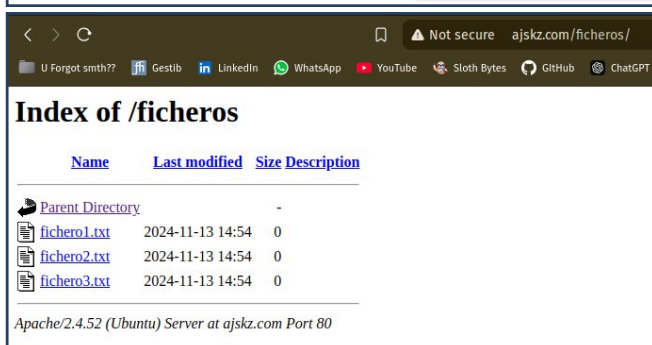
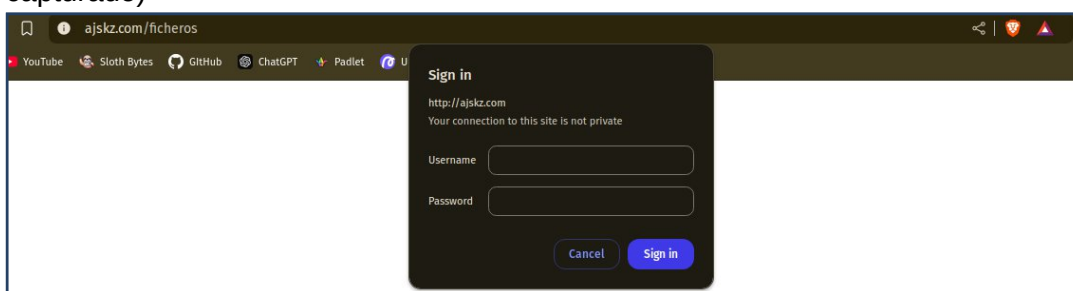


## Práctica 5. HTTPS

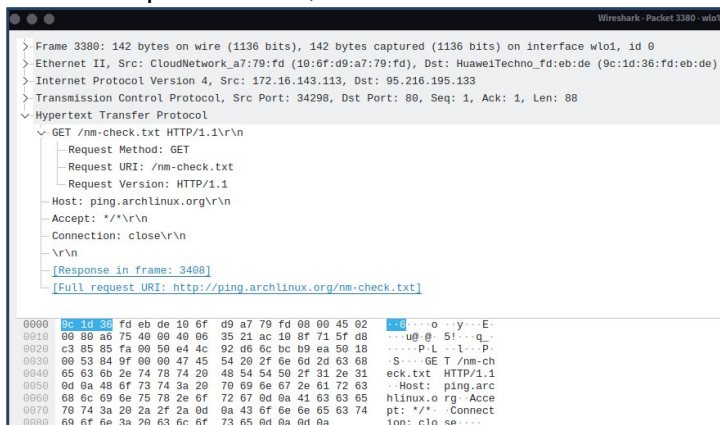
Lee detenidamente cada uno de los puntos antes de realizar las tareas solicitadas.

1. Abre wireshark y empieza a capturar tráfico. Abre un navegador y accede a [www.sitio1.com/ficheros](http://www.sitio1.com/ficheros) e introduce las credenciales de un usuario con acceso. Dirígite al Wireshark y detén la captura de tráfico. Filtra por HTTP. Busca una trama con la siguiente información: **GET /ficheros/ HTTP/1.1** (Captura de página personal creada previamente, "sitio1", con solicitud de login del navegador. Captura del contenido del archivo "ficheros" creado previamente y captura de imagen del trafico capturado)



No.	Time	Source	Destination	Protocol	Length	Info
3380	18.235735782	172.16.143.113	95.216.195.133	HTTP	142	GET /nm-check.txt HTTP/1.1

2. Inspecciona la trama en los apquetes capturados de HTTP y obtén las credenciales de acceso. (Captura de los datos de Hypertext Transfer Protocol del paquete localizado previamente, mostrando información sobre autenticación de usuario).



```
aj@apache:/etc/apache2/sites-available$ sudo openssl genpkey -algorithm RSA -pkeyopt rsa_keygen_bits:2048 -out ajskz.key
```

Ver apartado **Recursos** para más información.

```

aj@apache:/etc/apache2/sites-available$ ls -l
total 28
-rw-r--r-- 1 root root 1332 dic 4 2023 000-default.conf
-rw-r--r-- 1 root root 500 nov 13 15:34 ajskz.conf
-rw-r--r-- 1 root root 1245 nov 25 19:57 ajskz.crt
-rw-r--r-- 1 root root 1704 nov 25 19:49 ajskz.key
-rw-r--r-- 1 root root 237 nov 7 18:22 ajsvt.conf
-rw-r--r-- 1 root root 6338 dic 4 2023 default-ssl.conf

```

4. Activa el módulo HTTPS y haz un restart. (Captura de sudo a2enmod para activar el modulo de ssl y su resultado, y posterior reinicio de apache)

```

aj@apache:/etc/apache2/sites-available$ sudo a2enmod ssl
Considering dependency setenvif for ssl:
Module setenvif already enabled
Considering dependency mime for ssl:
Module mime already enabled
Considering dependency socache_shmcb for ssl:
Enabling module socache_shmcb.
Enabling module ssl.
See /usr/share/doc/apache2/README.Debian.gz on how to configure SSL and create self-signed certificates.
To activate the new configuration, you need to run:
systemctl restart apache2
aj@apache:/etc/apache2/sites-available$ sudo systemctl restart apache2

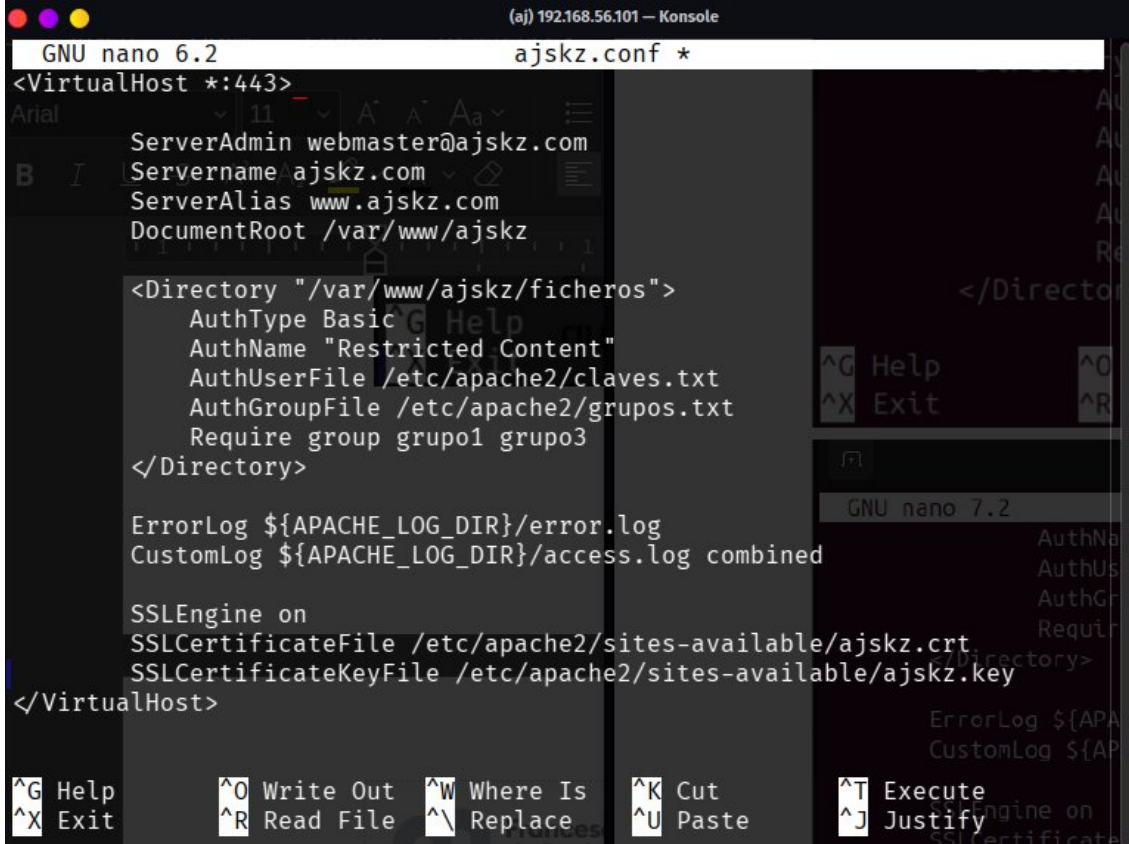
```

5. Copia el fichero de plantilla de SSL “default-ssl.conf” en sitio1.conf. **¡OJO!** RECUERDA COPIAR ANTES EL “DIRECTORY” CON LOS PERMISOS A SITIO1/FICHEROS CONFIGURADOS EN LA PRACTICA 4. Modifica el fichero sitio1.conf para que sitio1 se conecte por HTTPS con la clave y el certificado que antes hemos creado. Añade el directory con la configuración de usuarios y grupos. Luego guarda los cambios. (Captura de sitio1.conf donde se vea un nuevo Directory con la configuración de conexión vía SSL según el fichero copiado, junto con la configuración de prácticas anteriores)

```

aj@apache:/etc/apache2/sites-available$ sudo cp ajskz.conf ajcopia.conf
[sudo] password for aj:
aj@apache:/etc/apache2/sites-available$ ls
000-default.conf ajcopia.conf ajskz.conf ajskz.crt ajskz.key ajsvt.conf default-ssl.conf
aj@apache:/etc/apache2/sites-available$ sudo cp default-ssl.conf default-sslcopia.conf
aj@apache:/etc/apache2/sites-available$ ls
000-default.conf ajcopia.conf ajskz.conf ajskz.crt ajskz.key ajsvt.conf default-ssl.conf default-sslcopia.conf

```



```

GNU nano 6.2 ajskz.conf *
<VirtualHost *:443>
    ServerAdmin webmaster@ajskz.com
    ServerName ajskz.com
    ServerAlias www.ajskz.com
    DocumentRoot /var/www/ajskz

    <Directory "/var/www/ajskz/ficheros">
        AuthType Basic
        AuthName "Restricted Content"
        AuthUserFile /etc/apache2/claves.txt
        AuthGroupFile /etc/apache2/grupos.txt
        Require group grupo1 grupo3
    </Directory>

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

    SSLEngine on
    SSLCertificateFile /etc/apache2/sites-available/ajskz.crt
    SSLCertificateKeyFile /etc/apache2/sites-available/ajskz.key
</VirtualHost>

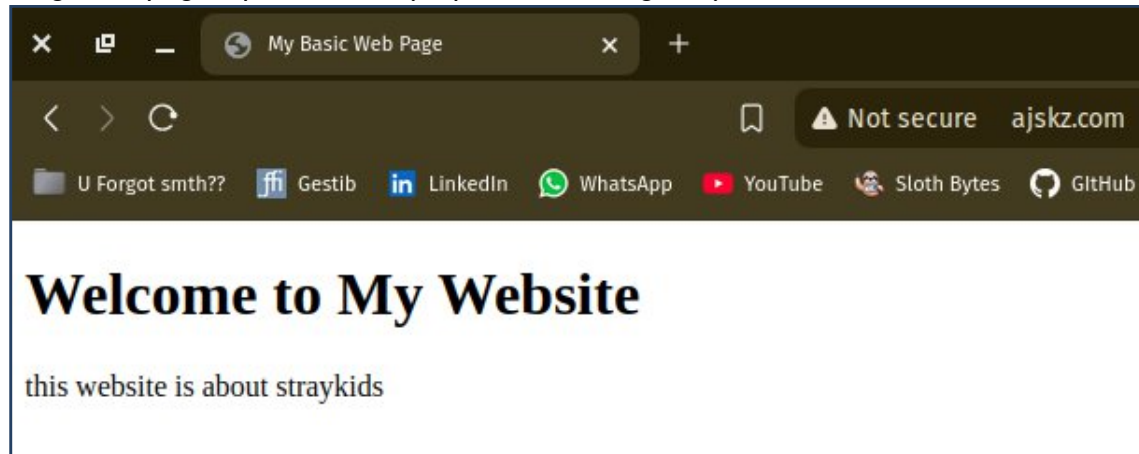
```



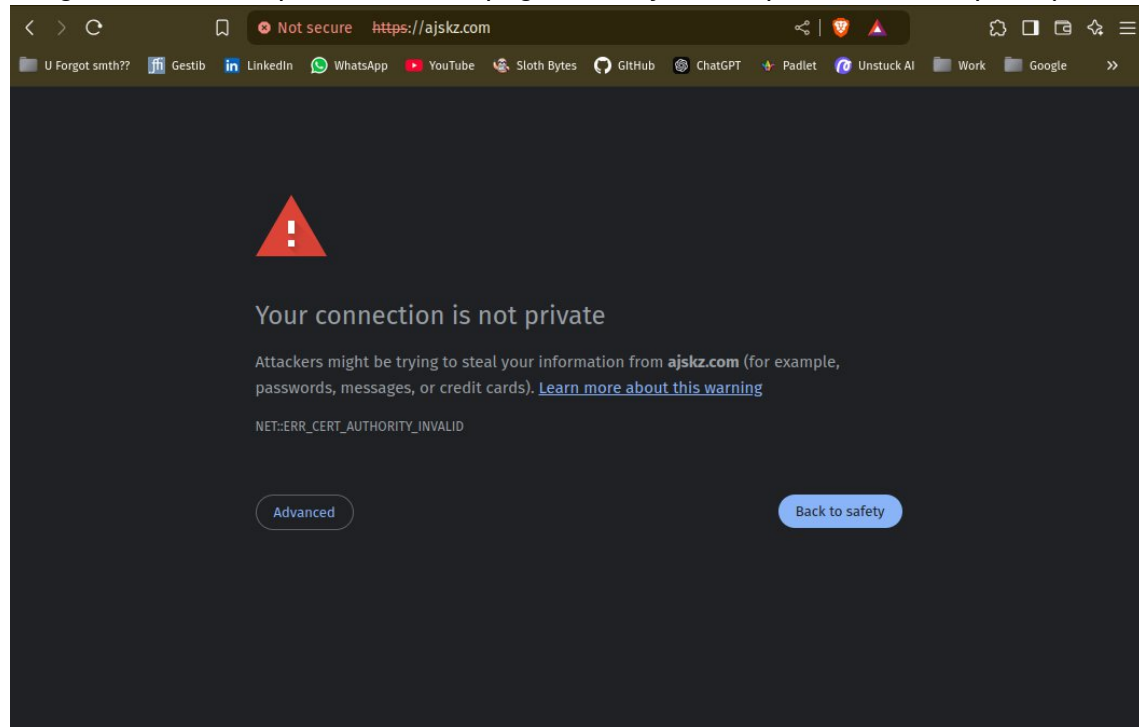
6. Comprueba la sintaxis y realiza un reload. (Captura del comando `apache2ctl -t` y un reload)

```
aj@apache:/etc/apache2/sites-available$ sudo apache2ctl -t
AH00558: apache2: Could not reliably determine the server's fully qualified domain name, using 127.0.1.1. Set the 'ServerName' directive globally to suppress this message
Syntax OK
aj@apache:/etc/apache2/sites-available$ sudo systemctl reload apache2
Unknown command verb reload.
aj@apache:/etc/apache2/sites-available$ sudo systemctl reload apache2
```

7. Abre un nuevo navegador y dirígete a `http://www.sitio1.com` y comprueba si ahora te dirige a la página por defecto. (Captura del navegador)

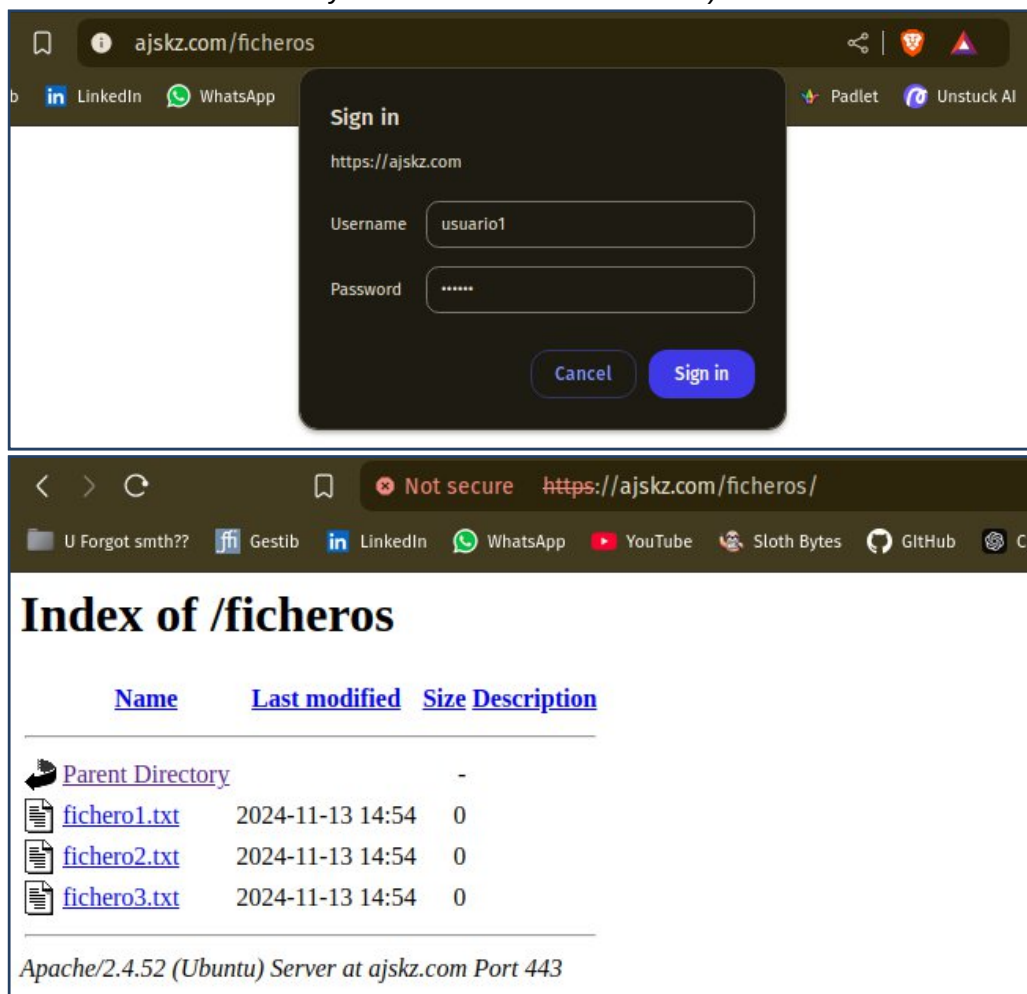


8. Dirígete ahora a **`https://www.sitio1.com`**. y comprueba que vuelve a salir la página que creamos en su momento. Comprueba que accedes mediante https. (Captura del navegador accediendo a la web creada vía https, Si el navegador te solicita “aceptar riesgos adicionales” para entrar a la página, incluye las capturas de estos pasos)

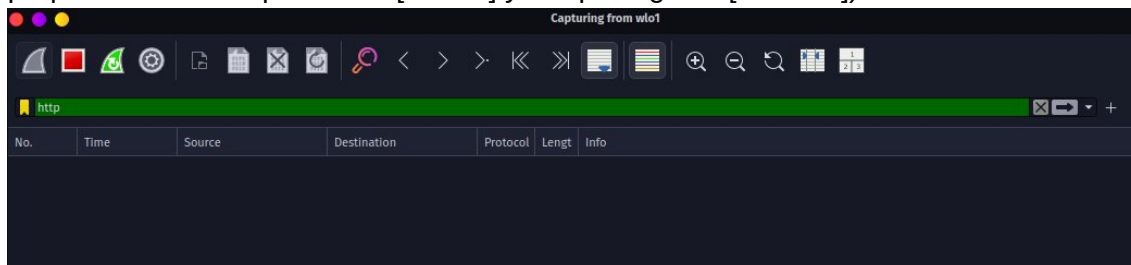




9. Cierra el navegador y abre Wireshark e inicia la captura de tráfico. Abre el navegador y dirígete a <https://www.sitio1.com/ficheros>. Introduce las credenciales de un usuario válido. Comprueba que accedes mediante https. Detén la captura de tráfico. (Imagen del navegador con URL a carpeta ficheros, empezando por https solicitando credenciales y tras acceder correctamente)



10. Detén la captura. Filtra por http y observa que no se ha capturado nada porque hemos accedido por https, por tanto las credenciales han sido encriptadas. Filtra por ssl y comprueba que el tráfico está encriptado. (Captura de tráfico http y captura de tráfico empleando TLS/SSL. Esta segunda captura debería mostrar transferencias de paquetes entre maquina host [cliente] y maquina guest [servidor]).



### Recursos:

<https://techexpert.tips/es/apache-es/habilitar-https-en-apache/>

**PASO 3:** <https://medium.com/@yakuphanbilgic3/create-self-signed-certificates-and-keys-with-openssl-4064f9165ea3>

Tutorial creando un certificado propio tipo CA (como si fuera de entidad certificadora):

<https://luisgomezcaballero.com/es/apache-http-server-configurar-https-2/>

### Condiciones de entrega:

- La práctica se **debe** entregar de forma **individual**, cada uno debe presentar sus propias respuestas. Sin embargo, se puede trabajar en equipo.
- Se debe entregar un documento de texto (.pdf, .docx, .odt, etc.)
- En la portada del documento debe aparecer el nombre completo del alumno.
- La nota comprenderá un valor numérico entre 0 y 10.
- **La fecha límite de entrega es el 28 de noviembre de 2024 a las 23:59:59.**
- **Se podrá entregar hasta 72 horas más tarde de la fecha límite pero con una penalización sobre su puntuación (no será posible aspirar al 10).**