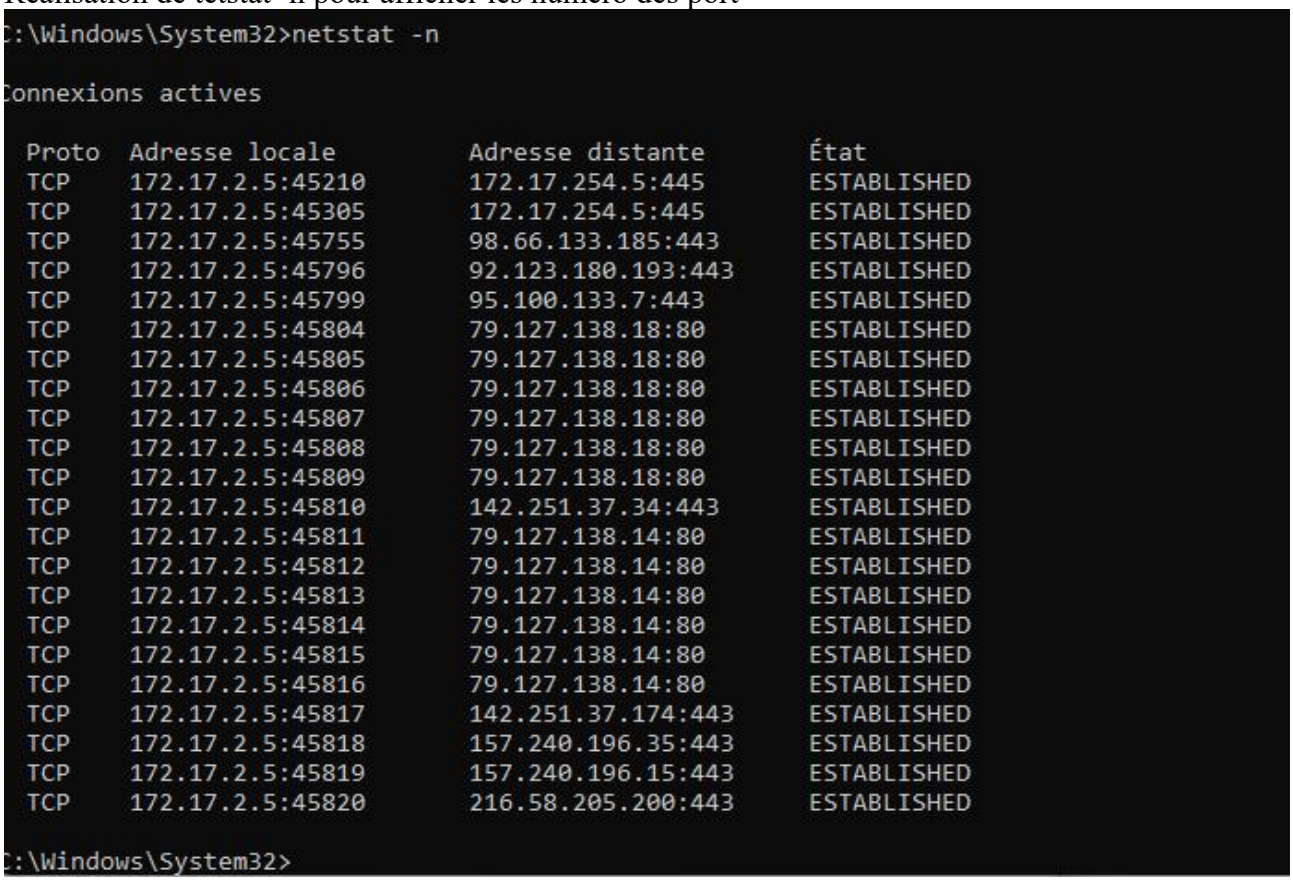
TP3-Les ports logiciels

1. Connexion Dureau à distance (RPD)

Le but de cette question et de réaliser une connexion a distance entre 2 machine a l'aide le IP

Realisation de tetstat -n pour afficher les numéro des port



```
C:\Windows\System32>netstat -n

Connexions actives

  Proto  Adresse locale         Adresse distante       État
  TCP    172.17.2.5:45210       172.17.254.5:445       ESTABLISHED
  TCP    172.17.2.5:45305       172.17.254.5:445       ESTABLISHED
  TCP    172.17.2.5:45755       98.66.133.185:443      ESTABLISHED
  TCP    172.17.2.5:45796       92.123.180.193:443     ESTABLISHED
  TCP    172.17.2.5:45799       95.100.133.7:443       ESTABLISHED
  TCP    172.17.2.5:45804       79.127.138.18:80       ESTABLISHED
  TCP    172.17.2.5:45805       79.127.138.18:80       ESTABLISHED
  TCP    172.17.2.5:45806       79.127.138.18:80       ESTABLISHED
  TCP    172.17.2.5:45807       79.127.138.18:80       ESTABLISHED
  TCP    172.17.2.5:45808       79.127.138.18:80       ESTABLISHED
  TCP    172.17.2.5:45809       79.127.138.18:80       ESTABLISHED
  TCP    172.17.2.5:45810       142.251.37.34:443      ESTABLISHED
  TCP    172.17.2.5:45811       79.127.138.14:80       ESTABLISHED
  TCP    172.17.2.5:45812       79.127.138.14:80       ESTABLISHED
  TCP    172.17.2.5:45813       79.127.138.14:80       ESTABLISHED
  TCP    172.17.2.5:45814       79.127.138.14:80       ESTABLISHED
  TCP    172.17.2.5:45815       79.127.138.14:80       ESTABLISHED
  TCP    172.17.2.5:45816       79.127.138.14:80       ESTABLISHED
  TCP    172.17.2.5:45817       142.251.37.174:443     ESTABLISHED
  TCP    172.17.2.5:45818       157.240.196.35:443     ESTABLISHED
  TCP    172.17.2.5:45819       157.240.196.15:443     ESTABLISHED
  TCP    172.17.2.5:45820       216.58.205.200:443     ESTABLISHED

C:\Windows\System32>
```

je réalisé âpres un IPconfig pour avoir les diffèrent IP des différente machine .

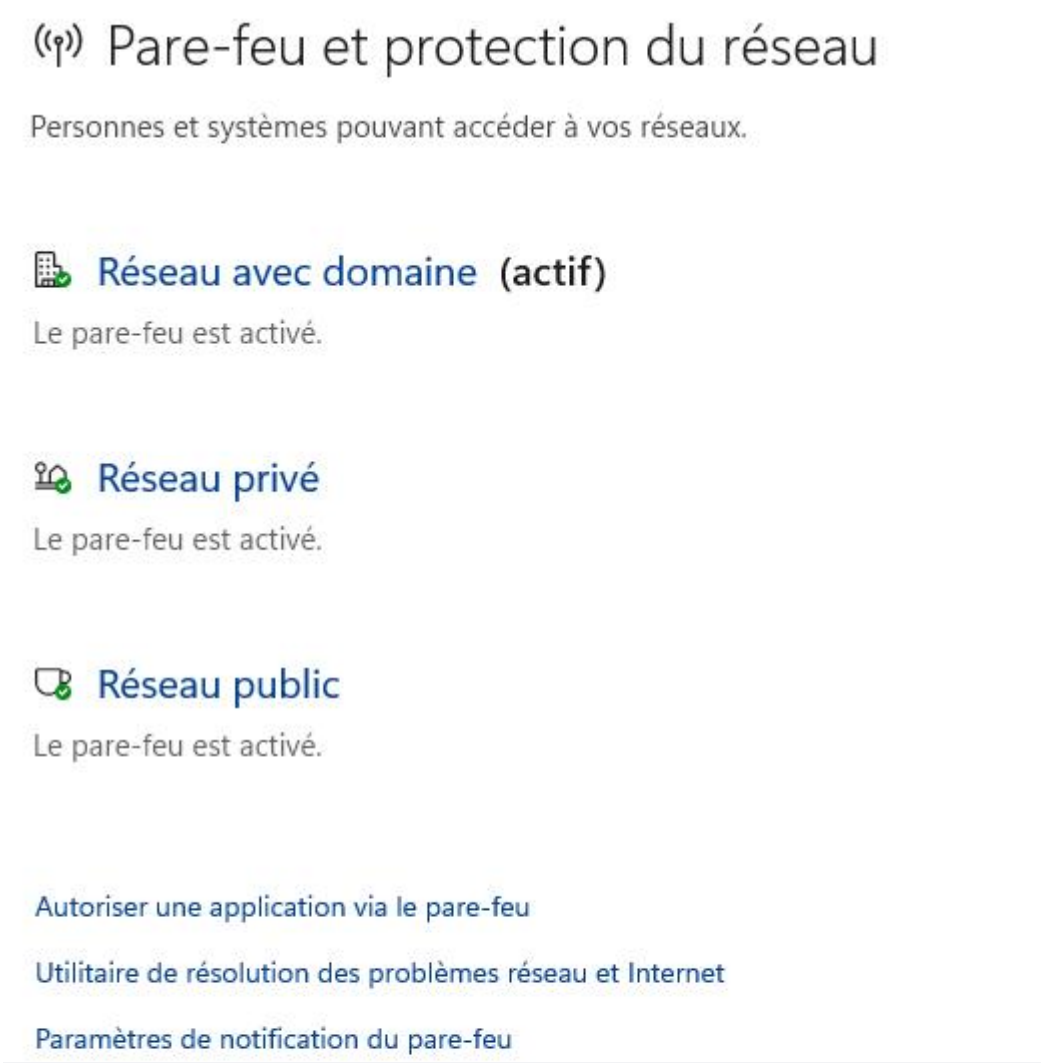
TP3-Les ports logiciels

```
:\Windows\System32>ipconfig

onfiguration IP de Windows


arte Ethernet vEthernet (Default Switch) :

   Suffixe DNS propre à la connexion. . . :
   Adresse IPv6 de liaison locale. . . . .: fe80::e1b8:ff83:a292:cfeb%32
   Adresse IPv4. . . . . . . . . . . . . .: 172.28.80.1
   Masque de sous-réseau. . . . . . . . . : 255.255.240.0
   Passerelle par défaut. . . . . . . . . :

arte Ethernet Ethernet :

   Suffixe DNS propre à la connexion. . . : prince.local
   Adresse IPv6 de liaison locale. . . . .: fe80::799d:d2f6:3731:5c6b%3
   Adresse IPv4. . . . . . . . . . . . . .: 172.17.2.5
   Masque de sous-réseau. . . . . . . . . : 255.255.0.0
   Passerelle par défaut. . . . . . . . . : 172.17.250.3

arte Ethernet Ethernet 2 :

   Suffixe DNS propre à la connexion. . . :
   Adresse IPv6 de liaison locale. . . . .: fe80::98f8:f579:7a9c:4400%14
   Adresse d'autoconfiguration IPv4 . . . : 169.254.47.166
   Masque de sous-réseau. . . . . . . . . : 255.255.0.0
```

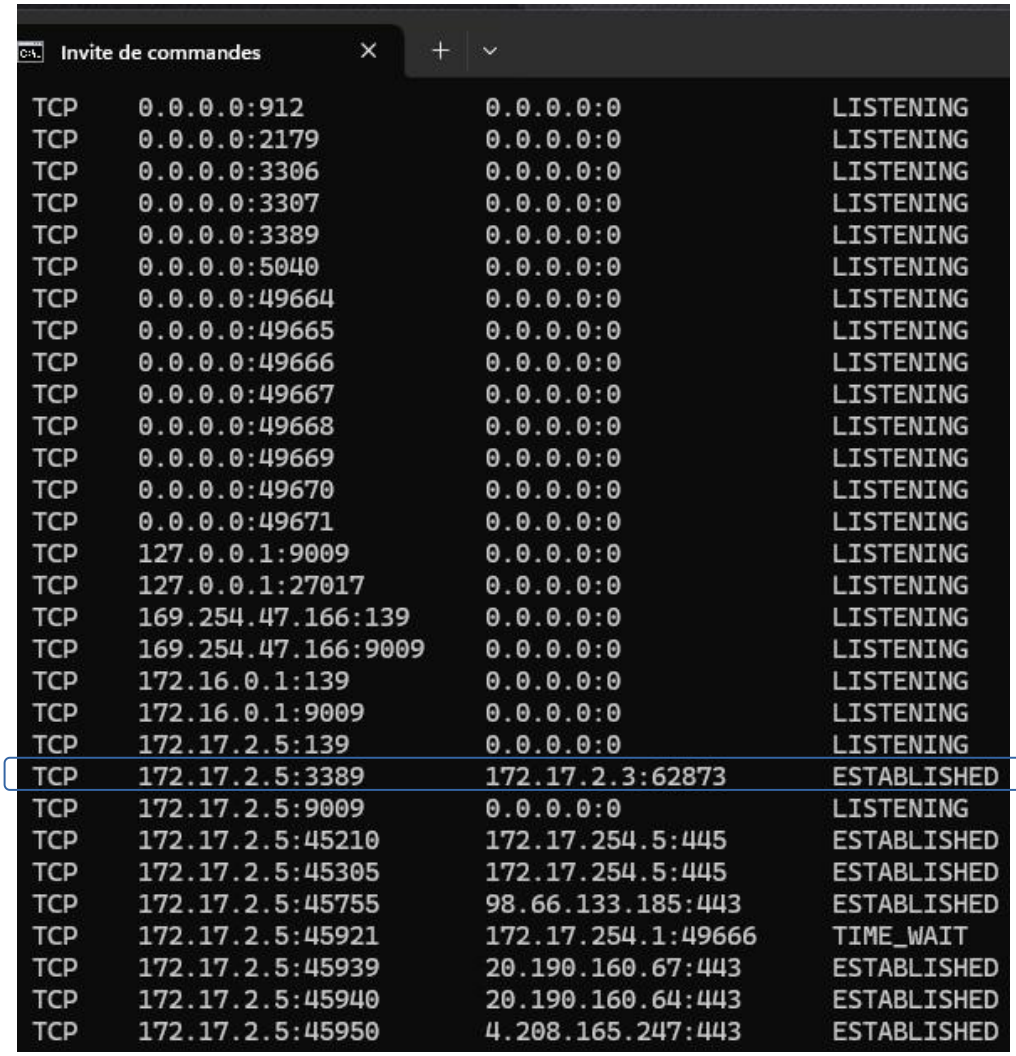
je réalise ensuite un Ping de la machine a la quel je vais essayer de me connecter .

```
C:\Windows\System32>ping 172.17.2.3

Envoi d'une requête 'Ping'  172.17.2.3 avec 32 octets de données :
Réponse de 172.17.2.3 : octets=32 temps=1 ms TTL=128
Réponse de 172.17.2.3 : octets=32 temps=2 ms TTL=128
Réponse de 172.17.2.3 : octets=32 temps=2 ms TTL=128
Réponse de 172.17.2.3 : octets=32 temps=1 ms TTL=128

Statistiques Ping pour 172.17.2.3:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 1ms, Maximum = 2ms, Moyenne = 1ms

C:\Windows\System32>
```

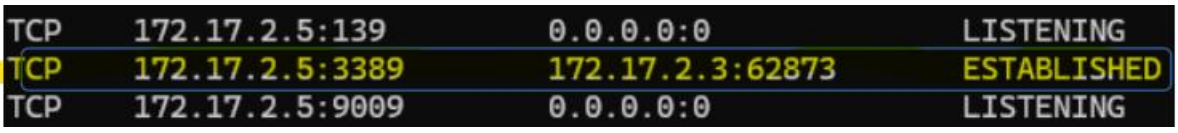
TP3-Les ports logiciels



TP3-Les ports logiciels



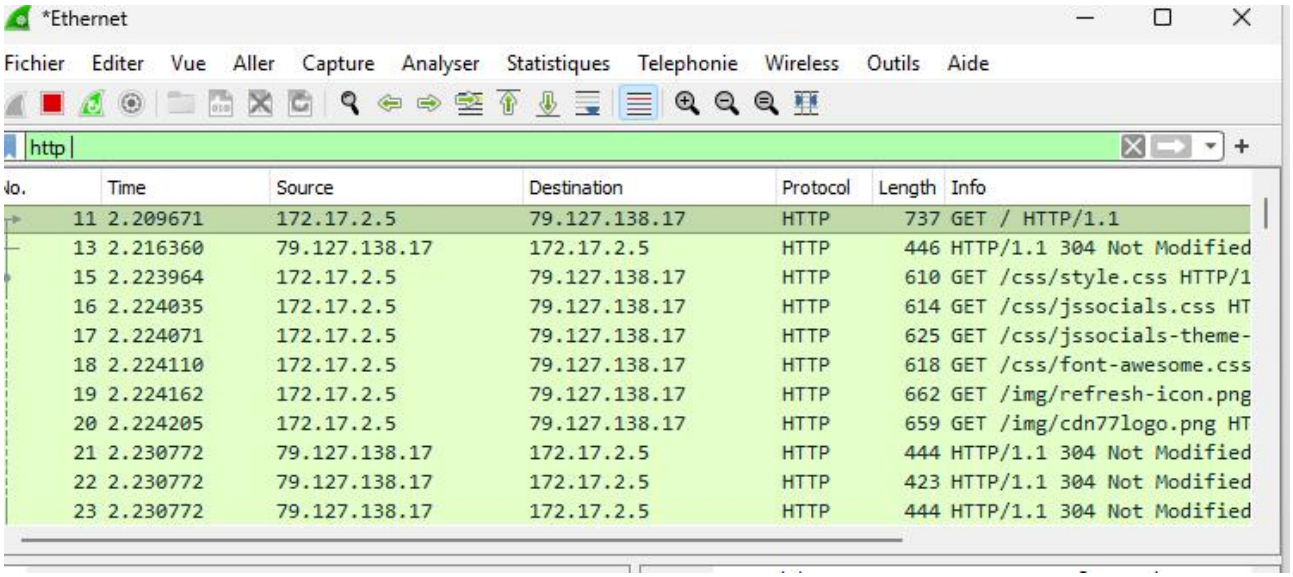
Quel est le port d'écoute du serveur Terminal Server ?

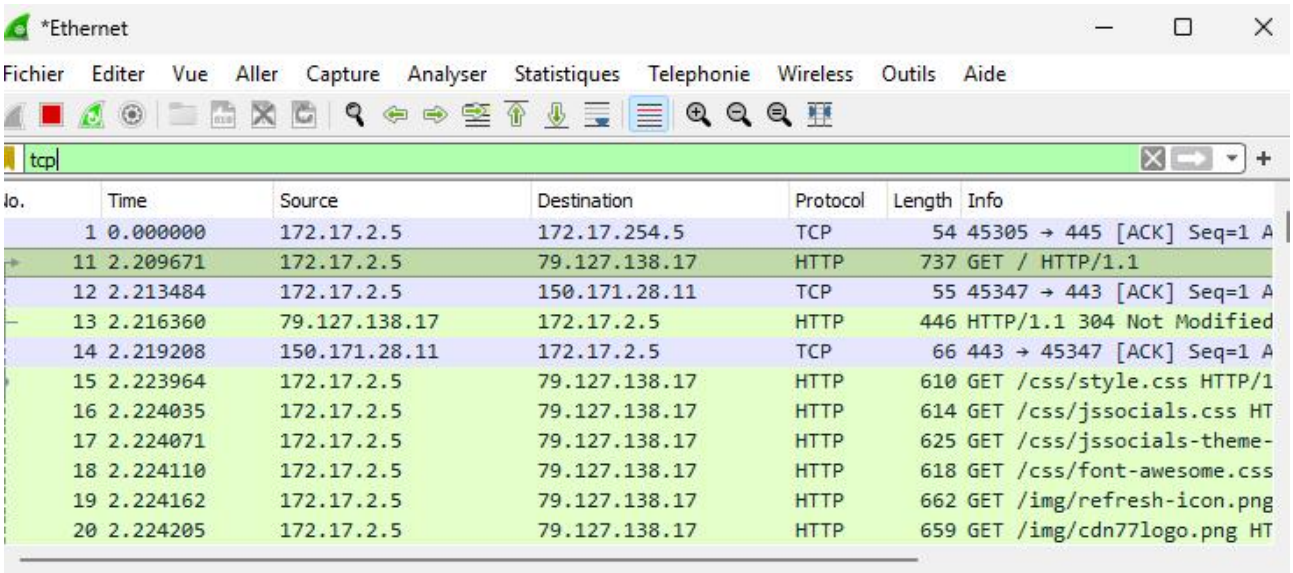


Apres avoir saisie la commande netstat -an, j'obtiens le port d'écoute terminal serveur

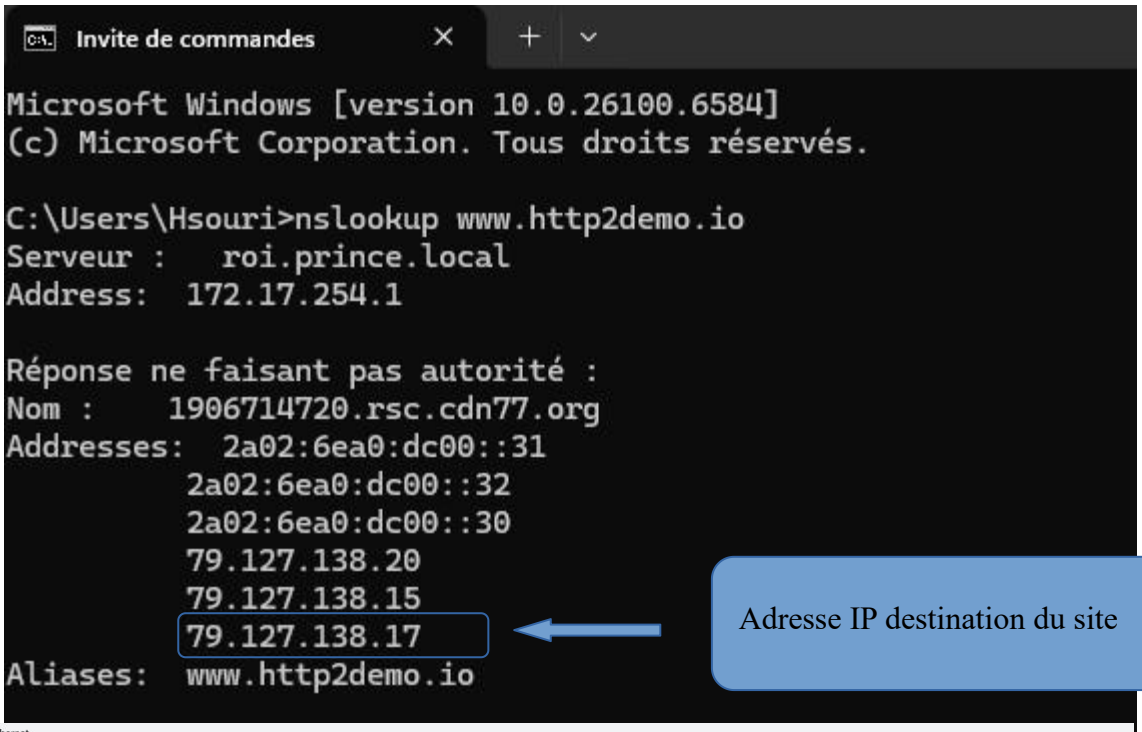
TP3-Les ports logiciels

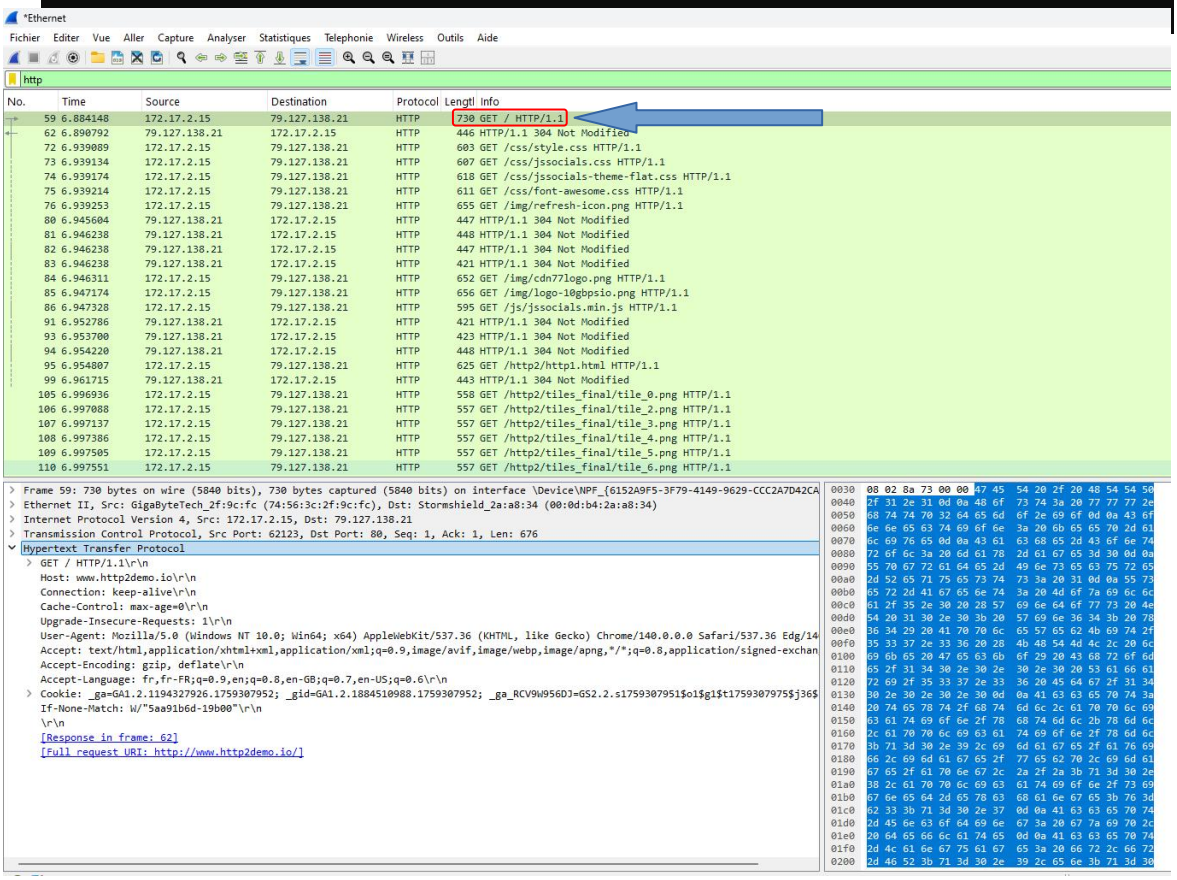
2. Capture de trames HTTP



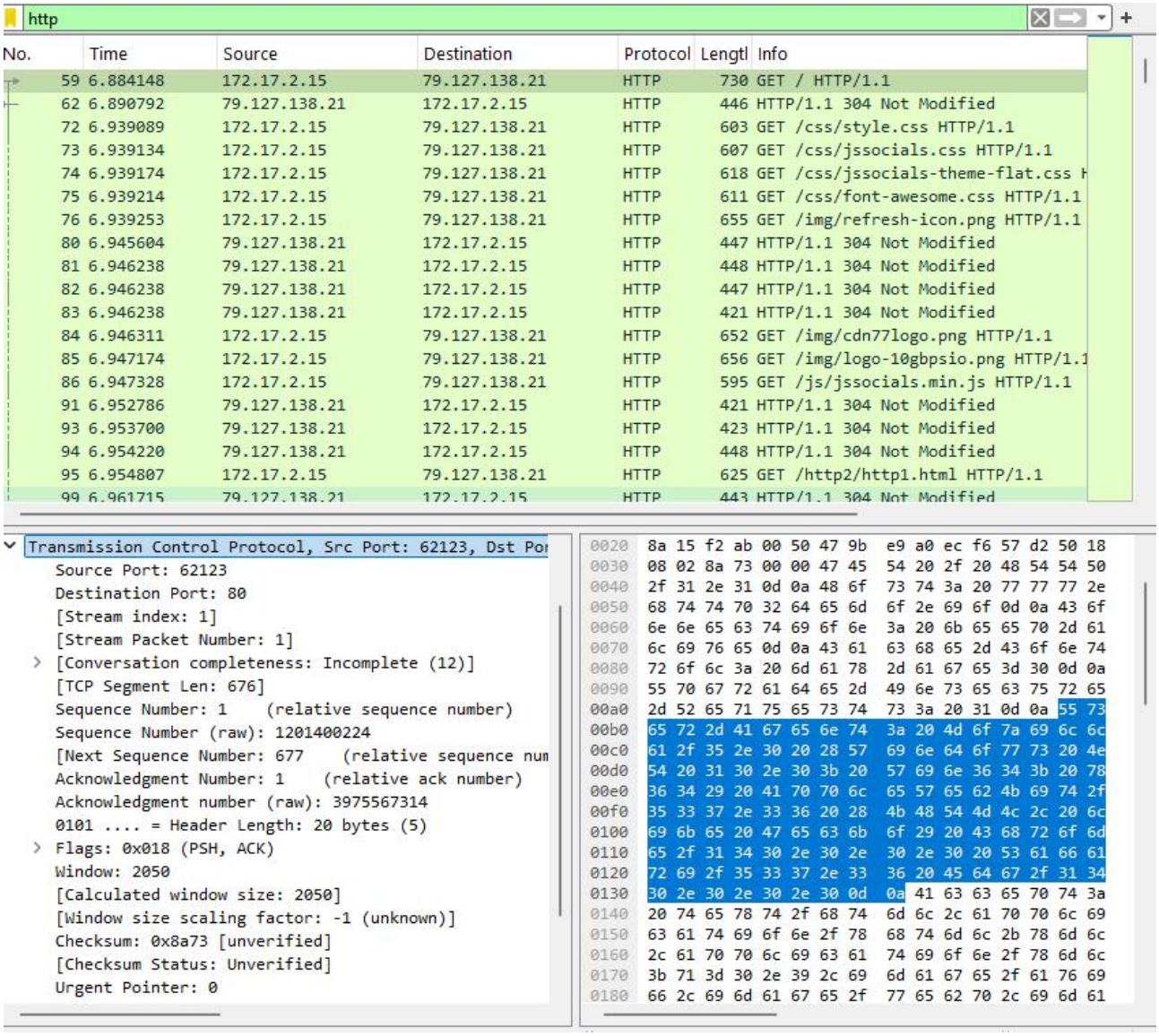


TP3-Les ports logiciels



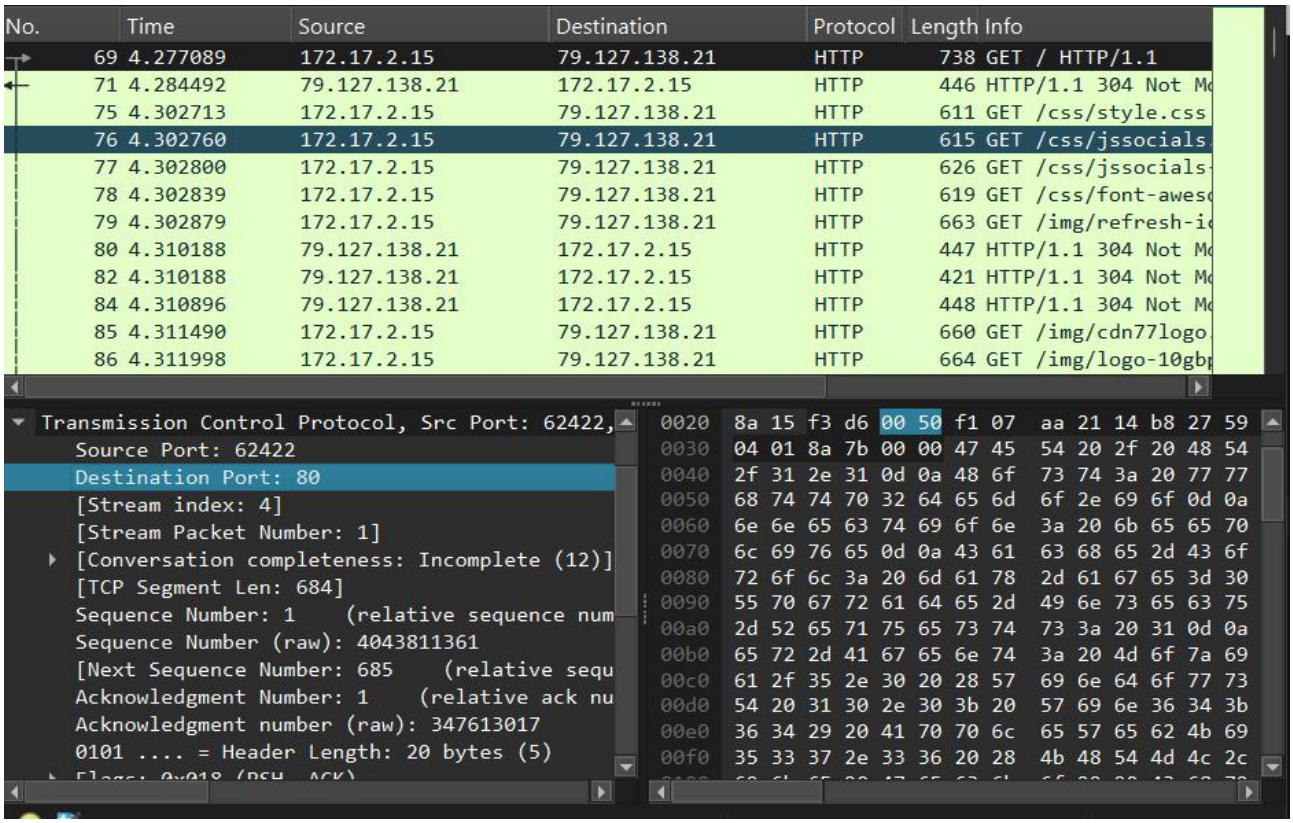


TP3-Les ports logiciels



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

TP3-Les ports logiciels



le nom du protocole transport utilisé par une trame HTTP est TCP

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

Le PDU qui encapsule les données applicatives HTTP dépend de la couche du modèle OSI ou TCP/IP

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

L'en-tête TCP a une longueur minimale de 20 octets.

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

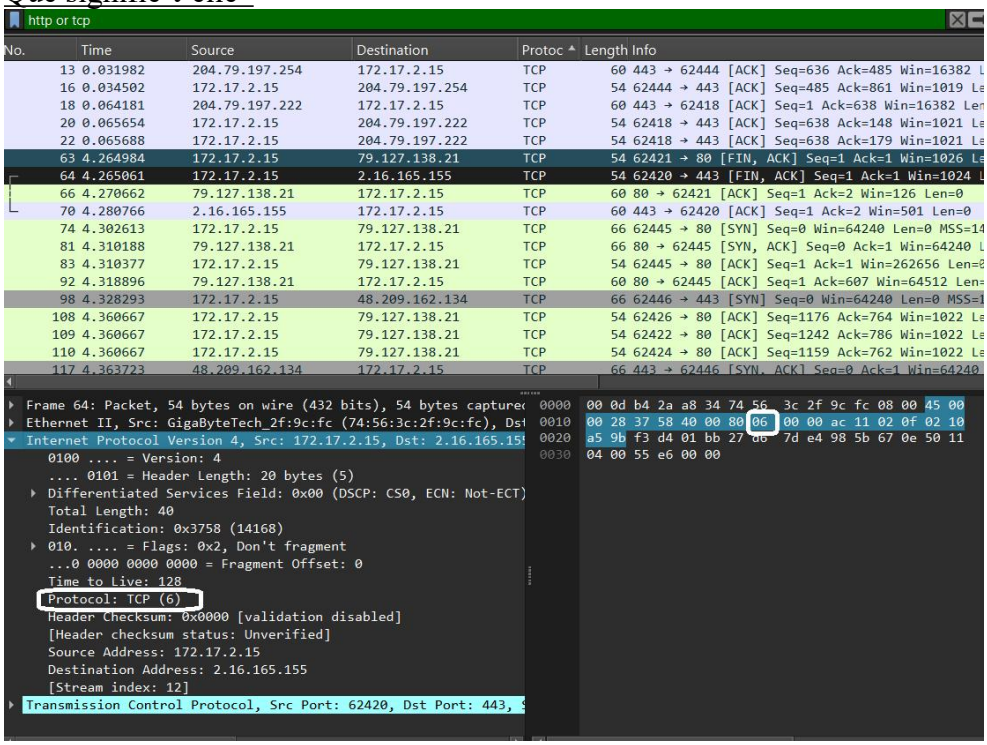
Le port destination est 80 décimal et 0x50 en hexadécimal
Et le port source est 62420 en décimal et 0xf3d4 en hexadécimal

Quelle est la longueur de l'en-tête de réseau ?

L'en-tête réseaux a une longueur de 20 octets

TP3-Les ports logiciels

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



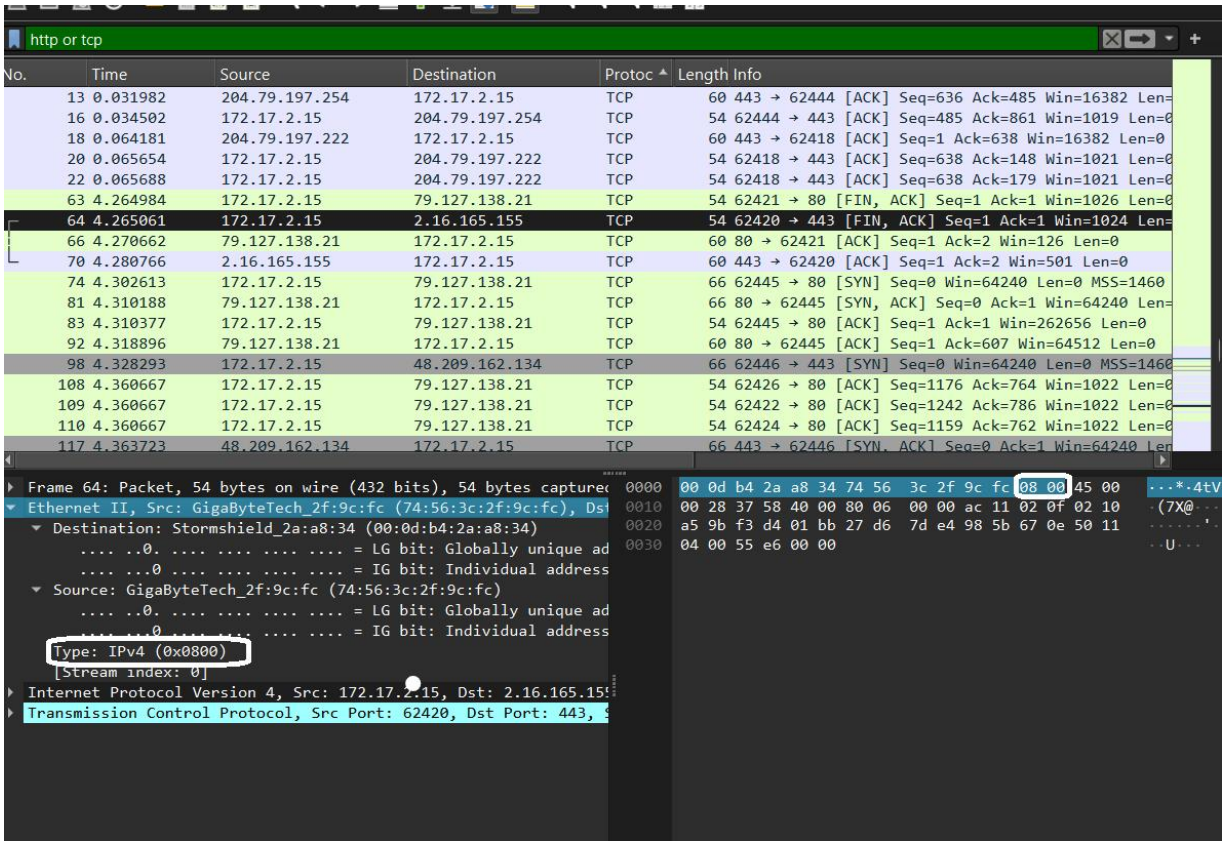
La valeur presente est 0x06 soit 6 en decimal et elle signifie que c'est une TCP

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

La valeur du port source est 172.17.2.15 en décimal et (ac 11 02 0f) en hexadécimale
La valeur du port destination est 2.16.165.155 en décimal et (02 10 a5 9b) en hexadécimale

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

TP3-Les ports logiciels



La valeur contenue dans le champ EtherType est 0x08 00 elle signifie que c'est une connexion en IPv4

Quelles sont les valeurs des adresses MAC destination et source ?

La valeur de l'adresse MAC destination est (00:0d:b4:2a:a8:34)
La valeur de l'adresse MAC source est (74:56:3c:2f:9c:fc)

Repérez les trames associées à la mise en place de la connexion TCP entre le client et le serveur (cf. Chapitre 4 - pages 2, 3 et 8 : Three-way handshake).
Pour chacune d'entre-elles, identifiez le champ Flags dans l'en-tête de segment :

Que signifie le contenu de ce champ pour chacun des 3 segments TCP ? Quelle est la raison de la mise en place de ce mode connecté ?

Le contenue de ce champ fait référence au «Three-way handshake»

Premièrement le SYN = client émet un segment (synchronization)
Deuxiement le SYN ACK = le serveur reçoit le segment SYN et envoie un ACK (acknowledge) en retour
Et pour finir le client renvoie un ACK pour valider

TP3-Les ports logiciels