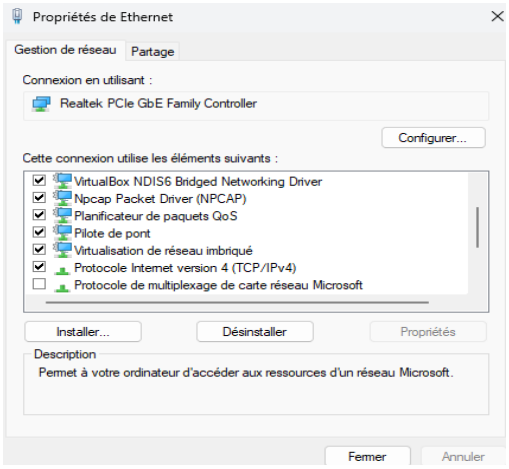
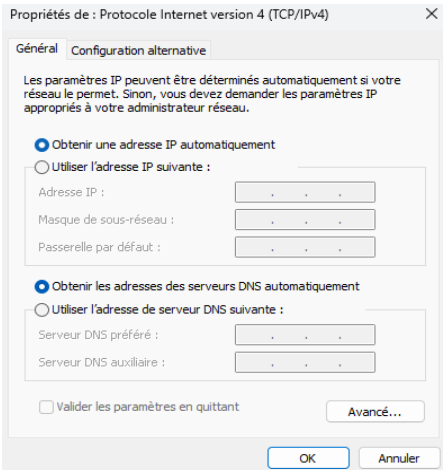
TP4 : analyse de trames DHCP avec Wireshark

Sommaire

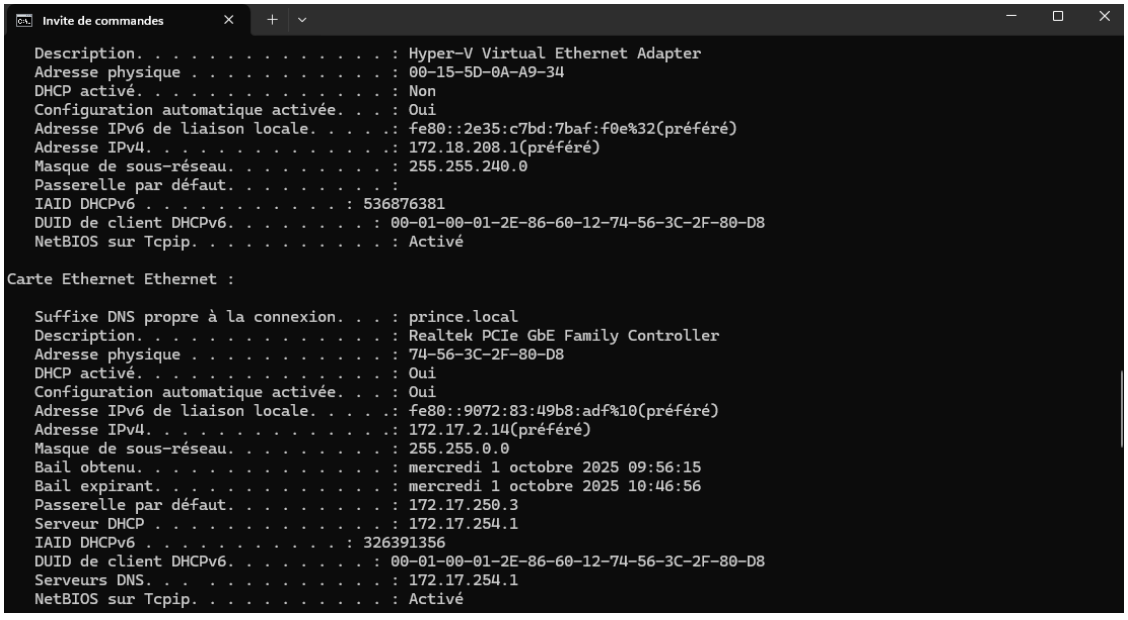
1) Processus d'acquisition d'une adresse IPV4

2) Capture de trames DHCP avec Wireshark





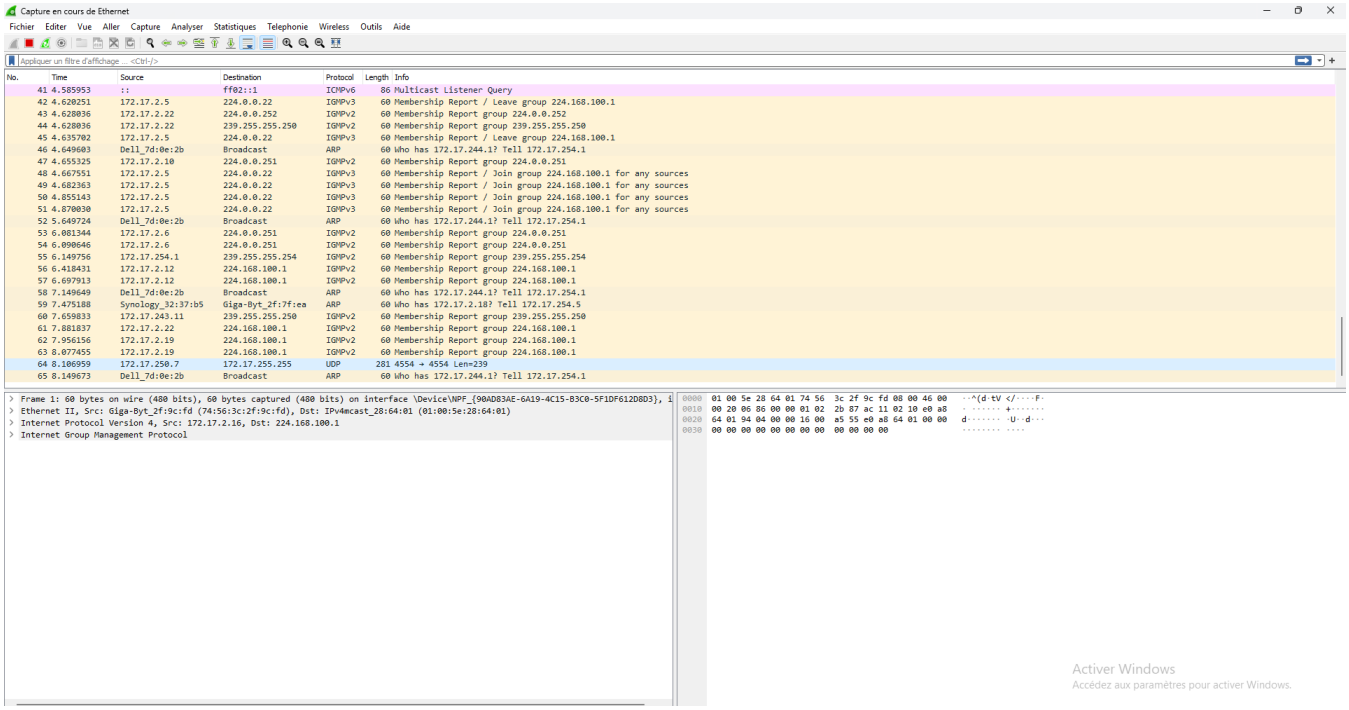
Saisie de ipconfig /all dans l'invite de commandes:



l’adresse IP attribuée par le serveur DHCP « ROI » à mon poste de travail est 172.17.2.14

DHCP activé: Oui
Masque de sous-réseau: 255.255.0.0
Bail obtenu: mercredi 1 octobre 2025 09:56:15
Bail expirant: mercredi 1 octobre 2025 10:46:56
Passerelle par défaut: 172.17.250.3
Serveur DHCP: 172.17.254.1
Serveur DNS: 172.17.254.1

Démarrage d’une capture de trames sur Wireshark:

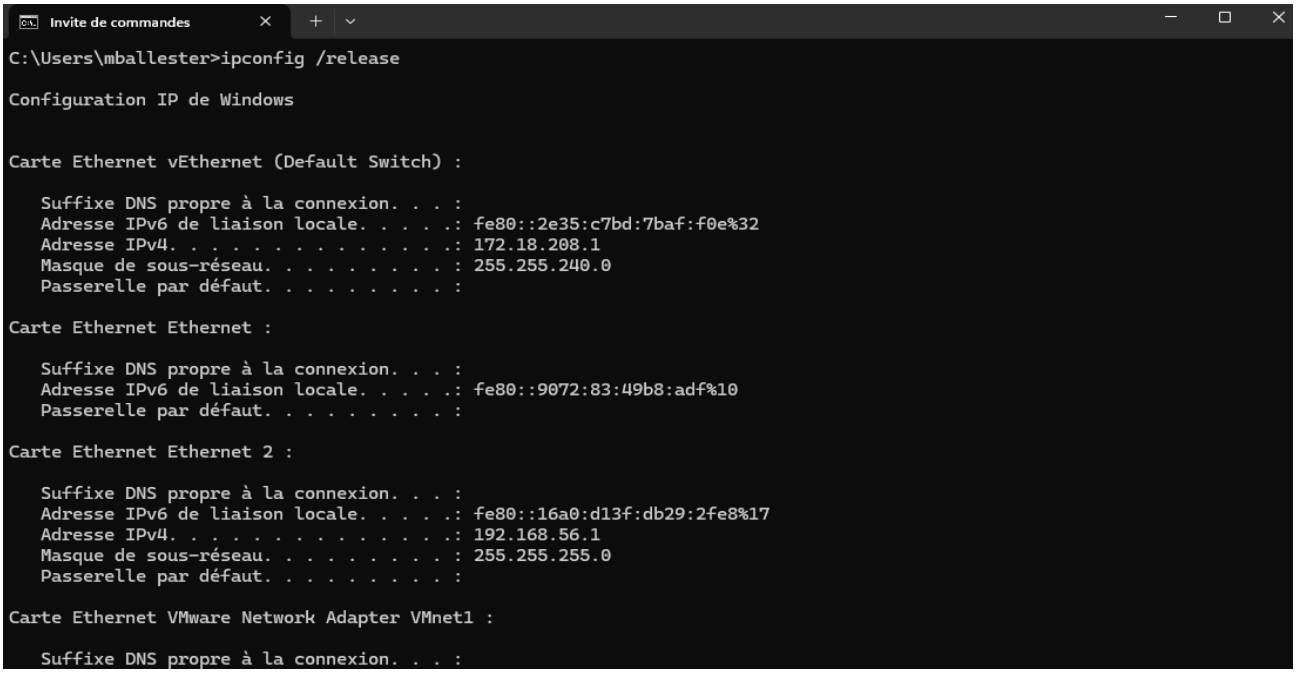


Utilisation des commandes:

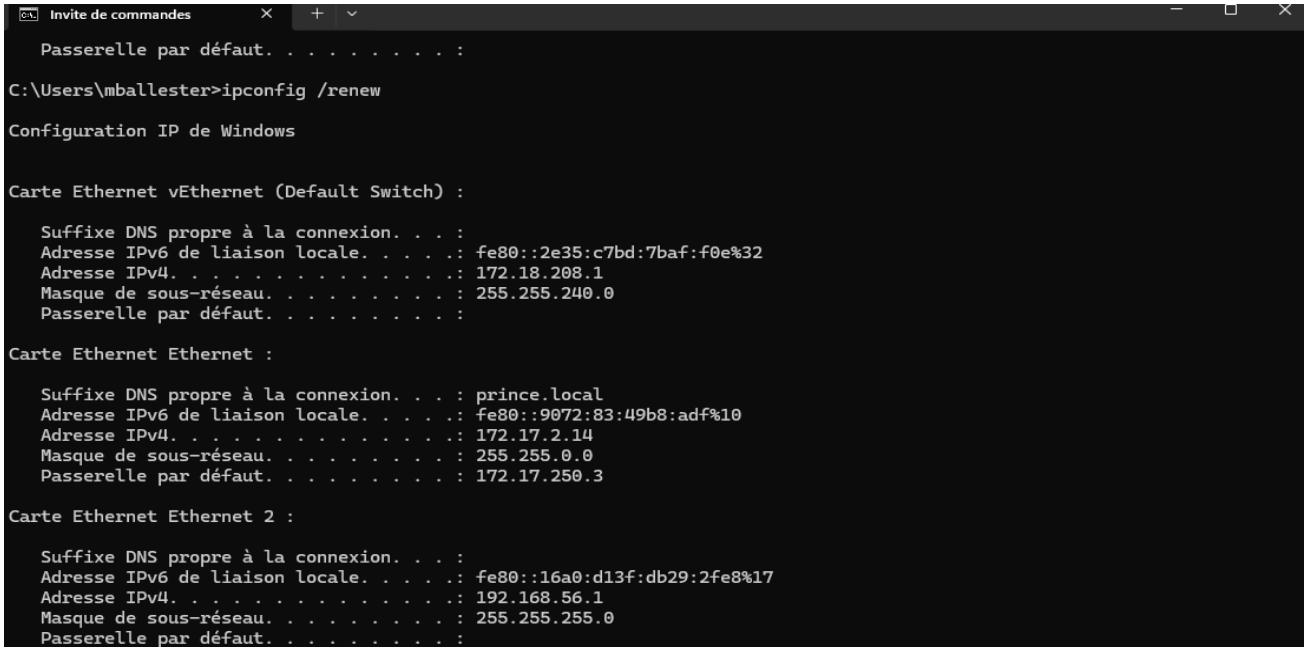
- ipconfig /release (libérations de l’adresse IP)
- ipconfig /renew (renouvellement ou obtention d’un bail)

dans l’invite de commandes

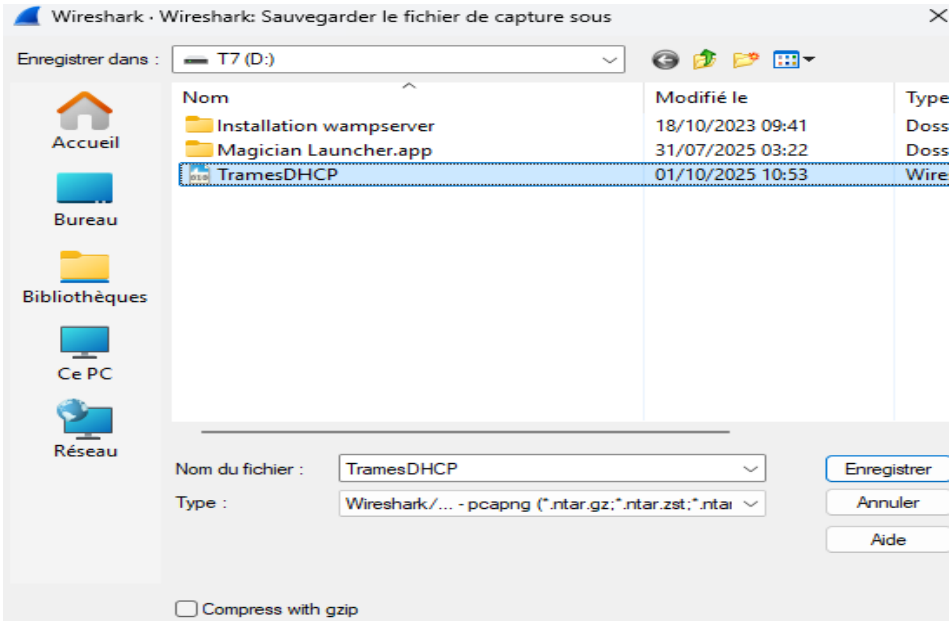
ipconfig /release:



ipconfig /renew:



Enregistrement de la capture de trames dans un fichiers:



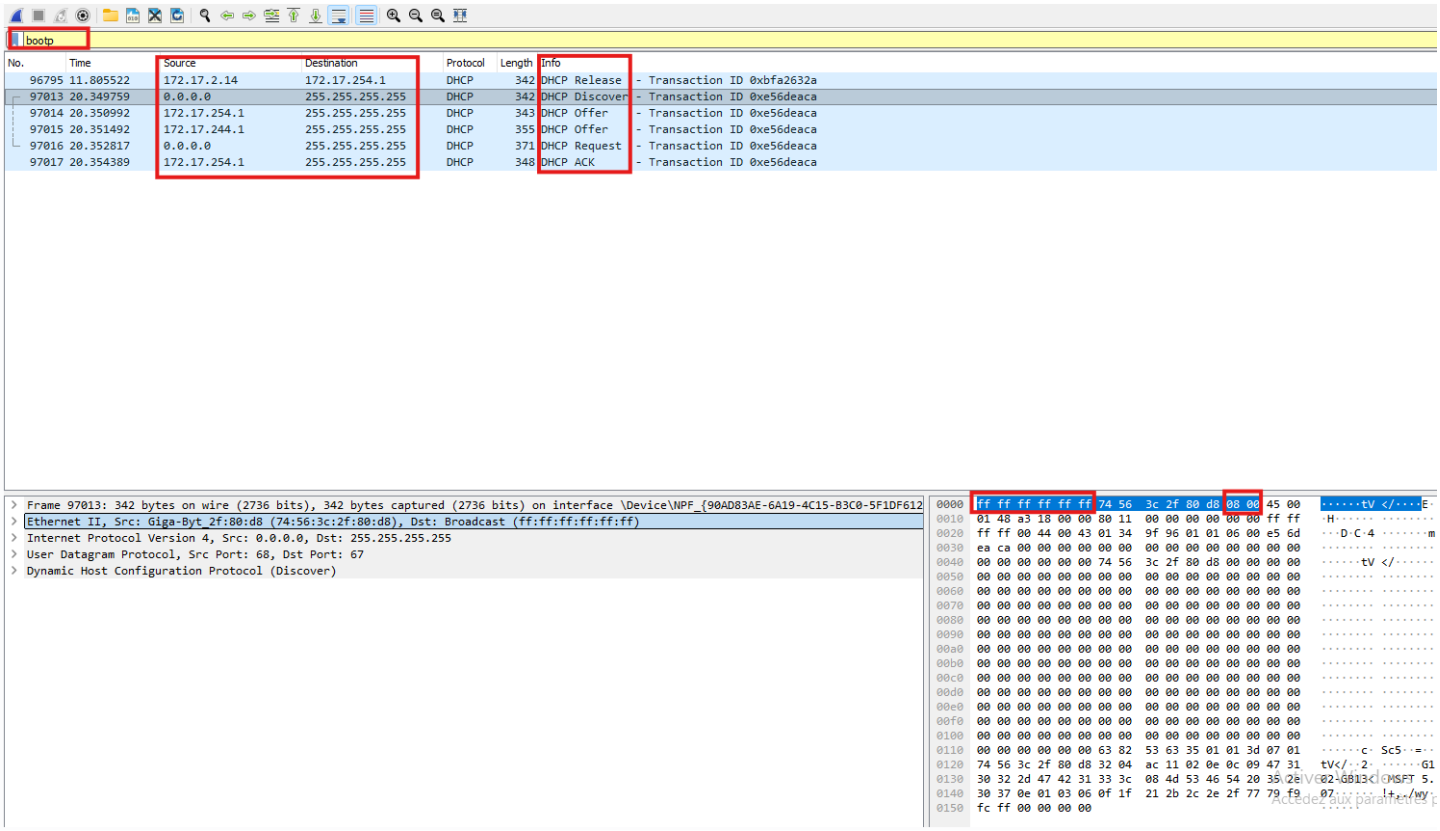
Renseignement grâce a la commande ipconfig /release:
Adresse IPv4:
Masque de sous-réseau:
Passerelle par défaut:

```
Carte Ethernet Ethernet :

   Suffixe DNS propre à la connexion. . . :
   Adresse IPv6 de liaison locale. . . . .: fe80::9072:83:49b8:adf%10
   Passerelle par défaut. . . . . :
```

Renseignement grâce a la commande ipconfig /renew:
Adresse IPv4: 172.17.2.14
Masque de sous-réseau: 255.255.0.0
Passerelle par défaut: 172.17.250.3

```
Carte Ethernet Ethernet :

   Suffixe DNS propre à la connexion. . . : prince.local
   Adresse IPv6 de liaison locale. . . . .: fe80::9072:83:49b8:adf%10
   Adresse IPv4. . . . . . . . . . . . . .: 172.17.2.14
   Masque de sous-réseau. . . . . . . . . : 255.255.0.0
   Passerelle par défaut. . . . . . . . . : 172.17.250.3
```

Limitations de l’affichage des Trames:



3) Etude de la trame DHCP DISCOVER

Adresse MAC Source et Destinations de la Trame DHCP:

- MAC Source: 74-56-3c-2f-80-d8
- MAC Destination: FF-FF-FF-FF-FF-FF

Caractéristique de l’adresse de couche 2 de destination de cette trame :

- C’est une Adresse envoyer en Broadcast

Quel est le champ qui suit immédiatement les deux adresses MAC ?:

- C’est le champ Ethertype qui suis immédiatement les deux adresses MAC

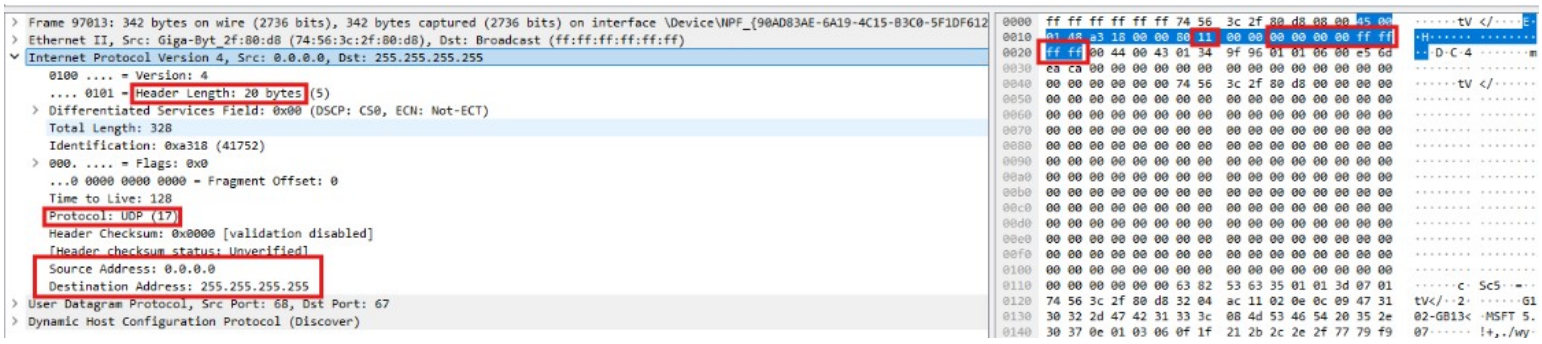
Quelle valeur contient-il ? Que signifie t-elle :

- Il contient la valeur 0800 ce qui signifie que derrière il va y avoir un paquet IP

Quels sont les protocoles inclus dans cette trame ?:

- Il y a le protocole IP
- le protocole UDP
- et le protocole DHCP

Sélection de l’en tête IP de la Trame DHCP:



Quel est le champ de l’en-tête IP permettant de connaître le protocole de transport des messages DHCP ? Préciser la valeur de ce champ ainsi que le nom du protocole:

- Il s’agit du champ protocole, la valeur de ce champ ici est de 11(17 en hexa) il s’agit donc du protocole UDP

Renseignez ci-dessous les champs d’en-tête IP suivants :
Version = 4
I**HL (val. déci. et hexa.)** = 20 octets (5 decimal, 0x05 hexadecimal)
Protocole (val. déci. et hexa.) = UDP (11 decimal, 17 hexadecimal)
Source adresses (val. déci. et hexa.) = 0.0.0.0 en décimal et 00.00.00.00 en hexadécimal
Destination adresses (val. déci. et hexa.) = 255.255.255.255 en décimal FF-FF-FF-FF en hexadécimal

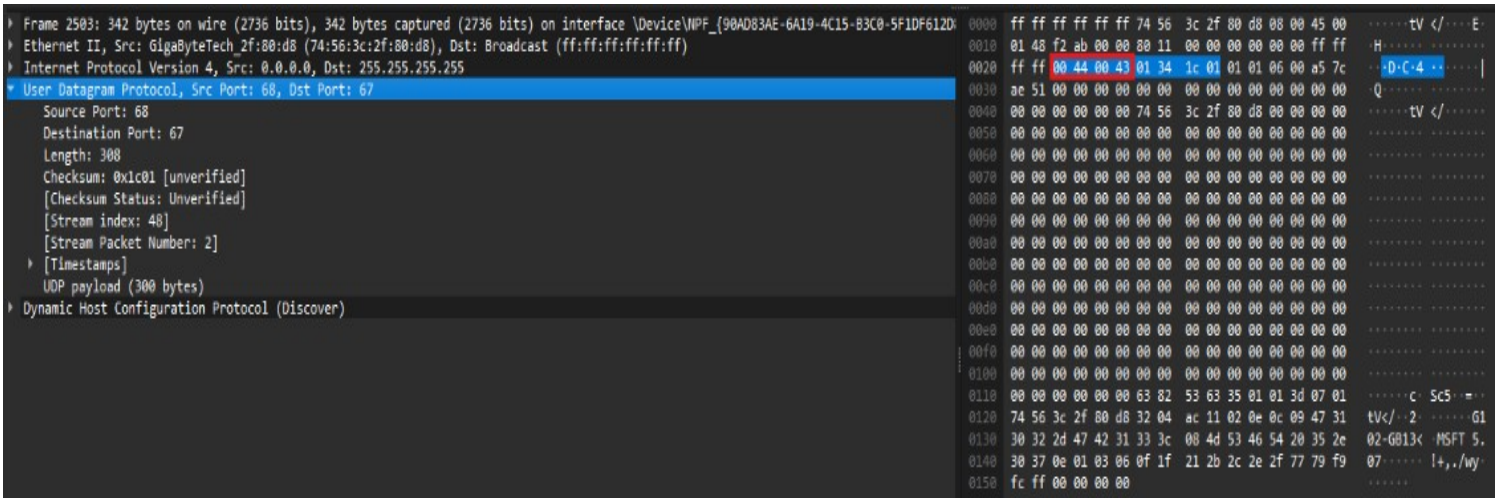
Que signifie la valeur contenue dans le champ adresse IP source ?:

- La valeur 0.0.0.0 qui est contenu dans le champ adresse IP source signifie que la machine qui envoie la Trame n’a pas encore d’adresse IP attribuer il chercher donc a en obtenir une via une trame DHCP

Caractérisez l’adresse de couche 3 de destination de cette trame :

- Elle est en broadcast, elle envoie donc la trame a toute les machines du reseaux

Sélection de l’en tête du datagram UDP de la Trame DHCP:



Quel est le nom du champ de l’en-tête de transport permettant le démultiplexage de protocole ?:

- C’est le champ Port qui permet le démultiplexage de protocole

Quel est le port UDP utilisé par le client DHCP ? Identifier la valeur hexadécimale correspondante figurant dans le volet des octets (octets de position 0×02 et 0×03 ligne 0020):

- Le port utilisé part le client DHCP est le port 68

- La valeur en hexadécimal du port 68 est 00 44

Quel est le protocole applicatif encapsulé dans le datagramme UDP ?:

- Le protocole applicatif encapsulé dans le datagramme UDP est DHCP

Quel est le port UDP utilisé par le serveur DHCP pour écouter et recevoir la requête du client ? Identifier la valeur hexadécimale correspondante figurant dans le volet des octets:

- Le port UDP utilisé par le serveur DHCP est le port 67
- La valeur du port 67 en hexadécimal est 00 43

Sélection de la section Bootstrap Protocol ou Dynamic Host Configuration Protocol (Discover) de la trame DHCP Discover :