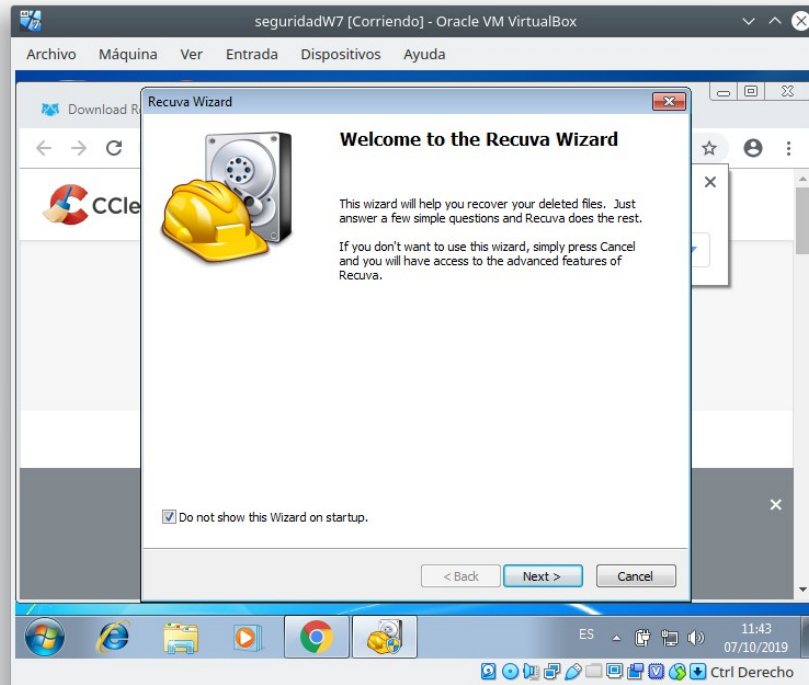


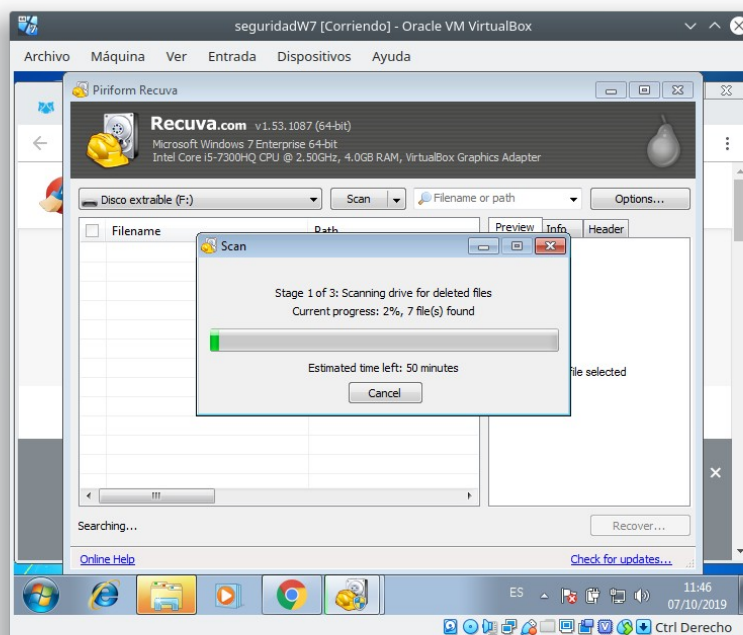
SAD.T2P6: Recuperación de datos

RECUVA

Recuva es de Windows así que utilizare una maquina de Windows 7

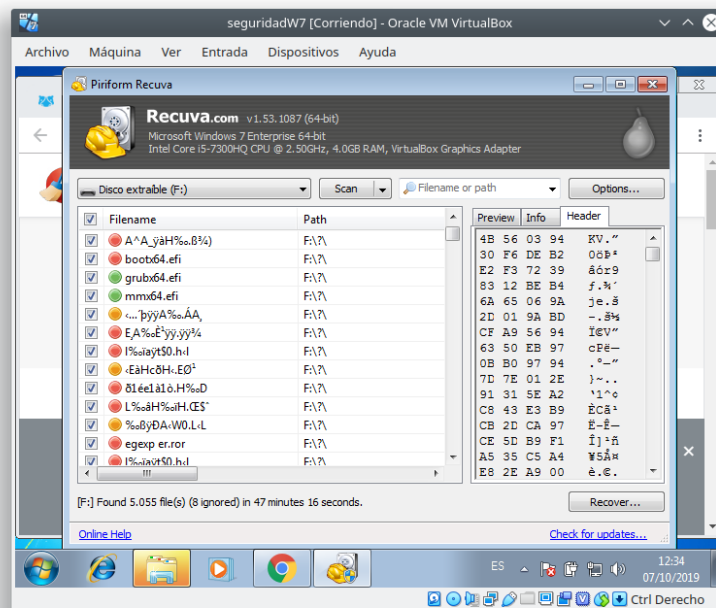


Una vez instalado se busca en la unidad extraíble USB si encuentra algo de los ficheros borrados.



SAD.T2P6: Recuperación de datos

Esta memoria USB básicamente es una que utilizo para ISO live de Linux ¿Que encontrara?

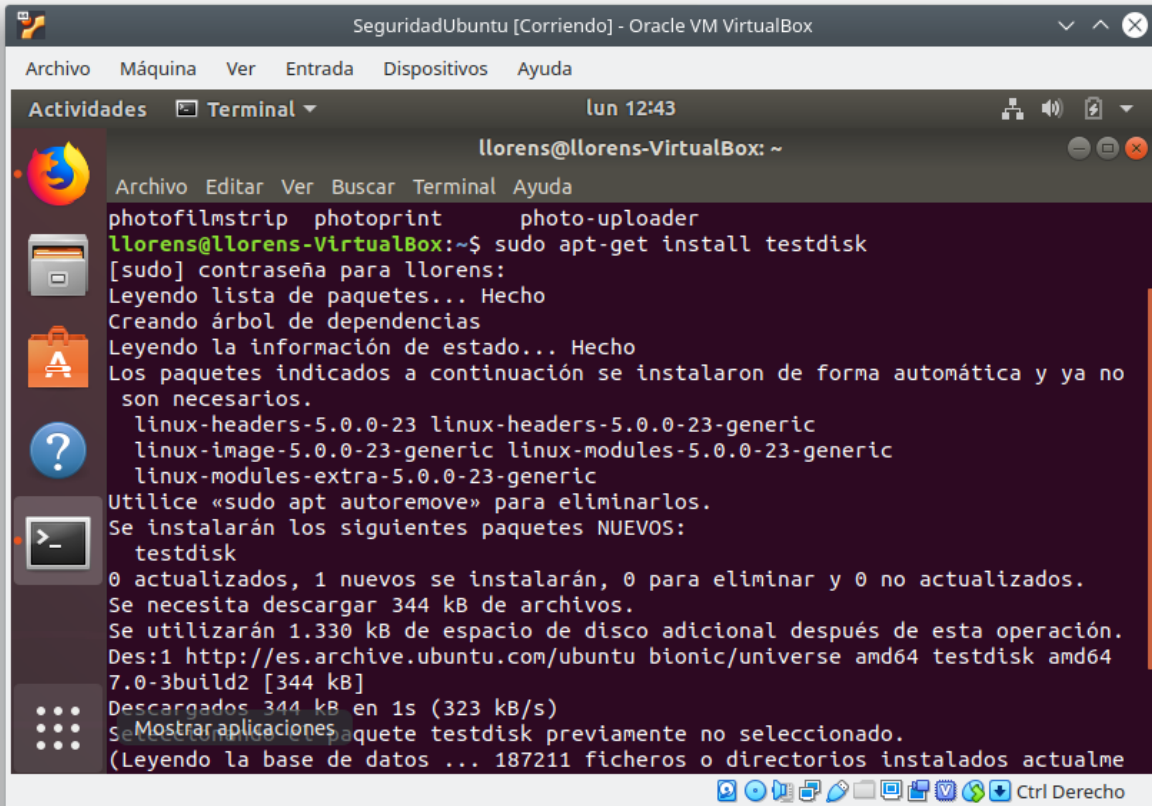


Básicamente a recuperado algo de los archivos de arranque,etc.Aunque hay que añadir que la mayoría son archivos corruptos o sin ninguna funcionalidad.

En la tarea siguiente en el otro software agregare fotos, borrar e intentare recuperarlas.

PHOTOREC

Nos vamos a la maquina virtual de UBUNTU e instalamos dicho software. En esta ocasión se llama testdisk



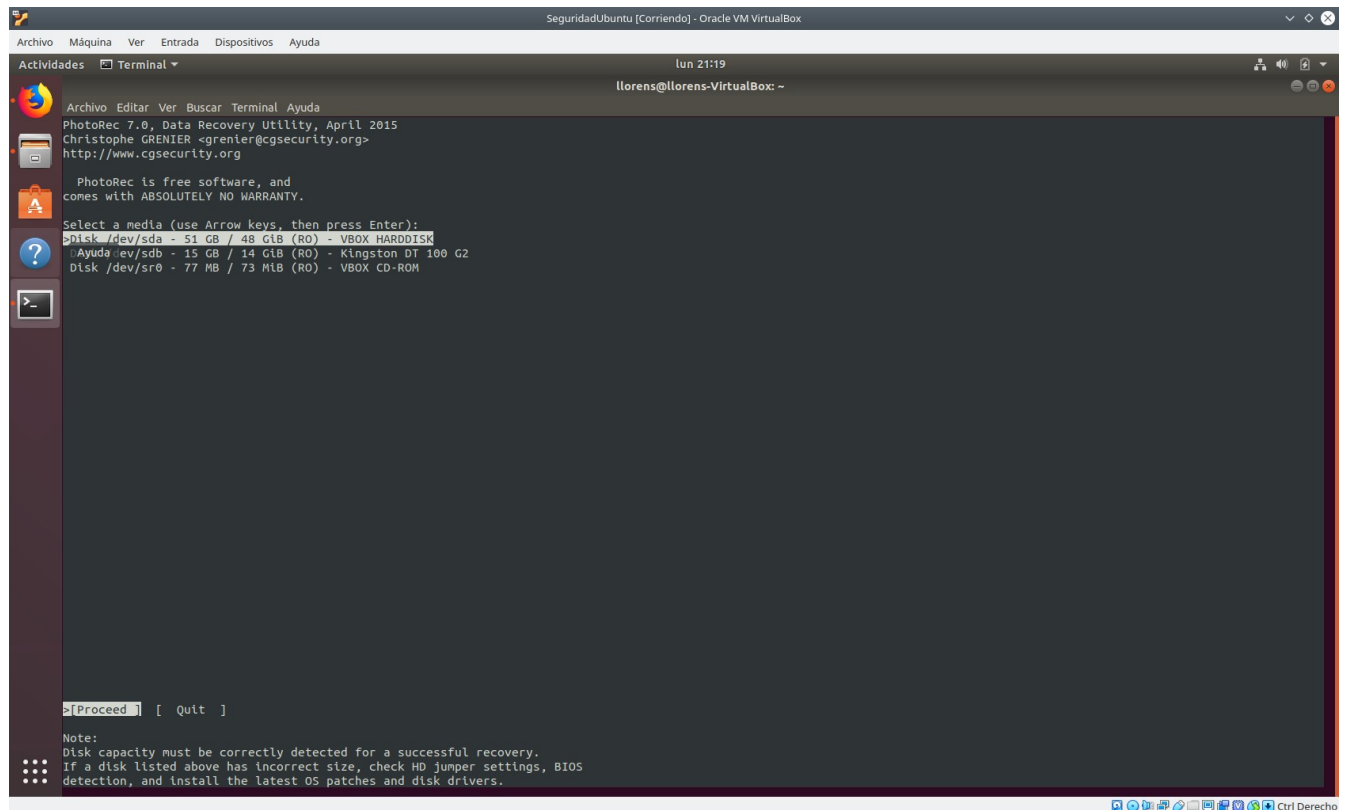
The screenshot shows a terminal window titled "SeguridadUbuntu [Corriendo] - Oracle VM VirtualBox". The terminal output shows the installation of testdisk using apt-get. The user runs the command "sudo apt-get install testdisk". The terminal shows the following output:

```
llorens@llorens-VirtualBox: ~  
photofilmstrip photoprint photo-uploader  
llorens@llorens-VirtualBox:~$ sudo apt-get install testdisk  
[sudo] contraseña para llorens:  
Leyendo lista de paquetes... Hecho  
Creando árbol de dependencias  
Leyendo la información de estado... Hecho  
Los paquetes indicados a continuación se instalaron de forma automática y ya no son necesarios.  
linux-headers-5.0.0-23 linux-headers-5.0.0-23-generic  
linux-image-5.0.0-23-generic linux-modules-5.0.0-23-generic  
linux-modules-extra-5.0.0-23-generic  
Utilice «sudo apt autoremove» para eliminarlos.  
Se instalarán los siguientes paquetes NUEVOS:  
testdisk  
0 actualizados, 1 nuevos se instalarán, 0 para eliminar y 0 no actualizados.  
Se necesita descargar 344 kB de archivos.  
Se utilizarán 1.330 kB de espacio de disco adicional después de esta operación.  
Des:1 http://es.archive.ubuntu.com/ubuntu bionic/universe amd64 testdisk amd64 7.0-3build2 [344 kB]  
Descargados 344 kB en 1s (323 kB/s)  
Se seleccionó el paquete testdisk previamente no seleccionado.  
(Leyendo la base de datos ... 187211 ficheros o directorios instalados actualme
```

SAD.T2P6: Recuperación de datos

Para iniciarlo (hay que ponerla maquina en pantalla completa si no te pedira que alargues el terminal)
Y entraremos como sudo por que si no no detectara el USB

Sudo photorec....



The screenshot shows a terminal window titled "SeguridadUbuntu [Corriendo] - Oracle VM VirtualBox". The terminal output displays the PhotoRec 7.0 interface. It includes the version, author (Christophe GRENIER), and website (http://www.cgsecurity.org). A disclaimer states: "PhotoRec is free software, and comes with ABSOLUTELY NO WARRANTY." The prompt "Select a media (use Arrow keys, then press Enter):" is followed by a list of detected disks: "Disk /dev/sda - 51 GB / 48 GiB (RO) - VBOX HARDISK", "Disk /dev/sdb - 15 GB / 14 GiB (RO) - Kingston DT 100 G2", and "Disk /dev/sr0 - 77 MB / 73 MiB (RO) - VBOX CD-ROM". At the bottom, there are options "[Proceed]" and "[Quit]", and a note about disk capacity detection.

```
lun 21:19
llorens@llorens-VirtualBox: ~
Archivo Editar Ver Buscar Terminal Ayuda
PhotoRec 7.0, Data Recovery Utility, April 2015
Christophe GRENIER <grenier@cgsecurity.org>
http://www.cgsecurity.org

PhotoRec is free software, and
comes with ABSOLUTELY NO WARRANTY.

Select a media (use Arrow keys, then press Enter):
Disk /dev/sda - 51 GB / 48 GiB (RO) - VBOX HARDISK
Disk /dev/sdb - 15 GB / 14 GiB (RO) - Kingston DT 100 G2
Disk /dev/sr0 - 77 MB / 73 MiB (RO) - VBOX CD-ROM

[Proceed] [Quit ]

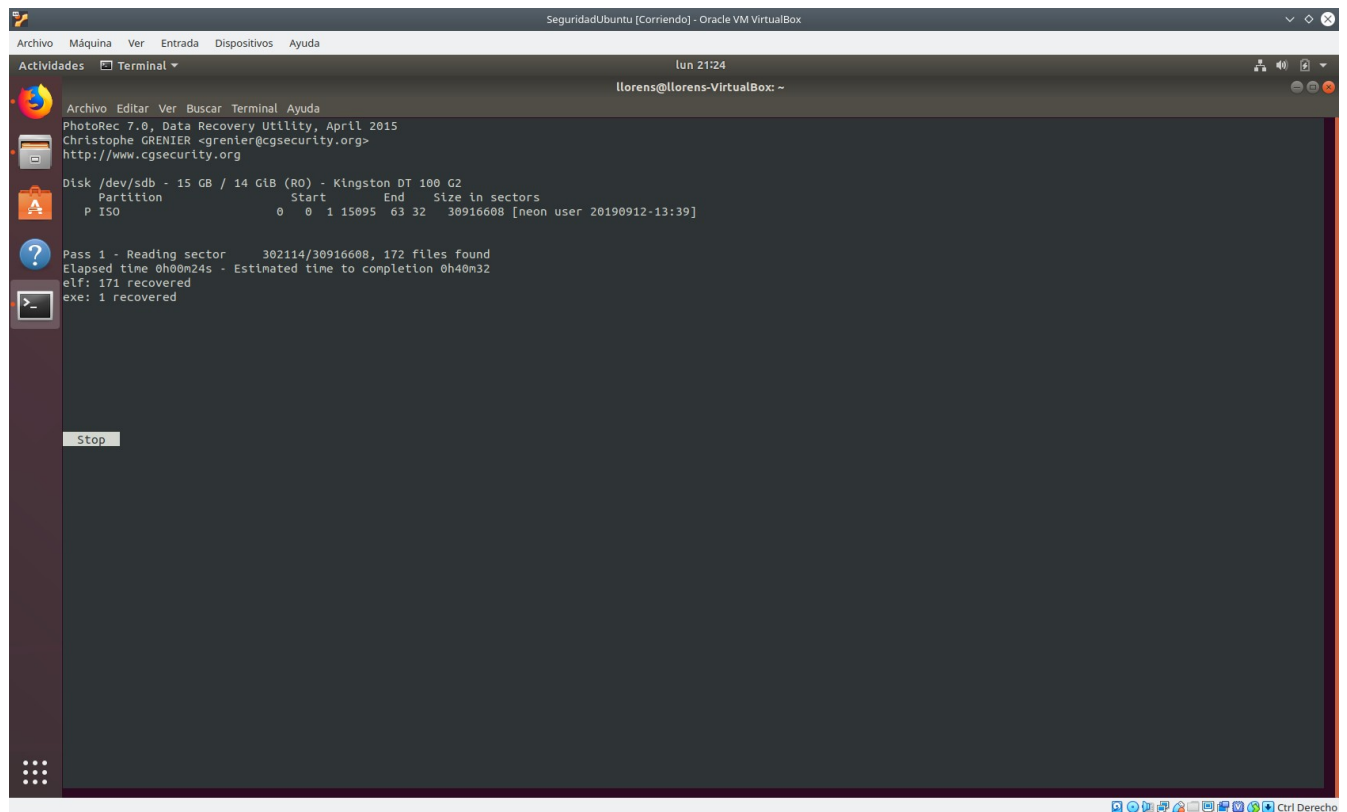
Note:
Disk capacity must be correctly detected for a successful recovery.
If a disk listed above has incorrect size, check HD jumper settings, BIOS
detection, and install the latest OS patches and disk drivers.
```

Como se aprecia detecta ya el USB como repito hay que usar sudo.

SAD.T2P6: Recuperación de datos

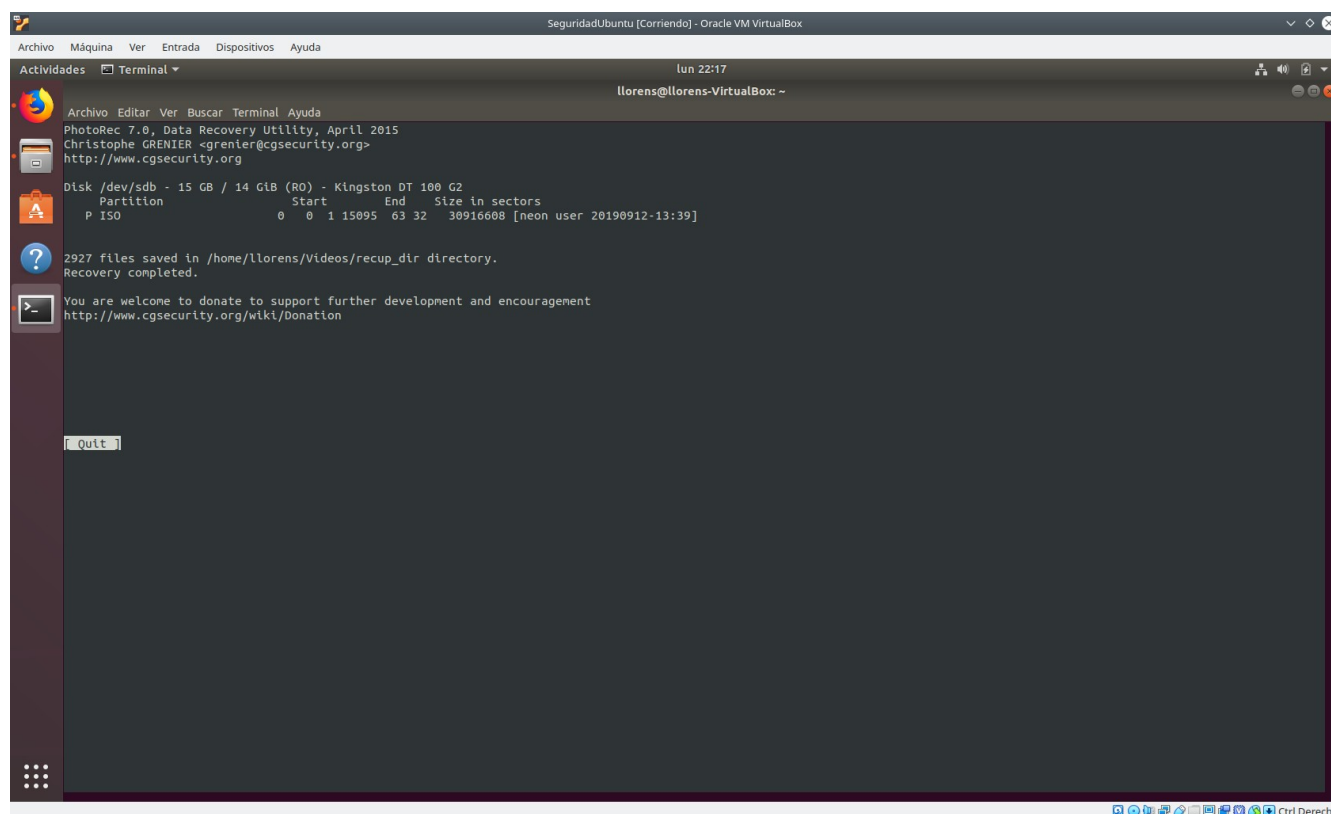
Procedemos a recuperar archivos, anteriormente no recupere archivos para poderlos comparar. Después agregare unas fotos e intentare recuperar las fotos. Seguidamente are un borrado seguro e intentare recuperarlas de nuevo.

Este no previsualiza los archivos seleccionas el directorio y seguidamente realiza el recuperado.



SAD.T2P6: Recuperación de datos

Después de terminar de recuperar los archivos son 2927 archivos recuperados.



Para verlo mas gráficamente enseñó algunos archivos recuperados se ve que las fotos de Ubuntu de la ISO si que la ha recuperado. De todas formas voy a hacerlo otra vez pero con fotos de personas.

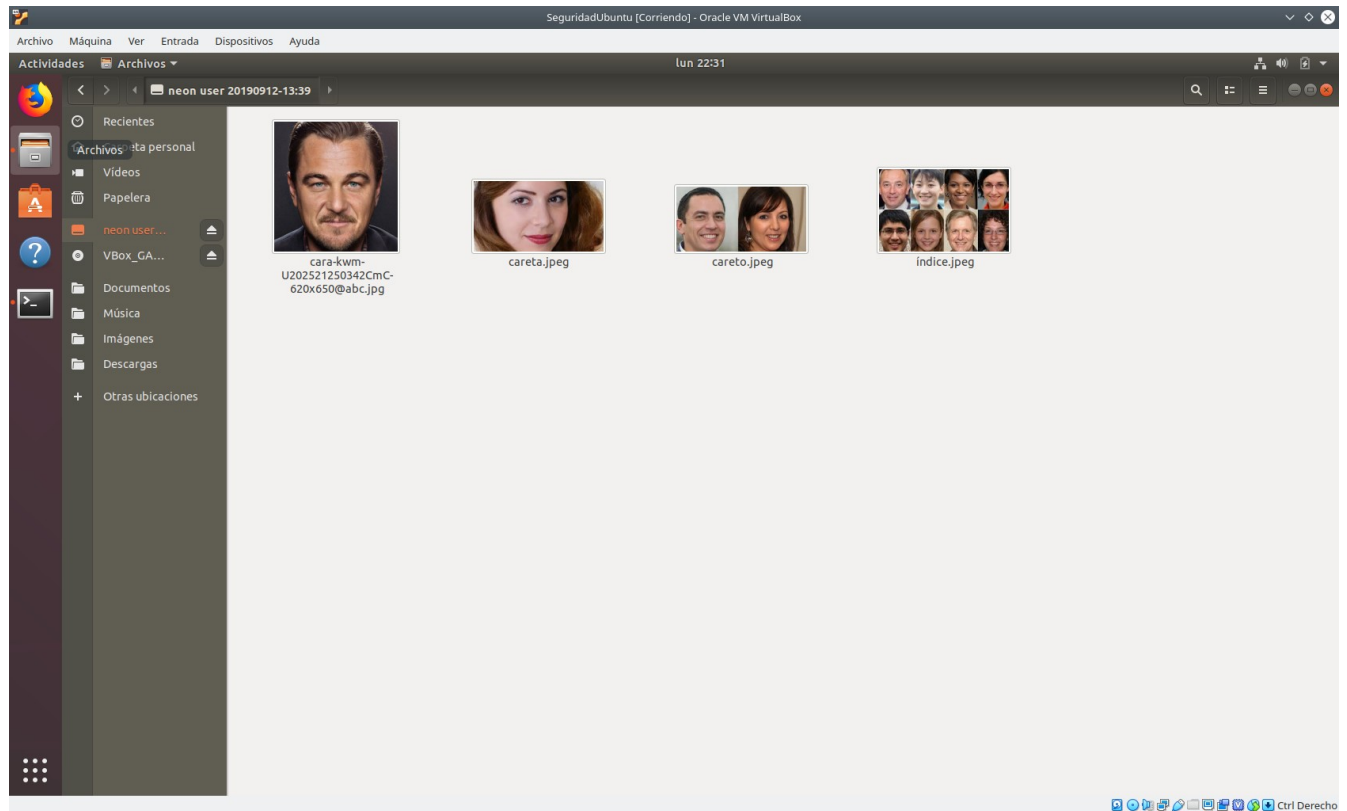
Pero primero voy a realizar un borrado seguro y comprobaremos si recupera algún archivo

NOTA DE REPASO:

(accidentalmente se me borro la captura y los archivos ya no los tengo para demostrarlo)

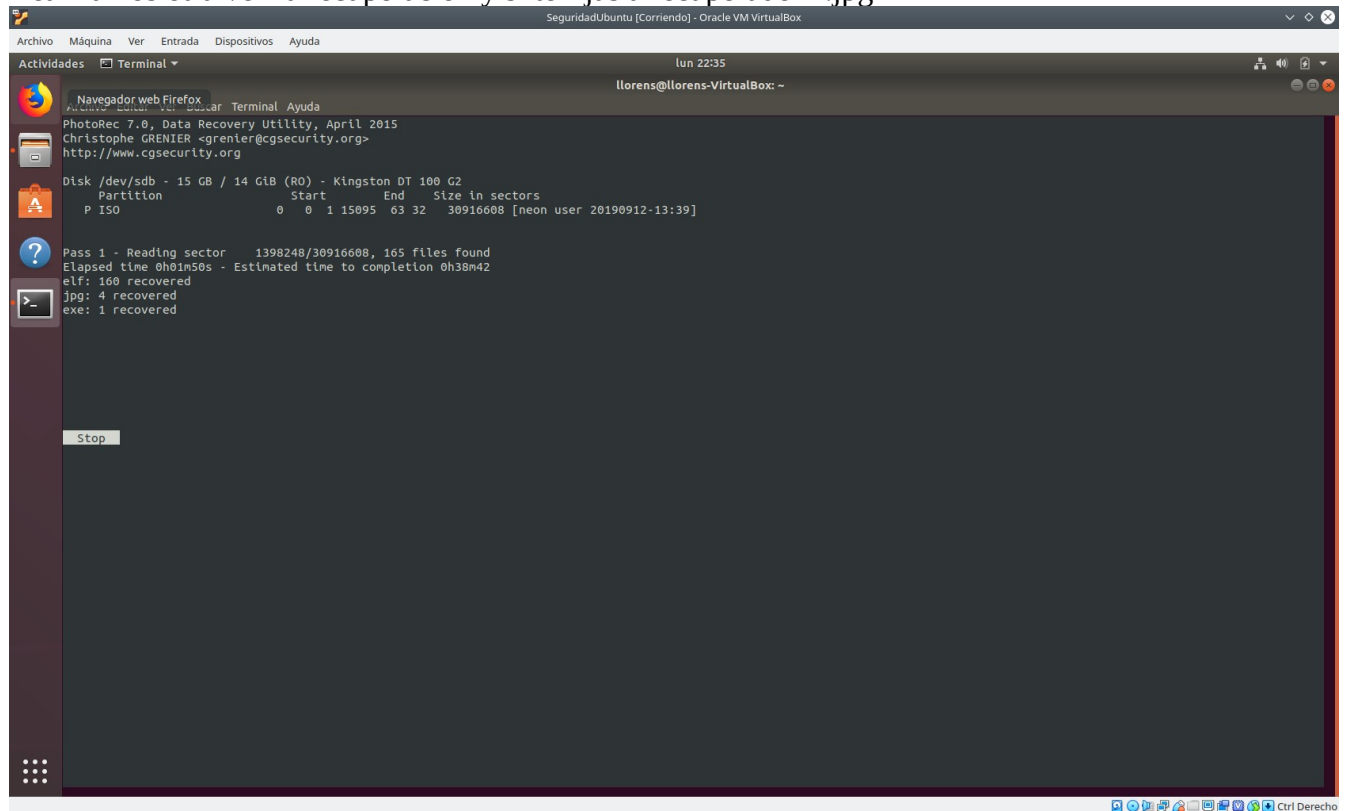
SAD.T2P6: Recuperación de datos

Supongamos que tenemos estas fotos y por error las eliminamos
¿Se recuperarían?



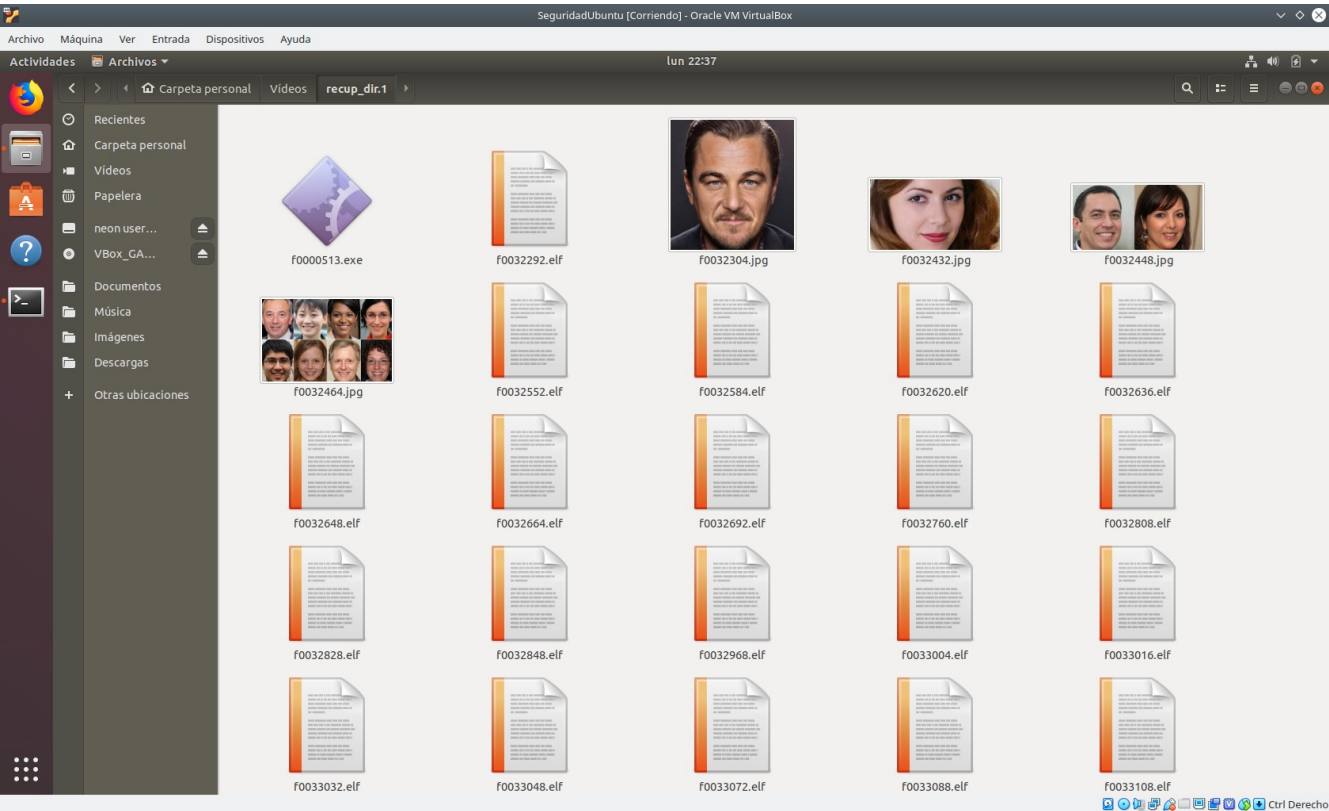
SAD.T2P6: Recuperación de datos

Realizamos otra vez la recuperacion y si te fijas a recuperado 4 .jpg



Pues si y esta vez no ha tardado mucho tiempo, recuerda que el directorio de recuperacion es ./videos

SAD.T2P6: Recuperación de datos



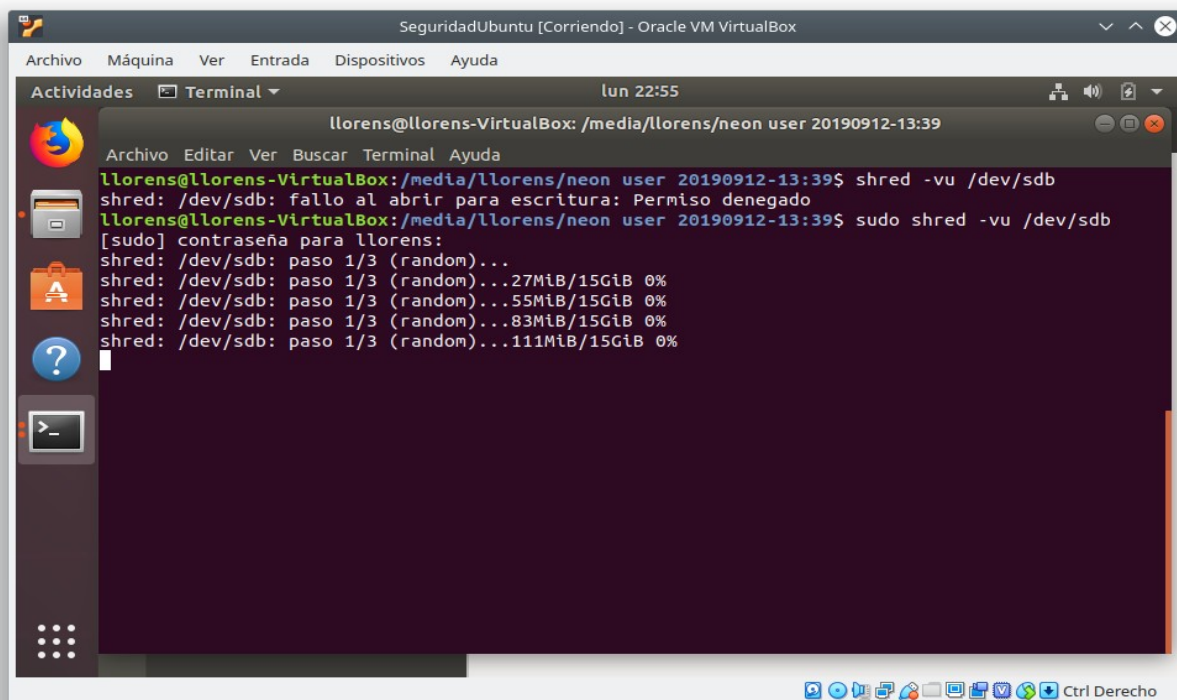
SAD.T2P6: Recuperación de datos

Ahora voy a realizar un borrado seguro googleando es SHRED ya venia con Ubuntu.

Para ellos nos iremos al directorio del pen USB y escribimos “sudo shred -vu /dev/sdb” a ver que pasa

-v verbose o verborragico, muestra el progreso en pantalla

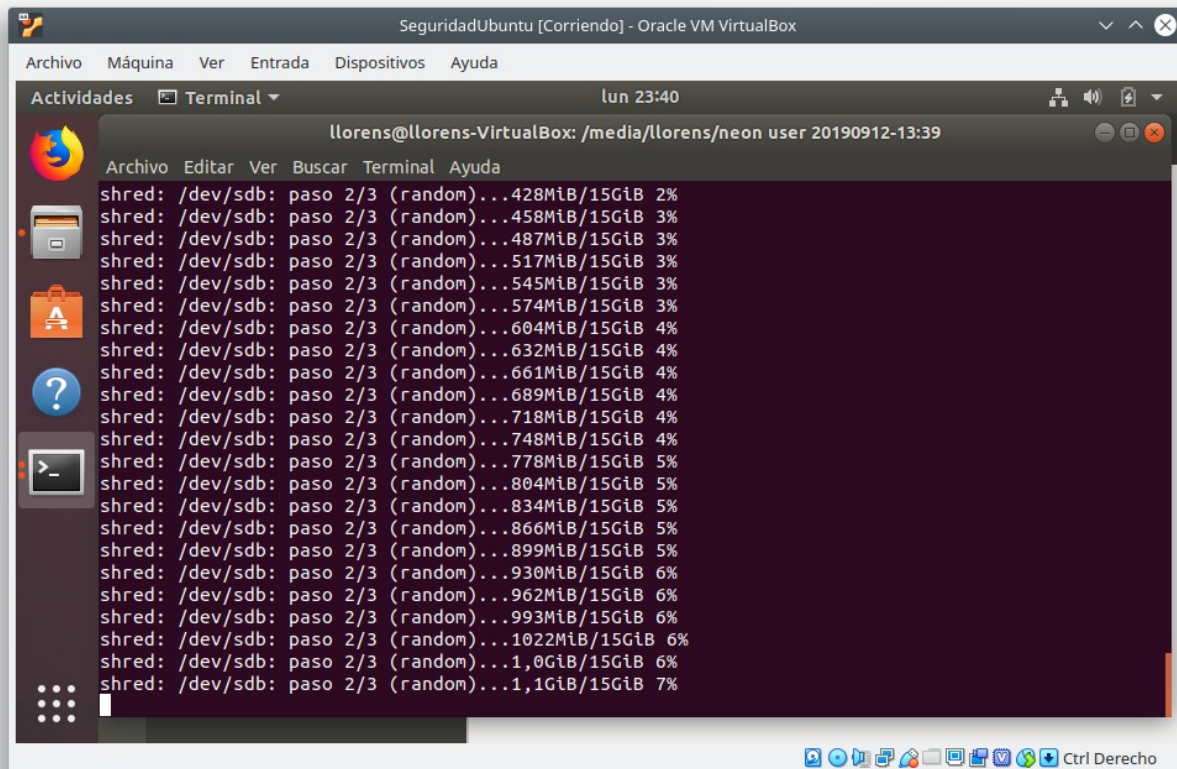
-u trunca y elimina el archivo después de sobrescribirlo



```
SeguridadUbuntu [Corriendo] - Oracle VM VirtualBox
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda
Actividades  Terminal  lun 22:55
llorens@llorens-VirtualBox: /media/llorens/neon user 20190912-13:39
Archivo Editar Ver Buscar Terminal Ayuda
llorens@llorens-VirtualBox: /media/llorens/neon user 20190912-13:39$ shred -vu /dev/sdb
shred: /dev/sdb: fallo al abrir para escritura: Permiso denegado
llorens@llorens-VirtualBox: /media/llorens/neon user 20190912-13:39$ sudo shred -vu /dev/sdb
[sudo] contraseña para llorens:
shred: /dev/sdb: paso 1/3 (random)...
shred: /dev/sdb: paso 1/3 (random)...27MiB/15GiB 0%
shred: /dev/sdb: paso 1/3 (random)...55MiB/15GiB 0%
shred: /dev/sdb: paso 1/3 (random)...83MiB/15GiB 0%
shred: /dev/sdb: paso 1/3 (random)...111MiB/15GiB 0%
```

El proceso es lento....

SAD.T2P6: Recuperación de datos

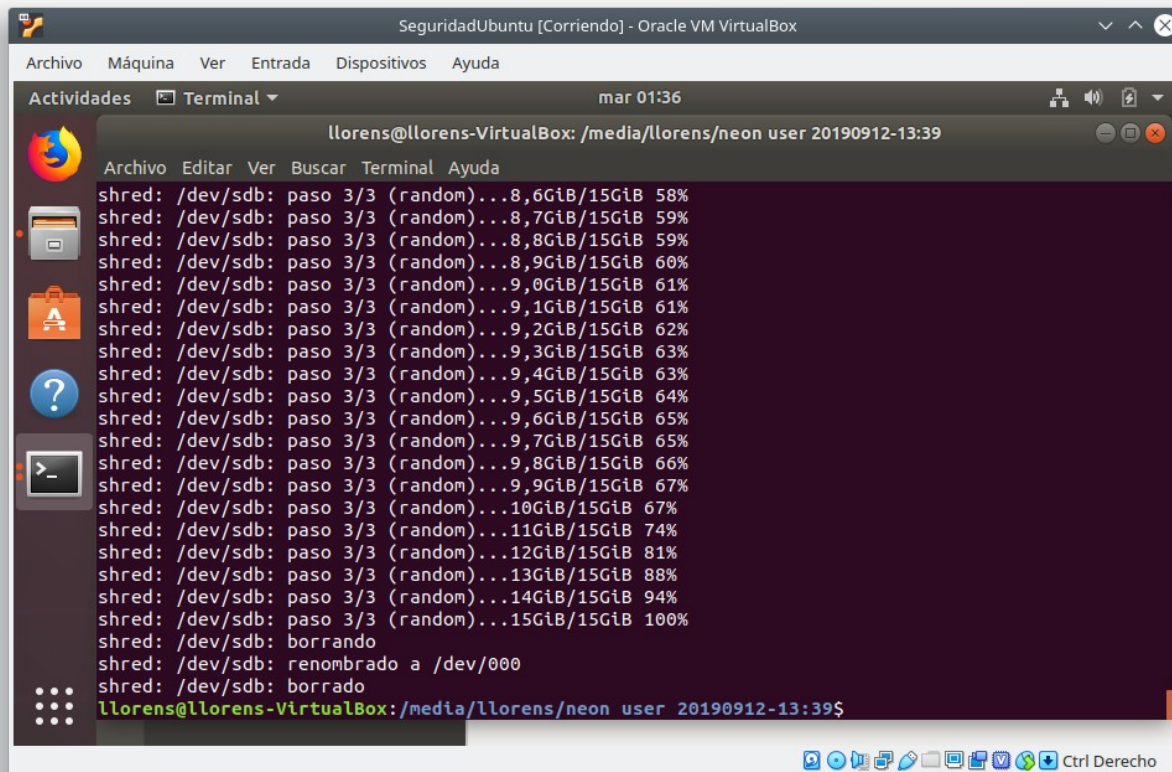


The screenshot shows a terminal window titled "SeguridadUbuntu [Corriendo] - Oracle VM VirtualBox". The terminal output displays the progress of the 'shred' command being executed on /dev/sdb. The command is running in a loop, and the progress is shown as a percentage of the total size of the device (15GiB).

```
llorens@llorens-VirtualBox: /media/llorens/neon user 20190912-13:39
shred: /dev/sdb: paso 2/3 (random)...428MiB/15GiB 2%
shred: /dev/sdb: paso 2/3 (random)...458MiB/15GiB 3%
shred: /dev/sdb: paso 2/3 (random)...487MiB/15GiB 3%
shred: /dev/sdb: paso 2/3 (random)...517MiB/15GiB 3%
shred: /dev/sdb: paso 2/3 (random)...545MiB/15GiB 3%
shred: /dev/sdb: paso 2/3 (random)...574MiB/15GiB 3%
shred: /dev/sdb: paso 2/3 (random)...604MiB/15GiB 4%
shred: /dev/sdb: paso 2/3 (random)...632MiB/15GiB 4%
shred: /dev/sdb: paso 2/3 (random)...661MiB/15GiB 4%
shred: /dev/sdb: paso 2/3 (random)...689MiB/15GiB 4%
shred: /dev/sdb: paso 2/3 (random)...718MiB/15GiB 4%
shred: /dev/sdb: paso 2/3 (random)...748MiB/15GiB 4%
shred: /dev/sdb: paso 2/3 (random)...778MiB/15GiB 5%
shred: /dev/sdb: paso 2/3 (random)...804MiB/15GiB 5%
shred: /dev/sdb: paso 2/3 (random)...834MiB/15GiB 5%
shred: /dev/sdb: paso 2/3 (random)...866MiB/15GiB 5%
shred: /dev/sdb: paso 2/3 (random)...899MiB/15GiB 5%
shred: /dev/sdb: paso 2/3 (random)...930MiB/15GiB 6%
shred: /dev/sdb: paso 2/3 (random)...962MiB/15GiB 6%
shred: /dev/sdb: paso 2/3 (random)...993MiB/15GiB 6%
shred: /dev/sdb: paso 2/3 (random)...1022MiB/15GiB 6%
shred: /dev/sdb: paso 2/3 (random)...1,0GiB/15GiB 6%
shred: /dev/sdb: paso 2/3 (random)...1,1GiB/15GiB 7%
```

Después cuando termine volveré a intentar a recuperar algo con Photorec

SAD.T2P6: Recuperación de datos



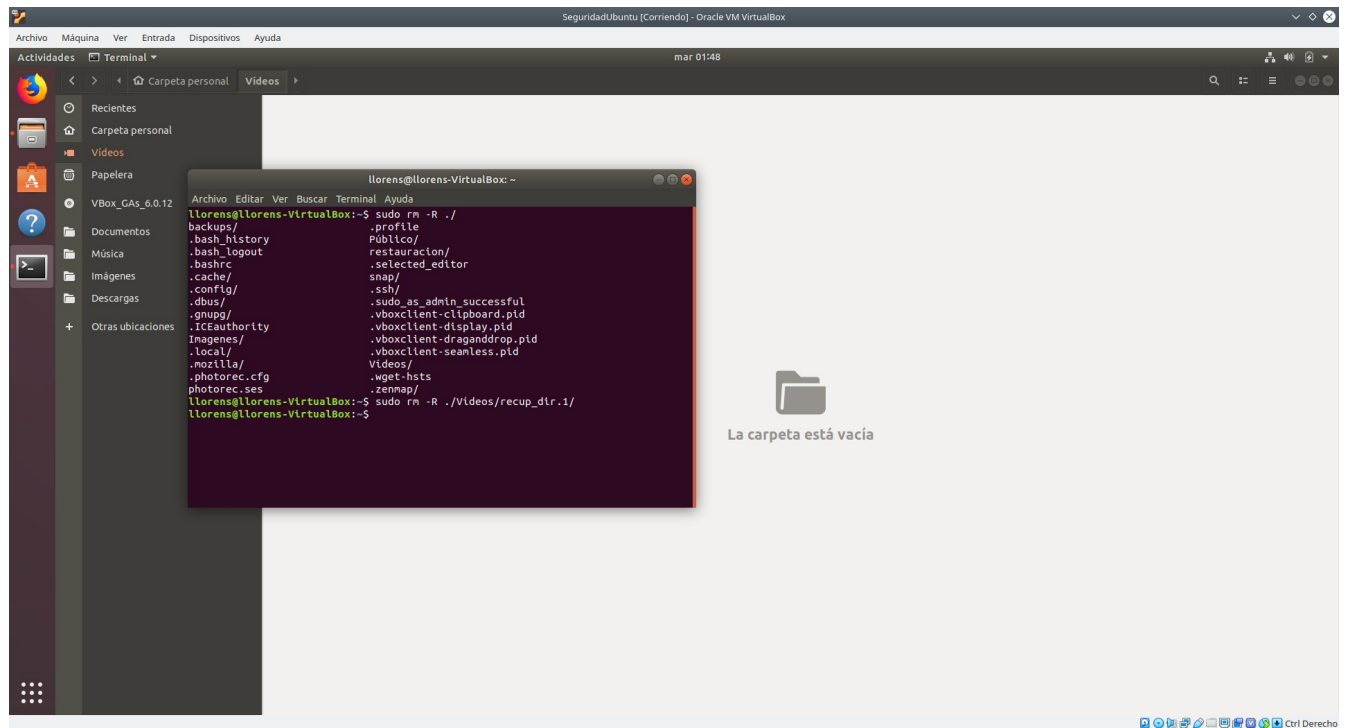
```
llorens@llorens-VirtualBox: /media/llorens/neon user 20190912-13:39$ shred: /dev/sdb: paso 3/3 (random)...8,6GiB/15GiB 58%
shred: /dev/sdb: paso 3/3 (random)...8,7GiB/15GiB 59%
shred: /dev/sdb: paso 3/3 (random)...8,8GiB/15GiB 59%
shred: /dev/sdb: paso 3/3 (random)...8,9GiB/15GiB 60%
shred: /dev/sdb: paso 3/3 (random)...9,0GiB/15GiB 61%
shred: /dev/sdb: paso 3/3 (random)...9,1GiB/15GiB 61%
shred: /dev/sdb: paso 3/3 (random)...9,2GiB/15GiB 62%
shred: /dev/sdb: paso 3/3 (random)...9,3GiB/15GiB 63%
shred: /dev/sdb: paso 3/3 (random)...9,4GiB/15GiB 63%
shred: /dev/sdb: paso 3/3 (random)...9,5GiB/15GiB 64%
shred: /dev/sdb: paso 3/3 (random)...9,6GiB/15GiB 65%
shred: /dev/sdb: paso 3/3 (random)...9,7GiB/15GiB 65%
shred: /dev/sdb: paso 3/3 (random)...9,8GiB/15GiB 66%
shred: /dev/sdb: paso 3/3 (random)...9,9GiB/15GiB 67%
shred: /dev/sdb: paso 3/3 (random)...10GiB/15GiB 67%
shred: /dev/sdb: paso 3/3 (random)...11GiB/15GiB 74%
shred: /dev/sdb: paso 3/3 (random)...12GiB/15GiB 81%
shred: /dev/sdb: paso 3/3 (random)...13GiB/15GiB 88%
shred: /dev/sdb: paso 3/3 (random)...14GiB/15GiB 94%
shred: /dev/sdb: paso 3/3 (random)...15GiB/15GiB 100%
shred: /dev/sdb: borrando
shred: /dev/sdb: renombrado a /dev/000
shred: /dev/sdb: borrado
llorens@llorens-VirtualBox: /media/llorens/neon user 20190912-13:39$
```

Una vez concluido el nombre de la unidad a cambiado.

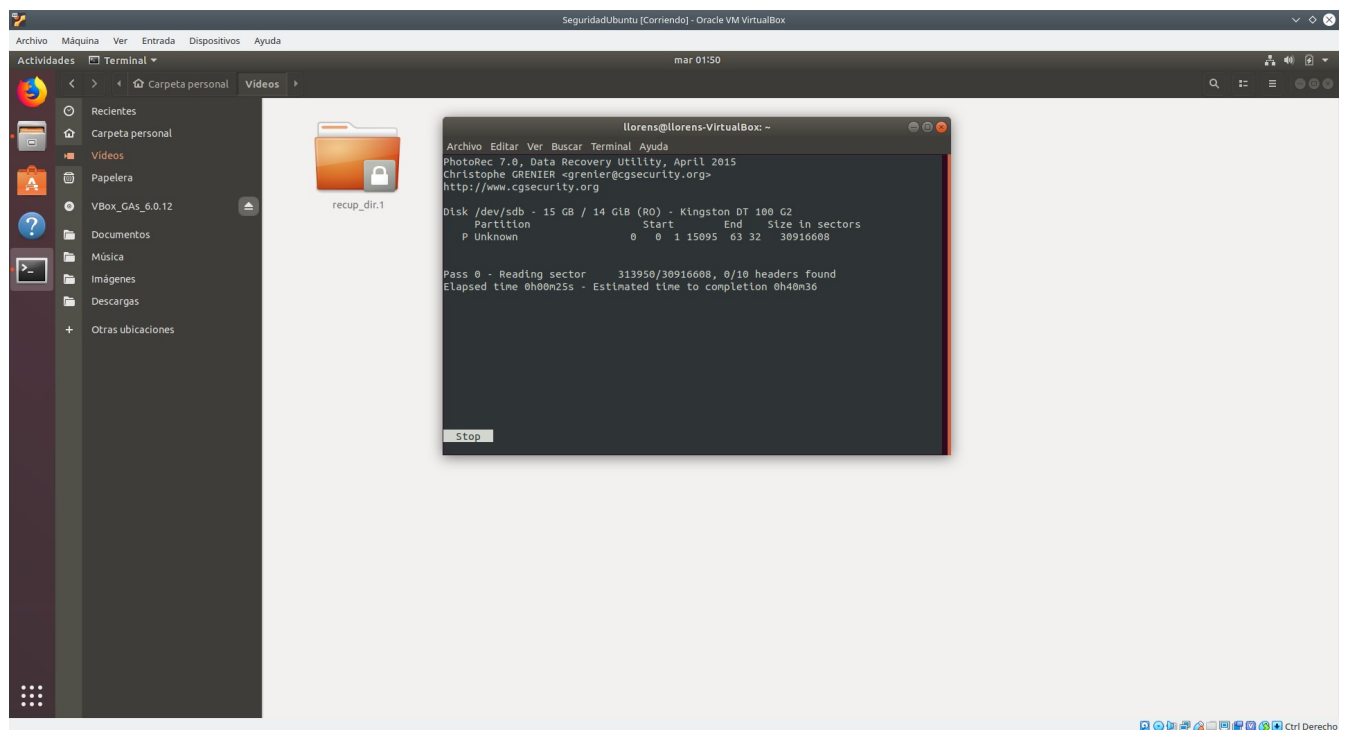
Ahora volvemos a pasar el Photorec y veremos si recupera algo.

SAD.T2P6: Recuperación de datos

Primero antes de todo los archivos que recuperamos los borraremos del directorio de videos.

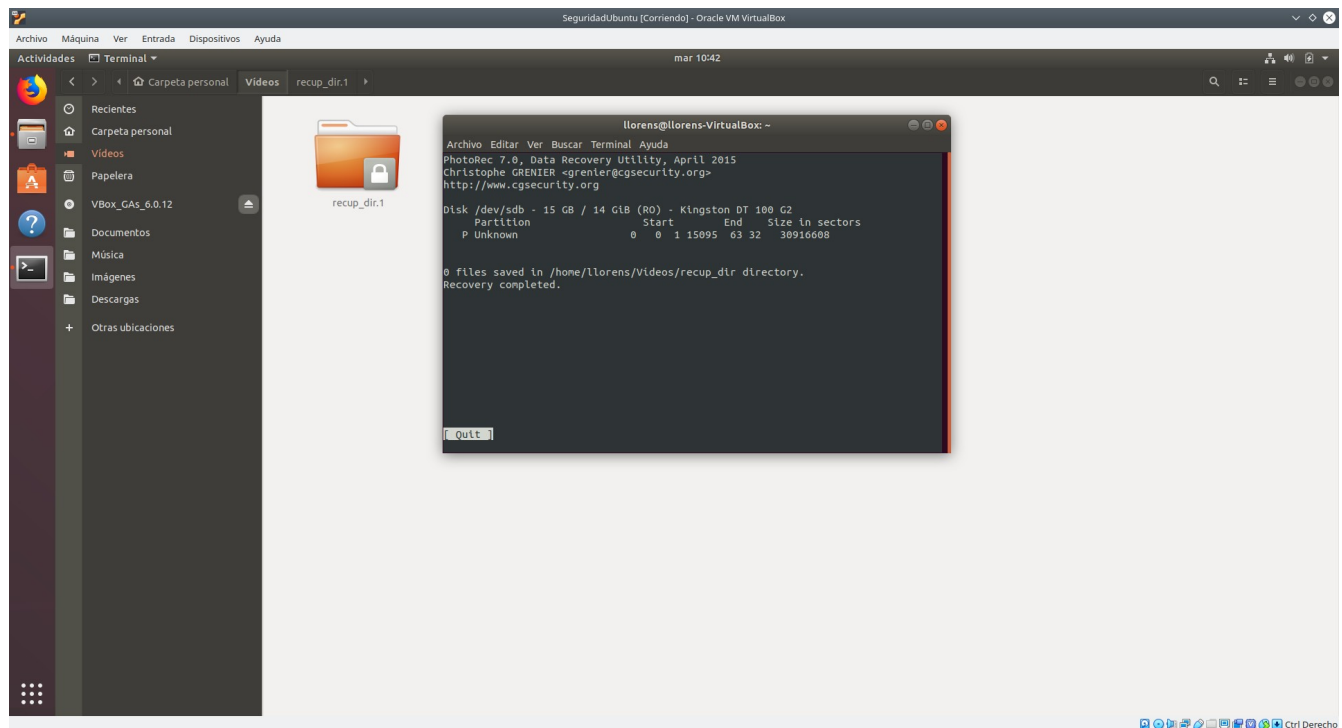


Ahora si a pasar Photorec con el directorio de recuperación Videos



SAD.T2P6: Recuperación de datos

Se aprecia en la captura anterior como se vuelve a crear el directorio recup_dir.1, ahora esperaremos y esperaremos a que finalice a ver que cantidad de archivos recupera. Anteriormente las imágenes que puse y elimine ya las habría recuperado. Pero esperar.



Después de realizar la recuperación dice que ha recuperado 0 archivos, anteriormente recordemos que habían archivos corruptos de la antigua ISO, imágenes de esta y las fotos de personas que introduje y borre después. Con SHRED jamas recuperaran nada.

Quizás existan empresas especializadas que puedan recuperar la información,pero eso ya es otro campo mas especializado de hardware.

Con esto doy concluida la practica ya que los procesos son muy lentos. Supongo que el software restante ara lo mismo. Mas gráficamente o menos pero lo importante es que lo haga.