VERACRYPT

Herramienta de cifrado de archivos y volúmenes

INDICE

- Introducción
- algoritmos de encriptación
- Productividad
- Contenedores VeraCrypt
- volumen oculto
- Conclusión

INTRODUCCIÓN

- VeraCrypt es un proyecto gratuito y abierto.
- Utiliza el cifrado sobre la marcha.
- Esta herramienta es compatible con Linux, Windows y Mac OS X.
- Esta herramienta puede encriptar particiones completas de disco y puede usar autenticación antes de cargar un disco que está completamente encriptado.

ALGORITMOS DE ENCRIPTACIÓN

Algorithm	Designer(s)	Key Size (Bits)	Block Size (Bits)	Mode of Operation
AES	J. Daemen, V. Rijmen	256	128	XTS
Serpent	R. Anderson, E. Biham, L. Knudsen	256	128	XTS
Twofish	B. Schneier, J. Kelsey, D. Whiting, D. Wagner, C. Hall, N. Ferguson	256	128	XTS
AES-Twofish		256; 256	128	XTS
AES-Twofish-Serpent		256; 256; 256	128	XTS
Serpent-AES		256; 256	128	XTS
Serpent-Twofish-AES		256; 256; 256	128	XTS
Twofish-Serpent		256; 256	128	XTS

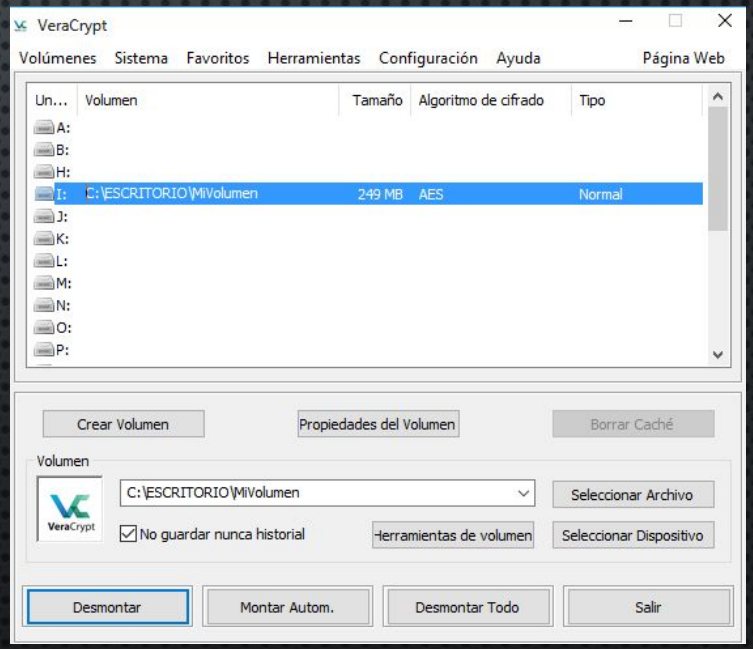
También se admiten las siguientes funciones hash: RIPEMD-160, SHA-256, SHA-512, Whirlpool. Esta.

PRODUCTIVIDAD

- El impacto en el rendimiento del cifrado del disco es particularmente notable.
- todos los datos deben pasar a través de la CPU para ser descifrados.
- VeraCrypt admite la paralelización para el cifrado de sistemas multi-core.
- la aceleración de hardware AES para mejorar aún más el rendimiento.

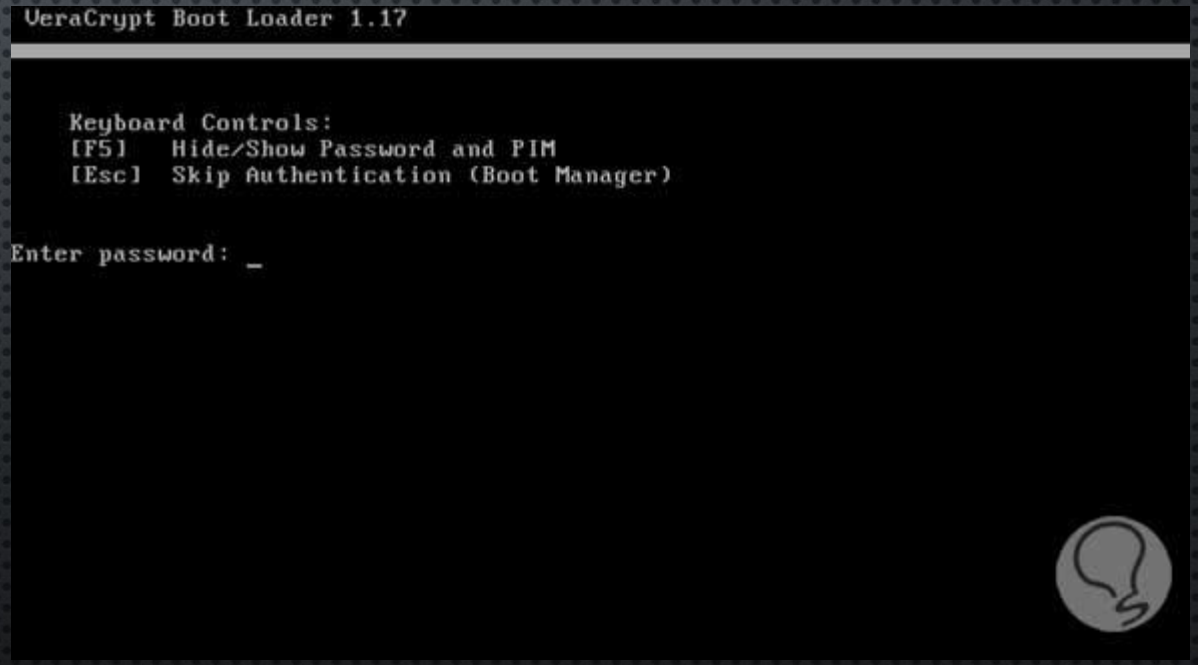
CONTENEDORES VERACRYPT

- EN VERACRYPT, UN CONTENEDOR DONDE SE ENCRIPTAN TODOS LOS ARCHIVOS.
- SE MONTAN LAS UNIDADES ESCRIBIENDO LA CONTRASEÑA CORRECTA.
- SE PUEDE UTILIZAR LA LLAVE PARA MONTAR CONTENEDOR.



VOLUMEN OCULTO

- Este cifrado es el más seguro.
- El cifrado del sistema funciona gracias a la autenticación antes de arrancar el sistema.
- Esta funcionalidad se implementa utilizando el bootloader de VeraCrypt.



Conclusión

- VeraCrypt es una herramienta de cifrado de archivos muy potente que soporta diversos tipos de algoritmos de cifrado.
- Herramienta muy útil para cifrar las unidades del HD, archivos individuales o unidades flash USB por completo.