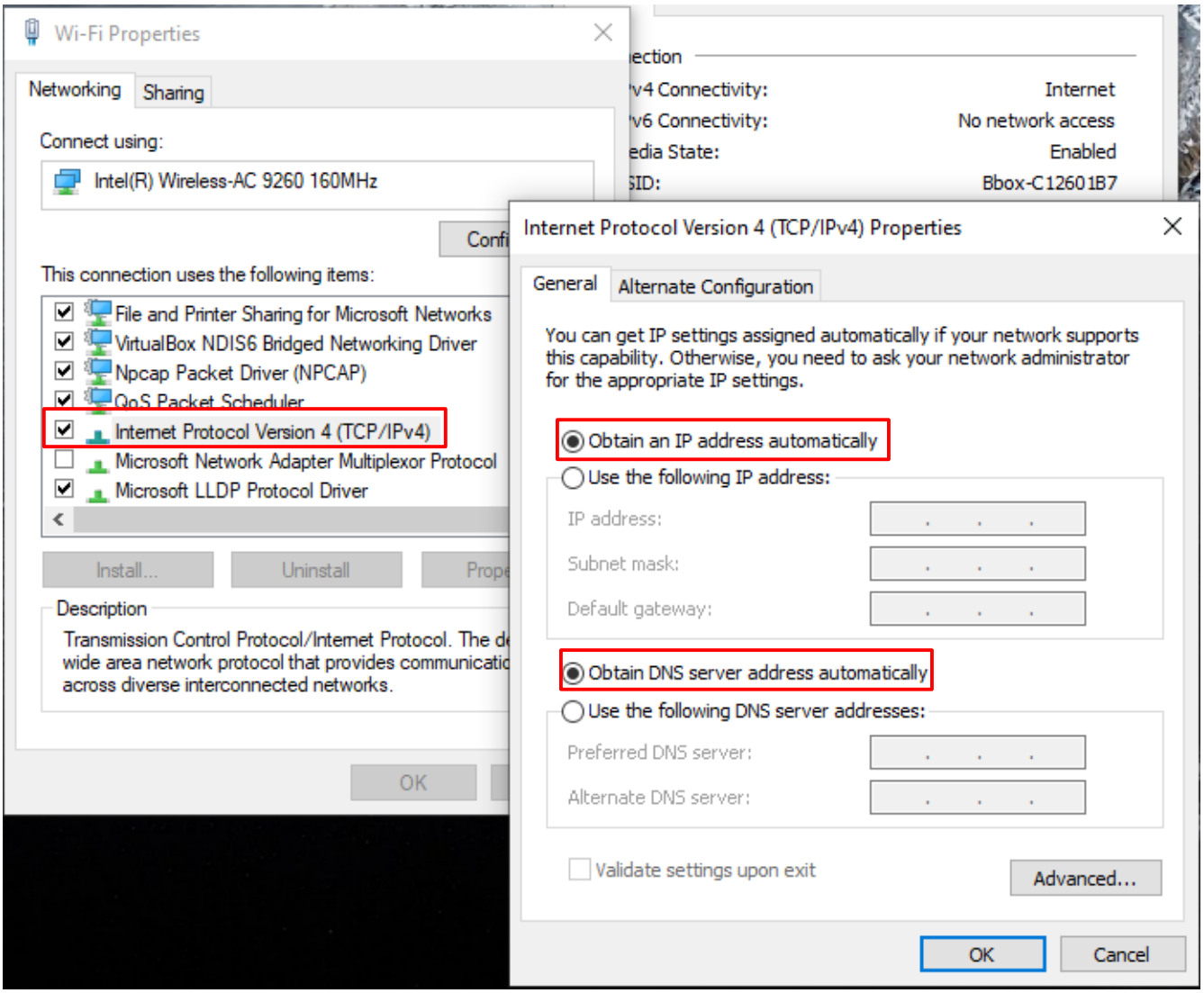
TP4 : analyse de trames DHCP avec Wireshark

Sommaire

1. Capture de trames DHCP avec Wireshark.....2
2. Etude de la trame DHCP DISCOVER.....6

1. Capture de trames DHCP avec Wireshark

→ On modifie les propriétés de **TCP/IPv4** de manière à obtenir les paramètres IP **automatiquement** :



3

→ On saisit la commande **ipconfig /all** dans l'invite de commande :

```
Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . : lan
   Description . . . . . . . . . . . : Intel(R) Wireless-AC 9260 160MHz
   Physical Address. . . . . . . . . : D8-3B-BF-B7-EB-84
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   IPv4 Address. . . . . . . . . . . : 192.168.1.16(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : Thursday, October 17, 2024 6:05:54 PM
   Lease Expires . . . . . . . . . . : Friday, October 18, 2024 6:59:39 PM
   Default Gateway . . . . . . . . . : 192.168.1.254
   DHCP Server . . . . . . . . . . . : 192.168.1.254
   DNS Servers . . . . . . . . . . . : 192.168.1.254
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

* L'adresse IP attribuée par la box est l'adresse **192.168.1.16**

* DHCP activé : **Oui**

* Masque de sous-réseau : **255.255.255.0**

* Bail obtenu : **Jeudi 17 Octobre 2024 18:05:54**

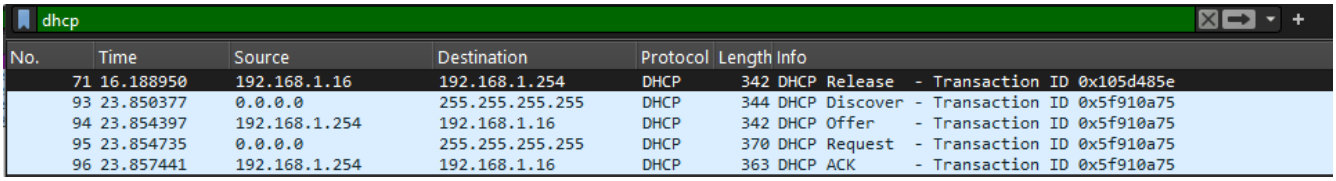
* Bail expirant : **Vendredi 18 Octobre 2024 18:59:39**

* Passerelle par défaut : **192.168.1.254**

* Serveur DHCP : **192.168.1.254**

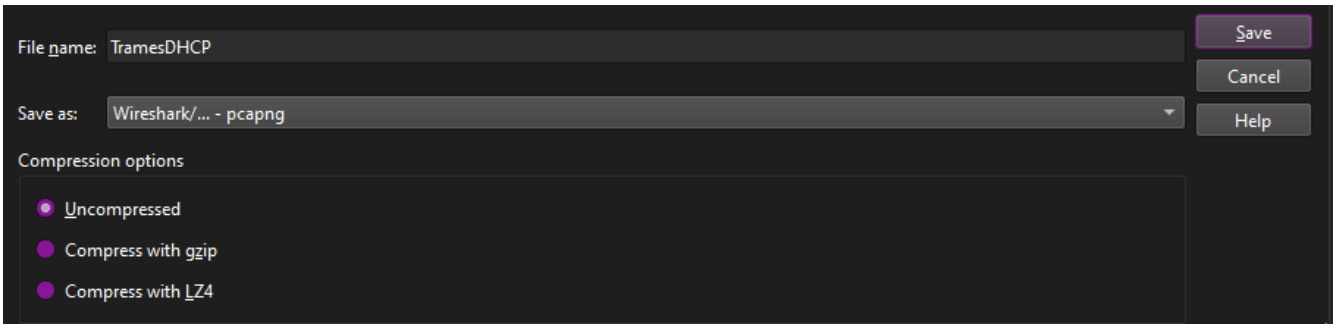
* Serveur DNS : **192.168.1.254**

→ On démarre une **capture de trame** sur WireShark et on tape les commandes **ipconfig /release** puis **ipconfig /renew** pour créer du **traffic** :



4

→ On arrête la capture de trames et on **enregistre** les informations capturées dans un fichier TramesDHCP :



→ Renseignements obtenus à l'aide de la commande **ipconfig /release** :

```
Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   Default Gateway . . . . . . . . . :
```

***** Adresse IPv4 : **0.0.0.0 (aucune)**

***** Masque de sous réseau : **0.0.0.0 (aucun)**

***** Passerelle par défaut : **255.255.255.255 (broadcast)**

→ Renseignements obtenus à l'aide de la commande **ipconfig /renew** :

```
Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . : lan
   IPv4 Address. . . . . . . . . . . : 192.168.1.16
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.1.254
```

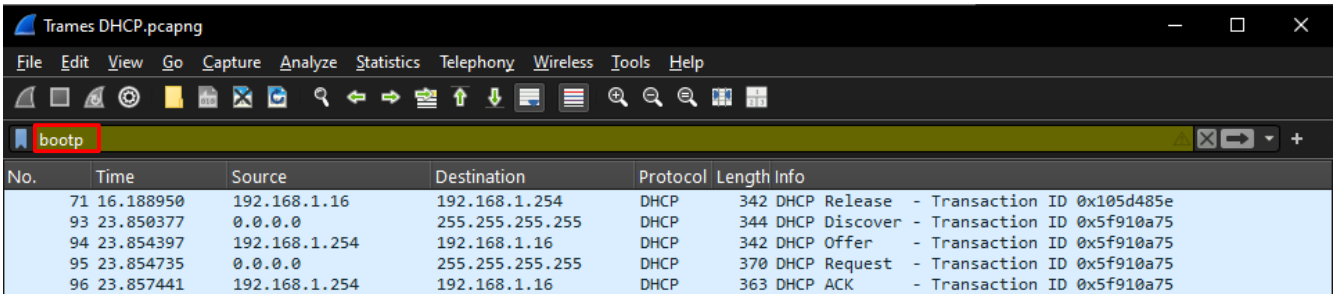
***** Adresse IPv4 : **192.168.1.16**

***** Masque de sous réseau : **255.255.255.0**

***** Passerelle par défaut : **192.168.1.254**

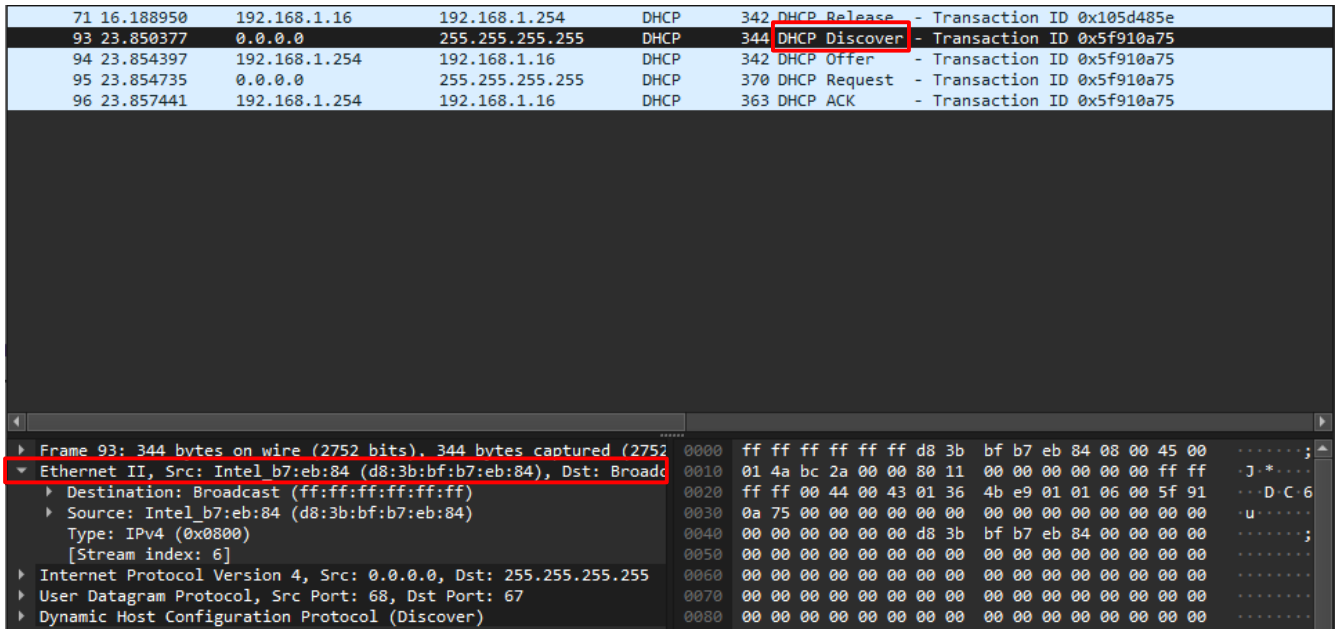
5

→ On ouvre le fichier **TramesDHCP** enregistré juste avant et on applique un filtre **bootp** :



2. Etude de la trame DHCP DISCOVER

→ On développe l'**en-tête Ethernet** de la trame **DHCP Discover** :



***** Adresse MAC source : **FF:FF:FF:FF:FF:FF (broadcast)**

***** Adresse MAC destination : **D8:3B:BF:B7:EB:84**

***** 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 **Ethertype**.

***** Il contient la valeur **08 00** qui signifie que **l'en-tête Ethernet** transporte un **paquet IPv4**.

***** Les protocoles inclus dans cette trames sont :

- Le protocole **Ethernet**

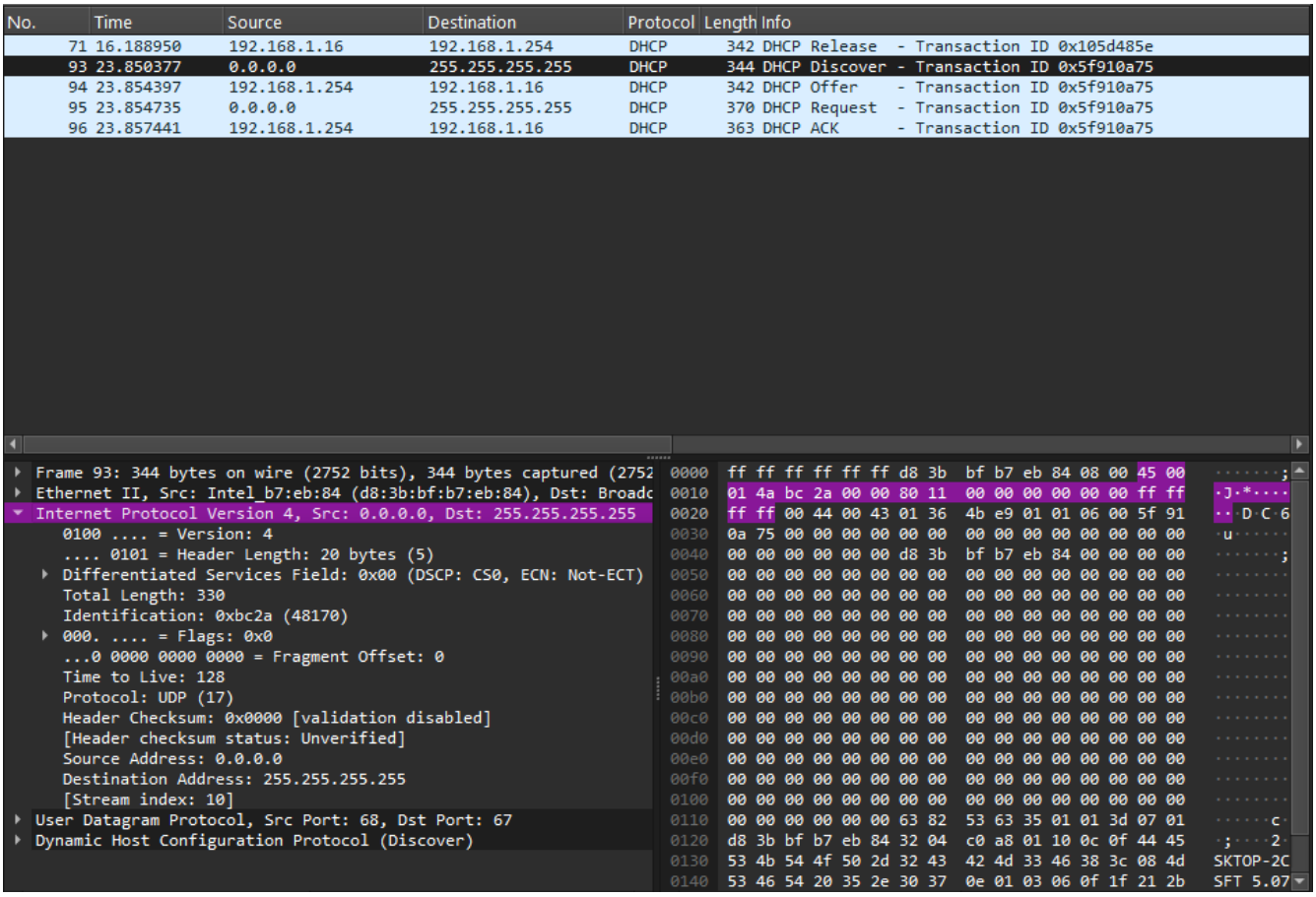
- Le protocole **IP**

- Le protocole **UDP**

- Le protocole **DHCP**

1

→ On développe l'**en-tête réseau** de la trame **DHCP Discover** :



***** Le champ de l'en-tête IP permettant de connaître le protocole de transport des messages DHCP est le champ **Protocole (10ème octet de l'en-tête)**. Ce champ vaut **11** ce qui correspond au protocole **UDP**.

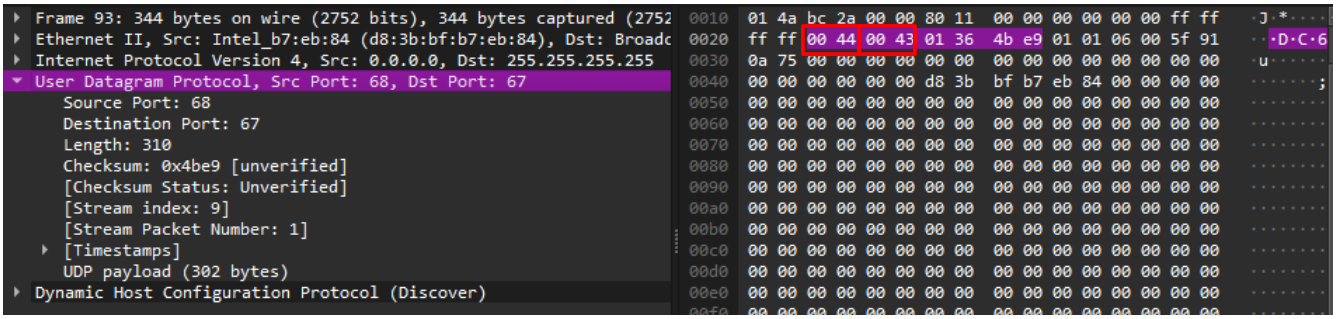
***** Champs de l'en-tête IP :

- Version : **4**
- IHL : **5 / 45**
- Protocole : **17 / 11**
- Adresse source : **0.0.0.0 / 00:00:00:00**
- Adresse destination : **255.255.255.255 / FF:FF:FF:FF**

***** La valeur contenue dans le champ adresse IP source signifie que le client **n'a pas d'adresse IP assignée** et en **demande** une au **serveur DHCP**.

* L'adresse de couche 3 de destination de cette trame est **le port DHCP / BOOTP**.

→ On développe l'**en-tête de transport** de la trame **DHCP Discover** :



* 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 **68 (00 44)**.

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

* Le **port UDP** utilisé par le **serveur** DHCP pour écouter et recevoir la requête du client est le port **67 (00 43)**.

→ On développe la section **Bootstrap Protocol** contenu dans la trame **DHCP Discover** :