**P2- Qüestionari sessió 2 - Anàlisis dels protocols Telnet, FTP, HTTP i HTTPS**

**Preguntes TCP**

**1.**

La connexió de TCP es pot filtrar a partir del procés de handshake. D’aquesta manera ens sortiran tots els paquets d’establiment de la connexió.

El handshake té tres estats, SYN, SYN-ACK i ACK. Per tant, si utilitzem els filtres tcp.flags.syn == 1 i tcp.flags.ack == 1, trobarem el procés d’establiment de la connexió.

A més depenent del protocol que utilitzem per establir la connexió, podem utilitzar un filtre o un altre. El filtre és “tcp.port==XX”.

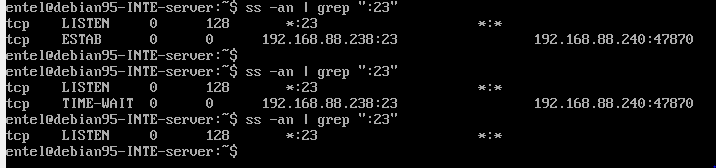
On XX és el port que utilitza el protocol, per exemple telnet utilitza el port 23, però el protocol ftp utilitza el 20 i el 21.

**2.**

LISTEN: Quan el servidor està a l’espera de què clients es connectin.

ESTAB: Quan la connexió s’ha establert

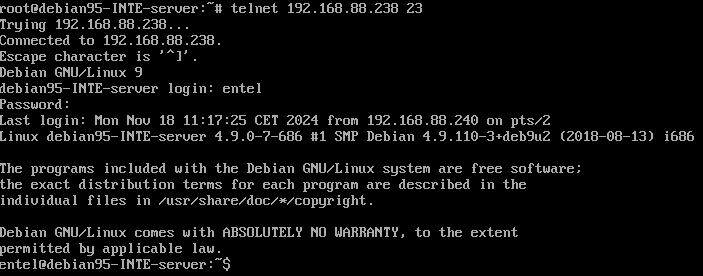
TIME-WAIT: Quan el client es desconnecta, espera un temps fins que no arribi cap resposta d’aquest. Després ja acaba i torna a estar solament en Listen.

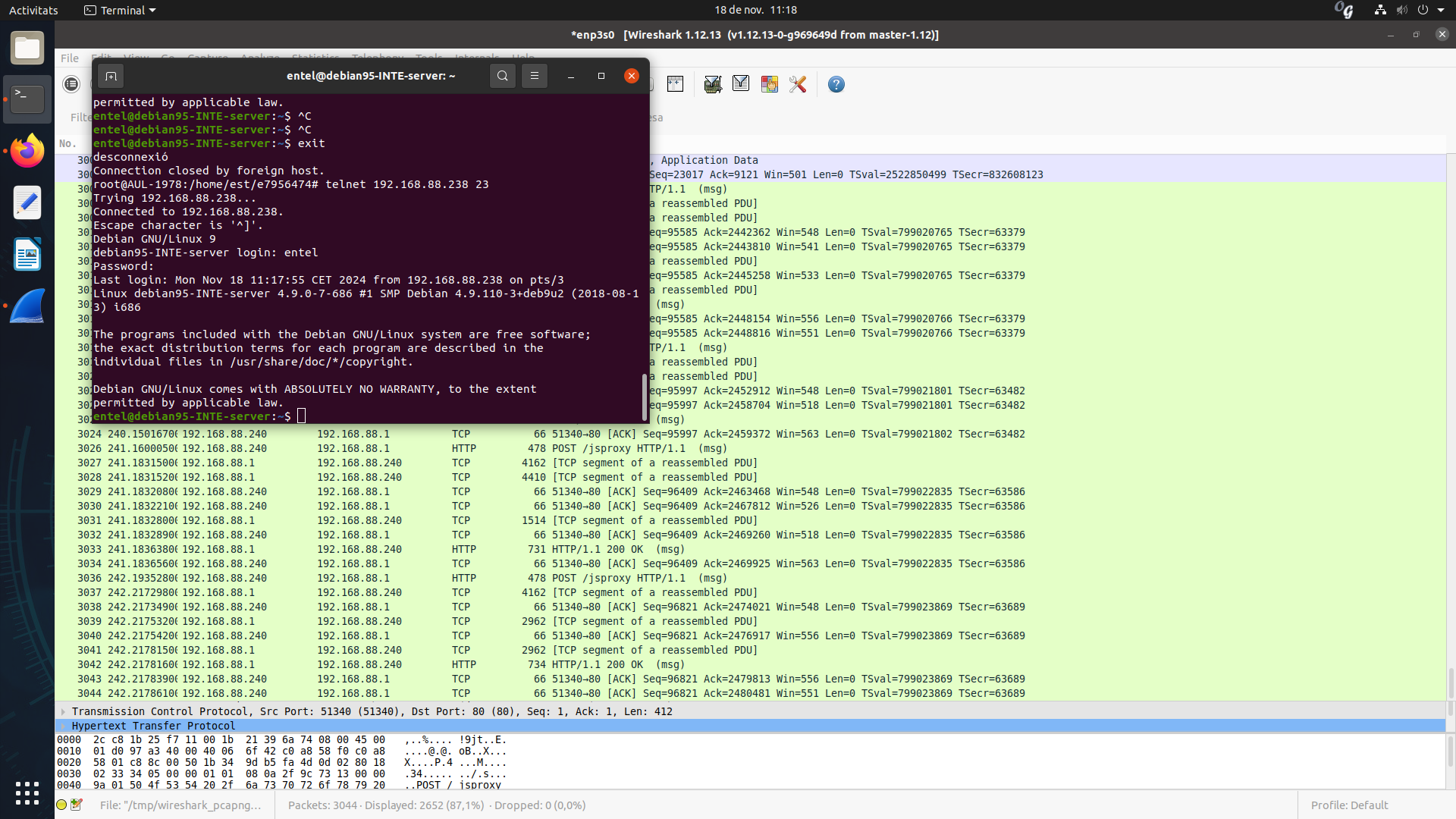


**Preguntes Telnet**

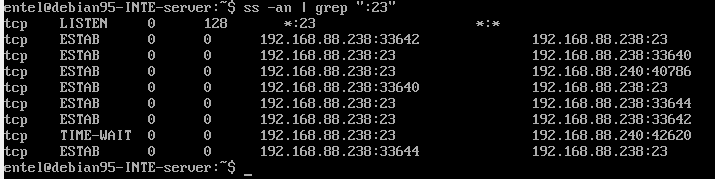
**3.**

Si, accepta més d’un client, ho podem comprovar entrant al servidor des de diferents terminals o ordinadors.



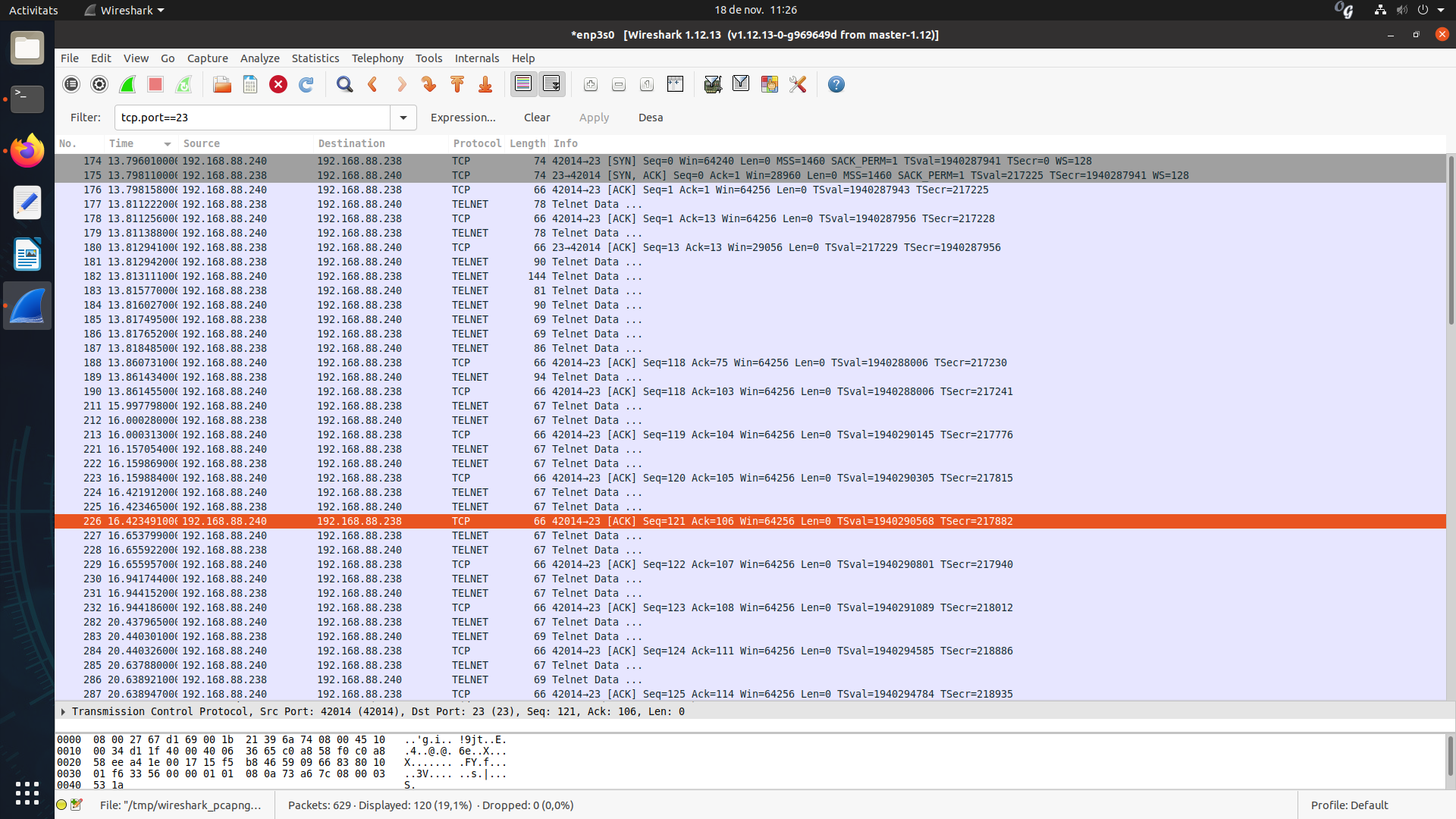


Utilitzem la comanda ss -an | grep “:23” per veure els clients connectats al port 23, què és el port telnet, cada client connectat genera una connexió TCP.

Mirant la captura podem diferenciar els estats estab que són clients que s'han connectat i estats time\_wait que són clients que potser s’han desconnectat o han caigut.

**4.**

A una connexió telnet, les comandes s’escriuen directament a la nostra consola, i aquestes s’envien al servidor i s’executen a la terminal del servidor. Al wireshark es pot veure que quan executem una comanda, es transfereixen les dades de la comanda en el paquet “Telnet Data …”



**Preguntes FTP**

**7.**

FTP utilitza dues connexions. Una connexió de control que es manté activa durant tota la connexió per enviar missatges entre servidor i client. I una connexió de dades que s’activa quan s’han de transferir dades i es desactiva quan s’ha acabat la transferència.

**8.**

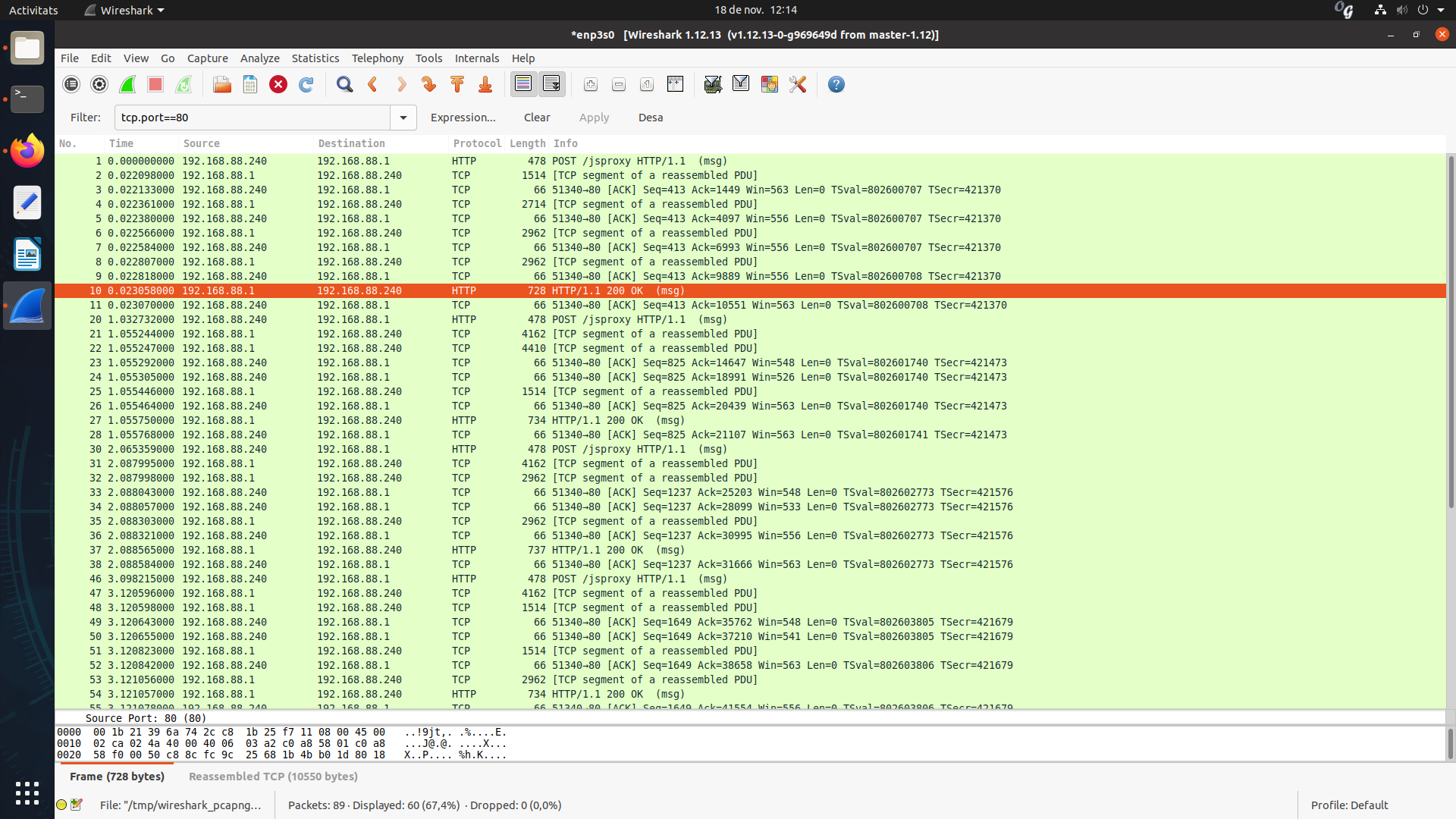
En les connexions FTP el port 20 és qui s’encarrega d’establir aquesta connexió de dades.

**Preguntes HTTP**

**9.**

Sí, és possible fer més d’una petició HTTP. Amb la versió HTTP/1.1, no es tanca la connexió TCP quan es fa una petició, d’aquesta manera permet que es rebin més peticions en una mateixa connexió.

**10.**

****

La versió que es fa servir es HTTP / 1.1.

El mètode utilitzat és el mètode post que serveix per enviar dades al servidor.

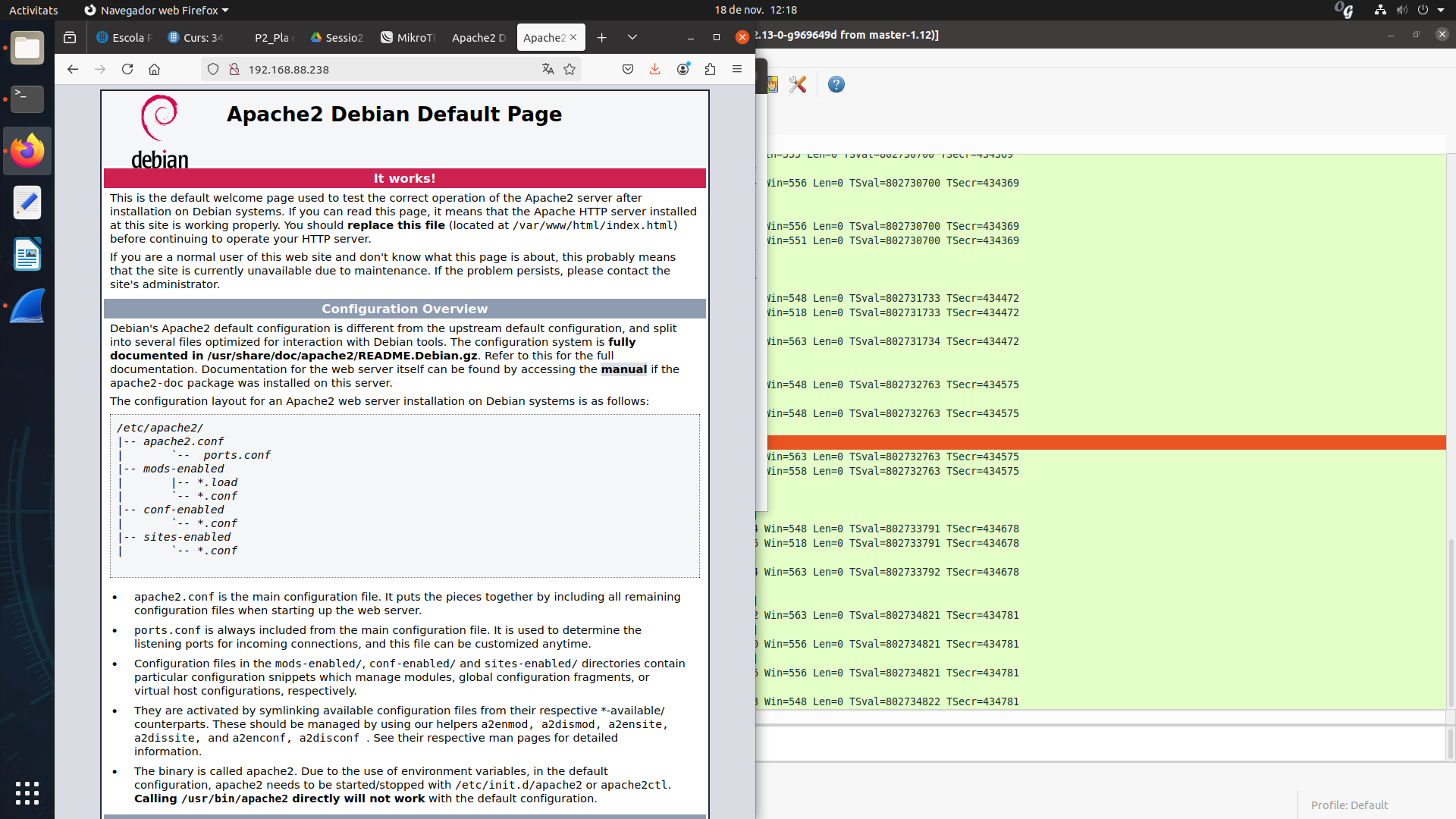
Codis de resposta:

200 significa que tot ha sortir correctament

En cas de que surti algun 400 o més gran, com 404, es un error

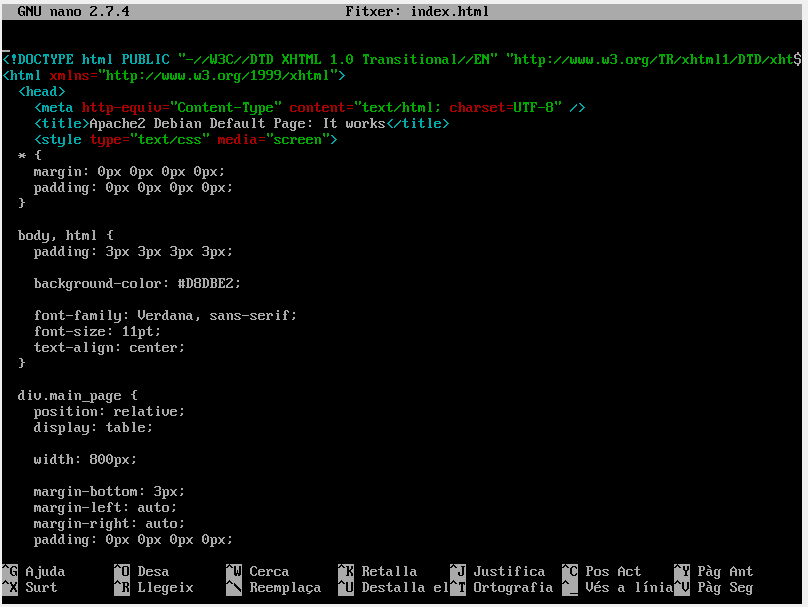
**11.**

Quan obrim la pagina del servidor Web de la nostra VM, ens surt un pagina relacionada amb Debian.



Aquesta té recursos de text, imatge i links.

Les URL relatives son els directoris on estan aquests recursos, per exemple el text que com ens indica la pagina se'ns genera un arxiu index.html a /var/www/html/index.html

****

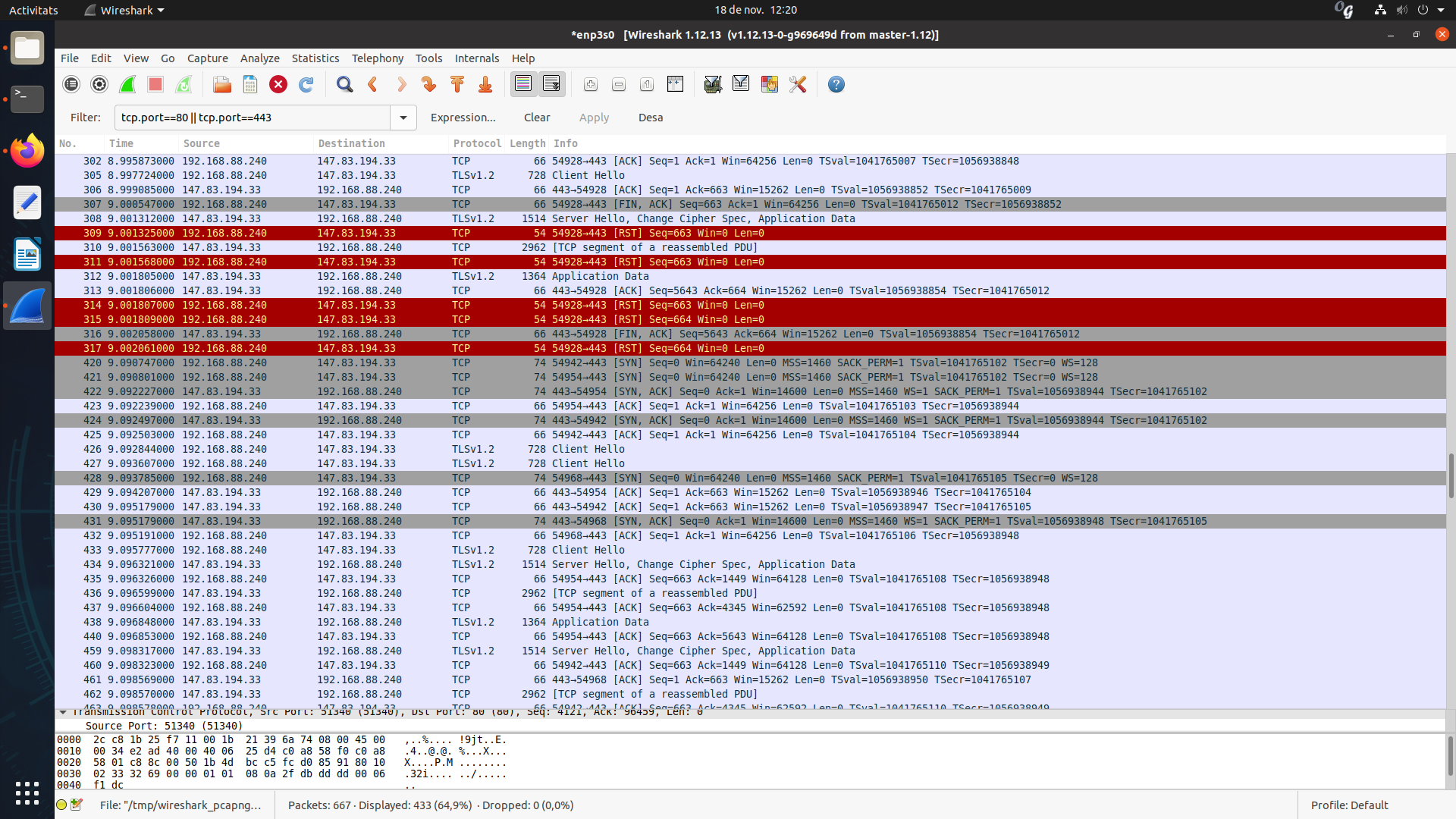
I les URL absolutes són les URL que ens mostren el contingut de la pagina web, com pot ser la que surt en el fitxer index.html, “<http://www.w3.org/1999/xhtml>”.

**12.**

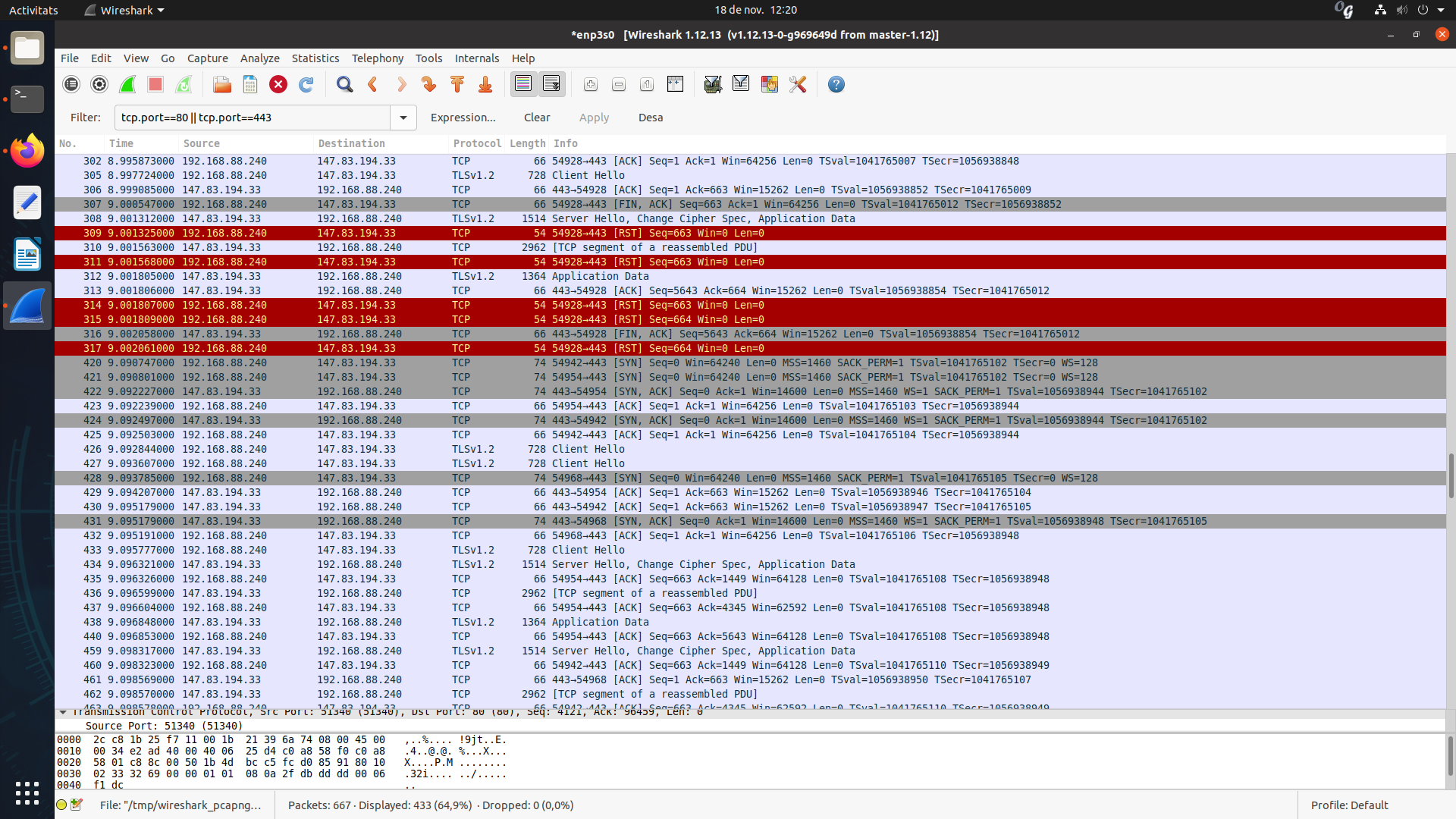
En cas que no es trobi un recurs al servidor, aquest retorna un codi de resposta HTTP d'error, en comptes de retornar un 200 com a codi de resposta, que significa que tot a sortir correctament, retornarà un codi de resposta més gran de 400, possiblement 404.

**Preguntes HTTPS**

**13.**



A la captura de wireshark es pot veure com alguns paquets intenten connectar-se a TCP a partir del port 443, que és el port que utilitza HTTPS, la versió segura de HTTP. El missatge que ens redirigeix són els missatges [SYN], i els missatges [SYN,ACK] són la resposta del servidor. I per últim el missatge ACK, que són la confirmació de què ens hem connectat a la versió segura del servidor.

**14.**

Per comprovar que la connexió és segura amb Wireshark, podem filtrar pel port 443, que és l'estàndard per HTTPS. HTTPS utilitza el protocol TLS per xifrar les comunicacions, i podem identificar una connexió segura observant el handshake TLS, amb missatges com "Client Hello" i "Server Hello".