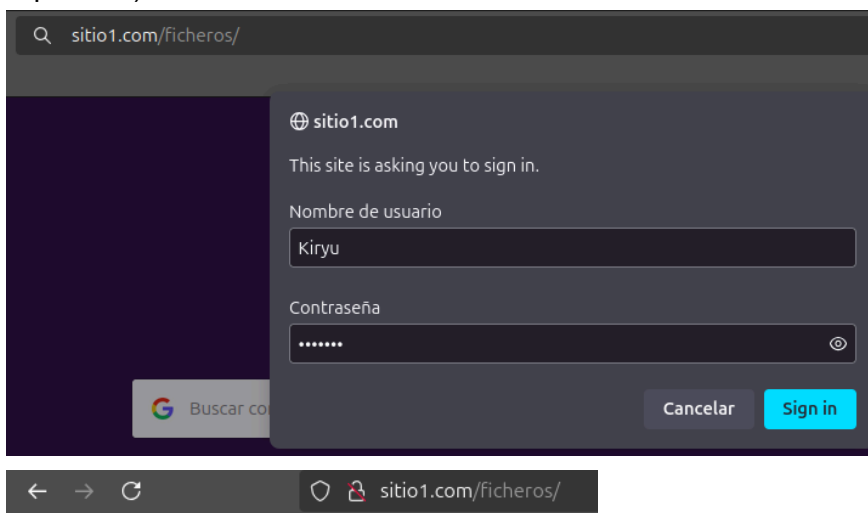


Práctica 6. HTTPS





Pedro Capó Lozano

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 e introduce las credenciales de un usuario con acceso. Dirígete 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)



Index of /ficheros

Name	Last modified	Size	Description
 Parent Directory		-	
 fichero1.txt	2024-11-06 15:19	0	
 fichero2.txt	2024-11-06 15:19	0	
 fichero3.txt	2024-11-06 15:19	0	

Apache/2.4.58 (Ubuntu) Server at sitio1.com Port 80

No.	Time	Source	Destination	Protocol	Length	Info
10	46.984417468	192.168.56.100	192.168.56.101	HTTP	434	GET /ficheros/ HTTP/1.1

2. Inspecciona la trama en los paquetes 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).

```

> Frame 10: 432 bytes on wire (3472 bits), 434 bytes captured (3472 bits) on interface vboxnet0, id 0
> Ethernet II, Src: 0a:00:27:00:00:00 (0a:00:27:00:00:00), Dst: PCSSystemtec_b1:f6:85 (08:00:27:b1:f6:85)
> Internet Protocol Version 4, Src: 192.168.56.100, Dst: 192.168.56.101
> Transmission Control Protocol, Src Port: 46612, Dst Port: 80, Seq: 1, Ack: 1, Len: 368
> Hypertext Transfer Protocol
  > GET /ficheros/ HTTP/1.1\r\n
    > [Expert Info (Chat/Sequence): GET /ficheros/ HTTP/1.1\r\n]
      [GET /ficheros/ HTTP/1.1\r\n]
      [Severity level: Chat]
      [Group: Sequence]
      Request Method: GET
      Request URI: /ficheros/
      Request Version: HTTP/1.1
      Host: sitio1.com\r\n

Request URI: /ficheros/
Request Version: HTTP/1.1
Host: sitio1.com\r\n
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:132.0) Gecko/20100101 Firefox/132.0\r\n
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n
Accept-Language: es-ES,es;q=0.8,en-US;q=0.5,en;q=0.3\r\n
Accept-Encoding: gzip, deflate\r\n
Connection: keep-alive\r\n
Upgrade-Insecure-Requests: 1\r\n
Priority: u=0, i\r\n
\r\n
[Full request URI: http://sitio1.com/ficheros/]
[HTTP request 1/1]
[Response in frame: 12]

```

3. Dirígete al directorio `/etc/apache2/sites-available` y genera mediante `openssl` el certificado autofirmado para `sitio1`. Comprueba que se han creado los certificados en el directorio. (Captura de comando para crear `.key` y `.crt`, y su resultado. Captura del contenido de certificado creado [verificación mediante `openssl`]. Captura del contenido de la carpeta `sites-available` tras creación)

[illegible]

Detalles de la clave y certificados auto-firmados a generar:

- Formato del certificado a generar: X.509
- Duración del certificado: 365 días
- Clave privada **sin** encriptación DES

- Para la clave; utilizar el algoritmo RSA con un tamaño de clave de 2048 bits
- La clave y el certificado deben tener un nombre específicos; ej. sitio1.key y sitio1.crt (o equivalentes a los sitios web creados)

(Opcional) Certificado y clave, con estos detalles, se pueden crear en una única instrucción.

Ver apartado **Recursos** para más información.

```
pedro@pedro:/etc/apache2/sites-available$ sudo openssl req -x509 -new -nodes  
-key sitio1.key -sha256 -days 365 -out sitio1  
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]:.  
State or Province Name (full name) [Some-State]:.  
Locality Name (eg, city) []:.  
Organization Name (eg, company) [Internet Widgits Pty Ltd]:.  
Organizational Unit Name (eg, section) []:.  
Common Name (e.g. server FQDN or YOUR name) []:192.168.56.101  
Email Address []:.  
pedro@pedro:/etc/apache2/sites-available$
```

```
pedro@pedro:/etc/apache2/sites-available$ sudo openssl x509 -in sitio1.crt -  
text -noout  
Certificate:  
  Data:  
    Version: 3 (0x2)  
    Serial Number:  
      43:8f:72:3c:ca:6d:ab:01:8c:3b:06:70:b0:65:ae:de:d2:ee:4f:c6  
    Signature Algorithm: sha256WithRSAEncryption  
    Issuer: CN = 192.168.56.101  
    Validity  
      Not Before: Nov 14 17:10:36 2024 GMT  
      Not After : Nov 14 17:10:36 2025 GMT  
    Subject: CN = 192.168.56.101  
    Subject Public Key Info:  
      Public Key Algorithm: rsaEncryption  
      Public-Key: (2048 bit)  
      Modulus:
```

```
pedro@pedro:/etc/apache2/sites-available$ ls  
000-default.conf  sitio1          sitio1.crt  sitio2.conf  
default-ssl.conf  sitio1.conf    sitio1.key  
pedro@pedro:/etc/apache2/sites-available$
```

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)

```
pedro@pedro:/etc/apache2/sites-available$ sudo a2enmod ssl
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
pedro@pedro:/etc/apache2/sites-available$ sudo systemctl restart apache2
pedro@pedro:/etc/apache2/sites-available$
```

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)

```
pedro@pedro:/etc/apache2/sites-available$ sudo cp sitio1.conf sitio1copia.conf
[sudo] password for pedro:
pedro@pedro:/etc/apache2/sites-available$ ls
000-default.conf  sitio1      sitio1copia.conf  sitio1.key
default-ssl.conf  sitio1.conf sitio1.crt        sitio2.conf
pedro@pedro:/etc/apache2/sites-available$ sudo cp default-ssl.conf default-sslcopia.conf
pedro@pedro:/etc/apache2/sites-available$ ls
000-default.conf  sitio1      sitio1.crt
default-ssl.conf  sitio1.conf sitio1.key
default-sslcopia.conf  sitio1copia.conf  sitio2.conf
```

```
pedro@pedro: /etc/apache2/sites-available
GNU nano 7.2 sitio1.conf *
<VirtualHost *:443>

    ServerAdmin webmaster@localhost

    ServerName sitio1.com
    DocumentRoot /var/www/sitio1

    <Directory /var/www/sitio1>
        AuthType Basic
        AuthName "Acceso restringido"
        AuthUserFile /etc/apache2/claves.txt
        AuthGroupFile /etc/apache2/grupos.txt
        Require group Dragon Mejores
    </Directory>

^G Help      ^O Write Out  ^W Where Is   ^K Cut
^X Exit      ^R Read File  ^\ Replace    ^U Paste

pedro@pedro: /etc/apache2/sites-available
GNU nano 7.2 sitio1.conf *
    AuthName "Acceso restringido"
    AuthUserFile /etc/apache2/claves.txt
    AuthGroupFile /etc/apache2/grupos.txt
    Require group Dragon Mejores
</Directory>

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

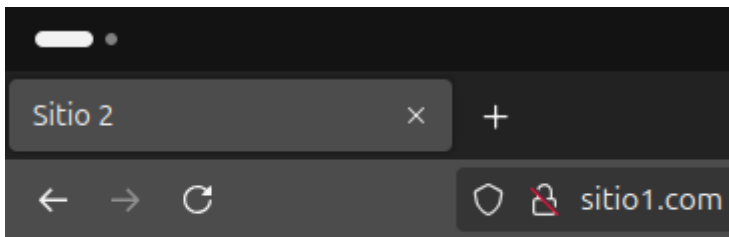
    SSLEngine on
    SSLCertificateFile /etc/apache2/sites-available/sitio1.crt
    SSLCertificateKeyFile /etc/apache2/sites-available/sitio1.key
</VirtualHost>
```

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

```
pedro@pedro:/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 sup
press this message
Syntax OK

pedro@pedro:/etc/apache2/sites-available$ sudo systemctl reload apache2
pedro@pedro:/etc/apache2/sites-available$
```

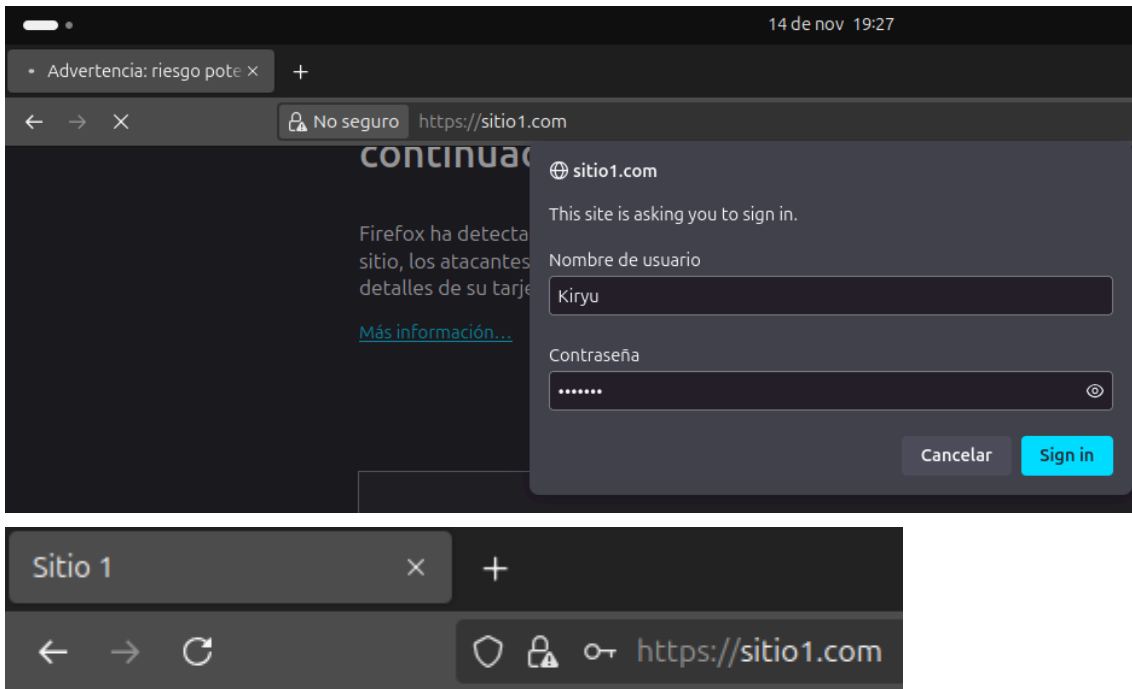
7. Abre un nuevo navegador y dirígete a <http://www.sitio1.com> y comprueba si ahora te dirige a la página por defecto. (Captura del navegador)



Saludos desde el sitio 2

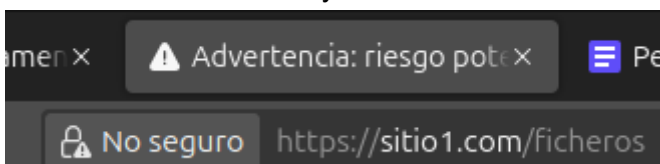
8. Dirígete ahora a **<https://www.sitio1.com>**. y comprueba que vuelve a salir la página que creamos en su momento. Comprueba que accedes mediante https. (Captura del navegador accediendo a la web creada vía https, Si el navegador te solicita “aceptar riesgos adicionales” para entrar a la página, incluye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

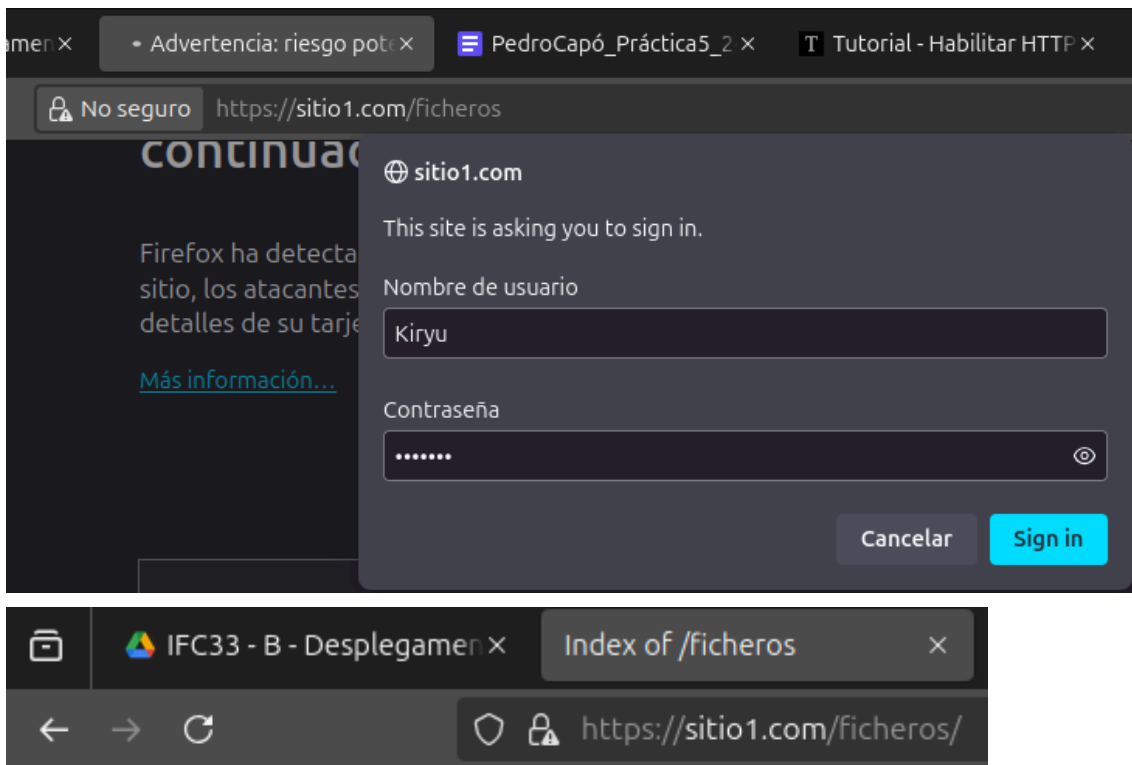








Bienvenido al Sitio 1

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)





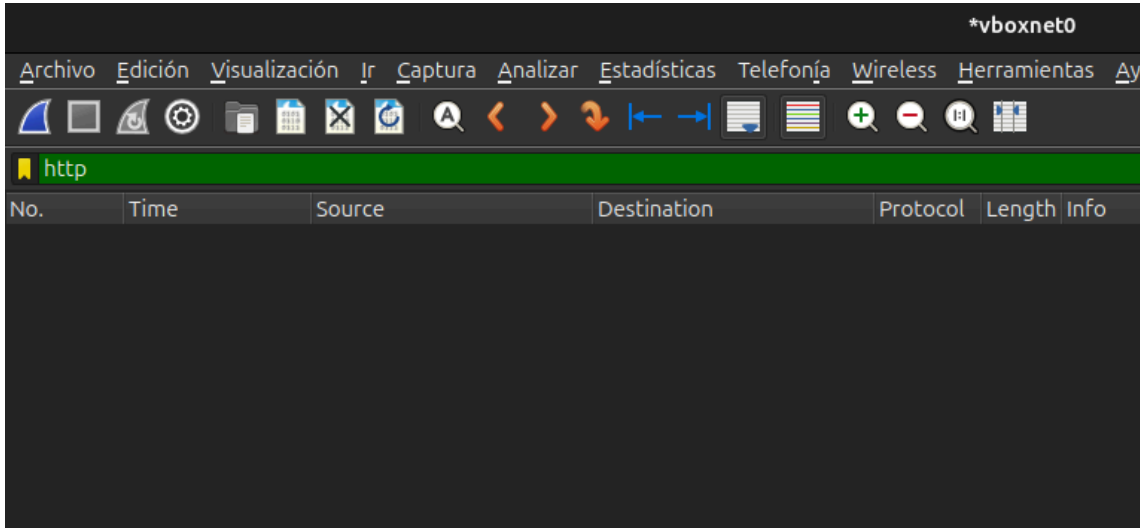
Index of /ficheros

<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
 Parent Directory		-	
 fichero1.txt	2024-11-06 15:19	0	
 fichero2.txt	2024-11-06 15:19	0	
 fichero3.txt	2024-11-06 15:19	0	

Apache/2.4.58 (Ubuntu) Server at sitio1.com Port 443

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

trafico empleando TLS/SSL. Esta segunda captura debería mostrar transferencias de paquetes entre maquina host [cliente] y maquina guest [servidor]).



No.	Time	Source	Destination	Protocol	Length	Info
4	0.004379499	192.168.56.100	192.168.56.101	TLSv1.3	1947	Client Hello (SNI=siti01.com)
6	0.011634817	192.168.56.101	192.168.56.100	TLSv1.3	1416	Server Hello, Change Cipher Spec, Application Data, Application D...
8	0.024442889	192.168.56.100	192.168.56.101	TLSv1.3	130	Change Cipher Spec, Application Data
9	0.025553864	192.168.56.100	192.168.56.101	TLSv1.3	623	Application Data
10	0.025628389	192.168.56.101	192.168.56.100	TLSv1.3	145	Application Data
11	0.025956738	192.168.56.101	192.168.56.100	TLSv1.3	145	Application Data
13	0.030527551	192.168.56.101	192.168.56.100	TLSv1.3	808	Application Data
15	2.940576483	192.168.56.100	192.168.56.101	TLSv1.3	704	Application Data
16	2.941966354	192.168.56.101	192.168.56.100	TLSv1.3	558	Application Data
20	7.945277232	192.168.56.101	192.168.56.100	TLSv1.3	90	Application Data
23	7.945748343	192.168.56.100	192.168.56.101	TLSv1.3	90	Application Data
29	29.938762080	192.168.56.100	192.168.56.101	TLSv1.3	1947	Client Hello (SNI=siti01.com)
31	29.940128752	192.168.56.101	192.168.56.100	TLSv1.3	1416	Server Hello, Change Cipher Spec, Application Data, Application D...