




**Belkasoft** X  
Evidence Center

**"Belkasoft Evidence Center X es una herramienta de gran utilidad para análisis forense digital, a la hora de identificar y recuperar información, clasificándola por tipo de fichero, que complementa los procesos de investigación manuales que desarrollamos en Securízame."**



**LORENZO MARTÍNEZ RODRÍGUEZ**  
Ingeniero Informático de profesión,  
con gran experiencia en el mundo  
de la seguridad informática  
España 

---

## INTRODUCCIÓN

En Securízame llevamos a cabo investigaciones de incidentes de ciberseguridad y encargos de peritaje informático forense de forma habitual. Dependiendo del caso, la metodología que empleamos habitualmente implica la identificación de fuentes de evidencia a analizar, a partir de la interpretación y correlación de artefactos forenses de sistema, de usuario y de sistema de ficheros.

Sin embargo, hay varias herramientas que los profesionales del análisis forense podemos utilizar para automatizar y potenciar parte de este análisis.

En el ámbito forense, entre las suites comerciales más conocidas y veteranas, se encuentra Belkasoft Evidence Center. Dispone de una versión de prueba completamente funcional. Hemos podido probar la versión 1.0.5969 de BEC X y queremos exponer nuestra experiencia con la herramienta.

Las fases de una investigación de análisis forense digital comprenden la adquisición de evidencias, el análisis e interpretación de las mismas, la generación del informe de resultados y la presentación de estos a quien corresponda.

## LA GUI

Las herramientas de análisis forense deben ser lo más intuitivas posibles para sus usuarios. La complejidad operativa puede derivar en errores humanos, que pueden arruinar la investigación.

Belkasoft Evidence Center X muestra una interfaz gráfica minimalista que guía al analista a las operaciones disponibles.

### LA ADQUISICIÓN O INGESTA DE DATOS

La herramienta permite la creación de casos en los que los orígenes de datos a analizar tienen múltiples fuentes. Desde imágenes de disco o volcados de memoria existentes, hasta la creación de imágenes desde dispositivos móviles Android o Apple. Llama la atención esto último, al ser poco común en suites de este tipo, que habitualmente suelen estar especializadas únicamente en forense de dispositivos móviles o en el tratamiento de imágenes de volúmenes correspondientes a sistemas operativos Windows o Linux.

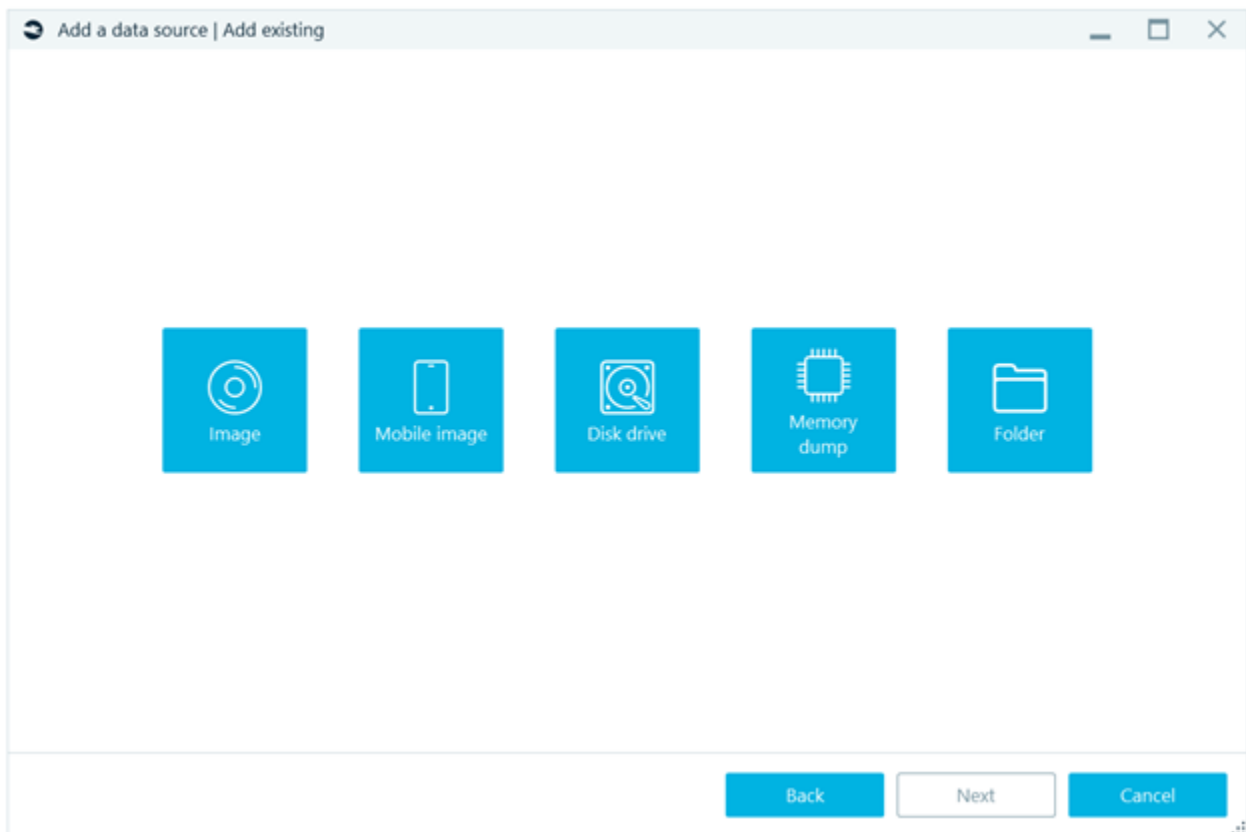


Ilustración 1: Añadir fuente de evidencia

Las opciones posibles dentro de la ingesta de datos conforman la identificación de diferente tipo de ficheros, carving en espacio libre de los sistemas de ficheros y espacio no particionado, así como identificación de imágenes que pertenezcan a categorías para identificar armas, drogas o pornografía.

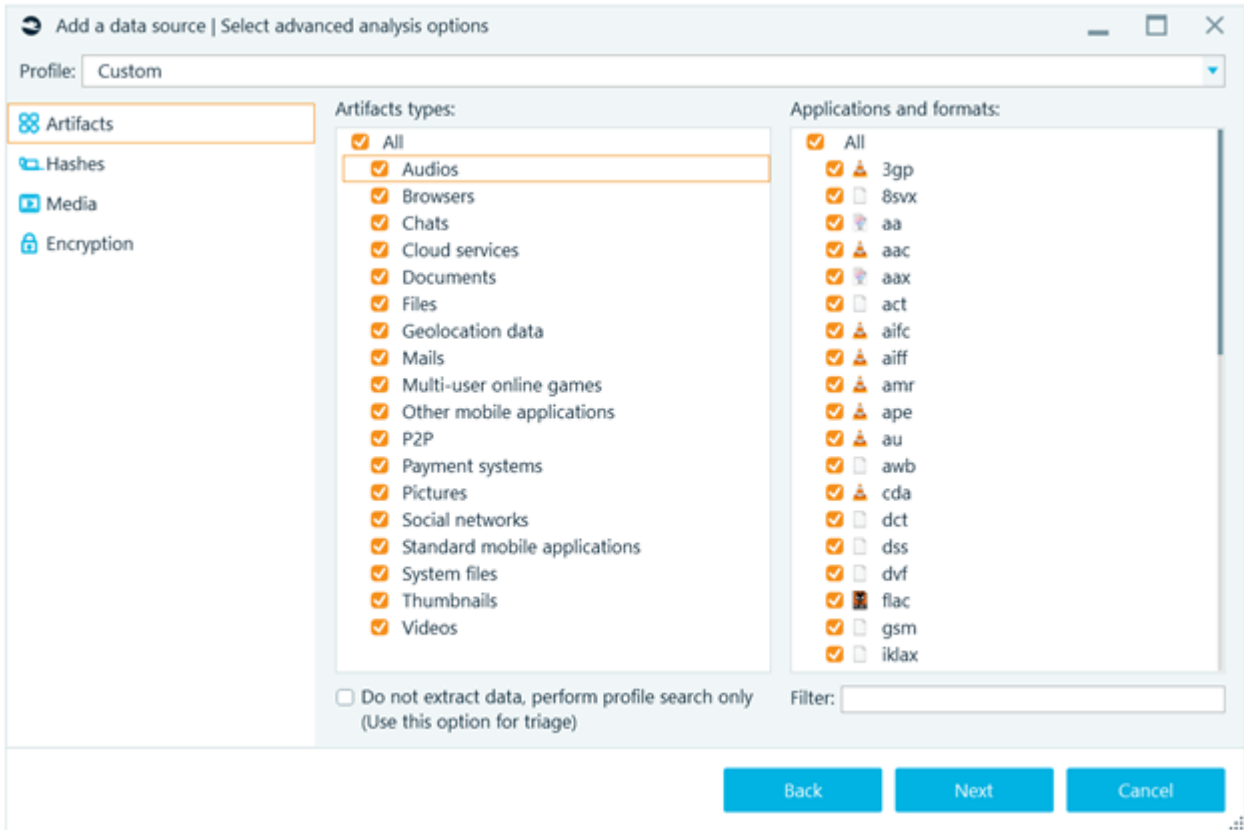


Ilustración 2: Tipos de ficheros a identificar

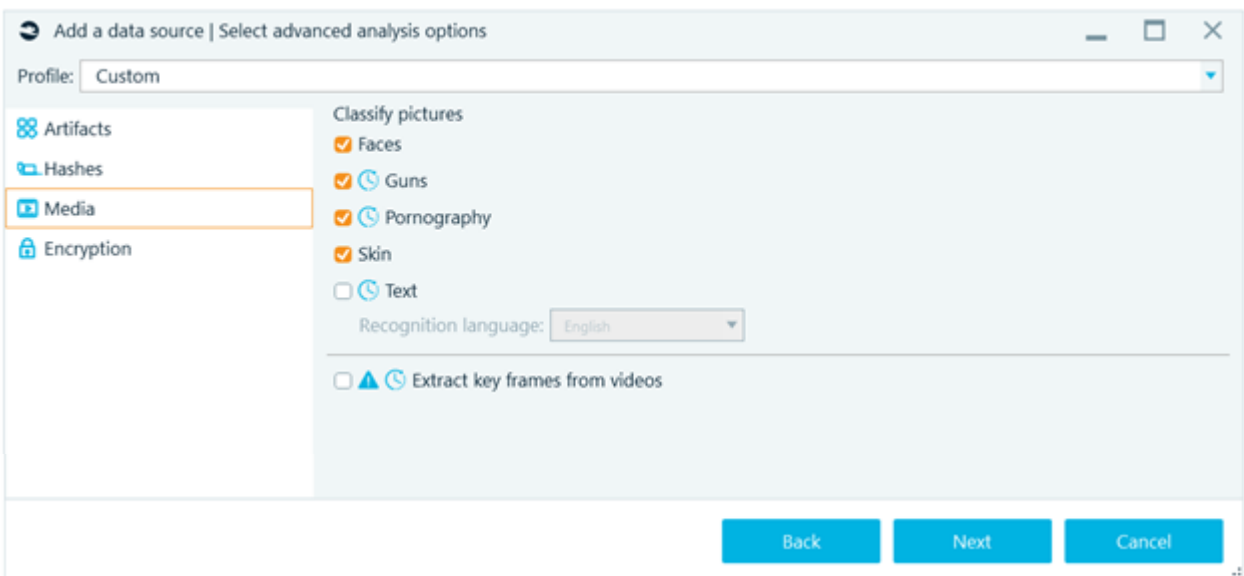


Ilustración 3: Identificación avanzada en imágenes

Dependiendo de las opciones seleccionadas y el tamaño de las evidencias a adquirir, el proceso podrá tardar varias horas.

## EL ANÁLISIS

Una vez terminada la ingesta y la clasificación de información, la herramienta permitirá al usuario acceder a los diferentes elementos identificados, según el tipo de fichero, permitiéndolo tanto en los sistemas de ficheros actuales de los volúmenes seleccionados, así como en las Shadow Copies de los mismos.

La potencia de las herramientas forenses de este tipo viene dada por la cantidad de aplicaciones soportadas para su identificación e interpretación. Así BEC X clasifica los contenidos identificados las evidencias como Audios, Navegación, Chats, Documentos, documentos cifrados, buzones de correo, aplicaciones móviles, imágenes, ficheros de sistema, thumbnails y videos.

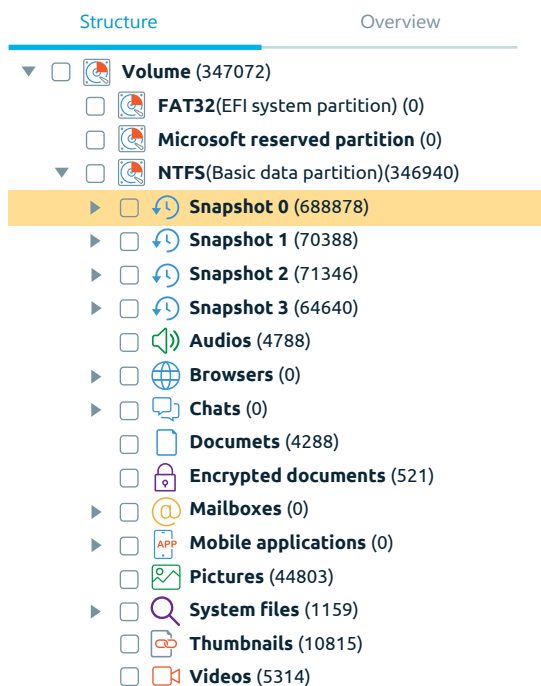


Ilustración 4: Índice de resultados obtenidos

En los resultados obtenidos, BEC X permite llevar a cabo búsquedas acotadas entre rangos de fecha/hora de inicio y fin. La identificación de actividad en un periodo de tiempo es vital en investigaciones, puesto que en muchos casos lo importante es poner el foco en qué sucedió en un sistema en una fecha en concreto.

## GENERACIÓN DE INFORMES

Toda investigación siempre termina en un informe escrito. La calidad del mismo dependerá de la cantidad y utilidad de la información extraída y procesada y, por supuesto, de la habilidad y experiencia del analista.

La estructura y cuerpo del informe dependerá de los requerimientos de cada caso, de los findings extraídos de las fuentes de evidencia y de su relevancia para la investigación. Belkasoft Evidence Center X permite exportar a diferentes formatos las evidencias seleccionadas.

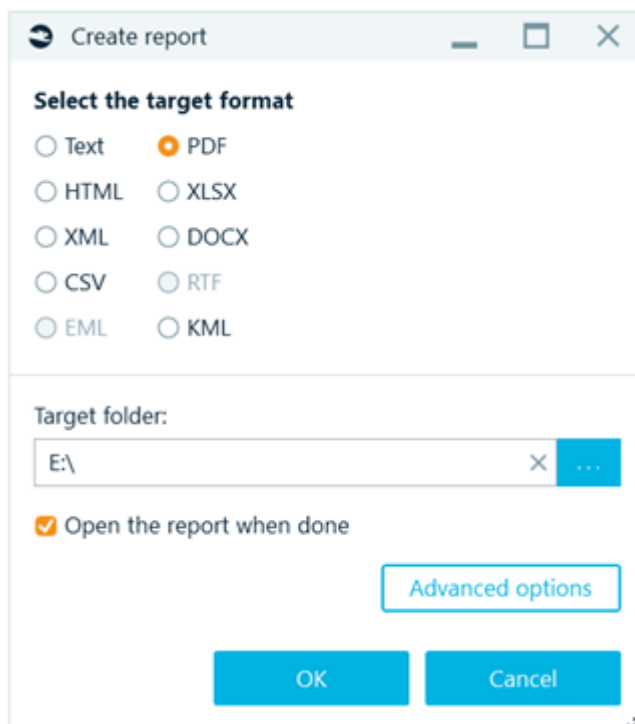


Ilustración 5: Formatos de informe

El procesamiento de esta salida, puede ayudar al analista a identificar posibles puntos de evidencia que inicialmente no haya tenido en cuenta, que pueden resultar clave en la investigación. Estos resultados podrán ser además añadidos como anexos en un soporte de almacenamiento no-reescribible.

## CONCLUSIONES

Belkasoft Evidence Center X es una herramienta de gran utilidad para análisis forense digital, a la hora de identificar y recuperar información, clasificándola por tipo de fichero, que complementa los procesos de investigación manuales que desarrollamos en Securízame.

Sus capacidades para identificar de forma automatizada el contenido de imágenes que puedan ser ilegales es muy interesante para cierto tipo de investigaciones.

Asimismo, es igualmente útil la posibilidad de llevar a cabo búsquedas ciegas en correos electrónicos y mensajes de chat de algunos sistemas de mensajería.



702 San Conrado Terrace, Unit 1  
Sunnyvale CA 94085 (USA)  
+1 (650) 272-03-84

Try free at <https://belkasoft.com/trial>  
30 days trial