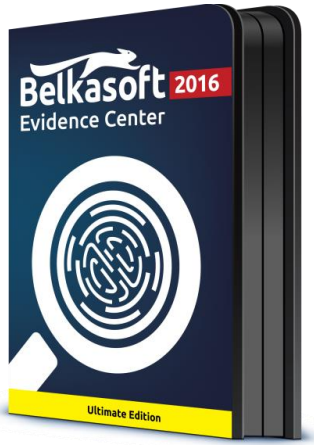
Belkasoft
forensics made easier

Evidence Center 2016
contra los delitos cibernéticos



Acerca de Belkasoft

- Empresa rusa con la sede en San Petersburgo
- Oficina en los EEUU
- En el mercado a partir de 2010
- Miles de usuarios en más de 70 países del mundo
- Fuertes contactos con las instituciones académicas
- Miembro y patrocinador de asociaciones internacionales
  - IACIS (“Titanium Sponsor”)
  - HTCIA (“Star Supporter”)

Nuestros clientes

Belkasoft

POLITI

PRICEWATERHOUSECOOPERS

中華人民共和國香港特別行政區政府
The Government of the Hong Kong Special Administrative Region of the People's Republic of China

DEPARTMENT OF JUSTICE · FEDERAL BUREAU OF INVESTIGATION

U.S. DEPARTMENT OF HOMELAND SECURITY

DEPARTMENT OF THE ARMY · UNITED STATES OF AMERICA · 1775

SUSSEX POLICE

BEREITSCHAFTSPOLIZEI THÜRINGEN

Bundeskriminalamt

AFP
AUSTRALIAN FEDERAL POLICE

משטרת ישראל

POLIS

Deloitte.

ERNST & YOUNG
Quality In Everything We Do

Air Canada

Gendarmerie nationale

POLICJA

Qué problemas afectan más a las investigaciones digitales?

- El uso ámplio de encriptado
- Los datos se almacenan más en la nube
- No hay soporte suficiente para Windows 10
- Cantidad de datos a analizar (¡Terabites en cada dispositivo!)
- Las redes sociales y mensajes instantáneos replazan al correo

Qué ofrece Evidence Center para abordar los problemas mencionados :

- El uso ámplio de encriptado
  - Más énfasis en el análisis en vivo de la memoria RAM
  - Se actualizó la integración con Passware Kit Forensic
- Los datos se almacenan más en la nube
  - Soporte nativo de las apps en la nube (Dropbox, OneDrive, etc)
- No hay soporte suficiente para Windows 10
  - Soporta Edge, IE 10 y 11, los jumplists nuevos y claves de registro
- Cantidad de datos a analizar (¡Terabites en cada dispositivo!)
  - Análisis de Hash Set
  - Algoritmos mejorados de búsqueda
- Las redes sociales y mensajes instantáneos reemplazan al correo
  - Más análisis en vivo de la memoria RAM y artefactos nativos

Contra delito cibernético: Fuentes de datos

Belkasoft

Todas las fuentes posibles:

• Almacenamiento	Discos duros y medios extraíbles
• Imágenes de disco	E01, Ex01, FTK, X-Ways, raw (DD), SMART, Atola
• Imágenes lógicas	L01, Lx01
• Dispositivos móviles	iPhone/iPad, backups de Android y Blackberry
• Volcados de memoria	UFED , JTAG/chip-off
• Máquinas virtuales	VMWare, Virtual PC, Virtual Box, XenServer
• Memoria volátil	Volcados de memoria RAM Análisis de la memoria fragmentada con BelkaCarving™
• Memoria virtual	Archivos de hibernación y paginación

Contra delito cibernético: Los SO más usados

Belkasoft

Tanto las computadoras como móviles:

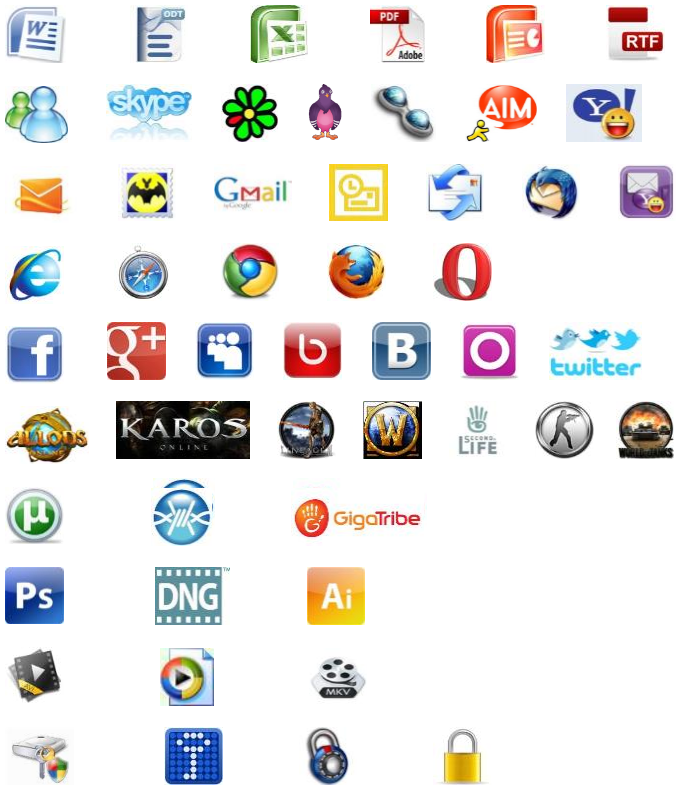
BEC 2017: Ayuda a explorar los sistemas de archivos

- FAT, FAT32, exFAT, etc.
- NTFS
- HFS, HFS+
- ext2, ext3, ext4
- YAFFS, YAFFS2
- Etc.

Contra delito cibernético: Análisis forense

Belkasoft

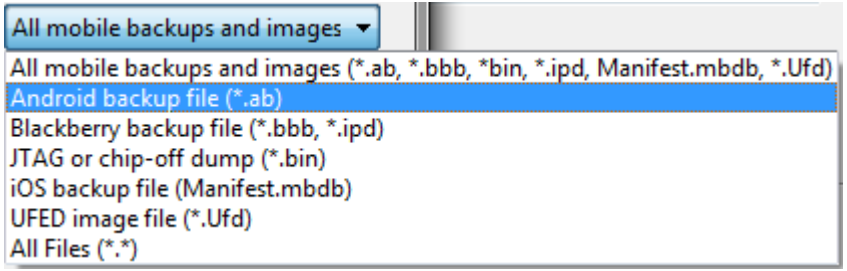
- Documentos de Office
- Emails
- Apps móviles
- Bases de datos SQLite
- Registros
- Archivos de sistema
- Historial de navegación
- Chats de los mensajeros instantáneos
- Chats de las redes sociales (Facebook, Twitter)
- Chats de los juegos multijugador
- Imágenes
- Vídeos
- Archivos encriptados

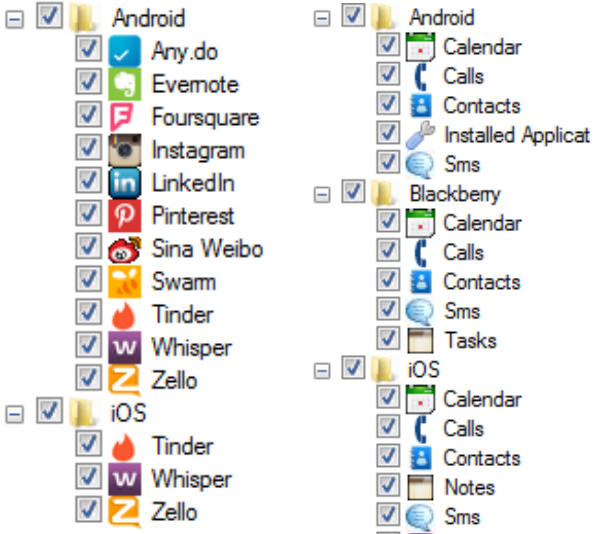


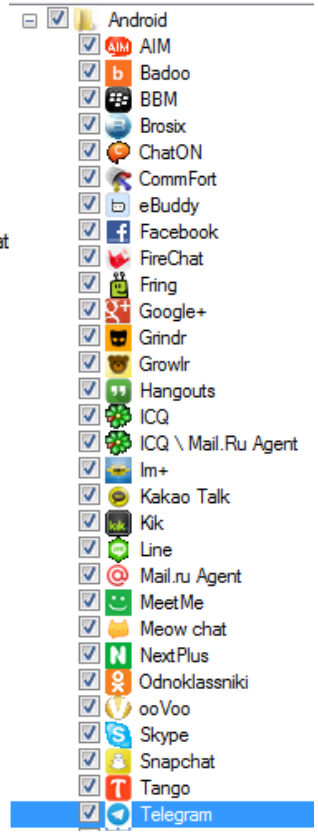
BEC 2017: Localiza, analiza y recupera los datos de mas de 700 aplicaciones

Contra delito cibernético: foco en los móviles

- Varias fuentes de datos
- Se encuentran y se montan de forma automática
- Versiones móviles para las apps
- más populares
- Apps móviles en vez de los navegadores
- SQLite como el formato predeterminado







Qué hay dentro de tu memoria RAM?

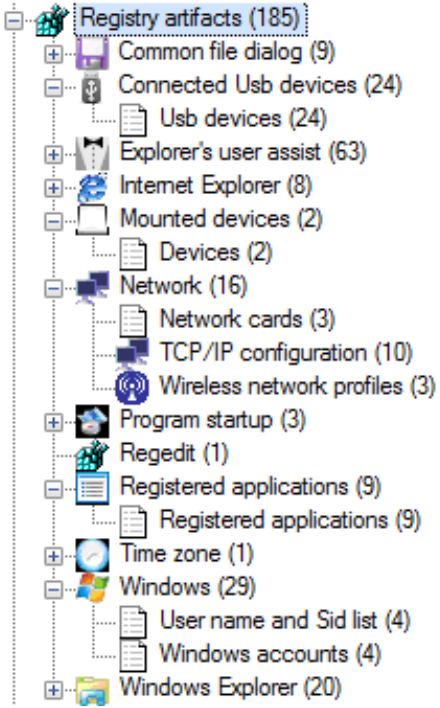
- EL dump puede ser creado con el Capturador gratuito de RAM Belkasoft Live RAM Capturer
- También la Hibernación y el archivo de página (pagefile) pueden ser analizados
- Muchos artefactos extraídos fuera de la caja.
  - Comunicaciones por Redes Sociales
  - Chats IM
  - Buscadores
  - Valores de Registro
  - Fotos etc.
- La lista de procesos se muestra tanto para procesos vivos como muertos. **(No olvides checar nuestra opción BelkaCarving!)**
- La memoria de procesamiento puede ser investigada en HexViewer
- Artefactos encontrados se rompen por proceso.

BEC 2017: Soporte nativo de SQLite

- **SQLite Viewer incorporado**
- **Soporte nativo de SQLite** permite recuperar más evidencia
- También se soportan las bases SQLite **dañadas y destruídas**
- **Analizando los freelists** se recuperan los registros eliminados
  - P.ej. Se pueden recuperar las historias borradas de Skype
- Soporte de los **registros por diario/archivos WAL**
- Búsqueda y carving en el **espacio sin asignar**

BEC 2017: Analiza tanto los registros presentes como los eliminados

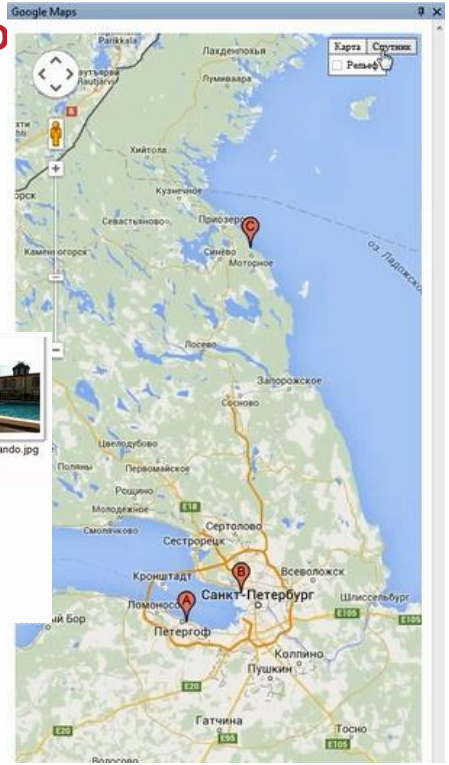
- **Parsing nativo de registros**
- Permite analizar hasta los **registros muy dañados**
  - Sobre todo, usando carving
- **Visor de registros incorporado**
- **Centenares de las claves importantes para la investigación se extraen** de forma nativa
  - Memoria USB
  - Configuración de IP y hotspots conectados
  - Últimos programas ejecutados, archivos abiertos, UserAssists
  - ShellBags
  - Cuentas de usuario y datos de acceso



BEC 2017: Soporta todo tipo de análisis de imágenes y vídeo

- **Geolocalización**
- **Detección de pornografía** (tono de piel)
- **Detección de rostros** (tanto de frente como de perfil)
- **Detección de textos** (en documentos escaneados y fotografiados)
  - Reconoce e indexa el texto de modo automático
  - Después es posible buscar en el texto
- **Detección de falsificación**
  - Busca las fotos editados
- **Detección de cámara**
  - Determina qué cámara fue usada

  (hasta si los metadatos EXIF se eliminarón)
- **Extracción de fotogramas clave del vídeo**
  - No hace falta gastar horas mirando vídeos



Detección de las fotos falsificadas

Belkasoft

Belkasoft
forensics made easier

3

1.jpg
700 x 465

23%

The picture might have been modified

Verdict

We cannot give you a certain answer. Sorry...

Further Details

The image signature is quite ambiguous and its metadata lacking important information. Although it looks like an untouched original, we cannot confidently claim it.

Possible Cameras:

Unable to detect any camera for the image

Contributions of individual signature components:		
Thumbnail	Is thumbnail match	✓
Compression	Image compression	✓
Resolution	The actual image resolution	✗
EXIF	Exif metadata tags	✓

Belkasoft

Belkasoft
forensics made easier

7

C:\Program Files (x86)\Belkasoft Evidence Center Ultimate\Samples\Pictures\TextDetection\english_text.jpg
1748 x 2480

93%

The picture was modified

Verdict

We are very confident that the image was manipulated.

Further Details

The image metadata contain traces of using a graphics editing software, namely, ACD Systems Digital Imaging.

of the wineglass—like all the chinaware and glassware we use for that matter—is sure to have some traces of grease which are left when we touch it with our fingers. And as it doesn't weigh the rim the water displaced by the pins bulges. You can't see it, but if you went to the pains of reckoning the volume of one pin and of comparing it with the volume of the bulge above the rim of the wineglass you would realize that the former volume is hundreds of times smaller than the latter, which explains why a "full" wineglass will still have enough room for another few hundred pins.

The wider the mouth of the wineglass is, the more pins it can take, because there is a larger bulge. A rough reckoning will make the point clear. A pin is about 25 mm. long and half a millimeter thick. You can easily reckon the volume of this cylinder by invoking the well-known geometrical formula $\left(\frac{\pi d^2}{4}\right)l$; it will be equal to 5 mm³. Together with the head, the pin will have a total volume of not more than 5.5 mm³. Let us now reckon the volume of the water in the bulge. The diameter of the wineglass mouth is 9 cm. or 90 mm. The area of such a circle is about 6,400 mm². Assuming that the bulge is not more than 1 mm. high, we thus get a volume of 6,400 mm³, which is 1,200 times more than the volume of the pin. In other words, a "full" wineglass of water can take more than a thousand pins. And indeed we can get the wineglass to take a thousand pins if we are careful enough. To the eye they seem to occupy the whole of the wineglass and even stick out of it. But still no water spills out.

Fig. 66. How many pins in the wineglass?

UNPLEASANT PROPERTY

Anyone who has ever had to handle a kerosene lamp most likely knows what annoying surprises it can spring on one. You fill a tank with it and then wipe the tank dry on the outside. An hour later it's wet

Possible Cameras:

Unable to detect any camera for the image

Contributions of individual signature components:		
Thumbnail	Is thumbnail match	✓
Compression	Image compression	✓
Resolution	The actual image resolution	✗
EXIF	Exif metadata tags	✓

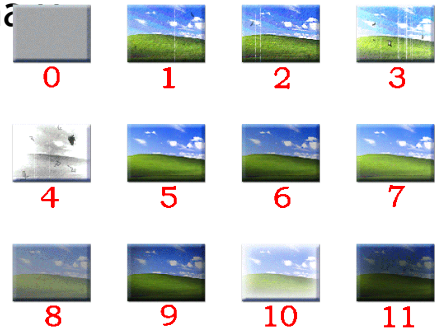
BEC 2017: Buscando la evidencia en los sitios poco comunes

Los jumplists: no se conocen ámpliamente, se limpian rara vez, se guardan por siempre

- Contienen la información de los archivos que se abrían, se veían, se ejecutaban...
- Además sobre los archivos eliminados o guardados en los dispositivos remotos o externos
- **Prueba de acceso:** contienen el nombre completo, la ruta, fecha tiempo de acceso, nombre de equipo y la dirección MAC...

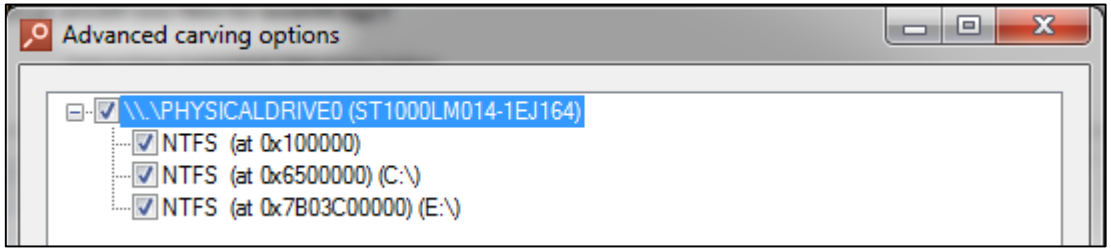
Las miniaturas: no son sólo imágenes

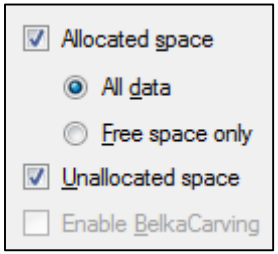
- Se guardan las imágenes pequeñas de archivos de muchos formatos, tales como JPEG, GIF, DOC/DOCX, XLS/XLSX, PDF y mucho más



Carving ayuda a encontrar los datos eliminados y ocultos

- No analiza el sistema de archivos (que ya puede estar eliminada o dañada)
- Busca las “firmas”: sequencias de bites típicos para una aplicación o formato
- Encuentra los datos incluso si el nombre del archivo se ha cambiado
- Encuentra los datos incluso si estan encorporados en otro archivo
- Efectivo para el análisis del espacio asignado y sin asignar





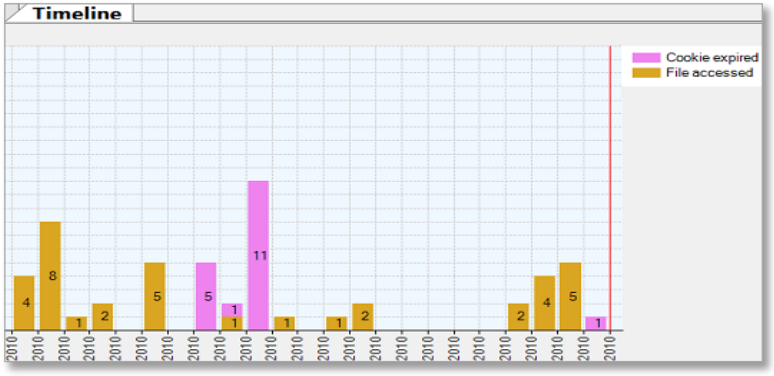
Memoria RAM (volátil) guarda mucha evidencia

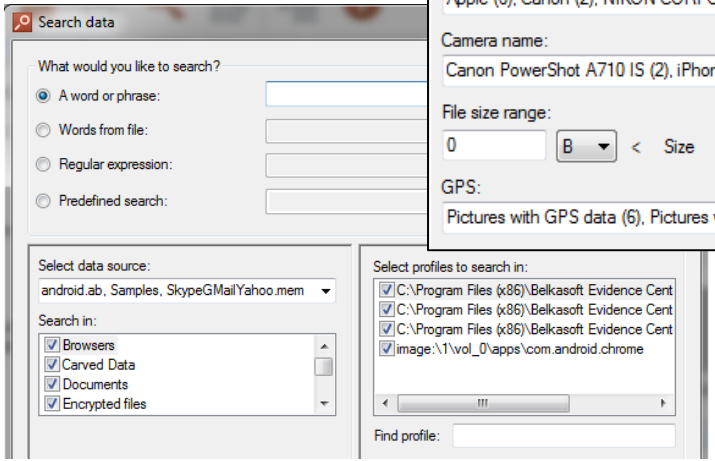
- Tipos de evidencia:
  - claves de cifrado TrueCrypt, PGP, BitLocker
  - Las charlas recientes en las redes sociales
  - Navegación en el modo privado
- BelkaCarving™ recupera los datos fragmentados de los volcados de memoria
- Soporta los volcados de memoria binarios, análisis de archivos de hibernación y paginación

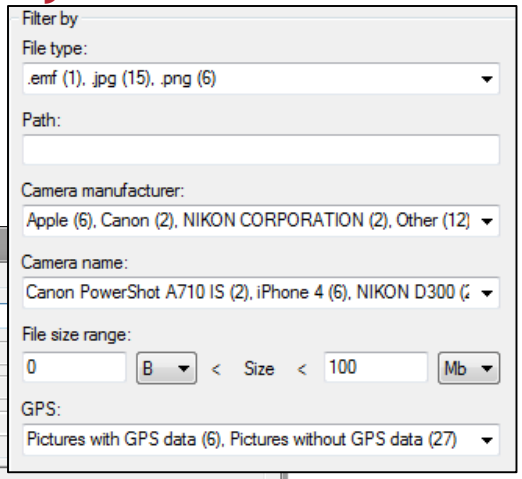
¡Evidence Center automáticamente extrae los archivos de hibernación y paginación incluso de las máquinas virtuales anidadas!

Restringe sus resultados con líneas de tiempo, búsqueda y filtros

- Líneas de tiempo textuales y gráficas
- Una variedad de filtros
- Búsqueda predeterminada

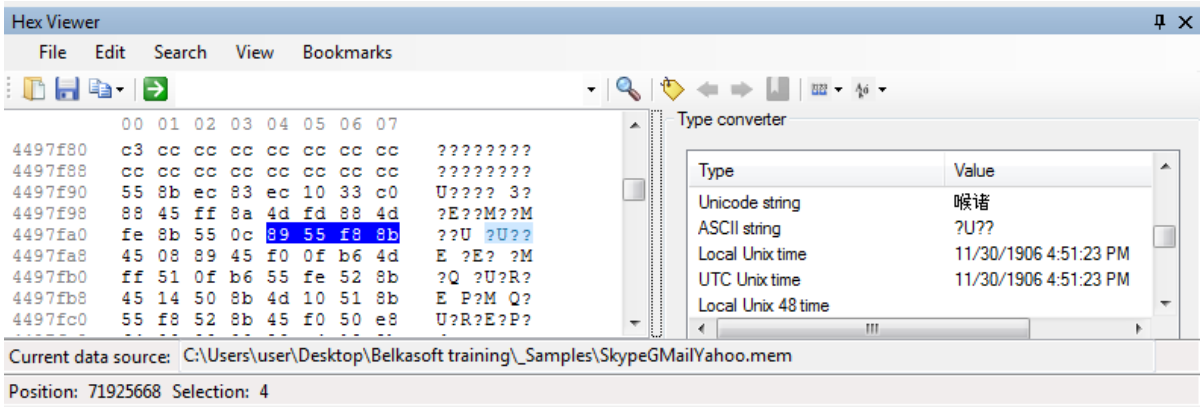


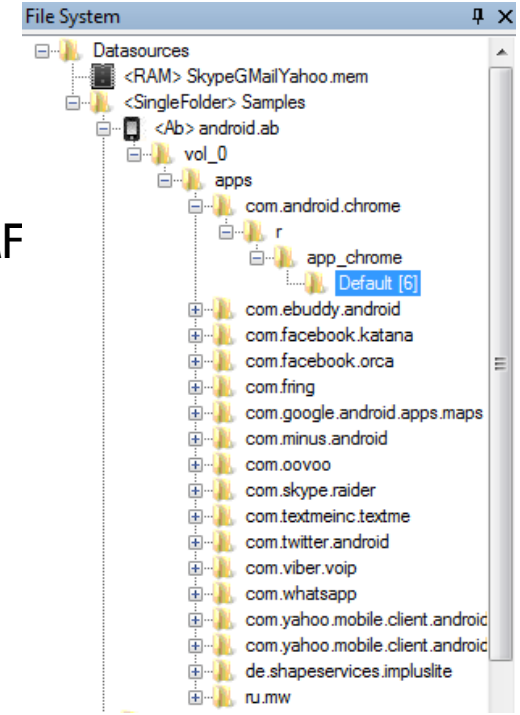




BEC 2017: también para los expertos:

- HexViewer para un archivo o partición
- Carving personalizado con la búsquda an HexViewer
- Análisis de los archivos y carpetas especiales: $Log, $MF
- $OrphanFiles etc.





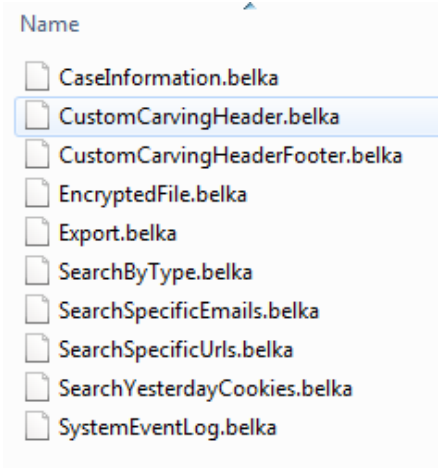
BEC 2017: Módulo de scripts

- Extensiones de usuario se pueden escribir en C# simplificado
- Una base de scripts existentes
- Carving rersonalizado, búsqueda personalizada, procesamiento de casos personalizado...

Files | Picture List | SQLite Viewer | CustomCarvingHeader.belka - ...

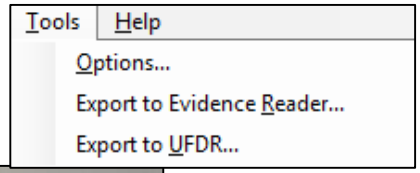
File Run

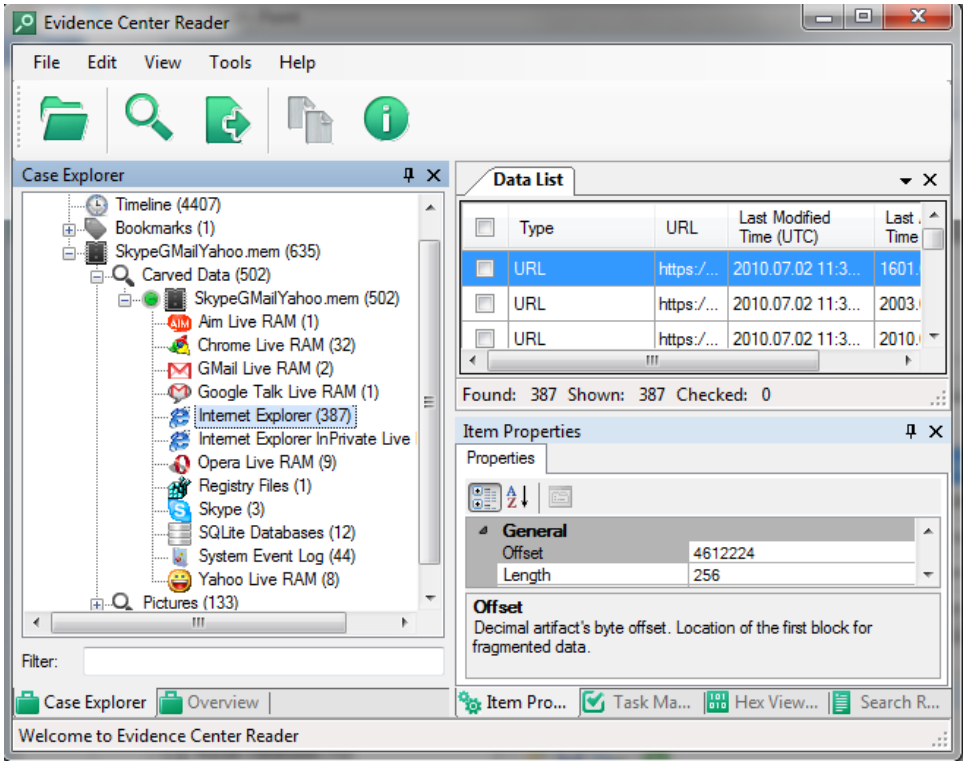
```
// Create signature to search
ByteSearchSignature jpegSinature =
  new ByteSearchSignature(
    new byte[3] { 0xFF, 0xD8, 0xFF }, // signature to search
    10000, // max length of the carved results
    "JPEG" // signature name
    );

// Add signature to the carver
byteSearch.AddSignature(jpegSinature);
```



BEC 2017: colaboración

- Belkasoft Evidence Reader: una herramienta gratuita de solo lectura
- Licencia flotante o portátil
- Team edition – para trabajar en grupo





Antes de despedirnos

Belkasoft

Artículos sobre análisis forense digital escritos por Belkasoft:

http://belkasoft.com/articles

Nuestros datos de contacto

- sales@belkasoft.com
- o contacta nuestros distribuidores locales

Versión de prueba gratuíta

- belkasoft.com/trial
-

¡Gracias!