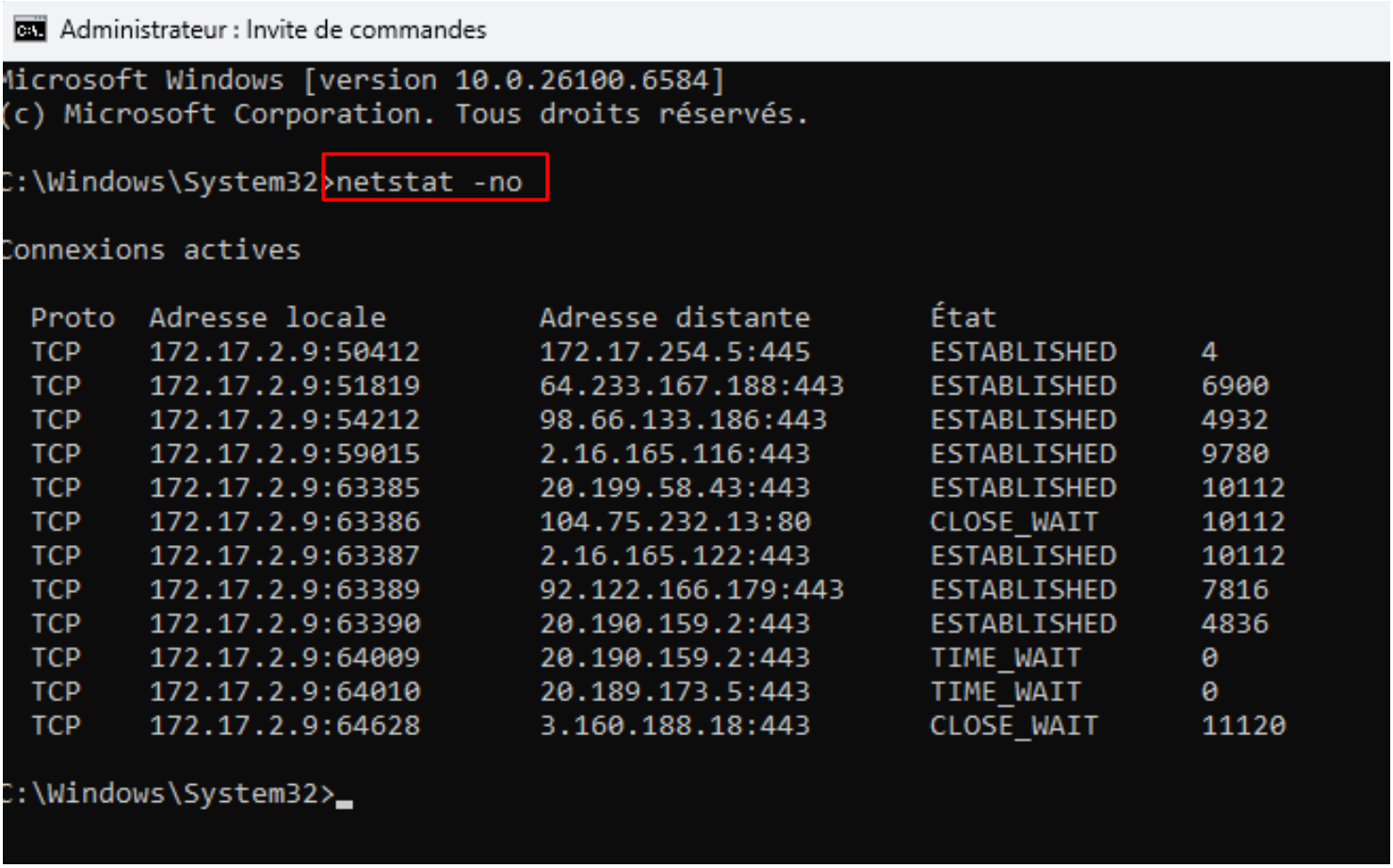
TP 3- Les ports loiciels

Nesrine EL AHMADI

BTS SIO

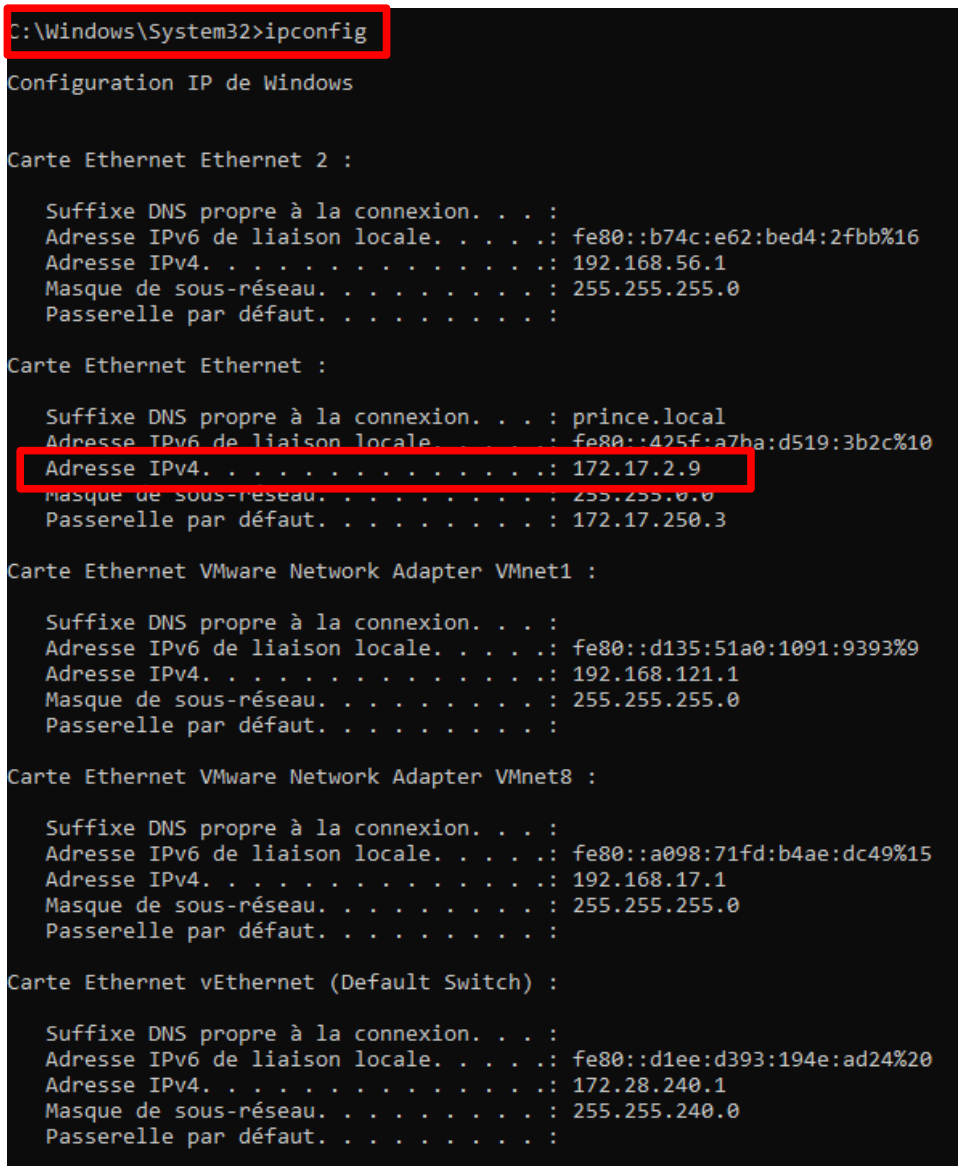
Sommaire

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.



1. Connexion Bureau à distance (RDP)

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

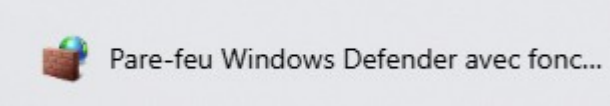


Capture 1

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

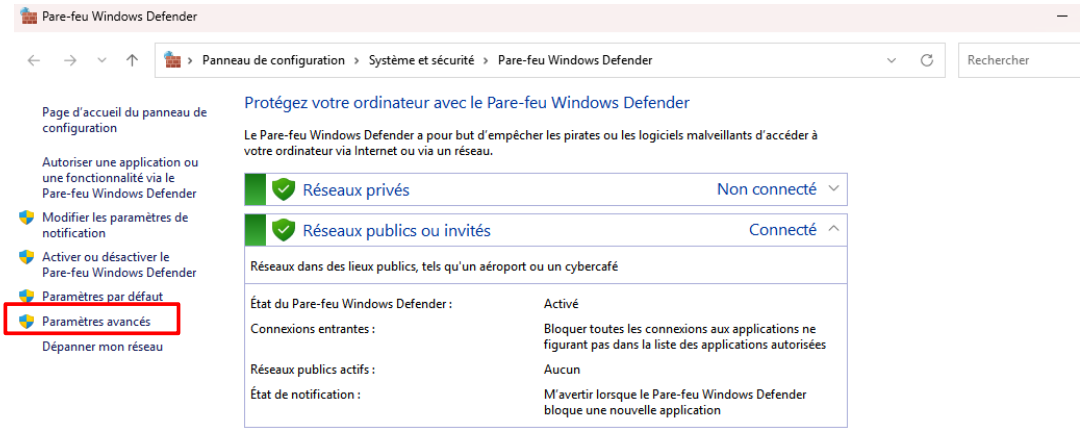
Pour cela on execute le protocole suivant :

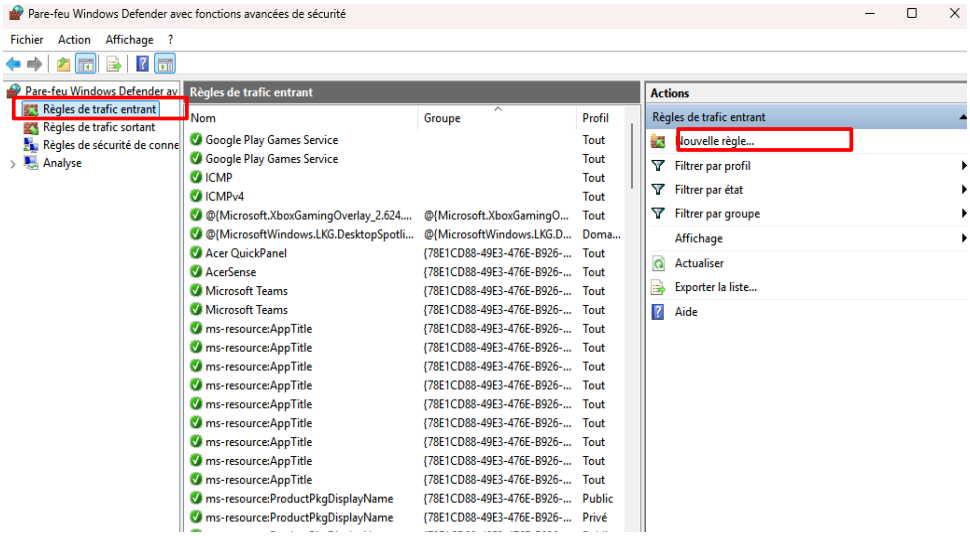
---On va dans l'outil Pare-feu Windows (Capture 2).



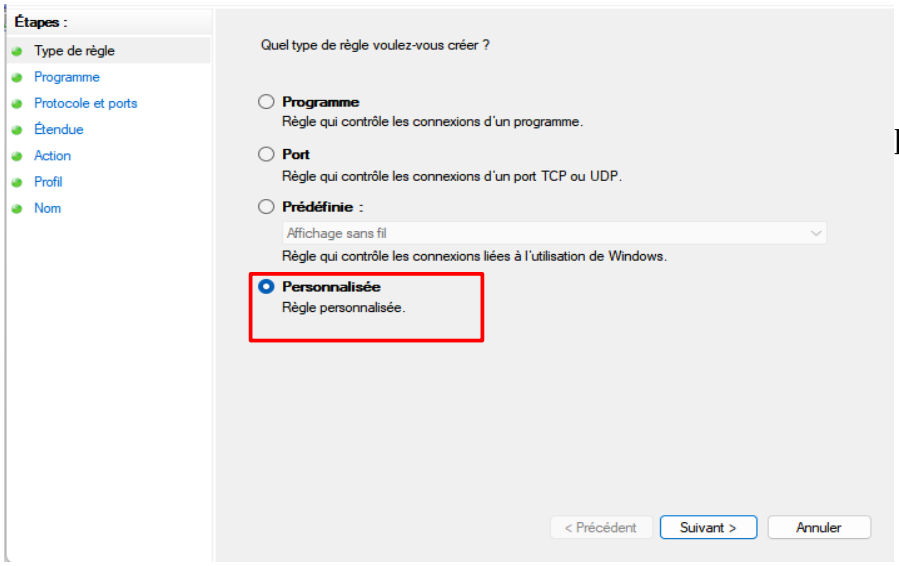
Capture 2

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

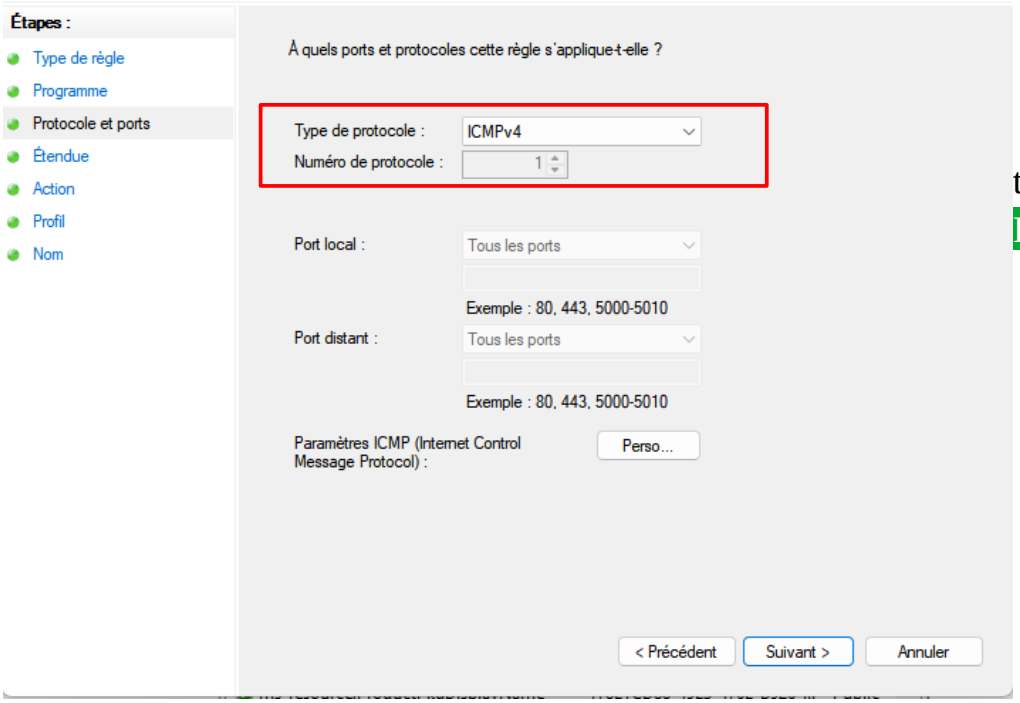




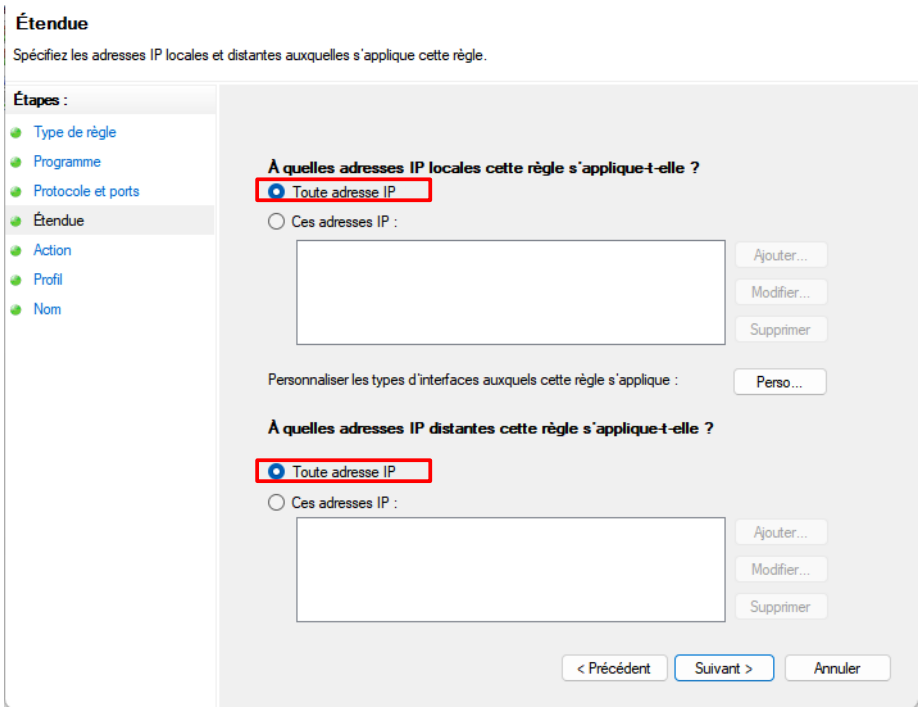
On créer une nouvelle règle.

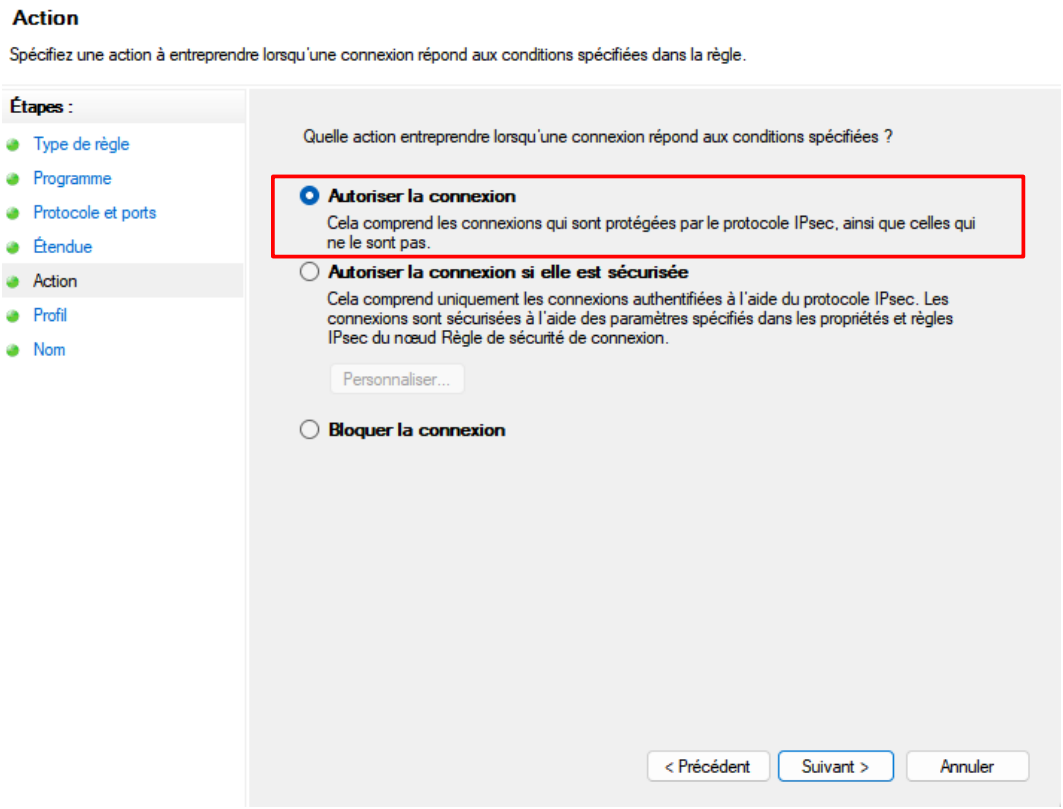


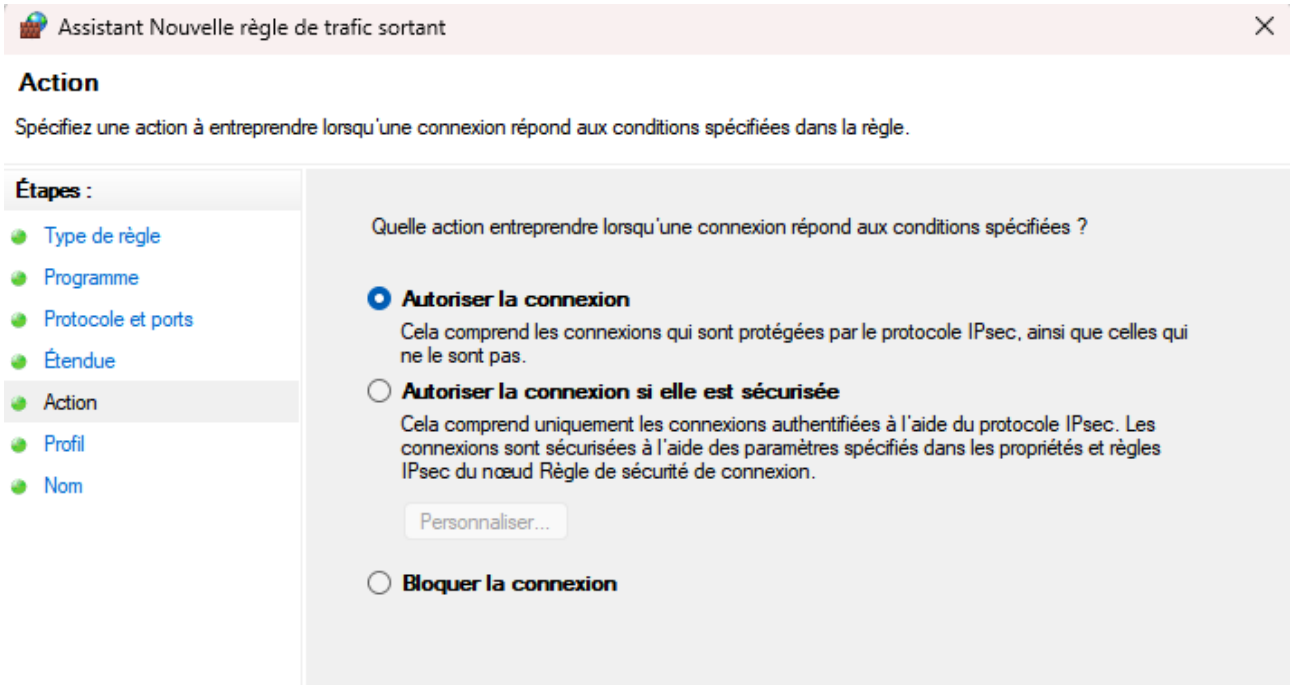
On choisis personnalisée.



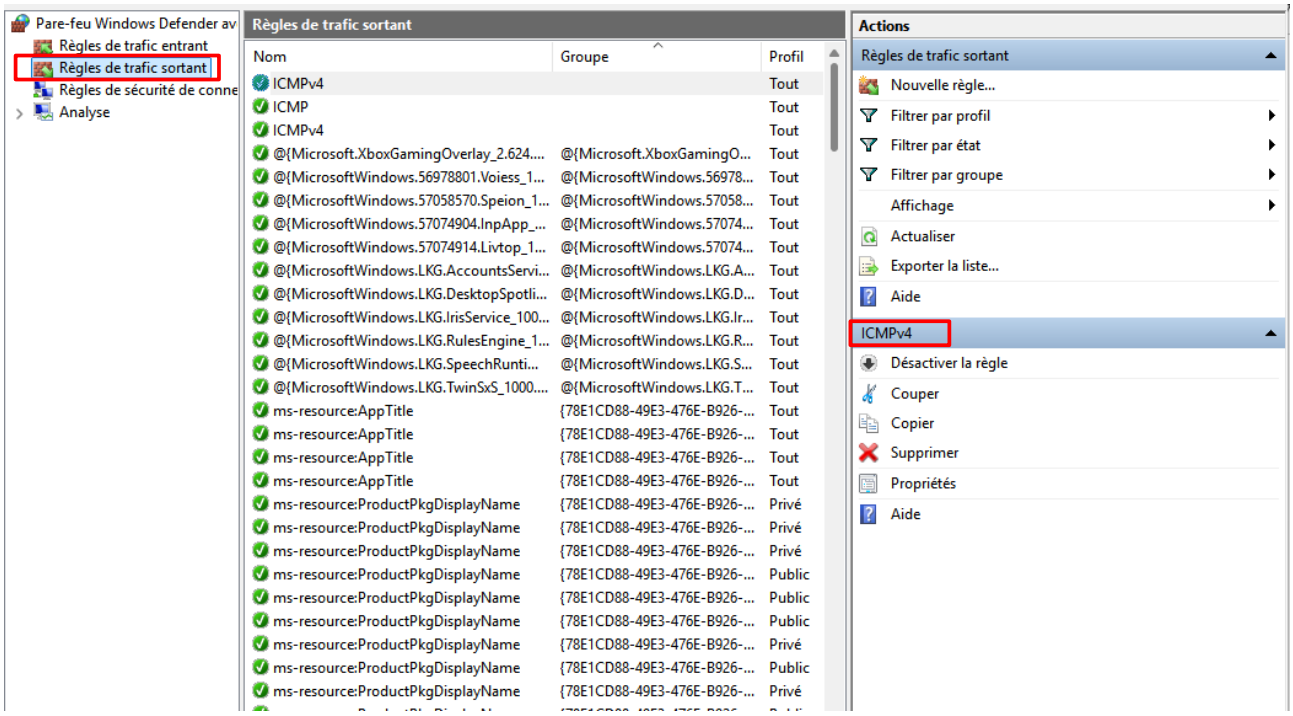
On choisis en type de protocole ICMPv4

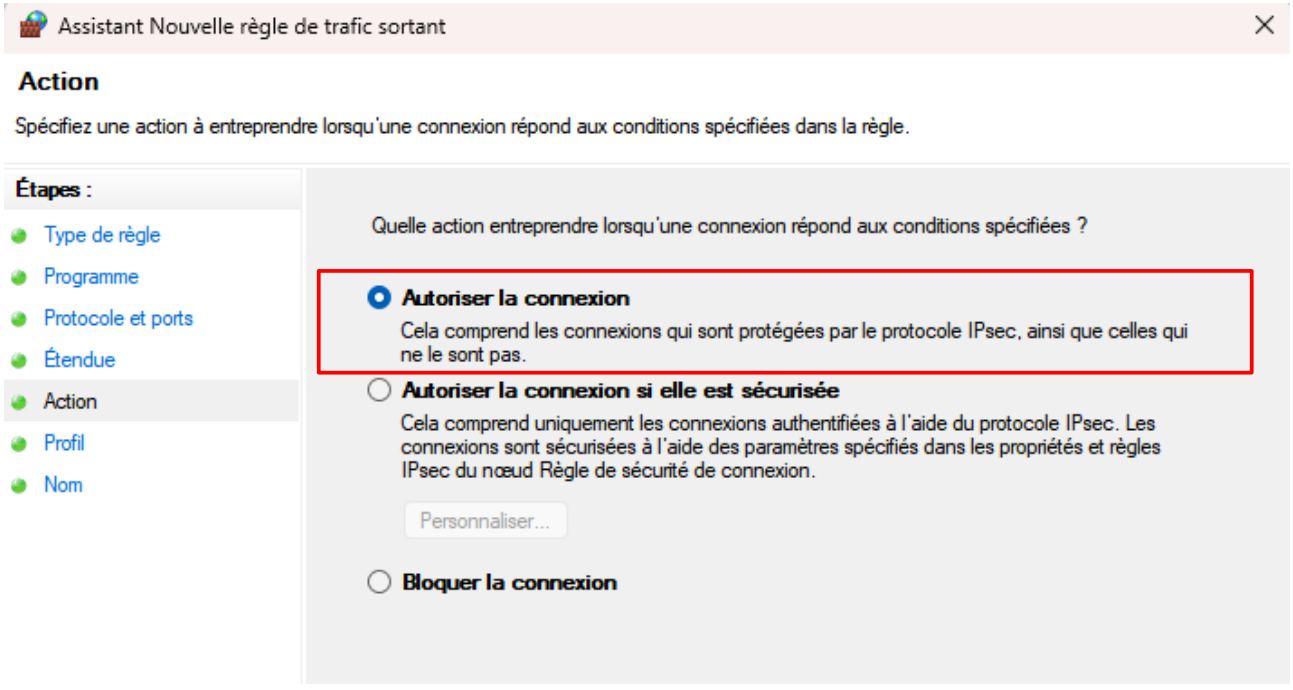

Étendue
Spécifiez les adresses IP locales et distantes auxquelles s'applique cette règle.
Étapes :
Type de règle
Programme
Protocole et ports
Étendue
Action
Profil
Nom
À quelles adresses IP locales cette règle s'applique-t-elle ?
Toute adresse IP
Ces adresses IP :
Ajouter...
Modifier...
Supprimer
Personnaliser 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
< Précédent
Suivant >
Annuler

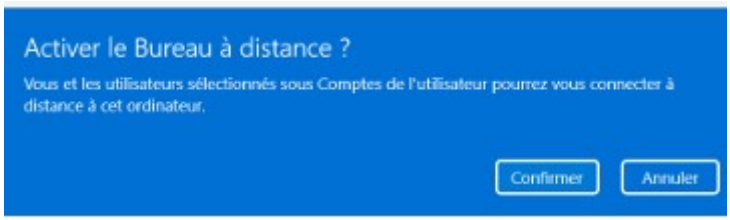

Action
Spécifiez une action à entreprendre lorsqu'une connexion répond aux conditions spécifiées dans la règle.
Étapes :
Type de règle
Programme
Protocole et ports
Étendue
Action
Profil
Nom
Quelle action entreprendre lorsqu'une connexion répond aux conditions spécifiées ?
Autoriser la connexion
Cela 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)


Pare-feu Windows Defender av
Règles de trafic entrant
Règles de trafic sortant
Règles de sécurité de conne
Analyse
Règles de trafic sortant
Nom
Groupe
Profil
ICMPv4 Tout
ICMP Tout
ICMPv4 Tout
@{Microsoft.XboxGamingOverlay_2.624.... @{Microsoft.XboxGamingO... Tout
@{MicrosoftWindows.56978801.Voiess_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.AccountsServi... @{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: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
Règles de trafic sortant
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


Assistant Nouvelle règle de trafic sortant
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

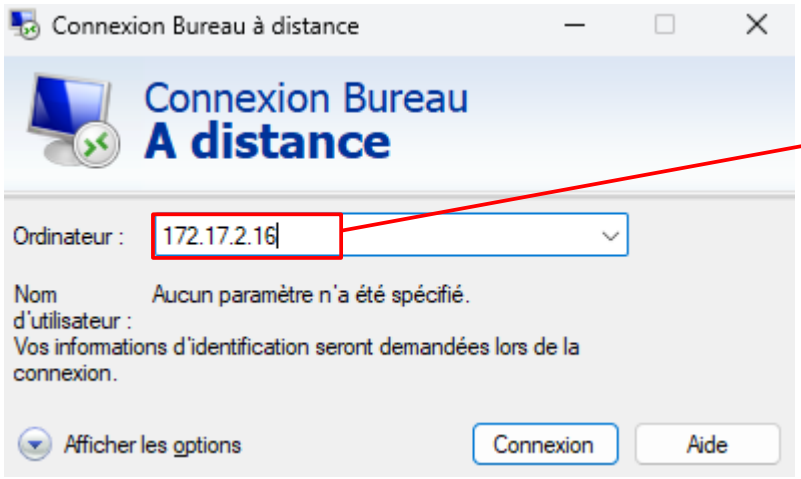


Afin d'observer les connexions du trafic entrants avec les ports et leurs états, on exécute la commande ***netstat -an*** dans l'invite de commande.

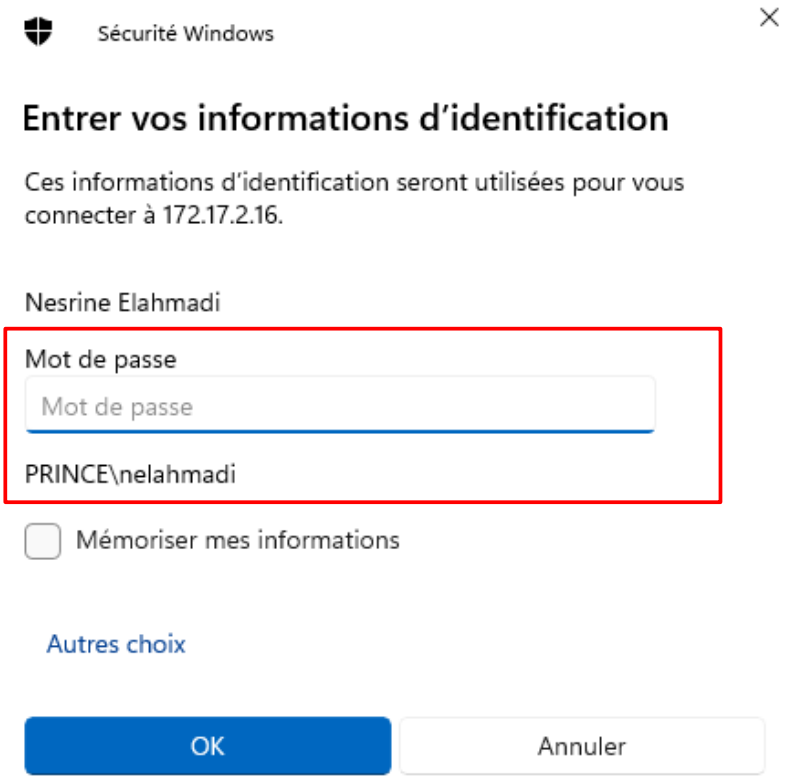
```
C:\Windows\System32>netstat -an

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
```

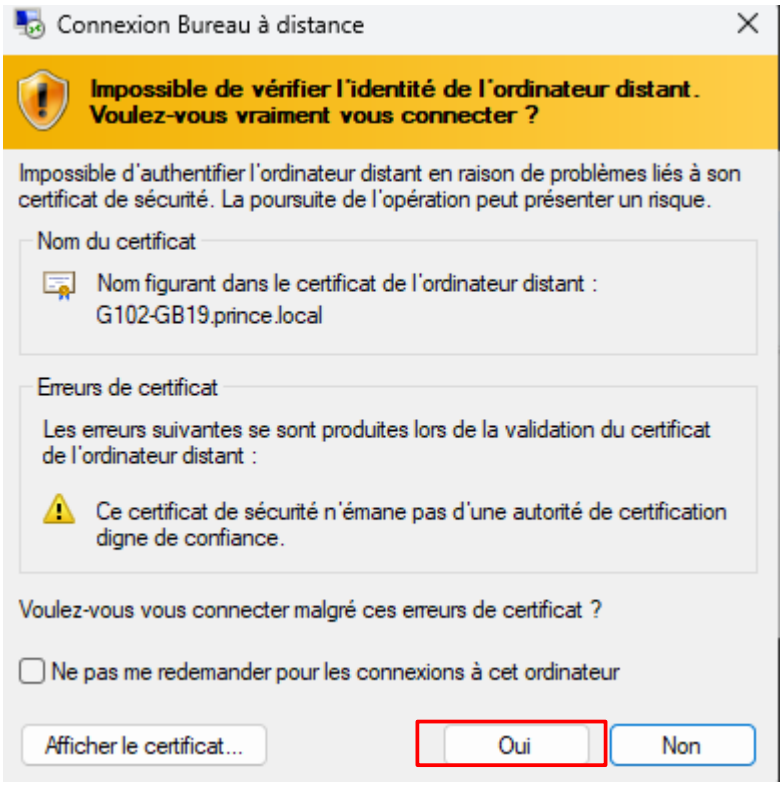
Le port d’écoute du serveur Terminal Server est : 3389

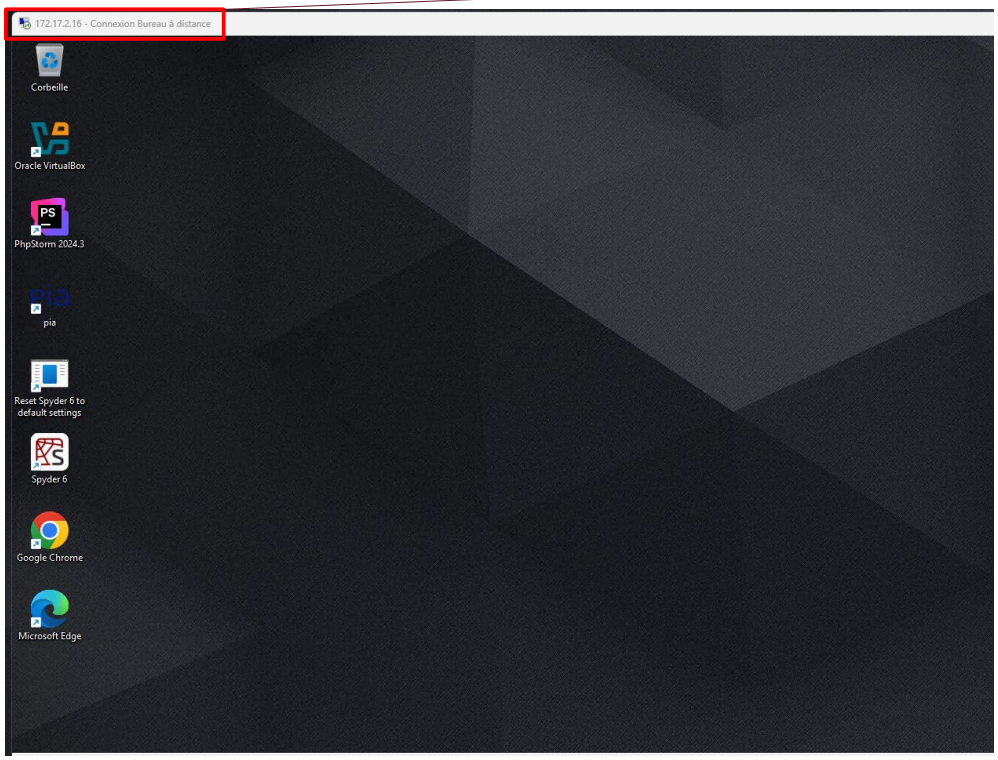
On procède maintenant a la connexion bureau à distance :



@IP du voisin



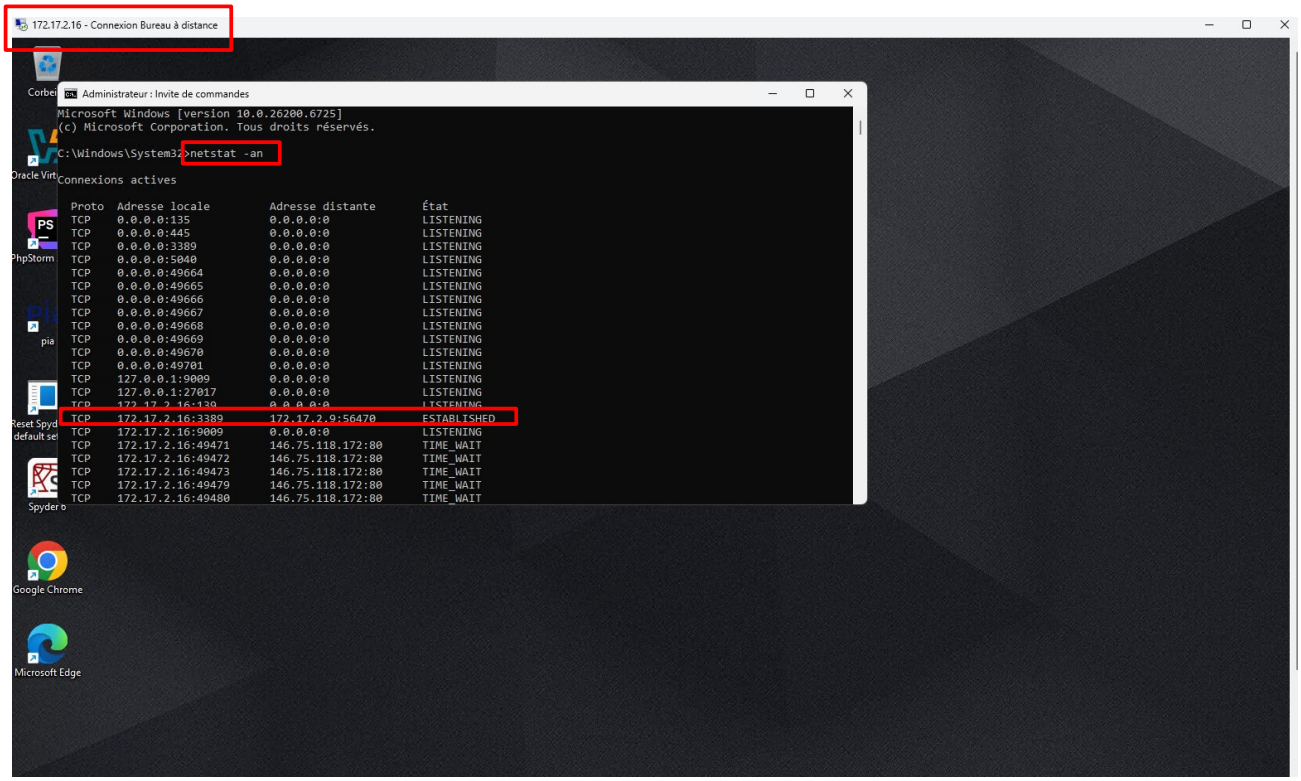




Communication bureau a distance établie

On a donc accès a la machine de mon voisin

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

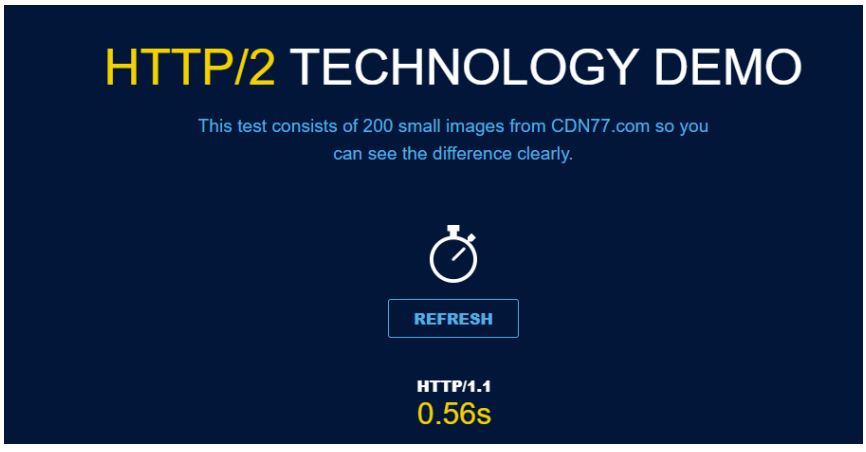


On voit ici que la connexion au serveur Terminal Server est établie.

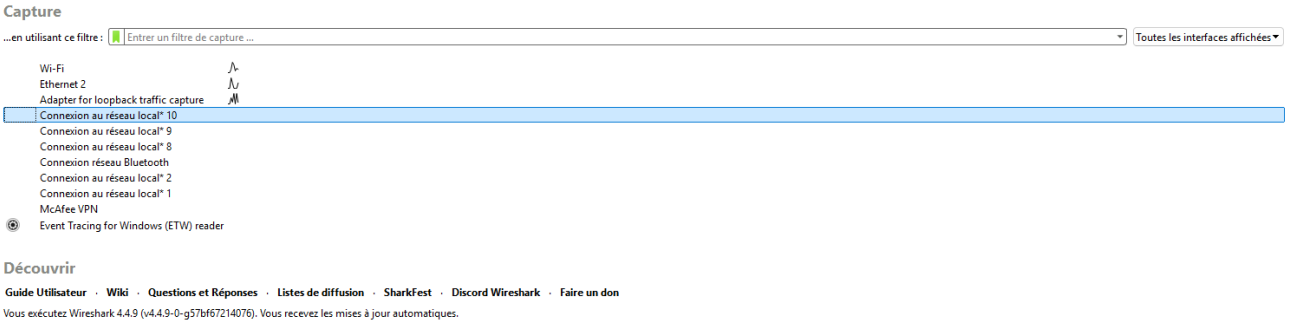
Pour finir on se DECONNECTE.

2. Capture de trames HTTP

On va a l’adresse www.http2demo.io/ (capture 2 et 3)et on lance un capture de trame sur Wireshark en même temps.



Capture 2



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

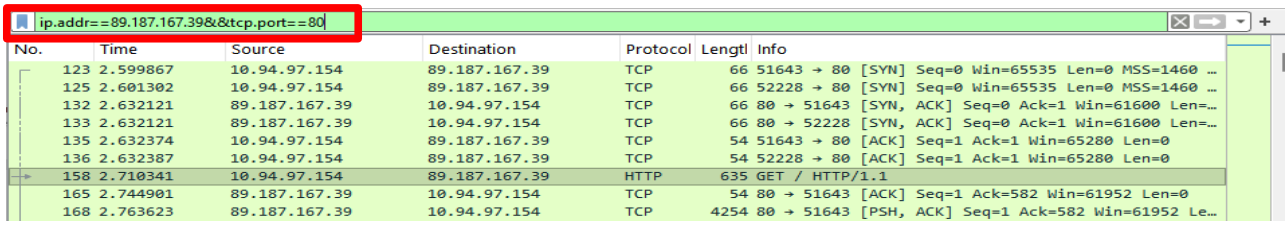
(nous permet de filtrer par la suite les trames)

Capture 4 : commande nslookup

On ping cette adresse (Capture 5):

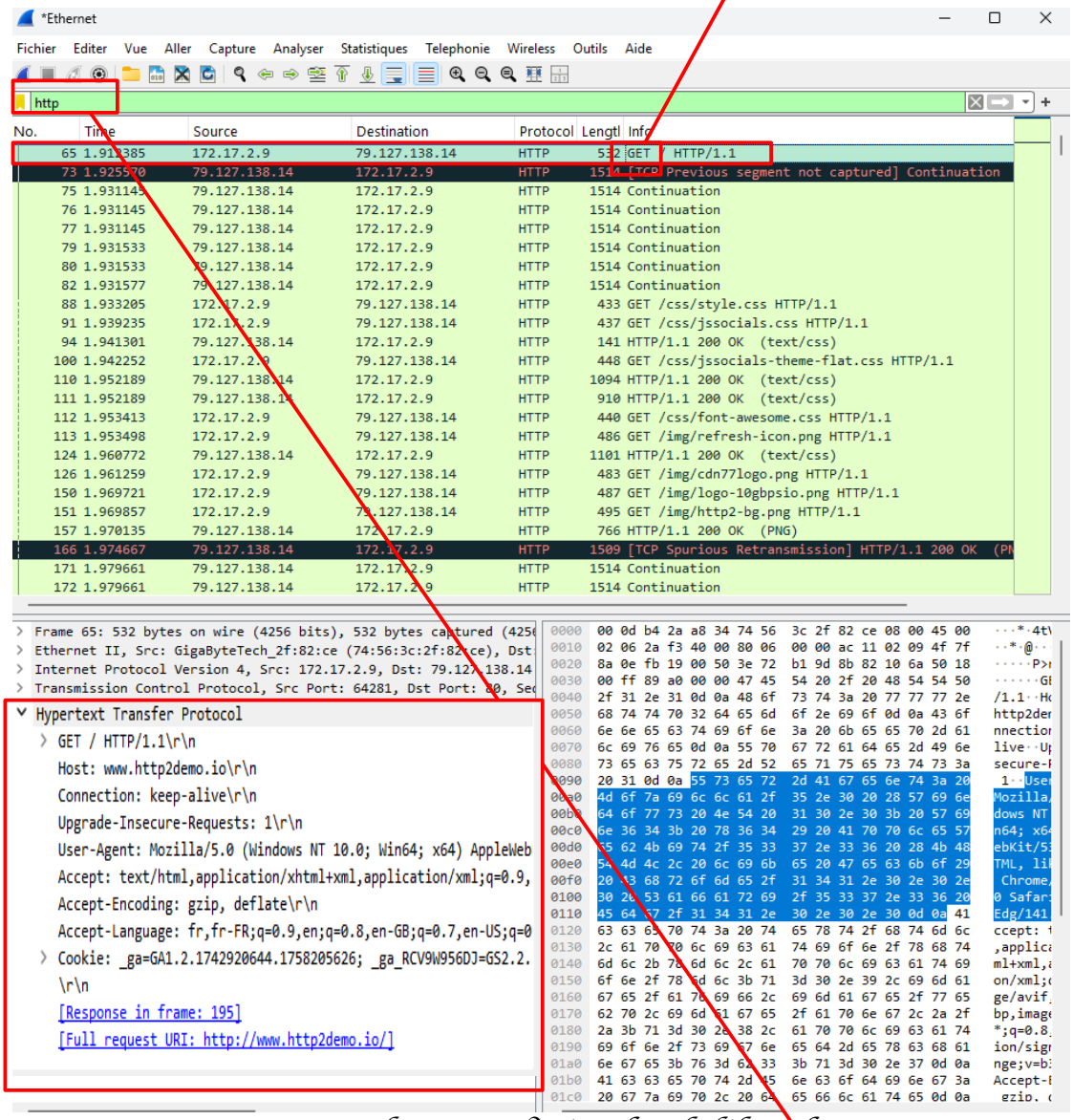
```
C:\Windows\System32>ping http2demo.io

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



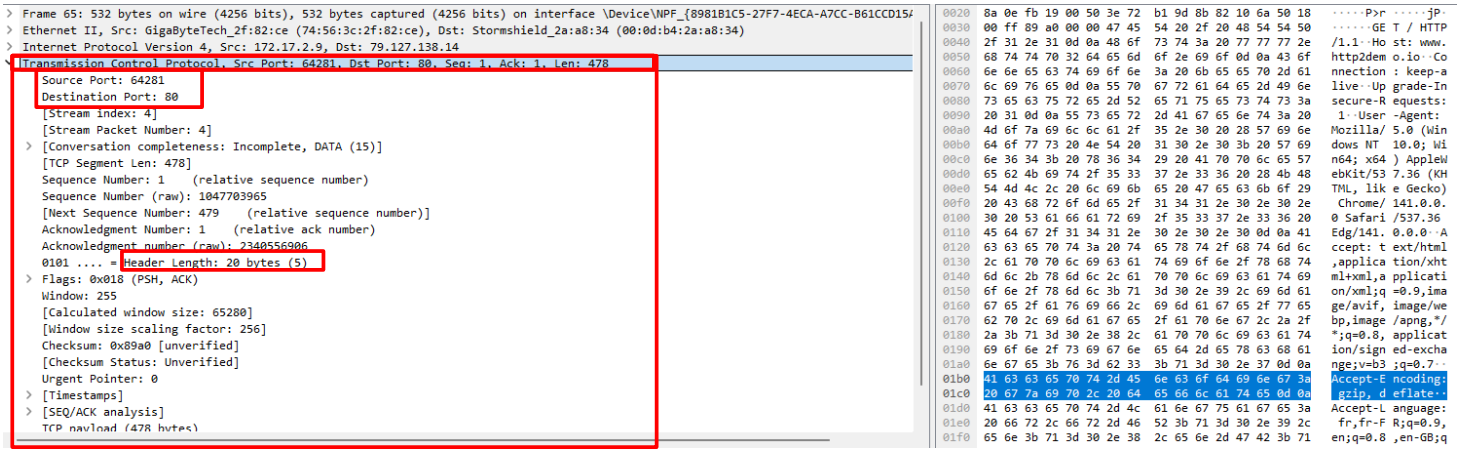
On repère la trame correspondant a la requête http (méthode GET).

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



Capture 6 : Capture de trame Wireshark filtre http

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



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 ?**

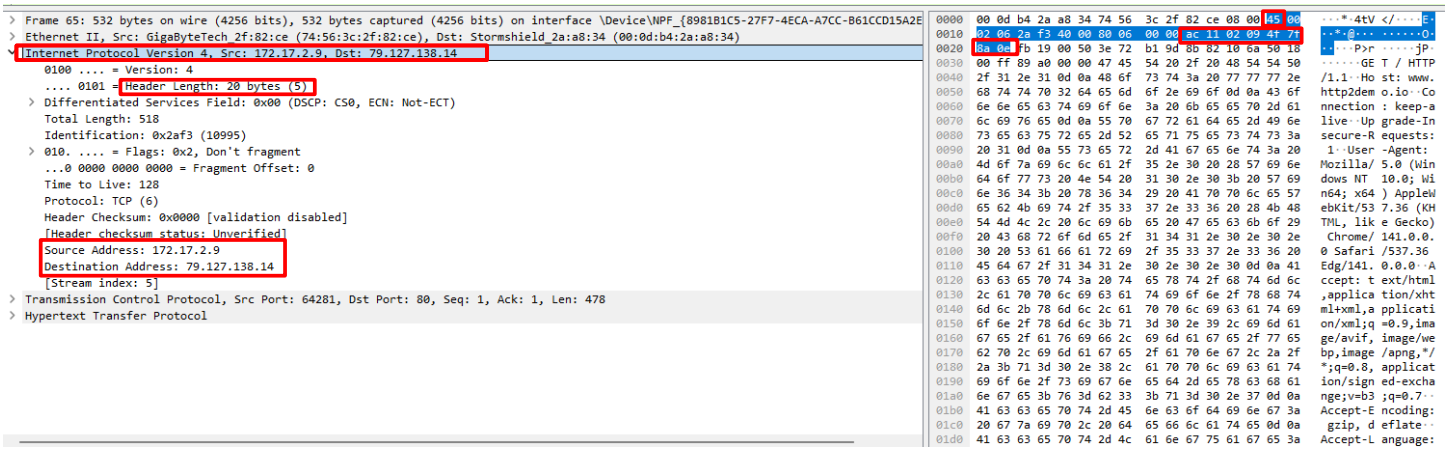
▪ La longueur de l'en-tête est de 14 octets (Header Length =20 bytes (5)).

---**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 a **l'en-tête Réseau (Capture 8)**



Capture 8

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

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

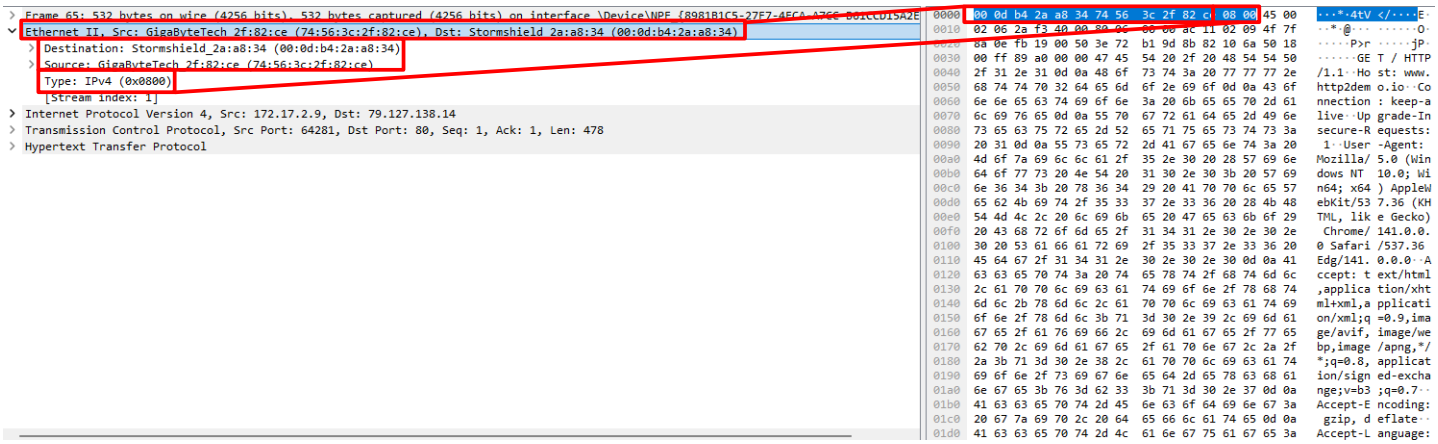
---Valeur et signification du champ protocole :

▪ 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 a **l'en-tête Ethernet (Capture 9)**



---Valeur et signification du champ EtherType :

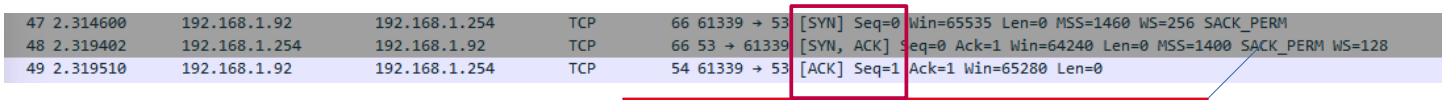
▪ Le champ Ethertype ce trouve a la fin de l'en-tête Ethernet (2 derniers octets). C'est ici la valeur 0800 caractéristique du protocole IPv4.

---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

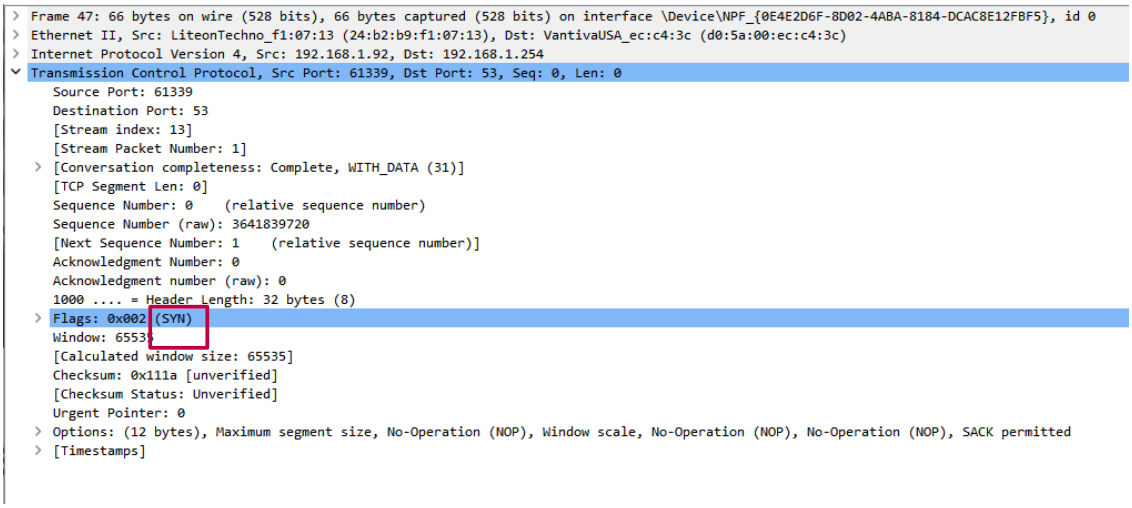
---Trames associées à la mise en place de la connexion TCP entre le client et le serveur



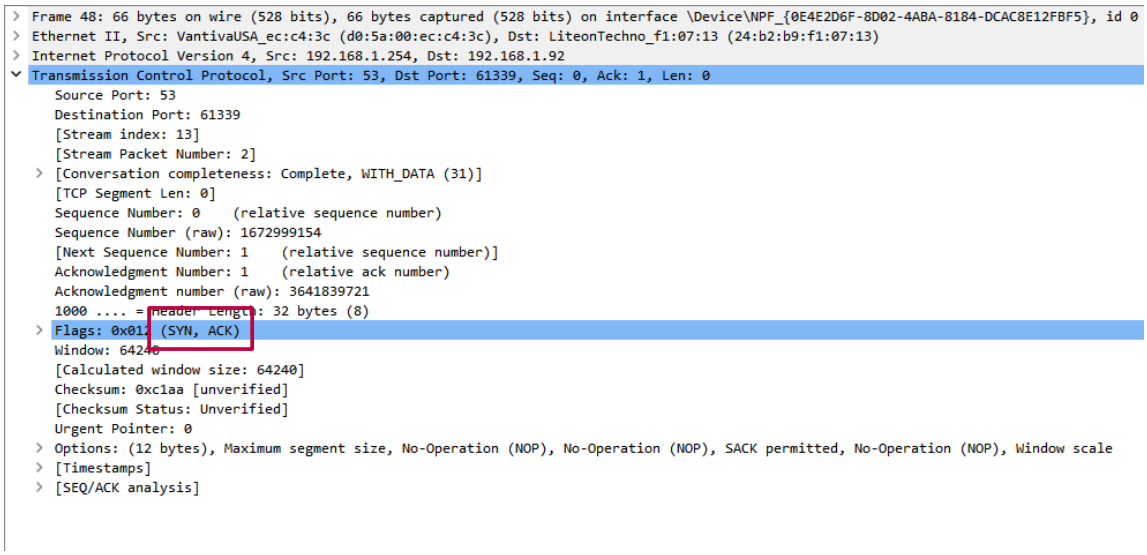
Les addresses IP sont différentes du reste du TP car cette partie a était faite avec mon ordinateur personnel

---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 .

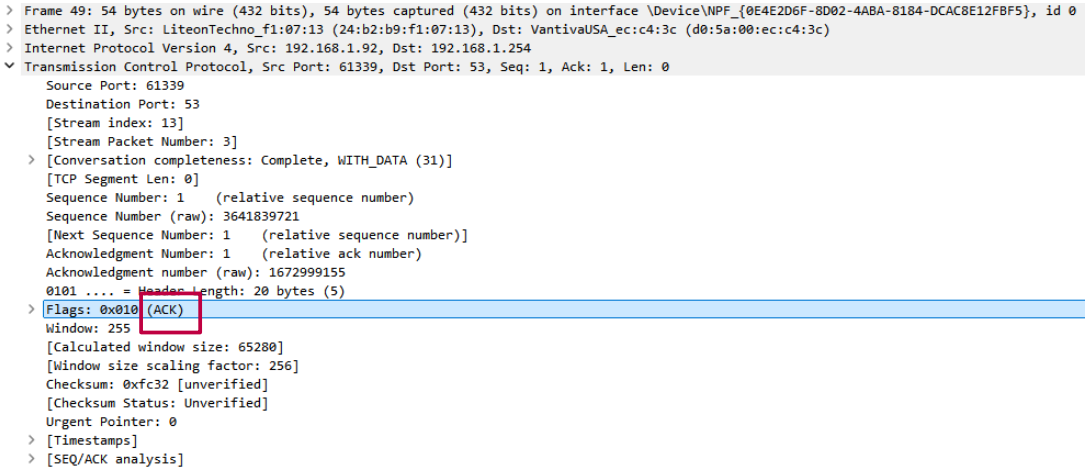


Puis le SYN/ACK signifie que le serveur a bien reçu cette demande qu'il accepte et qu'il en demande un en retour .



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

C'est 3 trames constituent le 3 way handshake



Ce mode connecté est mis en place pour :

- Assurer la fiabilité puisque chaque segment est accusé de reception.

-Assurer le séquencement : ils arrivent dans le bonne ordre.

- Et garantis l'integrité.

RIS : remise, intégrité , séquencement