

TP 5 – Trames ARP, ICMP et DNS

Table des matières :

4.1. Capture de trames ARP et ICMP.....	1
4.2 Capture de trames ARP, DNS et ICMP.....	6
4.3. Commande Tracert et capture de trames ICMP.....	11

4.1. Capture de trames ARP et ICMP.

J'ai ping le serveur aviateur (172.17.254.5) et pris une capture de trame en ayant entré la commande « arp or icmp »

The screenshot displays two windows from a Windows 10 desktop. On the left is the Wireshark network protocol analyzer, showing a capture of ICMP Echo (ping) requests and replies between 172.17.254.5 and 172.17.2.13. The packet list shows several successful ping responses. The packet details pane for packet 13 is expanded, showing the Ethernet II, Internet Protocol Version 4, and Internet Control Message Protocol (ICMP Echo (ping) reply) layers. On the right is the Windows Command Prompt, showing the execution of the command 'C:\Users\Mnovello>ping 172.17.254.5'. The output shows four successful pings with 32 bytes of data, 1ms TTL, and 1ms response time. Below the command prompt output, the statistics for the ping are shown: 4 packets sent, 4 received, 0% loss, and a round-trip time of 0ms.

No.	Time	Source	Destination	Protocol	Length	Info
13	2.535859	172.17.2.13	172.17.254.5	ICMP	74	Echo (ping) request id=0x0001, seq=1/256, ttl=128 (reply)
14	2.535571	172.17.254.5	172.17.2.13	ICMP	74	Echo (ping) reply id=0x0001, seq=1/256, ttl=64 (request)
29	3.539235	172.17.2.13	172.17.254.5	ICMP	74	Echo (ping) request id=0x0001, seq=2/512, ttl=128 (reply)
30	3.539797	172.17.254.5	172.17.2.13	ICMP	74	Echo (ping) reply id=0x0001, seq=2/512, ttl=64 (request)
32	4.542665	172.17.2.13	172.17.254.5	ICMP	74	Echo (ping) request id=0x0001, seq=3/768, ttl=128 (reply)
33	4.543528	172.17.254.5	172.17.2.13	ICMP	74	Echo (ping) reply id=0x0001, seq=3/768, ttl=64 (request)
38	5.547070	172.17.2.13	172.17.254.5	ICMP	74	Echo (ping) request id=0x0001, seq=4/1024, ttl=128 (reply)
39	5.547886	172.17.254.5	172.17.2.13	ICMP	74	Echo (ping) reply id=0x0001, seq=4/1024, ttl=64 (request)
42	7.134214	Giga-Byt_2f19d13	Synology_321371b5	ARP	42	Who has 172.17.254.5? Tell 172.17.2.13
43	7.134976	Synology_321371b5	Giga-Byt_2f19d13	ARP	60	172.17.254.5 is at 00:11:32:32:32:37:1b5

Frame 13: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0
Ethernet II, Src: Giga-Byt_2f19d13 (74:56:3c:2f:19:d13), Dst: Synology_321371b5 (08:00:27:19:d1:37:1b5)
Internet Protocol Version 4, Src: 172.17.2.13, Dst: 172.17.254.5
Internet Control Message Protocol
Echo (ping) reply id=0x0001, seq=4/1024, ttl=64 (request)

Microsoft Windows [version 10.0.26100.6584]
(c) Microsoft Corporation. Tous droits réservés.
C:\Users\Mnovello>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 = 1ms, Moyenne = 0ms
C:\Users\Mnovello>

J'ai effectué la commande « arp -a » pour vérifier la présence de l'association @IP-@MAC correspondant à Aviateur

```
C:\Users\Mnovello>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 = 1ms, Moyenne = 0ms

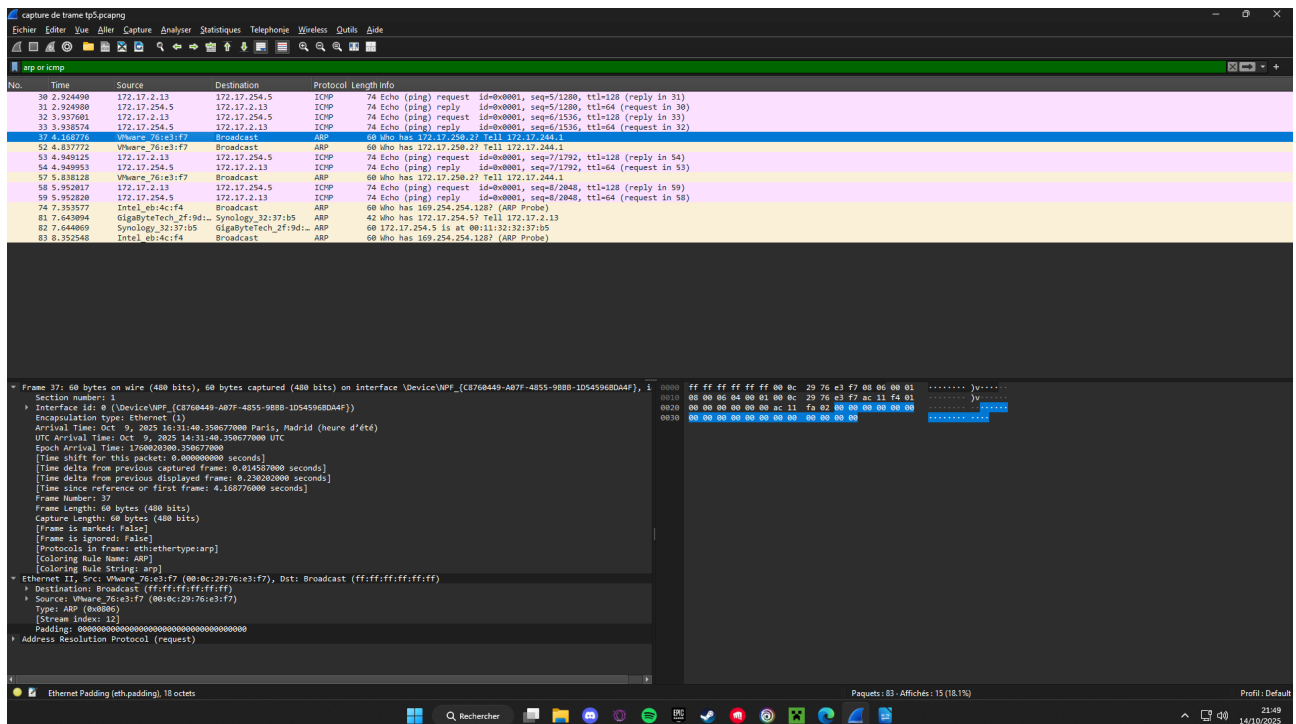
C:\Users\Mnovello>arp -d
La suppression de l'entrée ARP a échoué : L'opération demandée nécessite une élévation.

C:\Users\Mnovello>arp -a

Interface : 172.17.2.13 --- 0x11
Adresse Internet    Adresse physique    Type
172.17.5.27         00-57-7e-28-9b-41  dynamique
172.17.5.72         c0-35-32-5b-e3-81  dynamique
172.17.244.1        00-0c-29-76-e3-f7  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-e3-00  dynamique
172.17.254.1        d4-ae-52-7d-0e-2b  dynamique
172.17.254.5        00-11-32-32-37-b5  dynamique
172.17.254.6        00-11-32-a6-21-99  dynamique
172.17.255.255      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
224.168.100.1       01-00-5e-28-64-01  statique
239.255.102.18      01-00-5e-7f-66-12  statique
239.255.255.250     01-00-5e-7f-ff-fa  statique
239.255.255.254     01-00-5e-7f-ff-fe  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
224.0.0.2           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
224.168.100.1       01-00-5e-28-64-01  statique
239.255.102.18      01-00-5e-7f-66-12  statique
239.255.255.250     01-00-5e-7f-ff-fa  statique
```

J'ai sélectionné une frame ARP pour répondre aux questions suivantes :



- Quelle signification ont les octets de position 0×0C et 0×0D ligne 0000 ?

EtherType = 0x0806 (ARP)

- Quelle est la fonction de la trame ARP Request ?

Elle demande qui possède l'adresse IP 172.17.244.2 afin d'obtenir l'adresse MAC correspondante

- Quelle signification ont les octets de position 0×04 et 0×05 ligne 0010 ?

les octets de position 0×04 et 0×05 ligne 0010 correspondent aux octets 00 01 ce qui signifie que le hardware type est Ethernet 1

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

La longueur d'un message ARP est de 28 octets

- Quelle est la longueur de la trame ARP Request ?

La longueur de la trame ARP request est de 60 octets

- Quelle est la longueur de la trame ARP Reply ?

La longueur de la trame ARP Reply est de 60 octets

- Combien d'octets sont utilisés pour le padding ?

Il y a 18 octets qui sont utilisés pour le padding

- @MAC destination = ff:ff:ff:ff:ff:ff

- @MAC source = 00:0c:29:76:e3:f7

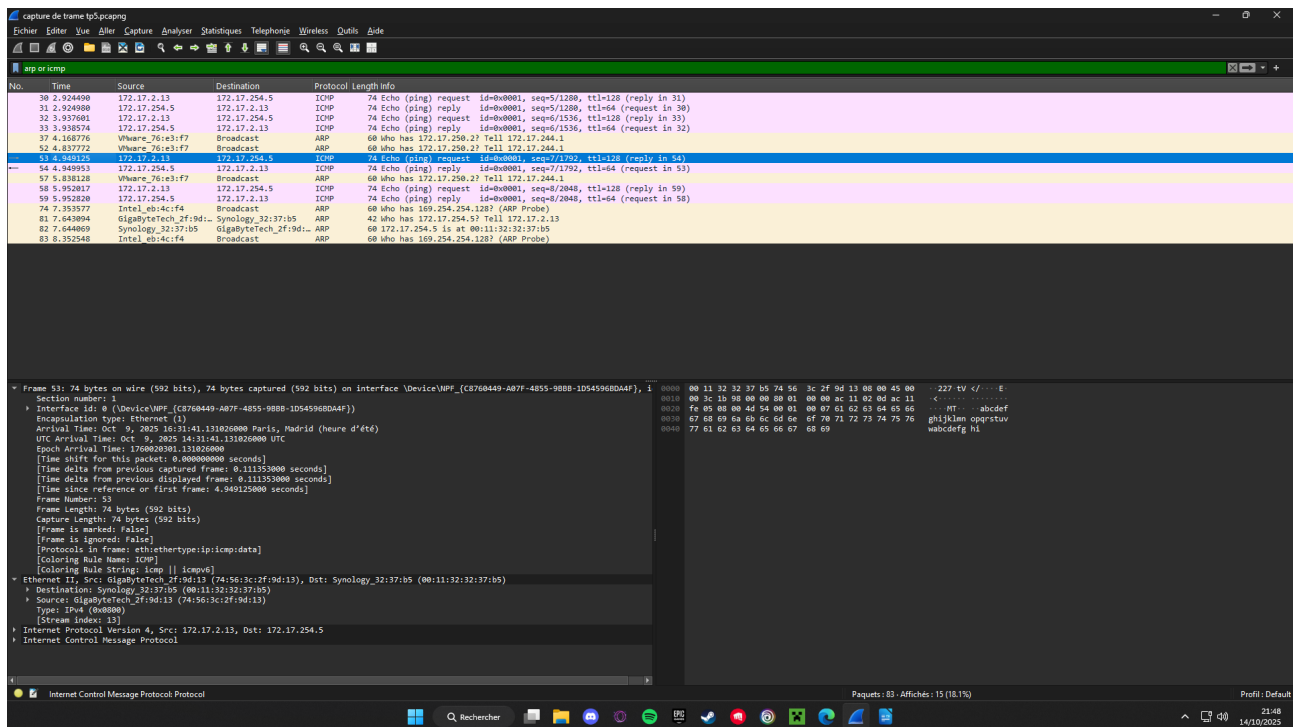
- Ethernet Type = 0806

- Opcode (valeurs hexa.) = 00 01

- @MAC de la cible = 00:00:00:00:00:00

▪ @IP de la cible = 172.17.244.2

J'ai sélectionné une frame ICMP Echo Request pour répondre aux questions:



▪ Sélectionnez une frame ICMP Echo Request. A l'aide du Chapitre 5 (pages 4 et 5), répondez aux questions suivantes : Quelle signification ont les octets de position 0x0C et 0x0D ligne 0000 ?

C'est un paquet IP (0800) qui indique que la trame transporte un paquet IPv4

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

▪ Quelle est la longueur de la trame ?

La longueur de la trame est de 74 octets

▪ Quelle est la longueur du paquet IP ?

La longueur du paquet IP est de 60 octets

▪ Quelle est la longueur du message ICMP ?

La longueur du message ICMP est de 40 octets

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

La signification est que l'octet correspond au champ code =0 (code du message) et type =8 (Protocole ICMP Echo request)

▪ A quoi correspondent les octets à partir de l'octet 0x0A, ligne 00020 ?

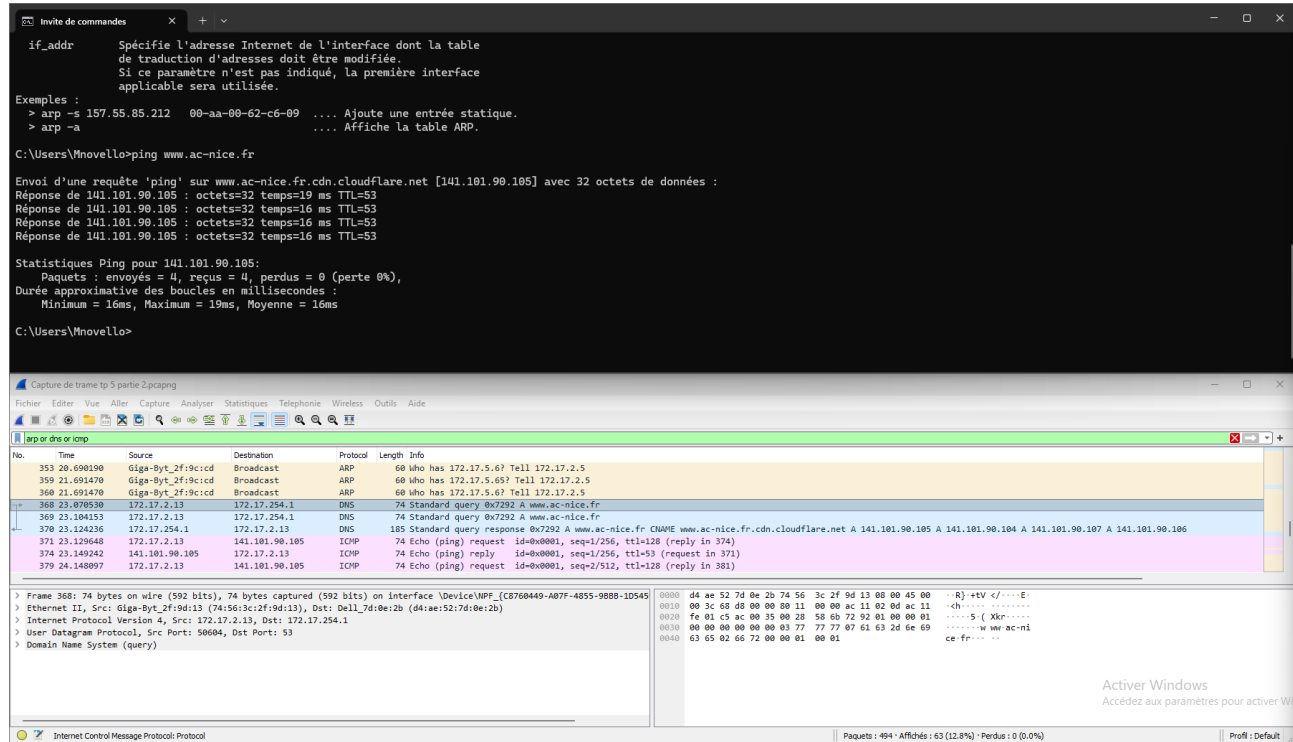
Ce sont les octets ASCII ou l'on trouve toutes les données du message ICMP

▪ Sélectionnez une trame ICMP Echo Reply. Quelle est le nom et la valeur de l'octet de position 0x02 ligne 00020 ?

Sa valeur est 0x00 ce qui signifie que le champ ICMP type = 0 et le champ code = 0

4.2 Capture de trames ARP, DNS et ICMP.

J'ai réalisé un ping vers le serveur www.ac-nice.fr



■ La liste des trames commence par une requête et une réponse ARP. Quelle est la machine dont l'adresse MAC est recherchée ?

La machine dont l'adresse MAC est recherché est la machine 172.17.5.65

■ Complétez les rubriques ci-dessous : Trame ARP request

@MAC destination = ff:ff:ff:ff:ff:ff

@MAC source = 74 56 3c 2f 9c cd

Ethernet Type = 08 06

Opcode (valeurs hexa.) = 00 01

@MAC de la cible = 00:00:00:00:00:00

@IP de la cible = 172.17.5.65

▪ Pour quelle 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 avant d'envoyer les trames ICMP pour ping la machine doit d'abord savoir vers quelle adresse IP l'envoyer et c'est le rôle du DNS

▪ Consultez 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 :

```
www.ac-nice.fr
-----
Nom d'enregistrement. : www.ac-nice.fr
Type d'enregistrement : 5
Durée de vie . . . . : 441011
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 . . . . : 441011
Longueur de données . : 4
Section . . . . . : Réponse
Enregistrement (hôte) : 141.101.90.105
```

J'ai bien la présence de l'enregistrement DNS ac-nicfe.fr avec l'adresse IP associé qui est 141.101.90.105

J'ai effectué une deuxième capture de trame en ayant pin www.ac-nice.fr et je ne constate pas de trame DNS affiché :

File Edit View All Capture Analyser Statistics Telephonie Wireless Outils Aide
10/23

File Edit View All Capture Analyser Statistics Telephonie Wireless Outils Aide

File Edit View All Capture Analyser Statistics Telephonie Wireless Outils Aide

No.	Time	Source	Destination	Protocol	Length	Info
11	4.036196	Dell_7d70e12b	Broadcast	ARP	60	Who has 172.17.244.1? Tell 172.17.254.1
12	4.564432	Vhware_22:87:6d	Broadcast	ARP	60	Who has 172.17.244.15? Tell 172.17.243.11
14	4.847608	Dell_7d70e12b	Broadcast	ARP	60	Who has 172.17.244.1? Tell 172.17.254.1
21	5.486178	Vhware_22:87:6d	Broadcast	ARP	60	Who has 172.17.244.15? Tell 172.17.243.11
22	5.847790	Dell_7d70e12b	Broadcast	ARP	60	Who has 172.17.244.1? Tell 172.17.254.1
23	4.486352	Vhware_22:87:6d	Broadcast	ARP	60	Who has 172.17.244.15? Tell 172.17.243.11
24	7.058834	Dell_7d70e12b	Broadcast	ARP	60	Who has 172.17.244.1? Tell 172.17.254.1
27	7.496797	172.17.2.13	141.101.90.106	ICMP	74	Echo (ping) request id=0x0001, seq=13/3328, ttl=128 (reply in 28)
28	7.512714	141.101.90.106	172.17.2.13	ICMP	74	Echo (ping) reply id=0x0001, seq=13/3328, ttl=53 (request in 27)
29	7.847404	Dell_7d70e12b	Broadcast	ARP	60	Who has 172.17.244.1? Tell 172.17.254.1
32	8.507790	172.17.2.13	141.101.90.106	ICMP	74	Echo (ping) request id=0x0001, seq=14/3584, ttl=128 (reply in 33)
33	8.524861	141.101.90.106	172.17.2.13	ICMP	74	Echo (ping) reply id=0x0001, seq=14/3584, ttl=53 (request in 32)
35	8.847457	Dell_7d70e12b	Broadcast	ARP	60	Who has 172.17.244.1? Tell 172.17.254.1
37	9.514719	172.17.2.13	141.101.90.106	ICMP	74	Echo (ping) request id=0x0001, seq=15/3840, ttl=128 (reply in 38)
38	9.538390	141.101.90.106	172.17.2.13	ICMP	74	Echo (ping) reply id=0x0001, seq=15/3840, ttl=53 (request in 37)
41	10.523638	172.17.2.13	141.101.90.106	ICMP	74	Echo (ping) request id=0x0001, seq=16/4096, ttl=128 (reply in 44)
44	10.539385	141.101.90.106	172.17.2.13	ICMP	74	Echo (ping) reply id=0x0001, seq=16/4096, ttl=53 (request in 43)
51	11.066826	Dell_7d70e12b	Broadcast	ARP	60	Who has 172.17.244.1? Tell 172.17.254.1
53	13.847820	Dell_7d70e12b	Broadcast	ARP	60	Who has 172.17.244.1? Tell 172.17.254.1
56	14.847627	Dell_7d70e12b	Broadcast	ARP	60	Who has 172.17.244.1? Tell 172.17.254.1

```

> Frame 11: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface \Device\NPF_{C8760449-A077-4855-9080-1D545968044F},
Ethernet II, Src: Dell_7d70e12b (d4ae52:7d:0e:12:b), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
> Address Resolution Protocol (request)

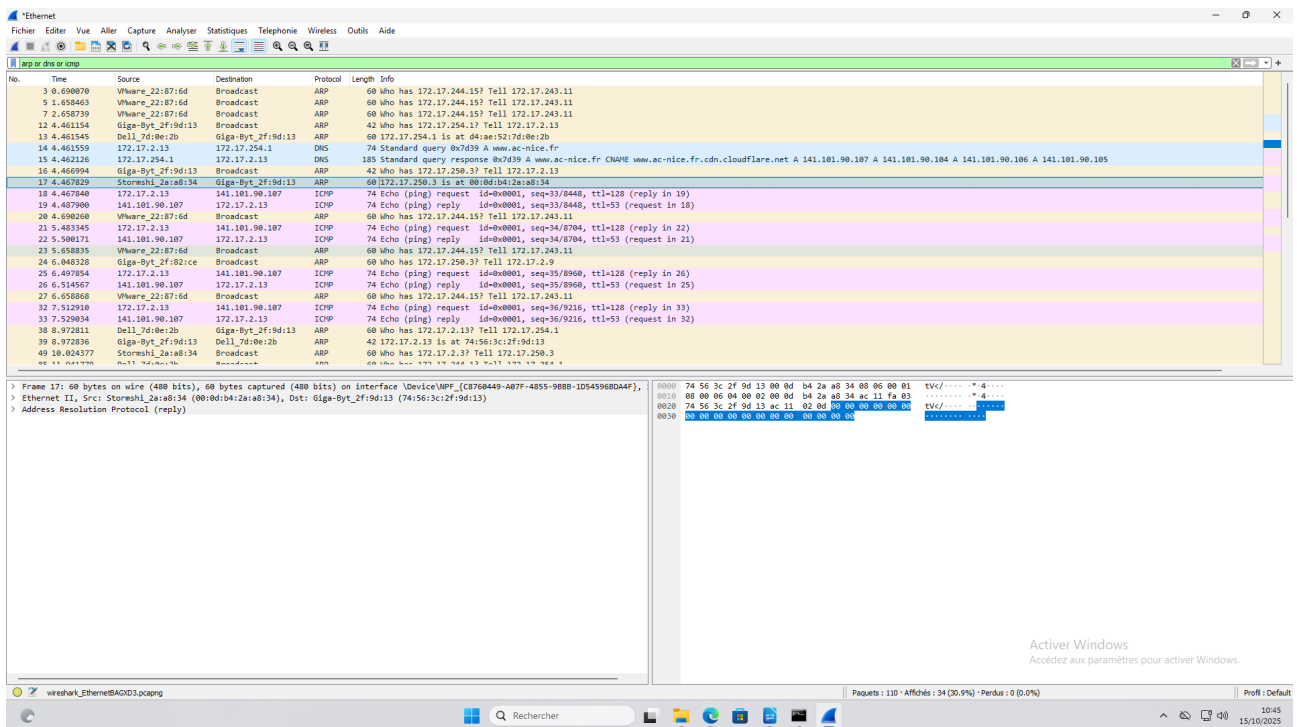
0000  ff ff ff ff ff ff 14 00 52 7d 0e 2b 00 06 00 01  ....[S]....
0010  00 00 00 00 00 00 01 00 52 7d 0e 2b 00 06 00 01  ....[S]....
0020  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ....
0030  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ....

```

Activer Windows
 Accédez aux paramètres pour activer Windows.

Internet Control Message Protocol: Protocol
Paquets : 56 - Affichés : 20 (35.7%) - Perdus : 0 (0.0%)
Profil : Default

J'ai visualiser de nouveau une requête DNS :



▪ Quels sont les différents protocoles encapsulés dans une trame DNS ?

Liaison = Ethernet II

Réseau = IPv4

Transport = UDP

Application = DNS

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

La machine destinataire dans la requête DNS est la mienne, son IP est donc : 172.17.254.1

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

EtherType = 0x0800 (08 00) ce qui signifie que la trame transporte un paquet IPv4

Champ TTL = 0x07 (40) signifie que le paquet peut traversé 64 routeurs avant d'être supprimé

▪ Quelle est l'EtherType = 0x0800 a longueur de l'en-tête IP ?

Longueur de l'en tête IP est de 20 octets

▪ Quelle est la longueur de l'en-tête de transport dans cette trame ?

La longueur de l'en tête de transport est de 8 octets

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

Les octets de position 0x04 et 0x05 ligne 0020 signifie que le port de destination est DNS (53)

▪ 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 ?

61 63 2d 6e 69 63 65 = ac nice

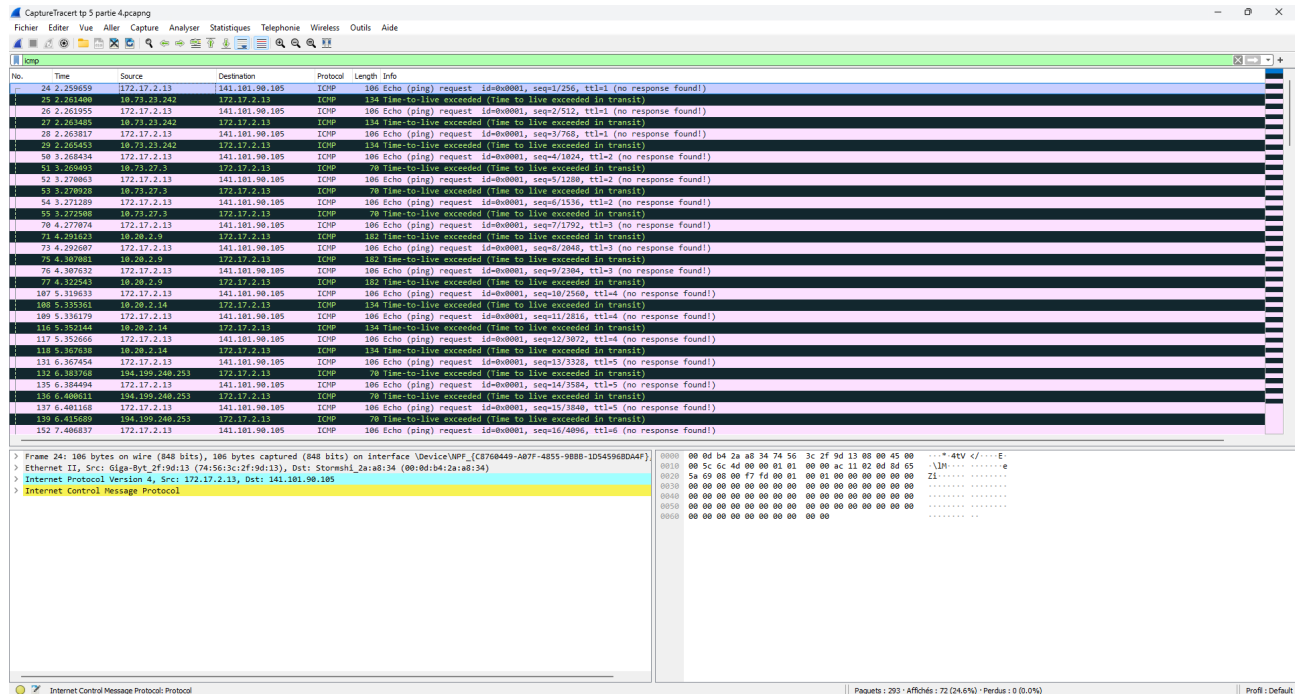
66 72 = fr

▪ 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.

Adresse IP du serveur = 141.101.90.105 = 8D 65 5A 69

4.3. Commande Tracert et capture de trames ICMP.

J'ai effectué une capture de trame en saisissant la commande tracert www.ac-nice.fr. depuis l'invite de commande :



- Sélectionnez la première trame ICMP Echo request. Développez l'en-tête IP. Quelle est l'adresse IP Destination (valeurs déci. et hexa.) ?

L'adresse IP destination est 141.101.90.105 =

- Sélectionnez le champ TTL. Quelle est la valeur portée par ce champ (valeurs déci. et hexa.) ?

La valeur portée par ce champ est 01 =

- 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 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 TTL dans la trame ICMP Time-to-live exceeded est de 11 = 0b en héra