

TP5 – Trames ARP, ICMP, DNS

SAOU Rayan

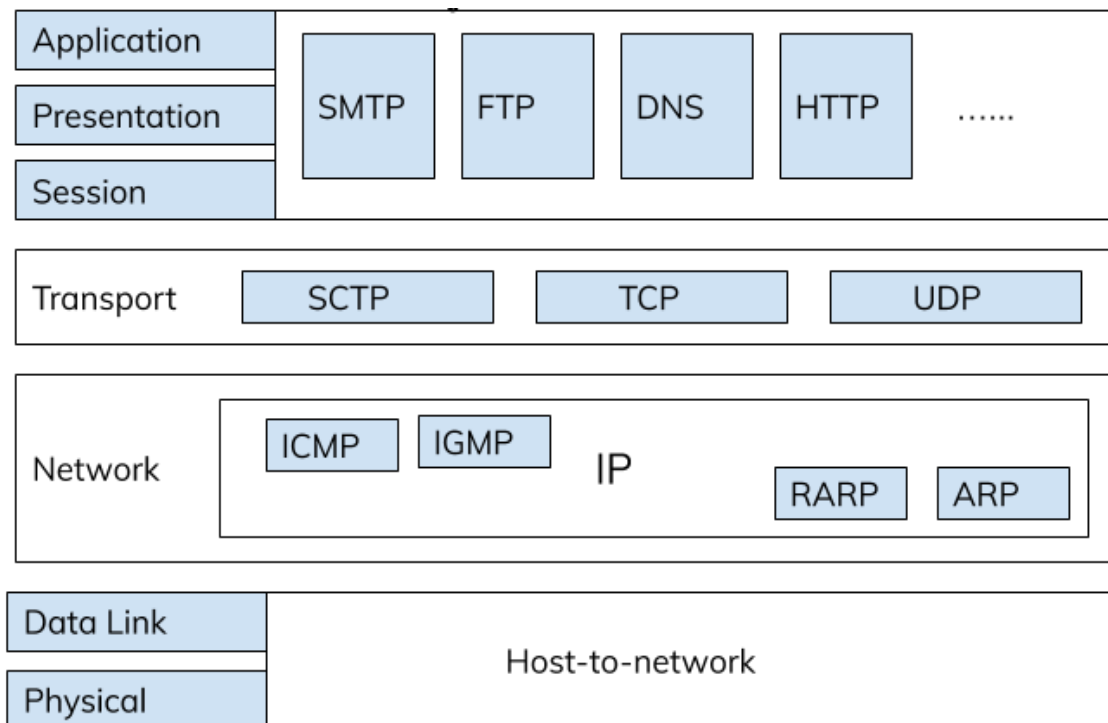


Table des matières

Table des matières	1
1. Capture de trames ARP et ICMP	1
2. Capture de trames ARP, DNS et ICMP	5
3. Commande Tracert et capture de trames ICMP	10

1. Capture de trames ARP et ICMP.

Nous ouvrons **Wireshark** et nous démarrons notre capture de trame. Ensuite nous démarrons notre invite de commande et nous faisons une commande **ping** à **172.17.254.5** (Aviateur)

```
C:\Users\Rayan>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=12 ms TTL=64
Réponse de 172.17.254.5 : octets=32 temps=9 ms TTL=64
Réponse de 172.17.254.5 : octets=32 temps=9 ms TTL=64
Réponse de 172.17.254.5 : octets=32 temps=12 ms 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 = 9ms, Maximum = 12ms, Moyenne = 10ms
```

Figure 1: Commande ping à Aviateur

Nous arrêtons ensuite notre capture de trame et nous voyons que la trame ARP est bien partie donc nous n'avons pas besoin d'effectuer la commande **arp -d *** pour vider le cache ARP.

No.	Time	Source	Destination	Protocol	Length	Info
38	8.502808	Synology_32:3...	LiteonTechno_...	ARP	60	Who has 172.17.5.72? Tell 172.17.254.5
39	8.502850	LiteonTechno_...	Synology_32:3...	ARP	42	172.17.5.72 is at c0:35:32:5b:e3:81

Figure 2 : Trames ARP capturées avec Wireshark

Et nous pouvons aussi vérifier avec la commande **arp -a** pour consulter le cache ARP et confirmer l'association IP-MAC.

```
Interface : 172.17.5.72 --- 0x10
Adresse Internet      Adresse physique      Type
172.17.2.1           74-56-3c-2f-9c-17    dynamique
172.17.2.3           74-56-3c-2f-81-87    dynamique
172.17.2.6           74-56-3c-2f-7f-f1    dynamique
172.17.2.8           74-56-3c-2f-9c-f7    dynamique
172.17.2.11          74-56-3c-2f-7b-a0    dynamique
172.17.2.12          74-56-3c-2f-9c-c6    dynamique
172.17.2.13          74-56-3c-2f-9d-13    dynamique
172.17.2.14          74-56-3c-2f-80-d8    dynamique
172.17.2.15          74-56-3c-2f-9c-fc    dynamique
172.17.2.17          74-56-3c-2f-9c-f6    dynamique
172.17.5.27          d0-57-7e-28-9b-41    dynamique
172.17.5.40          40-ae-30-c1-f4-bd    dynamique
172.17.5.65          10-7c-61-4c-33-1c    dynamique
172.17.250.3         00-0d-b4-2a-a8-34    dynamique
172.17.250.6         00-a5-bf-e9-d6-00    dynamique
172.17.250.7         00-a5-bf-e9-e8-00    dynamique
172.17.254.1         d4-ae-52-7d-0e-2b    dynamique
172.17.254.5         00-11-32-32-37-b5    dynamique
```

Figure 3 : Résultat de la commande arp -a

La signification des octets de position **0x0C** et **0x0D** ligne 0000 est le **champ Ether-type**, dans notre champ actuel 0806 signifie qu'il s'agit d'un message ARP.

La fonction de la trame **ARP Request** est de pouvoir demander aux autres machines localement (**broadcast**) pour savoir l'adresse MAC avec l'IP qui lui est associée.

La longueur d'un message **ARP** contenu dans la trame est de **28 octets**.

La longueur de la trame ARP Request est de **60 octets**.

```

▼ Frame 38: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface \Device\NPF_{D5BE8195-EC5E-4F01-B6CC-E8BDF2FA8F85}
  Section number: 1
  ▶ Interface id: 0 (\Device\NPF_{D5BE8195-EC5E-4F01-B6CC-E8BDF2FA8F85})
    Encapsulation type: Ethernet (1)
    Arrival Time: Oct 9, 2025 16:22:15.850266000 Paris, Madrid (heure d'été)
    UTC Arrival Time: Oct 9, 2025 14:22:15.850266000 UTC
    Epoch Arrival Time: 1760019735.850266000
    [Time shift for this packet: 0.000000000 seconds]
    [Time delta from previous captured frame: 0.105625000 seconds]
    [Time delta from previous displayed frame: 0.000000000 seconds]
    [Time since reference or first frame: 8.502808000 seconds]
    Frame Number: 38
    Frame Length: 60 bytes (480 bits)
  
```

Figure 4 : Informations sur la longueur de la trame ARP Request

Et pour la longueur de la trame ARP Reply il s'agit de **42 octets**.

```

39 8.502850 LiteonTechno... Synology_32:3... ARP 42 172.17.5.72 is at c0:35:32:5b:e3:
38 8.502808 Synology_32:3... LiteonTechno... ARP 60 Who has 172.17.5.72? Tell 172.17.

▼ Frame 39: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface \Device\NPF_{D5BE8195-EC5E-4F01-B6CC-E8BDF2FA8F85}
  Section number: 1
  ▶ Interface id: 0 (\Device\NPF_{D5BE8195-EC5E-4F01-B6CC-E8BDF2FA8F85})
    Encapsulation type: Ethernet (1)
    Arrival Time: Oct 9, 2025 16:22:15.850308000 Paris, Madrid (heure d'été)
    UTC Arrival Time: Oct 9, 2025 14:22:15.850308000 UTC
    Epoch Arrival Time: 1760019735.850308000
    [Time shift for this packet: 0.000000000 seconds]
    [Time delta from previous captured frame: 0.000042000 seconds]
    [Time delta from previous displayed frame: 0.000042000 seconds]
    [Time since reference or first frame: 8.502850000 seconds]
    Frame Number: 39
    Frame Length: 42 bytes (336 bits)
  
```

Figure 5 : Informations sur la longueur de la trame ARP Reply

Tandis que le **nombre d'octets** utilisé pour le padding est de. **18**

Nous pouvons donc remplir les informations sur la trame ARP Request :

- Adresse MAC Destination : **c0:35:32:5b:e3:81**
- Adresse MAC Source : **00:11:32:32:37:b5**
- Ethertype : **08 06** (ARP)
- Opcode (en hexa.) : **00 01** (Request)
- L'adresse MAC Target : **00:00:00:00:00:00**
- Et l'adresse IP de la Target : **172.17.5.72**

Nous sélectionnons ensuite notre trame ICMP Echo Request et nous pouvons déduire les points suivants.

```

Frame 8: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{D5BE8195-EC5E-4F01-B6CC-E8BDF2FA8F85},
Ethernet II, Src: LiteonTechno_5b:e3:81 (c0:35:32:5b:e3:81), Dst: Synology_32:37:b5 (00:11:32:32:37:b5)
  Destination: Synology_32:37:b5 (00:11:32:32:37:b5)
  Source: LiteonTechno_5b:e3:81 (c0:35:32:5b:e3:81)
  Type: IPv4 (0x0800)
  [Stream index: 4]
Internet Protocol Version 4, Src: 172.17.5.72, Dst: 172.17.254.5
Internet Control Message Protocol
0000  00 11 32 32 37 b5 c0 35 32 5b e3 81 08 00 45 00  ..227..5 2[....E
0010  00 3c 03 08 00 00 80 01 dc 48 ac 11 05 48 ac 11  <.....H...H..
0020  fe 05 08 00 4d 33 00 01 00 28 61 62 63 64 65 66  ...H3... (abcdef
0030  67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76  ghijklm opqrstuv
0040  77 61 62 63 64 65 66 67 68 69  wabdefgh

```

Figure 6 : Informations sur la trame ICMP Echo Request

- Les octets de **position 0x0C et 0x0D** ligne 0000, est le champ Ethertype qui est de **0800**, il s'agit donc d'un paquet IP encapsulé.
- Dans l'octet de position **0x07** ligne 0010, il s'agit de la valeur en hexa **01**, c'est-à-dire le protocole ICMP.

```

0000  00 11 32 32 37 b5 c0 35 32 5b e3 81 08 00 45 00
0010  00 3c 03 08 00 00 80 01 dc 48 ac 11 05 48 ac 11
0020  fe 05 08 00 4d 33 00 01 00 28 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

```

Figure 7 : Trame brute (en hexadécimal) avec le champ Ethertype et le champ protocole ICMP

- La longueur de la trame est de **74 octets**.

```

Frame 8: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{D5BE8195-EC5E-4F01-B6CC-E8BDF2FA8F85},
Section number: 1
  Interface id: 0 (\Device\NPF_{D5BE8195-EC5E-4F01-B6CC-E8BDF2FA8F85})
  Encapsulation type: Ethernet (1)
  Arrival Time: Oct 9, 2025 16:22:10.792938000 Paris, Madrid (heure d'été)
  UTC Arrival Time: Oct 9, 2025 14:22:10.792938000 UTC
  Epoch Arrival Time: 1760019730.792938000
  [Time shift for this packet: 0.000000000 seconds]
  [Time delta from previous captured frame: 0.322686000 seconds]
  [Time delta from previous displayed frame: 0.000000000 seconds]
  [Time since reference or first frame: 3.445480000 seconds]
  Frame Number: 8
  Frame Length: 74 bytes (592 bits)

```

Figure 8 : Informations sur la trame ICMP

- La longueur du paquet IP est de **20 octets**.

- Et la longueur du message ICMP est de **40 octets**
- La signification de l'octet de position 0x02 ligne 0020 est de 08, il s'agit donc du **type ICMP Request**.
- A partir de l'octet de position 0x0A de la ligne 0020, il y a **les données applicatives**.

Nous sélectionnons ensuite notre trame **ICMP Echo Reply**. Et nous pouvons donc aussi répondre et remplir les informations suivantes.

Figure 9 : Informations sur la trame ICMP Echo Reply

- Le nom et la valeur de l'octet de position 0x02 ligne 0020, il s'agit du type ICMP, dans le cas présent, il est à **00**, donc **Echo Reply**.

Figure 10 : Section ICMP développée pour afficher le champ type ICMP

2. Capture de trames ARP, DNS et ICMP

Nous allons capturer des trames ICMP depuis une commande ping vers le serveur `ac-nice.fr`, mais avant nous allons vider notre cache ARP en effectuant la commande `arp -d *`.

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

Et nous démarrons notre capture de trames avec Wireshark.

La machine dont l'adresse MAC est recherchée est le routeur Stormshield.

1143	6.588570	LiteonTechno_...	Broadcast	ARP	42	Who has 172.17.250.3? Tell 172.17.5.72
1144	6.591018	Stormshield_2...	LiteonTechno_...	ARP	60	172.17.250.3 is at 00:0d:b4:2a:a8:34

Figure 11 : Trames capturées de l'échange ARP

C'est-à-dire 00:0d:b4:2a:a8:34 (Adresse MAC du routeur Stormshield).

Nous pouvons ainsi remplir les informations suivantes :

- Adresse **MAC Destination** : ff:ff:ff:ff:ff:ff
- Adresse **MAC Source** : c0:35:32:5b:e3:81
- L'Ethertype est **0806** en hexadécimal c'est-à-dire que c'est un **message ARP**

0000	c0 35 32 5b e3 81 00 0d	b4 2a a8 34 08 06 00 01	-52[. . . . * 4 . .
0010	08 00 06 04 00 02 00 0d	b4 2a a8 34 ac 11 fa 03 * 4
0020	c0 35 32 5b e3 81 ac 11	05 48 00 00 00 00 00 00	-52[. . . . H
0030	00 00 00 00 00 00 00 00	00 00 00 00

Figure 12 : Trame brute (en hexadécimal) du message ARP Request

- L'**Opcode** est **01**, donc une **ARP Request**.
- **MAC Cible** : 00:00:00:00:00:00
- Et **l'IP Cible** : 172.17.250.3
 - La raison pour laquelle nous trouvons un échange de requête ARP avant l'envoi de requête DNS est dû au fait que **nous avons supprimé notre cache ARP pendant notre capture** puis nous avons fait un *ping* au serveur web ac-nice.fr, pour faire cela on doit avoir accès au routeur, mais nous ne connaissons pas le routeur ; **la requête ARP devient donc vitale** pour pouvoir échanger avec le routeur et faire sortir la requête sur Internet.

Nous consultons notre cache DNS et nous voyons notre présence du site www.ac-nice.fr avec la commande `ipconfig /displaydns`

```

www.ac-nice.fr
-----
Nom d'enregistrement. : www.ac-nice.fr
Type d'enregistrement : 5
Durée de vie . . . . : 296
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 . . . . : 296
Longueur de données . : 4
Section . . . . . : Réponse
Enregistrement (hôte) : 141.101.90.104

Nom d'enregistrement. : www.ac-nice.fr.cdn.cloudflare.net
Type d'enregistrement : 1
Durée de vie . . . . : 296
Longueur de données . : 4
Section . . . . . : Réponse
Enregistrement (hôte) : 141.101.90.105

```

Figure 13 : Résultat de la commande `ipconfig /displaydns` pour le site www.ac-nice.fr

Quand nous refaisons une requête ping sur le même site, nous ne revoyons logiquement **aucune requête DNS**.

Nous vidons notre cache DNS en effectuant la commande `ipconfig /flushdns` et nous refaisons notre capture de trame et notre ping.

```

C:\Windows\System32>ipconfig /flushdns

Configuration IP de Windows

Cache de résolution DNS vidé.

```

Figure 14 : Résultat de la commande `ipconfig /flushdns` dans l'invite de commande

Nous faisons une commande `ping` vers le serveur web ac-nice.fr pour obtenir notre trame DNS.

Nous pouvons observer ci-dessous la trame.

```

13 76571584 172.17.5.8 172.17.254.1 DNS 70 Standard query 0xd7aa A ac-nice.fr
14 8.050995 172.17.254.1 172.17.5.8 DNS 86 Standard query response 0xd7aa A ac-nice.fr A 185.75.143.93
15 8.070997 172.17.5.8 185.75.143.93 ICMP 74 Echo (ping) request id=0x0001, seq=15/3840, ttl=128 (reply in 16)
16 8.160767 185.75.143.93 172.17.5.8 ICMP 74 Echo (ping) reply id=0x0001, seq=15/3840, ttl=51 (request in 15)
19 8.873877 VMware_22:87:... Broadcast ARP 60 Who has 172.17.244.15? Tell 172.17.243.11
20 9.076880 172.17.5.8 185.75.143.93 ICMP 74 Echo (ping) request id=0x0001, seq=16/4096, ttl=128 (reply in 21)
21 9.184763 185.75.143.93 172.17.5.8 ICMP 74 Echo (ping) reply id=0x0001, seq=16/4096, ttl=51 (request in 20)
22 9.693211 VMware_22:87:... Broadcast ARP 60 Who has 172.17.244.15? Tell 172.17.243.11
23 10.096876 172.17.5.8 185.75.143.93 ICMP 74 Echo (ping) request id=0x0001, seq=17/4352, ttl=128 (reply in 24)
24 10.208821 185.75.143.93 172.17.5.8 ICMP 74 Echo (ping) reply id=0x0001, seq=17/4352, ttl=51 (request in 23)
45 10.717143 VMware_22:87:... Broadcast ARP 60 Who has 172.17.244.15? Tell 172.17.243.11
46 11.103999 172.17.5.8 185.75.143.93 ICMP 74 Echo (ping) request id=0x0001, seq=18/4608, ttl=128 (reply in 48)
48 11.134649 185.75.143.93 172.17.5.8 ICMP 74 Echo (ping) reply id=0x0001, seq=18/4608, ttl=51 (request in 46)
57 12.970162 VMware_22:87:... Broadcast ARP 60 Who has 172.17.244.15? Tell 172.17.243.11

Frame 13: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface \Device\NPF_{D5BE8195-E...}
Ethernet II, Src: LiteonTechno_5b:e3:81 (c0:35:32:5b:e3:81), Dst: Dell_7d:0e:2b (d4:ae:52:7d:0e:2b)
Internet Protocol Version 4, Src: 172.17.5.8, Dst: 172.17.254.1
User Datagram Protocol, Src Port: 61722, Dst Port: 53
Source Port: 61722
Destination Port: 53
Length: 36
Checksum: 0x29b8 [unverified]
[Checksum Status: Unverified]
[Stream index: 3]
[Stream Packet Number: 1]
[Timestamps]
UDP payload (28 bytes)
Domain Name System (query)
0000 d4 ae 52 7d 0e 2b c0 35 32 5b e3 81 08 00 45 00 ...R]+5 2[...E
0010 00 38 5b 24 00 00 80 11 84 64 ac 11 05 08 ac 11 8[...d...
0020 fe 01 f1 1e 00 35 00 25 29 88 d7 aa 01 00 80 01 ...5 $)...
0030 00 00 00 00 00 00 07 61 63 2d 6e 69 63 65 02 66 ... a-c-nice f
0040 72 00 00 01 00 01 ...
  
```

Figure 15 : Trame capturée de la requête DNS pour `www.ac-nice.fr`

- Dans une trame DNS les différents protocoles encapsulés sont ;
 - Le protocole DNS encapsulé dans **UDP**
 - **UDP** encapsulé dans **IPv4**
 - Et **IPv4** encapsulé dans **Ethernet**

La machine destinataire de la requête DNS est le **serveur DNS** (ici ROI), elle a pour **IP : 172.17.254.1**

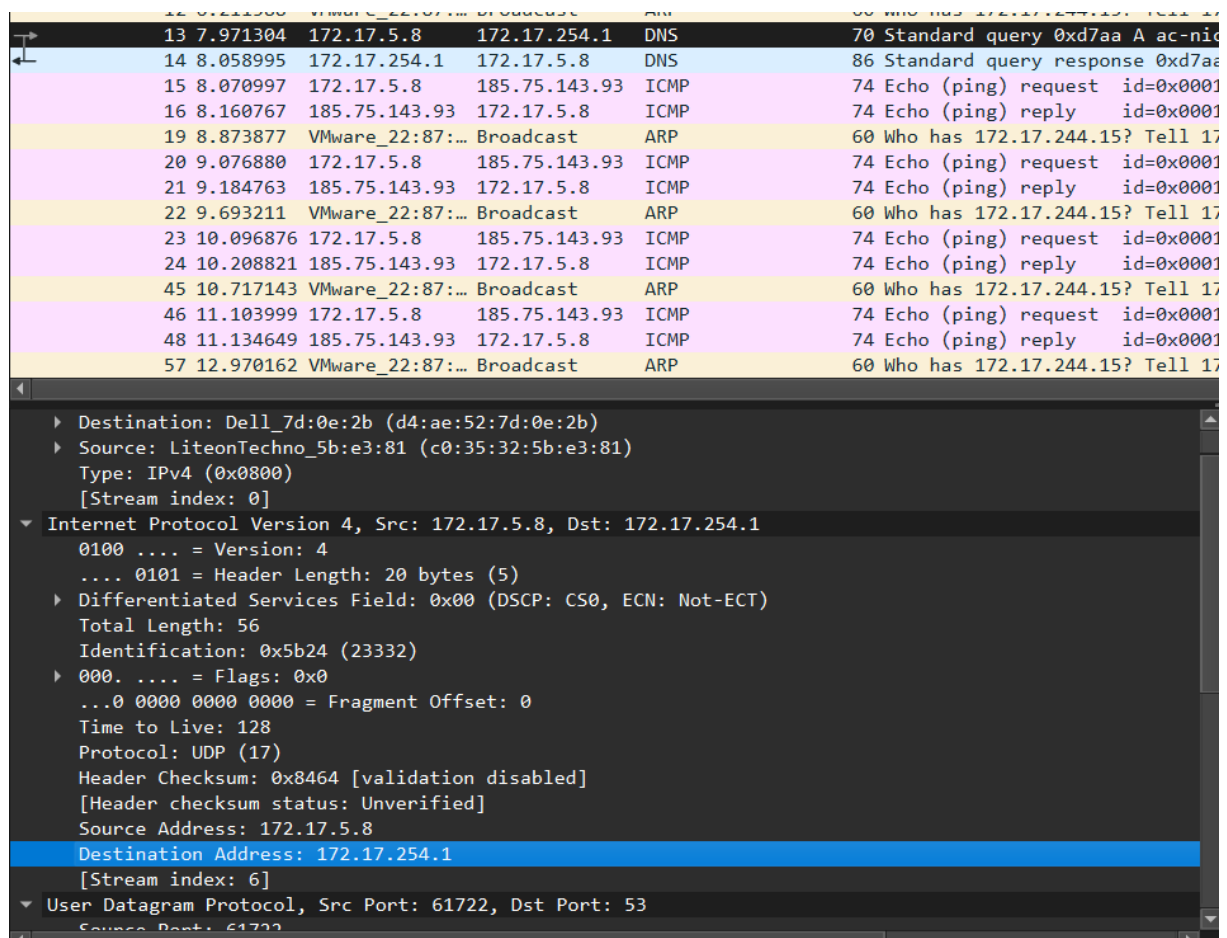


Figure 16 : Adresse IP destination en surbrillance dans la trame DNS

La signification des bits de positions **0x0C**, **0x0D** ligne 0000 et **0x07** ligne 0010 est :

- Le champ Ethertype, ici **0800** signifie IPv4.
- La longueur de l'en tête IP est de **20 octets**.
- La longueur de l'en tête Transport (UDP) est de **8 octets**.
- La signification qu'ont les octets de position **0x04** et **0x05** ligne 0020 s'agit du champ Port destination, ici il est à « **00 35** » en hexadécimal, donc **53** en décimal.
- Les valeurs hexadécimales correspondant au site www.ac-nice.fr est : « **03 77 77 77 07 61 63 2d 6e 69 63 65 02 66 72 00** »
- Les valeurs hexadécimales de l'adresse IP du serveur web de l'Académie de Nice est : « **8d 65 5a 6b** » et en décimal cela nous donne : « **141.101.90.107** ».

3. Commande Tracert et capture de trames ICMP.

Nous commençons une nouvelle capture de trame sur Wireshark que nous intitulerons CaptureTracert.

Puis nous ouvrons notre invite de commande et nous tapons la commande suivante : **tracert www.ac-nice.fr**

Une fois la commande terminée, nous arrêtons la capture de trames et nous filtrons les captures avec le filtre **icmp**.

No.	Time	Source	Destination	Protocol	Length	Info
40	4.247143	10.73.23.242	172.17.5.8	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
38	4.242684	10.73.23.242	172.17.5.8	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
36	4.238285	10.73.23.242	172.17.5.8	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
39	4.244003	172.17.5.8	141.101.90.107	ICMP	106	Echo (ping) request id=0x0001, seq=23/5888, ttl=1 (no response found!)
37	4.240209	172.17.5.8	141.101.90.107	ICMP	106	Echo (ping) request id=0x0001, seq=22/5632, ttl=1 (no response found!)
35	4.231028	172.17.5.8	141.101.90.107	ICMP	106	Echo (ping) request id=0x0001, seq=21/5376, ttl=1 (no response found!)

Figure 17 : Trame ICMP suite à la commande tracert

- Quand nous développons l'en-tête IP, nous pouvons déduire l'IP Destination qui est : **141.101.90.107** en décimal et **8d 65 5a 6b** en hexadécimal.
- La valeur portée par le champ TTL en **décimal** est **1** et **01** en hexadécimal
- La valeur portée par le champ Type dans la section correspondant au message ICMP est **8 (Echo request)** et **08** en hexadécimal

Nous sélectionnons la première trame avec le message d'erreur **ICMP TTL exceeded** et nous développons la section correspondant au message ICMP et nous voyons dans le champ Type la valeur **11**, soit **0B** en hexadécimal.