

---

---

# TP3 Les ports logiciels

## Table des matières







1. Connexion sécurisée à une machine Linux depuis un client SSH Windows.....	2
2. Connexion Bureau à distance (RDP).....	2
3. Capture de trames HTTP.....	2

---

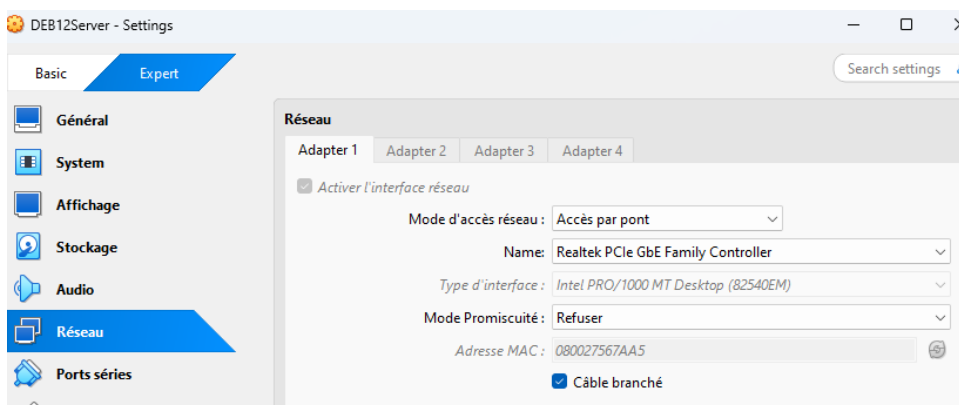
---

# 1. Connexion sécurisée à une machine Linux depuis un client SSH Windows.

Téléchargez et installez, depuis votre machine hôte, putty.exe 64 bits (putty.org).

 Pageant	15/10/2024 17:04	Raccourci	1 Ko
 PSFTP	15/10/2024 17:04	Raccourci	1 Ko
 PuTTY Manual	15/10/2024 17:04	Raccourci	1 Ko
 PuTTY Web Site	15/10/2024 17:04	Raccourci	1 Ko
 PuTTY	15/10/2024 17:04	Raccourci	2 Ko
 PuTTYgen	15/10/2024 17:04	Raccourci	1 Ko

Vérifiez que la carte réseau de la VM DEB12Server soit en accès par pont et que la configuration IP soit prévue pour être obtenue automatiquement auprès du serveur DHCP ROI (cf. TP2 B1 pages 6 et 7). Vérifiez, avec la commande ip address, l'obtention des paramètres (adresse IP 172 .17.X.Y) (capture d'écran à réaliser)



```
root@deb12server: ~# ip -c 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 noprefixroute
        valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:56:7a:a5 brd ff:ff:ff:ff:ff:ff
    inet 172.17.110.19/16 brd 172.17.255.255 scope global dynamic enp0s3
        valid_lft 85305sec preferred_lft 85305sec
    inet6 fe80::a00:27ff:fe56:7aa5/64 scope link
        valid_lft forever preferred_lft forever
root@deb12server: ~#_
```

---

Vérifiez les paramètres IP de la carte réseau de votre machine physique à l'aide de la commande ipconfig /all depuis une invite de commandes (capture d'écran à réaliser) : les deux machines doivent être dans le même réseau IP

```
C:\Users\avandesquille>ipconfig

Configuration IP de Windows

Carte Ethernet vEthernet (Default Switch) :

    Suffixe DNS propre à la connexion. . . :
    Adresse IPv6 de liaison locale. . . . . : fe80::8fae:3686:817f:fc09%10
    Adresse IPv4. . . . . : 172.24.16.1
    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::d8f6:5b6a:7e91:c3c2%4
    Adresse IPv4. . . . . : 172.17.2.3
    Masque de sous-réseau. . . . . : 255.255.0.0
    Passerelle par défaut. . . . . : 172.17.250.2
```

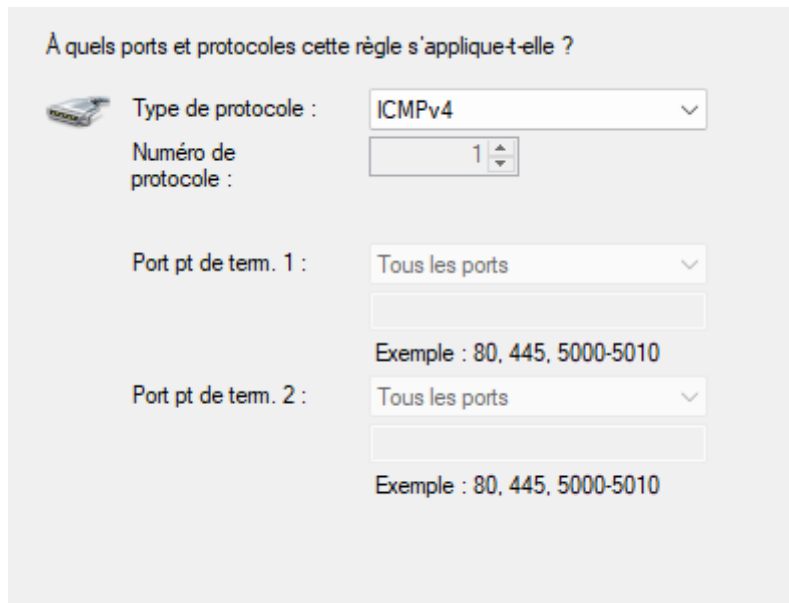
Je vérifie la connectivité entre les deux machines à l'aide d'un ping effectué depuis votre machine Linux (capture d'écran à réaliser). (l'adresse ip de ma machine physique est : 172.17.2.3

```
root@deb12server: ~#ping 172.17.2.3
PING 172.17.2.3 (172.17.2.3) 56(84) bytes of data.
64 bytes from 172.17.2.3: icmp_seq=1 ttl=128 time=0.912 ms
64 bytes from 172.17.2.3: icmp_seq=2 ttl=128 time=0.430 ms
64 bytes from 172.17.2.3: icmp_seq=3 ttl=128 time=0.355 ms
64 bytes from 172.17.2.3: icmp_seq=4 ttl=128 time=0.433 ms
^C
--- 172.17.2.3 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3077ms
rtt min/avg/max/mdev = 0.355/0.532/0.912/0.221 ms
```

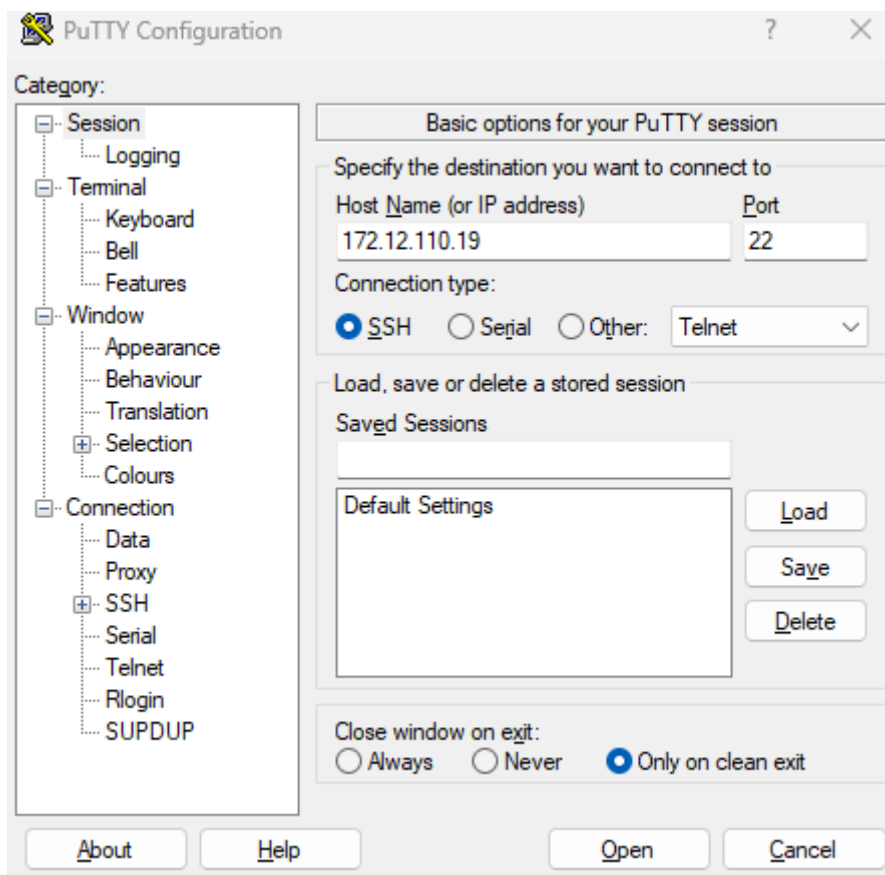
---

---

voici ma règle personnalisée permettant d'autoriser les trames ICMP à entrer

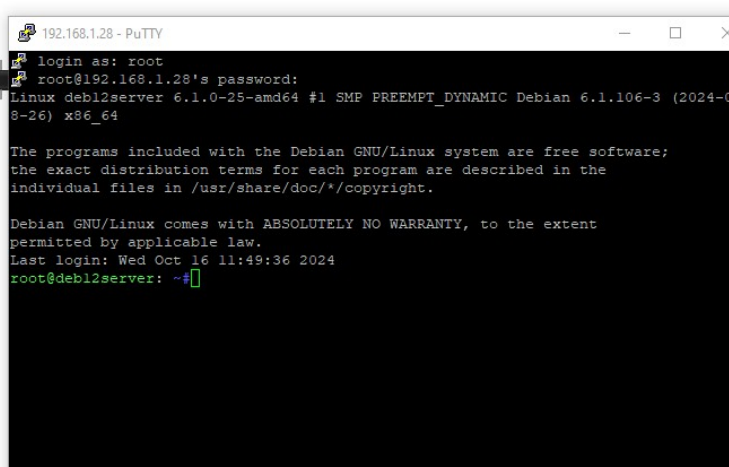


Lancez PuTTY depuis votre machine Windows (client SSH) et saisissez l'adresse IP de votre VM DEB12Server (serveur SSH) dans le champ Host Name, sélectionnez SSH puis cliquez sur Open :



---

puis à partir de Putty j'ai accédé à mon serveur

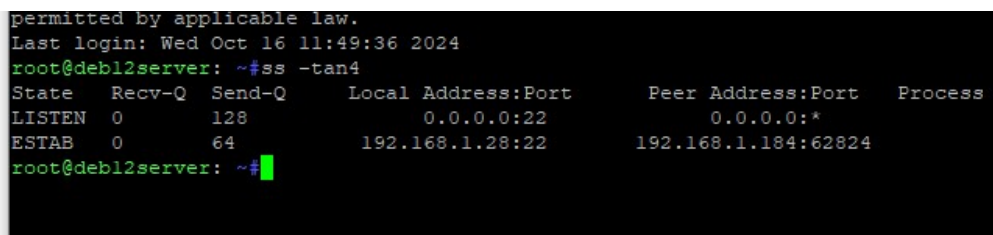


```
192.168.1.28 - PuTTY
login as: root
root@192.168.1.28's password:
Linux deb12server 6.1.0-25-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.106-3 (2024-08-26) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Wed Oct 16 11:49:36 2024
root@deb12server: ~#
```

▪ Dans cette console, saisissez la commande `ss -tan4` (cf. TP2 B1). Montrez sur la capture d'écran que la connexion SSH est établie.



```
permitted by applicable law.
Last login: Wed Oct 16 11:49:36 2024
root@deb12server: ~#ss -tan4
State Recv-Q Send-Q Local Address:Port Peer Address:Port Process
LISTEN 0 128 0.0.0.0:22 0.0.0.0:*
ESTAB 0 64 192.168.1.28:22 192.168.1.184:62824
root@deb12server: ~#
```

- Sur quel port écoute le service sshd du serveur SSH DEB12Server ? Le port 22
- Quel est le port dynamique assigné par le système d'exploitation Windows au client SSH durant la connexion TCP afin qu'il puisse écouter sur ce port et recevoir les réponses du serveur SSH DEB12Server ? Le port dynamique est le port 62824

- Ne fermez pas la session SSH. Ouvrez une invite de commande sur la machine Windows et saisissez la commande netstat (connexions TCP actives) puis netstat -an (connexions TCP actives et ports d'écoute). Montrez sur la capture d'écran que la connexion SSH est établie.

```

C:\Users\axel1>netstat

Connexions actives

    Proto Adresse locale      Adresse distante    État
    ---  ---
    TCP   127.0.0.1:49674     DESKTOP-M8V8CNS:64805 ESTABLISHED
    TCP   127.0.0.1:59822     DESKTOP-M8V8CNS:59850 ESTABLISHED
    TCP   127.0.0.1:59826     DESKTOP-M8V8CNS:59849 ESTABLISHED
    TCP   127.0.0.1:59849     DESKTOP-M8V8CNS:59826 ESTABLISHED
    TCP   127.0.0.1:59850     DESKTOP-M8V8CNS:59822 ESTABLISHED
    TCP   127.0.0.1:64805     DESKTOP-M8V8CNS:49674 ESTABLISHED
    TCP   192.168.1.184:55373 41:https            ESTABLISHED
^C
C:\Users\axel1>netstat -an

```

- Pour vous déconnecter de la session SSH depuis la console Linux, tapez logout ou utilisez la combinaison des touches Ctrl+D.

```

C:\Users\axel1>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   0.0.0.0:5040        0.0.0.0:0          LISTENING
    TCP   0.0.0.0:5357        0.0.0.0:0          LISTENING
    TCP   0.0.0.0:5426        0.0.0.0:0          LISTENING
    TCP   0.0.0.0:7680        0.0.0.0:0          LISTENING
    TCP   0.0.0.0:27036       0.0.0.0:0          LISTENING
    TCP   0.0.0.0:28190       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   0.0.0.0:49671       0.0.0.0:0          LISTENING
    TCP   0.0.0.0:49678       0.0.0.0:0          LISTENING
    TCP   0.0.0.0:54235       0.0.0.0:0          LISTENING
    TCP   0.0.0.0:54288       0.0.0.0:0          LISTENING
    TCP   0.0.0.0:57621       0.0.0.0:0          LISTENING
    TCP   0.0.0.0:64819       0.0.0.0:0          LISTENING
    TCP   127.0.0.1:1337      0.0.0.0:0          LISTENING
    TCP   127.0.0.1:6463      0.0.0.0:0          LISTENING
    TCP   127.0.0.1:13331     0.0.0.0:0          LISTENING
    TCP   127.0.0.1:13333     0.0.0.0:0          LISTENING
    TCP   127.0.0.1:13344     0.0.0.0:0          LISTENING
    TCP   127.0.0.1:24830     0.0.0.0:0          LISTENING
    TCP   127.0.0.1:27060     0.0.0.0:0          LISTENING
    TCP   127.0.0.1:28189     0.0.0.0:0          LISTENING
    TCP   127.0.0.1:49674     0.0.0.0:0          LISTENING
    TCP   127.0.0.1:49674     127.0.0.1:64805    ESTABLISHED
    TCP   127.0.0.1:55000     0.0.0.0:0          LISTENING
    TCP   127.0.0.1:59804     0.0.0.0:0          LISTENING
    TCP   127.0.0.1:59822     0.0.0.0:0          LISTENING
    TCP   127.0.0.1:59822     127.0.0.1:59850    ESTABLISHED
    TCP   127.0.0.1:59826     0.0.0.0:0          LISTENING
    TCP   127.0.0.1:59826     127.0.0.1:59849    ESTABLISHED
    TCP   127.0.0.1:59849     127.0.0.1:59826    ESTABLISHED
    TCP   127.0.0.1:59850     127.0.0.1:59822    ESTABLISHED
    TCP   127.0.0.1:64805     127.0.0.1:49674    ESTABLISHED
    TCP   127.0.0.1:65444     0.0.0.0:0          LISTENING
    TCP   192.168.1.184:139   0.0.0.0:0          LISTENING
    TCP   192.168.1.184:55373 35.186.224.41:443  ESTABLISHED
    TCP   192.168.1.184:57407 104.18.29.130:443  ESTABLISHED
    TCP   192.168.1.184:60589 155.133.248.43:443 ESTABLISHED
    TCP   192.168.1.184:61871 44.218.14.96:443   ESTABLISHED
    TCP   192.168.1.184:62453 104.199.65.9:4070  ESTABLISHED
    TCP   192.168.1.184:62459 162.159.133.234:443 ESTABLISHED
    TCP   192.168.1.184:62824 192.168.1.28:22    ESTABLISHED
    TCP   192.168.1.184:62921 35.169.218.226:443 ESTABLISHED
    TCP   192.168.1.184:62997 104.18.12.46:80    TIME_WAIT
    TCP   192.168.1.184:62998 104.18.12.46:80    TIME_WAIT
    TCP   192.168.1.184:62999 104.18.12.46:80    TIME_WAIT
    TCP   192.168.1.184:63000 104.18.12.46:80    TIME_WAIT
    TCP   192.168.1.184:63002 104.18.12.46:80    TIME_WAIT
    TCP   192.168.1.184:63003 104.18.12.46:80    TIME_WAIT
    TCP   192.168.1.184:63004 104.18.12.46:80    TIME_WAIT
    TCP   192.168.1.184:63005 104.18.12.46:80    TIME_WAIT
    TCP   192.168.1.184:63006 104.18.12.46:80    TIME_WAIT

```

---

---

## 2. Connexion Bureau à distance (RDP).

L'adresse ip de mon voisin est 172.17.2.21

-Assurez-vous de la connectivité entre votre machine physique et la sienne : réalisez un ping de sa station depuis votre machine physique (capture d'écran). Pensez aux règles de Pare-feu des deux machines.

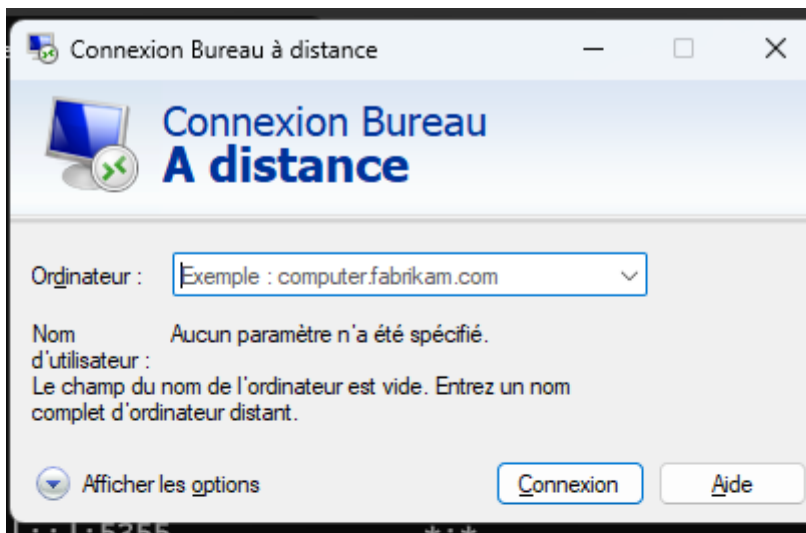
```
Statistiques Ping pour 172.17.2.21:
  Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
  Minimum = 0ms, Maximum = 0ms, Moyenne = 0ms
C:\Users\axandesquille>
```

Saisissez la commande netstat -an depuis l'invite de commandes de votre station Windows :

```
TCP 0.0.0.0:3389 0.0.0.0:0 LISTENING
```

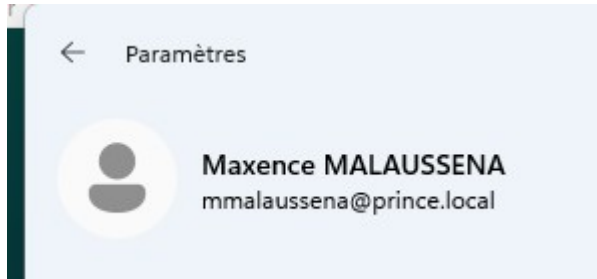
Quel est le port d'écoute du serveur Terminal Server ? 3389

voici ce que qu'on m'affiche grace à la commande mstsc



---

Saisissez l'adresse IP de la station de votre voisin qui a également autorisé les connexions à distance à son ordinateur, cliquez sur Connexion puis saisissez le mot de passe de l'administrateur du serveur distant (utilisez votre compte de domaine qui est membre du groupe 1sio lui-même membre du groupe local Administrateurs de chaque machine inscrite dans le domaine Prince)



Saisissez la commande netstat -an depuis l'invite de commande de la station de votre voisin via le bureau à distance. Vous constatez que la connexion au serveur Terminal Server est établie :

```
Minimum = 0ms, Maximum = 0ms, Moyenne = 0ms
C:\Users\mmalaussena>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 0.0.0.0:2179 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 0.0.0.0:7680 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 0.0.0.0:49672 0.0.0.0:0 LISTENING
TCP 127.0.0.1:27017 0.0.0.0:0 LISTENING
TCP 172.17.2.21:139 0.0.0.0:0 LISTENING
TCP 172.17.2.21:3389 172.17.2.23:63676 ESTABLISHED
TCP 172.17.2.21:7680 172.17.2.16:50305 TIME_WAIT
```

### 3. Capture de trames HTTP.

j'ouvre votre navigateur internet et affichez la page d'accueil du site <http://www.http2demo.io/>.

la capture est arrêté et un filtre est appliqué pour n'afficher que les trames http et TCP qui nous intéressent. Spécifiez par exemple l'adresse IP du serveur http. Retrouvez cette adresse IP comme indiqué ci-dessous

l'adresse ip est 195.181.175.40

The screenshot shows a Wireshark capture of network traffic. The top pane displays a list of packets. Packet 118 is highlighted, showing an HTTP GET request from 172.17.2.23 to 195.181.175.40. The middle pane shows the details of this packet, including the Hypertext Transfer Protocol section with fields like Host, User-Agent, and Accept-encoding. The bottom pane shows the raw packet data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	172.17.110.20	172.17.110.18	TCP	66	50569 → 7680 [SYN] Seq=0 Win=64240 Len=0 MSS=1460
2	0.000395	172.17.110.18	172.17.110.20	TCP	60	7680 → 50569 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
108	0.503462	172.17.110.20	172.17.110.18	TCP	66	[TCP Retransmission] [TCP Port numbers reused] 50569 → 7680 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
110	0.503883	172.17.110.18	172.17.110.20	TCP	60	7680 → 50569 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
118	0.666398	172.17.2.23	195.181.175.40	HTTP	737	GET / HTTP/1.1
126	1.023589	195.181.175.40	172.17.2.23	HTTP	430	HTTP/1.1 304 Not Modified
128	1.029091	172.17.2.23	195.181.175.40	HTTP	601	GET /css/style.css HTTP/1.1
129	1.029192	172.17.2.23	195.181.175.40	HTTP	605	GET /css/jssocials.css HTTP/1.1
130	1.029256	172.17.2.23	195.181.175.40	HTTP	616	GET /css/jssocials-theme-flat.css HTTP/1.1
131	1.029339	172.17.2.23	195.181.175.40	HTTP	609	GET /css/font-awesome.css HTTP/1.1
132	1.029372	172.17.2.23	195.181.175.40	HTTP	653	GET /img/refresh-icon.png HTTP/1.1
133	1.029400	172.17.2.23	195.181.175.40	HTTP	650	GET /img/cdn77logo.png HTTP/1.1
138	1.042688	172.17.2.23	195.181.172.3	HTTP	625	GET /http2/http1.html HTTP/1.1
139	1.094599	172.17.110.20	172.17.110.18	TCP	66	[TCP Retransmission] [TCP Port numbers reused] 50569 → 7680 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
140	1.094833	172.17.110.18	172.17.110.20	TCP	60	7680 → 50569 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
141	1.383849	172.17.2.23	195.181.175.40	TCP	650	[TCP Retransmission] 64612 → 80 [PSH, ACK] Seq=1 Ack=597 Win=0 Len=0
147	1.450608	172.17.2.23	195.181.175.40	TCP	605	[TCP Retransmission] 64614 → 80 [PSH, ACK] Seq=1 Ack=597 Win=0 Len=0
148	1.473302	172.17.2.23	195.181.172.3	TCP	625	[TCP Retransmission] 64618 → 80 [PSH, ACK] Seq=1 Ack=597 Win=0 Len=0
149	1.487179	195.181.175.40	172.17.2.23	HTTP	429	HTTP/1.1 304 Not Modified
150	1.487425	195.181.175.40	172.17.2.23	HTTP	429	HTTP/1.1 304 Not Modified
151	1.487658	195.181.175.40	172.17.2.23	HTTP	384	HTTP/1.1 304 Not Modified
152	1.487742	195.181.175.40	172.17.2.23	HTTP	430	HTTP/1.1 304 Not Modified
153	1.487932	195.181.175.40	172.17.2.23	HTTP	405	HTTP/1.1 304 Not Modified
154	1.489345	195.181.175.40	172.17.2.23	TCP	60	80 → 64612 [ACK] Seq=1 Ack=597 Win=126 Len=0

Frame 118: 737 bytes on wire (5896 bits), 737 bytes captured (5896 bits) on interface eth0

Ethernet II, Src: Giga-Byt\_2f:81:71 (74:56:3c:2f:81:71), Dst: Cisco-C3745... (74:4f:65:4c:00:00)

Internet Protocol Version 4, Src: 172.17.2.23, Dst: 195.181.175.40

Transmission Control Protocol, Src Port: 64613, Dst Port: 80, Seq: 64613, Len: 737

Hypertext Transfer Protocol

- GET / HTTP/1.1\r\n
- Host: www.http2demo.io\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/62.0.3202.62 Safari/537.36\r\n
- Accept: text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q=0.8\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
- Cookie: \_ga=GA1.2.150416580.1729177803; \_gid=GA1.2.744134529.1729177803\r\n
- If-None-Match: W/"5aa91b6d-19b00"\r\n\r\n

[Full request URI: <http://www.http2demo.io/>]

[HTTP request 1/2]

[Response in frame: 126]

[Next request in frame: 128]

Paquets : 909 · Affichés : 492 (54.1%) · Perdus : 0 (0.0%) · Profil : Default

---

---

Je Saisi, depuis l'invite de commandes, la commande nslookup www.http2demo.io pour obtenir l'adresse IP du serveur web

```
C:\Users\avandesquille>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:c700::21
           2a02:6ea0:c700::112
           2a02:6ea0:c700::19
           2a02:6ea0:c700::107
           2a02:6ea0:c700::101
           2a02:6ea0:c700::18
           2a02:6ea0:c700::11
           37.19.194.81
           169.150.255.183
           169.150.255.180
           195.181.170.19
           195.181.175.41
           212.102.56.179
           207.211.211.27
Aliases: www.http2demo.io
```

## la trame correspondant à votre requête http données applicative

> Frame 118: 737 bytes on wire (5896 bits), 737 bytes captured (5896 bits) on interface \Device\NPF_{8A3505B0-8D86-4B72-8AC4-B98FFB2F}	0030 01 fb 90 af 00 00 47 45 54 20 2f 20 48 54 54 50
> Ethernet II, Src: Giga-Byt_2f:81:71 (74:56:3c:2f:81:71), Dst: Cisco_97:2c:56 (00:1f:ca:97:2c:56)	0040 2f 31 2e 31 0d 0a 48 6f 73 74 3a 20 77 77 77 2e
> Internet Protocol Version 4, Src: 172.17.2.23, Dst: 195.181.175.40	0050 68 74 74 70 32 64 65 6d 6f 2e 69 6f 0d 0a 43 6f
> Transmission Control Protocol, Src Port: 64613, Dst Port: 80, Seq: 1, Ack: 1, Len: 683	0060 6e 6e 65 63 74 69 6f 6e 3a 20 6b 65 65 70 2d 61
> Hypertext Transfer Protocol	0070 6c 69 76 65 0d 0a 55 70 67 72 61 64 65 2d 49 6e
> GET / HTTP/1.1\r\n	0080 73 65 63 75 72 65 2d 52 65 71 75 65 73 74 73 3a
Host: www.http2demo.io\r\n	0090 20 31 0d 0a 55 73 65 72 2d 41 67 65 6e 74 3a 20
Connection: keep-alive\r\n	00a0 4d 6f 7a 69 6c 6c 61 2f 35 2e 30 20 28 57 69 6e
Upgrade-Insecure-Requests: 1\r\n	00b0 64 6f 77 73 20 4e 54 20 31 30 2e 30 3b 20 57 69
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/129.0.0.0 Safari/537.36	00c0 6e 36 34 3b 20 78 36 34 29 20 41 70 70 6c 65 57
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8	00d0 65 62 4b 69 74 2f 35 33 37 2e 33 36 20 28 4b 48
Referer: http://www.http2demo.io/\r\n	00e0 54 4d 4c 2c 20 6c 69 6b 65 20 47 65 63 6b 6f 29
Accept-Encoding: gzip, deflate\r\n	00f0 20 43 68 72 6f 6d 65 2f 31 32 39 2e 30 2e 30 2e
Accept-Language: fr,fr-FR;q=0.9,en;q=0.8,en-GB;q=0.7,en-US;q=0.6	0100 30 20 53 61 66 61 72 69 2f 35 33 37 2e 33 36 20
Cookie: _ga=GA1.2.150416580.1729177803; _gid=GA1.2.744134529.1729177772	0110 45 64 67 2f 31 32 39 2e 30 2e 30 2e 30 0d 0a 41
If-None-Match: W/"5aa91b6d-19b00"\r\n	0120 63 63 65 70 74 3a 20 74 65 78 74 2f 68 74 6d 6c
\r\n	0130 2c 61 70 70 6c 69 63 61 74 69 6f 6e 2f 78 68 74
[Full request URI: http://www.http2demo.io/]	0140 6d 6c 2b 78 6d 6c 2c 61 70 70 6c 69 63 61 74 69
[HTTP request 1/2]	0150 6f 6e 2f 78 6d 6c 3b 71 3d 30 2e 39 2c 69 6d 61
[Response in frame: 126]	0160 67 65 2f 61 76 69 66 2c 69 6d 61 67 65 2f 77 65
[Next request in frame: 128]	0170 62 70 2c 69 6d 61 67 65 2f 61 70 6e 67 2c 2a 2f
	0180 2a 3b 71 3d 30 2e 38 2c 61 70 70 6c 69 63 61 74
	0190 69 6f 6e 2f 73 69 67 6e 65 64 2d 65 78 63 68 61
	01a0 6e 67 65 3b 76 3d 62 33 3b 71 3d 30 2e 37 0d 0a
	01b0 52 65 66 65 72 65 72 3a 20 68 74 74 70 3a 2f 2f
	01c0 77 77 77 2e 68 74 74 70 32 64 65 6d 6f 2e 69 6f
	01d0 2f 0d 0a 41 63 63 65 70 74 2d 45 6e 63 6f 64 69

## la section correspondant à l'en-tête Transport

The screenshot displays the Transport section of an HTTP request in Wireshark. The left pane shows the packet list and details for the selected packet (Frame 118). The right pane shows the raw packet data in hexadecimal and ASCII. The details pane is expanded to show the Hypertext Transfer Protocol section, which includes the request line and various headers.

Transmission Control Protocol (tcp), 20 byte(s)

Paquets : 909 • Affichés : 492 (54.1%) • Perdus : 0

---

---

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

Le protocole de transport utilisé est TCP

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

Segment

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

20 octets

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

Port source : 64161 (décimal) 0xFAA1 en hexadécimal

Port destination : 80 (décimal) 0x0050 en hexadécimal

## Section entête Réseaux :

The screenshot shows a Wireshark capture of an HTTP GET request. The packet list pane on the left shows the following structure:

- Frame 118: 737 bytes on wire (5896 bits), 737 bytes captured (5896 bits) on interface \Device\NPF\_{8A3505B0-BD86-4B72-8AC4-B98FB25D6}
- Ethernet II, Src: Giga-Byt\_2f:81:71 (74:56:3c:2f:81:71), Dst: Cisco\_97:2c:56 (00:1f:ca:97:2c:56)
- Internet Protocol Version 4, Src: 172.17.2.23, Dst: 195.181.175.40
  - 0100 .... = Version: 4
  - .... 0101 = Header Length: 20 bytes (5)
  - > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
  - Total Length: 723
  - Identification: 0x428d (17037)
  - > 010. .... = Flags: 0x2, Don't fragment
  - ...0 0000 0000 0000 = Fragment Offset: 0
  - Time to Live: 128
  - Protocol: TCP (6)
  - Header Checksum: 0x9491 [validation disabled]
  - [Header checksum status: Unverified]
  - Source Address: 172.17.2.23
  - Destination Address: 195.181.175.40
- Transmission Control Protocol, Src Port: 64613, Dst Port: 80, Seq: 1, Ack: 1, Len: 683
- Hypertext Transfer Protocol

The packet bytes pane on the right shows the raw data in hexadecimal and ASCII. The first 20 bytes (0000-0010) represent the network layer header:

```
0000 00 1f ca 97 2c 56 74 56 3c 2f 81 71 08 00 45 00  ....VtV </q...E...
0010 02 d3 42 8d 40 00 50 06 94 91 ac 11 92 17 c5 b5  ..B@... ..INP...
0020 14 2b 7c 65 00 50 d6 fb 81 8b e3 20 31 4e 50 18  ..E.P... ..INP...
0030 01 fb 90 af 00 00 47 45 54 20 2f 20 48 54 54 50  ....GE T / HTTP...
0040 2f 31 2e 31 0d 0a 48 6f 73 74 3a 20 77 77 77 2e  /1.1..Ho st: www.
0050 68 74 74 70 32 64 65 6d 6f 2e 69 6f 8d 0a 43 6f  http2dem.o.io..Co
0060 6e 6e 65 63 74 69 6f 6e 3a 20 6b 65 65 70 2d 61  nnection : keep-a
0070 6c 69 76 65 0d 0a 55 70 67 72 61 64 65 2d 49 6e  live..Up grade-In
0080 73 65 63 75 72 65 2d 52 65 71 75 65 73 74 73 3a  secure-R equests:
0090 20 31 0d 0a 55 73 65 72 2d 41 67 65 6e 74 3a 20  1..User -Agent:
00a0 4d 6f 7a 69 6c 6c 61 2f 35 2e 30 20 28 57 69 6e  Mozilla/ 5.0 (Win
00b0 64 6f 77 73 20 4e 54 20 31 30 2e 30 3b 20 57 69  dows NT 10.0; Mi
00c0 6e 36 34 3b 20 78 36 34 29 20 41 70 70 6c 65 57  n64; x64 ) AppleH
00d0 65 62 4b 69 74 2f 35 33 37 2e 33 36 20 28 4b 48  ebKit/53 7.36 (KH
00e0 54 4d 4c 2c 20 6c 69 6b 65 20 47 65 63 6b 6f 29  TML, lik e Gecko)
00f0 20 43 68 72 6f 6d 65 2f 31 32 39 2e 30 2e 30 2e  Chrome/ 129.0.0.
0100 30 20 53 61 66 61 72 69 2f 35 33 37 2e 33 36 20  0 Safari /537.36
0110 45 64 67 2f 31 32 39 2e 30 2e 30 2e 30 0d 0a 41  Edg/129. 0.0.0..A
0120 63 63 65 70 74 3a 20 74 65 78 74 2f 68 74 6d 6c  ccept: t ext/html
0130 2c 61 70 70 6c 69 63 61 74 69 6f 6e 2f 78 68 74  ,applica tion/xht
0140 6d 6c 2b 78 6d 6c 2c 61 70 70 6c 69 63 61 74 69  ml+xml,a pplicati
0150 6f 6e 2f 78 6d 6c 3b 71 3d 30 2e 39 2c 69 6d 61  on/xml;q =0.9,ima
0160 67 65 2f 61 76 69 66 2c 69 6d 61 67 65 2f 77 65  ge/avif, image/we
0170 62 70 2c 69 6d 61 67 65 2f 61 70 6e 67 2c 2a 2f  bp,image /png,*/
0180 2a 3b 71 3d 30 2e 38 2c 61 70 70 6c 69 63 61 74  *;q=0.8, applicat
0190 69 6f 6e 2f 73 69 67 6e 65 64 2d 65 78 63 68 61  ion/sign ed-excha
01a0 6e 67 65 3b 76 3d 62 33 3b 71 3d 30 2e 37 0d 0a  nge;v=b3 ;q=0.7..
01b0 52 65 66 65 72 65 72 3a 20 68 74 74 70 3a 2f 2f  Referer: http://
01c0 77 77 77 2e 68 74 74 70 32 64 65 6d 6f 2e 69 6f  www.http 2demo.io
01d0 2f 0d 0a 41 63 63 65 70 74 2d 45 6e 63 6f 64 69  /.Accep t-Encodi
```

Quelle est la longueur de l'en-tête de réseau ? 20 octets

Repérez le champ Protocole figurant dans l'en-tête Réseau. Quelle est la valeur présente ? 6

Que signifie-t-elle ? 6 correspond au protocole TCP

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

Adresse ip source :

172.17.12.23 (décimal)

AC.11.0C.17 (hexadécimal)

adresse ip destination :

195.181.175.48 (décimal)

C3.B5.AF.30 (hexadécimal)

## Section entête Ethernet

The screenshot shows a network traffic capture in Wireshark. The left pane displays the packet list, and the right pane shows the packet details. The selected packet is Frame 118, which is an Ethernet II frame containing an Internet Protocol Version 4 (IPv4) packet and a Hypertext Transfer Protocol (HTTP) message.

**Ethernet II Header:**

- Src: Giga-Byt\_2f:81:71 (74:56:3c:2f:81:71)
- Dst: Cisco\_97:2c:56 (00:1f:ca:97:2c:56)
- Version: 4
- Header Length: 20 bytes (5)
- Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
- Total Length: 723
- Identification: 0x428d (17037)
- Flags: 0x2, Don't fragment
- Fragment Offset: 0
- Time to Live: 128
- Protocol: TCP (6)
- Header Checksum: 0x9491 [validation disabled]
- Source Address: 172.17.2.23
- Destination Address: 195.181.175.40

**Hypertext Transfer Protocol Header:**

- Src Port: 64613, Dst Port: 80, Seq: 1, Ack: 1, Len: 683

The packet bytes pane shows the raw data in hexadecimal and ASCII. The ASCII portion of the packet body includes the text: "HTTP/1.1 200 OK (text/html)" and "Content-Type: text/html".

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

0800 ou 0x0800

indique la trame ethernet informe que la couche réseaux à traiter est IPv4

Quelles sont les valeurs des adresses MAC destination et source ?

MAC destination : 00:1f:ca:97:2c:56

MA source : 74:56:3c:2f:81:71

je réalise une capture d'écran des 3 trames mettant en place la connexion TCP entre le client et le serveur (cf. Chapitre 4 - pages 3 et 8 : Three-way handshake)

Time	Source	Destination	Protocol	Length	Info
1 0.000000	172.17.110.20	172.17.110.18	TCP	66	50569 → 7680 [SYN] Seq=0 Win=64240 Len=0 MSS=1460
2 0.000395	172.17.110.18	172.17.110.20	TCP	60	7680 → 50569 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
108 0.503462	172.17.110.20	172.17.110.18	TCP	66	[TCP Retransmission] [TCP Port numbers reused] 50569 → 7680 [SYN] Seq=0 Win=64240 Len=0 MSS=1460
110 0.503883	172.17.110.18	172.17.110.20	TCP	60	7680 → 50569 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
118 0.666398	172.17.2.23	195.181.175.40	HTTP	737	GET / HTTP/1.1
126 1.023589	195.181.175.40	172.17.2.23	HTTP	430	HTTP/1.1 304 Not Modified
128 1.029091	172.17.2.23	195.181.175.40	HTTP	601	GET /css/style.css HTTP/1.1
129 1.029192	172.17.2.23	195.181.175.40	HTTP	605	GET /css/jssocials.css HTTP/1.1
130 1.029256	172.17.2.23	195.181.175.40	HTTP	616	GET /css/jssocials-theme-flat.css HTTP/1.1
131 1.029339	172.17.2.23	195.181.175.40	HTTP	609	GET /css/font-awesome.css HTTP/1.1
132 1.029372	172.17.2.23	195.181.175.40	HTTP	653	GET /img/refresh-icon.png HTTP/1.1
133 1.029400	172.17.2.23	195.181.175.40	HTTP	650	GET /img/cdn77logo.png HTTP/1.1
138 1.042688	172.17.2.23	195.181.172.3	HTTP	625	GET /http2/http1.html HTTP/1.1
139 1.094599	172.17.110.20	172.17.110.18	TCP	66	[TCP Retransmission] [TCP Port numbers reused] 50569 → 7680 [SYN] Seq=0 Win=64240 Len=0 MSS=1460
140 1.094833	172.17.110.18	172.17.110.20	TCP	60	7680 → 50569 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
141 1.383849	172.17.2.23	195.181.175.40	TCP	650	[TCP Retransmission] 64612 → 80 [PSH, ACK] Seq=1 Ack=597 Win=126 Len=0
147 1.450608	172.17.2.23	195.181.175.40	TCP	605	[TCP Retransmission] 64612 → 80 [PSH, ACK] Seq=1 Ack=597 Win=126 Len=0
148 1.473302	172.17.2.23	195.181.172.3	TCP	625	[TCP Retransmission] 64618 → 80 [PSH, ACK] Seq=1 Ack=597 Win=126 Len=0
149 1.487179	195.181.175.40	172.17.2.23	HTTP	429	HTTP/1.1 304 Not Modified
150 1.487425	195.181.175.40	172.17.2.23	HTTP	429	HTTP/1.1 304 Not Modified
151 1.487658	195.181.175.40	172.17.2.23	HTTP	384	HTTP/1.1 304 Not Modified
152 1.487742	195.181.175.40	172.17.2.23	HTTP	430	HTTP/1.1 304 Not Modified

3 trames :

Time	Source	Destination	Protocol	Length	Info
150 1.487425	195.181.175.40	172.17.2.23	HTTP	429	HTTP/1.1 304 Not Modified
151 1.487658	195.181.175.40	172.17.2.23	HTTP	384	HTTP/1.1 304 Not Modified
152 1.487742	195.181.175.40	172.17.2.23	HTTP	430	HTTP/1.1 304 Not Modified
153 1.487932	195.181.175.40	172.17.2.23	HTTP	405	HTTP/1.1 304 Not Modified
154 1.489345	195.181.175.40	172.17.2.23	TCP	60	80 → 64612 [ACK] Seq=1 Ack=597 Win=126 Len=0

```

> Frame 2: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on 0
  Ethernet II, Src: PcsCompu_8b:1e:28 (08:00:27:8b:1e:28), Dst: PcsCompu_2b:5b:a6 (08:00:27:2b:5b:a6)
    Destination: PcsCompu_2b:5b:a6 (08:00:27:2b:5b:a6)
    Source: PcsCompu_8b:1e:28 (08:00:27:8b:1e:28)
      Address: PcsCompu_8b:1e:28 (08:00:27:8b:1e:28)
        ..0. .... = LG bit: Globally unique address
        ..0. .... = IG bit: Individual address
      Type: IPv4 (0x0800)
      Padding: 000000000000
    Internet Protocol Version 4, Src: 172.17.110.18, Dst: 172.17.110.20
    Transmission Control Protocol, Src Port: 7680, Dst Port: 50569, Seq=0, Win=64240, Len=0
  
```

Time	Source	Destination	Protocol	Length	Info
154 1.489345	195.181.175.40	172.17.2.23	TCP	60	80 → 64612 [ACK] Seq=1 Ack=597 Win=126 Len=0

```

> Frame 108: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on 0
  Ethernet II, Src: PcsCompu_2b:5b:a6 (08:00:27:2b:5b:a6), Dst: PcsCompu_8b:1e:28 (08:00:27:8b:1e:28)
    Destination: PcsCompu_8b:1e:28 (08:00:27:8b:1e:28)
    Source: PcsCompu_2b:5b:a6 (08:00:27:2b:5b:a6)
      Address: PcsCompu_2b:5b:a6 (08:00:27:2b:5b:a6)
        ..0. .... = LG bit: Globally unique address
        ..0. .... = IG bit: Individual address
      Type: IPv4 (0x0800)
    Internet Protocol Version 4, Src: 172.17.110.20, Dst: 172.17.110.18
    Transmission Control Protocol, Src Port: 50569, Dst Port: 7680, Seq=1, Ack=1, Win=0, Len=0
  
```

Time	Source	Destination	Protocol	Length	Info
154 1.489345	195.181.175.40	172.17.2.23	TCP	60	80 → 64612 [ACK] Seq=1 Ack=597 Win=126 Len=0

```

> Frame 118: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on 0
  Ethernet II, Src: PcsCompu_8b:1e:28 (08:00:27:8b:1e:28), Dst: PcsCompu_2b:5b:a6 (08:00:27:2b:5b:a6)
    Destination: PcsCompu_2b:5b:a6 (08:00:27:2b:5b:a6)
    Source: PcsCompu_8b:1e:28 (08:00:27:8b:1e:28)
      Address: PcsCompu_8b:1e:28 (08:00:27:8b:1e:28)
        ..0. .... = LG bit: Globally unique address
        ..0. .... = IG bit: Individual address
      Type: IPv4 (0x0800)
      Padding: 000000000000
    Internet Protocol Version 4, Src: 172.17.110.18, Dst: 172.17.110.20
    Transmission Control Protocol, Src Port: 7680, Dst Port: 50569, Seq=0, Win=64240, Len=0
  
```

Combien de connexions TCP ont été établies ? 3

---

---