TP n° 03

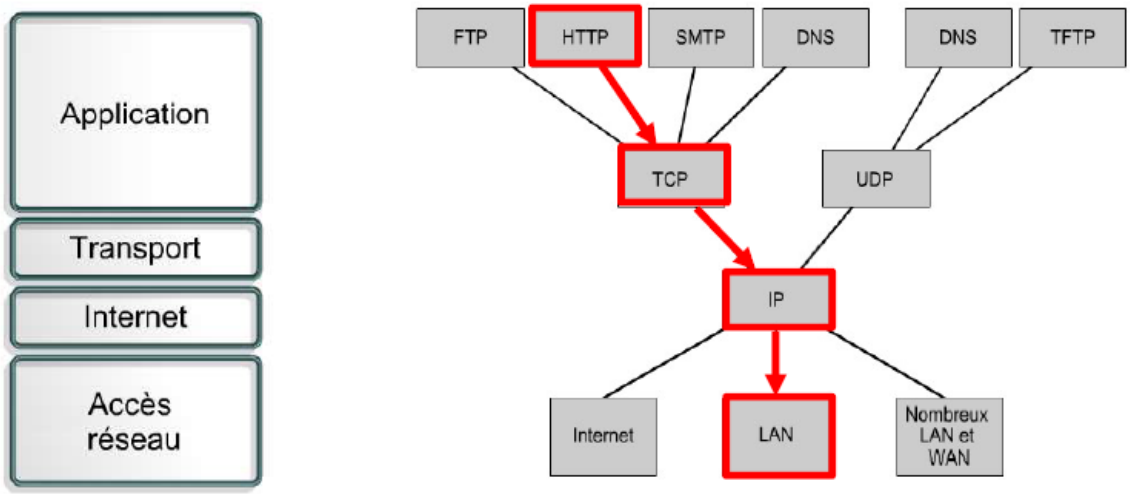
Analyse du protocoleEthernet sousWireshark

1. Objectif

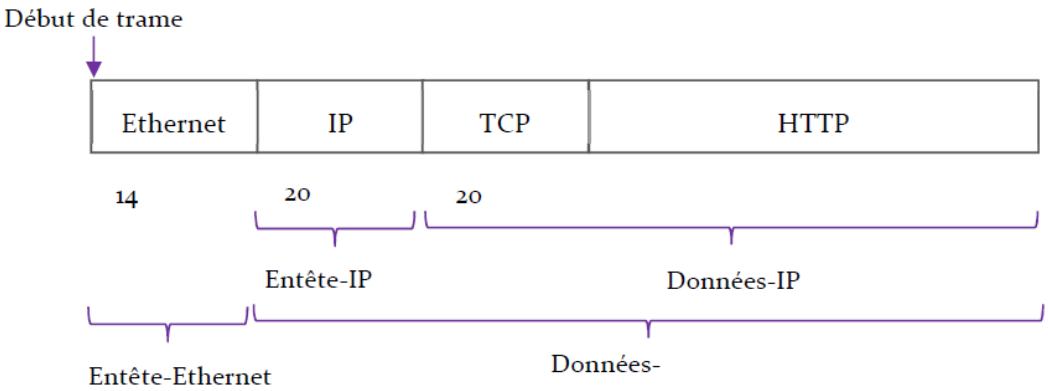
L'objectif de ce TP est l'étude du fonctionnement du protocole Ethernet via l'analyse du trafic en utilisant Wireshark.

2. Encapsulation dans la pile TCP/IP

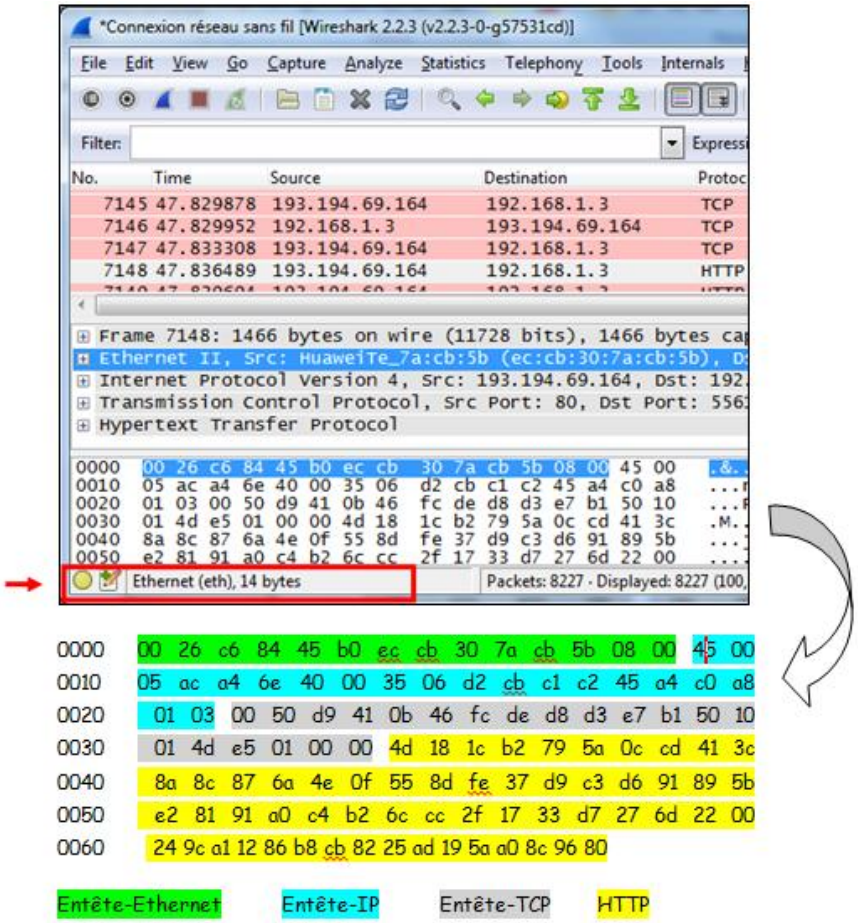
Par exemple pour un message HTTP l'ordre d'encapsulation est « HTTP-TCP-IP-Ethernet ».
Noter que pour Wireshark, il sera affiché inversement « Ethernet-IP-TCP-HTTP ».



La figure suivante illustre la structure d'une trame capturée :



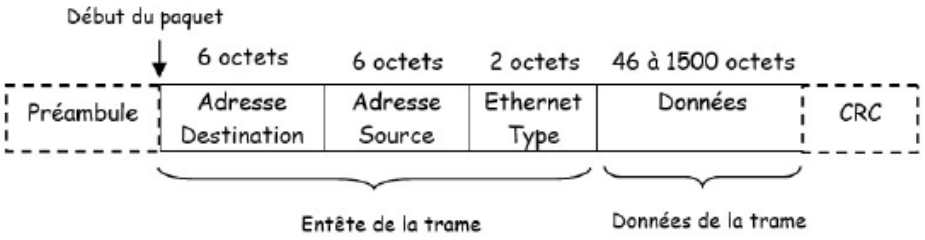
La trame Ethernet contient l' « Entête Ethernet » et le champ « Données Ethernet ». Ce dernier contient le paquet IP dont la structure n'est pas reconnue par la couche Ethernet, et ainsi c'est à la couche supérieure de déterminer son en-tête et ses données. De même pour le champ Données IP qui contient le message TCP, et ainsi de suite. La figure suivante illustre la structure (ainsi que la succession des entêtes des différents protocoles encapsulés) pour un message http capturé.



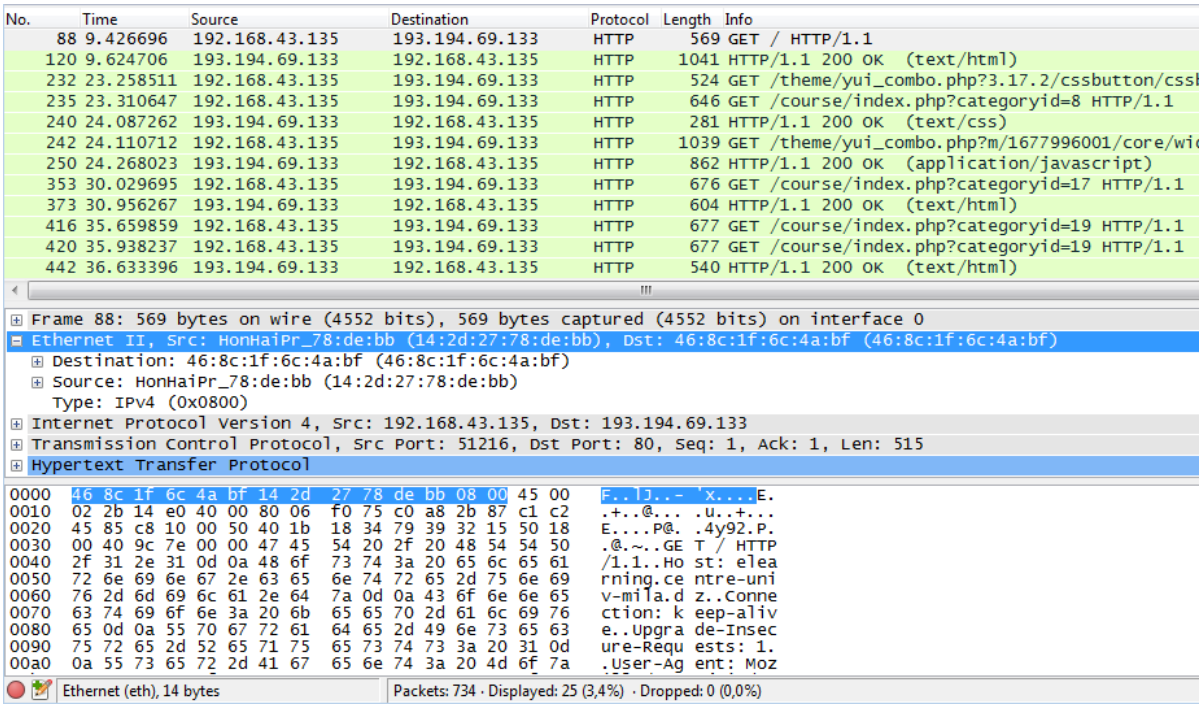
La taille des en-têtes d'un paquet peut être calculée en sachant sa structure (les différents champs qui les constituent). Par exemple, l'entête Ethernet est de 14 octets, l'entête IP et TCP sont de 20 octets chacun. Noter que la taille de l'entête peut être variable, qui est le cas de l'entête HTTP.
Wireshark affiche aussi, tout en bas dans la barre d'état, la taille d'entête du protocole sélectionné dans la zone (2). Dans la figure précédente, la barre d'état indique que la taille de l'entête Ethernet est de 14 octets.

3. Protocole Ethernet

Voici la structure de la trame Ethernet :



Soit un trafic réseau capturé à l'aide de Wireshark. Sélectionner un paquet dans la zone (1), et dans la zone (2) appuyer sur [+] du niveau Ethernet pour voir les différents champs d'en-tête Ethernet.



Noter que :

☐ Le champ « Préambule » ne figure pas dans la trame car il ne contient pas de données utiles, et il est seulement un mécanisme pour aider la carte réseau à identifier le début de la trame.

☐ Il y a une adresse de destination et une adresse source. Wireshark déchiffre les 3 premiers octets de l'adresse et nous indique le fabricant de la carte. Par exemple Huawei.

☐ Les trames Ethernet sont généralement de type "Ethernet II". Ceci est connu grâce au champ « Type ». Noter que dans le cas d'une trame Ethernet I (IEEE 802.3), il y a le champ « Longueur » au lieu de « Type », et qui indique la longueur de la trame Ethernet.

☐ Le champ « Type » contient une valeur hexadécimale qui indique le protocole de la couche supérieure concerné par la trame. Par exemple, si sa valeur est 0x0800 donc la trame est destinée au protocole IP, et ainsi le champ « Données » de la trame Ethernet contient le paquet IP.

☐ Le champ « Données » commence par l'en-tête du protocole de la couche Internet (dans le cas de la figure, c'est l'entête du paquet IP).

☐ Le champ « Données » peut contenir des données de remplissage dans le cas d'une trame de taille inférieure à 64 octets.

☐ Il n'y a pas de champ CRC. Il existe mais il est invisible pour le système ou pour Wireshark, car il est directement utilisé (consommé) par l'équipement (niveau Ethernet) qui envoi et/ou reçoit les trames où il calcule la somme de contrôle et vérifie la présence d'erreurs.

4. Le protocole ARP

ARP est utilisé pour trouver l'adresse Ethernet (l'@ MAC) correspondante à une adresse IP locale. Les combinaisons [@IP - @MAC] sont sauvegardées dans une mémoire cache qui peut être manipulée en utilisant des commandes comme suit :

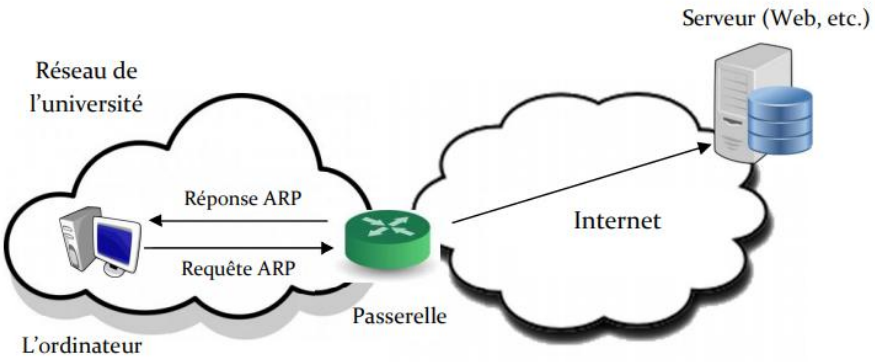
1. Consulter le cache ARP : Taper la commande « arp –a » dans l'invite de commande.

```
C:\Windows\system32\cmd.exe
Microsoft Windows [version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. Tous droits réservés.

C:\Users\Meriem.MERIEM-PC>arp -a

Interface : 192.168.43.232 --- 0xc
  Adresse Internet      Adresse physique      Type
  192.168.43.1          46-8c-1f-6c-4a-bf     dynamique
  192.168.43.135        14-2d-27-78-de-bb     dynamique
  192.168.43.255        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

Interface : 192.168.56.1 --- 0x12
  Adresse Internet      Adresse physique      Type
  192.168.56.255        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

C:\Users\Meriem.MERIEM-PC>_
```

2. Supprimer une entrée dans le cache ARP : Lancer l'invite de commande cette fois-ci en cliquant avec le bouton droit et en choisissant " exécuter en tant qu'administrateur ". Ensuite, taper la commande : « arp –d @IP »
   Par exemple, pour effacer l'@IP 192.168.1.1 de la cache ARP, on tape : arp –d 192.168.1.1

4.1. Capture d'un trafic ARP

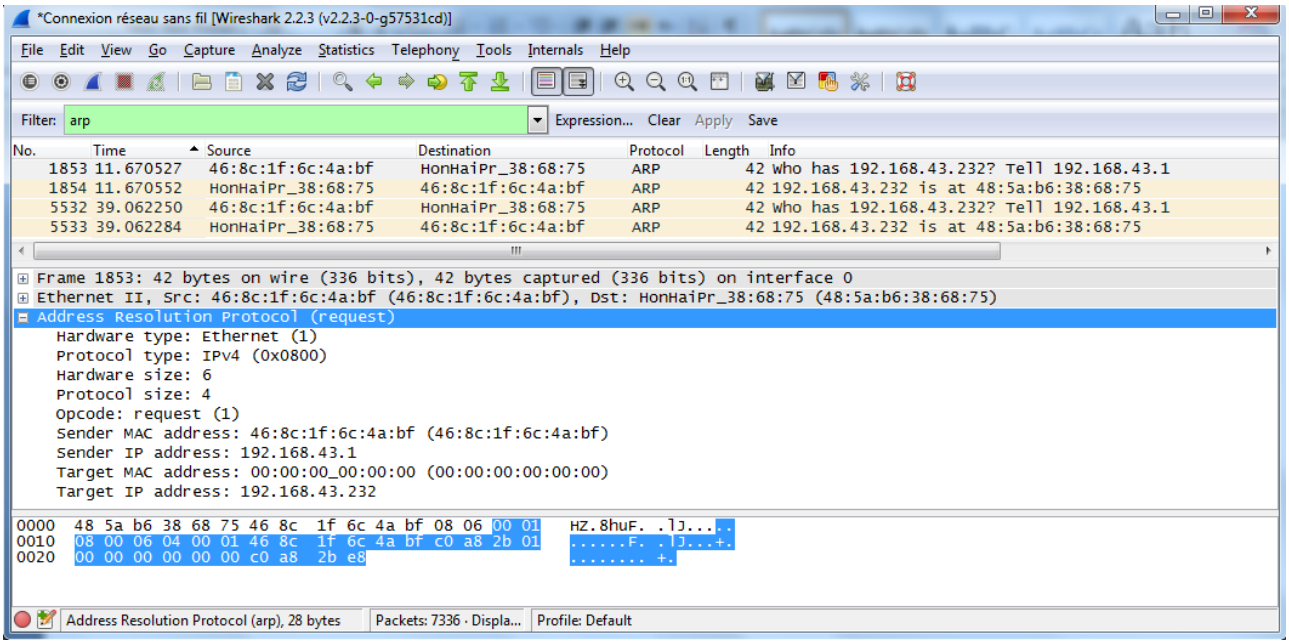
Dans la salle de TP, la connexion d'un ordinateur au réseau internet se fait selon le schéma dans la figure suivante :



Toute requête lancée par l'ordinateur passe par la passerelle. Ceci est aussi le schéma de connexion de l'ordinateur de la maison connecté à Internet à travers un modem. Dans ce cas, ce modem est la passerelle. Rappeler que la passerelle est l'équipement (généralement un routeur) local que la machine utilise pour se connecter au réseau internet.

```
C:\Windows\system32\cmd.exe

C:\Users\Meriem.MERIEM-PC>netstat -r
===========================================================================
Liste d 24...00 ff 51 2a 72 8c ......Kaspersky Security Data Escort Adapter
 14...48 5a b6 38 68 75 ......Microsoft Virtual WiFi Miniport Adapter
 12...48 5a b6 38 68 75 ......Realtek RTL8188EE 802.11bgn Wi-Fi Adapter
 11...a0 1d 48 d1 37 a7 ......Realtek PCIe FE Family Controller
 18...08 00 27 00 84 8c ......VirtualBox Host-Only Ethernet Adapter
  1...........................Software Loopback Interface 1
 28...00 00 00 00 00 00 00 e0 Carte Microsoft ISATAP
 13...00 00 00 00 00 00 00 e0 Teredo Tunneling Pseudo-Interface
 19...00 00 00 00 00 00 00 e0 Carte Microsoft ISATAP #3
===========================================================================

IPv4 Table de routage
===========================================================================
Destination réseau    Masque réseau  Adr. passerelle   Adr. interface  Métrique
          0.0.0.0          0.0.0.0     192.168.43.1   192.168.43.232     25
        127.0.0.0        255.0.0.0         On-link         127.0.0.1    306
        127.0.0.1  255.255.255.255         On-link         127.0.0.1    306
  127.255.255.255  255.255.255.255         On-link         127.0.0.1    306
    192.168.43.0    255.255.255.0         On-link    192.168.43.232    281
  192.168.43.232  255.255.255.255         On-link    192.168.43.232    281
  192.168.43.255  255.255.255.255         On-link    192.168.43.232    281
```

En utilisant le navigateur web pour charger une page web (ex. la page Google), pour que la requête puisse être envoyée au serveur, l'ordinateur doit connaitre l'@MAC de la passerelle, et ainsi il va utiliser le protocole ARP pour la trouver. L'échange de paquets ARP capturé par Wireshark a donné ceci :

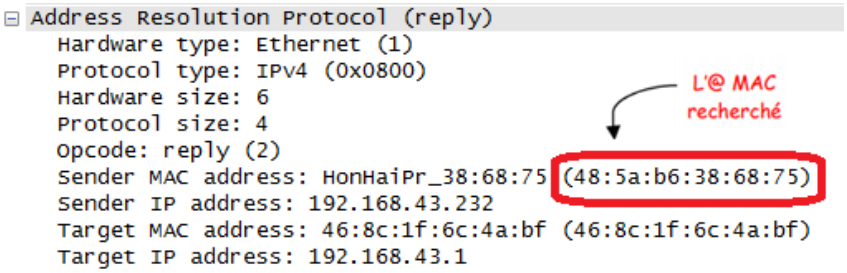


Noter qu'un filtre est appliqué pour n'afficher que les paquets ARP.
Il existe deux types de paquets ARP (distingués par la colonne Info de la zone 1) :
1. Paquet Demande : La ligne Info de ce paquet contient « Who has 192.168.43.232? … » (Voir la trame n° 1853).
2. Paquet Réponse : La ligne Info de ce paquet contient « @IP is at @MAC », voir la trame n° 1854.
En sélectionnant la trame n°1853 et cliquant sur [+] de « Adresse Resolution Protocol » dans la zone (2). Les champs suivants s'affichent :

- « Hardware Type » et « Protocol Type » : qui indiquent que la carte réseau dont on cherche son @ physique est une carte Ethernet, et on dispose de son adresse logique qui est une @IP.
- « Hardware size » et « Protocol size » : définissent la taille de l'@ physique (matériel) et celle logique (protocole) sur 6 octets et 4 octets, respectivement.
- « Opcode » : contient la valeur request (1) qui indique qu'il s'agit d'une requête.
- « Sender MAC » « Sender IP » « Target MAC » et « Target IP » : définissent, respectivement, l'@ MAC (Ethernet) et IP de l'émetteur, et l'@ MAC et IP du destinataire.

En sélectionnant la trame n° 1854 et cliquant sur [+] de « Adresse Resolution Protocol », les champs qui changent de valeurs par rapport à la trame précédente sont :

- « Opcode » où il contient la valeur reply (2) qui veut dire que c'est une trame de réponse.
- « Sender MAC » « Sender IP » « Target MAC » et « Target IP » : où leurs valeurs sont inversées (Sender devient Target et Target devient Sender) puisque le destinataire devient lui l'émetteur.



Dans le paquet de requête, l'émetteur connaît ses @ MAC et IP ainsi que l'adresse IP de la cible (c'est l'adresse IP pour laquelle on cherche l'@ MAC), donc il les remplit. L'@ MAC cible n'est pas connue, pour cela il met 00 : 00 : 00 : 00 : 00 :00. Cette adresse sera remplie par l'expéditeur une fois il reçoit la demande ARP.

5. Travail demandé

I. Capturez un trafic réseau comme suit : lancez une capture Wireshark, ensuite chargez une page web (ex. entrez dans le site : elearning.centre-univ-mila.dz et consultez des cours) via votre navigateur. Arrêtez la capture après un moment.

1. Donnez le n° d'un paquet contenant un message GET de HTTP.
2. Quelle est l'adresse MAC de destination dans ce paquet ? Est-ce l'adresse Ethernet de votre ordinateur ? Expliquez.
3. Donnez le n° d'un paquet contenant un message OK de HTTP.
4. Quelle est l'adresse MAC source dans ce paquet ? Est-ce l'adresse Ethernet du serveur web hébergeant la page web demandée ? Expliquez.
5. Quelle est l'adresse de broadcast Ethernet ? Donnez le numéro d'une trame de diffusion Ethernet.
6. Quel champ dans l'en-tête Ethernet permettant de déterminer à quel protocole de la couche supérieure la trame est destinée ?
7. Donnez un exemple (n° du paquet capturé) d'un paquet destiné au protocole IP. Quelle est la valeur du champ précédent dans ce cas ?
8. Pour un paquet HTTP combien d'octets pour chacune des entêtes : Ethernet, IP et TCP ?

II. Dans cette partie, on essaie de faire en sorte que la machine utilise le protocole ARP pour découvrir l'adresse MAC du routeur local (la passerelle). Ensuite on analyse le trafic capturé.

1. Quelle est l'adresse IP de la passerelle ?
2. L'@IP de la passerelle existe-elle dans le cash ARP ?
3. Effacez l'@IP de la passerelle du cache ARP.
4. Lancez une capture en utilisant Wireshark, et utilisez le navigateur web pour charger une page web. Une fois le trafic ARP est capturé, arrêtez la capture.
5. Filtrez les paquets capturés pour n'afficher que les paquets ARP.
6. Donnez le n° d'un paquet ARP demande.
7. Quel est le n° de son paquet ARP réponse ?
8. Quelle est la valeur du champ « Opcode » pour chacun des deux paquets ?
9. Quelle est la taille de l'en-tête ARP pour une demande ? Qu'en est-il d'une réponse ?
10. Quelle est l'adresse MAC cible pour le paquet ARP demande ?
11. Complétez le schéma suivant par les informations des deux paquets ARP :