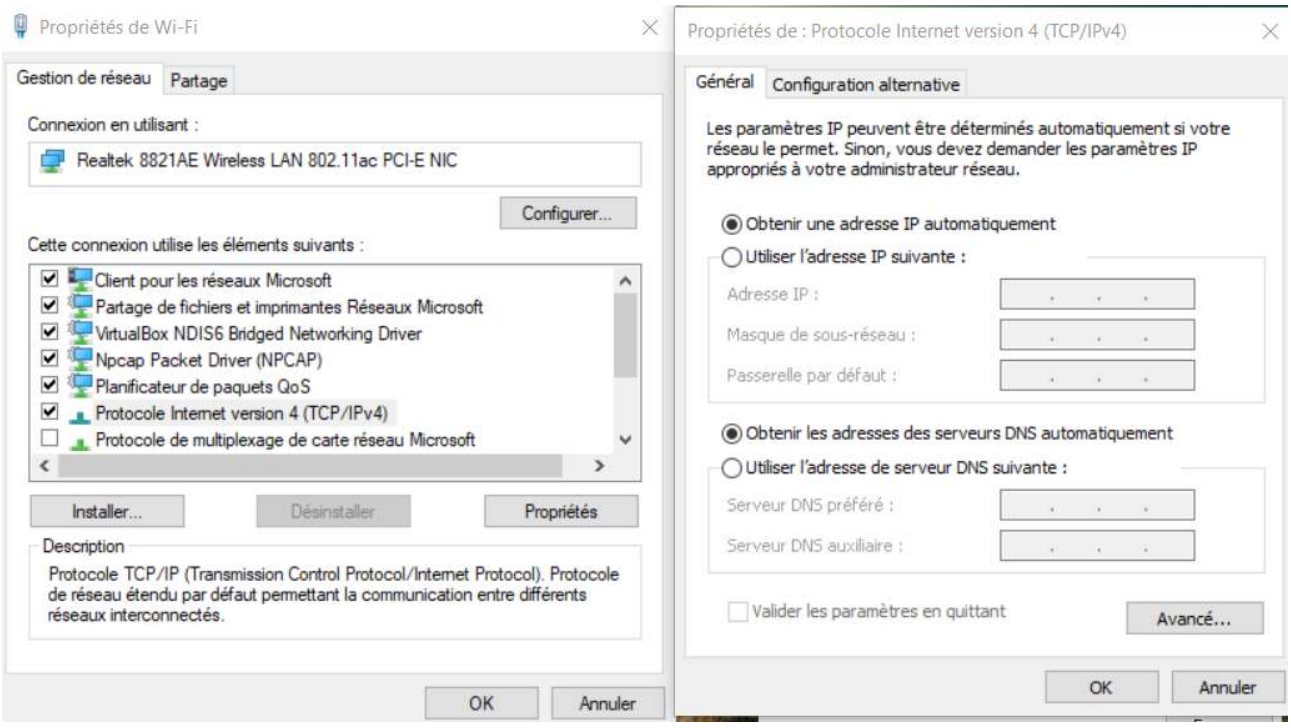
TD4 : analyse de trames DHCP avec Wireshark

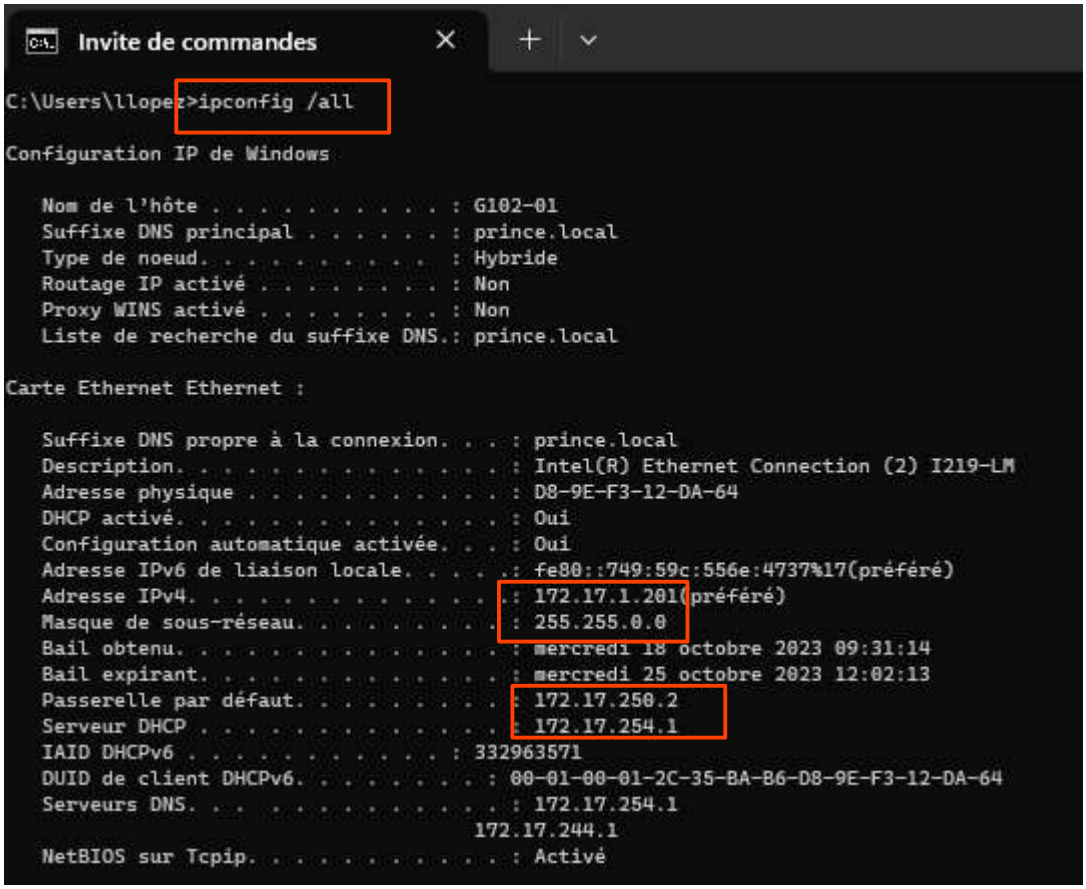
Sommaire

1. Capture de trames DHCP avec Wireshark

On doit affiche les connexions réseau et on fait clique droit sur la carte réseau puis sélectionner Propriétés



Sur l'invite de commande, on saisit la commande « ipconfig /all » :



Quelle est l'adresse IP attribuée par le serveur DHCP « ROI » à votre poste de travail ?

C'est 172.17.1.201

▪ **Renseignez les autres éléments ci-dessous :**

DHCP activé : Oui

Masque de sous-réseau:255.255.0.0

Bail obtenu : Mercredi 18 octobre 2023 à 9h31min et 14 secondes

Bail expirant : Mercredi 25 octobre 2023 à 12h02min et 13 secondes

Passerelle par défaut : 172.17.250.2

Serveur DHCP : 172.17.254.1

Serveur DNS : 172.17.254.1

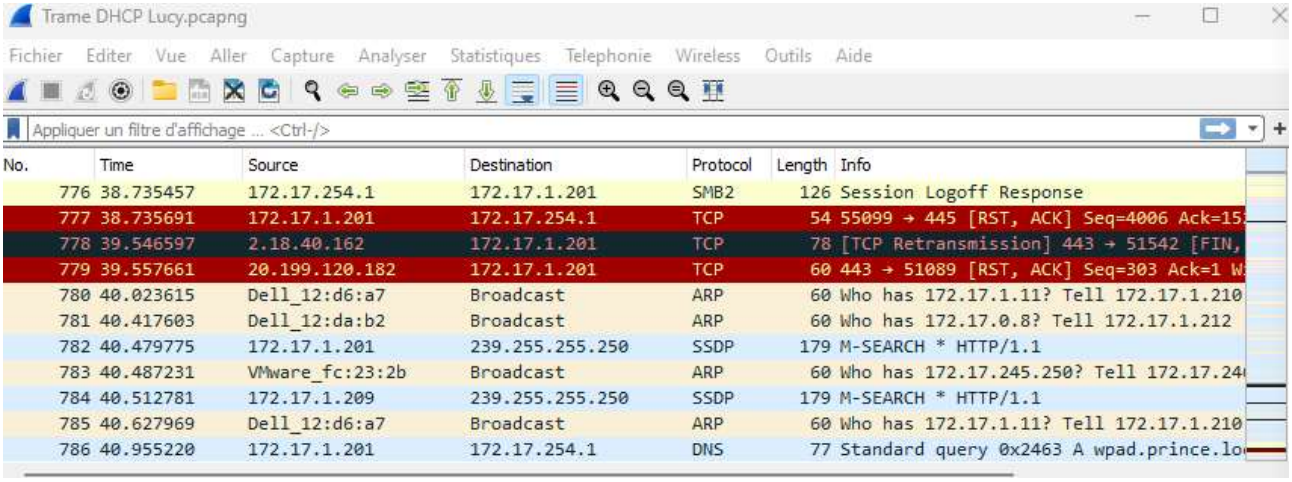
Alors que la commande ipconfig ne renvoie que les informations suivantes :

```
Carte Ethernet Ethernet :

   Suffixe DNS propre à la connexion. . . : prince.local
   Adresse IPv6 de liaison locale. . . . .: fe80::749:59c:556e:4737%17
   Adresse IPv4. . . . . . . . . . . . . .: 172.17.1.201
   Masque de sous-réseau. . . . . . . . . : 255.255.0.0
   Passerelle par défaut. . . . . . . . . : 172.17.250.2

Carte Ethernet Ethernet 2 :
```

Ensuite, on démarre une une capture de trame avec Wireshark sur l'invite de commande avec les commandes :**ipconfig /release** et **ipconfig /renew**



▪ A partir des renseignements obtenus à l'aide de la commande **ipconfig /release**, renseignez les éléments ci-dessous :

Adresse IPv4 :0.0.0.0

Masque de sous-réseau : 0.0.0.0

Passerelle par défaut :Aucune passerelle

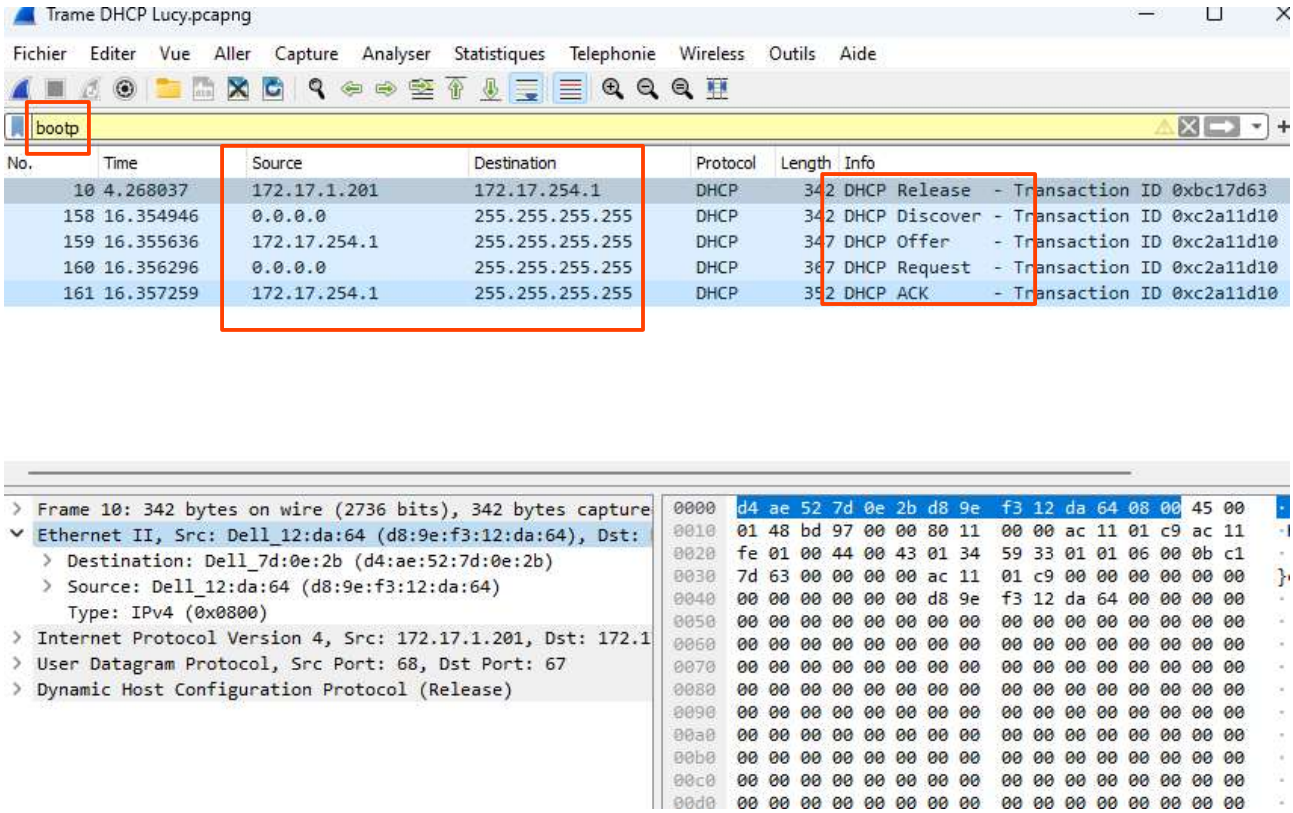
▪ A partir des renseignements obtenus à l'aide de la commande **ipconfig /renew**, renseignez les éléments ci-dessous :

Adresse IPv4 : 172.17.1.201

Masque de sous-réseau : 255.255.0.0

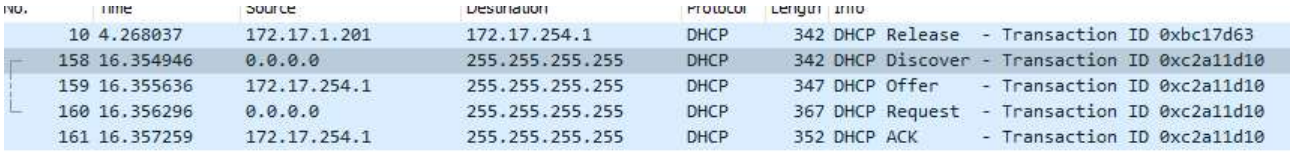
Passerelle par défaut : 172.17.250.2

Sur Wireshark, on limite l'affichage des trames à celles encapsulant les protocoles DHCP (zone Filter), comme DHCP est une extension du protocole BOOTP, dans la zone filtrer, on tappe BOOTP : (Voir la trame « Trame DHCP Lucy »)

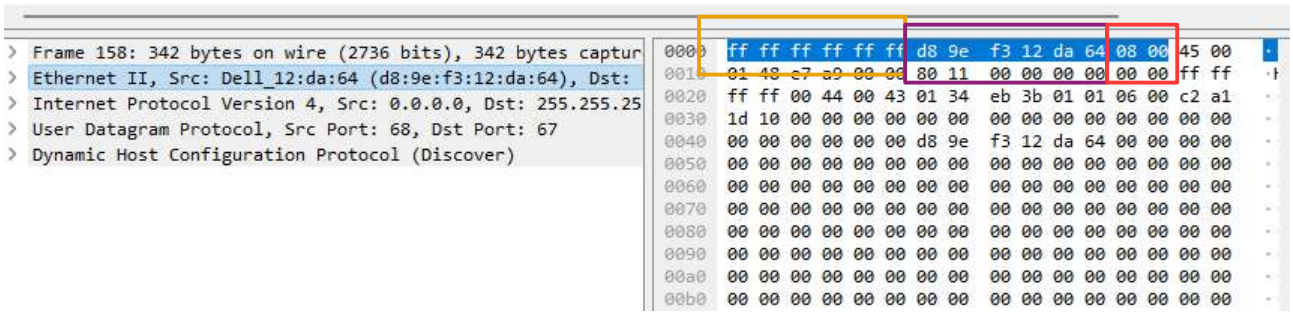


2. Etude de la trame DHCP DISCOVER.

▪ Sélectionnez, comme dans la figure ci-dessus, la section Ethernet (en-tête de trame) de la trame DHCPDISCOVER et identifiez les adresses MAC source et destination dans le volet des octets :



No.	Time	Source	Destination	Protocol	Length	Info
10	4.268037	172.17.1.201	172.17.254.1	DHCP	342	DHCP Release - Transaction ID 0xbc17d63
158	16.354946	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0xc2a11d10
159	16.355636	172.17.254.1	255.255.255.255	DHCP	347	DHCP Offer - Transaction ID 0xc2a11d10
160	16.356296	0.0.0.0	255.255.255.255	DHCP	367	DHCP Request - Transaction ID 0xc2a11d10
161	16.357259	172.17.254.1	255.255.255.255	DHCP	352	DHCP ACK - Transaction ID 0xc2a11d10



```
> Frame 158: 342 bytes on wire (2736 bits), 342 bytes captur
> Ethernet II, Src: Dell_12:da:64 (d8:9e:f3:12:da:64), Dst:
> Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.255.25
> User Datagram Protocol, Src Port: 68, Dst Port: 67
> Dynamic Host Configuration Protocol (Discover)
```

```
0000  ff ff ff ff ff ff d8 9e  f3 12 da 64 08 00 45 00
0010  01 48 c7 a9 00 00 80 11  00 00 00 00 00 00 ff ff
0020  ff ff 00 44 00 43 01 34  eb 3b 01 01 06 00 c2 a1
0030  1d 10 00 00 00 00 00 00  00 00 00 00 00 00 00 00
0040  00 00 00 00 00 00 d8 9e  f3 12 da 64 00 00 00 00
0050  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
0060  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
0070  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
0080  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
0090  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00a0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00b0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
```

L’adresse mac destination est FF:FF:FF:FF:FF:FF et l’adresse source est d8 9e f3 12 da 64

▪ Caractérisez l’adresse de couche 2 de destination de cette trame :

L’adresse de destination de couche 2 est une adresse de Broadcast (en couche 2 = FF:FF:FF:FF:FF:FF)

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

Le champs qui suis les deux adresses mac est le Champ Ethertype

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

La valeur est 0800 cela signifie que le protocole de la couche 3 est le protocole IPv4

▪ Quels sont les protocoles inclus dans cette trame ?

Les protocoles sont :

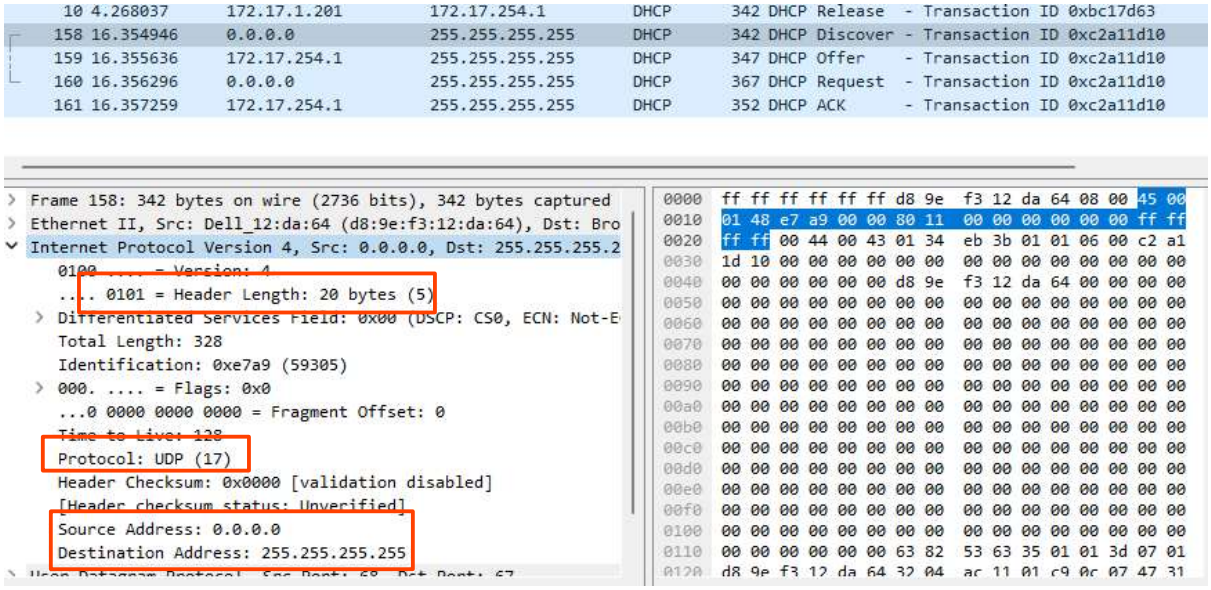
-Dans la couche réseau (couche 2) c’est le protocole Ethernet

-Dans la couche internet (couche 3) c’est le protocole IPv4

-Dans la couche transport (couche 4) C’est le protocole UDP

-Dans la couche application (couche 5,6,7), c’est le protocole DHCP .

Puis on sélectionne, l'en-tête IP contenu dans la trame DHCP Discover :



▪ 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.

▪ Renseignez ci-dessous les champs d'en-tête IP suivants :

Version = IPv4 donc c'est version 4

IHL (val. déci. et hexa.) = 20 bytes (en hexadécimal 5) et 5 en décimal

Protocole (val. déci. et hexa.) = 17 (en hexadécimal 11)

Source address (val. déci. et hexa.) = 0.0.0.0 (en héxadécimal 0.0.0.0)

Destination address (val. déci. et hexa.) = 255.255.255.255 (en héxadécimal FF:FF:FF:FF)

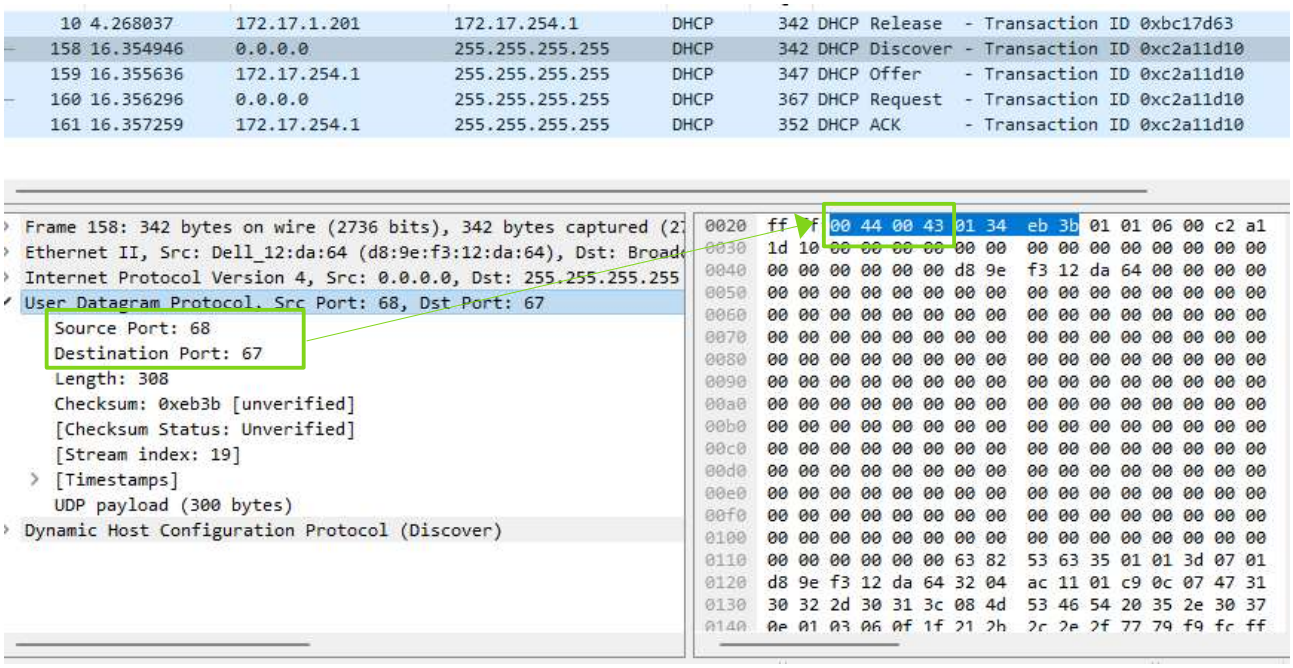
▪ Que signifie la valeur contenue dans le champ adresse IP source ?

Cela veut dire que la machine source n'a pas adresse IP

▪ Caractérisez l'adresse de couche 3 de destination de cette trame :

L’adresse de destination est 255.255.255.255 donc c’est une adresse de broadcast (en hexadécimal FF:FF:FF:FF)

Troisièmement, on sélectionne, l’en-tête du datagramme UDP contenu dans la trame DHCP Discover.



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

Le champ port est le nom du champ permettant le démultiplexage de protocole (ici c’est les 4 1er octets (port source et port destination)

▪ 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 UDP utilisé par le client est le 00 44 = 68 donc DHCP

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

C’est en hexadécimal 00 44 et 00 43 ce qui correspond en décimal 67/68 qui est le protocole applicatif 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 est 00 43 = 67

Pour finir, on sélectionne la section Bootstrap Protocol contenu dans la trame DHCP Discover :