



I.E.S Jacarandá

Despliegue de Aplicaciones Web

Memoria de Prácticas: Servidor Web con HTTPS

Profesor: Manuel García Blanca
Rodríguez

Autora: Nadia Lia Correa Morales

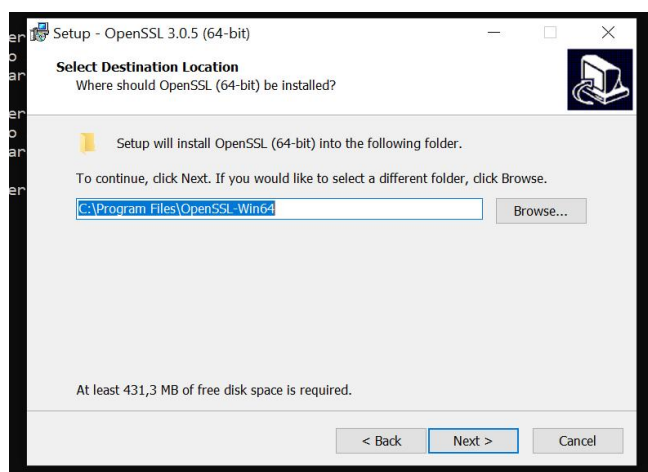
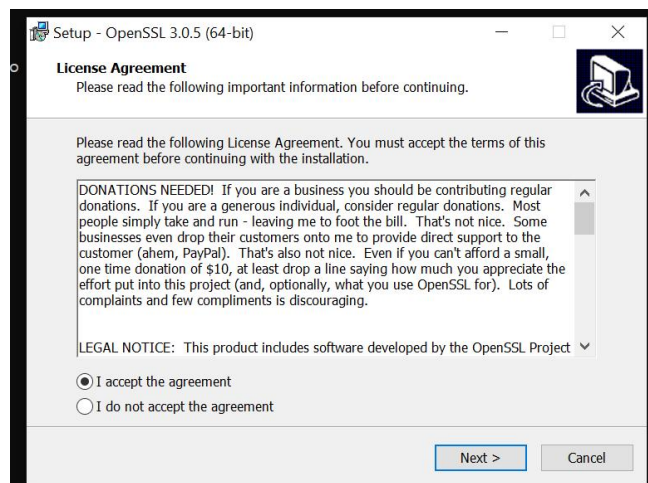
2DAW

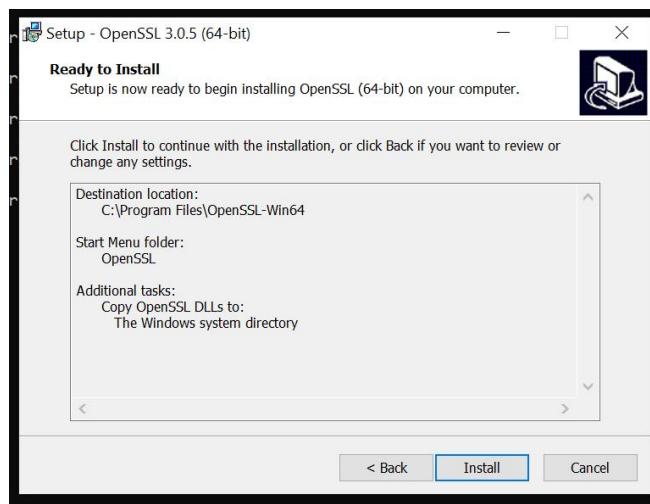
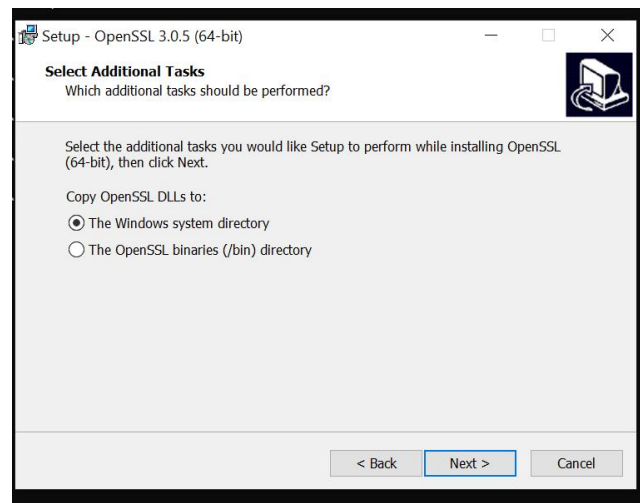
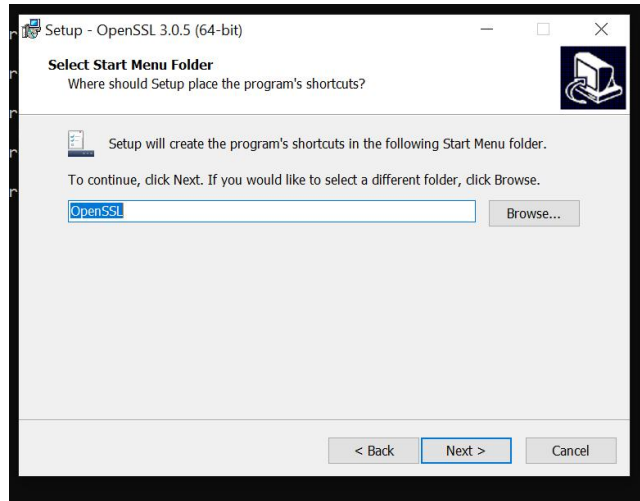
Memoria de prácticas Servidor Web (https)

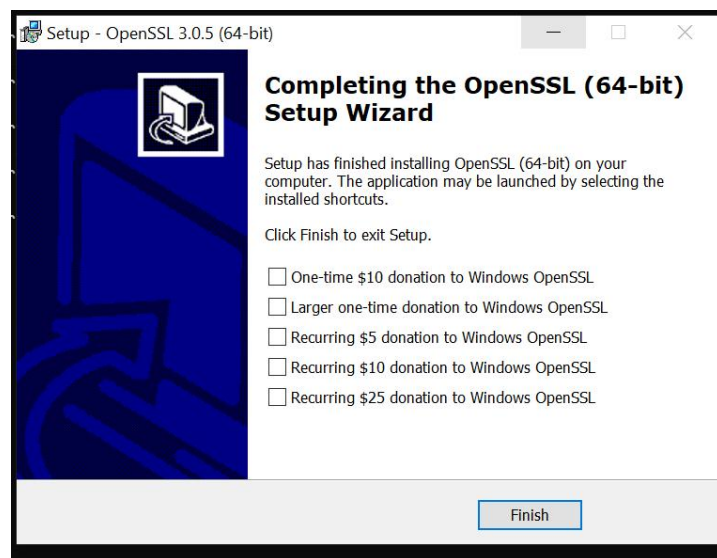
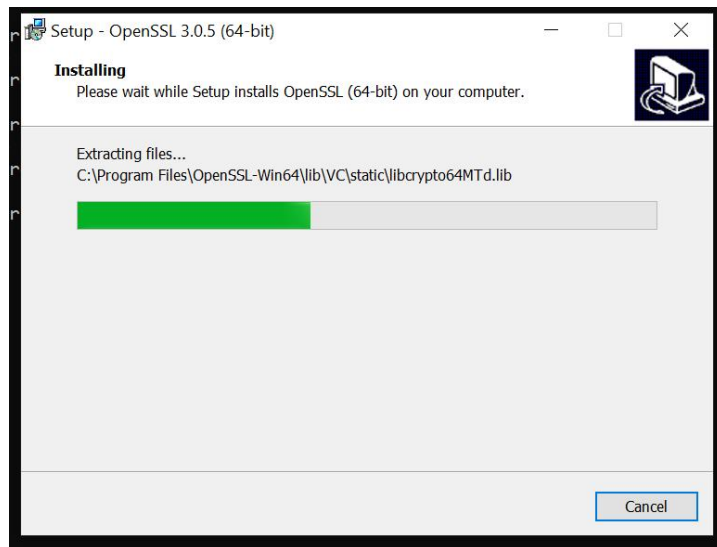
1. Descargar OPENSSL disponible en <https://slproweb.com/products/Win32OpenSSL.html>

Download Win32/Win64 OpenSSL		
Download Win32/Win64 OpenSSL today using the links below!		
File	Type	Description
Win64 OpenSSL v3.0.5 Light EXE MSI	5MB Installer	Installs the most commonly used essentials of Win64 OpenSSL v3.0.5 (Recommended for users by the creators of OpenSSL). Only installs on 64-bit versions of Windows. Note that this is a default build of OpenSSL and is subject to local and state laws. More information can be found in the legal agreement of the installation.
Win64 OpenSSL v3.0.5 EXE MSI	140MB Installer	Installs Win64 OpenSSL v3.0.5 (Recommended for software developers by the creators of OpenSSL). Only installs on 64-bit versions of Windows. Note that this is a default build of OpenSSL and is subject to local and state laws. More information can be found in the legal agreement of the installation.

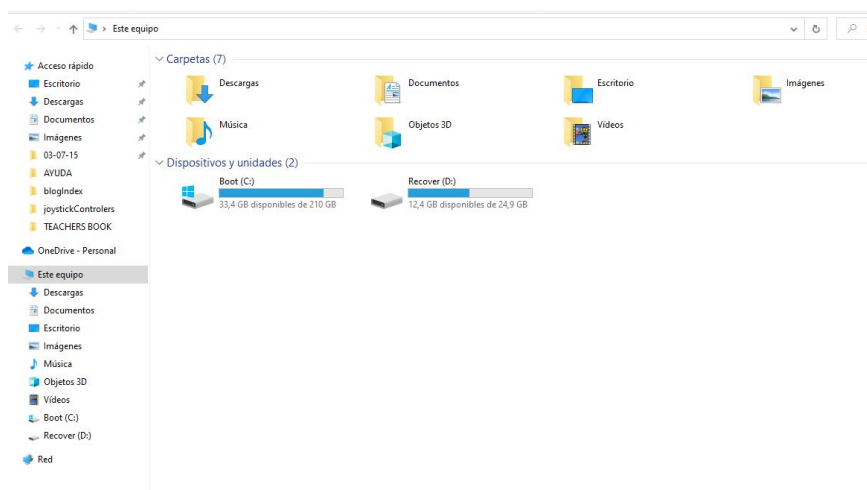
2. Ejecutar el EXE descargado y seguir los pasos de instalación por defecto



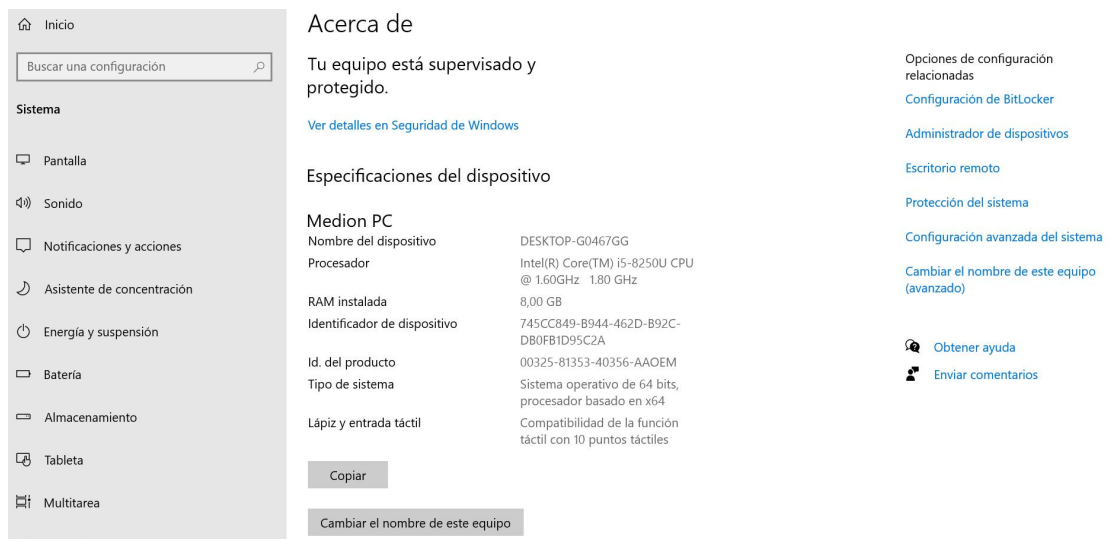




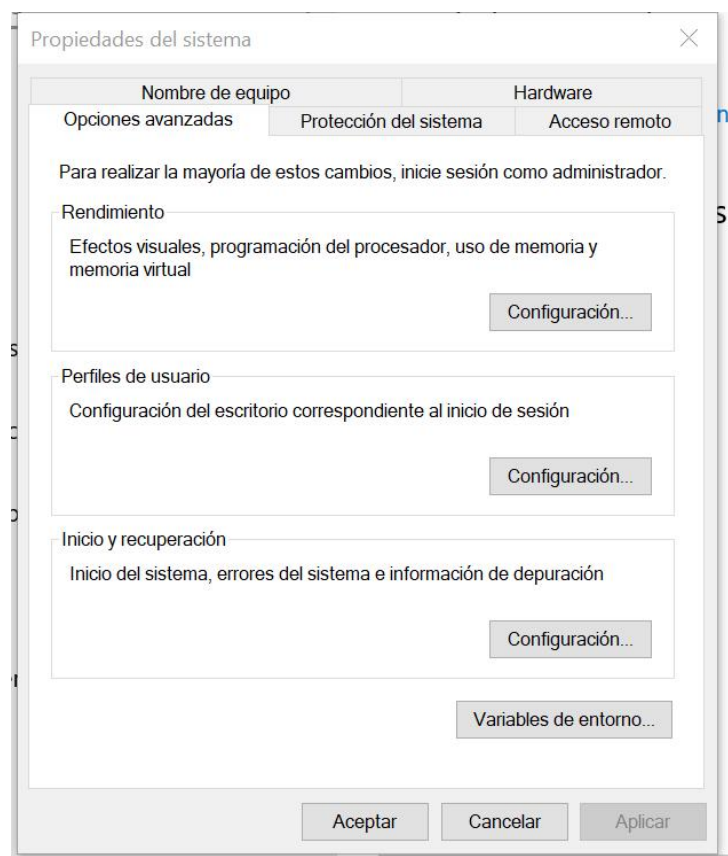
3. Una vez instalado OPENSSL hay que cambiar una variable de entorno en la configuración de Windows. Para ello ve a equipo da click derecho y selecciona propiedades



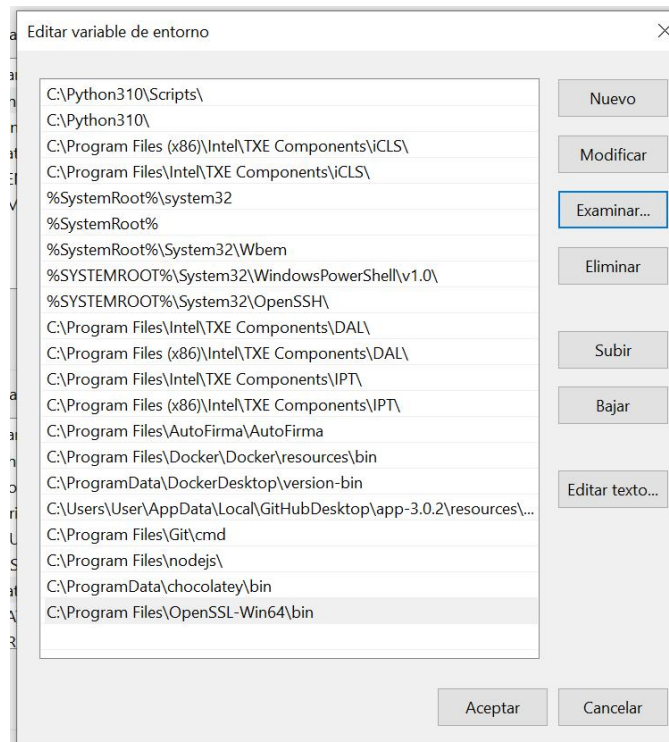
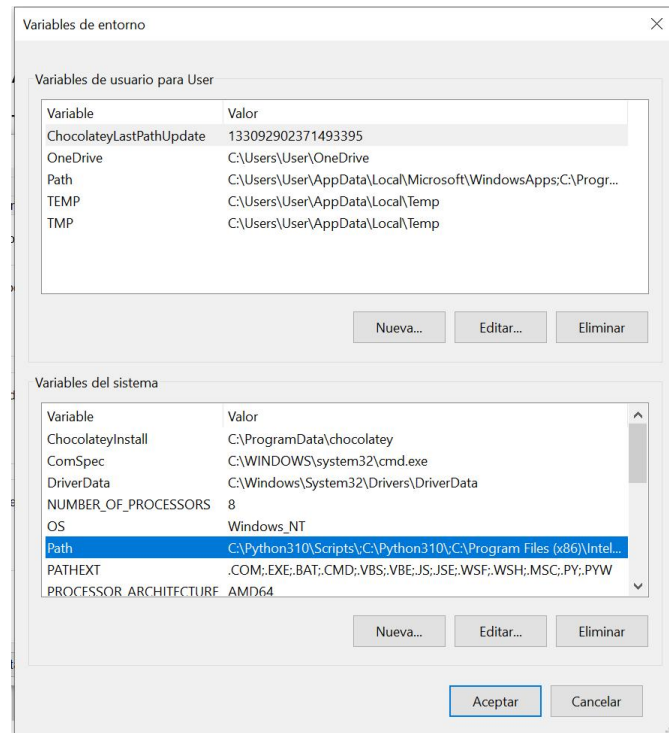
4. Selecciona configuración avanzada



5. Da click en variables de entorno



6. Doble click en path para añadir OPENSSL como variable de entorno. Para añadirla debes dar click en examinar y seleccionar la carpeta bin. Luego da click en aceptar.



7. Para comprobar que la instalación y la configuración de la variable de entorno esté correcta escribimos openssl version en el CMD

```
Microsoft Windows [Versión 10.0.19044.2130]
(c) Microsoft Corporation. Todos los derechos reservados.

C:\Users\User>openssl version
OpenSSL 3.0.5 5 Jul 2022 (Library: OpenSSL 3.0.5 5 Jul 2022)

C:\Users\User>
```

8. Ahora que ya tenemos el OPENSSL tenemos que generar un certificado crt y una clave key para poder agregar HTTPS a una app web (este certificado funciona para pruebas locales o para cuando necesitas HTTPS para pasar la seguridad del navegador, pero no para un sitio web ya que ese tipo de certificados son de pago y se consiguen por medio del proveedor de hosting)
- 9.
10. Para generar la clave key ejecutamos el comando

```
openssl genrsa -out C:\Users\User\Desktop\clave.key 2048
```

```
C:\Users\User>openssl genrsa -out C:\Users\User\Desktop\clave.key 2048

C:\Users\User>
```

11. Para generar el certificado ejecutamos el siguiente comando en el que incluiremos la clave key, la ruta donde se guardará el certificado y el número de días de validez.
- ```
openssl req -new -x509 -sha256 -key C:\Users\User\Desktop\clave.key -out C:\Users\User\Desktop\certificado.crt -days 365
```
12. Se te pedirán algunos datos como el código del país, provincia, localidad, nombre de la organización, etc. Completa los datos solicitados.

```
C:\Users\User>openssl req -new -x509 -sha256 -key C:\Users\User\Desktop\clave.key -out C:\Users\User\Desktop\certificado.crt -days 365
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.

Country Name (2 letter code) [AU]:SP
State or Province Name (full name) [Some-State]:Se
Locality Name (eg, city) []:Seville
Organization Name (eg, company) [Internet Widgits Pty Ltd]:NadiaC
Organizational Unit Name (eg, section) []:NONE
Common Name (e.g. server FQDN or YOUR name) []:NadiaC
Email Address []:ncormor536@gmail.com
```



13. Ahora para personalizar la configuración hay que obtener la configuración por defecto del servidor ejecutando el siguiente comando

```
$ docker run --rm httpd:2.4 cat /usr/local/apache2/conf/httpd.conf > my-httpd.conf
```

```
C:\Users\User\Desktop\2DAW\DESPLIEGUE\pruebaWeb>docker run --rm httpd:2.4 cat /usr/local/apache2/conf/httpd.conf > my-httpd.conf
```

14. Obtén el archivo de configuración https ejecutando el siguiente comando

```
$ docker run --rm httpd:2.4 cat /usr/local/apache2/conf/extra/httpd-ssl.conf > my-httpd-ssl.conf
```

```
C:\Users\User>docker run --rm httpd:2.4 cat /usr/local/apache2/conf/extra/httpd-ssl.conf > my-httpd-ssl.conf
```

15. Obtén el archivo mime.type ejecutando el comando

```
$ docker run --rm httpd:2.4 cat /usr/local/apache2/conf/mime.types > my-mime.types
```

```
C:\Users\User\Desktop\2DAW\DESPLIEGUE\httpsServer>docker run --rm httpd:2.4 cat /usr/local/apache2/conf/mime.types > my-mime.types
```

16. Crea las carpetas para replicar el orden en el que se distribuyen en el contenedor para guardar los archivos obtenidos. Hay que cambiarle el nombre a los archivos para que se correspondan con los del contenedor. Guarda el archivo my-mime.types con el nombre de mime.types y el archivo my-httpd.conf con el nombre httpd.conf en la carpeta de conf, añade una carpeta llamada extra en la guardes my-httpd-ssl.conf con el nombre httpd-ssl.conf. Por último guarda la clave y el certificado en la carpeta conf.

Escritorio > 2DAW > DESPLIEGUE > httpsServer > conf

| Nombre

extra  
httpd.conf  
mime.types  
server.crt  
server.key



17. En el documento httpd.conf debes descomentar (eliminar el símbolo #) de las siguientes líneas:

```
...
#LoadModule socache_shmcb_module modules/mod_socache_shmcb.so
...
#LoadModule ssl_module modules/mod_ssl.so
...
#Include conf/extra/httpd-ssl.conf
...
```

18. Una vez hayas cambiado las configuraciones ejecuta

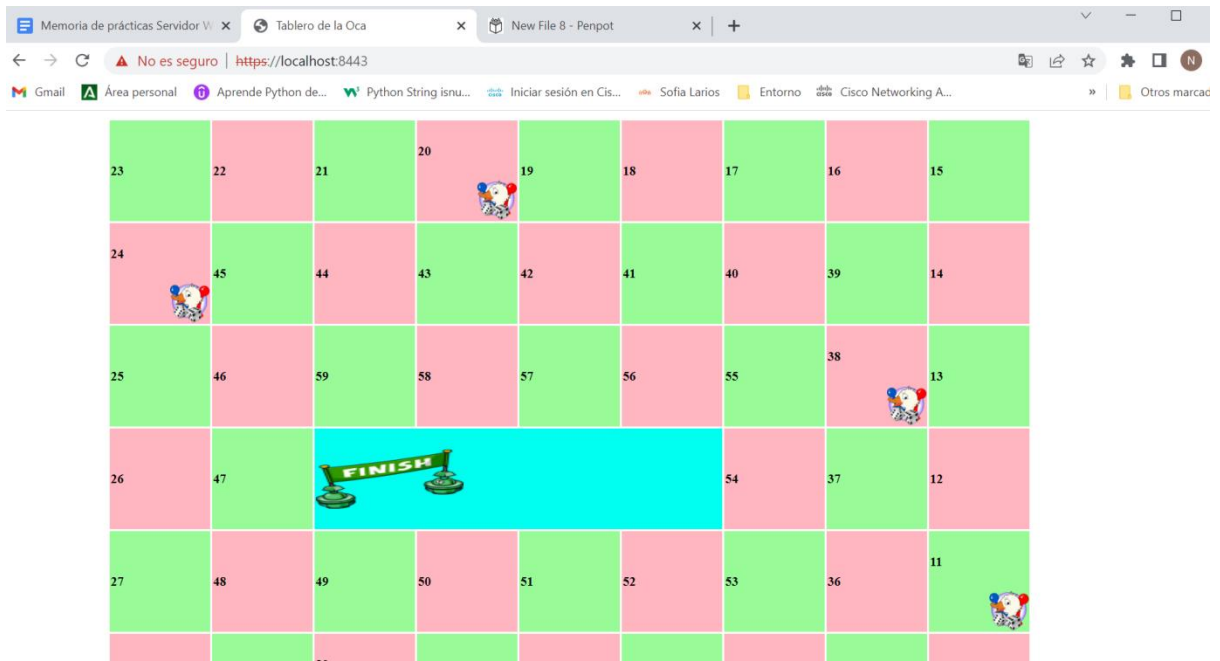
```
$ docker run -dit --name apachehttps -p 8080:80 -p 8443:443 -
v %cd%/docs:/usr/local/apache2/htdocs/ -v %cd%/conf:/usr/local/apache2/conf/
httpd:2.4
```

19. Para ver que el servidor está levantado ejecuta

```
$ docker ps -a
```

| CONTAINER ID | IMAGE         | COMMAND            | CREATED        | STATUS                    | PORTS                                       |
|--------------|---------------|--------------------|----------------|---------------------------|---------------------------------------------|
| a56ae9e03f70 | httpd:2.4     | "httpd-foreground" | 19 minutes ago | Up 50 seconds             | 0.0.0.0:8080->80/tcp, 0.0.0.0:8443->443/tcp |
| apachehttps  | httpd:2.4     | "httpd-foreground" | 4 days ago     | Exited (0) 31 minutes ago |                                             |
| 5c813742ee55 | my-apache-app |                    |                |                           |                                             |

20. Para comprobar que funciona accede a https://localhost:8443



## **Bibliografia**

What is SSL:

<https://www.websecurity.digicert.com/es/es/security-topics/what-is-ssl-tls-https>

How to install OPENSSL:

<https://www.youtube.com/watch?v=jSkQ27sTto0>

Download OPENSSL

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

Generar crt y key para HTTPS

<https://parzibyte.me/blog/2020/01/02/openssl-windows-generar-crt-key-https/>