

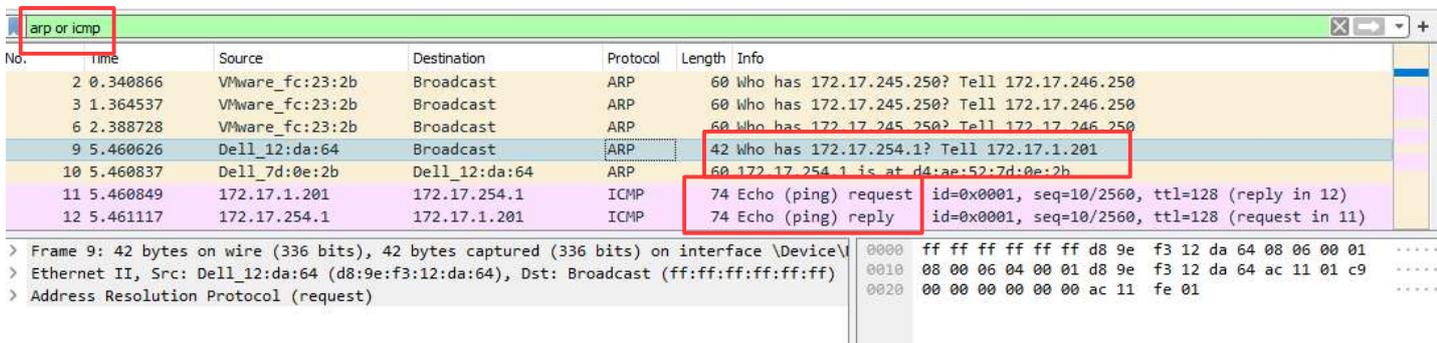
TP 5 – Trames ARP, ICMP et DNS

Sommaire :

1. Capture de trames ARP et ICMP :.....1
2. Capture de trames ARP, DNS et ICMP.....4
3. Commande Tracert et capture de trames ICMP.....7

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 » sur 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 0x0C et 0x0D ligne 0000 ?

L'échange dans les octets de position 0x0C et 0x0D 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 0x04 et 0x05 ligne 0010 ?

La signification des octets de position 0x04 et 0x05 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 qui correspondent 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 0020 ?**

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 0x02 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 :

No.	Time	Source	Destination	Protocol	Length	Info
16	3.377912	172.17.1.201	172.17.254.1	DNS	74	Standard query 0xia50 A www.ac-nice.fr
17	3.378418	172.17.254.1	172.17.1.201	DNS	126	Standard query response 0xia50 A www.ac-nice.fr CNAME cs
18	3.384543	Dell_12:da:64	Broadcast	ARP	42	Who has 172.17.250.2? Tell 172.17.1.201
19	3.384743	Cisco_97:2c:56	Dell_12:da:64	ARP	60	172.17.250.2 is at 00:1f:ca:97:2c:56
20	3.384753	172.17.1.201	93.184.221.161	ICMP	74	Echo (ping) request id=0x0001, seq=26/6656, ttl=128 (re
21	3.416621	93.184.221.161	172.17.1.201	ICMP	74	Echo (ping) reply id=0x0001, seq=26/6656, ttl=56 (req
26	3.980962	VMware_96:18:19	Broadcast	ARP	60	Who has 172.17.245.10? Tell 172.17.246.10
27	4.000275	VMware_22:87:6d	Broadcast	ARP	60	Who has 172.17.244.15? Tell 172.17.243.11
28	4.399301	172.17.1.201	93.184.221.161	ICMP	74	Echo (ping) request id=0x0001, seq=27/6912, ttl=128 (re
29	4.430946	93.184.221.161	172.17.1.201	ICMP	74	Echo (ping) reply id=0x0001, seq=27/6912, ttl=56 (req
30	4.723577	VMware_fc:23:2b	Broadcast	ARP	60	Who has 172.17.245.250? Tell 172.17.246.250
32	4.980658	VMware_96:18:19	Broadcast	ARP	60	Who has 172.17.245.10? Tell 172.17.246.10
33	5.411373	172.17.1.201	93.184.221.161	ICMP	74	Echo (ping) request id=0x0001, seq=28/7168, ttl=128 (re
34	5.442808	93.184.221.161	172.17.1.201	ICMP	74	Echo (ping) reply id=0x0001, seq=28/7168, ttl=56 (req
35	5.723738	VMware_fc:23:2b	Broadcast	ARP	60	Who has 172.17.245.250? Tell 172.17.246.250

> Frame 18: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface
 > Ethernet II, Src: Dell_12:da:64 (d8:9e:f3:12:da:64), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
 > Address Resolution Protocol (request)

```

0000 ff ff ff ff ff ff d8 9e f3 12 da 64 08 06 00 01
0010 08 00 06 04 00 01 d8 9e f3 12 da 64 ac 11 01 c9
0020 00 00 00 00 00 00 ac 11 fa 02
  
```

- 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)

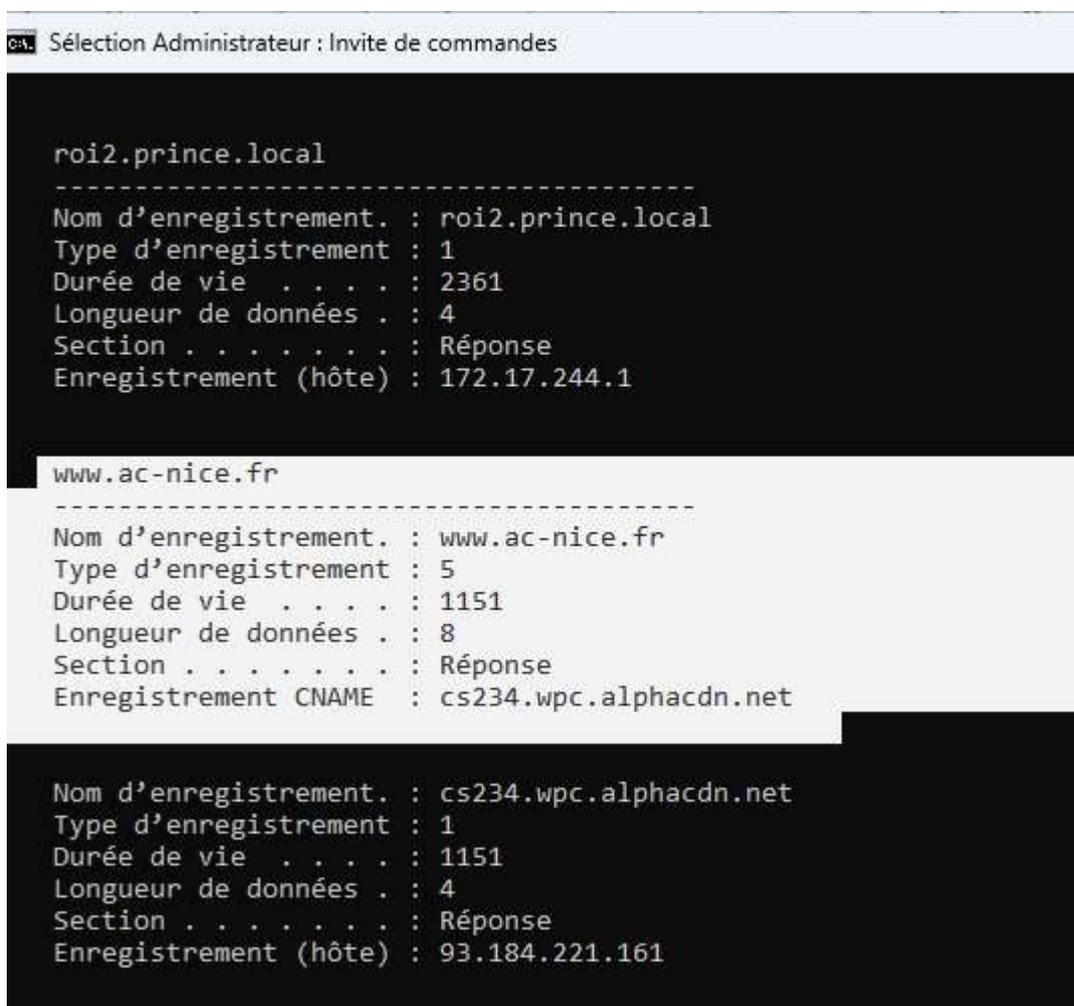
- Complétez les rubriques ci-dessous :

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 :



```
Sélection Administrateur : Invite de commandes

roi2.prince.local
-----
Nom d'enregistrement. : roi2.prince.local
Type d'enregistrement : 1
Durée de vie . . . . : 2361
Longueur de données . : 4
Section . . . . . : Réponse
Enregistrement (hôte) : 172.17.244.1

www.ac-nice.fr
-----
Nom d'enregistrement. : www.ac-nice.fr
Type d'enregistrement : 5
Durée de vie . . . . : 1151
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 . . . . : 1151
Longueur de données . : 4
Section . . . . . : Réponse
Enregistrement (hôte) : 93.184.221.161
```

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 »

No.	Time	Source	Destination	Protocol	Length	Info
12	7.847152	172.17.1.201	93.184.221.161	ICMP	74	Echo (ping) request id=0x0001, seq=34/8704, ttl=128 (reply in 13)
13	7.879641	93.184.221.161	172.17.1.201	ICMP	74	Echo (ping) reply id=0x0001, seq=34/8704, ttl=56 (request in 12)
18	8.855790	172.17.1.201	93.184.221.161	ICMP	74	Echo (ping) request id=0x0001, seq=35/8960, ttl=128 (reply in 19)
19	8.887540	93.184.221.161	172.17.1.201	ICMP	74	Echo (ping) reply id=0x0001, seq=35/8960, ttl=56 (request in 18)
21	9.868959	172.17.1.201	93.184.221.161	ICMP	74	Echo (ping) request id=0x0001, seq=36/9216, ttl=128 (reply in 22)
22	9.901491	93.184.221.161	172.17.1.201	ICMP	74	Echo (ping) reply id=0x0001, seq=36/9216, ttl=56 (request in 21)
24	10.882903	172.17.1.201	93.184.221.161	ICMP	74	Echo (ping) request id=0x0001, seq=37/9472, ttl=128 (reply in 25)
25	10.914324	93.184.221.161	172.17.1.201	ICMP	74	Echo (ping) reply id=0x0001, seq=37/9472, ttl=56 (request in 24)

Frame 12: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface Ethernet II, Src: Dell_12:da:64 (d8:9e:f3:12:da:64), Dst: Cisco_97:2c:56 (00:1f:00:00:00:00), Protocol: Internet Protocol Version 4, Src: 172.17.1.201, Dst: 93.184.221.161, Length: 74, Info: Internet Control Message Protocol	0000 00 1f ca 97 2c 56 d8 9e f3 12 da 64 08 00 45 00 0010 00 3c e9 bb 00 00 80 01 00 00 ac 11 01 c9 5d b8 0020 dd a1 08 00 4d 39 00 01 00 22 61 62 63 64 65 66 0030 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76 0040 77 61 62 63 64 65 66 67 68 69
---	--

No.	Time	Source	Destination	Protocol	Length	Info
12	3.261816	Vmware_96:18:19	Broadcast	ARP	60	Who has 172.17.245.10? Tell 172.17.246.10
14	3.377608	Dell_12:da:64	Broadcast	ARP	42	Who has 172.17.254.1? Tell 172.17.1.201
15	3.377901	Dell_7d:0e:2b	Dell_12:da:64	ARP	60	172.17.254.1 is at d4:ae:52:7d:0e:2b
16	3.377912	172.17.1.201	172.17.254.1	DNS	74	Standard query 0x1a50 A www.ac-nice.fr
17	3.378418	172.17.254.1	172.17.1.201	DNS	126	Standard query response 0x1a50 A www.ac-nice.fr CNAME cs234.wpc.alphacdn.com
18	3.384543	Dell_12:da:64	Broadcast	ARP	42	Who has 172.17.250.2? Tell 172.17.1.201
19	3.384743	Cisco_97:2c:56	Dell_12:da:64	ARP	60	172.17.250.2 is at 00:1f:ca:97:2c:56
20	3.384753	172.17.1.201	93.184.221.161	ICMP	74	Echo (ping) request id=0x0001, seq=26/6656, ttl=128 (reply in 21)
21	3.416621	93.184.221.161	172.17.1.201	ICMP	74	Echo (ping) reply id=0x0001, seq=26/6656, ttl=56 (request in 20)
26	3.980962	Vmware_96:18:19	Broadcast	ARP	60	Who has 172.17.245.10? Tell 172.17.246.10
27	4.000275	Vmware_22:87:6d	Broadcast	ARP	60	Who has 172.17.244.15? Tell 172.17.243.11
28	4.399301	172.17.1.201	93.184.221.161	ICMP	74	Echo (ping) request id=0x0001, seq=27/6912, ttl=128 (reply in 29)

> Frame 17: 126 bytes on wire (1008 bits), 126 bytes captured (1008 bits) on interface Ethernet II, Src: Dell_7d:0e:2b (d4:ae:52:7d:0e:2b), Dst: Dell_12:da:64 (d8:9e:f3:12:da:64), Protocol: Internet Protocol Version 4, Src: 172.17.254.1, Dst: 172.17.1.201, Length: 126, Info: User Datagram Protocol, Src Port: 53, Dst Port: 52050, Domain Name System (response)	0000 d8 9e f3 12 da 64 d4 ae 52 7d 0e 2b 08 00 45 00d..R]--+E- 0010 00 70 19 06 00 00 80 11 c9 89 ac 11 fe 01 ac 11p..... 0020 01 c9 00 35 cb 52 00 5c 8b cf 1a 50 81 80 00 01S-R-\ ...P.... 0030 00 02 00 00 00 00 03 77 77 77 07 61 63 2d 6e 69w ww-ac-ni 0040 63 65 02 66 72 00 00 01 00 01 c0 0c 00 05 00 01 ce-fr..... 0050 00 00 11 ca 00 18 05 63 73 32 33 34 03 77 70 63c s234-wpc 0060 08 61 6c 70 68 61 63 64 6e 03 6e 65 74 00 c0 2c -alphacd n-net-.. 0070 00 01 00 01 00 00 0a 43 00 04 5d b8 dd a1C ...]
--	---

▪ **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 0x04 et 0x05 ligne 0020 ?**

Les octets de position 0x04 et 0x05 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 hexadécimales des octets sont :

```

> Frame 16: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{DE509220-0000 d4 ae 52 7d 0e 2b d8 9e f3 12 da 64 08 00 45 00}
> Ethernet II, Src: Dell_12:da:64 (d8:9e:f3:12:da:64), Dst: Dell_7d:0e:2b (d4:ae:52:7d:0e:2b)
> Internet Protocol Version 4, Src: 172.17.1.201, Dst: 172.17.254.1
> User Datagram Protocol, Src Port: 52050, Dst Port: 53
v Domain Name System (query)
  Transaction ID: 0x1a50
  > Flags: 0x0100 Standard query
  Questions: 1
  Answer RRs: 0
  Authority RRs: 0
  Additional RRs: 0
  v Queries
    v www.ac-nice.fr: type A, class IN
      Name: www.ac-nice.fr
      Flags: Length: 141
0000 d4 ae 52 7d 0e 2b d8 9e f3 12 da 64 08 00 45 00  ..R}..+.. ...d--E.
0010 00 3c f3 98 00 00 80 11 00 00 ac 11 01 c9 ac 11  <.....
0020 fe 01 cb 52 00 35 00 28 58 27 1a 50 01 00 00 01  ...R.5 (X'.P...
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.....
  
```

- **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.

*Wi-Fi

Fichier Editer Vue Aller Capture Analyser Statistiques Telephonie Wireless Outils Aide

icmp

No.	Time	Source	Destination	Protocol	Length	Info
37251	43.961623	37.77.34.103	192.168.1.133	ICMP	70	Time-to-live exceeded (Time to live exceeded in tra
37254	43.962945	192.168.1.133	93.184.221.161	ICMP	106	Echo (ping) request id=0x0001, seq=132/33792, ttl=6
37276	43.983348	37.77.34.103	192.168.1.133	ICMP	70	Time-to-live exceeded (Time to live exceeded in tra
41441	49.559438	192.168.1.133	93.184.221.161	ICMP	106	Echo (ping) request id=0x0001, seq=133/34048, ttl=7
41459	49.579834	152.195.108.129	192.168.1.133	ICMP	70	Time-to-live exceeded (Time to live exceeded in tra
41467	49.582173	192.168.1.133	93.184.221.161	ICMP	106	Echo (ping) request id=0x0001, seq=134/34304, ttl=7
41491	49.602897	152.195.108.129	192.168.1.133	ICMP	70	Time-to-live exceeded (Time to live exceeded in tra
41495	49.604758	192.168.1.133	93.184.221.161	ICMP	106	Echo (ping) request id=0x0001, seq=135/34560, ttl=7
41519	49.630592	152.195.108.129	192.168.1.133	ICMP	70	Time-to-live exceeded (Time to live exceeded in tra
1587...	166.351528	192.168.1.133	93.184.221.161	ICMP	106	Echo (ping) request id=0x0001, seq=136/34816, ttl=8
1587...	166.371412	93.184.221.161	192.168.1.133	ICMP	106	Echo (ping) reply id=0x0001, seq=136/34816, ttl=8
1587...	166.373908	192.168.1.133	93.184.221.161	ICMP	106	Echo (ping) request id=0x0001, seq=137/35072, ttl=8
1587...	166.417220	93.184.221.161	192.168.1.133	ICMP	106	Echo (ping) reply id=0x0001, seq=137/35072, ttl=8

> Frame 158755: 106 bytes on wire (848 bits), 106 bytes captured (848 bits) on interface 0
 > Ethernet II, Src: CyberTAN_b4:3d:6b (60:14:b3:b4:3d:6b), Dst: FreeSpace_08:00:27:00:00:00
 > Internet Protocol Version 4, Src: 192.168.1.133, Dst: 93.184.221.161
 > Internet Control Message Protocol

```

0000  70 fc 8f 56 be a1 60 14  b3 b4 3d 6b 08 00 45 00  p...V...
0010  00 5c 2b d4 00 00 08 01  89 46 c0 a8 01 85 5d b8  -\+.....
0020  dd a1 08 00 f7 74 00 01  00 8a 00 00 00 00 00 00  .....t..
0030  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  .....
0040  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  .....
0050  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  .....
0060  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  .....
  
```

```

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.