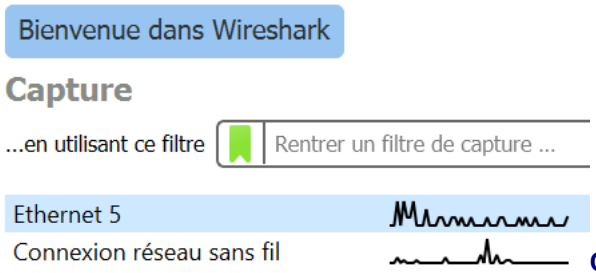
Thème 2 – TP Analyse d'une trame ARP avec Wireshark

Wireshark est un "sniffer" ou un visualiseur/analyseur de trames circulant sur le réseau. Il supporte plusieurs centaines de protocoles et permet de :

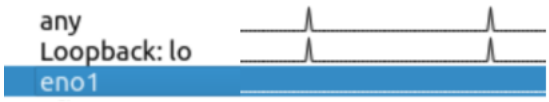
- examiner les données qui transitent sur le réseau ;
- enregistrer les captures dans un fichier sur le disque ;
- créer des filtres et des règles de colorations ;
- décrypter des protocoles.

Un logiciel analyseur de trame (sniffeur) est capable de afficher sous une forme lisible pour un utilisateur.

- **Lancez Wireshark *(en tant qu'administrateur)* et vérifiez que vous avez bien la liste des interfaces réseaux à partir desquelles vous allez pouvoir analyser les trames. Par exemple :**

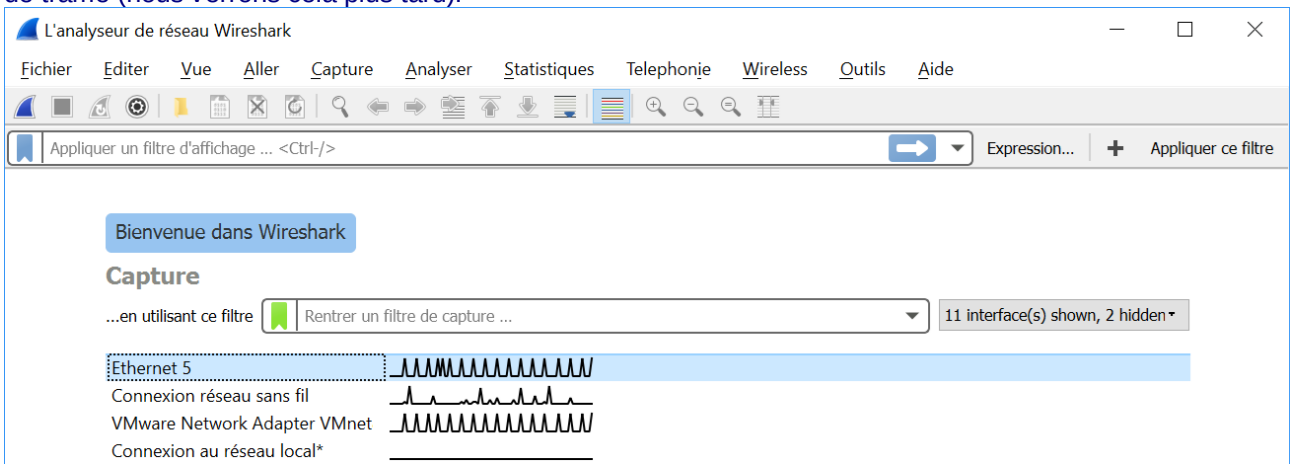


Cap

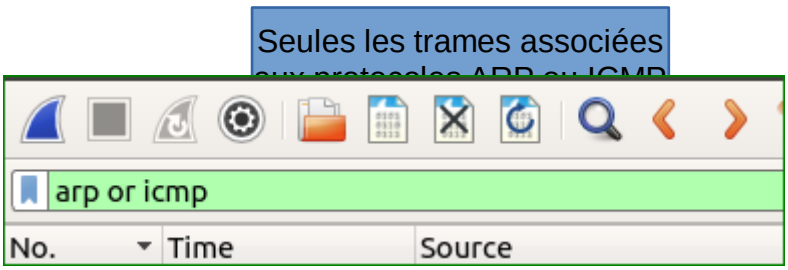


Capture Ubuntu

L'analyseur de trame va récupérer toutes les trames qui vont s'échanger entre les différents postes. Pour limiter le nombre de trames échangées, il vaut mieux ne pas générer d'autre trafic que celui que l'on souhaite analyser, ou alors restreindre les trames que l'on veut récupérer en mettant en place un filtre dans l'analyseur de trame (nous verrons cela plus tard).



Vous avez la possibilité de mettre en place un filtre :

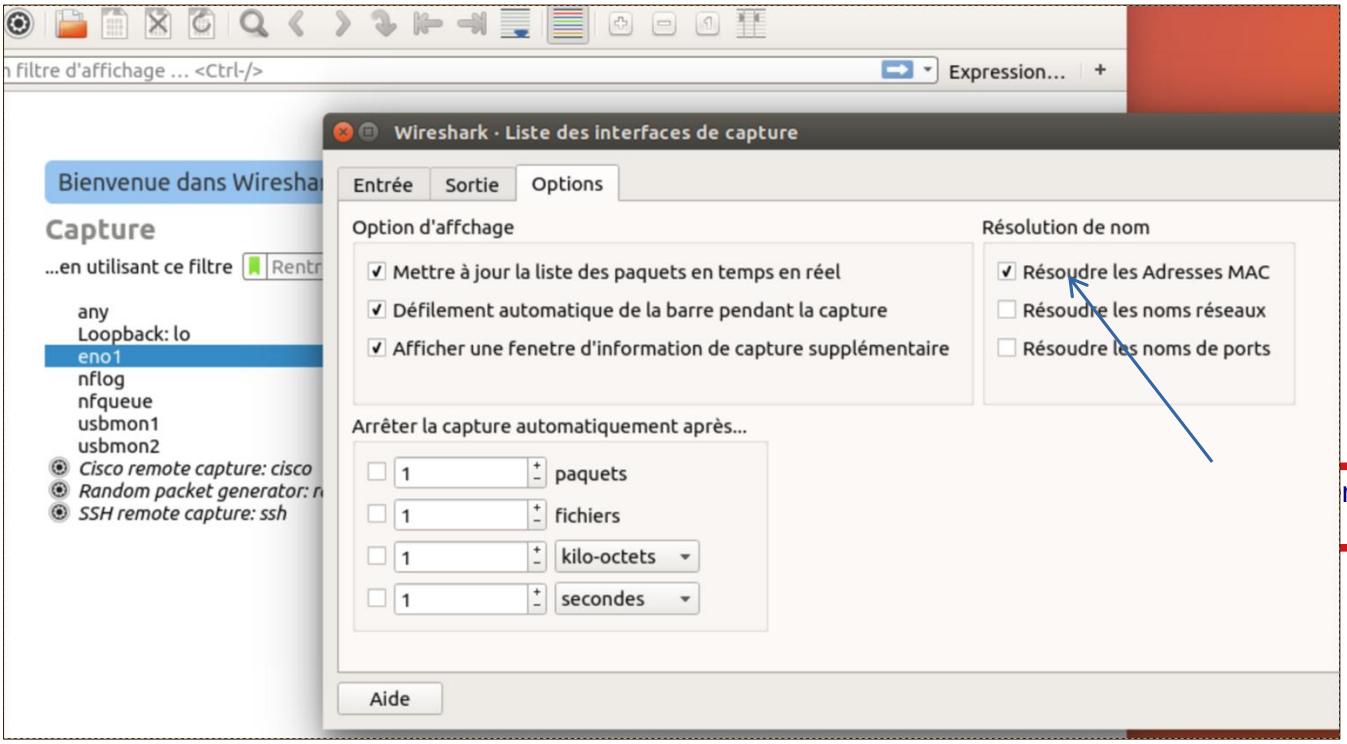


Il est nécessaire ensuite de :

- générer du trafic réseau (un ping par exemple sur l'adresse IP de votre voisin ou de la passerelle) ;
- arrêter la capture des données réseau via l'icône « carré rouge » représentant le « stop » ;
- analyser les données capturées.

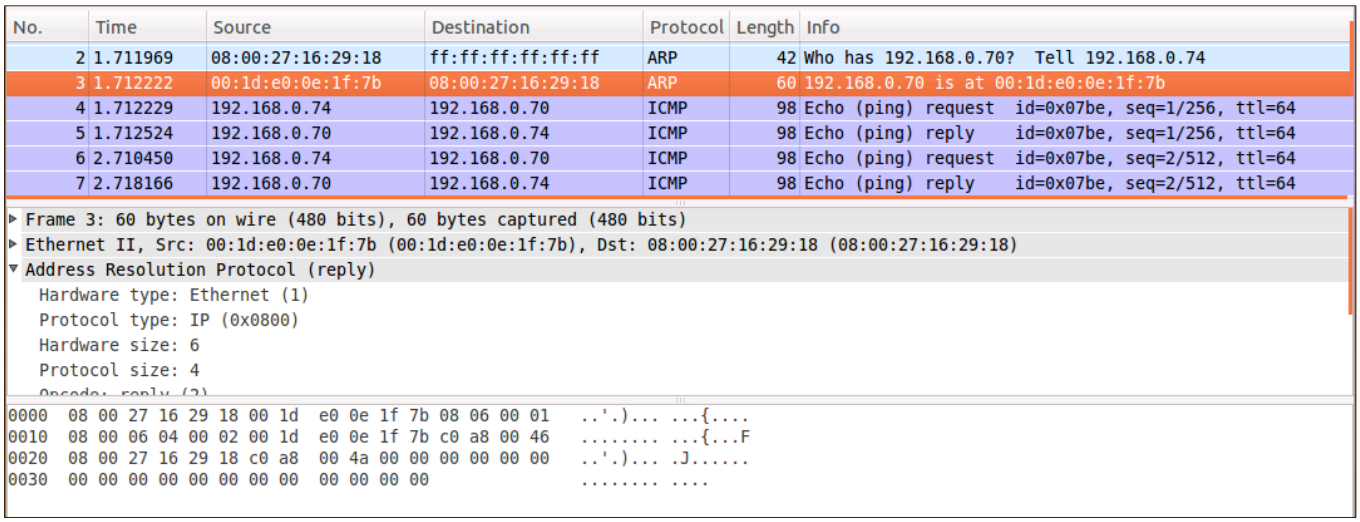
Pour analyser les requêtes ARP, il faut, éventuellement, vider le cache ARP.
Utiliser la commande **arp -d** pour le vider et arp -a pour afficher son contenu

Les options de la capture peuvent être gérées via l'icône « options de capture » puis l'onglet « Options » :



n HEXA.

Le but est ici d'analyser des trames « ARP » .



La partie supérieure (en couleur) affiche le résumé pour chaque trame capturée :

- adresses IP source et destination,
- protocole utilisé et un résumé sur le contenu de la trame.

La partie intermédiaire affiche, par rapport à la trame sélectionnée, les unités de données de protocole (PDU) encapsulées dans la trame que l'on peut développer via les flèches.

La partie Inférieure affiche le contenu de la trame sélectionnée en hexadécimal et en partie droite, une traduction avec les caractères affichables.

Travail à faire 1 Capture de la trame

- Lancez une invite de commandes (cmd) **en mode administrateur** et à l'aide de la commande i**pconfig** récupérez votre adresse IP pour la donner à votre voisin de droite et notez la sienne (10.10.y.x).
- Videz le cache arp de votre poste (arp – d *), puis affichez-le arp -a. (voir arp / ? pour l'aide)
- Lancez wireshark **en mode administrateur**, sélectionnez l'interface Ethernet, mettre en place le filtre **arp or icmp** puis démarrez la capture puis basculez sur votre invite de commandes.
- Lancez un ping vers le poste de votre voisin de droite et attendez qu'au moins une réponse soit affichée avant d'arrêter le ping (CTRL+D).
- Stoppez la capture de trame.

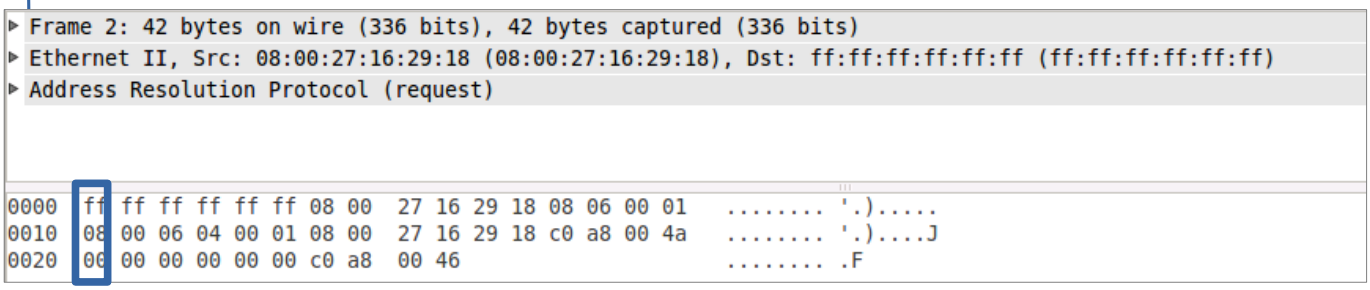
Par rapport à votre ping, vous devriez obtenir une analyse conforme à celle ci-dessous (Rappel : les adresses IP et MAC ne correspondent pas avec ce que vous avez) :

No.	Time	Source	Destination	Protocol	Length	Info
2	1.711969	08:00:27:16:29:18	ff:ff:ff:ff:ff:ff	ARP	42	Who has 192.168.0.70? Tell 192.168.0.74
3	1.712222	00:1d:e0:0e:1f:7b	08:00:27:16:29:18	ARP	60	192.168.0.70 is at 00:1d:e0:0e:1f:7b
4	1.712229	192.168.0.74	192.168.0.70	ICMP	98	Echo (ping) request id=0x07be, seq=1/256, ttl=64
5	1.712524	192.168.0.70	192.168.0.74	ICMP	98	Echo (ping) reply id=0x07be, seq=1/256, ttl=64
6	2.710450	192.168.0.74	192.168.0.70	ICMP	98	Echo (ping) request id=0x07be, seq=2/512, ttl=64
7	2.718166	192.168.0.70	192.168.0.74	ICMP	98	Echo (ping) reply id=0x07be, seq=2/512, ttl=64

On constate que nous avons 6 trames dont 2 trames ARP et 4 trames ICMP (2 « ping request » avec les 2 « ping reply » correspondants aux réponses aux ping).

Travail à faire 2 Analyse de la trame

Q1. En lisant la colonne « Info », expliquez VOS deux trames ARP capturées



Pour observer le détail d'une trame il suffit de la sélectionner.
En cliquant sur la flèche située à gauche on étend les informations relatives à ce niveau :

```
▼ Ethernet II, Src: 08:00:27:16:29:18 (08:00:27:16:29:18), Dst: ff:ff:ff:ff:ff:ff (ff:ff:ff:ff:ff:ff)
  ▶ Destination: ff:ff:ff:ff:ff:ff (ff:ff:ff:ff:ff:ff)
  ▶ Source: 08:00:27:16:29:18 (08:00:27:16:29:18)
    Type: ARP (0x0806)
```

me en hexa

```
▼ Ethernet II, Src: 08:00:27:16:29:18 (08:00:27:16:29:18), Dst: ff:ff:ff:ff:ff:ff
  ▶ Destination: ff:ff:ff:ff:ff:ff (ff:ff:ff:ff:ff:ff)
  ▶ Source: 08:00:27:16:29:18 (08:00:27:16:29:18)
    Type: ARP (0x0806)
▼ Address Resolution Protocol (request)
    Hardware type: Ethernet (1)
    Protocol type: IP (0x0800)
0000  ff ff ff ff ff ff 08 00  27 16 29 18 08 06 00 01   ........ '.).....
0010  08 00 06 04 00 01 08 00  27 16 29 18 c0 a8 00 4a   ........ '.)....J
0020  00 00 00 00 00 00 c0 a8  00 64                     ........ .d
```

Quand on clique sur une ligne, on peut voir le détail en HEXA dans la fenêtre « dessous » :

Analyse de la première trame

- Sélectionnez la première ligne de trame ARP qui doit être une **ARP Request**.
- Cliquez sur la flèche qui précède le mot Frame et lisez les informations inscrites.

Q2. Quelle est la taille de la trame ?

- Réduisez les détails de Frame et développez Ethernet.

Q3. Quelle est l'adresse MAC source ?

Q4. Quelle est l'adresse MAC de destination ? Pourquoi ?

Q5. Combien de symboles en HEXA sont-ils utilisés pour identifier le type de trame ? Dire à combien d'octets cela correspond.

Q6. Repérez les symboles en HEXA pour identifier une trame ethernet ARP.

- Réduisez les détails d'Ethernet et développez Address Resolution Protocol.

Q7. Quelles sont les valeurs des champs suivants :

Sender Mac Address		Adresse physique (MAC) de l'émetteur
Sender IP Address		Adresse IP de l'émetteur

Target MAC Address		Adresse physique (MAC) du destinataire (cible)
Target IP Address		Adresse IP du destinataire (cible)

Q8. Expliquez la valeur de l'adresse physique (MAC) du destinataire dans ce cas bien précis ?

Q9. Quelle est la valeur de « l'Opcode » (toujours dans le détail ARP) ? Sur combien d'octets est codé ce champ ? A quoi correspond-il ?

Analyse de la deuxième trame

- Sélectionnez la seconde ligne de trame ARP qui doit être une **ARP Reply** et développez Ethernet.

Q10. Quelle est l'adresse MAC de destination et à quel poste appartient-elle ?

Q11. Quelle est l'adresse MAC source et à quel poste appartient-elle ?

Q12. Quel est le type de trame Ethernet et sa valeur en hexadécimal ?

- Réduisez les détails d'Ethernet et développez Address Resolution Protocol.

Q13. Quelles sont les valeurs des champs suivants :

Sender Mac Address		Adresse physique (MAC) de l'émetteur
Sender IP Address		Adresse IP de l'émetteur
Target MAC Address		Adresse physique (MAC) du destinataire (cible)
Target IP Address		Adresse IP du destinataire (cible)

Le ping peut maintenant être effectué puisque le système connaît toutes les adresses MAC correspondantes aux adresses IP.

Q14. Quelle est la valeur de « l'Opcode » (toujours dans le détail ARP) ? A quoi correspond-il ?

Travail à faire 3 Tromper ARP avec une adresse inexistante : le principe

- Utilisez la commande manuelle (arp -s) pour modifier l'adresse matérielle de la passerelle par défaut *(donnez-lui par exemple **08:00:02:22:22:20** qui est une fausse adresse)*

- Vérifiez les entrées du cache arp

- Faites un ping sur la passerelle. Notez le résultat et expliquez-le.

- Faites un ping au-delà de la passerelle. Notez le résultat et expliquez-le.

- Supprimez cette entrée incorrecte

- Testez à nouveau

- Supprimez l'entrée permanente.

À noter qu'un « sudo ip n flush dev eno1 » ne supprime pas les entrées permanentes !

Travail à faire 4 Capture d'une trame vers un réseau distant

- Videz le cache arp de votre poste (arp – d *). Que constatez-vous lorsque vous affichez ensuite le cache (arp – a)?
- **Démarrez une nouvelle capture** puis basculez sur votre invite de commandes
- Lancez un ping vers la **passerelle par défaut** (10.40.250.254) et attendez qu'au moins une réponse soit affichée avant d'arrêter le ping (CTRL+D). Stoppez la capture de trame.
- Y-a-t-il une trame ARP dans la capture ? Pourquoi ?
- Analysez les adresses Mac et IP utilisées dans la trame ICMP Reply

@ MAC Source		**hôte source**	
@ IP Source			
@ MAC de destination		**hôte** destination	
@ IP de destination			

- Videz à nouveau le cache arp de votre poste (arp – d).
- **Démarrez une nouvelle capture** puis **l**ancez un ping vers le DNS de google **8.8.8.8** et attendez qu'au moins une réponse soit affichée avant d'arrêter le ping (CTRL+D).Stoppez la capture de trame.
- Y-a-t-il une trame ARP dans la capture ? Pourquoi ?
- Analysez les adresses Mac et IP utilisées dans la trame ICMP Reply

@ MAC Source		**hôte source**	
@ IP Source			
@ MAC de destination		**hôte** destination	
@ IP de destination			

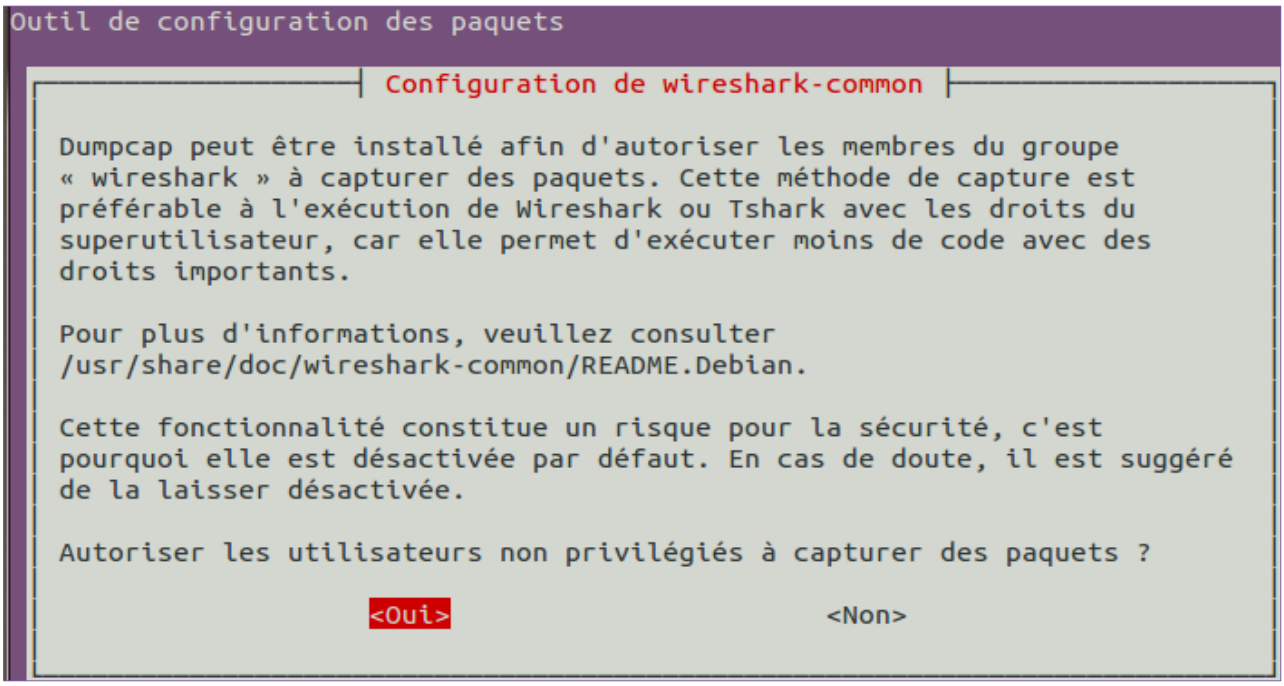
- Quelles conclusions tirez vous de ces deux dernières manipulations (ping vers la passerelle et ping vers le DNS) au sujet d'ARP et d'ICMP.

Annexe - Installez Wireshark sous Ubuntu.

Par défaut, wireshark **doit être utilisé sous l'identité de root :** il faut dans ce cas le lancer en ligne de commande avec la commande : *sudo wireshark* (validez les deux « warning » qui apparaissent).

> Mais il est plus simple d'accorder à un utilisateur non « root » de pouvoir « sniffer ». Pour cela, il doit y avoir un groupe « wireshark » avec l'utilisateur *sio* dedans (si vous vous connectez avec le login « *sio* »).

- Dans un terminal saisissez la commande suivante : *sudo dpkg-reconfigure wireshark-common.*



- ➢ Sélectionnez « Oui » et validez.

Cela ajoute un groupe « wireshark ». Tous les membres du groupe seront capables de « sniffer » sans être « root ».

Il est donc nécessaire d'ajouter l'utilisateur avec lequel votre session est lancé au groupe précédemment créé par la commande suivante :
sudo gpasswd -a nom_user wireshark (nom_user = *sio* si vous vous connectez avec le login « *sio* ») ou ***sudo usermod -a -G nom_user wireshark***

Il est malheureusement nécessaire de redémarrer ubuntu (ce qui est extrêmement rare) pour que cette configuration soit active.

Pour vider le cache arp sous ubuntu :

- soit utiliser la commande (obsolète) « arp » présente dans le paquet « net-tools » (à installer éventuellement « apt install net-tools ») ; **sudo arp -d @IP**
- soit utiliser la commande « ip » : **sudo ip n flush @IP**