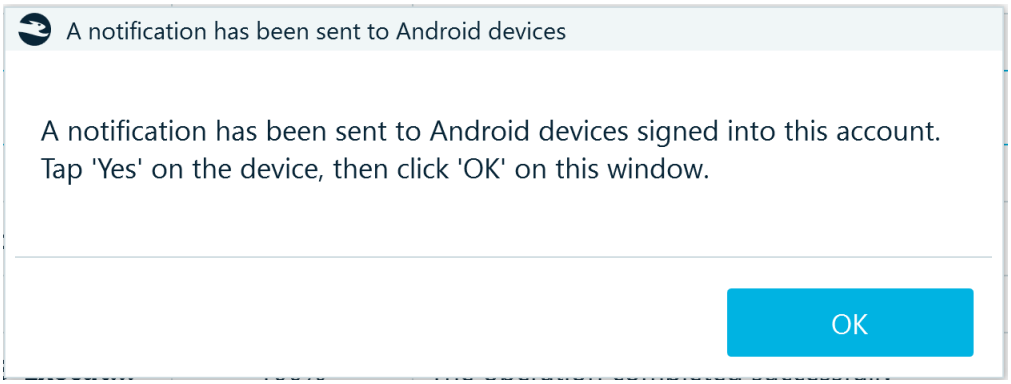
Task ‘Downloading cloud data’ will start:



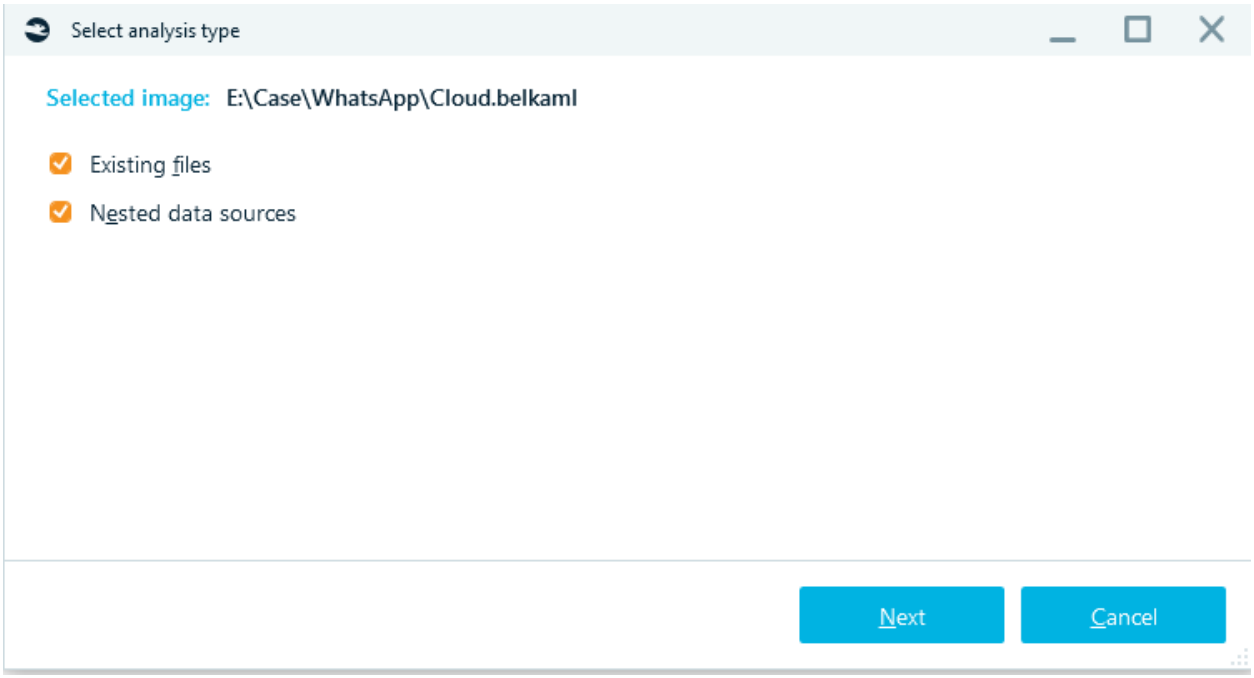
If two-factor authentication is enabled, enter the code from the phone.



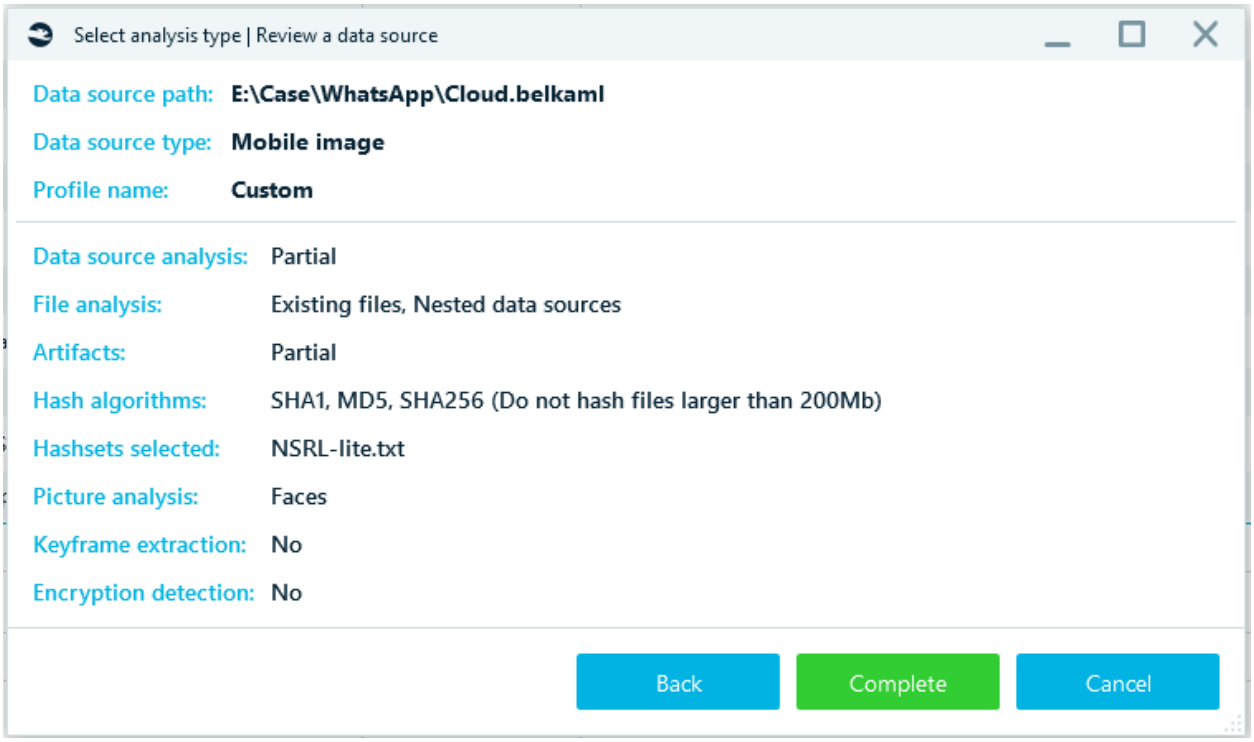
Phone verification may also be required:



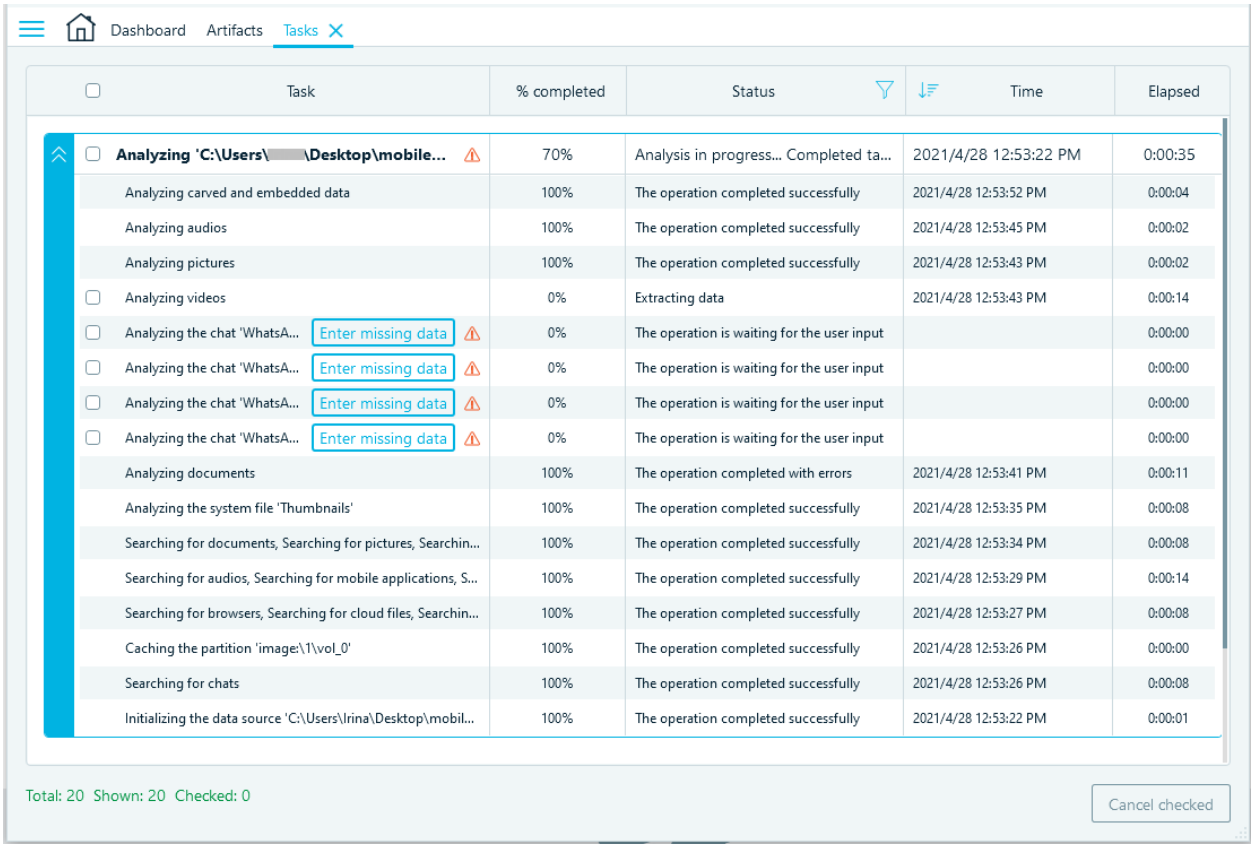
After the task is completed, window ‘Select analysis type’ appears with the choice of the type of analysis:



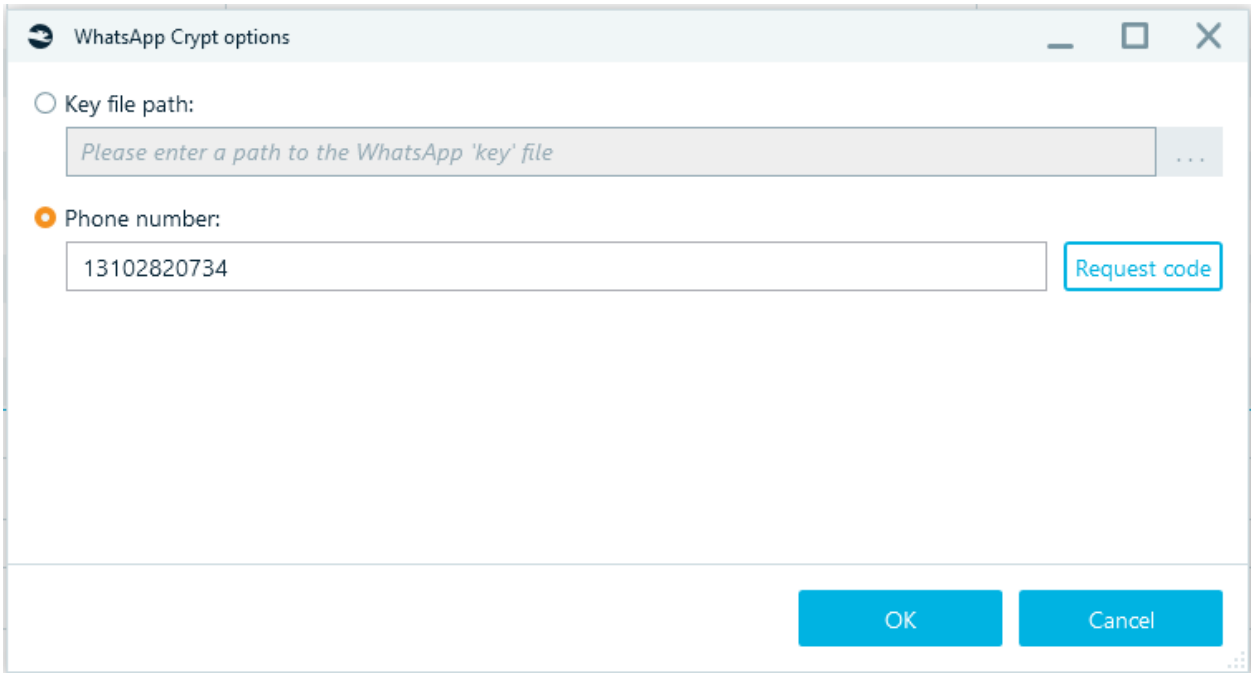
Select the required analysis parameters and press Complete:



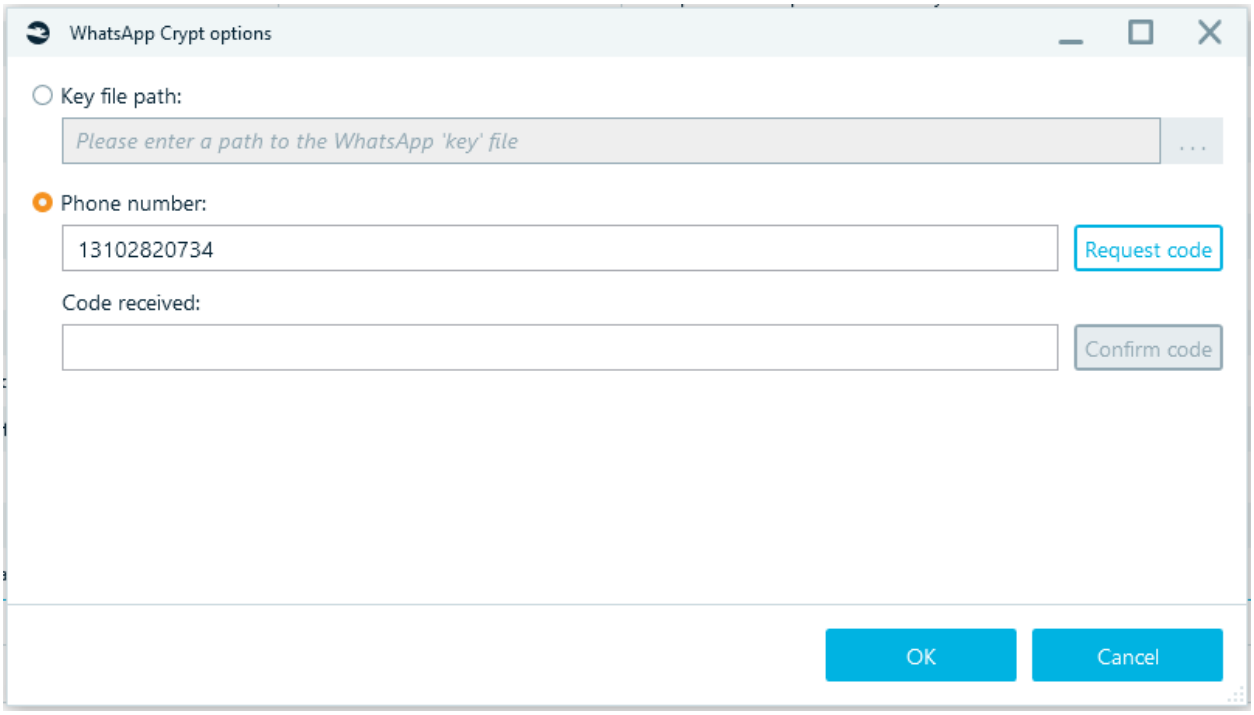
Press Enter missing data in **Tasks**.



In ‘WhatsApp Crypt options’ enter the path to the key file or choose to receive the code by phone number:



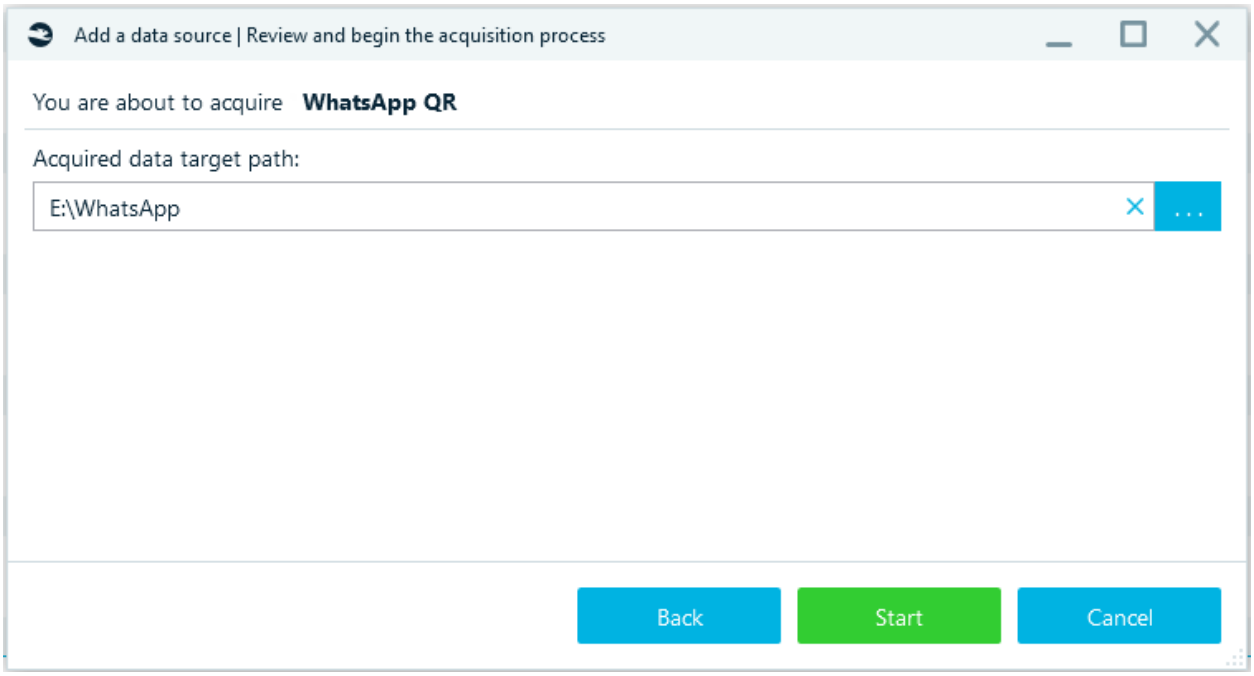
After pressing Request code, an SMS with a code will be sent to the specified phone number.



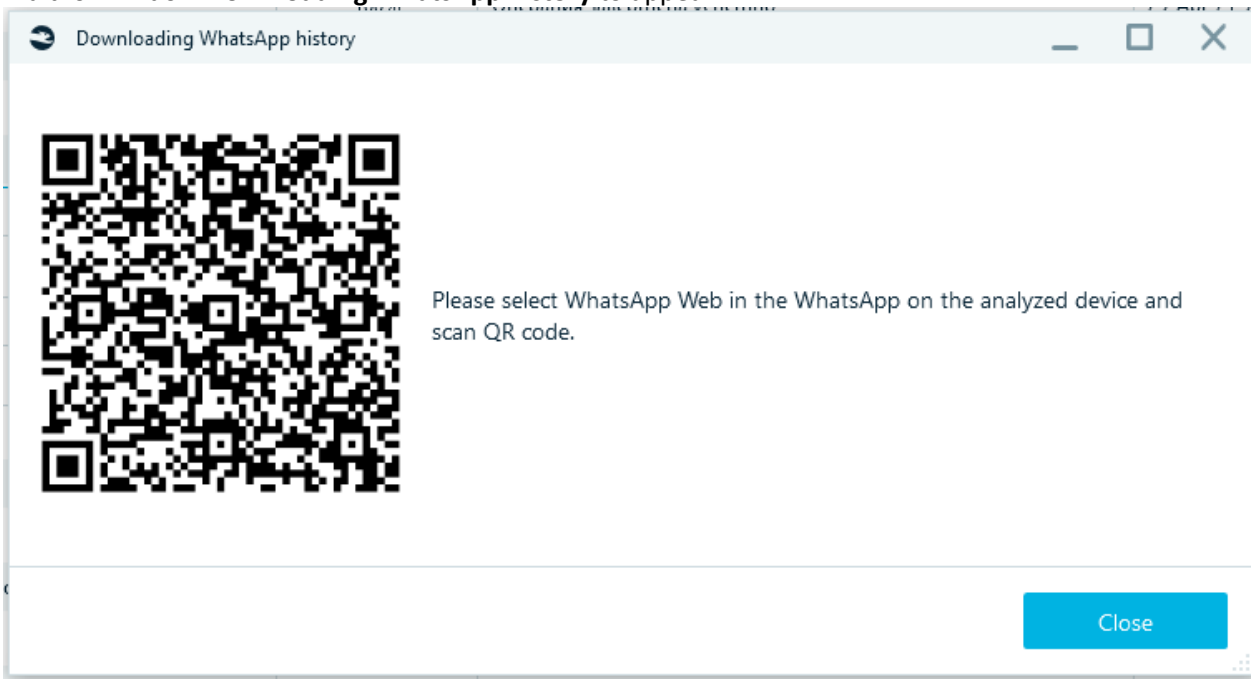
Enter code and press Confirm code. Click Ok - decryption will begin.

WhatsApp QR

WhatsApp data download using Web API (with a QR code). For iOS and Android.
Specify the **Target path** for acquired data, click **Start.**



Wait for window **Downloading WhatsApp history** to appear.

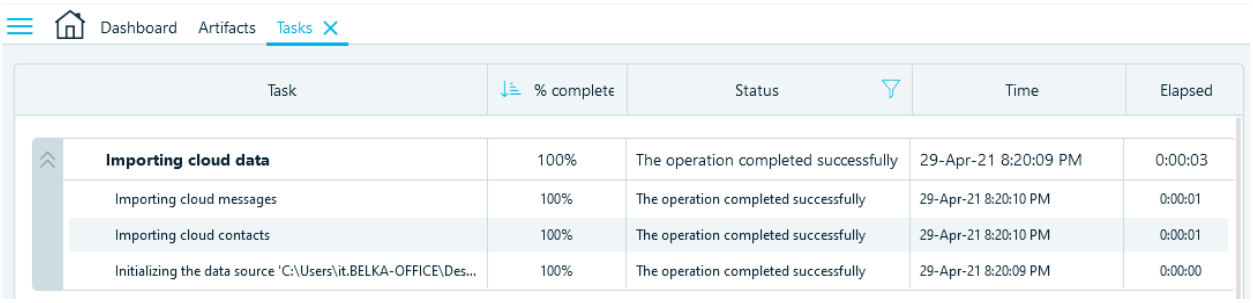


On your smartphone, open “WhatsApp Settings”, then “WhatsApp Web / Desktop” and “Link Device”.
Scan the QR code in the **Download WhatsApp History** window.

Task ‘Downloading cloud data’ will start:

After the task is completed, select analysis type in the appropriate window.

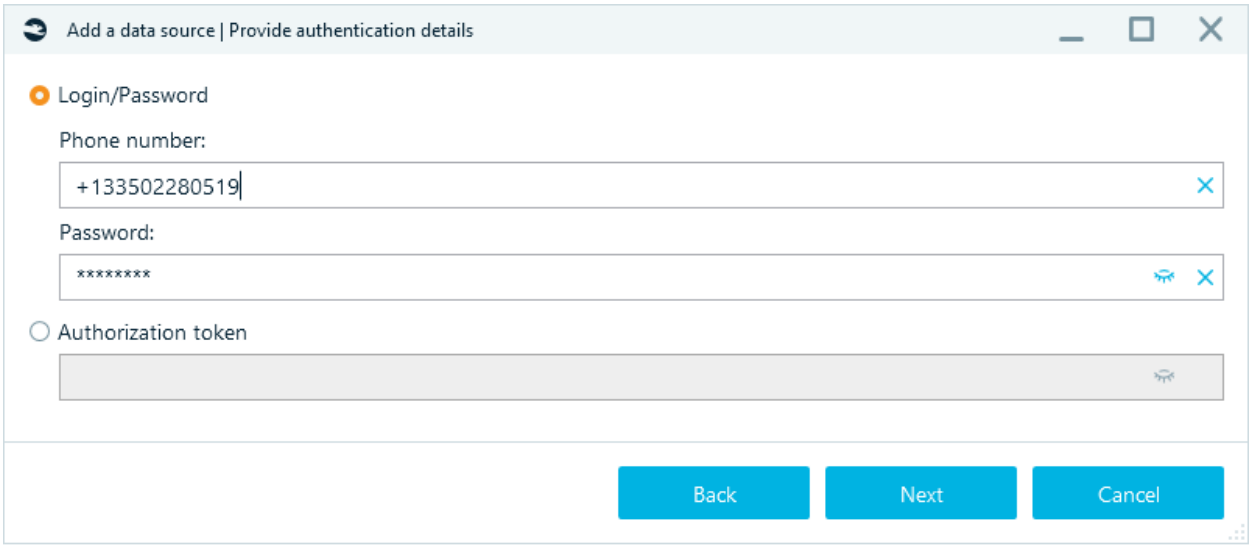
Task ‘Importing cloud data’ will start:



Note: If task is failed to complete and in log file: “Error occurred Please leave multi-device beta”, this means that the “Multi-device beta” option is enabled on the device, for a successful acquisition you need to disable it.

Note: The number of chat messages downloaded via the WhatsApp QR cloud acquisition method matches the number of messages displayed in the browser version of WhatsApp. However, older messages are not available in the browser version and can only be viewed on the phone or downloaded using the WhatsApp Cloud acquisition method. There is a workaround, but it is not considered forensically sound: older messages will be displayed and downloaded if a new message appears in an old chat.

VK



How to find data for an **Authorization token**:

Authorization token for iOS:

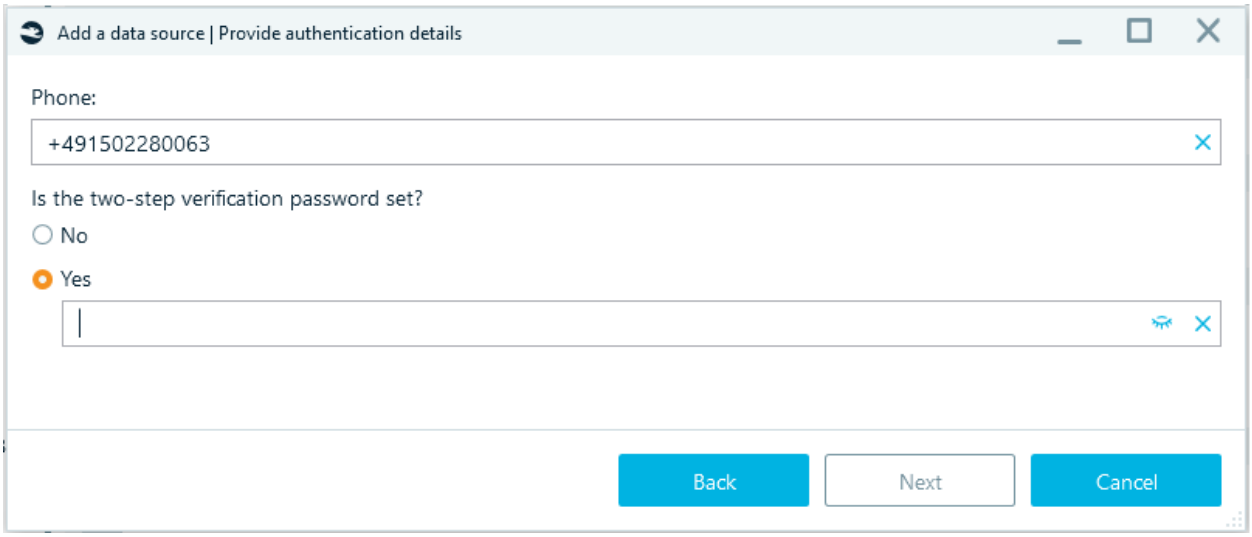
//private/var/mobile/containers/shared/AppGroup/group.com.vk.vkclient/Library/Preferences/group.com.vk.vkclient.plist
Tag **kVKMUDSessionKey**

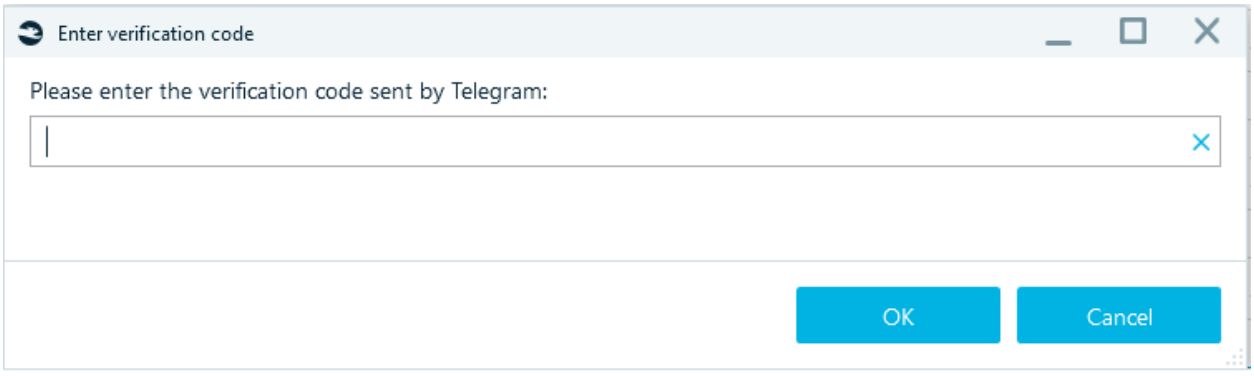
Authorization token for Android:

data/data/com.vkontakte.android/files/account.json
Tag **vk1.******

Telegram

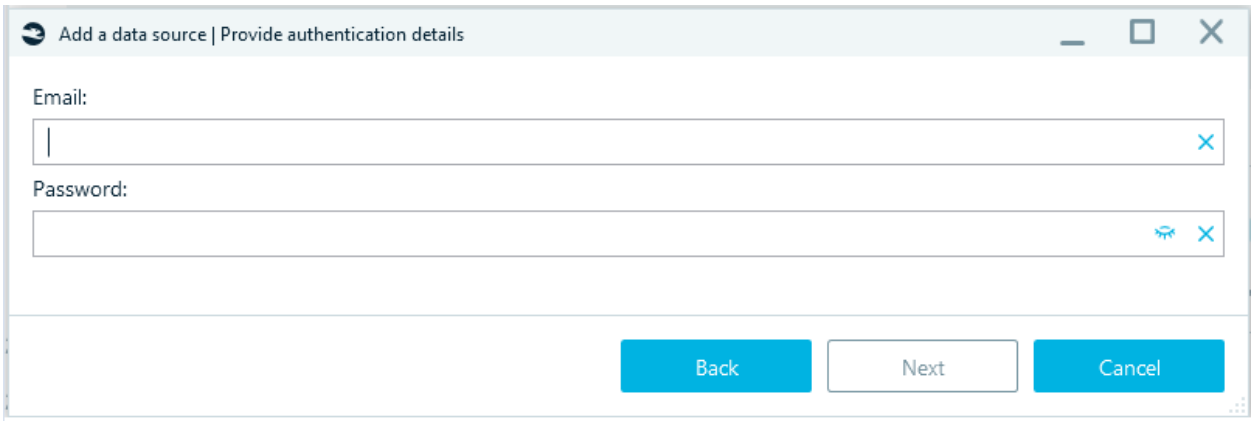
Telegram lets store an unlimited amount of data on its server. This functionality allows you to download Telegram cloud data.
You need to know the phone number and Two-Step Verification code.
You will also need access to Telegram to see the verification code (Passcode Lock Code may be required).

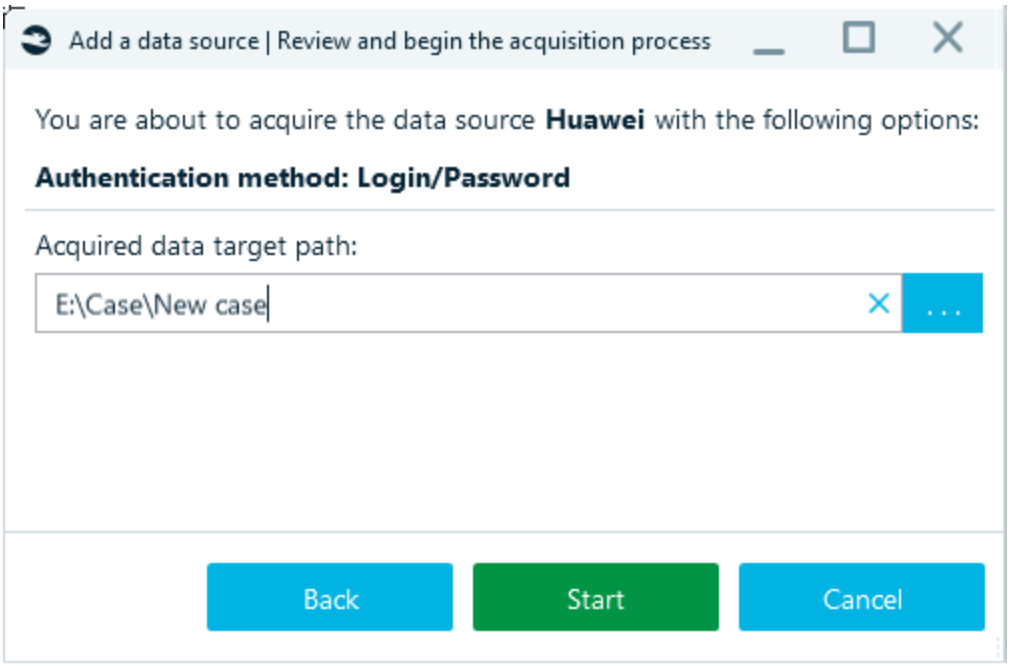




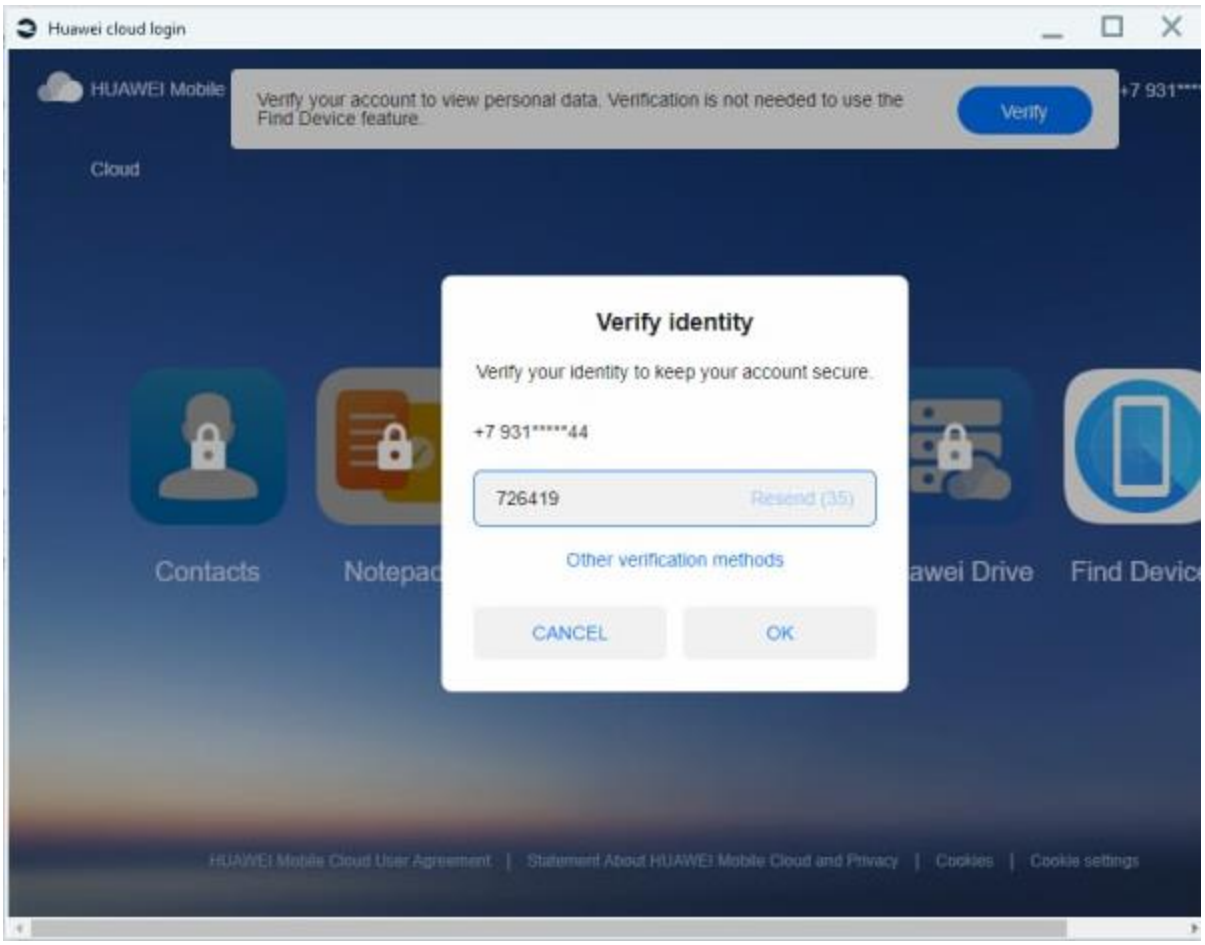
Huawei

This functionality allows you to download Huawei cloud data.
Enter credentials for Huawei Cloud and specify target folder:





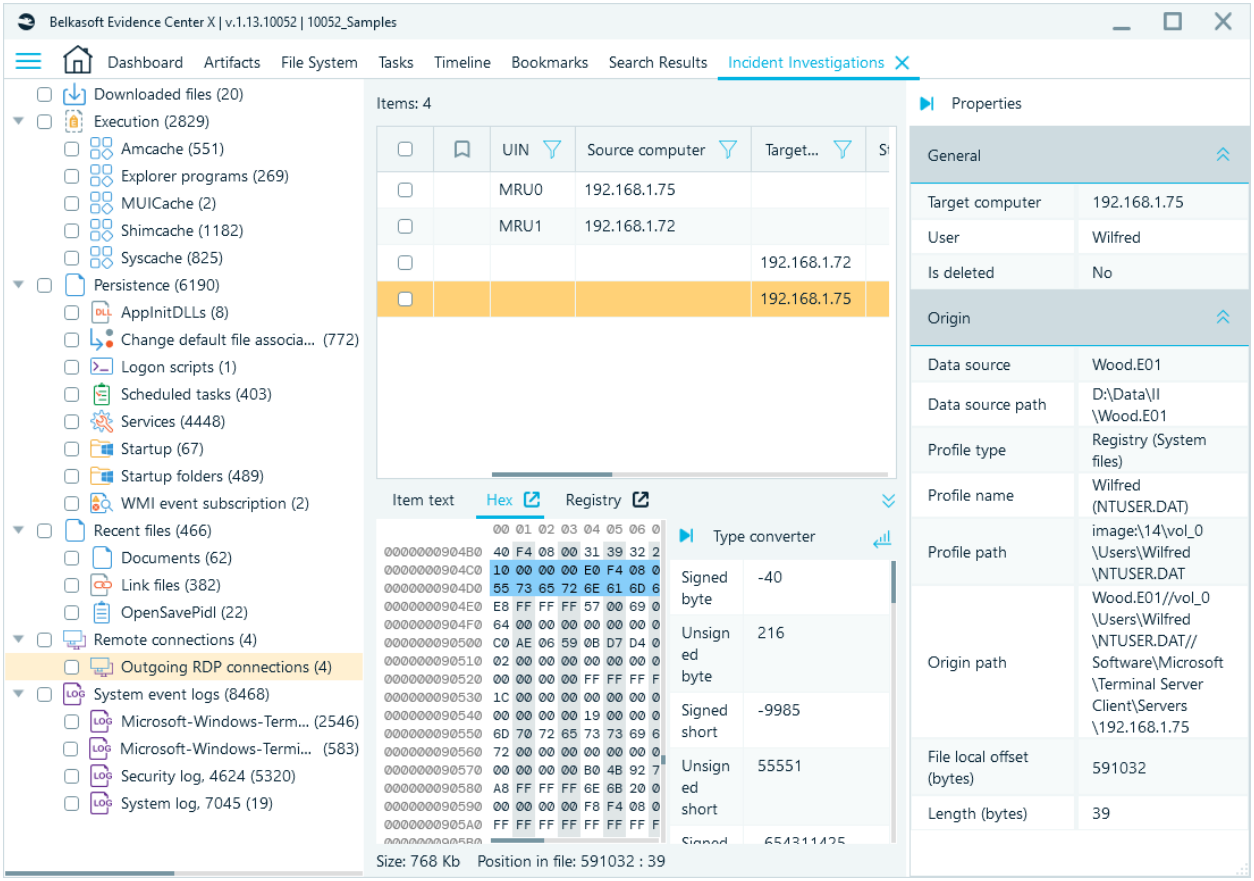
Then enter the code from the device:



After the data is downloaded, you can start the analysis.

Incident Investigation

Outgoing RDP connections



Outgoing RDP values are extracted from registry key HKEY_USERS\...\SOFTWARE\Microsoft\Terminal Server Client. Data is extracted for MRU keys (MRU – Most Recently Used).

Archives

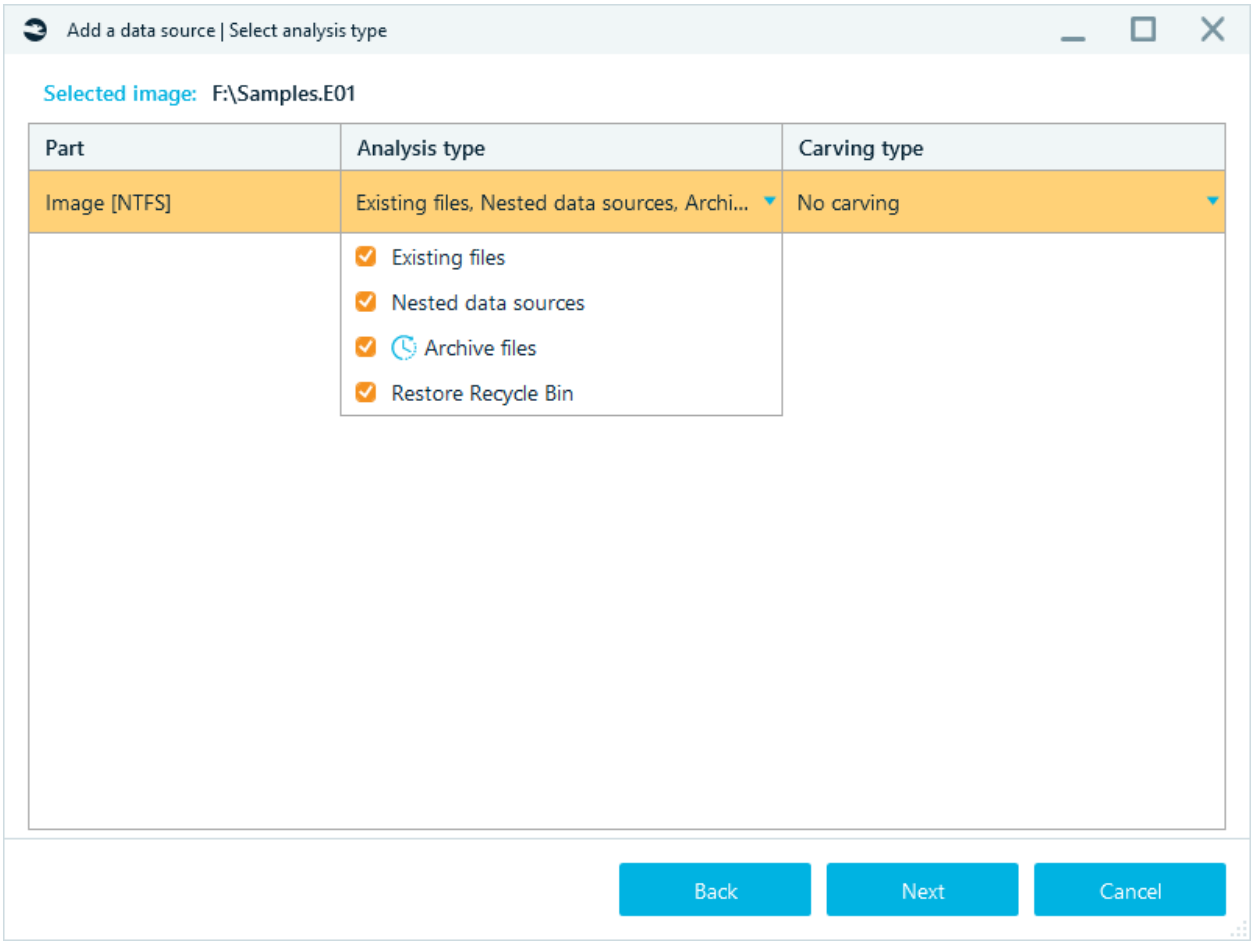
To extract data from the archives, select the appropriate item in Add data source window, hash counting is also configured there.
There are two options to analyze archives in Belkasoft X:

- Standard archive analysis. Performed when the archive of interest is added directly as an Image data source. Standard analysis extracts and analyzes data only within the first nesting level of an archive.
- Advanced **Archive files** analysis. This method extracts and analyzes archives up to the second nesting level of the data source. It searches for nested archives in added data sources.

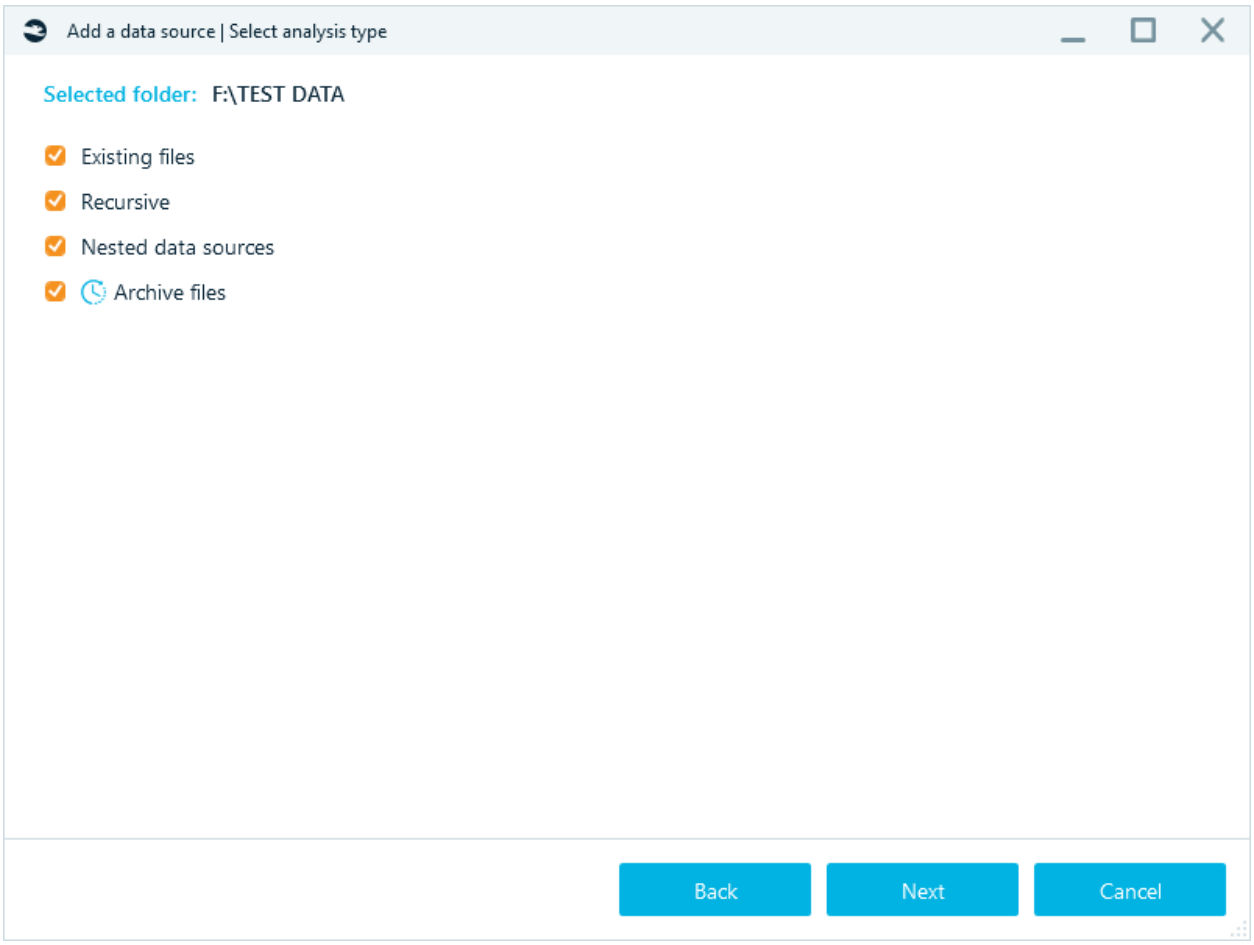
These two methods can be combined–one may add an archive containing other archives as an Image data source and turn on the Archive file analysis option–the archives located inside the first level archive will be extracted and analyzed.

Advanced **Archive files** analysis can be switched on in the **Select analysis type** page of the **Add a data source** window. This page looks different for different types of data sources.

For Images and Disk drives:

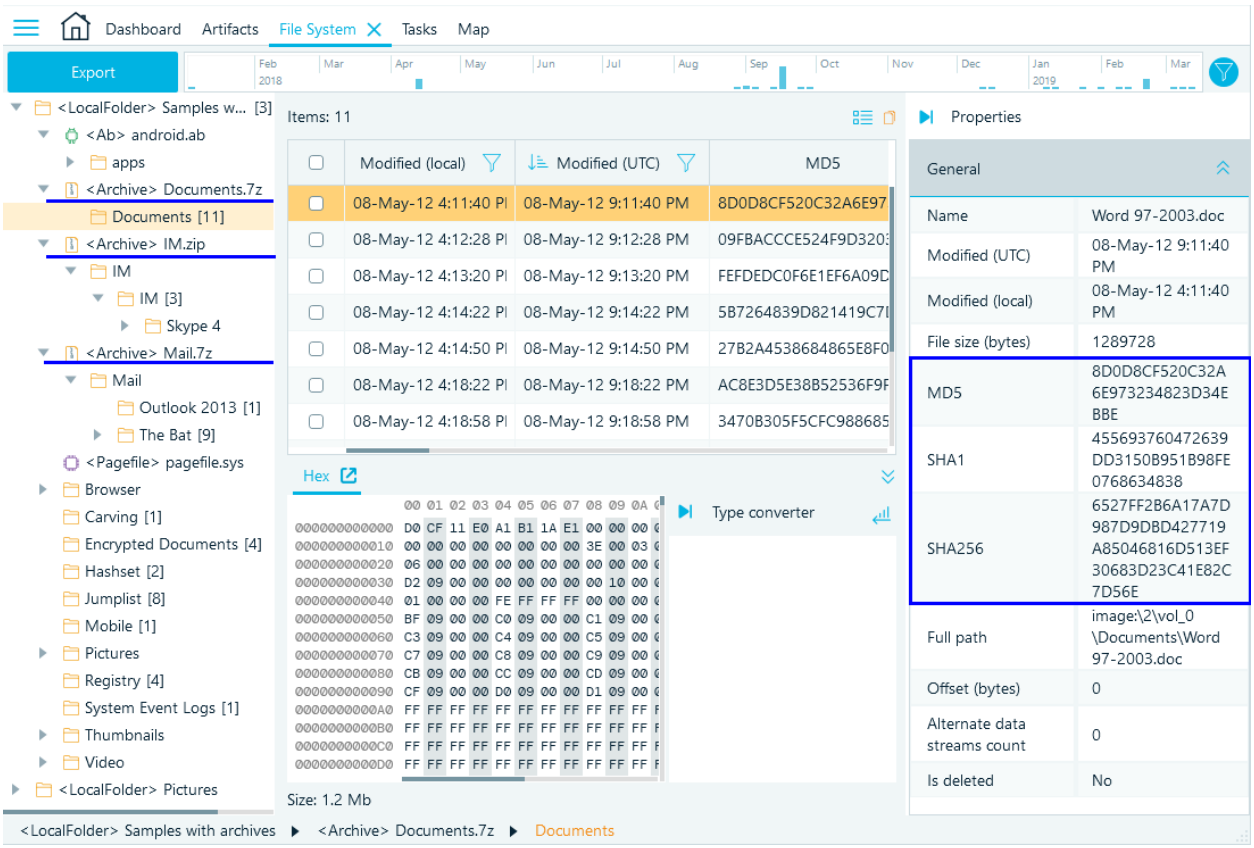


For Folders and Mobile images:



Please note that archive analysis is a time consuming process, that is why the **Archive files** option is unchecked by default. Use the **Archive files** option together with the **Nested data sources** checkbox.

In File System tab archives are shown as follows:



Export and import a Concordance eDiscovery load file

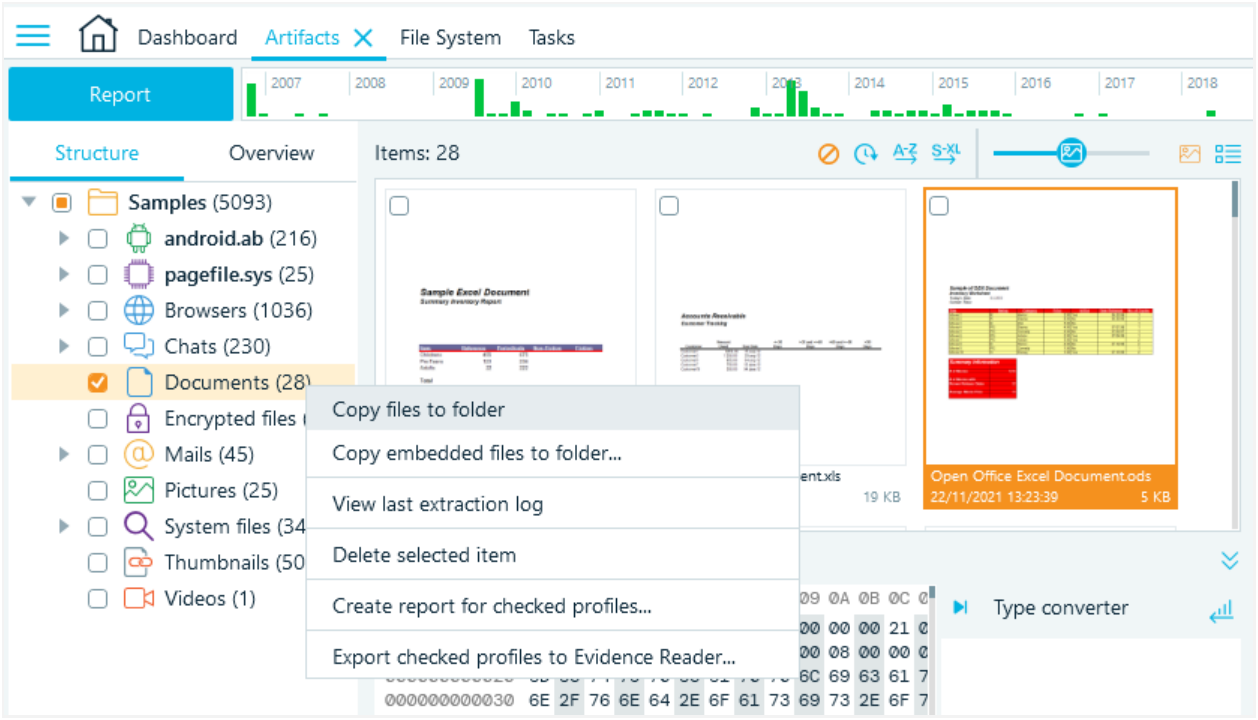
Concordance eDiscovery load file is used to import electronically stored data into the Concordance database. It is a delimited text file with .DAT file extension, which contains the metadata of the document and related OCR data for the record.

Belkasoft X supports both export to the load file and import from it.

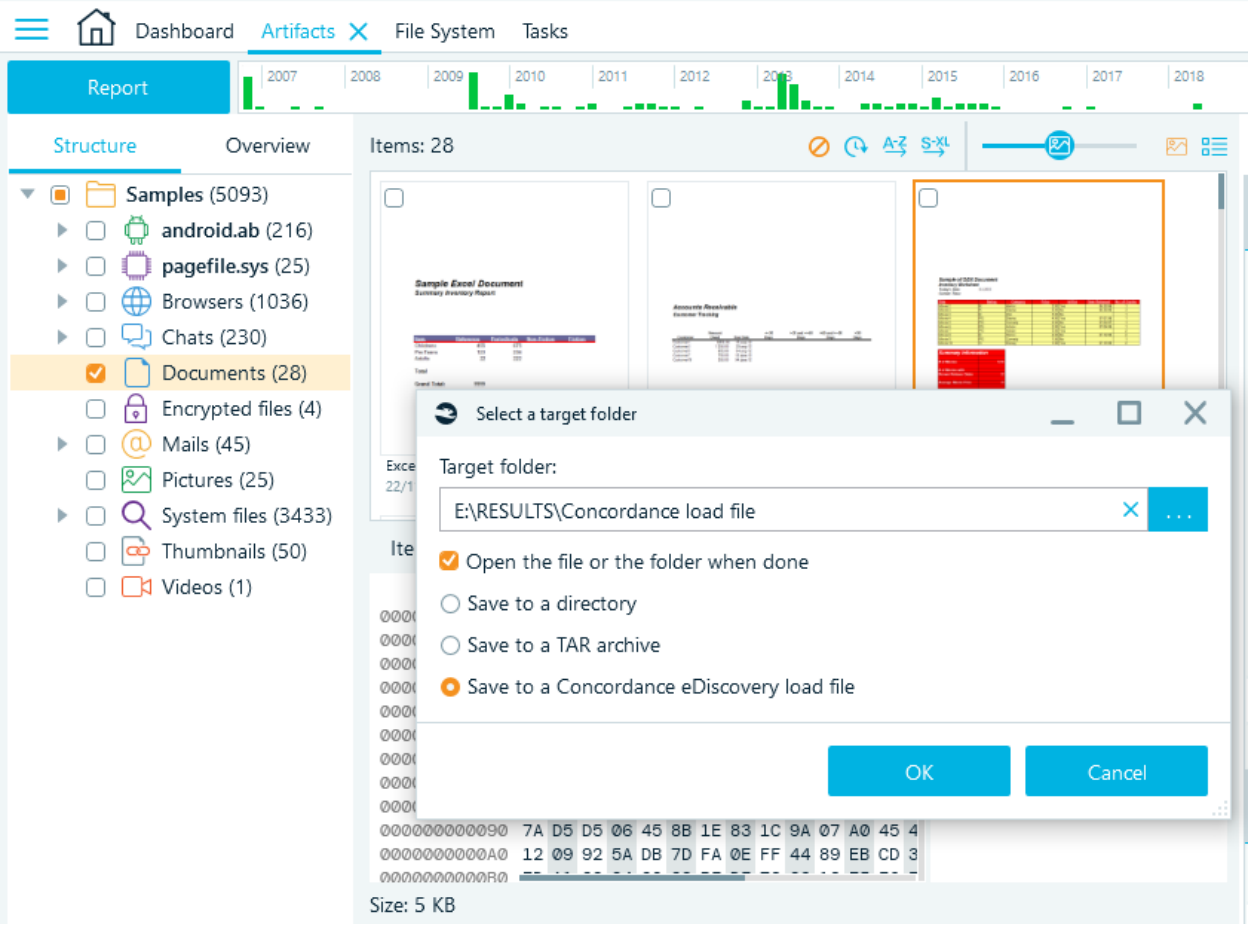
Export to load file is available from two tabs - **File system** and **Artifacts**.

Load file export from the Artifacts tab

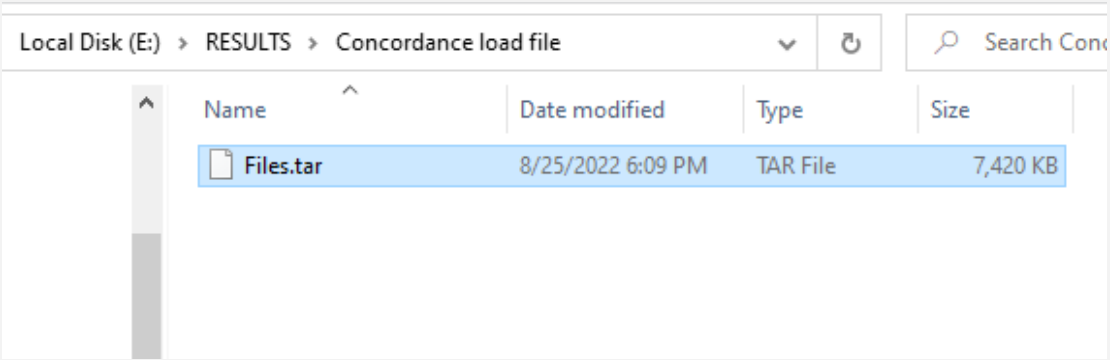
Go to the **Structure** pane in the **Artifacts** tab and check the files, which should be exported to load file. This can be done either in the Tree view or in the Grid/Gallery view. Right click the selection and choose **Copy files to folder** from a drop-down menu.



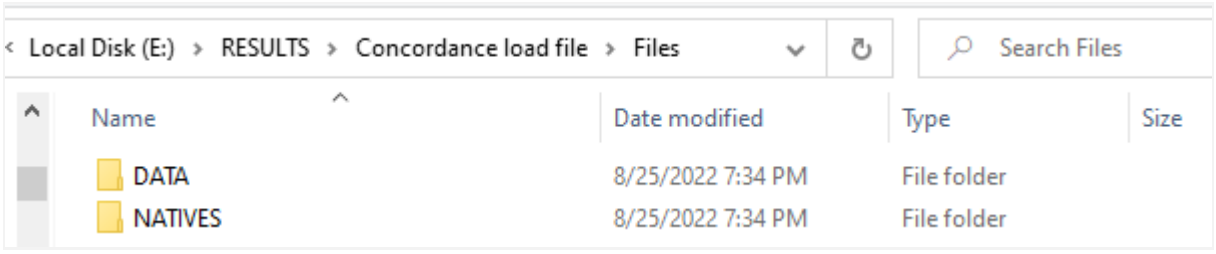
Choose **Save to a Concordance eDiscovery load file** and select a destination path in the **Select a target folder** window, click **OK**.



The resulting file is a **.TAR** archive containing two folders: DATA and NATIVES.



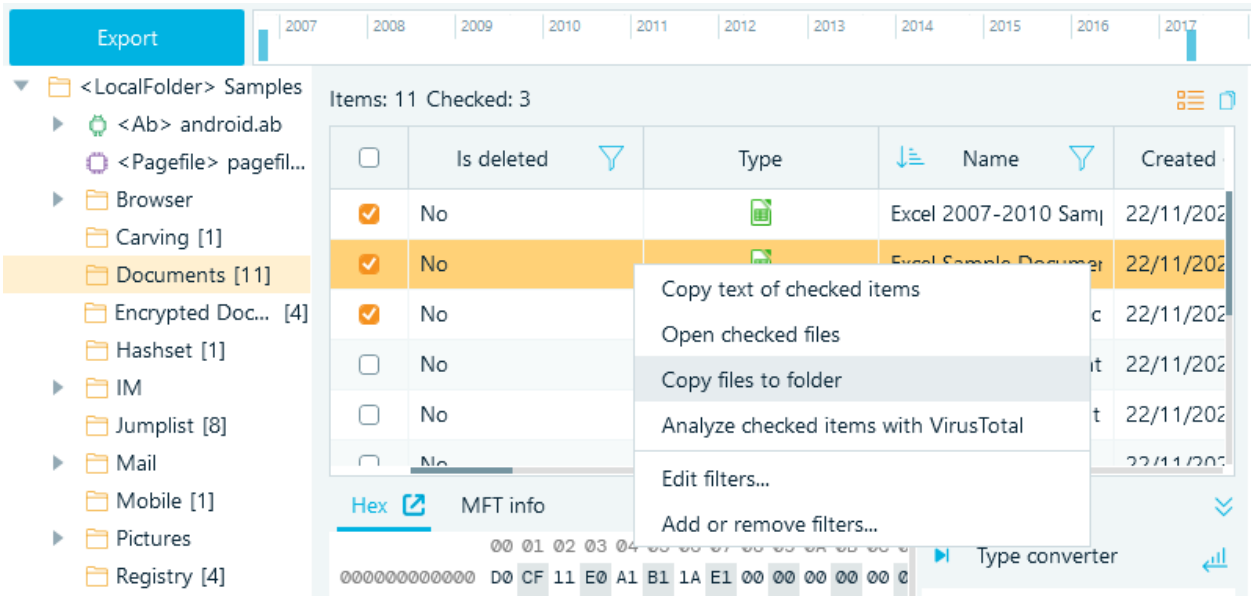
The DATA directory contains the **.DAT** file, which is used for import. The native files are exported in the NATIVE directory.



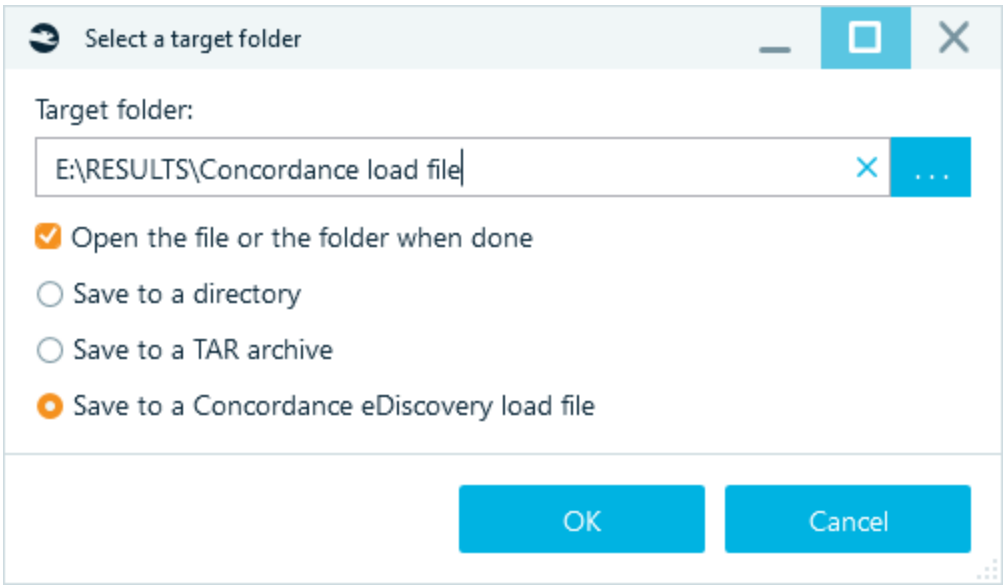
Export is available in the **Overview** pane of the **Artifacts** tab as well.

Load file export from the File system tab

Go to the File system tab. Pick the folder of interest or just check a number of files and right-click the selection. Choose **Copy files and folders recursively** or **Copy files to folder** for Tree and Grid views respectively.

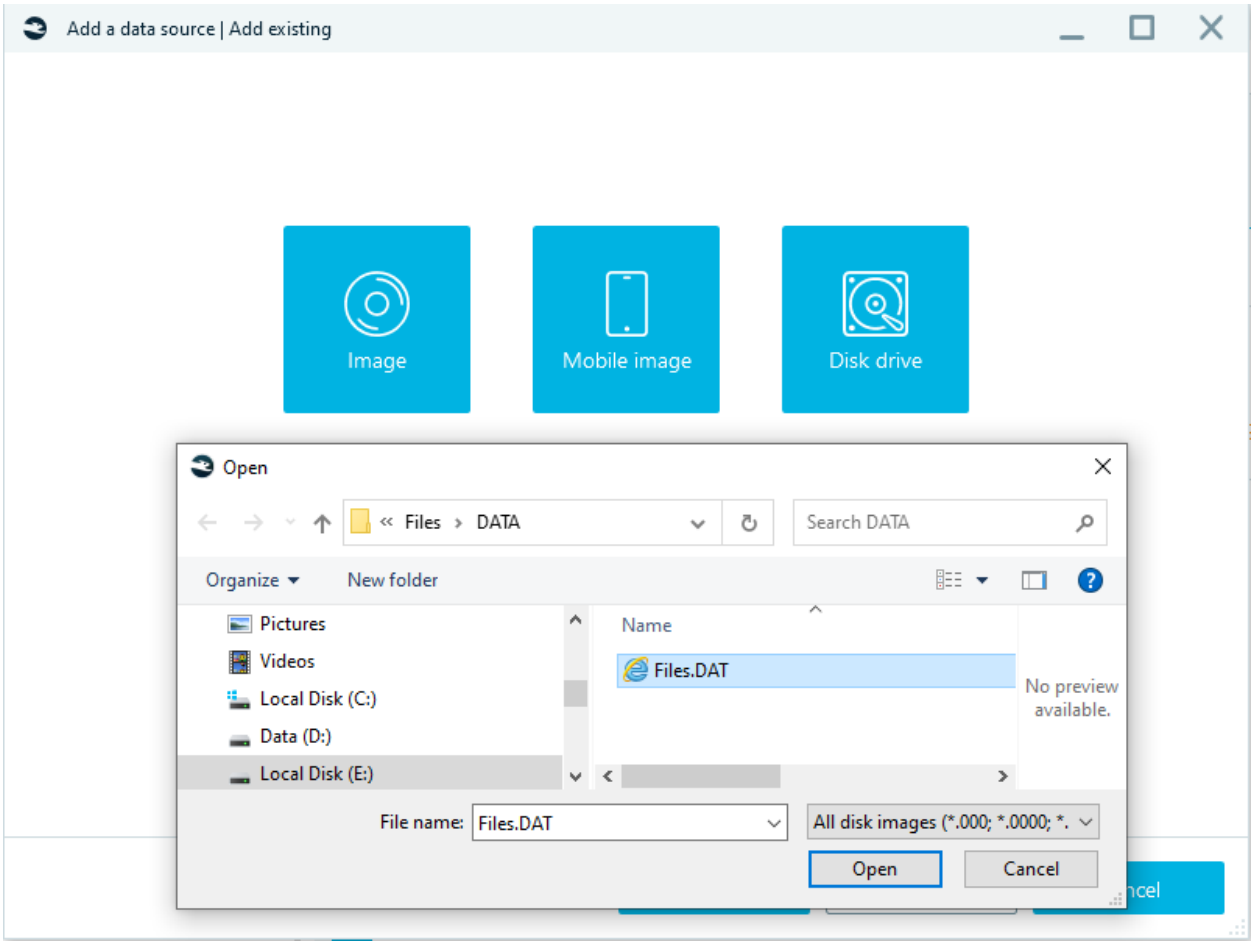


Indicate the target folder, select **Save to a Concordance eDiscovery file** and click **OK**.

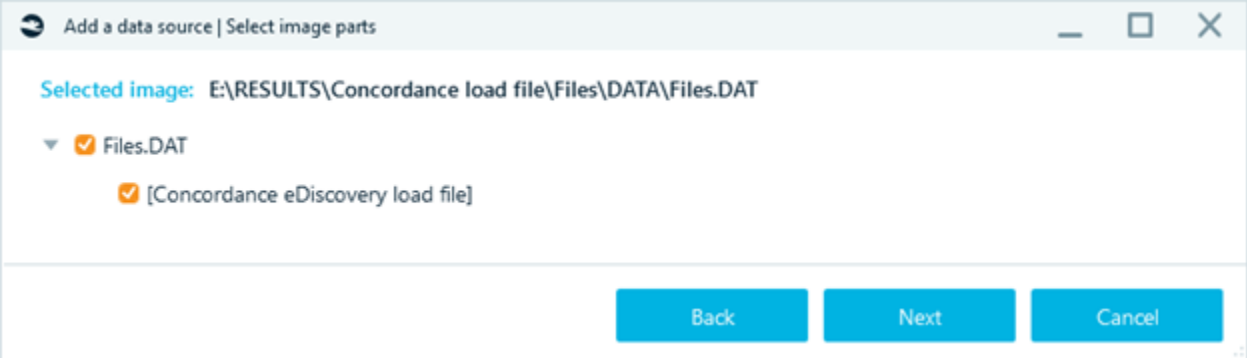


Import the load file

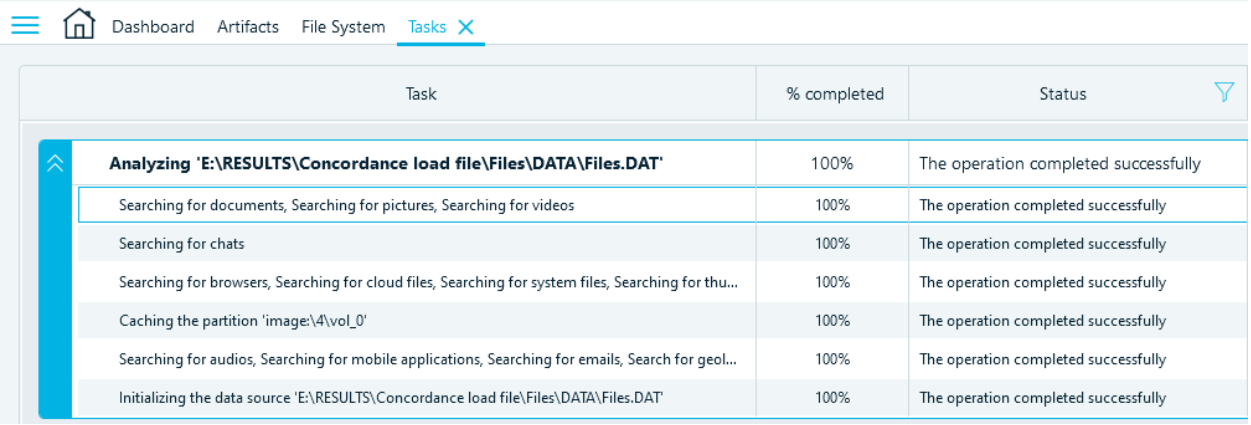
To import the **Concordance load file** created by Belkasoft X or a third party tool, simply add it as a data source: Dashboard - Add existing - Image - browse to the Concordance **.DAT** file.



Click **Next**, then analyze the **.DAT** file as a regular data source.

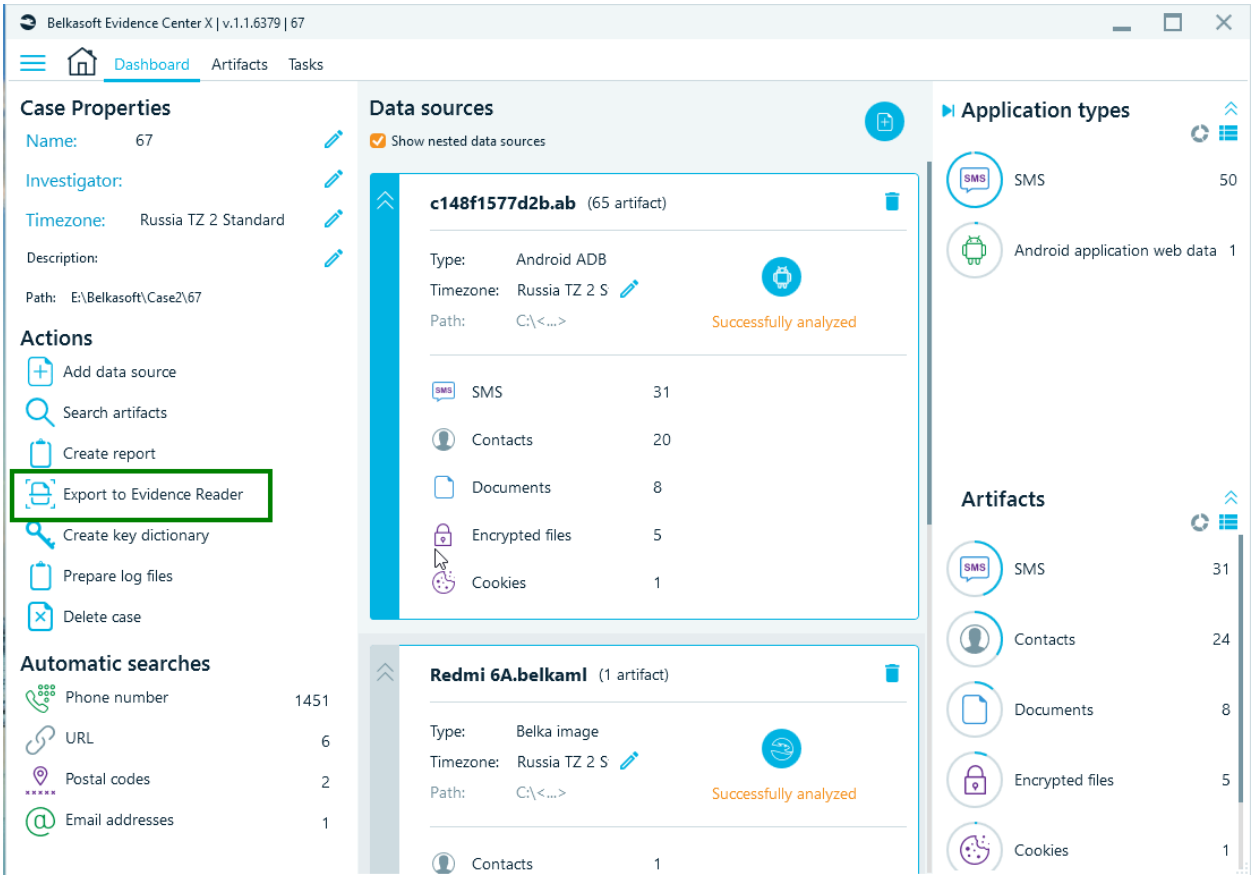


Keep track of the analysis progress in the **Tasks** tab.



Export to Evidence Reader

Export to Evidence Reader function allows you to share all your findings with anyone with a PC, even if they do not have a paid Belkasoft Evidence Center X license. Evidence Reader is a free product, which helps a user to review cases or their parts exported from Belkasoft X.

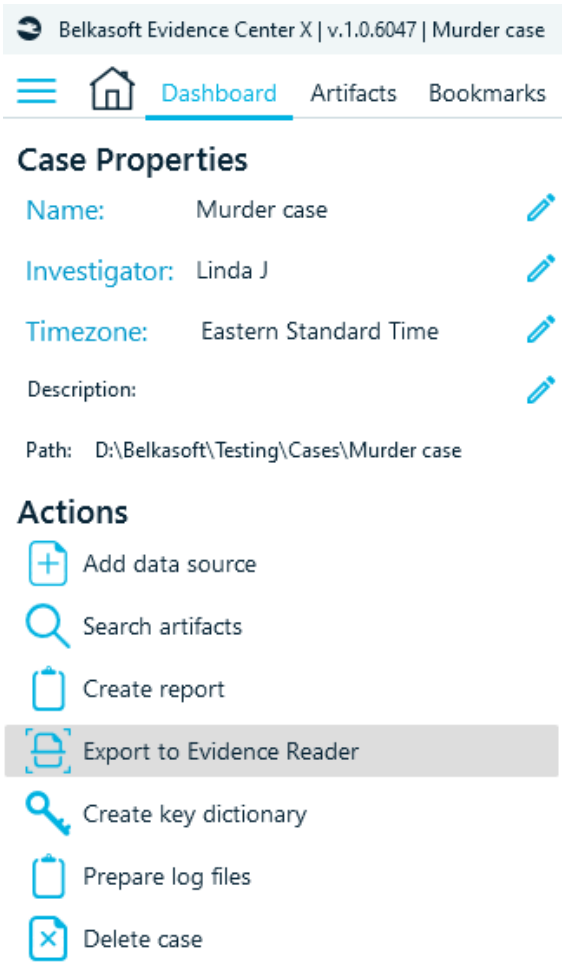


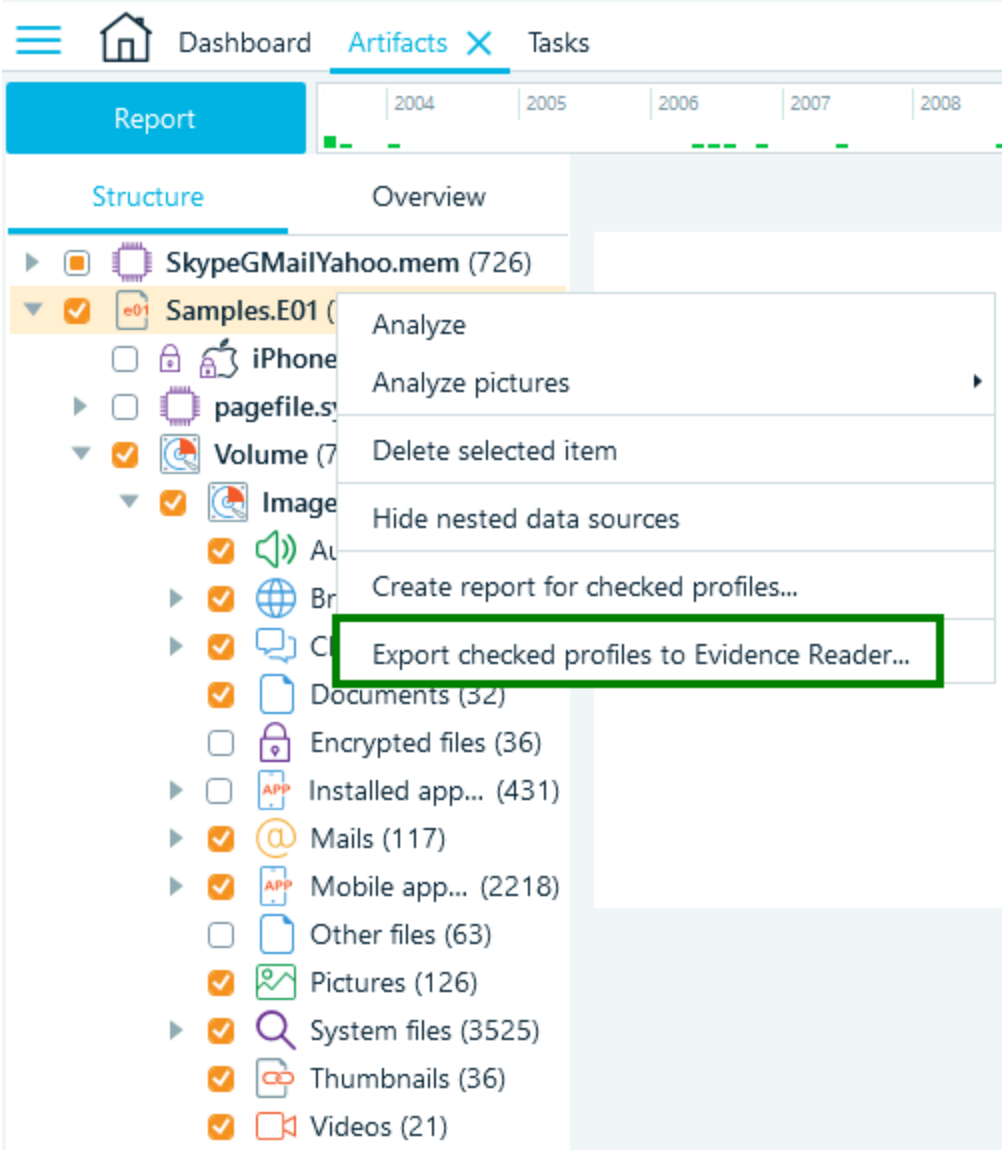
Evidence Reader works in read-only mode, is portable, does not require any installation. And is particularly useful for splitting work on a case. Apart from splitting work among several investigators, Evidence Reader helps you with long-running cases. Consider this, if you would like to make sure that your case database is read without flaws in a year or more from the day it was created, export your case to Evidence Reader. Since Belkasoft X is evolving quickly, in a year or two, an older case may become unreadable by a newer versions of Belkasoft X. At that point, the best way to open such case would be to use Evidence Reader created at the time as export to Reader was performed.

Exporting data to Evidence Reader

There are two ways to export case data to Evidence Reader:

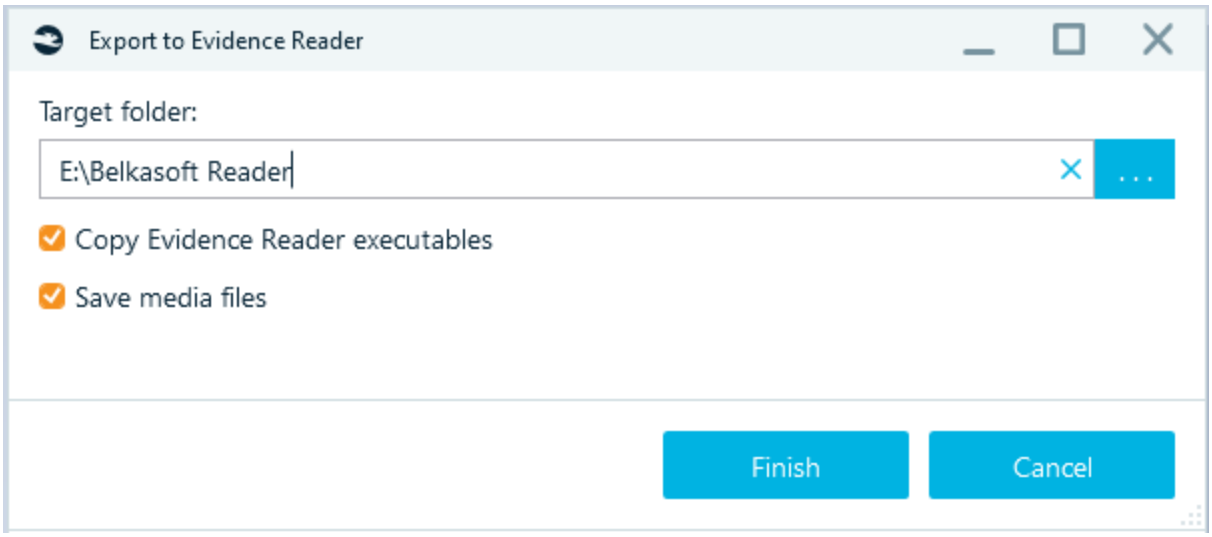
- if you want to export all profiles, then go to **Dashboard** window and select **Export to Evidence Reader** item from the **Actions** list
- if you want to export the selected data sources and profiles, then go to **Artifacts** window Structure view, open drop-down menu and select **Export checked profiles to Evidence Reader**


Belkasoft Evidence Center X | v.1.0.6047 | Murder case
Dashboard
Artifacts
Bookmarks
Case Properties
Name:
Murder case
Investigator:
Linda J
Timezone:
Eastern Standard Time
Description:
Path:
D:\Belkasoft\Testing\Cases\Murder case
Actions
Add data source
Search artifacts
Create report
Export to Evidence Reader
Create key dictionary
Prepare log files
Delete case



On the next screen of the export process, you will be asked for a target path for output files. Here you can also choose to **Copy Evidence Reader executables** to the target folder and to **Save media files**.

- **Copy Evidence Reader executables.** If you export Reader multiple times, you may decide not to include it to every folder and only do this for the first time. This helps you to save disk space and time spent for exporting.
- **Save media files.** This option saves all media (pictures, videos, etc.) from the original case to the Evidence reader, so that media files can be examined even when the original data source is disconnected.



Click on the **Finish** button and wait until the task is completed. Inside the target folder, you will find a subfolder with the case name, which contains all needed files. You can copy all the subfolder contents and give to another user.

Reconnect Amazon S3

To reattach an **Amazon S3** data source after the case was exported to the **Evidence reader**, one will need to enter Amazon credentials once again (more details about this are described in the corresponding section).

Why can't I export data to Evidence Reader?

If **Export to Evidence Reader** button or menu item is greyed out, this means that your SMS plan is expired. It is not allowed to create Evidence Reader cases after the support expiration, so please renew your SMS plan.
In addition, trial version of Belkasoft X and Academic version of Belkasoft X does not allow exporting data to Evidence Reader.

Evidence Reader limitations

Reader has an interface similar to Belkasoft X, but a bit more simplified. Particularly, you will not be able to

- create a case
- acquire data
- add or delete data sources
- analyze or re-analyze a data source
- check for malware
- do hashset analysis
- extract keyframes from videos
- analyze pictures
- and so on

However, you will be able to:

- Do searches
- Run reports
- Create, edit, and delete bookmarks

It also has different color scheme to help distinguishing Evidence Reader from Belkasoft X: