Eliminación de datos del disco duro

Sumi Espinal Elizabeth
Universidad Mayor De San Andrés
Carrera De Informática
Simulación de Sistemas
ely_sum@yahoo.es

RESUMEN

En este trabajo se describe la forma de eliminar los datos de los Discos Duros de forma segura y definitiva, utilizando herramientas de informática forense como Eraser y Active KillDisk.

Palabras clave

Informática Forense, Eliminación de datos, Formatear, Disco Duro, Eraser,Active KillDisk.

1. INTRODUCCIÓN

La informática (o computación) forense es la ciencia de adquirir, preservar, obtener y presentar datos que han sido procesados electrónicamente y guardados en un medio computacional. Desde 1984, el Laboratorio del FBI y otras agencias que persiguen el cumplimiento de la ley empezaron a desarrollar programas para examinar evidencia computacional.

La informática forense está adquiriendo una gran importancia, debido al aumento del valor de la información y la utilización que se le da a la misma. Es por esto que cuando se realiza un crimen, muchas veces la información queda almacenada en forma digital. Aunque la mayoría de la gente tenga claro que un simple borrado no es suficiente, muchos creen que un formateado del disco impedirá la recuperación de los datos. Y esto no es así, existen diversas herramientas que permiten recuperar ficheros de un disco formateado con excelentes resultados. Por tanto, necesitamos algo que vaya más allá de un simple formateo, algo que nos permita eliminar datos de un disco duro definitivamente.

Antes de continuar con el próximo apartado, debemos de considerar la intencionalidad con la que una determinada persona desea borrar los datos de un disco duro, generalmente suele ser con la finalidad de evitar u obstaculizar la integridad de la evidencia digital, si se ve inmerso en un proceso judicial.

Por esta razón es necesario considerar que la información que se otorga acá está enfocado a describir las opciones que un usuario común y corriente tiene para escoger una herramienta que le sea útil para realizar el proceso de borrado de su disco duro.

Ahora, veamos de una forma casera, si vale el término, porque queremos borrar sin dejar ningún indicio cualquier contenido de nuestro computador. Cuando vamos a deshacernos del PC, ya sea que lo vendamos o lo regalemos, es importante borrar todos los datos.

Esto es útil para un particular, pero es realmente crítico para los bancos y empresas.

Por lo tanto hay que asegurarse de haber borrado total de los datos de los discos duros para impedir que datos confidenciales sean recuperados por otros.

Como mencionamos anteriormente un simple borrado o formateo no es suficiente, y mostraremos un ejemplo para mostrar esta situación.

Efectivamente, si bien es cierto que el formateo vuelve a cero al disco, éste no lo vuelve completamente a cero.

Veamos el caso de un disco en el que hemos escrito los bits: 0101.

Entonces, lo formateamos (lo llenamos de ceros) en el disco duro habrán puros ceros.

Pero vemos que donde antes habían 1, los 0 aún tienen un magnetismo residual. Este magnetismo puede ser leído con equipos especializados (existen empresas especializadas en este tipo de recuperación de datos).

De esto se puede deducir que antes habían los datos 0101 a pesar del formateo.

Ahora consideremos otro ejemplo que nos muestra que incluso se pueden recuperar datos, aun cuando se hayan escrito encima. Por ejemplo, en el disco del caso precedente, si escribimos 0011.

Los dos 1 no tienen el mismo magnetismo: uno es más fuerte que el otro. Por lo que podemos deducir lo que había antes. Lo mismo para los dos ceros.

Resultado: Podemos deducir el magnetismo precedente (0101) a pesar que hemos escrito ceros (0000) y luego otros datos (0011).

Por lo tanto es posible en ciertos casos recuperar antiguos datos de un disco duro, a pesar de haberlo formateado y de haber escrito encima nuevos datos. (Pero esto sólo se puede hacer con equipos especiales).

De aquí que sea importante que encontremos métodos eficaces para borrar completamente el disco duro.

Como información, la armada americana funde sus discos

duros para asegurarse que nadie pueda recuperar los datos contenidos en él.

Otros utilizan aparatos que generan un potente campo magnético pero destruyen al mismo tiempo el disco duro. Todos no disponemos de estos medios, pero felizmente existen programas que hacen lo necesario.

2. ELIMINACIÓN DE DATOS DEL DISCO DURO

La eliminación de datos del disco duro, no es sólo apretar el botón de eliminación o la opción de formateo, estas opciones no aseguran la eliminación de los datos de manera definitiva, existe la posibilidad de que los datos sean recuperados por otras personas, las cuales pueden utilizar esta información recuperada para distintos fines o interés propio, perjudicando así a el/los dueño(s) de la información.

Cuando los archivos son borrados o suprimidos en DOS, Win9x, WinNT/2000, etc., el contenido de los archivos no es verdaderamente borrado. A menos que se utilice algún software especial que ofrezca un alto grado de seguridad en el proceso de eliminación, los datos "borrados", permanecen en un área llamada espacio de almacenamiento no-asignado (Unallocated File Space) Unallocated File Space es el área llamada espacio de almacenamiento no-asignado . Igual sucede con el file slack asociado al archivo antes de que éste fuera borrado. Consecuentemente, siguen existiendo los datos, escondidos pero presentes, y pueden ser detectados mediante herramientas de software para el análisis de la computación forense.

Para eliminar la información definitivamente del disco duro podemos usar una herramienta llamada Eraser, active KillDisk, etc.

Los dos 1 no tienen el mismo magnetismo: uno es más fuerte que el otro. Por lo que podemos deducir lo que había antes. Lo mismo para los dos ceros.

Resultado: Podemos deducir el magnetismo precedente (0101) a pesar que hemos escrito ceros (0000) y luego otros datos (0011).

Por lo tanto es posible en ciertos casos recuperar antiguos datos de un disco duro, a pesar de haberlo formateado y de haber escrito encima nuevos datos. (Pero esto sólo se puede hacer con equipos especiales).

De aquí que sea importante que encontremos métodos eficaces para borrar completamente el disco duro.

Como información, la armada americana funde sus discos duros para asegurarse que nadie pueda recuperar los datos contenidos en él.

Otros utilizan aparatos que generan un potente campo magnético pero destruyen al mismo tiempo el disco duro. Todos no disponemos de estos medios, pero felizmente existen programas que hacen lo necesario.

2. ELIMINACIÓN DE DATOS DEL DISCO DURO

La eliminación de datos del disco duro, no es sólo apretar el botón de eliminación o la opción de formateo, estas opciones no aseguran la eliminación de los datos de manera definitiva, existe la posibilidad de que los datos sean recuperados por otras personas, las cuales pueden utilizar esta información recuperada para distintos fines o interés propio, perjudicando así a el/los dueño(s) de la información.

Cuando los archivos son borrados o suprimidos en DOS, Win9x, WinNT/2000, etc., el contenido de los archivos no es verdaderamente borrado. A menos que se utilice algún software especial que ofrezca un alto grado de seguridad en el proceso de eliminación, los datos "borrados", permanecen en un área llamada espacio de almacenamiento no-asignado (Unallocated File Space) Unallocated File Space es el área llamada espacio de almacenamiento no-asignado . Igual sucede con el file slack asociado al archivo antes de que éste fuera borrado.

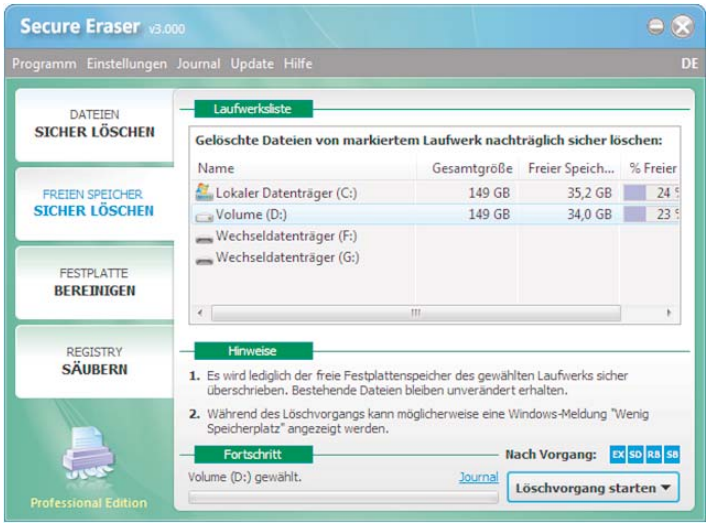

Figura 1. Herramienta Eraser

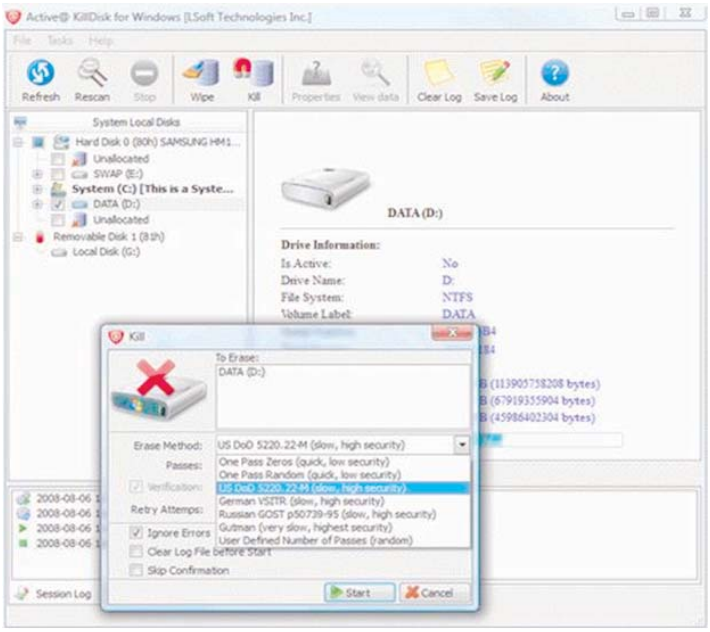

Figura 1. Herramienta Active KillDisk

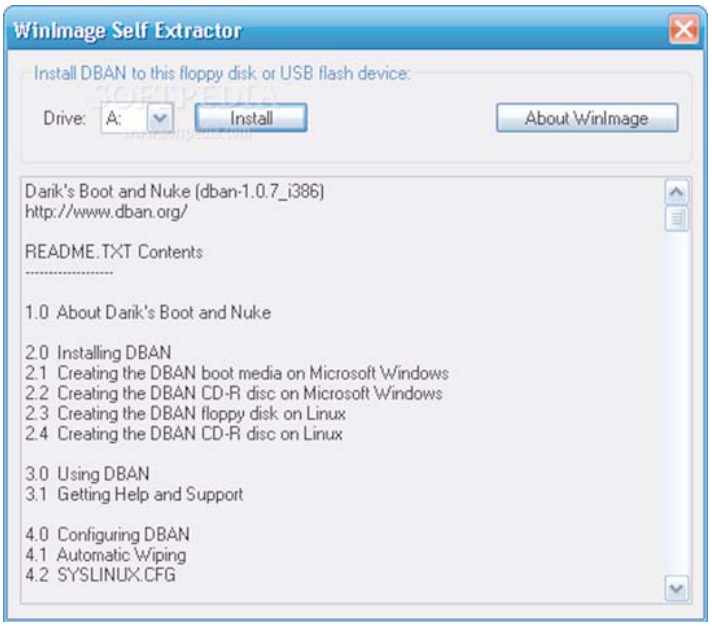

Figura 3. Herramienta Dark's Boot and Nuke

Consecuentemente, siguen existiendo los datos, escondidos pero presentes, y pueden ser detectados mediante herramientas de software para el análisis de la computación forense.

Para eliminar la información definitivamente del disco duro podemos usar una herramienta llamada Eraser, active KillDisk, etc.

Active KillDisk es una herramienta diseñada para eliminar los datos de un disco rígido, de manera segura.

Si deseamos eliminar la información almacenada en un disco rígido, debemos apuntar directamente a la partición que la contiene. Existen muchas herramientas para realizar esta tarea, pero pocas que aseguran que los datos no se vuelven a recuperar. Una de las que asegura la inaccesibilidad de tales datos, es Active KillDisk.

Esta herramienta trabaja en el mismo nivel de las particiones existentes y por lo tanto, no deja rastro de su actividad después de eliminar los datos.

Active KillDisk soporta todos los tipos de controladoras, como IDE, SATA y SCSI. Además, trabaja con todos los tipos de particiones de ficheros, como FAT, NTFS, EXT, entre otras.

Para trabajar con dicha herramienta, se la debe copiar en un CD ó diskette y luego debe ser ejecutada en la fase de booteo del ordenador.

Para el final ponemos a consideración el programa Darik's Boot and Nuke permite utilizar Mersenne-Twister para borrar los discos duros. Este es una mini-distribución Linux que cabe en un disquete (o un CD). Sólo hay que arrancar el PC desde él y lanzar el borrado del disco. Este software soporta los discos XT, IDE, PATA, SATA y SCSI.

Para el archivo EXE (para disquete/USB), se ejecuta, insertando el disquete o memoria USB, seleccionando el lector correspondiente y haz clic en el botón "Install". Esto va a escribir sobre el disquete o la memoria USB. Se debe grabar el archivo ISO con el programa de grabación de costumbre.

Arrancar el PC desde el disquete, memoria USB o CD. En la pantalla, presionar simplemente ENTER.

Esperar que termine el arranque. Al cabo de un momento, aparecerá la pantalla siguiente. (Cuando aparece esta pantalla, ya puedes retirar el disquete/llave USB/Cd).

Presionar la tecla M y selecciona el método "PRNG Stream" (con las flechas arriba/abajo y ENTER).

Presionar R, entra el valor 8 (=número de pasadas) y presionar ENTER.

Luego, seleccionar el disco duro, presionando SPACE. Ahora presiona F10 para iniciar el borrado de datos y espera que termine la operación.

Es sumamente advertir que se borrará todo el disco duro (archivos, particiones…todo!). Es decir que la recuperación de datos será imposible.

Después de la última pasada de datos aleatorios, el disco es borrado con ceros.

3. CONCLUSIONES

La forma de como eliminar los datos o información de los Discos Duros es muy importante, porque no basta solo eliminar o formatear la información, sino que se debe utilizar Herramientas apropiadas, esto es esencial para realizar una eliminación segura y definitiva de la información confidencial.

Hemos visto 2 herramientas para entorno gráfico, pero como sabemos la mejor forma de hacer actividades cercana al hardware es mejor trabajar con software para entorno de texto o línea de comandos y el último software descrito cumple con esas características.

4. REFERENCIAS

[1] Sitio Web: http://www.genbeta.com/windows/como-eliminar-datos-del-disco-duro-definitivamente Consultado en: 10/09/09

[2] Sitio Web: http://www.ontrackdatarecovery.es/software-disco-duro/dataeraser.aspx

Consultado en: 09/09/09

[3] Sitio Web: http://www.dosbit.com/2009/04/06-secure-eraser-destrucción-segura-de-los-archivos-y-carpetas-alojados-en-el-sistema

Consultado en: 07/09/09