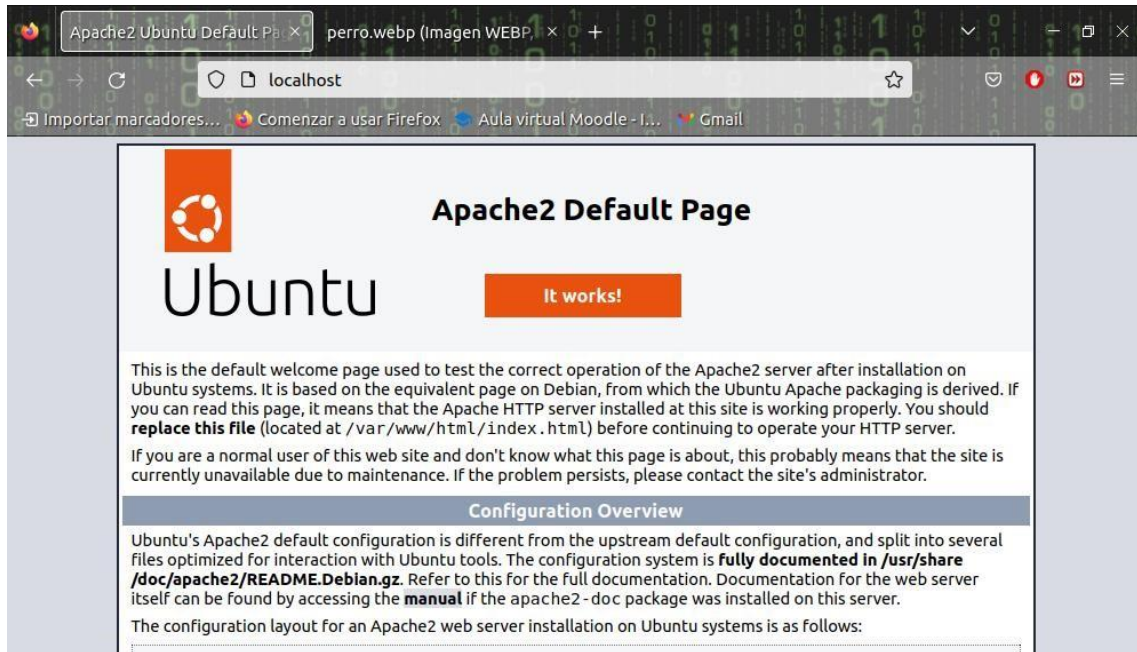


Visualización de seq number con wireshark

1 – Dentro de nuestra máquina virtual con Ubuntu, escribimos en la terminal “sudo apt-get update” para comprobar nuevas actualizaciones.

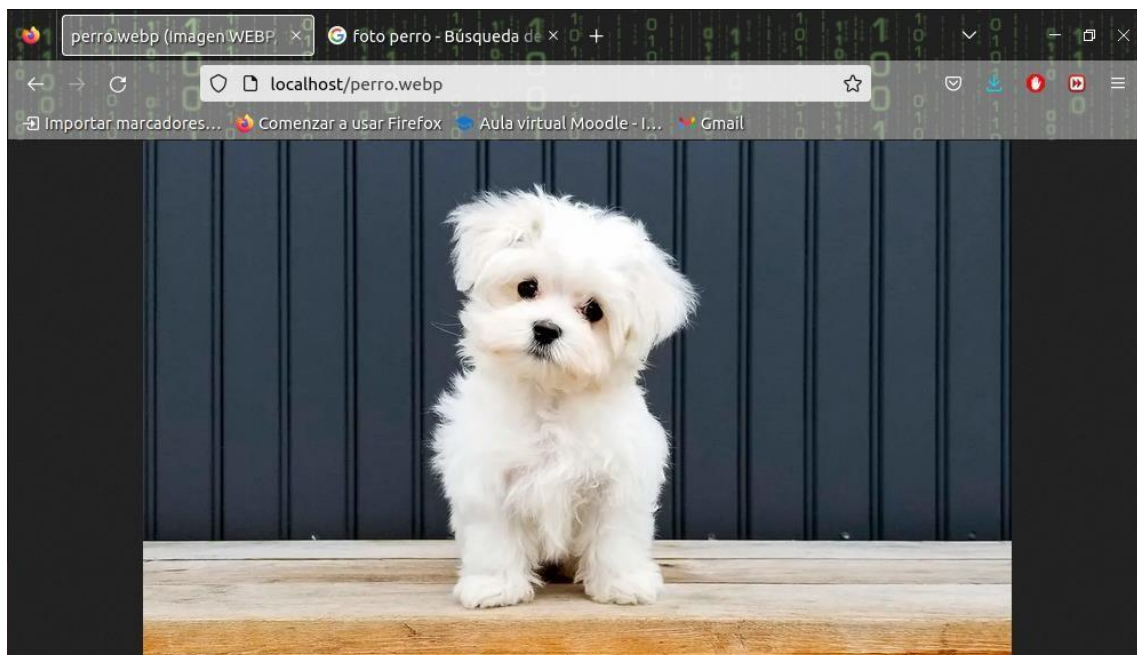
2 – Instalamos Apache: “sudo apt-get install apache2”.

3 – Comprobamos que Apache funciona buscando “localhost” en el navegador de Ubuntu.



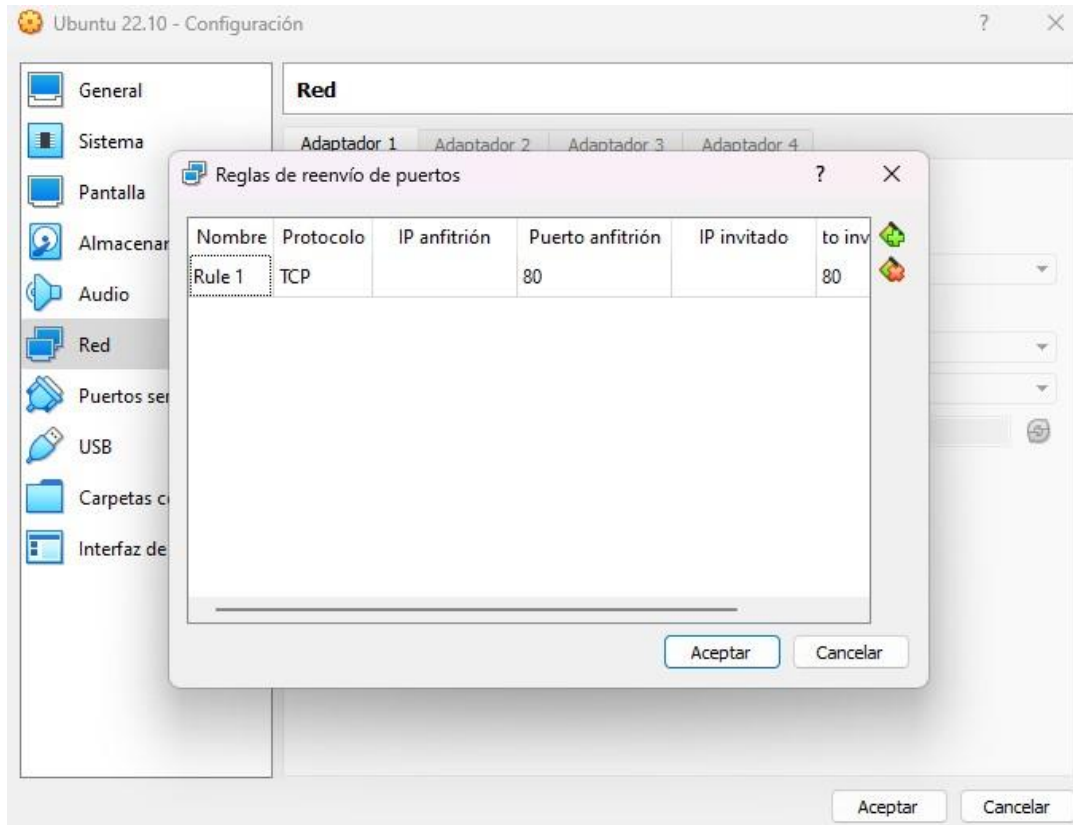
4 – Descargamos cualquier foto de Google y la guardamos con un nombre sencillo. En este caso “perro.webp”.

4 – Comprobamos que podemos visualizar la foto desde “localhost/nombredelafoto” (se debe haber guardado en la carpeta “/var/www/html/perro.webp”).

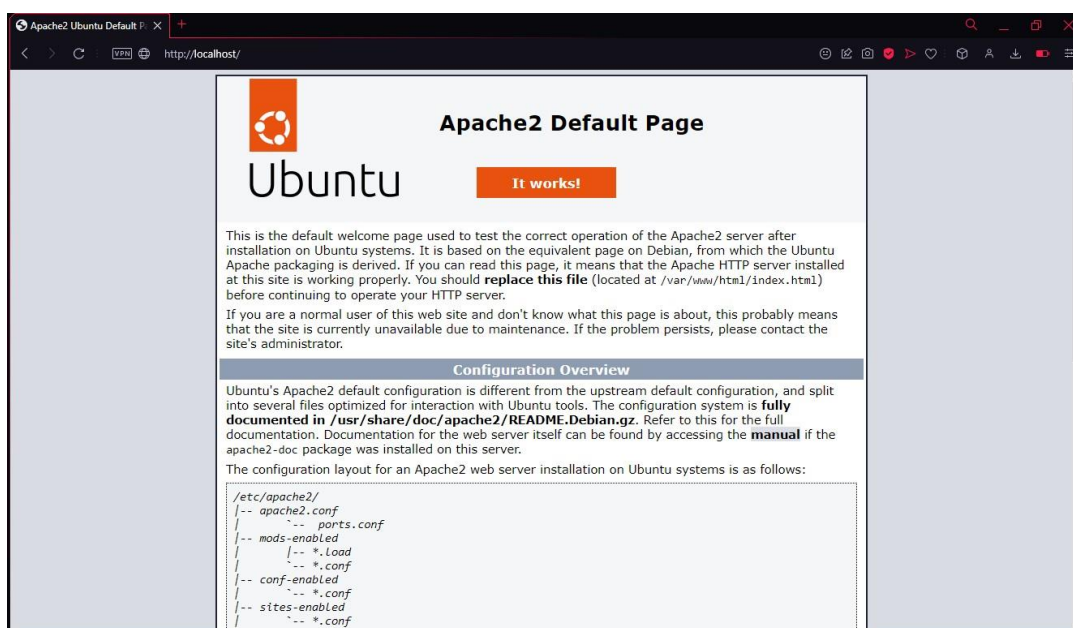


5 Para poder visualizar la foto desde Windows, es decir, acceder al Apache de nuestra máquina virtual desde la máquina anfitriona, se deberán seguir los siguientes pasos:

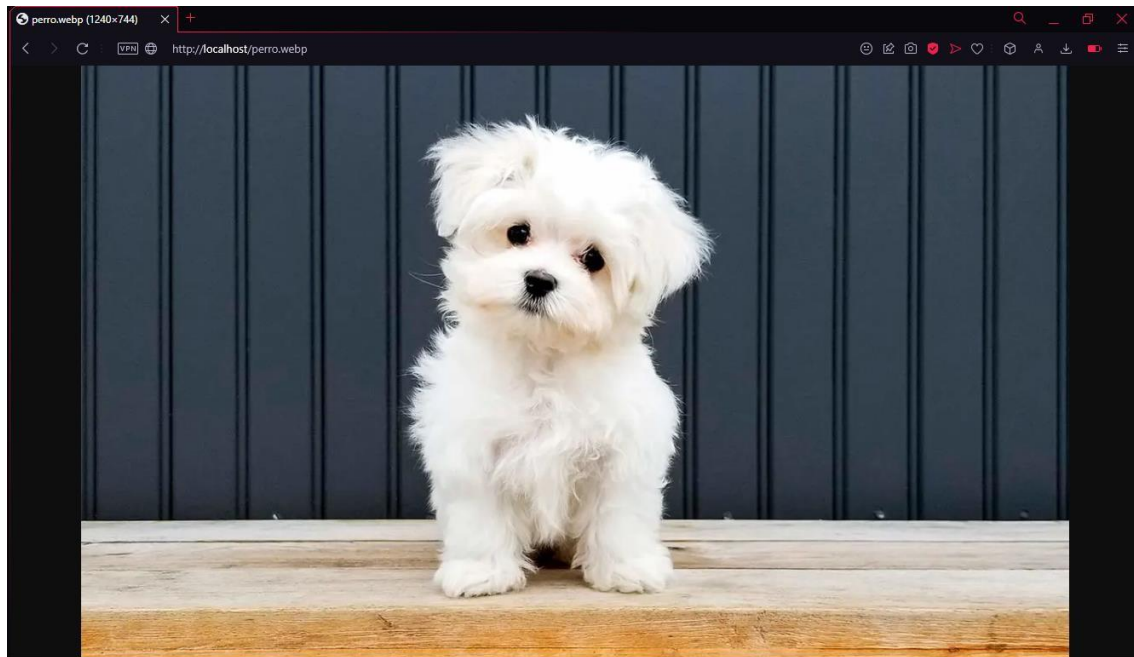
- Entrar en la configuración de la máquina virtual.
- Seleccionar el apartado de “red”.
- Ampliar apartado de “avanzadas”.
- Seleccionar “reenvío de puertos”.
- Seleccionar los puertos anfitrión y de invitado como 80 (http) con protocolo TCP:



6 – Desde el navegador de la máquina anfitriona buscamos “http://localhost” para comprobar que ha funcionado:



6 Buscamos la imagen con “http://localhost/perro.webp”:



Visualización de esta última búsqueda con Wireshark:

1 – Observamos el primer sequence number, que siempre es 0. El raw es 81547867. El acknowledgement number al principio también siempre es 0, así como su raw. El flag SYN está activo (1) y el ACK no (0).

Wireshark interface showing network traffic analysis. The selected packet (No. 1) is a TCP SYN packet from 192.168.73.170 to 192.168.73.184. The details pane shows the following information:

- Ethernet II:** Src: IntelCor_03:e1:ed (1c:4d:70:03:e1:ed), Dst: d6:06:d6:10:9d:7a (d6:06:d6:10:9d:7a)
- Internet Protocol Version 4:** Src: 192.168.73.170, Dst: 192.168.73.184
- Transmission Control Protocol:**
 - Source Port: 50014
 - Destination Port: 8013
 - [Stream index: 0]
 - [Conversation completeness: Incomplete (37)]
 - [TCP Segment Len: 0]
 - Sequence Number: 0 (relative sequence number)
 - Sequence Number (raw): 81547867
 - [Next Sequence Number: 1 (relative sequence number)]

The raw packet data (hex) is shown at the bottom: 0000 d6 06 d6 10 9d 7a 1c 4d 70 03 e1 ed 08 00 45 00 ... z M p ... E

2 En el segundo segmento, el sequence number es 1 y el raw 0. El acknowledgement number es 1 y su raw 81547868 (como observamos, se ha sumado 1 por el flag SYN).

Wireshark packet capture showing a TCP SYN segment. The packet list shows a SYN segment from 192.168.73.170 to 192.168.73.184. The packet details pane shows the TCP segment with Seq=1, Ack=1, and Len=0. The raw data pane shows the hex and ASCII representation of the packet, with the sequence number raw value highlighted as 0000.

3 – En el tercer segmento, el sequence number es 0 y su raw es 81547867. El acknowledgement es 0 en ambos casos.

Wireshark packet capture showing a TCP segment. The packet list shows a segment from 192.168.73.170 to 192.168.73.184. The packet details pane shows the TCP segment with Seq=0, Ack=0, and Len=0. The raw data pane shows the hex and ASCII representation of the packet, with the sequence number raw value highlighted as 0000.

La captura completa de wireshark se encuentra en la entrega del aula virtual, pero he tomado algunas notas sobre el sequence y el acknowledgement number:

SEQUENCE NUMBER

El sequence number es un contador utilizado para hacer un seguimiento de los bytes enviados.

En el primer paquete, este será 0 (el acknowledgement number también será 0). En el segundo paquete, el sequence number también será 0 como en el primero, pero ya el ACK será 1. En el tercero, ambos serán 1.

El flag ACK solo está desactivado en el primer segmento que manda el cliente solicitando la conexión.

El flag SYN incrementa el sequence number en 1, pero el flag ACK no.

A efectos del número de secuencia, el SYN equivale a 1 byte.

El número de ACK indica el número del primer byte que se espera recibir en el siguiente segmento.

El initial sequence number (ISN) es random.