
www.eysglobal.com

# **MÓDULO 3**:

# UTILIZACIÒN DE HERRAMIENTAS

Utilización de herramientas:

- Encase
- WinHex

# ENCASE

EnCase proporciona las herramientas más avanzadas para el Análisis Forense de Sistemas e Investigaciones Digitales. Con un entorno gráfico intuitivo, flexible y un rendimiento sin igual, EnCase proporciona a los investigadores todo lo necesario para realizar análisis a gran escala en investigaciones complejas con precisión y seguridad.

Desarrollador: Guidance Software
Página de la herramienta:
https://www.guidancesoftware.com/products/Pages/EnCase-Forensic/Search.aspx

# ENCASE

paginación y clusters sin asignar.

- Adquisición de imágenes forenses utilizando técnicas no invasivas con soporte para múltiples sistemas: Windows, MAC OS, Linux, Solaris, HP UX
- Soporte Unicode completo
- Capacidad para análisis concurrente de múltiples sistemas
- Herramientas de búsqueda avanzada
- Soporte para RAID 0,1 y 5
- Soporte para Sistemas de Fichero NTFS comprimidos
- Gestión de filtros compuestos
- Tiempos de respuesta únicos gracias a múltiples caches a nivel de sector y algoritmos de búsqueda optimizados

# ENCASE


EnCase Forensic produce una duplicación binaria exacta del medio original, y luego la verifica generando valores hash MD5 de las imágenes y asignando valores de CRC a los datos; de esta forma trabaja sobre una imagen forense y no sobre el dispositivo. Con estas verificaciones es posible ver cuándo la evidencia ha sido manipulada indebidamente, para mantenerla con validez a efectos legales para su uso en procedimientos judiciales.

# ENCASE

**Tipo de Herramienta: Suite para el análisis forense digital**.

Uso: Herramienta instalable de gran calidad, de las punteras en el mercado. Posee gran cantidad de opciones, con una interfaz de usuario intuitiva y de fácil uso, teniendo un aspecto muy similar a las páginas web, lo que facilita su uso y aprendizaje.

Descripción: EnCase Forensics es el estándar mundial en la tecnolgía de investigación digital para profesionales forenses que necesitan para llevar a cabo la recogida eficaz de datos forenses e investigaciones usando un proceso repetible y defendible.

# ENCASE

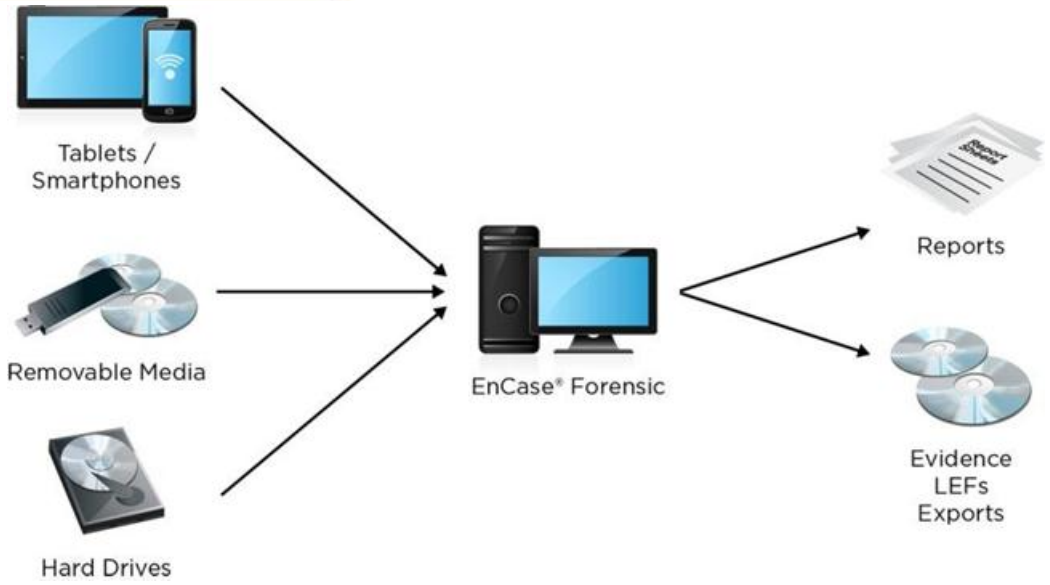
Los principales objetivos que persigue Guidance Software en su herramienta de análisis forense son:

•Adquisición rápida de datos de cualquier tipo de dispositivos.

•Descubrir posibles pruebas con el análisis forense a nivel de disco.

•Producir informes detallados de los análisis.

•Mantener la integridad de las pruebas de forma fiable para una posible utilización en algún juicio.



# ENCASE

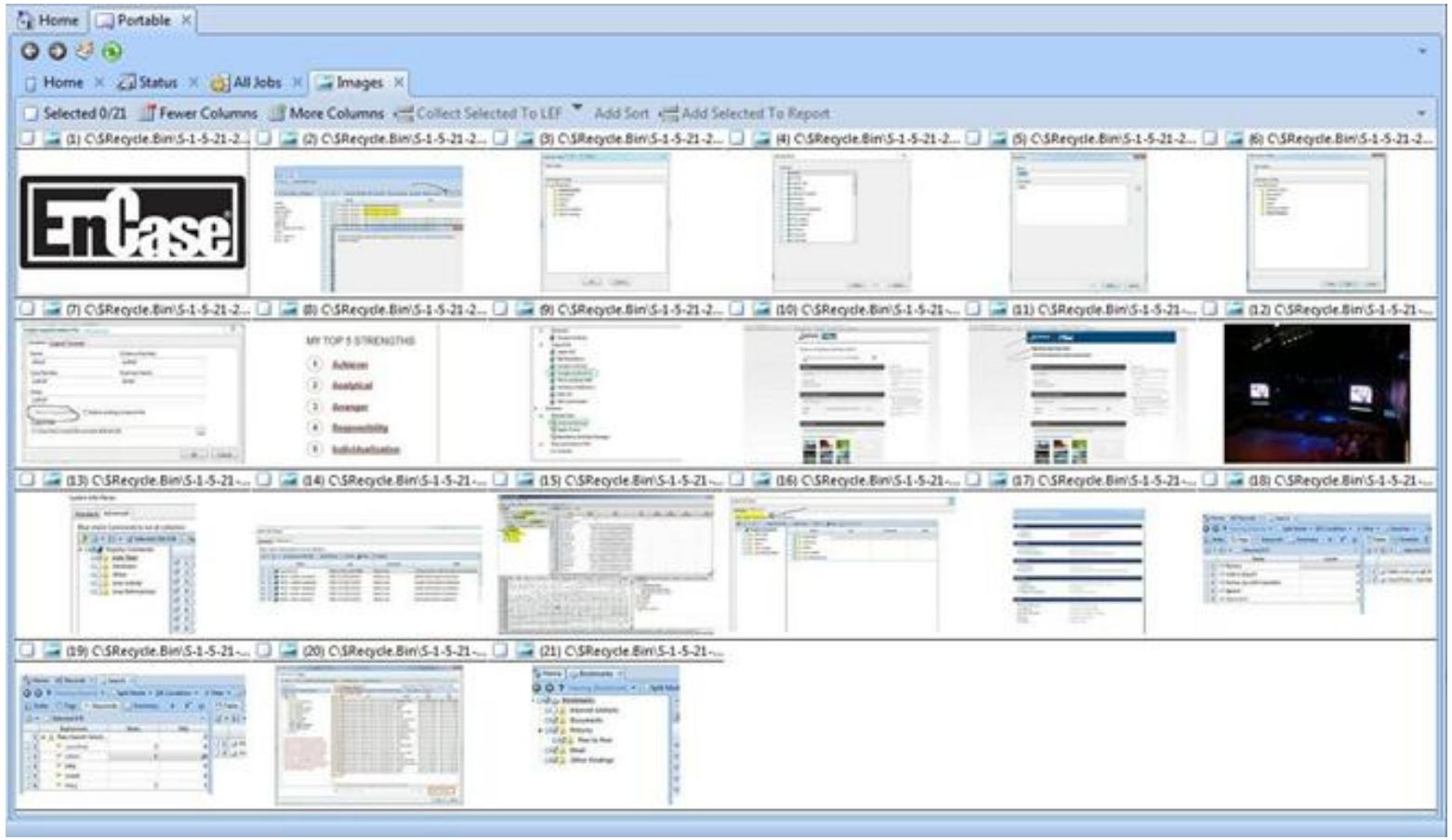



Foto descargada de https://www.guidancesoftware.com/products/Pages/encase-forensic/triage.aspx

# ENCASE

Con el estándar de EnCase se gana en velocidad y en poder en el análisis forense digital pero además de estas grandes ventajas dispone de:

•Adquiere y analiza datos rápidamente de casi cualquier ordenador, teléfonos inteligentes y tabletas de cualquier solución de software de análisis forense digital.
•Aumenta la confianza en los resultados adquiridos con EnCase gracias a que utiliza la probado estándar de corte-referenciado del análisis digital forense.
•Descubre las pruebas potenciales más rápido usando las capacidades de búsqueda avanzada

# ENCASE

•Aumenta la productividad mediante la vista previa de los resultados a medida que se adquieren los datos. Una vez creados los archivos de imagen, se puede buscar y analizar varias unidades o medios de comunicación de forma simultánea.
•Mejorar la eficiencia mediante la automatización de tareas comunes de investigación con EnScript, la solución scripting de en EnCase Forensic.
•Preservar la integridad de las evidencias.

# ENCASE

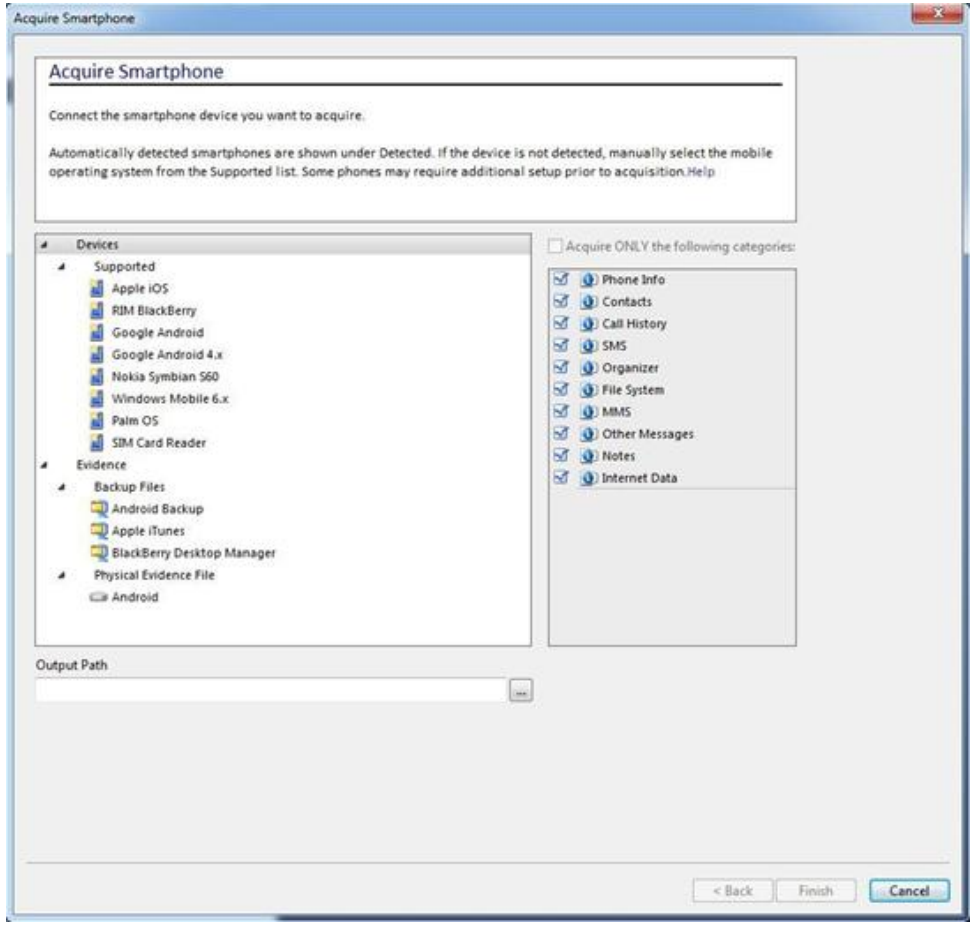



Foto descargada de https://www.guidancesoftware.com/products/Pages/EnCase-Forensic/Collect.aspx

# ENCASE

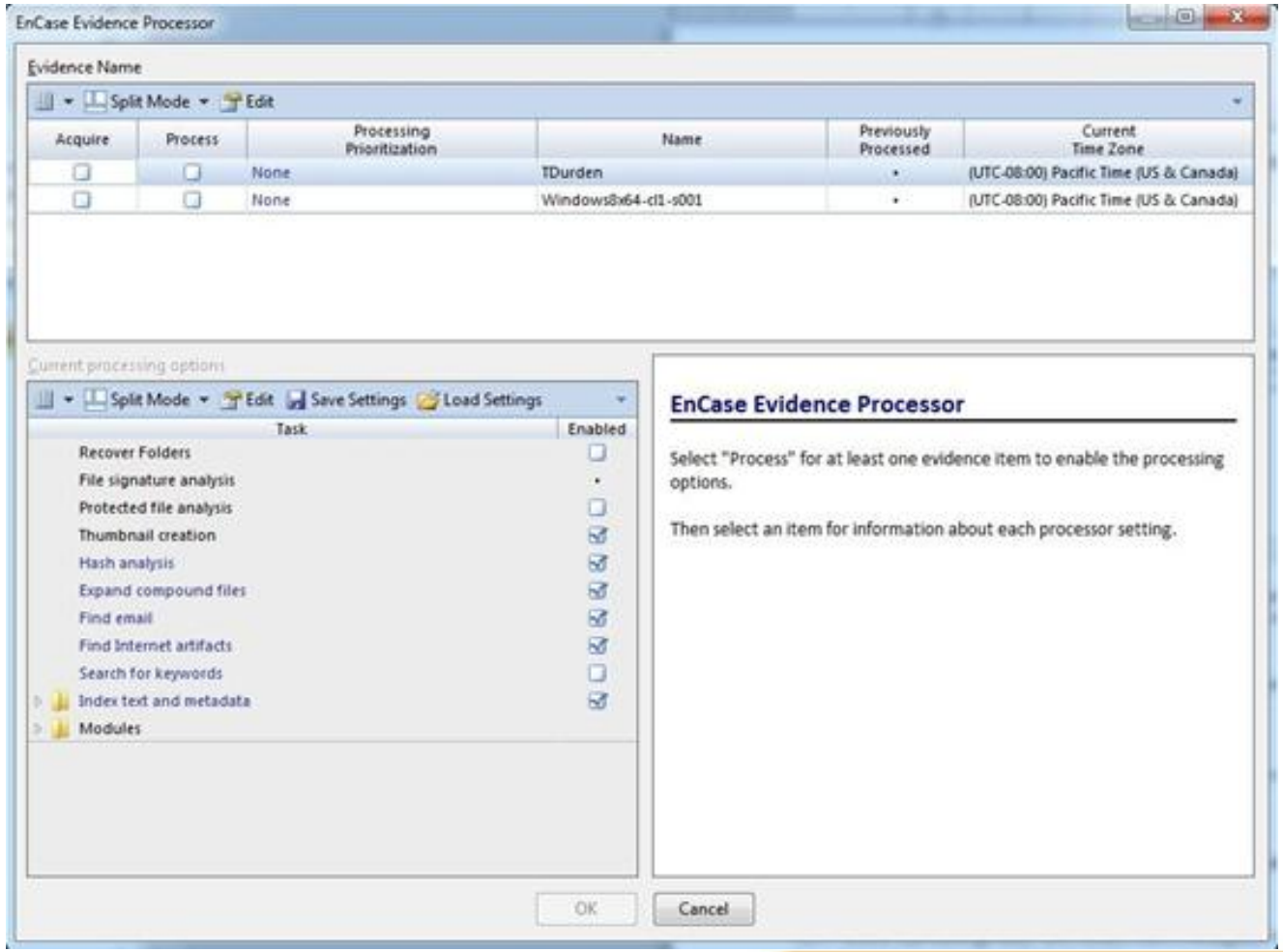
La herramienta tiene una interfaz de usuario intuitiva, con una GUI parecida a la de un navegador Web. También permite compartir los resultados con el resto de la gente involucrada en el caso, para facilitar y agilizar los trámites.

Permite la revision simple de e-mails, entendiendo el contexto de correo electrónico basado en la evidencia potencial en el hilo de la conversación y el contexto relacionado.

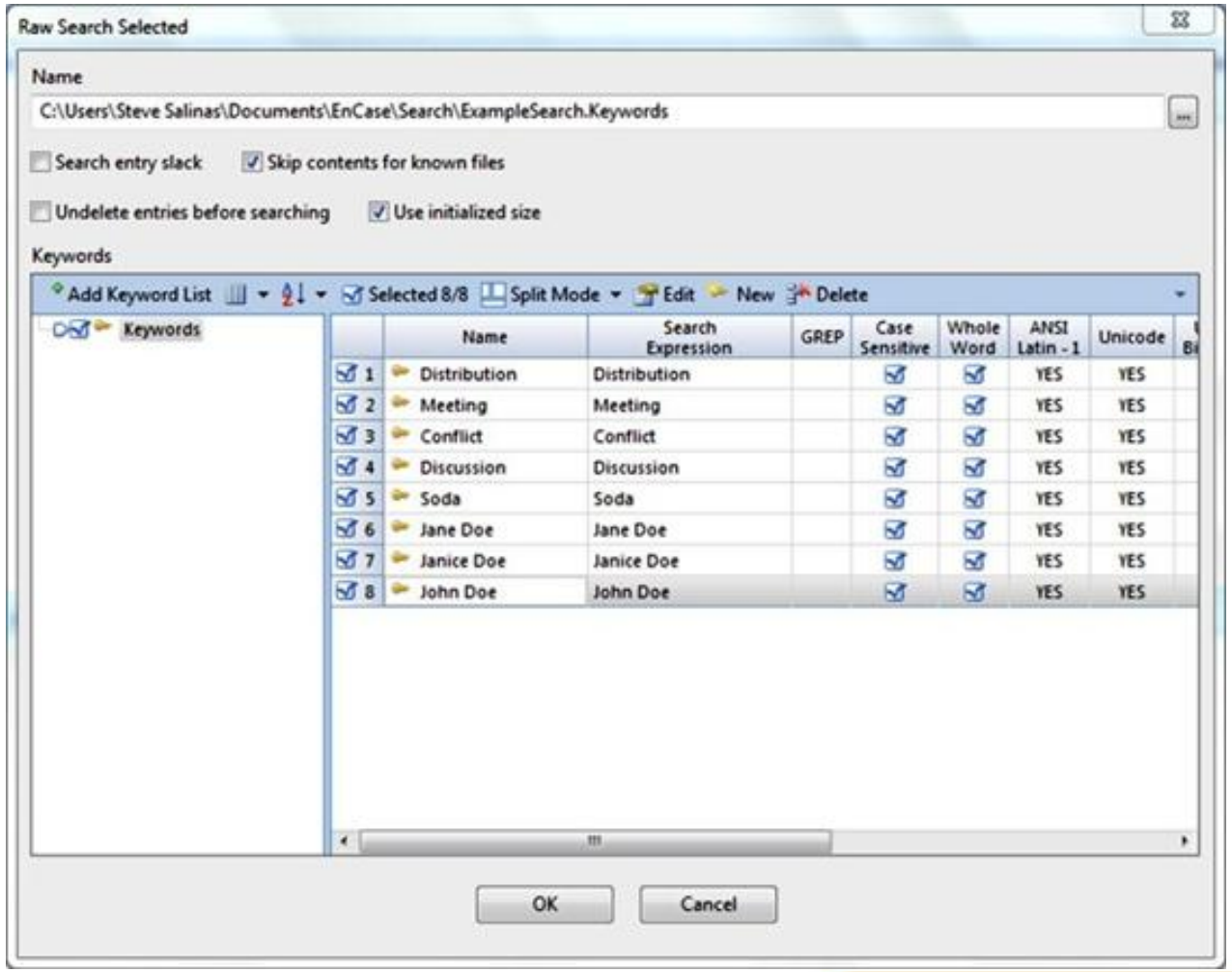
El nuevo motor de indexación del procesador de pruebas, rediseñado, permite consultas más potentes y un procesamiento más rápido, además de la capacidad de automatizar tareas, crear plantillas basadas en perfiles de casos, y de fácil integración con los resultados forenses.

Amplio tipo de archivo y de sistemas operativoss (OS) soportados por EnCase Forensic. En la versión 7, también están integradas EnCase Decryption Suite, EnCase Physical Disk Emulator, EnCase Virtual File System, and EnCase FastBloc SE.

# ENCASE


EnCase Evidence Processor
Evidence Name
Split Mode
Edit
Acquire
Process
Processing Prioritization
Name
Previously Processed
Current Time Zone
None
TDurden
(UTC-08:00) Pacific Time (US & Canada)
None
Windows8x64-cl1-s001
(UTC-08:00) Pacific Time (US & Canada)
Current processing options
Split Mode
Edit
Save Settings
Load Settings
Task
Enabled
Recover Folders
File signature analysis
Protected file analysis
Thumbnail creation
Hash analysis
Expand compound files
Find email
Find Internet artifacts
Search for keywords
Index text and metadata
Modules
EnCase Evidence Processor
Select "Process" for at least one evidence item to enable the processing options.
Then select an item for information about each processor setting.
OK
Cancel

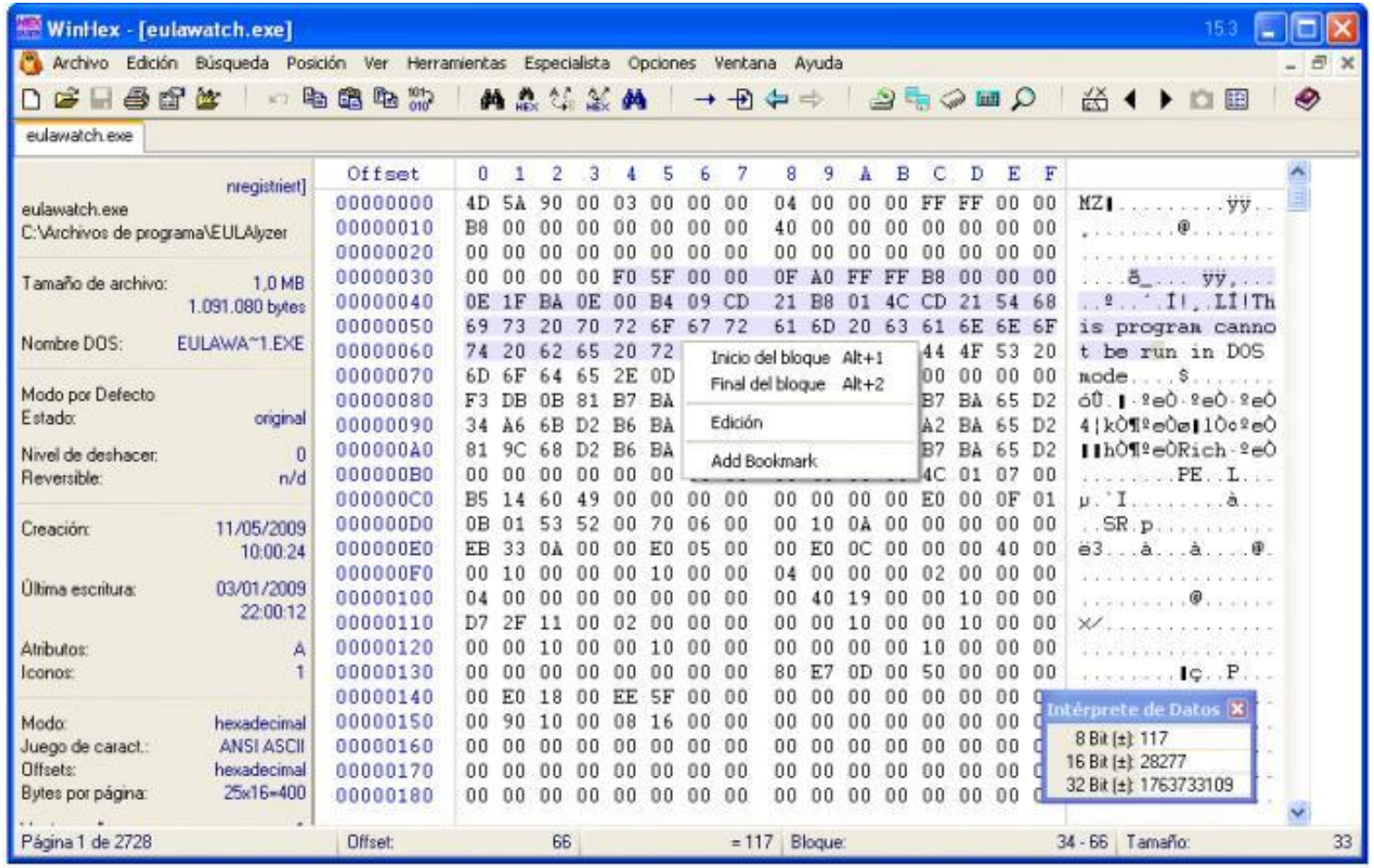
# ENCASE


Raw Search Selected
Name
C:\Users\Steve Salinas\Documents\EnCase\Search\ExampleSearch.Keywords
Search entry slack
Skip contents for known files
Undelete entries before searching
Use initialized size
Keywords
Add Keyword List
Selected 8/8
Split Mode
Edit
New
Delete
Keywords
Name
Search Expression
GREP
Case Sensitive
Whole Word
ANSI Latin - 1
Unicode
1 Distribution Distribution YES YES
2 Meeting Meeting YES YES
3 Conflict Conflict YES YES
4 Discussion Discussion YES YES
5 Soda Soda YES YES
6 Jane Doe Jane Doe YES YES
7 Janice Doe Janice Doe YES YES
8 John Doe John Doe YES YES
OK
Cancel

# WINHEX


WinHex
Software para informática forense y recuperación de archivos, Editor hexadecimal de Archivos. Apropiado también para peritaje informático, procesamiento de datos de bajo nivel y seguridad informática. Inspecciona archivos binarios, recupera datos borrados o perdidos en unidades dañadas. Un editor hexadecimal es capaz de mostrar completamente el contenido de cada tipo de archivo. A diferencia de un editor de texto, uno hexadecimal incluso muestra los códigos de control y el código ejecutable, usando un número de dos dígitos basado en el sistema de numeración hexadecimal.

# WINHEX


WinHex - [eulawatch.exe]
Archivo Edición Búsqueda Posición Ver Herramientas Especialista Opciones Ventana Ayuda
eulawatch.exe
nregistriert]
eulawatch.exe
C:\Archivos de programa\EULAlyzer
Tamaño de archivo: 1,0 MB 1.091.080 bytes
Nombre DOS: EULAWA~1.EXE
Modo por Defecto
Estado: original
Nivel de deshacer: 0
Reversible: n/d
Creación: 11/05/2009 10:00:24
Última escritura: 03/01/2009 22:00:12
Atributos: A
Iconos: 1
Modo: hexadecimal
Juego de caract.: ANSI ASCII
Offsets: hexadecimal
Bytes por página: 25x16=400
Offset 0 1 2 3 4 5 6 7 8 9 A B C D E F
00000000 4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00
00000010 B8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00
00000020 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000030 00 00 00 00 F0 5F 00 00 0F A0 FF FF B8 00 00 00
00000040 0E 1F BA 0E 00 B4 09 CD 21 B8 01 4C CD 21 54 68
00000050 69 73 20 70 72 6F 67 72 61 6D 20 63 61 6E 6E 6F
00000060 74 20 62 65 20 72 44 4F 53 20
00000070 6D 6F 64 65 2E 0D 00 00 00 00
00000080 F3 DB 0B 81 B7 BA B7 BA 65 D2
00000090 34 A6 6B D2 B6 BA A2 BA 65 D2
000000A0 81 9C 68 D2 B6 BA B7 BA 65 D2
000000B0 00 00 00 00 00 00 4C 01 07 00
000000C0 B5 14 60 49 00 00 00 00 00 00 00 00 E0 00 0F 01
000000D0 0B 01 53 52 00 70 06 00 00 10 0A 00 00 00 00 00
000000E0 EB 33 0A 00 00 E0 05 00 00 E0 0C 00 00 00 40 00
000000F0 00 10 00 00 00 10 00 00 04 00 00 00 02 00 00 00
00000100 04 00 00 00 00 00 00 00 00 40 19 00 00 10 00 00
00000110 D7 2F 11 00 02 00 00 00 00 00 10 00 00 10 00 00
00000120 00 00 10 00 00 10 00 00 00 00 00 00 00 10 00 00
00000130 00 00 00 00 00 00 00 00 80 E7 0D 00 50 00 00 00
00000140 00 E0 18 00 EE 5F 00 00 00 00 00 00 00 00 00 00
00000150 00 90 10 00 08 16 00 00 00 00 00 00 00 00 00 00
00000160 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000170 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000180 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Inicio del bloque Alt+1
Final del bloque Alt+2
Edición
Add Bookmark
Intérprete de Datos
8 Bit [±]: 117
16 Bit [±]: 28277
32 Bit [±]: 1763733109
Página 1 de 2728
Offset: 66
= 117
Bloque: 34 - 66
Tamaño: 33

# WINHEX

Estas son algunas de las características clave de "WinHex":

Clonación de disco, creación de imágenes de disco:

· Es útil para producir duplicados exactos de discos/unidades, por ejemplo, para guardar el tiempo para una instalación completa del sistema operativo y otro software para varios ordenadores y discos del mismo tipo, o para restaurar una instalación en ejecución en caso de pérdida de datos/Windows dañado (restauración de una copia de seguridad). También es útil para especialistas forenses en informática, debido a que necesitan trabajar en una copia al buscar pruebas en el disco de objeto. Puedes clonar directamente, o desde un archivo de imagen. Menú: Herramientas | Herramientas de disco | Clonar discos

# WINHEX


WinHex

Editor de RAM:

· Por ejemplo, para la depuración (programación), para examinar y manipular cualquier programa en ejecución y, en particular, videojuegos (cheating). Herramientas | Editor de RAM

Análisis de archivos:

· Por ejemplo, para determinar el tipo de datos recuperados como cadenas de clúster perdidas por ScanDisk o chkdsk. Ejemplos: Herramientas | Analizar archivos

# WINHEX

Borra archivos o discos confidenciales:

· así que nadie (tampoco los informáticos de análisis forense) podrá recuperarlos. Para borrar un archivo de modo seguro utiliza el Administrador de archivos | Eliminar irreversiblemente. Para limpiar el disco abre el disco con el editor de disco y utiliza Editar | Rellenar sectores de disco. Por ejemplo, rellena con cero bytes (valor hexadecimal 00) o bytes aleatorios. WinHex funciona de acuerdo con la norma en DoD 5220.22-M. Consulta X-Ways Security.

# WINHEX

**Borra el espacio no utilizado y el margen de retraso:**

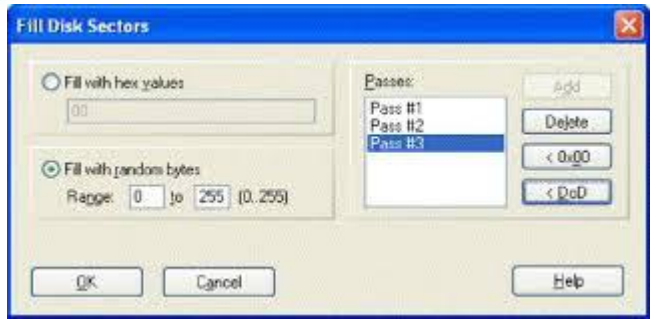
·para cerrar pérdidas de seguridad, destruir con seguridad los archivos clasificados previamente existentes que han sido eliminados de la manera tradicional, o reducir el tamaño de las copias de seguridad de los discos (como copias de seguridad de WinHex o Norton Ghost), ya que el espacio inicializado puede ser comprimido en 99%. En las unidades NTFS, WinHex incluso se ofrecerá a limpiar todos los registros de archivo $Mft (tabla maestra de archivos) que no se utilizan actualmente debido a que todavía pueden contener nombres y fragmentos de archivos previamente almacenados en ellos. El espacio no utilizado puede encontrarse en el final no utilizado del último clúster asignado a un archivo, que generalmente contiene rastros de los archivos previamente existentes. El margen de retraso - como todo lo demás - está procesado por WinHex muy rápido. Consulta X-Ways Security.

# WINHEX

Edita convenientemente la estructura de datos:
· Utiliza plantillas personalizadas. Descarga un tutorial. Vista | Administrador de plantillas

División de archivos que no caben en un disco:
· Administrador de archivos | Dividir/Concatenar
· WinHex como una herramienta de aprendizaje y reconocimiento
Estarás sorprendido al encontrar texto eliminado hace tiempo en los archivos DOC. Descubre lo que varios programas de software guardan en sus archivos. Estudia formatos de archivo desconocidos y aprende cómo funcionan. Investiga, por ejemplo, cómo están estructurados los archivos ejecutables y cómo se cargan en la memoria RAM. Las posibilidades son prácticamente ilimitadas. Aquí es otra importante:
·

# WINHEX




Manipula archivos guardados del juego:
· para cualquier juego de ordenador, siguiendo las instrucciones existentes desde sitios que engañan en Internet o para el desarrollo de tus propios trucos.

Actualización de máquina de discos MP3 y Microsoft Xbox con una unidad de disco duro más grande:
· Para actualizar el nuevo disco duro debe estar preparado en primer lugar. Esto es donde necesitas WinHex. Ofrece instrucciones para Nomad MP3 jukebox de Creative, DAP jukebox y Microsoft Xbox. También puedes cambiar el nombre de tu Xbox.

# WINHEX

Manipulación de texto:

· que uno no debería modificar, por ejemplo en archivos binarios. No es conveniente, pero es posible traducir prácticamente cualquier software en otro lenguaje de edición de texto en los archivos ejecutables, por ejemplo, si el código fuente no está disponible (por ejemplo, se pierde). O deseas editar texto en archivos de cierto tipo binario que la aplicación no permite modificar. Por ejemplo, los programadores pueden encontrar que su compilador crea automáticamente un archivo de configuración de su proyecto cuyo nombre de archivo (nombre de la aplicación + cfg) entra en conflicto con un archivo que su propio software utiliza. Si tus leyes locales y la licencia lo permiten, edita el archivo ejecutable del compilador que funciona sin problemas (por ejemplo, con la extensión de nombre de archivo "CNF").

· Visualiza y manipula archivos que usualmente no se pueden editar porque están protegidos por Windows (por ejemplo, el archivo de intercambio, archivos temporales de Internet Explorer), mediante el editor de disco. Herramientas | Editor de discos

# WINHEX

- Visualiza y manipula archivos que usualmente no se pueden editar porque están protegidos por Windows (por ejemplo, el archivo de intercambio, archivos temporales de Internet Explorer), mediante el editor de disco. Herramientas | Editor de discos.

# WINHEX

Visualiza, edita y repara áreas del sistema:
· como el registro de arranque maestro con sus sectores de inicio y la tabla de partición. Herramientas | Editor de disco | Botón de acceso

Oculta datos o descubre los datos ocultos:
· por ejemplo, detrás del supuesto final de archivos JPG (esteganografía), o en partes no utilizadas de unidades lógicas o discos físicos. WinHex admite específicamente el acceso a sectores excedentes que no están en uso por el sistema operativo ya que no se agregan a un clúster o cilindro.

# WINHEX

Copia y pega:

· Utiliza copiar y pegar o copiar y escribir (= sobrescribir) con archivos, discos y RAM. Puedes copiar libremente desde un disco y escribir el contenido del portapapeles en un disco, sin relación con los límites del sector.

Opciones de deshacer ilimitadas:

· Al editar, invierte cualquiera de sus pasos. Está limitado sólo por el espacio disponible en el disco. Editar | Deshacer

Salta atrás y adelante:

· WinHex mantiene un historial de tus saltos y te permite volver atrás e ir adelante en la cadena, como un navegador de Internet. Posición | Anterior/siguiente

# WINHEX

Secuencias de comandos:

· Edición automatizada de archivos mediante secuencias de comandos, para acelerar las tareas rutinarias recurrentes o llevar a cabo ciertas tareas en ordenadores remotos desatendidos. La capacidad de ejecutar secuencias de comandos otras que las secuencias de comandos de ejemplo suministradas se limita a los titulares de una licencia profesional. Las secuencias de comandos se pueden ejecutar desde el centro de inicio o la línea de comandos. Mientras se ejecuta una secuencia de comandos, puedes presionar Esc para cancelar. Con su amplia gama de aplicaciones, las secuencias de comandos reemplazan la función de rutina conocida desde las versiones anteriores de WinHex. Obtén más información acerca de las secuencias de comandos en la ayuda del programa.

# WINHEX


API (interfaz de programación de aplicaciones):

· Los usuarios profesionales pueden también hacer buen uso de las avanzadas capacidades de WinHex en sus propios programas escritos en Delphi, C o C++ o Visual Basic. La API de WinHex proporciona una interfaz cómoda para el acceso aleatorio a archivos y discos (a nivel de sector). Las funciones proporcionadas son similares a los comandos de secuencias de comandos.

# WINHEX

Recuperación de datos:
· para archivos eliminados erróneamente o generalmente después de una experimentada pérdida de datos. Se puede realizar manual o automáticamente. Hay un modo de recuperación automática de unidades FAT12, FAT16, FAT32 y NTFS llamado "Recuperación por nombre de archivo" que simplemente requiere que se especifique una o más máscaras de archivo (como GIF, John*DOC, etc.). WinHex hará el resto. A través del menú del botón de acceso, un mecanismo de recuperación está disponible para unidades FAT que vuelve a crear estructuras de directorio anidadas completas. Otro mecanismo ("Recuperación de archivos por tipo," antiguamente "recuperación de archivo") se puede utilizar en cualquier sistema de archivos y recupera todos los archivos de un tipo determinado en un momento

# WINHEX

Verificación del ordenador/forense:

· WinHex es una herramienta invaluable en manos de especialistas en investigación informática en la empresa privada y la aplicación de la ley.

# WINHEX

**Descarga de confianza (un problema de seguridad):**

· Al transferir material no clasificado desde una unidad de disco duro clasificada a los medios no clasificados debes estar seguro de que un archivo copiado no tendrá ninguna información extraña en ningún grupo o sector copiado falsamente junto con el archivo real, ya que este espacio todavía puede contener datos clasificados desde un tiempo cuando fue asignado a otro archivo. El comando Herramientas | Especialista en herramientas | Copia exactamente copia el archivo en su tamaño actual, no todos los sectores o grupos. Ni un byte más allá del final del archivo se copiará en el disco de destino. Minimiza tus riesgos de IT. Requiere una licencia de especialista.

# WINHEX

Cifrado de 128 bits:
· para hacer que los archivos no se puedan leer por otros. Editar | Convertir

Cálculo de la suma de comprobación/recopilación:
· para asegurar de que un archivo no está dañado y no fue manipulado, o para identificar archivos conocidos comunes. Herramientas | Calcular el hash

Generación de datos seudoaleatorios:
· para diversos fines (por ejemplo, simulación científica). Editar | Llenar el archivo

# WINHEX

Para utilizar WinHex necesitas:

* Sistema operativo: XP / 2000 / Vista / 2003 / 7

Link de descarga:
http://www.mediafire.com/?i47wlane54spuc5

Manual de Winhex:
http://www.mediafire.com/?7nd6c5fek87mmfp