­­

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.

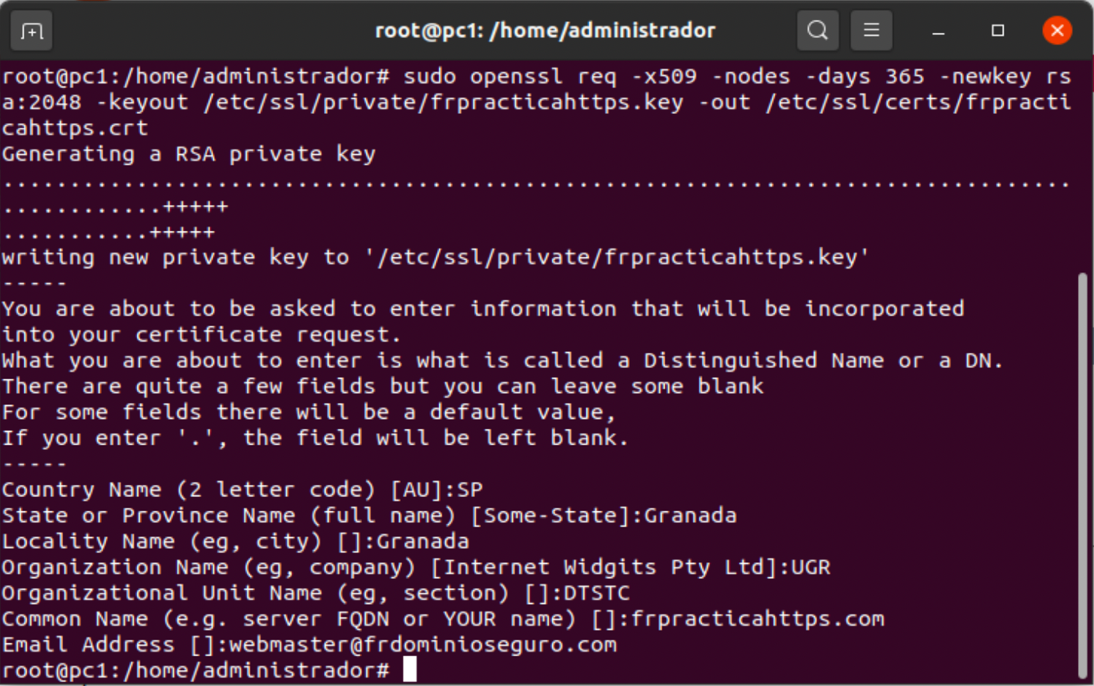
3) No olvidar escribir el nombre de cada integrante de la pareja y la isla en donde normalmente trabaja la pareja.

4) No se evaluarán tareas que ya se evaluaron en el laboratorio.

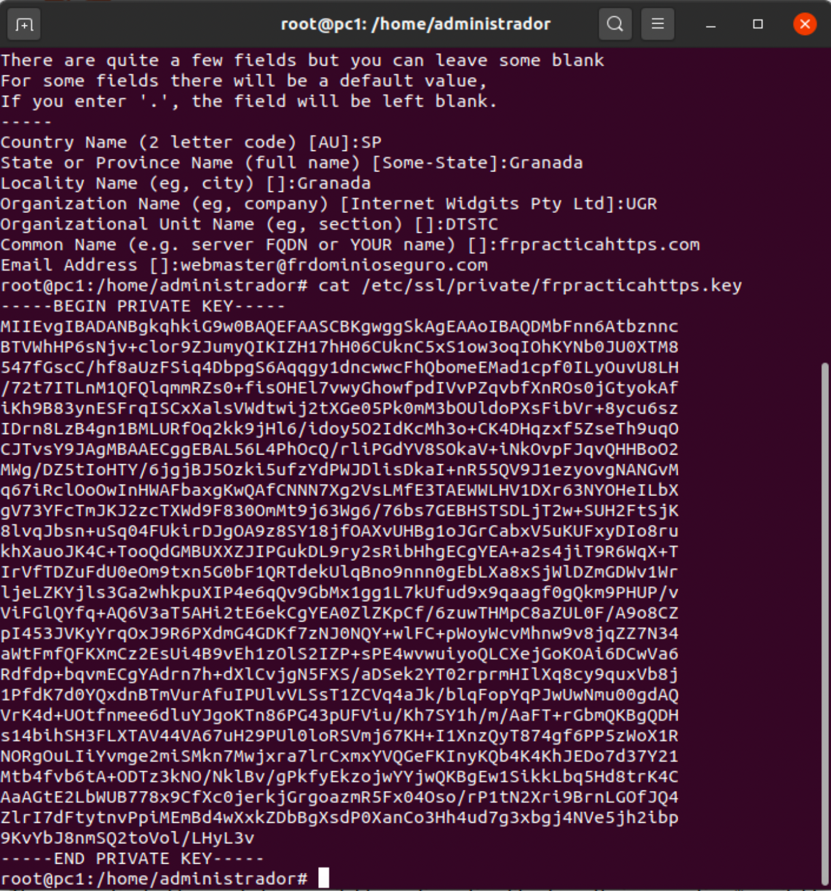
5) Adaptar el escenario virtualizado a la isla en donde normalmente trabaja la pareja.

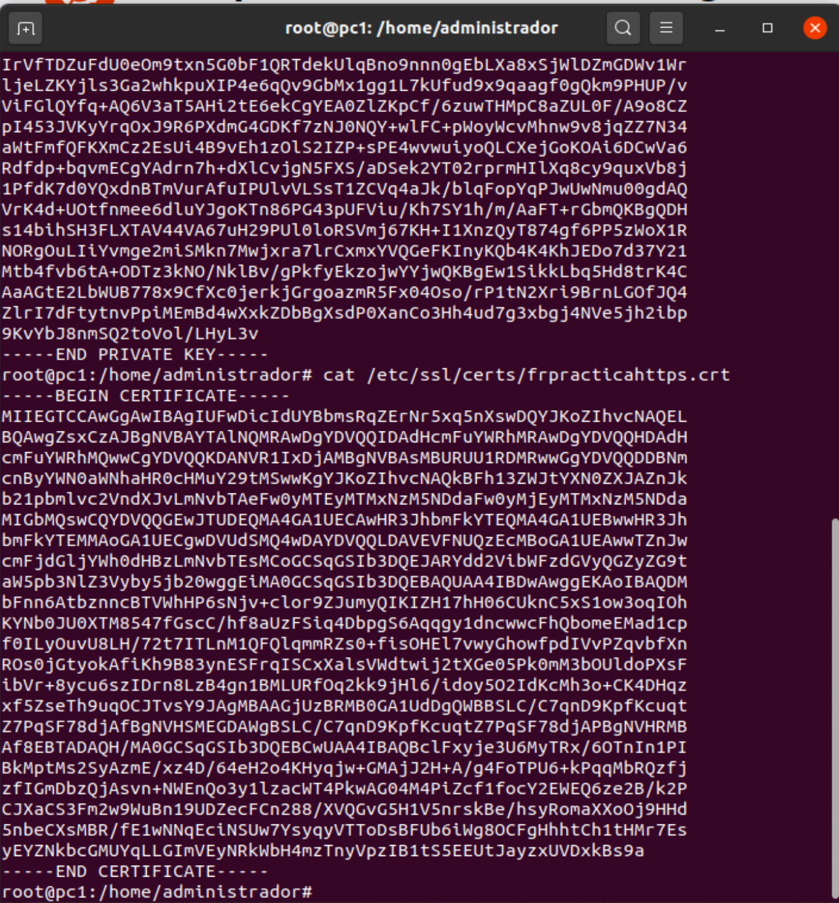
## Realización práctica: HTTPS

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.

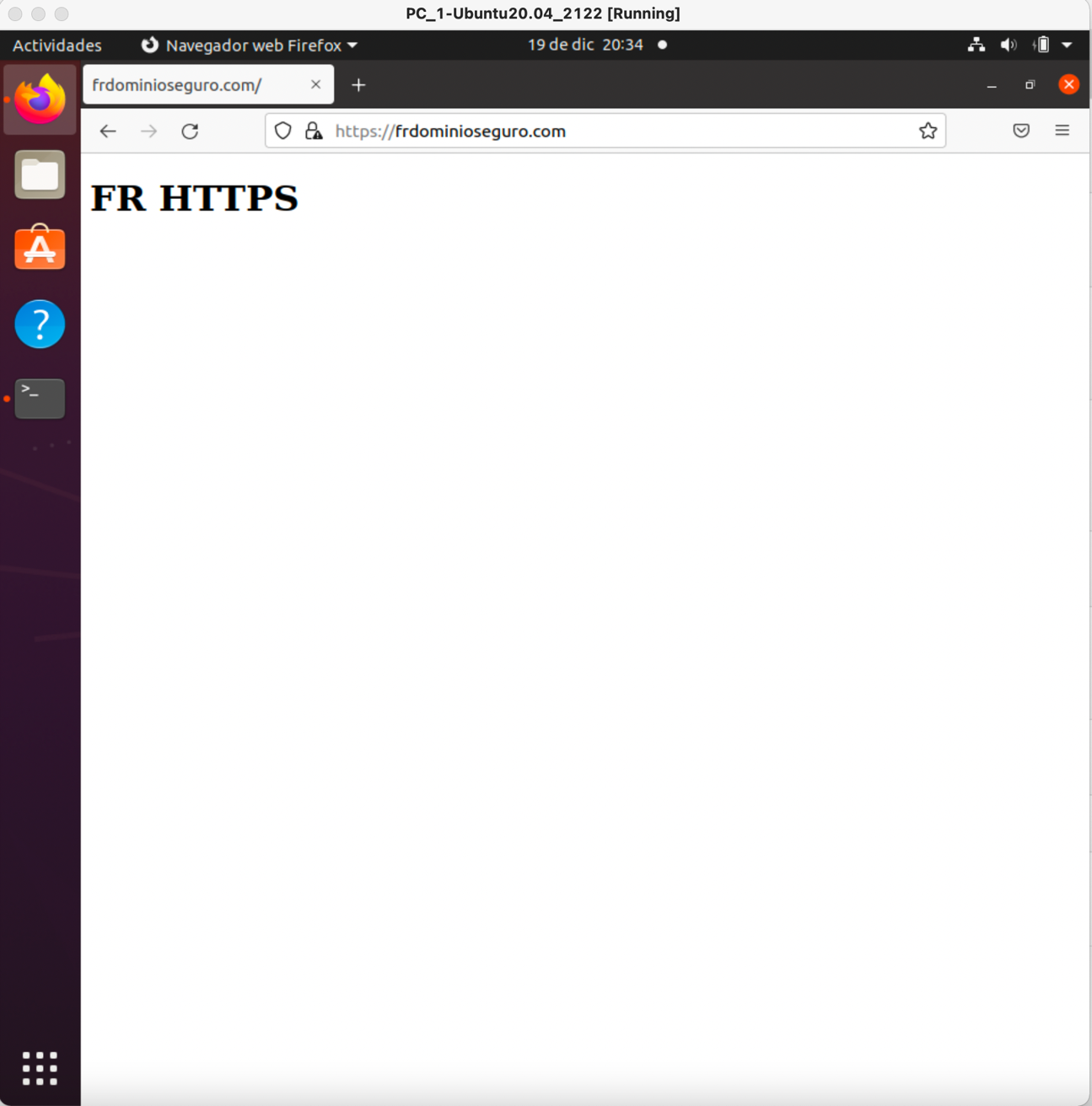


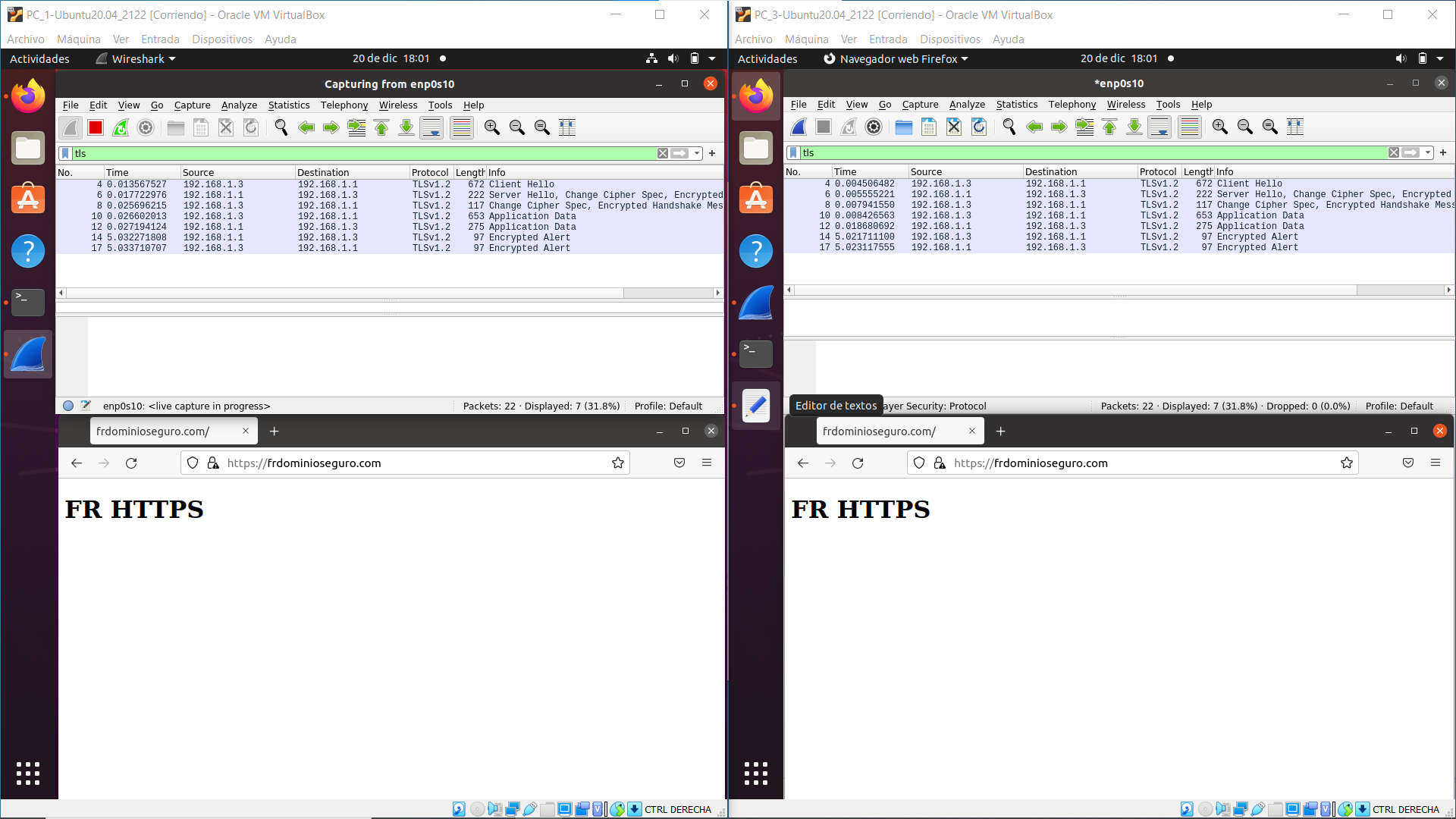
1. Inspeccione los ficheros frpracticahttps.crt y frpracticahttps.key.

frpracticahttps.key

frpracticahttps.crt

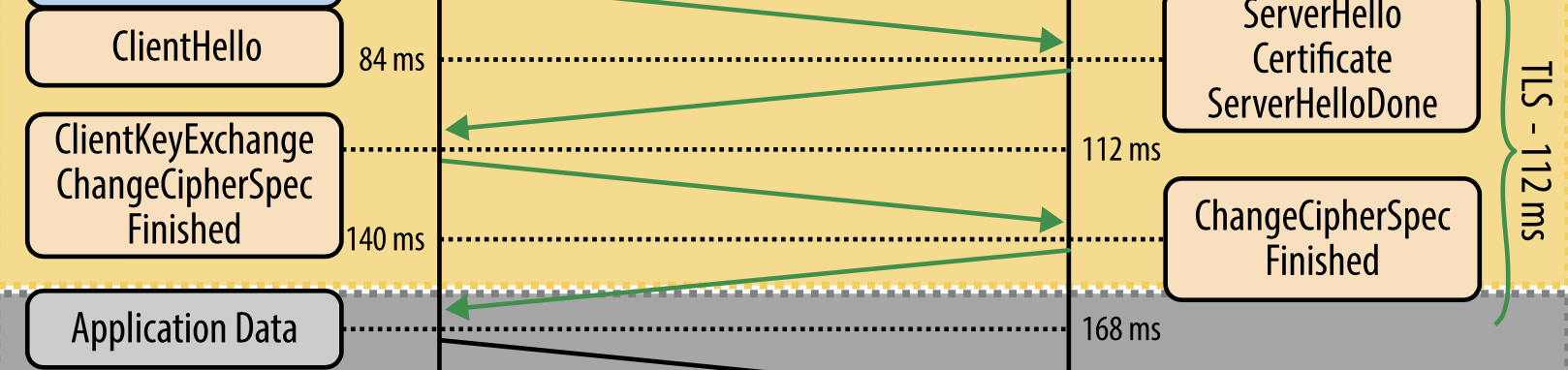
1. Cree un host virtual con una página de inicio que muestre el mensaje “FR HTTPS” y configúrelo para que funcione con HTTPS haciendo uso del certificado creado anteriormente. Compruebe su correcto funcionamiento usando un navegador.



1. 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.