



# TP 4- Analyse des trames DHCP avec Wireshark

Nesrine EL AHMADI

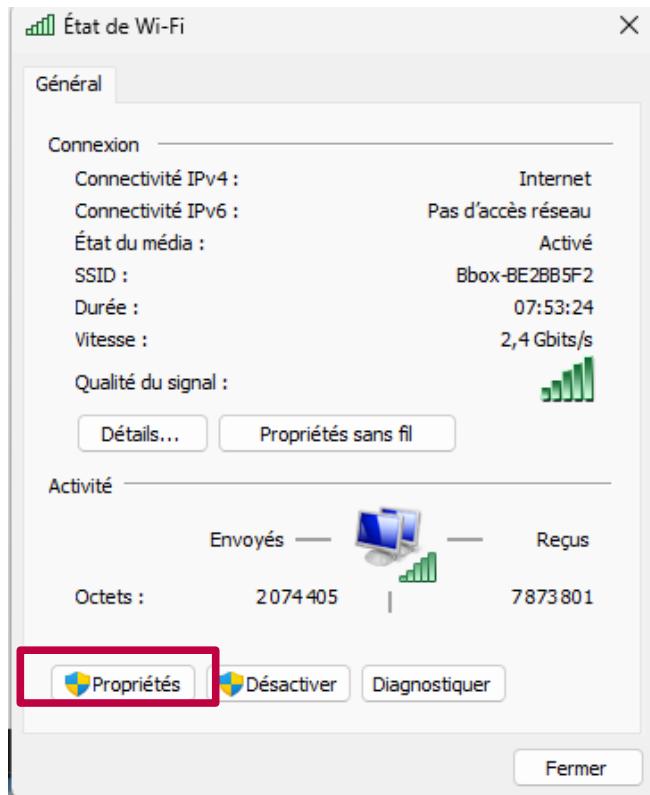
BTS SIO

## Table des matières

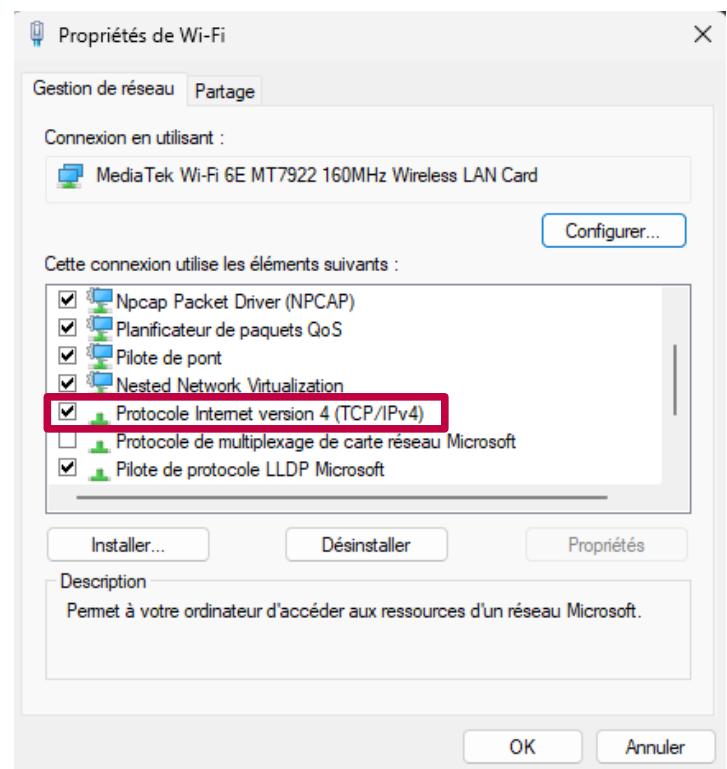
1. Capture de trames DHCP avec Wireshark .....	2
2. Étude de trame DHCP DISCOVER.....	11

## 1. Capture de trames DHCP avec Wireshark

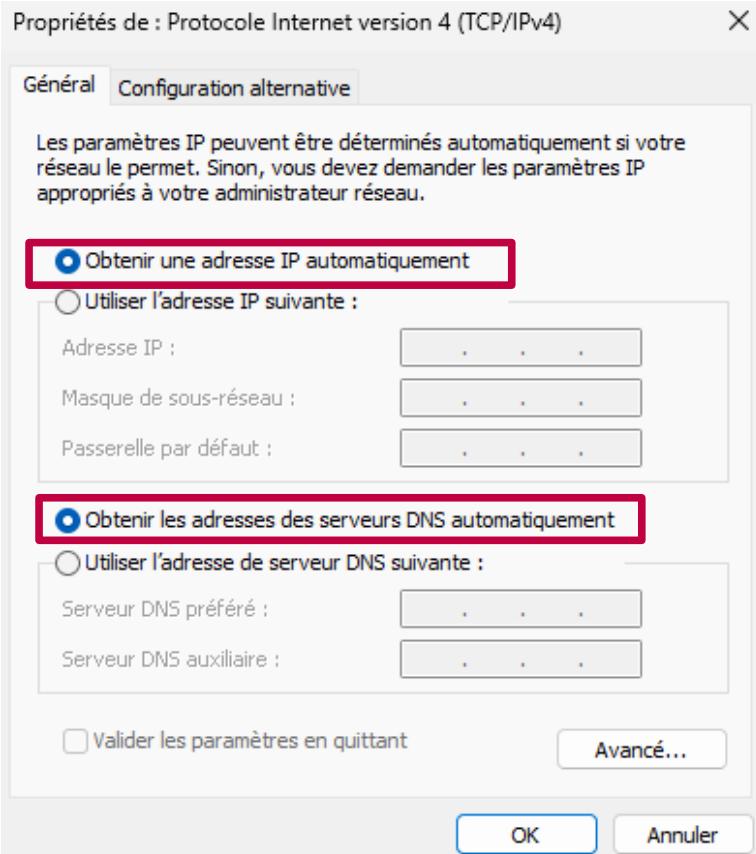
On modifie les propriétés TCP/IPv4 de manière à obtenir automatiquement les paramètre IP du serveur DHCP ( Capture 1, 2 et 3) .



Capture 1



Capture 2



Capture 3

→ On exécute la commande **ipconfig /all** dans l'invite de commande( capture 4).

## Capture 4

## *Capture 4*

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

- Adresse IP : 172.17.2.9

---D'autres éléments sont inscrits :

- DHCP activé : OUI

- Masque de sous-réseau : 255.255.0.0

- Bail obtenu : lundi 13 octobre 2025 16:49:41
  - Bail expirant : mardi 14 octobre 2025 16:49:32
  - Passerelle par défaut : 172.17.250.3
  - Serveur DHCP : 172.17.254.1

Serveur DNS :172.17.254.1

→ On exécute la commande **ipconfig** a titre de comparaison (capture 5).

→ Après avoir exécuté la commande **ipconfig /release** dans l'invite de commande on obtiens certaines informations ( capture 6 ) :

## *Capture 6*

Adresse IPv4 : 192.168.56.1

Masque de sous-réseau : 255.255.255.0

## Passerelle par défaut : ?

→ On exécute ensuite la commande **ipconfig /renew** ( capture 7 ) et obtiens :

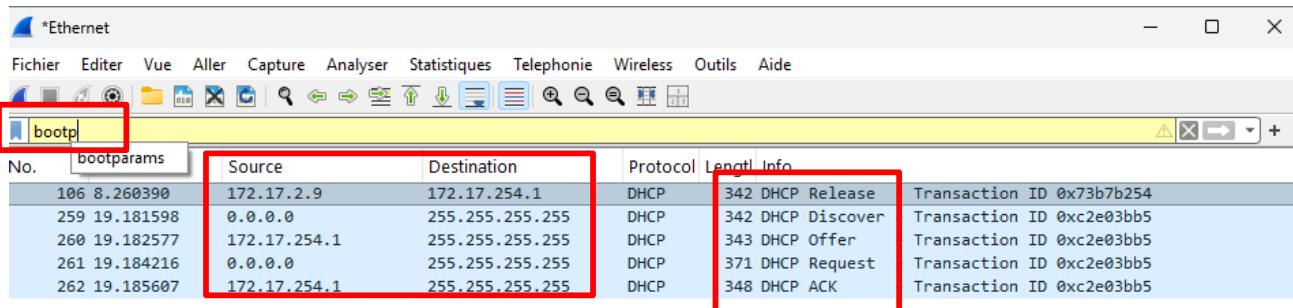
## *Capture 7*

Adresse IPv4 : 192.168.56.1

Masque de sous-réseau : 255.255.255.0

Passerelle par défaut : ?

→ On a fait une **capture de trames a l'aide de Wireshark** tout en générer un peu de trafic entre le poste de travail et le serveur DHCP. On a ensuite limité l'affichage des trames a celle encapsulant les protocoles DHCP ( Capture 8 ).



No.	bootparams	Source	Destination	Protocol	Length	Info
106	8.260390	172.17.2.9	172.17.254.1	DHCP	342	DHCP Release Transaction ID 0x73b7b254
259	19.181598	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover Transaction ID 0xc2e03bb5
260	19.182577	172.17.254.1	255.255.255.255	DHCP	343	DHCP Offer Transaction ID 0xc2e03bb5
261	19.184216	0.0.0.0	255.255.255.255	DHCP	371	DHCP Request Transaction ID 0xc2e03bb5
262	19.185607	172.17.254.1	255.255.255.255	DHCP	348	DHCP ACK Transaction ID 0xc2e03bb5

### Capture 8

On obtient plusieurs trames comme **DHCP RELEASE** ( généré par la commande ipconfig /release), **DHCP DISCOVER** (conséquence de la commande ipconfig / renew), **DHCP OFFER** ( réponse du serveur ), **DHCP REQUEST** (réponse du client pour faire valider son adresse IP) et la trame **DHCP ACK** ( pour confirmer l'attribution)

## 2. Étude de trame DHCP DISCOVER

→ On s'intéresse a la trame **DHCP DISCOVER** et on développe l'en-tête Ethernet ( capture 9)

The screenshot shows the Wireshark interface with the following details:

**Network List:** \*Ethernet

**File Menu:** Fichier, Editer, Vue, Aller, Capture, Analyser, Statistiques, Téléphonie, Wireless, Outils, Aide

**Toolbar:** File, Edit, View, Go, Capture, Analyze, Statistics, Phone, Wireless, Tools, Help

**Search Bar:** bootp

**Table Headers:** No., Time, Source, Destination, Protocol, Length, Info

**Table Data:**

No.	Time	Source	Destination	Protocol	Length	Info
106	8.260390	172.17.2.9	172.17.254.1	DHCP	342	DHCP Release - Transaction ID 0x73b7b254
259	19.181598	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0xc2e03bb5
260	19.182577	172.17.254.1	255.255.255.255	DHCP	343	DHCP Offer - Transaction ID 0xc2e03bb5
261	19.184216	0.0.0.0	255.255.255.255	DHCP	371	DHCP Request - Transaction ID 0xc2e03bb5
262	19.185607	172.17.254.1	255.255.255.255	DHCP	348	DHCP ACK - Transaction ID 0xc2e03bb5

**Frame Details:** Frame 259: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) (0.000 seconds on air) [Raw data (HEX/BIN)]

**Ethernet II, Src: GigaByteTech\_2f:82:ce (74:56:3c:2f:82:ce), Dst: Broadcast (ff:ff:ff:ff:ff:ff)**

**Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.255.255.255**

**User Datagram Protocol, Src Port: 68, Dst Port: 67**

**Dynamic Host Configuration Protocol (Discover)**

**Hex View:** Shows the raw hex data of the captured frame, starting with 0000 and ending at 0150.

*Capture 9*

**---A l'aide de la l'en-tête de trame DHCP DISCOVER on identifie l'adresse MAC source et destination.**

- MAC source : 74:56:3c:2f:82:ce
- MAC destination: ff:ff:ff:ff:ff:ff

**--- Caractérisez l'adresse de couche 2 de destination de cette trame :**

C'est une adresse en broadcast c'est dire qu'elle est diffusé à tout le monde afin de savoir à qui est ce que l'adresse MAC appartient.

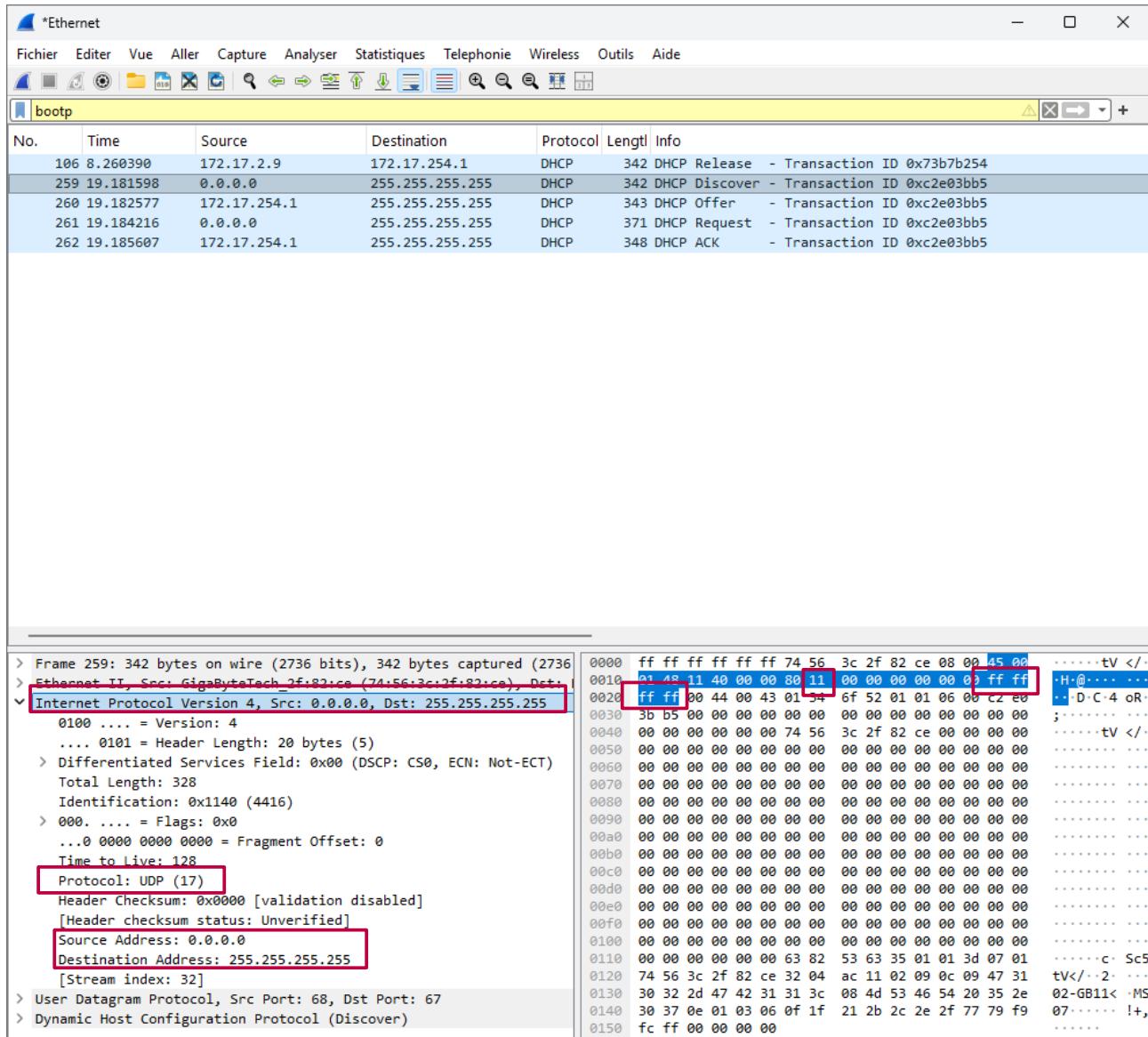
**--- Quel est le champ qui suit immédiatement les deux adresses MAC ? Quelle valeur contient-il ? Que signifie t-elle ?**

Ce qui se trouve juste après les deux adresses MAC est le champ Ethertype ( de 2 octets ) permettant le démultiplexage. Celui nous indique le protocole supérieur encapsulé dans la trame. Dans ce cas sa valeur est de 0x0800 donc IPv4.

**---Quels sont les protocoles inclus dans cette trame ?**

Dans une trame DHCP, plusieurs protocoles sont encapsulés. Tout commence par Ethernet qui transporte les adresses MAC et le champ Ethertype qui nous informe que le protocole supérieur encapsulé dans la trame est le protocole IPv4. Ensuite le datagramme UDP qui assure le transport entre les ports 67 et 68. Enfin, le protocole DHCP est encapsulé au niveau applicatif.

→ On sélectionne l'en-tête IP contenu dans la trame DHCP Discover ( Capture 10 )



## Capture 10

---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 protocole qui nous indique le protocole de couche 4 qui est encapsulé dans le paquet IP.

### Champ d'en-tête IP :

- Version : 4 ( IPv4)
- IHL (val.déci) : 20 octets (en hexadécimal) : 0x14
- Protocole (val.déci) : 17 (en hexadécimal) : 0x11
- Source adresse (val. Déci.) : 0.0.0.0 (client sans IP) (en hexadécimal) : 00 00 00 00
- Destination adresse (val déci) : 255.255.255.255 (en hexadécimal) : FF FF FF FF

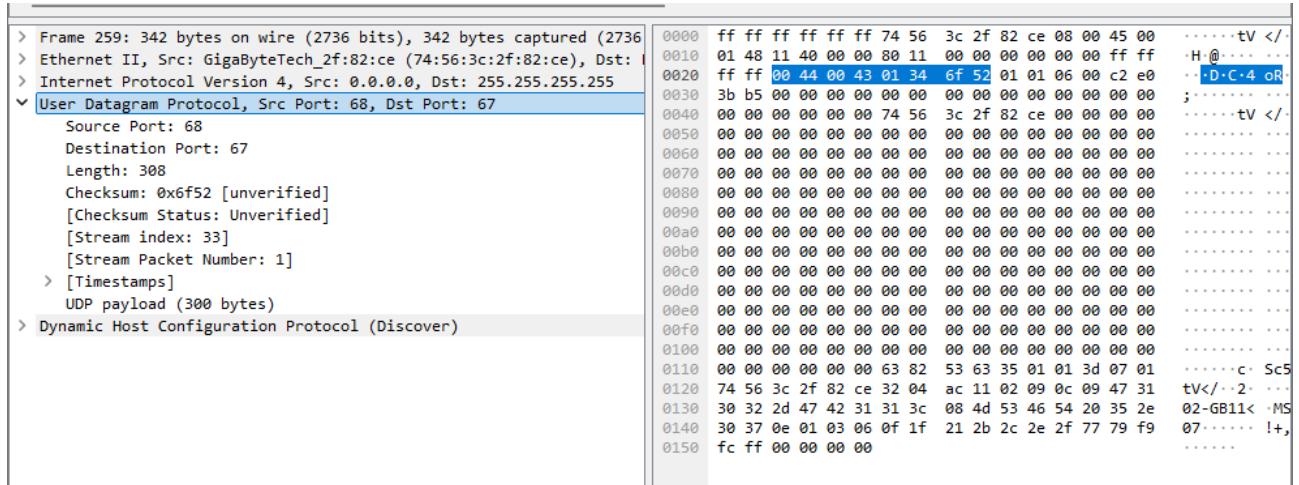
### ---Que signifie la valeur contenue dans le champ Adresse IP source ?

- Elle indique que le client ne possède pas encore d'adresse IP. Il envoie une requête DHCP pour obtenir dynamiquement une configuration réseau l'adresse 0.0.0.0 est utilisé temporairement pour la communication avec le serveur DHCP.

### ---Caractérisez l'adresse de couche 3 de destination de cette trame :

- L'adresse de couche 3 destination une adresse de broadcast . Elle permet d'envoyer sa requête à tous les hôtes du réseau, notamment le serveur DHCP sans connaître leur adresse IP .

### → On sélectionne l'en-tête du datagramme UDP contenu dans la trame DHCP DISCOVER (capture 11)



Frame 259: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits)  
Ethernet II, Src: GigaByteTech\_2f:82:ce (74:56:3c:2f:82:ce), Dst: Internet Protocol Version 4 (0.0.0.0)  
Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.255.255.255  
User Datagram Protocol, Src Port: 68, Dst Port: 67  
Source Port: 68  
Destination Port: 67  
Length: 308  
Checksum: 0x6f52 [unverified]  
[Checksum Status: Unverified]  
[Stream index: 33]  
[Stream Packet Number: 1]  
[Timestamps]  
UDP payload (300 bytes)  
Dynamic Host Configuration Protocol (Discover)

Hex	Dec	ASCII
0000	ff ff ff ff ff ff 74 56 3c 2f 82 ce 08 00 45 00	.....tV </
0010	01 48 11 40 00 00 80 11 00 00 00 00 00 ff ff	·H@.....
0020	ff ff 00 44 00 43 01 34 6f 52 01 01 06 00 c2 e0	··D·C·4 oR
0030	3b b5 00 00 00 00 00 00 00 00 00 00 00 00 00 00	;
0040	00 00 00 00 00 00 74 56 3c 2f 82 ce 00 00 00 00	.....tV </
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	.....
00c0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....
00d0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....
00e0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....
00f0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....
0100	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....
0110	00 00 00 00 00 00 63 82 53 63 35 01 01 3d 07 01	.....c Sc5
0120	74 56 3c 2f 82 ce 32 04 ac 11 02 09 0c 09 47 31	tV<..2..
0130	30 32 2d 47 42 31 31 3c 08 4d 53 46 54 20 35 2e	02-GB11<·MS
0140	30 37 0e 01 03 06 0f 1f 21 2b 2c 2e 2f 77 79 f9	07.....!+,
0150	fc ff 00 00 00 00	.....

### Capture 11

**---Quel est le nom de l'en-tête de transport permettant le démultiplexage de protocoles ?**

• C'est l'en-tête de segment ou ici datagramme car le protocole après le démultiplexage est UDP et on parle de datagramme UDP.

**--- Quel est le port UDP utilisé par le client DHCP ?**

• C'est le port 68 qui est utilisé par le client DHCP pour envoyer sa requête DHCP. ( La requête vient du client)

**---Identifier la valeur hexadécimale correspondante figurant dans le volet des octets :**

→ 00 44

**--- Quel est le protocole applicatif encapsulé dans le datagramme UDP ?**

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

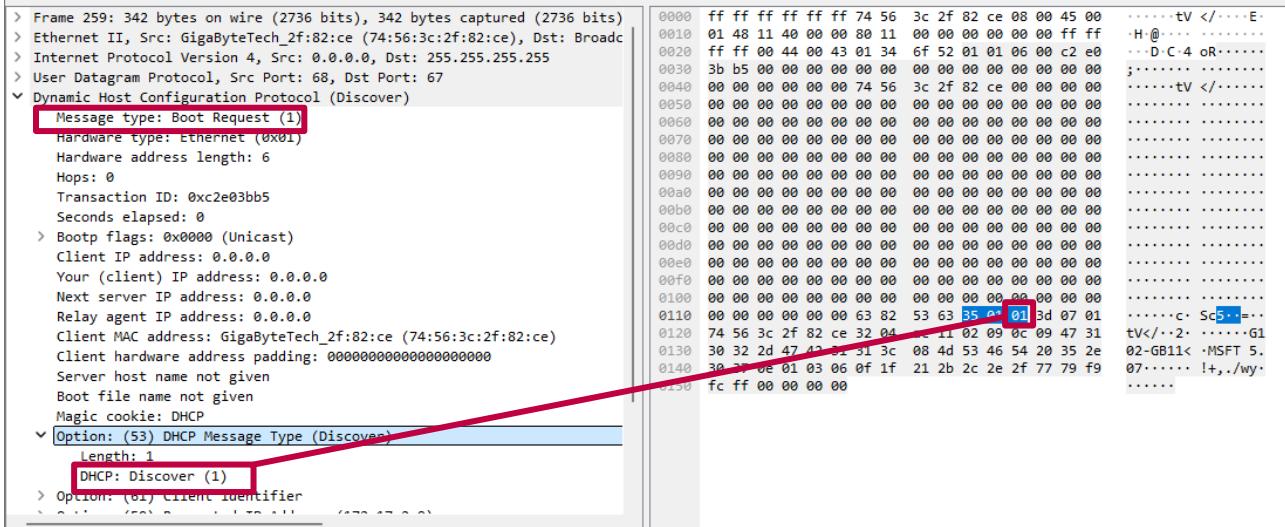
**---Quel est le port UDP utilisé par le serveur DHCP pour écouter et recevoir la requête du client ?**

C'est le port 67 (utilisé par le serveur )

**---Identifier la valeur hexadécimale correspondante figurant dans le volet des octets.**

→ 0x0043

→ On sélectionne la section Bootstrap Protocole contenu dans la trame DHCP DISCOVER ( Capture 12 )



Frame 259: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits)  
Ethernet II, Src: GigaByteTech\_2f:82:ce (74:56:3c:2f:82:ce), Dst: Broadcast  
Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.255.255.255  
User Datagram Protocol, Src Port: 68, Dst Port: 67  
Dynamic Host Configuration Protocol (Discover)  
Message type: Boot Request (1)  
Hardware type: Ethernet (0x1)  
Hardware address length: 6  
Hops: 0  
Transaction ID: 0xc2e03bb5  
Seconds elapsed: 0  
Bootp flags: 0x0000 (Unicast)  
Client IP address: 0.0.0.0  
Your (client) IP address: 0.0.0.0  
Next server IP address: 0.0.0.0  
Relay agent IP address: 0.0.0.0  
Client MAC address: GigaByteTech\_2f:82:ce (74:56:3c:2f:82:ce)  
Client hardware address padding: 000000000000000000000000  
Server host name not given  
Boot file name not given  
Magic cookie: DHCP  
Option: (53) DHCP Message Type (Discover)  
Length: 1  
[DHCP: Discover (1)]  
Option: (61) Client Identifier  
Length: 14  
Value: 00 03 06 0f 1f 21 2b 2c 2e 2f 77 79 f9  
fc ff 00 00 00 00

0000 ff ff ff ff ff ff 74 56 3c 2f 82 ce 08 00 45 00 .....tv </...E-  
0010 01 48 11 40 00 00 80 11 00 00 00 00 00 00 ff ff .H @.....  
0020 ff ff 00 44 00 43 01 34 6f 52 01 01 06 00 c2 e0 ..D C 4 oR.....  
0030 3b b5 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ;.....  
0040 00 00 00 00 00 00 74 56 3c 2f 82 ce 00 00 00 00 .....tv </.....  
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 .....  
00c0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
00d0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
00e0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
00f0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
0100 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
0110 00 00 00 00 00 00 63 82 53 63 35 01 3d 07 01 .....c Sc5.....  
0120 74 56 3c 2f 82 ce 32 04 0e 11 02 09 0c 09 47 31 tv</..2.....G1  
0130 30 32 2d 47 42 0e 31 3c 08 4d 53 46 54 20 35 2e 02-GB11c-MSFT 5.  
0140 30 31 0e 01 03 06 0f 1f 21 2b 2c 2e 2f 77 79 f9 07.....!+../wy.  
0150 fc ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....

## Capture 12

La valeur 1 montre que le message est un Boot Request. Si elle avait été de 2 ça signifierait qu'il sagit d'un boot Reply.