TP3 – Les ports logiciels

Sommaire

1) Connexion Bureau à distance (RDP)

L’adresse IP de mon voisin est donc 172.17.2.8
(capture d’ecran de l’invite de commande de mon voisin)

```
C:\Windows\System32>netstat -no

Connexions actives

  Proto  Adresse locale         Adresse distante       État
  TCP    172.17.2.8:57242       104.75.232.13:80       TIME_WAIT       0
  TCP    172.17.2.8:57247       20.42.65.89:443        TIME_WAIT       0
  TCP    172.17.2.8:57260       172.17.254.5:445       ESTABLISHED     4
  TCP    172.17.2.8:57261       95.100.133.25:443      ESTABLISHED     15188
  TCP    172.17.2.8:57262       40.126.32.140:443      ESTABLISHED     1800
  TCP    172.17.2.8:57264       102.133.96.237:443     ESTABLISHED     15188
  TCP    172.17.2.8:57266       172.17.2.21:7680       SYN_SENT        11468
  TCP    172.17.2.8:57267       13.107.4.254:443       ESTABLISHED     15188
  TCP    172.17.2.8:57268       150.171.44.254:443     ESTABLISHED     15188
  TCP    172.17.2.8:57269       204.79.197.222:443     ESTABLISHED     15188
  TCP    172.17.2.8:59945       98.66.133.186:443      ESTABLISHED     4340
  TCP    172.17.2.8:59962       172.17.254.5:445       ESTABLISHED     4
  TCP    172.17.2.8:60248       23.200.86.235:443      CLOSE_WAIT      8360
  TCP    172.17.2.8:60501       172.17.2.3:7680        ESTABLISHED     11468
  TCP    172.17.2.8:60506       172.17.2.23:7680       ESTABLISHED     11468
  TCP    172.17.2.8:60507       172.17.2.19:7680       ESTABLISHED     11468
  TCP    172.17.2.8:60521       172.17.2.19:7680       ESTABLISHED     11468
  TCP    172.17.2.8:60553       172.17.2.23:7680       ESTABLISHED     11468
  TCP    172.17.2.8:60554       172.17.2.9:7680        ESTABLISHED     11468
  TCP    172.17.2.8:60557       172.17.2.19:7680       ESTABLISHED     11468
  TCP    172.17.2.8:60558       172.17.2.1:7680        ESTABLISHED     11468
  TCP    172.17.2.8:60560       172.17.2.3:7680        ESTABLISHED     11468
```

je fait un ping pour m’assurer de la connectivité entre ma machine et celle de mon voisin :

```
C:\Users\mballester>ping 172.17.2.8

Envoi d’une requête 'Ping'  172.17.2.8 avec 32 octets de données
Réponse de 172.17.2.8 : octets=32 temps=2 ms TTL=128
Réponse de 172.17.2.8 : octets=32 temps=2 ms TTL=128
Réponse de 172.17.2.8 : octets=32 temps=2 ms TTL=128
Réponse de 172.17.2.8 : octets=32 temps=2 ms TTL=128

Statistiques Ping pour 172.17.2.8:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 2ms, Maximum = 2ms, Moyenne = 2ms
```

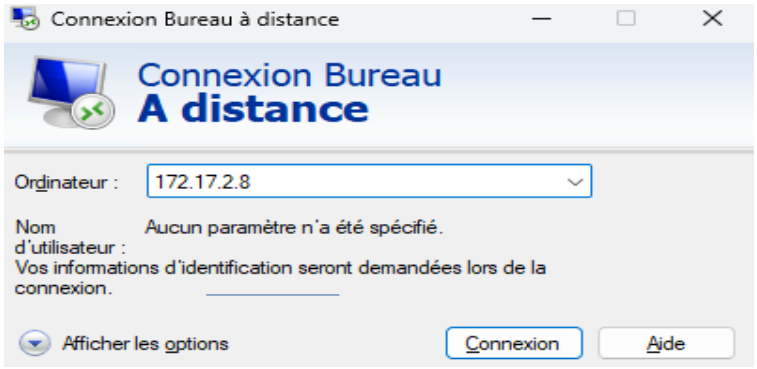
activation du paramètres bureau a distance

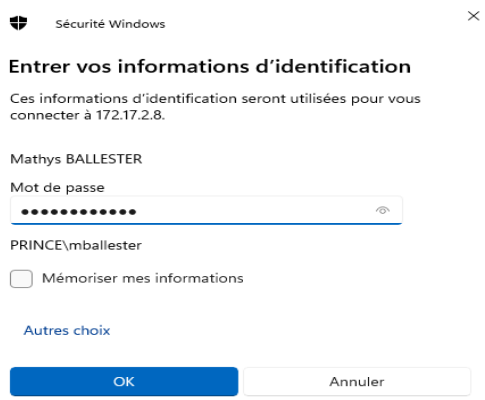
saisie de la commande netstat -an dans l'invite de commande :

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

Connexions actives

  Proto  Adresse locale          Adresse distante        État
  TCP    0.0.0.0:80             0.0.0.0:0              LISTENING
  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    0.0.0.0:902            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:912            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:2179           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:3306           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:3307           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    0.0.0.0:49664          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    0.0.0.0:61263          0.0.0.0:0              LISTENING
  TCP    127.0.0.1:27017        0.0.0.0:0              LISTENING
  TCP    172.17.2.14:139        0.0.0.0:0              LISTENING
```

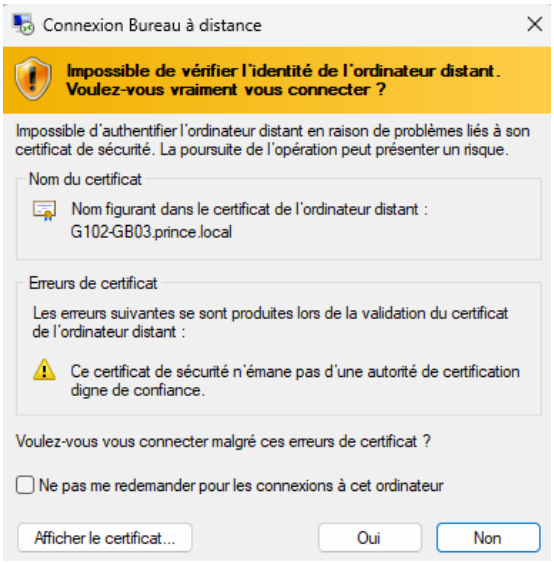
le port d'écoute du serveur Terminal Server est donc le port 3389

je saisie l'adresse IP de mon voisin sur connexion bureau a disatance puis je clique sur connexion

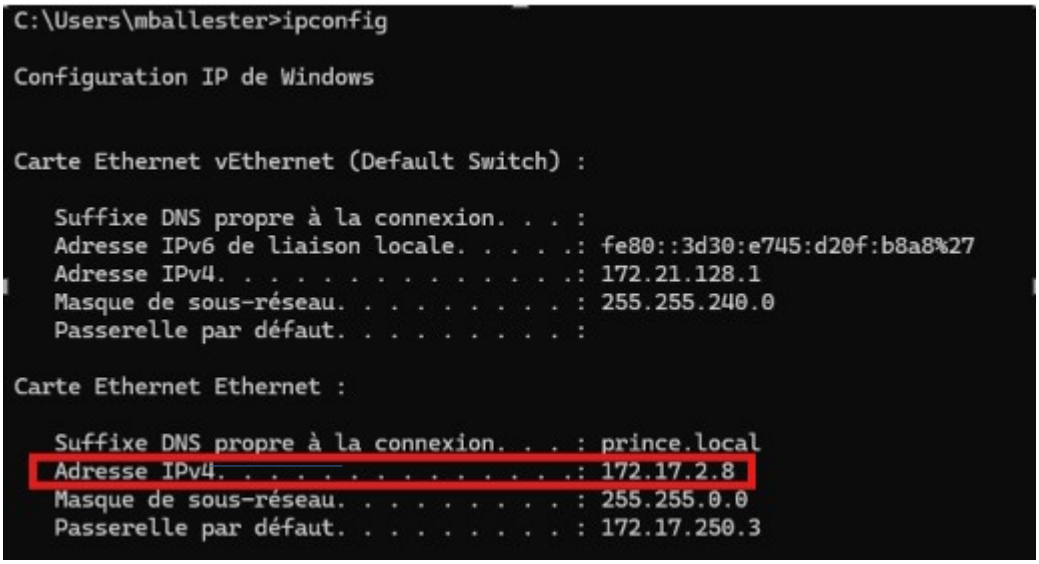




je clique sur oui :



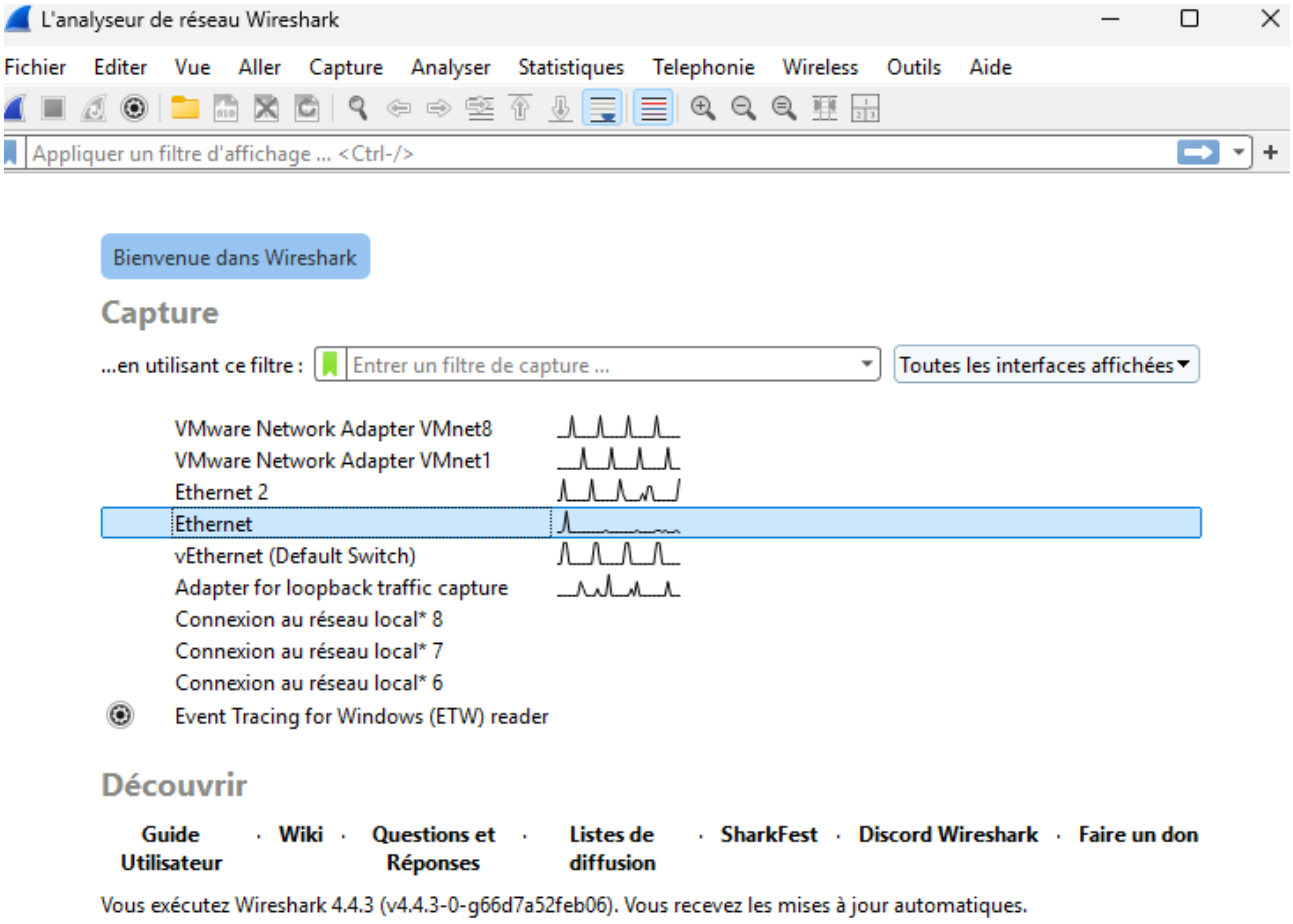
je tape netstat -an dans l'invite de commande de la machine de mon voisin :

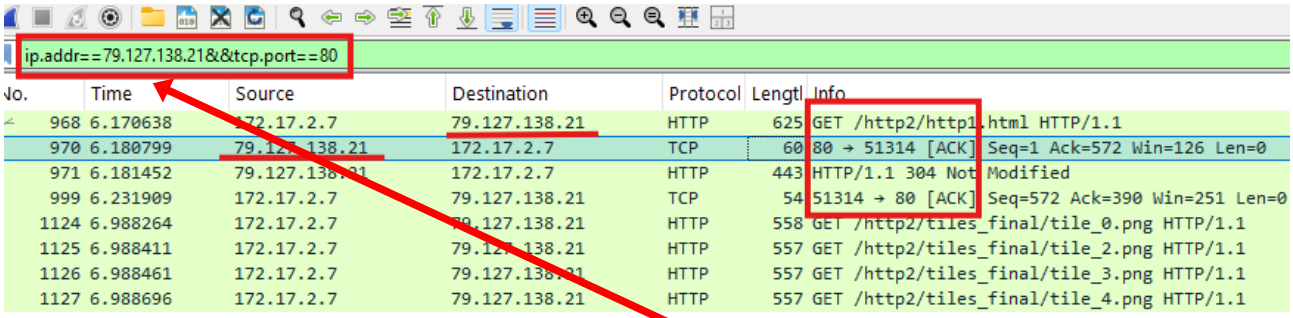


et je clique sur deconnecter pour bien me deconnecter de la machine de mon voisin.

2) Capture de trames HTTP

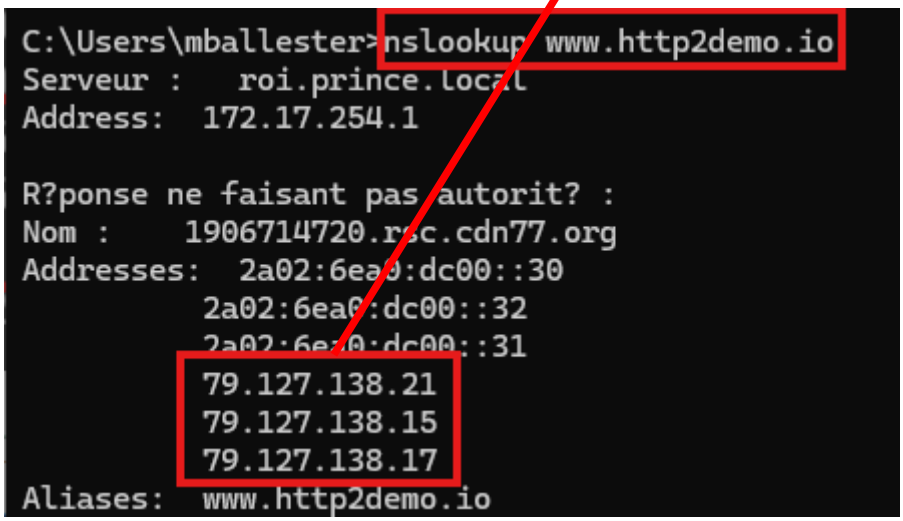
Lancement de wireshark:



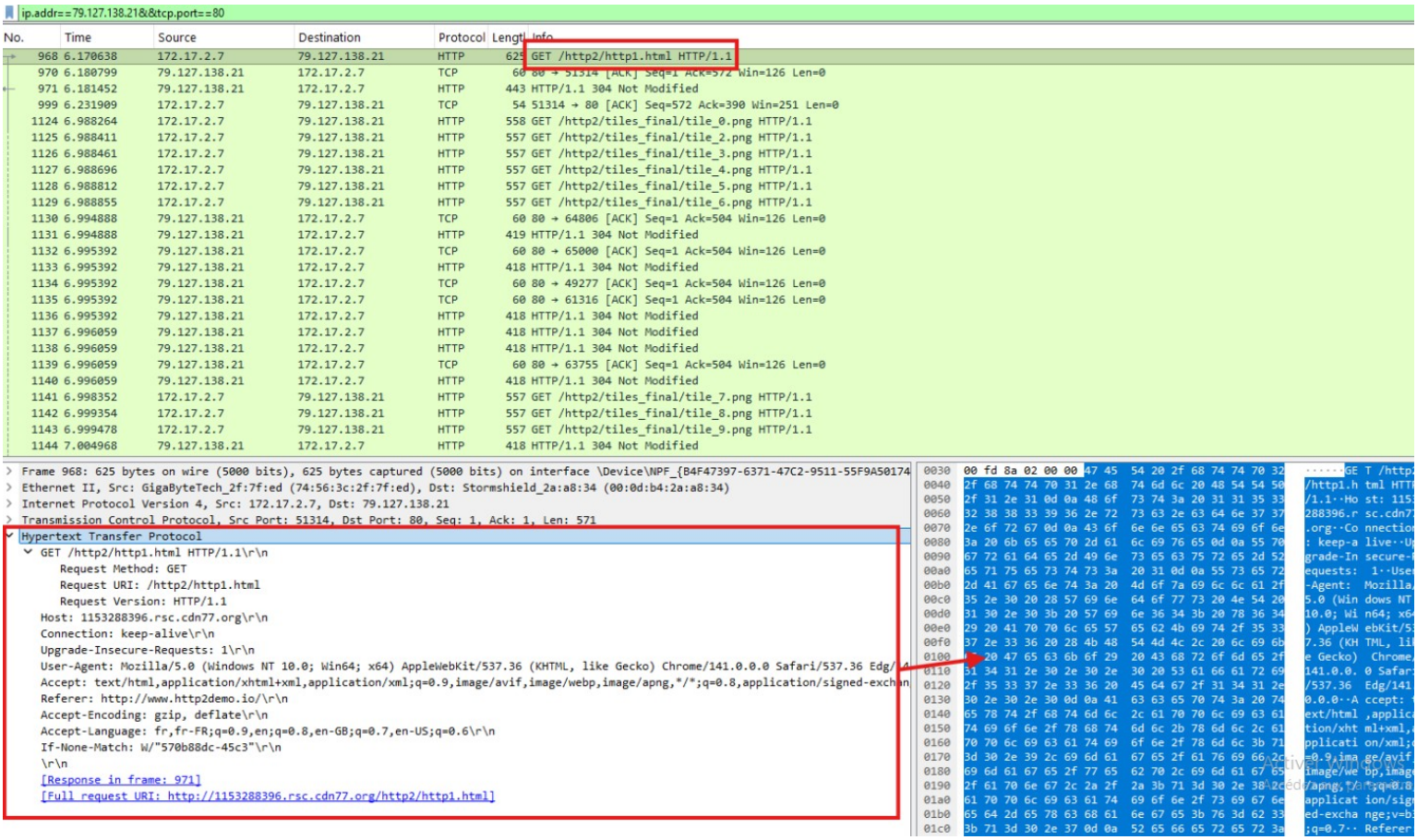


filtrage de la capture de trame a l'aide de l'adresse IP et du port TCP 80 du serveur http

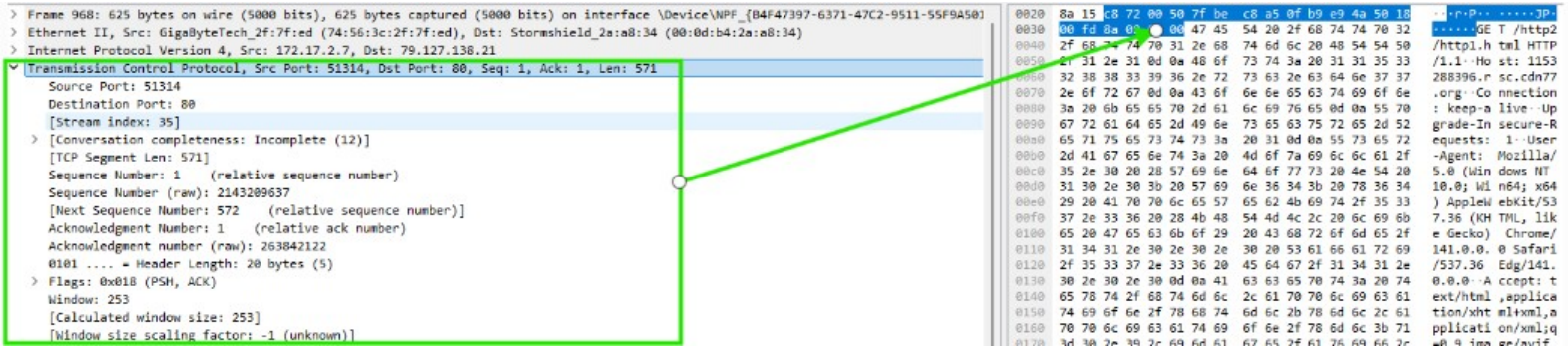
Saisie, depuis l'invite de commandes, la commande nslookup www.http2demo.io pour obtenir les adresses IP du serveur web:



Repérage de la Trame de notre requête http:



Développement de la section correspondant a l'en tête de transport :



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

- Le nom du protocole de transport utilisé par la une trame HTTP est le protocole TCP (06)

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

- Le nom de PDU encapsulent les données applicaties HTTP est le segment

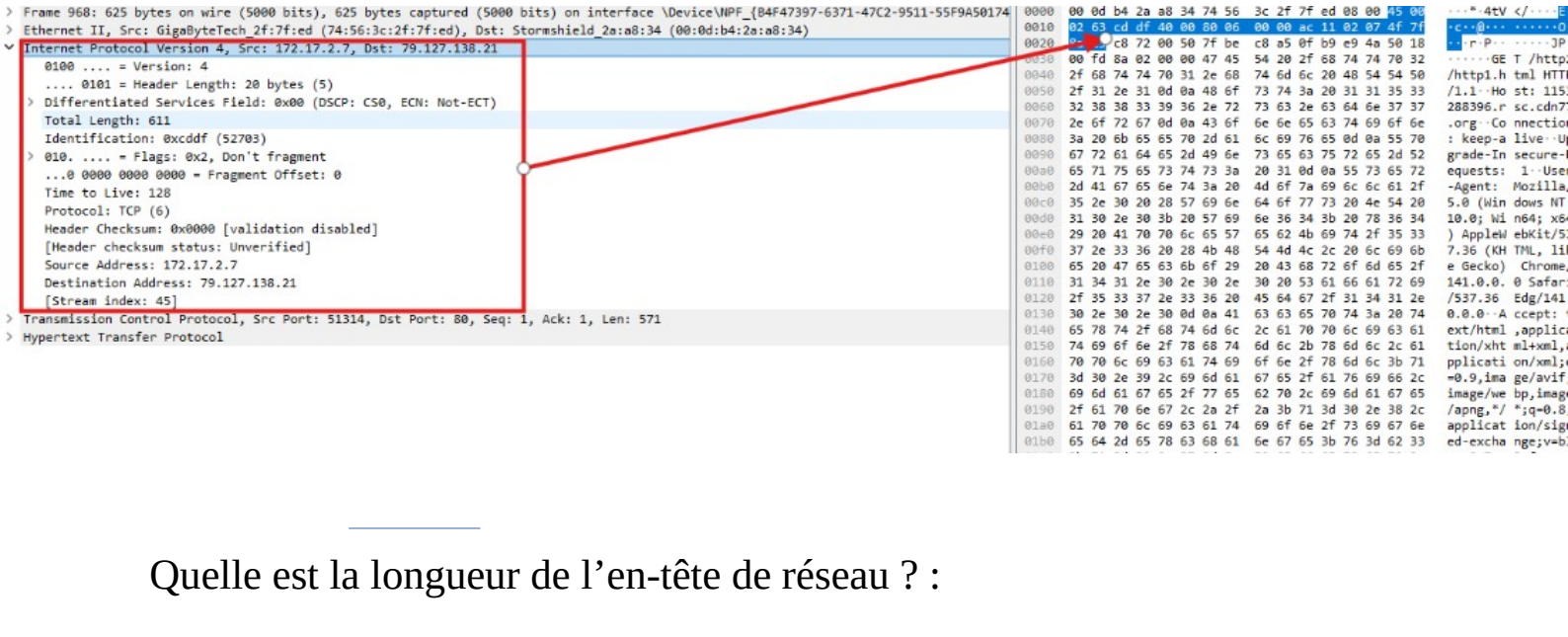
Quelle est la longueur de l’en-tête de transport ? :

- La longueur de l’en tête de transport est de 20 bytes (octets)

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

- la valeur en décimal du port source est 63937 et en hexadécimal ça valeur est F7A5
- la valeur en décimal du port destination est 80 soit 0050 en hexadécimal

Développement de la section correspondant a l’en tête Réseaux :



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

- La longueur de l’en tête de réseaux est de 20 bytes (octets)

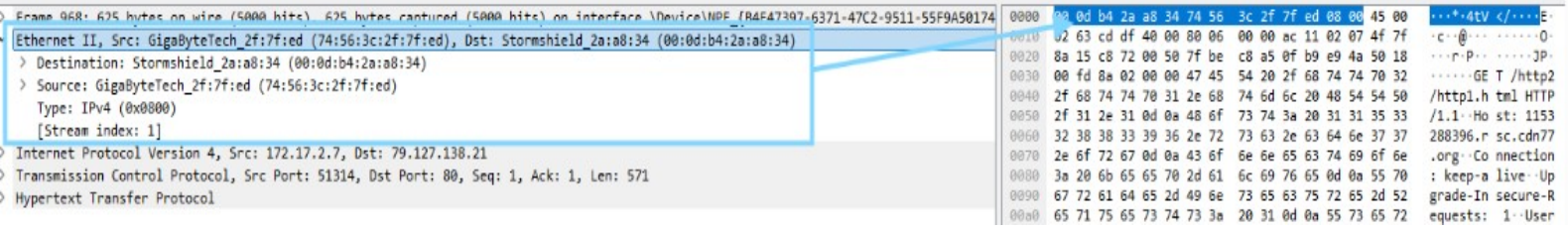
Repérez le champ Protocole figurant dans l’en-tête Réseau. Quelle est la valeur présente ?Que signifie-t-elle ? :

- La valeur du champ protocole est 06
- Cela signifie que derrière il va y avoir un segment TCP

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

- La valeur décimal de l’adresse IP source est 127.17.2.7 et ça valeur en hexadecimal est 7F-11-02-07
- La valeur décimal de l’adresse IP destination est 79.127.138.14 soit 4F-7F-8A-0E

Développement de la section correspondant a l’en tête Ethernet :



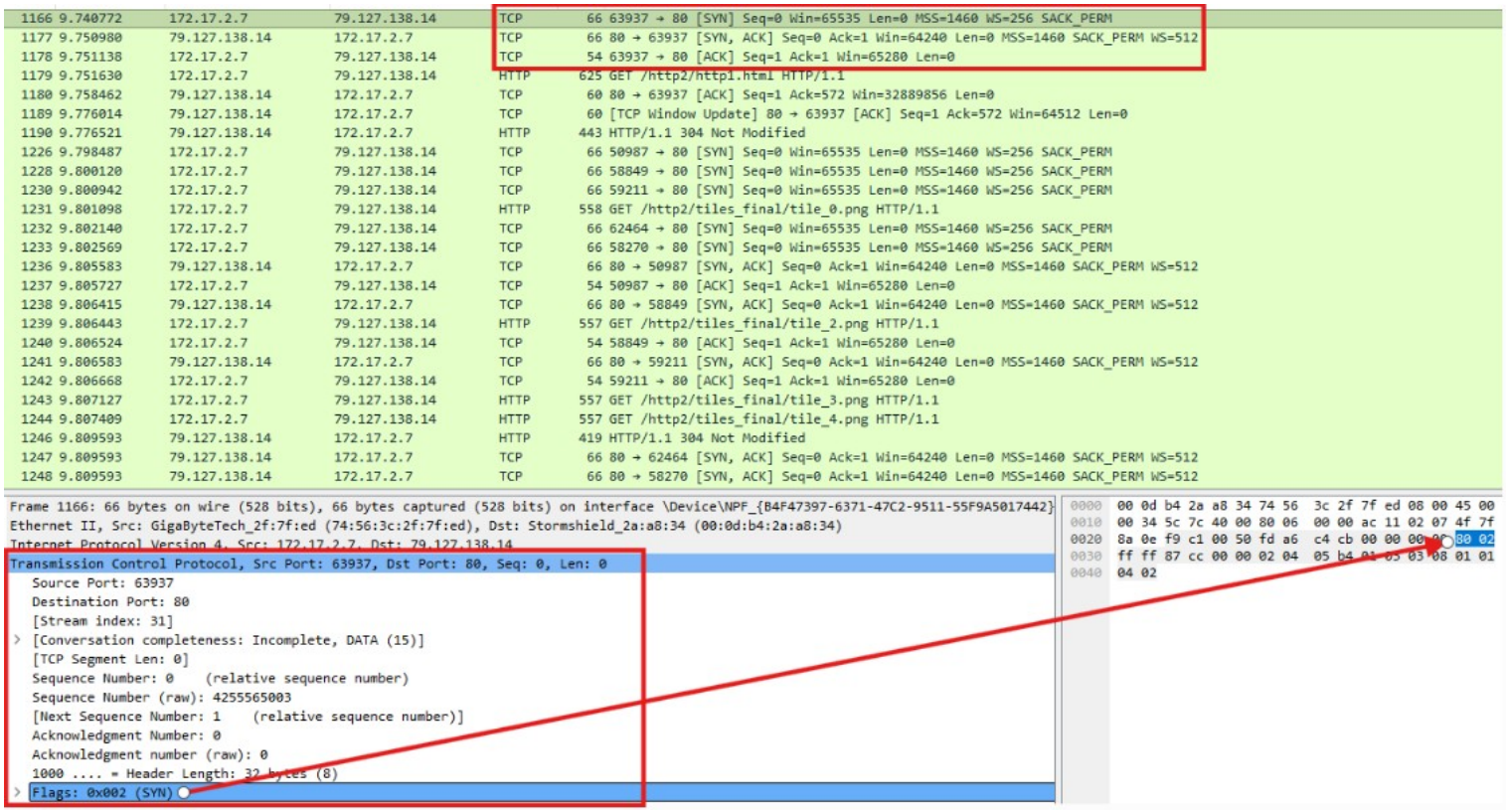
Repérez le champ EtherType. Quel est la valeur contenue ? Que signifie-t-elle ? :

- Le champ Ethertype contient la valeur 0800
- Ce qui signifie que derrière il va y avoir un paquet IP, c’est donc IPV4

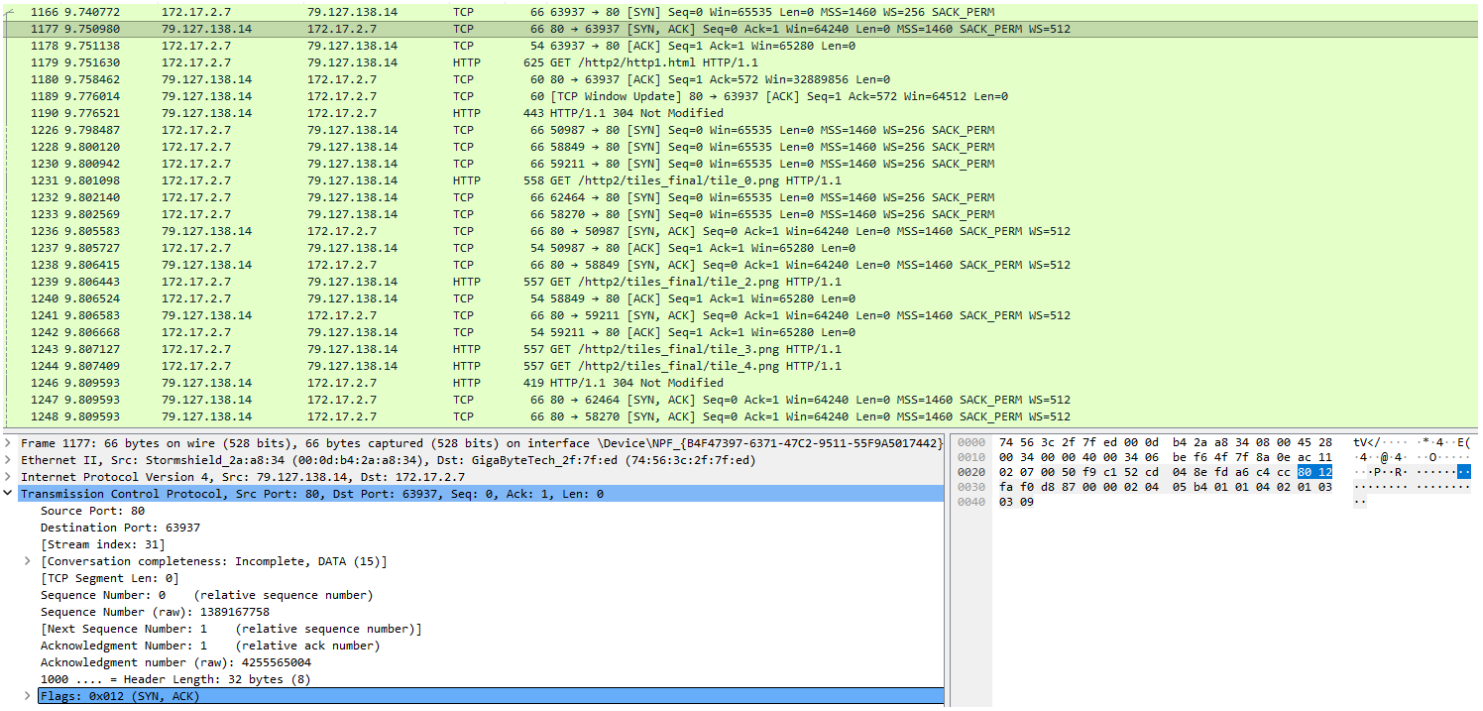
Quelles sont les valeurs des adresses MAC destination et source ? :

- Valeur MAC destination : 00-0d-b4-2a-a8-34
- Valeur MAC source : 74-56-3c-2f-7f-ed

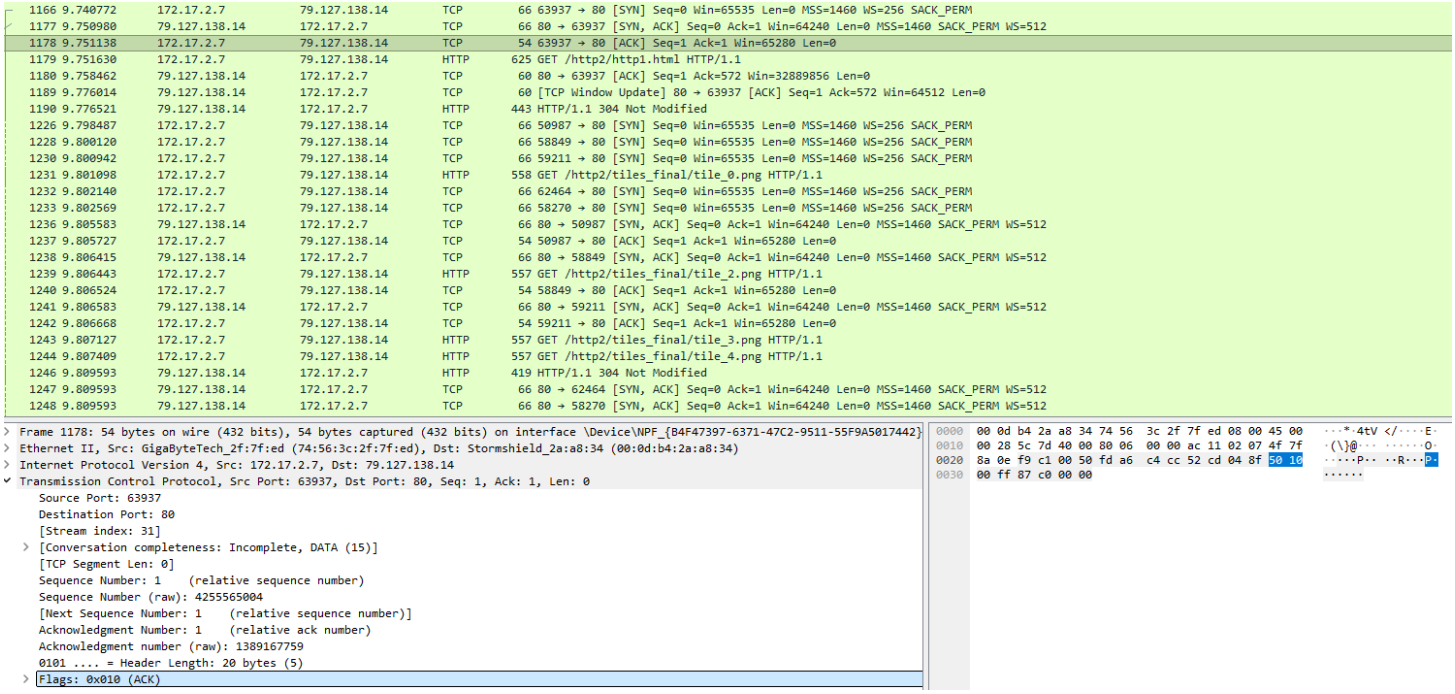
Repérage des trames associées à la mise en place de la connexion TCP entre le client et le serveur :



Le champ Flags dans l’en-tête de segment est : 0x002



Le champ Flags dans l’en-tête de segment est : 0x012



Le champ Flags dans l’en-tête de segment est : 0x010

Le contenu de ce champ signifie :

1. Pour le premier SYN : Cela signifie que le client veut initier une connexion avec le serveur
2. Pour le deuxième SYN + ACK : Cela signifie le serveur envoie lui aussi une demande de connexion et accepte la demande précédente du client
3. Pour le Troisième ACK : Cela signifie que le client accepte a son tour la demande du serveur

Quelle est la raison de la mise en place de ce mode connecté ? :

- La raison de la mise en place de ce mode connecté est que il est un moyen de s’assurer que les informations ont toutes été transmises et sans problème notamment en accusant réception systématiquement de les paquets reçu. Il garantit la remise (le paquet est bien arrivé), l’intégrité (sans erreur) et le séquencement (dans l’ordre). Il garantit donc plus de sécurité dans le transport.