

SEGURIDAD EN SISTEMAS OPERATIVOS

4º Grado en Informática – Complementos de Ing. del Software
Curso 2017-18

Práctica [1]. Administración de la seguridad en Linux

Sesión [6]. Cifrado de sistemas de archivos. Esteganografía y estegoanálisis.

Autor¹: Rubén Calvo Villazán

Ejercicio 1.

Encriptar un dispositivo USB:

Buscamos el dispositivo con `fdisk -l`, en este caso es `/dev/sdb1`

```
Device      Boot Start      End  Sectors  Size Id Type
/dev/sdb1   *      2048 30297215 30295168 14.5G  c W95 FAT32 (LBA)
root@valkyrie:~# cryptsetup -c aes -h sha256 -y -s 256 luksFormat /dev/sd
b1

WARNING!
=====
This will overwrite data on /dev/sdb1 irrevocably.

Are you sure? (Type uppercase yes): YES
Enter passphrase:
Verify passphrase:
root@valkyrie:~# █
```

Escribimos la orden con `cryptsetup` y le indicamos la contraseña para montar el dispositivo.

Luego creamos un sistema de archivos en un dispositivo mapeado test, en este caso `/dev/mapper/test`

1 Como autor declaro que los contenidos del presente documento son originales y elaborados por mi. De no cumplir con este compromiso, soy consciente de que, de acuerdo con la “Normativa de evaluación y de calificaciones de los estudiantes de la Universidad de Granada” esto “conllevará la calificación numérica de cero ... independientemente del resto de calificaciones que el estudiante hubiera obtenido ...”

Posteriormente creamos un directorio prueba en /mnt, le damos permisos 777 y montamos el dispositivo mapeado:

```
root@valkyrie:~# cryptsetup luksOpen /dev/sdb1 test
Enter passphrase for /dev/sdb1:
root@valkyrie:~# mkfs /dev/mapper/test
mke2fs 1.43.7 (16-Oct-2017)
Creating filesystem with 3786384 4k blocks and 948416 inodes
Filesystem UUID: f117e43b-7e81-4442-9595-5e5b366a2c71
Superblock backups stored on blocks:
    32768, 98304, 163840, 229376, 294912, 819200, 884736, 1605632, 26
54208

Allocating group tables: done
Writing inode tables: done
Writing superblocks and filesystem accounting information: done

root@valkyrie:~# mkdir /mnt/prueba
root@valkyrie:~# chmod 777 /mnt/prueba
root@valkyrie:~# mount /dev/mapper/test /mnt/prueba
root@valkyrie:~#
```

Desmontamos el dispositivo mapeado y cerramos cryptsetup:

```
root@valkyrie:~# umount /dev/mapper/test
root@valkyrie:~# cryptsetup luksClose /dev/mapper/test
```

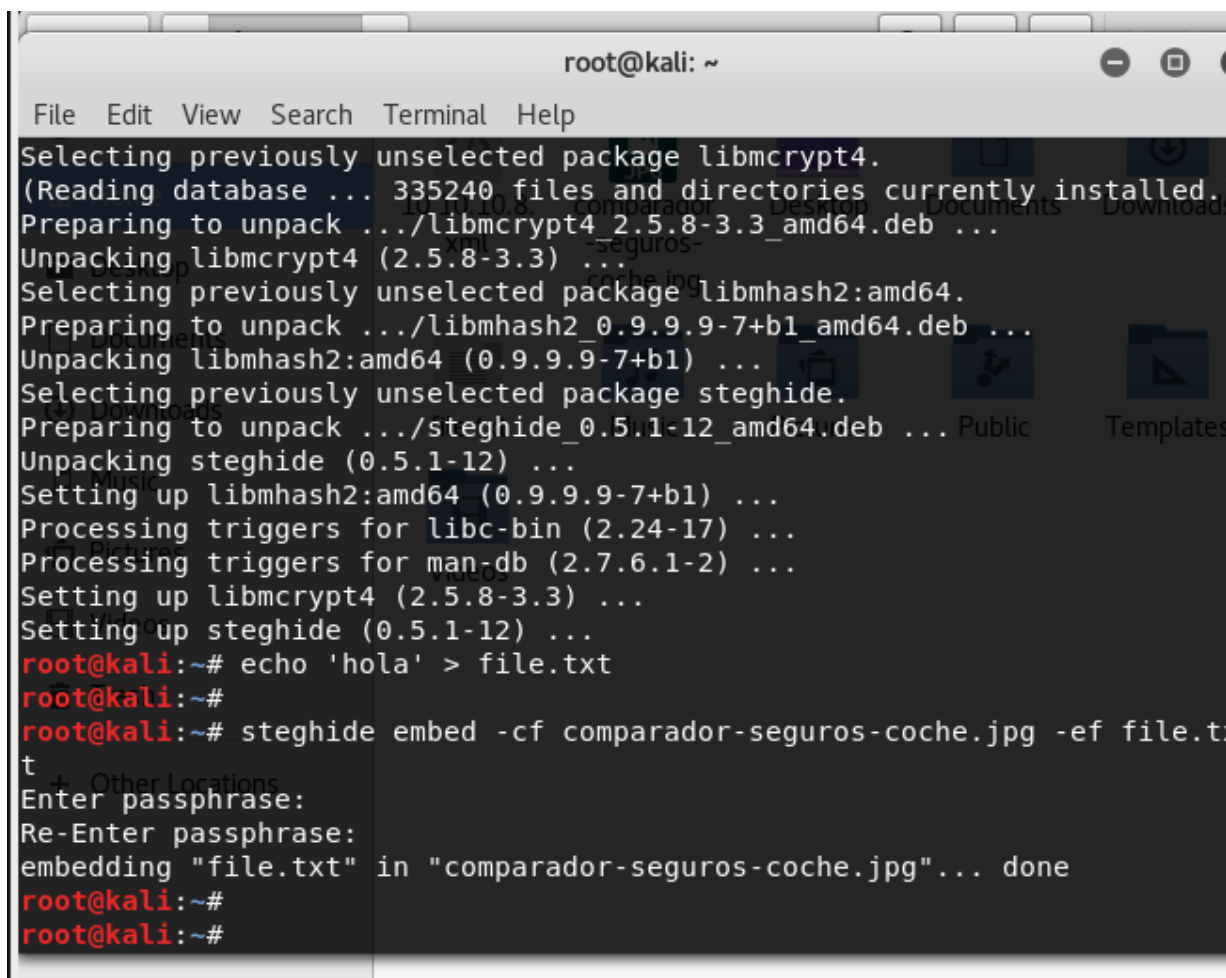
Retiramos el dispositivo.

Finalmente, cada vez que queramos montar el dispositivo nos pedirá la contraseña



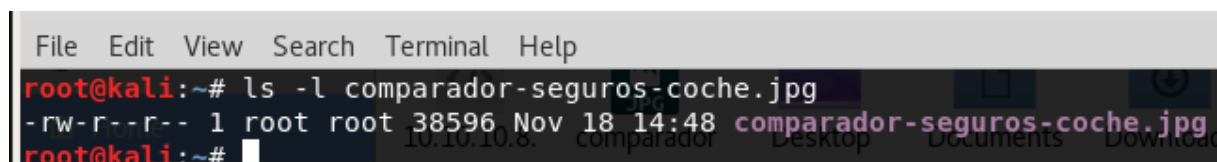
Ejercicio 2.

Instalamos steghide si no lo está.



```
root@kali: ~  
File Edit View Search Terminal Help  
Selecting previously unselected package libmcrypt4.  
(Reading database ... 335240 files and directories currently installed.)  
Preparing to unpack .../libmcrypt4_2.5.8-3.3_amd64.deb ...  
Unpacking libmcrypt4 (2.5.8-3.3) ...  
Selecting previously unselected package libmhash2:amd64.  
Preparing to unpack .../libmhash2_0.9.9.9-7+b1_amd64.deb ...  
Unpacking libmhash2:amd64 (0.9.9.9-7+b1) ...  
Selecting previously unselected package steghide.  
Preparing to unpack .../steghide_0.5.1-12_amd64.deb ...  
Unpacking steghide (0.5.1-12) ...  
Setting up libmhash2:amd64 (0.9.9.9-7+b1) ...  
Processing triggers for libc-bin (2.24-17) ...  
Processing triggers for man-db (2.7.6.1-2) ...  
Setting up libmcrypt4 (2.5.8-3.3) ...  
Setting up steghide (0.5.1-12) ...  
root@kali:~# echo 'hola' > file.txt  
root@kali:~#  
root@kali:~# steghide embed -cf comparador-seguros-coche.jpg -ef file.txt  
Enter passphrase:  
Re-Enter passphrase:  
embedding "file.txt" in "comparador-seguros-coche.jpg"... done  
root@kali:~#  
root@kali:~#
```

Escondemos el fichero de texto en la imagen

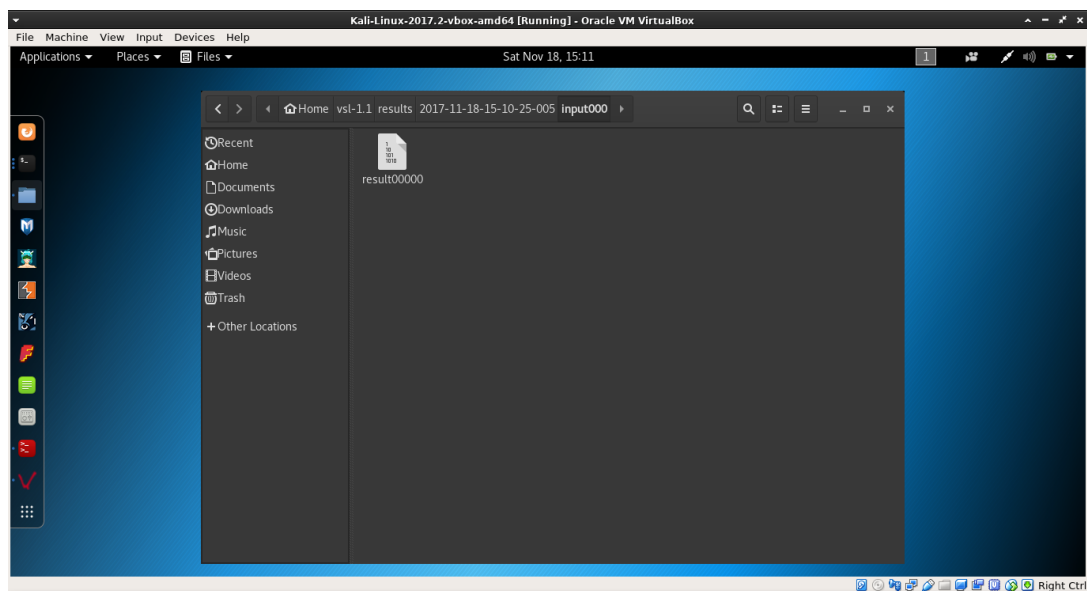
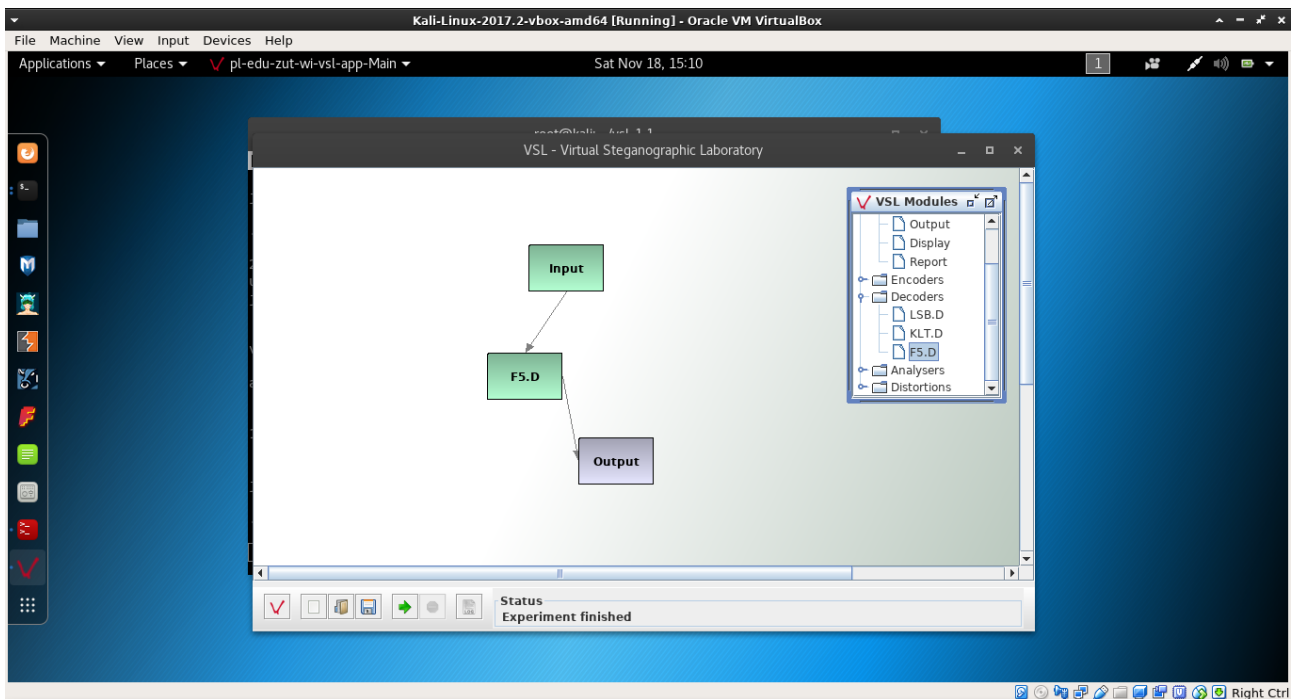


```
File Edit View Search Terminal Help  
root@kali:~# ls -l comparador-seguros-coche.jpg  
-rw-r--r-- 1 root root 38596 Nov 18 14:48 comparador-seguros-coche.jpg  
root@kali:~#
```

Ejercicio 3.

Analizamos la imagen con VSL:

Usamos el decodificador F5.D



Vemos que recuperamos el fichero de texto que previamente habíamos escondido.