

RAPPORT

TP: Architecture des Réseaux Informatiques

réalisé par :

- ◆ IDALIOUALI Imad
- ◆ JAADA Hamza

SOMMAIRE:

I. Introduction :	4
II. Capturer des trames :	5
III. Capturer une requête de ping :	7
IV. Résumé :	16

I. Introduction :

Wireshark est un logiciel de capture et d'analyse de paquets réseau. Il permet aux utilisateurs de visualiser le trafic réseau en temps réel et de capturer les paquets de données qui transitent sur un réseau. Ensuite, il peut analyser ces paquets pour fournir des informations utiles sur les protocoles de communication, les erreurs de transmission, les performances du réseau et les activités malveillantes.

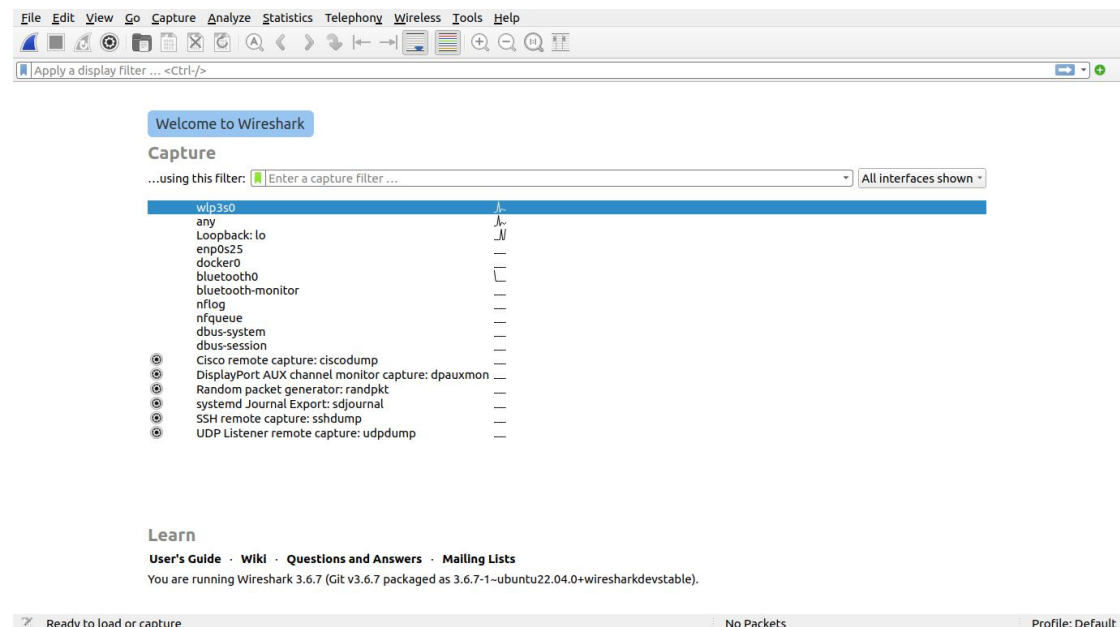
Wireshark prend en charge une grande variété de protocoles de communication réseau, tels que TCP, UDP, HTTP, DNS, DHCP, FTP, SMTP, etc. Il peut être utilisé pour dépanner les problèmes de réseau, résoudre les problèmes de performances, vérifier la conformité aux normes, détecter les attaques de sécurité, et plus encore.

Wireshark est un outil open source gratuit et multiplateforme qui peut être utilisé sur les systèmes d'exploitation Windows, Linux et macOS. Il est souvent utilisé par les professionnels de la sécurité réseau, les administrateurs réseau et les développeurs pour résoudre les problèmes de réseau et améliorer la sécurité.

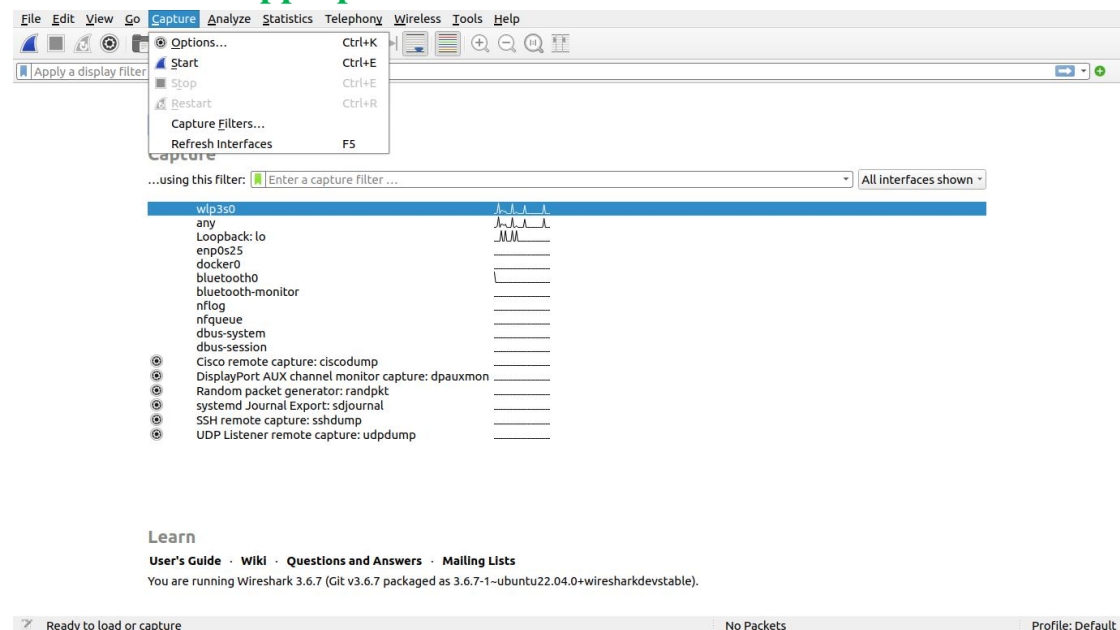
II. Capturer des trames :

Pour capturer des trames dans Wireshark, vous pouvez suivre les étapes suivantes :

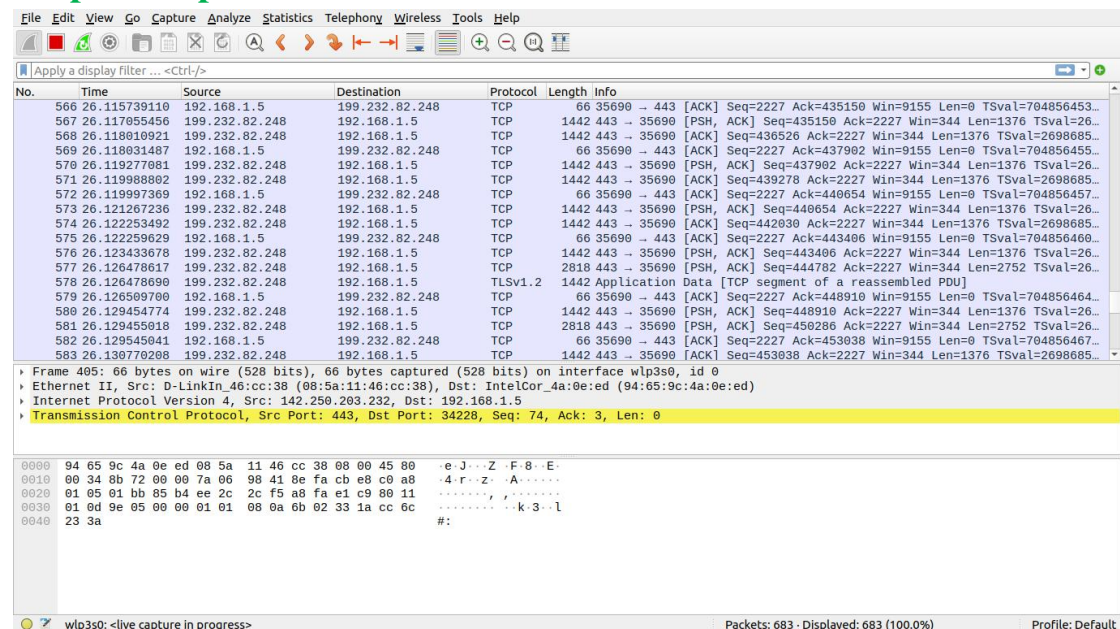
1. Ouvrez Wireshark sur votre ordinateur :



2. Sélectionnez l'interface réseau que vous souhaitez utiliser pour la capture de trames. Vous pouvez le faire en cliquant sur le menu "Capture" en haut de la fenêtre de Wireshark et en sélectionnant l'interface appropriée :



3. Commencez à capturer des trames en cliquant sur le bouton "Démarrer" ou en appuyant sur la touche "Ctrl + E" de votre clavier. Cela commencera à enregistrer toutes les trames qui passent par l'interface réseau sélectionnée :



on Trouve alors trois zones :

a) La zone de liste des paquets :

cette zone occupe la partie supérieure de la fenêtre de Wireshark et affiche la liste des paquets capturés. Chaque ligne de cette zone représente un paquet capturé et affiche des informations sommaires telles que l'heure d'arrivée, la source et la destination, le protocole utilisé, etc. Cette zone permet à l'utilisateur de sélectionner un paquet et de l'analyser en détail dans les deux zones inférieures.

b) La zone de détails du paquet :

cette zone est située dans la moitié inférieure gauche de la fenêtre de Wireshark et affiche les détails du paquet sélectionné dans la zone de liste des paquets. Cette zone affiche toutes les informations décodées du paquet telles que les en-têtes de protocole, les données, etc.

c) La zone d'arbre de paquets :

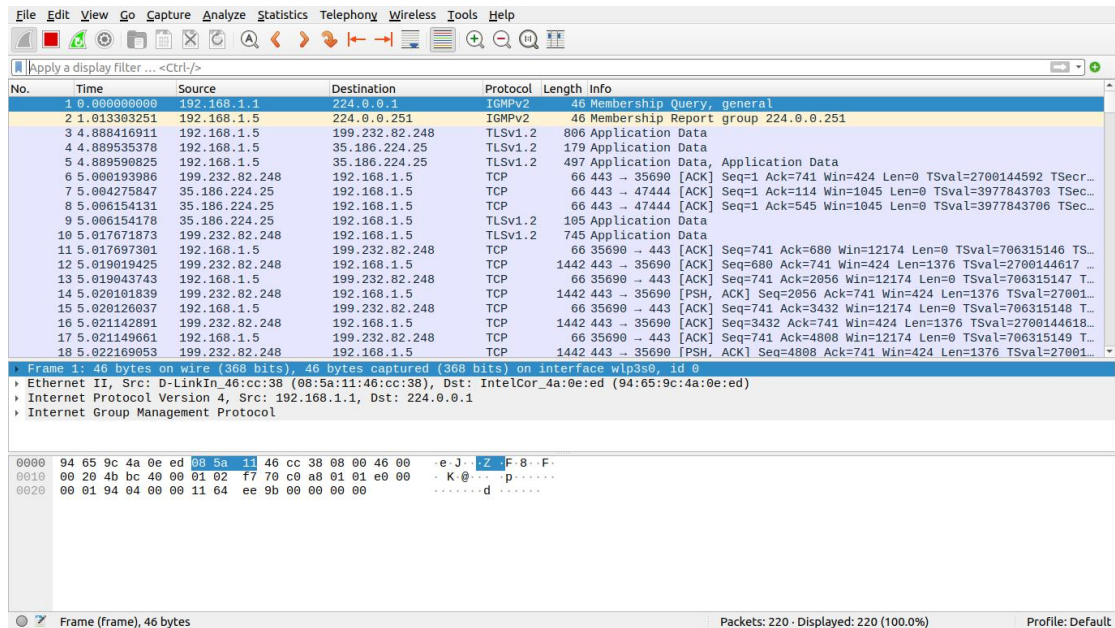
cette zone est située dans la moitié inférieure droite de la fenêtre de Wireshark et affiche une vue hiérarchique du paquet sélectionné dans la zone de liste des paquets. Cette vue est organisée en arbre, avec chaque nœud représentant un champ de protocole différent

dans le paquet. Cette zone permet à l'utilisateur de naviguer rapidement dans les différents champs du paquet et d'analyser en détail chaque aspect de la communication réseau.

III. Capturer une requête de ping :

Pour capturer une requête de ping (ICMP Echo Request) avec Wireshark, en suivez les étapes suivantes :

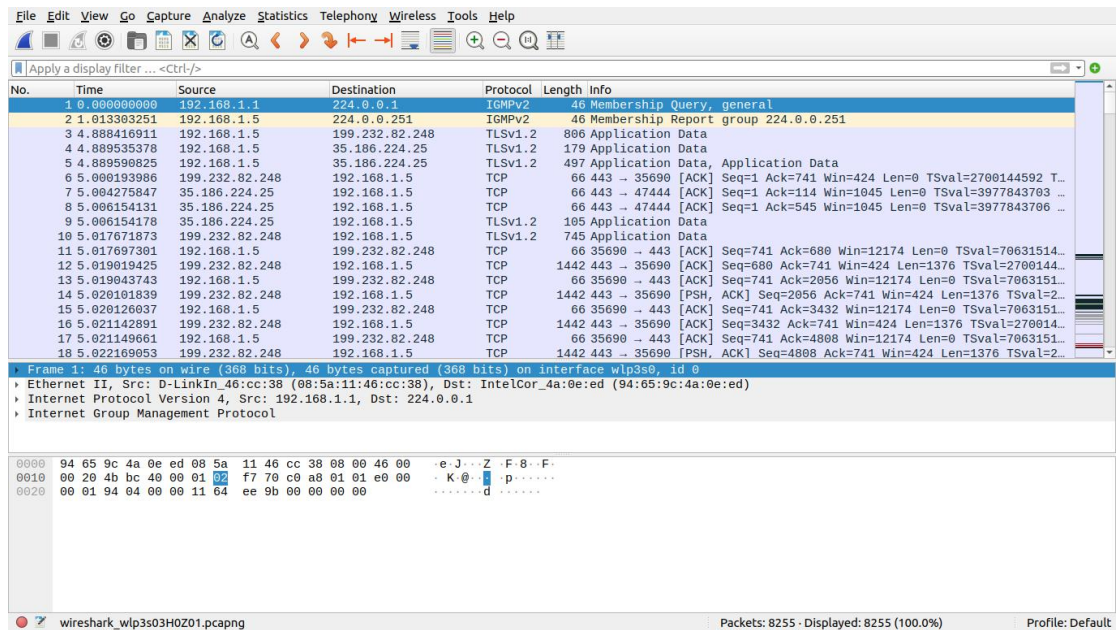
1. Démarrez la capture :



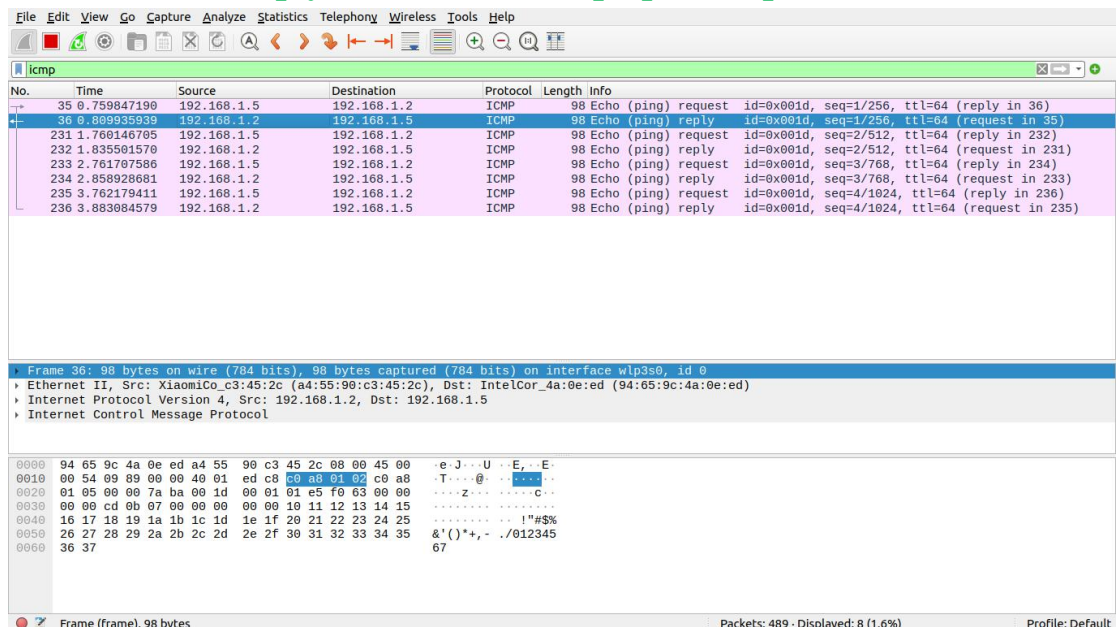
2. Exécutez la commande ping à partir de la ligne de commande :

```
imad@imad-ThinkPad-X250: ~  
imad@imad-ThinkPad-X250:~$ ping 192.168.1.2  
PING 192.168.1.2 (192.168.1.2) 56(84) bytes of data.  
64 bytes from 192.168.1.2: icmp_seq=1 ttl=64 time=96.3 ms  
64 bytes from 192.168.1.2: icmp_seq=2 ttl=64 time=120 ms  
64 bytes from 192.168.1.2: icmp_seq=3 ttl=64 time=39.3 ms  
64 bytes from 192.168.1.2: icmp_seq=4 ttl=64 time=63.2 ms  
^C  
--- 192.168.1.2 ping statistics ---  
4 packets transmitted, 4 received, 0% packet loss, time 3002ms  
rtt min/avg/max/mdev = 39.347/79.590/119.558/30.679 ms  
imad@imad-ThinkPad-X250:~$
```


3. Une fois que vous avez envoyé la requête de ping, retournez à l'interface de Wireshark et arrêtez la capture :



4. Pour filtrer les résultats de la capture et afficher uniquement les requêtes de ping, saisissez "icmp" dans la barre de filtre. Vous devriez maintenant voir les paquets ICMP Echo Request et Echo Reply dans la liste des paquets capturés :



5. Exercice 1 : Analyse de la requête de ping :

a) Type: 8 (Echo (ping) request) :

	Adresse Mac physique		Adresse IP		ICMP (Request)
	Source	Destination	Source	Destination	
Trame "echo request" Ping aller	94 65 9c 4a 0e ed	a4 55 90 c3 45 2c	192.168.1.5	192.168.1.2	

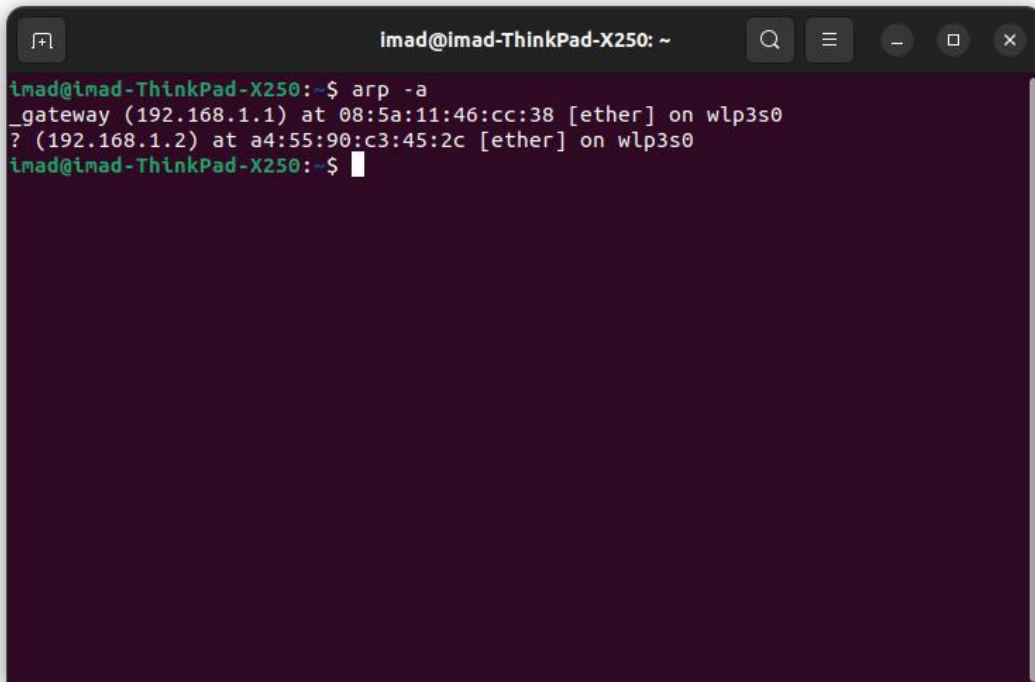
- ◆ *Sur quel type de codage(du système de numération) est codée l'adresse MAC physique?* L'adresse MAC (Media Access Control) est codée en hexadécimal.
- ◆ *Sur combien d'octets est codée l'adresse MAC physique?* L'adresse MAC (Media Access Control) physique est codée sur 6 octets, ce qui équivaut à 48 bits.
- ◆ *A quoi correspondent les trois premiers octets?* Les trois premiers octets de l'adresse MAC (Media Access Control) correspondent à l'identifiant d'organisation unique (OUI), qui permet d'identifier le fabricant de la carte réseau ou du périphérique qui contient cette adresse MAC.
- ◆ *Et les autres octets?* Les trois derniers octets de l'adresse MAC (Media Access Control) sont appelés "identificateur d'interface", et ils sont attribués par le fabricant de la carte réseau ou du périphérique. Ces trois octets représentent les 24 derniers bits de l'adresse MAC.

b) Type: 8 (Echo (ping) reply) :

	Adresse Mac physique		Adresse IP		ICMP (Request)
	Source	Destination	Source	Destination	
Trame "echo request" Ping aller	a4 55 90 c3 45 2c	94 65 9c 4a 0e ed	192.168.1.2	192.168.1.5	

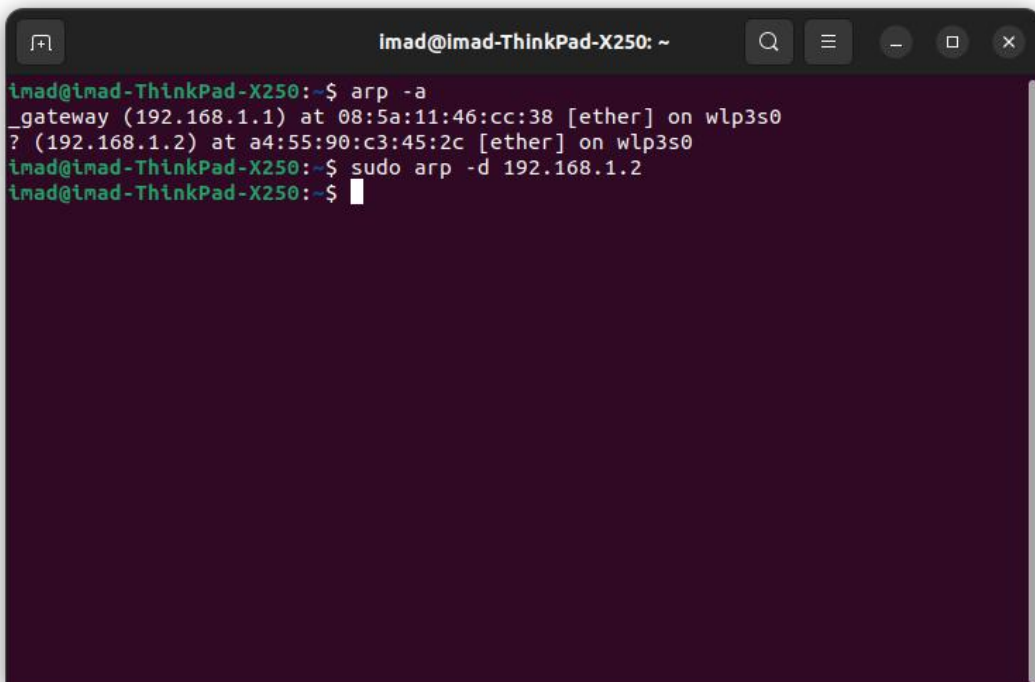
6. Analyse ARP et ICMP :

a) consultez et videz la table (cache) ARP :



```
imad@imad-ThinkPad-X250: ~  
imad@imad-ThinkPad-X250:~$ arp -a  
_gateway (192.168.1.1) at 08:5a:11:46:cc:38 [ether] on wlp3s0  
? (192.168.1.2) at a4:55:90:c3:45:2c [ether] on wlp3s0  
imad@imad-ThinkPad-X250:~$
```

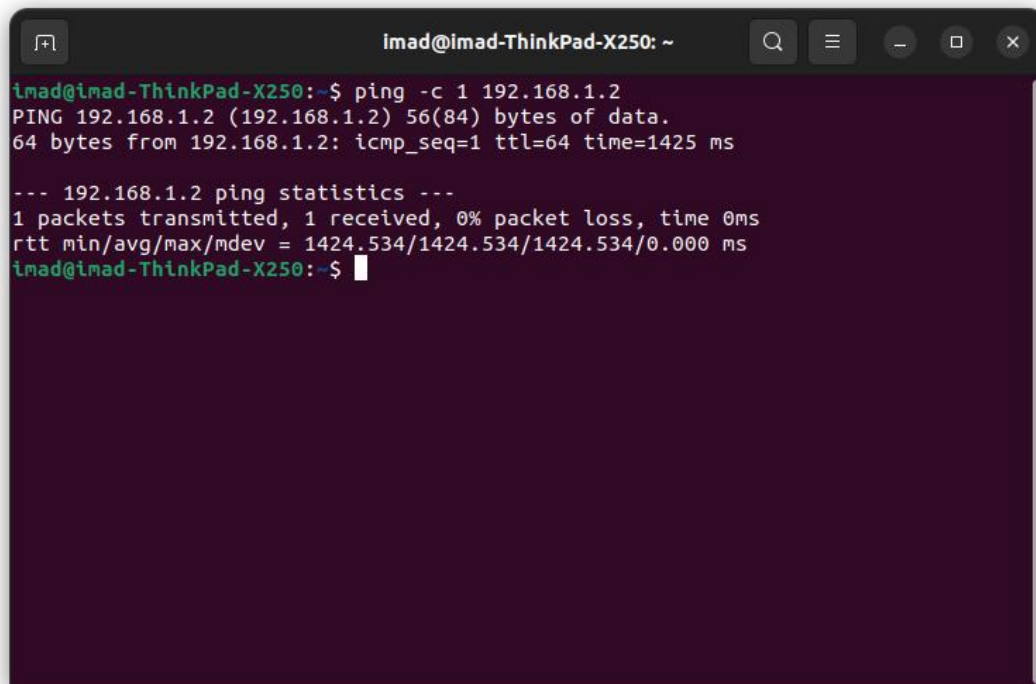
Cette commande affiche la table ARP en cache de votre machine, qui contient les adresses MAC correspondant aux adresses IP des différents périphériques sur le réseau local. Si vous souhaitez vider la table ARP, vous pouvez généralement le faire en utilisant la commande suivante :



```
imad@imad-ThinkPad-X250: ~  
imad@imad-ThinkPad-X250:~$ arp -a  
_gateway (192.168.1.1) at 08:5a:11:46:cc:38 [ether] on wlp3s0  
? (192.168.1.2) at a4:55:90:c3:45:2c [ether] on wlp3s0  
imad@imad-ThinkPad-X250:~$ sudo arp -d 192.168.1.2  
imad@imad-ThinkPad-X250:~$
```

Il est important de noter que vider la table ARP peut entraîner des perturbations temporaires de la connectivité réseau de votre machine, car elle devra récupérer les adresses MAC des périphériques sur le réseau local.

b) lancer un ping vers la machine voisine en ne générant qu'un seul paquet de demande d'écho :

A terminal window titled 'imad@imad-ThinkPad-X250: ~' with standard window controls. The terminal shows the execution of the command 'ping -c 1 192.168.1.2'. The output indicates a successful ping to 192.168.1.2 with 56(84) bytes of data, a TTL of 64, and a time of 1425 ms. It also displays ping statistics: 1 packet transmitted, 1 received, 0% packet loss, and an rtt of 1424.534 ms.

```
imad@imad-ThinkPad-X250:~$ ping -c 1 192.168.1.2
PING 192.168.1.2 (192.168.1.2) 56(84) bytes of data.
64 bytes from 192.168.1.2: icmp_seq=1 ttl=64 time=1425 ms

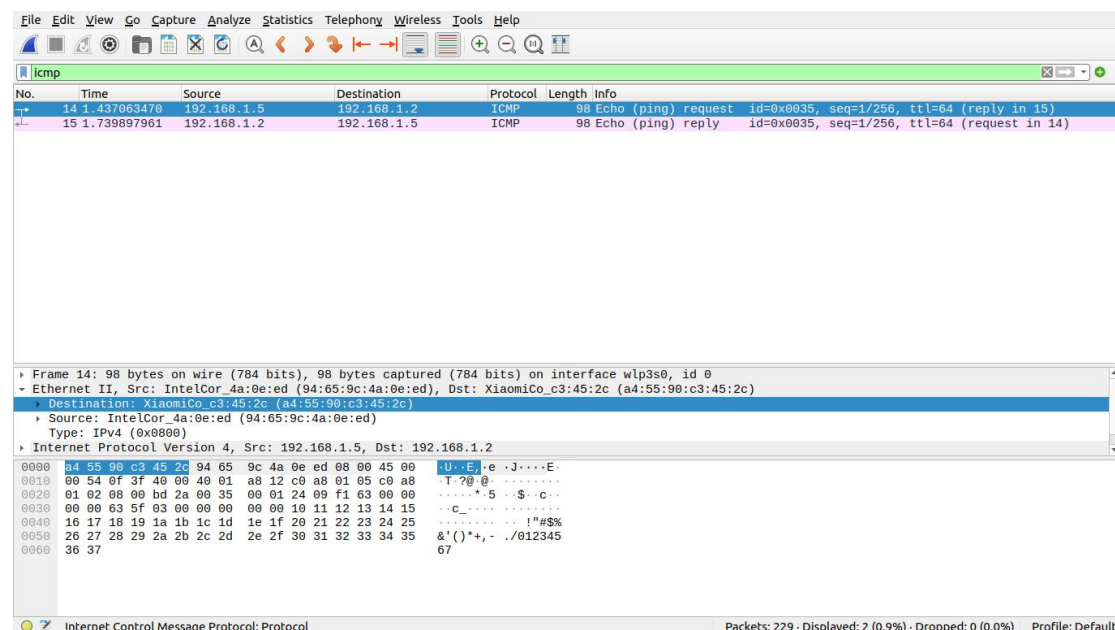
--- 192.168.1.2 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 1424.534/1424.534/1424.534/0.000 ms
imad@imad-ThinkPad-X250:~$
```

Le format d'un message ARP (Address Resolution Protocol) est composé des champs suivants :

- ◆ Type de matériel (Hardware Type) : indique le type de matériel utilisé pour les adresses MAC, généralement Ethernet (valeur 1).
- ◆ Type de protocole (Protocol Type) : indique le type de protocole de la couche réseau utilisé, généralement IPv4 (valeur 0x0800) ou IPv6 (valeur 0x86DD).
- ◆ Longueur des adresses matérielles (Hardware Address Length) : indique la taille en octets des adresses MAC, généralement 6.
- ◆ Longueur des adresses protocoles (Protocol Address Length) : indique la taille en octets des adresses de protocole, généralement 4 pour IPv4.
- ◆ Opcode : indique le type d'opération, soit une demande ARP (valeur 1) soit une réponse ARP (valeur 2).
- ◆ Adresse MAC source (Sender Hardware Address) : l'adresse MAC de l'émetteur de la trame ARP.
- ◆ Adresse IP source (Sender Protocol Address) : l'adresse IP de l'émetteur de la trame ARP.

- ◆ Adresse MAC cible (Target Hardware Address) : l'adresse MAC de la machine dont on veut connaître l'adresse IP, ou l'adresse MAC de la machine qui répond à la demande ARP.

En résumé, le message ARP est utilisé pour associer une adresse IP à une adresse MAC en demandant à une machine de répondre avec son adresse MAC correspondante. Les différents champs dans le format de la trame ARP permettent de spécifier les adresses MAC et IP associées et le type d'opération ARP.



Le format d'un message ICMP (Internet Control Message Protocol) est composé des champs suivants :

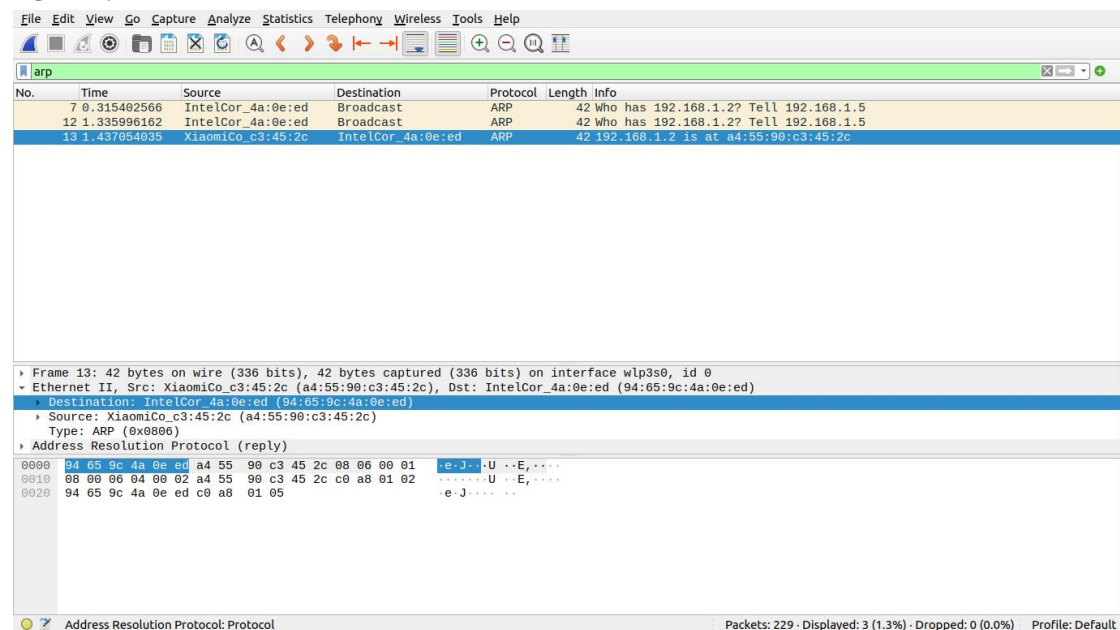
- ◆ Type : indique le type de message ICMP.
- ◆ Code : permet de préciser la nature du message ou de donner plus de détails sur l'erreur, en fonction du type de message.
- ◆ Somme de contrôle (Checksum) : permet de vérifier l'intégrité des données ICMP en utilisant un algorithme de hachage.
- ◆ Données supplémentaires (Data) : champ facultatif, contenant des informations complémentaires en fonction du type et du code du message ICMP.

Le rôle de chaque champ est le suivant :

- ◆ Le type permet de définir la nature du message ICMP, et peut prendre différentes valeurs en fonction de l'opération à effectuer. Par exemple, le type 8 (Echo Request) est utilisé pour envoyer une demande d'écho, tandis que le type 3 (Destination Unreachable) est utilisé pour indiquer qu'un paquet n'a pas pu être acheminé.

- ◆ Le code est utilisé pour fournir des informations supplémentaires sur le type de message ICMP. Par exemple, le code 0 pour le type 3 (Destination Unreachable) indique que la destination est inaccessible, tandis que le code 1 pour le même type indique que la communication est interdite.

En résumé, le protocole ICMP est utilisé pour transmettre des messages de contrôle et de diagnostic sur le réseau Internet. Les différents champs dans le format de la trame ICMP permettent de spécifier le type et le code de message, de vérifier l'intégrité des données, et de fournir des informations complémentaires en fonction du type et du code de message ICMP.



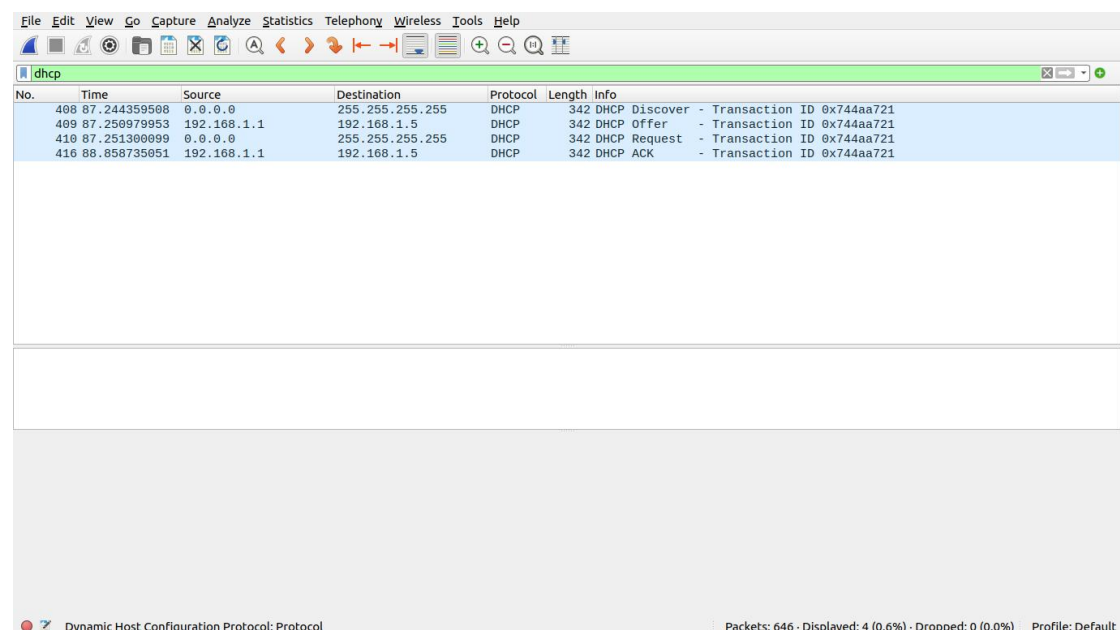
No.	Time	Source	Destination	Protocol	Length	Info
7	0.315402566	IntelCor_4a:0e:ed	Broadcast	ARP	42	Who has 192.168.1.2? Tell 192.168.1.5
12	1.335996162	IntelCor_4a:0e:ed	Broadcast	ARP	42	Who has 192.168.1.2? Tell 192.168.1.5
13	1.437054035	XiaomiCo_c3:45:2c	IntelCor_4a:0e:ed	ARP	42	192.168.1.2 is at a4:55:90:c3:45:2c

Frame 13: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface wlp3s0, id 0
 Ethernet II, Src: XiaomiCo_c3:45:2c (a4:55:90:c3:45:2c), Dst: IntelCor_4a:0e:ed (94:65:9c:4a:0e:ed)
 Destination: IntelCor_4a:0e:ed (94:65:9c:4a:0e:ed)
 Source: XiaomiCo_c3:45:2c (a4:55:90:c3:45:2c)
 Type: ARP (0x0806)
 Address Resolution Protocol (reply)

0000 94 65 9c 4a 0e ed a4 55 90 c3 45 2c 08 06 00 01 e J . . . U . . E, . . .
 0010 08 00 06 04 00 02 a4 55 90 c3 45 2c c0 a8 01 02 U . . E, . . .
 0020 94 65 9c 4a 0e ed c0 a8 01 05 e J

Address Resolution Protocol: Protocol Packets: 229 · Displayed: 3 (1.3%) · Dropped: 0 (0.0%) Profile: Default

7. Exercice 3 : Analyse du DHCP :



No.	Time	Source	Destination	Protocol	Length	Info
408	87.244359508	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x744aa721
409	87.250979953	192.168.1.1	192.168.1.5	DHCP	342	DHCP Offer - Transaction ID 0x744aa721
410	87.251300099	0.0.0.0	255.255.255.255	DHCP	342	DHCP Request - Transaction ID 0x744aa721
416	88.858735051	192.168.1.1	192.168.1.5	DHCP	342	DHCP ACK - Transaction ID 0x744aa721

Dynamic Host Configuration Protocol: Protocol Packets: 646 · Displayed: 4 (0.6%) · Dropped: 0 (0.0%) Profile: Default

a) les messages DHCP utilisent UDP ou TCP :

Les messages DHCP (Dynamic Host Configuration Protocol) utilisent le protocole de couche de transport UDP (User Datagram Protocol), et non TCP (Transmission Control Protocol).

b) les adresses IP source et destination utilisées dans le DHCP Discover et Request :

Ce message est envoyé en utilisant l'adresse IP source 0.0.0.0 et l'adresse IP destination 255.255.255.255, qui représente une diffusion de niveau réseau (broadcast) sur toutes les interfaces du réseau.

c) valeurs dans le DHCP Discover permettent de le différencier du message DHCP Request :

Le DHCP Discover et le DHCP Request sont deux messages différents utilisés dans le processus de configuration dynamique des adresses IP. Voici les valeurs qui permettent de différencier ces deux types de messages :

- ◆ Type de message : Le champ "type de message" (Message Type) du message DHCP Discover est défini à 1, alors que le champ "type de message" du message DHCP Request est défini à 3.
- ◆ Adresses IP source et destination : Les adresses IP source et destination utilisées dans le DHCP Discover et le DHCP Request sont différentes. Dans le DHCP Discover, l'adresse IP source est généralement 0.0.0.0, tandis que l'adresse IP destination est une adresse de diffusion (broadcast) de niveau réseau, telle que 255.255.255.255. Dans le DHCP Request, l'adresse IP source est généralement l'adresse IP que le client a reçue de l'un des serveurs DHCP en réponse au DHCP Discover, tandis que l'adresse IP destination est l'adresse IP du serveur DHCP qui a fourni cette adresse IP.
- ◆ Options : Les messages DHCP Discover et DHCP Request contiennent des options différentes. Le DHCP Discover peut inclure des options telles que le type de matériel, l'ID de client DHCP, les options de classe, etc. Le DHCP Request, quant à lui, contient des options telles que l'adresse IP offerte par le serveur DHCP, l'adresse IP du serveur DHCP, le masque de sous-réseau, la passerelle par défaut, les serveurs DNS, etc.

En résumé, le DHCP Discover est utilisé par un client pour découvrir les serveurs DHCP disponibles sur le réseau, tandis que le DHCP Request est

utilisé pour demander l'adresse IP offerte par un serveur DHCP spécifique. Les valeurs telles que le type de message, les adresses IP source et destination, ainsi que les options incluses dans chaque message permettent de les différencier facilement.

d) l'adresse du serveur DHCP :

L'adresse du serveur DHCP peut varier en fonction de la configuration du réseau et de la façon dont le serveur DHCP est configuré. En général, il y a deux façons principales pour un client DHCP de découvrir l'adresse du serveur DHCP :

- ◆ **Broadcast de niveau réseau :** Lorsqu'un client DHCP démarre, il envoie un message DHCP Discover en utilisant l'adresse IP source 0.0.0.0 et l'adresse IP destination de diffusion (broadcast) de niveau réseau, qui est généralement 255.255.255.255. Le serveur DHCP qui reçoit ce message peut répondre en envoyant un message DHCP Offer contenant une adresse IP disponible pour le client, ainsi que l'adresse IP du serveur DHCP.
- ◆ **Configuration statique :** Dans certains cas, l'adresse IP du serveur DHCP peut être configurée statiquement sur le client ou sur le réseau. Dans ce cas, le client sait déjà quelle adresse IP utiliser pour communiquer avec le serveur DHCP.

Il est important de noter que l'adresse IP du serveur DHCP peut également être affectée par la configuration du réseau et la topologie. Par exemple, si le réseau est segmenté en plusieurs sous-réseaux, il peut y avoir plusieurs serveurs DHCP configurés sur chaque sous-réseau pour servir les clients sur ce sous-réseau. Dans ce cas, l'adresse IP du serveur DHCP dépendra du sous-réseau sur lequel se trouve le client.

IV. Résumé :

Wireshark est un outil de capture de paquets qui permet de capturer et d'analyser le trafic réseau en temps réel. Dans ce rapport, nous avons examiné comment utiliser Wireshark pour capturer des trames de données à partir d'un réseau. Nous avons discuté des différentes options de capture disponibles dans Wireshark, y compris la sélection de l'interface réseau, la définition des filtres de capture et la configuration des options de capture avancées.

Nous avons également discuté des différents types de trames que l'on peut capturer avec Wireshark, tels que les trames Ethernet, les trames Wi-Fi et les trames TCP/IP. Nous avons également examiné comment interpréter les données capturées en utilisant Wireshark, en utilisant les fonctionnalités de décodage automatique de protocole pour identifier les protocoles utilisés et en utilisant les outils de filtrage pour trouver des informations spécifiques dans les données capturées.