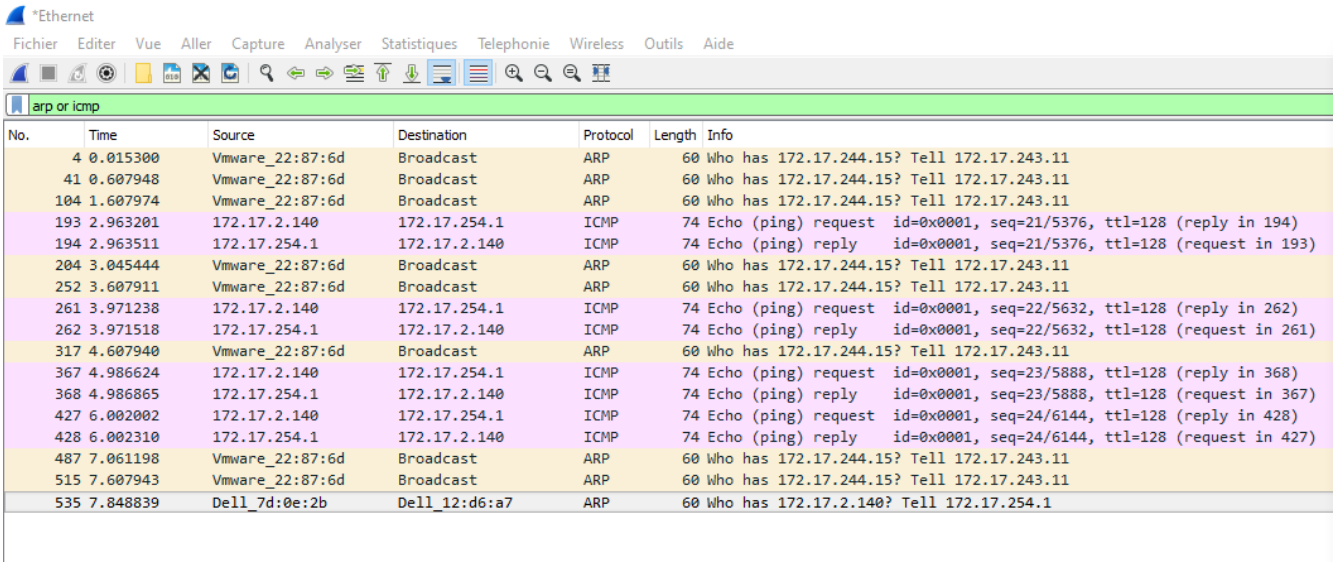
RUGGERI BSIO1
Jamy

TP3: Trames ARP, ICMP et DNS

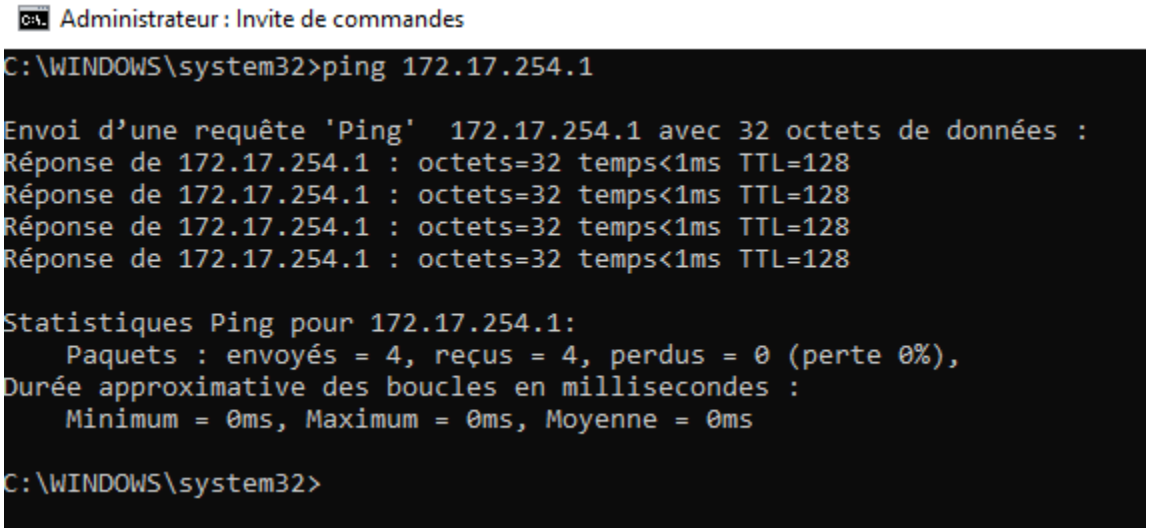
1) Capture de trames ARP et ICMP

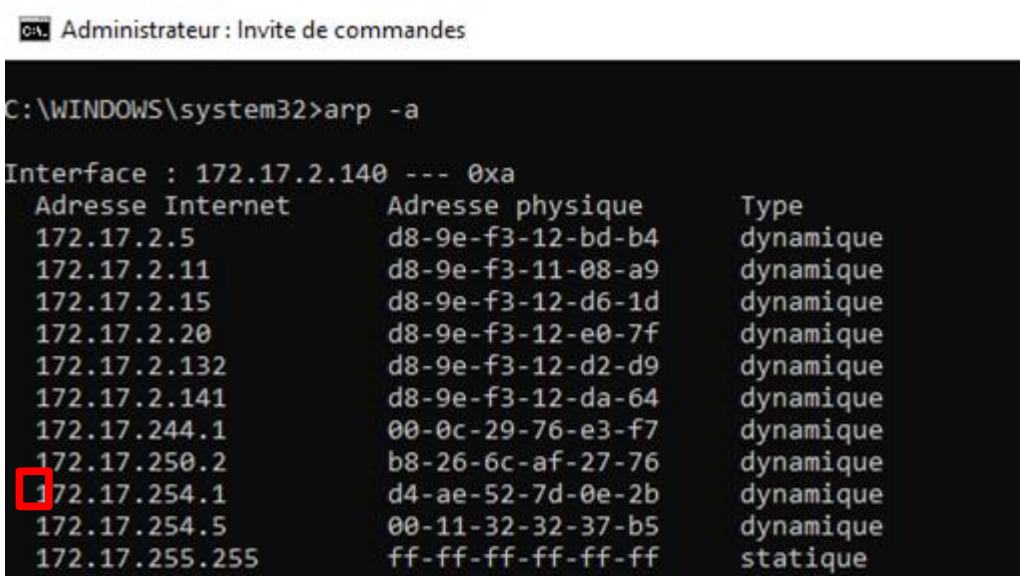


No.	Time	Source	Destination	Protocol	Length	Info
4	0.015300	Vmware_22:87:6d	Broadcast	ARP	60	Who has 172.17.244.15? Tell 172.17.243.11
41	0.607948	Vmware_22:87:6d	Broadcast	ARP	60	Who has 172.17.244.15? Tell 172.17.243.11
104	1.607974	Vmware_22:87:6d	Broadcast	ARP	60	Who has 172.17.244.15? Tell 172.17.243.11
193	2.963201	172.17.2.140	172.17.254.1	ICMP	74	Echo (ping) request id=0x0001, seq=21/5376, ttl=128 (reply in 194)
194	2.963511	172.17.254.1	172.17.2.140	ICMP	74	Echo (ping) reply id=0x0001, seq=21/5376, ttl=128 (request in 193)
204	3.045444	Vmware_22:87:6d	Broadcast	ARP	60	Who has 172.17.244.15? Tell 172.17.243.11
252	3.607911	Vmware_22:87:6d	Broadcast	ARP	60	Who has 172.17.244.15? Tell 172.17.243.11
261	3.971238	172.17.2.140	172.17.254.1	ICMP	74	Echo (ping) request id=0x0001, seq=22/5632, ttl=128 (reply in 262)
262	3.971518	172.17.254.1	172.17.2.140	ICMP	74	Echo (ping) reply id=0x0001, seq=22/5632, ttl=128 (request in 261)
317	4.607940	Vmware_22:87:6d	Broadcast	ARP	60	Who has 172.17.244.15? Tell 172.17.243.11
367	4.986624	172.17.2.140	172.17.254.1	ICMP	74	Echo (ping) request id=0x0001, seq=23/5888, ttl=128 (reply in 368)
368	4.986865	172.17.254.1	172.17.2.140	ICMP	74	Echo (ping) reply id=0x0001, seq=23/5888, ttl=128 (request in 367)
427	6.002002	172.17.2.140	172.17.254.1	ICMP	74	Echo (ping) request id=0x0001, seq=24/6144, ttl=128 (reply in 428)
428	6.002310	172.17.254.1	172.17.2.140	ICMP	74	Echo (ping) reply id=0x0001, seq=24/6144, ttl=128 (request in 427)
487	7.061198	Vmware_22:87:6d	Broadcast	ARP	60	Who has 172.17.244.15? Tell 172.17.243.11
515	7.607943	Vmware_22:87:6d	Broadcast	ARP	60	Who has 172.17.244.15? Tell 172.17.243.11
535	7.848839	Dell_7d:0e:2b	Dell_12:d6:a7	ARP	60	Who has 172.17.2.140? Tell 172.17.254.1

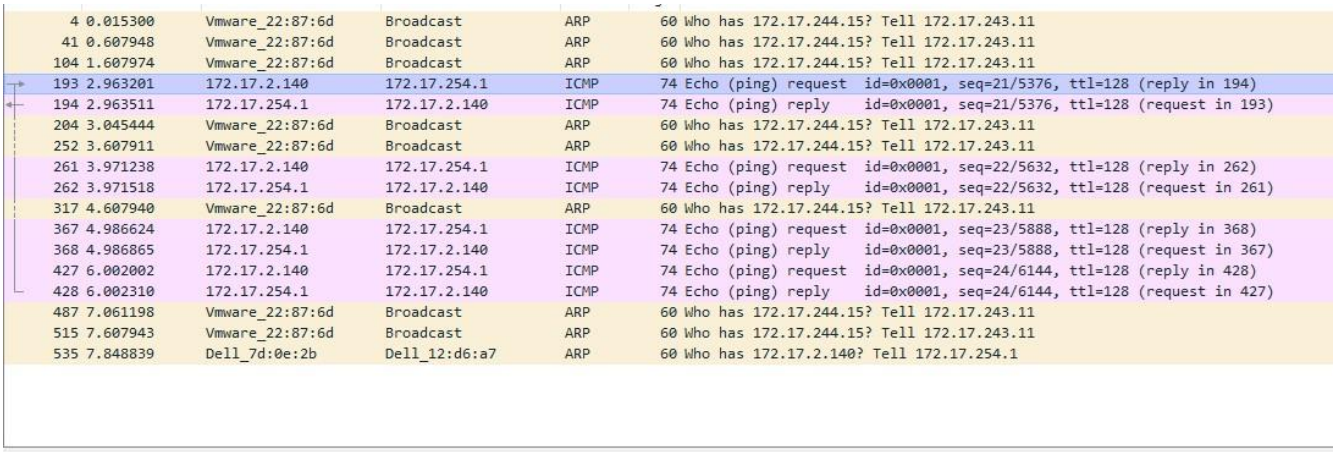
1ère étape: Une capture de trames à été lancée en même temps que nous effectuons un ping sur le Serveur ROI. Nous observons donc avec le filtre les échanges de trames ARP et ICMP.

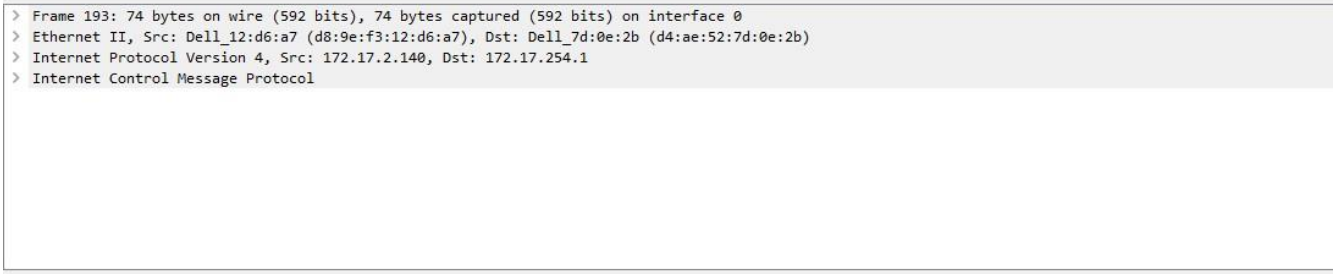
2ème étape: Voici une capture d'écran effectuer lors d'une ping du Serveur ROI.

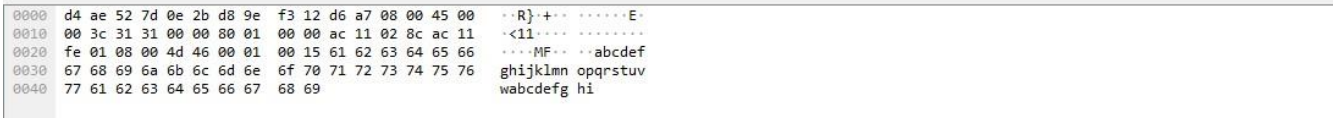


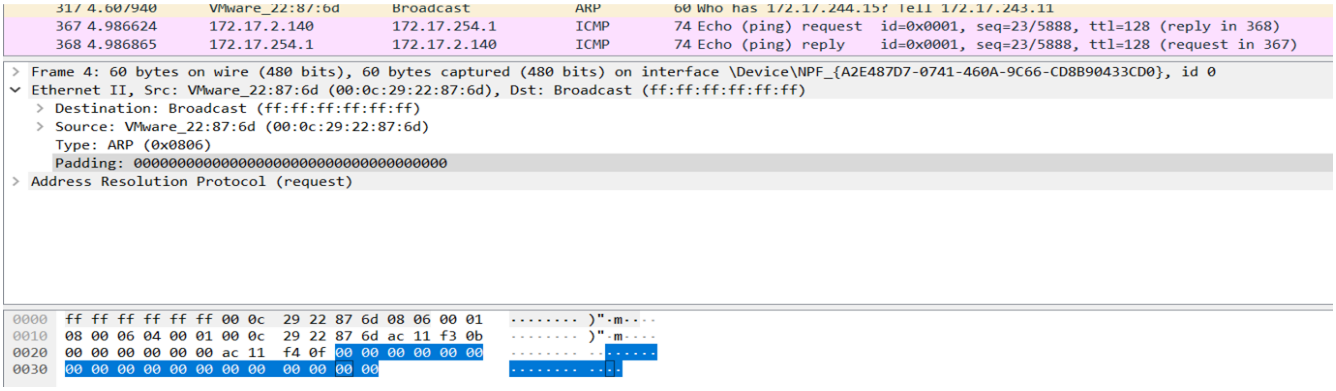


3ème étape: On observe par la suite avec la commande “arp -a” qu’une fois les échanges ARP effectuer entre la machine et le serveur ROI, l’adresse MAC et l’adresse IP de ROI apparaît donc dans le cache ARP.









<u>Analysez l'échange de trames ARP (Request et Reply) précédant l'échange de trames ICMP :</u>

Quelle signification ont les octets de position 0×0C et 0×0D ligne 0000 ?
Les octets 13 et 14 signifient que le champ Ethertype est 0806 (ARP)

Quelle est la fonction de la trame ARP Request ?
La trame ARP Request permet d'obtenir l'adresse MAC d'une machine locale.

Quelle signification ont les octets de position 0×04 et 0×05 ligne 0010 ?
Les octets numéro 5 et 6 de la ligne 0010 sont 00 01 ce qui signifie que c'est une requête ARP.

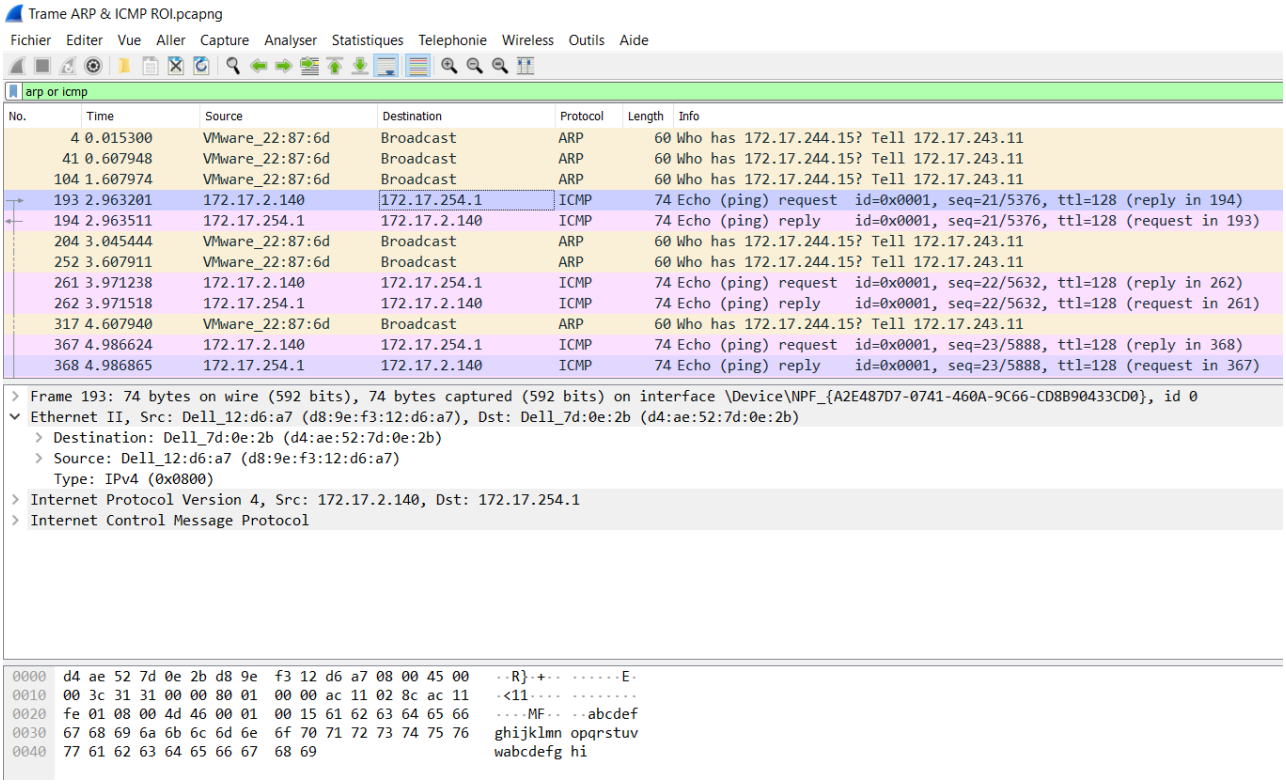
Quelle est la longueur d'un message ARP ?
Le message ARP est sur 16 bits.

Quelle est la longueur de la trame ARP Request ?
La trame ARP Request est d'une longueur de 60 octets

Quelle est la longueur de la trame ARP Reply ?
La trame ARP Reply est d'une longueur de 60 octets

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

Trame ARP request
@MAC destination = ff ff ff ff ff ff
@MAC source = d4 ae 52 7d 0e 2b
Ethernet Type = 0806
Opcode (valeurs hexa.) = 00 01
@MAC de la cible = 00 00 00 00 00 00
@IP de la cible = Ac 11 f4 0f



Sélectionnez une trame ICMP Echo Request:

Quelle signification ont les octets de position 0×0C et 0×0D ligne 0000 ?
Le 13 et 14ème octet de la ligne 0000 on comme valeur 0800 ce qui signifie qu'ils représentent tout deux le champ Ethertype (IPv4).

Quelle signification a l'octet de position 0×07 ligne 0010 ?
Le 8ème octet représente la valeur 01 donc le protocole de transport Datagramme UDP.

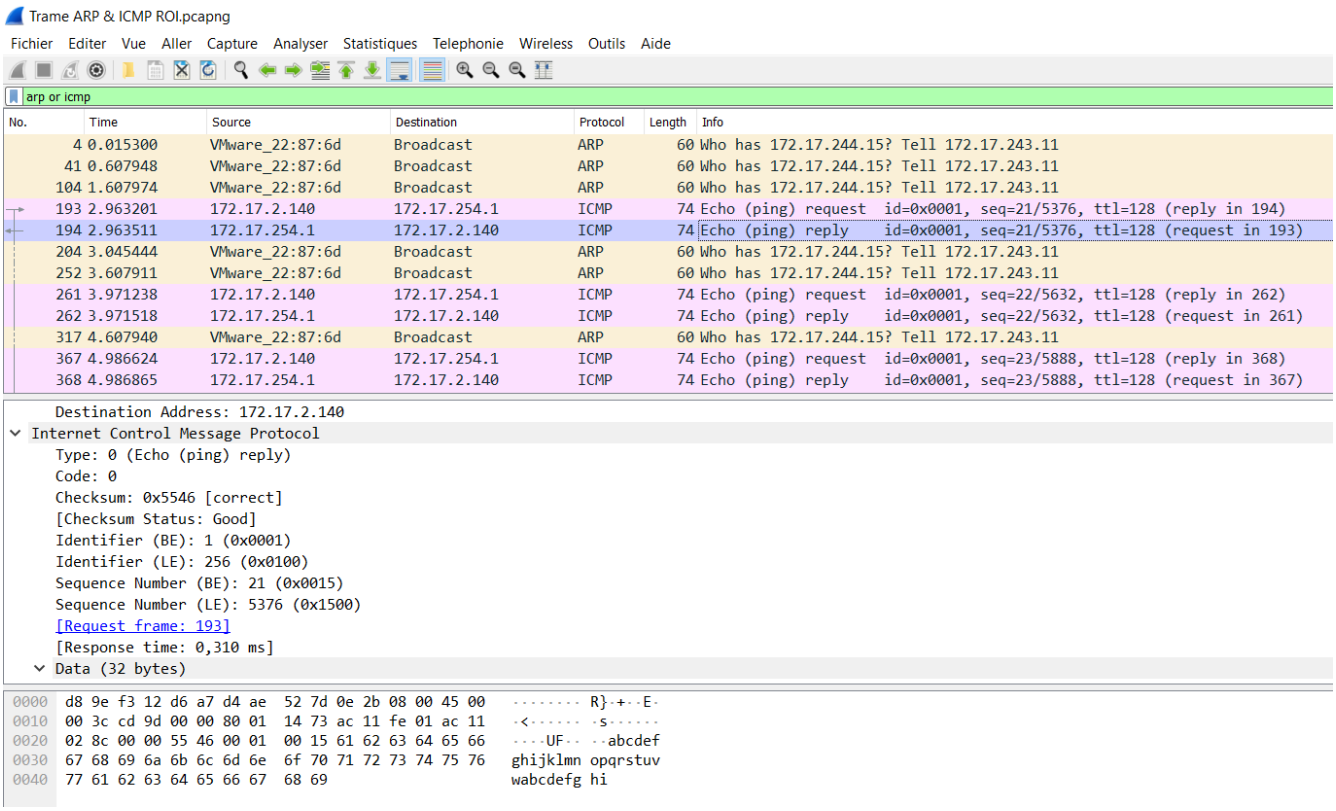
Quelle est la longueur de la trame ? La longueur de la trame est de 74 octets

Quelle est la longueur du paquet IP ? La longueur du paquet IP est de 20 octets

Quelle est la longueur du message ICMP ?
Le message ICMP avec les données est de 40 octets

Quelle signification ont les octets de position 0×02 et 0×03, ligne 00020 ?
Le 3ème octet de la lgine 00020 représente le type 08, le 4ème le code 0. Cela signifie donc que c'est une trame ICMP echo request.

A quoi correspondent les octets à partir de l'octet 0×0A, ligne 00020 ?
A partir du 11ème octet, les octets représentes les données de la trames.



<u>Sélectionnez une trame ICMP Echo Reply:</u>

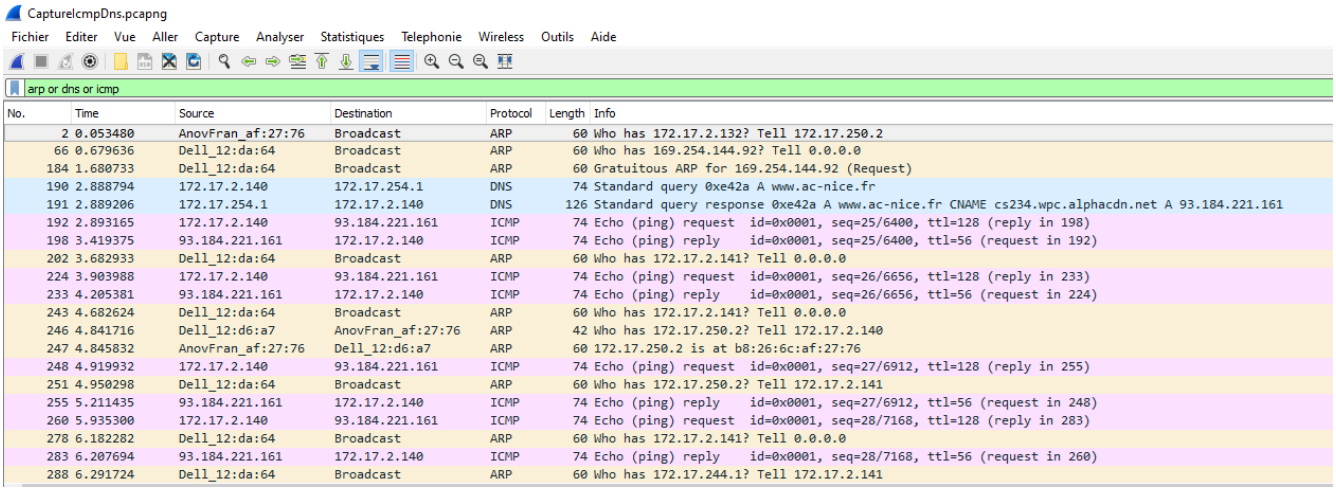
Quelles sont les noms et valeurs des octets de position 0×02 et 0×03, ligne 00020 ?
L'octet de position 0x02 est d'une valeur hexa de 00, il signifie que le type ici présent est le Type 0, et l'octet de position 0x03 à comme valeur hexa 00 et représente lui le Code 0. Cela signifie donc que c'est une trame ICMP echo reply.

---

2) Capture de trames ARP, DNS et ICMP

```
Administrateur : Invite de commandes

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

Envoi d'une requête 'ping' sur cs234.wpc.alphacdn.net [93.184.221.161] avec 32 octets de données :
Réponse de 93.184.221.161 : octets=32 temps=526 ms TTL=56
Réponse de 93.184.221.161 : octets=32 temps=301 ms TTL=56
Réponse de 93.184.221.161 : octets=32 temps=291 ms TTL=56
Réponse de 93.184.221.161 : octets=32 temps=272 ms TTL=56

Statistiques Ping pour 93.184.221.161:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 272ms, Maximum = 526ms, Moyenne = 347ms
```

1ère étape: En démarrant une capture de trames, nous effectuons un ping vers le serveur web de ***www.ac-nice.fr***



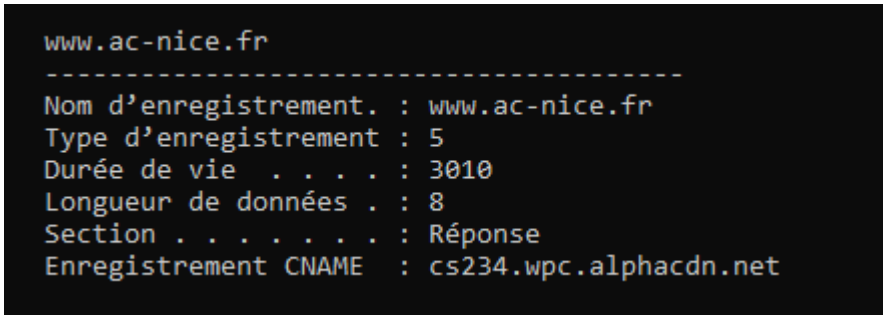
No.	Time	Source	Destination	Protocol	Length	Info
2	0.053480	AnovFran_af:27:76	Broadcast	ARP	60	Who has 172.17.2.132? Tell 172.17.250.2
66	0.679636	Dell_12:da:64	Broadcast	ARP	60	Who has 169.254.144.92? Tell 0.0.0.0
184	1.680733	Dell_12:da:64	Broadcast	ARP	60	Gratuitous ARP for 169.254.144.92 (Request)
190	2.888794	172.17.2.140	172.17.254.1	DNS	74	Standard query 0xe42a A www.ac-nice.fr
191	2.889206	172.17.254.1	172.17.2.140	DNS	126	Standard query response 0xe42a A www.ac-nice.fr CNAME cs234.wpc.alphacdn.net A 93.184.221.161
192	2.893165	172.17.2.140	93.184.221.161	ICMP	74	Echo (ping) request id=0x0001, seq=25/6400, ttl=128 (reply in 198)
198	3.419375	93.184.221.161	172.17.2.140	ICMP	74	Echo (ping) reply id=0x0001, seq=25/6400, ttl=56 (request in 192)
202	3.682933	Dell_12:da:64	Broadcast	ARP	60	Who has 172.17.2.141? Tell 0.0.0.0
224	3.903988	172.17.2.140	93.184.221.161	ICMP	74	Echo (ping) request id=0x0001, seq=26/6656, ttl=128 (reply in 233)
233	4.205381	93.184.221.161	172.17.2.140	ICMP	74	Echo (ping) reply id=0x0001, seq=26/6656, ttl=56 (request in 224)
243	4.682624	Dell_12:da:64	Broadcast	ARP	60	Who has 172.17.2.141? Tell 0.0.0.0
246	4.841716	Dell_12:d6:a7	AnovFran_af:27:76	ARP	42	Who has 172.17.250.2? Tell 172.17.2.140
247	4.845832	AnovFran_af:27:76	Dell_12:d6:a7	ARP	60	172.17.250.2 is at b8:26:6c:af:27:76
248	4.919932	172.17.2.140	93.184.221.161	ICMP	74	Echo (ping) request id=0x0001, seq=27/6912, ttl=128 (reply in 255)
251	4.950298	Dell_12:da:64	Broadcast	ARP	60	Who has 172.17.250.2? Tell 172.17.2.141
255	5.211435	93.184.221.161	172.17.2.140	ICMP	74	Echo (ping) reply id=0x0001, seq=27/6912, ttl=56 (request in 248)
260	5.935300	172.17.2.140	93.184.221.161	ICMP	74	Echo (ping) request id=0x0001, seq=28/7168, ttl=128 (reply in 283)
278	6.182282	Dell_12:da:64	Broadcast	ARP	60	Who has 172.17.2.141? Tell 0.0.0.0
283	6.207694	93.184.221.161	172.17.2.140	ICMP	74	Echo (ping) reply id=0x0001, seq=28/7168, ttl=56 (request in 260)
288	6.291724	Dell_12:da:64	Broadcast	ARP	60	Who has 172.17.244.1? Tell 172.17.2.141

2ème étape: Ici on remarque que la liste des trames commence par une requête et une réponse ARP.

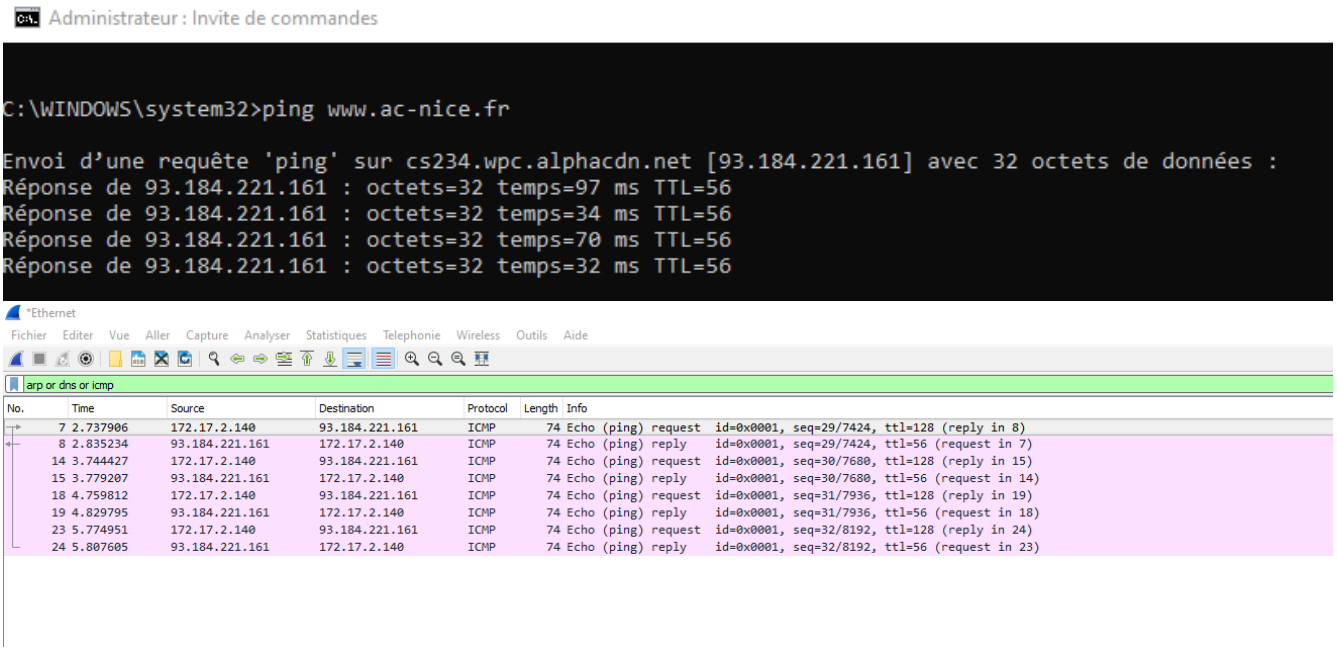
Quelle est l'adresse MAC recherchée ?
L'adresse MAC recherché est celle qui correspond également à l'adresse IP 172.17.2.132
Complétez les rubriques ci-dessous :

Trame ARP request
@MAC destination = ff ff ff ff ff ff @MAC source = B8 26 6c af 27 76 Ethernet Type = ARP
Opcode (valeurs hexa.) = 01 @MAC de la cible = 00 00 00 00 00 00 @IP de la cible = ac 11 02 84

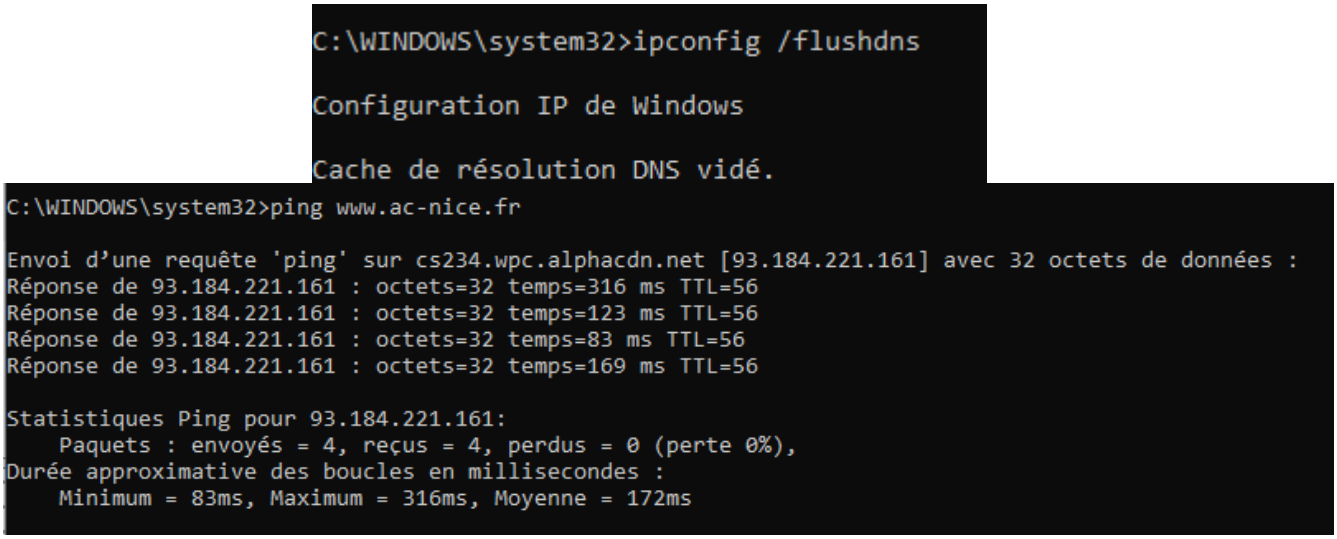
Pour quelle raison trouve-t-on ensuite une requête DNS avant l'exécution de la commande ping proprement dite ?
La requête DNS nous permet d'obtenir l'adresse d'un serveur DNS sur lequel le nom du domaine du site internt peut y figurer. Par la suite nous pouvons donc obetenir l'adresse IP du site.



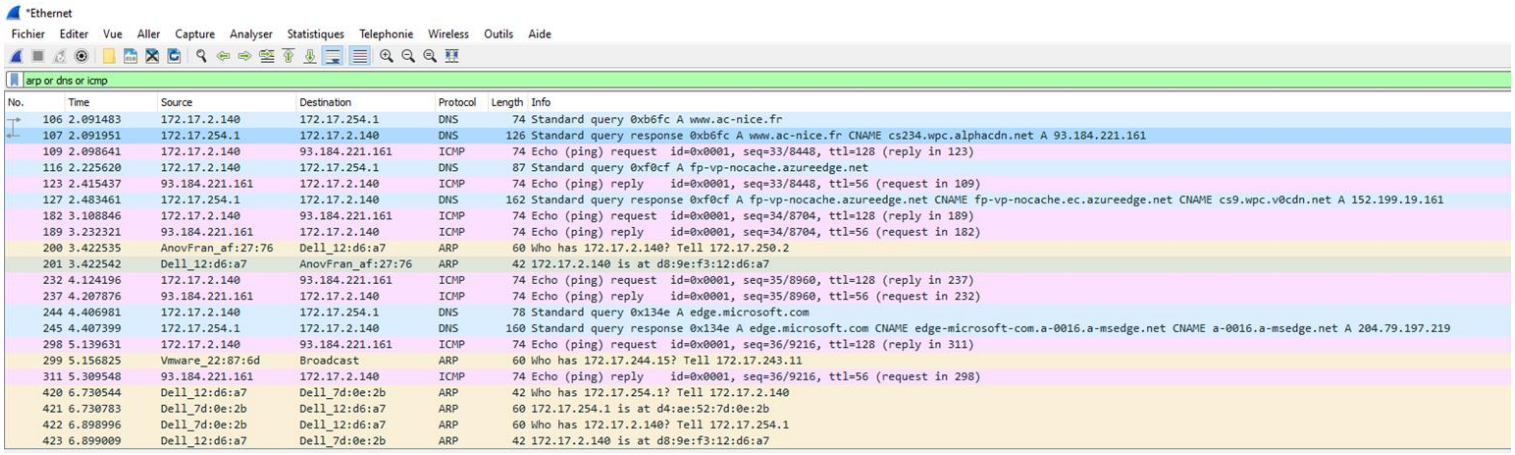
3ème étape: Ici nous constatons donc la présence de l'enregistrement DNS www.ac-nice.fr via la commande "**ipconfig /displaydns**" qui nous permet d'obtenir tout les caches DNS.



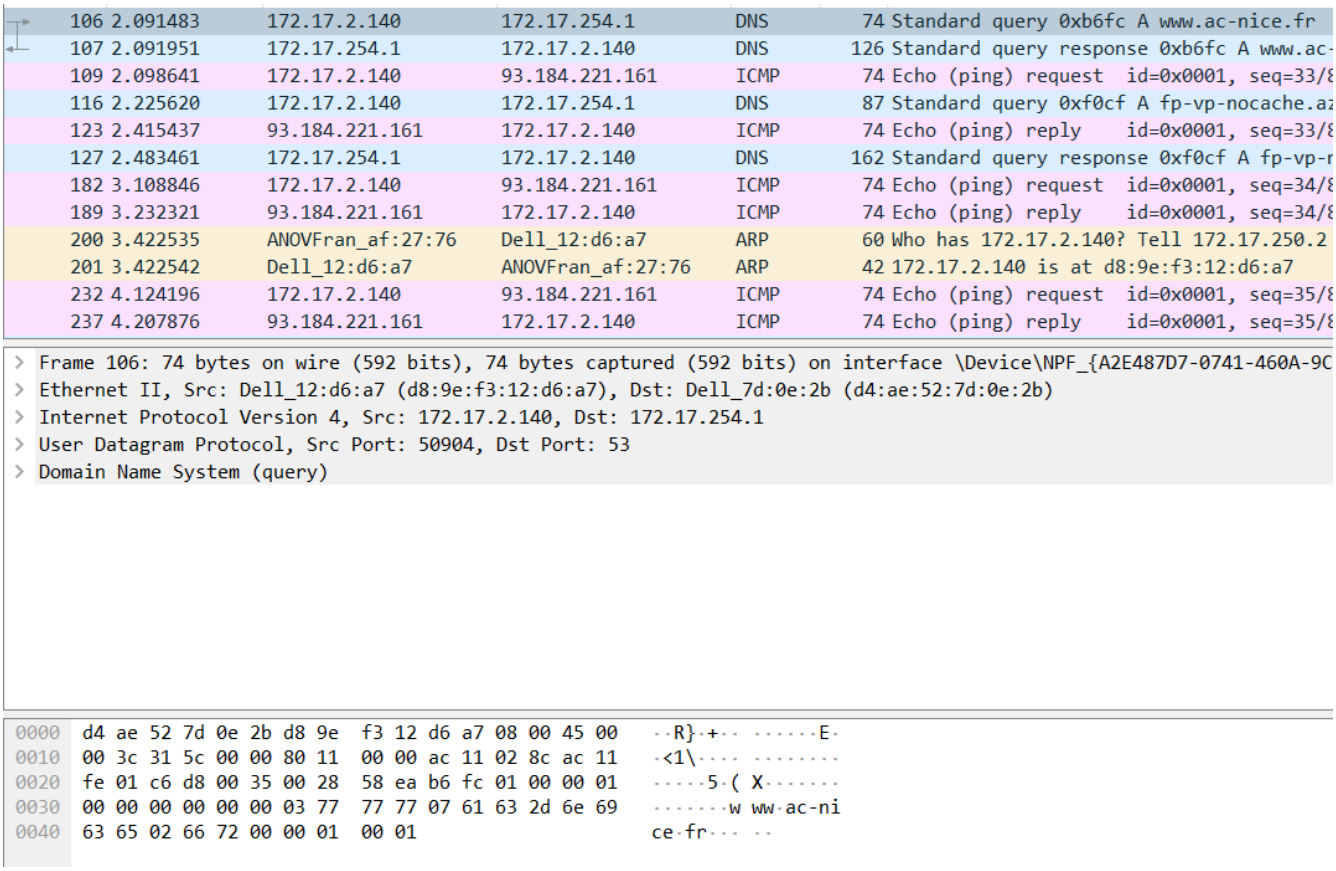
4ème étape: Si nous effectuons donc de nouveau un ping de ce domaine avec une capture de trame en même temps, nous constatons donc qu'il n'y a plus de requête DNS puisque les informations DNS pour ce nom de domaine sont déjà présentent dans le cache DNS.



5ème étape: Avec la commande "ipconfig /flushdns" nous vidons donc le cache DNS. Une fois cette manipulation effectuer une nouvelle capture de trames est lancé accompagner d'un nouveau ping du domain ac-nice.fr



6ème étape: Cette fois-ci avec le cache DNS vidé les requête DNS font leur apparition.



Quels sont les différents protocoles encapsulés dans une trame DNS ?
Dans une trame DNS on retrouve donc le champ ethertype IPv4, le protocole de transport Datagramme UDP ainsi que le protocole applicatif 00 35.

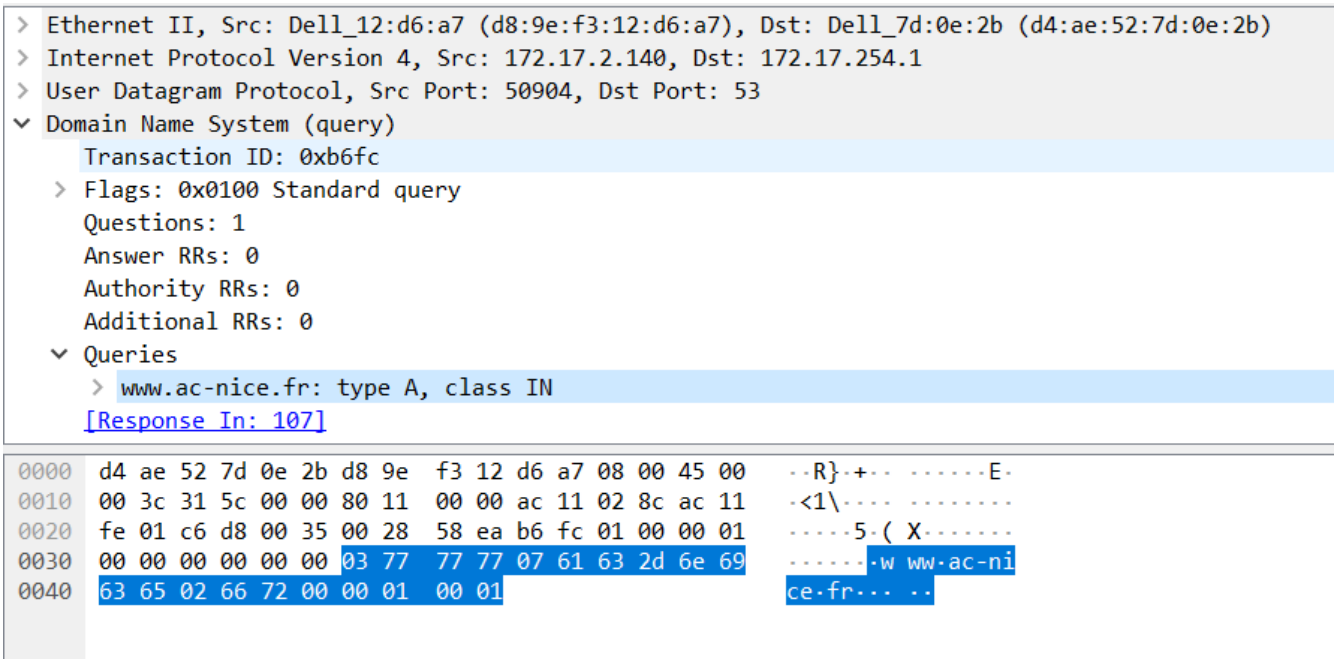
Quelle est la machine destinataire de la requête DNS ?

La machine destinataire de la requête DNS est le rooteur qui contacte donc par la suite un serveur DNS.

Quelle est l'adresse IP de la machine destinataire de la requête DNS ?
172.17.254.1

Quelle signification ont les octets de position 0×0C, 0×0D ligne 0000 et 0×07 ligne 0010 ?
Ils ont comme valeur 0800, ce qui signifie qu'ils représentent le champ Ethertype IPv4. Le 8ème octet représente la valeur 11 donc le Datagramme UDP.

Quelle signification ont les octets de position 0×04 et 0×05 ligne 0020 ?
Les octets 5 et 6 de la valeur 0020 ont la valeur 00 35 donc ils représente à eux deux le port DNS 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 acnice.fr ?

03 77 77 77 07 61 63 2d 6e 69 63 65 02 66 72 00 00 01 00 01

Sélectionnez la trame comportant la réponse à la requête 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.

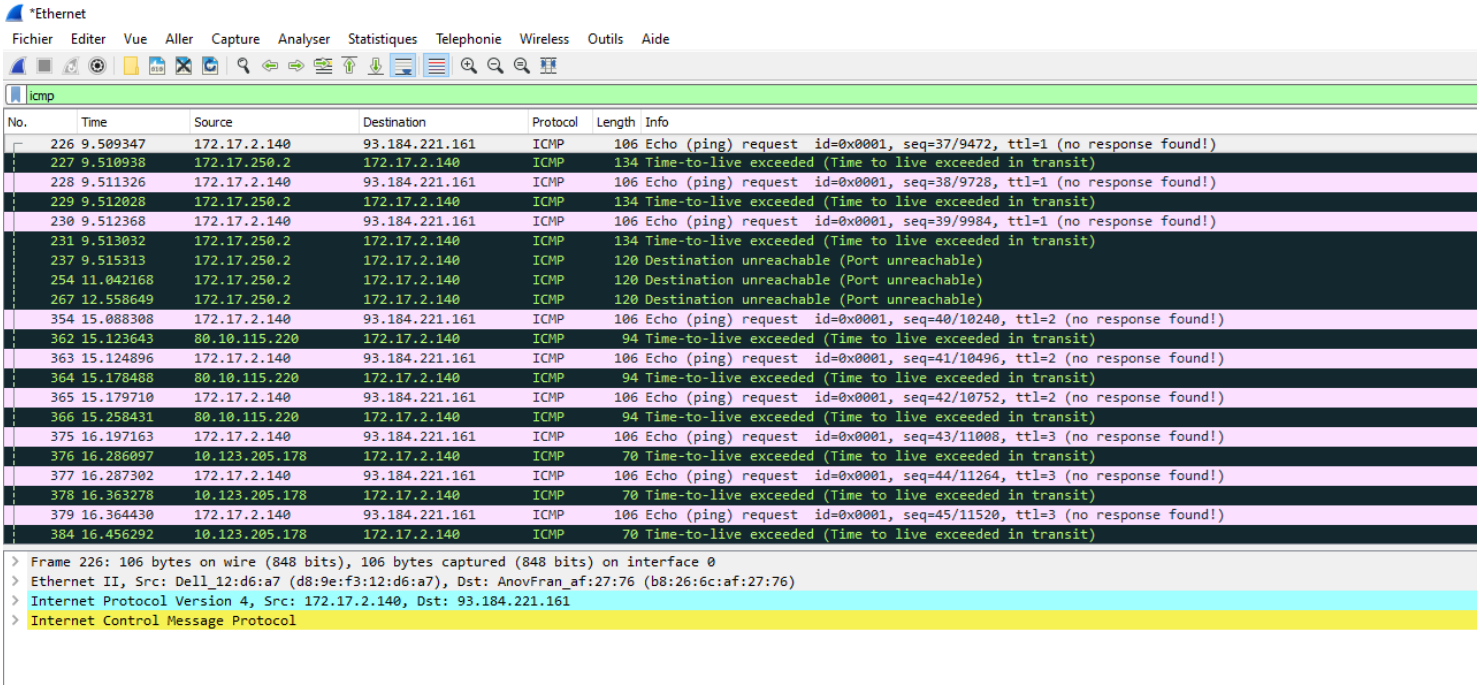
Adresse IP serveur web hébergeur en hexa : 5d b8 dd a1
Adresse IP serveur web hébergeur en deci : 93.184.221.161

---

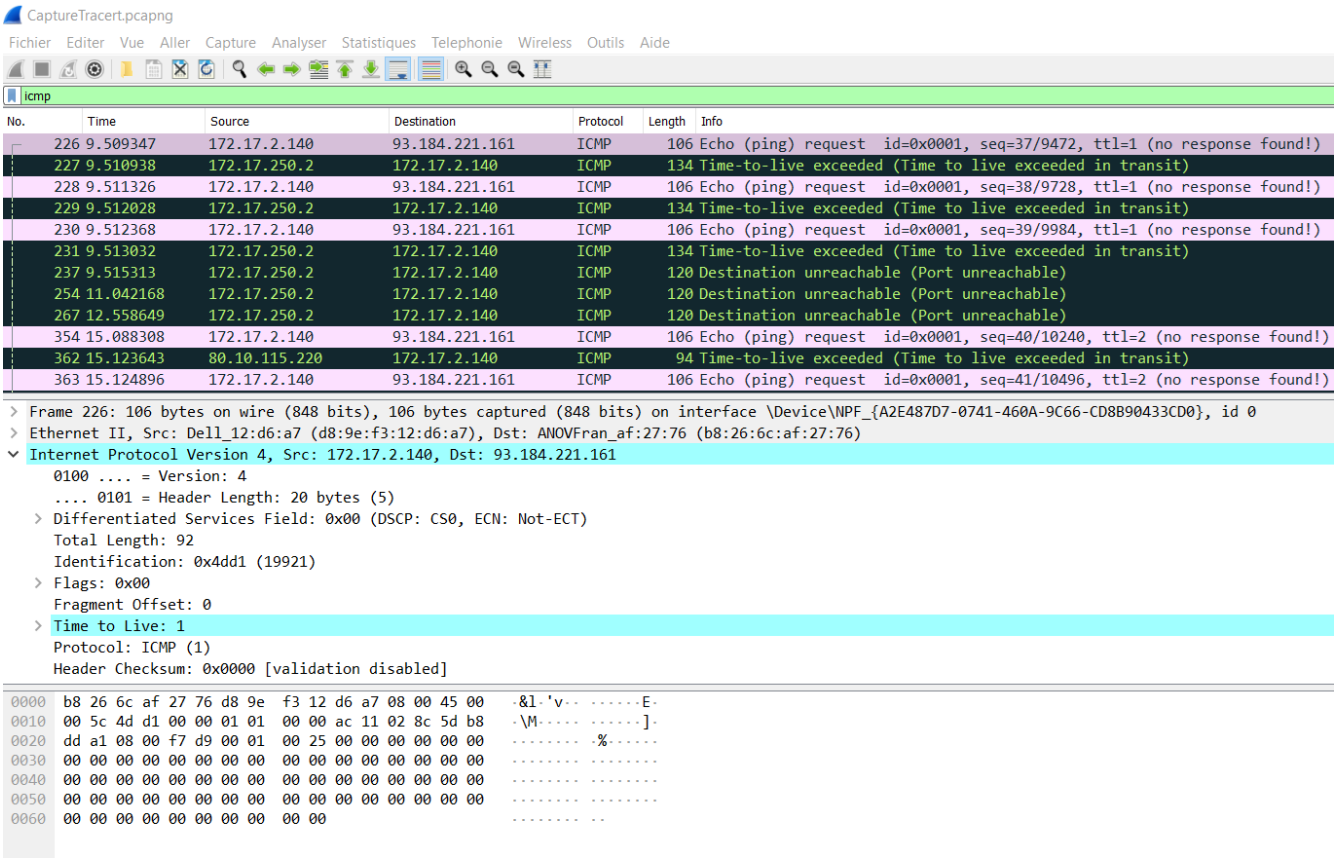
3) *Commande tracert et capture de trames ICMP*

```
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     1 ms    <1 ms    <1 ms  172.17.250.2
  2    35 ms    53 ms    78 ms  radius.lnput658.lnput658.rbci.orange.net [80.10.115.220]
  3    88 ms    76 ms    91 ms  10.123.205.178
  4    35 ms    41 ms    35 ms  ae46-0.niidf201.rbci.orange.net [193.252.98.249]
  5    34 ms    34 ms    37 ms  81.253.184.182
  6    33 ms    41 ms    41 ms  bundle-ether311.partr1.paris.opentransit.net [193.251.131.0]
  7    55 ms    56 ms    45 ms  verizondigitalmedia-11.gw.opentransit.net [193.251.255.52]
  8    34 ms    34 ms    34 ms  ae-65.core1.paa.edgecastcdn.net [152.195.108.129]
  9    33 ms    47 ms    66 ms  93.184.221.161

Itinéraire déterminé.

C:\WINDOWS\system32>
```

1ère étape: La commande tracert nous permet de connaître tous les routeurs se trouvant sur le chemin entre la machine locale qui effectue la commande et une destination donnée, comme dans notre cas ici présent avec le site internet de l'Académie de Nice.



2ème étape: Ici nous avons donc démarrer une capture de trames en effectuant simultanément la commande tracert vue précédemment, et en saisissant dans la zone de filtre seulement les trames ICMP.



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

Deci : 93.184.221.161

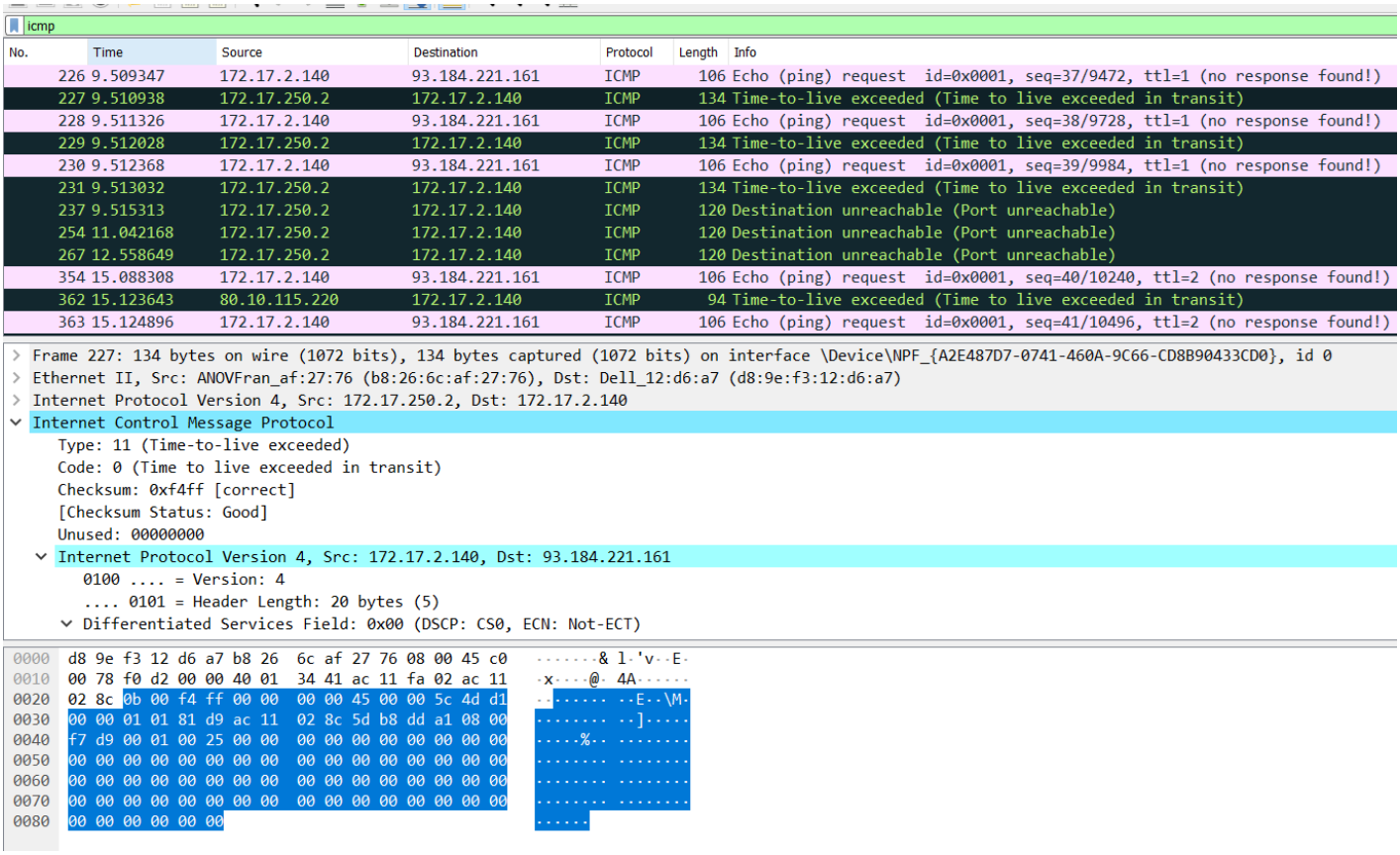
Hexa : 5d b8 dd a1

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

La valeur portée par le champ TTL (Time to Live) est égal à 01 en hexa et donc 1 en décimal.

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

La velur portée par le champ Type est 08 en hexa et 8 en décimal.



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 cette fois-ci 11 en hexa et donc 17 en décimal.