

Telefonica



Curso de Ciberseguridad

Telefonica



Laboratorios TIPS Estenografía & Criptografía

HIDDEN FILES

UN ATACANTE PUEDE QUERER ESCONDER ARCHIVOS PARA QUE NO SEAN DETECTADOS POR EL SISTEMA

attrib +h (archivo/directorio)

Uso de ADS (Alternative Data Streaming) en filesystems en NTFS

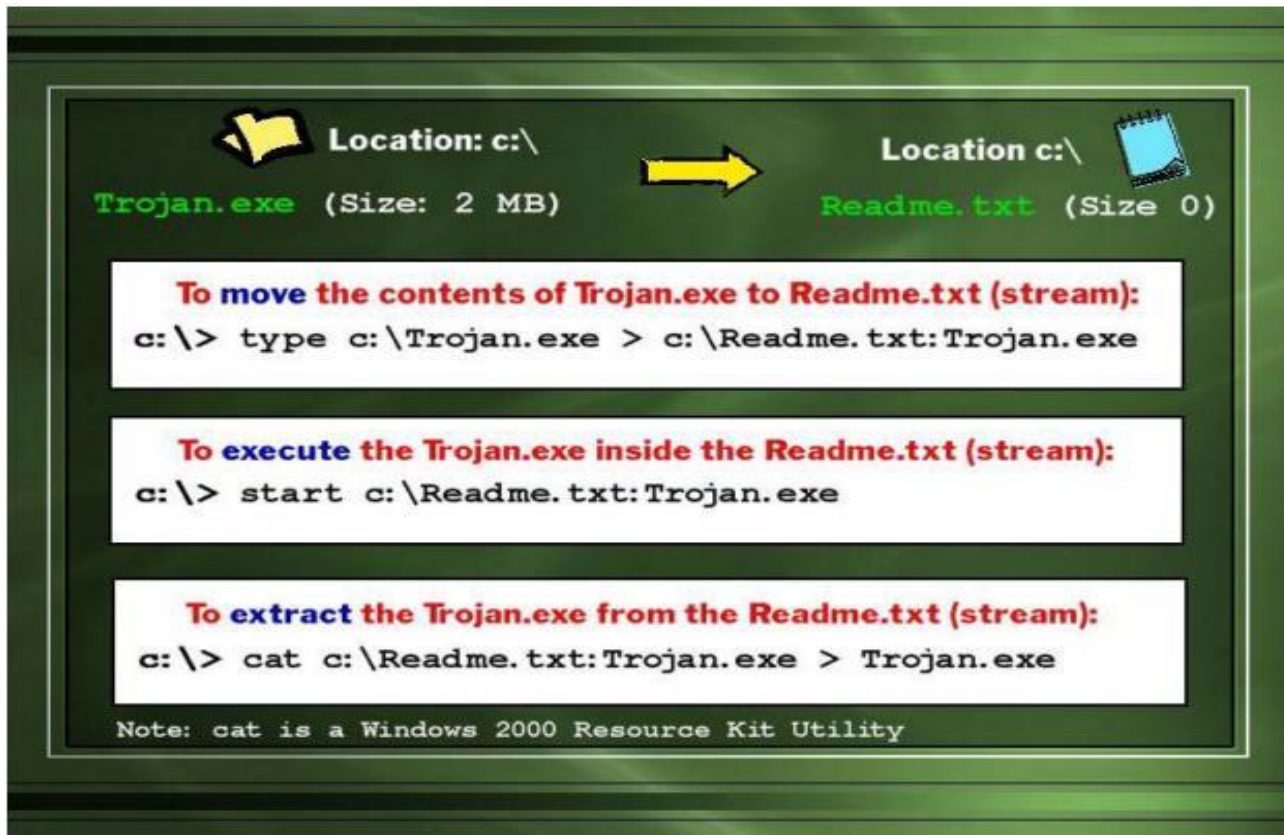
Esto permite almacenar datos en archivos ocultos enlazados a los visibles, teniendo la posibilidad de enlazar varios flujos al mismo archivo

HIDDEN FILES

UN ATACANTE PUEDE QUERER ESCONDER ARCHIVOS PARA QUE NO SEAN DETECTADOS POR EL SISTEMA

1. Crear un archivo de texto por línea de comandos: `notepad hola.txt`
2. Escribir algo, cerrarlo y guardarlo
3. Realizar un `DIR` y ver su tamaño
4. Escribir: `notepad hola.txt:hidden.txt` y agregar nuevo texto
5. Realizar otro `DIR` y ver el tamaño del archivo (se vera igual al punto 3)
6. Abrir `hola.txt` y se comprueba la información original
7. Escribir `type hola.txt:hidden.txt` y se vera un error de sintaxis
8. Para acceder a la información oculta: `notepad hola.txt:hidden.txt`
9. TOOLS: **MAKESTRM.EXE** = mueve datos de un archivo a un data stream enlazado al archivo original

HIDDEN FILES



The diagram illustrates a process for handling a Trojan file. It shows a transition from a file named **Trojan.exe** (Size: 2 MB) to a file named **Readme.txt** (Size 0). A yellow arrow points from the Trojan.exe file to the Readme.txt file. Below this, three white boxes provide instructions on how to move the contents, execute the Trojan, and extract it back.

Location: c:
Trojan.exe (Size: 2 MB)

Location c:
Readme.txt (Size 0)

To move the contents of Trojan.exe to Readme.txt (stream):
`c:\> type c:\Trojan.exe > c:\Readme.txt:Trojan.exe`

To execute the Trojan.exe inside the Readme.txt (stream):
`c:\> start c:\Readme.txt:Trojan.exe`

To extract the Trojan.exe from the Readme.txt (stream):
`c:\> cat c:\Readme.txt:Trojan.exe > Trojan.exe`

Note: cat is a Windows 2000 Resource Kit Utility

HIDDEN FILES

MAS TOOLS

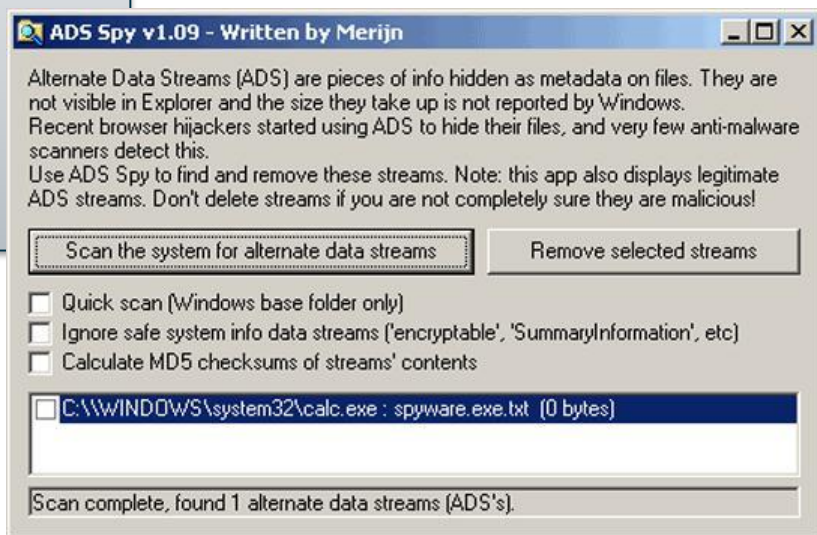
STREAMS

LNS

SFIND

ADS SPY

LADS



ESTEGANOGRAFIA

**Es el proceso de esconder datos, dentro de otros tipos de datos
Lo mas usado originalmente, es hacerlo dentro de imágenes digitales**

IMAGEHIDE: ESCONDE TEXTO SIN INCREMENTAR EL TAMAÑO DEL ARCHIVO ORIGINAL

BLINDSIDE: ESCONDE INFORMACION EN ARCHIVOS BMP

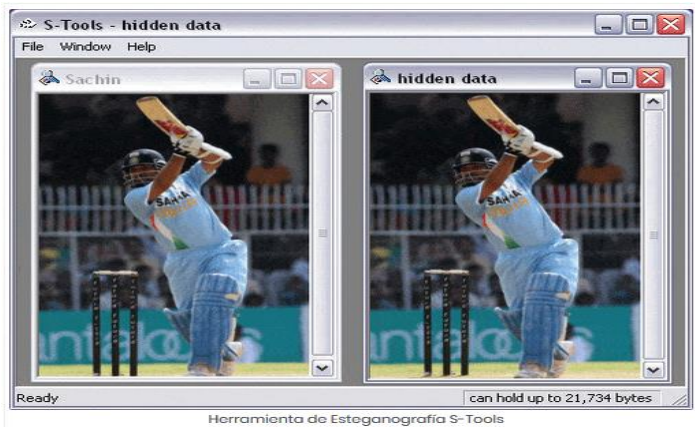
MP3STEGO: ESCONDE DENTRO DE ARCHIVOS MP3, COMPRIMIDA Y CIFRADA

SNOW: AGREGA INFORMACION EN TEXTOS ASCII MEDIANTE ESPACIOS EN BLANCO

GIFSHUFFLE: ESCONDE INFORMACION EN IMÁGENES GIF

**ES MUY DIFICIL DETECTAR UN CASO DE ESTEGANOGRAFIA, AUNQUE NO IMPOSIBLE
(SE USAN PATRONES, CAMBIOS EN LA PALETA, ETC)**

ESTEGANOGRAFIA



S-TOOLS

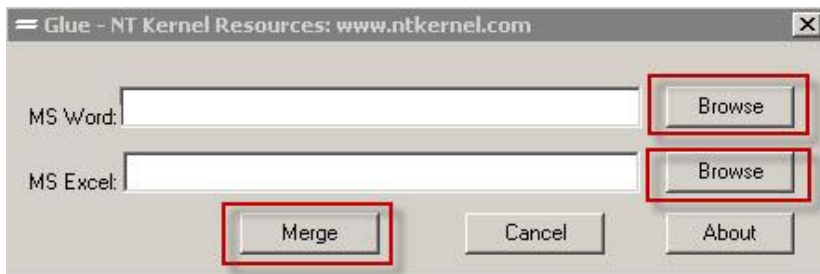
Oculta archivos en archivos BMP, GIF y WAV.

Permite ocultar varios archivos en un audio/imagen y sus datos se comprimen antes de ser cifrados y luego ocultos.

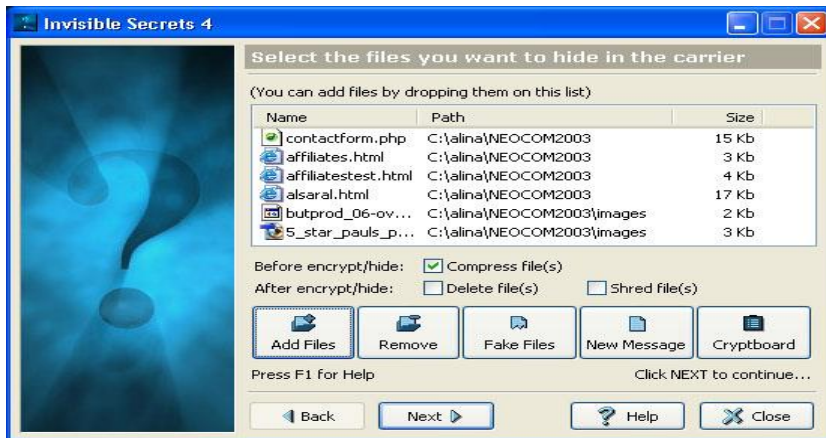
File Juicer (macOS)

SilentEye (Windows / Linux / macOS)

ESTEGANOGRAFIA

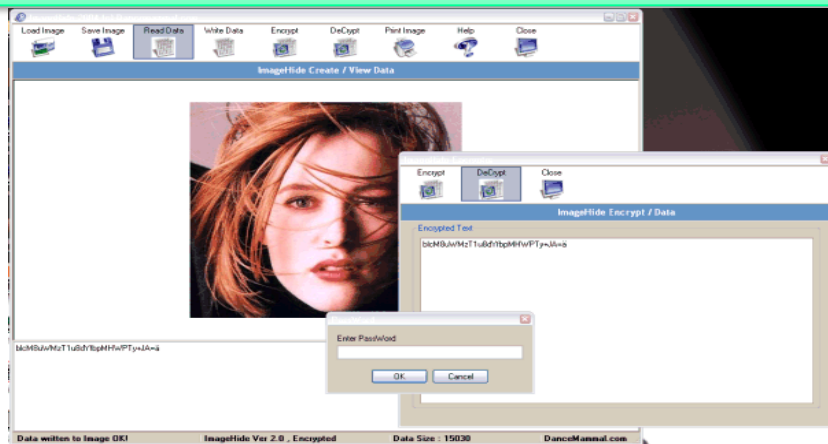


MERGE STREAM:
PERMITE HACER UN
MERGE ENTRE
ARCHIVOS DE WORD Y
EXCEL O VICEVERSA

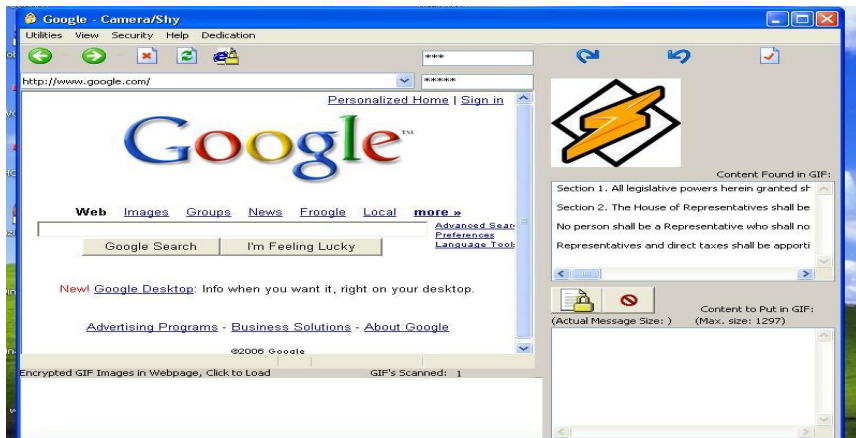


INVISIBLE SECRETS 4:
UNA SUITE DE
HERRAMIENTAS QUE
NOS PERMITE
TRABAJAR CON
ARCHIVOS OCULTOS,
CARPETAS, ETC

ESTEGANOGRAFIA

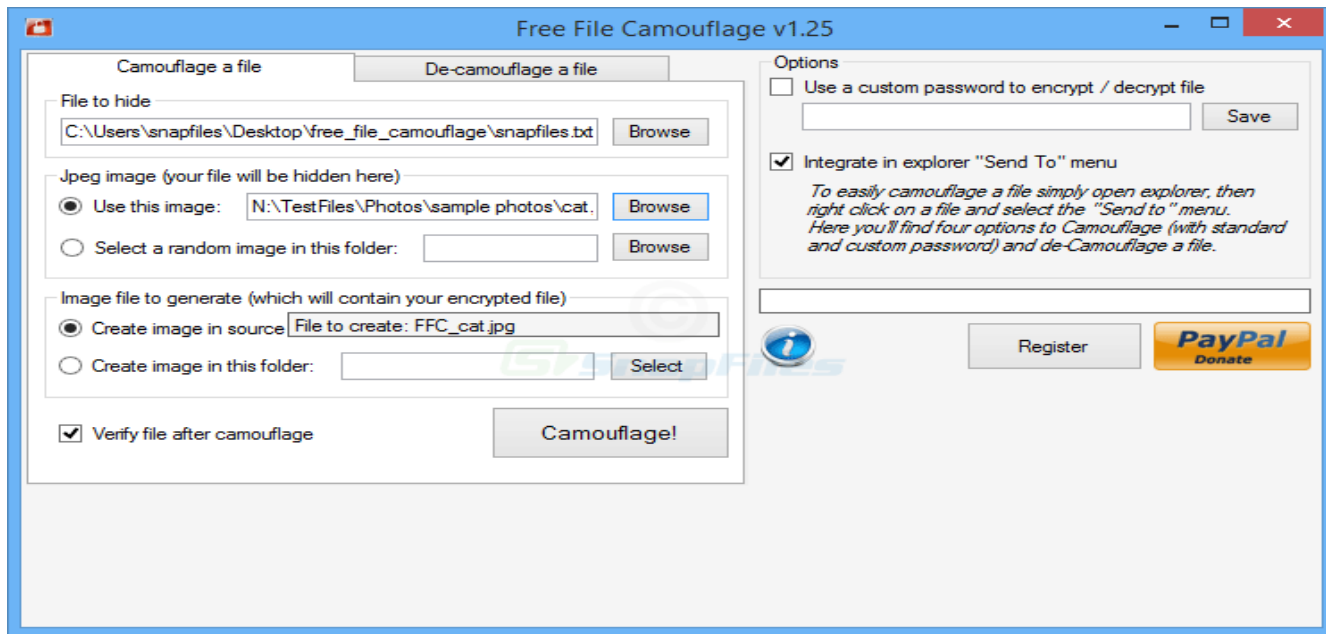


IMAGEHIDE: UNO DE LOS MEJORES PROGRAMAS DE ESTEGANOGRAFIA, PERMITIENDO ENCRIPCACION Y PROTECCION



CAMERA/SHY: PERMITE TRABAJAR CON IMÁGENES GIF, PARA ASI PODER APROVECHAR EL BAJO TAMAÑO DE LOS MISMOS

ESTEGANOGRAFIA



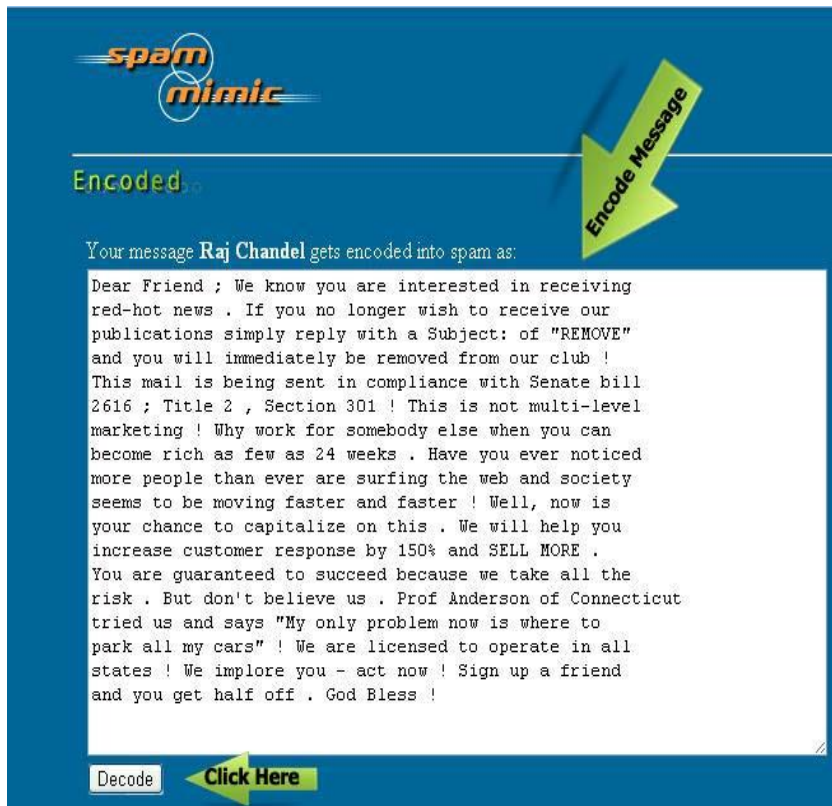
**Free file Camouflage: MUY
SENCILLO DE UTILIZAR Y CON UNA
INTERFAZ MUY AMIGABLE**

ESTEGANOGRAFIA

Es posible utilizar una técnica manual, sin necesidad de herramientas

- 1- Dentro de la carpeta donde están los dos archivos .jpg ingresamos por consola (pepe.jpg y juan.jpg)
- 2- El archivo a ocultar lo comprimimos con RAR y le ponemos de nombre ocultar.rar (ejemplo juan.jpg comprimido = ocultar.rar)
- 3- copy /b juan.jpg+ocultar.rar pruebaocultada.jpg
- 4- A simple vista se verá únicamente la imagen de juan.jpg
- 5- Para ver la otra imagen, debemos renombrar pruebaocultada.jpg a pruebaocultada.rar
- 6- ingresamos y veremos la imagen (juan.jpg)

ESTEGANOGRAFIA



SPAMMIMIC: UNA
DE LAS MEJORES
WEBS, QUE PERMITE
CODIFICAR EL
CONTENIDO DE UN
MAIL, Y A LA VEZ
DESCODIFICARLO
ONLINE, SIN
NECESIDAD DE
PROGRAMA ALGUNO

ESTEGANOGRAFIA

Ocultar un archivo de texto dentro de una imagen, utilizando la tools **STEGHIDE**

Teniendo los 2 archivos (texto e imagen) dentro del mismo directorio ejecutamos:

```
C:\steghide>steghide embed -cf images.jpeg -ef 1.txt
Anotar salvoconducto:
Re-ingresar salvoconducto:
adjuntando "1.txt" en "images.jpeg"... hecho
```

ESTEGANOGRAFIA

Para descubrir el archivo oculto: steghide extract -sf imagen.jpg

Aquí nos pedirá la contraseña que utilizamos al guardarlo

```
C:\steghide>steghide extract -sf images.jpeg
Anotar salvoconducto:
anotó los datos extraídos e/"1.txt".
```

IMPORTANTE: El archivo oculto puede tener cualquier formato, pero el archivo contenedor solo puede ser un “.jpg”, “.bmp”, “.wmv” o “.au”.

Si quisiéramos información sobre el archivo que ocultamos:

```
C:\steghide>steghide info images.jpeg
"images.jpeg":
  formato: jpeg
  capacidad: 355.0 Byte
¿Intenta informarse sobre los datos adjuntos? (s/n) s
Anotar salvoconducto:
  archivo adjunto "1.txt":
    tamaño: 16.0 Byte
    encriptado: rijndael-128, cbc
    compactado: si
```

Tools y pasos necesarios Lab 01 (Steghide)

En Kali:

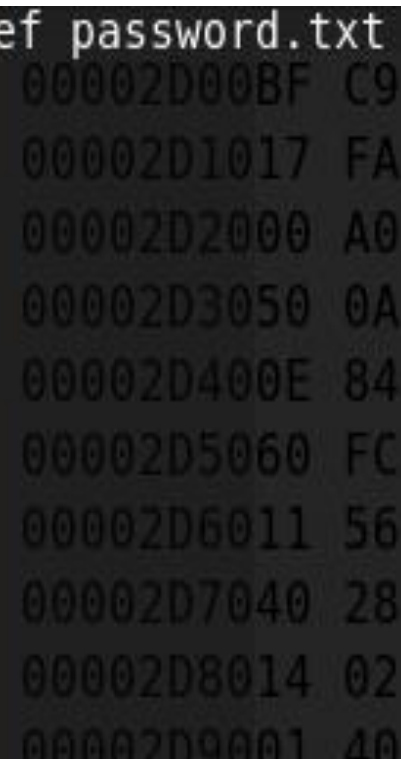
```
apt install steghide  
apt install ghex
```

Pasos:

- 1- Conseguir una imagen
- 2- Realizar una copia de la misma
- 3- La original, cargarla en el GHEX para verificar como termina el hexadecimal y su tamaño
- 4- Crear un archivo de texto llamado password.txt y que su contenido diga: Password PEPE
- 5- Probar: `steghide embed -cf nombrecopiaimagen -ef password.txt`
- 6- Nos pedirá una password para cifrarlo y protegerlo (NO OLVIDARSE CUAL USARAN)
- 7- Comparar los valores de los archivos original y copia y luego cargar el copia en el GHEX
- 8- Verificar como termina el hexadecimal de copia
- 9- Copiarlo a otra carpeta y procedemos a extraer el mensaje secreto:
- 10- `steghide extract -sf nombrecopiaimagen` (nos pedirá el password)
- 11- `cat password.txt`

Tools y pasos necesarios Lab 01 (Steghide)

```
root@kali:~/Desktop# steghide embed -cf index.jpeg -ef password.txt
Enter passphrase:
Re-Enter passphrase:
embedding "password.txt" in "index.jpeg"... done
root@kali:~/Desktop# rm password.txt
root@kali:~/Desktop# steghide extract -sf index.jpeg
Enter passphrase:
wrote extracted data to "password.txt".
root@kali:~/Desktop# ls
'index (copy).jpeg'  index.jpeg  password.txt
root@kali:~/Desktop# cat password.txt
PEPE
```



Tools y pasos necesarios Lab 02 (VeraCrypt)

← → ↻ 🏠 🔒 veracrypt.fr/en/Downloads.html

Home

Source Code

Downloads

Documentation

Donate

Forums

Note to publishers: If you intend to host our files on your server, please instead consider linking to this software is concerned. Thank you.


[Supported versions of operating systems](#)

PGP Public Key: https://www.idrix.fr/VeraCrypt/VeraCrypt_PGP_public_key.asc (ID=0x680D16DE,

Latest Stable Release

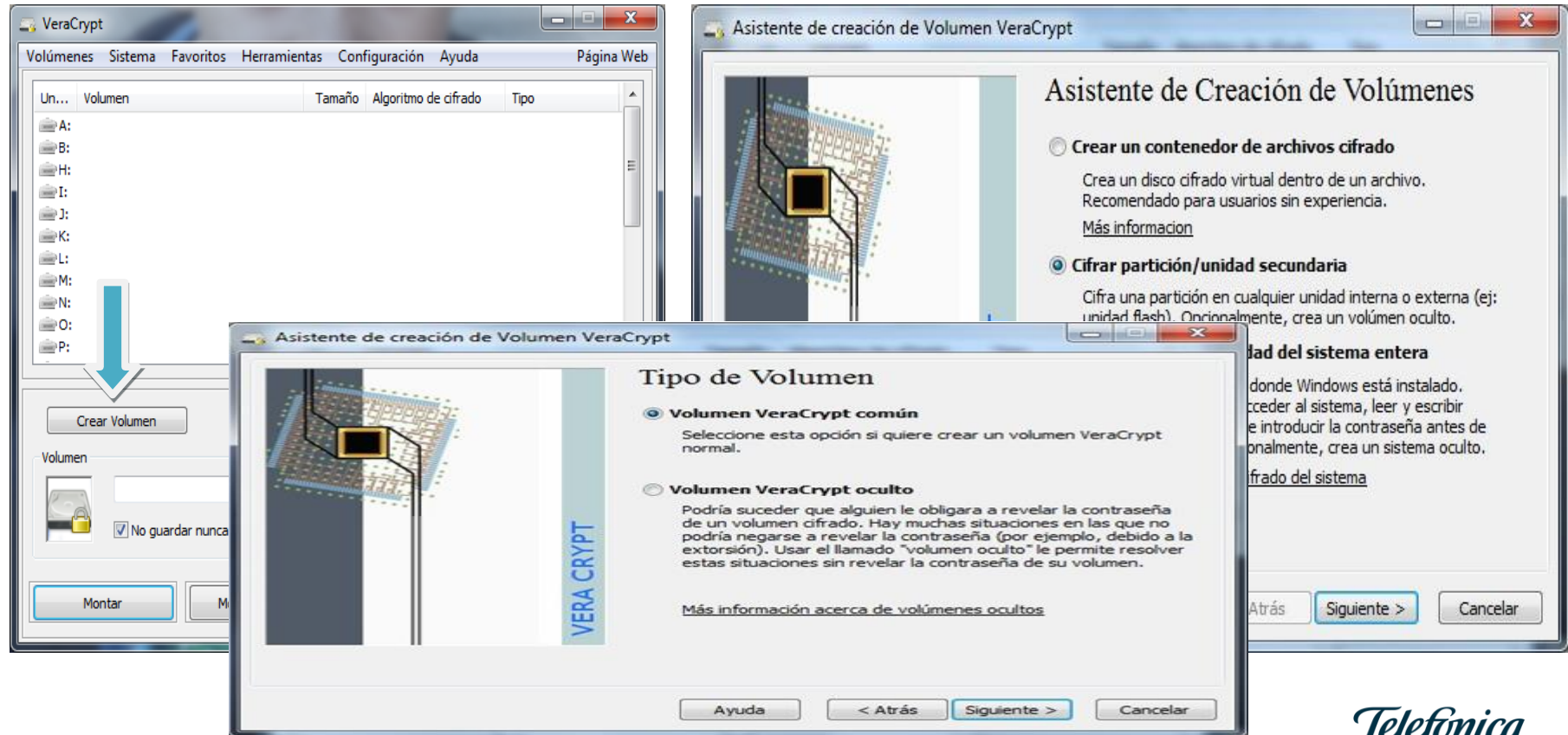
For Windows: 1.23-Hotfix-2 (Monday October 8, 2018)

For FreeBSD, Linux and MacOSX: 1.23 (Wednesday September 12, 2018)

-  **Windows:**
 - Installer: [VeraCrypt Setup 1.23-Hotfix-2.exe \(34.1 MB\)](#) (PGP Signature)
 - Portable version: [VeraCrypt Portable 1.23-Hotfix-2.exe \(34 MB\)](#) (PGP Signature)
 - Source code: [VeraCrypt_1.23-Hotfix-2_Source.zip \(24.1 MB\)](#) (PGP Signature)
 - SHA256 Checksum: [veracrypt-1.23-Hotfix-2-sha256sum.txt](#) (PGP Signature)

Telefonica

Tools y pasos necesarios Lab 02 (VeraCrypt)



Tools y pasos necesarios Lab 02 (VeraCrypt)

Asistente de creación de Volumen VeraCrypt

Ubicación del volumen

▼

Seleccionar Dispositivo

☒ No guardar nunca historial

Los volúmenes VeraCrypt cifrados alojados en dispositivos pueden ser creados en particiones de discos duros, unidades de estado sólido, tarjetas de memoria USB, y en cualquier otro dispositivo de almacenamiento soportado.

Seleccionar Partición o Dispositivo

Dispositivo	Unidad	Tamaño	Etiqueta
Disco Duro 0:		149 GB	
\Device\Harddisk0\Partition 1	C:	93.1 GB	
\Device\Harddisk0\Partition 2	D:	47.1 GB	PROFESORES
Disco extraíble 1:		15.1 GB	
\Device\Harddisk1\Partition 1	G:	15.1 GB	

Asistente de creación de Volumen VeraCrypt

Ubicación del volumen

\Device\Harddisk1\Partition 1 ▼ **Seleccionar Dispositivo**

☒ No guardar nunca historial

Los volúmenes VeraCrypt cifrados alojados en dispositivos pueden ser creados en particiones de discos duros, unidades de estado sólido, tarjetas de memoria USB, y en cualquier otro dispositivo de almacenamiento soportado. Las particiones también pueden ser cifradas conservando datos.

Además, estos volúmenes VeraCrypt pueden ser creados dentro de dispositivos que no contengan ninguna partición (incluyendo discos duros y unidades de estado sólido).

Nota: Un dispositivo que contiene particiones puede ser cifrado por completo conservando datos (usando una única clave) sólo si es la unidad donde Windows está instalado y desde la que arranca.

Ayuda < Atrás Siguiente > Cancelar

VERA CRYPT

Aceptar Cancelar

Tools y pasos necesarios Lab 02 (VeraCrypt)



Tools y pasos necesarios Lab 02 (VeraCrypt)

The image shows the VeraCrypt Volume Creation Wizard with two main windows and a warning dialog box.

Asistente de creación de Volumen VeraCrypt (Left Window):

- Contraseña del Volumen:** Fields for password and confirmation, both masked with dots.
- ☐ Usar archivo-llave (Keyfile button)
- ☐ Mostrar contraseña
- ☐ Use PIM
- Warning Text:** Es muy importante que elija una buena contraseña. Debería evitar elegir una que contenga sólo una palabra que se pueda encontrar en un diccionario (o una combinación de 2, 3, o 4 de estas palabras). No debería contener nombres ni fechas de nacimiento. No debería ser fácil de adivinar. Una buena contraseña es una combinación aleatoria de letras mayúsculas y minúsculas, números, y caracteres especiales como @ ^ = \$ * + etc. Recomendamos la elección de una contraseña

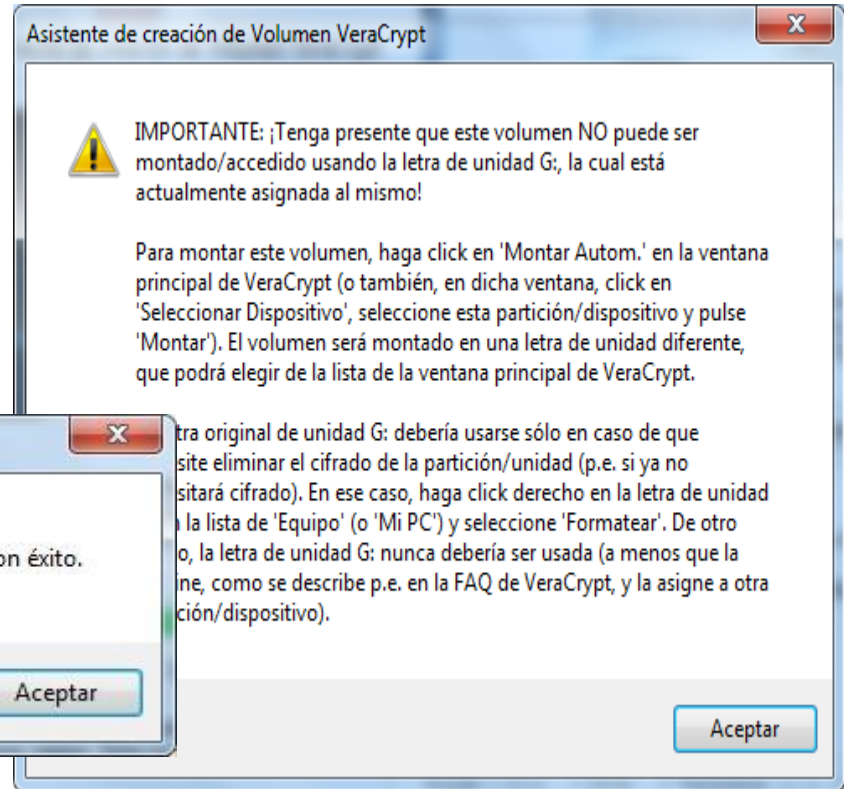
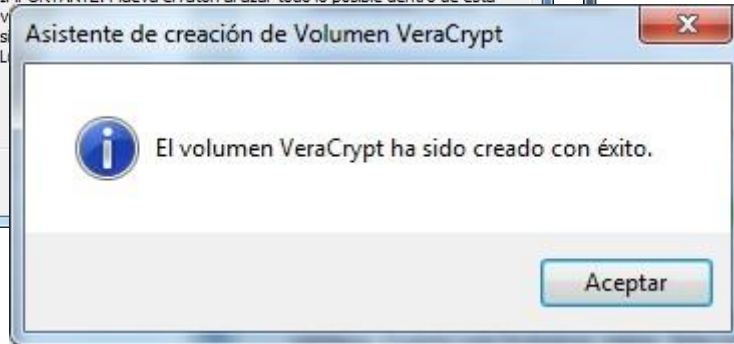
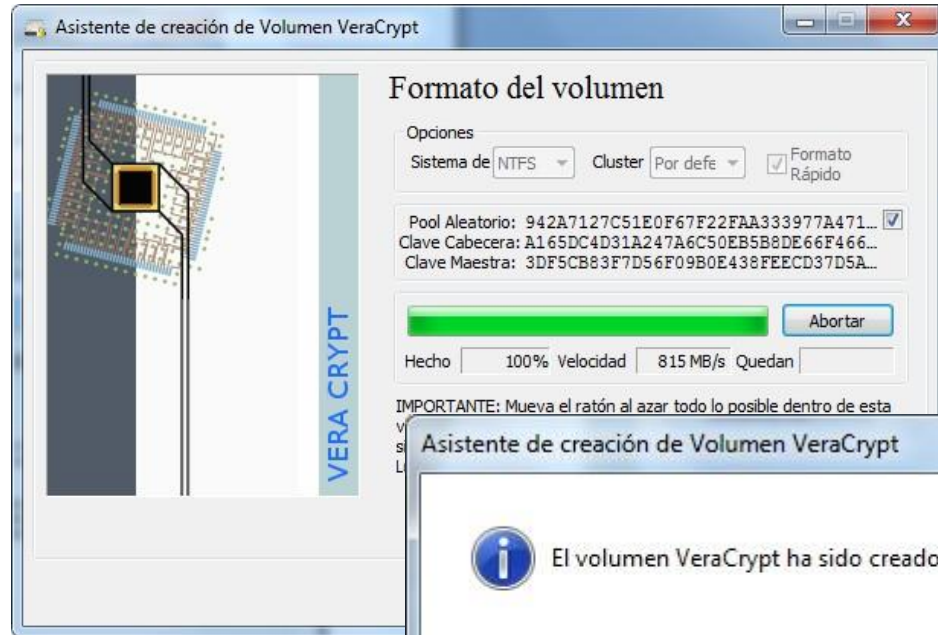
Asistente de creación de Volumen VeraCrypt (Right Window):

- Archivos grandes:** ☒ Sí, ☐ No
- Question:** ¿Tiene intención de almacenar archivos de más de 4 GB en este volumen VeraCrypt?
- Note:** Nota: Dependiendo de su elección, VeraCrypt elegirá un sistema de archivos adecuado para el volumen VeraCrypt (pero lo podrá cambiar en el siguiente paso).
- Buttons:** Ayuda, < Atrás, **Siguiente >**, Cancelar

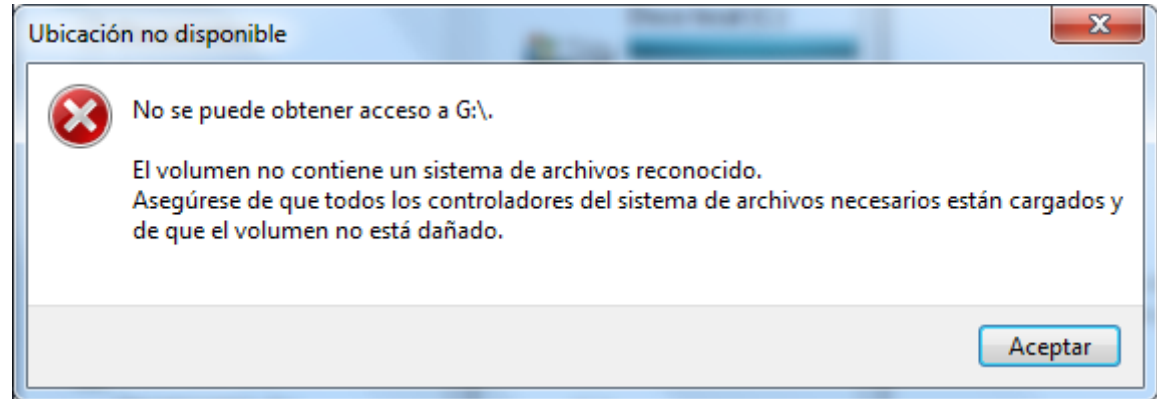
Asistente de creación de Volumen VeraCrypt (Warning Dialog Box):

- Warning Icon:** Yellow triangle with exclamation mark.
- Text:** AVISO: ¡Las contraseñas cortas son fáciles de romper usando técnicas de fuerza bruta!
- Text:** Recomendamos la elección de una contraseña de más de 20 caracteres.
- Text:** ¿Seguro que desea utilizar una contraseña corta?
- Buttons:** **Sí**, **No**

Tools y pasos necesarios Lab 02 (VeraCrypt)

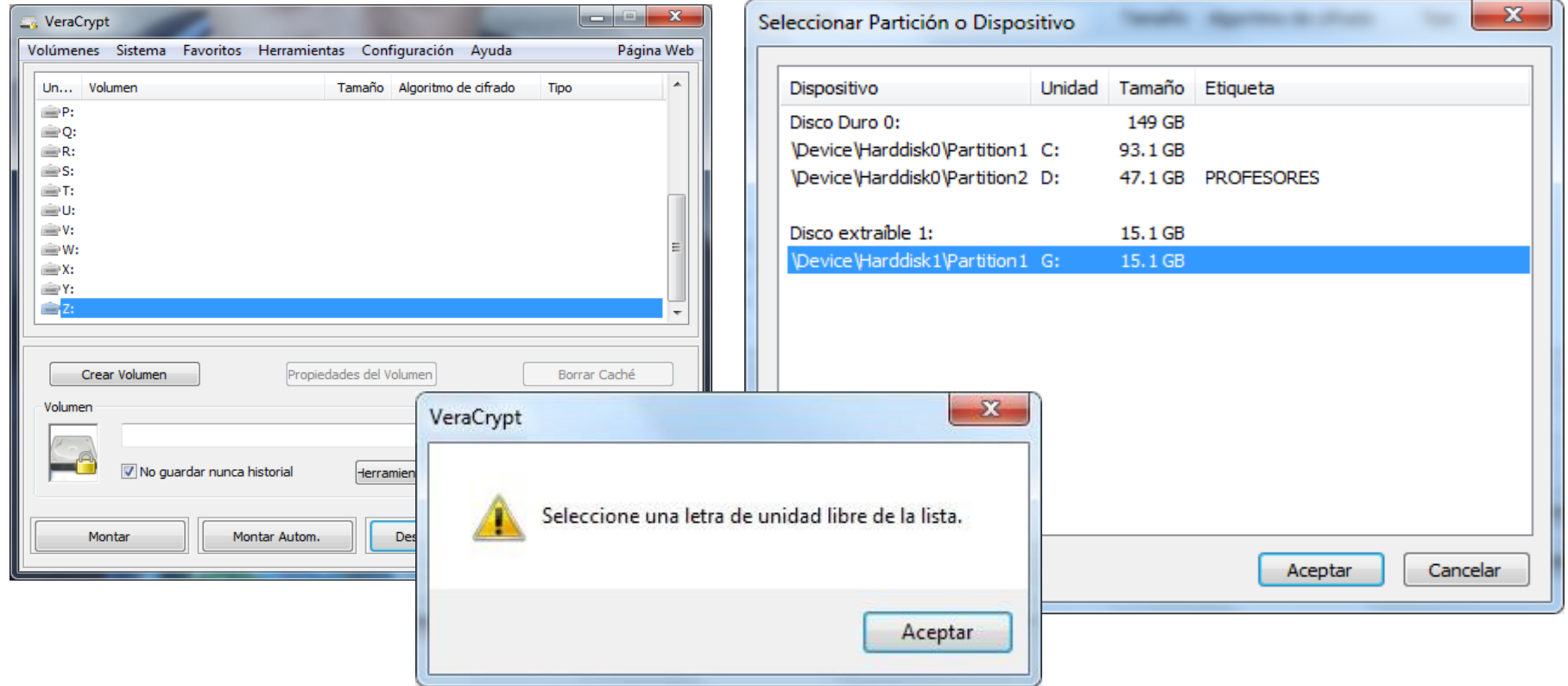


Tools y pasos necesarios Lab 02 (VeraCrypt)

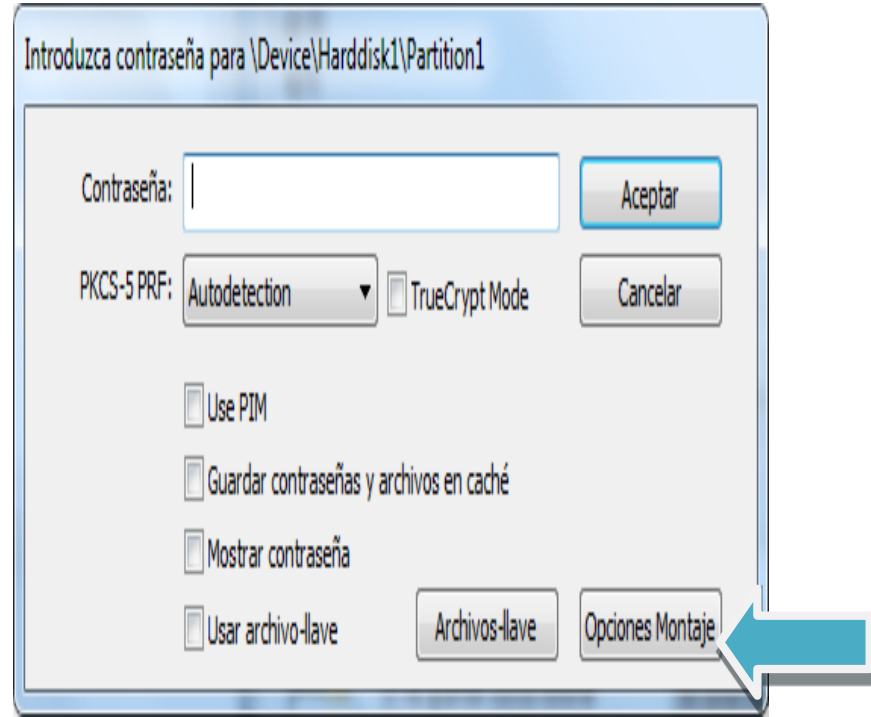
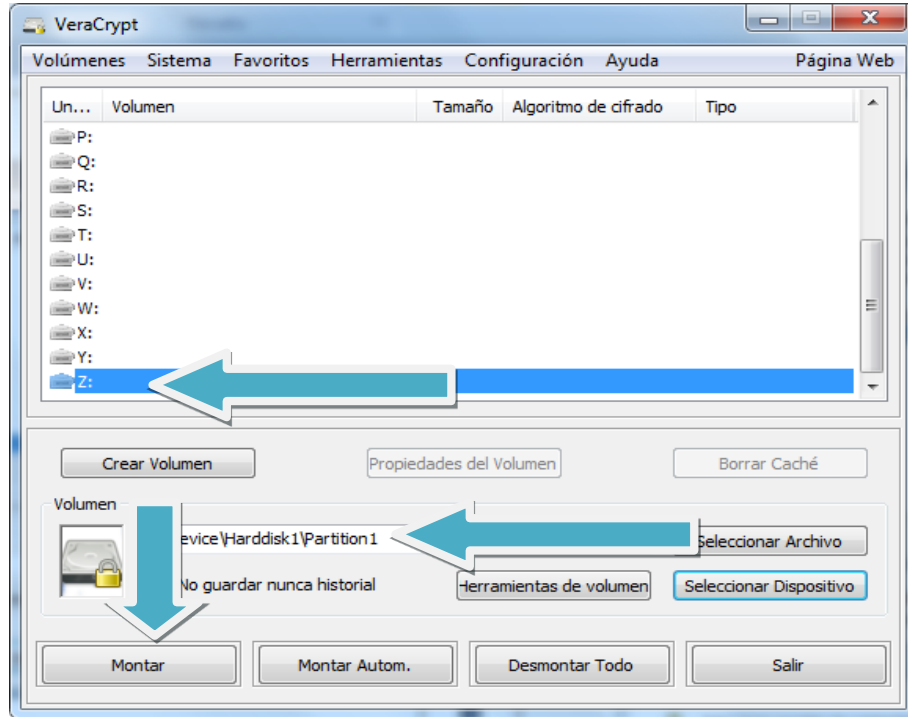


ATENCIÓN: la unidad pedirá ser formateada debido al cifrado, NO HACERLO

Tools y pasos necesarios Lab 02 (VeraCrypt)



Tools y pasos necesarios Lab 02 (VeraCrypt)



Tools y pasos necesarios Lab 02 (VeraCrypt)

VeraCrypt - Opciones de Montaje

☐ Montar volumen como sólo lectura Aceptar

☒ Montar volumen como unidad extraíble Cancelar

☐ Usar copia de seguridad de cabecera insertada en volumen si es posible

☐ Montar partición usando cifrado del sistema sin autenticación de pre-arranque

Volume Label in Windows:

Protección de Volumen Oculto

☐ Proteger volumen oculto contra daños por escritura en el volumen externo

Contraseña volumen oculto:
(vacío para usar caché)

PKCS-5 PRF: Autodetection ▼

☐ Use PIM

☐ Mostrar Contraseña

☐ Usar Archivos-llave Archivos-llave

[¿Que es la protección de volumen oculto?](#)

Introducir Contraseña de Volumen VeraCrypt

Contraseña: Aceptar

PKCS-5 PRF: Autodetection ▼ ☐ TrueCrypt Mode Cancelar

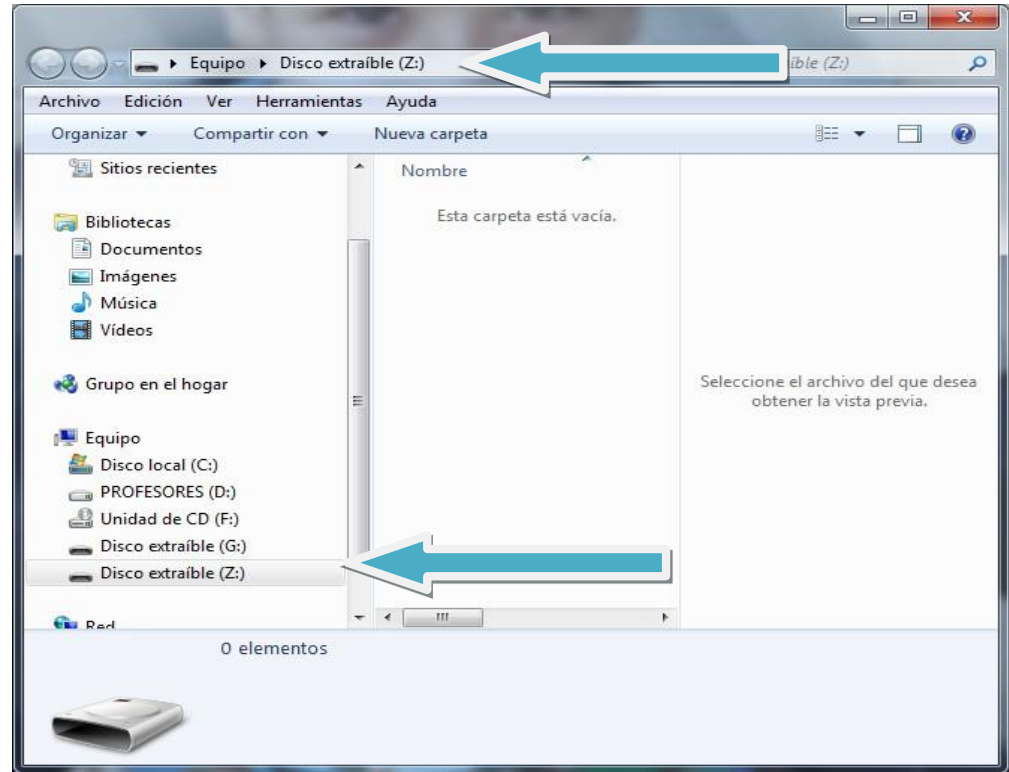
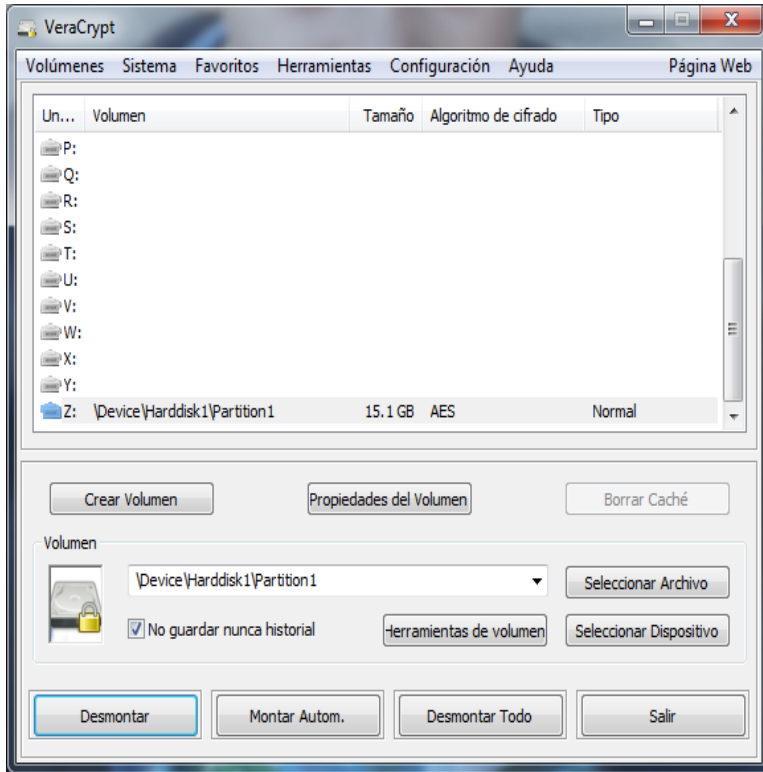
☐ Use PIM

☐ Guardar contraseñas y archivos en caché

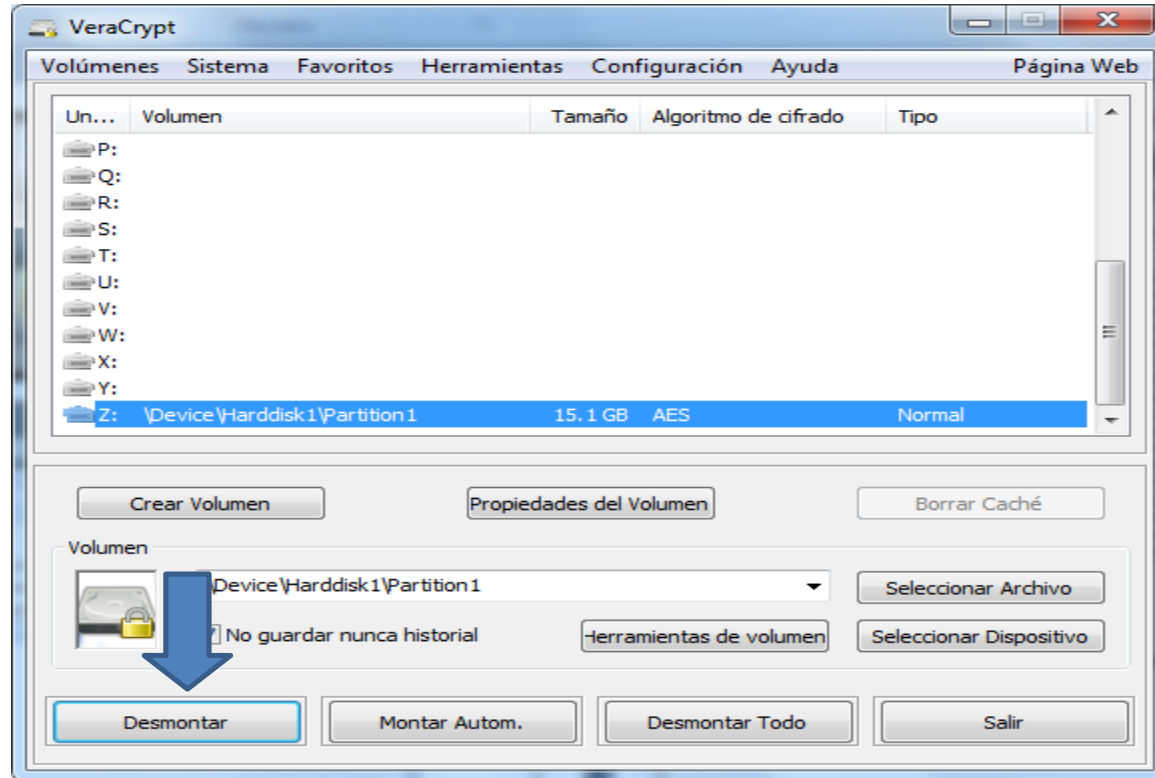
☐ Mostrar contraseña

☐ Usar archivo-llave Archivos-llave Opciones Montaje

Tools y pasos necesarios Lab 02 (VeraCrypt)



Tools y pasos necesarios Lab 02 (VeraCrypt)



Tools y pasos necesarios Lab 03 (Snow)

No es seguro | darkside.com.au/snow/

SNOW exploits the Steganographic Nature Of Whitespace. Locating trailing whitespace in explains the [logo](#)). And it uses the [ICE](#) encryption algorithm, so the name is thematically co

It's free!

As of 16 June 2013, SNOW is available under an Apache 2.0 licece. The usual conditions a to hear about it.

Recent changes

Prior to 22 November 1998 the DOS version, contained in *snowdos.zip*, had a bug affecting could not be decrypted by the other versions, and vice versa. The bug was caused by bit-shi

The source version, when compiled under Unix, also had a bug where it could not read data appended by DOS. This has also been fixed as of 22 November 1998.

- Documentation
 - [How it works](#)
 - [Manual page](#)
 - [About the logo](#)
- Download source
 - [snow-20130616.tar.gz](#) (16210 bytes)
 - [snow.zip](#) (22071 bytes)
- Download DOS/Windows executable
 - 16-bit executable [snwdos16.zip](#) (27001 bytes)
 - 32-bit executable [snwdos32.zip](#) (30961 bytes)

equipo > Documentos >

Nombre

- Archivos de Outlook
- Image-ExifTool-10.94
- Mis archivos de origen de datos
- Plantillas personalizadas de Office
- TagsRevisited
- Virtual Machines
- docu01.txt
- docutrucho.txt
- Lab_Crypto&Steg.pptx
- SNOW.DOC
- SNOW.EXE

Tools y pasos necesarios Lab 03 (Snow)

Pasos:

- 1- Copiamos el SNOW a una carpeta
- 2- Dentro de la misma creamos un archivo de texto con un mensaje (docu01.txt)
- 3- echo "prueba de documento" >> docu01.txt y luego verificamos su contenido con more
- 4- Utilizamos SNOW para poder esconder un mensaje dentro del archivo creado
- 5- snow -C -p password -m "mensajesecreto" docu01.txt docutrucho.txt
- 6- Verificamos con el notepad el archivo creado y el original, lo mismo el tamaño
- 7- Copiamos el archivo docutrucho.txt a otra carpeta y lo abrimos para ver el mensaje
- 8- snow -C -p password docutrucho.txt

Tools y pasos necesarios Lab 04 (OpenPuff)

embeddedsw.net/OpenPuff_Steganography_Home.html



INFO@EMBEDDED SW.NET



+1 949-287-8623



Home

About Us ▾

Security & Software ▾

Hardware & Machinery ▾

Resources ▾

EMBEDDED SW

Delivering Advanced & Reliable Innovation

[HOME](#) > [SOFTWARE](#) > [OPENPUFF STEGANOGRAPHY](#)

OpenPuff - Yet *not* another steganography SW



[Download binary for Windows/Linux](#) / λ [Source Page](#)

λ [Randomness](#) / λ [Video Tutorials & Youtube](#) / λ [For Experts](#)

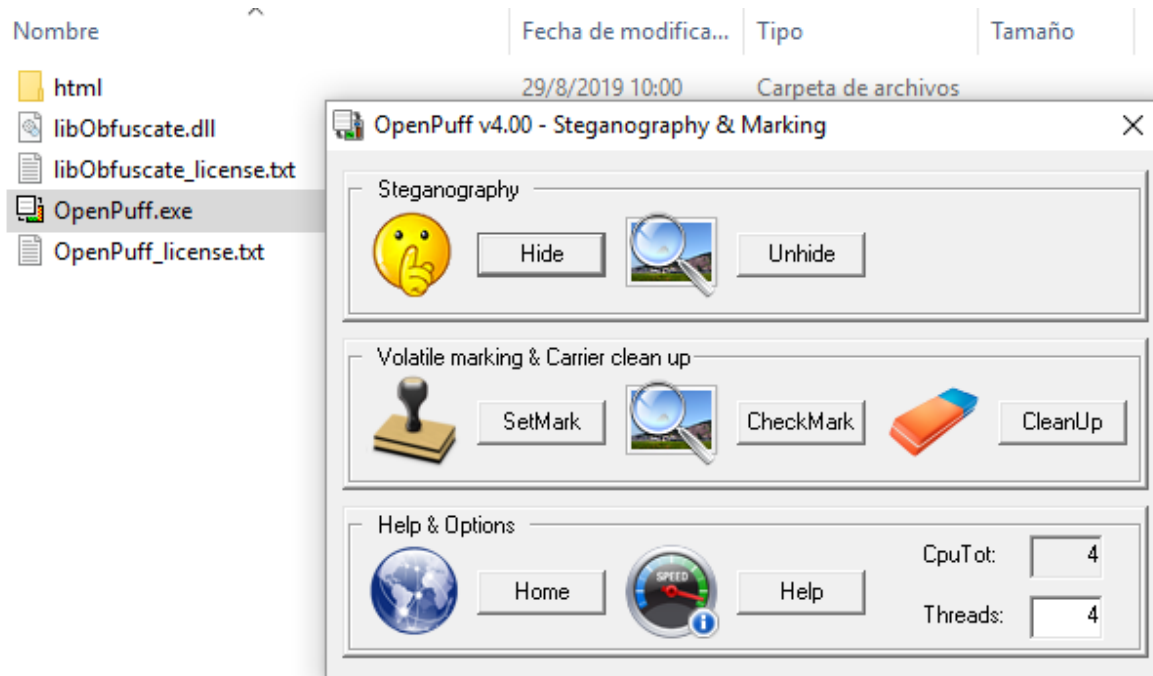
λ [Papers & Articles](#) / λ [Thesis](#) / λ [Lectures](#) / λ [Web Reviews](#)

Telefonica

Tools y pasos necesarios Lab 04 (OpenPuff)

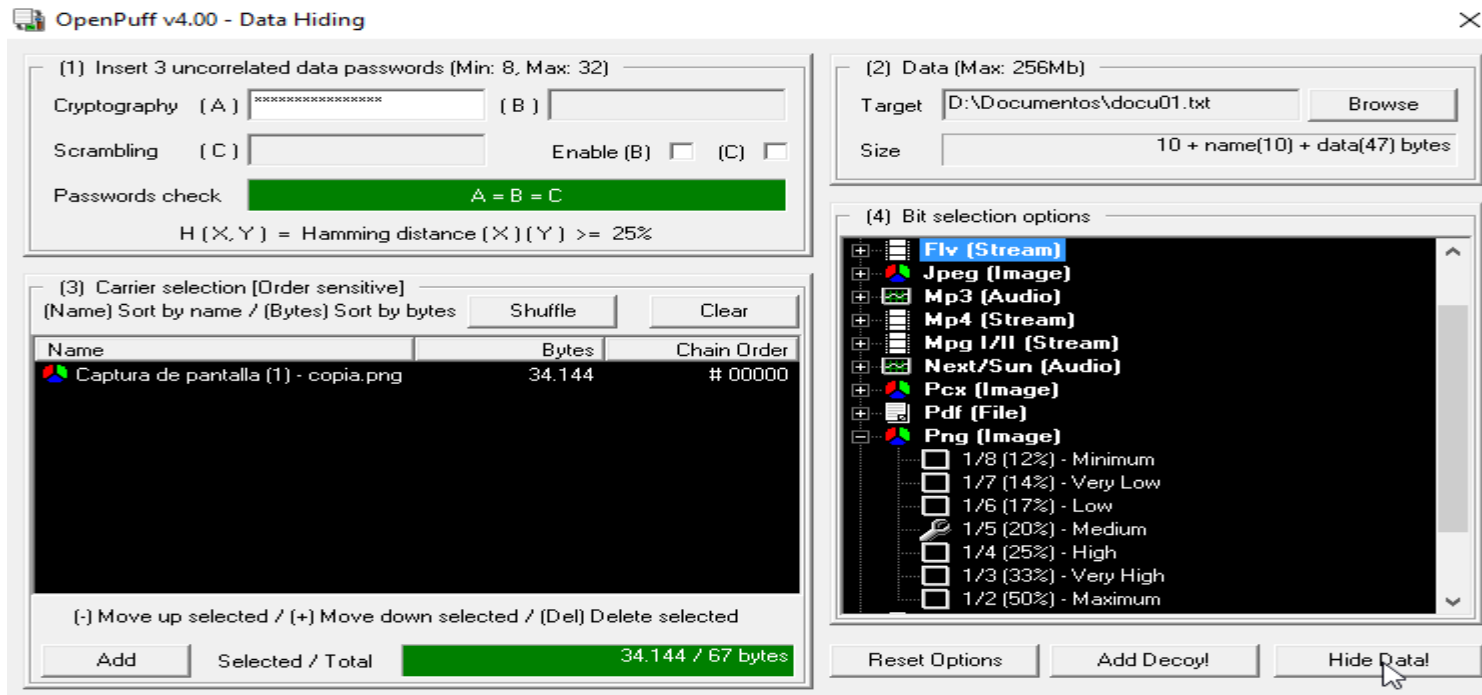
Pasos:

1- Copiamos el OPENPUFF a una carpeta

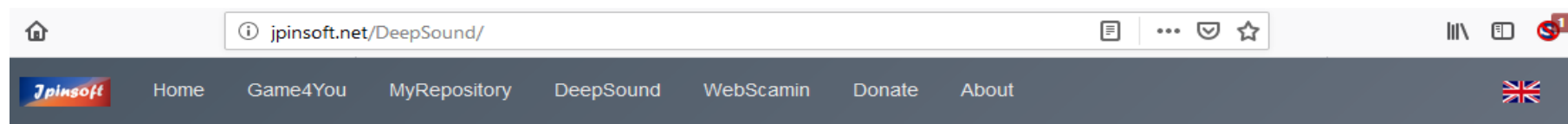


Tools y pasos necesarios Lab 04 (OpenPuff)

- 1- Usamos una clave (desclickeamos las demás opciones)
- 2- Seleccionamos el archivo a ocultar
- 3- Seleccionamos el archivo donde queremos esconder los datos
- 4- Ejecutamos Hide Data



Tools y pasos necesarios Lab 05 (DeepSound)



Overview

[Download](#)

[Documentation](#)

DeepSound overview

DeepSound is a steganography tool and audio converter that hides secret data into audio files. The application also enables you to extract secret files directly from audio files or audio CD tracks.

DeepSound might be used as copyright marking software for wave, flac, wma, ape, and audio CD. DeepSound also support encrypting secret files using AES-256(Advanced Encryption Standard) to improve data protection.

The application additionally contains an easy to use Audio Converter Module that can encode several audio formats (FLAC, MP3, WMA, WAV, APE) to others (FLAC, MP3, WAV, APE).




Tools y pasos necesarios Lab 05 (DeepSound)

DeepSound 2.0

Hide Data Inside Audio Audio Converter Settings Help




Open carrier files Add secret files Encode secret files Extract secret files

Carrier audio files ;

	File	Dir	Size (MB)
	APE ape	D:\Audio	22.4 MB
	FLAC.flac	D:\Audio	25.9 MB
	WMA.wma	D:\Audio	21.4 MB

Secret files in D:\Audio\WMA.wma:

Output audio file quality ☐ Low ☒ Normal ☐ High Free space for secret files : 7.8 MB

	Secret file name	Size (MB)
	D:\SecretFiles\SecretFile1.pdf	3.4 MB
	D:\SecretFiles\SecretFile2.doc	0.2 MB
	D:\SecretFiles\SecretFile3.jpg	< 0.1 MB

Output directory : [C:\Users\Jospin\Documents\](C:\Users\Jospin\Documents) [Donate](#)

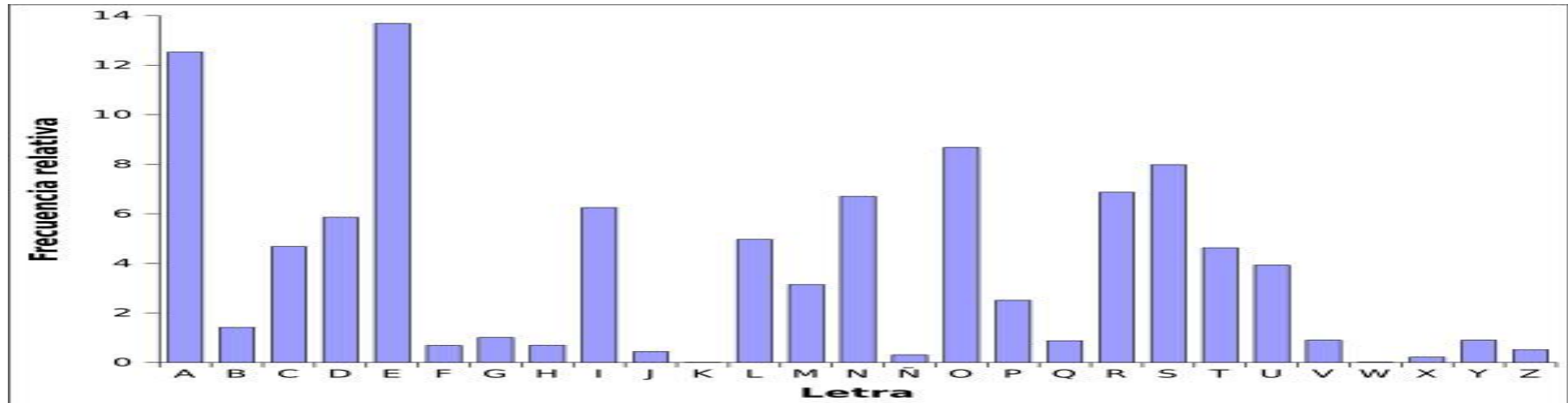
Tools y pasos necesarios Lab 06 (Criptografía Cesar)

Sabiendo que el siguiente texto cifrado:

“iwxsiwyqiniptohigmjvhspsqseojefixsxmtsgiw ev”

se ha obtenido, deben descifrarlo teniendo en cuenta la siguiente tabla de frecuencias característica del español:

E = 15% A = 13% O = 9% L = 8% S = 8% N = 7%



Telefónica



Telefónica
