Belkasoft Evidence Center X

"Belkasoft Evidence Center X is a very useful tool for digital forensic analysis, that identifies and retrieves information, classifying it by type of file, which complements the manual investigation processes that we develop at Securízame."

LORENZO MARTÍNEZ RODRÍGUEZ
Computer Science Engineer,
who has an extensive experience in
IT security consulting companies,
as well as multinational security vendors
Spain 🇪🇸

INTRODUCTION

At Securízame we carry out investigations of cyber security incidents and commissions of computer forensic expertise on a regular basis. Depending on the case, the methodology that we usually use implies the identification of sources of evidence to be analyzed, from of the interpretation and correlation of system, user and system forensic artifacts of files.

However, there are several tools that forensic professionals can use to automate and enhance part of this analysis.

In the forensic field, among the best known and most veteran commercial suites is Belkasoft Evidence Center. A fully functional trial version is available. We have been able to test the version 1.0.5969 of Belkasoft X and we want to present our experience with the tool.

The phases of a digital forensic analysis investigation include the acquisition of evidence, their analysis and interpretation, the generation of the results report and the presentation of these to whom it may concern.

THE GUI

Forensic analysis tools should be as intuitive as possible for their users. The operational complexity can lead to human errors, which can ruin the research.

Belkasoft Evidence Center X shows a minimalist graphic interface that guides the analyst to the available operations.

THE ACQUISITION OR INTAKE OF DATA

The tool allows the creation of cases in which the data sources to be analyzed have multiple sources. From disk images or existing memory dumps, to the image creation from Android or Apple mobile devices. This is striking, being rare in suites of this type, which are usually specialized solely in forensics of mobile devices or in the treatment of volume images for Windows or Linux operating systems.

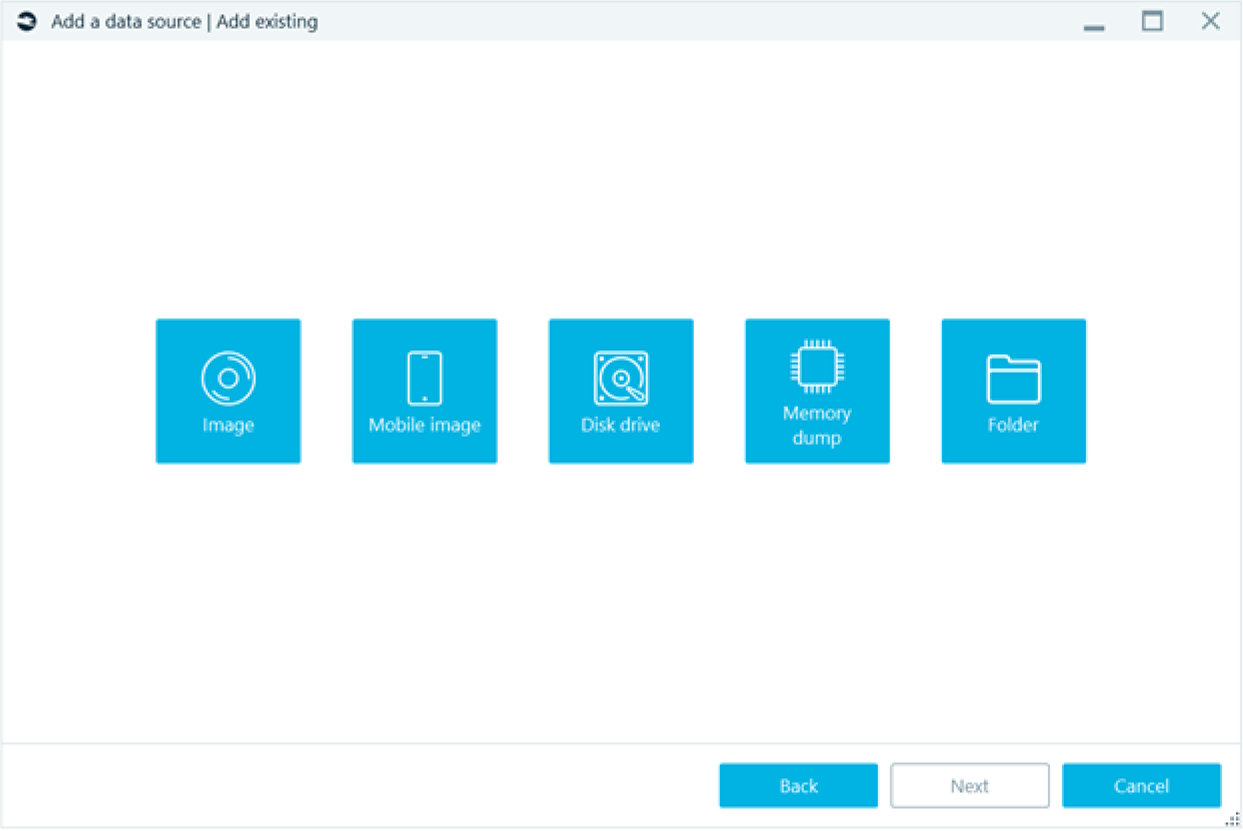
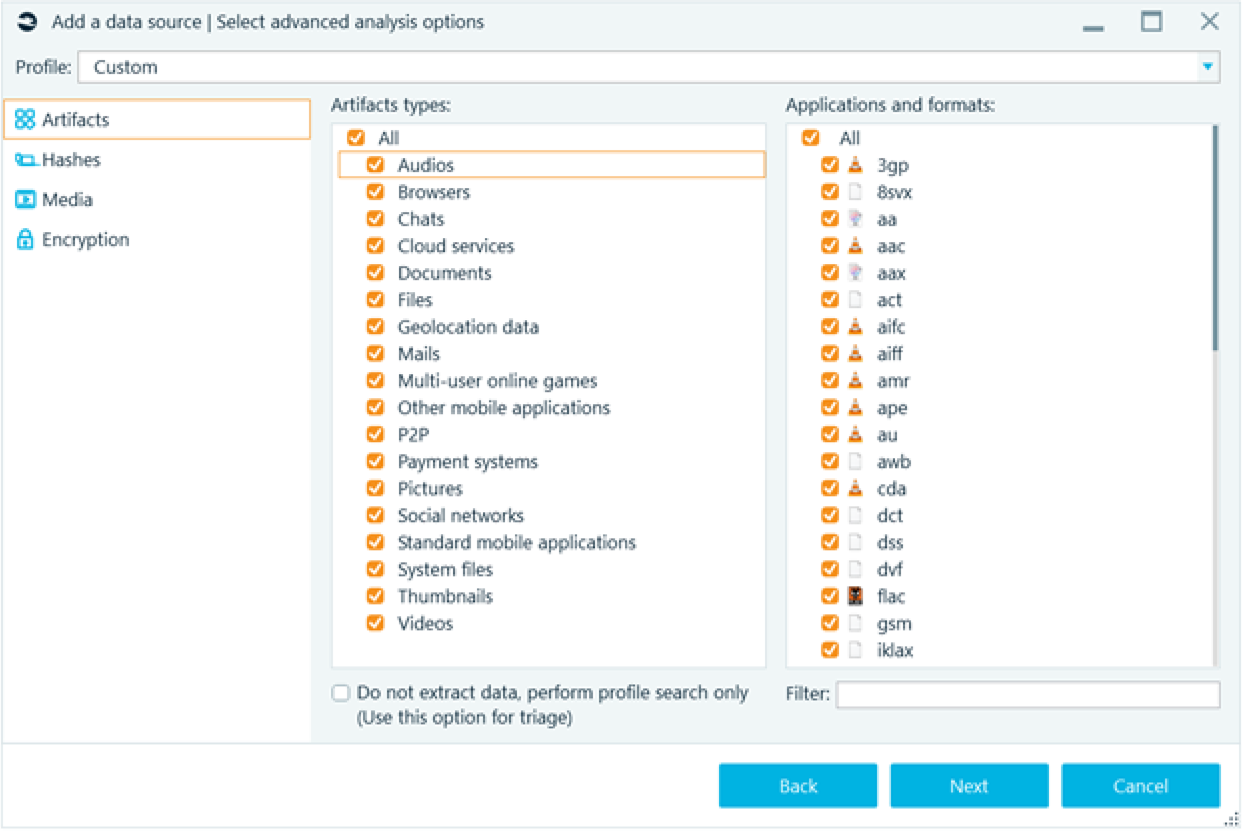


Figure 1. Add data source

The possible options within the data analysis make up the identification of different type of files, carving in free space of file systems and unallocated space, as well as identification of images that belong to categories to identify weapons, drugs or pornography.



Add a data source | Select advanced analysis options

Profile: Custom

- Artifacts
- Hashes
- Media
- Encryption

Artifacts types:

- ☑ All
- ☑ Audios
- ☑ Browsers
- ☑ Chats
- ☑ Cloud services
- ☑ Documents
- ☑ Files
- ☑ Geolocation data
- ☑ Mails
- ☑ Multi-user online games
- ☑ Other mobile applications
- ☑ P2P
- ☑ Payment systems
- ☑ Pictures
- ☑ Social networks
- ☑ Standard mobile applications
- ☑ System files
- ☑ Thumbnails
- ☑ Videos

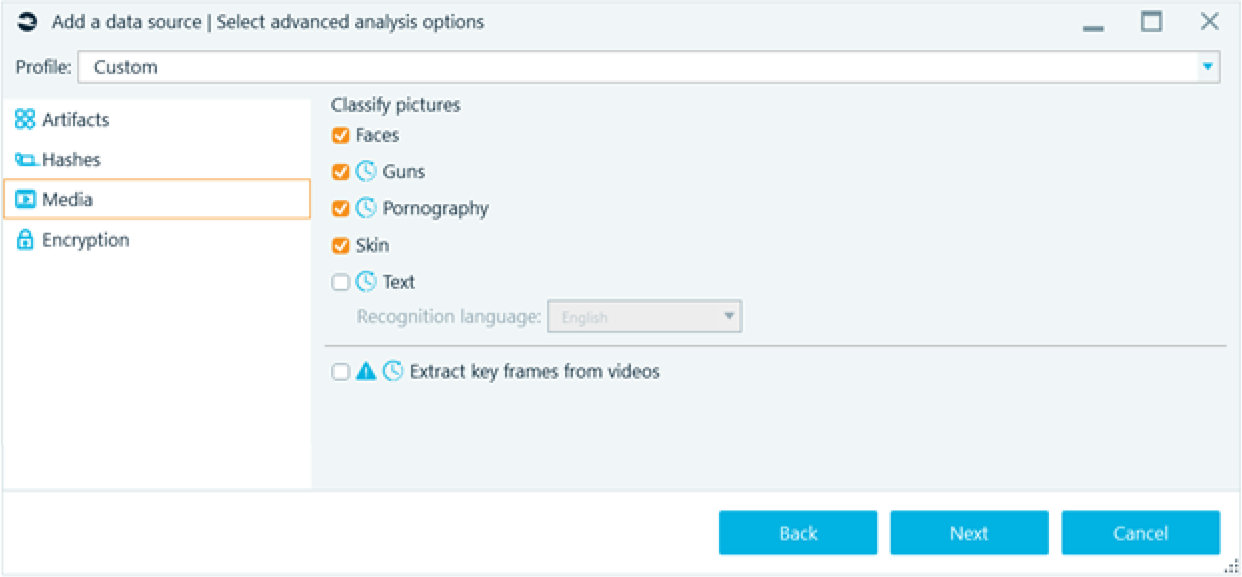
Applications and formats:

- ☑ All
- ☑ 3gp
- ☑ 8svx
- ☑ aa
- ☑ aac
- ☑ aax
- ☑ act
- ☑ aifc
- ☑ aiff
- ☑ amr
- ☑ ape
- ☑ au
- ☑ awb
- ☑ cda
- ☑ dct
- ☑ dss
- ☑ dvf
- ☑ flac
- ☑ gsm
- ☑ iklax

□ Do not extract data, perform profile search only (Use this option for triage)

Filter:

Figure 2. Types of files to identify



Add a data source | Select advanced analysis options

Profile: Custom

- Artifacts
- Hashes
- Media
- Encryption

Classify pictures

- ☑ Faces
- ☑ Guns
- ☑ Pornography
- ☑ Skin
- □ Text

Recognition language: English

□ Extract key frames from videos

Figure 3. Advanced identification in images

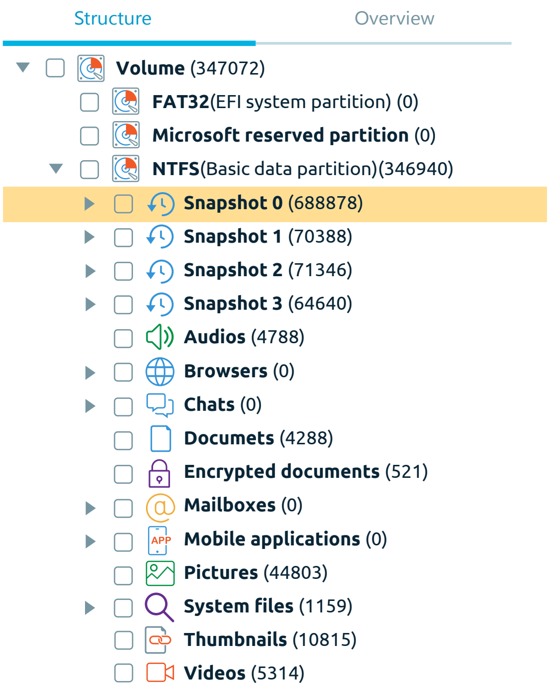
Depending on the options selected and the size of the evidence to be acquired, the process may take several hours.

THE ANALYSIS

Once the acquisition and classification of information is completed, the tool will allow the user to access the different elements identified, according to the type of file, allowing it both on the current file systems of the selected volumes, as well as in the Shadow Copies of them.

The power of forensic tools of this type is given by the amount of supported applications for identification and interpretation. Thus BEC X classifies contents identified evidence such as Audios, Browsers, Chats, Documents, Encrypted documents, Mailboxes, Mobile applications, Pictures, System files, Thumbnails and Videos.

In the results obtained, BEC X allows to carry out narrow searches between ranges of start and end date/time. Identifying activity over a period of time is vital in investigations, since in many cases the important thing is to focus on what happened in a system on a specific date.



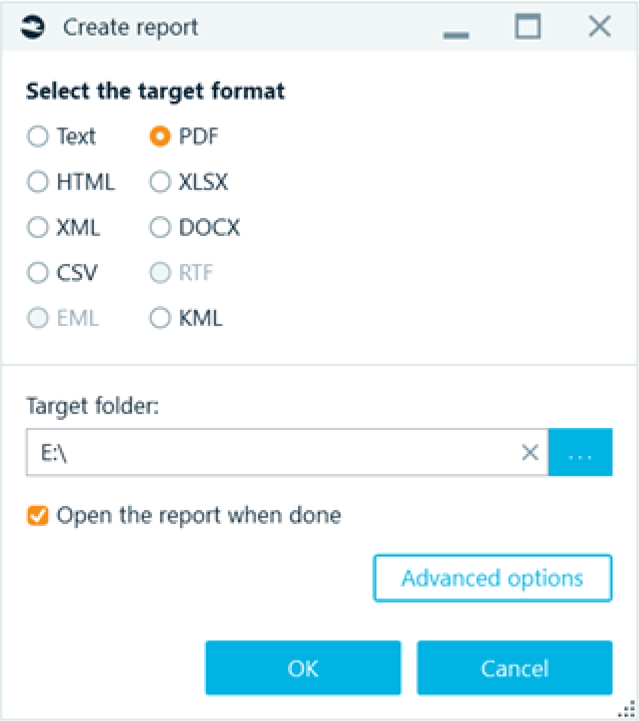
- □ **Volume** (347072)
  - □ **FAT32**(EFI system partition) (0)
  - □ **Microsoft reserved partition** (0)
  - □ **NTFS**(Basic data partition)(346940)
    - □ **Snapshot 0** (688878)
    - □ **Snapshot 1** (70388)
    - □ **Snapshot 2** (71346)
    - □ **Snapshot 3** (64640)
    - □ **Audios** (4788)
    - □ **Browsers** (0)
    - □ **Chats** (0)
    - □ **Documets** (4288)
    - □ **Encrypted documents** (521)
    - □ **Mailboxes** (0)
    - □ **Mobile applications** (0)
    - □ **Pictures** (44803)
    - □ **System files** (1159)
    - □ **Thumbnails** (10815)
    - □ **Videos** (5314)

Figure 4. Index of results obtained

REPORT GENERATION

Every investigation always ends in a written report. The quality of it will depend on the quantity and usefulness of the information extracted and processed and, of course, the analyst skill and experience.

The structure and body of the report will depend on the requirements of each case, the findings extracted from sources of evidence and their relevance to the research. Belkasoft Evidence Center X allows the evidences to be exported to different formats.



Select the target format

○ Text ● PDF
○ HTML ○ XLSX
○ XML ○ DOCX
○ CSV ○ RTF
○ EML ○ KML

Target folder:

E:\

☑ Open the report when done

Figure 5. Report formats

Processing this output can help the analyst identify possible breakpoints evidence that initially did not take into account, which may be key in the investigation. These results may also be added as annexes in a support of non-rewritable storage.

CONCLUSION

Belkasoft Evidence Center X is a very useful tool for digital forensic analysis, that identifies and retrieves information, classifying it by type of file, which complements the manual investigation processes that we develop at Securízame.

Its capabilities to automatically identify the content of pictures that may be illegal is very interesting for certain types of investigations.

It is also useful to carry out blind searches in the email and chat messages from some messaging systems.