TRUECRYPT

TrueCrypt es una aplicación para cifrar y ocultar datos que el usuario considere reservados empleando para ello diferentes algoritmos de cifrado como AES, SERPENT o Twofish o una combinación de los mismos, o lo que es lo mismo permite crear un volumen virtual cifrado en un archivo de forma rápida y transparente.

Existen versiones para sistemas operativos Windows XP/2000/2003/Vista/7, MACoSy Linux y la última versión es la 7.1a, publicada el 7 de febrero de 2012.

TrueCrypt se distribuye gratuitamente y su código fuente está disponible, aunque bajo una licencia restrictiva.

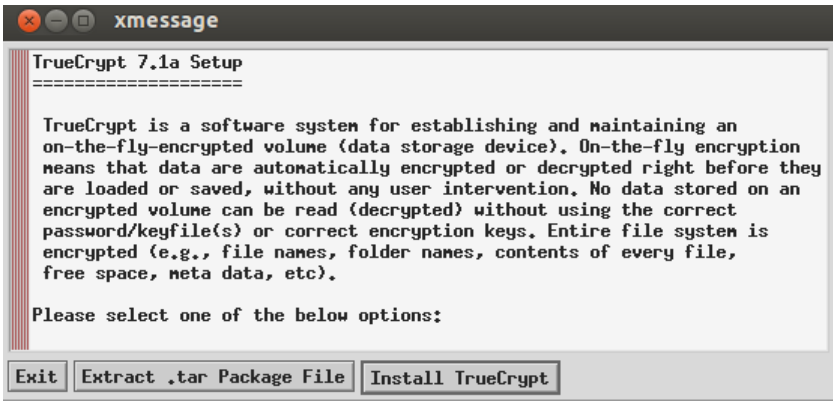
Existen varias formas de encriptar información como:

- Una archivo llamado como nosotros deseemos mezclado con los demás archivos dentro de un pendrive, y que solo es posible abrir con truecrypt, dentro del cual estaran todos los archivos encryptados (el problema es que se puede eliminar como cualquier otro archivo)
- Una partición completa del pendrive oculta, lo que permite que al pinchar el pendrive simplemente no ocurre nada, es como si no hubiéramos pinchado nada, ya que la partición esta oculta y esta todo sin formato (generalmente en windows nos dira si deseamos formatear la unidad, y a que según el no tiene formato).
- Particionar un pendrive en dos, dejando una partición normal y la otra oculta, con lo que al pinchar un pendrive por ejemplo de 1GB, aparecería como un pendrive de 512MB y no se vería nada mas, y al montar con Truecrypt la partición oculta, nos montaría otro pendrive de 512MB con los datos ocultos.

Sea cual sea el sistema utilizado cuando ejecutamos truecrypt y montamos la unidad encryptada lo que nos generara siempre sera otra unidad diferenciada donde estén todos los datos encryptados.

INSTALACION DE TRUECRYPT EN UBUNTU

Para instalar truecrypt debemos bajarnos desde la pagina oficial www.truecrypt.org el archivo para ubuntu – linux standart 32 bits, y abrirlo con el gestor de archivadores para descomprimir el instalador que tenemos dentro (truecrypt-7.1a-setup-x86) y lo ejecutamos desde el terminal, apareciendo la siguiente pantalla:



Pulsamos a Install Treucrypt y aceptamos la licencia, nos pedirá la clave de administración para poder instalarlo y terminara la instalación.

Nos generara entonces un acceso directo al programa denominado truecrypt y el programa estará instalado.

NOTA IMPORTANTE: La instalación en linux tiene el problema de que para poder montar unidades el usuario debe ser administrador o introducir contraseña de administración por lo que para poder utilizarlo en un usuario normal debemos incluir en el fichero /etc/sudoers la siguiente linea:

- usuario ALL=(root) NOPASSWD:/usr/bin/truecrypt

donde usuario sera el nombre del usuario que deseemos que puede ejecutar truecrypt sin preguntarle la contraseña de administración

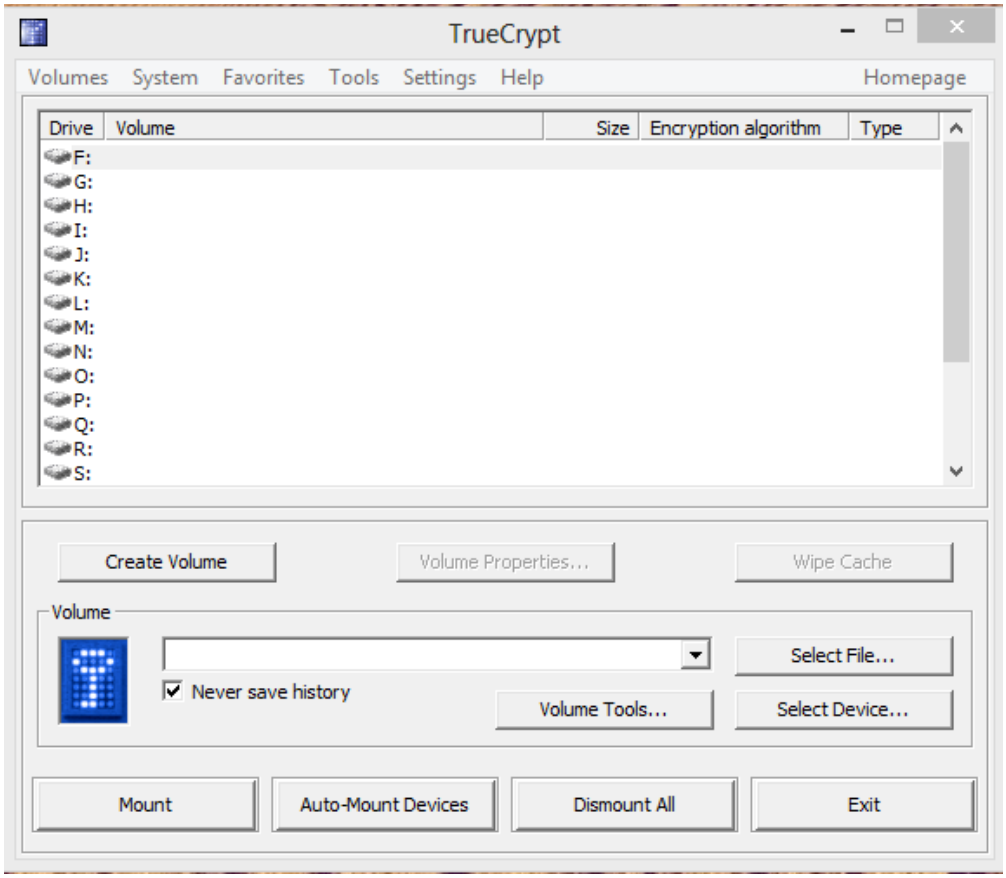
INSTALACION DE TRUECRYPT EN WINDOWS

Se instala como una aplicación normal, solo debemos descargarla desde www.truecrypt.org e instalarla.

Existe también una versión portable que podemos llevar en nuestro pendrive para poder desencryptar nuestros datos en cualquier lugar donde tengan windows.

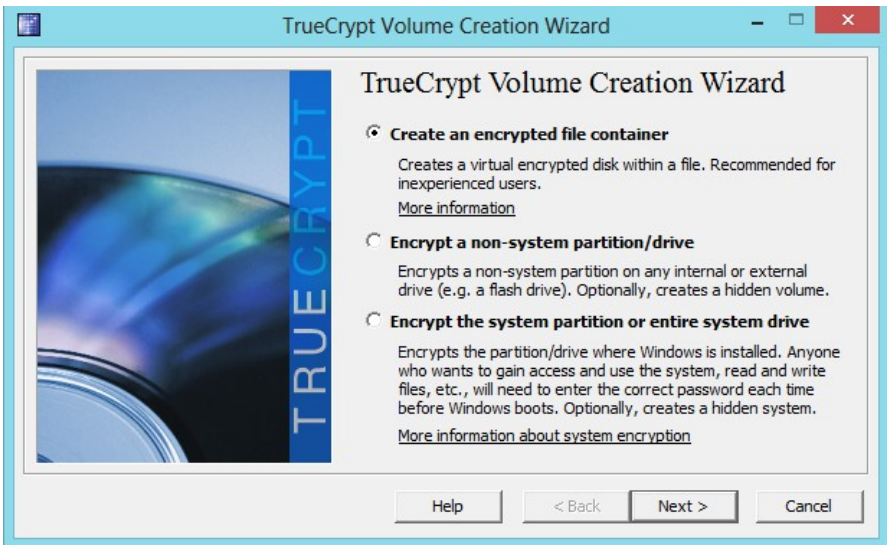
GENERAR ARCHIVOS ENCRYPTADOS DESDE TRUECRYPT

El programa truecrypt es idéntico tanto en linux como en windows por lo que lo explicado aquí sirve para los dos sistemas.



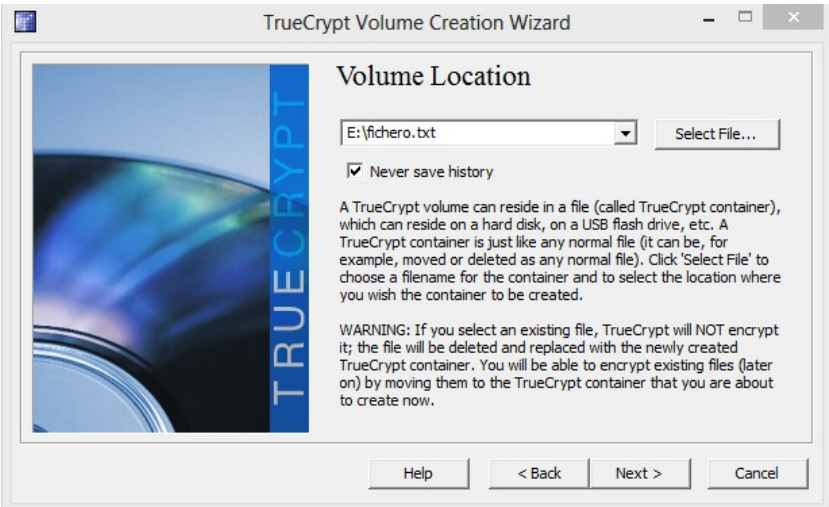
Al iniciar el programa truecrypt nos aparece la siguiente ventana donde podemos tanto crear como montar unidades encryptadas, en nuestro caso vamos a crear un fichero encryptado denominado fichero.txt por ejemplo.

Así que le damos a Create Volume y nos aparece la ventana de selección de creación:

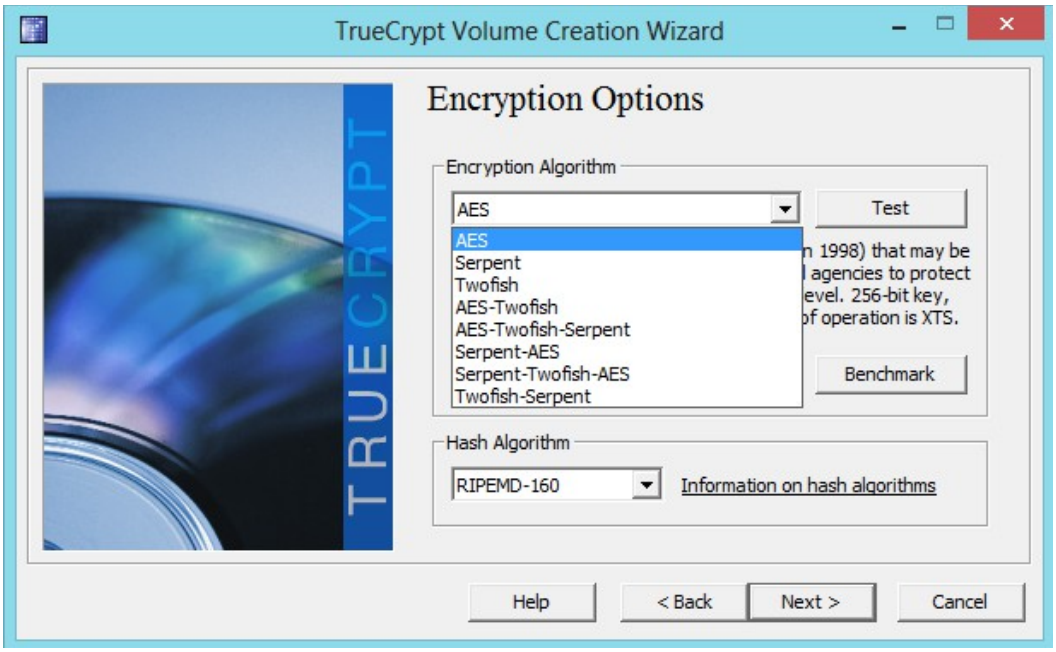


En nuestro caso como deseamos crear un fichero encryptado le damos a la primera opción Create Encrypted file container, tras lo cual nos preguntara si deseamos crear un fichero normal encryptado o uno oculto, para este ejemplo lo haremos normal.

Nos aparece entonces donde deseamos crear dicho fichero, le indicamos que el pendrive que tenemos pinchado

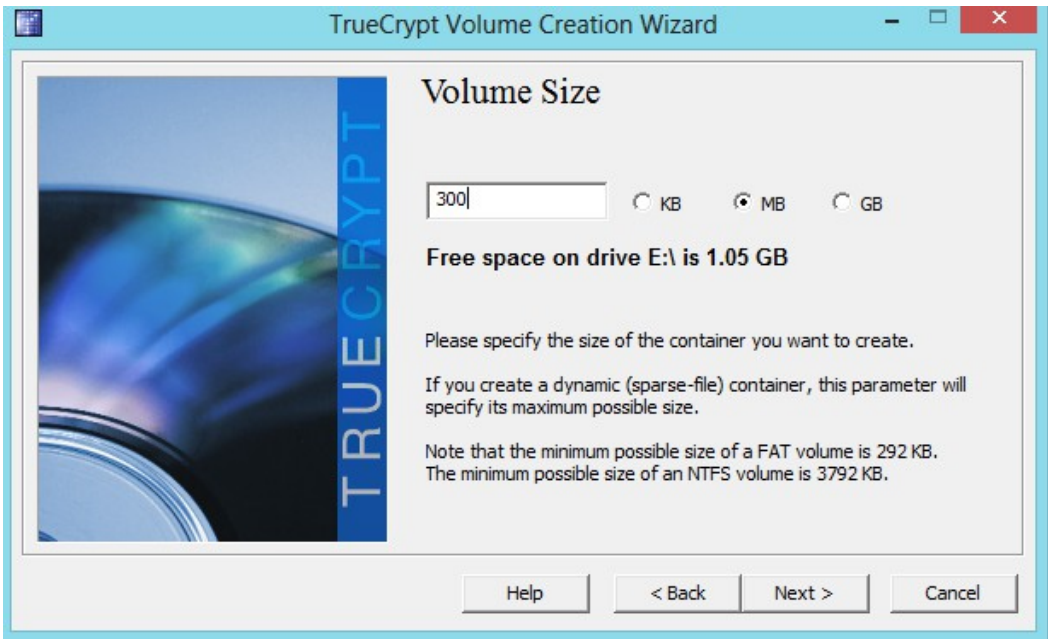


A continuación nos pregunta con que sistema encryptacion deseamos proteger nuestro fichero:



En principio con un sistema AES tendríamos suficiente, pero cada uno es libre de aplicar uno u otro según la elección del usuario, y después nos pregunta que tipo de algoritmo de clave queremos, RIPEMD-160, SHA-512 o Whirlpool, aquí seleccionaremos SHA-512, con lo que habremos protegido el fichero con un algoritmo de cifrado AES-SHA de 512bits, un protocolo bastante fuerte y fiable.

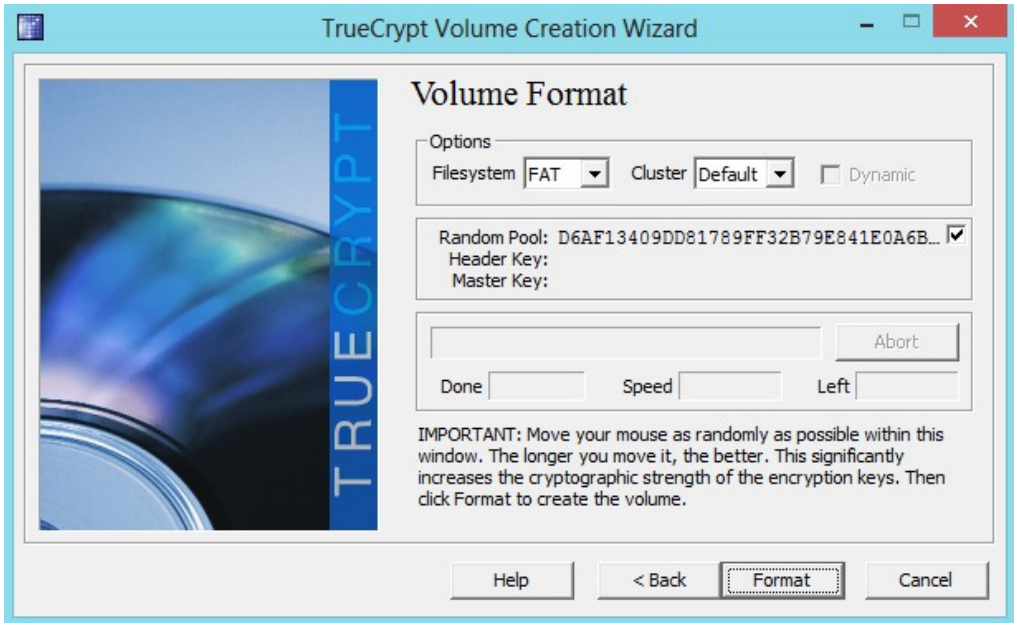
Nuestro fichero sera como un volumen de datos, como un pendrive encryptado pinchado en el ordenador por lo que deberemos asignarle que tamaño de archivo deseamos que tenga, teniendo en cuenta los documentos que deseemos meter dentro, en principio este sistema que hemos creado sera para guardar documentos que no van a ocupar gran parte de nuestros ficheros guardados ya que si no utilizaríamos cualquiera de los otros sistemas (Encyptacion de partición o Encryptacion de unidad entera), por lo aplicaremos un tamaño de 300Mb por ejemplo.



A continuación nos pedirá la contraseña de para cifrar el archivo, hay que tener en cuenta que en la contraseña puede ser el punto mas debil de nuestro sistema, ya que si aplicamos una contraseña sencilla no sirve de nada aplicarles grandes sistemas de encryptacion pues con fuerza bruta seria sencillo romperla.

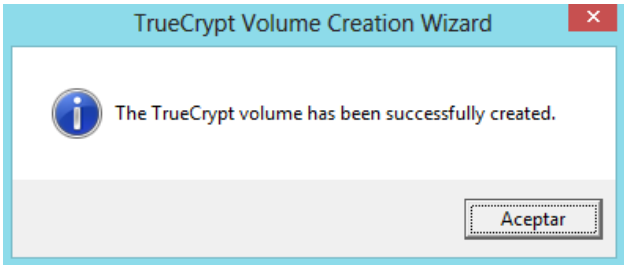
Existe una opción llamada Use Keyfiles donde permite asociar un fichero dentro del sistema como segunda contraseña, es decir, solo se podrá descomprimir si la contraseña es correcta y el archivo que indicaste coinciden, dando mas seguridad que la simple contraseña pero también tienes que tener dicho archivo en el lugar donde quieras desencryptarlo, dejándote solo la opción de llevarlo siempre junto al fichero encryptado, o solo poder desencryptarlo en un lugar, por lo que no la usaremos por ahora.

Lo siguiente que preguntara sera el sistema con el cual deseas formatear dicho volumen, aunque este dentro de un fichero para poder montarlo necesita un sistema.



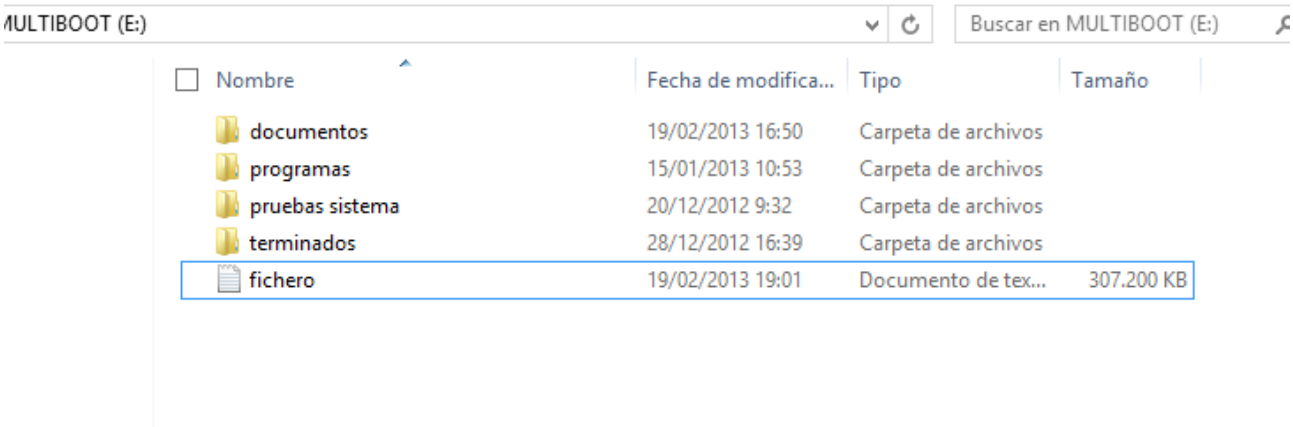
Dejamos FAT si no vamos a colocar archivos de mas de 4GB, que en nuestro caso al ser de 300Mb nunca va a suceder y la damos a Format.

Comenzara el formateo e ira rápido, hasta el final, donde se parara unos minutos (es normal) y si todo a funcionado correctamente nos dará una ventana de confirmación de la creación.



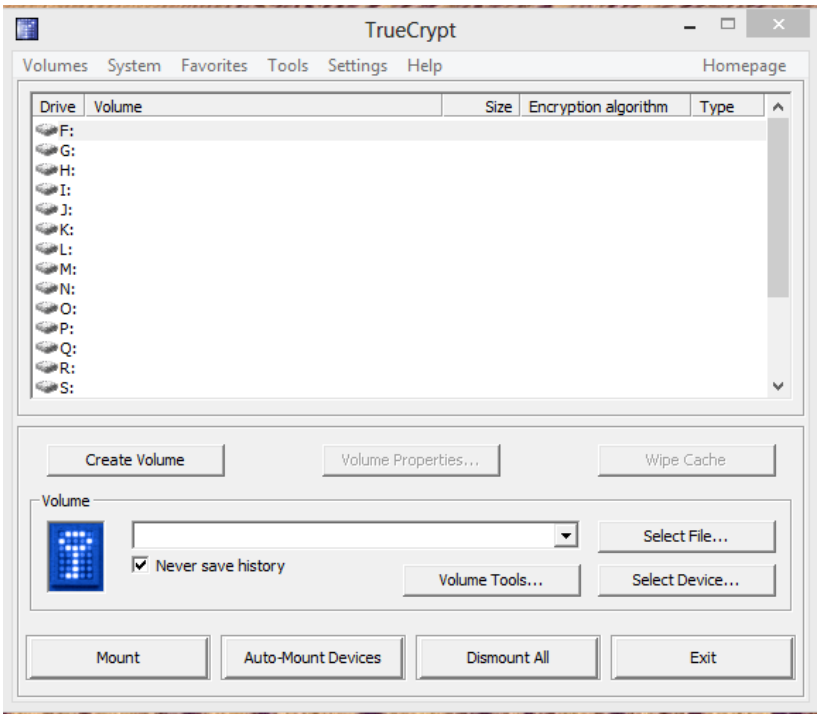
Aceptamos y volverá a aparecer la ventana de creación de ficheros por si queremos continuar generando mas ficheros encryptados, así que cancelamos.

Si miramos ahora nuestro pendrive veremos el fichero creado denominado fichero.txt que si abrimos nos aparecerán miles de caracteres indescifrables, con lo que tendremos nuestro fichero encryptado creado.

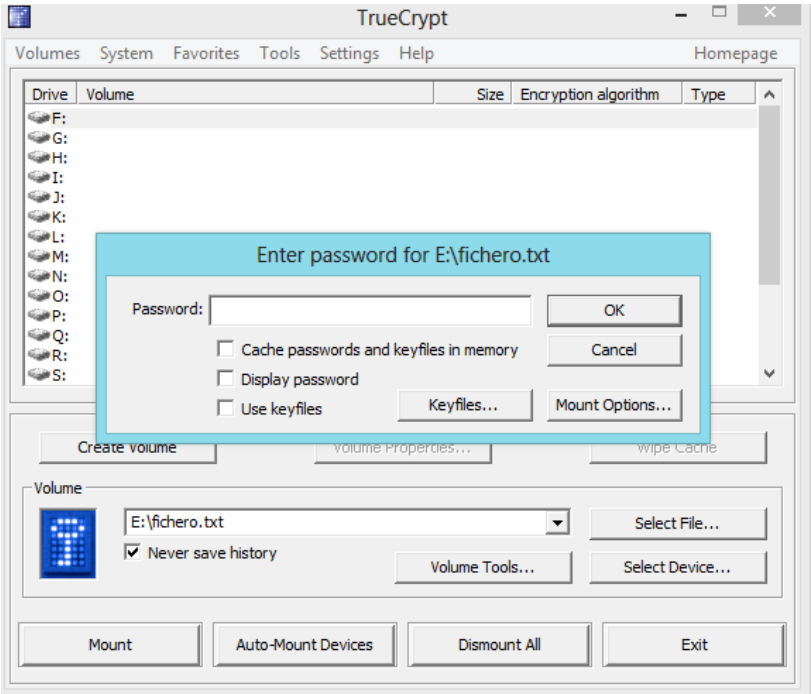


ABRIR UN FICHERO ENCRYPTADO CON TRUECRYPT

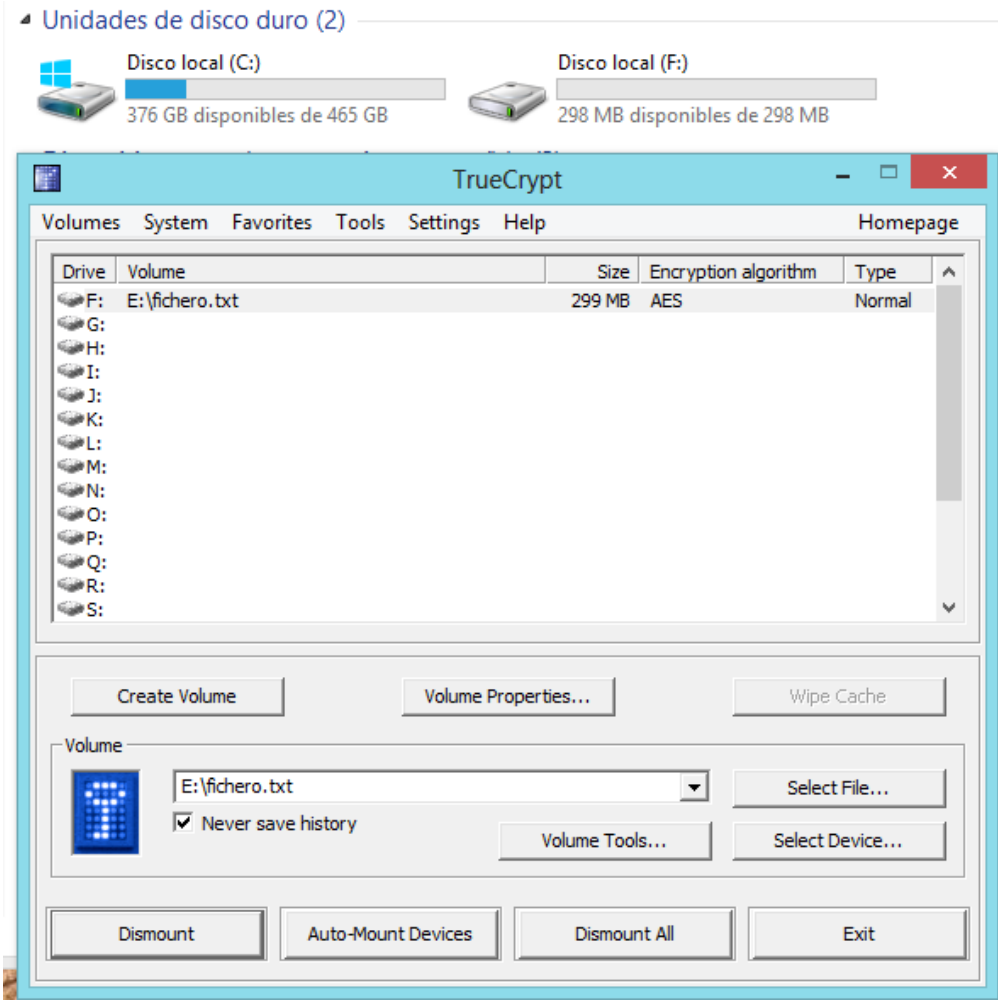
Abrimos truecrypt y le damos a Select File y seleccionamos el fichero que tenemos encryptado.



Le damos a MOUNT y nos pedirá la clave de acceso



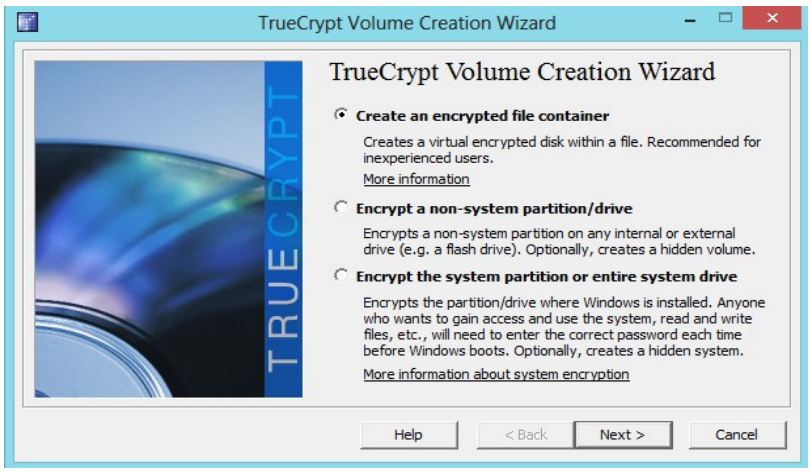
La escribimos y nos montara el archivo como una unidad aparte donde podremos colocar y abrir cualquier fichero que tengamos encryptado.



Después de terminar de trabajar con los ficheros es recomendable que desmontemos la unidad mediante Dismount ALL, aunque si reiniciamos el sistema comprobaremos que la unidad estará desmontada, pero asi nos aseguraremos de que todos los datos se guardan correctamente.

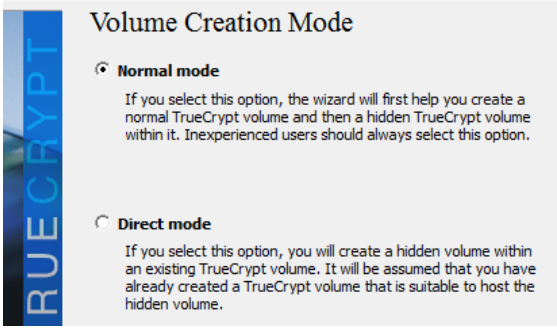
ENCRYPTAR UN PENDRIVE COMPLETAMENTE

Iniciamos el programa truecrypt y le damos a Create Volume; nos aparecerá la ventana de creación de encryptacion

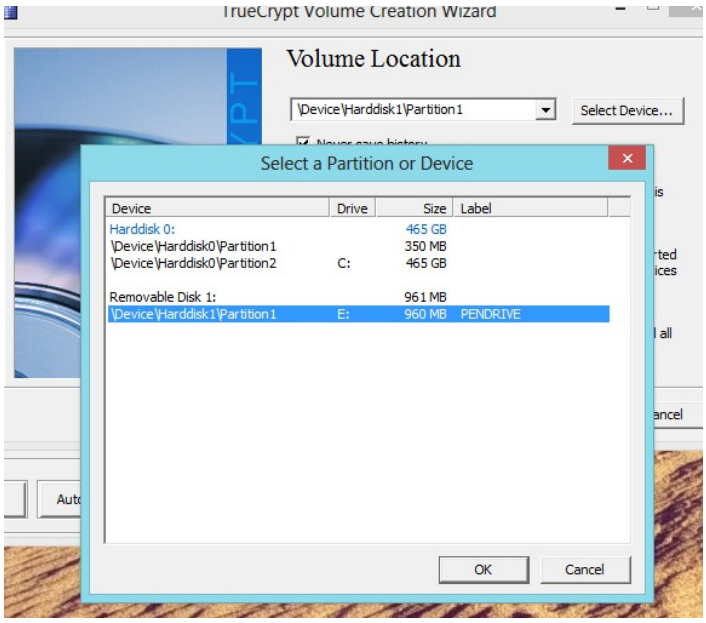


Seleccionaremos en esta ocasión Encrypt a non-system partition/drive y nos aparecerá la opción de crearlo oculto o no.

Vamos a ocultar todo el pendrive por lo que seleccionamos Hidden Truecrypt volume y nos preguntara de que modo queremos crear el volumen, seleccionaremos Normal mode para que nos vaya guiando en todo el proceso.



Nos preguntara en la siguiente ventana cual es el dispositivo que queremos encryptar **(cuidado, todo el contenido de dicho dispositivo se borrara)**

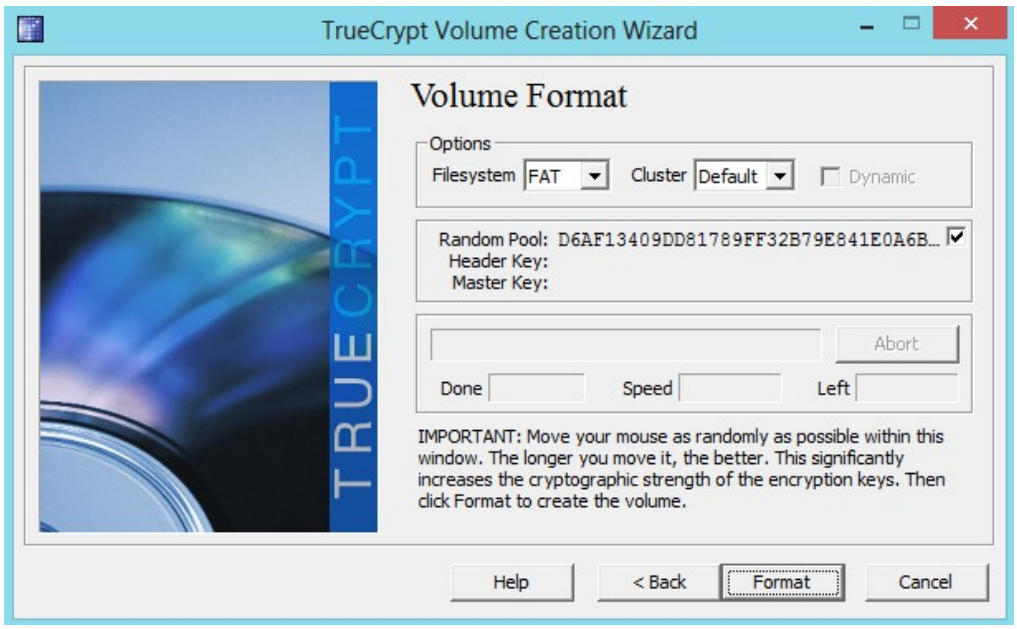


Así que seleccionaremos el pendrive de 1GB que tenemos para probar, hay que seleccionar la partición, le damos a siguiente y aparece la pantalla de elección de encryptacion.

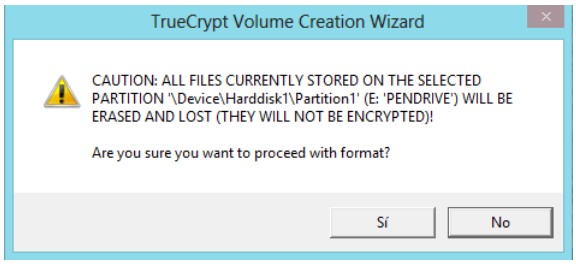
En principio con un sistema AES tendríamos suficiente, pero cada uno es libre de aplicar uno u otro según la elección del usuario, y después nos pregunta que tipo de algoritmo de clave queremos, RIPEMD-160, SHA-512 o Whirlpool, aquí seleccionaremos SHA-512, con lo que habremos protegido el fichero con un algoritmo de cifrado AES-SHA de 512bits, un protocolo bastante fuerte y fiable.

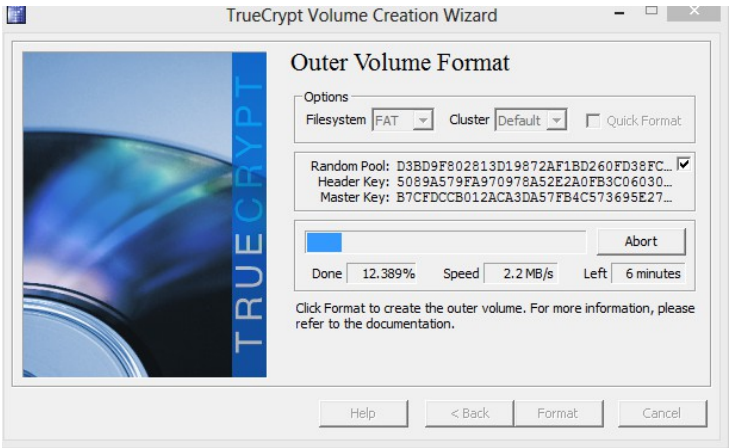
Le damos a siguiente y nos mostrara la pantalla de selección de tamaño, como le hemos asignado todo el pendrive no nos dejara realizar ninguna acción, así que le damos a siguiente y nos pedirá la contraseña para protegerlo.

Le escribimos la contraseña que deseemos y NO marcamos Use Keyfiles (explicado anteriormente), así que le damos a siguiente para ver la pantalla de formateo de la unidad.



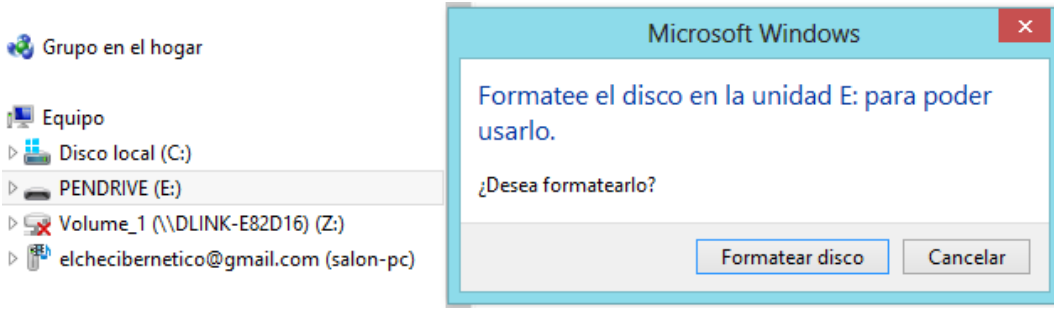
Seleccionamos FAT, y le damos a formatear, nos saldrá una ventana advirtiéndonos de que todos los datos de la memoria van a ser eliminados, así que aceptamos y comenzara a formatear la unidad.





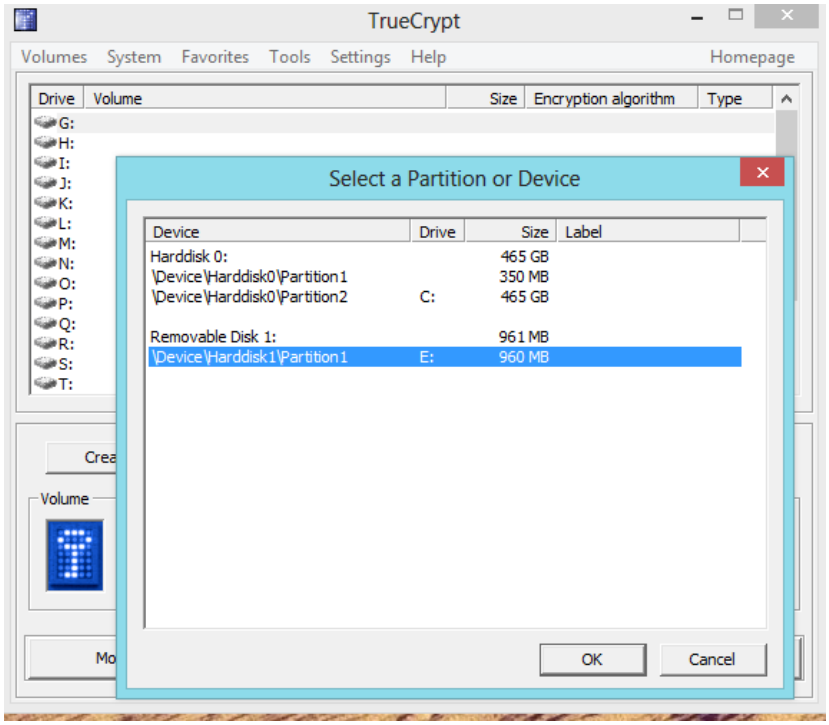
Comenzara el formateo e ira rápido, hasta el final, donde se parara unos minutos (es normal) y volverá a aparecer la ventana de creación de volúmenes por si queremos continuar generando mas volúmenes encryptados, así que cancelamos.

Si en este momento pinchamos despinchamos la unidad o vamos al explorador de archivos en windows, nos preguntara si deseamos formatear la unidad, ya que no la reconoce y en linux ni siquiera preguntara nada como si estuviera pinchado nada.

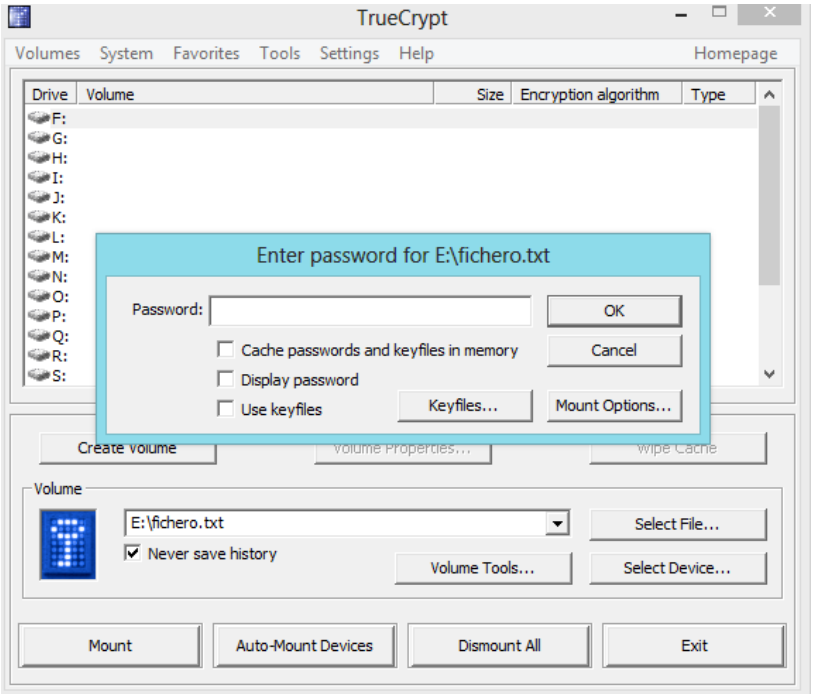


ABRIR UNA UNIDAD ENCRYPTADA CON TRUECRYPT

Abrimos truecrypt y le damos a Select Device y seleccionamos la partición del pendrive que tenemos encryptado.

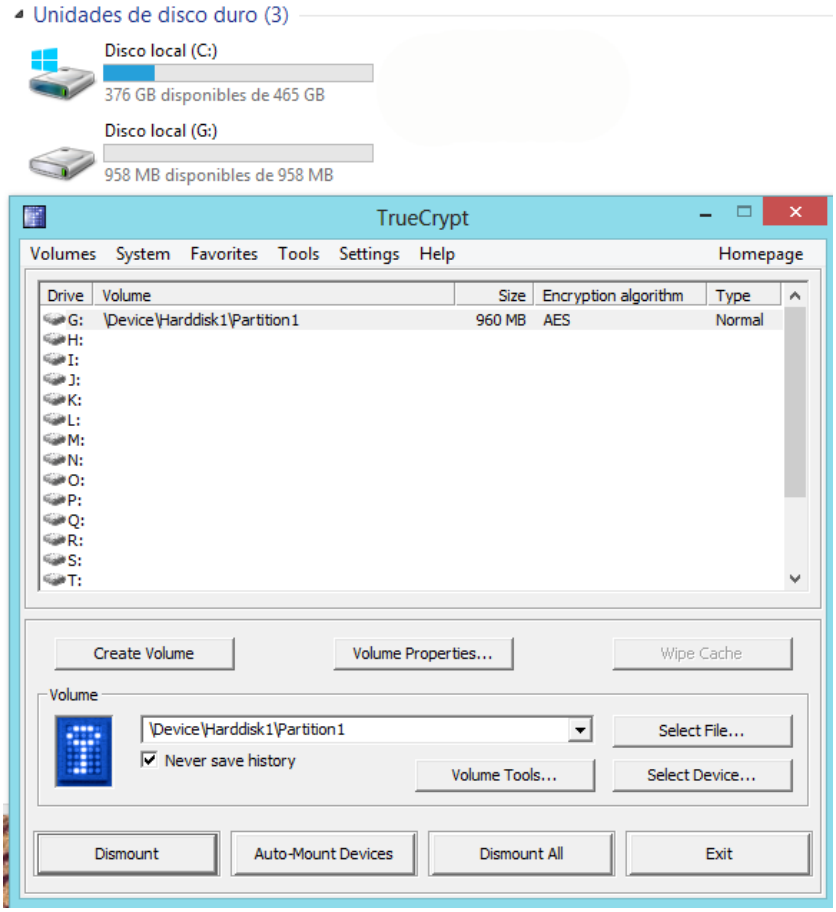


Le damos a MOUNT y nos pedirá la clave de acceso



La escribimos y nos montara el pendrive como una unidad aparte donde podremos colocar y abrir cualquier fichero que tengamos encryptado.

NOTA: Si os da error en la contraseña comprobad que le habéis dado a la partición encryptada y no a la unidad.



Después de terminar de trabajar con los ficheros es recomendable que desmontemos la unidad mediante Dismount ALL, aunque si reiniciamos el sistema comprobaremos que la unidad estará desmontada, pero así nos aseguraremos de que todos los datos se guardan correctamente.

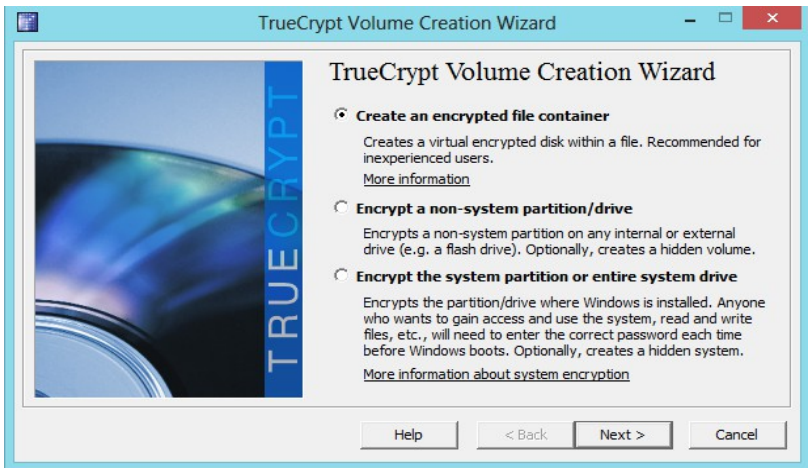
SISTEMA MIXTO DE ENCRYPTADO, MITAD ENCRYPTADO Y MITAD NORMAL

Una buena opción para montar una pendrive encryptado y que se pueda utilizar normalmente seria partir el pendrive en dos particiones, la cual una estaría normal como si de un pendrive normal se tratase y la otra partición estaría oculta y encryptada.

Para el ejemplo utilizaremos un pendrive de 1Gb, de los cuales 500Mb seran normales y los otros 500mb estarán en una partición oculta y encryptada.

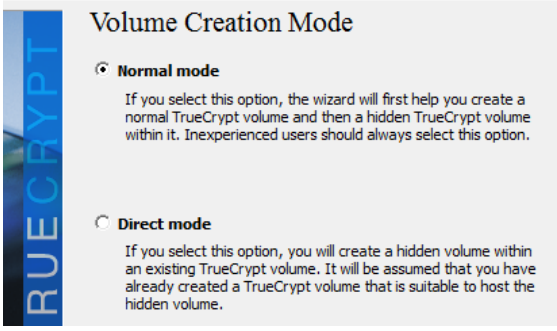
Para poder utilizar este sistema debemos primero partir el pendrive con un programa de particiones, sea en windows o en linux.

Tenemos por tanto una unidad con dos particiones a partes iguales por lo que vamos a encryptar una de las partes, para ello nos dirigimos al programa truecrypt y seleccionaremos Create Volume y nos aparecerá la ventana de creación de encryptacion

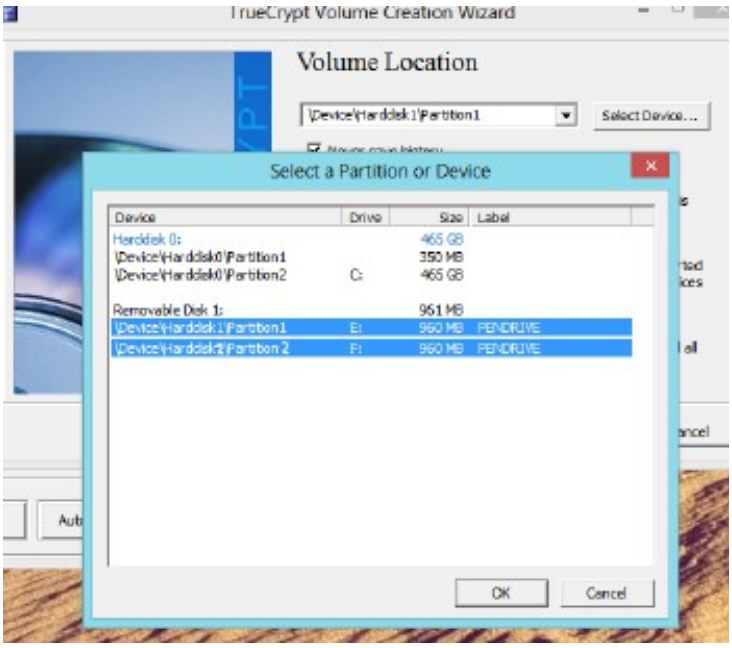


Seleccionaremos en esta ocasión Encrypt a non-system partition/drive y nos aparecerá la opción de crearlo oculto o no.

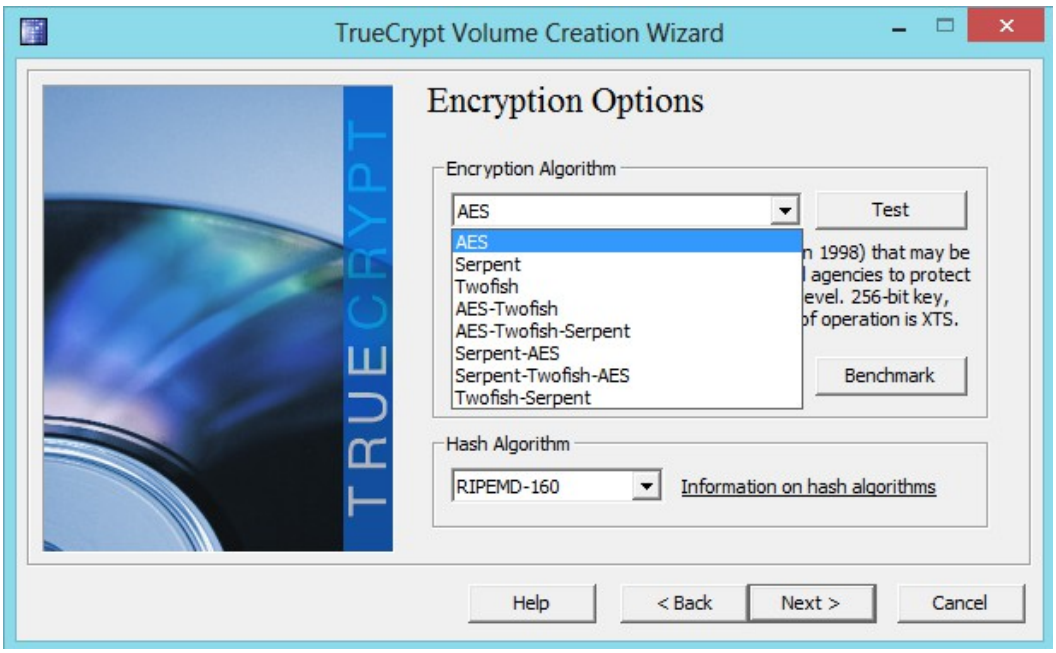
Vamos a ocultar parte del pendrive por lo que seleccionamos Hidden Truecrypt volume y nos preguntara de que modo queremos crear el volumen, seleccionaremos Normal mode para que nos vaya guiando en todo el proceso.



Nos preguntara en la siguiente ventana cual es el dispositivo que queremos encryptar **(cuidado, todo el contenido de dicho dispositivo se borrara)**



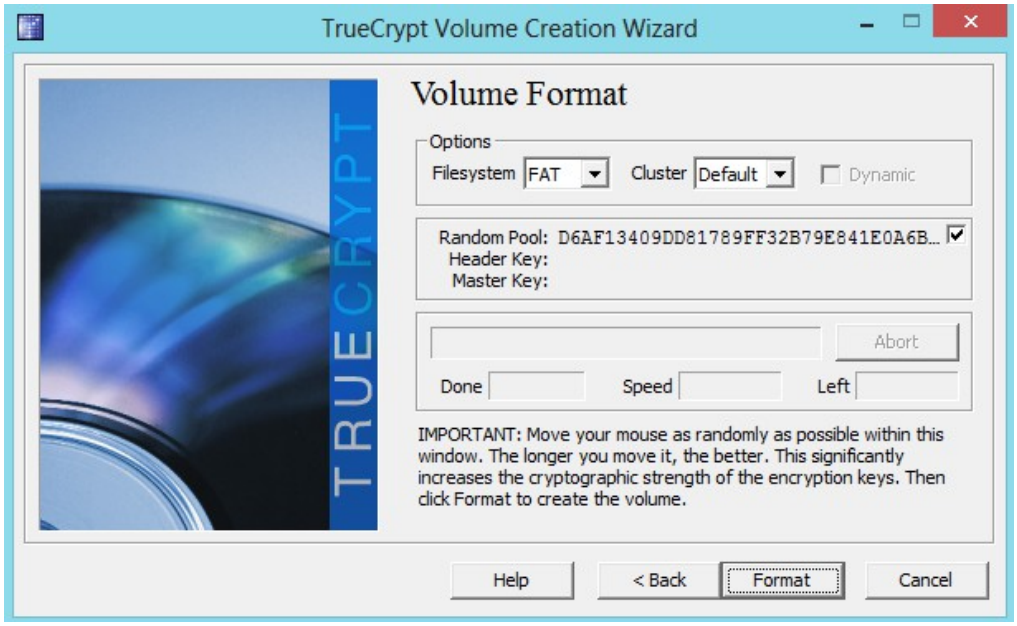
Seleccionaremos una de la particiones del pendrive de 1GB que tenemos para probar, hay que seleccionar cualquiera de las dos particiones y le damos a siguiente y aparece la pantalla de elección de encryptacion.



En principio con un sistema AES tendríamos suficiente, pero cada uno es libre de aplicar uno u otro según la elección del usuario, y después nos pregunta que tipo de algoritmo de clave queremos, RIPEMD-160, SHA-512 o Whirlpool, aquí seleccionaremos SHA-512, con lo que habremos protegido el fichero con un algoritmo de cifrado AES-SHA de 512bits, un protocolo bastante fuerte y fiable.

Le damos a siguiente y nos mostrara la pantalla de selección de tamaño, como le hemos asignado todo el tamaño de la partición no nos dejara realizar ninguna acción, así que le damos a siguiente y nos pedirá la contraseña para protegerlo.

Le escribimos la contraseña que deseemos y NO marcamos Use Keyfiles (explicado anteriormente), así que le damos a siguiente para ver la pantalla de formateo de la unidad.



Seleccionamos FAT, y le damos a formatear, nos saldra una ventana advirtiéndonos de que todos los datos de la memoria van a a ser eliminados, asi que aceptamos y comenzara a formatear la unidad.

Al finalizar tendremos una unidad que al pincharla en el ordenador nos dirá que ocupa 500mb y la otra no saldrá ya que estará oculta.

Para poder abrirla simplemente utilizamos el anterior apartado ABRIR UNA UNIDAD ENCRYPTADA CON TRUECRYPT ya que simplemente tendremos que seleccionar la partición encryptada como si de una unidad cualquiera se tratase.