APUNTS:

*eth-trames*

*ip-datagrames*

*tcp-segments MSS-1460 bytes*

*Ethernet-1500 bytes*

Enviat dades hostB →ACKNOWLEDGMENT

ex: cada 4bytes enviar un ACK

ex: cada 8bytes…

cada x la connexió el tamany augmenta si la connexió va bé → tamany de finestra

inicial 1bytes

timeouts configurats so-> enviar a l'inici de connexió -> dacord amb els paràmetres de connexió

normalment 3seg -> veure Wireshark

C S (servidor caigut)

| --- SYN→- |

| timeout3 seg - retornar a fer SYN N vegades

| --- SYN→- |

| |

rto: retransmissió 0 → l’estableix el SO

**UDP:**

no connexió, no verifica connexió transporta info

Protocols DNS RIP, altres

Ports:

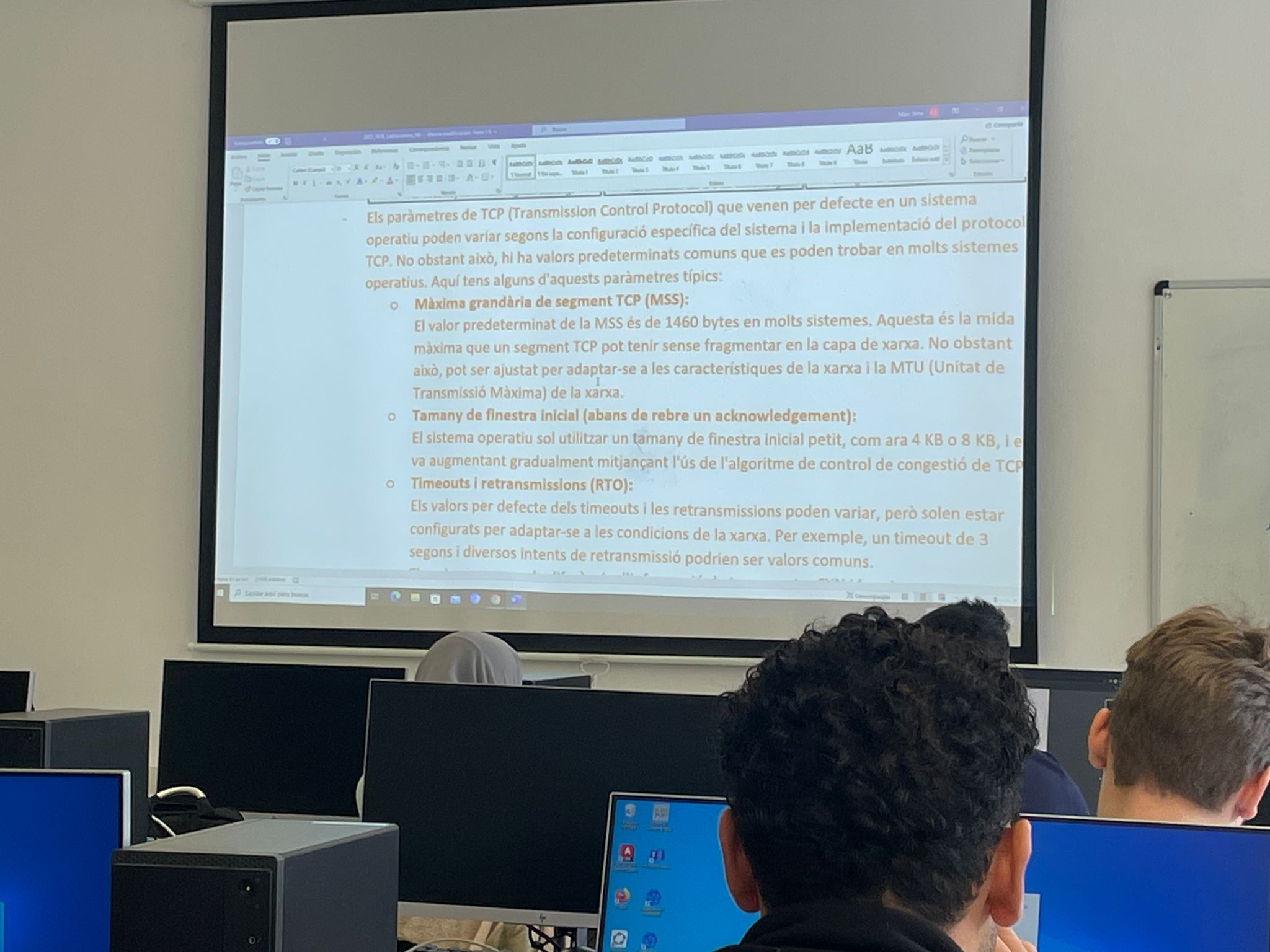
num associat dispositius amb IP de 0-65535 ports disponibles x dispositiu, NO ES FÍSIC

permeten tenir múltiples serveis i apps en el mateix dispositiu,

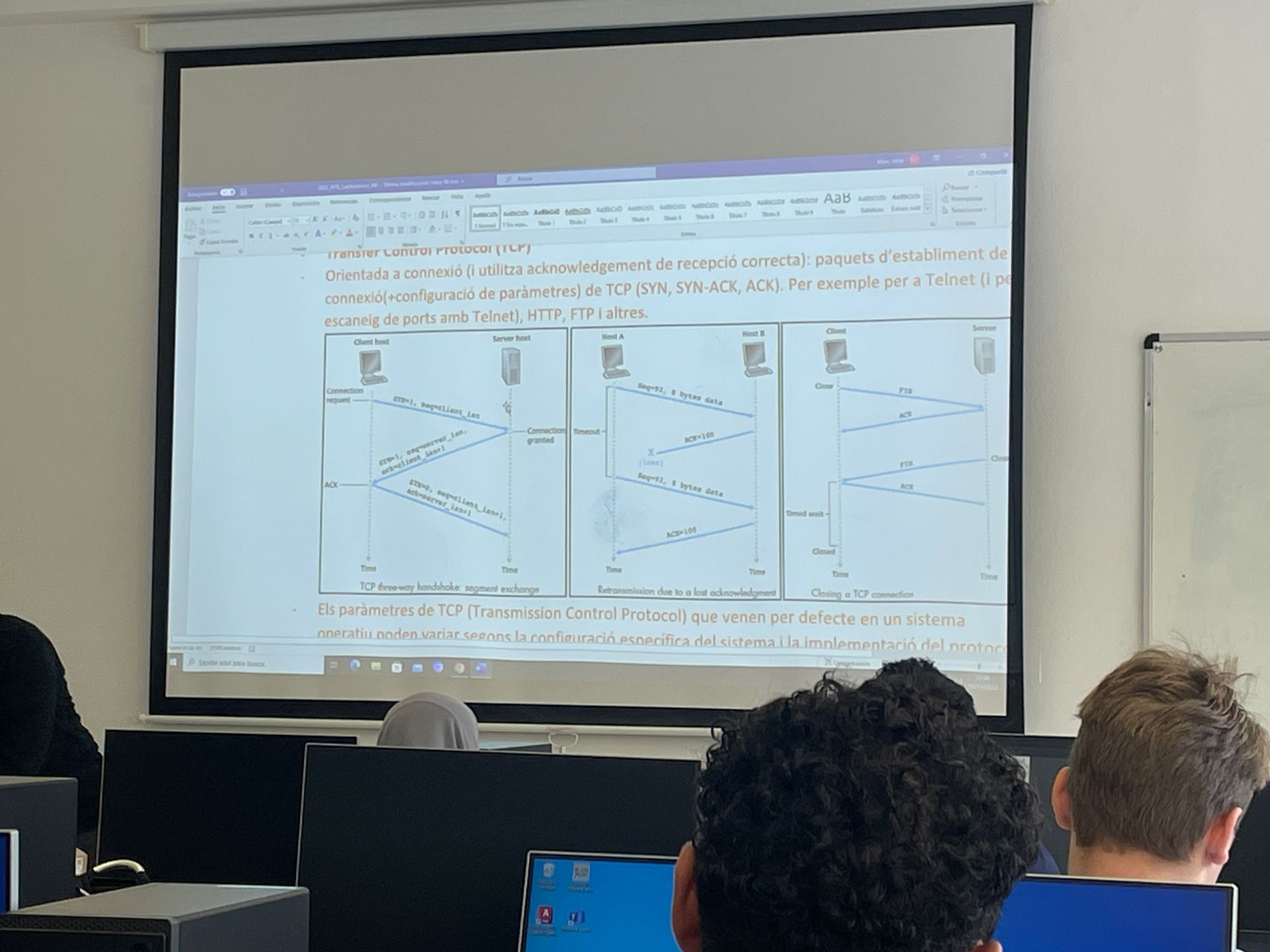
TCP:

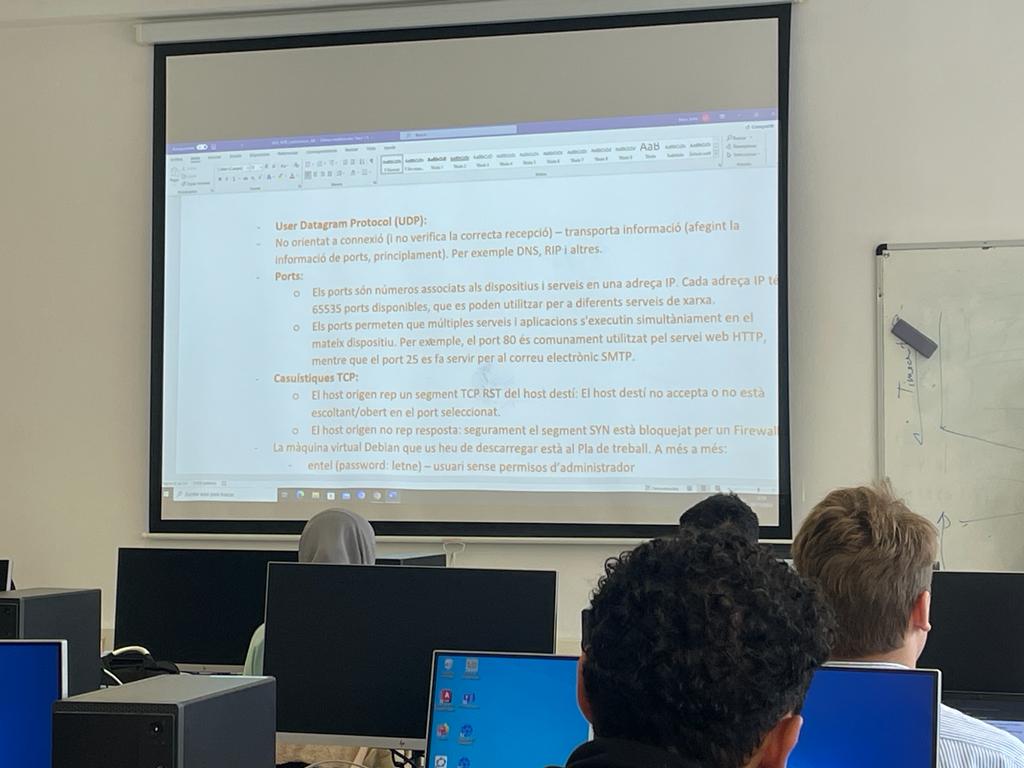
host origen rep segment TCP RST del host desti: desti no accepta o no escolta el port seleccionat

host origen no rep resposta: segment SYS bloquejat per un firewall



Els podem veure en la diferència de temps entre SYN i la primera retransmissió





* root (password: toor) - usuari administrador

**Primera part - Preparació de l'escenari**

1. Arrenqueu un dels dos PCs del laboratori amb Linux i l’altra amb Windows

2. Deixeu el router Mikrotik amb la seva configuració per defecte

3. Connecteu els dos PCs del laboratori als ports que formen la interfície bridge

4. Connecteu el port 1 del router a la xarxa de l’Escola

5. Canvieu el nom del’identificador de la xarxa Wi-Fi per un que pugueu reconèixer

6. Comproveu que teniu connectivitat entre els dos PCs.

7. Descarregueu-vos la imatge de la màquina virtual (VM) en el PC que heu

arrencat amb Windows. Importeu-la i arranqueu-la amb Virtual Box

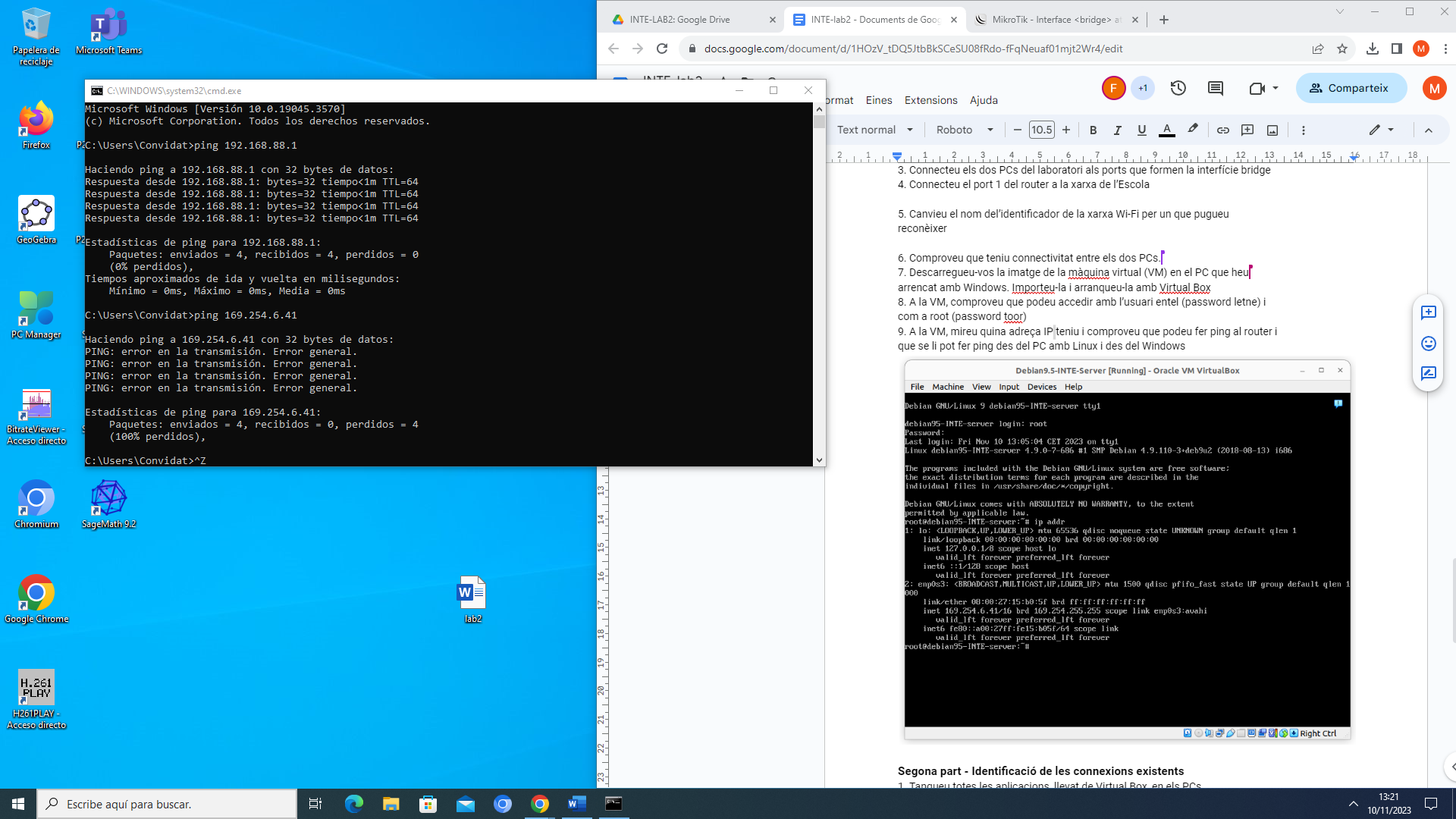
8. A la VM, comproveu que podeu accedir amb l’usuari entel (password letne) i

com a root (password toor)

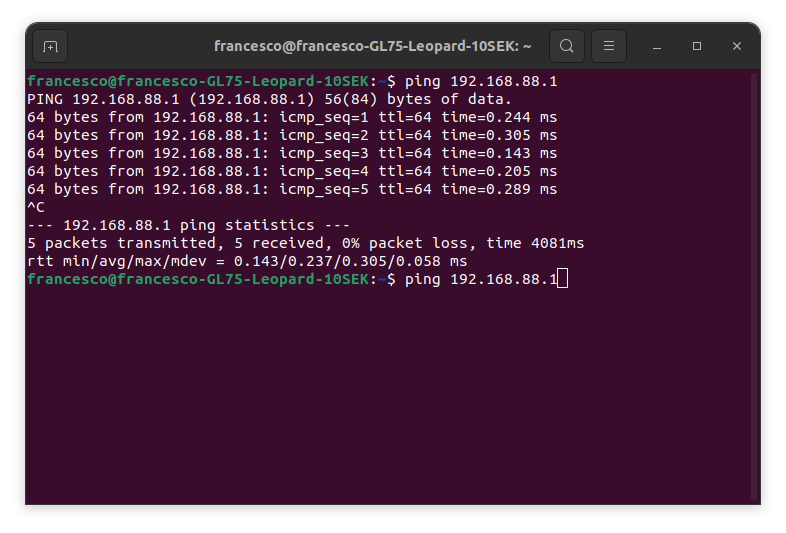
9. A la VM, mireu quina adreça IP teniu i comproveu que podeu fer ping al router i

que se li pot fer ping des del PC amb Linux i des del Windows

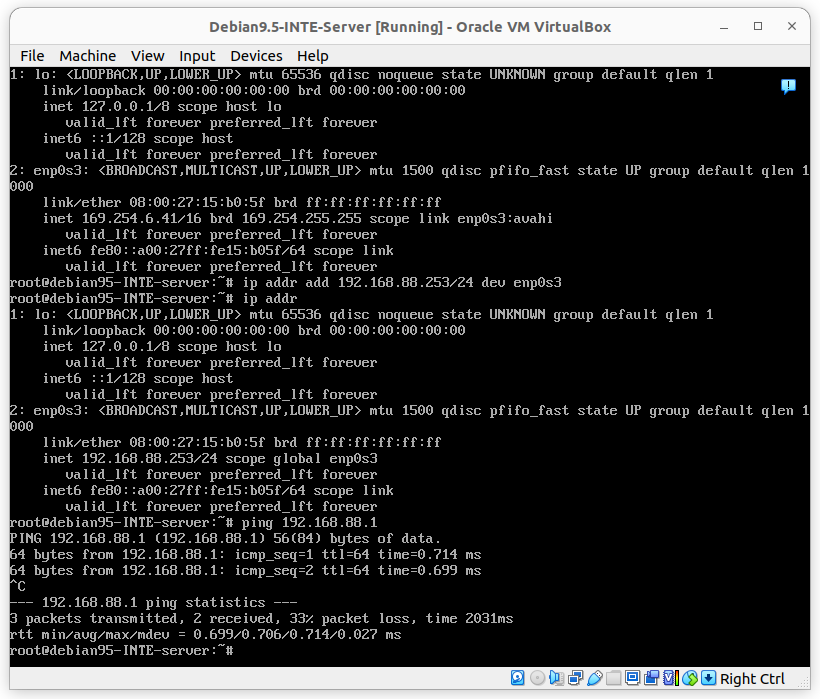
ping des de windows:



ping des de linux:



ping i ip addr des de VM:



**Segona part - Identificació de les connexions existents**

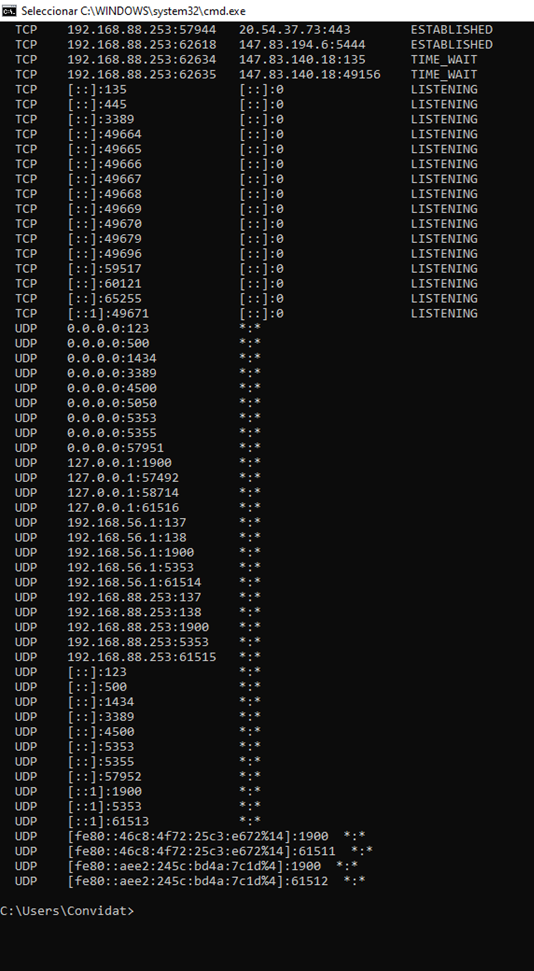
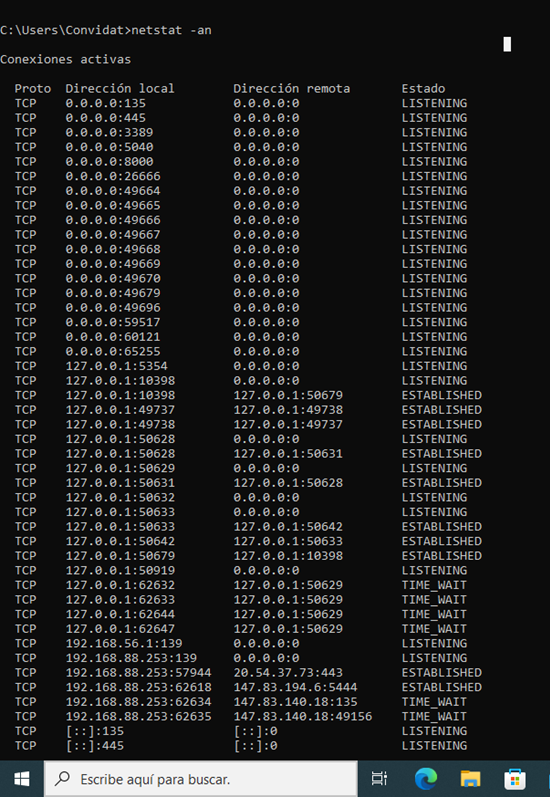
1. Tanqueu totes les aplicacions, llevat de Virtual Box, en els PCs.

2. Utilitzant netstat (o ss en Linux) en els PCs i la VM mireu:

1. Llista de connexions TCP

2. Llista de connexions UDP

WINDOWS:



LINUX:

VIRTUAL BOX:

3. Llista de ports TCP i UDP que estan a l’escolta (anoteu-los pel cas de la VM)

VIRTUAL BOX:

3. Compareu la informació pels 3 casos (Windows 10, Ubuntu i VM) i fixeu-vos en les diferències

4. A partir de la informació anterior identifiqueu quins serveis TCP/IP està corrent la VM.

5. Al PC amb Linux, al vostre portàtil i smartphone, busqueu les connexions que

teniu actives i, si cal obrint i tancant aplicacions, mireu a quins

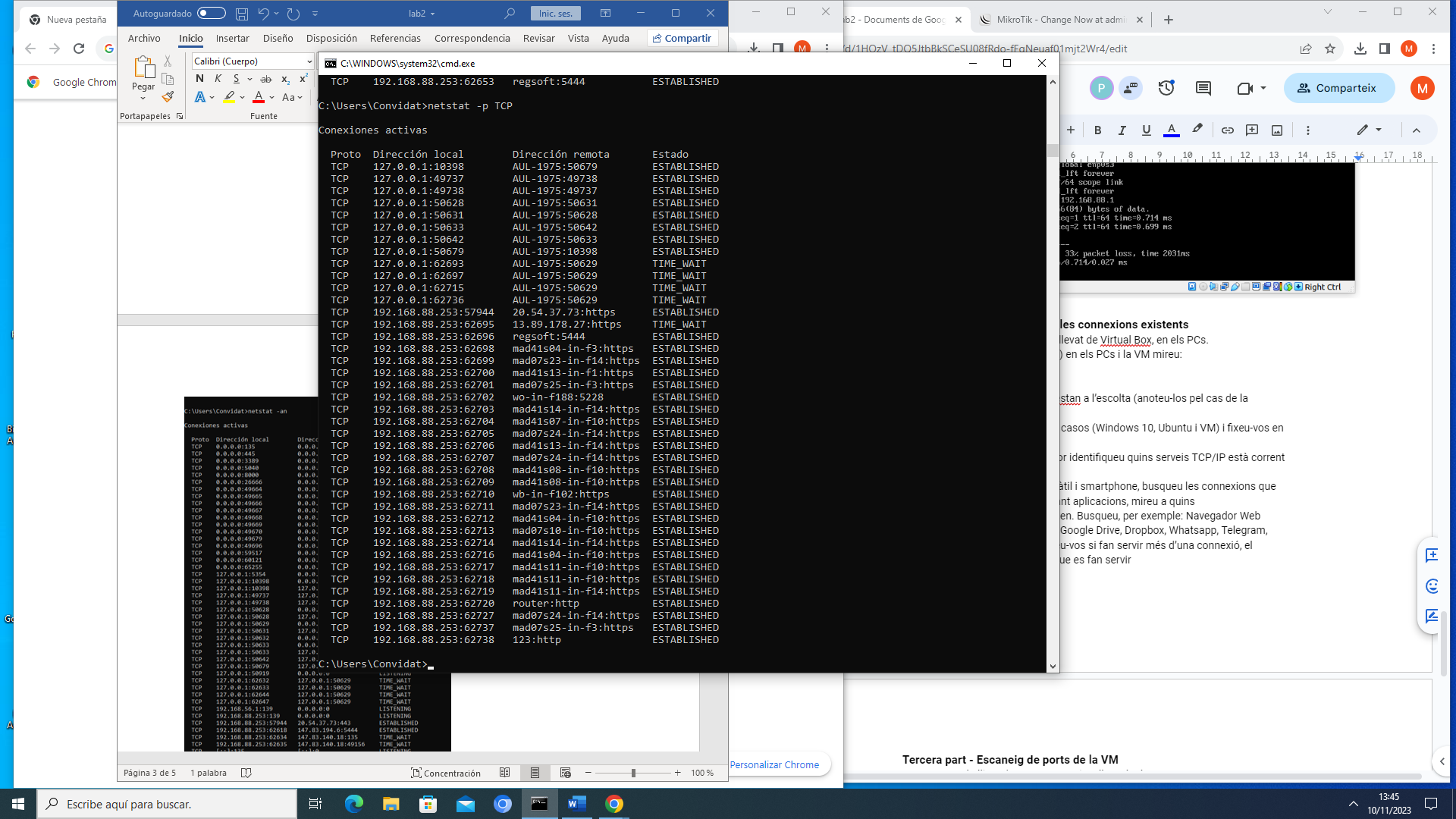
processos/aplicacions corresponen. Busqueu, per exemple: Navegador Web

(Chrome, Safari, Firefox, Edge,...), Google Drive, Dropbox, Whatsapp, Telegram,

Instagram,...En tots els casos fixeu-vos si fan servir més d’una connexió, el

protocol de transport i els ports que es fan servir

WINDOWS amb chrome obert:

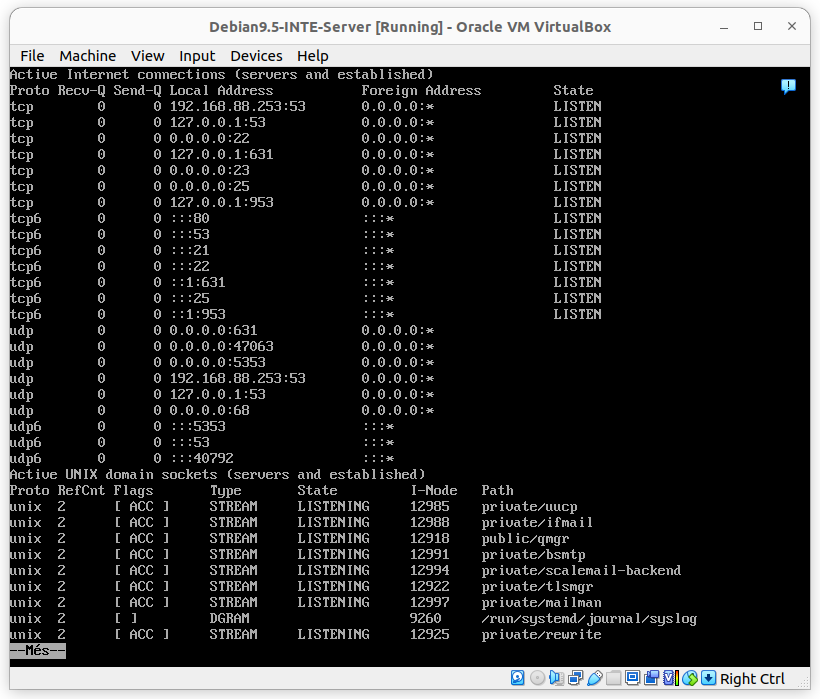


LINUX chrome:

MÒBIL: no app

**Tercera part - Escaneig de ports de la VM**

1. Recupereu la llista de ports que tenia a l’escolta la VM



2. Des d’uns dels PCs amb Linux, poseu a capturar Wireshark i després, obriu una

consola i escriviu “telnet” deixeu un espai en blanc, poseu la IP de la màquina

virtual, un altre espai en blanc i després el port que voleu veure si està actiu i

doneu-li a enter. Per exemple: “telnet 192.168.88.10 25”.

PORT 25 WIRESHARK:

PORT NO OBERT 20 wireshark:

3. Repetiu la operació per tots els ports de la llista fins el 80 inclòs, i per un que no

hi sigui

4. Compareu el que veieu a la consola i al Wireshark per cada cas. Mireu per cada

cas com podem esbrinar si el port està obert o no.

5. Repetiu l’escaneig de ports fent servir ara una eina que l’automatitzi com ara la

que hi ha l’app “IP Tools” o nmap si teniu Linux al vostre portàtil.

**Quarta part - Determinació de paràmetres per defecte de TCP**

1. Comenceu una captura Wireshark nova en un dels PCs Linux i repetiu l’escaneig

d’un port d'una màquina d'Internet a un port obert. Per exemple, podeu

fer telnet 8.8.8.8 80.

2. Atureu la captura després d'un parell de minuts.

3. Revisant la captura identifiqueu i calculeu si cal, els valors dels següents

paràmetres de TCP que venen per defecte en el sistema operatiu que esteu fent

servir: opcions, valor de la finestra inicial, RTO inicial, evolució del RTO quan hi

ha pèrdues, nombre de retransmissions màxim en cas de pèrdues.

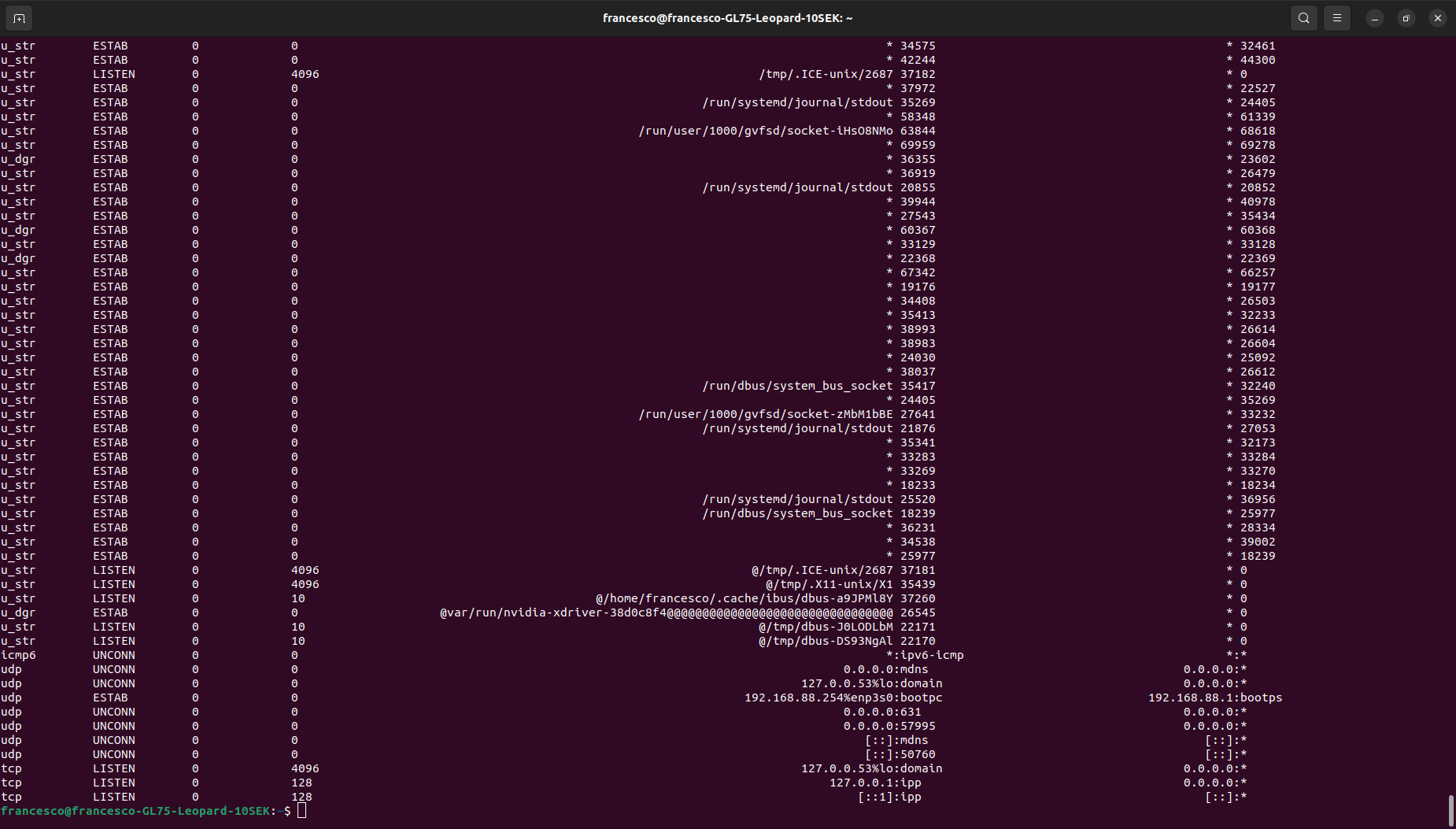
4. Repetiu el procés per amb una aplicació diferent, per exemple amb un navegador

(http://8.8.8.8:80) i un sistema operatiu diferent. Mireu si els valors per defecte

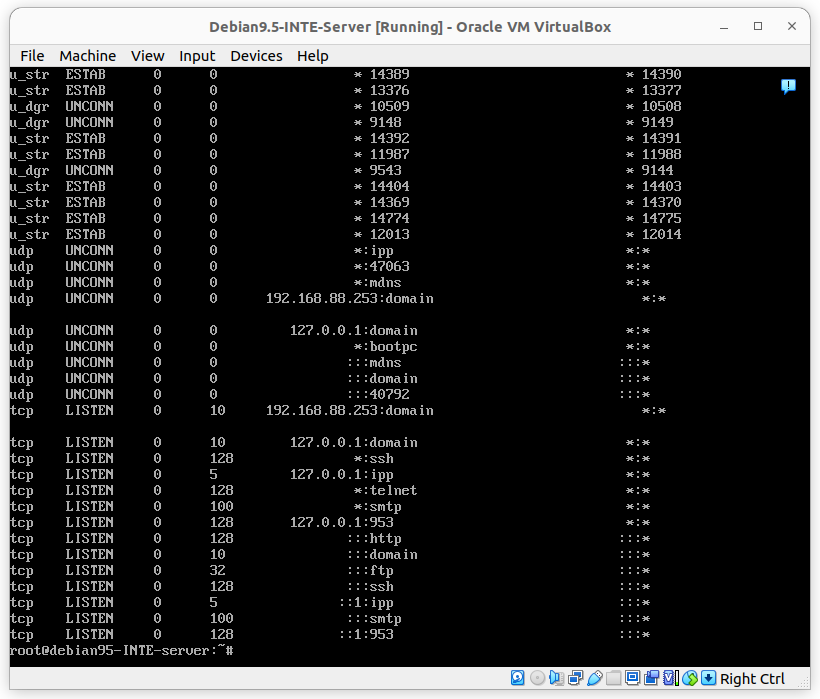
són els mateixos o no.

ss -a

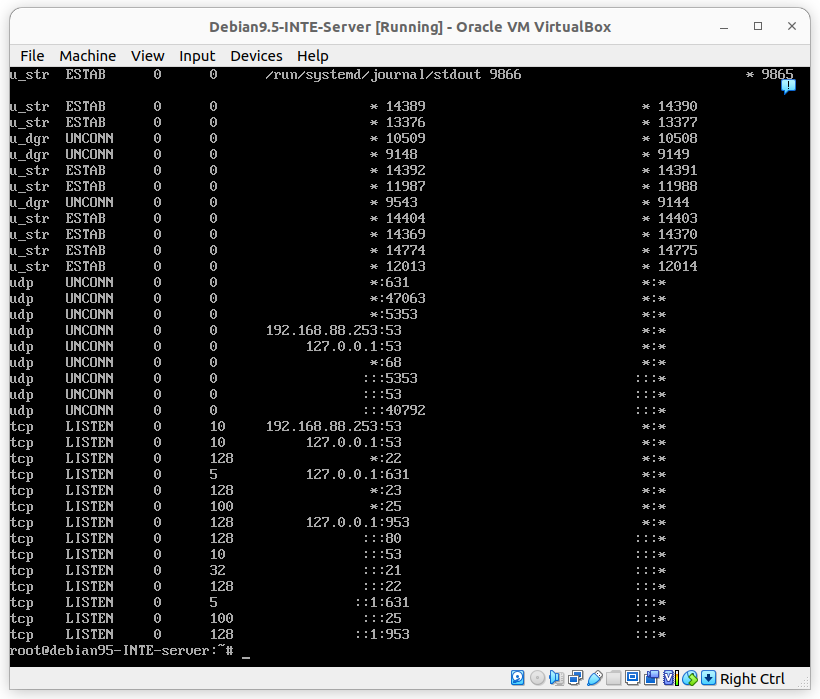




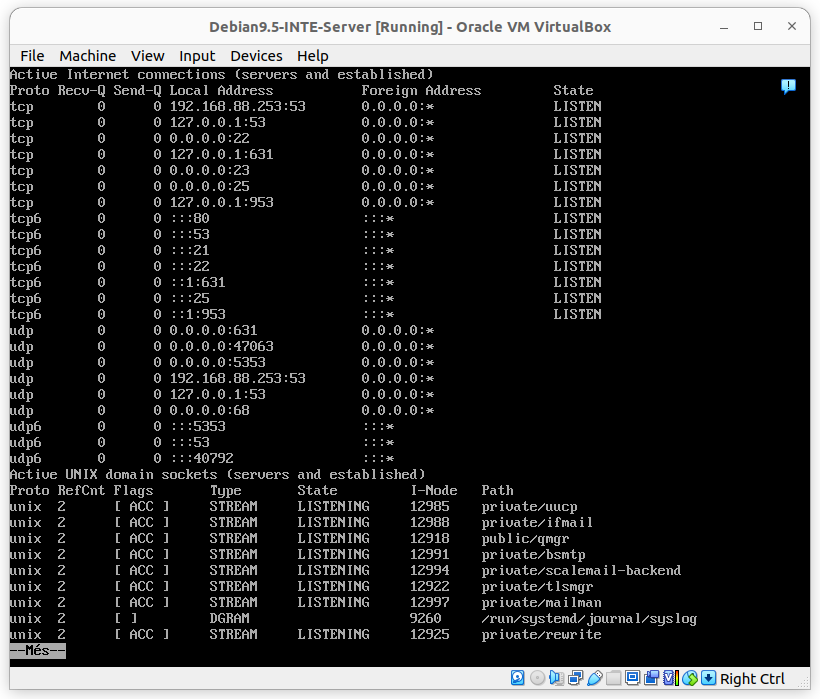
ss -a



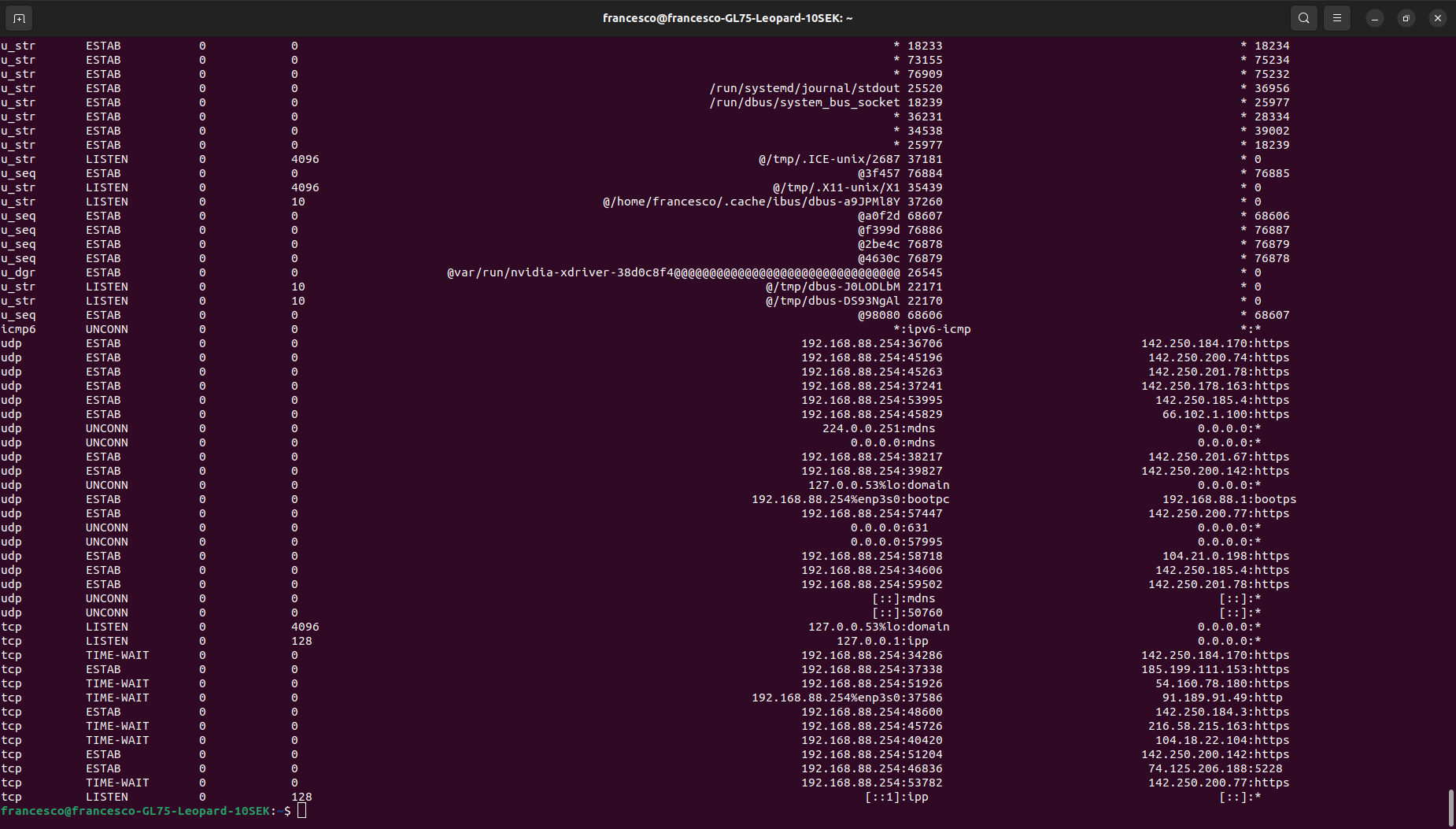
ss -an

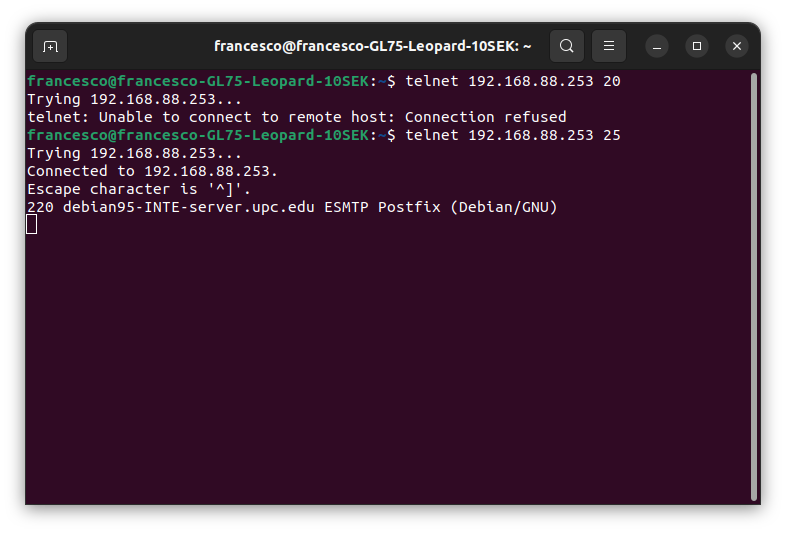


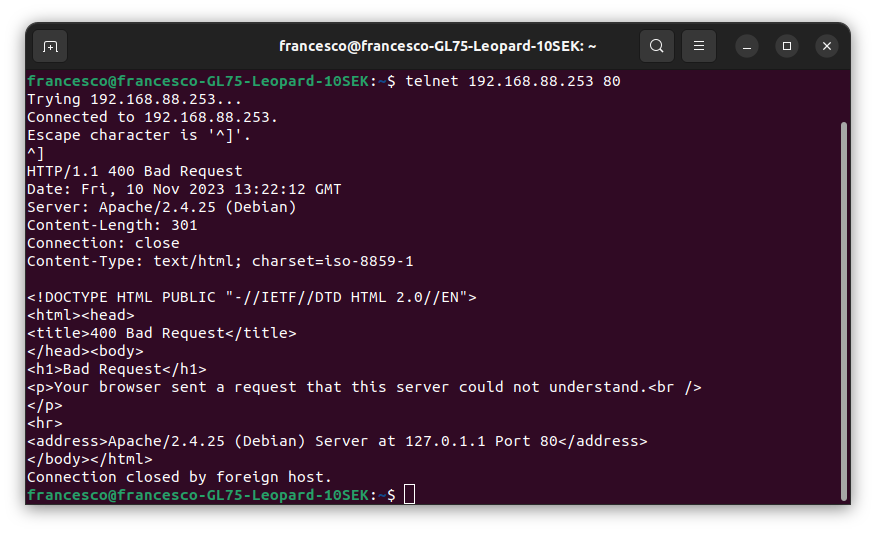
netstat -an|more

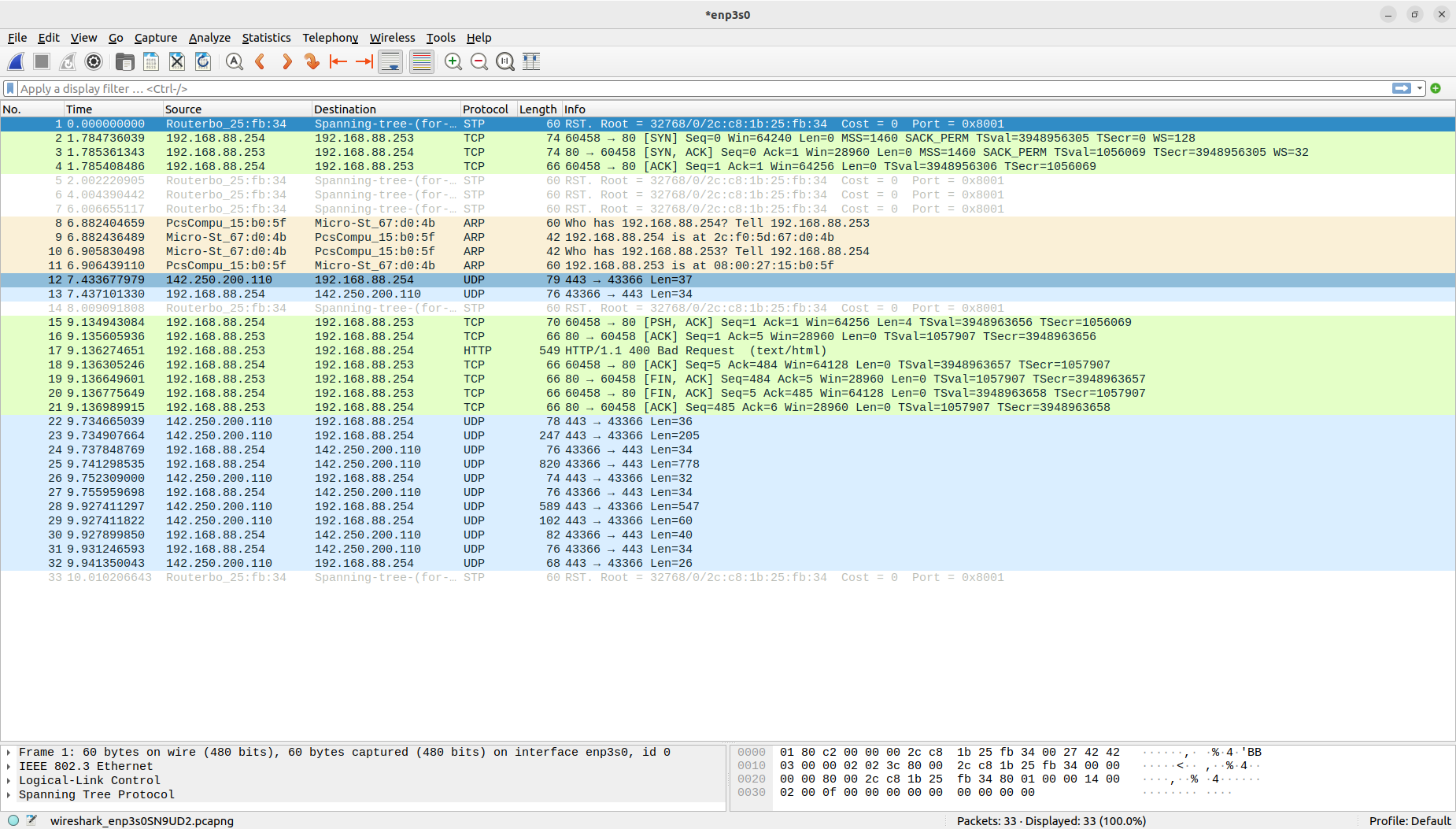


després d’obrir chorme (amb ss -a):



telnet:





Es fa amb el handshake en el 1r syn… (pregunta 6)

