TP5 – Trames ARP, ICMP, DNS

SAOU Rayan

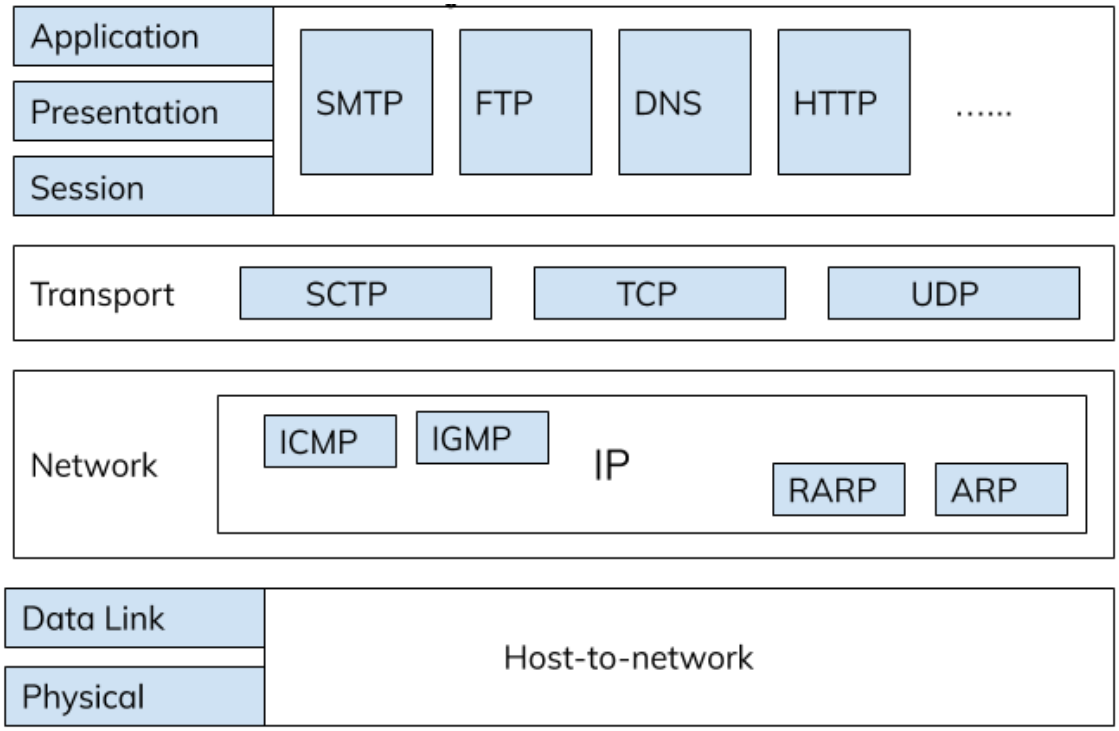


Table des matières

---

1. Capture de trames ARP et ICMP.

Nous ouvrons **Wireshark** et nous démarrons notre capture de trame. Ensuite nous démarrons notre invite de commande et nous faisons une commande ***ping*** à *172.17.254.5* (Aviateur)

```
C:\Users\Rayan>ping 172.17.254.5

Envoi d'une requête 'Ping'  172.17.254.5 avec 32 octets de données :
Réponse de 172.17.254.5 : octets=32 temps=12 ms TTL=64
Réponse de 172.17.254.5 : octets=32 temps=9 ms TTL=64
Réponse de 172.17.254.5 : octets=32 temps=9 ms TTL=64
Réponse de 172.17.254.5 : octets=32 temps=12 ms TTL=64

Statistiques Ping pour 172.17.254.5:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 9ms, Maximum = 12ms, Moyenne = 10ms
```

Figure 1: Commande ping à Aviateur

Nous arrêtons ensuite notre capture de trame et nous voyons que la trame ARP est bien partie donc nous n'avons pas besoin d'effectuer la commande ***arp -d ** pour vider le cache ARP.

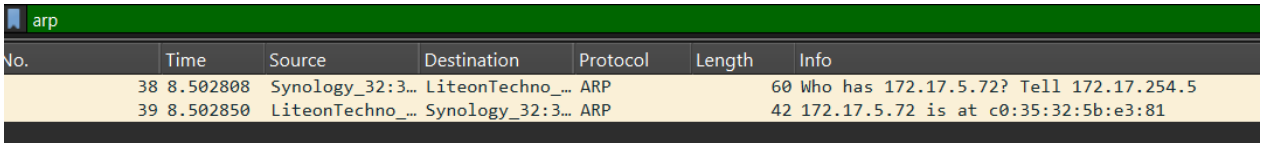


Figure 2 : Trames ARP capturées avec Wireshark

Et nous pouvons aussi vérifier avec la commande ***arp -a*** pour consulter le cache ARP et confirmer l'association IP-MAC.

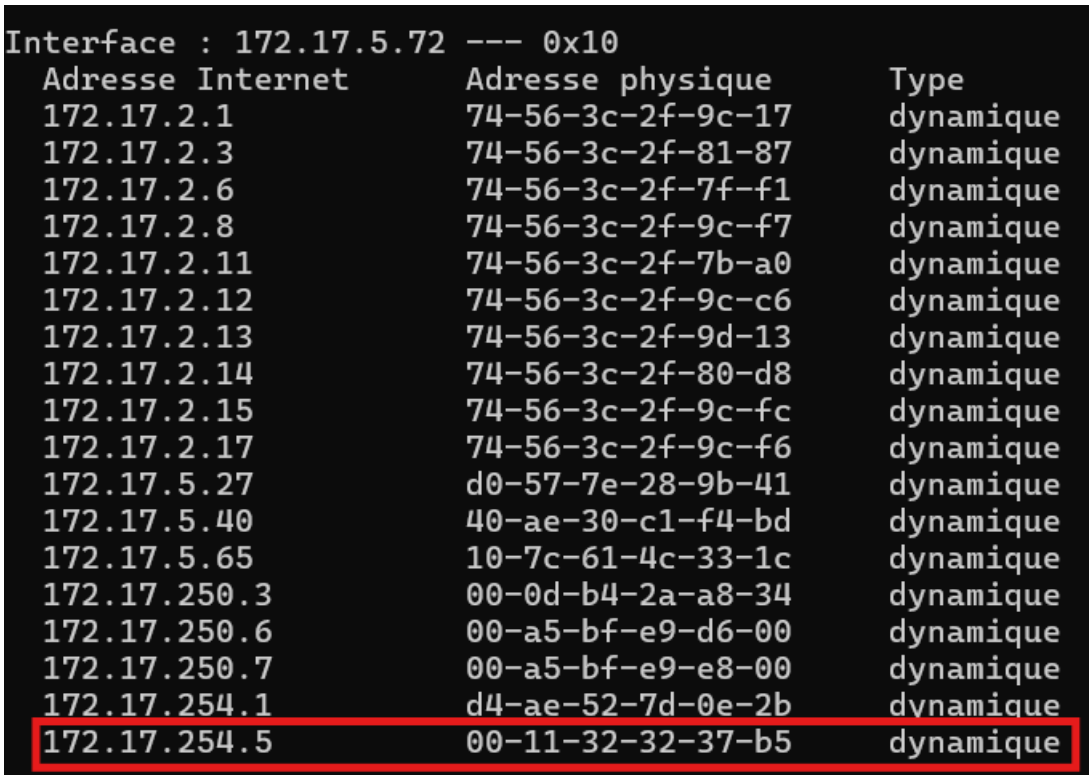


Figure 3 : Résultat de la commande arp -a

La signification des octets de position **0x0C** et **0x0D** ligne 0000 est le ***champ Ether-type***, dans notre champ actuel 0806 signifie qu'il s'agit d'un message ARP.

La fonction de la trame **ARP Request** est de pouvoir demander aux autres machines localement (**broadcast**) pour savoir l'adresse MAC avec l'IP qui lui est associée.

La longueur d'un message **ARP** contenu dans la trame est de **28 octets**.

La longueur de la trame ARP Request est **de 60 octets**.

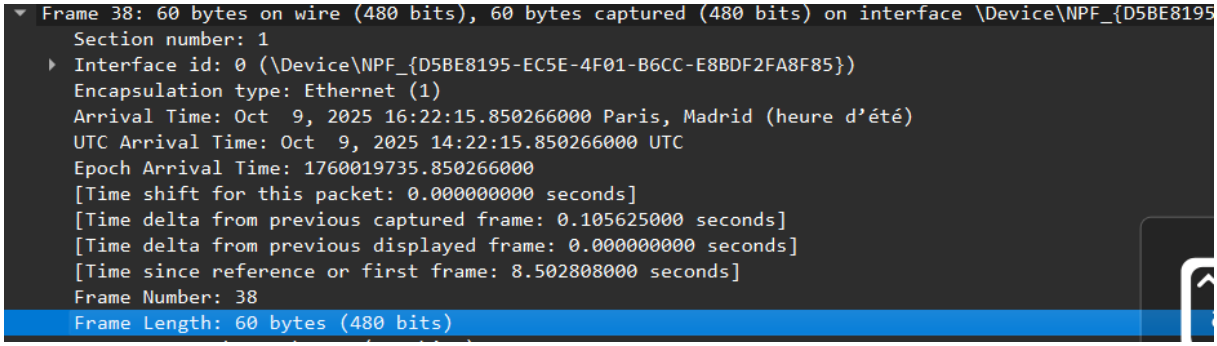


Figure 4 : Informations sur la longueur de la trame ARP Request

Et pour la longueur de la trame ARP Reply il s'agit de **42 octets**.

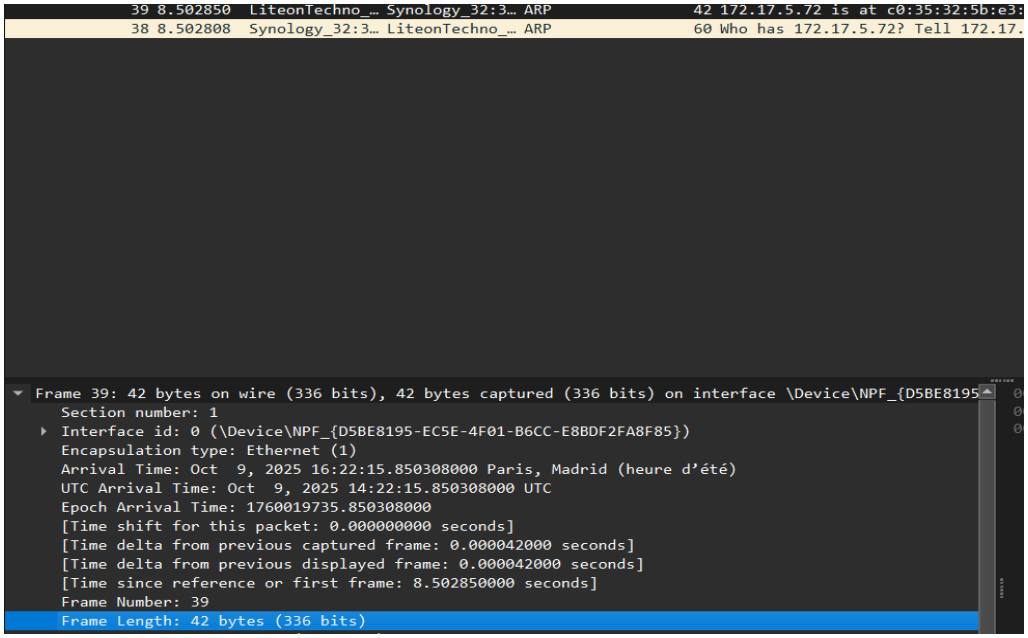


Figure 5 : Informations sur la longueur de la trame ARP Reply

Tandis que **le nombre d'octets** utilisé pour le padding est de. **18**

Nous pouvons donc remplir les informations sur la trame ARP Request :

- **Adresse MAC Destination** : ***c0:35:32:5b:e3:81***
- **Adresse MAC Source** : ***00:11:32:32:37:b5***
- **Ethertype** : ***08 06*** (ARP)
- **Opcode (en hexa.)** : ***00 01*** (Request)
- **L'adresse MAC Target** ***: 00:00:00:00:00:00***
- **Et l'adresse IP de la Target** : ***172.17.5.72***

Nous sélectionnons ensuite notre trame ICMP Echo Request et nous pouvons déduire les points suivants.

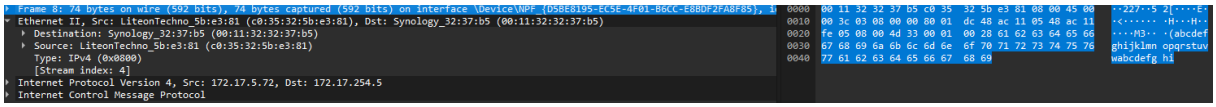


Figure 6 : Informations sur la trame ICMP Echo Request

- Les octets de **position 0x0C et 0x0D** ligne 0000, est le champ Ethertype qui est de **0800**, il s'agit donc d'un paquet IP encapsulé.
- Dans l'octet de position 0x07 ligne 0010, il s'agit de la valeur en hexa 01, c'est-à-dire le protocole ICMP.

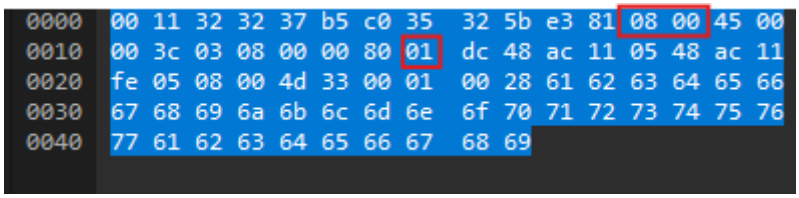


Figure 7 : Trame brute (en hexadécimal) avec le champ Ethertype et le champ protocole ICMP

- La longueur de la trame est de **74 octets.**

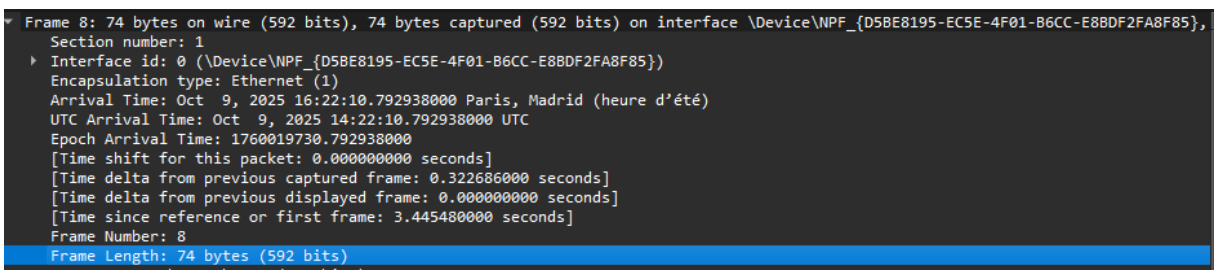


Figure 8 : Informations sur la trame ICMP

- La longueur du paquet IP est de **20 octets**.

- Et la longueur du message ICMP est de **40 octets**
- La signification de l'octet de position 0x02 ligne 0020 est de 08, il s'agit donc du **type ICMP Request**.
- A partir de l'octet de position 0x0A de la ligne 0020, il y **a les données applicatives**.

Nous sélectionnons ensuite notre trame **ICMP Echo Reply**. Et nous pouvons donc aussi répondre et remplir les informations suivantes.

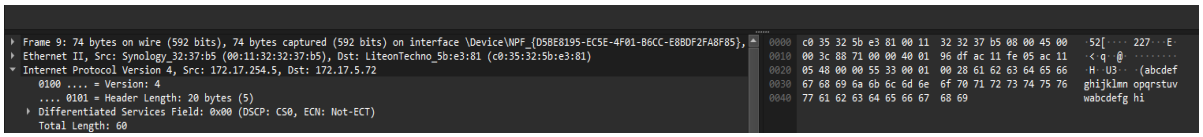


Figure 9 : Informations sur la trame ICMP Echo Reply

- Le nom et la valeur de l'octet de position 0x02 ligne 0020, il s'agit du type ICMP, dans le cas présent**, il est à 00, donc Echo Reply**.

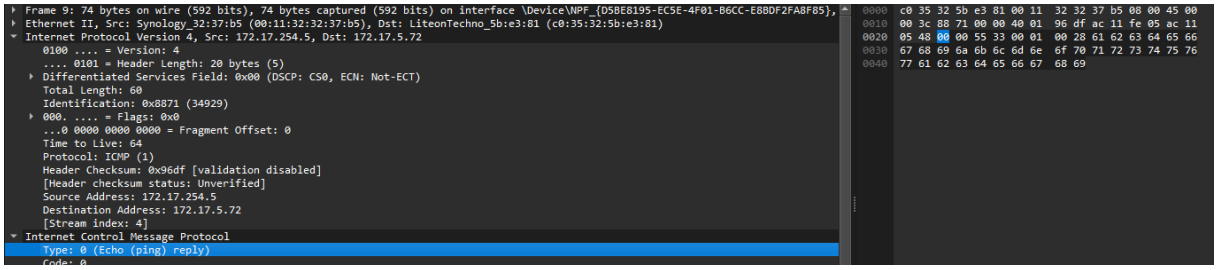
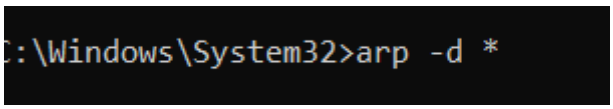


Figure 10 : Section ICMP développée pour afficher le champ type ICMP

2. Capture de trames ARP, DNS et ICMP

Nous allons capturer des trames ICMP depuis une commande ping vers le serveur ac-nice.fr, mais avant nous allons vider notre cache ARP en effectuant la commande ***arp -d ****.



Et nous démarrons notre capture de trames avec Wireshark.

La machine dont l'adresse MAC est recherchée est le routeur Stormshield.

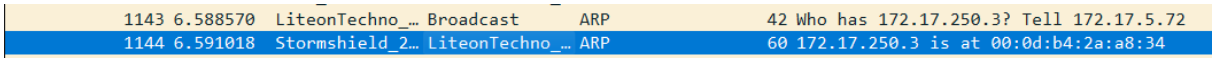


Figure 11 : Trames capturées de l'échange ARP

C'est-à-dire 00:0d:b4:2a:a8:34 (Adresse MAC du routeur Stormshield).

Nous pouvons ainsi remplir les informations suivantes :

- Adresse **MAC Destination** : ff:ff:ff:ff:ff:ff
- Adresse **MAC Source** : c0:35:32:5b:e3:81
- L'Ethertype est **0806** en hexadécimal c'est-à-dire que c'est **un message ARP**

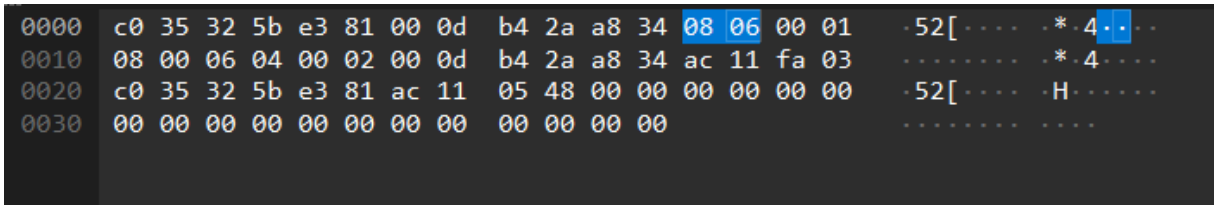


Figure 12 : Trame brute (en hexadécimal) du message ARP Request

- **L'Opcode** est **01**, donc une **ARP Request**.
- **MAC Cible** : 00:00:00:00:00:00
- **Et l'IP Cible** : 172.17.250.3

  - La raison pour laquelle nous trouvons un échange de requête ARP avant l'envoi de requête DNS est dû au fait que **nous avons supprimer notre cache ARP pendant notre capture** puis nous avons fait un ***ping*** au serveur web ac-nice.fr, pour faire cela on doit avoir accès au routeur, mais nous ne connaissons pas le routeur ; **la requête ARP devient donc vitale** pour pouvoir échanger avec le routeur et faire sortir la requête sur Internet.

Nous consultons notre cache DNS et nous voyons notre présence du site www.ac-nice.fr avec la commande ***ipconfig /displaydns***

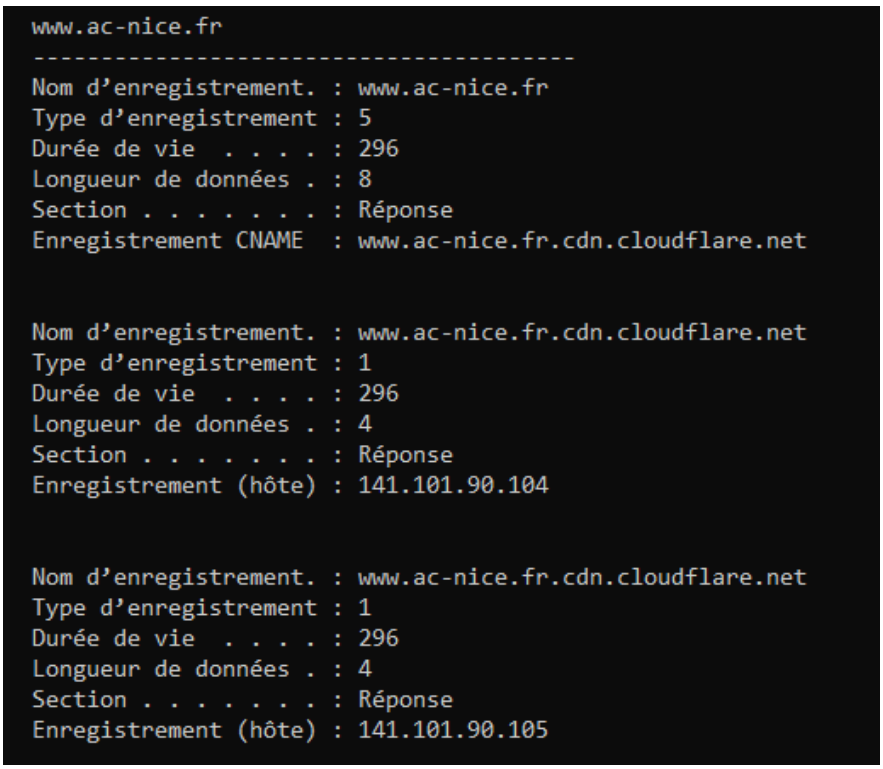


Figure 13 : Résultat de la commande ipconfig /displaydns pour le site www.ac-nice.fr

Quand nous refaisons une requête ping sur le même site, nous ne revoyons logiquement **aucune requête DNS**.

Nous vidons notre cache DNS en effectuant la commande ***ipconfig /flushdns*** et nous refaisons notre capture de trame et notre ping.

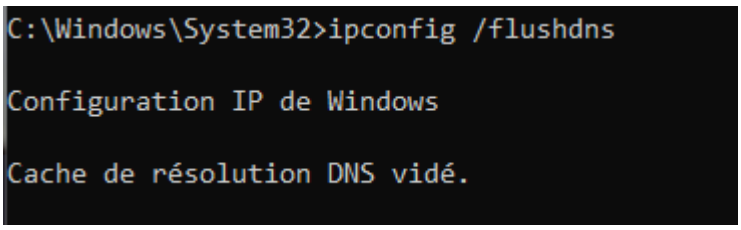


Figure 14 : Résultat de le commande ipconfig /flushdns dans l'invite de commande

Nous faisions une commande ***ping*** vers le serveur web ac-nice.fr pour obtenir notre trame DNS.

Nous pouvons observer ci-dessous la trame.

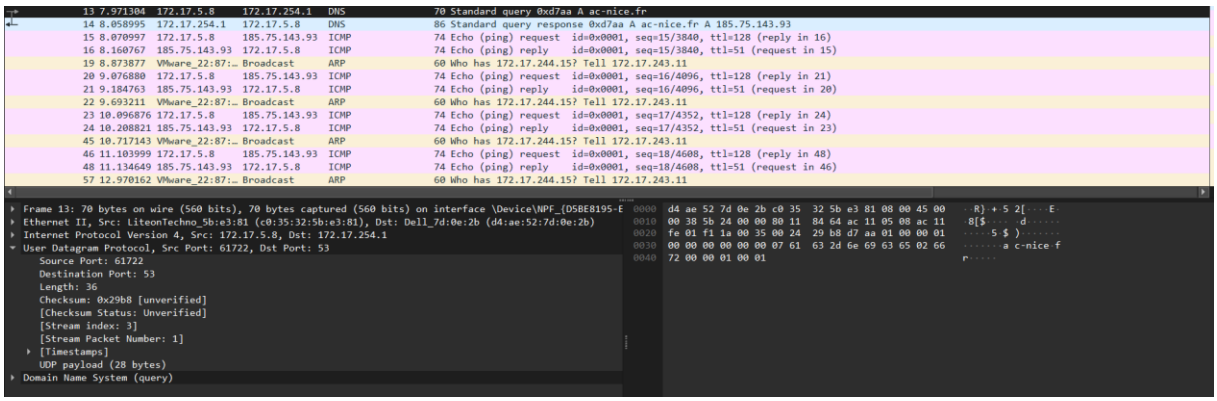


Figure 15 : Trame capturée de la requête DNS pour www.ac-nice.fr

- Dans une trame DNS les différents protocoles encapsulés sont ;
  - Le protocole **DNS** encapsulé dans **UDP**
  - **UDP** encapsulé dans **IPv4**
  - Et **IPv4** encapsulé dans **Ethernet**

La machine destinataire de la requête DNS est le **serveur DNS** (ici ROI), elle a pour IP : ***172.17.254.1***

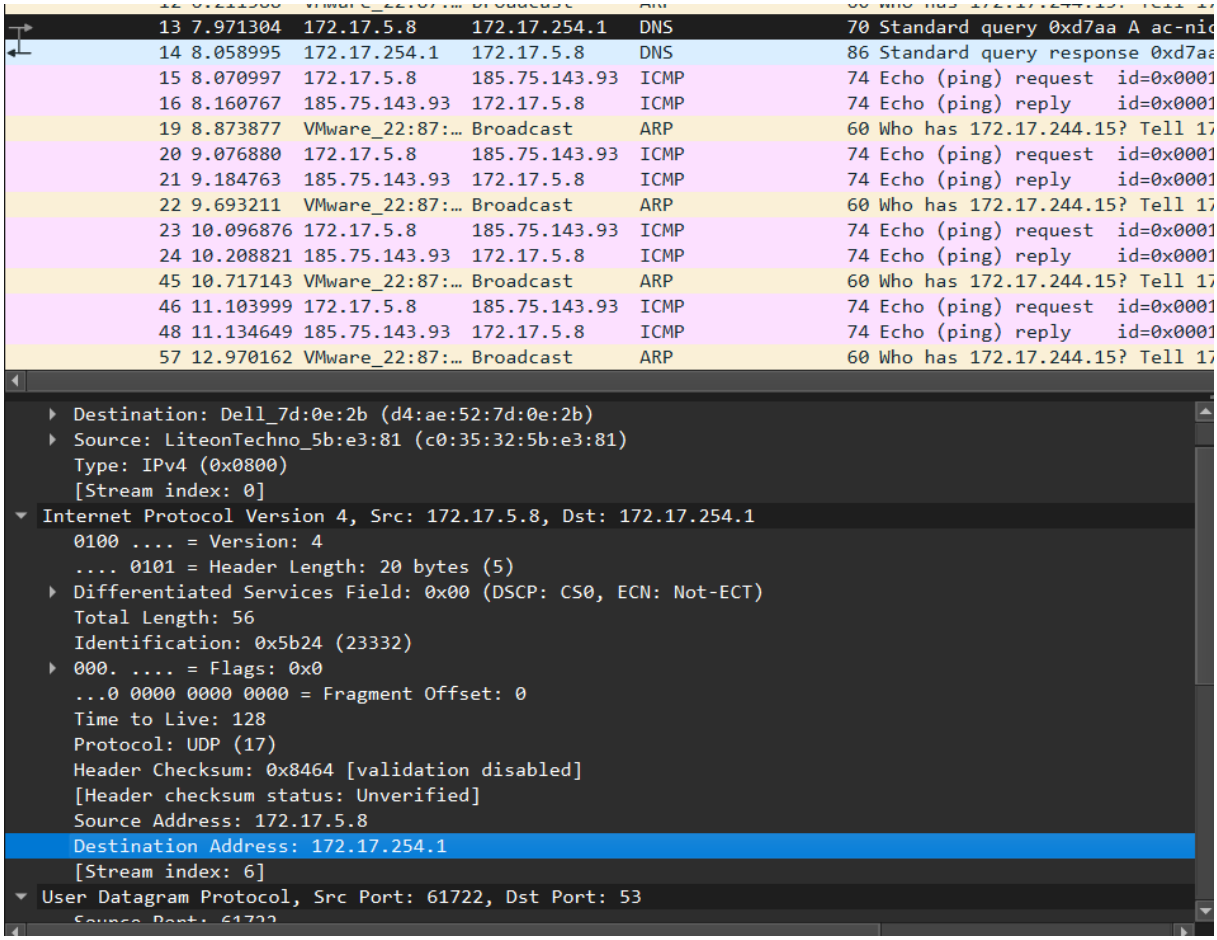


Figure 16 : Adresse IP destination en surbrillance dans la trame DNS

La signification des bits de positions **0×0C**, **0×0D** ligne 0000 et **0×07** ligne 0010 est :

- Le champ Ethertype, ici ***0800*** signifie IPv4.
- La longueur de l'en tête IP est de **20 octets.**
- La longueur de l'en tête Transport (**UDP**) est de **8 octets**.
- La signification qu'ont les octets de position **0×04** et **0×05** ligne 0020 s'agit du champ Port destination, ici il est à **« 00 35 »** en hexadécimal, donc **53** en décimal.
- Les valeurs hexadécimales correspondant au site www.ac-nice.fr est : **« 03 77 77 77 07 61 63 2d 6e 69 63 65 02 66 72 00 »**
- Les valeurs hexadécimales de l'adresse IP du serveur web de l'Académie de Nice est : **« 8d 65 5a 6b »** et en décimal cela nous donne : **« 141.101.90.107 »**.

3. Commande Tracert et capture de trames ICMP.

Nous commençons une nouvelle capture de trame sur Wireshark que nous intitulerons CaptureTracert.

Puis nous ouvrons notre invite de commande et nous tapons la commande suivante : ***tracert*** ***www.ac-nice.fr***

Une fois la commande terminée, nous arrêtons la capture de trames et nous filtrons les captures avec le filtre ***icmp.***

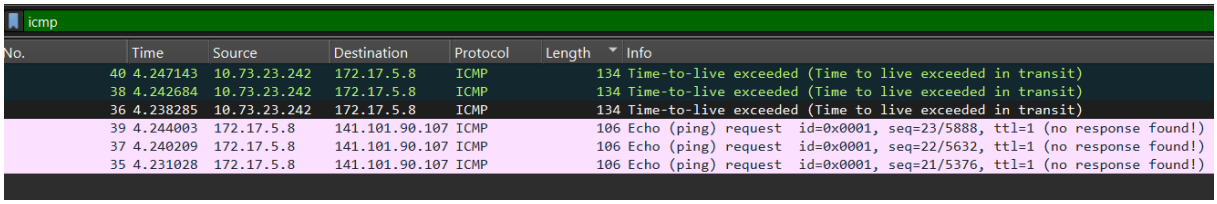


Figure 17 : Trame ICMP suite à la commande tracert

- Quand nous développons l'en-tête IP, nous pouvons déduire **l'IP Destination** qui est : ***141.101.90.107*** en décimal et ***8d 65 5a 6b*** en hexadécimal.

- La valeur portée par le champ TTL en **décimal est 1** et ***01*** en hexadécimal
- La valeur portée par le champ Type dans la section correspondant au message ICMP est ***8*** (**Echo request**) et ***08*** en hexadécimal

Nous sélectionnons la première trame avec le message d'erreur ***ICMP TTL exceeded*** et nous développons la section correspondant au message ICMP et nous voyons dans le champ Type la valeur **11**, sois ***0B*** en hexadécimal.