TrueCrypt - Almacenamiento seguro de archivos

Short Description:

TrueCrypt mantiene seguros tus archivos al impedir que alguien los abra sin la contraseña correcta. Funciona como una *caja fuerte* electrónica, donde puedes almacenar tus archivos bajo llave, de manera segura.

Online Installation Instructions:

Descargar TrueCrypt

- ***Dada la falta de claridad sobre el estado del desarrollo de TrueCrypt, como sobre la última versión disponible en el sitio web de los creadores (véase la explicación al lado), a continuación ofrecemos la versión 7.1a de los archivos de los programas de instalación.***
- ***Pulsa** el enlace de abajo para descargar el programa de instalación correspondiente a tu sistema operativo.*
- Guarda el archivo instalador en tu computadora, luego pulsa **Buscar** y **pulsa dos veces** el archivo.
- *Luego de instalar TrueCrypt exitosamente, puedes borrar el programa de instalación de tu computadora.*

TrueCrypt:

- ***Versión para MS Windows** [1] **(firma de verificación** [2]**)***
- ***Versión para Mac OS X** [3] **(firma de verificación** [4]**)***
- ***Versión para Linux 32 bit** [5] **(firma de verificación** [6]**)***
- ***Versión para Linux 64 bit** [7] **(firma de verificación** [8]**)***
- ***Versión para el panel de control Linux 32 bit** [9] **(firma de verificación** [10]**)***
- ***Versión para el panel de control Linux 64 bit** [11] **(firma de verificación** [12]**)***
- ***Código fuente** [13] **(firma de verificación** [14]**)***
- ***Versiones históricas** [15]*

- *TrueCrypt Foundation public GPG key: Copia keys.mozilla.org [16] (copia local [17]). Véanse las instrucciones sobre cómo verificar la firma del software desde el proyecto Tor [18].*

- Véase también https://truecrypt.ch/downloads/ [19]

El 28 de mayo de 2014, los desarrolladores del sitio web de TrueCrypt comenzaron a informar a los usuarios que a partir de ese momento suspenderían el desarrollo de TrueCrypt. Aun no aclaran las circunstancias que llevaron a esta situación. Los desarrolladores del sitio ofrecen la nueva versión 7.2 de TrueCrypt, de funcionalidad reducida. Pese a este nuevo lanzamiento, recomendamos que continúes utilizando la versión 7.1a anterior (véanse las instrucciones para descargarla), hasta que sepamos más acerca de lo que ha sucedido y de los planes futuros para el desarrollo de TrueCrypt. Para alternativas a TrueCrypt por favor consulta «GNU Linux, Mac OS y otros programas compatibles con Microsoft Windows» en la siguiente sección.

Página de inicio

www.truecrypt.org [20]

Requisitos para la computadora

- Windows 2000/XP/2003/Vista/7
- Derechos de administrador para la instalación o creación de volúmenes, pero no para acceder a volúmenes existentes

Versión utilizada en esta guía

- 7.1a

Última revisión del presente capítulo

- Junio de 2015

Licencia

- Programa informático gratuito y de código abierto

Versión portátil

- **Guías prácticas para TrueCrypt portátil** [21]

Lectura necesaria

- Guía capítulo **4. Cómo proteger los archivos sensibles de tu computadora** [22]

Qué obtienes a cambio:

- La capacidad de proteger tus archivos eficazmente de intrusos o accesos no autorizados
- La capacidad de almacenar de manera fácil y segura copias de tus archivos importantes

GNU Linux, Mac OS y otros programas compatibles con Microsoft Windows:

Nota: **TrueCrypt** también se encuentra disponible en **GNU Linux** y **Mac OS**.

Muchas distribuciones de **GNU Linux**, como **Ubuntu** [23], disponen de cifrado y descifrado sobre la marcha para el disco completo, como una característica estándar; puedes decidir utilizarla al instalar el sistema. Además, también recomendamos la activación del cifrado de la capeta de inicio durante la instalación. También puedes agregar la funcionalidad de cifrado a tu sistema **Linux** mediante la integración de **dm-crypt** [24] y **cryptsetup y LUKS** [25]. Otra opción es utilizar **ScramDisk para Linux SD4L** [26], un programa de cifrado y descifrado sobre la marcha gratis y de código abierto.

Para **Mac OS** puedes usar **FileVault**, que es parte del sistema operativo, para ofrecer cifrado y descifrado *sobre la marcha* para el contenido completo de tu disco o tu carpeta de inicio y todas las subcarpetas.

Un programa alternativo en **Microsoft Windows** cuyo uso recomendamos es:

- DiskCryptor [27], una solución de cifrado de código abierto que ofrece el cifrado de todas las particiones del disco, incluida la del sistema.
- **AxCrypt** [28] es un programa gratis y de código abierto capaz de cifrar archivos individuales.

Para las versiones MS Windows 7 Ultimate o Enterprise o MS Windows 8 Pro y Enterprise puedes utilizar **BitLocker** [29] para el cifrado del disco completo. Nota: BitLocker es un programa cerrado de Microsoft, que no se somete a una auditoría independiente para establecer el nivel de protección y privacidad que ofrece a tu información.

1.1 Lo que debes saber sobre esta herramienta antes de empezar

TrueCrypt protege tu información de accesos no autorizados bloqueándola con una contraseña que tú crearás. ¡Si olvidas esa contraseña pierdes acceso a tu información! **TrueCrypt** utiliza un proceso llamado cifrado para proteger tus archivos. Ten en cuenta que el uso del cifrado es ilegal en algunos países. En lugar de cifrar archivos específicos, **TrueCrypt** crea un área protegida, o *volumen*, en tu computadora. Puedes almacenar tus archivos de forma segura en este volumen cifrado.

TrueCrypt ofrece la posibilidad de crear un volumen cifrado común u oculto. Ambos mantendrán tus archivos confidenciales, pero un volumen oculto te permite esconder información importante detrás de datos menos sensibles, con el objeto de protegerla, aunque te veas forzado a revelar la existencia de tu volumen **TrueCrypt**. Esta guía proporciona información detallada sobre ambos volúmenes.

Offline Installation Instructions :

Para instalar TrueCrypt

- *Lee la breve **introducción** de las **Guías Prácticas** [30].*
- ***Pulsa** sobre el ícono de **TrueCrypt** ubicado abajo para guardar y ejecutar el programa de instalación.*
- *Lee la siguiente sección antes de continuar.*
- *Después de haber instalado **TrueCrypt** exitosamente, puedes eliminar el archivo de instalación de tu computadora.*

TrueCrypt:

[31] ES [32]

Instalar TrueCrypt y Crear Volúmenes Comunes

Lista de las secciones en esta página:

- **2.0 Cómo instalar TrueCrypt**

- **2.1 Acerca de TrueCrypt**
- **2.2 Cómo crear un Volumen común**
- **2.3 Cómo crear un Volumen común en un dispositivo de memoria USB**
- **2.4 Cómo crear un Volumen común (Continuación)**

2.0 Cómo instalar TrueCrypt

Paso 1. **Pulsa dos veces** TrueCrypt Setup 7.1a ; la ventana *Abrir archivo - Advertencia de seguridad* puede aparecer. Si aparece, **pulsa** Ejecutar para activar la pantalla de la *Licencia* de **TrueCrypt**.

Paso 2. **Marca** la opción *Acepto y me comprometo a cumplir con los términos de la licencia* para habilitar el botón de *Aceptar*, **pulsa** Next > para activar la siguiente pantalla:

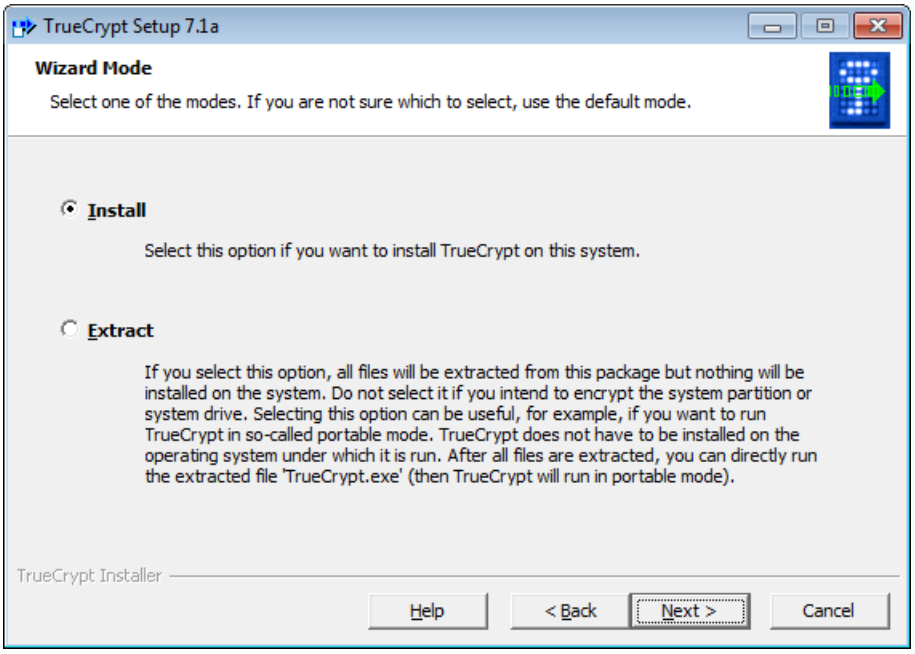


Figura 1: Modo asistente en el modo de instalación por defecto

- Modo *Instalación*: Esta es una opción para usuarios que no desean ocultar el hecho de que utilizan **TrueCrypt** en su computadora.
- Modo de *extracción*: Esta es una opción para usuarios que desean llevar una versión portátil de **TrueCrypt** en un dispositivo de memoria USB y no desean instalar **TrueCrypt** en su computadora.

Nota: Algunas opciones (como el cifrado de la partición y del disco completo) no funcionan con solo extraer **TrueCrypt**.

Nota: A pesar de recomendar el modo *Instalación* por defecto, aun podrás utilizar **TrueCrypt** en modo portátil más tarde. Para averiguar cómo utilizar el modo **TrueCrypt viajero**, puedes consultar la **página TrueCrypt portátil** [21].

Paso 3. **Pulsa** Next > para activar la siguiente pantalla:

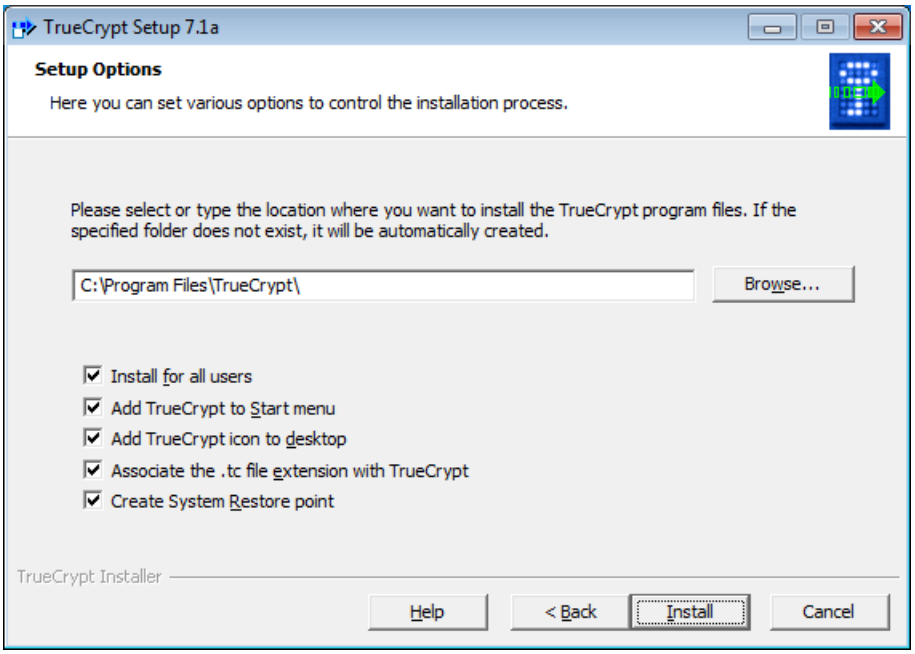


Figura 2: Ventana de opciones de configuración

Paso 4. **Pulsa** [Install] para activar la pantalla de *Instalación* y comenzar a instalar **TrueCrypt** en tu sistema.

Paso 5. **Pulsa** [OK] y luego [Finish] para finalilzar.

Nota: Instamos a todos los usuarios a consultar la documentación de ayuda de **TrueCrypt** [33] después de terminar este tutorial.

2.2 Cómo crear un Volumen común

TrueCrypt te permite crear dos tipos de volúmenes: *Oculto* y *Común*. En esta sección aprenderás cómo crear un *Volumen común* para almacenar tus archivos.

Para crear un *Volumen común* con **TrueCrypt**, sigue los siguientes pasos:

Paso 1. **Pulsa dos veces**  o **selecciona Inicio > Programas > TrueCrypt > TrueCrypt** para abrir **TrueCrypt**.

Paso 2. **Selecciona** una unidad de la lista en el panel de **TrueCrypt** como se indica a continuación:

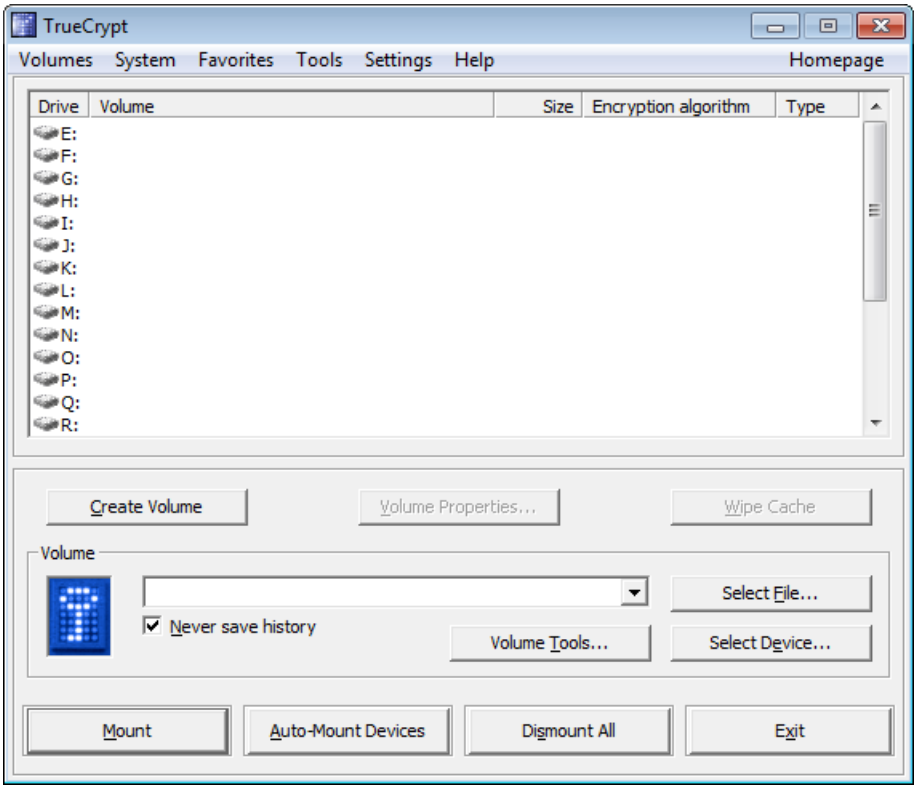


Figura 3: Panel de control de TrueCrypt

Paso 3. **Pulsa** Create Volume para activar el *asistente para la creación de volúmenes TrueCrypt* como sigue:

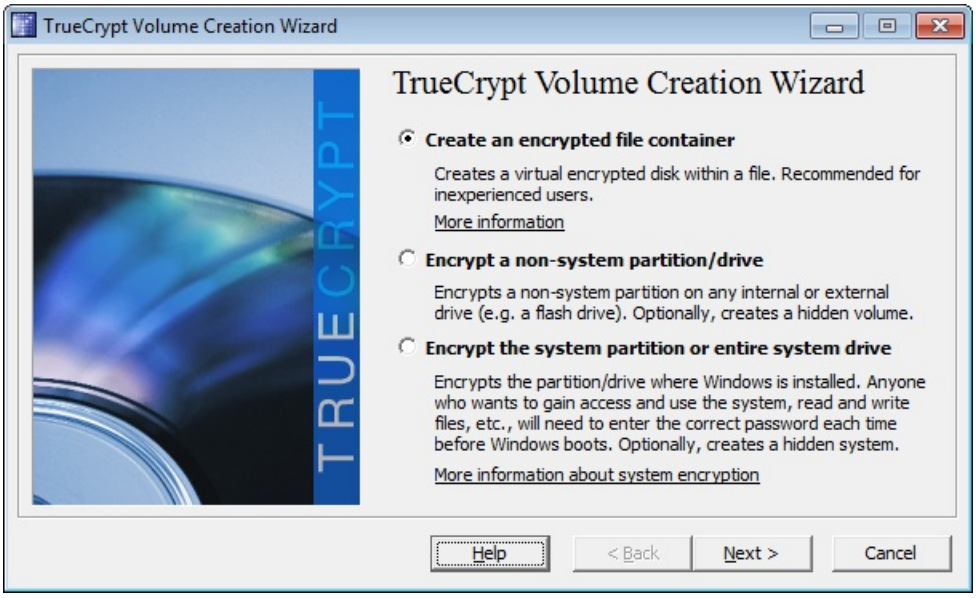


Figura 4: Ventana del asistente para la creación de volúmenes TrueCrypt

La *Figura 4* presenta tres opciones para cifrar un *Volumen común*. En este capítulo, utilizamos la opción *Crear un contenedor para archivos cifrados*. Favor de consultar la documentación de **TrueCrypt** [34] para la descripción de las otras dos opciones.

Paso 4. **Pulsa** Next > para activar la siguiente pantalla:

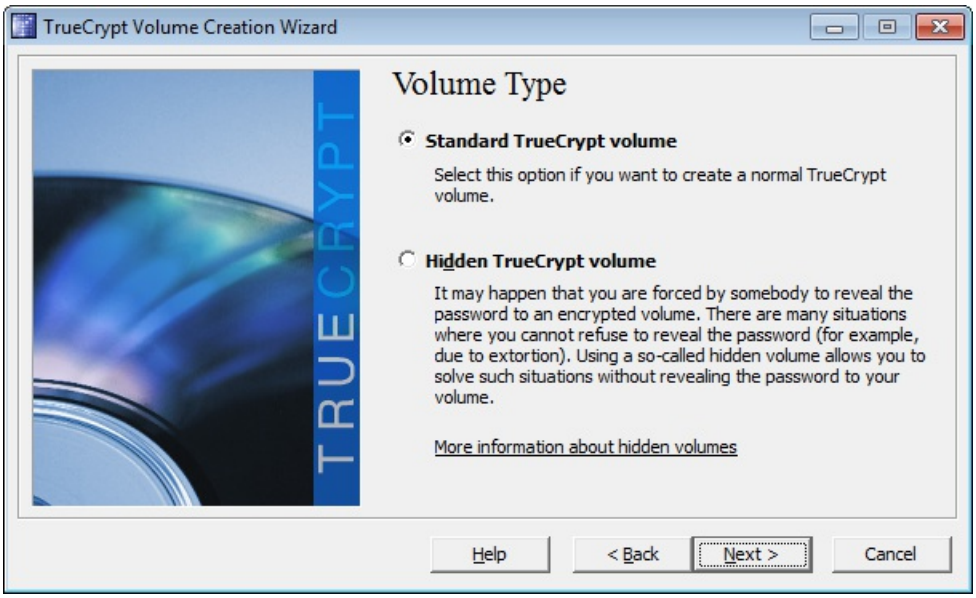


Figura 5: Ventana del tipo de volumen

La ventana del *Asistente para la creación de tipos de volumen* te permite especificar si deseas crear un Volumen **TrueCrypt** *Común* u *Oculto*.

Importante: Para mayor información sobre *Cómo crear un Volumen oculto*, considera consultar la página **Volúmenes ocultos** [35].

Paso 5. **Elige** la opción *Volumen TrueCrypt estándar*.

Paso 6. **Pulsa** Next > para activar la siguiente pantalla:

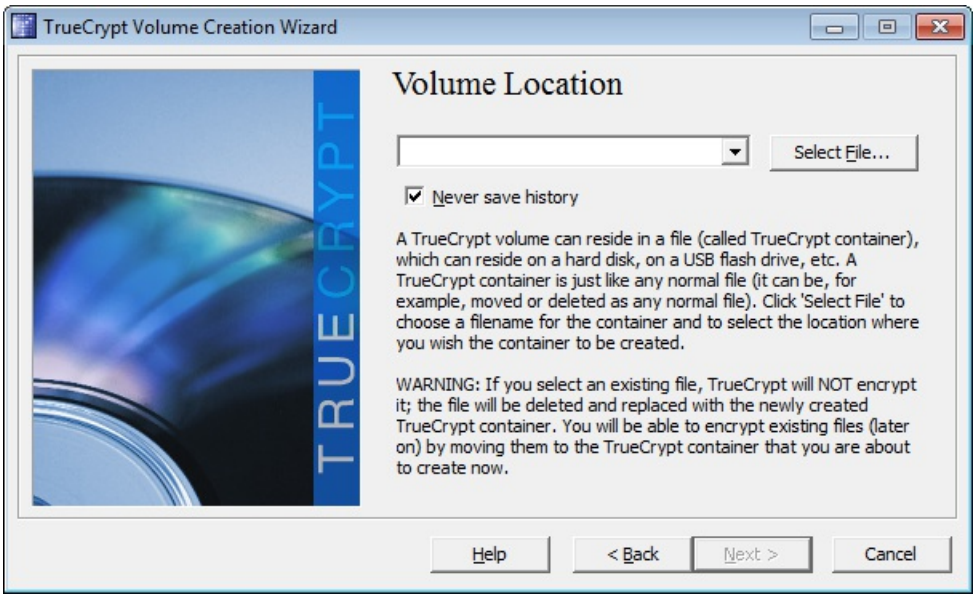


Figura 6: Asistente para la creación de volúmenes - Panel de ubicación del volumen

Puedes especificar dónde quieres almacenar tu *Volumen común* mediante el *asistente para la creación de volúmenes - Pantalla de ubicación del volumen*. Este archivo se puede almacenar como cualquier otro archivo.

Paso 7. **Ingresa** el nombre del archivo en el campo de texto o **pulsa** Select File... para activar la siguiente pantalla:

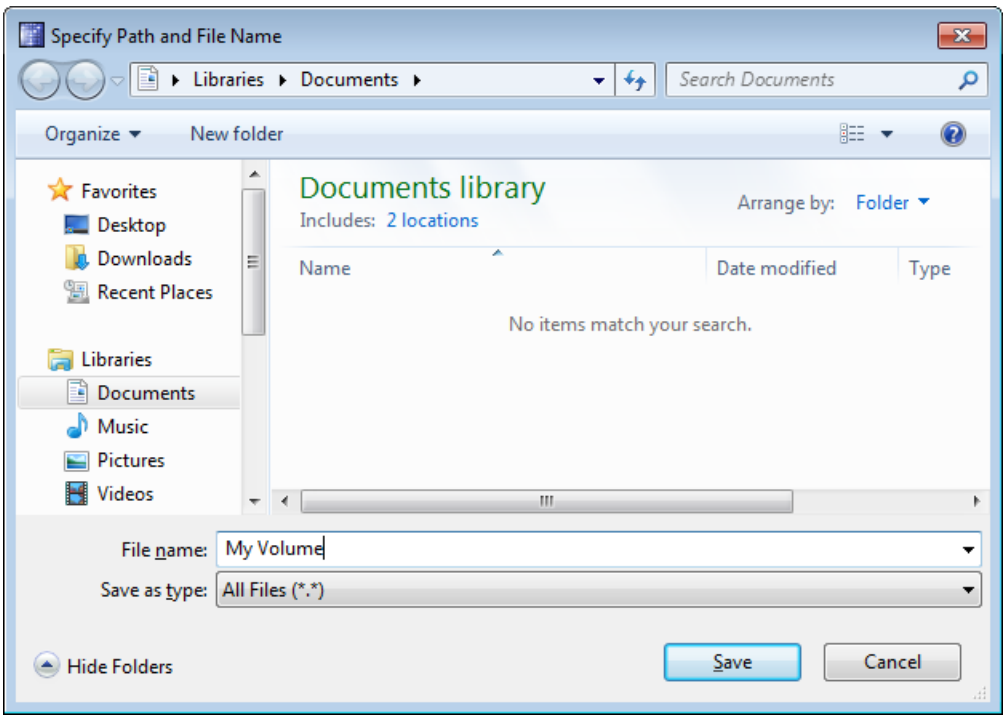


Figura 7: Ventana de navegación para la especificación de la ruta de acceso y el nombre del archivo

Nota: Un volumen de **TrueCrypt** puede contenerse dentro de un archivo normal. Esto significa que se puede mover, copiar o ¡hasta borrar! Debes recordar tanto la ubicación como el nombre del archivo. No obstante, debes elegir un nuevo nombre de archivo para el volumen que creas (consultar la sección **2.3 Cómo crear un Volumen común en un dispositivo de memoria USB**). En este tutorial crearemos nuestro Volumen común en la carpeta **Mis documentos** y lo llamaremos *My volume* como se muestra en la *Figura 7* de arriba.

Consejo: Puedes utilizar cualquier nombre y extensión de archivo. Por ejemplo, puedes llamar *Recetas.doc* a tu Volumen común, de modo que parezca un documento de *Word* o *Vacaciones.mpg*, para que parezca un archivo de vídeo. Esta es una forma de disfrazar la existencia de tu Volumen común.

Paso 8. **Pulsa** Save para cerrar la ventana de *Especificación de la ruta y el nombre del archivo* y regresar a la ventana del *Asistente para la creación de volúmenes* como sigue:

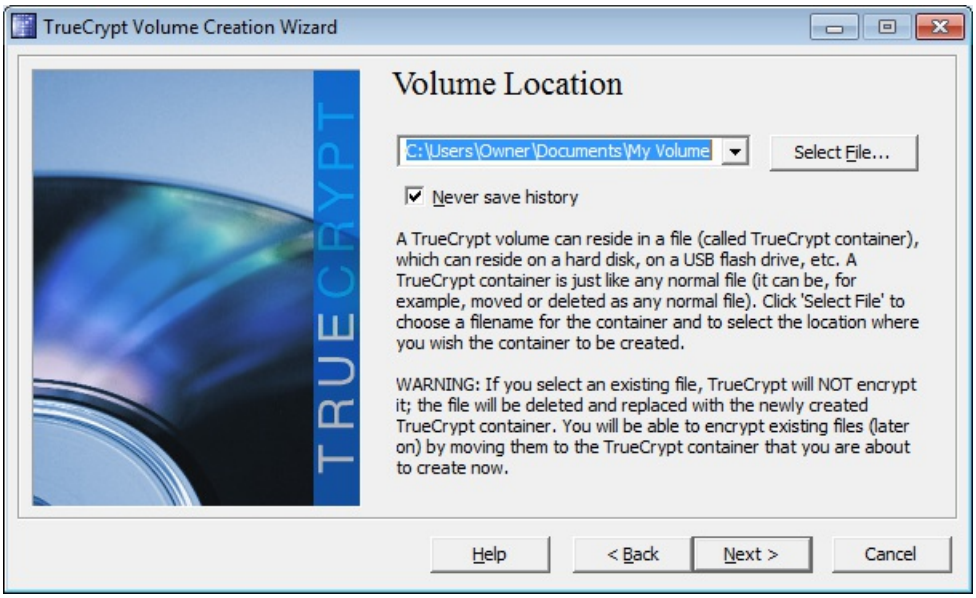


Figura 8: Asistente para la creación de volúmenes TrueCrypt que muestra el panel de ubicación del volumen

Paso 9. **Pulsa** Next > para activar *Figura 9*.

2.3 Cómo crear un Volumen común en un dispositivo de memoria USB

Para crear un *Volumen común* **TrueCrypt** en un dispositivo de memoria USB, sigue los pasos 1 a 7 de la sección **2.2 Cómo crear un Volumen común**, donde activas la pantalla *Selecciona un volumen TrueCrypt*. En lugar de elegir *Mis documentos* para la ubicación de tu archivo **desplázate** hasta tu dispositivo de memoria USB y **escógelo**. Luego, **ingresa** un nombre de archivo y crea allí el *Volumen común*.

2.4 Cómo crear un Volumen común (continuación)

En esta etapa, estás listo para escoger un método de cifrado específico (o *algoritmo* como se lo llama en la pantalla) para codificar la información que almacenarás en tu *Volumen común*.

Figura 9: Panel de opciones del asistente para la creación de volúmenes

Nota: Puedes dejar las opciones por defecto como aparecen aquí. Todos los algoritmos que se presentan en estas dos opciones se consideran seguros.

Paso 10. **Pulsa** Next > para activar el *Asistente para la creación de volúmenes TrueCrypt* como sigue:

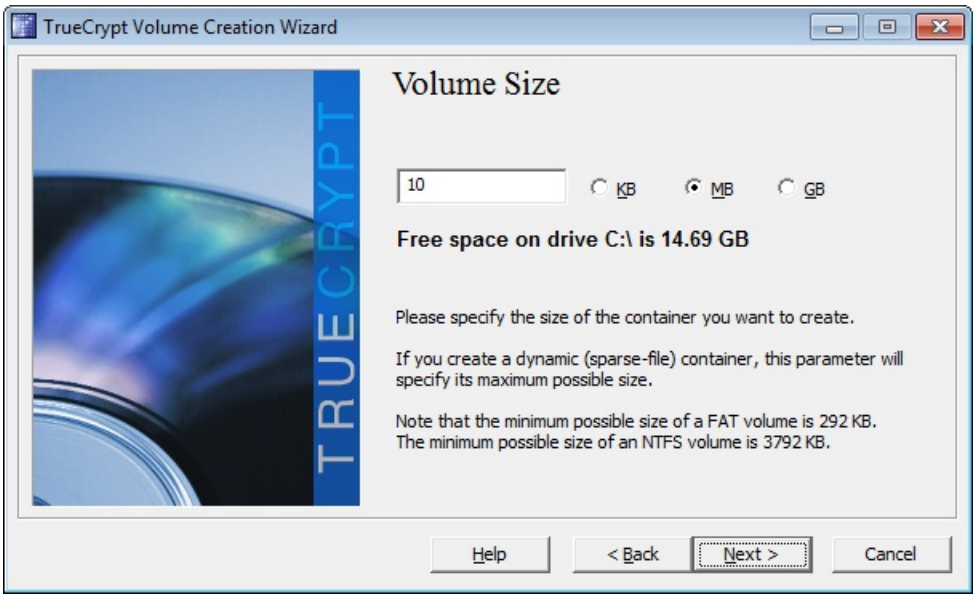


Figura 10: Asistente para la creación de volúmenes TrueCrypt que muestra el panel de tamaño del volumen

El panel de *Tamaño del volumen* te permite especificar el tamaño del *Volumen común*. En este ejemplo, se fija en 10 Megabytes. No obstante, puedes especificar un tamaño diferente. Considera el tamaño de los documentos y tipos de archivos que deseas almacenar para fijar un tamaño de volumen adecuado para estos.

Consejo: Si más tarde deseas guardar una copia de respaldo de tu Volumen común en un CD, deberás fijar el tamaño en 700 MB o menos.

Paso 11. **Ingresa** el tamaño específico del volumen en el campo de texto y luego **pulsa** Next > para activar la siguiente pantalla:

Figura 11: Asistente para la creación de volúmenes TrueCrypt que muestra el panel de contraseña del volumen

Importante: La elección de una contraseña segura y sólida es una de las tareas más importantes que llevarás a cabo al crear un *Volumen común*. Una buena contraseña protegerá tu volumen cifrado y cuanto más sólida sea, mejor. No tienes que crear tus propias contraseñas ni recordarlas si utilizas un programa generador de contraseñas como **KeePass**. Por favor, consulta **KeePass** [36], para obtener más información acerca de la creación y el almacenado de las contraseñas.

Paso 12. **Ingresa tu contraseña y luego vuelve a ingresarla** en el campo de texto marcado *Confirmar*.

Importante: El botón *Next* permanecerá desactivado hasta que las contraseñas de ambos campos coincidan. Si tu contraseña no es particularmente segura, verás una advertencia que te lo indica. ¡Piensa en cambiarla! Aunque **TrueCrypt** funcione con cualquier contraseña que escojas, tu información puede no estar tan segura.

Paso 13. **Pulsa** Next > para activar la siguiente pantalla:

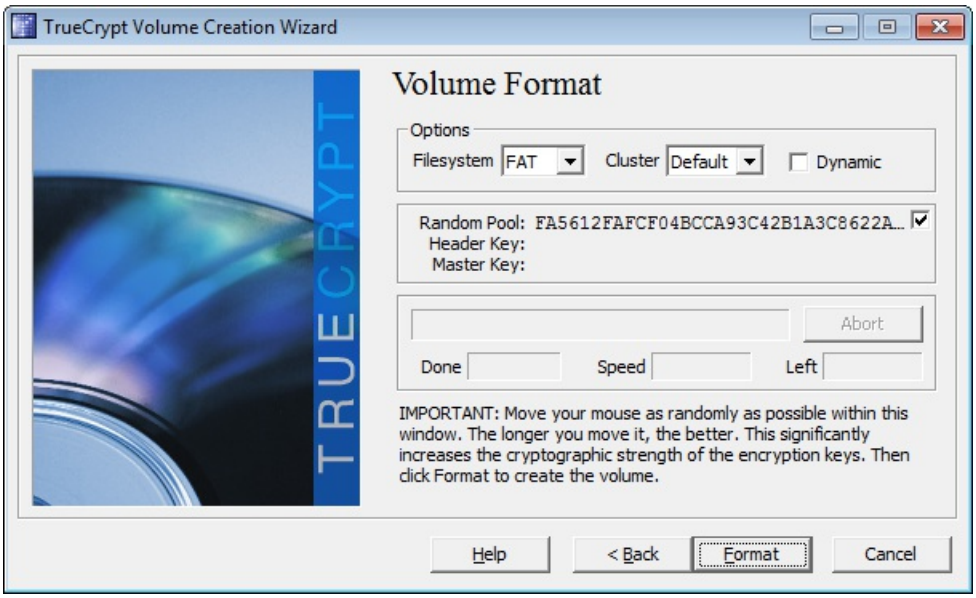


Figura 12: Asistente para la creación de volúmenes TrueCrypt que muestra el panel de formateo del volumen

TrueCrypt está listo para crear un *Volumen común*. Mueve tu ratón de manera aleatoria dentro del *Asistente para la creación de volúmenes* por unos segundos. Cuanto más tiempo lo muevas, mejor será la calidad de la clave de cifrado.

Paso 14. **Pulsa** Format para comenzar a crear tu Volumen común.

TrueCrypt creará un archivo llamado *My volume* en la carpeta *Mis documentos* previamente especificada. Este archivo ha de contener un *Volumen común* de 10 Megabytes de tamaño, que puedes utilizar para almacenar tus archivos de manera segura.

Luego de crear satisfactoriamente un *Volumen común*, aparecerá el siguiente cuadro de diálogo:

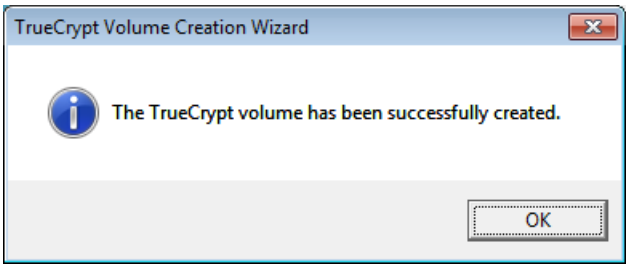


Figura 13: Pantalla del mensaje que muestra que el volumen TrueCrypt se ha creado satisfactoriamente

Paso 15. **Pulsa** OK para finalizar la creación de tu *Volumen común* y regresar al panel de control de **TrueCrypt**.

Paso 16. **Pulsa** Exit para cerrar el *asistente para la creación de volúmenes TrueCrypt*.

Montar un Volumen Común

Lista de las secciones en esta página:

- **3.0 Cómo montar un Volumen común**
- **3.1 Cómo desmontar un Volumen común**

3.0 Cómo montar un Volumen común

En **TrueCrypt**, *montar* un *Volumen común* se refiere a habilitarlo para su uso. En esta sección, aprenderás cómo montar tu nuevo Volumen común.

Para empezar a montar tu Volumen común, sigue los siguientes pasos:

Paso 1. **Pulsa dos veces** o **selecciona Inicio > Programas > TrueCrypt > TrueCrypt** para abrir **TrueCrypt**.

Paso 2. **Selecciona** cualquier unidad de la lista según se muestra a continuación:

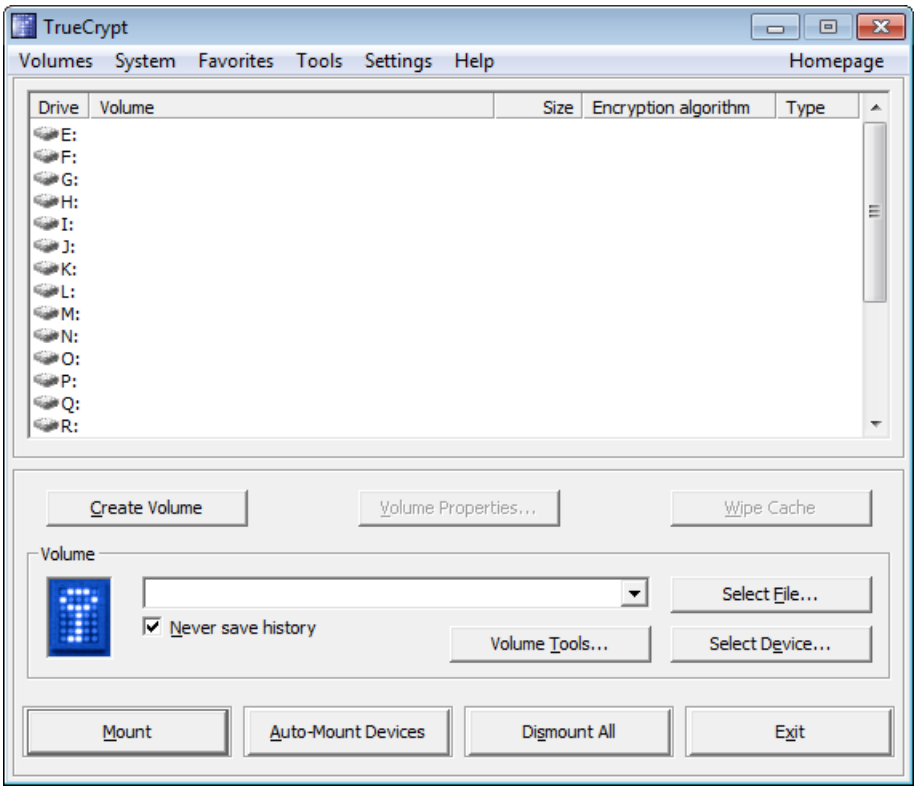


Figura 1: Panel de control de TrueCrypt

En este ejemplo, se montará el Volumen común como la unidad M:.

Nota: En la *Figura 1*, se ha seleccionado la unidad *M:* para montar el *Volumen común*; no obstante, puedes elegir cualquier otra unidad de la lista.

Paso 3. **Pulsa** 

La pantalla "Selecciona un volumen TrueCrypt" aparecerá como se muestra a continuación.

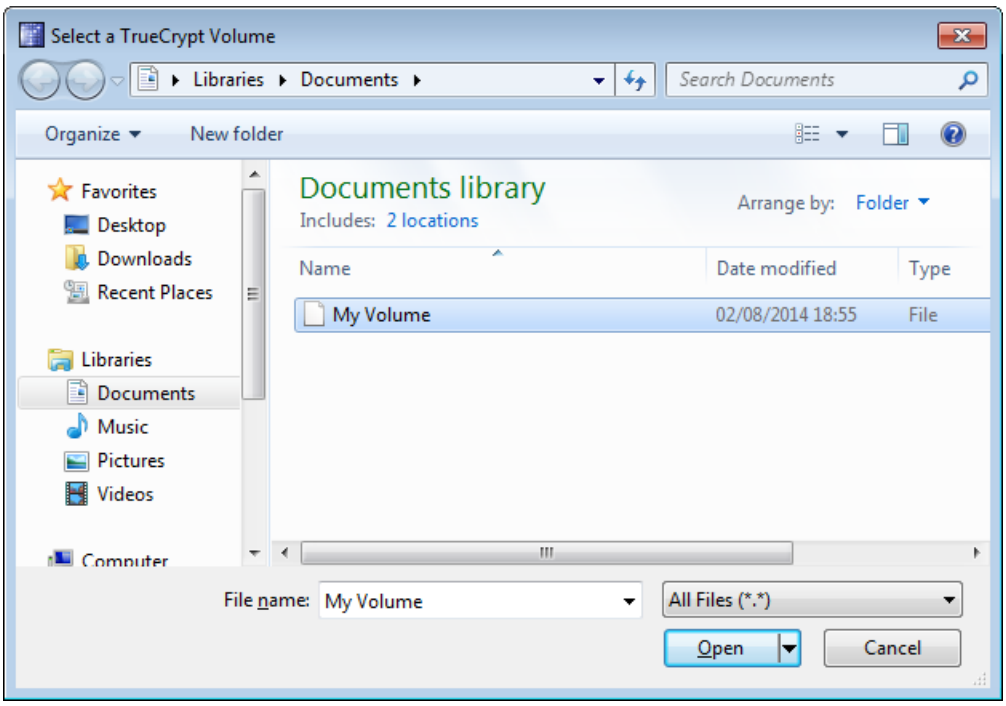


Figura 2: Pantalla para Seleccionar un volumen TrueCrypt

Paso 4. **Selecciona** el archivo del Volumen común que creaste, luego **pulsa** 

para cerrar *Figura 2* y regresar al panel de control de **TrueCrypt**.

Paso 5. **Pulsa** 

para activar la pantalla de solicitud de *Ingrese la contraseña* como sigue:

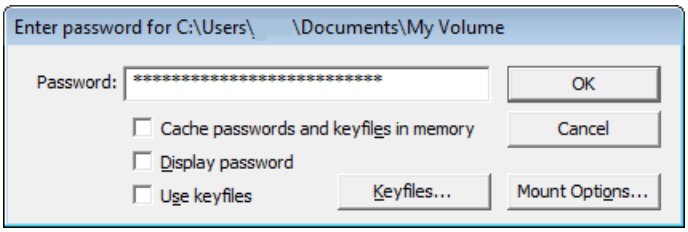


Figura 3: Pantalla de solicitud de Ingrese la contraseña

Paso 6. **Ingrese** la contraseña en el campo de texto *Contraseña*.

Paso 7. **Pulsa** OK para comenzar a montar el *Volumen común*.

Nota: Si la contraseña que ingresaste era incorrecta, **TrueCrypt** solicitará que la vuelvas a ingresar y **pulses** OK. Si la contraseña es correcta, el *Volumen común* se montará como sigue:

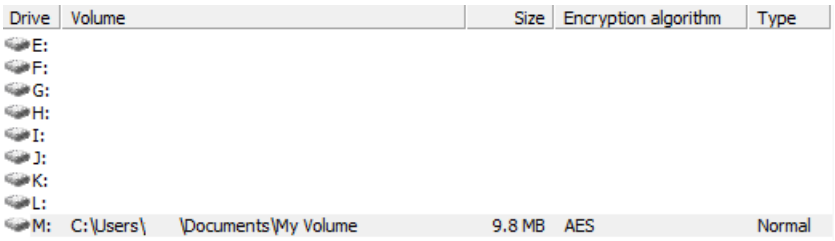


Figura 4: Panel de control de TrueCrypt que muestra el Volumen común recientemente montado

Paso 8. **Pulsa dos veces** la entrada resaltada en **TrueCrypt** o la letra de la unidad correspondiente en la pantalla de *Mi computadora* para acceder al Volumen común (ahora montado en la unidad *M*: de tu computadora).

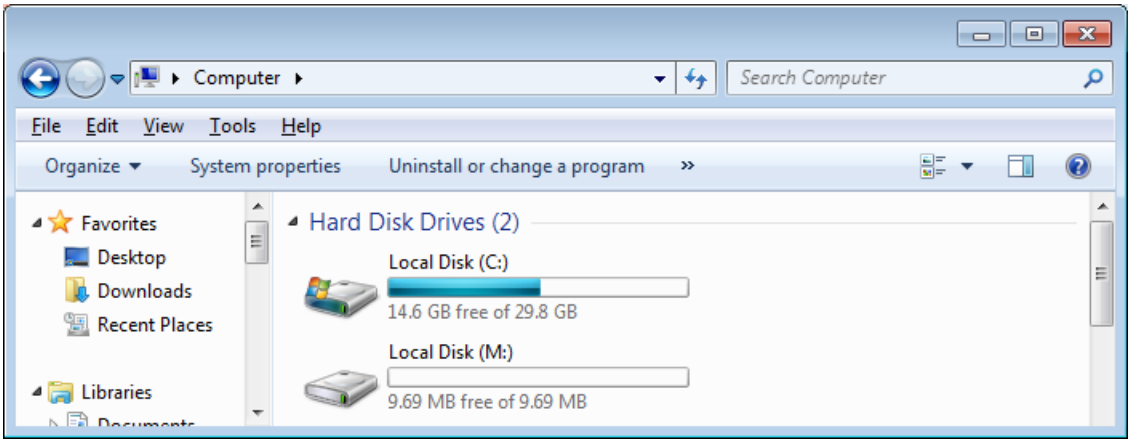


Figura 5: Acceso al Volumen común por medio de la pantalla Mi computadora

Nota: Hemos montado satisfactoriamente el Volumen común *Mi volumen* en el disco virtual *M*:. Este disco virtual se comporta como un disco real, salvo que está completamente cifrado. Cualquier archivo que copies, muevas o guardes en este disco virtual, se cifrará automáticamente (en un proceso conocido como cifrado sobre la marcha).

Puedes guardar y hacer copias de archivos del *Volumen común* del mismo modo en que harías con cualquier disco normal (por ejemplo, arrastrándolas y soltándolas). Cuando mueves un archivo fuera del *Volumen común*, este se descifra automáticamente. Inversamente, si mueves un archivo al *Volumen común*, **TrueCrypt** lo cifra automáticamente. Si tu computadora falla o se apaga de pronto, **TrueCrypt** cierra el *Volumen común* de inmediato.

Importante: Luego de transferir los archivos al volumen **TrueCrypt**, asegúrate de que no queden rastros de los archivos en la computadora o dispositivo de memoria USB de donde vinieron. Por favor, consulta el capítulo **6. Cómo destruir información sensible** [37].

3.1 Cómo desmontar un Volumen común

En **TrueCrypt**, *desmontar* un *Volumen común* simplemente significa inhabilitar su uso.

Para cerrar o desmontar un *Volumen común* y hacer que sus archivos sean accesibles solo a personas con una contraseña, sigue los siguientes pasos:

Paso 1. **Selecciona** el volumen de la lista de volúmenes montados de la ventana principal de **TrueCrypt** como se indica a continuación:

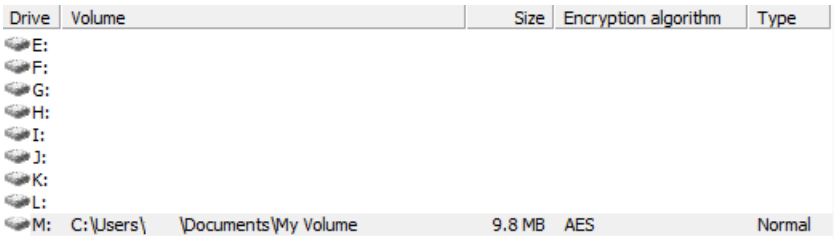


Figure 17: Selección del Volumen común a ser desmontado

Paso 2. **Pulsa** Dismount para desmontar o cerrar tu Volumen común **TrueCrypt**.

Importante: Asegúrate de desmontar tu volumen **TrueCrypt** antes de dejar tu computadora en modo de *espera* o de *hibernación*. Mejor aún, siempre apaga tu computadora de escritorio o portátil si planeas dejarla desatendida. Esto impedirá que alguien obtenga la contraseña de tu volumen.

Para recuperar un archivo almacenado en un Volumen común cerrado o desmontado, tendrás que volver a montarlo.

Guardar una copia de respaldo de tu volumen

Es muy importante que guardes copias de tus documentos, archivos y carpetas regularmente. Guardar copias de respaldo de tu volumen **TrueCrypt** es vital y (afortunadamente) muy fácil de hacer. No olvides desmontar tu volumen antes de hacer una copia de respaldo del mismo.

Paso 1. **Desplázate** hasta el archivo de tu *Volumen común* (en la *Figura 1* más abajo, está localizado en la carpeta *Mis documentos*).

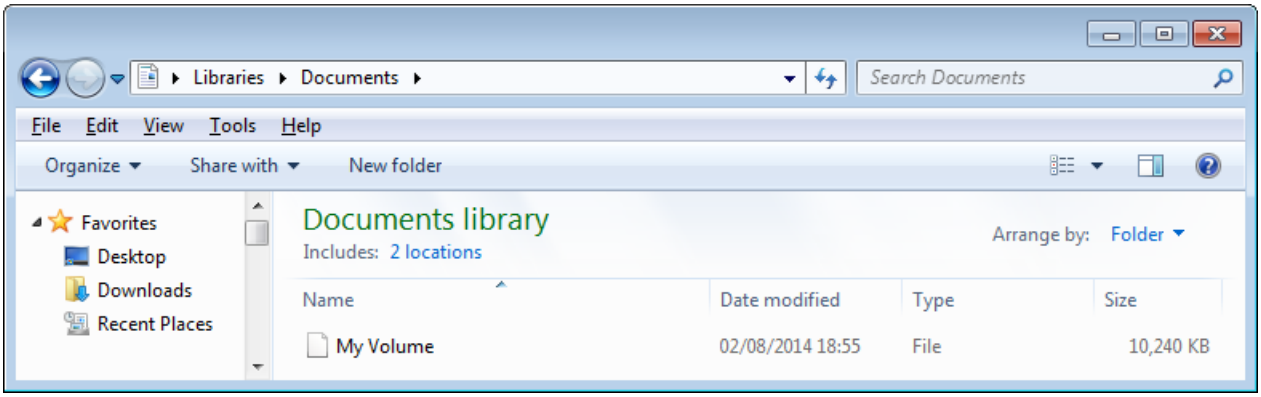


Figura 1: Ventana de Mis documentos que muestra el archivo My volume

Paso 2. **Guarda** el archivo en un dispositivo de memoria externa como un CD, DVD o un dispositivo de memoria USB.

Consejo: Si tienes grandes cantidades de información que deseas cifrar y guardar repetidamente, ¿por qué no crear un nuevo *Volumen común* que tenga el mismo tamaño que un CD o DVD? Esta es una técnica de almacenamiento seguro.

Antes de realizar una copia de respaldo del Volumen común en el dispositivo extraíble, asegúrate de que el tamaño del dispositivo corresponda al tamaño de tu volumen.

Medio de respaldo	Tamaño sugerido del volumen TrueCrypt
CD	700 MB
DVD	3900 MB
Dispositivo USB	Se sugiere el 25% de la capacidad total (por ejemplo: para un dispositivo USB de 128 MB, utiliza 30 MB para tu Volumen común)

Volúmenes Ocultos

Lista de las temas en esta página:

- **5.0 Acerca de los volúmenes ocultos**
- **5.1 Cómo crear un Volumen oculto**
- **5.2 Cómo montar un Volumen oculto**

- **5.3 Consejos acerca de cómo utilizar la característica del disco oculto de manera segura**

5.0 Acerca de los volúmenes ocultos

En **TrueCrypt**, un *Volumen oculto* se almacena dentro de tu *Volumen común* cifrado, pero su existencia permanece oculta. Aunque «montes» o abras tu Volumen común, no es posible encontrar ni probar la existencia del Volumen oculto. Si te fuerzan a revelar tu contraseña y la ubicación de tu Volumen común, se revelará su contenido pero **no** la existencia del Volumen oculto dentro del mismo.

Imagina un maletín con un compartimiento secreto. En la sección normal de tu maletín, guardas archivos que no te importa que sean confiscados o que se pierdan y mantienes los archivos importantes y privados en el compartimiento secreto. El propósito del compartimiento secreto (especialmente uno bien diseñado), es el de ocultar su propia existencia y por tanto, los documentos dentro del mismo.

5.1 Cómo crear un Volumen oculto

La creación de un *Volumen oculto* **TrueCrypt** es similar a la de un *Volumen común* de **TrueCrypt**: Incluso algunos de los paneles, pantallas y ventanas son iguales.

Paso 1. **Abre TrueCrypt**.

Paso 2. **Pulsa** 

para activar el *asistente para la creación de volúmenes TrueCrypt*.

Paso 3. **Pulsa** 

para aceptar la opción por defecto *Crear un contenedor para archivos cifrados*.

Paso 4. **Elige** la opción *Volumen TrueCrypt oculto* como sigue:

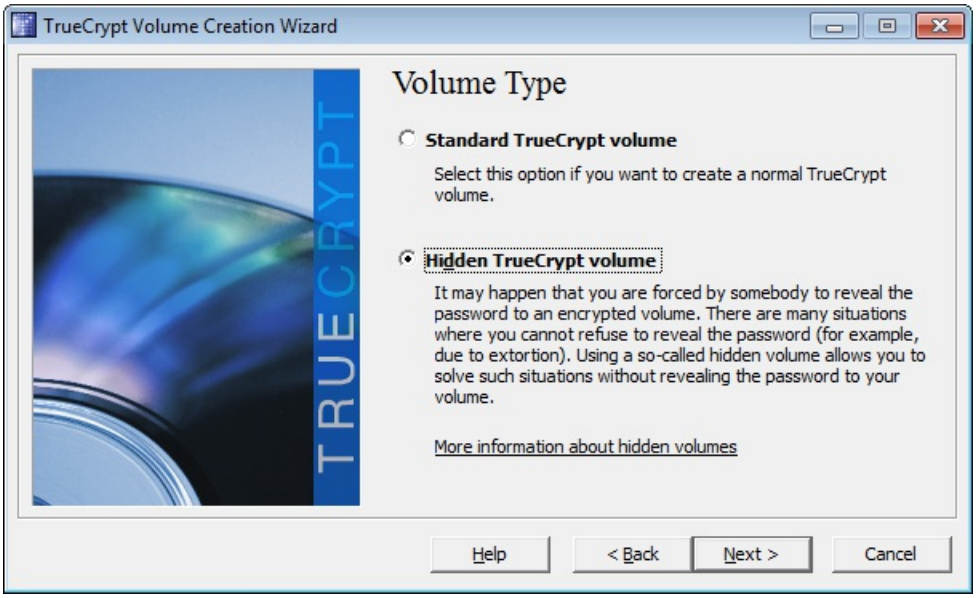


Figura 1: Ventana del asistente para la creación de volumen con la opción de volumen TrueCrypt oculto habilitada

Paso 5. **Pulsa** 

para activar la siguiente pantalla:

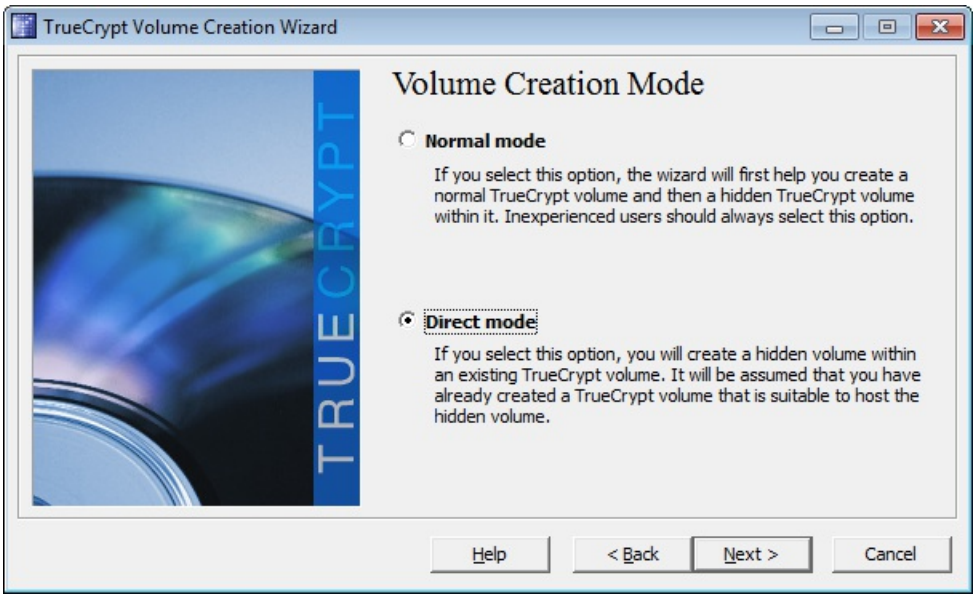


Figura 2: Ventana del asistente para la creación de volúmenes de TrueCrypt - Ventana de modos

- *Modo directo*: Esta opción te permite crear el *Volumen oculto* dentro de un *Volumen común* existente.
- *Modo normal*: Esta opción te permite crear un *Volumen común* completamente nuevo donde almacenar el *Volumen oculto*.

En este ejemplo, utilizaremos el *Modo directo*.

Nota: Si prefieres crear un nuevo *Volumen común*, ten a bien repetir el proceso de la sección **Cómo crear un Volumen común** [38].

Paso 6. **Elige** la opción *Modo directo* y luego **pulsa** Next > para activar la ventana para la *Creación de volúmenes TrueCrypt - Ubicación del volumen*.

Nota: Asegúrate de que el *Volumen común* se encuentre desmontado antes de seleccionarlo.

Paso 7. **Pulsa** Select File... para activar la siguiente pantalla:

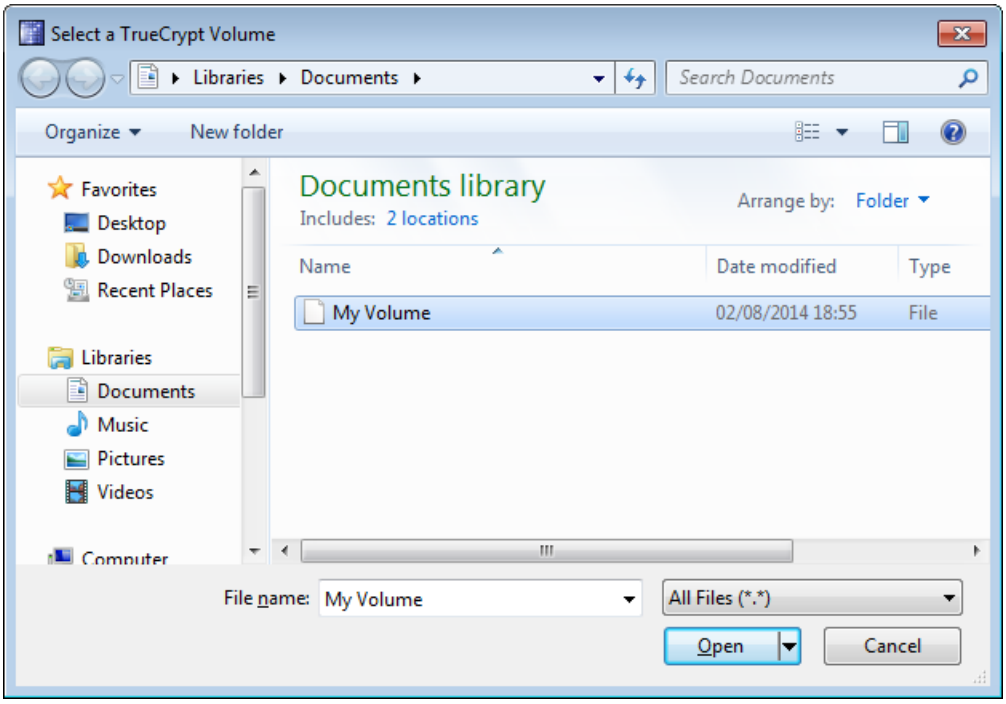


Figura 3: Ventana del asistente para la creación de volúmenes de TrueCrypt - Selecciona un volumen TrueCrypt

Paso 8. **Localiza** el archivo de volumen a través de la ventana *Selecciona un volumen TrueCrypt* como se muestra en la *Figura 3*.

Paso 9. **Pulsa** Open para regresar al *Asistente para la creación de volúmenes TrueCrypt*.

Paso 10. **Pulsa** Next > para activar la pantalla *Ingrese la contraseña*.

Paso 11. **Ingresa** la contraseña que utilizaste al crear el *Volumen común* en el campo de texto *Contraseña* para activar la siguiente pantalla:

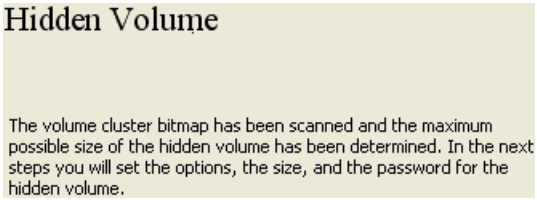


Figura 4: Asistente para la creación de volúmenes TrueCrypt - Panel de mensaje del Volumen oculto

Paso 12. **Pulsa** Next > luego de leer el mensaje para activar la pantalla *Opciones de cifrado del Volumen oculto*.

Nota: Deja tal como están los parámetros por defecto del *Algoritmo de cifrado* y del *Algoritmo Hash* para el *Volumen oculto*.

Paso 13. **Pulsa** Next > para activar la siguiente pantalla:

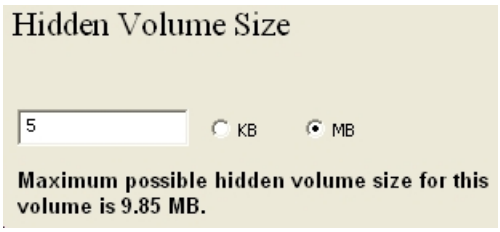


Figura 5: Asistente para la creación de volúmenes TrueCrypt - Ventana de tamaño del Volumen oculto

Se te solicitará que especifiques el tamaño del *Volumen oculto*.

Nota: Considera el tipo de documentos, la cantidad y el tamaño requerido para almacenarlos. Deja algo de espacio para el *Volumen común*. Si seleccionas el tamaño máximo disponible para el *Volumen oculto*, no podrás agregar ningún otro archivo al *Volumen común* original.

Si el tamaño de tu *Volumen común* es de 10 Megabytes (MB) y especificas un tamaño de *Volumen oculto* de 5 MB (como se muestra en la *Figura 6* anterior), tendrás dos volúmenes (uno oculto y otro común) de aproximadamente 5 MB cada uno.

Asegúrate de que la información que almacenes en el *Volumen común* no exceda los 5 MB que has fijado. Esto es porque el programa **TrueCrypt** no detecta automáticamente, por sí mismo, la existencia de un *Volumen oculto*, y puede sobrescribirlo accidentalmente. Si excedes el tamaño previamente establecido, te arriesgas a perder archivos almacenados en el Volumen oculto.

Paso 14. **Ingresa** el tamaño deseado del Volumen oculto en el campo de texto correspondiente, como se muestra en la *Figura 5*.

Paso 15. **Pulsa** Next > para activar la ventana *Contraseña del Volumen oculto*.

Ahora debes crear una contraseña para el Volumen oculto *diferente* de la que utilizas para proteger tu Volumen común. Nuevamente, recuerda escoger una contraseña sólida. Por favor, consulta el capítulo **KeePass** [36] para aprender más acerca de la creación de contraseñas sólidas.

Consejo: Si crees que te verás forzado a revelar el contenido de tus volúmenes **TryeCrypt**, almacena tu contraseña para el Volumen común en **KeePass** y crea una contraseña sólida que tengas que recordar solo para el Volumen oculto. Esto te ayudará a esconder tu Volumen oculto, ya que no dejarás ningún rastro de su existencia.

Paso 16. **Crea** una contraseña e **ingrésala** allí dos veces, luego **pulsa** Next > para activar la siguiente pantalla:

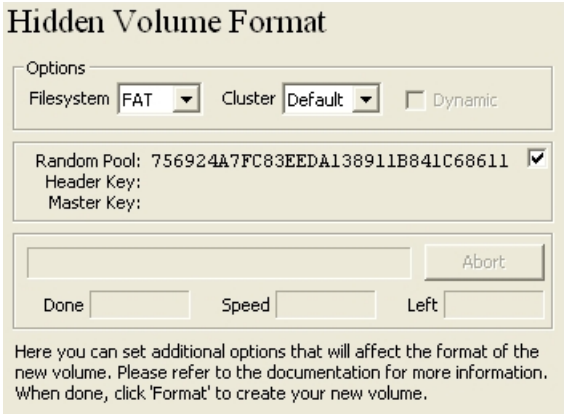


Figura 6: Asistente para la creación de volúmenes TrueCrypt - Panel de formateo del Volumen oculto

Deja las opciones por defecto del *Sistema de* archivo y *Cluster* tal como están.

Paso 17. **Mueve** el ratón alrededor de la pantalla para aumentar la solidez criptográfica del cifrado y luego **pulsa** Format para formatear el Volumen oculto.

Después de formatear el Volumen oculto, aparecerá la siguiente pantalla

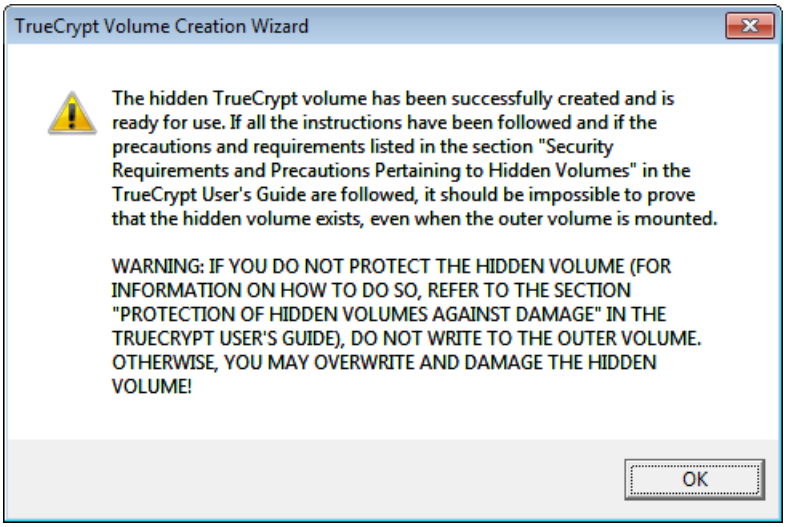


Figura 7: Ventana de mensaje del Asistente para la creación de volúmenes TrueCrypt

Nota: La *Figura 7* confirma que has creado satisfactoriamente un Volumen oculto y también te advierte del peligro de sobrescribir los archivos en el Volumen oculto cuando almacenes archivos en el Volumen común.

Paso 18. **Pulsa** OK para activar la ventana *Volumen oculto creado* y luego **pulsa** Exit y regresa a panel de control de **TrueCrypt**.

El Volumen oculto ya se ha creado dentro del Volumen común. Ahora puedes almacenar documentos en el Volumen oculto, que permanece invisible incluso para quien obtenga la contraseña para ese Volumen común en particular.

5.2 Cómo montar un Volumen oculto

El método para montar un *Volumen oculto* o hacer que sea accesible para su uso, es el mismo que para un *Volumen común*, la única diferencia es que utilizas la contraseña que acabas de crear para el *Volumen oculto*.

Para *montar* o abrir el *Volumen oculto*, sigue los siguientes pasos:

Paso 1. **Selecciona** una unidad de la lista (en este ejemplo, es la unidad *K:*):

Figura 8: Unidad seleccionada para montar en la pantalla de volumen de TrueCrypt

Paso 2. **Pulsa** Select File... para activar la ventana *Selecciona un volumen TrueCrypt*.

Paso 3. **Desplázate** hasta el archivo de volumen *TrueCrypt* y **selecciónalo** (el mismo archivo que para el Volumen común).

Paso 4. **Pulsa** 

para regresar al *panel de control de **TrueCrypt**.

Paso 5. **Pulsa** 

para activar la pantalla de solicitud de *Ingrese la contraseña* como sigue:

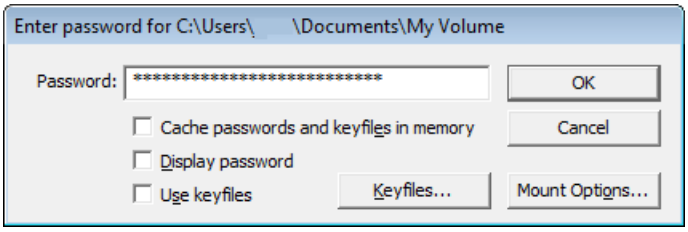


Figura 9: Pantalla Ingrese la contraseña

Paso 6. **Ingresa** la contraseña que usaste para crear el Volumen oculto y luego **pulsa** 

.

Tu Volumen oculto ya está montado (o abierto) como sigue:

Figura 10: Pantalla principal de TrueCrypt que muestra el Volumen oculto recientemente montado

Paso 7. **Pulsa dos veces** sobre la entrada o accede a ella a través de la ventana *Mi computadora*.

5.3 Consejos acerca de cómo utilizar la característica del disco oculto de manera segura

El propósito de la característica del disco oculto es escapar a la potencial situación de peligro *aparentemente* entregando tus archivos cifrados, cuando alguien en una posición de poder demande verlos, sin estar realmente forzado a revelar tu información más sensible. Además de proteger tu información, esto puede permitirte que evites poner en peligro tu seguridad, la de tus colegas o compañeros. Para que esta técnica sea efectiva, debes crear una situación en la que la persona que demande ver tus archivos se satisfaga con lo que le muestres y te deje ir.

Para esto, quizá quieras implementar algunas de las sugerencias siguientes:

- Coloca en el Volumen común algunos documentos confidenciales que no te importe exponer. Esta información deberá ser lo suficientemente sensible como para que la mantengas en un volumen cifrado.
- Ten en cuenta que alguien que exija ver tus archivos puede saber de Volúmenes ocultos. No obstante, si utilizas **TrueCrypt** correctamente, esta persona no podrá probar la existencia de tu Volumen oculto, lo que hará tu negativa más fácil de creer.
- Actualiza los archivos en el Volumen común semanalmente. Esto creará la impresión de que realmente utilizas esos archivos.

Siempre que montes un volumen **TrueCrypt**, puedes elegir habilitar la característica *Proteger Volumen oculto contra daños causados por la escritura en el Volumen externo*. Una característica *muy* importante, que te permite agregar nuevos archivos «señuelo» a tu Volumen común sin riesgo de borrar o sobrescribir accidentalmente el contenido cifrado de tu Volumen oculto.

Como se mencionó anteriormente, si excedes el límite de almacenamiento en tu Volumen común puedes destruir tus archivos ocultos. No habilites la característica *Proteger el Volumen oculto* si te fuerzan a montar un volumen **TrueCrypt**, porque para hacerlo tendrás que ingresar la contraseña secreta de tu Volumen oculto y revelarás claramente la existencia de dicho volumen. No obstante, cuando actualices los archivos señuelo en privado *siempre* debes habilitar esta opción.

Para utilizar la característica *Proteger el Volumen oculto* sigue los siguientes pasos:

Paso 1. **Pulsa** 

en la pantalla de solicitud de *Ingrese la contraseña* que se muestra en la *Figura 9*, arriba. Esto activará la ventana de *Opciones de montaje* como sigue:

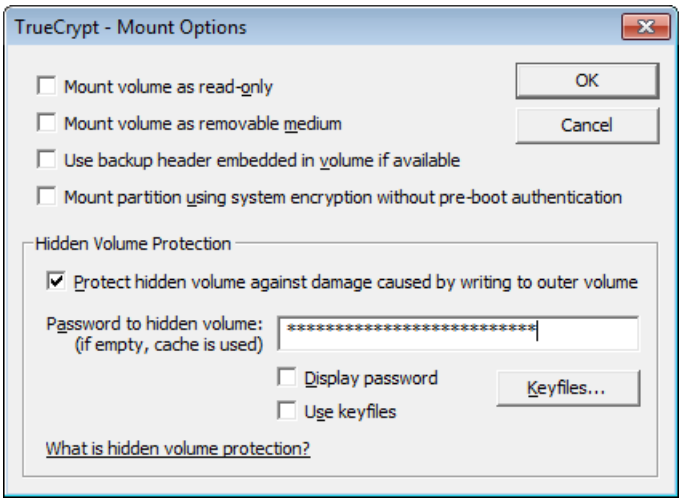


Figure 11: Ventana de opciones de montaje

Paso 2. **Marca** la opción *Protect hidden volume against damage caused by writting to outer volume (Proteger el Volumen oculto contra daños ocasionados por la escritura en el volumen externo)*.

Paso 3. **Ingresa** la contraseña en tu Volumen oculto y luego **pulsa** OK.

Paso 4. **Pulsa** Mount para montar tu Volumen común. Luego de montarlo satisfactoriamente, podrás agregar archivos señuelo sin dañar tu Volumen oculto.

Paso 5. **Pulsa** Dismount para desmontar tu Volumen común o inhabilitar su uso, cuando hayas terminado de modificar su contenido.

Recuerda: Sólo debes hacer esto cuando actualices los archivos en tu Volumen común. Si te ves forzado a revelar tu Volumen común a alguien, no debes utilizar la característica *Proteger Volumen oculto*.

Preguntas Frecuentes y Revisión

7.0 Preguntas frecuentes y revisión

Pregunta: *¿Voy a tener que pasar todo mi tiempo ingresando contraseñas en **TrueCrypt**?

Respuesta: *No, sólo deberás ingresarla una vez, cuando abras el Volumen común. Una vez que lo hayas hecho, podrás abrir cualquier archivo sin tener que ingresar la contraseña cada vez que lo hagas.*

Pregunta: *¿Puedo desinstalar fácilmente **TrueCrypt** si ya no lo quiero? Si lo hago, ¿mis archivos permanecerán cifrados?*

Respuesta: *Sí, **TrueCrypt** puede eliminarse fácilmente al seleccionar **Inicio > Programas > TrueCrypt > Desinstalar TrueCrypt**.*

*Más tarde puedes volver a instalar a TrueCrypt para acceder a los archivos de cualquier volumen que hayas creado. Si transfieres el volumen a otra computadora, aun necesitarás tu contraseña y el programa **TrueCrypt** para acceder al mismo.*

Pregunta: Las diferentes versiones de **Windows** ¿traerán pantallas diferentes cuando trate de cargar y utilizar **TrueCrypt**?*

Respuesta: *Es posible que su apariencia sea ligeramente distinta, pero el contenido será el mismo.*

Pregunta: *¿Qué tipo de archivos requiere cifrado?*

Respuesta: *Lo ideal es que cifres todos tus documentos, fotografías y cualquier otro archivo que contenga información privada y sensible. Si pierdes tu computadora, o si la confiscan, la información en tu Volumen **TrueCrypt** se mantendrá segura.*

Pregunta: *¿Cómo de seguros estarán los archivos?*

Respuesta: ***TrueCrypt*** ha sido probado y examinado independientemente por expertos en seguridad para ver cómo realiza todas las funciones o si las realiza como alega. Los resultados generales demuestran que **TrueCrypt** ofrece un nivel de protección muy alto. Elegir una contraseña sólida es esencial para la seguridad de tu volumen.

La característica de disco oculto en **TrueCrypt** ofrece un nivel de seguridad único para la información almacenada en la computadora. El usuario deberá tener un control excelente del programa y sus funciones básicas, así como una capacidad experta para evaluar su propia situación de seguridad, y de cuándo será útil el uso de la característica de disco oculto.

Pregunta: *Recuérdame nuevamente, ¿cómo monto mi Volumen común, en lugar del oculto?*

Respuesta: *Todo depende de la contraseña que ingreses en la casilla de la contraseña. Si ingresas la contraseña del Volumen común, **TrueCrypt** montará ese Volumen común. Si ingresas la contraseña del Volumen oculto, **TrueCrypt** montará ese Volumen oculto. Si alguien te obliga a abrir tu volumen **TrueCrypt** para ver qué clase de información guardas, abres el Volumen común. Se espera que esto sea suficiente para librarte de la situación y de problemas.*

Pregunta: *¿Es posible dañar o borrar el Volumen oculto inadvertidamente?*

Respuesta: *Sí. Si continuas agregando archivos al Volumen común **TrueCrypt** hasta que no quede suficiente espacio libre (para que exista el disco oculto), sobrescribirás tu disco oculto automáticamente. Existe una opción en el menú de **TrueCrypt** que puede proteger tu disco oculto de ser sobrescrito, pero si activas esta opción puedes identificar la existencia del disco oculto a un adversario cuando el volumen esté abierto.*

Pregunta: *¿Puedo cambiar el tamaño del disco oculto luego de crearlo?*

Respuesta: *No. Tendrás que crear otro disco oculto y mover tu archivos manualmente al mismo.*

Pregunta: ¿Puedo utilizar herramientas como **chkdsk**, **Desfragmentador de disco**, y otras en los contenidos de un volumen **TrueCrypt** montado?

Respuesta: Los volúmenes ***TrueCrypt*** se comportan como dispositivos de disco físico reales, de modo que es posible utilizar cualquier herramienta para verificar, reparar o desfragmentar los contenidos de cualquier volumen **TrueCrypt** montado.

Pregunta: *¿Es posible cambiar la contraseña de un Volumen oculto?*

Respuesta: Sí. La característica de Cambio de contraseña se puede utilizar tanto para Volúmenes comunes como Volúmenes ocultos. Solo ingresa la contraseña del Volumen oculto en el campo «Contraseña actual» de la pantalla de solicitud «Cambio de contraseña de volumen.»

Pregunta: *¿Cuándo debo utilizar la característica de disco oculto?*

Respuesta: *Utiliza la característica de disco oculto cuando necesites ocultar la existencia de cierta información en tu computadora. Nota que esto no es lo mismo que utilizar un Volumen común, donde proteges el acceso a la información.*

Visita Preguntas y Respuestas detalladas sobre **TrueCrypt** [39].

7.1 Preguntas de revisión del Volumen común

- ¿Qué es cifrado?
- ¿Qué es un *Volumen común*?
- ¿Cómo puedes crear un *Volumen común* en un dispositivo de memoria USB?
- ¿Cuáles son las formas distintas de desmontar un *Volumen común*?
- ¿Cómo puedes escoger y mantener una buena contraseña para tu *Volumen común*?
- ¿Cuáles son las posibilidades de crear un archivo de respaldo de tu *Volumen común*?
- ¿Cuáles son algunos de los métodos para disimular la presencia de tu *Volumen común* en la computadora?

7.2 Preguntas de revisión del Volumen oculto

- ¿Cuál es la principal diferencia entre un *Volumen común* y un *Volumen oculto*?
- ¿Qué tipos de archivos debes colocar en un *Volumen común*, si también tienes uno oculto?
- ¿Dónde está ubicado el *Volumen oculto*?
- ¿Cuál es el tamaño ideal de un *Volumen oculto*?
- ¿Cuáles son las ventajas y desventajas de proteger tu *Volumen oculto* de un borrado accidental?

TrueCrypt Portátil

Short Description:

Truecrypt mantiene seguros tus archivos evitando que cualquiera sin la contraseñas correcta pueda abrir tus documentos y archivos ocultos. Este trabaja como una caja fuerte electrónica, la cual puedes utilizar para guardar de manera segura

tus archivos.

6.1 Diferencias entre las versiones instalada y portátil de TrueCrypt

Las herramientas portátiles no se instalan en una computadora local, por ello, su existencia y uso pueden pasar desapercibidos. No obstante, ten en cuenta que tu dispositivo de memoria USB o externo y las herramientas portátiles son solo tan seguros como la computadora que utilizas; y pueden estar expuestos a programas informáticos publicitarios (adware), maliciosos (malware), espías (spyware) y virus.

Al igual que para muchas de las herramientas portátiles que documentamos aquí, **TrueCrypt portátil** te permite utilizar una herramienta simple y poderosa de cifrado sin ser detectada. Si tienes a **TrueCrypt portátil** en un dispositivo extraíble o de memoria USB podrás utilizarlo desde estaciones de trabajo diferentes.

Existen muy pocas diferencias entre la versión instalada y la **TrueCrypt portátil**; principalmente **TrueCrypt portátil** no permite el cifrado del sistema o disco completo.

Para obtener más información acerca de las diferencias entre **TrueCrypt** y **TrueCrypt portátil** visita **andryou.com/truecrypt/docs/truecrypt-portable.php** [40].

6.2 Descarga, extracción y uso de TrueCrypt portátil

Nota: La carpeta en la que se extrae el **TrueCrypt portátil** se debe crear manualmente en el dispositivo extraíble, dispositivo de memoria USB o disco de computadora antes del proceso de la extracción.

Paso 1. **Desplázate** hasta donde deseas extraer el programa **TrueCrypt portátil** y luego **pulsa el botón derecho del ratón** para activar el menú asociado.

Paso 2. **Selecciona** la opción *Nuevo* para activar la *subcarpeta* del submenú, como se muestra en la *Figura 1* a continuación:

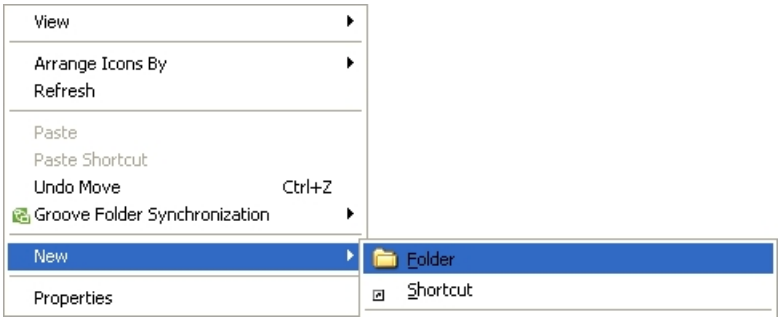


Figura 1: Explorador de Windows y la subcarpeta

Paso 3. **Ingresa** el nombre de la carpeta.

Nota: Puedes darle un nombre menos obvio para ocultar la existencia del programa **TrueCrypt portátil**.

Se puede extraer al **TrueCrypt portátil** desde el mismo archivo donde se encuentra la versión de la instalación:

Paso 1. **Desplázate** hasta el archivo **TrueCrypt** de tu computadora.

Paso 2. **Pulsa dos veces** TrueCrypt Setup 7.1a.exe ; puede aparecer la ventana *Abrir archivo - Advertencia de seguridad*; si aparece, **pulsa** Next > para activar el asistente de instalación de **TrueCrypt**.

Paso 5. **Elige** la opción **Extraer** para extraer el **TrueCrypt** portátil a una unidad externa o dispositivo de memoria USB como se muestra en la *Figura 3* a continuación:

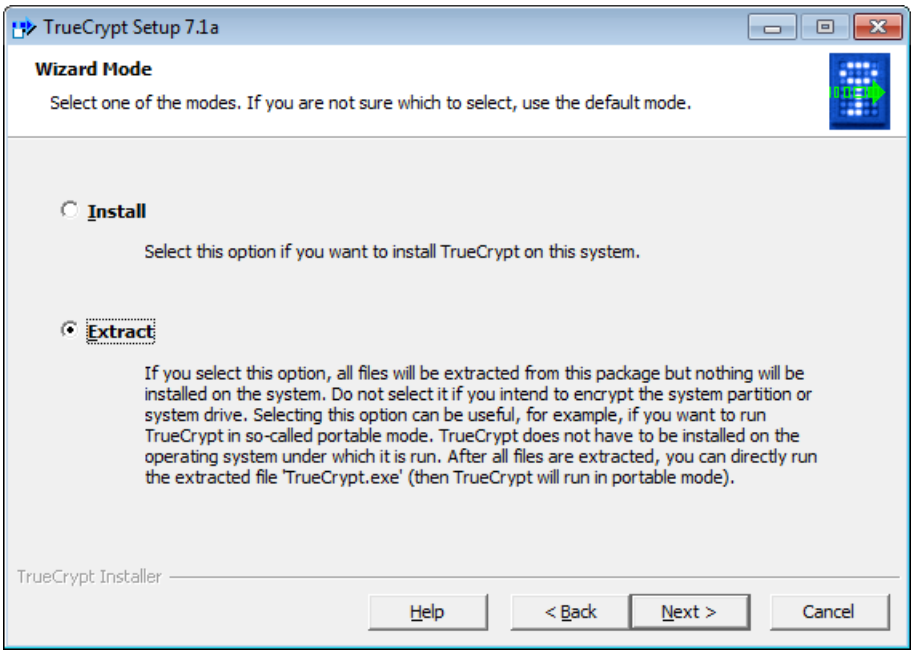
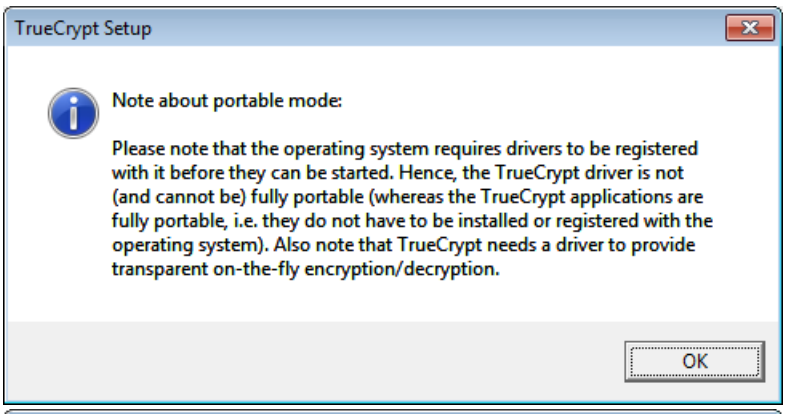
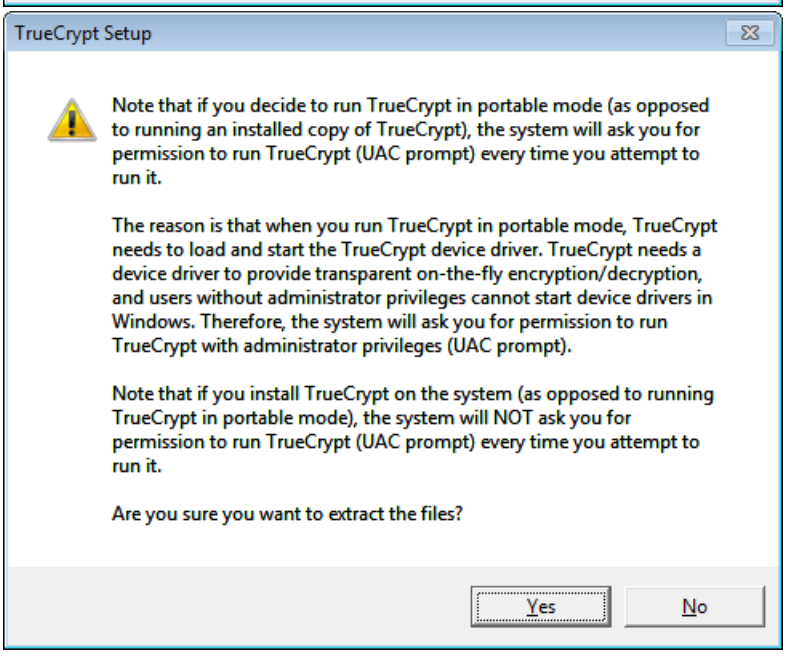


Figura 3: Ventana del asistente de modo - Selecciona uno de los modos

Paso 6. **Pulsa** Next > para activar la dos pantallas siguientes:





Pulsa OK y Yes respectivamente para activar la ventana de las **Opciones de extracción** como sigue:

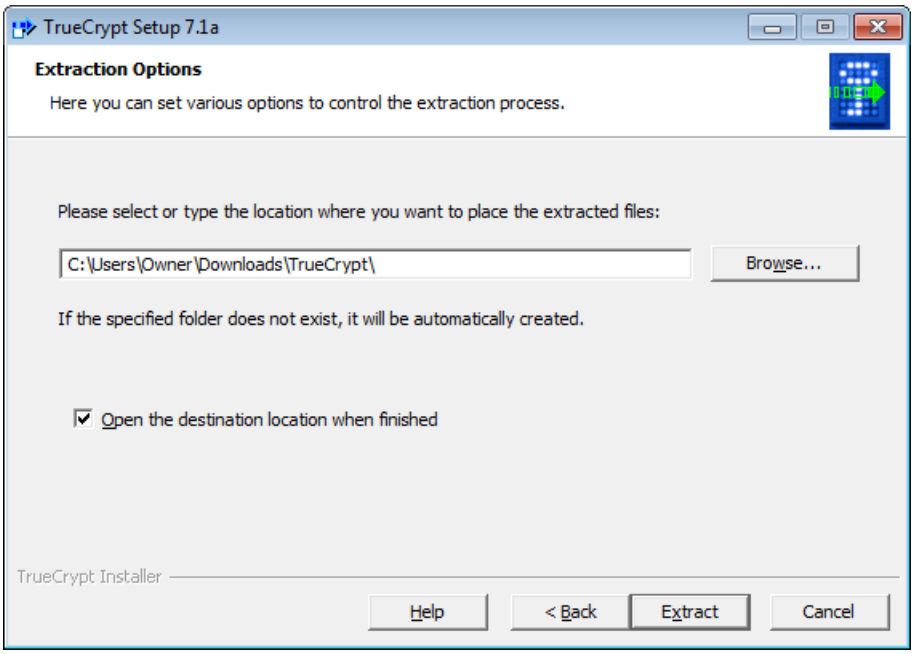


Figura 4: Ventana de opciones de extracción

Paso 7. **Pulsa** Browse... para activar la ventana *Buscar carpeta* como sigue:

Figura 5: Ventana de buscar carpeta

Paso 8. **Desplázate** hasta tu carpeta de destino en la unidad externa o el dispositivo de memoria USB y luego **pulsa** OK para regresar a la ventana de *Opciones de extracción* como sigue:

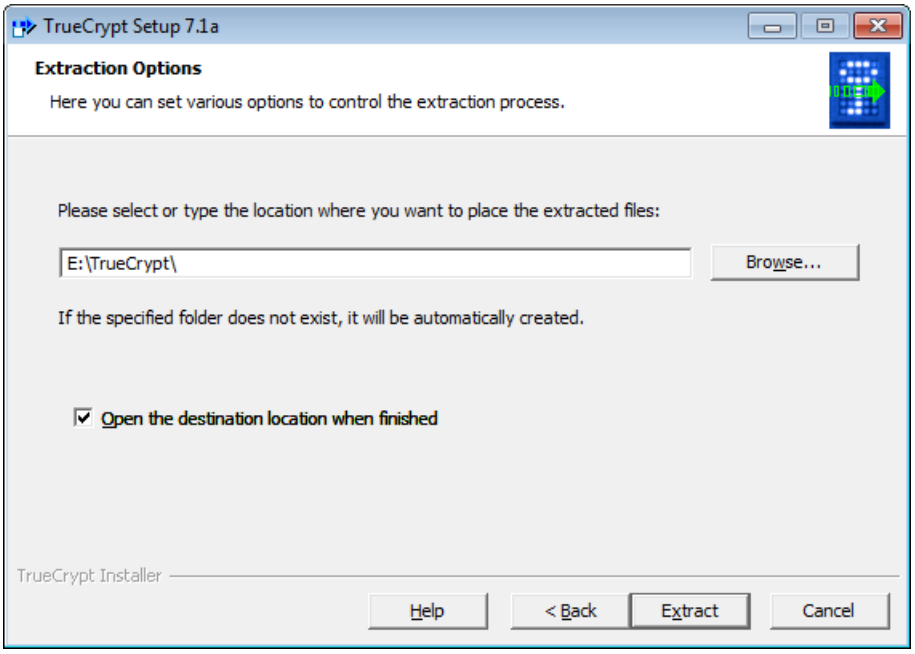


Figura 6: Ventana de Opciones de extracción que muestra la carpeta de destino

Paso 9. **Pulsa** Extract para comenzar a extraer **TrueCrypt** a tu unidad extraíble o dispositivo de memoria USB; unos segundos más tarde, aparecerán las pantallas siguientes:

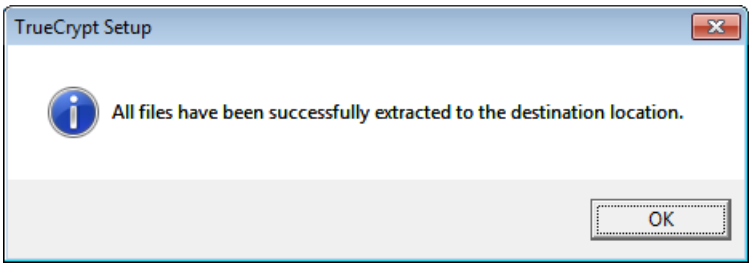


Figura 7: Cuadro de diálogo emergente de confirmación y ventana de Extracción completa de TrueCrypt

Paso 10. **Pulsa** OK y luego **pulsa** Finish para completar el proceso de la instalación.

Si la opción estaba habilitada (suele estarlo por defecto), aparecerá la siguiente pantalla:

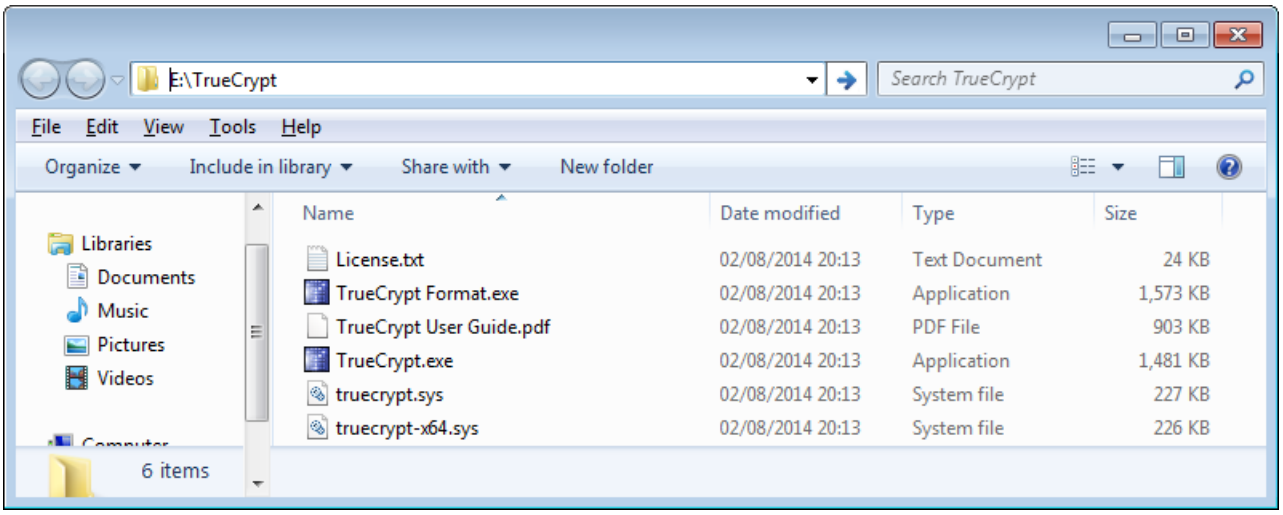


Figura 8: Ejemplo de TrueCrypt portátil extraído a una unidad extraíble

Paso 11. **Desplázate** hasta él y luego **pulsa dos veces** TrueCrypt.exe para ejecutar el **TrueCrypt portátil**.

Considera consultar el capítulo **Truecrypt** [41] en la sección **Guía práctica** para las instrucciones de cómo utilizar **TrueCrypt**.

6.3 ¿Cómo eliminar todos los rastros de la extracción de TrueCrypt portátil?

Importante: Luego de haber extraído **TrueCrypt portátil** satisfactoriamente a tu dispositivo externo o extraíble, debes **borrar** el archivo de instalación de tu computadora para eliminar todo rastro de haber descargado e instalado **TrueCrypt portátil**.

Paso 1. **Desplázate** hacia la carpeta en la que descargaste el **TrueCrypt portátil**, y luego **pulsa el botón derecho del ratón** el archivo de instalación TrueCrypt Setup 7.1a.exe para activar el menú emergente de **Windows**; luego, **selecciona** el comando **Borrar** para moverlo a tu **Papelera de reciclaje**.

Paso 2. **Pulsa dos veces** Recycle Bin para abrir la ventana asociada, y luego **selecciona** y **borra** el archivo.

Nota: Si tienes instalado el **CCleaner** [42] o el **Eraser** [43], puedes utilizar cualquiera de ellos para eliminar todos los rastros de la descarga e instalación de **TrueCrypt portátil**.

URL de origen (Obtenido en *20/06/2015 - 21:22*): https://info.securityinabox.org/es/truecrypt_principal

Enlaces:
[1] https://info.securityinabox.org/sbox/programs/truecrypt/TrueCrypt%20Setup%207.1a.exe
[2] https://info.securityinabox.org/sbox/programs/truecrypt/TrueCrypt%20Setup%207.1a.exe.sig
[3] https://info.securityinabox.org/sbox/programs/truecrypt/TrueCrypt%207.1a%20Mac%20OS%20X.dmg
[4] https://info.securityinabox.org/sbox/programs/truecrypt/TrueCrypt%207.1a%20Mac%20OS%20X.dmg.sig
[5] https://info.securityinabox.org/sbox/programs/truecrypt/truecrypt-7.1a-linux-x86.tar.gz
[6] https://info.securityinabox.org/sbox/programs/truecrypt/truecrypt-7.1a-linux-x86.tar.gz.sig
[7] https://info.securityinabox.org/sbox/programs/truecrypt/truecrypt-7.1a-linux-x64.tar.gz
[8] https://info.securityinabox.org/sbox/programs/truecrypt/truecrypt-7.1a-linux-x64.tar.gz.sig
[9] https://info.securityinabox.org/sbox/programs/truecrypt/truecrypt-7.1a-linux-console-x86.tar.gz
[10] https://info.securityinabox.org/sbox/programs/truecrypt/truecrypt-7.1a-linux-console-x86.tar.gz.sig

[11] https://info.securityinabox.org/sbox/programs/truecrypt/truecrypt-7.1a-linux-console-x64.tar.gz
[12] https://info.securityinabox.org/sbox/programs/truecrypt/truecrypt-7.1a-linux-console-x64.tar.gz.sig
[13] https://info.securityinabox.org/sbox/programs/truecrypt/TrueCrypt%207.1a%20Source.zip
[14] https://info.securityinabox.org/sbox/programs/truecrypt/TrueCrypt%207.1a%20Source.zip.sig
[15] https://info.securityinabox.org/sbox/programs/truecrypt/VersionHistory.txt
[16] https://keys.mozilla.org/pks/lookup?op=get&search=0xE3BA73CAF0D6B1E0
[17] https://info.securityinabox.org/sbox/programs/truecrypt/F0D6B1E0.asc
[18] https://www.torproject.org/docs/verifying-signatures.html.en
[19] https://truecrypt.ch/downloads/
[20] http://www.truecrypt.org
[21] https://info.securityinabox.org/es/truecrypt_portatil
[22] https://info.securityinabox.org/es/chapter-4
[23] http://www.ubuntu.com/
[24] http://www.saout.de/misc/dm-crypt/
[25] http://code.google.com/p/cryptsetup/
[26] http://sd4l.sourceforge.net/
[27] https://diskcryptor.net/wiki/Main_Page
[28] http://www.axantum.com/AxCrypt/
[29] http://windows.microsoft.com/en-us/windows7/products/features/bitlocker
[30] https://info.securityinabox.org/es/guiaspracticas
[31] https://info.securityinabox.org/sbox/programs/TrueCrypt-Setup.exe
[32] https://info.securityinabox.org/sbox/programs/TrueCrypt-es.zip
[33] http://andryou.com/truecrypt/docs/index.php
[34] http://www.truecrypt.org/docs/
[35] https://info.securityinabox.org/es/truecrypt_volumenesocultos
[36] https://info.securityinabox.org/es/keepass_principal
[37] https://info.securityinabox.org/es/chapter-6
[38] https://info.securityinabox.org/es/truecrypt_instalar_volumenescomunes#2.2
[39] http://andryou.com/truecrypt/faq.php
[40] http://andryou.com/truecrypt/docs/truecrypt-portable.php
[41] https://info.securityinabox.org/es/truecrypt_principal
[42] https://info.securityinabox.org/es/ccleaner_principal
[43] https://info.securityinabox.org/es/eraser_principal