TP 3 : Les ports logiciel : Hidaoui Mohamed-Amine BTS SIO 1

Sommaire :

Utilisation des commandes :

utilisation de netstat -a sur le terminal de commande (pour la suite du TP certaine commande ont ete faite chez moi avec les moyen du bord et la perte de certain screenshot fait en classe (désolé))

```
kametocorp1234@penguin:~$ netstat -a
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
udp        0      0 0.0.0.0:bootpc          0.0.0.0:*
Active UNIX domain sockets (servers and established)
Proto RefCnt Flags       Type       State         I-Node   Path
unix  3      [ ]         STREAM     CONNECTED     2595
unix  2      [ ACC ]     STREAM     LISTENING     2691     /tmp/.X11-unix/X0
unix  3      [ ]         STREAM     CONNECTED     2521
unix  2      [ ACC ]     STREAM     LISTENING     2693     /tmp/.X11-unix/X1
unix  3      [ ]         STREAM     CONNECTED     3902
unix  2      [ ]         DGRAM      CONNECTED     131393
unix  3      [ ]         STREAM     CONNECTED     2789
unix  2      [ ]         DGRAM                    3308     /run/user/1000/systemd/notify
unix  2      [ ACC ]     STREAM     LISTENING     3311     /run/user/1000/systemd/private
unix  3      [ ]         STREAM     CONNECTED     2498
unix  2      [ ACC ]     STREAM     LISTENING     3361     /run/user/1000/bus
unix  3      [ ]         STREAM     CONNECTED     2594
unix  3      [ ]         STREAM     CONNECTED     3783     /run/dbus/system_bus_socket
unix  2      [ ACC ]     STREAM     LISTENING     3364     /run/user/1000/gnupg/S.dirmngr
unix  3      [ ]         DGRAM      CONNECTED     3309
unix  2      [ ACC ]     STREAM     LISTENING     3366     /run/user/1000/gnupg/S.gpg-agent.bro
wser
unix  2      [ ACC ]     STREAM     LISTENING     3368     /run/user/1000/gnupg/S.gpg-agent.ext
ra
unix  2      [ ACC ]     STREAM     LISTENING     3370     /run/user/1000/gnupg/S.gpg-agent.ssh
unix  2      [ ACC ]     STREAM     LISTENING     3372     /run/user/1000/gnupg/S.gpg-agent
unix  2      [ ACC ]     STREAM     LISTENING     3374     /run/user/1000/pulse/native
unix  2      [ ]         DGRAM                    2686
unix  2      [ ACC ]     STREAM     LISTENING     3376     /run/user/1000/pipewire-0
unix  2      [ ]         DGRAM      CONNECTED     131503
unix  2      [ ACC ]     STREAM     LISTENING     3378     /run/user/1000/pk-debconf-socket
```

netstat -n :

```
kametocorp1234@penguin:~$ netstat -n
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
Active UNIX domain sockets (w/o servers)
Proto RefCnt Flags       Type       State         I-Node   Path
unix  3      [ ]         STREAM     CONNECTED     2595
unix  3      [ ]         STREAM     CONNECTED     2521
unix  3      [ ]         STREAM     CONNECTED     3902
unix  2      [ ]         DGRAM      CONNECTED     131393
unix  3      [ ]         STREAM     CONNECTED     2789
unix  2      [ ]         DGRAM                    3308     /run/user/1000/systemd/notify
unix  3      [ ]         STREAM     CONNECTED     2498
unix  3      [ ]         STREAM     CONNECTED     2594
unix  3      [ ]         STREAM     CONNECTED     3783     /run/dbus/system_bus_socket
unix  3      [ ]         DGRAM      CONNECTED     3309
unix  2      [ ]         DGRAM                    2686
```

Partie 1 : Connexion de bureau à distance

utilisation de la commande ipconfig (“ip a” sous linux) :

connexion etablie en TP classe avec kevin
mon ip et de 127.0.0.1 et en classe 172.17.2.6

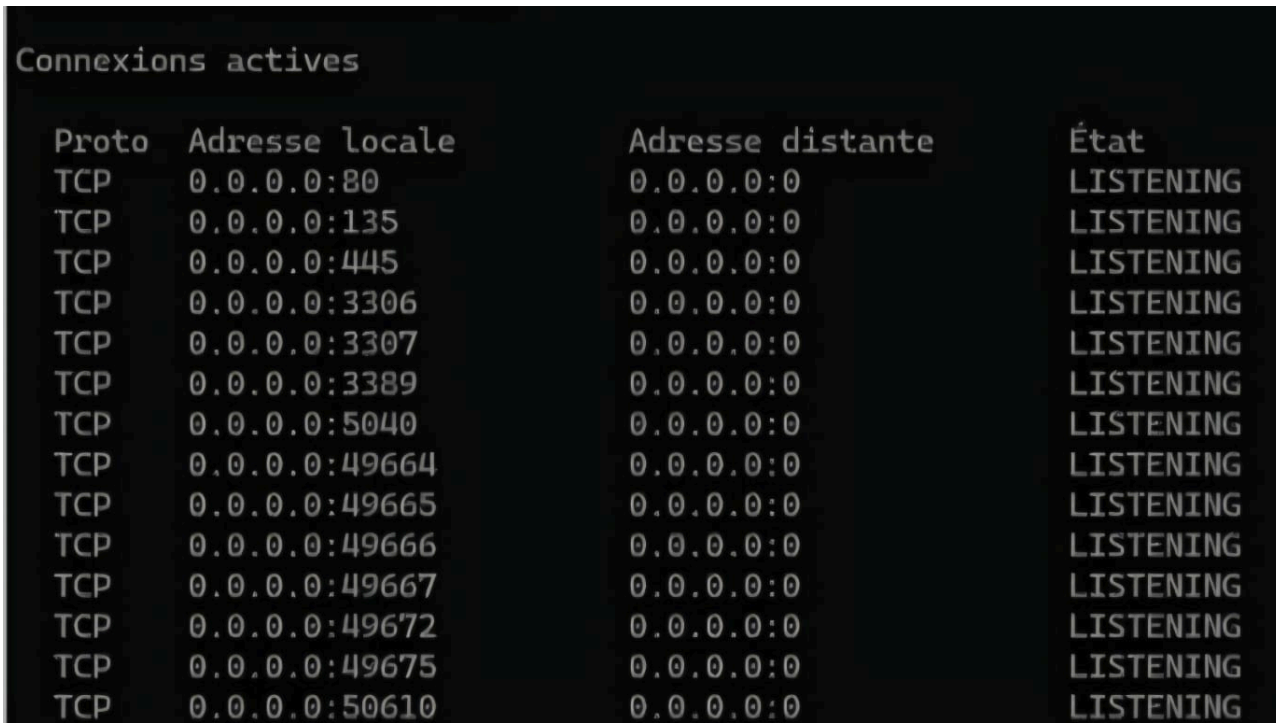
```
kametocorp1234@penguin:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
5: eth0@if6: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
en 1000
    link/ether 00:16:3e:de:39:50 brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 100.115.92.205/28 brd 100.115.92.207 scope global eth0
       valid_lft forever preferred_lft forever
    inet6 2001:861:56c3:ad80:216:3eff:fede:3950/64 scope global dynamic mngtmpaddr
       valid_lft 86009sec preferred_lft 14009sec
    inet6 fe80::216:3eff:fede:3950/64 scope link
       valid_lft forever preferred_lft forever
```

Ensuite ping de la machine de kevin avec la commande ping <entrer ip kevin> :

```
C:\Users\mhidaoui>ping 172.17.5.26

Envoi d'une requête 'Ping'  172.17.5.26 avec 32 octets de données :
Réponse de 172.17.5.26 : octets=32 temps=14 ms TTL=128
Réponse de 172.17.5.26 : octets=32 temps=29 ms TTL=128
Réponse de 172.17.5.26 : octets=32 temps=49 ms TTL=128
Réponse de 172.17.5.26 : octets=32 temps=59 ms TTL=128

Statistiques Ping pour 172.17.5.26:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 14ms, Maximum = 59ms, Moyenne = 37ms

C:\Users\mhidaoui>
```

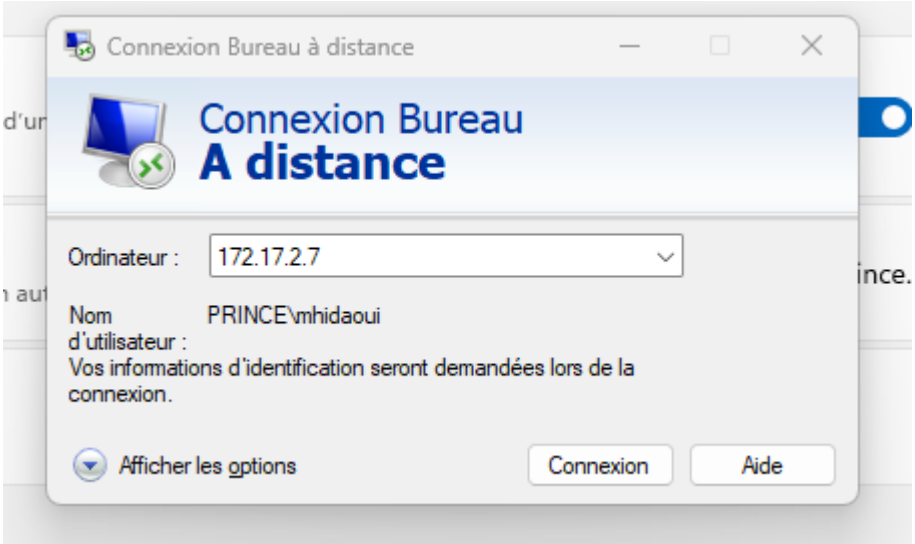
connexion bureau à distance (paramètre > bureau à distance > activé)
sans screenshot

commande netstat -an pour savoir sur quelle port écoute le serveur terminal :



Et le port d'ecoute et la ligne de commande TCP numéro 6 soit :
"TCP 0.0.0.0:3389 0.0.0.0:0 LISTENING"
donc le port : **0.0.0.0:3389**

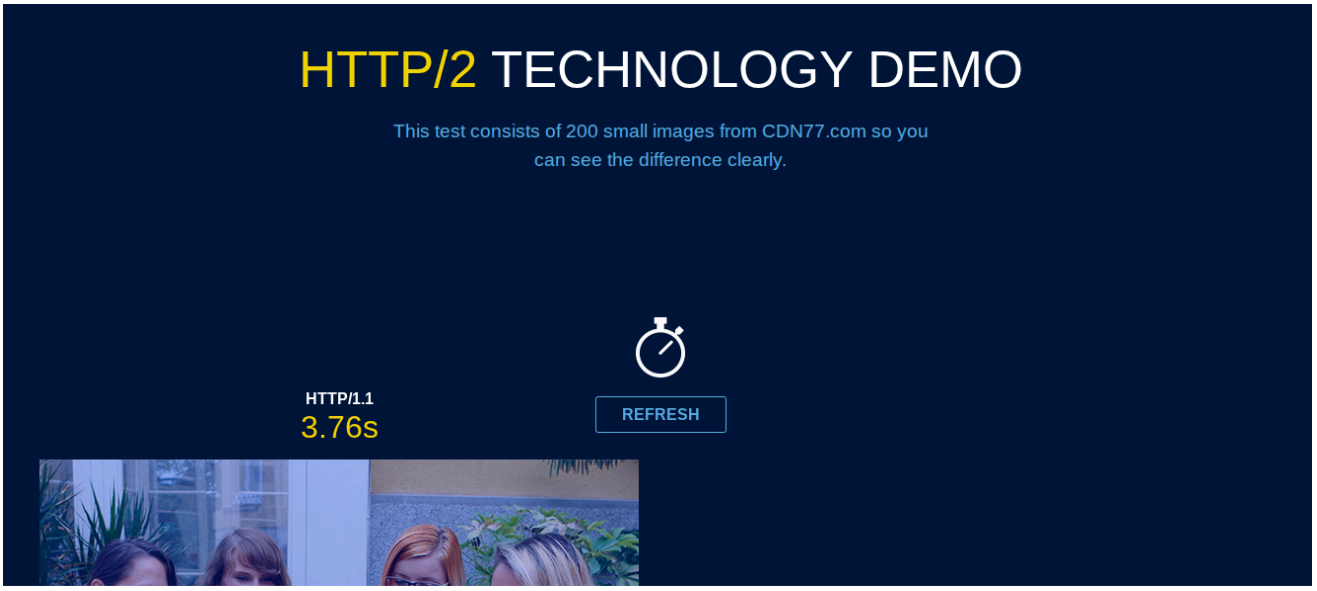
Connexion bureau à distance avec l'ip de Rayan :



qui m'a permis d'avoir accès à sa session BTS SIO avec l'encoche blanche qui affiche mon IP et sur l'invite de commande une des ligne la concernant affiche une connexion établie (pas de screenshot du au faite que je n'étais pas sur ma session même avec l'utilisation d'une clé USB)

Partie 2 : Capture de Trame HTTP

Affichage du site "http://www.http2demo.io/"



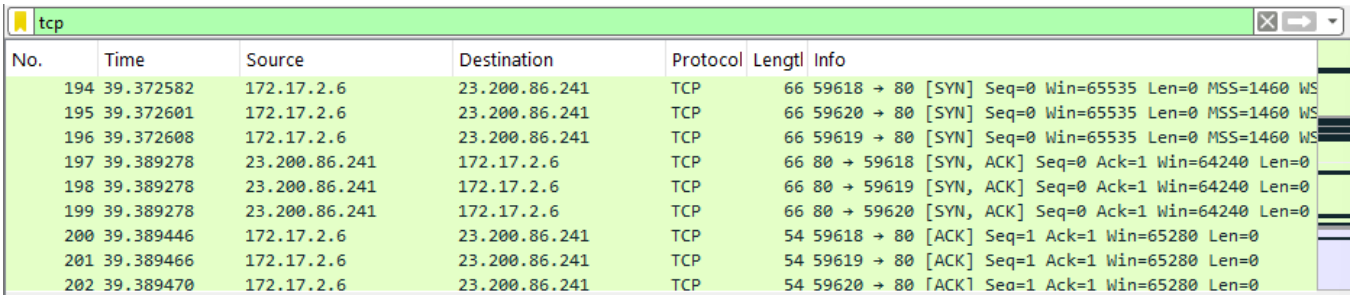
Arrêt de la capture de la trame avec le filtre HTTP et TCP :

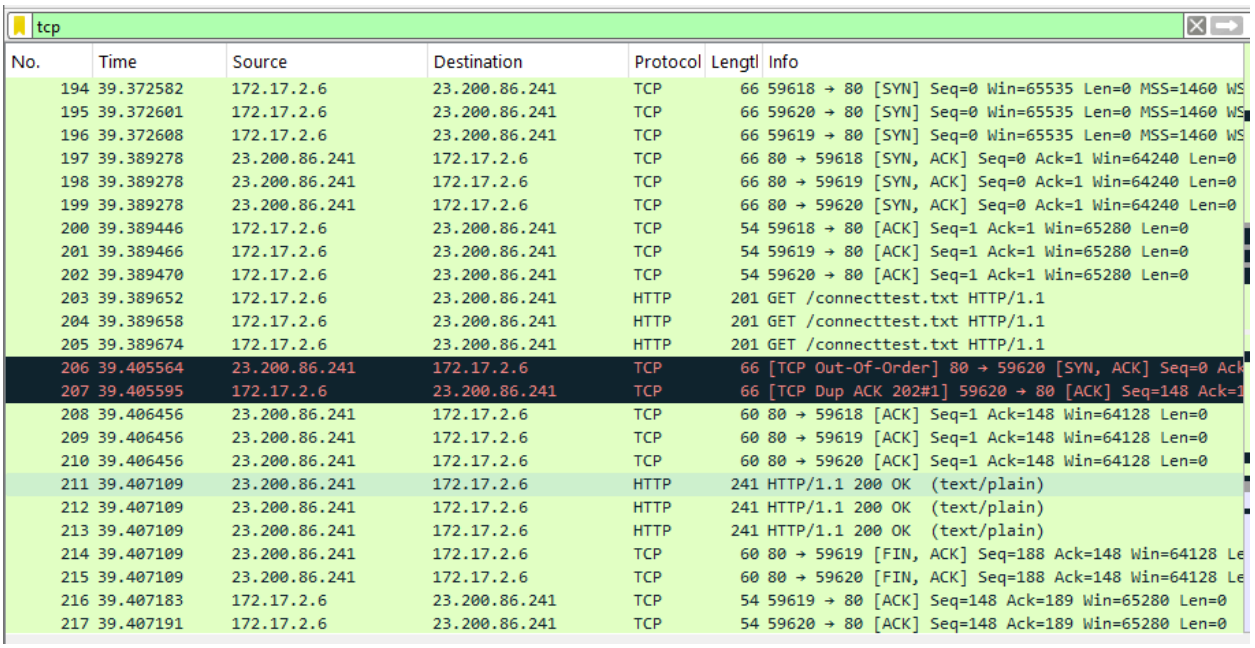
HTTP :

http

No.	Time	Source	Destination	Protocol	Lengtl	Info
203	39.389652	172.17.2.6	23.200.86.241	HTTP	201	GET /connecttest.txt HTTP/1.1
204	39.389658	172.17.2.6	23.200.86.241	HTTP	201	GET /connecttest.txt HTTP/1.1
205	39.389674	172.17.2.6	23.200.86.241	HTTP	201	GET /connecttest.txt HTTP/1.1
211	39.407109	23.200.86.241	172.17.2.6	HTTP	241	HTTP/1.1 200 OK (text/plain)
212	39.407109	23.200.86.241	172.17.2.6	HTTP	241	HTTP/1.1 200 OK (text/plain)
213	39.407109	23.200.86.241	172.17.2.6	HTTP	241	HTTP/1.1 200 OK (text/plain)
8749…	75.889400	172.17.2.6	23.200.87.13	HTTP	201	GET /connecttest.txt HTTP/1.1
8749…	75.889401	172.17.2.6	23.200.87.13	HTTP	201	GET /connecttest.txt HTTP/1.1
8749…	75.889893	172.17.2.6	23.200.87.13	HTTP	201	GET /connecttest.txt HTTP/1.1
8749…	75.907560	23.200.87.13	172.17.2.6	HTTP	241	HTTP/1.1 200 OK (text/plain)
8749…	75.907560	23.200.87.13	172.17.2.6	HTTP	241	HTTP/1.1 200 OK (text/plain)
8749…	75.908259	23.200.87.13	172.17.2.6	HTTP	241	HTTP/1.1 200 OK (text/plain)

TCP :



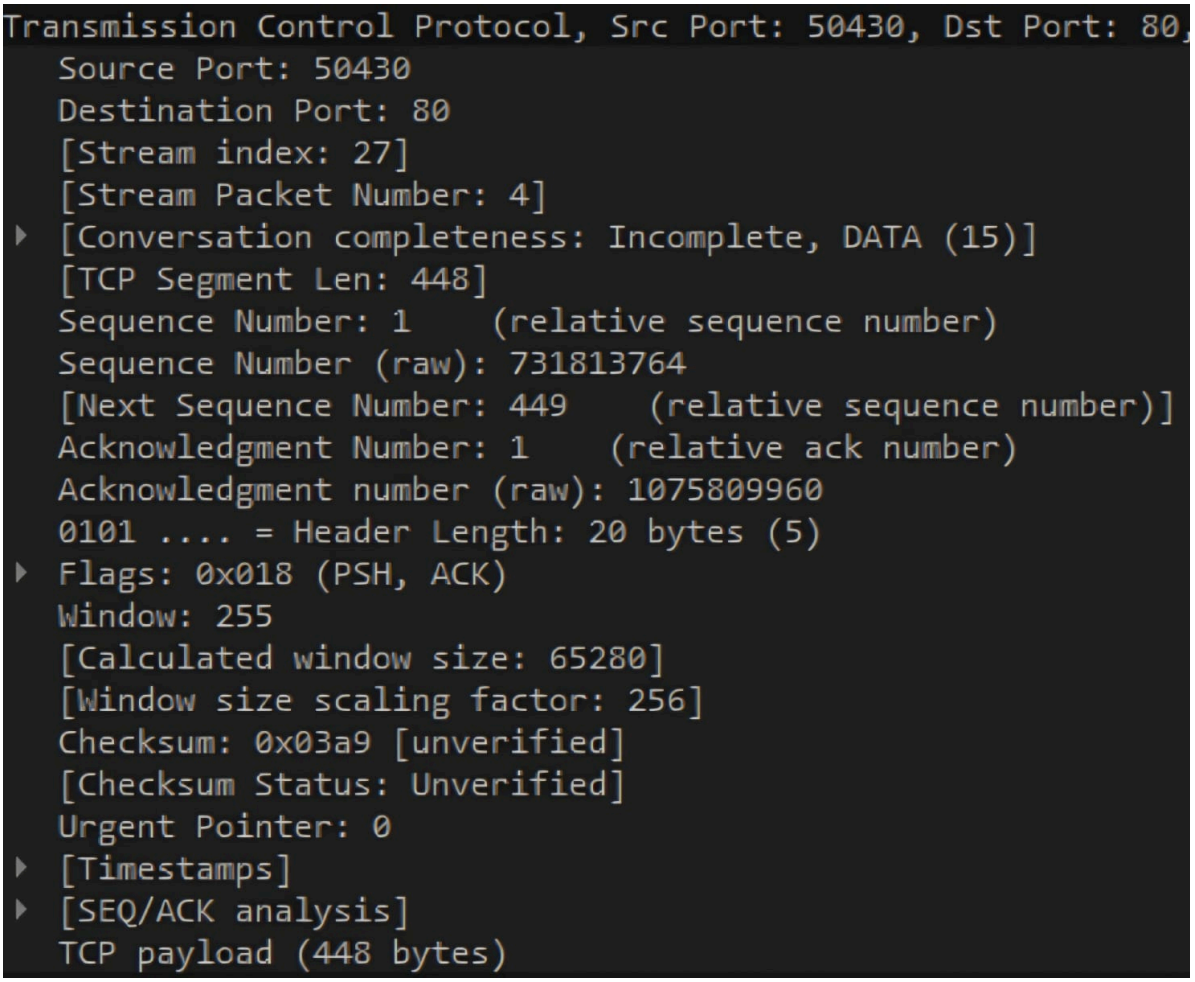


Exécution sur le terminal de commande de la commande :
> “**nslookcup** www.hppt2demo.io” ce qui nous donne ses 3 ip :

```
79.127.138.14
79.127.138.21
79.127.138.18
```

en les copiant et collant une par une sur le filtre de la trame de l’application wireshark ou découvre que celle du milieu et celle qui correspond à la requête http soit : 79.127.138.14

voici un screenshot de E.T de transport de la trame :

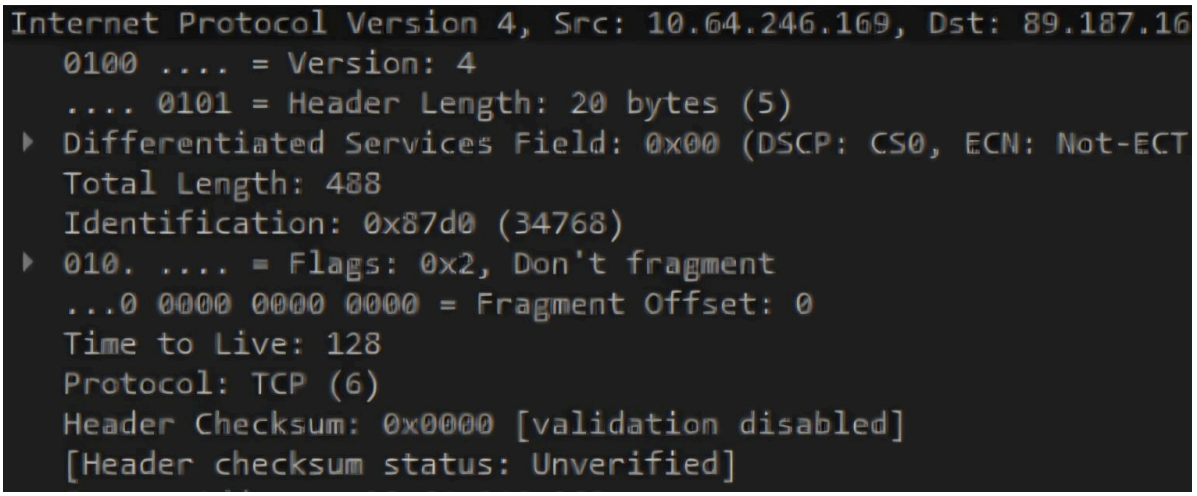


Sous-Partie : Questions :

1. **Nom protocole transport utilisé pour une trame HTTP :** TCP.
2. **Nom PDU encapsulant les données applicatives HTTP :** Segment TCP.
3. **Longueur de E.T de transport :** 20 octets
4. **Valeurs des ports source et destination :**

- Décimal : source = 50430 et destination = 80
- Hexadécimal : source = 0xC4FE et destination = 0x0050

Voici la section développer de E.T réseau :



Sous-Partie : Questions :

1. **Longueur de l'en-tête réseau :** 20 octets

2. **Champ Protocol :**
   Valeur = 6 → protocole TCP

3. **Adresses IP source et destination :**

- Source : 10.64.246.169
- hexadécimal : 0A 40 F6 A9

- Destination : 89.187.167.41
- hexadécimal : 59 BB A7 29

Voici la section de E.T d'ethernet :

Sous-Partie : Questions :

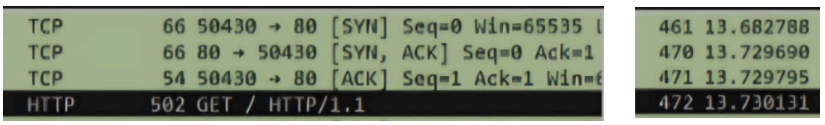
1. **Champ EtherType :**

   Valeur = 0x0800
   Signifie que la trame transporte un paquet IPv4

2. **Adresses MAC :**

- Destination : f6:f9:66:89:f3:f7
- Source : d0:57:7e:28:9b:41

Screenshot pour identifier les trois trame de la connexion TCP (Deux partie (Information) et (Numérotations)) :



3. **a. Quelle est la valeur du champ EtherType et que représente-t-elle ?**

   b. Quelles sont les adresses MAC source et destination ?

   c. Quelles trames composent le three-way handshake TCP et quels sont leurs flags ?

Trame 461 :
Source → Destination : 10.64.246.169 → 89.187.167.41
Flags TCP : [SYN]
Rôle : demande de synchro. envoyée par le client au serveur

Trame 470 :
Source → Destination : 89.187.167.41 → 10.64.246.169
Flags TCP : [SYN, ACK]
Rôle : rép serveur confirmant la demande et synchro. en retour

Trame 471 :
Source → Destination : 10.64.246.169 → 89.187.167.41
Flags TCP : [ACK]

Rôle : confirmation finale du client

Ces trois trames **(SYN → SYN/ACK → ACK)** = **three-way handshake** = connexion TCP entre le client et le serveur avant l'envoi de la requête HTTP dernière ligne du screenshot (472).

4. **Que signifient les champs des 3 segments TCP du handshake et pourquoi ce mode connecté est-il utilisé ? (Plus détaillé)**

Segment 1 (SYN) : le client envoie une requête de synchronisation pour initier la connexion et propose un numéro de séquence initial.

Segment 2 (SYN, ACK) : le serveur accuse réception du SYN du client (ACK) et envoie à son tour un SYN avec son propre numéro de séquence initial.

Segment 3 (ACK) : le client accuse réception du SYN du serveur, confirmant ainsi la connexion.

Raison du mode connecté :
Le protocole TCP utilise ce mécanisme pour établir une communication fiable et ordonnée entre deux hôtes, garantissant que les deux parties sont prêtes à échanger des données avant de commencer la transmission mais aussi sécurisé sans risque de modification ou oublie d'informations contrairement au protocole UDP.