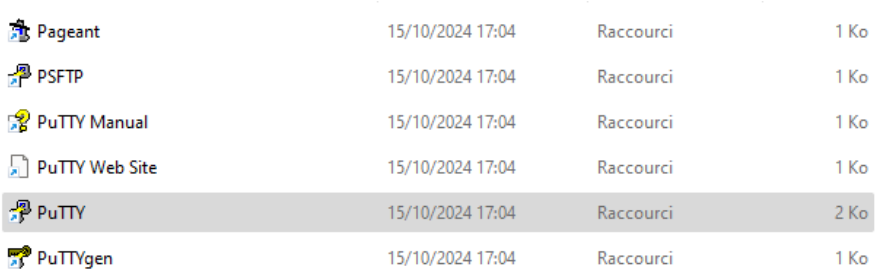
TP3 Les ports logiciels

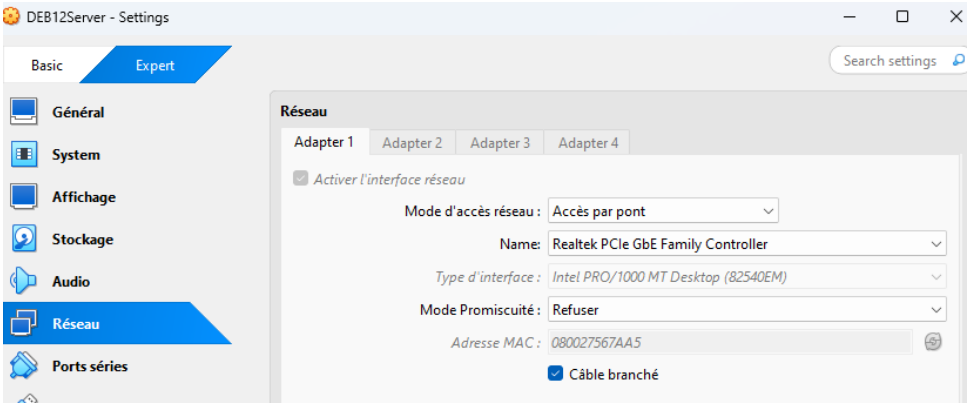
Table des matières

1. Connexion sécurisée à une machine Linux depuis un client SSH Windows.

Téléchargez et installez, depuis votre machine hôte, putty.exe 64 bits (putty.org).

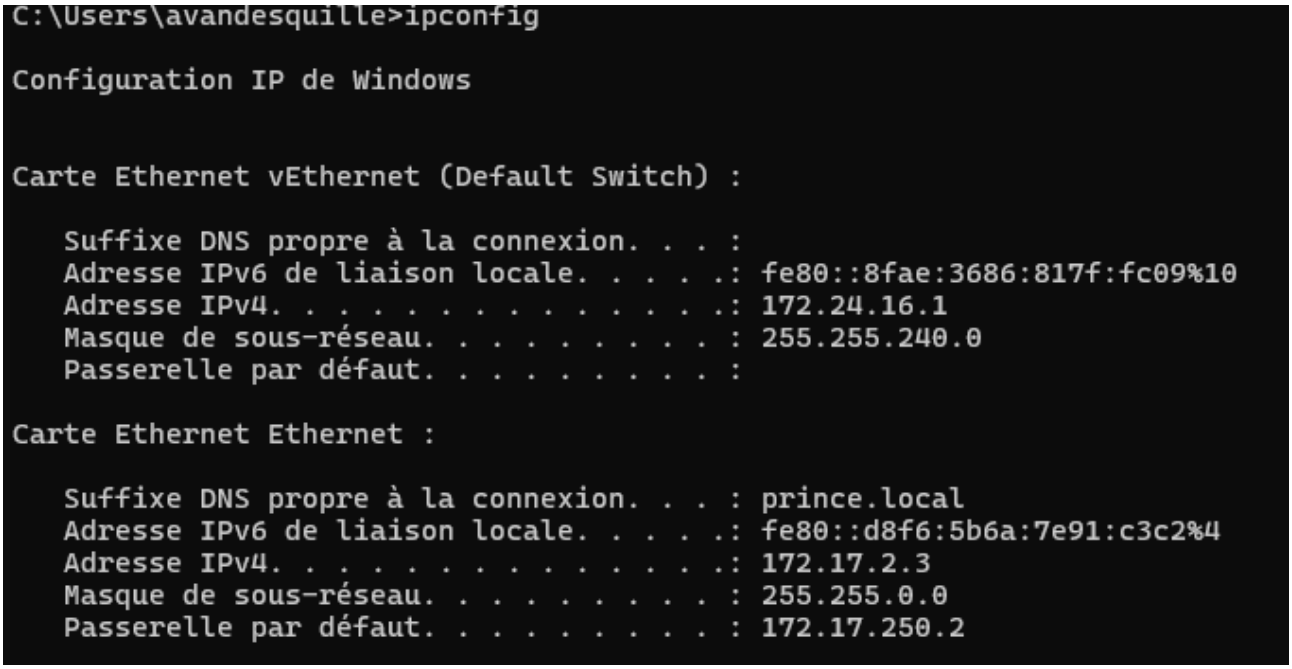


Vérifiez que la carte réseau de la VM DEB12Server soit en accès par pont et que la configuration IP soit prévue pour être obtenue automatiquement auprès du serveur DHCP ROI (cf. TP2 B1 pages 6 et 7). Vérifiez, avec la commande ip address, l'obtention des paramètres (adresse IP 172 .17.X.Y) (capture d'écran à réaliser)

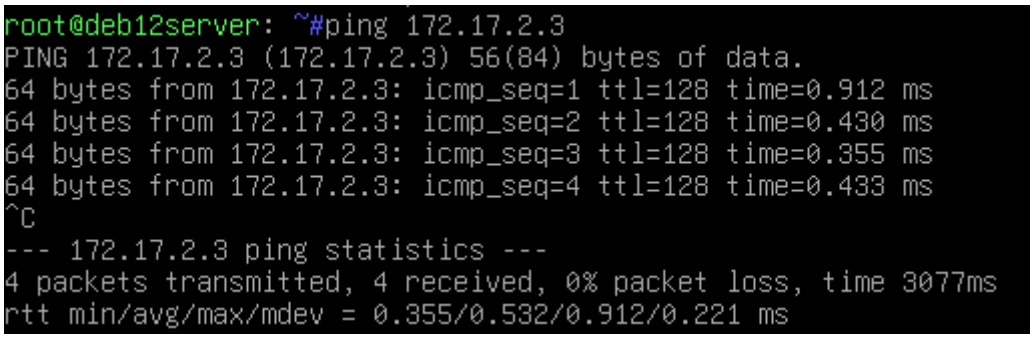



```
root@deb12server: ~#ip -c a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:56:7a:a5 brd ff:ff:ff:ff:ff:ff
    inet 172.17.110.19/16 brd 172.17.255.255 scope global dynamic enp0s3
       valid_lft 85305sec preferred_lft 85305sec
    inet6 fe80::a00:27ff:fe56:7aa5/64 scope link
       valid_lft forever preferred_lft forever
root@deb12server: ~#_
```

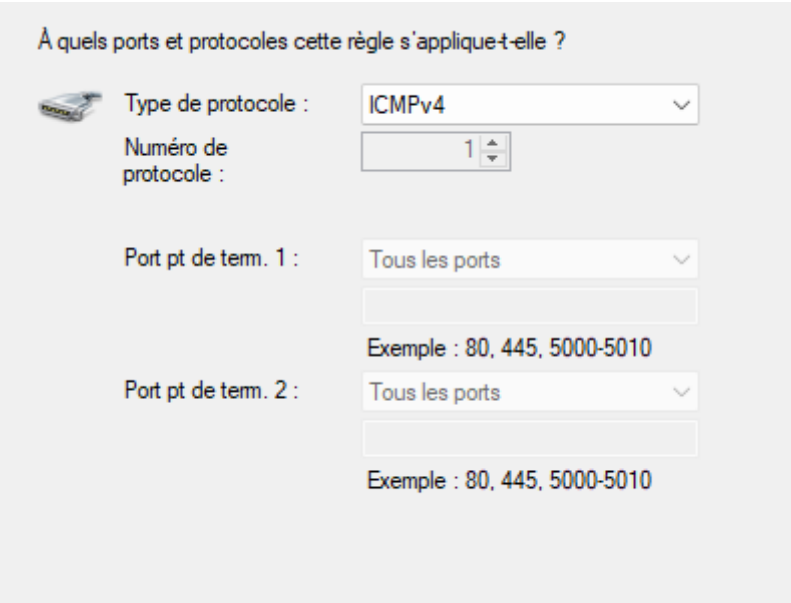
Vérifiez les paramètres IP de la carte réseau de votre machine physique à l'aide de la commande ipconfig /all depuis une invite de commandes (capture d'écran à réaliser) : les deux machines doivent être dans le même réseau IP



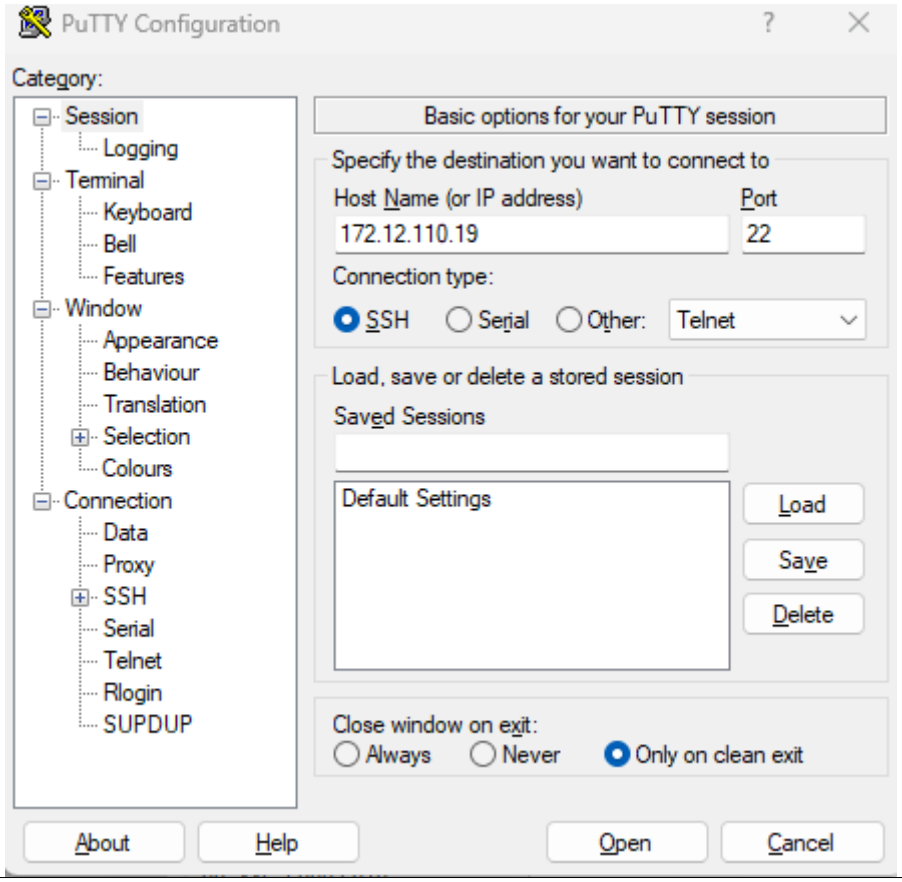
Je vérifie la connectivité entre les deux machines à l'aide d'un ping effectué depuis votre machine Linux (capture d'écran à réaliser). (l'adresse ip de ma machine physique est : 172.17.2.3



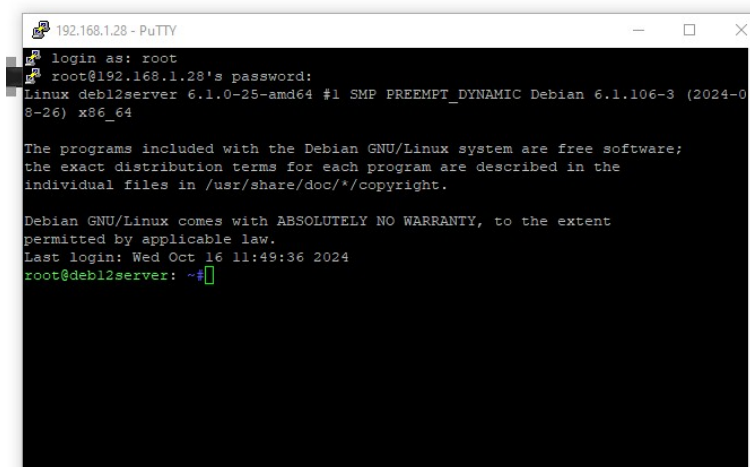
voici ma règle personnaliser permettant d’autoriser les trames ICMP à entrer



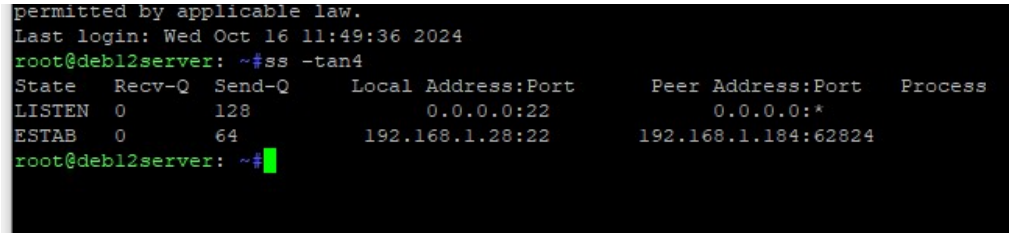
Lancez PuTTY depuis votre machine Windows (client SSH) et saisissez l’adresse IP de votre VM DEB12Server (serveur SSH) dans le champ Host Name, sélectionnez SSH puis cliquez sur Open :



puis à paritir de Putty j’ai accéder a mon serveur



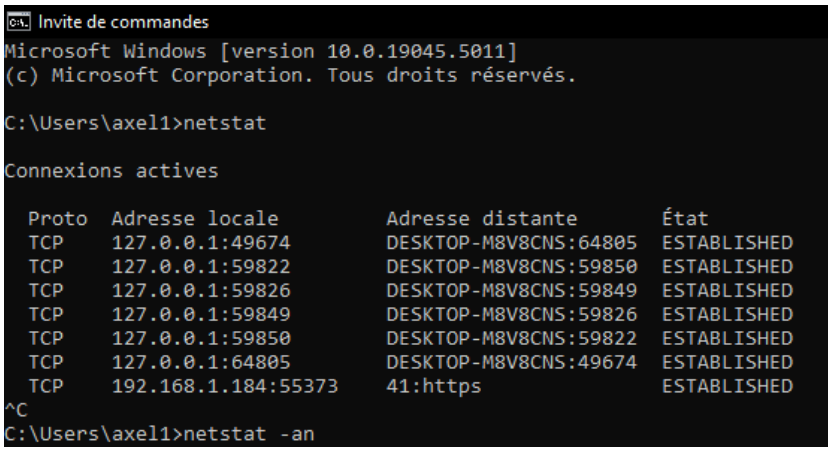
▪Dans cette console, saisissez la commande ss –tan4 (cf. TP2 B1). Montrez sur la capture d’écran que la connexion SSH est établie.



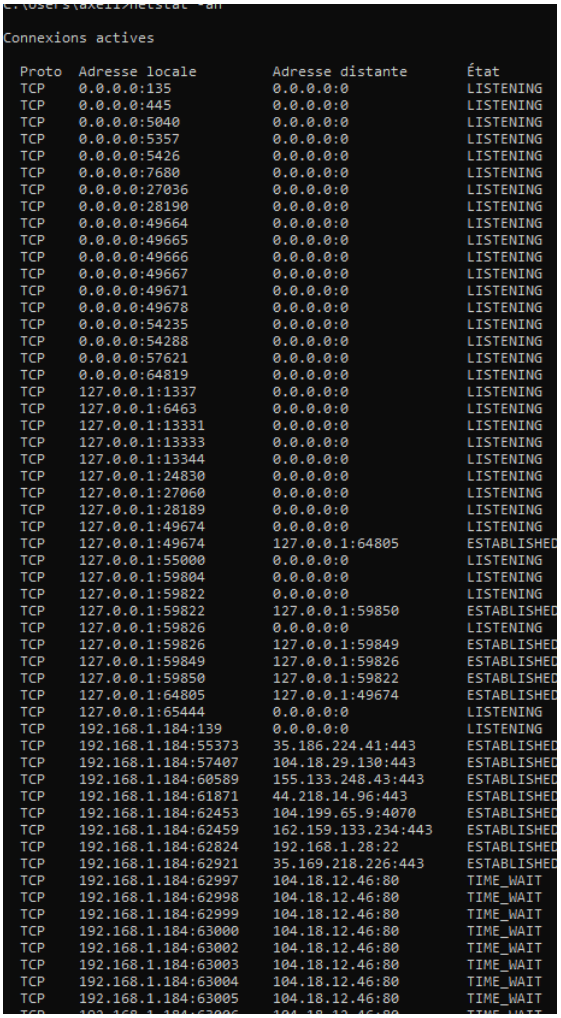
▪ Sur quel port écoute le service sshd du serveur SSH DEB12Server ? Le port 22

▪ Quel est le port dynamique assigné par le système d’exploitation Windows au client SSH durant la connexion TCP afin qu’il puisse écouter sur ce port et recevoir les réponses du serveur SSH DEB12Server ? Le port dynamique est le port 62824

▪ Ne fermez pas la session SSH. Ouvrez une invite de commande sur la machine Windows et saisissez la commande netstat (connexions TCP actives) puis netstat –an (connexions TCP actives et ports d'écoute). Montrez sur la capture d'écran que la connexion SSH est établie.



▪ Pour vous déconnecter de la session SSH depuis la console Linux, tapez logout ou utilisez la combinaison des touches Ctrl+D.



2. Connexion Bureau à distance (RDP).

L’adresse ip de mon voisin est 172.17.2.21

-Assurez-vous de la connectivité entre votre machine physique et la sienne : réalisez un ping de sa station depuis votre machine physique (capture d’écran). Pensez aux règles de Pare-feu des deux machines.

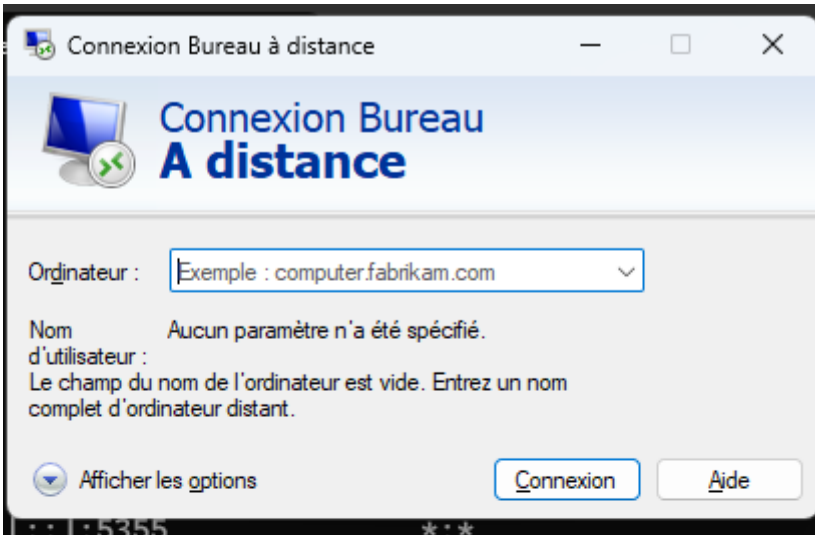
```
Statistiques Ping pour 172.17.2.21:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 0ms, Maximum = 0ms, Moyenne = 0ms

C:\Users\avandesquille>
```

Saisissez la commande netstat –an depuis l’invite de commandes de votre station Windows :

```
  TCP    0.0.0.0:3389           0.0.0.0:0              LISTENING
```

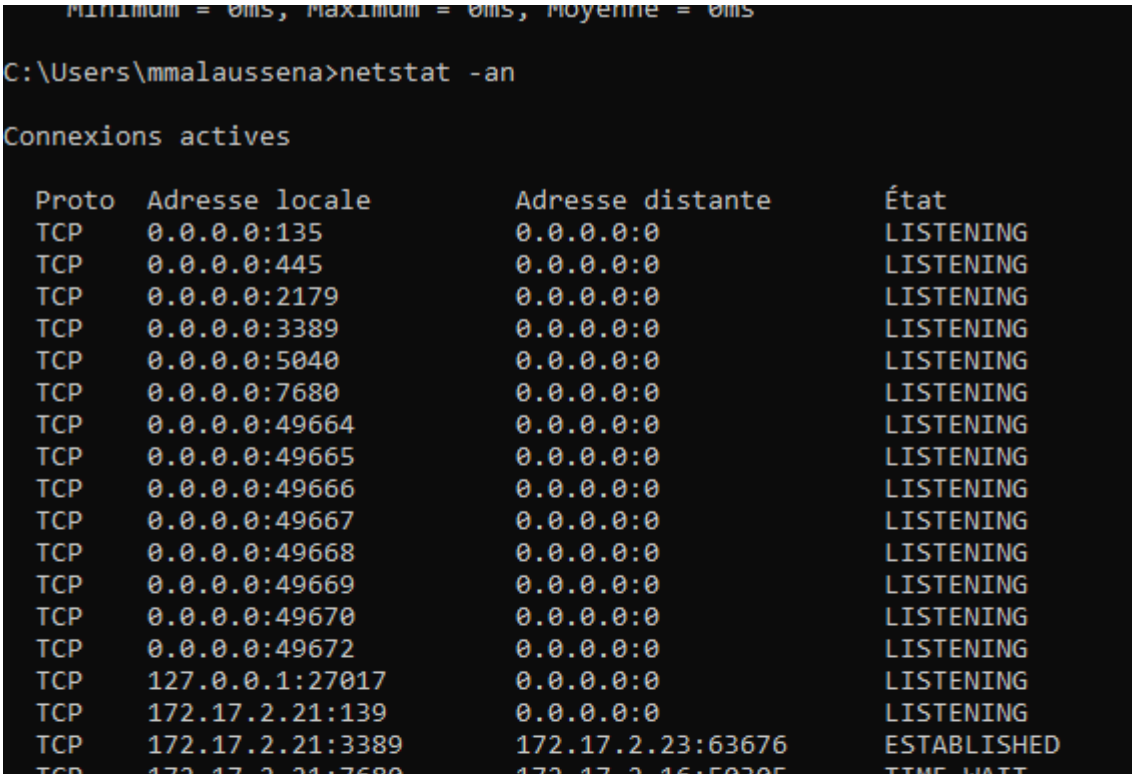
Quel est le port d’écoute du serveur Terminal Server ? 3389

voici ce que qu’on m’affiche grace à la commande mstsc



Saisissez l’adresse IP de la station de votre voisin qui a également autorisé les connexions à distance à son ordinateur, cliquez sur Connexion puis saisissez le mot de passe de l’administrateur du serveur distant (utilisez votre compte de domaine qui est membre du groupe 1sio lui-même membre du groupe local Administrateurs de chaque machine inscrite dans le domaine Prince)

Saisissez la commande netstat –an depuis l’invite de commande de la station de votre voisin via le bureau à distance. Vous constatez que la connexion au serveur Terminal Server est établie :

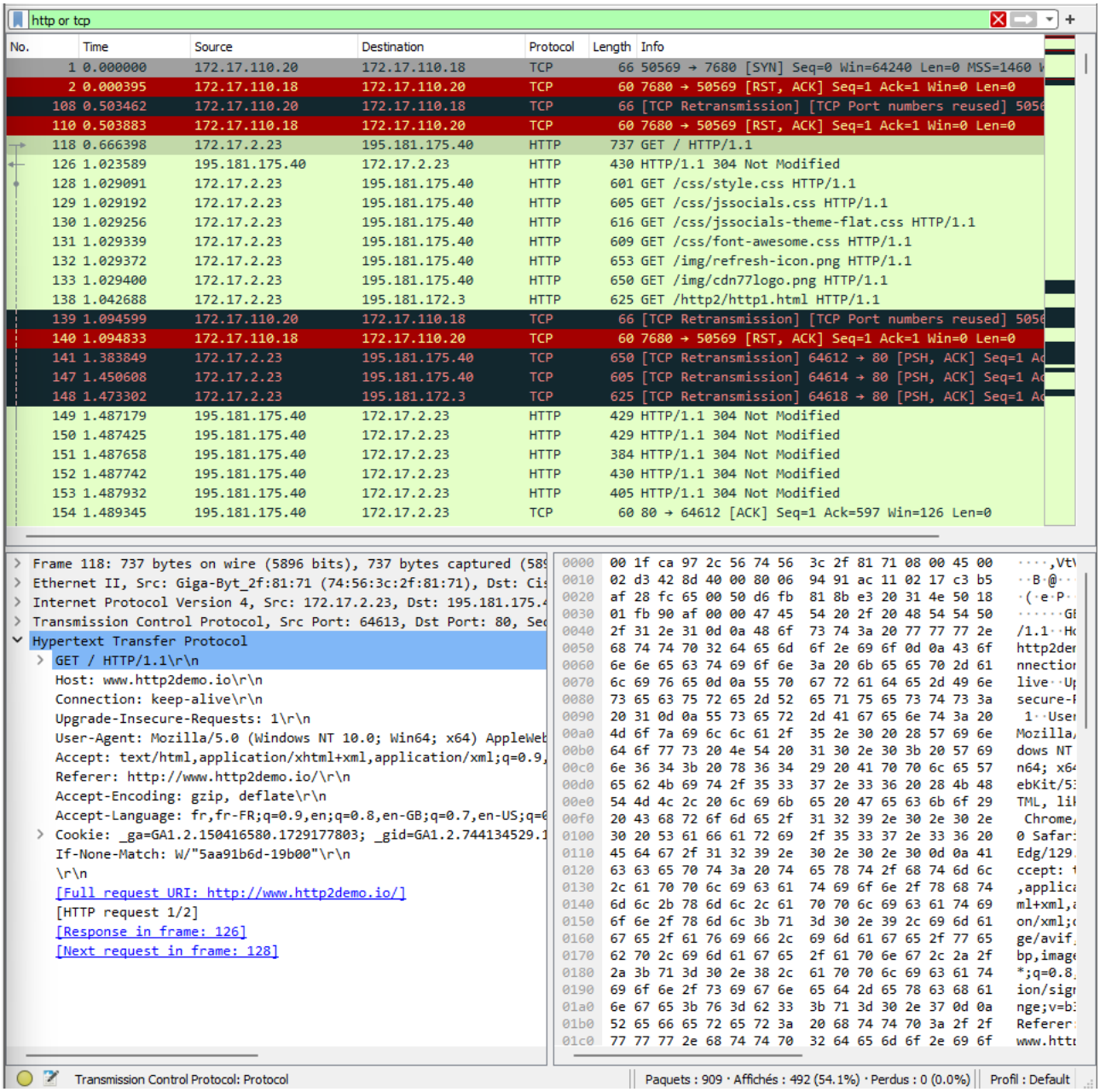


3. Capture de trames HTTP.

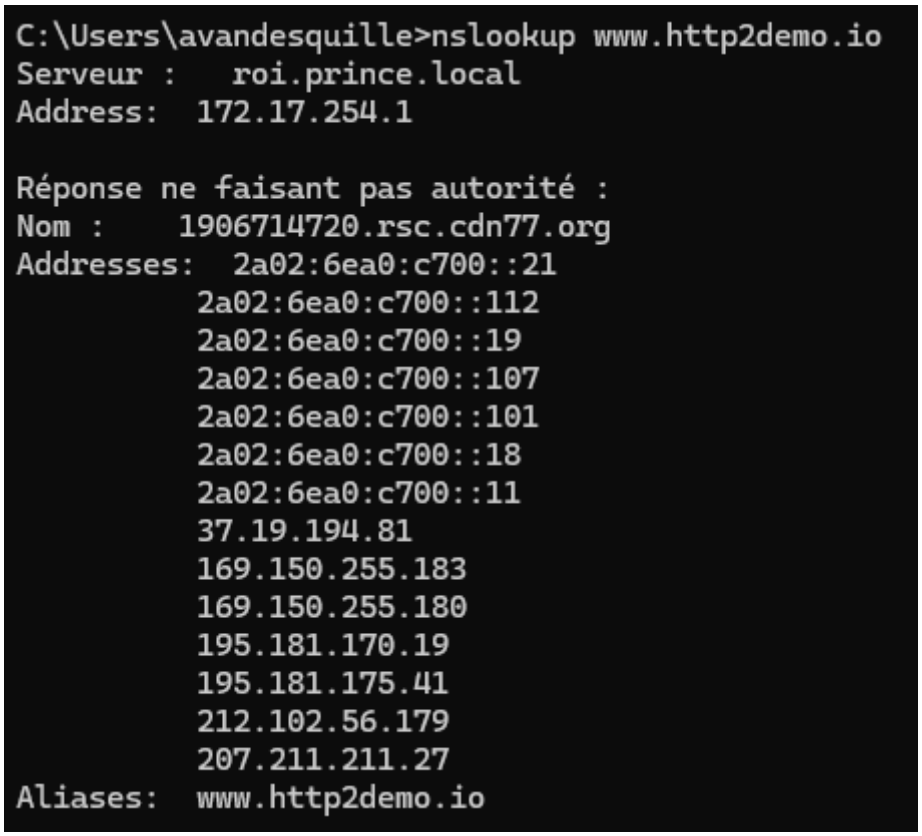
j’ouvre votre navigateur internet et affichez la page d’accueil du site http://www.http2demo.io/.

la capture est arreté et un filtre est appliqué pour n’afficher que les trames http et TCP qui nous intéressent. Spécifiez par exemple l’adresse IP du serveur http. Retrouvez cette adresse IP comme indiqué ci-dessous

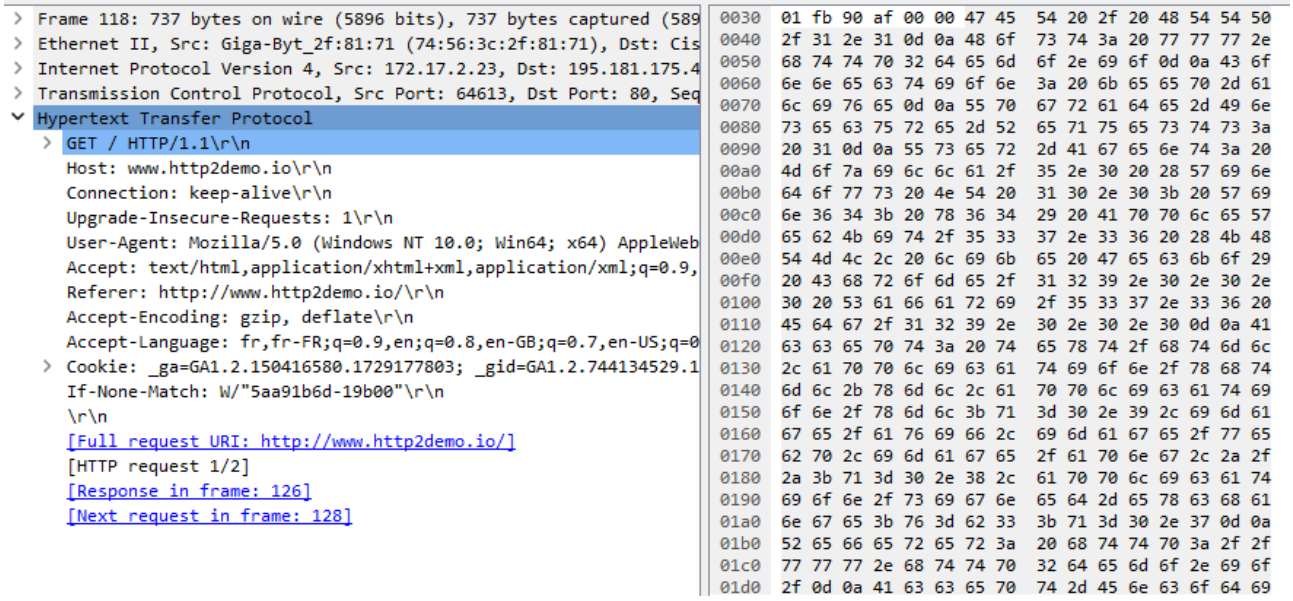
l’adresse ip est 195.181.175.40



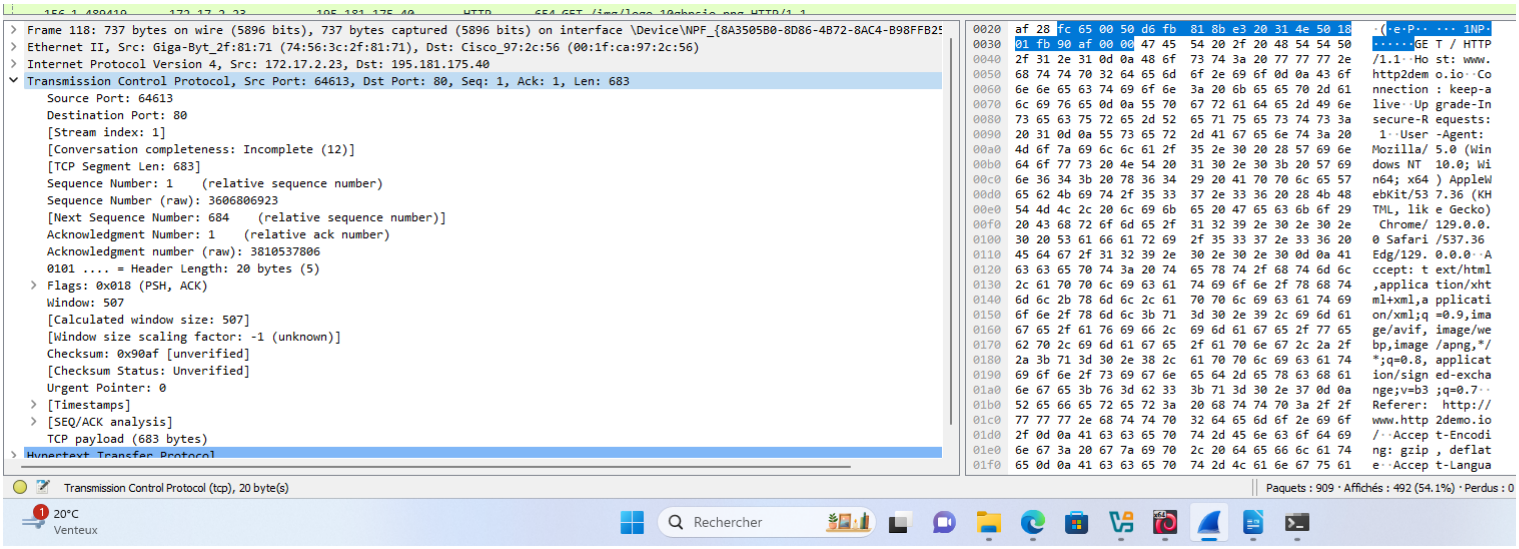
Je Saisi, depuis l’invite de commandes, la commande nslookup www.http2demo.io pour obtenir l’adresse IP du serveur web



la trame correspondant à votre requête http données applicative



la section correspondant à l’en-tête Transport



Quel est le nom du protocole transport utilisé par une trame HTTP ?

Le protocole de transport utilisé est TCP

Quel est le nom du PDU encapsulant les données applicatives HTTP ?

Segment

Quelle est la longueur de l’en-tête de transport ?

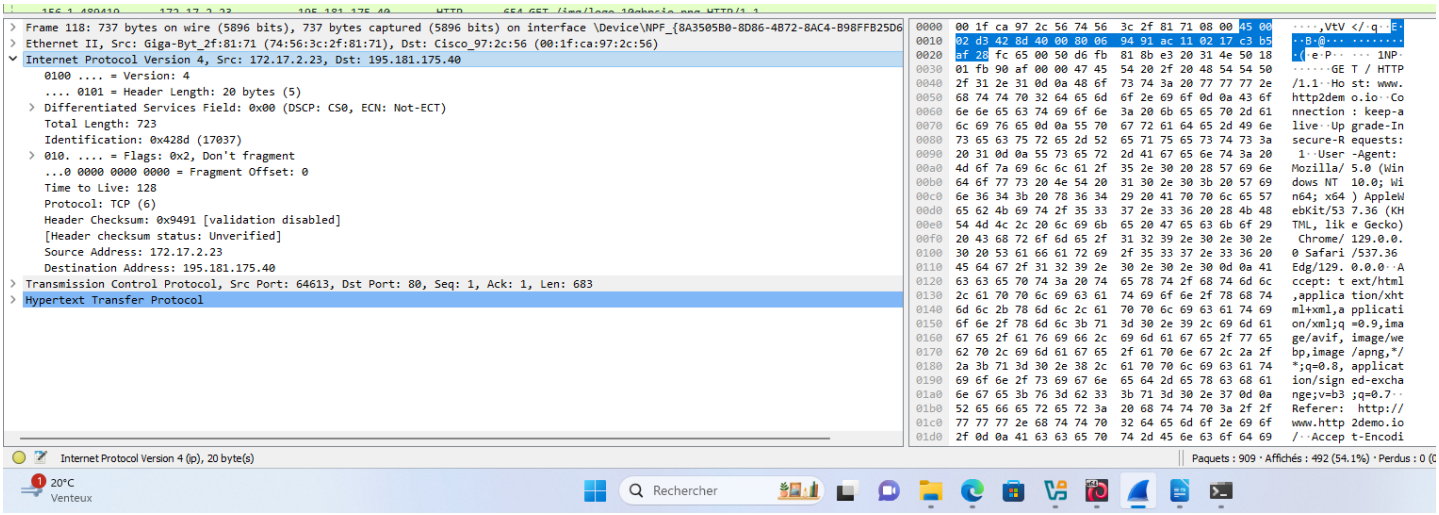
20 octets

Quelles sont les valeurs décimale et hexadécimale correspondant aux ports source et destination ?

Port source : 64161 (décimal) 0xFAA1 en héxadécimal

Port destnation : 80 (décimal) 0x0050 en héxadécimal

Section entête Résaux :



Quelle est la longueur de l’en-tête de réseau ? 20 ocets

Repérez le champ Protocole figurant dans l’en-tête Réseau. Quelle est la valeur présente ? 6

Que signifie-t-elle ? 6 correspond au protocole TCP

Quelles sont les valeurs décimales et hexadécimales des adresses IP source et destination ?

Adresse ip source :

172.17.12.23 (décimal)

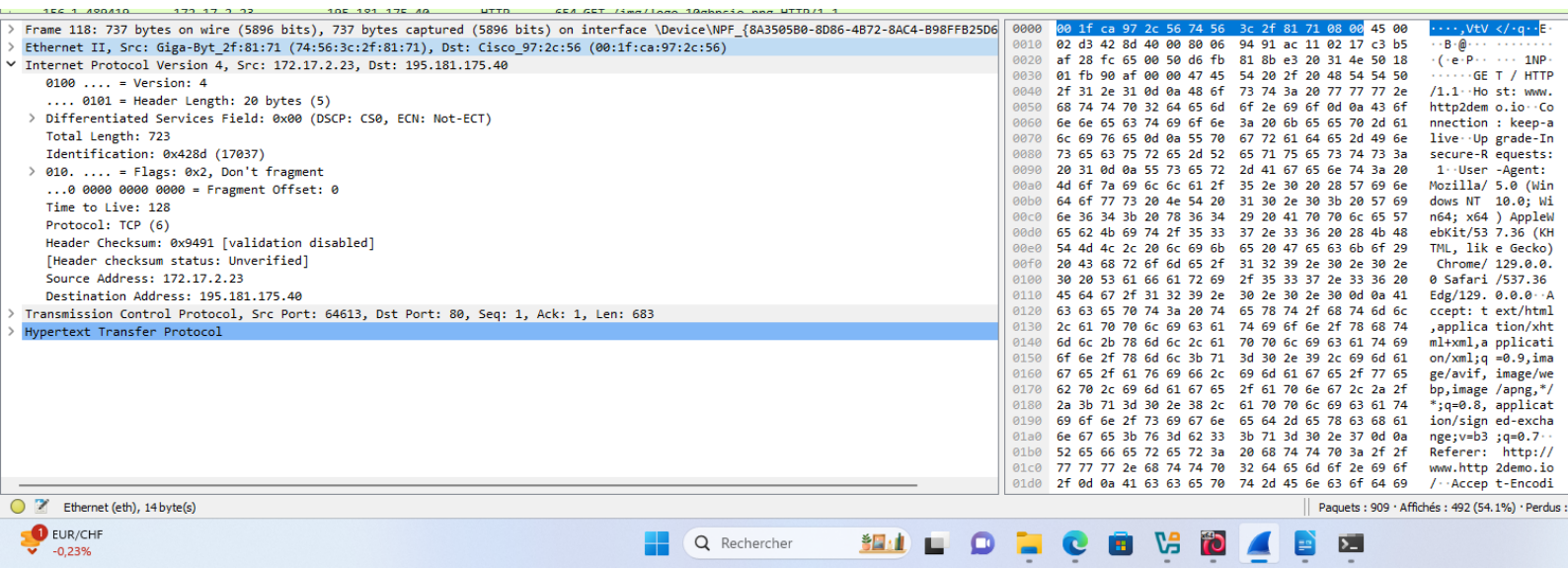
AC.11.0C.17 (héxadécimal)

adresse ip destination :

195.181.175.48 (décimal)

C3.B5.AF.30 (héxadécimal)

Section entête Ethernet



Repérez le champ EtherType. Quel est la valeur contenue ? Que signifie-t-elle ?

0800 ou 0x0800

indique la trame ethernet informe que la couche résaux à traiter est IPv4

Quelles sont les valeurs des adresses MAC destination et source ?

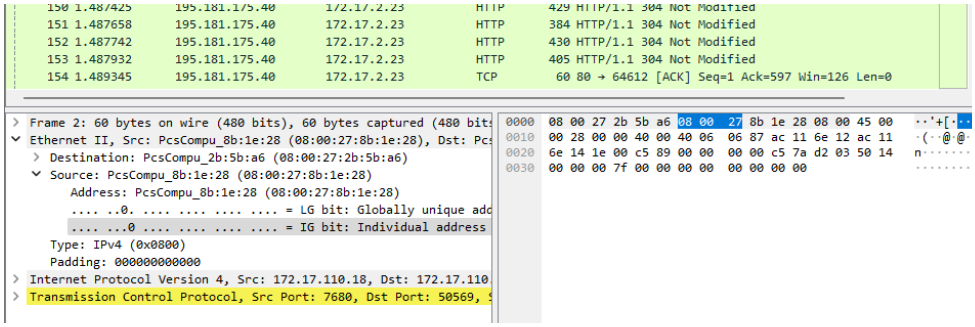
MAC destination : 00:1f:ca:97:2c:56

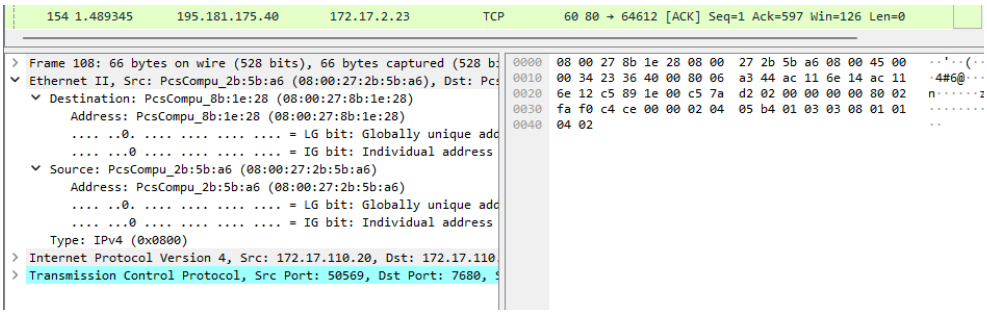
MA source : 74:56:3c:2f:81:71

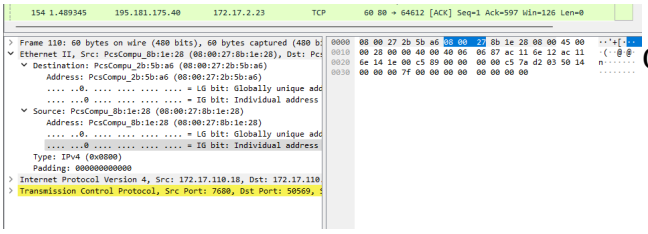
je réalisez une capture d’écran des 3 trames mettant en place la connexion TCP entre le client et le serveur (cf. Chapitre 4 - pages 3 et 8 : Three-way handshake)

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	172.17.110.20	172.17.110.18	TCP	66	50569 → 7680 [SYN] Seq=0 Win=64240 Len=0 MSS=1460
2	0.000395	172.17.110.18	172.17.110.20	TCP	60	7680 → 50569 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
108	0.503462	172.17.110.20	172.17.110.18	TCP	66	[TCP Retransmission] [TCP Port numbers reused] 505
110	0.503883	172.17.110.18	172.17.110.20	TCP	60	7680 → 50569 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
118	0.666398	172.17.2.23	195.181.175.40	HTTP	737	GET / HTTP/1.1
126	1.023589	195.181.175.40	172.17.2.23	HTTP	430	HTTP/1.1 304 Not Modified
128	1.029091	172.17.2.23	195.181.175.40	HTTP	601	GET /css/style.css HTTP/1.1
129	1.029192	172.17.2.23	195.181.175.40	HTTP	605	GET /css/jssocials.css HTTP/1.1
130	1.029256	172.17.2.23	195.181.175.40	HTTP	616	GET /css/jssocials-theme-flat.css HTTP/1.1
131	1.029339	172.17.2.23	195.181.175.40	HTTP	609	GET /css/font-awesome.css HTTP/1.1
132	1.029372	172.17.2.23	195.181.175.40	HTTP	653	GET /img/refresh-icon.png HTTP/1.1
133	1.029400	172.17.2.23	195.181.175.40	HTTP	650	GET /img/cdn77logo.png HTTP/1.1
138	1.042688	172.17.2.23	195.181.172.3	HTTP	625	GET /http2/http1.html HTTP/1.1
139	1.094599	172.17.110.20	172.17.110.18	TCP	66	[TCP Retransmission] [TCP Port numbers reused] 505
140	1.094833	172.17.110.18	172.17.110.20	TCP	60	7680 → 50569 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
141	1.383849	172.17.2.23	195.181.175.40	TCP	650	[TCP Retransmission] 64612 → 80 [PSH, ACK] Seq=1 A
147	1.450608	172.17.2.23	195.181.175.40	TCP	605	[TCP Retransmission] 64614 → 80 [PSH, ACK] Seq=1 A
148	1.473302	172.17.2.23	195.181.172.3	TCP	625	[TCP Retransmission] 64618 → 80 [PSH, ACK] Seq=1 A
149	1.487179	195.181.175.40	172.17.2.23	HTTP	429	HTTP/1.1 304 Not Modified
150	1.487425	195.181.175.40	172.17.2.23	HTTP	429	HTTP/1.1 304 Not Modified
151	1.487658	195.181.175.40	172.17.2.23	HTTP	384	HTTP/1.1 304 Not Modified
152	1.487742	195.181.175.40	172.17.2.23	HTTP	430	HTTP/1.1 304 Not Modified

3 trames :







Combien de connexions TCP ont été établies ? 3