

# TP3 – Les ports logiciels

## SOMMAIRE

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

## 1. Connexion Bureau à distance (RDP) :

1)

Pour connaître mon adresse IP j'ai effectué un ipconfig /all et je me suis aperçue que mon adresse IP était 172.17.2.13

```
Carte Ethernet Ethernet :

Suffixe DNS propre à la connexion. . . : prince.local
Description. . . . . : Realtek PCIe GbE Family Controller
Adresse physique . . . . . : 74-56-3C-2F-9D-13
DHCP activé. . . . . : Oui
Configuration automatique activée. . . : Oui
Adresse IPv6 de liaison locale. . . . : fe80::35af:39f7:fda1:8705%15(préfééré)
Adresse IPv4. . . . . : 172.17.2.13(préfééré)
Masque de sous-réseau. . . . . : 255.255.0.0
Bail obtenu. . . . . : mercredi 1 octobre 2025 08:08:58
Bail expirant. . . . . : mercredi 1 octobre 2025 10:26:07
Passerelle par défaut. . . . . : 172.17.250.3
Serveur DHCP . . . . . : 172.17.254.1
IAID DHCPv6 . . . . . : 326391356
DUID de client DHCPv6. . . . . : 00-01-00-01-2C-DD-CE-E0-74-56-3C-2F-9D-13
Serveurs DNS. . . . . : 172.17.254.1
NetBIOS sur Tcpi. . . . . : Activé
```

L'adresse IP de ma machine est : 172.17.2.13

L'adresse IP de la machine voisine est : 172.17.2.9

```
C:\Users\Mnovello>ping 172.17.2.9

Envoi d'une requête 'Ping' 172.17.2.9 avec 32 octets de données :
Réponse de 172.17.2.9 : octets=32 temps=1 ms TTL=128
Réponse de 172.17.2.9 : octets=32 temps=2 ms TTL=128
Réponse de 172.17.2.9 : octets=32 temps=2 ms TTL=128
Réponse de 172.17.2.9 : octets=32 temps=2 ms TTL=128

Statistiques Ping pour 172.17.2.9:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
    Durée approximative des boucles en millisecondes :
        Minimum = 1ms, Maximum = 2ms, Moyenne = 1ms
```

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

Exiger que les appareils utilisent l'authentification au niveau du réseau pour se connecter (recommandé)

Port du Bureau à distance

3389

Nom du PC

Utiliser ce nom pour se connecter à ce PC à partir d'un autre appareil

G102-GB18.prince.local

J'ai activé le bureau à distance pour pouvoir me connecter ou que mon voisin puisse se connecter

```
C:\Users\Mnovello>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    0.0.0.0:49664          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    0.0.0.0:49671          0.0.0.0:0              LISTENING
TCP    0.0.0.0:49672          0.0.0.0:0              LISTENING
TCP    0.0.0.0:49673          0.0.0.0:0              LISTENING
TCP    0.0.0.0:49722          0.0.0.0:0              LISTENING
TCP    0.0.0.0:65046          0.0.0.0:0              LISTENING
TCP    127.0.0.1:27017         0.0.0.0:0              LISTENING
TCP    172.17.2.13:139        0.0.0.0:0              LISTENING
TCP    172.17.2.13:64649      172.17.254.5:445       ESTABLISHED
TCP    172.17.2.13:65006      95.100.133.18:443      TIME_WAIT
TCP    172.17.2.13:65031      95.100.133.20:443      TIME_WAIT
TCP    172.17.2.13:65048      172.17.254.1:135       TIME_WAIT
TCP    172.17.2.13:65049      172.17.254.1:49666     TIME_WAIT
TCP    172.17.2.13:65050      172.17.254.1:135       TIME_WAIT
TCP    172.17.2.13:65051      172.17.254.1:49666     TIME_WAIT
TCP    172.17.2.13:65057      95.100.133.27:443      TIME_WAIT
TCP    172.26.224.1:139       0.0.0.0:0              LISTENING
```

Le port d'écoute du Terminale Server est 3389

Connexion Bureau à distance

Connexion Bureau A distance

Ordinateur :

172.17.2.9

Nom d'utilisateur :

Aucun paramètre n'a été spécifié.

Vos informations d'identification seront demandées lors de la connexion.

Afficher les options

Connexion

Aide

Impossible de vérifier l'identité de l'ordinateur distant.

Voulez-vous vraiment vous connecter ?

Impossible d'authentifier l'ordinateur distant en raison de problèmes liés à son certificat de sécurité. La poursuite de l'opération peut présenter un risque.

Nom du certificat

Nom figurant dans le certificat de l'ordinateur distant :

G102-GB11.prince.local

Erreurs de certificat

Les erreurs suivantes se sont produites lors de la validation du certificat de l'ordinateur distant :

Ce certificat de sécurité n'émane pas d'une autorité de certification digne de confiance.

Voulez-vous vous connecter malgré ces erreurs de certificat ?

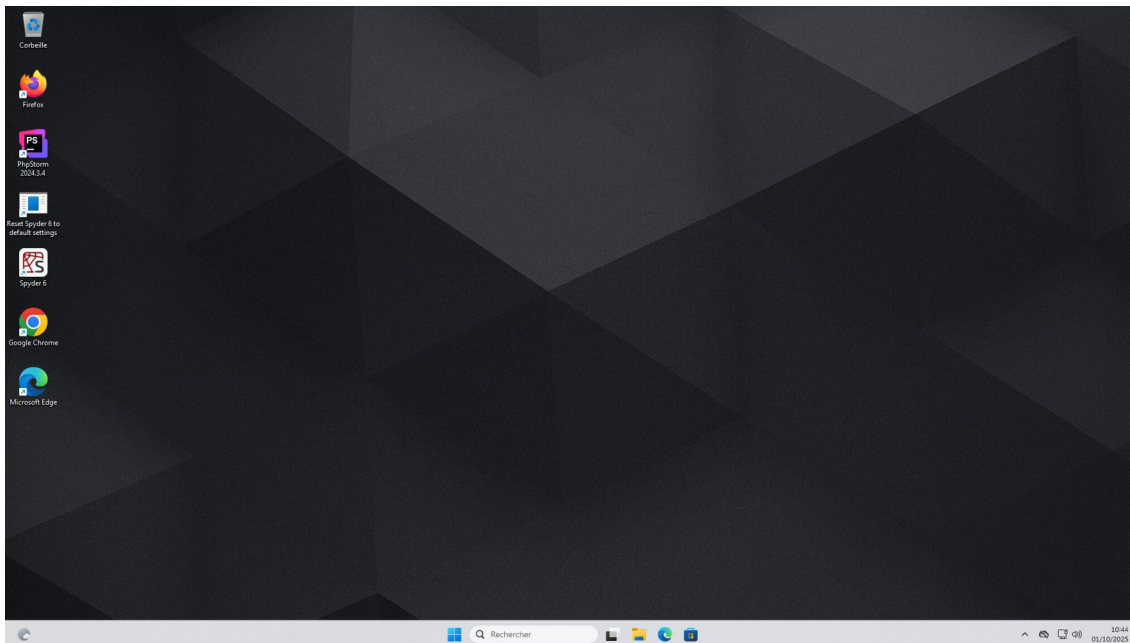
☐ Ne pas me redemander pour les connexions à cet ordinateur

Afficher le certificat...

Oui

Non

La connexion sur le bureau de mon voisin a été établie.



Invite de commandes			
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	127.0.0.1:27017	0.0.0.0:0	LISTENING
TCP	172.17.2.9:139	0.0.0.0:0	LISTENING
TCP	172.17.2.9:3389	172.17.2.13:65395	ESTABLISHED
TCP	172.17.2.9:49675	172.17.254.1:135	TIME_WAIT
TCP	172.17.2.9:49685	172.17.254.1:445	ESTABLISHED
TCP	172.17.2.9:49692	172.17.254.1:49666	TIME_WAIT
TCP	172.17.2.9:49704	172.17.254.1:135	TIME_WAIT
TCP	172.17.2.9:49705	172.17.254.1:49666	TIME_WAIT
TCP	172.17.2.9:49721	172.17.254.1:49688	TIME_WAIT
TCP	172.17.2.9:50392	172.17.254.5:445	ESTABLISHED
TCP	172.17.2.9:50396	4.210.40.181:443	TIME_WAIT
TCP	172.17.2.9:50398	23.200.87.13:80	TIME_WAIT
TCP	172.17.2.9:50399	23.200.87.13:80	TIME_WAIT
TCP	172.17.2.9:50400	23.200.87.13:80	TIME_WAIT
TCP	172.17.2.9:50403	20.190.159.75:443	TIME_WAIT
TCP	172.17.2.9:50405	150.171.22.17:443	TIME_WAIT
TCP	172.17.2.9:50420	52.165.237.15:443	TIME_WAIT
TCP	172.17.2.9:50421	52.165.237.15:443	TIME_WAIT
TCP	172.17.2.9:50430	13.107.213.43:443	CLOSE_WAIT
TCP	172.17.2.9:50432	52.109.68.130:443	ESTABLISHED
TCP	172.17.2.9:50433	23.200.86.235:443	ESTABLISHED
TCP	172.17.2.9:50434	204.79.197.222:443	ESTABLISHED
TCP	172.17.2.9:50436	150.171.27.11:80	TIME_WAIT
TCP	172.17.2.9:50437	150.171.22.17:443	TIME_WAIT

## 2. Capture de trames HTTP :

1)

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

Réponse ne faisant pas autorité :
DNS request timed out.
        timeout was 2 seconds.
Nom :      1906714720.rsc.cdn77.org
Addresses: 79.127.138.15
           79.127.138.18
           79.127.138.20
Aliases:   www.http2demo.io
```

J'ai effectué la commande nslookup [www.http2demo.io](http://www.http2demo.io) pour connaître l'adresse du serveur.

ip.addr==79.127.138.18&&tcp.port==80						
No.	Time	Source	Destination	Protocol	Length	Info
27	1.738506	172.17.2.16	79.127.138.18	TCP	66	54153 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=
30	1.739222	172.17.2.16	79.127.138.18	TCP	66	54155 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=
32	1.749075	79.127.138.18	172.17.2.16	TCP	66	80 → 54155 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 M
33	1.749155	172.17.2.16	79.127.138.18	TCP	54	54155 → 80 [ACK] Seq=1 Ack=1 Win=65280 Len=0
78	2.061349	172.17.2.16	79.127.138.18	HTTP	532	GET / HTTP/1.1
81	2.069021	79.127.138.18	172.17.2.16	TCP	60	80 → 54155 [ACK] Seq=1 Ack=479 Win=64512 Len=0
82	2.076743	79.127.138.18	172.17.2.16	TCP	1514	80 → 54155 [ACK] Seq=1 Ack=479 Win=64512 Len=1460 [
83	2.076743	79.127.138.18	172.17.2.16	TCP	1514	80 → 54155 [ACK] Seq=1461 Ack=479 Win=64512 Len=146

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

Le nom est le protocole TCP

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

Le nom du PDU encapsulant les données applicative est le segment

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

header length : 20 bytes (5)

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

Port source = 54155 = d3 8b

Port destination = 80 = 00 50

```

> Frame 78: 532 bytes on wire (4256 bits), 532 bytes captured (4256) on interface 0
> Ethernet II, Src: Giga-Byt_2f:9c:fd (74:56:3c:2f:9c:fd), Dst: Stc...
> Internet Protocol Version 4, Src: 172.17.2.16, Dst: 79.127.138.18
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 518
    Identification: 0x5c0e (23566)
  > 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: 172.17.2.16
    Destination Address: 79.127.138.18
  > Transmission Control Protocol, Src Port: 54155, Dst Port: 80, Seq...
  > Hypertext Transfer Protocol

```

0000	00 0d b4 2a a8 34 74 56 3c 2f 9c fd 08 00 45 00	...*.4t)
0010	02 06 5c 0e 40 00 80 06 00 00 ac 11 02 10 4f 7f	...@...
0020	8a 12 d3 8b 00 50 f6 d5 02 c9 8e f4 7d 64 50 18	...P...
0030	00 ff 89 ab 00 00 47 45 54 20 2f 20 48 54 54 50	.....Gi
0040	2f 31 2e 31 0d 0a 48 6f 73 74 3a 20 77 77 77 2e	/1.1..Hc
0050	68 74 74 70 32 64 65 6d 6f 2e 69 6f 0d 0a 43 6f	http2der
0060	6e 6e 65 63 74 69 6f 6e 3a 20 6b 65 65 70 2d 61	nnection
0070	6c 69 76 65 0d 0a 55 70 67 72 61 64 65 2d 49 6e	live..Up
0080	73 65 63 75 72 65 2d 52 65 71 75 65 73 74 73 3a	secure-f
0090	20 31 0d 0a 55 73 65 72 2d 41 67 65 6e 74 3a 20	1..User
00a0	4d 6f 7a 69 6c 6c 61 2f 35 2e 30 20 28 57 69 6e	Mozilla,
00b0	64 6f 77 73 20 4e 54 20 31 30 2e 30 3b 20 57 69	dows NT
00c0	6e 36 34 3b 20 78 36 34 29 20 41 70 70 6c 65 57	n64; x64
00d0	65 62 4b 69 74 2f 35 33 37 2e 33 36 20 28 4b 48	ebKit/5:
00e0	54 4d 4c 2c 20 6c 69 6b 65 20 47 65 63 6b 6f 29	TML, lil
00f0	20 43 68 72 6f 6d 65 2f 31 34 30 2e 30 2e 30 2e	Chrome,
0100	30 20 53 61 66 61 72 69 2f 35 33 37 2e 33 36 20	0 Safari:
0110	45 64 67 2f 31 34 30 2e 30 2e 30 2e 30 0d 0a 41	Edg/140.
0120	63 63 65 70 74 3a 20 74 65 78 74 2f 68 74 6d 6c	ccept: f
0130	2c 61 70 70 6c 69 63 61 74 69 6f 6e 2f 78 68 74	,applic
0140	6d 6c 2b 78 6d 6c 2c 61 70 70 6c 69 63 61 74 69	ml+xml,i
0150	6f 6e 2f 78 6d 6c 3b 71 3d 30 2e 39 2c 69 6d 61	on/xml;c
0160	67 65 2f 61 76 69 66 2c 69 6d 61 67 65 2f 77 65	ge/avif
0170	62 70 2c 69 6d 61 67 65 2f 61 70 6e 67 2c 2a 2f	bp,image
0180	2a 3b 71 3d 30 2e 38 2c 61 70 70 6c 69 63 61 74	*;q=0.8
0190	69 6f 6e 2f 73 69 67 6e 65 64 2d 65 78 63 68 61	ion/sign
01a0	6e 67 65 3b 76 3d 62 33 3b 71 3d 30 2e 37 0d 0a	nge;v=b:
01b0	41 63 63 65 70 74 2d 45 6e 63 6f 64 69 6e 67 3a	Accept-i
01c0	20 67 7a 69 70 2c 20 64 65 66 6c 61 74 65 0d 0a	ezip. (

Internet Protocol Version 4 (ip), 20 byte(s) | Paquets : 2628 · Affichés : 548 (20.9%) · Perdus : 0 (0.0%) | Profil : Default

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

Header length : 20 bytes (5)

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

Protocole TCP, sa valeur est 06

Que signifie-t-elle ?

Cela signifie que c'est un TCP

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

Adresse IP source = 172.17.2.16 = ac 11 02 10

Adresse IP destination = 79.127.138.18 = 4f 7f 8a 12

```

> Frame 78: 532 bytes on wire (4256 bits), 532 bytes captured (4256
Ethernet II, Src: Giga-Byt_2f:9c:fd (74:56:3c:2f:9c:fd), Dst: Sto
  Destination: Stormshi_2a:a8:34 (00:0d:b4:2a:a8:34)
  Source: Giga-Byt_2f:9c:fd (74:56:3c:2f:9c:fd)
  Type: IPv4 (0x0800)
> Internet Protocol Version 4, Src: 172.17.2.16, Dst: 79.127.138.1
  Transmission Control Protocol, Src Port: 54155, Dst Port: 80, Seq
  Hypertext Transfer Protocol
0000 00 0d b4 2a a8 34 74 56 3c 2f 9c fd 08 00 45 00 ...*4t
0010 02 06 5c 0e 40 00 80 06 00 00 ac 11 02 10 4f 7f ...\.@..
0020 8a 12 d3 8b 00 50 f6 d5 02 c9 8e f4 7d 64 50 18 .....P..
0030 00 ff 89 ab 00 00 47 45 54 20 2f 20 48 54 54 50 .....GI
0040 2f 31 2e 31 0d 0a 48 6f 73 74 3a 20 77 77 77 2e .../1.1..H
0050 68 74 74 70 32 64 65 6d 6f 7e 69 6f 0d 0a 43 6f httpdter
0060 6e 6e 65 63 74 69 6f 6e 3a 20 6b 65 65 70 2d 61 nnection
0070 6c 69 76 65 0d 0a 55 70 67 72 61 64 65 2d 49 6e live..Up
0080 73 65 63 75 72 65 2d 52 65 71 75 65 73 74 73 3a secure-f
0090 20 31 0d 0a 55 73 65 72 2d 41 67 65 6e 74 3a 20 1..User
00a0 4d 6f 7a 69 6c 6c 61 2f 35 2e 30 20 28 57 69 6e Mozilla,
00b0 64 6f 77 73 20 4e 54 20 31 30 2e 30 3b 20 57 69 dows NT
00c0 6e 36 34 3b 20 78 36 34 29 20 41 70 70 6c 65 57 n64; x64
00d0 65 62 4b 69 74 2f 35 33 37 2e 33 36 20 28 4b 48 ebKit/5:
00e0 54 4d 4c 2c 20 6c 69 6b 65 20 47 65 63 6b 6f 29 TML, lil
00f0 20 43 68 72 6f 6d 65 2f 31 34 30 2e 30 2e 30 2e Chrome,
0100 30 20 53 61 66 61 72 69 2f 35 33 37 2e 33 36 20 0 Safari:
0110 45 64 67 2f 31 34 30 2e 30 2e 30 2e 30 0d 0a 41 Edg/140
0120 63 63 65 70 74 3a 20 74 65 78 74 2f 68 74 6d 6c ccept: t
0130 2c 61 70 70 6c 69 63 61 74 69 6f 6e 2f 78 68 74 , applica
0140 6d 6c 2b 78 6d 6c 2c 61 70 70 6c 69 63 61 74 69 ml+xml;
0150 6f 6e 2f 78 6d 6c 3b 71 3d 30 2e 39 2c 69 6d 61 on/xml;
0160 67 65 2f 61 76 69 66 2c 69 6d 61 67 65 2f 77 65 ge/avif;
0170 62 70 2c 69 6d 61 67 65 2f 61 70 6e 67 2c 2a 2f bp,image
0180 2a 3b 71 3d 30 2e 38 2c 61 70 70 6c 69 63 61 74 *;q=0.8;
0190 69 6f 6e 2f 73 69 67 6e 65 64 2d 65 78 63 68 61 ion/sign
01a0 6e 67 65 3b 76 3d 62 33 3b 71 3d 30 2e 37 0d 0a nge;v=b;
01b0 41 63 63 65 70 74 2d 45 6e 63 6f 64 69 6e 67 3a Accept-i
01c0 20 67 7a 69 70 2c 20 64 65 66 6c 61 74 65 0d 0a ezip.

```

- Repérez le champ EtherType. Quel est la valeur contenue ?

### Que signifie-t-elle ?

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

- 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).

30	1.739222	172.17.2.16	79.127.138.18	TCP	66 54155 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=0
32	1.749075	79.127.138.18	172.17.2.16	TCP	66 80 → 54155 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 WS=0
33	1.749155	172.17.2.16	79.127.138.18	TCP	54 54155 → 80 [ACK] Seq=1 Ack=1 Win=65280 Len=0
78	2.061349	172.17.2.16	79.127.138.18	HTTP	532 GET / HTTP/1.1



30	1.739222	172.17.2.16	79.127.138.18	TCP	66	54155 → 80	[SYN]	Seq=0 Win=65535 Len=0 MSS=1460 WS=
32	1.749075	79.127.138.18	172.17.2.16	TCP	66	80 → 54155	[SYN, ACK]	Seq=0 Ack=1 Win=64240 Len=0 M
33	1.749155	172.17.2.16	79.127.138.18	TCP	54	54155 → 80	[ACK]	Seq=1 Ack=1 Win=65280 Len=0
78	2.061349	172.17.2.16	79.127.138.18	HTTP	532	GET / HTTP/1.1		
81	2.069021	79.127.138.18	172.17.2.16	TCP	60	80 → 54155	[ACK]	Seq=1 Ack=479 Win=64512 Len=0
82	2.076743	79.127.138.18	172.17.2.16	TCP	1514	80 → 54155	[ACK]	Seq=1 Ack=479 Win=64512 Len=1460
83	2.076743	79.127.138.18	172.17.2.16	TCP	1514	80 → 54155	[ACK]	Seq=1461 Ack=479 Win=64512 Len=1460
84	2.076743	79.127.138.18	172.17.2.16	TCP	1514	80 → 54155	[ACK]	Seq=2921 Ack=479 Win=64512 Len=1460

> Internet Protocol Version 4, Src: 172.17.2.16, Dst: 79.127.138.18  
 > Transmission Control Protocol, Src Port: 54155, Dst Port: 80,  
   Source Port: 54155  
   Destination Port: 80  
   [Stream index: 6]  
   [Conversation completeness: Incomplete, DATA (15)]  
   [TCP Segment Len: 0]  
   Sequence Number: 0 (relative sequence number)  
   Sequence Number (raw): 4141155016  
   [Next Sequence Number: 1 (relative sequence number)]  
   Acknowledgment Number: 0  
   Acknowledgment number (raw): 0  
   1000 .... = Header Length: 32 bytes (8)  
   > Flags: 0x002 (SYN)  
   Window: 65535  
   [Calculated window size: 65535]  
   Checksum: 0x87d9 [unverified]  
   [Checksum Status: Unverified]  
   Urgent Pointer: 0  
   > Options: (12 bytes), Maximum segment size, No-Operation (NO  
   > [Timestamps]

0000 00 0d b4 2a a8 34 74 56 3c 2f 9c fd 08 00 45 00 ...\*4tV <  
 0010 00 34 5c 05 40 00 80 06 00 00 ac 11 02 10 4f 7f ...4\@...  
 0020 8a 12 d3 8b 00 50 f6 d5 02 c8 00 00 00 00 80 02 ...P...  
 0030 ff ff 87 d9 00 00 02 04 05 b4 01 03 03 08 01 01 .....  
 0040 04 02 ..

32	1.749075	79.127.138.18	172.17.2.16	TCP	66	80 → 54155	[SYN, ACK]	Seq=0 Ack=1 Win=64240 Len=0 M
33	1.749155	172.17.2.16	79.127.138.18	TCP	54	54155 → 80	[ACK]	Seq=1 Ack=1 Win=65280 Len=0
78	2.061349	172.17.2.16	79.127.138.18	HTTP	532	GET / HTTP/1.1		
81	2.069021	79.127.138.18	172.17.2.16	TCP	60	80 → 54155	[ACK]	Seq=1 Ack=479 Win=64512 Len=0
82	2.076743	79.127.138.18	172.17.2.16	TCP	1514	80 → 54155	[ACK]	Seq=1 Ack=479 Win=64512 Len=1460
83	2.076743	79.127.138.18	172.17.2.16	TCP	1514	80 → 54155	[ACK]	Seq=1461 Ack=479 Win=64512 Len=1460
84	2.076743	79.127.138.18	172.17.2.16	TCP	1514	80 → 54155	[ACK]	Seq=2921 Ack=479 Win=64512 Len=1460

> Internet Protocol Version 4, Src: 79.127.138.18, Dst: 172.17.2.16  
 > Transmission Control Protocol, Src Port: 80, Dst Port: 54155,  
   Source Port: 80  
   Destination Port: 54155  
   [Stream index: 6]  
   [Conversation completeness: Incomplete, DATA (15)]  
   [TCP Segment Len: 0]  
   Sequence Number: 0 (relative sequence number)  
   Sequence Number (raw): 2398387555  
   [Next Sequence Number: 1 (relative sequence number)]  
   Acknowledgment Number: 1 (relative ack number)  
   Acknowledgment number (raw): 4141155017  
   1000 .... = Header Length: 32 bytes (8)  
   > Flags: 0x012 (SYN, ACK)  
   Window: 64240  
   [Calculated window size: 64240]  
   Checksum: 0x1289 [unverified]  
   [Checksum Status: Unverified]  
   Urgent Pointer: 0  
   > Options: (12 bytes), Maximum segment size, No-Operation (NO  
   > [Timestamps]

0000 74 56 3c 2f 9c fd 00 0d b4 2a a8 34 08 00 45 28 tV</...  
 0010 00 34 00 00 40 00 34 06 be e9 4f 7f 8a 12 ac 11 ...4\@4...  
 0020 02 10 00 50 d3 8b 8e f4 7d 63 f6 d5 02 c9 80 12 ...P...  
 0030 fa f0 12 89 00 00 02 04 05 b4 01 01 04 02 01 03 .....  
 0040 03 09 ..

33	1.749155	172.17.2.16	79.127.138.18	TCP	54	54155 → 80 [ACK]	Seq=1 Ack=1 Win=65280 Len=0
78	2.061349	172.17.2.16	79.127.138.18	HTTP	532	GET / HTTP/1.1	
81	2.069021	79.127.138.18	172.17.2.16	TCP	60	80 → 54155 [ACK]	Seq=1 Ack=479 Win=64512 Len=0
82	2.076743	79.127.138.18	172.17.2.16	TCP	1514	80 → 54155 [ACK]	Seq=1 Ack=479 Win=64512 Len=1460
83	2.076743	79.127.138.18	172.17.2.16	TCP	1514	80 → 54155 [ACK]	Seq=1461 Ack=479 Win=64512 Len=1460
84	2.076743	79.127.138.18	172.17.2.16	TCP	1514	80 → 54155 [ACK]	Seq=2921 Ack=479 Win=64512 Len=1460

> Internet Protocol Version 4, Src: 172.17.2.16, Dst: 79.127.138.18 ▾ Transmission Control Protocol, Src Port: 54155, Dst Port: 80, Source Port: 54155 Destination Port: 80 [Stream index: 6] [Conversation completeness: Incomplete, DATA (15)] [TCP Segment Len: 0] Sequence Number: 1 (relative sequence number) Sequence Number (raw): 4141155017 [Next Sequence Number: 1 (relative sequence number)] Acknowledgment Number: 1 (relative ack number) Acknowledgment number (raw): 2398387556 0101 .... = Header Length: 20 bytes (5) > Flags: 0x010 (ACK) Window: 255 [Calculated window size: 65280] [Window size scaling factor: 256] Checksum: 0x87cd [unverified] [Checksum Status: Unverified] Urgent Pointer: 0 > [Timestamps]		0000 00 0d b4 2a a8 34 74 56 3c 2f 9c fd 08 00 45 00 ...*..4tV < 0010 00 28 5c 06 40 00 80 06 00 00 ac 11 02 10 4f 7f ..(\. @... 0020 8a 12 d3 8b 00 50 f6 d5 02 c9 8e f4 7d 64 50 10 .....P.. 0030 00 ff 87 cd 00 00 .....
---	--	--

▪ 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 ?

SYN = TCP client émet un segment SYN

SYN ACK = Le serveur reçoit le segment SYN et répond par un SYN ACK

ACK = Le client reçoit le segment SYN ACK et répond avec le segment ACK