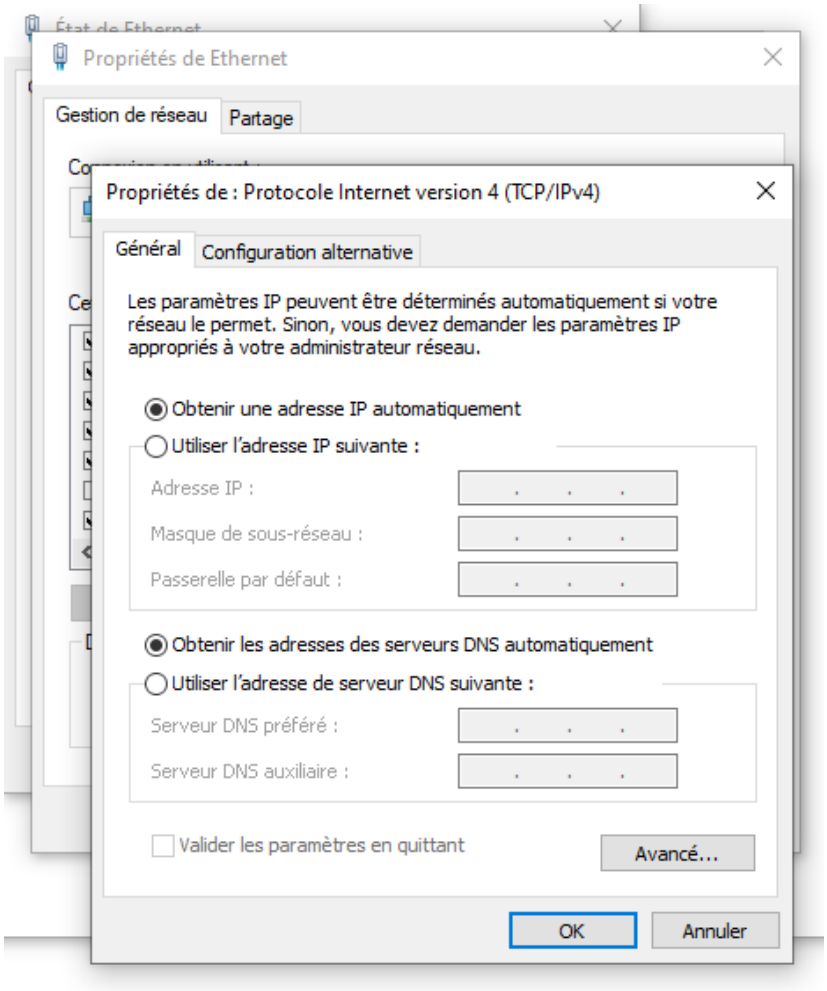
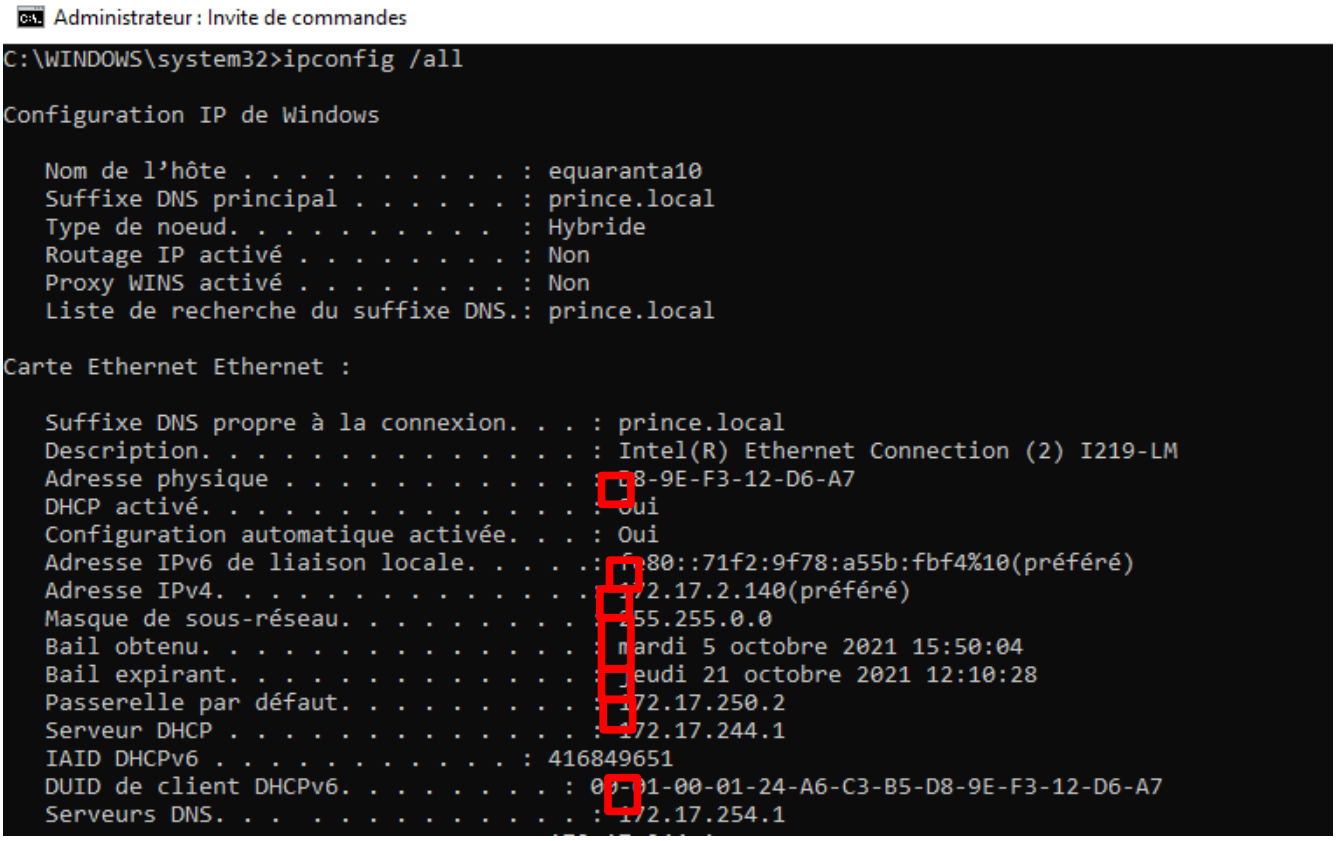
TP2: analyse de trames DHCP avec Wireshark

2) Capture de trames DHCP avec Wireshark



1ère étape: Vérifier les propriétés TCP/IPv4 de notre machine physique. Celle-ci doivent être définies de manière à obtenir automatiquement les paramètres IP.



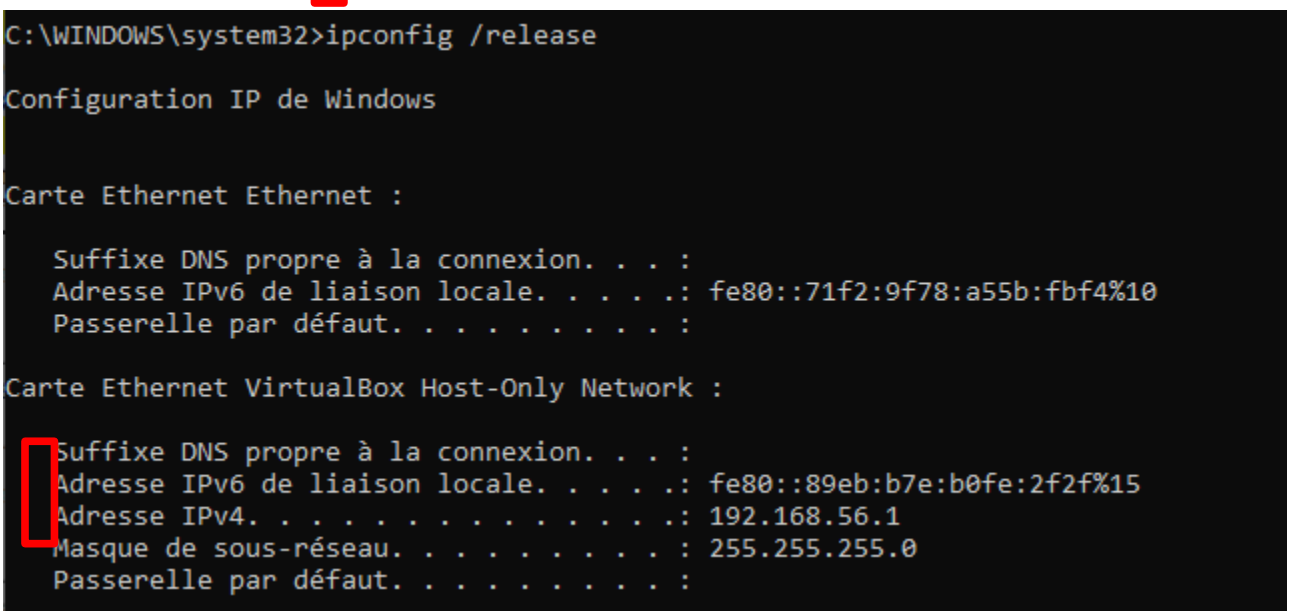
2ème étape: Une invite de commande (cmd) est ouverte depuis notre machine physique, dans celle-ci la commande "**ipconfig /all**".

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

Adresse IP : 172.17.2.140

Renseignez les autres éléments ci-dessous :

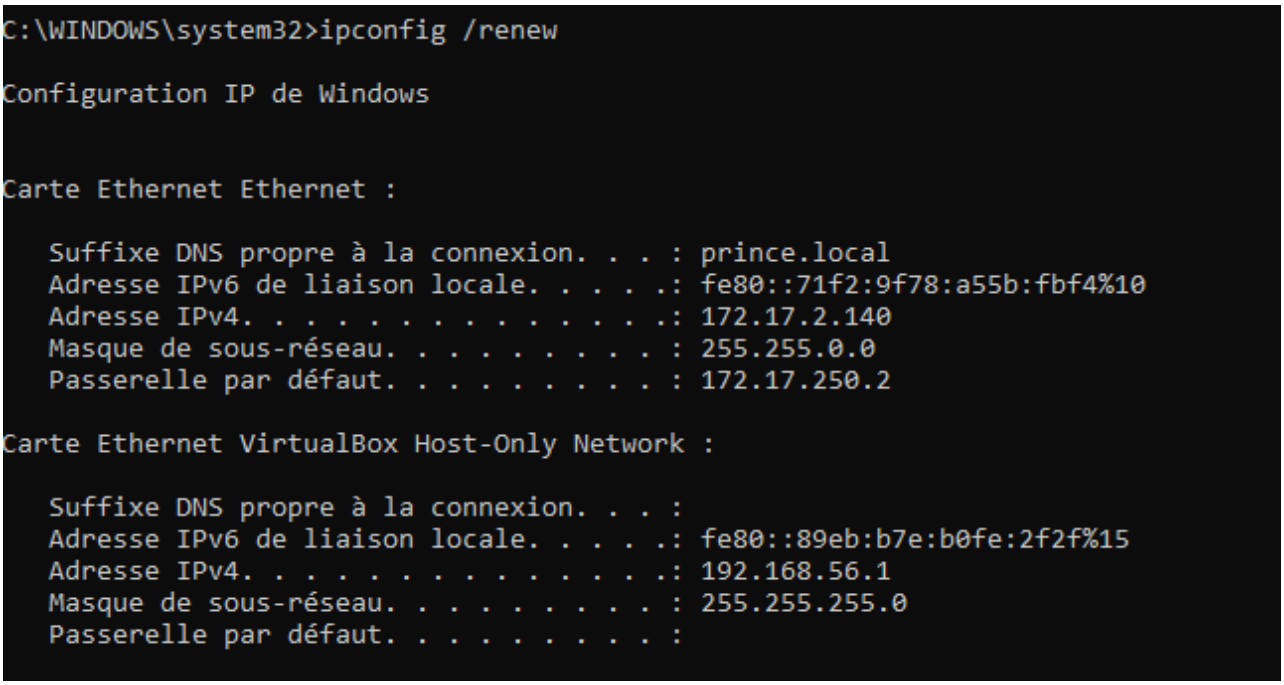
DHCP activé : Oui
Masque de sous-réseau : 255.255.0.0
Bail obtenu : mardi 5 octobre 2021 15:50:04
Bail expirant : jeudi 21 octobre 2021 12:10:28
Passerelle par défaut : 172.17.250.1
Serveur DHCP : 172.17.244.1
Serveur DNS : 172.17.254.1



3ème étape : Durant une capture de trame sur Wireshark, la commande "**ipconfig /release**" est éffectuée, celle-ci permet de libérer l'adresse IP qui avait été obtenue.

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

Adresse IPv4 : 192.168.56.1
Masque de sous-réseau : 255.255.255.0
Passerelle par défaut : Absence de passerelle par défaut

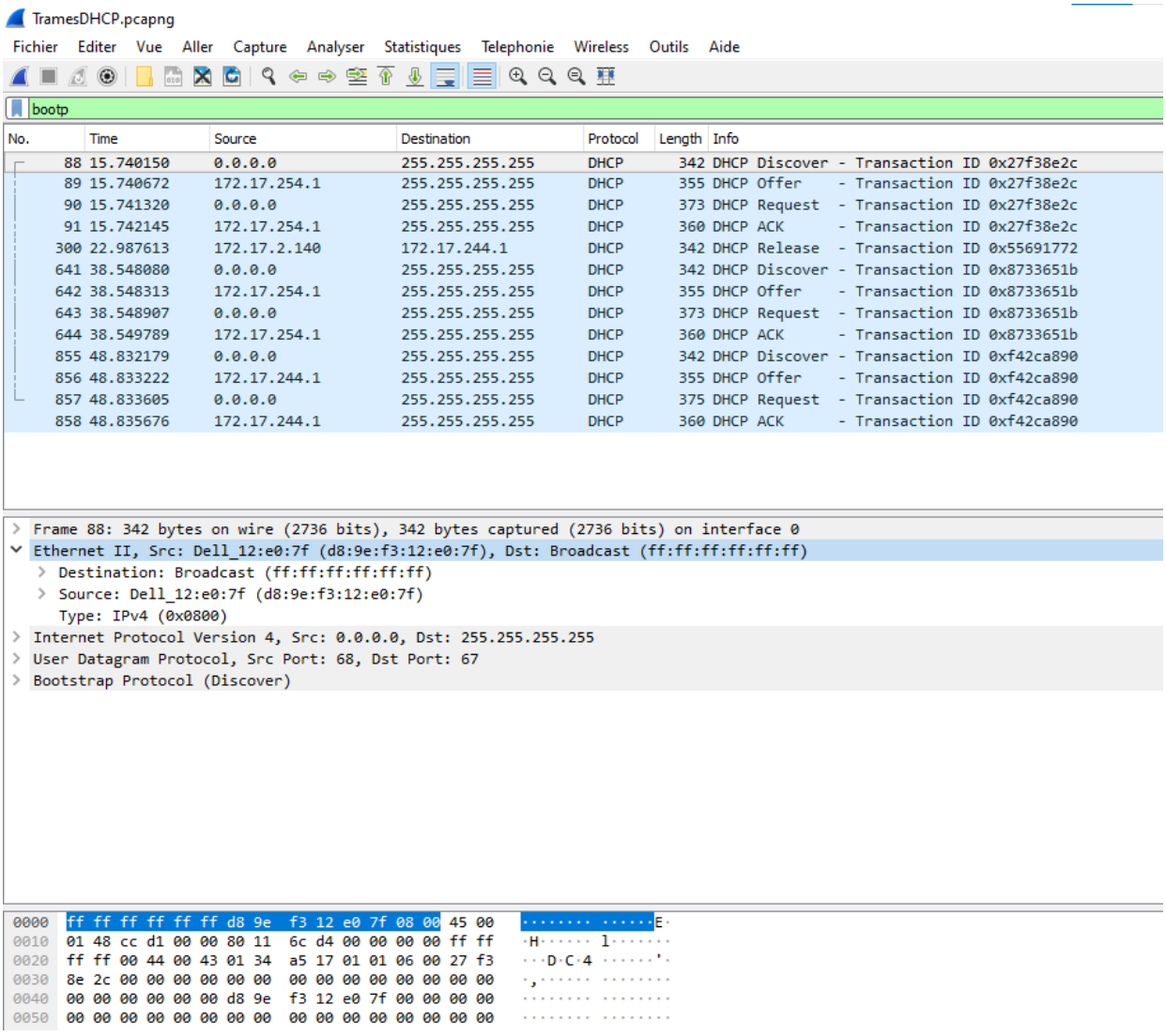


4ème étape: Ici nous saisissions la commande "**ipconfig /renew**", celle-ci envoie une requête à un serveur DHCP dont l'objectif est d'obtenir ou de renouveler un bail pour une adresse IP.

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

Adresse IPv4 : 192.168.56.1
Masque de sous-réseau : 255.255.255.0
Passerelle par défaut : Absence de passerelle par défaut

4) Etude de la trame DHCP Discover



Identifiez les adresses MAC source et destination dans le volet des octets :
Adresse MAC destination : ff ff ff ff ff ff
Adresse Mac source : d8 9e f3 12 e0 7f

Caractérisez l'adresse de couche 2 de destination de cette trame :
L'adresse de couche 2 de destination de la trame est représenté par ff ff ff ff ff ff, celle-ci signifie donc que c'est une adresse de broadcast.

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

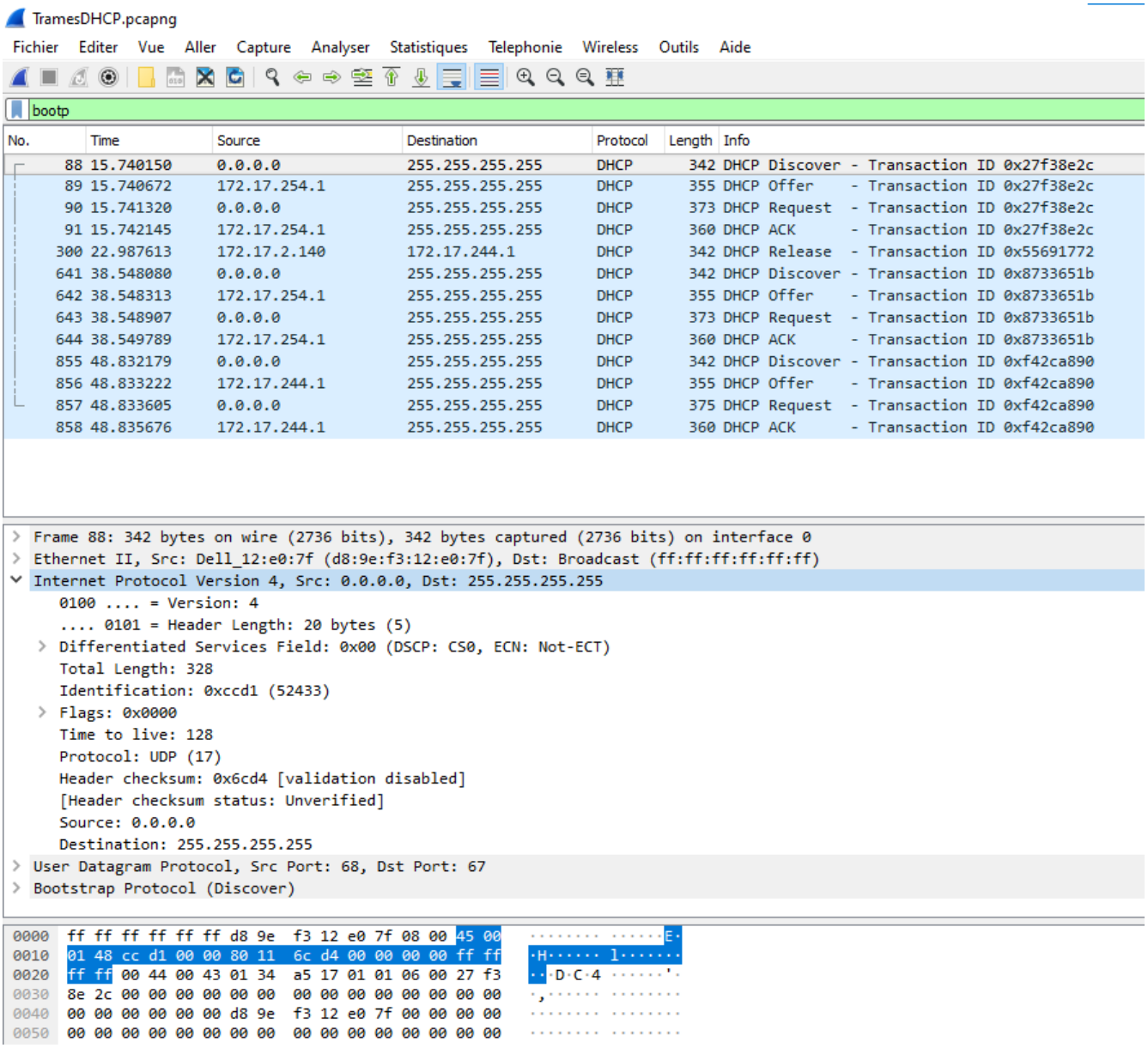
Le champ Ethertype.

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

Il contient la valeur 0800.
Elle signifie donc que suit l'en-tête IP après le champ Ethertype.

Quels sont les protocoles inclus dans cette trame ?

Dans cette trame on retrouve donc un protocole
- Datagramme UDP (11)
- IPv4 (0800)
- Port source : 68 (44)
- Port destination 67 (43)



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.

Ce champ ce nomme le champ protocole, celui-ci est dans cette exemple de trame le protocole de transport Datagramme UDP (11)

Renseignez ci-dessous les champs d'en-tête IP suivants : Version = 4

IHL (val. déci. et hexa.) = Hexa : 45 00 01 48 cc d1 00 00 80 11 6c d4 00 00 00 00 ff ff ff ff
Déci : 69 0 1 72 204 209 0 0 128 17 108 212 0 0 0 0 255 255 255 255

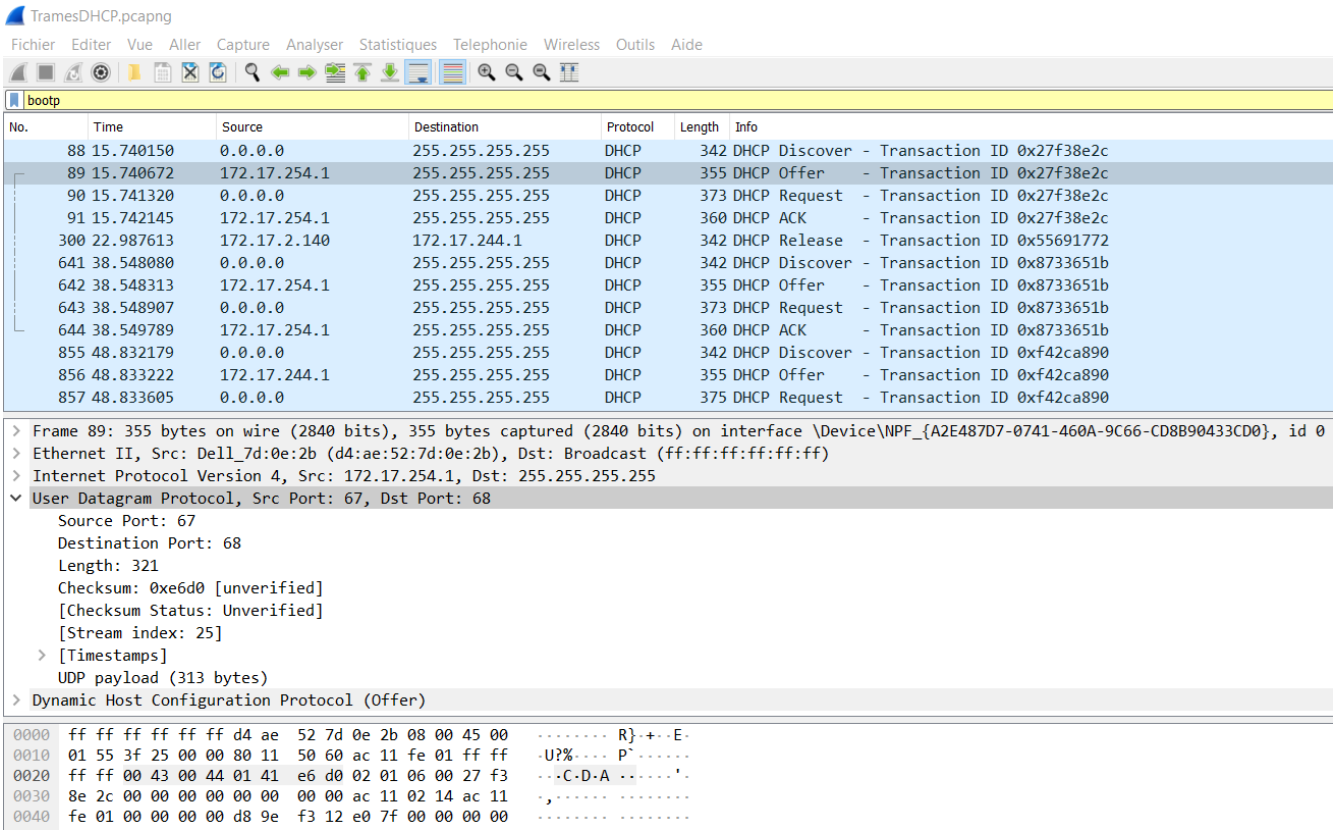
Protocole (val. déci. et hexa.) = UDP, Hexa : 11, Déci : 17

Source address (val. déci. et hexa.) = Hexa : 00 00 00 00, Deci : 0 0 0 0

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

Que signifie la valeur contenue dans le champ adresse IP source ?
Cela signifie qu'il n'y a pas encore d'adresse ip connue dans ce champ.

Caractérisez l'adresse de couche 3 de destination de cette trame :
L'adresse de chouche 3 est donc une adresse de broadcast(diffusion) en 255.255.255.255

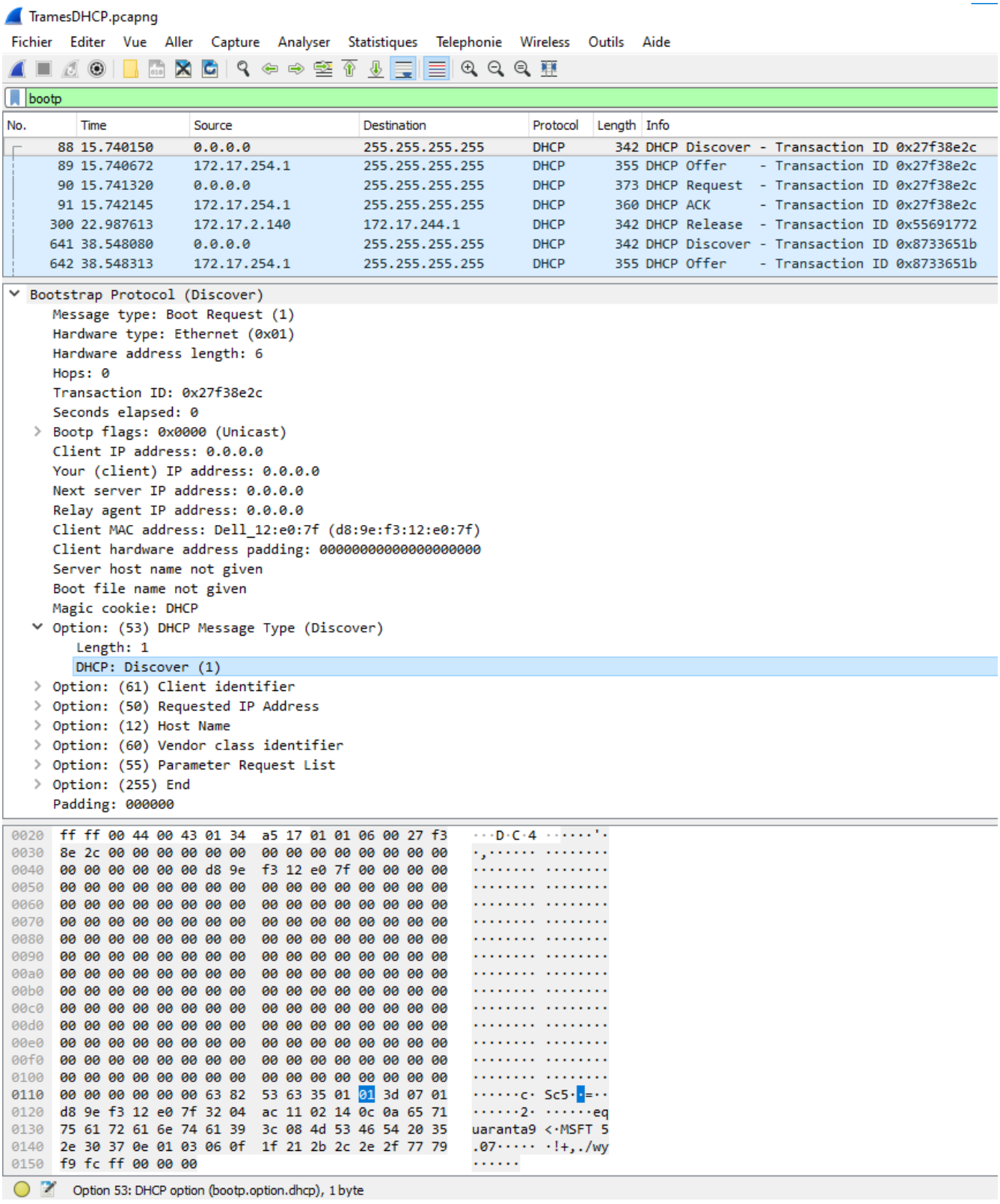


Quel est le nom du champ de l'en-tête de transport permettant le démultiplexage de protocole ?

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) ;
0043 et 0044

Quel est le protocole encapsulé dans le datagramme UDP ?
Le protocole encapsulé dans le datagramme UDP est un protocle 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 serveur DHCP écoute sur le port 0043 soit le port 67 tandis que le client écoute sur le port 00 44 soit 68



Ici la section Bootstrap Protocol à été développée pour observer le contenu dans la trame DHCP Discover.