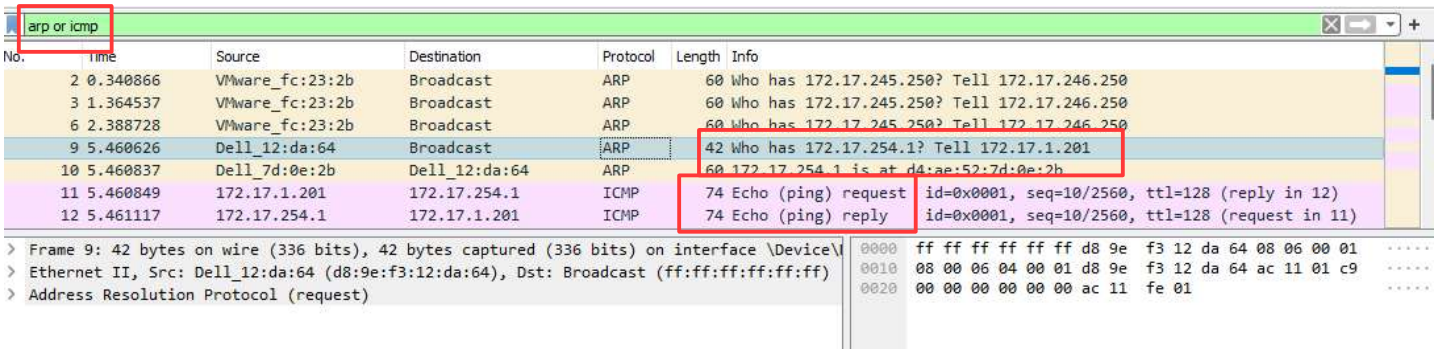
TP 5 – Trames ARP, ICMP et DNS

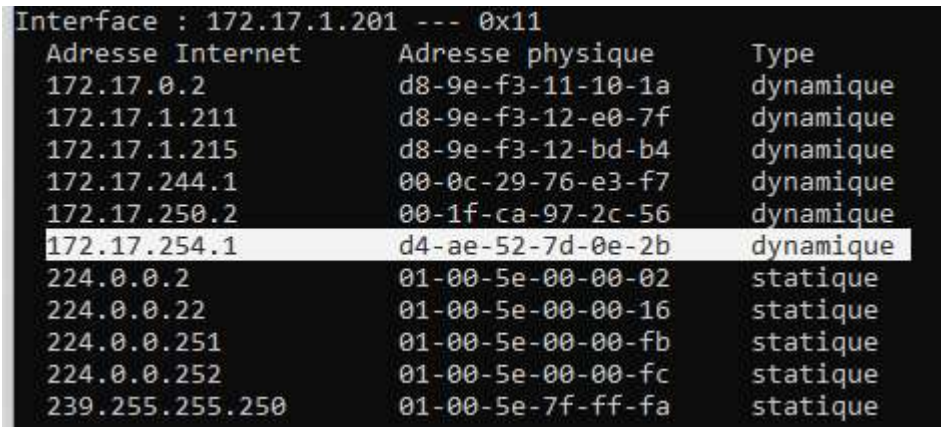
Sommaire :

1. Capture de trames ARP et ICMP :

Avec le logiciel Wireshark, on va capturer les trames ICMP et ARP en saisissant la commande « ping roi » sir l'invite de commande :



▪ Après la saisie de la commande ping, consultez le contenu du cache ARP et vérifiez la présence de l'association @IP-@MAC correspondant à ROI.



```
Interface : 172.17.1.201 --- 0x11
  Adresse Internet      Adresse physique      Type
  172.17.0.2            d8-9e-f3-11-10-1a     dynamique
  172.17.1.211          d8-9e-f3-12-e0-7f     dynamique
  172.17.1.215          d8-9e-f3-12-bd-b4     dynamique
  172.17.244.1          00-0c-29-76-e3-f7     dynamique
  172.17.250.2          00-1f-ca-97-2c-56     dynamique
  172.17.254.1          d4-ae-52-7d-0e-2b     dynamique
  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
```

▪ Analysez l’échange de trames ARP (Request et Reply) précédant l’échange de trames ICMP : Quelle signification ont les octets de position 0×0C et 0×0D ligne 0000 ?

L’échange dans les octets de position 0×0C et 0×0D ligne 0000 est 08 06 qui correspond au protocole ARP.

Quelle est la fonction de la trame ARP Request ?

La trame ARP request demande a toutes les machines (avec un broadcast de couche 2 avec FF:FF:FF:FF:FF:FF) leur adresse Mac en sachant qu’elle connaît l’adresse IP de la machine qu’elle veut joindre.

Ici, elle demande qui a l’adresse IP 172.17.254.1 et lui dit qu’il faut répondre à ma machine qui a comme adresse IP 172.17.1.201

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

La signification des octets de position 0×04 et 0×05 ligne 0010 sont 00 01 (1 en décimal) qui correspond a une « request » du protocole ARP

Quelle est la longueur d’un message ARP ? 28 octets

Quelle est la longueur de la trame ARP Request ? 42 octets

Quelle est la longueur de la trame ARP Reply ? 60 octets

Combien d’octets sont utilisés pour le padding ? Il n’y en a pas pour ARP request et pour ARP reply il y a 18 octets

Trame ARP Request
@MAC destination = FF:FF:FF:FF:FF:FF @MAC source =d8:9e:f3:12:da:64 Ethernet Type = 08 06 (pour dire que c'est ARP)
Opcode (valeurs hexa.) = 00 01 (1 en décimal) @MAC de la cible = 00:00:00:00:00:00 @IP de la cible = 172.17.254.1

▪ **Sélectionnez une trame ICMP Echo Request. Quelle signification ont les octets de position 0×0C et 0×0D ligne 0000 ?**

Les octets de position 0×0C et 0×0D à la ligne 0000, sont 08 00 qi correspond à IPv4 dans la couche Internet (couche 3)

▪ **Quelle signification a l'octet de position 0×07 ligne 0010 ?**

L'octet de position 0×07 à la ligne 0010 est 01 qui correspond au protocole ICMP

▪ **Quelle est la longueur de la trame ?** 74 octets

▪ **Quelle est la longueur du paquet IP ?** 20 octets

▪ **Quelle est la longueur du message ICMP ?** 40 octets

▪ **Quelle signification a l'octet de position 0×02 ligne 00020 ?**

Cela correspond au Type: 8 (Echo (ping) request) (en hexadécimal 08)

▪ **A quoi correspondent les octets à partir de l'octet 0×0A, ligne 0020 ?**

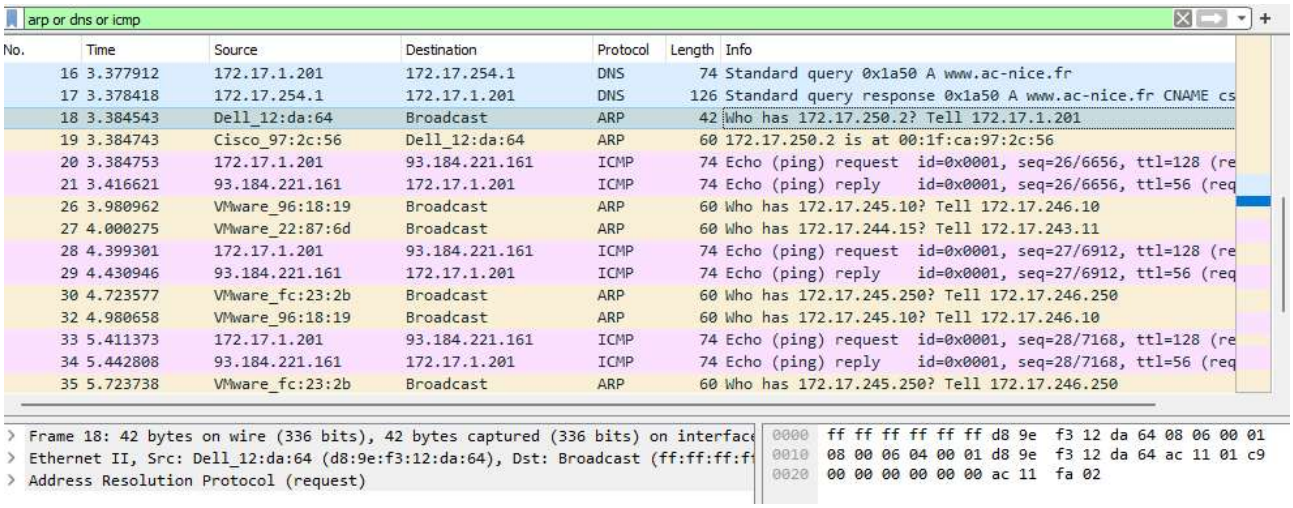
A partir de l'octet 0×0A à la ligne 0020, qui est 61 en hexadécimal, il y a l'alphabet.

▪ Sélectionnez une trame ICMP Echo Reply. Quelle est le nom et la valeur de l'octet de position 0×02 ligne 0020 ?

Cela correspond au Type: 0 (Echo (ping) reply) (00 en hexadécimal)

2. Capture de trames ARP, DNS et ICMP.

On ouvre une invite de commandes et effectuez une requête ping vers le serveur web www.ac-nice.fr puis on capture sa trame à l'aide de Wireshark :



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

L'adresse MAC recherchée est la passerelle (172.17.250.2)

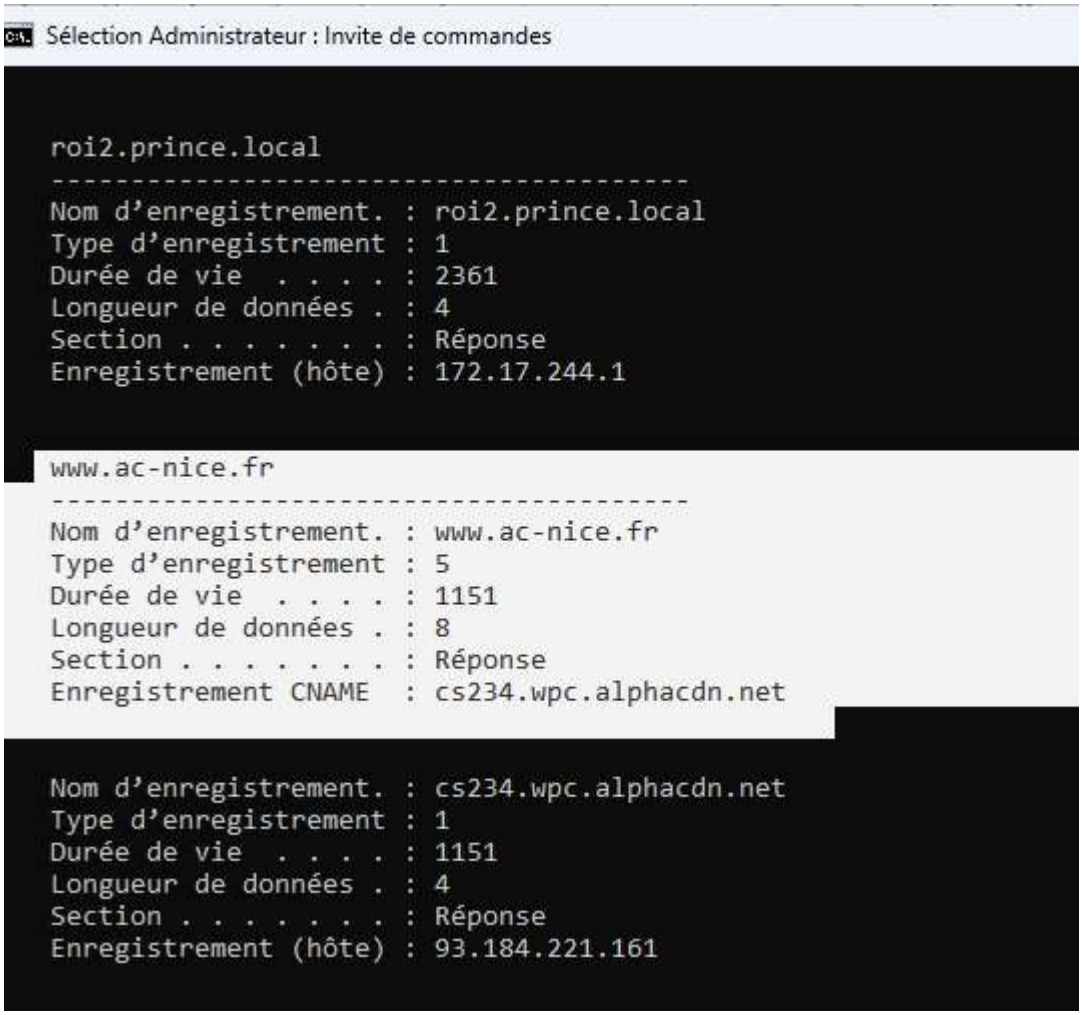
▪ Complétez les rubriques ci-dessous :

Trame ARP request
@MAC destination = FF:FF:FF:FF:FF:FF @MAC source = d8:9e:f3:12:da:64 Ethernet Type = 0806 (ARP)
Opcode (valeurs hexa.) =00 01 (1 en décimal) @MAC de la cible = 00:00:00:00:00:00 @IP de la cible = 172.17.250.2

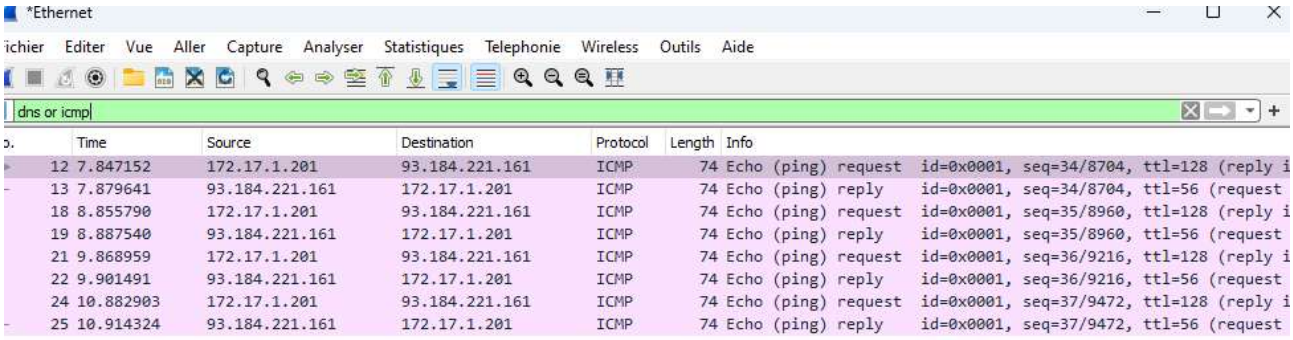
▪ Pour quelle raison trouve-t-on ensuite une requête DNS avant l'exécution de la commande ping proprement dite ?

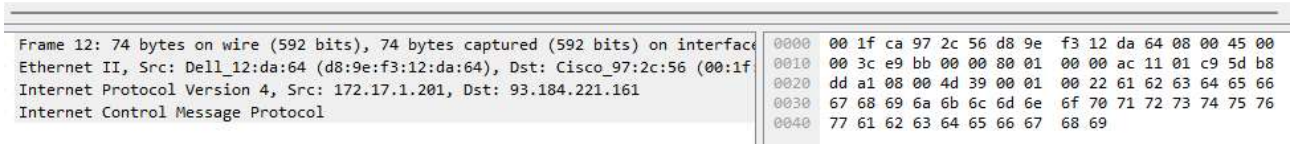
DNS transforme le nom de domaine « www.ac-nice.fr »en IP, puis ARP en sachant l'IP du domaine, demande en broadcast qui a cette IP et demande de lui répondre. Une fois qu'on a la réponse, ICMP peut faire sont PING (echo request et echo reply)

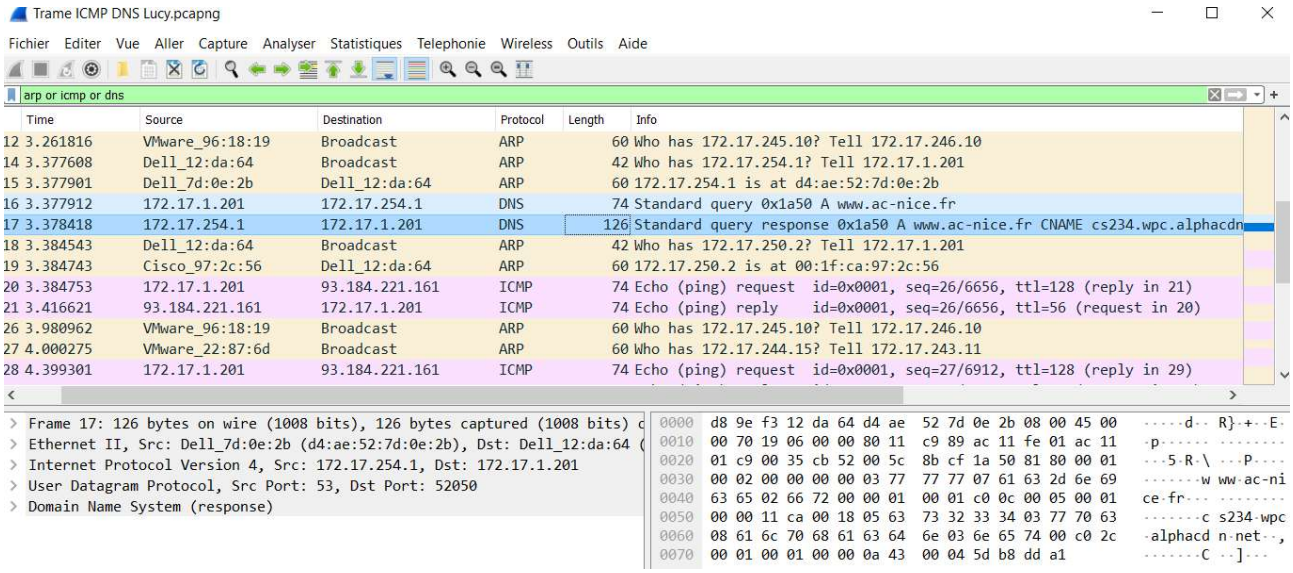
Puis, on consulte le cache DNS à l'aide de la commande ipconfig /displaydns et vérifiez la présence de l'enregistrement DNS ac-nice.fr et de l'adresse IP associée :



Ensuite on démarre une nouvelle capture et on saisit la commande « ping ac-nice.fr » dans l'invite de commandes. On ne doit pas constater de requête DNS puisque l'enregistrement est présent dans le cache DNS. Après , on vide le cache DNS à l'aide de la commande « ipconfig /flushdns »







▪ Quels sont les différents protocoles encapsulés dans une trame DNS ?

Dans une trame DNS, il y a :

- un en-tête Ethernet (donc protocole Ethernet)

- un en-tête Internet (donc protocole IPv4)

-un en-tête Transport (donc UDP)

-Les données applicatives (donc ici c'est le DNS)

▪ Quelle est la machine destinataire de la requête DNS ?

L'adresse de destination est d4:ae:52:7d:0e:2b

▪ Quelle est l’adresse IP de la machine destinataire de la requête DNS ?

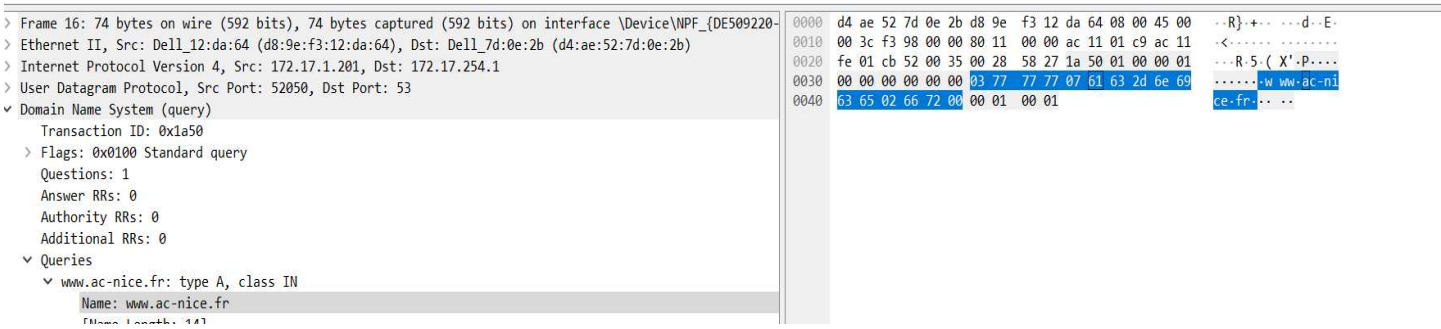
L’ Adresse de destination est 172.17.254.1

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

Les octets de position 0×04 et 0×05 à la ligne 0020 c’est 00 35 qui correspond a 53 qui est le protocole DNS.

▪ 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 ?

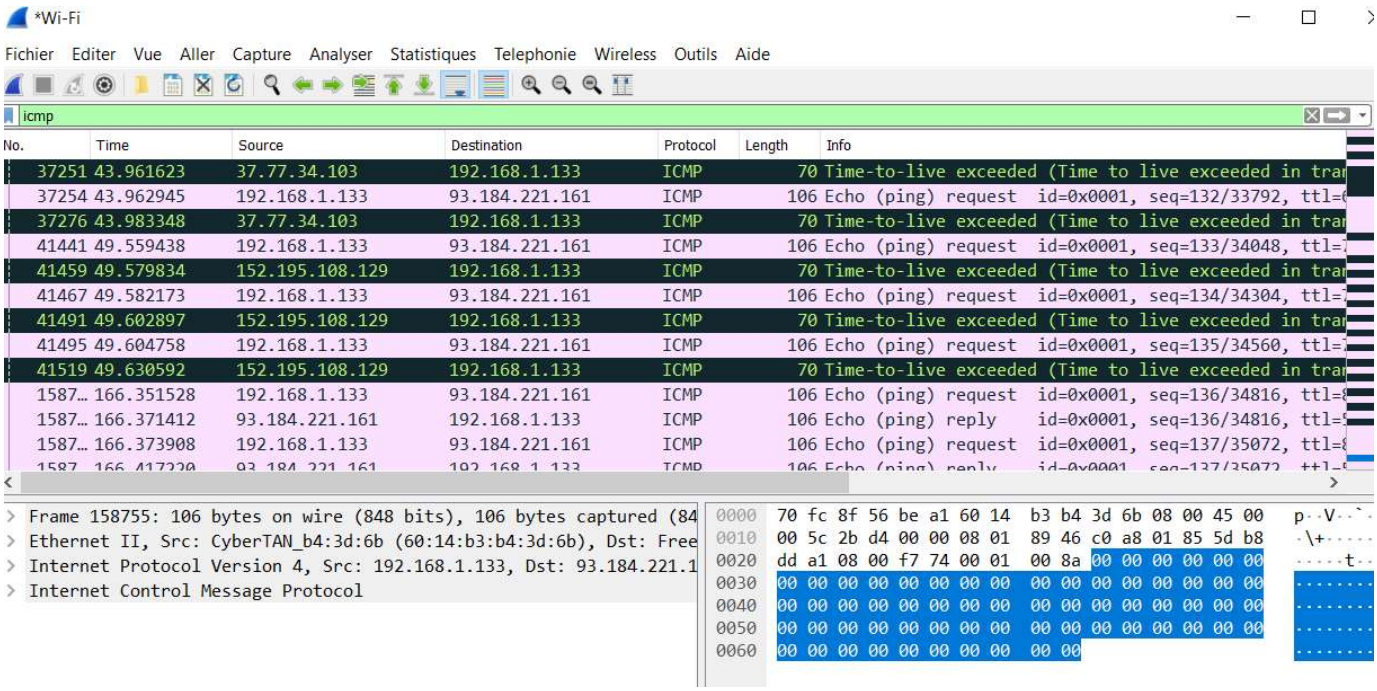
Pour le nom de domaine internet www.ac-nice.fr les valeurs en héxadécimales des octets sont :



▪ 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.

L’adresse IP du seveur web hébergeant le site est 93.184.221.161 (en décimal) et en hexadécimal c’est 5d b8 dd a1

3. Commande Tracert et capture de trames ICMP.




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

Détermination de l'itinéraire vers cs234.wpc.alphacdn.net [93.184.221.161]
avec un maximum de 30 sauts :

  1     5 ms     2 ms     4 ms  192.168.1.254
  2     *        *        *     Délai d'attente de la demande dépassé.
  3     *       20 ms     *     station1.multimania.isdnet.net [194.149.174.98]
  4    27 ms    22 ms    19 ms  193.253.13.65
  5    19 ms    19 ms    20 ms  193.253.13.206
  6    23 ms    27 ms    20 ms  edgecast1.th2-1.hopus.net [37.77.34.103]
  7    20 ms    21 ms    26 ms  ae-65.core1.paa.edgecastcdn.net [152.195.108.129]
  8    20 ms    43 ms    20 ms  93.184.221.161

Itinéraire déterminé.
```

▪ 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 est 93.184.221.161 en décimal et en hexadécimal 5d b8 dd a1 .

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

Dans le Time to Live la valeur portée par ce champ est 1 (en décimal) et 01 (en hexadécimal)

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

La valeur est dans le Type: 8 (Echo (ping) request) en décimal et en hexadécimal 08

▪ 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.) ?

La valeur portée par le champ Type est 11 (Time-to-live exceeded) en décimal et 0b en hexadécimal.