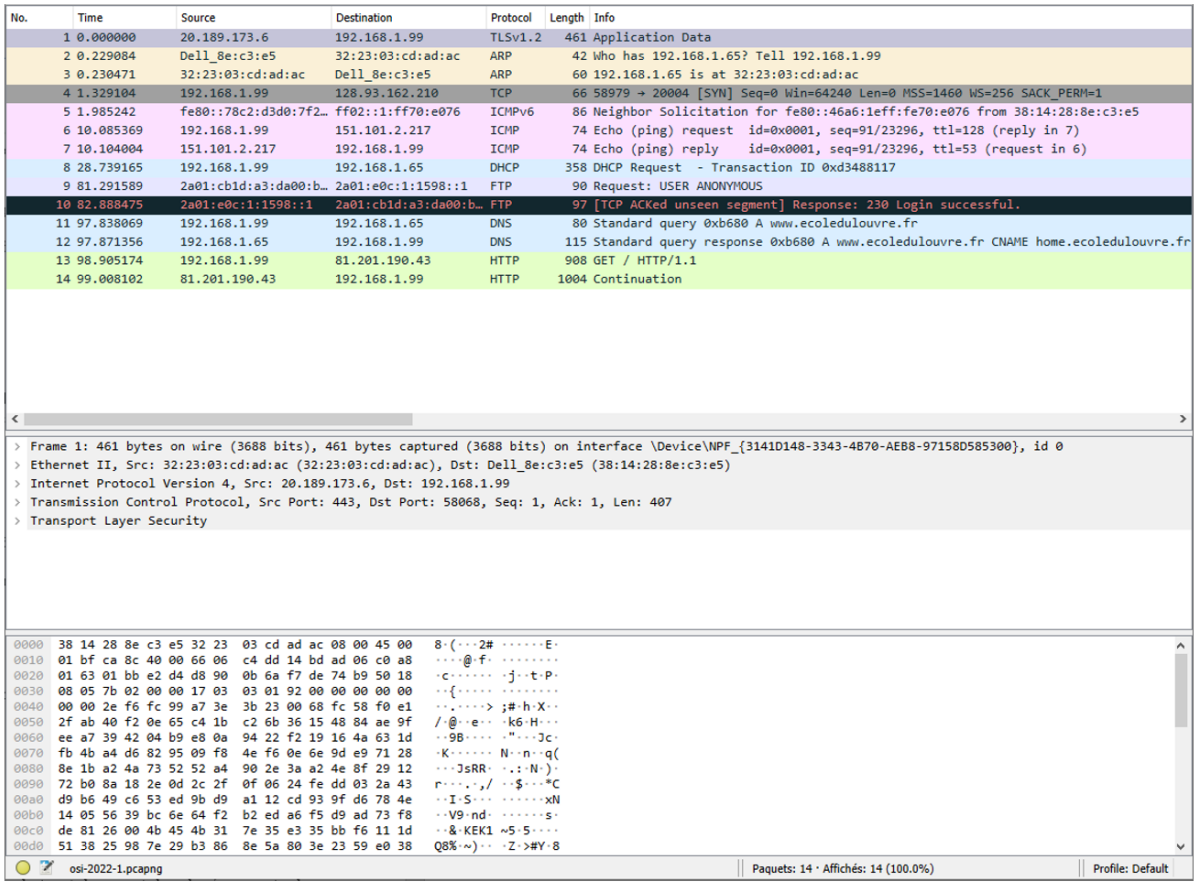
TP n°2 – Le Requin Filaire

1. Wireshark

Wireshark est un logiciel de captures et analyseur de trames réseaux. Pour plus d'informations, voir tout d'abord le tutoriel sur Wireshark disponible dans Moodle.

Ouvrez le fichier "1_simple_capture.pcapng" et répondez aux questions suivantes :

1. Trois fenêtres qui s'affichent dans le logiciel. Définissez la fonction de chacune d'entre elles.



2. Combien de paquets ont été capturés ?

3. Combien de protocoles différents sont présents ? Regardez pour cette réponse la colonne « Protocol » de la première fenêtre. Listez-les et indiquez à quelle couche du modèle OSI ils correspondent.

)

4. L'adresse IP de la machine sur laquelle a été faite la capture est 192.168.1.99, quelle est son adresse mac ? Identifiez pour cela un paquet dont l'IP source est 192.168.1.99, et

relevez l'adresse mac source.

5. Identifiez pour chacun des paquets les adresses mac source et destination présentes dans la couche Ethernet. Quelle est votre conclusion ? Vous devriez trouver constamment l'adresse mac trouvée précédemment (celle de 192.168.1.99). A qui correspond la deuxième adresse mac ? Quelle est son adresse IP ?

   Pour vous aider à répondre à cette question, voici la table ARP (correspondance entre adresses IP et adresses mac) de la machine sur laquelle a été faite la capture Wireshark. Regardez la deuxième colonne pour voir si vous trouvez la deuxième adresse mac trouvée précédemment.

```
Interface : 192.168.1.96 --- 0xb
  Adresse Internet      Adresse physique      Type
  192.168.1.65          32-23-03-cd-ad-ac     dynamique
  192.168.1.66          94-de-80-ac-b6-e6     dynamique
  192.168.1.75          00-04-4b-eb-6e-8e     dynamique
  192.168.1.76          48-b0-2d-2a-f2-70     dynamique
  192.168.1.79          9c-c9-eb-38-6a-9f     dynamique
  192.168.1.80          54-75-d0-d5-89-3a     dynamique
  192.168.1.90          48-51-c5-08-7a-cd     dynamique
  192.168.1.127         ff-ff-ff-ff-ff-ff     statique
```

6. Cette machine a également une adresse IPv6 que vous trouverez dans le paquet n°9 en source. Quelle est cette adresse ? Quelle est sa taille ? comparez-la par rapport à la taille de l'adresse IPv4. Vous trouverez également l'adresse IPv6 de liaison locale de cette machine dans le paquet n°5.

7. Vous remarquerez que l'adresse IPv6 destination dans ce paquet n°9 n'a pas la même taille, mais qu'elle comporte deux fois deux points « :: ». Il faudra compléter ces « :: » par autant de 0 manquants par rapport à l'adresse IP source. Ecrivez cette adresse IPv6 destination.

8. Remplissez le tableau ci-dessous pour les paquets 1, 2, 4, 5, 6, 8, 9, 11 et 13.

N° du paquet	**Taille du paquet en octets**	**Nb de Couches**	**Listes des Protocoles**	**Champ Type dans Entête Ethernet**	**Champ Protocol/ Next Header dans couche réseau**	**Port Source dans couche Transport**	**Port Dest. dans couche Transport**
1							
2							
4							
5							
6							

8							
9							
11							
13							

9. Effectuez une recherche pour indiquer la signification des ports 443, 67 et 68, 21, 53 et 80 que vous avez dû trouver dans le tableau précédent.

10. Le paquet n°9 correspond à une requête DHCP émise par la machine ayant effectuée la capture. Ouvrez le fichier "1_complete_capture.pcapng" et identifiez la réponse à cette requête effectuée par le serveur DHCP.

11. Après avoir répondu à ces questions, vous devriez pouvoir compléter le résultat de la commande ipconfig /all faite sur cette machine :

Nom de l'Hôte. . . . . :
Suffixe DNS propre à la connexion. . . :
Description. . . . . :
Adresse physique . . . . . :
DHCP activé. . . . . : Oui
Configuration automatique activée. . . : Oui
Adresse IPv6. . . . . .:
Adresse IPv6 de liaison locale. . . . .:
Adresse IPv4. . . . . .:
Masque de sous-réseau. . . . . :
Passerelle par défaut. . . . . :
Serveur DHCP . . . . . :
Serveurs DNS. . . . . :

12. Réalisez une capture Wireshark sur votre machine et essayez d'obtenir tous les protocoles présents que vous avez identifiés durant ce TP.

2. Capture de paquets HTTP et DNS.

Ouvrez le fichier "2_capture_navigation_web.pcapng".

1. Une partie de cette capture retrace la navigation d'un utilisateur sur un site web utilisant le protocole HTTP. Retrouvez le site web en question. Sur quelles pages l'utilisateur s'est-il rendu ?
2. Identifiez les paquets correspondant à une requête de la machine vers le serveur web, et les réponses du serveur vers la machine. Que contiennent les réponses du serveur ?

Ouvrez maintenant le fichier "2_capture_adresses.pcapng".

1. Identifiez les 10 adresses IP les plus présentes dans cette capture (Allez dans Satistics>IPv4 Statistics>All adresses). Chacune d'elle est présente dans plus de 5% des packets.
2. Parmi ces 10 adresses IP, cinq correspondent à des machines appartenant au même sous-réseau, et deux correspondent à des adresses IP réservées. Identifiez-les.
3. Parmi les 5 autres adresses, deux correspondent à des adresses réservées. Identifiez-les.
4. Les trois adresses IP restantes ont été récupérées via des requêtes DNS. Identifiez chacun des trois noms de domaine associés.