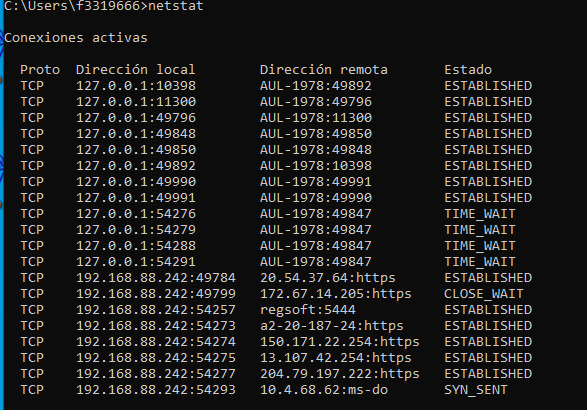
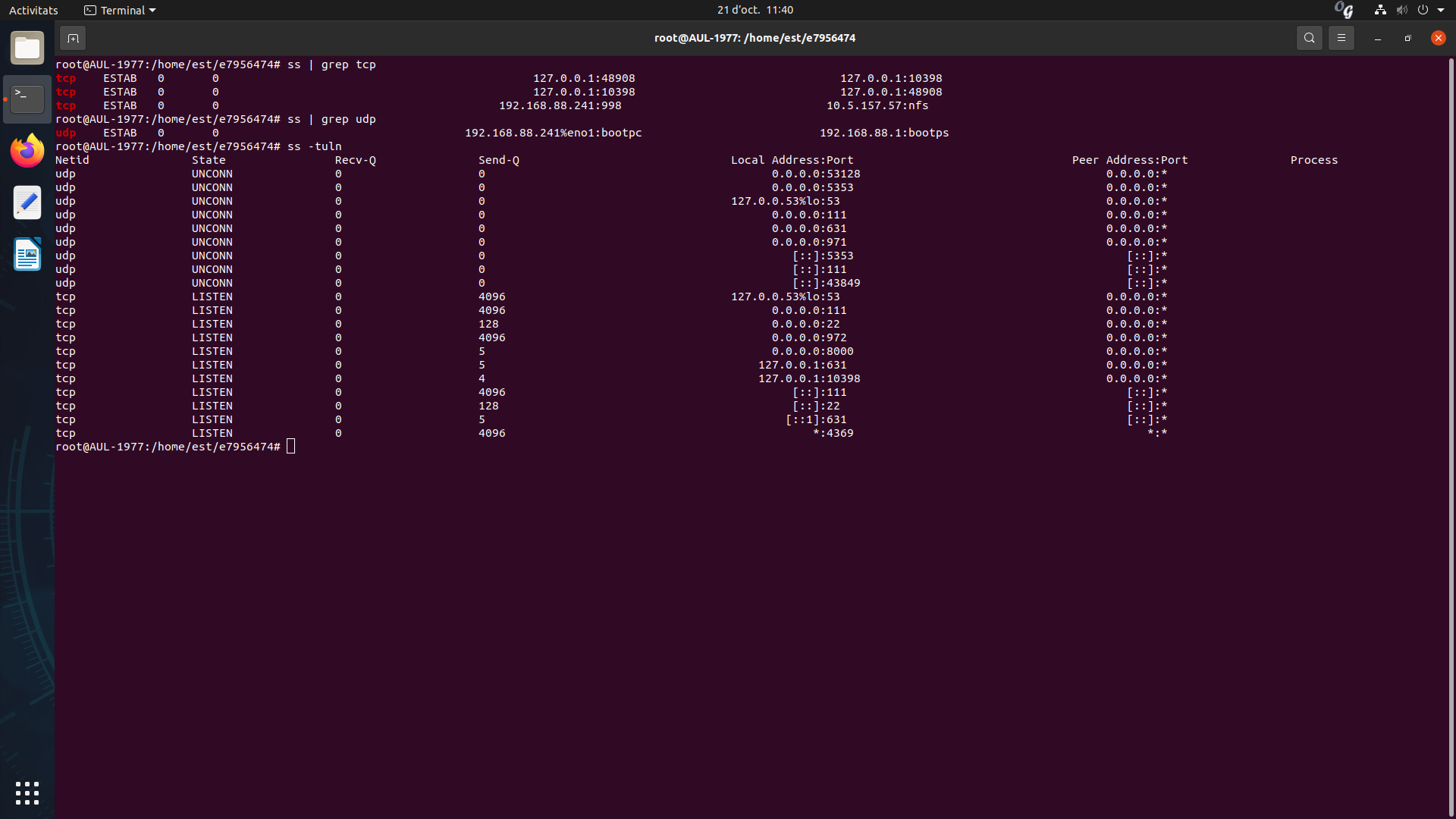
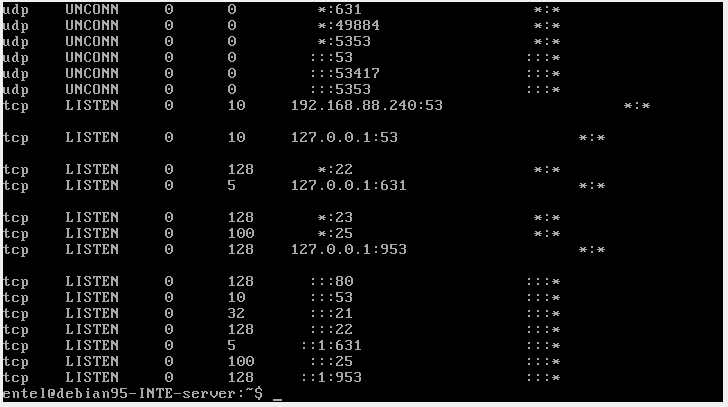
**P2-Qüestionari sessió 1 -Serveis, ports i connexions: anàlisi en local i escaneig de ports**

**1.**

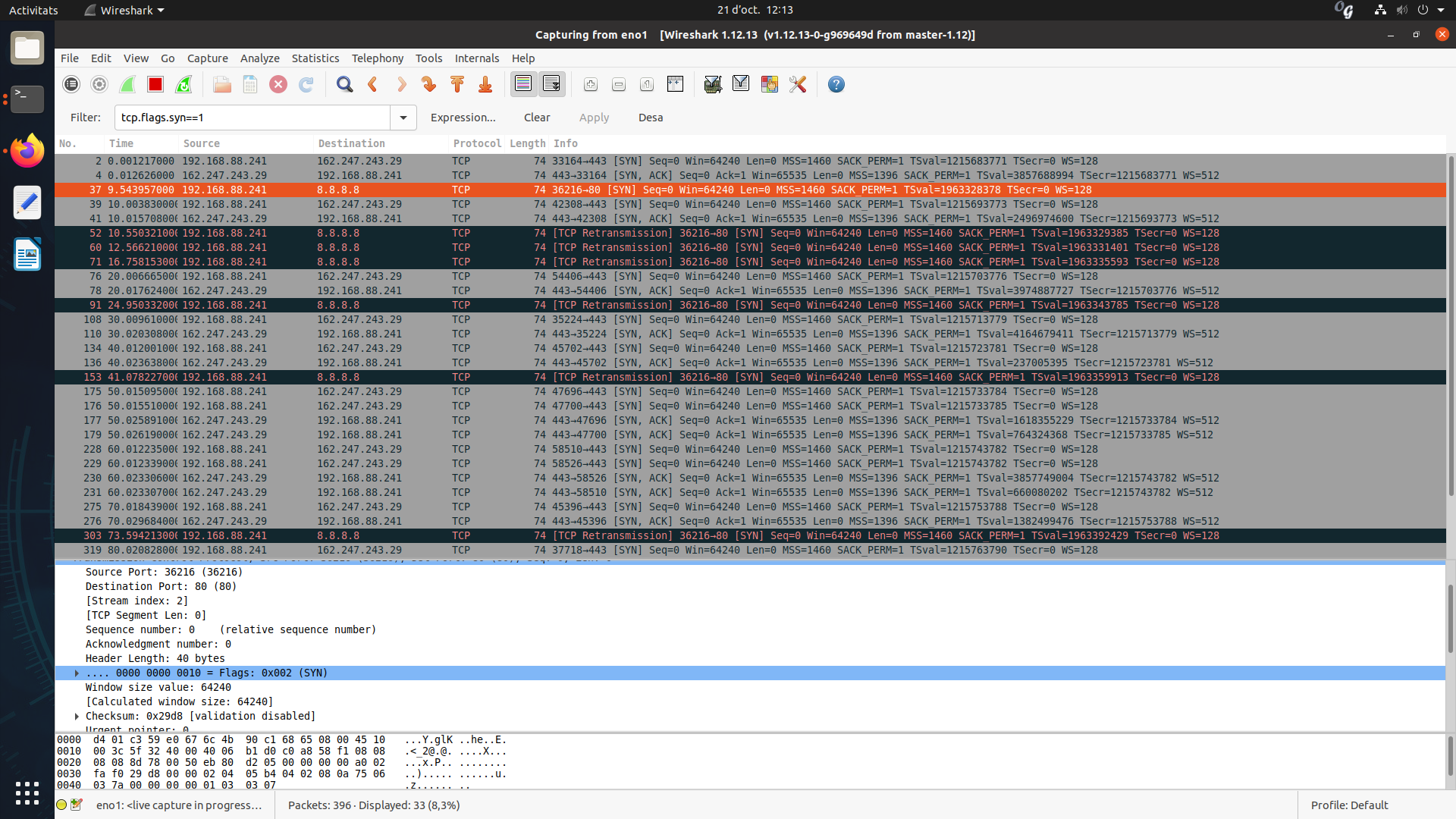
Amb netstat, ho escrivim a la cmd de Windows i ens surt el següent:



A linux, fem servir la comanda ss. Per a que ens surtin les connexions TCP, ho filtrem amb -tuln. On la t es per a tcp, la u es a udp i la l es per filtrar les que estan en estat ‘listen’.

Per últim a la máquina virtual, fem també servir ss igual que a linux.

**2. Quin protocol de transport es fa servir quan fem un escaneig de ports amb telnet?**

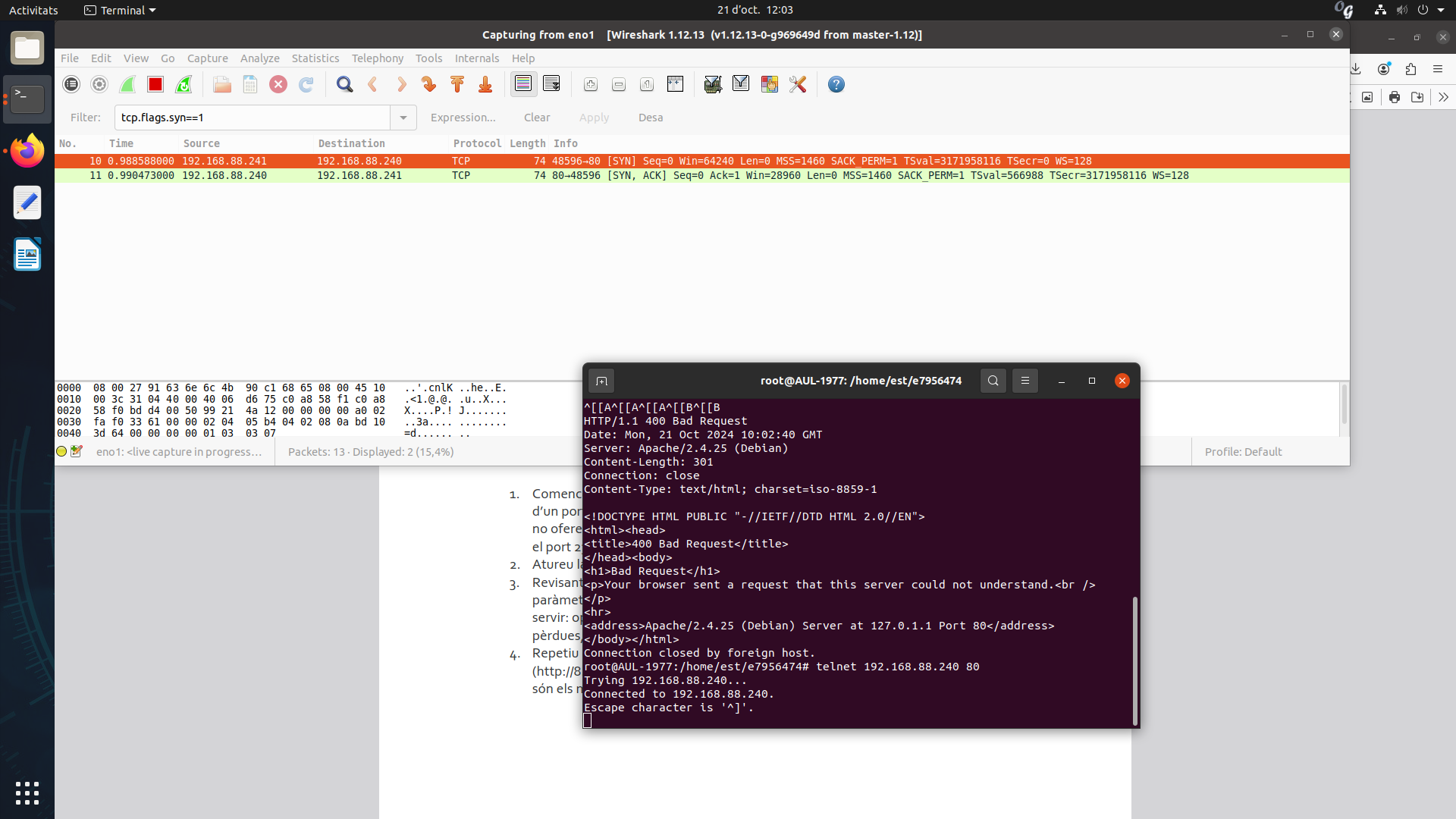
Quan fem servir telnet a la terminal i a la vegada capturem a Wireshark, podem veure que el protocol que es fa servir és TCP.

**3.**

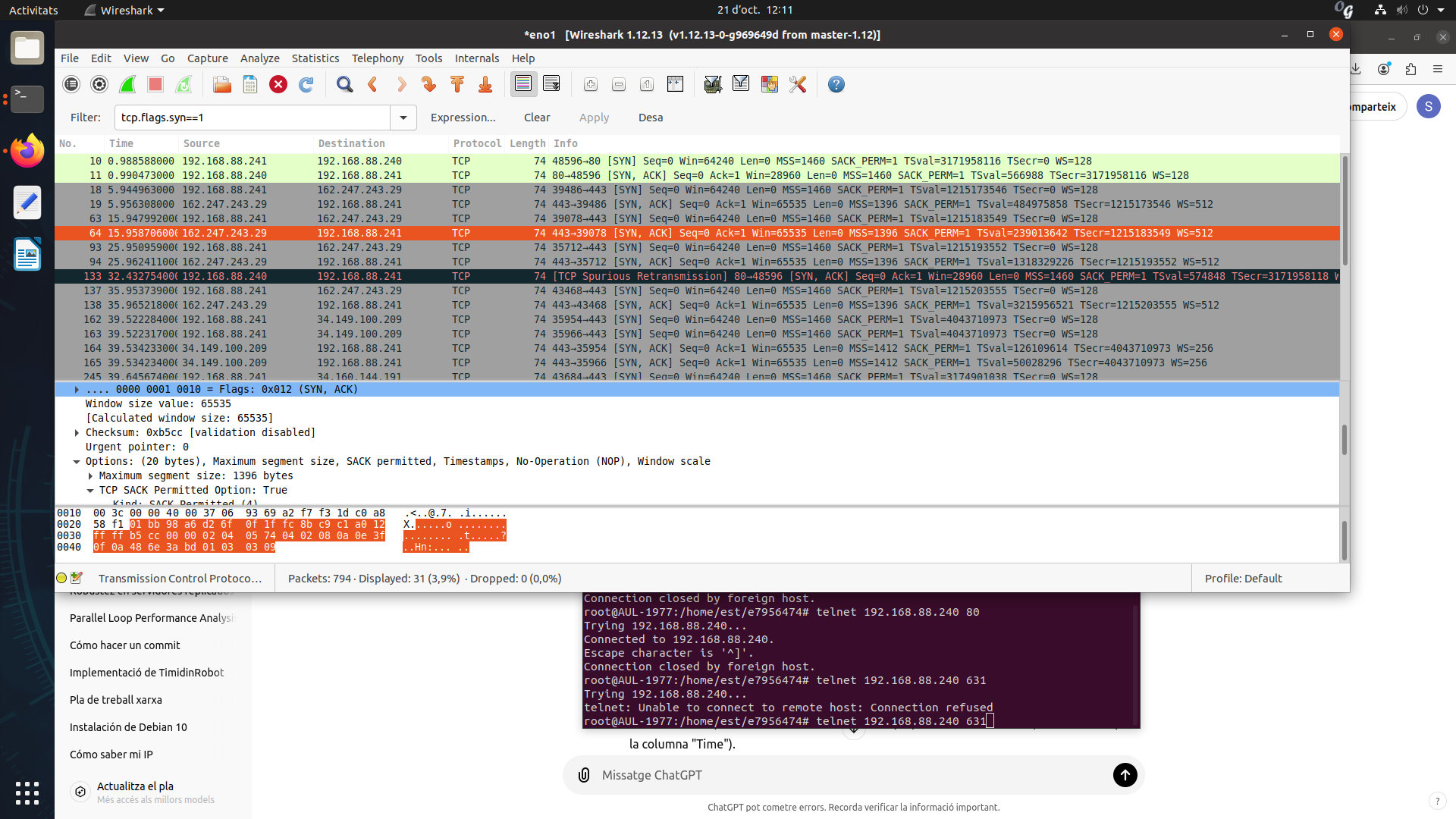
Telnet es un protocol que només accepta connexions amb el protocol TCP, per tant tots els ports UDP no es podran escanejar amb telnet.

A més, hi ha alguns serveis TCP que estan filtrats i tampoc són acceptats per telnet.

**4.**

Si el port està obert, a la terminal ens surtirá això:  


Significará que ens hem connectat al servidor de la màquina virtual que hem configurat.

Podem veure a WireShark que quan ho connectem surtem els següents tipus de missatges [SYN], [SYN-ACK]

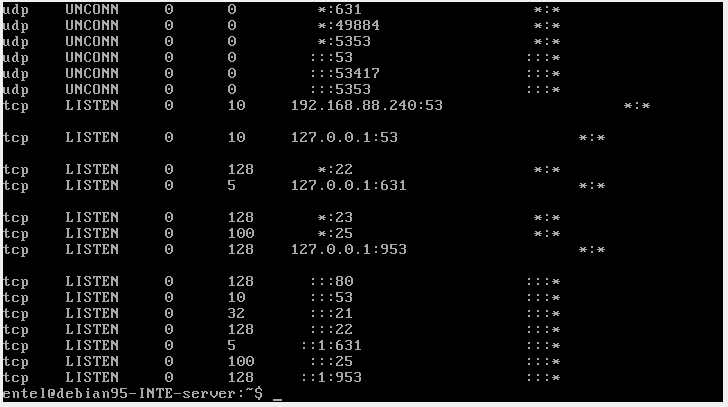
El missatge [SYN] l’envia l’ordinador a la maquina virtual buscant una connexió.

El missatge [SYN-ACK] és el missatge que envia la VM, quan ha reconegut al host i ha rebut la seva petició de connexió.

Si la connexió s’ha completat (no en el nostre cas) sortirá un missatge [ACK], que envía l’ordinador Linux al host dient que la connexió està establerta i es poden començar a intercanviar missatges.

**5.**

Com hem vist a la primera pregunta, amb la comanda ss podem veure els ports que estan en estat LISTEN.

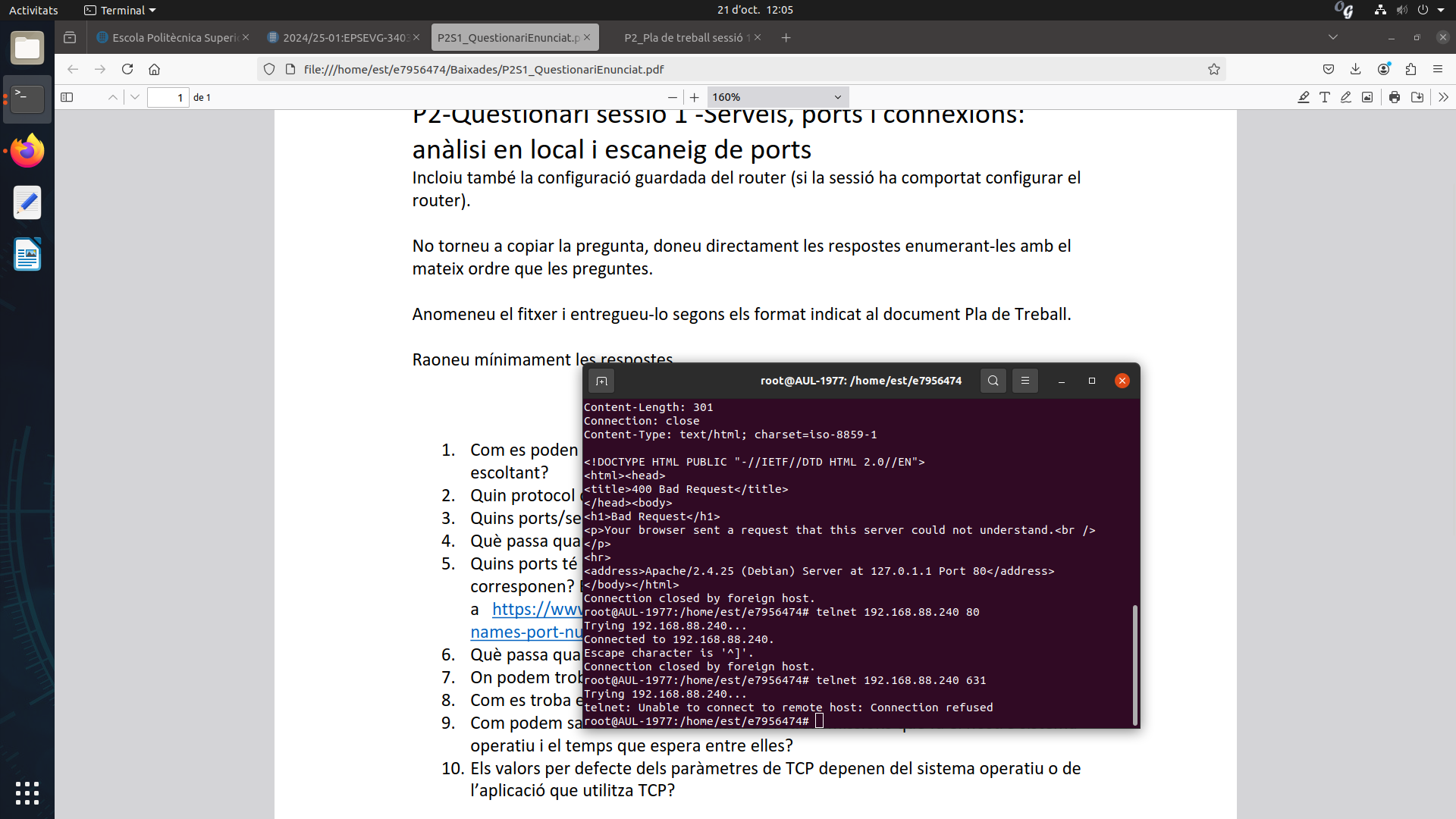


Ports:

* 53: port utilitzat per DNS, i pot utilitzar tant el protocol UDP com el TCP.
* 22: utilitzat per SSH (Secure Shell), utilitza el protocol TCP.
* 631: Utilitzat per IPP,
* 23: Utilitzat per a telnet,
* 25: Utilitzat per a SMTP (Simple Mail Transfer Protocol) i utilitza el protocol TCP
* 953: Utilitzat per BIND (DNS control port) i utilitza el protocol TCP.
* 80: Utilitzat per a HTTP (Hypertext Transfer Protocol) i utilitza TCP.
* 21: Utilitzat per FTP (File transfer protocol) i utilitza TCP.

**6.**

Si utilitzem telnet amb un port que no està obert, la connexió no funcionará i no ens podrem connectar al servidor. Per exemple ho fem amb el port 631.



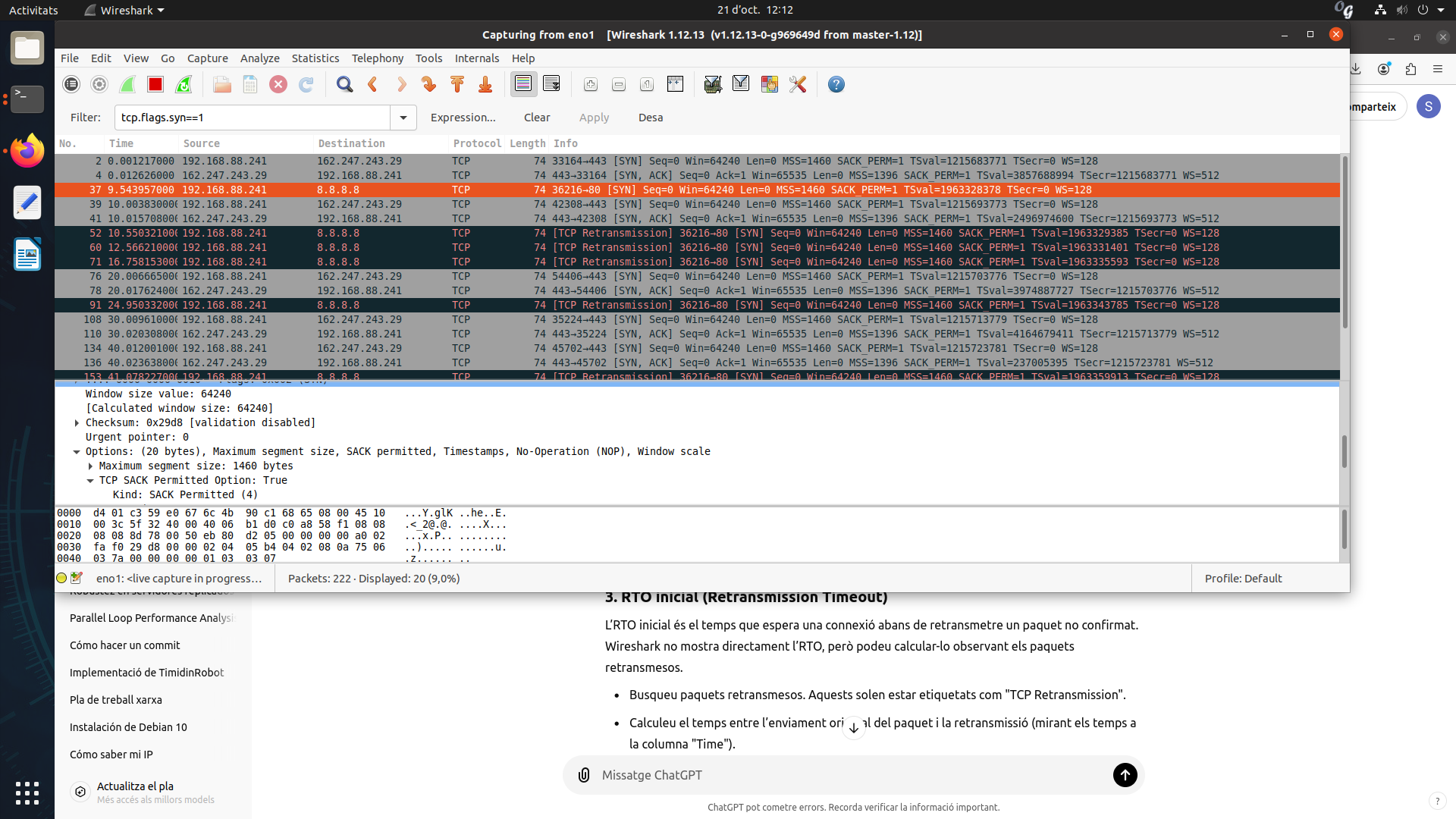
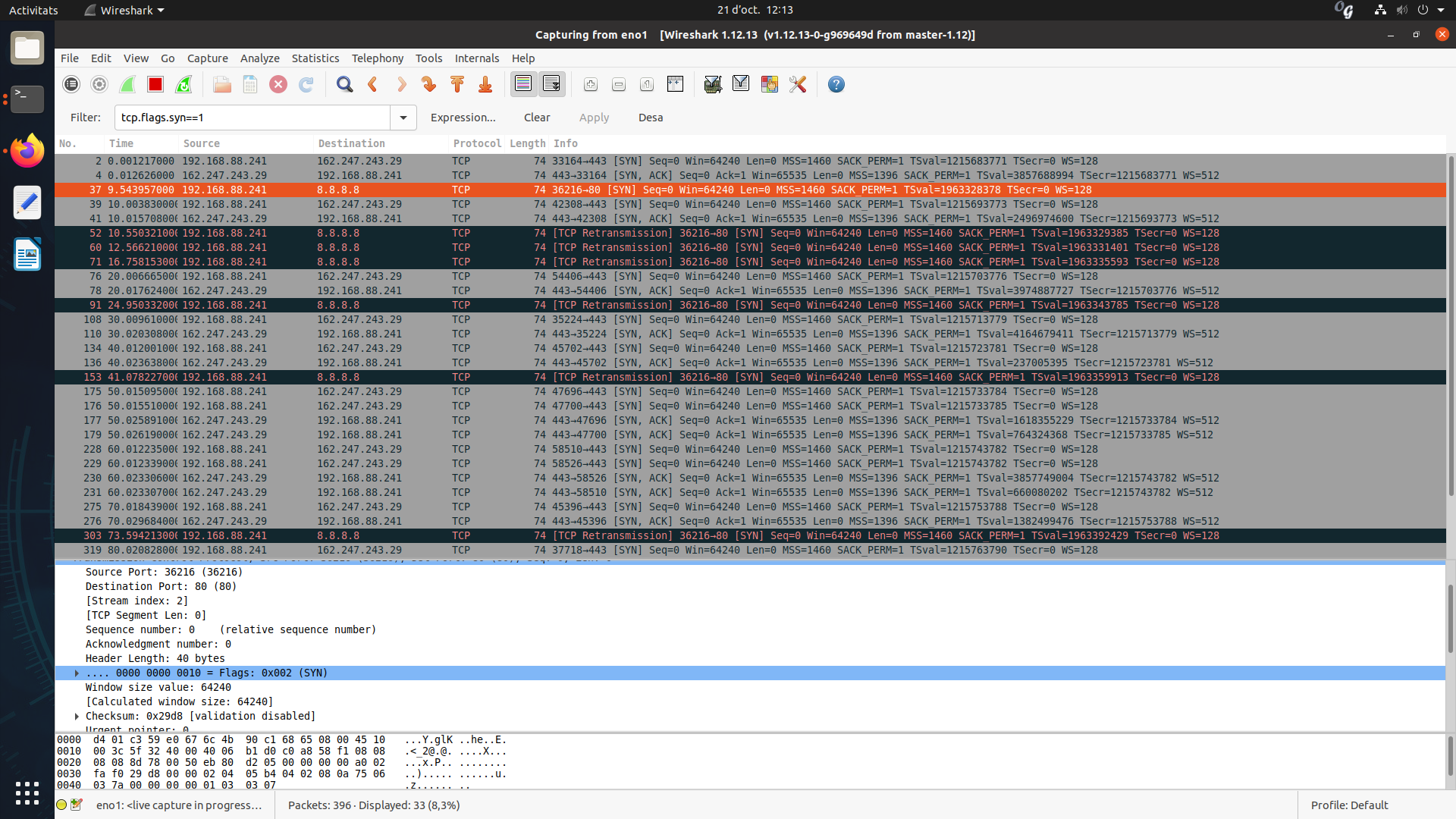
Ens surt un error ja que no es pot connectar a través d’aquest port.

Si ens fixem al wireshark, tindrem un missatge SYN, on l’ordinador linux intenta connectarse al servidor.

Pero en comptes de obtenir un missatge SYN-ACK de part del servidor, hauriem de rebre un missatge tipus RST. Aquest avisa al client que el port per on s’ha intentar establir una connexió està tancat i no es posible connectar-se.

**7.**

Dins d'un paquet SYN que envia el host A al host B, es poden observar diverses opcions TCP que s'envien per establir les característiques de la connexió. Aquestes opcions es troben dins de la capçalera del paquet TCP.



La longitud màxima de segment és de 1460 bytes, la qual cosa especifica la mida màxima que el host A pot gestionar en un sol segment TCP.  
Timestamps: permeten que TCP calculi l'RTT per al control de la congestió.  
SACK permitted: indica que permet els SACK (Selective Acknowledgment).

**8.**

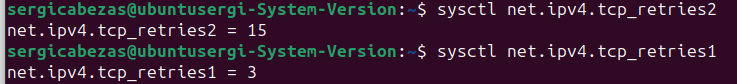
El RTO (Retransmission Timeout) inicial en TCP no es mostra directament en els paquets, però es calcula basant-se en el valor de RTT. Aquest valor no sempre està disponible al començament de la connexió. En aquests casos, el sistema operatiu sol utilitzar un valor de RTO inicial predeterminat, que generalment esta entre 1 i 3 segons. En el paquet SYN d’inici de la connexió, aquest valor de RTO inicial no és visible. No obstant això, un cop establerta la connexió, és possible veure el valor de RTT en paquets posteriors. A mesura que es transmeten i es reben dades, TCP ajusta dinàmicament el RTO en funció de les mesures de RTT observades, cosa que millora l'eficiència de les retransmissions.

**9.**

Es pot saber a partir dels paràmetres TCP del sistema operatiu. En sistemes Linux, sol estar en els arxius següents /proc/sys/net/ipv4/tcp\_retries2 o tcp\_retries1 aquests valors els podem obtenir a partir de les següents comandes:

sysctl net.ipv4.tcp\_retries2 per obtenir el màxim de retransmissions

sysctl net.ipv4.tcp\_retries1 per obtenir el temps d'espera.



**10.**

Els valors per defecte dels paràmetres tcp depenen en gran manera del sistema operatiu la mida de la finestra el rto el nombre màxim de retransmissions depenen d'aquest, però pot veure's influït per aplicacions que en necessitin alguna modificació específica d'algun d'aquests paràmetres**.**