Suiveng
Mateo

TP 3 – Les Ports Logiciels

Table des matières

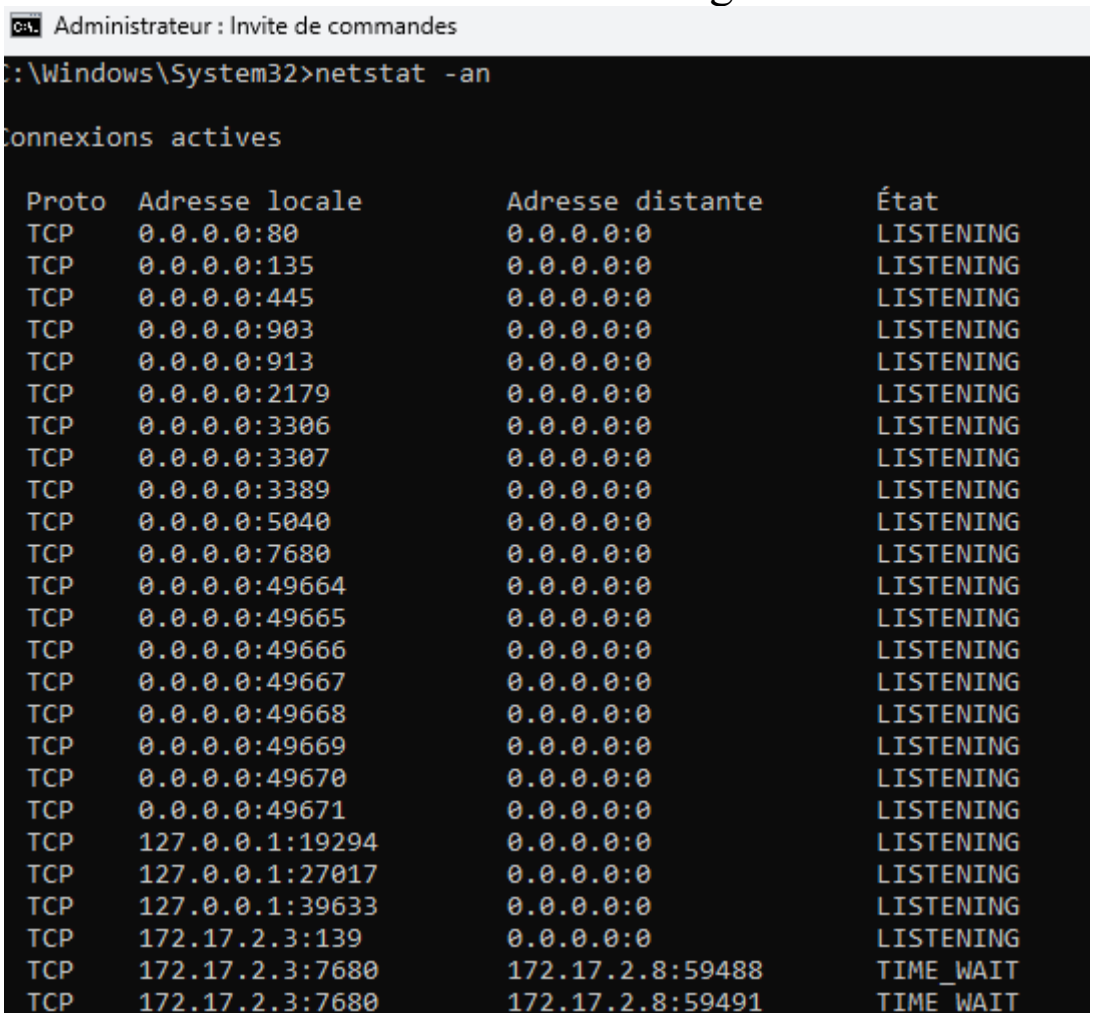
1. Connexion Bureau à distance (RDP)

Administrateur : Invite de commandes

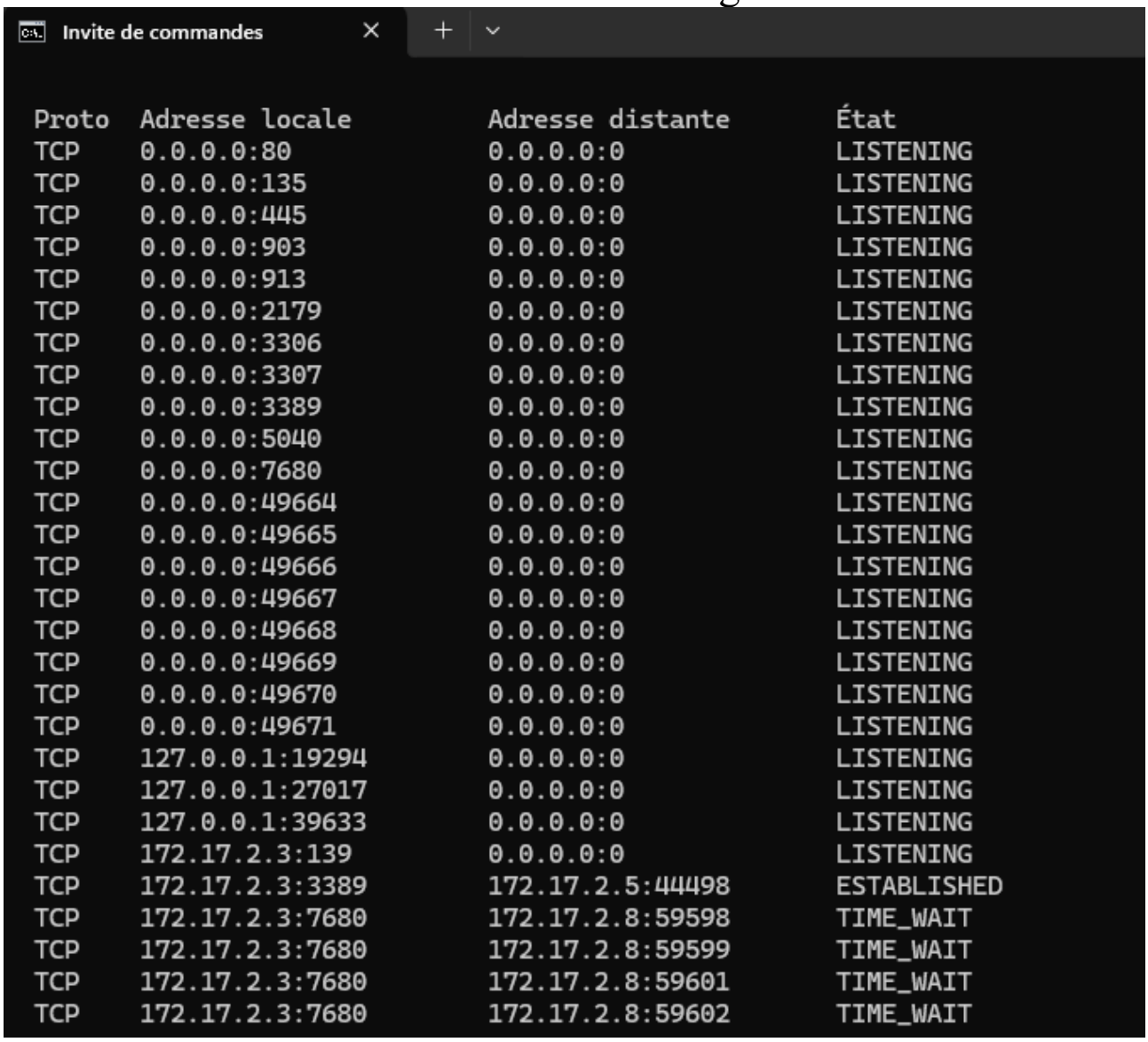
```
  TCP    172.17.2.3:62622       146.75.118.172:80      TIME_WAIT
  TCP    172.17.2.3:62623       146.75.118.172:80      TIME_WAIT
  TCP    172.17.2.3:62627       146.75.118.172:80      TIME_WAIT
  TCP    172.17.2.3:62628       146.75.118.172:80      TIME_WAIT
  TCP    172.17.2.3:62629       146.75.118.172:80      TIME_WAIT
  TCP    172.17.2.3:62634       146.75.118.172:80      TIME_WAIT
  TCP    172.17.2.3:62635       146.75.118.172:80      ESTABLISHED
  TCP    172.17.2.3:62636       79.127.138.20:80       ESTABLISHED
  TCP    172.17.2.3:62637       79.127.138.20:80       ESTABLISHED
  TCP    172.17.2.3:62638       79.127.138.20:80       ESTABLISHED
  TCP    172.17.2.3:62639       79.127.138.20:80       ESTABLISHED
  TCP    172.17.2.3:62640       79.127.138.20:80       ESTABLISHED
  TCP    172.17.2.3:62641       79.127.138.20:80       ESTABLISHED
  TCP    172.17.2.3:62642       157.240.196.35:443     ESTABLISHED
  TCP    172.17.2.3:62643       157.240.196.15:443     ESTABLISHED
  TCP    172.17.2.3:62644       216.239.36.178:443     ESTABLISHED
  TCP    172.17.2.3:62645       79.127.138.15:80       ESTABLISHED
  TCP    172.17.2.3:62646       142.250.203.226:443    ESTABLISHED
  TCP    172.17.2.3:62647       216.58.205.200:443     ESTABLISHED
  TCP    172.17.2.3:62648       79.127.138.15:80       ESTABLISHED
  TCP    172.17.2.3:62649       79.127.138.15:80       ESTABLISHED
  TCP    172.17.2.3:62650       79.127.138.15:80       ESTABLISHED
  TCP    172.17.2.3:62651       79.127.138.15:80       ESTABLISHED
  TCP    172.17.2.3:62652       79.127.138.15:80       ESTABLISHED
  TCP    172.17.2.3:62653       216.239.32.36:443      ESTABLISHED
```

```
C:\Windows\System32>ping 172.17.2.5

Envoi d'une requête 'Ping'  172.17.2.5 avec 32 octets de données :
Réponse de 172.17.2.5 : octets=32 temps=3 ms TTL=128
Réponse de 172.17.2.5 : octets=32 temps=2 ms TTL=128
Réponse de 172.17.2.5 : octets=32 temps=2 ms TTL=128
Réponse de 172.17.2.5 : octets=32 temps=2 ms TTL=128

Statistiques Ping pour 172.17.2.5:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 2ms, Maximum = 3ms, Moyenne = 2ms

C:\Windows\System32>
```

Suiveng
Mateo TP 3 – Les Ports Logiciels



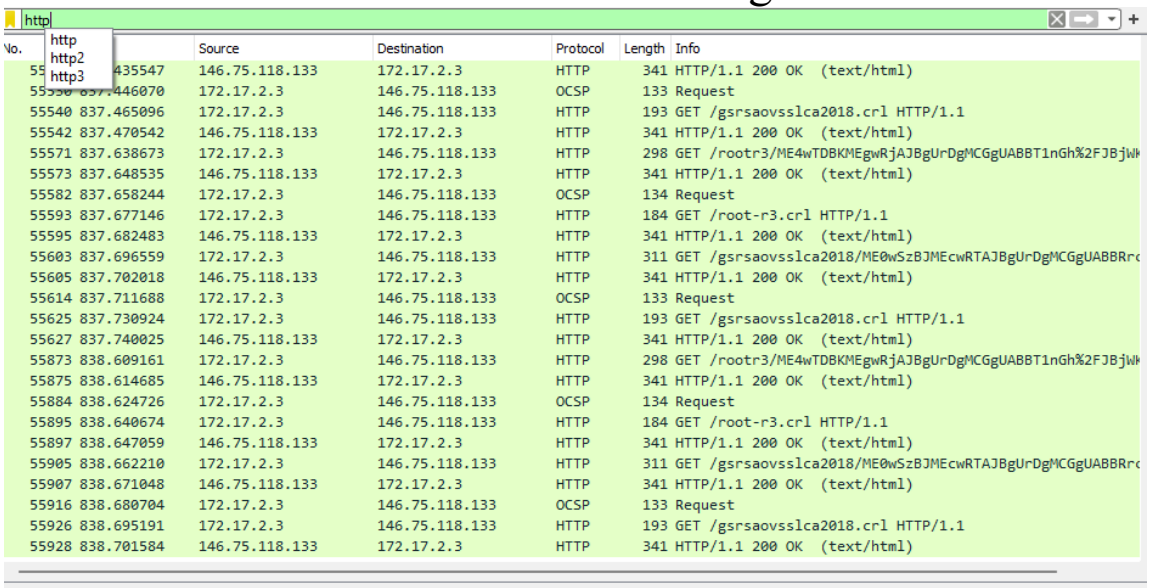
Quel est le port d’écoute du serveur Terminal Server ?
Le port d’écoute du serveur Terminal Server est 3389

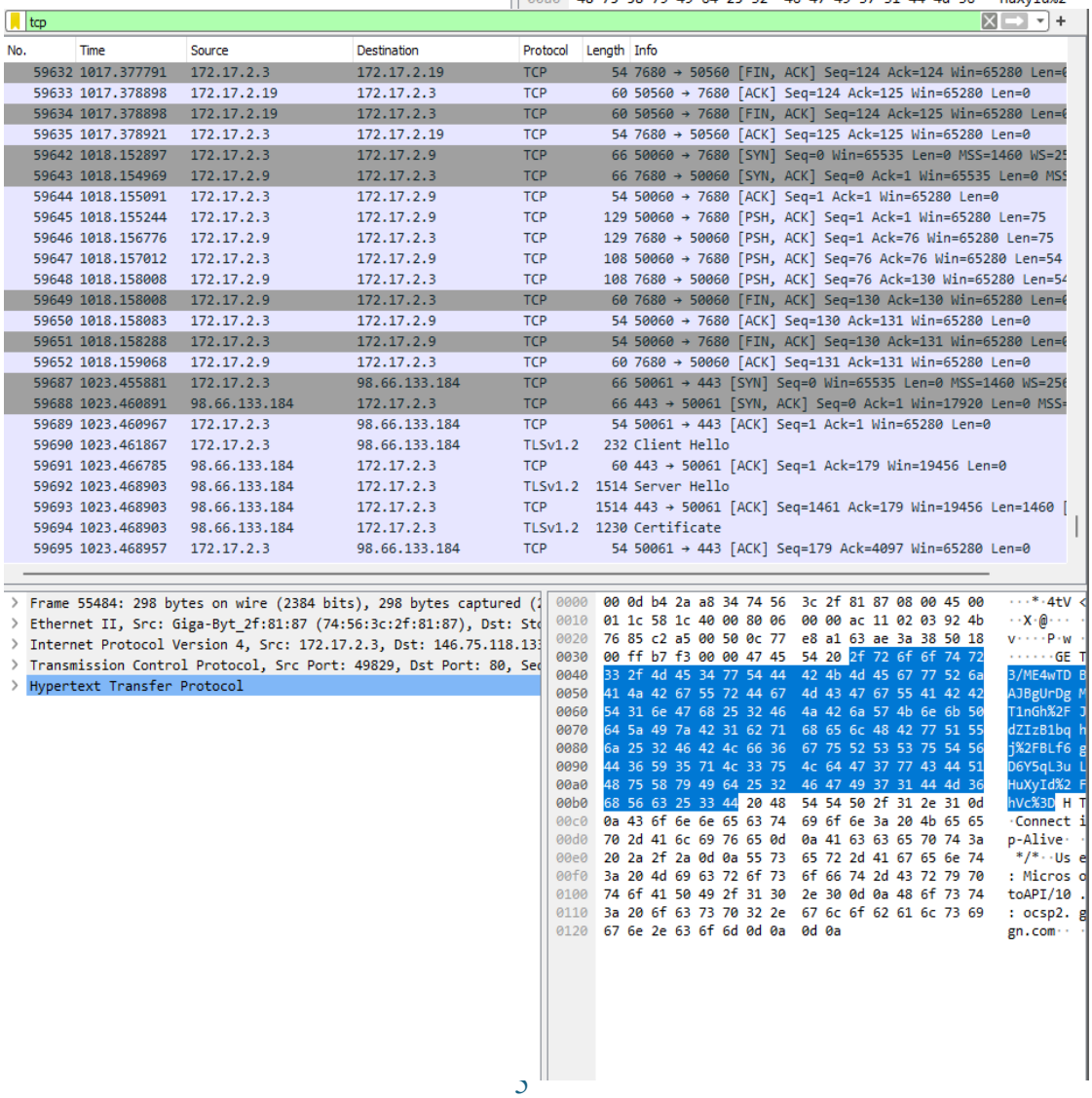


2. Capture de trames HTTP.

Suiveng
Mateo

TP 3 – Les Ports Logiciels

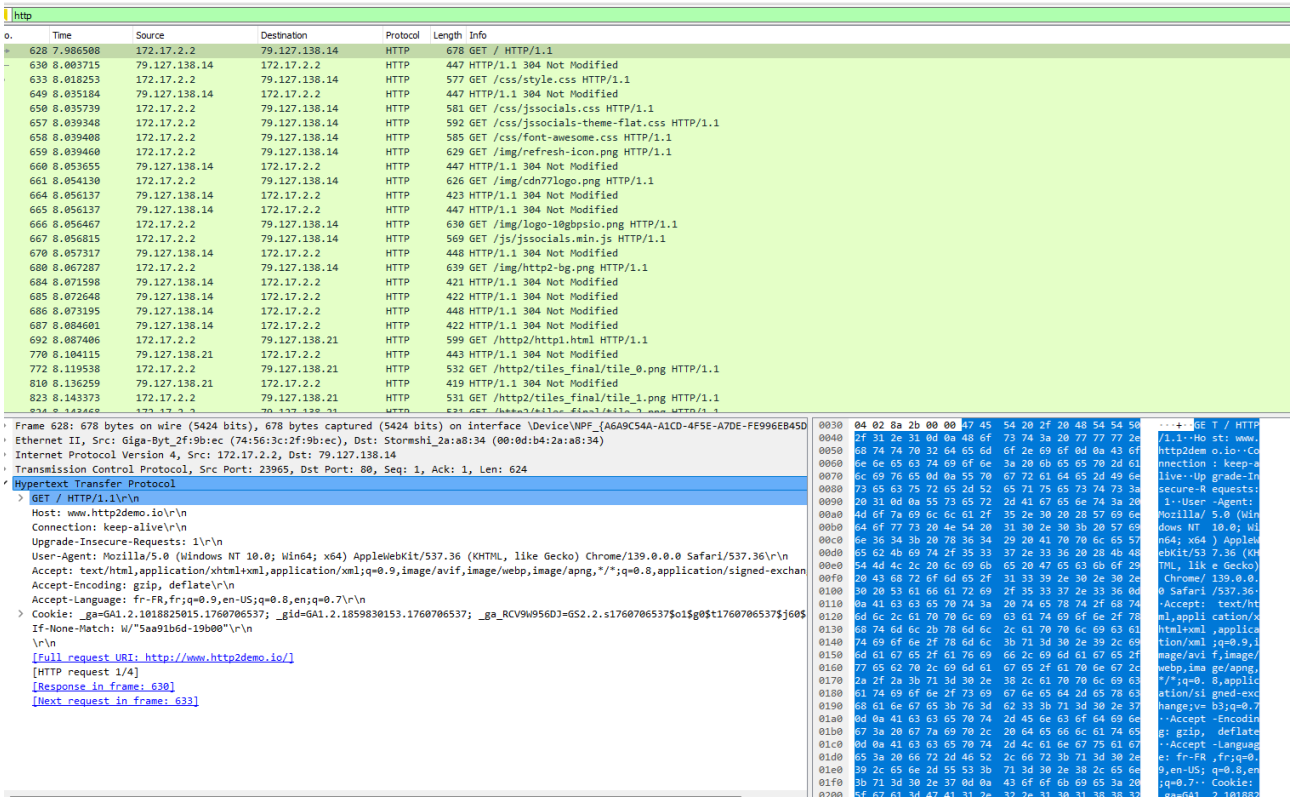




Suiveng
Mateo

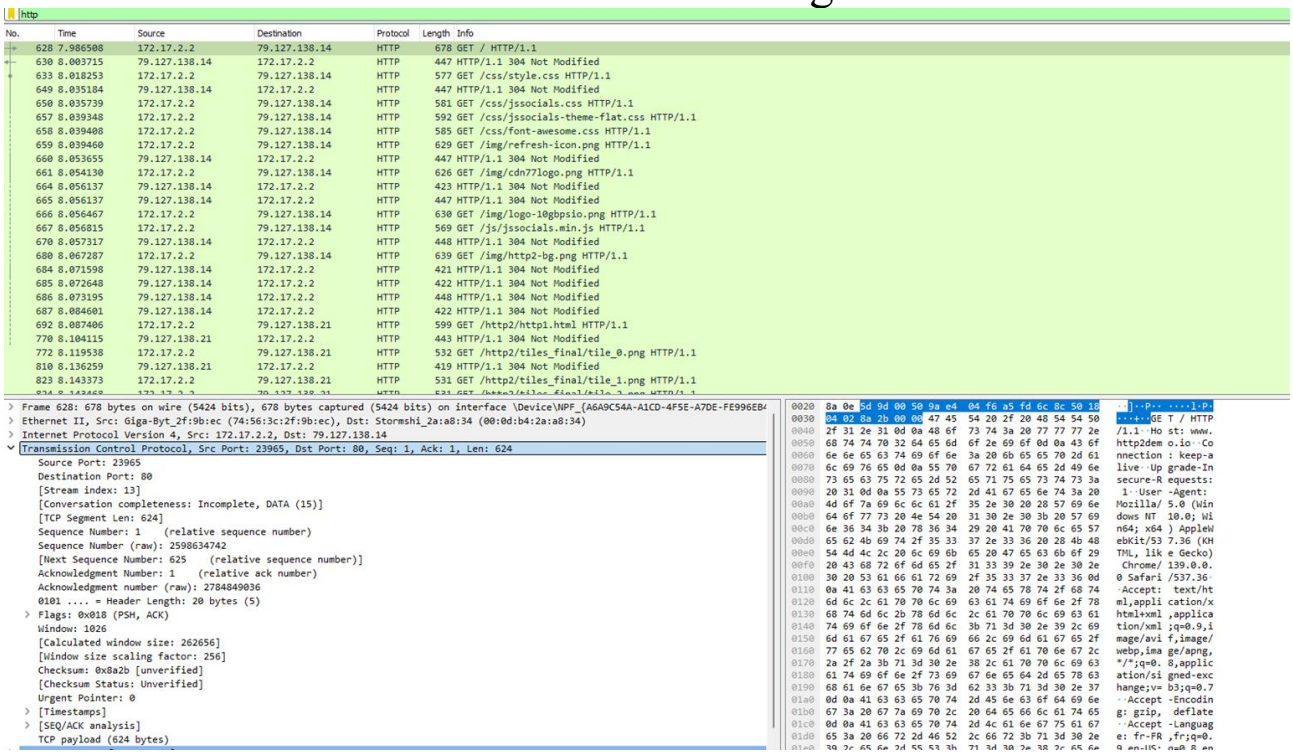
TP 3 – Les Ports Logiciels

```
C:\Users\msuiveng>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::30
          2a02:6ea0:dc00::32
          2a02:6ea0:dc00::31
          79.127.138.20
          79.127.138.17
          79.127.138.14
Aliases:  www.http2demo.io
```



Suiveng
Mateo

TP 3 – Les Ports Logiciels



Quel est le nom du protocole transport utilisé par une trame HTTP ?
Le protocole de transport utilisé est le Transmission Control Protocol (TCP).

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

L'unité de données de protocole (PDU) de la couche Transport qui encapsule les données applicatives (HTTP) est un Segment TCP (ou simplement Segment).

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

La longueur de l'en-tête de transport (TCP) est donc de 20 octets car "Header length: 20 bytes (5)"

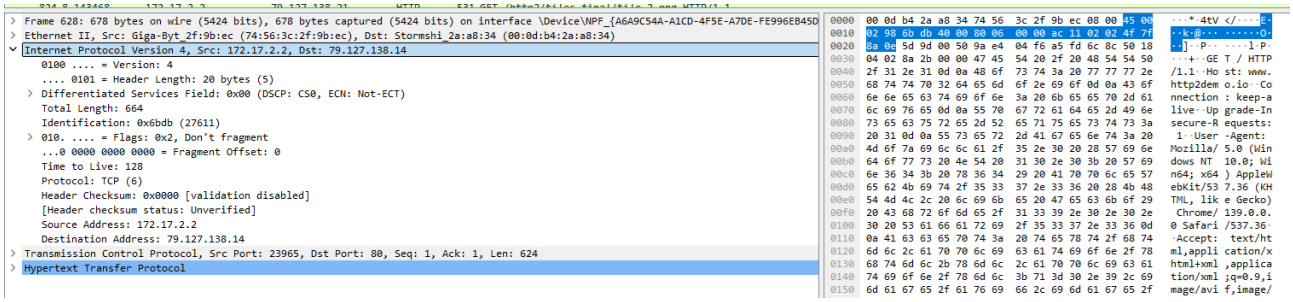
Suiveng
Mateo

TP 3 – Les Ports Logiciels

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

- La valeur décimale du port source est 23965 et sa valeur hexadécimale est 5d 9d
- La valeur décimale du port destination est 80 et sa valeur en hexadécimale est 00 50

Développez la section correspondant à l'en-tête Réseau :



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

La longueur de l'en-tête de réseau : 20 octets (20 bytes).

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

La valeur présente est TCP (6).

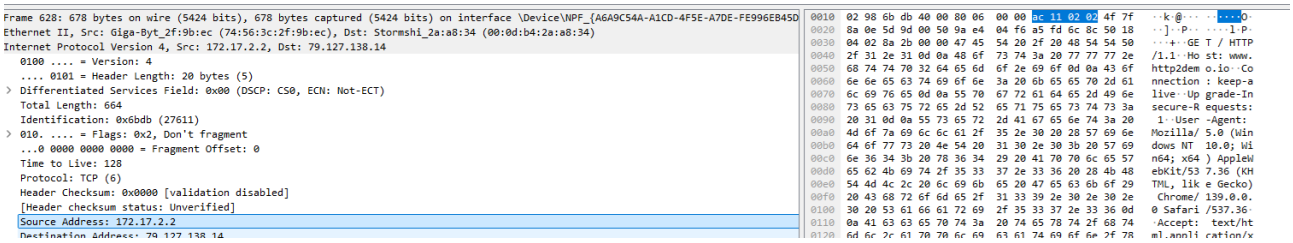
- Cela signifie que la charge utile de ce paquet IP est un segment TCP. Dans ce cas, ce segment TCP transporte lui-même les données de l'application (HTTP).

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

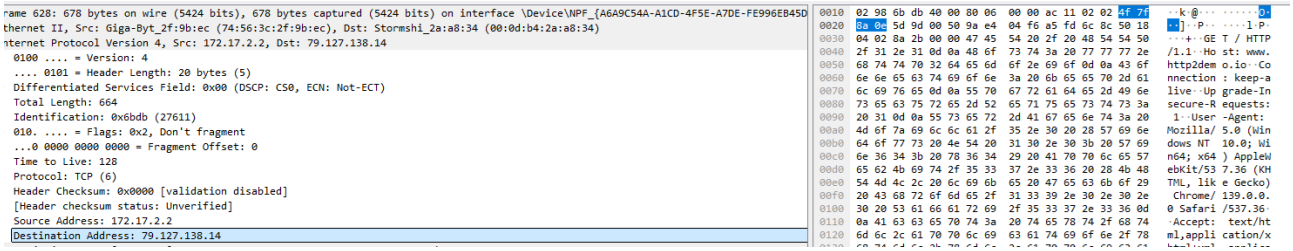
Suiveng
Mateo

TP 3 – Les Ports Logiciels

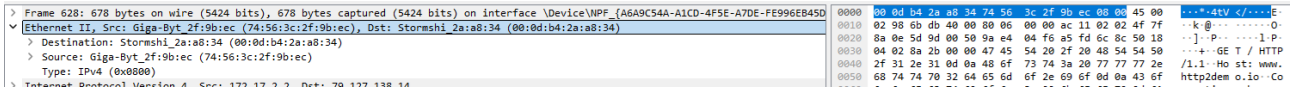
- La valeur décimale de l'IP source est 172.17.2.2 et sa valeur en hexadécimale est ac 11 02 02



- La valeur décimale de l'IP destination est 79.127.138.14 et sa valeur en hexadécimale est 4f 7f 8a 0e



- Développez la section correspondant à l'en-tête Ethernet :



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

-Valeur contenue : IPv4 (0x0800).

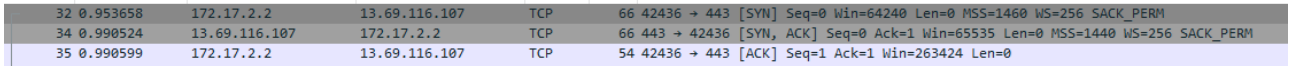
- Signification : La valeur hexadécimale 0x0800 est l'identifiant pour le protocole Internet Protocol version 4 (IPv4). Cela signifie que la charge utile de cette trame Ethernet est un paquet IPv4.

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

- Adresse MAC Destination : 00:0b:0d:4a:2a:a4

- Adresse MAC Source : 74:56:3c:2f:9b:ec

- Repérez les trames associées à la mise en place de la connexion TCP entre le client et le serveur

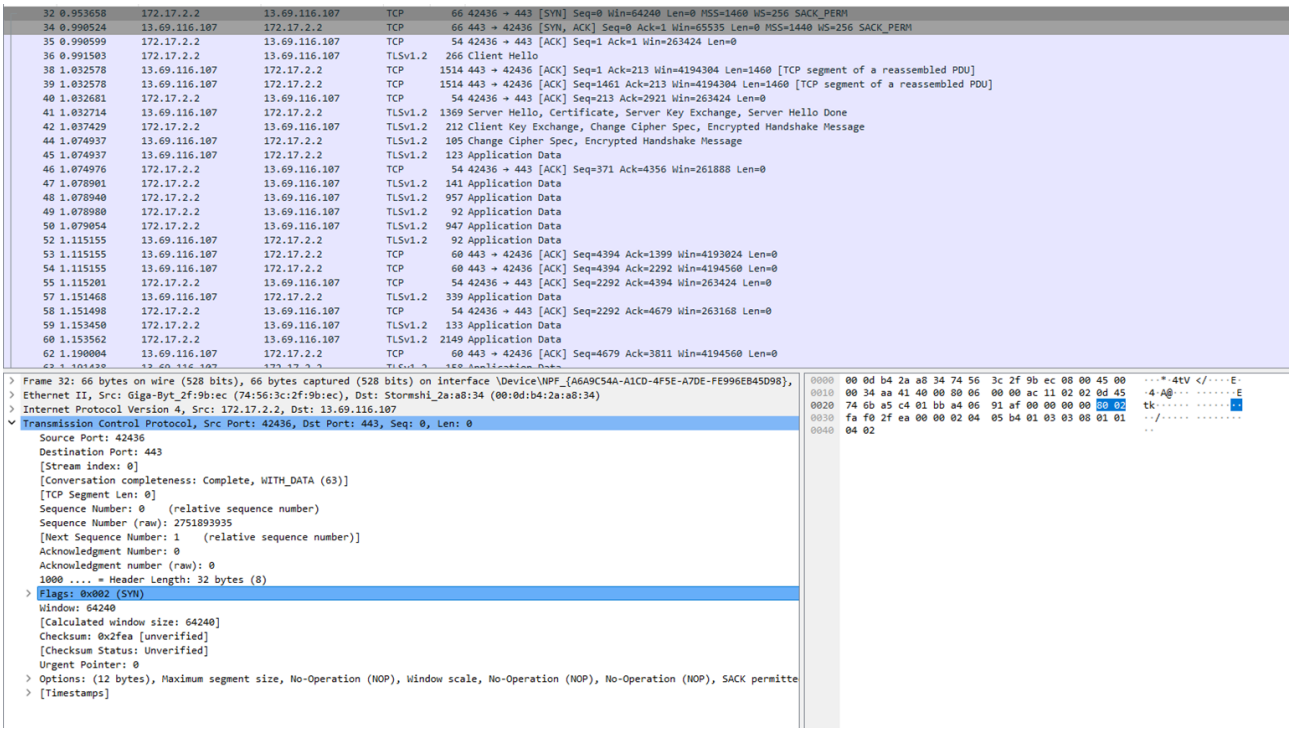


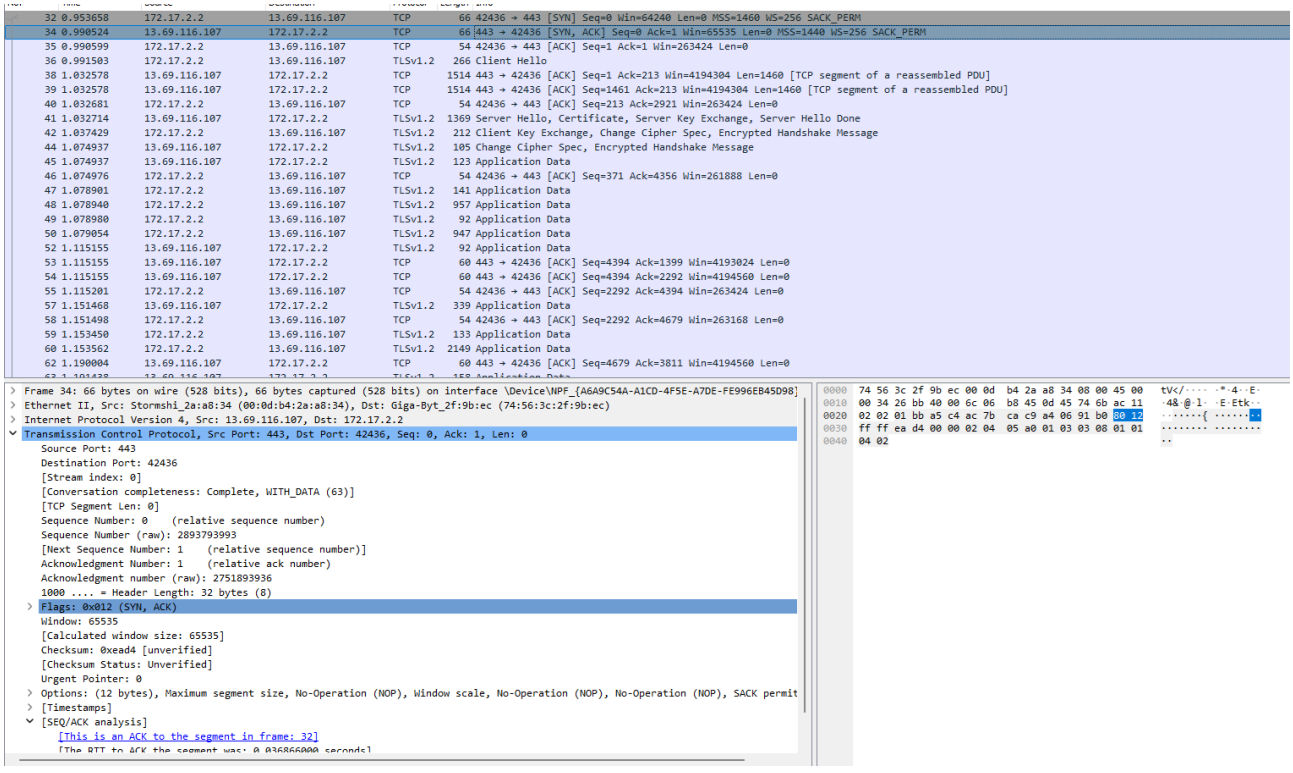
32	0.953658	172.17.2.2	13.69.116.107	TCP	66 42436 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
34	0.990524	13.69.116.107	172.17.2.2	TCP	66 443 → 42436 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1440 WS=256 SACK_PERM
35	0.990599	172.17.2.2	13.69.116.107	TCP	54 42436 → 443 [ACK] Seq=1 Ack=1 Win=263424 Len=0

Les trames associées à la mise en place de la connexion TCP entre le client et le serveur sont donc SYN, SYN/ACK, ACK

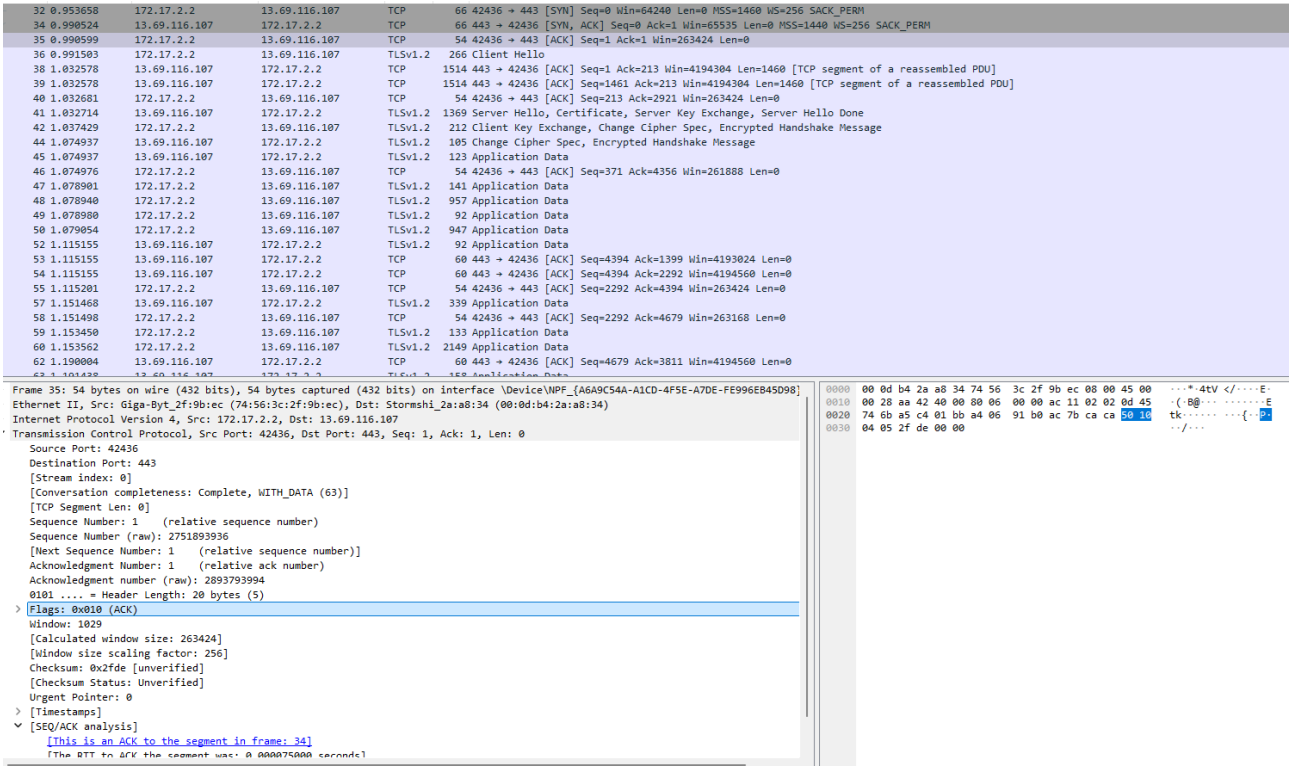
Suiveng
Mateo

TP 3 – Les Ports Logiciels





TP 3 – Les Ports Logiciels



<u>- 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 ?</u>

- Segment SYN : Le client envoie une requête de synchronisation pour initier la connexion

- Segment SYN/ACK : le serveur accuser de réception du SYN du client(ACK) et envoie à son tour un SYN

-Segment ACK : Le client SYN du serveur, confirme donc la connexion

La raison de la mise en place de ce mode connecté :

Le protocole TCP utilise ce moyen de communication pour que les deux parties puissent échanger des données sans risque de perte.