

PRACTICA 2.2 Y 2.3

ATHOS ORÍO CHOPERENA

Contenido

Practica 2.2: Copias de seguridad con herramientas específicas.....	2
Copia de seguridad con windows.....	8
Copias de seguridad con Linux.....	21
Practica 2.3: Recuperación de datos.....	38

Practica 2.2: Copias de seguridad con herramientas específicas.

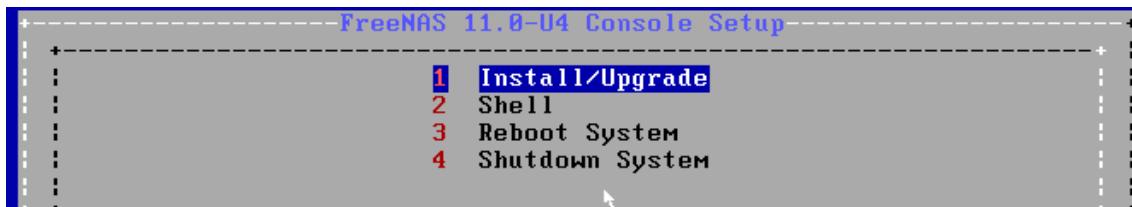
Es necesario realizar copias de seguridad, ya sea manualmente o de forma automática para tener cierta seguridad en los datos, ya sea por ataques de virus, fallos en hardware o cualquier otro motivo.

Estas copias de seguridad es recomendable que se hagan regularmente (en función de la cantidad de los datos generados y de su importancia será necesario que se realicen con mayor frecuencia).

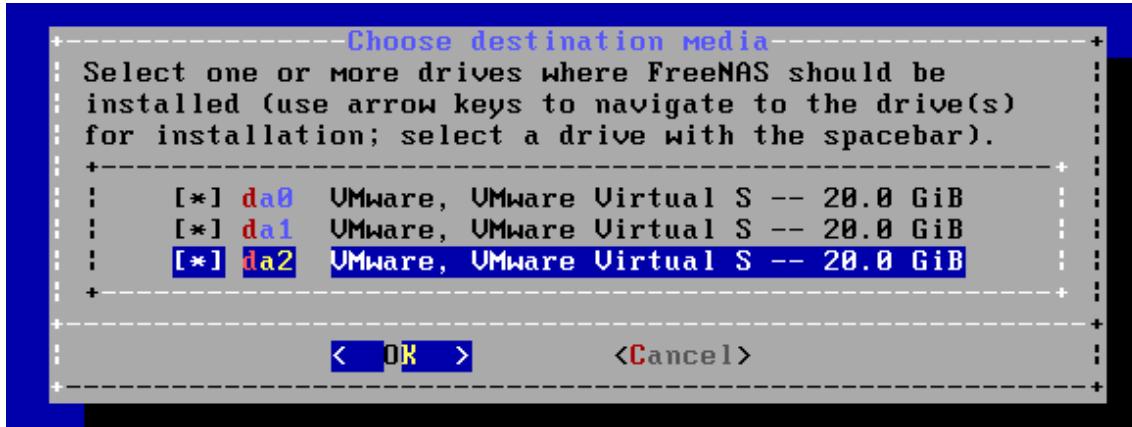
También es recomendable tener las copias de seguridad al menos en dos ubicaciones diferentes, para paliar posibles problemas de perdida de datos debidos a inundaciones, incendios o catástrofes naturales.

Para la realización de las copias de seguridad vamos a utilizar freeNas como destino. Para ello procederemos a la instalación de la máquina virtual con freeNas.

Según arrancamos nos preguntara si queremos instalar, o abrir una Shell, seleccionaremos instalar



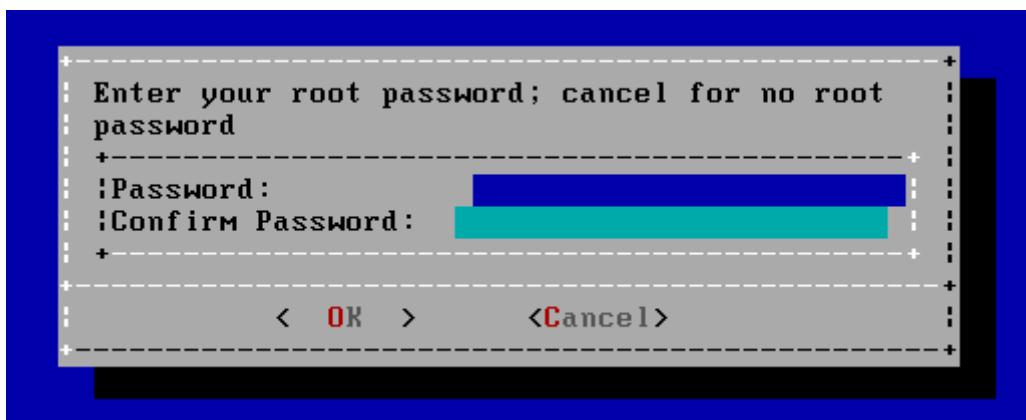
Ahora nos pregunta en que disco duro queremos instalar el sistema. Hemos añadido 3 discos para hacer un raid 5, así que seleccionamos los tres.



Nos dice que se borrarán los datos, y que no se podrán usar estos discos para compartir datos, entiendo que usara los tres discos para hacer un raid donde se instalará el sistema operativo.



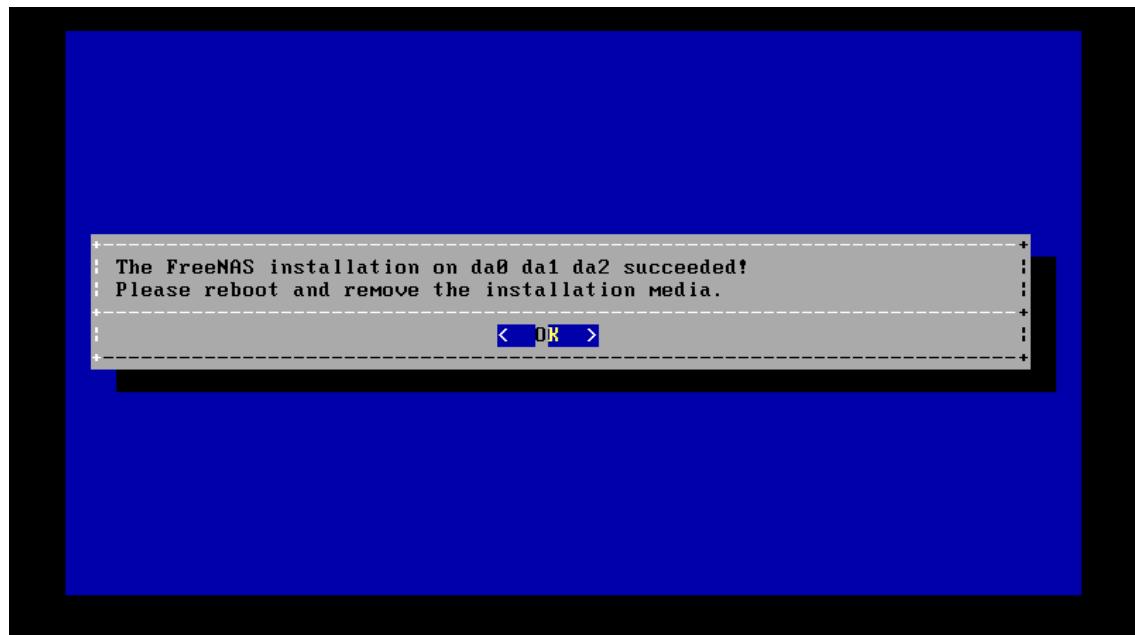
Seguidamente nos pregunta la contraseña de administrador que queremos para el sistema, la introducimos y seguimos con la instalación.



Tras esto comenzará la instalación.

```
da0p1 added
da0p2 added
da0 destroyed
da1 created
da1p1 added
da1p2 added
da1 destroyed
da2 created
da2p1 added
da2p2 added
da2 destroyed
da0 created
da0p1 added
da0p2 added
active set on da0
da1 created
da1p1 added
da1p2 added
active set on da1
da2 created
da2p1 added
da2p2 added
active set on da2
Installing base-os (1 of 5)
....10....20....30....40....50■
```

Tras esto, nos sale un mensaje indicando que la instalación se ha realizado correctamente y que reiniciemos el equipo.



Al reiniciar, el sistema se tira un rato haciendo inicio, generando certificados y alguna cosa más, y cuando termina, nos da un menú:

```
FreeBSD/amd64 (freenas.local) (ttyv0)

Console setup
-----
1) Configure Network Interfaces
2) Configure Link Aggregation
3) Configure VLAN Interface
4) Configure Default Route
5) Configure Static Routes
6) Configure DNS
7) Reset Root Password
8) Reset to Factory Defaults
9) Shell
10) System Update (requires networking)
11) Reboot
12) Shut Down

The web user interface is at:

http://192.168.40.156

Enter an option from 1-12: █
```

Lo primero que voy a hacer es configurar la tarjeta de red así que selecciono la opción 1

Nos irá preguntando una serie de opciones

```
http://192.168.1.10

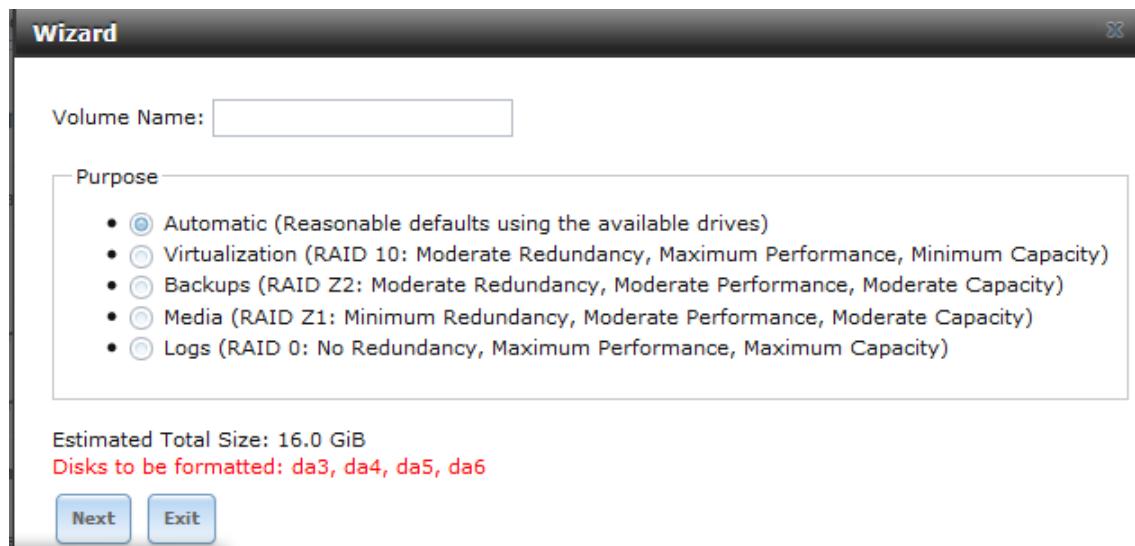
Enter an option from 1-12: 1
1) em0
Select an interface (q to quit): 1
Delete interface? (y/n) n
Reset network configuration? (y/n) n
Configure interface for DHCP? (y/n) n
Configure IPv4? (y/n) y
Interface name [em0]:
Several input formats are supported
Example 1 CIDR Notation:
    192.168.1.1/24
Example 2 IP and Netmask seperate:
    IP: 192.168.1.1
    Netmask: 255.255.255.0, /24 or 24
IPv4 Address [192.168.1.10]:192.168.1.10/24
Saving interface configuration: Ok
Configure IPv6? (y/n) █
```

Nos dice cómo podemos acceder al panel de control

```
The web user interface is at:  
http://192.168.1.10  
Enter an option from 1-12: ■
```

La primera vez que entramos, salta automáticamente el wizard, en el que nos pregunta sobre el idioma, la distribución de teclado y la zona horaria.

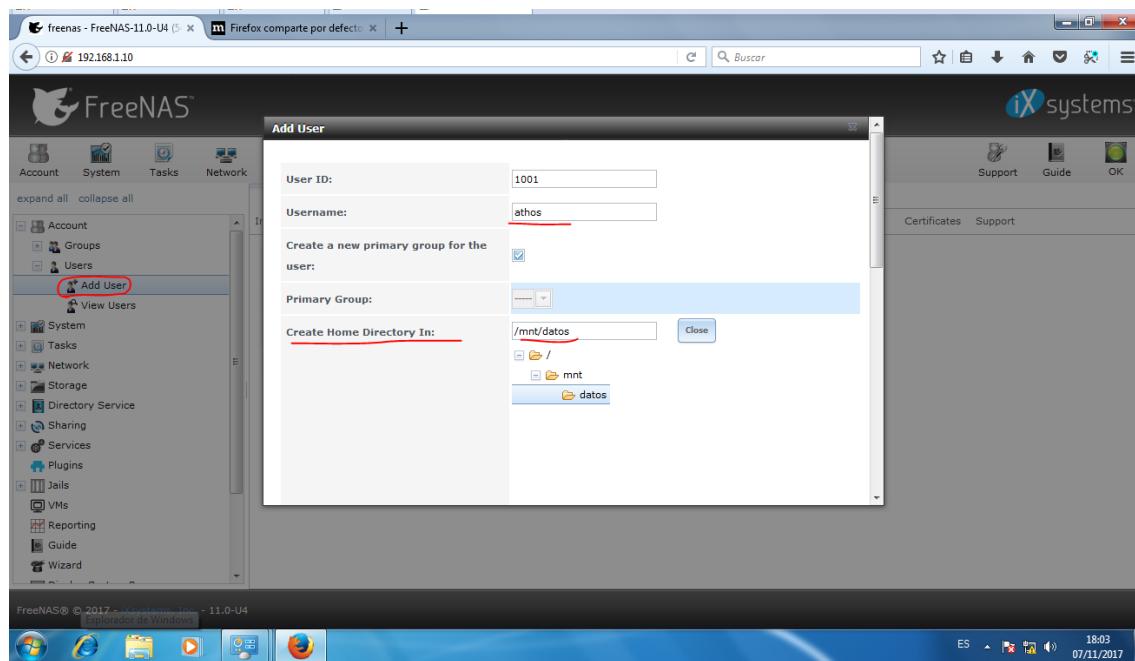
Seguidamente, nos sale un asistente para añadir una nueva unidad de datos, al principio había añadido 3 discos más (es decir, 6 en total contando los de la instalación del sistema operativo), pero me he dado cuenta de que alguna de las opciones no me dejaba seleccionarla, como la de backups raids z2, así que he añadido uno más y ya me ha dejado.



Selecciono Backups y pincho en siguiente. Pregunta una serie de cosas sobre que queremos compartir, las pasamos por alto porque lo haremos más adelante.

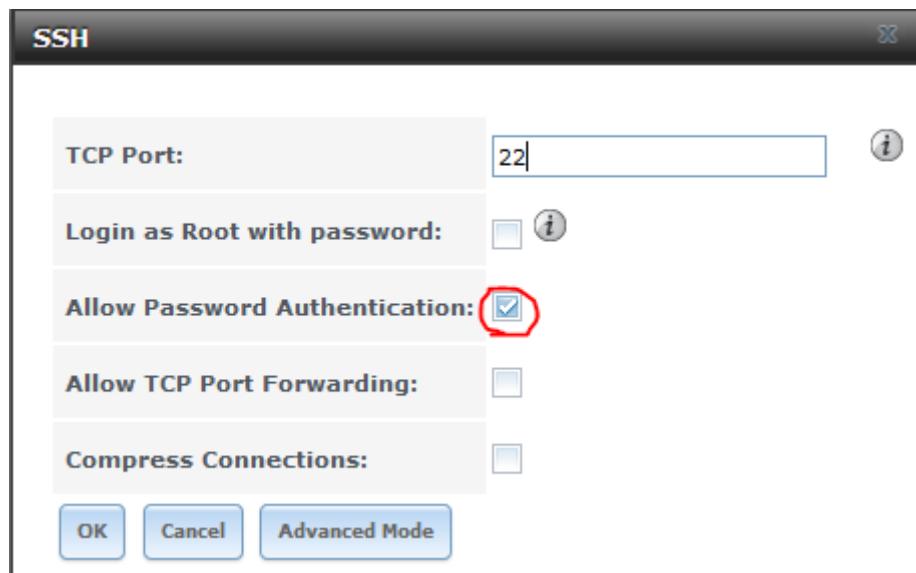
Ahora vamos a crear un usuario, para esto, nos dirigimos a la sección de usuarios y creamos uno nuevo.

Athos Orío Choperena.

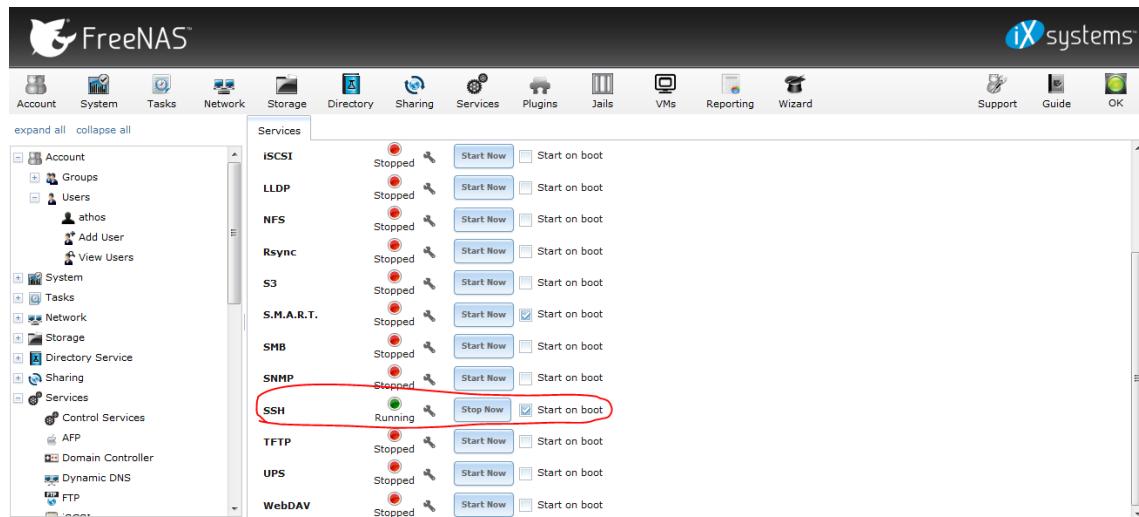


Y podemos comprobar como el usuario se ha creado.

Ahora vamos a activar el servicio ssh para poder hacer las copias de seguridad con cobian de forma segura.



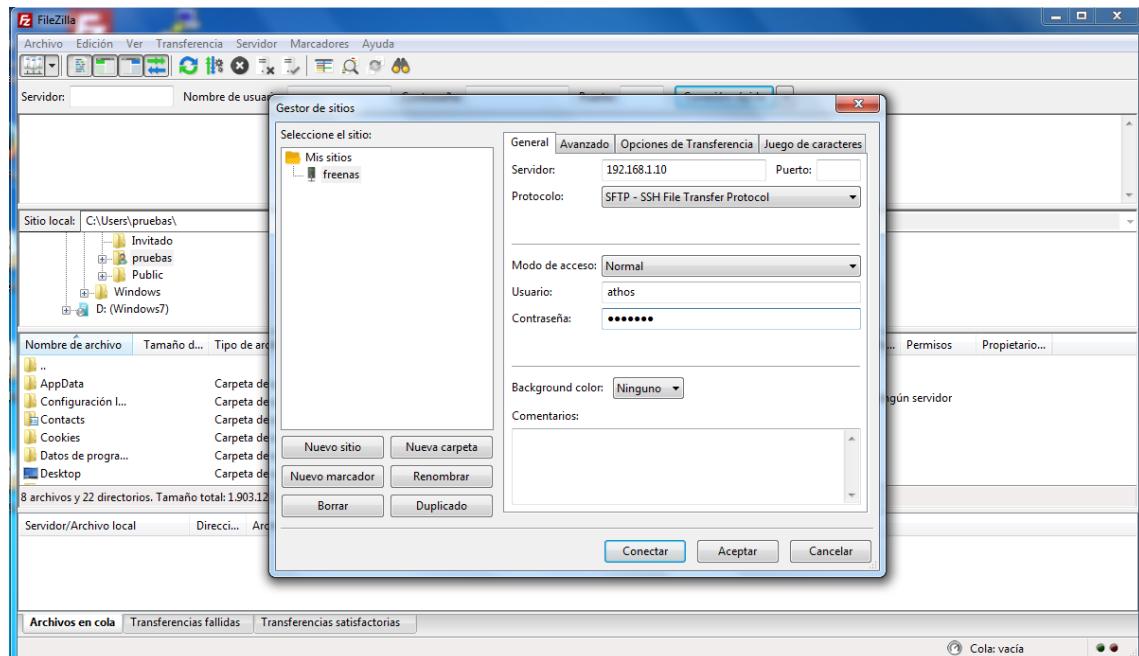
Y lo iniciamos



Copia de seguridad con windows

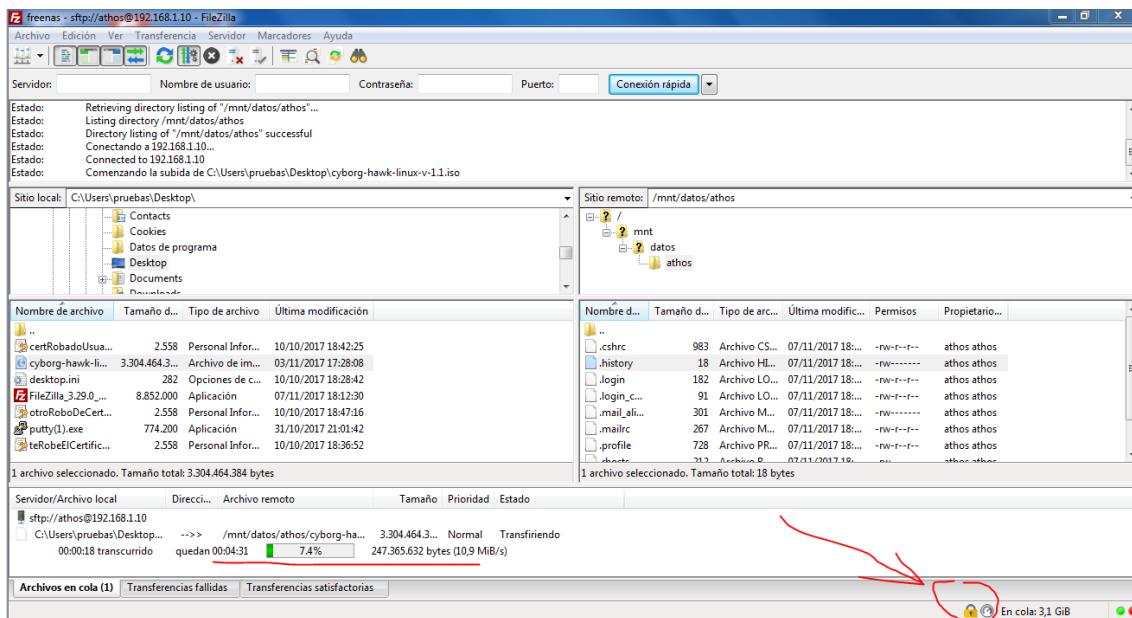
Vamos a hacer una prueba con filezilla para ver si nos deja conectarnos por sftp

Configuraremos una cuenta



Y probamos a conectarnos y a enviar algo

Athos Orío Choperena.



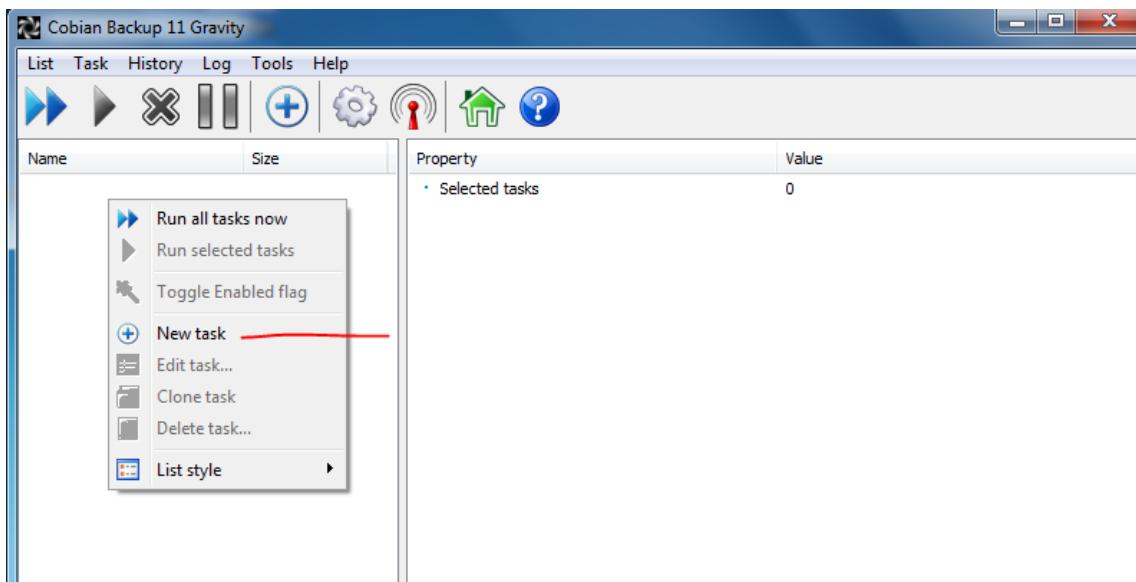
Y podemos comprobar que nos deja copiar cosas. Bien, ahora vamos a configurar cobian para que nos haga copias de seguridad.

Lo instalamos siguiendo el asistente.

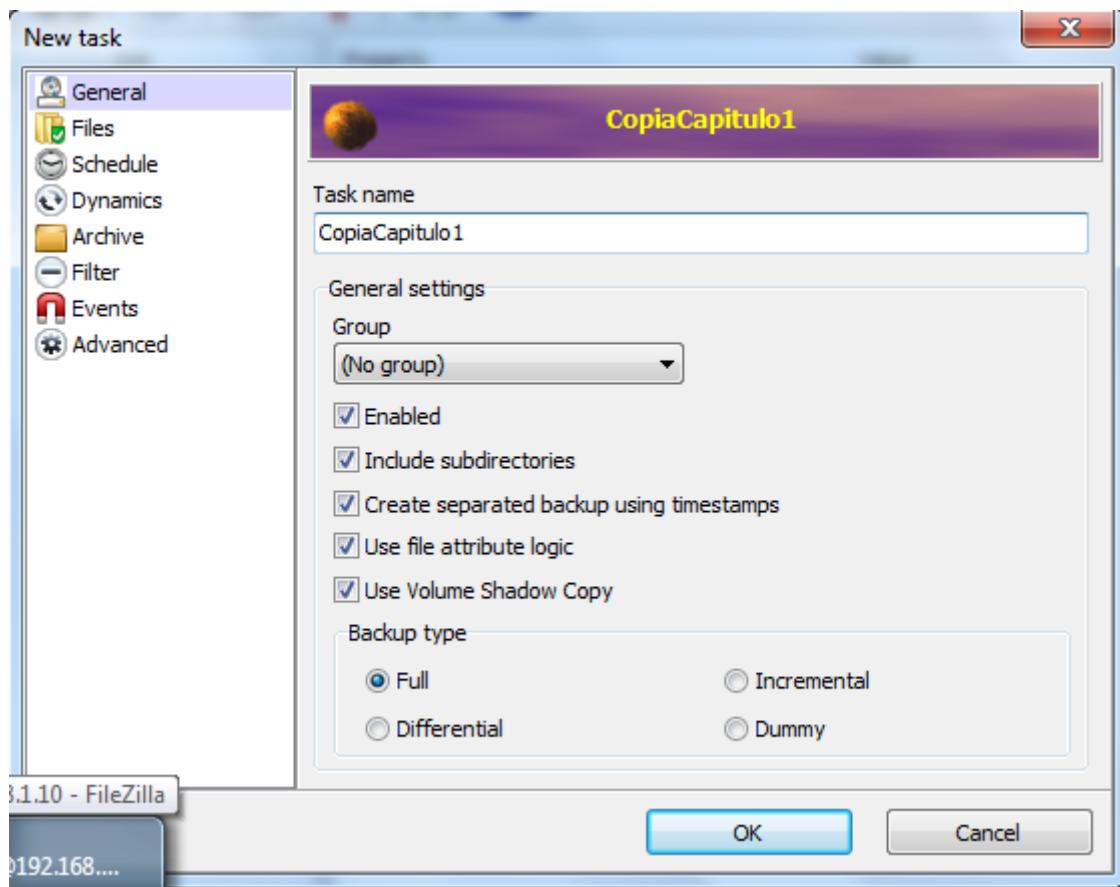


Una vez instalado abrimos cobian y creamos una nueva tarea

Athos Orío Choperena.

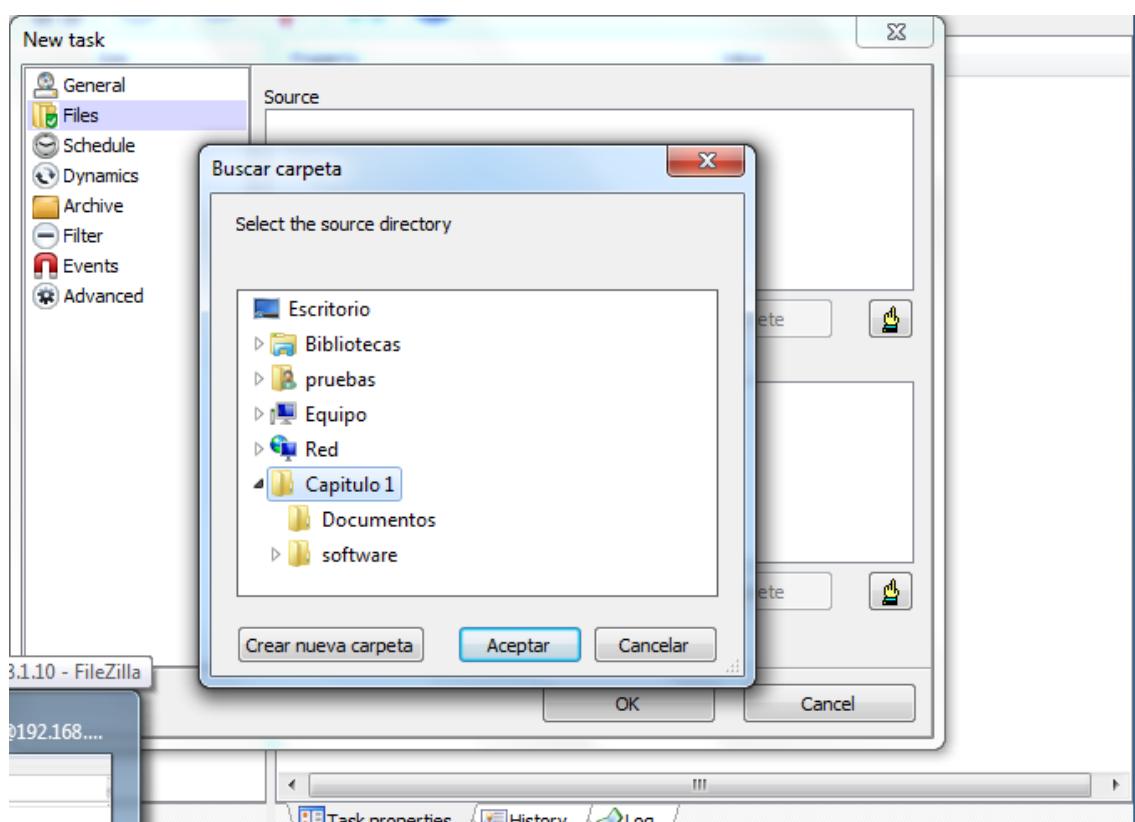
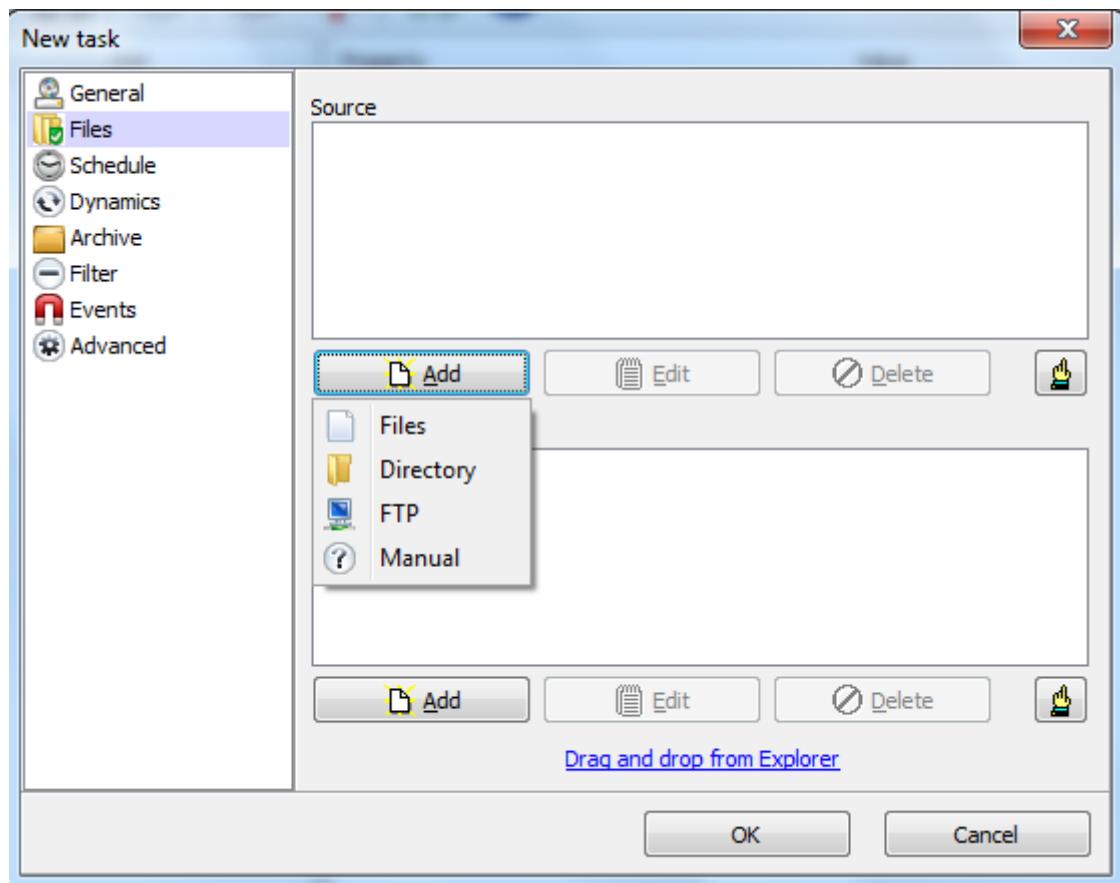


Le ponemos el nombre para poder identificar la tarea



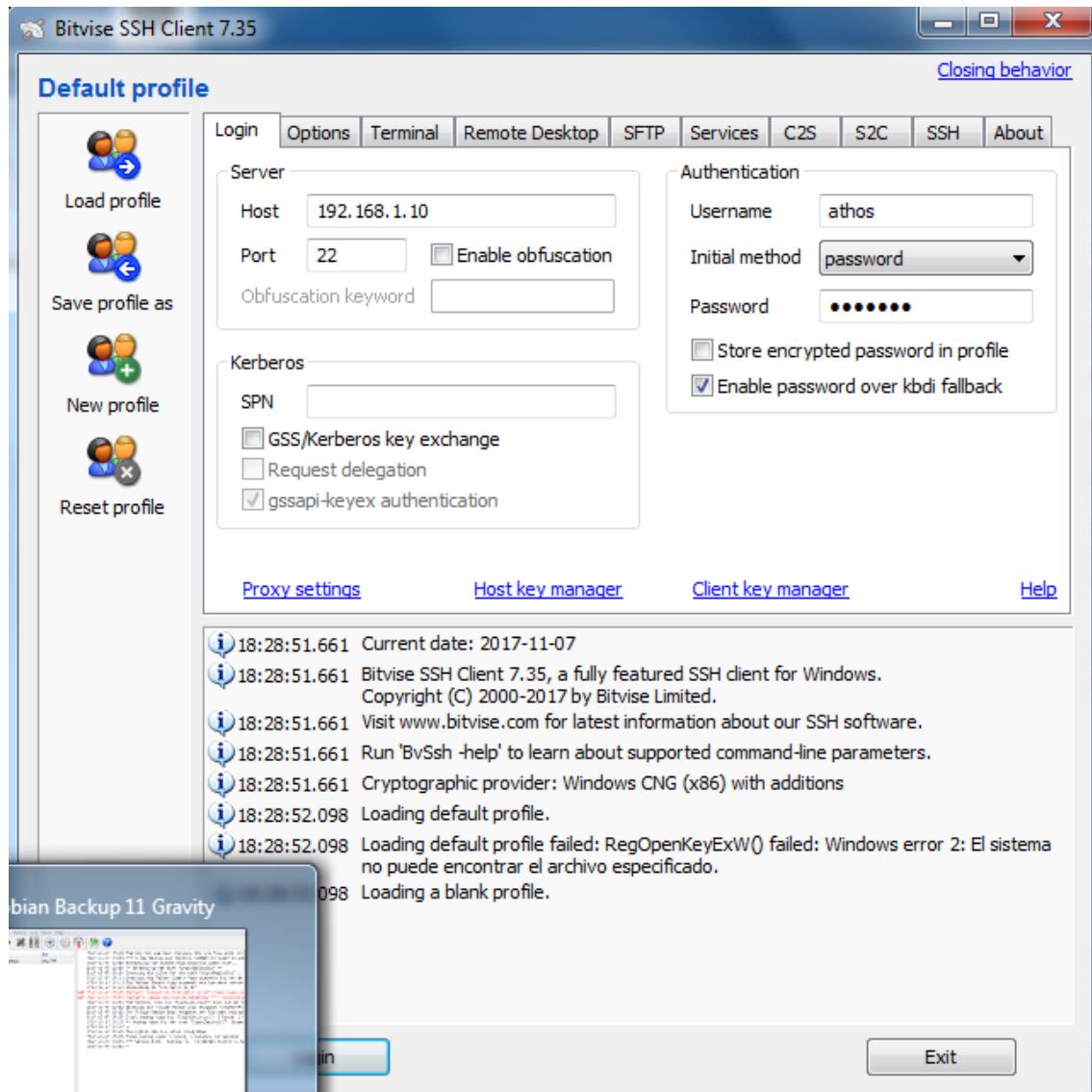
En la pestaña Files, seleccionamos en source el botón add y elegimos que es lo que queremos hacer el backup, en este caso será la carpeta capítulo1 que tenemos en el escritorio.

Athos Orío Choperena.

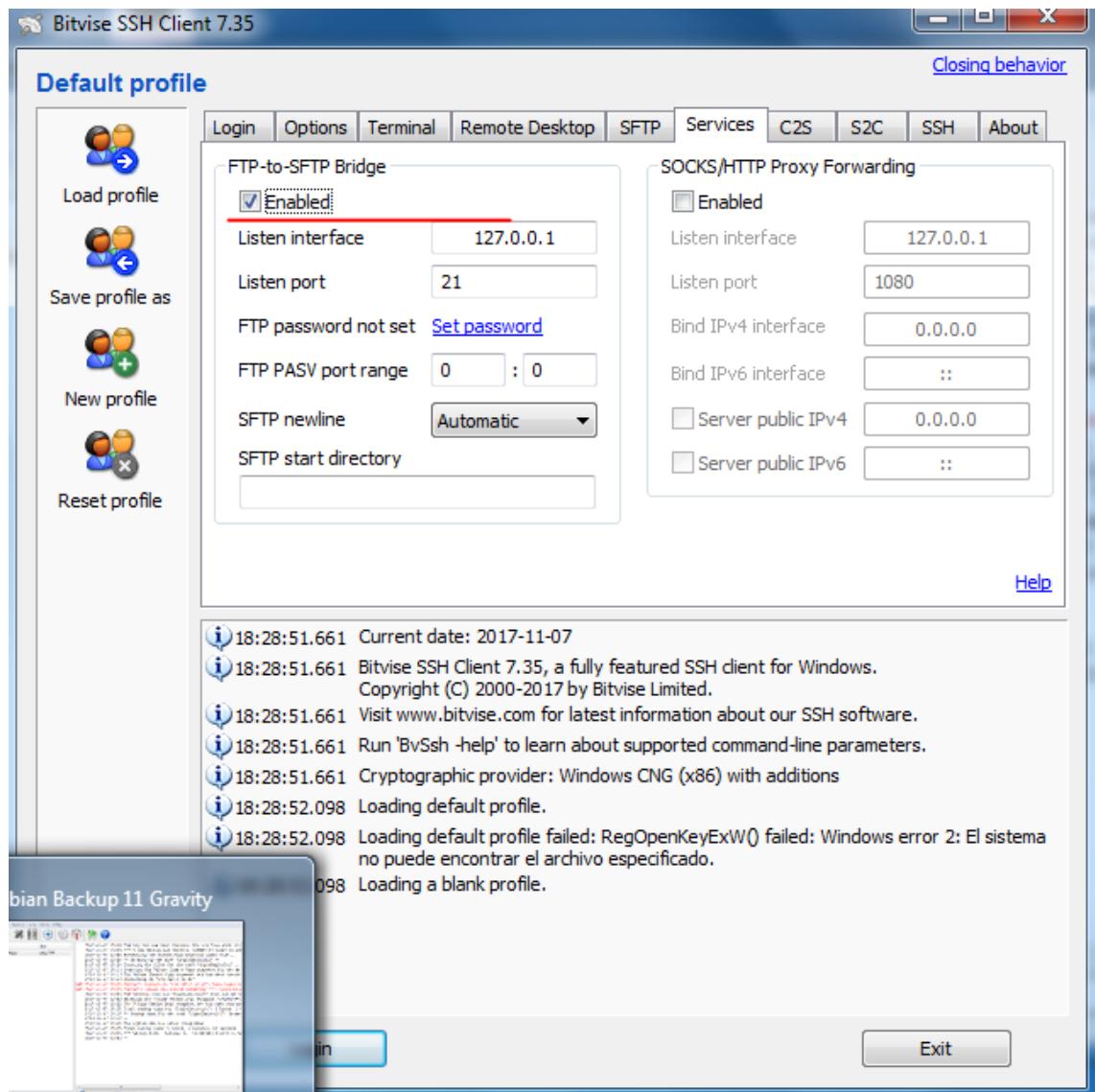


Como cobian no tiene cliente sftp, vamos a utilizar el software bitvise para que haga de túnel.

Lo instalamos y al abrirlo, podremos rellenar los datos de ssh de nuestro usuario en freenas

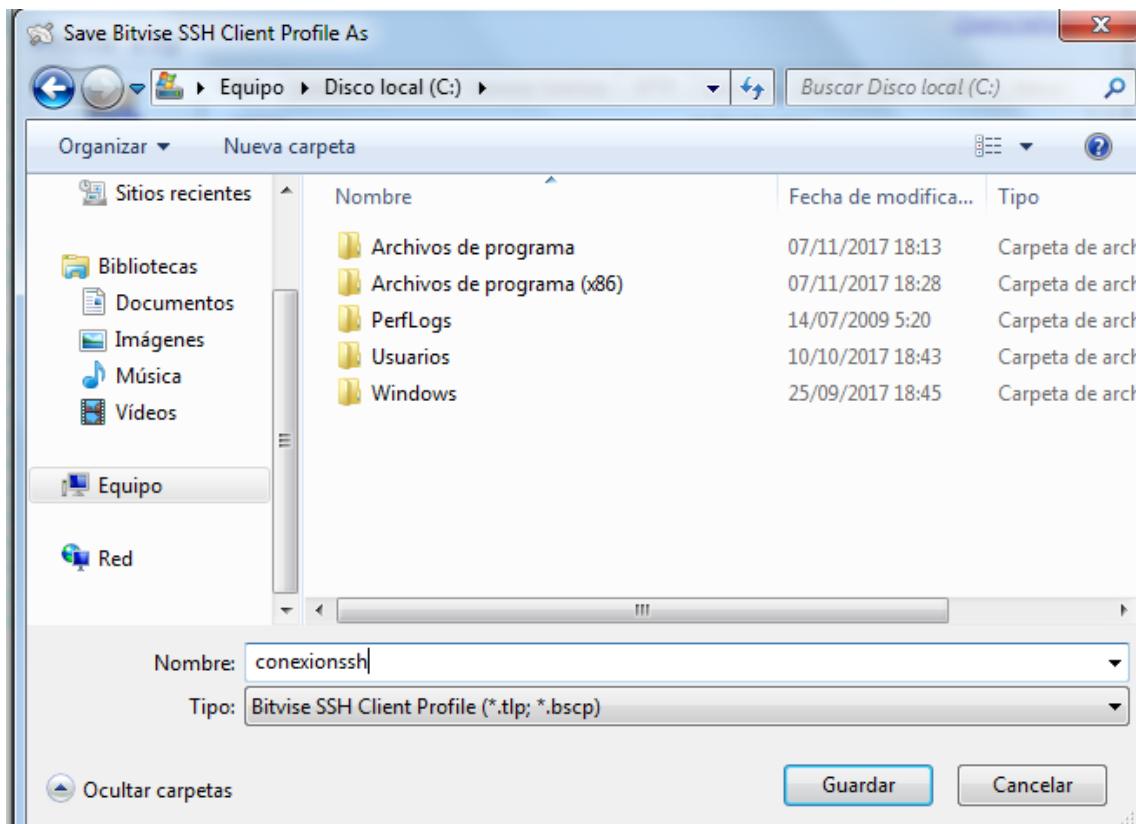


Y en services activamos ftp-to-sftp bridge

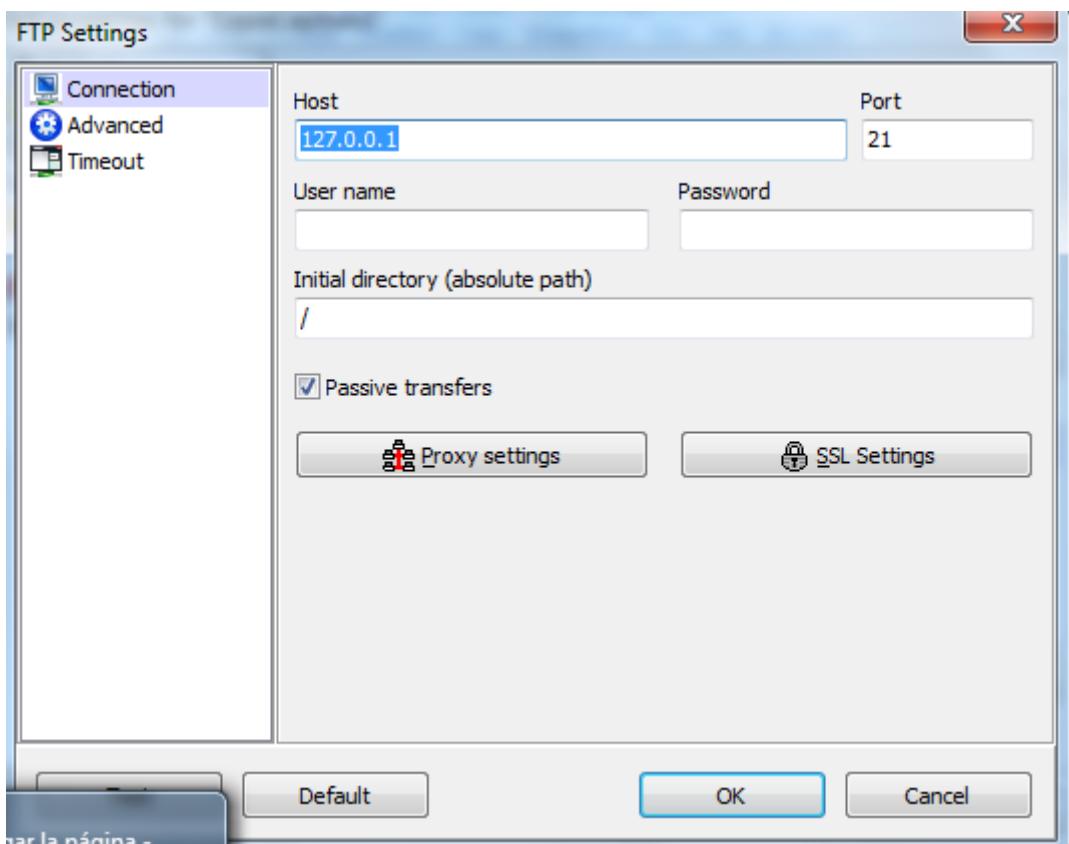


Guardamos la configuración que usaremos luego en cobian

Athos Orío Choperena.



Una vez hecho esto, en cobian ponemos como destino ftp con dirección 127.0.0.1 y puerto 21, para que bitvise haga de puente



En eventos Pre-Respaldo añadimos el comando que llamara al túnel:

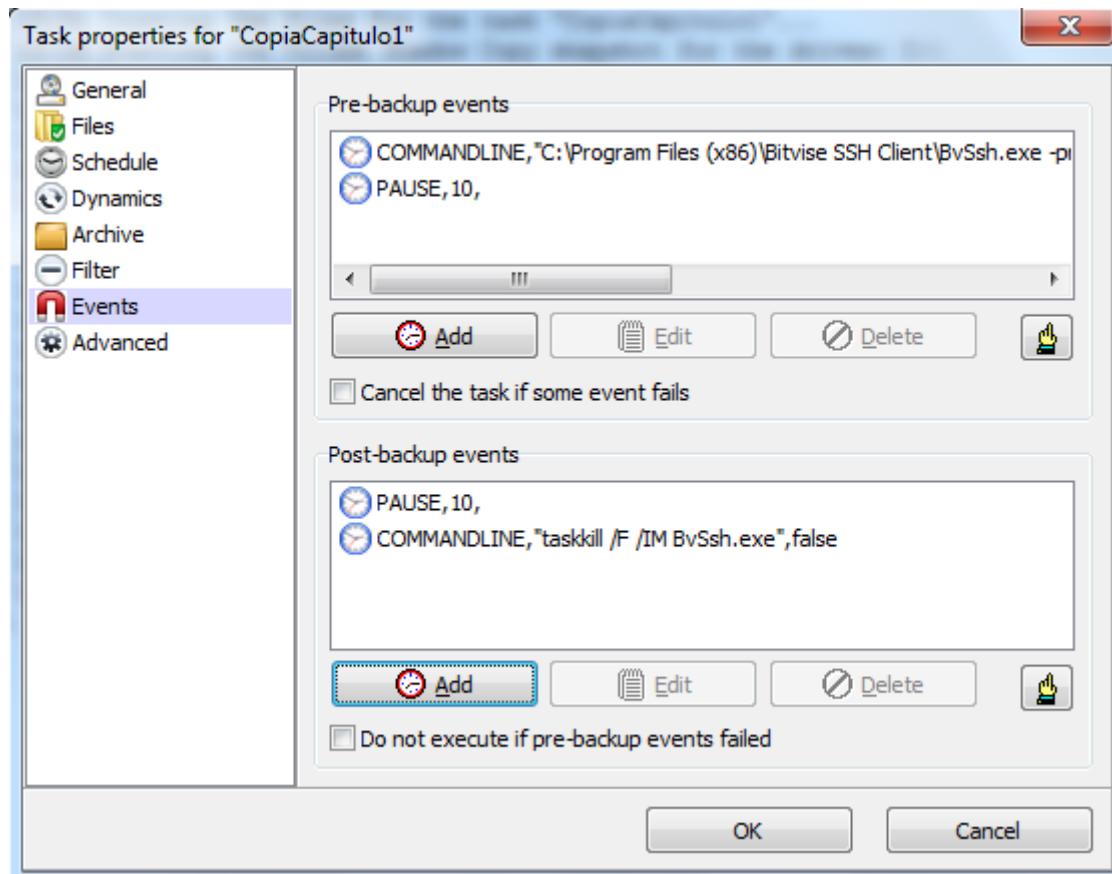
Athos Orío Choperena.

```
C:\Program Files (x86)\Bitvise SSH Client\BvSsh.exe -profile=C:\Users\pruebas.tlp -hide=main -  
loginonstartup -autoLogout -exitOnLogout",false
```

Añadimos una pausa de 10 segundos para que dé tiempo a conectarse

En eventos Post-respaldo añadimos un comando para que cierre la conexión si es que no se cerró, previamente ponemos una pausa de 10 segundos

Y debería quedar de la siguiente manera



Ahora ejecutamos la tarea y vemos como se hace la copia correctamente

The screenshot shows the Cobian Backup 11 Gravity interface. On the left, a tree view lists tasks: 'CopiaCapítulo1'. The main pane displays a detailed log of the backup process:

```

2017-11-07 18:51 The log tab has been cleared. The log file with its full content is still available from the Log menu
2017-11-07 18:51 Preventing the system from entering sleep mode...
2017-11-07 18:51 ** Backing up the task "CopiaCapítulo1"...
2017-11-07 18:51 Counting the files for the task "CopiaCapítulo1"...
2017-11-07 18:51 Executing the pre-backup events
2017-11-07 18:51 Executing the command "C:\Program Files (x86)\Birvise SSH Client\BuSsh.exe -profile=C:\Users\pruebas.rlp -hide=main -loginonstart=auto"
2017-11-07 18:51 The command "C:\Program Files (x86)\Birvise SSH Client\BuSsh.exe -profile=C:\Users\pruebas.tlp -hide=main -loginonstart=auto"
2017-11-07 18:51 Pausing the working thread "10" seconds
2017-11-07 18:52 The working thread was successfully paused
2017-11-07 18:52 Starting the Volume Shadow Copy snapshot for the drives: C:\*
2017-11-07 18:52 The Volume Shadow Copy snapshot set has been created successfully
2017-11-07 18:52 Connecting to "127.0.0.1:21"
2017-11-07 18:52 TLS is not available on this server. Trying a plain connection...
2017-11-07 18:52 The user "" has initiated a session on "127.0.0.1:21"
2017-11-07 18:52 The remote directory "Capítulo 1 2017-11-07 18:52:10 (Full)" was successfully created
2017-11-07 18:52 The remote directory has been changed to "Capítulo 1 2017-11-07 18:52:10 (Full)"
2017-11-07 18:52 Uploading the directory "C:\PRUEBAS\DESKTOP\ANDRÍDICO\BUSSH\SHADOWCOPY12\USERS\PRUEBAS\Desktop\Capítulo 1"
2017-11-07 18:52 Changing the history item to Parked. Reason: first backup
2017-11-07 18:52 Deleting the Volume Shadow Copy snapshot "da56a6d8-5bf9-4d11-a1e-f5a592732db5"
2017-11-07 18:52 The Volume Shadow Copy snapshot set has been successfully deleted
2017-11-07 18:52 Executing the post-backup events
2017-11-07 18:52 Pausing the working thread "10" seconds
2017-11-07 18:52 The working thread was successfully paused
2017-11-07 18:52 Executing the command "taskkill /F /IM BuSsh.exe" externally. Waiting for the user interface's response...
2017-11-07 18:52 The command "taskkill /F /IM BuSsh.exe" was successfully executed by the user interface
2017-11-07 18:52 Total backup time for "CopiaCapítulo1": 0 hours, 0 minutes, 35 seconds
2017-11-07 18:52 ** Backup done for the task "CopiaCapítulo1". Errors: 0. Processed files: 12. Backed up files: 12. Total size: 54,07 MB **
2017-11-07 18:52 --
2017-11-07 18:52 The system can now enter sleep mode
2017-11-07 18:52 Total backup time: 0 hours, 0 minutes, 38 seconds
2017-11-07 18:52 *** Backup done. Errors: 0. Processed files: 12. Backed up files: 12. Total size: 54,07 MB ***
2017-11-07 18:52 --

```

Below the log, a task properties window shows 'All tasks' and a file count of 12, size 54,07 MB.

The screenshot shows the FileZilla interface. On the left, a local directory tree shows files and folders like 'Desktop', 'Documents', 'Downloads', 'Entorno de red', and 'Favorites'. On the right, a 'Sitio remoto' (Remote Site) list shows a single entry: '/mnt/datos/athos' with a sub-item 'Capítulo 1 2017-11-07 18:52:10 (Full)'.

Si capturamos paquetes con wireshark vemos lo siguiente

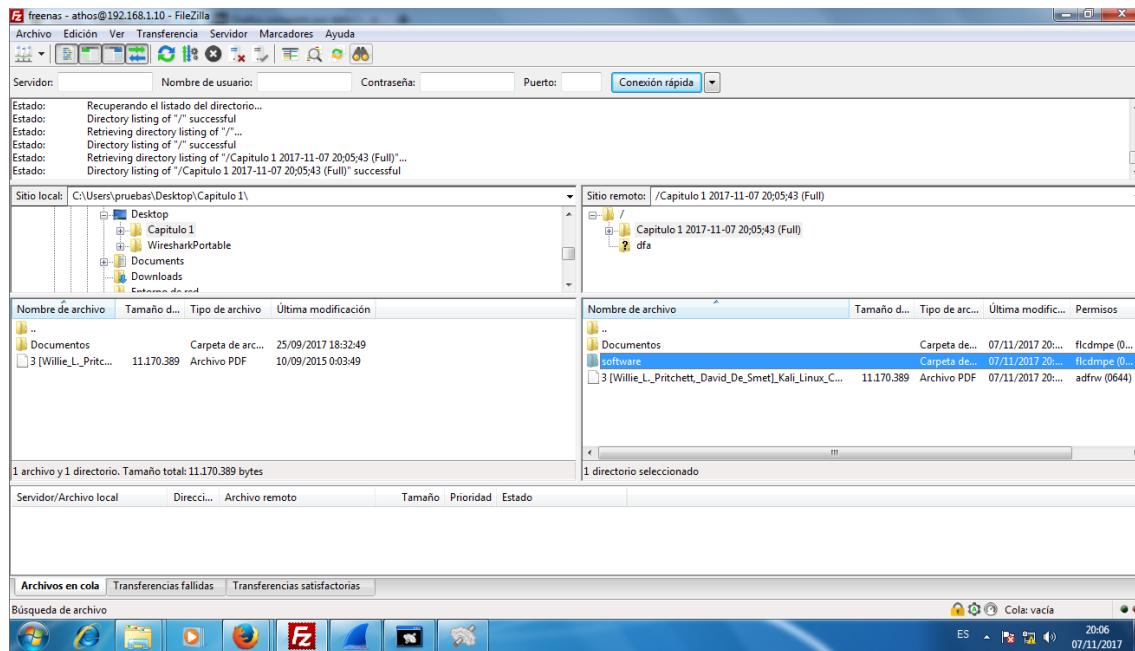
The screenshot shows a Wireshark capture window titled 'Conexión de área local [Wireshark 1.10.3 (SVN Rev 53022 from /trunk-1.10)]'. The packet list pane shows numerous TCP and SSH packets exchanged between two hosts, 192.168.1.5 and 192.168.1.10. Key observations include:

- HTTP traffic (port 80) between the two hosts.
- SSH traffic (port 22) used for remote access.
- TCP reassembly errors (reassembled PDU) indicated by green highlights in the Info column.
- Protocol analysis details at the bottom of the window, such as 'Frame 1: 92 bytes on wire (736 bits), 92 bytes captured (736 bits) on interface 0'.
- Network interface information: Ethernet II, Src: VMware_7d:5f:12 (00:0c:29:d5:f1:12), Dst: Broadcast (ff:ff:ff:ff:ff:ff).
- File navigation bar at the bottom.

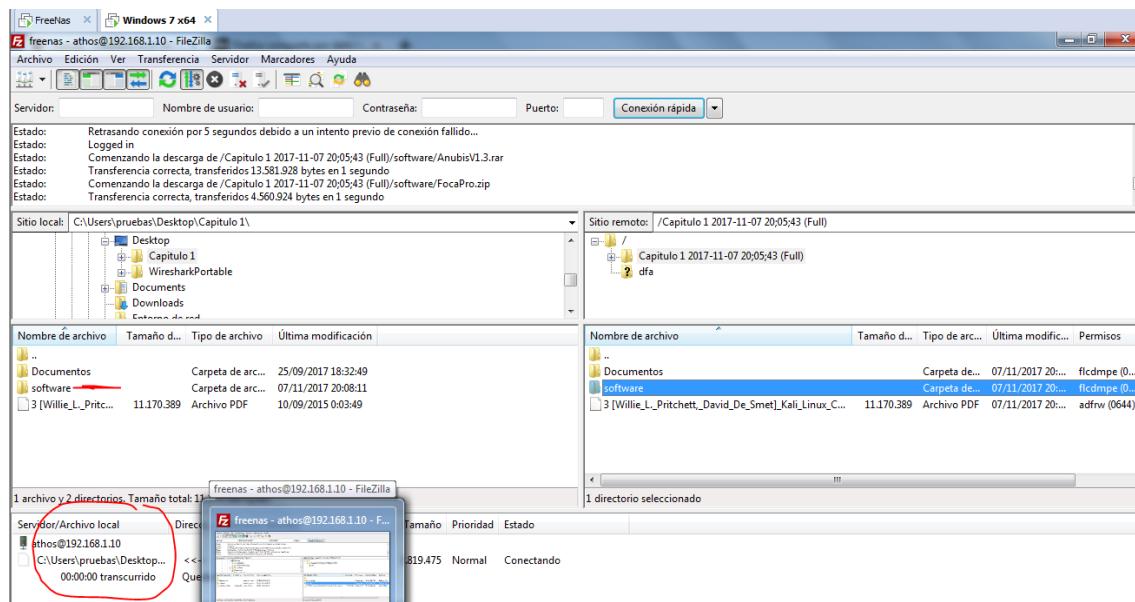
Athos Orío Choperena.

Como se ve toda la comunicación va encriptada.

Si perdiésemos un archivo, tendríamos que conectarnos al servidor, por el medio que sea (en este caso lo hacemos por ftp) y restaurar los archivos.

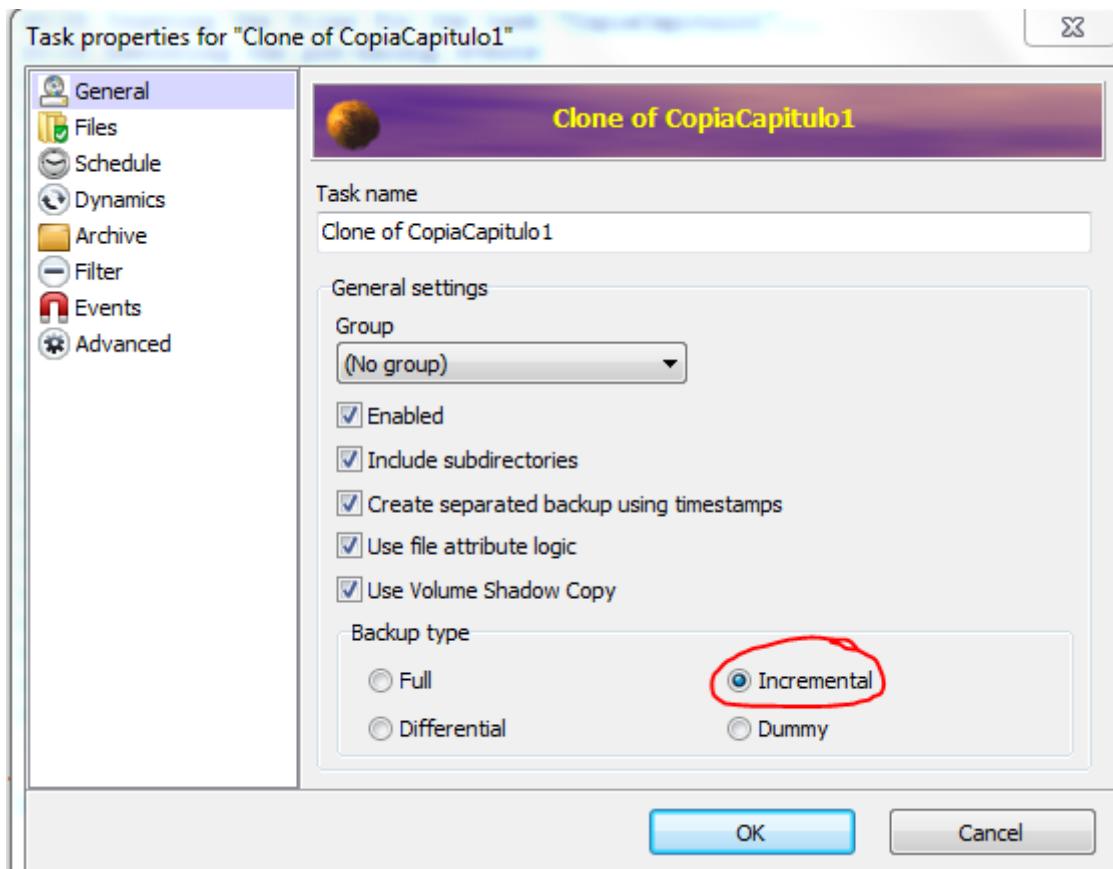


Como se ve, en el lado izquierdo, hemos perdido la carpeta software, solo tendríamos que arrastrarlo del servidor (derecha) a nuestro equipo (izquierda)

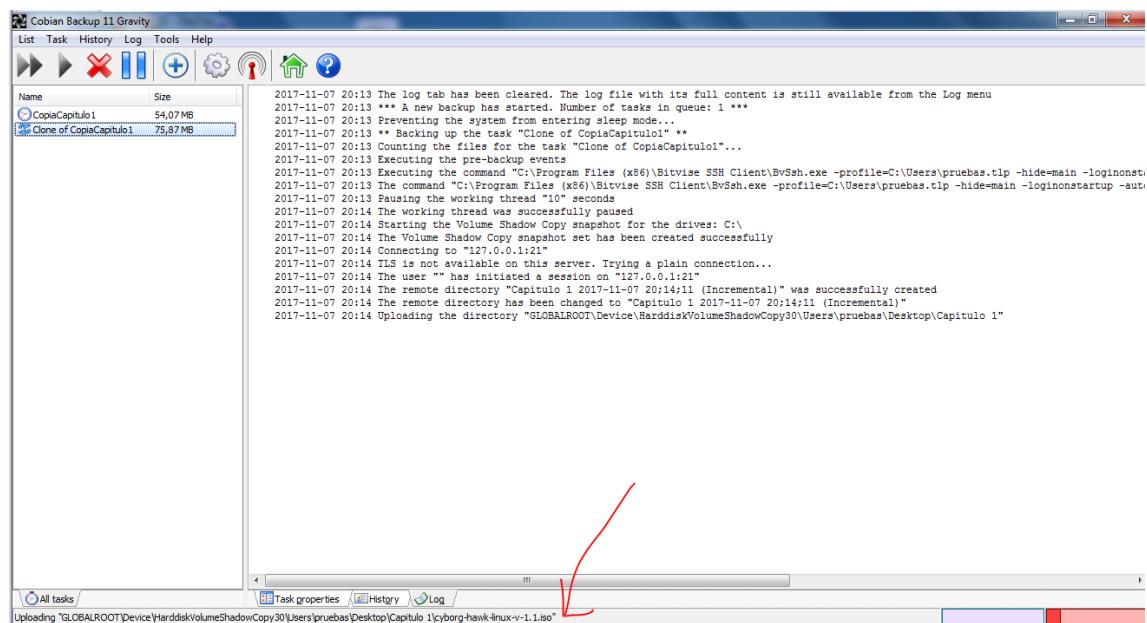


Como nota, en el configurador de la tarea, podemos configurar si queremos que la copia sea total, incremental o diferencial.

Así que vamos a duplicar la tarea anterior y haremos una copia incremental.

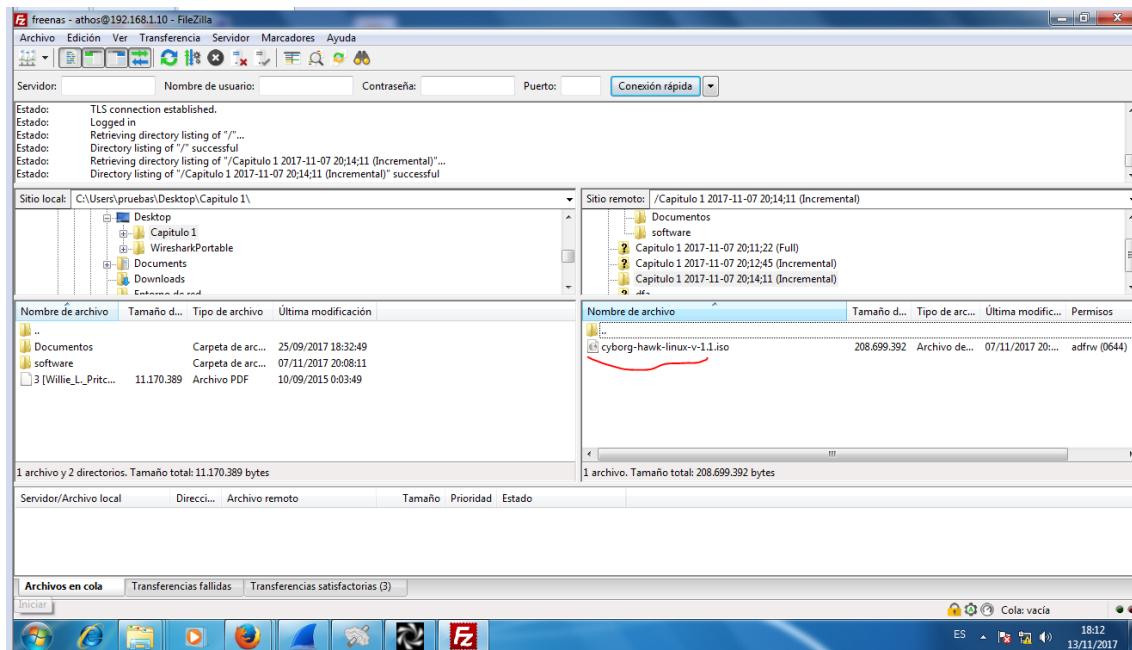


Ahora meteremos algún archivo nuevo y lo ejecutaremos.



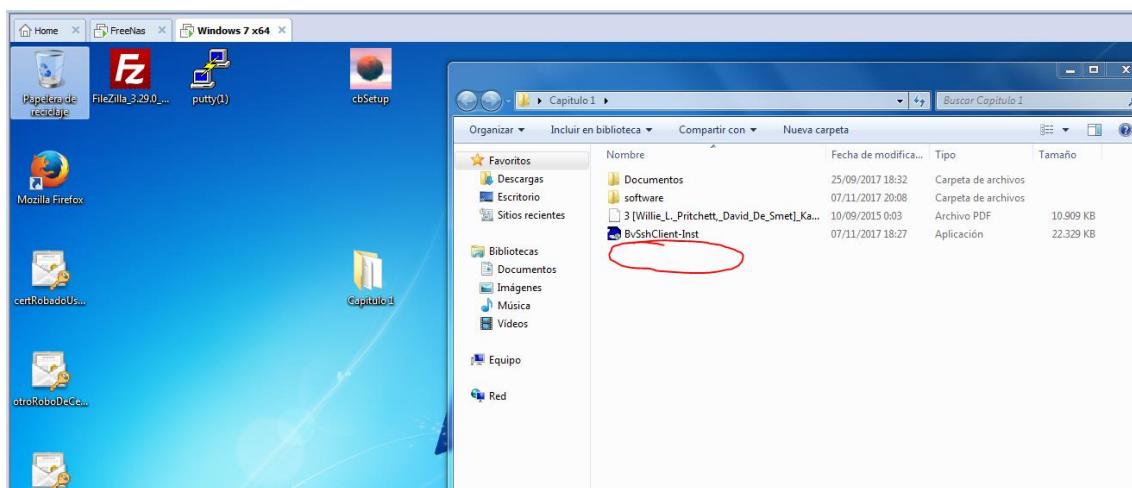
Si nos conectamos al ftp, veremos que se ha creado una nueva carpeta, y en su interior tenemos el archivo que se añadió después de la copia completa.

Athos Orío Choperena.



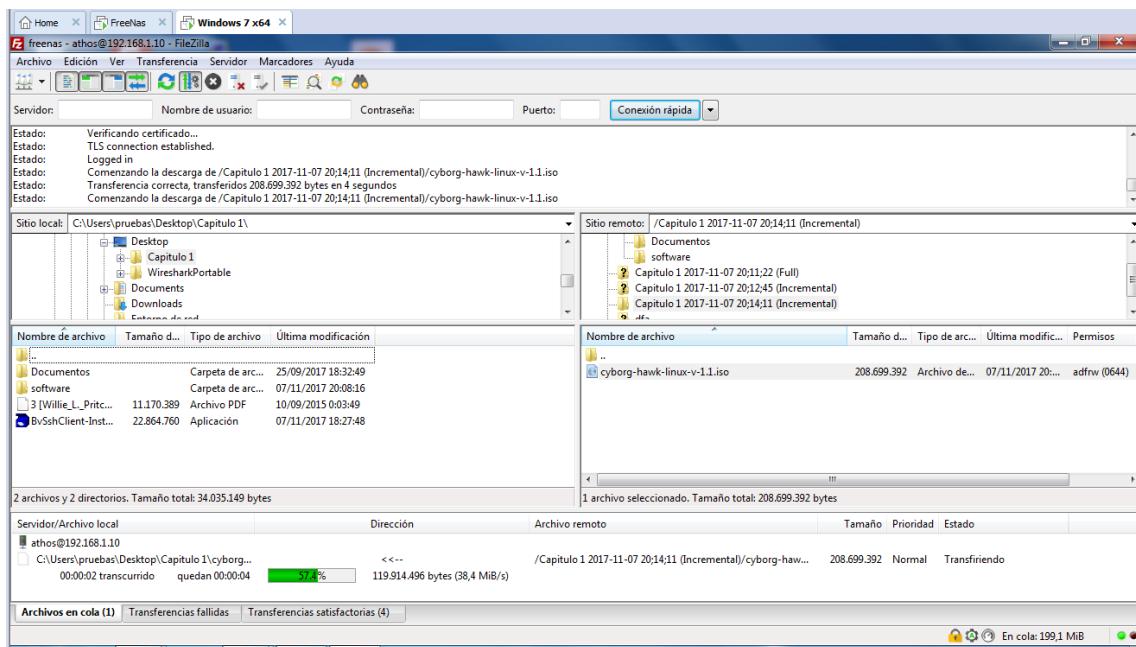
Si perdiésemos algún archivo, tendríamos que descargárnoslo desde la copia de seguridad.
Vamos a simularlo.

Borramos el archivo ciborg_xxxx.iso que teníamos en la carpeta capítulo 1

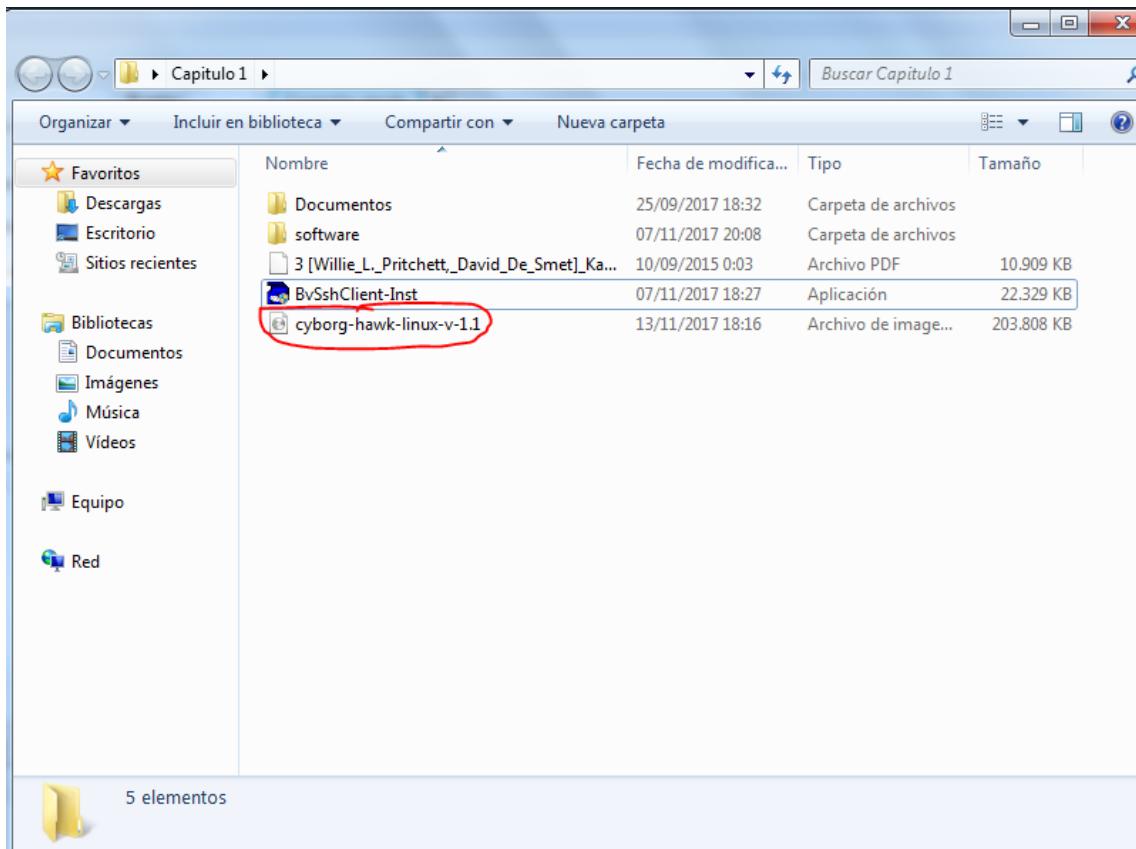


Ahora nos conectamos al ftp, y buscamos dentro de las copias que tenemos. Una vez encontrado el archivo, lo arrastraremos a la ubicación que queramos local

Athos Orío Choperena.



Y habremos recuperado el archivo perdido.



Copias de seguridad con Linux

Para realizar las copias de seguridad con Linux vamos a usar fwbackups, vamos a su página oficial y lo descargamos

The screenshot shows a Firefox browser window with the following details:

- Title Bar:** Applications ▾ Places ▾ Firefox ESR ▾ Tue 18:11
- Address Bar:** fwbackups - Download | Diffingo Solutions Inc. - Mozilla Firefox
www.diffingo.com/oss/fwbackups/download
- Page Content:**
 - Header:** Software hosted by Diffingo SOLUTIONS INC.
 - Navigation Sidebar:** Home, What is Open Source Software?, Announcements, fwbackups (Features, Screenshots, Download, FAQ, Documentation), audio-convert-mod, fwstab, Back to Diffingo.com.
 - Main Content:** fwbackups - Download Stable. It mentions the most recent version is 1.43.6 and provides links for source code (Linux) and Fedora SRPM package.
 - Right Sidebar:** Recent announcements (fwbackups 1.43.6 released, fwbackups 1.43.5 released, fwbackups 1.43.4 released, etc.).
- Bottom:** A note about Ctrl+Alt.

Viene comprimido así que lo descomprimiremos y miraremos las instrucciones de instalación.

```
root@athos: ~/fwbackups-1.43.6
File Edit View Search Terminal Help
you want to change it or regenerate `configure' using a newer version
of `autoconf'.

The simplest way to compile this package is:

1. netcd' to the directory containing the package's source code and type
`./configure' to configure the package for your system.

Running `configure' might take a while. While running, it prints
some messages telling which features it is checking for.

2. Type `make' to compile the package.

3. Optionally, type `make check' to run any self-tests that come with
the package, generally using the just-built uninstalled binaries.

4. Type `make install' to install the programs and any data files and
documentation. When installing into a prefix owned by root, it is
recommended that the package be configured and built as a regular
user, and only the `make install' phase executed with root
privileges.

5. Optionally, type `make installcheck' to repeat any self-tests, but
this time using the binaries in their final installed location.
This target does not install anything. Running this target as a
regular user, particularly if the prior `make install' required
root privileges, verifies that the installation completed
correctly.

6. You can remove the program binaries and object files from the
source code directory by typing `make clean'. To also remove the
files that `configure' created (so you can compile the package for
a different kind of computer), type `make distclean'. There is
also a `make maintainer-clean' target, but that is intended mainly
for the package's developers. If you use it, you may have to get
:
```

El primer paso es meterse en la carpeta que hemos descomprimido y ejecutar ./configure

```

root@athos: ~/fwbackups-1.43.6
File Edit View Search Terminal Help
checking whether make supports nested variables... yes
checking whether UID '0' is supported by ustar format... yes
checking whether GID '0' is supported by ustar format... yes
checking how to create a ustar tar archive... gnutar
checking for a Python interpreter with version >= 2.4... python
checking for python... /usr/bin/python
checking for python version... 2.7
checking for python platform... linux2
checking for python script directory... ${prefix}/lib/python2.7/dist-packages
checking for python extension module directory... ${exec_prefix}/lib/python2.7/dist-packages
checking whether NLS is requested... yes
checking for intltool >= 0.35.0... 0.51.0 found
checking for intltool-update... /usr/bin/intltool-update
checking for intltool-merge... /usr/bin/intltool-merge
checking for intltool-extract... /usr/bin/intltool-extract
checking for xgettext... /usr/bin/xgettext
checking for msgmerge... /usr/bin/msgmerge
checking for msgfmt... /usr/bin/msgfmt
checking for gmsgfmt... /usr/bin/gmsgfmt
checking for perl... /usr/bin/perl
checking for perl >= 5.8.1... 5.26.0
checking that generated files are newer than configure... done
configure: creating ./config.status
config.status: creating bin/Makefile
config.status: creating bin/fwbackups
config.status: creating pixmaps/Makefile
config.status: creating po/Makefile.in
config.status: creating src/Makefile
config.status: creating src/fwbackups/Makefile
config.status: creating src/fwbackups/operations/Makefile
config.status: creating src/fwbackups/_init_.py
config.status: creating src/fwbackups/const.py
config.status: creating Makefile
config.status: creating fwbackups.spec
config.status: executing po/stamp-it commands
root@athos:~/fwbackups-1.43.6#

```

Ahora ejecutamos make

```

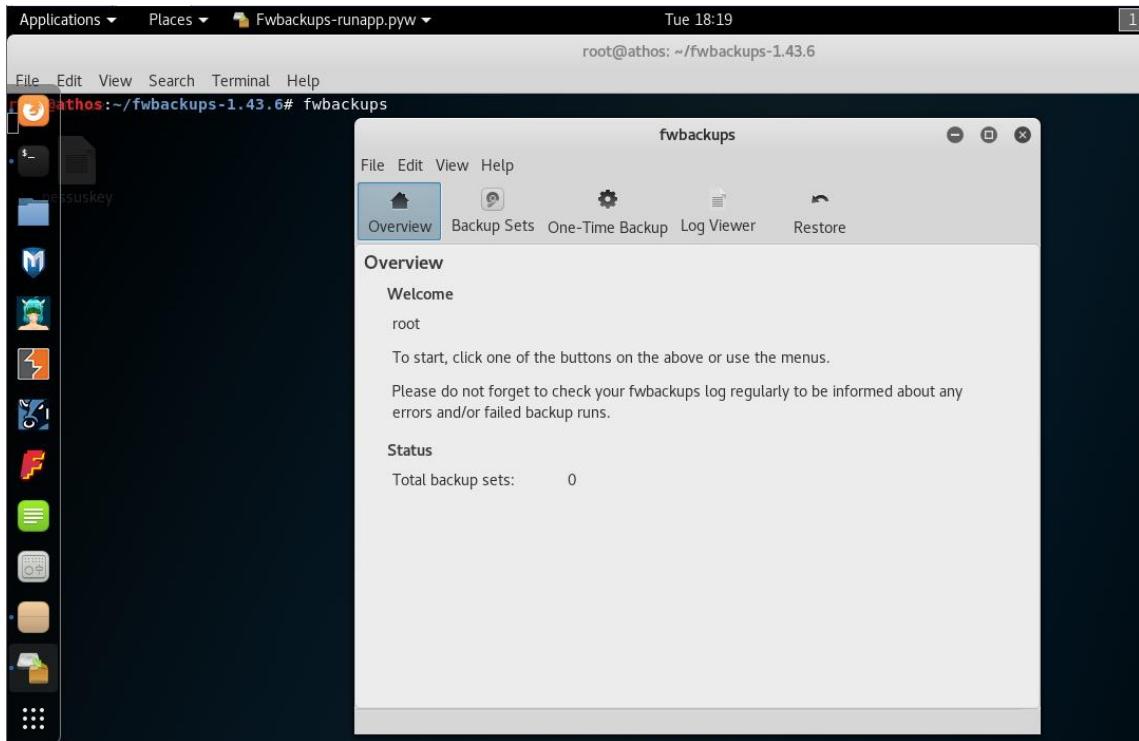
root@athos: ~/fwbackups-1.43.6
File Edit View Search Terminal Help
  && rm -f $file && /usr/bin/msgfmt -o $file is.po
file='echo lt | sed 's,.*,,` .gmo \
  && rm -f $file && /usr/bin/msgfmt -o $file lt.po
file='echo ms | sed 's,.*,,` .gmo \
  && rm -f $file && /usr/bin/msgfmt -o $file ms.po
file='echo oc | sed 's,.*,,` .gmo \
  && rm -f $file && /usr/bin/msgfmt -o $file oc.po
file='echo ru | sed 's,.*,,` .gmo \
  && rm -f $file && /usr/bin/msgfmt -o $file ru.po
file='echo sv | sed 's,.*,,` .gmo \
  && rm -f $file && /usr/bin/msgfmt -o $file sv.po
file='echo th | sed 's,.*,,` .gmo \
  && rm -f $file && /usr/bin/msgfmt -o $file th.po
file='echo uk | sed 's,.*,,` .gmo \
  && rm -f $file && /usr/bin/msgfmt -o $file uk.po
make[1]: Leaving directory '/root/fwbackups-1.43.6/po'
make all in pixmaps
make[1]: Entering directory '/root/fwbackups-1.43.6/pixmaps'
make[1]: Nothing to be done for 'all'.
make[1]: Leaving directory '/root/fwbackups-1.43.6/pixmaps'
make all in src
make[1]: Entering directory '/root/fwbackups-1.43.6/src'
make[1]: Nothing to be done for 'all'.
make[1]: Leaving directory '/root/fwbackups-1.43.6/src'
make all in src/fwbackups/operations
make[1]: Entering directory '/root/fwbackups-1.43.6/src/fwbackups/operations'
make[1]: Nothing to be done for 'all'.
make[1]: Leaving directory '/root/fwbackups-1.43.6/src/fwbackups/operations'
make all in src/fwbackups
make[1]: Entering directory '/root/fwbackups-1.43.6/src/fwbackups'
make[1]: Nothing to be done for 'all'.
make[1]: Leaving directory '/root/fwbackups-1.43.6/src/fwbackups'
make[1]: Entering directory '/root/fwbackups-1.43.6/src/fwbackups'
make[1]: Nothing to be done for 'all'.
make[1]: Leaving directory '/root/fwbackups-1.43.6/src/fwbackups'
make[1]: Entering directory '/root/fwbackups-1.43.6/src/fwbackups'
make[1]: Nothing to be done for 'all'.
make[1]: Leaving directory '/root/fwbackups-1.43.6/src/fwbackups'
root@athos:~/fwbackups-1.43.6# make

```

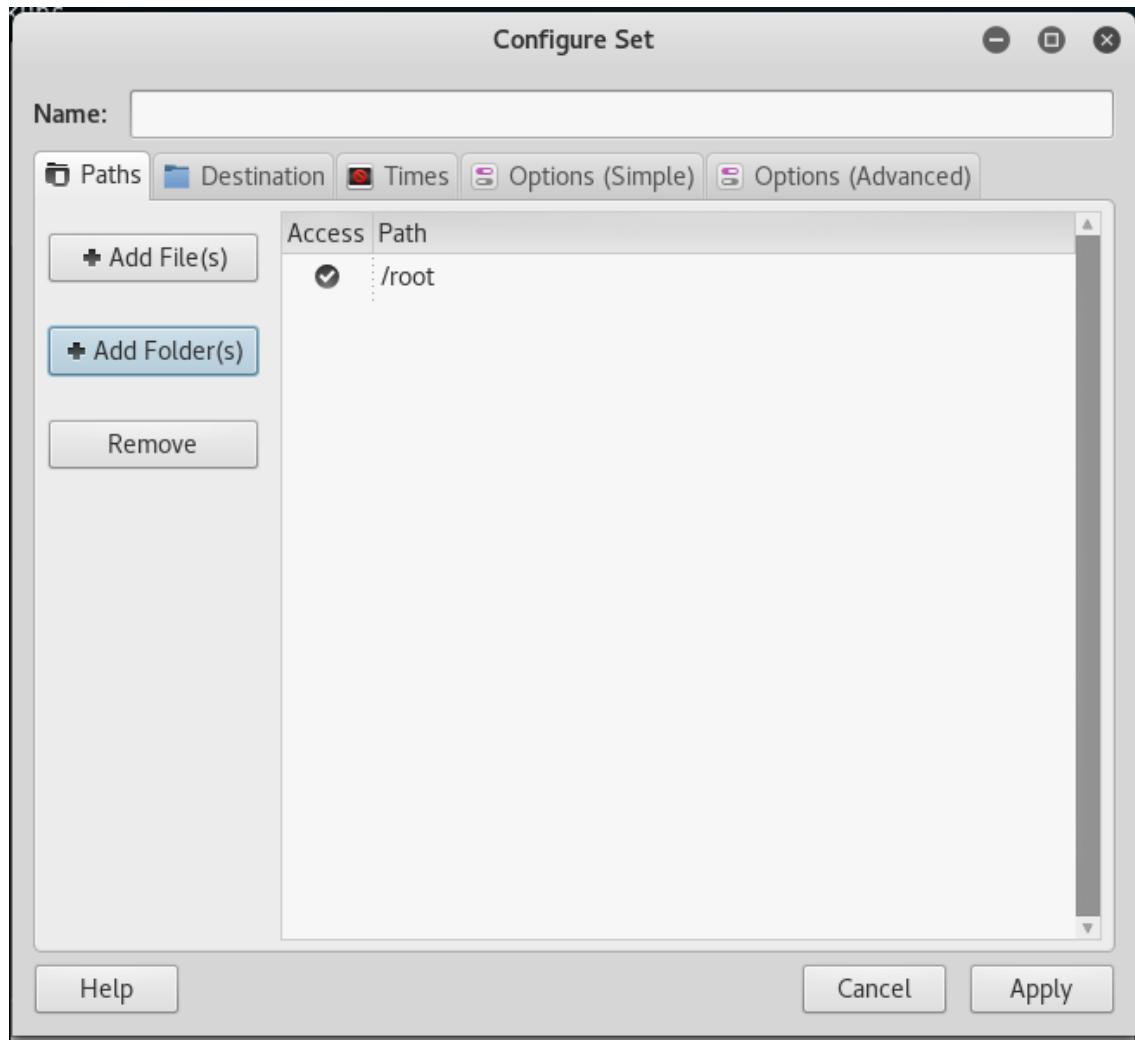
Y ahora make install

```
File Edit View Search Terminal Help
/bin/mkdir -p '/usr/local/share/fwbackups'
/usr/bin/install -c -m 644 BugReport.gladef fwbackups.glade fwbackups-autostart.desktop fwbackups-runapp.pyw '/usr/local/share/fwbackups'
make[2]: Leaving directory '/root/fwbackups-1.43.6/src'
make[1]: Leaving directory '/root/fwbackups-1.43.6/src'
Making install in src/fwbackups/operations
make[1]: Entering directory '/root/fwbackups-1.43.6/src/fwbackups/operations'
make[2]: Nothing to be done for 'install-exec-am'.
/bin/mkdir -p '/usr/local/lib/python2.7/dist-packages/fwbackups/operations'
/usr/bin/install -c -m 644 __init__.py backup.py restore.py '/usr/local/lib/python2.7/dist-packages/fwbackups/operations'
Byte-compiling python modules...
  init_.pybackup.pyrestore.py
Byte-compiling python modules (optimized versions) ...
  __init__.pybackup.pyrestore.py
make[2]: Leaving directory '/root/fwbackups-1.43.6/src/fwbackups/operations'
make[1]: Leaving directory '/root/fwbackups-1.43.6/src/fwbackups/operations'
Making install in src/fwbackups
make[1]: Entering directory '/root/fwbackups-1.43.6/src/fwbackups'
make[2]: Entering directory '/root/fwbackups-1.43.6/src/fwbackups'
make[2]: Nothing to be done for 'install-exec-am'.
/bin/mkdir -p '/usr/local/lib/python2.7/dist-packages/fwbackups'
/usr/bin/install -c -m 644 config.py const.py cron.py fwlogger.py i18n.py __init__.py interface.py sftp.py shutil_modded.py widgets.py '/usr/local/lib/python2.7/dist-packages/fwbackups'
Byte-compiling python modules...
config.pyconst.pycron.pyfwlogger.pyi18n.py __init__.pyinterface.pyshutil_modded.pywidgets.py schedule
Byte-compiling python modules (optimized versions) ...
config.pyconst.pycron.pyfwlogger.pyi18n.py __init__.pyinterface.pyshutil_modded.pywidgets.py
make[2]: Leaving directory '/root/fwbackups-1.43.6/src/fwbackups'
make[1]: Leaving directory '/root/fwbackups-1.43.6/src/fwbackups'
make[2]: Entering directory '/root/fwbackups-1.43.6'
make[2]: Nothing to be done for 'install-exec-am'.
make[2]: Nothing to be done for 'install-data-am'.
make[2]: Leaving directory '/root/fwbackups-1.43.6'
make[1]: Leaving directory '/root/fwbackups-1.43.6'
root@athos:~/fwbackups-1.43.6#
```

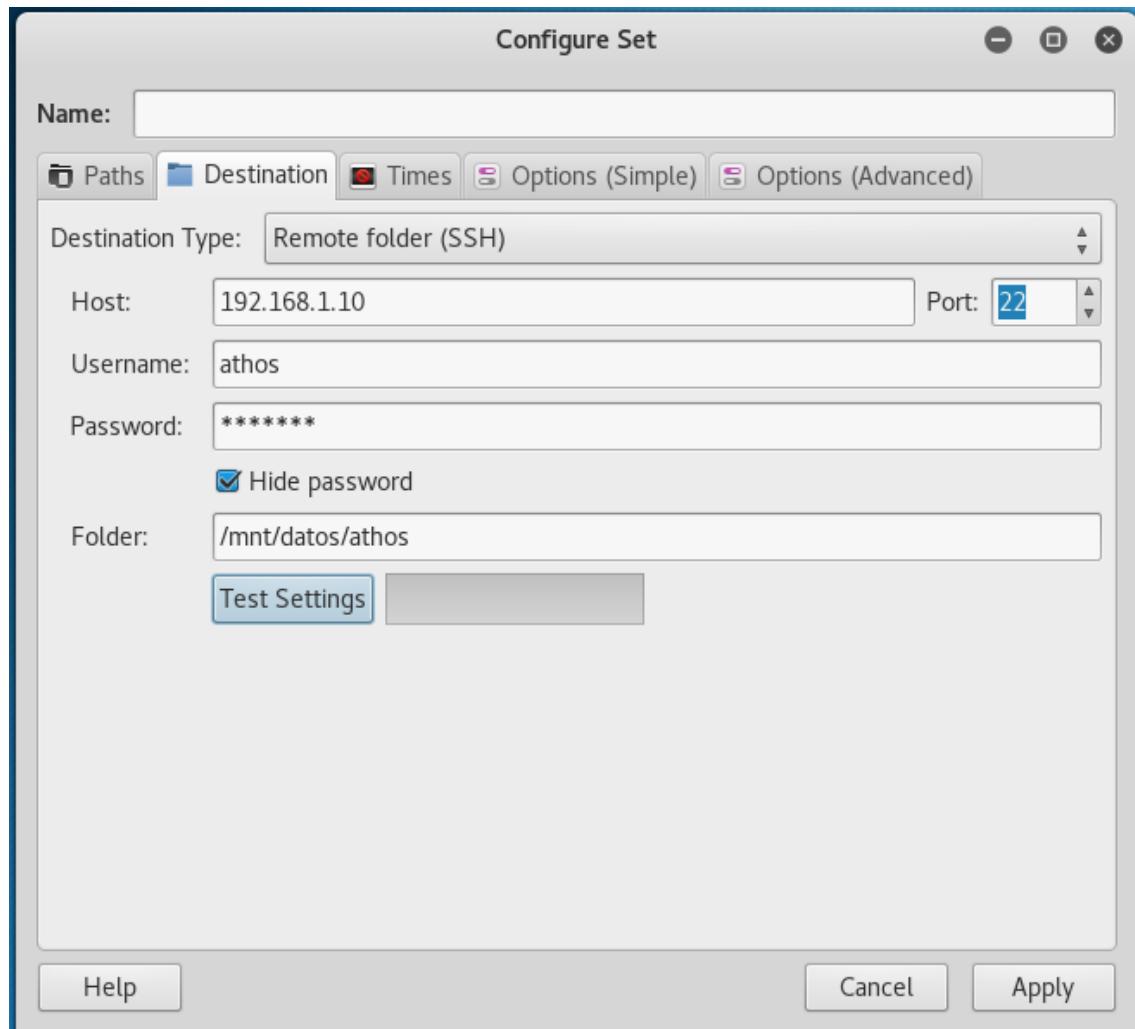
Ahora ejecutamos el programa con fwbackups



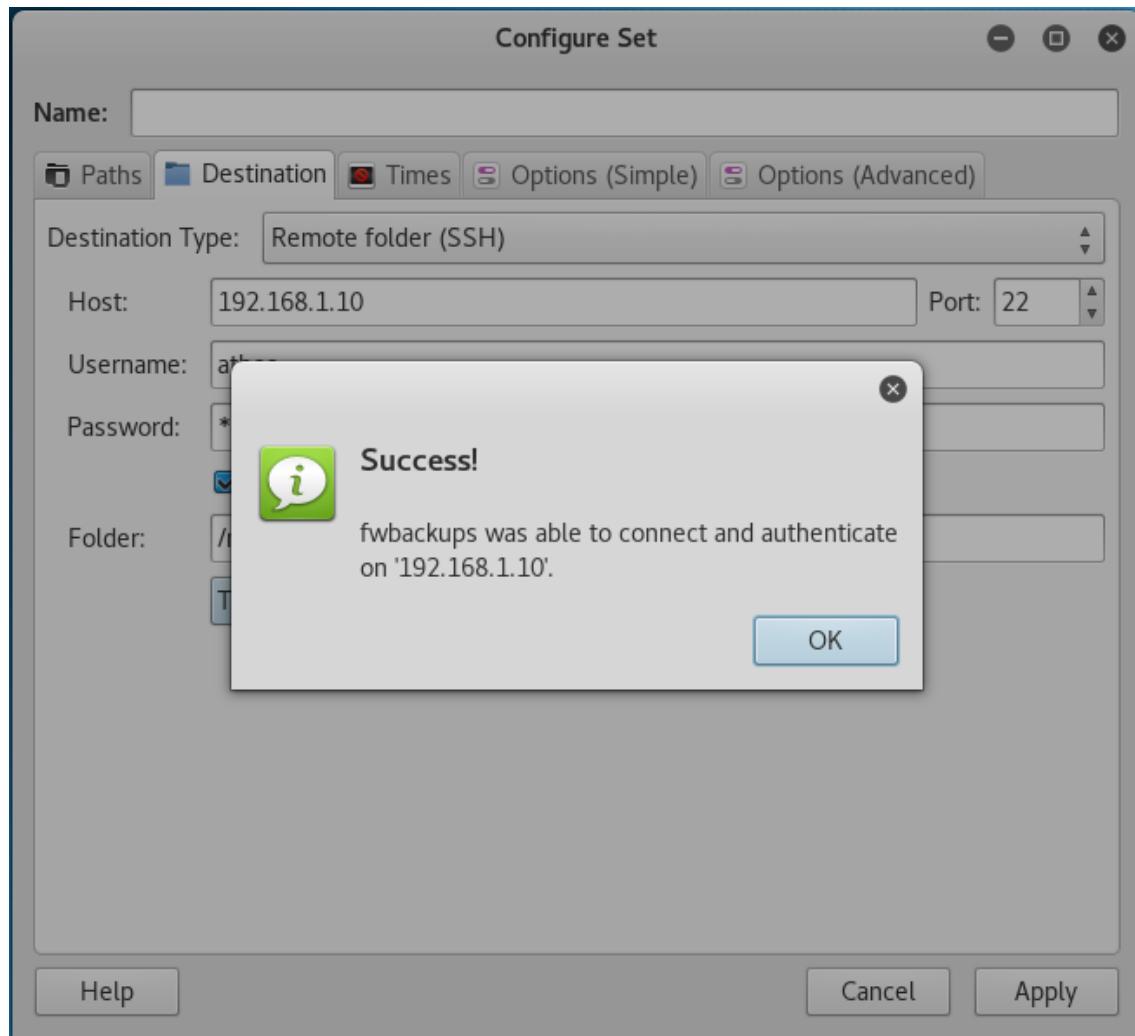
Pinchamos en backup sets y elegimos el directorio o directorios de los cuales queremos ejecutar la copia de seguridad



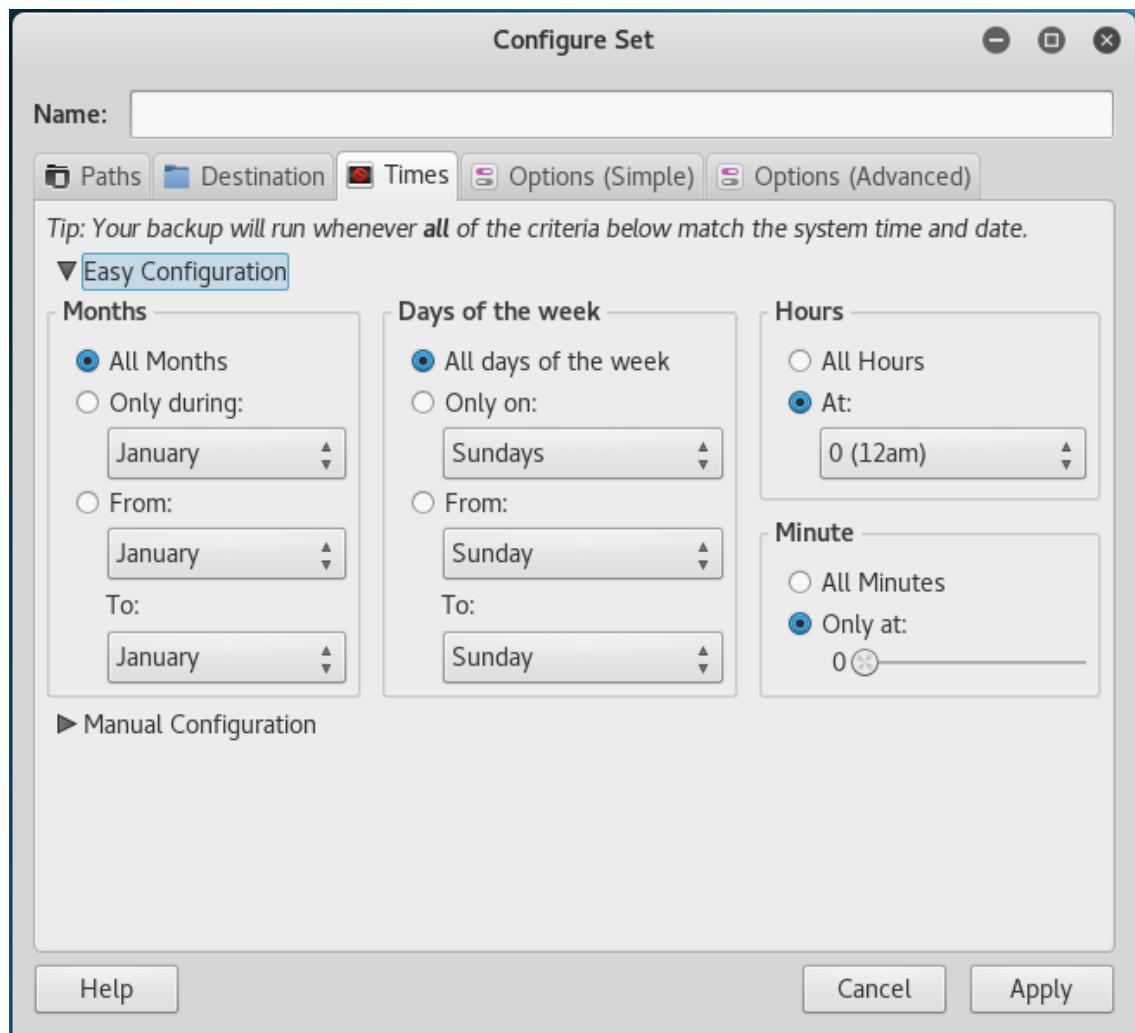
En la pestaña destination, elegimos el destino, en este caso haremos la copia por ssh.



Rellenamos los datos, y pinchamos en test settings para comprobar si la conexión se realiza de forma correcta.



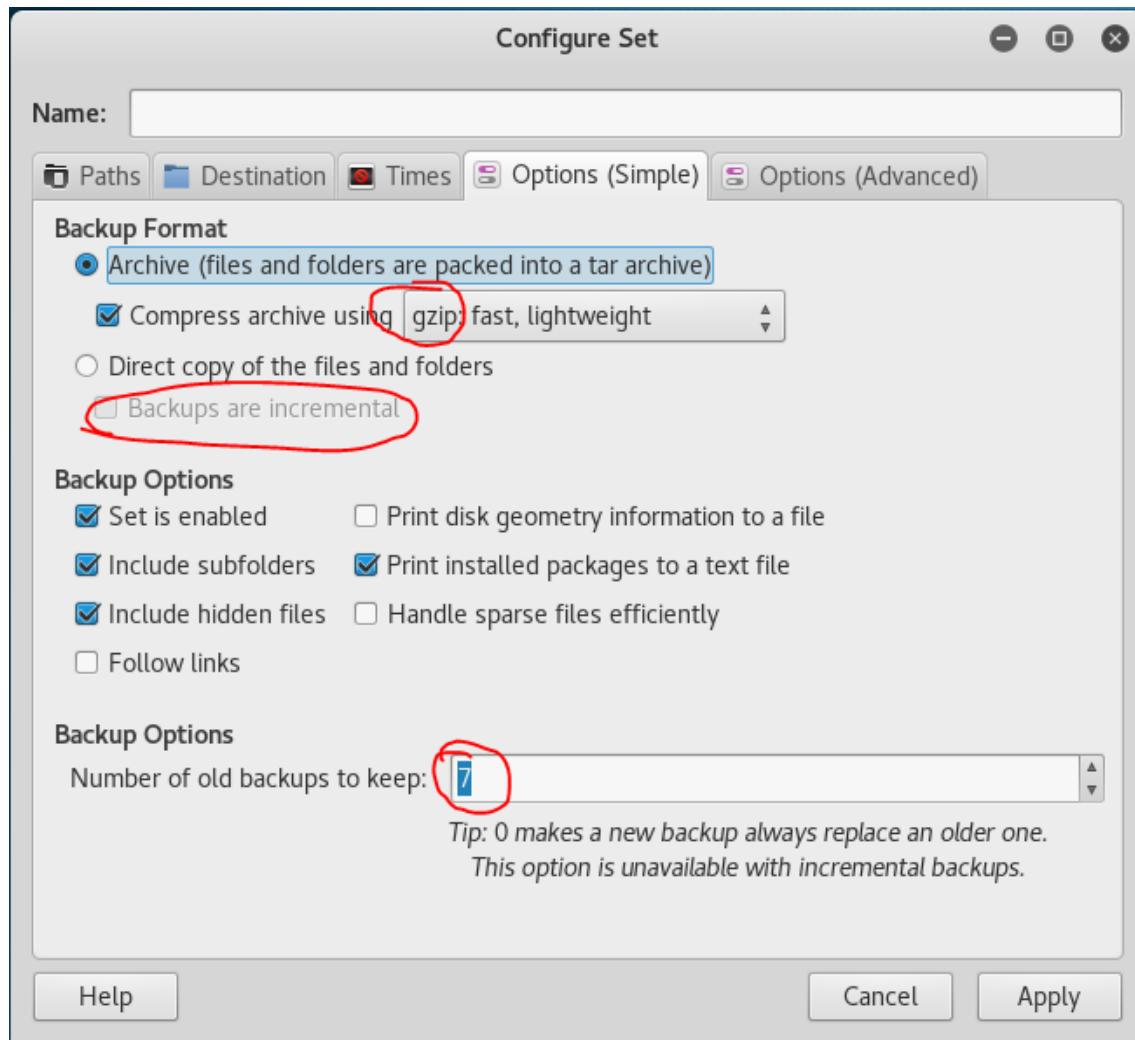
Seguimos a la pestaña times. En esta pestaña configuramos cuando queremos que se realice la copia de seguridad.



Lo configuramos para que haga la copia de seguridad todos los meses, todos los días de la semana, a las 12:00 de la mañana.

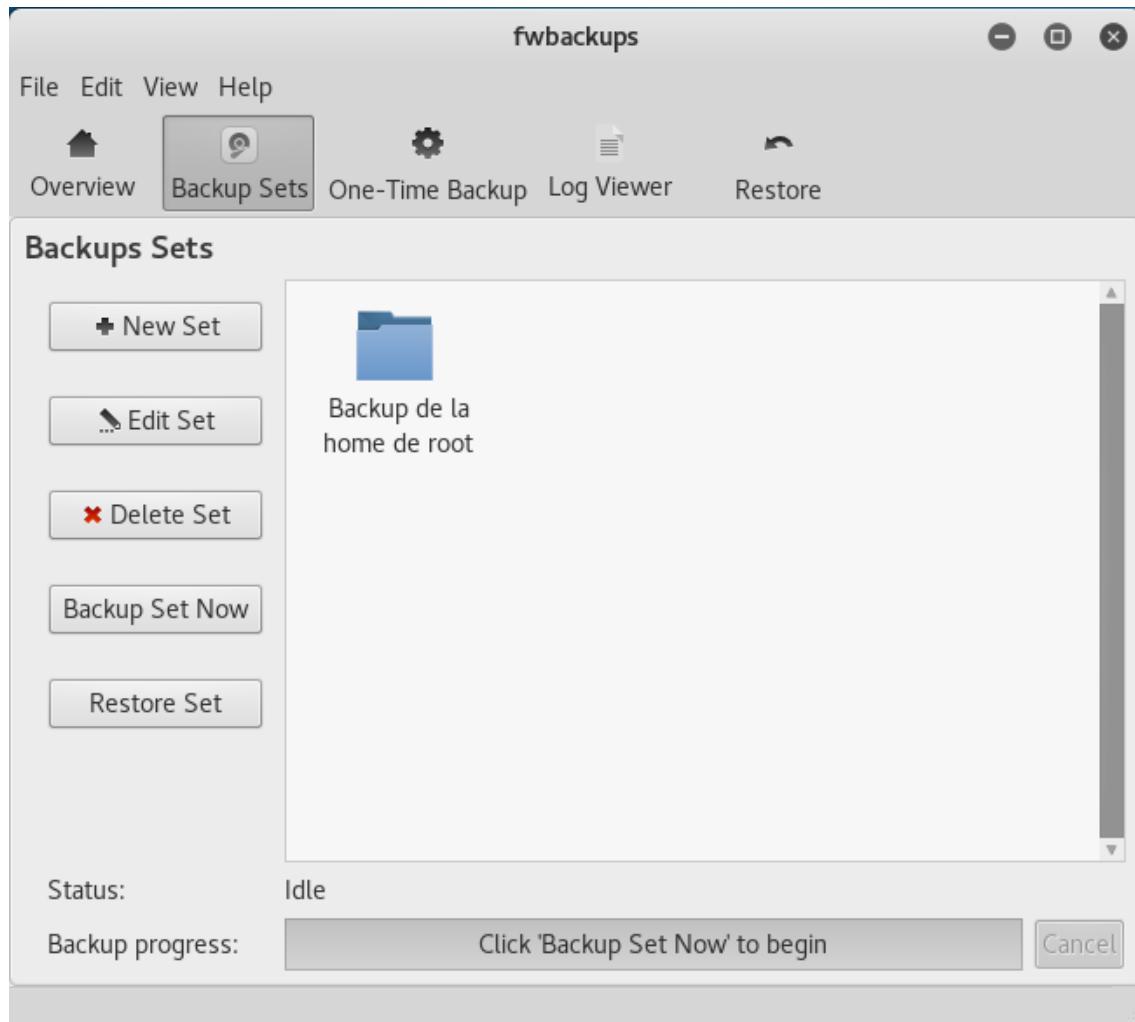
En la pestaña options (simple) entre otras cosas podemos configurar si queremos que se comprima , en este caso vamos a seleccionar gzip.

También podemos configurar el número de Backups que queremos que nos guarde, vamos a poner 7 para que nos guarde los últimos 7 días

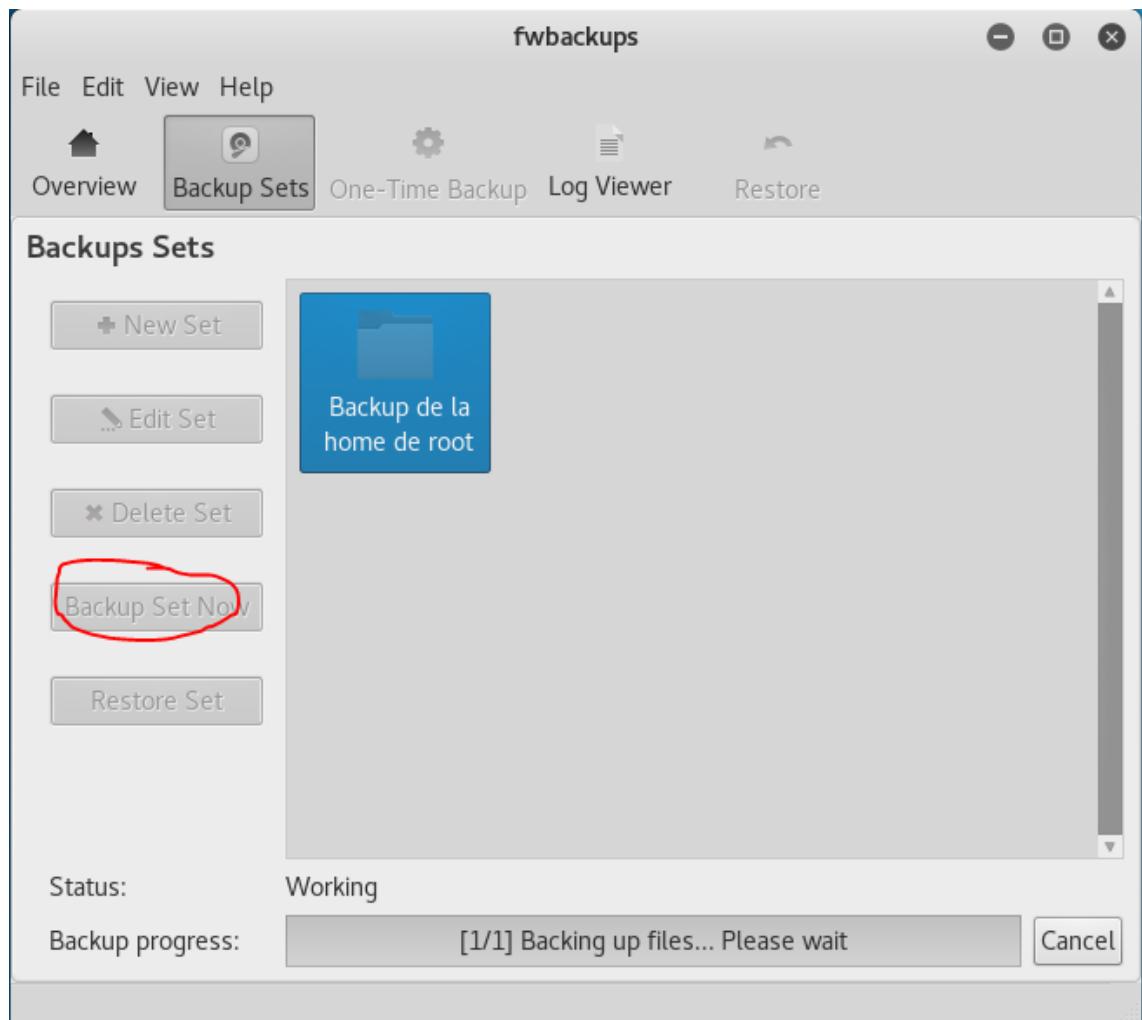


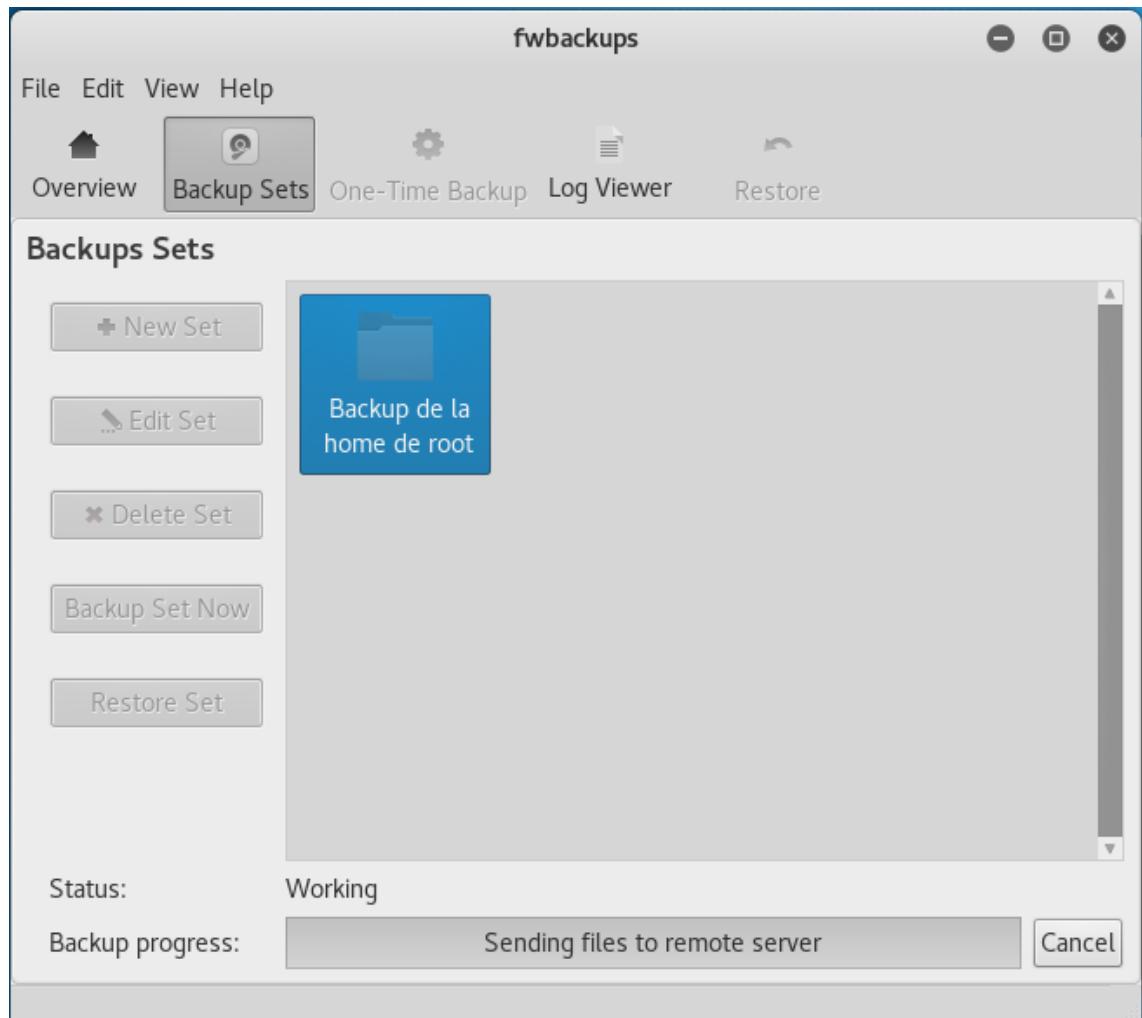
También tenemos la opción de hacer Backups incrementales, que en esta ocasión no vamos a utilizarlo.

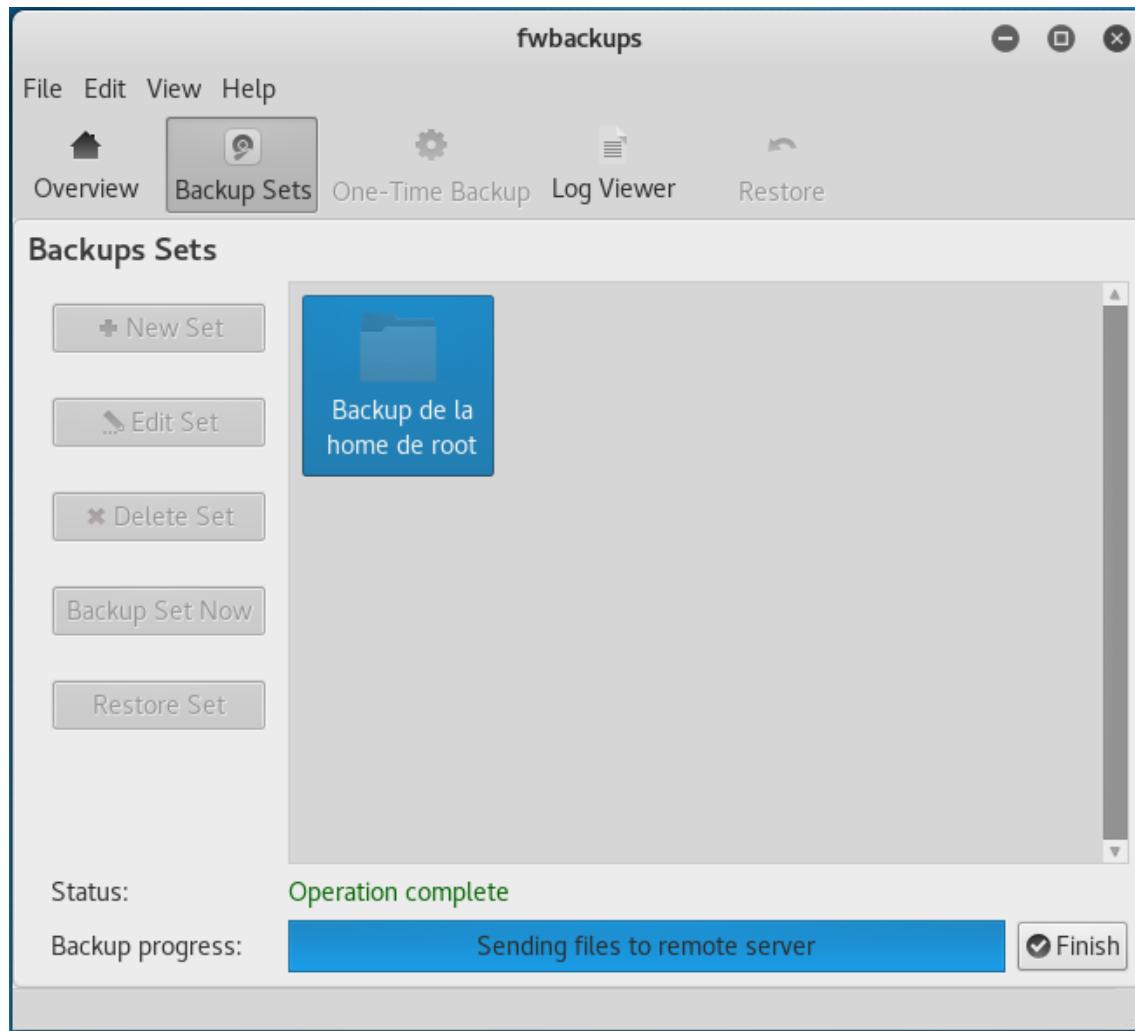
Una vez configurado el set lo veremos así



Para agilizar el proceso, vamos a hacer el backup ahora, pinchando en backup set now







Ahora, vamos a conectarnos por ssh para ver si realmente ha hecho la copia de seguridad.

```
root@athos:~# ssh athos@192.168.1.10 Backups Sets root@athos:~# 
athos@192.168.1.10's password:
Last login: Tue Nov 14 18:28:35 2017 from 192.168.1.5
FreeBSD 11.0-STABLE (FreeNAS.amd64) #0 r321665+25fe8ba8d06(freenas/11.0-stable):
Mon Sep 25 06:24:11 UTC 2017

        FreeNAS (c) 2009-2017, The FreeNAS Development Team
        All rights reserved.
        FreeNAS is released under the modified BSD license.

        For more information, documentation, help or support, go here:
        http://freenas.org

Welcome to FreeNAS
athos@freenas:~ % ls
Backup-Backup de la home de root-2017-11-14 18-36.tar.gz
Capítulo 1 2017-11-07 20:05:43 (Full)
Capítulo 1 2017-11-07 20:11:22 (Full)
Capítulo 1 2017-11-07 20:12:45 (Incremental)
Capítulo 1 2017-11-07 20:14:11 (Incremental)
Capítulo 1 2017-11-13 19:20:21 (Full)
Capítulo 1 2017-11-13 19:21:17 (Incremental)
cyborg-hawk-linux-v-1.1.iso
dfa
fads
athos@freenas:~ %
```

Athos Orío Choperena.

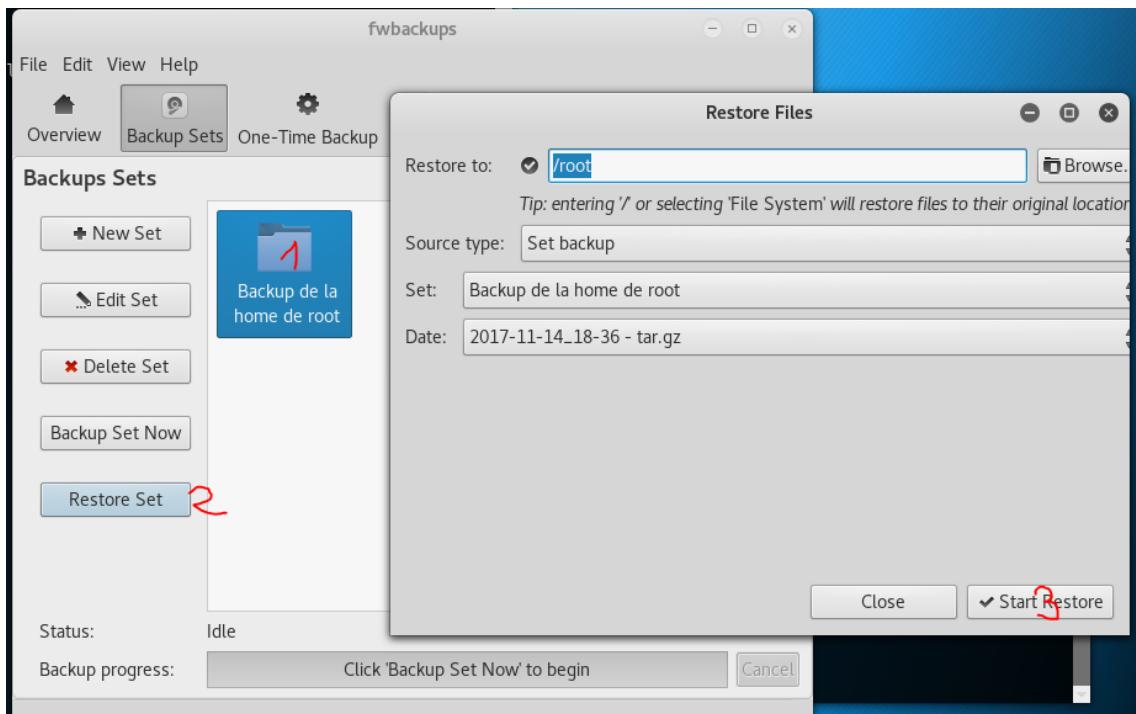
Como podemos ver, la copia de seguridad se ha realizado, ahora vamos a borrar algo de la home de root y lo recuperaremos

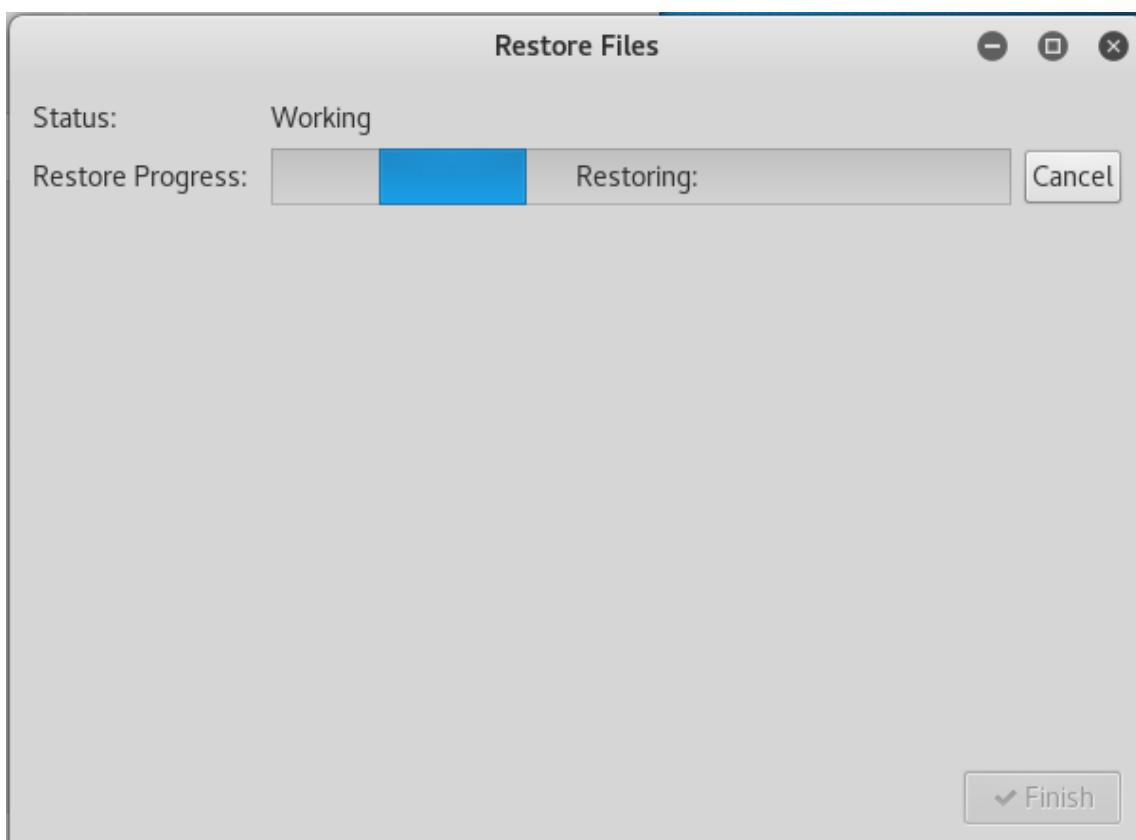
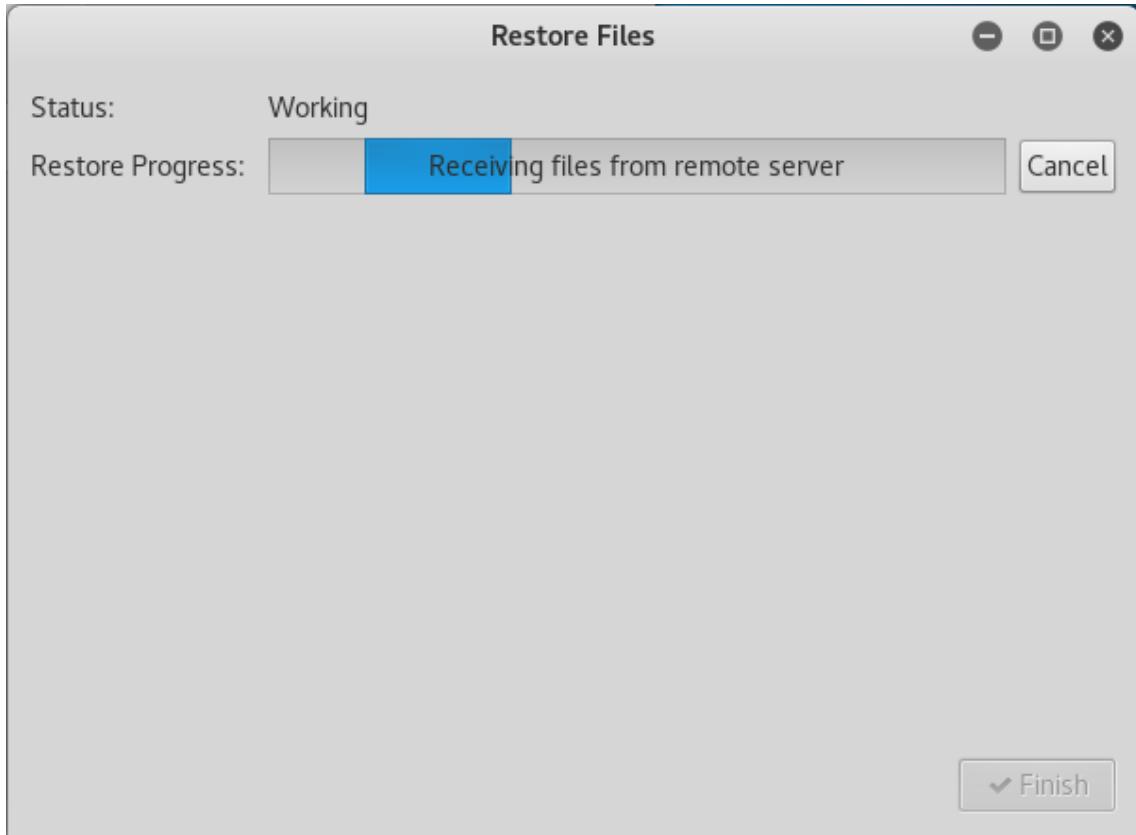
The screenshot shows a terminal window titled 'root@athos: ~'. The user has run several commands:

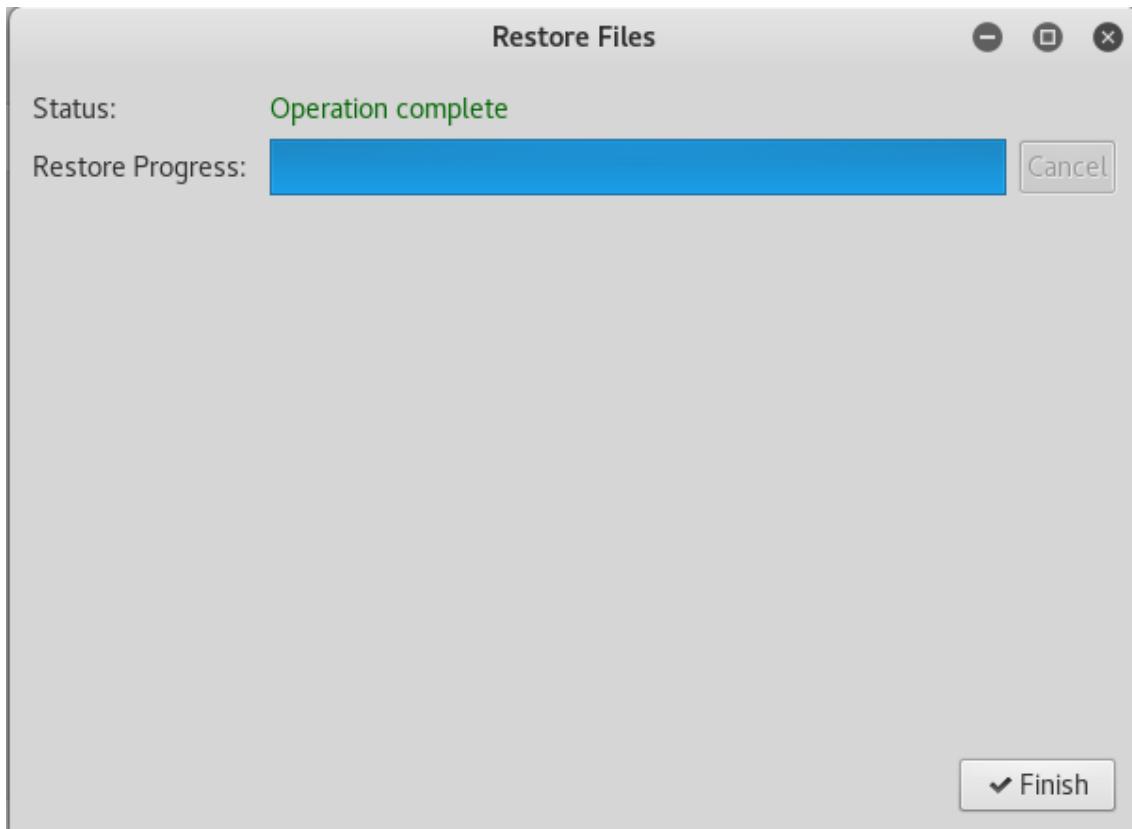
```
root@athos:~# ls
athos  Documents  Music  Public  Videos  fwbackups
core   Downloads  Pictures START  wordlist.txt
Desktop fwbackups-1.43.6  platawordlist.txt Templates
root@athos:~# rm -rf *
root@athos:~#
root@athos:~#
```

After running 'rm -rf *', the terminal shows an empty directory. A file browser window titled 'fwbackups' is open, showing a backup set named 'Backup de la home de root'. The 'Restore Files' dialog is open, with the restore path set to '/root'. The 'Source type' is 'Set backup', and the 'Set' is 'Backup de la home de root'. The 'Date' is '2017-11-14_18-36 - tar.gz'. The 'Start Restore' button is highlighted with a red circle.

Ahora, en fwbackups, vamos a darle a restaurar. Pinchamos en los pasos como se ve en la imagen





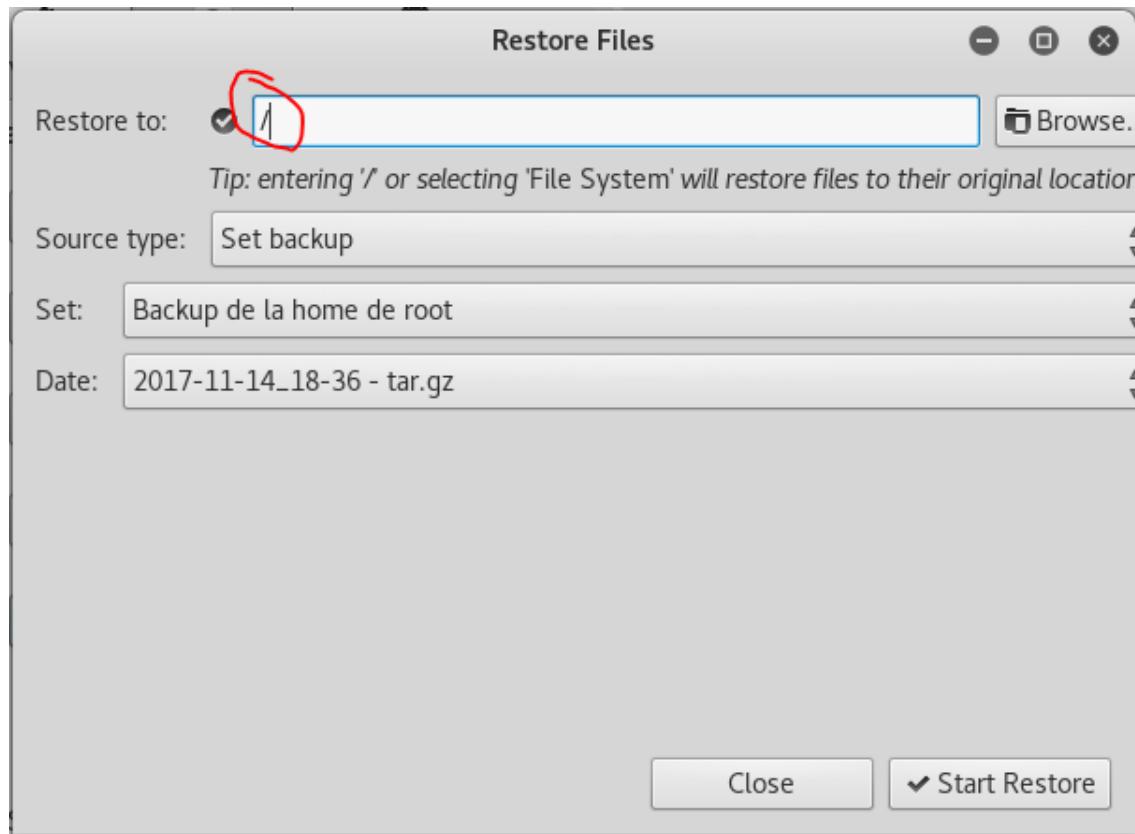


Y ahora comprobamos el home de root

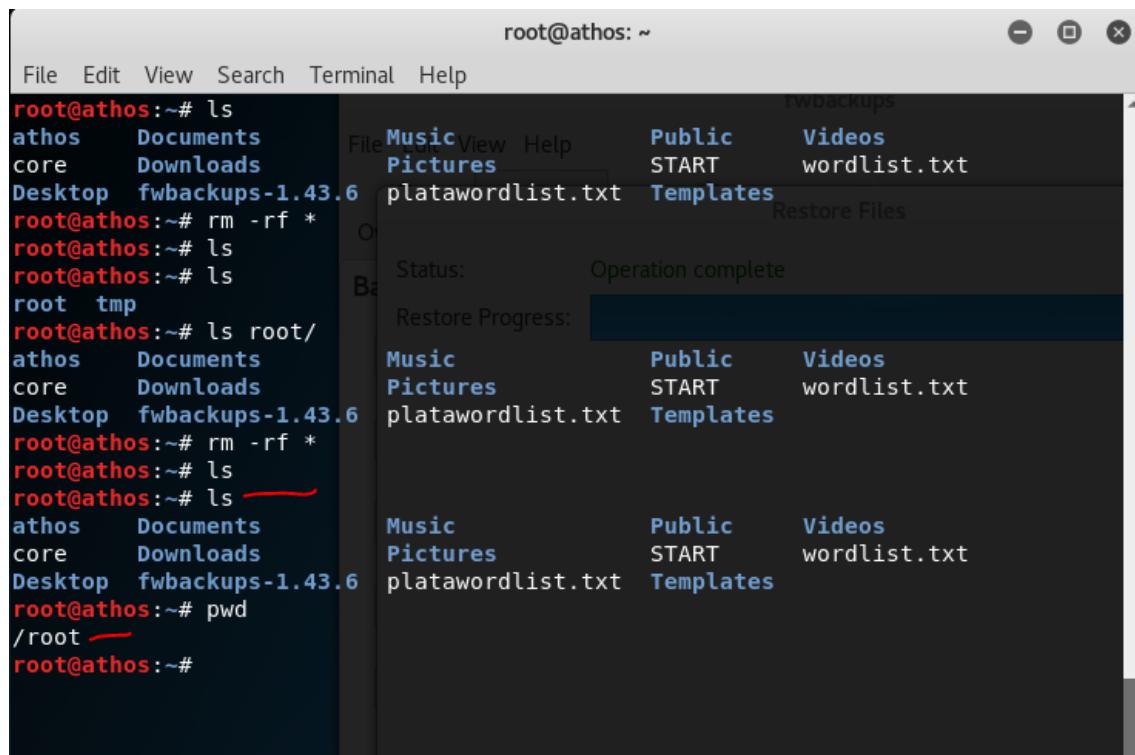
```
root@athos:~# ls
athos  Documents      Music          Public    Videos
core   Downloads      Pictures       START     wordlist.txt
Desktop fwbackups-1.43.6  platawordlist.txt Templates
root@athos:~# rm -rf *
root@athos:~# ls
root@athos:~# ls
root@athos:~# ls root/
athos  Documents      Music          Public    Videos
core   Downloads      Pictures       START     wordlist.txt
Desktop fwbackups-1.43.6  platawordlist.txt Templates
root@athos:~#
```

The terminal window shows a user with root privileges. It lists files in the current directory (~) and then uses the 'rm -rf *' command to delete them. After clearing the directory, it creates a new directory named 'root' inside the current directory (~). Finally, it lists the contents of the 'root' directory, which contains the same files as the parent directory (~).

Como vemos, nos ha creado una carpeta root dentro de root, que no es lo que queríamos, vamos a configurarlo de la manera correcta para que nos lo deje como estaba.



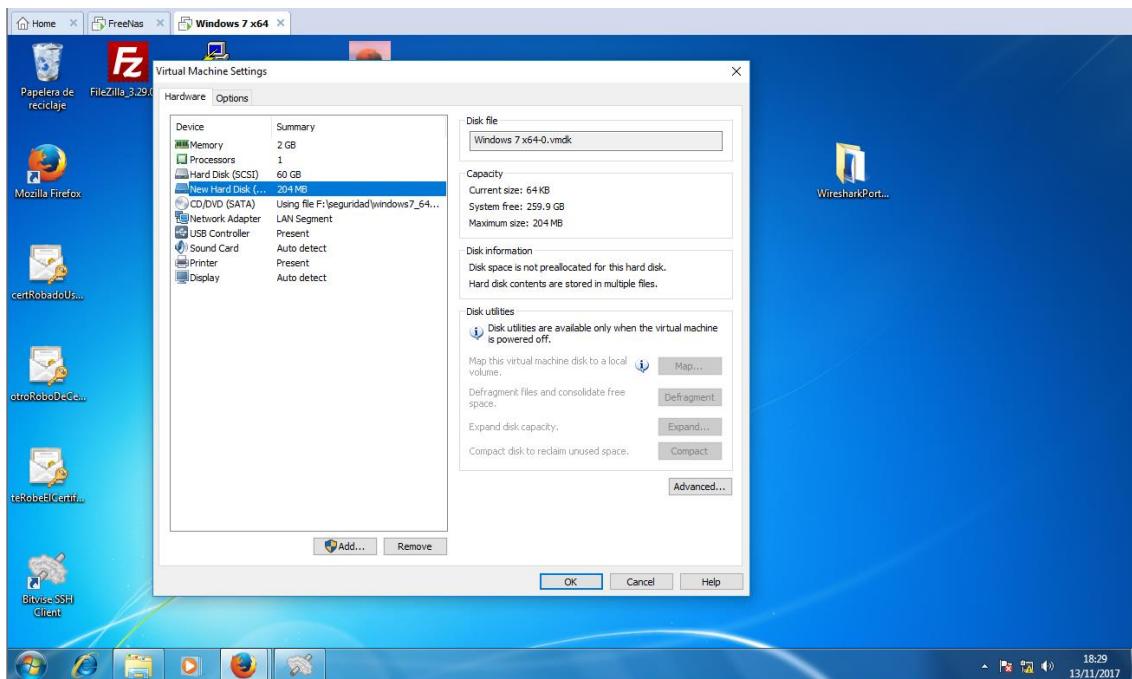
Y como podemos ver en la siguiente imagen, lo ha hecho correctamente



Practica 2.3: Recuperación de datos.

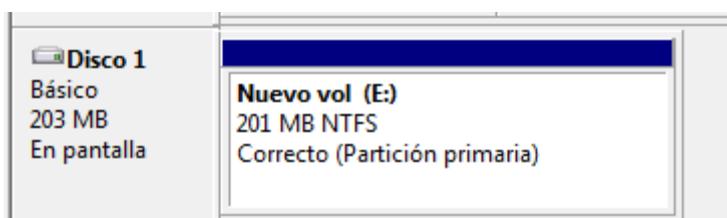
Es algo habitual, necesitar programas de recuperación de datos perdidos, ya por que los hemos borrado por error, o por algún virus, o que cuando vamos a abrir la unidad, resulta que no podemos acceder por cualquier motivo (por ejemplo que se ha quedado corrupta la tabla de particiones)

Para simular esto, vamos a añadir un disco duro en la máquina virtual, y vamos a añadir archivos, posteriormente vamos a romper la partición, vamos a borrar los archivos intencionadamente y posteriormente vamos a intentar recuperarlos.



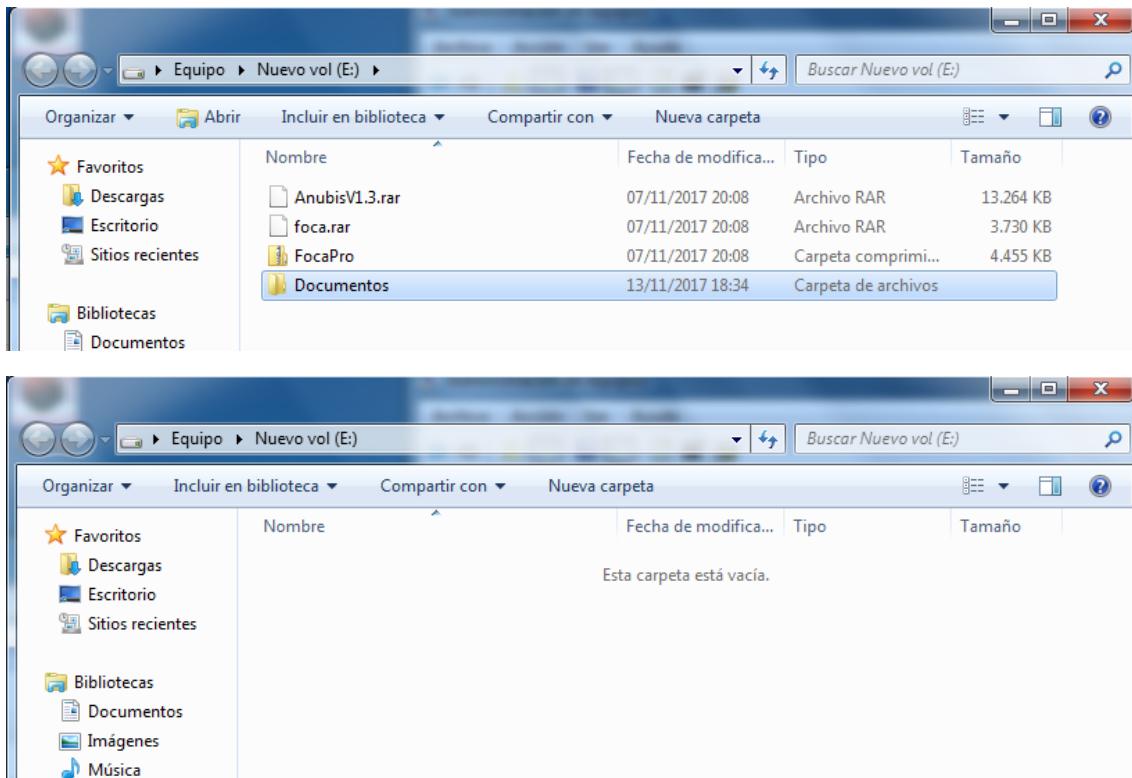
Hemos añadido un disco duro pequeño para minimizar el tiempo en el proceso de la recuperación de datos.

Primero vamos a probar con el sistema de ficheros ntfs



Copiamos datos dentro del volumen y posteriormente los borramos

Athos Orío Choperena.

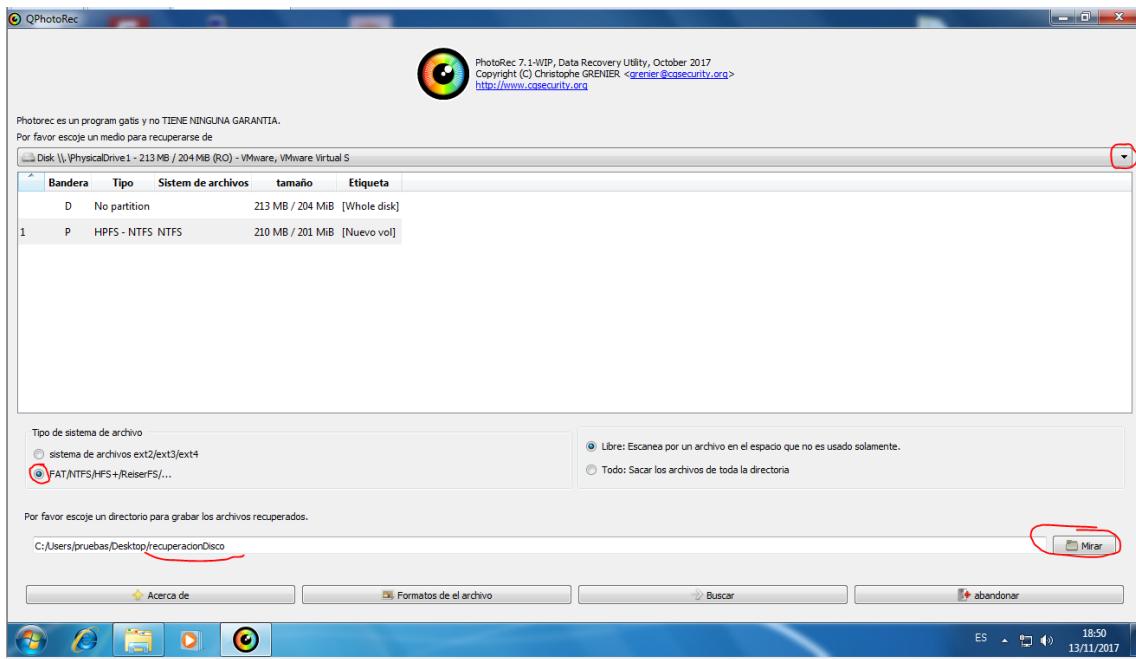


El primer programa que vamos a utilizar es testdisk. Nos lo descargamos desde la página oficial

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

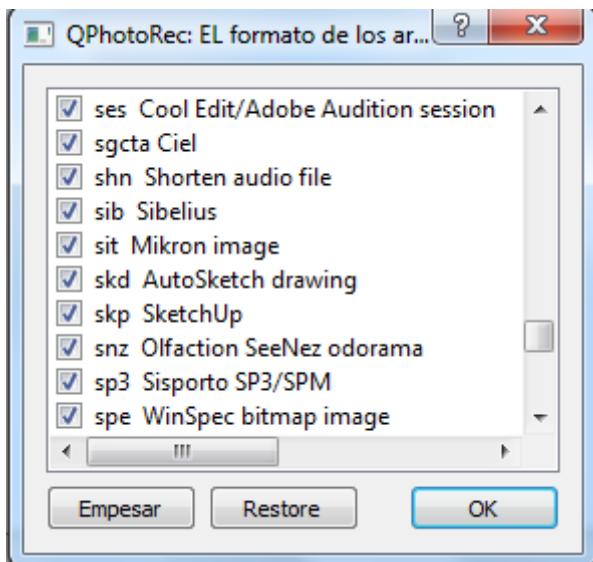
Hay varias herramientas, primero vamos a usar qphotorec a ver que nos recupera. Hay que tener en cuenta que nunca deberemos guardar los datos recuperados en la misma unidad que estamos recuperando, ya que puede sobrescribir los datos que estamos tratando de recuperar

Athos Orío Choperena.

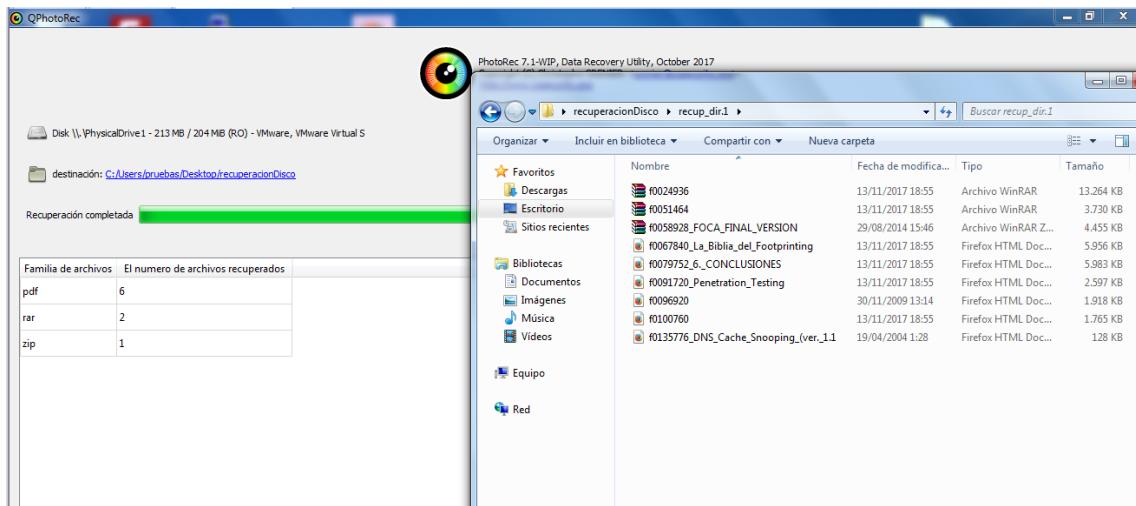


Seleccionamos la unidad, el tipo de sistema de ficheros y el destino de los datos recuperados, una vez hecho esto le damos a buscar.

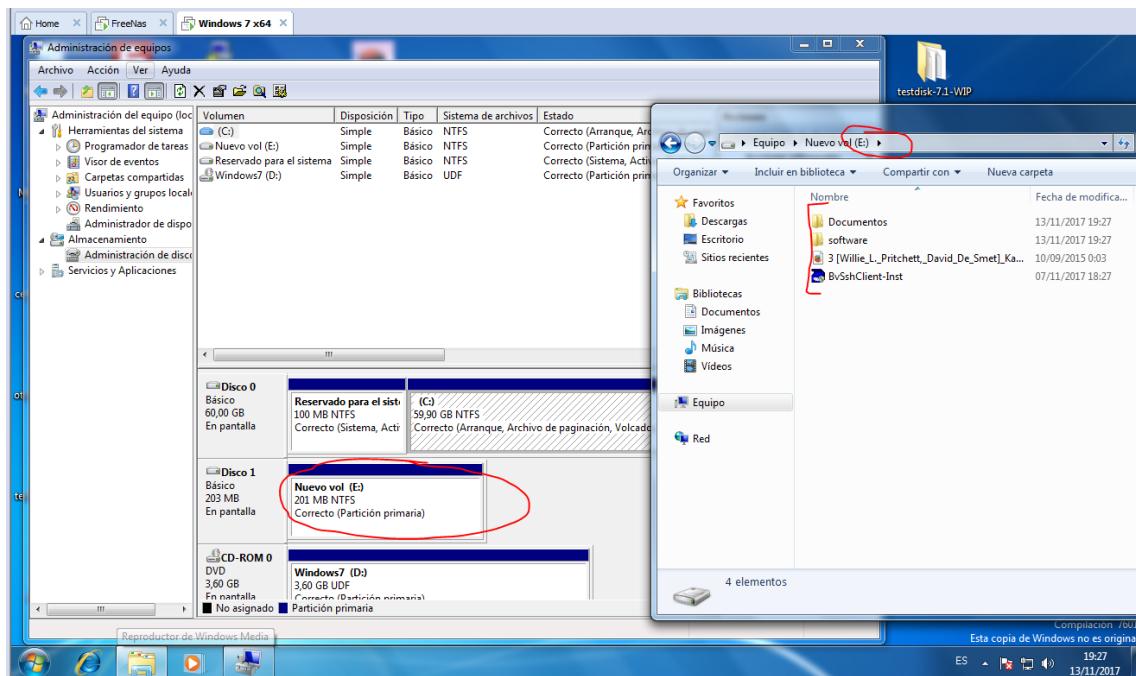
Podríamos pinchar previamente en formatos del archivo para elegir el tipo de archivos que queremos que busque



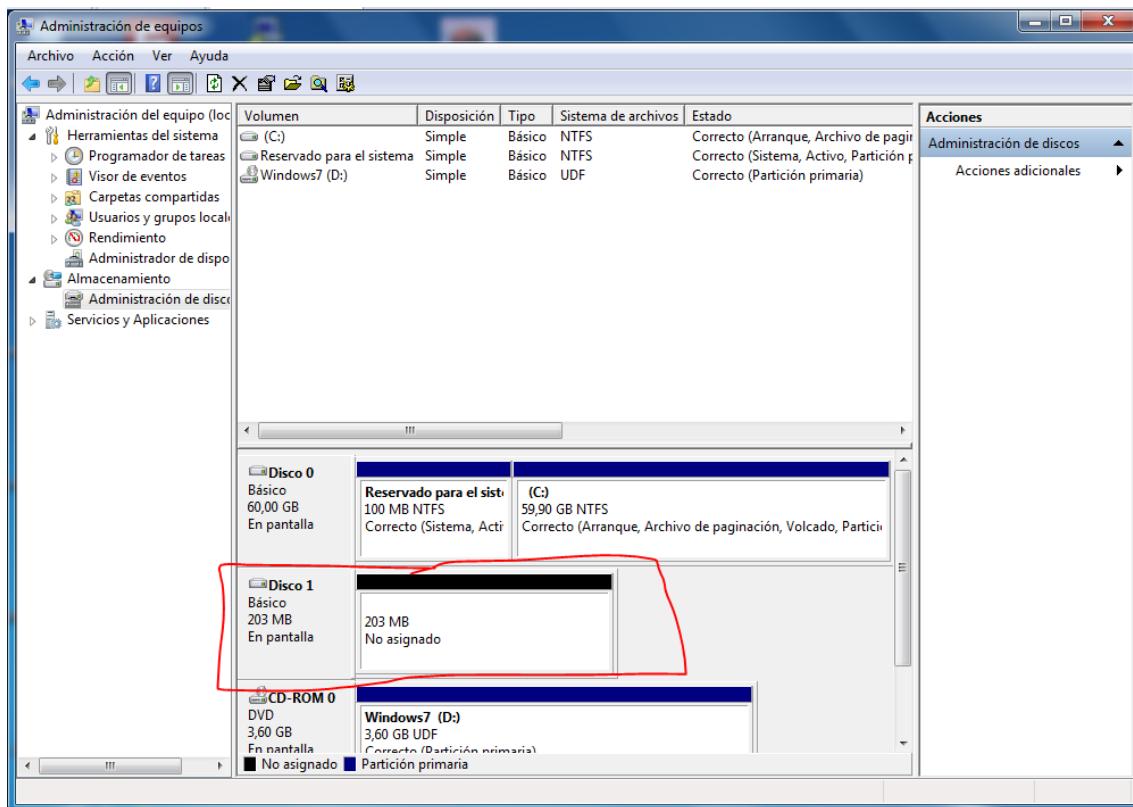
Como podemos ver, nos ha recuperado algunos ficheros



Otra cosa que puede hacer testdisk es recuperar una partición borrada, así que vamos a hacerlo.

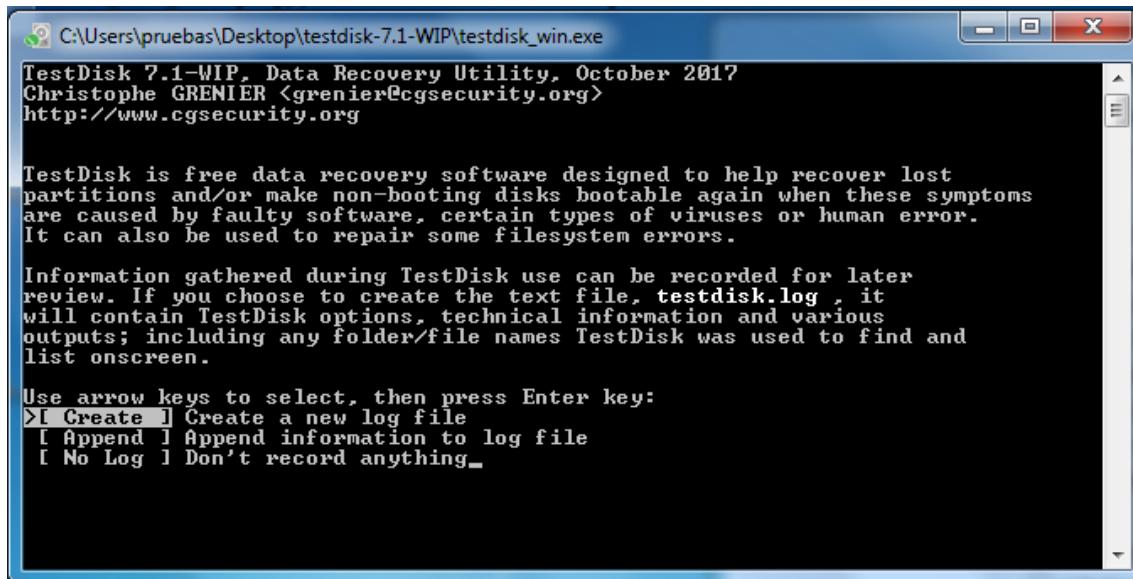


Y ahora borramos la partición.

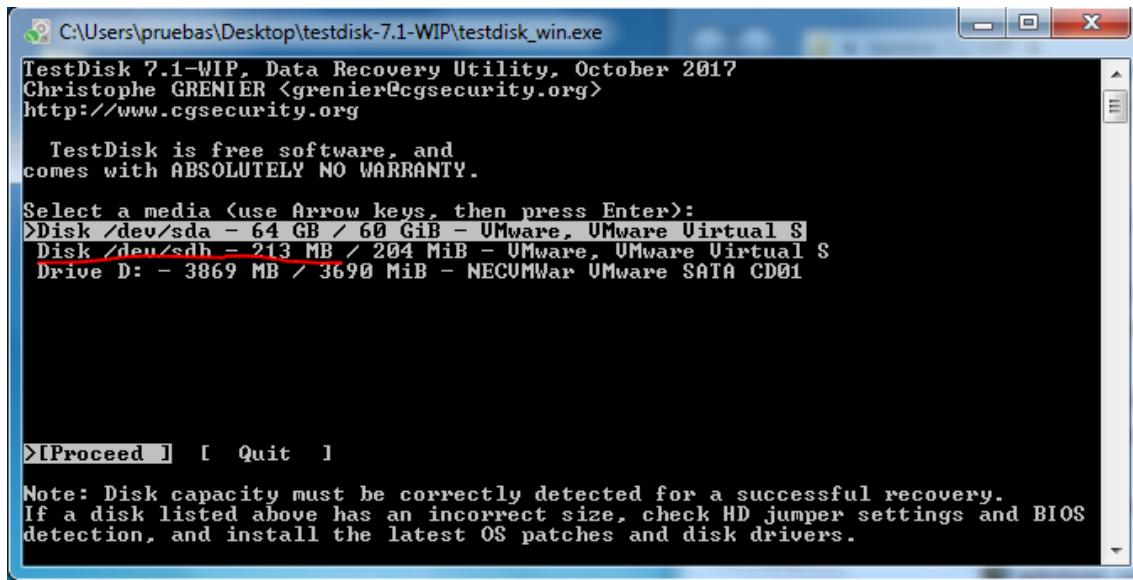


Ahora abrimos testdisk para intentar recuperarla.

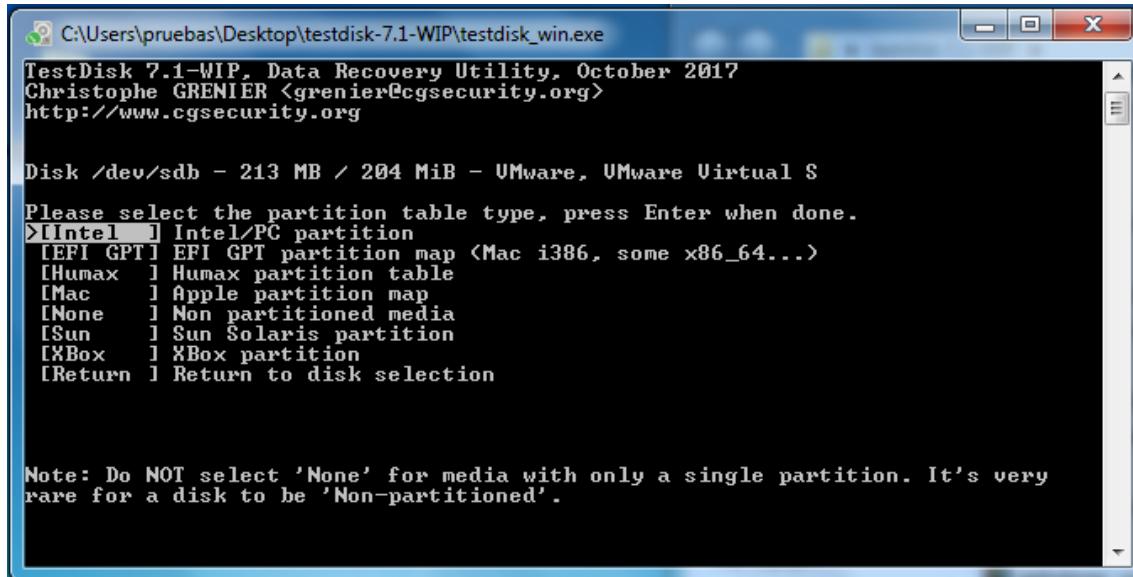
Lo primero que nos pregunta es si queremos que se cree un registro de las operaciones que se van a realizar. Podemos crear uno nuevo, añadir a uno existente o no crearlo, dejamos la opción por defecto y continuamos



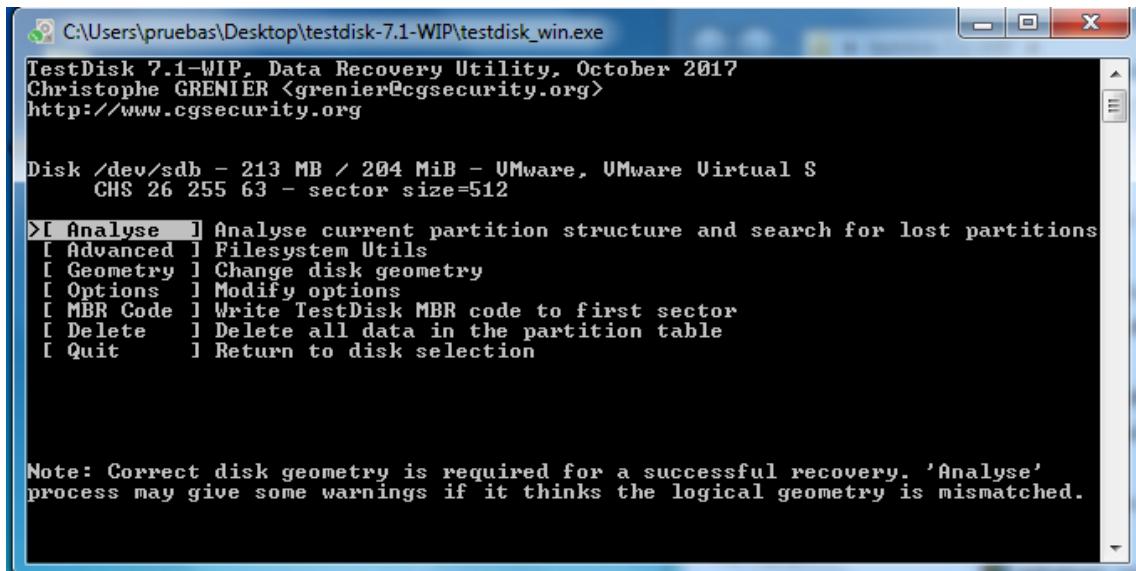
Ahora nos pregunta sobre qué disco queremos realizar la operación, utilizaremos el que creamos anteriormente de 200 megas



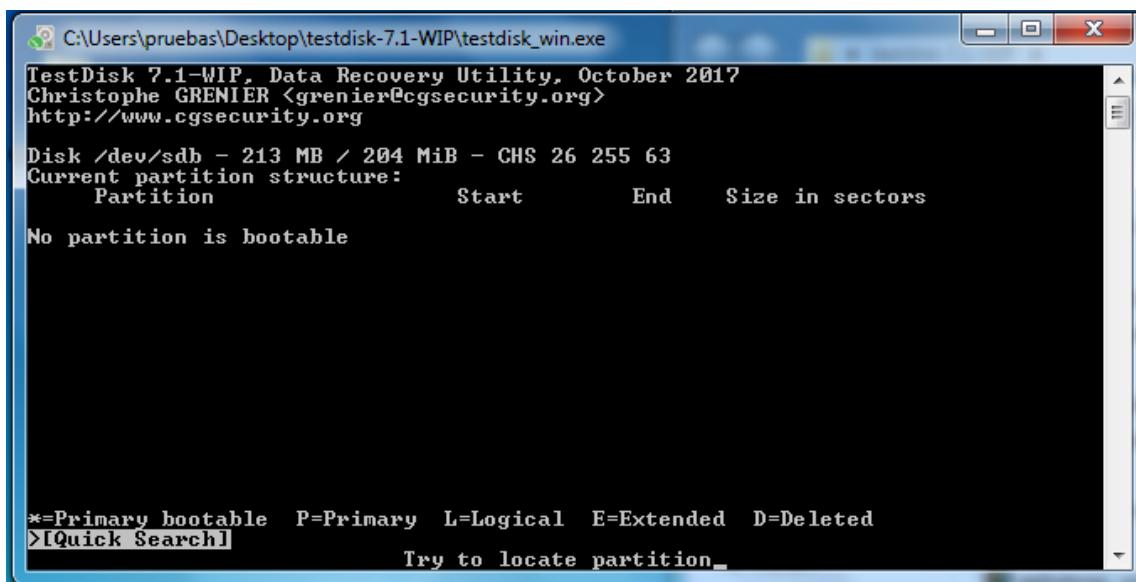
Ahora tenemos que decirle que tipo de sistema de ficheros tenía la unidad, en este caso sabemos que era ntfs así que seleccionamos Intel y le damos a siguiente



Nos pregunta que operación queremos hacer, así que seleccionamos analizar y continuamos

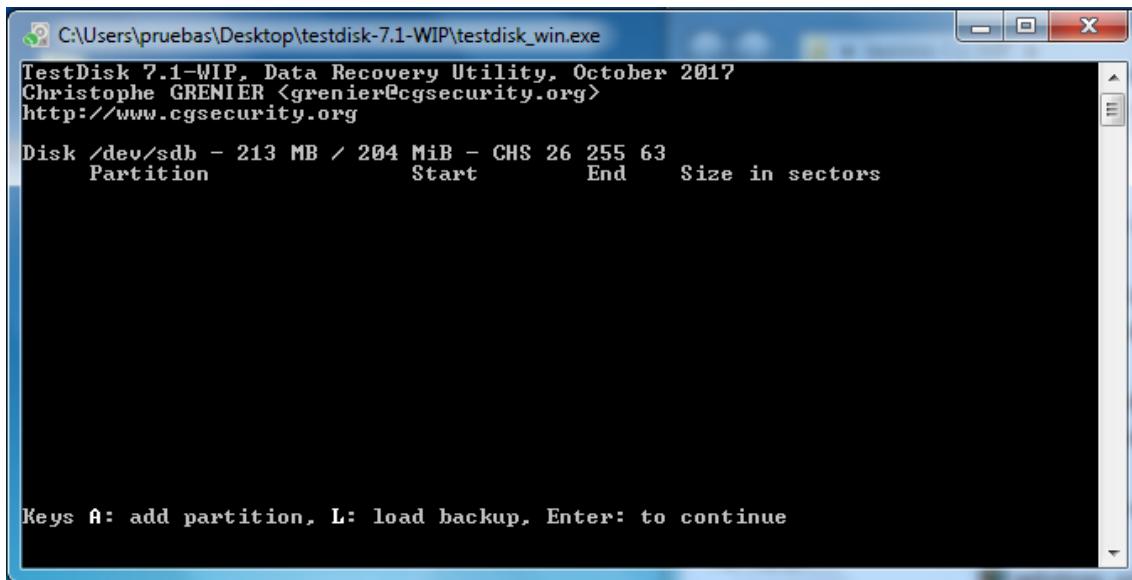


Nos avisa que actualmente no hay ninguna partición, así que le damos a buscar (quick search)

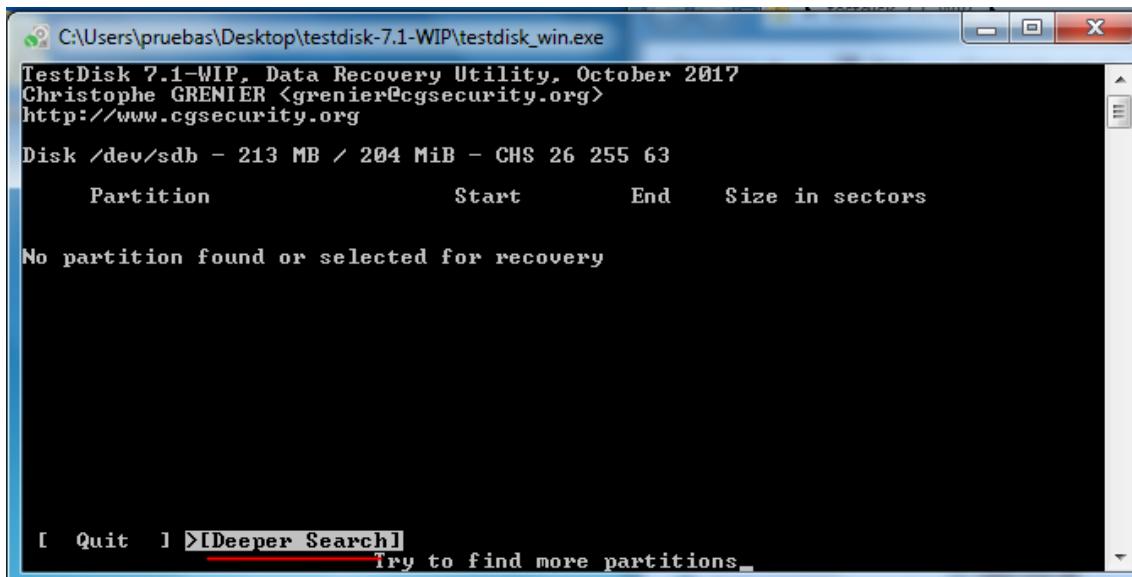


No nos ha encontrado nada, así que vamos a hacer un escaneo profundo

Athos Orío Choperena.

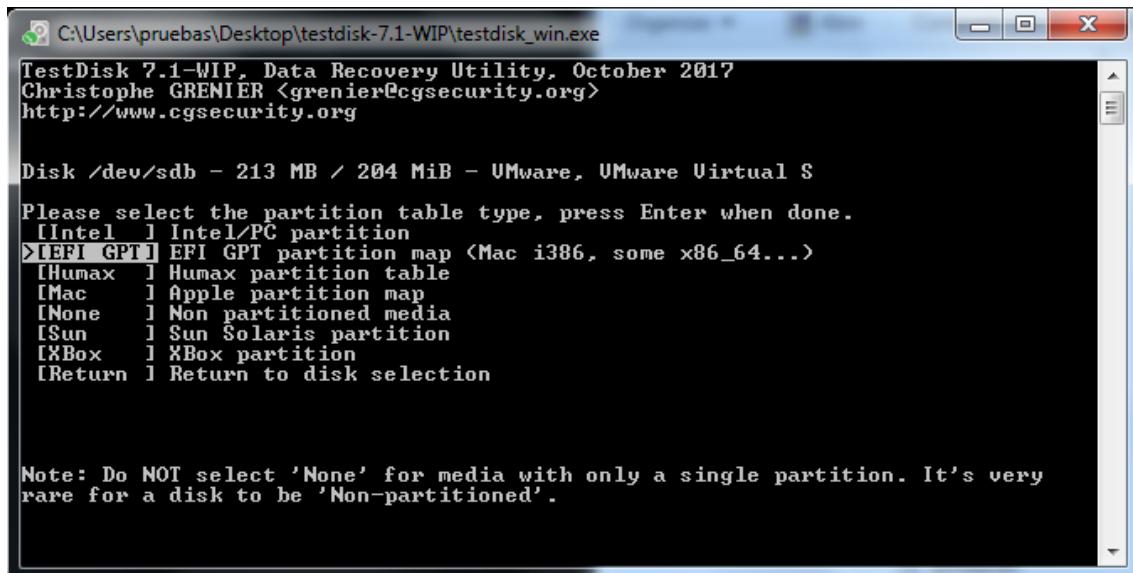


Pulsamos enter, y en la siguiente pantalla seleccionamos escaneo profundo (Deep search)

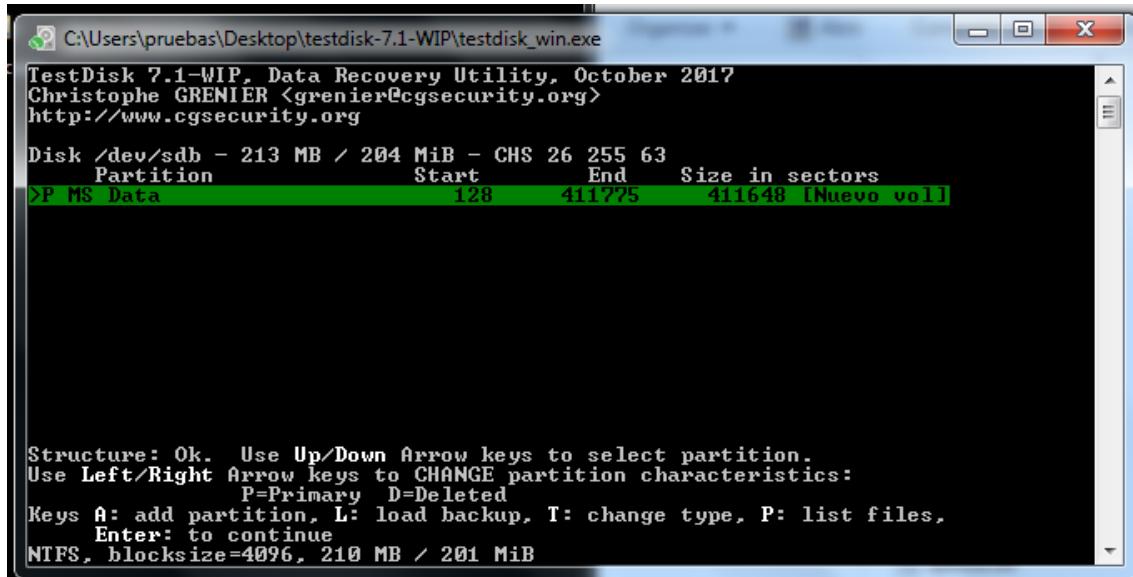


No ha encontrado nada, así que volvemos a pasos anteriores y vamos a seleccionar gpt (supongo que esto es porque es un disco virtual de vmware)

Athos Orío Choperena.

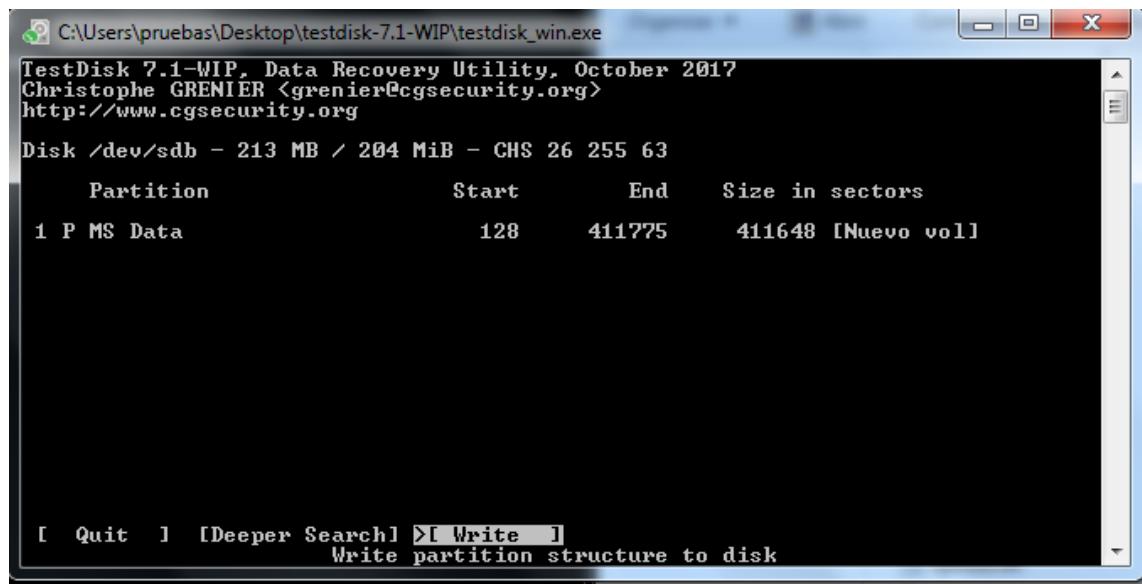


Analizamos como hemos hecho anteriormente y en esta ocasión nos encuentra nuestra partición perdida.



Pulsamos enter para continuar, y en la siguiente ventana, vamos a seleccionar write para escribir la tabla de particiones en disco. Con esto espero recuperar la tabla de particiones y poder acceder a los datos que había dentro.

Athos Orío Choperena.



C:\Users\pruebas\Desktop\testdisk-7.1-WIP\testdisk_win.exe

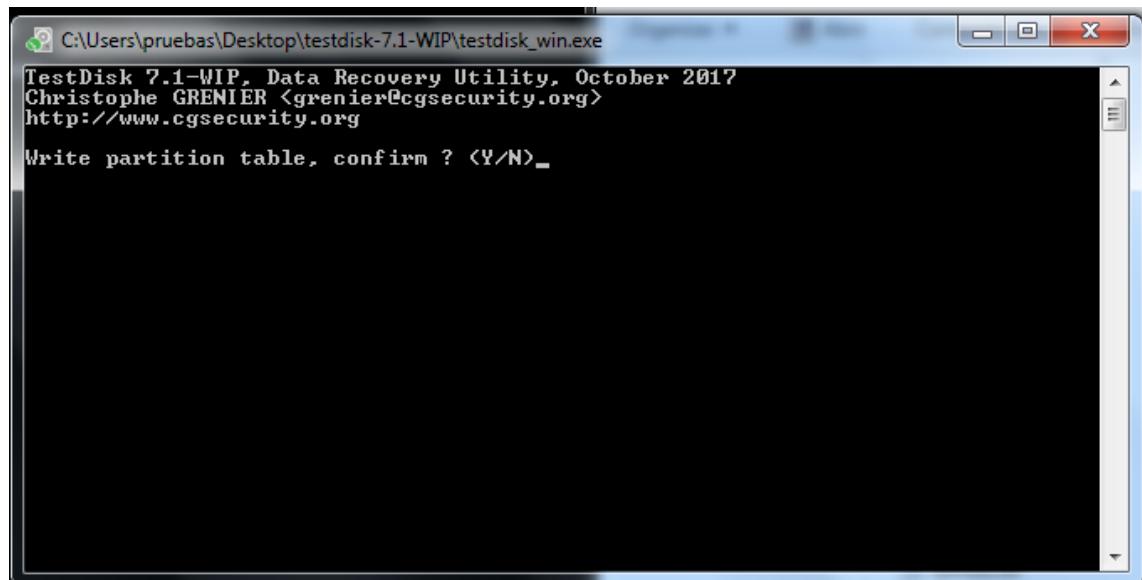
TestDisk 7.1-WIP, Data Recovery Utility, October 2017
Christophe GRENIER <grenier@cgsecurity.org>
<http://www.cgsecurity.org>

Disk /dev/sdb - 213 MB / 204 MiB - CHS 26 255 63

Partition	Start	End	Size in sectors
1 P MS Data	128	411775	411648 [Nuevo vol]

[Quit] [Deeper Search] >[Write]
Write partition structure to disk

Confirmamos que queremos escribir los cambios



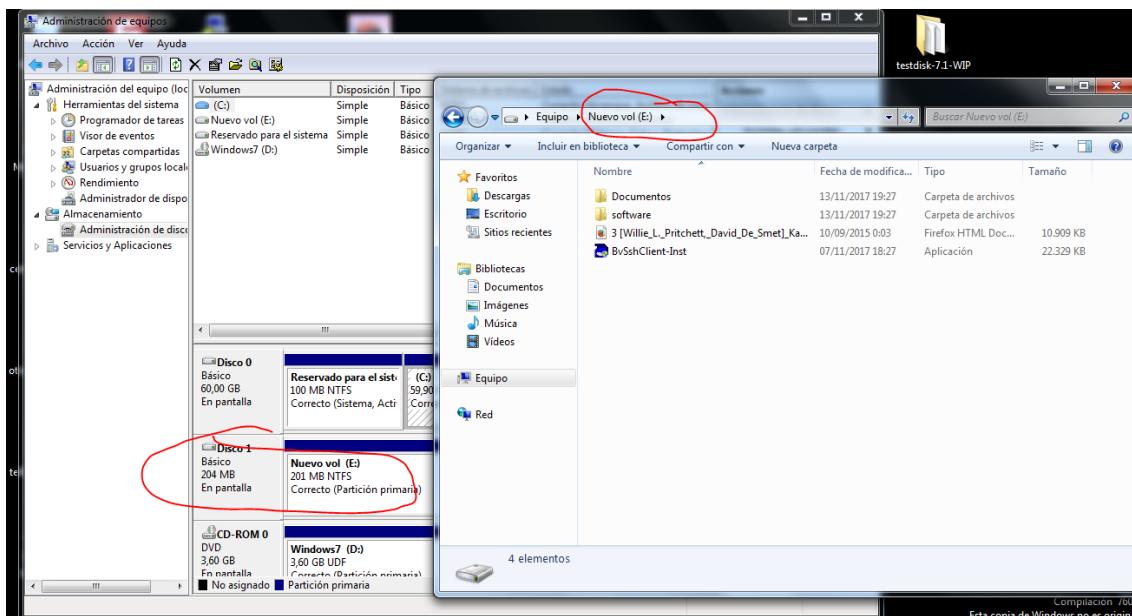
C:\Users\pruebas\Desktop\testdisk-7.1-WIP\testdisk_win.exe

TestDisk 7.1-WIP, Data Recovery Utility, October 2017
Christophe GRENIER <grenier@cgsecurity.org>
<http://www.cgsecurity.org>

Write partition table, confirm ? <Y/N>_

Nos avisa de que tenemos que reiniciar para que los cambios hagan efecto, así que reiniciamos.

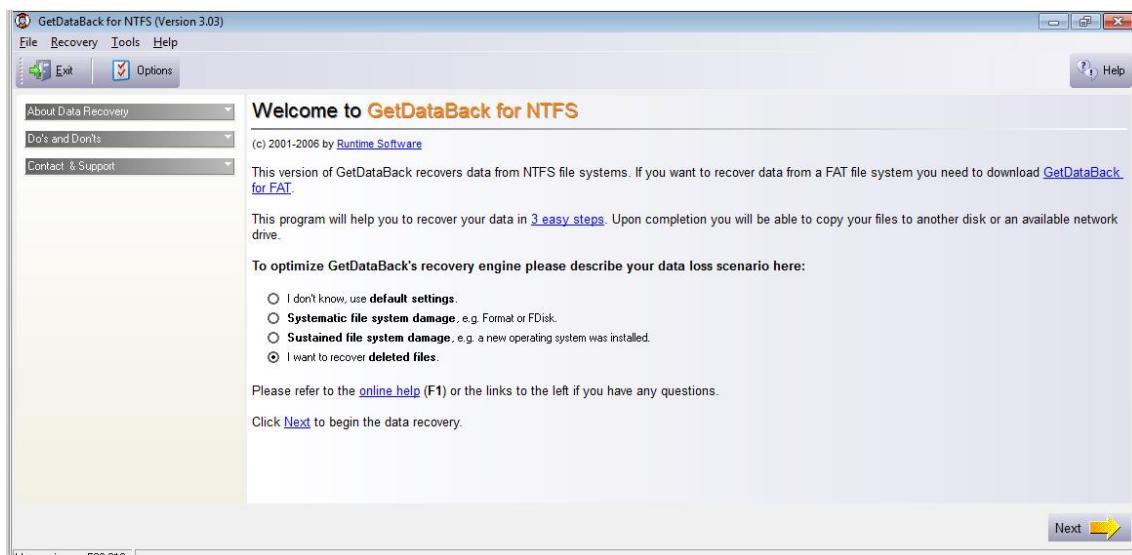
Y como podemos ver, hemos recuperado la partición perdida.



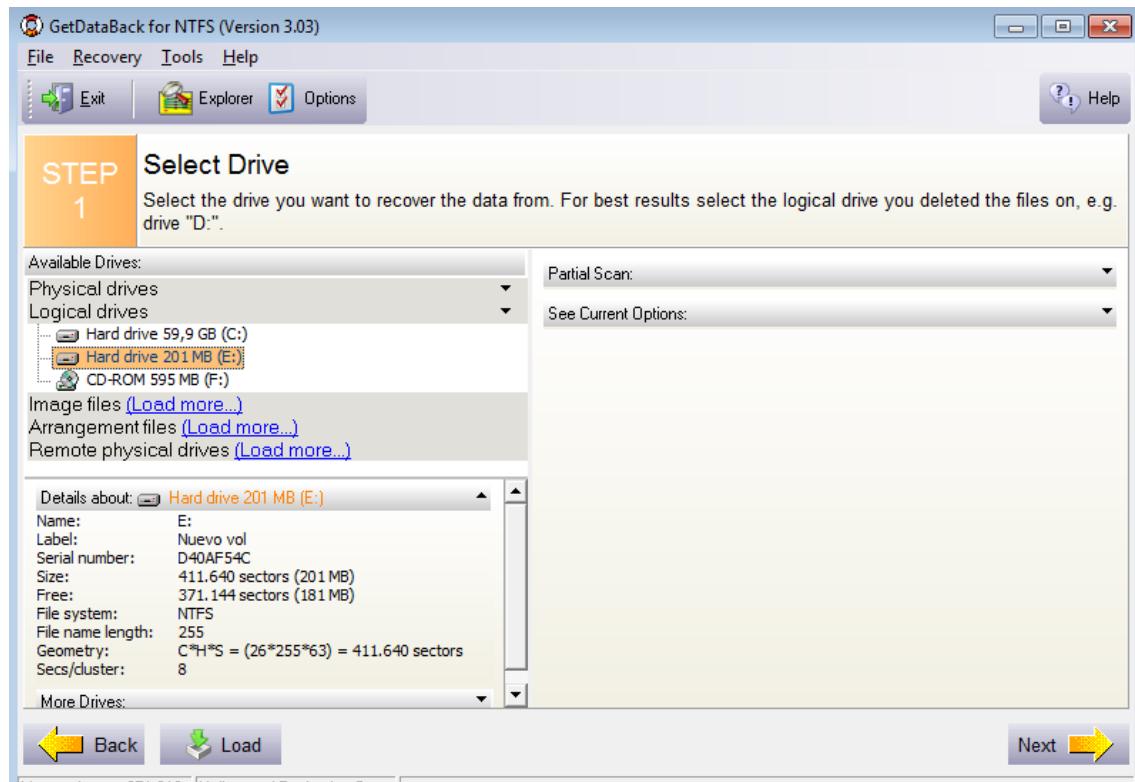
Hay que destacar que este programa (testdisk) está disponible para Windows o para Linux.

Existen infinidad de programas para este fin, no podemos probar todos, pero en esta práctica vamos a probar también el getdataback, que tiene dos versiones, una ntfs y otra fat. Esta herramienta viene incluida en el cd de hirens, así que lo vamos a descargar y lo probaremos.

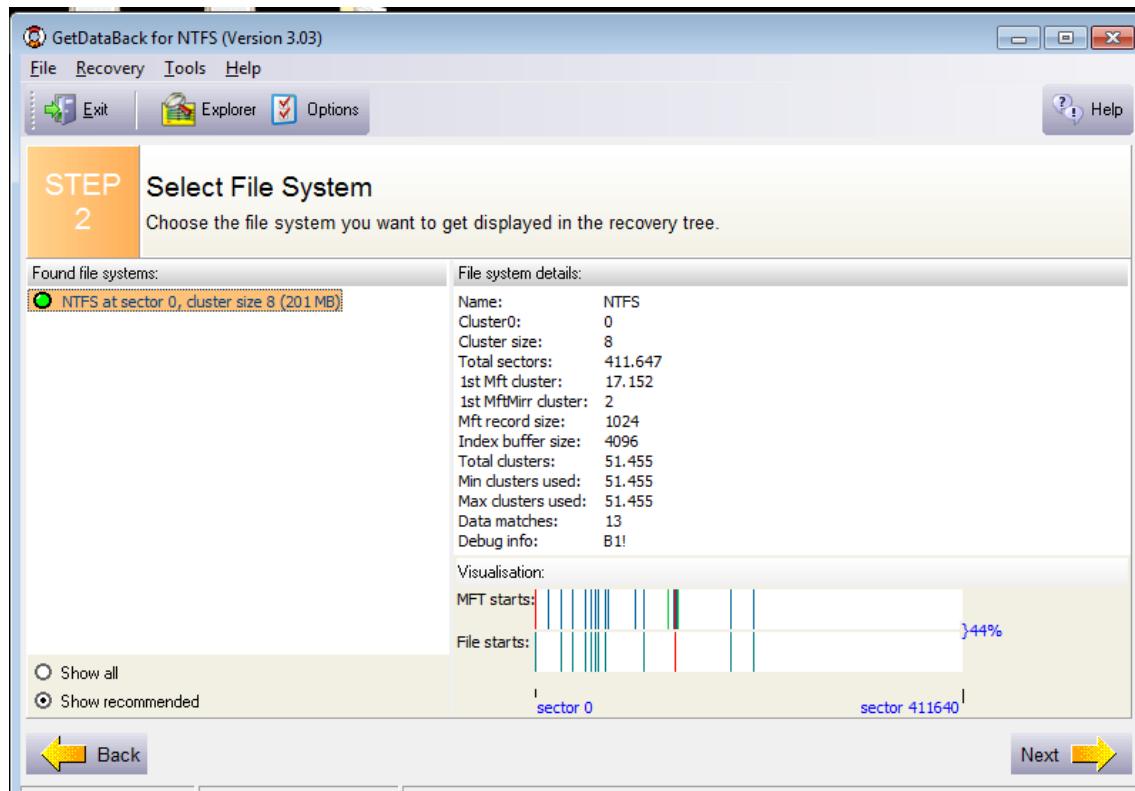
Seleccionamos la acción que queremos realizar, en este caso recuperar archivos borrados y pinchamos en siguiente.



En el menú de la izquierda, seleccionamos la unidad y hacemos click en siguiente

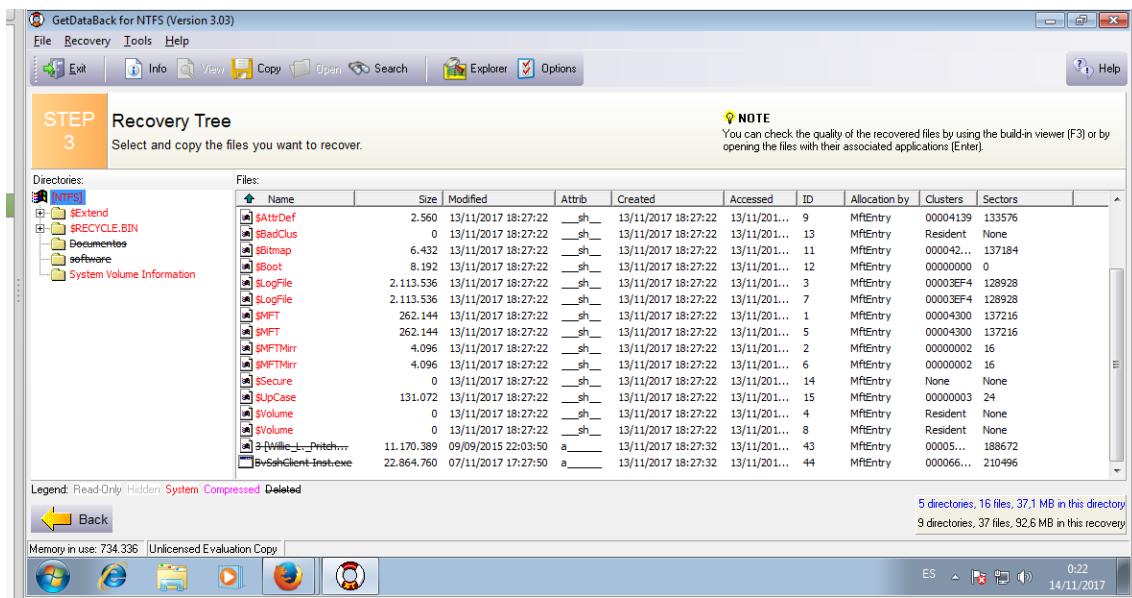


Realizara un escaneo y nos sacara información

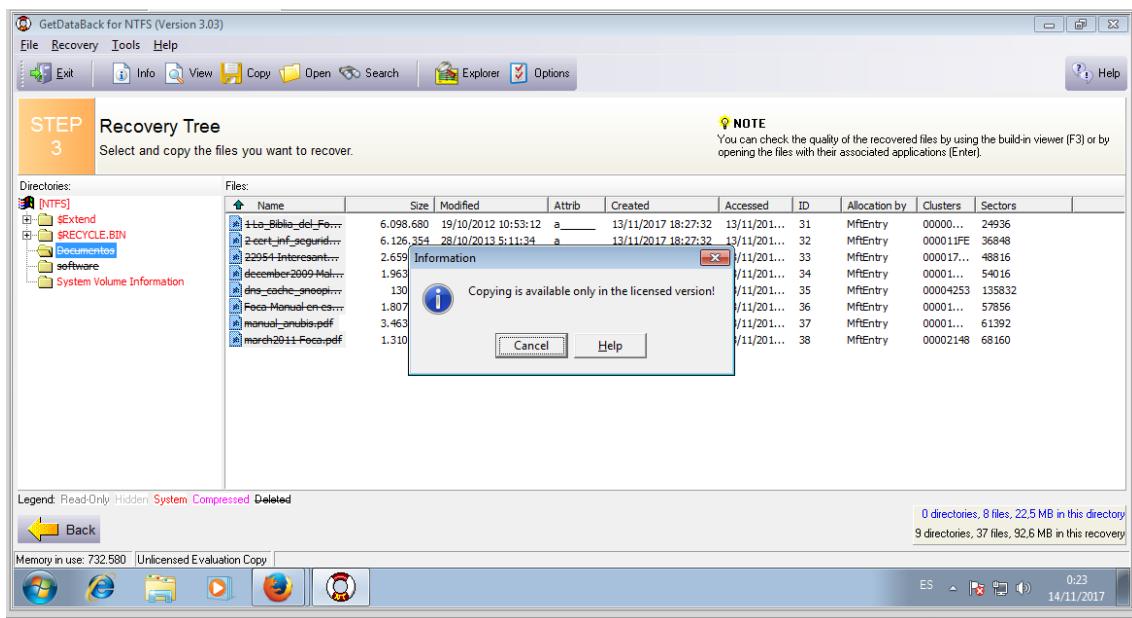


Pincharemos en siguiente y podremos ver los archivos y directorios eliminados, son los que están tachados, seleccionaremos los que queramos y pincharemos en copy

Athos Orío Choperena.



Como es un software de pago, nos avisa de que solo podemos recuperar los archivos si pagamos la licencia. Pero ese sería el proceso para recuperar los archivos



Al igual que estos dos programas que hemos visto, existen muchos más, gratuitos, de pago. Antes de dar los datos por perdidos, habría que probar unos cuantos programas por si acaso.