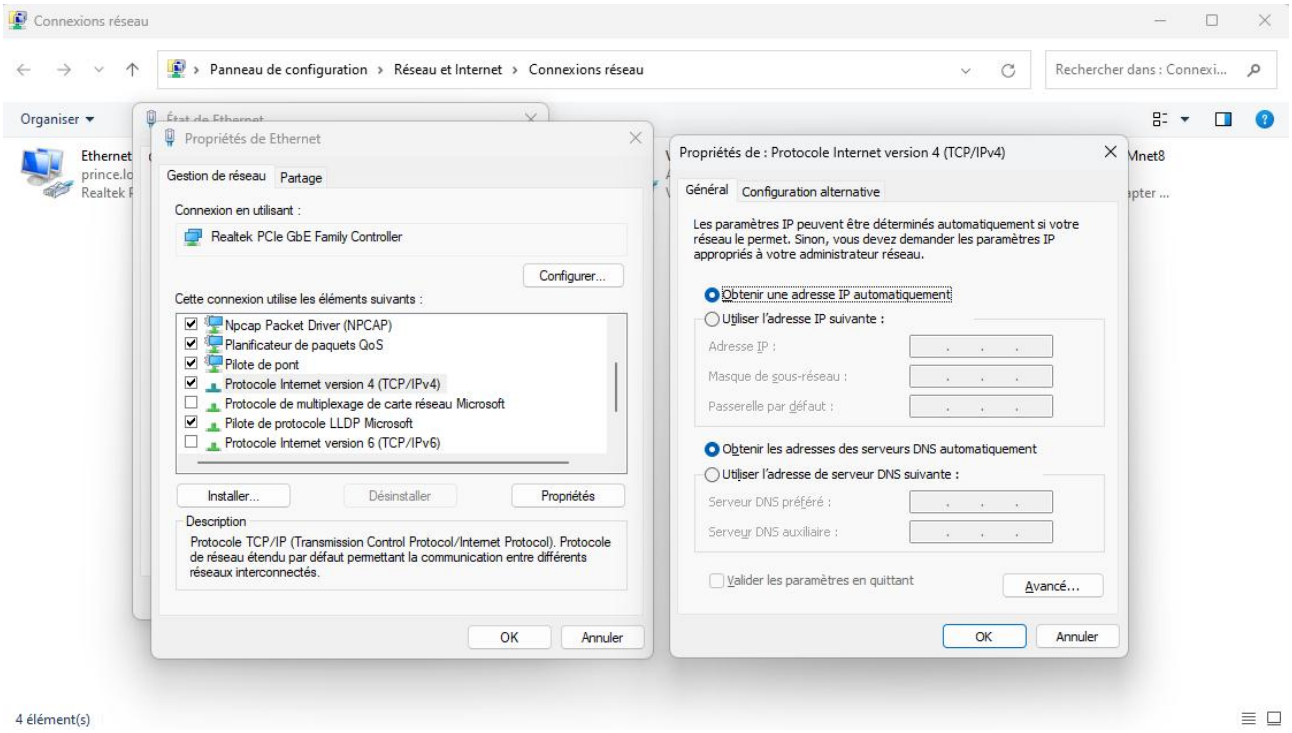
TP4 : analyse de trames DHCP avec Wireshark

Sommaire

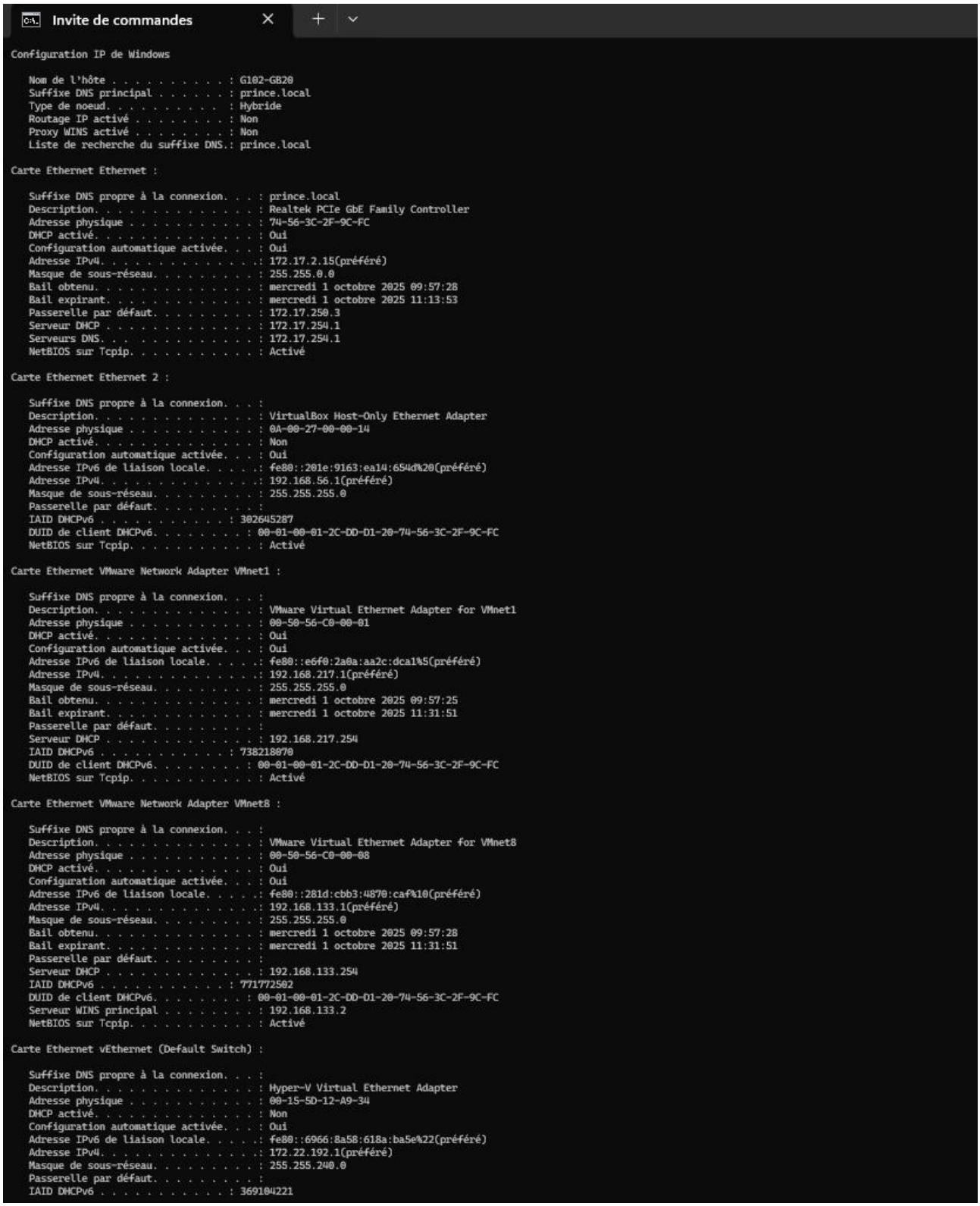
1. Capture de trames DHCP avec Wireshark. 1
4. Etude de la trame DHCP DISCOVER. 6

1. Capture de trames DHCP avec Wireshark.

Je définie les propriété TCP/IPv4 de ma machine de manière a obtenir une adresse IP automatiquement



TP4 : analyse de trames DHCP avec Wireshark



```
Invite de commandes

Configuration IP de Windows

   Nom de l'hôte . . . . . : G102-GB20
   Suffixe DNS principal . . . . . : prince.local
   Type de noeud. . . . . : Hybride
   Routage IP activé . . . . . : Non
   Proxy WINS activé . . . . . : Non
   Liste de recherche du suffixe DNS.: prince.local

Carte Ethernet Ethernet :

   Suffixe DNS propre à la connexion. . . : prince.local
   Description. . . . . : Realtek PCIe GbE Family Controller
   Adresse physique . . . . . : 74-56-3C-2F-9C-FC
   DHCP activé. . . . . : Oui
   Configuration automatique activée. . . : Oui
   Adresse IPv4. . . . . : 172.17.2.15(préféré)
   Masque de sous-réseau. . . . . : 255.255.0.0
   Bail obtenu. . . . . : mercredi 1 octobre 2025 09:57:28
   Bail expirant. . . . . : mercredi 1 octobre 2025 11:13:53
   Passerelle par défaut. . . . . : 172.17.250.3
   Serveur DHCP . . . . . : 172.17.254.1
   Serveurs DNS. . . . . : 172.17.254.1
   NetBIOS sur Tcpip. . . . . : Activé

Carte Ethernet Ethernet 2 :

   Suffixe DNS propre à la connexion. . . :
   Description. . . . . : VirtualBox Host-Only Ethernet Adapter
   Adresse physique . . . . . : 0A-00-27-00-00-14
   DHCP activé. . . . . : Non
   Configuration automatique activée. . . : Oui
   Adresse IPv6 de liaison locale. . . . .: fe80::201e:9163:ea14:654d%20(préféré)
   Adresse IPv4. . . . . : 192.168.56.1(préféré)
   Masque de sous-réseau. . . . . : 255.255.255.0
   Passerelle par défaut. . . . . :
   IAID DHCPv6 . . . . . : 302645287
   DUID de client DHCPv6. . . . . : 00-01-00-01-2C-DD-D1-20-74-56-3C-2F-9C-FC
   NetBIOS sur Tcpip. . . . . : Activé

Carte Ethernet VMware Network Adapter VMnet1 :

   Suffixe DNS propre à la connexion. . . :
   Description. . . . . : VMware Virtual Ethernet Adapter for VMnet1
   Adresse physique . . . . . : 00-50-56-C0-00-01
   DHCP activé. . . . . : Oui
   Configuration automatique activée. . . : Oui
   Adresse IPv6 de liaison locale. . . . .: fe80::e6f0:2a0a:aa2c:dca1%5(préféré)
   Adresse IPv4. . . . . : 192.168.217.1(préféré)
   Masque de sous-réseau. . . . . : 255.255.255.0
   Bail obtenu. . . . . : mercredi 1 octobre 2025 09:57:25
   Bail expirant. . . . . : mercredi 1 octobre 2025 11:31:51
   Passerelle par défaut. . . . . :
   Serveur DHCP . . . . . : 192.168.217.254
   IAID DHCPv6 . . . . . : 738218070
   DUID de client DHCPv6. . . . . : 00-01-00-01-2C-DD-D1-20-74-56-3C-2F-9C-FC
   NetBIOS sur Tcpip. . . . . : Activé

Carte Ethernet VMware Network Adapter VMnet8 :

   Suffixe DNS propre à la connexion. . . :
   Description. . . . . : VMware Virtual Ethernet Adapter for VMnet8
   Adresse physique . . . . . : 00-50-56-C0-00-08
   DHCP activé. . . . . : Oui
   Configuration automatique activée. . . : Oui
   Adresse IPv6 de liaison locale. . . . .: fe80::281d:cbb3:4870:caf%10(préféré)
   Adresse IPv4. . . . . : 192.168.133.1(préféré)
   Masque de sous-réseau. . . . . : 255.255.255.0
   Bail obtenu. . . . . : mercredi 1 octobre 2025 09:57:28
   Bail expirant. . . . . : mercredi 1 octobre 2025 11:31:51
   Passerelle par défaut. . . . . :
   Serveur DHCP . . . . . : 192.168.133.254
   IAID DHCPv6 . . . . . : 771772502
   DUID de client DHCPv6. . . . . : 00-01-00-01-2C-DD-D1-20-74-56-3C-2F-9C-FC
   Serveur WINS principal . . . . . : 192.168.133.2
   NetBIOS sur Tcpip. . . . . : Activé

Carte Ethernet vEthernet (Default Switch) :

   Suffixe DNS propre à la connexion. . . :
   Description. . . . . : Hyper-V Virtual Ethernet Adapter
   Adresse physique . . . . . : 00-15-5D-12-A9-34
   DHCP activé. . . . . : Non
   Configuration automatique activée. . . : Oui
   Adresse IPv6 de liaison locale. . . . .: fe80::6966:8a58:618a:ba5e%22(préféré)
   Adresse IPv4. . . . . : 172.22.192.1(préféré)
   Masque de sous-réseau. . . . . : 255.255.240.0
   Passerelle par défaut. . . . . :
   IAID DHCPv6 . . . . . : 369104221
```

TP4 : analyse de trames DHCP avec Wireshark

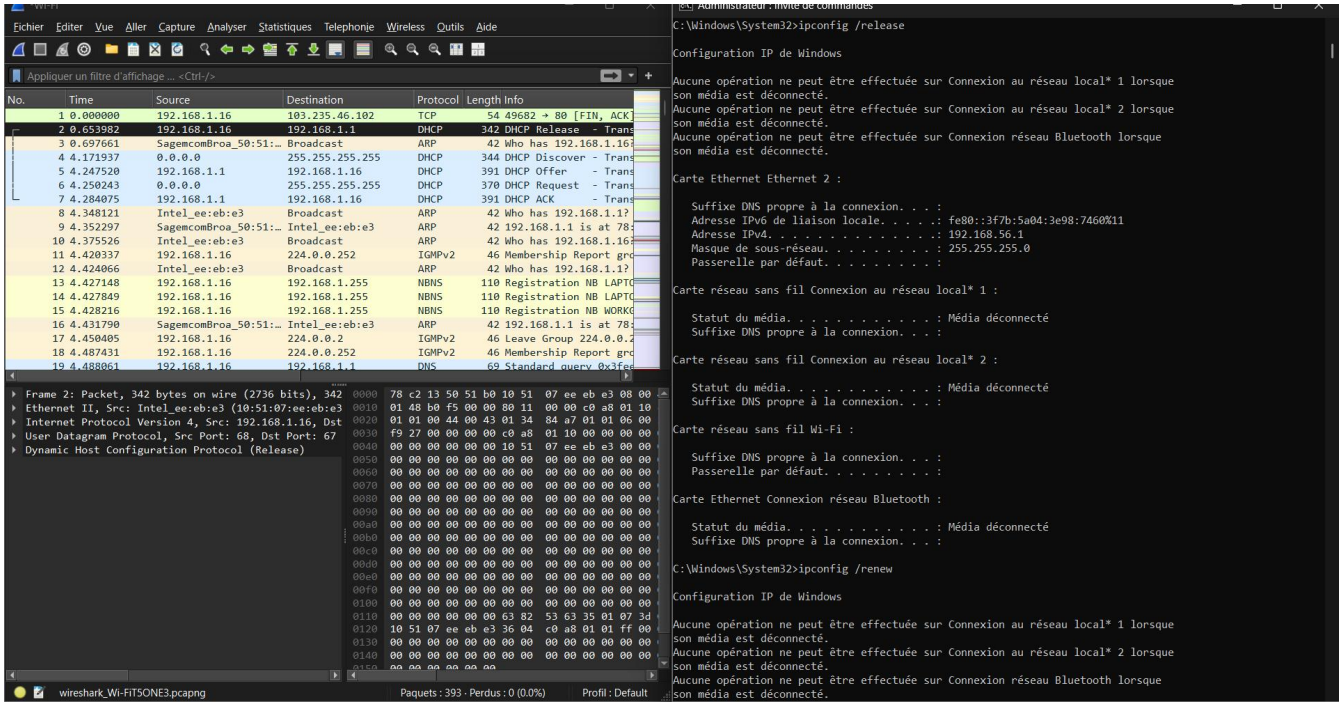
Quelle est l'adresse IP attribuée par le serveur DHCP « ROI » à votre poste de travail ?

```
Carte Ethernet Ethernet :

   Suffixe DNS propre à la connexion. . . : prince.local
   Description. . . . . . . . . . . . . . : Realtek PCIe GbE Family Controller
   Adresse physique . . . . . . . . . . . : 74-56-3C-2F-9C-FC
   DHCP activé. . . . . . . . . . . . . . : Oui
   Configuration automatique activée. . . : Oui
   Adresse IPv4. . . . . . . . . . . . . . : 172.17.2.15(préféré)
   Masque de sous-réseau. . . . . . . . . : 255.255.0.0
   Bail obtenu. . . . . . . . . . . . . . : mercredi 1 octobre 2025 09:57:28
   Bail expirant. . . . . . . . . . . . . : mercredi 1 octobre 2025 11:13:53
   Passerelle par défaut. . . . . . . . . : 172.17.250.3
   Serveur DHCP . . . . . . . . . . . . . : 172.17.254.1
   Serveurs DNS. . . . . . . . . . . . . . : 172.17.254.1
   NetBIOS sur Tcpip. . . . . . . . . . . : Activé
```

L'adresse IP attribuée par le serveur DHCP « ROI » à votre poste de travail est 172.17.254.1

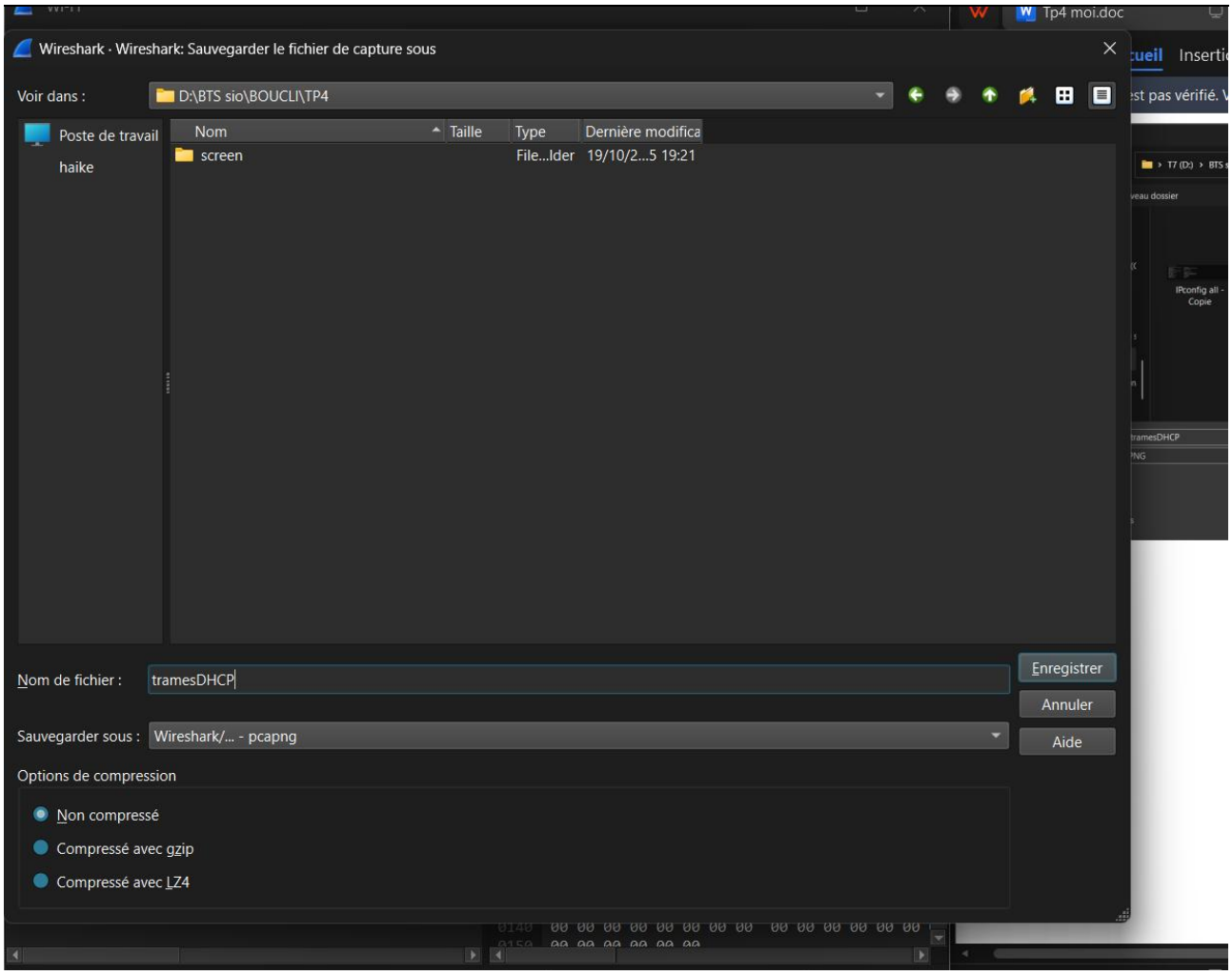
- Renseignez les autres éléments ci-dessous :

DHCP activé : oui
Masque de sous-réseau : 255.255.0.0
Bail obtenu : mercredi 1 octobre 2025 09:57:28
Bail expirant : mercredi 1 octobre 2025 11:13:53
Passerelle par défaut:172.17.250.3
Serveur DHCP:172.17.254.1
Serveur DNS :172.17.254.1



Je réalise les commande - ipconfig /release et ipconfig /renew et demarre une caputure de trames que je vais ensuite enregistrer sous le nom de «TramesDHCP»

TP4 : analyse de trames DHCP avec Wireshark



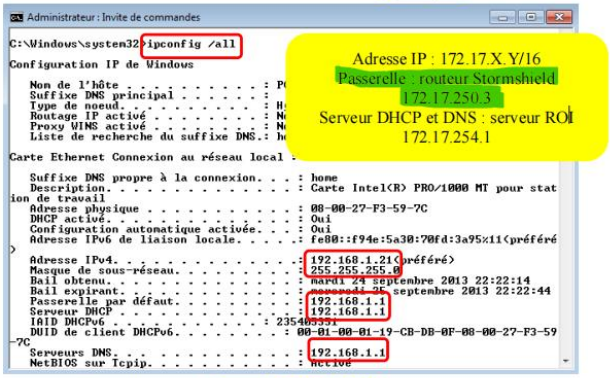
- A partir des renseignements obtenus à l'aide de la commande **ipconfig /release**, renseignez les éléments ci-dessous :

```
C:\Windows\System32>ipconfig /release

Configuration IP de Windows

Aucune opération ne peut être effectuée sur Connexion au réseau local* 1 lorsque
son média est déconnecté.
Aucune opération ne peut être effectuée sur Connexion au réseau local* 2 lorsque
son média est déconnecté.
Aucune opération ne peut être effectuée sur Connexion réseau Bluetooth lorsque
son média est déconnecté.

Carte Ethernet Ethernet 2 :

   Suffixe DNS propre à la connexion. . . :
   Adresse IPv6 de liaison locale. . . . .: fe80::3f7b:5a04:3e98:7460%11
   Adresse IPv4. . . . . . . . . . . . . .: 192.168.56.1
   Masque de sous-réseau. . . . . . . . . : 255.255.255.0
   Passerelle par défaut. . . . . . . . . :

Carte réseau sans fil Connexion au réseau local* 1 :

   Statut du média. . . . . . . . . . . . : Média déconnecté
   Suffixe DNS propre à la connexion. . . :

Carte réseau sans fil Connexion au réseau local* 2 :

   Statut du média. . . . . . . . . . . . : Média déconnecté
   Suffixe DNS propre à la connexion. . . :

Carte réseau sans fil Wi-Fi :

   Suffixe DNS propre à la connexion. . . :
   Passerelle par défaut. . . . . . . . . :

Carte Ethernet Connexion réseau Bluetooth :

   Statut du média. . . . . . . . . . . . : Média déconnecté
   Suffixe DNS propre à la connexion. . . :
```

commande fait à la maison

Adresse IPv4: 192.168.56.1
Masque de sous-réseau :255.255.255.0
Passerelle par défaut : 172.17.250.3

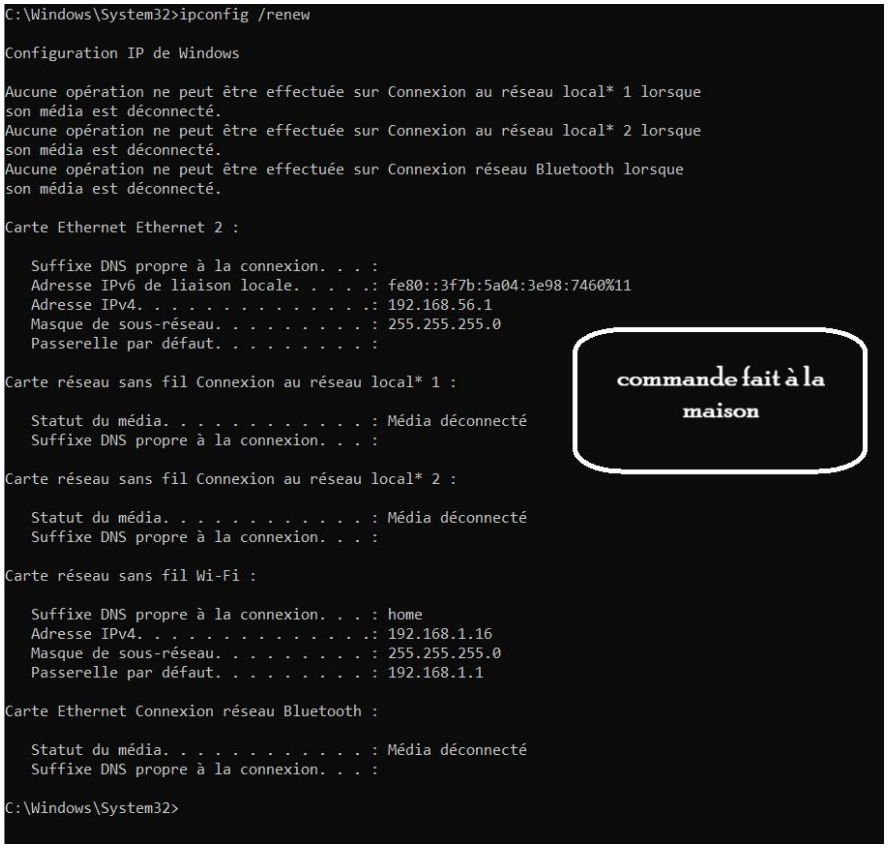
- Ouvrez une invite de commandes et saisissez la commande **ipconfig /all** :



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

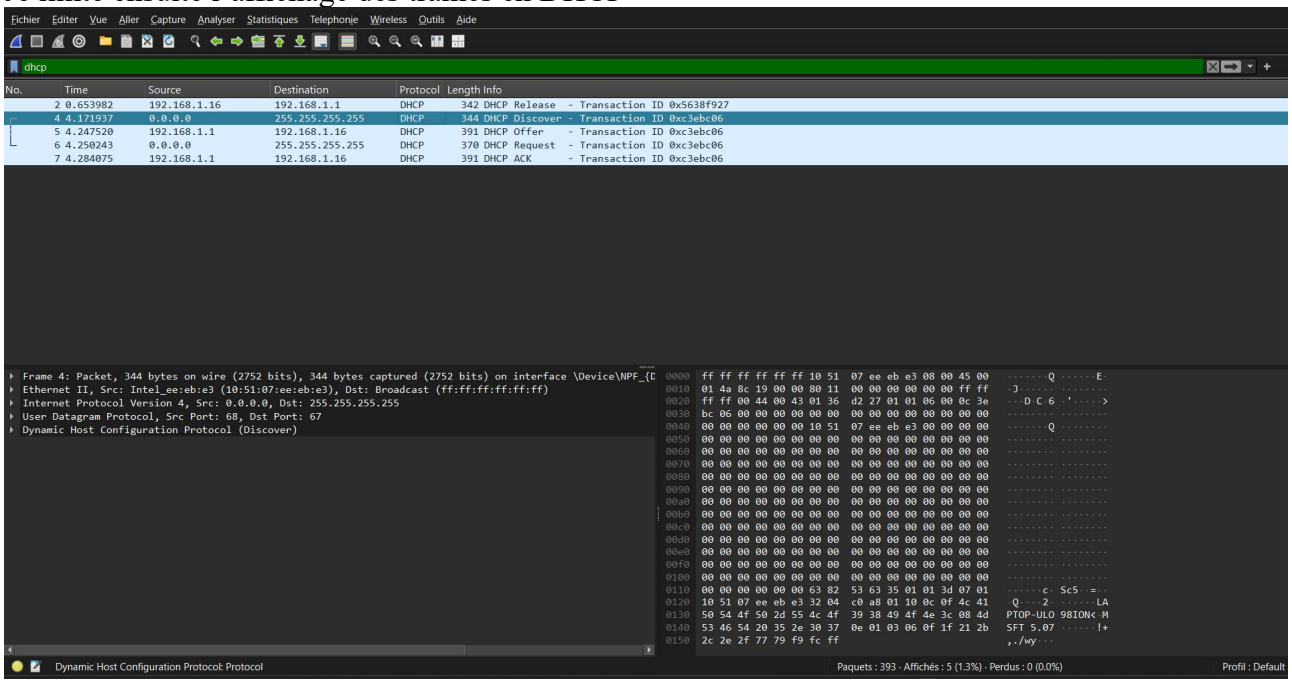
_____

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

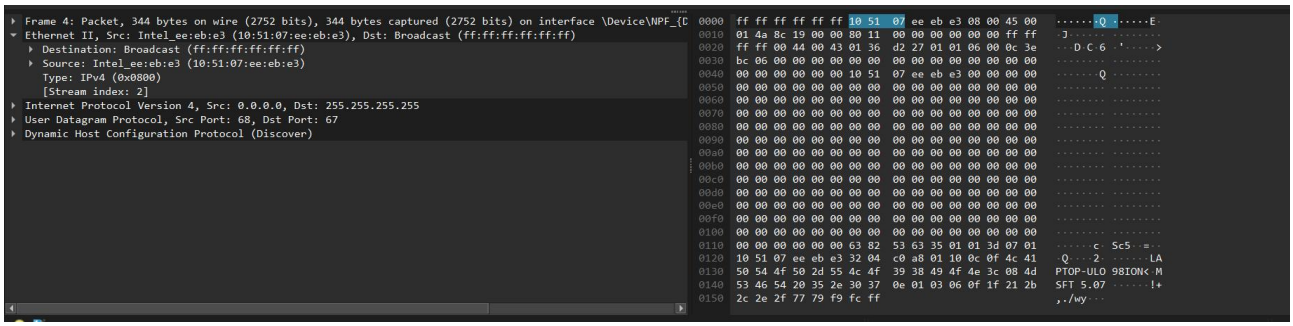


Adresse IPv4: 192.168.56.1
Masque de sous-réseau : 255.255.255.0
Passerelle par défaut: 172.17.250.3

Je limte ensuite l'affichage des trames en DHCP



4. 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 :
-Destination: Broadcast (ff:ff:ff:ff:ff:ff)
-Source: (10:51:07:ee:eb:e3)

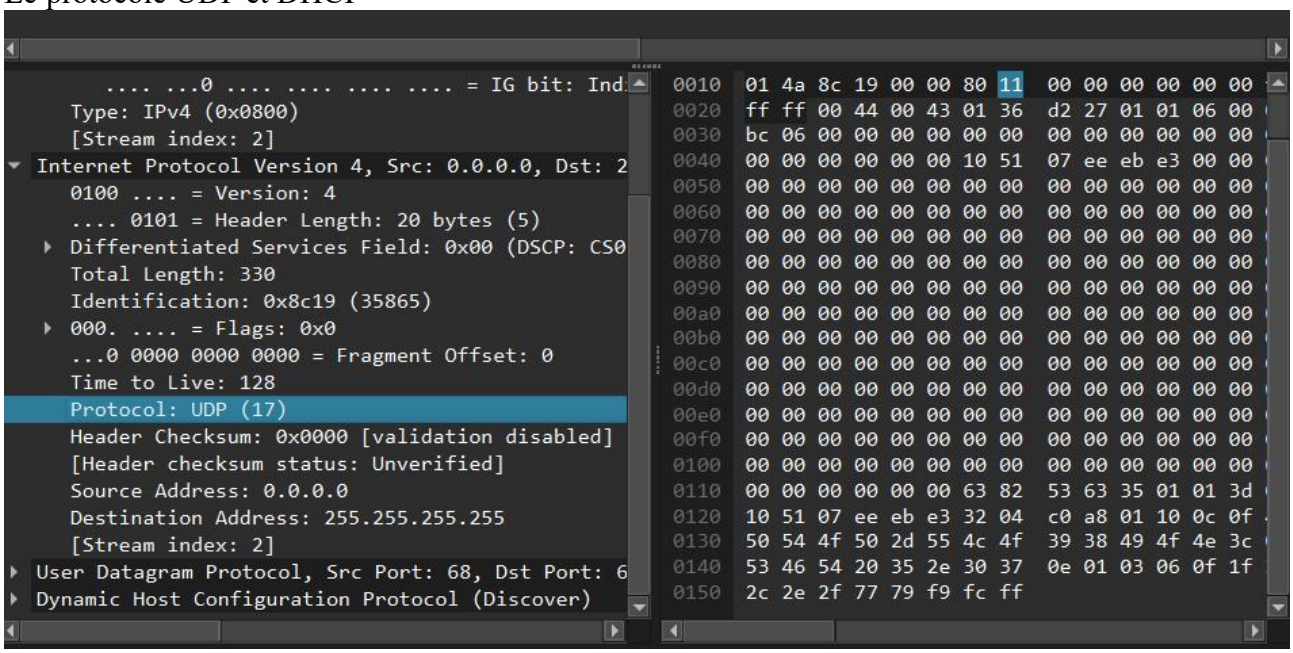
▪ Caractérisez l'adresse de couche 2 de destination de cette trame :
Destination MAC : tout les bits à 1 donc c'est une broadcast, car il ne connaît pas encore le serveur DHCP.

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

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

EtherType : 0x 80 00 et elle signifie que c'est une IPv4

▪ Quels sont les protocoles inclus dans cette trame ?
Le protocole UDP 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 protocol , qui est 11 en hexa 17 en decimale et c'est le protocol UDP

▪ Renseignez ci-dessous les champs d'en-tête IP suivants :
Version = 4
IHL (val. déci. et hexa.) = 20 octets, 5, 0x 5
Protocole (val. déci. et hexa.) = UDP, 17, 11
Source address (val. déci. et hexa.) =0.0.0.0 / 00:00:00:00
Destination address (val. déci. et hexa.) = 255.255.255.255 / ff:ff:ff:ff

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

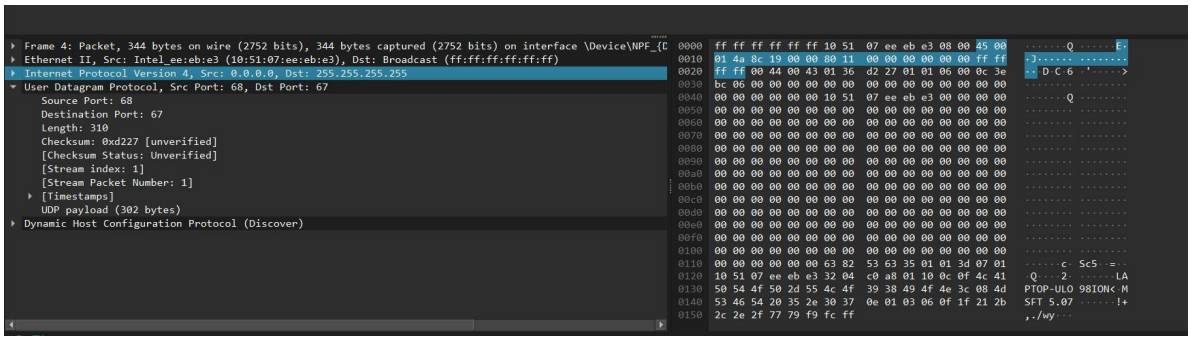
La machine chercher encore l'adresse source et donc c'est une adresse provisoire

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

L'adresse de couche 3 est une adresse destination en broadcast (255.255.255.255)

▪ Sélectionnez, comme dans la figure ci-dessous, l'en-tête du datagramme UDP contenu dans la trame DHCP Discover.

TP4 : analyse de trames DHCP avec Wireshark



▪ Quel est le nom du champ de l'en-tête de transport permettant le démultiplexage de protocole ?
Le champ 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 client DHCP est le 68 , valeur Hexa : 0x 00 44

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

Le protocol 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 client est le 67 soit le 0x 00 43 en Hexa

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