

## TP 5- Trames ARP, ICMP et DNS

Nesrine EL AHMADI

**BTS SIO**

### Table des matières

1. Capture de trames ARP et ICMP.....	2
2. Capture de trames ARP , DNS et ICMP.....	7

# 1. Capture de trames ARP et ICMP

On capture les trames grâce à l'outil Wireshark et on ping le **serveur ROI** ( Capture 1 ).

```
C:\Windows\System32>ping 172.17.254.5

Envoi d'une requête 'Ping' 172.17.254.5 avec 32 octets de données :
Réponse de 172.17.254.5 : octets=32 temps<1ms TTL=64
Réponse de 172.17.254.5 : octets=32 temps<1ms TTL=64
Réponse de 172.17.254.5 : octets=32 temps<1ms TTL=64
Réponse de 172.17.254.5 : octets=32 temps<1ms TTL=64

Statistiques Ping pour 172.17.254.5:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 0ms, Maximum = 0ms, Moyenne = 0ms
```

Capture 1

(La deuxième capture est le ping du serveur de mon ordinateur personnel car j'ai du refaire une partie du TP)

```
C:\Windows\System32>ping 192.168.1.254

Envoi d'une requête 'Ping' 192.168.1.254 avec 32 octets de données :
Réponse de 192.168.1.254 : octets=32 temps=5 ms TTL=64
Réponse de 192.168.1.254 : octets=32 temps=10 ms TTL=64
Réponse de 192.168.1.254 : octets=32 temps=9 ms TTL=64
Réponse de 192.168.1.254 : octets=32 temps=7 ms TTL=64

Statistiques Ping pour 192.168.1.254:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 5ms, Maximum = 10ms, Moyenne = 7ms

C:\Windows\System32>_
```

On filtre les trames en inscrivant **arp or icmp** dans Wireshark ( Capture 3) .

**\*Wi-Fi**

Fichier   Editor   Vue   Aller   Capture   Analyser   Statistiques   Telephonie   Wireless   Outils   Aide

**arp or icmp**

No.	Time	Source	Destination	Protocol	Length	Info
11	2.048841	192.168.1.92	192.168.1.254	ICMP	74	Echo (ping) request id=0x0001, seq=24/6144, ttl=128 (reply in 12)
12	2.068710	192.168.1.254	192.168.1.92	ICMP	74	Echo (ping) reply id=0x0001, seq=24/6144, ttl=64 (request in 11)
14	3.064107	192.168.1.92	192.168.1.254	ICMP	74	Echo (ping) request id=0x0001, seq=25/6400, ttl=128 (reply in 15)
15	3.074697	192.168.1.254	192.168.1.92	ICMP	74	Echo (ping) reply id=0x0001, seq=25/6400, ttl=64 (request in 14)
18	4.076950	192.168.1.92	192.168.1.254	ICMP	74	Echo (ping) request id=0x0001, seq=26/6656, ttl=128 (reply in 19)
19	4.084141	192.168.1.254	192.168.1.92	ICMP	74	Echo (ping) reply id=0x0001, seq=26/6656, ttl=64 (request in 18)
52	5.090711	192.168.1.92	192.168.1.254	ICMP	74	Echo (ping) request id=0x0001, seq=27/6912, ttl=128 (reply in 53)
53	5.096198	192.168.1.254	192.168.1.92	ICMP	74	Echo (ping) reply id=0x0001, seq=27/6912, ttl=64 (request in 52)
79	9.722274	6a:5a:00:ec:c4:37	LiteonTechno_f1:07:...	ARP	52	Who has 192.168.1.135? Tell 192.168.1.254
80	9.722274	6a:5a:00:ec:c4:37	LiteonTechno_f1:07:...	ARP	52	Who has 192.168.1.77? Tell 192.168.1.254
81	9.722274	6a:5a:00:ec:c4:37	LiteonTechno_f1:07:...	ARP	52	Who has 192.168.1.92? Tell 192.168.1.254
82	9.722312	LiteonTechno_f1:07:...	VantivaUSA_ec:c4:3c	ARP	42	192.168.1.92 is at 24:b2:b9:f1:07:13

— Avec PC

Capture 3

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

Interface : 192.168.1.92 --- 0x4
  Adresse Internet    Adresse physique    Type
  192.168.1.4         d0-05-2a-b2-d5-4b   dynamique
  192.168.1.143       14-c1-4e-01-fd-36   dynamique
  192.168.1.157       a0-d0-5b-c7-85-44   dynamique
  192.168.1.254       d0-5a-00-ec-c4-3c   dynamique
  192.168.1.255       ff-ff-ff-ff-ff-ff   statique
  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
  255.255.255.255     ff-ff-ff-ff-ff-ff   statique

Interface : 192.168.56.1 --- 0x12
  Adresse Internet    Adresse physique    Type
  192.168.56.255      ff-ff-ff-ff-ff-ff   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

C:\Windows\System32>

C:\Windows\System32>arp -d *

C:\Windows\System32>arp -a

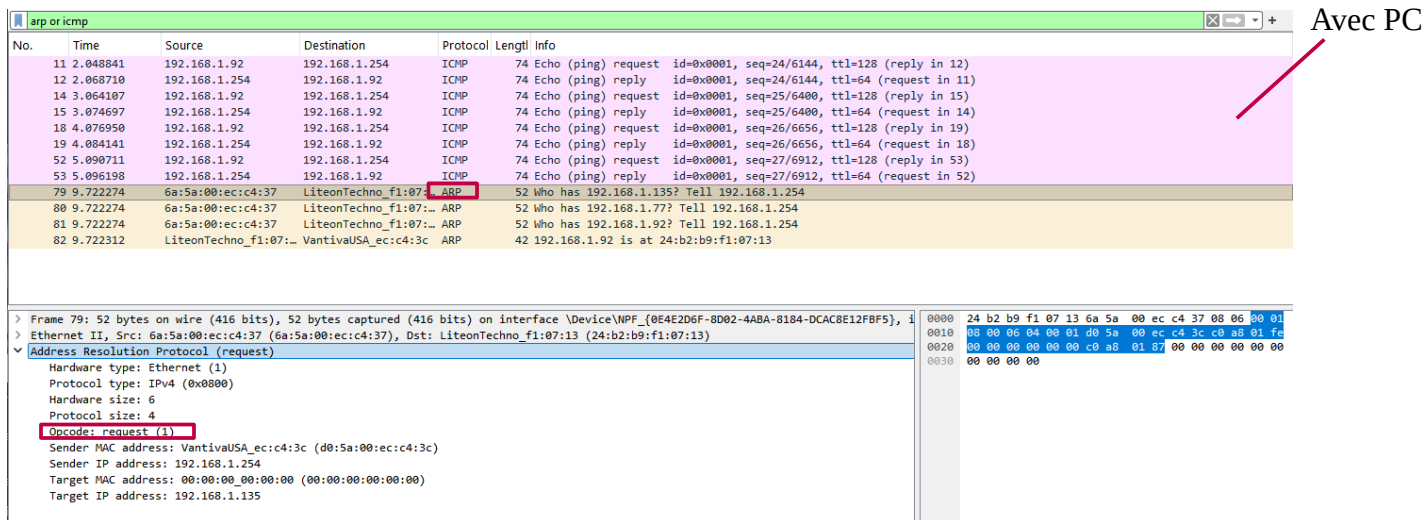
Interface : 192.168.1.92 --- 0x4
  Adresse Internet    Adresse physique    Type
  192.168.1.4         d0-05-2a-b2-d5-4b   dynamique
  192.168.1.143       14-c1-4e-01-fd-36   dynamique
  192.168.1.254       d0-5a-00-ec-c4-3c   dynamique
  224.0.0.2           01-00-5e-00-00-02   statique
  224.0.0.22          01-00-5e-00-00-16   statique

Interface : 192.168.56.1 --- 0x12
  Adresse Internet    Adresse physique    Type
  224.0.0.22          01-00-5e-00-00-16   statique

C:\Windows\System32>
```

On a pas l'@IP et l'@ MAC correspondant à Aviateur car cette partie du TP a été faite avec mon PC.

Grace au trames ARP ( Request et Reply ) ( Capture 4 ) précédant l'échange de trames ICMP on peut répondre aux questions suivantes :



No.	Time	Source	Destination	Protocol	Length	Info
11	2.048841	192.168.1.92	192.168.1.254	ICMP	74	Echo (ping) request id=0x0001, seq=24/6144, ttl=128 (reply in 12)
12	2.068710	192.168.1.254	192.168.1.92	ICMP	74	Echo (ping) reply id=0x0001, seq=24/6144, ttl=64 (request in 11)
14	3.064107	192.168.1.92	192.168.1.254	ICMP	74	Echo (ping) request id=0x0001, seq=25/6400, ttl=128 (reply in 15)
15	3.074697	192.168.1.254	192.168.1.92	ICMP	74	Echo (ping) reply id=0x0001, seq=25/6400, ttl=64 (request in 14)
18	4.076950	192.168.1.92	192.168.1.254	ICMP	74	Echo (ping) request id=0x0001, seq=26/6656, ttl=128 (reply in 19)
19	4.084141	192.168.1.254	192.168.1.92	ICMP	74	Echo (ping) reply id=0x0001, seq=26/6656, ttl=64 (request in 18)
52	5.090711	192.168.1.92	192.168.1.254	ICMP	74	Echo (ping) request id=0x0001, seq=27/6912, ttl=128 (reply in 53)
53	5.096198	192.168.1.254	192.168.1.92	ICMP	74	Echo (ping) reply id=0x0001, seq=27/6912, ttl=64 (request in 52)
79	9.722274	6a:5a:00:ec:c4:37	LiteonTechno_f1:07:13	ARP	52	Who has 192.168.1.135? Tell 192.168.1.254
80	9.722274	6a:5a:00:ec:c4:37	LiteonTechno_f1:07:13	ARP	52	Who has 192.168.1.77? Tell 192.168.1.254
81	9.722274	6a:5a:00:ec:c4:37	LiteonTechno_f1:07:13	ARP	52	Who has 192.168.1.92? Tell 192.168.1.254
82	9.722312	LiteonTechno_f1:07:13	VantivaUSA_ec:c4:3c	ARP	42	192.168.1.92 is at 24:b2:b9:f1:07:13

Frame 79: 52 bytes on wire (416 bits), 52 bytes captured (416 bits) on interface \Device\NPF_{0E4E2D6F-8D02-4ABA-8184-DCAC8E12FBF5}, 1	
Ethernet II, Src: 6a:5a:00:ec:c4:37 (6a:5a:00:ec:c4:37), Dst: LiteonTechno_f1:07:13 (24:b2:b9:f1:07:13)	
Address Resolution Protocol (request)	
Hardware type: Ethernet (1)	
Protocol type: IPv4 (0x0800)	
Hardware size: 6	
Protocol size: 4	
Opcode: request (1)	
Sender MAC address: VantivaUSA_ec:c4:3c (d0:5a:00:ec:c4:3c)	
Sender IP address: 192.168.1.254	
Target MAC address: 00:00:00:00:00:00 (00:00:00:00:00:00)	
Target IP address: 192.168.1.135	

## Capture 4

### ---Quelle signification ont les octets de position 0x0C et 0x0D ligne 0000 ?

Ce sont les octets 12 et 13 de la trame Ethernet. Ils correspondent au champ EtherType , et indique que le protocole encapsulé est ARP ( 0806) .

### ---Quelle est la fonction de la trame ARP REQUEST ?

Elle permet à une machine de demander l'adresse MAC associée à une adresse IP cible.

### ---Quelle signification ont les octets de position 0x04 et 0x05 ligne 0010 ?

Ce sont les octets 4 et 5 du message ARP. Ils correspondent au champ « Operation » du protocole ARP. ARP Request (0x0001), ARP Reply (0x0002).

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

Un message ARP fait 28 octets.

### --- Quelle est la longueur de la trame ARP Request ?

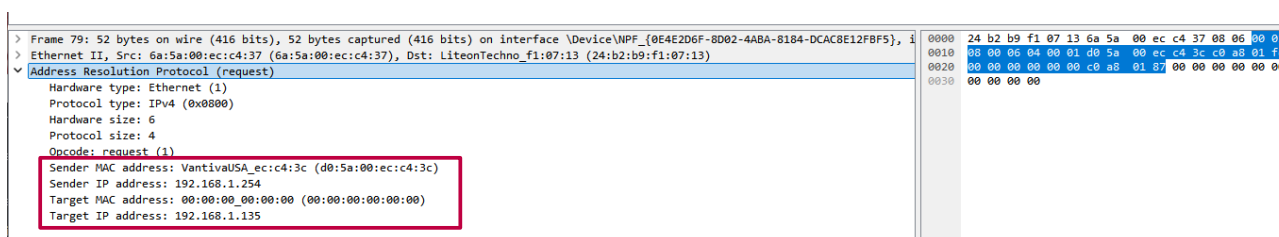
La longueur de la trame ARP Request est de **42 octets** ( 14 octets Ethernet + 28 octets (ARP)).

### --- Quelle est la longueur de la trame ARP Reply ?

La trame ARP Reply fait **42 octets**. Elle a la même structure mais le champ opération change (**0x0002**).

### ---Combien d'octets sont utilisés pour le padding ?

Le padding est ajouté pour atteindre la taille minimal Ethernet qui est de 64..Si la trame est de 42 octets alors le padding est de **22 octets**



### Trame ARP Request

**Adresse MAC destination : 24:b2:b9:f1:07:13**

**Adresse MAC source : 6a:5a:00:ec:c4:37**

**Ethernet Type : 0806**

**Opcode(valeur hexa.) : 0001 (request)**

**Adresse MAC de la cible : 00 :00:00:00:00:00**

**Adresse IP de la cible : 192.168.1.135**

En sélectionnant une trame **ICMP Echo Request** ( Capture 4 ) on peut répondre aux questions suivantes :

No.	Time	Source	Destination	Protocol	Length	Info
11	2.048841	192.168.1.92	192.168.1.254	ICMP	74	Echo (ping) request id=0x0001, seq=24/6144, ttl=128 (r...
12	2.068710	192.168.1.254	192.168.1.92	ICMP	74	Echo (ping) reply id=0x0001, seq=24/6144, ttl=64 (re...
14	3.064107	192.168.1.92	192.168.1.254	ICMP	74	Echo (ping) request id=0x0001, seq=25/6400, ttl=128 (r...
15	3.074697	192.168.1.254	192.168.1.92	ICMP	74	Echo (ping) reply id=0x0001, seq=25/6400, ttl=64 (re...
18	4.076950	192.168.1.92	192.168.1.254	ICMP	74	Echo (ping) request id=0x0001, seq=26/6656, ttl=128 (r...
19	4.084141	192.168.1.254	192.168.1.92	ICMP	74	Echo (ping) reply id=0x0001, seq=26/6656, ttl=64 (re...
52	5.090711	192.168.1.92	192.168.1.254	ICMP	74	Echo (ping) request id=0x0001, seq=27/6912, ttl=128 (r...
53	5.096198	192.168.1.254	192.168.1.92	ICMP	74	Echo (ping) reply id=0x0001, seq=27/6912, ttl=64 (re...
79	9.722274	6a:5a:00:ec:c4:37	LiteonTechno_f1:07:...	ARP	52	Who has 192.168.1.135? Tell 192.168.1.254
80	9.722274	6a:5a:00:ec:c4:37	LiteonTechno_f1:07:...	ARP	52	Who has 192.168.1.77? Tell 192.168.1.254
81	9.722274	6a:5a:00:ec:c4:37	LiteonTechno_f1:07:...	ARP	52	Who has 192.168.1.92? Tell 192.168.1.254
82	9.722312	LiteonTechno_f1:07:...	VantivaUSA_ec:c4:3c	ARP	42	192.168.1.92 is at 24:b2:b9:f1:07:13

> Frame 11: 74 bytes on wire (592 bits), 74 bytes captured (5...)	0000	d0 5a 00 ec c4 3c 24 b2 b9 f1 07 13 08 00 45 00	.Z...<\$.....E
> Ethernet II, Src: LiteonTechno_f1:07:13 (24:b2:b9:f1:07:13)	0010	00 3c 30 14 00 00 80 01 86 02 c0 a8 01 5c c0 a8	.<0.....\.
> Internet Protocol Version 4, Src: 192.168.1.92, Dst: 192.168.1.254	0020	01 fe 08 00 4d 43 00 01 00 18 61 62 63 64 65 66	...MC...abcde
> Internet Control Message Protocol	0030	67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76	ghijklmn opqrstu
	0040	77 61 62 63 64 65 66 67 68 69	wabdefg hi

Capture 4 ( ICMP Request )

**---Quelles signification ont les octets de position 0x0C et 0x0D ligne 0000 ?**

Ce sont les octets 12 et 13 de l'en-tête Ethernet. Il contient le champ Ethertype **0x0800** ce qui signifie que le protocole encapsulé est **IPv4**.

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

Cet octet fait partie du champ Opcode . Sa valeur est **0001** ce qui signifie que le protocole encapsulé est ICMP.

**---Quelle est la longueur de la trame ?**

La trame fait **74 octets** au total.

> Frame 11: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on	0000	d0 5a 00 ec c4 3c 24 b2 b9 f1 07 13 08 00 45 00
> Ethernet II, Src: LiteonTechno_f1:07:13 (24:b2:b9:f1:07:13), Dst: Vanti	0010	00 3c 30 14 00 00 80 01 86 02 c0 a8 01 5c c0 a8
> Internet Protocol Version 4, Src: 192.168.1.92, Dst: 192.168.1.254	0020	01 fe 08 00 4d 43 00 01 00 18 61 62 63 64 65 66
0100 .... = Version: 4	0030	67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76
.... 0101 = Header Length: 20 bytes (5)	0040	77 61 62 63 64 65 66 67 68 69
> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)		
Total Length: 60		
Identification: 0x3014 (12308)		
> 000. .... = Flags: 0x0		
...0 0000 0000 0000 = Fragment Offset: 0		
Time to Live: 128		
Protocol: ICMP (1)		
Header Checksum: 0x8602 [validation disabled]		
[Header checksum status: Unverified]		
Source Address: 192.168.1.92		
Destination Address: 192.168.1.254		
[Stream index: 4]		
> Internet Control Message Protocol		

### ---Quelle est la longueur du paquet IP ?

La taille totale du paquet IP est de **70 octets**.

### ---Quelle est la longueur du message ICMP ?

L'en-tête IP fait **20 octets** donc  $70-20=50$  octets pour le message ICMP.

Le message ICMP fait **50 octets**.

> Frame 11: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on	0000	d0 5a 00 ec c4 3c 24 b2 b9 f1 07 13 08 00 45 00
> Ethernet II, Src: LiteonTechno_f1:07:13 (24:b2:b9:f1:07:13), Dst: Vanti	0010	00 3c 30 14 00 00 80 01 86 02 c0 a8 01 5c c0 a8
> Internet Protocol Version 4, Src: 192.168.1.92, Dst: 192.168.1.254	0020	01 fe 08 00 4d 43 00 01 00 18 61 62 63 64 65 66
> Internet Control Message Protocol	0030	67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76
Type: 8 (Echo (ping) request)	0040	77 61 62 63 64 65 66 67 68 69
Code: 0		
Checksum: 0x4d43 [correct]		
[Checksum Status: Good]		
Identifier (BE): 1 (0x0001)		
Identifier (LE): 256 (0x0100)		
Sequence Number (BE): 24 (0x0018)		
Sequence Number (LE): 6144 (0x1800)		
[Response frame: 12]		
> Data (32 bytes)		

### ---Quelle signification a l'octet de position 0x02 ligne 00020 ?

C'est le 3ième octet du message ICMP .

Il correspond au champ « code ». Le 0x00 signifie echo request ou echo reply. Le type nous affirme que c'est une echo request.

### ---A quoi correspondent les octets a partir de l'octet 0x0A, ligne 00020?

Ils correspondent aux données ICMP.

On sélectionne une trame **ICMP Echo Reply**.

---Quelle est le nom et la valeur de l'octet de position 0x02 ligne 00020 ?

C'est le champ code de valeur 0x00.

## 2. Capture de trames ARP , DNS et ICMP

On démarre une capture sur Wireshark et on vide le cache ARP sur l'invite de commande grace a la commande arp -d\* (Capture 5).

```
C:\Windows\System32>arp -d *

C:\Windows\System32>arp -a

Interface : 192.168.1.92 --- 0x4
  Adresse Internet    Adresse physique    Type
  192.168.1.4         d0-05-2a-b2-d5-4b   dynamique
  192.168.1.143       14-c1-4e-01-fd-36   dynamique
  192.168.1.254       d0-5a-00-ec-c4-3c   dynamique
  224.0.0.2           01-00-5e-00-00-02   statique
  224.0.0.22          01-00-5e-00-00-16   statique

Interface : 192.168.56.1 --- 0x12
  Adresse Internet    Adresse physique    Type
  224.0.0.22          01-00-5e-00-00-16   statique

C:\Windows\System32>
```

Capture 5

On effectue un ping vers le serveur web [www.ac-nice.fr](http://www.ac-nice.fr) ( Capture 6 ).

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

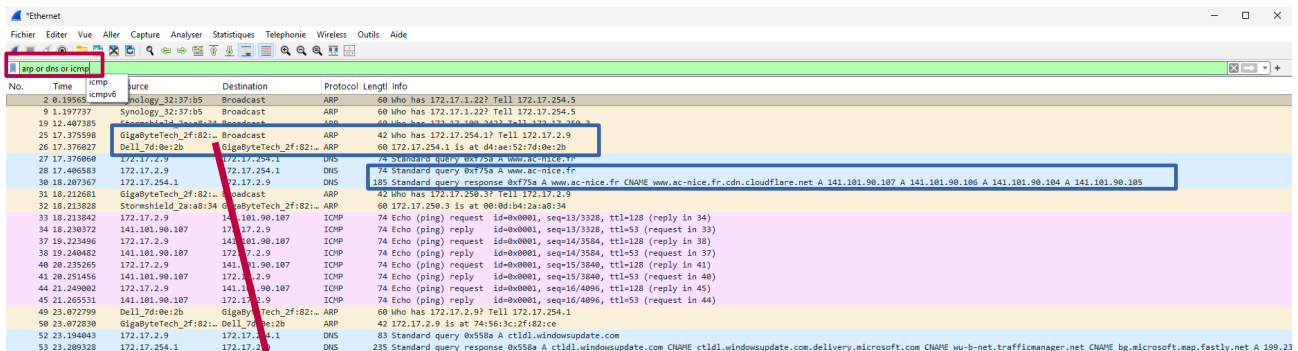
Envoi d'une requête 'ping' sur www.ac-nice.fr.cdn.cloudflare.net [141.101.90.107] avec 32 octets de données :
Réponse de 141.101.90.107 : octets=32 temps=17 ms TTL=53
Réponse de 141.101.90.107 : octets=32 temps=17 ms TTL=53
Réponse de 141.101.90.107 : octets=32 temps=16 ms TTL=53
Réponse de 141.101.90.107 : octets=32 temps=16 ms TTL=53

Statistiques Ping pour 141.101.90.107:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
    Durée approximative des boucles en millisecondes :
        Minimum = 16ms, Maximum = 17ms, Moyenne = 16ms
```

Capture 6



On filtre la capture faite sur Wireshark en inscrivant **ARP or DNS or ICMP** dans *filter* ( Capture 7 ).



Capture 7

**---Quelle est l'adresse MAC recherchée ?**

La machine dont l'adresse MAC est recherché est la machine dont l'adresse IP est 172.17.5.254.

Trame ARP request	
@MAC destination : ff:ff:ff:ff:ff:ff	
@MAC source : 2f:82: (je n'ai pas la suite car je n'ai pas développé l'en-tête)	
Ethernet Type :0x0806	
Opcode (valeur hexa.) :0x0001	
@MAC de la cible : d4:ae:52:7d:0e:2b	
@IP de la cible :172.17.254.1	

**---Pour quel raison trouve t-on ensuite une requête DNS avant l'échange de trames ICMP suite à l'exécution de la commande ping proprement dite ?**

Parce que la commande ping [www.ac-nice.fr](http://www.ac-nice.fr) utilise un nom de domaine et pas une adresse IP.

Avant d'envoyer les trames ICMP, le système doit résoudre le nom en adresse IP via une requête DNS.

On consulte le cache DNS a l'aide de la commande `ipconfig /displaydns` dans l'invite de commande afin de vérifiez la présence de l'enregistrement DNS `ac-nice.fr` et de l'adresse IP associée.

```

C:\Windows\System32>ipconfig /displaydns
Configuration IP de Windows

    fe3cr.delivery.mp.microsoft.com
    -----
    Nom d'enregistrement. : fe3cr.delivery.mp.microsoft.com
    Type d'enregistrement : 5
    Durée de vie . . . . : 1367038
    Longueur de données . : 8
    Section . . . . . : Réponse
    Enregistrement CNAME : fe3.delivery.mp.microsoft.com

    Nom d'enregistrement. : fe3.delivery.mp.microsoft.com
    Type d'enregistrement : 5
    Durée de vie . . . . : 1367038
    Longueur de données . : 8
    Section . . . . . : Réponse
    Enregistrement CNAME : glb.cws.prod.dcat.dsp.trafficmanager.net

    Nom d'enregistrement. : glb.cws.prod.dcat.dsp.trafficmanager.net
    Type d'enregistrement : 1
    Durée de vie . . . . : 1367038
    Longueur de données . : 4
    Section . . . . . : Réponse
    Enregistrement (hôte) : 13.85.23.206

    www.ac-nice.fr
    -----
    Nom d'enregistrement. : www.ac-nice.fr
    Type d'enregistrement : 5
    Durée de vie . . . . : 1372547
    Longueur de données . : 8
    Section . . . . . : Réponse
    Enregistrement CNAME : www.ac-nice.fr.cdn.cloudflare.net

    Nom d'enregistrement. : www.ac-nice.fr.cdn.cloudflare.net
    Type d'enregistrement : 1
    Durée de vie . . . . : 1372547
    Longueur de données . : 4
    Section . . . . . : Réponse
    Enregistrement (hôte) : 141.101.90.106

```

On fait une nouvelle capture sur Wireshark et on exécute a nouveau un ping [www.ac-nice.fr](http://www.ac-nice.fr) dans l'invite de commande.

```

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

Envoi d'une requête 'ping' sur www.ac-nice.fr.cdn.cloudflare.net [141.101.90.107] avec 32 octets de données :
Réponse de 141.101.90.107 : octets=32 temps=10 ms TTL=53
Réponse de 141.101.90.107 : octets=32 temps=15 ms TTL=53
Réponse de 141.101.90.107 : octets=32 temps=14 ms TTL=53
Réponse de 141.101.90.107 : octets=32 temps=12 ms TTL=53

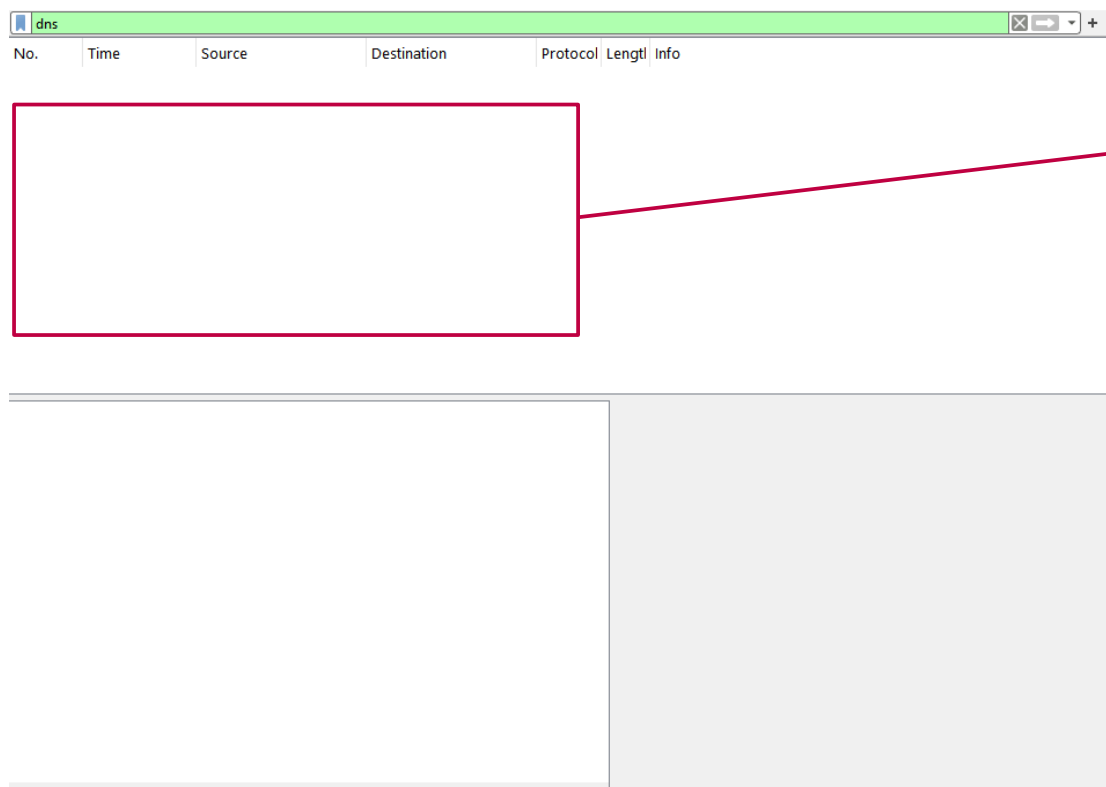
Statistiques Ping pour 141.101.90.107:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 10ms, Maximum = 15ms, Moyenne = 12ms

C:\Windows\System32>

```

→ Il n'y a pas de requête DNS ( Capture 9 ) car l'enregistrement est dans le cache DNS.

Fichier Editer Vue Aller Capture Analyser Statistiques Telephonie Wireless Outils Aide						
Appliquer un filtre d'affichage ... <Ctrl-/>						
No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.1.92	192.168.1.143	TCP	164	50363 → 8009 [PSH, ACK] Seq=1 Ack=1 Win=254 Len=...
2	0.029207	192.168.1.143	192.168.1.92	TCP	164	8009 → 50363 [PSH, ACK] Seq=1 Ack=111 Win=639 Le...
3	0.077402	192.168.1.92	192.168.1.143	TCP	54	50363 → 8009 [ACK] Seq=111 Ack=111 Win=254 Len=0
4	0.077706	95.101.110.32	192.168.1.92	TLSv1.2	86	Application Data
5	0.078301	192.168.1.92	95.101.110.32	TLSv1.2	90	Application Data
6	0.098997	95.101.110.32	192.168.1.92	TCP	54	443 → 58179 [ACK] Seq=33 Ack=37 Win=602 Len=0
7	2.106099	192.168.1.92	141.101.90.106	ICMP	74	Echo (ping) request id=0x0001, seq=32/8192, ttl...
8	2.137863	141.101.90.106	192.168.1.92	ICMP	74	Echo (ping) reply id=0x0001, seq=32/8192, ttl...
9	2.669173	192.168.1.157	192.168.1.255	UDP	77	37975 → 15600 Len=35
10	3.138178	192.168.1.92	141.101.90.106	ICMP	74	Echo (ping) request id=0x0001, seq=33/8448, ttl...
11	3.150287	141.101.90.106	192.168.1.92	ICMP	74	Echo (ping) reply id=0x0001, seq=33/8448, ttl...
12	3.191880	141.101.90.104	192.168.1.92	TCP	54	443 → 55762 [ACK] Seq=1 Ack=1 Win=15 Len=0
13	3.191938	192.168.1.92	141.101.90.104	TCP	54	[TCP ACKed unseen segment] 55762 → 443 [ACK] Seq=...
14	3.527398	192.168.1.92	192.168.1.4	TCP	164	58754 → 8009 [PSH, ACK] Seq=1 Ack=1 Win=251 Len=...
15	3.532523	192.168.1.4	192.168.1.92	TCP	164	8009 → 58754 [PSH, ACK] Seq=1 Ack=111 Win=388 Le...
16	3.574207	192.168.1.92	192.168.1.4	TCP	54	58754 → 8009 [ACK] Seq=111 Ack=111 Win=251 Len=0
17	4.155091	192.168.1.92	141.101.90.106	ICMP	74	Echo (ping) request id=0x0001, seq=34/8704, ttl...
> Frame 1: 164 bytes on wire (1312 bits), 164 bytes captured (1312 bits) > Ethernet II, Src: LiteonTechno_f1:07:13 (24:b2:b9:f1:07:13), Dst: Googl > Internet Protocol Version 4, Src: 192.168.1.92, Dst: 192.168.1.143 > Transmission Control Protocol, Src Port: 50363, Dst Port: 8009, Seq: 1,						
		0000 14 c1 4e 01 fd 36 24 b2 b9 f1 07 13 08 00 45 00 0010 00 96 38 c3 40 00 80 06 3d 63 c0 a8 01 5c c0 a8 0020 01 8f c4 bb 1f 49 fa 0c b9 f5 53 38 1a 4b 50 18 0030 00 fe b9 ac 00 00 17 03 03 00 69 30 f9 ef 5f e3 0040 2a 6e d4 e5 e1 b2 40 8c 6e 0b 4a 9f 22 ec 3d ae 0050 9b 5f c6 4b 69 29 92 d3 d4 a3 3a 36 15 5a 6b ec 0060 f1 ab 50 a6 bb e8 44 b1 ea 49 4e 80 5c 02 a8 92 0070 23 c5 87 71 94 02 4b a5 7a 30 8a e1 cf c3 c0 b5 0080 79 5a 3d e9 20 9a 4d d7 90 81 46 ee 35 f8 42 b5 0090 ef a0 78 91 c8 02 ce be 2e 5b a9 89 b1 85 59 91 00a0 c1 26 ab a6				



On vide le cache DNS à l'aide de la commande `ipconfig /flushdns` (capture 10), et on lance une nouvelle capture pour une requête DNS ( Capture 11 ).

```
C:\Windows\System32>ipconfig /flushdns
Configuration IP de Windows
Cache de résolution DNS vidé.
C:\Windows\System32>
```

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.1.92	192.168.1.143	TCP	164	50363 → 8009 [PSH, ACK] Seq=1 Ack=1 Win=253 Len=110
2	0.042596	192.168.1.143	192.168.1.92	TCP	164	8009 → 50363 [PSH, ACK] Seq=1 Ack=111 Win=639 Len=110
3	0.092410	192.168.1.92	192.168.1.143	TCP	54	50363 → 8009 [ACK] Seq=111 Ack=111 Win=252 Len=0
4	0.544514	192.168.1.92	141.101.90.107	QUIC	1292	Initial, DCID=1e818946f00e0d52, PKN: 9, CC, PADDING
5	1.060716	192.168.1.157	192.168.1.255	UDP	77	41777 → 15600 Len=35
6	1.942394	192.168.1.92	192.168.1.254	TCP	66	62805 → 53 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PE...
7	1.945307	192.168.1.92	141.101.90.107	TLSv1.2	307	Application Data
8	1.977592	192.168.1.254	192.168.1.92	TCP	66	53 → 62805 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1400 SAC...
9	1.977701	192.168.1.92	192.168.1.254	TCP	54	62805 → 53 [ACK] Seq=1 Ack=1 Win=65280 Len=0
10	1.978271	192.168.1.92	192.168.1.254	TCP	56	62805 → 53 [PSH, ACK] Seq=1 Ack=1 Win=65280 Len=2 [TCP PDU rea...
11	1.978311	192.168.1.92	192.168.1.254	DNS	86	Standard query 0x3450 A www.ac-nice.fr
12	1.982642	192.168.1.254	192.168.1.92	TCP	54	53 → 62805 [ACK] Seq=1 Ack=3 Win=64256 Len=0
13	1.982642	192.168.1.254	192.168.1.92	TCP	54	53 → 62805 [ACK] Seq=1 Ack=35 Win=64256 Len=0
14	2.001438	192.168.1.254	192.168.1.92	DNS	199	Standard query response 0x3450 A www.ac-nice.fr CNAME www.ac-n...
15	2.002560	192.168.1.92	192.168.1.254	TCP	54	62805 → 53 [FIN, ACK] Seq=35 Ack=146 Win=65280 Len=0
16	2.007712	192.168.1.254	192.168.1.92	TCP	54	53 → 62805 [FIN, ACK] Seq=146 Ack=36 Win=64256 Len=0
17	2.007752	192.168.1.92	192.168.1.254	TCP	54	62805 → 53 [ACK] Seq=36 Ack=147 Win=65280 Len=0
18	2.015776	141.101.90.107	192.168.1.92	TLSv1.2	454	Application Data
19	2.035010	192.168.1.92	141.101.90.107	TLSv1.2	218	Application Data
20	2.036334	192.168.1.92	141.101.90.107	TLSv1.2	193	Application Data
21	2.037274	192.168.1.92	141.101.90.107	TLSv1.2	175	Application Data
22	2.038092	192.168.1.92	141.101.90.107	TLSv1.2	170	Application Data
23	2.038886	192.168.1.92	141.101.90.107	TLSv1.2	198	Application Data
24	2.039838	192.168.1.92	141.101.90.107	TLSv1.2	185	Application Data
25	2.040811	192.168.1.92	141.101.90.107	TLSv1.2	177	Application Data
26	2.041628	192.168.1.92	141.101.90.107	TLSv1.2	181	Application Data

No.	Time	Source	Destination	Protocol	Length	Info
11	1.978311	192.168.1.92	192.168.1.254	DNS	86	Standard query 0x3450 A www.ac-nice.fr
14	2.001438	192.168.1.254	192.168.1.92	DNS	199	Standard query response 0x3450 A www.ac-nice.fr CNAME www.ac-nice.fr.cdn.cl...
289	2.467137	192.168.1.92	192.168.1.254	DNS	90	Standard query 0xb0ba HTTPS edge.microsoft.com
291	2.467246	192.168.1.92	192.168.1.254	DNS	90	Standard query 0xca7c A edge.microsoft.com
296	2.486890	192.168.1.254	192.168.1.92	DNS	192	Standard query response 0xca7c A edge.microsoft.com CNAME edge-microsoft-co...
297	2.486890	192.168.1.254	192.168.1.92	DNS	206	Standard query response 0xb0ba HTTPS edge.microsoft.com CNAME edge-microsof...

```

> Frame 11: 86 bytes on wire (688 bits), 86 bytes captured (688 bits) on interface \Device\NPF...
> Ethernet II, Src: LiteonTechno f1:07:13 (24:b2:b9:f1:07:13), Dst: VantivaUSA_ec:c4:3c (d0:5a:f4:c4:3c)
> Internet Protocol Version 4, Src: 192.168.1.92, Dst: 192.168.1.254
> Transmission Control Protocol, Src Port: 62805, Dst Port: 53, Seq: 3, Ack: 1, Len: 32
> [2 Reassembled TCP Segments (34 bytes): #10(2), #11(32)]
> Domain Name System (query)

```

### ---Quels sont les différents protocoles encapsulés dans une trame DNS ?

Ethernet encapsule IPv4, qui encapsule TCP, lui-même encapsulant le message DNS au niveau applicatif.

### ---Quelle est la machine destinataire de la requête DNS ? Quelle est son IP (en-tête IP)

La machine destinataire est le serveur DNS.

Son adresse IP est : 192.168.1.254

### ---Quelle signification ont les octets de position 0x0C et 0x0D ligne 0000 et 0x07 ligne 0010 ?

0x0C et 0x0D ligne 0000 → champ Ethertype dans Ethernet. Sa valeur **0x0800** → protocole encapsulé = IPv4

0x07 ligne 0010 → champ protocole dans l'en-tête IP. Sa valeur 0x06 → protocole de transport = TCP

### ---Quelle signification ont les octets de position 0x04 et 0x05 ligne 0020 ?

Ce sont les octets 4 et 5 de l'en-tête TCP . Ils correspondent au champ « Source Port ». Sa valeur : signifie que la requête est faite par le client (**62805**)

On développe la section Domain Name System (query) et plus précisément Queries ( Capture 12 ).

The image shows a Wireshark packet capture. The packet list on the left shows a series of packets. Packet 11 is a DNS query from 192.168.1.92 to 192.168.1.254. Packet 12 is a DNS response from 192.168.1.254 to 192.168.1.92. The packet details for packet 11 show the domain 'www.ac-nice.fr' and the transaction ID '0x3450'. The packet bytes on the right show the raw data of the query and response.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.1.92	192.168.1.143	TCP	164	50363 → 8009 [PSH, ACK] Seq=1 Ack=1 Win=253 Len=110
2	0.042596	192.168.1.143	192.168.1.92	TCP	164	8009 → 50363 [PSH, ACK] Seq=1 Ack=111 Win=639 Len=110
3	0.092410	192.168.1.92	192.168.1.143	TCP	54	50363 → 8009 [ACK] Seq=111 Ack=111 Win=252 Len=0
6	1.942394	192.168.1.92	192.168.1.254	TCP	66	62805 → 53 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
7	1.945307	192.168.1.92	141.101.90.107	TLSv1.2	307	Application Data
8	1.977592	192.168.1.254	192.168.1.92	TCP	66	53 → 62805 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1400 SACK_PERM
9	1.977701	192.168.1.92	192.168.1.254	TCP	54	62805 → 53 [ACK] Seq=1 Ack=1 Win=65280 Len=0
10	1.978271	192.168.1.92	192.168.1.254	TCP	56	62805 → 53 [PSH, ACK] Seq=1 Ack=1 Win=65280 Len=2 [TCP PDU reassemb...]
11	1.978311	192.168.1.92	192.168.1.254	DNS	86	Standard query 0x3450 A www.ac-nice.fr
12	1.982642	192.168.1.254	192.168.1.92	TCP	54	53 → 62805 [ACK] Seq=1 Ack=3 Win=64256 Len=0
13	1.982642	192.168.1.254	192.168.1.92	TCP	54	53 → 62805 [ACK] Seq=1 Ack=35 Win=64256 Len=0
14	2.001438	192.168.1.254	192.168.1.92	DNS	199	Standard query response 0x3450 A www.ac-nice.fr CNAME www.ac-nice.f...
15	2.002560	192.168.1.92	192.168.1.254	TCP	54	62805 → 53 [FIN, ACK] Seq=35 Ack=146 Win=65280 Len=0
16	2.007712	192.168.1.254	192.168.1.92	TCP	54	53 → 62805 [FIN, ACK] Seq=146 Ack=36 Win=64256 Len=0
17	2.007752	192.168.1.92	192.168.1.254	TCP	54	62805 → 53 [ACK] Seq=36 Ack=147 Win=65280 Len=0
18	2.015776	141.101.90.107	192.168.1.92	TLSv1.2	454	Application Data
19	2.035010	192.168.1.92	141.101.90.107	TLSv1.2	218	Application Data

Frame 11: 86 bytes on wire (688 bits), 86 bytes captured (688 bits) on interface \Device\NPF...  
> Ethernet II, Src: LiteonTechno\_f1:07:13 (24:b2:b9:f1:07:13), Dst: VantivaUSA\_ec:c4:3c (d0:5a:4c:00:00:00)  
> Internet Protocol Version 4, Src: 192.168.1.92, Dst: 192.168.1.254  
> Transmission Control Protocol, Src Port: 62805, Dst Port: 53, Seq: 3, Ack: 1, Len: 32  
> [2 Reassembled TCP Segments (34 bytes): #10(2), #11(32)]

Domain Name System (query)  
Length: 32  
Transaction ID: 0x3450  
Flags: 0x0100 Standard query  
Questions: 1  
Answer RRs: 0  
Authority RRs: 0  
Additional RRs: 0  
Queries  
> www.ac-nice.fr: type A, class IN  
[Response In: 14]

0000 00 20 34 50 01 00 00 01 00 00 00 00 00 00 03 77  
0010 77 77 07 61 63 2d 6e 69 63 65 02 66 72 00 00 01  
0020 00 01

Capture 12

### ---Quels sont les valeurs hexadécimales des octets correspondant au nom du domaine internet ac-nice.fr ?

02 61 63 → « ac »

04 6E 69 63 65 → « nice »

02 66 72 -> »fr »

00 → fin du nom

On sélectionne la trame comportant la réponse à la requête DNS et on développe la section Domain Name System (response) et plus particulièrement la rubrique answers. (Capture 13)

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.1.92	192.168.1.143	TCP	164	50363 → 8009 [PSH, ACK] Seq=1 Ack=1 Win=253 Len=110
2	0.042596	192.168.1.143	192.168.1.92	TCP	164	8009 → 50363 [PSH, ACK] Seq=1 Ack=111 Win=639 Len=110
3	0.092410	192.168.1.92	192.168.1.143	TCP	54	50363 → 8009 [ACK] Seq=111 Ack=111 Win=252 Len=0
6	1.942394	192.168.1.92	192.168.1.254	TCP	66	62805 → 53 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
7	1.945307	192.168.1.92	141.101.90.107	TLSv1.2	307	Application Data
8	1.977592	192.168.1.254	192.168.1.92	TCP	66	53 → 62805 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1400 SACK_PER...
9	1.977701	192.168.1.92	192.168.1.254	TCP	54	62805 → 53 [ACK] Seq=1 Ack=1 Win=65280 Len=0
10	1.978271	192.168.1.92	192.168.1.254	TCP	56	62805 → 53 [PSH, ACK] Seq=1 Ack=1 Win=65280 Len=2 [TCP PDU reassemb...
11	1.978311	192.168.1.92	192.168.1.254	DNS	86	Standard query 0x3450 A www.ac-nice.fr
12	1.982642	192.168.1.254	192.168.1.92	TCP	54	53 → 62805 [ACK] Seq=1 Ack=3 Win=64256 Len=0
13	1.982642	192.168.1.254	192.168.1.92	TCP	54	53 → 62805 [ACK] Seq=1 Ack=35 Win=64256 Len=0
14	2.001438	192.168.1.254	192.168.1.92	DNS	199	Standard query response 0x3450 A www.ac-nice.fr CNAME www.ac-nice.f...
15	2.002560	192.168.1.92	192.168.1.254	TCP	54	62805 → 53 [FIN, ACK] Seq=35 Ack=146 Win=65280 Len=0
16	2.007712	192.168.1.254	192.168.1.92	TCP	54	53 → 62805 [FIN, ACK] Seq=146 Ack=36 Win=64256 Len=0
17	2.007752	192.168.1.92	192.168.1.254	TCP	54	62805 → 53 [ACK] Seq=36 Ack=147 Win=65280 Len=0
18	2.015776	141.101.90.107	192.168.1.92	TLSv1.2	454	Application Data
19	2.035010	192.168.1.92	141.101.90.107	TLSv1.2	218	Application Data

> Frame 11: 86 bytes on wire (688 bits), 86 bytes captured (688 bits) on interface \Device\NPF\_{...}

> Ethernet II, Src: LiteonTechno\_f1:07:13 (24:b2:b9:f1:07:13), Dst: VantivaUSA\_ec:c4:3c (d0:5a:00:00:00:00)

> Internet Protocol Version 4, Src: 192.168.1.92, Dst: 192.168.1.254

> Transmission Control Protocol, Src Port: 62805, Dst Port: 53, Seq: 3, Ack: 1, Len: 32

> [2 Reassembled TCP Segments (34 bytes): #10(2), #11(32)]

Domain Name System (query)

Length: 32

Transaction ID: 0x3450

Flags: 0x0100 Standard query

Questions: 1

Answer RRs: 0

Authority RRs: 0

Additional RRs: 0

Queries

[Response In: 14]

0000 00 20 34 50 01 00 00 01 00 00 00 00 00 00 03 77  
0010 77 77 07 61 63 2d 6e 69 63 65 02 66 72 00 00 01  
0020 00 01

--- Rechercher les valeurs hexadécimales et décimales de l'adresse IP du serveur web hébergeant le site de l'académie de Nice.

```
C:\Windows\System32>nslookup www.ac-nice.fr
Serveur :  bbox.lan
Address:  192.168.1.254

Réponse ne faisant pas autorité :
Nom :      www.ac-nice.fr.cdn.cloudflare.net
Addresses: 2a06:98c1:3200::90:83
            2a06:98c1:3200::90:82
            2a06:98c1:3200::90:80
            2a06:98c1:3200::90:81
            141.101.90.105
            141.101.90.106
            141.101.90.107
            141.101.90.104
Aliases:   www.ac-nice.fr

C:\Windows\System32>
```

Conversion hexadécimale de l'@ip : 141.101.90.104

141 → 8D

101 → 65

90 → 5A

104 → 68

### 3. Commande Tracert et capture de trames ICMP

(Partie faite avec un ordinateur du labo)

On exécute la **commande Tracert** dans l'invite de commande ce qui va nous permettre de connaître tout les routeurs entre la machine local et l'adresse de destination ( Capture 14 ).



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

Détermination de l'itinéraire vers www.ac-nice.fr.cdn.cloudflare.net [141.101.90.107]
avec un maximum de 30 sauts :

 1  1 ms    1 ms    1 ms    10.73.23.242
 2  1 ms    1 ms    1 ms    10.73.27.3
 3  5 ms    5 ms    5 ms    10.20.2.9
 4  5 ms    5 ms    5 ms    10.20.2.14
 5  5 ms    5 ms    5 ms    194.199.240.253
 6  6 ms    6 ms    5 ms    te0-0-0-2-ren-nr-marseille2-rtr-091.noc.renater.fr [193.51.190.154]
 7 18 ms   16 ms   16 ms    et-0-1-1-ren-nr-marseille2-rtr-131.noc.renater.fr [193.55.205.56]
 8 15 ms   16 ms   16 ms    hu0-2-0-0-ren-nr-lyon2-rtr-091.noc.renater.fr [193.51.177.255]
 9 15 ms   15 ms   15 ms    et-5-3-1-ren-nr-paris2-rtr-131.noc.renater.fr [193.51.177.238]
10 17 ms   16 ms   16 ms    equinix-paris.cloudflare.com [195.42.144.143]
11 17 ms   16 ms   16 ms    141.101.67.109
12 16 ms   16 ms   16 ms    141.101.90.107

Itinéraire déterminé.
```

## Capture 14

On démarre une capture de trames sur Wireshark et on saisis Tracert [www.ac-nice.fr](http://www.ac-nice.fr).

On limite l'affichage des trames a celles encapsulant le protocole ICMP ( Capture 15 ).

The image shows a Wireshark packet capture window. The packet list is filtered for ICMP. The packet details pane shows the structure of an ICMP Echo (ping) request.

No.	Time	Source	Destination	Protocol	Length	Info
22	8.264496	172.17.2.9	141.101.90.107	ICMP	106	Echo (ping) request id=0x0001, seq=57/14592, ttl=1 no response found
23	8.265926	10.73.23.242	172.17.2.9	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
24	8.266332	172.17.2.9	141.101.90.107	ICMP	106	Echo (ping) request id=0x0001, seq=58/14848, ttl=1 no response found
25	8.267885	10.73.23.242	172.17.2.9	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
26	8.268206	172.17.2.9	141.101.90.107	ICMP	106	Echo (ping) request id=0x0001, seq=59/15104, ttl=1 no response found
27	8.269855	10.73.23.242	172.17.2.9	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
35	9.281467	172.17.2.9	141.101.90.107	ICMP	106	Echo (ping) request id=0x0001, seq=60/15360, ttl=2 no response found
36	9.282471	10.73.27.3	172.17.2.9	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
37	9.282936	172.17.2.9	141.101.90.107	ICMP	106	Echo (ping) request id=0x0001, seq=61/15616, ttl=2 no response found
38	9.283912	10.73.27.3	172.17.2.9	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
39	9.284367	172.17.2.9	141.101.90.107	ICMP	106	Echo (ping) request id=0x0001, seq=62/15872, ttl=2 no response found
40	9.285415	10.73.27.3	172.17.2.9	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
51	10.296184	172.17.2.9	141.101.90.107	ICMP	106	Echo (ping) request id=0x0001, seq=63/16128, ttl=3 no response found
52	10.301554	10.20.2.9	172.17.2.9	ICMP	182	Time-to-live exceeded (Time to live exceeded in transit)
53	10.302319	172.17.2.9	141.101.90.107	ICMP	106	Echo (ping) request id=0x0001, seq=64/16384, ttl=3 no response found
54	10.307467	10.20.2.9	172.17.2.9	ICMP	182	Time-to-live exceeded (Time to live exceeded in transit)
55	10.308272	172.17.2.9	141.101.90.107	ICMP	106	Echo (ping) request id=0x0001, seq=65/16640, ttl=3 no response found
56	10.313495	10.20.2.9	172.17.2.9	ICMP	182	Time-to-live exceeded (Time to live exceeded in transit)
61	11.311671	172.17.2.9	141.101.90.107	ICMP	106	Echo (ping) request id=0x0001, seq=66/16896, ttl=4 no response found
62	11.316560	10.20.2.14	172.17.2.9	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
63	11.317215	172.17.2.9	141.101.90.107	ICMP	106	Echo (ping) request id=0x0001, seq=67/17152, ttl=4 no response found
64	11.322039	10.20.2.14	172.17.2.9	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
65	11.323063	172.17.2.9	141.101.90.107	ICMP	106	Echo (ping) request id=0x0001, seq=68/17408, ttl=4 no response found
66	11.328067	10.20.2.14	172.17.2.9	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
69	12.341117	172.17.2.9	141.101.90.107	ICMP	106	Echo (ping) request id=0x0001, seq=69/17664, ttl=5 no response found
70	12.346380	194.199.240.253	172.17.2.9	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
71	12.347168	172.17.2.9	141.101.90.107	ICMP	106	Echo (ping) request id=0x0001, seq=70/17920, ttl=5 no response found
72	12.352077	194.199.240.253	172.17.2.9	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
73	12.352585	172.17.2.9	141.101.90.107	ICMP	106	Echo (ping) request id=0x0001, seq=71/18176, ttl=5 no response found
74	12.357590	194.199.240.253	172.17.2.9	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
79	13.360700	172.17.2.9	141.101.90.107	ICMP	106	Echo (ping) request id=0x0001, seq=72/18432, ttl=6 no response found

Frame 22: 106 bytes on wire (848 bits), 106 bytes captured (848 bits) on interface  
 Ethernet II, Src: GigaByteTech\_2f:82:ce (74:56:3c:2f:82:ce), Dst: Stormshield\_00:00:00:00:00:00  
 Internet Protocol Version 4, Src: 172.17.2.9, Dst: 141.101.90.107  
 Internet Control Message Protocol

Capture 15

On sélectionne la première **trame ICMP request** et on développe l'**en-tête IP** (Capture 16 ).

capture.tracert.pcapng

Fichier Editer Vue Aller Capture Analyser Statistiques Telephonie Wireless Outils Aide

icmp

No.	Time	Source	Destination	Protocol	Length	Info
22	8.264496	172.17.2.9	141.101.90.107	ICMP	106	Echo (ping) request id=0x0001, seq=57/14592, ttl=1 (no response found)
23	8.265926	10.73.23.242	172.17.2.9	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
24	8.266332	172.17.2.9	141.101.90.107	ICMP	106	Echo (ping) request id=0x0001, seq=58/14848, ttl=1 (no response found)
25	8.267885	10.73.23.242	172.17.2.9	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
26	8.268286	172.17.2.9	141.101.90.107	ICMP	106	Echo (ping) request id=0x0001, seq=59/15104, ttl=1 (no response found)
27	8.269855	10.73.23.242	172.17.2.9	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
35	9.281467	172.17.2.9	141.101.90.107	ICMP	106	Echo (ping) request id=0x0001, seq=60/15360, ttl=2 (no response found)
36	9.282471	10.73.27.3	172.17.2.9	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
37	9.282936	172.17.2.9	141.101.90.107	ICMP	106	Echo (ping) request id=0x0001, seq=61/15616, ttl=2 (no response found)
38	9.283912	10.73.27.3	172.17.2.9	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
39	9.284367	172.17.2.9	141.101.90.107	ICMP	106	Echo (ping) request id=0x0001, seq=62/15872, ttl=2 (no response found)
40	9.285415	10.73.27.3	172.17.2.9	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
51	10.296184	172.17.2.9	141.101.90.107	ICMP	106	Echo (ping) request id=0x0001, seq=63/16128, ttl=3 (no response found)
52	10.301554	10.20.2.9	172.17.2.9	ICMP	182	Time-to-live exceeded (Time to live exceeded in transit)
53	10.302319	172.17.2.9	141.101.90.107	ICMP	106	Echo (ping) request id=0x0001, seq=64/16384, ttl=3 (no response found)
54	10.307467	10.20.2.9	172.17.2.9	ICMP	182	Time-to-live exceeded (Time to live exceeded in transit)
55	10.308272	172.17.2.9	141.101.90.107	ICMP	106	Echo (ping) request id=0x0001, seq=65/16640, ttl=3 (no response found)
56	10.313495	10.20.2.9	172.17.2.9	ICMP	182	Time-to-live exceeded (Time to live exceeded in transit)
61	11.311671	172.17.2.9	141.101.90.107	ICMP	106	Echo (ping) request id=0x0001, seq=66/16896, ttl=4 (no response found)
62	11.316560	10.20.2.14	172.17.2.9	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
63	11.317215	172.17.2.9	141.101.90.107	ICMP	106	Echo (ping) request id=0x0001, seq=67/17152, ttl=4 (no response found)
64	11.322039	10.20.2.14	172.17.2.9	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
65	11.323063	172.17.2.9	141.101.90.107	ICMP	106	Echo (ping) request id=0x0001, seq=68/17408, ttl=4 (no response found)
66	11.328067	10.20.2.14	172.17.2.9	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
69	12.341117	172.17.2.9	141.101.90.107	ICMP	106	Echo (ping) request id=0x0001, seq=69/17664, ttl=5 (no response found)
70	12.346380	194.199.240.253	172.17.2.9	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
71	12.347168	172.17.2.9	141.101.90.107	ICMP	106	Echo (ping) request id=0x0001, seq=70/17920, ttl=5 (no response found)
72	12.352077	194.199.240.253	172.17.2.9	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
73	12.352585	172.17.2.9	141.101.90.107	ICMP	106	Echo (ping) request id=0x0001, seq=71/18176, ttl=5 (no response found)
74	12.357590	194.199.240.253	172.17.2.9	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
79	13.369792	172.17.2.9	141.101.90.107	ICMP	106	Echo (ping) request id=0x0001, seq=72/18432, ttl=6 (no response found)

> Frame 22: 106 bytes on wire (848 bits), 106 bytes captured (848 bits) on interface 0  
 Ethernet II, Src: GigaByteTech\_2f:82:ce (74:56:3c:2f:82:ce), Dst: Stormshie  
 > Internet Protocol Version 4, Src: 172.17.2.9, Dst: 141.101.90.107  
 0100 .... = Version: 4  
 .... 0101 = Header Length: 20 bytes (5)  
 > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)  
 Total Length: 92  
 Identification: 0x362f (13871)  
 > 000. .... = Flags: 0x0  
 ...0 0000 0000 0000 = Fragment Offset: 0  
 > Time to Live: 1  
 Protocol: ICMP (1)  
 Header Checksum: 0x0000 [validation disabled]  
 [Header checksum status: Unverified]  
 Source Address: 172.17.2.9  
 Destination Address: 141.101.90.107  
 [Stream index: 4]  
 > Internet Control Message Protocol

0000 00 0d b4 2a a8 34 74 56 3c 2f 82 ce 08 00 45 00 ...\*.4tV </...E  
 0010 00 5c 36 2f 00 00 01 01 00 00 ac 11 02 09 8d 65 ...6/...9.....E  
 0020 5a 6b 08 00 f7 c5 00 01 00 39 00 00 00 00 00 00 ...Zk...9.....E  
 0030 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 .....  
 0050 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 .....  
 .....

Capture 16

--- Adresse IP Destination (valeur décimale) : 141.101.90.187  
 (valeur hexa.) :8D 65 5A BB

On sélectionne le champ **TTL** .( Capture 17 )

> Frame 22: 106 bytes on wire (848 bits), 106 bytes captured (848 bits) on interface	0000 00 0d b4 2a a8 34 74 56 3c 2f 82 ce 08 00 45 00 ...*4tV </....E
> Ethernet II, Src: GigaByteTech_2f:82:ce (74:56:3c:2f:82:ce), Dst: Stormshie	0010 00 5c 36 2f 00 00 01 01 00 00 ac 11 02 09 8d 65 ..\6/....e
> Internet Protocol Version 4, Src: 172.17.2.9, Dst: 141.101.90.107	0020 5a 6b 08 00 f7 c5 00 01 00 39 00 00 00 00 00 7k.....9.....
0100 .... = Version: 4	0030 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
.... 0101 = Header Length: 20 bytes (5)	0040 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)	0050 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
Total Length: 92	0060 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
Identification: 0x362f (13871)	
> 000. .... = Flags: 0x0	
...0 0000 0000 0000 = Fragment Offset: 0	
> Time to Live: 1	
Protocol: ICMP (1)	
Header Checksum: 0x0000 [validation disabled]	
[Header checksum status: Unverified]	
Source Address: 172.17.2.9	
Destination Address: 141.101.90.107	
[Stream index: 4]	
> Internet Control Message Protocol	

Capture 17

---Quelle est la valeur portée par ce champ ( val.déci.) : **1** (val.hexa) :**0x01**

On développe la section correspondant au message ICMP ( Capture 18 )

> Frame 35: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface	0000 00 11 32 32 37 b5 74 56 3c 2f 82 ce 08 00 45 00 ...227.tV </....E
> Ethernet II, Src: GigaByteTech_2f:82:ce (74:56:3c:2f:82:ce), Dst: Synology	0010 00 3c 3f 4e 00 00 80 01 00 00 ac 11 02 09 ac 11 ..<?N.....
> Internet Protocol Version 4, Src: 172.17.2.9, Dst: 172.17.254.5	0020 fe 05 08 00 4d 52 00 01 00 09 61 62 63 64 65 66 ..MR...abcdef
> Internet Control Message Protocol	0030 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76 ghijklmn opqrstuv
Type: 8 (Echo (ping) request)	0040 77 61 62 63 64 65 66 67 68 69 wabcdefg hi
Code: 0	
Checksum: 0x4d52 [correct]	
[Checksum Status: Good]	
Identifier (BE): 1 (0x0001)	
Identifier (LE): 256 (0x0100)	
Sequence Number (BE): 9 (0x0009)	
Sequence Number (LE): 2304 (0x0900)	
[Response frame: 36]	
> Data (32 bytes)	

Capture 18

---Quelle est la valeur portée par le champ Type ?

Valeur décimal : **8**

Valeur hexadécimal : **0x08**

On sélectionne la trame comportant un message d'erreur ICMP Time-to-live exceeded. On développe la section correspondant au message ICMP ( Capture 19 ).

The image shows the Wireshark packet capture details for frame 23. The left pane shows the packet list with frame 23 selected. The middle pane shows the packet details for frame 23, with the 'Time to Live: 1' field highlighted. The right pane shows the raw packet data in hexadecimal and ASCII.

```

> Frame 23: 134 bytes on wire (1072 bits), 134 bytes captured (1072 bits) on
> Ethernet II, Src: Stormshield_2a:a8:34 (00:0d:b4:2a:a8:34), Dst: GigaByteE
> Internet Protocol Version 4, Src: 10.73.23.242, Dst: 172.17.2.9
  > Internet Control Message Protocol
    Type: 11 (Time-to-live exceeded)
    Code: 0 (Time to live exceeded in transit)
    Checksum: 0x6271 [correct]
    [Checksum Status: Good]
    Unused: 00000000
  > Internet Protocol Version 4, Src: 172.17.2.9, Dst: 141.101.90.107
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 92
    Identification: 0x362f (13871)
    > 000. .... = Flags: 0x0
    ... 0 0000 0000 0000 = Fragment Offset: 0
    > Time to Live: 1
      Protocol: ICMP (1)
      Header Checksum: 0x8016 [validation disabled]
      [Header checksum status: Unverified]
      Source Address: 172.17.2.9
      Destination Address: 141.101.90.107
      [Stream index: 4]
    > Internet Control Message Protocol
  
```

Raw packet data (hex):

```

0000 74 56 3c 2f 82 ce 00 0d b4 2a a8 34 08 00 45 c0 tV</... *4..E.
0010 00 78 fb bb 00 00 40 01 ad b4 0a 49 17 f2 ac 11 .x...@...I...
0020 02 09 0b 00 62 71 00 00 00 00 45 00 00 5c 36 2f .bq...E...6/
0030 00 00 01 01 80 16 ac 11 02 09 8d 65 5a 6b 08 00 .....eZk..
0040 f7 c5 00 01 00 39 00 00 00 00 00 00 00 00 00 00 .....9.....
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 .....
0070 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
0080 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
  
```

Capture 19

The image shows the Wireshark packet capture packet list and details for ICMP Time-to-live exceeded messages. The packet list shows a series of ICMP Echo (ping) requests and responses. The details pane shows the structure of the ICMP message, including the Type, Code, Checksum, and Source/Destination addresses.

No.	Time	Source	Destination	Protocol	Length	Info
22	8.264496	172.17.2.9	141.101.90.107	ICMP	106	Echo (ping) request id=0x0001, seq=57/14592, ttl=1 (no response found)
23	8.265926	10.73.23.242	172.17.2.9	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
24	8.266332	172.17.2.9	141.101.90.107	ICMP	106	Echo (ping) request id=0x0001, seq=58/14848, ttl=1 (no response found)
25	8.267885	10.73.23.242	172.17.2.9	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
26	8.268206	172.17.2.9	141.101.90.107	ICMP	106	Echo (ping) request id=0x0001, seq=59/15104, ttl=1 (no response found)
27	8.269855	10.73.23.242	172.17.2.9	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
35	9.281467	172.17.2.9	141.101.90.107	ICMP	106	Echo (ping) request id=0x0001, seq=60/15360, ttl=2 (no response found)
36	9.282471	10.73.27.3	172.17.2.9	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
37	9.282936	172.17.2.9	141.101.90.107	ICMP	106	Echo (ping) request id=0x0001, seq=61/15616, ttl=2 (no response found)
38	9.283912	10.73.27.3	172.17.2.9	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
39	9.284367	172.17.2.9	141.101.90.107	ICMP	106	Echo (ping) request id=0x0001, seq=62/15872, ttl=2 (no response found)
40	9.285415	10.73.27.3	172.17.2.9	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
51	10.296184	172.17.2.9	141.101.90.107	ICMP	106	Echo (ping) request id=0x0001, seq=63/16128, ttl=3 (no response found)
52	10.301554	10.20.2.9	172.17.2.9	ICMP	182	Time-to-live exceeded (Time to live exceeded in transit)
53	10.302319	172.17.2.9	141.101.90.107	ICMP	106	Echo (ping) request id=0x0001, seq=64/16384, ttl=3 (no response found)
54	10.307467	10.20.2.9	172.17.2.9	ICMP	182	Time-to-live exceeded (Time to live exceeded in transit)
55	10.308272	172.17.2.9	141.101.90.107	ICMP	106	Echo (ping) request id=0x0001, seq=65/16640, ttl=3 (no response found)
56	10.313495	10.20.2.9	172.17.2.9	ICMP	182	Time-to-live exceeded (Time to live exceeded in transit)
61	11.311671	172.17.2.9	141.101.90.107	ICMP	106	Echo (ping) request id=0x0001, seq=66/16896, ttl=4 (no response found)
62	11.316560	10.20.2.14	172.17.2.9	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
63	11.317215	172.17.2.9	141.101.90.107	ICMP	106	Echo (ping) request id=0x0001, seq=67/17152, ttl=4 (no response found)
64	11.322039	10.20.2.14	172.17.2.9	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
65	11.323063	172.17.2.9	141.101.90.107	ICMP	106	Echo (ping) request id=0x0001, seq=68/17408, ttl=4 (no response found)
66	11.328067	10.20.2.14	172.17.2.9	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
69	12.341117	172.17.2.9	141.101.90.107	ICMP	106	Echo (ping) request id=0x0001, seq=69/17664, ttl=5 (no response found)
70	12.346380	194.199.240.253	172.17.2.9	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
71	12.347168	172.17.2.9	141.101.90.107	ICMP	106	Echo (ping) request id=0x0001, seq=70/17920, ttl=5 (no response found)
72	12.352077	194.199.240.253	172.17.2.9	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
73	12.352585	172.17.2.9	141.101.90.107	ICMP	106	Echo (ping) request id=0x0001, seq=71/18176, ttl=5 (no response found)
74	12.357590	194.199.240.253	172.17.2.9	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
79	13.369792	172.17.2.9	141.101.90.107	ICMP	106	Echo (ping) request id=0x0001, seq=72/18432, ttl=6 (no response found)

Details for frame 23:

```

> Frame 23: 134 bytes on wire (1072 bits), 134 bytes captured (1072 bits) on
> Ethernet II, Src: Stormshield_2a:a8:34 (00:0d:b4:2a:a8:34), Dst: GigaByteE
> Internet Protocol Version 4, Src: 10.73.23.242, Dst: 172.17.2.9
  > Internet Control Message Protocol
    Type: 11 (Time-to-live exceeded)
    Code: 0 (Time to live exceeded in transit)
    Checksum: 0x6271 [correct]
    [Checksum Status: Good]
    Unused: 00000000
  
```

Raw packet data (hex):

```

0000 74 56 3c 2f 82 ce 00 0d b4 2a a8 34 08 00 45 c0 tV</... *4..E.
0010 00 78 fb bb 00 00 40 01 ad b4 0a 49 17 f2 ac 11 .x...@...I...
0020 02 09 0b 00 62 71 00 00 00 00 45 00 00 5c 36 2f .bq...E...6/
0030 00 00 01 01 80 16 ac 11 02 09 8d 65 5a 6b 08 00 .....eZk..
0040 f7 c5 00 01 00 39 00 00 00 00 00 00 00 00 00 00 .....9.....
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 .....
0070 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
0080 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
  
```

Capture 19

**---Quelle est la valeur portée par le champ Type ?**

Valeur décimal : 11

Valeur Hexadécimal : 0x0B