TP 5- Trames ARP, ICMP et DNS

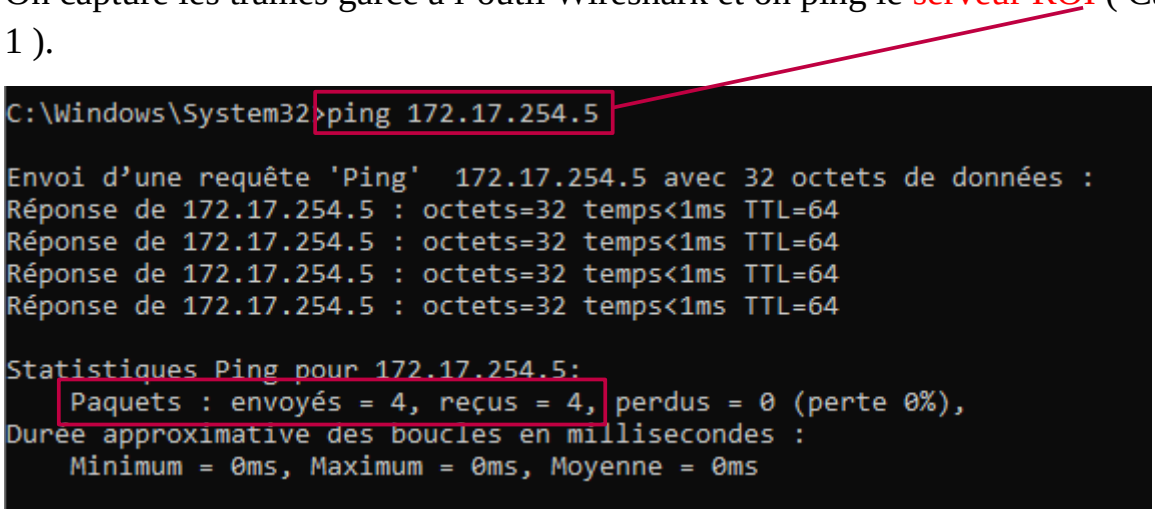
Nesrine EL AHMADI

BTS SIO

Table des matières

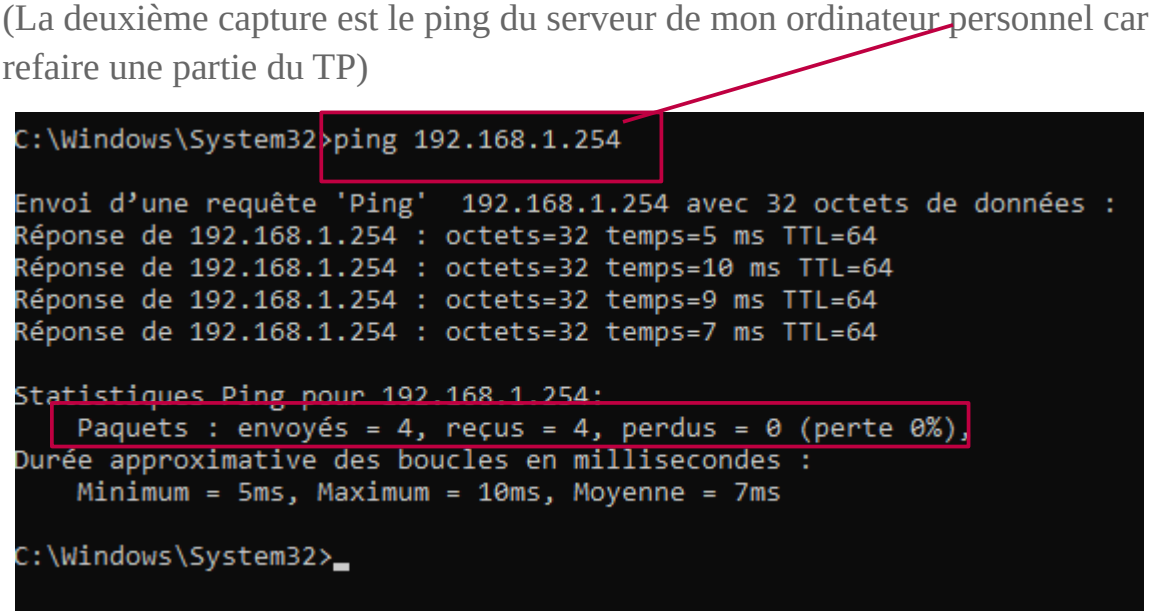
1. Capture de trames ARP et ICMP

On capture les trames garce a l'outil Wireshark et on ping le serveur ROI (Capture 1).

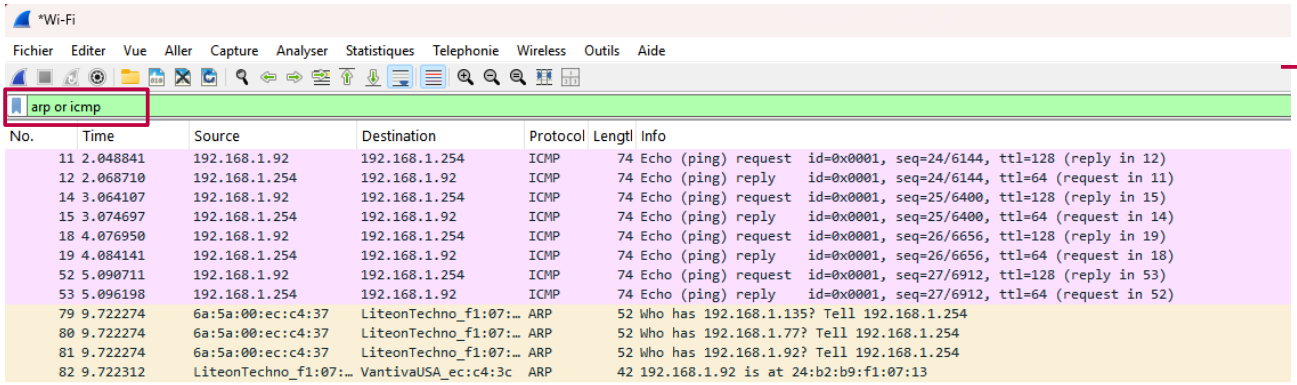


Capture 1

(La deuxième capture est le ping du serveur de mon ordinateur personnel car j'ai du refaire une partie du TP)



On filtre les trames en inscrivant arp or icmp dans Wireshark (Capture 3) .



Avec PC

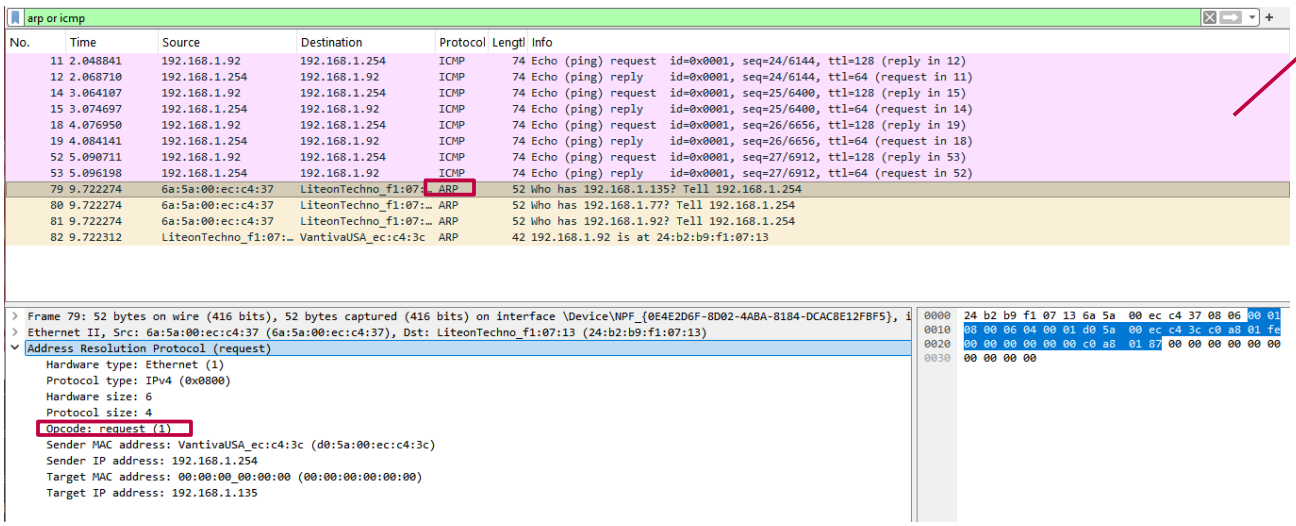
Capture 3

```
C:\Windows\System32>arp -a

Interface : 192.168.1.92 --- 0x4
  Adresse Internet      Adresse physique      Type
  192.168.1.4           d0-05-2a-b2-d5-4b     dynamique
  192.168.1.143         14-c1-4e-01-fd-36     dynamique
  192.168.1.157         a0-d0-5b-c7-85-44     dynamique
  192.168.1.254         d0-5a-00-ec-c4-3c     dynamique
  192.168.1.255         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
  224.0.0.251           01-00-5e-00-00-fb     statique
  224.0.0.252           01-00-5e-00-00-fc     statique
  239.255.255.250       01-00-5e-7f-ff-fa     statique
  255.255.255.255       ff-ff-ff-ff-ff-ff     statique

Interface : 192.168.56.1 --- 0x12
  Adresse Internet      Adresse physique      Type
  192.168.56.255        ff-ff-ff-ff-ff-ff     statique
  224.0.0.22            01-00-5e-00-00-16     statique
  224.0.0.251           01-00-5e-00-00-fb     statique
  224.0.0.252           01-00-5e-00-00-fc     statique
  239.255.255.250       01-00-5e-7f-ff-fa     statique

C:\Windows\System32>
```

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

C:\Windows\System32>arp -a

Interface : 192.168.1.92 --- 0x4
  Adresse Internet      Adresse physique      Type
  192.168.1.4           d0-05-2a-b2-d5-4b     dynamique
  192.168.1.143         14-c1-4e-01-fd-36     dynamique
  192.168.1.254         d0-5a-00-ec-c4-3c     dynamique
  224.0.0.2             01-00-5e-00-00-02     statique
  224.0.0.22            01-00-5e-00-00-16     statique

Interface : 192.168.56.1 --- 0x12
  Adresse Internet      Adresse physique      Type
  224.0.0.22            01-00-5e-00-00-16     statique

C:\Windows\System32>
```

On a pas l'@IP et l'@ MAC correspondant à Aviateur car cette partie du TP a été faite avec mon PC.

Grace au **trames ARP (Request et Reply) (Capture 4)** précédent l'échange de **trames ICMP** on peut répondre aux questions suivantes :



Avec PC

Capture 4

---Quelle signification ont les octets de position 0x0C et 0x0D ligne 0000 ?

Ce sont les octets 12 et 13 de la trame Ethernet. Ils correspondent au champ EtherType , et indique que le protocole encapsulé est ARP (0806) .

---Quelle est la fonction de la trame ARP REQUEST ?

Elle permet à une machine de **demander l'adresse MAC** associée à une **adresse IP cible**.

---Quelle signification ont les octets de position 0x04 et 0x05 ligne 0010 ?

Ce sont les octets 4 et 5 du message ARP. Ils corespondent au champ « Operation » du protocole ARP. ARP Request (0x0001), ARP Reply (0x0002).

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

Un message ARP fait 28 octets.

--- Quelle est la longueur de la trame ARP Request ?

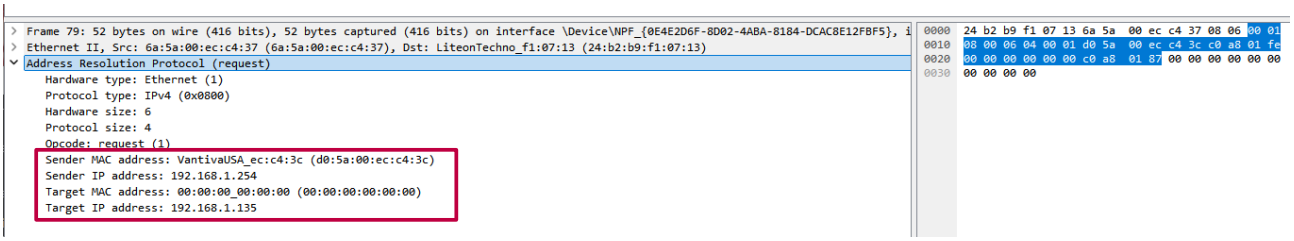
La longueur de la trame ARP Request est de 42 octets (14 octets Ethernet + 28 octets (ARP).

--- Quelle est la longueur de la trame ARP Reply ?

La trame ARP Reply fait 42 octets. Elle a la même structure mais le champ opération change (0x0002).

---Combien d'octets sont utilisés pour le padding ?

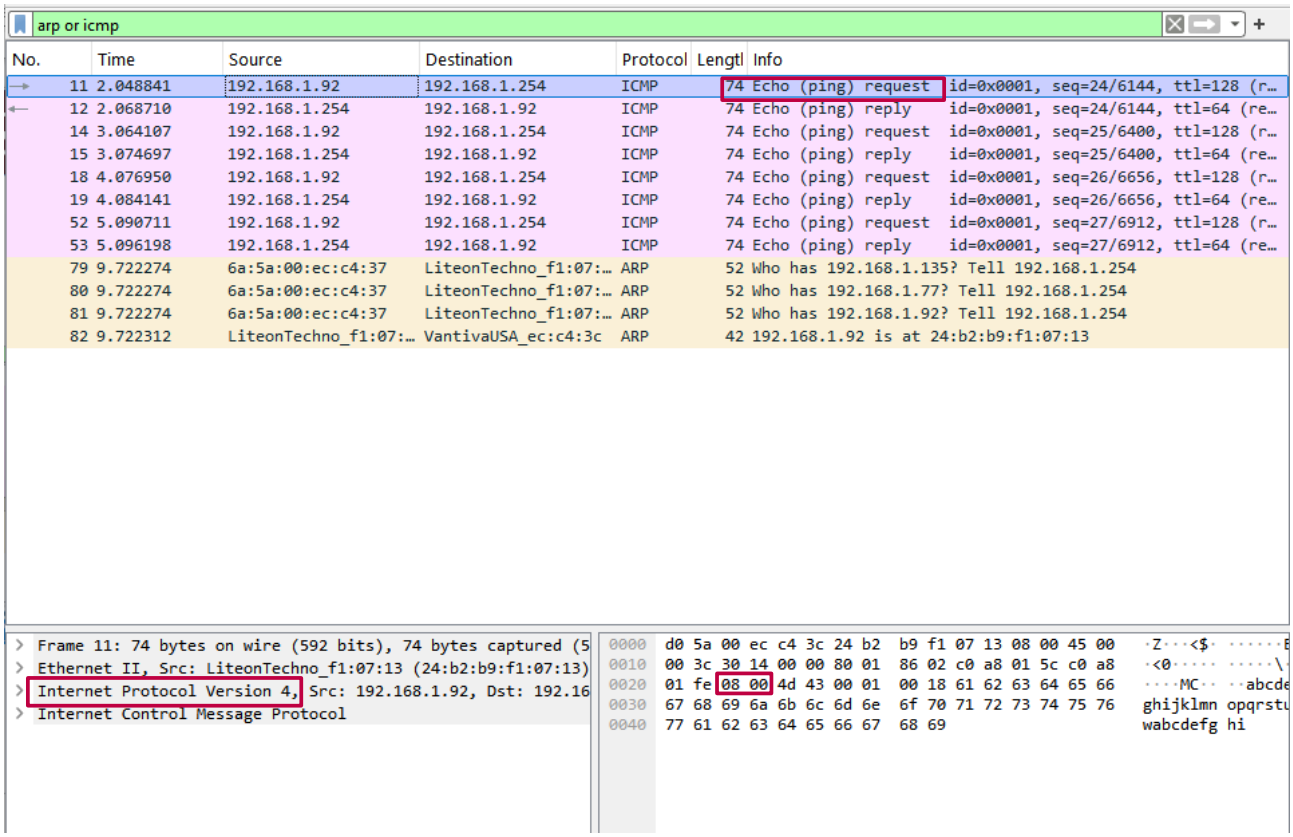
Le padding est ajouté pour atteindre la taille minimal Ethernet qui est de 64..Si la trame est de 42 octets alors le padding est de 22 octets



Trame ARP Request

Adresse MAC destination : 24:b2:b9:f1:07:13
Adresse MAC source : 6a:5a:00:ec:c4:37
Ethernet Type : 0806
Opcode(valeur hexa.) : 0001 (request)
Adresse MAC de la cible : 00 :00:00:00:00:00
Adresse IP de la cible : 192.168.1.135

En sélectionnant une trame ICMP Echo Request (Capture 4) on peut répondre au questions suivantes :



Capture 4 (ICMP Request)

---Quelles signification ont les octets de position 0x0C et 0x0D ligne 0000 ?

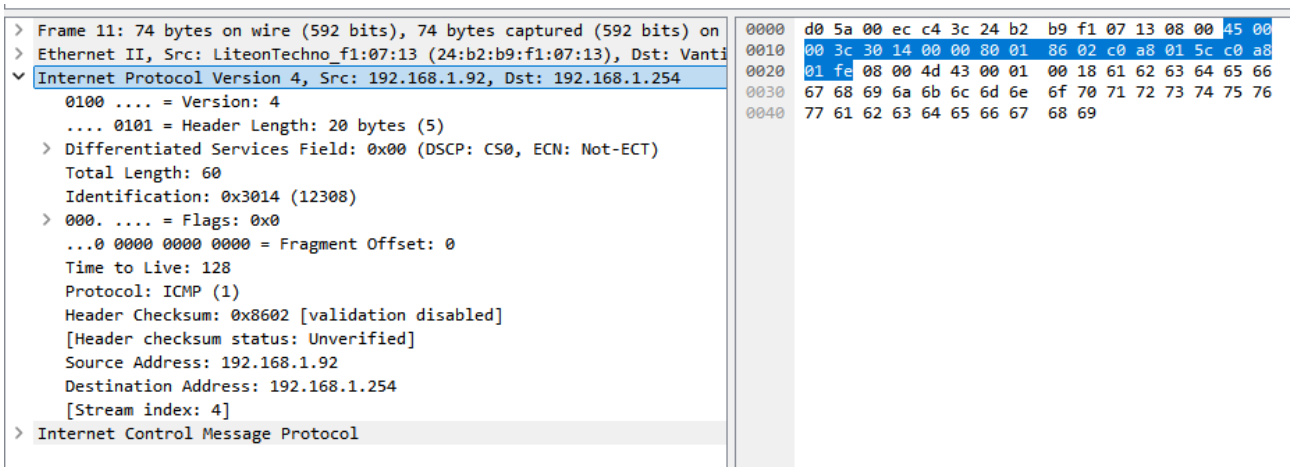
Ce sont les octets 12 et 13 de l'en-tête Ethernet. Il contient le champ Ethertype 0x0800 ce qui signifie que le protocole encapsulé est IPv4 .

---Quelle signification a l'octet de position 0x07 ligne 0010 ?

Cet octet fait partie du champ Opcode . Sa valeur est 0001 ce qui signifie que le protocole encapsulé est ICMP.

---Quelle est la longueur de la trame ?

La trame fait 74 octets au total.



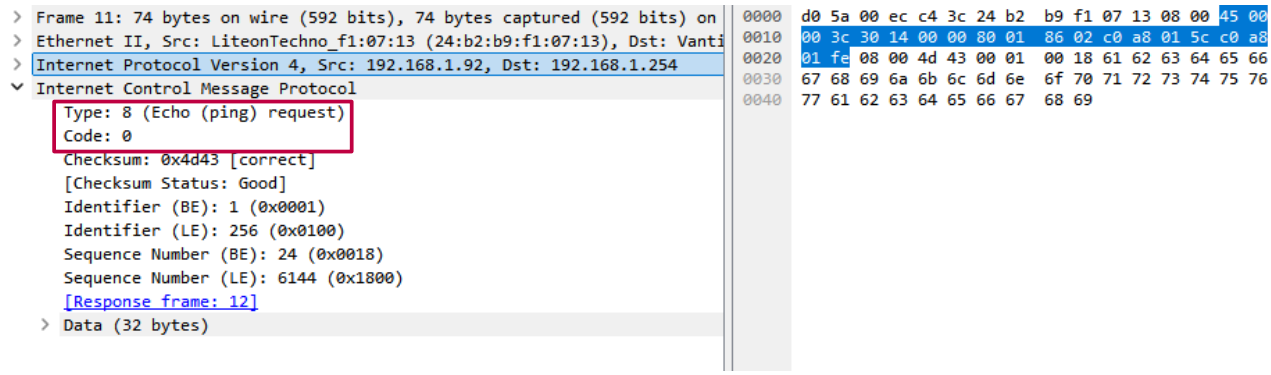
---Quelle est la longueur du paquet IP ?

La taille totale du paquet IP est de 70 octets.

---Quelle est la longueur du message ICMP ?

L'en-tête IP fait 20 octets donc 70-20=50 octts pour le message ICMP.

Le message ICMP fait 50 octets.



---Quelle signification a l'octet de position 0x02 ligne 00020 ?

C'est le 3ième octet du message ICMP .

Il correspond au champ « code ». Le 0x00 signifie echo request ou echo reply. Le type nous affire que c'est une echo request.

---A quoi correspondent les octets a partir de l'octet 0x0A, ligne 00020?

Ils correspondent aux données ICMP.

On sélectionne une trame ICMP Echo Reply .

---Quelle est le nom et la valeur de l'octet de position 0x02 ligne 00020 ?

C'est le champ code de valeur 0x00.

2. Capture de trames ARP , DNS et ICMP

On démarre une capture sur Wireshark et on vide le cache ARP sur l'invite de commande grace a la commande arp -d* (Capture 5).

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

C:\Windows\System32>arp -a

Interface : 192.168.1.92 --- 0x4
  Adresse Internet      Adresse physique      Type
  192.168.1.4           d0-05-2a-b2-d5-4b     dynamique
  192.168.1.143         14-c1-4e-01-fd-36     dynamique
  192.168.1.254         d0-5a-00-ec-c4-3c     dynamique
  224.0.0.2             01-00-5e-00-00-02     statique
  224.0.0.22            01-00-5e-00-00-16     statique

Interface : 192.168.56.1 --- 0x12
  Adresse Internet      Adresse physique      Type
  224.0.0.22            01-00-5e-00-00-16     statique

C:\Windows\System32>
```

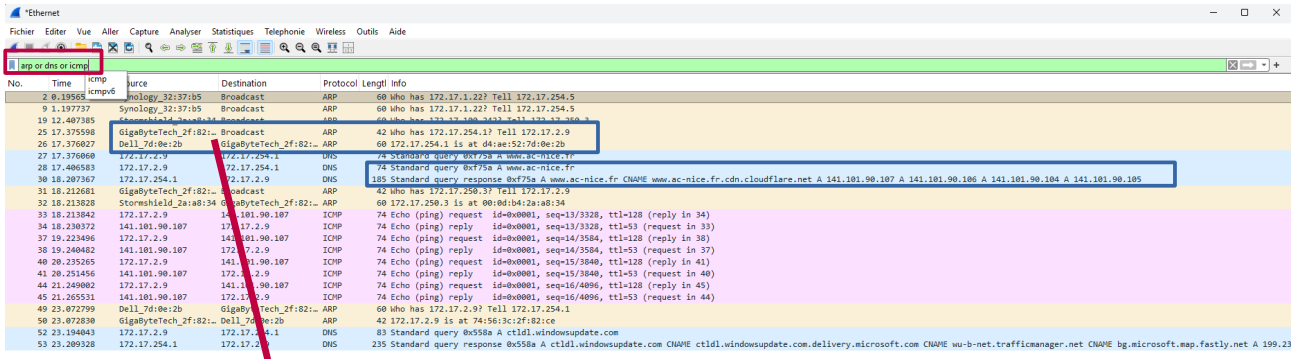
Capture 5

On effectue un ping vers le serveur web www.ac-nice.fr (Capture 6).

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

Envoi d'une requête 'ping' sur www.ac-nice.fr.cdn.cloudflare.net [141.101.90.107] avec 32 octets de données :
Réponse de 141.101.90.107 : octets=32 temps=17 ms TTL=53
Réponse de 141.101.90.107 : octets=32 temps=17 ms TTL=53
Réponse de 141.101.90.107 : octets=32 temps=16 ms TTL=53
Réponse de 141.101.90.107 : octets=32 temps=16 ms TTL=53

Statistiques Ping pour 141.101.90.107:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 16ms, Maximum = 17ms, Moyenne = 16ms
```

Capture 6

On filtre la capture faite sur Wireshark en inscrivant ARP or DNS or ICMP dans *filter (Capture 7).*



Capture 7

---**<u>Quelle est l'adresse MAC recherchée ?</u>**

La machine dont l'adresse MAC est recherché est la machine dont l'adresse IP est 172.17.5.254.

Trame ARP request
@MAC destination : ff:ff:ff:ff:ff:ff @MAC source : 2f:82: (je n'ai pas la suite car je n'ai pas developpé l'en-tête) Ethernet Type :0x0806
Opcode (valeur hexa.) :0x0001 @MAC de la cible : d4:ae:52:7d:0e:2b @IP de la cible :172.17.254.1

---**<u>Pour quel raison trouve t-on ensuite une requête DNS avant l'échange de trames ICMP suite à l'exécution de la commande ping proprement dite ?</u>**

Parce que la commande ping www.ac-nice.fr utilise un nom de domaine et pas une adresse IP.

Avant d'envoyer les trames ICMP, le système doit résoudre le nom en adresse IP via une requête DNS.

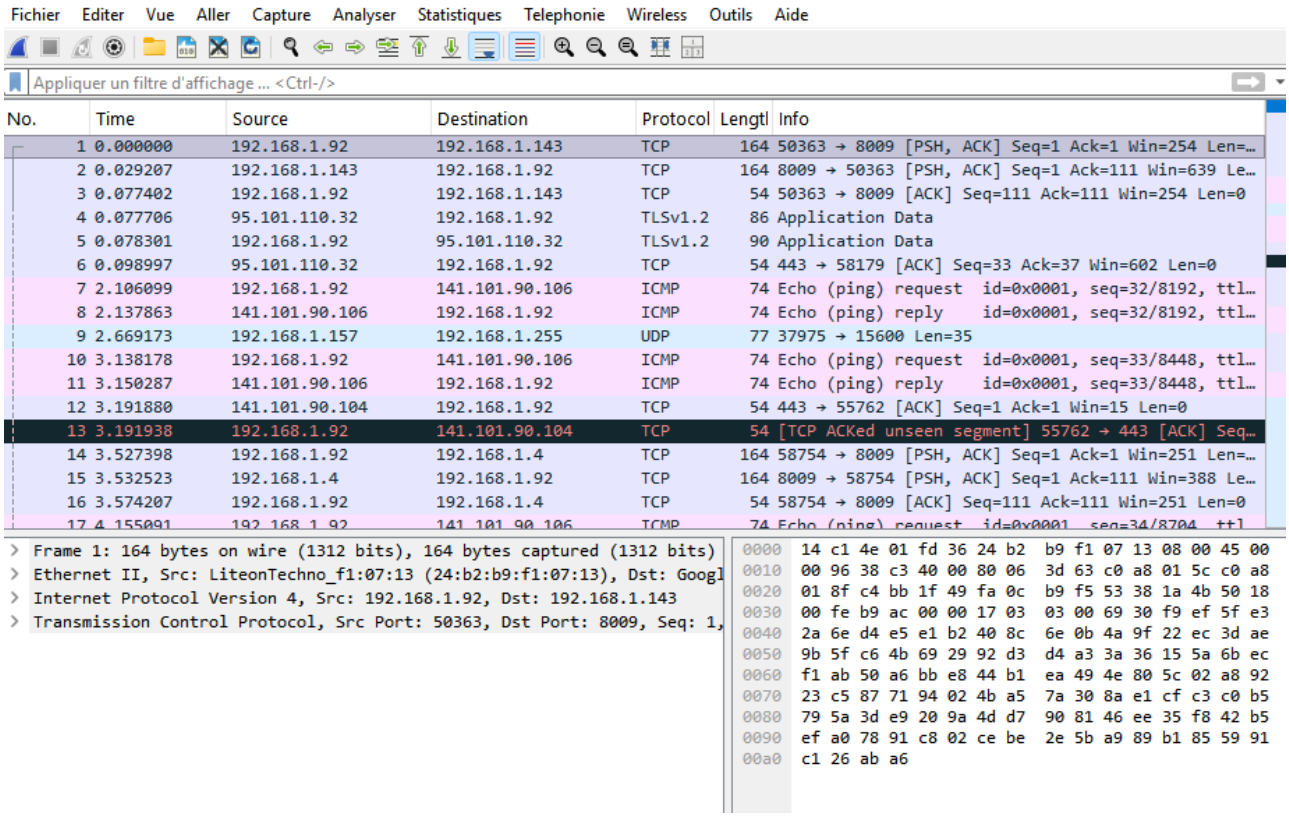
On consulte le cache DNS a l'aide de la commande ipconfig /displaydns dans l'invite de commande afin de vérifiez la présence de l'enregistrement DNS ac-nice.fr et de l'adresse IP associée.

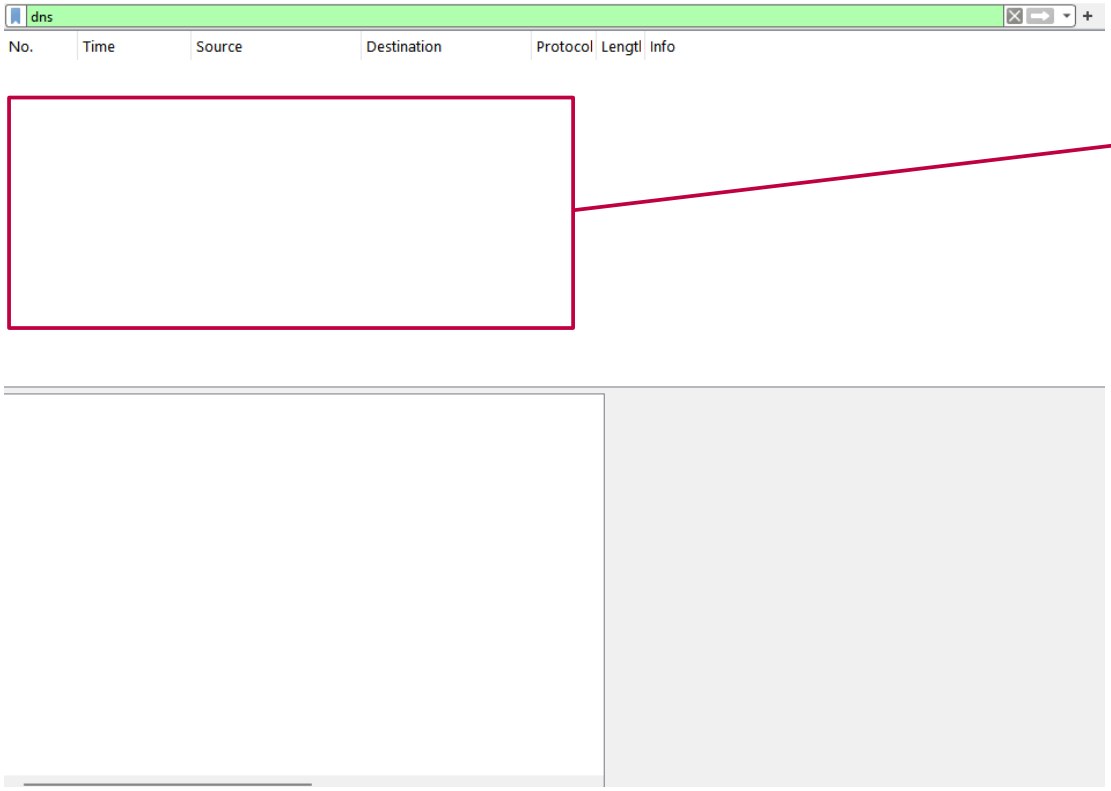
```
C:\Windows\System32>ipconfig /displaydns

Configuration IP de Windows

    fe3cr.delivery.mp.microsoft.com
    ----------------------------------------
    Nom d'enregistrement. : fe3cr.delivery.mp.microsoft.com
    Type d'enregistrement : 5
    Durée de vie  . . . . : 1367038
    Longueur de données . : 8
    Section . . . . . . . : Réponse
    Enregistrement CNAME  : fe3.delivery.mp.microsoft.com


    Nom d'enregistrement. : fe3.delivery.mp.microsoft.com
    Type d'enregistrement : 5
    Durée de vie  . . . . : 1367038
    Longueur de données . : 8
    Section . . . . . . . : Réponse
    Enregistrement CNAME  : glb.cws.prod.dcat.dsp.trafficmanager.net


    Nom d'enregistrement. : glb.cws.prod.dcat.dsp.trafficmanager.net
    Type d'enregistrement : 1
    Durée de vie  . . . . : 1367038
    Longueur de données . : 4
    Section . . . . . . . : Réponse
    Enregistrement (hôte) : 13.85.23.206

  www.ac-nice.fr
  ----------------------------------------
  Nom d'enregistrement. : www.ac-nice.fr
  Type d'enregistrement : 5
  Durée de vie  . . . . : 1372547
  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  . . . . : 1372547
  Longueur de données . : 4
  Section . . . . . . . : Réponse
  Enregistrement (hôte) : 141.101.90.106
```

On fait une nouvelle capture sur Wireshark et on exécute a nouveau un ping www.ac-nice.fr dans l'invite de commande.

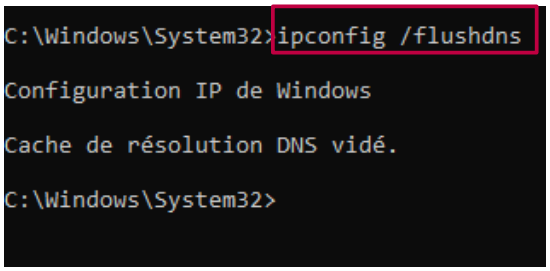
```
C:\Windows\System32>ping www.ac-nice.fr

Envoi d'une requête 'ping' sur www.ac-nice.fr.cdn.cloudflare.net [141.101.90.107] avec 32 octets de données :
Réponse de 141.101.90.107 : octets=32 temps=10 ms TTL=53
Réponse de 141.101.90.107 : octets=32 temps=15 ms TTL=53
Réponse de 141.101.90.107 : octets=32 temps=14 ms TTL=53
Réponse de 141.101.90.107 : octets=32 temps=12 ms TTL=53

Statistiques Ping pour 141.101.90.107:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 10ms, Maximum = 15ms, Moyenne = 12ms

C:\Windows\System32>
```

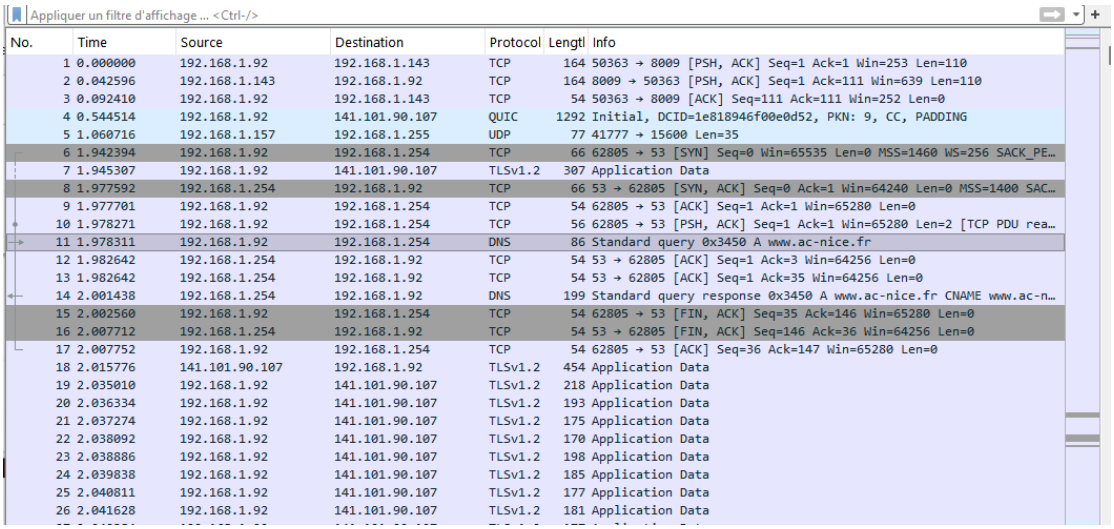
→ Il n'y a pas de requête DNS (Capture 9) car l'enregistrement est dans le cache DNS.

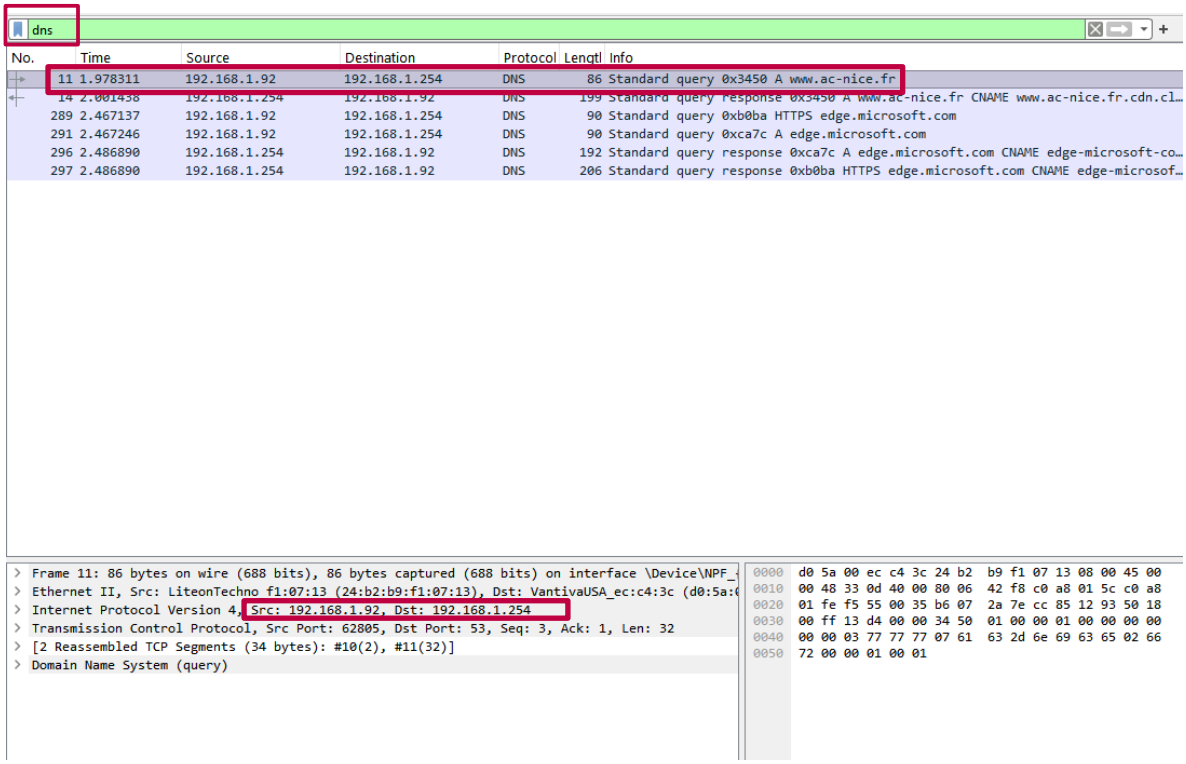




On vide le cache DNS a l'aide de la commande ipconfig /flushdns (capture 10), et on lance une nouvelle capture pour une requête DNS (Capture 11).







---<u>Quels sont les différents protocoles encapsulés dans une trame DNS ?</u>

Ethernet encapsule IPv4, qui encapsule TCP, lui-même encapsulant le message DNS au niveau applicatif.

---<u>Quelle est la machine destinataire de la requête DNS ? Quelle est son IP (en-tête IP)</u>

La machine destinataire est le serveur DNS.

Son adresse IP est : 192.168.1.254

---Quelle signification ont les octets de position 0x0C et 0x0D ligne 0000 et 0x07 ligne 0010 ?

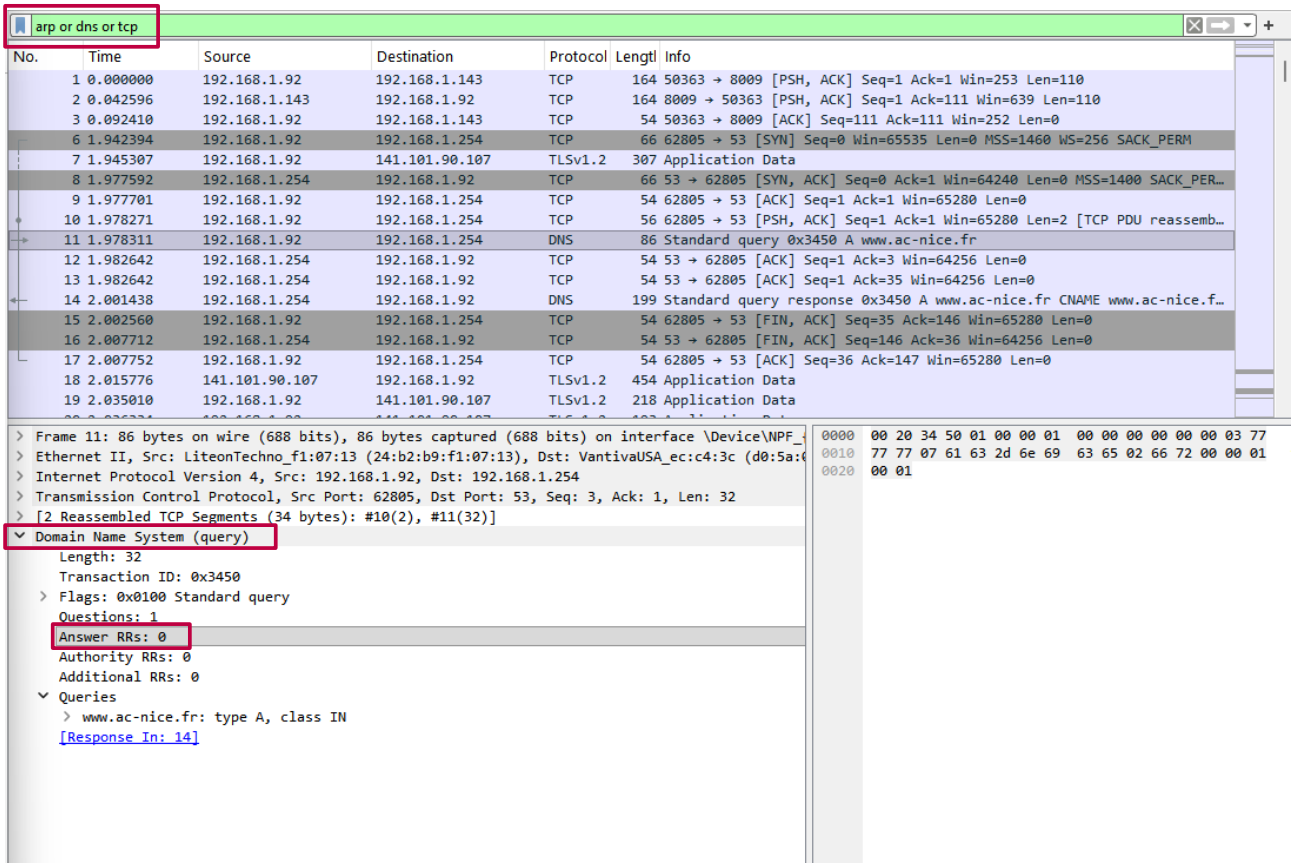
0x0C et 0x0D ligne 0000 → champ Ethertype dans Ethernet. Sa valeur 0x0800 → protocole encapsulé = IPv4

0x07 ligne 0010 → champ protocole dans l'en-tête IP. Sa valeur 0x06 → protocole de transport = TCP

---Quelle signification ont les octets de position 0x04 et 0x05 ligne 0020 ?

Ce sont les octets 4 et 5 de l'en-tête TCP . Ils correspondent au champ « Source Port ». Sa valeur : signifie que la requête est faite par le client (62805)

On développe la section Domain Name System (query) et plus précisément Queries (Capture 12).



Capture 12

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

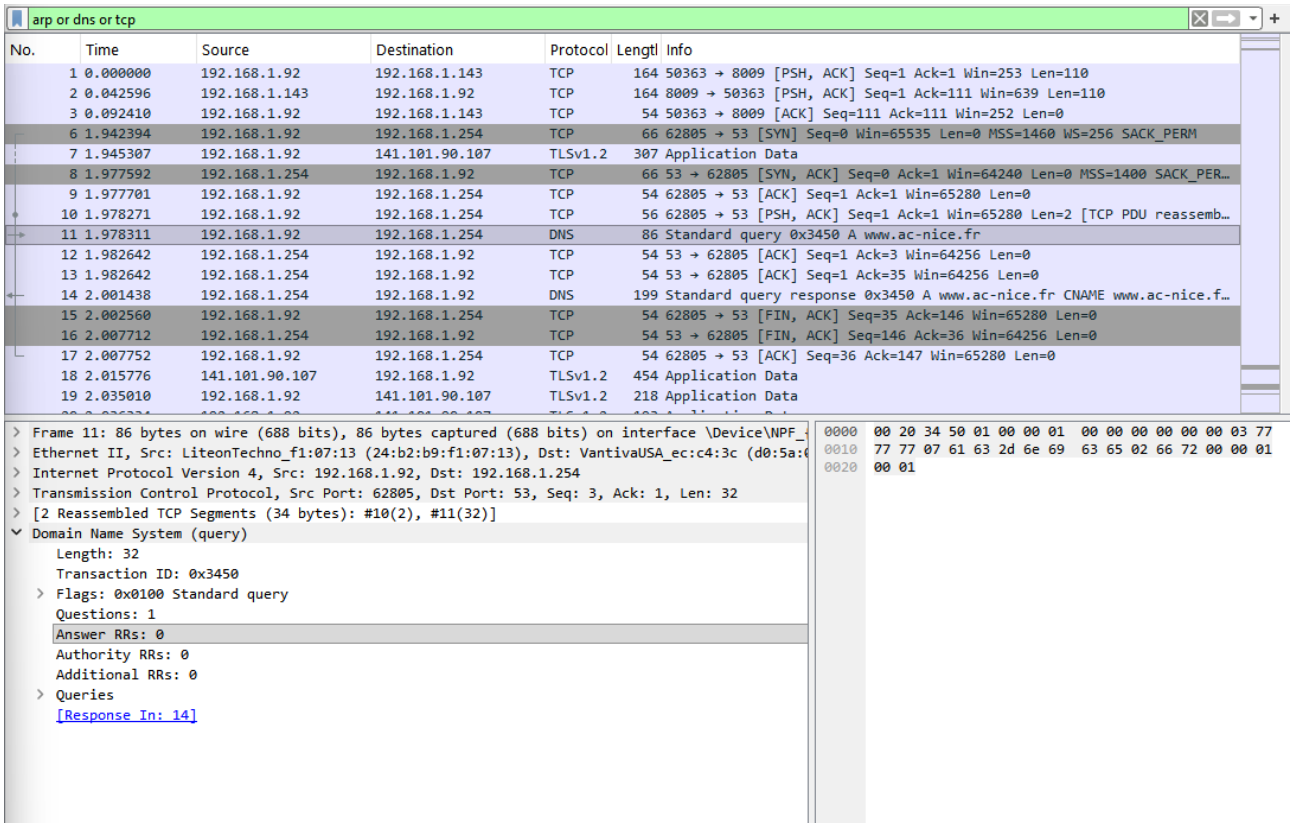
02 61 63 → « ac »

04 6E 69 63 65 → « nice »

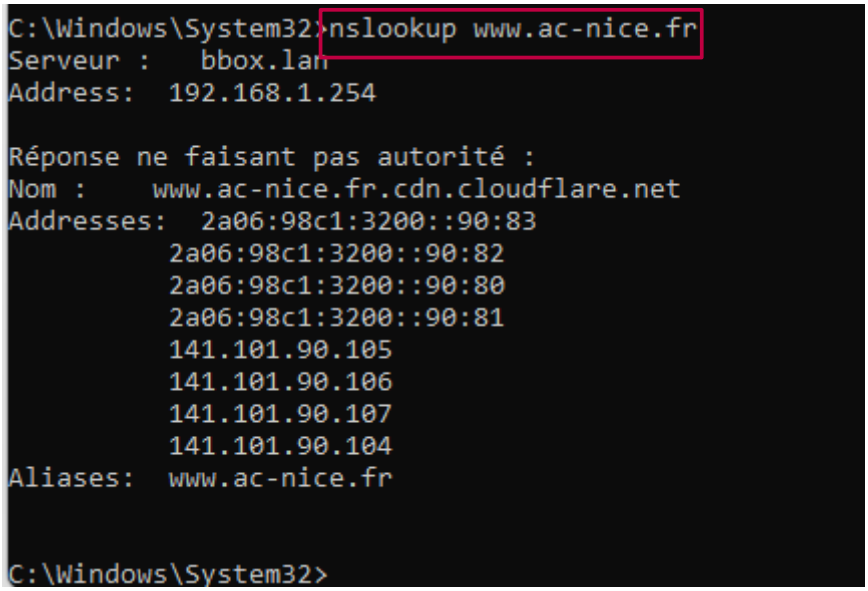
02 66 72 -> »fr »

00→ fin du nom

On sélectionne la trame comportant la réponse à la requête DNS et on développe la section Domain Name System (response) et plus particulièrement la rubrique answers. (Capture 13)



--- Rechercher les valeurs hexadécimales et décimales de l'adresse IP du serveur web hébergeant le site de l'académie de Nice.



Conversion hexadécimale de l'@ip : 141.101.90.104

141 → 8D

101 → 65

90 → 5A

104 → 68

3. Commande Tracert et capture de trames ICMP

(Partie faite avec un ordinateur du labo)

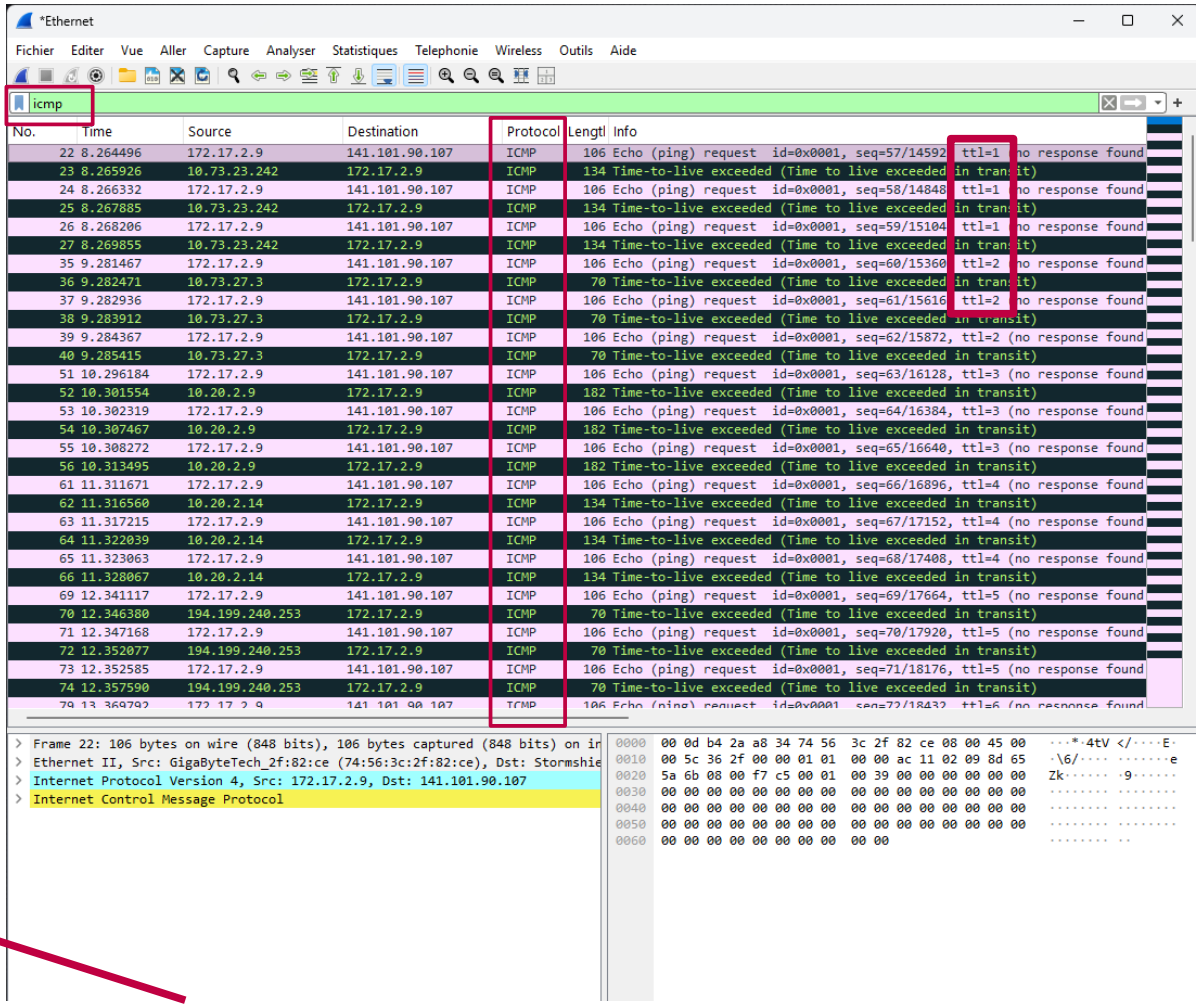
On exécute la ***commande Tracert*** dans l'invite de commande ce qui va nous permettre de connaître tout les routeurs entre la machine local et l'adresse de destination (Capture 14).

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

Détermination de l'itinéraire vers www.ac-nice.fr.cdn.cloudflare.net [141.101.90.107]
avec un maximum de 30 sauts :

  1     1 ms     1 ms     1 ms  10.73.23.242
  2     1 ms     1 ms     1 ms  10.73.27.3
  3     5 ms     5 ms     5 ms  10.20.2.9
  4     5 ms     5 ms     5 ms  10.20.2.14
  5     5 ms     5 ms     5 ms  194.199.240.253
  6     6 ms     6 ms     5 ms  te0-0-0-2-ren-nr-marseille2-rtr-091.noc.renater.fr [193.51.190.154]
  7    18 ms    16 ms    16 ms  et-0-1-1-ren-nr-marseille2-rtr-131.noc.renater.fr [193.55.205.56]
  8    15 ms    16 ms    16 ms  hu0-2-0-0-ren-nr-lyon2-rtr-091.noc.renater.fr [193.51.177.255]
  9    15 ms    15 ms    15 ms  et-5-3-1-ren-nr-paris2-rtr-131.noc.renater.fr [193.51.177.238]
 10    17 ms    16 ms    16 ms  equinix-paris.cloudflare.com [195.42.144.143]
 11    17 ms    16 ms    16 ms  141.101.67.109
 12    16 ms    16 ms    16 ms  141.101.90.107

Itinéraire déterminé.
```

Capture 14

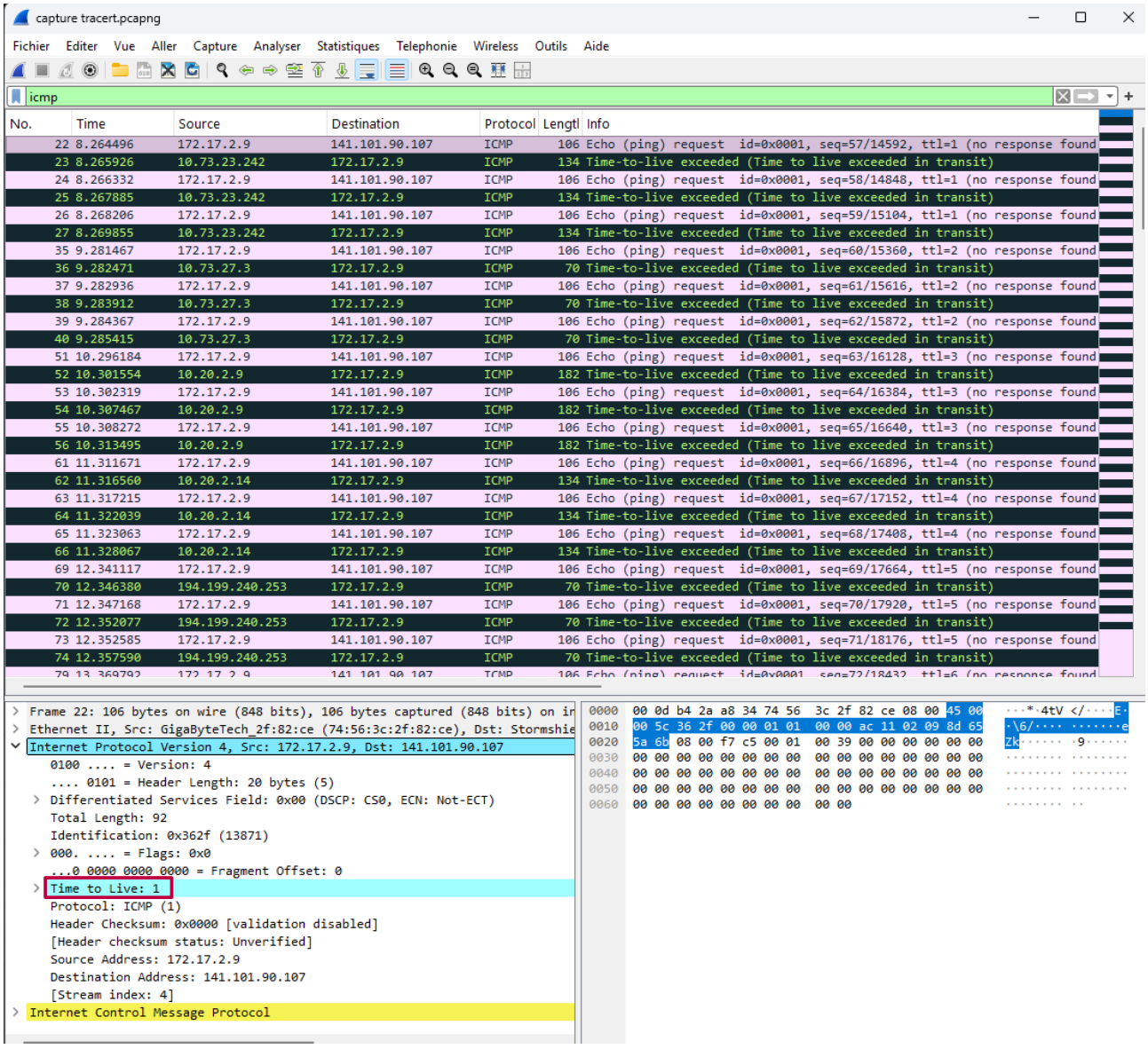
On démarre une capture de trames sur Wireshark et on saisis Tracert www.ac-nice.fr.

On limite l'affichage des trames a celles encapsulant le protocole ICMP (Capture 15).



Capture 15

On sélectionne la première **trame ICMP** request et on développe l'**en-tête IP** (Capture 16).

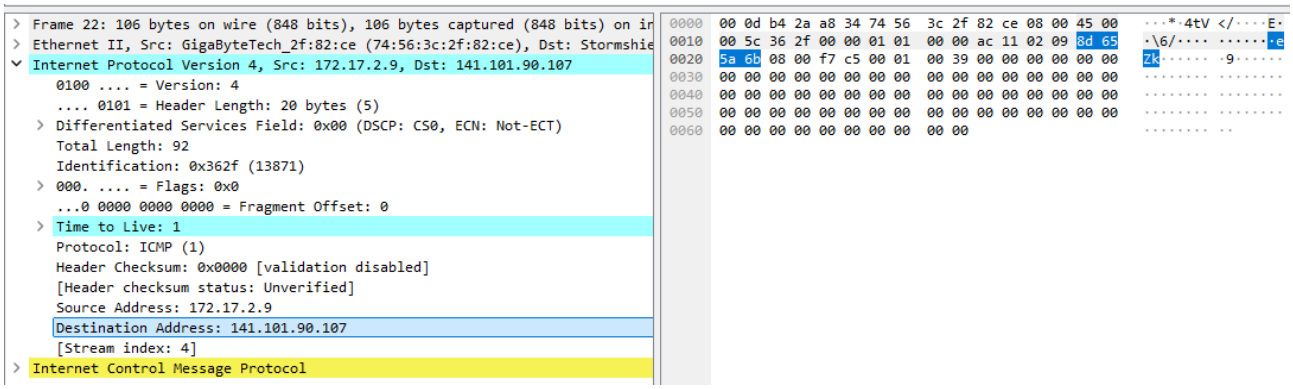


Capture 16

<u>--- Adresse IP Destination (valeur décimale) : 141.101.90.187</u>

<u>(valeur hexa.) :8D 65 5A BB</u>

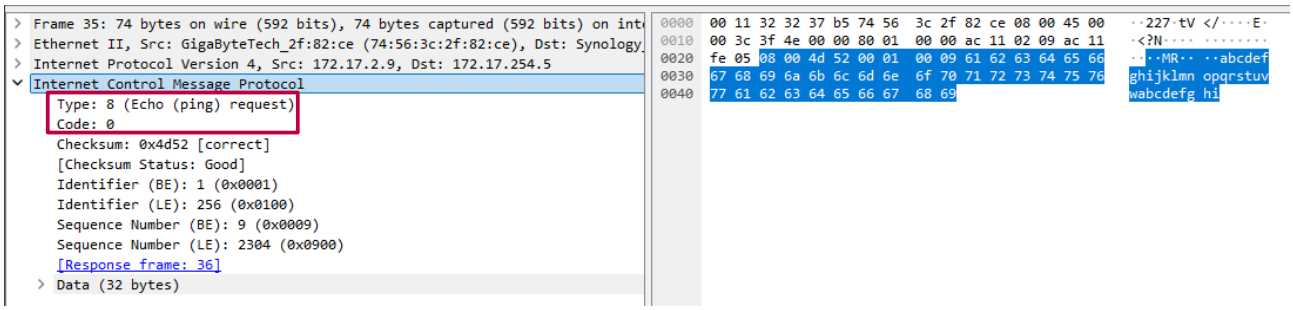
On sélectionne le champ **TTL** .(Capture 17)



Capture 17

<u>---Quelle est la valeur portée par ce champ (val.déci.) : 1 (val.hexa) :0x01</u>

On développe la section correspondant au message ICMP (Capture 18)

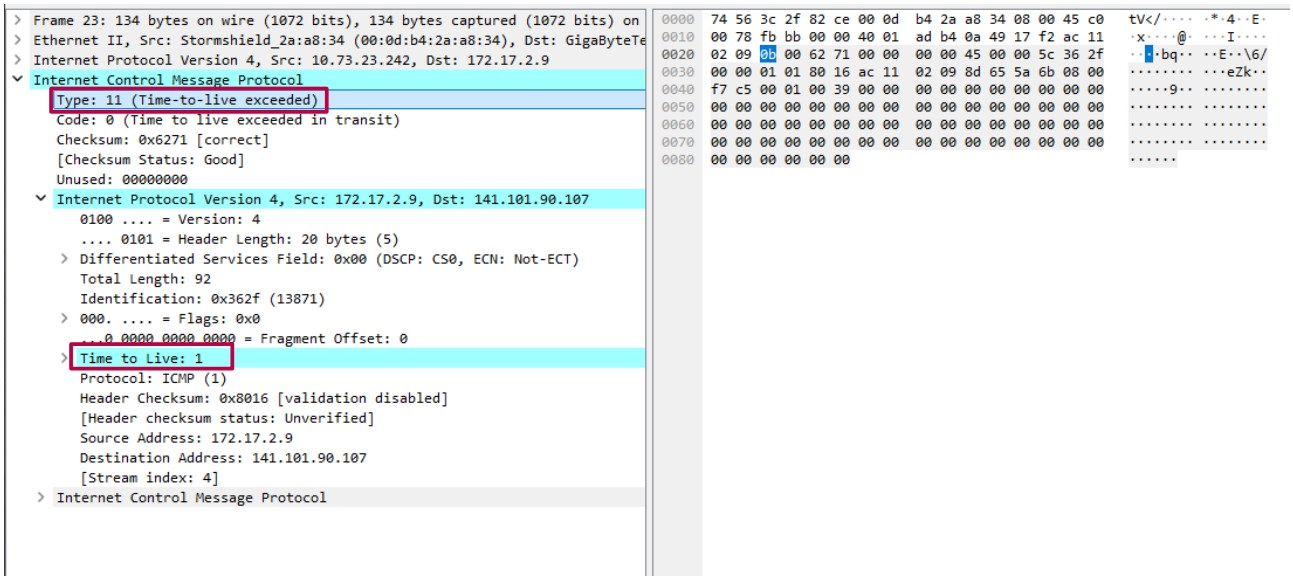


Capture 18

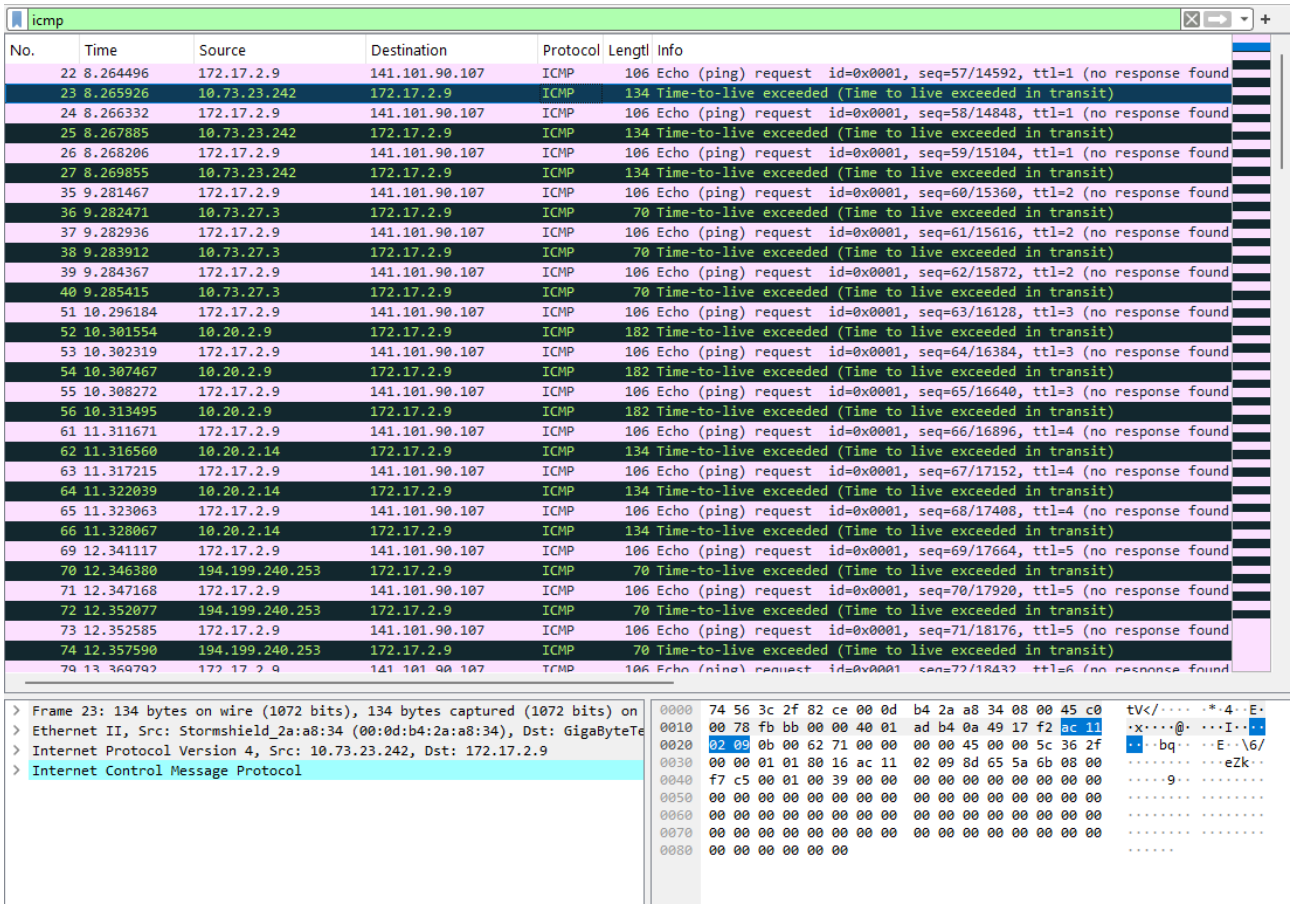
<u>---Quelle est la valeur portée par le champ Type ?</u>

Valeur décimal : 8 Valeur hexadécimal : 0x08

On sélectionne la trame comportant un message d'erreur ICMP Time-to-live exceeded. On développe la section correspondant au message ICMP (Capture 19).



Capture 19



Capture 19

---Quelle est la valeur portée par le champ Type ?

Valeur décimal : 11 Valeur Hexadécimal : 0x0B