Wireshark

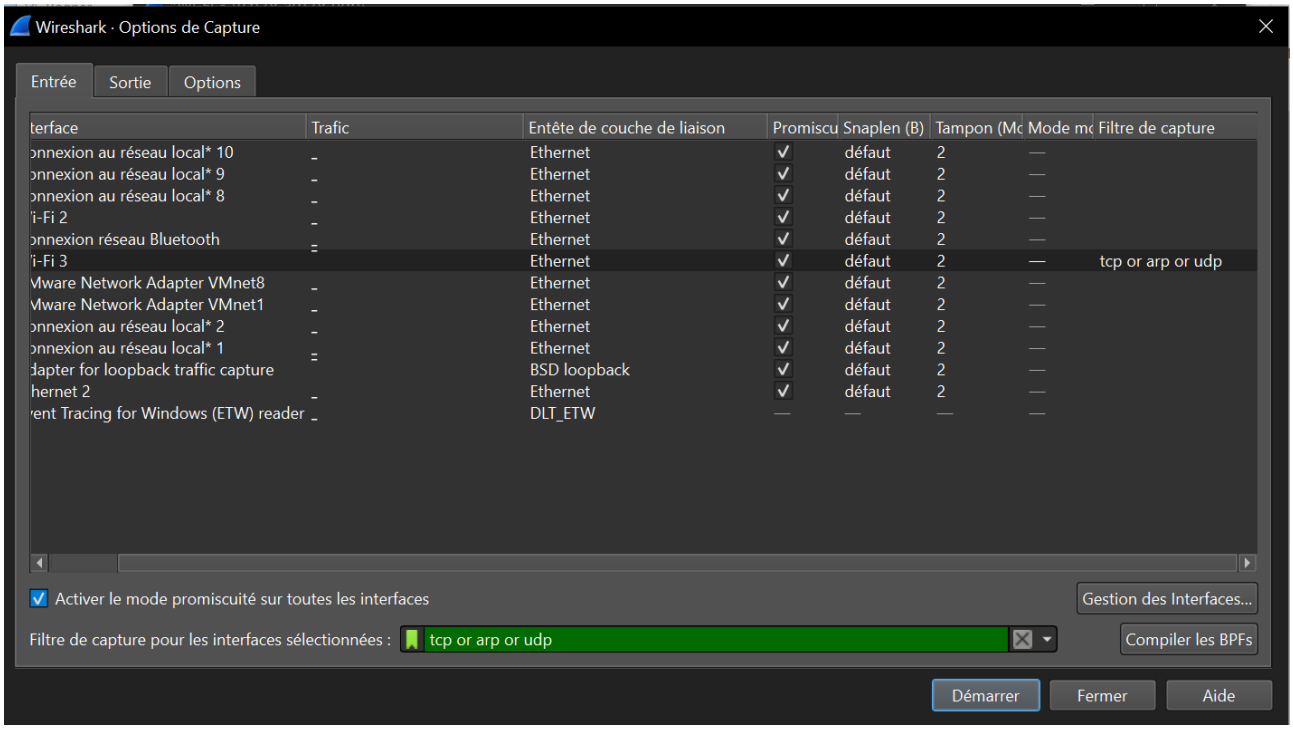
PARTIE 1 :

Quelle est la différence entre une trame et un paquet ? Qu'est-ce que le format pcap/pcapng ?

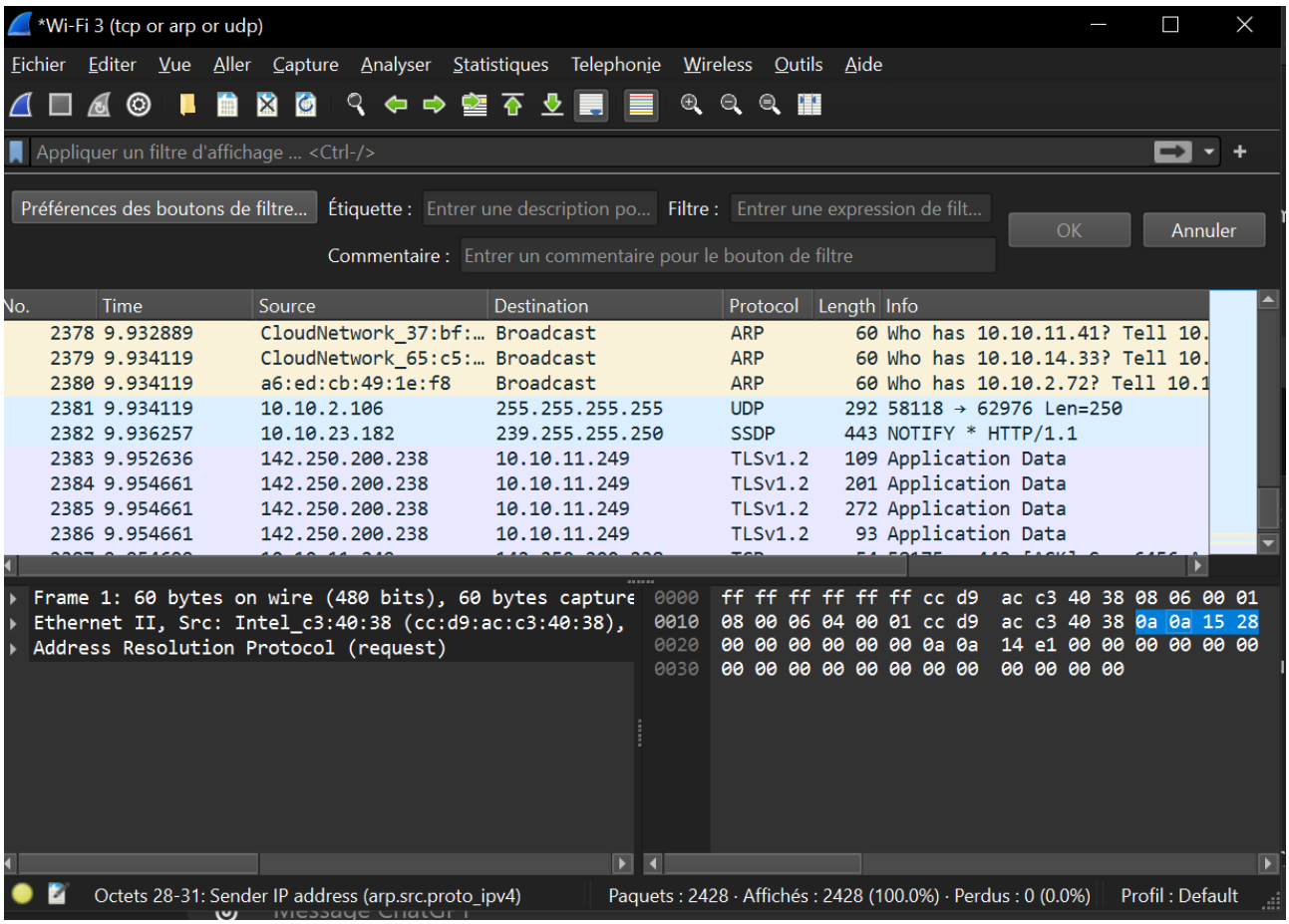
Une trame est utilisée pour envoyer des données entre un seul réseau, tandis qu'un paquet est utilisé pour envoyer des données d'un réseau à un autre, puis vers un périphérique spécifique sur ce réseau

Un fichier PCAP est un fichier issu d'un sniffe de flux réseaux (par exemple avec **Wireshark** ou **TCPDump**), ce sniff réseaux ayant été traité avec la librairie **libpcap** qui produit justement un enregistrement au format **PCAP** (ou **PCAPNG** parfois). Ces fichiers peuvent alors être transportés, stockés et rouverts plus tard, on voit alors tout l'intérêt de savoir les manipuler avec précisions.

Nous allons installer Wireshark sur Windows et nous allons analyser l'interface connecté à Alcasar et nous allons appliquer les filtres pour analyser les paquets ARP, UDP et TCP

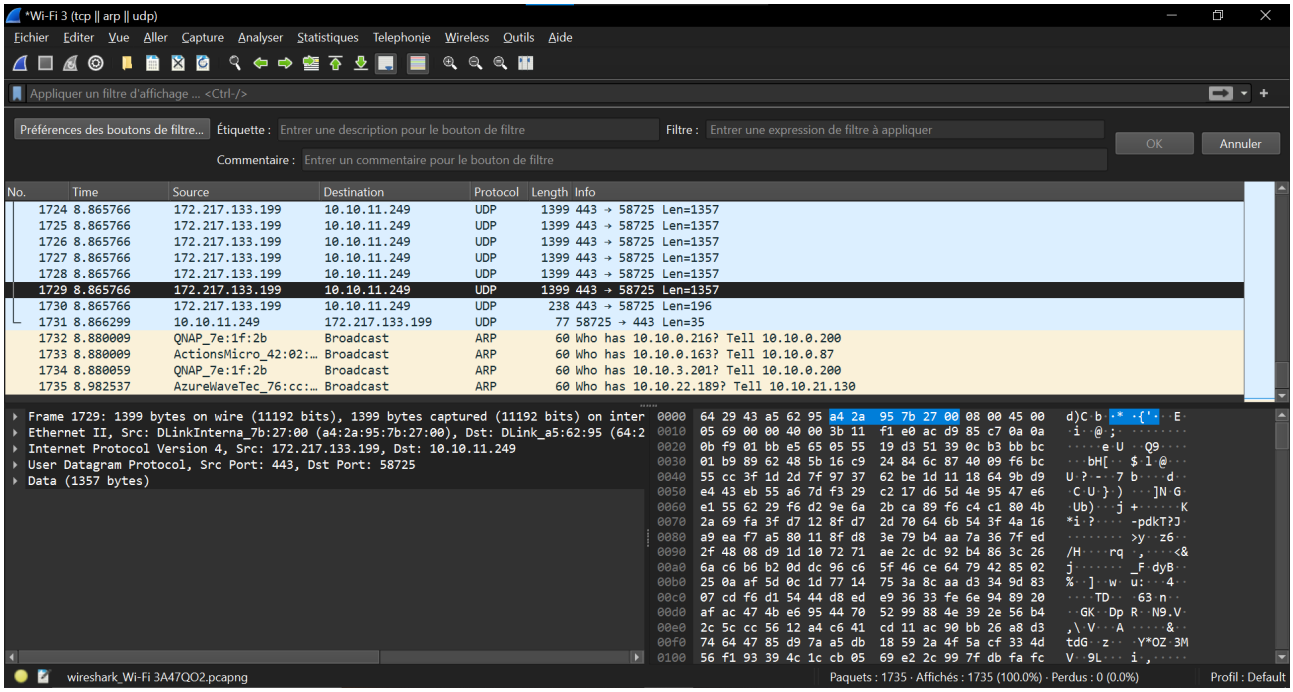


Et voici ce que cela donne

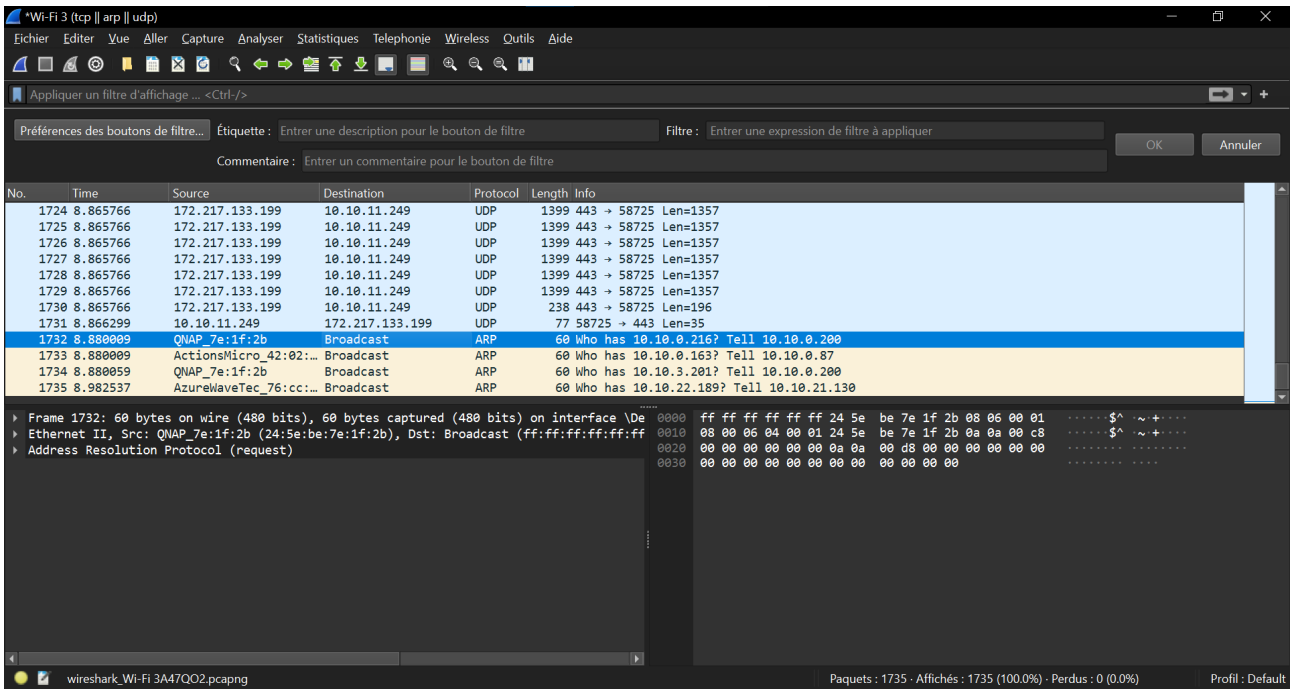


Et nous voyons ici une trame :

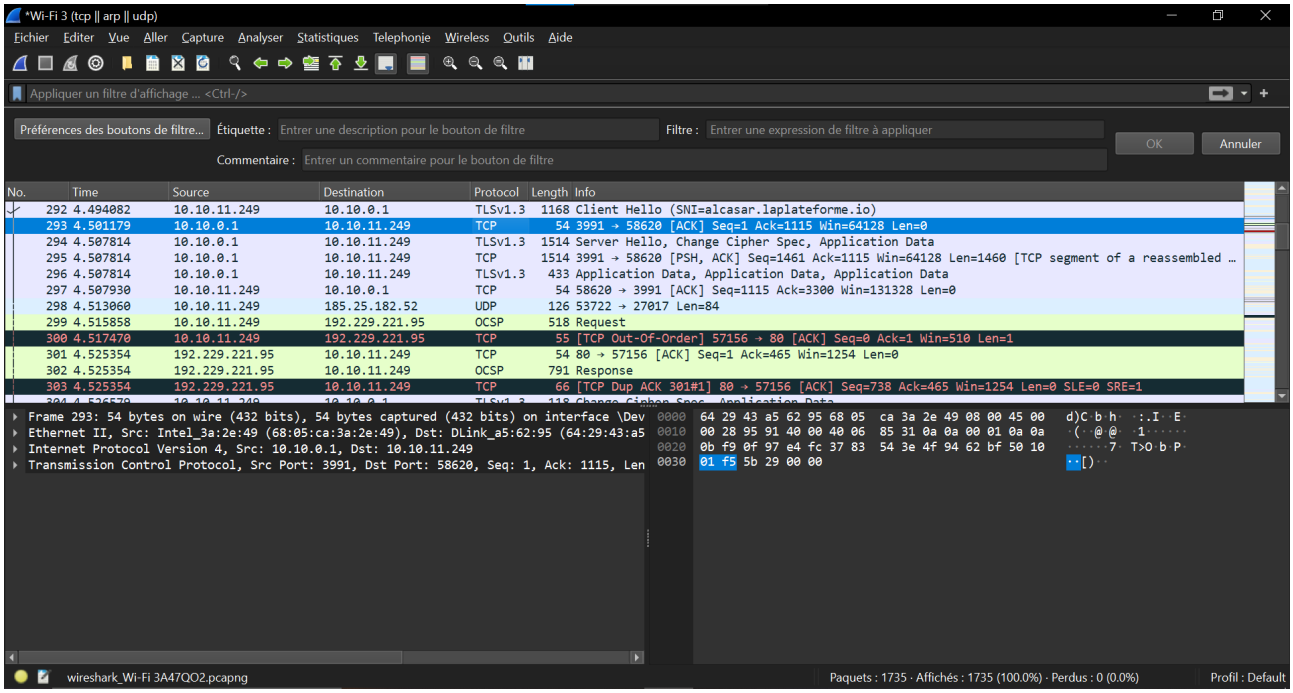
UDP :



ARP :

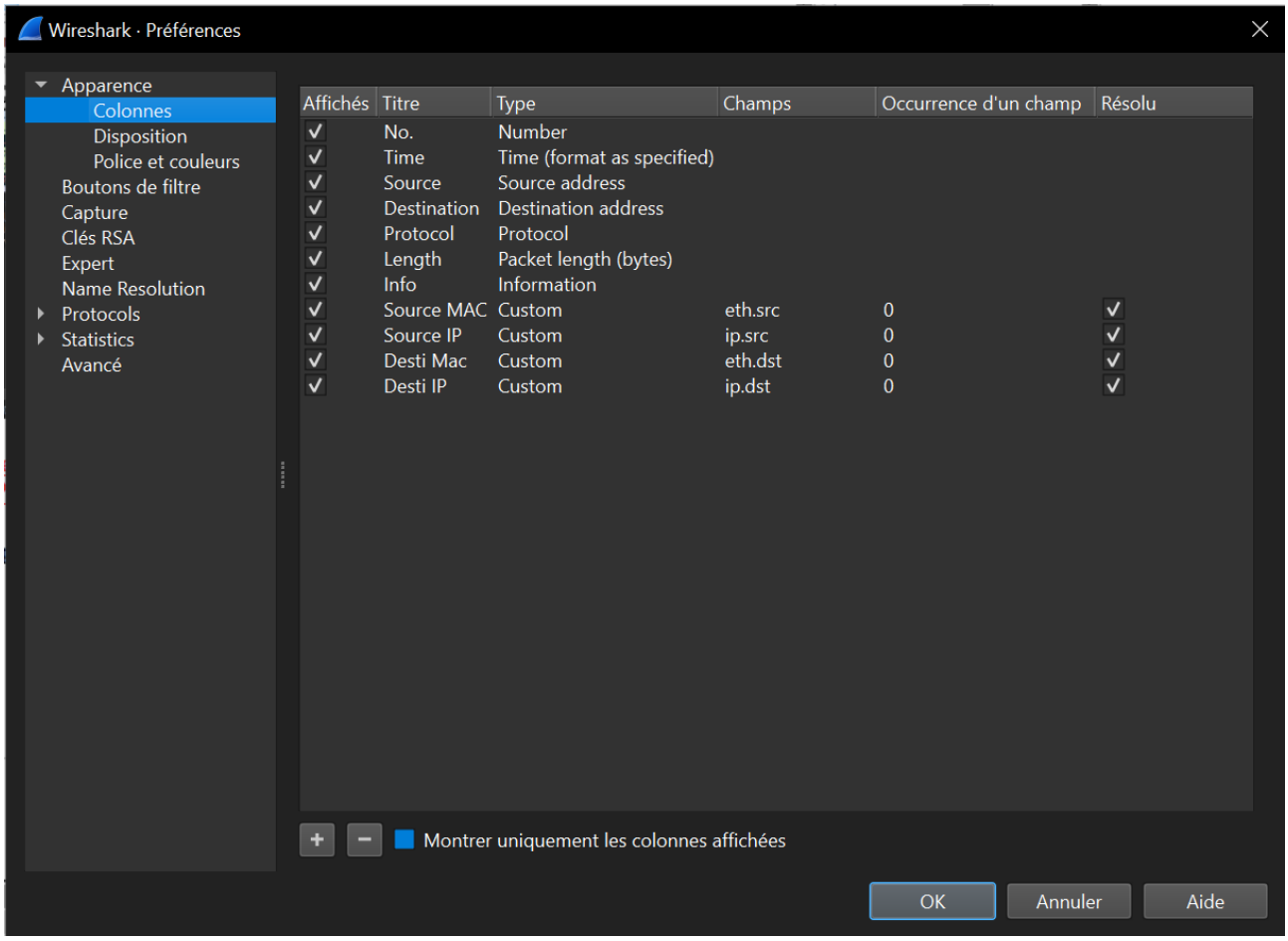


TCP :

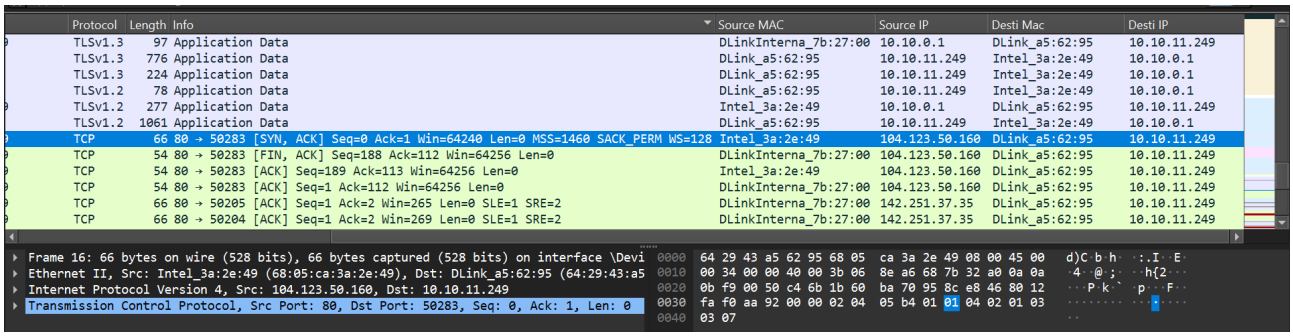


Quelles sont les adresses MAC sources, les IP sources et les adresses MAC sources, les IP destinations des données capturées ?

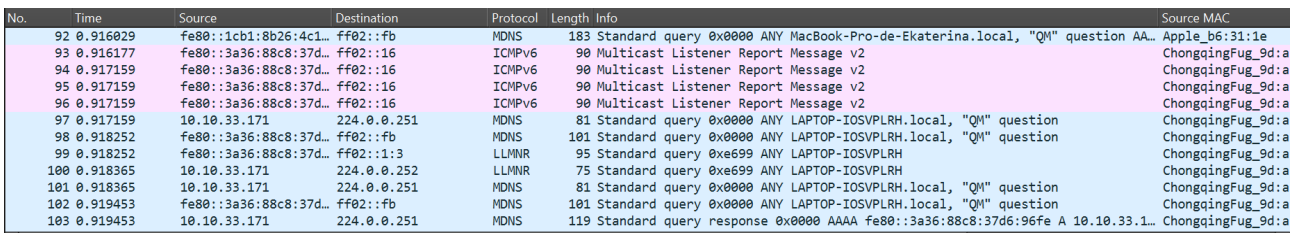
D'abord, pour pouvoir voir toute ces données, il nous faut pouvoir les ajouter sur nos colonnes d'affichage, nous allons aller dans l'onglet éditer et ensuite dans préférences :



Maintenant, on peut voir ces infos là avec les paquets TCP par exemple



Référencez d'autres trames ou paquets circulants sur le réseau. Identifiez leurs protocoles et leur fonction.



Il y a par exemple des trames avec les protocoles MDNS LLMNR et ICPMv6

Spécifications des Formats des Messages ARP, UDP et TCP :

ARP (Address Resolution Protocol)

Le message ARP est utilisé pour mapper une adresse IP à une adresse MAC. Le format d'un message ARP est le suivant :

- **Hardware Type (2 bytes)**: Typiquement 1 pour Ethernet.
- **Protocol Type (2 bytes)**: Typiquement 0x0800 pour IPv4.
- **Hardware Address Length (1 byte)**: Taille de l'adresse MAC (6).
- **Protocol Address Length (1 byte)**: Taille de l'adresse IP (4).
- **Operation (2 bytes)**: 1 pour la requête, 2 pour la réponse.
- **Sender Hardware Address (6 bytes)**: Adresse MAC de l'expéditeur.
- **Sender Protocol Address (4 bytes)**: Adresse IP de l'expéditeur.
- **Target Hardware Address (6 bytes)**: Adresse MAC du destinataire (souvent 0 pour une requête).
- **Target Protocol Address (4 bytes)**: Adresse IP du destinataire.

UDP (User Datagram Protocol)

Le format d'un segment UDP est le suivant :

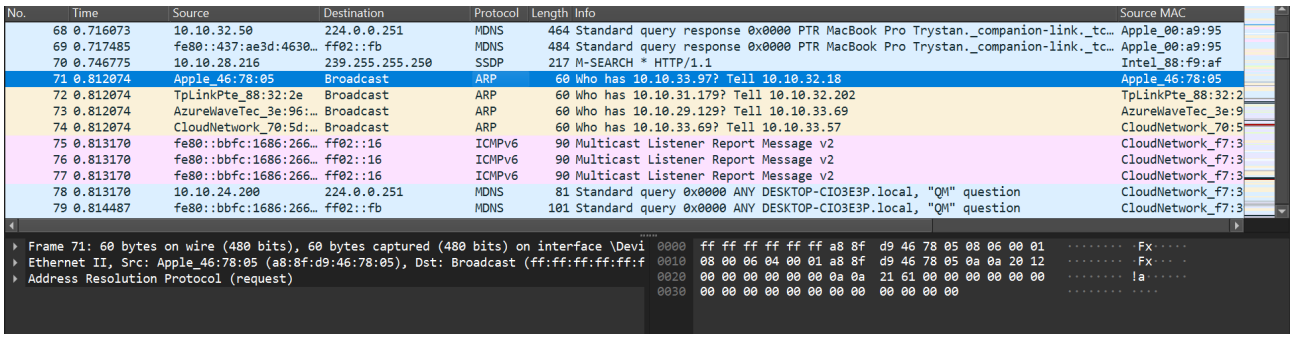
- **Source Port (2 bytes)**: Port source.
- **Destination Port (2 bytes)**: Port destination.
- **Length (2 bytes)**: Longueur totale du segment UDP (en-tête + données).
- **Checksum (2 bytes)**: Vérifie l'intégrité des données.

TCP (Transmission Control Protocol)

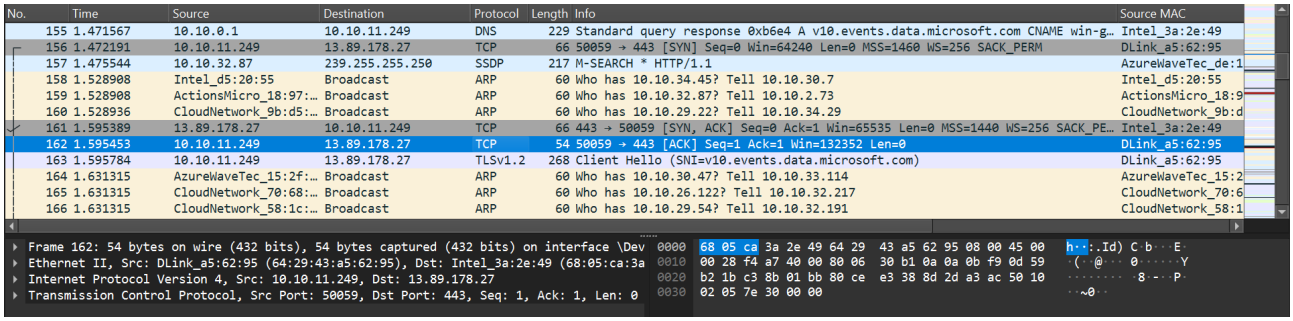
Le format d'un segment TCP est le suivant :

- **Source Port (2 bytes)**: Port source.
- **Destination Port (2 bytes)**: Port destination.
- **Sequence Number (4 bytes)**: Numéro de séquence.
- **Acknowledgment Number (4 bytes)**: Numéro d'accusé de réception (si ACK est défini).
- **Data Offset (4 bits)**: Longueur de l'en-tête TCP.
- **Reserved (3 bits)**: Réservé pour une utilisation future.
- **Flags (9 bits)**: URG, ACK, PSH, RST, SYN, FIN.
- **Window Size (2 bytes)**: Taille de la fenêtre de réception.
- **Checksum (2 bytes)**: Vérifie l'intégrité des données.
- **Urgent Pointer (2 bytes)**: Pointe vers les données urgentes (si URG est défini).
- **Options (variable)**: Options TCP (si présentes).
- **Data (variable)**: Données encapsulées.

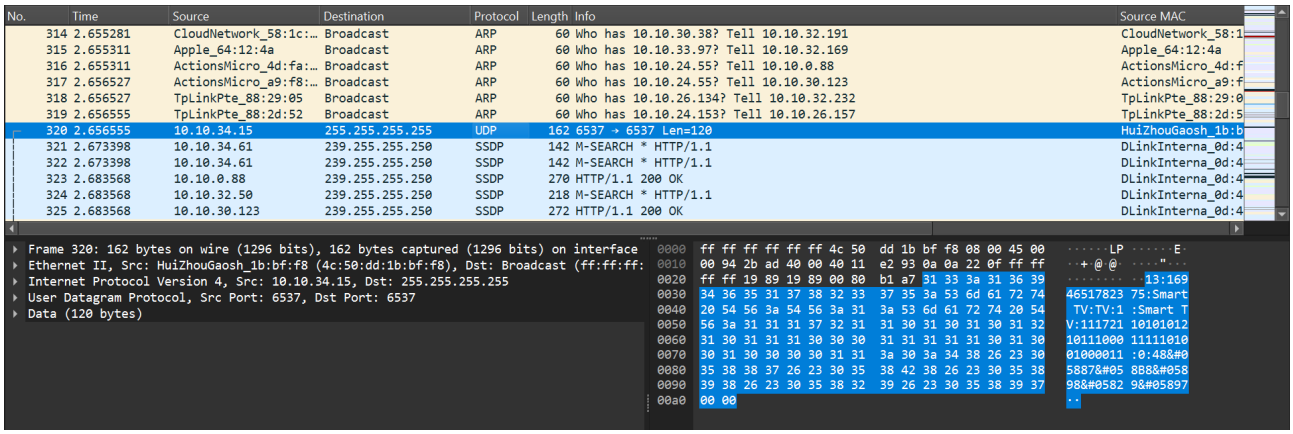
Une capture ARP en hexadécimal (En bas à droite)



Une capture TCP en hexadécimal :

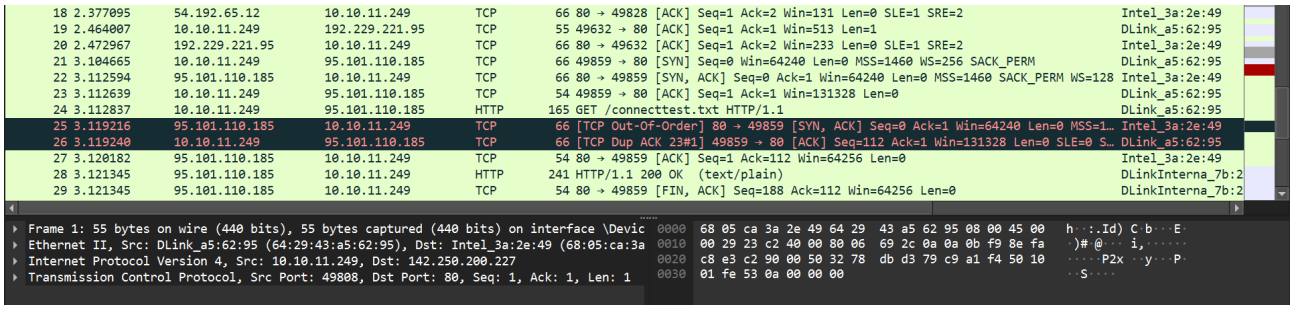


Et une capture UDP en hexadécimal :

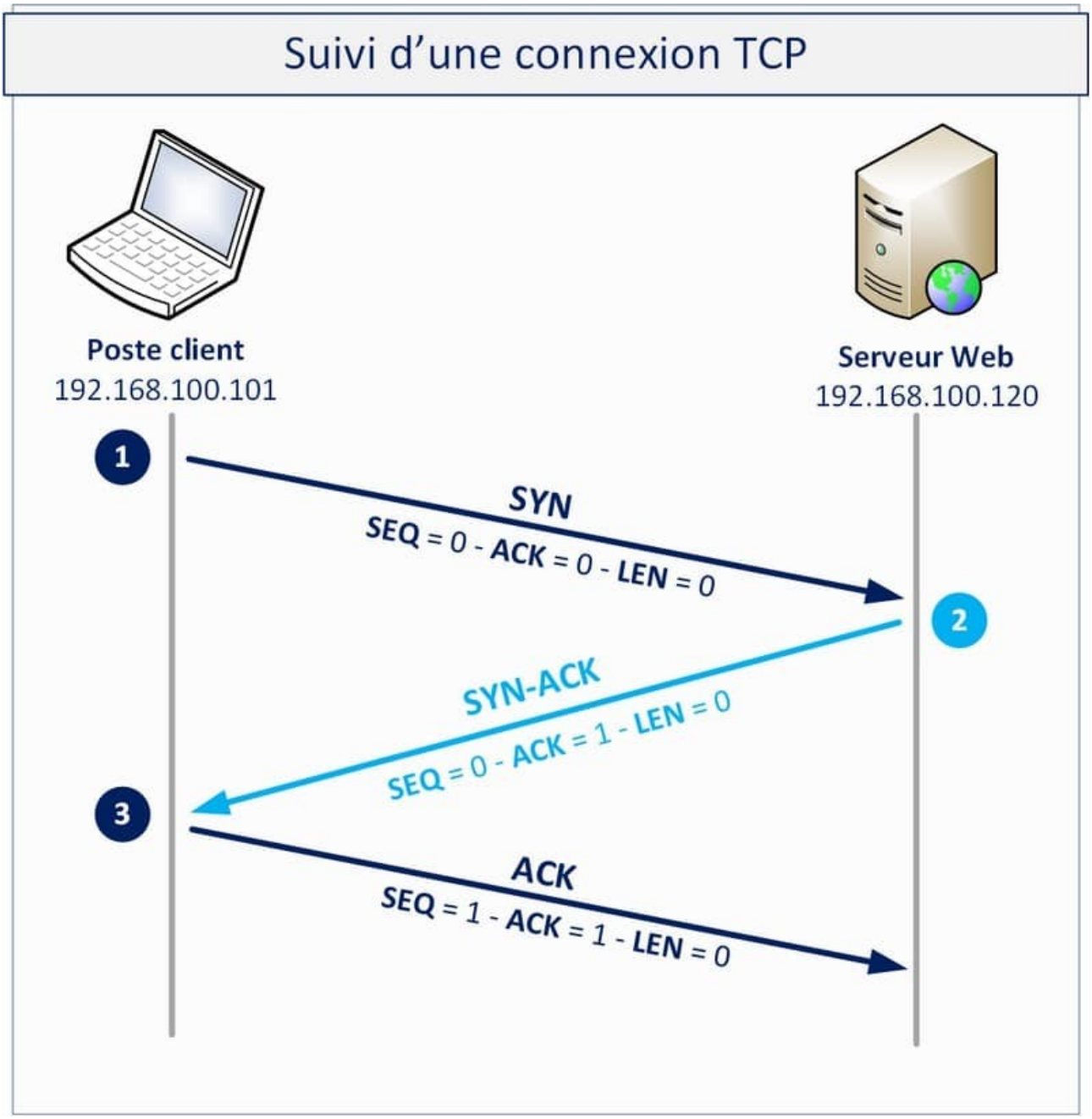


Les paquets surlignés en noir correspondent aux paquets du poste client vers le serveur Web

Les paquets surlignés en vert correspondent aux paquets du serveur Web vers le poste client



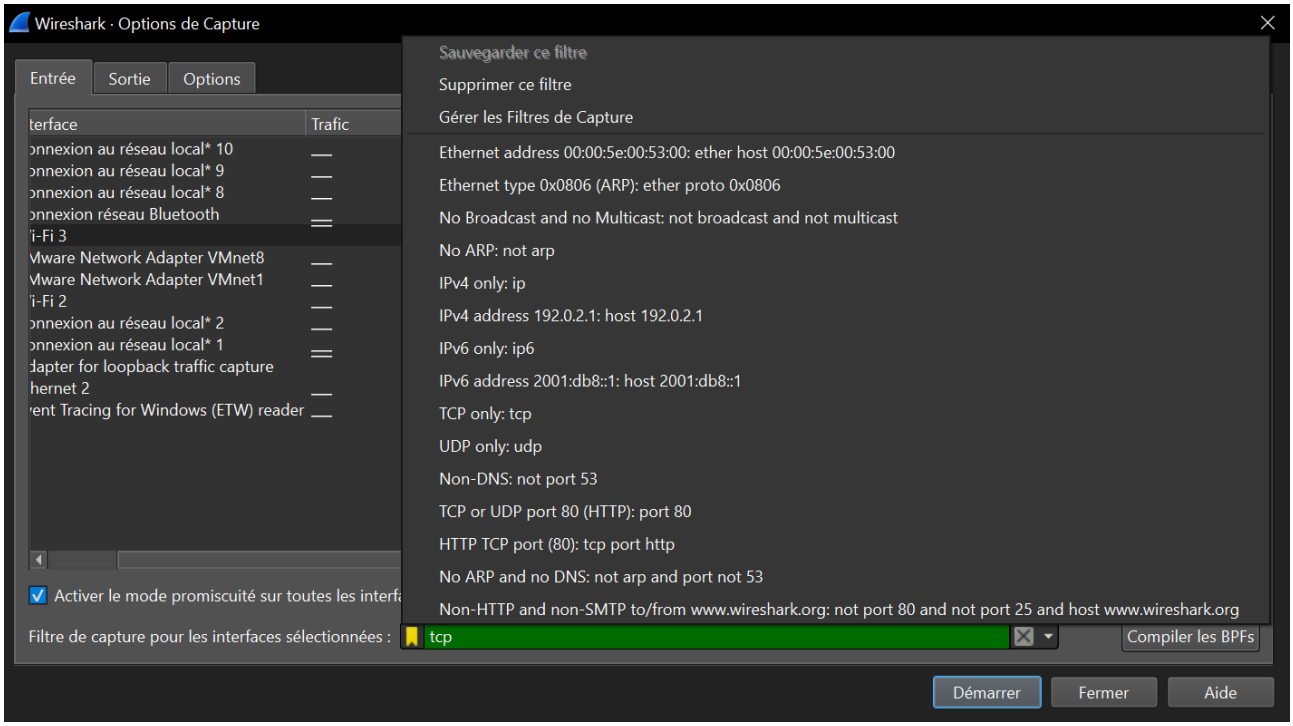
Décrivez le mécanisme de connexion avec un diagramme.



Comme vous pouvez le constater, lorsqu'on écoute un réseau, beaucoup de

messages circulent. Trouver le message qui nous intéresse revient parfois à chercher une aiguille dans une botte de foin !
Il est donc fondamental d'apprendre à utiliser les filtres de Wireshark. Documentez-vous sur le sujet et faites quelques tests pour n'afficher que les trames qui vous intéressent.

Dans l'onglet capture et dans option, on peut sélectionner plusieurs filtres prédéfinis en bas de la fenêtre en cliquant sur le logo à gauche de la barre.



On peut appliquer plusieurs filtres en même temps en séparant chaque élément par "||"