



Práctica 3 - Sesiones I y II - Servicios de red avanzados

Entregable

Información básica y requisitos para la entrega de las tareas

- 1) Ser concisos y breves en la respuesta a cada tarea.
- 2) Ceñirse al espacio dedicado para cada tarea.
- 3) No olvidar escribir el nombre de cada integrante de la pareja y la isla en donde normalmente trabaja la pareja.
- 4) No se evaluarán tareas que ya se evaluaron en el laboratorio.
- 5) Adaptar el escenario virtualizado a la isla en donde normalmente trabaja la pareja.

Realización práctica: HTTPS

- 1) Cree un certificado SSL con la utilidad openssl para asociarlo al sitio frpracticahttps.com. Nombre el fichero del certificado como frpracticahttps.crt y el nombre del fichero de la clave privada como frpracticahttps.key.

```
root@pc1:/home/administrador
root@pc1:/home/administrador# sudo openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout /etc/ssl/private/frpracticahttps.key -out /etc/ssl/certs/frpracticahttps.crt
Generating a RSA private key
.....+
.....+
writing new private key to '/etc/ssl/private/frpracticahttps.key'
-----
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]:Granada
Locality Name (eg, city) []:Granada
Organization Name (eg, company) [Internet Widgits Pty Ltd]:UGR
Organizational Unit Name (eg, section) []:DTSTC
Common Name (e.g. server FQDN or YOUR name) []:frpracticahttps.com
Email Address []:webmaster@frdominioseguro.com
root@pc1:/home/administrador#
```



- 2) Inspeccione los ficheros `frpracticahttps.crt` y `frpracticahttps.key`.

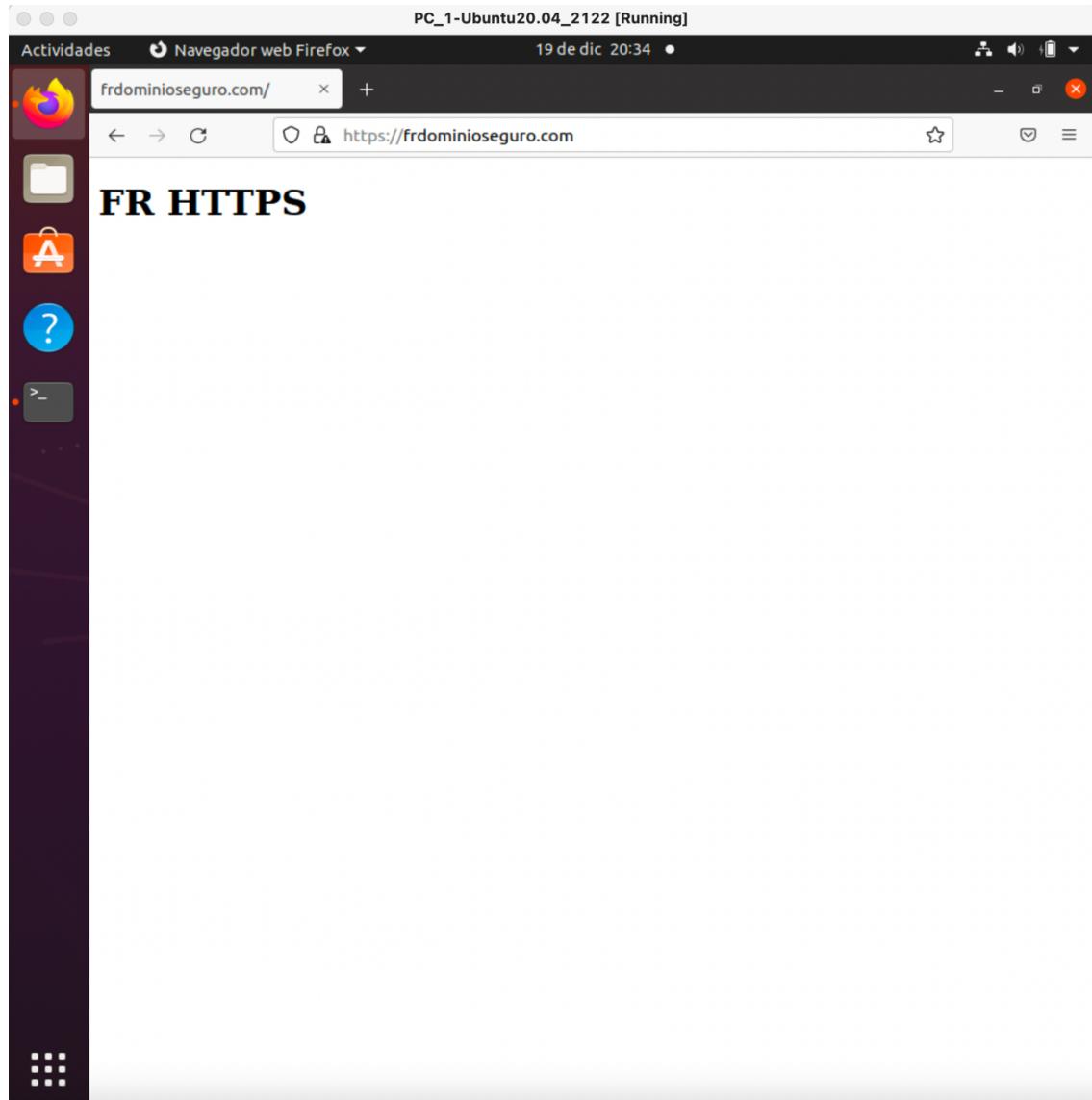
```
root@pc1:/home/administrador
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:SP
State or Province Name (full name) [Some-State]:Granada
Locality Name (eg, city) [:]Granada
Organization Name (eg, company) [Internet Widgits Pty Ltd]:UGR
Organizational Unit Name (eg, section) [:]DTSTC
Common Name (e.g. server FQDN or YOUR name) [:]frpracticahttps.com
Email Address []:webmaster@frdominioseguro.com
root@pc1:/home/administrador# cat /etc/ssl/private/frpracticahttps.key
-----BEGIN PRIVATE KEY-----
MIIEVgIBADANBgkqhkiG9w0BAQEASCBKgwggSkAgEAoIBAQDmBfnn6Atbznn
BTWWhP6snjv+clr9ZJumyQIKIZH17h06CUknCsxiow3oqIoHKNb0JU0XTM8
547FGscC/hfauzFSi4dpg56Aqqgy1dnccwcfh0bomeEMad1cpf0IlyOuv8LH
/72t7ITLnM1QF0lqmRs0+fsi0HEl7wvYghofpdIVvPzqvbFxNROs0jGtyokAf
ikh9B83ynESFrqIScxXalsVWdtwlj2tXGe05Pk0m3b0UldoPxSfBvR+8ycu6sz
IDrn8LzB4gn18MLURf0q2kk9H16/ldoy502IdKcmh3o+CK4DHqzf5seTh9uq0
CJTvsY9AgMBAEcgEBAL56L4Ph0cQ/r1lPGdyv850ka+v+lnk0vpF3qvhOHBo02
Mwg/DZ5tIoHTY/6jg2z50zk15ufzYdpWDJlIsDkaI+nR55QV9J1ezyoVgNANGvM
q671Rc1oo0WnHWAFbaxgKwQafCNNTXg2VsLMFe3TAEWLHV1DXr63NYoHeILbX
gV7tCtmKJ2zcT9R6PxdnG4GDkf7z1J0NQY+wLFC+pwoyCvMhnw9v8jqZZ7N34
aWtfmfQFKmc2EsUl4B9vEh1z0LS2ZP+sPE4wwvu1yoQLCxejGoKOAl6DcwVa6
Rdfdp+bqvNfcgAdrn7h+dxlcvjgn5FXS/+DSek2YT02rprmH1lxq8cy9quxb8j
1Pfdk7deYQxdnB7nVraAfuiPU1vVLSt1ZCvq4aJk/b1qFopYqPjwUwNm00gdAQ
Vrk4d+U0tfmee6duYjgoKTn86P43pUFViu/kh7SY1h/m/AaFT+rGbmQKBgQDH
s14bhsh3FLXTAV44VA67uh29PUL0l0RSVmj67KH+I1XnzQyT874gf6PP5zWoX1R
NORgouLIiyVmgz2mSMkn7Mwjxra7lrCmxnyQGeFKInyQb44KhEDo7d37Y21
Mtbd4fb6tA+0DTz3kNO/NklBv/gPkyEkzoyWYjwQKBgEw1SikkLbq5Hd8trK4C
AaAGtE2lbwUB778x9Fc0jerkjGrgoaznR5Fx04Os0/rP1t2Xrl9BrnLGOfJQ4
Zlr17dftytvnPpiMemBd4wxXkZDbBgXsdP0XanCo3Hh4ud7g3xbgj4Nve5jh21bp
9KvYbJ8nmSQ2toVol/LHyL3v
-----END PRIVATE KEY-----
root@pc1:/home/administrador#
```

frpracticahttps.key

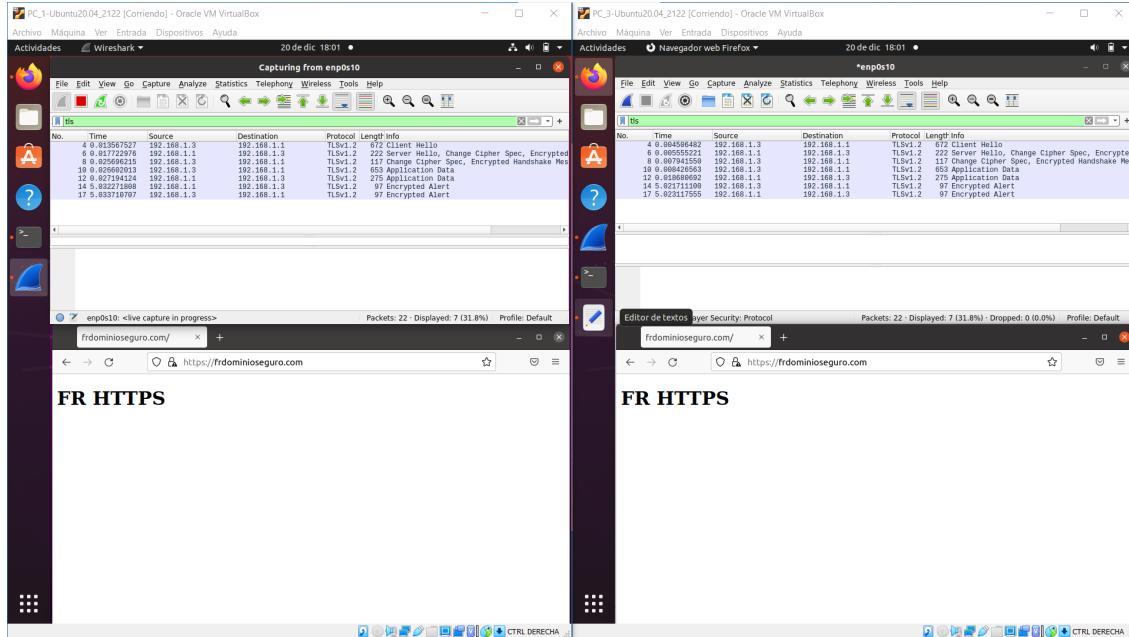
```
root@pc1:/home/administrador
IrVfTDZuFdU0e0m9txn5G0bF1QRTdekUlq8n09nnn0gEbLxa8x5jWldZmGDWv1Wr
ljelZKJls3Ga2whkpuIP4e6Qv9GbX1gg17kUfu9x9qaagf0gQkm9PHUP/v
ViFGLOyFq+A06V3a15Ah12tE6ekCgYe0zLZKpcf/6zuwTHMpC8aZUL0F/A908CZ
pi453JVKyYrq0xJ9R6PxmdC4GDKf7zNj0NQY+wLFC+pwoyCvMhnw9v8jqZZ7N34
aWtfmfQFKmc2EsUl4B9vEh1z0LS2ZP+sPE4wwvu1yoQLCxejGoKOAl6DcwVa6
Rdfdp+bqvNfcgAdrn7h+dxlcvjgn5FXS/+DSek2YT02rprmH1lxq8cy9quxb8j
1Pfdk7deYQxdnB7nVraAfuiPU1vVLSt1ZCvq4aJk/b1qFopYqPjwUwNm00gdAQ
Vrk4d+U0tfmee6duYjgoKTn86P43pUFViu/kh7SY1h/m/AaFT+rGbmQKBgQDH
s14bhsh3FLXTAV44VA67uh29PUL0l0RSVmj67KH+I1XnzQyT874gf6PP5zWoX1R
NORgouLIiyVmgz2mSMkn7Mwjxra7lrCmxnyQGeFKInyQb44KhEDo7d37Y21
Mtbd4fb6tA+0DTz3kNO/NklBv/gPkyEkzoyWYjwQKBgEw1SikkLbq5Hd8trK4C
AaAGtE2lbwUB778x9Fc0jerkjGrgoaznR5Fx04Os0/rP1t2Xrl9BrnLGOfJQ4
Zlr17dftytvnPpiMemBd4wxXkZDbBgXsdP0XanCo3Hh4ud7g3xbgj4Nve5jh21bp
9KvYbJ8nmSQ2toVol/LHyL3v
-----END PRIVATE KEY-----
root@pc1:/home/administrador# cat /etc/ssl/certs/frpracticahttps.crt
-----BEGIN CERTIFICATE-----
MIIEGTCAwGgAwIBAgIUFwDiciUYBbnsRqZErNrx5q5nXswDQYJKoZIhvcNAQEL
BQAwgZsxCza0EcwgYDwQAYTALNQMRawDgYDVQOIDAdHcmFuYWRhMRawDgYDVQHQdAdH
cmFuYWRhM0qwCgYDvQ0QKDAnVR1IxdjAMBvNBAsMBRUU1RDMRrwGgYDVQ0QDBNm
cnBytWNa0hRa0CHMuY29tMSwvKgYJkozIhvcNQkbfh13ZwJtYXN0ZXJAznjk
b21pbmlvc2VndJvLmNbVtaefw0yHTEyMThxNzMSNdaFw0yMjeYMTMxnzMSNda
MIGbMqsWCQyDVQGEwJTUDeqMA4GA1UEAwHR3JhbmcFkyTeQMA4GA1UEBwwHr3j
bmFkYTeMmA0G1UECgwDVudsM04wDAYDVQQLDAVEFVNQzEcMboGA1UEAwvTzNjw
cmFjdGljYwh0dHBzLmNbVtEsMcoGCSqGSib3DQEJARYdd2VibWFzdGvYQGzyZG9t
aW5pb3NLZ3Vby5jz20wggelMA0GCSqGSib3DQEBAQAA4IBDwAwggEKAoIBAQDM
bfnn6AtbznnCTVWhP6sNjv+clr9ZJumyQIKIZH17h06CUknCsxiow3oqIoH
KYNb0JU0XTM8547fgscC/hfauzFSi4dpg56Aqqgy1dnccwcfh0bomeEMad1cp
f0IlyOuvU8LH/72t7ITLnM1QF0lqmRs0+fsi0HEl7wvYghofpdIVvPzqvbFxN
R0s0jGtyokAf1kh9B83ynESFrqIScxXalsVWdtwiJ2tXGe05Pk0m3b0UldoPxSf
ibVr+8ycu6szIDrn8LzB4gn18MLURf0q2kk9H16/ldoy502IdKcmh3o+CK4DHqz
xf5ZseTh9uq0CJTvsY9JAgMBAAGjUzBRMB0GA1udDgQWBBSLC/C7qnD9KpfKcuqt
Z7PqSF78dJaBqgNVHSMEGDwgbS8Lc/C7qnD9KpfKcuqtZ7pSF78djaPBgNVHMRB
Af8EBTADAOH/MA0GCSqGSib3DQEBCwUA4IBAOBc1Fxyje3U6MyTrx/60TnIn1PI
BkMptMs2SyAzmE/xz4D/64eH2o4KHyqjw+GMAjJ2H+A/g4F0TPU6+kPqqMBRQzfj
zfIGmDbzQjAsvn+NWEQo3y1lzacNt4PKwAG04M4Plzcf1focY2EWEQ6ze2B/k2P
CJXacS3Fm2w9Wubn19UDZecFc288/XQVGvGSH1V5nrskBe/hsyRomaXXooj9HHd
5nbeCxSMBR/fE1wNNqEc1NSuW7syqyVTTodsbFUb6iwg80CFghhtCh1thMr7Es
yEYZnkbcGMUYqLLGImVEyNRkWbH4nztNyvPzIB1t5SEEUtJayzxUVdxkBs9a
-----END CERTIFICATE-----
root@pc1:/home/administrador#
```



- 3) Cree un host virtual con una página de inicio que muestre el mensaje “FR HTTPS” y configúrelo para que funcione con HTTPS haciendo uso del certificado creado anteriormente. Compruebe su correcto funcionamiento usando un navegador.

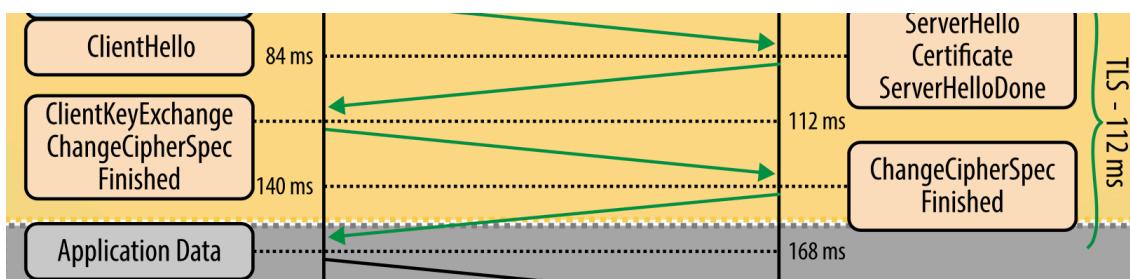


- 4) Abra Wireshark en su equipo y capture los mensajes que se generan cuando accede al sitio creado anteriormente. ¿Qué mensajes TLS se intercambian la aplicación cliente (navegador web) y el servidor (Apache) durante el inicio de la conexión? ¿Qué información relevante se intercambia en esos mensajes? ¿Es posible ver los mensajes del protocolo HTTP?



PC_1 (Servidor, 192.168.1.1), PC_3(Cliente, 192.168.1.3)

Se intercambian los mensajes del TLS handshake. Primero vemos el Client Hello del cliente al servidor, a continuación, como respuesta, el servidor envía al cliente el Server Hello (respuesta a cliente), el certificado SSL del servidor, se produce el intercambio de claves (en el servidor) y envía un Server Hello Done. El cliente lo recibe, realiza su intercambio de claves y envía el Encrypted Handshake Message. Finalmente, el servidor devuelve el Finished tras el Change Cipher Spec y comienza a intercambiar la información de la aplicación, en nuestro caso la información de index.html de nuestra página web. Es decir, el diagrama estudiado:



No se pueden ver mensajes del protocolo HTTP porque están cifrados.



UNIVERSIDAD
DE GRANADA

Fundamentos de Redes

3º del Grado en Ingeniería
Informática



Dept. Teoría de la Señal,
Telemática y Comunicaciones