PHOTOREC

INFORMÁTICA FORENSE

ANÁLISIS DE SISTEMAS

02/12/2017

PHOTOREC

INTEGRANTES

CARNET	APELLIDOS	NOMBRES
QT01132516	Quijano torres	Medvin Ricardo
MF01132606	Mejía Flores	José William
SP01132338	Sánchez Palacios	Williams Ernesto

POTHOREC CONTENIDO

PRESENTACIÓN

El análisis forense digital se corresponde con un conjunto de técnicas destinadas a extraer información valiosa de discos, sin alterar el estado de los mismos. Esto permite buscar datos que son conocidos previamente, tratando de encontrar un patrón o comportamiento determinado, o descubrir información que se encontraba oculta. En este post se introducirá el tema, así como la utilidad del mismo, ya sea dentro o fuera de una investigación.

En el presente documento se plasmará como poder hacer un análisis forense utilizando el programa PhotoRec, este es un software diseñado para para la recuperación de archivos perdidos.

incluyendo videos, documentos y archivos de los discos duros y CDRoms, así como imágenes perdidas (por eso el nombre PhotoRecovery) de las memorias de las cámaras fotográficas, MP3 players, PenDrives, etc. PhotoRec ignora el sistema de archivos y hace una búsqueda profunda de los datos, funcionando incluso si su sistema de archivos está muy dañado o ha sido re-formateado.

PhotoRec es una aplicación libre y Open Source multi-plataforma distribuida bajo Licencia Pública General GNU (GPLV v2+). PhotoRec acompaña a TestDisk, una aplicación para recuperar particiones perdidas en una amplia variedad de sistemas de archivos y que hace que los discos que no son booteables, sean booteables de nuevo.

JUSTIFICACIÓN

La presente investigación se enfocará en estudiar de la forma de hacer un análisis forense con el software PhotoRec el cual está para Linux, de esta manera podremos realizar la recuperación de información de la cual ya se cree extraviado y verificaremos la efectivad con la cual se pueden hacer las recuperaciones de los datos y está a su vez pueden servir de prueba evidentes a favor o en contra en u juzgado.

OBJETIVOS

OBJETIVO GENERAL

Determinar de qué manera se realiza un análisis forense a información almacenado dentro de una computadora utilizando el software PhotoRec, por el cual se realizarán varias pruebas para determinar su funcionalidad, vialidad, con-fiabilidad y respuesta de los datos obtenidos

OBJETIVOS ESPECÍFICOS

1. Identificar los tipos de información que se almacena en los bits.
2. Verificar los datos que se pueden recuperar dentro del análisis forense
3. Practicar la forma de recuperación de datos.

ANTECEDENTES

PhotoRec es un software de recuperación de datos de archivos diseñado para recuperar archivos perdidos, incluidos vídeo, documentos y archivos de discos duros, CD-ROM e imágenes perdidas (por lo tanto, el nombre de Photo Recovery) de la memoria de la cámara digital. PhotoRec ignora el sistema de archivos y va en busca de los datos subyacentes, por lo que seguirá funcionando incluso si el sistema de archivos de su medio se ha dañado o re formateado severamente.

PhotoRec es gratuito: esta aplicación multiplataforma de código abierto se distribuye bajo la Licencia pública general de GNU (GPLV v2 +). PhotoRec es un programa complementario a TestDisk, una aplicación para recuperar particiones perdidas en una amplia variedad de sistemas de archivos y hacer que los discos que no son de arranque se puedan volver a arrancar.

Para mayor seguridad, PhotoRec usa acceso de solo lectura para manejar la unidad o la tarjeta de memoria de la que está a punto de recuperar los datos perdidos. Importante: Tan pronto como se borre accidentalmente una imagen o archivo, o descubra que falta alguno, NO guarde más imágenes o archivos en ese dispositivo de memoria o unidad de disco duro; de lo contrario, puede sobrescribir sus datos perdidos. Esto significa que al usar PhotoRec, no debe elegir escribir los archivos recuperados en la misma partición en la que se almacenaron.

MATERIALES Y MÉTODOS

1. Área de estudio**:** Se realizará la recuperación de archivos con la ayuda del software PhotoRec de un disco duro y se procederá a la recuperación de toda la información que fue borrada y dañada y se harán capturas de pantalla para verificar que ha sido recuperado la información.

2. Materiales y equipos:

- Una computadora con Linux
- software PhotoRec
- Disco duro dañado

3. se describirán brevemente, los métodos y procedimientos que se planee usar dando, si fuera el caso, las citas bibliográficas correspondientes, si ya fueran conocidos, e indicando claramente si se trata de desarrollar nuevos métodos o procedimientos.

4. Duración:

Inicio: 06 de noviembre de 2017

Finalización: 01 de diciembre de 2017

PRESUPUESTO

DETALLE	COSTO
Depuración del equipo (3)	$ 30.00 c/u
Internet	$ 25.00
Impresiones	$ 20.00
Transporte (3)	$ 15.00
Comunicación	$ 15.00
Imprevistos	$ 50.00
TOTAL	$ 215.00

CRONOGRAMA DE ACTIVIDADES

Fecha responsable	06-11 nov.	12-17 nov.	19-25 nov.	26-1 dic.
Medvin Torres **Willian Flores** **willians Sanchez**	Buscar información del programa			
Medvin Torres **Willian Flores** **willians Sanchez**	Instalación	Perfil		
Medvin Torres **Willian Flores** **willians Sanchez**	Prueba inicial	Resolver problemas o errores	Creación de un manual de instalación	
Medvin Torres **Willian Flores** **willians Sanchez**			Pruebas finales	Entrega de documentación final

INSTALACIÓN Y USO DE PHOTOREC

Como hemos mencionado anteriormente, PhotoRec acompaña a TestDisk por lo tanto vamos a instalar lo siguiente desde una Terminal:

Para eso utilizaremos el siguiente comando: apt-get install testdisk.

```
root@palacios:/home/williams# apt-get install testdisk
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
testdisk ya está en su versión más reciente (7.0-3).
El paquete indicado a continuación se instaló de forma automática y ya no es necesario.
  linux-image-3.16.0-4-amd64
Utilice «apt autoremove» para eliminarlo.
0 actualizados, 0 nuevos se instalarán, 0 para eliminar y 0 no actualizados.
root@palacios:/home/williams#
```

El software no tiene interfaz gráfica y está en inglés, pero es muy fácil de usar y de comprender.

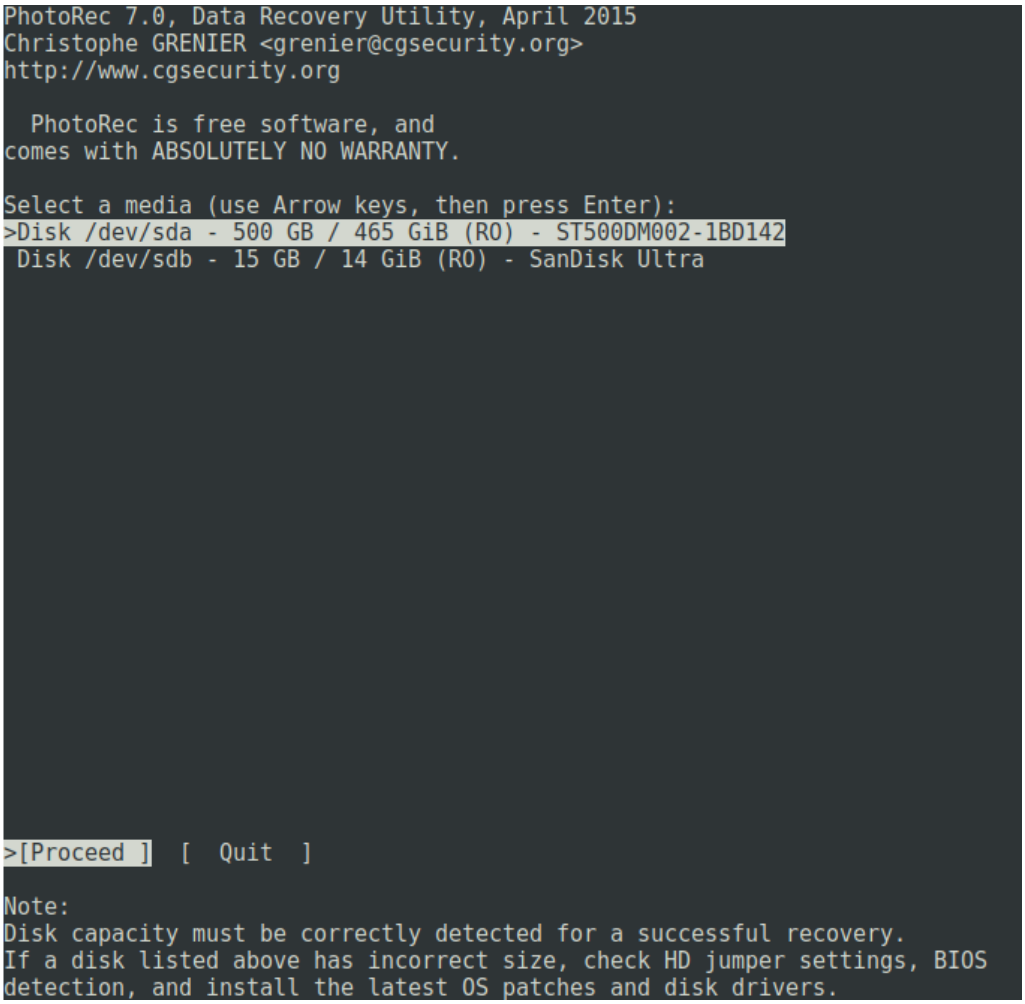
También lo podemos encontrar más información en http://www.cgsecurity.org

Proceso de recuperación de datos con PhotoRec

Iniciamos desde la Terminal el siguiente comando:

```
1# photorec
```

Nos aparecen todos los discos o memorias USB conectadas al ordenador, seleccionamos la que vamos a recuperar los datos y damos enter.



Texto 1: PhotoRec 7.0, utilidad de recuperación de datos, abril de 2015

Texto 2: Christophe GRENIER <grenier@cgsecurity.org>

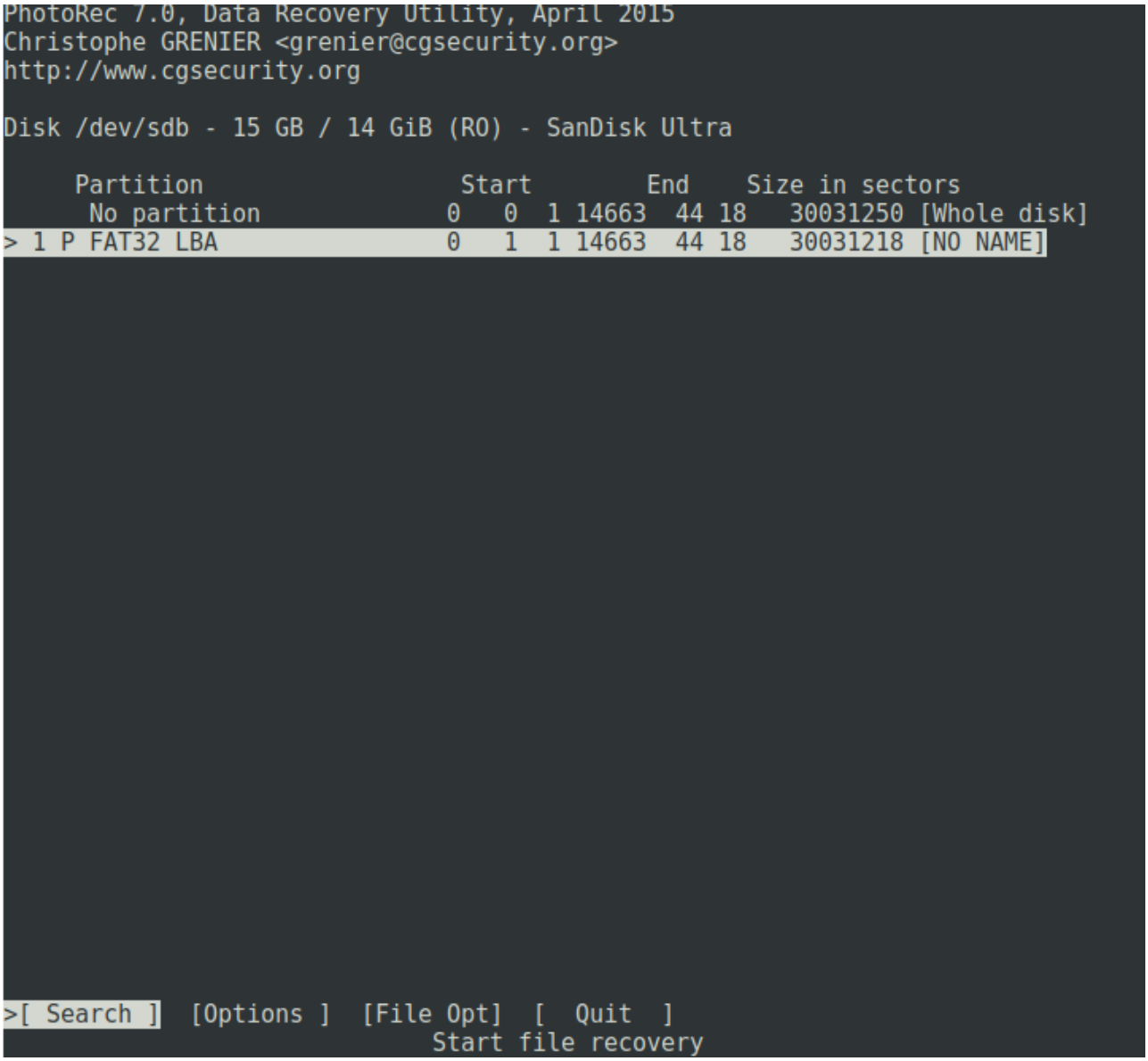
Texto 3: http://www.cgsecurity.org

Texto 4: PhotoRec es software libre, y NO CONTIENE ABSOLUTAMENTE NINGUNA GARANTÍA.

Texto 5: Seleccione un medio (use las teclas de flecha, luego presione Intro):

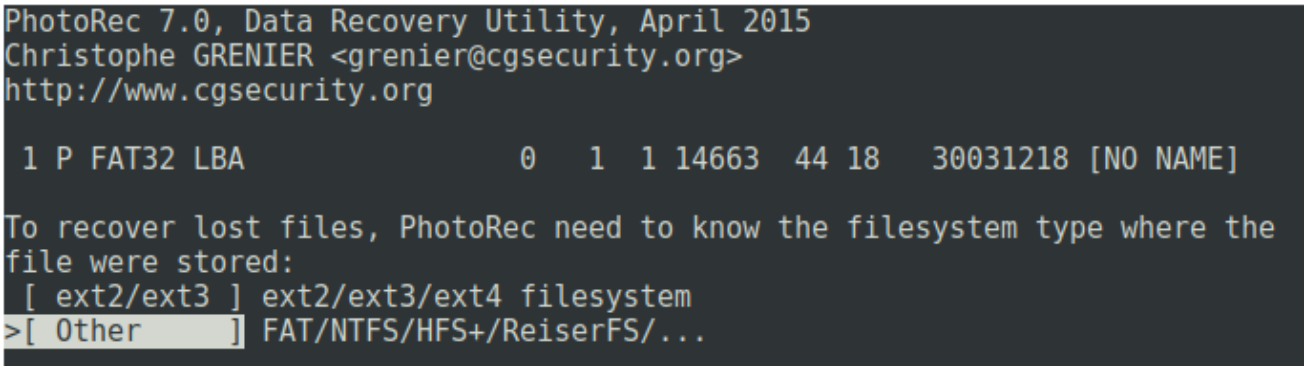
Texto 6: [Proceda] [Salir

A continuación, tendremos que seleccionar la partición a recuperar. En nuestro caso, solo tenemos una partición así que la seleccionamos y pulsamos enter.

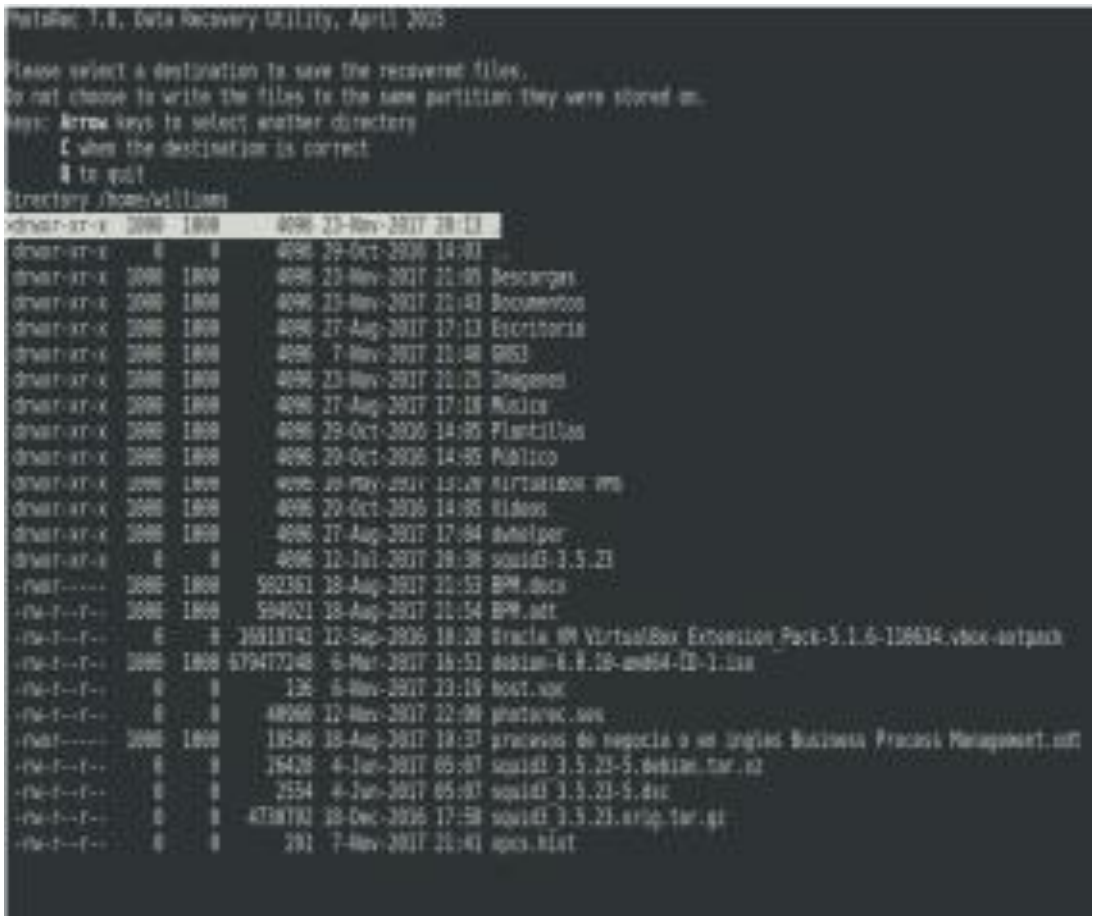


Texto 7: Disco / dev / sda - 500 GB / 465 GiB (RO) - ST500DM002-1BD142

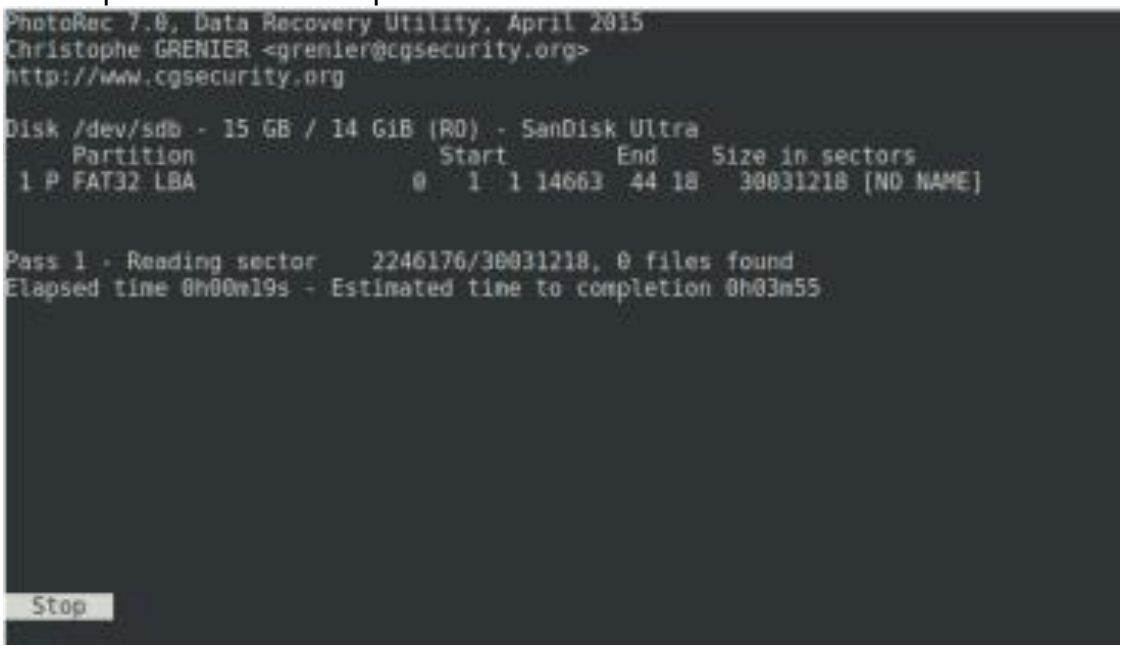
El programa a continuación nos preguntará por el sistema de archivos del disco o partición.



Ahora debemos seleccionar el destino donde guardaremos los archivos recuperados.



Ahora el sistema comenzará a buscar los archivos eliminados. El proceso tardará un buen rato dependiendo de la capacidad del disco.



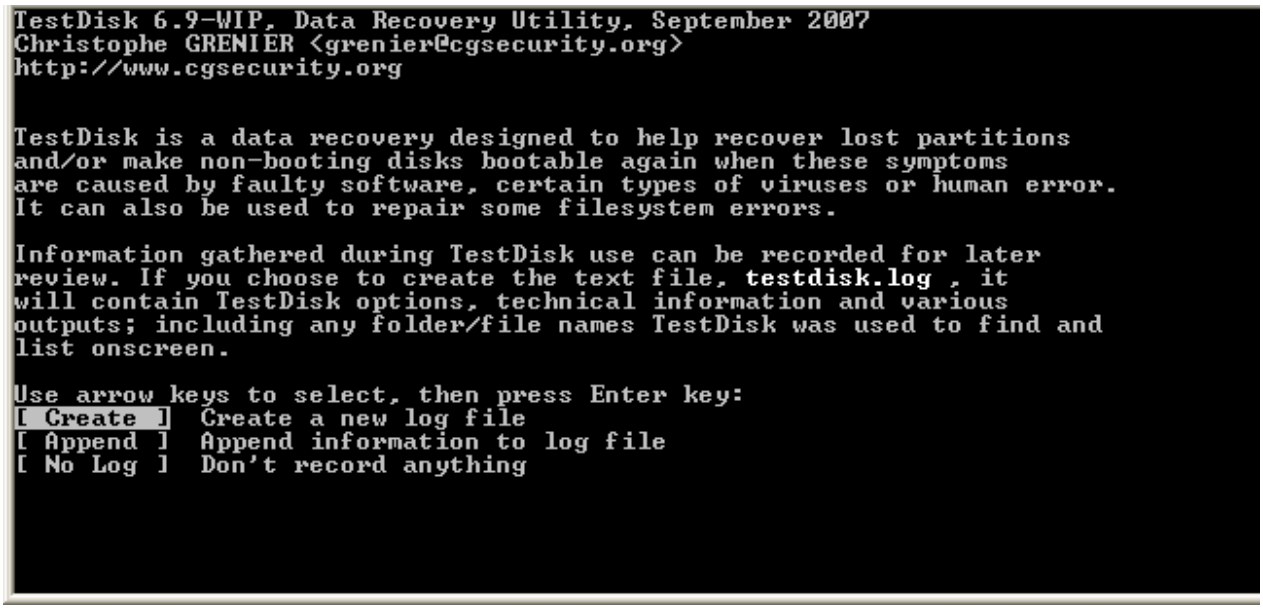
Ahora ya tenemos nuestra información recuperada y almacenada en la carpeta destino.

Proceso de recuperación de datos con TestDisk

Ahora el sistema comenzará a buscar los archivos eliminados. El proceso tardará un buen rato dependiendo de la capacidad del disco.

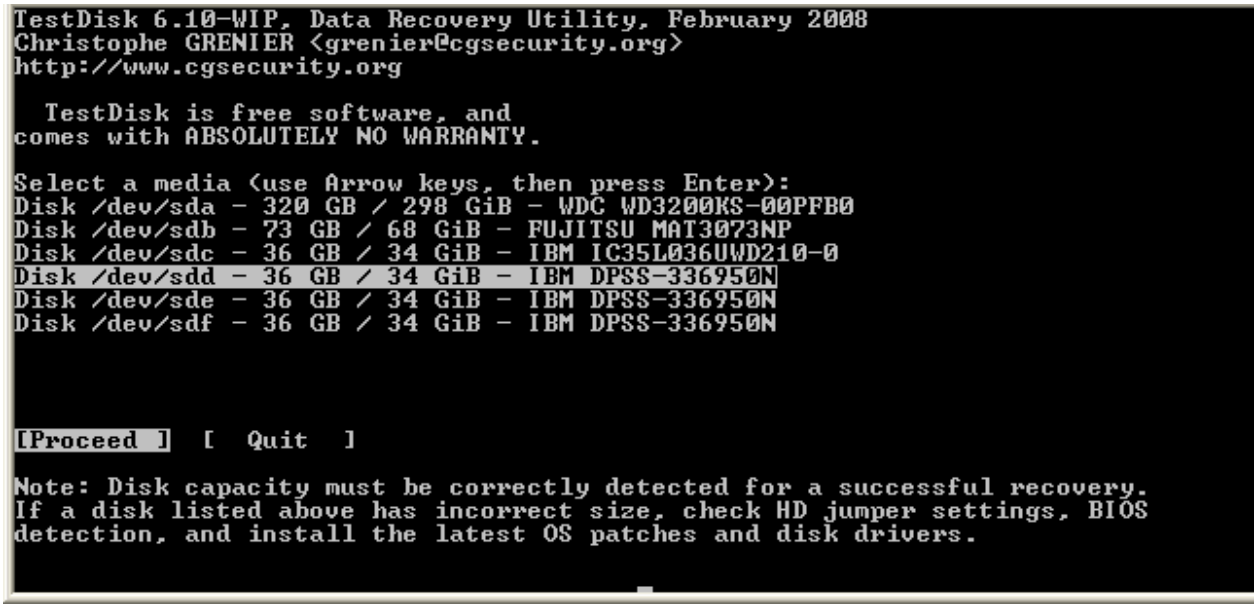
Ahora ya tenemos nuestra información recuperada y almacenada en la carpeta destino

- Seleccione Crear solamente si tiene una razón para añadir datos al registro o si se ejecuta TestDisk desde un archivo media de solo lectura y debe crearse la imagen en otro lugar.
- Presione Entrar para continuar.



Selección de disco

Todos los discos duros deben ser detectados y listados con su tamaño correcto por TestDisk:

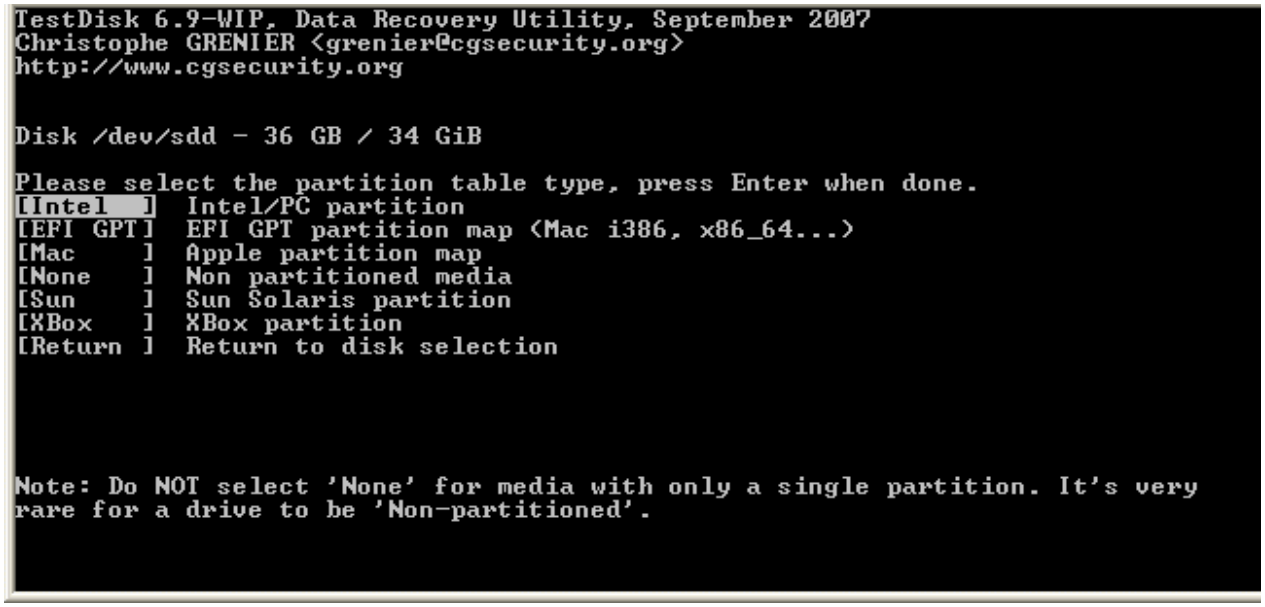


- Use las teclas flecha arriba/abajo para seleccionar su disco duro con la/s partición/es perdida/s.
- Presione Entrar para continuar.

Si está disponible, use /dev/rdisk* en un dispositivo limpio en lugar de '/dev/disk* para acelerar la transferencia de datos.

Selección del tipo de la Tabla de particiones

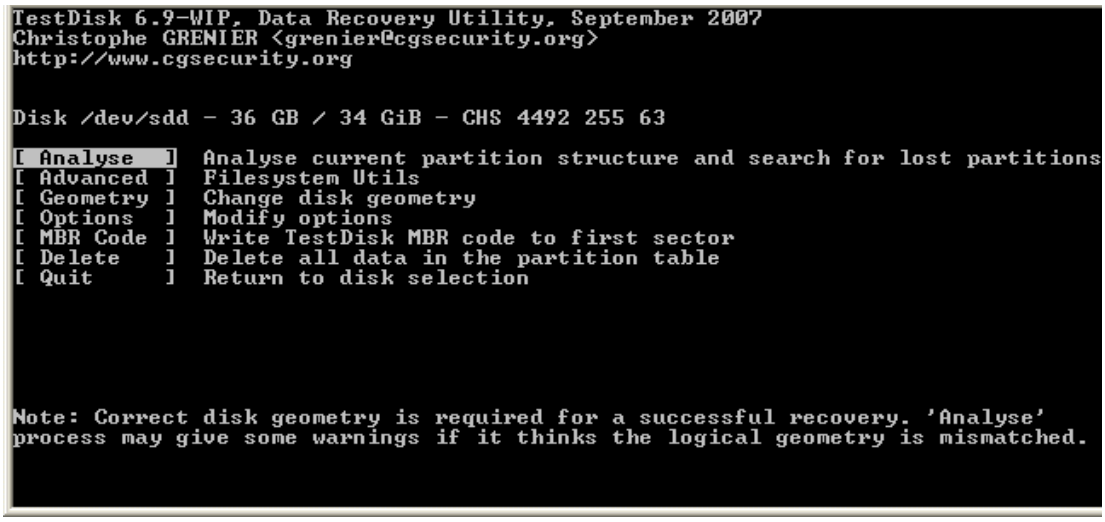
TestDisk nos muestra los tipos de Tabla de particiones.



- Seleccionar el tipo de Tabla de partición - normalmente el valor por defecto, del tipo de tabla de particiones, es el correcto como auto detecta TestDisk.
- Presione Entrar para continuar.

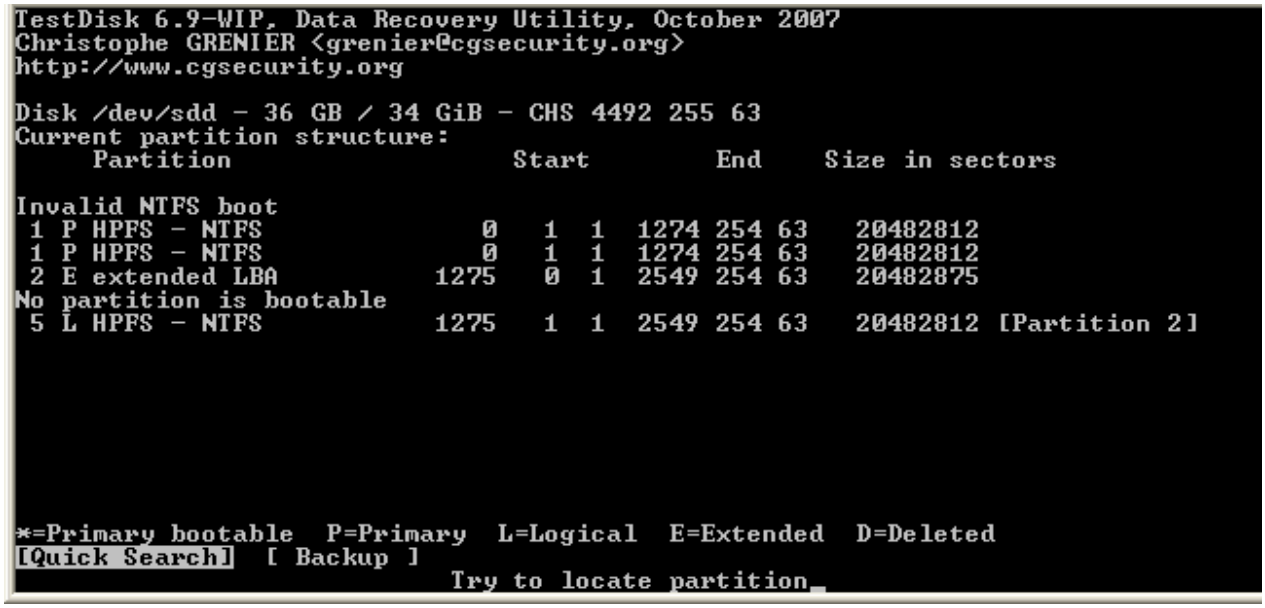
Estado actual de la tabla de particiones

TestDisk muestra los menús



- Utilice el menú por defecto "Analyse" (Analizar), para comprobar la estructura de su partición actual y buscar particiones perdidas.
- Confirmar el análisis presionando Entrar para continuar.

Ahora, se muestra la estructura de su partición actual. Examine las particiones desaparecidas y los errores en la estructura actual de sus particiones.



La primera partición está repetida en la lista por que apunta a una partición dañada o con una tabla de entrada de partición no válida.
Puntos de arranque NTFS no válidos en un sector de arranque NTFS defectuoso, por lo que esto es un sistema de archivos dañado.
Sólo una partición lógica (etiqueta de partición 2) está disponible en la partición extendida.
Una partición lógica ha desaparecido.

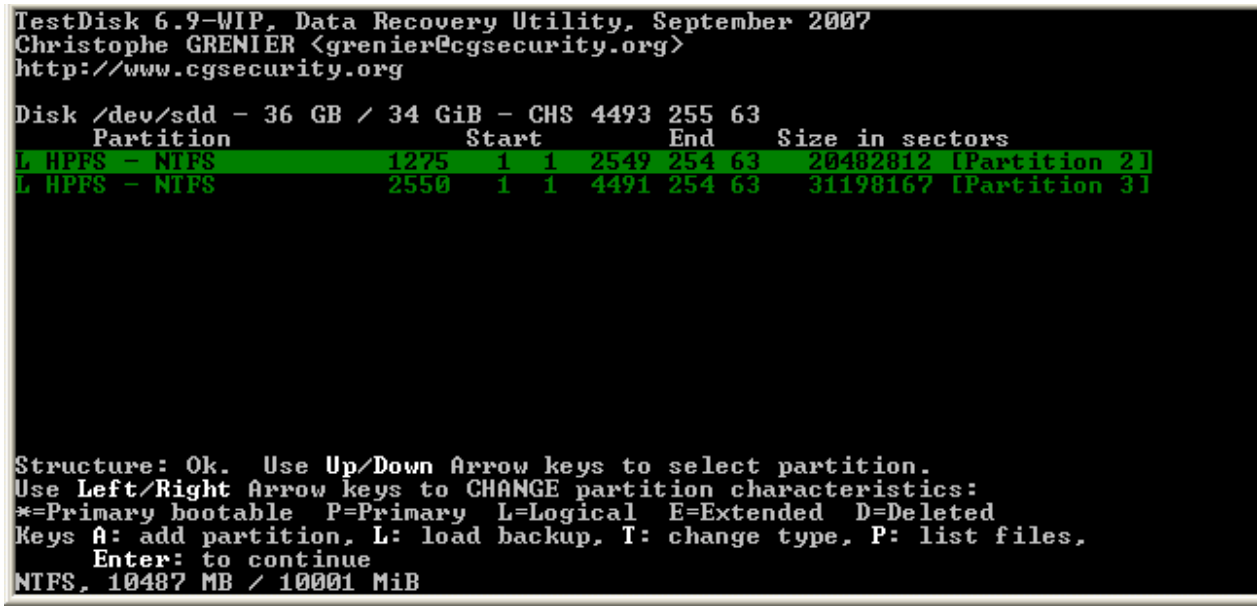
- Confirmar seleccionando ***Quick Search*** (Búsqueda Rápida) y presionar "Entrar" para continuar.

Búsqueda Rápida de particiones

- Confirme que está conforme y coincide (con su SO), el Sistema Operativo presentado, para la búsqueda rápida de particiones creadas en la unidad seleccionada bajo dicho SO, para continuar.

TestDisk muestra los primeros resultados en tiempo real.

Durante la ***Búsqueda Rápida***, TestDisk ha encontrado 2 particiones incluyendo la partición lógica desaparecida etiquetada ***Partition 3***.

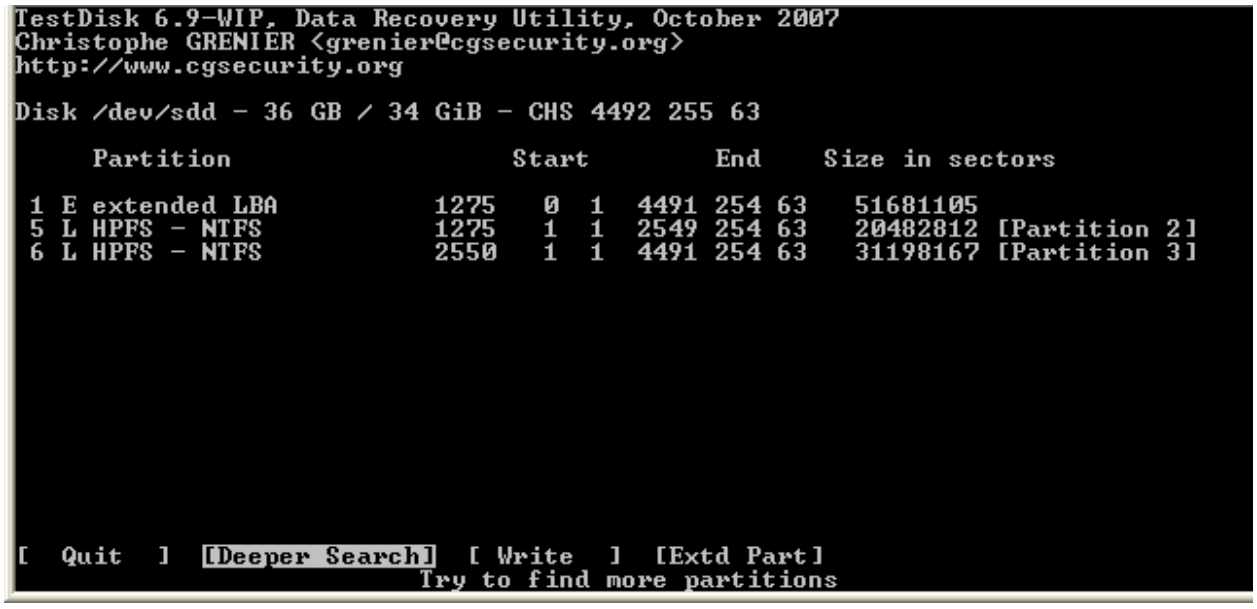


- Seleccionar la partición (queda resaltada), y presione ***p*** para listar los archivos, (para volver a la pantalla anterior, pulse ***q*** para Salir).

Todos los directorios y datos están correctamente listados.

- Presionar Entrar para continuar.

¿Guardar la tabla de particiones o buscar más particiones?

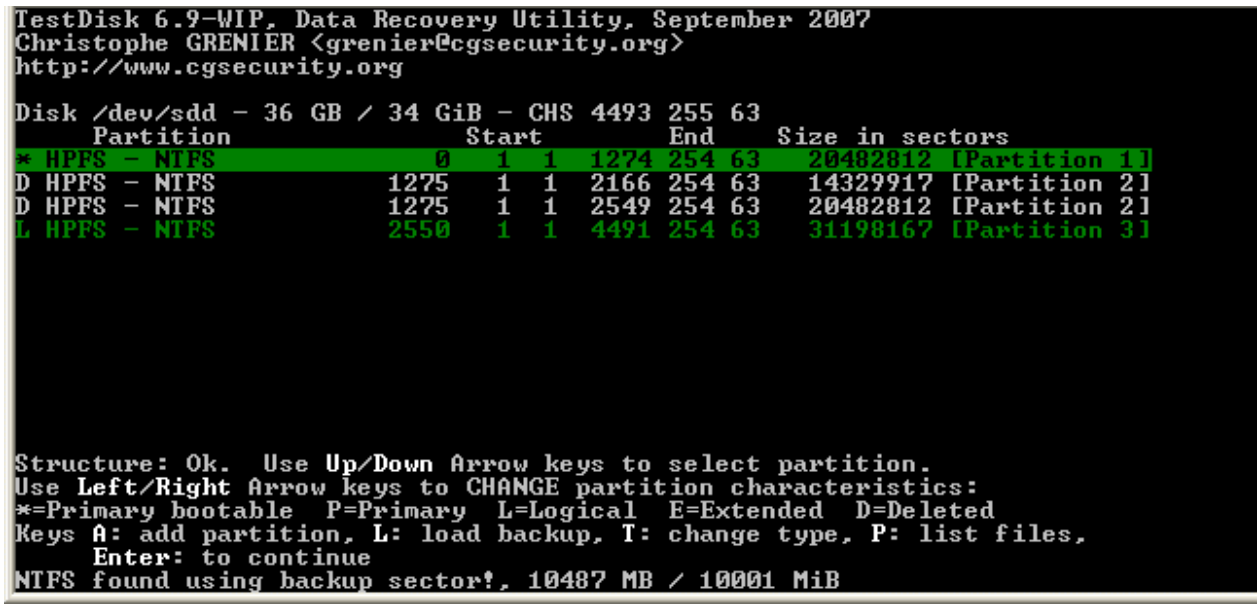


- ***Cuando todas las particiones están disponibles*** y los datos correctamente listados, puede ir al menú **Escribir** para guardar la estructura de la partición. El menú Extd Partle da la oportunidad de decidir si la partición extendida usará todo el espacio disponible en disco o sólo el espacio (mínimo) requerido.

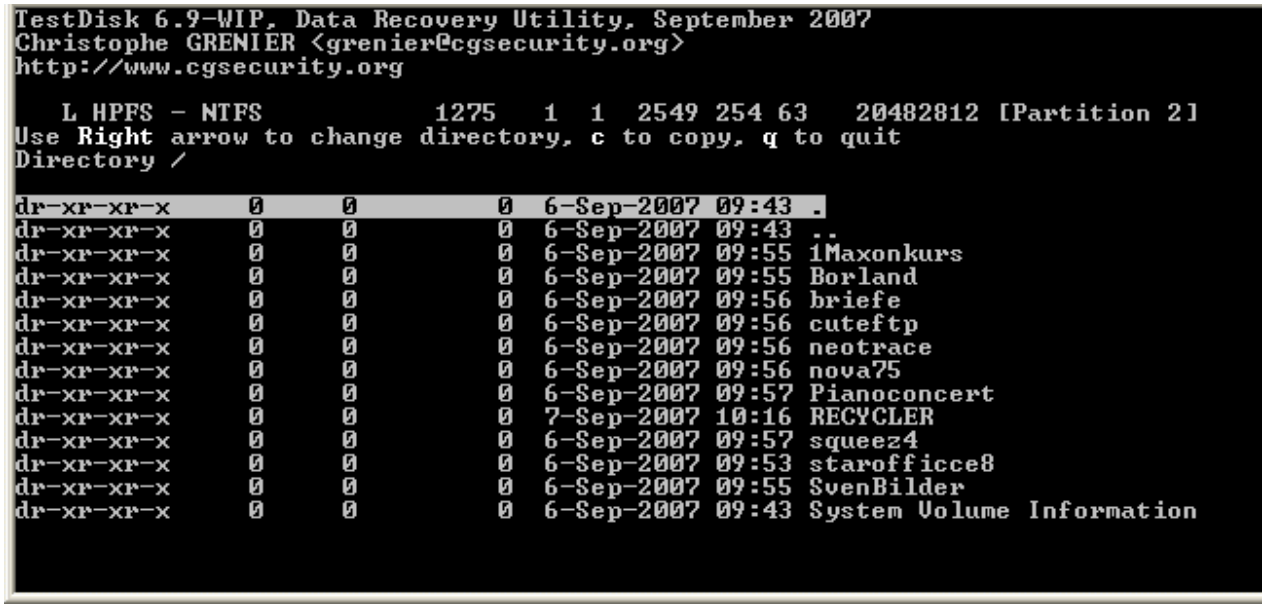
- ***Ya que una partición, la primera, todavía falta***, seleccionar el menú ***Deeper Search***(Búsqueda Profunda), (si no se realiza ya de forma automática), y Presionar Entrar para continuar.

Una partición está todavía desaparecida: Búsqueda más profunda

Después de realizar la búsqueda profunda, los resultados se muestran como sigue: La primera partición '***"Partición 1"'*** fue encontrada usando la copia de seguridad del sector de arranque. ¡En la última línea de su pantalla, puede leer el mensaje" NTFS encontrado usando la copia de seguridad del sector!***"*** Y el tamaño de su partición. La "partición 2" aparece dos veces con diferentes tamaños. Ambas particiones se enumeran con el estado ***D*** de borradas, porque se superponen una a la otra.



- Seleccione la primera partición Partición2 y presione ***p*** para listar sus datos.
- Presione ***q*** para Salir y volver a la pantalla anterior.
- Deje esta partición Partición2, con un sistema de archivos dañado, marcada como D(borrada).
- Resalte la segunda partición 2 debajo
- Presione ***p*** para listar sus archivos.



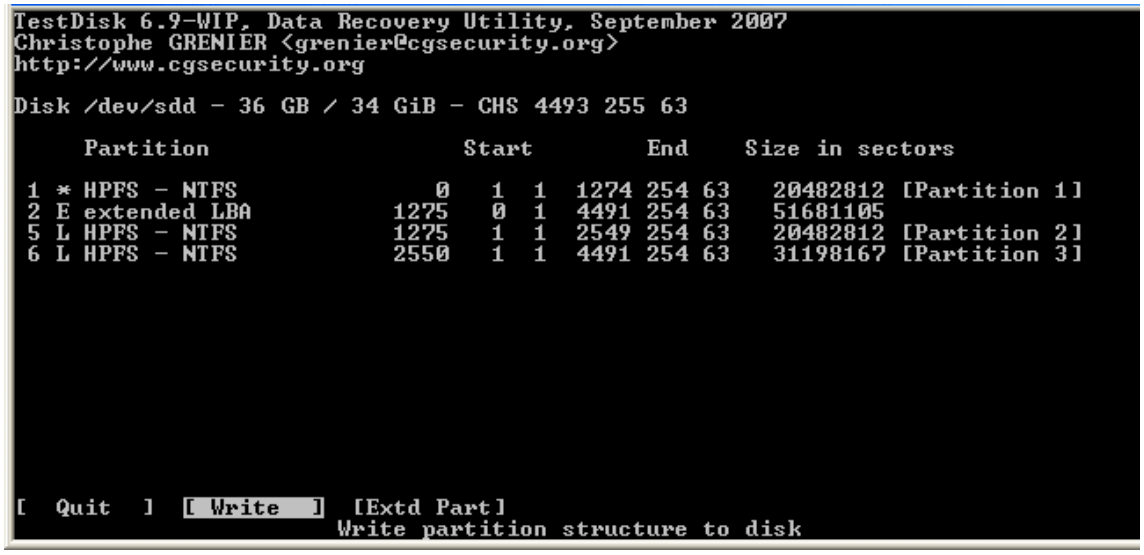
Utilice las flechas izquierdas/derecha para desplazarse entre sus carpetas y ver sus archivos de más verificaciones.

- Presione ***q*** para Salir y volver a la pantalla anterior.
- El estado de disponibilidad para las particiones Primarias es: *(Iniciable), L(Lógica) y D(Suprimida).

Usando las teclas: Flecha izquierda/derecha, cambie el estado de la partición seleccionada a ***L(Lógica)***

Recuperación de la tabla de particiones

Ahora es posible escribir la nueva estructura de la tabla de particiones.

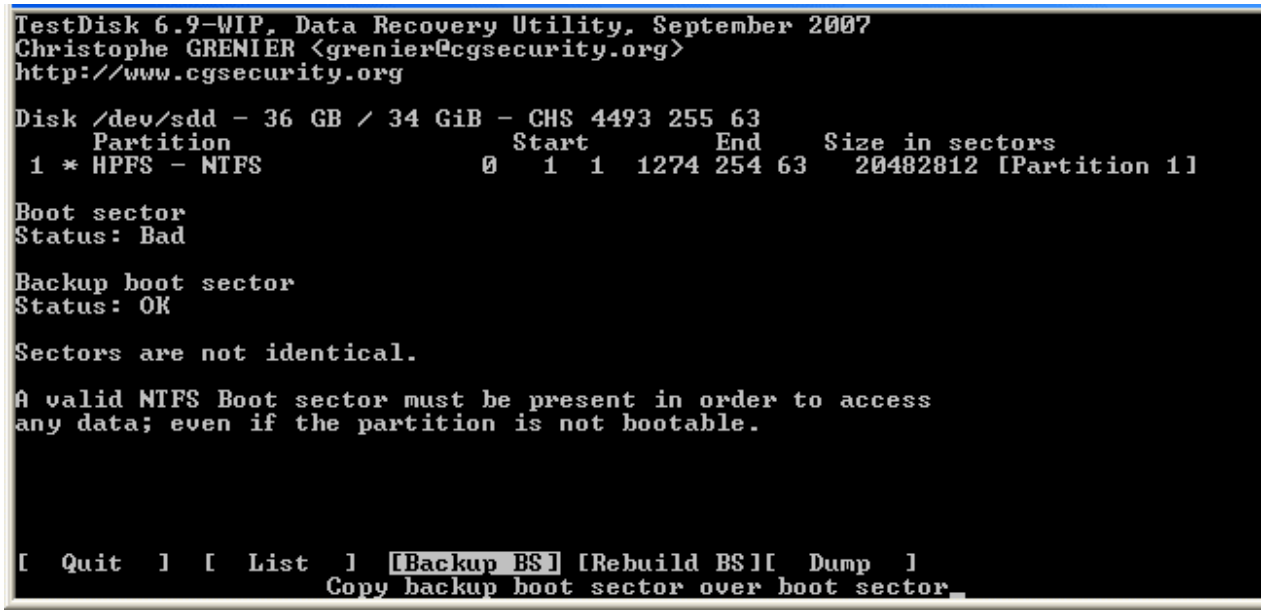


- Confirmar en ***Escribir*** presionando Entrar, y hecho.

Ahora, todas las particiones están registradas en la tabla de particiones

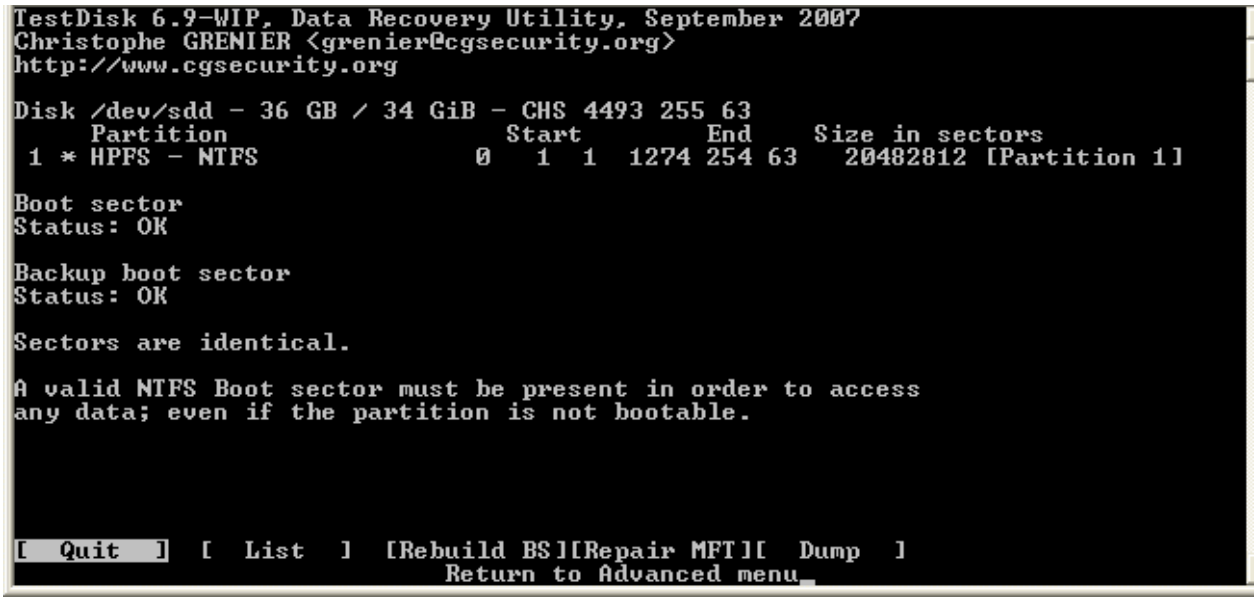
Recuperar el Sector de Arranque NTFS

El Sector de Arranque de la primera partición llamado Partition 1 está aún dañado. Es hora de arreglarlo. El estado del Sector de Arranque NTFS es malo y la copia de seguridad del Sector de Arranque es válida. Los sectores de arranque no son idénticos.



- Para sobre escribir el Sector de Arranque con la Copia de Seguridad del sector de arranque, seleccione ***Backup BS***, y validar presionando Entrar, usar y para confirmar y después OK.

Más información acerca de la reparación de su Sector de Arranque en TestDisk elementos del menú. El siguiente mensaje expuesto:



TestDisk nos muestra ***Tiene que reiniciar su computadora para acceder a sus datos*** por consiguiente presione Entrar, otra vez y reinicie su equipo.

CONCLUCIÒN

Testdisk Recupera Particiones y Particiones de Arranque

Testdisk sirve para recuperar particiones y para reparar particiones de inicio o “booteables” ya sea por fallas de software, ciertos tipos de virus o error humano.

Entre sus principales características:

- Arreglar tablas de particiones, recuperar particiones borradas.
- Recuperar el sector de arranque (o boot) de particiones FAT32 desde un backup
- Reconstruir sectores de arranque FAT12/FAT16/FAT32
- Arreglar tablas FAT
- Reconstruir sectores de arranque de NTFS
- Recuperar archivos de sistemas de archivos FAT, NTFS y ext2
- Copiar archivos desde particiones borradas FAT, NTFS y ext2/etx3.

Esta aplicación es de código abierto y está bajo la licencia GPL y es gratis. Además, funciona en varias plataformas como:

- DOS
- Windows (NT4, 2000, XP, 2003, Vista)
- Linux
- FreeBSD, NetBSD, OpenBSD
- SunOS
- MacOS

Además, soporta una gran cantidad de sistemas de archivos como BeOS, BSD, CramFS, FAT 12/16/32, HFS, JFS, ext2, ext3, Linux RAID md, Linux Swap, LVM 1 y 2, Mac mapas de partición, NSS, NTFS, entre otros

PhotoRec Recupera Archivos Borrados

PhotoRec es un software diseñado para recuperar archivos perdidos incluyendo videos, documentos y archivos de los discos duros y CDRoms, así como imágenes perdidas (por eso el nombre PhotoRecovery) de las memorias de las cámaras fotográficas, MP3 players, PenDrives, etc. PhotoRec ignora el sistema de archivos y hace una búsqueda profunda de los datos, funcionando incluso si su sistema de archivos está muy dañado o ha sido re-formateado.

Este programa utiliza para mayor seguridad un acceso sólo de lectura para manejar el disco o la memoria de donde se recuperarán los datos. PhotoRec es gratis, de código abierto y está bajo la licencia GPL y viene junto con Testdisk. Además, es multiplataforma y funciona en:

- DOS/Win9x
- Windows NT 4/2000/XP/2003
- Linux
- FreeBSD, NetBSD, OpenBSD
- Sun Solaris
- Mac OS X

Reconoce más de 180 tipos de archivos para una lista completa La lista entera de formatos que reconoce PhotoRec

ANEXOS

Donde van a parar los archivos eliminados

Cuando borramos un archivo, no lo hemos eliminado físicamente, lo que hemos conseguido en realidad es que el sistema operativo no nos lo muestre más, le hemos indicado que no queremos saber nada de él... pero eso no significa que no exista la información que contiene. De hecho, sigue repartida en distintos clústeres del disco duro (zona mínima de información que reconoce el sistema operativo). Aunque lo borremos de la famosa papelera de reciclaje, aún la información persistirá en los magnetizados clústeres del nuestro disco. ¿Cuándo se borra entonces? Pues cuando ese espacio sea machacado por otra información, cuando se sobrescriba algo en esa misma zona del disco duro.

Imagen de PhotoRec

Imagen de TestDisk

BIBLIOGRAFIA

Información

http://www.cgsecurity.org/wiki/PhotoRec_ES

https://www.redeszone.net/gnu-linux/photorec-recupera-archivos-eliminados-desde-ubuntu/

http://www.tribulinux.com/testdisk-y-photorec-para-reparar-particiones-y-recuperar-archivos-en-linux-windows-macos.html

Instalación

https://portallinux.es/photorec-recuperacion-de-datos/

Ejemplo de cómo recuperar archivos de una USB

https://www.youtube.com/watch?v=hM9zwyx0kAg

https://www.youtube.com/watch?v=UpAMmsLrybs