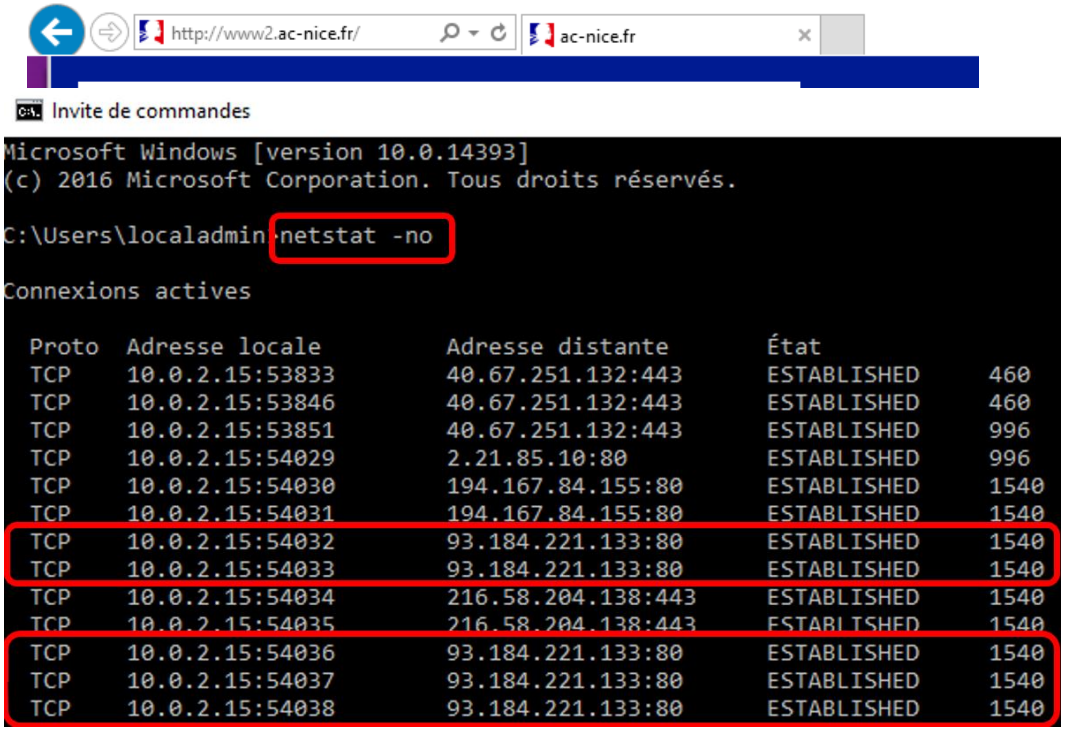
Sommaire

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.

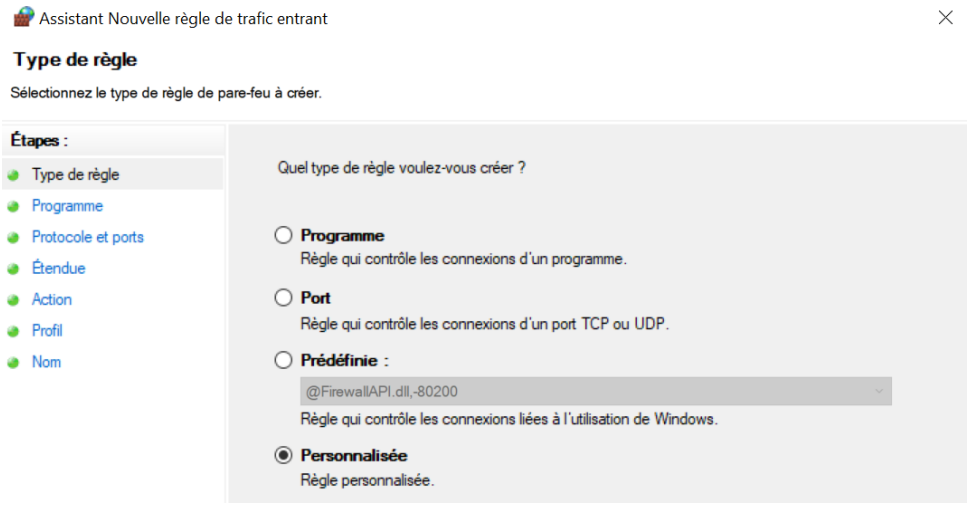
- La commande netstat **sans attribut** n'affiche que les **connexions TCP actives** (état « **Established** »).
- **netstat –a** (a pour all) affiche toutes les **connexions TCP actives** (état « **Established** ») ainsi que les **ports TCP** et **UDP d'écoute** (état « **Listening** »).
- **netstat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

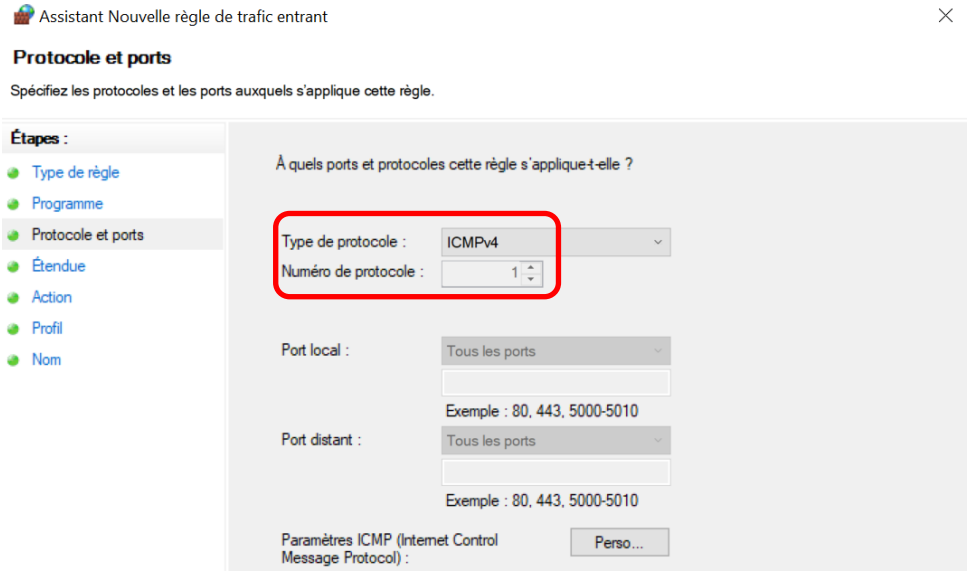


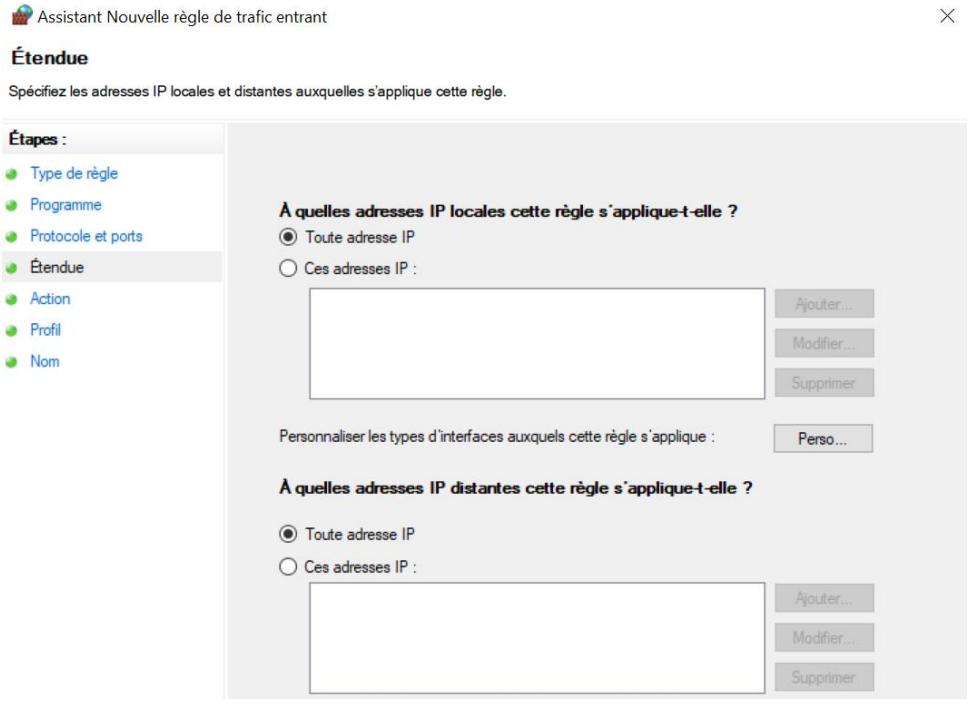
1. Connexion Bureau à distance (RDP).

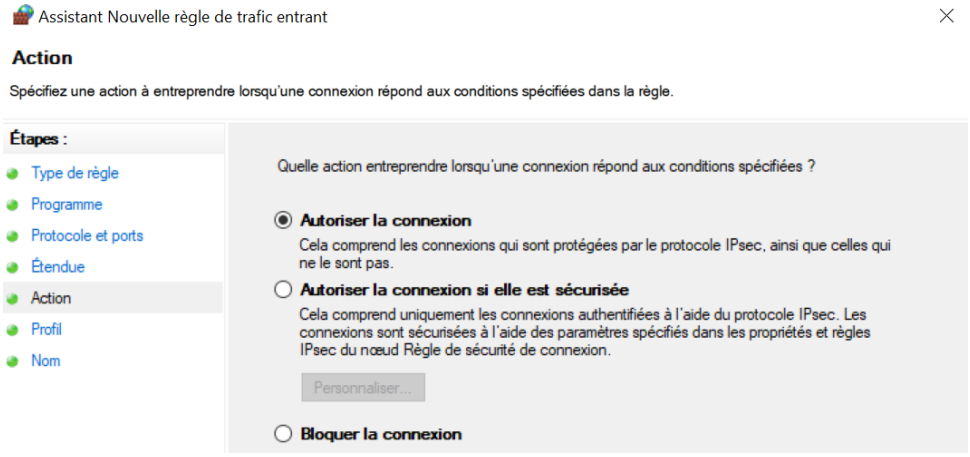
Remote Desktop Protocol (**RDP**) est un protocole qui permet à un utilisateur de se connecter sur un serveur Windows **Terminal Server**.

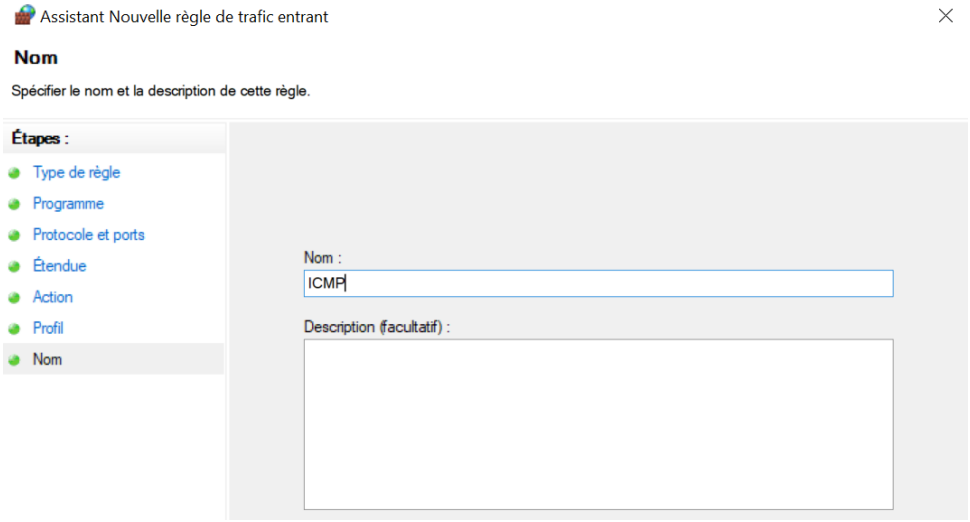
- Demandez à votre voisin l'adresse IP **172 .17.X.Y** obtenue par la carte réseau de sa machine physique.
- Assurez-vous de la connectivité entre votre machine physique et la sienne : réalisez un ping de sa station depuis votre machine physique (capture d'écran). Pensez aux règles de Pare-feu des deux 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 :


Assistant Nouvelle règle de trafic entrant
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.


Assistant Nouvelle règle de trafic entrant
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...

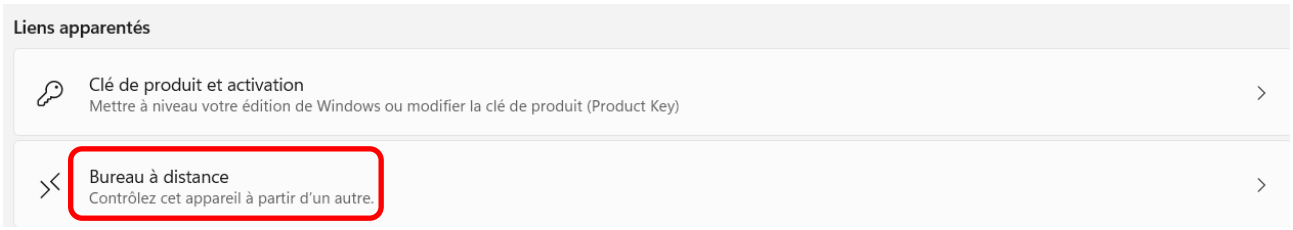

Assistant Nouvelle règle de trafic entrant
Étendue
Spécifiez les adresses IP locales et distantes auxquelles s'applique cette règle.
Étapes :
Type de règle
Programme
Protocole et ports
Étendue
Action
Profil
Nom
À quelles adresses IP locales cette règle s'applique-t-elle ?
Toute adresse IP
Ces adresses 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

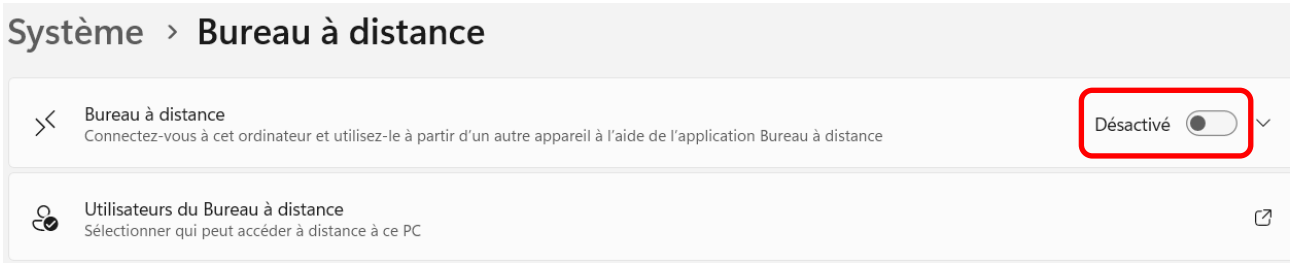


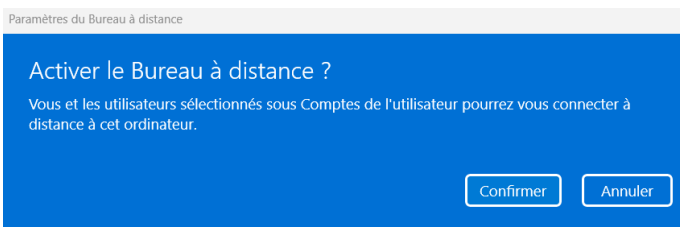


☞ Procédez de la même façon pour le **trafic sortant** (sélectionnez **Autoriser la connexion**).

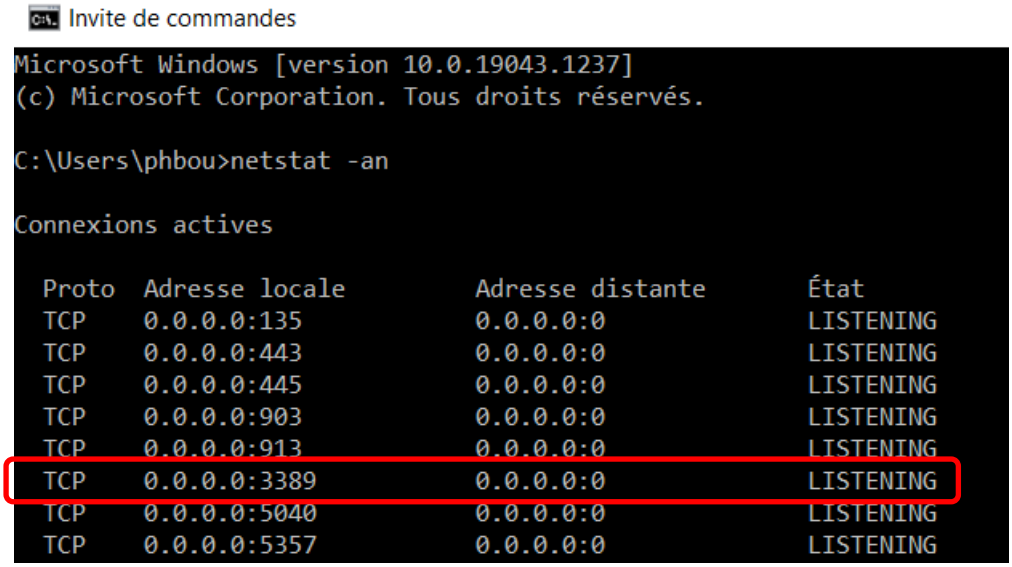
- Cliquez droit sur le bouton **Démarrer** de votre station et sélectionnez **Système** puis **Bureau à distance**. Activez le Bureau à distance :





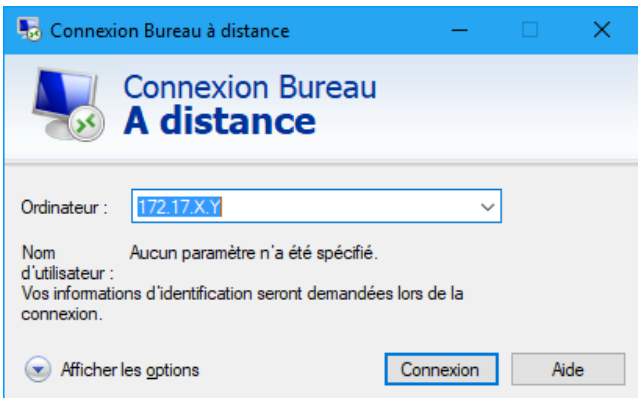


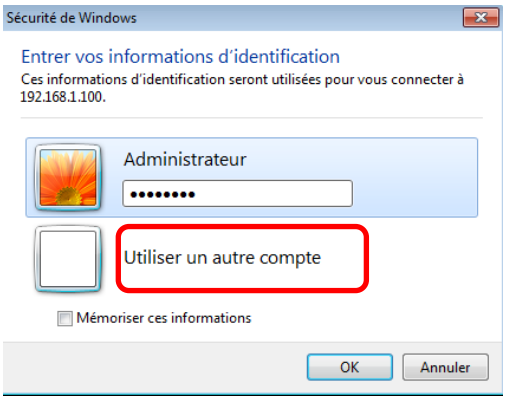
- Saisissez la commande **netstat –an** depuis l'invite de commandes de votre station Windows :



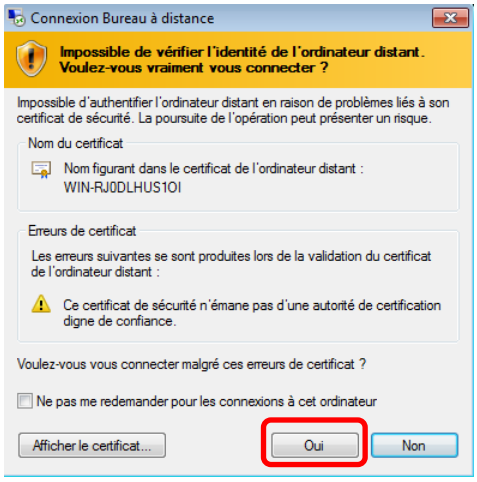
Quel est le port d'écoute du serveur Terminal Server ? _____

- 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**) :

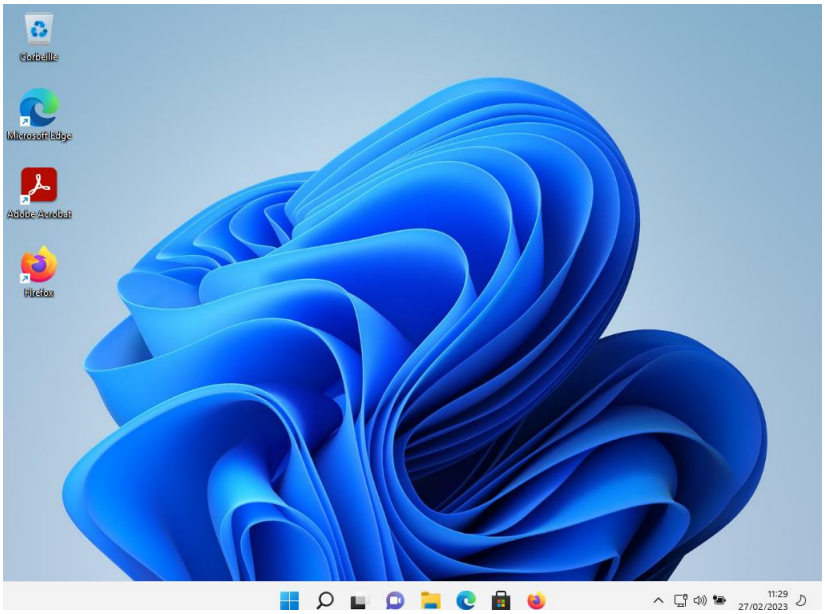




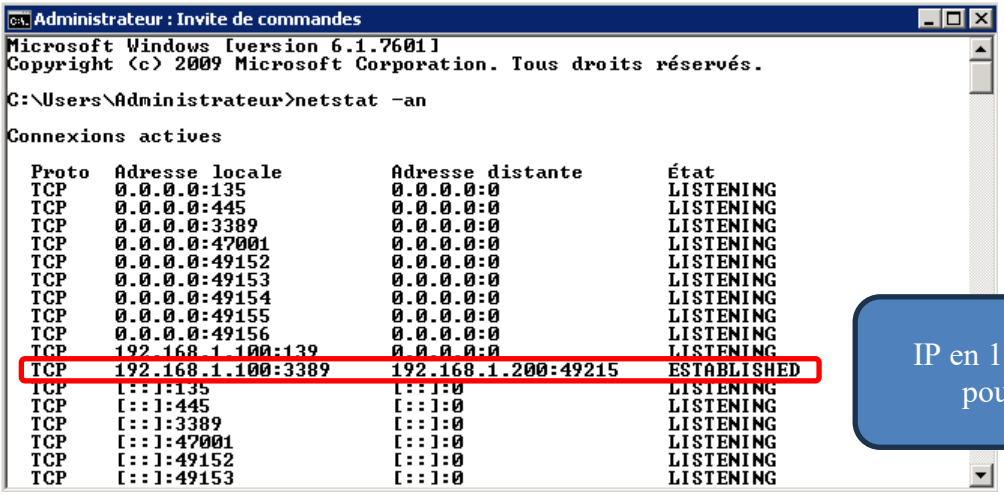
- Cliquez sur **Oui** :



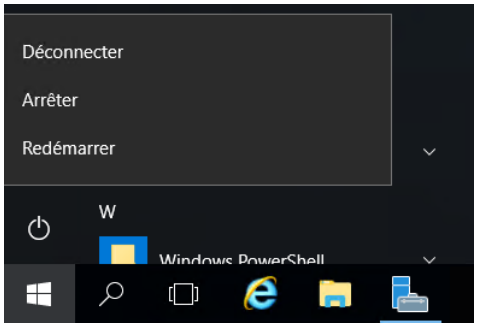
- Vous accédez à la machine Windows 11 de votre voisin :



- 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 :

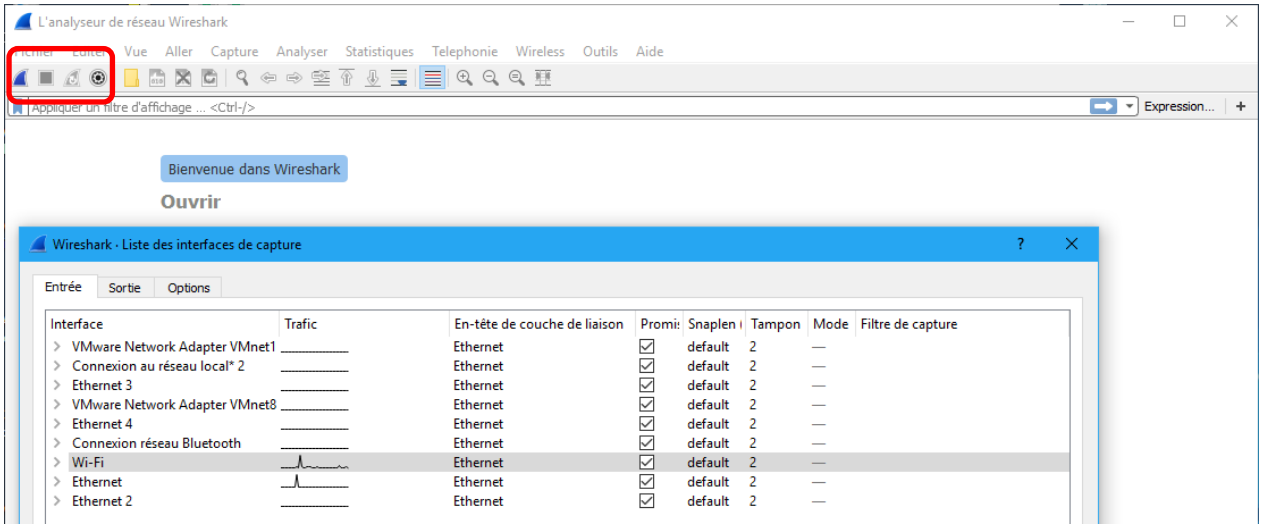


- Cliquez droit sur **Démarrer** puis sur **Déconnecter** pour fermer la connexion à distance (ne pas cliquer sur la croix !) :

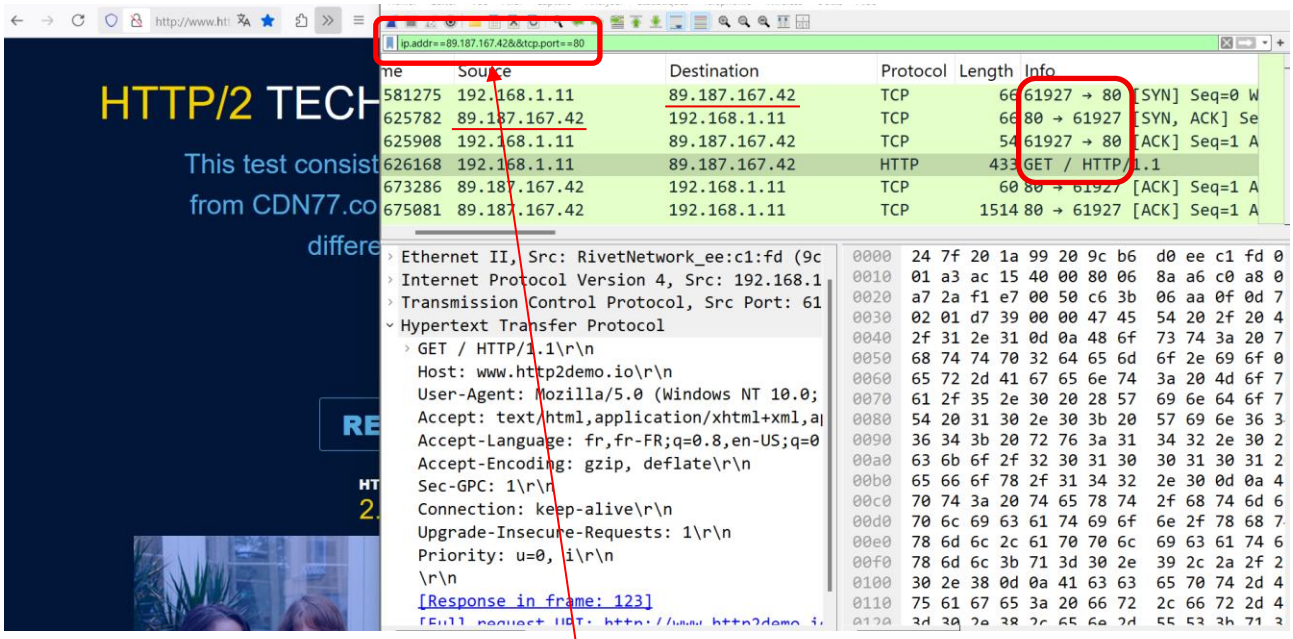


2. Capture de trames HTTP.

- 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) :

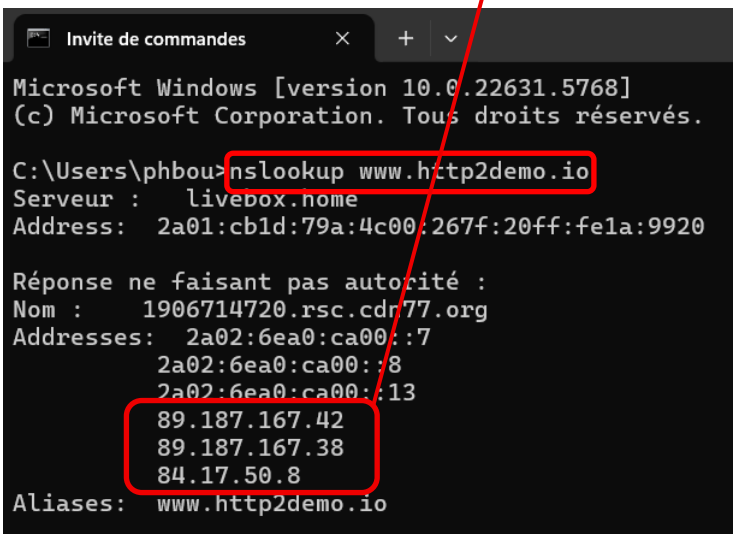


- Ouvrez votre navigateur internet et affichez la page d'accueil du site http://www.http2demo.io/.

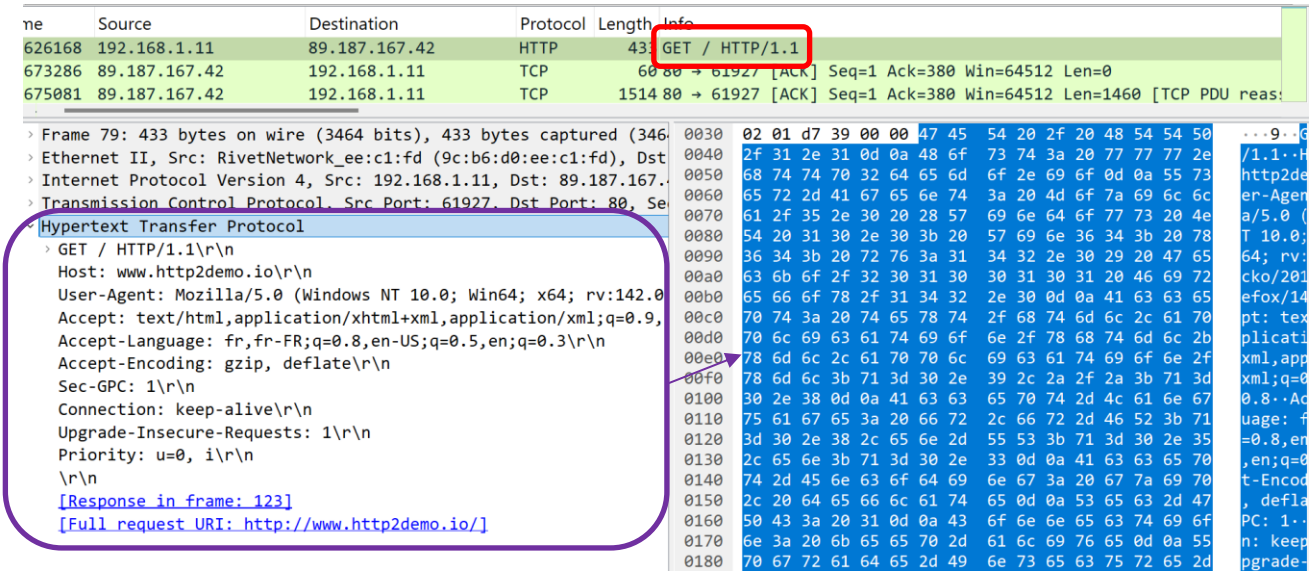


- Arrêtez la capture et appliquez un filtre pour n'afficher que les trames **http** et **TCP** qui nous intéressent. Spécifiez par exemple l'adresse IP ainsi que le port TCP 80 du serveur http. Retrouvez cette adresse IP comme indiqué ci-dessous :

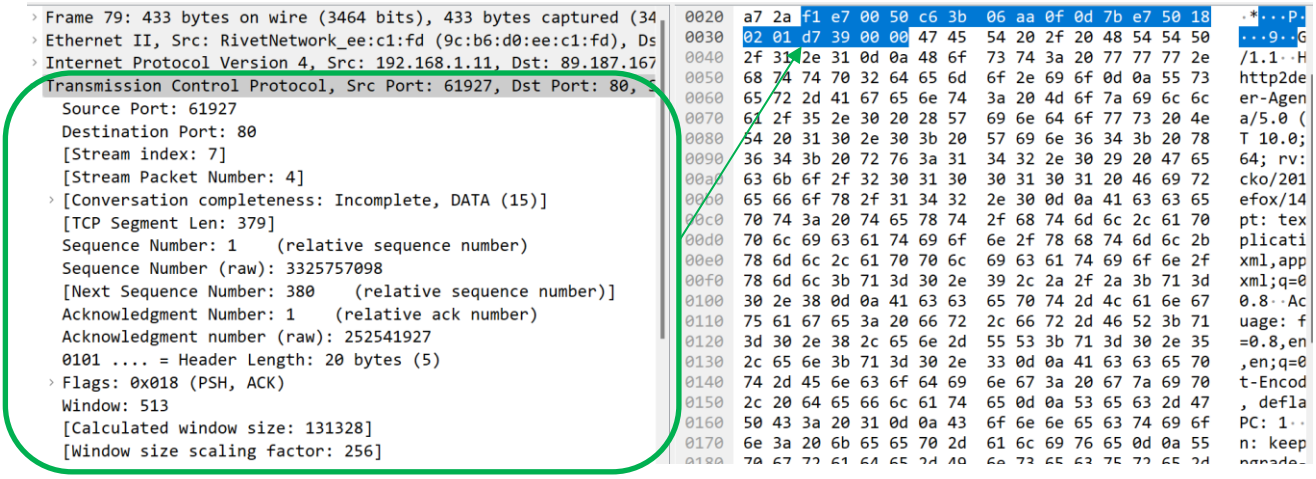
  ➔ Saisissez, depuis l'invite de commandes, la commande **nslookup www.http2demo.io** pour obtenir les adresses IP du serveur web (enregistrement **www** associé au nom de domaine **http2demo.io**).



- 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) :



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



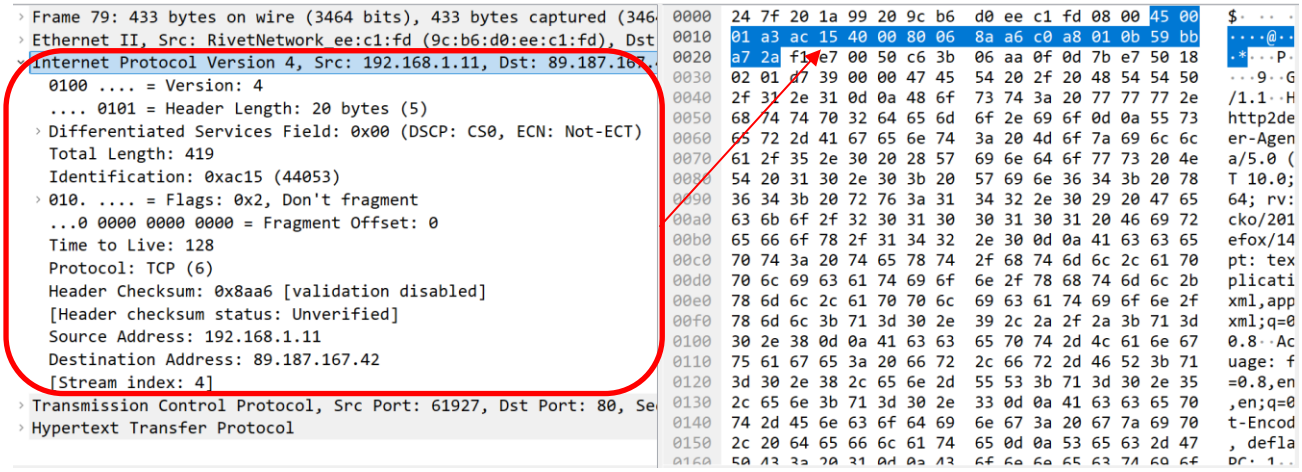
Quel est le nom du protocole transport utilisé par une trame HTTP ?

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 :



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

  _____

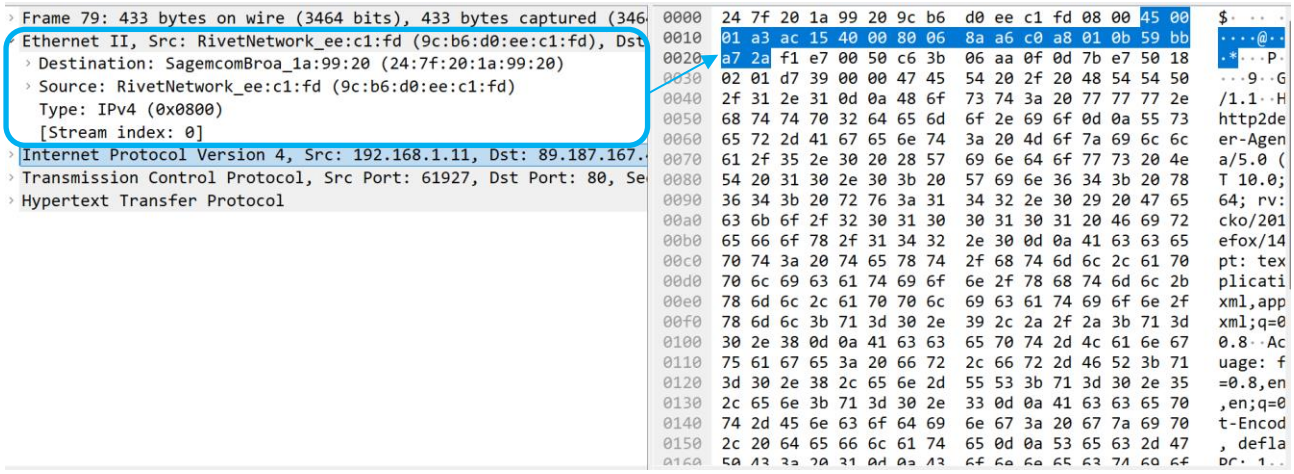
- Repérez le champ Protocole figurant dans l'en-tête Réseau. Quelle est la valeur présente ?_____

  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 :



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

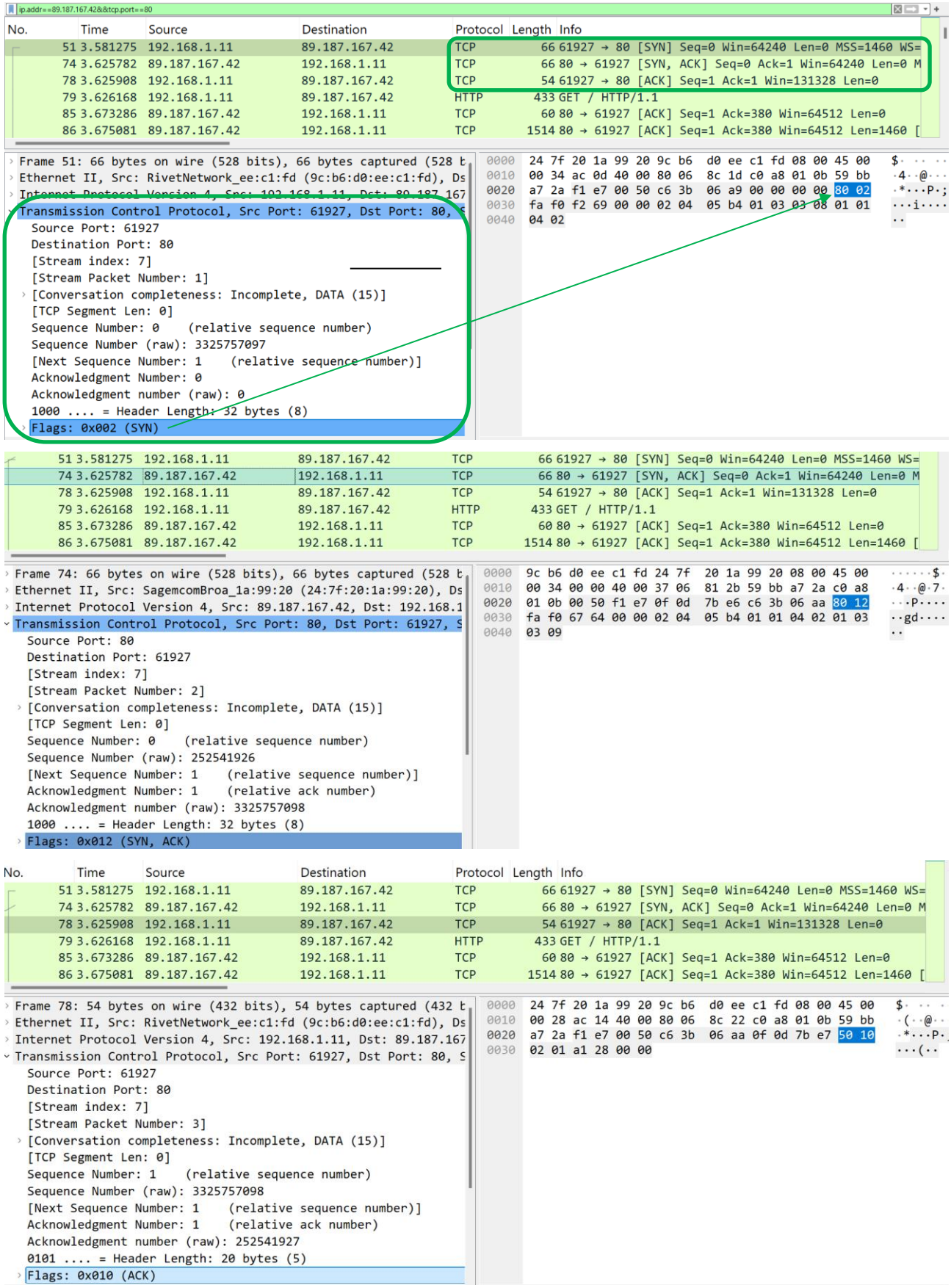
  _____

- 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 :



- 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 ?