UNIVERSIDAD LUTERANA SALVADOREÑA

FACULTAD DE CIENCIAS DEL HOMBRE Y LA NATURALEZA

LICENCIATURA EN CIENCIAS DE LA COMPUTACIÓN

NOMBRE DEL PROYECTO

PhotoRec

MATERIA

Análisis de sistemas

INTEGRANTES:

Williams Ernesto Sanchez Palacios	SP01132338
Medvin Ricardo Quijano Torres	QT01132516
José William Mejia Flores	MF01132606

DOCENTE:

LIC. JOSÉ LUIS ALVARADO AGUILAR

SAN SALVADOR, 14 DE NOVIEMBRE DE 2017

Indice

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 plasmara como poder hacer un analisis 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 una análisis forense con el software PhotoRec el cual esta 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 dato y esta a su ves pueden servir de prueba evidentes a favor o en contra en u juzgado

OBJETIVO GENERAL

Determinar de que manera se realiza un análisis forense a información almacenados dentro de una computadora utilizando el software PhotoRec, por el cual se realizaran 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 latarjeta 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 realizara 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 a sido recuperado la información.

2. Materiales y equipos:

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

3. Métodos y procedimientos: 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

ANEXOS

INSTALACIÓN

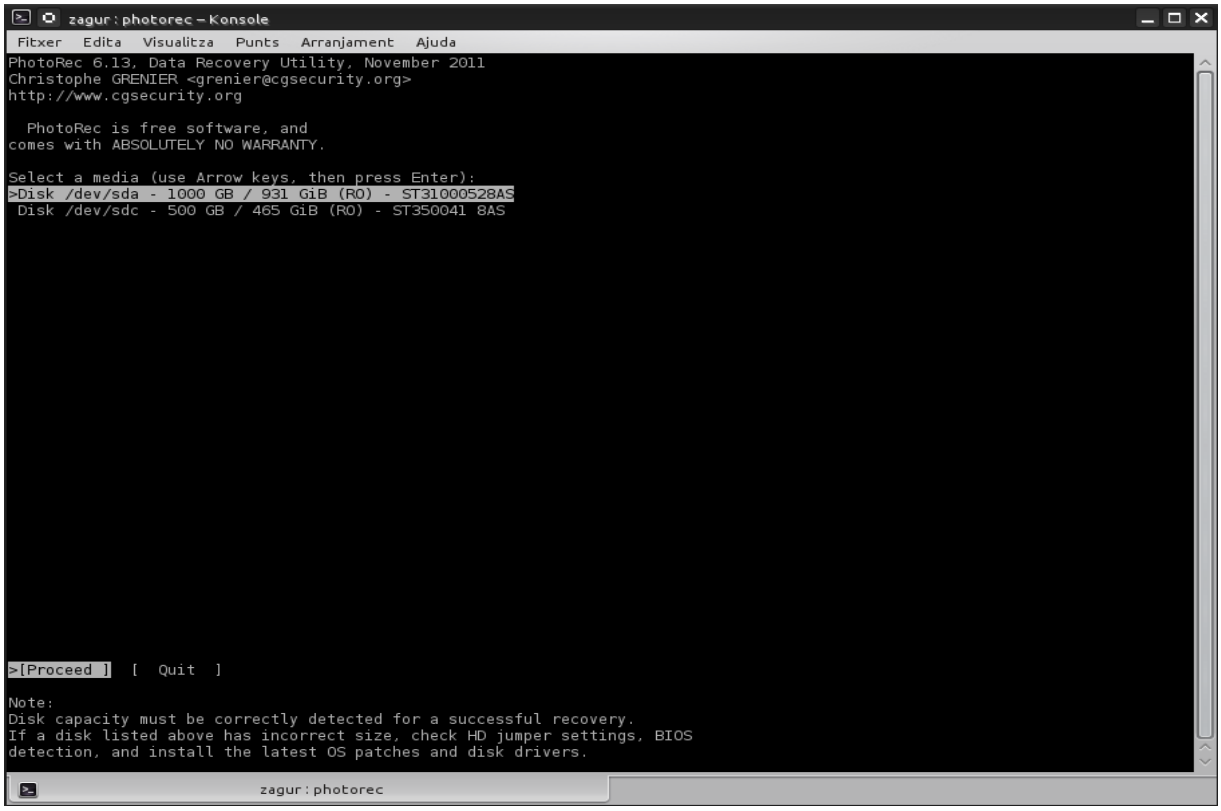
Como hemos mencionado anteriormente, PhotoRec acompaña a TestDisk por lo tanto vamos a instalar lo siguiente desde una Terminal:

```
1# apt-get install testdisk
```

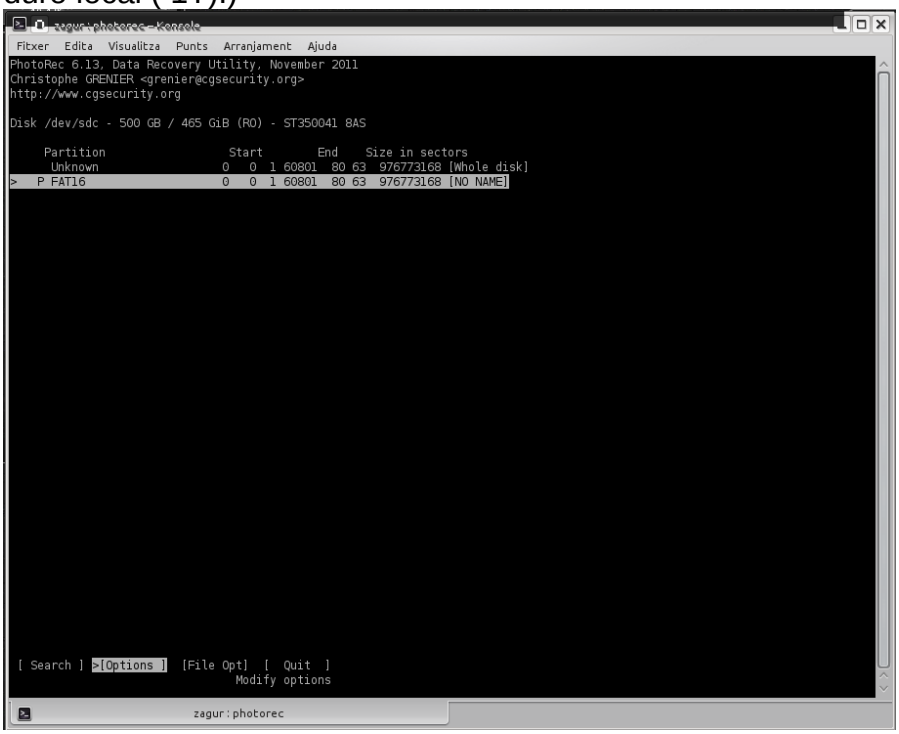
El software no tiene interfaz gráfica y está en inglés, pero es muy fácil de usar y de comprender.
Proceso de recuperación de datos
Iniciamos desde la Terminal el siguiente comando:

```
1# photorec
```

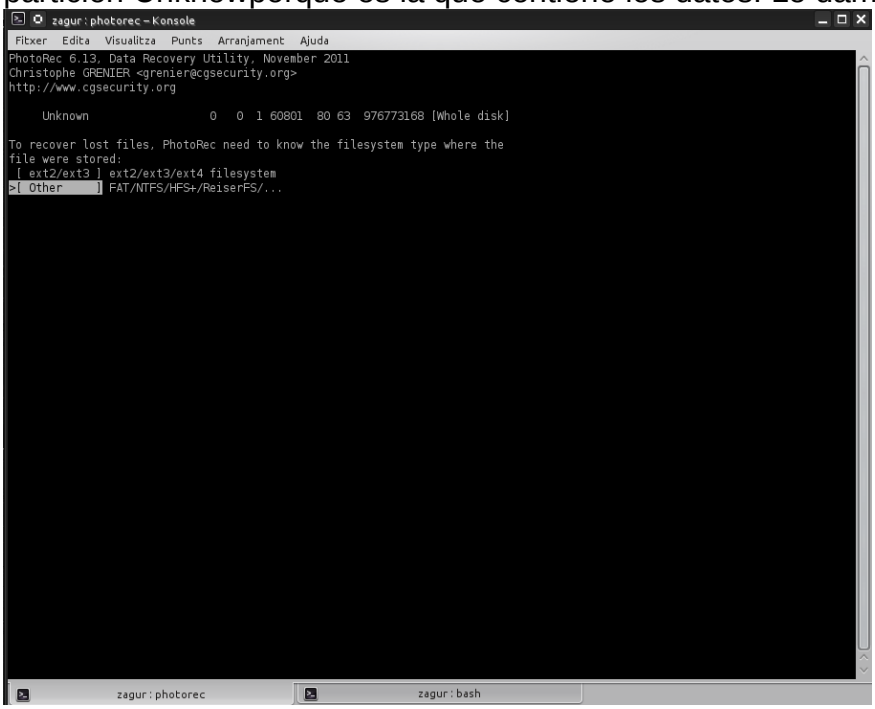
Después de poner la contraseña nos encontramos con la siguiente ventana:



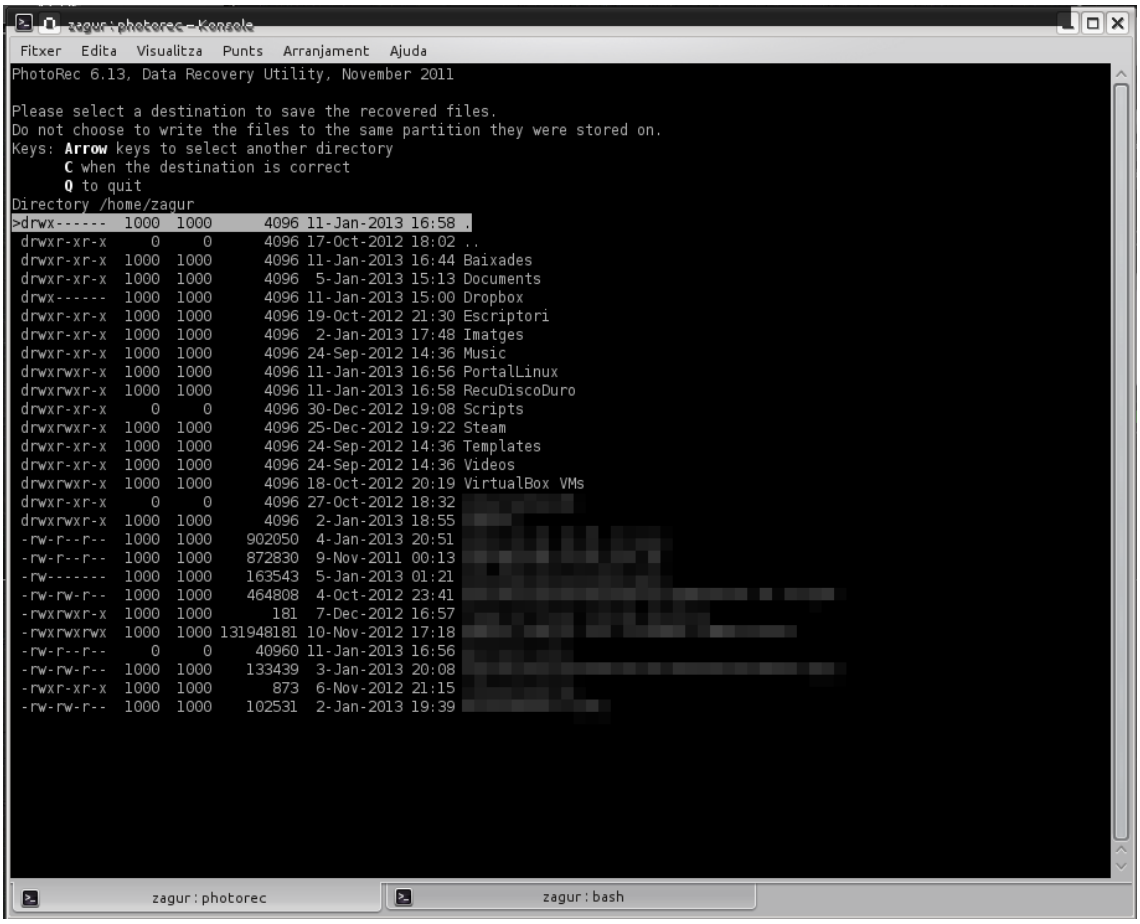
Usando las flechas seleccionamos nuestro disco duro dañado que anteriormente hemos mirado que punto de montaje tiene. (Podemos ver dos discos, el externo (500 GB) y el disco duro local (1T).)



Aquí nos pregunta que partición hay que recuperar. En este caso escogeremos la partición Unknowporqué es la que contiene los datos. Le damos a enter y seguimos.



Seleccionamos el sistema de ficheros que tiene nuestro disco duro dañado. En este caso escogemos la opción “Other” porqué es un disco extraible que desde siempre a funcionado con Windows.



BIBLIOGRAFÍA

Información

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

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

Instalacion

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

Ejemplo de como recuperar archivos de una usb

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

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