

## TP 3- Les ports logiciels

Nesrine EL AHMADI

BTS SIO

### Sommaire

1. Connexion Bureau à distance (RDP).....	2
2. Capture de trames HTTP.....	12

La commande netstat -no nous permet d'obtenir les connexions actives avec leur ports associées.

La commande **netstat -no** est utilisée dans l'invite de commande Windows pour afficher les connexions réseau actives.

Elle montre les adresses IP locales et distantes, les ports utilisés, l'état de chaque connexion, et le numéro du processus (PID) associé.

```
Administrator : Invite de commandes
Microsoft Windows [version 10.0.26100.6584]
(c) Microsoft Corporation. Tous droits réservés.

C:\Windows\System32>netstat -no

Connexions actives

Proto  Adresse locale        Adresse distante      État
TCP    172.17.2.9:50412    172.17.254.5:445    ESTABLISHED      4
TCP    172.17.2.9:51819    64.233.167.188:443   ESTABLISHED      6900
TCP    172.17.2.9:54212    98.66.133.186:443   ESTABLISHED      4932
TCP    172.17.2.9:59015    2.16.165.116:443    ESTABLISHED      9780
TCP    172.17.2.9:63385    20.199.58.43:443    ESTABLISHED     10112
TCP    172.17.2.9:63386    104.75.232.13:80    CLOSE_WAIT       10112
TCP    172.17.2.9:63387    2.16.165.122:443    ESTABLISHED     10112
TCP    172.17.2.9:63389    92.122.166.179:443   ESTABLISHED     7816
TCP    172.17.2.9:63390    20.190.159.2:443    ESTABLISHED     4836
TCP    172.17.2.9:64009    20.190.159.2:443    TIME_WAIT        0
TCP    172.17.2.9:64010    20.189.173.5:443    TIME_WAIT        0
TCP    172.17.2.9:64628    3.160.188.18:443   CLOSE_WAIT      11120

C:\Windows\System32>
```

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

On fait un **ipconfig** (*Capture 1*) dans l’invite de commande afin d’obtenir notre adresse IP.

## *Capture 1*

Après avoir demandais l'IP de mon voisin ,on autoriser les trames ICMP .

Pour cela on execute le protocole suivant :

---On va dans l'outil Pare-feu Windows ( Capture 2 ).



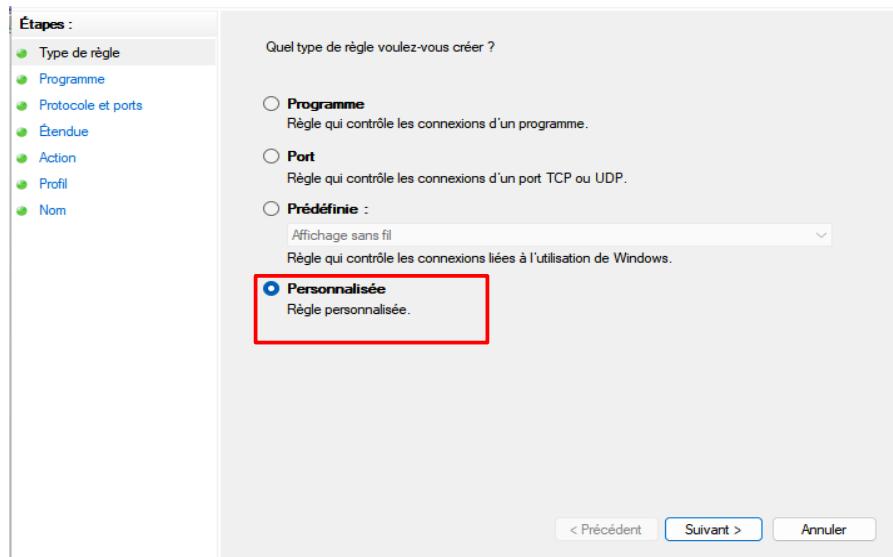
*Capture 2*

---On régle les paramètres pour les trames entrantes ICMP ( 6 Captures suivantes).

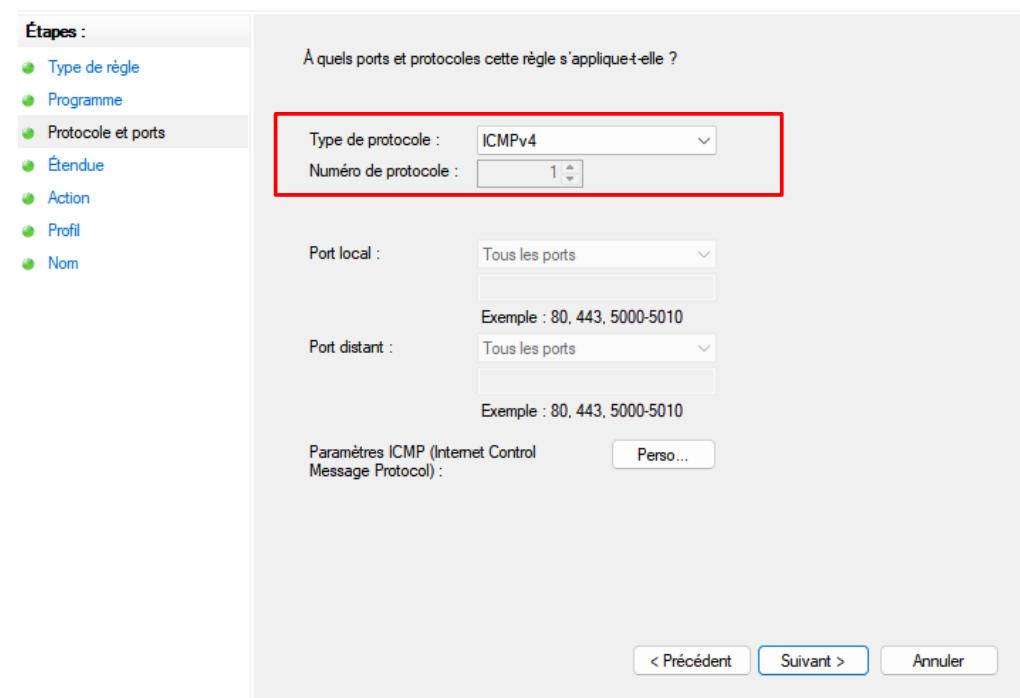
A screenshot of the Windows Firewall settings page. The left sidebar shows "Paramètres avancés" highlighted with a red box. The main area shows ICMP configuration: "Réseaux privés" is set to "Non connecté" and "Réseaux publics ou invités" is set to "Connecté". Under "Réseaux publics ou invités", the "État du Pare-feu Windows Defender" is "Activé", "Connexions entrantes" is set to "Bloquer toutes les connexions aux applications ne figurant pas dans la liste des applications autorisées", and "Réseaux publics actifs" and "État de notification" are both set to "Aucun".

A screenshot of the Windows Firewall rules list. The left sidebar shows "Règles de trafic entrant" highlighted with a red box. The main pane lists various traffic rules, including ICMP and Microsoft Teams. On the right, a "Actions" pane shows a context menu for a selected rule, with "Nouvelle règle..." highlighted with a red box.

On crée une nouvelle règle.



On choisit personnalisée.



On choisit en type de protocole ICMPv4

**Étendue**

Spécifiez les adresses IP locales et distantes auxquelles s'applique cette règle.

**Étapes :**

- Type de règle
- Programme
- Protocole et ports
- **Étendue**
- Action
- Profil
- Nom

**A quelles adresses IP locales cette règle s'applique-t-elle ?**

**Toute adresse IP**

Ces adresses IP :

**Ajouter...**

**Modifier...**

**Supprimer**

Personnaliser les types d'interfaces auxquels cette règle s'applique : **Perso ...**

**A quelles adresses IP distantes cette règle s'applique-t-elle ?**

**Toute adresse IP**

Ces adresses IP :

**Ajouter...**

**Modifier...**

**Supprimer**

**< Précédent** **Suivant >** **Annuler**

## Action

Spécifiez une action à entreprendre lorsqu'une connexion répond aux conditions spécifiées dans la règle.

**Étapes :**

- Type de règle
- Programme
- Protocole et ports
- **Étendue**
- **Action**
- Profil
- Nom

Quelle action entreprendre lorsqu'une connexion répond aux conditions spécifiées ?

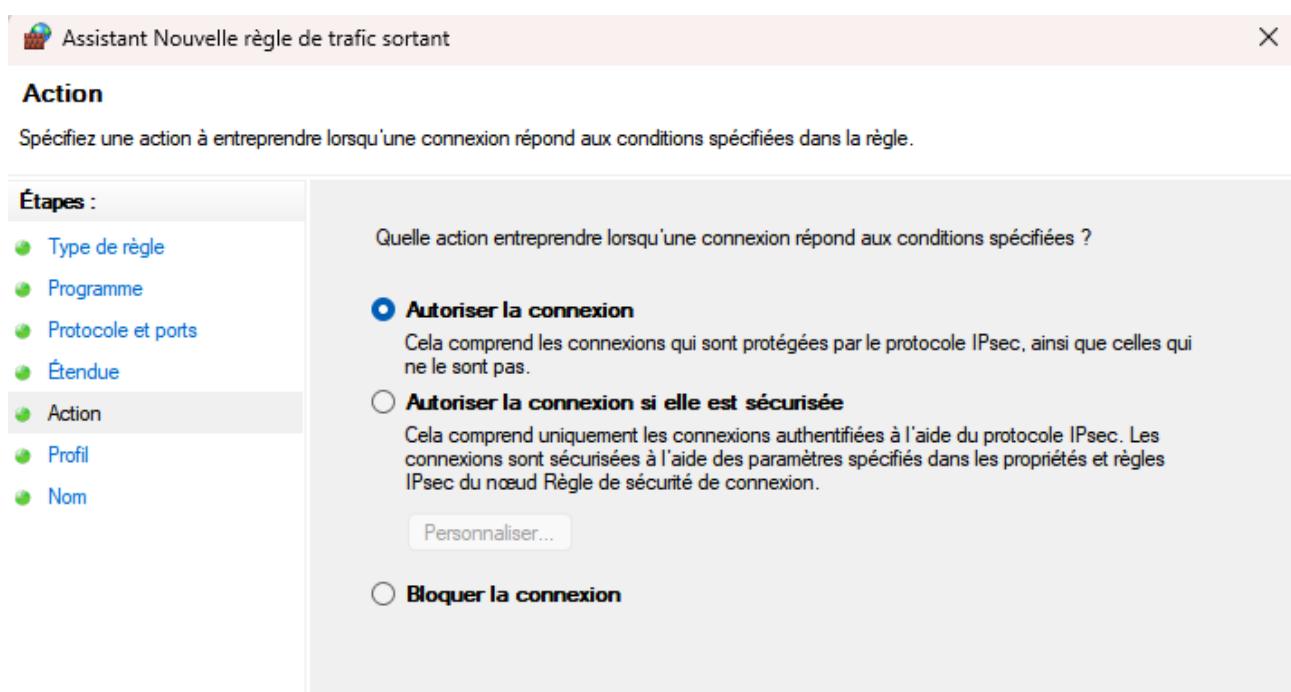
**Autoriser la connexion**  
Cela comprend les connexions qui sont protégées par le protocole IPsec, ainsi que celles qui ne le sont pas.

**Autoriser la connexion si elle est sécurisée**  
Cela comprend uniquement les connexions authentifiées à l'aide du protocole IPsec. Les connexions sont sécurisées à l'aide des paramètres spécifiés dans les propriétés et règles IPsec du nœud Règle de sécurité de connexion.

**Personnaliser...**

**Bloquer la connexion**

**< Précédent** **Suivant >** **Annuler**



---On fait de même pour le trafic sortant et on sélectionne autoriser la connexion ( les 2 Captures suivantes )

**Règles de trafic sortant**

Nom	Groupe	Profil
ICMPv4	Tout	Tout
ICMP	Tout	Tout
ICMPv4	Tout	Tout
@{Microsoft.XboxGamingOverlay_2.624...}	@{Microsoft.XboxGamingO...	Tout
@{MicrosoftWindows.56978801.Voie..._1...	@{MicrosoftWindows.56978...	Tout
@{MicrosoftWindows.57058570.Speion_1...	@{MicrosoftWindows.57058...	Tout
@{MicrosoftWindows.57074904.InpApp_...	@{MicrosoftWindows.57074...	Tout
@{MicrosoftWindows.57074914.Livtop_1...	@{MicrosoftWindows.57074...	Tout
@{MicrosoftWindows.LKG.AccountsServ..._1...	@{MicrosoftWindows.LKG.A...	Tout
@{MicrosoftWindows.LKG.DesktopSpotli...	@{MicrosoftWindows.LKG.D...	Tout
@{MicrosoftWindows.LKG.IrisService_100...	@{MicrosoftWindows.LKG.Ir...	Tout
@{MicrosoftWindows.LKG.RulesEngine_1...	@{MicrosoftWindows.LKG.R...	Tout
@{MicrosoftWindows.LKG.SpeechRunti...	@{MicrosoftWindows.LKG.S...	Tout
@{MicrosoftWindows.LKG.TwinSxS_1000...	@{MicrosoftWindows.LKG.T...	Tout
ms-resource:AppTitle	(78E1CD88-49E3-476E-B926-...)	Tout
ms-resource:AppTitle	(78E1CD88-49E3-476E-B926-...)	Tout
ms-resource:AppTitle	(78E1CD88-49E3-476E-B926-...)	Tout
ms-resource:ProductPkgDisplayName	(78E1CD88-49E3-476E-B926-...)	Privé
ms-resource:ProductPkgDisplayName	(78E1CD88-49E3-476E-B926-...)	Privé
ms-resource:ProductPkgDisplayName	(78E1CD88-49E3-476E-B926-...)	Privé
ms-resource:ProductPkgDisplayName	(78E1CD88-49E3-476E-B926-...)	Public
ms-resource:ProductPkgDisplayName	(78E1CD88-49E3-476E-B926-...)	Public
ms-resource:ProductPkgDisplayName	(78E1CD88-49E3-476E-B926-...)	Public
ms-resource:ProductPkgDisplayName	(78E1CD88-49E3-476E-B926-...)	Privé
ms-resource:ProductPkgDisplayName	(78E1CD88-49E3-476E-B926-...)	Public
ms-resource:ProductPkgDisplayName	(78E1CD88-49E3-476E-B926-...)	Privé

**Actions**

- Nouvelle règle...
- Filtrer par profil
- Filtrer par état
- Filtrer par groupe
- Affichage
- Actualiser
- Exporter la liste...
- Aide

**ICMPv4**

- Désactiver la règle
- Couper
- Copier
- Supprimer
- Propriétés
- Aide

**Action**

Spécifiez une action à entreprendre lorsqu'une connexion répond aux conditions spécifiées dans la règle.

**Étapes :**

- Type de règle
- Programme
- Protocole et ports
- Étendue
- Action**
- Profil
- Nom

Quelle action entreprendre lorsqu'une connexion répond aux conditions spécifiées ?

**Autoriser la connexion**  
Cela comprend les connexions qui sont protégées par le protocole IPsec, ainsi que celles qui ne le sont pas.

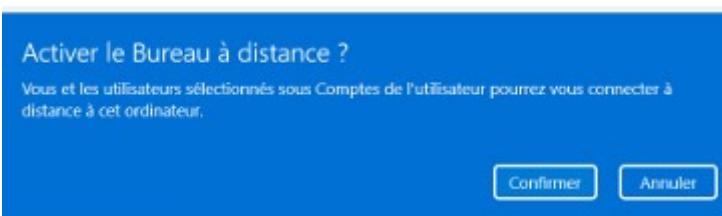
**Autoriser la connexion si elle est sécurisée**  
Cela comprend uniquement les connexions authentifiées à l'aide du protocole IPsec. Les connexions sont sécurisées à l'aide des paramètres spécifiés dans les propriétés et règles IPsec du nœud Règle de sécurité de connexion.

[Personnaliser...](#)

**Bloquer la connexion**

Liens apparentés

- Cle de produit et activation
- Bureau à distance **Désactivé**
- Utilisateurs du Bureau à distance



Afin d'observer les connexions du trafic entrants avec les ports et leurs états, on exécute la commande **netstat -an** dans l'invite de commande.

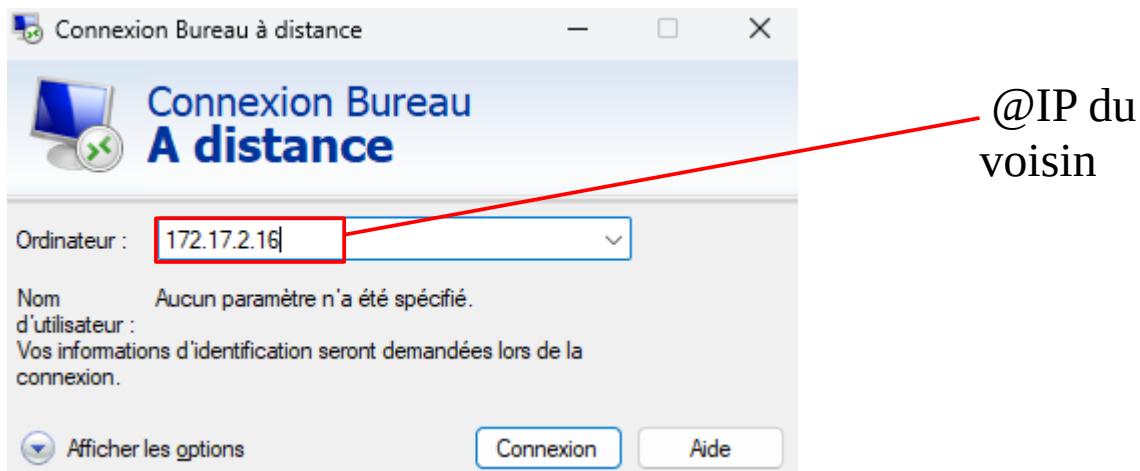
```
C:\Windows\System32>netstat -an

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    0.0.0.0:902          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    0.0.0.0:3389          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    127.0.0.1:27017        0.0.0.0:0          LISTENING
  TCP    172.17.2.9:139         0.0.0.0:0          LISTENING
  TCP    172.17.2.9:50412        172.17.254.5:445 ESTABLISHED
  TCP    172.17.2.9:51819        64.233.167.188:443 ESTABLISHED
  TCP    172.17.2.9:54212        98.66.133.186:443 ESTABLISHED
  TCP    172.17.2.9:63386        104.75.232.13:80  CLOSE_WAIT
  TCP    172.17.2.9:63387        2.16.165.122:443 ESTABLISHED
  TCP    172.17.2.9:63389        92.122.166.179:443 ESTABLISHED
  TCP    172.17.2.9:63390        20.190.159.2:443 ESTABLISHED
  TCP    172.17.2.9:64009        20.190.159.2:443 TIME_WAIT
  TCP    172.17.2.9:64010        20.189.173.5:443 TIME_WAIT
  TCP    172.17.2.9:64628         3.160.188.18:443 CLOSE_WAIT
  TCP    172.26.48.1:139         0.0.0.0:0          LISTENING
  TCP    192.168.17.1:139         0.0.0.0:0          LISTENING
  TCP    192.168.56.1:139         0.0.0.0:0          LISTENING
  TCP    192.168.121.1:139        0.0.0.0:0          LISTENING
```

Le port d'écoute du serveur Terminal Server est : 3389

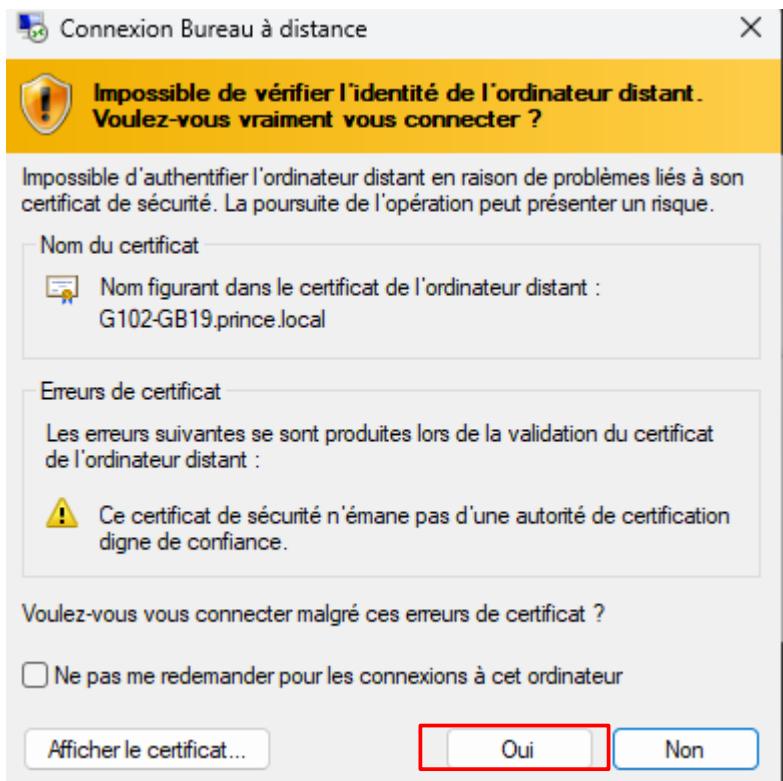
On procède maintenant à la connexion bureau à distance :



Autres choix

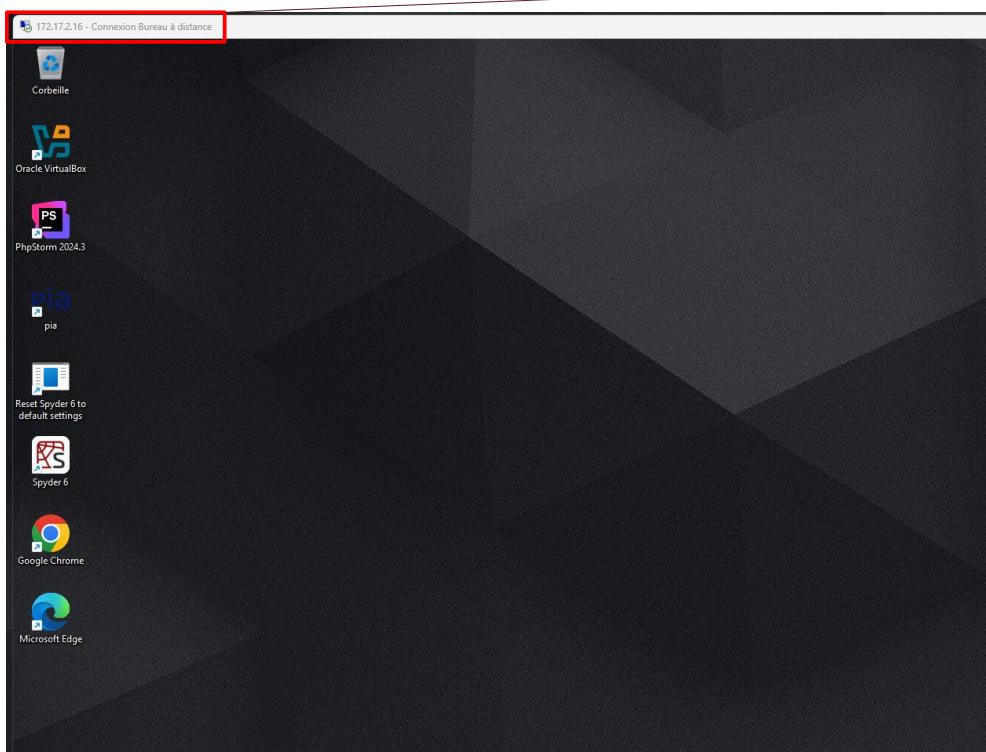
OK

Annuler



Communication  
bureau a distance  
établie

On a donc accès à  
la machine de  
mon voisin



Dans l'invite de commande de mon voisin je saisi la commande netstat -an :

```
Corbel [Administrator : Invité de commandes
Microsoft Windows [version 10.0.26200.6725]
(c) Microsoft Corporation. Tous droits réservés.

C:\Windows\System32>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  0.0.0.0:3389          0.0.0.0:0          LISTENING
TCP  0.0.0.0:5840          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  0.0.0.0:49701         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  172.17.2.16:130        0.0.0.0:0          LISTENING
TCP  172.17.2.16:3389        172.17.2.9:56478 ESTABLISHED
TCP  172.17.2.16:9009        0.0.0.0:0          LISTENING
TCP  172.17.2.16:49471       146.75.118.172:80 TIME_WAIT
TCP  172.17.2.16:49472       146.75.118.172:80 TIME_WAIT
TCP  172.17.2.16:49473       146.75.118.172:80 TIME_WAIT
TCP  172.17.2.16:49479       146.75.118.172:80 TIME_WAIT
TCP  172.17.2.16:49480       146.75.118.172:80 TIME_WAIT
```

On voit ici que la connexion au serveur Terminal Server est établie.

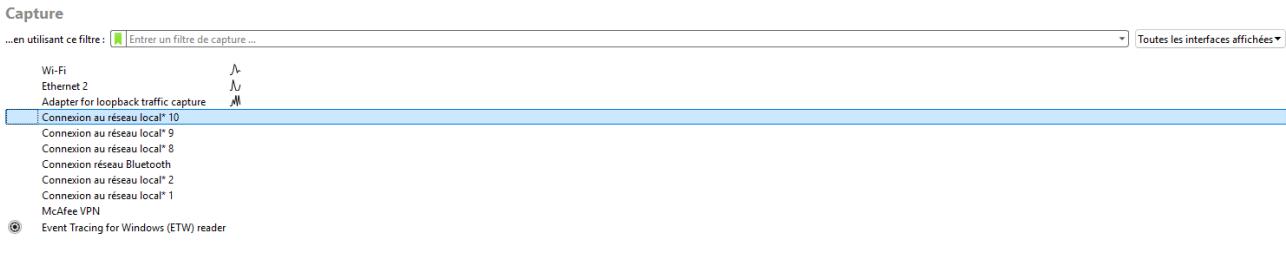
Pour finir on se DECONNECTE.

## 2. Capture de trames HTTP

On va à l'adresse [www.http2demo.io/](http://www.http2demo.io/) (capture 2 et 3 )et on lance un capture de trame sur Wireshark en même temps.



Capture 2



## Découvrir

Guide Utilisateur · Wiki · Questions et Réponses · Listes de diffusion · SharkFest · Discord Wireshark · Faire un don

Vous exécutez Wireshark 4.4.9 (v4.4.9-0-g57bf67214076). Vous recevez les mises à jour automatiques.

## Capture 3

On saisi ensuite la commande `nslookup www.http2demo.io` ( Capture 4 )dans l'invite de commande pour obtenir l'adresse IP du serveur web.

```
C:\Windows\System32>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::30
            2a02:6ea0:dc00::32
            79.127.138.14
            79.127.138.17
            79.127.138.20
Aliases:  www.http2demo.io

C:\Windows\System32>
```

@IP

(nous permet de filtrer par la suite les trames )

## Capture 4 : commande nslookup

On ping cette adresse ( Capture 5 ):

```
C:\Windows\System32>ping http2demo.io

Envoi d'une requête 'ping' sur http2demo.io [95.168.192.200] avec 32 octets de données :
Réponse de 95.168.192.200 : octets=32 temps=39 ms TTL=45
Réponse de 95.168.192.200 : octets=32 temps=36 ms TTL=45
Réponse de 95.168.192.200 : octets=32 temps=36 ms TTL=45
Réponse de 95.168.192.200 : octets=32 temps=40 ms TTL=45

Statistiques Ping pour 95.168.192.200:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 36ms, Maximum = 40ms, Moyenne = 37ms

C:\Windows\System32>
```

## Capture 5 : commande ping

ip.addr==89.187.167.39&&tcp.port==80						
No.	Time	Source	Destination	Protocol	Length	Info
123	2.599867	10.94.97.154	89.187.167.39	TCP	66	51643 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 ...
125	2.601302	10.94.97.154	89.187.167.39	TCP	66	52228 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 ...
132	2.632121	89.187.167.39	10.94.97.154	TCP	66	80 → 51643 [SYN, ACK] Seq=0 Ack=1 Win=61600 Len=...
133	2.632121	89.187.167.39	10.94.97.154	TCP	66	80 → 52228 [SYN, ACK] Seq=0 Ack=1 Win=61600 Len=...
135	2.632374	10.94.97.154	89.187.167.39	TCP	54	51643 → 80 [ACK] Seq=1 Ack=1 Win=65280 Len=0
136	2.632387	10.94.97.154	89.187.167.39	TCP	54	52228 → 80 [ACK] Seq=1 Ack=1 Win=65280 Len=0
158	2.710341	10.94.97.154	89.187.167.39	HTTP	635	GET / HTTP/1.1
165	2.744901	89.187.167.39	10.94.97.154	TCP	54	80 → 51643 [ACK] Seq=1 Ack=582 Win=61952 Len=0
168	2.763623	89.187.167.39	10.94.97.154	TCP	4254	80 → 51643 [PSH, ACK] Seq=1 Ack=582 Win=61952 Len=...

On repère la trame correspondant à la requête http ( méthode GET).

→ on développe la section correspondant au **protocole applicatif**  
**(Capture 6)**

\*Ethernet

Fichier Editer Vue Aller Capture Analyser Statistiques Téléphonie Wireless Outils Aide

http

No.	Time	Source	Destination	Protocol	Length	Info
65	1.913885	172.17.2.9	79.127.138.14	HTTP	514	514 [GET / HTTP/1.1]
73	1.925510	79.127.138.14	172.17.2.9	HTTP	1514	[TCP Previous segment not captured] Continuation
75	1.931145	79.127.138.14	172.17.2.9	HTTP	1514	Continuation
76	1.931145	79.127.138.14	172.17.2.9	HTTP	1514	Continuation
77	1.931145	79.127.138.14	172.17.2.9	HTTP	1514	Continuation
79	1.931533	79.127.138.14	172.17.2.9	HTTP	1514	Continuation
80	1.931533	79.127.138.14	172.17.2.9	HTTP	1514	Continuation
82	1.931577	79.127.138.14	172.17.2.9	HTTP	1514	Continuation
88	1.933205	172.17.2.9	79.127.138.14	HTTP	433	GET /css/style.css HTTP/1.1
91	1.939235	172.17.2.9	79.127.138.14	HTTP	437	GET /css/jssocials.css HTTP/1.1
94	1.941301	79.127.138.14	172.17.2.9	HTTP	141	HTTP/1.1 200 OK (text/css)
100	1.942252	172.17.2.9	79.127.138.14	HTTP	448	GET /css/jssocials-theme-flat.css HTTP/1.1
110	1.952189	79.127.138.14	172.17.2.9	HTTP	1094	HTTP/1.1 200 OK (text/css)
111	1.952189	79.127.138.14	172.17.2.9	HTTP	918	HTTP/1.1 200 OK (text/css)
112	1.953413	172.17.2.9	79.127.138.14	HTTP	440	GET /css/font-awesome.css HTTP/1.1
113	1.953498	172.17.2.9	79.127.138.14	HTTP	486	GET /img/refresh-icon.png HTTP/1.1
124	1.960772	79.127.138.14	172.17.2.9	HTTP	1101	HTTP/1.1 200 OK (text/css)
126	1.961259	172.17.2.9	79.127.138.14	HTTP	483	GET /img/cdn77logo.png HTTP/1.1
150	1.969721	172.17.2.9	79.127.138.14	HTTP	487	GET /img/logo-10gbpsio.png HTTP/1.1
151	1.969857	172.17.2.9	79.127.138.14	HTTP	495	GET /img/http2-bg.png HTTP/1.1
157	1.970135	79.127.138.14	172.17.2.9	HTTP	766	HTTP/1.1 200 OK (PNG)
166	1.974667	79.127.138.14	172.17.2.9	HTTP	1509	[TCP Spurious Retransmission] HTTP/1.1 200 OK (P)
171	1.979661	79.127.138.14	172.17.2.9	HTTP	1514	Continuation
172	1.979661	79.127.138.14	172.17.2.9	HTTP	1514	Continuation

```

> Frame 65: 532 bytes on wire (4256 bits), 532 bytes captured (4256 bits)
> Ethernet II, Src: GigaByteTech_2f:82:ce (74:56:3c:2f:82:ce), Dst: 79.127.138.14
> Internet Protocol Version 4, Src: 172.17.2.9, Dst: 79.127.138.14
> Transmission Control Protocol, Src Port: 64281, Dst Port: 80, Seq=1, Ack=1, Len=4256
  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/58.0.3029.80 Safari/537.36\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9, application/javascript;q=0.8, application/xml;q=0.9, application/xml+rss;q=0.9, image/webp,*/*;q=0.8\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=GA1.2.1742920644.1758205626; _ga_RCVW9W56Dj=GS2.2.\r\n
  Response in frame: 195
  Full request URI: http://www.http2demo.io/

```

```

0000 00 0d b4 2a a8 34 74 56 3c 2f 82 ce 08 00 45 00 ...*.4t
0010 02 06 2a f3 40 00 80 06 00 00 ac 11 02 09 4f 7f ...@...
0020 8a 0e fb 19 00 50 0e 3e 72 b1 9d 8b 82 10 6a 50 18 .....P>
0030 00 ff 89 a0 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 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 0e 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 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 61 2f 35 2e 30 28 57 69 6e Mozilla
00b0 64 6f 77 73 20 4e 54 20 31 30 2e 30 20 57 69 down NT
00c0 6e 36 34 3b 20 78 36 34 29 20 41 70 70 6c 65 57 n64; x6
00d0 55 62 4b 69 74 2f 35 33 37 2e 33 36 20 28 4b 48 ekit/5.
00e0 51 4d 4c 2c 20 6c 69 6b 65 20 47 65 63 6b 6f 29 TML, li
00f0 20 3 68 72 6f 6d 65 2f 31 34 31 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 57 2f 31 34 31 2e 30 2e 30 2d 0a 41 Edge/141
0120 63 63 65 70 74 3a 20 74 65 78 74 2f 68 74 6d 6c ccept: 1
0130 2c 61 78 0d 65 63 61 74 69 6f 2f 78 68 74 ,appli
0140 6d 6c 2b 78 6d 6c 61 70 70 6c 69 63 61 74 69 ml+xml,;
0150 6f 6e 2f 78 6d 6c 71 3d 30 2e 39 2c 69 6d 61 on/xml;;
0160 67 65 2f 61 78 66 2c 69 6d 61 67 65 2f 77 65 ge/avif,
0170 62 70 2c 69 6d 61 67 65 2f 61 70 66 67 2c 2a 2f bp,image
0180 2a 3b 71 3d 30 2e 38 2c 61 70 6c 69 63 61 74 *;q=0.8,
0190 69 6f 6e 2f 73 69 57 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;=b:
01b0 41 63 63 65 70 74 20 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 ezi. o

```

Capture 6 : Capture de trame Wireshark filtre http

→ on développe la section correspondant à l'**en-tête Transport** (Capture 7)

```

> Frame 65: 532 bytes on wire (4256 bits), 532 bytes captured (4256 bits) on interface \Device\NPF_{8981B1C5-27F7-4ECA-A7CC-B61CCD15\
> Ethernet II, Src: GigaByteTech_2f:82:ce (74:56:3c:2f:82:ce), Dst: Stormshield_2a:a8:34 (00:0d:b4:2a:a8:34)
> Internet Protocol Version 4, Src: 172.17.2.9, Dst: 79.127.138.14
> Transmission Control Protocol, Src Port: 64281, Dst Port: 80, Seq: 1, Ack: 1, Len: 478
Source Port: 64281
Destination Port: 80
[Stream index: 4]
[Stream Packet Number: 4]
> [Conversation completeness: Incomplete, DATA (15)]
[TCP Segment Len: 478]
Sequence Number: 1      (relative sequence number)
Sequence Number (raw): 1047703965
[Next Sequence Number: 479      (relative sequence number)]
Acknowledgment Number: 1      (relative ack number)
Acknowledgment number (raw): 7348556906
0181 .... = Header Length: 20 bytes (5)
> Flags: 0x018 (PSH, ACK)
Window: 255
[Calculated window size: 65280]
[Window size scaling factor: 256]
Checksum: 0x89ad [unverified]
[Checksum Status: Unverified]
Urgent Pointer: 0
> [Timestamps]
> [SEQ/ACK analysis]
TCP payload (478 bytes)

```

0020 8a 0e fb 19 00 50 3e 72 b1 9d 8b 82 10 6a 50 18	.... P> . . . . .
0030 00 ff 89 a0 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 2e	/1.1-Ho st: www.
0050 68 74 74 70 32 64 6d 6f 2e 69 6f 0d 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 28 57 69 6e	Mozilla/ 5.0 (Win
00b0 64 6f 77 73 28 4e 54 20 31 30 2e 30 3b 28 57 69	dows NT 10.0; Wi
00c0 6e 36 34 3b 28 78 2b 36 34 29 20 41 70 78 6c 65 57	n64; x64 ) AppleW
00d0 65 62 4b 69 74 2f 35 33 37 2e 33 36 28 28 48 48	eWebKit/53 7.36 (KH
00e0 54 4d 4c 2c 20 6d 69 6b 65 20 47 65 63 6b 6f 29	TML, like Gecko)
00f0 20 43 68 72 6f 6d 65 2f 31 34 31 2e 30 2e 30 2e 30 2e	Chrome/ 141.0.0.
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 34 31 29 30 2e 30 2e 30 0d 0a 41	Edg/141. 0.0.0..A
0120 63 63 65 70 74 3a 28 74 65 78 74 2f 68 74 6d 6c	ccept: t ext/html
0130 2c 61 70 78 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 78 6c 69 63 61 74 69	m+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 /apng,*
0180 2a 3b 71 3d 30 2e 38 2c 61 70 78 6c 69 63 61 74	*;q=0.8, applicat
0190 69 6f 6e 2f 73 69 67 6c 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;b3 ;q=0.7..
01b0 41 63 63 65 70 74 2d 45 6e 63 6f 64 69 6e 67 3a	Accept- E ncoding:
01c0 20 67 7a 69 70 2c 20 64 65 66 6c 61 74 65 0d 0a	gzip, d eflate..;
01d0 41 63 63 65 70 74 2d 4c 61 6e 67 75 61 67 65 3a	Accept- L anguage:
01e0 20 66 72 2c 66 72 2d 46 52 3b 71 3d 30 2e 39 2c	fr,fr-F R;q=0.9,
01f0 65 6e 3b 71 3d 30 2e 38 2c 65 6e 2d 47 42 3b 71	en;q=0.8 ,en-GB;q

## Capture 7

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

- On peut voir que le protocole utilisé est le protocole TCP.

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

- Le nom du PDU (Protocol Data Unit) encapsulant les données applicatives HTTP est le segment.

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

- La longueur de l'en-tête est de 14 octets ( Header Length =20 bytes (5)).

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

- Le port source 64281 en valeur **décimal** et FB39 en **hexadécimal**.
- Le port destination 80 en valeur **décimal** et 0050 en **hexadécimal**.

→ on développe la section correspondant à l'en-tête Réseau ( Capture 8 )

Frame 65: 532 bytes on wire (4256 bits), 532 bytes captured (4256 bits) on interface \Device\NPF\_{8981B1C5-27F7-4ECA-A7CC-B61CCD15A2E  
> Ethernet II, Src: GigaByteTech 2f:82:ce (74:56:3c:2f:82:ce), Dst: Stormshield\_2a:a8:34 (00:0d:b4:2a:a8:34)  
+ Internet Protocol Version 4, Src: 172.17.2.9, Dst: 79.127.138.14  
0100 .... = Version: 4  
.... 0101 [Header Length: 20 bytes (5)]  
> Differentiated Services Field: 0x00 (DSSCP: CS0, ECN: Not-ECT)  
Total Length: 518  
Identification: 0x2af3 (10995)  
> 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: 172.17.2.9  
Destination Address: 79.127.138.14  
[Stream index: 5]  
> Transmission Control Protocol, Src Port: 64281, Dst Port: 80, Seq: 1, Ack: 1, Len: 478  
> Hypertext Transfer Protocol

0000 00 0d b4 2a a8 34 74 56 3c 2f 82 ce 08 00 45 00 ... 4tV </...-E-  
0010 07 06 2a f3 40 00 80 06 00 0d ac 11 02 09 47 71 ... Pr ...jp  
0020 8a 0a fb 19 00 50 3e 72 b1 9d 8d 82 10 6a 50 18 ...P...O-  
0030 00 ff 89 a0 00 0d 47 45 54 2f 28 54 54 50 ..... GE T / HTTP  
0040 2f 31 2e 31 0d 0a 48 6f 73 74 3a 29 77 77 2e /1.1 - Ho st: www.  
0050 68 74 74 70 32 64 65 6d 6f 2e 69 6f 0d 0a 43 6f httpd2em o.io...Co  
0060 6e 6a 65 63 74 69 6f 6e 3a 28 6b 65 65 70 2d 61 nnection : keep-a  
0070 6c 69 76 65 0d 0a 55 70 67 72 61 65 65 2d 49 6e live : Up grade-In  
0080 73 65 63 75 72 65 2d 52 65 71 75 65 73 74 3a 29 secur...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 28 57 69 6e Mozilla/ 5.0 (win  
00b0 64 6f 77 73 20 44 54 20 31 30 2e 30 3b 20 57 69 dows NT 10.0; Wi  
00c0 6e 36 34 3b 20 78 36 34 29 2e 41 70 70 6c 65 57 n64; x64 ) AppleW  
00d0 65 62 4b 69 74 2f 35 33 37 2e 33 38 26 28 4b 48 ebkit/53.7.36 (KH  
00e0 54 4d 4c 2c 20 6c 69 6b 65 28 47 65 63 6b 6f 29 TNL, lik e Gecko)  
00f0 20 43 68 72 6f 6d 65 2f 31 34 31 2e 30 2e 30 2e Chrome/ 141.0.0.  
0100 30 20 53 61 66 61 72 69 24 35 33 37 2e 33 36 20 0 Safari /537.36  
0110 45 64 67 2f 31 34 31 2e 30 2e 30 2e 30 0d 0a 41 Edg/141.0.0.0 - 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 6d 2f 78 68 74 ,applica tion/xht  
0140 6d 6c 2b 78 6d 6c 2c 61 76 70 6c 69 63 61 74 69 ml+xml,a pplicati  
0150 6f 6c 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/wif, image/we  
0170 62 70 2c 69 6d 61 67 65 2f 61 70 6c 67 2c 2f bp,image /apng,/br  
0180 2a 3b 71 3d 30 2e 38 2c 61 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 65 3b 76 3d 62 33 3b 71 3d 30 2e 37 0d 0a nge;v=b3 ;q=0.7..  
01b0 41 63 63 65 70 74 2d 45 66 63 6f 64 69 66 67 3a Accept-E ncoding:  
01c0 20 67 7a 69 70 2c 20 64 65 66 6c 61 74 65 0d 0a gzip, d eflate..  
01d0 41 63 63 65 70 74 2d 4c 61 6e 67 75 61 67 65 3a Accept-L anguage:

Capture 8

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

La longueur de l'en-tête réseau est de 20 octets ( bytes)

### ---Valeur et signification du champ protocole :

- La valeur présente dans le champ protocole est le « 06 » ce qui signifie que le protocole suivant est le protocole TCP. Il y aura donc un segment TCP.

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

IP source : 172.17.2.9

soit en hexadécimale : AC.11.02.09

IP destination : 79.127.138.14

soit en hexadécimale : 4F.7F.8A.0E

→ on développe la section correspondant à l'en-tête Ethernet ( Capture 9 )

```
> Frame 65: 532 bytes on wire (4256 bits), 532 bytes captured (4256 bits) on interface \Device\NPF_{8981B1C5-27F7-4FC4-A76C-801CLD15A2E}
> Ethernet II, Src: GigaByteTech_2f:82:ce (74:56:3c:2f:82:ce), 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:82:ce (74:56:3c:2f:82:ce)
> Type: IPv4 (0x0800)
[Stream index: 1]
> Internet Protocol Version 4, Src: 172.17.2.9, Dst: 79.127.138.14
> Transmission Control Protocol, Src Port: 64281, Dst Port: 80, Seq: 1, Ack: 1, Len: 478
> Hypertext Transfer Protocol
0000  00 0d b4 2a a8 34 74 56 3c 2f 82 e1 08 00 45 00  ...*4tV </...E
0010  00 0d b4 2a a8 34 74 56 3c 2f 82 e1 08 00 45 00  ...@...-...-0
0020  00 ff 89 a0 00 00 47 45 54 20 2f 20 48 54 54 50  ....GE T / HTTP
0030  00 ff 89 a0 00 00 47 45 54 20 2f 20 48 54 54 50  ...@...-...-0
0040  2f 31 2e 31 0d 0a 48 6f 73 74 3a 20 77 77 77 20  /1.1-Ho st: www.
0050  68 74 70 32 64 65 6d 6f 2e 69 6f 0d 0a 43 6f  http2dem.o.io-Co
0060  6e 6e 65 74 69 6f 6d 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 6a  live-Up grade-In
0080  73 65 63 72 65 2d 52 65 71 75 65 73 74 3a 20  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 63 61 2f 35 2e 30 28 57 69 6a Mozilla/ 5.0 (Win
00b0  64 6f 77 73 20 4e 54 20 31 30 2e 30 3b 2d 57 69  dows NT 10.0; Wi
00c0  6e 36 34 3b 20 78 36 34 29 20 41 70 70 65 57  n64; x64 ) AppleW
00d0  65 62 4b 69 74 2f 35 33 37 2e 33 36 20 28 4b 48  ekit/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 34 31 2e 30 2e 30 2e  Chrome/ 141.0.0.
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 34 31 2e 30 2e 30 00 0a 41  Edg/141.0.0.0_A
0120  63 63 65 70 74 3a 20 74 65 78 74 2f 68 74 6d 6a  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 plicati
0150  67 6e 2f 78 6d 6c 71 3d 30 2e 39 2c 69 6d 61  on/xmlq ,o.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 2f  bp,image /apng,/
0180  2a 59 71 5d 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  41 63 63 65 78 74 2d 45 66 63 6f 64 69 6e 67 3a Accept-E ncoding:
01c0  20 67 7a 69 70 2c 20 64 65 66 6c 61 74 65 0d 0a gzip, d eflate-
01d0  41 63 63 65 70 74 2d 4c 61 6e 67 75 61 67 65 3a Accept-L anguge:
```

### ---Valeur et signification du champ EtherType :

- Le champ Ethertype se trouve à la fin de l'en-tête Ethernet ( 2 derniers octets). C'est ici la valeur 0800 caractéristique du protocole IPv4.

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

- MAC source est :** 00:0d:b4:2a:a8:34
- MAC destination est :** 74:56:3c:2f:82:ce

### ---Trames associées à la mise en place de la connexion TCP entre le client et le serveur

47 2.314600	192.168.1.92	192.168.1.254	TCP	66 61339 → 53 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
48 2.319402	192.168.1.254	192.168.1.92	TCP	66 53 → 61339 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1400 SACK_PERM WS=128
49 2.319510	192.168.1.92	192.168.1.254	TCP	54 61339 → 53 [ACK] Seq=1 Ack=1 Win=65280 Len=0

Les adresses IP sont différentes du reste du TP car cette partie a été faite avec mon ordinateur personnel

### ---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 Ack est la première trame du client vers le serveur. Le client demande ici une demande de liaison au serveur .

```
> Frame 47: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF_{0E4E2D6F-8D02-4ABA-8184-DCAC8E12FBF5}, id 0
> Ethernet II, Src: LiteonTechno_f1:07:13 (24:b2:b9:f1:07:13), Dst: VantivaUSA_ec:c4:3c (d0:5a:00:ec:c4:3c)
> Internet Protocol Version 4, Src: 192.168.1.92, Dst: 192.168.1.254
> Transmission Control Protocol, Src Port: 61339, Dst Port: 53, Seq: 0, Len: 0
    Source Port: 61339
    Destination Port: 53
    [Stream index: 13]
    [Stream Packet Number: 1]
    > [Conversation completeness: Complete, WITH_DATA (31)]
    [TCP Segment Len: 0]
    Sequence Number: 0      (relative sequence number)
    Sequence Number (raw): 3641839720
    [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: 0x111a [unverified]
        [Checksum Status: Unverified]
        Urgent Pointer: 0
    > Options: (12 bytes), Maximum segment size, No-Operation (NOP), Window scale, No-Operation (NOP), No-Operation (NOP), SACK permitted
    > [Timestamps]
```

Puis le SYN/ACK signifie que le serveur a bien reçu cette demande qu'il accepte et qu'il en demande un en retour .

```
> Frame 48: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF_{0E4E2D6F-8D02-4ABA-8184-DCAC8E12FBF5}, id 0
> Ethernet II, Src: VantivaUSA_ec:c4:3c (d0:5a:00:ec:c4:3c), Dst: LiteonTechno_f1:07:13 (24:b2:b9:f1:07:13)
> Internet Protocol Version 4, Src: 192.168.1.92, Dst: 192.168.1.254
> Transmission Control Protocol, Src Port: 53, Dst Port: 61339, Seq: 0, Ack: 1, Len: 0
    Source Port: 53
    Destination Port: 61339
    [Stream index: 13]
    [Stream Packet Number: 2]
    > [Conversation completeness: Complete, WITH_DATA (31)]
    [TCP Segment Len: 0]
    Sequence Number: 0      (relative sequence number)
    Sequence Number (raw): 1672999154
    [Next Sequence Number: 1      (relative sequence number)]
    Acknowledgment Number: 1      (relative ack number)
    Acknowledgment number (raw): 3641839721
    1000 .... = Header Length: 32 bytes (8)
    > Flags: 0x01 (SYN, ACK)
        Window: 64240
        [Calculated window size: 64240]
        Checksum: 0xc1aa [unverified]
        [Checksum Status: Unverified]
        Urgent Pointer: 0
    > Options: (12 bytes), Maximum segment size, No-Operation (NOP), No-Operation (NOP), SACK permitted, No-Operation (NOP), Window scale
    > [Timestamps]
    > [SEQ/ACK analysis]
```

Enfin le ACK est l'accusé de réception de du client.

C'est 3 trames constituent le 3 way handshake

```

> Frame 49: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface \Device\NPF_{0E4E2D6F-8D02-4ABA-8184-DCAC8E12FBF5}, id 0
> Ethernet II, Src: LiteonTechno_f1:07:13 (24:b2:b9:f1:07:13), Dst: VantivaUSA_ec:c4:3c (d0:5a:00:ec:c4:3c)
> Internet Protocol Version 4, Src: 192.168.1.92, Dst: 192.168.1.254
> Transmission Control Protocol, Src Port: 61339, Dst Port: 53, Seq: 1, Ack: 1, Len: 0
    Source Port: 61339
    Destination Port: 53
    [Stream index: 13]
    [Stream Packet Number: 3]
    > [Conversation completeness: Complete, WITH_DATA (31)]
    [TCP Segment Len: 0]
    Sequence Number: 1      (relative sequence number)
    Sequence Number (raw): 3641839721
    [Next Sequence Number: 1      (relative sequence number)]
    Acknowledgment Number: 1      (relative ack number)
    Acknowledgment number (raw): 1672999155
    0101 .... = Header length: 20 bytes (5)
    > Flags: 0x010 (ACK) ACK
    Window: 255
    [Calculated window size: 65280]
    [Window size scaling factor: 256]
    Checksum: 0xfc32 [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
    > [Timestamps]
    > [SEQ/ACK analysis]

```

Ce mode connecté est mis en place pour :

- Assurer la **fiabilité** puisque chaque segment est accusé de réception.
- Assurer le **séquencement** : ils arrivent dans le bon ordre.
- Et garantir l'**intégrité**.

RIS : remise, intégrité , séquencement