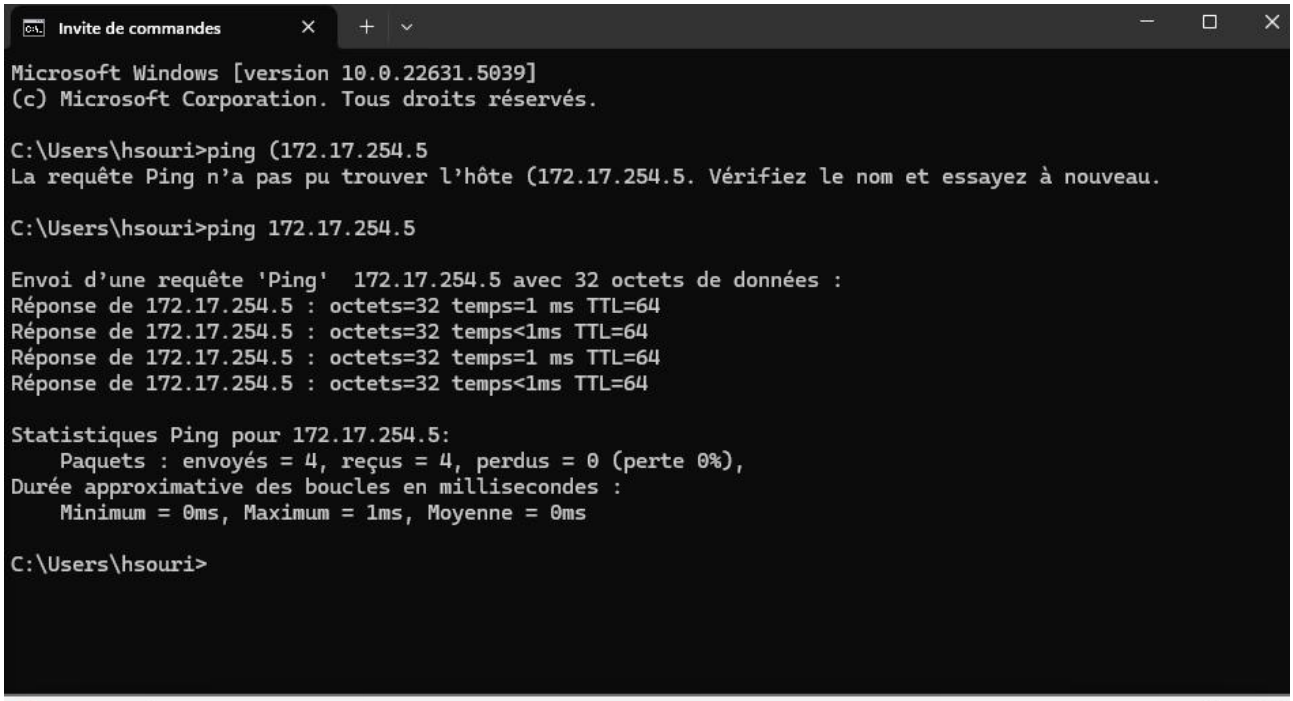
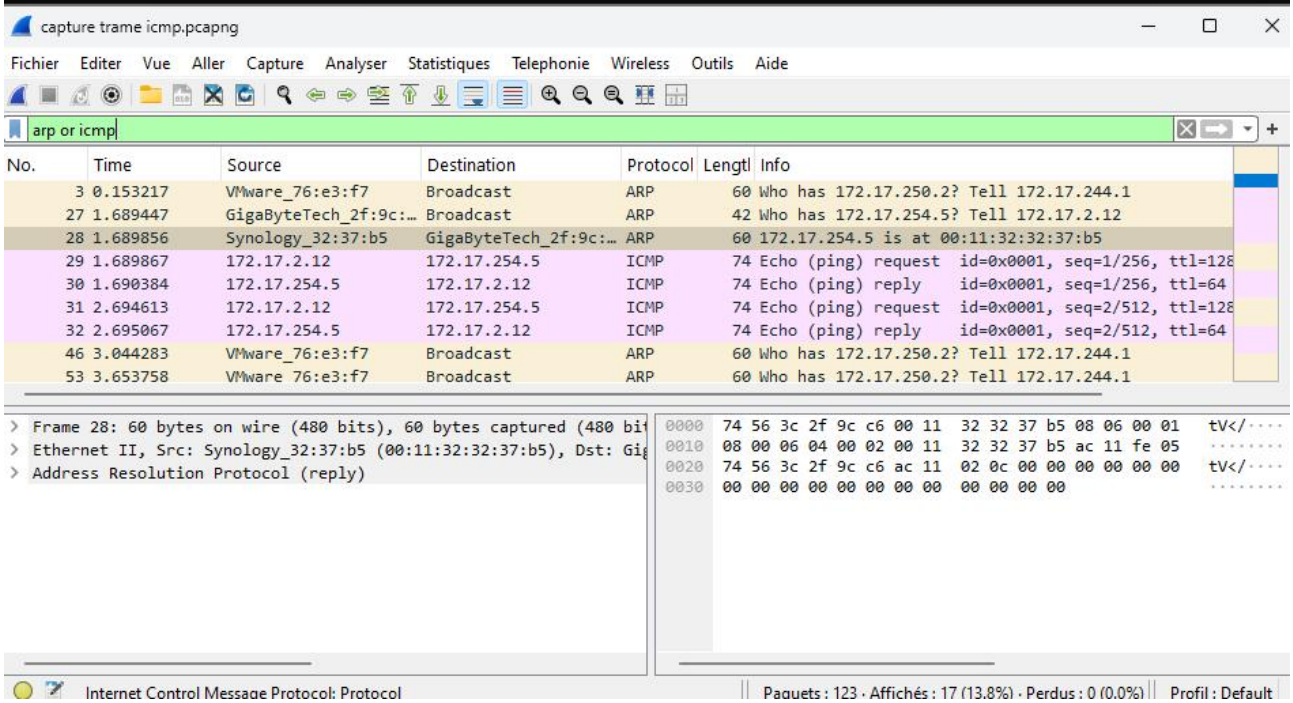
TP 5 – Trames ARP, ICMP et DNS

Sommaire

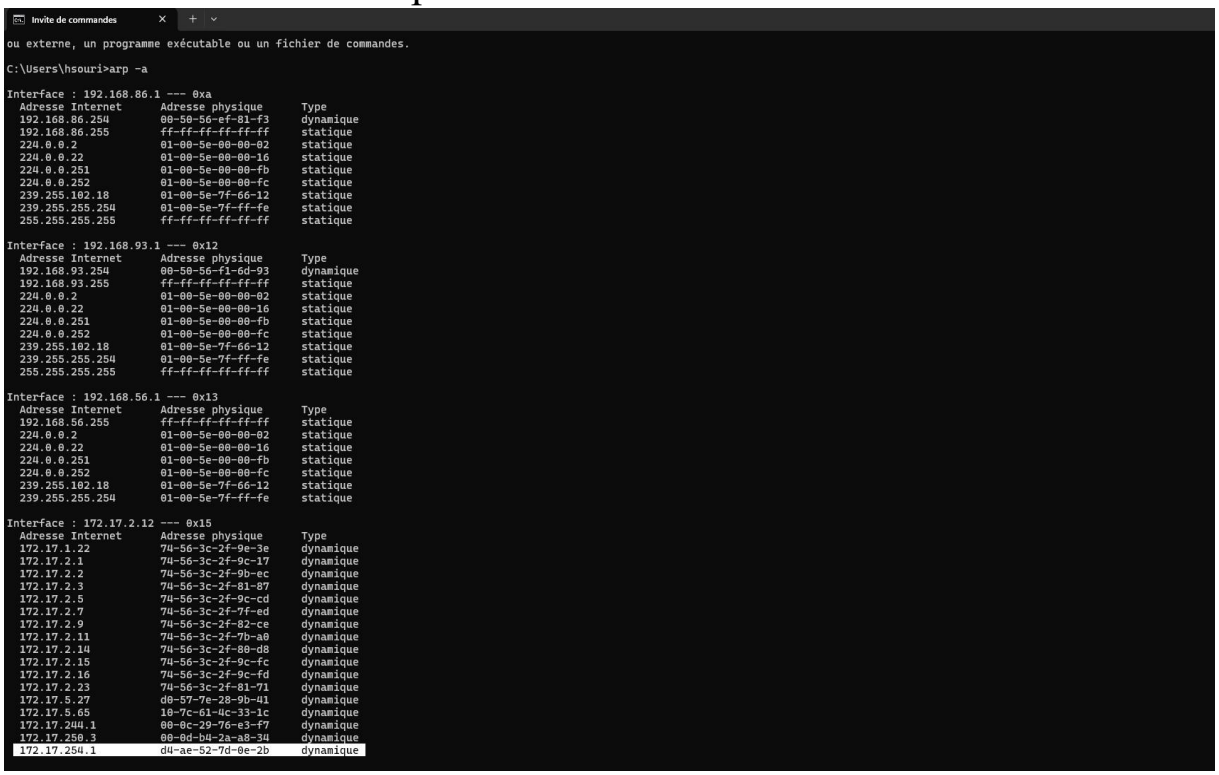
4.1. Capture de trames ARP et ICMP.





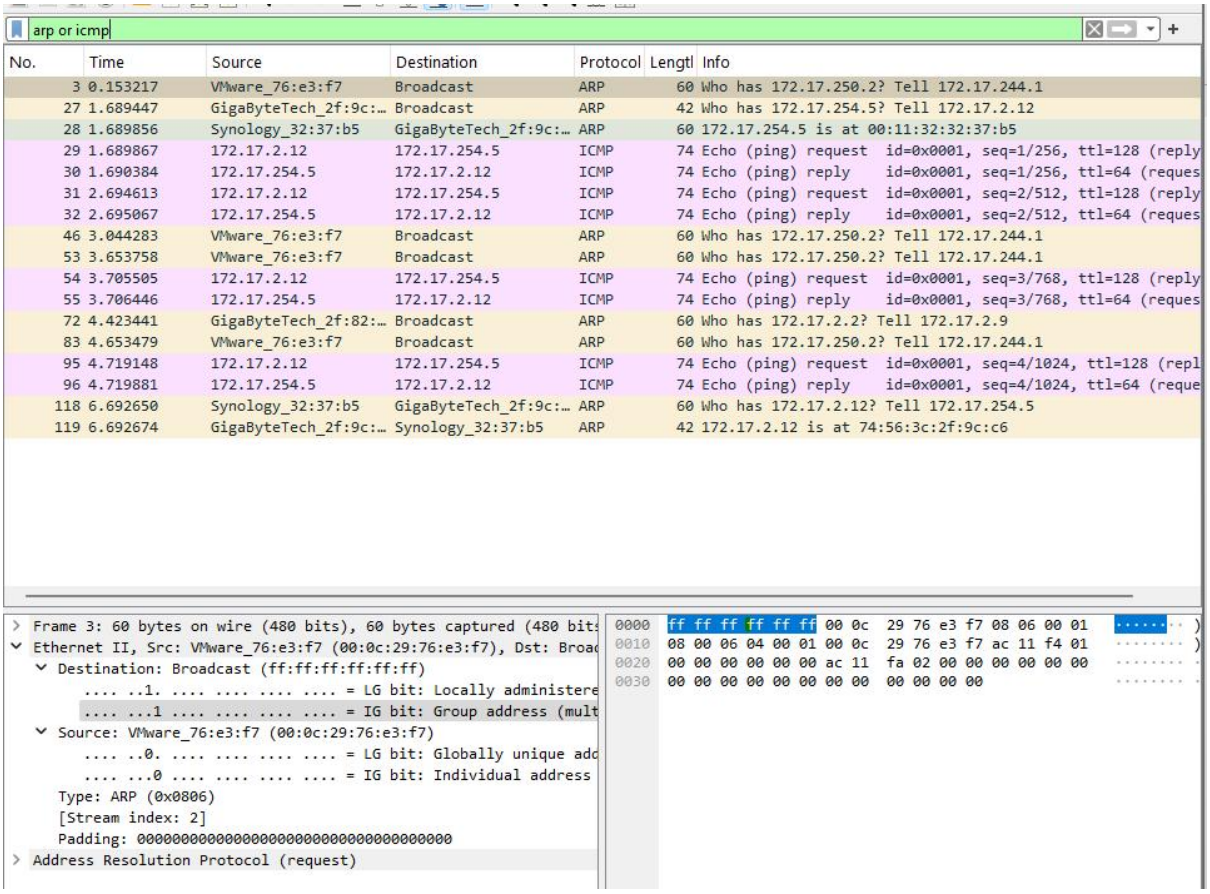
TP 5 – Trames ARP, ICMP et DNS

J’ai pinguez le serveur Aviateur (172.17.254.5) et fait une ca pture de trame avec un filtre icmp



```
Invite de commandes
ou externe, un programme exécutable ou un fichier de commandes.

C:\Users\hsouri>arp -a

Interface : 192.168.86.1 --- 0xa
  Adresse Internet      Adresse physique      Type
  192.168.86.254        00-50-56-ef-81-f3     dynamique
  192.168.86.255        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
  239.255.102.18        01-00-5e-7f-66-12     statique
  239.255.255.254       01-00-5e-7f-ff-fe     statique
  255.255.255.255       ff-ff-ff-ff-ff-ff     statique

Interface : 192.168.93.1 --- 0x12
  Adresse Internet      Adresse physique      Type
  192.168.93.254        00-50-56-f1-6d-93     dynamique
  192.168.93.255        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
  239.255.102.18        01-00-5e-7f-66-12     statique
  239.255.255.254       01-00-5e-7f-ff-fe     statique
  255.255.255.255       ff-ff-ff-ff-ff-ff     statique

Interface : 192.168.56.1 --- 0x13
  Adresse Internet      Adresse physique      Type
  192.168.56.255        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
  239.255.102.18        01-00-5e-7f-66-12     statique
  239.255.255.254       01-00-5e-7f-ff-fe     statique

Interface : 172.17.2.12 --- 0x15
  Adresse Internet      Adresse physique      Type
  172.17.1.22           74-56-3c-2f-9e-3e     dynamique
  172.17.2.1            74-56-3c-2f-9c-17     dynamique
  172.17.2.2            74-56-3c-2f-9b-ec     dynamique
  172.17.2.3            74-56-3c-2f-81-87     dynamique
  172.17.2.5            74-56-3c-2f-9c-cd     dynamique
  172.17.2.7            74-56-3c-2f-7f-ed     dynamique
  172.17.2.9            74-56-3c-2f-82-ce     dynamique
  172.17.2.11           74-56-3c-2f-7b-a0     dynamique
  172.17.2.14           74-56-3c-2f-80-d8     dynamique
  172.17.2.15           74-56-3c-2f-9c-fc     dynamique
  172.17.2.16           74-56-3c-2f-9c-fd     dynamique
  172.17.2.23           74-56-3c-2f-81-71     dynamique
  172.17.5.27           d0-57-7e-28-9b-41     dynamique
  172.17.5.65           10-7c-61-4c-33-1c     dynamique
  172.17.244.1          00-0c-29-76-e3-f7     dynamique
  172.17.250.3          00-0d-b4-2a-a8-34     dynamique
  172.17.254.1          d4-ae-52-7d-0e-2b     dynamique
```

j’ai réaliser une commande, arp -a pour vérifier la présence de l’association @IP-@MAC correspondant à Aviateur



```
arp or icmp

No.  Time      Source              Destination         Protocol Lengtl Info
     3 0.153217 VMware_76:e3:f7     Broadcast           ARP        60 Who has 172.17.250.2? Tell 172.17.244.1
    27 1.689447 GigaByteTech_2f:9c:… Broadcast          ARP        42 Who has 172.17.254.5? Tell 172.17.2.12
    28 1.689856 Synology_32:37:b5   GigaByteTech_2f:9c:… ARP        60 172.17.254.5 is at 00:11:32:32:37:b5
    29 1.689867 172.17.2.12         172.17.254.5        ICMP       74 Echo (ping) request  id=0x0001, seq=1/256, ttl=128 (reply
    30 1.690384 172.17.254.5        172.17.2.12         ICMP       74 Echo (ping) reply    id=0x0001, seq=1/256, ttl=64 (reques
    31 2.694613 172.17.2.12         172.17.254.5        ICMP       74 Echo (ping) request  id=0x0001, seq=2/512, ttl=128 (reply
    32 2.695067 172.17.254.5        172.17.2.12         ICMP       74 Echo (ping) reply    id=0x0001, seq=2/512, ttl=64 (reques
    46 3.044283 VMware_76:e3:f7     Broadcast           ARP        60 Who has 172.17.250.2? Tell 172.17.244.1
    53 3.653758 VMware_76:e3:f7     Broadcast           ARP        60 Who has 172.17.250.2? Tell 172.17.244.1
    54 3.705505 172.17.2.12         172.17.254.5        ICMP       74 Echo (ping) request  id=0x0001, seq=3/768, ttl=128 (reply
    55 3.706446 172.17.254.5        172.17.2.12         ICMP       74 Echo (ping) reply    id=0x0001, seq=3/768, ttl=64 (reques
    72 4.423441 GigaByteTech_2f:82:… Broadcast          ARP        60 Who has 172.17.2.2? Tell 172.17.2.9
    83 4.653479 VMware_76:e3:f7     Broadcast           ARP        60 Who has 172.17.250.2? Tell 172.17.244.1
    95 4.719148 172.17.2.12         172.17.254.5        ICMP       74 Echo (ping) request  id=0x0001, seq=4/1024, ttl=128 (repl
    96 4.719881 172.17.254.5        172.17.2.12         ICMP       74 Echo (ping) reply    id=0x0001, seq=4/1024, ttl=64 (reque
   118 6.692650 Synology_32:37:b5   GigaByteTech_2f:9c:… ARP        60 Who has 172.17.2.12? Tell 172.17.254.5
   119 6.692674 GigaByteTech_2f:9c:… Synology_32:37:b5  ARP        42 172.17.2.12 is at 74:56:3c:2f:9c:c6

> Frame 3: 60 bytes on wire (480 bits), 60 bytes captured (480 bits
v Ethernet II, Src: VMware_76:e3:f7 (00:0c:29:76:e3:f7), Dst: Broad
  v Destination: Broadcast (ff:ff:ff:ff:ff:ff)
      .... ..1. .... .... .... .... = LG bit: Locally administere
      .... ...1 .... .... .... .... = IG bit: Group address (mult
  v Source: VMware_76:e3:f7 (00:0c:29:76:e3:f7)
      .... ..0. .... .... .... .... = LG bit: Globally unique add
      .... ...0 .... .... .... .... = IG bit: Individual address
    Type: ARP (0x0806)
    [Stream index: 2]
    Padding: 00000000000000000000000000000000000000
> Address Resolution Protocol (request)

0000  ff ff ff ff ff ff 00 0c  29 76 e3 f7 08 06 00 01   ........ )vc.....
0010  08 00 06 04 00 01 00 0c  29 76 e3 f7 ac 11 f4 01   ........ )v......
0020  00 00 00 00 00 00 ac 11  fa 02 00 00 00 00 00 00   ........ ........
0030  00 00 00 00 00 00 00 00  00 00 00 00               ........ ....
```

TP 5 – Trames ARP, ICMP et DNS

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

C'est le champ EtherType = 0x0806, ce qui signifie ARP.

Quelle est la fonction de la trame ARP Request ?

C'est une requête pour trouver l'adresse client elle demande :(who has «IP cible»?) et(tell «IP source») pour découvrir l'adresse MAC associée a l'adresse IP

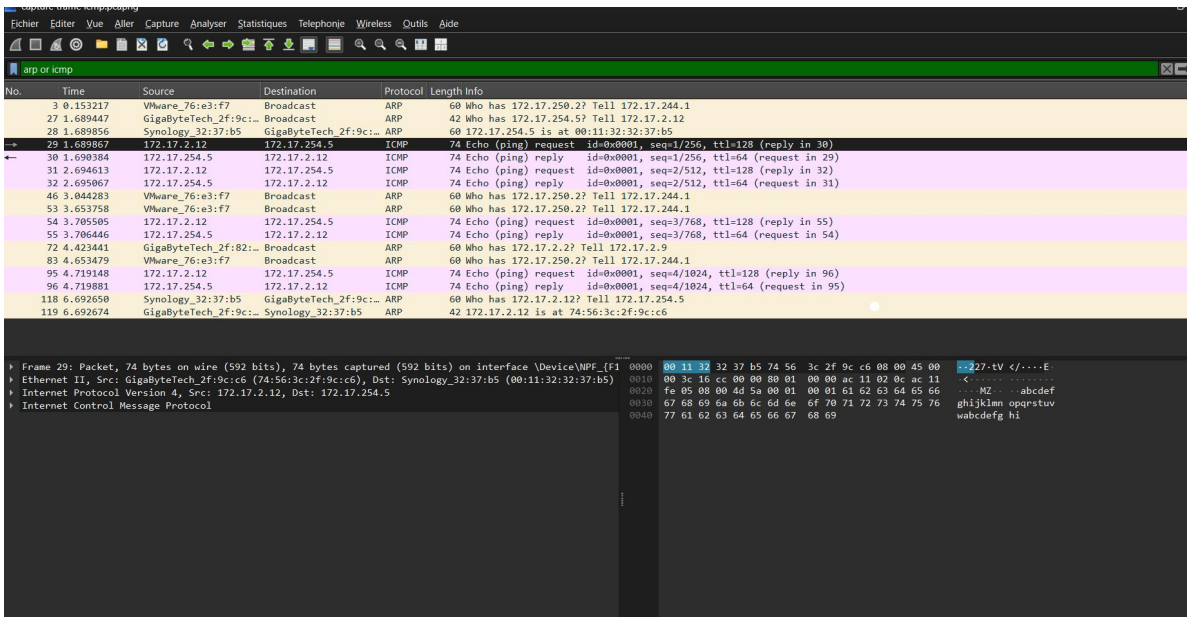
Quelle signification ont les octets de position 0×04 et 0×05 ligne 0010 ?

Ces les octets 0x 00 01 c'est l'Opcode=0x00 01 donc une ARP Request

Quelle est la longueur d'un message ARP contenu dans la trame ? 28 octets
Quelle est la longueur de la trame ARP Request ? 60 octets
Quelle est la longueur de la trame ARP Reply ? 42 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 = 00:0c:29:76:e3:f7 Ethernet Type = 0x0806
Opcode (valeurs hexa.) =0x0001 @MAC de la cible = 00:00:00:00:00:00 @IP de la cible = 172.17.250.2



TP 5 – Trames ARP, ICMP et DNS

Quelle signification ont les octets de position 0×0C et 0×0D ligne 0000 ?
C'est le champ Ethertype =0x0800 ce qui signifie IPv4

Quelle signification a l'octet de position 0×07 ligne 0010 ?
C'est le 2eme octet de l'adresse MAC source ,
0x56 (6 octets source = 74:56:3c:2f:9c:c6).

Quelle est la longueur de la trame ? 74 octets (74 bytes on wire)

Quelle est la longueur du paquet IP ? 60 octets

Quelle est la longueur du message ICMP ? 40 octets (60 − 20 octets d'en-tête IP = 40).

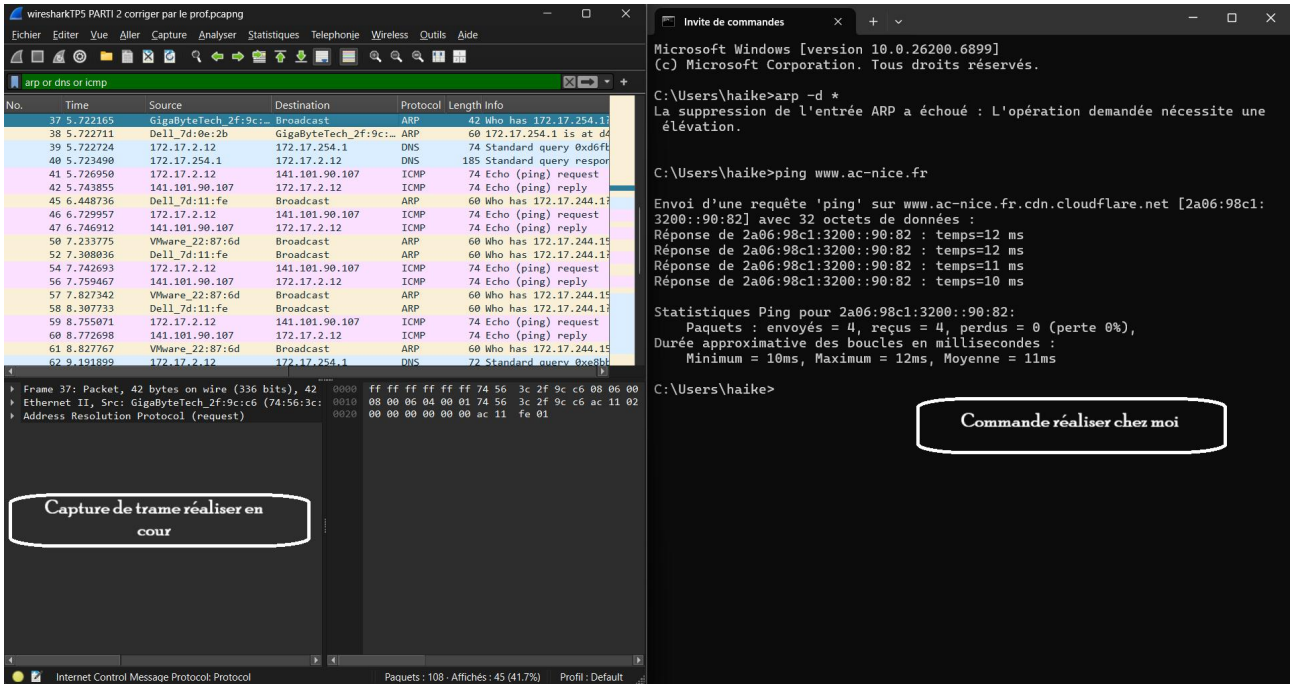
Quelle signification a l'octet de position 0×02 ligne 00020 ?
C'est une trame de type ICMP echo request

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

Sélectionnez une trame ICMP Echo Reply. Quelle est le nom et la valeur de l'octet de position 0×02 ligne 00020 ?
C'est un octet de position de type (ICMP) et l'octet 0x03 signifie que c'est une trame ICMP type 0 = echo reply

4.2. Capture de trames ARP, DNS et ICMP

TP 5 – Trames ARP, ICMP et 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 rechercher est 172.17.254.1

Trame ARP request
@MAC destination = ff:ff:ff:ff:ff:ff @MAC source = 74:56:3c:2f:7f:bf Ethernet Type =0x0806 (arp)
Opcode (valeurs hexa.) = 0000 (request) @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 ?

TP 5 – Trames ARP, ICMP et DNS

Avant d'envoyer les trames ICMP la machine doit savoir vers quel adresse IP l'envoyer, c'est le DNS qui s'en occupe

▪ 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 :
J'ai effectué la commande :

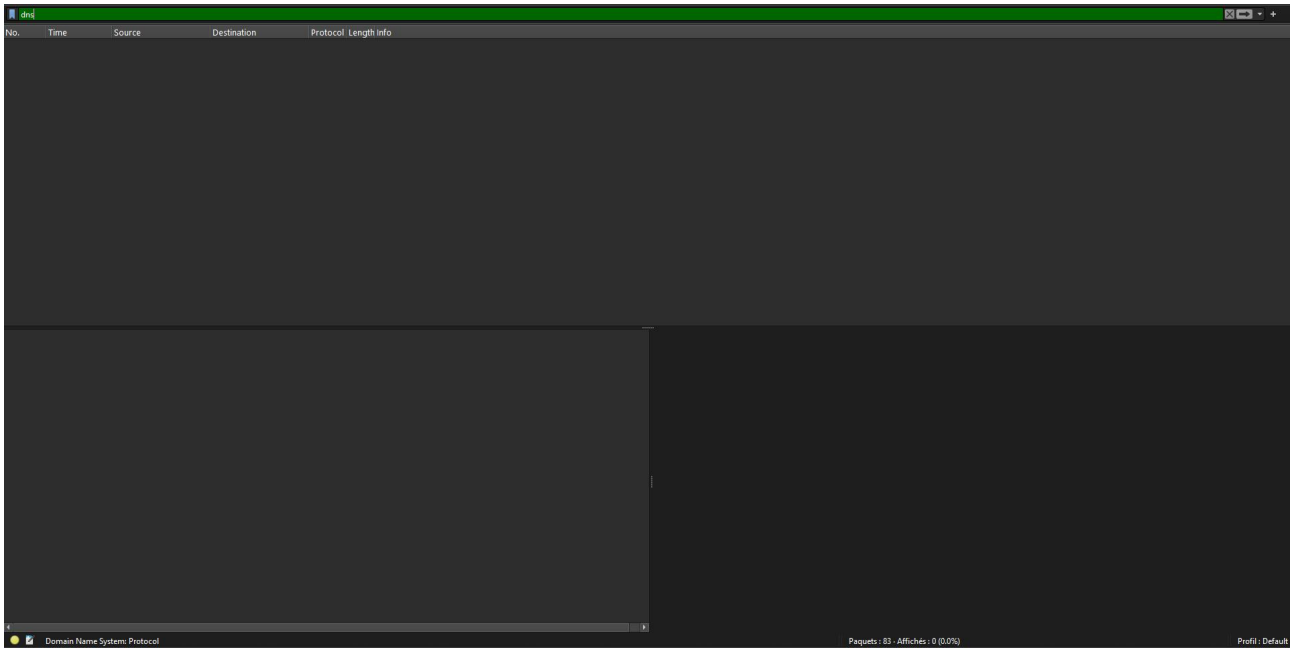
```
C:\Users\haike>ipconfig /displaydns
```

Et je cherche la présence de l'enregistrement DNS

```
www.ac-nice.fr
----------------------------------------
Nom d'enregistrement. : www.ac-nice.fr
Type d'enregistrement : 5
Durée de vie  . . . . : 87273
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  . . . . : 87273
Longueur de données . : 4
Section . . . . . . . : Réponse
Enregistrement (hôte) : 141.101.90.107
```

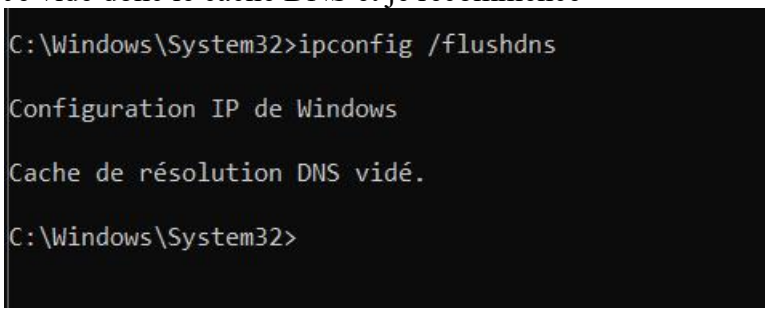
Je démarre une nouvelle capture et je ressaisie la commande ping www.ac-nice.fr

TP 5 – Trames ARP, ICMP et DNS

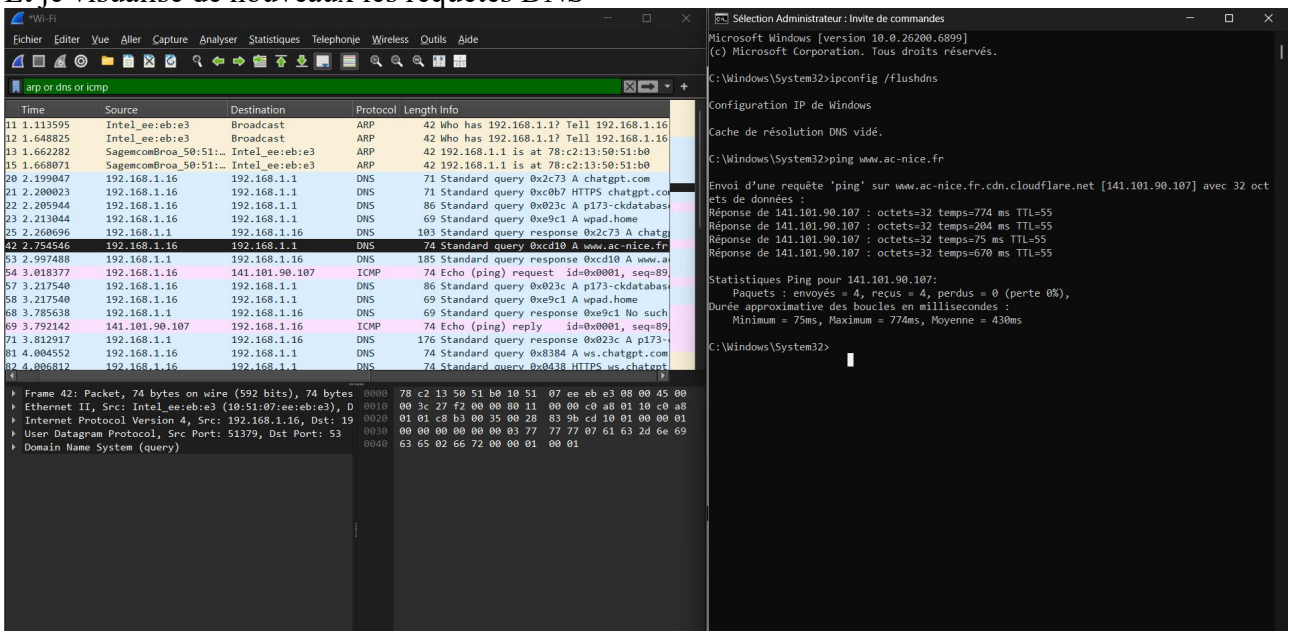


Je constate qu'il na pas de DNS

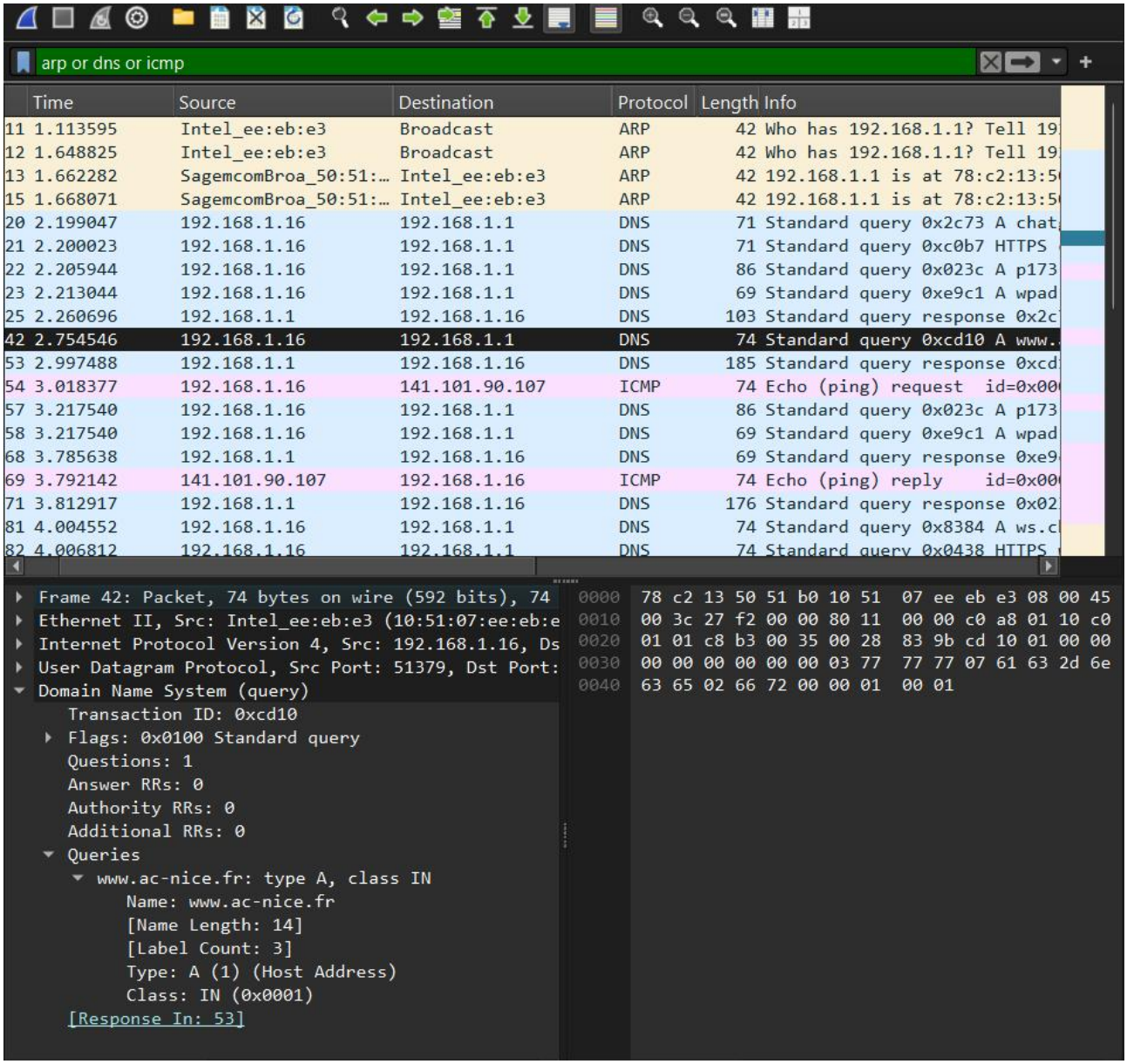
Je vide donc le cache DNS et je recommence



Et je visualise de nouveaux les requêtes DNS



TP 5 – Trames ARP, ICMP et DNS



Quels sont les différents protocoles encapsulés dans une trame DNS ?
Ethernet ,IP, UDP, DNS

Quelle est la machine destinataire de la requête DNS ? Quelle est son IP (cf. en-tête IP) ?
Destination IP : 192.168.1.1

Quelle signification ont les octets de position 0×0C, 0×0D ligne 0000 et 0×07 ligne 0010 ?
C'est l'EtherType = 0x0800 → protocole IPv4 et le datagram UDP

- Quelle est la longueur de l'en-tête IP ?

20 octets

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

UDP=8octets

TP 5 – Trames ARP, ICMP et DNS

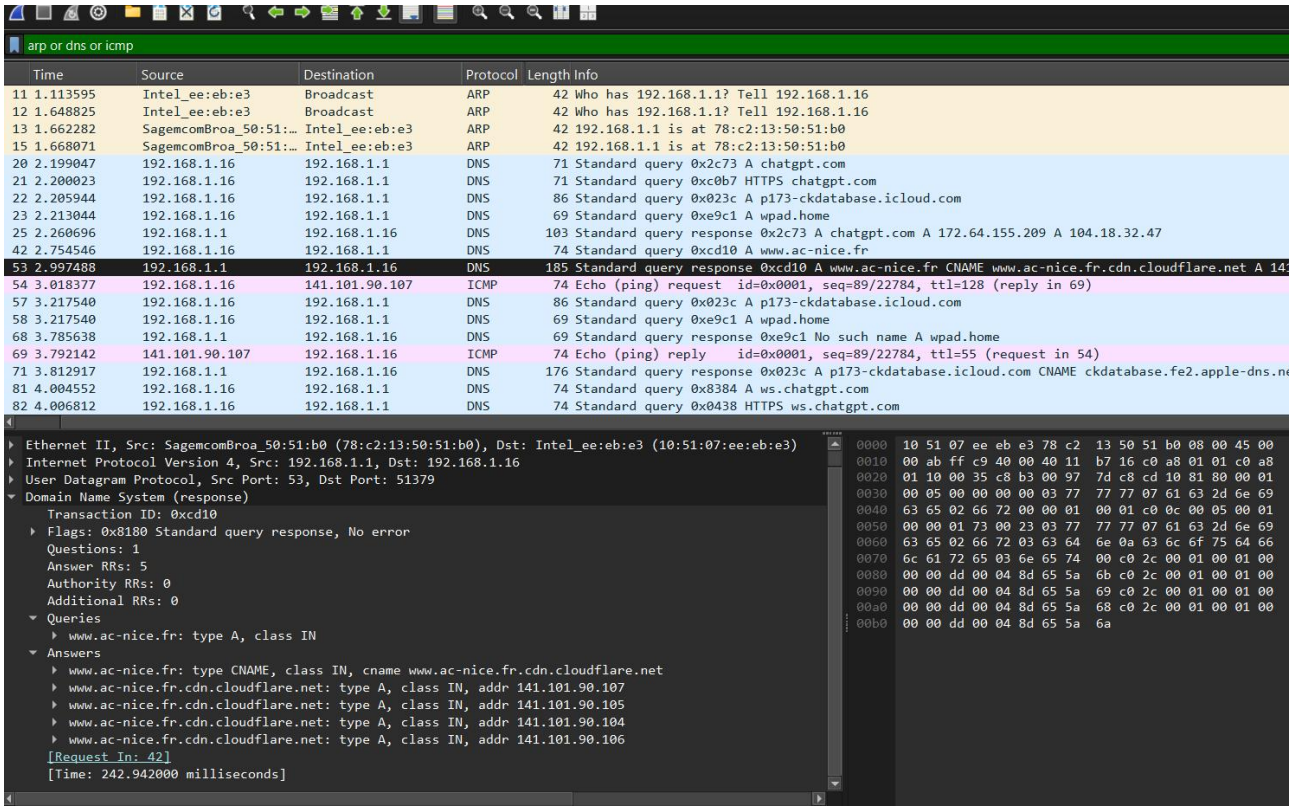
- Quelle signification ont les octets de position 0×04 et 0×05 ligne 0020 ?

0x0035 = 53 → Port DNS standard (UDP/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 ac nice.fr ?
La valeur en Hexa du nom de domaine est 07 61 63 2d 6e 69 63 65 02 66 72 00 = ac nice.fr et 03 77 77 77 07 61 63 2d 6e 69 63 65 02 66 72 00 = www.ac-nice.fr

▪ 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.

Je sélectionne la trame comportant la trame DNS et plus précisément la réponse a la requete DNS

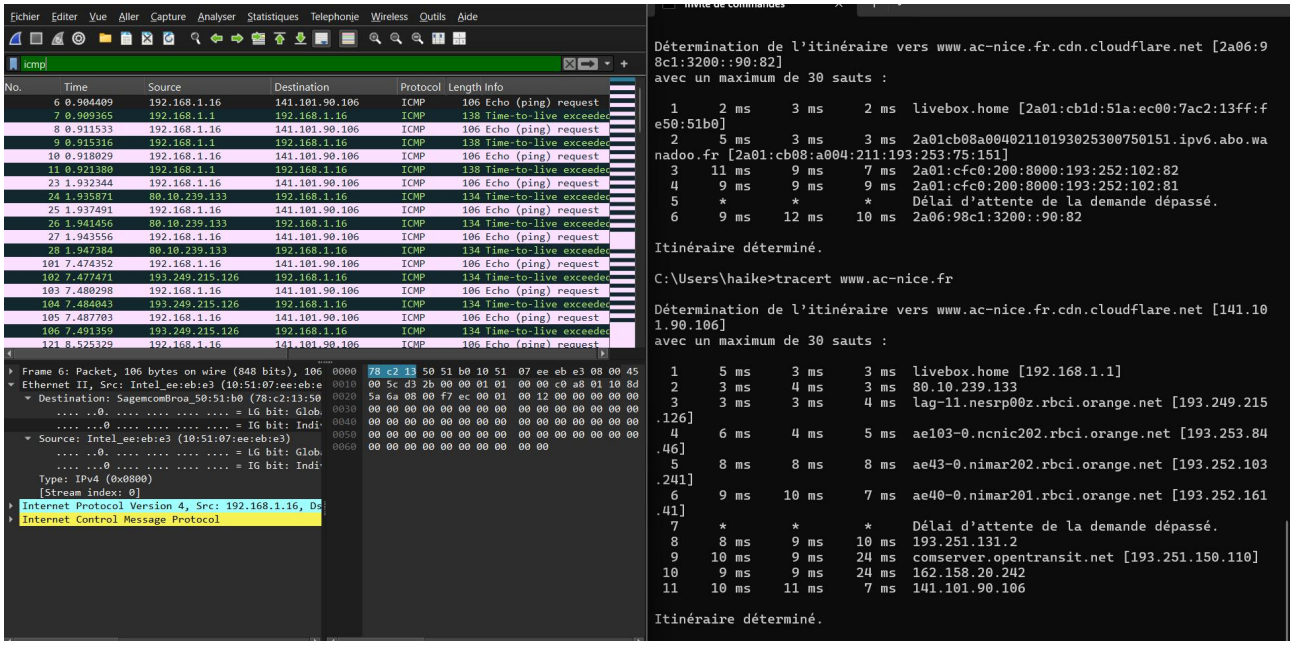


Je constate plusieur adresse IP :

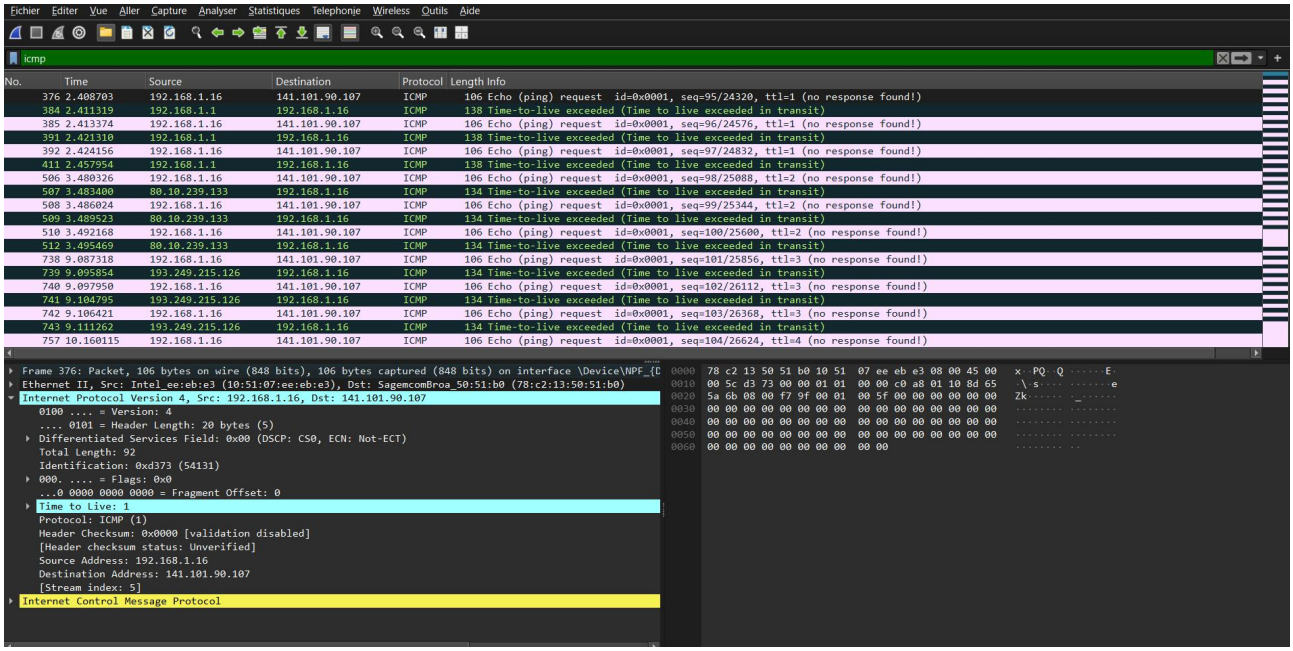
- Décimal : 141.101.90.104 → 141.101.90.107
- Hexadécimal : 8D.65.5A.68 → 8D.65.5A.6B

4.3. Commande Tracert et capture de trames ICMP.

Je saisie la commande tracert et obient cette trame



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

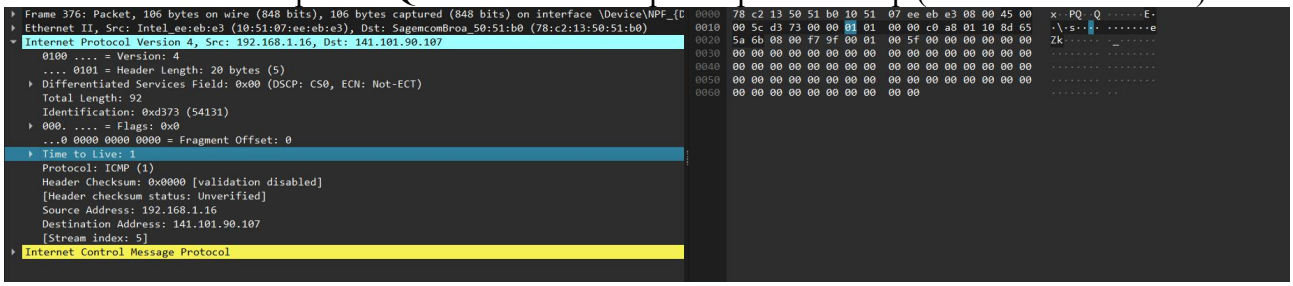


- Decimale: 141.101.90.107

- Hexadecimale: 0x 8d 65 5a 6b

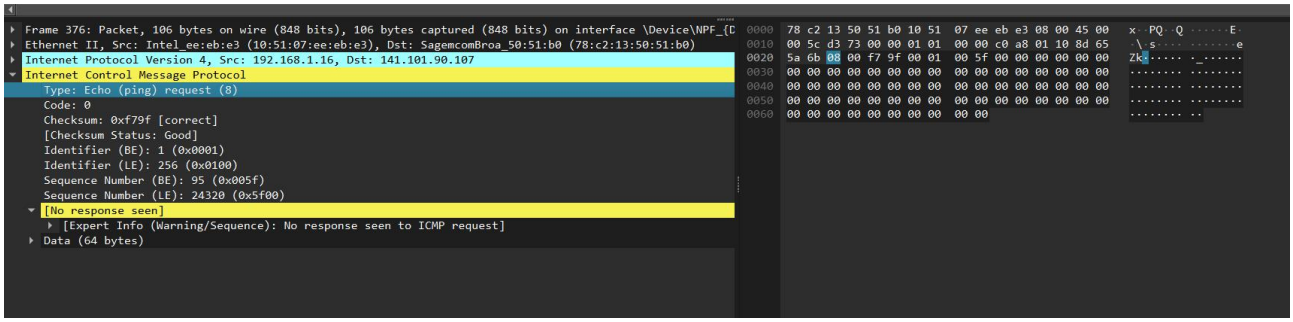
TP 5 – Trames ARP, ICMP et DNS

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



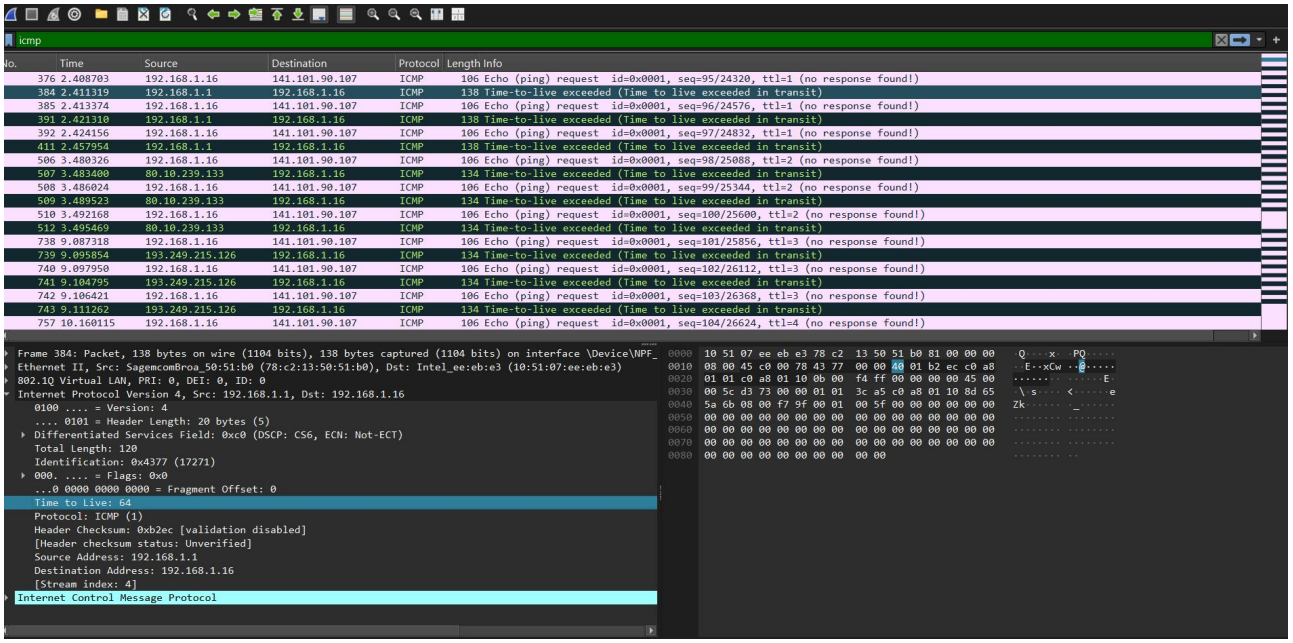
-Decimale: 1
-Hexadecimale: 0x 01

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



-Decimale:8
-Hexadecimales:0x08

▪ 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.) ?



-Decimale:64

-Hexadecimale:0x40