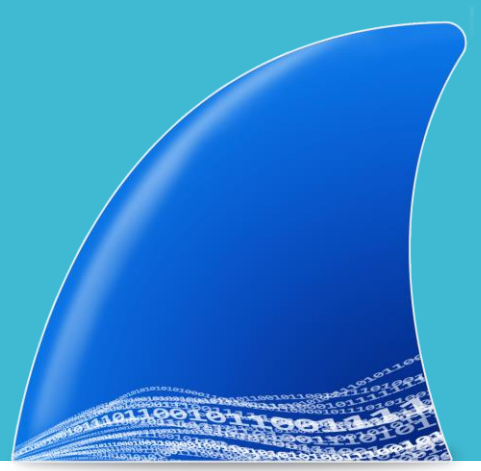
TP B1 : Wireshark

Hego Maxence

Installation :



Pour Windows :

- Télécharger Wireshark sur le site officiel : https://www.wireshark.org/download.html
- Exécuter en tant que administrateur : permet de capturer le trafic sur la ou les cartes réseaux

Pour Linux :

- sudo apt install wireshark
- sudo wireshark

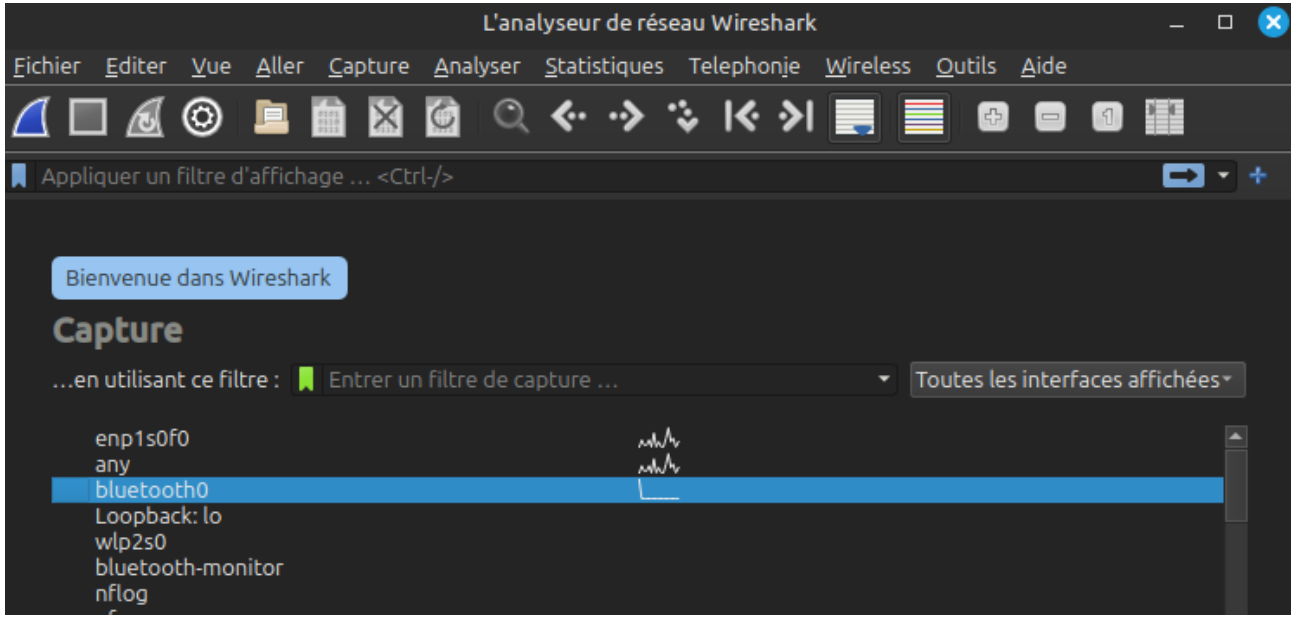
WIRESHARK

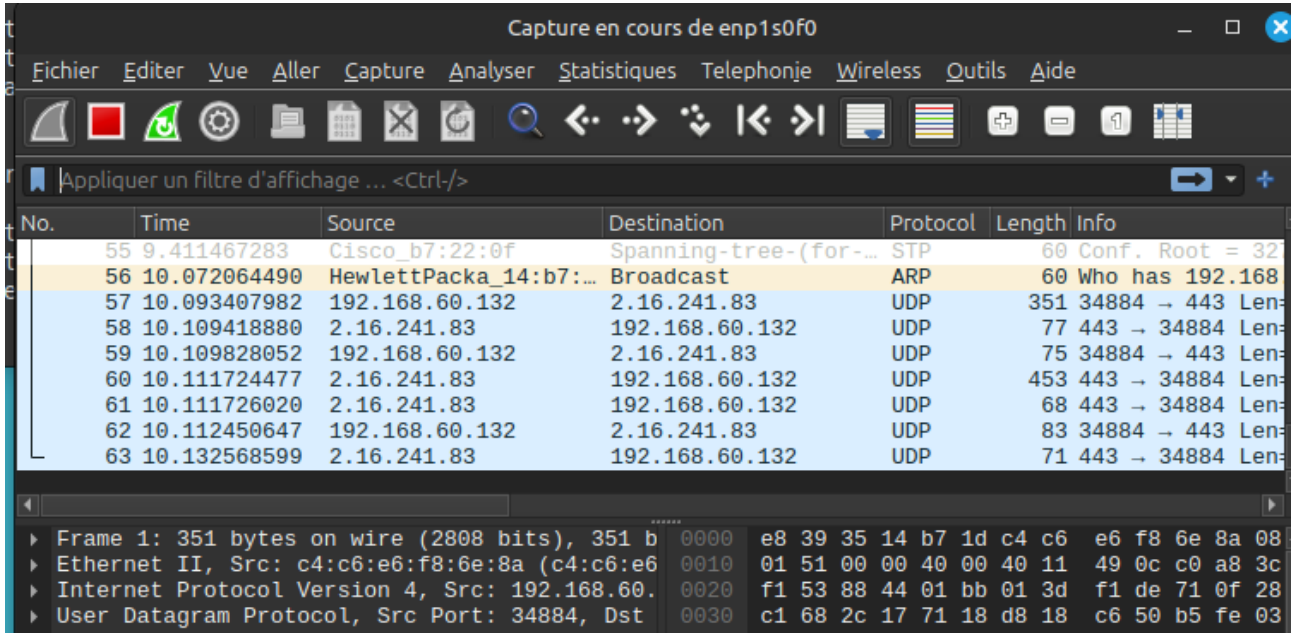
Utilisation :

Lancement wireshark :

- Une liste des interfaces apparaît
- On sélectionne notre carte réseau (ici : enp1s0f0)

La capture de la trame fonctionne





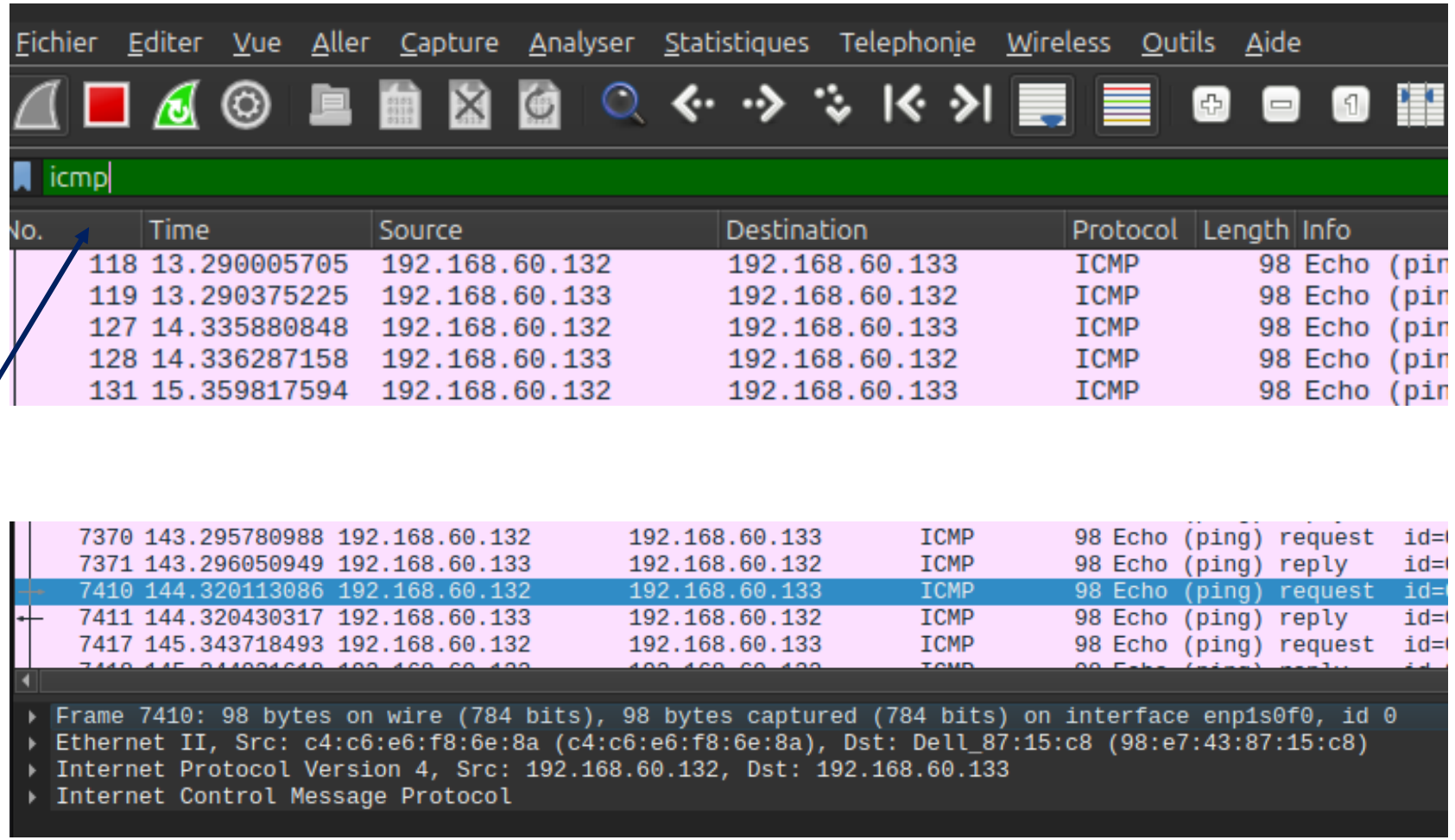
Capture trame ICMP :

Ping de mon voisin :
- ping 192.168.60.133

Filtrage :

On entre le protocole que l'on souhaite analyser, ici ICMP

En cliquant sur une des frames, on obtient des informations sur cette frame.

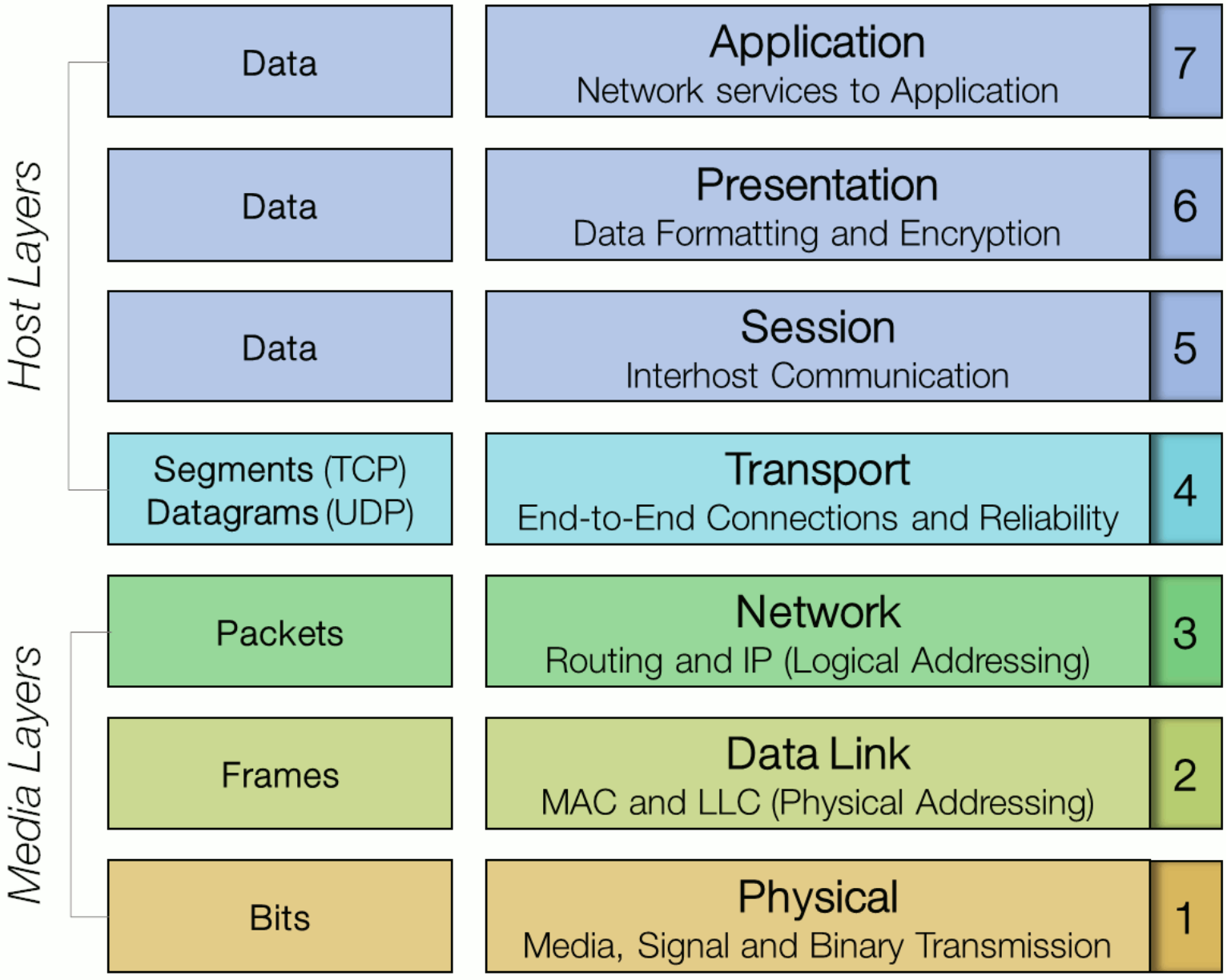


Analyse d'une Frame : Le modèle OSI :

Le **modèle OSI** est un modèle conceptuel utiliser pour faciliter la compréhension des réseaux.

Il est divisé en **sept couches,** à chacune de ces couches est associé une **PDU ou Protocole Data Units**.

Une Frame est la PDU de la seconde couche de ce modèle.

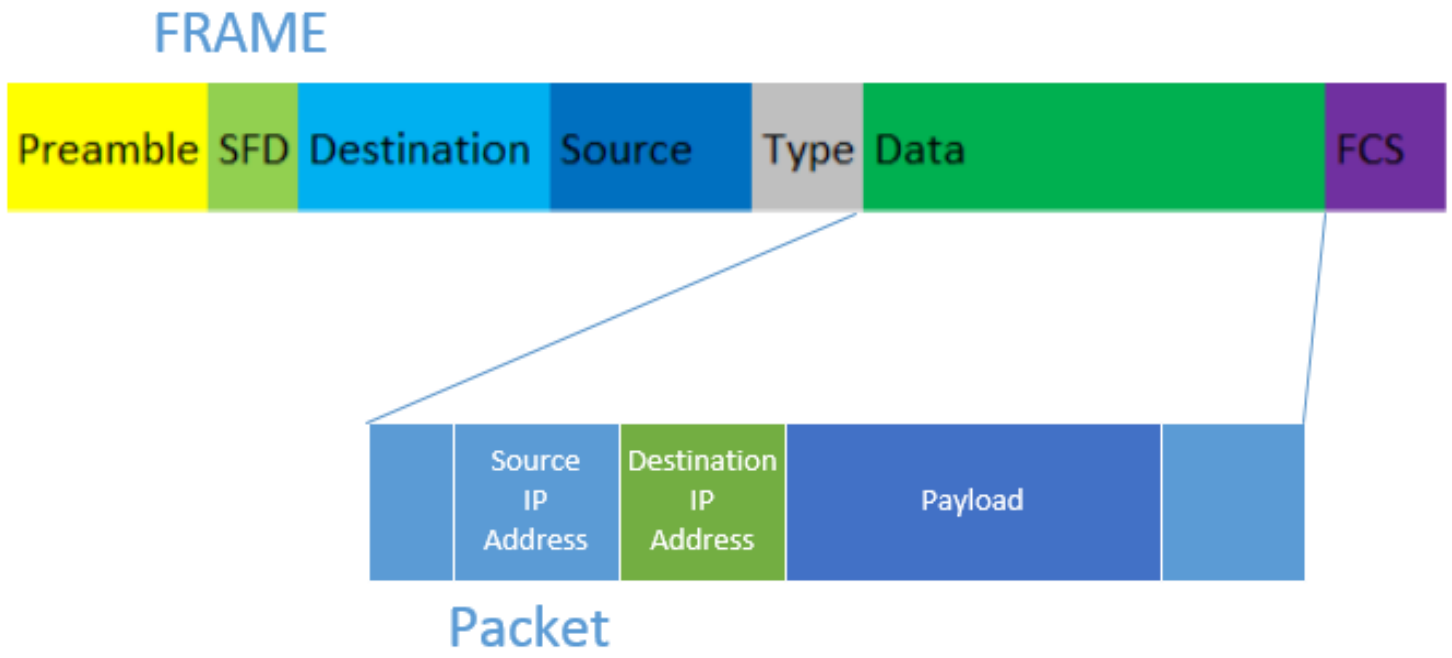


Composition d'une Frame:

Une frame = ethernet header + packet + ethernet trailer

Le packet est le PDU de la troisième couche du modèle OSI.

Le Header d'une frame est composé du :
Preamble, SFD, Destination, Source et Type.



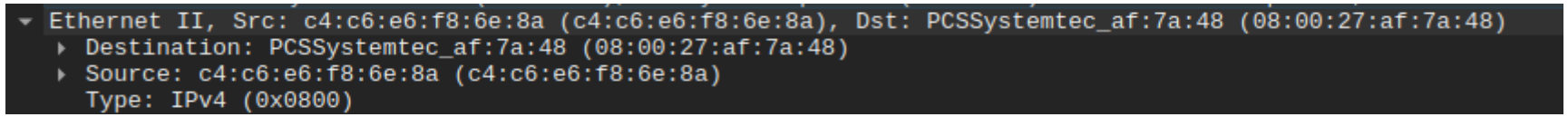
Analyse de la frame dans Wireshark:

Dans Wireshark, on peut retrouver les éléments du Ethernet header d'une frame ICMP notamment l'adresse MAC source et destination.

Adresse Mac :

- L'adresse Mac est **un identifiant unique à chaque machine** composée de 12 caractères hexadécimaux.

- **Adresse mac source** : identifiant de la machine qui envoie le Ping
- **Adresse mac destination** : identifiant de la machine qui reçoit le Ping



La Mac adresse se trouve bien dans la partie Ethernet :

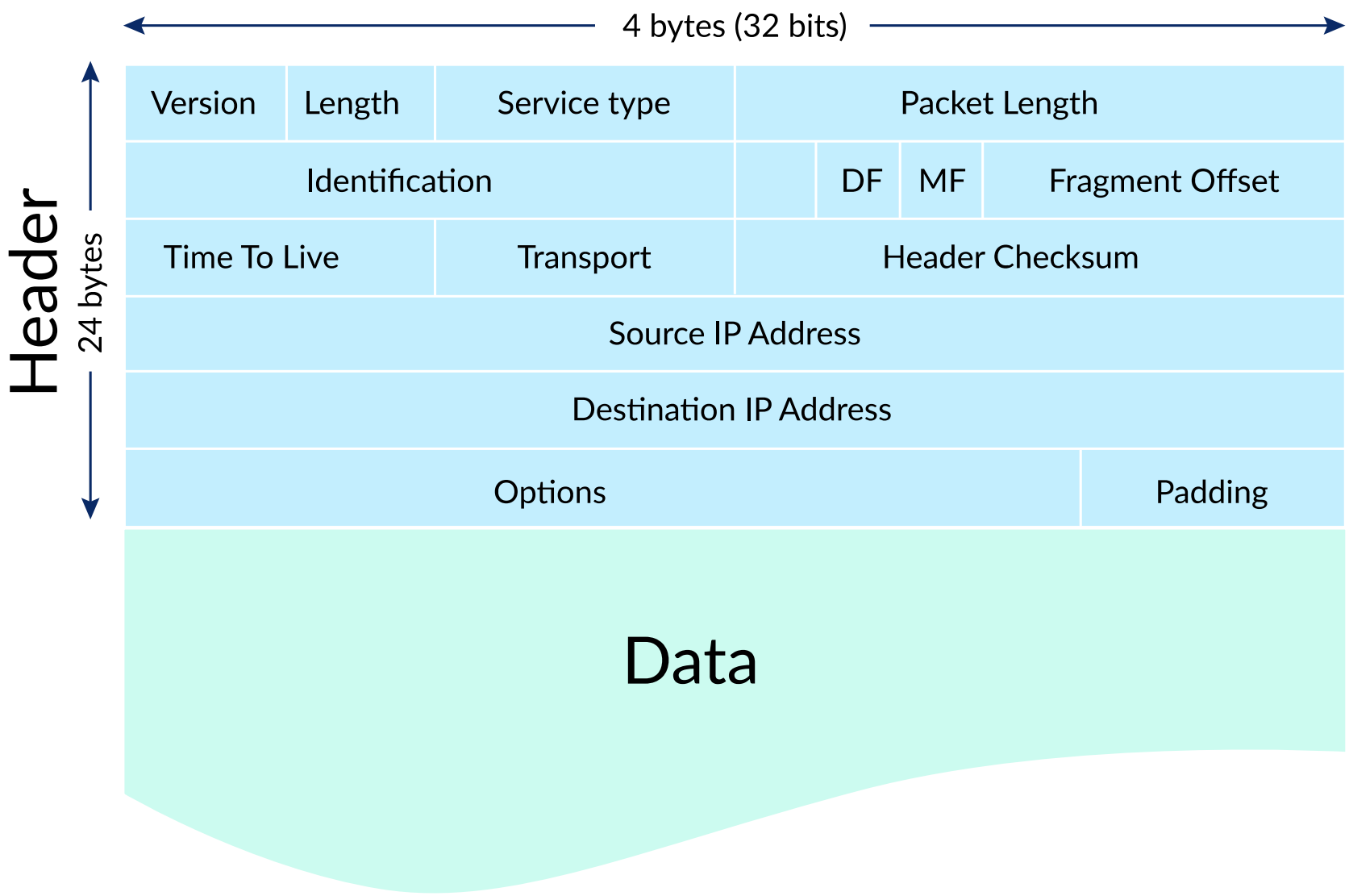
- **Destination** : 08 : 00 :27 : af : 7a : 48
- **Source** : c4 : c6 : e6 : f8 : 6e : 8a

Composition d'un packet :

Un packet est composé du segment (PDU de la troisième couche) + de l'IPV4 header.

On retroue dans l'IPV4 header :

L'adresse IP source et destinataire, le TTL, la taille des données ou encore le type de protocole (ICPM, TCP, UDP)



Analyse du packet dans wireshark : Adresse IP

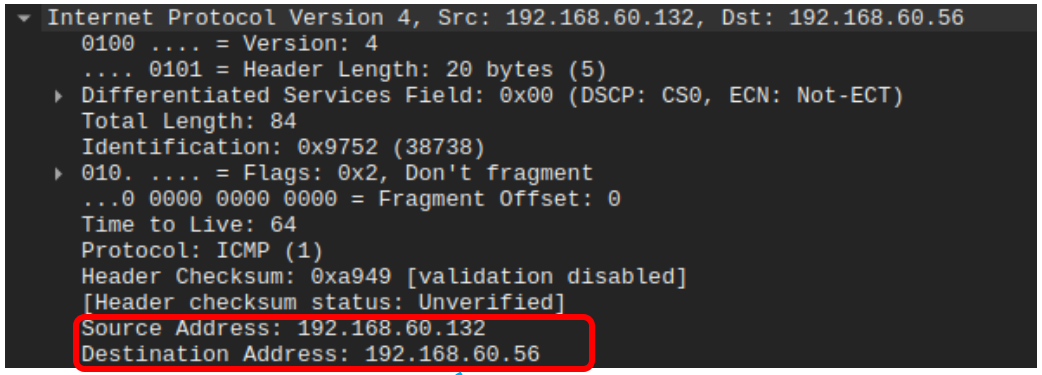
Dans Wireshark, on peut retrouver les éléments de l'IPV4 Header.

Notamment l'adresse IP source et destinataire, le TTL ou la taille des données.

Adresse IP :

- **L'adresse IP est l'identifiant** que prennent les machines en utilisant le **protocole IP**.

- **L'adresse IP source :** IP de la machine qui envoie le PING
- **L'adresse IP destination :** IP de la machine qui reçoit le PING



On retrouve l'adresse IP dans l'IPV4 Header

Analyse du packet dans wireshark : TTL et numéros de frame

Le TTL ou Time To Live et le numéro de frame font tout les deux parties de l'IPV4 header.

Time To Live :

- Le TTL ou Time To Live sert à déterminer la durée de vie d'un paquet sur le réseau.
- Il permet d'éviter que des paquets inutiles occupent la bande passante.

identifiant :

- L'identifiant permet de repérer entre autres les anomalies ou les paquets manquants lors d'une transmission

On peut trouver également le numéro de frame :
18922 frame capturé par Wireshark pendant l'analyse

Analyse du packet dans wireshark : Taille de la frame et des données

Avec wireshark on retrouve également la taille de la frame et la taille des données qui renseignent sur deux éléments différents.

Taille des données :

- La taille des données correspond à la taille de la charge utile ou payload du paquet
- Ce sont les données des couches supérieurs encapsulées
- Si la taille dépasse 1500 octets le paquet peut être fragmenté

Taille de la frame :

- La taille de la trame correspond à la taille total : payload + en têtes.
- Une frame a une taille minimum de 64 octet

Analyse du packet dans wireshark : Le code type ICMP

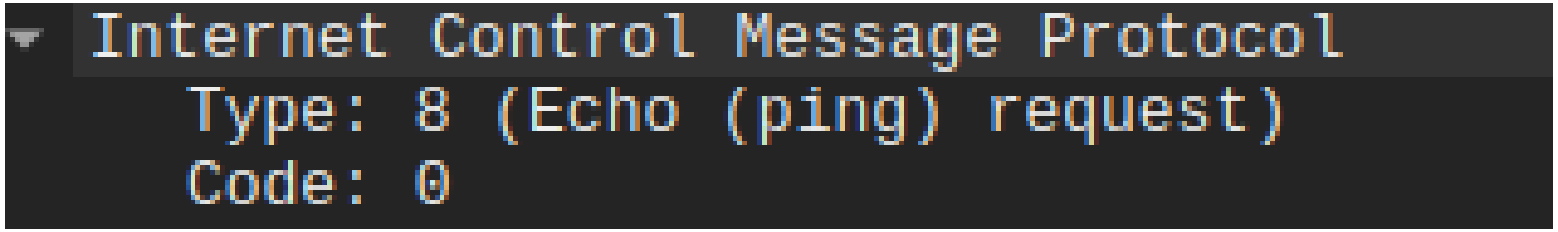
Le code type ICMP permet d'indiquer le type de message utilisé.

Il est souvent utilisé pour indiquer le type d'erreur rencontré lors d'un PING.

Code type ICMP :

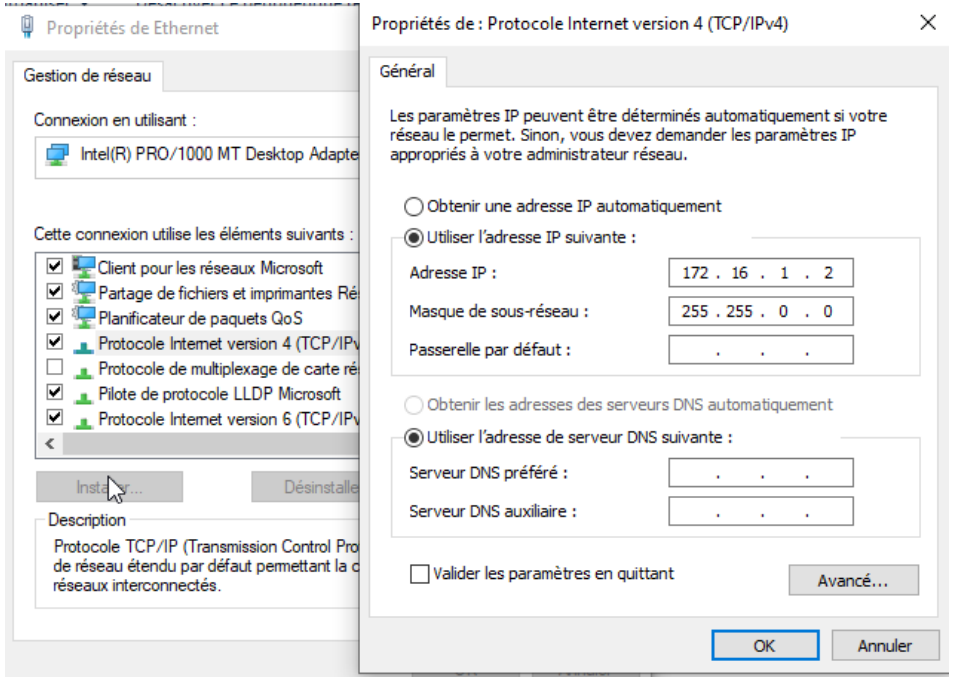
- Le code type o o correspond au code de réponse ping
- Le code type 8 o correspond au code de requête ping

- Pour cette frame, comme il s'agit d'une echo request, le code type est 8 o.



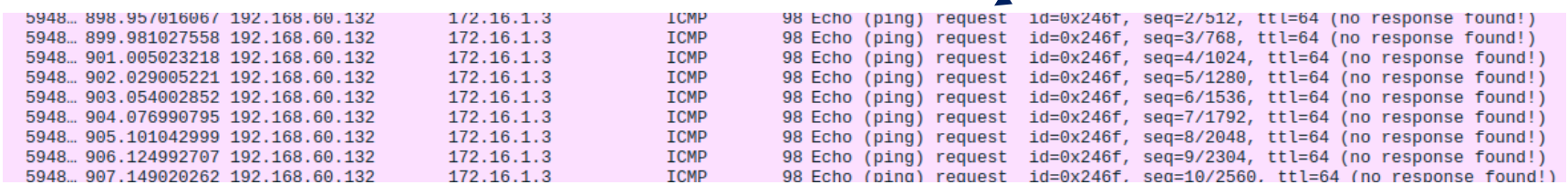
Modification des paramètres IP :

On modifie les paramètres IP pour que l'adresse IP de la VM soit 172



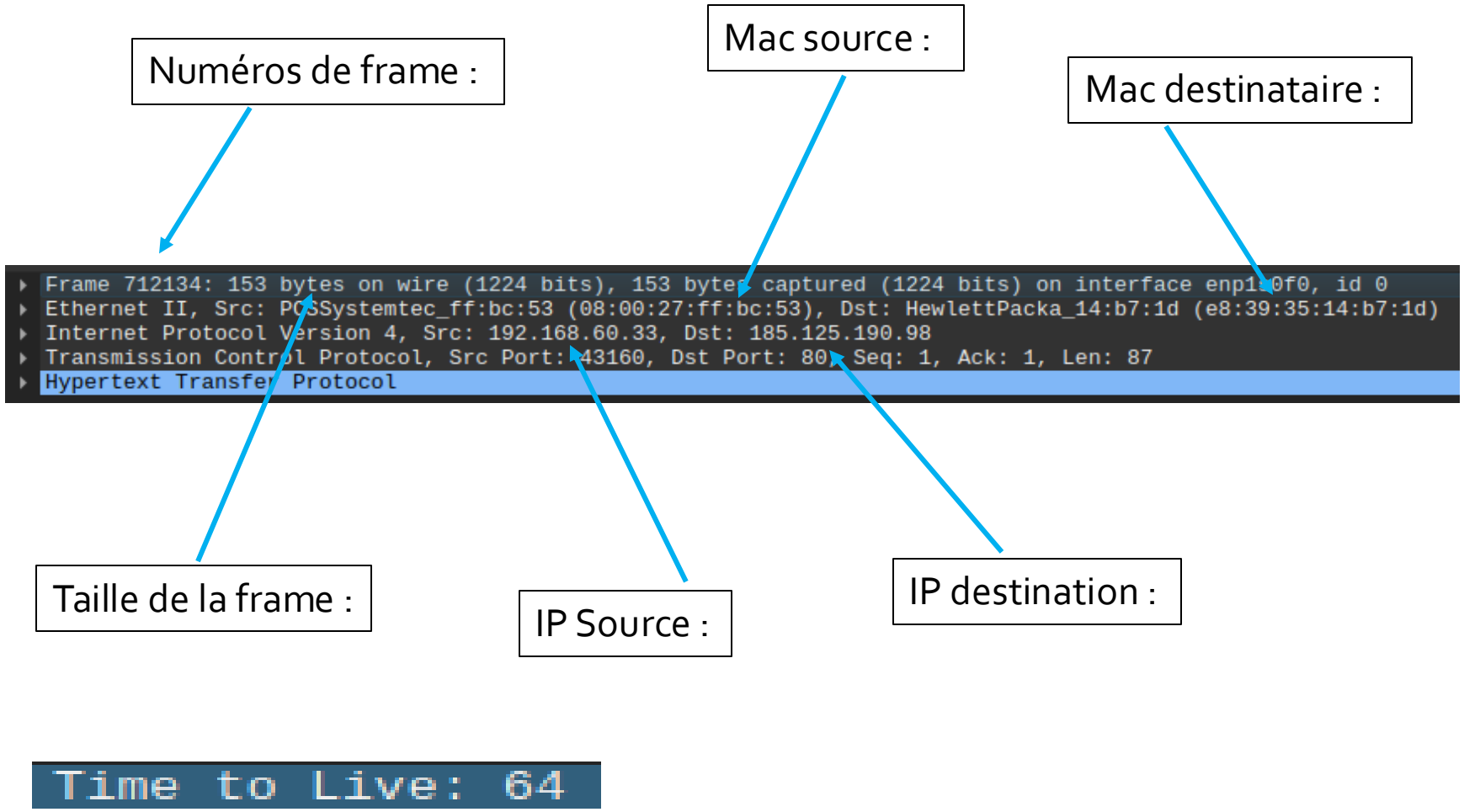
Apres avoir modifier l'IP de la VM on Ping :

Le Ping affiche des erreurs, on voit ces erreurs dans wireshark



Analyse du protocole http et https :

On analyse sur une frame les éléments clé du protocole http et https.



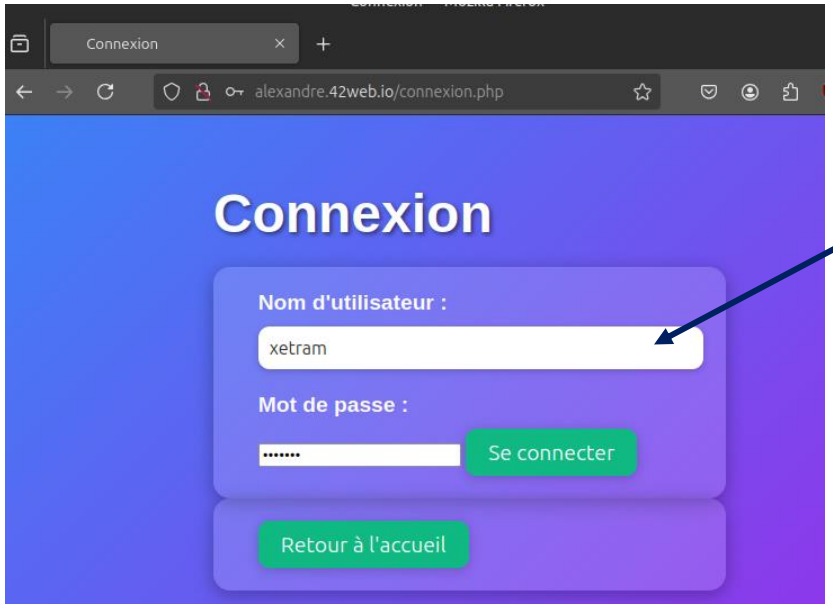
Analyse du protocole http :

On se connecte sur le site d'Alexandre.

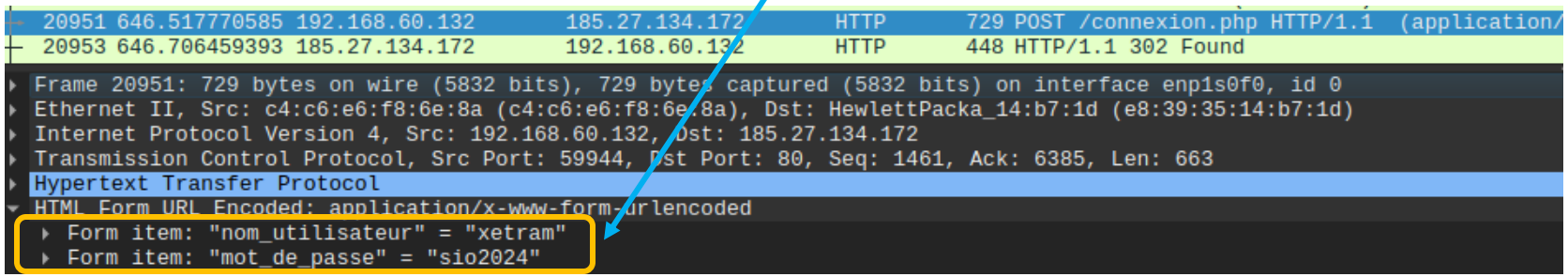
Le site est en http et demande une connexion.

Avec Wireshark on peut retrouver le mot de passe et le login utilisé pour se connecter au site.

Le Protocole HTTP est risqué pour la protection de nos données.



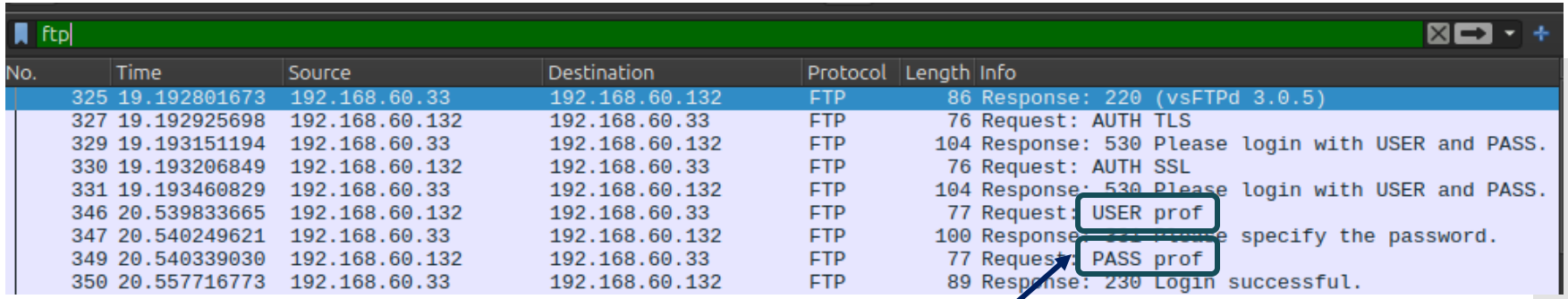
On retrouve le nom d'utilisateur et le mot de passe du site en http :



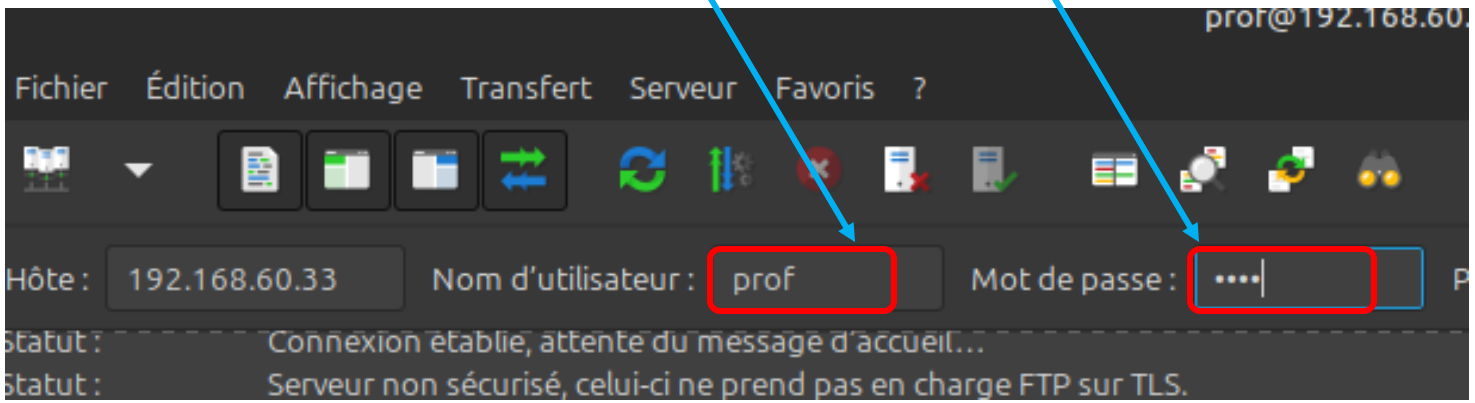
Analyse du protocole FTP :

On capture la trame de connexion d'un client vers le serveur FTP crée lors du TP précédent.

Le FTP ne chiffre pas les données, cela représente un risque pour la sécurité.



On retrouve le nom d'utilisateur et le mot de passe du serveur FTP



Le protocole SFTP :

Afin de protéger les données, on peut utiliser le protocole SFTP.

Voici les étapes pour passer du FTP au SFTP.

Pour plus d'informations, voir TP FTP

```
sio@sio2024:~$ sudo openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout
 /etc/ssl/private/vsftpd.pem -out /etc/ssl/private/vsftpd.pem
[sudo] Mot de passe de sio :
Generating a RSA private key
.....................................................+++++
.....................................................................
.....+++++
writing new private key to '/etc/ssl/private/vsftpd.pem'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:
State or Province Name (full name) [Some-State]:
Locality Name (eg, city) []:
Organization Name (eg, company) [Internet Widgits Pty Ltd]:
Organizational Unit Name (eg, section) []:
Common Name (e.g. server FQDN or YOUR name) []:prof
Email Address []:
```

On génère une clé RSA qui sera utiliser pour le cryptage des données.

Commande : sudo openssl req –x509 –nodes –days 365 –newkey rsa:2048 –keyout /etc/ssl/private/vsftpd.pem -out /etc/ssl/private/vsftd.pem

```
# This option specifies the location of the RSA certificate to use for SSL
# encrypted connections.
rsa_cert_file=/etc/ssl/private/vsftpd.pem
rsa_private_key_file=/etc/ssl/private/vsftpd.pem
ssl_enable=YES
allow_anon_ssl=NO
force_local_data_ssl=YES
force_local_logins_ssl=YES
ssl_tlsv1=YES
ssl_sslv2=NO
ssl_sslv3=NO
require_ssl_reuse=NO
ssl_ciphers=HIGH
```

On modifie le fichier vsftpd.conf