Incursionando en la recuperación de datos con PC Inspector File Recovery

Ricaldi Canaviri Pedro
Universidad Mayor De San Andrés
Carrera De Informática
Simulación de Sistemas
pedro_mc@hotmail.com

RESUMEN

Una de las grandes dificultades que enfrenta un usuario surge cuando accidentalmente borra un archivo de suma importancia y la situación inesperada nos lleva al límite de la desesperación por revertir el accidente ocasionado, es en este punto donde surgen varios programas para la recuperación de archivos, también utilizados como herramientas en Informática Forense, pero al encontrarlos lo frustrante pondría resultar el no saber como utilizarlos. A partir de este problema, el presente artículo tiene como objetivo la enseñanza del manejo para la recuperación de archivos con el programa PC Inspector File Recovery.

Palabras clave

FAT, Tabla de asignación de archivos, Unidades Lógicas

1. INTRODUCCIÓN

En la Informática Forense los investigadores utilizan programas de recuperación de archivos para buscar y restaurar datos borrados. Estos programas localizan los datos que el ordenador a marcado como eliminados pero que aun no han sido sobrescritos.

A continuación se explicara como utilizar el programa PC Inspector File Recovery, este es un programa el cual sirve para recuperar datos ya sean borrados accidentalmente o luego de un formateo del disco duro.

2. ALMACENAMIENTO DE ARCHIVOS EN LE DISCO DURO

Una pregunta muy hecha por usuarios no muy metidos en el tema es, ¿como se pueden recuperar los datos, si ya han sido borrados?

Es una pregunta, muy escuchada, pero tiene respuesta

Cuando nosotros borramos un archivo del sistema, lo que hacemos es borrar su dirección de la tabla de asignación de archivos, es decir, el sistema pierde la ubicación física del archivo en el disco duro, de modo que no tiene más acceso a este porque no sabe en donde está, pero la información continúa en el disco duro, hasta que sea reemplazada al copiar, mover o crear un archivo.

La información es perdida en su totalidad, si luego de eliminar el archivo, se desfragmenta el disco.

Vamos a profundizarnos más en este tema, a modo simbólico, para poder tener una noción mejor de lo que vamos a hacer. El disco duro de nuestro sistema esta dividido en pistas y sectores, como si fuera una torta, con muchísimas porciones (ver figura 1)

Podemos identificar como SEC, a los sectores (las porciones), y a PISTA como las pistas, que son líneas circulares a lo largo de todo el disco.

Cuando nosotros creamos, copiamos o movemos un archivo, un registro de este se crea en la Tabla de Asignación de archivos, o más conocida como FAT.

Supongamos que copiamos una foto de un CD a nuestro disco duro, el sistema lo que hará es buscar un lugar o lugares libres en el disco duro libre, y meterá en el archivo (ver figura 2).

Ahora, el archivo ya está guardado en el disco duro, pero cuando nuestro sistema operativo quiera acceder a el, ¿como sabe donde está?

La Tabla de Asignación de archivos, guarda su dirección, digamos que tiene un registro de todos los ficheros para que cuando Windows quiera acceder, La FAT le diga en que parte está, (ver figura 3).

Se puede ver como la Tabla de asignación de archivos, guarda la ubicación de todos los ficheros.

Cuando nosotros eliminamos un archivo, el sistema borra la línea de dicho archivo de la FAT, y si formateamos la unidad, se regenera toda la FAT, es decir el archivo permanece en el disco, pero no registrado.

Cuando nosotros creamos algo en el disco duro, como un archivo ejecutable, el cabezal del disco duro busca la primer pista/sector que no esté registrada en la Tabla de Asignación de archivos y loo copia en esa zona, es por eso, lo que no está registrado en la FAT, es tomado como espacio libre.

Es por eso que cuando eliminamos archivos sin querer, se recomienda no tocar nada más del sistema, para no escribir encima de cuya información perdida.

Lo que los programas de recuperación de datos hacen, es intentar reconstruir parte perdida de la FAT, accediendo directamente y físicamente al disco (pistas y sectores), sin consentimiento del sistema de archivos, e intentando recuperar información.

Figura 1.

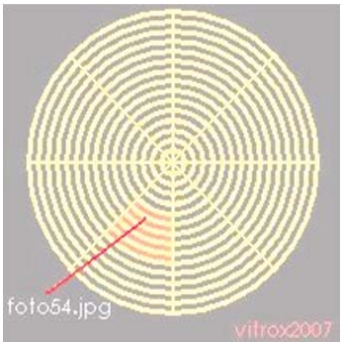

Figura 2.

Representación del disco y almacenamiento de un archivo

Se espera haber dejado claro todo esto.

3. MANEJO DEL PROGRAMA PC INSPECTOR FILE RECOVERY

Primero que nada, tendríamos que descargar el programa recuperador de datos, desde su sitio oficial (Sitio Oficial de PC Inspector File Recovery: http://www.pcinspector.de/).

Una vez que hemos descargado el fichero instalador, lo ejecutamos y lo instalamos, en cuanto terminemos la instalación, aparecerá un nuevo icono en el escritorio para iniciar el programa.

Podemos ver la pantalla principal del programa, permitiéndonos escoger el sistema de lenguaje, para toda la aplicación y sus extensiones, elegimos Spanish y hacemos click en el signo OK verde para continuar (ver figura 4).

En seguida podemos ver como PC Inspector File Recovery, nos explica de un modo gráfico y simple, las opciones del programa, entre ellas se encuentran Recuperar archivos eliminados, Encontrar datos perdidos, Encontrar la unidad perdida (ver figura 5). Es notorio como el programa, a medida que nos vamos profundizando, va explicando todo lo que se puede hacer, y entre ellas recomendaciones, y nos damos cuenta que recuperar datos es fácil y rápido.

4. RECUPERAR ARCHIVOS ELIMINADOS

Esta suele ser la opción más utilizada por los usuarios de PC Inspector File Recovery, ya que esta, como su título lo explica, permite recuperar archivos eliminados accidentalmente, como así también carpetas (sus ficheros interiores).

Inmediatamente, luego de presionar este botón, el programa

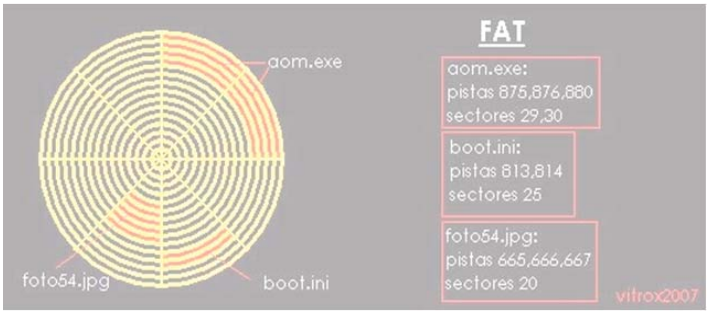

Figura 3. Tabla de asignación de archivos en la FAT

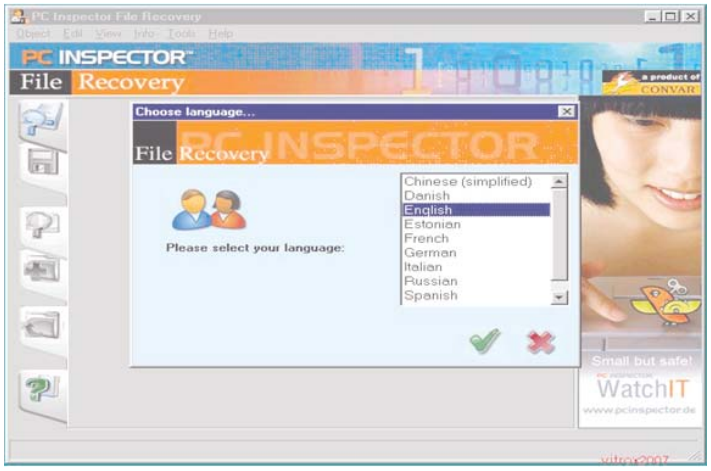

Figura 4. Pantalla principal de PC Inspector File Recovery

empezará a analizar nuestras unidades (discos duros, pendrives y disketteras), y nos mostrará una imagen como esta, de acuerdo a la cantidad de componentes conectados cuando iniciamos el programa.

Ahora, nos aparecerán todas nuestras unidades, divididas en dos secciones, las lógicas (particiones), y físicas (discos tangibles), y nosotros seleccionaremos cual inspeccionar en busca de fragmentos de archivos a recuperar, (ver figura 6).

Supongamos, que hemos eliminado archivos de la unidad D:, lo que tendríamos que hacer es hacerle click a dicha unidad en esta parte del programa, y luego apretar el botón 'Encontrar Unidades Lógicas', se abrirá una ventana (ver figura 7).

Bueno, en esta parte del programa, nos permite que seleccionemos en que zona del disco duro buscar los archivos eliminados por error para recuperar (ver figura 7), nos permite elegir un rango de tal sector a tal otro, como por ejemplo el escogido en la imagen de ejemplo.

Esta parte del proceso de recuperación, es bastante lenta, pensemos, que analizar 20GB de un disco de 80GB, tardaría

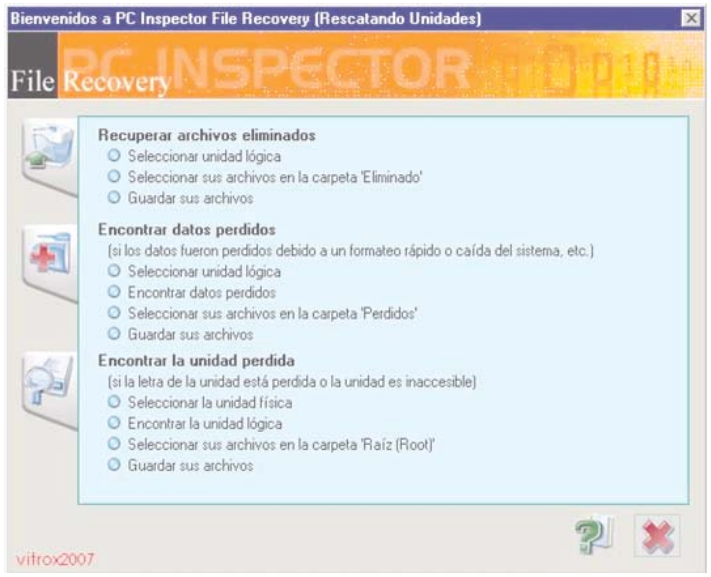

Figura 5. Opciones del programa

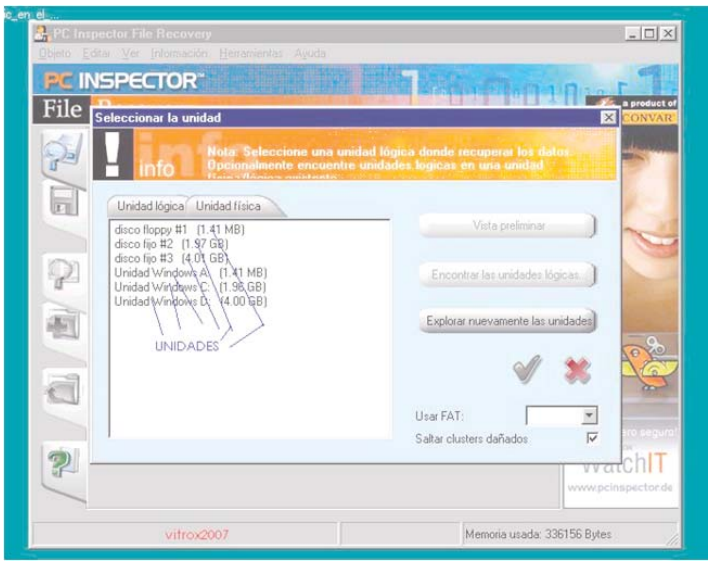

Figura 6. Selección de una unidad

Figura 7. Búsqueda de un archivo en una unidad

aproximadamente una hora, pero siempre es ideal, si es que se desea recuperar la información en perfecto estado y sin falta, analizar el disco duro completo, y aguardar esas horas de búsqueda, que nos rendirán muy bien.

Una vez que finalicemos de analizar todos los sectores, teóricamente aparecerían todas las unidades lógicas, y al entrar en algunas de ellas (con doble click), accederíamos a la zona de recuperación.

El programa ahora es una especie de explorador de Windows, de archivos eliminados.

Ahora, nos deslizaremos entre las carpetas, como si estuviéramos en nuestro disco duro sano, y buscaremos los nombres de los archivos eliminados por error.

Cuando los encontramos, tendríamos que darle con el segundo botón del ratón y luego Guardar En.

Luego elegir la ubicación en el disco donde se deberá guardar el archivo eliminado por error.

5. FUNCIONES ÚTILES E INTERESANTES DEL PROGRAMA

Si crees que el programa se acabo aquí, estas equivocado, PC Inspector File Recovery integra muchas más herramientas muy interesantes que utilizar, las veremos a continuación

Una vez que estamos ya en el explorador de archivos del programa, con el disco seleccionado, es posible buscar directamente los archivos a recuperar, es decir, supongamos que recordamos el archivo que eliminamos sin querer, este se llamaba “Auto.exe”, lo podemos buscar directamente sin estar revisando toda la unidad hasta encontrar coherencias, ¿como? desde el botón “Encontrar Archivos”.

También se puede encontrar información exacta sobre el disco duro, esto es ideal para cuando tenemos un disco duro el cual debemos colocar en una máquina relativamente vieja, esa que nos piden el número de cabezales, sectores, etc. y no lo sabemos, PC Inspector, nos informa de ello.

A esto lo podemos lograr entrando en su menú a información de unidad.

Bueno, ya tenemos la información suficiente para poder empezar a recuperar datos en modo profesional con nuestras unidades.

6. CONCLUSIÓN

Se ha podido notar que haciendo uso del programa PC Inspector File Recovery es posible recuperar archivos eliminados por accidente, lo limitante de este programa ocurre cuando el sector a donde pertenecía el archivo a recuperar haya sido sobrescrito.

PC Inspector File Recovery por su manejo es una herramienta que se utiliza en Informática forense, además de ser una herramienta de distribución libre.

Si hay formateo del sistema, no es recomendable instalar Windows para luego descargar esta aplicación y recuperar los archivos, la instalación de Windows, puede modificar todos los ficheros de los sectores a restaurar y así perder muchísima información.

7. REFERENCIAS

[1]http://www.pcinspector.de/Sites/file_recovery/info.htm?language=5

[2]http://www.fotosok.com/recuperardatos/index.htm

[3]http://www.vsantivirus.com/pcinspector.htm