Seguridade Pasiva

Adrián Gómez Lois

Contenido

1. Obxectivos.

Con estas prácticas chegaremos a ver as copias de seguridade, o clonado de unidades e o borrado seguro das mismas.

As copias de seguridade permítenos salvagardar a información desexada en outras ubicacións ou dispositivos, dita información pode ser restaurada en calqueira punto.

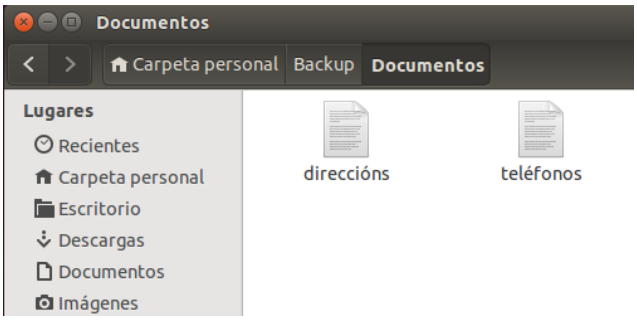
As clonacións son importantes para salvagardar os cambios actuáis dun sistema e poder replicalo noutro equipo co fin de axilizarnos as labores de instalación é configuración inicial destes ou tamén usados en técnicas de análise forense.

Todo co fin de intentar protexer a nosa información almacenada. Tamén faremos borrado seguro da información o cal e un punto interesante e que se debería ter en conta en moitos casos, xa que a información sempre pode estar recuperable en calquer punto a menos que se faga o borrado seguro adecuado.

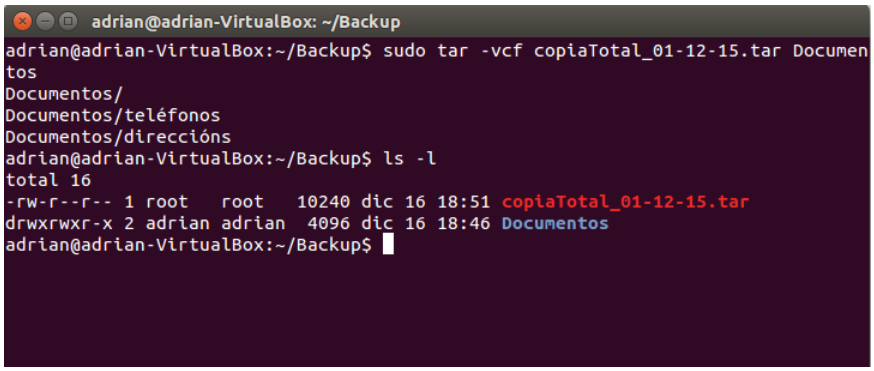
2. Copias de seguridade con ferramentas do sistema.

Realizaremos unha copia de seguridade en Linux coa utilidade tar, ferramenta a cal xa está incorporada nun sistema Ubuntu.

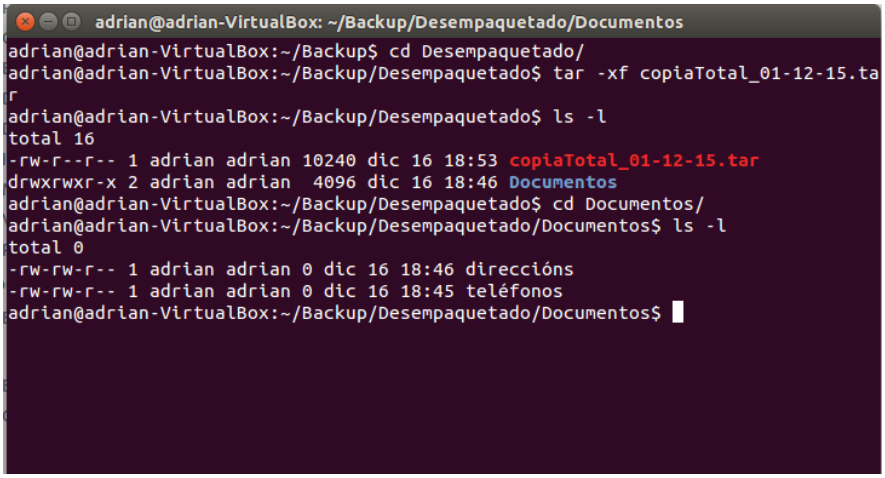
Creamos unha cartafol con dous ficheiros.



Realizamos a copia de seguridade da carpeta backup con tar –vcf.

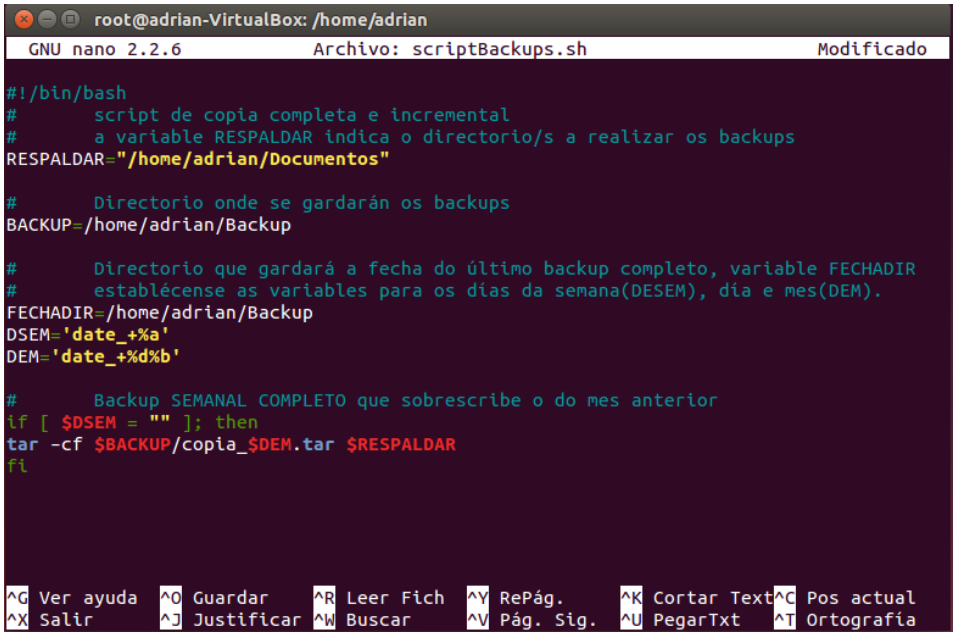


Agora creamos un cartafol para o desempaquetado, e procemos con tar –xf.

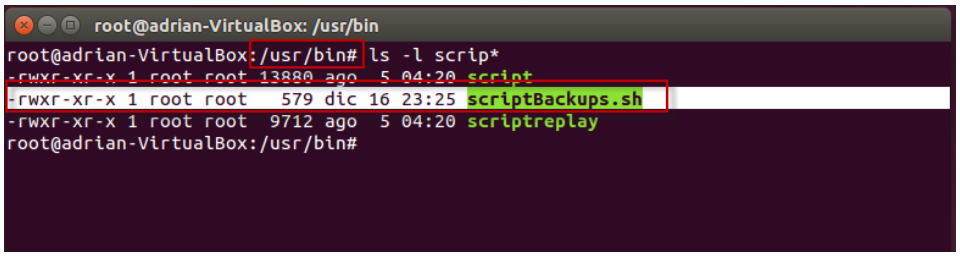


Temos que saber que podemos programar para así automatizar copias de seguridade.

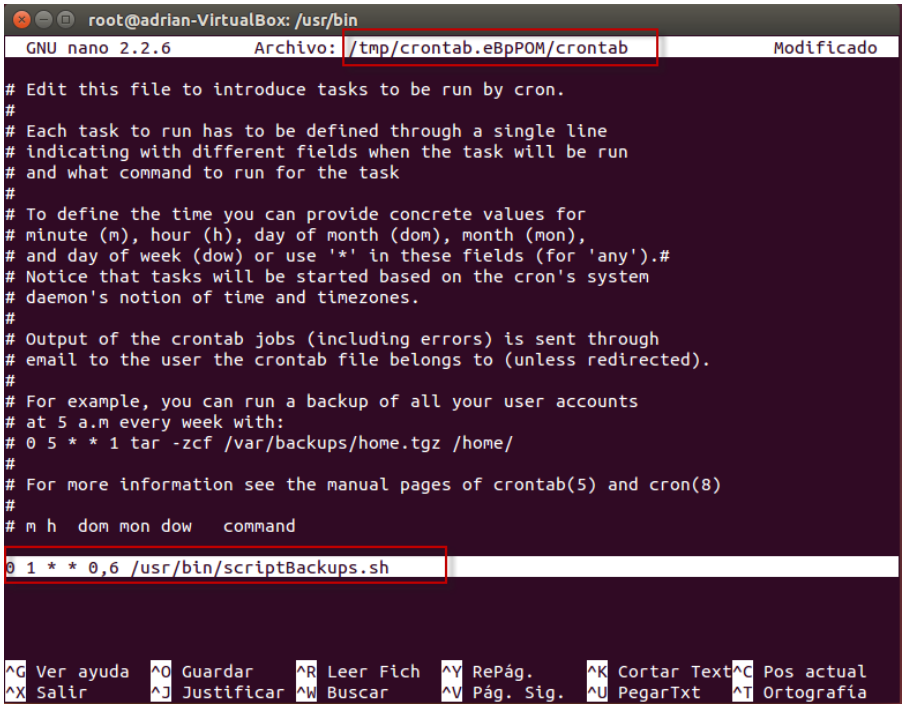
Para iso aproveitando os ficheiros anteriores vamos facer o seguinte script. O cal fai uso de tar –cf para realizar a copia de seguridade.



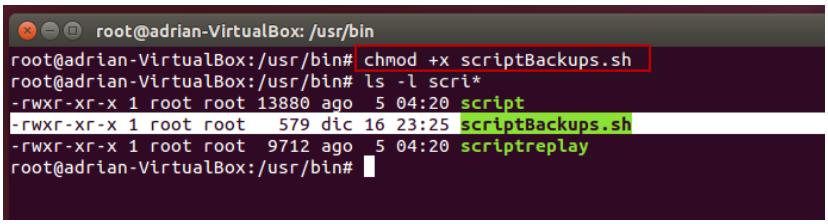
Vamos guárdalo en /usr/bin.



Agora con contrab automatizamos a lanzamento do anterior script nun día da semana e hora en cuestión, neste exemplo púxeno para que se ejecutase o script.sh para realizar os bacukps todos os días da semana a 01:00 da mañá.



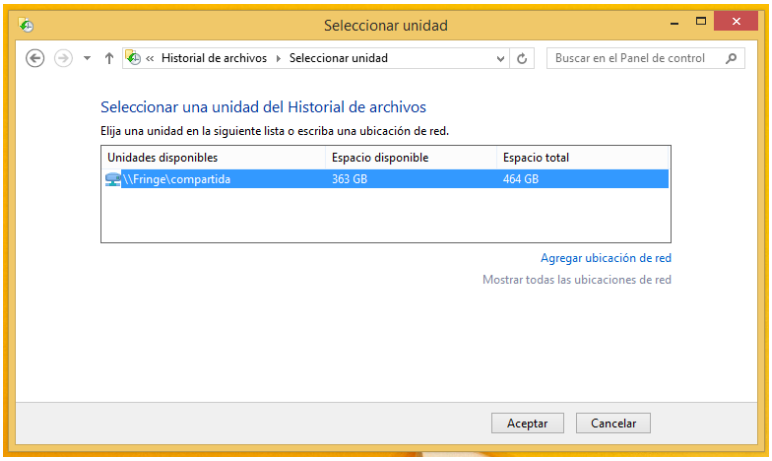
Simplemente quedaría darlle permisos de ejecución (+x) o script.sh.



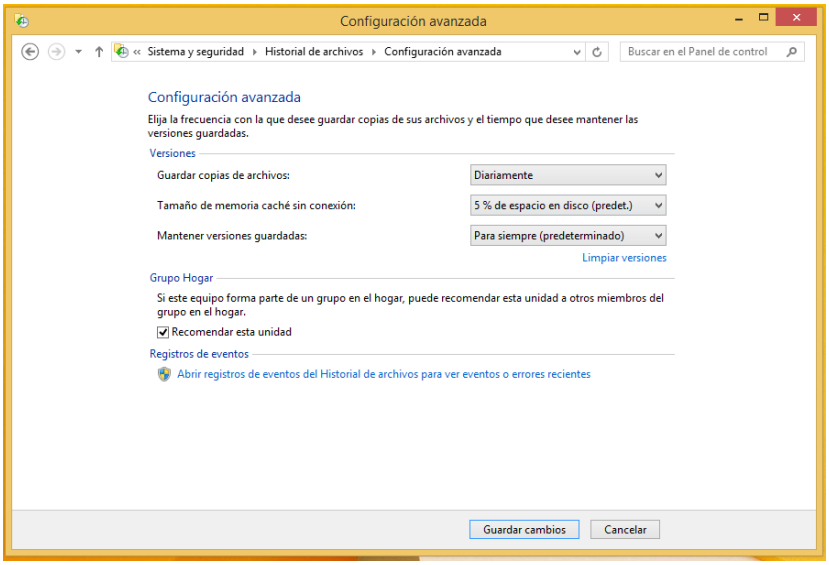
En Windows existe a posibilidade de facer copias de seguridade cunha ferramenta propiamente integrada.

No panel de control de Windows podemos encontrar a utilidade chamada “Historial de ficheiros” (en Windows 8), no asistente pediranos unha ubicación donde almacenar a copia de seguridade.
Para facer neste exemplo dous pasos desta práctica empezarei por realizar a copia de seguridade nunha unidade de rede. Polo que selecciono outro equipo da e deixarei a copia nunha carpeta compartida.

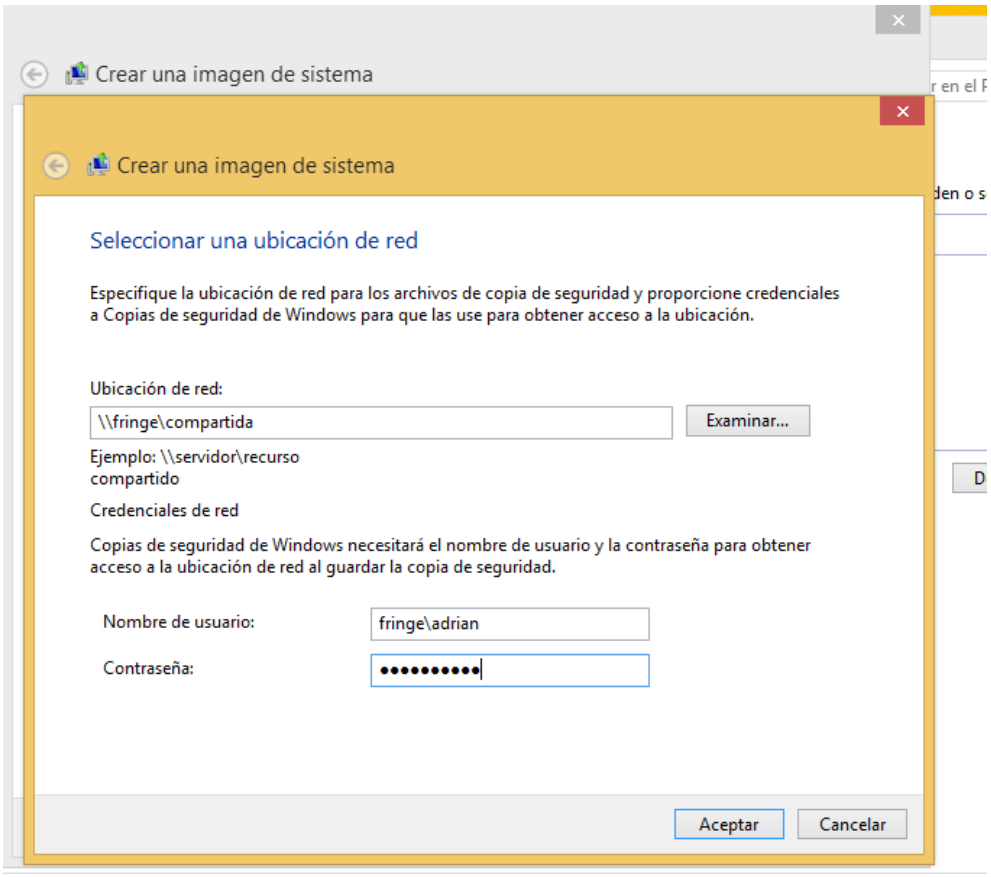
A copia contendrá unha imaxen do sistema actual completa.

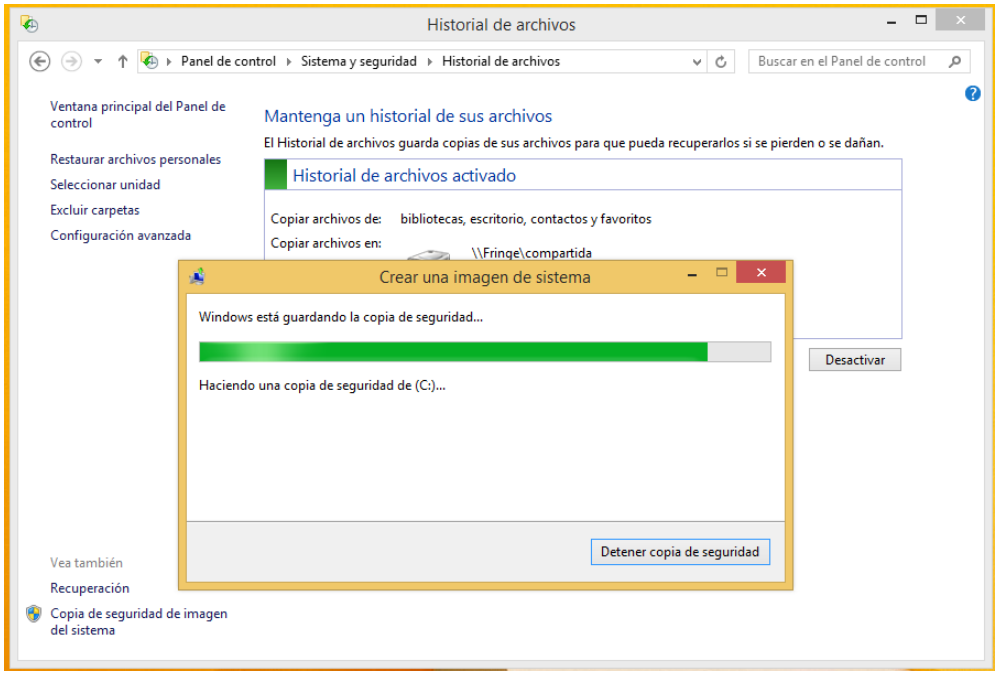


Configuro a copia como exemplo, para que se faga de forma diaria.

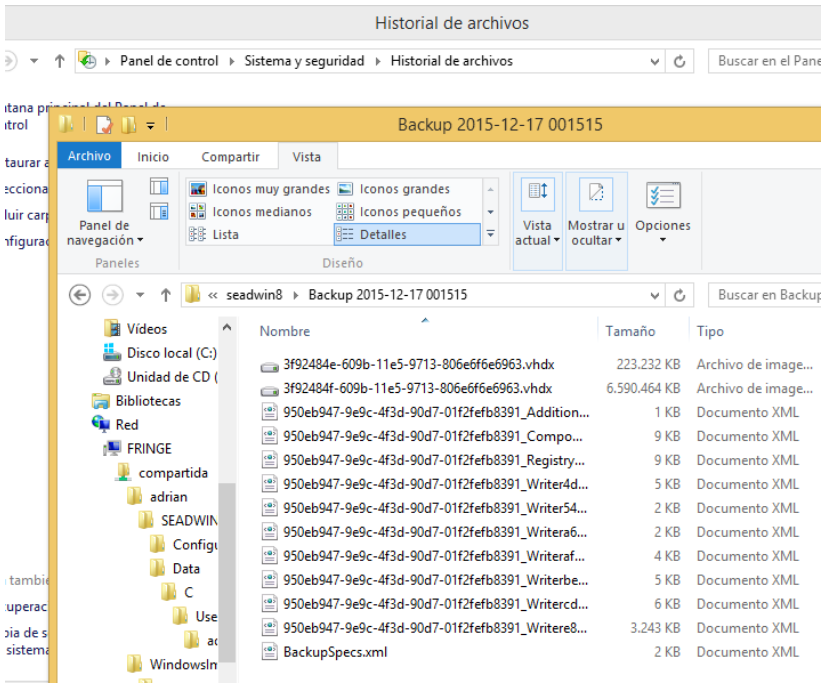


Referencio un usuario e contraseña para ter acceso a ese recurso compartido e poder realizar a copia de seguridade.



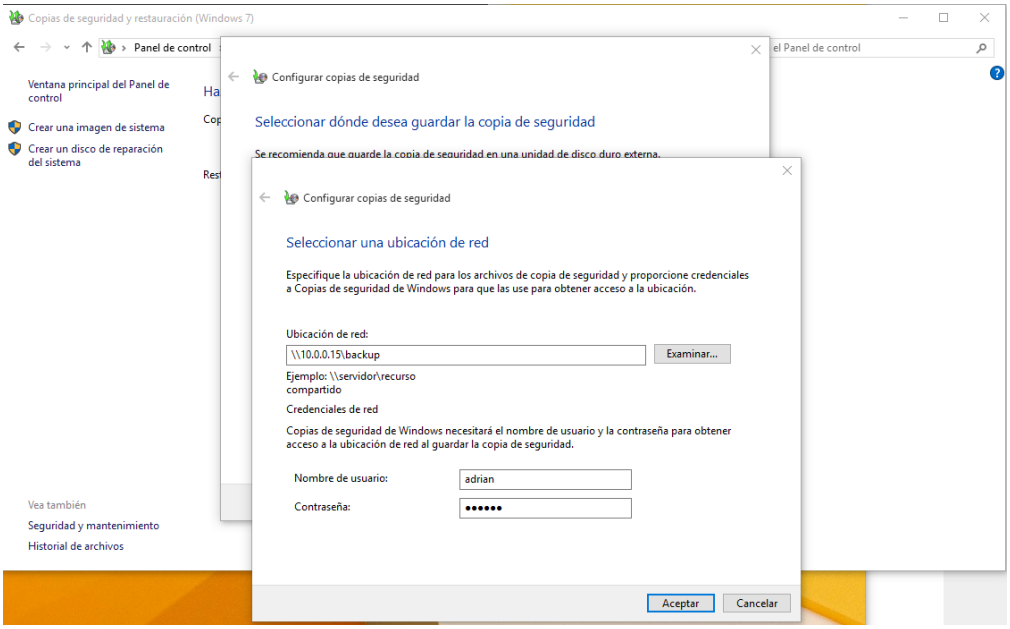


Vemos como se fixo correctamente o bakcup completo do sistema actual.

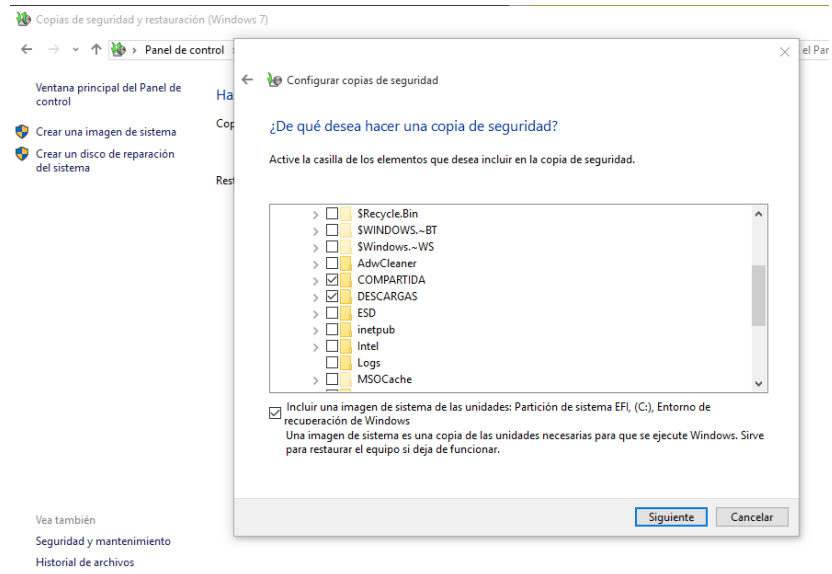


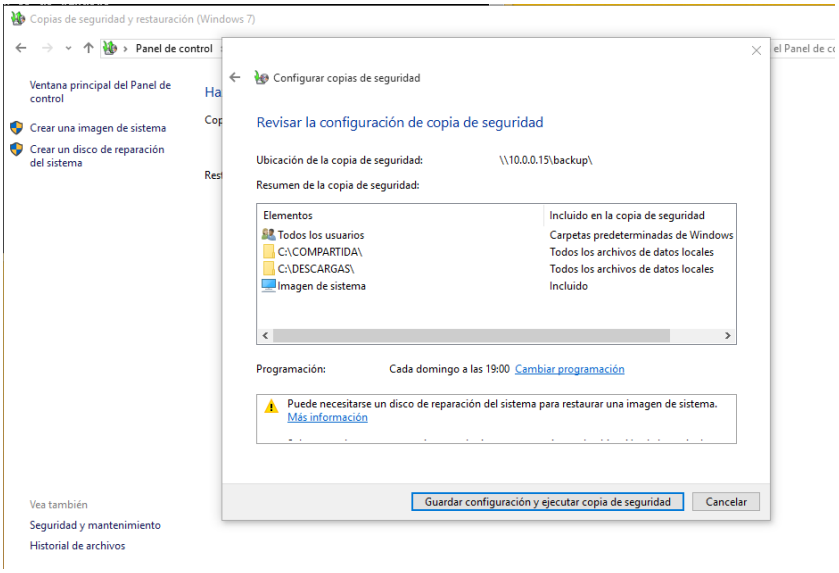
Neste outro exemplo farase unha copia de seguridade de determinadas zonas ou ficheiros internos personais.

Neste caso ubicarei a copia de esos datos noutro equipo da rede.

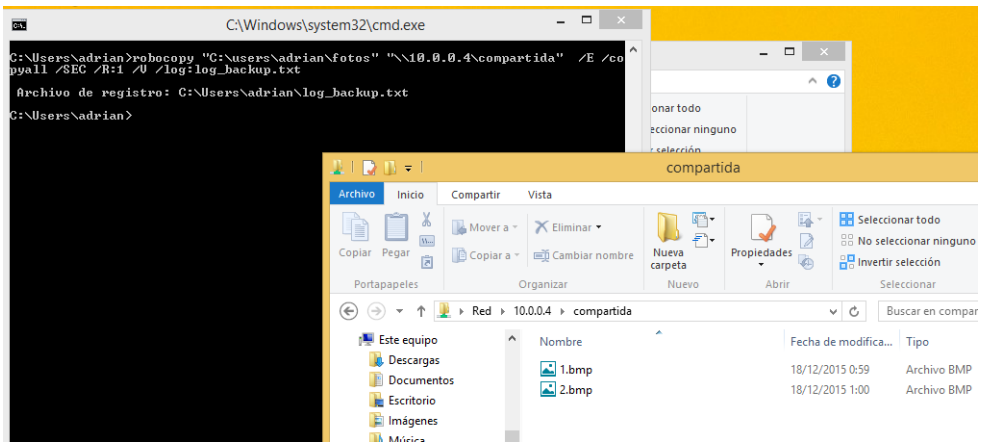


Eleximos os datos dos que queramos realizar o backup, a maiores xa lle idicamos a fecha/hora facer o backup, neste caso cada Domingo as 19:00.

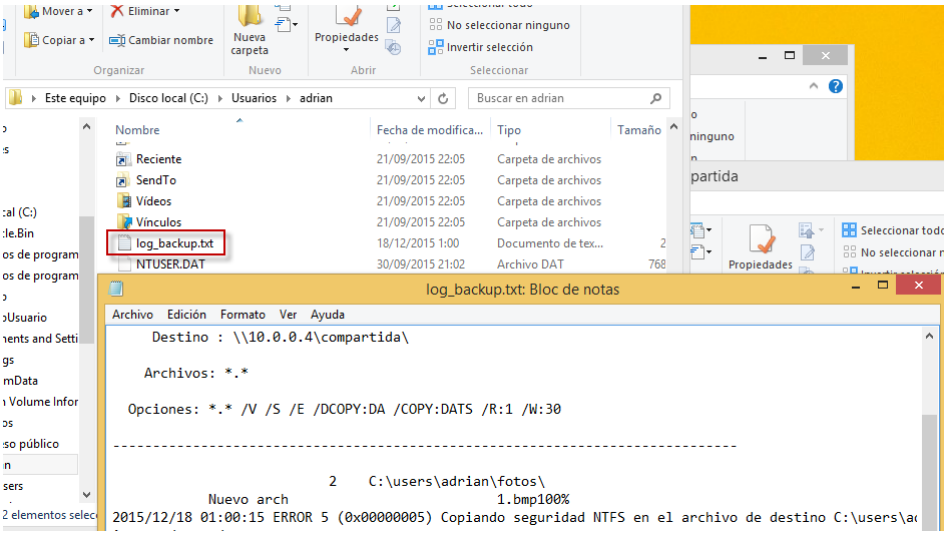




Como último exemplo podemos realizar unha copia de seguridade con robocoy e que este a copia nunha unidade de rede.



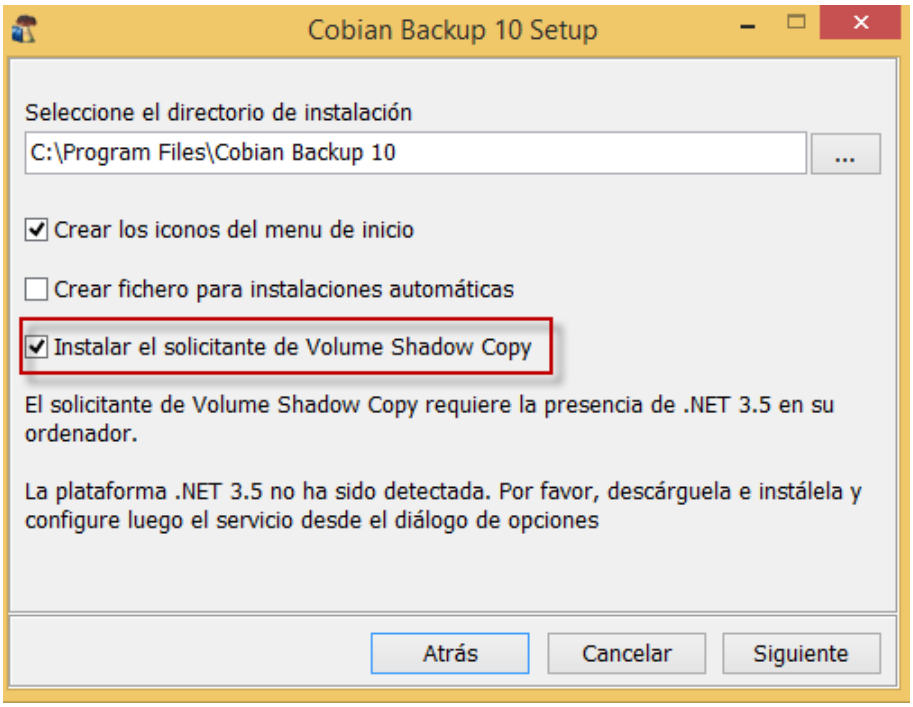
Podemos ter un control e monitoreo das nosas copias en todo momento, xa que se nos xenera un log no noso directorio persoal.



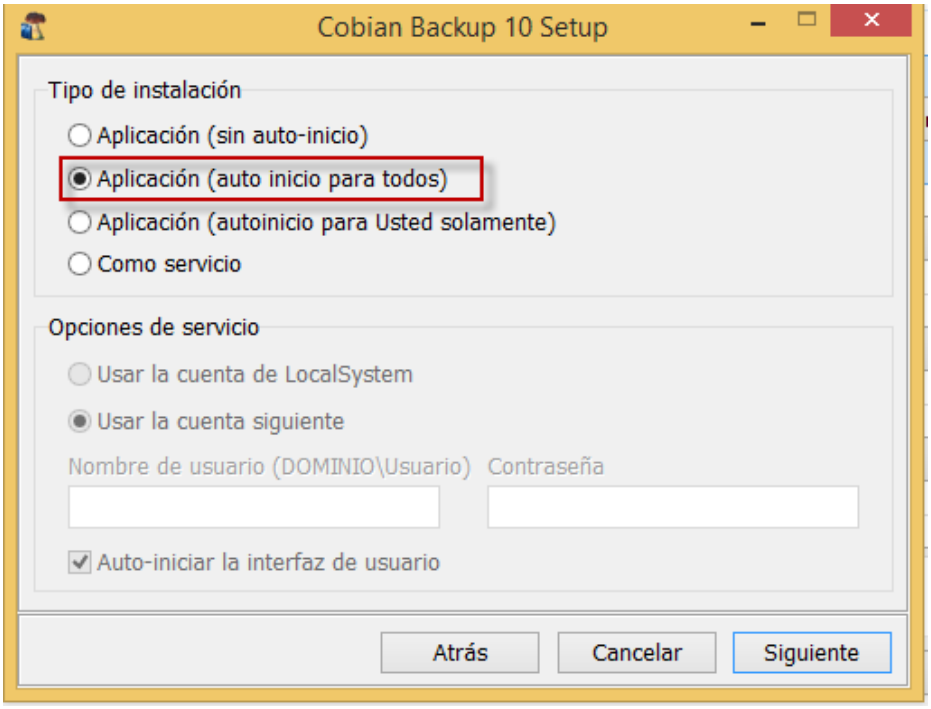
3. Copias de seguridade con aplicación específicas.

A parte das utilidades internas de cada sistema temos a opción de realizar copias de seguridade con ferramentas de terceiros.

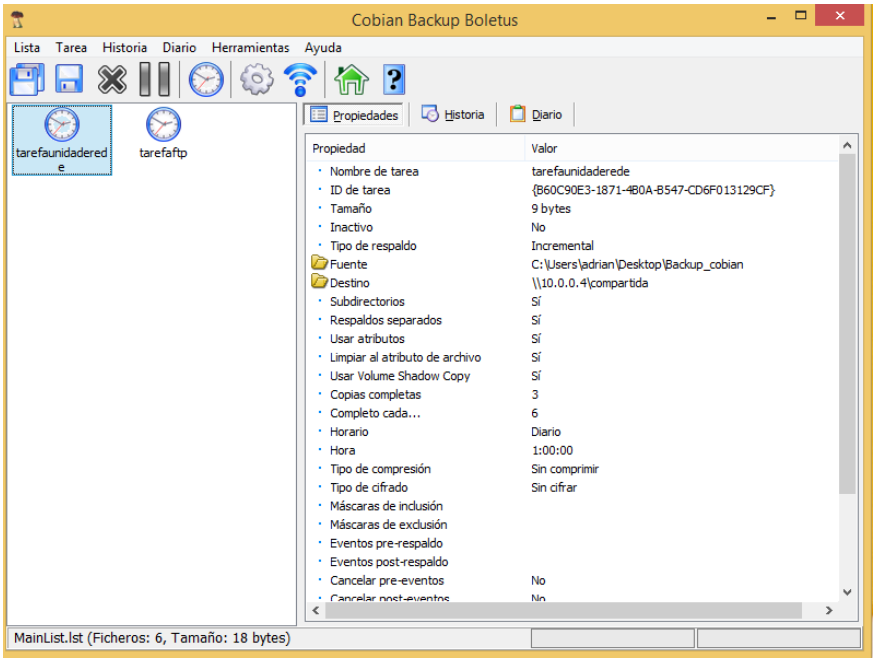
No caso de Windows usaremos Cobian Backup 10, co solicitante de volumen ShadowCopy.



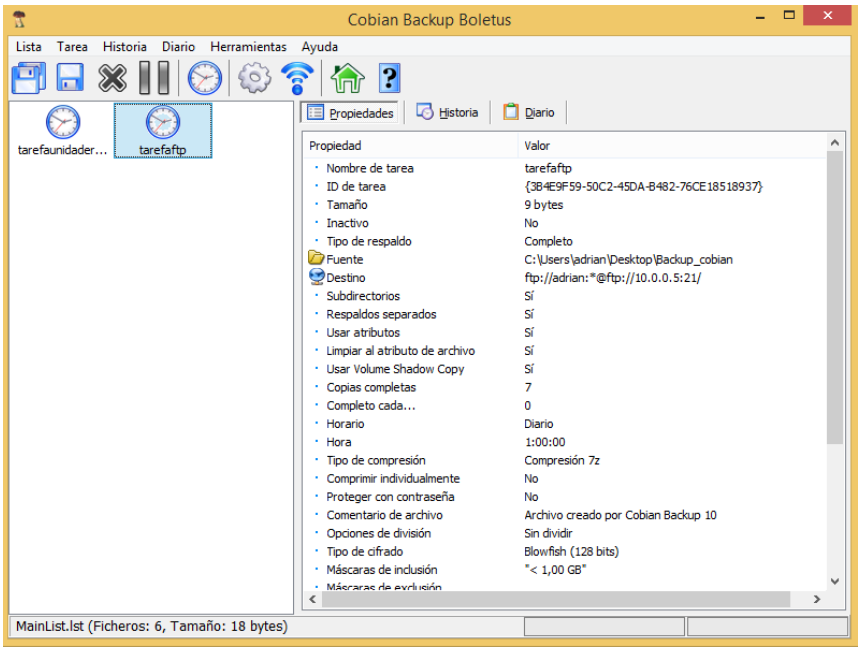
Marcamos que o instale para todos os usuarios e NON como servizo xa que de ese modo non funcionaría o ShadowCopy



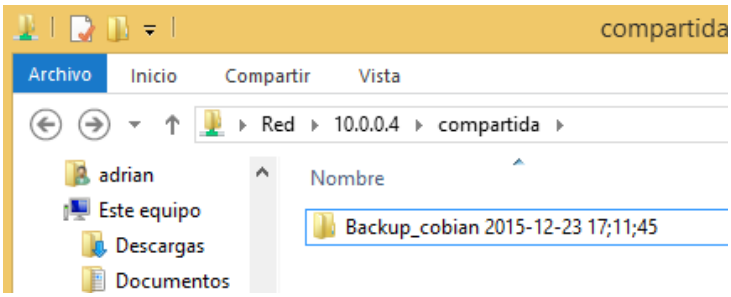
Creamos duas tarefas, a primeira chamada “tarefaunidaderede”, cas características:
- Fará unha copia de seguridade incremental sen compresión nunha unidade de rede.
- Cada 6 copias incrementais para unha completa.
- Manteranse 3 copias completas.
- Cada copia farase diariamente ás 1.00 da mañá.



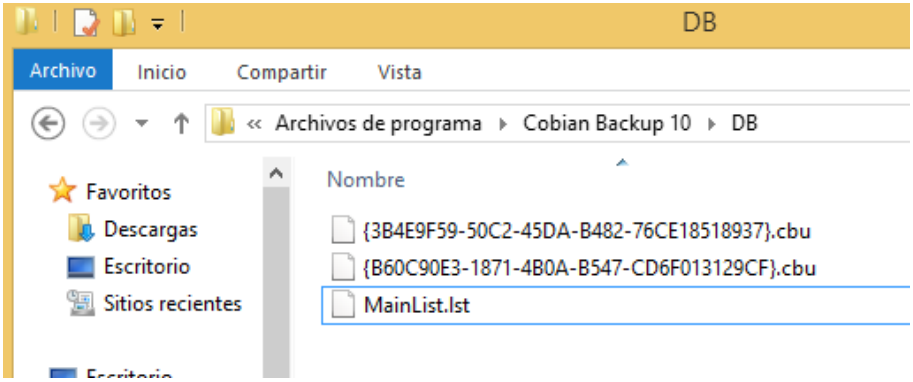
A segunda tarefa chamada “tarefaftp” terá as seguintes características principais:
- Subirá a copia ao servidor FTP que teñades configurado.
- Fará unha copia de seguridade completa de forma manual.
- Manterá ata 7 copias completas.
- Aplica un filtro para que só almacene os arquivos de menos de 1GB.
- Estará comprimida e encriptada con AES 128 bits



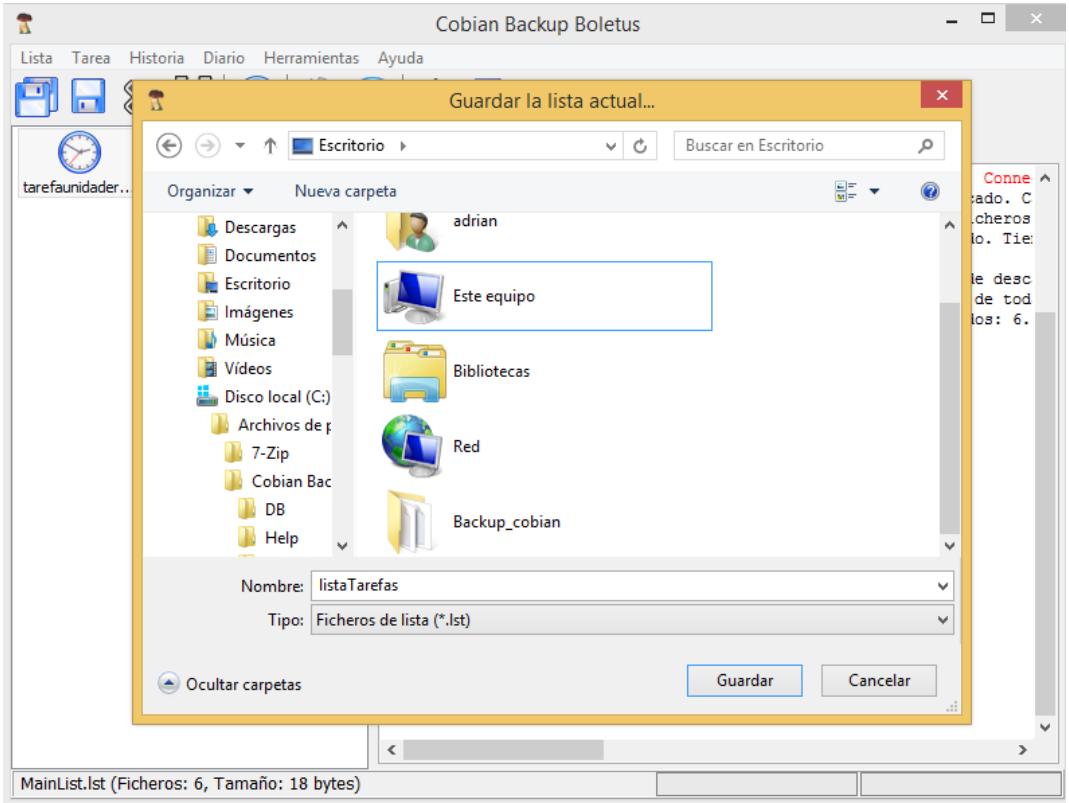
Como comprobante vemos que realizou esta copia de proba na unidade de rede indicada na primeira tarefa.



Agora gardaremos as tarefas nunha lista única. Por defecto xenérase na propia carpeta de instalación de "Archivos de Programa\Cobian Backup 10\DB" un .lst cos seus .cbu que sería os ficheiros que guardan a información de cada tarefa creada.



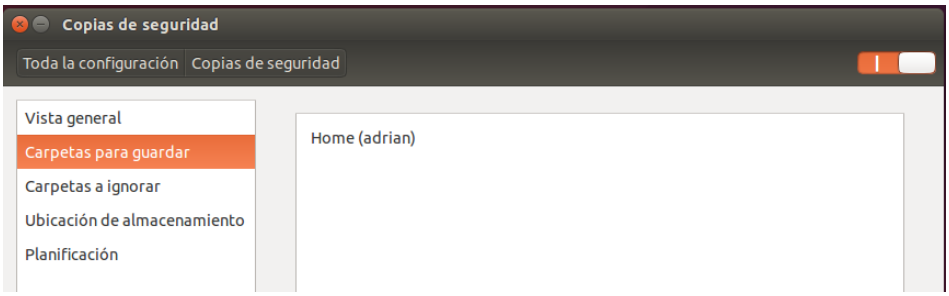
Ainda que temos tamén a posibilidade de gardar unha lista na ubicación que queiramos.



No caso de realizar copias de seguridade con software de terceiros para sistemas Linux.

Neste caso usaremos Dejà Dup, na nova versión de Ubuntu este pasa a ser “Copias de seguridade” nativamente no sistema.

Realiza un backup no propio sistema (en /home/deja-dup) de forma semanal e que se manteña 1 ano. Fai copia de /home/<<usuario>>



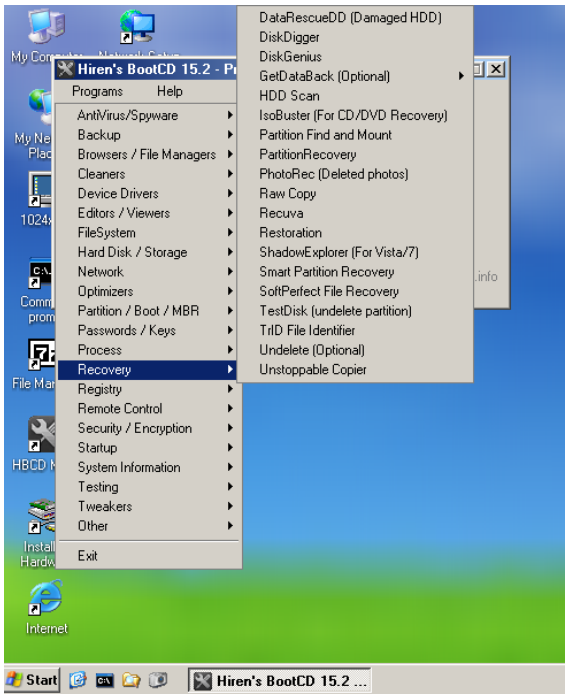
Adicionalmente establécese unha contrasinal para cifrar o bakcup.

4. Comparativa de software de recuperación de datos.

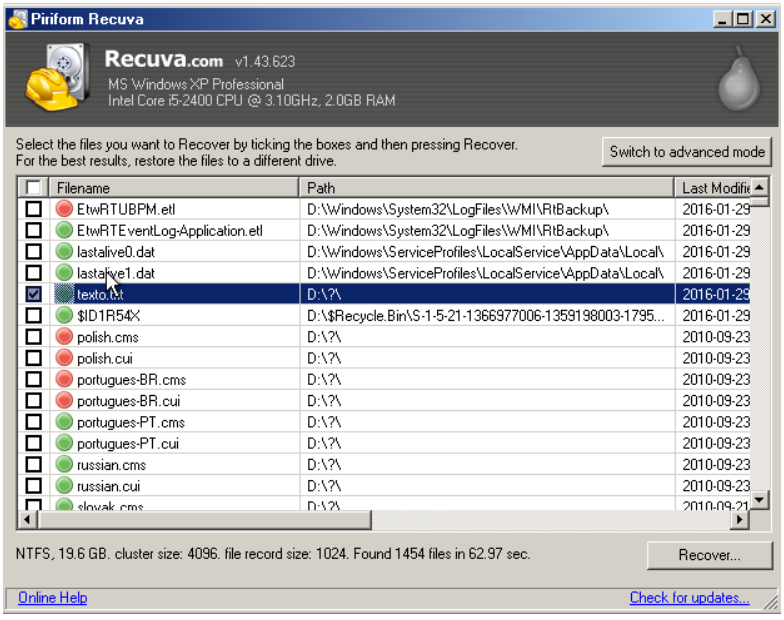
Para esta comparativa faremos uso de diversas ferramentas para a recuperación de información.

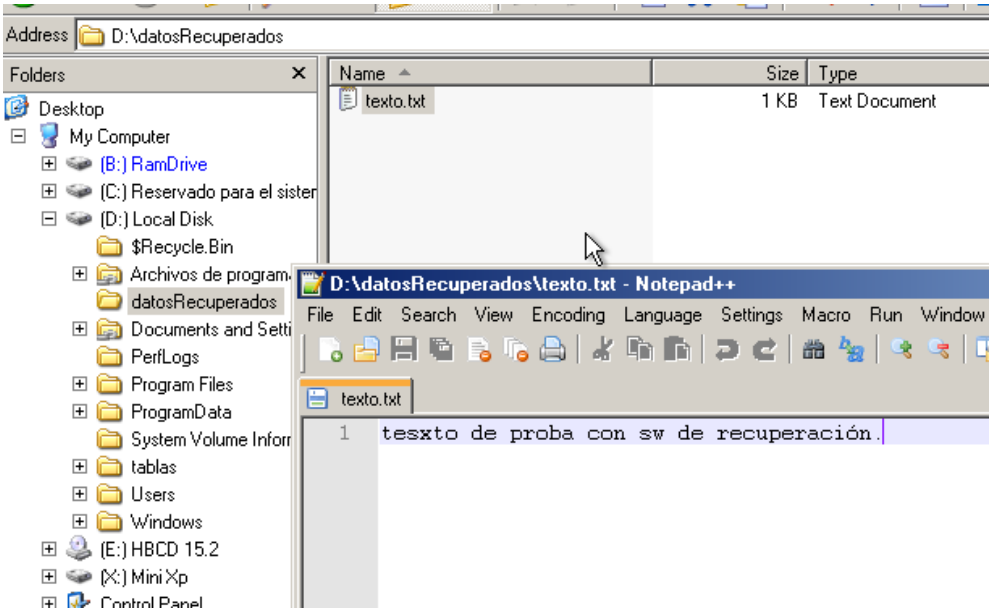
O normal nestes casos e facer uso de sistemas Live, xa que este cárgase na memoria RAM diste modo evitamos a posible alteración do disco propio do sistema o cal queremos recuperar os datos eliminados.

Comezaremos por **Recuva** execútase a través de Hiren's Boot e ten unha interfaz amigable.

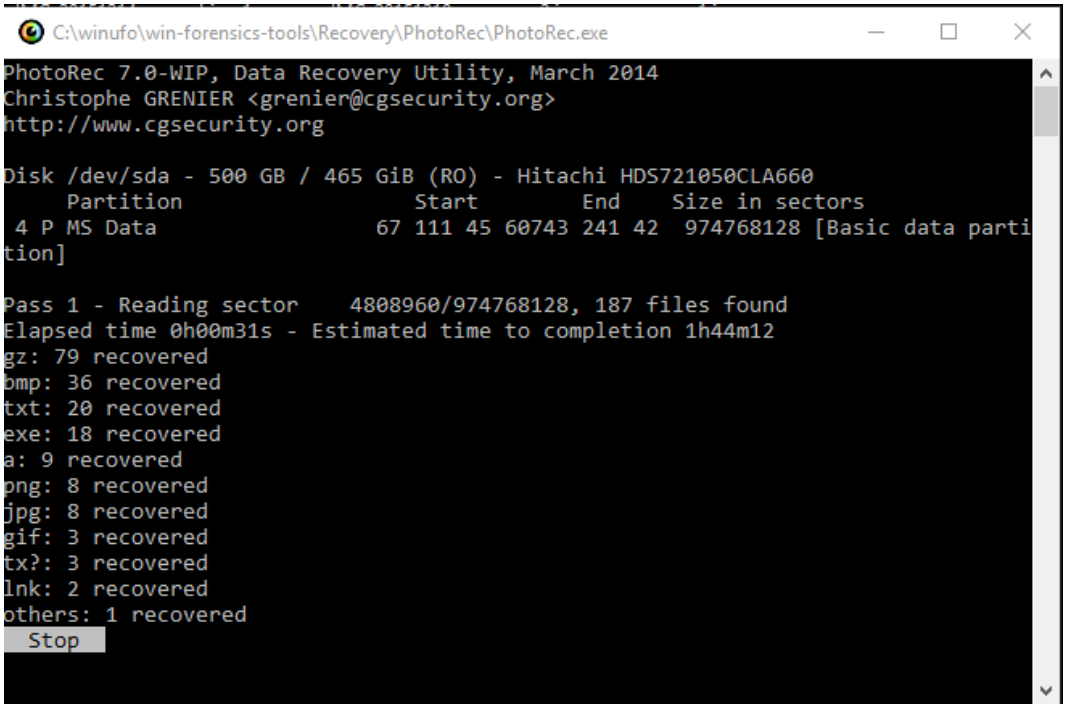


Neste exemplo para que se a búsqueda non tardase demasiado, creei un ficheiro de texto simple e borreino, o cal con Recuva despois de facilitarlle o path de búsqueda non lle levou demasiado tempo encontralo e recuperalo por completo.

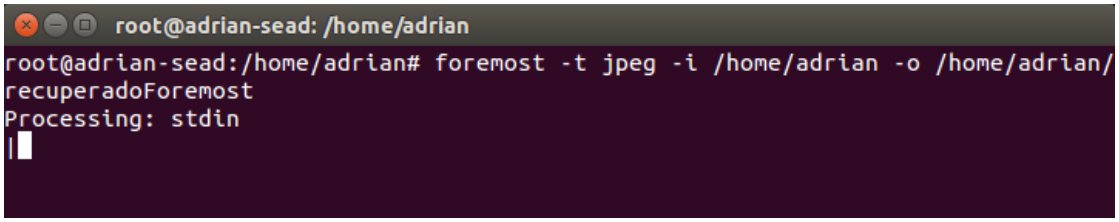




PhotoRec e outra ferramenta especializada na recuperación de ficheiros de tipo formato de imaxen. E por consola de comandos faise intuitivo interactuar con ela, nas probas realizadas como vemos, despois de seleccionar o directorio e os principais e habituais parámetros de búsqueda, xa empezou a recuperar ficheiros que previamente se eliminaran, o único pero e que é lenta a hora de recostruir e resturar os ficheiros encontrados.

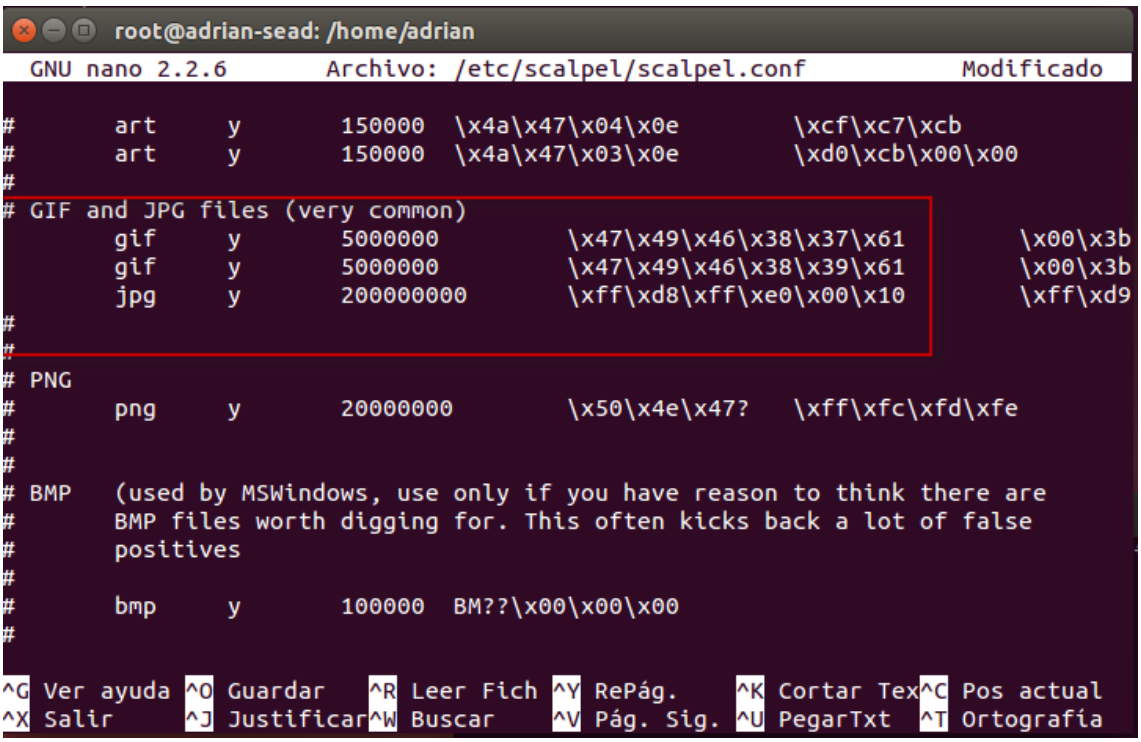


Foremost e outra ferramenta de recovey data, na que como exemplo intento recuperar uns ficheiros de imaxe creados. Simplemente especificamos o tipo de ficheiro co modificador –t, e co –o especificamos a directorio de saída onde se gardarán os ficheiros recuperados.
E sinxela de usar, o único inconvinte e quizás que tarda un chisco máis do normal para recuperar so dúas imaxes jpg de pouco tamaño.



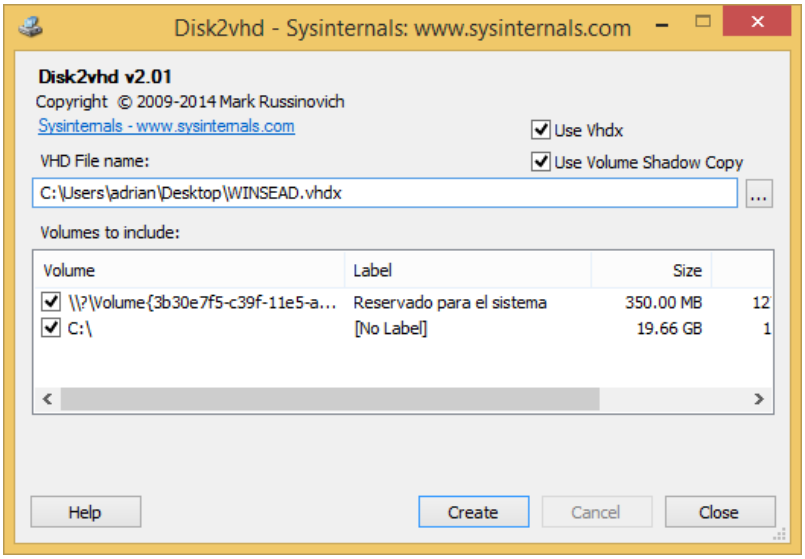
Scalpel e outra ferramenta para usada para recuperación de datos, o interesante de esta ferramenta e que no ficheiro de configuración, por defecto "/etc/scalpel/scalpel.conf" podemos elexir entre que tipos de formato podemos incluir ou excluir nas búsquedas, de modo que así se axilize o tempo de da posible recuperación de datos.
A sintaxis sería sinxela o igual que foremost. O único inconvinte e que non se pode usar no mesmo sistema no que se queren recuperar os datos.

sudo scalpel /home/usuario/documentos -o /home/cartafolRecupera

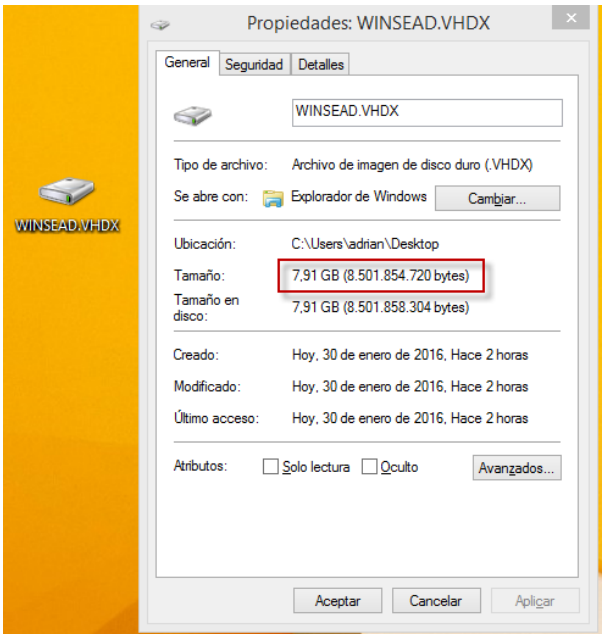


5. Actualización segura de sistema, virtualización de discos e borrado seguro.

Disk2vhd e unha ferramente de sysinternal un partner importante de Microsoft, a cal está dispoñible de forma gratuita e que permite facer unha clonado do disco. Curiosamente podemos facer o clonado de dito disco co propio equipo correndo.



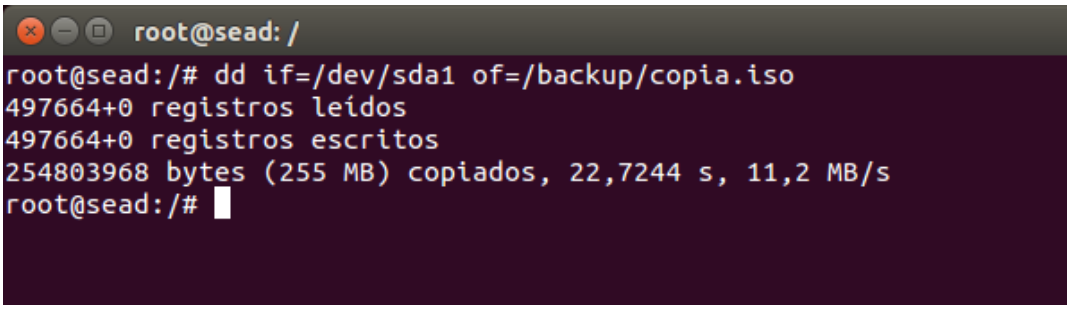
Vemos que ainda que todo o disco ocuparía uns 20GB, este aparece comprimido en apenas 8GB.



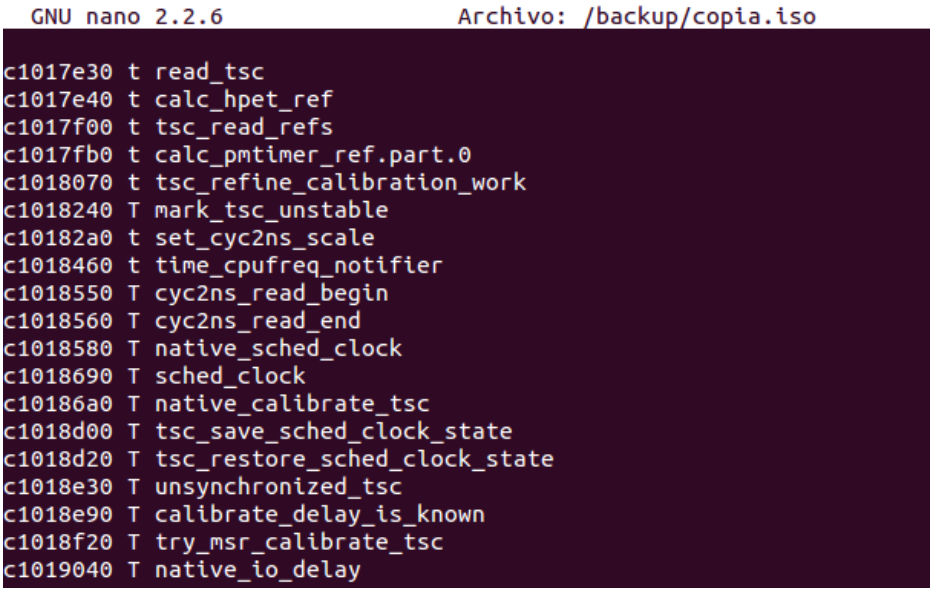
No caso de cargar esta imaxe nunha máquina virtual en virtualbox por problemas de compatibilidade drivers pode darse o caso de que nos falle o sector de arrinque do sistema. Para recupéralo podemos seguir estos pasos:
http://www.zonasystem.com/2014/02/recuperacion-de-arranque-en-windows-7.html

DD (Dataset Definition) e a ferramenta por comandos usada en entornos Linux para poder facer copias exactas de unidades, cartafoles ou arquivos.

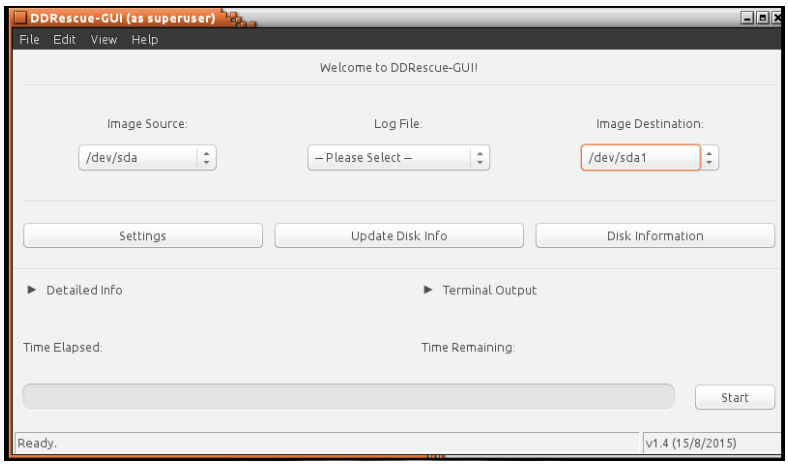
Neste exemplo copiase unha das unidades do sistema.



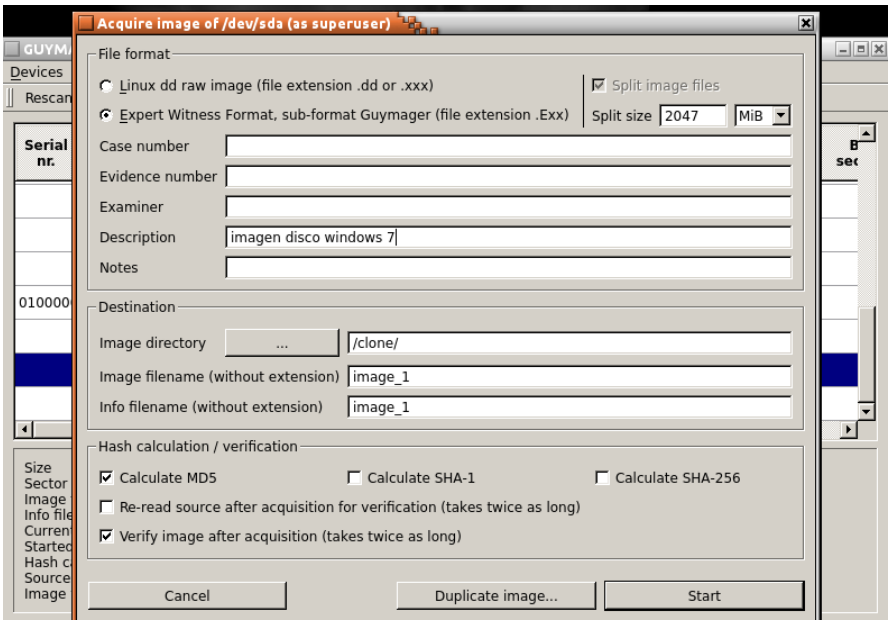
O contido do ficheiro .iso



Outra forma **sería a interfaz gráfica de DD** que a podemos encontrar en Caine, un LiveCD especializado con ferramentas de análise forense.
Seleccionando orixe e destino da imaxe a realizar, o destino pode ser un dispositivo extraible.



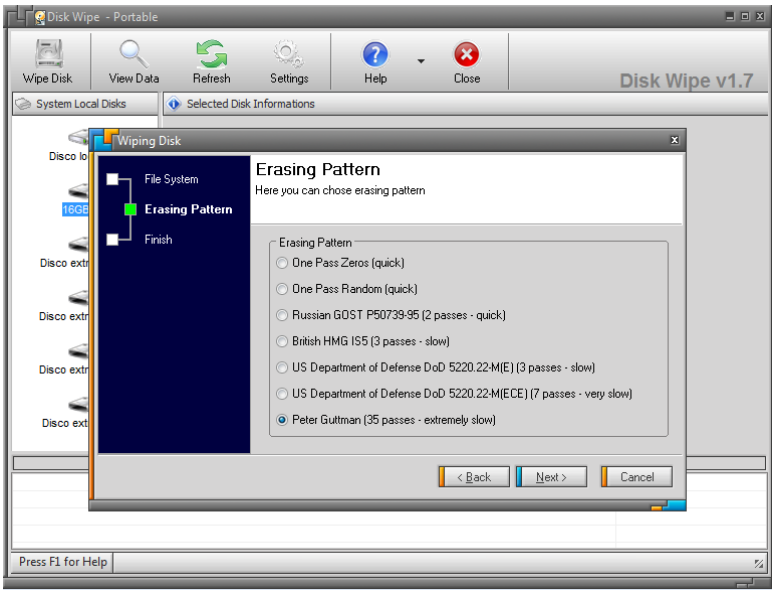
Dentro de Caine tamén podemos facer uso de **Guymager** outra ferramenta para crear imaxes ou clones de discos.



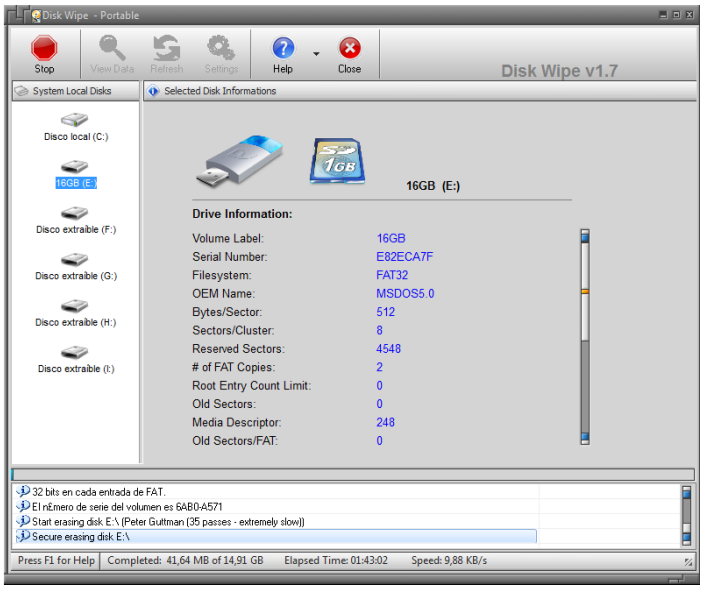
Borrado seguro de unidades.

Sempre que escribimos información nun dispositivo, ainda que o formateemos esta sigue permanezendo ahí de forma oculta. Aconséllase o borrado seguro a un formateo e escribir un número de veces encima do eliminado, e decir, básicamente unha sobreescritura, depende o número de veces será máis o menos difícil a sua recuperación.

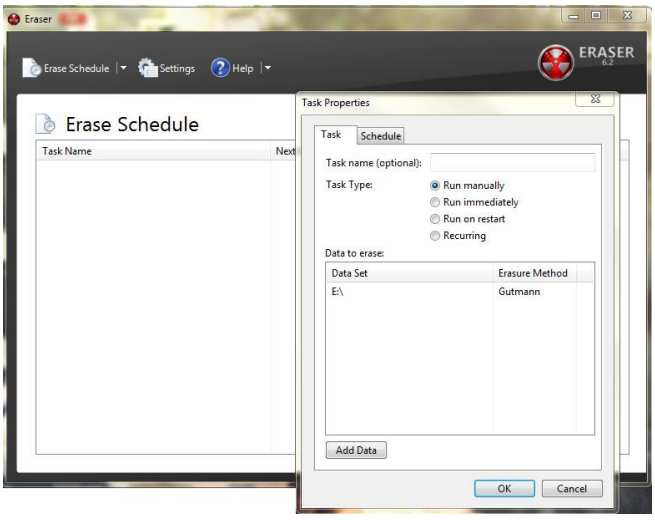
Disk Wipe e unha utilidade que nos permitirá facer un borrado seguro de dispositivos ou discos. Podendo establecer o tipo de técnica para a cantidade de veces de sobreescritura.



Neste caso realizase un borrado de 35 sobreescrituras nun pendrive de 16GB.



Eraser e outra utilidade para o borrado seguro, también con posibilidade establecer o tipo de técnica para o seu borrado seguro e a selección de unidades a borrar. Máis sinxela que Disk Wipi polo que estiven probando. Pero persoalmente quédome con Disk Wipe.



6. Conclusións

Chegamos as conclusións de que podemos facer bakcups de calqueira información que teñamos e as utilidades que os propios sistemas incorporan.

A información almacenada en unidades pódense replicar (clonar), recuperar información e borrar de forma segura con utilidades disponibles de forma gratuita, obviamente cas suas limitacións o tratarse de ferramentas free.

Técnicas como as de esta práctica úsanse sobretodo para o análise forense. Víronse utilidades a nivel software de sistema pero no mercado existen “station docks” de clonado nas que se fan copia bit a bit dun mismo disco ou outro dispositivo suelen se usar a niveis profesionais debido o seu elevado coste.

Hai que entender con isto de que ninguna información está segura pese a ser borrada, e sempre hay posibilidade dunha posible recuperación da misma, usando as utilidades axeitadas.