TP3 – Les ports logiciels

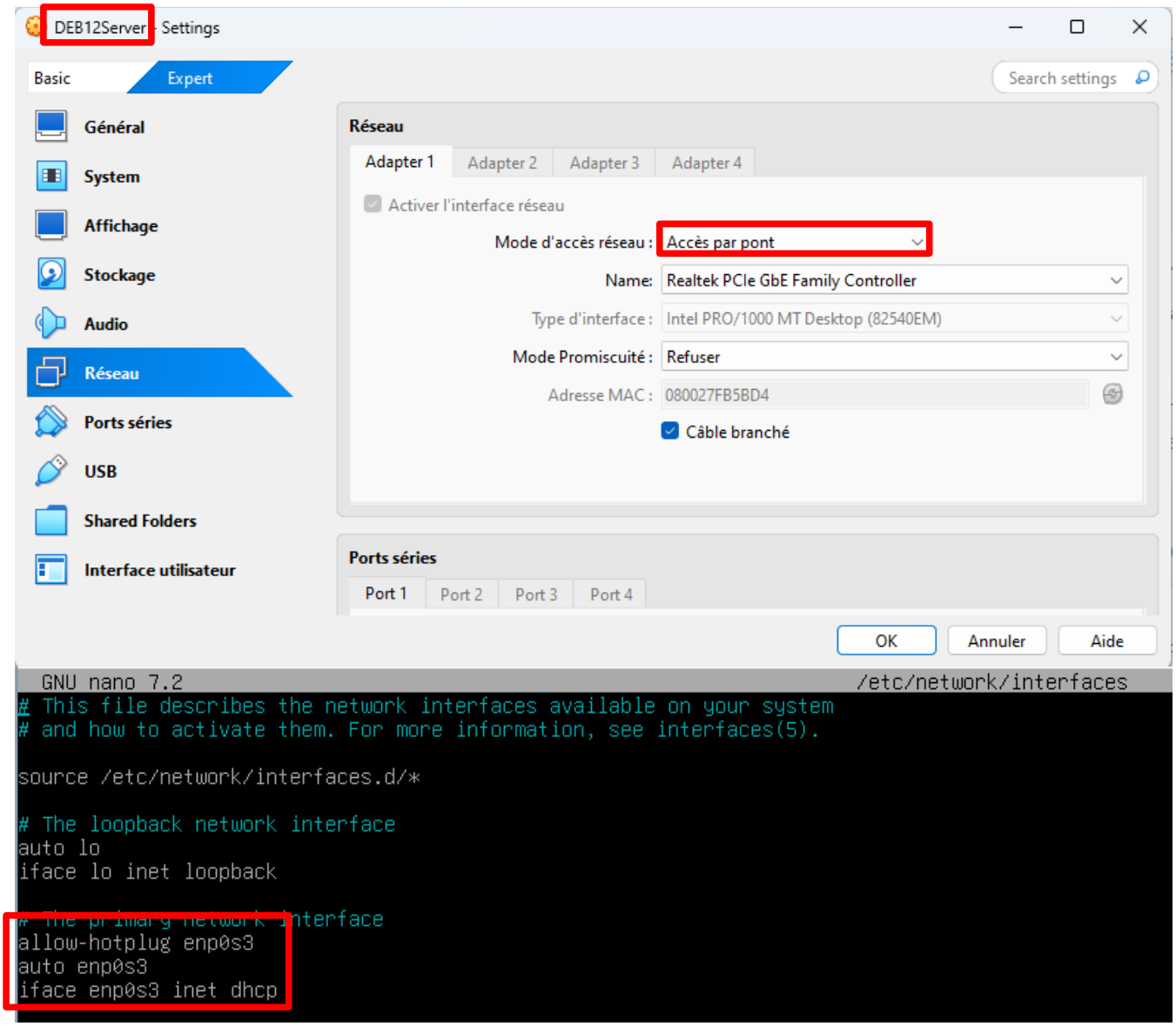
Sommaire

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

→ On télécharge **putty.exe** depuis la machine hôte :

putty	04/10/2024 15:54	Application	1 625 Ko

→ On vérifie que la carte réseau de la machine serveur soit en **accès par pont** et qu'elle récupère **automatiquement** son adresse IP auprès du **serveur DHCP ROI (172 .17.X.Y)** :



3

```
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:fb:5b:d4 brd ff:ff:ff:ff:ff:ff
    inet 172.17.110.17/16 brd 172.17.255.255 scope global dynamic enp0s3
       valid_lft 86046sec preferred_lft 86046sec
    inet6 fe80::a00:27ff:fefb:5bd4/64 scope link
       valid_lft forever preferred_lft forever
```

→ On vérifie les paramètres IP de la carte réseau sur la **machine physique** avec **ipconfig /all** pour s'assurer que les deux machines sont dans le **même réseau** :

```
Carte Ethernet Ethernet :

   Suffixe DNS propre à la connexion. . . : prince.local
   Description. . . . . . . . . . . . . . : Realtek PCIe GbE Family Controller
   Adresse physique . . . . . . . . . . . : 74-56-3C-2F-9C-F0
   DHCP activé. . . . . . . . . . . . . . : Oui
   Configuration automatique activée. . . : Oui
   Adresse IPv6 de liaison locale. . . . .: fe80::6b83:74d3:2ac4:5035%9(préféré)
   Adresse IPv4. . . . . . . . . . . . . .: 172.17.2.21(préféré)
   Masque de sous-réseau. . . . . . . . . : 255.255.0.0
   Bail obtenu. . . . . . . . . . . . . . : vendredi 11 octobre 2024 14:40:52
   Bail expirant. . . . . . . . . . . . . : samedi 12 octobre 2024 04:53:56
   Passerelle par défaut. . . . . . . . . : 172.17.250.2
   Serveur DHCP . . . . . . . . . . . . . : 172.17.254.1
   IAID DHCPv6 . . . . . . . . . . . : 326391356
   DUID de client DHCPv6. . . . . . . . : 00-01-00-01-2C-DF-41-0E-74-56-3C-2F-9C-F0
   Serveurs DNS. . .  . . . . . . . . . . : 172.17.254.1
                                    172.17.244.1
                                    80.10.246.2
                                    8.8.8.8
   NetBIOS sur Tcpip. . . . . . . . . . . : Activé
```

***Elles sont bien toutes les deux dans le **réseau ROI**.

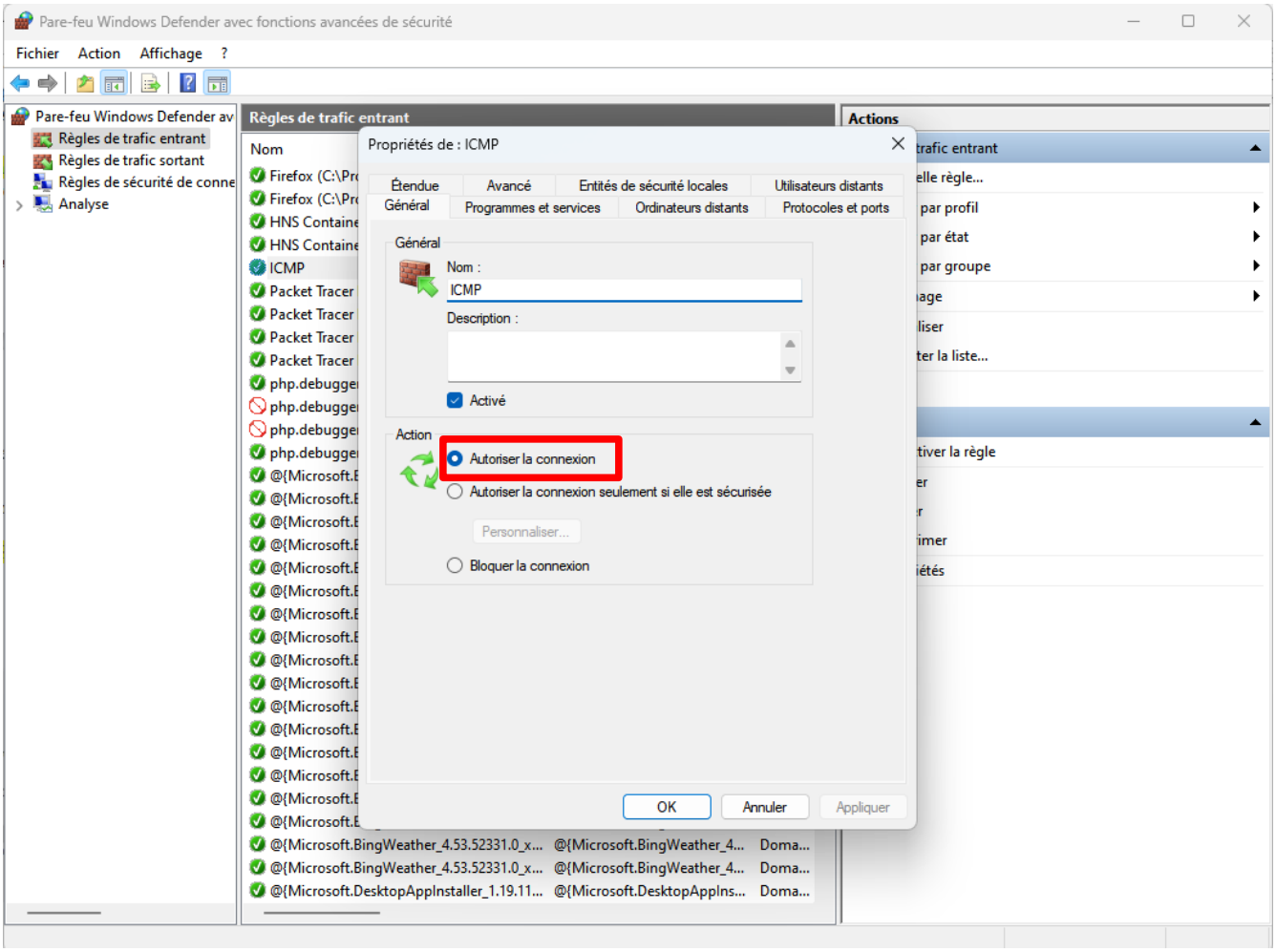
→ On teste la **connectivité** entre les deux machines avec un **ping** :

```
root@DEB12Server: ~#ping 172.17.2.21
PING 172.17.2.21 (172.17.2.21) 56(84) bytes of data.
64 bytes from 172.17.2.21: icmp_seq=1 ttl=128 time=0.932 ms
64 bytes from 172.17.2.21: icmp_seq=2 ttl=128 time=0.432 ms
64 bytes from 172.17.2.21: icmp_seq=3 ttl=128 time=0.360 ms
64 bytes from 172.17.2.21: icmp_seq=4 ttl=128 time=0.505 ms
^C
--- 172.17.2.21 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3069ms
rtt min/avg/max/mdev = 0.360/0.557/0.932/0.222 ms
```

4

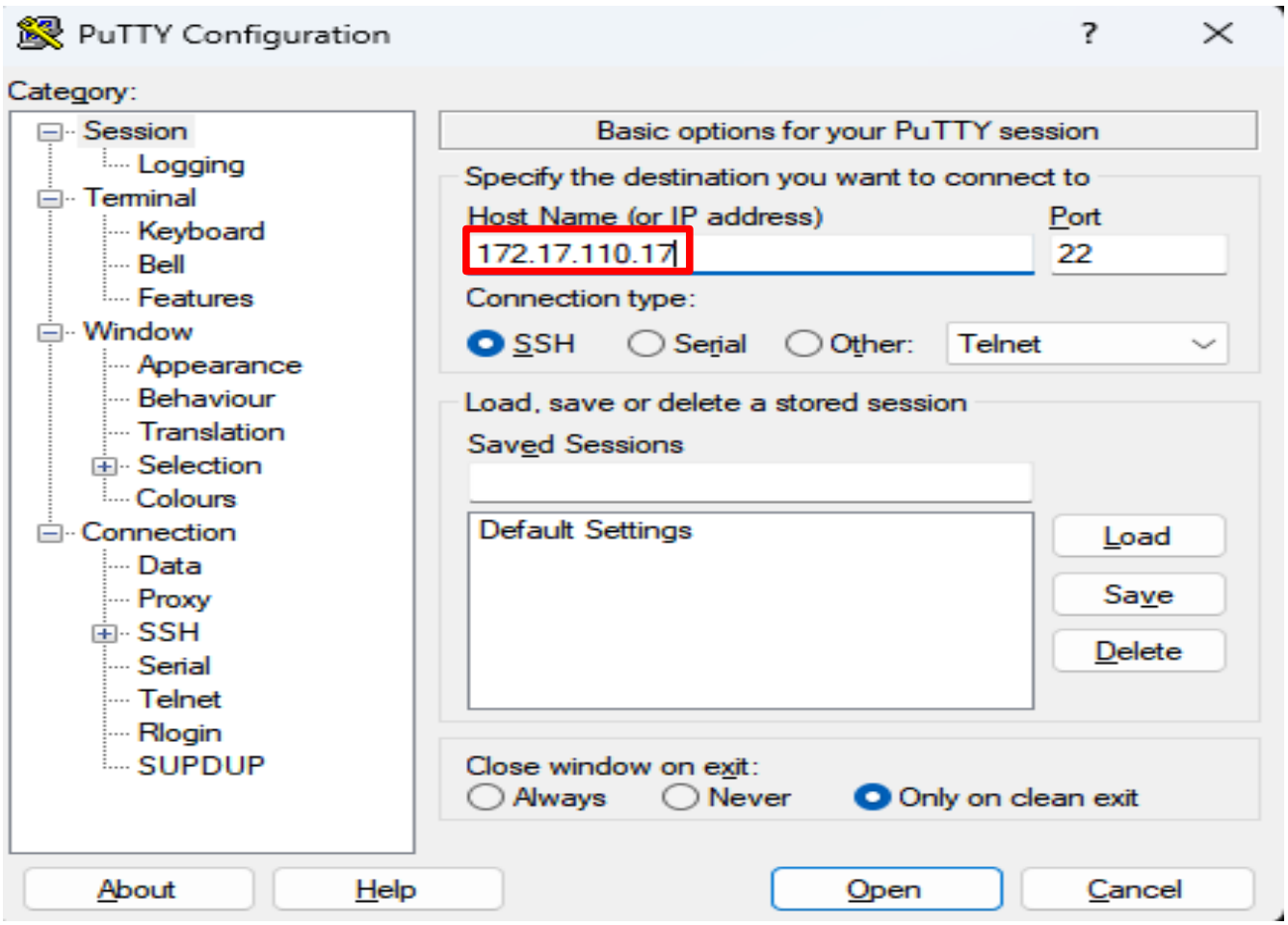
***** Les **trames** sont reçues par la machine hôte, la **connectivité** est bien présente.

→ On autorise le **protocole ICMP** dans le **pare-feu Windows** en trafic entrant et sortant :

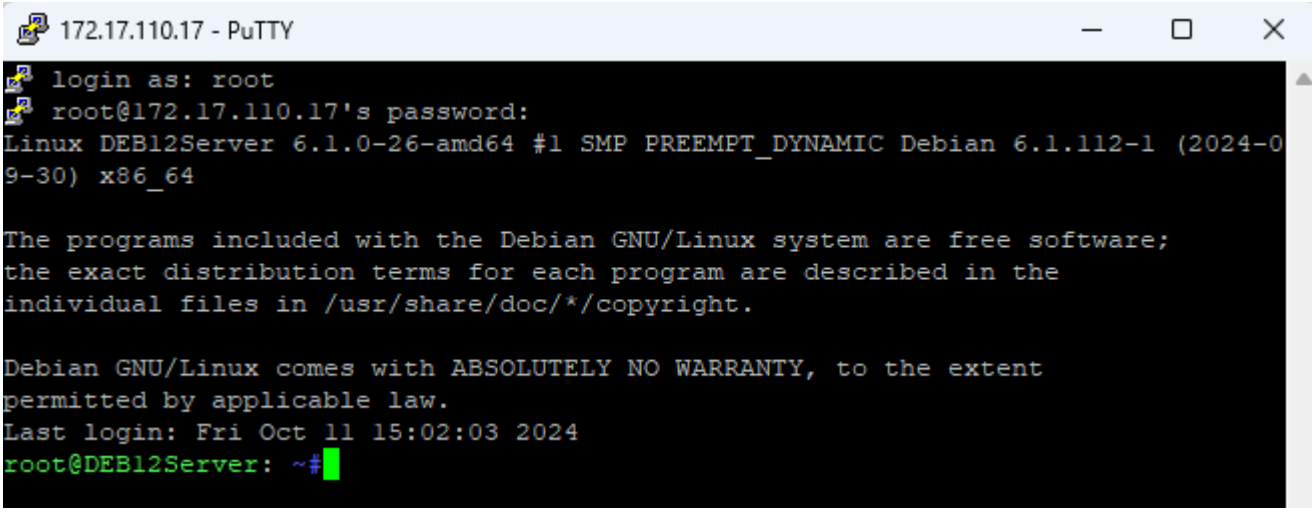


5

→ On lance **putty** depuis la machine hôte et on saisit l'IP de la machine serveur :



→ On ouvre une **session SSH** puis on saisit le **login** et le **mot de passe** :



→ On observe la **connexion TCP** qui a été établie avec la commande **ss -tan4** sur cette console :

```
root@DEB12Server: ~#ss -tan4
State    Recv-Q    Send-Q      Local Address:Port      Peer Address:Port    Process
LISTEN   0         128               0.0.0.0:22             0.0.0.0:*
ESTAB    0         64          172.17.110.17:22        172.17.2.21:50938
```

***** Le **port d'écoute** du **serveur SSH DEB12Server** est le port **22**.

***** Le **port dynamique** assigné par **Windows** au **client SSH** durant la connexion TCP est le port **50938**.

→ On saisit la commande **netstat** puis **netstat -an** sur la machine hôte :

```
C:\Windows\System32>netstat

Connexions actives

  Proto  Adresse locale         Adresse distante       État
  TCP    172.17.2.21:7680       G102-GB11:49479        TIME_WAIT
  TCP    172.17.2.21:7680       G102-GB11:49481        TIME_WAIT
  TCP    172.17.2.21:7680       G102-GB19:51108        TIME_WAIT
  TCP    172.17.2.21:7680       G102-GB19:51114        TIME_WAIT
  TCP    172.17.2.21:7680       G102-GB02:57645        TIME_WAIT
  TCP    172.17.2.21:7680       G102-GB02:57648        TIME_WAIT
  TCP    172.17.2.21:7680       G102-GB02:57650        TIME_WAIT
  TCP    172.17.2.21:7680       G102-GB02:57651        TIME_WAIT
  TCP    172.17.2.21:7680       G102-GB02:57653        TIME_WAIT
  TCP    172.17.2.21:50311      20.199.120.151:https   ESTABLISHED
  TCP    172.17.2.21:50431      aviateur:microsoft-ds  ESTABLISHED
  TCP    172.17.2.21:50902      aviateur:microsoft-ds  ESTABLISHED
  TCP    172.17.2.21:50910      150.171.85.254:https   CLOSE_WAIT
  TCP    172.17.2.21:50912      13.107.226.254:https   CLOSE_WAIT
  TCP    172.17.2.21:50921      13.107.246.254:https   CLOSE_WAIT
  TCP    172.17.2.21:50938      172.17.110.17:ssh      ESTABLISHED
  TCP    172.17.2.21:50957      52.123.242.159:https   ESTABLISHED
  TCP    172.17.2.21:50958      192.229.221.95:http    ESTABLISHED
  TCP    172.17.2.21:50959      a95-100-200-73:https   ESTABLISHED
  TCP    172.17.2.21:50961      52.168.117.171:https   ESTABLISHED
  TCP    172.17.2.21:50962      13.107.18.254:https    ESTABLISHED
  TCP    172.17.2.21:50963      150.171.73.254:https   ESTABLISHED
  TCP    172.17.2.21:50964      13.107.213.254:https   ESTABLISHED
  TCP    172.17.2.21:50965      204.79.197.222:https   ESTABLISHED
  TCP    172.17.2.21:50966      152.199.19.161:https   ESTABLISHED
  TCP    172.17.2.21:50967      13.107.246.43:https    ESTABLISHED
  TCP    172.17.2.21:50968      20.187.64.58:https     ESTABLISHED
  TCP    172.17.2.21:50969      152.199.19.161:https   ESTABLISHED
  TCP    172.17.2.21:50970      172.202.65.254:https   ESTABLISHED
  TCP    172.17.2.21:50971      40.112.186.181:https   ESTABLISHED
```

```
TCP    172.17.2.21:50938      172.17.110.17:22       ESTABLISHED
```

1

→ On se **déconnecte** de la **session SSH** :

2. Connexion Bureau à distance (RDP)

→ On récupère l'adresse IP de la machine physique du **voisin** :

172.17.2.19

→ On **ping** sa machine pour s'assurer de la connectivité entre nos machines :

```
C:\Users\nflavigny>ping 172.17.2.19

Envoi d'une requête 'Ping'  172.17.2.19 avec 32 octets de données :
Réponse de 172.17.2.19 : octets=32 temps<1ms TTL=128
Réponse de 172.17.2.19 : octets=32 temps=1 ms TTL=128
Réponse de 172.17.2.19 : octets=32 temps<1ms TTL=128
Réponse de 172.17.2.19 : octets=32 temps<1ms TTL=128

Statistiques Ping pour 172.17.2.19:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 0ms, Maximum = 1ms, Moyenne = 0ms
```

→ On saisit la commande **netstat -an** sur la machine hôte :

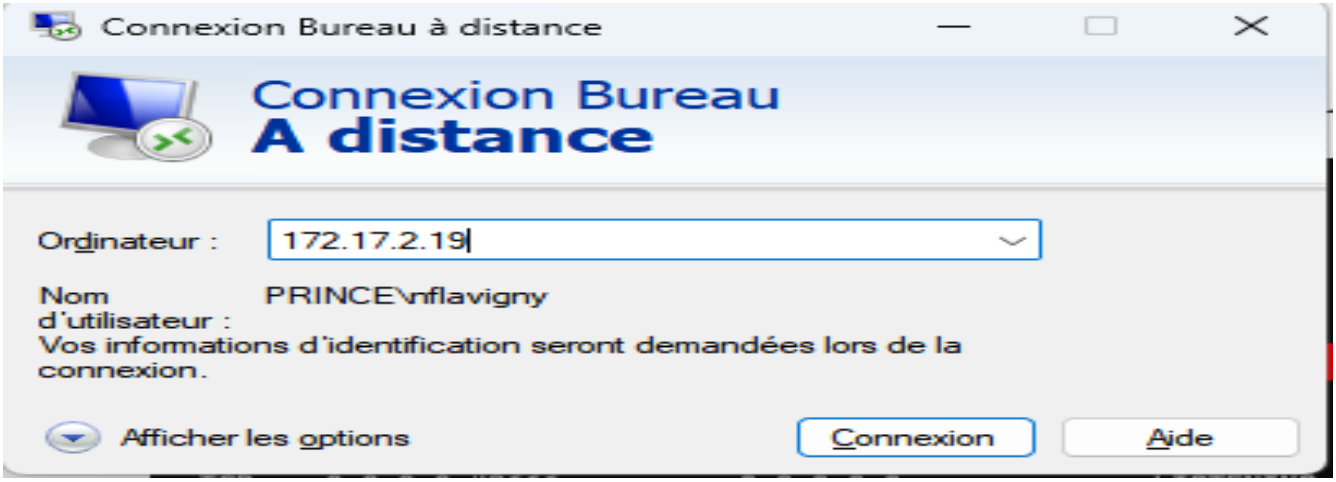
```
C:\Users\nflavigny>netstat -an

Connexions actives

  Proto  Adresse locale         Adresse distante       État
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:2179           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:3389           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:5040           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:7680           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49664          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49665          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49666          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49667          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49668          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49669          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49670          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49672          0.0.0.0:0              LISTENING
  TCP    127.0.0.1:27017        0.0.0.0:0              LISTENING
  TCP    172.17.2.21:139        0.0.0.0:0              LISTENING
  TCP    172.17.2.21:7680       172.17.2.9:50211       TIME_WAIT
  TCP    172.17.2.21:7680       172.17.2.9:50223       TIME_WAIT
  TCP    172.17.2.21:7680       172.17.2.16:51359      TIME_WAIT
  TCP    172.17.2.21:7680       172.17.2.24:57917      TIME_WAIT
  TCP    172.17.2.21:7680       172.17.2.24:57918      TIME_WAIT
  TCP    172.17.2.21:7680       172.17.2.24:57919      TIME_WAIT
```

***** Le port d'écoute du serveur Terminal Server est **3389**

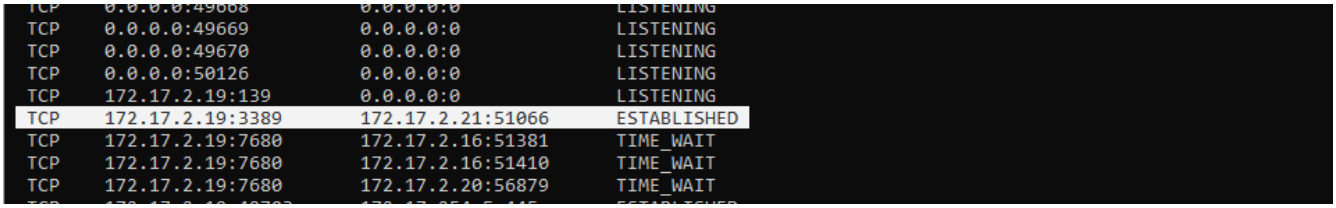
9

→ On saisit **mstsc** dans la zone de recherche windows :

→ On saisit **l'adresse IP de notre voisin** puis on se connecte sur son bureau :



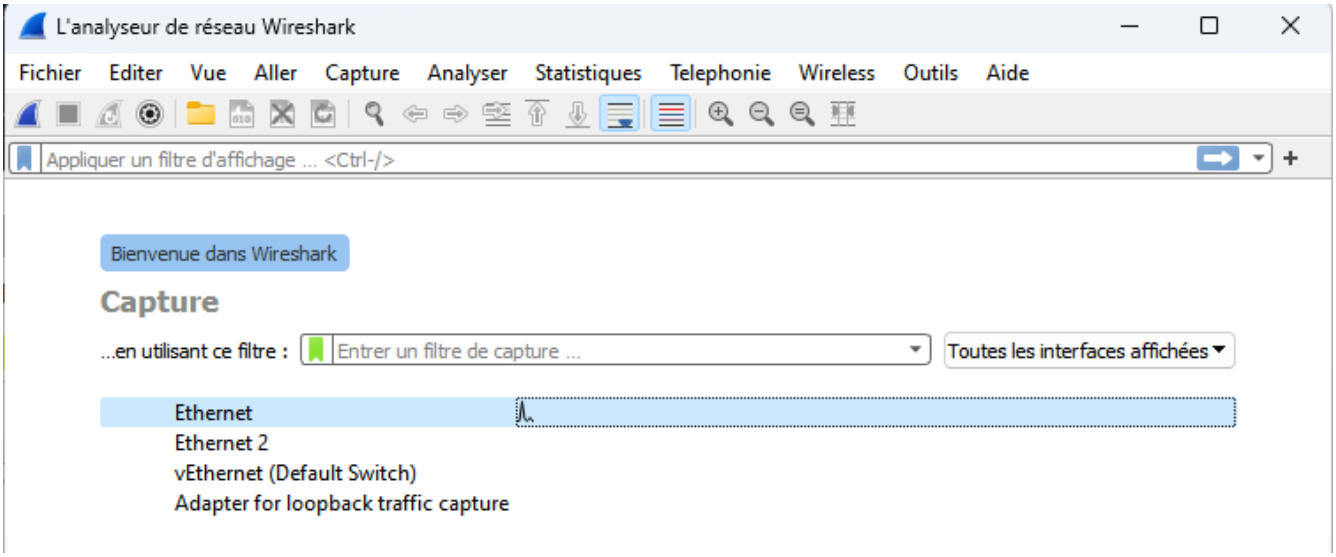
→ On saisit la commande **netstat -an** depuis son invite de commande :



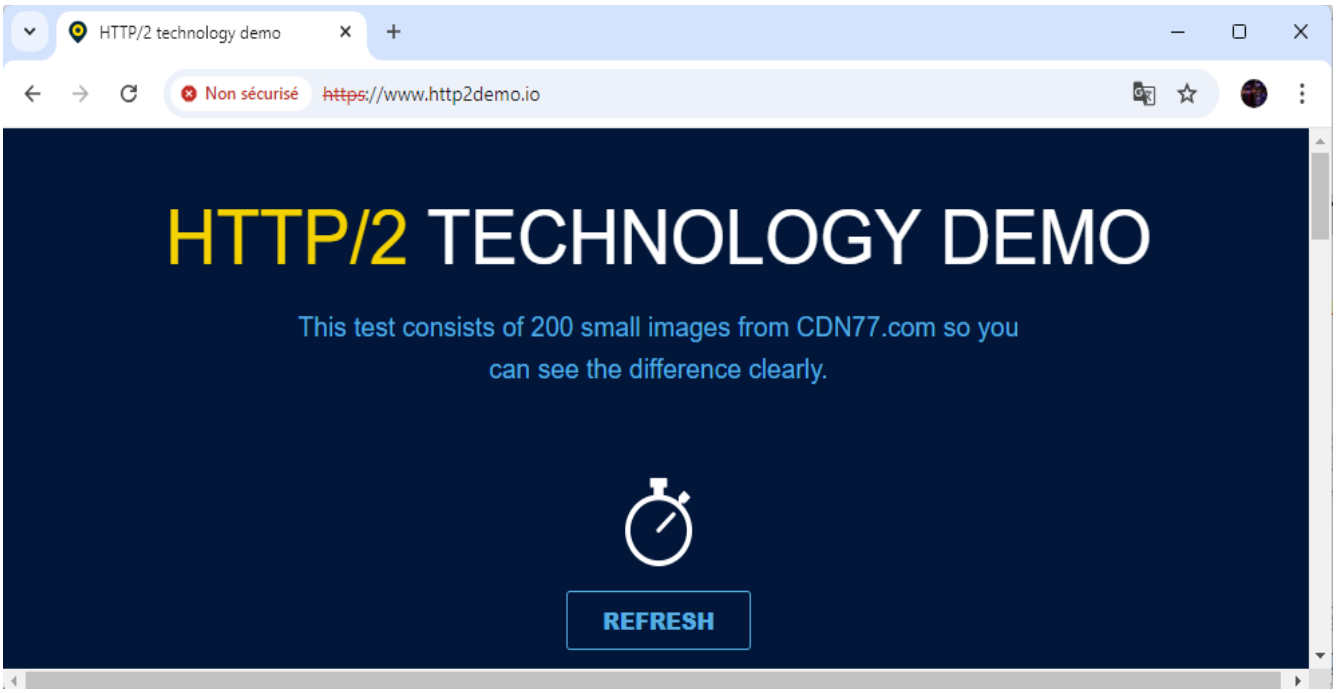
***** On se déconnecte de sa session en appuyant sur **déconnecter**

3. Capture de trames HTTP

→ On lance **Wireshark** en tant qu'**Administrateur** sur la machine physique puis on sélectionne la carte réseau :



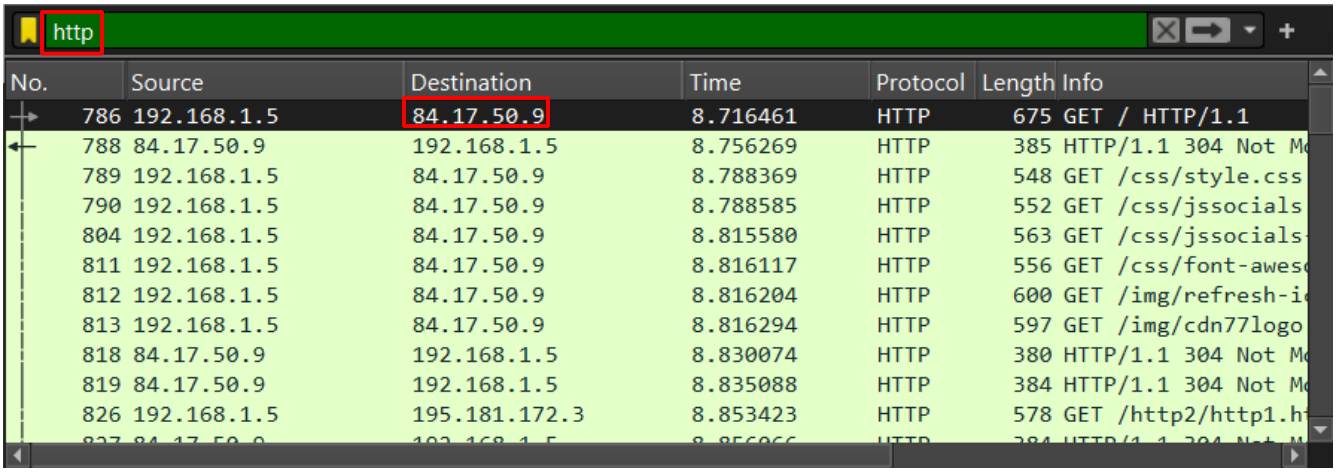
→ On ouvre le navigateur internet et on affiche la page d'accueil du site **http://www.http2demo.io/** :



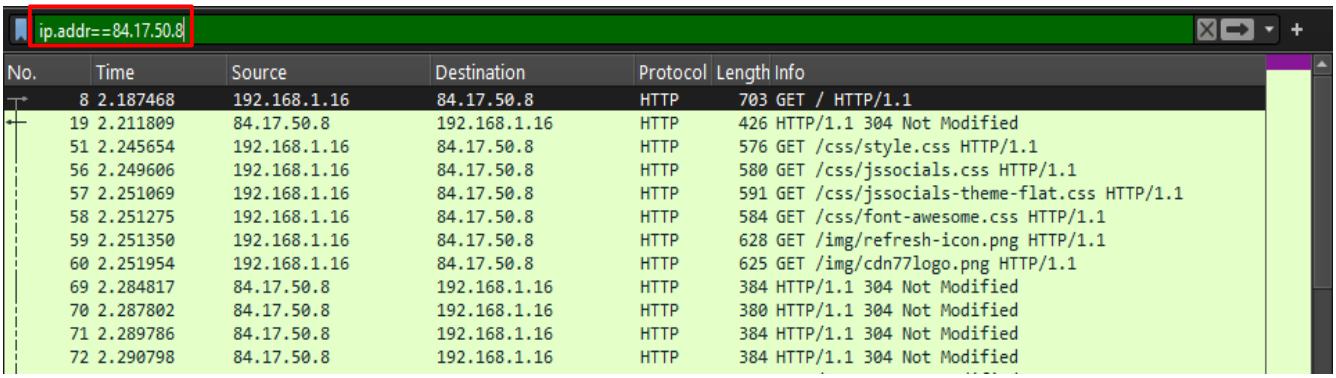
11

→ On saisit la commande **nslookup www.http2demo.io** pour trouver l'adresse IP du **serveur http** :

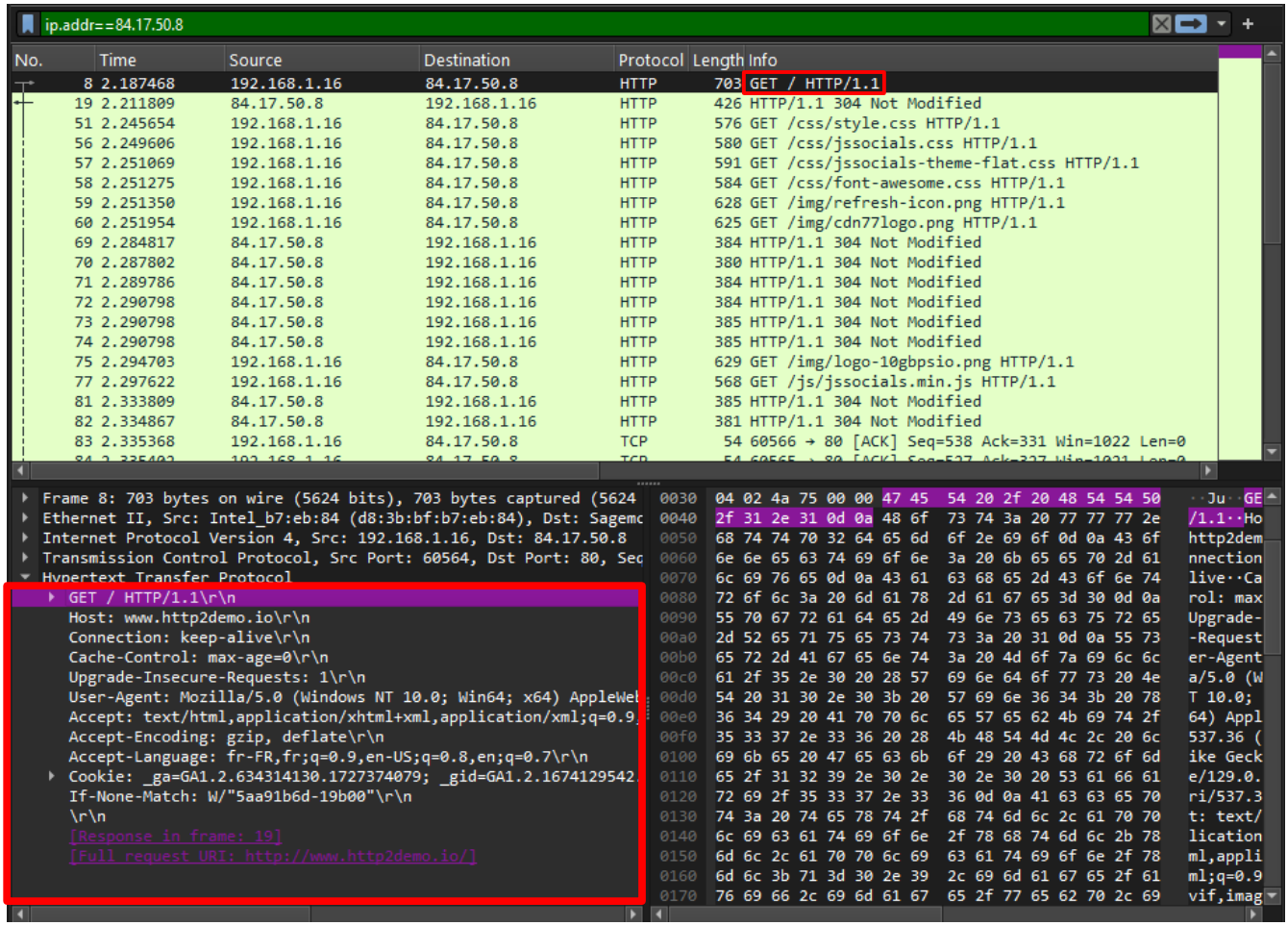
```
C:\Windows\system32>nslookup www.http2demo.io
Server:  bbox.lan
Address:  192.168.1.254

Non-authoritative answer:
Name:    1906714720.rsc.cdn77.org
Addresses:  2a02:6ea0:ca00::8
          2a02:6ea0:ca00::7
          84.17.50.9
          89.187.167.38
Aliases:  www.http2demo.io
```



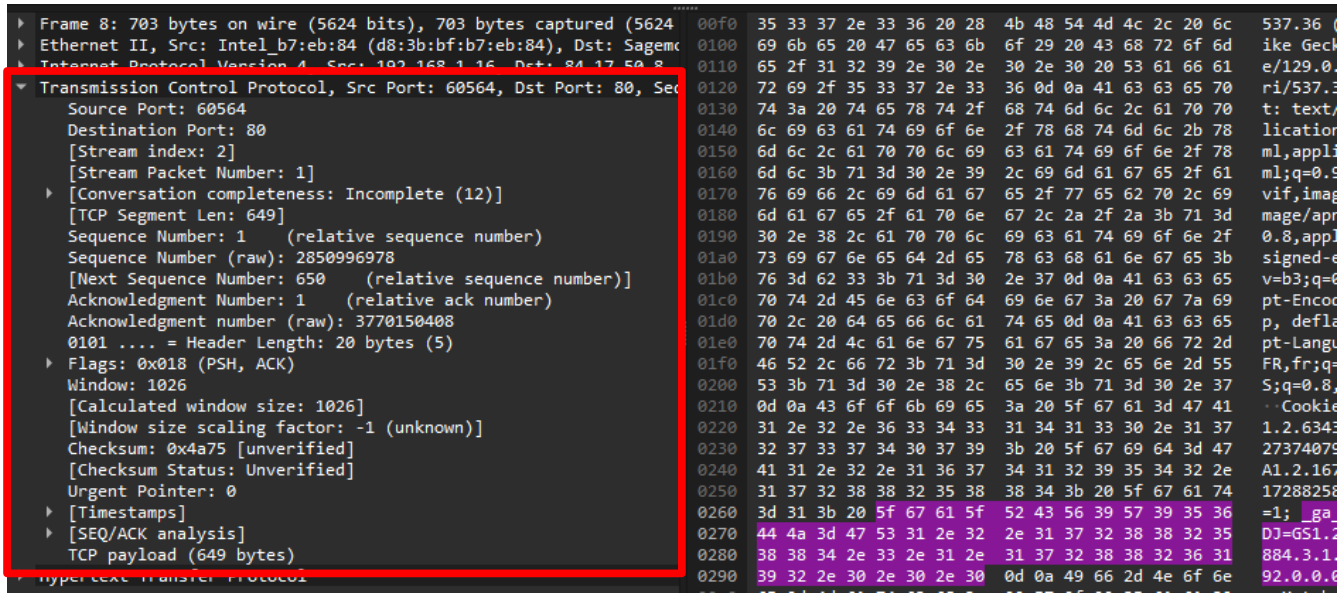
→ On applique un **filtre** où on spécifie l'adresse IP du **serveur http** qu'on vient de trouver :



→ On récupère la **trame** correspondant à la **requête http** puis on développe la section **protocole applicatif** :



→ On développe l'**en-tête de transport** :



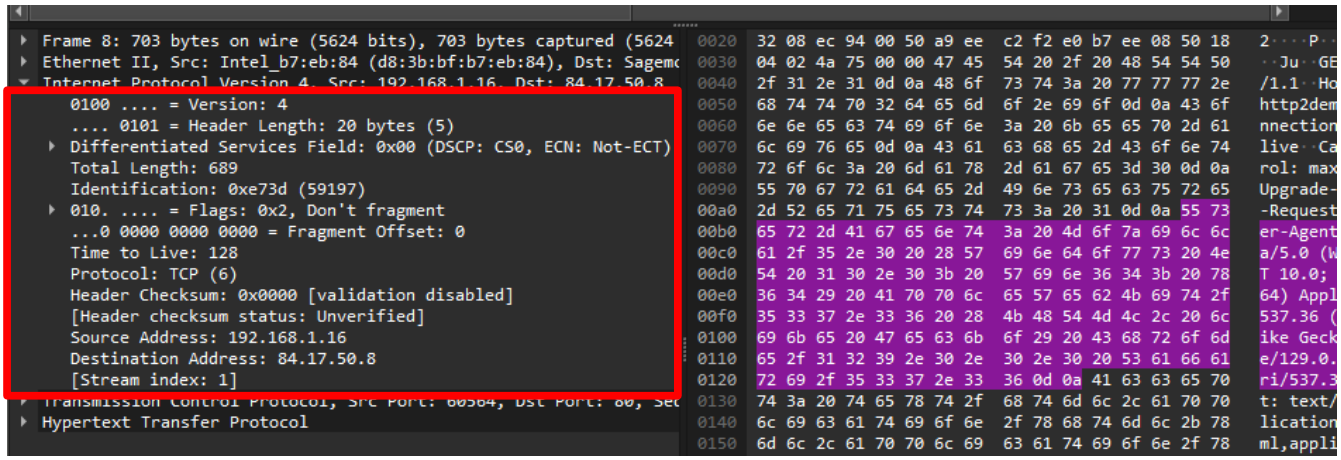
***** Le nom du **protocole** utilisé par une **trame http** est le protocole **TCP**.

***** Le nom du **PDU** encapsulant les **données applicatives http** est un **segment**.

***** La longueur de **l'en-tête de transport** est de **20 octets**.

***** Les valeurs **décimales** correspondant aux **port source** et aux **port destination** sont les ports **60564** et **80**. Les valeurs **hexadécimales** correspondantes sont **ec 94** et **00 50**.

→ On développe **l'en-tête Réseau** :

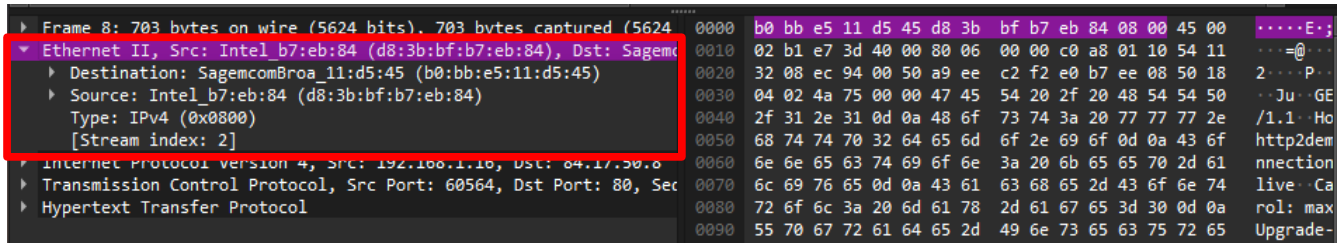


* La **longueur** de **l'en-tête réseau** est de **20 octets**.

* La valeur du **champ protocole** figurant dans l'en-tête réseau est **06**. Elle représente le **protocole TCP**.

* Les valeurs **décimales** des **adresses ip source** et **destination** sont **192.168.1.16** et **87.17.50.8** soit **c0 a8 01 10** et **54 11 32 08** en **hexadécimale**.

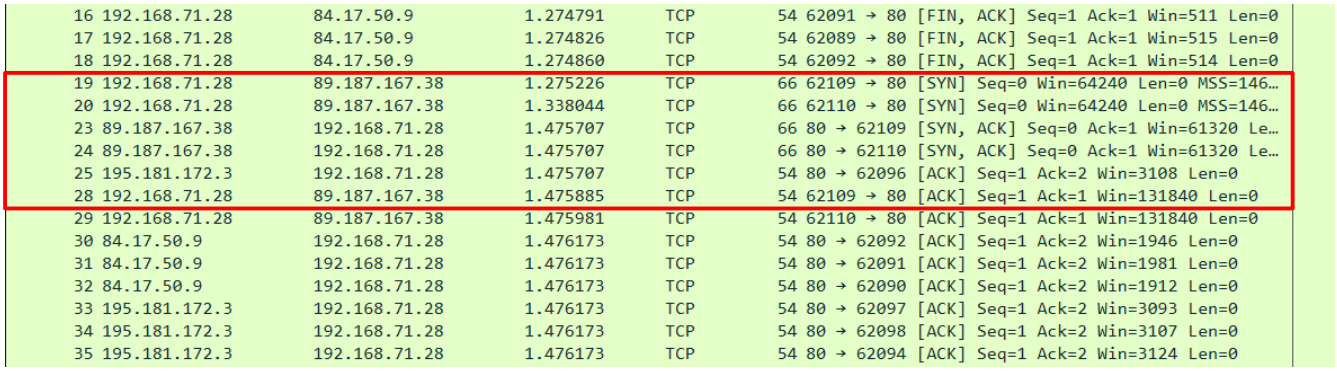
→ On développe **l'en-tête Ethernet** :

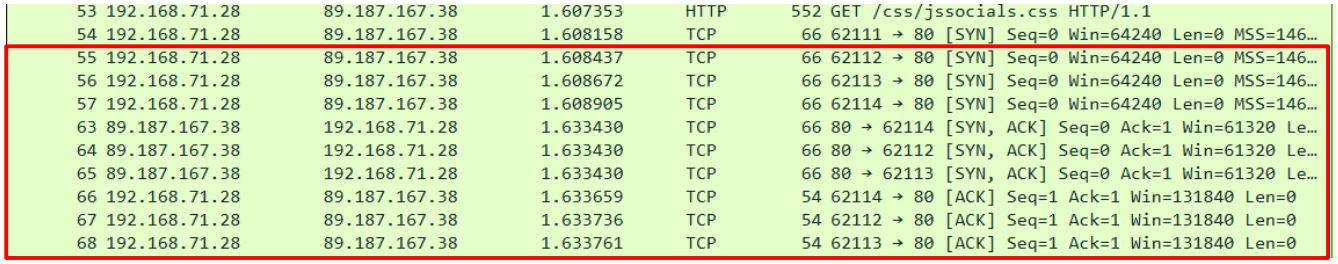


* Le **champ EtherType** se situe sur les **2 derniers octets** de l'en-tête Ethernet soit les octets **13** et **14**. La valeur contenue est **08 00** qui signifie **IPv4**.

* Les valeurs des **adresses MAC destination** et **source** sont **b0:bb:e5:11:d5:45** et **d8:3b:bf:b7:eb:84**.

→ On modifie le **filtre** et on réalise une capture d'écran des **3 trames** mettant en place la **connexion TCP** entre le client et le serveur :





53	192.168.71.28	89.187.167.38	1.607353	HTTP	552 GET /css/jssocials.css HTTP/1.1
54	192.168.71.28	89.187.167.38	1.608158	TCP	66 62111 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=146…
55	192.168.71.28	89.187.167.38	1.608437	TCP	66 62112 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=146…
56	192.168.71.28	89.187.167.38	1.608672	TCP	66 62113 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=146…
57	192.168.71.28	89.187.167.38	1.608905	TCP	66 62114 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=146…
63	89.187.167.38	192.168.71.28	1.633430	TCP	66 80 → 62114 [SYN, ACK] Seq=0 Ack=1 Win=61320 Le…
64	89.187.167.38	192.168.71.28	1.633430	TCP	66 80 → 62112 [SYN, ACK] Seq=0 Ack=1 Win=61320 Le…
65	89.187.167.38	192.168.71.28	1.633430	TCP	66 80 → 62113 [SYN, ACK] Seq=0 Ack=1 Win=61320 Le…
66	192.168.71.28	89.187.167.38	1.633659	TCP	54 62114 → 80 [ACK] Seq=1 Ack=1 Win=131840 Len=0
67	192.168.71.28	89.187.167.38	1.633736	TCP	54 62112 → 80 [ACK] Seq=1 Ack=1 Win=131840 Len=0
68	192.168.71.28	89.187.167.38	1.633761	TCP	54 62113 → 80 [ACK] Seq=1 Ack=1 Win=131840 Len=0

* Il y a ici **5 connexions TCP** établies.