

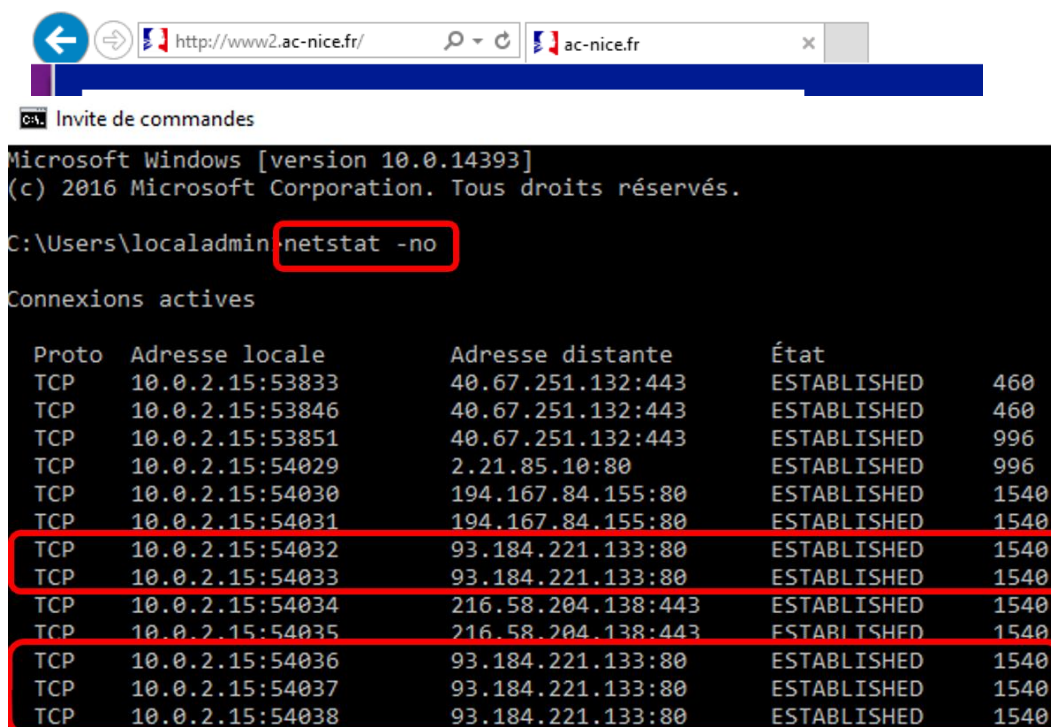
TP3 – Les ports logiciels

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.

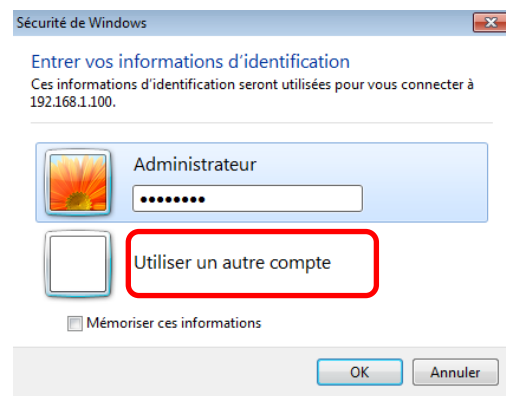
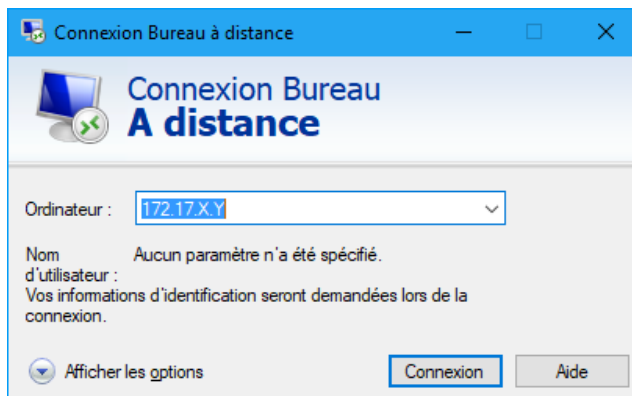
C:\Users\phbou>netstat -an

Connexions actives

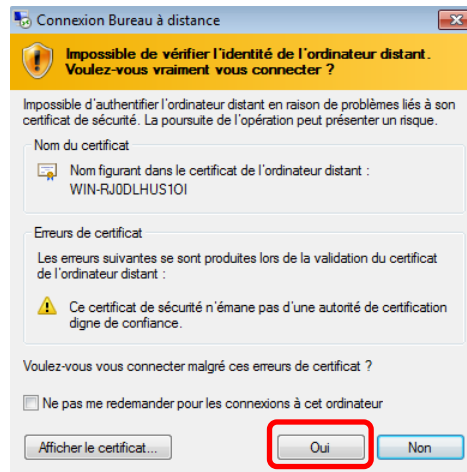
Proto  Adresse locale      Adresse distante     État
TCP    0.0.0.0:135          0.0.0.0:0            LISTENING
TCP    0.0.0.0:443          0.0.0.0:0            LISTENING
TCP    0.0.0.0:445          0.0.0.0:0            LISTENING
TCP    0.0.0.0:903          0.0.0.0:0            LISTENING
TCP    0.0.0.0:913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

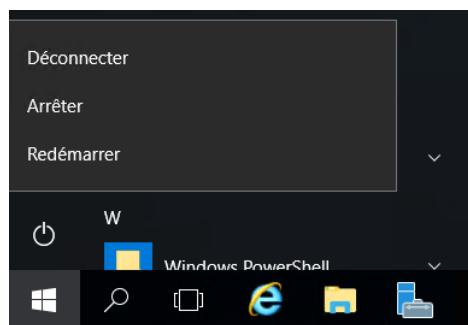
Connexions actives

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

```

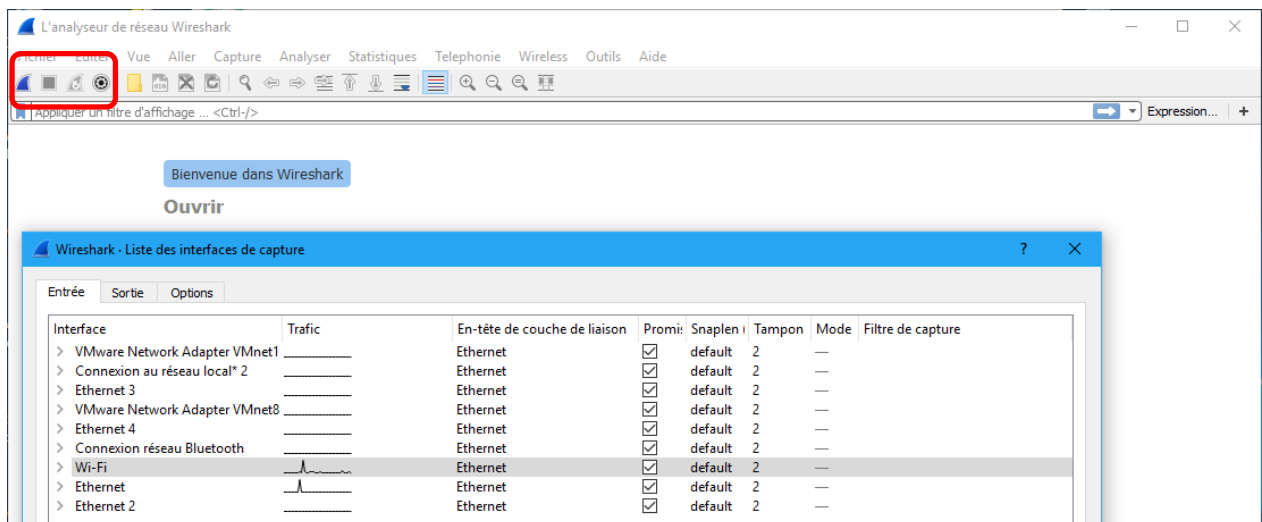
IP en 172.17.X.Y
pour vous

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

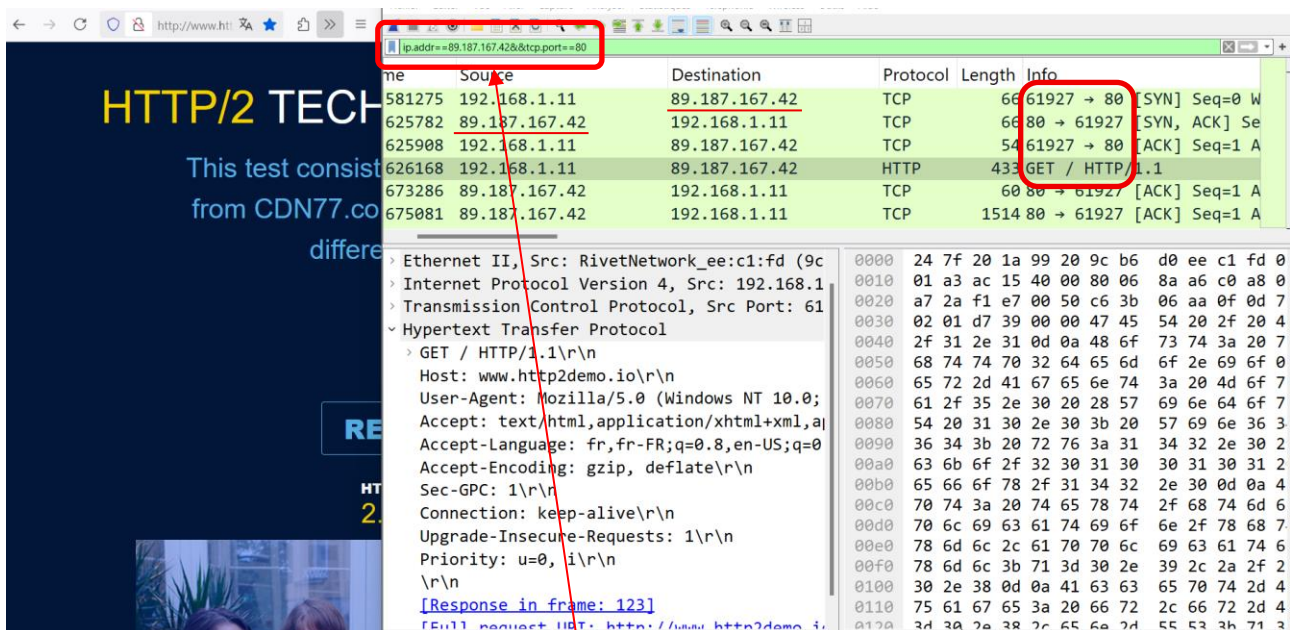


2. Capture de trames HTTP.

- 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** ainsi que le **port TCP 80** 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 les adresses IP du serveur web (enregistrement **www** associé au nom de domaine **http2demo.io**).

```

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

C:\Users\phbou>nslookup www.http2demo.io
Serveur : livebox.nome
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
           2a02:6ea0:ca00::13
           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 : méthode GET) et développez la section correspondant au **protocole applicatif** (attention les adresses IP figurant ci-après sont différentes de celles figurant ci-dessus) :

| ne | Source | Destination | Protocol | Length | Info |
|--------|---------------|---------------|----------|--------|---|
| 626168 | 192.168.1.11 | 89.187.167.42 | HTTP | 43 | GET / HTTP/1.1 |
| 673286 | 89.187.167.42 | 192.168.1.11 | TCP | 60 | 80 → 61927 [ACK] Seq=1 Ack=380 Win=64512 Len=0 |
| 675081 | 89.187.167.42 | 192.168.1.11 | TCP | 1514 | 80 → 61927 [ACK] Seq=1 Ack=380 Win=64512 Len=1460 [TCP PDU reas: ...] |

| | |
|---|--|
| <pre> > Frame 79: 433 bytes on wire (3464 bits), 433 bytes captured (3464 > Ethernet II, Src: RivetNetwork_ee:c1:fd (9c:b6:d0:ee:c1:fd), Dst: > Internet Protocol Version 4, Src: 192.168.1.11, Dst: 89.187.167. > Transmission Control Protocol, Src Port: 61927, Dst Port: 80, Se Hypertext Transfer Protocol GET / HTTP/1.1\r\n Host: www.http2demo.io\r\n User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:142.0 Accept: text/html,application/xhtml+xml,application/xml;q=0.9, Accept-Language: fr,fr-FR;q=0.8,en-US;q=0.5,en;q=0.3\r\n Accept-Encoding: gzip, deflate\r\n Sec-GPC: 1\r\n Connection: keep-alive\r\n Upgrade-Insecure-Requests: 1\r\n Priority: u=0, i\r\n \r\n [Response in frame: 123] [Full request URI: http://www.http2demo.io/] </pre> | <pre> 0030 02 01 d7 39 00 00 47 45 54 20 2f 20 48 54 50 0040 2f 31 2e 31 0d 0a 48 6f 73 74 3a 20 77 77 7e 0050 68 74 74 70 32 64 65 6d 6f 2e 69 6f 0d 0a 55 73 0060 65 72 2d 41 67 65 6e 74 3a 20 4d 6f 7a 69 6c 6c 0070 61 2f 35 2e 30 20 28 57 69 6e 64 6f 77 73 20 4e 0080 54 20 31 30 2e 30 3b 20 57 69 6e 36 34 3b 20 78 0090 36 34 3b 20 72 76 3a 31 34 32 2e 30 29 20 47 65 00a0 63 6b 6f 2f 32 30 31 30 30 31 30 31 20 46 69 72 00b0 65 66 6f 78 2f 31 34 32 2e 30 0d 0a 41 63 63 65 00c0 70 74 3a 20 74 65 78 74 2f 68 74 6d 6c 2c 61 70 00d0 70 6c 69 63 61 74 69 6f 6e 2f 78 68 74 6d 6c 2b 00e0 78 6d 6c 2c 61 70 70 6c 69 63 61 74 69 6f 6e 2f 00f0 78 6d 6c 3b 71 3d 30 2e 39 2c 2a 2f 2a 3b 71 3d 0100 30 2e 38 0d 0a 41 63 63 65 70 74 2d 4c 61 6e 67 0110 75 61 67 65 3a 20 66 72 2c 66 72 2d 46 52 3b 71 0120 3d 30 2e 38 2c 65 6e 2d 55 53 3b 71 3d 30 2e 35 0130 2c 65 6e 3b 71 3d 30 2e 33 0d 0a 41 63 63 65 70 0140 74 2d 45 6e 63 6f 64 69 6e 67 3a 20 67 7a 69 70 0150 2c 20 64 65 66 6c 61 74 65 0d 0a 53 65 63 2d 47 0160 50 43 3a 20 31 0d 0a 43 6f 6e 6e 65 63 74 69 6f 0170 6e 3a 20 6b 65 65 70 2d 61 6c 69 76 65 0d 0a 55 0180 70 67 72 61 64 65 2d 49 6e 73 65 63 75 72 65 2d </pre> |
|---|--|

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

| | |
|--|---|
| <pre> > Frame 79: 433 bytes on wire (3464 bits), 433 bytes captured (3464 > Ethernet II, Src: RivetNetwork_ee:c1:fd (9c:b6:d0:ee:c1:fd), Ds > Internet Protocol Version 4, Src: 192.168.1.11, Dst: 89.187.167. Transmission Control Protocol, Src Port: 61927, Dst Port: 80, S Source Port: 61927 Destination Port: 80 [Stream index: 7] [Stream Packet Number: 4] [Conversation completeness: Incomplete, DATA (15)] [TCP Segment Len: 379] Sequence Number: 1 (relative sequence number) Sequence Number (raw): 3325757098 [Next Sequence Number: 380 (relative sequence number)] Acknowledgment Number: 1 (relative ack number) Acknowledgment number (raw): 252541927 0101 = Header Length: 20 bytes (5) Flags: 0x018 (PSH, ACK) Window: 513 [Calculated window size: 131328] [Window size scaling factor: 256] </pre> | <pre> 0020 a7 2a f1 e7 00 50 c6 3b 06 aa 0f 0d 7b e7 50 18 0030 02 01 d7 39 00 00 47 45 54 20 2f 20 48 54 50 0040 2f 31 2e 31 0d 0a 48 6f 73 74 3a 20 77 77 7e 0050 68 74 74 70 32 64 65 6d 6f 2e 69 6f 0d 0a 55 73 0060 65 72 2d 41 67 65 6e 74 3a 20 4d 6f 7a 69 6c 6c 0070 61 2f 35 2e 30 20 28 57 69 6e 64 6f 77 73 20 4e 0080 54 20 31 30 2e 30 3b 20 57 69 6e 36 34 3b 20 78 0090 36 34 3b 20 72 76 3a 31 34 32 2e 30 29 20 47 65 00a0 63 6b 6f 2f 32 30 31 30 30 31 30 31 20 46 69 72 00b0 65 66 6f 78 2f 31 34 32 2e 30 0d 0a 41 63 63 65 00c0 70 74 3a 20 74 65 78 74 2f 68 74 6d 6c 2c 61 70 00d0 70 6c 69 63 61 74 69 6f 6e 2f 78 68 74 6d 6c 2b 00e0 78 6d 6c 2c 61 70 70 6c 69 63 61 74 69 6f 6e 2f 00f0 78 6d 6c 3b 71 3d 30 2e 39 2c 2a 2f 2a 3b 71 3d 0100 30 2e 38 0d 0a 41 63 63 65 70 74 2d 4c 61 6e 67 0110 75 61 67 65 3a 20 66 72 2c 66 72 2d 46 52 3b 71 0120 3d 30 2e 38 2c 65 6e 2d 55 53 3b 71 3d 30 2e 35 0130 2c 65 6e 3b 71 3d 30 2e 33 0d 0a 41 63 63 65 70 0140 74 2d 45 6e 63 6f 64 69 6e 67 3a 20 67 7a 69 70 0150 2c 20 64 65 66 6c 61 74 65 0d 0a 53 65 63 2d 47 0160 50 43 3a 20 31 0d 0a 43 6f 6e 6e 65 63 74 69 6f 0170 6e 3a 20 6b 65 65 70 2d 61 6c 69 76 65 0d 0a 55 0180 70 67 72 61 64 65 2d 49 6e 73 65 63 75 72 65 2d </pre> |
|--|---|

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 :

| | |
|--|--|
| <pre> > Frame 79: 433 bytes on wire (3464 bits), 433 bytes captured (346 > Ethernet II, Src: RivetNetwork ee:c1:fd (9c:b6:d0:ee:c1:fd), Dst > Internet Protocol Version 4, Src: 192.168.1.11, Dst: 89.187.167. 0100 = Version: 4 0101 = Header Length: 20 bytes (5) > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT) Total Length: 419 Identification: 0xac15 (44053) > 010. = Flags: 0x2, Don't fragment ...0 0000 0000 0000 = Fragment Offset: 0 Time to Live: 128 Protocol: TCP (6) Header Checksum: 0x8aa6 [validation disabled] [Header checksum status: Unverified] Source Address: 192.168.1.11 Destination Address: 89.187.167.42 [Stream index: 4] > Transmission Control Protocol, Src Port: 61927, Dst Port: 80, Se > Hypertext Transfer Protocol </pre> | <pre> 0000 24 7f 20 1a 99 20 9c b6 d0 ee c1 fd 08 00 45 00 \$. . . 0010 01 a3 ac 15 40 00 80 06 8a a6 c0 a8 01 0b 59 bb . . . @ . 0020 a7 2a f1 e7 00 50 c6 3b 06 aa 0f 0d 7b e7 50 18 . * . . P . 0030 02 01 d7 39 00 00 47 45 54 20 2f 20 48 54 54 50 . . . 9 . G 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 55 73 http2de 0060 65 72 2d 41 67 65 6e 74 3a 20 4d 6f 7a 69 6c 6c er-Agen 0070 61 2f 35 2e 30 20 28 57 69 6e 64 6f 77 73 20 4e a/5.0 (0080 54 20 31 30 2e 30 3b 20 57 69 6e 36 34 3b 20 78 T 10.0; 0090 36 34 3b 20 72 76 3a 31 34 32 2e 30 29 20 47 65 64; rv: 00a0 63 6b 6f 2f 32 30 31 30 30 31 30 31 20 46 69 72 cko/201 00b0 65 66 6f 78 2f 31 34 32 2e 30 0d 0a 41 63 63 65 efox/14 00c0 70 74 3a 20 74 65 78 74 2f 68 74 6d 6c 2c 61 70 pt: tex 00d0 70 6c 69 63 61 74 69 6f 6e 2f 78 68 74 6d 6c 2b plicati 00e0 78 6d 6c 2c 61 70 70 6c 69 63 61 74 69 6f 6e 2f xml,app 00f0 78 6d 6c 3b 71 3d 30 2e 39 2c 2a 2f 2a 3b 71 3d xml;q=0 0100 30 2e 38 0d 0a 41 63 63 65 70 74 2d 4c 61 6e 67 0.8. Ac 0110 75 61 67 65 3a 20 66 72 2c 66 72 2d 46 52 3b 71 uage: f 0120 3d 30 2e 38 2c 65 6e 2d 55 53 3b 71 3d 30 2e 35 =0.8,en 0130 2c 65 6e 3b 71 3d 30 2e 33 0d 0a 41 63 63 65 70 ,en;q=0 0140 74 2d 45 6e 63 6f 64 69 6e 67 3a 20 67 7a 69 70 t-Encod 0150 2c 20 64 65 66 6c 61 74 65 0d 0a 53 65 63 2d 47 , defla 0160 50 a3 3a 20 31 0d 0a a3 6f 6a 6a 65 63 74 69 6f pr: 1.. </pre> |
|--|--|

- 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** :

| | |
|--|--|
| <pre> > Frame 79: 433 bytes on wire (3464 bits), 433 bytes captured (346 > Ethernet II, Src: RivetNetwork_ee:c1:fd (9c:b6:d0:ee:c1:fd), Dst > Destination: SagemcomBroa_1a:99:20 (24:7f:20:1a:99:20) > Source: RivetNetwork_ee:c1:fd (9c:b6:d0:ee:c1:fd) Type: IPv4 (0x0800) [Stream index: 0] > Internet Protocol Version 4, Src: 192.168.1.11, Dst: 89.187.167. > Transmission Control Protocol, Src Port: 61927, Dst Port: 80, Se > Hypertext Transfer Protocol </pre> | <pre> 0000 24 7f 20 1a 99 20 9c b6 d0 ee c1 fd 08 00 45 00 \$. . . 0010 01 a3 ac 15 40 00 80 06 8a a6 c0 a8 01 0b 59 bb . . . @ . 0020 a7 2a f1 e7 00 50 c6 3b 06 aa 0f 0d 7b e7 50 18 . * . . P . 0030 02 01 d7 39 00 00 47 45 54 20 2f 20 48 54 54 50 . . . 9 . G 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 55 73 http2de 0060 65 72 2d 41 67 65 6e 74 3a 20 4d 6f 7a 69 6c 6c er-Agen 0070 61 2f 35 2e 30 20 28 57 69 6e 64 6f 77 73 20 4e a/5.0 (0080 54 20 31 30 2e 30 3b 20 57 69 6e 36 34 3b 20 78 T 10.0; 0090 36 34 3b 20 72 76 3a 31 34 32 2e 30 29 20 47 65 64; rv: 00a0 63 6b 6f 2f 32 30 31 30 30 31 30 31 20 46 69 72 cko/201 00b0 65 66 6f 78 2f 31 34 32 2e 30 0d 0a 41 63 63 65 efox/14 00c0 70 74 3a 20 74 65 78 74 2f 68 74 6d 6c 2c 61 70 pt: tex 00d0 70 6c 69 63 61 74 69 6f 6e 2f 78 68 74 6d 6c 2b plicati 00e0 78 6d 6c 2c 61 70 70 6c 69 63 61 74 69 6f 6e 2f xml,app 00f0 78 6d 6c 3b 71 3d 30 2e 39 2c 2a 2f 2a 3b 71 3d xml;q=0 0100 30 2e 38 0d 0a 41 63 63 65 70 74 2d 4c 61 6e 67 0.8. Ac 0110 75 61 67 65 3a 20 66 72 2c 66 72 2d 46 52 3b 71 uage: f 0120 3d 30 2e 38 2c 65 6e 2d 55 53 3b 71 3d 30 2e 35 =0.8,en 0130 2c 65 6e 3b 71 3d 30 2e 33 0d 0a 41 63 63 65 70 ,en;q=0 0140 74 2d 45 6e 63 6f 64 69 6e 67 3a 20 67 7a 69 70 t-Encod 0150 2c 20 64 65 66 6c 61 74 65 0d 0a 53 65 63 2d 47 , defla 0160 50 a3 3a 20 31 0d 0a a3 6f 6a 6a 65 63 74 69 6f pr: 1.. </pre> |
|--|--|

- 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).
Pour chacune d'entre-elles, identifiez le champ Flags dans **l'en-tête de segment** :

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|----------|---------------|---------------|----------|--------|---|
| 51 | 3.581275 | 192.168.1.11 | 89.187.167.42 | TCP | 66 | 61927 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS= |
| 74 | 3.625782 | 89.187.167.42 | 192.168.1.11 | TCP | 66 | 80 → 61927 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 M |
| 78 | 3.625908 | 192.168.1.11 | 89.187.167.42 | TCP | 54 | 61927 → 80 [ACK] Seq=1 Ack=1 Win=131328 Len=0 |
| 79 | 3.626168 | 192.168.1.11 | 89.187.167.42 | HTTP | 433 | GET / HTTP/1.1 |
| 85 | 3.673286 | 89.187.167.42 | 192.168.1.11 | TCP | 60 | 80 → 61927 [ACK] Seq=1 Ack=380 Win=64512 Len=0 |
| 86 | 3.675081 | 89.187.167.42 | 192.168.1.11 | TCP | 1514 | 80 → 61927 [ACK] Seq=1 Ack=380 Win=64512 Len=1460 [|

| | |
|--|---|
| <p>Frame 51: 66 bytes on wire (528 bits), 66 bytes captured (528 b</p> <p>Ethernet II, Src: RivetNetwork_ee:c1:fd (9c:b6:d0:ee:c1:fd), Ds</p> <p>Internet Protocol Version 4, Src: 192.168.1.11, Dst: 89.187.167</p> <p>Transmission Control Protocol, Src Port: 61927, Dst Port: 80, S</p> <p>Source Port: 61927</p> <p>Destination Port: 80</p> <p>[Stream index: 7]</p> <p>[Stream Packet Number: 1]</p> <p>[Conversation completeness: Incomplete, DATA (15)]</p> <p>[TCP Segment Len: 0]</p> <p>Sequence Number: 0 (relative sequence number)</p> <p>Sequence Number (raw): 3325757097</p> <p>[Next Sequence Number: 1 (relative sequence number)]</p> <p>Acknowledgment Number: 0</p> <p>Acknowledgment number (raw): 0</p> <p>1000 = Header Length: 32 bytes (8)</p> <p>Flags: 0x002 (SYN)</p> | <p>0000 24 7f 20 1a 99 20 9c b6 d0 ee c1 fd 08 00 45 00 \$. . . .</p> <p>0010 00 34 ac 0d 40 00 80 06 8c 1d c0 a8 01 0b 59 bb .4..@...</p> <p>0020 a7 2a f1 e7 00 50 c6 3b 06 a9 00 00 00 00 80 02 ...P.;</p> <p>0030 fa f0 f2 69 00 00 02 04 05 b4 01 03 03 08 01 01 ...i....</p> <p>0040 04 02 ..</p> |
|--|---|

| | |
|---|--|
| <p>Frame 74: 66 bytes on wire (528 bits), 66 bytes captured (528 b</p> <p>Ethernet II, Src: SagemcomBroa_1a:99:20 (24:7f:20:1a:99:20), Ds</p> <p>Internet Protocol Version 4, Src: 89.187.167.42, Dst: 192.168.1</p> <p>Transmission Control Protocol, Src Port: 80, Dst Port: 61927, S</p> <p>Source Port: 80</p> <p>Destination Port: 61927</p> <p>[Stream index: 7]</p> <p>[Stream Packet Number: 2]</p> <p>[Conversation completeness: Incomplete, DATA (15)]</p> <p>[TCP Segment Len: 0]</p> <p>Sequence Number: 0 (relative sequence number)</p> <p>Sequence Number (raw): 252541926</p> <p>[Next Sequence Number: 1 (relative sequence number)]</p> <p>Acknowledgment Number: 1 (relative ack number)</p> <p>Acknowledgment number (raw): 3325757098</p> <p>1000 = Header Length: 32 bytes (8)</p> <p>Flags: 0x012 (SYN, ACK)</p> | <p>0000 9c b6 d0 ee c1 fd 24 7f 20 1a 99 20 08 00 45 00\$.</p> <p>0010 00 34 00 00 40 00 37 06 81 2b 59 bb a7 2a c0 a8 .4..@.7.</p> <p>0020 01 0b 00 50 f1 e7 0f 0d 7b e6 c6 3b 06 aa 80 12 ...P....</p> <p>0030 fa f0 67 64 00 00 02 04 05 b4 01 01 04 02 01 03 ..gd....</p> <p>0040 03 09 ..</p> |
|---|--|

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|----------|---------------|---------------|----------|--------|---|
| 51 | 3.581275 | 192.168.1.11 | 89.187.167.42 | TCP | 66 | 61927 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS= |
| 74 | 3.625782 | 89.187.167.42 | 192.168.1.11 | TCP | 66 | 80 → 61927 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 M |
| 78 | 3.625908 | 192.168.1.11 | 89.187.167.42 | TCP | 54 | 61927 → 80 [ACK] Seq=1 Ack=1 Win=131328 Len=0 |
| 79 | 3.626168 | 192.168.1.11 | 89.187.167.42 | HTTP | 433 | GET / HTTP/1.1 |
| 85 | 3.673286 | 89.187.167.42 | 192.168.1.11 | TCP | 60 | 80 → 61927 [ACK] Seq=1 Ack=380 Win=64512 Len=0 |
| 86 | 3.675081 | 89.187.167.42 | 192.168.1.11 | TCP | 1514 | 80 → 61927 [ACK] Seq=1 Ack=380 Win=64512 Len=1460 [|

| | |
|--|--|
| <p>Frame 78: 54 bytes on wire (432 bits), 54 bytes captured (432 b</p> <p>Ethernet II, Src: RivetNetwork_ee:c1:fd (9c:b6:d0:ee:c1:fd), Ds</p> <p>Internet Protocol Version 4, Src: 192.168.1.11, Dst: 89.187.167</p> <p>Transmission Control Protocol, Src Port: 61927, Dst Port: 80, S</p> <p>Source Port: 61927</p> <p>Destination Port: 80</p> <p>[Stream index: 7]</p> <p>[Stream Packet Number: 3]</p> <p>[Conversation completeness: Incomplete, DATA (15)]</p> <p>[TCP Segment Len: 0]</p> <p>Sequence Number: 1 (relative sequence number)</p> <p>Sequence Number (raw): 3325757098</p> <p>[Next Sequence Number: 1 (relative sequence number)]</p> <p>Acknowledgment Number: 1 (relative ack number)</p> <p>Acknowledgment number (raw): 252541927</p> <p>0101 = Header Length: 20 bytes (5)</p> <p>Flags: 0x010 (ACK)</p> | <p>0000 24 7f 20 1a 99 20 9c b6 d0 ee c1 fd 08 00 45 00 \$. . . .</p> <p>0010 00 28 ac 14 40 00 80 06 8c 22 c0 a8 01 0b 59 bb .(.@...</p> <p>0020 a7 2a f1 e7 00 50 c6 3b 06 aa 0f 0d 7b e7 50 10 ...P..</p> <p>0030 02 01 a1 28 00 00 ...()</p> |
|--|--|

- 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 ?