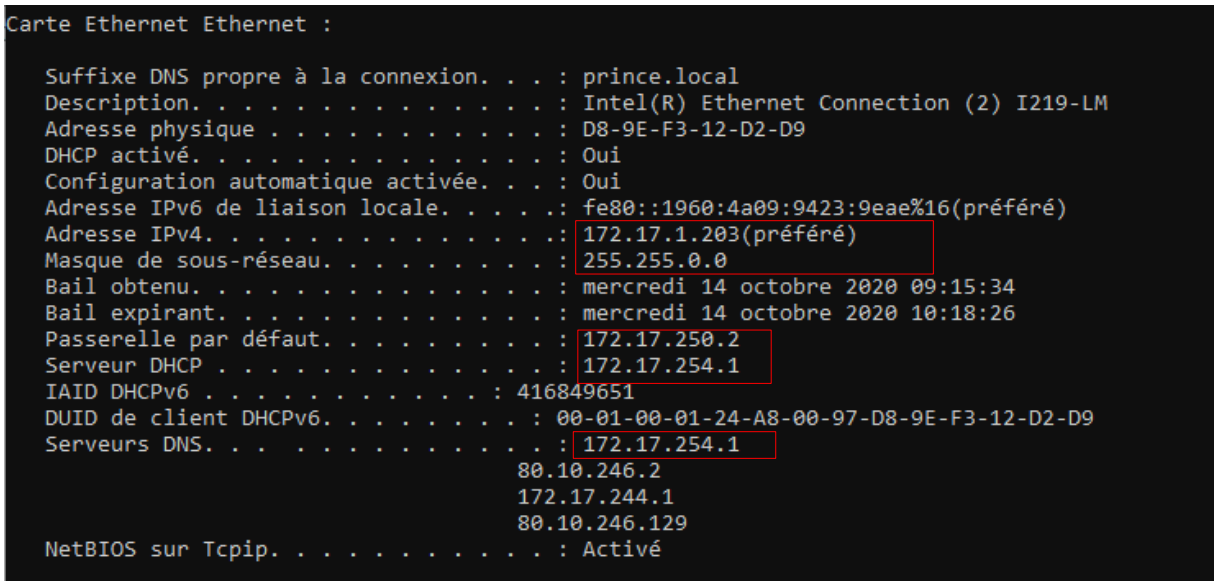
Compte-Rendu TP2Bloc1exSI2-TrameDHCP

2.Capture de trames DHCP avec Wireshark



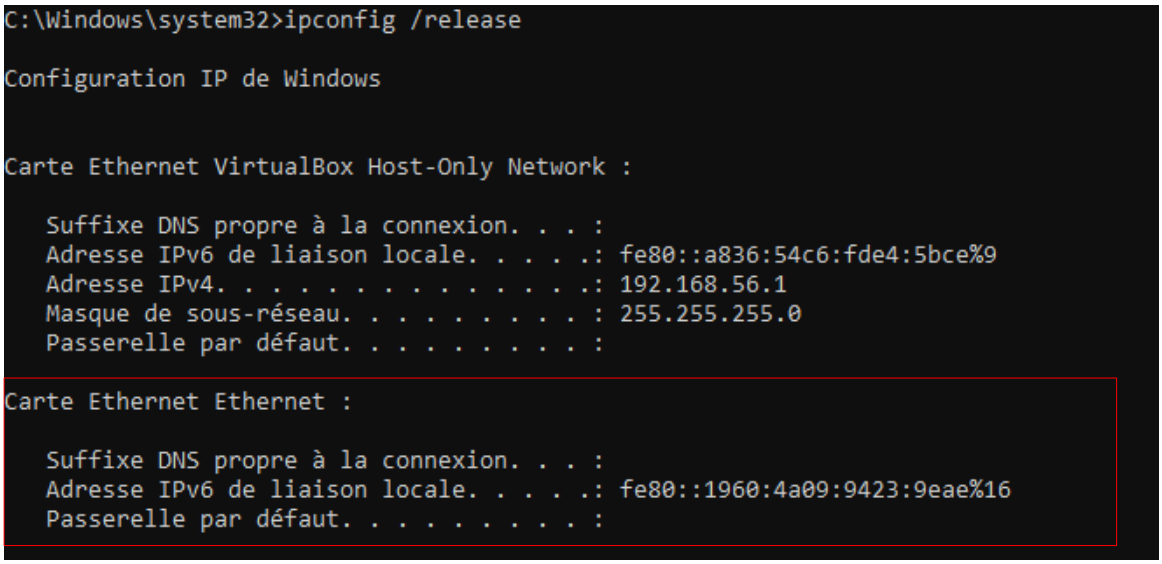
```
Carte Ethernet Ethernet :

   Suffixe DNS propre à la connexion. . . : prince.local
   Description. . . . . . . . . . . . . . : Intel(R) Ethernet Connection (2) I219-LM
   Adresse physique . . . . . . . . . . . : D8-9E-F3-12-D2-D9
   DHCP activé. . . . . . . . . . . . . . : Oui
   Configuration automatique activée. . . : Oui
   Adresse IPv6 de liaison locale. . . . .: fe80::1960:4a09:9423:9eae%16(préféré)
   Adresse IPv4. . . . . . . . . . . . . .: 172.17.1.203(préféré)
   Masque de sous-réseau. . . . . . . . . : 255.255.0.0
   Bail obtenu. . . . . . . . . . . . . . : mercredi 14 octobre 2020 09:15:34
   Bail expirant. . . . . . . . . . . . . : mercredi 14 octobre 2020 10:18:26
   Passerelle par défaut. . . . . . . . . : 172.17.250.2
   Serveur DHCP . . . . . . . . . . . . . : 172.17.254.1
   IAID DHCPv6 . . . . . . . . . . . : 416849651
   DUID de client DHCPv6. . . . . . . . : 00-01-00-01-24-A8-00-97-D8-9E-F3-12-D2-D9
   Serveurs DNS. . .  . . . . . . . . . . : 172.17.254.1
                                 80.10.246.2
                                 172.17.244.1
                                 80.10.246.129
   NetBIOS sur Tcpip. . . . . . . . . . . : Activé
```

L'adresse IP attribuée par le serveur est 172.17.1.203

Renseignez les autres éléments :

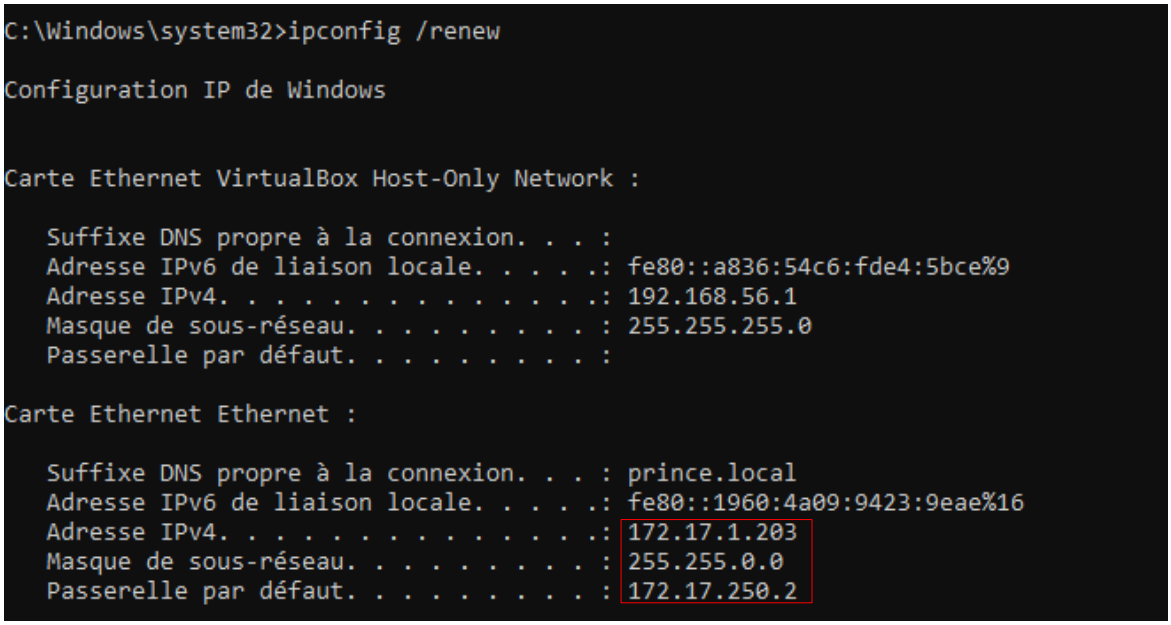
- Masque de sous-réseau : 255.255.0.0
- Bail obtenu : Mercredi 14 Octobre 2020 09 :15 :34
- Bal expirant : Mercredi 14 Octobre 2020 10 :18 :26
- Passerelle par défaut : 172.17.250.2
- Serveur DHCP : 172.17.254.1
- Serveur DNS : 172.17.254.1



Adresse IPv4 : 0.0.0.0

Masque de sous-réseau : 0.0.0.0

Passerelle par défaut : 0.0.0.0

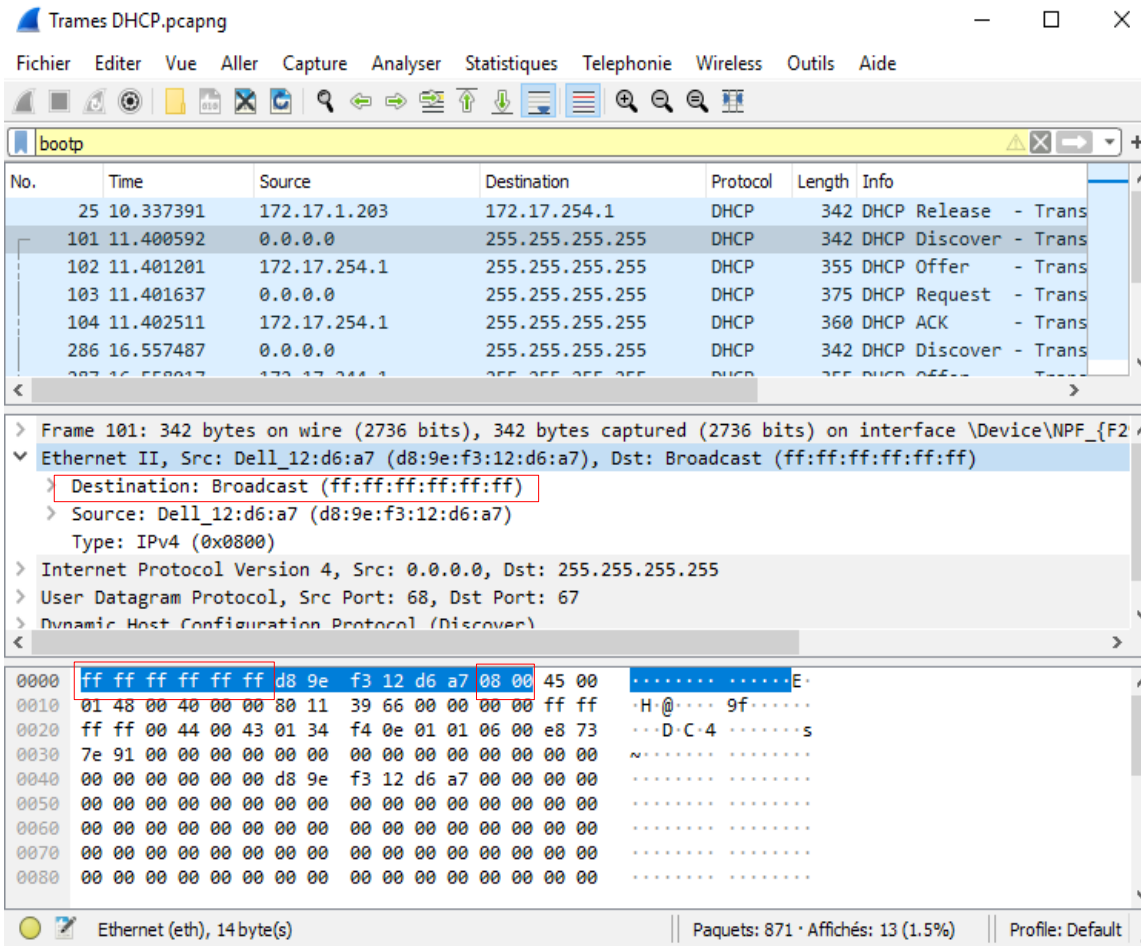


Adresse IPv4 : 172.17.1.203

Masque de sous-réseau : 255.255.0.0

Passerelle par défaut : 172.17.250.2

4. Etude de la trame DHCP Discover



L’adresse MAC Source de la trame DHCP Discover dans le volet des octets est :

d8 :9e :f3 :12 :d6 :a7 :08 :00

L’adresse MAC destination de la trame DHCP Discover dans le volet des octets est : ff :ff :ff :ff :ff :ff

L’adresse de couche 2 de destination de cette trame est une adresse de broadcast.

Le champ qui suit immédiatement les deux adresses MAC est le champ éthertype.

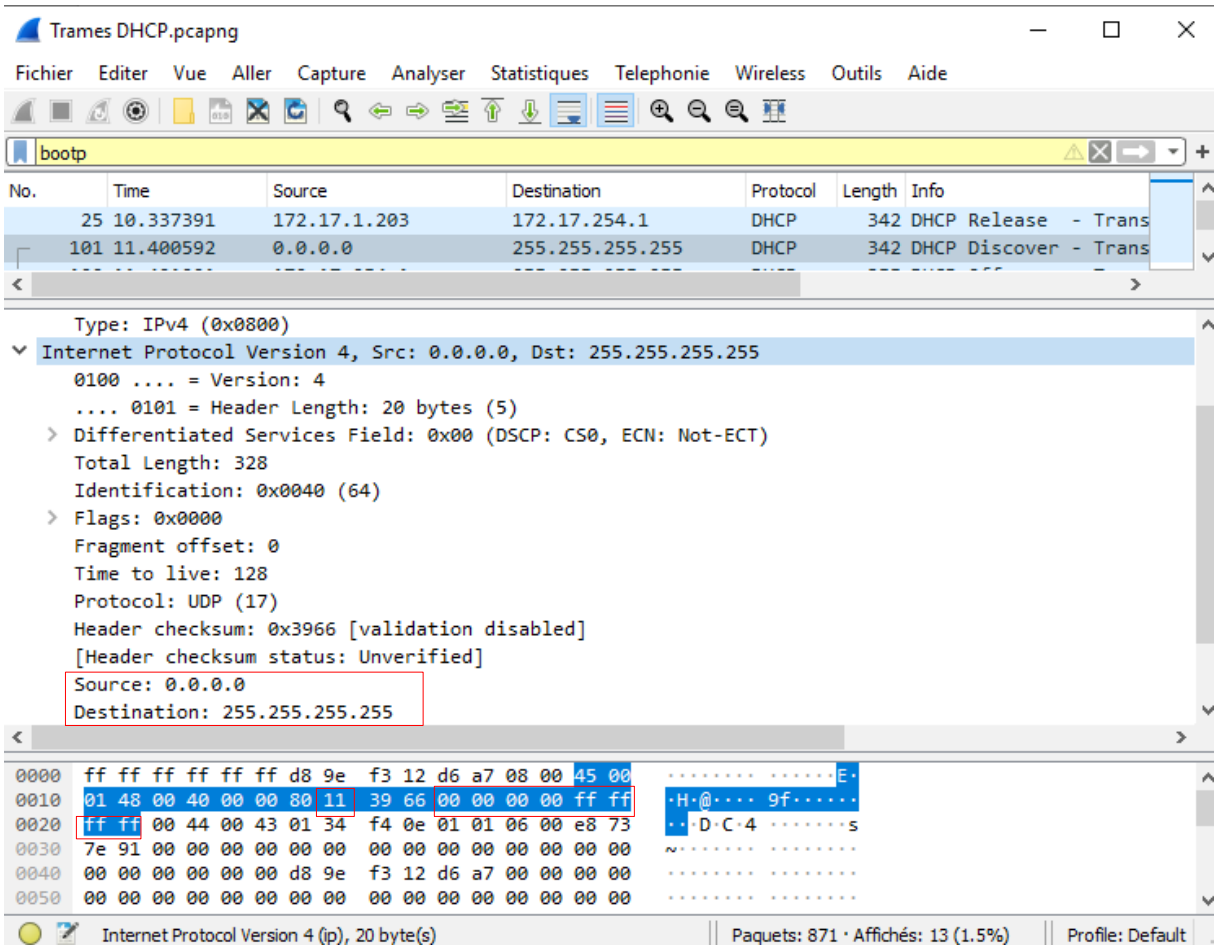
Le champ éthertype comporte la valeur : 08 00 , ce qui signifie que le protocole IPv4 sera transporté derrière l’en-tête de trame, soit un paquet IP.

Cette trame inclut les protocoles :

IPv4

UDP (valeur 11 dans l’en-tête IP)

DHCP (valeur 00 43 pour le port destination 67, dans l'en-tête de transport)



Le champ de l'en-tête IP permettant de connaître le protocole de transport des messages DCHP est le champ sur la ligne 10 qui porte la valeur 11, soit le protocole UDP.

Version : 4

IHL (val. Déci. Et Hexa.) = 20 en décimale et 14 en héxadécimale

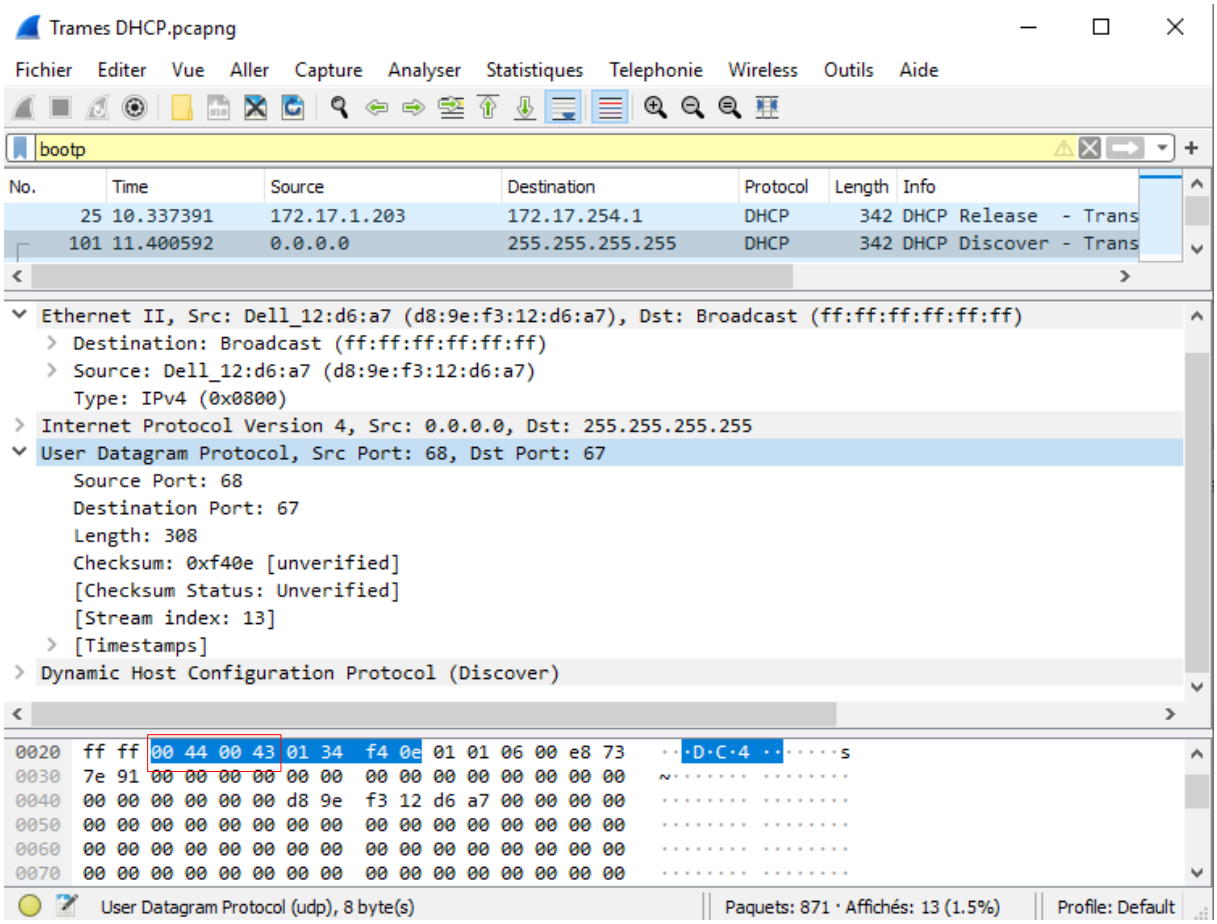
Protocole (val. Déci. et Hexa.) = 11 en hexadécimale et 17 en décimale

Source address (val déci. et hexa.) = 00.00.00.00 en héxadécimale et 0.0.0.0 en décimale

Destination address (val déci. et hexa) = ff ff ff ff en héxadécimale et 255.255.255.255 en décimale

La valeur contenue dans le champ adresse IP source signifie qu'il n'y a pas d'adresse IP attribué à la machine.

L'adresse de couche 3 de destination de cette trame est une adresse IP de broadcast.



Le nom du champ de l'en-tête de transport permettant le démultiplexage de protocole est le champ port.

Le port UDP utilisé par le client DHCP est le port correspondant à la valeur hexadécimale 00 44, soit le port 68.

Le protocole encapsulé dans le datagramme UDP est le protocole DHCP.

Le serveur DHCP utilise le port 67 pour recevoir et écouter la requête. Elle correspond à la valeur 00 43 en héxadécimale.