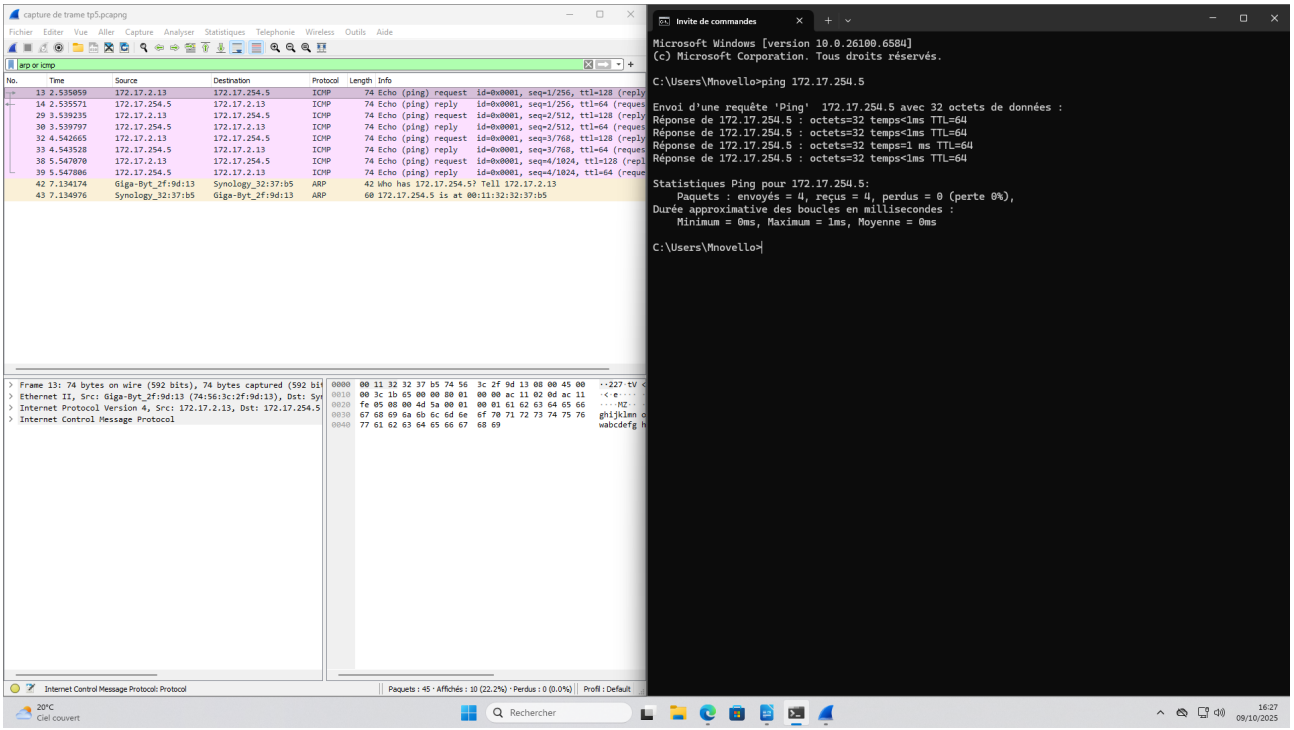
TP 5 – Trames ARP, ICMP et DNS

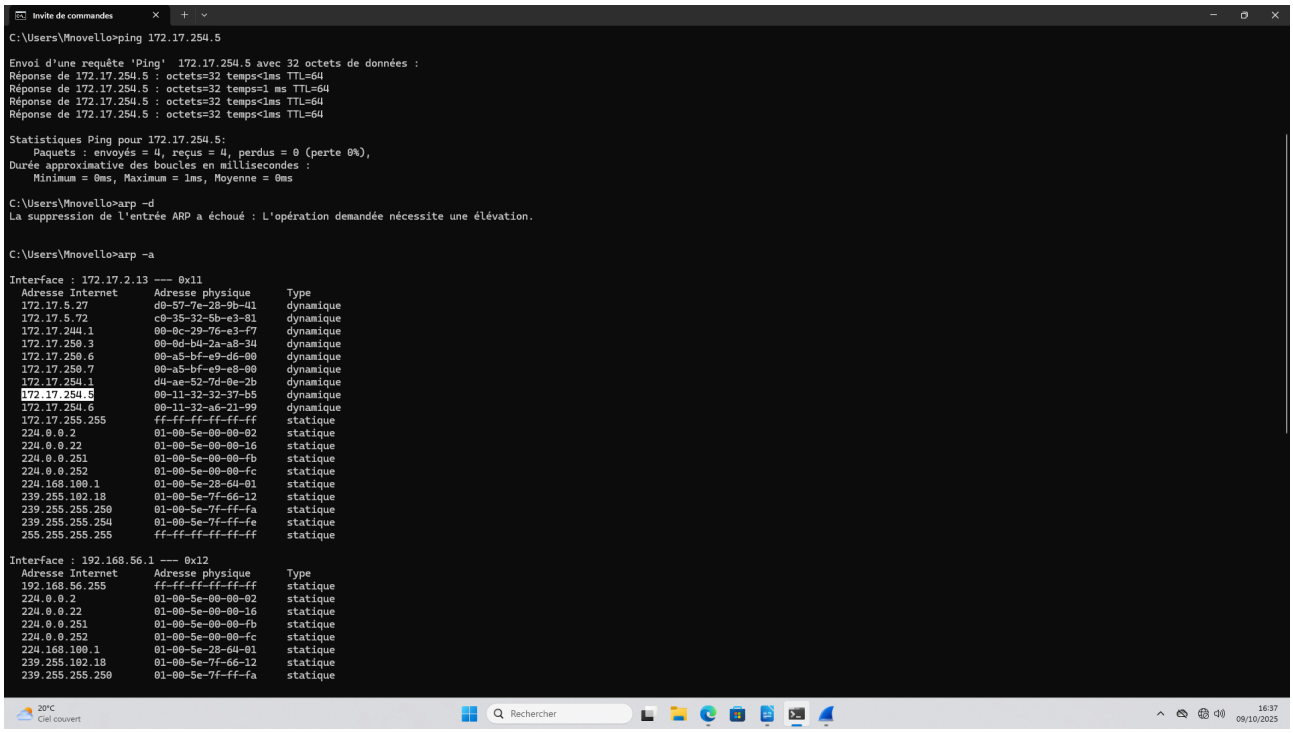
Table des matières :

4.1. Capture de trames ARP et ICMP.

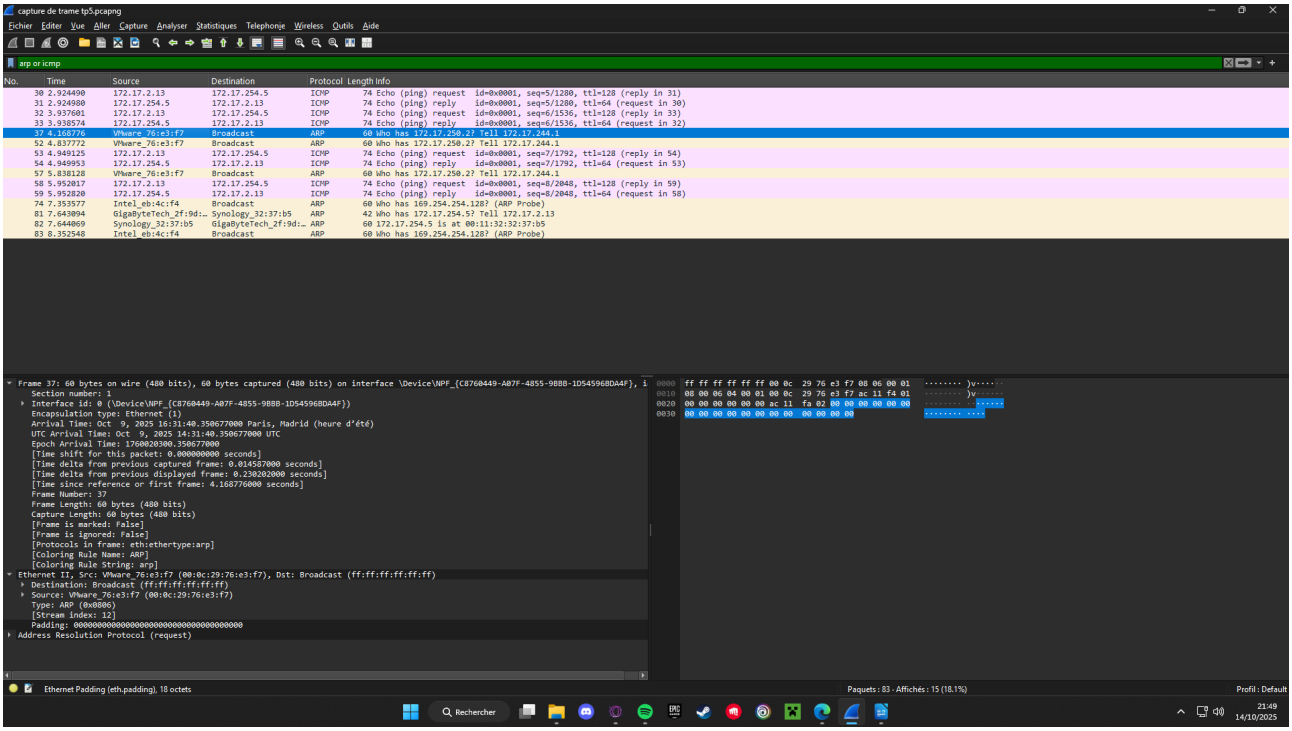
J’ai ping le serveur aviateur (172.17.254.5) et pris une capture de trame en ayant entrer la commande « arp or icmp"



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



J’ai sélectionné une trame 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 de28 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

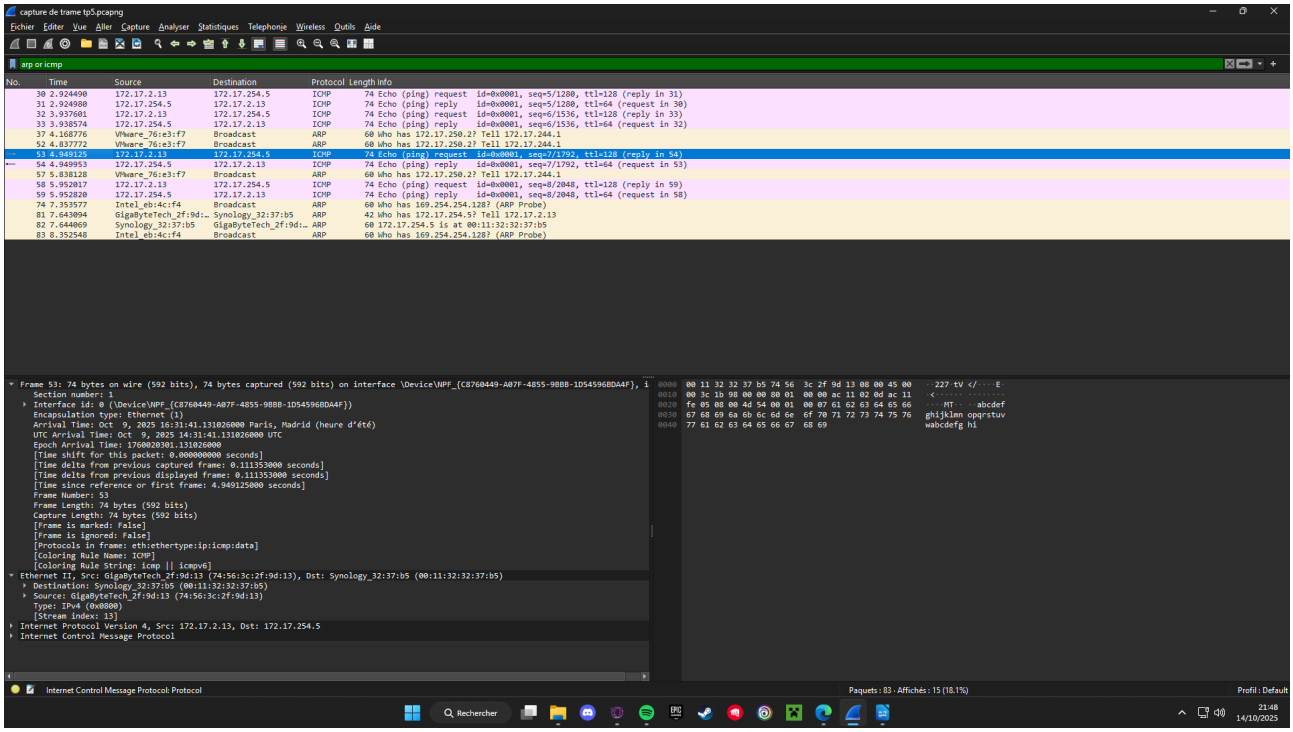
▪Ethernet Type = 0806

▪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 trame ICMP Echo Request pour répondre aux questions:



▪ Sélectionnez une trame ICMP Echo Request. A l’aide du Chapitre 5 (pages 4 et 5), répondez aux questions suivantes : Quelle signification ont les octets de position 0×0C et 0×0D ligne 0000 ?

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

▪Quelle signification a l’octet de position 0×07 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 0×02 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 0×0A, ligne 00020 ?

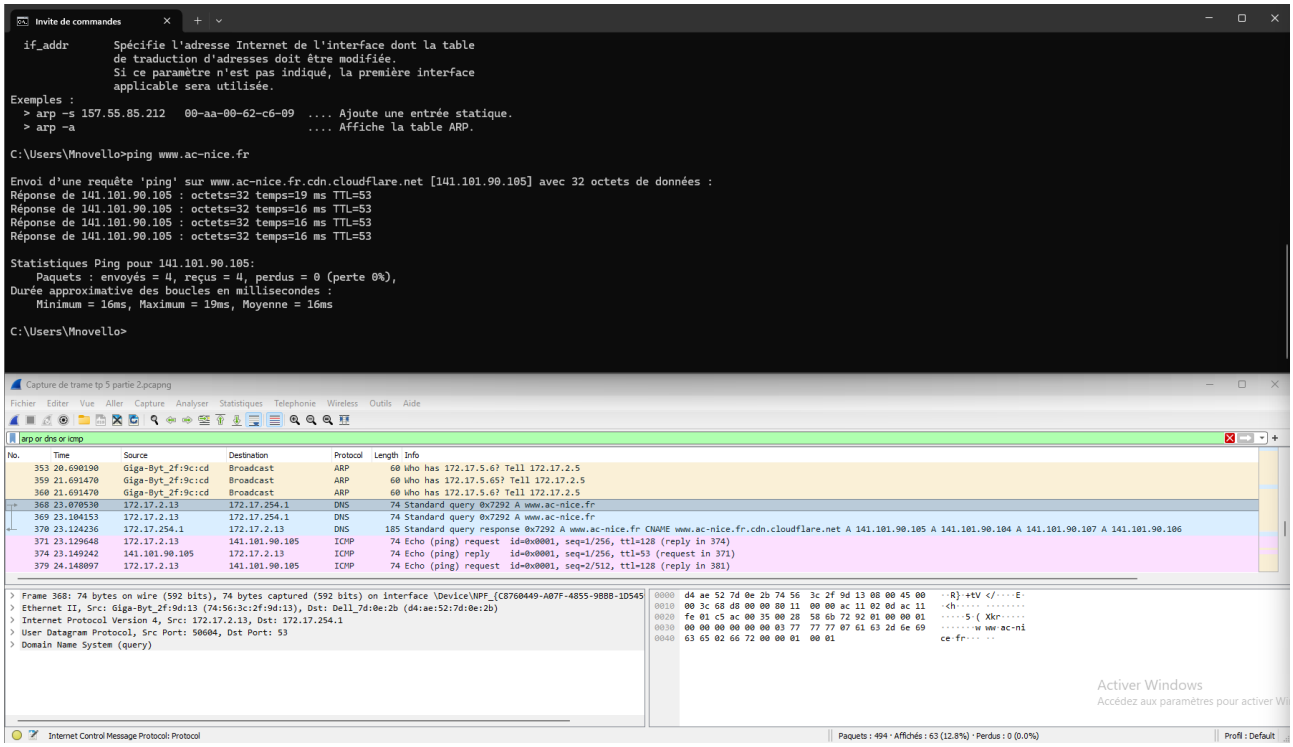
Ce sont les octets ASCII ou l’on trouve toutes les données du message ICMP

▪ Sélectionnez une trame ICMP Echo Reply. Quelle est le nom et la valeur de l’octet de position 0×02 ligne 00020 ?

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

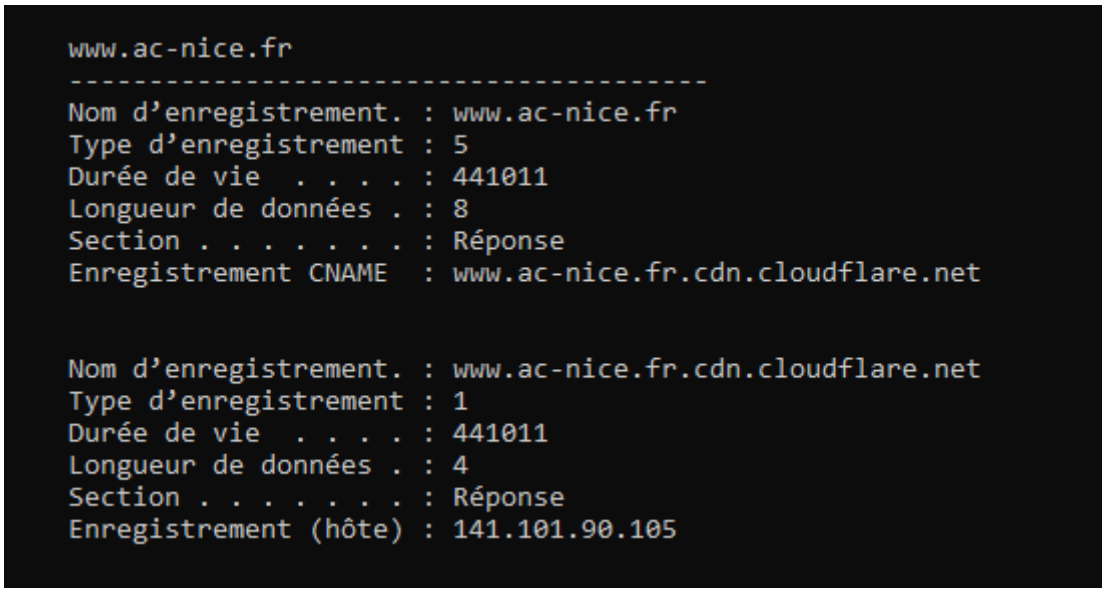
@MAC de la cible = 00:00:00:00:00:00

@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 ?

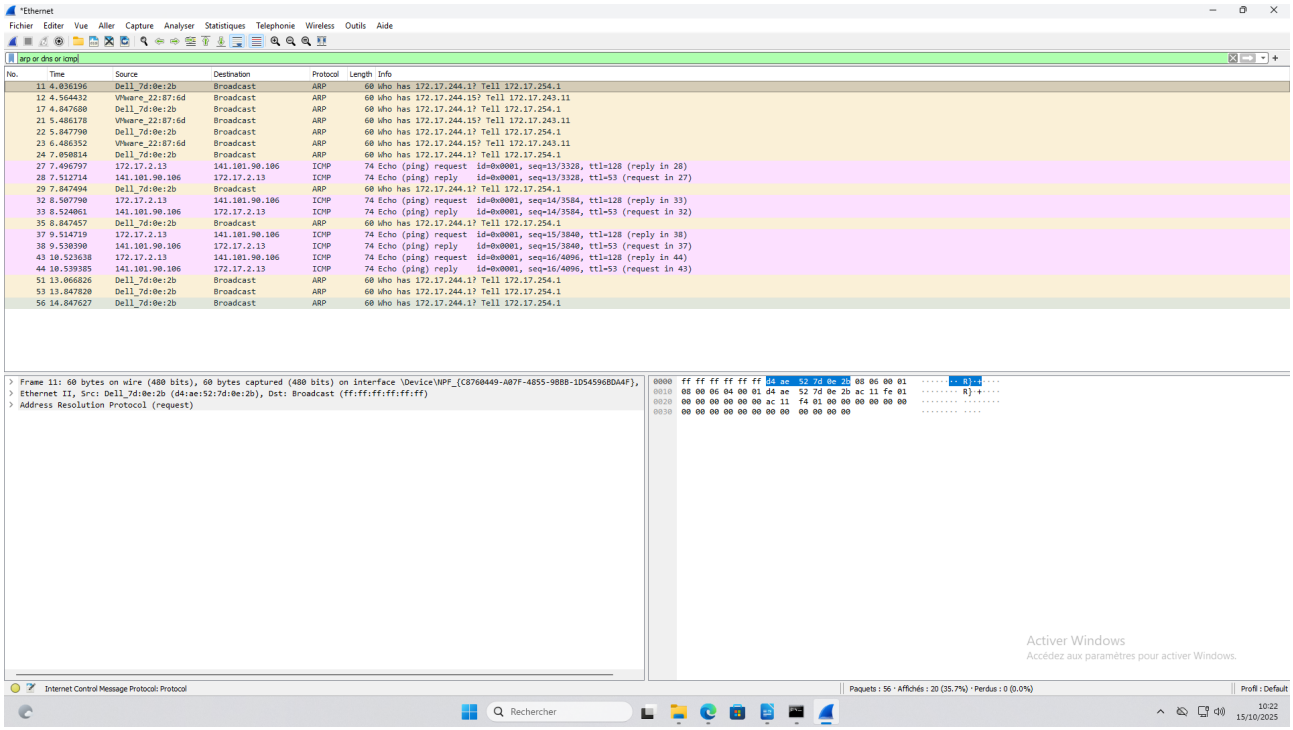
Parce que avant d'envoyer les trames ICMP pour ping la machine doit d'abord savoir vers quelle adresse IP l'envoyer et c'est le rôle du DNS

▪ 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 :

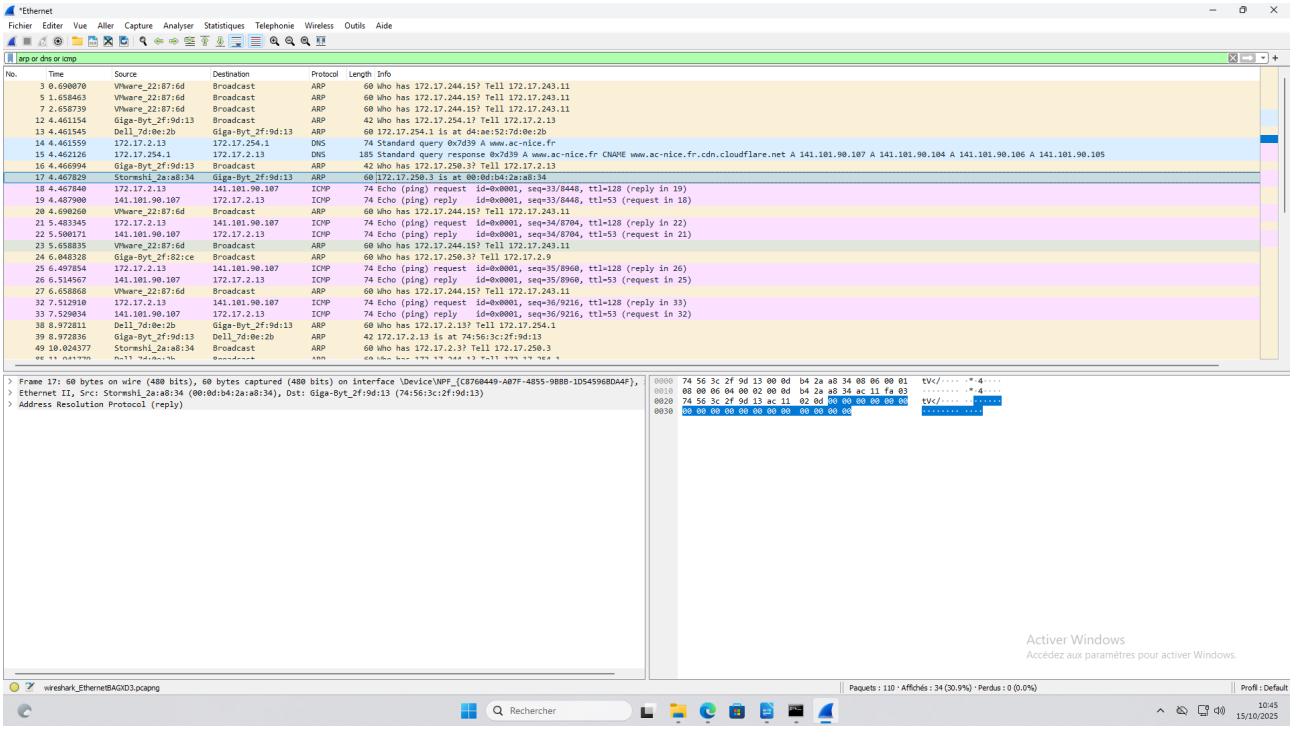


J'ai bien la présence de l'enregistrement DNS ac-nicfe.fr avec l'adresse IP associé qui est 141.101.90.105

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



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 0×0C, 0×0D ligne 0000 et 0×07 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 0×04 et 0×05 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

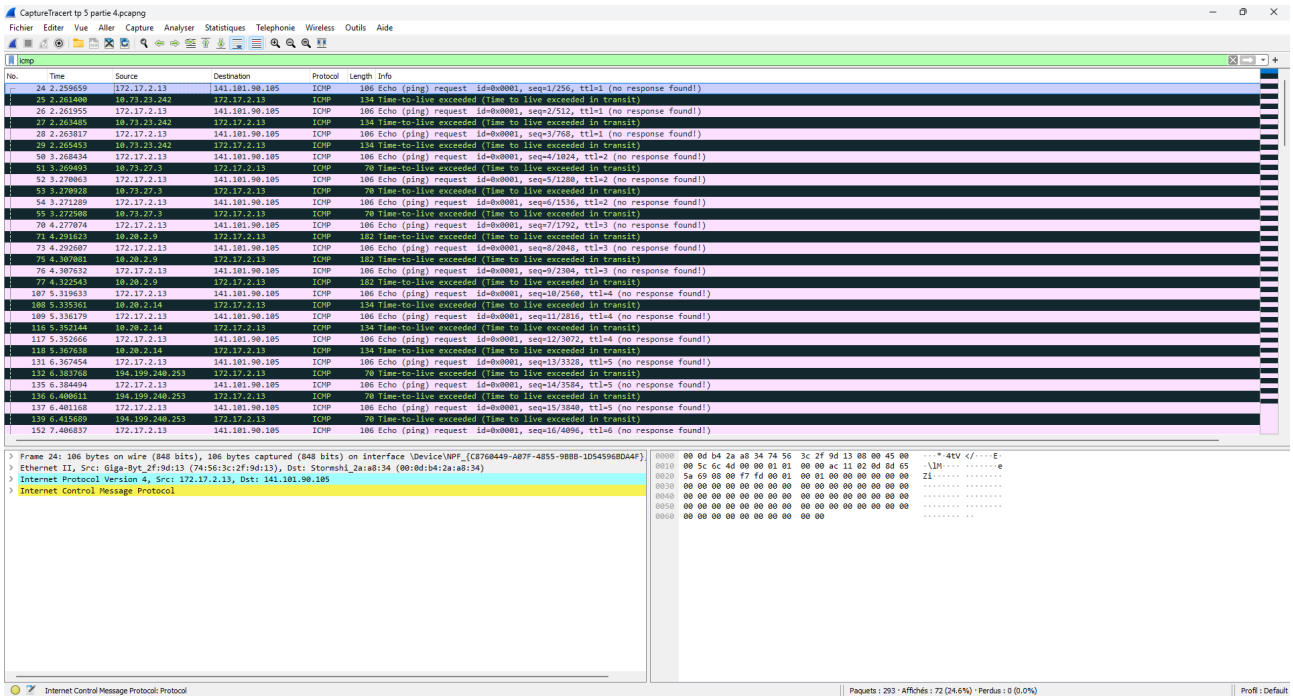
66 72 = fr

▪ 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 héxa