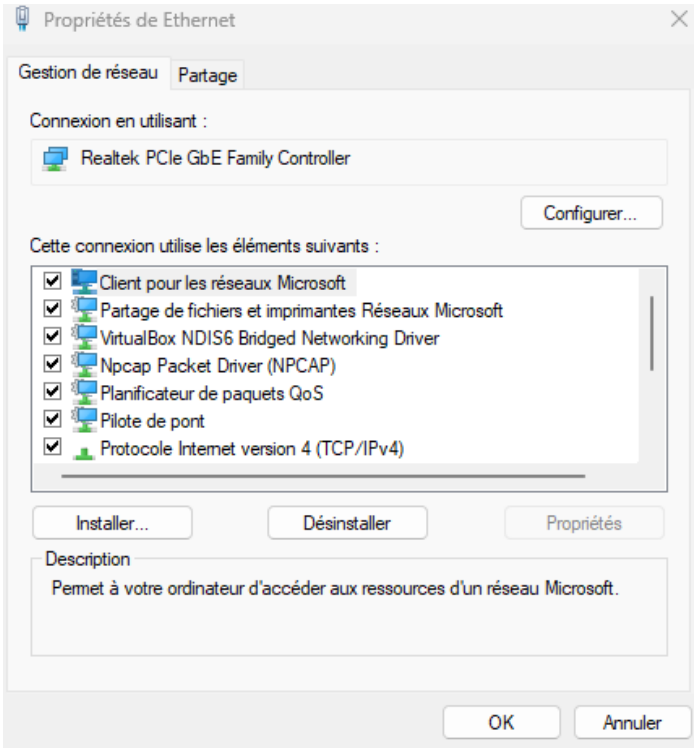
TP4 : analyse de trames DHCP avec Wireshark

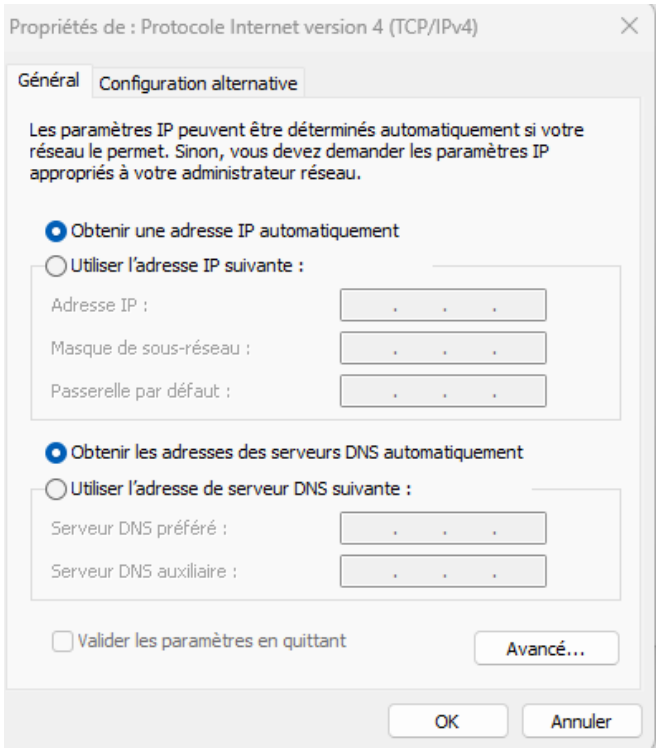
1. Processus d’acquisition d’une adresse IPv4

2. Capture de trames DHCP avec Wireshark.

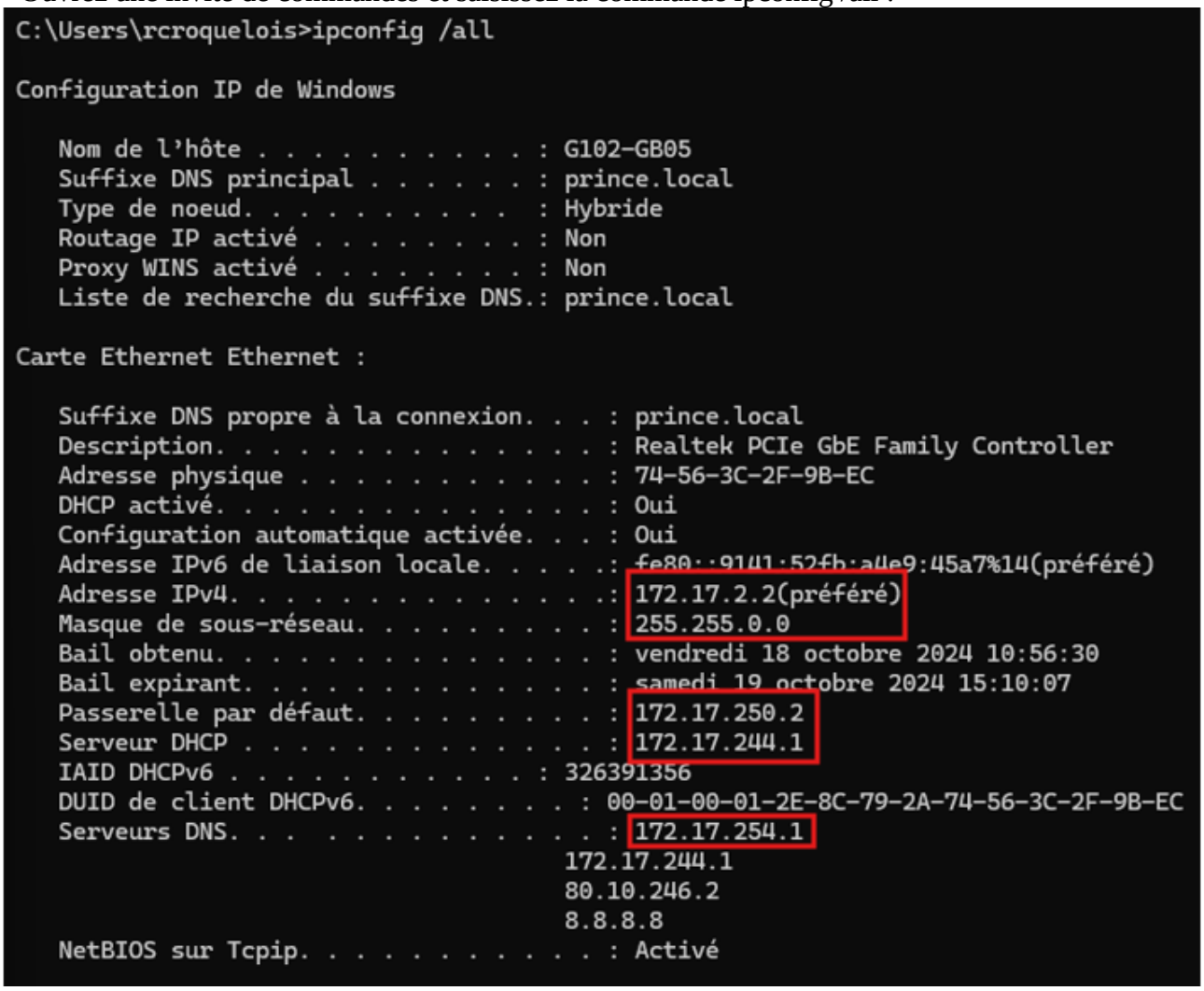
▪ Les propriétés TCP/IPv4 de votre machine physique doivent être définies de manière à obtenir automatiquement les paramètres IP (adresse IP, masque de sous-réseau, passerelle ainsi que l’adresse du serveur DNS) auprès du serveur DHCP ROI :

Afficher les connexions réseau et cliquer droit sur la carte réseau puis sélectionner Propriétés :





▪ Ouvrez une invite de commandes et saisissez la commande ipconfig /all :



Quelle est l'adresse IP attribuée par le serveur DHCP « ROI » à votre poste de travail ?
172.17.2.2

▪ Renseignez les autres éléments ci-dessous :

DHCP activé : oui

Masque de sous-réseau : 255.255.0.0

Bail obtenu : vendredi 18 octobre 2024 10 :56 :30

Bail expirant : samedi 19 octobre 2024 15 :10 :07

Passerelle par défaut : 172.17.250.2

Serveur DHCP : 172.17.244.1

Serveur DNS : 172.17.254.1 / 172.17.244.1 / 80.10.246.2 / 8.8.8.8

A titre de comparaison, la commande ipconfig ne renvoie que les informations suivantes :

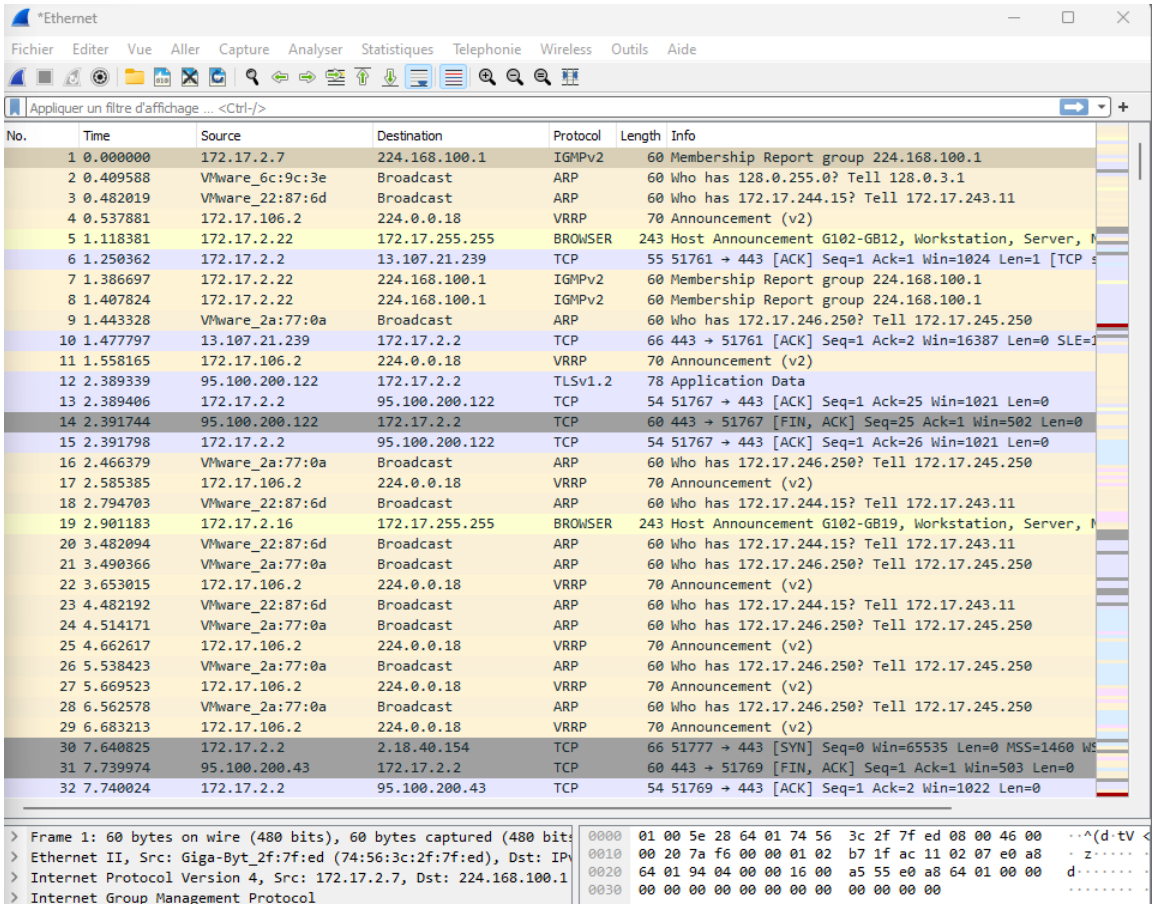
```
C:\Users\rcroquelois>ipconfig

Configuration IP de Windows


Carte Ethernet Ethernet :

   Suffixe DNS propre à la connexion. . . : prince.local
   Adresse IPv6 de liaison locale. . . . .: fe80::9141:52fb:a4e9:45a7%14
   Adresse IPv4. . . . . . . . . . . . . .: 172.17.2.2
   Masque de sous-réseau. . . . . . . . . : 255.255.0.0
   Passerelle par défaut. . . . . . . . . : 172.17.250.2
```

▪ Démarrez une capture de trames à l'aide de Wireshark



▪ Vous allez générer un peu de trafic entre votre poste de travail et le serveur « Roi ». Ouvrez une invite de commandes et tapez successivement les commandes : - ipconfig /release - ipconfig /renew

```
C:\Users\rcroquelois>ipconfig /release

Configuration IP de Windows


Carte Ethernet Ethernet :

   Suffixe DNS propre à la connexion. . . :
   Adresse IPv6 de liaison locale. . . . .: fe80::9141:52fb:a4e9:45a7%14
   Passerelle par défaut. . . . . :

Carte Ethernet Ethernet 2 :

   Suffixe DNS propre à la connexion. . . :
   Adresse IPv6 de liaison locale. . . . .: fe80::507e:75c4:c3b6:eaa9%16
   Adresse IPv4. . . . . . . . . . . . . .: 192.168.56.1
   Masque de sous-réseau. . . . . : 255.255.255.0
   Passerelle par défaut. . . . . :

Carte Ethernet vEthernet (Default Switch) :

   Suffixe DNS propre à la connexion. . . :
   Adresse IPv6 de liaison locale. . . . .: fe80::f17d:fb8f:bdf3:628f%18
   Adresse IPv4. . . . . . . . . . . . . .: 172.23.48.1
   Masque de sous-réseau. . . . . : 255.255.240.0
   Passerelle par défaut. . . . . :

C:\Users\rcroquelois>
```

```
C:\Users\rcroquelois>ipconfig /renew

Configuration IP de Windows


Carte Ethernet vEthernet (Default Switch) :

   Suffixe DNS propre à la connexion. . . :
   Adresse IPv6 de liaison locale. . . . .: fe80::f17d:fb8f:bdf3:628f%18
   Adresse IPv4. . . . . . . . . . . . . .: 172.23.48.1
   Masque de sous-réseau. . . . . : 255.255.240.0
   Passerelle par défaut. . . . . :

Carte Ethernet Ethernet :

   Suffixe DNS propre à la connexion. . . : prince.local
   Adresse IPv6 de liaison locale. . . . .: fe80::9141:52fb:a4e9:45a7%14
   Adresse IPv4. . . . . . . . . . . . . .: 172.17.2.2
   Masque de sous-réseau. . . . . : 255.255.0.0
   Passerelle par défaut. . . . . : 172.17.250.2

Carte Ethernet Ethernet 2 :

   Suffixe DNS propre à la connexion. . . :
   Adresse IPv6 de liaison locale. . . . .: fe80::507e:75c4:c3b6:eaa9%16
   Adresse IPv4. . . . . . . . . . . . . .: 192.168.56.1
   Masque de sous-réseau. . . . . : 255.255.255.0
   Passerelle par défaut. . . . . :
```

▪ Ne fermez pas l’invite de commandes, revenez à la fenêtre de Wireshark et cliquez sur le bouton Arrêt de la capture et enregistrez les informations capturées dans un fichier nommez « TramesDHCP » :

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

Adresse IPv4 : 172.23.48.1

Masque de sous-réseau : 255.255.255.0

Passerelle par défaut : vide

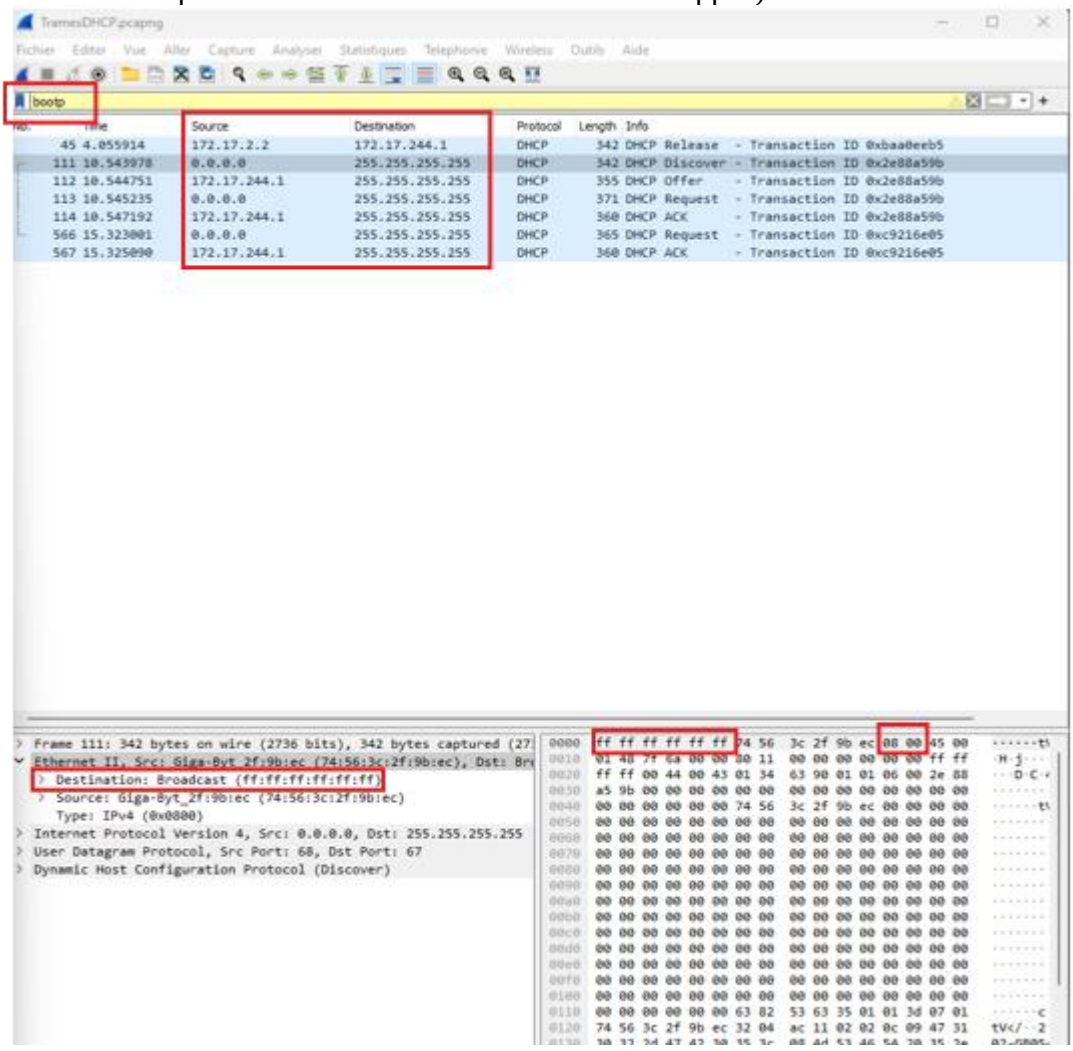
▪ A partir des renseignements obtenus à l'aide de la commande ipconfig /renew, renseignez les éléments ci-dessous :

Adresse IPv4 : 172.17.2.2

Masque de sous-réseau : 255.255.0.0

Passerelle par défaut : 172.17.250.2

▪ Limitez l'affichage des trames à celles encapsulant les protocoles DHCP (zone Filter). Rappelezvous que le protocole DHCP est une extension du protocole BOOTP (Bootstrap protocole). A l'exception des adresses physiques et logiques, la fenêtre de capture obtenue devrait ressembler à celle figurant ci-après (la trame 506 DHCP DISCOVER a ici été sélectionnée et la section correspondant à l'en-tête Ethernet a été développée) :



3. 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 :

Adresse MAC source : 74 : 56 : 3c : 2f : 9b : ec

Adresse MAC destination : ff : ff : ff : ff : ff : ff

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

L'adresse de la couche 2 est une adresse broadcast, elle est donc inconnue.

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

On peut voir que c'est le champ IPv4 (0800).

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

Ceci est la valeur 0800 ce qui signifie que nous sommes sous IPv4

▪ Quels sont les protocoles inclus dans cette trame ?

Nous avons les protocoles :

-Ethernet

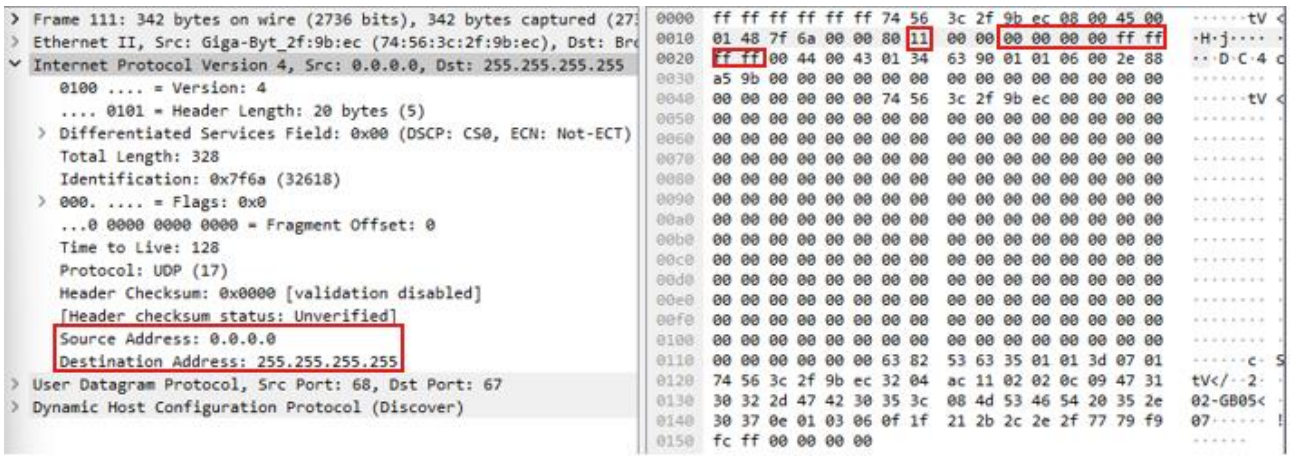
-Réseau IP

-Transport UDP

-BOOTP

-Et DHCP

▪ Sélectionnez, comme dans la figure ci-dessous, 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.

C’est le champ 11, qui est donc le protocole UDP

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

Version = 4

IHL (val. déci. et hexa.) = déci : 20 hexa : 45

Protocole (val. déci. et hexa.) = déci : 11 hexa : 17

Source address (val. déci. et hexa.) = déci : 0.0.0.0 hexa : 00 00 00 00

Destination address (val. déci. et hexa.) = déci : 255.255.255.255 hexa : ff : ff : ff : ff : ff : ff

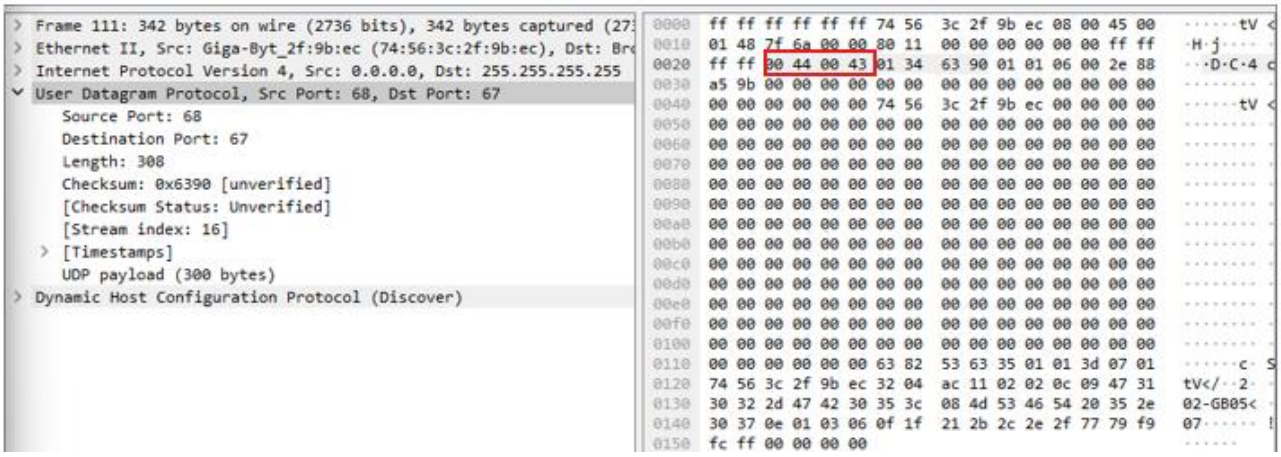
▪ Que signifie la valeur contenue dans le champ adresse IP source ?

C’est l’adresse IP de la machine qui a effectuée la requête.

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

L’adresse de la couche 3 est une broadcast, elle est donc inconnue.

▪ Sélectionnez, comme dans la figure ci-dessous, 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 ?

C'est le champ UDP

▪ 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 port 68 et sa valeur hexadécimale est 00 44.

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

Le protocole applicatif encapsulé dans UDP est le protocole 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 le port 67 et sa valeur hexadécimale est 00 43.

▪ Sélectionnez la section Bootstrap Protocol contenu dans la trame DHCP Discover :