

TP3 – Les ports logiciels

Sommaire

1) Connexion Bureau à distance (RDP).....	1
1) Capture de trames HTTP.....	4

1) Connexion Bureau à distance (RDP)

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

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

Proto  Adresse locale      Adresse distante    État                Conn
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
```

Systeme > Bureau à distance

Bureau à distance
Connectez-vous à cet ordinateur et utilisez-le à partir d'un autre appareil à l'aide de l'application Bureau à distance. Activé

Nom du PC
Utiliser ce nom pour se connecter à ce PC à partir d'un autre appareil. G102-GB13.prince.local

Utilisateurs du Bureau à distance
Sélectionner qui peut accéder à distance à ce PC. ✎

activation du paramètres bureau a distance

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

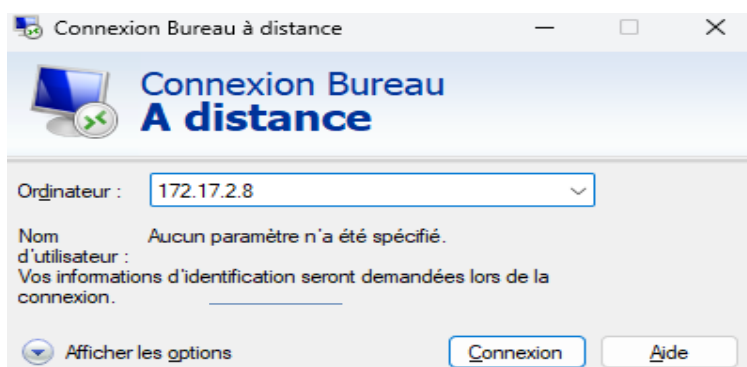
```
C:\Users\mballester>netstat -an

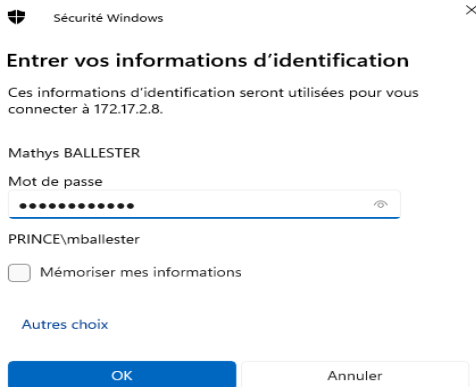
Connexions actives

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
```

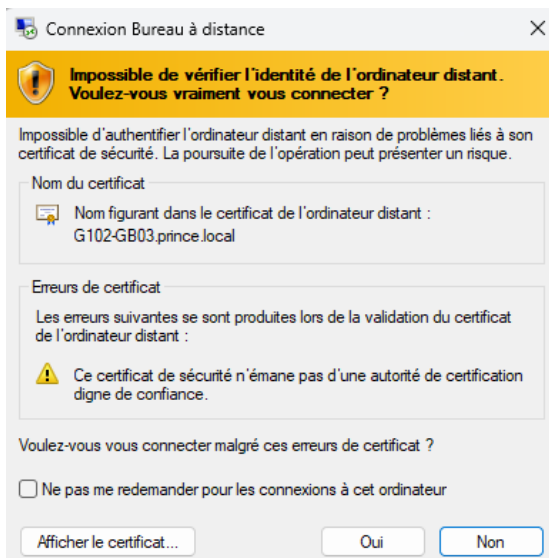
le port d'écoute du serveur Terminal Server est donc le port 3389

je saisis l'adresse IP de mon voisin sur connexion bureau a distance puis je clique sur connexion





je clique sur oui :



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

```
C:\Users\mballester>ipconfig

Configuration IP de Windows

Carte Ethernet vEthernet (Default Switch) :

    Suffixe DNS propre à la connexion. . . . :
    Adresse IPv6 de liaison locale. . . . . : fe80::3d30:e745:d20f:b8a8%27
    Adresse IPv4. . . . . : 172.21.128.1
    Masque de sous-réseau. . . . . : 255.255.240.0
    Passerelle par défaut. . . . . :

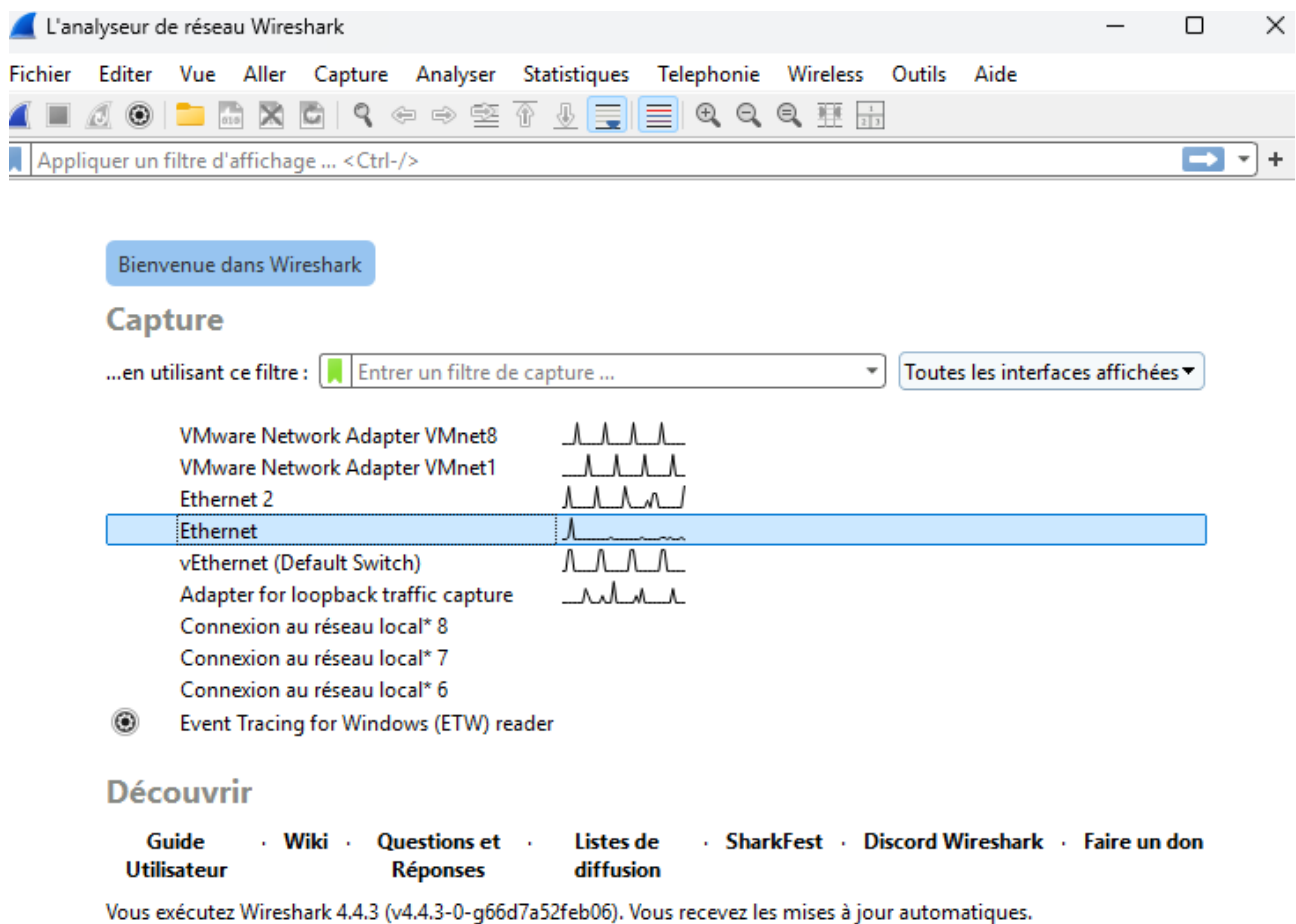
Carte Ethernet Ethernet :

    Suffixe DNS propre à la connexion. . . . : prince.local
    Adresse IPv4. . . . . : 172.17.2.8
    Masque de sous-réseau. . . . . : 255.255.0.0
    Passerelle par défaut. . . . . : 172.17.250.3
```

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

2) Capture de trames HTTP

Lancement de wireshark:



No.	Time	Source	Destination	Protocol	Length	Info
968	6.170638	172.17.2.7	79.127.138.21	HTTP	625	GET /http2/http1.html HTTP/1.1
970	6.180799	79.127.138.21	172.17.2.7	TCP	60	80 → 51314 [ACK] Seq=1 Ack=572 Win=126 Len=0
971	6.181452	79.127.138.21	172.17.2.7	HTTP	443	HTTP/1.1 304 Not Modified
999	6.231909	172.17.2.7	79.127.138.21	TCP	54	51314 → 80 [ACK] Seq=572 Ack=390 Win=251 Len=0
1124	6.988264	172.17.2.7	79.127.138.21	HTTP	558	GET /http2/tiles_final/tile_0.png HTTP/1.1
1125	6.988411	172.17.2.7	79.127.138.21	HTTP	557	GET /http2/tiles_final/tile_2.png HTTP/1.1
1126	6.988461	172.17.2.7	79.127.138.21	HTTP	557	GET /http2/tiles_final/tile_3.png HTTP/1.1
1127	6.988696	172.17.2.7	79.127.138.21	HTTP	557	GET /http2/tiles_final/tile_4.png HTTP/1.1

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:

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

R?ponse ne faisant pas autorit? :
Nom : 1906714720.rsc.cdn77.org
Addresses: 2a02:6ea0:dc00::30
           2a02:6ea0:dc00::32
           2a02:6ea0:dc00::31
           79.127.138.21
           79.127.138.15
           79.127.138.17
Aliases: www.http2demo.io
```

Repérage de la Trame de notre requête http:

ip.addr==79.127.138.21&&tcp.port==80

No.	Time	Source	Destination	Protocol	Length	Info
968	6.170638	172.17.2.7	79.127.138.21	HTTP	625	GET /http2/http1.html HTTP/1.1
970	6.180799	79.127.138.21	172.17.2.7	TCP	60	80 → 51314 [ACK] Seq=1 Ack=572 Win=126 Len=0
971	6.181452	79.127.138.21	172.17.2.7	HTTP	443	HTTP/1.1 304 Not Modified
999	6.231909	172.17.2.7	79.127.138.21	TCP	54	51314 → 80 [ACK] Seq=572 Ack=390 Win=251 Len=0
1124	6.988264	172.17.2.7	79.127.138.21	HTTP	558	GET /http2/tiles_final/tile_0.png HTTP/1.1
1125	6.988411	172.17.2.7	79.127.138.21	HTTP	557	GET /http2/tiles_final/tile_2.png HTTP/1.1
1126	6.988461	172.17.2.7	79.127.138.21	HTTP	557	GET /http2/tiles_final/tile_3.png HTTP/1.1
1127	6.988696	172.17.2.7	79.127.138.21	HTTP	557	GET /http2/tiles_final/tile_4.png HTTP/1.1
1128	6.988812	172.17.2.7	79.127.138.21	HTTP	557	GET /http2/tiles_final/tile_5.png HTTP/1.1
1129	6.988855	172.17.2.7	79.127.138.21	HTTP	557	GET /http2/tiles_final/tile_6.png HTTP/1.1
1130	6.994888	79.127.138.21	172.17.2.7	TCP	60	80 → 64806 [ACK] Seq=1 Ack=504 Win=126 Len=0
1131	6.994888	79.127.138.21	172.17.2.7	HTTP	419	HTTP/1.1 304 Not Modified
1132	6.995392	79.127.138.21	172.17.2.7	TCP	60	80 → 65000 [ACK] Seq=1 Ack=504 Win=126 Len=0
1133	6.995392	79.127.138.21	172.17.2.7	HTTP	418	HTTP/1.1 304 Not Modified
1134	6.995392	79.127.138.21	172.17.2.7	TCP	60	80 → 49277 [ACK] Seq=1 Ack=504 Win=126 Len=0
1135	6.995392	79.127.138.21	172.17.2.7	TCP	60	80 → 61316 [ACK] Seq=1 Ack=504 Win=126 Len=0
1136	6.995392	79.127.138.21	172.17.2.7	HTTP	418	HTTP/1.1 304 Not Modified
1137	6.996059	79.127.138.21	172.17.2.7	HTTP	418	HTTP/1.1 304 Not Modified
1138	6.996059	79.127.138.21	172.17.2.7	HTTP	418	HTTP/1.1 304 Not Modified
1139	6.996059	79.127.138.21	172.17.2.7	TCP	60	80 → 63755 [ACK] Seq=1 Ack=504 Win=126 Len=0
1140	6.996059	79.127.138.21	172.17.2.7	HTTP	418	HTTP/1.1 304 Not Modified
1141	6.998352	172.17.2.7	79.127.138.21	HTTP	557	GET /http2/tiles_final/tile_7.png HTTP/1.1
1142	6.999354	172.17.2.7	79.127.138.21	HTTP	557	GET /http2/tiles_final/tile_8.png HTTP/1.1
1143	6.999478	172.17.2.7	79.127.138.21	HTTP	557	GET /http2/tiles_final/tile_9.png HTTP/1.1
1144	7.004968	79.127.138.21	172.17.2.7	HTTP	418	HTTP/1.1 304 Not Modified

```

> Frame 968: 625 bytes on wire (5000 bits), 625 bytes captured (5000 bits) on interface \Device\NPF_{B4F47397-6371-47C2-9511-55F9A50174}
> Ethernet II, Src: GigaByteTech_2f:7f:ed (74:56:3c:2f:7f:ed), Dst: Stormshield_2a:a8:34 (00:0d:b4:2a:a8:34)
> Internet Protocol Version 4, Src: 172.17.2.7, Dst: 79.127.138.21
> Transmission Control Protocol, Src Port: 51314, Dst Port: 80, Seq: 1, Ack: 1, Len: 571
  Hypertext Transfer Protocol
    GET /http2/http1.html HTTP/1.1\r\n
      Request Method: GET
      Request URI: /http2/http1.html
      Request Version: HTTP/1.1
      Host: 1153288396.rsc.cdn77.org\r\n
      Connection: keep-alive\r\n
      Upgrade-Insecure-Requests: 1\r\n
      User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/141.0.0.0 Safari/537.36 Edg/141.0.0.0 Safari/537.36 Edg/141.0.0.0
      Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;q=0.7\r\n
      Referer: http://www.http2demo.io/\r\n
      Accept-Encoding: gzip, deflate\r\n
      Accept-Language: fr,fr-FR;q=0.9,en;q=0.8,en-GB;q=0.7,en-US;q=0.6\r\n
      If-None-Match: W/"570b88dc-45c3"\r\n
      \r\n
    [Response in frame: 971]
    [Full request URI: http://1153288396.rsc.cdn77.org/http2/http1.html]
  
```

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

```

> Frame 968: 625 bytes on wire (5000 bits), 625 bytes captured (5000 bits) on interface \Device\NPF_{B4F47397-6371-47C2-9511-55F9A50174}
> Ethernet II, Src: GigaByteTech_2f:7f:ed (74:56:3c:2f:7f:ed), Dst: Stormshield_2a:a8:34 (00:0d:b4:2a:a8:34)
> Internet Protocol Version 4, Src: 172.17.2.7, Dst: 79.127.138.21
> Transmission Control Protocol, Src Port: 51314, Dst Port: 80, Seq: 1, Ack: 1, Len: 571
  Source Port: 51314
  Destination Port: 80
  [Stream index: 35]
  [Conversation completeness: Incomplete (12)]
  [TCP Segment Len: 571]
  Sequence Number: 1 (relative sequence number)
  Sequence Number (raw): 2143209637
  [Next Sequence Number: 572 (relative sequence number)]
  Acknowledgment Number: 1 (relative ack number)
  Acknowledgment number (raw): 263842122
  0101 ... = Header Length: 20 bytes (5)
  Flags: 0x01B (PSH, ACK)
  Window: 253
  [Calculated window size: 253]
  [Window size scaling factor: -1 (unknown)]
  
```

Quel est le nom du protocole transport utilisé par une frame 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 51314 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 :

The screenshot shows a network packet capture analysis tool. On the left, the details of an Internet Protocol Version 4 (IPv4) header are displayed. A red box highlights the header fields, and a red arrow points from the 'Total Length: 611' field to the corresponding hex value '0000' in the hex dump on the right.

```

> Frame 968: 625 bytes on wire (5000 bits), 625 bytes captured (5000 bits) on interface \Device\NPF_{B4F47397-6371-47C2-9511-55F9A50174}
> Ethernet II, Src: GigaByteTech 2f:7f:ed (74:56:3c:2f:7f:ed), Dst: Stormshield_2a:a8:34 (00:0d:b4:2a:a8:34)
< Internet Protocol Version 4, Src: 172.17.2.7, Dst: 79.127.138.21
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
  Total Length: 611
  Identification: 0xcddf (52703)
  > 010. .... = Flags: 0x2, Don't fragment
  ...0 0000 0000 0000 = Fragment Offset: 0
  Time to Live: 128
  Protocol: TCP (6)
  Header Checksum: 0x0000 [validation disabled]
  [Header checksum status: Unverified]
  Source Address: 172.17.2.7
  Destination Address: 79.127.138.21
  [Stream index: 45]
> Transmission Control Protocol, Src Port: 51314, Dst Port: 80, Seq: 1, Ack: 1, Len: 571
> Hypertext Transfer Protocol
  
```

Hex dump (relevant parts):

```

0000 00 0d b4 2a a8 34 74 56 3c 2f 7f ed 08 00 45 00 ...* Atv </...E
0010 02 63 cd df 40 00 80 06 00 00 ac 11 02 07 4f 7f ...@... ..JP
0020 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ...r P... ..JP
0030 00 fd 8a 02 00 00 47 45 54 20 2f 68 74 74 70 32 .....GE T /http
0040 2f 68 74 74 70 31 2e 68 74 6d 6c 20 48 54 54 50 /http.h tml HTTP
0050 2f 31 2e 31 0d 0a 48 6f 73 74 3a 20 31 31 35 33 /1.1..Ho st: 115:
0060 32 38 38 33 39 36 2e 72 73 63 2e 63 64 6e 37 37 288396.r sc.cdn7
0070 2e 6f 72 67 0d 0a 43 6f 6e 6e 65 63 74 69 6f 6e .org..Co nnection
0080 3a 20 6b 65 65 70 2d 61 6c 69 76 65 0d 0a 55 70 : keep-a live..U
0090 67 72 61 64 65 2d 49 6e 73 65 63 75 72 65 2d 52 grade-In secure-
00a0 65 71 75 65 73 74 73 3a 20 31 0d 0a 55 73 65 72 equests: 1..User
00b0 2d 41 67 65 6e 74 3a 20 4d 6f 7a 69 6c 6c 61 2f -Agent: Mozilla,
00c0 35 2e 30 20 28 57 69 6e 64 6f 77 73 20 4e 54 20 5.0 (Win dows NT
00d0 31 30 2e 30 3b 20 57 69 6e 36 34 3b 20 78 36 34 10.0; W! n64; x8
00e0 29 20 41 70 70 6c 65 57 65 62 4b 69 74 2f 35 33 ) AppleW ebKit/5
00f0 37 2e 33 36 20 28 4b 48 54 4d 4c 2c 20 6c 69 6b 7.36 (KH TML, li
0100 65 20 47 65 63 6b 6f 29 20 43 68 72 6f 6d 65 2f e Gecko) Chrome
0110 31 34 31 2e 30 2e 30 2e 30 20 53 61 66 61 72 69 141.0.0.0 Safar
0120 2f 35 33 37 2e 33 36 20 45 64 67 2f 31 34 31 2e /537.36 Edg/141
0130 30 2e 30 2e 30 0d 0a 41 63 63 65 70 74 3a 20 74 0.0.0..A ccept:
0140 65 78 74 2f 68 74 6d 6c 2c 61 70 70 6c 69 63 61 ext/html ,applic
0150 74 69 6f 6e 2f 78 68 74 6d 6c 2b 78 6d 6c 2c 61 tion/xht ml+xml,
0160 70 70 6c 69 63 61 74 69 6f 6e 2f 78 6d 6c 3b 71 pplicati on/xml;
0170 3d 30 2e 39 2c 69 6d 61 67 65 2f 61 76 69 66 2c =0.9,ima ge/avif
0180 69 6d 61 67 65 2f 77 65 62 70 2c 69 6d 61 67 65 image/we bp,imag
0190 2f 61 70 6e 67 2c 2a 2f 2a 3b 71 3d 30 2e 38 2c /apng,*/* ;q=0.8
01a0 61 70 70 6c 69 63 61 74 69 6f 6e 2f 73 69 67 6e applicat ion/sign
01b0 65 64 2d 65 78 63 68 61 6e 67 65 3b 76 3d 62 33 ed-excha nge;v=
  
```

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 172.17.2.7 et ça valeur en hexadécimal est 11-02-07-07
- 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 :

```

Frame 968: 625 bytes on wire (5000 bits) - 625 bytes captured (5000 bits) on interface \Device\NPF_{84F47397-6371-47C2-9511-55F9A50174}
Ethernet II, Src: GigaByteTech_2f:7f:ed (74:56:3c:2f:7f:ed), Dst: Stormshield_2a:a8:34 (00:0d:b4:2a:a8:34)
  > Destination: Stormshield_2a:a8:34 (00:0d:b4:2a:a8:34)
  > Source: GigaByteTech_2f:7f:ed (74:56:3c:2f:7f:ed)
  Type: IPv4 (0x0800)
  [Stream index: 1]
Internet Protocol Version 4, Src: 172.17.2.7, Dst: 79.127.138.21
Transmission Control Protocol, Src Port: 51314, Dst Port: 80, Seq: 1, Ack: 1, Len: 571
Hypertext Transfer Protocol
0000 00 0d b4 2a a8 34 74 56 3c 2f 7f ed 08 00 45 00  ....*4tv </....E-
0010 82 63 cd df 40 00 80 06 00 00 ac 11 02 07 4f 7f  ..c..@... ..0-
0020 8a 15 c8 72 00 50 7f be c8 a5 0f b9 e9 4a 50 18  ..r.P... ..JP-
0030 00 fd 8a 02 00 00 47 45 54 20 2f 68 74 74 70 32  ..GE T /http2
0040 2f 68 74 74 70 31 2e 68 74 6d 6c 20 48 54 54 50  /http1.h tml HTTP
0050 2f 31 2e 31 0d 0a 48 6f 73 74 3a 20 31 31 35 33  /1.1..Ho st: 1153
0060 32 38 38 33 39 36 2e 72 73 63 2e 63 64 6e 37 37  288396.r sc.cdn77
0070 2e 6f 72 67 0d 0a 43 6f 6e 6e 65 63 74 69 6f 6e  .org..Co nnection
0080 3a 20 6b 65 65 70 2d 61 6c 69 76 65 0d 0a 55 70  : keep-a live..Up
0090 67 72 61 64 65 2d 49 6e 73 65 63 75 72 65 2d 52  grade-In secure-R
00a0 65 71 75 65 73 74 73 3a 20 31 0d 0a 55 73 65 72  equests: 1..User
  
```

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 :

1166	9.740772	172.17.2.7	79.127.138.14	TCP	66	63937 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
1177	9.750980	79.127.138.14	172.17.2.7	TCP	66	80 → 63937 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM WS=512
1178	9.751138	172.17.2.7	79.127.138.14	TCP	54	63937 → 80 [ACK] Seq=1 Ack=1 Win=65280 Len=0
1179	9.751630	172.17.2.7	79.127.138.14	HTTP	625	GET /http2/http1.html HTTP/1.1
1180	9.758462	79.127.138.14	172.17.2.7	TCP	60	80 → 63937 [ACK] Seq=1 Ack=572 Win=32889856 Len=0
1189	9.776014	79.127.138.14	172.17.2.7	TCP	60	[TCP Window Update] 80 → 63937 [ACK] Seq=1 Ack=572 Win=64512 Len=0
1190	9.776521	79.127.138.14	172.17.2.7	HTTP	443	HTTP/1.1 304 Not Modified
1226	9.798487	172.17.2.7	79.127.138.14	TCP	66	50987 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
1228	9.800120	172.17.2.7	79.127.138.14	TCP	66	58849 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
1230	9.800942	172.17.2.7	79.127.138.14	TCP	66	59211 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
1231	9.801098	172.17.2.7	79.127.138.14	HTTP	558	GET /http2/tiles_final/tile_0.png HTTP/1.1
1232	9.802140	172.17.2.7	79.127.138.14	TCP	66	62464 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
1233	9.802569	172.17.2.7	79.127.138.14	TCP	66	58270 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
1236	9.805583	79.127.138.14	172.17.2.7	TCP	66	80 → 50987 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM WS=512
1237	9.805727	172.17.2.7	79.127.138.14	TCP	54	50987 → 80 [ACK] Seq=1 Ack=1 Win=65280 Len=0
1238	9.806415	79.127.138.14	172.17.2.7	TCP	66	80 → 58849 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM WS=512
1239	9.806443	172.17.2.7	79.127.138.14	HTTP	557	GET /http2/tiles_final/tile_2.png HTTP/1.1
1240	9.806524	172.17.2.7	79.127.138.14	TCP	54	58849 → 80 [ACK] Seq=1 Ack=1 Win=65280 Len=0
1241	9.806503	79.127.138.14	172.17.2.7	TCP	66	80 → 59211 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM WS=512
1242	9.806668	172.17.2.7	79.127.138.14	TCP	54	59211 → 80 [ACK] Seq=1 Ack=1 Win=65280 Len=0
1243	9.807127	172.17.2.7	79.127.138.14	HTTP	557	GET /http2/tiles_final/tile_3.png HTTP/1.1
1244	9.807409	172.17.2.7	79.127.138.14	HTTP	557	GET /http2/tiles_final/tile_4.png HTTP/1.1
1246	9.809593	79.127.138.14	172.17.2.7	HTTP	419	HTTP/1.1 304 Not Modified
1247	9.809593	79.127.138.14	172.17.2.7	TCP	66	80 → 62464 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM WS=512
1248	9.809593	79.127.138.14	172.17.2.7	TCP	66	80 → 58270 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM WS=512

Frame 1166: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF_{B4F47397-6371-47C2-9511-55F9A5017442}; Ethernet II, Src: GigaByteTech_2f:7f:ed (74:56:3c:2f:7f:ed), Dst: Stormshield_2a:a8:34 (00:0d:b4:2a:a8:34); Internet Protocol Version 4, Src: 172.17.2.7, Dst: 79.127.138.14

Transmission Control Protocol, Src Port: 63937, Dst Port: 80, Seq: 0, Len: 0

Source Port: 63937
Destination Port: 80
[Stream index: 31]
> [Conversation completeness: Incomplete, DATA (15)]
[TCP Segment Len: 0]
Sequence Number: 0 (relative sequence number)
Sequence Number (raw): 4255565003
[Next Sequence Number: 1 (relative sequence number)]
Acknowledgment Number: 0
Acknowledgment number (raw): 0
1000 = Header Length: 32 bytes (8)
> Flags: 0x002 (SYN)

0000 00 0d b4 2a a8 34 74 56 3c 2f 7f ed 00 00 45 00
0010 00 34 5c 7c 40 00 80 06 00 00 ac 11 02 07 4f 7f
0020 8a 0e f9 c1 00 50 fd a6 c4 cb 00 00 00 00 00 00
0030 ff ff 87 cc 00 00 02 04 05 b4 01 05 05 08 01 01
0040 04 02

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

1166	9.740772	172.17.2.7	79.127.138.14	TCP	66	63937	→ 80	[SYN]	Seq=0	Win=65535	Len=0	MSS=1460	WS=256	SACK_PERM		
1177	9.750980	79.127.138.14	172.17.2.7	TCP	66	80	→ 63937	[SYN, ACK]	Seq=0	Ack=1	Win=64240	Len=0	MSS=1460	SACK_PERM	WS=512	
1178	9.751138	172.17.2.7	79.127.138.14	TCP	54	63937	→ 80	[ACK]	Seq=1	Ack=1	Win=65280	Len=0				
1179	9.751630	172.17.2.7	79.127.138.14	HTTP	625	GET	/http2/http1.html	HTTP/1.1								
1180	9.758462	79.127.138.14	172.17.2.7	TCP	60	80	→ 63937	[ACK]	Seq=1	Ack=572	Win=32889856	Len=0				
1189	9.776014	79.127.138.14	172.17.2.7	TCP	60	[TCP Window Update]	80	→ 63937	[ACK]	Seq=1	Ack=572	Win=64512	Len=0			
1190	9.776521	79.127.138.14	172.17.2.7	HTTP	443	HTTP/1.1	304	Not Modified								
1226	9.798487	172.17.2.7	79.127.138.14	TCP	66	50987	→ 80	[SYN]	Seq=0	Win=65535	Len=0	MSS=1460	WS=256	SACK_PERM		
1228	9.800120	172.17.2.7	79.127.138.14	TCP	66	58849	→ 80	[SYN]	Seq=0	Win=65535	Len=0	MSS=1460	WS=256	SACK_PERM		
1230	9.800942	172.17.2.7	79.127.138.14	TCP	66	59211	→ 80	[SYN]	Seq=0	Win=65535	Len=0	MSS=1460	WS=256	SACK_PERM		
1231	9.801098	172.17.2.7	79.127.138.14	HTTP	558	GET	/http2/tiles_final/tile_0.png	HTTP/1.1								
1232	9.802140	172.17.2.7	79.127.138.14	TCP	66	62464	→ 80	[SYN]	Seq=0	Win=65535	Len=0	MSS=1460	WS=256	SACK_PERM		
1233	9.802569	172.17.2.7	79.127.138.14	TCP	66	58270	→ 80	[SYN]	Seq=0	Win=65535	Len=0	MSS=1460	WS=256	SACK_PERM		
1236	9.805583	79.127.138.14	172.17.2.7	TCP	66	80	→ 50987	[SYN, ACK]	Seq=0	Ack=1	Win=64240	Len=0	MSS=1460	SACK_PERM	WS=512	
1237	9.805727	172.17.2.7	79.127.138.14	TCP	54	50987	→ 80	[ACK]	Seq=1	Ack=1	Win=65280	Len=0				
1238	9.806415	79.127.138.14	172.17.2.7	TCP	66	80	→ 58849	[SYN, ACK]	Seq=0	Ack=1	Win=64240	Len=0	MSS=1460	SACK_PERM	WS=512	
1239	9.806443	172.17.2.7	79.127.138.14	HTTP	557	GET	/http2/tiles_final/tile_2.png	HTTP/1.1								
1240	9.806524	172.17.2.7	79.127.138.14	TCP	54	58849	→ 80	[ACK]	Seq=1	Ack=1	Win=65280	Len=0				
1241	9.806583	79.127.138.14	172.17.2.7	TCP	66	80	→ 59211	[SYN, ACK]	Seq=0	Ack=1	Win=64240	Len=0	MSS=1460	SACK_PERM	WS=512	
1242	9.806668	172.17.2.7	79.127.138.14	TCP	54	59211	→ 80	[ACK]	Seq=1	Ack=1	Win=65280	Len=0				
1243	9.807127	172.17.2.7	79.127.138.14	HTTP	557	GET	/http2/tiles_final/tile_3.png	HTTP/1.1								
1244	9.807409	172.17.2.7	79.127.138.14	HTTP	557	GET	/http2/tiles_final/tile_4.png	HTTP/1.1								
1246	9.809593	79.127.138.14	172.17.2.7	HTTP	419	HTTP/1.1	304	Not Modified								
1247	9.809593	79.127.138.14	172.17.2.7	TCP	66	80	→ 62464	[SYN, ACK]	Seq=0	Ack=1	Win=64240	Len=0	MSS=1460	SACK_PERM	WS=512	
1248	9.809593	79.127.138.14	172.17.2.7	TCP	66	80	→ 58270	[SYN, ACK]	Seq=0	Ack=1	Win=64240	Len=0	MSS=1460	SACK_PERM	WS=512	

> Frame 1177: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF_{B4F47397-6371-47C2-9511-55F9A5017442} [Ethernet II, Src: Stormshield_2a:a8:34 (00:0d:b4:2a:a8:34), Dst: GigaByteTech_2f:7f:ed (74:56:3c:2f:7f:ed)]
 > Internet Protocol Version 4, Src: 79.127.138.14, Dst: 172.17.2.7
 > Transmission Control Protocol, Src Port: 80, Dst Port: 63937, Seq: 0, Ack: 1, Len: 0
 Source Port: 80
 Destination Port: 63937
 [Stream index: 31]
 > [Conversation completeness: Incomplete, DATA (15)]
 [TCP Segment Len: 0]
 Sequence Number: 0 (relative sequence number)
 Sequence Number (raw): 1389167758
 [Next Sequence Number: 1 (relative sequence number)]
 Acknowledgment Number: 1 (relative ack number)
 Acknowledgment number (raw): 4255565004
 1000 = Header Length: 32 bytes (8)
 > Flags: 0x012 (SYN, ACK)

```

0000 74 56 3c 2f 7f ed 00 0d b4 2a a8 34 00 00 45 28 tV</...>*.4.-E(
0010 00 34 00 00 40 00 34 06 be f6 4f 7f 8a 0e ac 11 .4.@.4.-0....
0020 02 07 00 50 f9 c1 52 cd 04 8e fd a6 c4 cc 80 1a ...P..R.....4
0030 fa f0 d8 87 00 00 02 04 05 b4 01 01 04 02 01 03 .....
0040 03 09
  
```

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

1166	9.740772	172.17.2.7	79.127.138.14	TCP	66	63937	→ 80	[SYN]	Seq=0	Win=65535	Len=0	MSS=1460	WS=256	SACK_PERM		
1177	9.750980	79.127.138.14	172.17.2.7	TCP	66	80	→ 63937	[SYN, ACK]	Seq=0	Ack=1	Win=64240	Len=0	MSS=1460	SACK_PERM	WS=512	
1178	9.751138	172.17.2.7	79.127.138.14	TCP	54	63937	→ 80	[ACK]	Seq=1	Ack=1	Win=65280	Len=0				
1179	9.751630	172.17.2.7	79.127.138.14	HTTP	625	GET	/http2/http1.html	HTTP/1.1								
1180	9.758462	79.127.138.14	172.17.2.7	TCP	60	80	→ 63937	[ACK]	Seq=1	Ack=572	Win=32889856	Len=0				
1189	9.776014	79.127.138.14	172.17.2.7	TCP	60	[TCP Window Update]	80	→ 63937	[ACK]	Seq=1	Ack=572	Win=64512	Len=0			
1190	9.776521	79.127.138.14	172.17.2.7	HTTP	443	HTTP/1.1	304	Not Modified								
1226	9.798487	172.17.2.7	79.127.138.14	TCP	66	50987	→ 80	[SYN]	Seq=0	Win=65535	Len=0	MSS=1460	WS=256	SACK_PERM		
1228	9.800120	172.17.2.7	79.127.138.14	TCP	66	58849	→ 80	[SYN]	Seq=0	Win=65535	Len=0	MSS=1460	WS=256	SACK_PERM		
1230	9.800942	172.17.2.7	79.127.138.14	TCP	66	59211	→ 80	[SYN]	Seq=0	Win=65535	Len=0	MSS=1460	WS=256	SACK_PERM		
1231	9.801098	172.17.2.7	79.127.138.14	HTTP	558	GET	/http2/tiles_final/tile_0.png	HTTP/1.1								
1232	9.802140	172.17.2.7	79.127.138.14	TCP	66	62464	→ 80	[SYN]	Seq=0	Win=65535	Len=0	MSS=1460	WS=256	SACK_PERM		
1233	9.802569	172.17.2.7	79.127.138.14	TCP	66	58270	→ 80	[SYN]	Seq=0	Win=65535	Len=0	MSS=1460	WS=256	SACK_PERM		
1236	9.805583	79.127.138.14	172.17.2.7	TCP	66	80	→ 50987	[SYN, ACK]	Seq=0	Ack=1	Win=64240	Len=0	MSS=1460	SACK_PERM	WS=512	
1237	9.805727	172.17.2.7	79.127.138.14	TCP	54	50987	→ 80	[ACK]	Seq=1	Ack=1	Win=65280	Len=0				
1238	9.806415	79.127.138.14	172.17.2.7	TCP	66	80	→ 58849	[SYN, ACK]	Seq=0	Ack=1	Win=64240	Len=0	MSS=1460	SACK_PERM	WS=512	
1239	9.806443	172.17.2.7	79.127.138.14	HTTP	557	GET	/http2/tiles_final/tile_2.png	HTTP/1.1								
1240	9.806524	172.17.2.7	79.127.138.14	TCP	54	58849	→ 80	[ACK]	Seq=1	Ack=1	Win=65280	Len=0				
1241	9.806583	79.127.138.14	172.17.2.7	TCP	66	80	→ 59211	[SYN, ACK]	Seq=0	Ack=1	Win=64240	Len=0	MSS=1460	SACK_PERM	WS=512	
1242	9.806668	172.17.2.7	79.127.138.14	TCP	54	59211	→ 80	[ACK]	Seq=1	Ack=1	Win=65280	Len=0				
1243	9.807127	172.17.2.7	79.127.138.14	HTTP	557	GET	/http2/tiles_final/tile_3.png	HTTP/1.1								
1244	9.807409	172.17.2.7	79.127.138.14	HTTP	557	GET	/http2/tiles_final/tile_4.png	HTTP/1.1								
1246	9.809593	79.127.138.14	172.17.2.7	HTTP	419	HTTP/1.1	304	Not Modified								
1247	9.809593	79.127.138.14	172.17.2.7	TCP	66	80	→ 62464	[SYN, ACK]	Seq=0	Ack=1	Win=64240	Len=0	MSS=1460	SACK_PERM	WS=512	
1248	9.809593	79.127.138.14	172.17.2.7	TCP	66	80	→ 58270	[SYN, ACK]	Seq=0	Ack=1	Win=64240	Len=0	MSS=1460	SACK_PERM	WS=512	

> Frame 1178: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface \Device\NPF_{B4F47397-6371-47C2-9511-55F9A5017442} [Ethernet II, Src: GigaByteTech_2f:7f:ed (74:56:3c:2f:7f:ed), Dst: Stormshield_2a:a8:34 (00:0d:b4:2a:a8:34)]
 > Internet Protocol Version 4, Src: 172.17.2.7, Dst: 79.127.138.14
 > Transmission Control Protocol, Src Port: 63937, Dst Port: 80, Seq: 1, Ack: 1, Len: 0
 Source Port: 63937
 Destination Port: 80
 [Stream index: 31]
 > [Conversation completeness: Incomplete, DATA (15)]
 [TCP Segment Len: 0]
 Sequence Number: 1 (relative sequence number)
 Sequence Number (raw): 4255565004
 [Next Sequence Number: 1 (relative sequence number)]
 Acknowledgment Number: 1 (relative ack number)
 Acknowledgment number (raw): 1389167759
 0101 = Header Length: 20 bytes (5)
 > Flags: 0x010 (ACK)

```

0000 00 0d b4 2a a8 34 74 56 3c 2f 7f ed 00 00 45 00 ...*4tv</...E
0010 00 28 5c 7d 40 00 00 06 00 00 ac 11 02 07 4f 7f .(\)@... ..0
0020 8a 0e f9 c1 00 50 fd a6 c4 cc 52 cd 04 8f 50 1a .....P..R...4
0030 00 ff 87 c0 00 00
  
```

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 séquençement (dans l'ordre). Il garantit donc plus de sécurité dans le transport.

