



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

BELKASOFT TRIAGE USER REFERENCE

Contents

[Contents](#)

[About](#)

[Technical characteristics](#)

[Legal notes and disclaimers](#)

[Quick start](#)

[Step 1: RAM acquisition](#)

[Step 2: Scanning device](#)

[Detecting Hashes and Skin](#)

[Detecting nested data sources](#)

[Step 3: Export Results](#)

[Belkasoft T support](#)

About

Belkasoft Triage (or, for short, **Belkasoft T**) is a new digital forensic and incident response tool developed specifically for a quick triage of a live computer and making a partial image of important data. **Belkasoft T** is designed to be launched when an investigator or a first responder is right on the crime scene and needs to obtain specific digital evidence to **speed up** the investigative process.

Technical characteristics

Belkasoft T is preinstalled on a dongle which has a certain amount of the flash memory. This dongle uses a USB port, versions 2.0 and 3.0. Triage can be launched on computers and laptops under 64- and 32-bit Windows operating systems (Windows 10, 8 and 7 are supported). Belkasoft T can be also launched on virtual machines provided that it's usb-dongle is hooked.

Legal notes and disclaimers

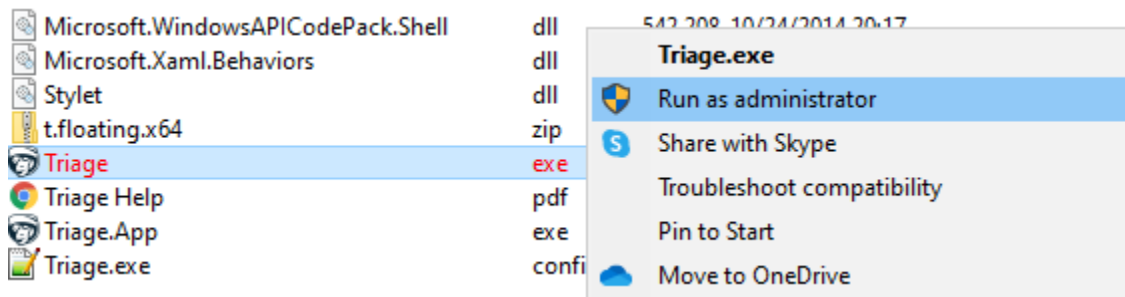
TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, IN NO EVENT SHALL BELKASOFT OR ITS SUPPLIERS BE LIABLE FOR ANY DIRECT, SPECIAL, INCIDENTAL, INDIRECT, PUNITIVE, CONSEQUENTIAL OR OTHER DAMAGES WHATSOEVER (INCLUDING, BUT NOT LIMITED TO, DAMAGES FOR: LOSS OF PROFITS, LOSS OF CONFIDENTIAL OR OTHER INFORMATION, BUSINESS INTERRUPTION, PERSONAL INJURY, LOSS OF PRIVACY, FAILURE TO MEET ANY DUTY (INCLUDING OF GOOD FAITH OR OF REASONABLE CARE), NEGLIGENCE, AND ANY OTHER PECUNIARY OR OTHER LOSS WHATSOEVER) ARISING OUT OF OR IN ANY WAY RELATED TO THE USE OF OR INABILITY TO USE THE SOFTWARE, THIS REFERENCE DOCUMENT OR SUPPORT SERVICES, THE PROVISION OF OR FAILURE TO PROVIDE SUPPORT SERVICES, OR OTHERWISE UNDER OR IN CONNECTION WITH ANY PROVISION OF THIS DOCUMENT, EVEN IN THE EVENT OF THE FAULT, TORT (INCLUDING NEGLIGENCE), STRICT LIABILITY, BREACH OF CONTRACT OR BREACH OF WARRANTY OF BELKASOFT OR ANY SUPPLIER, AND EVEN IF BELKASOFT OR ANY SUPPLIER HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Quick start

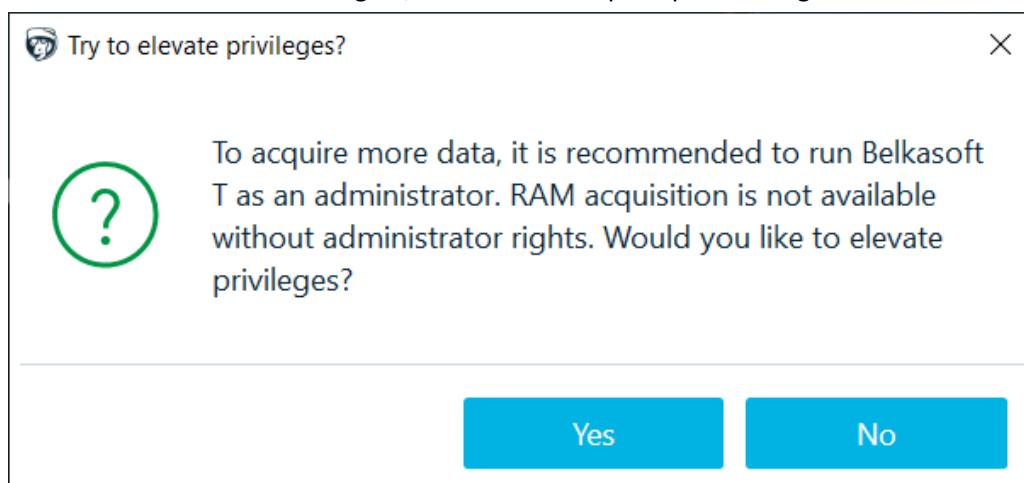
Insert the dongle into the scanned computer and run the **Triage.exe** file - the product is ready to work. No installation required. Easy-to-use.

Three options to launch **Belkasoft T**:

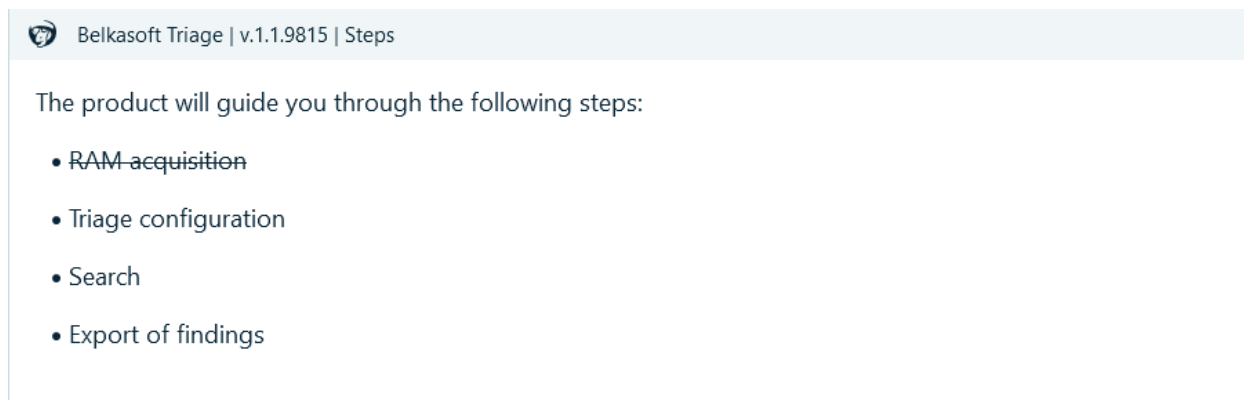
1. Run **Belkasoft T** as administrator, it allows to acquire RAM and collect all detected profiles



2. Run without administration rights, **Belkasoft T** will prompt about rights elevation.



If it is impossible to elevate the rights, the user will not be able to acquire the RAM and perhaps some of the profiles will not be collected

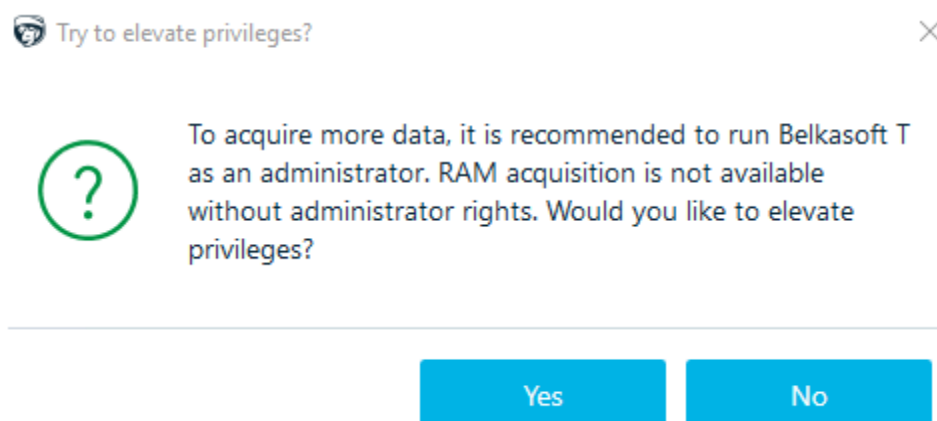


3. **Belkasoft T** allows rights elevation based on Windows Win32k Elevation of Privilege Vulnerability. It allows users to elevate the rights and use the product as administrator.

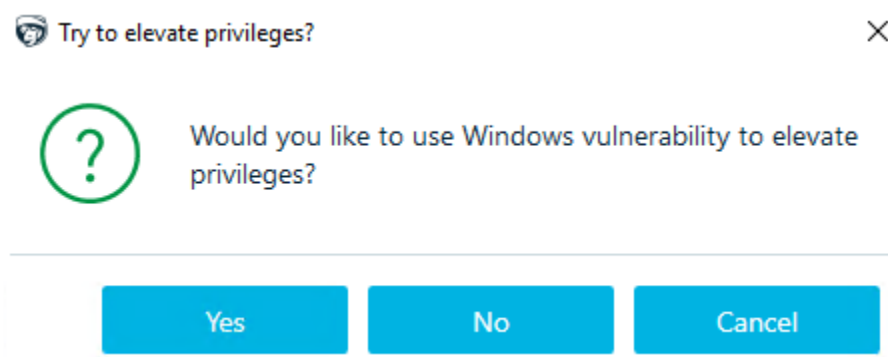
The list of vulnerable operational systems:

- Windows 10 1803: all builds up to 17134.1967 (included), before the update on 02-09-2021;
- Windows 10 1809: all builds up to 17763.1728 (included), before the update on 02-09-2021;
- Windows 10 1903: all builds;
- Windows 10 1909: all builds up to 18363.1350 (included), before the update on 02-09-2021;
- Windows 10 2004: all builds up to 19041.789 (included), before the update on 02-09-2021;
- Windows 10 20H2: all builds up to 19042.789 (included), before the update on 02-09-2021.

In order to use the vulnerability, launch **Triage.exe**. Click **Yes** when offered to elevate privileges.



If OS is vulnerable to the privilege elevation exploit, the following window will be displayed next:

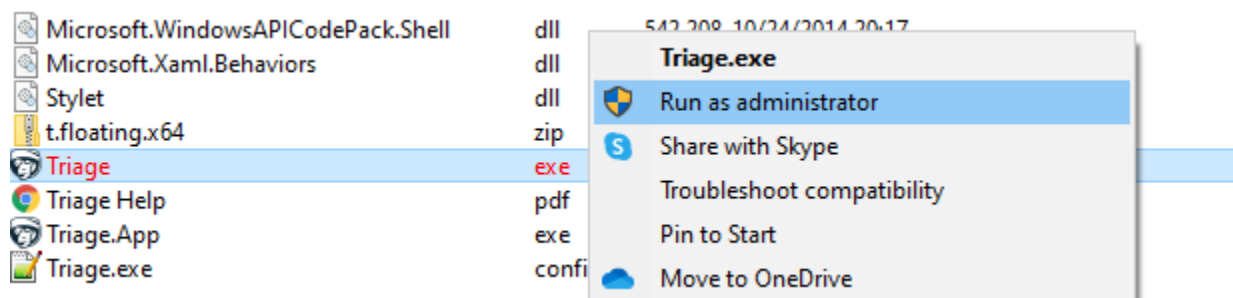


Click **Yes** and Belkasoft T will be launched with the elevated privileges.

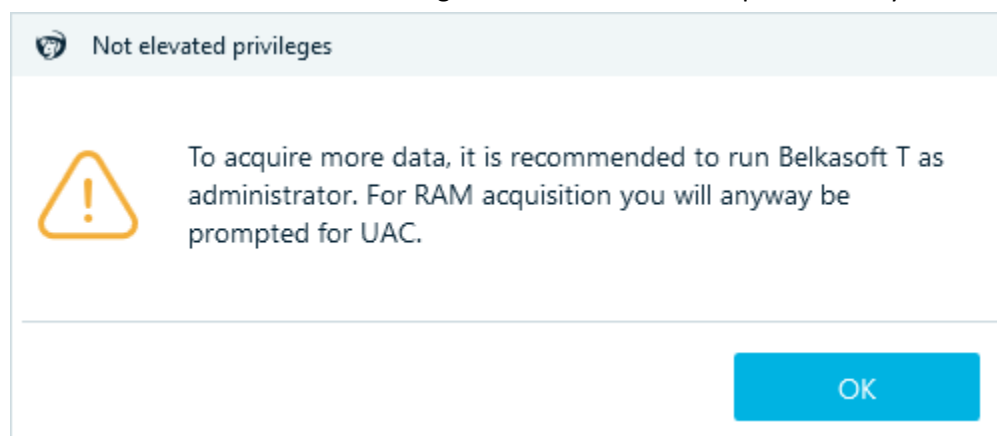
Step 1: RAM acquisition

Acquiring a memory dump is the first thing to do before the found device will be turned off.

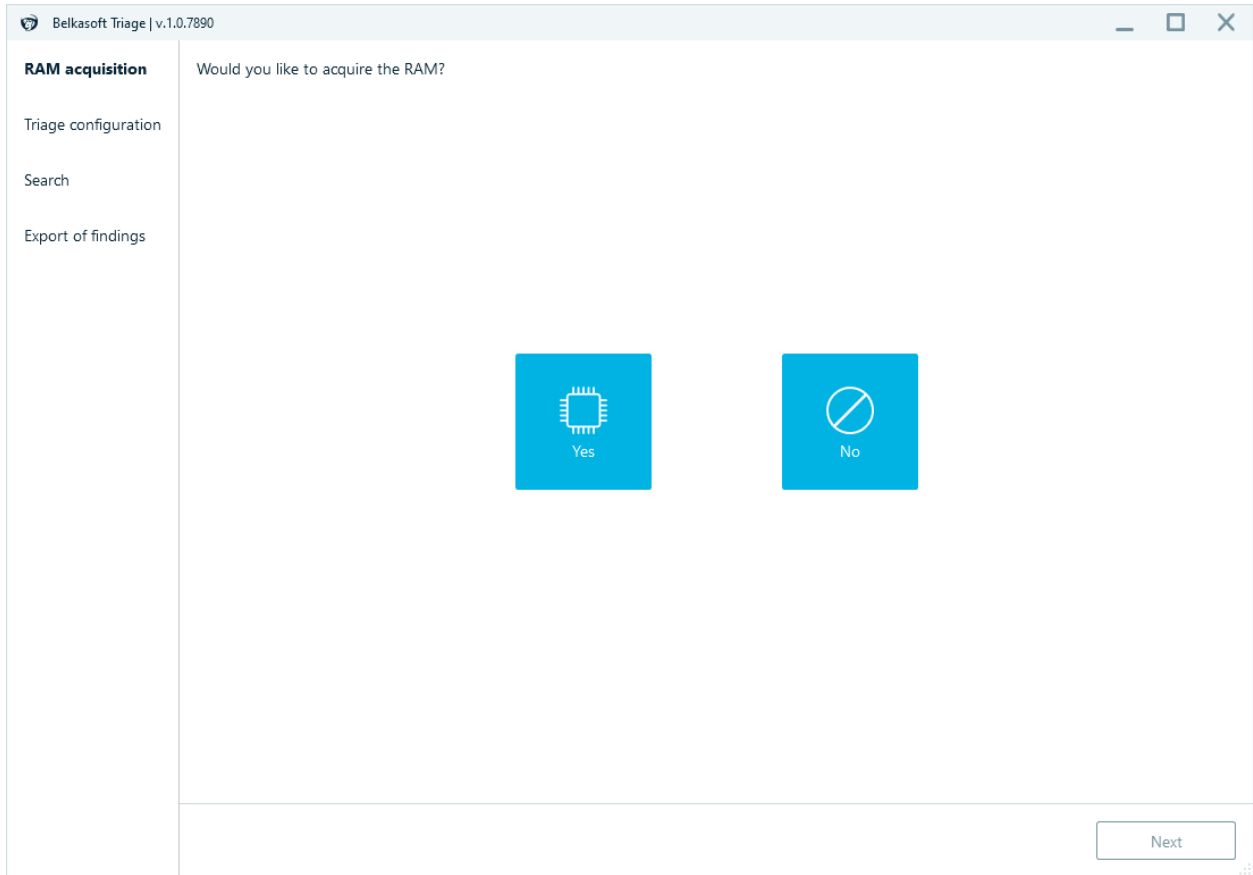
Please note that a memory dump can only be acquired by a user with administrator rights. If you need this option, run Belkasoft T as administrator from the context menu.



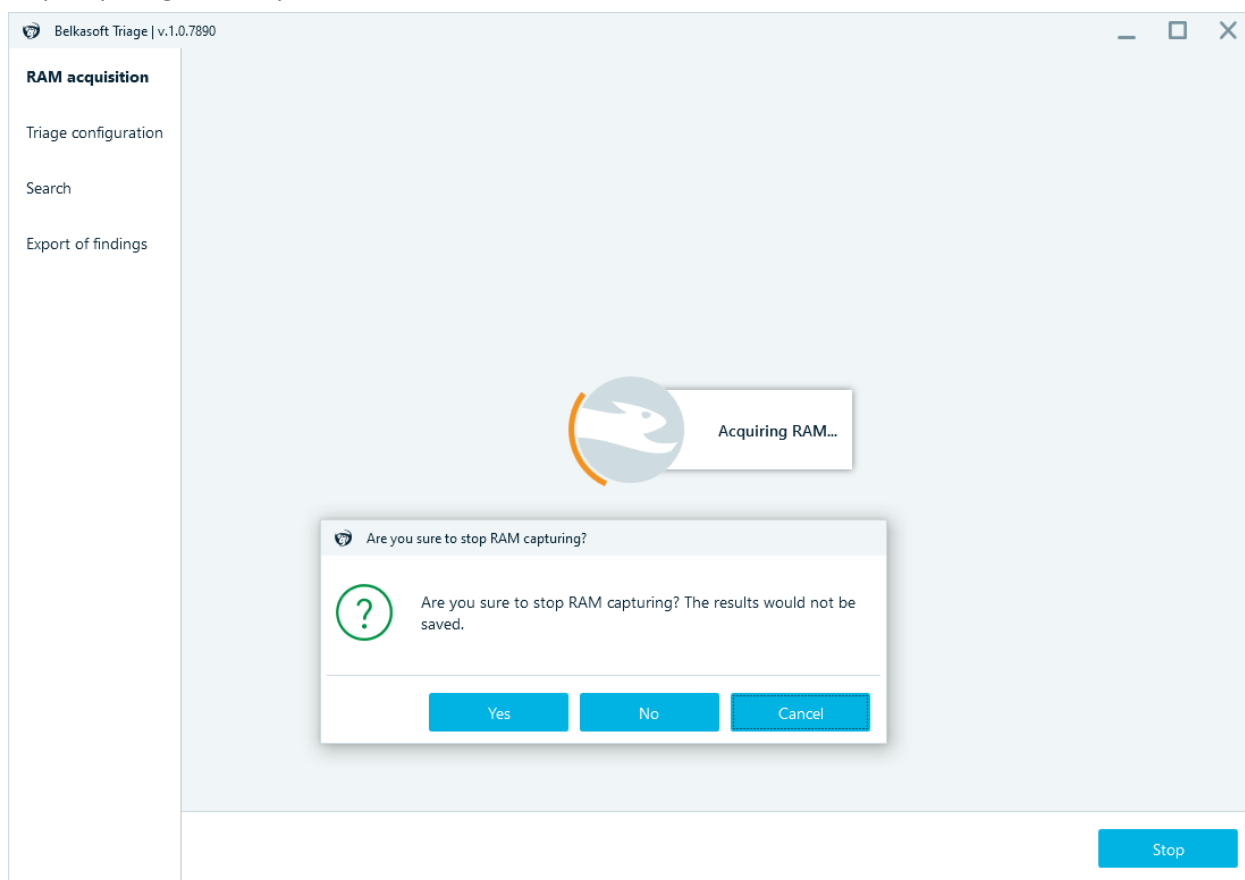
Belkasoft T without administrative rights does not allow to acquire memory.



If the memory dump has already been collected, just skip this step. If not, press **YES**, select the folder for saving images and start RAM acquisition.

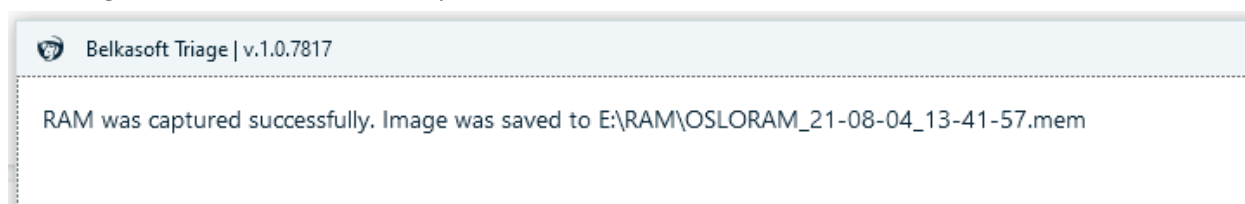


Stop acquiring RAM any time

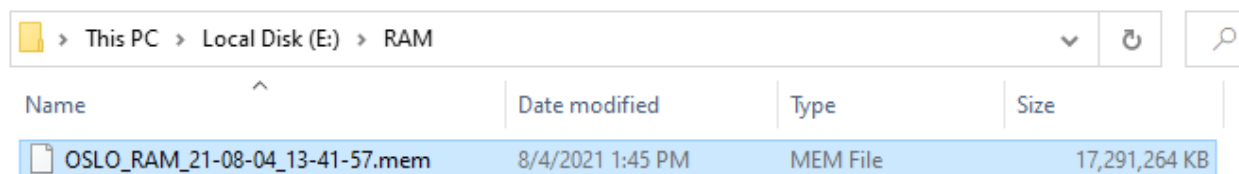


By default the RAM dump will be placed on the dongle's flash card or one can choose any other storage location, both within the investigated computer or on a removable drive. Copy it to another computer for the analysis.

A message about the successful completion:

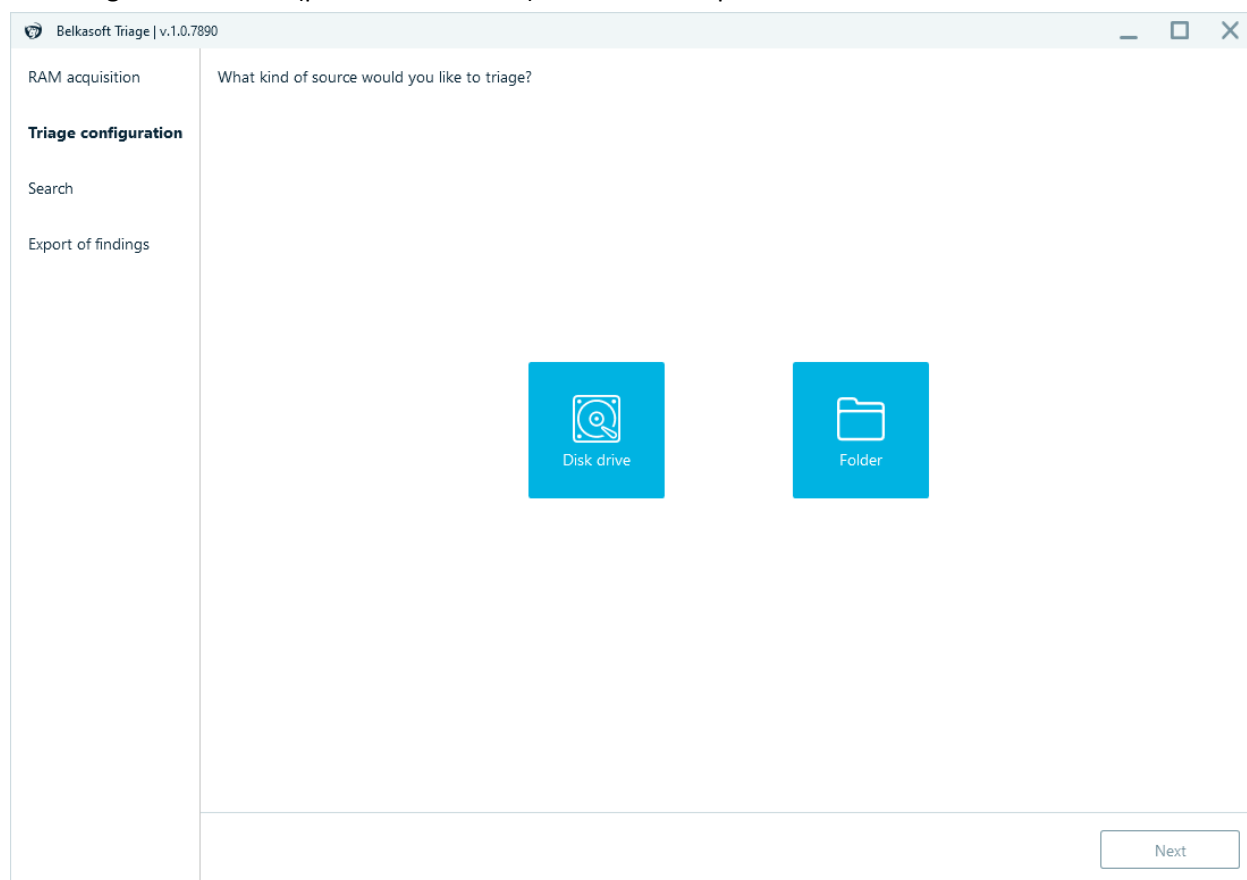


Memory dumps are acquired as .mem files:

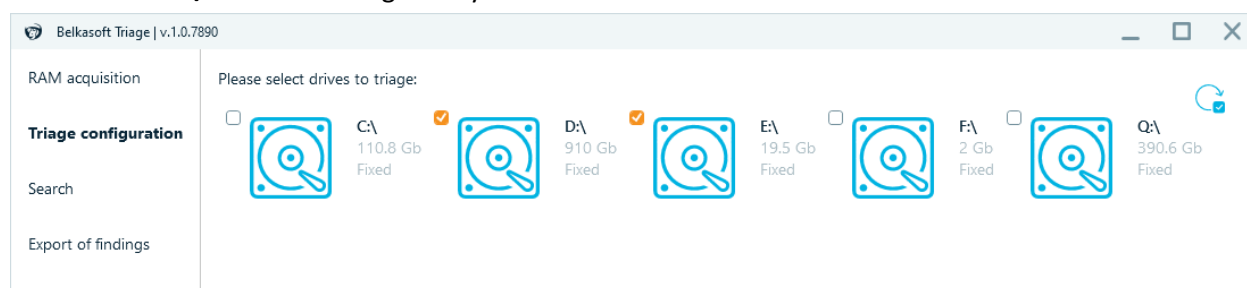


Step 2: Scanning device

Select logical **Disk Drive** (pick one or several) or **Folder** to explore.



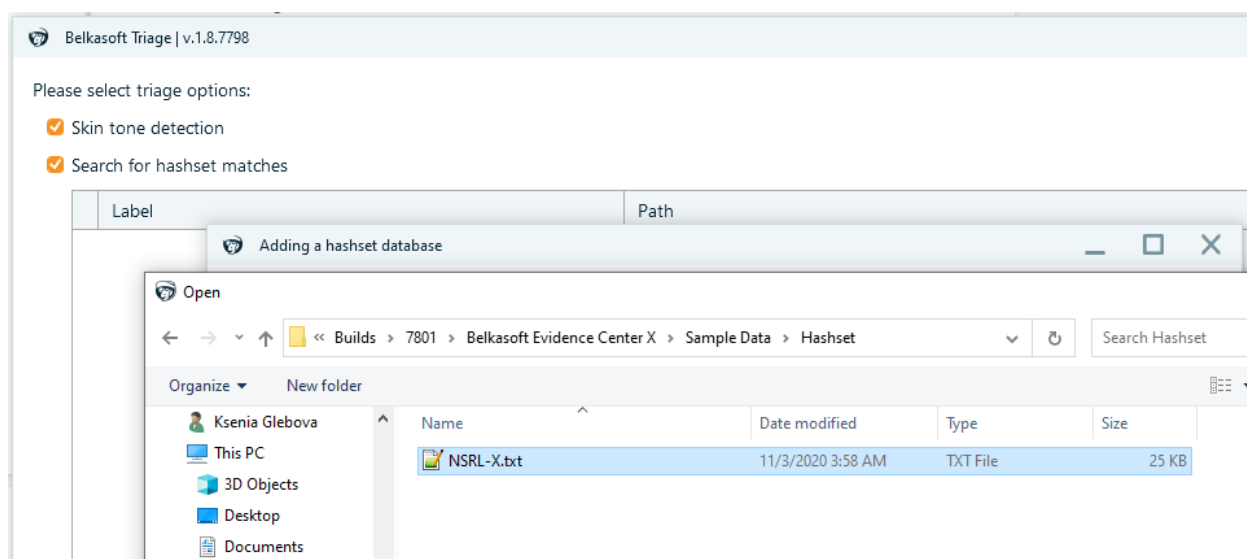
Check the **Drive/Drivers** for triage-analysis or choose the **Folder**.



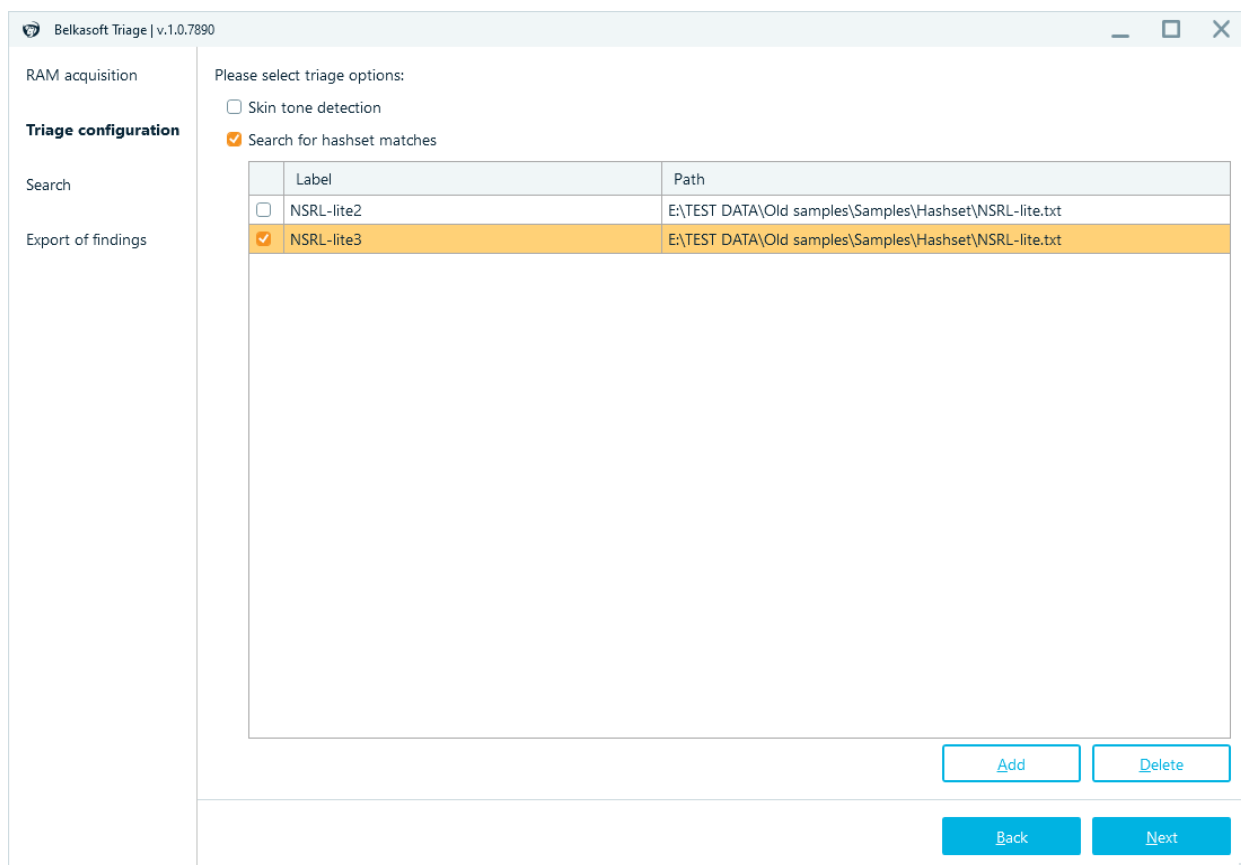
Set the additional options:

- Skin tone detection (Note, this operation can take a long time if there are a lot of pictures on the device)
- Search for hashset matches

If you have a hashset file or a database, click on the **Add** button to browse for it.



In order to delete the previously added hashset database, check its checkbox and click on the **Delete** button. Only checked lines will be deleted.



Please note - Hashset databases could be huge and their attachment may take a while. To save time on a scene, it's always better to link hashset databases in advance. The database will be converted and stored in Triage\HashSets\<hashset database label> upon a click on the 'Next' button of the **Triage configuration** page.

Check analysis options on the review page and **Start** the triage analysis.

| Belkasoft Triage v.1.0.7890 | |
|-------------------------------|--|
| RAM acquisition | |
| Triage configuration | <p>Selected type of source: Disk</p> <p>Selected disks for triage: D:\, E:\</p> <p>Is skin detection selected: Yes</p> <p>Is hashset matching detected: Yes</p> <p>Selected hashset databases: NSRL-X</p> |
| Search | |
| Export of findings | |

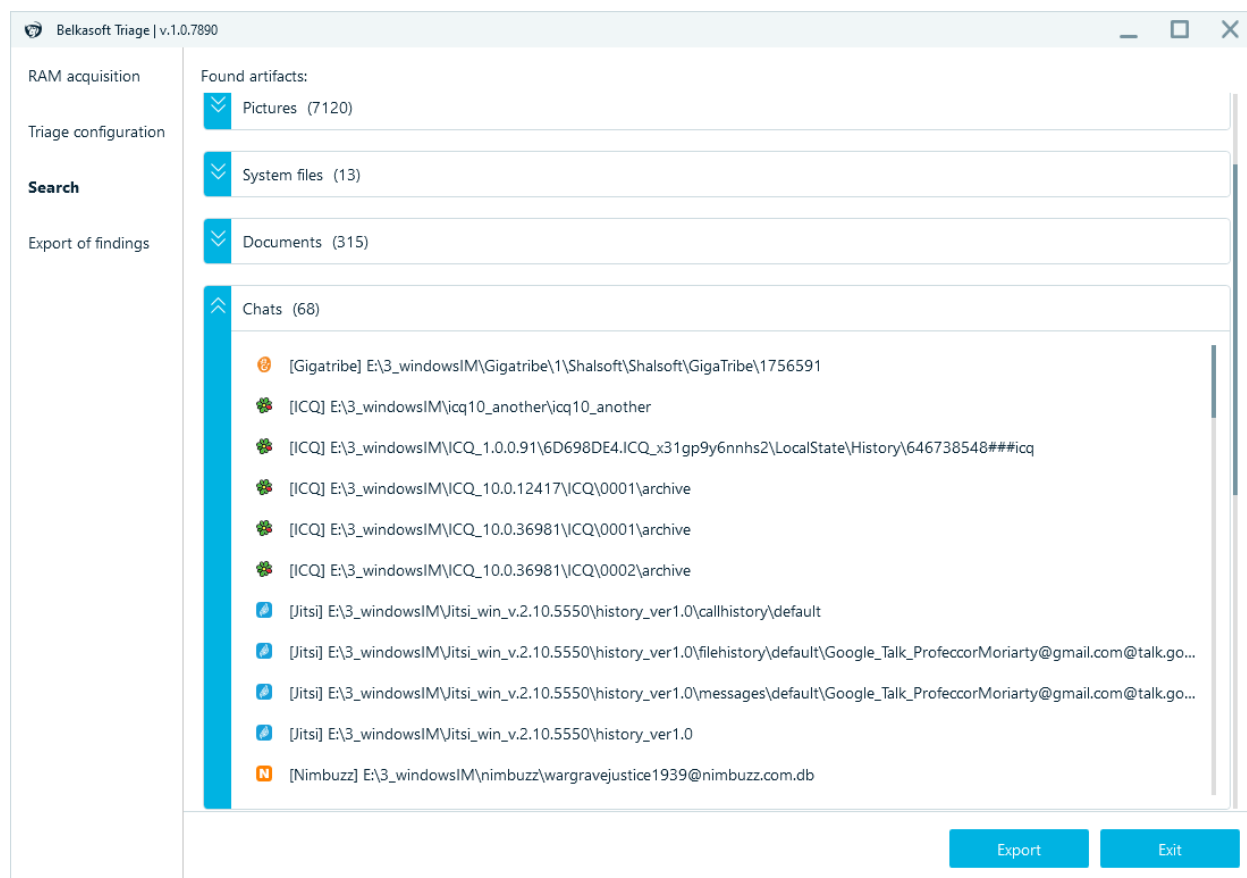
Stop the analysis at any time as soon as the required profile/data is detected.

| System event log (2) | |
|----------------------|--|
| | D:\Builds\5023x86\Belkasoft Evidence Center\Samples\System Event Logs\Setup.evtx |
| | D:\Builds\9800.4977\Belkasoft Evidence Center x64\Samples\System Event Logs\Setup.evtx |

| Videos (221) | |
|--------------|--|
|--------------|--|

Stop Search Exit

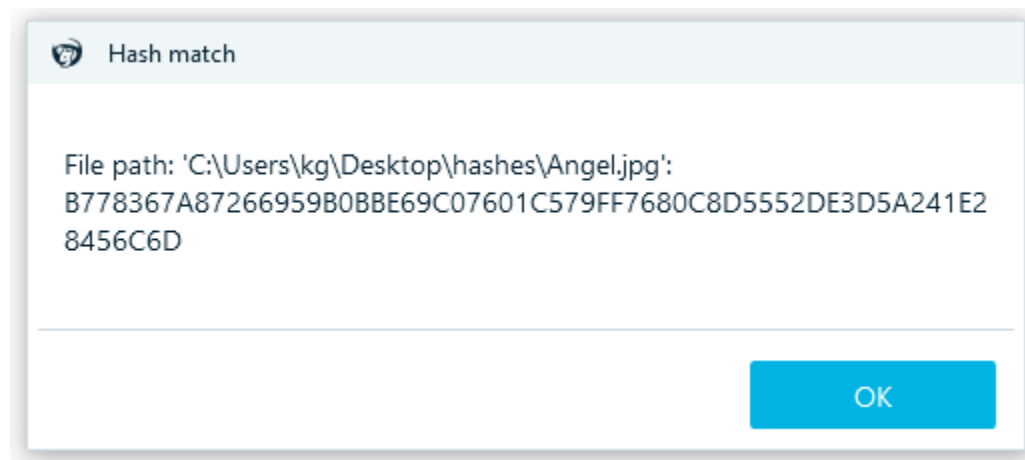
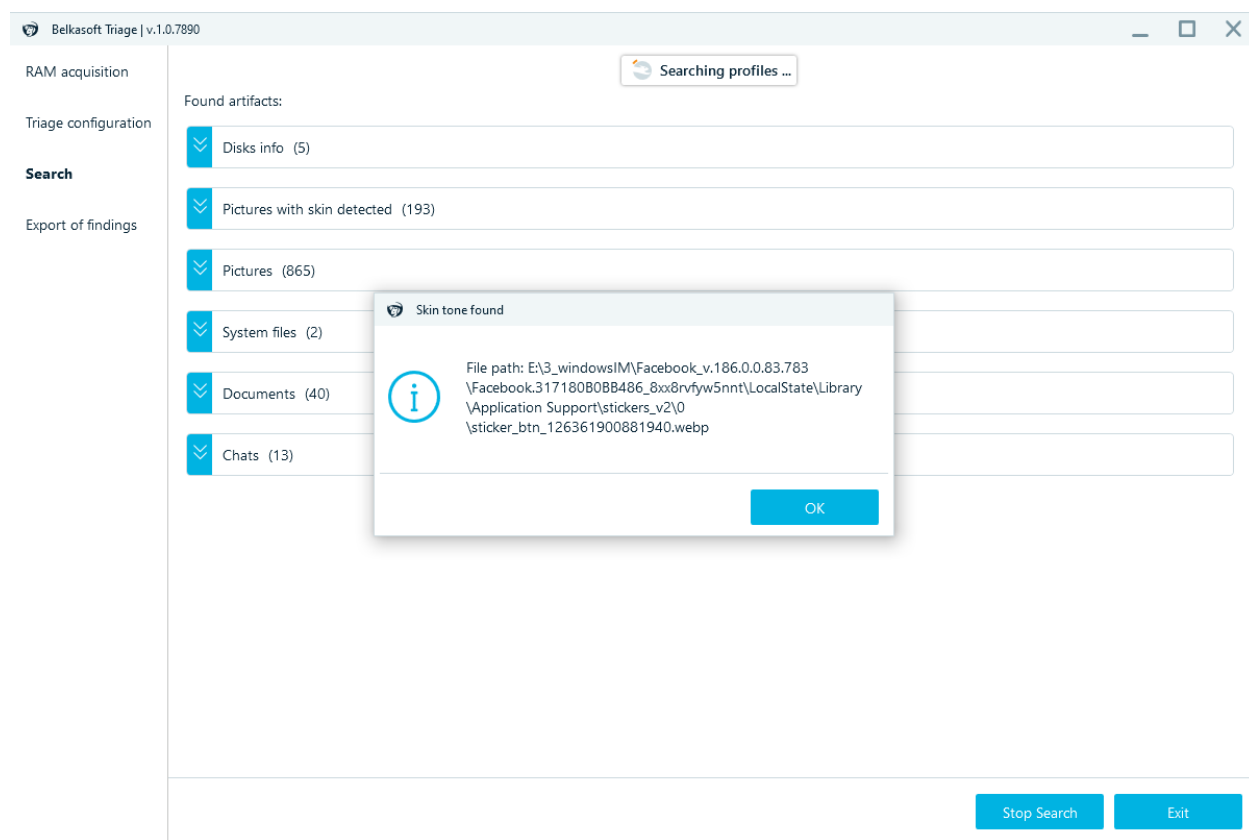
All found results are instantly displayed on the screen. Expand **detected profiles** to view the information:



Detecting Hashes and Skin

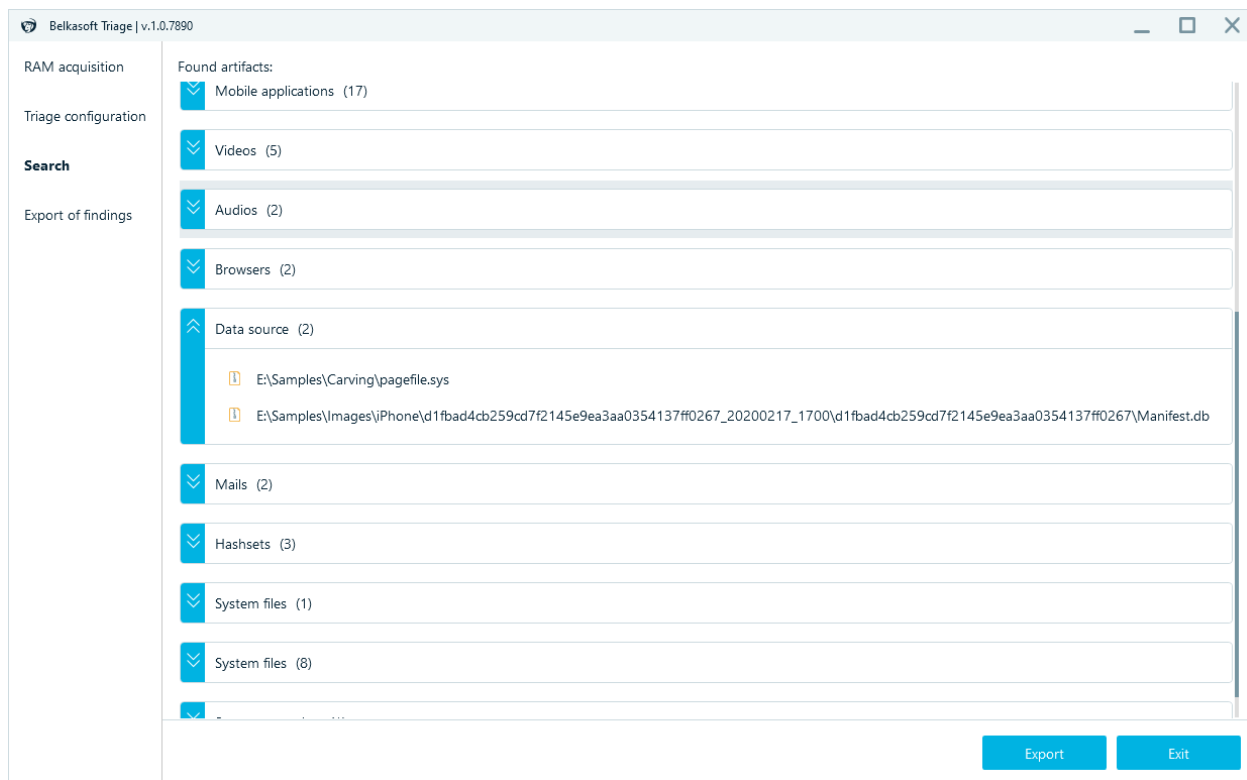
When the first match of the **hashes/skin** occurs, a notification window pops up, it appears just once, for

the first match detected.



Detecting nested data sources

Detected **Mobile backups**, **Virtual machines**, **Memory files** are presented under the **Data Source** section.



Please note: Belkasoft T detects encrypted drives, virtual machines, archives and other nested data sources but doesn't search inside them.

List of detected files:

hiberfil.sys, pagefile.sys

*.vdi

*.vmdk

*.mbdb or Manifest.db (iTunes)

*.dmg

*.ab

descript.xml (Miui backup)

info.xml (Huawei backup)

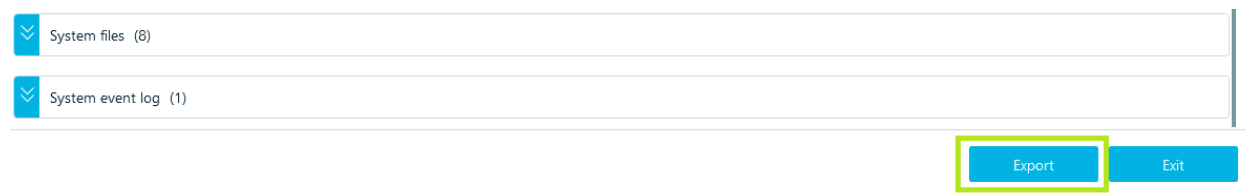
*.aff4

*.af4

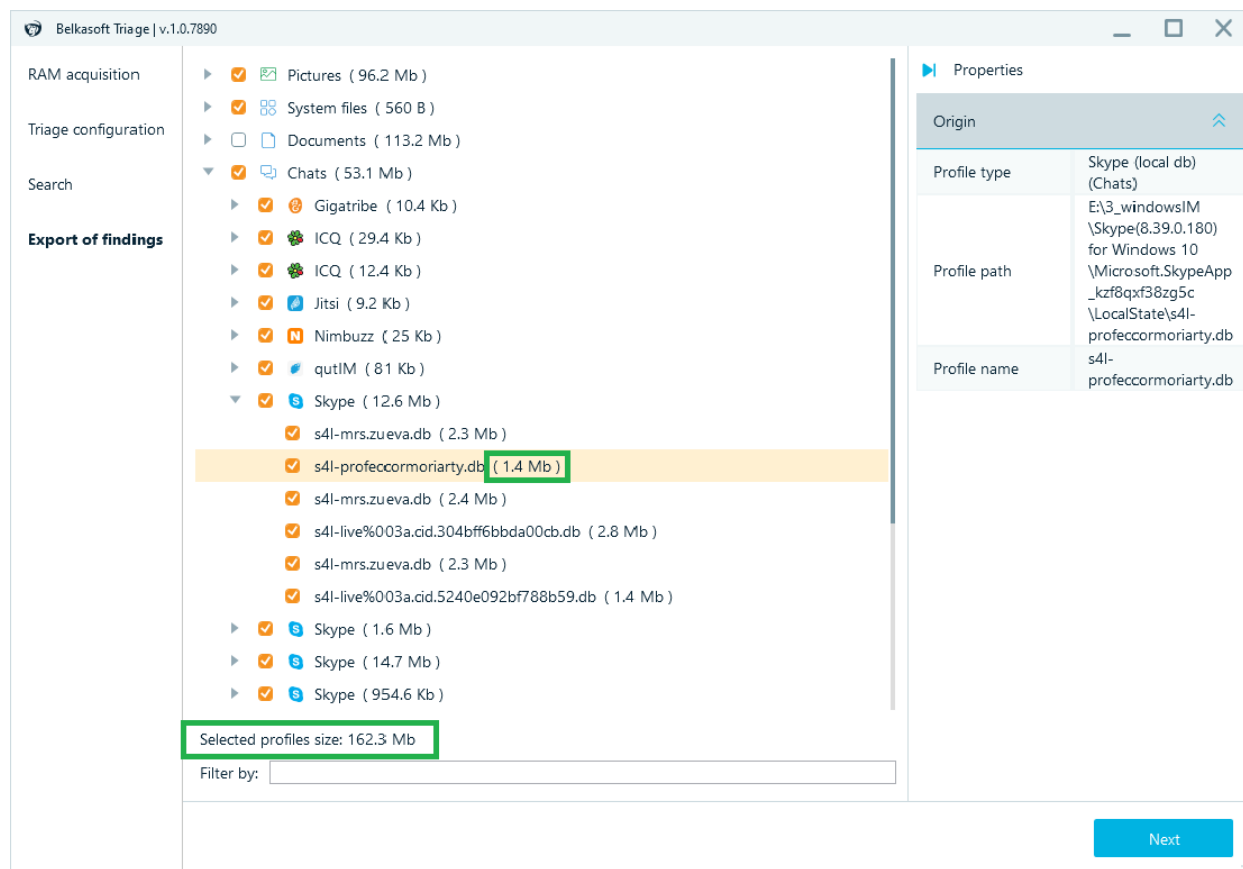
For a closer look all this data can be selected, exported and then analyzed with our flagship tool Belkasoft X.

Step 3: Export Results

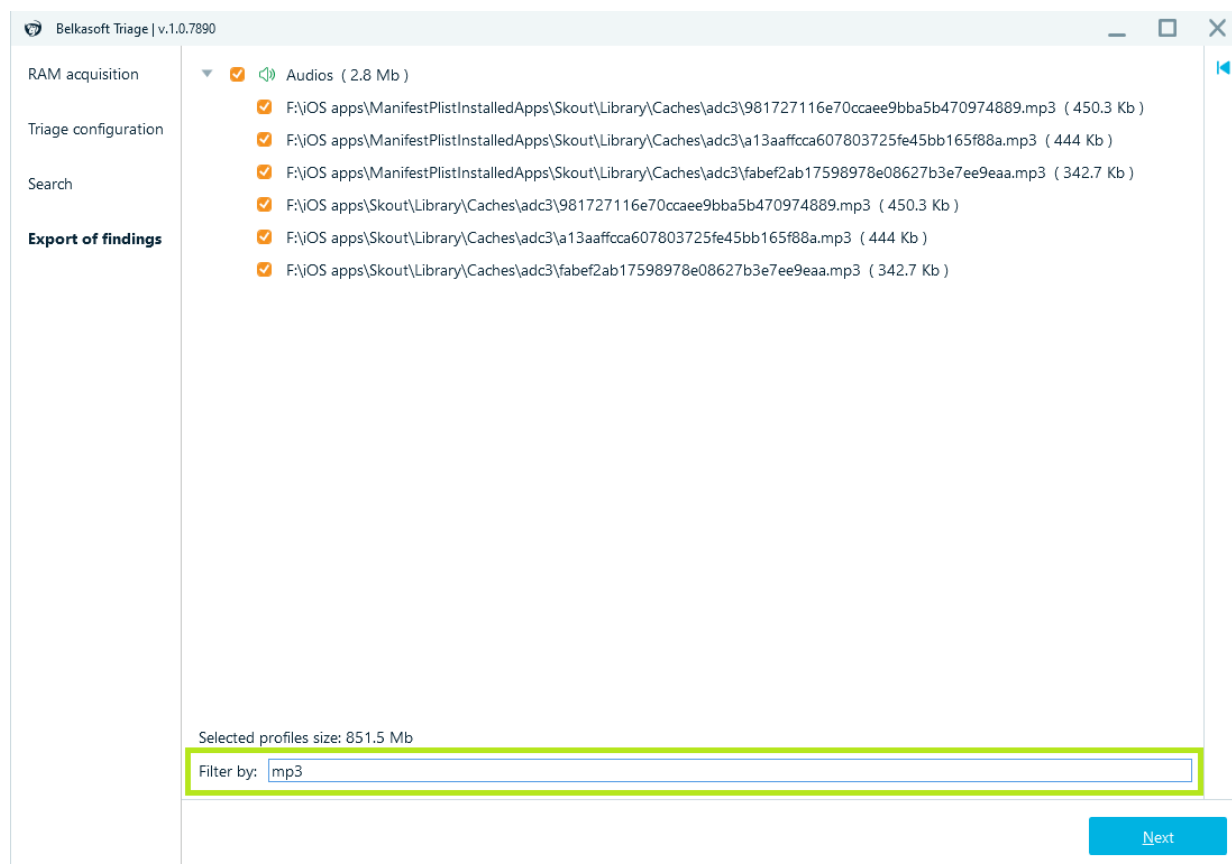
Wait until the analysis completion or **Stop** the analysis as soon as the required data has been found. Press the **Export** button to view the result.



Belkasoft T instantly calculates **the size** of all profiles and the total size. The total amount may exceed the real one, because some of the artifacts found may belong to several different types of detected objects.

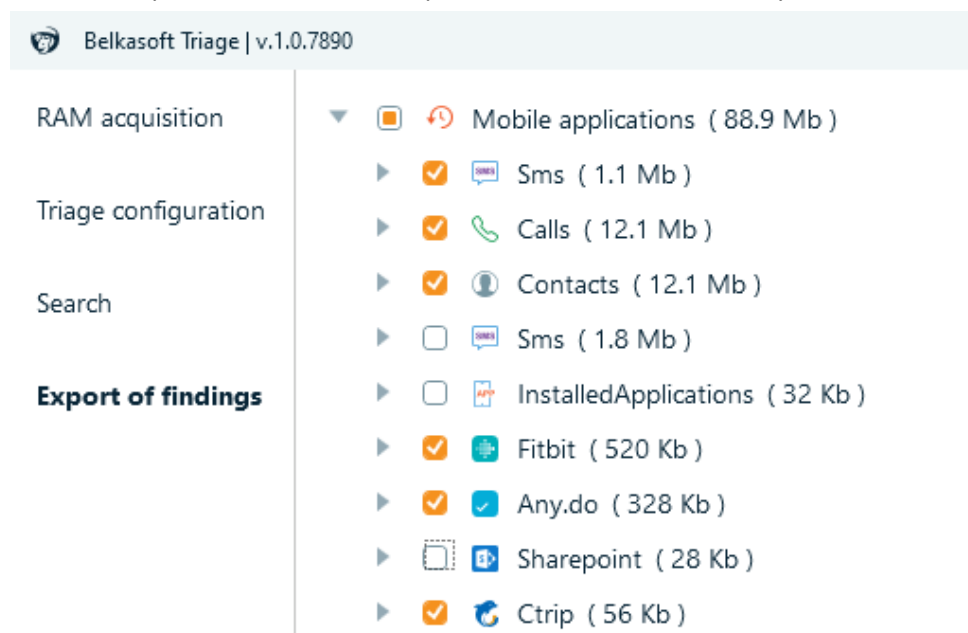


Types 3 or more symbols for **filtering** artifacts:

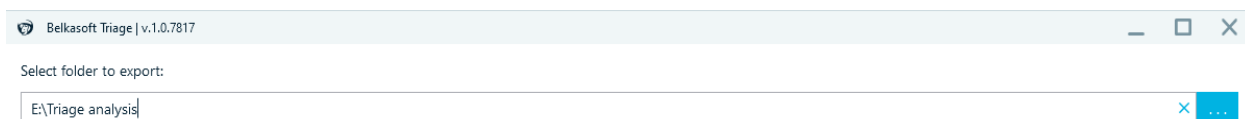


The **Properties** panel on the right contains information about the detected profile/artifact. Select the item to view its properties. **Preview** documents/pictures/videos with default Windows viewer by double clicking on it.

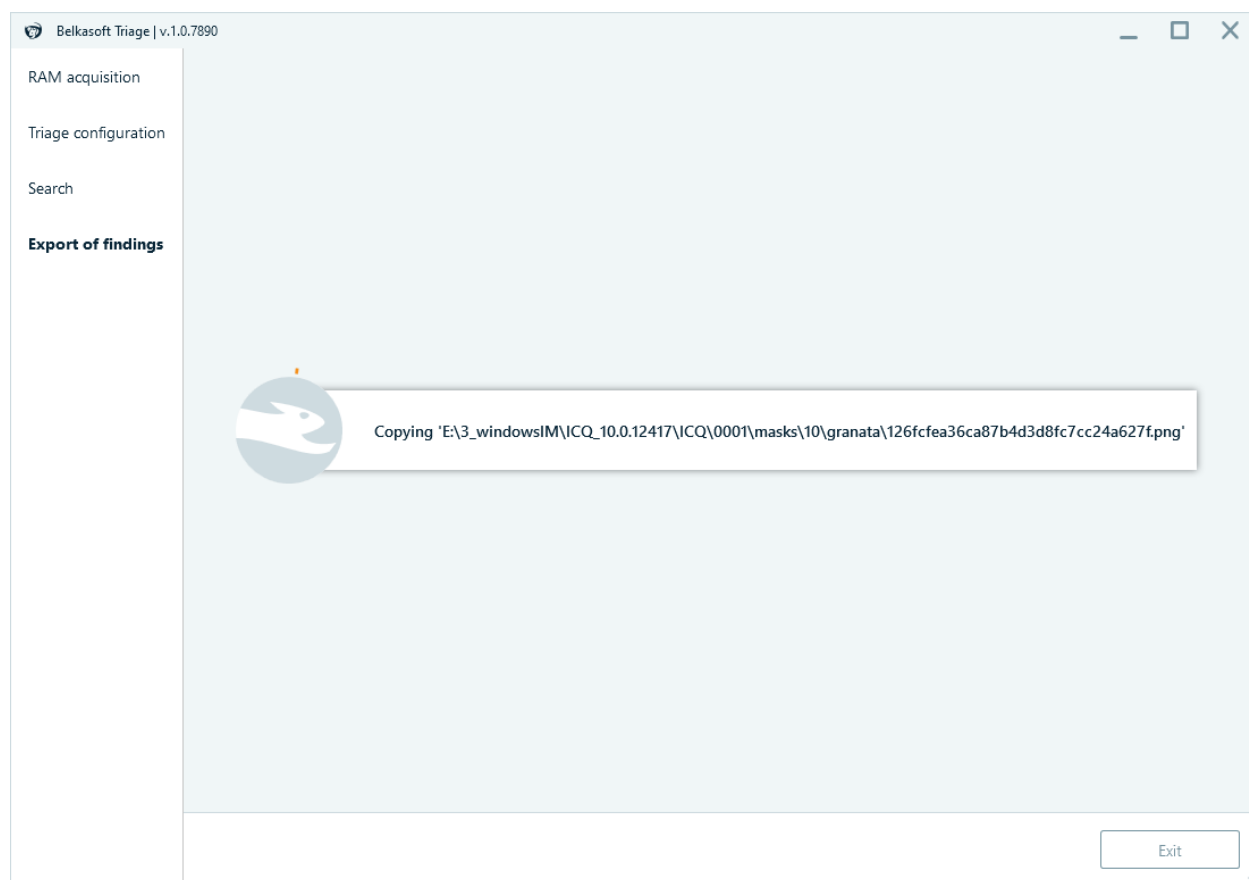
Check all or part of the items for export. All checks are enabled by default.



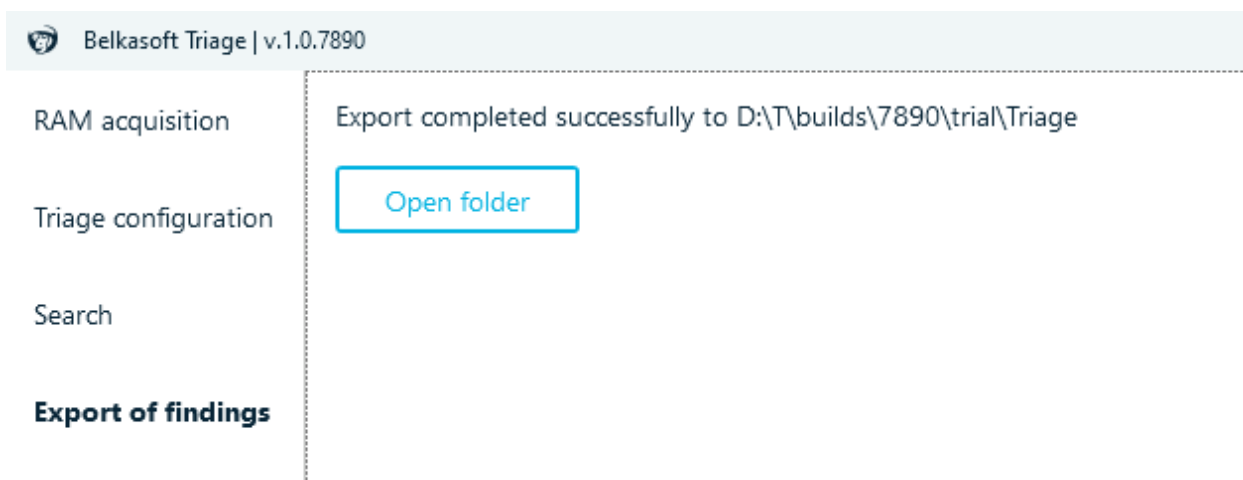
Press **Next** and select the export folder:



Observe the progress on the next screen:



All saved data is stored on the dongle or in the chosen location.



Open folder for viewing the results.

| > This PC > Local Disk (E:) > T | | | |
|---------------------------------|------------------|----------------|------------|
| Name | Date modified | Type | Size |
| T_21-08-04_13-9-55.belkaml | 8/4/2021 1:10 PM | BELKAML File | 371 KB |
| T_21-08-04_13-9-55.tar | 8/4/2021 1:10 PM | WinRAR archive | 130,720 KB |

Analyze the results with **Belkasoft X** <https://belkasoft.com/x>.

Belkasoft T support

Product is available for downloading at the customer portal

<https://belkasoft.com/triage>

Still have questions? Feel free to communicate with our support team

<https://belkasoft.com/support>