Diana Margarian 22 octobre 2023

TP 5 : TRAMES ARP, ICMP ET DNS

Sommaire : COMPTE RENDU

4.1 Capture de trames ARP et ICMP

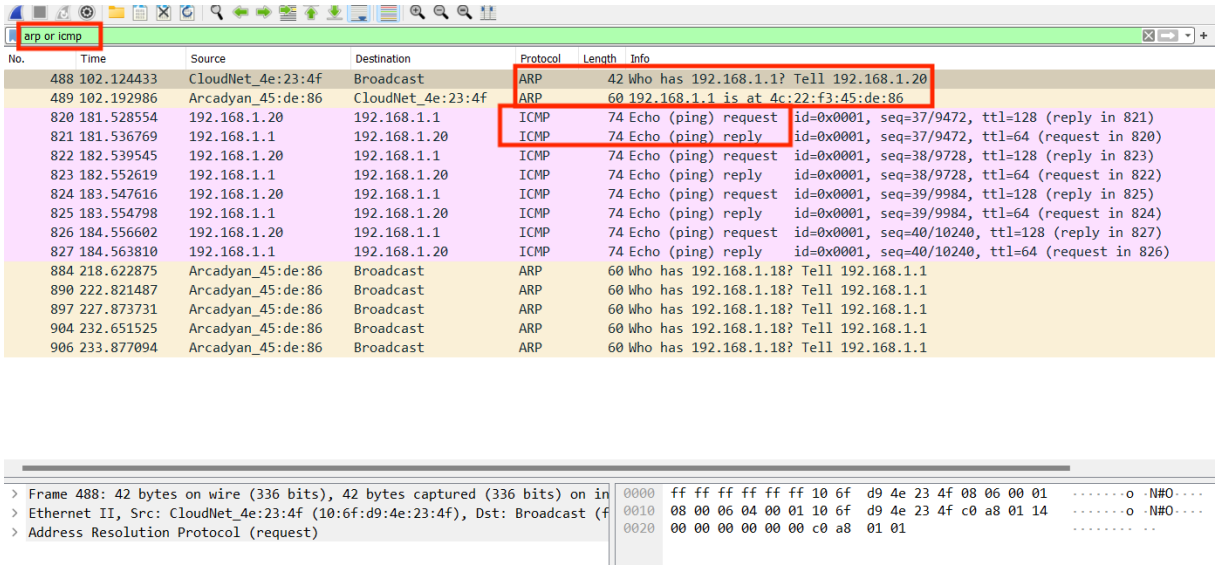
Capture des trames ICMP par la saisie d'une commande ping depuis votre machine physique.

→ J'ai ouvert Wireshark, en sélectionnant ma carte réseau et j'ai démarré une capture de trames.

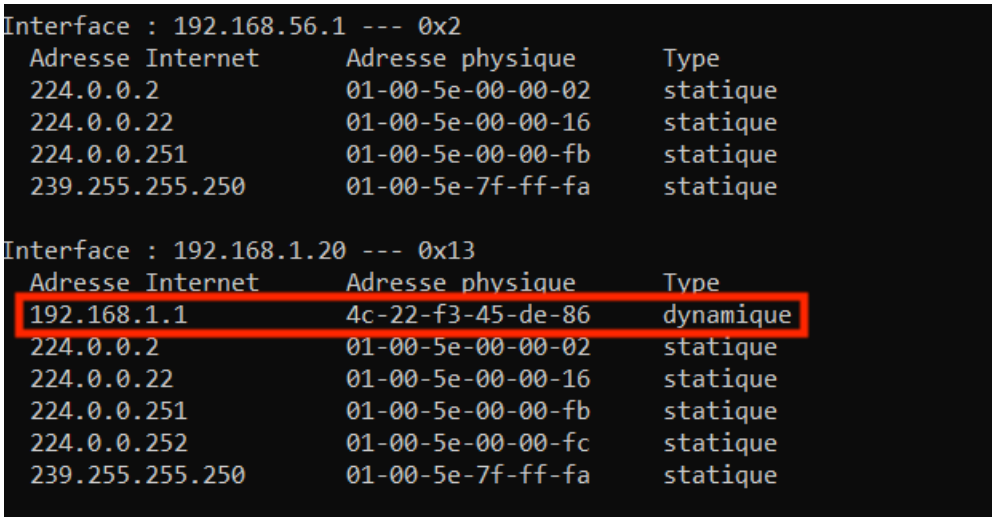
➔ J'ai ensuite ping mon routeur :

```
C:\Windows\System32> ping 192.168.1.1

Envoi d'une requête 'Ping'  192.168.1.1 avec 32 octets de données :
Réponse de 192.168.1.1 : octets=32 temps=8 ms TTL=64
Réponse de 192.168.1.1 : octets=32 temps=13 ms TTL=64
Réponse de 192.168.1.1 : octets=32 temps=7 ms TTL=64
Réponse de 192.168.1.1 : octets=32 temps=7 ms TTL=64

Statistiques Ping pour 192.168.1.1:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 7ms, Maximum = 13ms, Moyenne = 8ms

C:\Windows\System32>
```

➔ L'échange démarre avec une requête et une réponse ARP pour l'adresse MAC du serveur. Ensuite l'échange de trames ICMP a lieu. J'ai arrêté la capture car les 8 trames ICMP sont obtenues :



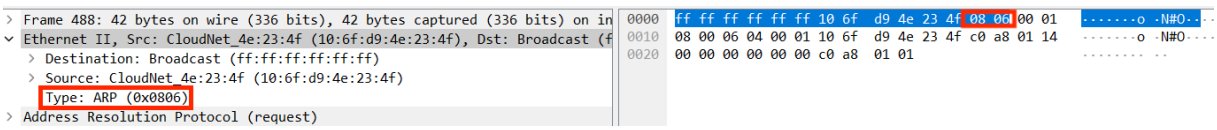
➔ Après la saisie de la commande ping, j'ai consulté le contenu du cache ARP et vérifiez la présence de l'association @IP-@MAC correspondant à mon routeur.



Analyse l'échange de trames ARP précédant l'échange de trames ICMP :

- Quelle signification ont les octets de position 0xOC et OxOD ligne 0000 ?

  Les octets de position 0x0C et 0x0D ligne 0000 ont pour signification le champ Ethertype (0806) qui correspond à ARP :

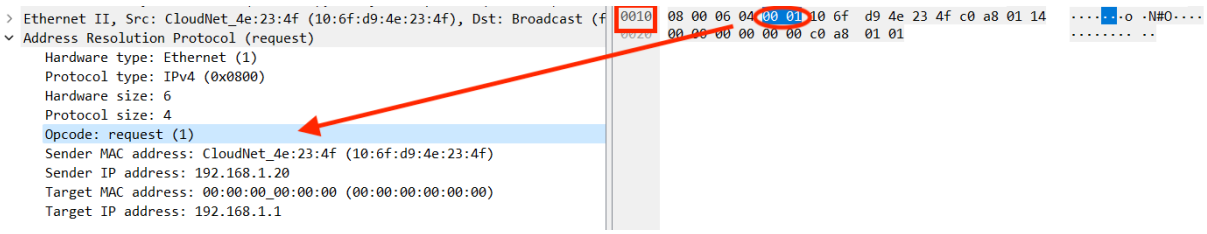


- Quelle est la fonction de la trame ARP Request ?

La fonction de la trame ARP REQUEST est d'envoyer en broadcast. Pour permettre de dire à qui correspond cette @IP. Son but est de recevoir l'adresse MAC de celle qui détient @IP.

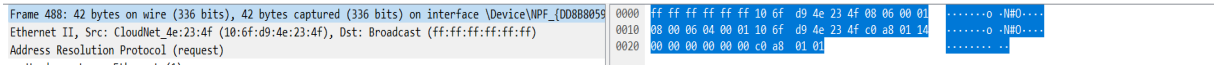
- Quelle signification ont les octets de position Ox04 et 0x05 ligne 0010 ?

La signification des octets position Ox04 et Ox0S ligne 0010 est l'Opcode, elle est pour but de demander l'adresse @MAC à partir d'une adresse IP (00 01).



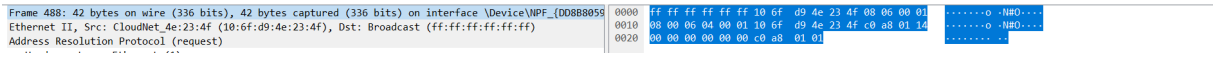
- Quelle est la longueur d'un message ARP contenu dans la trame ?

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



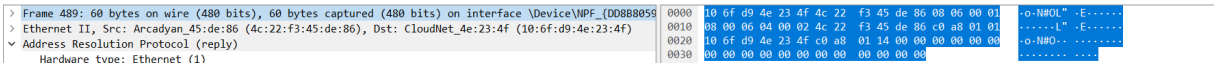
- Quelle est la longueur de la trame ARP Request ?

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 42 octets.



- Combien d'octets sont utilisés pour le padding ?

Aucune padding utilisé. (000000000000000…)

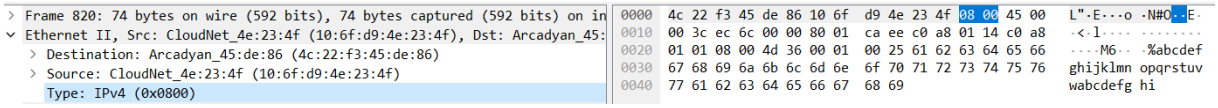
->

Trame ARP request
@MAC destination = ff : ff : ff : ff : ff : ff @MAC source = 10 6f d9 4e 23 4f Ethernet Type = 00 01
Opcode (valeurs hexa.) = 00 01 @MAC de la cible = 00 : 00 : 00 : 00 : 00 : 00 @IP de la cible = 192.168.1.1

J'ai sélectionné une trame ICMP Echo Request.

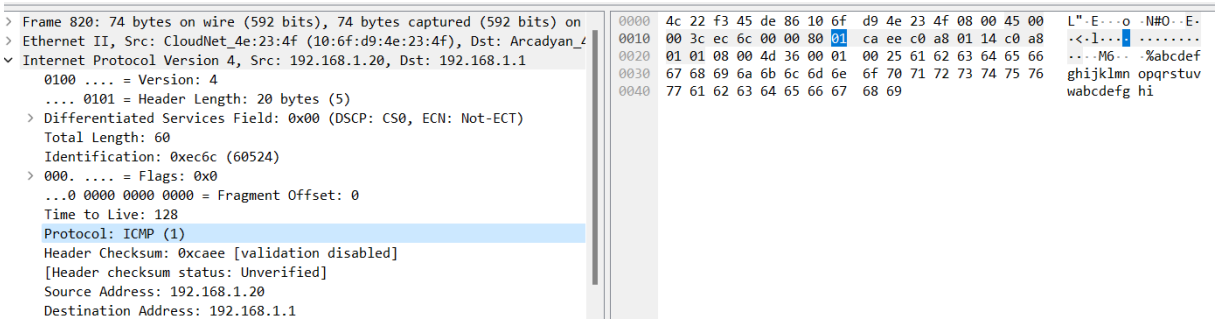
- Quelle signification ont les octets de position 0x0C et 0xOD ligne 0000 ?

  La signification de ces octets de position se reposent au champ Ethertype 08 00 qui correspond à l'IPv4.



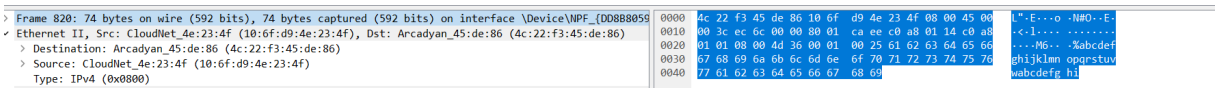
- Quelle signification a l'octet de position 0x07 ligne 0010 ?

  La signification a l'octet de position 0x07 ligne 0010 se reposent au protocole utiliser ICMP (1).



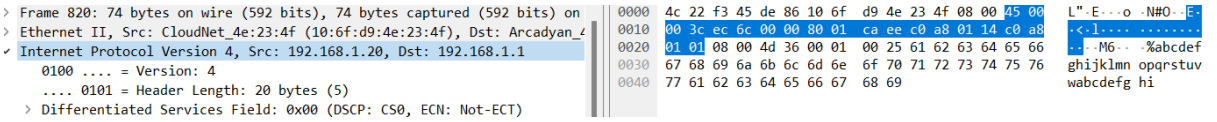
- Quelle est la longueur de la trame ?

  La longueur de la trame est de 74 octets.



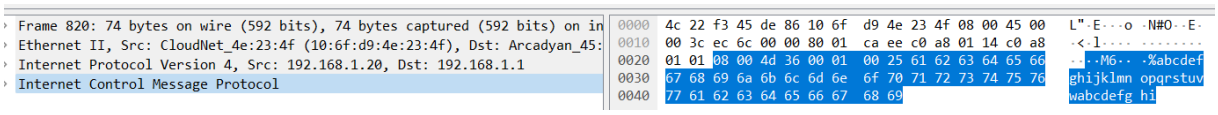
- Quelle est la longueur du paquet IP ?

La longueur du paquet IP est de 20 octets.



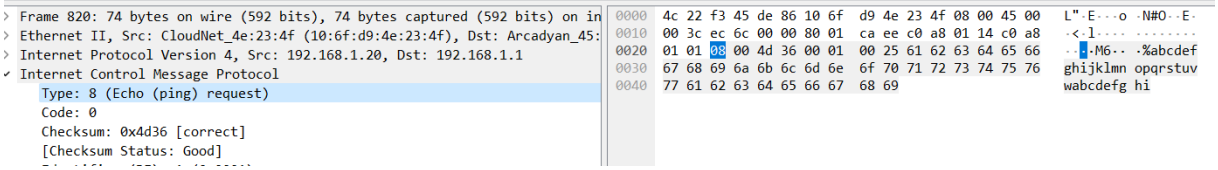
- Quelle est la longueur du message ICMP ?

La longueur du message ICMP est de 40 octets.

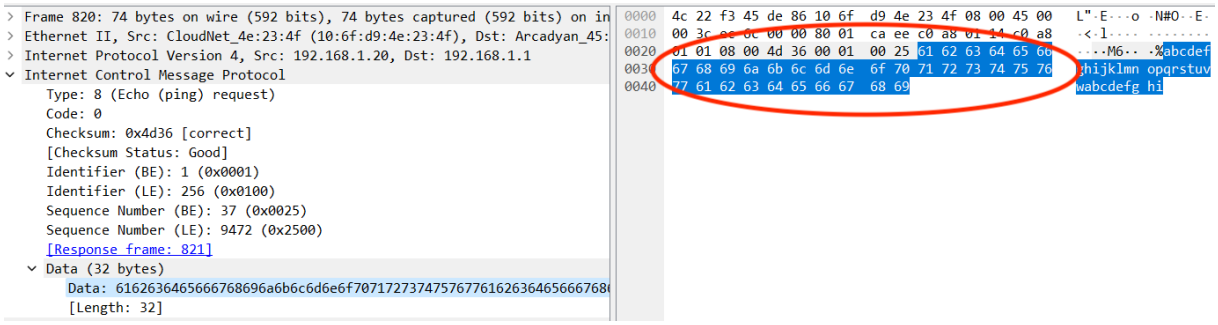


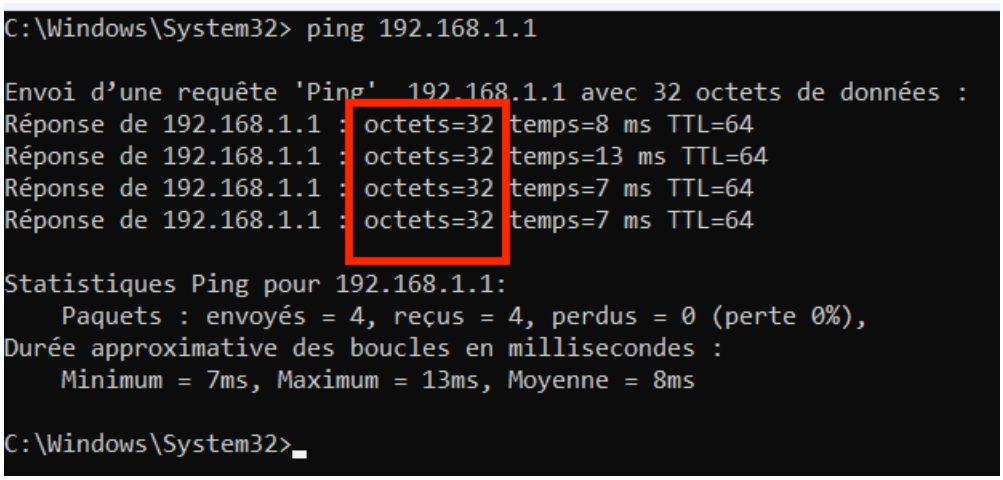
- Quelle signification a l'octet de position 0x02 ligne 0020 ?

La signification de l'octet de position 0x02 ligne 0020 correspond au type de message.



- A quoi correspondent les octets à partir de l'octet 0xOA, ligne 0020 ?

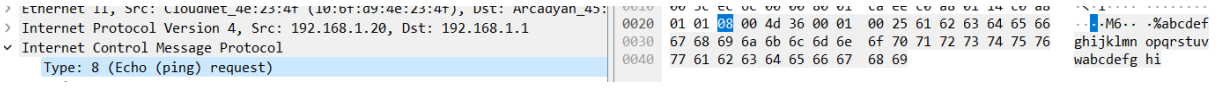




Je remarque que les octets correspondent à la commande PING que l'on retrouve dans l'invite de commande.

Quelle est le nom et la valeur de l'octet de position 0x02 ligne 0020 ?

Le nom et la valeur de l'octet de position 0x02 ligne 0020 correspond au type de message (type (0)) pour ECHO ping Reply.



4.2 Capture de trames ARP, DNS et ICMP

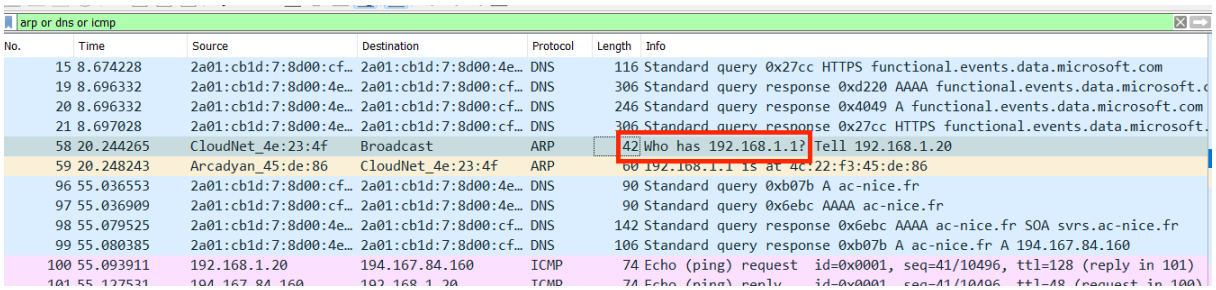
→ Démarrez une capture de trames.

→ Ouvrir l'invite de commande, videz le cache ARP, puis effectuez la requête ping vers le serveur web www.ac-nice.fr :

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

Envoi d'une requête 'ping' sur ac-nice.fr [194.167.84.160] avec 32 octets de données :
Réponse de 194.167.84.160 : octets=32 temps=33 ms TTL=48
Réponse de 194.167.84.160 : octets=32 temps=34 ms TTL=48
Réponse de 194.167.84.160 : octets=32 temps=33 ms TTL=48
Réponse de 194.167.84.160 : octets=32 temps=33 ms TTL=48

Statistiques Ping pour 194.167.84.160:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 33ms, Maximum = 34ms, Moyenne = 33ms

C:\Windows\System32>
```

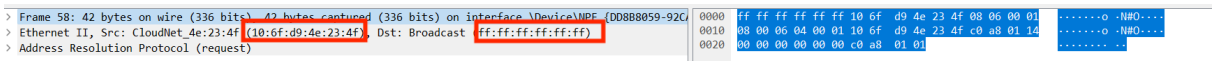
- La liste des trames commence par une requête et une réponse ARP. Quelle est l'adresse MAC recherchée ?

L'adresse MAC recherchée lors de la première trames ARP est l'adresse MAC de mon routeur 192.168.1.1.



➔

Trame ARP request
@MAC destination = ff : ff : ff : ff : ff : ff @MAC source = 10 6f d9 4e 23 4f Ethernet Type = 00 01
Opcode (valeurs hexa.) = 00 0A @MAC de la cible = 00 : 00 : 00 : 00 : 00 : 00 @IP de la cible = 192.168.1.1



- Pour quelle raison trouve-t-on ensuite une requête DNS avant l'exécution de la commande ping proprement dit ?

  DNS (Domain Name System)

  La raison pour laquelle suit une trame DNS est que pour effectuer correctement la commande PING il est nécessaire de posséder l'adresse @IP c'est là que le protocole DNS entre en jeux. Son travail est d'associer l'adresse de la page web a une adresse IP.

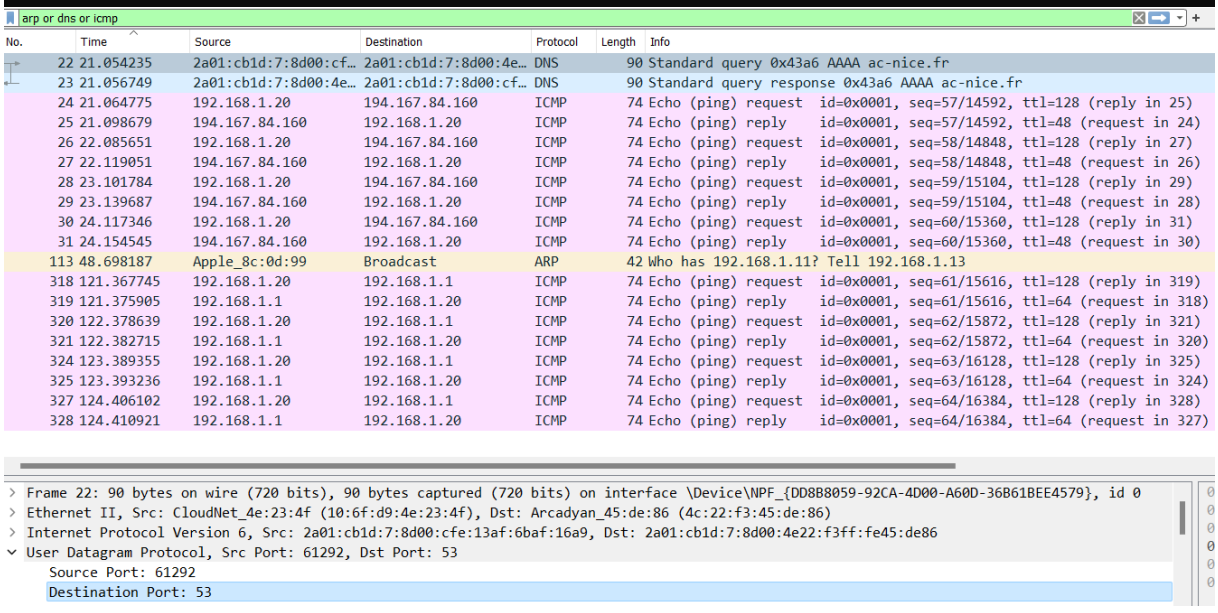
➔ J'ai consulté le cache DNS à l'aide de la commande **ipconfig /displaydns** et j'ai vérifié la présence de **l'enregistrement DNS** ac-nice.fr et de l'adresse IP associée.

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

Configuration IP de Windows

    ac-nice.fr
    ----------------------------------------
    Nom d'enregistrement. : ac-nice.fr
    Type d'enregistrement : 1
    Durée de vie  . . . . : 21216
    Longueur de données . : 4
    Section . . . . . . . : Réponse
    Enregistrement (hôte) : 194.167.84.160
```

➔ J'ai fait une nouvelle capture de trame. J'ai re saisi la commande **ping www.ac-nice.fr** dans l'invite de commandes.

➔ J'ai vidé le cache du DNS à l'aide de la commande **ipconfig /flushdns** et j'ai à nouveau fait une nouvelle capture de trame afin de visualiser de nouveau une requête DNS.

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

Envoi d'une requête 'ping' sur ac-nice.fr [194.167.84.160] avec 32 octets de données :
Réponse de 194.167.84.160 : octets=32 temps=33 ms TTL=48
Réponse de 194.167.84.160 : octets=32 temps=33 ms TTL=48
Réponse de 194.167.84.160 : octets=32 temps=33 ms TTL=48
Réponse de 194.167.84.160 : octets=32 temps=35 ms TTL=48

Statistiques Ping pour 194.167.84.160:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 33ms, Maximum = 35ms, Moyenne = 33ms

C:\Windows\System32> ipconfig /flushdns

Configuration IP de Windows

Cache de résolution DNS vidé.

C:\Windows\System32>
```



- Quels sont les différents protocoles encapsules dans une trame DNS ?

Les différents protocoles encapsules dans une trame DNS est l'UDP, IP, Ethernet.

- Quelle est la machine destinataire de la requête DNS ?

La machine destinataire de la requête DNS est mon routeur 192.168.1.1

- Quelle est l'adresse IP de la machine destinataire de la requête DNS ?

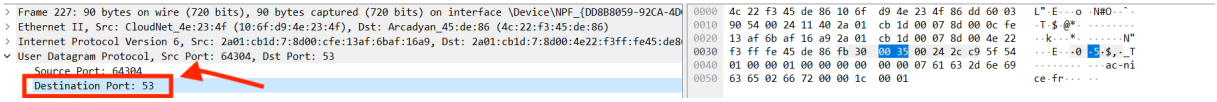
L’adresse IP de la machine destinataire de la requête DNS est 192.168.1.1

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

La signification que les octets de position 0x0C, 0x0D ligne 0000 et 0x07 ligne 0010 est qu’ils correspondent au protocole UDP. Valeur 17 :

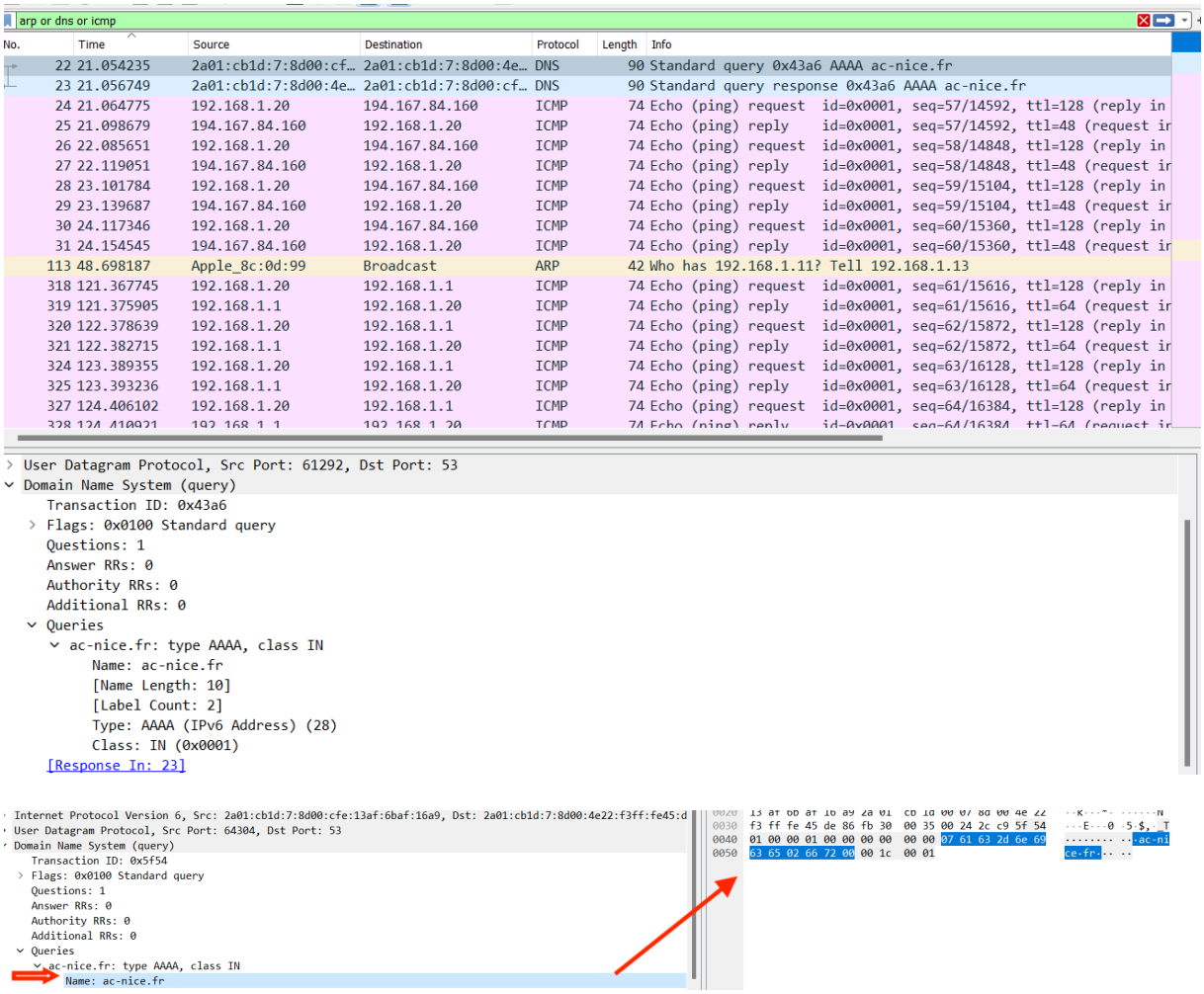
- Quelle signification ont les octets de position 0×04 et 0×05 ligne 0020 ?

La signification que les octets de position 0x04 et 0x05 ligne 0020 est qu’ils correspondent au port DNS de destination. Valeur 53 :

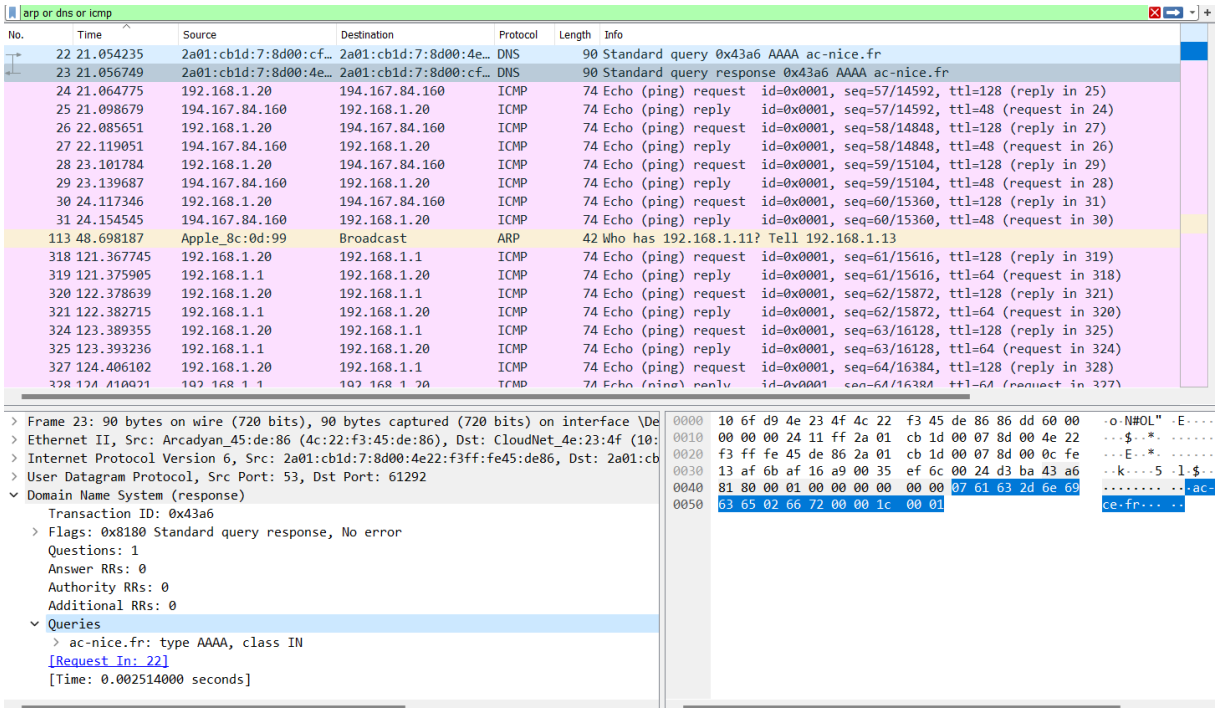


- Développez la section **Domain Name System (query)** et plus précisément la rubrique **Queries.** Quels sont les valeurs hexadécimales des octets correspondant au nom de domaine internet ac- nice.fr ?

Les valeurs hexadécimales des octets correspondant au nom de domaine ac-nice.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. (Je n'ai pas de rubrique Answers)

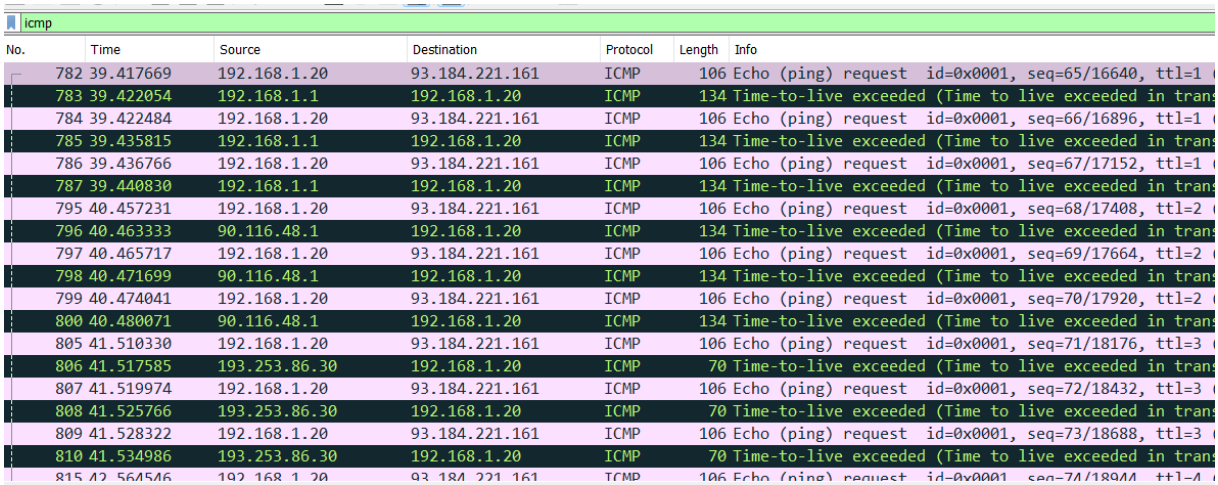


4.3 Commande Tracert et capture de trames ICMP

° La commande **tracert** permet de connaitre tous les routeurs entre la machine locale et une destination donnée, par exemple le site web de l'Académie de Nice (**tracert www.ac-nice.fr**) :

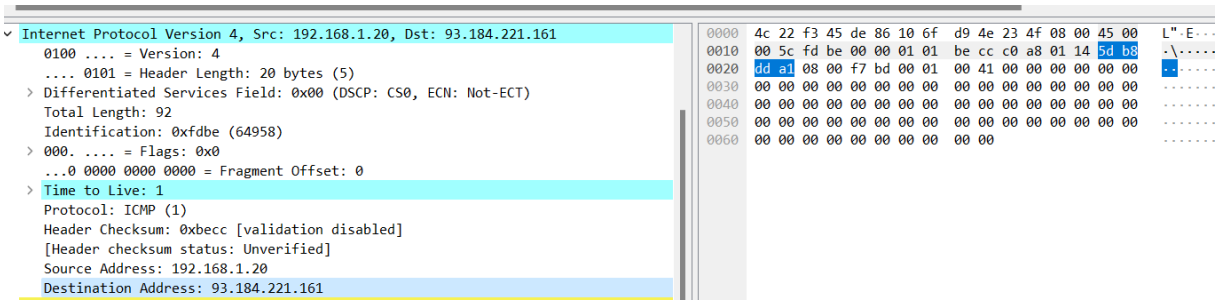
➔ Démarrez une capture de trames depuis votre machine physique.

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



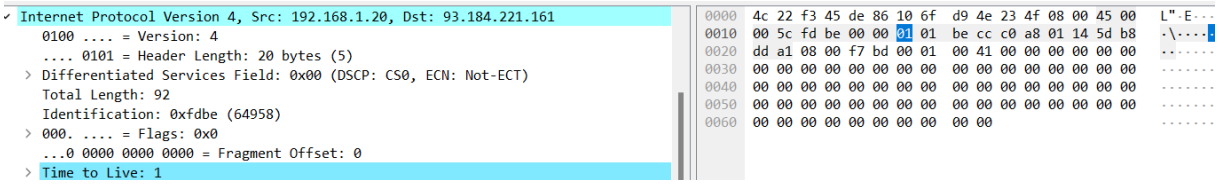
- Sélectionnez la première trame ICMP **Echo request**. Développez l'**en-tête IP**. Quelle est l'adresse IP **Destination** (valeurs déci. Et hexa.) ?

L'adresse de destination dans la première trame ICMP Echo Request en hexa est 5d b8 dd a1 et en décimale 93.184.221.161



- Sélectionnez le champ **TTL**. Quelle est la valeur portée par ce champ (valeurs déci. Et hexa.) ?

La valeur portée par le champ TTL est 1.



- 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 ?

La valeur portée par le champ Type est 11 en décimale et en hexa 0b.