

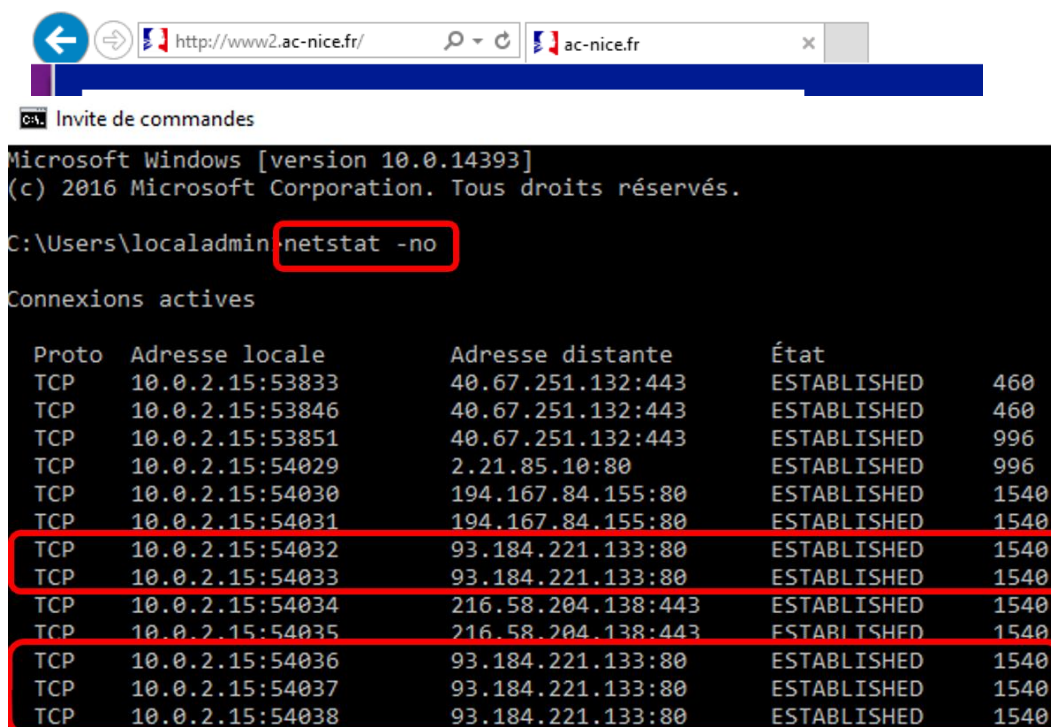
## TP3 – Les ports logiciels

### Sommaire

1. Connexion Bureau à distance (RDP)..... 1
2. Capture de trames HTTP..... 6

**Rappel :** la commande **netstat** (network statistics) permet sur une **machine Windows** d'obtenir des informations sur les **connexions réseau en cours** sur la machine ainsi qu'un certain nombre de statistiques.

- ☞ La commande netstat **sans attribut** n'affiche que les **connexions TCP actives** (état « **Established** »).
- ☞ **netstat -a** (a pour all) affiche toutes les **connexions TCP actives** (état « **Established** ») ainsi que les **ports TCP et UDP d'écoute** (état « **Listening** »).
- ☞ **netstat -n** affiche les **numéros de port** au format numérique **sans résolution de nom**.



```
Microsoft Windows [version 10.0.14393]
(c) 2016 Microsoft Corporation. Tous droits réservés.

C:\Users\localadmin>netstat -n

Connexions actives

Proto  Adresse locale        Adresse distante       État                    PID
TCP    10.0.2.15:53833        40.67.251.132:443      ESTABLISHED            460
TCP    10.0.2.15:53846        40.67.251.132:443      ESTABLISHED            460
TCP    10.0.2.15:53851        40.67.251.132:443      ESTABLISHED            996
TCP    10.0.2.15:54029        2.21.85.10:80          ESTABLISHED            996
TCP    10.0.2.15:54030        194.167.84.155:80      ESTABLISHED            1540
TCP    10.0.2.15:54031        194.167.84.155:80      ESTABLISHED            1540
TCP    10.0.2.15:54032        93.184.221.133:80      ESTABLISHED            1540
TCP    10.0.2.15:54033        93.184.221.133:80      ESTABLISHED            1540
TCP    10.0.2.15:54034        216.58.204.138:443     ESTABLISHED            1540
TCP    10.0.2.15:54035        216.58.204.138:443     ESTABLISHED            1540
TCP    10.0.2.15:54036        93.184.221.133:80      ESTABLISHED            1540
TCP    10.0.2.15:54037        93.184.221.133:80      ESTABLISHED            1540
TCP    10.0.2.15:54038        93.184.221.133:80      ESTABLISHED            1540
```

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

**Remote Desktop Protocol (RDP)** est un protocole qui permet à un utilisateur de se connecter sur un serveur Windows **Terminal Server**.

- Demandez à votre voisin l'adresse IP **172.17.X.Y** obtenue par la carte réseau de sa machine physique.
- 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** :
  - ☞ Le pare-feu de Windows bloque par défaut le protocole ICMP qui permet d'effectuer des pings sur les machines. Pour pouvoir autoriser les trames ICMP, allez dans **Pare-feu Windows avec fonctions avancées de sécurité / Règles de trafic entrant**. Créez une règle afin d'autoriser les trames ICMP à entrer :

**Type de règle**

Sélectionnez le type de règle de pare-feu à créer.

**Étapes :**

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

Quel type de règle voulez-vous créer ?

☐ **Programme**  
Règle qui contrôle les connexions d'un programme.

☐ **Port**  
Règle qui contrôle les connexions d'un port TCP ou UDP.

☐ **Prédéfinie :**  
@FirewallAPI.dll,-80200  
Règle qui contrôle les connexions liées à l'utilisation de Windows.

☒ **Personnalisée**  
Règle personnalisée.

**Protocole et ports**

Spécifiez les protocoles et les ports auxquels s'applique cette règle.

**Étapes :**

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

À quels ports et protocoles cette règle s'applique-t-elle ?

Type de protocole : ICMPv4

Numéro de protocole : 1

Port local : Tous les ports

Exemple : 80, 443, 5000-5010

Port distant : Tous les ports

Exemple : 80, 443, 5000-5010

Paramètres ICMP (Internet Control Message Protocol) : Perso...

**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

**À 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...

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

☒ Toute adresse IP

☐ Ces adresses IP :

Ajouter...  
Modifier...  
Supprimer

## 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

## Nom

Spécifier le nom et la description de cette règle.

### Étapes :

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

Nom :

ICMP

Description (facultatif) :

➡ Procédez de la même façon pour le **trafic sortant** (sélectionnez **Autoriser la connexion**).

- Cliquez droit sur le bouton **Démarrer** de votre station et sélectionnez **Système** puis **Bureau à distance**. Activez le Bureau à distance :

### Liens apparentés



Clé de produit et activation

Mettez à niveau votre édition de Windows ou modifiez la clé de produit (Product Key)



Bureau à distance

Contrôlez cet appareil à partir d'un autre.



## Système > Bureau à distance



Bureau à distance

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

Désactivé



Utilisateurs du Bureau à distance

Sélectionner qui peut accéder à distance à ce PC



### Paramètres du Bureau à distance


#### Activer le Bureau à distance ?

Vous et les utilisateurs sélectionnés sous Comptes de l'utilisateur pourrez vous connecter à distance à cet ordinateur.


Confirmer

Annuler


## Système > Bureau à distance


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

Activé 

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

PC-01

 **Utilisateurs du Bureau à distance**  
Sélectionner qui peut accéder à distance à ce PC



Utilisateurs du Bureau à distance

Les utilisateurs ci-dessous peuvent se connecter à cet ordinateur, ainsi que les membres du groupe Administrateurs, même s'ils n'apparaissent pas ici.

Ajouter... Supprimer

Pour créer des nouveaux comptes d'utilisateur ou ajouter des utilisateurs aux groupes, ouvrez [Comptes d'utilisateur](#) dans le Panneau de configuration.

OK Annuler

Votre compte de domaine est membre du groupe Administrateurs sur chaque machine physique

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

```
C:\> Invite de commandes

Microsoft Windows [version 10.0.19043.1237]
(c) Microsoft Corporation. Tous droits réservés.

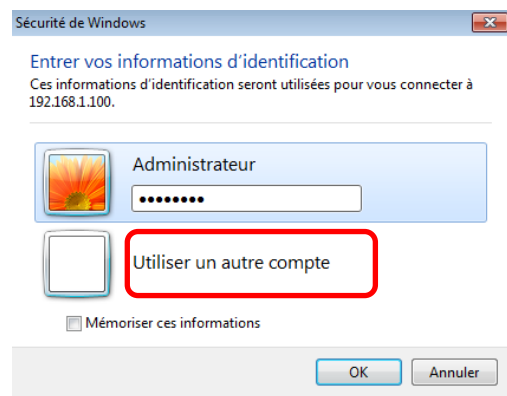
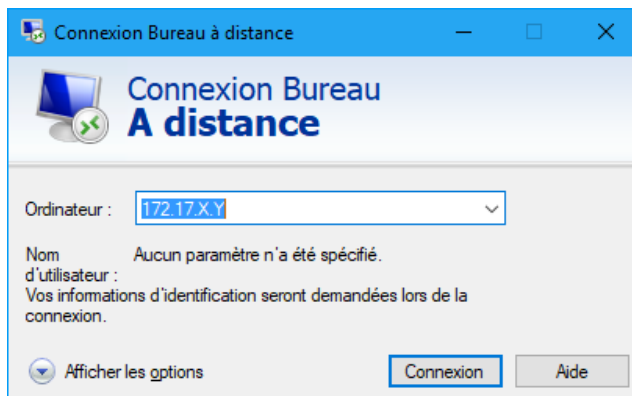
C:\Users\phbou>netstat -an

Connexions actives

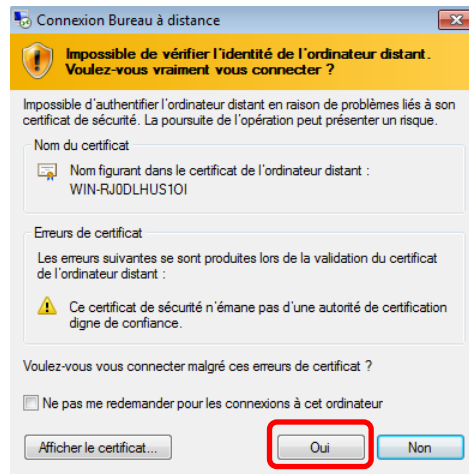
Proto  Adresse locale      Adresse distante     État
TCP    0.0.0.0:135          0.0.0.0:0            LISTENING
TCP    0.0.0.0:443          0.0.0.0:0            LISTENING
TCP    0.0.0.0:445          0.0.0.0:0            LISTENING
TCP    0.0.0.0:903          0.0.0.0:0            LISTENING
TCP    0.0.0.0:913          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    0.0.0.0:5357         0.0.0.0:0            LISTENING
```

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

- A partir de votre **station physique**, saisissez **mstsc** dans la **zone de recherche** (programme **Connexion Bureau à distance**).
- 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**) :



- Cliquez sur **Oui** :



- Vous accédez à la machine Windows 11 de votre voisin :



- 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 :

```

C:\Users\Administrateur>netstat -an

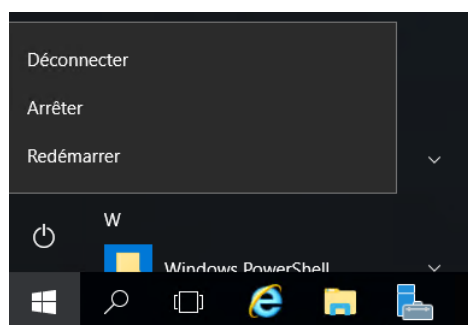
Connexions actives

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 0.0.0.0:47001 0.0.0.0:0 LISTENING
TCP 0.0.0.0:49152 0.0.0.0:0 LISTENING
TCP 0.0.0.0:49153 0.0.0.0:0 LISTENING
TCP 0.0.0.0:49154 0.0.0.0:0 LISTENING
TCP 0.0.0.0:49155 0.0.0.0:0 LISTENING
TCP 0.0.0.0:49156 0.0.0.0:0 LISTENING
TCP 192.168.1.100:139 0.0.0.0:0 LISTENING
TCP 192.168.1.100:3389 192.168.1.200:49215 ESTABLISHED
TCP [::]:135 [::]:0 LISTENING
TCP [::]:445 [::]:0 LISTENING
TCP [::]:3389 [::]:0 LISTENING
TCP [::]:47001 [::]:0 LISTENING
TCP [::]:49152 [::]:0 LISTENING
TCP [::]:49153 [::]:0 LISTENING

```

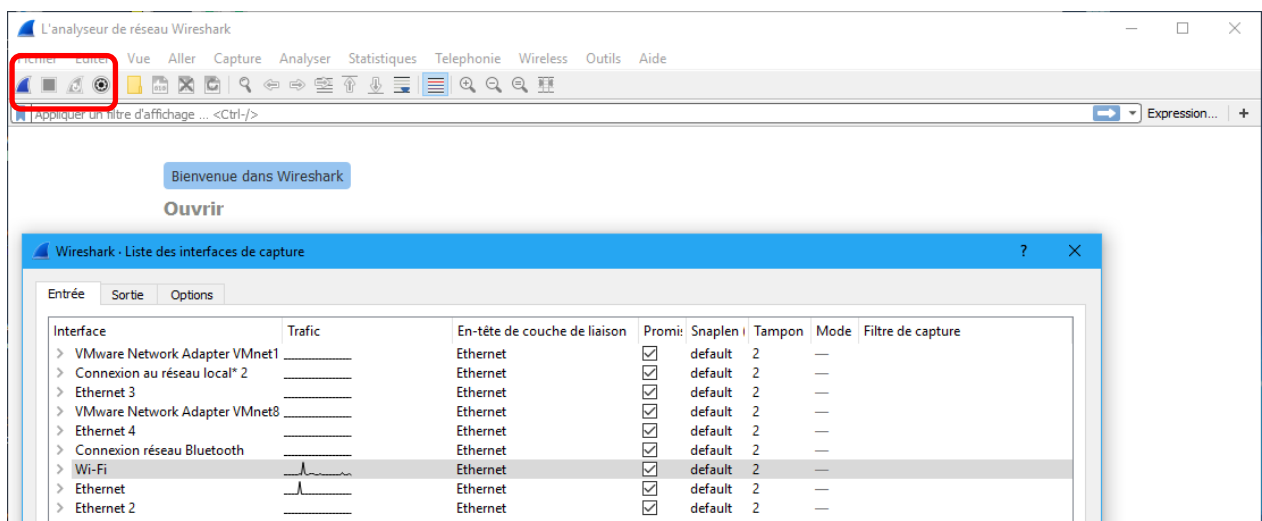
IP en 172.17.X.Y  
pour vous

- Cliquez droit sur **Démarrer** puis sur **Déconnecter** pour fermer la connexion à distance (ne pas cliquer sur la croix !) :



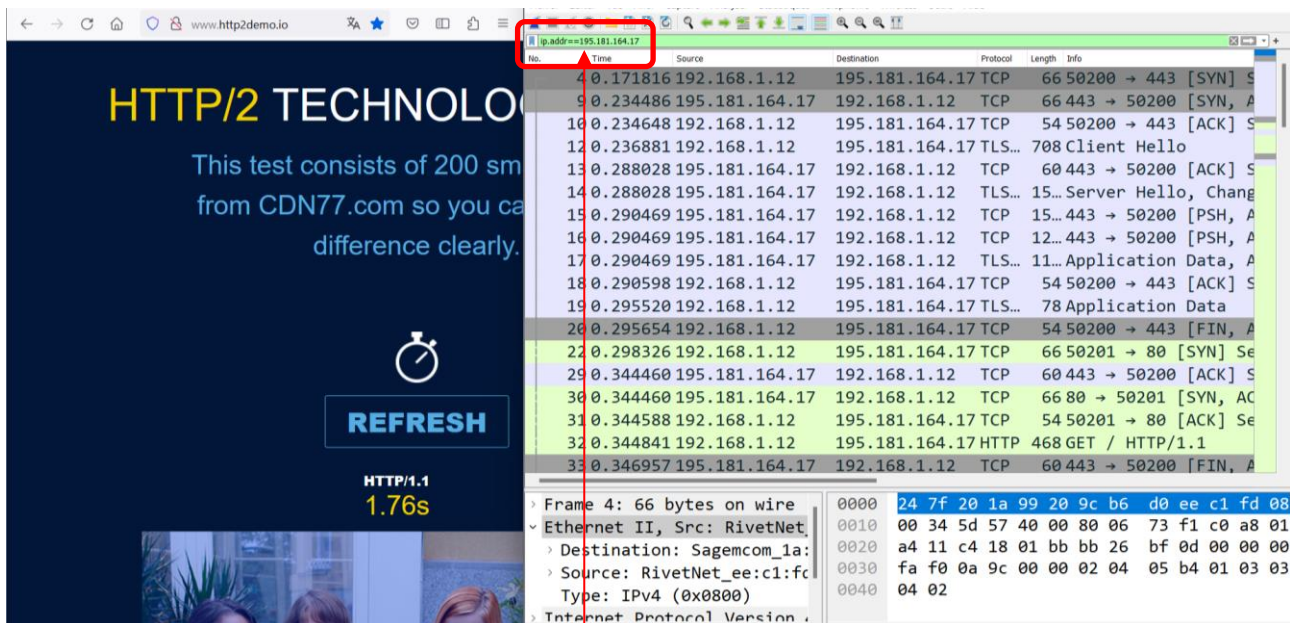
## 2. Capture de trames HTTP.

- A partir de votre station physique, lancez Wireshark en tant qu'administrateur (cliquez droit sur le programme Wireshark puis sélectionner **Exécuter en tant qu'administrateur**), sélectionnez votre carte réseau afin de démarrer la capture de trames (carte Ethernet physique pour vous) :



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





- Arrêtez la capture et appliquez un **filtre** 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 :
  - ➔ Saisissez, depuis l'invite de commandes, la commande **nslookup www.http2demo.io** pour obtenir l'adresse IP du serveur web (enregistrement **www** associé au nom de domaine **http2demo.io**).

```

Microsoft Windows [version 10.0.22631.4169]
(c) Microsoft Corporation. Tous droits réservés.

C:\Users\phbou>nslookup www.http2demo.io
Serveur : livebox.home
Address: 192.168.1.1

Réponse ne faisant pas autorité :
Nom : 1906714720.rsc.cdn77.org
Addresses: 2a02:6ea0:c700::18
           2a02:6ea0:c700::112
           2a02:6ea0:c700::107
           2a02:6ea0:c700::21
           2a02:6ea0:c700::101
           2a02:6ea0:c700::19
           2a02:6ea0:c700::11
           169.150.255.184
           169.150.255.180
           37.19.194.81
           212.102.56.179
           195.181.170.18
           195.181.175.41
           207.211.211.26
Aliases: www.http2demo.io
  
```

```

Microsoft Windows [version 10.0.22631.5768]
(c) Microsoft Corporation. Tous droits réservés.

C:\Users\phbou>nslookup www.http2demo.io
Serveur : livebox.home
Address: 2a01:cb1d:79a:4c00:267f:20ff:fe1a:9920

Réponse ne faisant pas autorité :
Nom : 1906714720.rsc.cdn77.org
Addresses: 2a02:6ea0:ca00::7
           2a02:6ea0:ca00::8
           89.187.167.42
           89.187.167.38
           84.17.50.8
Aliases: www.http2demo.io
  
```

- Repérez la trame correspondant à votre requête http (demande de la page d'accueil du site) et développez la section correspondant au **protocole applicatif** :

Wireshark packet capture showing an HTTP GET request. The packet list on the left shows a GET request from 192.168.1.12 to 195.181.164.17. The packet details pane on the right shows the Hypertext Transfer Protocol section with the request line 'GET / HTTP/1.1' and various headers. The packet bytes pane on the right shows the raw data in hexadecimal and ASCII.

- Développez la section correspondant à l'en-tête Transport :

Wireshark packet capture showing the Transport section of the HTTP request. The packet details pane on the right shows the Transmission Control Protocol section with the sequence number 2865989900 and the acknowledgment number 1524618516. The packet bytes pane on the right shows the raw data in hexadecimal and ASCII.

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

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

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

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

- Développez la section correspondant à l'en-tête Réseau :



Frame 40: 468 bytes on wire (3744 bits), 468 bytes captured (3744 bits) on interface 0	0000	24 7f 20 1a 99 20 9c b6 d0 ee c1 fd 08 00 45 00	\$ . . . . . E .
Ethernet II, Src: RivetNet ee:c1:fd (9c:b6:d0:ee:c1:fd), Dst: Sagemcom_1a:99:20 (24:7f:20:1a:99:20)	0010	01 c6 5c f8 40 00 80 06 72 be c0 a8 01 0c c3 b5	.. \ . @ . . . r . . . . .
Internet Protocol Version 4, Src: 192.168.1.12, Dst: 195.181.164.17	0020	a4 11 c3 b0 00 50 aa d3 89 0c 5a df d5 14 50 18	.... P . . . . Z . . . . P .
Version: 4	0030	01 fe f1 08 00 00 47 45 54 20 2f 20 48 54 54 50	.... GE T / HTTP
Header Length: 20 bytes (5)	0040	2f 31 2e 31 0d 0a 48 6f 73 74 3a 20 77 77 77 2e	/1.1..Ho st: www.
Differentiated Services Field: 0x00 (DSCP: CS0)	0050	68 74 74 70 32 64 65 6d 6f 2e 69 6f 0d 0a 55 73	http2dem o.io..Us
Total Length: 454	0060	65 72 2d 41 67 65 6e 74 3a 20 4d 6f 7a 69 6c 6c	er-Agent : Mozill
Identification: 0x5cf8 (23800)	0070	61 2f 35 2e 30 20 28 57 69 6e 64 6f 77 73 20 4e	a/5.0 (W indows N
Flags: 0x2, Don't fragment	0080	54 20 31 30 2e 30 3b 20 57 69 6e 36 34 3b 20 78	T 10.0; Win64; x
Fragment Offset: 0	0090	36 34 3b 20 72 76 3a 31 30 39 2e 30 29 20 47 65	64; rv:1 09.0) Ge
Time to Live: 128	00a0	63 6b 6f 2f 32 30 31 30 30 31 30 31 20 46 69 72	cko/2010 0101 Fir
Protocol: TCP (6)	00b0	65 66 6f 78 2f 31 31 38 2e 30 0d 0a 41 63 63 65	efox/118 .0..Acce
Header Checksum: 0x72be [validation disabled]	00c0	70 74 3a 20 74 65 78 74 2f 68 74 6d 6c 2c 61 70	pt: text /html,ap
[Header checksum status: Unverified]	00d0	70 6c 69 63 61 74 69 6f 6e 2f 78 68 74 6d 6c 2b	plicatio n/xhtmll+
Source Address: 192.168.1.12	00e0	78 6d 6c 2c 61 70 70 6c 69 63 61 74 69 6f 6e 2f	xml,appl ication/
Destination Address: 195.181.164.17	00f0	78 6d 6c 3b 71 3d 30 2e 39 2c 69 6d 61 67 65 2f	xml;q=0. 9,image/
	0100	61 76 69 66 2c 69 6d 61 67 65 2f 77 65 62 70 2c	avif,ima ge/webp,
	0110	2a 2f 2a 3b 71 3d 30 2e 38 0d 0a 41 63 63 65 70	*/*;q=0. 8..Accep
	0120	74 2d 4c 61 6e 67 75 61 67 65 3a 20 66 72 2c 66	t-Langua ge: fr,f
	0130	72 2d 46 52 3b 71 3d 30 2e 38 2c 65 6e 2d 55 53	r-FR;q=0 .8,en-US

- Quelle est la longueur de l'en-tête de réseau ?  
\_\_\_\_\_
- Repérez le **champ Protocole** figurant dans l'en-tête Réseau. Quelle est la valeur présente ?  
Que signifie-t-elle ?  
\_\_\_\_\_
- Quelles sont les valeurs décimales et hexadécimales des **adresses IP source et destination** ?  
\_\_\_\_\_
- Développez la section correspondant à l'**en-tête Ethernet** :  
\_\_\_\_\_

Frame 40: 468 bytes on wire (3744 bits), 468 bytes captured (3744 bits) on interface 0	0000	24 7f 20 1a 99 20 9c b6 d0 ee c1 fd 08 00 45 00	\$ . . . . . E .
Ethernet II, Src: RivetNet ee:c1:fd (9c:b6:d0:ee:c1:fd), Dst: Sagemcom_1a:99:20 (24:7f:20:1a:99:20)	0010	01 c6 5c f8 40 00 80 06 72 be c0 a8 01 0c c3 b5	.. \ . @ . . . r . . . . .
Destination: Sagemcom_1a:99:20 (24:7f:20:1a:99:20)	0020	a4 11 c3 cb 00 50 aa d3 89 0c 5a df d5 14 50 18	.... P . . . . Z . . . . P .
Source: RivetNet ee:c1:fd (9c:b6:d0:ee:c1:fd)	0030	01 fe f1 08 00 00 47 45 54 20 2f 20 48 54 54 50	.... GE T / HTTP
Type: IPv4 (0x0800)	0040	2f 31 2e 31 0d 0a 48 6f 73 74 3a 20 77 77 77 2e	/1.1..Ho st: www.
Internet Protocol Version 4, Src: 192.168.1.12, Dst: 195.181.164.17	0050	68 74 74 70 32 64 65 6d 6f 2e 69 6f 0d 0a 55 73	http2dem o.io..Us
Transmission Control Protocol, Src Port: 50123, Dst Port: 80	0060	65 72 2d 41 67 65 6e 74 3a 20 4d 6f 7a 69 6c 6c	er-Agent : Mozill
Hypertext Transfer Protocol	0070	61 2f 35 2e 30 20 28 57 69 6e 64 6f 77 73 20 4e	a/5.0 (W indows N
	0080	54 20 31 30 2e 30 3b 20 57 69 6e 36 34 3b 20 78	T 10.0; Win64; x
	0090	36 34 3b 20 72 76 3a 31 30 39 2e 30 29 20 47 65	64; rv:1 09.0) Ge
	00a0	63 6b 6f 2f 32 30 31 30 30 31 30 31 20 46 69 72	cko/2010 0101 Fir
	00b0	65 66 6f 78 2f 31 31 38 2e 30 0d 0a 41 63 63 65	efox/118 .0..Acce
	00c0	70 74 3a 20 74 65 78 74 2f 68 74 6d 6c 2c 61 70	pt: text /html,ap
	00d0	70 6c 69 63 61 74 69 6f 6e 2f 78 68 74 6d 6c 2b	plicatio n/xhtmll+
	00e0	78 6d 6c 2c 61 70 70 6c 69 63 61 74 69 6f 6e 2f	xml,appl ication/
	00f0	78 6d 6c 3b 71 3d 30 2e 39 2c 69 6d 61 67 65 2f	xml;q=0. 9,image/
	0100	61 76 69 66 2c 69 6d 61 67 65 2f 77 65 62 70 2c	avif,ima ge/webp,
	0110	2a 2f 2a 3b 71 3d 30 2e 38 0d 0a 41 63 63 65 70	*/*;q=0. 8..Accep
	0120	74 2d 4c 61 6e 67 75 61 67 65 3a 20 66 72 2c 66	t-Langua ge: fr,f
	0130	72 2d 46 52 3b 71 3d 30 2e 38 2c 65 6e 2d 55 53	r-FR;q=0 .8,en-US

- Repérez le **champ EtherType**. Quel est la valeur contenue ? Que signifie-t-elle ?  
\_\_\_\_\_
- Quelles sont les valeurs des **adresses MAC destination et source** ?  
\_\_\_\_\_
- Modifiez le filtre et réalisez une capture d'écran des 3 trames mettant en place la **connexion TCP** entre le client et le serveur (cf. Chapitre 4 - pages 2, 3 et 8 : Three-way handshake).

Time	Source	Destination	Protocol	Length	Info
40.171816	192.168.1.12	195.181.164.17	TCP	66	50200 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
90.234486	195.181.164.17	192.168.1.12	TCP	66	443 → 50200 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM WS=51
100.234648	192.168.1.12	195.181.164.17	TCP	54	50200 → 443 [ACK] Seq=1 Ack=1 Win=131328 Len=0
120.236881	192.168.1.12	195.181.164.17	TLS...	708	Client Hello
130.288028	195.181.164.17	192.168.1.12	TCP	60	443 → 50200 [ACK] Seq=1 Ack=655 Win=64512 Len=0
140.288028	195.181.164.17	192.168.1.12	TLS...	15...	Server Hello, Change Cipher Spec, Application Data
150.290469	195.181.164.17	192.168.1.12	TCP	15...	443 → 50200 [PSH, ACK] Seq=1461 Ack=655 Win=64512 Len=1460 [TCP segment of
160.290469	195.181.164.17	192.168.1.12	TCP	12...	443 → 50200 [PSH, ACK] Seq=2921 Ack=655 Win=64512 Len=1176 [TCP segment of
170.290469	195.181.164.17	192.168.1.12	TLS...	11...	Application Data, Application Data, Application Data
180.290598	192.168.1.12	195.181.164.17	TCP	54	50200 → 443 [ACK] Seq=655 Ack=5192 Win=131328 Len=0
190.295520	192.168.1.12	195.181.164.17	TLS...	78	Application Data
200.295654	192.168.1.12	195.181.164.17	TCP	54	50200 → 443 [FIN, ACK] Seq=679 Ack=5192 Win=131328 Len=0
220.298326	192.168.1.12	195.181.164.17	TCP	66	50201 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
250.333817	192.168.1.12	34.107.221.82	TCP	66	50202 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
290.344460	195.181.164.17	192.168.1.12	TCP	60	443 → 50200 [ACK] Seq=5192 Ack=679 Win=64512 Len=0
300.344460	195.181.164.17	192.168.1.12	TCP	66	80 → 50201 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM WS=512
310.344588	192.168.1.12	195.181.164.17	TCP	54	50201 → 80 [ACK] Seq=1 Ack=1 Win=131328 Len=0
320.344841	192.168.1.12	195.181.164.17	HTTP	468	GET / HTTP/1.1

Frame 4: 66 bytes on wire (528 bits), 66 bytes	0000	24 7f 20 1a 99 20 9c b6 d0 ee c1 fd 08 00 45 00	\$. . . . .E.
↳ Ethernet II, Src: RivetNet_ee:c1:fd (9c:b6:d0:ee:c1:fd),	0010	00 34 5d 57 40 00 80 06 73 f1 c0 a8 01 0c c3 b5	-4]w@... s.....
↳ Destination: Sagemcom_1a:99:20 (24:7f:20:1a:99:20)	0020	a4 11 c4 18 01 bb bb 26 bf 0d 00 00 00 00 80 02	.....& .....
↳ Source: RivetNet_ee:c1:fd (9c:b6:d0:ee:c1:fd)	0030	fa f0 0a 9c 00 00 02 04 05 b4 01 03 03 08 01 01	.....
Type: IPv4 (0x0800)	0040	04 02	..
↳ Internet Protocol Version 4. Src: 192.168.1.12, Dest: 34.107.221.82			

- Combien de connexion(s) TCP ont été établie(s) ? \_\_\_\_\_