Actividad 11. Cifrado con Veracrypt

Veracrypt es un software de código abierto para cifrar archivos, carpetas, unidades USB extraíbles, discos duros completos, e incluso el disco duro donde se encuentra el propio sistema operativo instalado. **VeraCrypt** es multiplataforma, actualmente es compatible con sistemas operativos Microsoft Windows, cualquier sistema basado en Linux, y también es compatible con macOS.

Este software está basado en el popular **TrueCrypt 7.1a.** Debemos recordar que el proyecto TrueCrypt cerró, y ya no tendremos nuevas actualizaciones de dicho software.

Sin embargo, **VeraCrypt** ha cogido el testigo e incorpora todas las características de **TrueCrypt** y muchas mejoras de seguridad y rendimiento.

PRINCIPALES CARACTERÍSTICAS DE VERACRYPT

- Creación de discos cifrados virtuales en un simple archivo: podremos crear un archivo cifrado a modo de contenedor, en el cual esté toda la información importante. Este archivo lo podremos montar para su lectura y escritura con VeraCrypt, este método es ideal para moverlo a cualquier sitio e incluso para enviarlo por email, subirlo a un servidor FTP o Samba y más. Gracias a que tenemos un simple archivo que contiene toda la información confidencial, podremos guardarlo a buen recaudo grabándolo en un CD o DVD, e incluso copiarlo en un pendrive.
- Cifrado de dispositivos de almacenamiento extraíble como USB, tarjetas SD e incluso discos duros. En este caso, todo el dispositivo de almacenamiento extraíble estará complemente cifrado, Windows nos indicará que necesita formato el disco para poder leerlo, siempre debemos

pinchar en cancelar y abrirlo con VeraCrypt, introduciendo la correspondiente clave de descrifrado.

- Cifrado de cualquier partición de estos dispositivos de almacenamiento extraíble.
- Cifrado de la partición o disco completo donde Windows esté instalado. Esto nos permite hacer exactamente la misma función que Bitlocker, cifrará el disco duro o SSD por completo, para que tanto el sistema operativo como todos nuestros archivos estén a salvo frente a posibles robos.
- El cifrado y el descifrado es automático y se hace en tiempo real, siendo completamente transparente al usuario.
- El cifrado y descifrado si utilizamos AES se puede acelerar si el procesador del equipo soporta AES-NI, proporcionando una mayor velocidad de lectura y escritura.
- Posibilidad de crear un volumen «oculto» para evitar que un posible atacante nos fuerce a revelar la contraseña del volumen (chantaje, extorsión etc.)

Una vez que ya conocemos sus principales características, vamos a ver cómo descargar e instalar VeraCrypt en nuestro ordenador con Windows 10 Pro.

Descarga e instalación de VeraCrypt

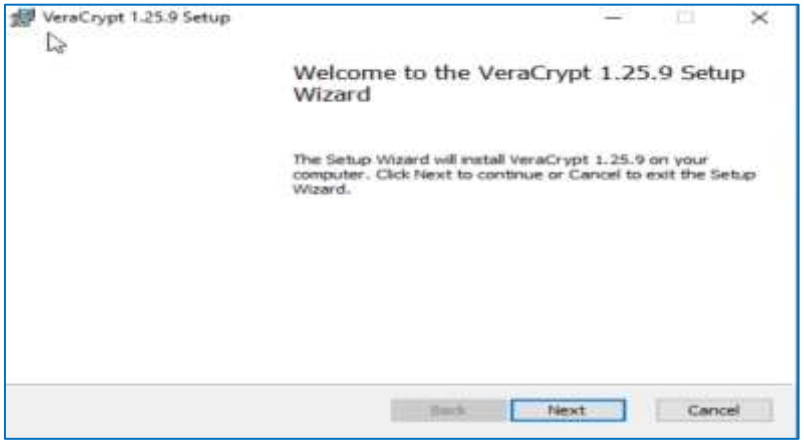
Lo primero que tenemos que hacer es descargar VeraCrypt, la descarga se realiza directamente a través de la página web oficial, en la sección descargas:

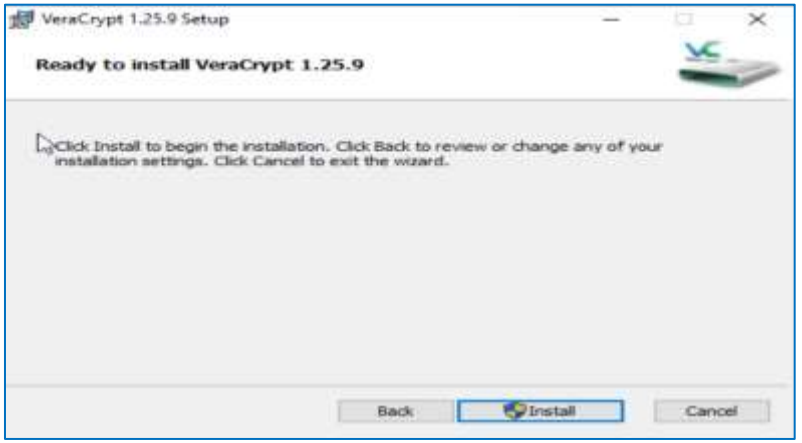
Descargar VeraCrypt

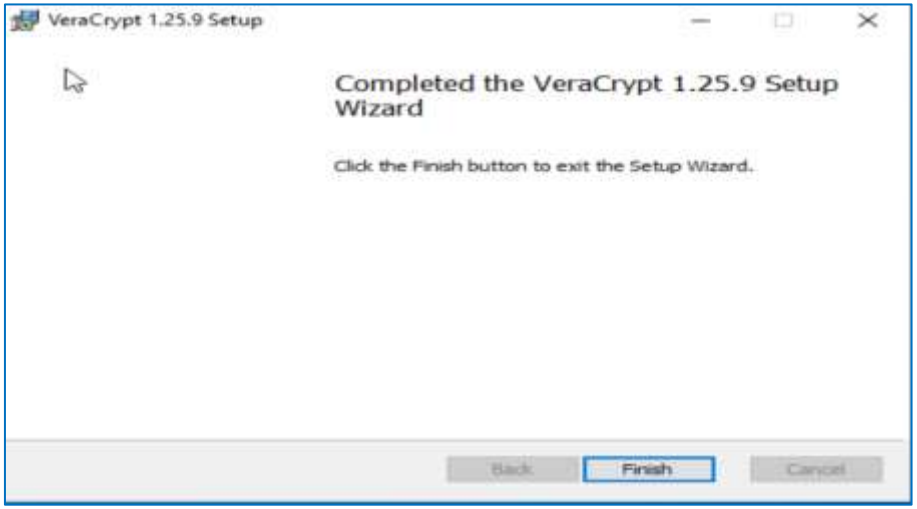
En esta web vamos a poder descargar todas las versiones de **VeraCrypt**, tanto para Windows, Linux, macOS, FreeBSD e incluso directamente el código fuente.

Debemos recordar que **VeraCrypt** es un programa completamente gratuito, no tendremos que pagar absolutamente nada por descargarlo o utilizarlo, lo podremos usar libremente sin ningún problema.

Instalación en Windows

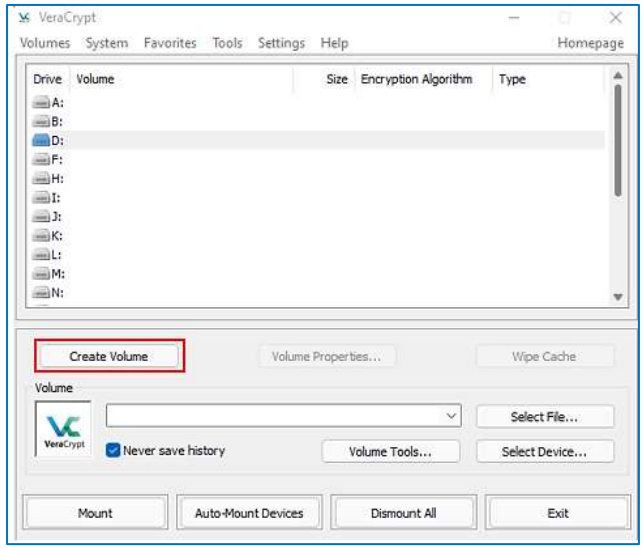

VeraCrypt 1.25.9 Setup
Welcome to the VeraCrypt 1.25.9 Setup Wizard
The Setup Wizard will install VeraCrypt 1.25.9 on your computer. Click Next to continue or Cancel to exit the Setup Wizard.
Back
Next
Cancel


VeraCrypt 1.25.9 Setup
Ready to install VeraCrypt 1.25.9
Click Install to begin the installation. Click Back to review or change any of your installation settings. Click Cancel to exit the wizard.
Back
Install
Cancel


VeraCrypt 1.25.9 Setup
Completed the VeraCrypt 1.25.9 Setup Wizard
Click the Finish button to exit the Setup Wizard.
Back
Finish
Cancel

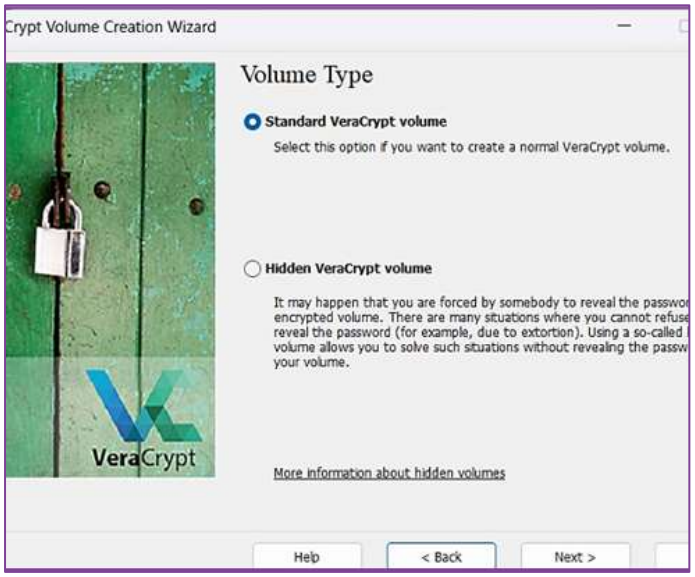
Crear un fichero contenedor encriptado:

1. Seleccionamos **Create Volume**:

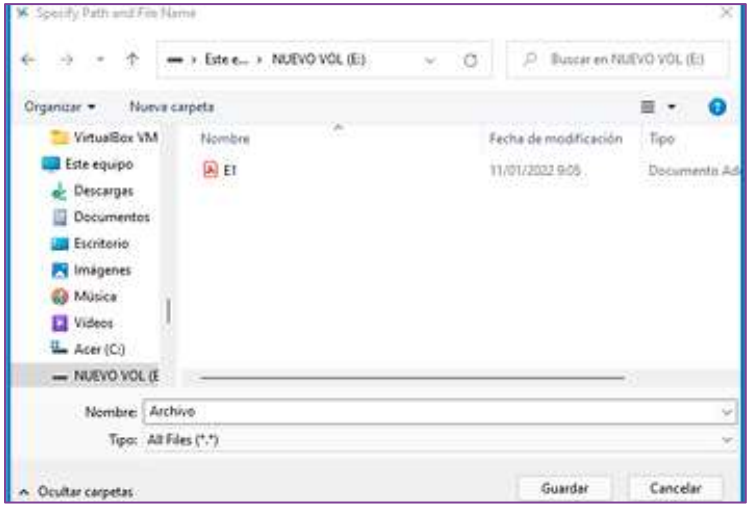


2. Seleccionamos la opción **Create an encrypted file container**:

3. Seleccionamos la opción **Standard Veracrypt volume**:



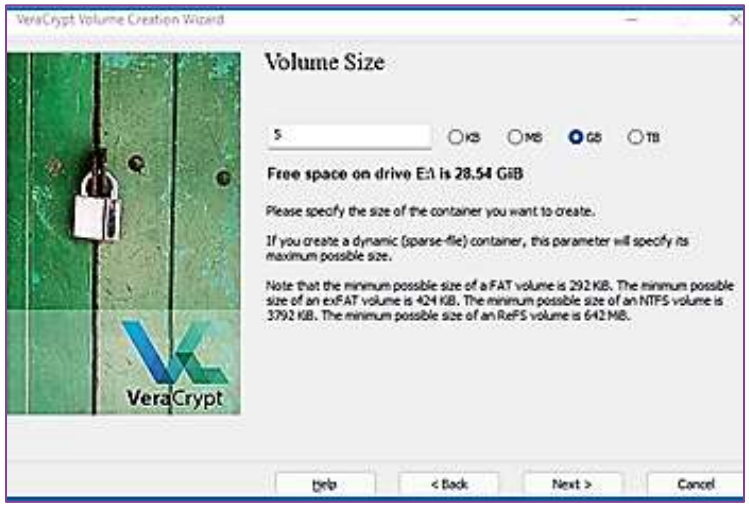
4. Le indicamos la ubicación y nombre de la carpeta contenedora:



5. Seleccionamos el dispositivo a encriptar:

6. Seleccionamos el algoritmo de encriptado:

7. Nos muestra el tamaño del volumen que vamos a crear:



8. Le indicamos la contraseña:

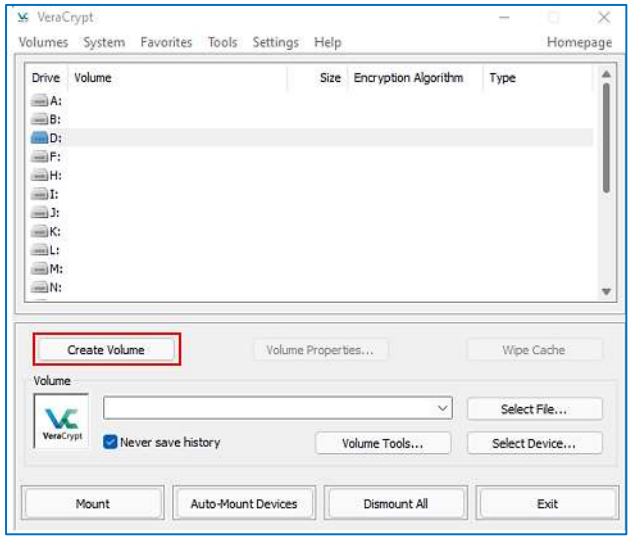
9. Para aumentar la fuerza de las claves de encriptado, movemos el ratón, hasta que aparezca la barra de color verde. A continuación, pulsamos **Format**:

10. Comienza el formateo. Dependiendo del tamaño de la unidad, tardará más o menos.

11. Finaliza el formateo.

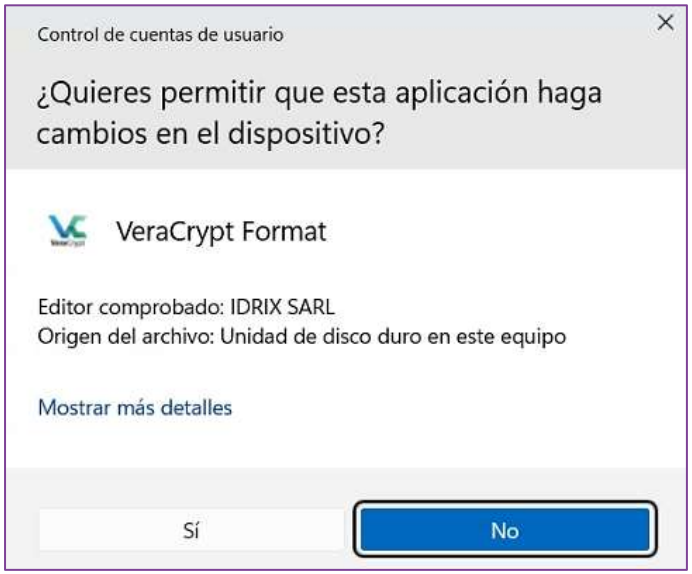
Crear una unidad encriptada:

1. Seleccionamos **Create Volume**:

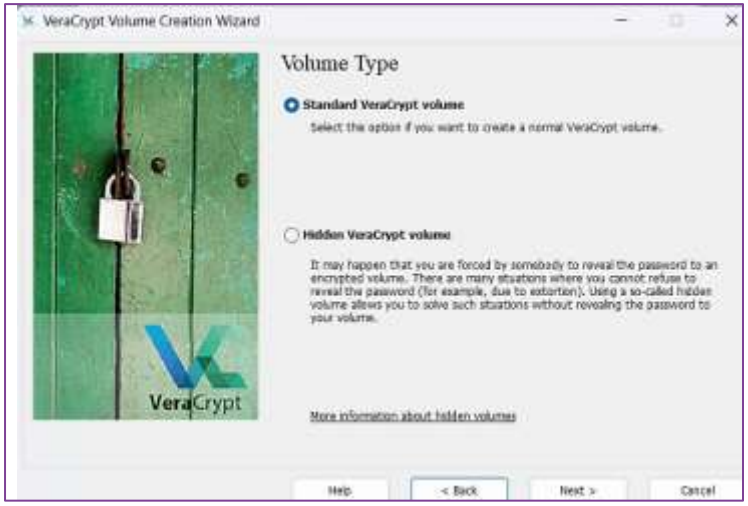


2. Seleccionamos la opción **Encrypt a non-system partition/Drive**:

3. Le indicamos **Sí** para permitir hacer cambios en el dispositivo:

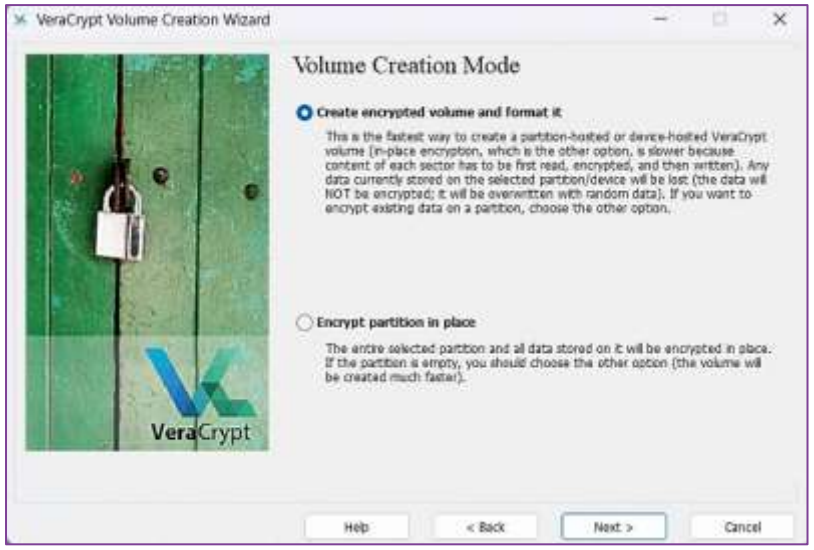


4. Seleccionamos la opción **Standard Veracrypt volume**:



5. Seleccionamos el dispositivo a encriptar:

6. Seleccionamos la opción **Create encrypted volumen and format it**:

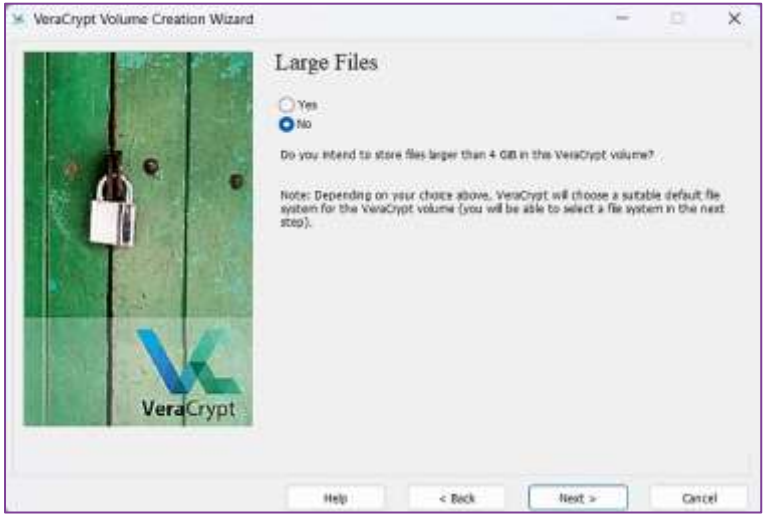


7. Seleccionamos el algoritmo de encriptado:

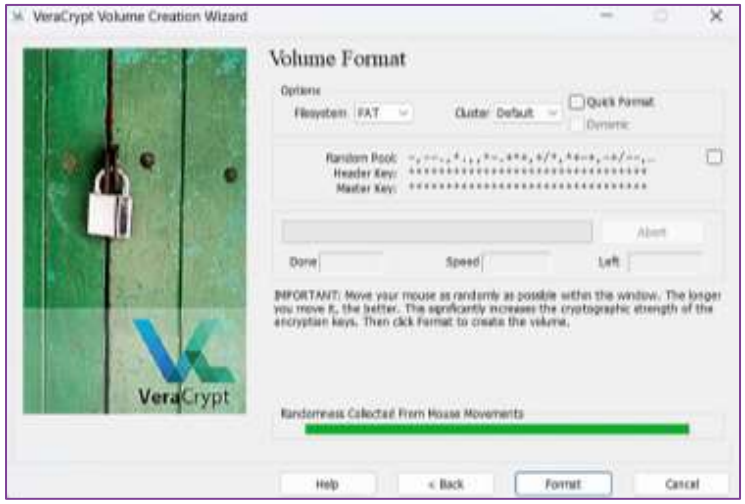
8. Nos muestra el tamaño del disco a encriptar:

9. Le indicamos la contraseña:

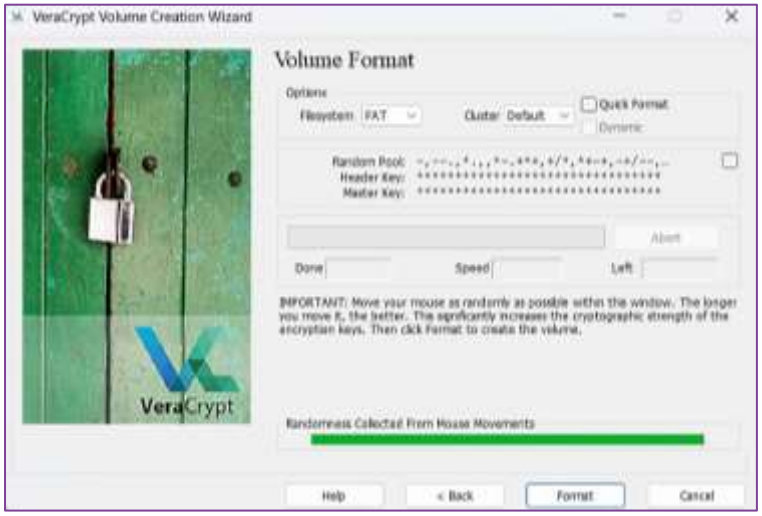
10. Si fuéramos a utilizar ficheros mayores de 4 GB, seleccionamos **Yes**, en caso contrario, seleccionamos **No:**



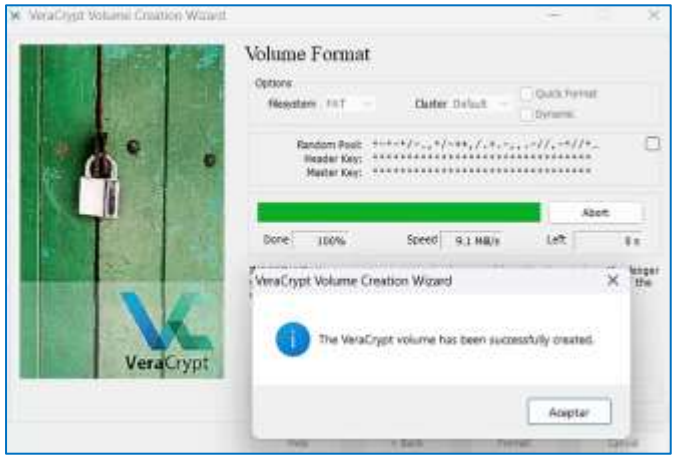
11. Para aumentar la fuerza de las claves de encriptado, moemos el ratón, hasta que aparezca la barra de color verde. A continuación, pulsamos **Format**:



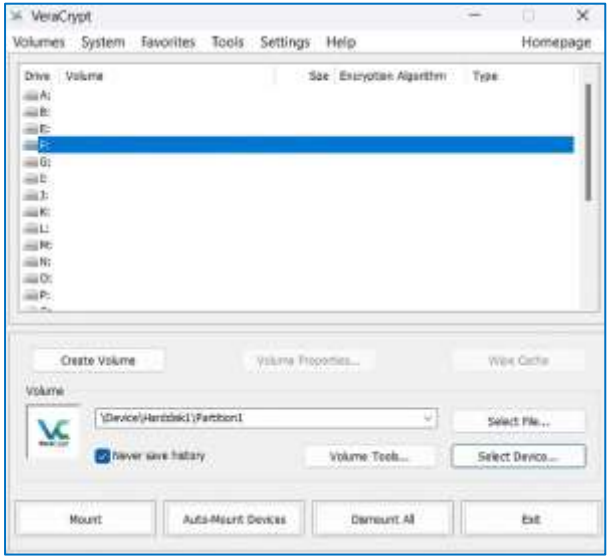
12. Comienza el formateo. Dependiendo del tamaño de la unidad, tardará más o menos.



13. Finaliza el formateo.



14. Si queremos visualizar el contenido de la unidad, tenemos que montarla. Para ello, seleccionamos una unidad disponible, seleccionamos el disco (**Select device)** y pulsamos **Mount**.



15. **Veracrypt** nos solicita la contraseña. Una vez escrita, aparecerá el disco encriptado como una unidad más: