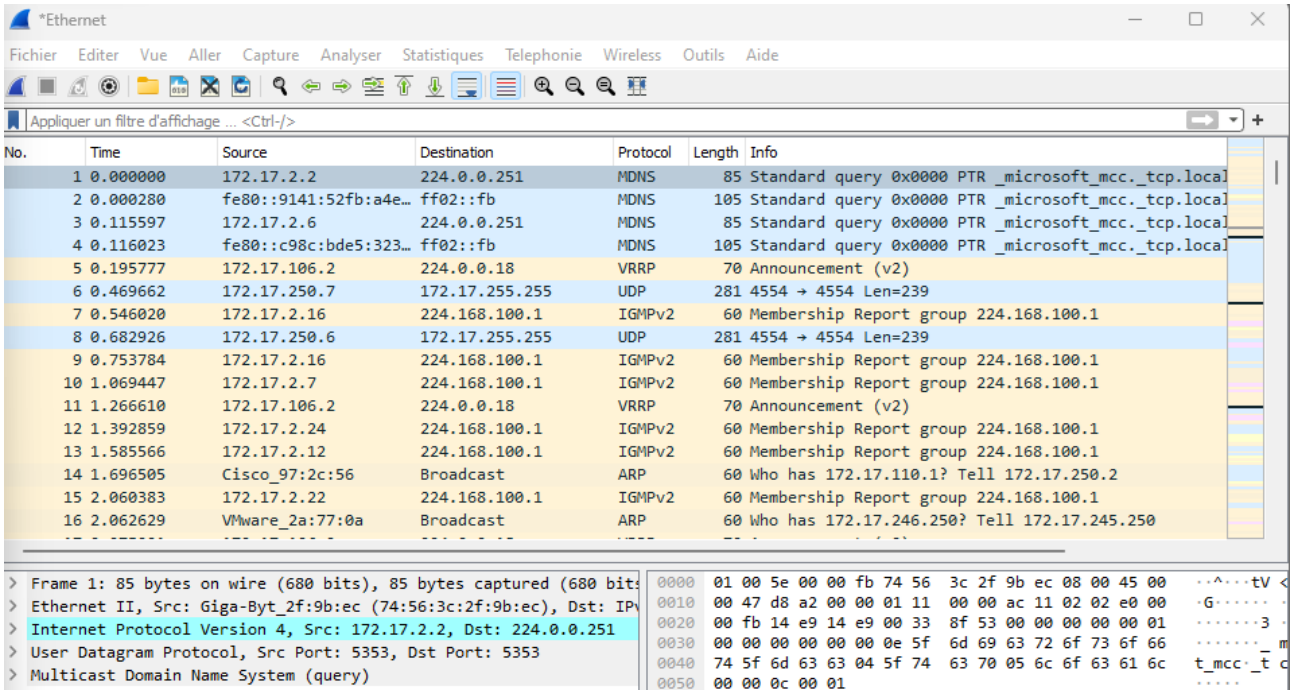
TP 5 – Trames ARP, ICMP et DNS

4.1. Capture de trames ARP et ICMP.

▪ Ouvrez Wireshark et démarrez une capture de trames.



▪ Pinguez le serveur ROI (172.17.254.1). Effectuez une capture d’écran.

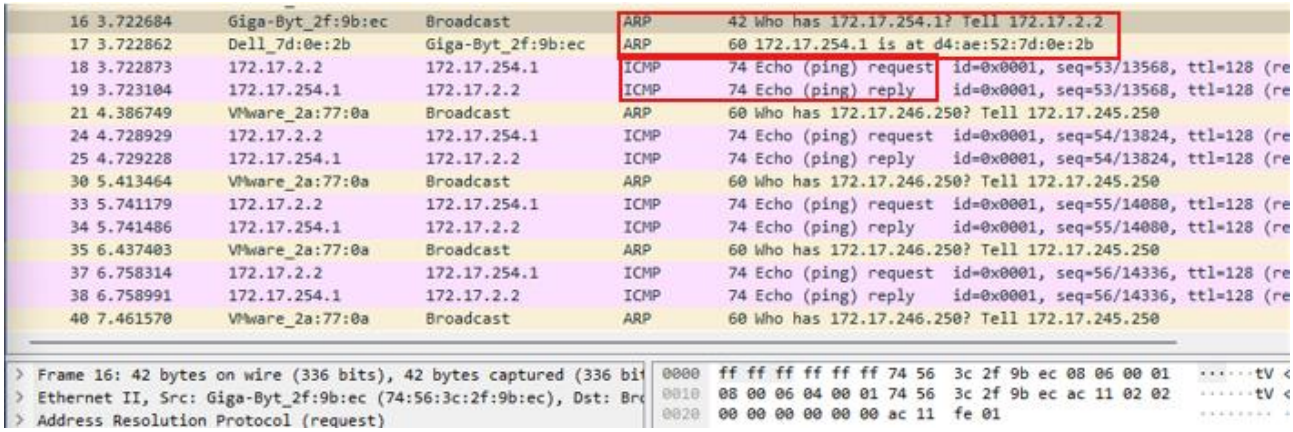
```
C:\Users\rcroquelois>ping 172.17.254.1

Envoi d'une requête 'Ping'  172.17.254.1 avec 32 octets de données :
Réponse de 172.17.254.1 : octets=32 temps<1ms TTL=128
Réponse de 172.17.254.1 : octets=32 temps<1ms TTL=128
Réponse de 172.17.254.1 : octets=32 temps<1ms TTL=128
Réponse de 172.17.254.1 : octets=32 temps=1 ms TTL=128

Statistiques Ping pour 172.17.254.1:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 0ms, Maximum = 1ms, Moyenne = 0ms
```

▪ L’échange démarre avec une requête et une réponse ARP pour obtenir l’adresse MAC du serveur ROI. Ensuite l’échange de trames ICMP a lieu. Arrêtez la capture une fois les 8 trames ICMP obtenues. Sauvegardez la sous le nom « CaptureICMP ».

Si vous ne visualisez pas d’échange ARP, videz le cache ARP (ouvrir une invite de commandes en tant qu’administrateur et saisir la commande arp –d *) puis recommencez une nouvelle capture et ressaisissez la commande ping.

```
C:\Windows\System32>arp -d *

C:\Windows\System32>arp -a

Interface : 172.17.2.2 --- 0xe
  Adresse Internet      Adresse physique      Type
  224.0.0.2             01-00-5e-00-00-02     statique

Interface : 192.168.56.1 --- 0x10
  Adresse Internet      Adresse physique      Type
  224.0.0.22            01-00-5e-00-00-16     statique

Interface : 172.23.48.1 --- 0x12
  Adresse Internet      Adresse physique      Type
```

▪ Après la saisie de la commande ping et la capture des trames ARP/ICMP, arrêtez cette dernière et consultez le contenu du cache ARP : vérifiez la présence de l’association @IP-@MAC correspondant à ROI (capture d’écran à réaliser).



▪ A l’aide du Chapitre 5 (page 2), analysez l’échange de trames ARP (Request et Reply) précédant l’échange de trames ICMP :

Quelle signification ont les octets de position 0×0C et 0×0D ligne 0000 ?

Ici on peut voir que les octets de position 0×0C et 0×0D sont le champ Ethertype et la valeur est 0806 ce qui signifie que c’est le protocole ARP

Quelle est la fonction de la trame ARP Request ?

La trame ARP request sert à demander l'adresse MAC d'une machine dont on connait l'adresse IP.

Quelle signification ont les octets de position 0×04 et 0×05 ligne 0010 ?

Ici les octets de position 0×04 et 0×05 sont la requête.

Quelle est la longueur d'un message ARP contenu dans la trame ?

28 octets

Quelle est la longueur de la trame ARP Request ?

42 octets

Quelle est la longueur de la trame ARP Reply ?

60 octets

Combien d'octets sont utilisés pour le padding ?

18 octets

▪ Complétez les rubriques ci-dessous :

Trame ARP Request
@MAC destination = ff: ff: ff: ff: ff: ff @MAC source = 74: 56: 3c: 2f: 9b: ec Ethernet Type = 0806
Opcode (valeurs hexa.) =00 01 @MAC de la cible = 00 : 00 : 00 : 00 : 00 : 00 @IP de la cible =172.17.254.1

▪ Sélectionnez une trame ICMP Echo Request. A l'aide du Chapitre 5 (pages 4 et 5), répondez aux questions suivantes :

Quelle signification ont les octets de position 0×0C et 0×0D ligne 0000 ?

Les octets de position 0×0C et 0×0D sont 08 00 ce qui veut dire que c’est le protocole IPv4.

Quelle signification a l’octet de position 0×07 ligne 0010 ?

L’octet de position 0x07 est 01 ce qui veut dire que c’est le protocole ICMP.

Quelle est la longueur de la trame ?

74 octets

Quelle est la longueur du paquet IP ?

20 octets

Quelle est la longueur du message ICMP ?

40 octets

Quelle signification a l’octet de position 0×02 ligne 00020 ?

L’octet de position 0×02 est ici 08 qui est le Type de ICMP qui correspond ici au ping request.

A quoi correspondent les octets à partir de l’octet 0×0A, ligne 00020 ?

Les octets à partir de l’octet 0×0A sont les Data.

▪ Sélectionnez une trame ICMP Echo Reply. Quelle est le nom et la valeur de l’octet de position 0×02 ligne 00020 ?

L’octet de position 0×02 est 00 qui est également le Type de ICMP qui est ici le ping reply.

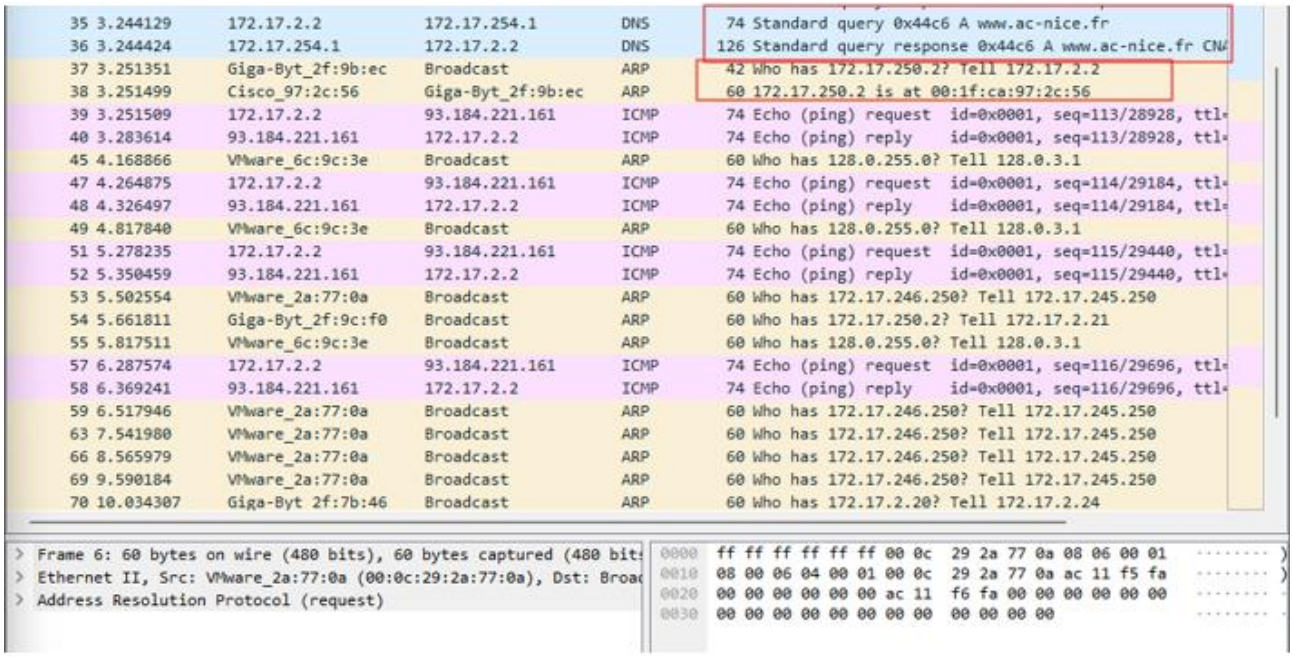
4.2. Capture de trames ARP, DNS et ICMP

▪ Démarrez une capture de trames depuis votre machine physique.

▪ Ouvrez une invite de commandes, videz le cache ARP (commande arp -d *) puis effectuez une requête ping vers le serveur web www.ac-nice.fr (ping « nom » et non plus ping « @IP ») :

```
C:\Windows\System32>ping www.ac-nice.fr

Envoi d'une requête 'ping' sur cs234.wpc.alphacdn.net [93.184.221.161] avec 32 octets de données :
Réponse de 93.184.221.161 : octets=32 temps=32 ms TTL=56
Réponse de 93.184.221.161 : octets=32 temps=32 ms TTL=56
Réponse de 93.184.221.161 : octets=32 temps=67 ms TTL=56
Réponse de 93.184.221.161 : octets=32 temps=32 ms TTL=56

Statistiques Ping pour 93.184.221.161:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 32ms, Maximum = 67ms, Moyenne = 40ms
```

▪ Arrêtez la capture et sauvegardez la sous le nom « CaptureIcmpDns »



▪ La liste des trames commence par une requête et une réponse ARP. Quelle est l'adresse MAC recherchée ?

Ici c'est celle de www.ac-nice.fr.

▪ Complétez les rubriques ci-dessous :

Trame ARP request
@MAC destination = ff : ff : ff : ff : ff : ff @MAC source = 74: 56: 3c: 2f: 9b: ec

Ethernet Type = 0806
Opcode (valeurs hexa.) = 00 01 @MAC de la cible = 00 : 00 : 00 : 00 : 00 : 00 @IP de la cible = 172.17.254.1

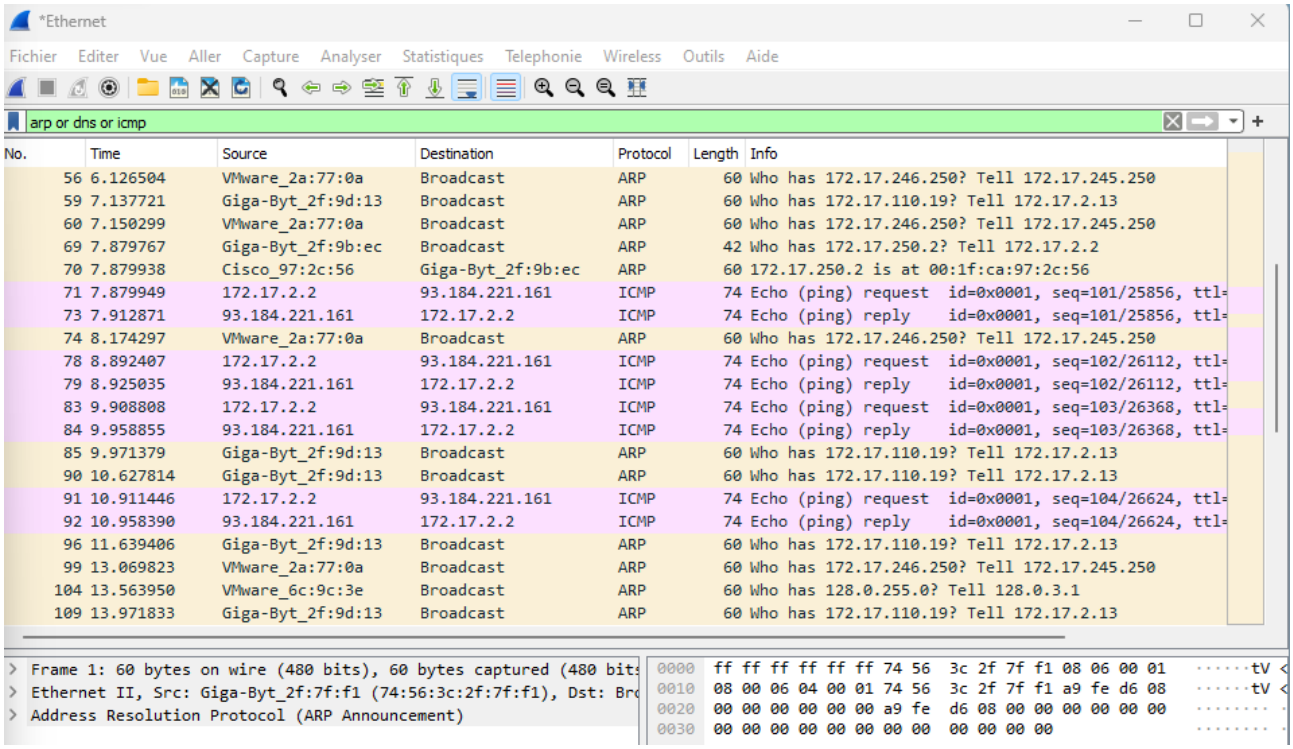
▪ Pour quelle raison trouve-t-on ensuite une requête DNS avant l'échange de trames ICMP suite à l'exécution de la commande ping proprement dite ?

C'est pour pouvoir connaître l'adresse IP de www.ac-nice.fr.

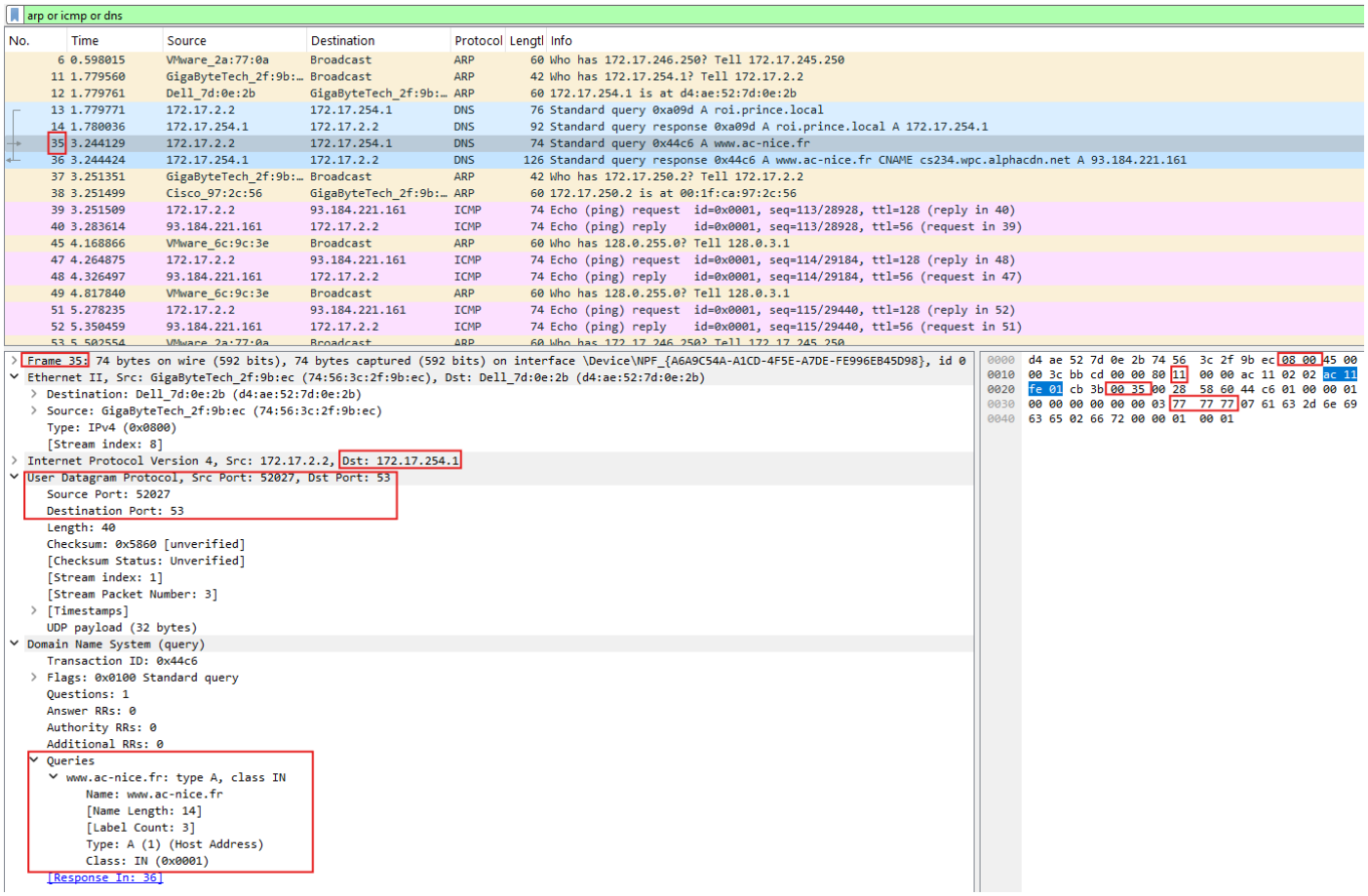
▪ Consultez le cache DNS à l'aide de la commande ipconfig /displaydns et vérifiez la présence de l'enregistrement DNS ac-nice.fr et de l'adresse IP associée :

```
www.ac-nice.fr
----------------------------------------
Nom d'enregistrement. : www.ac-nice.fr
Type d'enregistrement : 5
Durée de vie  . . . . : 2830
Longueur de données . : 8
Section . . . . . . . : Réponse
Enregistrement CNAME  : cs234.wpc.alphacdn.net


Nom d'enregistrement. : cs234.wpc.alphacdn.net
Type d'enregistrement : 1
Durée de vie  . . . . : 2830
Longueur de données . : 4
Section . . . . . . . : Réponse
Enregistrement (hôte) : 93.184.221.161
```

▪ Démarrez une nouvelle capture et ressaisissez la commande ping www.ac-nice.fr dans l'invite de commandes. Vous ne devriez pas constater de requête DNS puisque l'enregistrement est présent dans le cache DNS.



▪ Videz le cache DNS à l'aide de la commande ipconfig /flushdns et redémarrez une nouvelle capture afin de visualiser de nouveau une requête DNS (capture d'écran à faire) :



▪ Quels sont les différents protocoles encapsulés dans une trame DNS ?

Ici ce sont les protocoles IPv4 et UDP.

▪ Quelle est la machine destinataire de la requête DNS ? Quelle est son IP (en-tête IP) ?

La machine destinataire de la requête DNS sera le serveur ROI qui a comme IP 172.17.254.1

▪ Quelle signification ont les octets de position 0×0C, 0×0D ligne 0000 et 0×07 ligne 0010 ?

Les octets de position 0×0C et 0×0D appartiennent au champ Ethertype qui sont 08 00 ce qui veut dire que nous sommes sous IPv4 et l'octet 0×07 qui appartient au champ réseau et qui est 11 ce qui veut dire que nous sommes sous UDP.

▪ Quelle signification ont les octets de position 0×04 et 0×05 ligne 0020 ?

Les octets de position 0×04 et 0×05 sont 00 35 qui sont le port de destination. Ce qui correspond au port 53.

▪ Développez la section Domain Name System (query) et plus précisément la rubrique Queries. Quels sont les valeurs hexadécimales des octets correspondant au nom de domaine internet acnice.fr ?

Les valeurs hexadécimales des octets correspondant au nom de domaine internet acnice.fr sont 07 61 63 2d 6e 69 63 65 02 66 72 00.

▪ Sélectionnez la trame comportant la réponse à la requête DNS et développez la section Domain Name System (response) et plus particulièrement la rubrique Answers. Recherchez les valeurs hexadécimales et décimales de l'adresse IP du serveur web hébergeant le site de l'académie de Nice.

Les valeurs hexa sont c0 2c 00 01 00 01 00 00 09 be 00 01 5d b8 dd a1.

Et l'adresse IP est 93.184.221.161

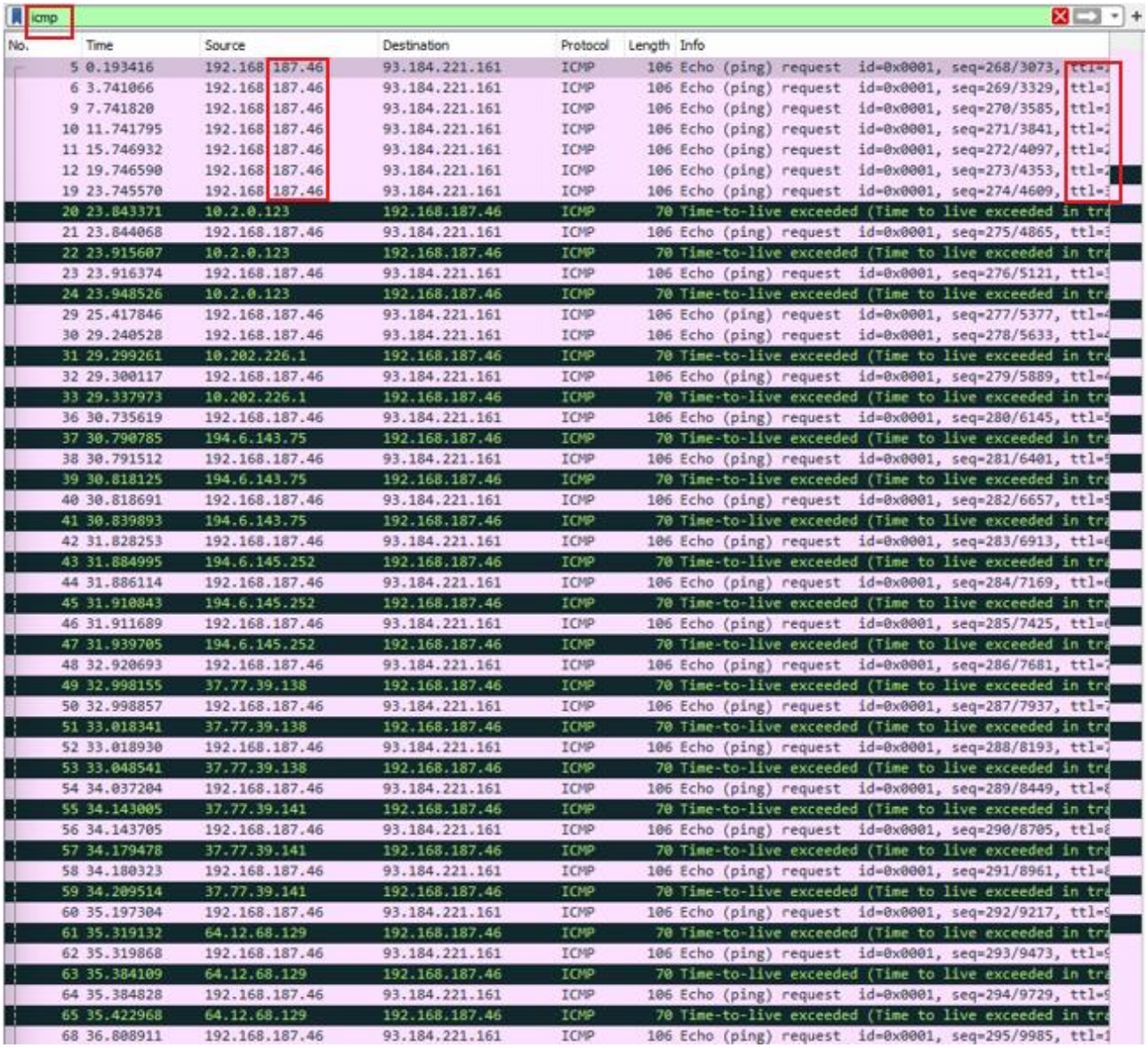
4.3. Commande Tracert et capture de trames ICMP.

▪ Démarrez une capture de trames depuis votre machine physique.

▪ Ouvrez une invite de commandes et saisissez la commande tracert www.ac-nice.fr.

▪ Une fois l'itinéraire déterminé, arrêtez la capture et sauvegardez la sous le nom « CaptureTracert ».

▪ Limitez l'affichage des trames à celles encapsulant le protocole ICMP (zone Filter) :



▪ Sélectionnez la première trame ICMP Echo request. Développez l’en-tête IP. Quelle est l’adresse IP Destination (valeurs déci. et hexa.) ?

L’adresse IP destination en décimale est 93.184.221.161 et en hexadécimale c’est 5d b8 dd a1.

▪ Sélectionnez le champ TTL. Quelle est la valeur portée par ce champ (valeurs déci. et hexa.) ?

La valeur déci du champ TTL est 1 et en hexa c’est 01.

▪ Développez la section correspondant au message ICMP. Quelle est la valeur portée par le champ Type (valeurs déci. et hexa.) ?

La valeur du champ Type en déci. est 8 et en hexa sa valeur est 08.

▪ Sélectionnez la trame, comportant un message d’erreur ICMP Time-to-live exceeded, envoyée par le premier routeur rencontré. Développez la section correspondant au message ICMP. Quelle est la valeur portée par le champ Type (valeurs déci. et hexa.) ?

La valeur du champ Type est 11 en déci et 0b en hexa.