# Rapport de TP Sécurité- Deuxième partie

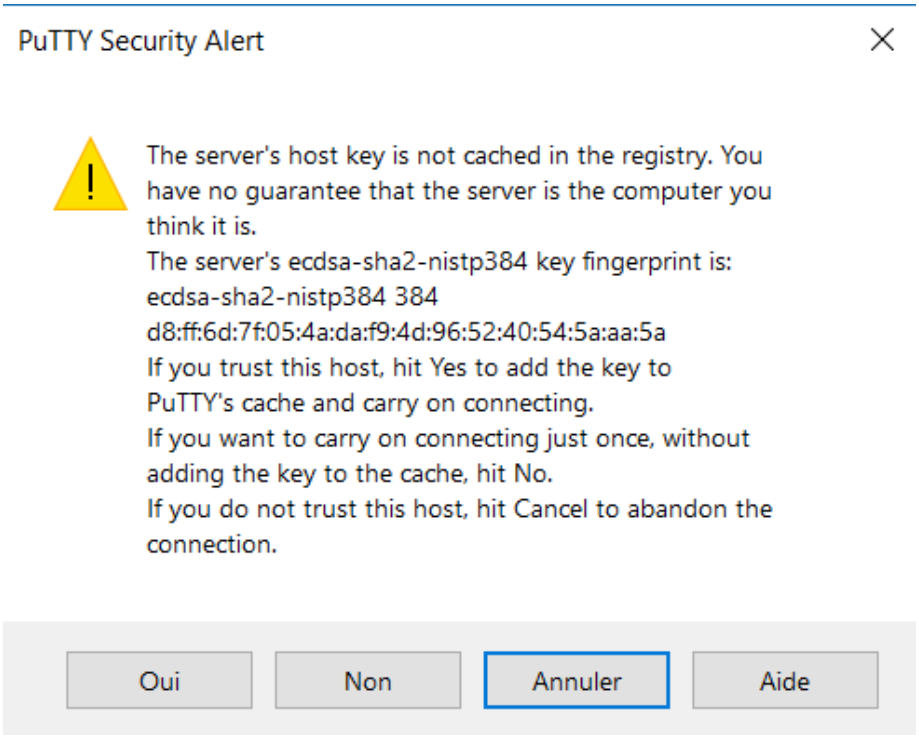
# Table des matières



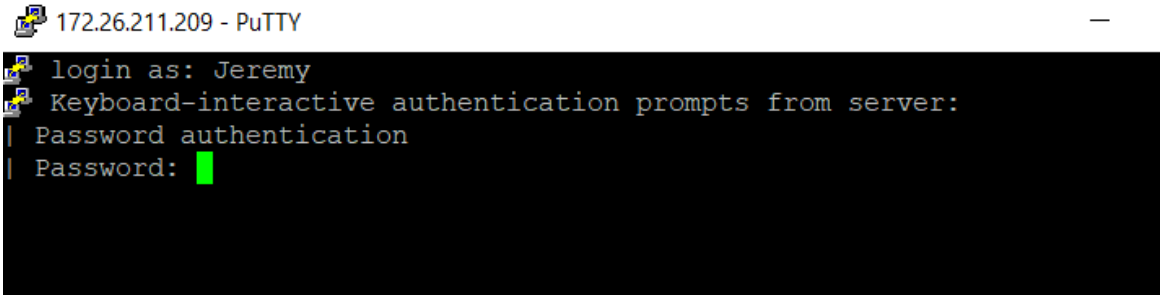
# Troisième TP : Administration SSH (Première partie)

Pour ce TP je travaille sur un seul ordinateur physique Windows.

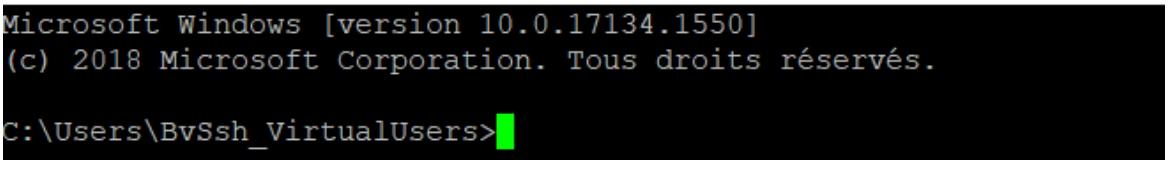
## Objectif 1 :

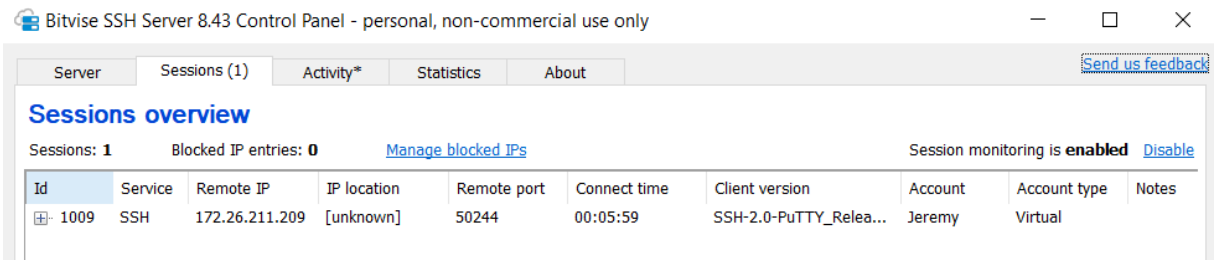



On essaye de se connecter grâce à PuTTY au serveur SSH, mais comme il ne connait pas l'hôte il nous prévient qu'il peut s'agir d'une machine inconnue, cependant on peut ajouter la clé de l'hôte afin de se connecter plus facilement.



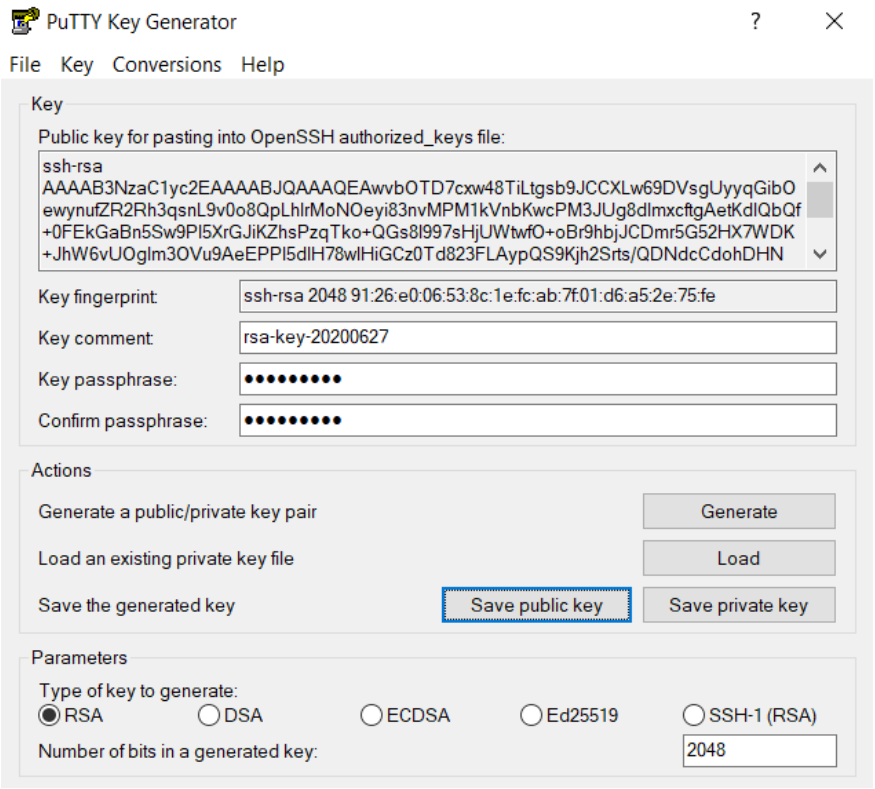

Une fois qu'on a rentré l'adresse IP dans PuTTY on peut se connecter à notre serveur SSH en rentrant notre MDP en utilisant le nom d'utilisateur que l'on a inscrit plus tôt.



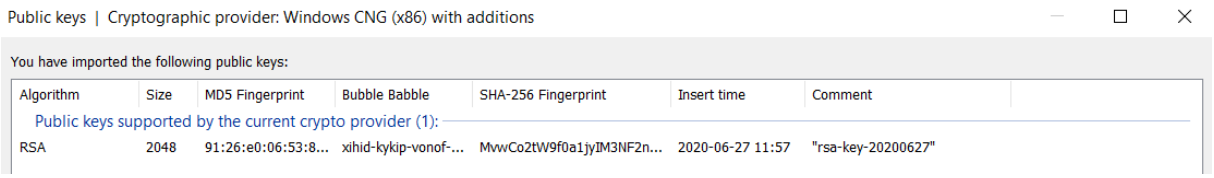




Comment on peut le voir dans notre serveur la connexion entre le client et le serveur est effectué.

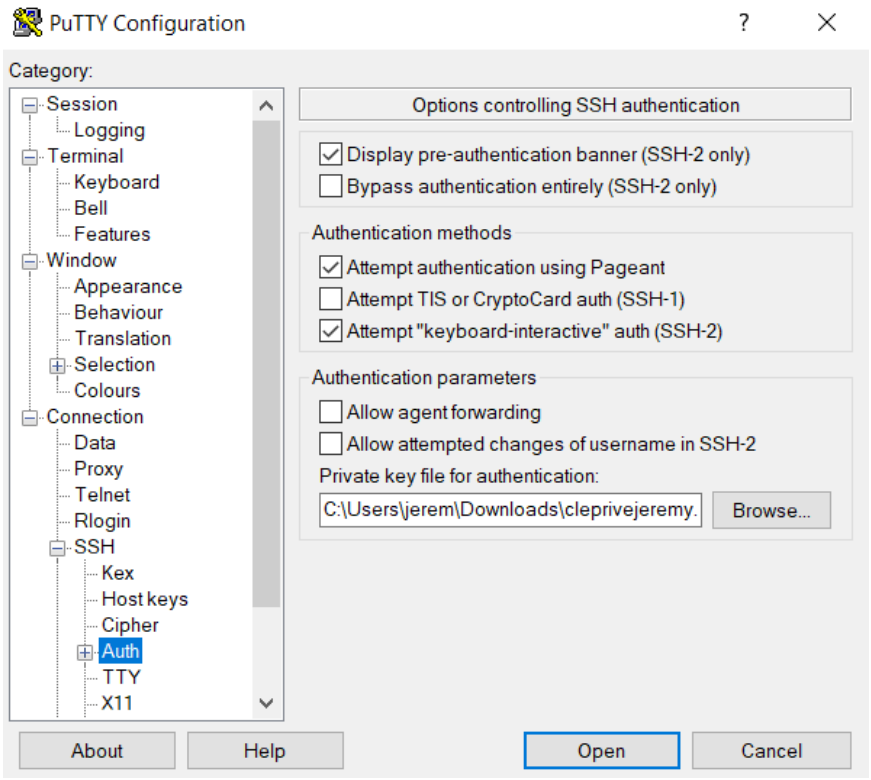
# Objectif 2 :



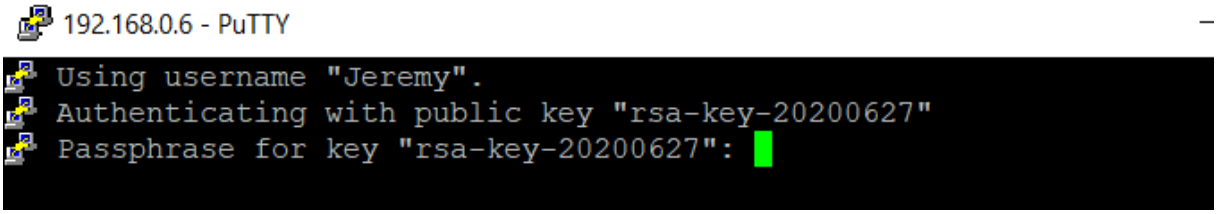

On utilise PuTTY Gen afin de générer une clef publique et privé afin les importer dans PuTTY et Bitvise.



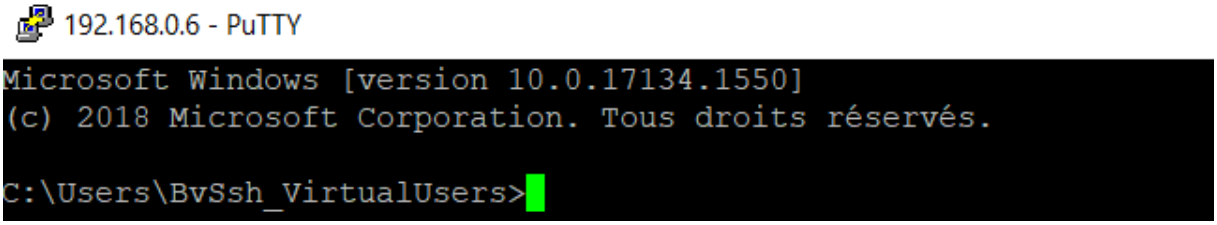

Dans Bitvise on ajoute la clé privée dans notre serveur SSH.




Enfin dans PuTTY on ajoute la clé privée que l'on a généré précédemment.




Maintenant, on lance la connexion entre le client et le serveur, désormais le serveur requière la passphrase qu'on a ajouté plus tôt.



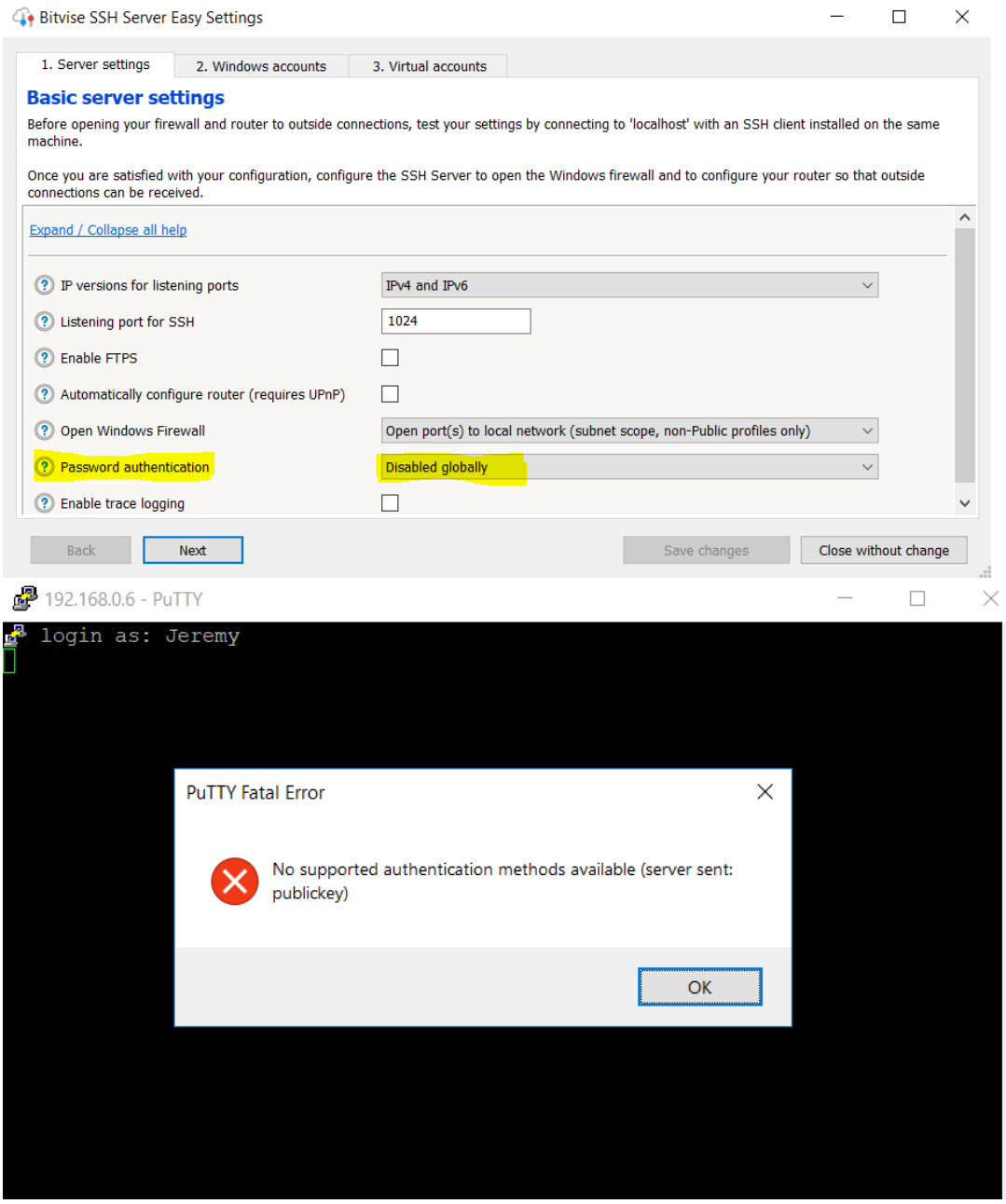

Une clé privée nous permet de nous connecter de manière plus sécuriser sans avoir à retenir plusieurs mots de passe par serveur, ici on a juste à posséder la passphrase pour se connecter.

On peut également désactiver la connexion par mot de passe pour plus de sécurité.

## Quatrième TP : Administration SSH (Deuxième partie)

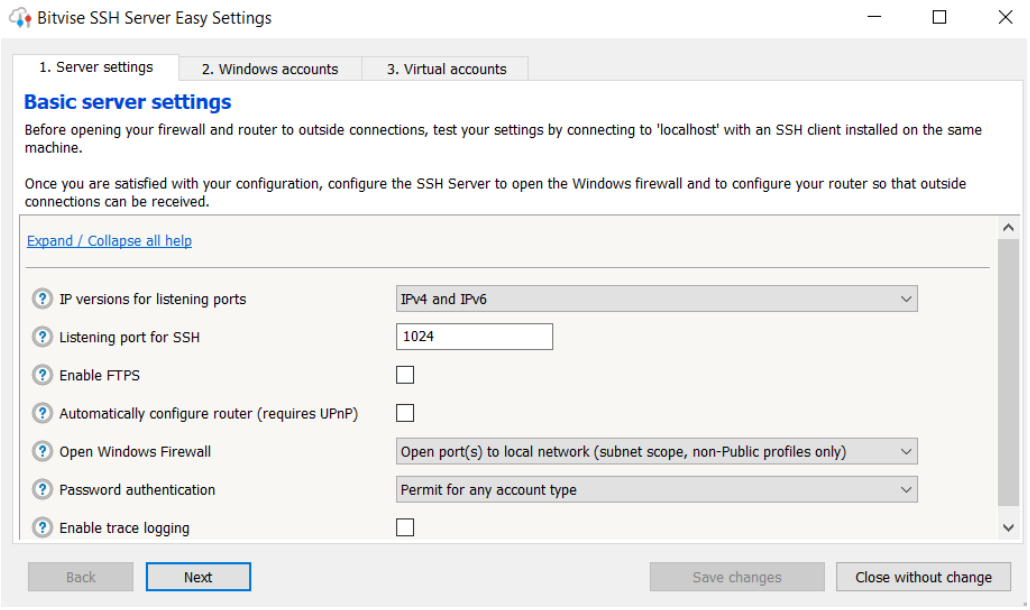
Il existe de nombreuses optimisations possibles :

1. Désactiver la connexion par mot de passe :

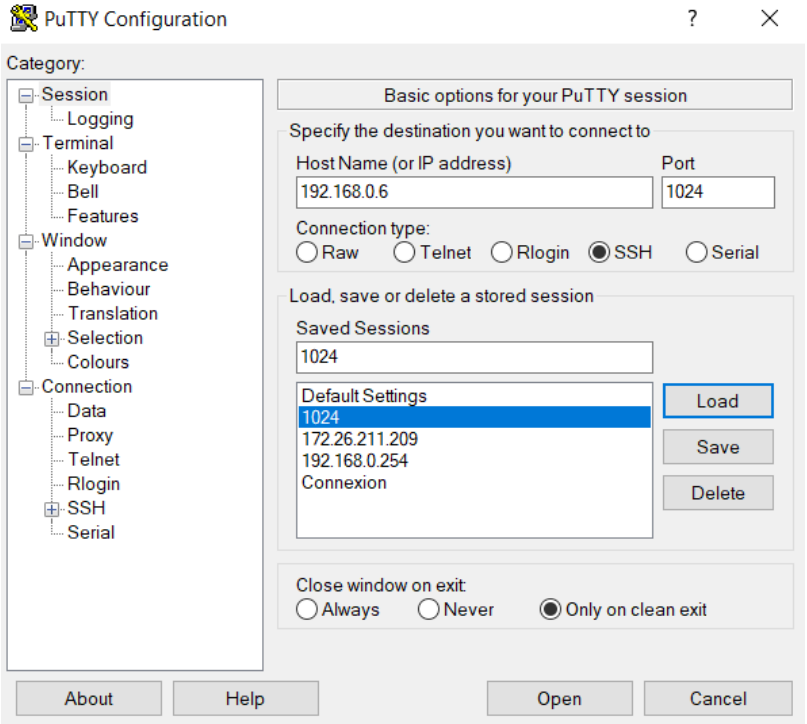



Jusqu'alors la connexion par MDP était possible cependant on peut faire sorte que cela ne soit plus possible, dans les options de notre serveur on peut désactiver la connexion par MDP.

2. Changer le port de connexion

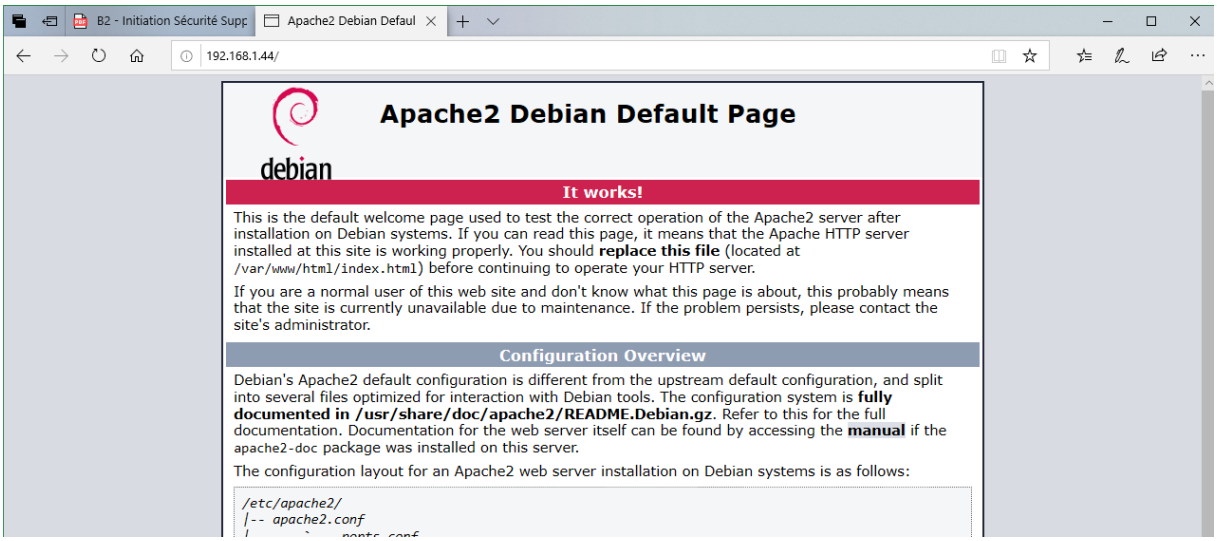



Dans notre serveur SSH on peut paramétrer le port d'écoute ici j'ai choisi le port 1024.

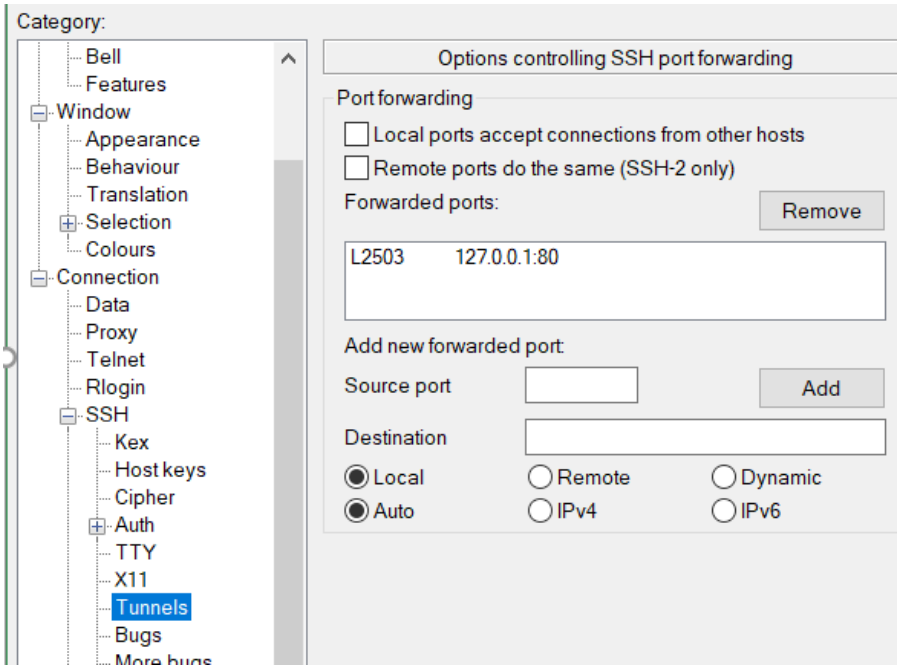



Enfin dans PuTTY on a juste à changer le port par celui correspondant au serveur.

## Tunnel SSH :

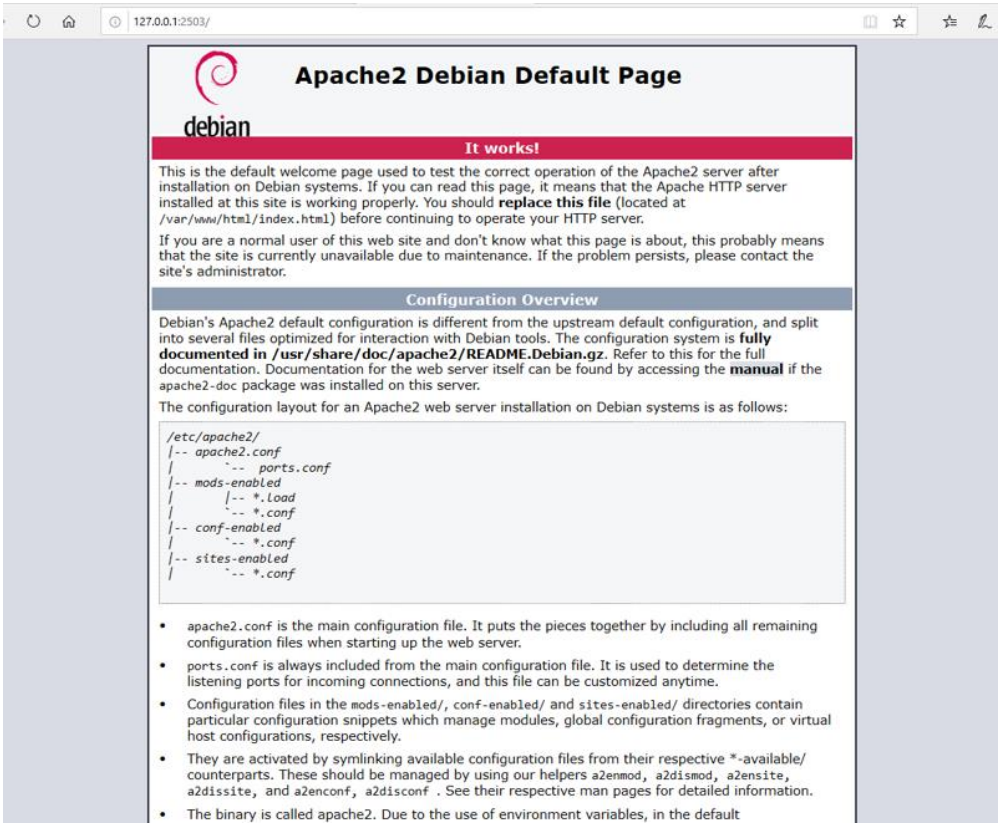



J’ai installé apache2 afin de simuler un serveur, nous allons utiliser un tunnel afin de faire de la redirection sur ce serveur afin de simuler un localhost.




Tout d’abord, dans PuTTY on configure notre tunnel.

Nous allons utiliser le port source 2503 afin de faire de la redirection.

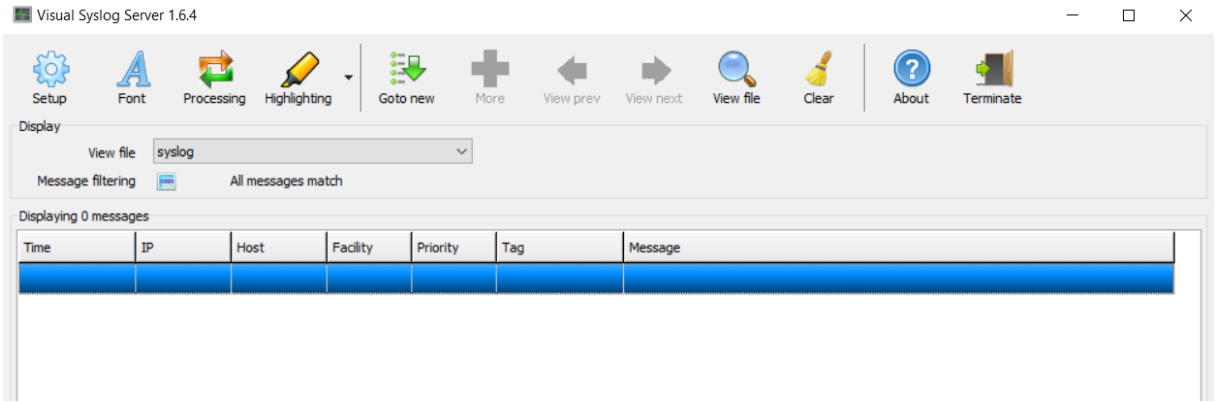



On voit bien que la connexion a eu lieu grâce au tunnel mis en place précédemment.

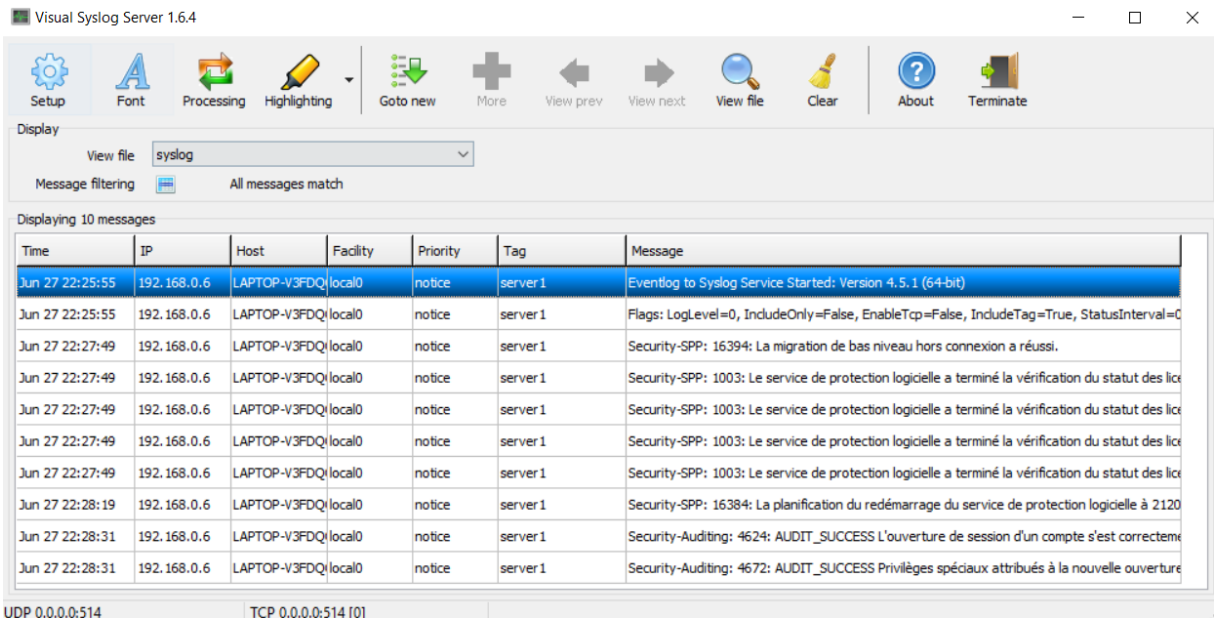
Le tunneling est un protocole de communication qui permet le transfert de données d'un réseau à un autre.  Il permet d'envoyer des communications sur un réseau privé à travers un réseau public, ce processus s'appelle l'encapsulation. Dans ce processus d'encapsulation, les paquets de données apparaissent comme s'ils étaient de nature publique sur un réseau public alors qu'en réalité ils sont considérés comme des paquets de données privés. Cela leur permet de passer inaperçus.

L'avantage de créer un tunnel SHH est qu'il permet de crypter et d'anonymiser les flux entre le client SHH et le serveur (ce qui représente une alternative à un VPN).

## Cinquième TP : Syslog




Le serveur Syslog nous permettra de gérer les logs es événements qui vont se produire.



```
C:\Windows\system32>evtsys -i -h 192.168.0.6 -f local0 -t server1 -l 0
Command completed successfully

C:\Windows\system32>net start evtsys

Le service Eventlog to Syslog a démarré.
```

Ensuite on installe Evtsys qui permet de transférer les événements vers notre serveur Syslog (-i Install service ; -h host Name of log host(s) ; f facility Facility level of syslog message).

## Vérification de la réception des logs

View file: syslog

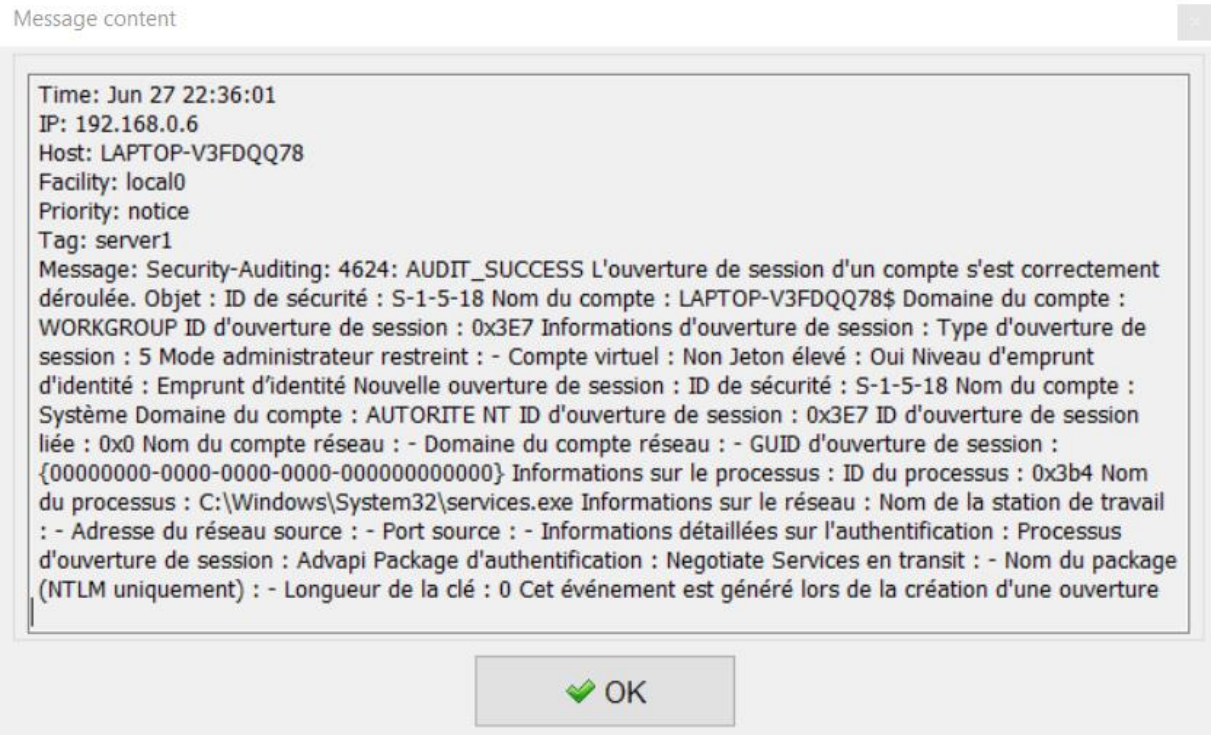
Message filtering: All messages match

Displaying 10 messages

| Time | IP | Host | Facility | Priority | Tag | Message |
|---|---|---|---|---|---|---|
| Jun 27 22:25:55 | 192.168.0.6 | LAPTOP-V3FDQ | local0 | notice | server1 | Eventlog to Syslog Service Started: Version 4.5.1 (64-bit) |
| Jun 27 22:25:55 | 192.168.0.6 | LAPTOP-V3FDQ | local0 | notice | server1 | Flags: LogLevel=0, IncludeOnly=False, EnableTcp=False, IncludeTag=True, StatusInterval= |
| Jun 27 22:27:49 | 192.168.0.6 | LAPTOP-V3FDQ | local0 | notice | server1 | Security-SPP: 16394: La migration de bas niveau hors connexion a réussi. |
| Jun 27 22:27:49 | 192.168.0.6 | LAPTOP-V3FDQ | local0 | notice | server1 | Security-SPP: 1003: Le service de protection logicielle a terminé la vérification du statut des lic |
| Jun 27 22:27:49 | 192.168.0.6 | LAPTOP-V3FDQ | local0 | notice | server1 | Security-SPP: 1003: Le service de protection logicielle a terminé la vérification du statut des lic |
| Jun 27 22:27:49 | 192.168.0.6 | LAPTOP-V3FDQ | local0 | notice | server1 | Security-SPP: 1003: Le service de protection logicielle a terminé la vérification du statut des lic |
| Jun 27 22:27:49 | 192.168.0.6 | LAPTOP-V3FDQ | local0 | notice | server1 | Security-SPP: 1003: Le service de protection logicielle a terminé la vérification du statut des lic |
| Jun 27 22:28:19 | 192.168.0.6 | LAPTOP-V3FDQ | local0 | notice | server1 | Security-SPP: 16384: La planification du redémarrage du service de protection logicielle à 2120 |
| Jun 27 22:28:31 | 192.168.0.6 | LAPTOP-V3FDQ | local0 | notice | server1 | Security-Auditing: 4624: AUDIT_SUCCESS L'ouverture de session d'un compte s'est correctem |
| Jun 27 22:28:31 | 192.168.0.6 | LAPTOP-V3FDQ | local0 | notice | server1 | Security-Auditing: 4672: AUDIT_SUCCESS Privilèges spéciaux attribués à la nouvelle ouverture |

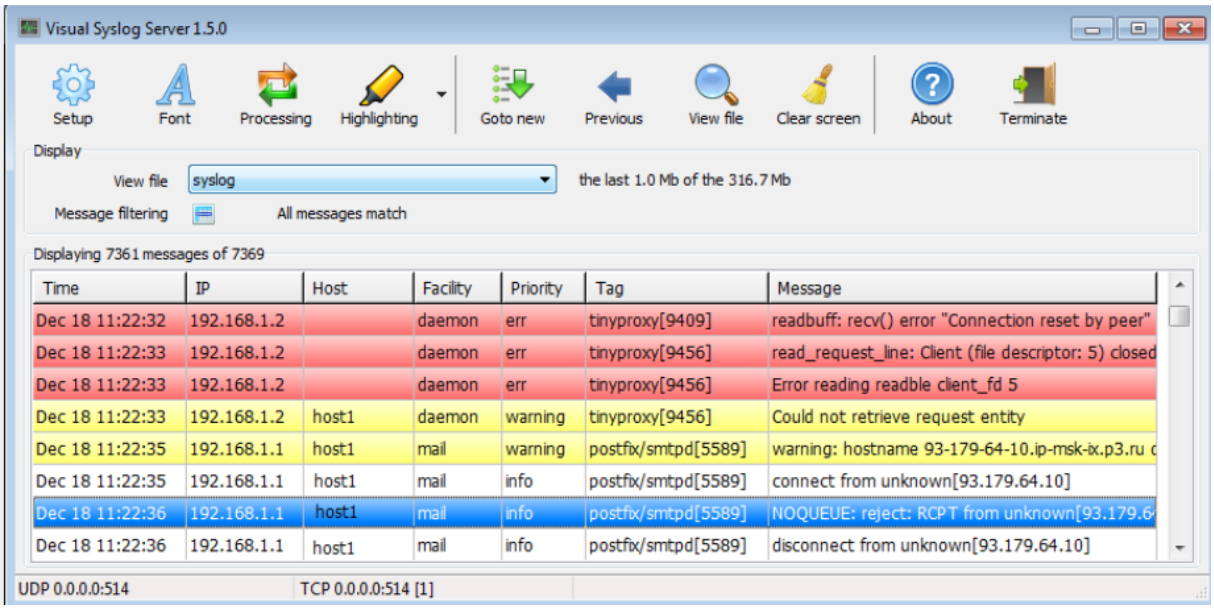
UDP 0.0.0.0:514 TCP 0.0.0.0:514 [0]

Après cette mise en place, on remarque que notre serveur Syslog reçoit bien les logs.




Ici par exemple, nous avons un log de connexion à un compte, on y retrouve l'heure de connexion, l'adresse IP, le nom d'hôte, la priorité et un message.

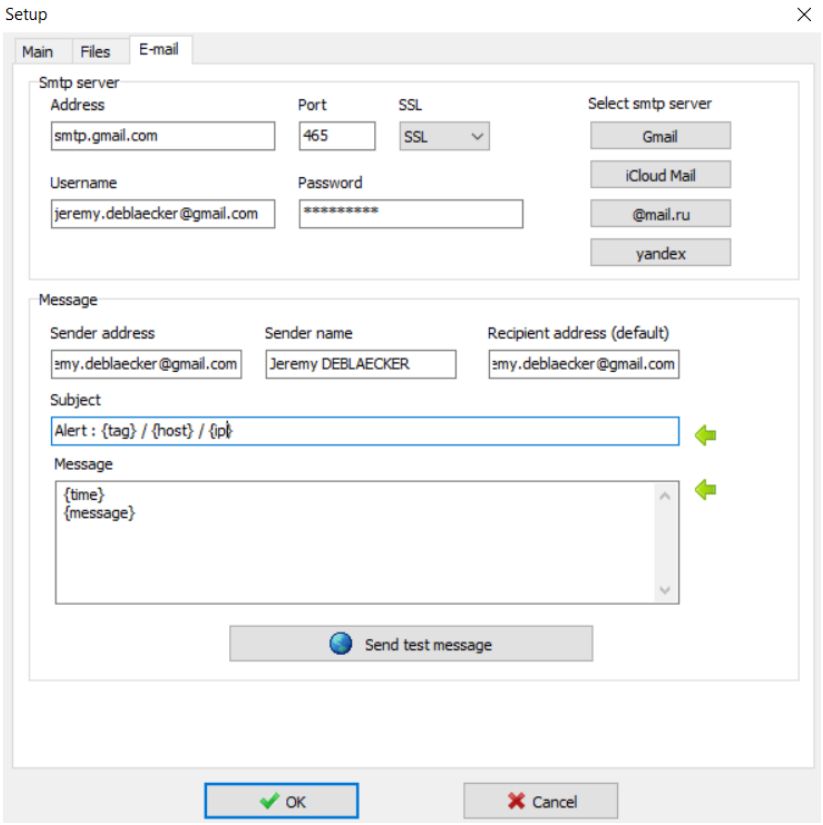
## Recherche / Identification (comprendre les niveaux de gravité...)




Il existe différent type de gravités, certains sont juste là pour fournir une information mais d'autres peuvent prévenir de problème plus grave (erreur de fonctionnement, système inutilisable…) :

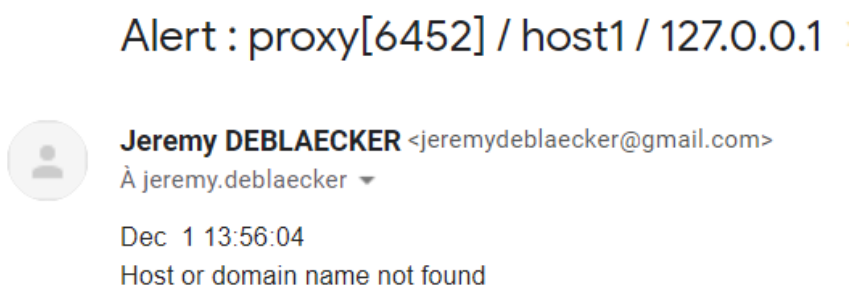
| Code | Gravité | Mot-clé | Description |
|---|---|---|---|
| 0 | Emergency | emerg (panic) | Système inutilisable. |
| 1 | Alert | alert | Une intervention immédiate est nécessaire. |
| 2 | Critical | crit | Erreur critique pour le système. |
| 3 | Error | err (error) | Erreur de fonctionnement. |
| 4 | Warning | warn (warning) | Avertissement (une erreur peut intervenir si aucune action n'est prise). |
| 5 | Notice | notice | Événement normal méritant d'être signalé. |
| 6 | Informational | info | Pour information. |
| 7 | Debugging | debug | Message de mise au point. |

## Paramétrage et émission d'alertes (exemple Mail)



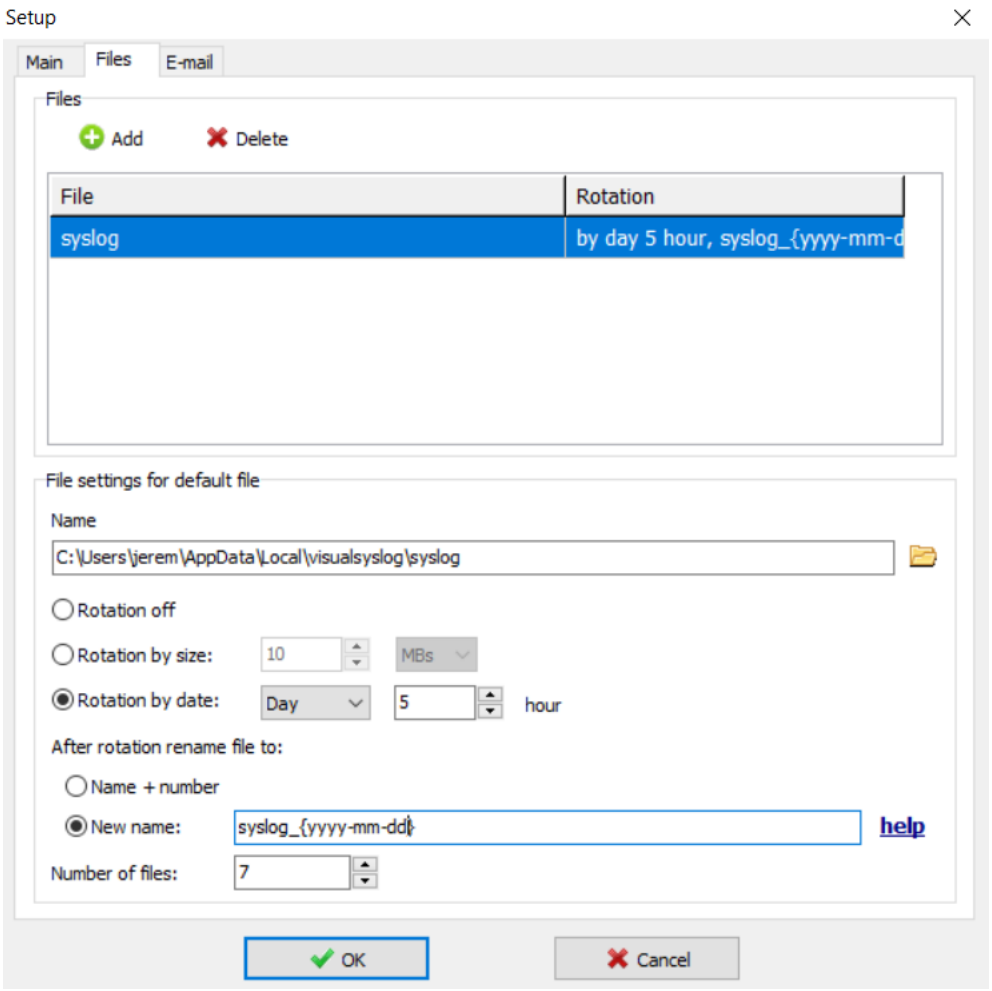

Nous allons maintenant paramétrer notre serveur afin de recevoir par email les différentes alertes dans nos logs.


Pour ce faire je dois activer dans mes paramètres mails, « Autoriser les applications moins sécurisées ».




Ensuite je vérifie que j'ai bien reçu l'email de test : l'opération a fonctionné.

## Rotation des fichiers de log




Nous mettons en place maintenant des fichiers de Logs, il créera toutes les 5 heures tous les jours un fichier contenant des logs.

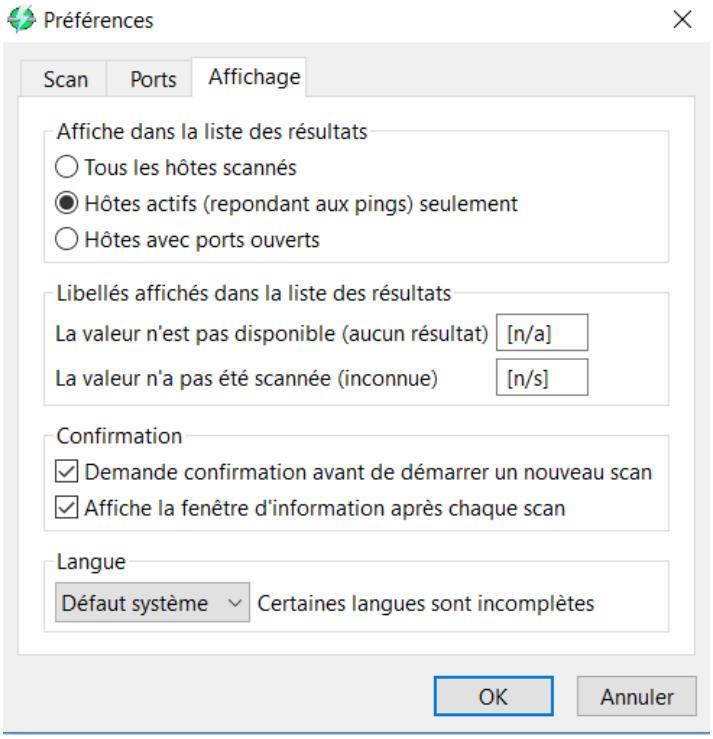
Sauvegarder ces logs est essentiel car requis par la loi, cependant ces logs peuvent être nombreuse c'est pour ca qu'il est également important de les filtrer avant de les envoyer par mail (par exemple, envoyer seulement les logs d'error).

Certains logs doivent être sauvegarder conformément à la Loi sur la Sécurité Quotidienne de 2001, mets ces logs doivent être anonymiser afin de protéger la vie privée des utilisateurs. Chaque entreprise est obligée de sauvegarder ces logs pendant un an afin que les autorités judiciaires puissent y accéder en cas de problème.

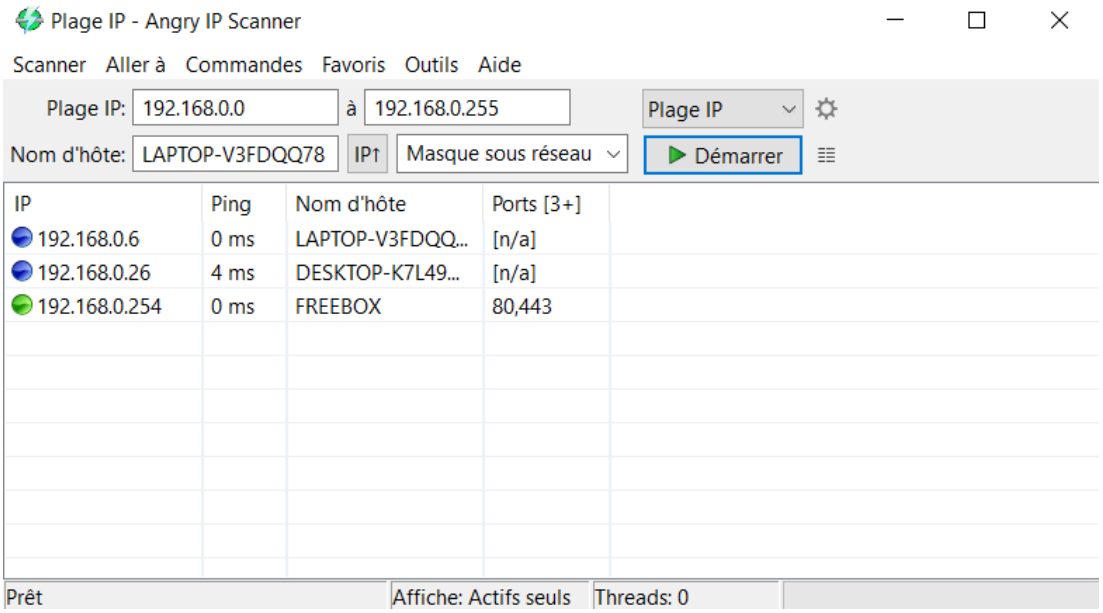
# Sixième TP : Découverte des Scanners

## Angry IP Scanner

Angry IP Scanner est un scanner d'adresse IP qui permet de récupérer les adresses IP d'un réseau.




Afin d'afficher seulement les IP actives, il suffit d'activer l'option hôte actif dans les paramètres.



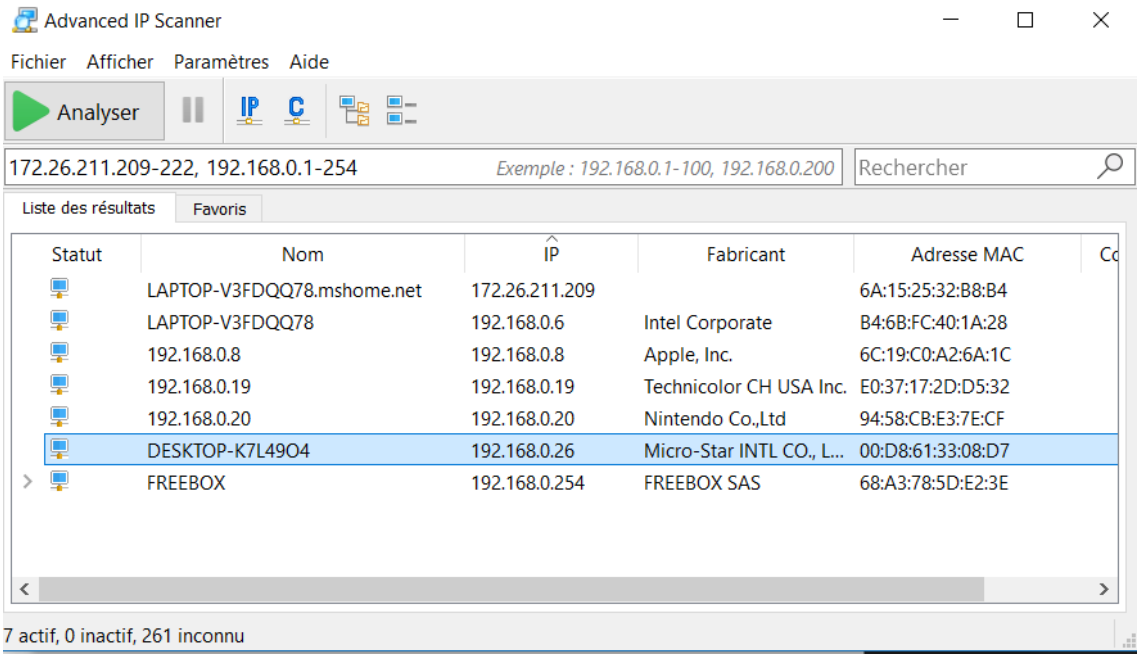

Angry IP Scanner est très simple d'utilisation puisqu'il suffit juste de rentrer la plage IP qui nous intéresse pour voir les résultats.

Comme vous pouvez le voir le scanner repère trois hôtes : mon ordinateur portable et fixe ainsi que ma Freebox.

Grâce au scanner, on peut connaitre l'adresse IP, le nom d'hôte et le port de chacun des périphériques connectés au réseau.

Malheureusement, je remarque que certains hôtes n'apparaissent pas, par exemple, je sais qu'il a des téléphones et des tablettes connectées à ce réseau qui ne sont pas prisent en compte par le scanner.

## Advanced IP Scanner

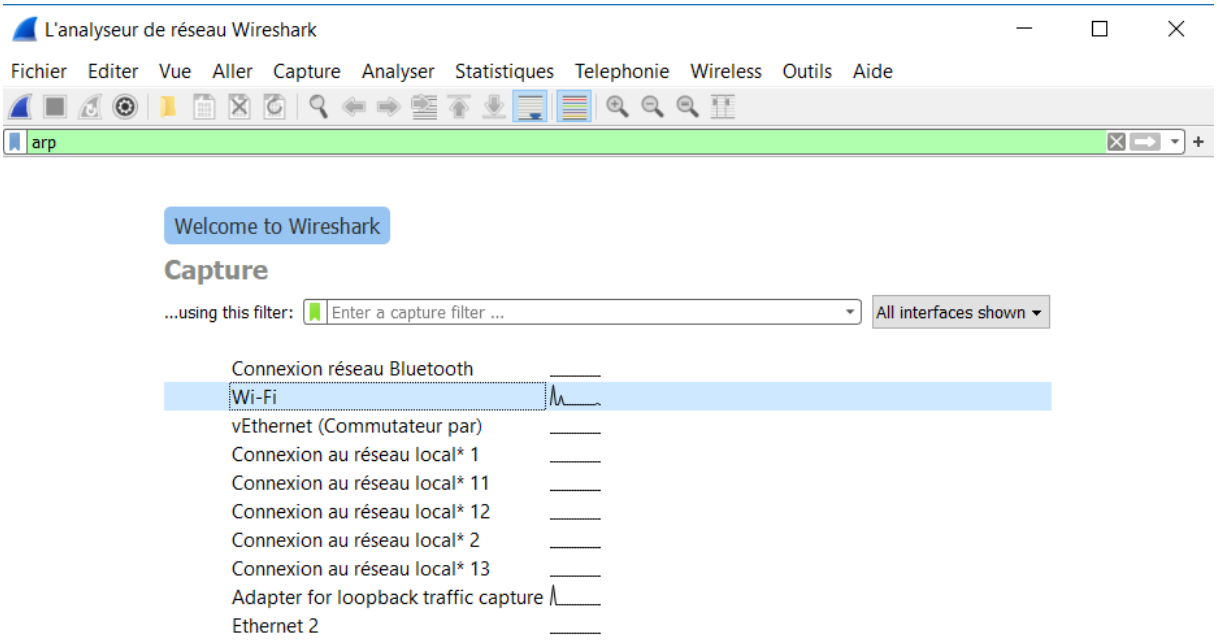



En utilisant Advanced IP Scanner je remarque, qu'il repère trois autres d'adresse IP, cependant il ne récupère pas le nom d'hôte de ces nouvelles IP. Je dois donc déduire à qui appartient ces IP : je remarque un produit Apple (surement mon téléphone), un produit Nintendo (une Switch) et la box Canal (fabricant technicolor CH USA).

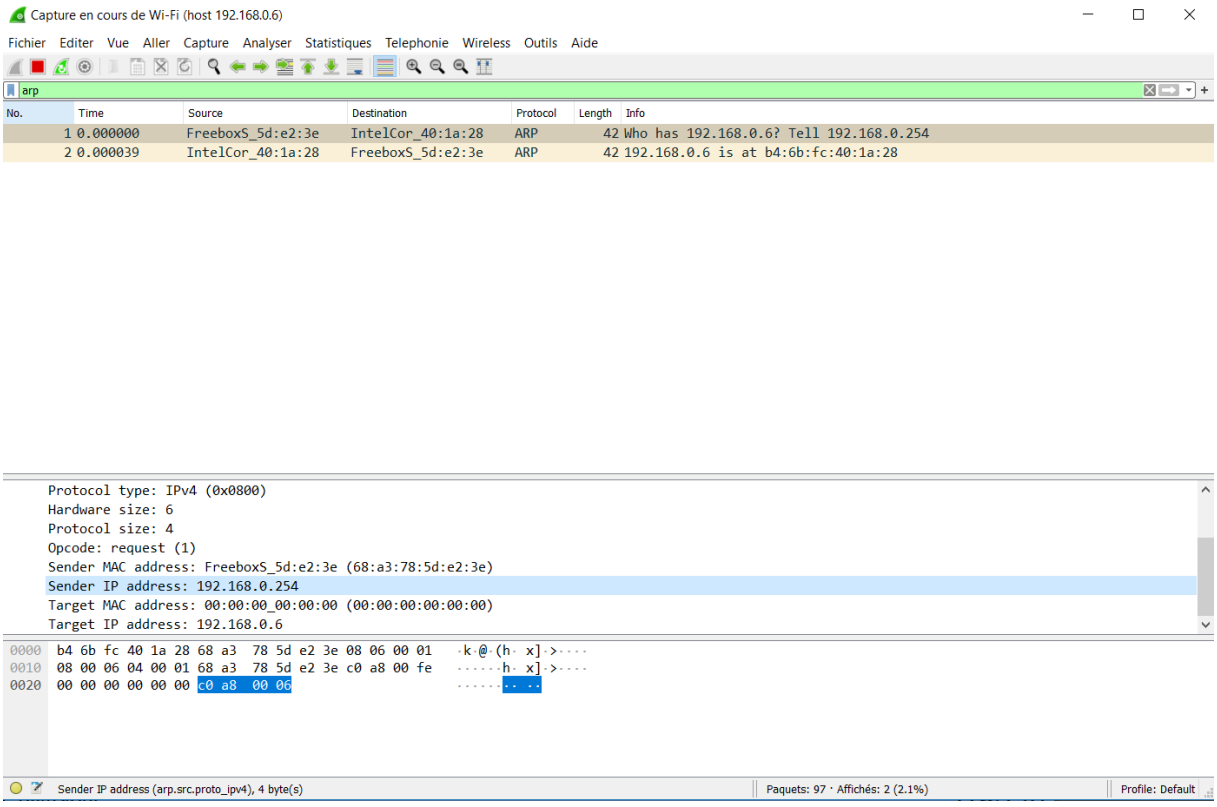
Cependant malgré ces nouveaux hôtes, certains n'apparaissent toujours pas (téléphone/tablette).

# Septième TP : Écoute et Analyse du réseau

## Étape #1




Sur Wireshark je capte les requêtes ARP sur le réseau entre mon PC et les périphériques.

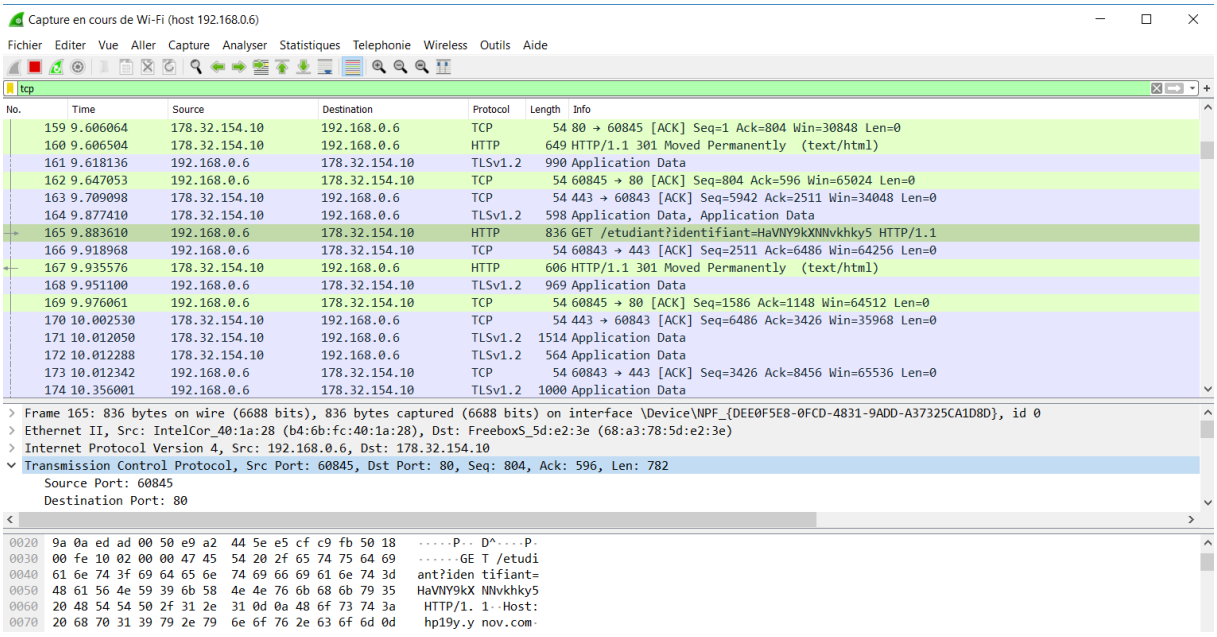



Ici je vois bien que ma Freebox envoie une requête vers mon PC et il lui répond.

```
Interface : 192.168.0.6 --- 0x18
  Adresse Internet      Adresse physique      Type
  192.168.0.5           f8-d0-ac-19-72-db     dynamique
  192.168.0.19          e0-37-17-2d-d5-32     dynamique
  192.168.0.20          94-58-cb-e3-7e-cf     dynamique
  192.168.0.26          00-d8-61-33-08-d7     dynamique
  192.168.0.42          a4-d9-31-65-3b-ca     dynamique
  192.168.0.254         68-a3-78-5d-e2-3e     dynamique
  192.168.0.255         ff-ff-ff-ff-ff-ff     statique
  224.0.0.22            01-00-5e-00-00-16     statique
  224.0.0.251           01-00-5e-00-00-fb     statique
  224.0.0.252           01-00-5e-00-00-fc     statique
  239.255.255.250       01-00-5e-7f-ff-fa     statique
  255.255.255.255       ff-ff-ff-ff-ff-ff     statique
```

En consultant le cache ARP de mon poste je vois bien que l'adresse ip qui m'a contacté est dans la liste des adresses IP.

## Étape #2




Depuis l'extranet d'Ynov je me connecte à mon compte, wireshark capte cette connexion. En effet mon ip (192.168.0.6) se connecte à ynov (178.32.154.10). On voit dans les informations de cette connexion que je fourni mes identifiants étudiants grâce au protocole HTTP.

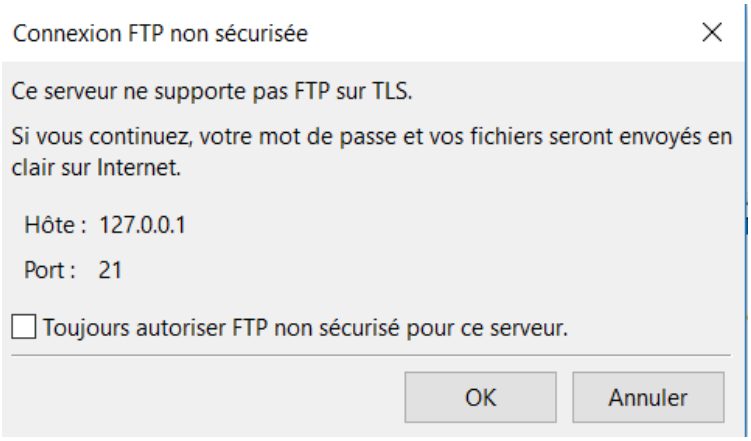
```
C:\Users\jerem>ping hp19y.ynov.com

Envoi d'une requête 'ping' sur reverseproxy2.ynov.com [178.32.154.10] avec 32 octets de données :
Réponse de 178.32.154.10 : octets=32 temps=44 ms TTL=56
Réponse de 178.32.154.10 : octets=32 temps=43 ms TTL=56
Réponse de 178.32.154.10 : octets=32 temps=43 ms TTL=56
Réponse de 178.32.154.10 : octets=32 temps=44 ms TTL=56

Statistiques Ping pour 178.32.154.10:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 43ms, Maximum = 44ms, Moyenne = 43ms
```

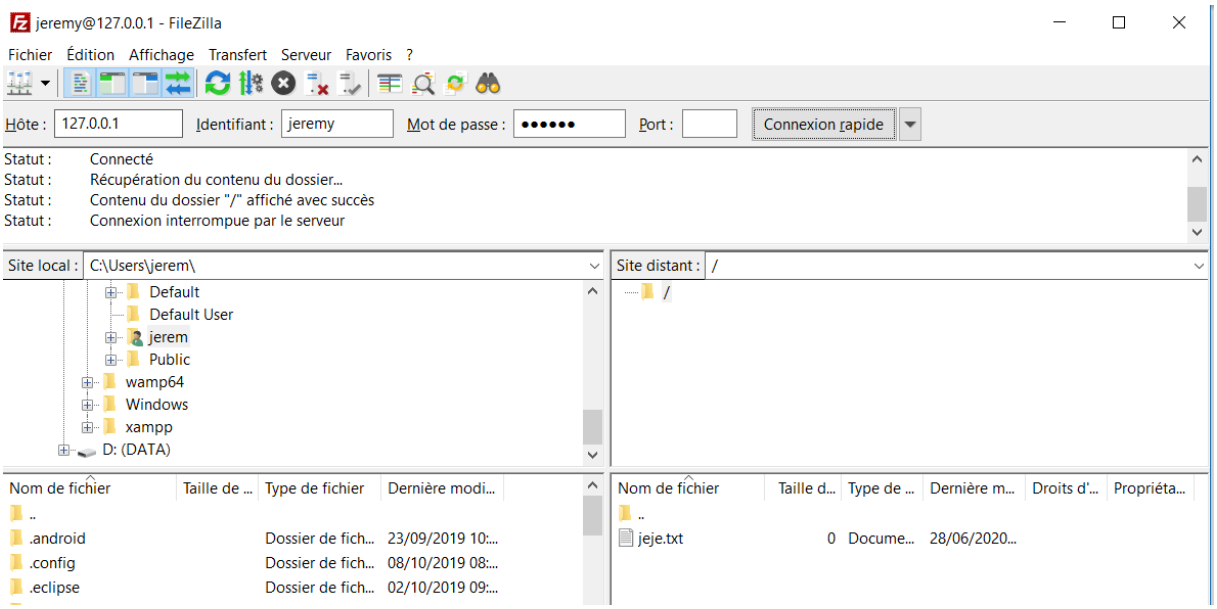
J'essaye de pinger Ynov depuis mon terminal afin de vérifier qu'il s'agit bien de son adresse IP, je remarque que c'est bien l'adresse IP d'Ynov.

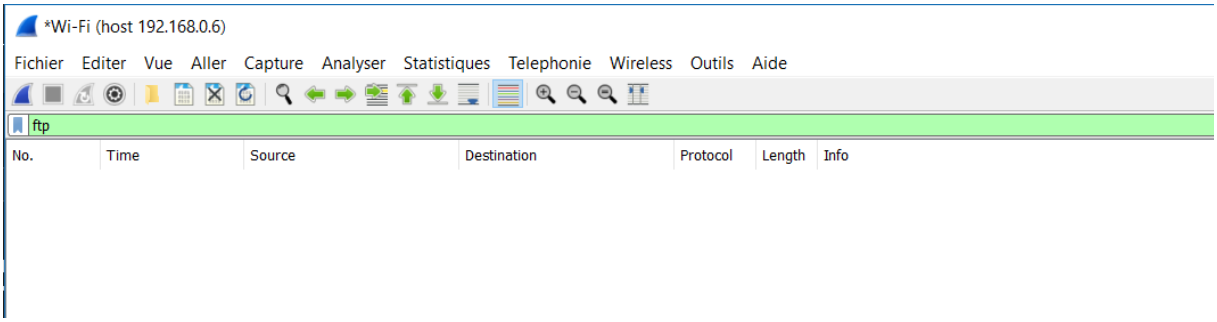
Le numéro de séquence est choisi aléatoirement par les machines quand elles communiquent entre elles, en effet la création d'un numéro de séquence permet d'identifier la session. La création d'un numéro de séquence permet d'éviter les piratages.

## Étape #3

J'ai essayé de créer une communication entre le serveur FTP et mon hôte mais malheureusement je n'ai pas réussi à créer de communication entre les deux.






J’ai pense cependant avoir paramétrer correctement FileZilla puisque j’arrive à récupérer le fichier que j’avais préalablement créé dans mes fichiers en utilisant le compte que j’avais créé.