

# TP3-Les ports logiciels

1. Connexion Bureau à distance (RPD).....	1
2. Capture de trames HTTP.....	5

## 1. Connexion Bureau à distance (RPD)

Le but de cette question est de réaliser une connexion à distance entre 2 machines à l'aide de l'IP

Réalisation de `netstat -n` pour afficher les numéros des ports

```
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 réalise après un IPconfig pour avoir les différents IP des différentes machines.

## TP3-Les ports logiciels

```
C:\Windows\System32>ipconfig

Configuration IP de Windows

Carte 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. . . . . :

Carte 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

Carte 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
    Passerelle par défaut. . . . . :
```

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

## 🔒 Pare-feu et protection du réseau

Personnes et systèmes pouvant accéder à vos réseaux.

### 🏢 Réseau avec domaine (actif)

Le pare-feu est activé.

### 🏠 Réseau privé

Le pare-feu est activé.

### 🌐 Réseau public

Le pare-feu est activé.

[Autoriser une application via le pare-feu](#)

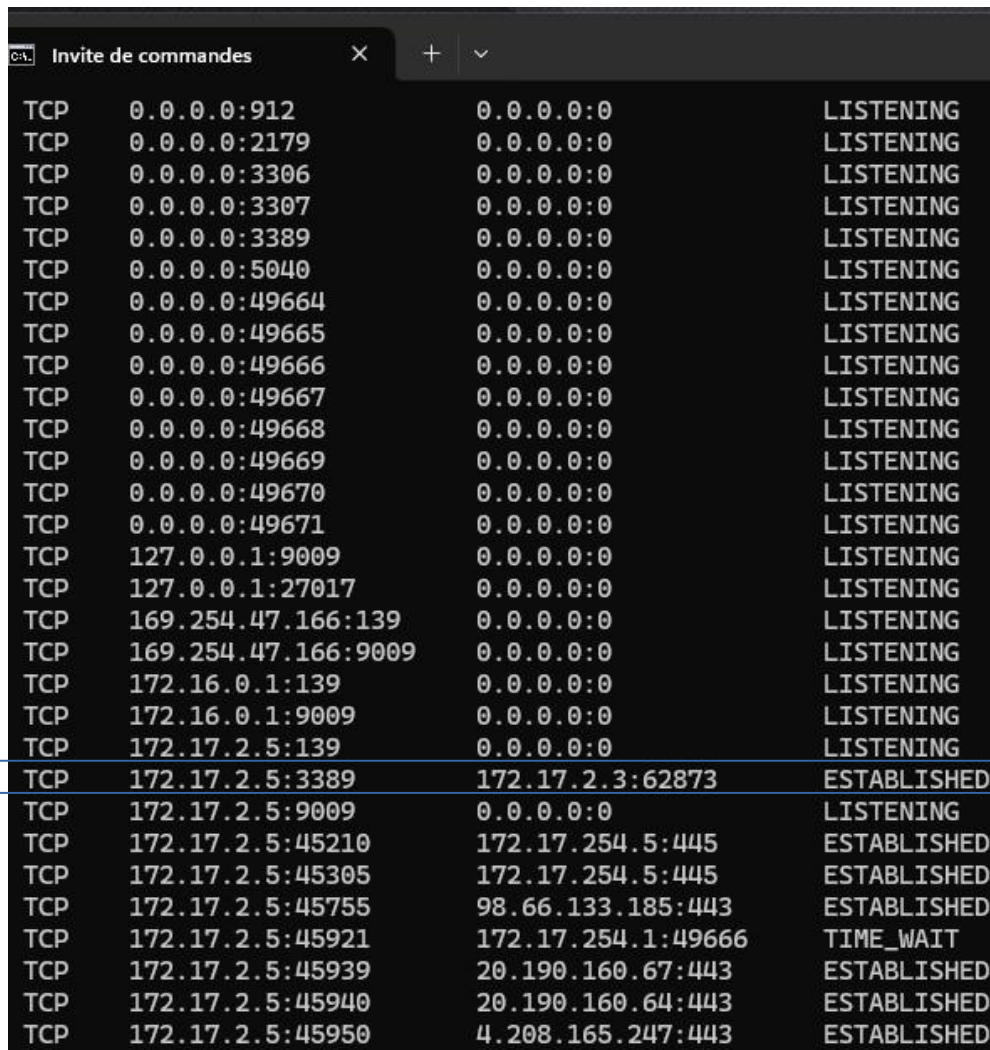
[Utilitaire de résolution des problèmes réseau et Internet](#)

[Paramètres de notification du pare-feu](#)

Système > Bureau à distance

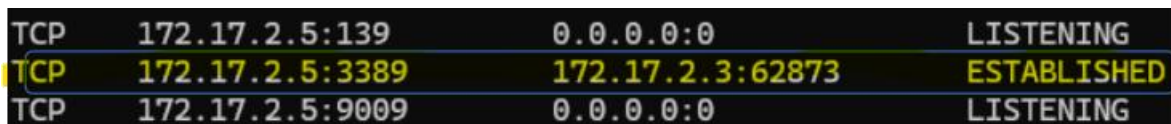
	<b>Bureau à distance</b> Connectez-vous à cet ordinateur et utilisez-le à partir d'un autre appareil à l'aide de l'application Bureau à distance	Activé 
	<b>Nom du PC</b> Utiliser ce nom pour se connecter à ce PC à partir d'un autre appareil	G102-GB07.prince.local
	<b>Utilisateurs du Bureau à distance</b> Sélectionner qui peut accéder à distance à ce PC	
<b>Support associé</b>		
	<b>Aide avec Bureau à distance</b>	
<a href="#">Connexion à votre PC à distance</a>		

## TP3-Les ports logiciels



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	0.0.0.0:49671	0.0.0.0:0	LISTENING
TCP	127.0.0.1:9009	0.0.0.0:0	LISTENING
TCP	127.0.0.1:27017	0.0.0.0:0	LISTENING
TCP	169.254.47.166:139	0.0.0.0:0	LISTENING
TCP	169.254.47.166:9009	0.0.0.0:0	LISTENING
TCP	172.16.0.1:139	0.0.0.0:0	LISTENING
TCP	172.16.0.1:9009	0.0.0.0:0	LISTENING
TCP	172.17.2.5:139	0.0.0.0:0	LISTENING
TCP	172.17.2.5:3389	172.17.2.3:62873	ESTABLISHED
TCP	172.17.2.5:9009	0.0.0.0:0	LISTENING
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	172.17.2.5:45921	172.17.254.1:49666	TIME_WAIT
TCP	172.17.2.5:45939	20.190.160.67:443	ESTABLISHED
TCP	172.17.2.5:45940	20.190.160.64:443	ESTABLISHED
TCP	172.17.2.5:45950	4.208.165.247:443	ESTABLISHED

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

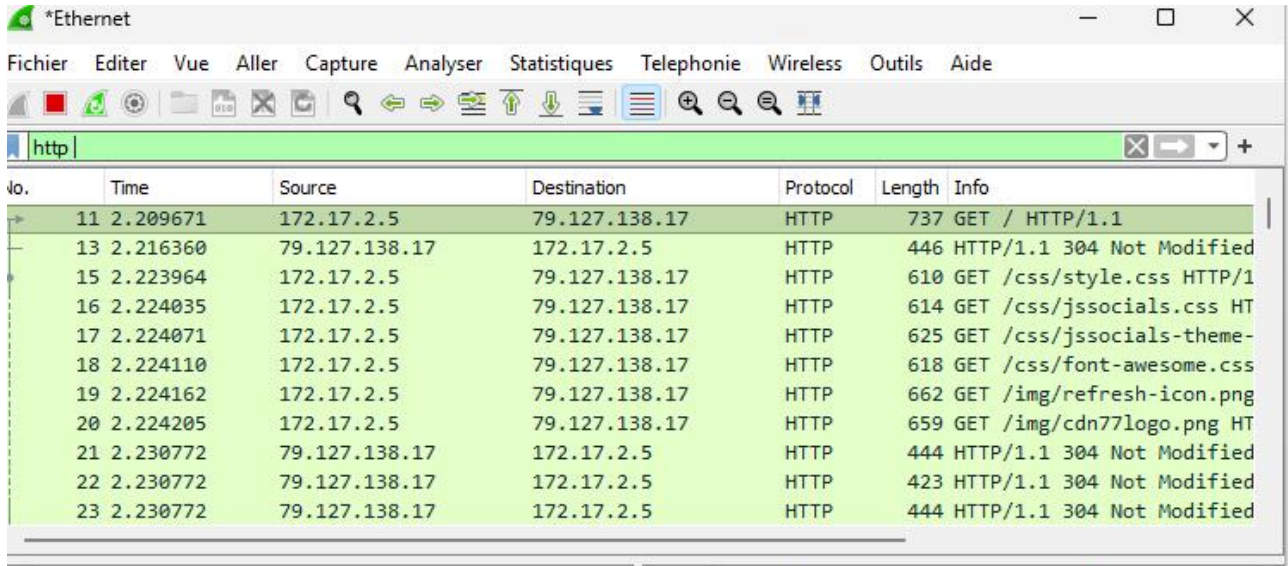


TCP	172.17.2.5:139	0.0.0.0:0	LISTENING
TCP	172.17.2.5:3389	172.17.2.3:62873	ESTABLISHED
TCP	172.17.2.5:9009	0.0.0.0:0	LISTENING

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

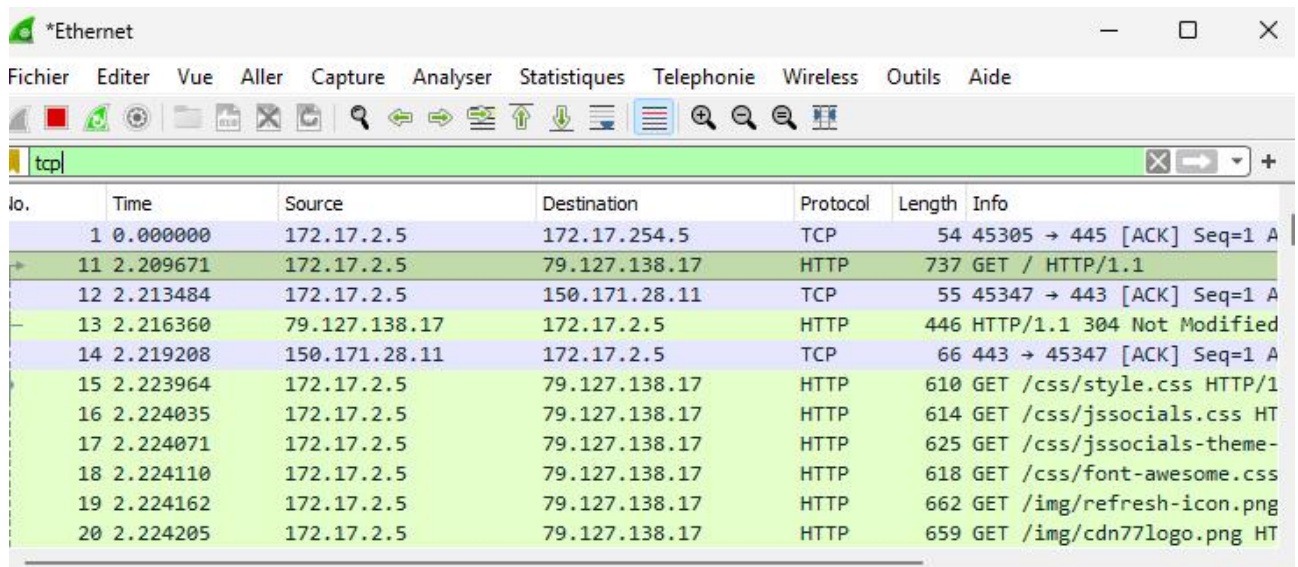
# TP3-Les ports logiciels

## 2. Capture de trames HTTP



The screenshot shows a Wireshark window titled '\*Ethernet' with the filter 'http' applied. The packet list pane displays 11 captured packets, all of which are HTTP requests. The first packet (no. 11) is a GET request for the root path. Subsequent packets (nos. 13-23) are GET requests for various CSS and image files. The 'Info' column for the first packet shows 'GET / HTTP/1.1'. The 'Info' column for the last three packets shows '304 Not Modified', indicating that the browser has cached the resources.

no.	Time	Source	Destination	Protocol	Length	Info
11	2.209671	172.17.2.5	79.127.138.17	HTTP	737	GET / HTTP/1.1
13	2.216360	79.127.138.17	172.17.2.5	HTTP	446	HTTP/1.1 304 Not Modified
15	2.223964	172.17.2.5	79.127.138.17	HTTP	610	GET /css/style.css HTTP/1
16	2.224035	172.17.2.5	79.127.138.17	HTTP	614	GET /css/jssocials.css HT
17	2.224071	172.17.2.5	79.127.138.17	HTTP	625	GET /css/jssocials-theme-
18	2.224110	172.17.2.5	79.127.138.17	HTTP	618	GET /css/font-awesome.css
19	2.224162	172.17.2.5	79.127.138.17	HTTP	662	GET /img/refresh-icon.png
20	2.224205	172.17.2.5	79.127.138.17	HTTP	659	GET /img/cdn77logo.png HT
21	2.230772	79.127.138.17	172.17.2.5	HTTP	444	HTTP/1.1 304 Not Modified
22	2.230772	79.127.138.17	172.17.2.5	HTTP	423	HTTP/1.1 304 Not Modified
23	2.230772	79.127.138.17	172.17.2.5	HTTP	444	HTTP/1.1 304 Not Modified



The screenshot shows a Wireshark window titled '\*Ethernet' with the filter 'tcp' applied. The packet list pane displays 11 captured packets. The first packet (no. 1) is a TCP ACK from 172.17.2.5 to 172.17.254.5. The second packet (no. 11) is an HTTP GET request. The third packet (no. 12) is a TCP ACK from 172.17.2.5 to 150.171.28.11. The fourth packet (no. 13) is an HTTP 304 Not Modified response. The fifth packet (no. 14) is a TCP ACK from 150.171.28.11 to 172.17.2.5. The remaining packets (nos. 15-20) are HTTP GET requests for various CSS and image files, similar to the first screenshot. The 'Info' column for the first packet shows '45305 → 445 [ACK] Seq=1 A'. The 'Info' column for the last three packets shows '304 Not Modified'.

no.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	172.17.2.5	172.17.254.5	TCP	54	45305 → 445 [ACK] Seq=1 A
11	2.209671	172.17.2.5	79.127.138.17	HTTP	737	GET / HTTP/1.1
12	2.213484	172.17.2.5	150.171.28.11	TCP	55	45347 → 443 [ACK] Seq=1 A
13	2.216360	79.127.138.17	172.17.2.5	HTTP	446	HTTP/1.1 304 Not Modified
14	2.219208	150.171.28.11	172.17.2.5	TCP	66	443 → 45347 [ACK] Seq=1 A
15	2.223964	172.17.2.5	79.127.138.17	HTTP	610	GET /css/style.css HTTP/1
16	2.224035	172.17.2.5	79.127.138.17	HTTP	614	GET /css/jssocials.css HT
17	2.224071	172.17.2.5	79.127.138.17	HTTP	625	GET /css/jssocials-theme-
18	2.224110	172.17.2.5	79.127.138.17	HTTP	618	GET /css/font-awesome.css
19	2.224162	172.17.2.5	79.127.138.17	HTTP	662	GET /img/refresh-icon.png
20	2.224205	172.17.2.5	79.127.138.17	HTTP	659	GET /img/cdn77logo.png HT

# TP3-Les ports logiciels

```
C:\> Invite de commandes

Microsoft Windows [version 10.0.26100.6584]
(c) Microsoft Corporation. Tous droits réservés.

C:\Users\Hsouri>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::31
           2a02:6ea0:dc00::32
           2a02:6ea0:dc00::30
           79.127.138.20
           79.127.138.15
           79.127.138.17
Aliases: www.http2demo.io
```

Adresse IP destination du site

The screenshot shows a Wireshark capture of an HTTP request. The packet list pane shows a GET request to 79.127.138.17. The packet details pane shows the request structure, including the Host, User-Agent, and Cookie headers. The packet bytes pane shows the raw data of the request.

No.	Time	Source	Destination	Protocol	Length	Info
59	6.884148	172.17.2.15	79.127.138.21	HTTP	730	GET / HTTP/1.1
62	6.890792	79.127.138.21	172.17.2.15	HTTP	446	HTTP/1.1 304 Not Modified
72	6.939089	79.127.138.21	79.127.138.21	HTTP	603	GET /css/style.css HTTP/1.1
73	6.939134	172.17.2.15	79.127.138.21	HTTP	607	GET /css/jssocials.css HTTP/1.1
74	6.939174	172.17.2.15	79.127.138.21	HTTP	618	GET /css/jssocials-theme-flat.css HTTP/1.1
75	6.939214	172.17.2.15	79.127.138.21	HTTP	611	GET /css/font-awesome.css HTTP/1.1
76	6.939253	172.17.2.15	79.127.138.21	HTTP	655	GET /img/refresh-icon.png HTTP/1.1
80	6.945604	79.127.138.21	172.17.2.15	HTTP	447	HTTP/1.1 304 Not Modified
81	6.946238	79.127.138.21	172.17.2.15	HTTP	448	HTTP/1.1 304 Not Modified
82	6.946238	79.127.138.21	172.17.2.15	HTTP	447	HTTP/1.1 304 Not Modified
83	6.946238	79.127.138.21	172.17.2.15	HTTP	421	HTTP/1.1 304 Not Modified
84	6.946311	172.17.2.15	79.127.138.21	HTTP	652	GET /img/cdn77logo.png HTTP/1.1
85	6.947174	172.17.2.15	79.127.138.21	HTTP	656	GET /img/logo-108bpsio.png HTTP/1.1
86	6.947328	172.17.2.15	79.127.138.21	HTTP	595	GET /js/jssocials.min.js HTTP/1.1
91	6.952786	79.127.138.21	172.17.2.15	HTTP	421	HTTP/1.1 304 Not Modified
93	6.953708	79.127.138.21	172.17.2.15	HTTP	423	HTTP/1.1 304 Not Modified
94	6.954228	79.127.138.21	172.17.2.15	HTTP	448	HTTP/1.1 304 Not Modified
95	6.954807	172.17.2.15	79.127.138.21	HTTP	625	GET /http2/http1.html HTTP/1.1
99	6.961715	79.127.138.21	172.17.2.15	HTTP	443	HTTP/1.1 304 Not Modified
105	6.996936	172.17.2.15	79.127.138.21	HTTP	558	GET /http2/tiles_final/tile_0.png HTTP/1.1
106	6.997088	172.17.2.15	79.127.138.21	HTTP	557	GET /http2/tiles_final/tile_2.png HTTP/1.1
107	6.997137	172.17.2.15	79.127.138.21	HTTP	557	GET /http2/tiles_final/tile_3.png HTTP/1.1
108	6.997386	172.17.2.15	79.127.138.21	HTTP	557	GET /http2/tiles_final/tile_4.png HTTP/1.1
109	6.997505	172.17.2.15	79.127.138.21	HTTP	557	GET /http2/tiles_final/tile_5.png HTTP/1.1
110	6.997551	172.17.2.15	79.127.138.21	HTTP	557	GET /http2/tiles_final/tile_6.png HTTP/1.1

Frame 59: 730 bytes on wire (5840 bits), 730 bytes captured (5840 bits) on interface \Device\NPF\_{6152A9F5-3F79-4149-9629-CC2A7042CA} Ethernet II, Src: GigabyteTech\_2f:9c:fc (74:56:3c:2f:9c:fc), Dst: Stormshield\_2a:a8:34 (08:0d:b4:2a:a8:34)  
> Internet Protocol Version 4, Src: 172.17.2.15, Dst: 79.127.138.21  
> Transmission Control Protocol, Src Port: 62123, Dst Port: 80, Seq: 1, Ack: 1, Len: 676  
> Hypertext Transfer Protocol  
 > GET / HTTP/1.1\r\n  
 Host: www.http2demo.io\r\n Connection: keep-alive\r\n Cache-Control: max-age=0\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/148.0.0.0 Safari/537.36 Edg/14  
 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,\*/\*;q=0.8,application/signed-exchange;v=b3;q=0.7\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 Cookie: \_ga=GA1.2.1194327926.1759307952; \_gid=GA1.2.1884510988.1759307952; \_ga\_RCV9w956D1=GS2.2.s1759307951s01\$g1\$t1759307955j365\r\n If-None-Match: W/"5a891b6d-19b00"\r\n \r\n [Response in frame: 62]  
 [Full request URI: http://www.http2demo.io/]

# TP3-Les ports logiciels

The screenshot displays a network traffic capture in Wireshark. The top pane shows a list of HTTP requests from 172.17.2.15 to 79.127.138.21. The bottom pane shows a detailed view of a TCP segment (No. 120) with the following metadata:

- Protocol: Transmission Control Protocol, Src Port: 62123, Dst Port: 80
- Source Port: 62123
- Destination Port: 80
- [Stream index: 1]
- [Stream Packet Number: 1]
- [Conversation completeness: Incomplete (12)]
- [TCP Segment Len: 676]
- Sequence Number: 1 (relative sequence number)
- Sequence Number (raw): 1201400224
- [Next Sequence Number: 677 (relative sequence number)]
- Acknowledgment Number: 1 (relative ack number)
- Acknowledgment number (raw): 3975567314
- 0101 .... = Header Length: 20 bytes (5)
- Flags: 0x018 (PSH, ACK)
- Window: 2050
- [Calculated window size: 2050]
- [Window size scaling factor: -1 (unknown)]
- Checksum: 0x8a73 [unverified]
- [Checksum Status: Unverified]
- Urgent Pointer: 0

The packet bytes pane shows the raw data in hexadecimal and ASCII format, starting with 0020 8a 15 f2 ab 00 50 47 9b e9 a0 ec f6 57 d2 50 18.

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

## TP3-Les ports logiciels

No.	Time	Source	Destination	Protocol	Length	Info
69	4.277089	172.17.2.15	79.127.138.21	HTTP	738	GET / HTTP/1.1
71	4.284492	79.127.138.21	172.17.2.15	HTTP	446	HTTP/1.1 304 Not Modified
75	4.302713	172.17.2.15	79.127.138.21	HTTP	611	GET /css/style.css
76	4.302760	172.17.2.15	79.127.138.21	HTTP	615	GET /css/jssocials
77	4.302800	172.17.2.15	79.127.138.21	HTTP	626	GET /css/jssocials
78	4.302839	172.17.2.15	79.127.138.21	HTTP	619	GET /css/font-awes
79	4.302879	172.17.2.15	79.127.138.21	HTTP	663	GET /img/refresh-ic
80	4.310188	79.127.138.21	172.17.2.15	HTTP	447	HTTP/1.1 304 Not Modified
82	4.310188	79.127.138.21	172.17.2.15	HTTP	421	HTTP/1.1 304 Not Modified
84	4.310896	79.127.138.21	172.17.2.15	HTTP	448	HTTP/1.1 304 Not Modified
85	4.311490	172.17.2.15	79.127.138.21	HTTP	660	GET /img/cdn77logo
86	4.311998	172.17.2.15	79.127.138.21	HTTP	664	GET /img/logo-10gb

Transmission Control Protocol, Src Port: 62422,	0020	8a 15 f3 d6	00 50	f1 07	aa 21 14 b8 27 59
Source Port: 62422	0030	04 01 8a 7b	00 00 47 45	54 20 2f 20 48 54	
Destination Port: 80	0040	2f 31 2e 31	0d 0a 48 6f	73 74 3a 20 77 77	
[Stream index: 4]	0050	68 74 74 70	32 64 65 6d	6f 2e 69 6f 0d 0a	
[Stream Packet Number: 1]	0060	6e 6e 65 63	74 69 6f 6e	3a 20 6b 65 65 70	
[Conversation completeness: Incomplete (12)]	0070	6c 69 76 65	0d 0a 43 61	63 68 65 2d 43 6f	
[TCP Segment Len: 684]	0080	72 6f 6c 3a	20 6d 61 78	2d 61 67 65 3d 30	
Sequence Number: 1 (relative sequence num	0090	55 70 67 72	61 64 65 2d	49 6e 73 65 63 75	
Sequence Number (raw): 4043811361	00a0	2d 52 65 71	75 65 73 74	73 3a 20 31 0d 0a	
[Next Sequence Number: 685 (relative sequ	00b0	65 72 2d 41	67 65 6e 74	3a 20 4d 6f 7a 69	
Acknowledgment Number: 1 (relative ack nu	00c0	61 2f 35 2e	30 20 28 57	69 6e 64 6f 77 73	
Acknowledgment number (raw): 347613017	00d0	54 20 31 30	2e 30 3b 20	57 69 6e 36 34 3b	
0101 .... = Header Length: 20 bytes (5)	00e0	36 34 29 20	41 70 70 6c	65 57 65 62 4b 69	
Flags: 0x018 (PSH, ACK)	00f0	35 33 37 2e	33 36 20 28	4b 48 54 4d 4c 2c	

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

The screenshot shows a Wireshark interface with a packet list and a packet details pane. The packet list shows several TCP packets. Packet 64 is selected, and its details are expanded to show the Internet Protocol Version 4 header and the Transmission Control Protocol (TCP) header. The TCP header shows the protocol number as 6, which is highlighted in a red box. The source and destination ports are also visible in the details pane.

No.	Time	Source	Destination	Protoc	Length	Info
13	0.031982	204.79.197.254	172.17.2.15	TCP	60	443 → 62444 [ACK] Seq=636 Ack=485 Win=16382 L
16	0.034502	172.17.2.15	204.79.197.254	TCP	54	62444 → 443 [ACK] Seq=485 Ack=861 Win=1019 Le
18	0.064181	204.79.197.222	172.17.2.15	TCP	60	443 → 62418 [ACK] Seq=1 Ack=638 Win=16382 Le
20	0.065654	172.17.2.15	204.79.197.222	TCP	54	62418 → 443 [ACK] Seq=638 Ack=148 Win=1021 Le
22	0.065688	172.17.2.15	204.79.197.222	TCP	54	62418 → 443 [ACK] Seq=638 Ack=179 Win=1021 Le
63	4.264984	172.17.2.15	79.127.138.21	TCP	54	62421 → 80 [FIN, ACK] Seq=1 Ack=1 Win=1026 Le
64	4.265061	172.17.2.15	2.16.165.155	TCP	54	62420 → 443 [FIN, ACK] Seq=1 Ack=1 Win=1024 L
66	4.270662	79.127.138.21	172.17.2.15	TCP	60	80 → 62421 [ACK] Seq=1 Ack=2 Win=126 Len=0
70	4.280766	2.16.165.155	172.17.2.15	TCP	60	443 → 62420 [ACK] Seq=1 Ack=2 Win=501 Len=0
74	4.302613	172.17.2.15	79.127.138.21	TCP	66	62445 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=14
81	4.310188	79.127.138.21	172.17.2.15	TCP	66	80 → 62445 [SYN, ACK] Seq=0 Ack=1 Win=64240 L
83	4.310377	172.17.2.15	79.127.138.21	TCP	54	62445 → 80 [ACK] Seq=1 Ack=1 Win=262656 Len=0
92	4.318896	79.127.138.21	172.17.2.15	TCP	60	80 → 62445 [ACK] Seq=1 Ack=607 Win=64512 Len=
98	4.328293	172.17.2.15	48.209.162.134	TCP	66	62446 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=
108	4.360667	172.17.2.15	79.127.138.21	TCP	54	62426 → 80 [ACK] Seq=1176 Ack=764 Win=1022 Le
109	4.360667	172.17.2.15	79.127.138.21	TCP	54	62422 → 80 [ACK] Seq=1242 Ack=786 Win=1022 Le
110	4.360667	172.17.2.15	79.127.138.21	TCP	54	62424 → 80 [ACK] Seq=1159 Ack=762 Win=1022 Le
117	4.363723	48.209.162.134	172.17.2.15	TCP	66	443 → 62446 [SYN, ACK] Seq=0 Ack=1 Win=64240

```
Frame 64: Packet, 54 bytes on wire (432 bits), 54 bytes captured on interface 0:000000000000 on interface 0:000000000000
Ethernet II, Src: GigaByteTech 2f:9c:fc (74:56:3c:2f:9c:fc), Dst: 02:10:a5:9b:00:00
Internet Protocol Version 4, Src: 172.17.2.15, Dst: 2.16.165.155
  0100 .... = Version: 4
  ... 0101 = Header Length: 20 bytes (5)
  Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
  Total Length: 40
  Identification: 0x3758 (14168)
  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: 172.17.2.15
  Destination Address: 2.16.165.155
  [Stream index: 12]
  Transmission Control Protocol, Src Port: 62420, Dst Port: 443, Seq: 62420, Len: 54
```

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

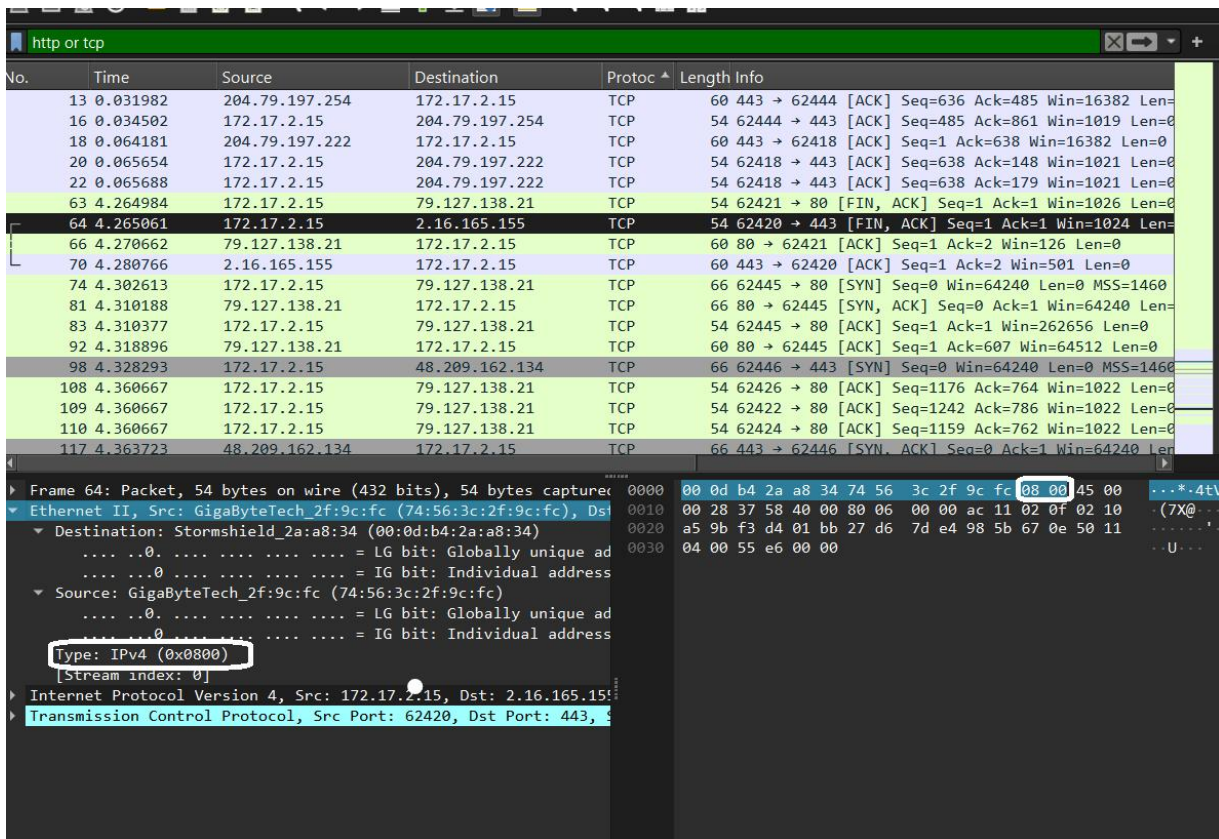
Quelles sont les valeurs décimales et hexadécimales des adresses IP source et destination ?

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

Premièrement le SYN = client émet un segment (synchronisation)

Deuxièmement 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