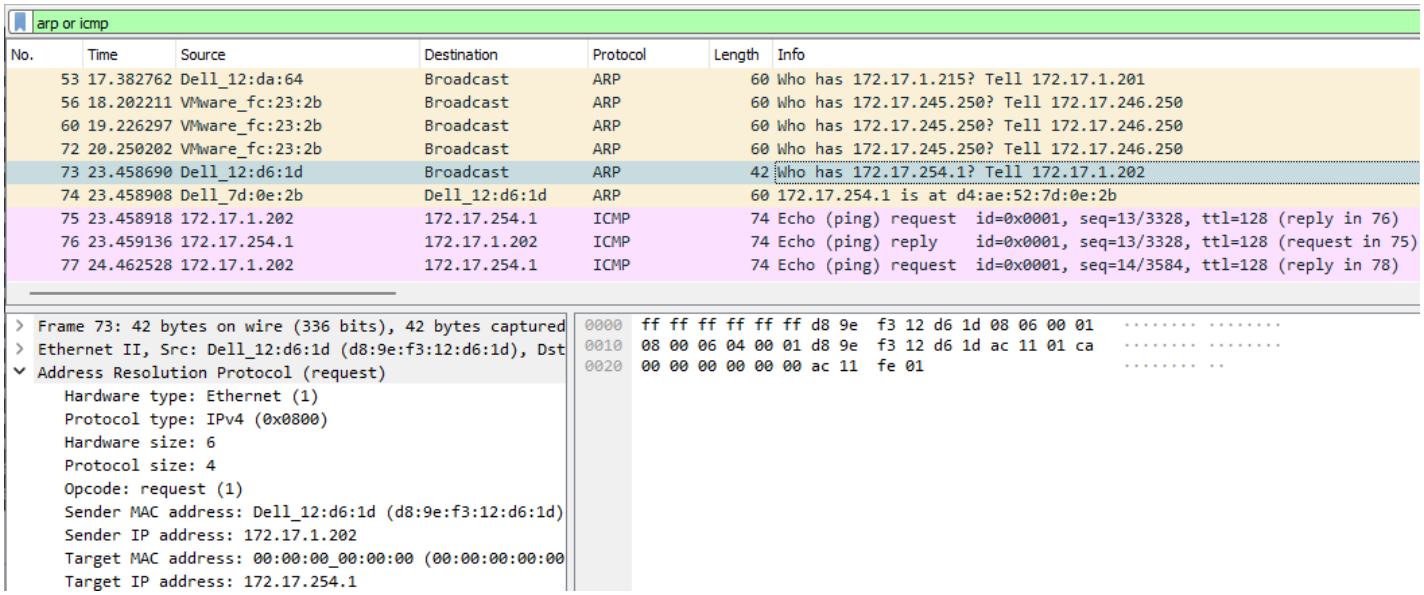
DUPUIS Laurent

TP 5 – Trames ARP, ICMP et DNS

Sommaire

1. Capture de trames ARP et ICMP

- Capture de trame suite au ping sur le serveur roi (Trame ARP et ICMP)



- Vérification du cache ARP pour vérifier la présence de ROI

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

Interface : 172.17.1.202 --- 0x8
  Adresse Internet      Adresse physique      Type
  172.17.0.1            d8-9e-f3-11-14-5f     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
  239.255.102.18        01-00-5e-7f-66-12     statique
  239.255.255.250       01-00-5e-7f-ff-fa     statique

Interface : 192.168.56.1 --- 0x11
  Adresse Internet      Adresse physique      Type
  224.0.0.22            01-00-5e-00-00-16     statique
  239.255.102.18        01-00-5e-7f-66-12     statique
  239.255.255.250       01-00-5e-7f-ff-fa     statique

Interface : 172.31.48.1 --- 0x12
  Adresse Internet      Adresse physique      Type
  224.0.0.22            01-00-5e-00-00-16     statique
  239.255.102.18        01-00-5e-7f-66-12     statique
  239.255.255.250       01-00-5e-7f-ff-fa     statique
```

- Les octets 0x0C et 0x0D, respectivement 08 06 signifient que dans Ethernet est encapsulé ARP.
- La trame ARP Request va demander en **broadcast** à toute les machines, laquelle possède une **IP précise** afin qu'elle lui renvoie son **Adresse MAC**.
- Les octets 0x04 et 0x05 ligne 0010 sont l'opcode, ici 00 01 (1) donc une request.

  Dans la reply, l'opcode est 00 02 (2)
- La longueur du message ARP dans la trame ARP request est de 28 bytes
- La longueur de la trame ARP Request est de 42 bytes
- La longueur de la tram ARP Reply est de 60 bytes
- 18 Octets sont utilisés pour le padding sur la Reply, 0 sont utilisés pour la Request
- TRAME ARP REQUEST :

  MAC Destination : FF:FF:FF:FF:FF:FF

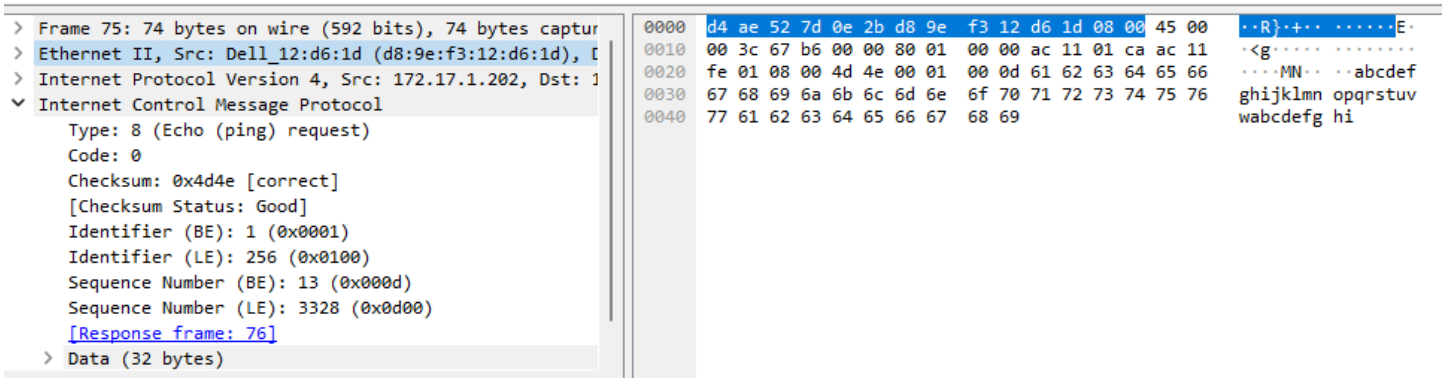
  MAC Source : d8:9e:f3:12:d6:1d

  Ethernet Type : 08 06

  Opcode : 00 01

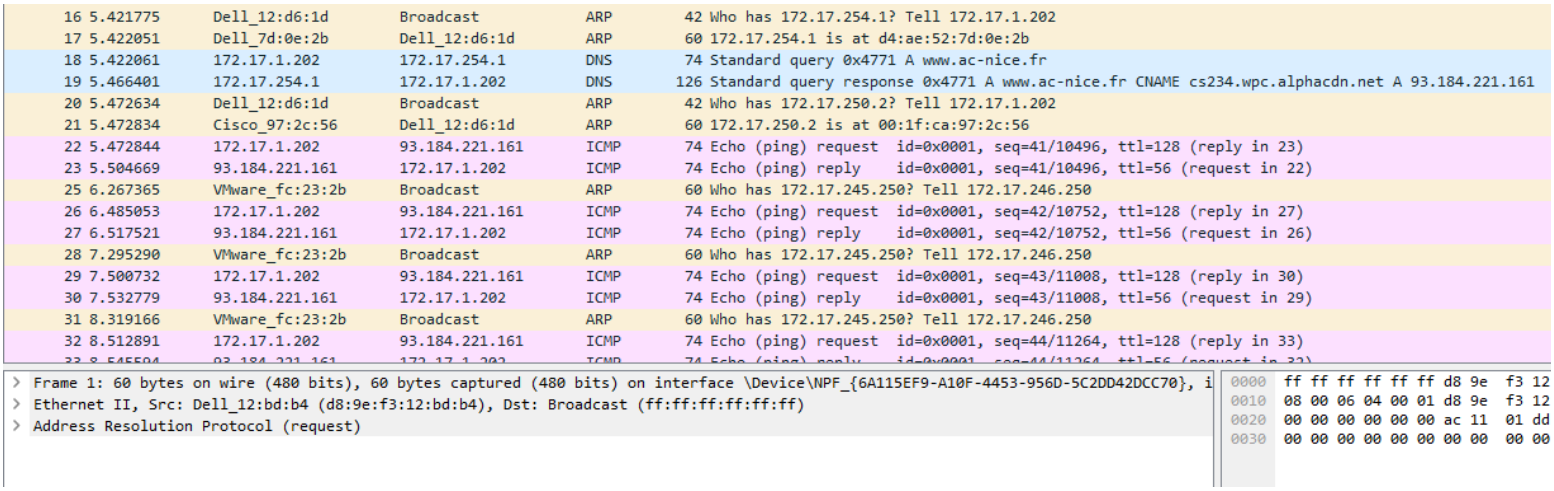
  MAC Cible : FF:FF:FF:FF:FF:FF

  IP Cible : 172.17.254.1



- Les octets 0x0C et 0x0D couche 0000, respectivement 08 00, signifie que dans la trame est encapsulé IPv4.
- L’octet 0x07 ligne 0010 a pour valeur 01, soit le protocole ICMP.
- Longueur de la trame : 74
- Longueur du paquet IP : 20
- Longueur du message ICMP : 40
- L’octet de position 0x02 ligne 0020 a pour valeur 08, qui est le type de message ICMP (request)
- 0x02 ligne 0020 de la trame ICMP Echo Reply est le champ Type, qui a pour valeur 00, soit une Reply.

2. Capture de trames ARP, DNS et ICMP



- L’adresse MAC recherchée est celle de la passerelle (172.17.250.2)

Trame ARP request
MAC Destination : FF:FF:FF:FF:FF:FF MAC Source : d8:e9:f3:12:d6

Ethernet Type:0806 (ARP)
Opcode = 00 01 (Request) MAC Cible : 00:00:00:00:00:00 IP Cible:172.17.250.2

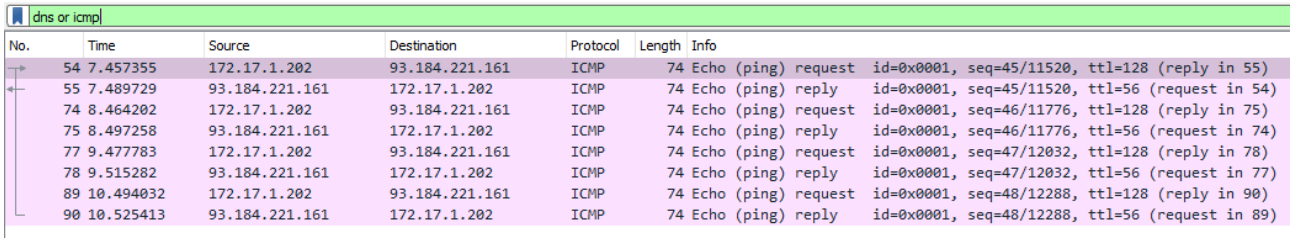
- Le ping via ICMP nécessite une adresse MAC. Pour obtenir l'adresse MAC, on doit passer par ARP à l'aide d'une IP. Pour obtenir l'ip, il faut convertir le nom de domaine en IP à l'aide de DNS.

```
Nom d'enregistrement. : roi.prince.local
Type d'enregistrement : 1
Durée de vie  . . . . : 575
Longueur de données . : 4
Section . . . . . . . : Supplémentaire
Enregistrement (hôte) : 172.17.254.1


Nom d'enregistrement. : roi2.prince.local
Type d'enregistrement : 1
Durée de vie  . . . . : 575
Longueur de données . : 4
Section . . . . . . . : Supplémentaire
Enregistrement (hôte) : 172.17.244.1


www.ac-nice.fr
----------------------------------------
Nom d'enregistrement. : www.ac-nice.fr
Type d'enregistrement : 5
Durée de vie  . . . . : 2127
Longueur de données . : 8
Section . . . . . . . : Réponse
Enregistrement CNAME  : cs234.wpc.alphacdn.net


Nom d'enregistrement. : cs234.wpc.alphacdn.net
Type d'enregistrement : 1
Durée de vie  . . . . : 2127
Longueur de données . : 4
Section . . . . . . . : Réponse
Enregistrement (hôte) : 93.184.221.161
```

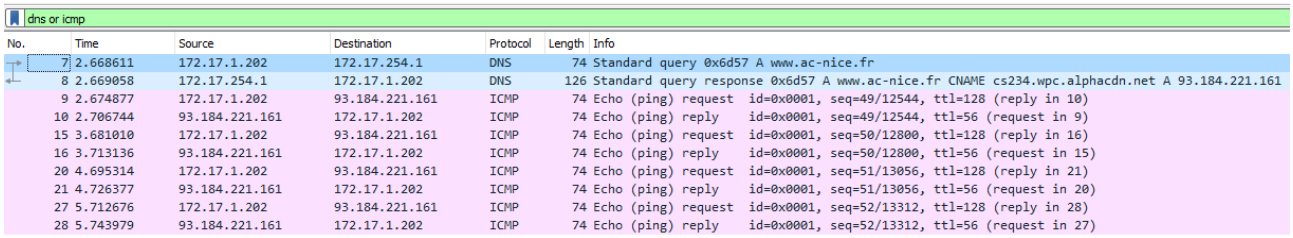


dns or icmp

No.	Time	Source	Destination	Protocol	Length	Info
54	7.457355	172.17.1.202	93.184.221.161	ICMP	74	Echo (ping) request id=0x0001, seq=45/11520, ttl=128 (reply in 55)
55	7.489729	93.184.221.161	172.17.1.202	ICMP	74	Echo (ping) reply id=0x0001, seq=45/11520, ttl=56 (request in 54)
74	8.464202	172.17.1.202	93.184.221.161	ICMP	74	Echo (ping) request id=0x0001, seq=46/11776, ttl=128 (reply in 75)
75	8.497258	93.184.221.161	172.17.1.202	ICMP	74	Echo (ping) reply id=0x0001, seq=46/11776, ttl=56 (request in 74)
77	9.477783	172.17.1.202	93.184.221.161	ICMP	74	Echo (ping) request id=0x0001, seq=47/12032, ttl=128 (reply in 78)
78	9.515282	93.184.221.161	172.17.1.202	ICMP	74	Echo (ping) reply id=0x0001, seq=47/12032, ttl=56 (request in 77)
89	10.494032	172.17.1.202	93.184.221.161	ICMP	74	Echo (ping) request id=0x0001, seq=48/12288, ttl=128 (reply in 90)
90	10.525413	93.184.221.161	172.17.1.202	ICMP	74	Echo (ping) reply id=0x0001, seq=48/12288, ttl=56 (request in 89)

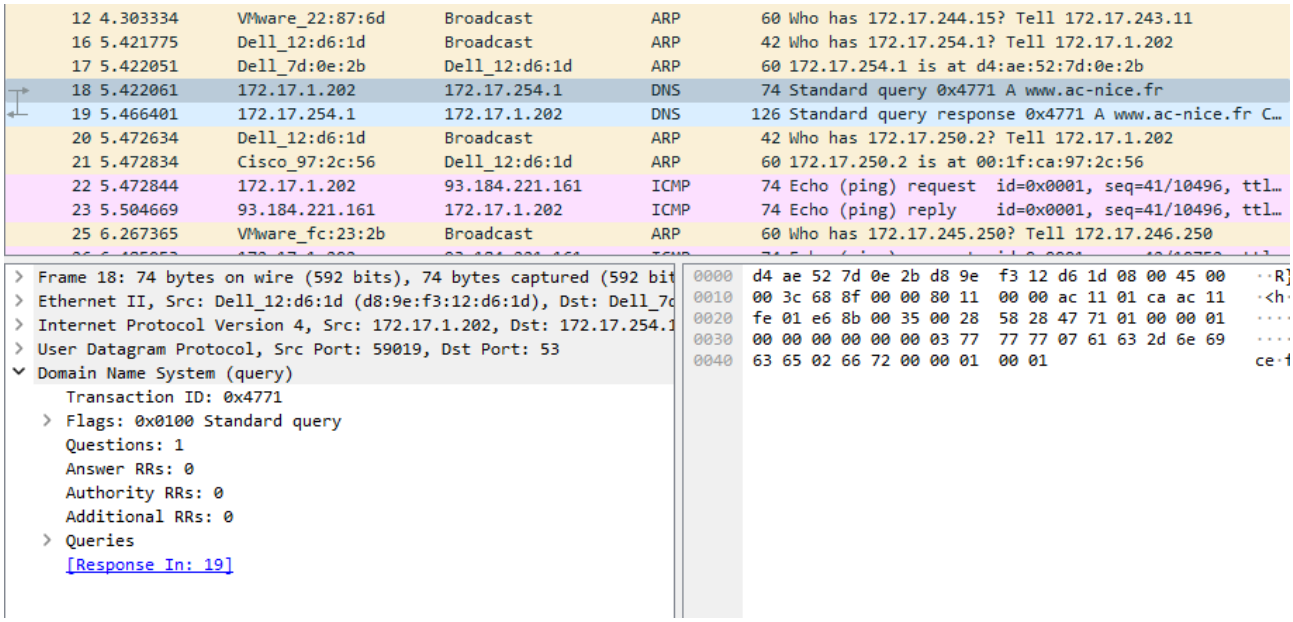
Aucune requête DNS

On vide le cache DNS afin de ré-obtenir une requête DNS



dns or icmp

No.	Time	Source	Destination	Protocol	Length	Info
7	2.668611	172.17.1.202	172.17.254.1	DNS	74	Standard query 0x6d57 A www.ac-nice.fr
8	2.669058	172.17.254.1	172.17.1.202	DNS	126	Standard query response 0x6d57 A www.ac-nice.fr CNAME cs234.wpc.alphacdn.net A 93.184.221.161
9	2.674877	172.17.1.202	93.184.221.161	ICMP	74	Echo (ping) request id=0x0001, seq=49/12544, ttl=128 (reply in 10)
10	2.706744	93.184.221.161	172.17.1.202	ICMP	74	Echo (ping) reply id=0x0001, seq=49/12544, ttl=56 (request in 9)
15	3.681010	172.17.1.202	93.184.221.161	ICMP	74	Echo (ping) request id=0x0001, seq=50/12800, ttl=128 (reply in 16)
16	3.713136	93.184.221.161	172.17.1.202	ICMP	74	Echo (ping) reply id=0x0001, seq=50/12800, ttl=56 (request in 15)
20	4.695314	172.17.1.202	93.184.221.161	ICMP	74	Echo (ping) request id=0x0001, seq=51/13056, ttl=128 (reply in 21)
21	4.726377	93.184.221.161	172.17.1.202	ICMP	74	Echo (ping) reply id=0x0001, seq=51/13056, ttl=56 (request in 20)
27	5.712676	172.17.1.202	93.184.221.161	ICMP	74	Echo (ping) request id=0x0001, seq=52/13312, ttl=128 (reply in 28)
28	5.743979	93.184.221.161	172.17.1.202	ICMP	74	Echo (ping) reply id=0x0001, seq=52/13312, ttl=56 (request in 27)

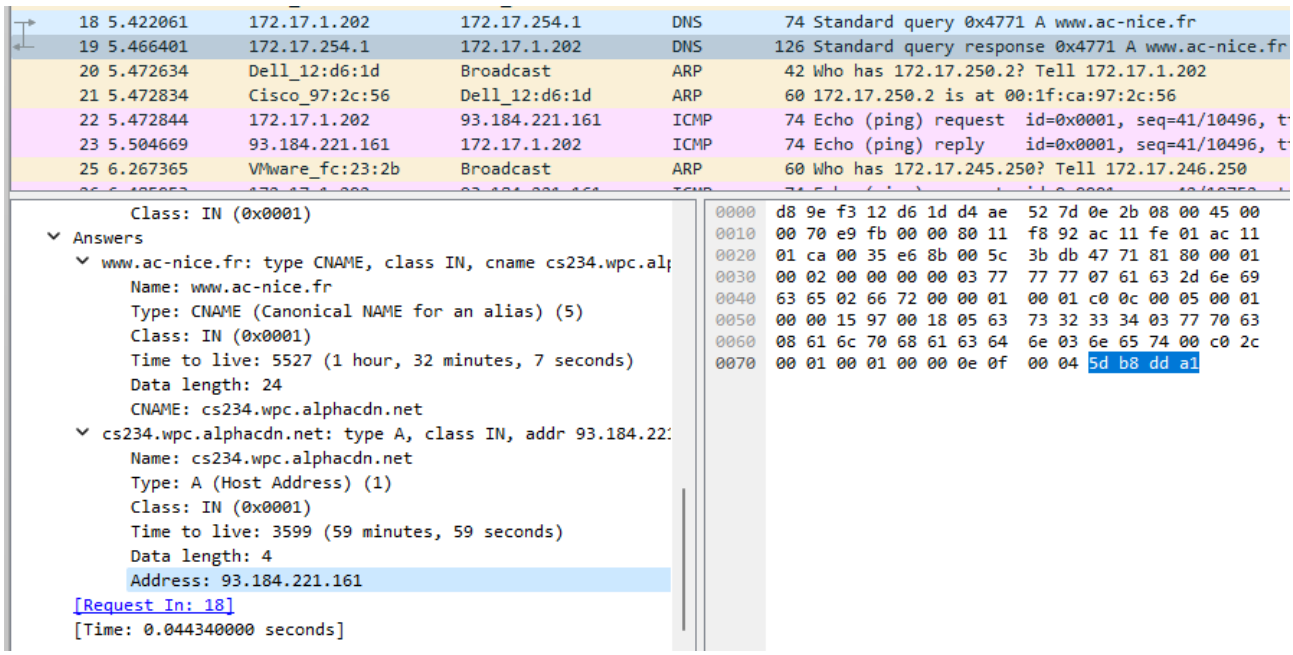


12	4.303334	VMware_22:87:6d	Broadcast	ARP	60	Who has 172.17.244.15? Tell 172.17.243.11
16	5.421775	Dell_12:d6:1d	Broadcast	ARP	42	Who has 172.17.254.1? Tell 172.17.1.202
17	5.422051	Dell_7d:0e:2b	Dell_12:d6:1d	ARP	60	172.17.254.1 is at d4:ae:52:7d:0e:2b
18	5.422061	172.17.1.202	172.17.254.1	DNS	74	Standard query 0x4771 A www.ac-nice.fr
19	5.466401	172.17.254.1	172.17.1.202	DNS	126	Standard query response 0x4771 A www.ac-nice.fr C…
20	5.472634	Dell_12:d6:1d	Broadcast	ARP	42	Who has 172.17.250.2? Tell 172.17.1.202
21	5.472834	Cisco_97:2c:56	Dell_12:d6:1d	ARP	60	172.17.250.2 is at 00:1f:ca:97:2c:56
22	5.472844	172.17.1.202	93.184.221.161	ICMP	74	Echo (ping) request id=0x0001, seq=41/10496, ttl…
23	5.504669	93.184.221.161	172.17.1.202	ICMP	74	Echo (ping) reply id=0x0001, seq=41/10496, ttl…
25	6.267365	VMware_fc:23:2b	Broadcast	ARP	60	Who has 172.17.245.250? Tell 172.17.246.250

```
> Frame 18: 74 bytes on wire (592 bits), 74 bytes captured (592 bit
> Ethernet II, Src: Dell_12:d6:1d (d8:9e:f3:12:d6:1d), Dst: Dell_7c
> Internet Protocol Version 4, Src: 172.17.1.202, Dst: 172.17.254.1
> User Datagram Protocol, Src Port: 59019, Dst Port: 53
v Domain Name System (query)
    Transaction ID: 0x4771
  > Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  > Queries
    [Response In: 19]
```

```
0000  d4 ae 52 7d 0e 2b d8 9e  f3 12 d6 1d 08 00 45 00   ··R}·+·· ····E·
0010  00 3c 68 8f 00 00 80 11  00 00 ac 11 01 ca ac 11   ·<h····· ········
0020  fe 01 e6 8b 00 35 00 28  58 28 47 71 01 00 00 01   ·····5·( X(Gq····
0030  00 00 00 00 00 00 03 77  77 77 07 61 63 2d 6e 69   ·······w ww·ac-ni
0040  63 65 02 66 72 00 00 01  00 01                    ce·fr··· ··
```

- Les différents protocoles utilisés dans une Trame DNS sont : Ethernet, IPv4, UDP, DNS
- La machine destinataire de la requête DNS est le routeur Cisco (172.17.250.2)
- L'ip du routeur est : 172.17.250.2
- Les octets de position 0x0C et 0x0D ligne 0000, respectivement 08 00 siginifie que ce qui est encapsulé dans Ethernet est IP. 0X07 ligne 0010 (11) est UDP.
- Les octets 0x04 et 0x05 ligne 0020, respectivement 00 35 (53) signifie que ce qui est encapsulé dans UDP est DNS.



- Trame DNS query : Valeur hexadécimales des octets correspondant au nom de domaine internet www.ac-nice.fr : 03 77 77 77 07 61 63 2d 6e 69 63 65 02 66 72 00
- Trame DNS response : Valeurs hexadécimales et décimales de l'adresse IP du serveur web hébergeant le site de l'académie de Nice : 5d b8 dd a1 (93.184.221.161)

3. Commande Tracert et capture de trames ICMP.

icmp

No.	Source	Destination	Protocol	Length	Info
14	192.168.1.4	93.184.221.161	ICMP	106	Echo (ping) request id=0x0001, seq=2945/33035, ttl=2 (no response found!)
18426 15.522386	192.168.1.4	93.184.221.161	ICMP	106	Echo (ping) request id=0x0001, seq=2946/33291, ttl=2 (no response found!)
22999 19.534206	192.168.1.4	93.184.221.161	ICMP	106	Echo (ping) request id=0x0001, seq=2947/33547, ttl=3 (no response found!)
27436 23.533369	192.168.1.4	93.184.221.161	ICMP	106	Echo (ping) request id=0x0001, seq=2948/33803, ttl=3 (no response found!)
28178 24.198281	194.199.224.233	192.168.1.4	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
31870 27.533024	192.168.1.4	93.184.221.161	ICMP	106	Echo (ping) request id=0x0001, seq=2949/34059, ttl=3 (no response found!)
36518 31.525185	192.168.1.4	93.184.221.161	ICMP	106	Echo (ping) request id=0x0001, seq=2950/34315, ttl=4 (no response found!)
41161 35.533055	192.168.1.4	93.184.221.161	ICMP	106	Echo (ping) request id=0x0001, seq=2951/34571, ttl=4 (no response found!)
45806 39.536000	192.168.1.4	93.184.221.161	ICMP	106	Echo (ping) request id=0x0001, seq=2952/34827, ttl=4 (no response found!)
50153 43.529783	192.168.1.4	93.184.221.161	ICMP	106	Echo (ping) request id=0x0001, seq=2953/35083, ttl=5 (no response found!)
50186 43.546124	212.194.170.74	192.168.1.4	ICMP	182	Time-to-live exceeded (Time to live exceeded in transit)
50187 43.546590	192.168.1.4	93.184.221.161	ICMP	106	Echo (ping) request id=0x0001, seq=2954/35339, ttl=5 (no response found!)
50219 43.565698	212.194.170.74	192.168.1.4	ICMP	182	Time-to-live exceeded (Time to live exceeded in transit)
50220 43.568172	192.168.1.4	93.184.221.161	ICMP	106	Echo (ping) request id=0x0001, seq=2955/35595, ttl=5 (no response found!)
50233 43.584744	212.194.170.74	192.168.1.4	ICMP	182	Time-to-live exceeded (Time to live exceeded in transit)
51169 44.587165	192.168.1.4	93.184.221.161	ICMP	106	Echo (ping) request id=0x0001, seq=2956/35851, ttl=6 (no response found!)
51191 44.603269	212.194.171.9	192.168.1.4	ICMP	182	Time-to-live exceeded (Time to live exceeded in transit)
51192 44.604131	192.168.1.4	93.184.221.161	ICMP	106	Echo (ping) request id=0x0001, seq=2957/36107, ttl=6 (no response found!)
51209 44.621001	212.194.171.9	192.168.1.4	ICMP	182	Time-to-live exceeded (Time to live exceeded in transit)
51212 44.622066	192.168.1.4	93.184.221.161	ICMP	106	Echo (ping) request id=0x0001, seq=2958/36363, ttl=6 (no response found!)
51231 44.638281	212.194.171.9	192.168.1.4	ICMP	182	Time-to-live exceeded (Time to live exceeded in transit)
56845 50.185115	192.168.1.4	93.184.221.161	ICMP	106	Echo (ping) request id=0x0001, seq=2959/36619, ttl=7 (no response found!)
56863 50.201992	212.194.171.141	192.168.1.4	ICMP	182	Time-to-live exceeded (Time to live exceeded in transit)
56864 50.203143	192.168.1.4	93.184.221.161	ICMP	106	Echo (ping) request id=0x0001, seq=2960/36875, ttl=7 (no response found!)
56882 50.219514	212.194.171.141	192.168.1.4	ICMP	182	Time-to-live exceeded (Time to live exceeded in transit)
56883 50.220388	192.168.1.4	93.184.221.161	ICMP	106	Echo (ping) request id=0x0001, seq=2961/37131, ttl=7 (no response found!)
56900 50.236062	212.194.171.141	192.168.1.4	ICMP	182	Time-to-live exceeded (Time to live exceeded in transit)
57948 51.227848	192.168.1.4	93.184.221.161	ICMP	106	Echo (ping) request id=0x0001, seq=2962/37387, ttl=8 (no response found!)
61881 55.036061	192.168.1.4	93.184.221.161	ICMP	106	Echo (ping) request id=0x0001, seq=2963/37643, ttl=8 (no response found!)
61889 55.053323	62.34.2.88	192.168.1.4	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
61890 55.054433	192.168.1.4	93.184.221.161	ICMP	106	Echo (ping) request id=0x0001, seq=2964/37899, ttl=8 (no response found!)
61912 55.071257	62.34.2.88	192.168.1.4	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
68424 60.604787	192.168.1.4	93.184.221.161	ICMP	106	Echo (ping) request id=0x0001, seq=2965/38155, ttl=9 (no response found!)
68433 60.620988	152.195.108.200	192.168.1.4	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
68437 60.622197	192.168.1.4	93.184.221.161	ICMP	106	Echo (ping) request id=0x0001, seq=2966/38411, ttl=9 (no response found!)
68453 60.640109	152.195.108.200	192.168.1.4	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
68454 60.641395	192.168.1.4	93.184.221.161	ICMP	106	Echo (ping) request id=0x0001, seq=2967/38667, ttl=9 (no response found!)
68484 60.658845	152.195.108.200	192.168.1.4	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
69595 61.644982	192.168.1.4	93.184.221.161	ICMP	106	Echo (ping) request id=0x0001, seq=2968/38923, ttl=10 (no response found!)
69617 61.662496	152.195.108.129	192.168.1.4	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
69622 61.664016	192.168.1.4	93.184.221.161	ICMP	106	Echo (ping) request id=0x0001, seq=2969/39179, ttl=10 (no response found!)
69659 61.686070	152.195.108.129	192.168.1.4	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
69660 61.687050	192.168.1.4	93.184.221.161	ICMP	106	Echo (ping) request id=0x0001, seq=2970/39435, ttl=10 (no response found!)
69678 61.704083	152.195.108.129	192.168.1.4	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
70684 62.700495	192.168.1.4	93.184.221.161	ICMP	106	Echo (ping) request id=0x0001, seq=2971/39691, ttl=11 (reply in 70705)
70705 62.718735	93.184.221.161	192.168.1.4	ICMP	106	Echo (ping) reply id=0x0001, seq=2971/39691, ttl=54 (request in 70684)
70710 62.720045	192.168.1.4	93.184.221.161	ICMP	106	Echo (ping) request id=0x0001, seq=2972/39947, ttl=11 (reply in 70723)
70723 62.739199	93.184.221.161	192.168.1.4	ICMP	106	Echo (ping) reply id=0x0001, seq=2972/39947, ttl=54 (request in 70710)
70727 62.740664	192.168.1.4	93.184.221.161	ICMP	106	Echo (ping) request id=0x0001, seq=2973/40203, ttl=11 (reply in 70745)
70745 62.757650	93.184.221.161	192.168.1.4	ICMP	106	Echo (ping) reply id=0x0001, seq=2973/40203, ttl=54 (request in 70727)
78088 69.201265	194.199.224.233	192.168.1.4	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)

```
C:\Users\dupui>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  bouygues [192.168.1.254]
  2     *        *        *     Délai d'attente de la demande dépassé.
  3     *        *        *     Délai d'attente de la demande dépassé.
  4     *        *        *     Délai d'attente de la demande dépassé.
  5    16 ms    19 ms    16 ms  be21.cbr01-poi.net.bbox.fr [212.194.170.74]
  6    16 ms    16 ms    16 ms  212.194.171.9
  7    16 ms    16 ms    15 ms  be5.cbr01-cro.net.bbox.fr [212.194.171.141]
  8     *       17 ms    16 ms  62.34.2.88
  9    16 ms    17 ms    17 ms  ae-130.border1.pam.edgecastcdn.net [152.195.108.200]
 10    17 ms    22 ms    17 ms  ae-65.core1.paa.edgecastcdn.net [152.195.108.129]
 11    18 ms    19 ms    17 ms  93.184.221.161

Itinéraire déterminé.
```

- Première trame ICMP Echo Request :

  IP Destination : 5d b8 dd a1 soit 93.184.221.161

  Champ TTL : 01 soit 1

  Valeur du champ Type : 08 soit 8

- Valeur du champ Type de la trame d’erreur TTL : 11 soit 0b