Seguridad y alta disponibilidad

En este libro se abarcara la asignatura de seguridad y alta disponibilidad del grado superior de informática.

Escrito por: Nicolás Madrid Gallego

Nicolás Madrid Gallego
IES GREGORIO PRIETO
Adopción de pautas de seguridad

ÍNDICE

UD1: "Adopción de pautas de seguridad informática".

Confidencialidad

- Windows EFS

- PGP

Integridad

- Windows SFC

- GNU/LINUX Rootkit hunter

DIsponibilidad

- Utilizar NMAP, ZNMAP

- MBSA

- Nessus

- Trabajo análisis vulnerabilidades con NMAP, Nessus y MBSA

Amenazas:

b) Busca en Internet al menos una noticia relacionada con amenazas físicas a sistemas informáticos respecto a:

c) Busca en Internet al menos una noticia relacionada con amenazas lógicas respecto a:

d) Busca al menos dos antivirus on line y realiza su comprobación en el PC para compararlos.

e) Instala al menos dos antivirus en modo local y realiza su comprobación en el PC para compararlos.

f) Instala al menos dos aplicaciones antimalware en modo local y realiza su comprobación en el PC para compararlos.

6. Seguridad física y ambiental:
a) Se necesita realizar un estudio de la ubicación y protección física de los equipos y servidores del aula, desde el punto de vista de:

a)Acondicionamiento físico (Extintores, Sistema de aire acondicionado, Generadores eléctricos autónomos, racks)

b)Robo o sabotaje: Control de acceso físico y vigilancia mediante personal y circuitos cerrados de televisión (CCTV).

c)Condiciones atmosféricas y naturales adversas (Ubicación de sistemas, centros de respaldo en ubicación diferente al centro de producción, mecanismos de control y regulación de temperatura, humedad, etc.)

b) Busca un único SAI para todos los sistemas informáticos del aula.
c) Instalación de una cámara IP y transmisión de la imagen por una red LAN.
d) Instalación de un SAI o UPS en un rack y su posterior uso.

7. Seguridad lógica:

a) Realizar una copia de seguridad con herramientas del sistema:
En GNU/Linux: tar y crontab, rsync.
En Windows: Copias de seguridad y Restaurar Sistema.

b) Realizar una copia de seguridad con aplicaciones específicas:
En Windows: Cobian Backup
En GNU/Linux: fwbackup.

c) Utiliza una herramienta de recuperación de datos:
En Windows: Recuva.
En GNU/Linux: TextDisk, Foremost, Scalpel.

d) Realiza un informe sobre los diferentes programas que existen en el mercado informático que permite crear imagenes de respaldo de tu equipo.

e) Realiza un informe con los servicios de almacenamiento que ofrecen las empresas: DELL, ESABE, HP

f) Realizar en un entorno simulado un medio de almacenamiento RAID 1 con máquinas virtuales Windows Server.

g) Control de acceso lógico: Realiza la creación de una cuenta de usuario y su contraseña (política fuerte de contraseñas - modo comando y modo gráfico) que permite posteriormente acceder o no al sistema en sistemas Windows y sistemas GNU/Linux .

h) Verifica la auditoria de control de acceso “Visor de sucesos” de dicho usuario en Windows y Linux .

i) Descargar el programa de evaluación CryptoForge para Sistemas Windows en la dirección de Internet: http://www.cryptoforge.com.ar/ y encripte y desencripte varios ficheros de tu ordenador, utilizando diferentes sistemas de cifrado.

j) Encriptar y desencriptar ficheros de texto en sistemas GNU/Linux utilizando el comando tr que permite realizar sustituciones carácter a carácter, utilizando la ayuda del manual.

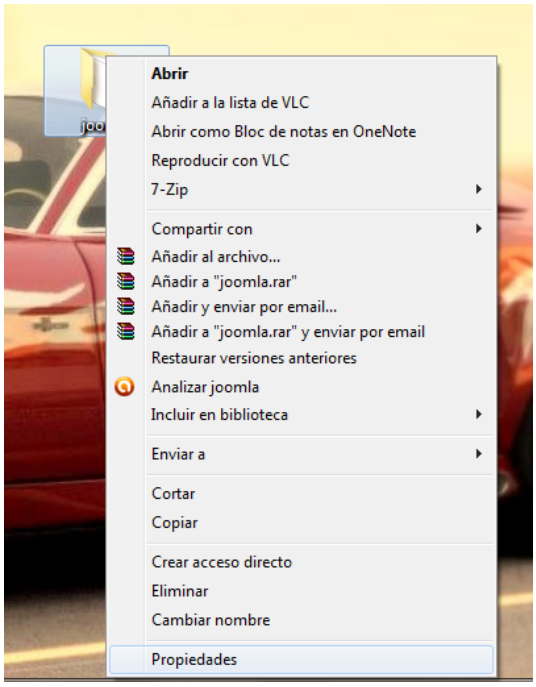
8. Análisis forense:

a) Utilizar una herramienta de Análisis forense para Windows y documente lo analizado con dicha herramienta.

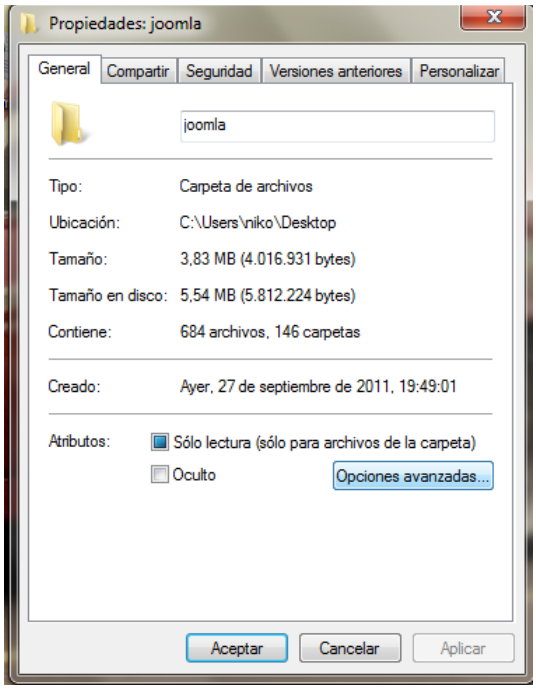
b) Utilizar una herramienta de Análisis forense para GNU/Linux y documente lo analizado con dicha herramienta.

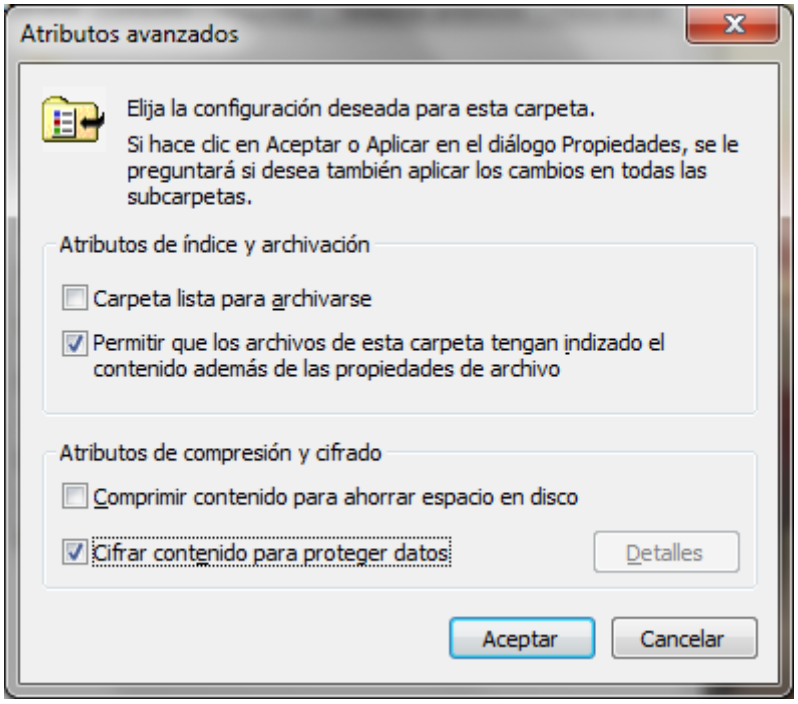
1.-Pasos de encriptación archivos mediante EFS

1.) Sobre la carpeta donde están los archivos pulsamos botón derecho/ propiedades,

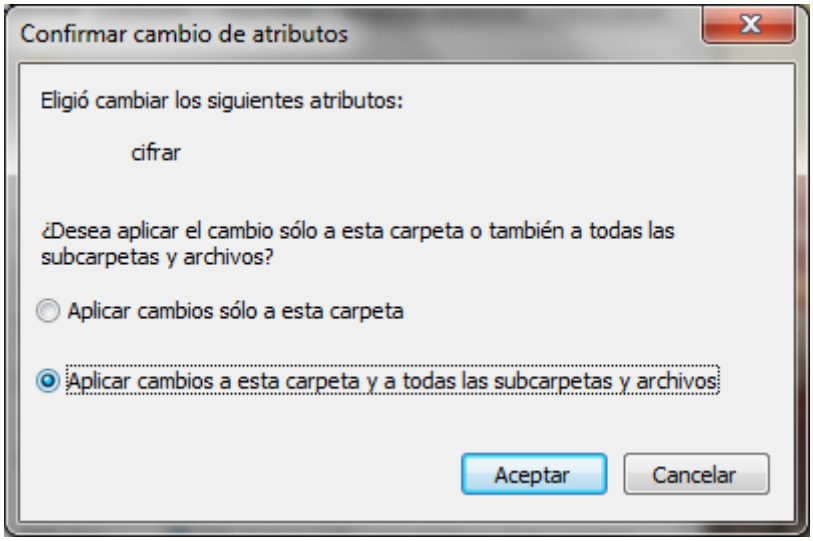


2.) Una vez alli en opciones generales de la carpeta pulsamos en opciones avanzadas, en la pantalla que nos aparece marcamos la opción “cifrar contenido para proteger datos”.

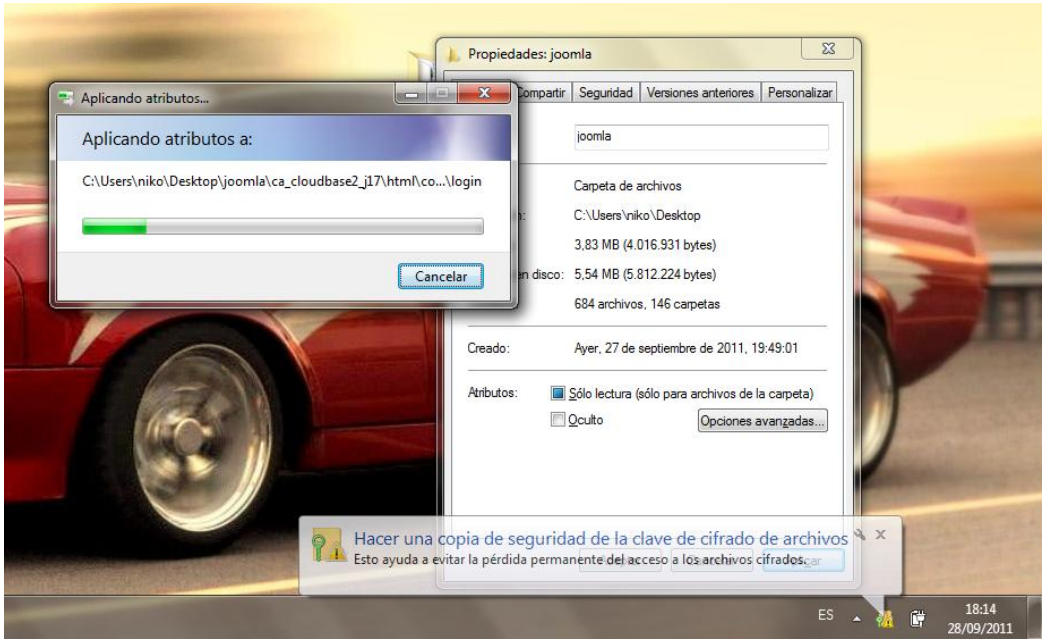




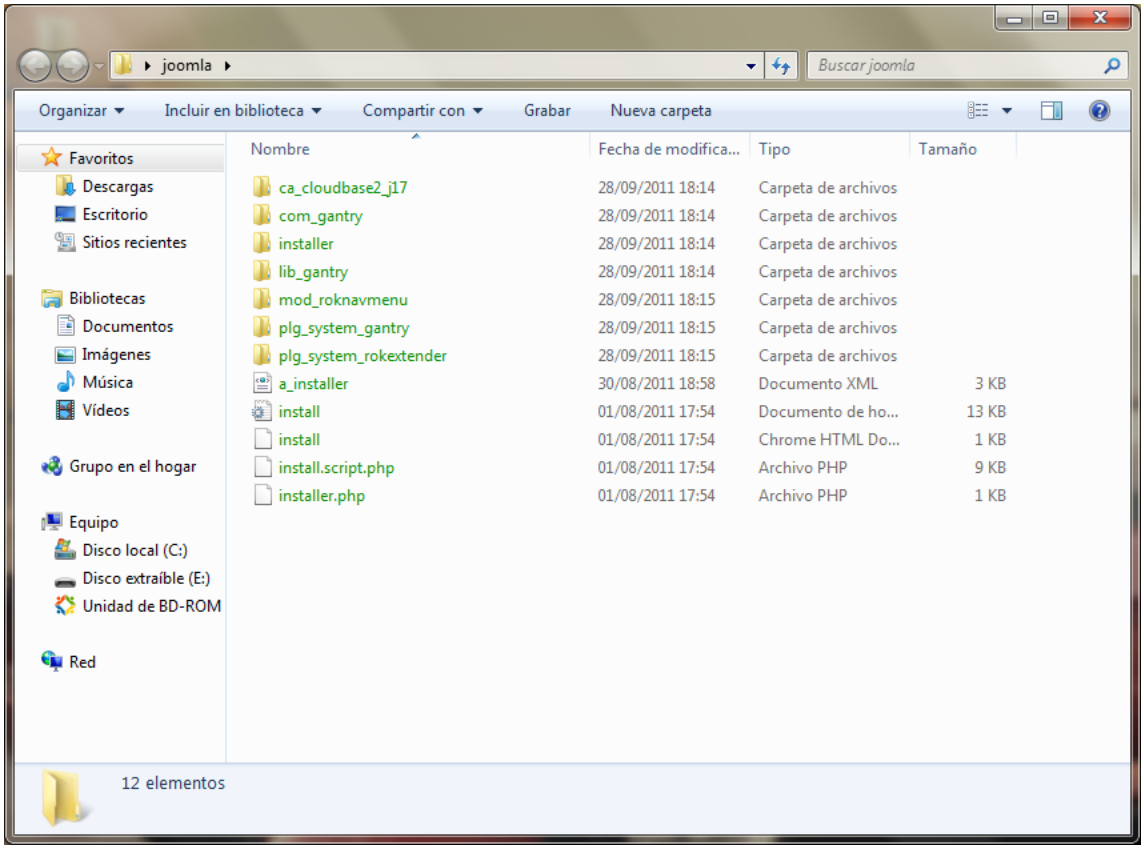
3.) Ahora aceptaremos y aplicaremos los cambios efectuados en esta carpeta, una vez aplicados nos aparecerá la siguiente pantalla en la que elegiremos la segunda opción puesto que la carpeta primaria contiene subcarpetas.



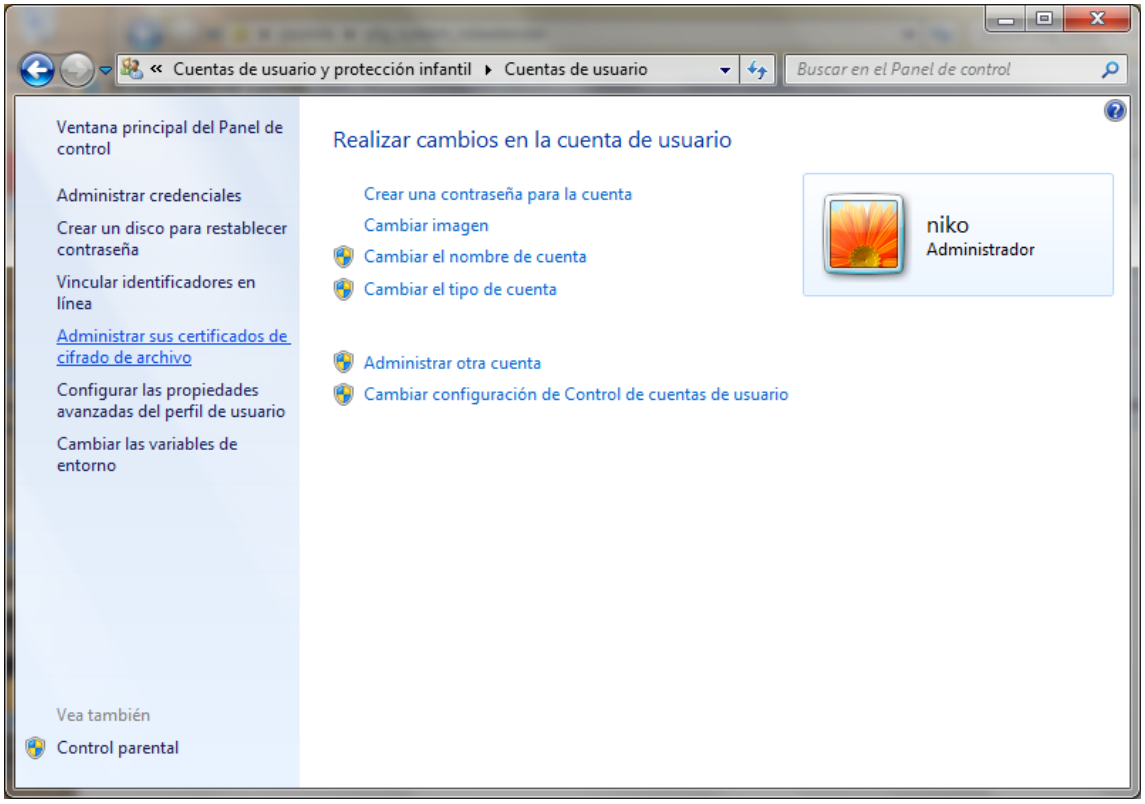
4.) Ahora dará comienzo el proceso de encriptación.



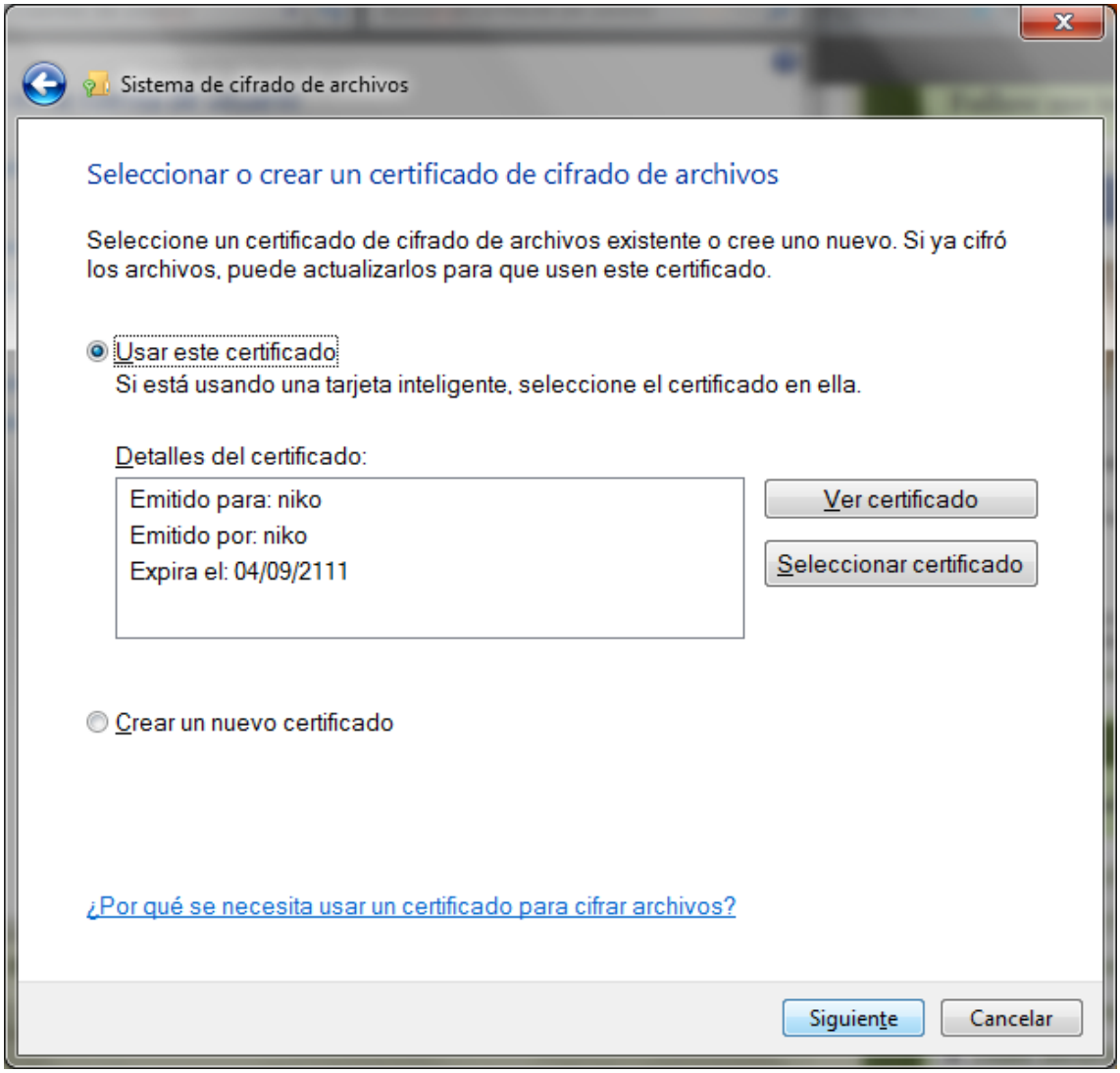
5.) Ahora al acceder a la carpeta podemos apreciar que los archivos que encontramos en su interior se han puesto de color verde:



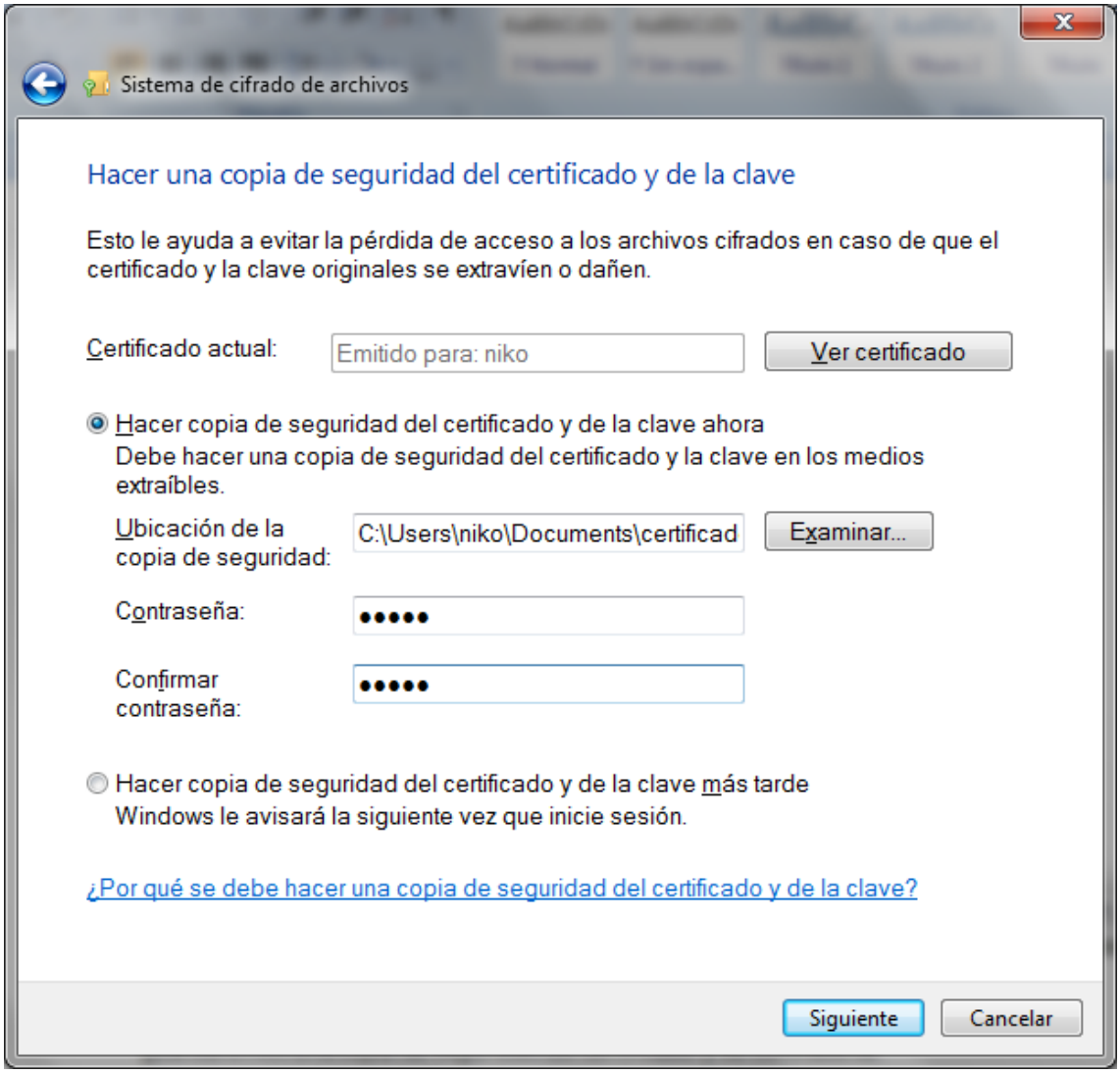
6.) Ahora nos dirigiremos a panel de control cuentas y protección infantil y una vez allí accederemos a la sección cuentas de usuario y accederemos a administrar sus certificados de cifrado de archivo.



7.) Una vez dentro deberemos de seguir los pasos del asistente y usar el certificado que nos propone el cifrado de archivos.

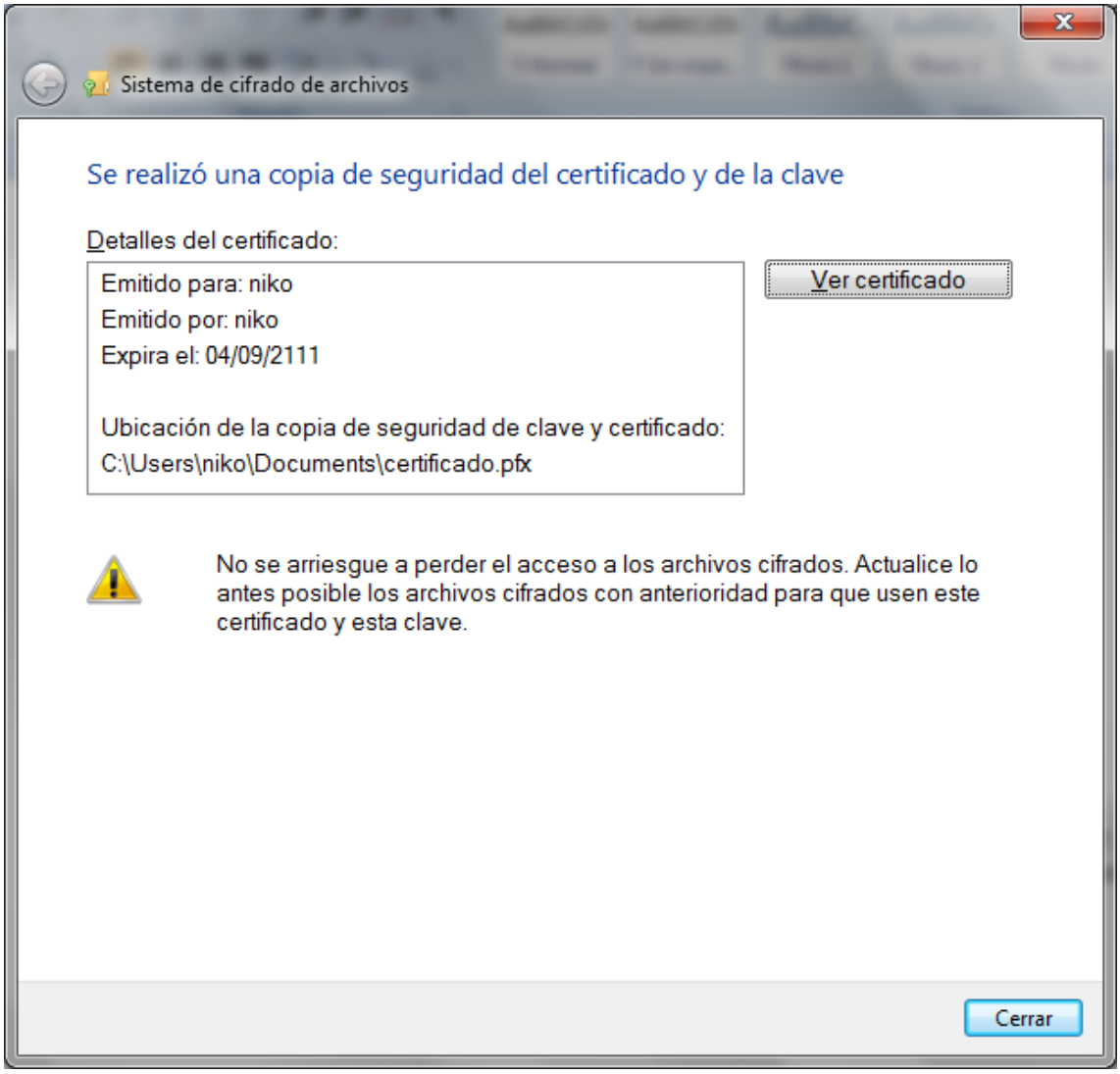


8.) Ahora deberemos de rellenar los siguientes campos, introduciendo el lugar donde guardaremos una copia de seguridad del certificado y su contraseña.



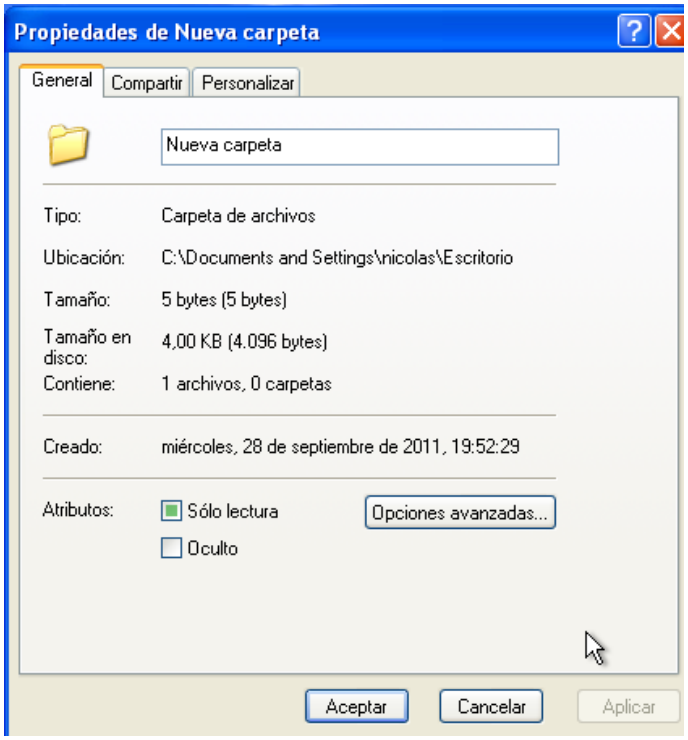
9.) En la pantalla que nos dice que indiquemos las unidades a las que queremos que se aplique el certificado marcamos especificar mas tarde.

10.) Por ultimo finalizamos el asistente:

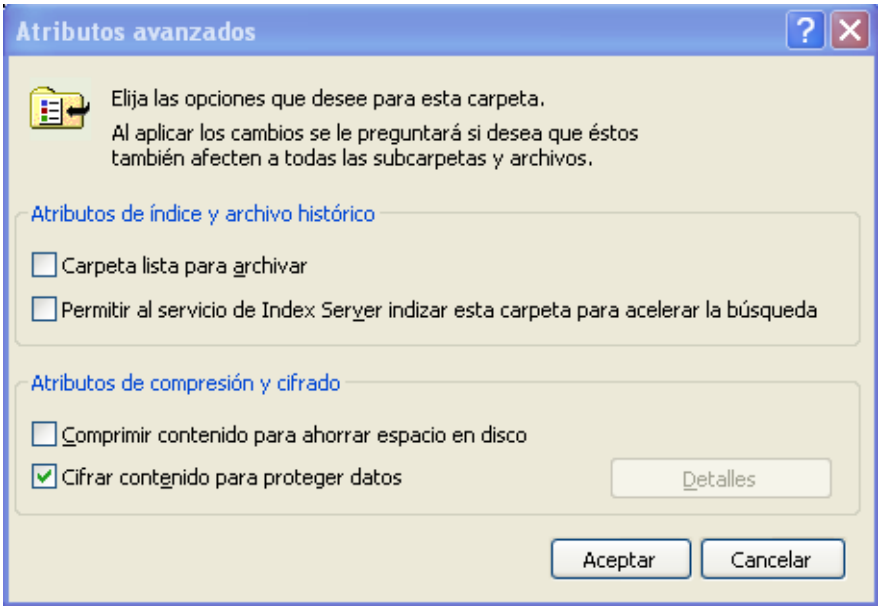

Sistema de cifrado de archivos
Se realizó una copia de seguridad del certificado y de la clave
Detalles del certificado:
Emitido para: niko
Emitido por: niko
Expira el: 04/09/2111
Ubicación de la copia de seguridad de clave y certificado:
C:\Users\niko\Documents\certificado.pfx
Ver certificado
No se arriesgue a perder el acceso a los archivos cifrados. Actualice lo antes posible los archivos cifrados con anterioridad para que usen este certificado y esta clave.
Cerrar

EN WINDOWS XP

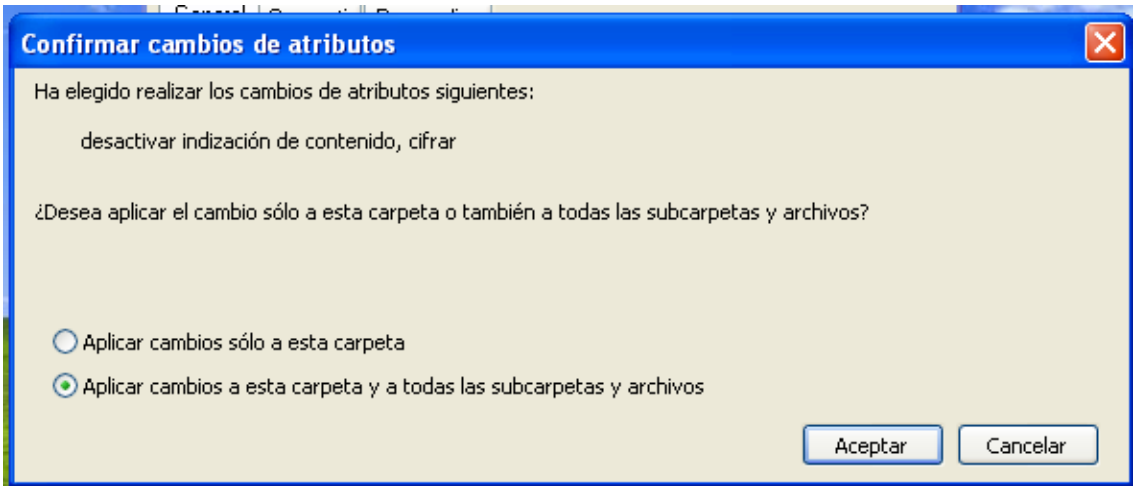
1.) Sobre la carpeta donde están los archivos pulsamos botón derecho/ propiedades,



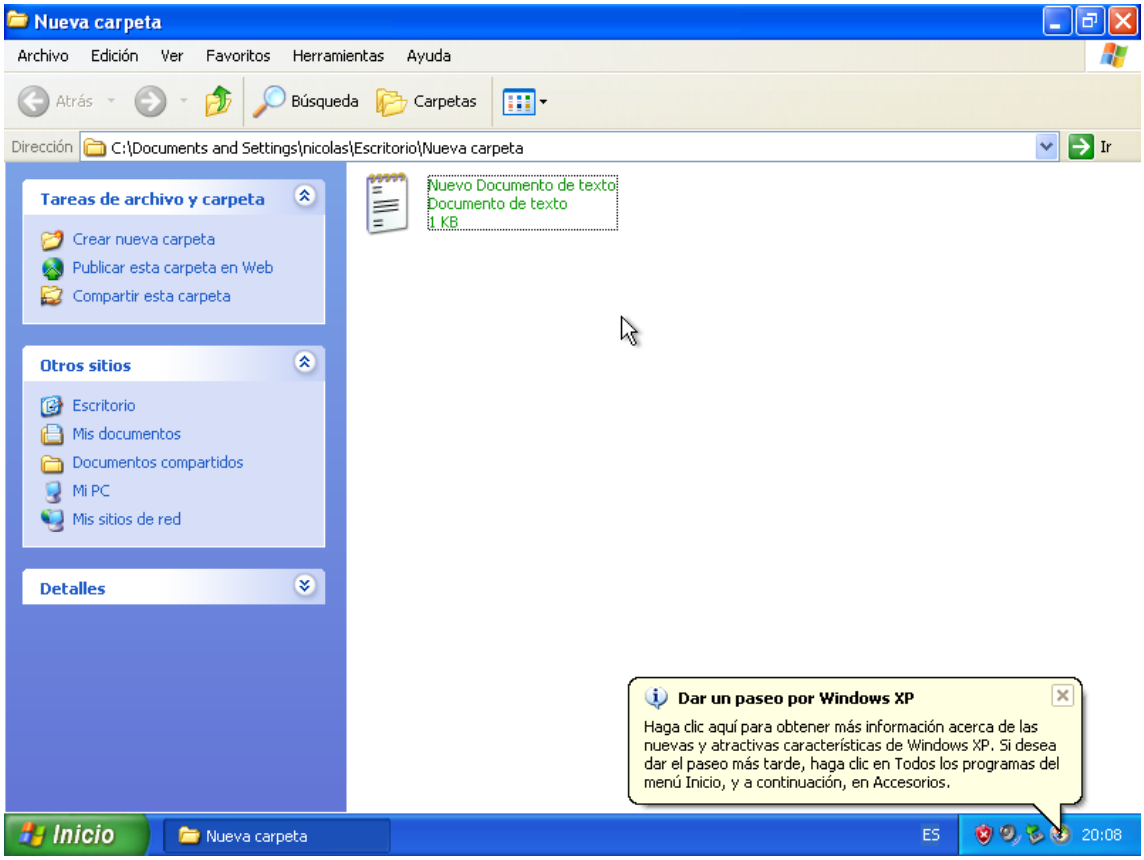
2.) Una vez alli en opciones generales de la carpeta pulsamos en opciones avanzadas, en la pantalla que nos aparece marcamos la opción “cifrar contenido para proteger datos”.



3.) Ahora aceptaremos y aplicaremos los cambios efectuados en esta carpeta, una vez aplicados nos aparecerá la siguiente pantalla en la que elegiremos la segunda opción puesto que la carpeta primaria contiene subcarpetas.



4.) Ahora al acceder a la carpeta podemos apreciar que los archivos que encontramos en su interior se han puesto de color verde:

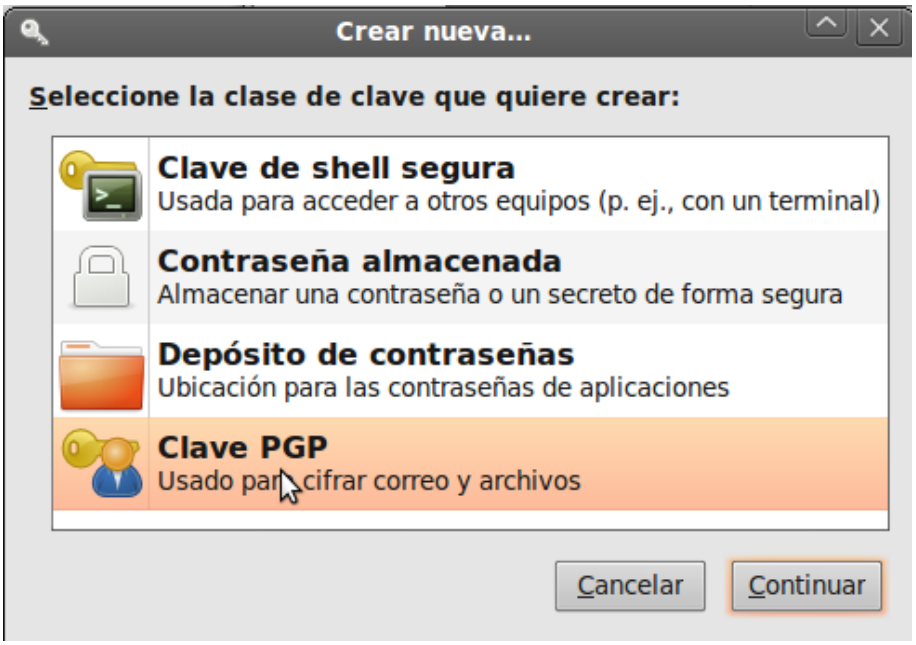


EN Linux PGP

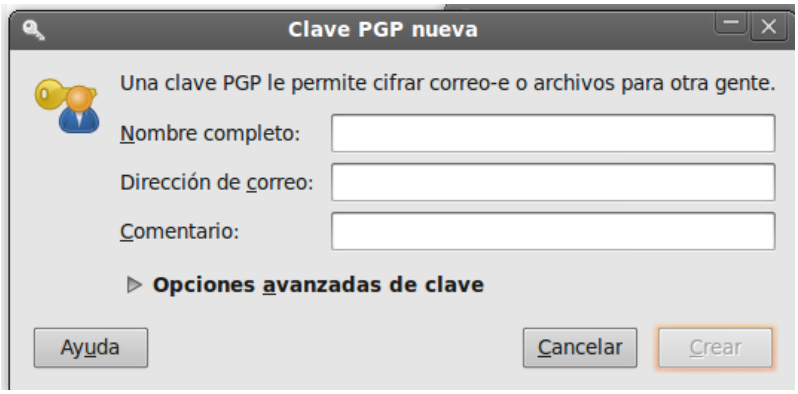
1.- Primero debemos de a aplicaciones y una vez allí ejecutar el programa contraseñas y claves de cifrado.

2.-Una vez realizado nos dirigiremos a la pestaña contraseñas y crearemos una nueva contraseña, para ello archivo crear nueva….

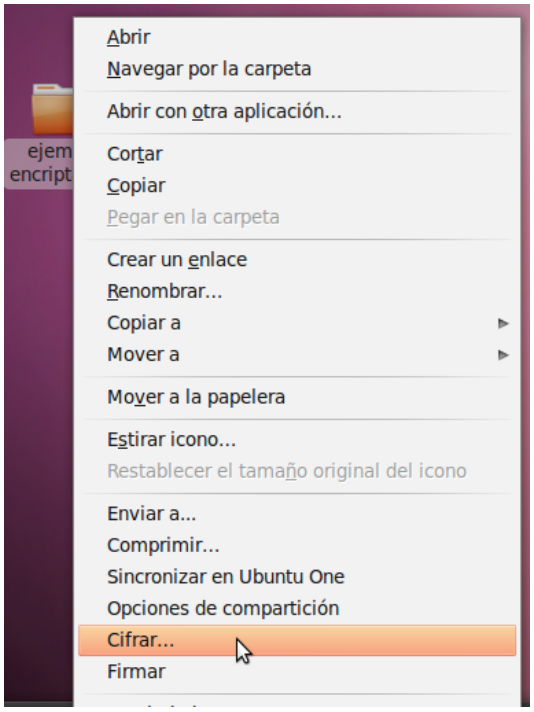
3.- Una vez realizados los pasos anteriores debemos de elegir la opción clave pgp.



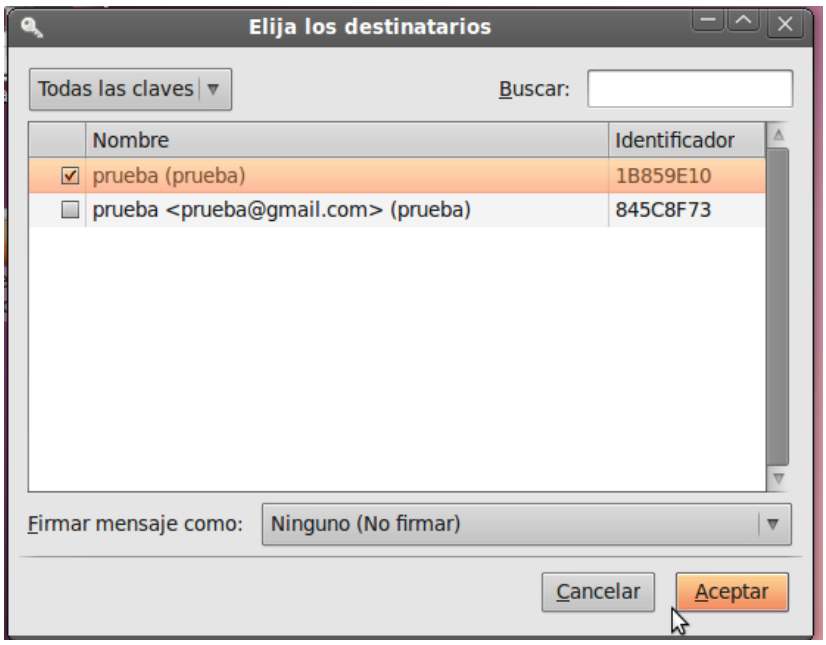
4.-Ahora deberemos de rellenar los campos requeridos para crear la contraseña.



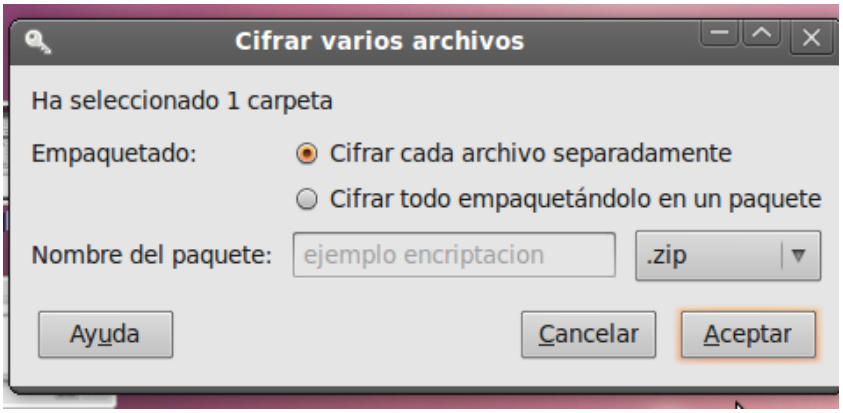
5.- Para cifrar una carpeta u archivo únicamente debemos de hacer doble click sobre dicho archivo y pulsar sobre la opción cifrar.



6.- Una vez hechos los pasos anteriores debemos de seleccionar la contraseña de cifrado con la que queremos cifrar el archivo.



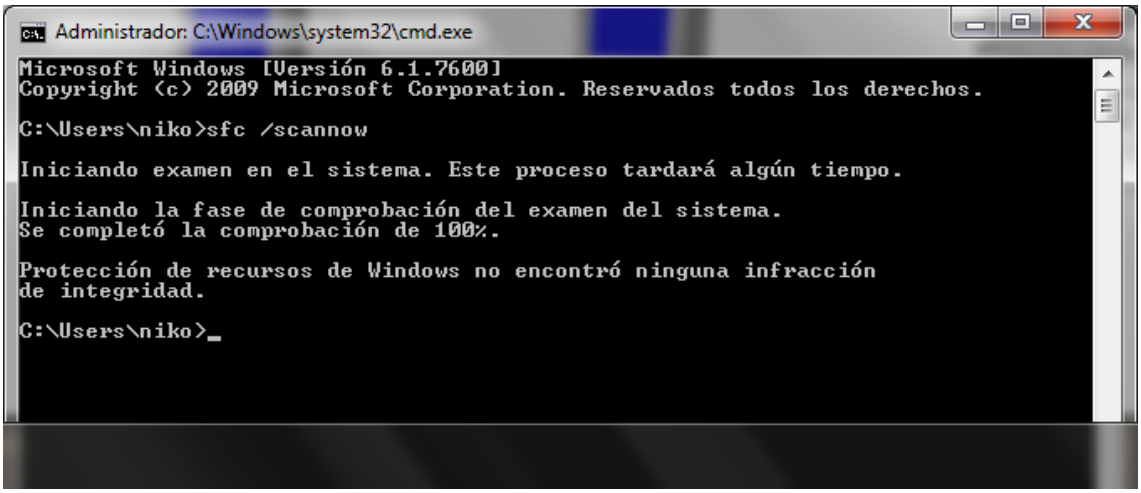
6.- Ahora deberemos de seleccionar las opciones deseadas y confirmar la encriptación del archivo. Una vez realizados estos pasos habremos cifrado el archivo o carpeta.



2.-REALIZACION DE LA VERIFICACIÓN DEL EQUIPO

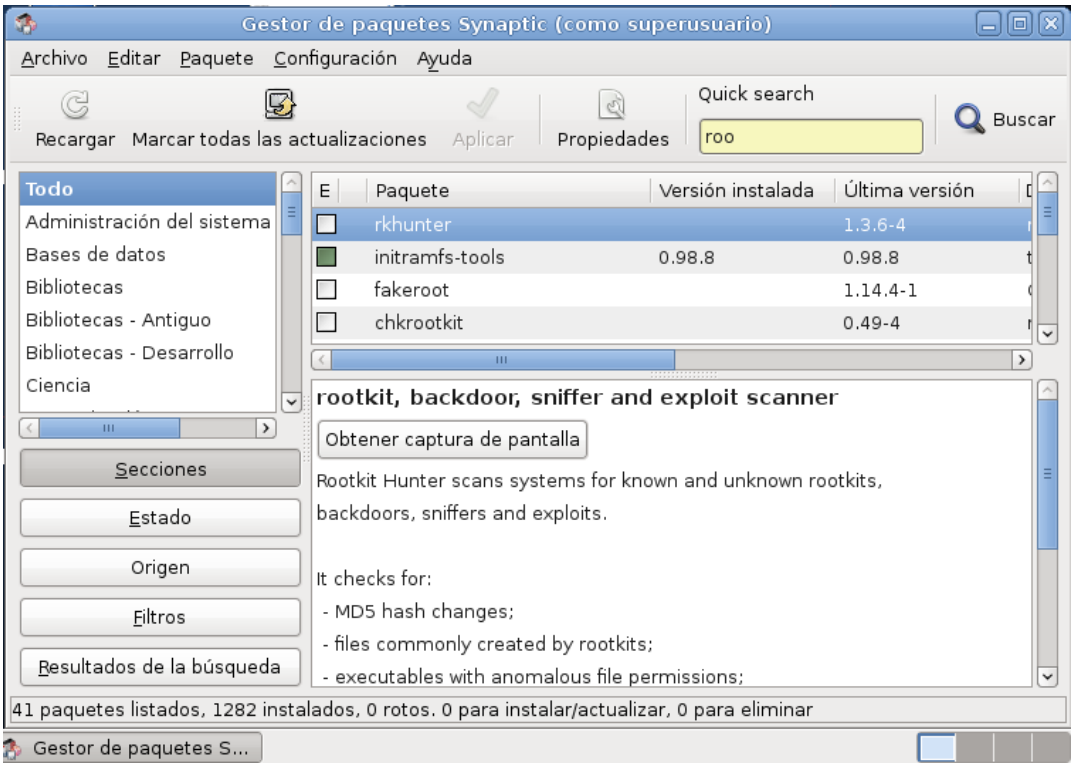
EN WINDOWS SFC

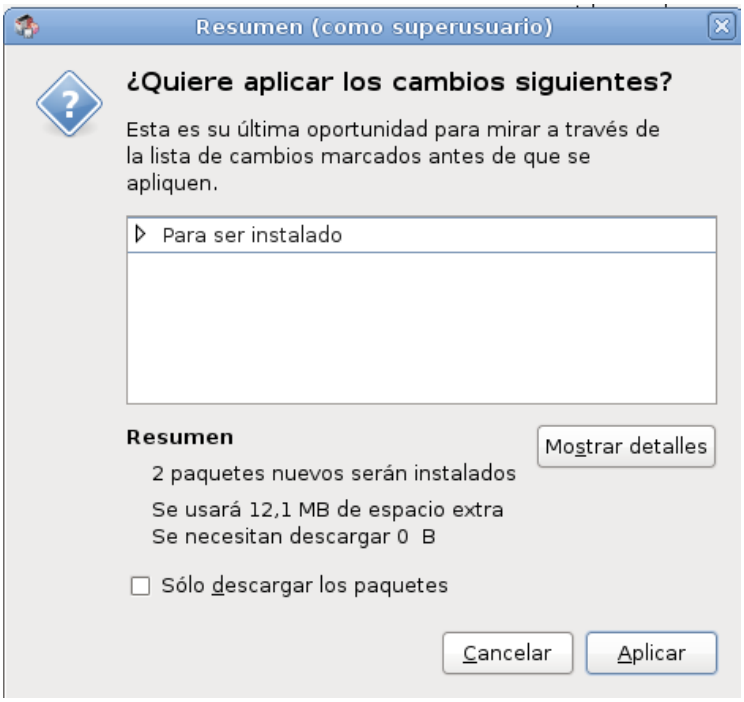
1. Debemos dirigirnos al terminal de Windows y ejecutarlo en modo administrador.
2. Una vez realizado el paso anterior deberemos de introducir el comando sfc /scannow, una vez hecho esto dará comienzo el examen del sistema, una vez finalizado nos mostrara si existen errores en nuestro sistema



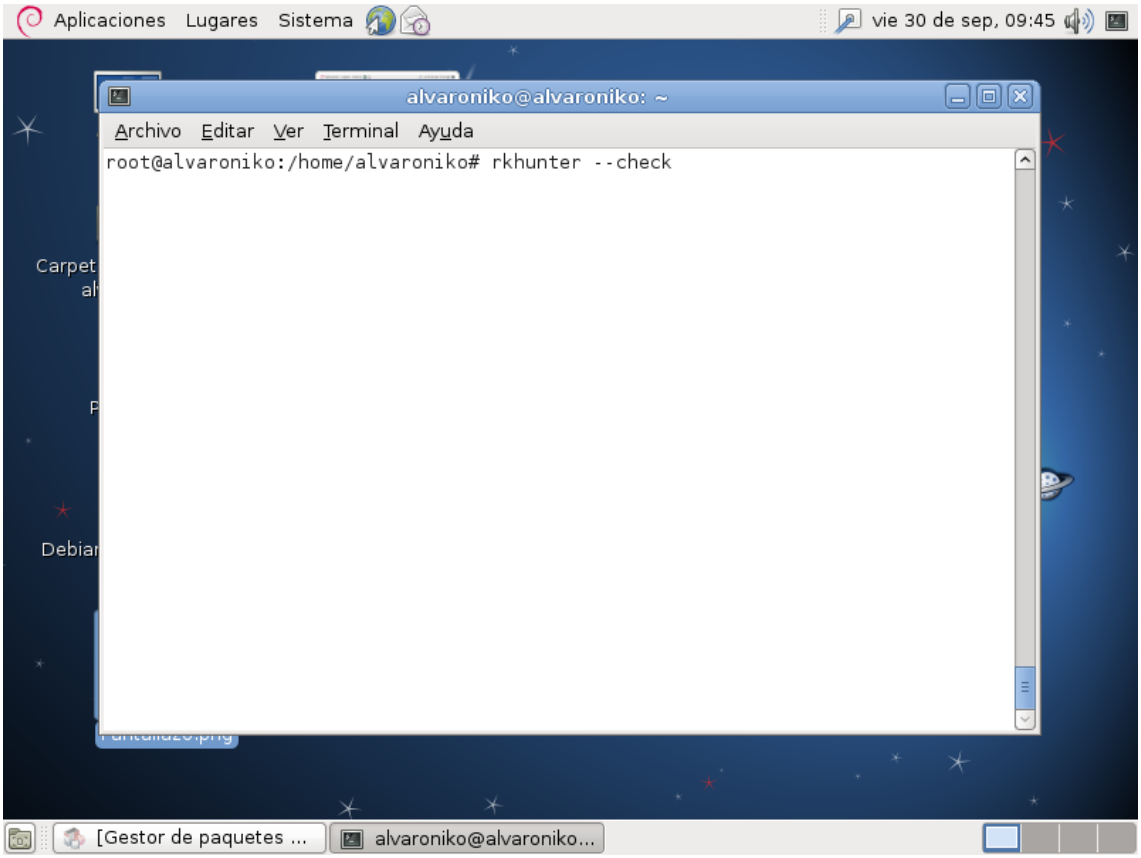
EN LINUX Rootkit hunter

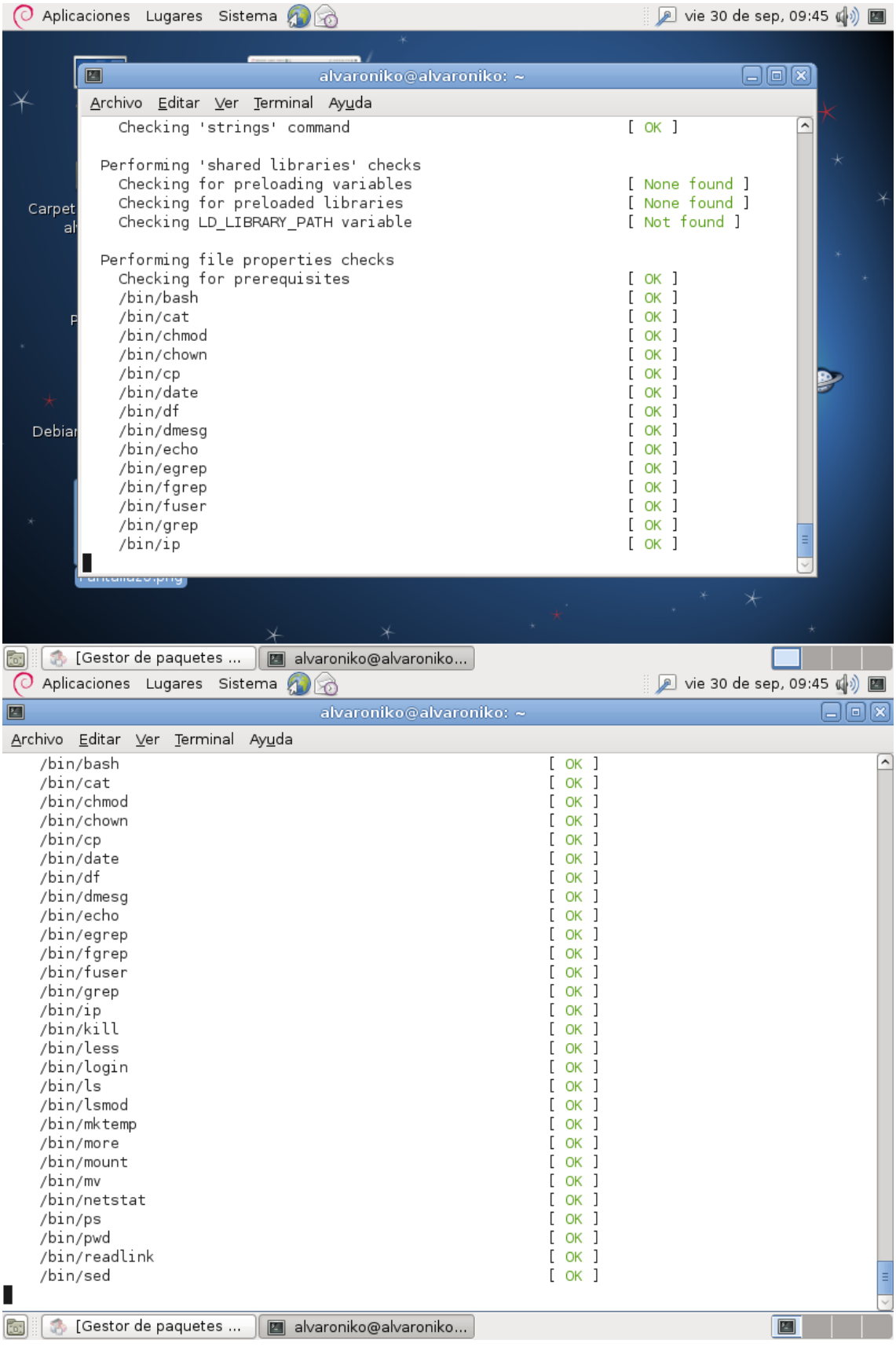
1.- Primero debemos de dirigirnos al gestor de paquetes synaptic, una vez allí buscamos el paquete rkhuter y lo instalamos.

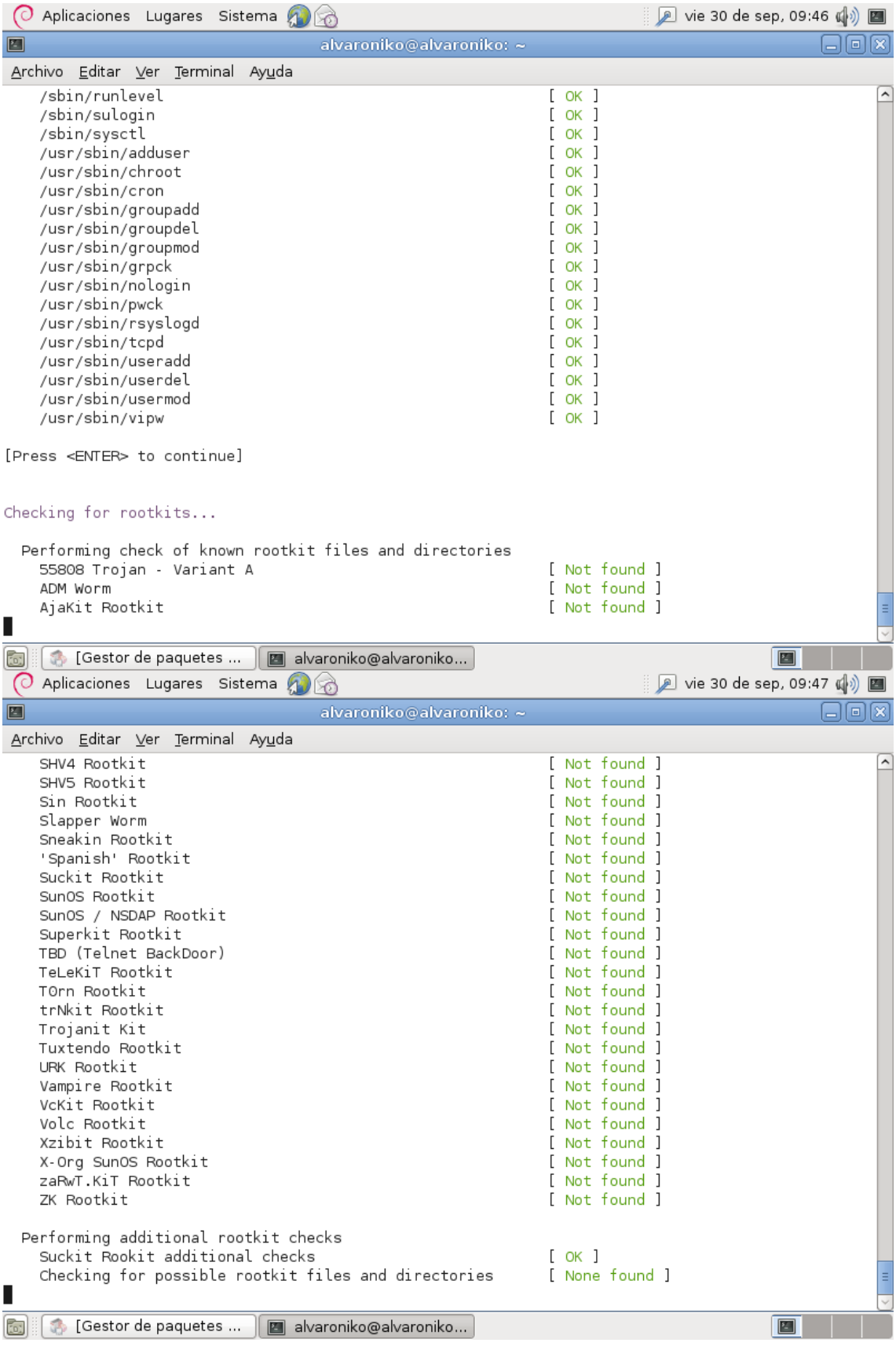




2.- una vez instalado para ejecutarlo deberemos de abrir un terminal nuevo e introducir el comando rkhunter –check. Una vez introducido este comando comenzara el análisis de nuestro sistema.



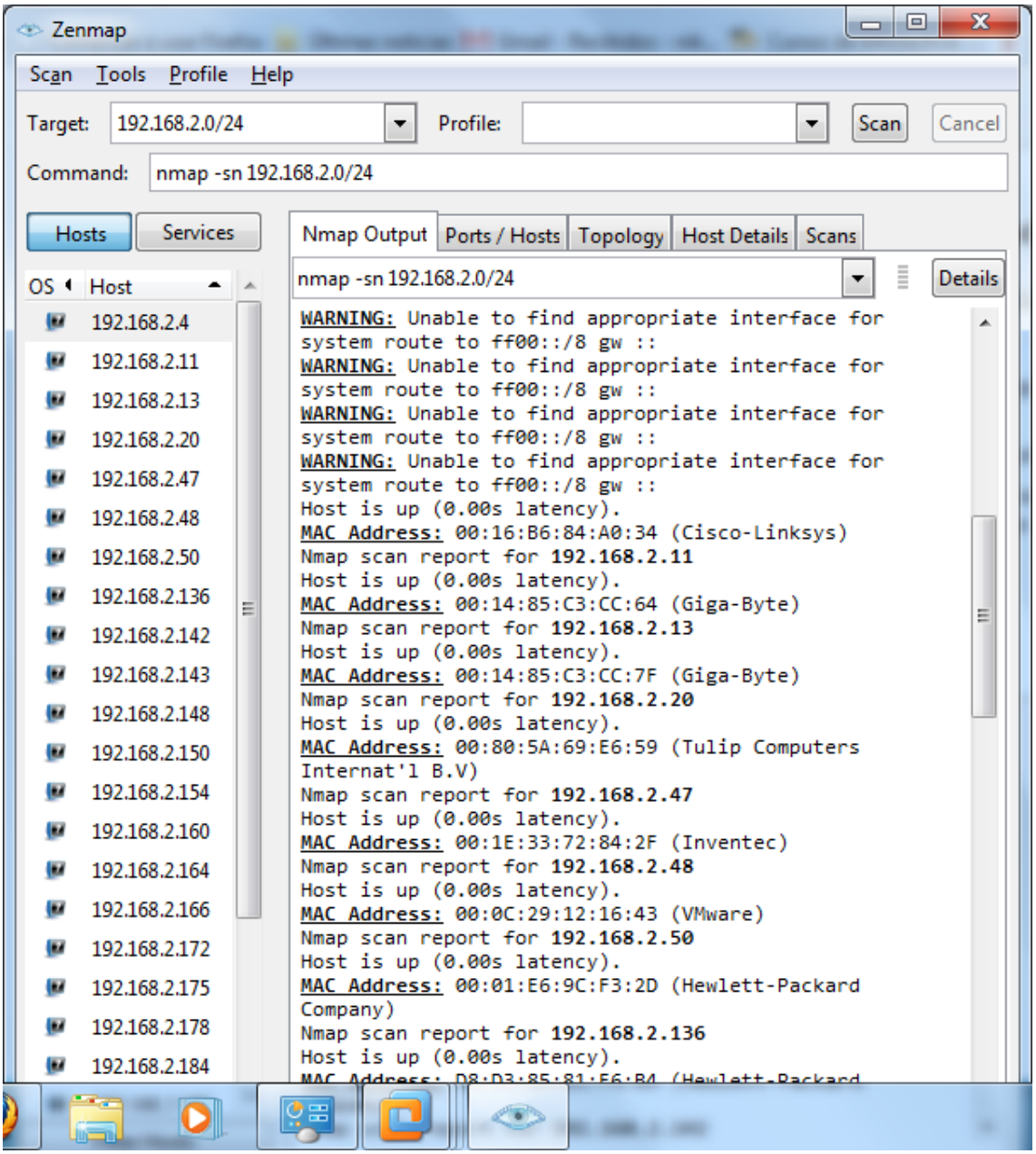

Aplicaciones Lugares Sistema
vie 30 de sep, 09:45
alvaroniko@alvaroniko: ~
Archivo Editar Ver Terminal Ayuda
Checking 'strings' command [OK]
Performing 'shared libraries' checks
Checking for preloading variables [None found]
Checking for preloaded libraries [None found]
Checking LD_LIBRARY_PATH variable [Not found]
Performing file properties checks
Checking for prerequisites [OK]
/bin/bash [OK]
/bin/cat [OK]
/bin/chmod [OK]
/bin/chown [OK]
/bin/cp [OK]
/bin/date [OK]
/bin/df [OK]
/bin/dmesg [OK]
/bin/echo [OK]
/bin/egrep [OK]
/bin/fgrep [OK]
/bin/fuser [OK]
/bin/grep [OK]
/bin/ip [OK]
[Gestor de paquetes ...
alvaroniko@alvaroniko...
Aplicaciones Lugares Sistema
vie 30 de sep, 09:45
alvaroniko@alvaroniko: ~
Archivo Editar Ver Terminal Ayuda
/bin/bash [OK]
/bin/cat [OK]
/bin/chmod [OK]
/bin/chown [OK]
/bin/cp [OK]
/bin/date [OK]
/bin/df [OK]
/bin/dmesg [OK]
/bin/echo [OK]
/bin/egrep [OK]
/bin/fgrep [OK]
/bin/fuser [OK]
/bin/grep [OK]
/bin/ip [OK]
/bin/kill [OK]
/bin/less [OK]
/bin/login [OK]
/bin/ls [OK]
/bin/lsmod [OK]
/bin/mktemp [OK]
/bin/more [OK]
/bin/mount [OK]
/bin/mv [OK]
/bin/netstat [OK]
/bin/ps [OK]
/bin/pwd [OK]
/bin/readlink [OK]
/bin/sed [OK]
[Gestor de paquetes ...
alvaroniko@alvaroniko...


Aplicaciones Lugares Sistema
vie 30 de sep, 09:46
alvaroniko@alvaroniko: ~
Archivo Editar Ver Terminal Ayuda
/sbin/runlevel [OK]
/sbin/sulogin [OK]
/sbin/sysctl [OK]
/usr/sbin/adduser [OK]
/usr/sbin/chroot [OK]
/usr/sbin/cron [OK]
/usr/sbin/groupadd [OK]
/usr/sbin/groupdel [OK]
/usr/sbin/groupmod [OK]
/usr/sbin/grpck [OK]
/usr/sbin/nologin [OK]
/usr/sbin/pwck [OK]
/usr/sbin/rsyslogd [OK]
/usr/sbin/tcpd [OK]
/usr/sbin/useradd [OK]
/usr/sbin/userdel [OK]
/usr/sbin/usermod [OK]
/usr/sbin/vipw [OK]
[Press <ENTER> to continue]
Checking for rootkits...
Performing check of known rootkit files and directories
55808 Trojan - Variant A [Not found]
ADM Worm [Not found]
AjaKit Rootkit [Not found]
[Gestor de paquetes ...
alvaroniko@alvaroniko...
Aplicaciones Lugares Sistema
vie 30 de sep, 09:47
alvaroniko@alvaroniko: ~
Archivo Editar Ver Terminal Ayuda
SHV4 Rootkit [Not found]
SHV5 Rootkit [Not found]
Sin Rootkit [Not found]
Slapper Worm [Not found]
Sneakin Rootkit [Not found]
'Spanish' Rootkit [Not found]
Suckit Rootkit [Not found]
SunOS Rootkit [Not found]
SunOS / NSDAP Rootkit [Not found]
Superkit Rootkit [Not found]
TBD (Telnet BackDoor) [Not found]
TeLeKiT Rootkit [Not found]
TOrn Rootkit [Not found]
trNkit Rootkit [Not found]
Trojanit Kit [Not found]
Tuxtendo Rootkit [Not found]
URK Rootkit [Not found]
Vampire Rootkit [Not found]
VcKit Rootkit [Not found]
Volc Rootkit [Not found]
Xzibit Rootkit [Not found]
X-Org SunOS Rootkit [Not found]
zaRwT.KiT Rootkit [Not found]
ZK Rootkit [Not found]
Performing additional rootkit checks
Suckit Rookit additional checks [OK]
Checking for possible rootkit files and directories [None found]
[Gestor de paquetes ...
alvaroniko@alvaroniko...

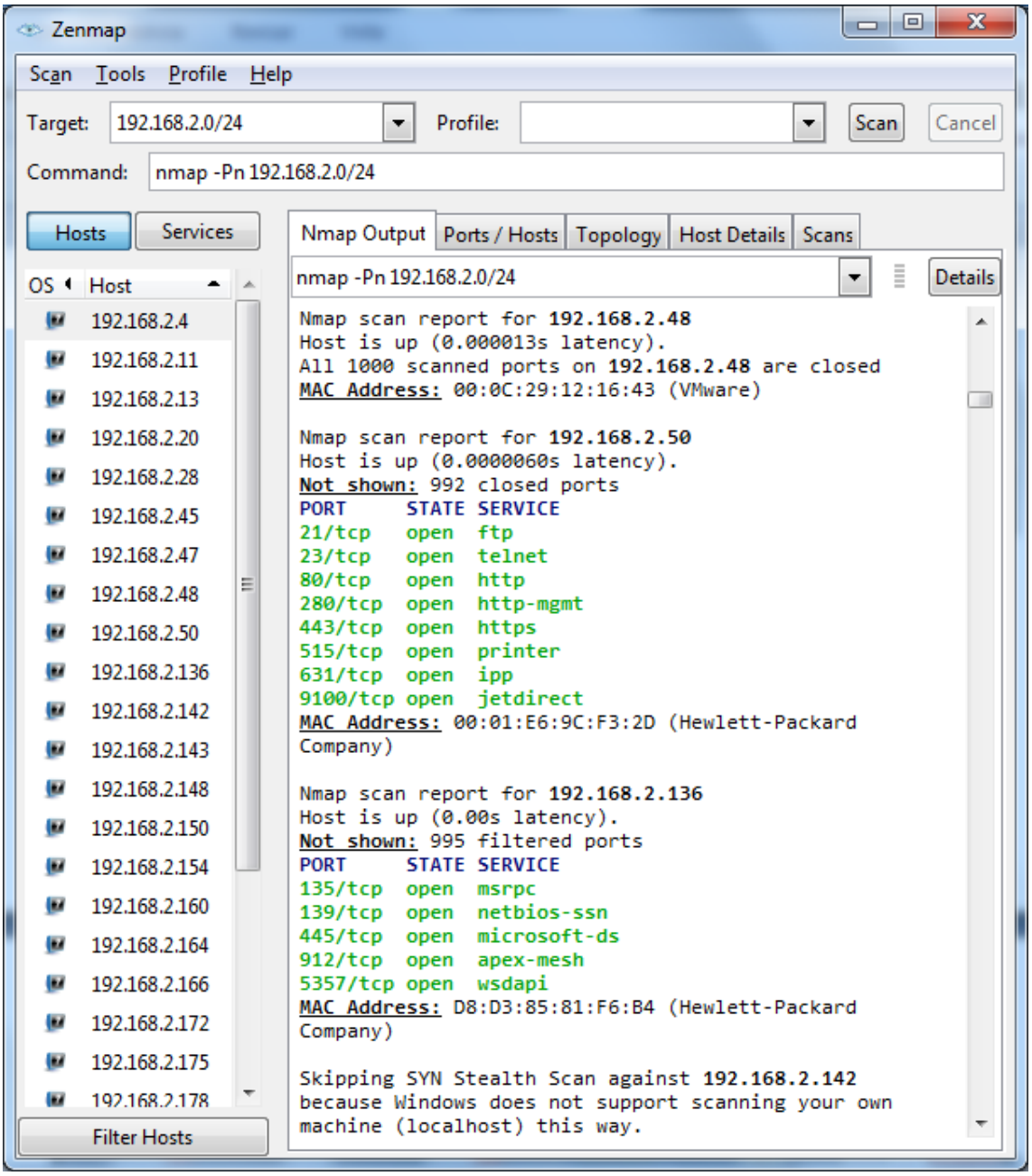
3.-NMAP

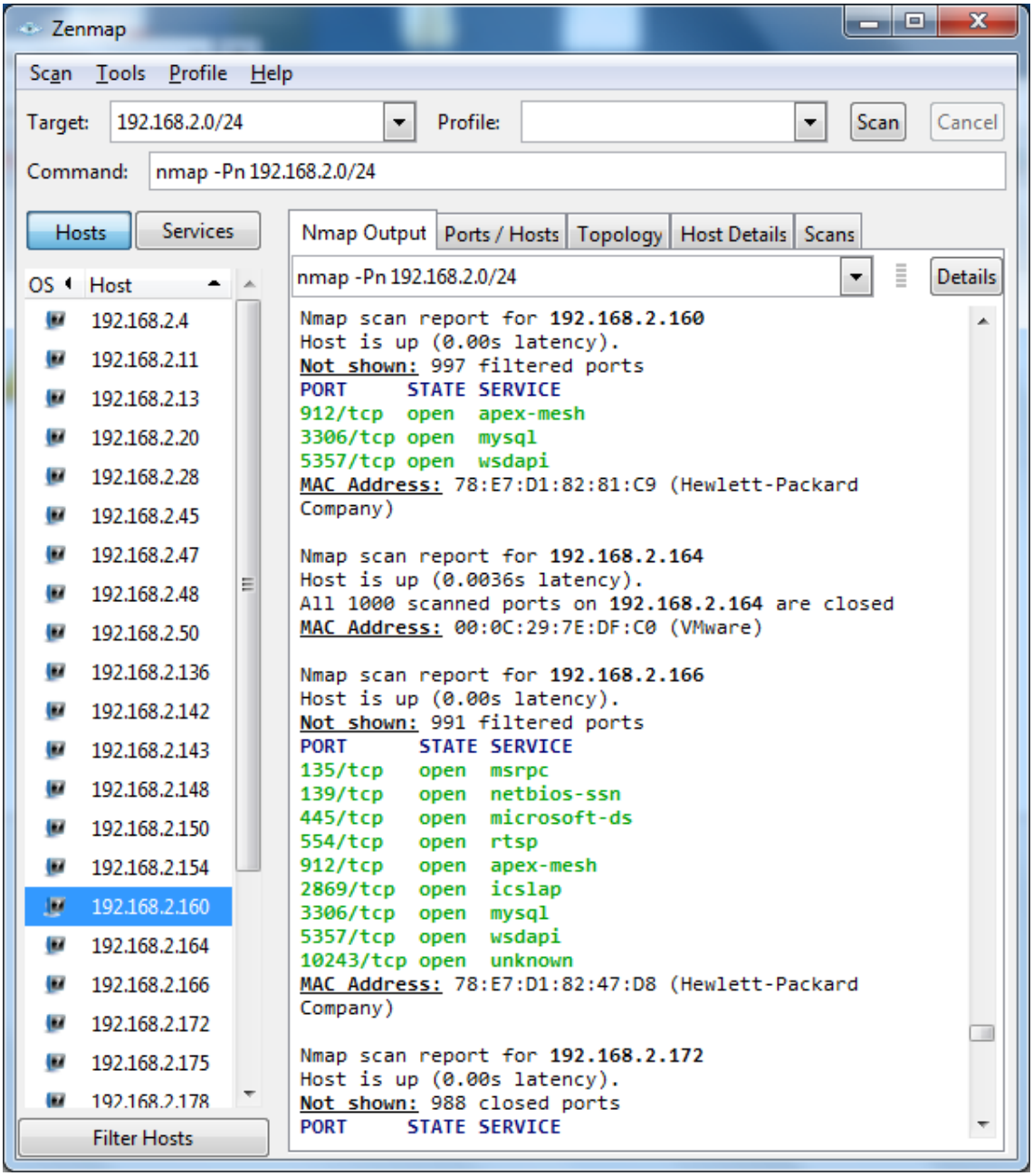
EN WINDOWS

1.- Una vez instalado el Nmap utilizaremos algunas de las opciones; en primer lugar utilizaremos el comando nmap –sn 192.168.2.0/24 para averiguar la mac de todos los ordenadores de la red 192.168.2.0.

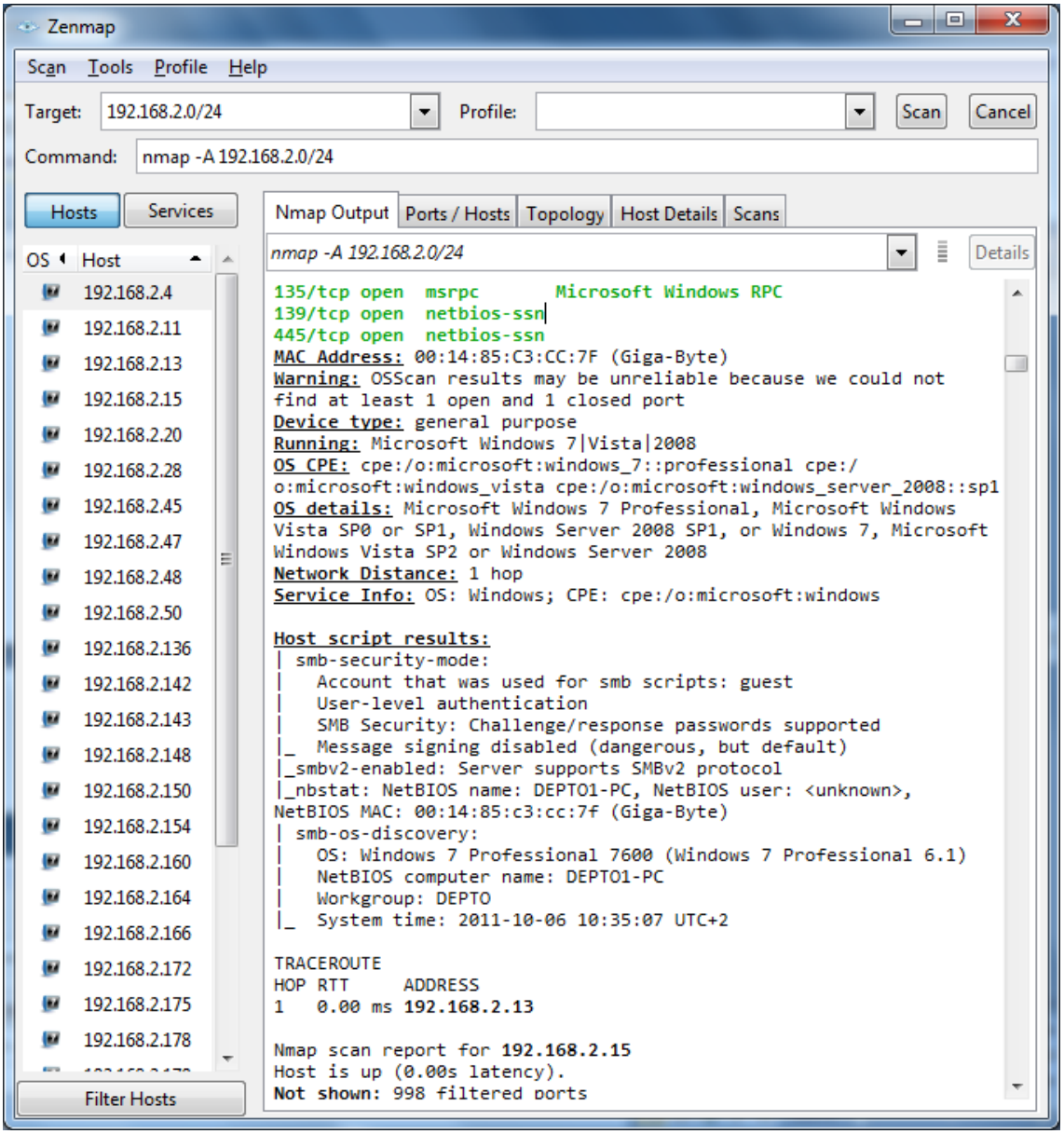


Otra opción muy atractiva es la de averiguar los puertos que tiene abiertos un ordenador, para ello deberemos de introducir el comando nmap –Pn 192.168.2.4/24.



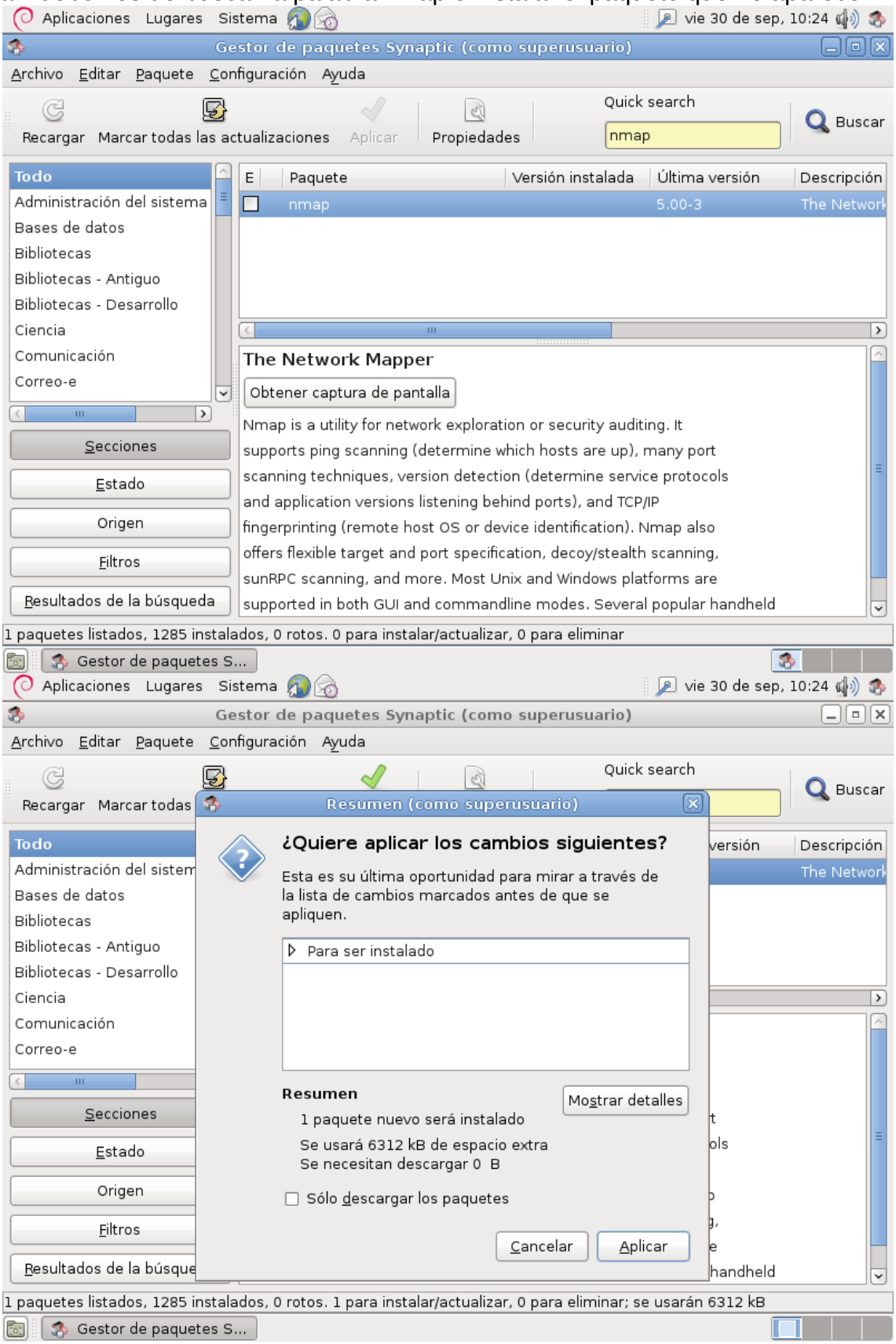

Zenmap
Scan Tools Profile Help
Target: 192.168.2.0/24
Profile:
Scan
Cancel
Command: nmap -Pn 192.168.2.0/24
Hosts
Services
OS Host
192.168.2.4
192.168.2.11
192.168.2.13
192.168.2.20
192.168.2.28
192.168.2.45
192.168.2.47
192.168.2.48
192.168.2.50
192.168.2.136
192.168.2.142
192.168.2.143
192.168.2.148
192.168.2.150
192.168.2.154
192.168.2.160
192.168.2.164
192.168.2.166
192.168.2.172
192.168.2.175
192.168.2.178
Filter Hosts
Nmap Output
Ports / Hosts
Topology
Host Details
Scans
nmap -Pn 192.168.2.0/24
Details
Nmap scan report for 192.168.2.160
Host is up (0.00s latency).
Not shown: 997 filtered ports
PORT STATE SERVICE
912/tcp open apex-mesh
3306/tcp open mysql
5357/tcp open wsdapi
MAC Address: 78:E7:D1:82:81:C9 (Hewlett-Packard Company)
Nmap scan report for 192.168.2.164
Host is up (0.0036s latency).
All 1000 scanned ports on 192.168.2.164 are closed
MAC Address: 00:0C:29:7E:DF:C0 (VMware)
Nmap scan report for 192.168.2.166
Host is up (0.00s latency).
Not shown: 991 filtered ports
PORT STATE SERVICE
135/tcp open msrpc
139/tcp open netbios-ssn
445/tcp open microsoft-ds
554/tcp open rtsp
912/tcp open apex-mesh
2869/tcp open icslap
3306/tcp open mysql
5357/tcp open wsdapi
10243/tcp open unknown
MAC Address: 78:E7:D1:82:47:D8 (Hewlett-Packard Company)
Nmap scan report for 192.168.2.172
Host is up (0.00s latency).
Not shown: 988 closed ports
PORT STATE SERVICE

Por último usaremos la opción nmap –A 192.168.2.0/24 para averiguar el sistema operativo y otras opciones de todos los host de la red 192.168.2.0/24.

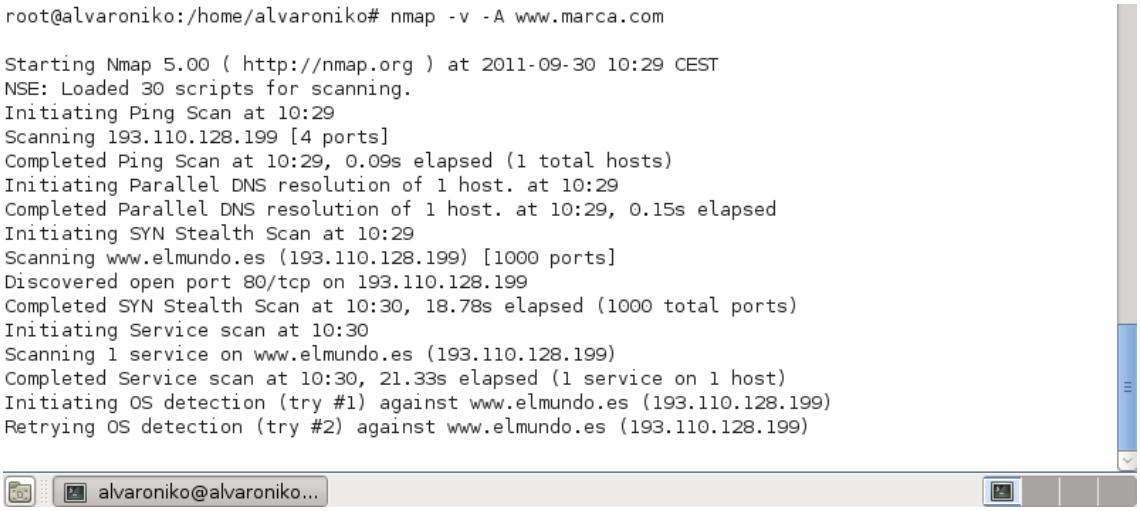


EN LINUX

1.- Primero nos debemos de dirigir al gestor de paquetes del synaptic. Una vez allí debemos de buscar la palabra nmap e instalar el paquete que no aparece.



2.- Para ejecutarlo únicamente se debe de abrir un nuevo terminal y teclear namap seguido de la opción deseada en nuestro caso el comando será nmap –v –A www.marca.com

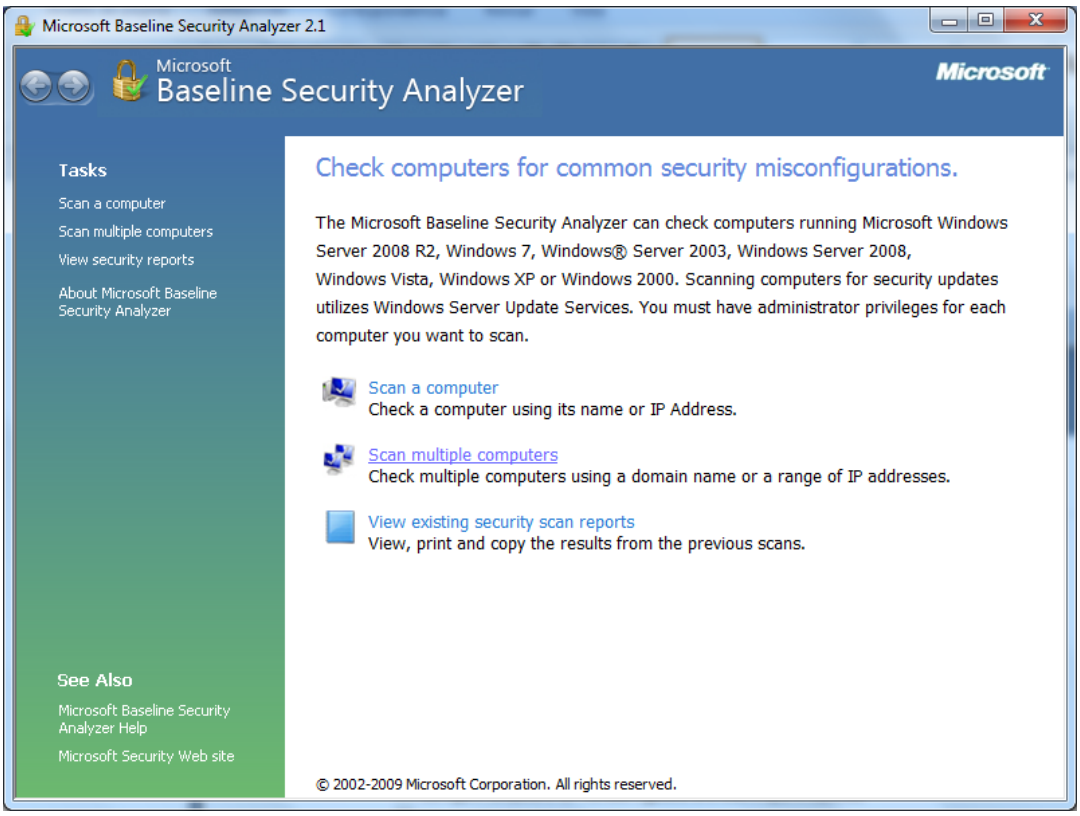


3.- Una vez ejecutadas esas opciones se procederá al análisis de la pagina web.

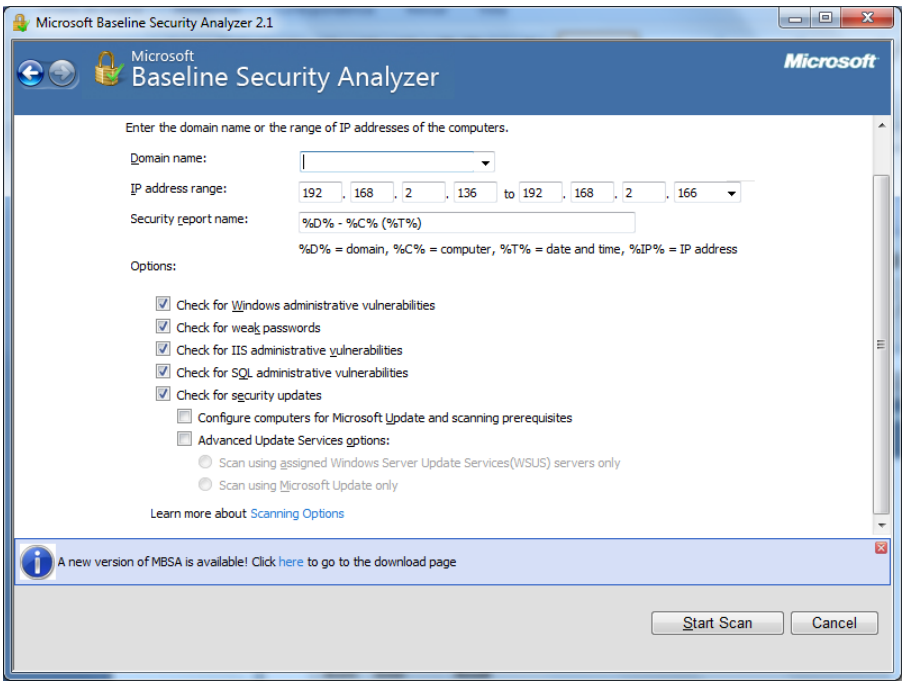
4.-MBSA

Para usar el BSA deberemos de seguir los siguientes pasos:

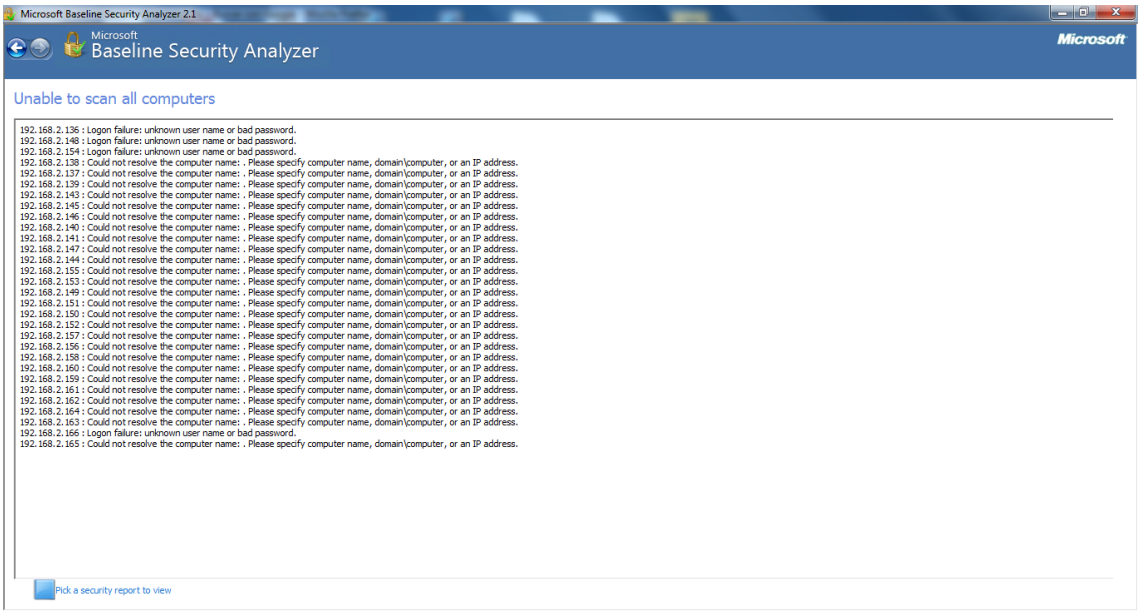
1.- Elegiremos la opcion scan multiples computers para analizar varios ordenadores:



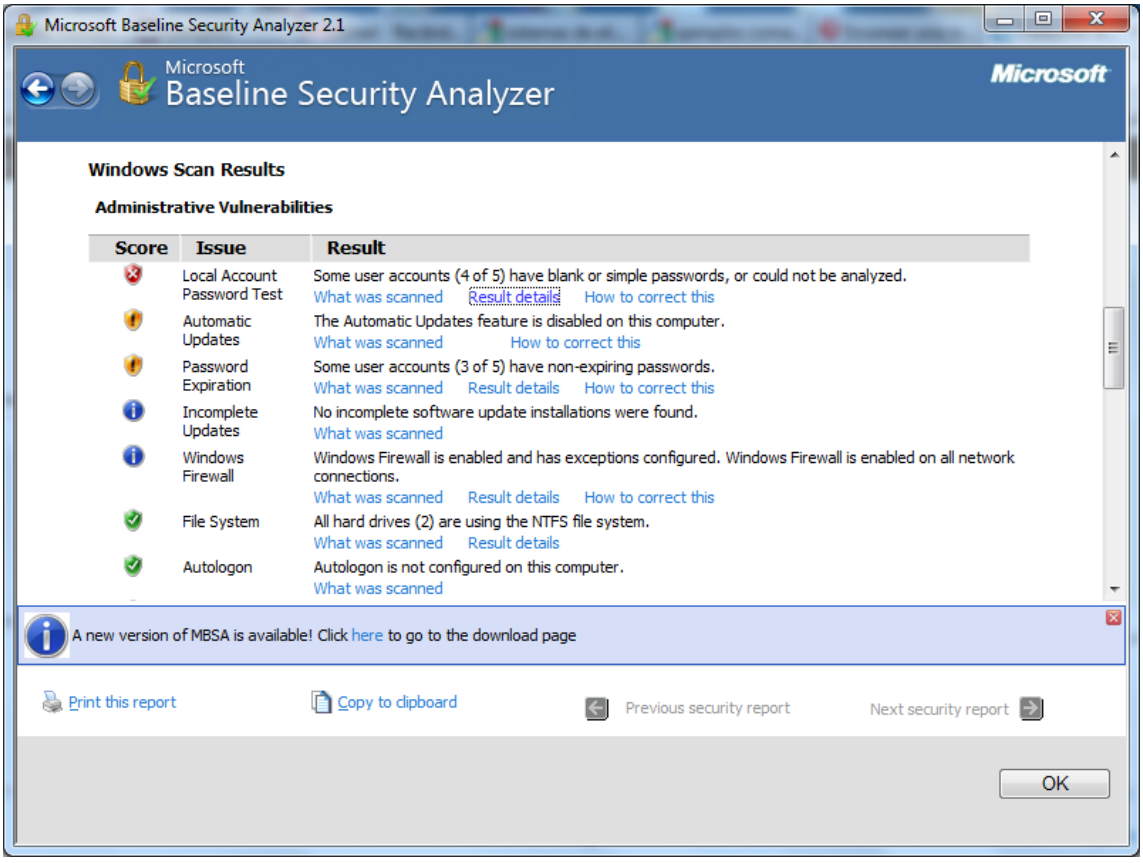
2.- Ahora deberemos de introducir el rango de direcciones que deseamos analizar:



3.- A continuación podremos observar cómo se realiza el análisis.



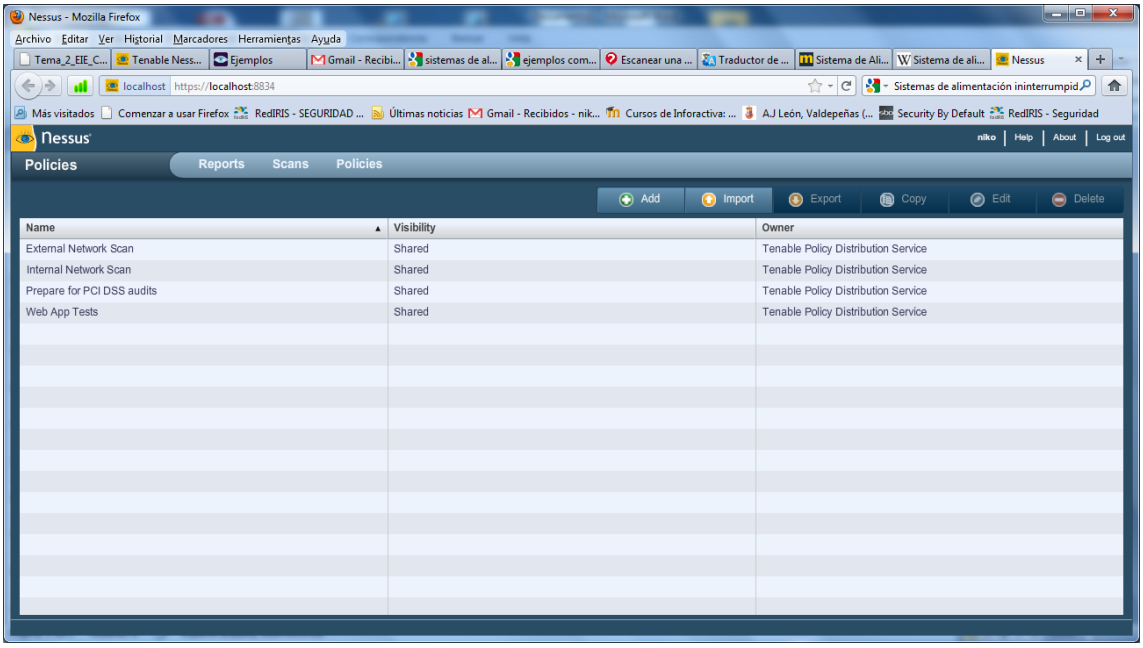
4.- Una vez finalizado el analisis podemos ver las vulnerabilidades existentes.



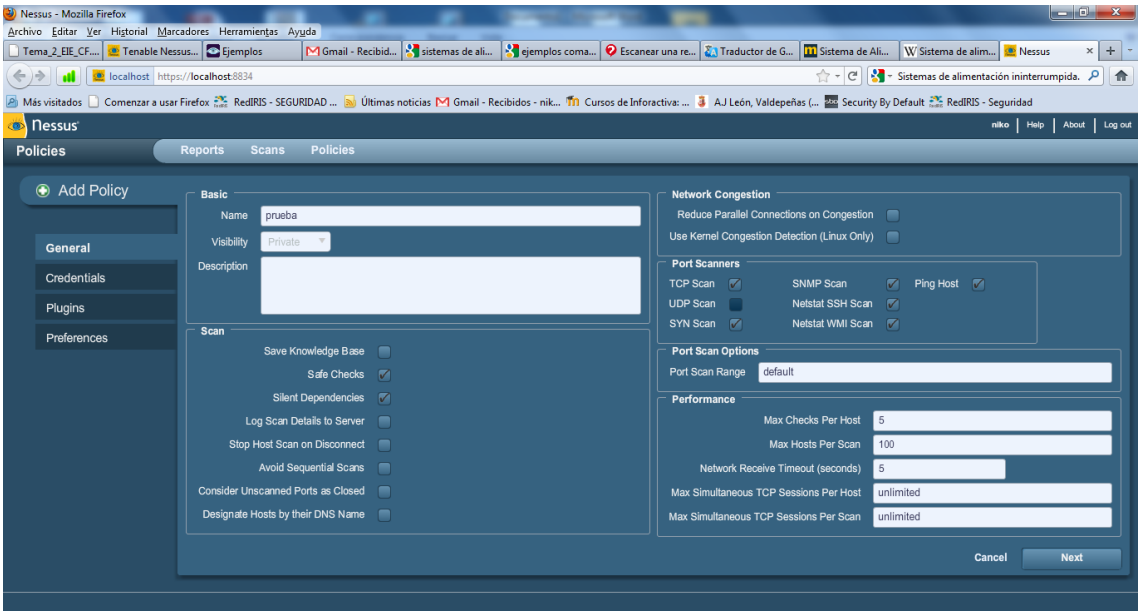
5.-NESSUS

Para utilizar nesus debemos de seguir los siguientes pasos

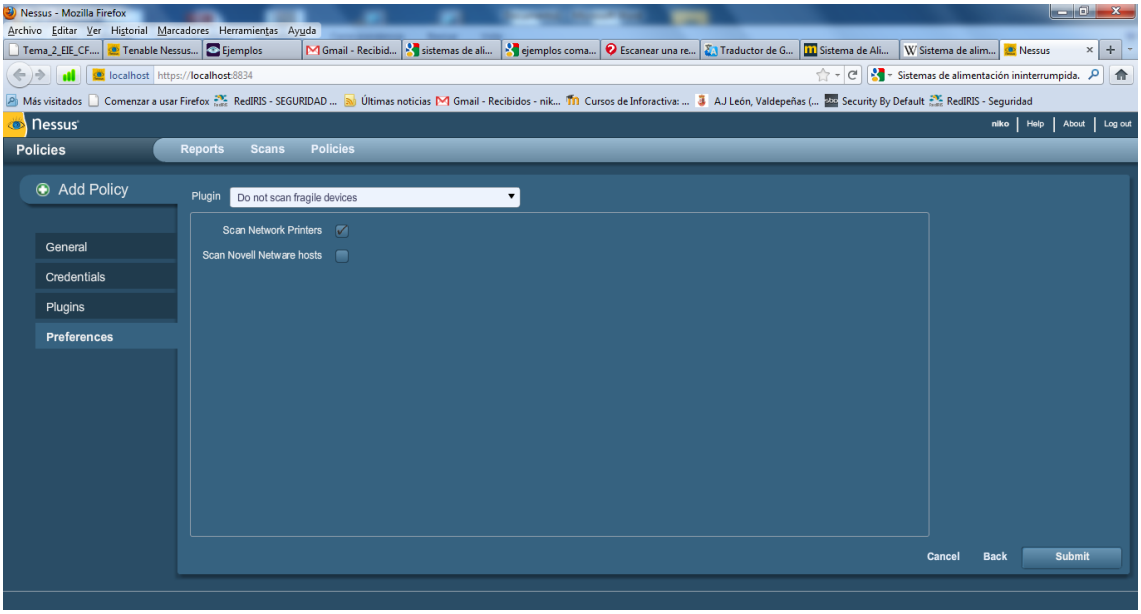
1.- En primer lugar nos dirigimos a policies, y a contibuación pulsamos sobre add.



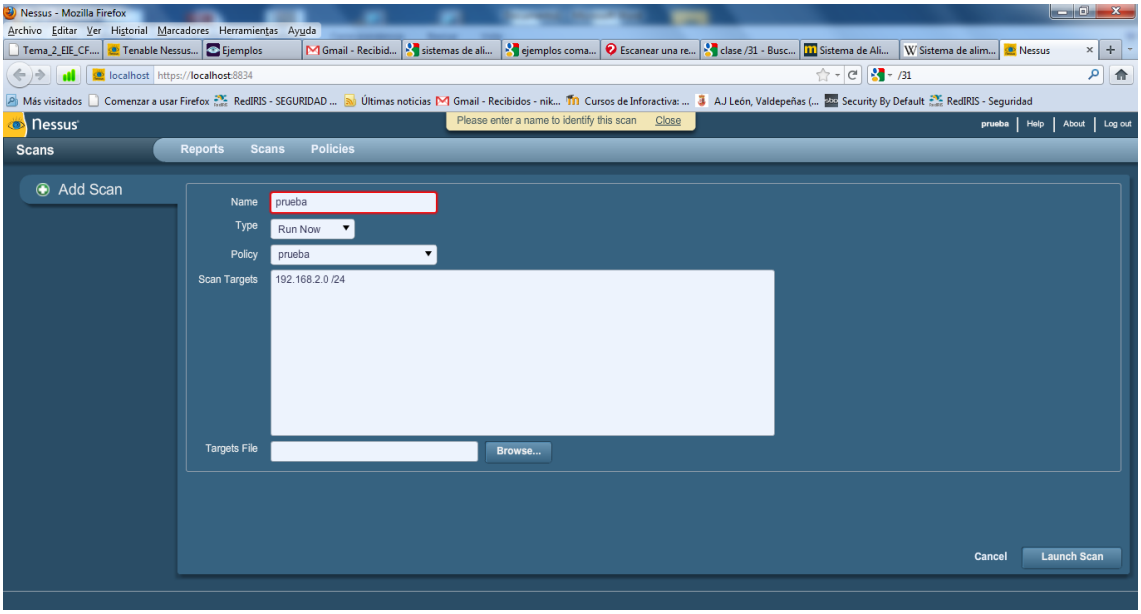
2.- En la pantalla que no aparece deberemos de rellenar en la sección los campos que se muestran en la imagen.



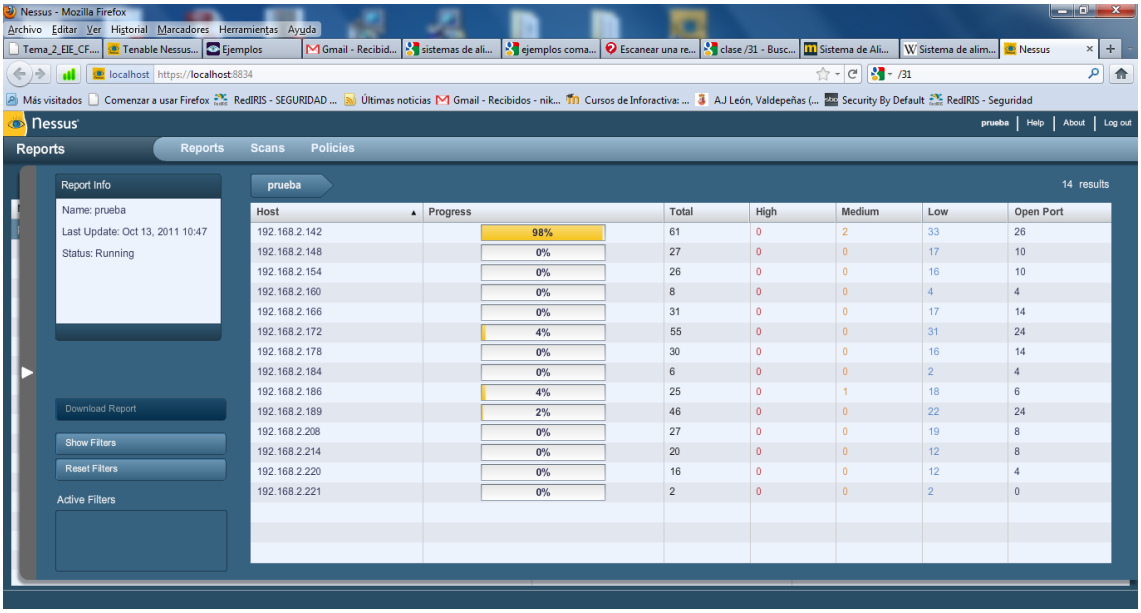
4.- Ahora en la seccion preferences seleccionamos en plugin la opcion Do not scan fragile devices.



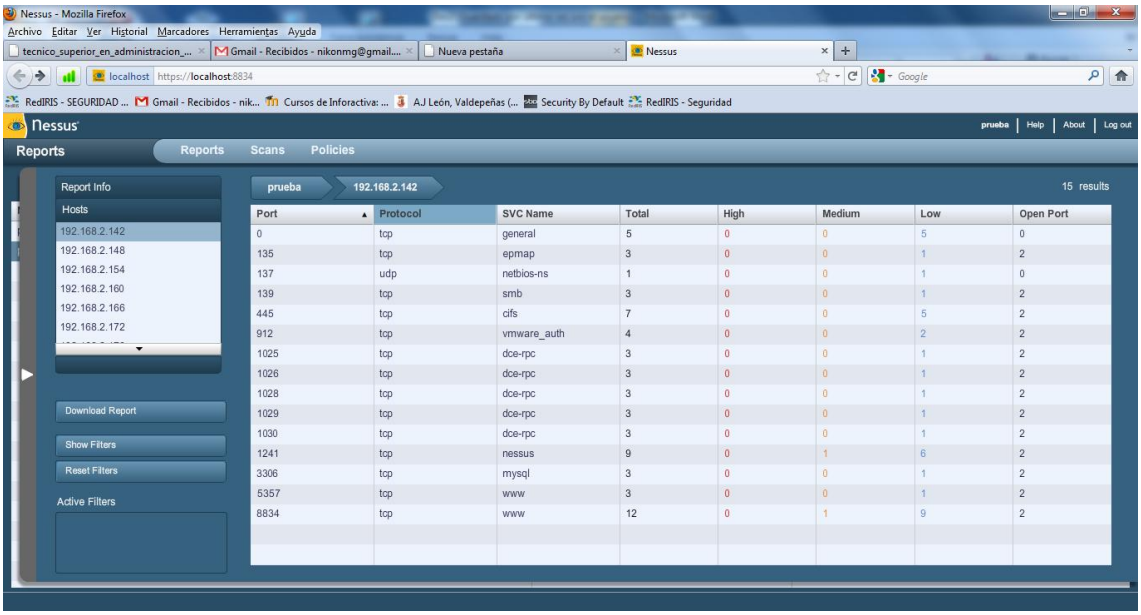
5.- Ahora nos dirigimos a scans seleccionamos el nombre y en scan targets introducimos la direccion que deseamos analizar.



6.-Ahora comenzara el analisis:

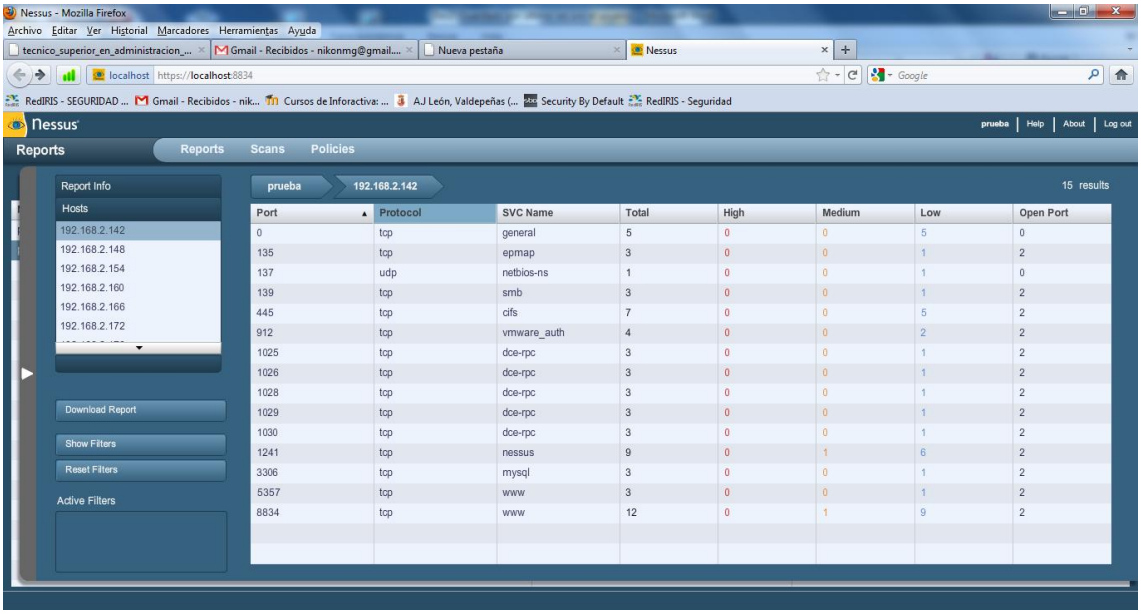


7.- Una vez finalizado podremos ver el análisis especifico de cada ordenador, pudiendo observar sus vulnerabilidades y los puertos que se encuentran abiertos.

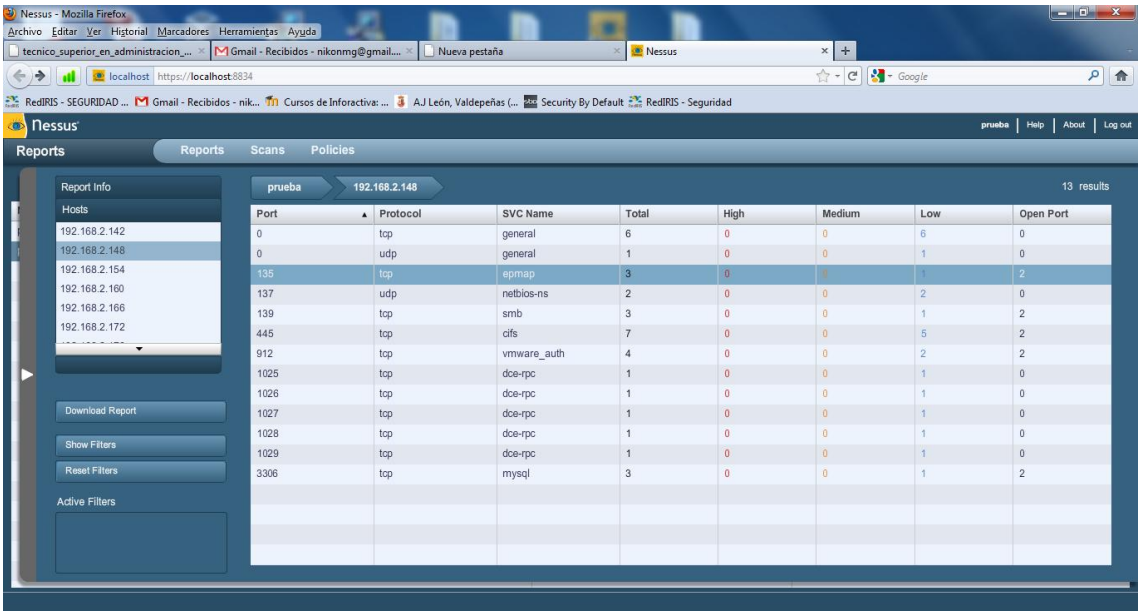


Trabajo análisis vulnerabilidades con Nessus.

En esta imagen podemos ver el análisis de puertos en nuestro ordenador, podemos observar que tenemos abiertos vario puertos entre ellos encontramos el 3306 del mysql, el 912 del wmware…:



En comparación con otro equipo de la red podemos observar los siguientes puertos y vulnerabilidades, en este equipo podemos observar que no tiene los puertos 5357 y 8834 que se corresponde con un servidor web:



5.1.-Jugar al Juego de Seguridad

1.- Ante una amenaza de denegación de servicios en el que nuestros routers de acceso a internet están siendo saturados por un ataque masivo de denegación de servicios. La informacion ni entra ni sale.

Para solucionar esta situación deberemos de usar un firewal; aunque también deberemos de pedir ayuda al proveedor de internet.

2.- Ante un troyano que nos amenzas con tomar el control de un ordenador y propagarse a los servidores centrales para sacar informacion confidencial.

La mejor solución es la implementación de un antivirus siempre y cuando este actualizado e incluya detección de troyanos.

3.- Ante la aparición de un HACK en nuestro sistema o pagina web con el objetivo de conseguir datos confidenciales; la mejor solución son las actualizaciones de software .

4.-Ante la aparición de un antivirus, la mejor solución es la instalación de un antivirus, este antivirus debe de estar actualizado.

5.- Ante un problema de ingeniería social deberemos de usar la protección de procedimientos de seguridad, actualizando las claves del sistema periódicamente, concienciar a los usuarios…

5.2.-Elaborar un resumen del ataque sufrido a IRC Hispano

Este ataque fue provocado por un usuario que fue expulsado de dicho chat. Dicho ataque se produjo mediante la saturación de peticiones por parte de un ordenador cliente, esto provoco la saturación del HUB y en primer lugar provoco que la red y el chat fuese más lento en un segundo ataque el atacante a su vez uso ordenadores zombies para saturar aun más la red, esto provoco que se perdiera la comunicación entre el HUB y el servidor y por tanto inutilizo el chat de IRC Hispano.

5.3.-Amenazas Físicas, noticia

http://www.elmundo.es/elmundo/2010/12/30/paisvasco/1293696305.html

Un incendio causa graves daños en la empresa Iparlat de Urnieta

Un incendio declarado en las instalaciones de la empresa Iparlat de Urnieta (Guipúzcoa) ha causado daños muy graves en la fábrica, han informado los bomberos de San Sebastián y el departamento vasco de Interior.

El fuego, que **no ha causado heridos**, se declaró en la planta de Iparlat en el polígono Erratzu de Urnieta sobre las 22.00 horas de anoche, por causas que se desconocen, y durante más de ocho horas, hasta las seis de esta mañana, los bomberos han estado trabajando para controlar las llamas, que han causado daños graves en la factoría.

El incendio **se ha extendido asimismo a un pabellón de otra empresa** anexo a Iparlat, y ha calcinado también un camión que se encontraba aparcado en el exterior de la empresa lechera.

En el lugar han estado trabajando **cinco dotaciones de bomberos** de San Sebastián, apoyadas por otras unidades del cuerpo de bomberos de Guipúzcoa.

Según han informado los Bomberos de San Sebastián, el incendio comenzó en uno de los pabellones de la empresa **en el que se almacenan las bobinas del material con el que se fabrican los tetrabricks** para la leche.

"Al principio **el mayor problema** era dividir la zona de producción de la nave donde estaba almacenado todo y se consiguió que no se propagase a otros pabellones", han señalado.

Según han detallado, las bobinas que han prendido fuego "están muy comprimidas", lo que conlleva que las tareas de extinción se alarguen "hasta que se enfríe y se apague todo por dentro". Además, los bomberos han explicado que **"el techo se ha caído y es más difícil atacar al núcleo del fuego"**, por lo que "se está echando agua por encima para ir poco a poco apagándolo".

El alcalde de Urnieta, Mikel Izagirre, ha estado presente en la nave durante gran parte de la noche hasta que la situación ha estado controlada.

Por su parte, el diputado general de Gipuzkoa, **Markel Olano**, se ha acercado esta mañana al lugar del siniestro para interesarse por lo sucedido.

5.4.-Noticia Amenaza lógica

http://www.elpais.com/articulo/internet/banda/rusa/infecta/redes/cientos/empresas/EE/UU/elpeputec/20080806elpepunet_4/Tes

Una banda organizada rusa ha infectado cientos de ordenadores de empresas e instituciones manipulando los sistemas de administración de redes, desde los que se gestionan los recursos informáticos de las organizaciones, en un ataque que ha hecho saltar la voz de alarma entre las firmas de seguridad de Estados Unidos.

Los piratas actuaban desde Rusia pero gestionaban el robo de datos personales y contraseñas desde un programa central que controlaba hasta 100.000 ordenadores infectados, y que estaba alojado en un centro de datos de Wisconsin, informa *The New York Times*.

La banda ha sido descubierta gracias a la empresa de seguridad informática SecureWorks, quien alertó a las autoridades federales de Estados Unidos. La banda vió cómo su sistema era bloqueado, pero al poco tiempo, lo reactivaron en un nuevo servidor instalado en Ucrania.

Este caso, presentado durante la feria de seguridad Black Hat que se celebra estos días en Las Vegas, ha hecho saltar las alertas respecto a la vulnerabilidad de las redes corporativas. Este ataque resulta peculiar porque va dirigido contra el software de administración de redes que utilizan las empresas para centralizar la gestión de todos sus ordenadores y con el que se realizan las actualizaciones de todos sus programas. El sistema ha logrado 378.000 infecciones en un plazo de 18 meses.

No es la primera vez que se ataca este tipo de sistemas, pero sí es el primer caso que el ataque logra tal repercusión. El nombre de las empresas afectadas se mantiene en el anonimato puesto que la investigación sigue abierta, pero se sabe que la banda rusa ha llegado a realizar transacciones bancarias gracias a su programa para robar datos, llamado Coreflood.

En algo más de un año los ordenadores infectados por la banda almacenaron 500 gigabytes de información que se acumuló en el centro de Wisconsi, según explica la empresa SecureWorks.

El malware que se utilizaba era capaz de realizar capturas de las pantallas, además de robar contraseñas. Así, los piratas podían ver información más completa, como los cuentas corrientes, sin tener que entrar en la página web del banco.

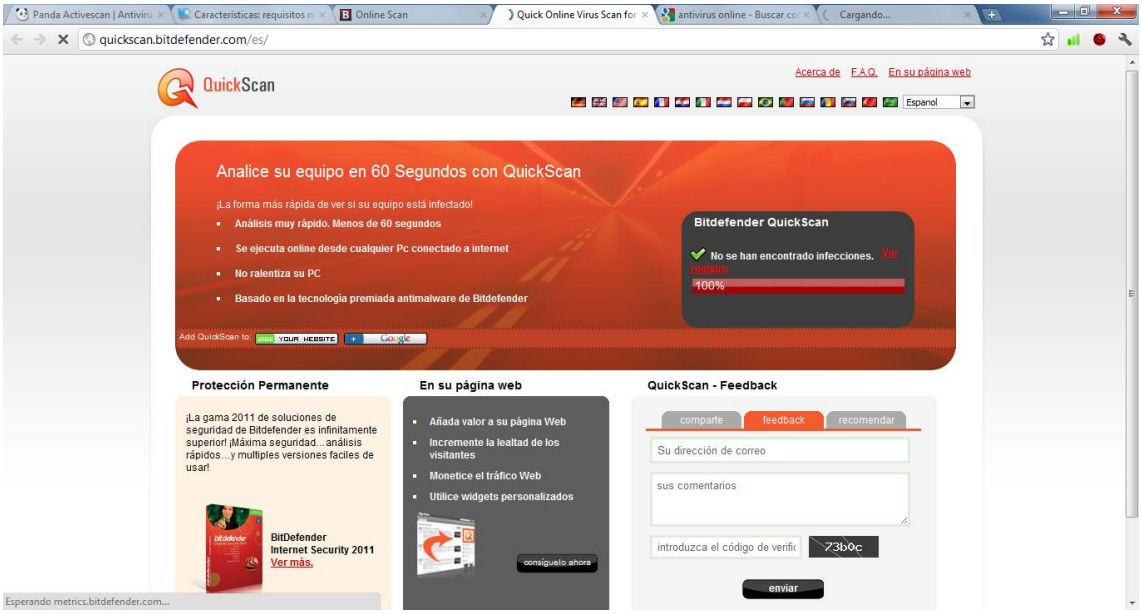
La banda rusa ha estado operando con total impunidad durante años, según el experto que descubrió el fraude, por lo que las firmas de seguridad reunidas en Black Hat , se han mostrado preocupadas ante la falta de atención de las

corporaciones en los casos de infecciones de malware, que permiten que las máquinas pasen a manos de delincuentes organizados.

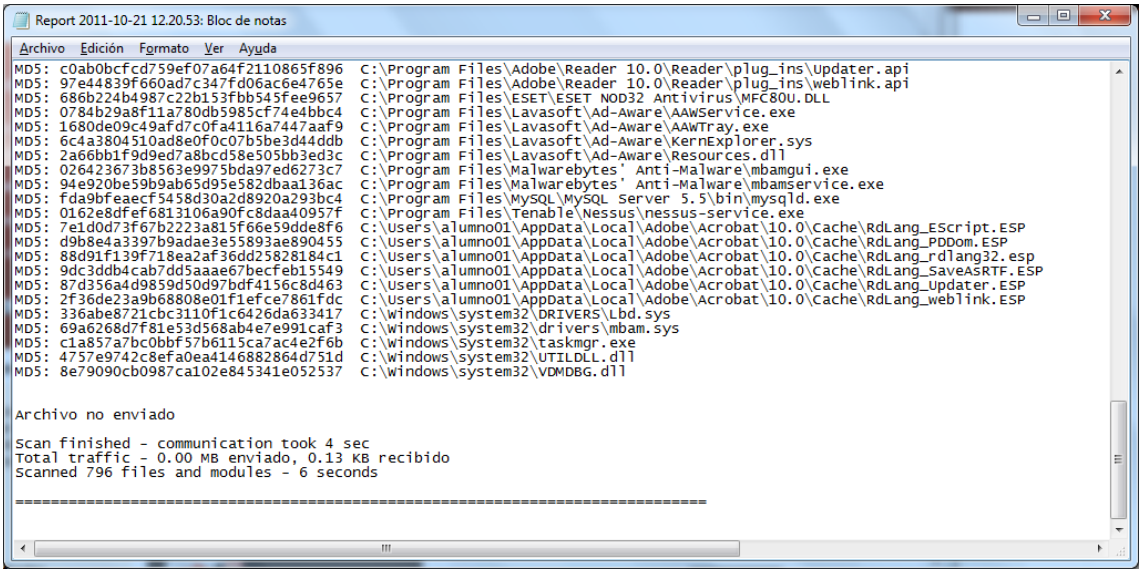
5.6.-Antivirus online

Usaremos el nod32 y el bitdefender

Para usar Bitdefender deberemos de dirigirnos a esta pagina web y pulsar sobre http://quickscan.bitdefender.com/es/ iniciar analisis



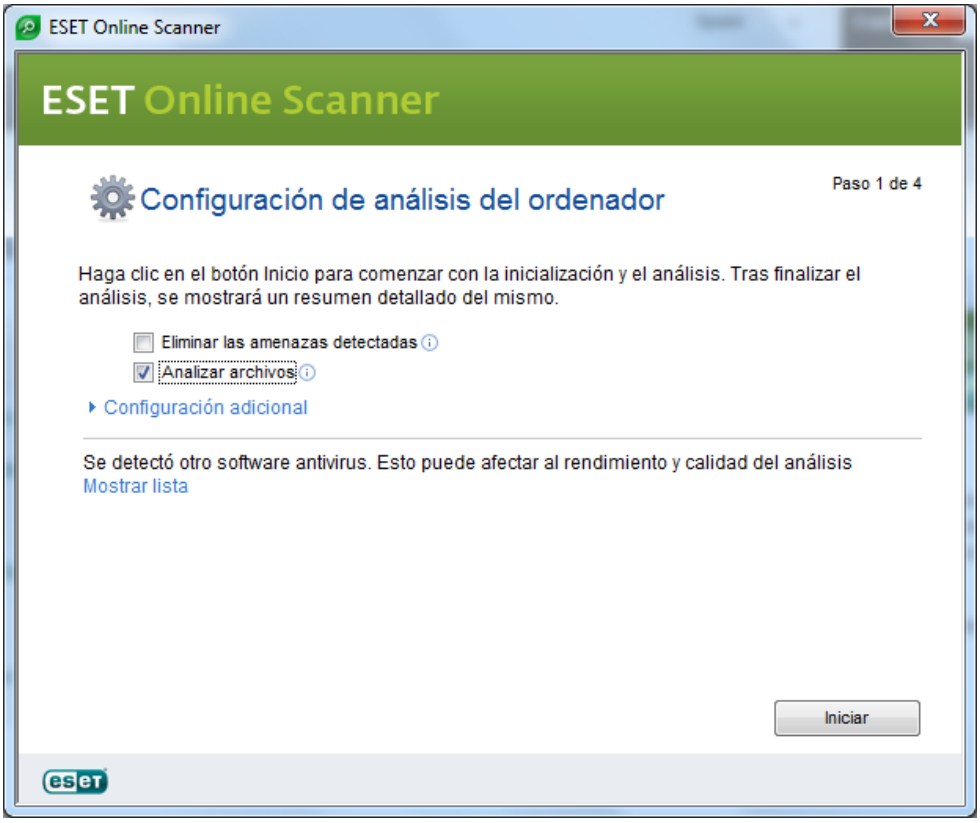
Una vez finalizados nos aparecerá un log con los resultados del análisis:



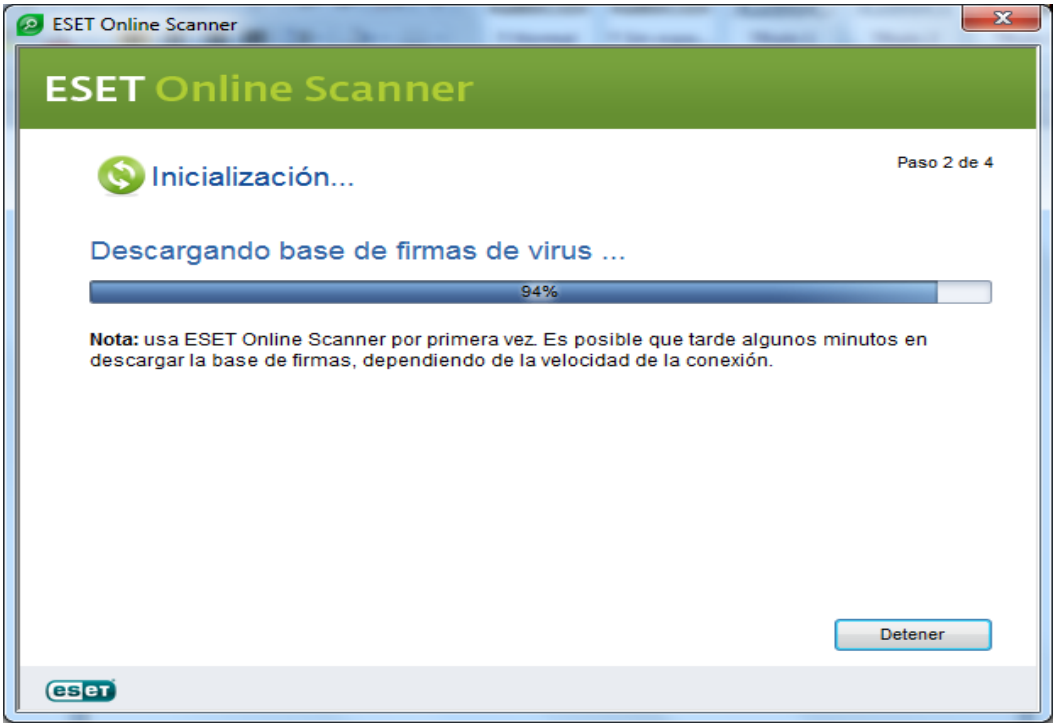
ESET

En primer lugar deberemos de dirigirnos a http://www.eset-la.com/online-scanner y pulsar sobre la opción iniciar análisis.

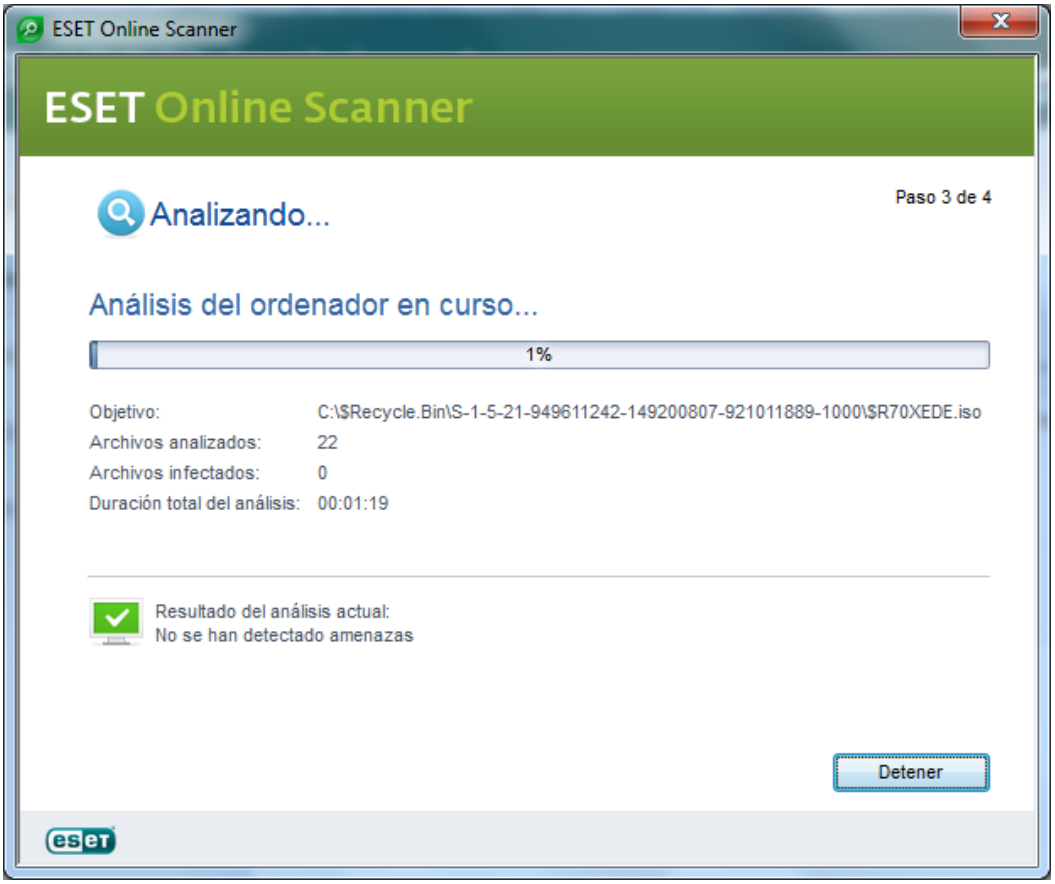
En las opciones del escáner seleccionamos Analizar archivos y pulsamos sobre iniciar



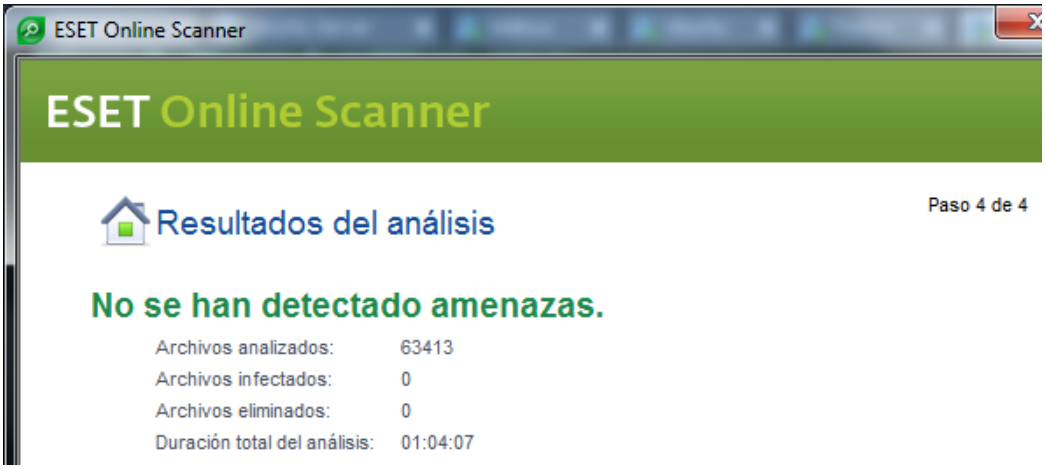
Antes del análisis El antivirus online se debe bajar la base de firmas:



Una vez descargada la bases de firmas dara comienzo el análisis:



Una vez finalizado podremos ver los resultados del analisis



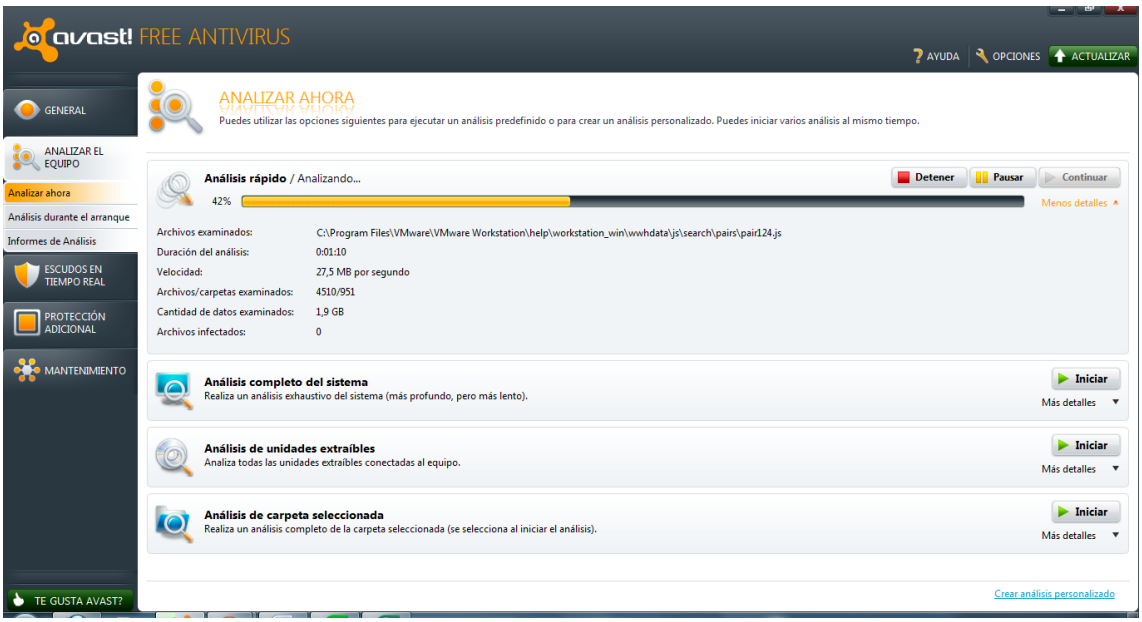
Comparación de los 2 antivirus online:

Antivirus online analizados	Archivos analizados	% CPU	Opciones de escaneo	tiempo de escaneo	Vulnerabilidades	virus encontrados	Desinfectados
Bitdefender	791	40	Estándar	6 segun.	0	0	0
NOd 32	63413	45	Estándar	1 hora y 4minutos	0	0	0

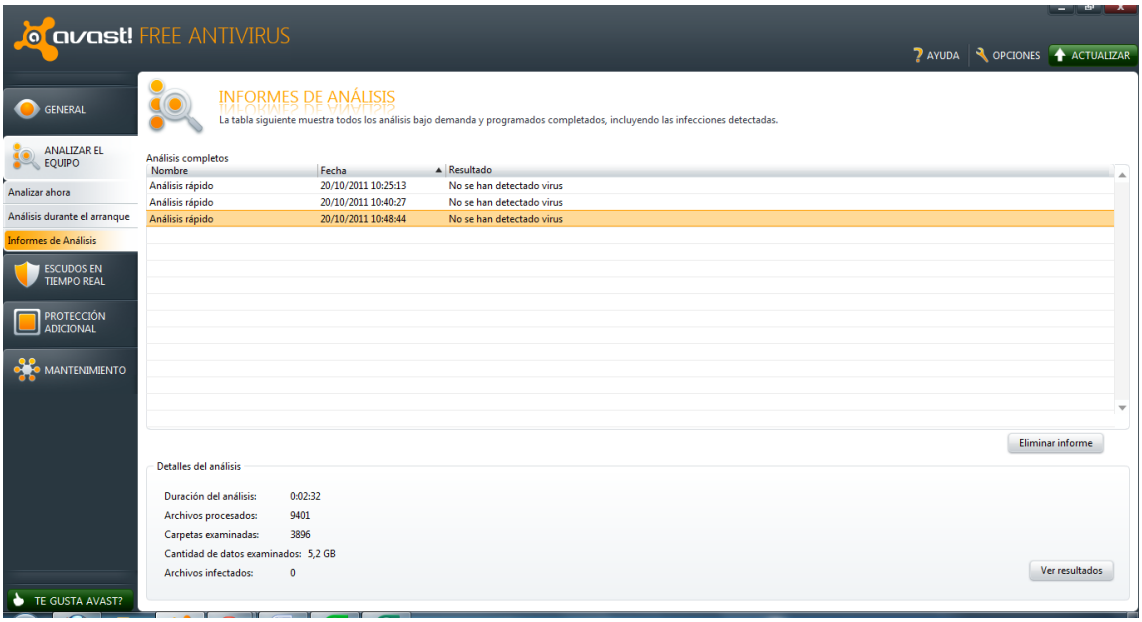
5.7.-ANTIVIRUS LOCALES

Usaremos el avast y nod 32 para analizar nuestro sistema**AVAST**

Una vez instalado seleccionamos la opción analizar ahora y elegimos el análisis rápido:

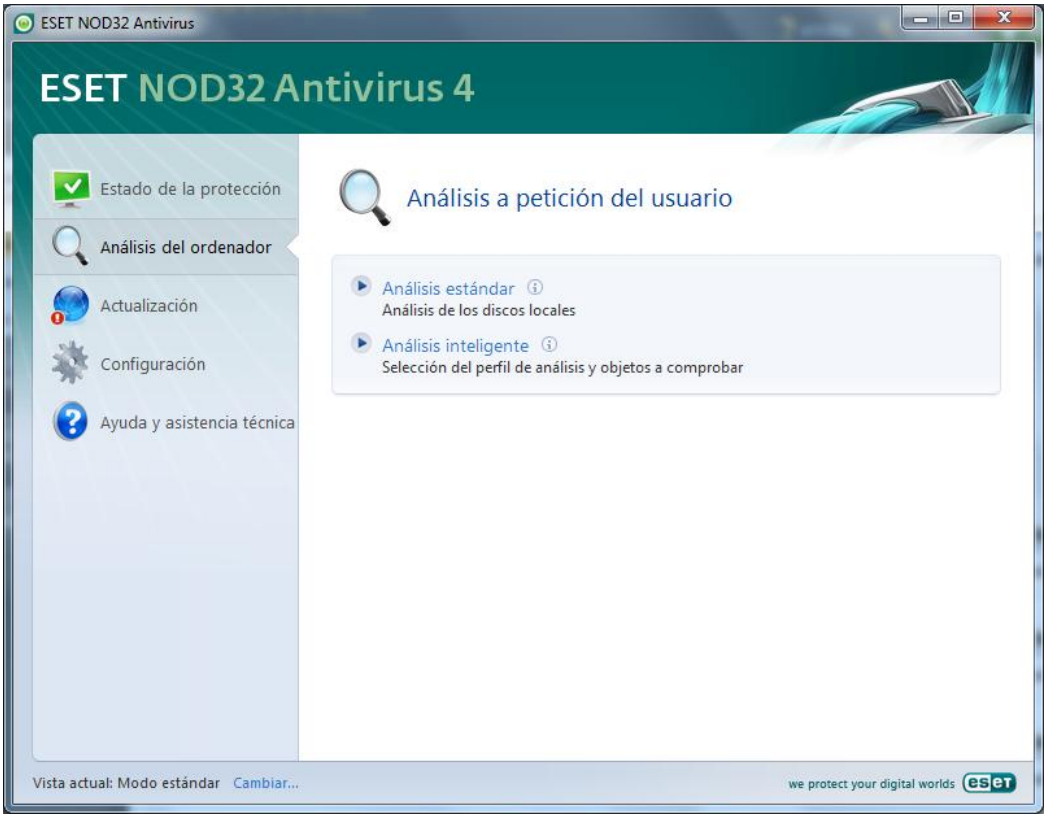


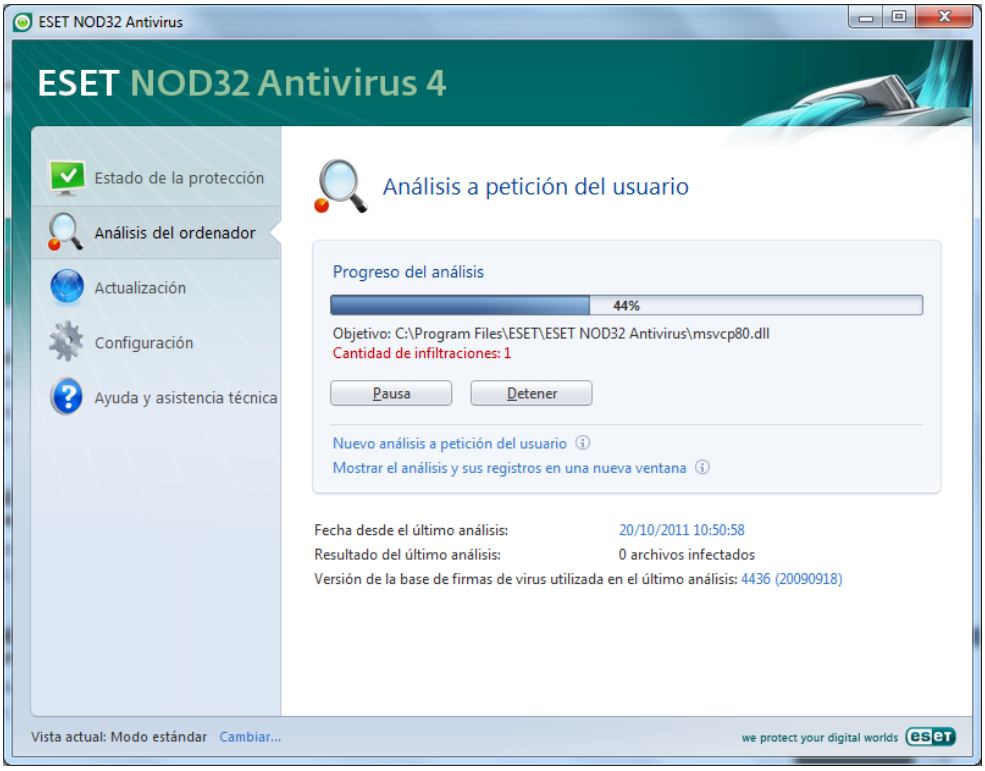
Una vez finalizado podremos ver los resultados del análisis:



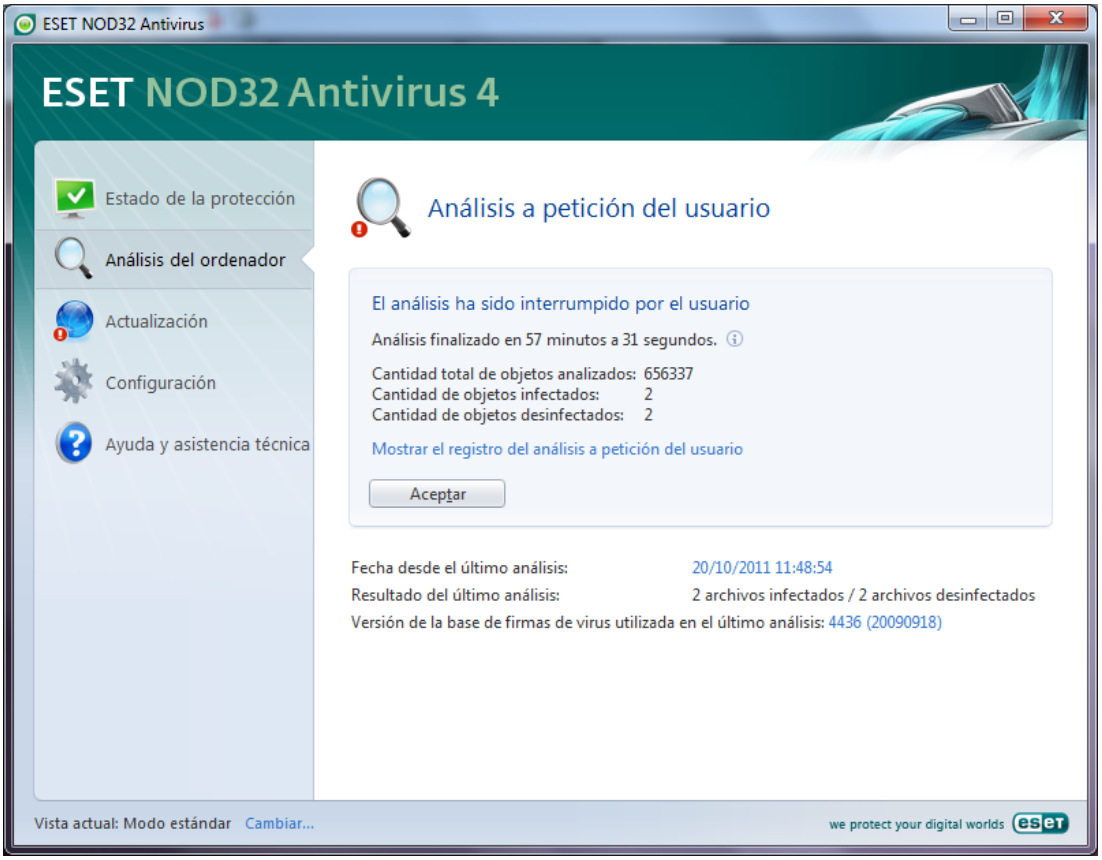
NOD32

En primer lugar nos dirigiremos a la pestaña análisis del ordenador y seleccionamos la opción análisis estándar para que el análisis de comienzo.





Una vez acabado podremos ver los resultados del análisis:



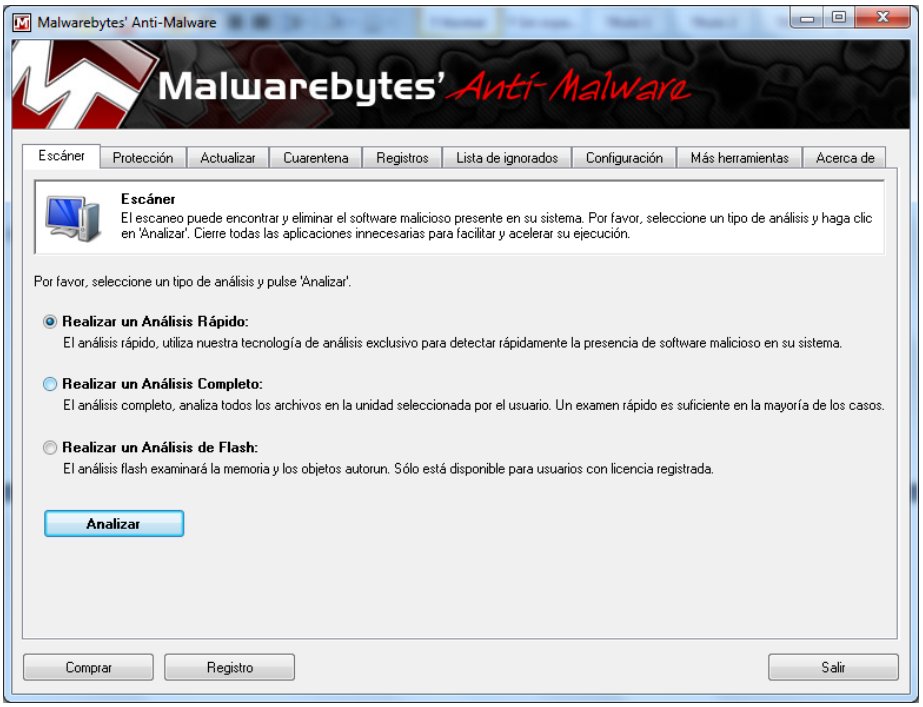
Comparación del análisis efectuado con el avast y con el NOD 32.

Antivirus analizados	Archivos analizados	% CPU	Opciones de escaneo	tiempo de escaneo	Vulnerabilidades	virus encontrados	Desinfectados
Avast	9401	40	Rápido	2 min	0	0	0
NOd 32	656337	50	Estándar	57 min y 37 según	2	2	2

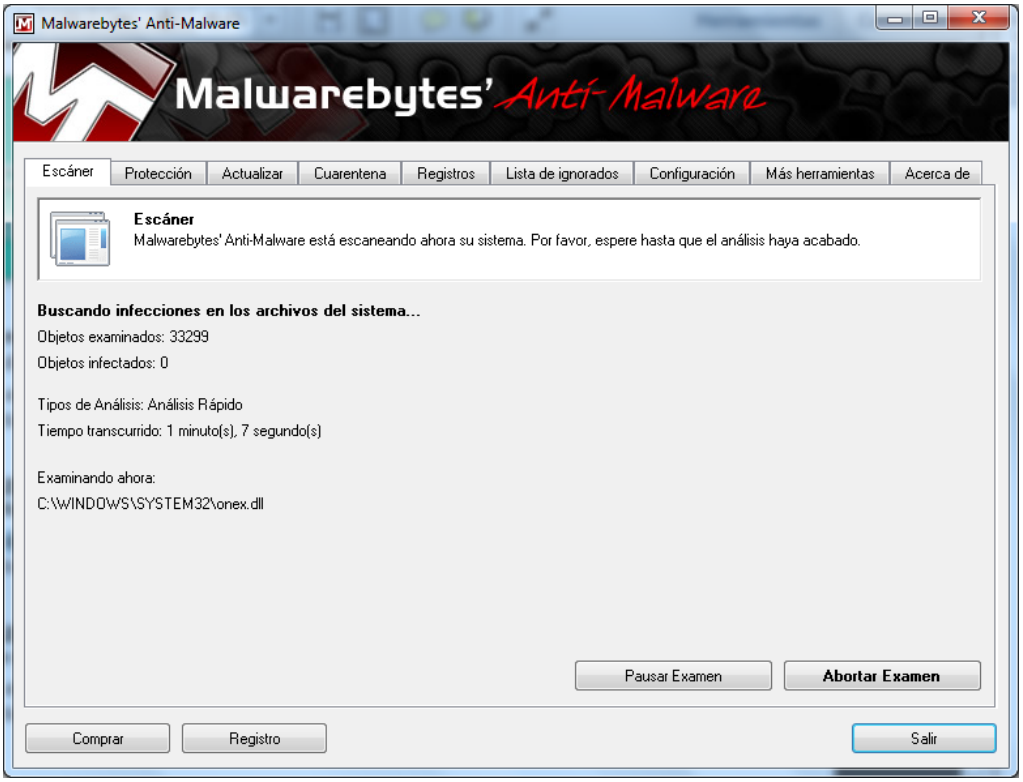
6.7.-Aplicaciones ANTI MALWARE

Usaremos el malwarebytes anti- malware y el ad-ware

1.-Una vez instalado el el malwarebytes anti- malware en la pestaña éscaner seleccionamos realizar análisis rápido.



Una vez finalizado el análisis podremos observar los resultados del análisis:



AD-WARE

Una vez instalado el Ad- ware pulsamos sobre la opción análisis inteligente para que de comienzo el análisis del sistema:

Una vez finalizado el proceso podremos ver el resultado del análisis:

Antimalware analizados	Archivos analizados	% CPU	Opciones de escaneo	tiempo de escaneo	Vulnerabilidades	virus encontrados	Desinfectados
Malwarebytes	16012	40	Inteligente	5 min	8	8	7
Ad-Ware	656337	50	Rápido	2 min	0	0	0

6.1-Seguridad física y ambiental:

a) Se necesita realizar **un estudio de la ubicación y protección física de los equipos y servidores del aula,** desde el punto de vista de:
a) Acondicionamiento físico (Extintores, Sistema de aire acondicionado, Generadores eléctricos autónomos, racks)

b) Robo o sabotaje: Control de acceso físico y vigilancia mediante personal y circuitos cerrados de televisión (CCTV).

c) Condiciones atmosféricas y naturales adversas.

Análisis previo de la seguridad en nuestra aula

En nuestra clase podemos encontrar varias debilidades, tanto lógicas como físicas, en nuestro caso nos centraremos en las amenazas físicas. Las principales amenazas que encontramos son:

La seguridad que encontramos para acceder al aula puesto que se utiliza una llave única para acceder a todas las aulas del centro.

En segundo lugar en nuestra aula no encontramos ningún extintor ni ningún aparato de aire acondicionado.

En último lugar debemos de destacar que en nuestra aula si se produce un fallo de suministro eléctrico los sistemas informáticos en funcionamiento se apagaran pudiendo estropearse, para evitar esta situación deberemos de usar SAIS o generadores.

Estudio sobre las medidas de seguridad que se deben adoptar en nuestra aula

En nuestra aula para poder garantizar la seguridad física de nuestros equipos debemos de abarcar la seguridad desde varios puntos de vistas:

1.-En primer lugar llevaremos a cabo un estudio sobre **el acondicionamiento físico**. Para llevar a cabo el acondicionamiento físico de nuestra aula deberemos de contar con los siguientes productos:

En primer lugar deberemos de tener extintores:

En nuestro caso elegiremos el modelo de extintor que podemos apreciar en la imagen; por el tamaño de nuestra aula con uno tendremos suficiente.

SH-SC 0610101 - EXTINTOR 1 KG

Ante un incendio, por pequeño que sea, hay que reaccionar rápidamente. Tener un extintor en un lugar fácilmente accesible es indispensable.

También deberemos de tener un sistema de aire acondicionado para asegurarnos de mantener una temperatura óptima en nuestros equipos (que no sea ni muy alta, ni muy baja), en nuestro caso hemos elegido el modelo que apreciamos en la imagen; por el tamaño de nuestra aula con un sistema de aire acondicionado tendremos suficiente:

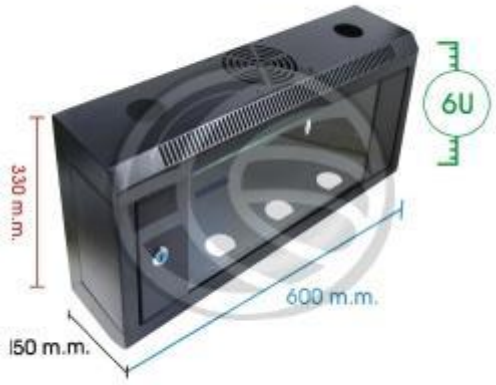
AIRE ACONDICIONADO DELONGHI INU CKP30EB'05

También deberemos de disponer de Generadores eléctricos autónomos para asegurarnos una corriente eléctrica continua en nuestra aula, es decir a prueba de fallos eléctricos. Puesto que cuando la corriente eléctrica falle se pondrá en marcha el generador y así nuestros equipos podrán seguir funcionando. En nuestro caso hemos elegido el generador que vemos en la imagen:

Generador Diesel TG6500-3 220v-380v Insonorizado Taigüer

Por último en el apartado de acondicionamiento físico también deberemos de usar armarios rack para agrupar nuestros router y switch y mantenerlos guardados bajo llave y de una manera más organizada. En nuestro caso hemos decidido usar el modelo de la imagen:

Armario rack de 19 RackMatic SOHORack mini de 6U y fondo 150



2.-En segundo lugar también debemos tener en **cuenta la seguridad desde el punto de vista de Robos o sabotajes…..**Para evitar estas situaciones deberemos de implementar las siguientes opciones:

En primer lugar deberemos de implementar medios de seguridad de control de acceso físico (en este punto también desarrollaremos el apartado **e) Ampliar el estudio realizado del apartado a) del aula con la implantación de sistemas biométricos**)

En primer lugar usaremos el **Lector automático de Matriculas CLPR-W-ACR** ; pudiendo así controlar el acceso no autorizado a nuestra aula puesto que toda persona que quiera entrar en nuestra aula deberá de tener una matrícula que le permita entrar.

Las tarjetas que usaremos para este lector serán **Tarjeta de banda magnética HiCo/LoCo** , Las tarjetas de banda magnética ofrecen diversidad de utilidades que no requieran de un nivel de seguridad muy elevado a un coste reducido.

Para mayor seguridad implementaremos el **Emisor Biométrico GO-BIO** que es Emisor biometrico de activación mediante huella digital para usos de alta seguridad en la puerta de nuestra aula para evitar el acceso no autorizado.

También usaremos el **Terminal de reconocimiento facial 3D Hanvon Face ID** para aumentar la seguridad de acceso a nuestra aula. La doble cámara permite un reconocimiento biométrico facial 3D de seguridad usando luz visible e infrarroja. Tecnología biométrica sin contacto seguro y rápido.

Otra opción **es contratar a vigilantes** para realizar tareas de supervisión de la seguridad física.

Por último también deberemos de **proporcionar seguridad mediante circuitos cerrados de televisión (CCTV)** para tener videovigilada nuestra aula en todo momento. Los sistemas de CCTV o videovigilancia permite la visualización remota de las cámaras en cualquier momento.

Los productos elegidos para nuestra empresa son:

Una **Cámara Domo SCC-B5003P** que nos permitirá grabar la actividad de nuestra aula tanto de día como de noche

Necesitaremos un grabador DVR para poder grabar todo lo que nuestras cámaras vayan grabando en nuestro caso hemos elegido el producto **Video Gravador Digital HIK Vision**

3.-Por último deberemos de realizar un **estudio sobre Condiciones atmosféricas y naturales adversas.**
En primer lugar nos centraremos en la ubicación del sistema en nuestra aula, en nuestro caso tendremos los router y switch guardados bajo llave en un amario rack.

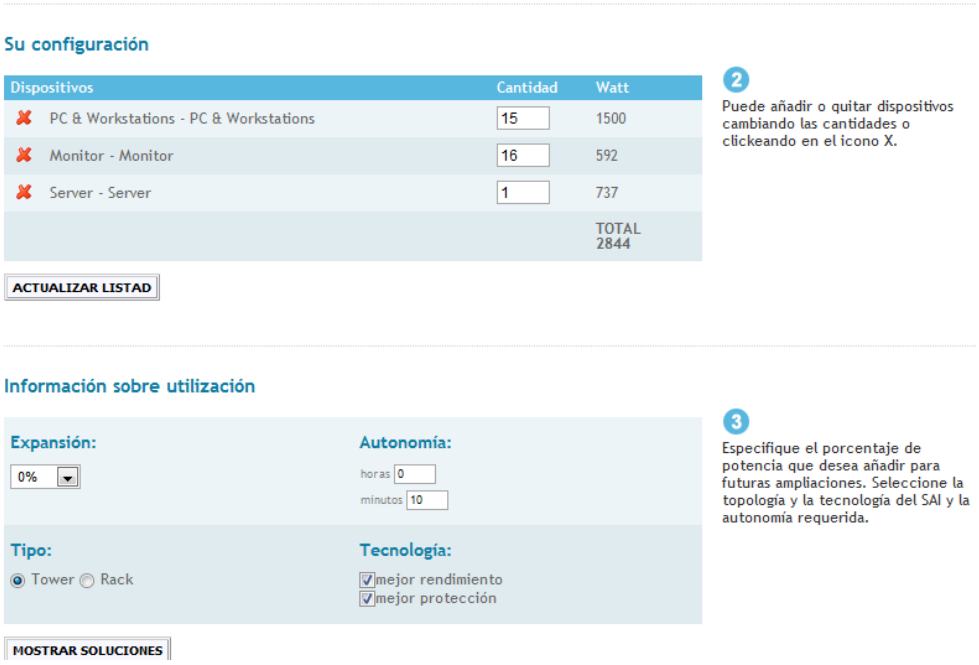
En cuanto a la protección de los datos deberemos de guardar las copias de respaldo de los sistemas en una ubicación física diferente a la del aula donde se encuentra nuestro equipo informático evitando así las vulnerabilidades ante ataques físicos.

CONCLUSIÓN

Una vez realizado el estudio de las medidas que se deben de implementar en nuestra aula para que esta sea segura llegamos a la conclusión de que nuestra aula carece prácticamente de cualquier medida de seguridad física. Por lo tanto se deberían de implementar la mayoría de las medidas de seguridad propuestas en el informe; de esta forma nuestra aula tendrá unas ciertas medidas de seguridad que nos protegerá de los principales ataques físicos que se pueden producir en nuestra aula.

6.2.-Busca un único SAI para todos los sistemas informáticos del aula.

En primer lugar deberemos de realizar un calculo energético de nuestra aula; para ello nos dirigimos a esta página web: http://www.riello-ups.com/?es/configuratore y seguimos los pasos que nos aparecen en pantalla. Una vez realizado nuestro análisis observaremos la siguiente conclusión, En nuestro caso se estima un consumo de 2844 W:



Ahora deberemos de pulsar sobre mostrar soluciones para que nos muestre sugerencias sobre los SAID que nos pueden interesar. En mi caso me ha recomendado el siguiente SAID, que tiene una autonomía de 17 minutos:

Mejor inversión

Sentinel Dual (High Power) - SDL

SDL 8000

Tecnología:
Puissance: 6400W / 8000VA

Autonomía: 17 min
% máximo de utilización: **44%**

Ir a ficha de producto

Características

• posibilidad de instalación en suelo (versión torre) o en armario (versión rack) simplemente extrayendo y rotando el sinóptico (con la llave suministrada)
• tensión filtrada, estabilizada y fiable (tecnología On Line a doble conversión (VFI según normativa EN50091-3) con filtros para la supresión de las perturbaciones atmosféricas
• Nivel de ruido audible muy reducido (<40dBA): permite la instalación sobre cualquier ambiente gracias al control digital PWM del sistema de ventilación dependiendo de la carga aplicada y del uso de la tecnología de alta frecuencia de conmutación en el inversor (>20kHz, valor superior al umbral audible)
• posibilidad de conexión a by-pass externo de mantenimiento con conmutación sin interrupciones (modelos DLD500-600)
• El usuario puede seleccionar los siguientes modos de funcionamiento:
–Active Mode para aumentar el rendimiento (hasta el 98%)
– Economy Mode: permite seleccionar la tecnología Line Interactive (VI), solo se trabaja con el inversor en caso de fluctuaciones de la red, alimentar la carga directamente, para cargas poco sensibles. La función es programable mediante software o planteada manualmente desde el SAI
– Smart Active: El SAI decide de manera autónoma la modalidad de funcionamiento (VI ó VFI) en base a la calidad de la red
– Relevador: El SAI puede ser seleccionado para funcionar solo con la red ausente (modalidad
aconsejada para luces de emergencia)
• conversión de frecuencia 50 o 60 Hz
• tensión de salida seleccionable (220-230-240V) monofase o (380-400-415)

trifase
• auto encendido al retorno de la red, programable desde el panel manual o mediante software PowerShield³
• auto apagado cuando no hay presencia de cargas conectadas
• by-pass activado, cuando se apaga el SAI se predispone automáticamente el funcionamiento a través de by-pass
• pre-alarma de fin de descarga de batería
• permite la programación de un tiempo de demora (delay), tras el encendido
• tensión filtrada, estabilizada y segura (tecnología On Line doble conversión (VFI según normativa
EN50091-3) con filtros EMI para la supresión de las perturbaciones atmosféricas
• en los modelos de 5 y 6 kVA además es posible programar dos tomas de salida de 10A (función
Power-Share) en casos de ausencia de la alimentación de red

Como esta solución satisface nuestros requerimientos será el elegido para satisfacer las necesidades de nuestra aula.

SOLUCIÓN UTILIZANDO VARIOS MODELOS DE SAID

Sin embargo si no queremos tener un único SAID también podremos usar la siguiente solución:

Back-UPS

APC Back-UPS 350, 230V

APC Back-UPS, 210 Watts / 350 VA, Entrada 230V / Salida 230V , Interface Port USB
Incluye: CD con software, Documentación en CD, Ctd. 1 - Cable de alimentación desconectable IEC de 1,2 m, Ctd. 1 - Cable de alimentación desconectable IEC de 1,8 m, Cable de teléfono, US-Bolt, Tarjeta de garantía
Tiempo de Conducción Estándar: Generalmente en existencias

Además de este SAID deberemos de tener otro para que se satisfagan nuestras necesidades, el segundo SAID tendrá una autonomía de 8 minutos:

Back-UPS

APC Back-UPS 500 Structured Wiring UPS, 230V

APC Back-UPS, 300 Watts / 500 VA, Entrada 230V / Salida 230V
Incluye: Cable Ethernet de cat. 6, CD con software, Guía de instalación, Manual del Usuario
Tiempo de Conducción Estándar: Generalmente en existencias

Una vez elegidos los 2 tipos de SAID que usaremos en nuestra aula deberemos de realizar un cálculo energético para saber el número de SAID que deberemos de tener en nuestra aula para asegurar nuestros equipos.

Una vez realizado los cálculos, para alcanzar los 2844 W necesarios deberemos de tener 10 SAID como los 2 modelos anteriores para satisfacer nuestras necesidades.

CONCLUSIÓN

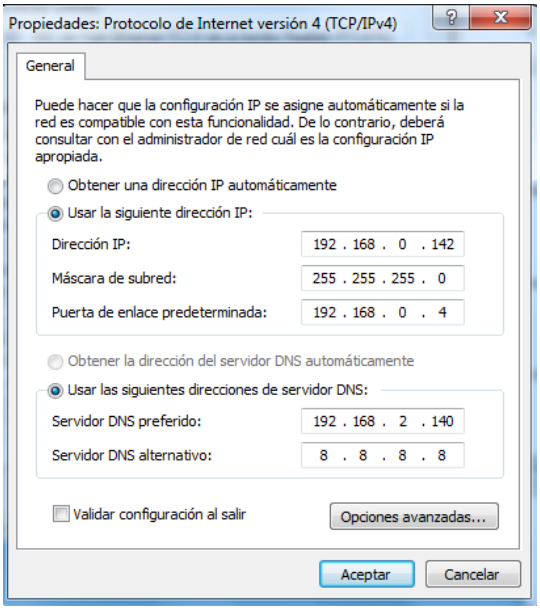
Como conclusión en mi opinión la mejor opción es la de elegir un SAID único ya que su tiempo de carga es mayor y ocupara menos espacio que los 10 SAID que deberemos de tener si elegimos la segunda opción.

c) Instalación de una cámara IP y transmisión de la imagen por una red LAN.

Instalación de una cámara ip

Pasos previos:

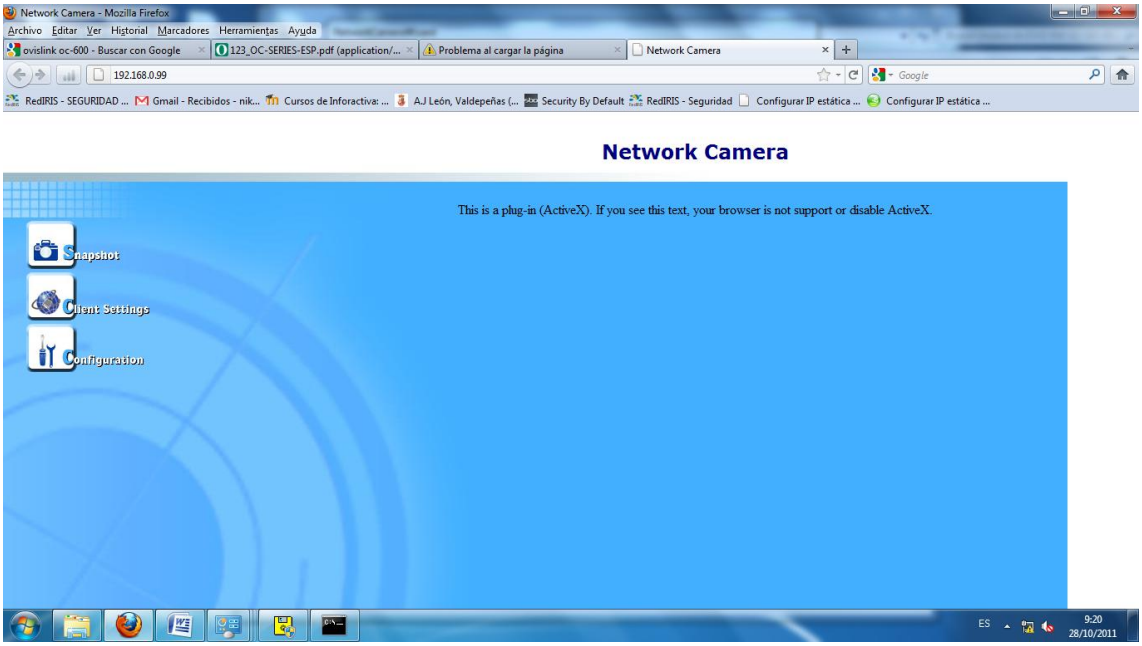
En primer lugar deberemos de tener en cuenta que nuestra cámara IP tiene un dirección 192.168.0.9, por lo tanto en primer lugar deberemos de configurar la IP de nuestro equipo con la dirección IP 192.168.0.142.



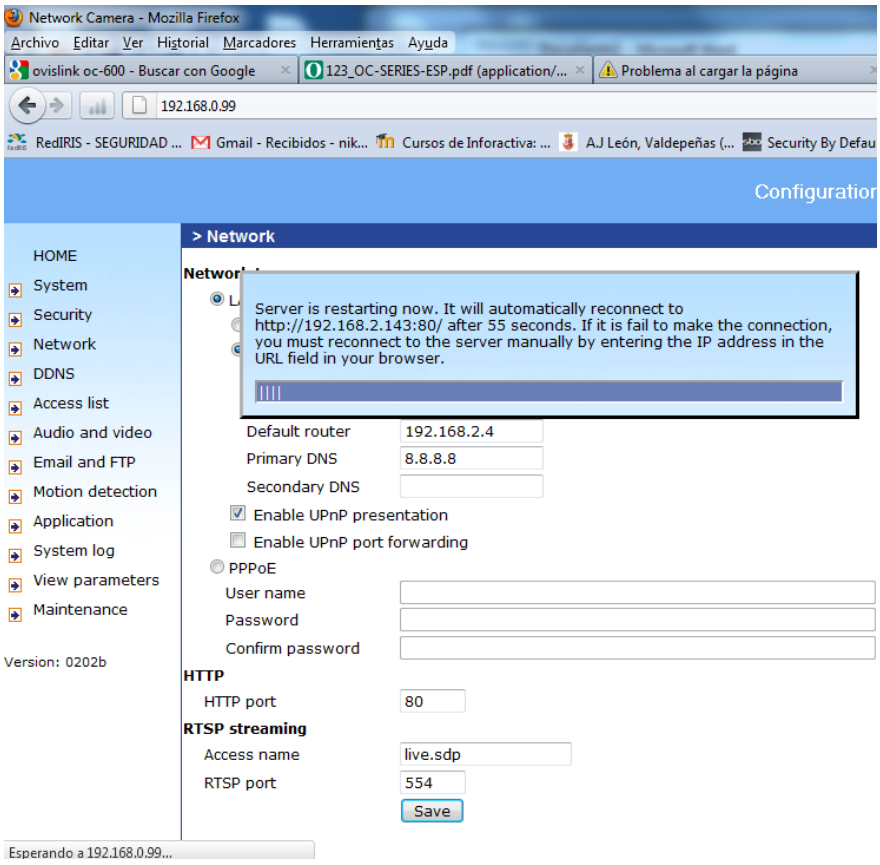
Proceso de Instalación.

1.- En primer lugar para instalar la cámara IP probamos con el software que viene en el CD adjunto pero al no ser compatible con Windows 7 no pudimos realizar la instalación de la cámara de esta forma.

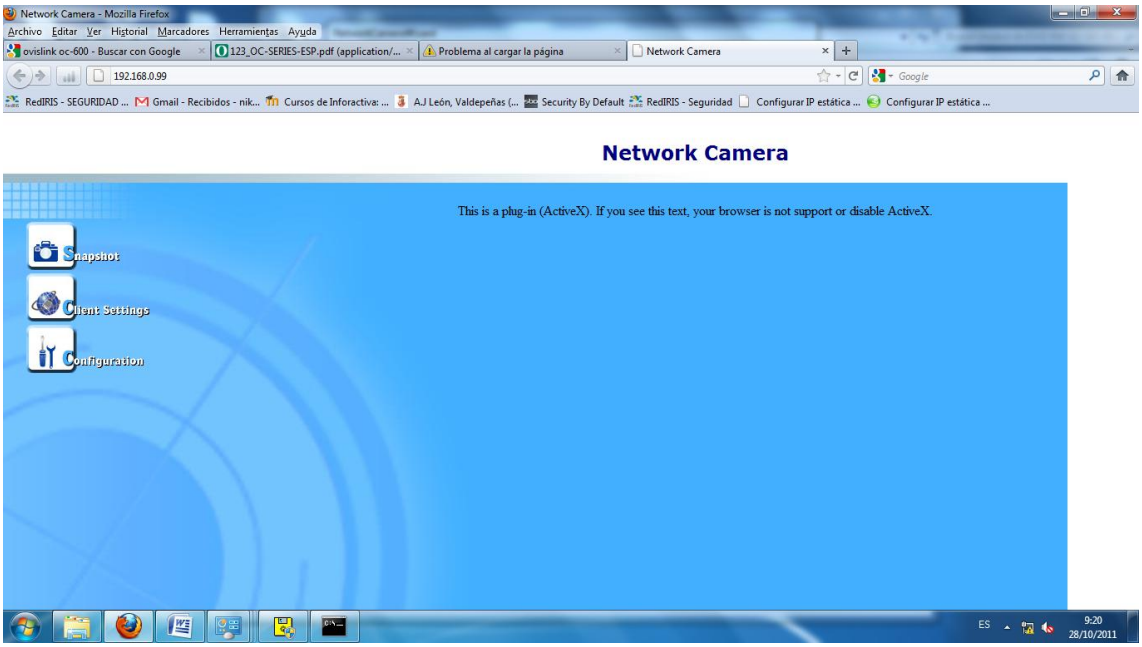
2.-Ahora en el navegador introducimos la dirección 192.168.0.99 y en la pantalla que nos aparece pulsamos sobre la opción configuration:



3.-En segundo lugar nos dirigimos a la sección network y configuramos los parámetros de red deseados, en nuestro caso configuraremos la ip, la puerta de enlace y los DNS para poder conectarla a la red de la clase:

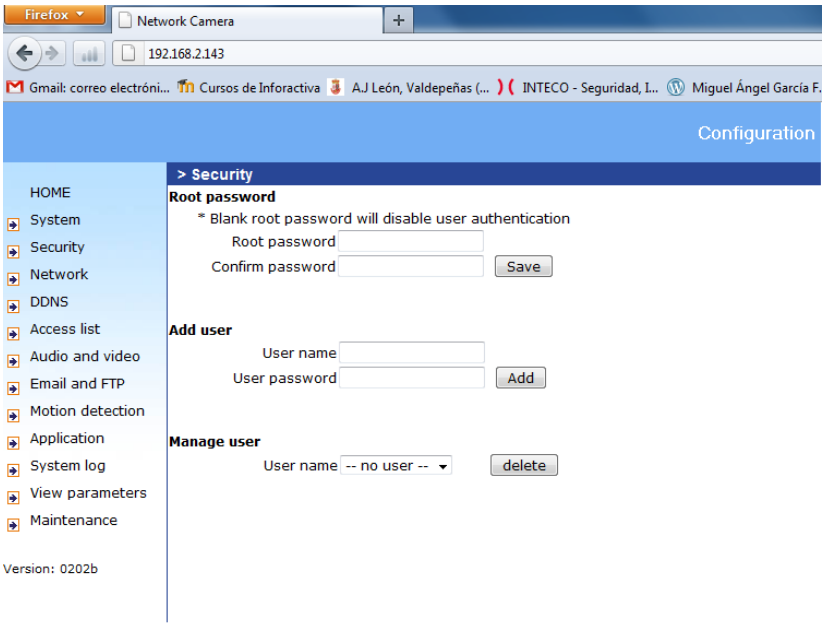


Una vez hecho esto para realizar una fotografía nos dirigimos a la dirección 192.168.099 y pulsamos sobre sbapshoot.

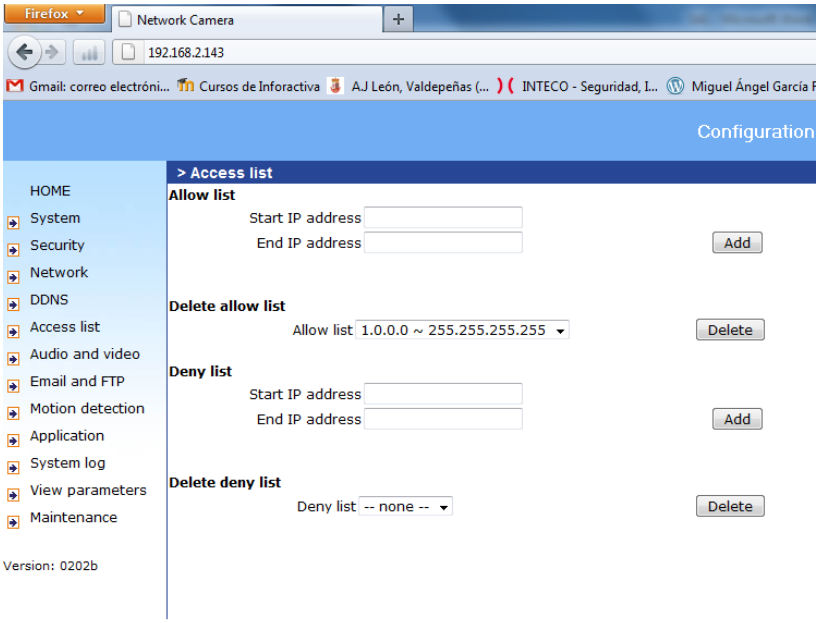


Otras opciones interesantes:

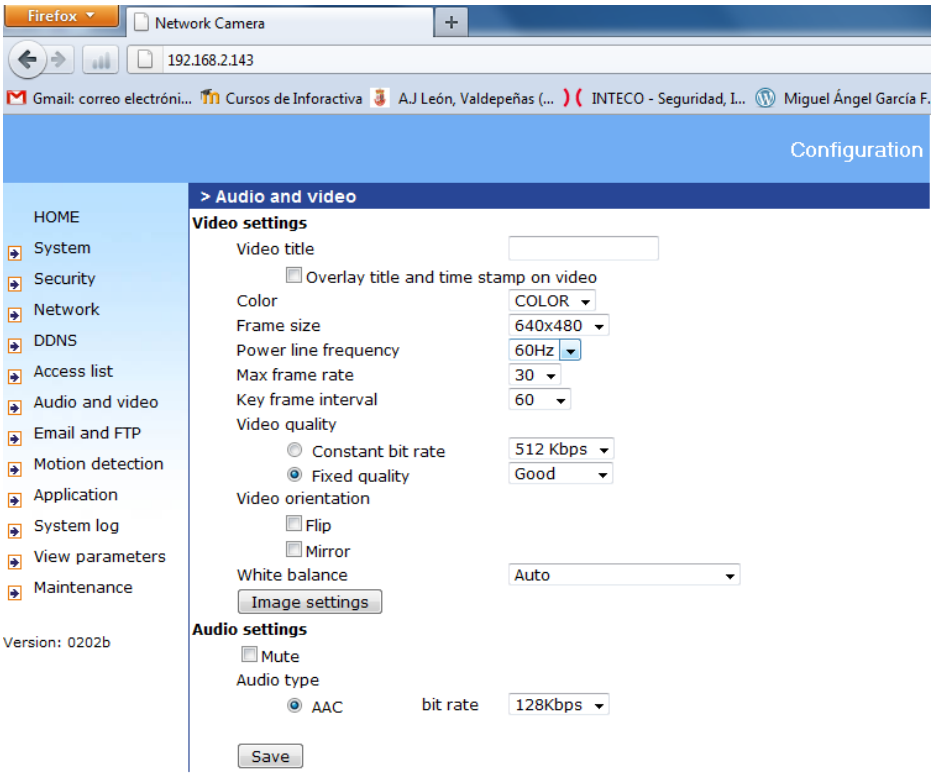
En la sección security podremos establecer parámetros como la contraseña del usuario root y añadir usuarios:



En acces list nos permitirá configurar listas de acceso, para permitir o denegar el acceso a esta cámara IP a unos host determinados en estas listas de acceso



Por último en la sección audio y video y introducimos los parámetros que deseemos.



Aquí ponemos las fotos que hechamos con la cámara ip:

Segunda cámara IP manual

Modelo elegido: El modelo elegido es una Panasonic BL-C131 para la configuración del mismo deberemos de instalar un programa específico que viene incluido en un CD con la cámara IP.

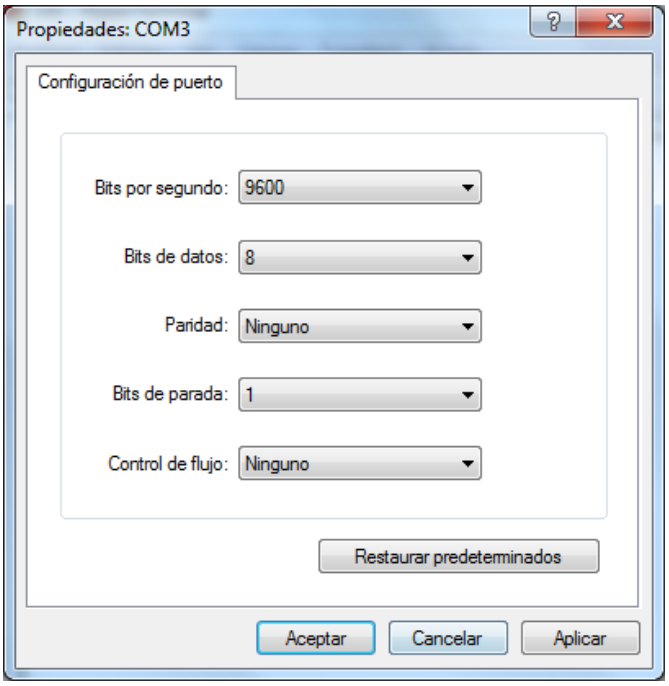
Manual de la cámara:

http://www.jiaying.com/support/panasonic/ip_cam_guides/C111_131/C111_C131_SG-en.pdf

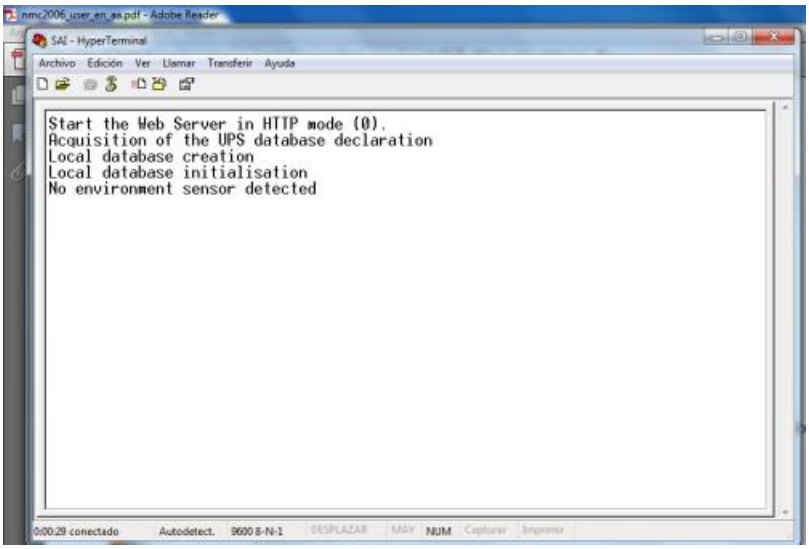
Configuración de SAI UPS SYSTEM Evolution 650

Instalamos el driver del adaptador de puerto serie y el hyperterminal.

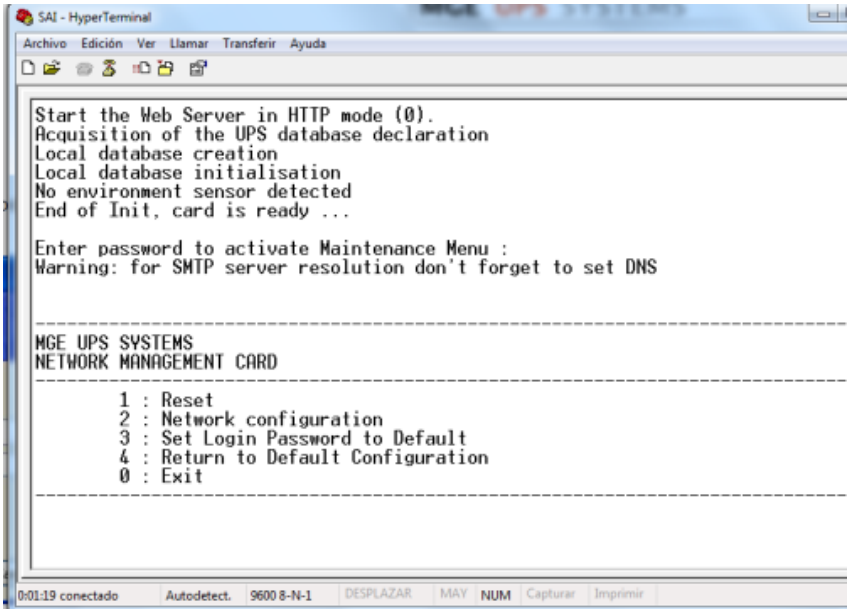
Arrancamos el hyperterminal, en el puerto COM3 con los siguientes parámetros:



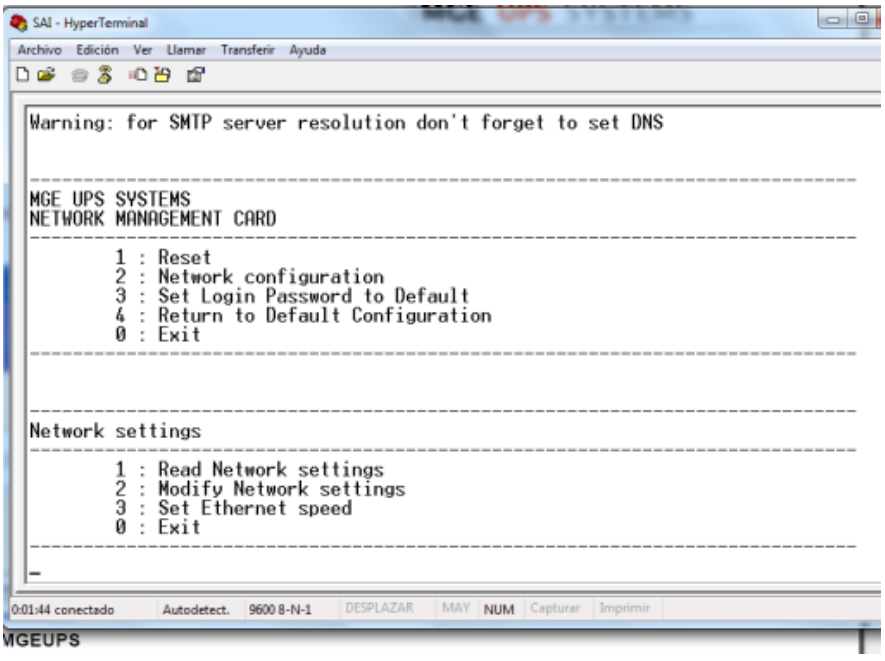
Esperamos a que conecte con el dispositivo.



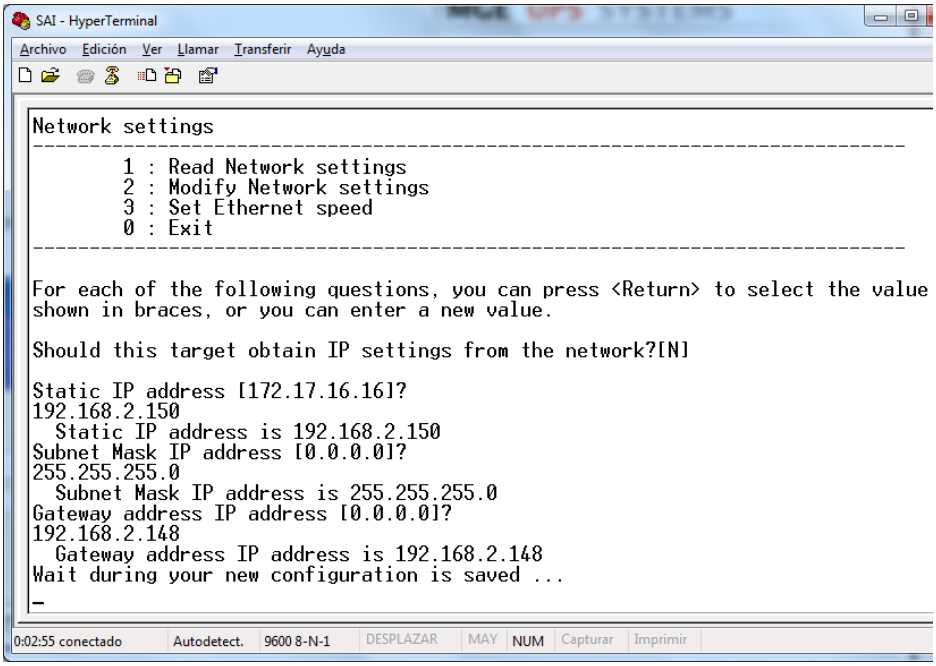
Una vez conectado con nuestra máquina, en el menú, pulsamos la opción de Reset, para restablecer los valores de fábrica.



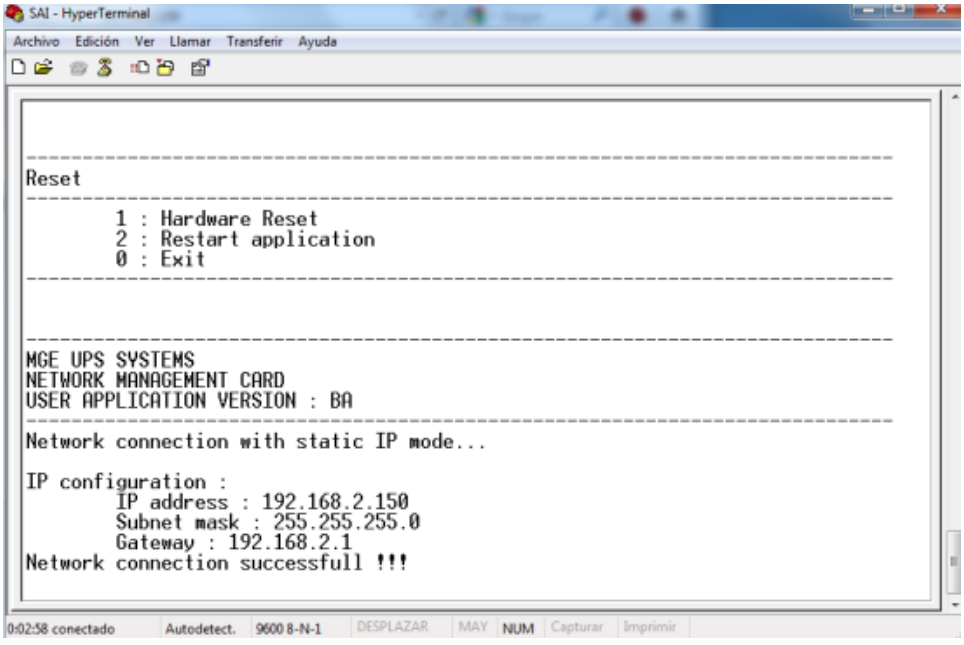
Como podemos observar nos a resteado el SAI.



Ahora vamos a configurar la IP del SAI para adaptarlo a las direcciones de nuestra red, en el menú, aplicamos la opción 2.

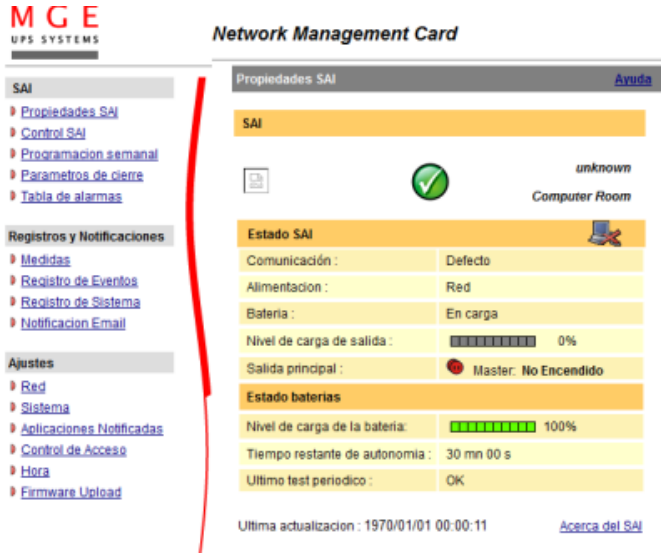


Comprobamos que nos ha guardado las direcciones con éxito.

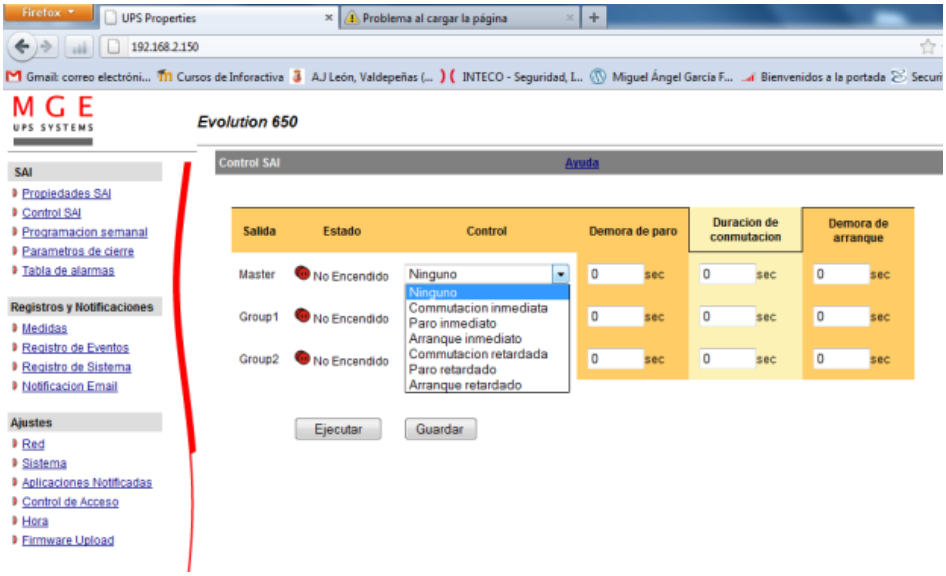


Una vez configurado y comprobado correctamente, procedemos a conectarnos al SAI vía navegador(introduciendo la ip configurada en la barra de direcciones), para entrar al modo configuración gráfico.

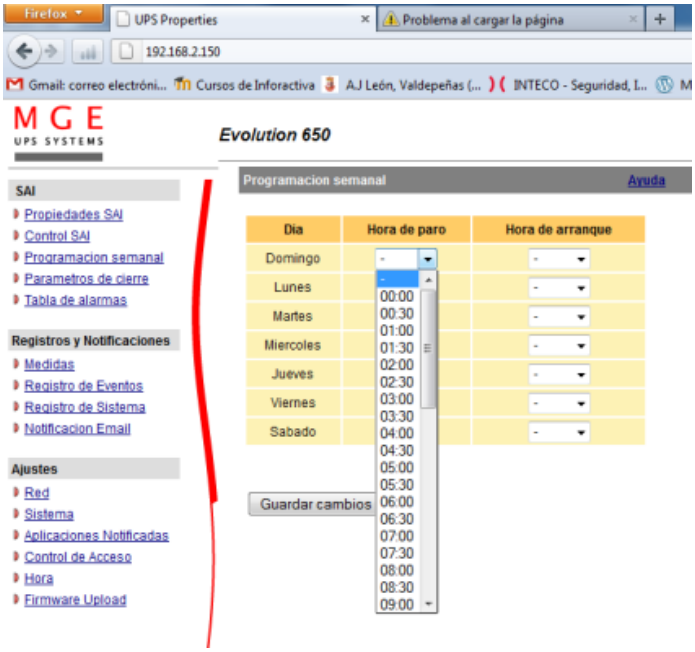
En esta pantalla podemos comprobar el estado de carga del SAI.



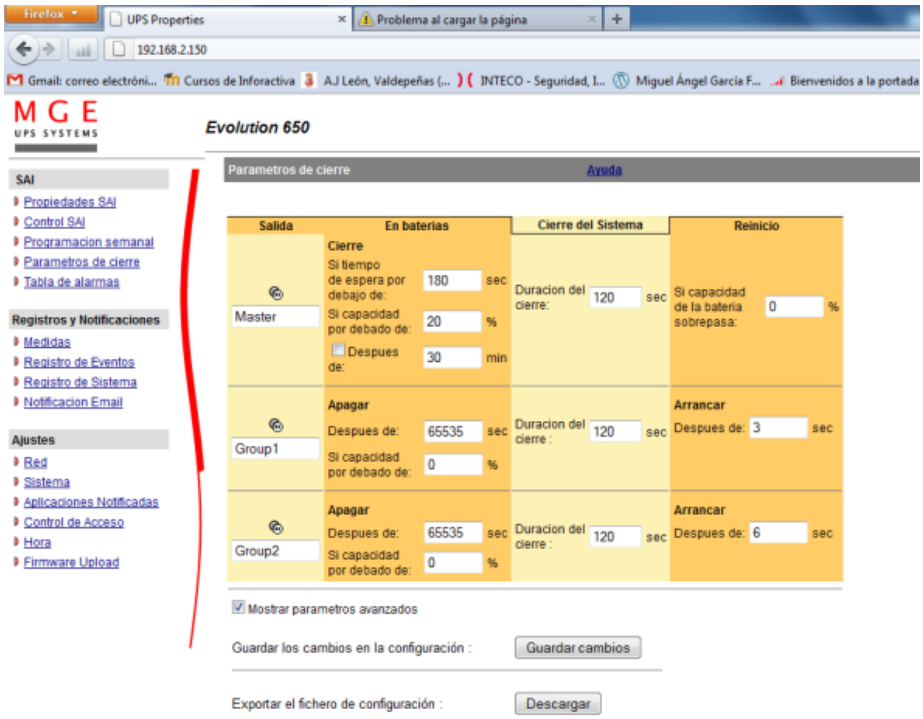
En la ventana de control de SAI, podemos configurar el tiempo de arranque, de parado etc.



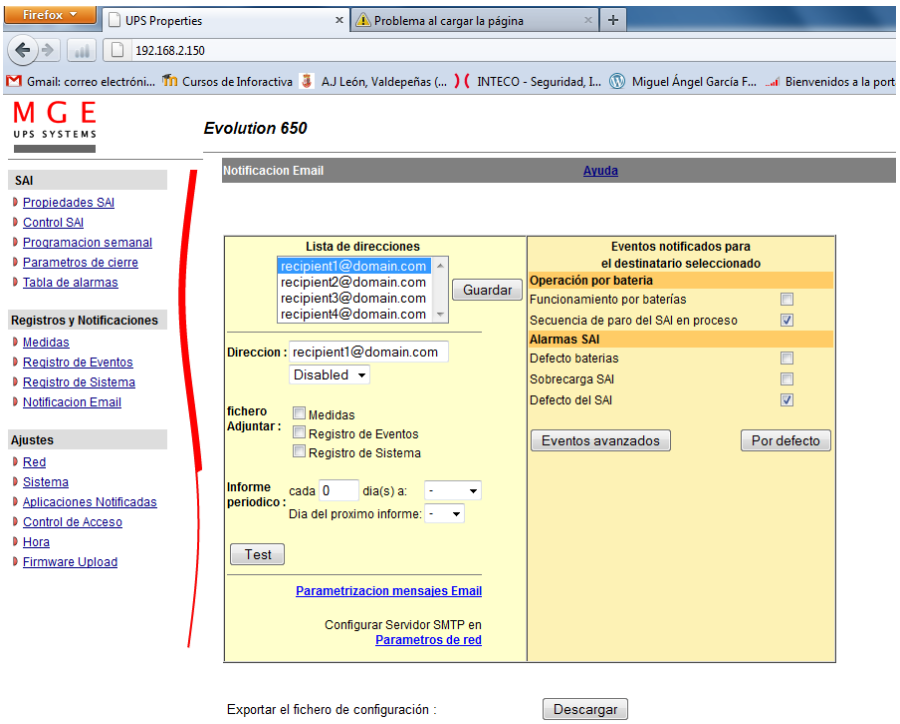
En la ventana de programación semanal, podemos configurar el arranque del SAI en el día y la hora deseado.



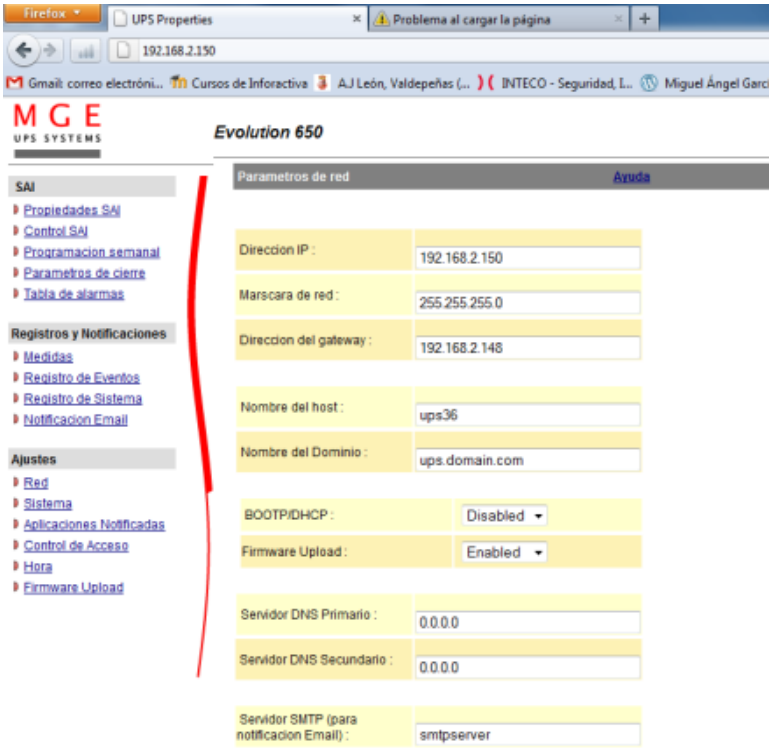
En la ventana de parámetros de cierre, podemos configurar los tiempos referidos a la duración de cierre en los distintos grupos.



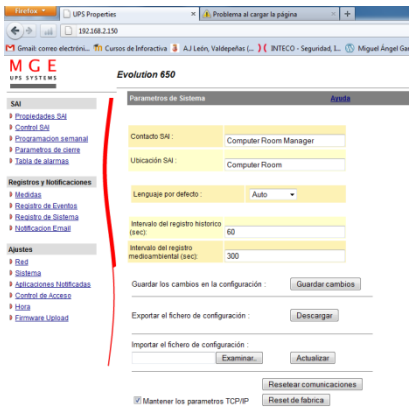
En la ventana de notificación email, podemos configurar el SAI para que nos mande informes detallados a nuestro servidor de correo.



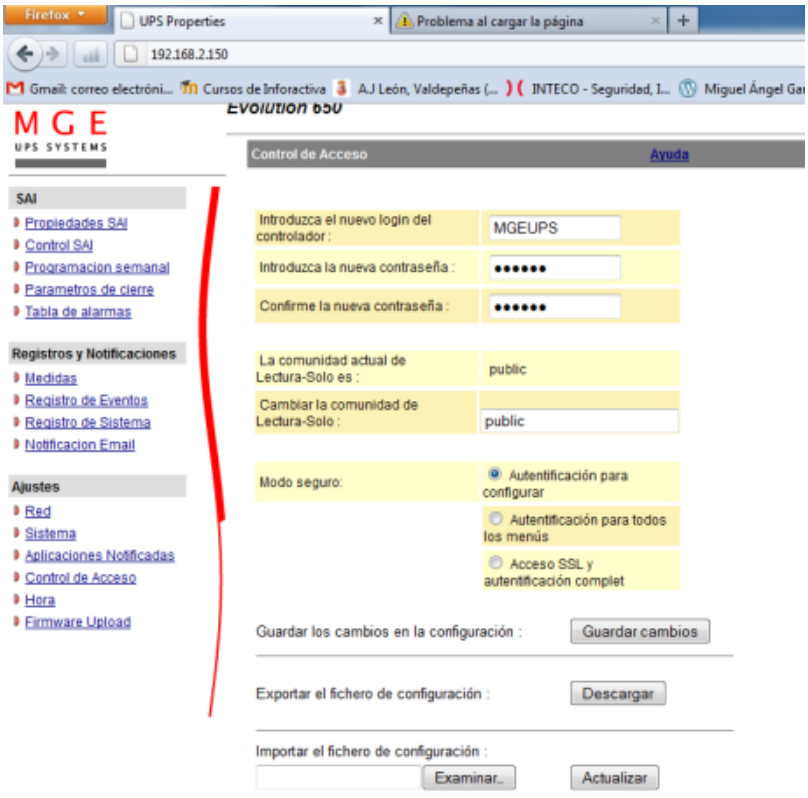
En la ventana de Parámetros de red, podemos configurar las IPs, las máscaras de red, la puerta de enlace, dominios, dns y otros parámetros relacionados con la red.



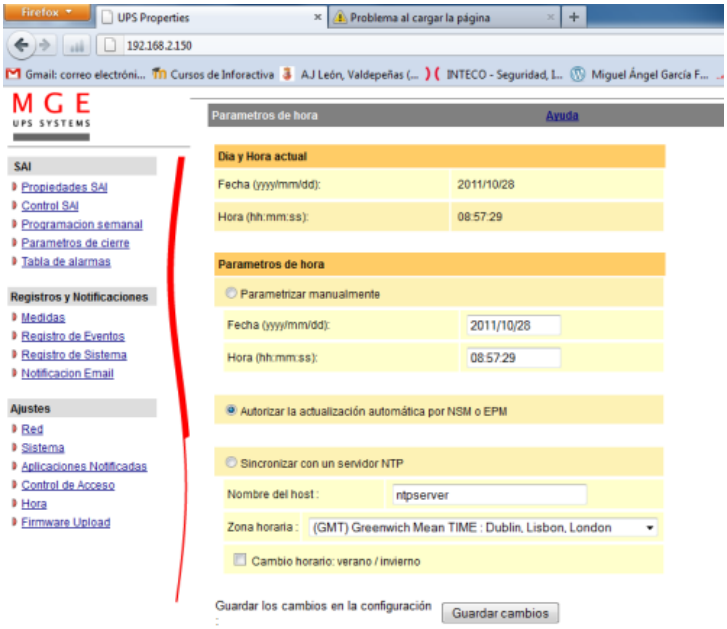
En ésta ventana configuramos nombres y datos relacionados con nuestra máquina física.



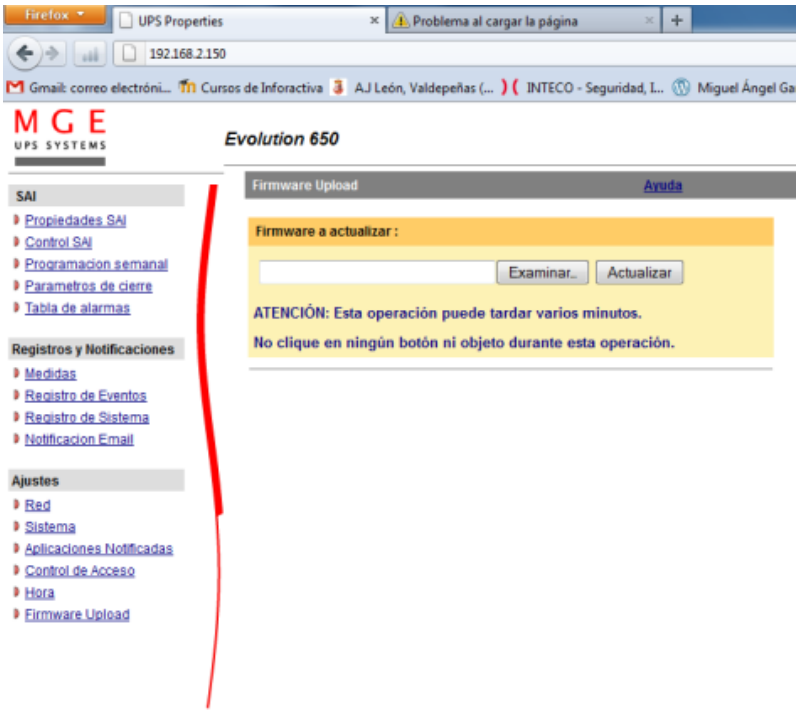
En la ventana de Control de Acceso, podemos cambiar las claves del SAI y el tipo de clave.



En la ventana de parámetros de hora, cambiamos los datos relacionados con la fecha y hora.



En la ventana de Firmware Upload, podemos actualizar la versión de nuestro firmware.



Segundo modelo de SAI

Enlace al manual:

http://www.integra-ups.com/downloads/productos/User%20Manual%20PRO%201%20a%203K%20_Am%C3%A9rica%20-%200608_.pdf

Para realizar la configuración de este SAI a diferencia del modelo configurado en clase para acceder a la configuración de este basta con instalar el programa que viene incluido con el CD y seguir los pasos que nos va indicando.

7. Seguridad lógica:

a) Realizar una copia de seguridad con herramientas del sistema:

LINUX:

TAR

Tar es una herramienta que nos permite crear copias de seguridad de los archivos deseados de una forma rápida y sencilla. Para utilizar tar en primer lugar deberemos de dirigirnos al terminal y una vez allí introducimos la opción que aparece en la imagen pare realizar una copia del archivo prueba en el escritorio y comprimido:

```
alvaroniko@alvaroniko:~/Escritorio$ tar -czvf /home/alvaroniko/Escritorio/prueba
1.tar.gz /home/alvaroniko/Escritorio/prueba1
```

Ahora para restaurar los archivos debemos de introducir el comando de la imagen:

```
alvaroniko@alvaroniko:~$ tar -xvf /home/alvaroniko/Escritorio/prueba1.tar.gz
```

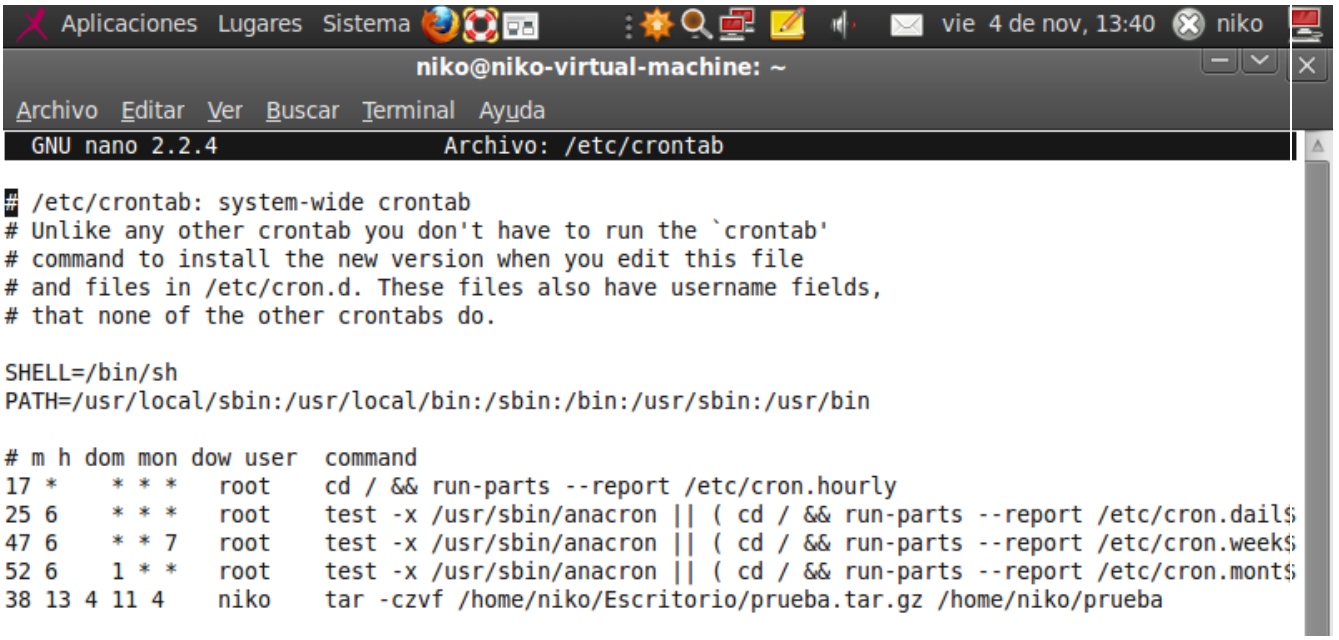
CRONTAB

Es un programa que nos permite programar la ejecución de procesos en nuestro Linux.

Para utilizar crontab en primer lugar deberemos de introducir el siguiente comando para ir al fichero de programación de tareas:

```
root@niko-virtual-machine:/home/niko# nano /etc/crontab
```

Ahora en segundo lugar deberemos de crear las instrucciones para que se realice una copia de seguridad en mi caso he agregado alfinal la siguiente línea: **38 13 4 11 4 niko tar /home/niko/Escritorio/prueba.tar.gz /home/niko/prueba. Donde 38 es el minuto, 13 es la hora, 4 el día del mes, 11 el mes y 4 el dia de la semana(0 domingo, 6 sabado)**



Ahora una vez llegue el momento indicado se realizara la copia de seguridad.

RSYNC

rsync es una aplicación libre para sistemas de tipo Unix y Microsoft Windows que ofrece transmisión eficiente de datos incrementales, que opera también con datos comprimidos y cifrados.

Para realizar la instalación de rsync, en primer lugar deberemos de isntalar el rsync, para ello tecleamos el comando apt-get install rsync:

```
# apt-get install rsync
```

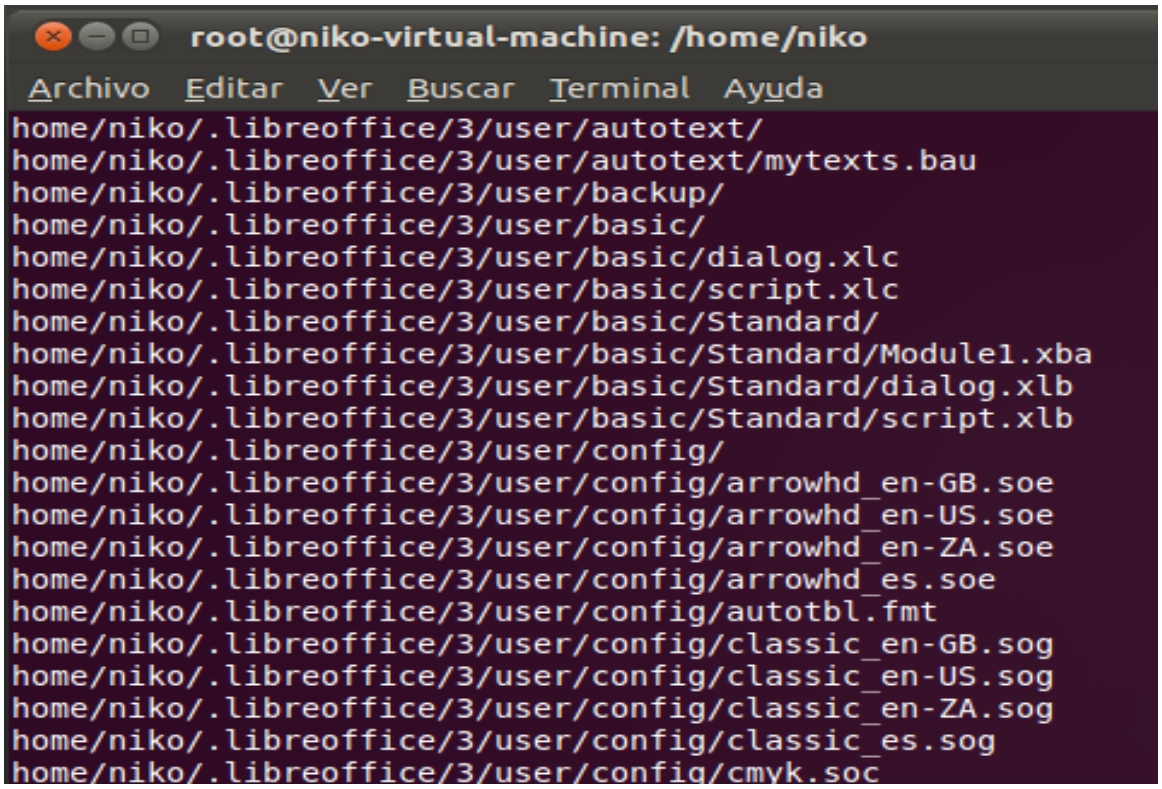
Una vez instalado deberemos de instalar el ssh tanto el cliente como el servidor, para asi poder realizar copias de seguridad a través de la red:

```
root@alumno02:/home/alumno02/Documentos# apt-get install ssh
```

Una vez instalado, realizaremos la copia del directorio /home del equipos 192.1682.100, para ello deberemos de introducir el comando **rsync –av /home niko@192.168.2.100:/home** para si poder realizar una copia del directorio /home del equipos 192.168.2.100:

```
root@niko-virtual-machine:/home/niko# rsync -av /home root@192.168.2.100:/home
The authenticity of host '192.168.2.100 (192.168.2.100)' can't be established.
RSA key fingerprint is 8b:4b:57:a8:04:39:9e:bd:b7:72:73:b5:3c:2d:09:10.
Are you sure you want to continue connecting (yes/no)?
```

En esta imagen podremos observar el proceso de copia de los archivos:



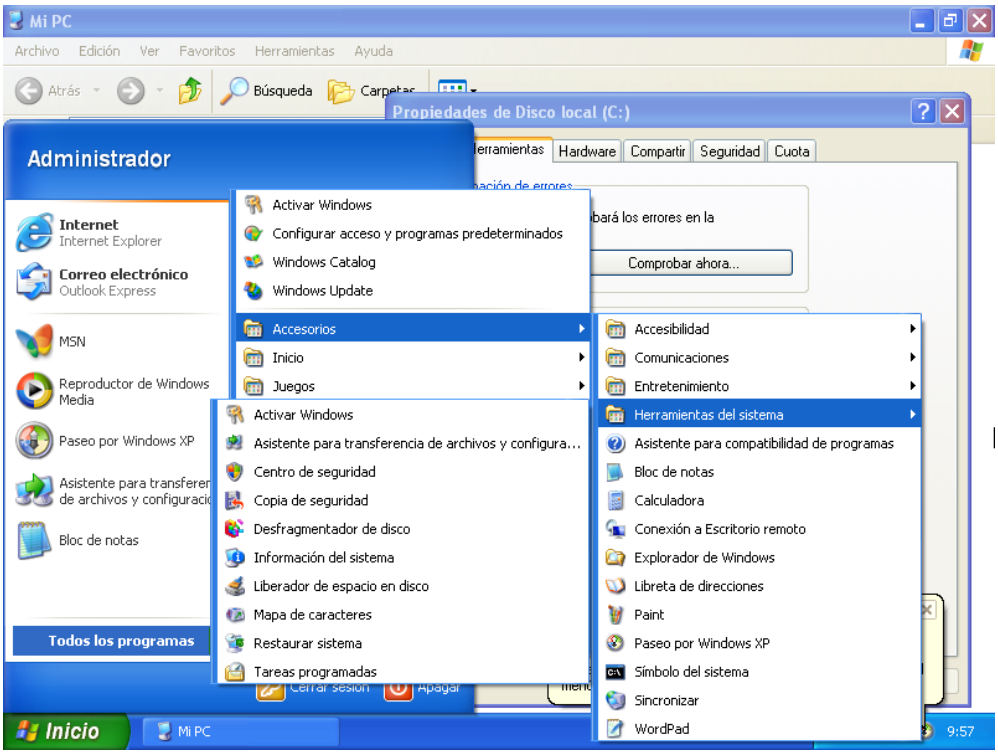
Una vez finalizado se habrá realizado la copia de seguridad, si queremos restaurarla solo tendremos que realizar el proceso inverso al realizado en los pasos anteriores.

EN XP

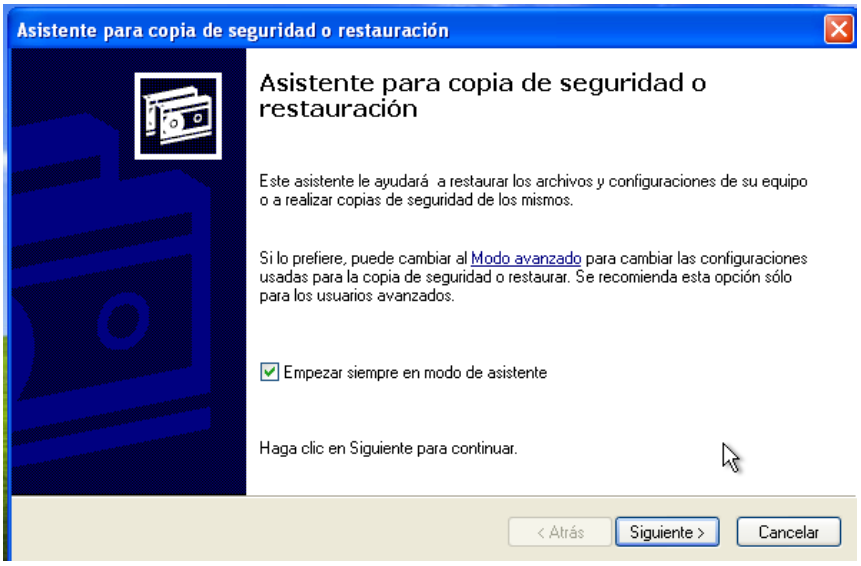
COPIAS DE SEGURIDAD

Windows XP viene con un gestor de copias de seguridad muy útil con el que prodremos realizar el mantenimiento de nuestro sistema sin utilizar programas de tercero.

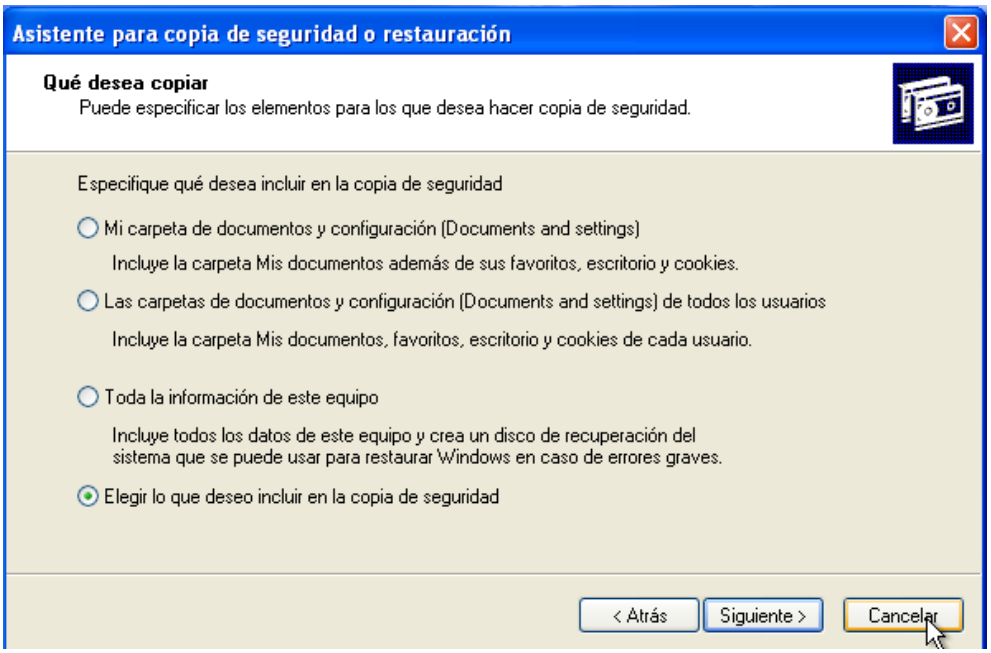
Para utilizarlo, en primer lugar nos dirigimos a inicio/todos los programas /accesorio/herramientas del sistema/copias de seguridad



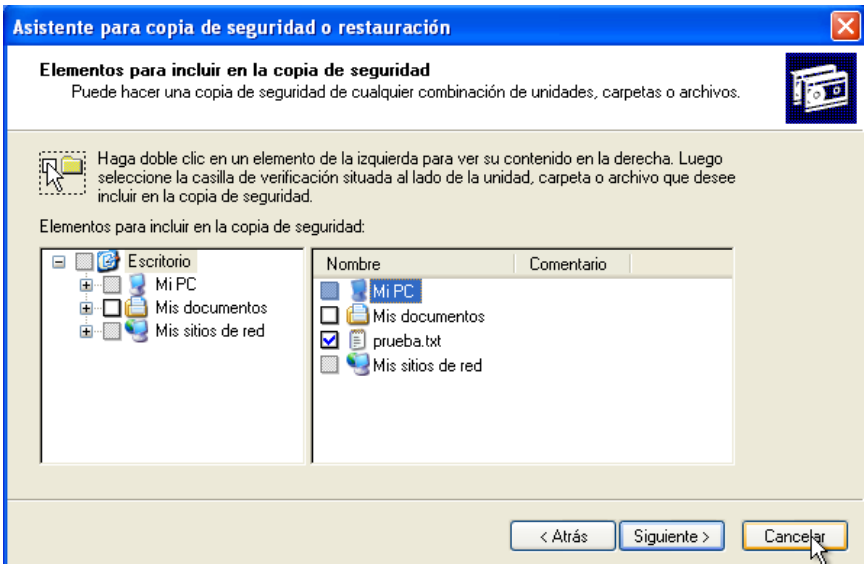
En la primera pantalla del asistente para copia de seguridad pulsamos sobre siguiente :



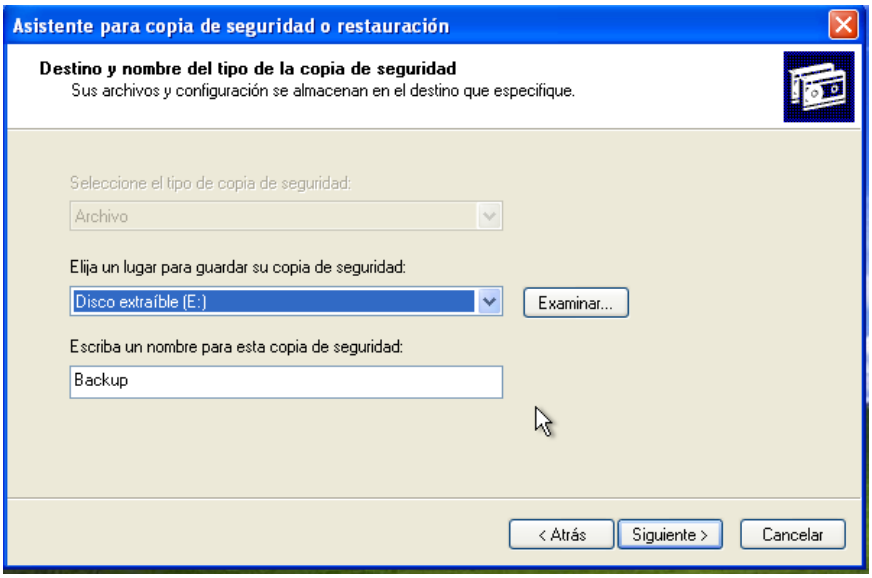
En la segunda pantalla elegimos la opción elegir lo que deseo incluir en la copia de seguridad



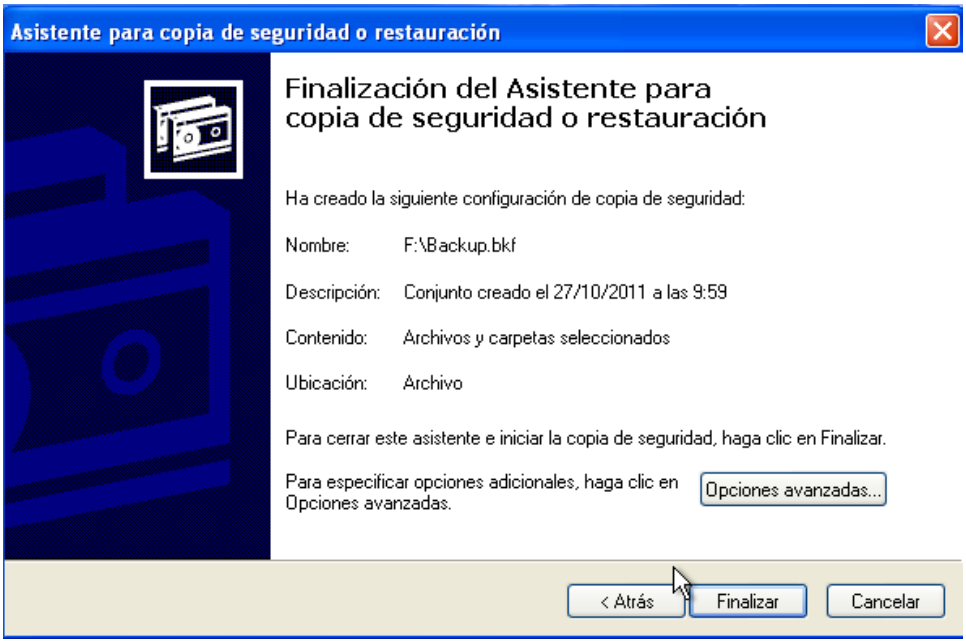
Ahora seleccionamos los archivos que queremos incluir en nuestra copia de seguridad

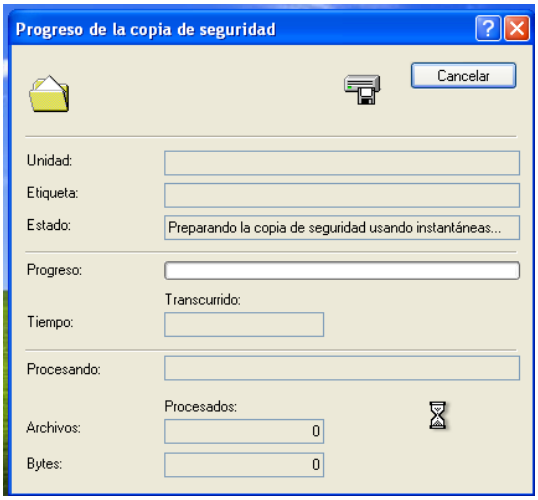


Ahora deberemos de seleccionar el destino de la copia de seguridad:

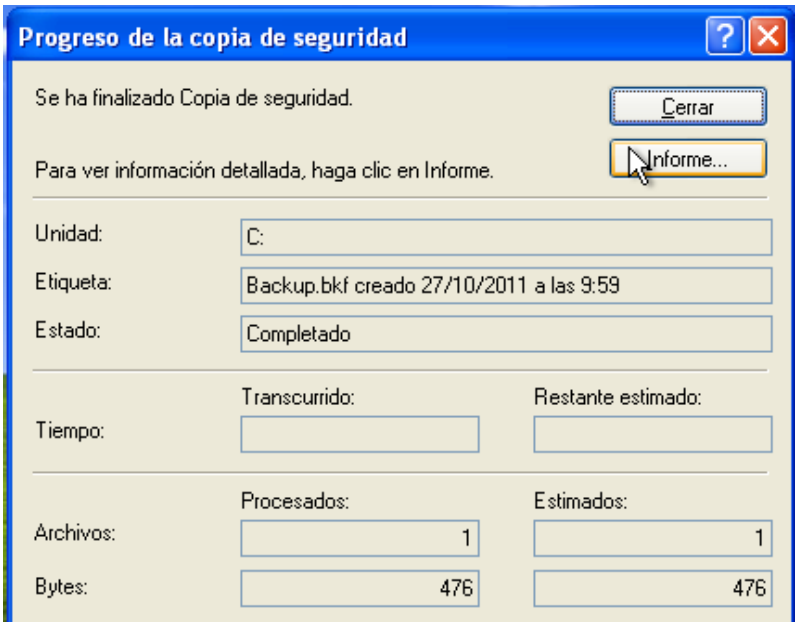


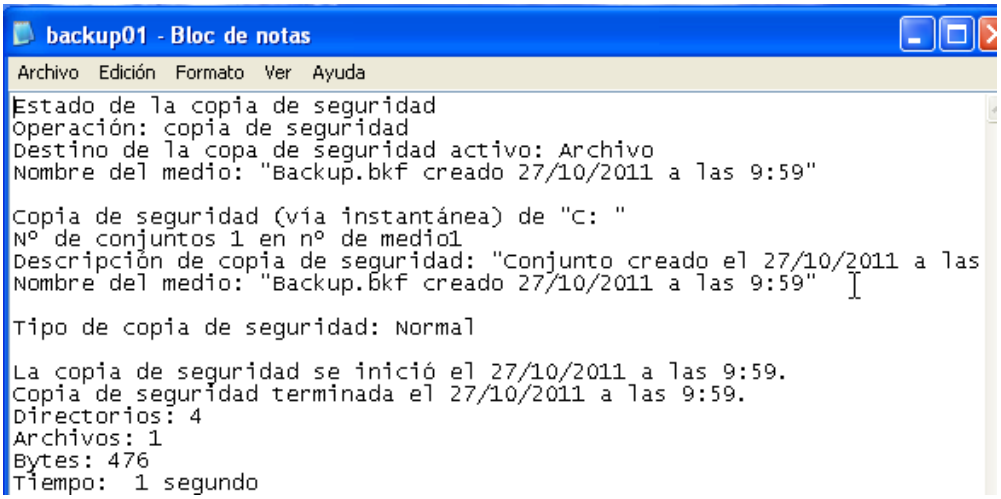
Ahora deberemos de finalizar para que de comienzo el proceso de copia de seguridad:





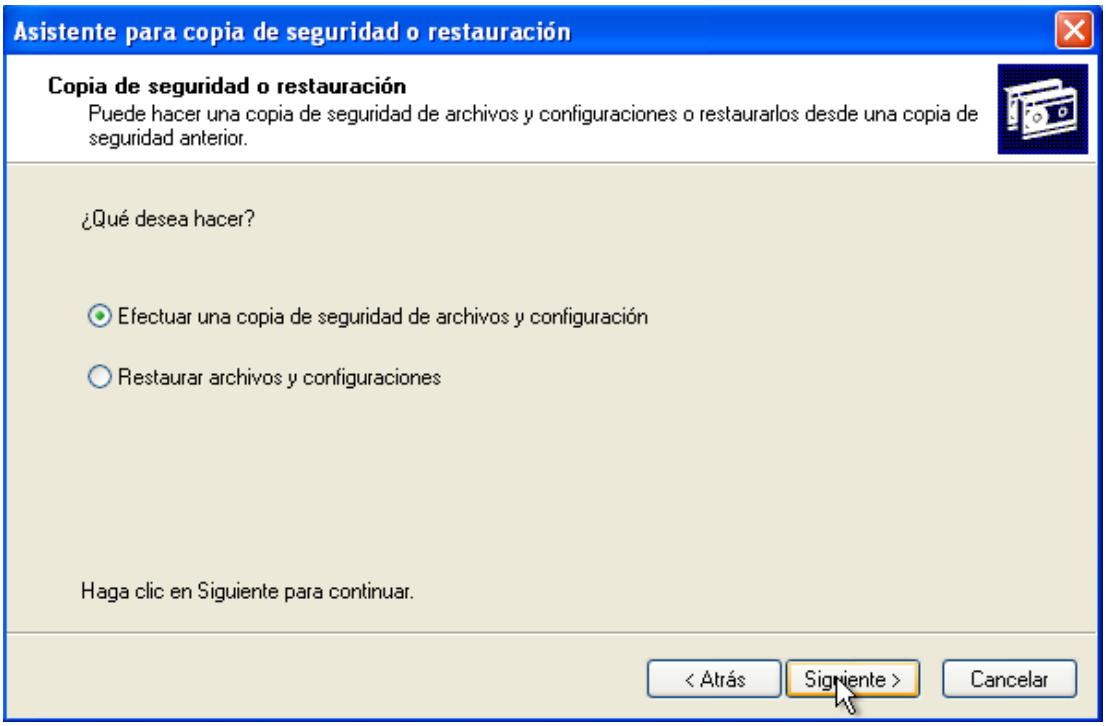
Una vez finalizado el proceso podemos ver el informe:



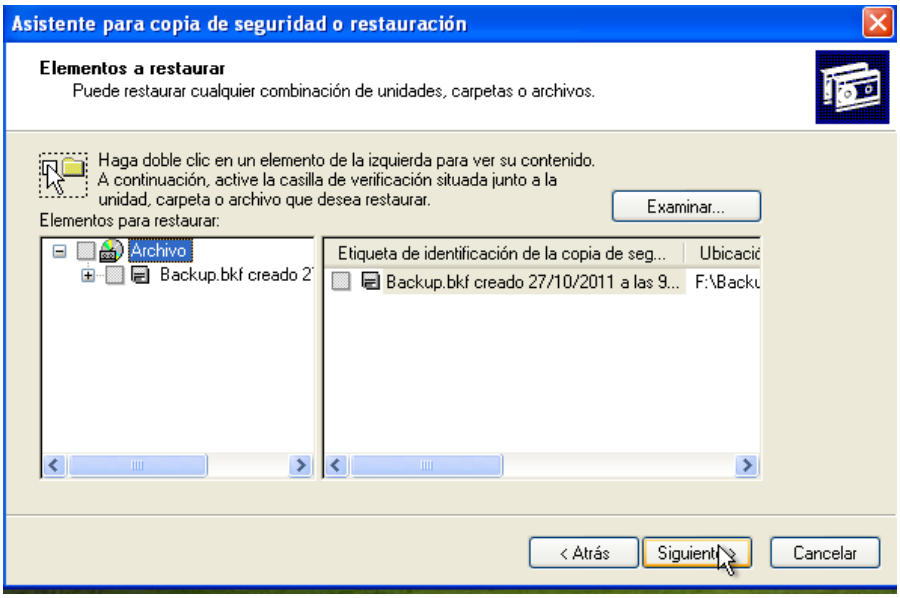


PROCESO DE RESTAURACION

En primer lugar nos dirigimos al asistente para copia de seguridad o restauración y seleccionamos la opción restaurar archivos y configuraciones:

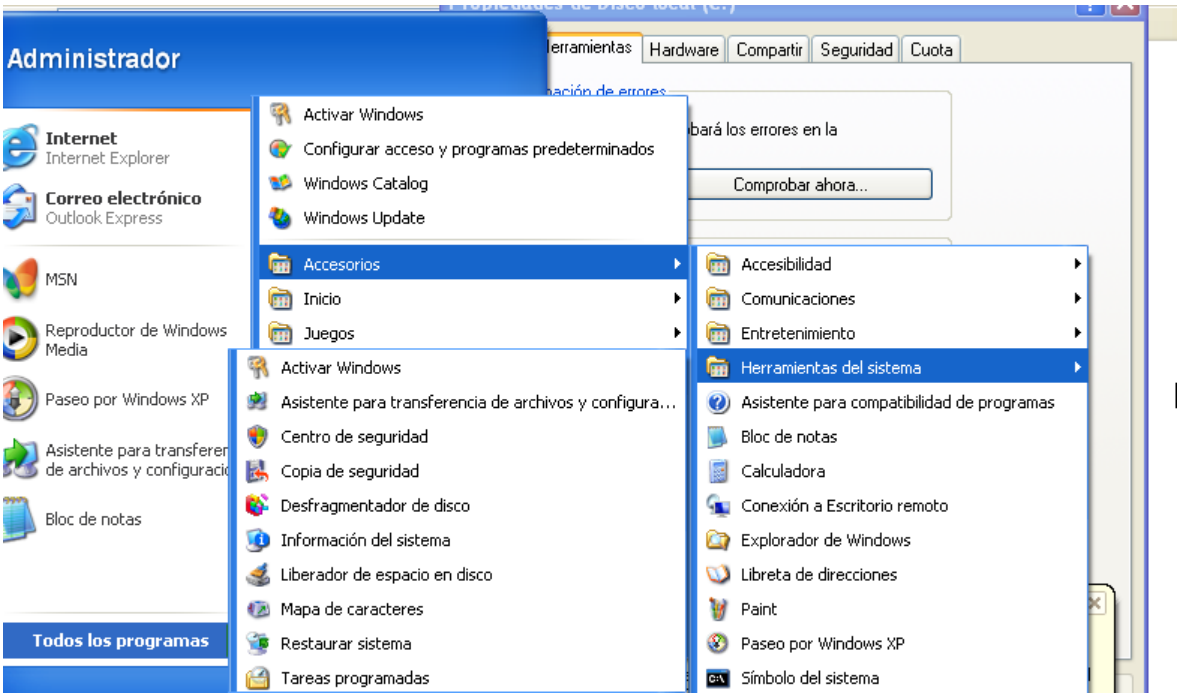


En la siguiente imagen seleccionamos el backup y pulsamos sobre siguiente para que se restaure la copia de seguridad

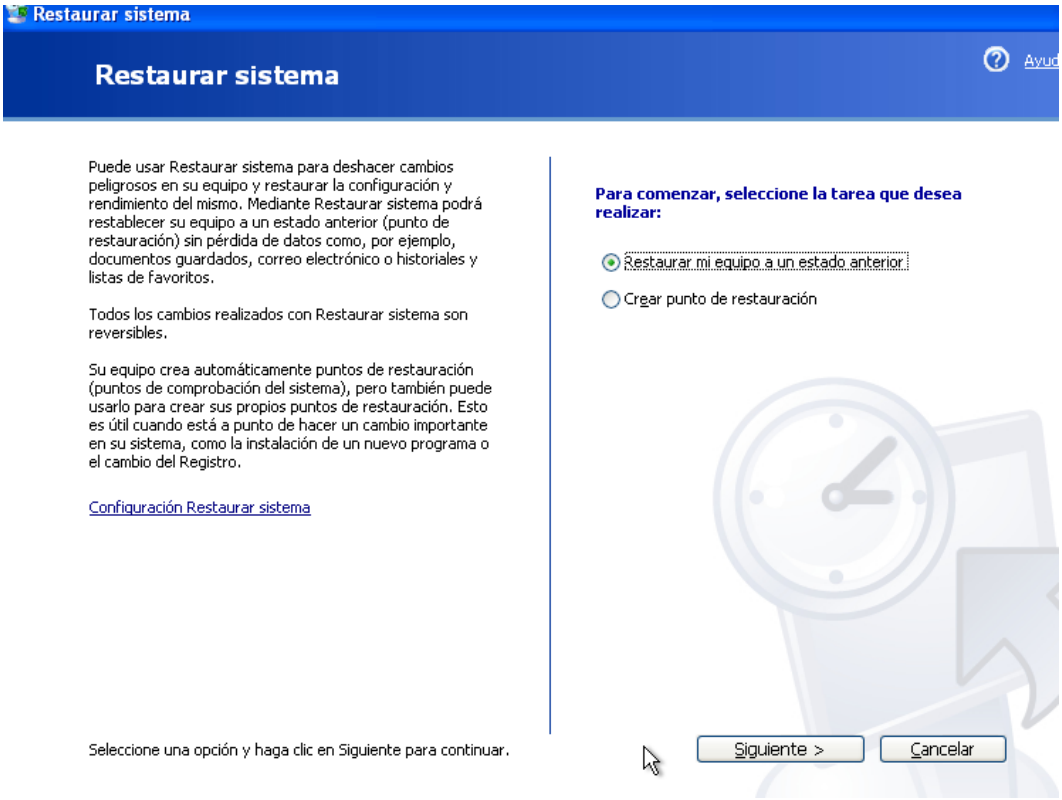


RESTAURACION DEL EQUIPOS A UN ESTADO ANTERIOR

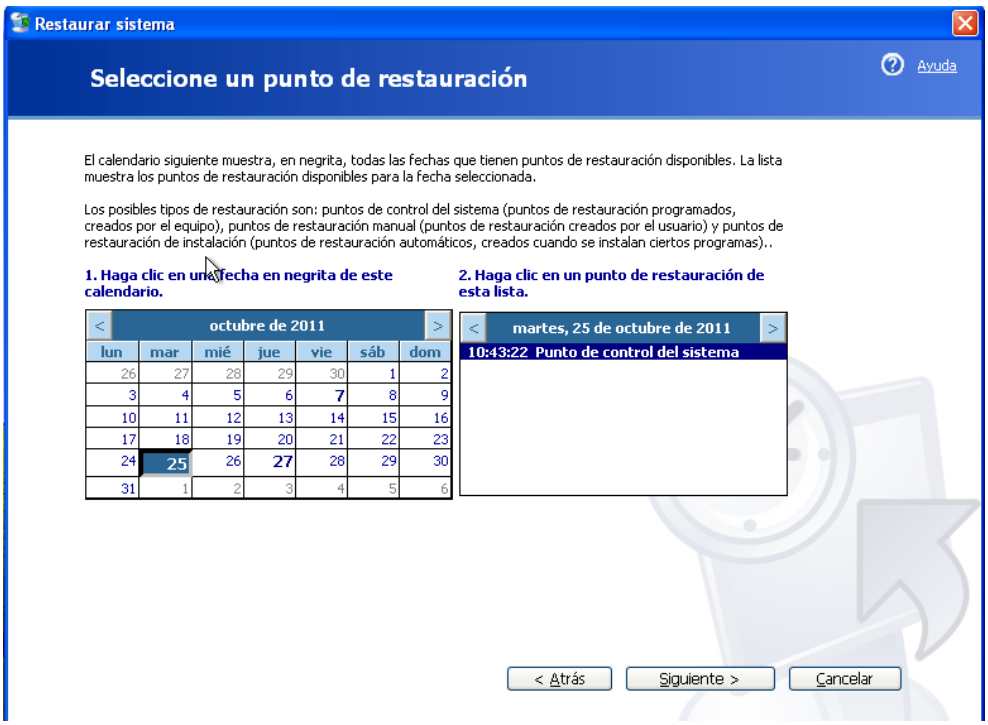
En primer lugar nos dirigimos a inicio/todos los programas/accesorio/herramientas del sistema/restaurar sistema



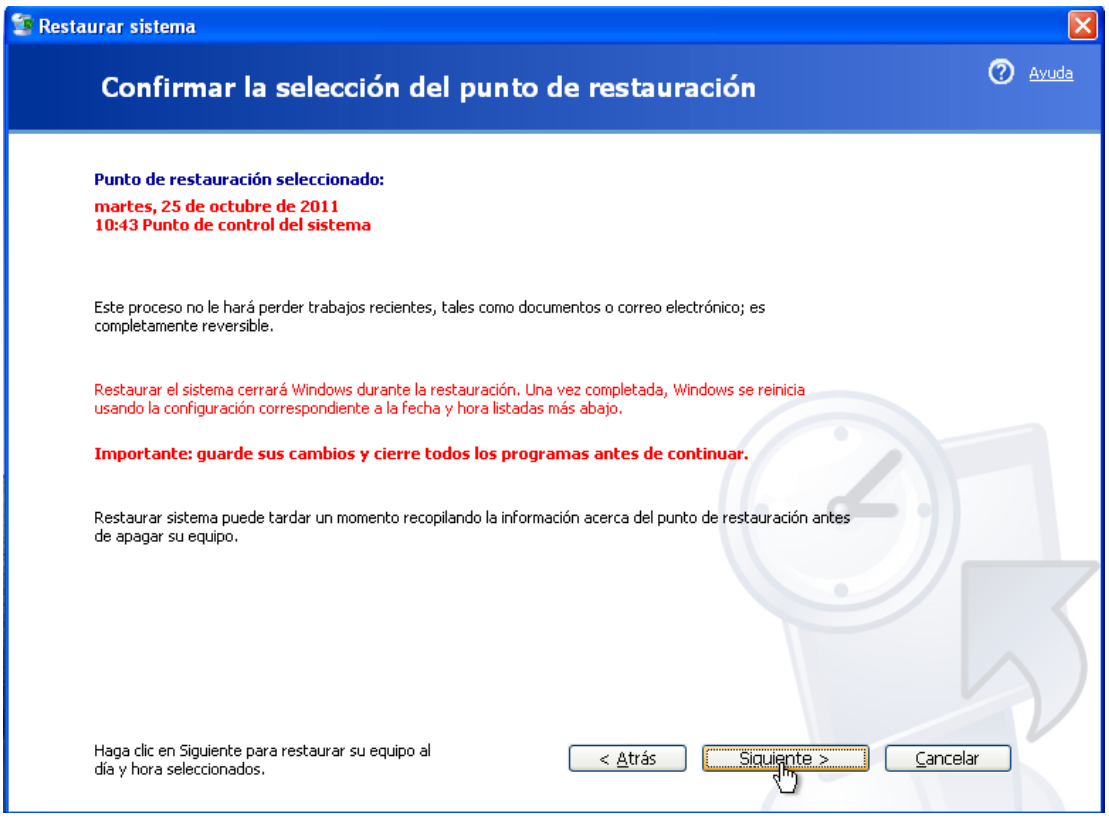
En primer lugar seleccionamos la opción restaurar mi equipo a un estado anterior y pulsamos siguiente:



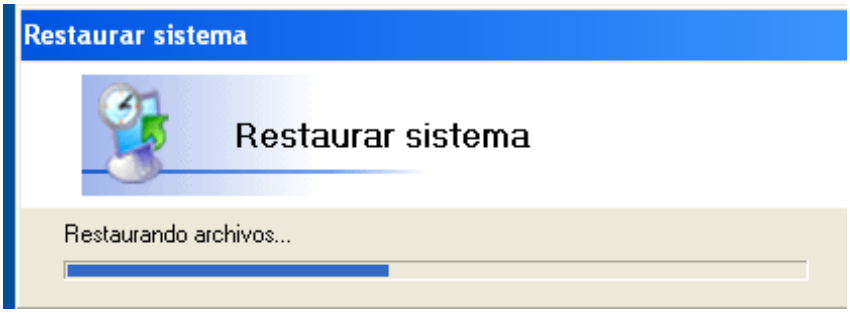
En el asistente seleccionamos la fecha deseada a la que se quiere restaurar y pulsamos sobre siguiente:



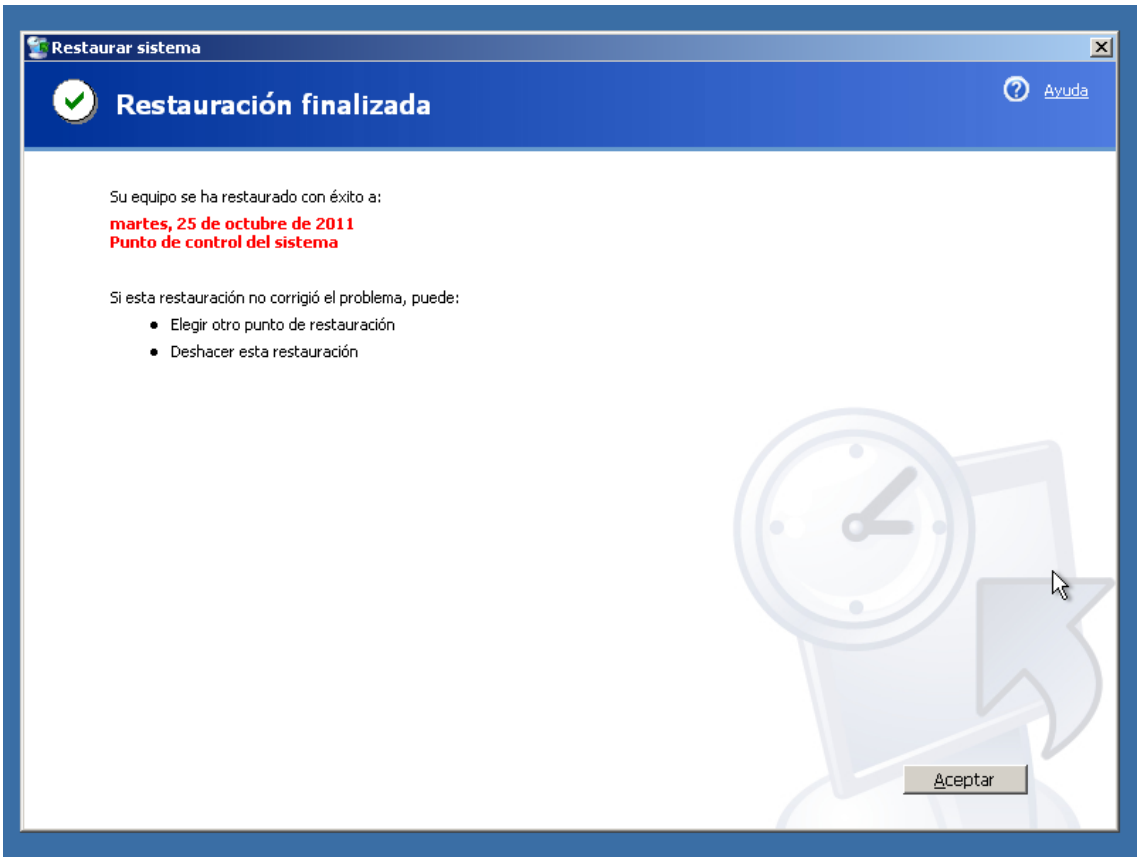
Hora tendremos que pulsar siguiente para confirmar la restauración de nuestro sistema:



Ahora reiniciara nuestro sistema y dará comienzo la restauración:



Una vez finalizado el proceso nos aparecerá la siguiente pantalla:

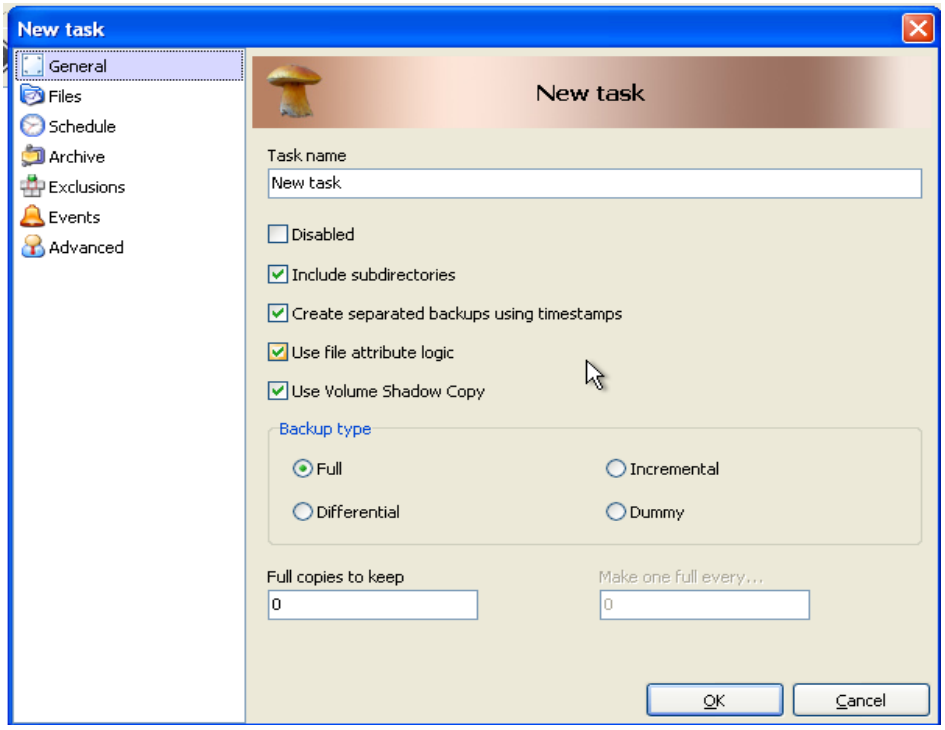


b) Realizar una copia de seguridad con aplicaciones específicas:

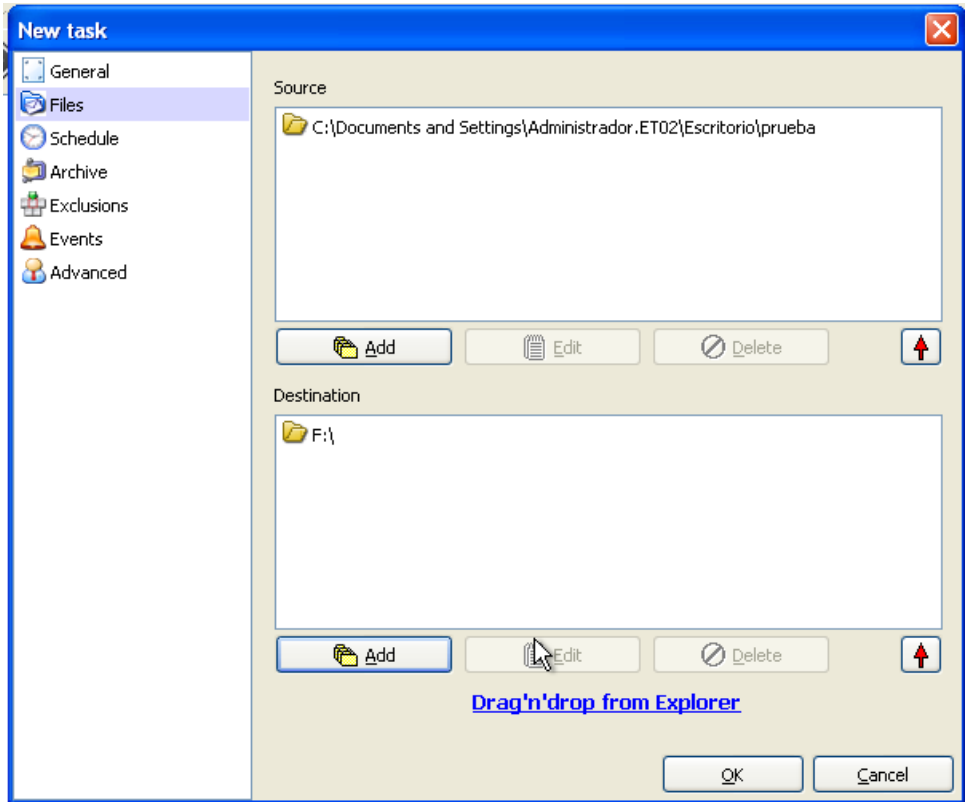
EN Windows

Cobian backup

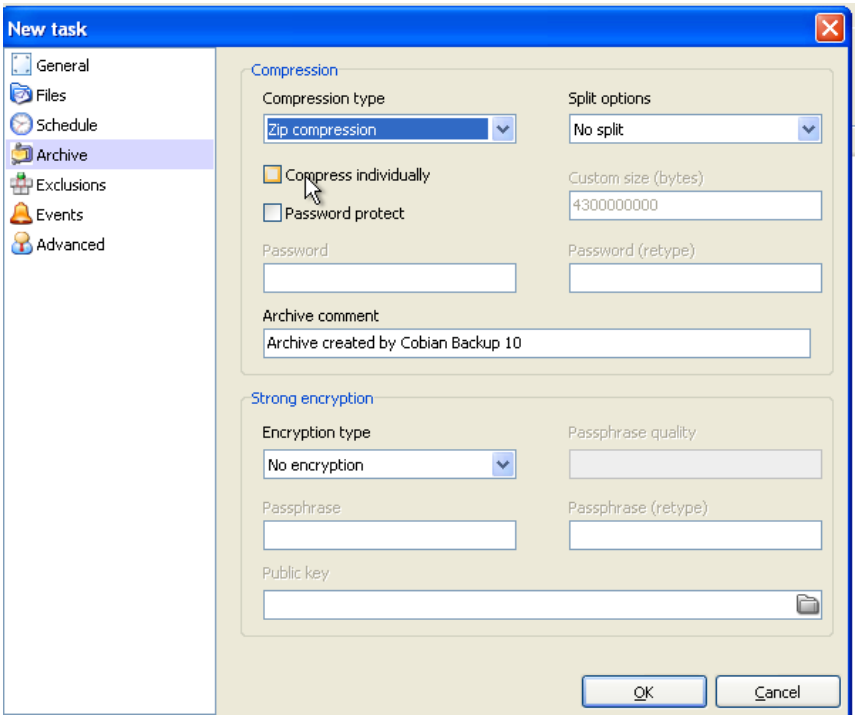
Es un programa que nos permite realizar copias de seguridad, para ello nos dirigimos a task y seleccionamos la sección new task. Una vez allí en la pestaña general podremos configurar el nombre de nuestra copia de seguridad:



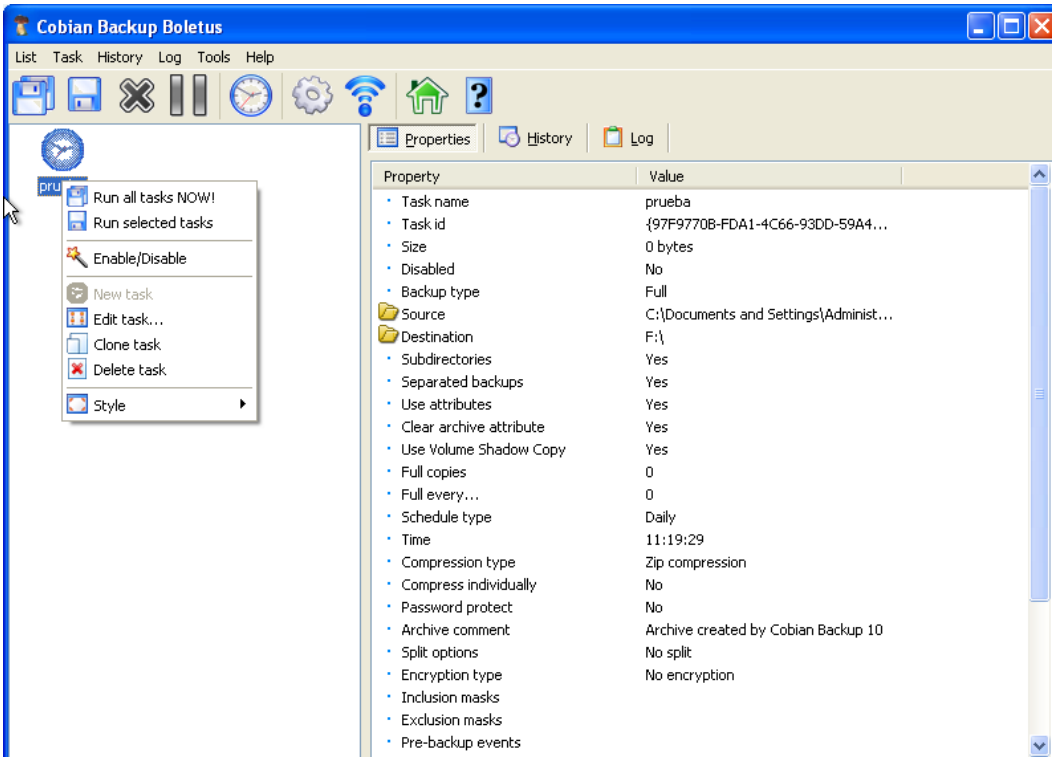
Ahora en la pestaña Files deberemos de seleccionar en source el lugar de destino y en destination el lugar de destino. Para ello seleccionamos add y seleccionamos el lugar deseado.



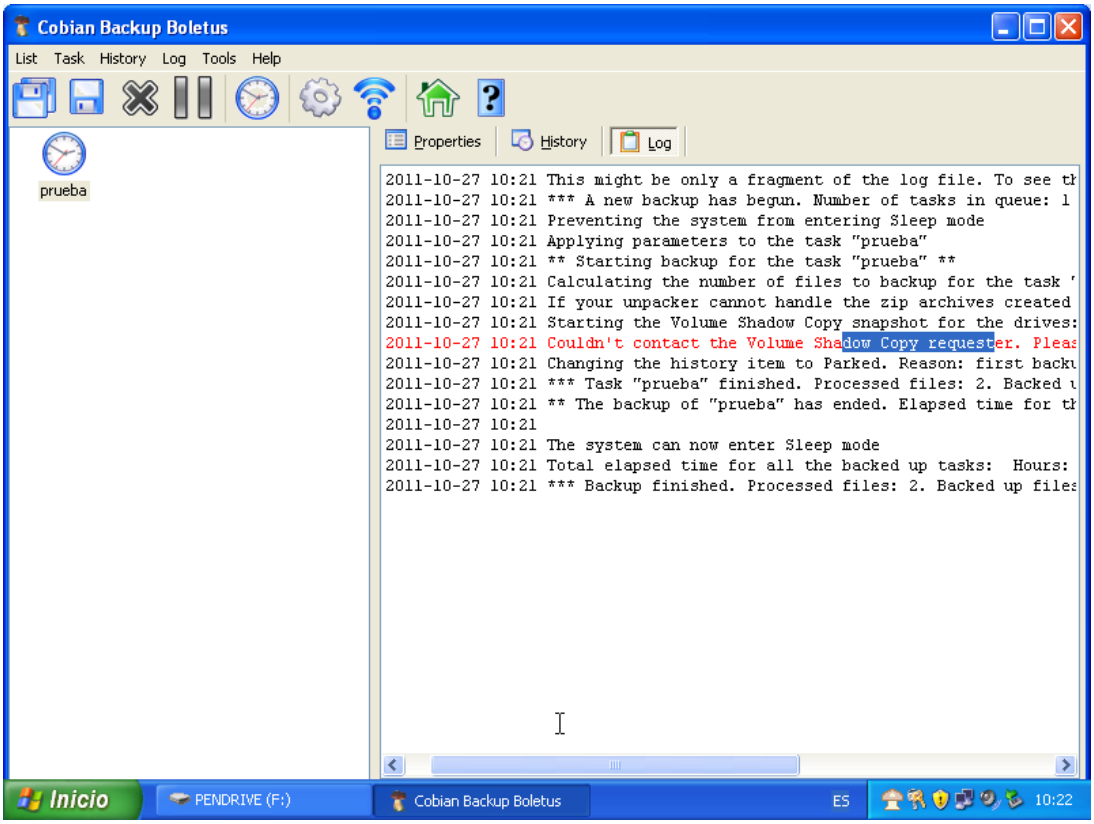
En la pestaña Archive podremos seleccionar el método de compresión en nuestro caso seleccionamos zip compression. Ahora pulsaremos sobre ok para aplicar los cambio de configuración:



Ahora para iniciar la copia de seguridad deberemos de pulsar el botón derecho sobre el task creado anteriormente u seleccionamos la opción runa ll task NOW!.



En esta imagen observamos el proceso de realización de la copia de seguridad:



Una vez finalizado se nos creara un archivo ZIP con la copia de seguridad.

EN LINUX

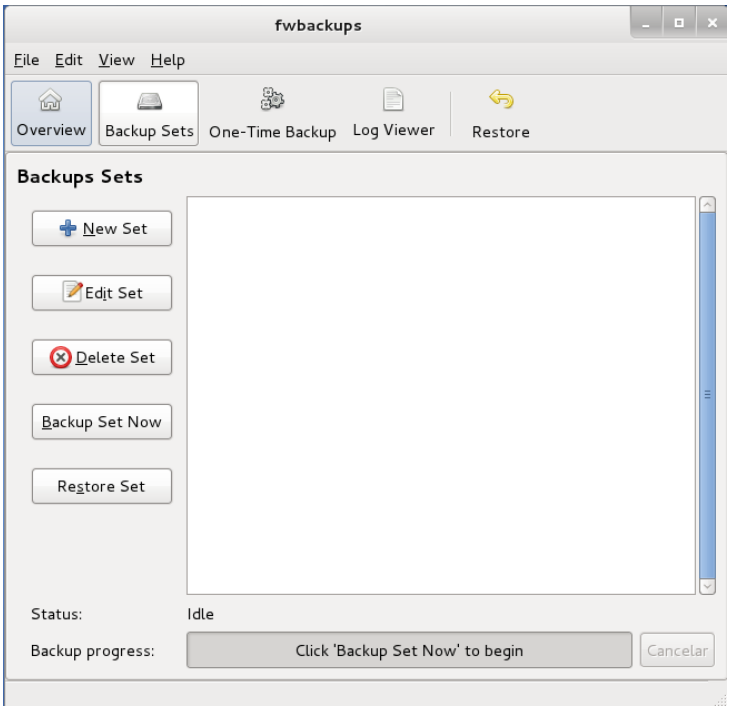
FWBACKUP

Es un programa que nos permite realizar y automatizar copias de seguridad en nuestros equipos. Para intslar FWBACKUP en nuestro equipo deberemos de seguir los siguientes pasos:

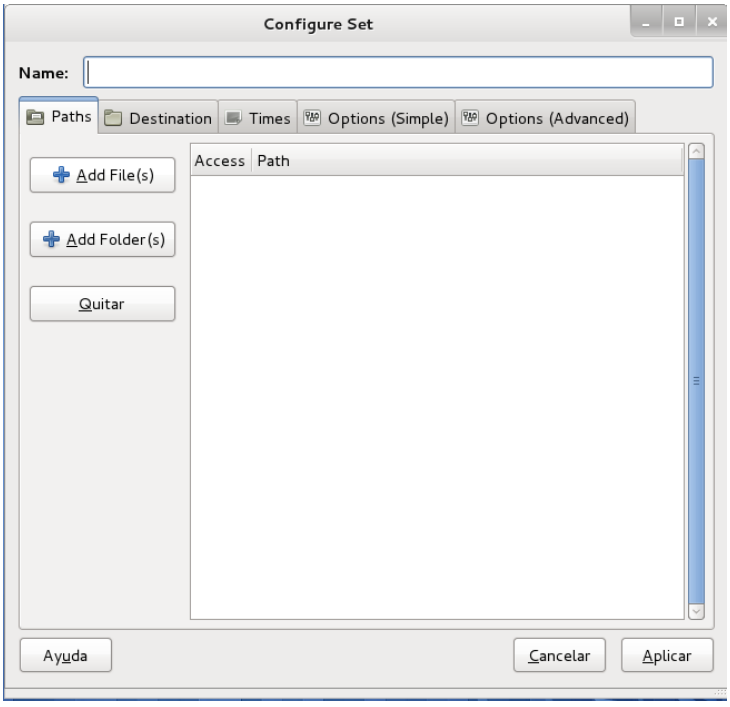
En primer lugar tecleamos yum install fwbackups:

```
[root@niko niko]# yum install fwbackups
Complementos cargados:langpacks, presto, refresh-packagekit
```

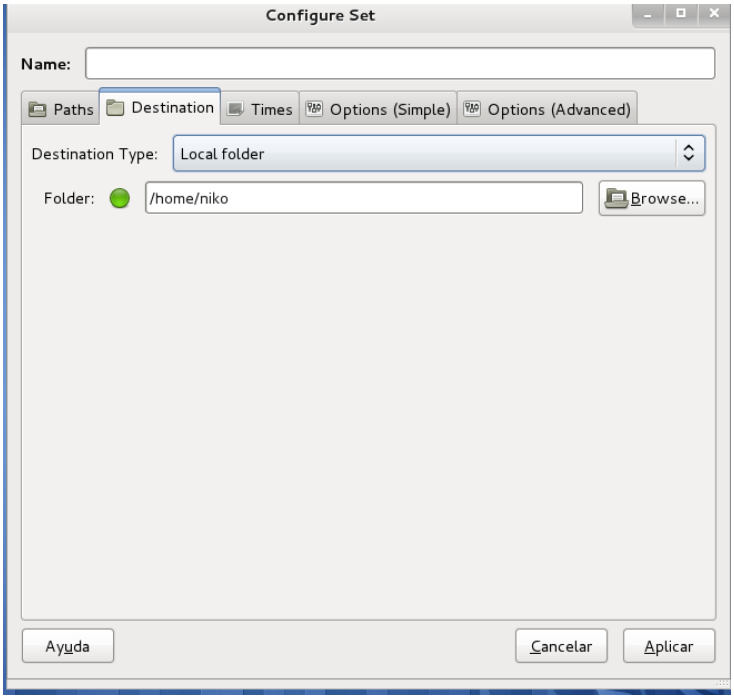
Una vez instalado deberemos de dirigirnos a las sección backup sets y pulsar sobre New Set para crear una nueva copia de seguridad:



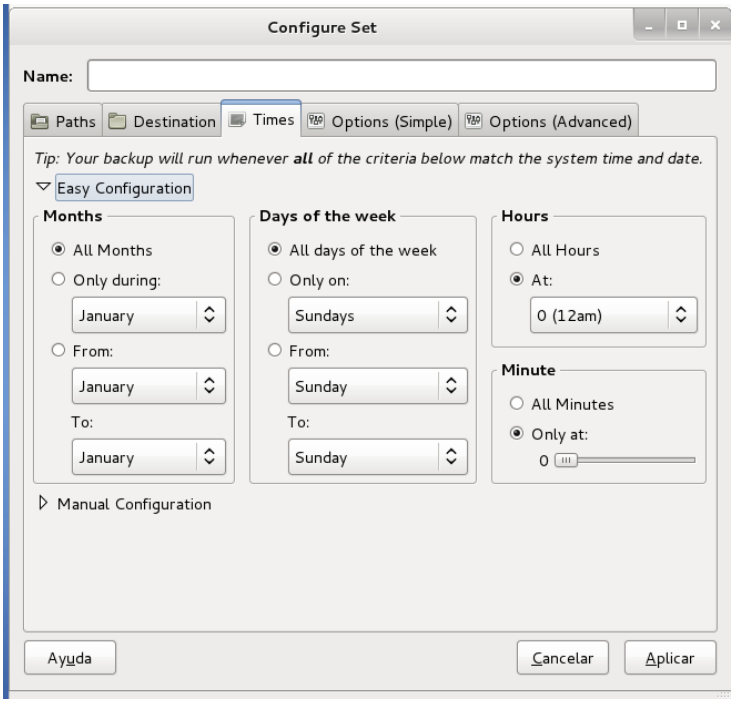
Ahora en la pestaña Paths deberemos de pulsar sobre Add File(s) para añadir los archivos de los que deseamos crear copias de seguridad:



Una vez añadidos los archivos deberemos de elegir el destino de la copia de seguridad en la pestaña Destination:

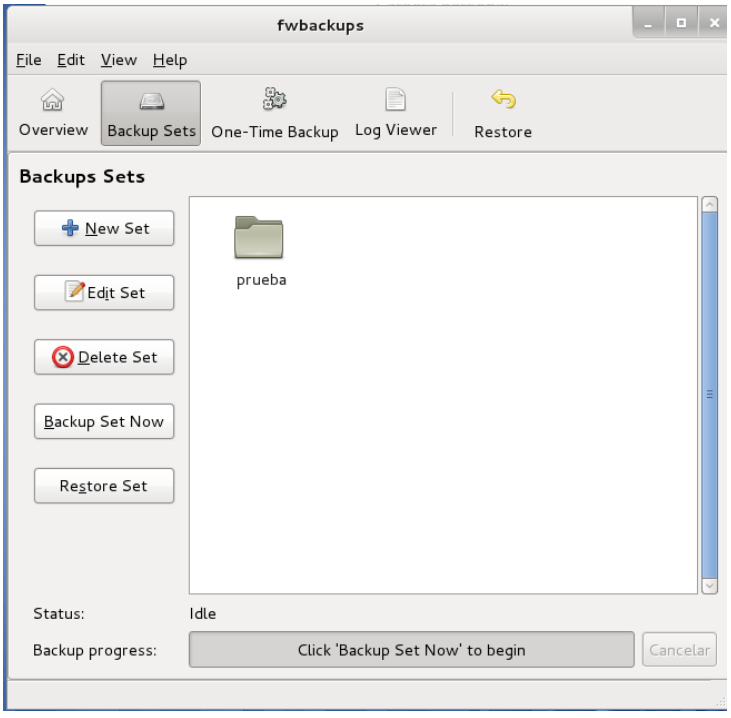


En la pestaña times podremos programar la realización de la copia de seguridad:

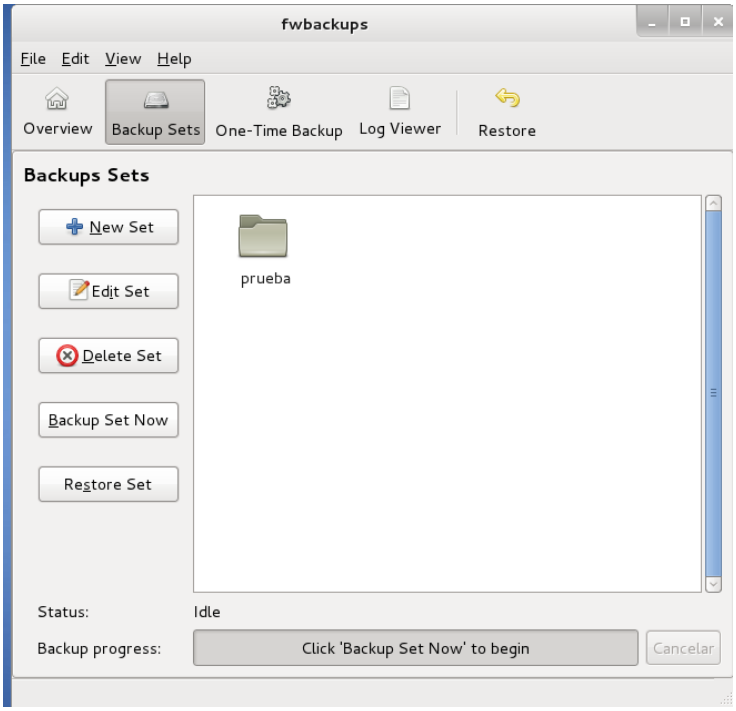


En la pestaña options (simple) podremos de configurar las opciones básicas de la copia de seguridad como son el formato del backup o las opciones del mismo. Una vez acabada la configuración de la copia de seguridad deberemos de pulsar sobre aplicar para guardar la copia de seguridad:

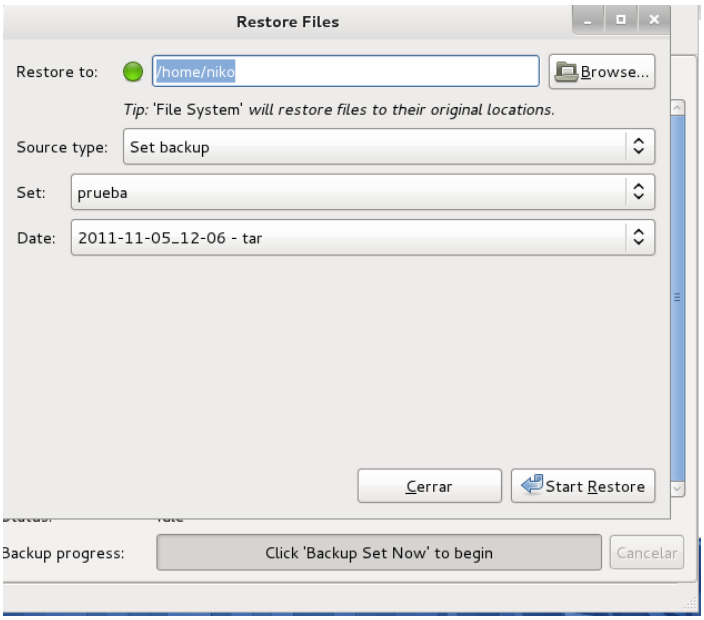
Ahora deberemos de pulsar sobre prueba y posteriormente pulsar sobre el botón Backup Set Now para que de comienzo la realización de la copia de seguridad:



Ahora para restaurar la copia de seguridad deberemos de pulsar sobre el botón Restore Set.



Por ultimo deberemos elegir el lugar de restauración en la sección Restore to. Una vez configurada la restauración deberemos de pulsar el botón start restore:



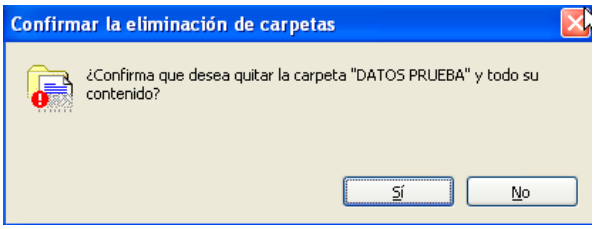
c) Utiliza una herramienta de recuperación de datos:

En Windows

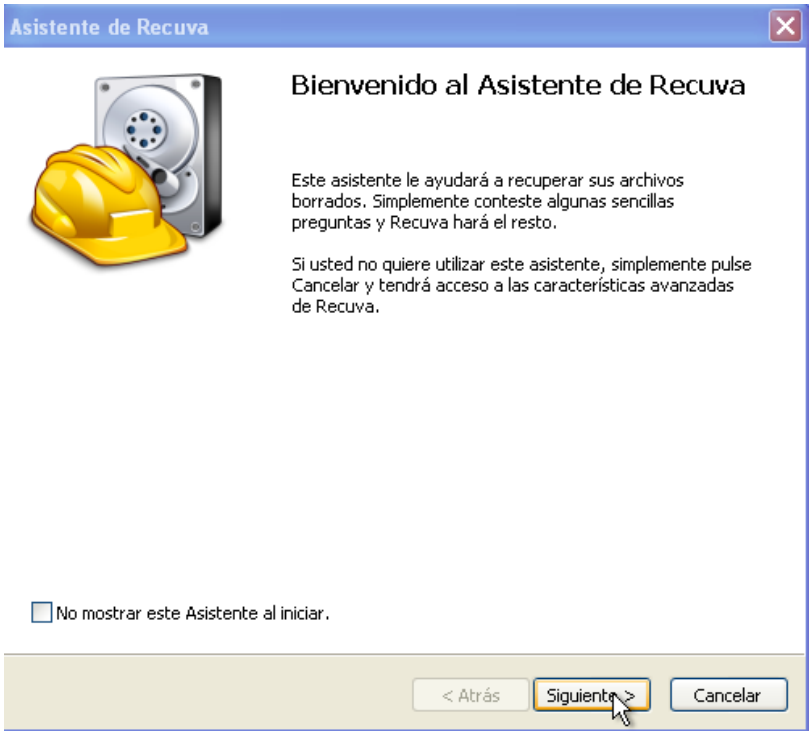
RECUVA

Este interesante programa sirve para recuperar archivos que hayas borrado sin querer; detecta los borrados y te permite seleccionarlos cómodamente.

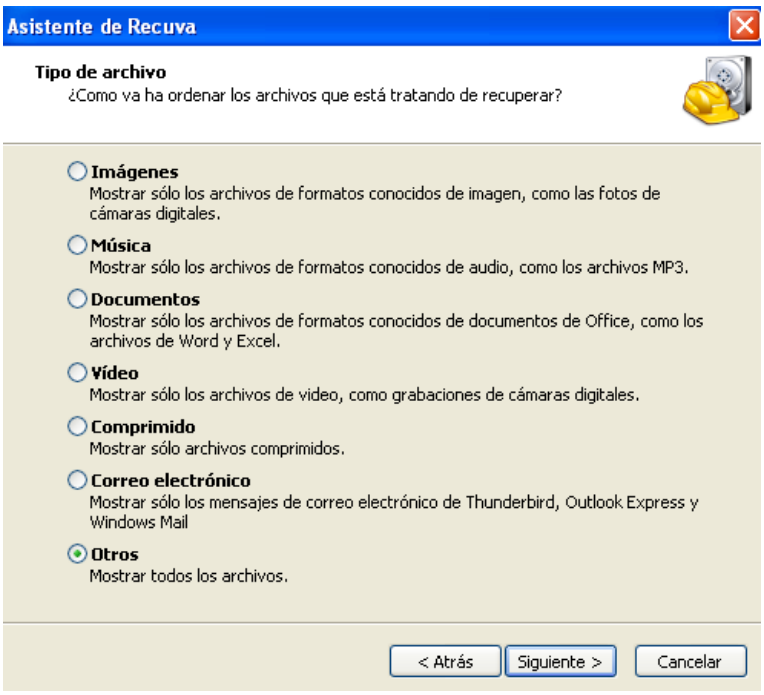
En primer lugar procederemos a la eliminación de la carpeta con el nombre DATOS PRUEBA:



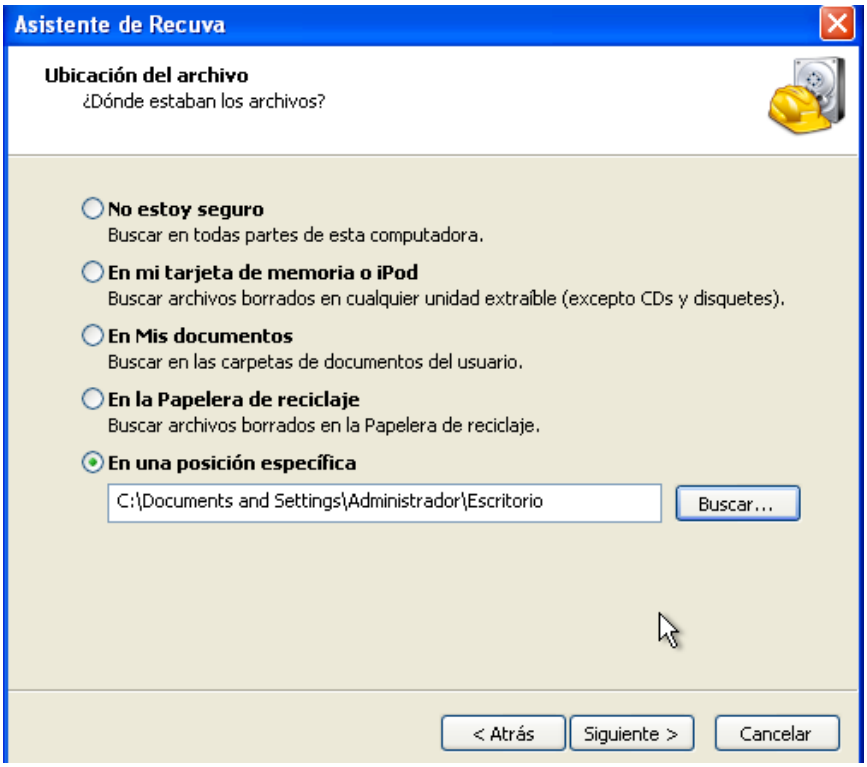
Ahora abrimos el Recuva, y pulsamos sobre siguiente.



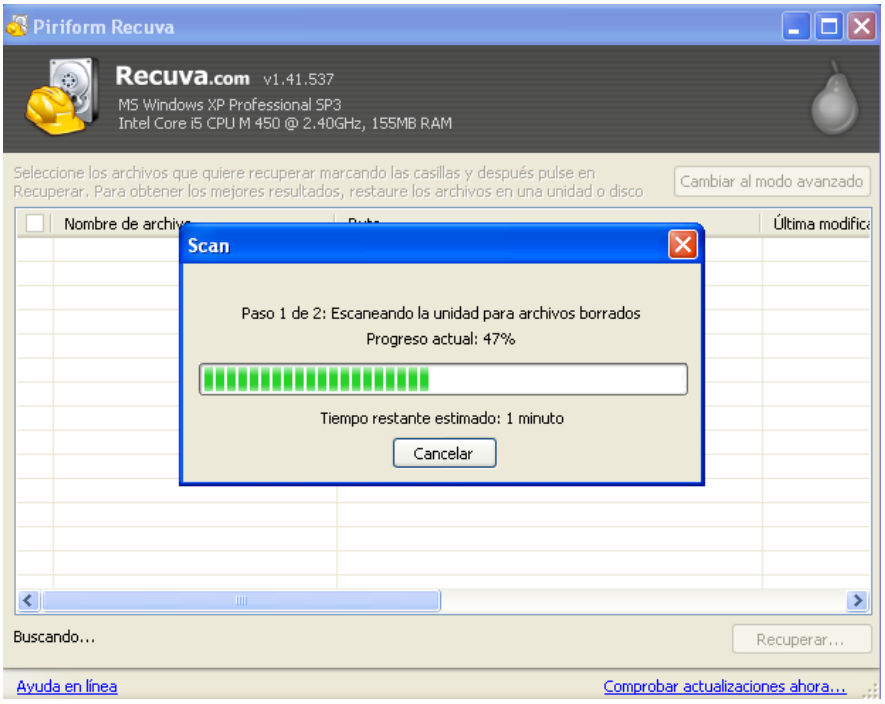
Como no queremos recuperar un tipo de archivo en concreto pulsaremos sobre otros para que se tenga más éxito en el proceso de recuperación:



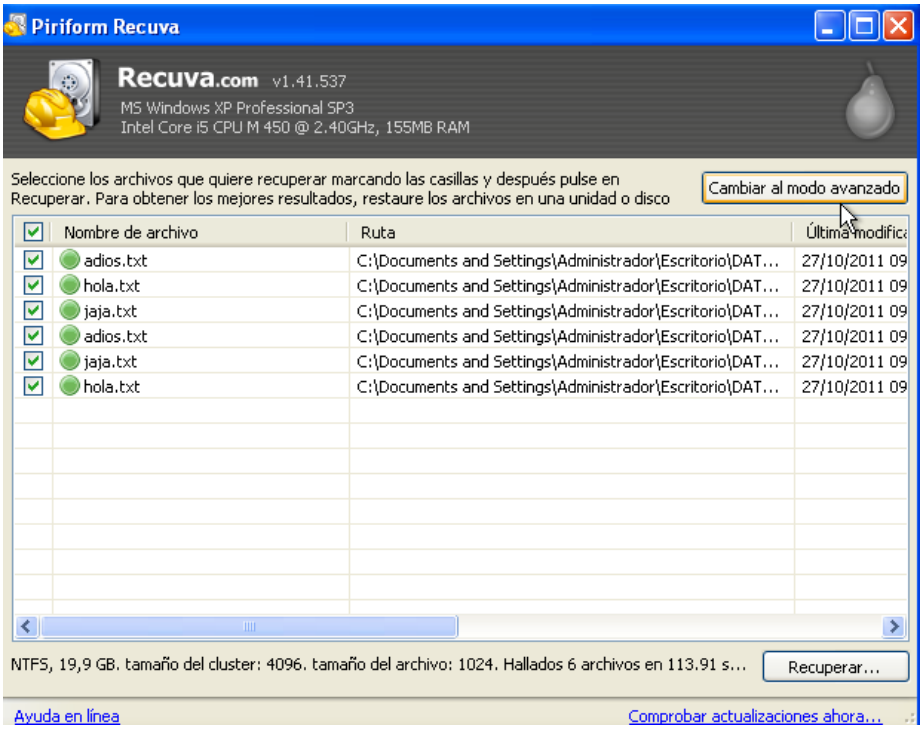
Como nos acordamos de la ruta en la que estaban los archivos, pues seleccionamos el Escritorio, para facilitar la búsqueda.



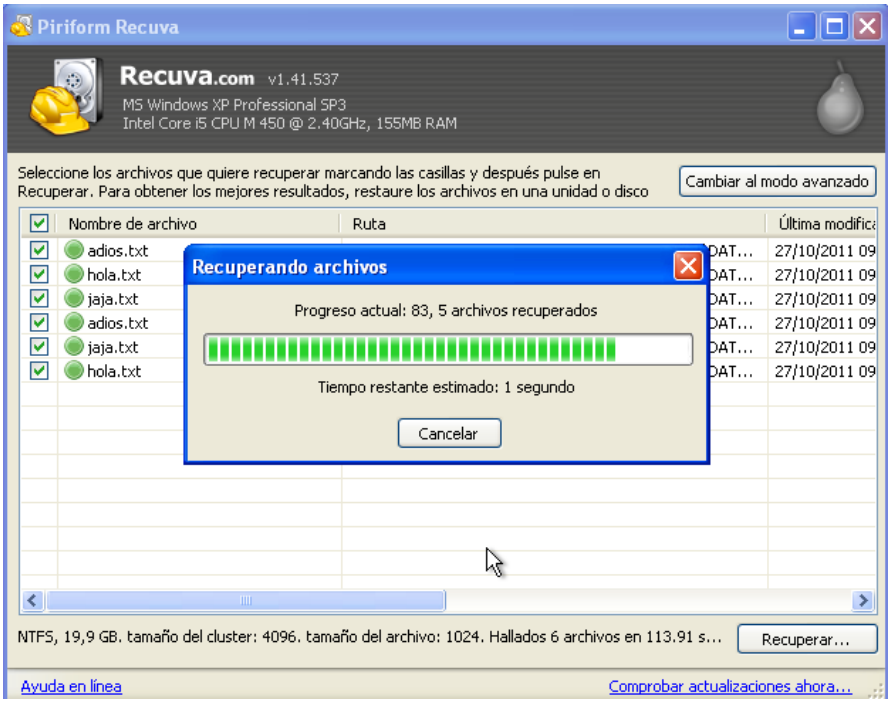
Comenzara a buscar todos los archivos que se hayan borrado en el Escritorio, esperaremos unos minutos.



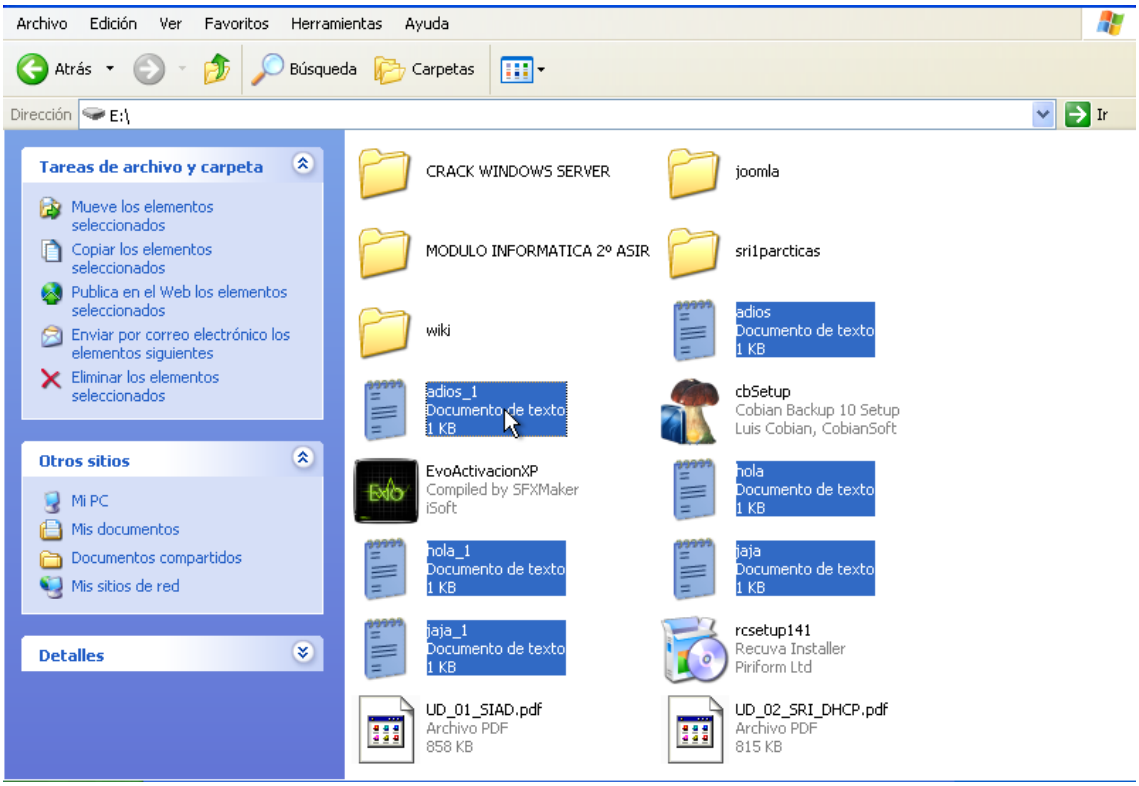
Tras esperar unos minutos, el Recuva nos ha encontrado estos ficheros, que son los que estaban dentro de la carpeta DATOS PRUEBA.



Para recuperarlos seleccionamos todos los archivos y como destino seleccionamos nuestro pendrive:



Podemos comprobar cómo los ficheros los ha recuperado.



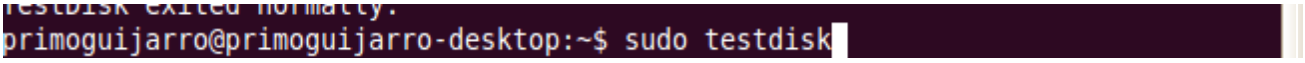
EN Linux

TESDISK

Primero deberemo de Instalar el paquete Testdisk, para ello abrimos el terminal y escribimos:

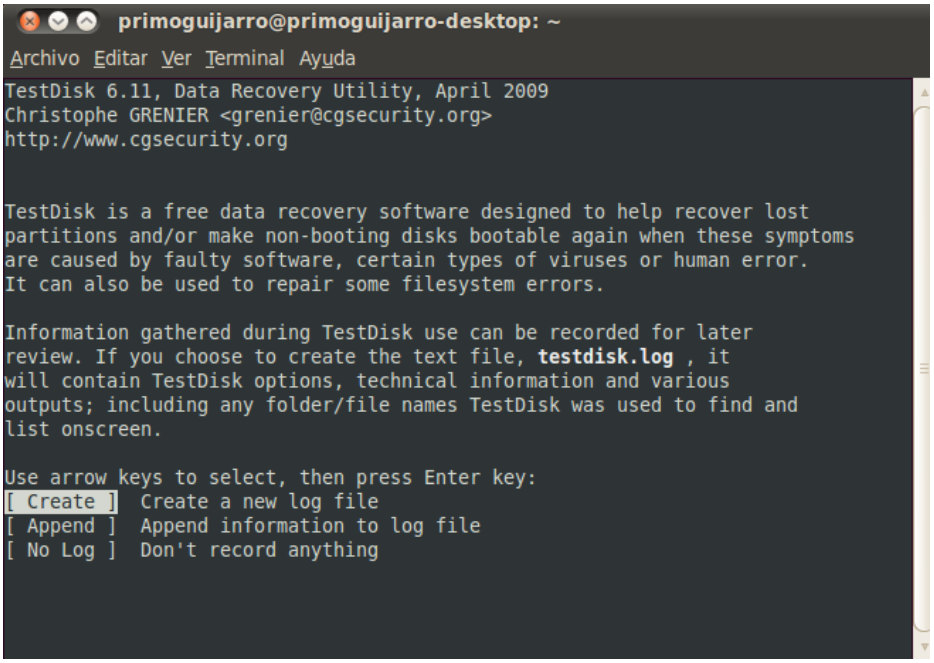
#sudo apt-get install Testdisk

Ahora para ejecutar el testdisk debermos de dirigirnos al terminal e introducir la palabra Testdisk

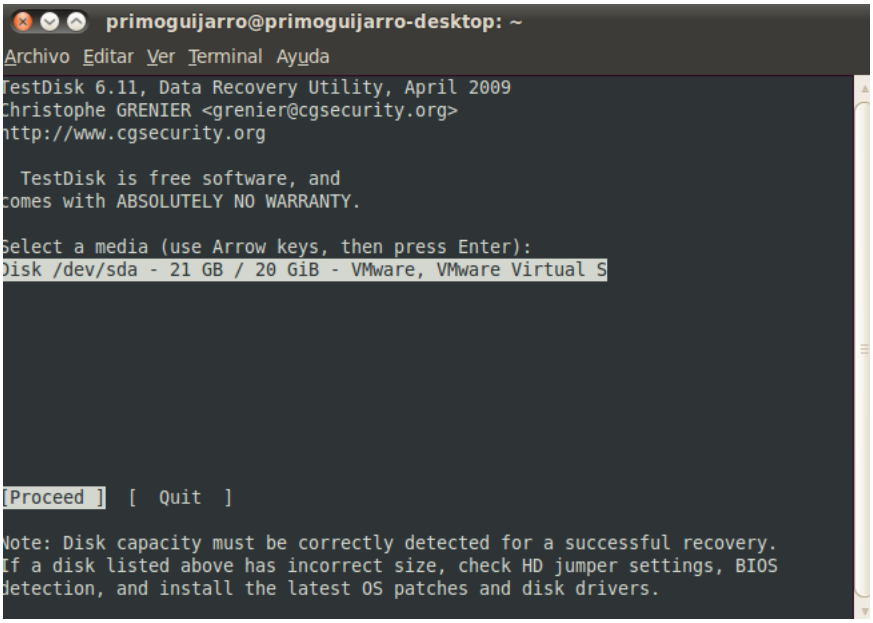


Una vez realizado el paso anterior deberemos de realizar los siguientes pasos para poder restaurar unos datos eliminados:

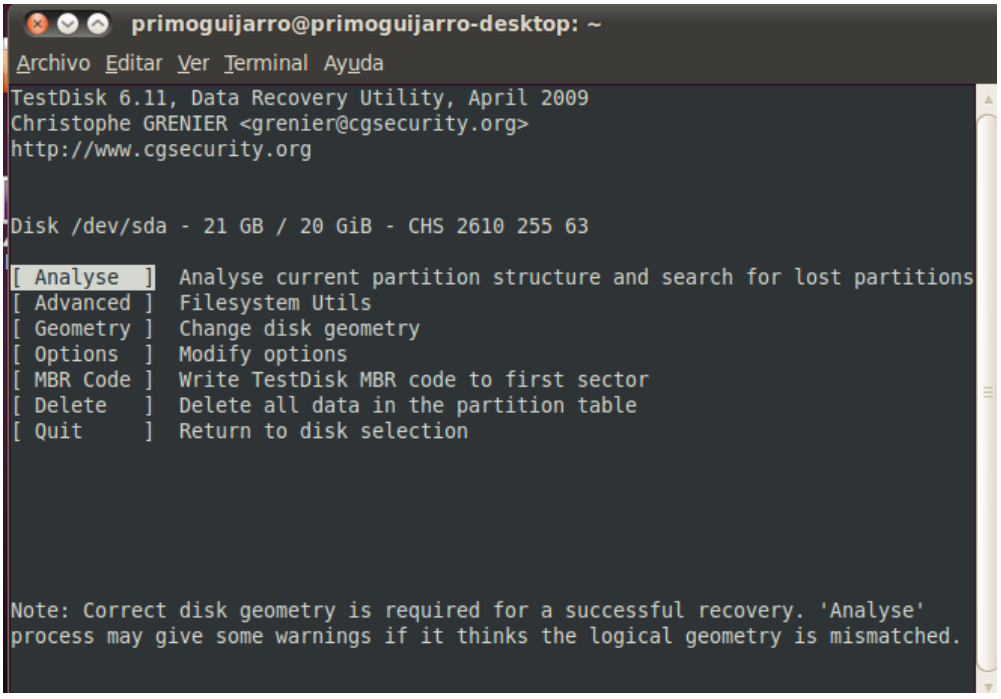
En primer lugar seleccionamos la opción Create para crear un fichero de log.



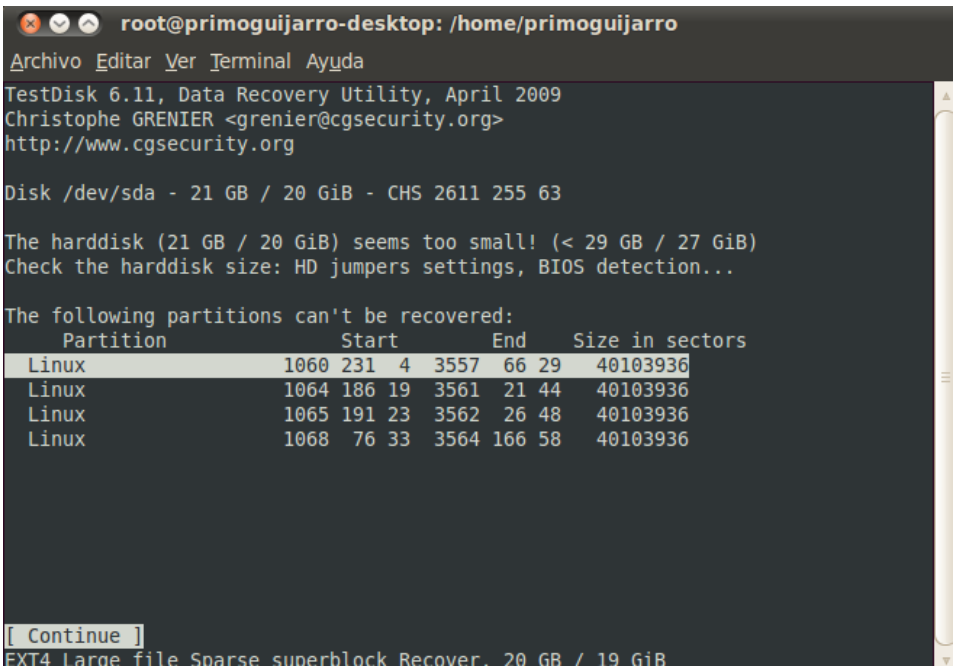
Nos detectara el disco duro, lo seleccionamos y le damos a Proceed para crear el log.



Ahora como no vamos a borrar ninguna partición para que la recupere, entonces analizaremos las particiones del disco duro, seleccionamos Analyse, para que así analice nuestro disco duro en busca de los archivos eliminados.



Nos muestra el análisis, de las particiones que ha encontrado. Donde podemos ver el tamaño de los sectores que tiene cada partición.



FOREMOST

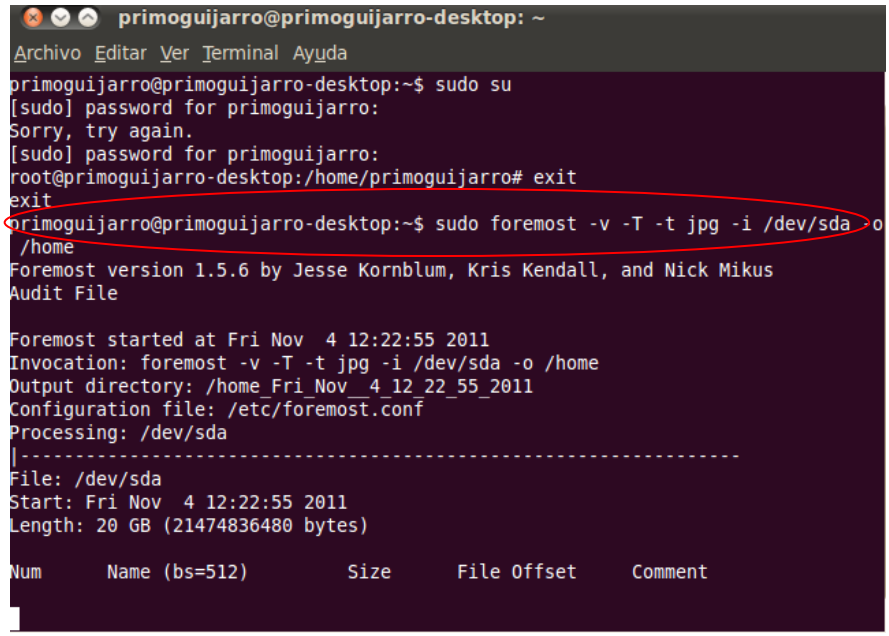
Es una herramienta para recuperación de datos en modo comando.

Para instalarla deberemos de introducir el siguiente comando en el terminal:

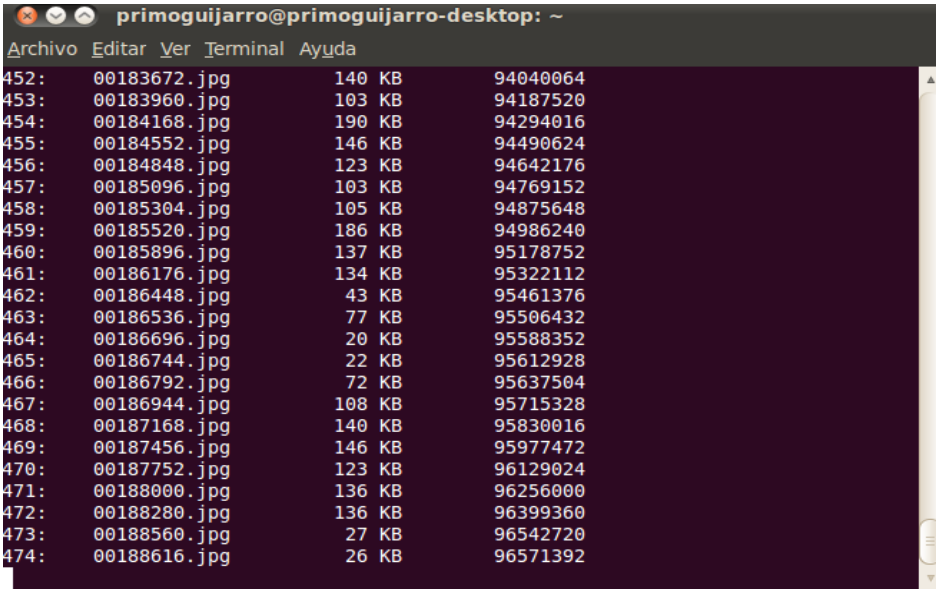
#sudo apt-get install foremost.

Ahora realizaremos un supuesto practico, el cual es el siguiente:

Queremos recuperar todas las imágenes jpg del disco duro local (sda), y queremos que se copien en /home.



Esta operación tardara unos minutos, pero podemos ir comprobando como está encontrando todas las imágenes, junto con su tamaño, y las ira copiando a la ruta de destino /home.



Scalpel

Es otra herramienta de análisis forense que nos permite recuperar ficheros u archivos perdidos.

Para instalarlo introducimos el siguiente comando:

 # sudo apt-get install scalpel

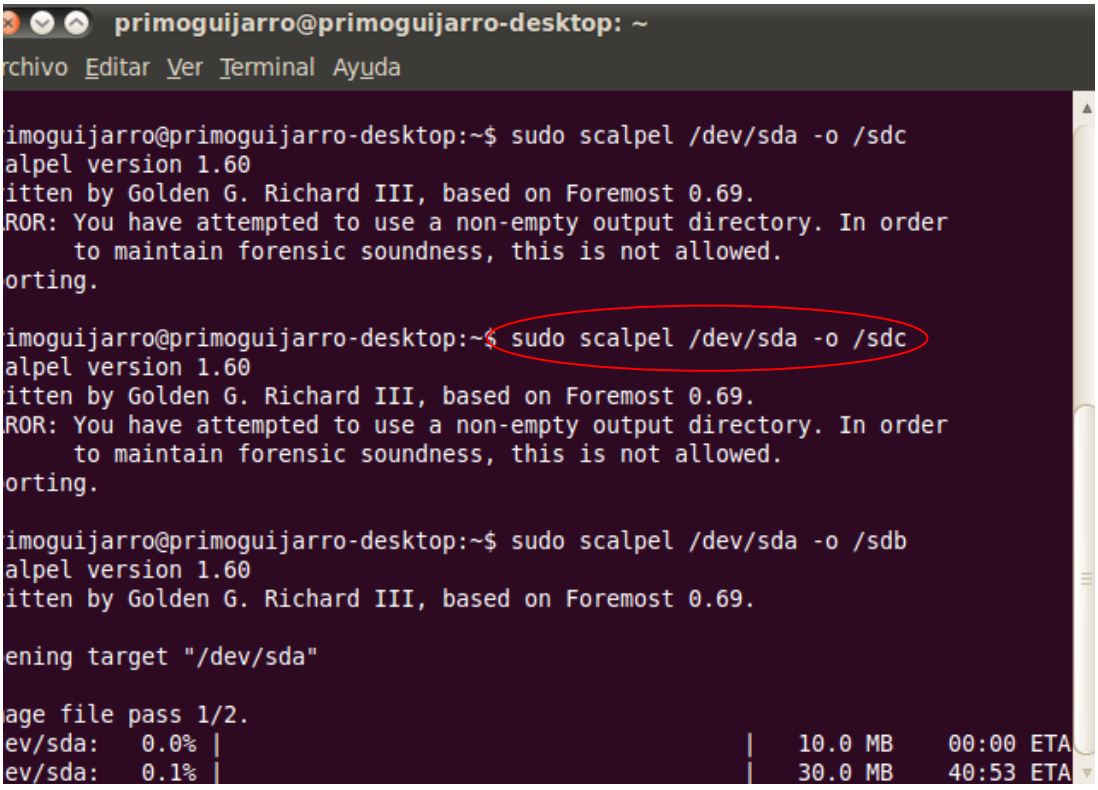
El siguiente escenario es el que queremos recuperar, bien tenemos nuestro disco duro (sda), y queremos que todos los archivos pdf se copien a nuestro pendrive (sdb).

Para que Scalpel, sepa que queremos copiar solamente los pdf vamos al archivo de configuración:

#sudo nano /etc/scalpe/scalpe.conf

Y descomentamos las líneas de pdf.

Ahora escribimos el siguiente comando.



Como podemos comprobar comienza a copiarse los ficheros de /dev/sda a /dev/sdb.

d) Realiza un informe sobre los diferentes programas que existen en el mercado informático que permite crear imagenes de respaldo de tu equipo.

INFORME:

1- Introducción

En este informe haremos un pequeño estudio sobre los principales programas que nos permiten crear imágenes de respaldo.

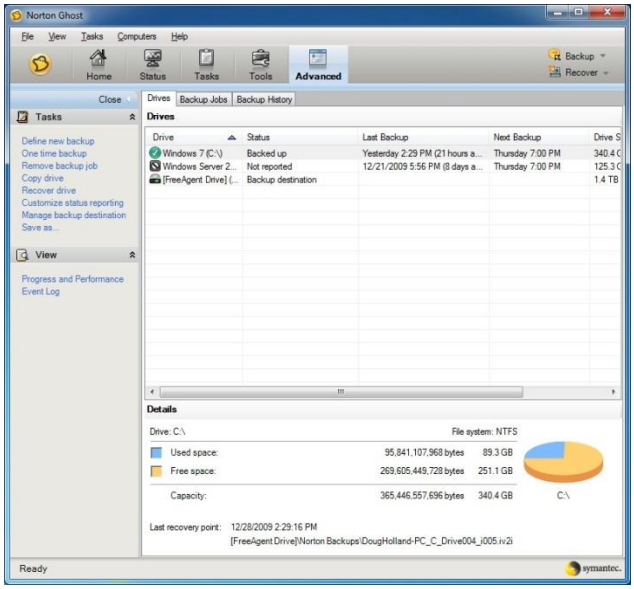
Una imagen del Sistema, es una copia de respaldo de todo el contenido de una partición (incluso de un conjunto de particiones). Ninguna distinción es hecha en el contenido. Se puede decir que una imagen del sistema es una "copia fiel" de la partición en un instante T (siendo T la hora del respaldo).

Los programas que nos permiten crear imágenes de respaldo son muy utiles puesto que nos permite restaurar nuestro equipo a estado anterior; por lo tanto nos otorga una gran seguridad tanto física como lógica ante ataques a nuestros equipos.

2.-Principales programas para crear imágenes de respaldo:

En la actualidad podremos encontrar una gran cantidad de programas para realizar imágenes de respaldo los más importantes son:

- **Norton Ghost:** Es el más popular de todos los programas que nos permiten realizar imágenes de respaldo.



Norton Ghost es una utilidad para realizar copias de seguridad que ha ganado fama con los años convirtiéndose en una de las más reconocidas.

A su facilidad de uso se une su flexibilidad. Norton Ghost permite backups automáticos, incrementales o completos, sin limitaciones en cuanto a dónde se exportarán los datos (discos externos, dispositivos Zip y Jaz, CD/DVD/Blu-Ray,...) y recuperables en cualquier momento, de manera completa o seleccionando unas carpetas y ficheros concretos.

Norton Ghost es el aliado perfecto para evitar perder tus datos por accidente. Recuperará tu sistema operativo y tus documentos aunque no puedas acceder a Windows.

Pros

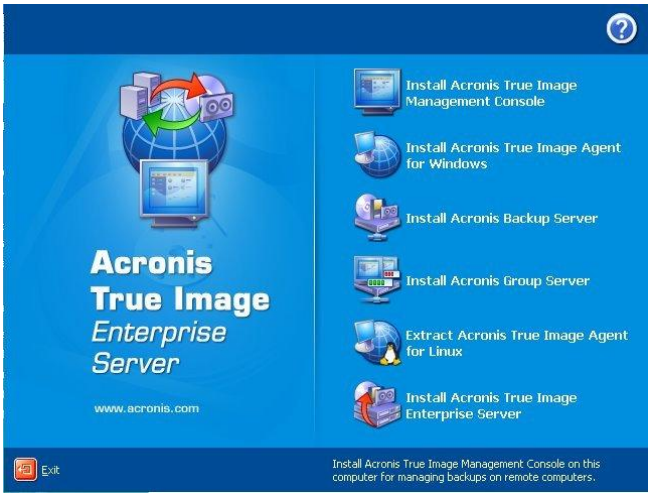
- Fácil de usar
- Copias completas o selectivas
- Tareas programadas
- Muy flexible y configurable

Contras

- No es compatible con particiones Linux ni Mac
- Es de pago

- **Acronis True Image:** Este programa quizás sea el segundo mas conocido del mercado después del Norton Ghost.

Acronis True Image es un completo sistema de creación y gestión de imágenes de disco. Con él podrás crear una copia exacta del contenido de tu disco duro, incluyendo todos los datos almacenados en tu ordenador, el sistema operativo entero, aplicaciones, etc.



Así, con Acronis True Image podrás recuperar totalmente el sistema tras un "accidente" informático, restaurando tu PC tal y como estaba antes del fallo, o simplemente reemplazar ficheros perdidos o dañados extrayéndolos de tu copia.

Acronis True Image permite crear imágenes y recuperarlas de forma muy rápida, con posibilidad de restaurar sólo determinadas carpetas o archivos.

Acronis True Image también permite comprimir la imagen, proteger su contenido mediante contraseña, realizar copias incrementales y más, todo ello además a través de una interfaz de diseño atractivo e intuitivo.

Pros

- Excelente asistente paso a paso
- Compatible con multitud de tecnologías
- Función Try & Decide
- Integración con Windows 7

Contras

- Es de pago

- Clonezilla

Clonezilla LiveCD es una distribución mínima de Linux que se basa en Partition Image, ntfsclone, DRBL y udpcast. Te permite clonar masivamente varios equipos a la vez. A diferencia de Ghost para Unix/Linux LiveCDs (G4L/G4U), Clonezilla guarda y restaura sólo los bloques utilizados en las unidades de disco duro, algo que aumenta la eficiencia de clon. Clonezilla LiveCD fue creada para llevar más poder y competencia en las tareas de partición y clonación de tu disco duro. Clonezilla LiveCD es compatible con los siguientes sistemas de archivos: ext2, ext3, ext4, reiserfs, xfs, jfs, fat16, fat32, ntfs y hfs +. Por lo tanto, puedes clonar los sistemas operativos Linux, Microsoft Windows e incluso Mac Apple basados en Intel. Para otros sistemas de archivos, Clonezilla utiliza dd para volcar la partición entera.

Pros

- Tiene licencia GPL, por lo tanto es gratis
- Es independiente del sistema operativo puesto que es un live CD

- EASEUS Todo Backup

EASEUS Todo Backup es un sistema de copias de seguridad para unidades de memoria completas y particiones.

Cumple varias funciones: clonar discos y particiones, crear copias de seguridad, restaurarlas y comprobar la integridad de las imágenes que crea. Aunque les llamemos copias de seguridad, el nombre adecuado es Ghost, que se

refiere a la copia física byte a byte de un disco.

EASEUS Todo Backup es especialmente útiles cuando se ha sufrido el ataque de un virus o se ha producido un error grave en el sistema operativo. Eso sí, las copias hay que guardarlas...

Leer más

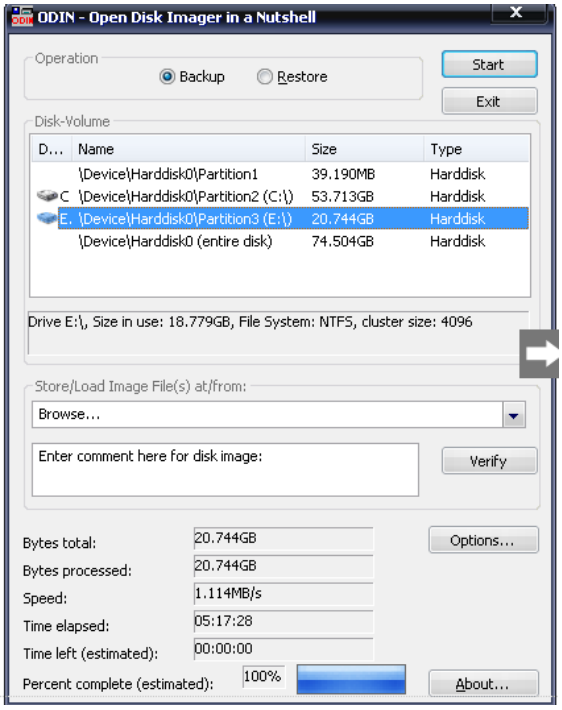
Pros

- Archivo de ayuda completo y fácil de entender
- Buena estructura y diseño de la interfaz
- Fácil de usar

Contras

- Hace falta unos conocimientos mínimos sobre las unidades y particiones

- **ODIN**



ODIN genera una imagen de tu disco duro o de las particiones que contenga.

Así podrás guardar una copia del contenido de tu ordenador en un único archivo y aprovechando el espacio al máximo, ya que comprime la copia en GZip o BZip2, y restaurarla posteriormente.

ODIN copia un disco entero o una única partición, ya sea de todo el contenido o sólo de los bloques usados. Además, la imagen se guarda en la misma carpeta del programa, pudiendo limitarla a un máximo de MB para que quepan en un CD/DVD.

Pros

- Copia todo el disco o una sola partición
- Imagen exacta o sólo del espacio usado
- Puede comprimir la imagen en Gzip o Bzip2

Contras

- Creación de la imagen demasiado lenta
- No deja escoger dónde guardar la copia

3.- Conclusiones.

Una vez realizado un breve análisis de los principales programas que nos permiten crear imágenes de respaldo llegamos a la conclusión de que si no nos importa pagar para obtener un programa de este tipo el más apto para

realizar imágenes de respaldo es el Norton Ghost puesto que de todos lo analizados en el apartado anterior es el que tiene un mayor número de funcionalidades y el más fiable de todos.

Sin embargo si se prefiere una opción gratuita la mejor opción es clonezilla puesto que es un programa muy fiable que nos permite crear imágenes de todas nuestras particiones de una forma eficiente, aunque para el proceso se necesiten conocimientos básicos de particiones es un programa muy recomendable.

e) Realiza un informe con los servicios de almacenamiento que ofrecen las empresas HP, Dell y ESABE:

1- Introducción

En este informe haremos un pequeño estudio sobre los principales características de los servicios de almacenamiento de las empresas HP, DELL y ESABE.

Un servicio de almacenamiento es un servicio que proporciona al ordenador de un usuario conexiones online con un sistema remoto para copiar y almacenar los ficheros de su ordenador. Los proveedores de copias de seguridad gestionada son empresas que suministran este tipo de servicios.

2.- Análisis de las principales empresas que nos otorgan estos servicios:

HP

En estos días, necesita obtener lo máximo de su inversión en almacenamiento; no puede darse el lujo de no hacerlo. Pero sin el conocimiento adecuado, la implementación, diseño, mantenimiento y gestión de su entorno de almacenamiento puede ser complicado y exigir mucho tiempo, en el mejor de los casos, o puede ser peligroso y caro, en el peor. Usted necesita un socio de servicio capaz de suministrar soporte de almacenamiento de extremo a extremo para todo su entorno.

Colabore con HP para atender el almacenamiento del cliente de la mejor forma posible Ya sea que planee una migración compleja, sólo necesite soporte tecnológico básico o precise servicios gestionados completamente, HP ha ayudado a miles de clientes en situaciones similares. Podemos ayudarle también a usted.

Con la ayuda de HP, puede mejorar su entorno de almacenamiento, reducir sus costes y optimizar la gestión del mismo. A diferencia de muchos competidores, tenemos el conocimiento y los recursos para ayudarlo a apoyar y gestionar no sólo su entorno de almacenamiento sino toda su infraestructura de tecnología, incluso servidores, redes, PC de sobremesa, software y mucho más.

Los Servicios de almacenamiento HP le ayudan a hacer funcionar su tecnología, para que así su negocio también pueda funcionar:

- **Operaciones:** Optimice procesos, consolide activos y reduzca costes.
- **Almacenamiento ecológico** Reduzca los costes de energía y refrigeración.
- **Infrastructura:** Aumente el acceso a la información y la entrega de servicios.

- **Centro de datos:** Reduzca los costes operativos y optimice la gestión

HP reconoce la importancia del crecimiento de su capacidad de almacenamiento de datos para su éxito competitivo. Es por eso que ofreceun amplio abanico de servicios de optimización de la infraestructura de almacenamiento que puede ayudarle a:

- Construir una base más sólida y segura para el crecimiento de su negocio
- Reducir los costes y la complejidad del almacenamiento
- Impulsar el ROI a través de una utilización mejorada de los activos
- Minimizar los riesgos de negocio relacionados con el almacenamiento
- Adaptarse rápidamente y de forma más eficiente al cambio del negocio y a la tecnología

Con ofertas de niveles de cobertura y opciones de personalización flexibles, los servicios de optimización de la infraestructura de almacenamiento HP incluyen:

Servicios profesionales de software para la gestión de datos:

Los servicios profesionales de software de HP para las soluciones de gestión de datos son flexibles y ampliables. Podemos asegurar la información crítica de su empresa mediante la creación de un reflejo de los datos en tiempo real entre las matrices de disco local y remota. Además, nuestros servicios pueden ayudarle a gestionar la recuperación de desastres y la replicación de datos, a la vez que mantienen la continuidad en la empresa. Nuestros asesores de servicios analizan su estrategia de copia de seguridad y recuperación, así como su habilidad para cumplir con los requisitos de la empresa y a continuación le recomiendan una solución.

Infraestructura de almacenamiento y servicios de transformación

Su información debe seguir evolucionando. Y los sistemas de gestión de datos de mañana serán totalmente diferentes a los de hoy en día. Los asesores de almacenamiento de HP pueden ayudarle a prepararse para este cambio y optimizar y transformar su almacenamiento. De este modo, pueden ayudarle a aumentar la eficiencia y en la transformación hacia un modelo de TI de servicio centrado.

Los asesores de almacenamiento de HP pueden ayudarle con la alineación, la planificación y el diseño, la implementación y el soporte. HP entiende el centro de datos y puede ayudarle, sin importar dónde se encuentre en el viaje de la innovación.

DELL

Además de la consultoría de infraestructura, Dell brinda un conjunto de ofertas sólidas de soporte durante el ciclo de vida, que incluyen soporte y mantenimiento de sistemas.

Los productos y servicios de Dell™ están diseñados para acelerar la implementación, de modo que pueda dedicar menos tiempo a la configuración y más tiempo a disfrutar de los beneficios de su solución:

- Los arreglos de la serie PS de Dell EqualLogic™ están diseñados para que se puedan implementar, configurar y poner en funcionamiento en menos de una hora.
- Los arreglos Dell | EMC CX4 pueden migrar datos sin interrupciones a diferentes tipos de unidades lógicas (LUN) y discos, lo que le permite implementar la mejor solución para sus cambiantes necesidades empresariales y de uso de aplicaciones sin tener tiempo de inactividad.
- Las opciones de servicio modular de Dell pueden ayudarlo a implementar una solución de respaldo simple para trasladar todo su centro de datos, lo que le ahorrará tiempo, dinero y recursos.

Algunos de nuestros servicios de implementación de almacenamiento incluyen:

- Traslados de almacenamiento y centro de datos de implementación de solución iSCSI
- Configuración e implementación de host VMware® ESX
- Implementación de soluciones de respaldo e implementación de software de replicación
- Servicios de migración de datos
- Implementación de SAN/DAS/NAS de Dell | EMC

La gran familia de soluciones de almacenamiento de Dell puede abordar las necesidades específicas y los requisitos complejos de las empresas de la actualidad. Desde las unidades de estado sólido (SSD) de baja latencia hasta la conectividad Ethernet de 10 Gigabits (10 GbE) de ancho de banda alto, Dell puede ayudarlo a alinear el valor de sus datos y aplicaciones con el rendimiento de almacenamiento que requieren. Cada solución tiene características que le permiten aprovechar al máximo su almacenamiento:

- El conjunto de funciones inteligentes con todo incluido de la serie PS de Dell EqualLogic™ permite funciones de almacenamiento en el nivel empresarial para organizaciones de prácticamente todos los tamaños.
- Dell Compellent™ Storage Center proporciona datos fluidos, que brindan lo mejor en eficiencia, agilidad y resistencia para cargas de trabajo que abarcan centros de datos principales y departamentales.
- Las funciones inteligentes de administración, junto con las opciones de unidades amplias, como SSD de baja latencia, unidades SCSI serial (SAS) de alto rendimiento y unidades seriales ATA (SATA) de gran capacidad, le

permiten organizar en niveles sus datos según sus necesidades empresariales.
- La integración de los niveles de aplicaciones con nuestros socios de software ayuda a garantizar la disponibilidad de sus aplicaciones esenciales

Principales características del servicio de almacenamiento DELL

Aceleración del tiempo de recuperación

El respaldo de datos es crucial para las organizaciones de todos los tamaños. Al considerar las opciones disponibles, respaldar y restaurar datos desde un disco generalmente es más rápido, más fácil y más confiable que respaldar datos desde una cinta. La cinta funciona sobre la base de un acceso secuencial, a diferencia de las capacidades de acceso aleatorio del disco. Este acceso aleatorio permite respaldos y restauraciones mucho más rápidos desde el disco en comparación con la cinta. Debido a los volúmenes de datos en aumento que se deben respaldar y proteger, además de la reducción de los períodos de respaldo, muchos departamentos de TI han agregado o se han cambiado a respaldos basados en discos. Sin embargo, en el caso del almacenamiento a largo plazo, tenga en cuenta que el respaldo en cinta ofrece una tecnología reconocida que puede ser muy rentable.

Almacenamiento a nivel de los archivos en su red

El almacenamiento adjunto en red (NAS) es un servidor de almacenamiento especializado con su propia dirección IP, que está disponible para varios clientes y servidores en una red de área local (LAN) o red de área extendida (WAN). Los protocolos de comunicación de red preinstalados se habilitan para que los clientes y servidores de entornos heterogéneos con diferentes sistemas operativos puedan leer y escribir datos en el servidor NAS. Las organizaciones pueden agregar arreglos de almacenamiento en disco, unidades de cinta o automatización de cintas a un servidor NAS de archivos/impresión, lo que permite simplificar las operaciones de administración y respaldo, mejorar la utilización de los recursos de almacenamiento y actuar como una plataforma centralizada para la ampliación rentable. Una puerta de enlace NAS se conecta a los arreglos de almacenamiento en disco o a los sistemas de automatización de cintas en una red de área de almacenamiento (SAN).

Optimización de la administración de información no estructurada

La información solo es valiosa si es accesible, pero hacer que los datos estén disponibles para el cumplimiento, los requisitos de gestión e inteligencia empresarial puede ser engorroso y costoso. Con las soluciones de almacenamiento de objetos Dell™, por fin podrá terminar con el dilema entre el costo y la accesibilidad y, a la vez, simplificar la administración de datos y ampliar la capacidad.

La plataforma de almacenamiento de objetos Dell DX está diseñada para acceder, almacenar y distribuir hasta miles de millones de archivos u otro contenido digital, desde el archivado hasta las ofertas de servicios en la nube. La plataforma utiliza una arquitectura de ampliación entre pares elegante, autoadministrada, probada para el futuro y rentable, que se basa en plataformas galardonadas de servidor en rack, basadas en estándares x86 de Dell. La plataforma está optimizada para almacenamiento e incluye un software completamente integrado para proporcionar una solución integral completa. Debido a que un tamaño no se adapta a todos los casos, Dell está creando soluciones para abordar mercados horizontales y verticales, como atención médica, correo electrónico y archivado de archivos, almacenamiento en la nube, eDiscovery y administración de contenido empresarial. Como parte de este desarrollo de soluciones, Dell está cultivando un ecosistema de proveedores de software independientes (ISV) que pueden aprovechar la plataforma de almacenamiento de objetos DX de Dell.

Consolidación y ampliación de su infraestructura de almacenamiento

Una red de área de almacenamiento (SAN) es una red de dispositivos de almacenamiento compartidos, como arreglos de almacenamiento en disco y automatización de cintas. La arquitectura de una SAN permite que los recursos de almacenamiento se compartan entre varios servidores de una red de área local (LAN) o red de área extendida (WAN). Debido a que los datos almacenados se administran en arreglos dedicados, la potencia de procesamiento de los servidores se optimiza para las aplicaciones empresariales, y se puede proporcionar capacidad de almacenamiento a los servidores y a las aplicaciones de acuerdo a sus necesidades. Las SAN también pueden mejorar la protección de datos, la continuidad empresarial y la capacidad de ampliación en comparación con otras opciones, como el almacenamiento adjunto directo (DAS). Finalmente, el almacenamiento en SAN puede simplificar la agrupación de datos por niveles y puede llevar a mejorar el uso de recursos.

ESABE

Byte pass es un servicio innovador de backup completo y eficiente que permite una recuperación inmediata y reciente de sus datos críticos. Es una solución flexible y económica que puede crecer con el negocio.

Resumen de las ventajas de byte pass:

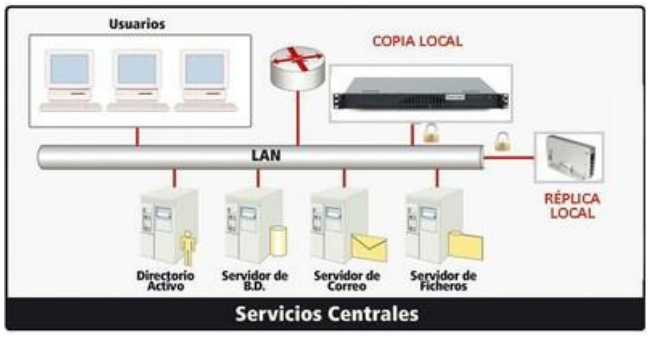
- Servicio totalmente gestionado por ESABE.
- Copia Local y/o Online
- Réplica Local y/o Remota
- Copia de sistemas y datos
- Servicio completo (Servicios Centrales, Delegaciones y móviles)
- Servicio eficiente (Copia + externalización, gestión, custodia y destrucción de soportes)
- Custodia en instalaciones de seguridad con Servicio BUNKER.
- Definición, Configuración e Instalación por personal de ESABE.
- Gestión de políticas de respaldo y recuperación centralizadas
- Monitorización de la plataforma local y remota.
- Servicio de respaldo de puestos de trabajo y de oficinas distribuidas
- Salvaguarda de versionado de documentos, ficheros e imágenes de sistema.
- Transmisión remota segura y cifrada (AES-256). Tanto local como remota.
- Soporte online 8 x 5 por personal especializado.

Copia Local

Mediante un dispositivo físico (appliance), conectado a la red del cliente, **gestionado por ESABE** y compuesto por servidor, discos y software, se consigue de una forma **automática:**

- **Copiar** todos los cambios producidos en los archivos informáticos (ficheros, bases de datos, correo, directorio activo y archivos abiertos).

- **Mantener distintas versiones** de los archivos respaldados.
- **Recuperar inmediatamente** la situación más reciente a cualquier contingencia. Disponer de un mecanismo de**recuperación predictible** (Fichero: 30'', Disco: 30').



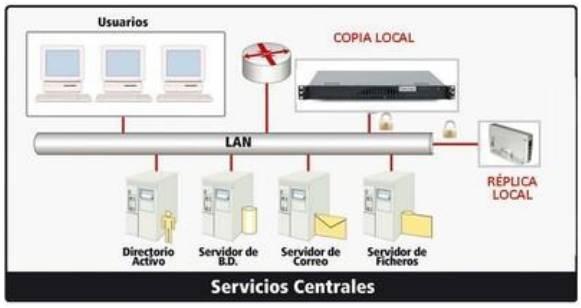
- **Restaurar completamente la imagen del Sistema** con la opción Bare Metal Universal Restore.

Réplica Local

La transmisión de información a través de redes de comunicaciones exige disponer de anchos de banda adecuados. En casos en los que no se disponga de esa capacidad, byte pass ofrece la posibilidad de asegurar también la protección frente a desastres, posibilitando la realización de una réplica local, con similares características a la réplica remota y que sea externalizable.

Esta funcionalidad permite:

- **Tener una copia externalizable en disco**, de los datos críticos y con cifrado seguro.
- Disponer de un mecanismo de recuperación en caso de pérdida de los datos del appliance local.



- Disponer de un **Soporte Técnico que nos ayude en la recuperación.**
- **Utilizar los servicios logísticos de ESABE** para transportar y custodiar los discos de réplica en un búnker de seguridad e **intercambiarlos periódicamente** (semana) para garantizar su actualización.

Réplica Remota

Con la Copia Local ya tenemos la mejor protección para respaldo. Ahora debemos asegurarnos que, en caso de desastre, también tengamos la mejor

protección. Para ello, byte pass ofrece esta opción con otro dispositivo gestionado por ESABE, en un Centro de Proceso de Datos seguro, que permite:

- **Tener una copia remota** de los datos críticos y **con cifrado seguro.**
- **Utilizar la logística y transporte de ESABE** para entregar una copia utilizable en el Centro de Proceso de Datos del cliente.
- Disponer de un mecanismo de **recuperación predictible** (Online y en menos de 24 horas).
- Disponer de un **Soporte técnico que nos facilita la recuperación.**

Copia Online

De forma totalmente automática, el servicio de Copia Online de *byte pass*, permite:

- **Hacer copias de seguridad frecuentes** de forma programada desde cualquier dominio de Internet.

- **Tener siempre una copia cifrada** de los archivos más confidenciales fuera de los Sistemas Corporativos de su empresa.
- **Recuperar su Copia de Seguridad** sobre cualquier ordenador, conociendo su clave única de cifrado.

Para utilizar este servicio, sólo se requiere una línea ADSL, no se necesita una infraestructura informática o conocimientos de IT. Es una solución ideal para Pymes, autónomos, oficinas o delegaciones sin recursos informáticos, trabajadores con mucha movilidad geográfica y información de alta confidencialidad.

Características y Ventajas

- **Más seguro:** Los datos se encriptan automáticamente con una clave privada que solamente conoce el usuario. La clave utilizada es AES 256, similar a las que utilizan las instituciones bancarias.
- **Más rápido:** Se hace una primera copia y posteriormente sólo se transmiten los cambios. Este sistema combinado con una gran capacidad de compresión, hace que las copias diarias se realicen en tan solo unos minutos.
- **Conexión Internet:** Solamente necesita una conexión ADSL para transmitir los datos a copiar. Funciona tanto en **ordenadores personales como en Servidores** con entorno Microsoft, Linux, Mac, NetWare y Unix.
- **Copia de Datos:** El sistema está orientado solamente a la Copia de Datos, no del sistema. Es decir, de aquella información crítica de la empresa que no depende del sistema operativo y que no podemos perder bajo ningún concepto. La copia se puede realizar de forma planificada o bien de forma continua.
- **Cumple con la Ley:** CCO cumple con lo que indica el RD 1720/2007 que desarrolla la LOPD, sobre los datos de nivel alto (copia diaria, externalización y cifrado).
- **Recuperación** de su Copia de Seguridad sobre cualquier ordenador, conociendo su clave única de cifrado, 24 horas al día, a través la web.

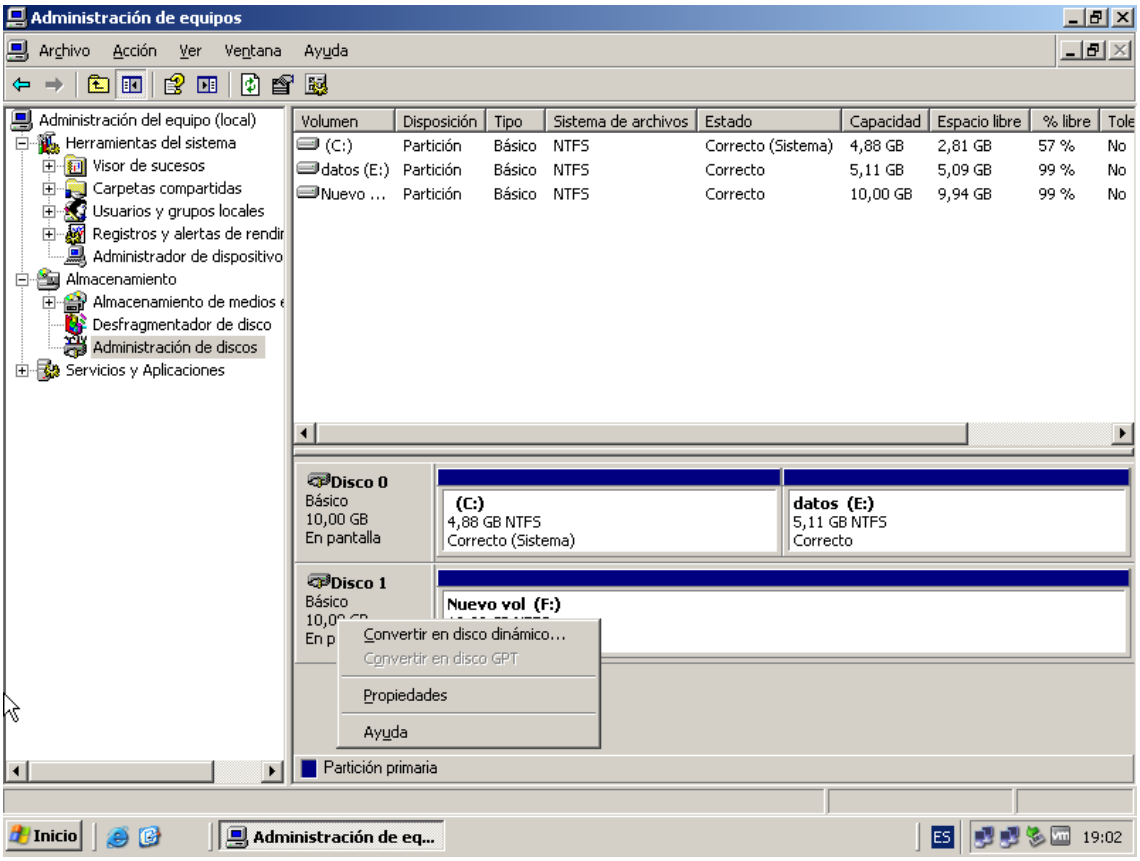
3.-CONCLUSIÓN

Después de realizar un análisis intensivos de los principales servicios de almacenamiento podemos llegar a la conclusión de que la empresa que nos ofrece las mejores soluciones en lo referente a servicios de almacenamiento es ESABE puesto que sus características son muy atractivas y nos permiten muchas funciones que no se encuentran disponibles en las otras empresas del sector.

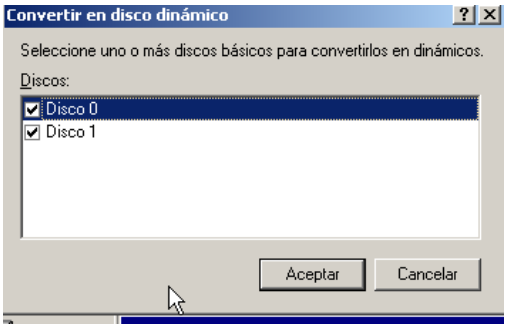
f) Realizar en un entorno simulado un medio de almacenamiento RAID 1 con máquinas virtuales Windows Server.

RAID1

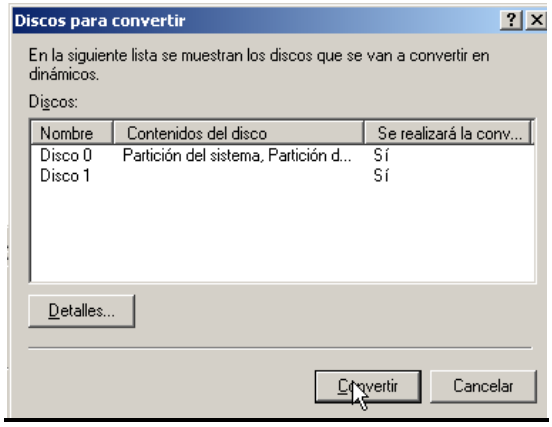
Para realizar un raid en primer lugar deberemos de convertir los discos duros que tenemos en nuestros equipos en discos dinámicos. Para ello nos dirigimos al administrador de equipos y posteriormente al administrador de disco. Una vez allí seleccionamos los discos duros que deseamos convertir en dinamicos y seleccionamos la opción convertir en disco dinámico:



Ahora nos aparecerá una pestaña en la que deberemos de seleccionar los discos que deseamos convertir en dinámicos:

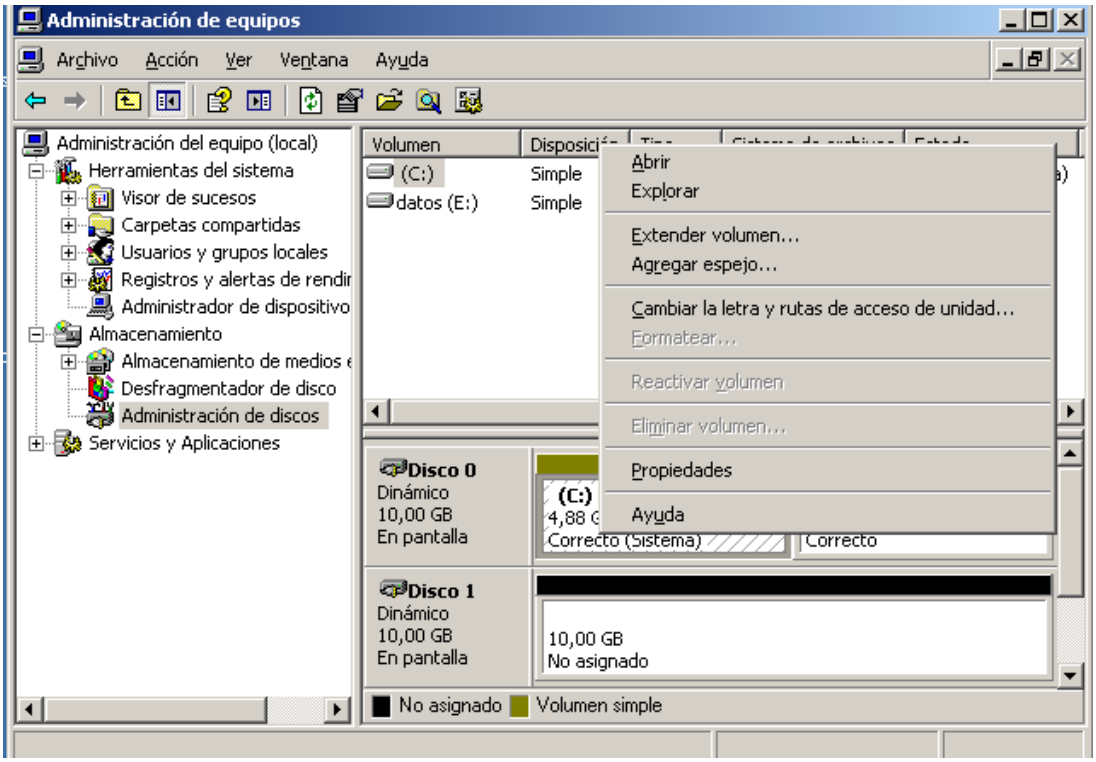


En esta imagen seleccionamos la opción convertir para que de comienzo el proceso de conversión:

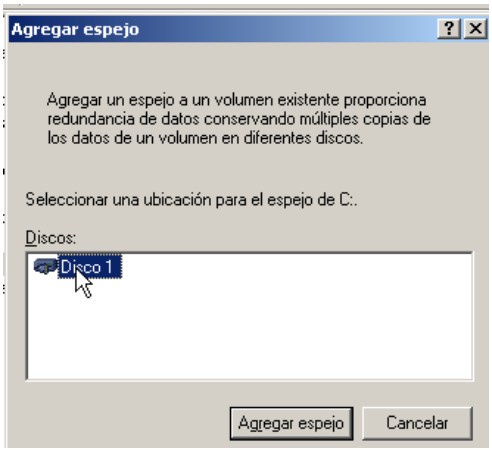


Ahora se reiniciara nuestro ordenador para que se apliquen los cambios.

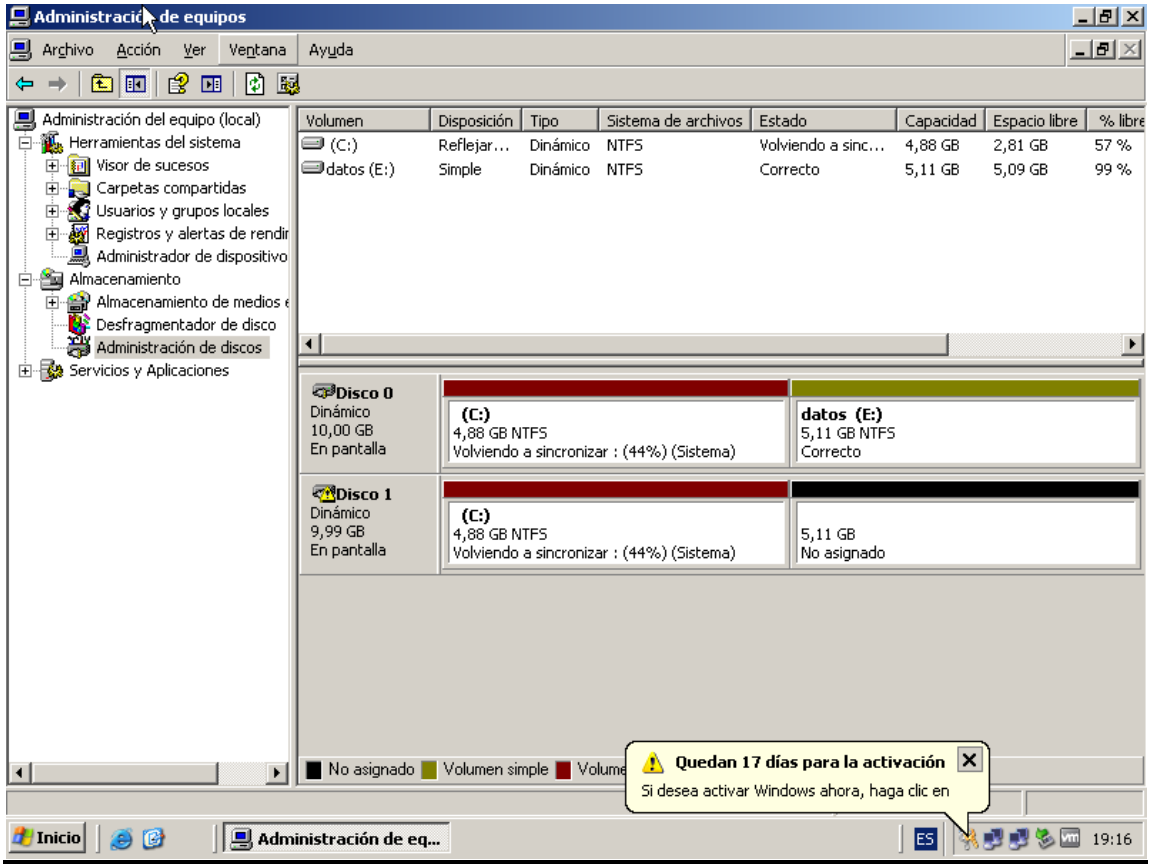
Una vez convertidos los discos en dinámicos deberemos de dirigirnos al administrador de discos y una vez allí seleccionamos la partición de la que deseamos crear el raid 1 y pulsamos botón derecho y elegimos la opción agregar espejo:



Ahora deberemos de elegir el disco que queremos utilizar para usar el RAID 1 y pulsamos agregar espejo:



Ahora se realizara el proceso de sincronización de los datos:



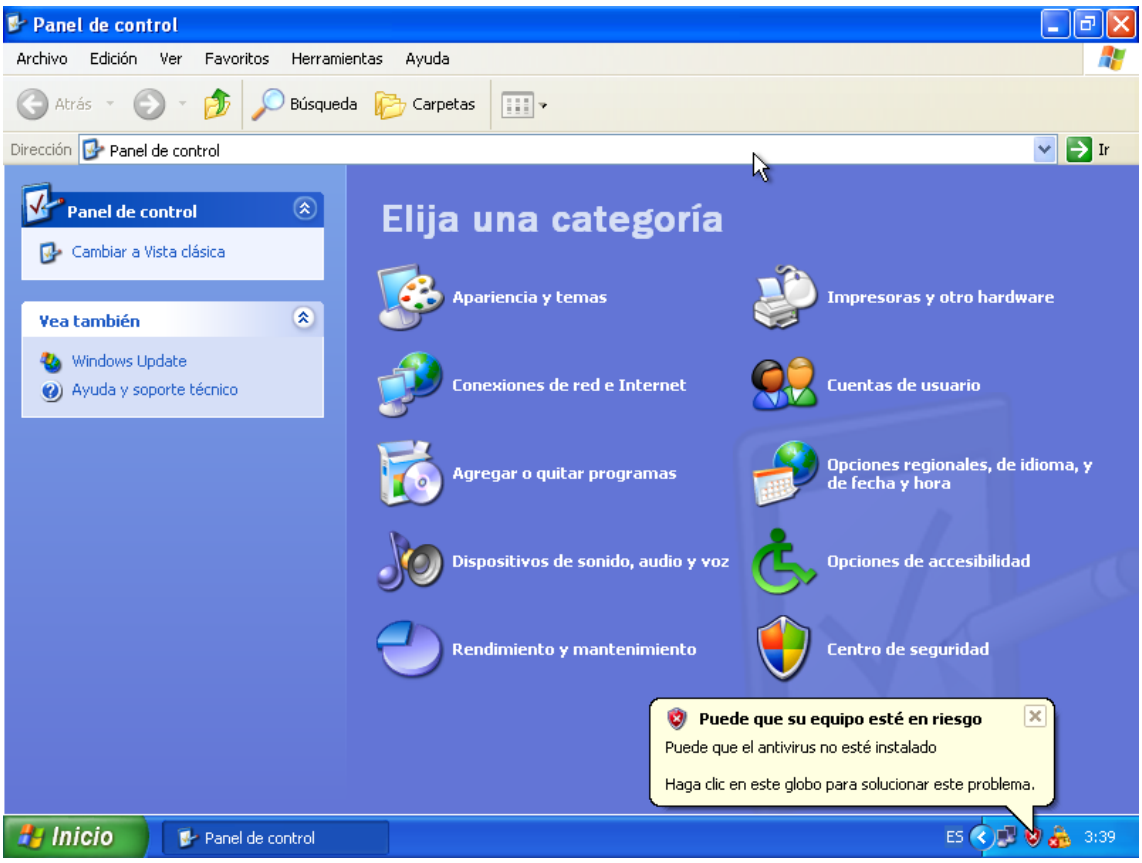
Como conclusión podremos probar su funcionamiento eliminando un HDD del raíz y comprobar que nuestro sistema funciona perfectamente.

g) Control de acceso lógico: Realiza la creación de una cuenta de usuario y su contraseña (política fuerte de contraseñas - modo comando y modo gráfico) que permite posteriormente acceder o no al sistema en sistemas Windows y sistemas GNU/Linux .

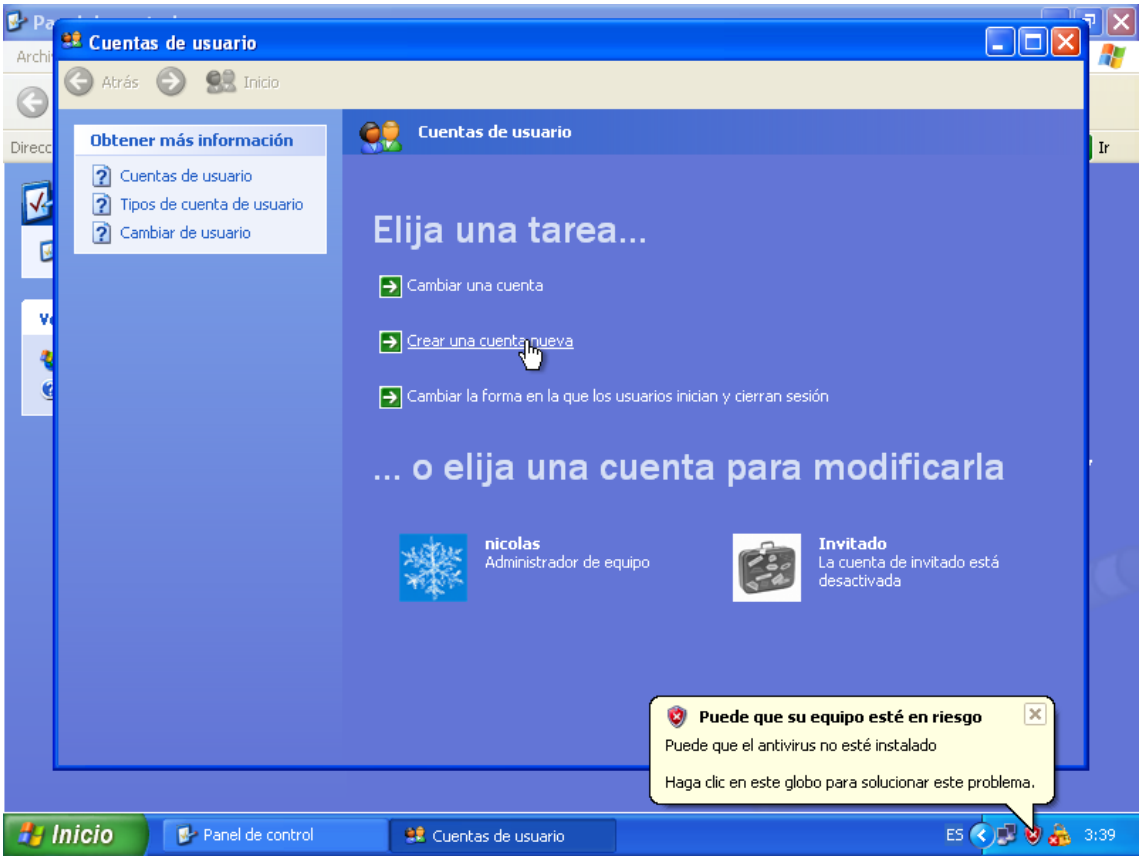
EN XP

Modo grafico:

Para crear una cuenta de usuario en primer lugar nos deberemos de dirigir al panel de control y posteriormente deberemos de dirigirnos a la sección cuentas de usuarios:

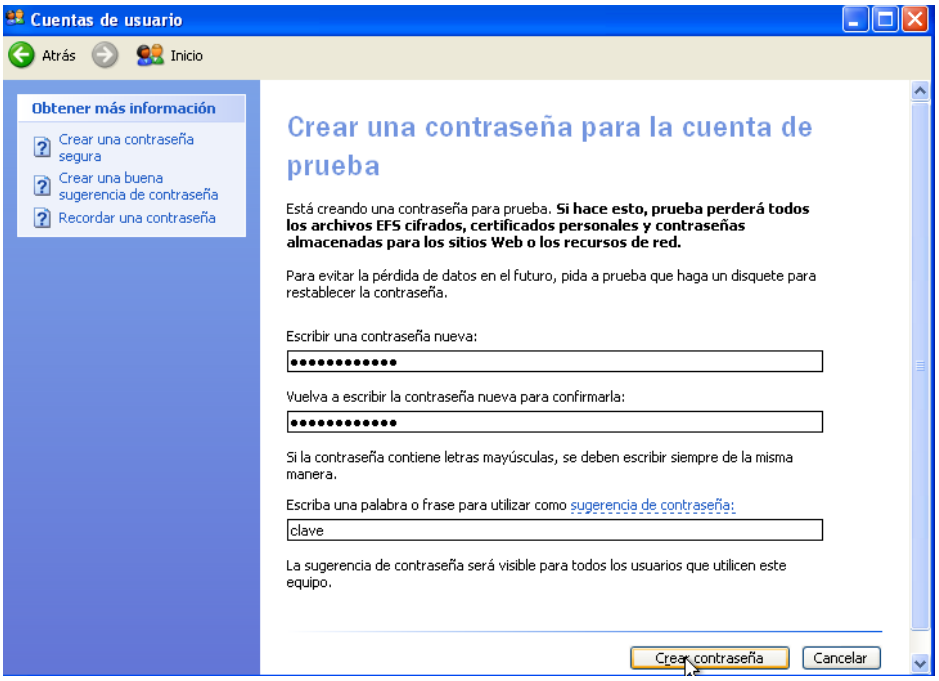


Una vez allí deberemos de seleccionar la opción crear una cuenta nueva:

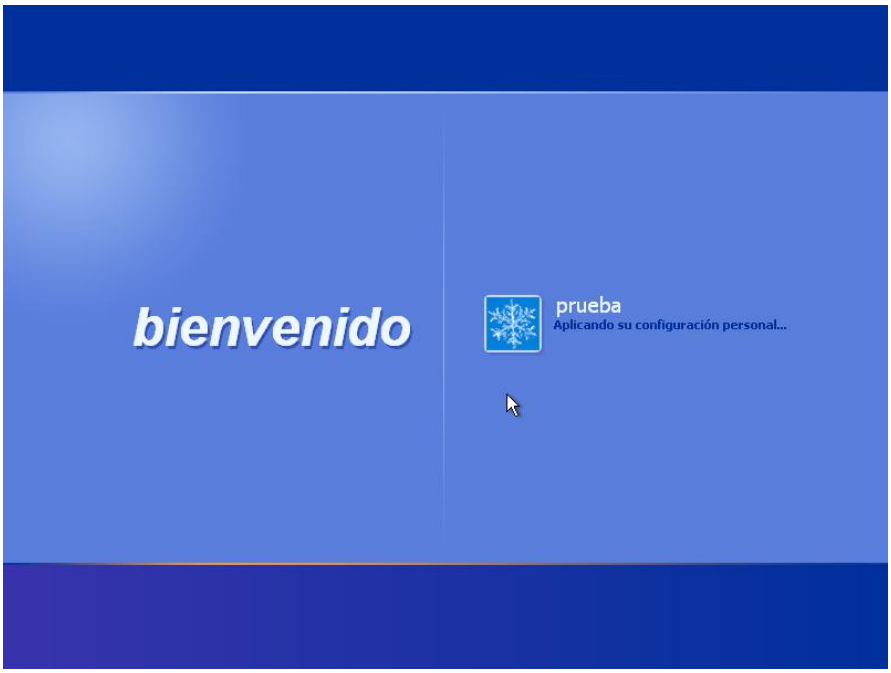


Una vez creada la cuenta deberemos de proceder a establecerme una contraseña, para ello pulsamos sobre la cuenta prueba y seleccionamos la opción establecer contraseña:

Ahora procederemos a establecer una contraseña segura en nuestro caso la contraseña elegida en C1av3-12E45 puesto que tiene mayúsculas minúsculas, números y caracteres especiales. Una vez introducida la contraseña pulsamos sobre la opción crear contraseña:



Ahora cerramos sesión y observaremos que podremos acceder a equipos con la cuenta creada sin ningún error:



Modo comando:

Para crear un usuario en modo terminal en Windows deberemos de introducir el siguiente comando en la consola:

Donde prueba1 es el nombre de usuario y C1av3-12E45 es la contraseña para ese usuario.

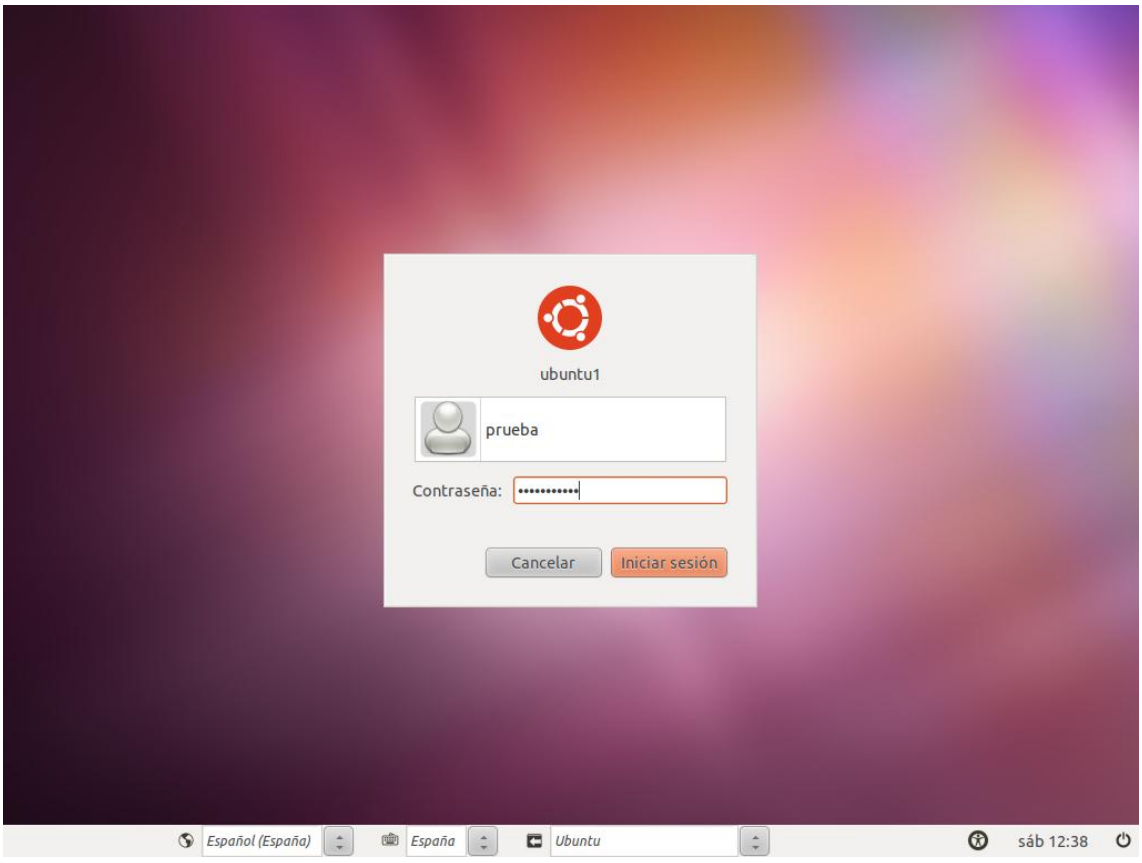
EN LINUX

Modo comando

Para crear una cuenta de usuario con una política de contraseña fuerte en Linux deberemos de dirigirnos al terminal e introducir el comando adduser prueba para crear el usuario prueba, una vez introducido el comando deberemos de introducir la contraseña en nuestro caso será C1av3-12E45.

```
root@ubuntu1:/home/niko# adduser prueba
Añadiendo el usuario `prueba' ...
Añadiendo el nuevo grupo `prueba' (1001) ...
Añadiendo el nuevo usuario `prueba' (1001) con grupo `prueba' ...
El directorio personal `/home/prueba' ya existe.  No se copiará desde `/etc/skel
'.
adduser: Aviso: El directorio personal «/home/prueba» no pertenece al usuario qu
e está creando.
Introduzca la nueva contraseña de UNIX:
Vuelva a escribir la nueva contraseña de UNIX:
passwd: contraseña actualizada correctamente
Cambiando la información de usuario para prueba
Introduzca el nuevo valor, o presione ENTER para el predeterminado
        Nombre completo []:
        Número de habitación []:
        Teléfono del trabajo []:
```

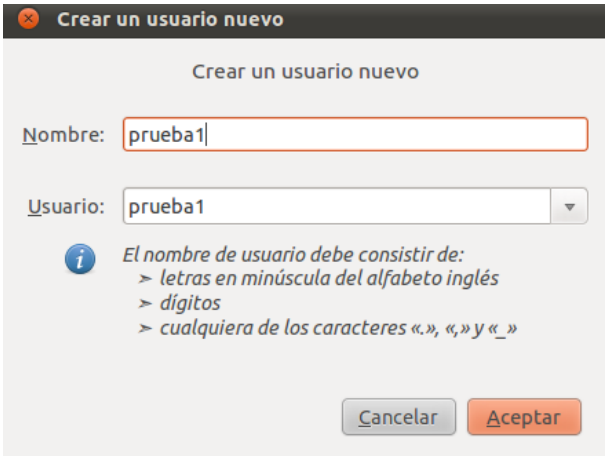
Una vez creado el usuario prueba cerramos sesión en nuestro equipo y comprobaremos que podemos acceder con el usuario creado sin problemas:



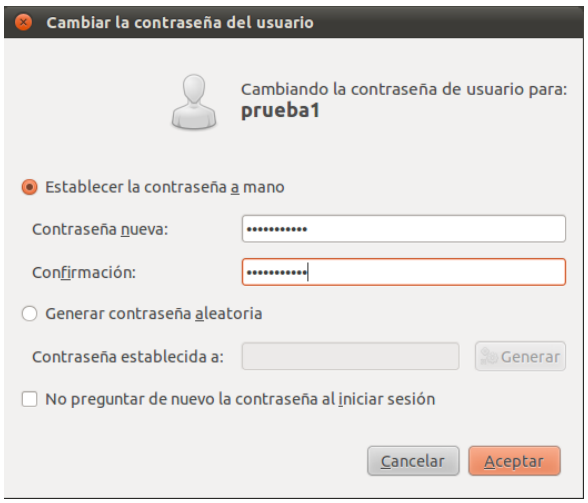
Modo Gráfico:

En primer lugar nos dirigimos a los ajustes de usurario y pulsamos en la opción añadir:

Ahora introducimos el nombre de usuario deseado:



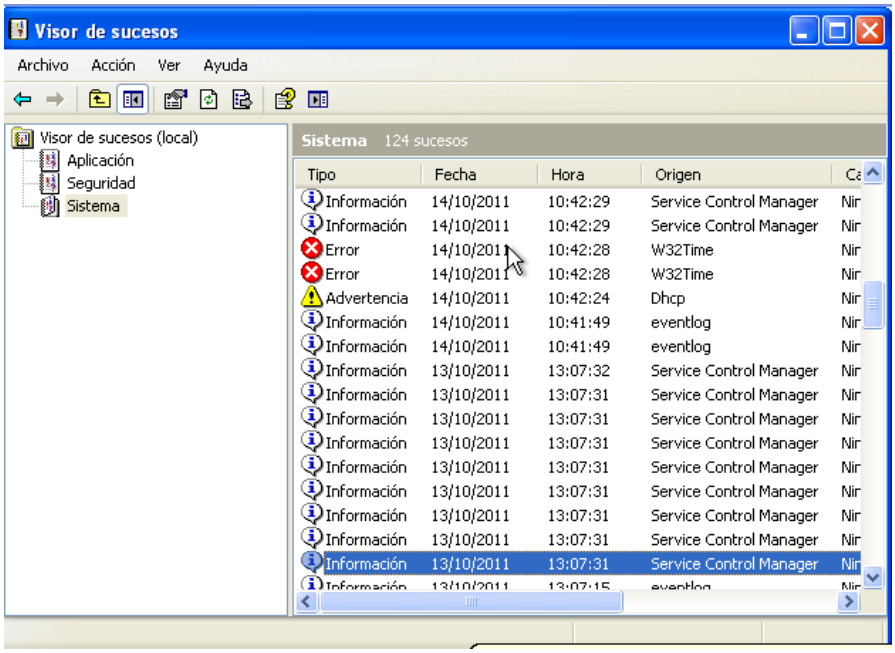
Ahora por ultimo deberemos de introducir la contraseña deseada, en nuestro caso C1av3-12E45:



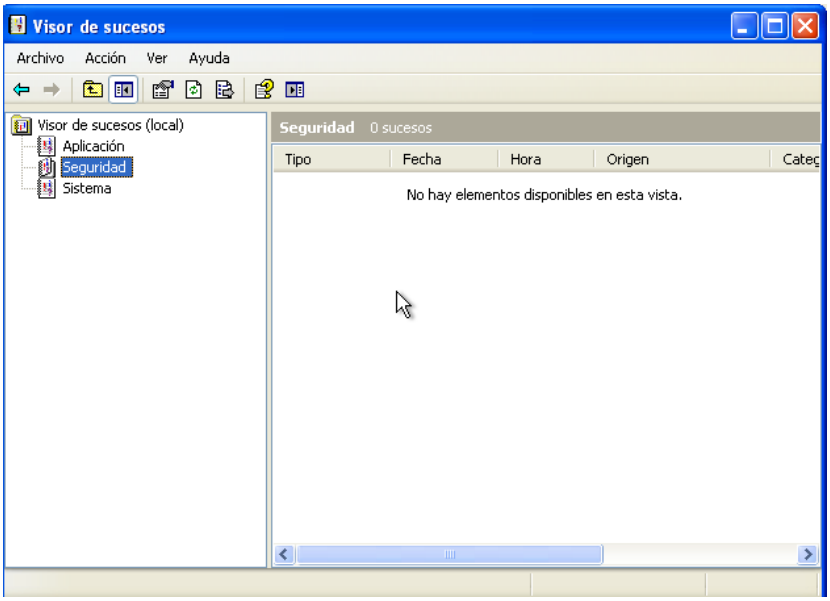
h) Verifica la auditoria de control de acceso "Visor de sucesos" de dicho usuario en Windows y Linux .

En XP

Para ir al visor de sucesos nos deberemos de dirigir al panel de control, posteriormente a la opción herramientas administrativas y posteriormente nos metemos en el visor de sucesos:



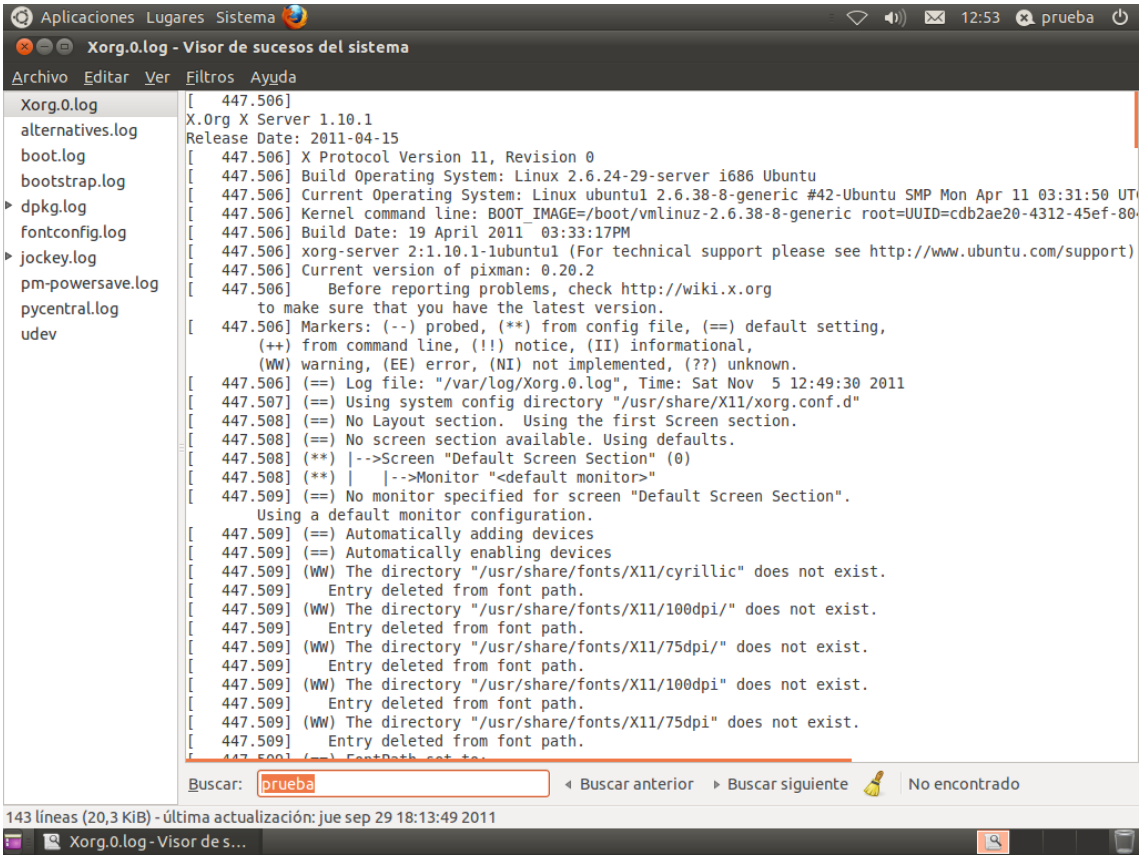
En este visor podemos observar varias secciones, la que nos interesa en la de seguridad que es donde se reflejan los parámetros de seguridad respecto a la autentificación de la cuenta. En nuestro caso observaremos que el registro esta vacio puesto que no ha ocurrido ningún problema de seguridad:



En linux

Para dirigirnos al visor de sucesos en Linux deberemos de dirigirnos a la pestaña sistema administración y pulsamos la opción visor de sucesos.

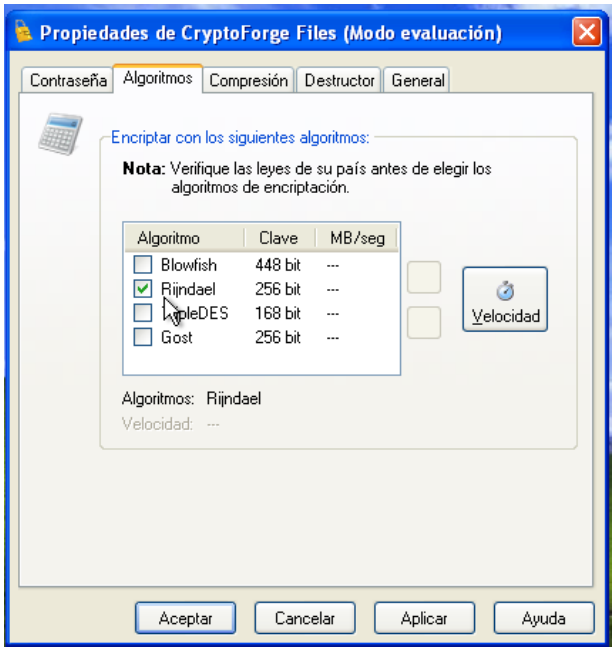
En la siguiente imagen podemos observar las diferentes secciones que encontramos en dicho visor de sucesos:



i) Descargar el programa de evaluación CryptoForge para Sistemas Windows y encripte y desencripte varios ficheros de tu ordenador, utilizando diferentes sistemas de cifrado.

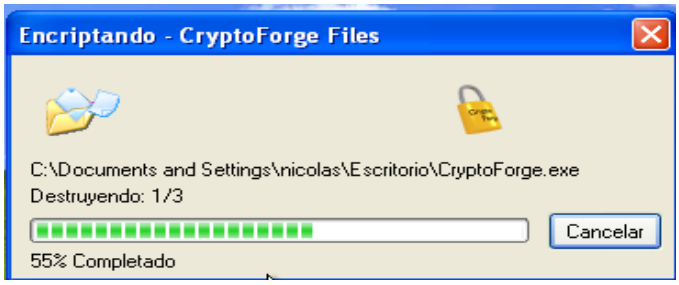
CryptoForge_ss un programa que nos permite encriptar y desencriptar archivos

Antes de realizar la encriptación podremos elegir los algoritmos de encriptación que deseamos utilizar, para ello nos dirigimos al programa y en algoritmos seleccionamos la opciones deseadas:



Para encriptar archivos debemos de hacer click derecho sobre un archivo y seleccionar la opción encriptar:

Ahora deberemos de introducir la contraseña de encriptación, una vez introducida pulsamos sobre aceptar para que de comienzo el proceso de enciptación:



Ahora para desencriptar deberemos de hacer click sobre el botón derecho y pulsamos la opción desencriptar.

Como el proceso de desencriptación lo realizaremos con el mismo usuario que realizo la encriptación no deberemos de introducir clave de descifrado:

j) Encriptar y desencriptar ficheros de texto en sistemas GNU/Linux utilizando el comando tr que permite realizar sustituciones carácter a carácter, utilizando la ayuda del manual.

TR

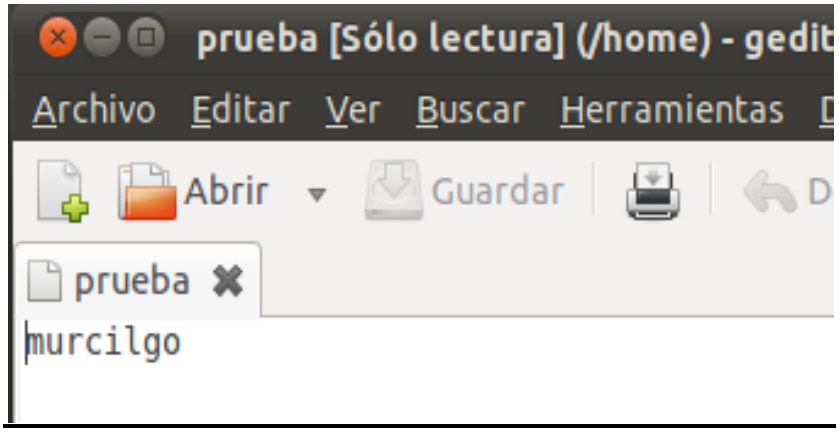
TR es una herramienta que nos permite encriptar y desencriptar cadenas de texto.

Algunos ejemplos del uso del tr son:

Con este primer ejemplo podremos eliminar las letras indicadas de una palabra o cadena de texto. En este ejemplo eliminaremos la a y la e de la palabra murciélago y introduciremos el resultado en el archivo prueba que se encuentra en el directorio /home/prueba:

```
root@ubuntu1:/home/niko# echo murcielago | tr -d ae > /home/prueba
```

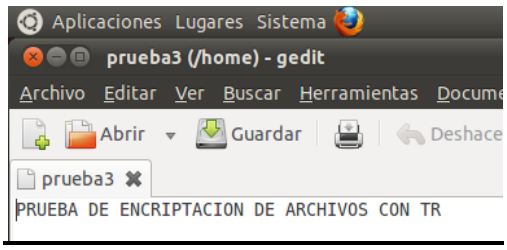
Aquí podemos ver el contenido del archivo prueba



Con las opciones que aparecen en la imagen podremos convertir una cadena de esto en minúsculas en una cadena de texto en letras mayúsculas. Eta opción se guardara en el fichero prueba3:

```
root@ubuntu1:/home/niko# echo 'Prueba de encriptacion de archivos con tr' | tr [
:lower:] [:upper:] > /home/prueba3
root@ubuntu1:/home/niko#
```

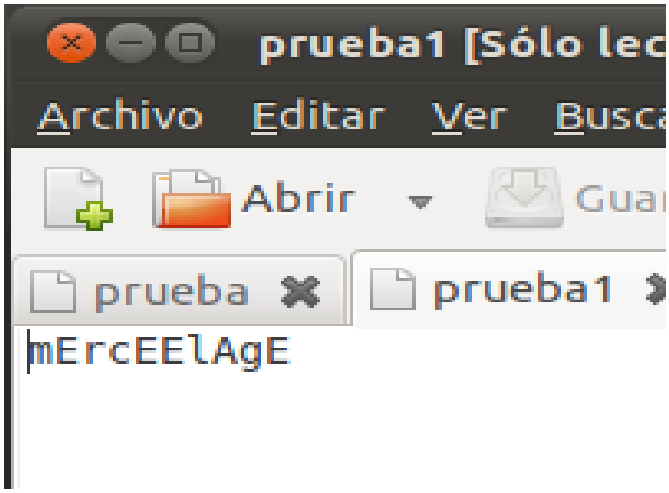
En esta imagen podremos ver el resultado del comando introducido en la imagen anterior



Por último utilizaremos una opción que nos permitirá sustitur las letras aeiou de una cadena de texto intoducida por una A o una E y también guardara los resultados en:

```
root@ubuntu1:/home/niko# echo murcielago | tr aeiou AE > /home/prueba1
```

Ahora en el archivo prueba1 podremos ver el siguiente resultado:



8. Análisis forense:

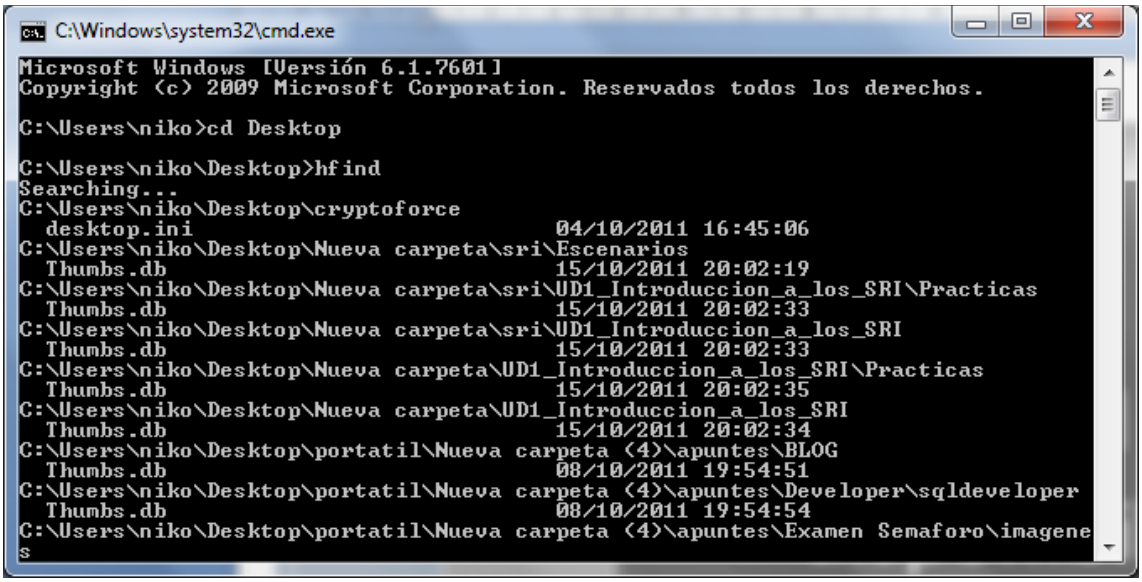
a) Utilizar una herramienta de Análisis forense para Windows y documente lo analizado con dicha herramienta.

Analisis forense

Hemos usado ForensicToolkit

HFIND

Con la opción hfind podremos buscar todos los archivos ocultos del directorio indicado. En nuestro caso aplicaremos este comando en nuestro escritorio, en donde podemos observar los siguientes archivos ocultos:

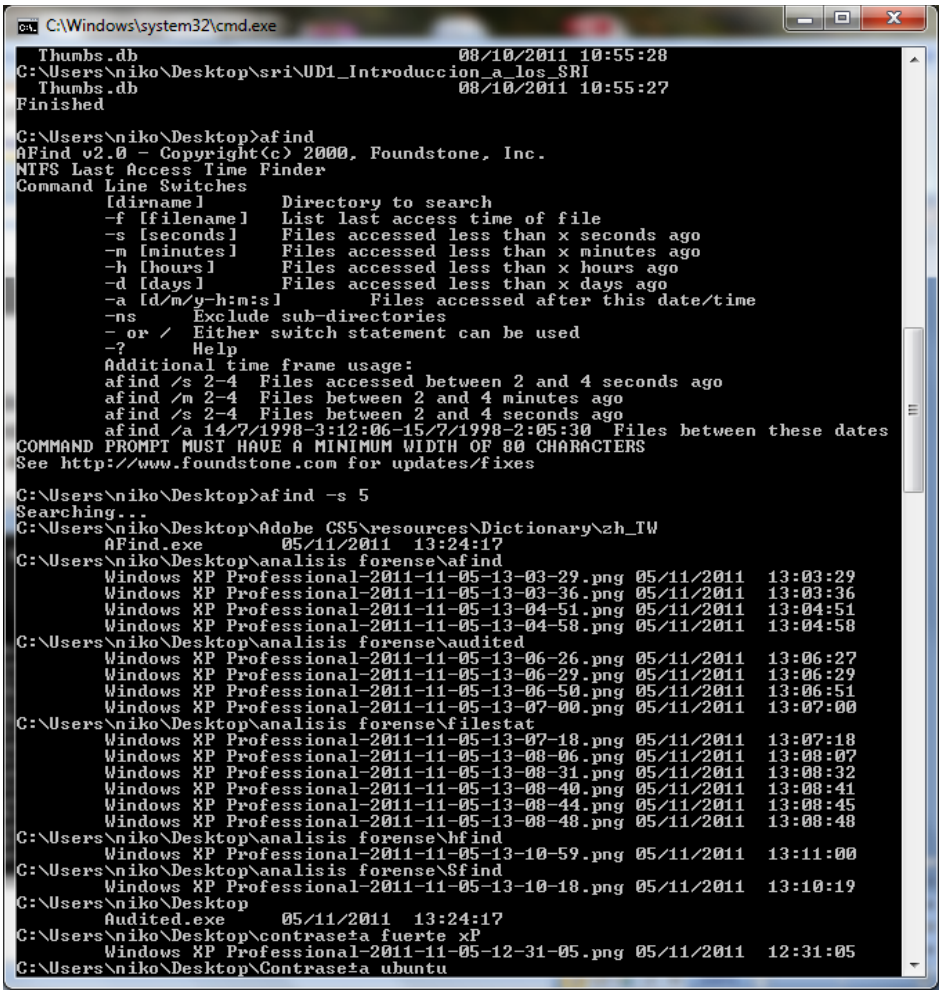


Afind

Con el comando afind podremos ver a que documentos se accedió en un momento dado como parámetro, en nuestro queremos saber los archivos que se han accedido hace 5 segundos , para ello introducimos el comando afind –s 5. En la siguiente imagen también podremos observar varias opciones que le podemos pasar como parámetro:

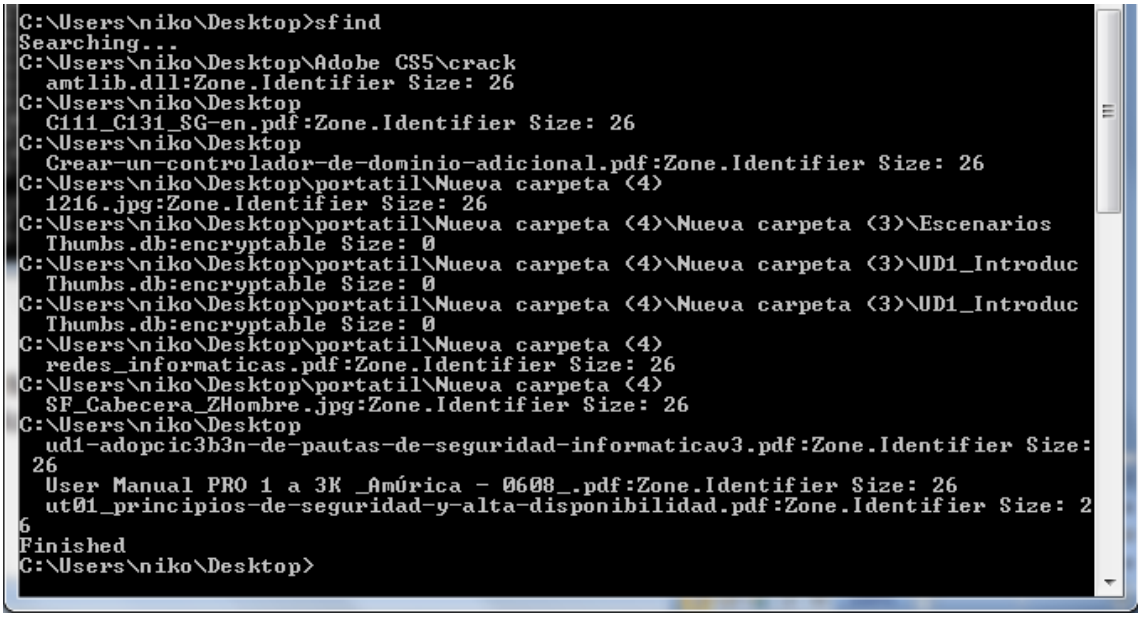
```
C:\Users\niko\Desktop>afind
AFind v2.0 - Copyright(c) 2000, Foundstone, Inc.
NTFS Last Access Time Finder
Command Line Switches
        [dirname]       Directory to search
        -f [filename]   List last access time of file
        -s [seconds]    Files accessed less than x seconds ago
        -m [minutes]    Files accessed less than x minutes ago
        -h [hours]      Files accessed less than x hours ago
        -d [days]       Files accessed less than x days ago
        -a [d/m/y-h:m:s]        Files accessed after this date/time
        -ns     Exclude sub-directories
        - or /  Either switch statement can be used
        -?      Help
        Additional time frame usage:
        afind /s 2-4  Files accessed between 2 and 4 seconds ago
        afind /m 2-4  Files between 2 and 4 minutes ago
        afind /s 2-4  Files between 2 and 4 seconds ago
        afind /a 14/7/1998-3:12:06-15/7/1998-2:05:30  Files between these dates
COMMAND PROMPT MUST HAVE A MINIMUM WIDTH OF 80 CHARACTERS
See http://www.foundstone.com for updates/fixes
```

El ejemplo indicado anteriormente se aprecia en la siguiente imagen:



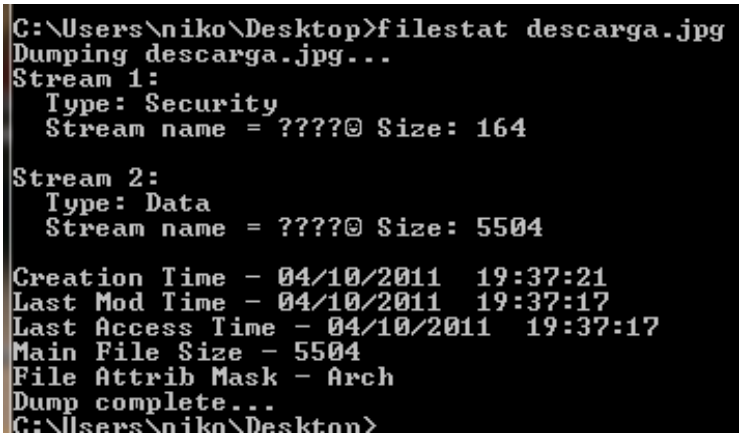
Sfind

Con esta herramienta podremos buscar flujos de datos ocultos en nuestro disco duro o en el directorio indicado. Para utilizar este parámetro deberemos de introducir sfind en el terminal:



Filestat

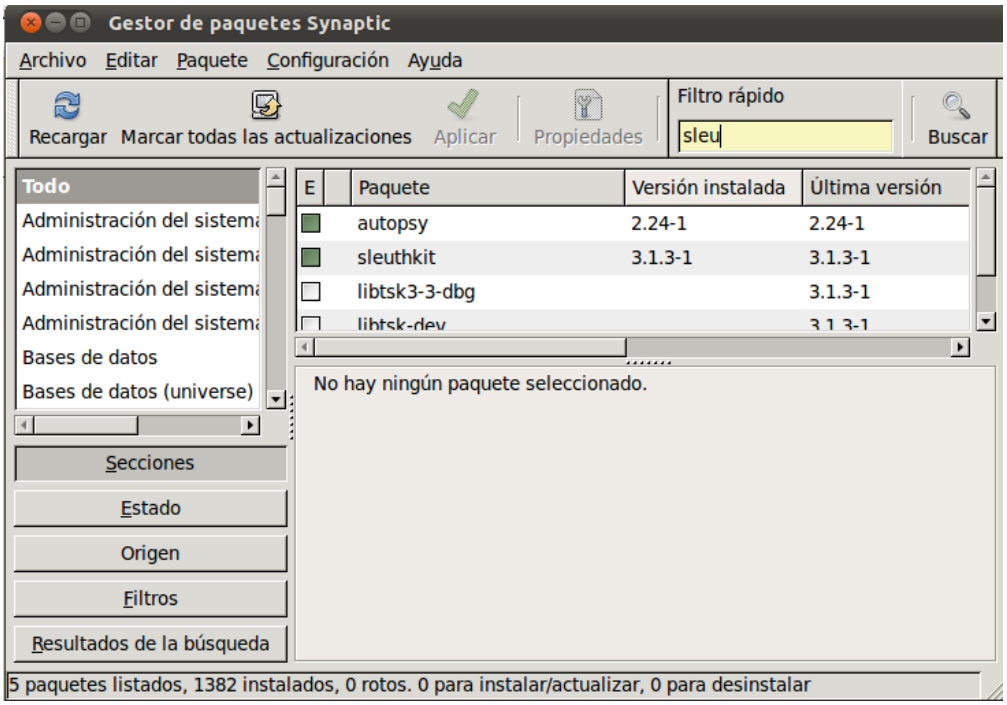
Con esta herramienta podremos obtener una lista completa de los atributos del archivo que le pasemos como parámetro, en nuestro caso lo haremos de la imagen desgarga.jpg que se muestra en nuestro escritorio. En la siguiente imagen podremos ver parámetros como el tiempo de creación, ultima modificación y el tamaño del archivo:



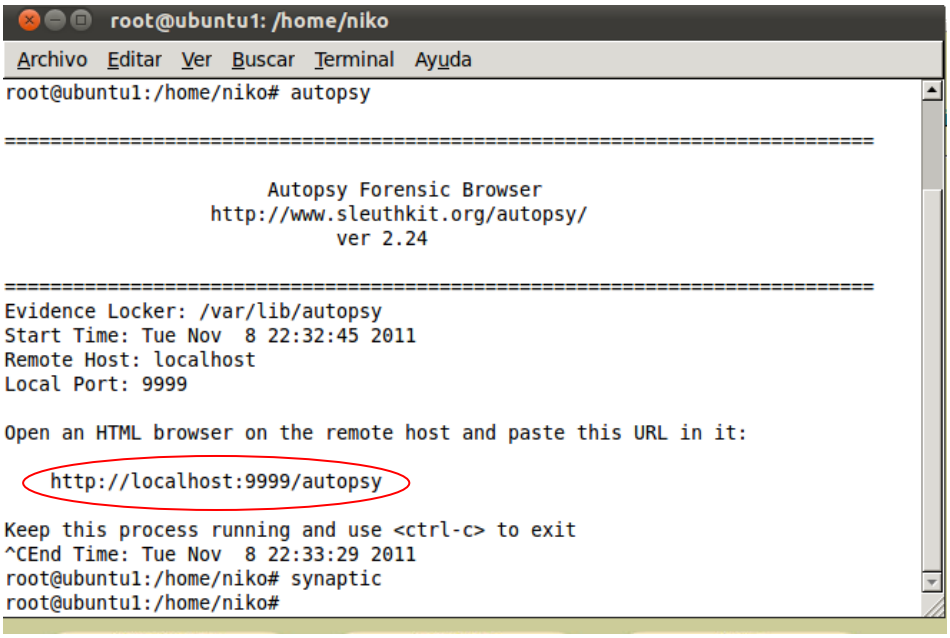
En Linux

SLEUTHKIT Y AUTOSPY

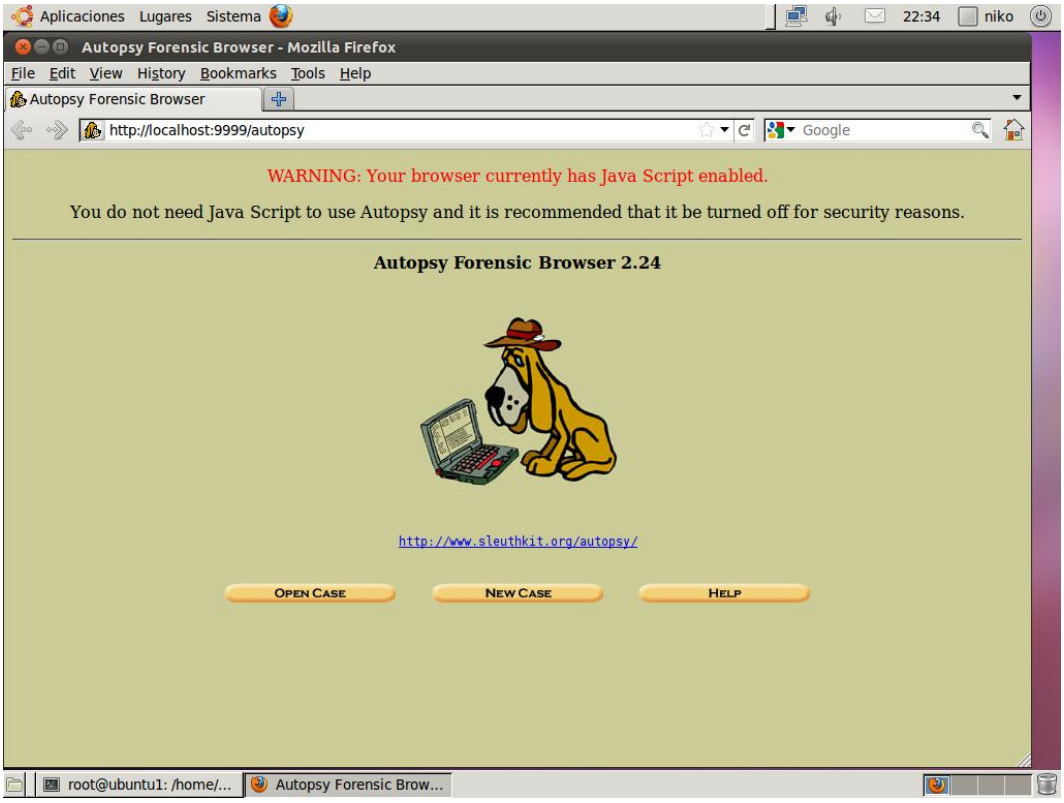
1.- En primer lugar instalaremos el paquete autopsy desde el synaptic:



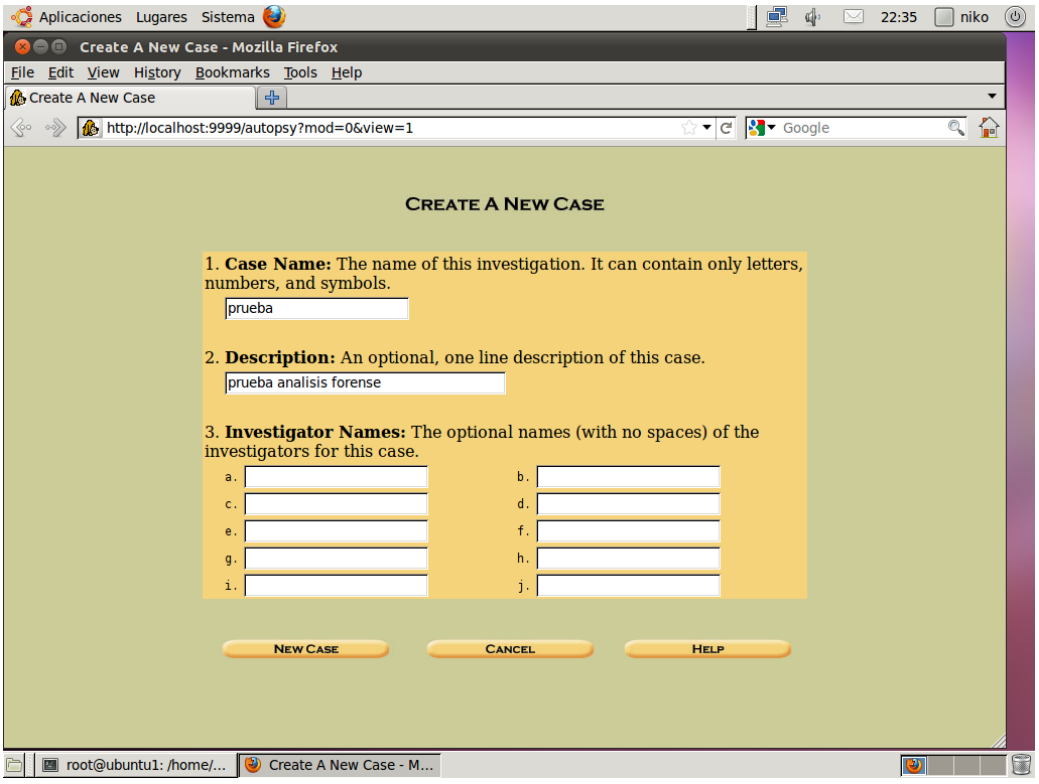
Una vez instalado nos dirigimos al terminal e introducimos la palabra autopsy y pulsamos sobre la dirección que aparece en la terminal:



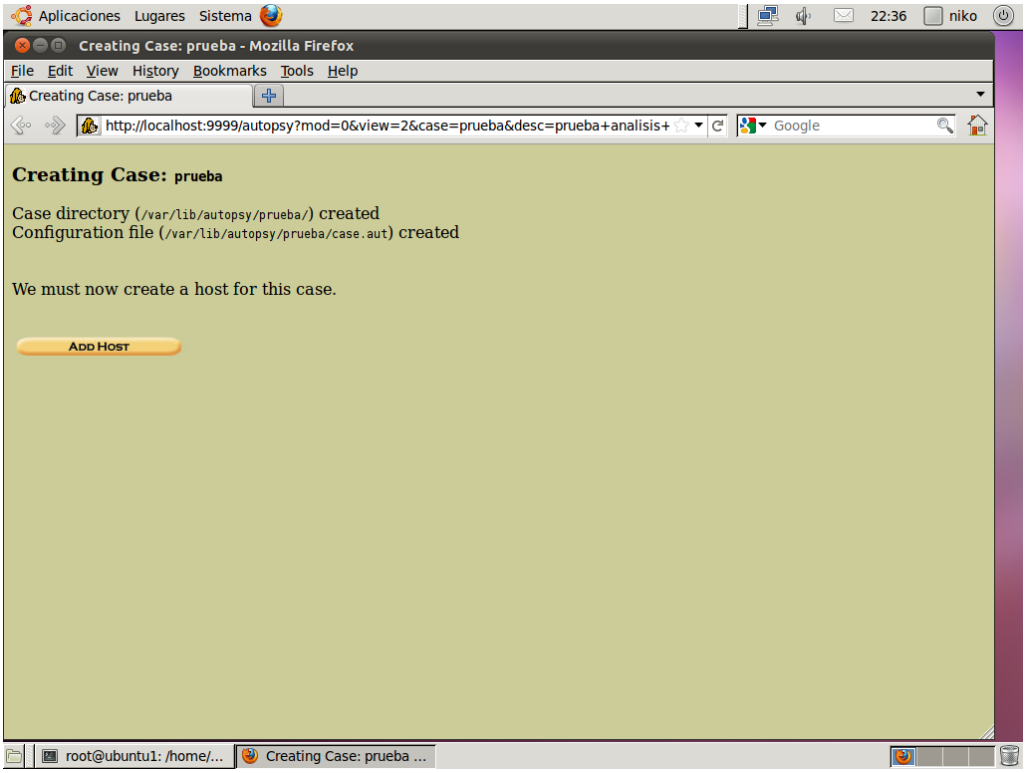
Ahora en la pagina principal del programa pulsamos sobre la opción New case para crear un nuevo caso:



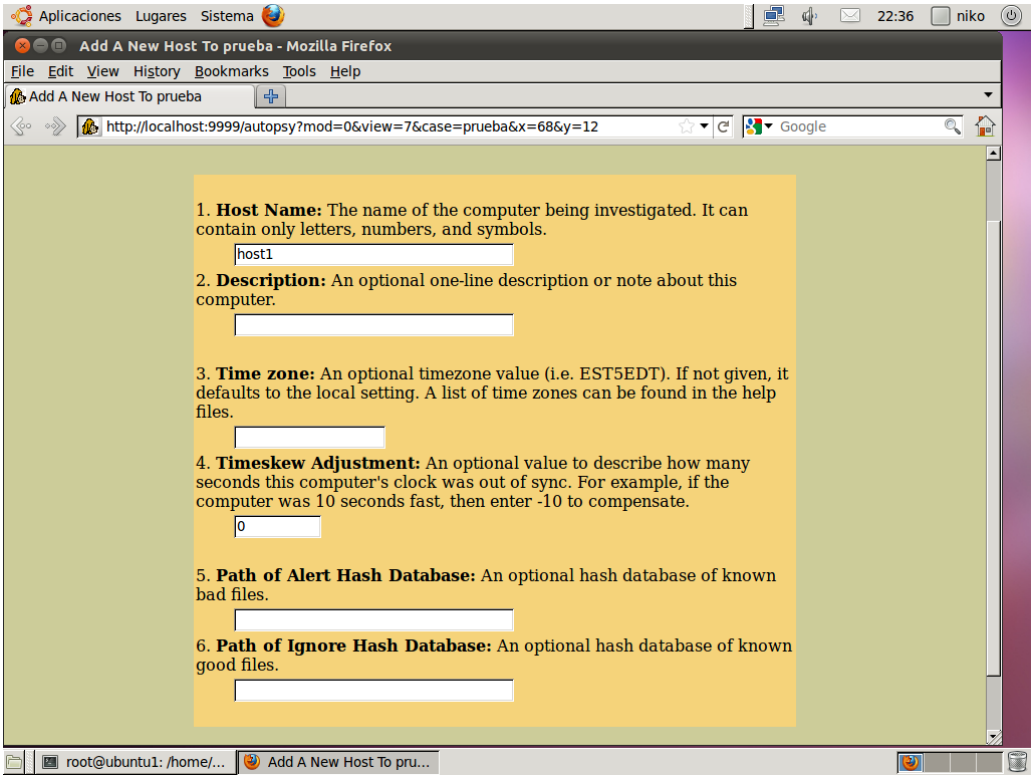
Ahora deberemos de introducir un nombre y una descripción para el caso, cuando acabemos pulsamos sobre New case:

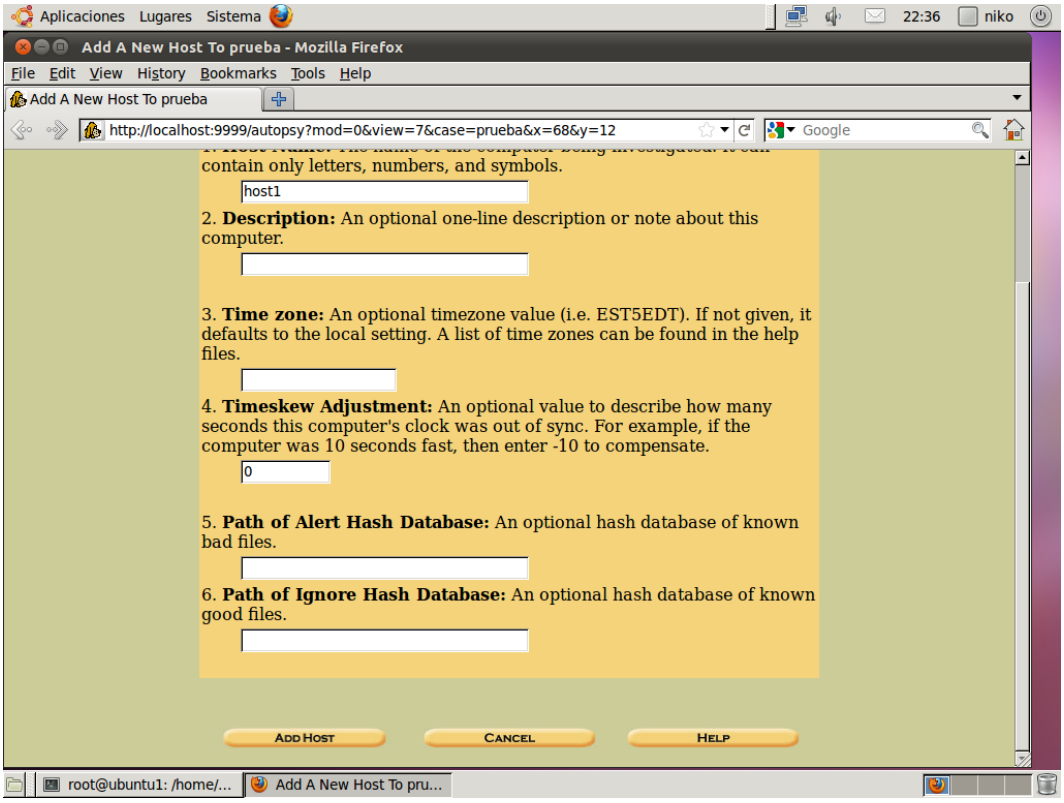


Una vez creadao el caso deberemos de pulsar sobre la opción Add Host para agregar un host:



Ahora introduciremos el nombre de host y dejamos las otras opciones vacias puesto que son valores opcionales, cuando acabemos pulsamos sobre Add Host:

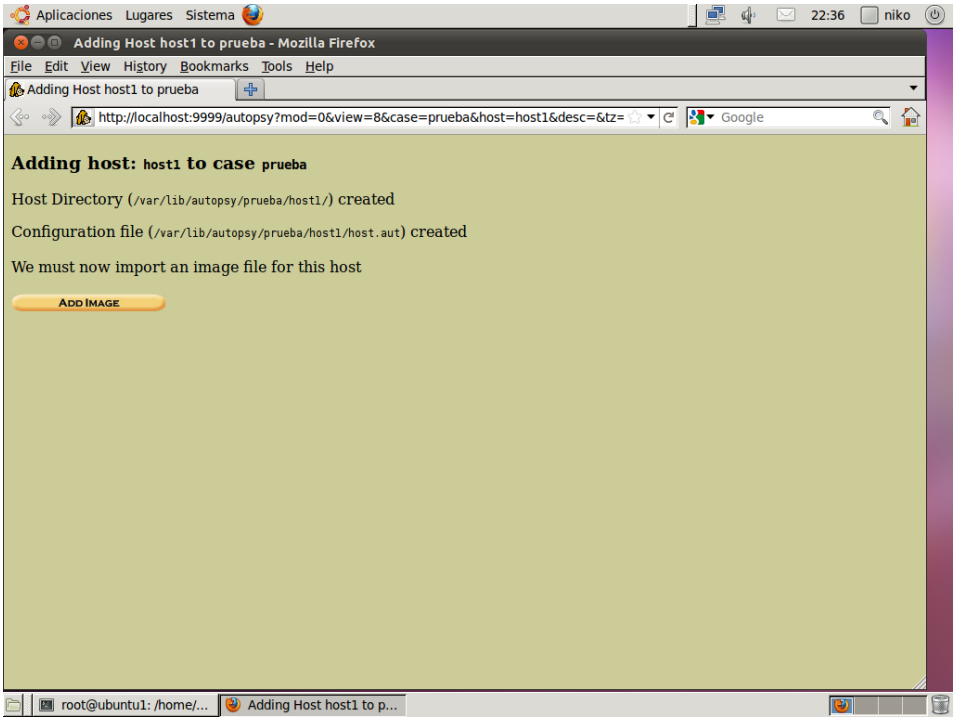




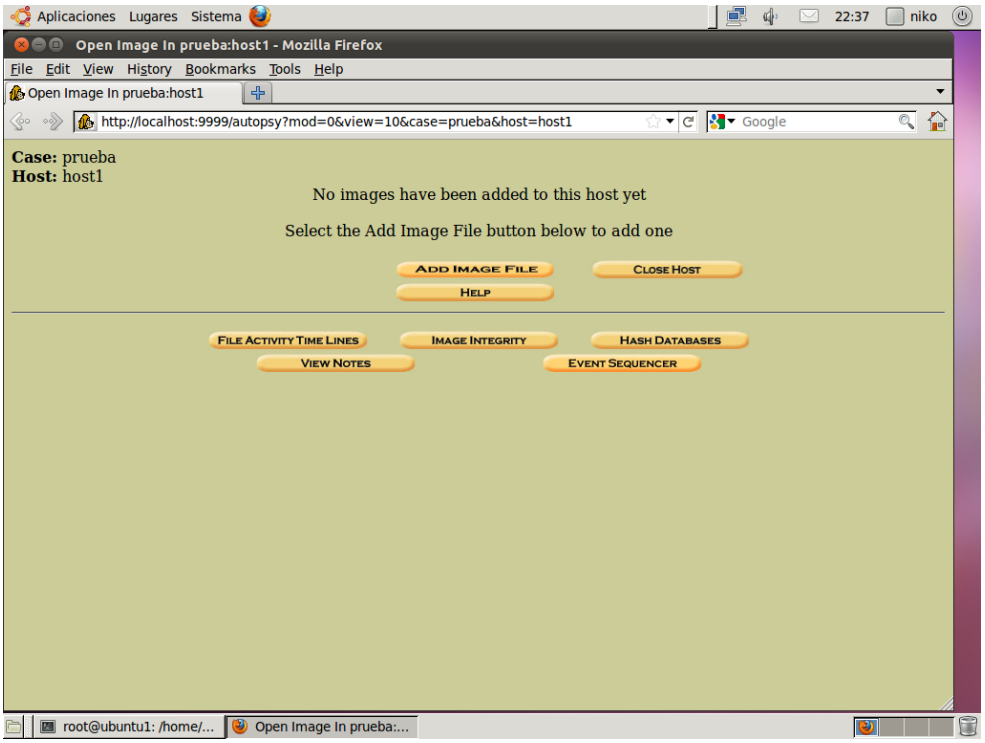
Ahora nos pedirá que especifiquemos una imagen, como no la tenemos creada procederemos a crearla. En nuestro caso realizaremos la imagen de nuestro usb, para ello introdimos el comando que aparece en pantalla puesto que nuestro dispositivo USB ha sido montado en /dev/sdb1 y queremos guardarlo en el escritorio:

```
niko@ubuntu1:~$ sudo dd if=/dev/sdb1 of=/home/niko/Escritorio/usb.iso
```

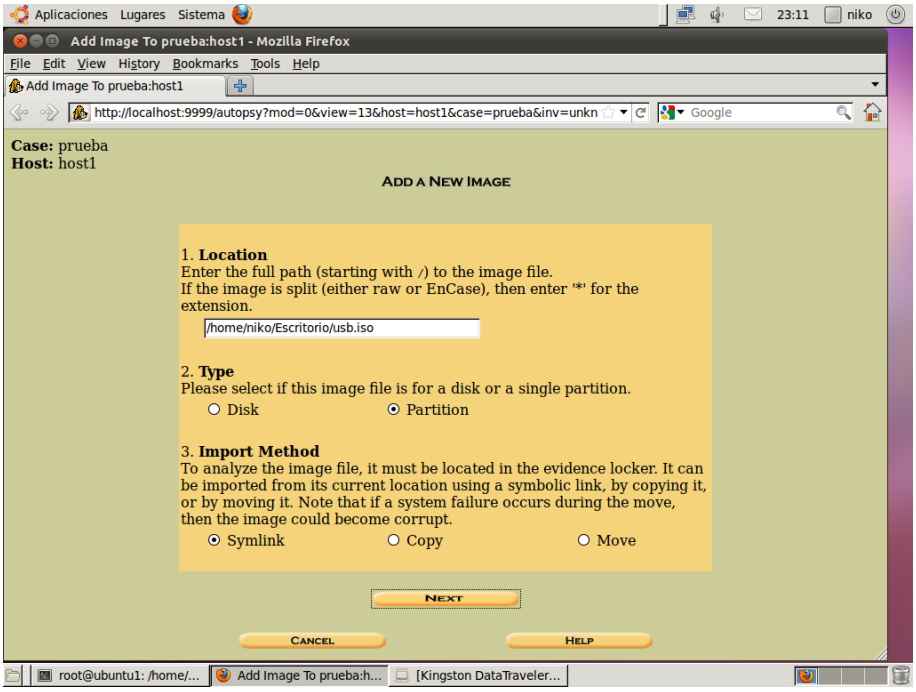
Una vez creada la imagen seleccionaremos la opción Add image para asi configurar el análisis a la imagen de nuestro usb.



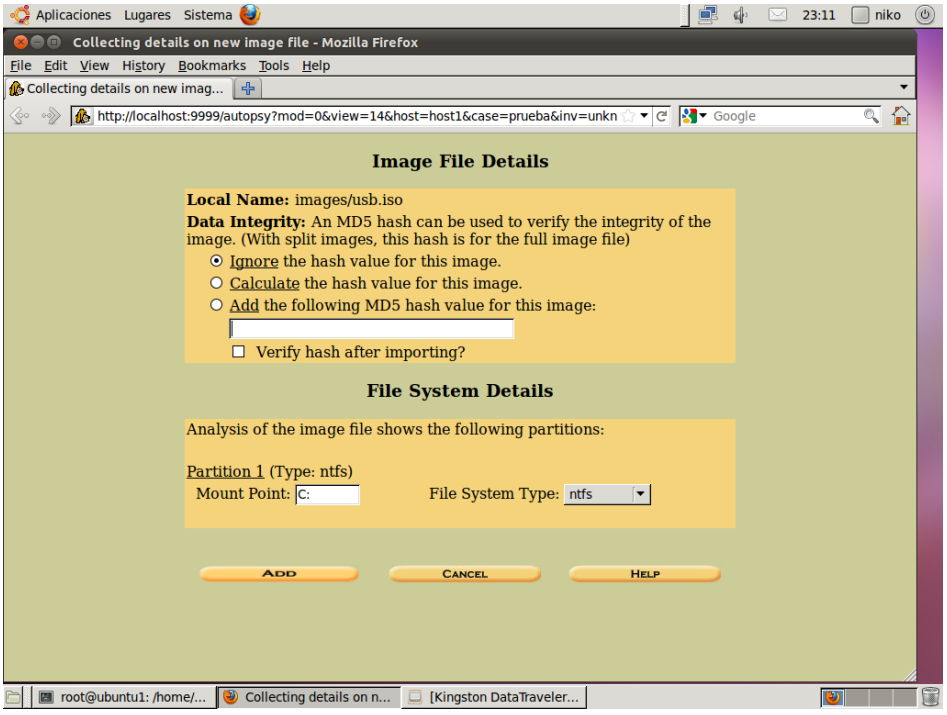
Ahora volveremos a pulsar sobre la opción add image file:



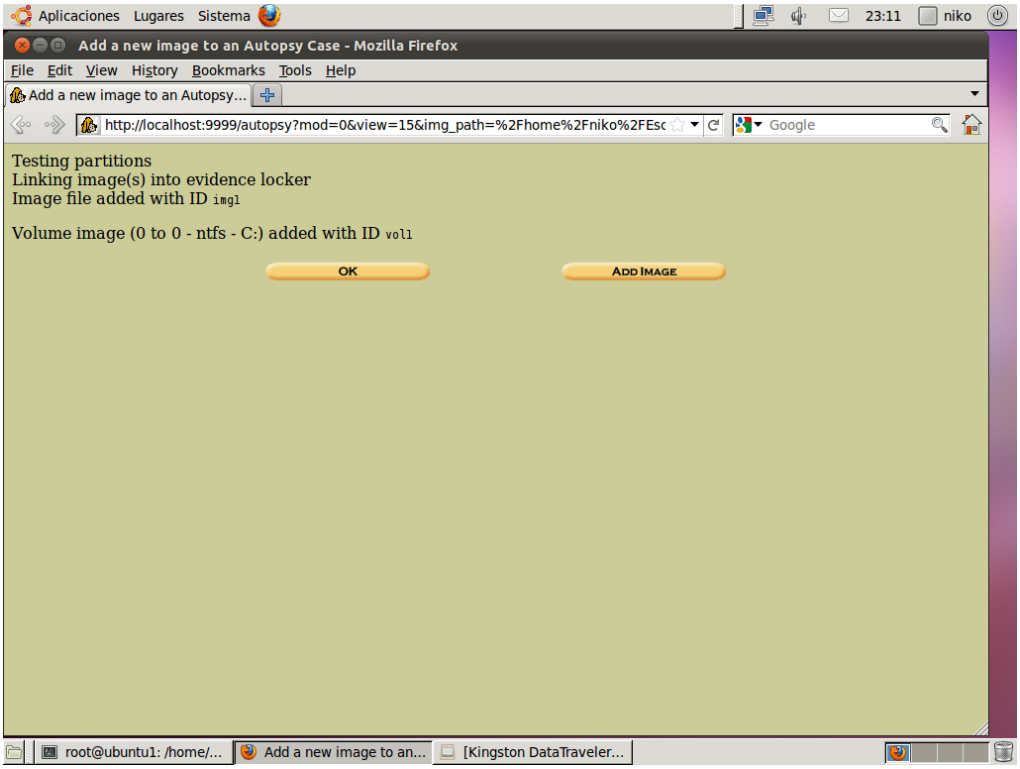
Ahora en la casilla Location deberemos de poner la ruta de la imagen que deseamos analizar, en Type deberemos de especificar si es una partición o un disco, en nuestro caso seleccionamos Partition y por ultimo en Import method dejamos el valor por defecto. Una vez configurados los aspectos de esta pantalla seleccionamos next:



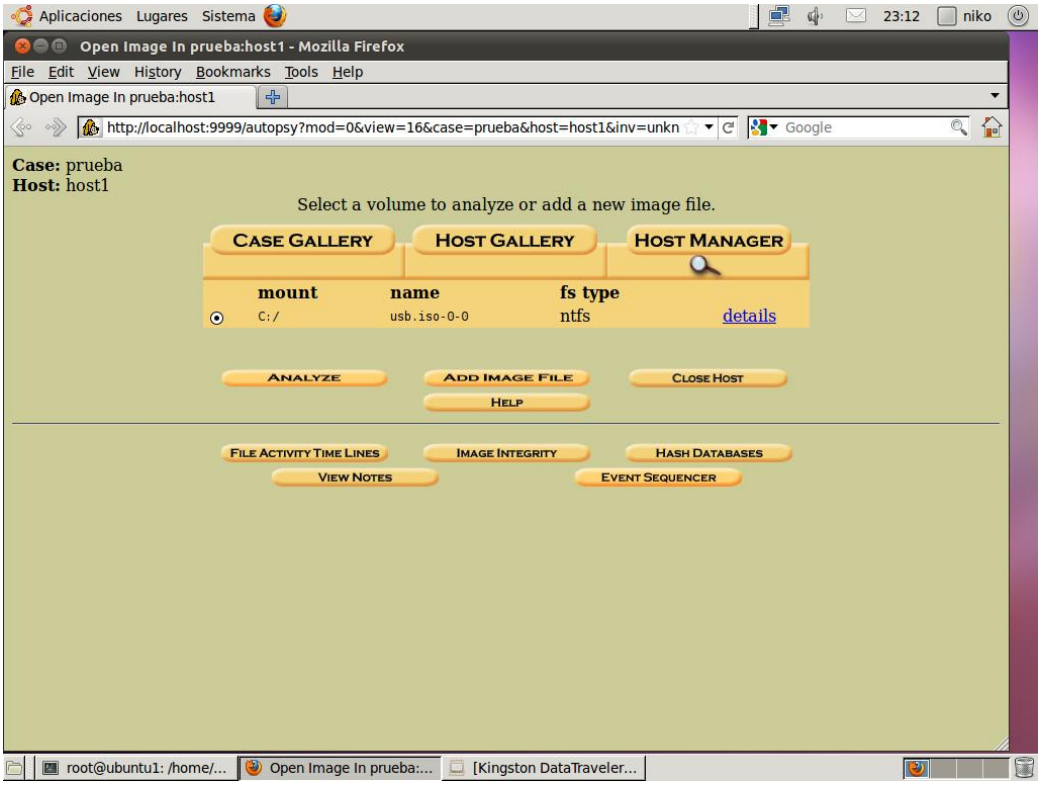
Ahora en la siguiente pantalla dejaremos las opciones por defecto y pulsaremos sobre la opción Add:



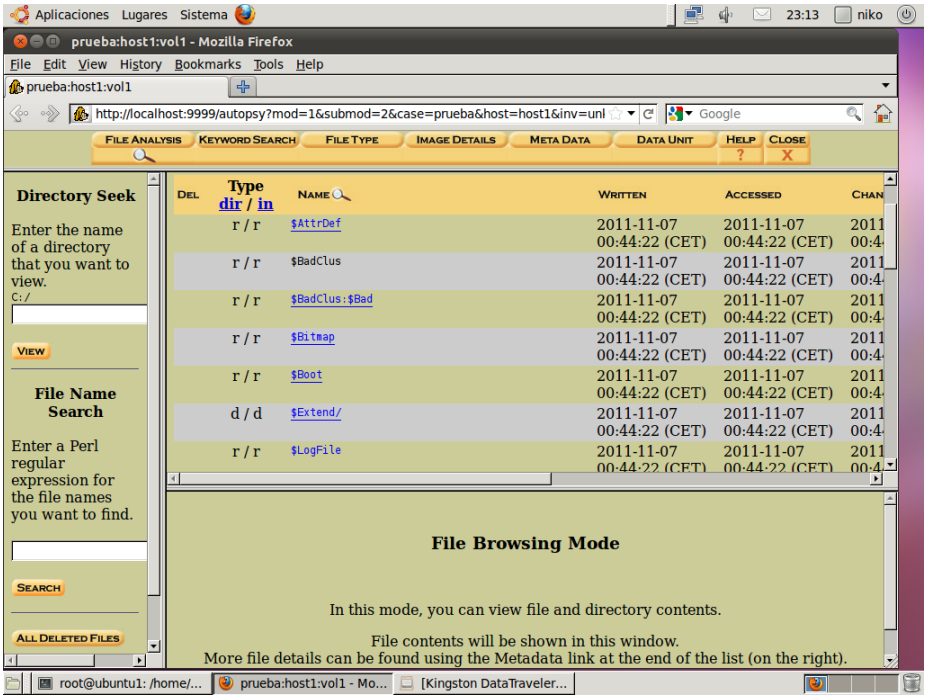
Ahora en la siguiente pantalla deberemos de pulsar sobre ok para comenzar el análisis de las particiones:



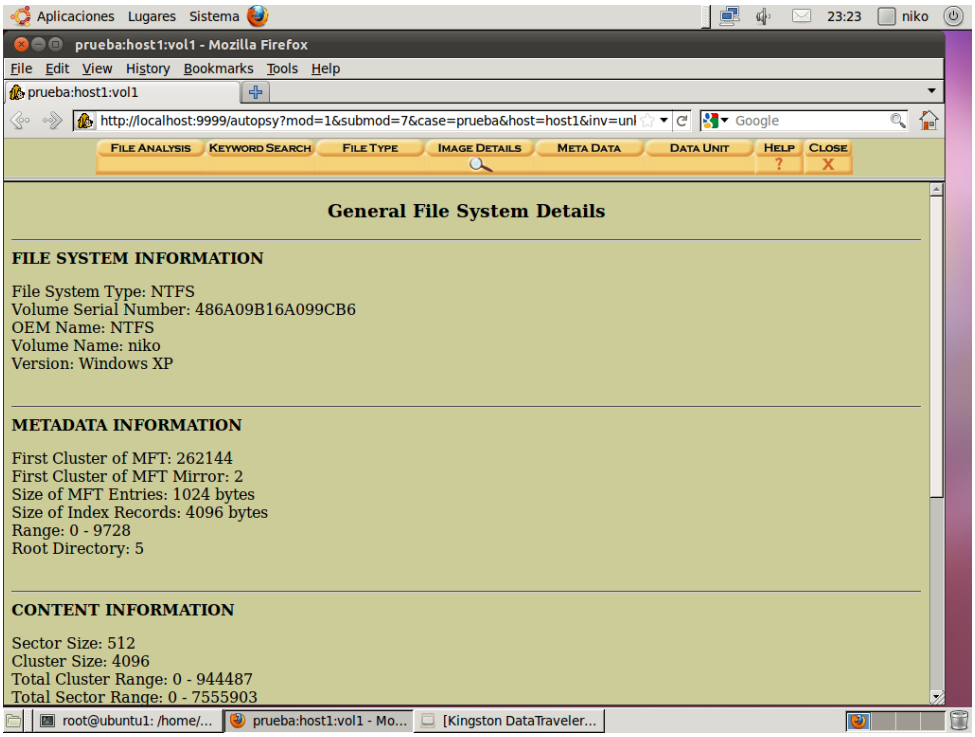
Ahora deberemos de pulsar sobre la opción ANALIZE para analizar nuestra imagen:



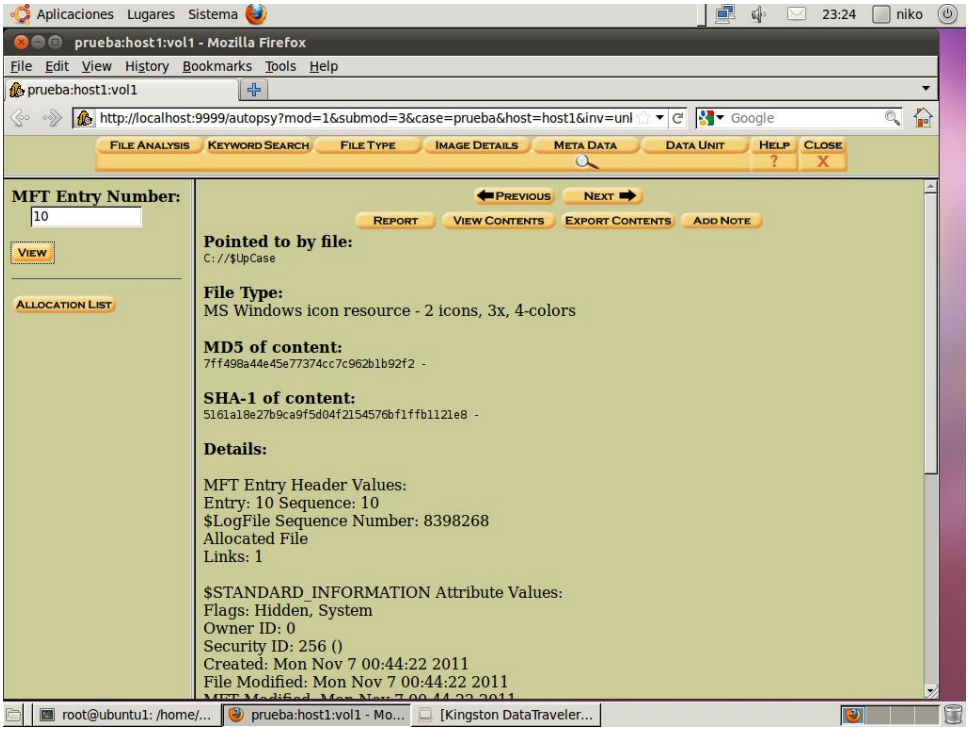
Ahora en la pantalla que nos aparece podremos ver los resultados del análisis en primer lugar nos dirigiremos a la pestaña File Analysys donde podremos observar todos los ficheros de la partición analizada tanto los ocultos como los no ocultos:



Ahora nos dirigiremos a la pestaña Image Details. En esta pestaña podremos observar todos los detalles referentes a la imagen:



Ahora nos dirigiremos a la pestaña Meta Data donde si introducimos un valor en la parte izquierda donde pone MFT ENTRY NUMBER y pulsamos sobre view para observar los resultados para un valor 10 de MTF:



Ahora para finalizar nos dirigimos a la pestaña DATA UNIT para ver la información cifrada de un cluster en concreto para ello en cluster number introducimos un valor y pulsamos sobre view: