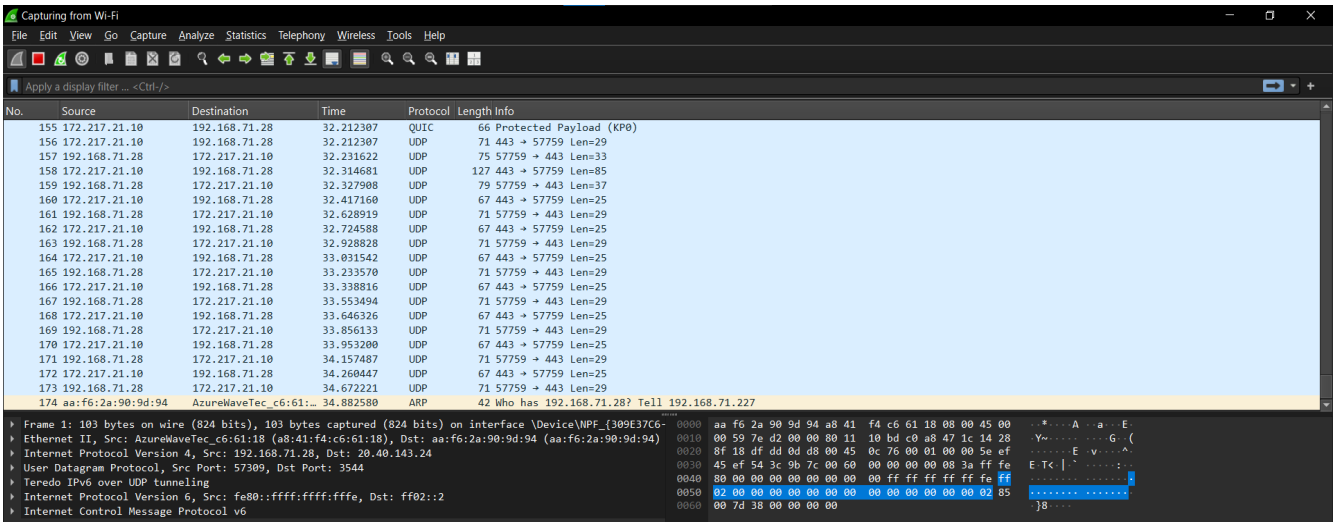
TP 5 – Trames ARP, ICMP et DNS

Sommaire

1. Capture de trames ARP et ICMP

→ On ouvre WireShark et on démarre une **capture de trame** :

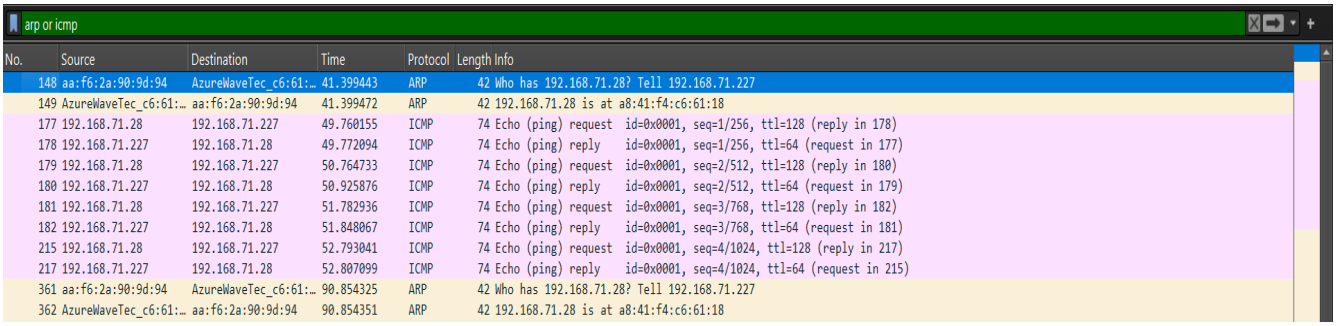


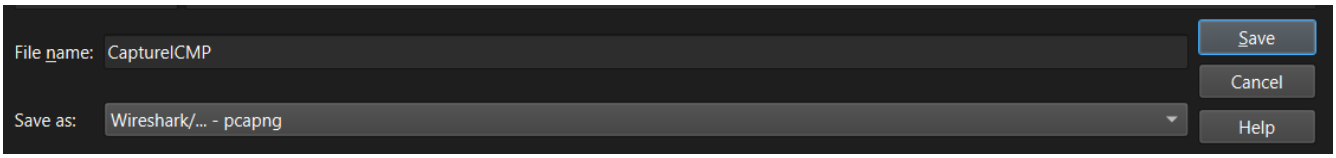
→ On **ping** le serveur :

```
C:\Users\Noah>ping 192.168.71.227

Pinging 192.168.71.227 with 32 bytes of data:
Reply from 192.168.71.227: bytes=32 time=12ms TTL=64
Reply from 192.168.71.227: bytes=32 time=161ms TTL=64
Reply from 192.168.71.227: bytes=32 time=65ms TTL=64
Reply from 192.168.71.227: bytes=32 time=14ms TTL=64

Ping statistics for 192.168.71.227:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 12ms, Maximum = 161ms, Average = 63ms
```

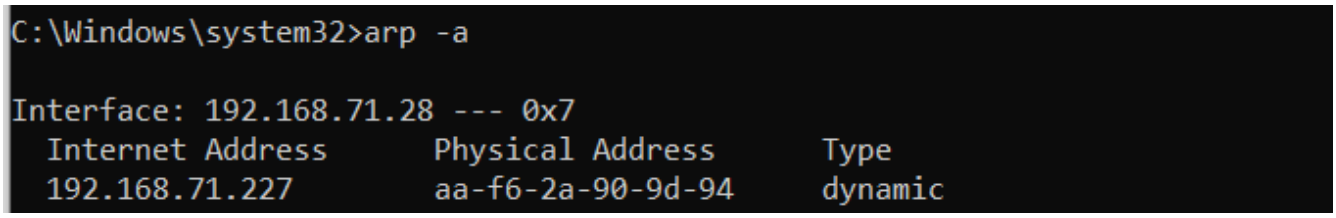
3

→ On applique un **filtre arp / icmp** et on sauvegarde les trames obtenues sous le nom **“CaptureICMP”** :

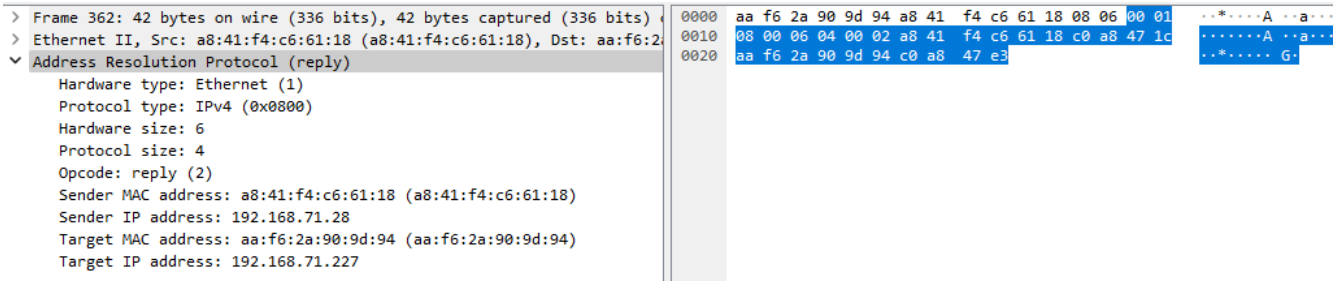




→ On arrête la capture de trames et on visualise le **cache ARP** avec la commande **arp -a** :



→ On analyse l’échange de **trames ARP** :



***** Les octets de position **0×0C** et **0×0D ligne 0000** sont le champ **Ethertype** qui représente ici **ARP (0806)**.

***** La fonction de la trame ARP Request est de demander quelle est **l’adresse MAC** d’une certaine adresse IP.

4

* Les octets de position **0×04** et **0×05 ligne 0010** indiquent si la requête est une **request (00 01)** ou une **reply(00 02)**.

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

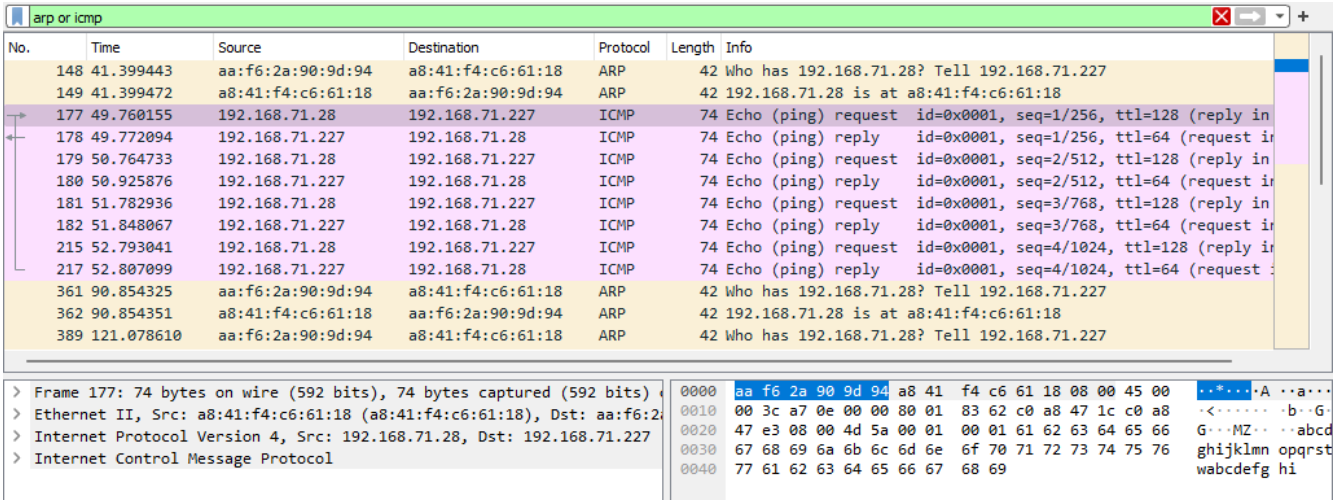
* La longueur de la trame ARP Request est de **48 octets**.

* La longueur de la trame ARP Reply est de **42 octets**.

* Il n'y a **aucuns** octets utilisés pour le padding.

Trame ARP request
@MAC destination = **AA:F6:2A:90:9D:94** @MAC source = **A8:41:F4:C6:61:18** Ethernet Type = **08 06**
Opcode (valeurs hexa.) = **00 01** @MAC de la cible = **00:00:00:00:00** @IP de la cible = **192.168.71.28**

→ On séléctionne une trame **ICMP Echo Request** :



5

* Les octets de position **0×0C** et **0×0D ligne 0000** signifient que l'**en-tête Ethernet** transporte un paquet **IPv4**.

* L'octet de position **0×07 ligne 0010** signifie que l'**en-tête IP** transporte le **protocole ICMP**.

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

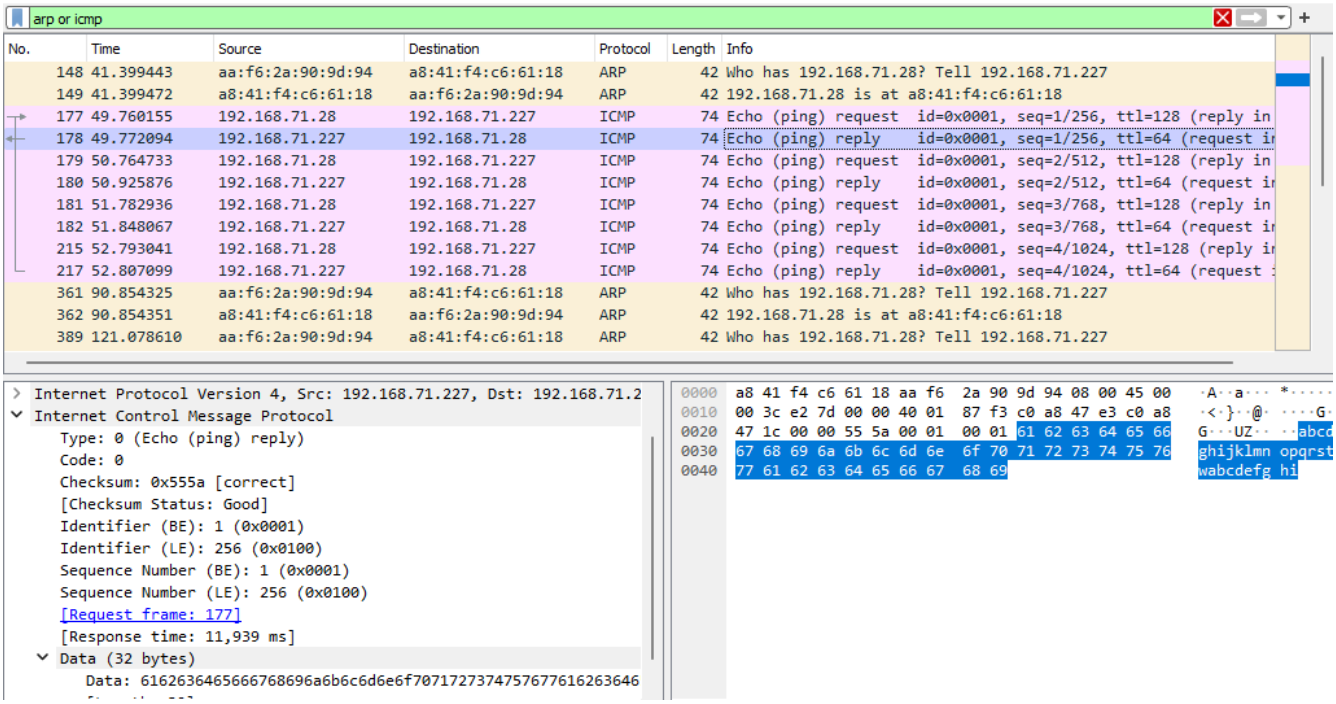
* La longueur du paquet IP est de **20 octets**.

* La longueur du message ICMP est de **40 octets**.

* L'octet de position **0×02 ligne 00020** signifie que le protocole ICMP transporte un message de type **echo ping request**.

* Les octets à partir de l'octet **0×0A**, **ligne 00020** sont les **données transportées**.

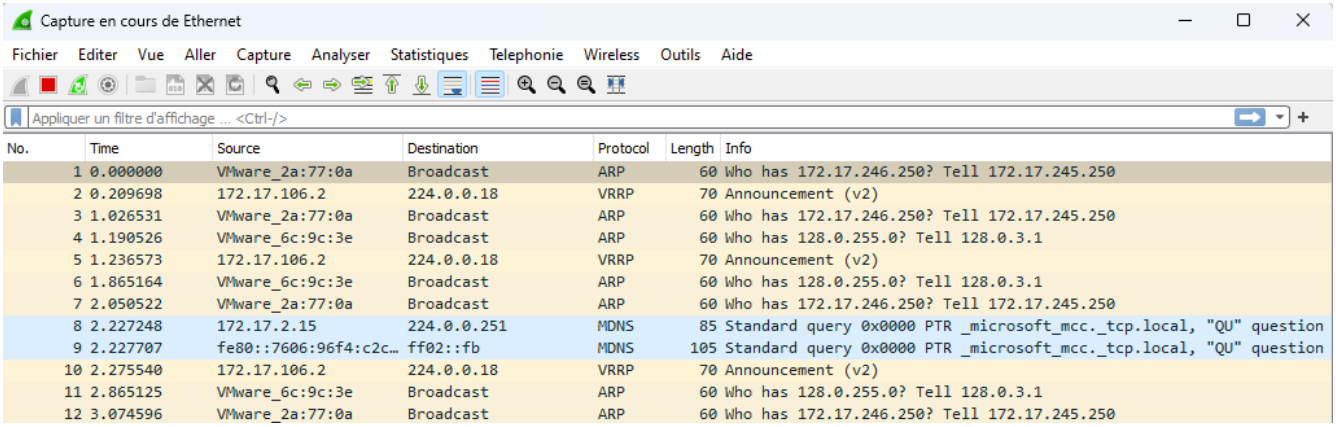
→ On sélectionne une trame **ICMP Echo Reply** :



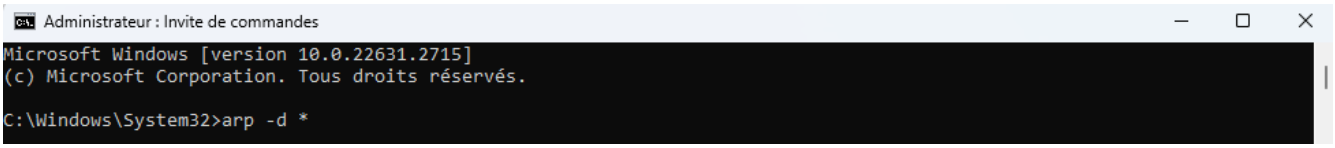
* L'octet de position **0×02 ligne 00020** renseigne le **type de message** transporté par le protocole ICMP, il vaut ici **00** qui correspond à un message **echo ping reply**.

1.2. Capture de trames ARP, DNS et ICMP

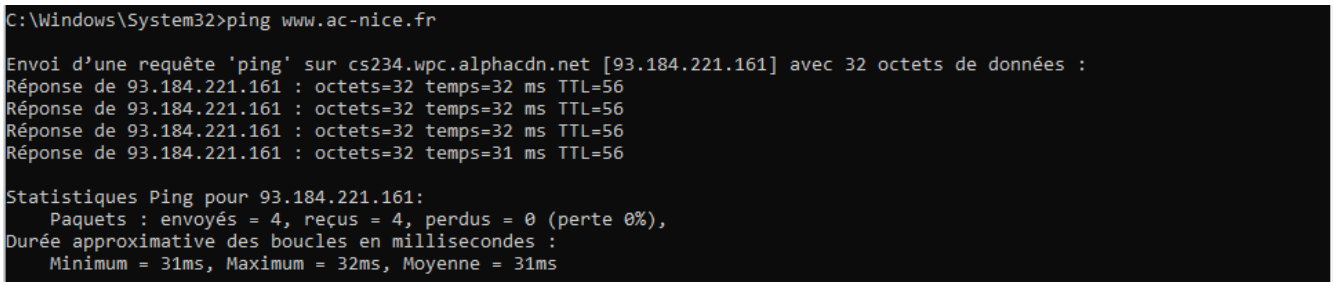
→ On démarre une nouvelle **capture de trames** Wireshark depuis la machine physique :



→ On vide le **cache ARP** avec la commande **arp -d *** en ouvrant l'invite de commande en tant qu'**administrateur** :

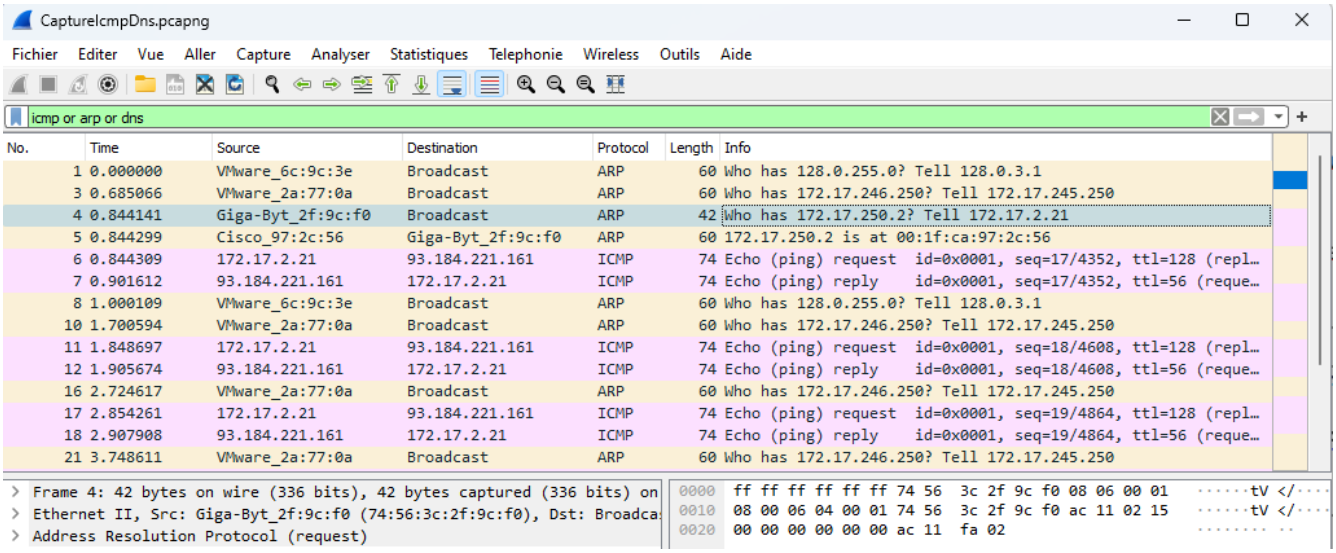


→ On **ping** le serveur web **www.ac-nice.fr** :



7

→ On arrête la capture et on la **sauvegarde** sous le nom “CaptureIcmpDns” :



***** L’adresse MAC recherchée est celle de l’adresse IP **172.17.250.2**.

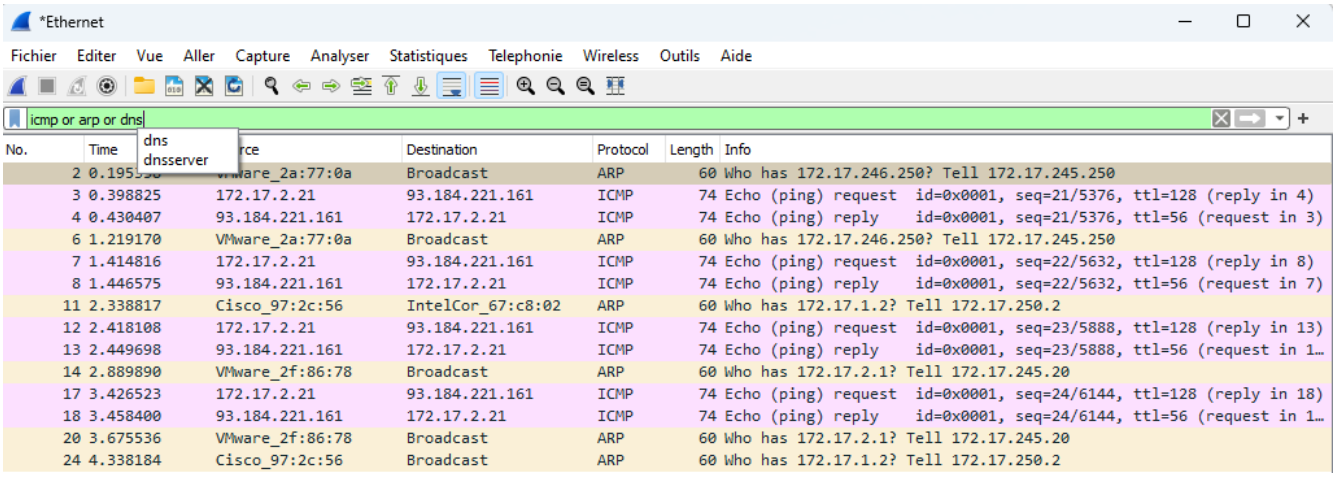
Trame ARP request
@MAC destination = **FF:FF:FF:FF:FF:FF** @MAC source = **74:56:3C:2F:9C:F0** Ethernet Type = **08 06**
Opcode (valeurs hexa.) = **00 01** @MAC de la cible = **00:00:00:00:00:00** @IP de la cible = **172.17.250.2**

***** On trouve une requête DNS avant l’échange de trames ICMP suite à l’exécution de la commande ping car le serveur ROI demande d’abord quelle est **l’adresse IP** du nom de domaine pour pouvoir envoyer le ping à cette adresse.

→ On consulte le **cache DNS** avec la commande **ipconfig /displaydns** et on vérifie que le nom de domaine **ac-nice.fr** est bien enregistré :

```
www.ac-nice.fr
----------------------------------------
Nom d'enregistrement. : www.ac-nice.fr
Type d'enregistrement : 5
Durée de vie  . . . . : 2023
Longueur de données . : 8
Section . . . . . . . : Réponse
Enregistrement CNAME  : cs234.wpc.alphacdn.net
```

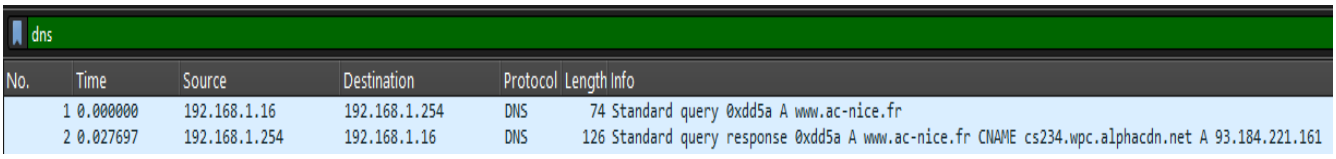
→ On démarre une capture de trame et on **ping** à nouveau le serveur web **www.ac-nice.fr :**



***** On n'observe aucune **requête DNS** car ce nom de domaine est déjà enregistré dans le **cache DNS**.

→ On vide le **cache DNS** avec la commande **ipconfig /flushdns** et on redémarre une capture pour observer une **requête DNS** :

```
C:\Windows\system32>ipconfig /flushdns

Windows IP Configuration

Successfully flushed the DNS Resolver Cache.
```



9

* Les **différents protocoles** encapsulés dans une trame DNS sont :

- Le protocole **Ethernet**
- Le protocole **IP**
- Le protocole **UDP**
- Le protocole **DNS**

* Le destinataire de la requête DNS est le **serveur DNS** de la box. Son IP est **192.168.1.254**.

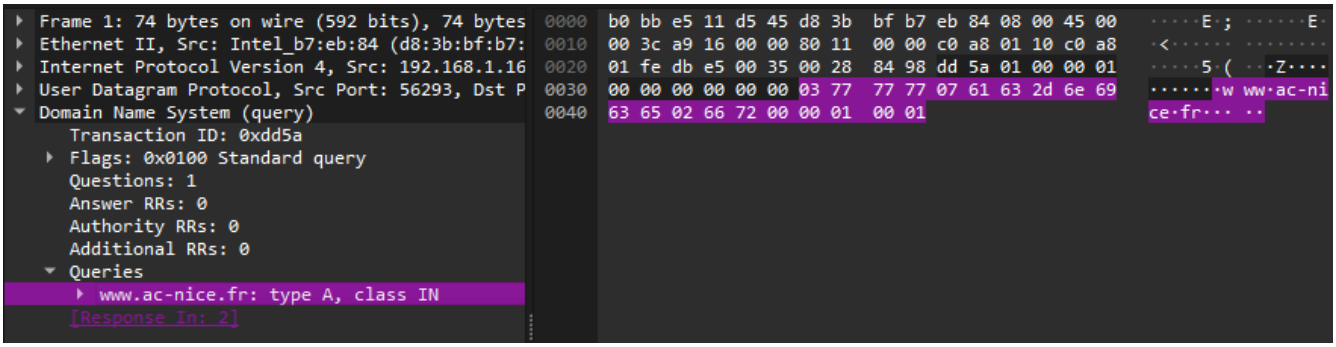
```
   DNS Servers . . . . . . . . . . . . : 192.168.1.254
```

* Les octets de position **0×0C**, **0×0D ligne 0000** signifient que l'**en-tête Ethernet** transporte un **paquet IPv4.**

* L'octet de position **0×07 ligne 0010** signifie que l'**en-tête IP** transporte un **datagramme UDP**.

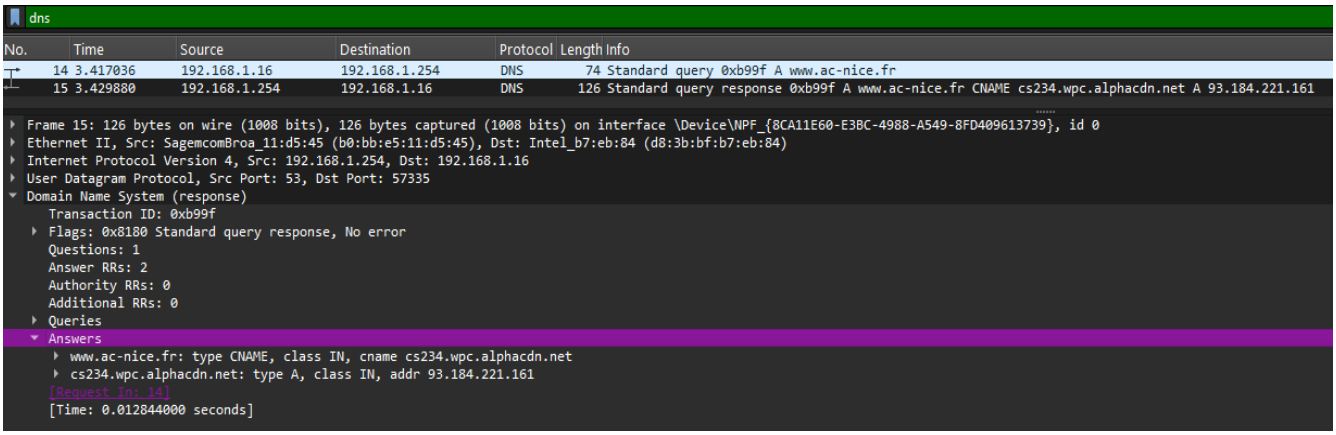
* Les octets de position **0×04** et **0×05 ligne 0020** signifient que le **port de destination** est **53**.

→ On développe la section **Domain Name System (query)** et plus précisément la rubrique **Queries** :



* Les valeurs hexadécimales des octets correspondant au nom de domaine internet ac nice.fr sont **03 77 77 77 07 61 63 2d 6e 69 63 65 02 66 72 00 00 01 00 01**.

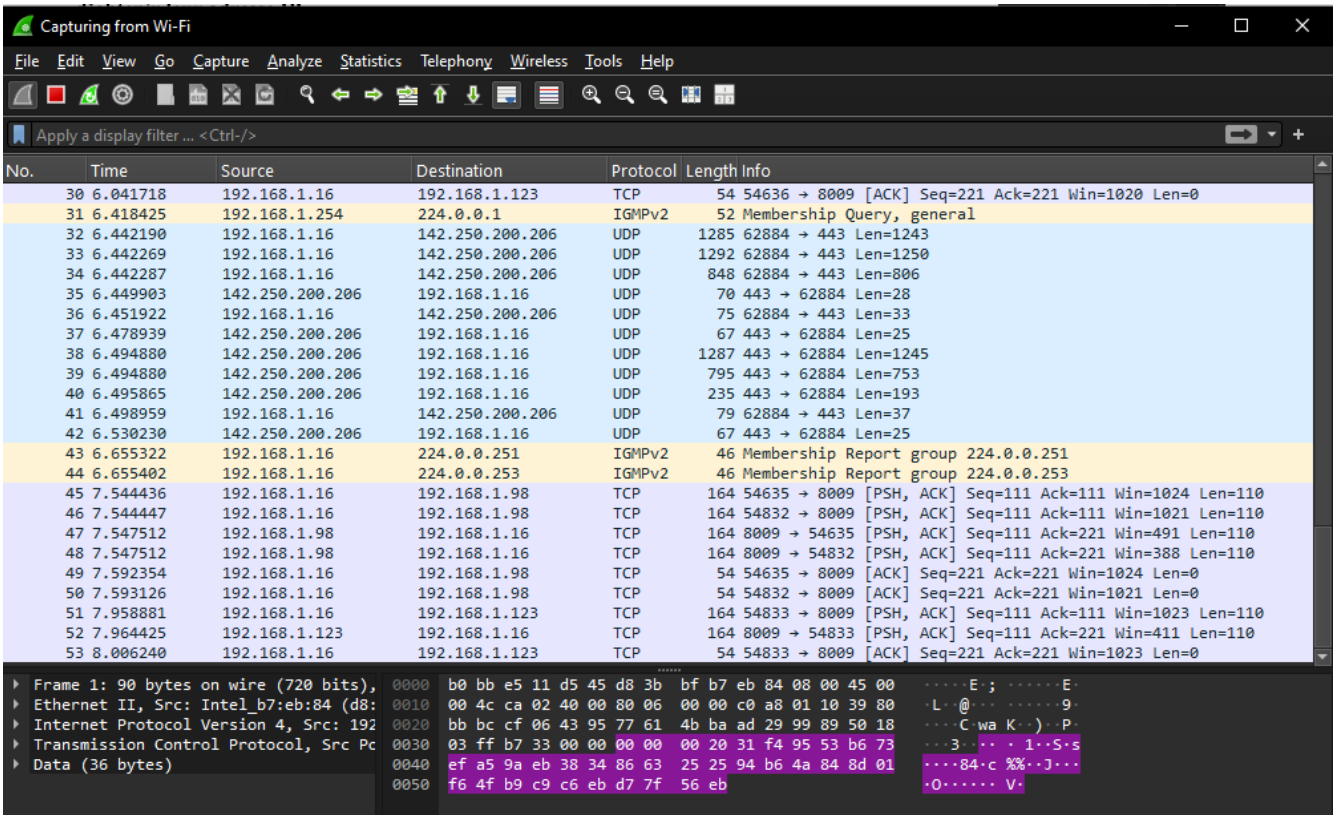
→ On sélectionne la trame comportant la réponse à la **requête DNS** et on développe la section **Domain Name System (response)**, plus particulièrement la rubrique **Answers** :



***** Les valeurs hexadécimales et décimales de l'adresse IP du serveur web hébergeant le site de l'académie de Nice sont : **5D:B8:DD:A1 / 93.184.221.161**.

2. Commande Tracert et capture de trames ICMP

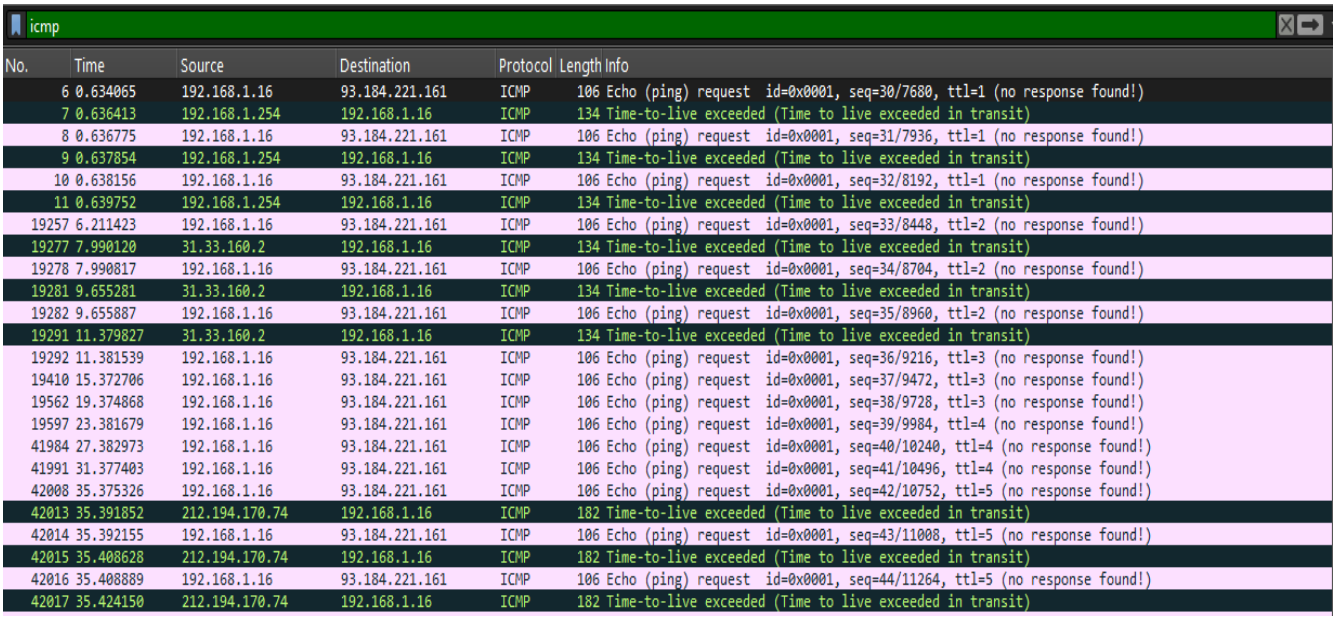
→ On démarre une nouvelle **capture de trame** Wireshark sur la machine physique :



→ On tape la commande **tracert www.ac-nice.fr** dans l'invite de commande :

```
C:\Windows\system32>tracert www.ac-nice.fr

Tracing route to cs234.wpc.alphacdn.net [93.184.221.161]
over a maximum of 30 hops:

  1     2 ms     1 ms     1 ms  bbox.lan [192.168.1.254]
  2  1778 ms  1664 ms  1724 ms  31-33-160-2.abo.bbox.fr [31.33.160.2]
  3     *        *        *     Request timed out.
  4     *        *        *     Request timed out.
  5    16 ms    16 ms    15 ms  be21.cbr01-poi.net.bbox.fr [212.194.170.74]
  6    17 ms    15 ms    15 ms  212.194.171.9
  7    15 ms    16 ms    15 ms  be5.cbr01-cro.net.bbox.fr [212.194.171.141]
  8     *        *       16 ms  62.34.2.88
  9    16 ms    16 ms    16 ms  ae-130.border1.pam.edgecastcdn.net [152.195.108.200]
 10    21 ms    16 ms    17 ms  ae-65.core1.paa.edgecastcdn.net [152.195.108.129]
 11    16 ms    15 ms    15 ms  93.184.221.161

Trace complete.
```

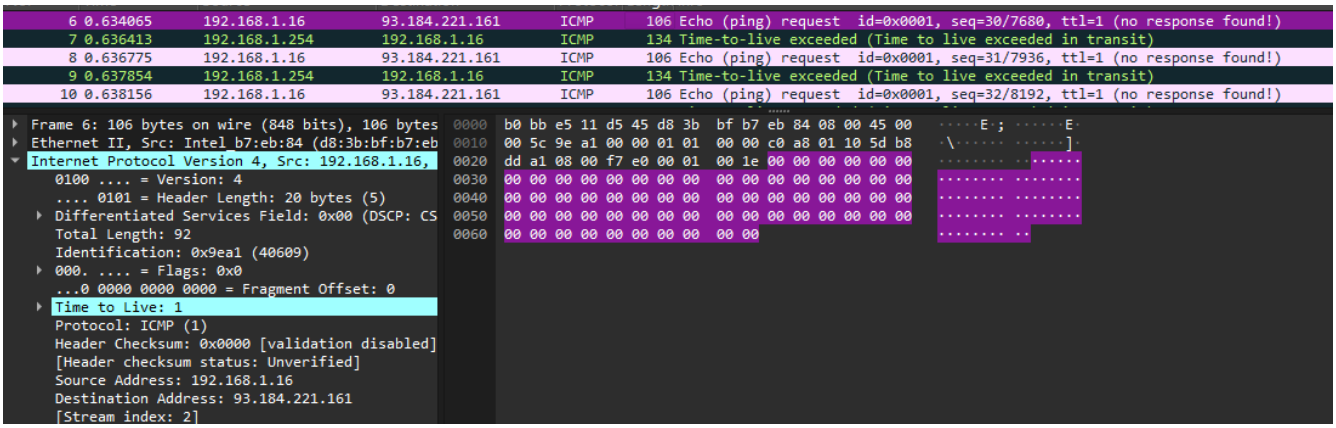
→ On arrête la capture et la **sauvegarde** sous le nom de “CaptureTracert” puis on applique un **filtre ICMP** :



icmp

No.	Time	Source	Destination	Protocol	Length	Info
6	0.634065	192.168.1.16	93.184.221.161	ICMP	106	Echo (ping) request id=0x0001, seq=30/7680, ttl=1 (no response found!)
7	0.636413	192.168.1.254	192.168.1.16	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
8	0.636775	192.168.1.16	93.184.221.161	ICMP	106	Echo (ping) request id=0x0001, seq=31/7936, ttl=1 (no response found!)
9	0.637854	192.168.1.254	192.168.1.16	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
10	0.638156	192.168.1.16	93.184.221.161	ICMP	106	Echo (ping) request id=0x0001, seq=32/8192, ttl=1 (no response found!)
11	0.639752	192.168.1.254	192.168.1.16	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
19257	6.211423	192.168.1.16	93.184.221.161	ICMP	106	Echo (ping) request id=0x0001, seq=33/8448, ttl=2 (no response found!)
19277	7.990120	31.33.160.2	192.168.1.16	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
19278	7.990817	192.168.1.16	93.184.221.161	ICMP	106	Echo (ping) request id=0x0001, seq=34/8704, ttl=2 (no response found!)
19281	9.655281	31.33.160.2	192.168.1.16	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
19282	9.655887	192.168.1.16	93.184.221.161	ICMP	106	Echo (ping) request id=0x0001, seq=35/8960, ttl=2 (no response found!)
19291	11.379827	31.33.160.2	192.168.1.16	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
19292	11.381539	192.168.1.16	93.184.221.161	ICMP	106	Echo (ping) request id=0x0001, seq=36/9216, ttl=3 (no response found!)
19410	15.372706	192.168.1.16	93.184.221.161	ICMP	106	Echo (ping) request id=0x0001, seq=37/9472, ttl=3 (no response found!)
19562	19.374868	192.168.1.16	93.184.221.161	ICMP	106	Echo (ping) request id=0x0001, seq=38/9728, ttl=3 (no response found!)
19597	23.381679	192.168.1.16	93.184.221.161	ICMP	106	Echo (ping) request id=0x0001, seq=39/9984, ttl=4 (no response found!)
41984	27.382973	192.168.1.16	93.184.221.161	ICMP	106	Echo (ping) request id=0x0001, seq=40/10240, ttl=4 (no response found!)
41991	31.377403	192.168.1.16	93.184.221.161	ICMP	106	Echo (ping) request id=0x0001, seq=41/10496, ttl=4 (no response found!)
42008	35.375326	192.168.1.16	93.184.221.161	ICMP	106	Echo (ping) request id=0x0001, seq=42/10752, ttl=5 (no response found!)
42013	35.391852	212.194.170.74	192.168.1.16	ICMP	182	Time-to-live exceeded (Time to live exceeded in transit)
42014	35.392155	192.168.1.16	93.184.221.161	ICMP	106	Echo (ping) request id=0x0001, seq=43/11008, ttl=5 (no response found!)
42015	35.408628	212.194.170.74	192.168.1.16	ICMP	182	Time-to-live exceeded (Time to live exceeded in transit)
42016	35.408889	192.168.1.16	93.184.221.161	ICMP	106	Echo (ping) request id=0x0001, seq=44/11264, ttl=5 (no response found!)
42017	35.424150	212.194.170.74	192.168.1.16	ICMP	182	Time-to-live exceeded (Time to live exceeded in transit)

→ On développe **l’en-tête IP** de la première trame **ICMP Echo request** :



```
    6 0.634065   192.168.1.16     93.184.221.161   ICMP   106 Echo (ping) request  id=0x0001, seq=30/7680, ttl=1 (no response found!)
    7 0.636413   192.168.1.254    192.168.1.16     ICMP   134 Time-to-live exceeded (Time to live exceeded in transit)
    8 0.636775   192.168.1.16     93.184.221.161   ICMP   106 Echo (ping) request  id=0x0001, seq=31/7936, ttl=1 (no response found!)
    9 0.637854   192.168.1.254    192.168.1.16     ICMP   134 Time-to-live exceeded (Time to live exceeded in transit)
   10 0.638156   192.168.1.16     93.184.221.161   ICMP   106 Echo (ping) request  id=0x0001, seq=32/8192, ttl=1 (no response found!)

▸ Frame 6: 106 bytes on wire (848 bits), 106 bytes
▸ Ethernet II, Src: Intel_b7:eb:84 (d8:3b:bf:b7:eb
▾ Internet Protocol Version 4, Src: 192.168.1.16,
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▸ Differentiated Services Field: 0x00 (DSCP: CS
    Total Length: 92
    Identification: 0x9ea1 (40609)
  ▸ 000. .... = Flags: 0x0
    ...0 0000 0000 0000 = Fragment Offset: 0
  ▸ Time to Live: 1
    Protocol: ICMP (1)
    Header Checksum: 0x0000 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.1.16
    Destination Address: 93.184.221.161
    [Stream index: 2]

0000  b0 bb e5 11 d5 45 d8 3b  bf b7 eb 84 08 00 45 00   .....E; ......E
0010  00 5c 9e a1 00 00 01 01  00 00 c0 a8 01 10 5d b8   .\...... ......]
0020  dd a1 08 00 f7 e0 00 01  00 1e 00 00 00 00 00 00   ........ ........
0030  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0040  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0050  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0060  00 00 00 00 00 00 00 00  00 00                     ........ ..
```

***** L’adresse IP destination est **93.184.221.161 / 5d b8 dd a1**.

***** La valeur portée par le champ TTL est **1 / 01**.

***** La valeur portée par le champ Type dans la section message ICMP est **8 / 08**.

***** La valeur portée par le champ Type dans la section message ICMP de le première trame comportant le message d’erreur ICMP Time-to-live exceeded est aussi **8 / 08**.