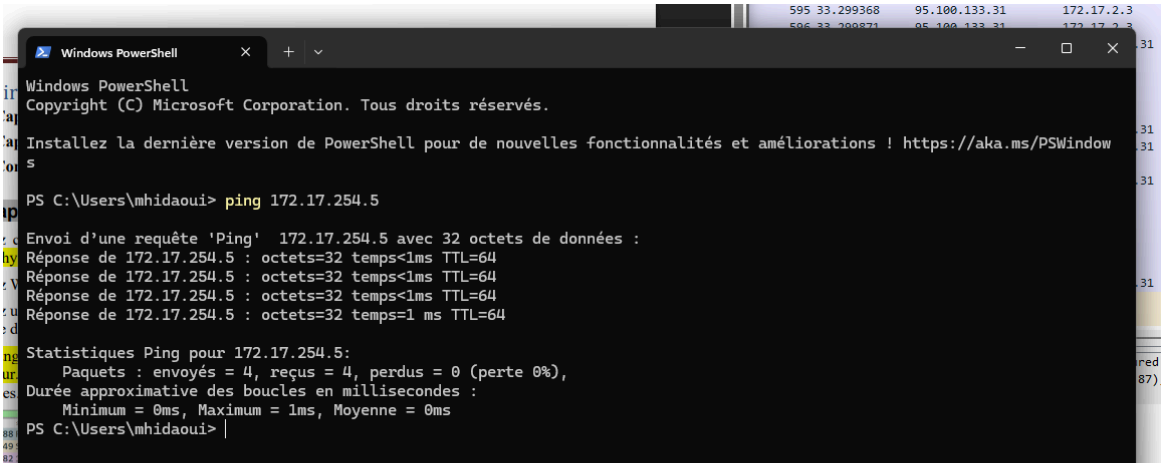
TP5 : Trames ARP, ICMP et DNS HIDAOUI Mohamed-Amine BTS SIO 1

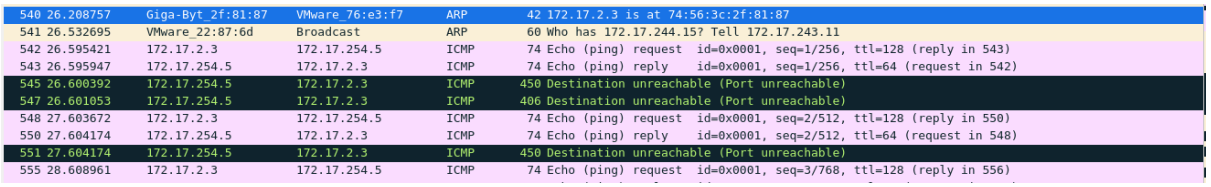
sommaire

4.1. Capture de trames ARP et ICMP.

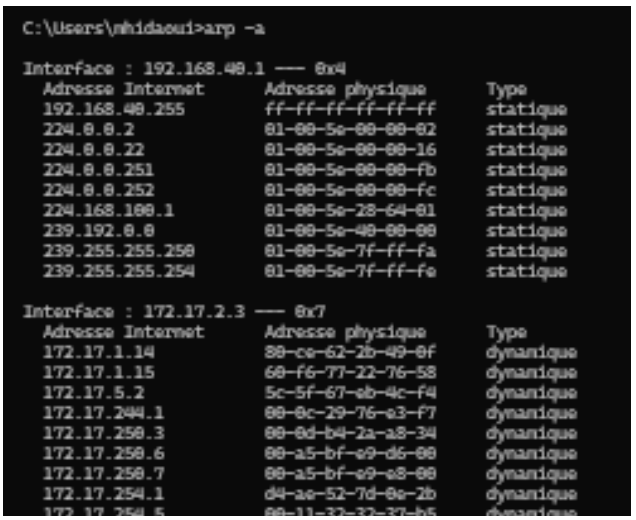
ping d' aviateur



Démarrage d'une trame WireShark



exécution de la commande "arp -a"



Partie ARP question

Signification : Type Ethernet = 0x0806 = protocole ARP

Fonction ARP Request : Recherche l'adresse MAC à l'aide d'une adresse IP donnée

Position 0x04 et 0x05 ligne 0010 : Protocol size = 0x04 = longueur de l'adresse IP en octets

message ARP : 28 octets

trame ARP Request : 42 octets = 14 octets Ethernet + 28 octets ARP

trame ARP Reply : 42 octets

padding : 18 octets

Rubriques

Trame ARP Request :

- **@MAC destination = ff:ff:ff:ff:ff:ff = broadcast**
- **@MAC source = 00:0c:29:22:87:6d**
- **Ethernet Type = 0x0806**
- **Opcode = 0x0001 = request**
- **@MAC de la cible = 00:00:00:00:00:00**
- **@IP de la cible = 172.17.244.15**

Partie Questions ICMP Echo Request

Signification : Type Ethernet = 0x0800 = protocole IPv4

Signification : TTL (Time To Live) = 128

Longueur de la trame : 74 octets

Longueur paquet IP : 60 octets

Longueur du message ICMP : 40 octets = 60 octets IP - 20 octets en-tête IP

Signification : Message type ICMP Echo Request

Octets à partir de 0x0A ligne 0020 :

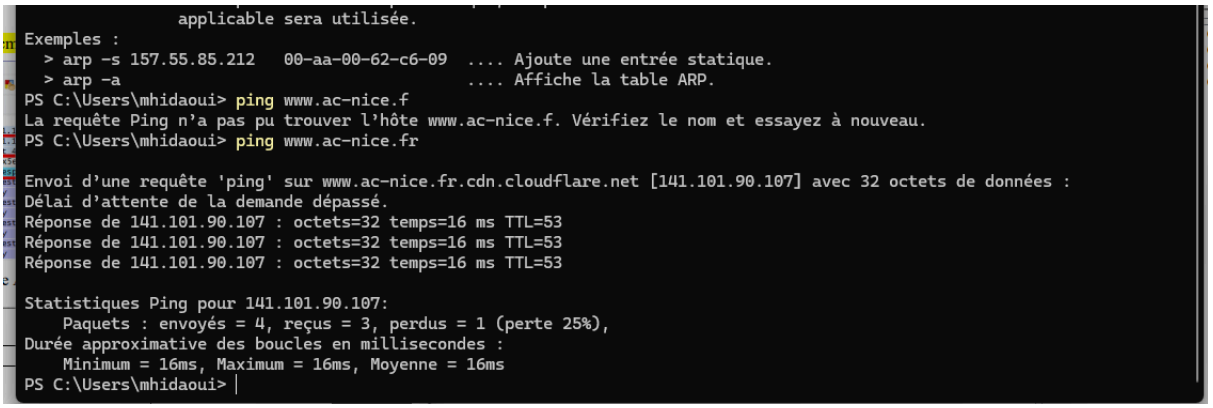
- **Octets 0x0A-0x0B : Sequence Number (LE) = 256 (0x0100)**
- **Octets suivants : Données (payload) du message ICMP = 32 octets**

Trame ICMP Echo Reply

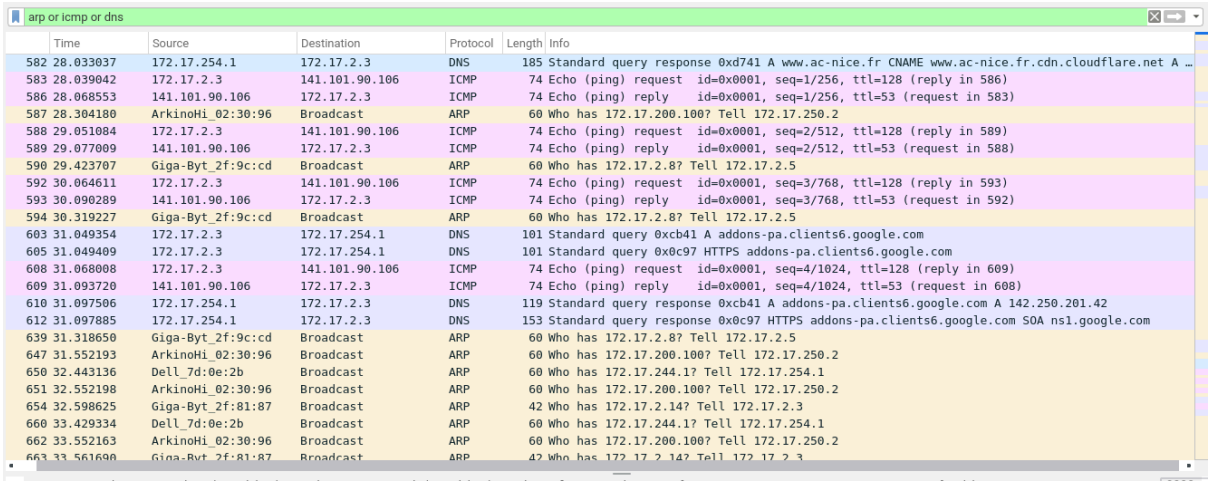
Nom et valeur position 0x02 ligne 0020 : Type ICMP = 0 = Echo Reply

4.2. Capture de trames ARP, DNS et ICMP

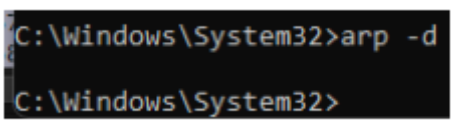
ping de “www.ac-nice.fr”



Trame qui à démarrer avant la commande ping



vide du cash ARP



Partie Question ARP, ICMP et DNS

Analyse de la capture réseau (trames ARP, DNS, ICMP) :

Identification de la machine recherchée

Machine dont l'adresse MAC est recherchée : 172.17.2.8

Rubriques

Trame ARP Request (Frame 594) :

- **@MAC destination = ff:ff:ff:ff:ff:ff = broadcast**
- **@MAC source = 74:56:3c:2f:9c:cd**
- **Ethernet Type = 0x0806**
- **Opcode = 0x0001 = request**
- **@MAC de la cible = 00:00:00:00:00:00**
- **@IP de la cible = 172.17.2.8**

Raison de la requête DNS avant ICMP

Execution de ping"www.ac-nice.fr au lieu d'une adresse IP, le système doit d'abord résoudre le nom en IP à l'aide de la requête DNS. La séquence est :

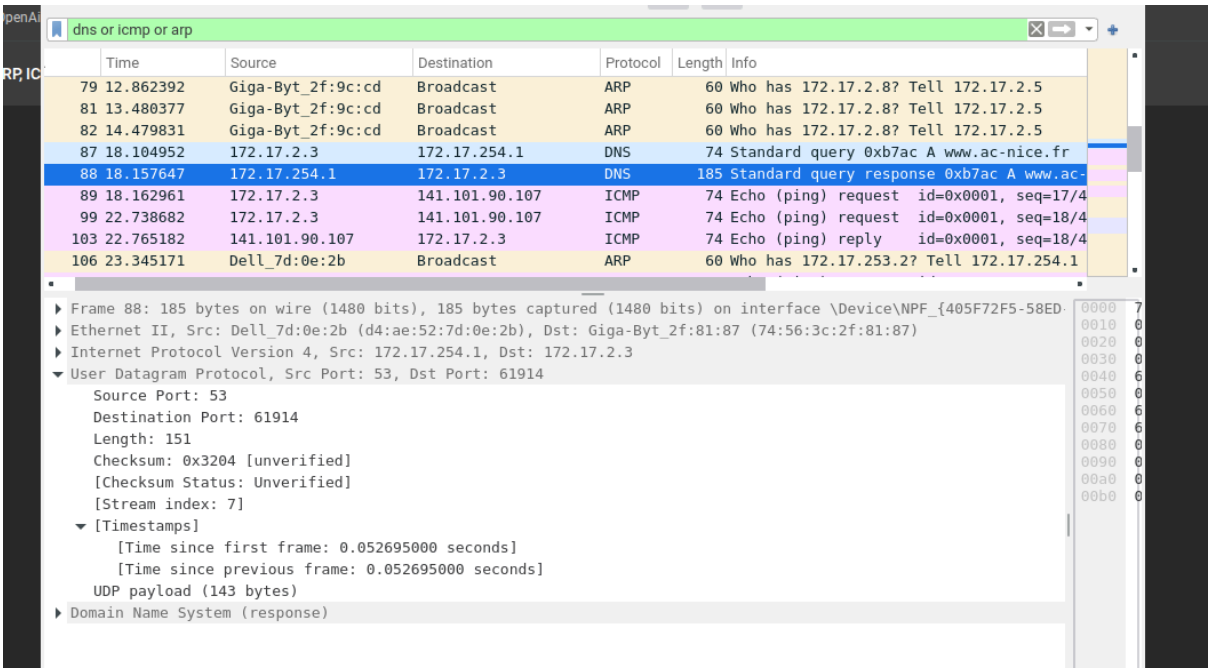
Exécution de ipconfig /displaydns

```
www.ac-nice.fr
----------------------------------------
Nom d'enregistrement. : www.ac-nice.fr
Type d'enregistrement : 5
Durée de vie  . . . . : 8714
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  . . . . : 8714
Longueur de données . : 4
Section . . . . . . . : Réponse
Enregistrement (hôte) : 141.101.90.106
```

Exécution de "ipconfig /flushdns"

```
Configuration IP de Windows

Cache de résolution DNS vidé.
```

Les Trames après le vide du cash DNS



Partie Questions analyse de la trame DNS

Protocoles encapsulés : Ethernet II → IPv4 → UDP → DNS

Destinataire : 172.17.254.1 (serveur DNS)

Signification des octets

Signification : Type Ethernet = 0x0800 IPv4

Signification : TTL (Time To Live) du paquet IP

En-tête IP : 20 octets

En-tête UDP : 8 octets

Signification : Port source UDP = 53 = 0x0035

"www.ac-nice.fr", les valeurs hexa. = 03 77 77 77 02 61 63 04 6e 69 63 65 02 66 72 00

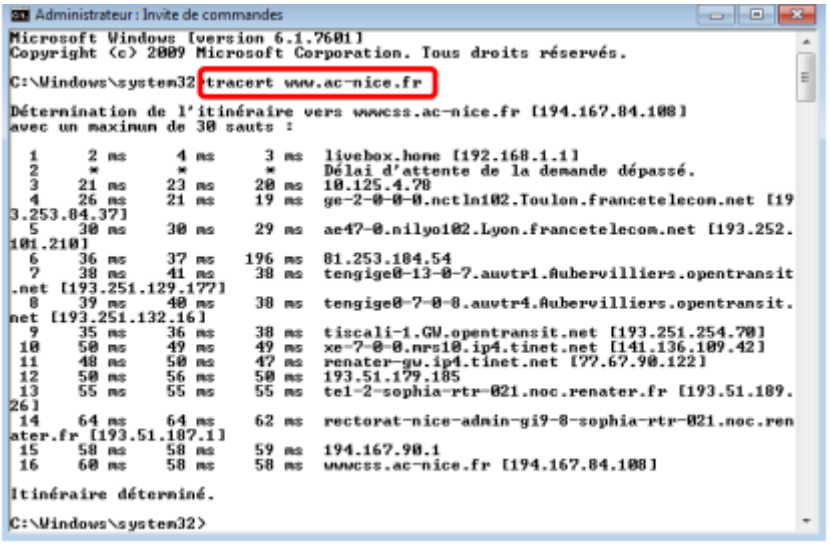
Answers, l'adresse IP du serveur web hébergeant www.ac-nice.fr :

Valeurs hexadécimales : AC 11 02 03

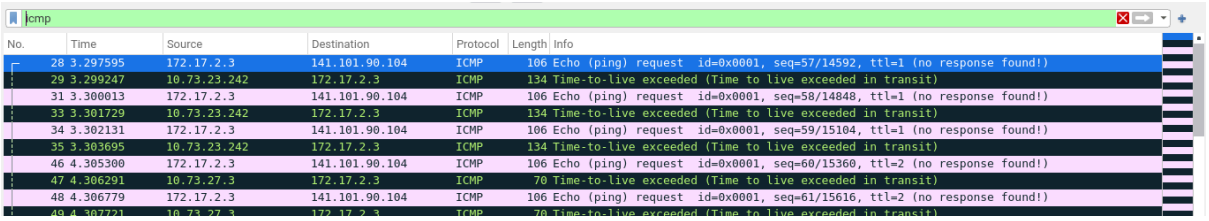
Valeurs décimales : 172.17.2.3

4.3. Commande Tracert et capture de trames ICMP

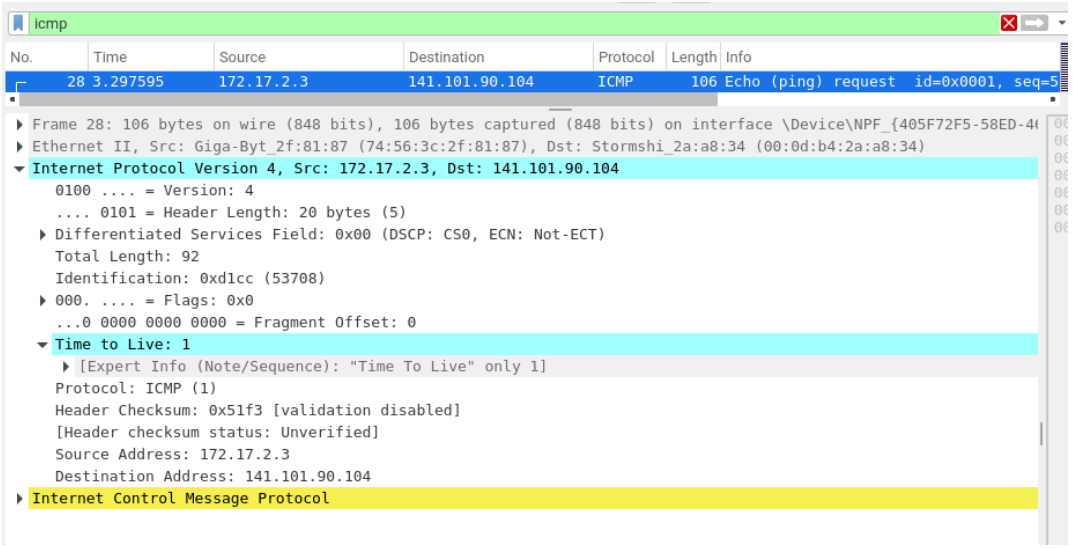
Oublie de faire un capture mais je l'ai fait pour la commande tracert www.ac-nice.fr



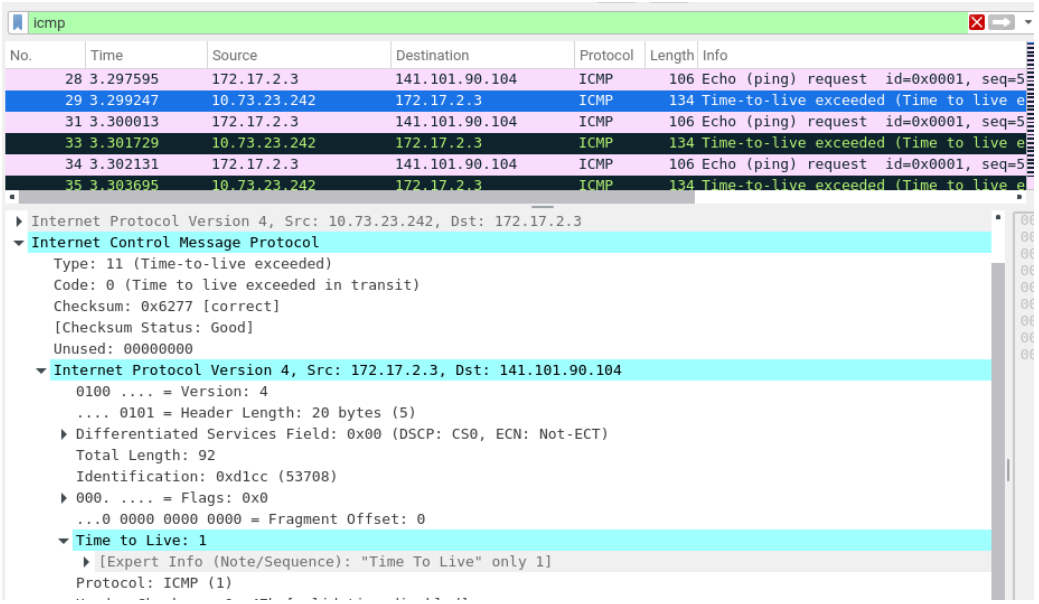
Trame apres la commande tracert www.ac-nice.fr



ICMP Echo Request et TTL



Message ICMP de la Trame “Time-to-live exceeded”



Partie Question Trame ICMP et Exceeded

Adresse IP Destination :

- **Valeur décimale : 141.101.90.104**
- **Valeur hexadécimale : 8D 65 5A 68**

Champ TTL (Time To Live) :

- **Valeur décimale : 1**
- **Valeur hexadécimale : 0x01**

Champ Type ICMP (Echo Request) :

- **Valeur décimale : 8**
- **Valeur hexadécimale : 0x08**

Champ Type ICMP (Time-to-live exceeded) :

- **Valeur décimale : 11**
- **Valeur hexadécimale : 0x0B**

Code ICMP :

- **Valeur décimale : 0 (Time to live exceeded in transit)**
- **Valeur hexadécimale : 0x00**