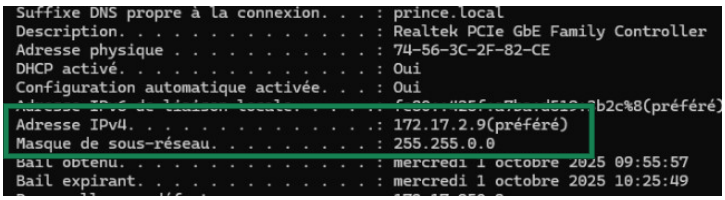
sommaire

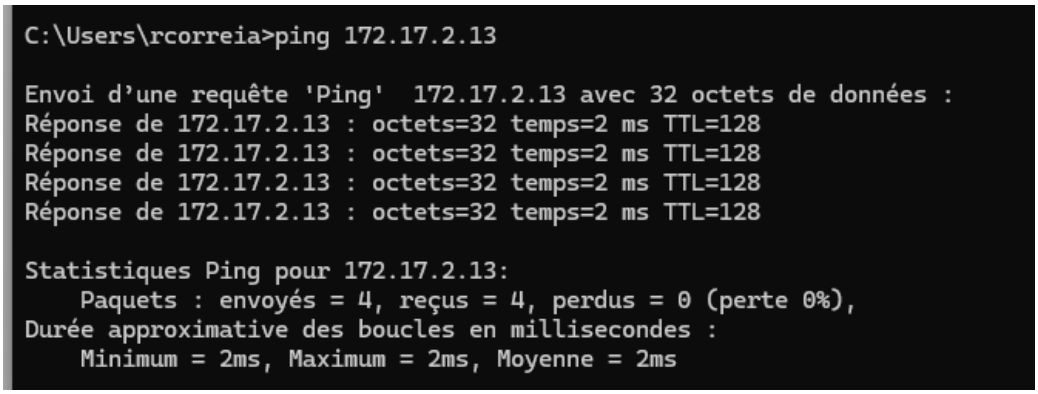
PARTI 1 -Connexion Bureau à distance (RDP)

Mon adresse :172.17.2.9

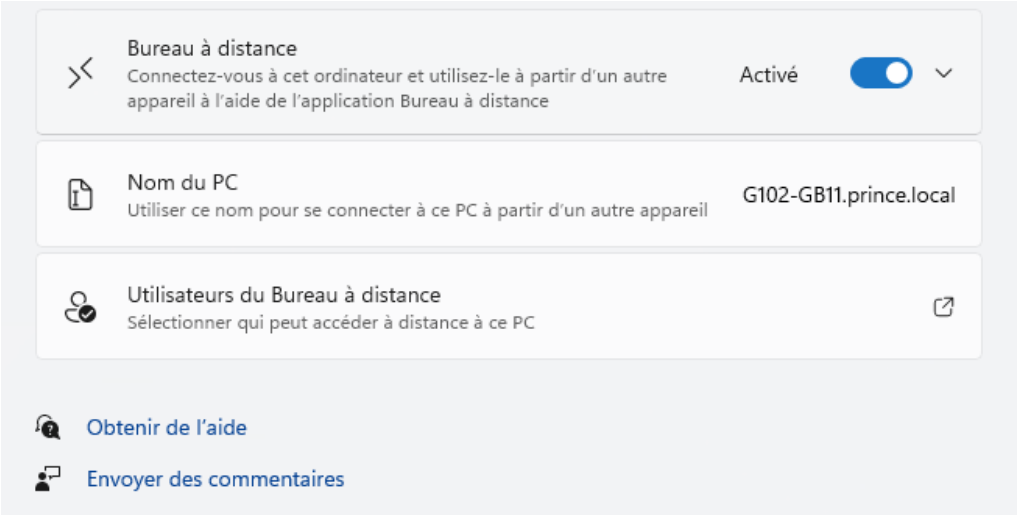


adresse voisin : 172.17.2.13

▪ ping de la station du voisin



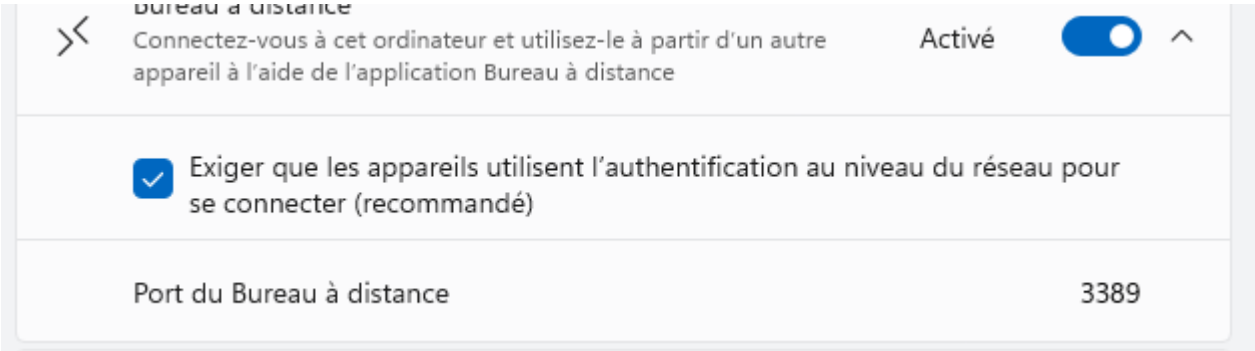
Activation du Bureau à distance



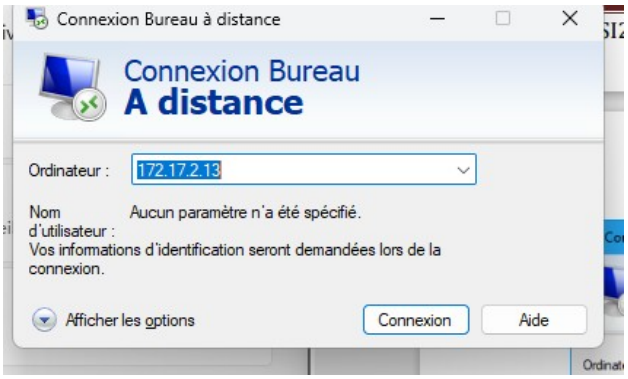
▪ Saisissez la commande netstat –an depuis l'invite de commandes de votre station Windows

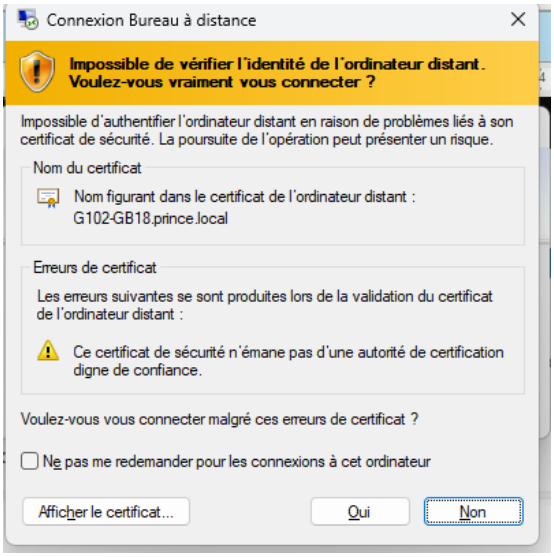
```
C:\Users\rcorreia>netstat -an

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    0.0.0.0:902            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    0.0.0.0:3389           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    0.0.0.0:49671          0.0.0.0:0              LISTENING
  TCP    127.0.0.1:27017        0.0.0.0:0              LISTENING
  TCP    172.17.2.9:139         0.0.0.0:0              LISTENING
  TCP    172.17.2.9:50430       172.17.254.5:445       ESTABLISHED
  TCP    172.17.2.9:58078       172.17.254.5:445       ESTABLISHED
  TCP    172.17.2.9:58321       95.100.133.19:443      TIME_WAIT
  TCP    172.17.2.9:58324       95.100.133.19:443      TIME_WAIT
  TCP    172.17.2.9:58327       95.100.133.19:443      TIME_WAIT
```

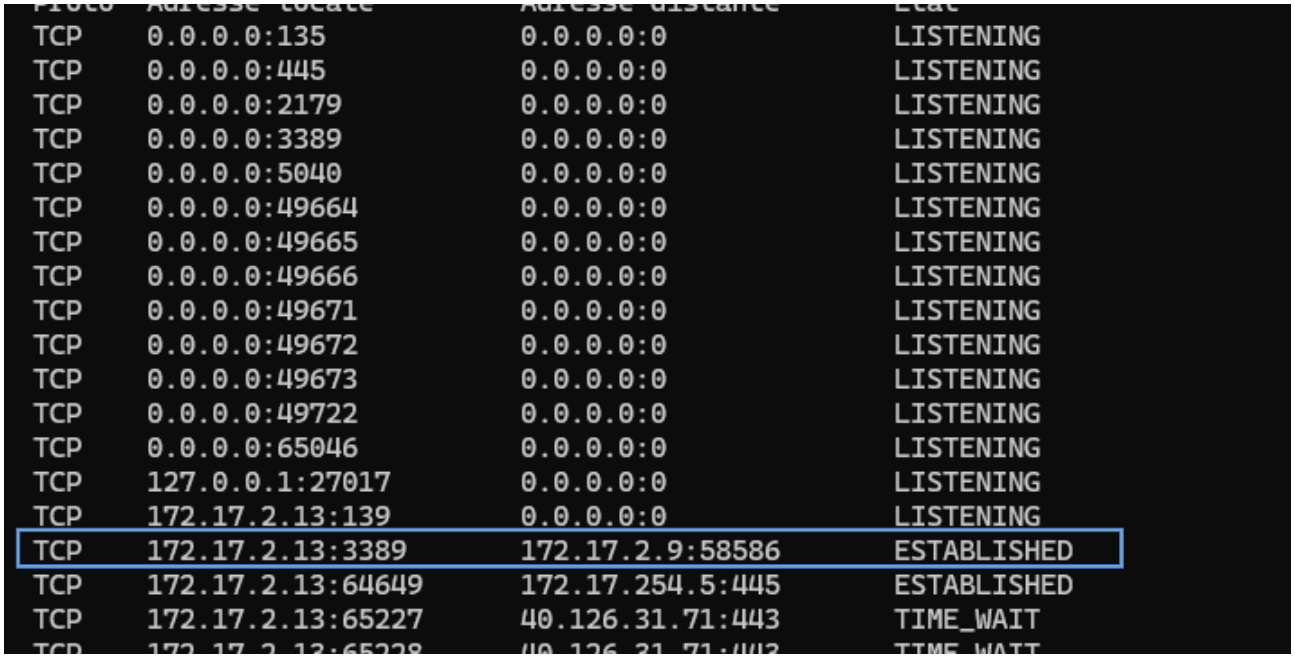
Quel est le port d'écoute du serveur Terminal Server ? Le TCP 0.0.0.0.3389



connection au bureau a distance





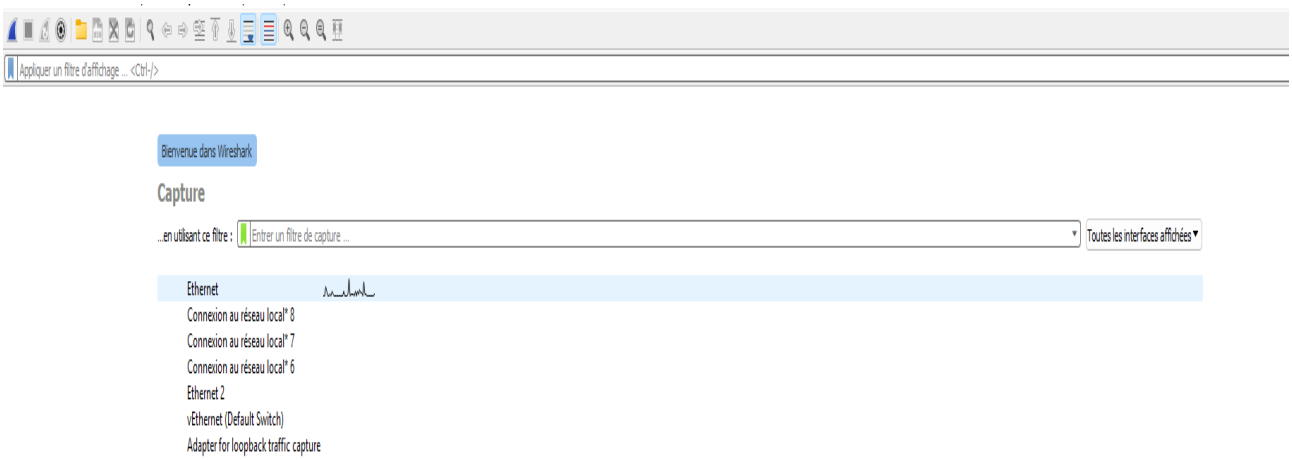


TCP	0.0.0.0:135	0.0.0.0:0	LISTENING
TCP	0.0.0.0:445	0.0.0.0:0	LISTENING
TCP	0.0.0.0:2179	0.0.0.0:0	LISTENING
TCP	0.0.0.0:3389	0.0.0.0:0	LISTENING
TCP	0.0.0.0:5040	0.0.0.0:0	LISTENING
TCP	0.0.0.0:49664	0.0.0.0:0	LISTENING
TCP	0.0.0.0:49665	0.0.0.0:0	LISTENING
TCP	0.0.0.0:49666	0.0.0.0:0	LISTENING
TCP	0.0.0.0:49671	0.0.0.0:0	LISTENING
TCP	0.0.0.0:49672	0.0.0.0:0	LISTENING
TCP	0.0.0.0:49673	0.0.0.0:0	LISTENING
TCP	0.0.0.0:49722	0.0.0.0:0	LISTENING
TCP	0.0.0.0:65046	0.0.0.0:0	LISTENING
TCP	127.0.0.1:27017	0.0.0.0:0	LISTENING
TCP	172.17.2.13:139	0.0.0.0:0	LISTENING
TCP	172.17.2.13:3389	172.17.2.9:58586	ESTABLISHED
TCP	172.17.2.13:64649	172.17.254.5:445	ESTABLISHED
TCP	172.17.2.13:65227	40.126.31.71:443	TIME_WAIT

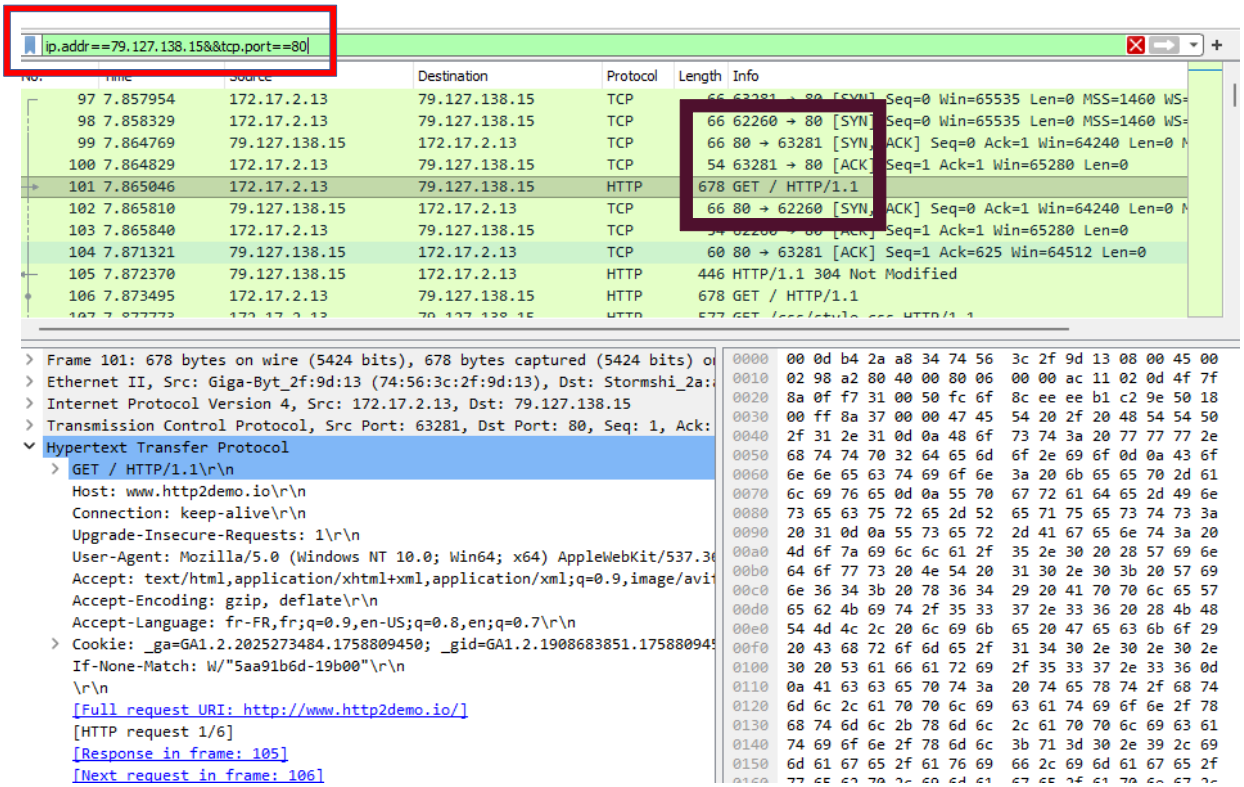
la session a etait arreter

2. Capture de trames HTTP

Wireshark lancé en mode admin

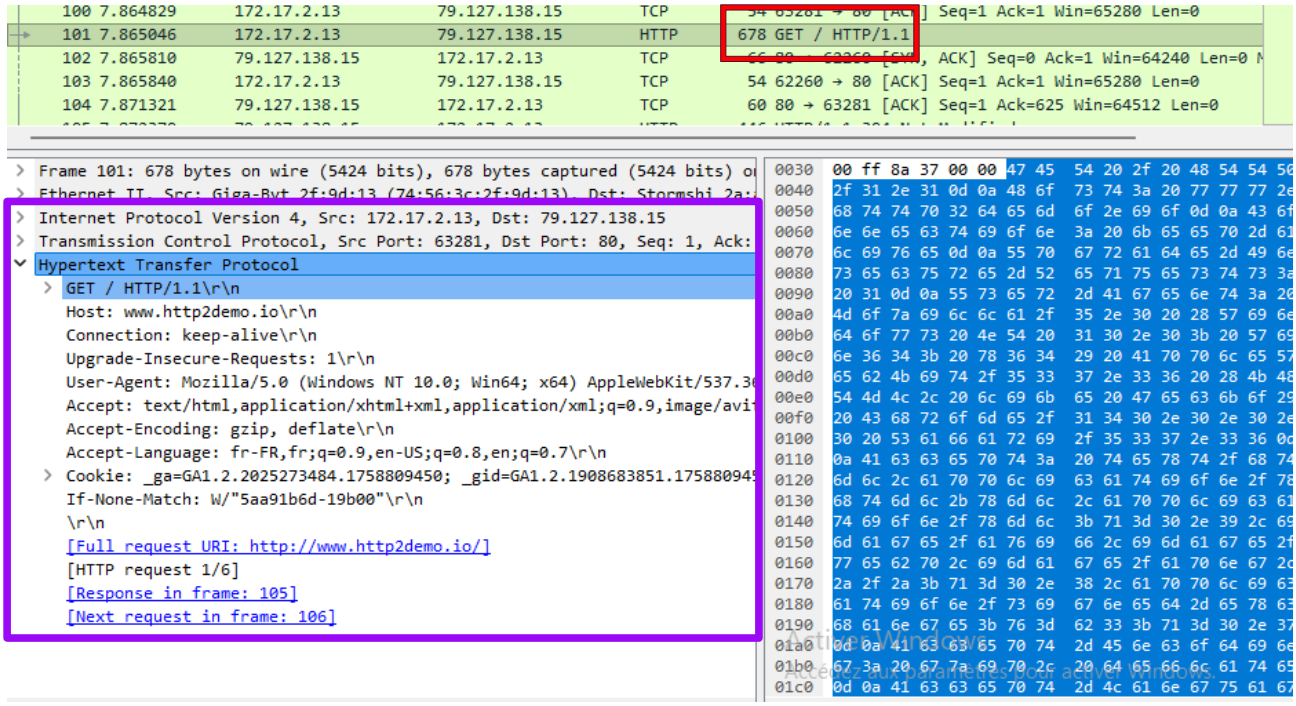


ont est aller sur l'adresse [HTTP/2 technology demo]

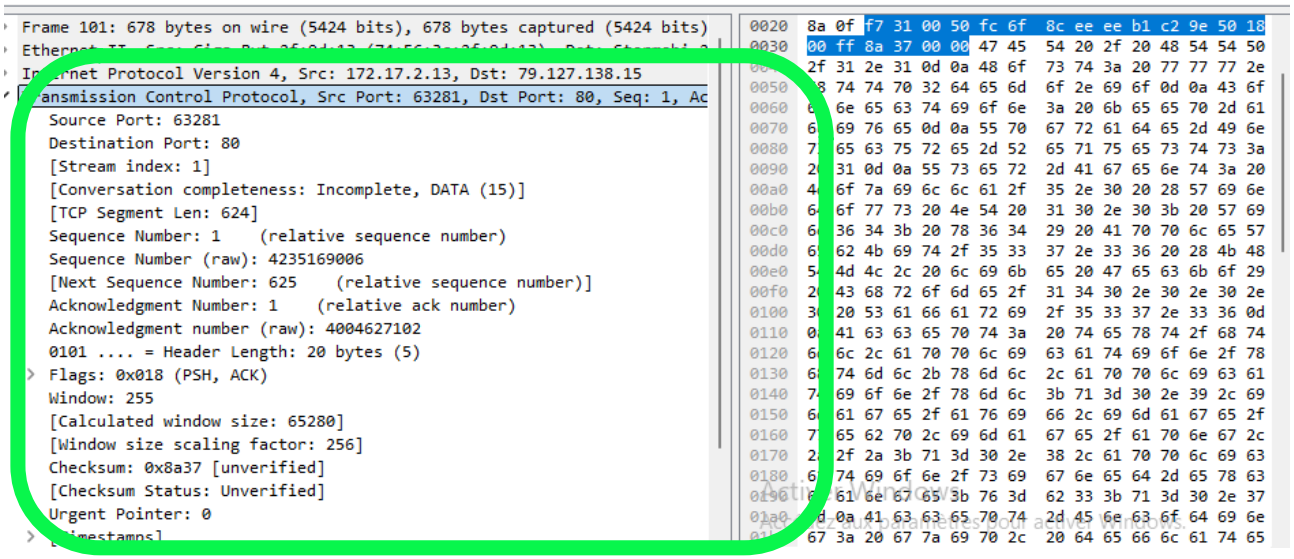


```
C:\Users\rcorreia>nslookup www.http2demo.io
Serveur :   roi.prince.local
Address:  172.17.254.1

Réponse ne faisant pas autorité :
Nom :    1906714720.rsc.cdn77.org
Addresses:  2a02:6ea0:dc00::32
          2a02:6ea0:dc00::31
          2a02:6ea0:dc00::30
          79.127.138.14
          79.127.138.20
          79.127.138.18
Aliases:  www.http2demo.io
```

trame http reperé

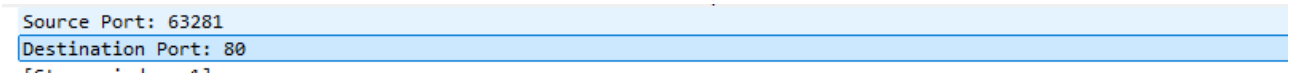


en-tête transport developpé

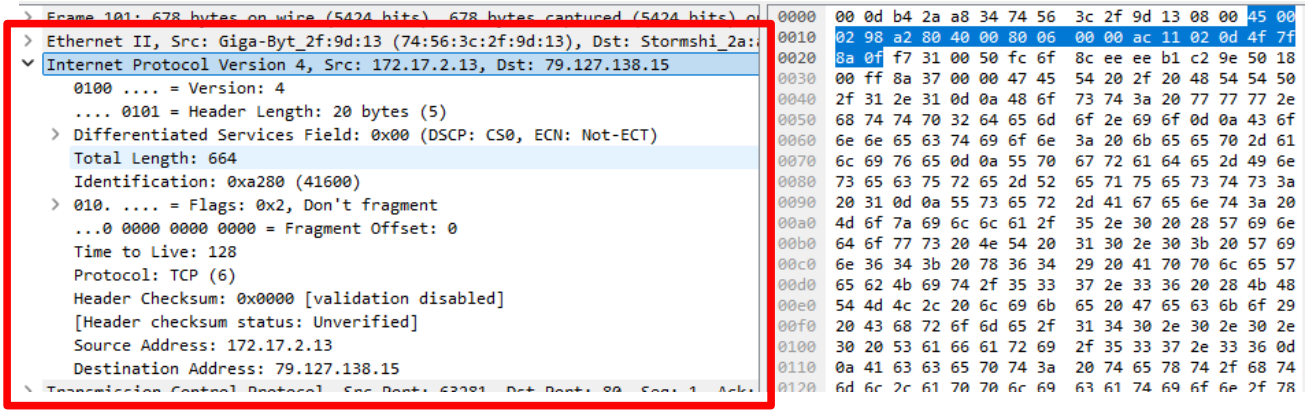


Quel est le nom du protocole transport utilisé par une trame HTTP ?
Le nom du protocole ce'st transmission Control Protocol ou TCP

Quel est le nom du PDU encapsulant les données applicatives HTTP ?
Le pdu de TCP c'est le segment
Quelle est la longueur de l'en-tête de transport ?
Elle est de 20 bytes
Quelles sont les valeurs décimale et hexadécimale correspondant aux ports source et destination ?
Port source : 80 / 00 50
port destination: 63281 / f7 31



Developez l'en-tete reseau



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

20 bytes

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

6

Que signifie-t-elle ?

Elle signifie que ont a un TCP , ont peut aussi avoir 1 1 qui veut dire UDP

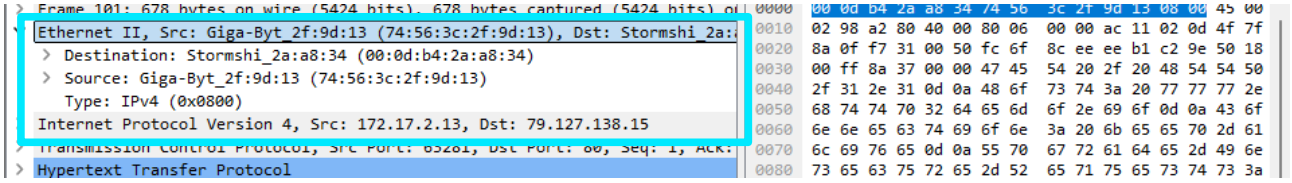
Quelles sont les valeurs décimales et hexadécimales des adresses IP source et destination ?

IP source : 172,17,2,13 / hexa : ac 11 02 0d

IP destination : 79,127,138,15 / hexa : 4f 7f 8a 0f

```
Source Address: 172.17.2.13
Destination Address: 79.127.138.15
```

en-tete Ethernet developé



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

0X800 ,elle signifie que cest un IPv4, si ont avais 0x806 ont aurais eu une trame ARP

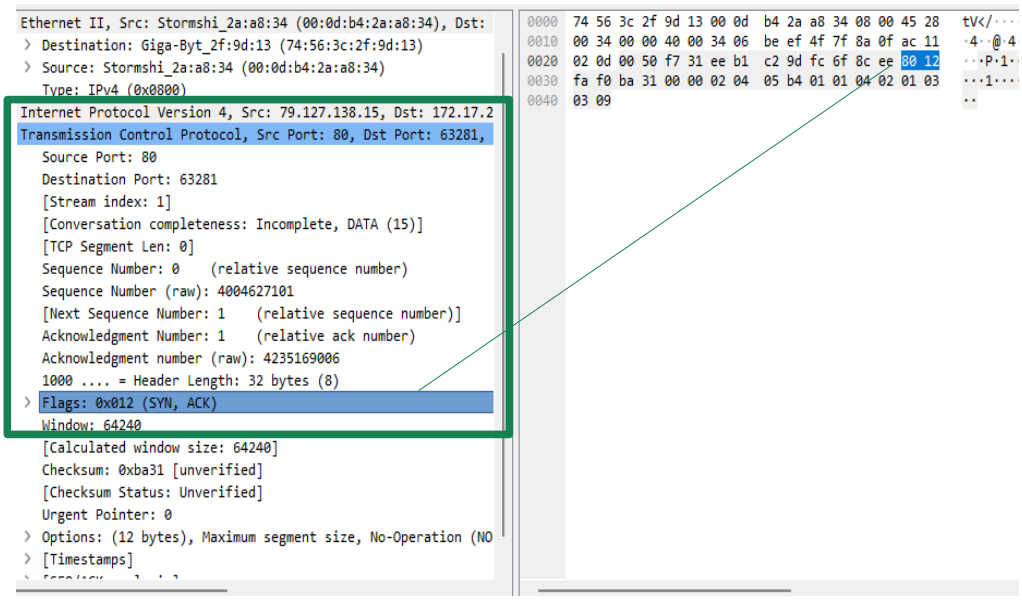
Quelles sont les valeurs des adresses MAC destination et source ?

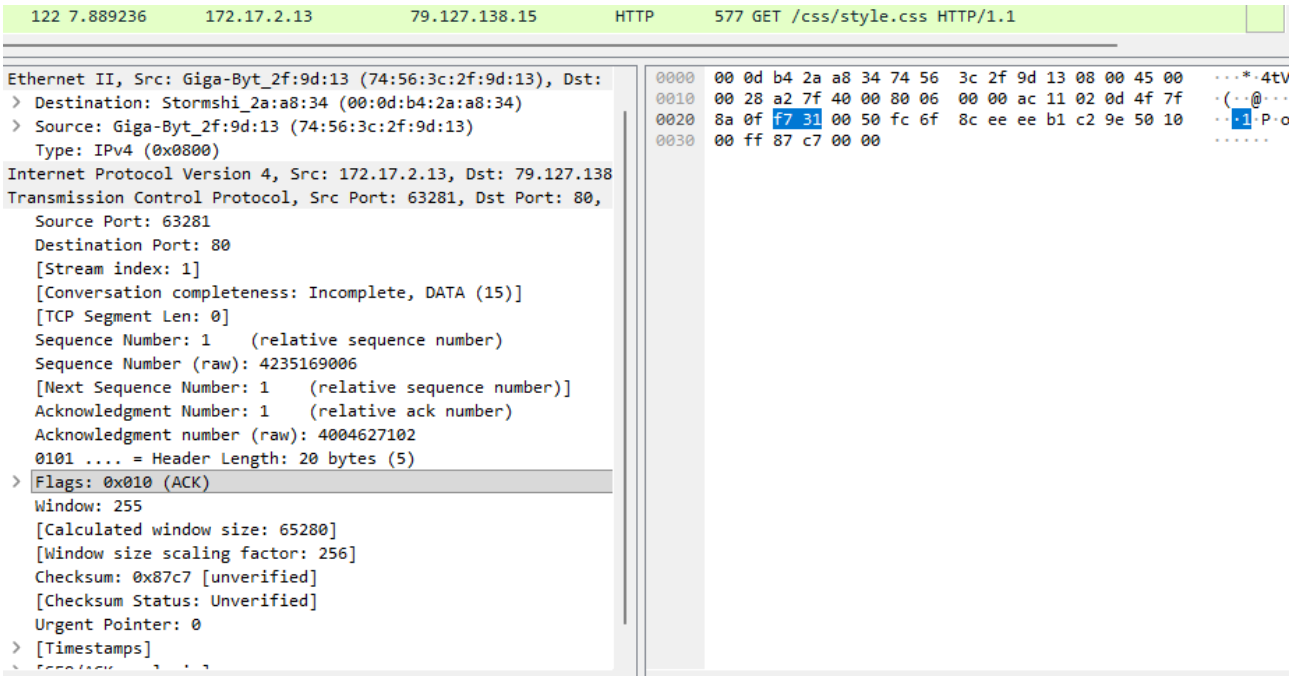
Mac source : 74:56:3c:2f:9d:13

mac Destination : 00:0d:b4:2a:a8:34

```
> Destination: Stormshi_2a:a8:34 (00:0d:b4:2a:a8:34)
> Source: Giga-Byt_2f:9d:13 (74:56:3c:2f:9d:13)
```

ont repere les trame de connexion tcp





que signifie le contenu de ce champ pour chacun des 3 segment tcp ?
c'est la poingé a 3 vois

sa etabli un un transport plus fiable en assurant les garanties RIS
Le serveur reçoit le segment SYN et répond par un segment SYN/ACK. Il faut comprendre ce message comme étant la superposition de deux messages : « j'accepte d'ouvrir une liaison de toi vers moi » (ACK) et « je souhaite moi aussi établir une liaison vers toi » (SYN). Le client reçoit le segment SYN/ACK et répond par un segment ACK

sa etabli un un transport plus fiable en assurant les garanties RIS.