Software para informática forense y recuperación de archivos "Winhex"

Espinoza Cruz Cristian Ignacio
Universidad Mayor De San Andrés
Carrera De Informática
Simulación de Sistemas
tiancris@hotmail.com

RESUMEN

Tener todos los bits de su ordenador al alcance de la mano se ha convertido en una realidad. WinHex es un editor hexadecimal universal, y al mismo tiempo posiblemente la más potente utilidad de sistema jamás creada. Apropiado para informática forense, recuperación de archivos, peritaje informático, procesamiento de datos de bajo nivel y seguridad informática.

Palabras clave

Digests, checksums.

1. INTRODUCCIÓN

La edición de es un potente software informático forense, con numerosas características forenses, transformándola así- en una poderosa herramienta de análisis de disco duro: la captura de espacio libre, el espacio de holgura, el espacio entre la partición, y el texto, la creación de un completamente detallado contenido de los discos de mesa con todos los archivos existentes y borrados y directorios e incluso secuencias de datos alternativas (NTFS), y mucho más.

Incorpora varios mecanismos de recuperación automática de archivos y permite recuperar los datos manualmente convenientemente. WinHex proporciona búsquedas rápidas y simultáneas que puede usar para examinar los medios de comunicación (o archivos de imagen) incluidos, los de holgura, para los archivos borrados, los datos ocultos y mucho más. Vía acceso físico, esto se puede realizar incluso si el volumen es indetectable por el sistema operativo por ejemplo debido a un sistema de archivos corruptos.

2. INFORMACIÓN GENERAL

2.1 Características

- Editor de discos (lógicos y físicos; soporta FAT, NTFS, Ext2/3, ReiserFS, Reiser4, UFS, CDFS, UDF).
- Editor de RAM (una manera de editar la memoria virtual de otros procesos).
- Edición de estructuras de datos mediante plantillas.
- Concatenar, partir, unir, analizar y comparar archivos.
- Funciones de búsqueda y remplazo especialmente flexibles.
- Clonado de discos.
- Imágenes de discos (comprimibles o divisibles en archivos de 650 MB).
- Automatización de la edición de archivos.
- Sofisticado mecanismo de deshacer y backup par discos y archivos.
- Encriptación de 128 bits, digests de 256 bits, CRC32, checksums.
- Borrado irreversible de datos confidenciales.
- Importación de todos los formatos de portapapeles.
- Formatos de conversión: Binario, HexaASCII, Intel-Hex y Motorola.

2.2 Editores Hexadecimales

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 (p.e. los caracteres de salto de línea y retorno) y el código ejecutable, usando un número de dos dígitos basado en el sistema de numeración hexadecimal.

Considere un byte como una secuencia de 8 bits. Cada bit puede ser un 0 o un 1, luego toma uno de dos estados posibles. Por lo tanto un byte puede tener 2•2•2•2•2•2•2•2 = 28 = 256 valores diferentes. Como 256 es el cuadrado de 16, el valor de un byte puede estar definido por un número de dos dígitos en sistema hexadecimal, donde cada dígito representa un cuarteto (o nibble) de un byte, es decir, 4 bits. Los dieciséis dígitos utilizados en el sistema de numeración hexadecimal son 0-9, A-F.

2.3 Bytes Significativos

Los microprocesadores difieren en la posición del byte menos significativo. Los procesadores Intel®, MIPS®, National Semiconductor y VAX lo colocan en primer lugar. Un valor multi-byte se almacena en la memoria desde el valor de byte más pequeño hasta el mayor. Por ejemplo, el valor hexadecimal 12345678 se guarda como 78 56 34 12. Este formato se conoce como littleendian (el pequeño al final).

Sin embargo, los procesadores Motorola et Sparc colocan el byte menos significativo en último lugar. Un valor multi-byte se almacena desde el valor mayor hasta el más pequeño. Por ejemplo, el valor hexadecimal 12345678 se guarda como 12

Cantidad de memoria adicional por cada macro:	0.5 KB
Número máximo de ventanas:	1000 (WinNT/2000), 500 (Win9x/Me)
Tamaño máximo de archivo o disco:	≈2000 GB
Número máximo de instancias simultáneas del programa:	99
Número máximo de posiciones:	limited by RAM only
Número máximo de entradas de teclado reversibles:	65535
Complejidad de encriptación:	128 bit
Longitud de los digest en los backups:	128/256 bit
Juegos de caracteres soportados:	ANSI-/IBM-ASCII, EBCDIC, Unicode (limited)
Presentación del offset:	hexadecimal/decimal

Figura 1. Especificaciones técnicas

34 56 78. Este formato se conoce como bigendian (el grande al final).

2.4 Consideraciones Técnicas

- En la mayoría de las ocasiones, una barra de progreso muestra el porcentaje completado de una operación. Sin embargo, durante las operaciones de búsqueda y reemplazo, indica la posición relativa en el archivo o disco actual.
- La interfaz de usuario tiene mejor aspecto si no se utiliza el tamaño de fuente extra grande en su sistema Windows.
- WinHex espera que su sistema esté funcionando en modo little-endian.
- Las claves que se especifican para operaciones de encriptación/desencriptación se guardan en el disco duro. En caso de que la opción de seguridad correspondiente esté activada, la clave se almacena encriptada en la RAM durante el tiempo que WinHex esté funcionando.
- Las operaciones de búsqueda y reemplazo generalmente funcionan más rápido si está activada la opción para distinguir mayúsculas de minúsculas y no se utilizan comodines.

3. FUNCIONES IMPORTANTES

3.1. Editor de archivos y editor de la memoria RAM

WinHex es un editor binario avanzada que proporciona acceso a todos los archivos, los grupos, sectores, bytes, aperitivos, y los bits dentro de su computadora. Es compatible con practicamente ilimitada y tamaños de disco hasta la region de terabytes (miles de gigabytes)! Uso de la memoria es mi-nimo. La velocidad de acceso es de primera categoria.

3.2. Examinar directorios para FAT, NTFS, Ext2/Ext3, ReiserFS, CDFS/ISO9660, UDF

Similar y tan facil de usar como el derecho del Explorador de Windows de la lista a mano. Este navegador de listas existentes, asi como archivos y directorios eliminados, con todos los detalles. Permite a la lista de cadenas de agregacion, para desplazarse a los archivos y directorios en el editor de discos, y copiar archivos de la unidad. Obras de archivos de imagen y las particiones, incluso si no está ¡Montado en Windows, debido a la ayuda nativa del sistema de archivos!

3.3. La clonacion de disco / imagen de disco en DOS y Windows

WinHex produce copias sector mas racional de los tipos de medios de comunicacion, ya sea a otros discos (clones, espejos) o archivos de imagen, utilizando el acceso al disco fisico o logico. Las copias son forense de sonido, que incluyen todo el espacio de holgura y de todo el espacio libre. Muy importante para los examinadores forenses, ya que permite trabajar en la copia. Los archivos de imagen, opcionalmente, se puede comprimir o dividir en archivos independientes. WinHex silencio puede generar archivos de registro que tomara nota de cualquier sector dañado que encuentre durante la clonacion. WinHex te permite verificar la integridad y autenticidad de los archivos de imagen antes de su restauración.

3.4. Recuperación de Datos

Con su editor de discos sofisticado, WinHex no solo provee la recuperación del archivo manual. WinHex es también capaz de recuperar automáticamente los archivos o incluso toda la estructura de directorios anidados. Existen varios mecanismos de recuperación de datos integrada:

a) Recuperación de archivos por nombre. Simplemente especifique una o varias mascaras de archivos (como *. gif, Smith *. doc, etc) y han WinHex hacer el resto. Trabajos en FAT12, FAT16, FAT32 y NTFS.

b) Recuperación de archivos por tipo. WinHex puede recuperar todos los archivos que pueden ser reconocidos por una determinada firma de archivo de encabezado (por ejemplo, archivos JPEG, documentos de MS Office). Esto funciona en prácticamente todos los sistemas de archivos.

c) Con el navegador del directorio antes mencionado se puede recuperar convenientemente y de forma selectiva los archivos listados y directorios.

d) Hay un modo especial de recuperación automática para FAT y NTFS unidades, accesible desde el menú del botón de acceso.

3.5. Editor de Disco

El editor de disco, que forma parte del menú Herramientas, permite acceder a disquetes y discos duros por debajo del nivel del sistema de archivos. Los discos consisten de sectores (por lo común unidades de 512 bytes). Se puede acceder al disco de manera lógica (controlada por el sistema operativo) o física (controlada por la BIOS). En la mayoría de los ordenadores se puede acceder incluso a unidades CD-ROM y DVD.

4. MODOS DE EDICIÓN

4.1. Modo de sólo lectura

Recomendado para la computadora los exámenes forenses. Los archivos o discos abiertos en este modo no pueden ser editados, sólo examinados. En otras palabras, están protegidos contra escritura.

4.2. Modo de edición por defecto

Las modificaciones de los archivos o discos abiertos en este modo se guardan en archivos temporales. Estos son creados dinámicamente. El comando "Guardar" del menú Archivo actualiza el archivo original o el disco.

4.1. Modo de edición directa

Sea cuidadoso cuando abra archivos o discos en este modo. Todas las modificaciones (entradas desde teclado, llenar/borrar bloques, pegar el portapapeles, reemplazos, etc.) se escriben directamente en el archivo original sin confirmación. No es necesario guardar el archivo manualmente después de haberlo modificado. En vez de eso, los cambios se guardan constante y automáticamente (por última vez al cerrar la ventana). De cualquier modo, puede utilizar el comando Guardar para asegurarse de que el buffer es vaciado en un momento determinado.

El modo de edición directa es recomendable en aquellos casos en que la transferencia de datos entre el archivo temporal y el original (y viceversa) consuma demasiado tiempo o espacio en disco. Este puede ser el caso al abrir muchos archivos grandes o cuando edite enormes cantidades de datos. Como no se necesitan archivos temporales en este modo de edición, generalmente es más rápido que el modo por defecto. El modo de edición directa es el único disponible cuando se utiliza el editor de RAM.

Incluso en el modo de edición directa la creación de un archivo temporal es inevitable cuando se altera el tamaño de un archivo.

5. CONSEJOS ÚTILES

- Si selecciona un bloque con el ratón, puede pulsar dos veces el botón derecho para anularlo.
- Puede definir un bloque de datos utilizando el teclado (SHIFT+arrow keys o ALT+1 y ALT+2).
- Use la tecla TAB para cambiar del modo hexadecimal al de texto y viceversa.
- Use la tecla INS para cambiar del modo overwrite al de insert y viceversa.
- CTRL+Q cierra todas las ventanas.
- ENTER muestra el Start Center.
- ESC aborta la operación en curso si la hay, en caso contrario anula la selección de bloque, se activará una ventana de dialogo.
- PAUSE detiene o continúa la operación en curso. SHIFT+F7 alterna entre los juegos de caracteres. (SHIFT+)ALT+F11 repite el último comando Mover Bloque.
- ALT+F2 re calcula el auto-hash después de que un fichero haya sido modificado.

6. CONCLUSIONES

WinHex es un instrumento de análisis forense en la recuperación y el análisis de la información digital. Se ha probado y validado la versión profesional y ha demostrado ser precisa y confiable en sus informes. Se tiene el más alto nivel de confianza en la eficacia WinHex digital en casos forenses.

La integración con el Explorador de Windows permite abrir muchos archivos de forma rápida y convenientemente para evaluar rápidamente lo que tengo. Que siga mejorando pues es un producto ejemplar. Un gran producto confiable y libre de errores.

7. REFERENCIAS

[1] X-Ways Software Technology AG,
http://www.x-ways.net/corporate/index-m.html

[2] Software Para Informática Forense,
http://www.x-ways.net/winhex/index-m.html

[3] Documento de Referencia Manual,
http://www.x-ways.net/winhex.zip