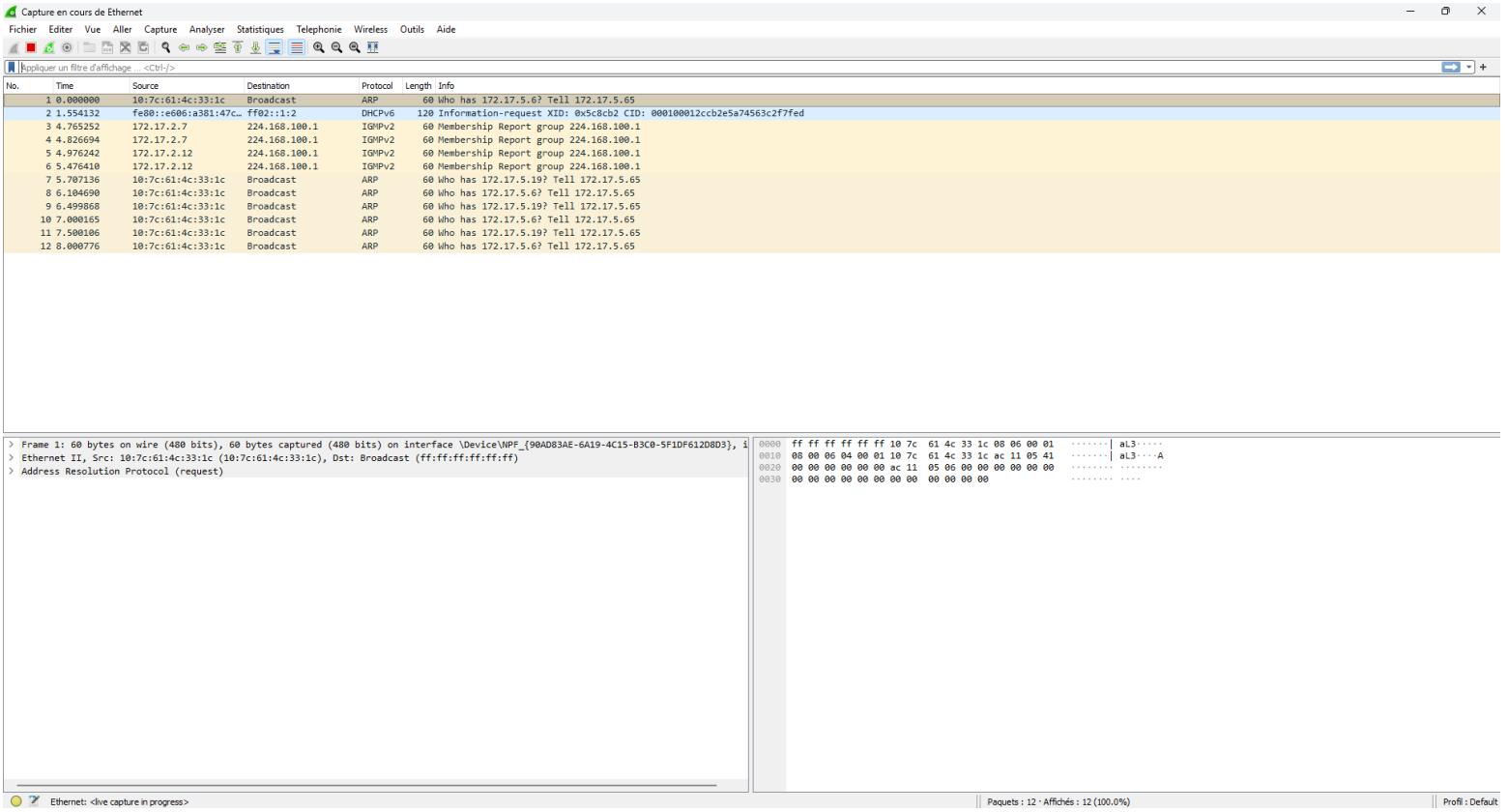
TP 5 – Trames ARP, ICMP et DNS

Sommaire

Captures de Trames ARP et ICMP :

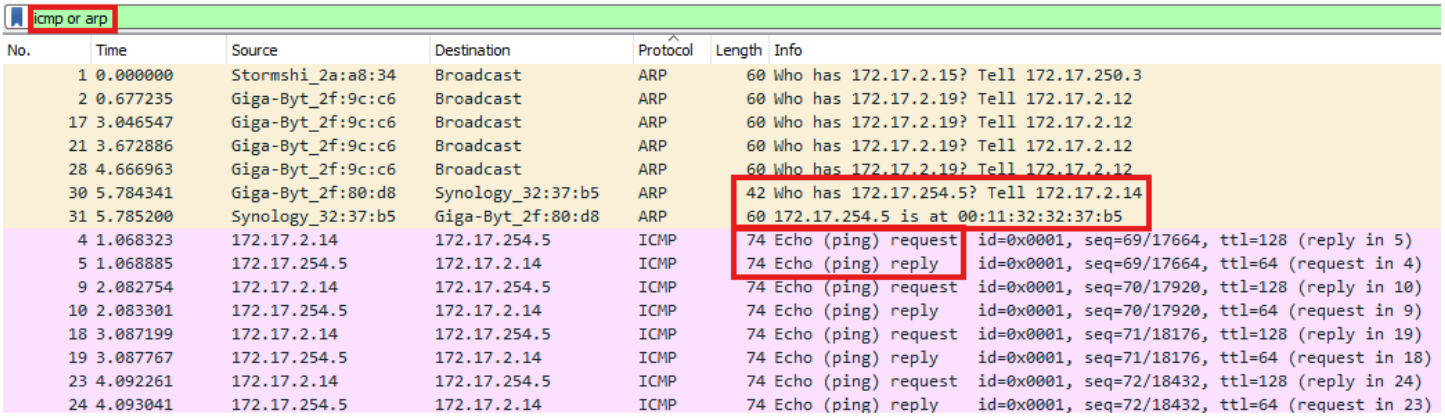
Ouverture de wireshark et lancement d’une capture de Trames :



Ping du serveur du serveur Aviateur (172.17.254.5) :

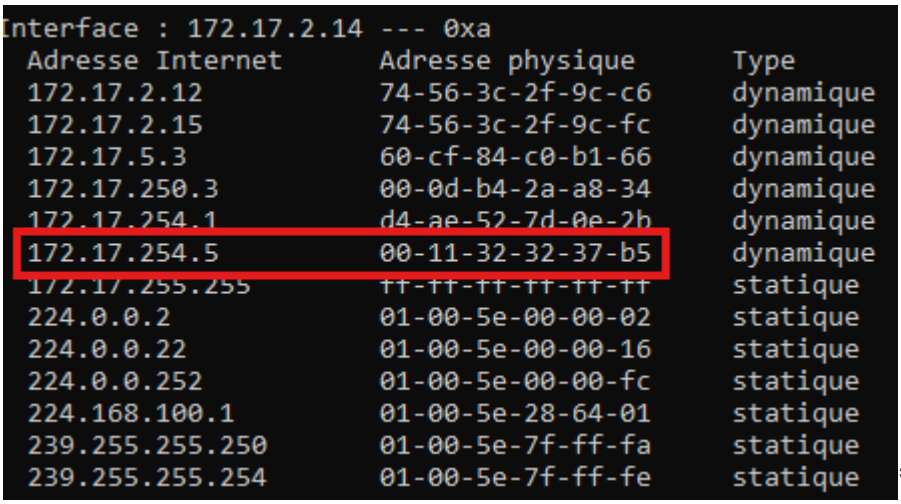
```
Microsoft Windows [version 10.0.26100.6584]
(c) Microsoft Corporation. Tous droits réservés.

C:\Users\mballester>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<1ms TTL=64
Réponse de 172.17.254.5 : octets=32 temps<1ms TTL=64
Réponse de 172.17.254.5 : octets=32 temps<1ms TTL=64
Réponse de 172.17.254.5 : octets=32 temps<1ms 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 = 0ms, Maximum = 0ms, Moyenne = 0ms

C:\Users\mballester>
```

Echange ARP et ICMP suite au ping de aviateur :



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	Stormshi_2a:a8:34	Broadcast	ARP	60	Who has 172.17.2.15? Tell 172.17.250.3
2	0.677235	Giga-Byt_2f:9c:c6	Broadcast	ARP	60	Who has 172.17.2.19? Tell 172.17.2.12
17	3.046547	Giga-Byt_2f:9c:c6	Broadcast	ARP	60	Who has 172.17.2.19? Tell 172.17.2.12
21	3.672886	Giga-Byt_2f:9c:c6	Broadcast	ARP	60	Who has 172.17.2.19? Tell 172.17.2.12
28	4.666963	Giga-Byt_2f:9c:c6	Broadcast	ARP	60	Who has 172.17.2.19? Tell 172.17.2.12
30	5.784341	Giga-Byt_2f:80:d8	Synology_32:37:b5	ARP	42	Who has 172.17.254.5? Tell 172.17.2.14
31	5.785200	Synology_32:37:b5	Giga-Byt_2f:80:d8	ARP	60	172.17.254.5 is at 00:11:32:32:37:b5
4	1.068323	172.17.2.14	172.17.254.5	ICMP	74	Echo (ping) request id=0x0001, seq=69/17664, ttl=128 (reply in 5)
5	1.068885	172.17.254.5	172.17.2.14	ICMP	74	Echo (ping) reply id=0x0001, seq=69/17664, ttl=64 (request in 4)
9	2.082754	172.17.2.14	172.17.254.5	ICMP	74	Echo (ping) request id=0x0001, seq=70/17920, ttl=128 (reply in 10)
10	2.083301	172.17.254.5	172.17.2.14	ICMP	74	Echo (ping) reply id=0x0001, seq=70/17920, ttl=64 (request in 9)
18	3.087199	172.17.2.14	172.17.254.5	ICMP	74	Echo (ping) request id=0x0001, seq=71/18176, ttl=128 (reply in 19)
19	3.087767	172.17.254.5	172.17.2.14	ICMP	74	Echo (ping) reply id=0x0001, seq=71/18176, ttl=64 (request in 18)
23	4.092261	172.17.2.14	172.17.254.5	ICMP	74	Echo (ping) request id=0x0001, seq=72/18432, ttl=128 (reply in 24)
24	4.093041	172.17.254.5	172.17.2.14	ICMP	74	Echo (ping) reply id=0x0001, seq=72/18432, ttl=64 (request in 23)

Contenu de cache ARP pour vérifiez la présence de l'association @IP-@MAC correspondant à Aviateur :



```
Interface : 172.17.2.14 --- 0xa
  Adresse Internet      Adresse physique      Type
  172.17.2.12           74-56-3c-2f-9c-c6     dynamique
  172.17.2.15           74-56-3c-2f-9c-fc     dynamique
  172.17.5.3            60-cf-84-c0-b1-66     dynamique
  172.17.250.3          00-0d-b4-2a-a8-34     dynamique
  172.17.254.1          d4-ae-52-7d-0e-2b     dynamique
  172.17.254.5          00-11-32-32-37-b5     dynamique
  172.17.255.255        ff-ff-ff-ff-ff-ff     statique
  224.0.0.2             01-00-5e-00-00-02     statique
  224.0.0.22            01-00-5e-00-00-16     statique
  224.0.0.252           01-00-5e-00-00-fc     statique
  224.168.100.1         01-00-5e-28-64-01     statique
  239.255.255.250       01-00-5e-7f-ff-fa     statique
  239.255.255.254       01-00-5e-7f-ff-fe     statique
```

*

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

- Les octets de position 0x0C et 0x0D signifie qu'il corresponde au champ ethertype qui correspond ici au protocol ARP (0806)

Quelle est la fonction de la trame ARP Request ? :

- La fonction de la trame ARP Request est de demander une adresse MAC par rapport a une adresse IP

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

- Ces octets corresponde au champ Opcode (00 01 pour une request et 00 02 pour une reply)

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

- La longeur d'un message ARP est de 28 octets

Quelle est la longueur de la trame ARP Request ? :

- La longueur de la trame ARP Request est de 42 octets

Quelle est la longueur de la trame ARP Reply ? :

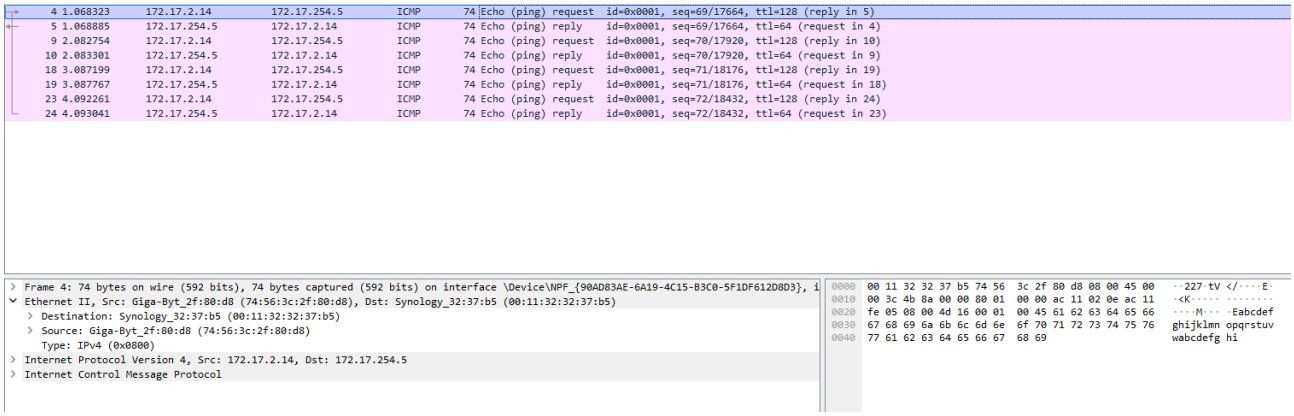
- La longueur de la trame ARP Reply est de 60 octets

Combien d’octets sont utilisés pour le padding ? :

- 18 octets sont utilisés pour le padding

Trame ARP Request
@MAC Destination = 00:11:32:32:37:b5 @MAC Source = 74:56:3c:2f:80:d8 Ethernet Type = 0806
Op code (valeur hexa.) = 00 01 @MAC de la cible = 00:11:32:32:37:b5 @IP de la cible = 172.17.254.5

Selection d’une Trame ICMP echo request :



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

- Les octets de position 0x0C et 0x0D corresponde au champ Ethertype, ce qui signifie que ici ils corresponde au protocole IP (0800)

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

- L’octet de position 0x07 ligne 10 est 01 ce qui correspond au protocole ICMP

Quelle est la longueur de la trame ? :
- La longueur de la trame est de 74 octets

Quelle est la longueur du paquet IP ? :
- La longueur du paquet IP est de 60 octets

Quelle est la longueur du message ICMP ? :
- La longueur du message ICMP est 40 octets

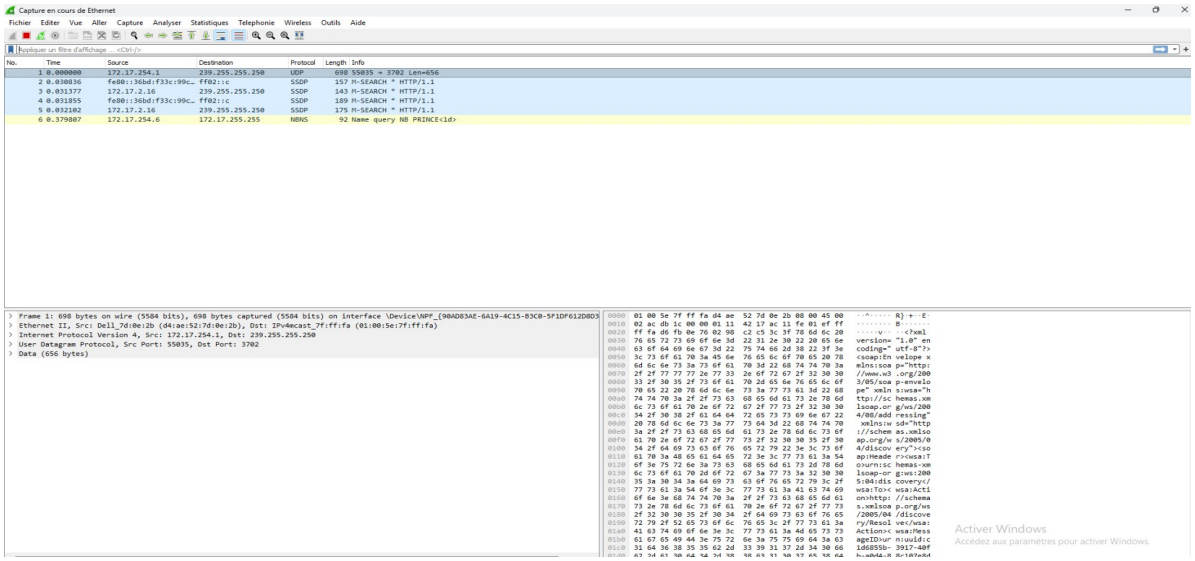
Quelle signification a l’octet de position 0×02 ligne 0020 ? :
- L’octet de position 0x02 ligne 0020 correspond au champ TYPE qui est ici 08 ce qui correspond bien a une echo request

A quoi correspondent les octets à partir de l’octet 0×0A, ligne 0020 ? :
- Les octets a partir de l’octet 0x0A ligne 0020 correspondent au données du message ICMP

Sélectionnez une trame ICMP Echo Reply. Quelle est le nom et la valeur de l’octet de position 0×02 ligne 0020 ? :
- L’octet de position 0x02 ligne 0020 correspond au champ TYPE, ici il a pour valeur 00 ce qui correspond bien a une echo reply

Captures de Trames ARP, DNS et ICMP :

démarrage d’une capture de trame :



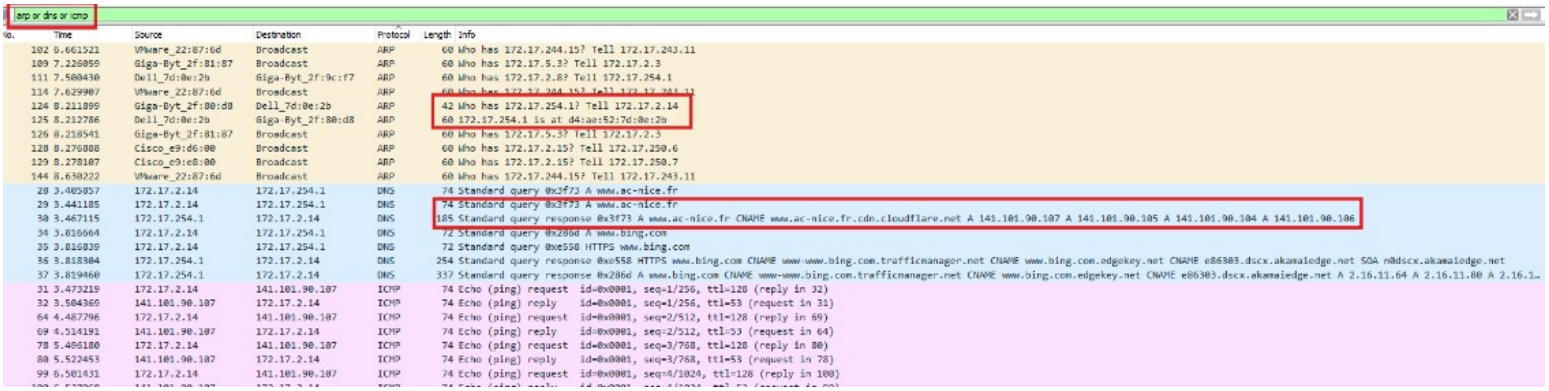
je vide la cache ARP a l’aide de la commande arp -b * :

```
Invite de commandes
Microsoft Windows [version 10.0.26100.6584]
(c) Microsoft Corporation. Tous droits réservés.

C:\Users\mballester>arp -b *

Affiche et modifie les tables de traduction d'adresses IP en adresses
physiques utilisées par le protocole de résolution d'adresses ARP.

ARP -s inet_addr eth_addr [if_addr]
ARP -d inet_addr [if_addr]
ARP -a [inet_addr] [-N if_addr] [-v]

  -a              Affiche les entrées ARP en cours en interrogeant les données
                  en cours du protocole. Si inet_addr est spécifié, seules les
                  adresses IP et physiques de l'ordinateur spécifié sont
                  affichées. Si plus d'une interface réseau utilise ARP, les
                  entrées de chaque table ARP sont affichées.
  -g              Identique à -a.
  -v              Affiche les entrées ARP en cours en mode verbeux. Toutes les
                  entrées non valides ainsi que celles de l'interface de retour
                  de bouclage sont affichées.
  inet_addr       Spécifie un adresse Internet.
  -N if_addr      Affiche les entrées ARP de chaque interface réseau spécifiée
                  par if_addr.
  -d              Supprime l'hôte spécifié par inet_addr. inet_addr peut
                  contenir le caractère générique * pour supprimer tous
                  les hôtes.
  -s              Ajoute l'hôte et associe l'adresse Internet inet_addr
                  avec l'adresse physique eth_addr. L'adresse physique
                  est donnée sous forme de 6 octets hexadécimaux séparés
                  par des tirets. L'entrée est permanente.
  eth_addr        Spécifie une adresse physique.
  if_addr         Spécifie l'adresse Internet de l'interface dont la table
                  de traduction d'adresses doit être modifiée.
                  Si ce paramètre n'est pas indiqué, la première interface
                  applicable sera utilisée.
Exemples :
  > arp -s 157.55.85.212   00-aa-00-62-c6-09  .... Ajoute une entrée statique.
  > arp -a                                    .... Affiche la table ARP.

C:\Users\mballester>
```

et ensuite je ping le serveur web www.ac-nice.fr :

```
C:\Users\mballester>ping www.ac-nice.fr

Envoi d'une requête 'ping' sur www.ac-nice.fr.cdn.cloudflare.net [141.101.90.104] avec 32 octets de données :
Réponse de 141.101.90.104 : octets=32 temps=16 ms TTL=53
Réponse de 141.101.90.104 : octets=32 temps=17 ms TTL=53
Réponse de 141.101.90.104 : octets=32 temps=17 ms TTL=53
Réponse de 141.101.90.104 : octets=32 temps=17 ms TTL=53

Statistiques Ping pour 141.101.90.104:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 16ms, Maximum = 17ms, Moyenne = 16ms

C:\Users\mballester>
```

Capture ICMP ARP DNS :



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

- La machine dont l'adresse MAC est recherchée est la machine qui possède l'adresse IP qui est ici 172.17.254.1

Trame ARP request
@MAC destination = d4:ae:52:7d:0e:2b @MAC source = 74:56:3c:2f:80:d8 Ethernet Type = 0806
Opcode (valeurs hexa.) = 01 @MAC de la cible = d4:ae:52:7d:0e:2b @IP de la cible = 172.17.254.1

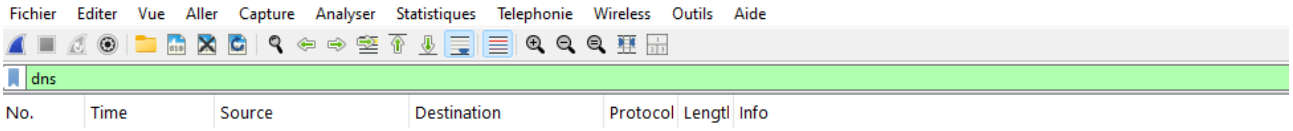
Pour quelle raison trouve-t-on ensuite une requête DNS avant l'échange de trames ICMP suite à l'exécution de la commande ping proprement dite ? :

- Avant d'envoyer les trames ICMP donc le ping, le nom du domaine doit être traduit en adresse IP. La traduction est realisé par une requête DNS. Le client interroge le serveur DNS pour obtenir l'adresse IP avant de pouvoir lancer le ping.

Consultation du cache DNS à l'aide de la commande ipconfig /displaydns et vérification de 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  . . . . : 293
Longueur de données . : 8
Section . . . . . . . : Réponse
Enregistrement CNAME  : www.ac-nice.fr.cdn.cloudflare.net


Nom d'enregistrement. : www.ac-nice.fr.cdn.cloudflare.net
Type d'enregistrement : 1
Durée de vie  . . . . : 293
Longueur de données . : 4
Section . . . . . . . : Réponse
Enregistrement (hôte) : 141.101.90.104


Nom d'enregistrement. : www.ac-nice.fr.cdn.cloudflare.net
Type d'enregistrement : 1
Durée de vie  . . . . : 293
Longueur de données . : 4
Section . . . . . . . : Réponse
Enregistrement (hôte) : 141.101.90.105
```

Démarrage d’une nouvelle capture et saisie de la commande ping www.ac-nice.fr dans l’invite de commandes :

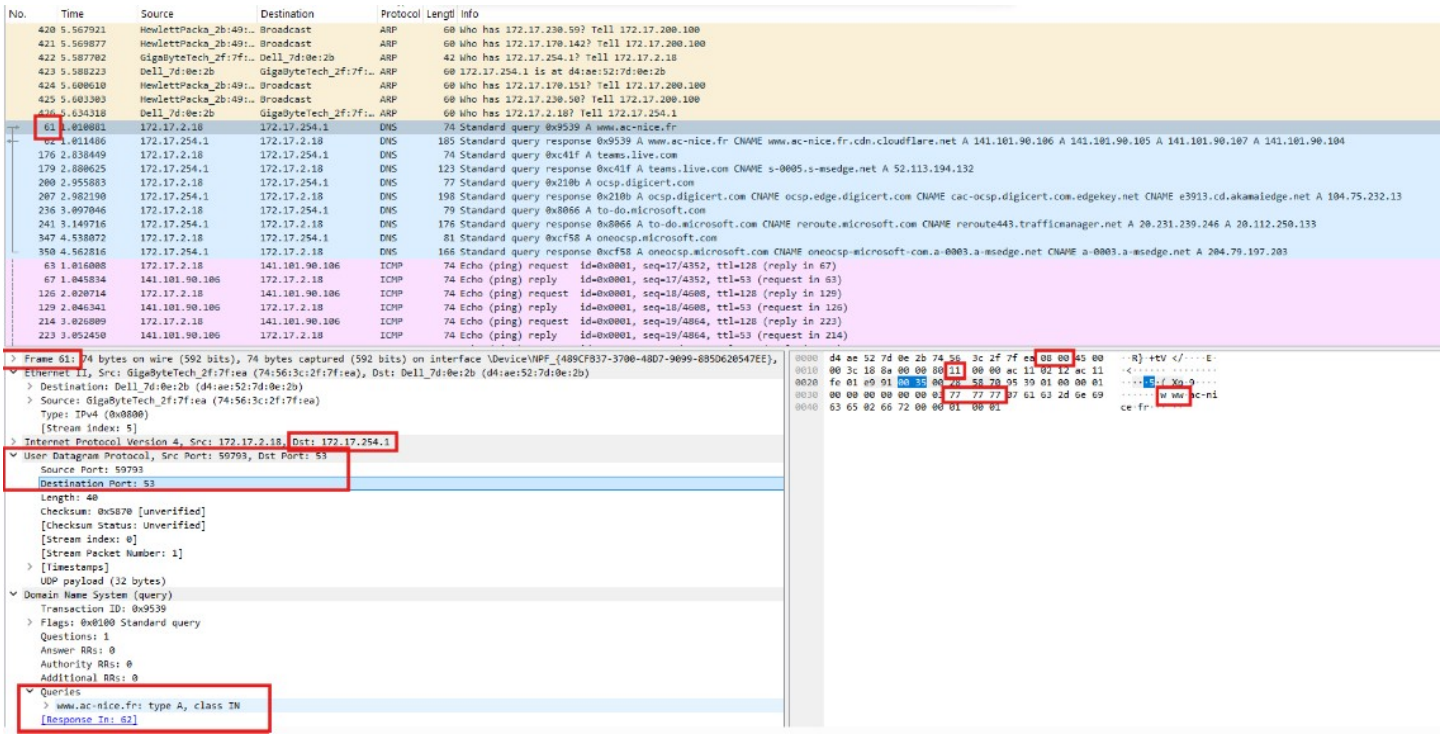


On ne constate pas de requête DNS puisque l’enregistrement est présent dans le cache DNS.

Vidage du cache DNS :

```
C:\Users\mballester>ipconfig /flushdns

Configuration IP de Windows

Cache de résolution DNS vidé.

C:\Users\mballester>
```

Redémarrage d’une capture pour re-visualiser la requêtes DNS :



les différents protocoles encapsulés dans une trame DNS sont :

- Le protocol IP
- Le protocol UDP
- Le protocol DNS

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

- La machine destinataire de la requête DNS est le serveur et il a pour 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 0x0C et 0x0D ligne 0000 corresponde au champ ethertype, il ont pour valeur 0800 ce qui signifie que derrière on va avoir le protocol IP

- l’octet 0x07 ligne 0010 correspond au champ protocol qui a ici pour valeur 11 (17 decimal) ce qui correspond au protocol UDP

Quelle est la longueur de l’en-tête IP ? :

- La longueur de l’en tête IP est de 20 bytes (octets)

Quelle est la longueur de l’en-tête de transport dans cette trame ? :

- La longueur de l’en tête de transport de cette trame (UDP) est de 8 octets

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

- Les octets de position 0x04 et 0x05 ligne 20 corresponde au champ port, ils ont pour valeur 0035 ici ce qui correspond au port destination (53) dont le port du serveur DNS

Quels sont les valeurs hexadécimales des octets correspondant au nom de domaine internet ac-nice.fr ? :

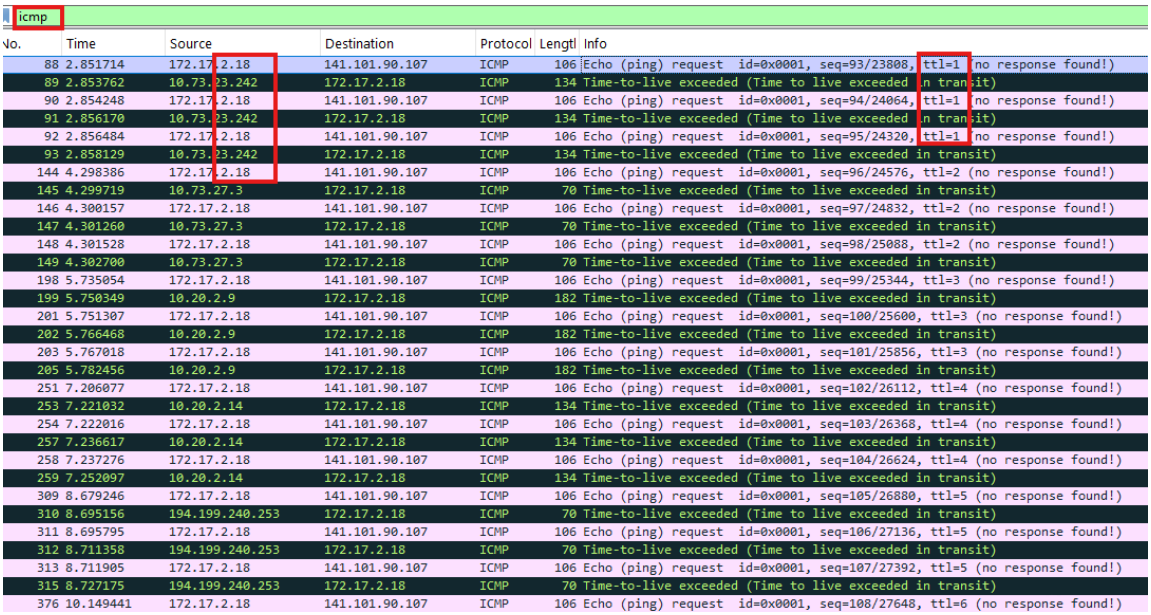
- Les valeurs hexadecimales des octets correspondant au nom de domaine internet ac-nice.fr sont : 61 63 2D 6E 69 63 65 02 66 72

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 :

Adresse décimale	**Adresse hexadécimale**
141.101.90.104	**8D 65 5A 68**
141.101.90.105	**8D 65 5A 69**
141.101.90.106	**8D 65 5A 6A**
141.101.90.107	**8D 65 5A 6B**

Commande Tracert et capture de trames ICMP

Capture de trame + saisie de la commande tracert www.ac-nice.fr dans l'invite de commande et filtrage des trames :



icmp

No.	Time	Source	Destination	Protocol	Length	Info
88	2.851714	172.17.2.18	141.101.90.107	ICMP	106	Echo (ping) request id=0x0001, seq=93/23808, ttl=1 (no response found!)
89	2.853762	10.73.23.242	172.17.2.18	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
90	2.854248	172.17.2.18	141.101.90.107	ICMP	106	Echo (ping) request id=0x0001, seq=94/24064, ttl=1 (no response found!)
91	2.856170	10.73.23.242	172.17.2.18	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
92	2.856484	172.17.2.18	141.101.90.107	ICMP	106	Echo (ping) request id=0x0001, seq=95/24320, ttl=1 (no response found!)
93	2.858129	10.73.23.242	172.17.2.18	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
144	4.298386	172.17.2.18	141.101.90.107	ICMP	106	Echo (ping) request id=0x0001, seq=96/24576, ttl=2 (no response found!)
145	4.299719	10.73.27.3	172.17.2.18	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
146	4.300157	172.17.2.18	141.101.90.107	ICMP	106	Echo (ping) request id=0x0001, seq=97/24832, ttl=2 (no response found!)
147	4.301260	10.73.27.3	172.17.2.18	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
148	4.301528	172.17.2.18	141.101.90.107	ICMP	106	Echo (ping) request id=0x0001, seq=98/25088, ttl=2 (no response found!)
149	4.302700	10.73.27.3	172.17.2.18	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
198	5.735054	172.17.2.18	141.101.90.107	ICMP	106	Echo (ping) request id=0x0001, seq=99/25344, ttl=3 (no response found!)
199	5.750349	10.20.2.9	172.17.2.18	ICMP	182	Time-to-live exceeded (Time to live exceeded in transit)
201	5.751307	172.17.2.18	141.101.90.107	ICMP	106	Echo (ping) request id=0x0001, seq=100/25600, ttl=3 (no response found!)
202	5.766468	10.20.2.9	172.17.2.18	ICMP	182	Time-to-live exceeded (Time to live exceeded in transit)
203	5.767018	172.17.2.18	141.101.90.107	ICMP	106	Echo (ping) request id=0x0001, seq=101/25856, ttl=3 (no response found!)
205	5.782456	10.20.2.9	172.17.2.18	ICMP	182	Time-to-live exceeded (Time to live exceeded in transit)
251	7.206077	172.17.2.18	141.101.90.107	ICMP	106	Echo (ping) request id=0x0001, seq=102/26112, ttl=4 (no response found!)
253	7.221032	10.20.2.14	172.17.2.18	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
254	7.222016	172.17.2.18	141.101.90.107	ICMP	106	Echo (ping) request id=0x0001, seq=103/26368, ttl=4 (no response found!)
257	7.236617	10.20.2.14	172.17.2.18	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
258	7.237276	172.17.2.18	141.101.90.107	ICMP	106	Echo (ping) request id=0x0001, seq=104/26624, ttl=4 (no response found!)
259	7.252097	10.20.2.14	172.17.2.18	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
309	8.679246	172.17.2.18	141.101.90.107	ICMP	106	Echo (ping) request id=0x0001, seq=105/26880, ttl=5 (no response found!)
310	8.695156	194.199.240.253	172.17.2.18	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
311	8.695795	172.17.2.18	141.101.90.107	ICMP	106	Echo (ping) request id=0x0001, seq=106/27136, ttl=5 (no response found!)
312	8.711358	194.199.240.253	172.17.2.18	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
313	8.711905	172.17.2.18	141.101.90.107	ICMP	106	Echo (ping) request id=0x0001, seq=107/27392, ttl=5 (no response found!)
315	8.727175	194.199.240.253	172.17.2.18	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
376	10.149441	172.17.2.18	141.101.90.107	ICMP	106	Echo (ping) request id=0x0001, seq=108/27648, ttl=6 (no response found!)

Quelle est l'adresse IP Destination (valeurs déci. et hexa.) ? :

- L'adresse IP destination est 141.101.90.107 en décimal et 8D 65 5A 6B en hexadécimal

Quelle est la valeur portée par ce champ (valeurs déci. et hexa.) ? :

- La valeur portée par ce champ est 1 en décimal et 01 en hexadécimal

Quelle est la valeur portée par le champ Type (valeurs déci. et hexa.) ? :

- La valeur portée par le champ Type est 8 en décimal et 08 en hexadécimal

Quelle est la valeur portée par le champ Type (valeurs déci. et hexa.) ? :

- La valeur portée par le champ Type est 11 en décimal et 0b en hexadécimal