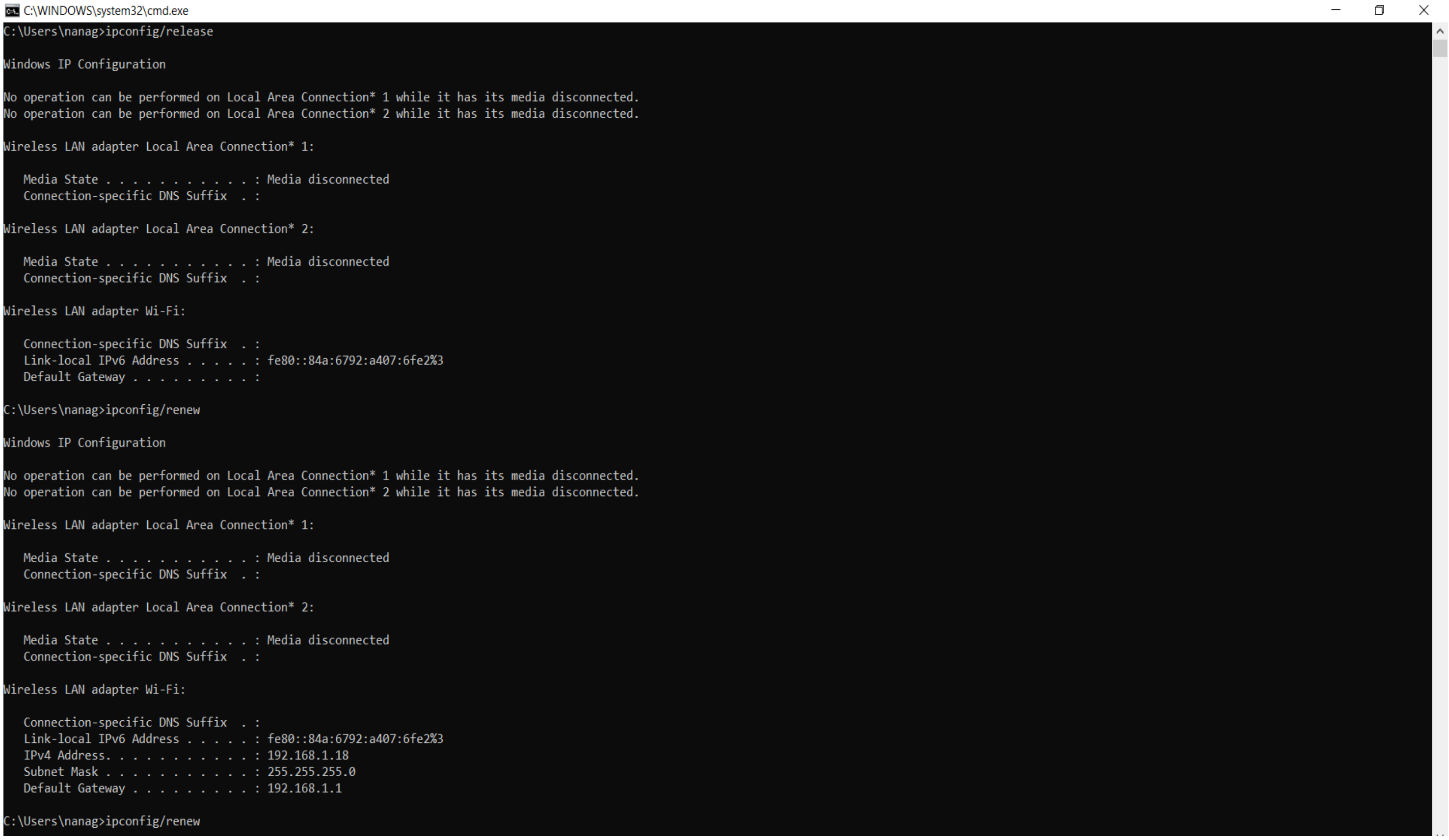
LAB 3

DHCP Experiment

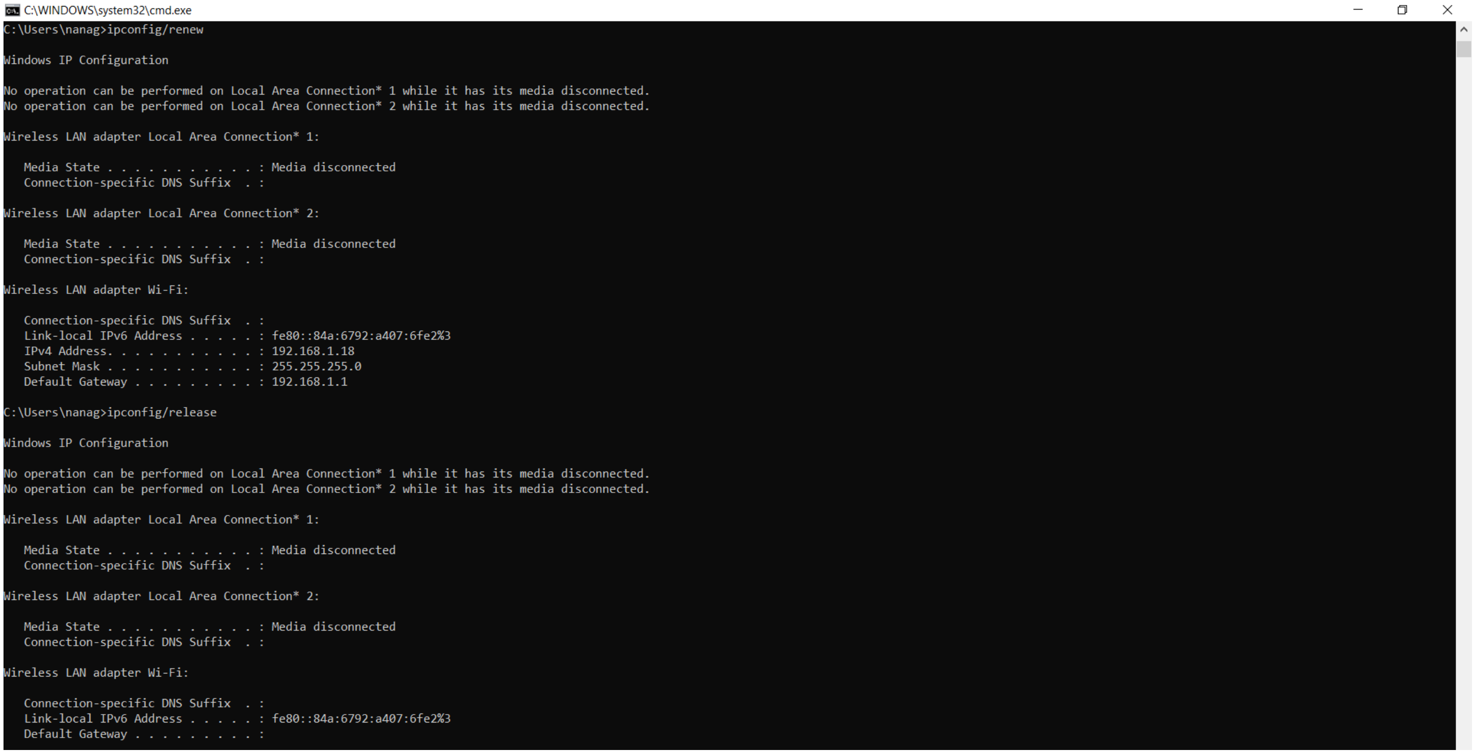
In order to observe DHCP in action, we'll perform several DHCP-related commands and capture the DHCP messages exchanged as a result of executing these commands. Do the following2 :

1. Begin by opening the Windows Command Prompt application (which can be found in your Accessories folder). As shown in Figure 1, enter "ipconfig /release". The executable for ipconfig is in C:\windows\system32. This command releases your current IP address, so that your host's IP address becomes 0.0.0.0.
2. Start up the Wireshark packet sniffer, as described in the introductory Wireshark lab and begin Wireshark packet capture.
3. Now go back to the Windows Command Prompt and enter "ipconfig /renew". This instructs your host to obtain a network configuration, including a new IP address. In Figure 1, the host obtains the IP address 192.168.1.108
4. Wait until the "ipconfig /renew" has terminated. Then enter the same command "ipconfig /renew" again.
5. When the second "ipconfig /renew" terminates, enter the command "ipconfig/release" to release the previously-allocated IP address to your computer.
6. Finally, enter "ipconfig /renew" to again be allocated an IP address for your computer.
7.
8. Stop Wireshark packet capture.

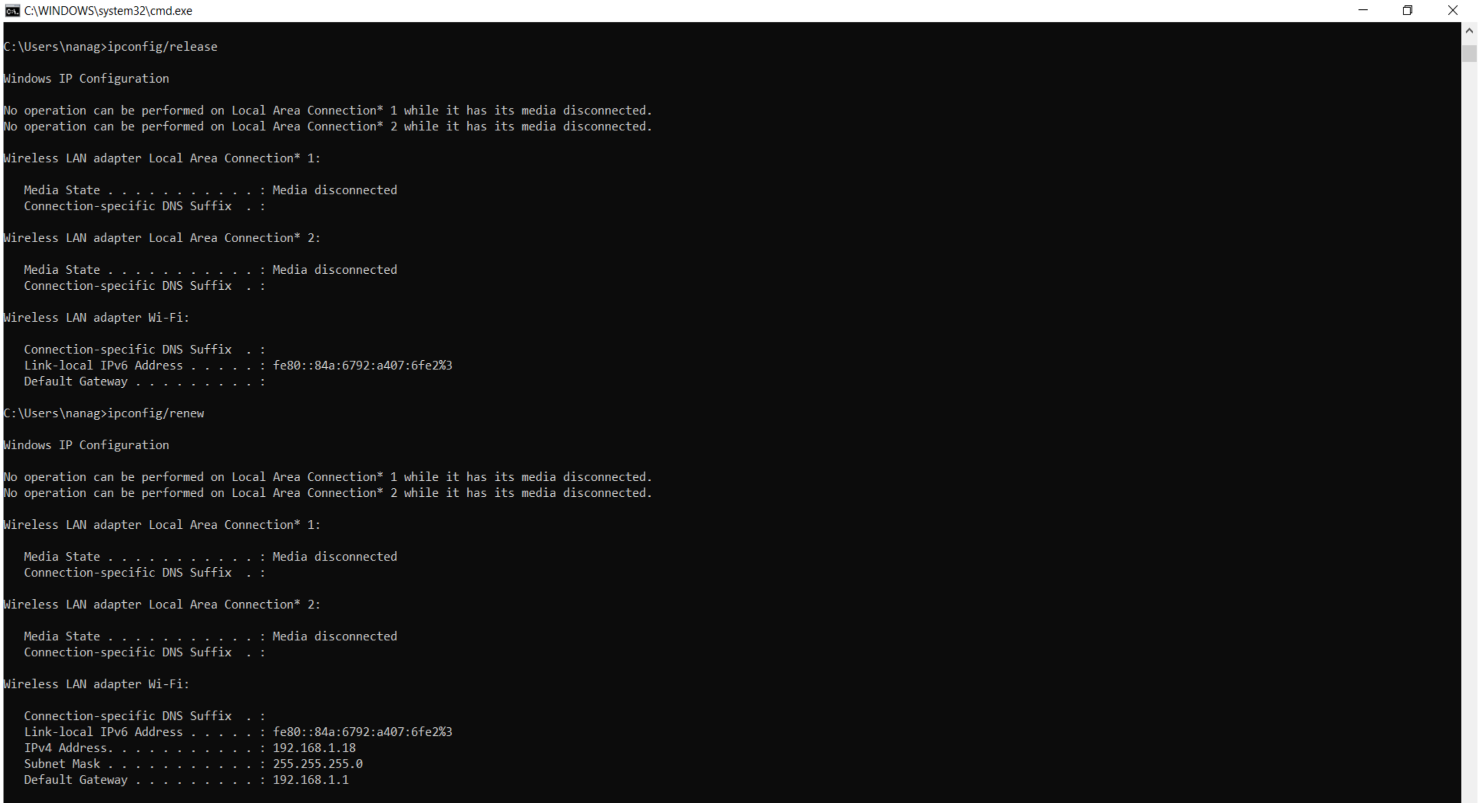


```
C:\Users\nanag>ipconfig/release

Windows IP Configuration

No operation can be performed on Local Area Connection* 1 while it has its media disconnected.
No operation can be performed on Local Area Connection* 2 while it has its media disconnected.

Wireless LAN adapter Local Area Connection* 1:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 2:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::84a:6792:a407:6fe2%3
   Default Gateway . . . . . . . . . :

C:\Users\nanag>ipconfig/renew

Windows IP Configuration

No operation can be performed on Local Area Connection* 1 while it has its media disconnected.
No operation can be performed on Local Area Connection* 2 while it has its media disconnected.

Wireless LAN adapter Local Area Connection* 1:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 2:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::84a:6792:a407:6fe2%3
   IPv4 Address. . . . . . . . . . . : 192.168.1.18
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.1.1

C:\Users\nanag>ipconfig/renew
```

LAB 3



```
C:\Users\nanag>ipconfig/renew

Windows IP Configuration

No operation can be performed on Local Area Connection* 1 while it has its media disconnected.
No operation can be performed on Local Area Connection* 2 while it has its media disconnected.

Wireless LAN adapter Local Area Connection* 1:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 2:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::84a:6792:a407:6fe2%3
   IPv4 Address. . . . . . . . . . . : 192.168.1.18
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.1.1

C:\Users\nanag>ipconfig/release

Windows IP Configuration

No operation can be performed on Local Area Connection* 1 while it has its media disconnected.
No operation can be performed on Local Area Connection* 2 while it has its media disconnected.

Wireless LAN adapter Local Area Connection* 1:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 2:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::84a:6792:a407:6fe2%3
   Default Gateway . . . . . . . . . :
```



```
C:\Users\nanag>ipconfig/release

Windows IP Configuration

No operation can be performed on Local Area Connection* 1 while it has its media disconnected.
No operation can be performed on Local Area Connection* 2 while it has its media disconnected.

Wireless LAN adapter Local Area Connection* 1:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 2:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::84a:6792:a407:6fe2%3
   Default Gateway . . . . . . . . . :

C:\Users\nanag>ipconfig/renew

Windows IP Configuration

No operation can be performed on Local Area Connection* 1 while it has its media disconnected.
No operation can be performed on Local Area Connection* 2 while it has its media disconnected.

Wireless LAN adapter Local Area Connection* 1:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 2:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::84a:6792:a407:6fe2%3
   IPv4 Address. . . . . . . . . . . : 192.168.1.18
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.1.1
```

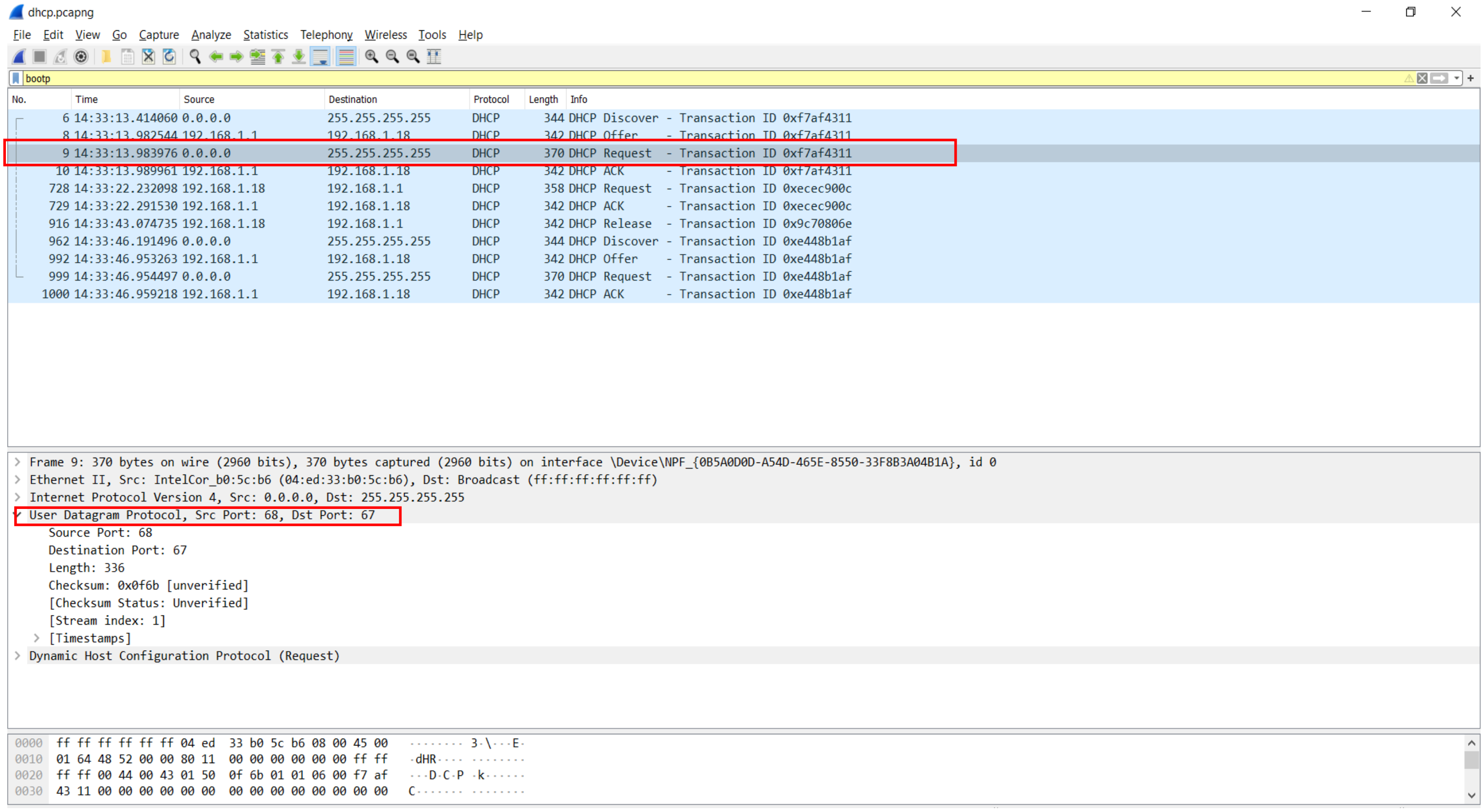
LAB 3

What to Hand In:

You should hand in a screen shot of the Command Prompt window similar to Figure 1 above. Whenever possible, when answering a question below, you should hand in a printout of the packet(s) within the trace that you used to answer the question asked. Annotate the printout3 to explain your answer. To print a packet, use File->Print, choose Selected packet only, choose Packet summary line, and select the minimum amount of packet detail that you need to answer the question. Answer the following questions:

1. Are DHCP messages sent over UDP or TCP?

Solution 1: DHCP messages are sent over UDP.



dhcp.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

bootp

```
No.   Time            Source        Destination      Protocol Length Info
    6 14:33:13.414060 0.0.0.0       255.255.255.255  DHCP      344 DHCP Discover - Transaction ID 0xf7af4311
    8 14:33:13.982544 192.168.1.1   192.168.1.18     DHCP      342 DHCP Offer    - Transaction ID 0xf7af4311
    9 14:33:13.983976 0.0.0.0       255.255.255.255  DHCP      370 DHCP Request  - Transaction ID 0xf7af4311
   10 14:33:13.989961 192.168.1.1   192.168.1.18     DHCP      342 DHCP ACK      - Transaction ID 0xf7af4311
  728 14:33:22.232098 192.168.1.18  192.168.1.1      DHCP      358 DHCP Request  - Transaction ID 0xecec900c
  729 14:33:22.291530 192.168.1.1   192.168.1.18     DHCP      342 DHCP ACK      - Transaction ID 0xecec900c
  916 14:33:43.074735 192.168.1.18  192.168.1.1      DHCP      342 DHCP Release  - Transaction ID 0x9c70806e
  962 14:33:46.191496 0.0.0.0       255.255.255.255  DHCP      344 DHCP Discover - Transaction ID 0xe448b1af
  992 14:33:46.953263 192.168.1.1   192.168.1.18     DHCP      342 DHCP Offer    - Transaction ID 0xe448b1af
  999 14:33:46.954497 0.0.0.0       255.255.255.255  DHCP      370 DHCP Request  - Transaction ID 0xe448b1af
 1000 14:33:46.959218 192.168.1.1   192.168.1.18     DHCP      342 DHCP ACK      - Transaction ID 0xe448b1af
```

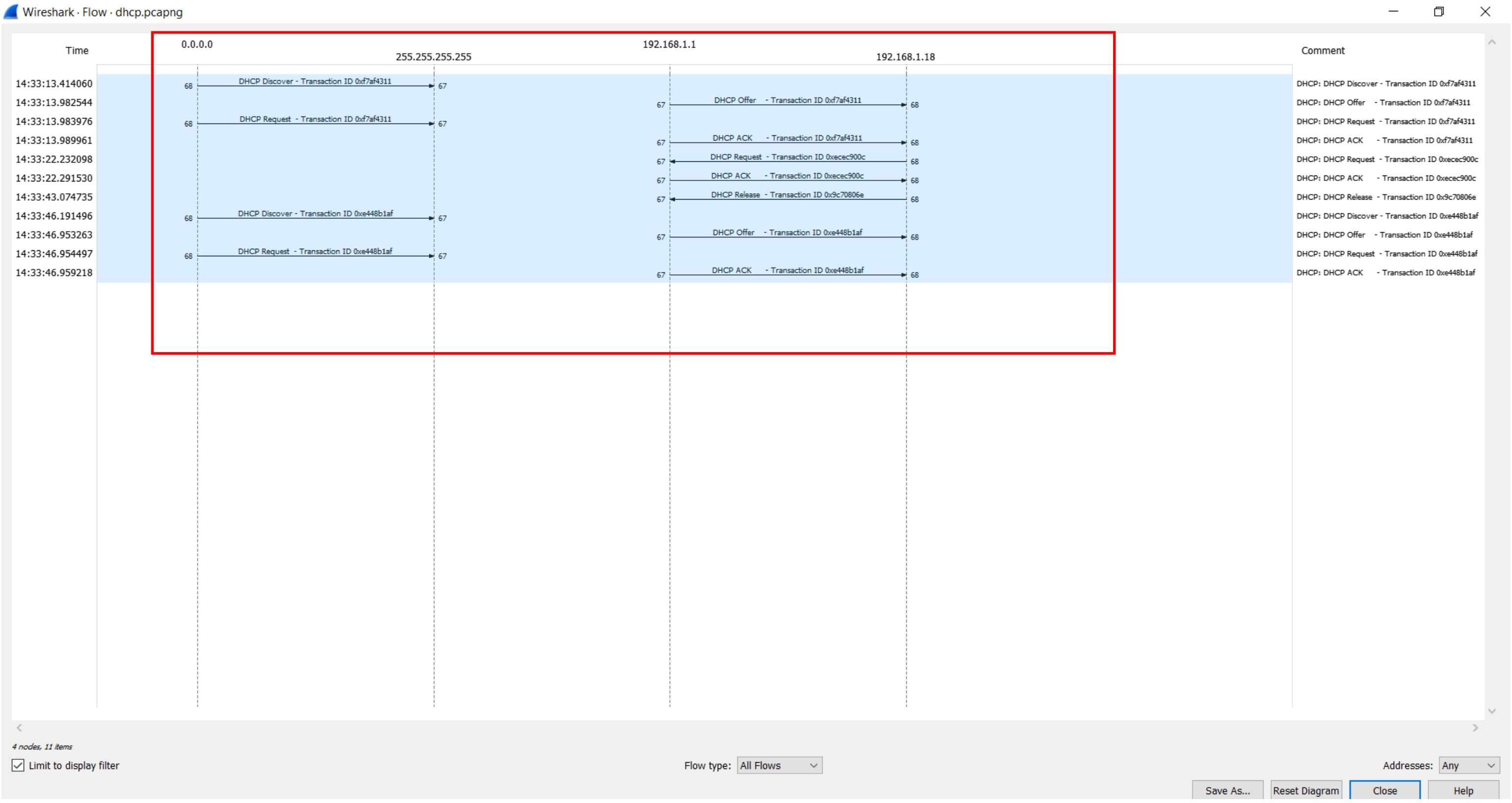
```
> Frame 9: 370 bytes on wire (2960 bits), 370 bytes captured (2960 bits) on interface \Device\NPF_{0B5A0D0D-A54D-465E-8550-33F8B3A04B1A}, id 0
> Ethernet II, Src: IntelCor_b0:5c:b6 (04:ed:33:b0:5c:b6), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
> Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.255.255.255
v User Datagram Protocol, Src Port: 68, Dst Port: 67
    Source Port: 68
    Destination Port: 67
    Length: 336
    Checksum: 0x0f6b [unverified]
    [Checksum Status: Unverified]
    [Stream index: 1]
  > [Timestamps]
> Dynamic Host Configuration Protocol (Request)
```

```
0000  ff ff ff ff ff ff 04 ed  33 b0 5c b6 08 00 45 00   ········ 3·\···E·
0010  01 64 48 52 00 00 80 11  00 00 00 00 00 00 ff ff   ·dHR···· ········
0020  ff ff 00 44 00 43 01 50  0f 6b 01 01 06 00 f7 af   ···D·C·P ·k······
0030  43 11 00 00 00 00 00 00  00 00 00 00 00 00 00 00   C······· ········
```

LAB 3

2. Draw a timing datagram illustrating the sequence of the first four-packet Discover/Offer/Request/ACK DHCP exchange between the client and server. For each packet, indicated the source and destination port numbers. Are the port numbers the same as in the example given in this lab assignment?

   Solution 2: Yes, all the port numbers are same as in the example given in this lab assignment. i.e. 67,68.



```
Time                 Comment
14:33:13.414060      DHCP: DHCP Discover - Transaction ID 0xf7af4311
14:33:13.982544      DHCP: DHCP Offer    - Transaction ID 0xf7af4311
14:33:13.983976      DHCP: DHCP Request  - Transaction ID 0xf7af4311
14:33:13.989961      DHCP: DHCP ACK      - Transaction ID 0xf7af4311
14:33:22.232098      DHCP: DHCP Request  - Transaction ID 0xecec900c
14:33:22.291530      DHCP: DHCP ACK      - Transaction ID 0xecec900c
14:33:43.074735      DHCP: DHCP Release  - Transaction ID 0x9c70806e
14:33:46.191496      DHCP: DHCP Discover - Transaction ID 0xe448b1af
14:33:46.953263      DHCP: DHCP Offer    - Transaction ID 0xe448b1af
14:33:46.954497      DHCP: DHCP Request  - Transaction ID 0xe448b1af
14:33:46.959218      DHCP: DHCP ACK      - Transaction ID 0xe448b1af
```

4 nodes, 11 items

☑ Limit to display filter

Flow type: All Flows

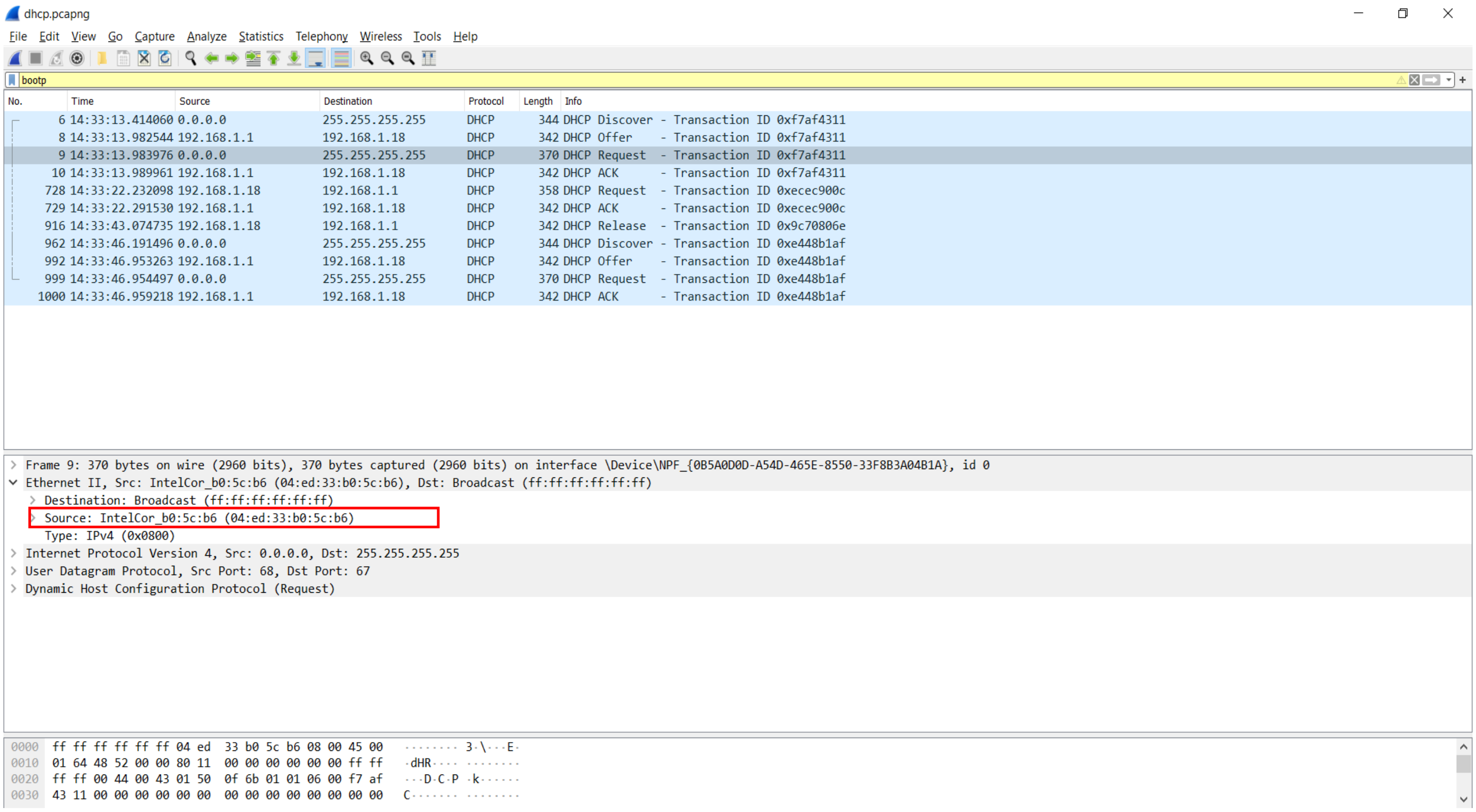
Addresses: Any

	Source Port No.	Destination Port No.
Discover	68	67
Offer	67	68
Request	68	67
ACK	67	68

LAB 3

3. What is the link-layer (e.g., Ethernet) address of your host?

Solution 3: Link-layer (e.g., Ethernet) address of your host – IntelCor_b0:5c:b6(04:ed:33:b0:5c:b6)



```
bootp
```

```
No.     Time            Source          Destination     Protocol Length Info
      6 14:33:13.414060 0.0.0.0         255.255.255.255 DHCP     344 DHCP Discover - Transaction ID 0xf7af4311
      8 14:33:13.982544 192.168.1.1     192.168.1.18    DHCP     342 DHCP Offer    - Transaction ID 0xf7af4311
      9 14:33:13.983976 0.0.0.0         255.255.255.255 DHCP     370 DHCP Request  - Transaction ID 0xf7af4311
     10 14:33:13.989961 192.168.1.1     192.168.1.18    DHCP     342 DHCP ACK      - Transaction ID 0xf7af4311
    728 14:33:22.232098 192.168.1.18    192.168.1.1     DHCP     358 DHCP Request  - Transaction ID 0xecec900c
    729 14:33:22.291530 192.168.1.1     192.168.1.18    DHCP     342 DHCP ACK      - Transaction ID 0xecec900c
    916 14:33:43.074735 192.168.1.18    192.168.1.1     DHCP     342 DHCP Release  - Transaction ID 0x9c70806e
    962 14:33:46.191496 0.0.0.0         255.255.255.255 DHCP     344 DHCP Discover - Transaction ID 0xe448b1af
    992 14:33:46.953263 192.168.1.1     192.168.1.18    DHCP     342 DHCP Offer    - Transaction ID 0xe448b1af
    999 14:33:46.954497 0.0.0.0         255.255.255.255 DHCP     370 DHCP Request  - Transaction ID 0xe448b1af
   1000 14:33:46.959218 192.168.1.1     192.168.1.18    DHCP     342 DHCP ACK      - Transaction ID 0xe448b1af
```

```
> Frame 9: 370 bytes on wire (2960 bits), 370 bytes captured (2960 bits) on interface \Device\NPF_{0B5A0D0D-A54D-465E-8550-33F8B3A04B1A}, id 0
v Ethernet II, Src: IntelCor_b0:5c:b6 (04:ed:33:b0:5c:b6), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
  > Destination: Broadcast (ff:ff:ff:ff:ff:ff)
  > Source: IntelCor_b0:5c:b6 (04:ed:33:b0:5c:b6)
    Type: IPv4 (0x0800)
> 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 (Request)
```

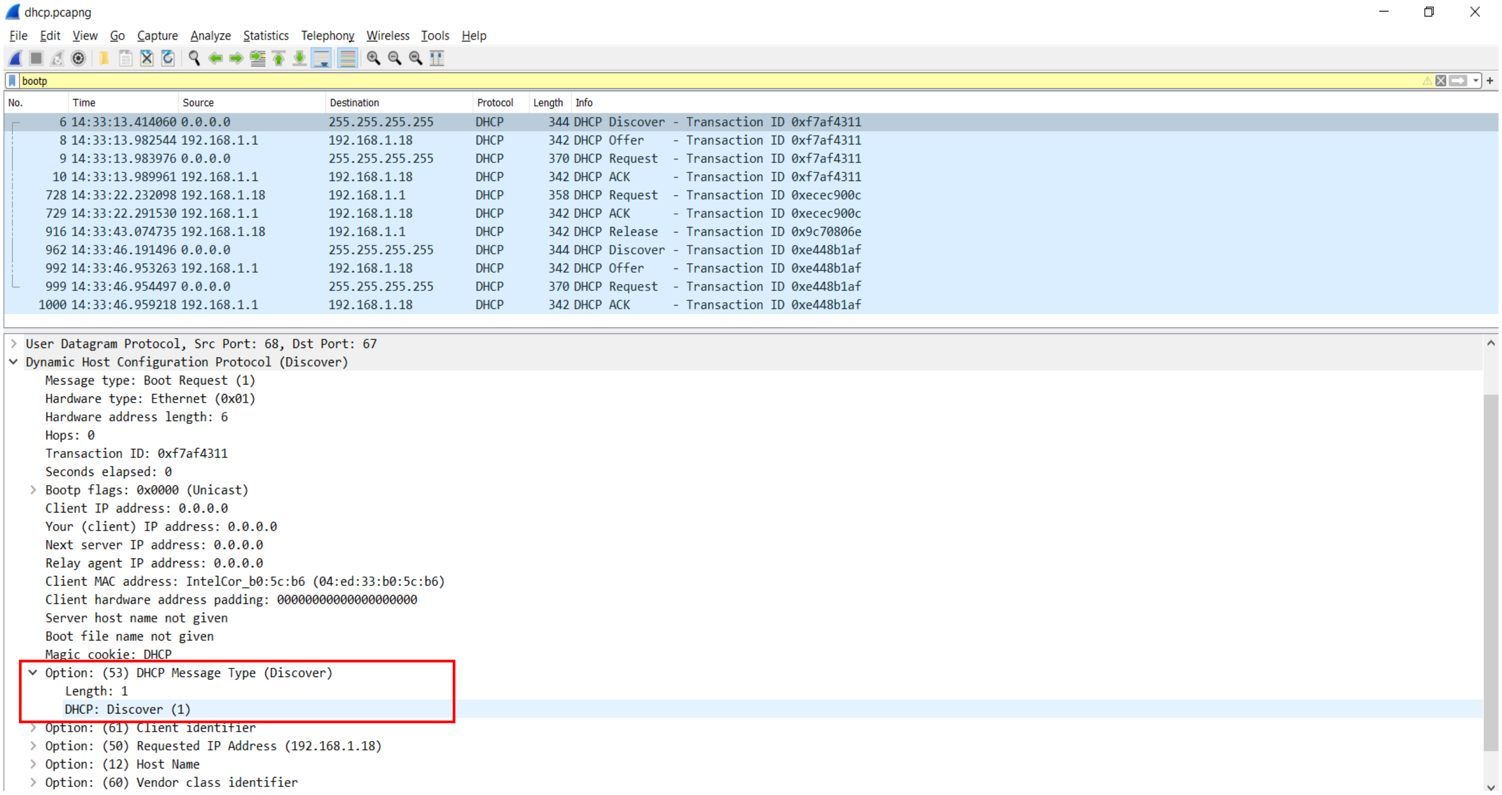
```
0000  ff ff ff ff ff ff 04 ed  33 b0 5c b6 08 00 45 00   ········ 3·\···E·
0010  01 64 48 52 00 00 80 11  00 00 00 00 00 00 ff ff   ·dHR···· ········
0020  ff ff 00 44 00 43 01 50  0f 6b 01 01 06 00 f7 af   ···D·C·P ·k······
0030  43 11 00 00 00 00 00 00  00 00 00 00 00 00 00 00   C······· ········
```

4. What values in the DHCP discover message differentiate this message from the DHCP request message?

Solution 4:

The Message type values differentiate DHCP discover & DHCP request message.

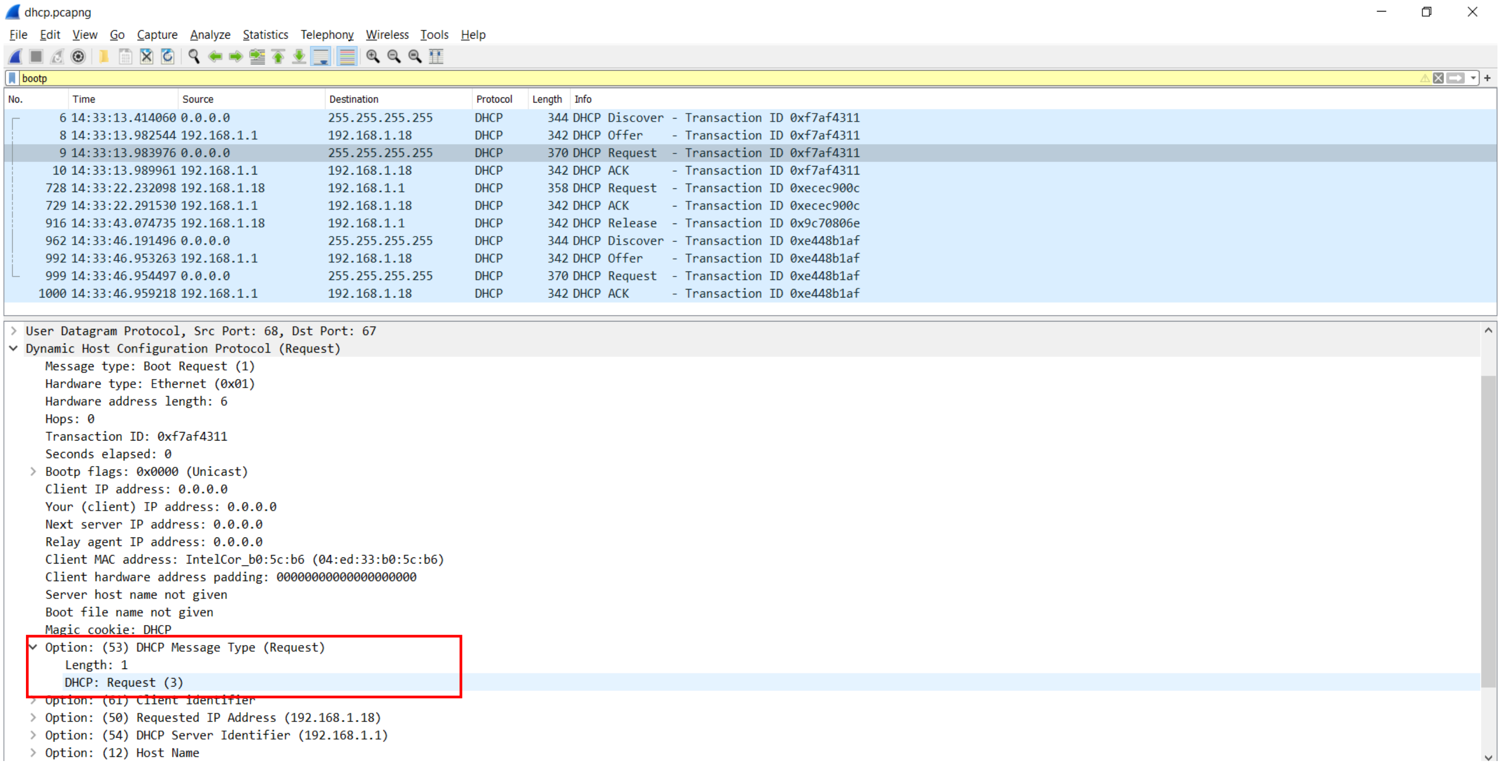
	Message Type Value
DHCP request	3
DHCP discover	1


dhcp.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
bootp

```
No.   Time            Source        Destination      Protocol Length Info
    6 14:33:13.414060 0.0.0.0       255.255.255.255  DHCP     344 DHCP Discover - Transaction ID 0xf7af4311
    8 14:33:13.982544 192.168.1.1   192.168.1.18     DHCP     342 DHCP Offer    - Transaction ID 0xf7af4311
    9 14:33:13.983976 0.0.0.0       255.255.255.255  DHCP     370 DHCP Request  - Transaction ID 0xf7af4311
   10 14:33:13.989961 192.168.1.1   192.168.1.18     DHCP     342 DHCP ACK      - Transaction ID 0xf7af4311
  728 14:33:22.232098 192.168.1.18  192.168.1.1      DHCP     358 DHCP Request  - Transaction ID 0xecec900c
  729 14:33:22.291530 192.168.1.1   192.168.1.18     DHCP     342 DHCP ACK      - Transaction ID 0xecec900c
  916 14:33:43.074735 192.168.1.18  192.168.1.1      DHCP     342 DHCP Release  - Transaction ID 0x9c70806e
  962 14:33:46.191496 0.0.0.0       255.255.255.255  DHCP     344 DHCP Discover - Transaction ID 0xe448b1af
  992 14:33:46.953263 192.168.1.1   192.168.1.18     DHCP     342 DHCP Offer    - Transaction ID 0xe448b1af
  999 14:33:46.954497 0.0.0.0       255.255.255.255  DHCP     370 DHCP Request  - Transaction ID 0xe448b1af
 1000 14:33:46.959218 192.168.1.1   192.168.1.18     DHCP     342 DHCP ACK      - Transaction ID 0xe448b1af
```

```
> User Datagram Protocol, Src Port: 68, Dst Port: 67
v Dynamic Host Configuration Protocol (Discover)
    Message type: Boot Request (1)
    Hardware type: Ethernet (0x01)
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0xf7af4311
    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: IntelCor_b0:5c:b6 (04:ed:33:b0:5c:b6)
    Client hardware address padding: 00000000000000000000
    Server host name not given
    Boot file name not given
    Magic cookie: DHCP
  v Option: (53) DHCP Message Type (Discover)
      Length: 1
      DHCP: Discover (1)
  > Option: (61) Client identifier
  > Option: (50) Requested IP Address (192.168.1.18)
  > Option: (12) Host Name
  > Option: (60) Vendor class identifier
```

LAB 3


dhcp.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

bootp

```
No.   Time            Source          Destination      Protocol Length Info
    6 14:33:13.414060 0.0.0.0         255.255.255.255  DHCP      344 DHCP Discover - Transaction ID 0xf7af4311
    8 14:33:13.982544 192.168.1.1     192.168.1.18     DHCP      342 DHCP Offer    - Transaction ID 0xf7af4311
    9 14:33:13.983976 0.0.0.0         255.255.255.255  DHCP      370 DHCP Request  - Transaction ID 0xf7af4311
   10 14:33:13.989961 192.168.1.1     192.168.1.18     DHCP      342 DHCP ACK      - Transaction ID 0xf7af4311
  728 14:33:22.232098 192.168.1.18    192.168.1.1      DHCP      358 DHCP Request  - Transaction ID 0xecec900c
  729 14:33:22.291530 192.168.1.1     192.168.1.18     DHCP      342 DHCP ACK      - Transaction ID 0xecec900c
  916 14:33:43.074735 192.168.1.18    192.168.1.1      DHCP      342 DHCP Release  - Transaction ID 0x9c70806e
  962 14:33:46.191496 0.0.0.0         255.255.255.255  DHCP      344 DHCP Discover - Transaction ID 0xe448b1af
  992 14:33:46.953263 192.168.1.1     192.168.1.18     DHCP      342 DHCP Offer    - Transaction ID 0xe448b1af
  999 14:33:46.954497 0.0.0.0         255.255.255.255  DHCP      370 DHCP Request  - Transaction ID 0xe448b1af
 1000 14:33:46.959218 192.168.1.1     192.168.1.18     DHCP      342 DHCP ACK      - Transaction ID 0xe448b1af
```

```
> User Datagram Protocol, Src Port: 68, Dst Port: 67
v Dynamic Host Configuration Protocol (Request)
    Message type: Boot Request (1)
    Hardware type: Ethernet (0x01)
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0xf7af4311
    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: IntelCor_b0:5c:b6 (04:ed:33:b0:5c:b6)
    Client hardware address padding: 00000000000000000000
    Server host name not given
    Boot file name not given
    Magic cookie: DHCP
  v Option: (53) DHCP Message Type (Request)
      Length: 1
      DHCP: Request (3)
  > Option: (61) Client identifier
  > Option: (50) Requested IP Address (192.168.1.18)
  > Option: (54) DHCP Server Identifier (192.168.1.1)
  > Option: (12) Host Name
```

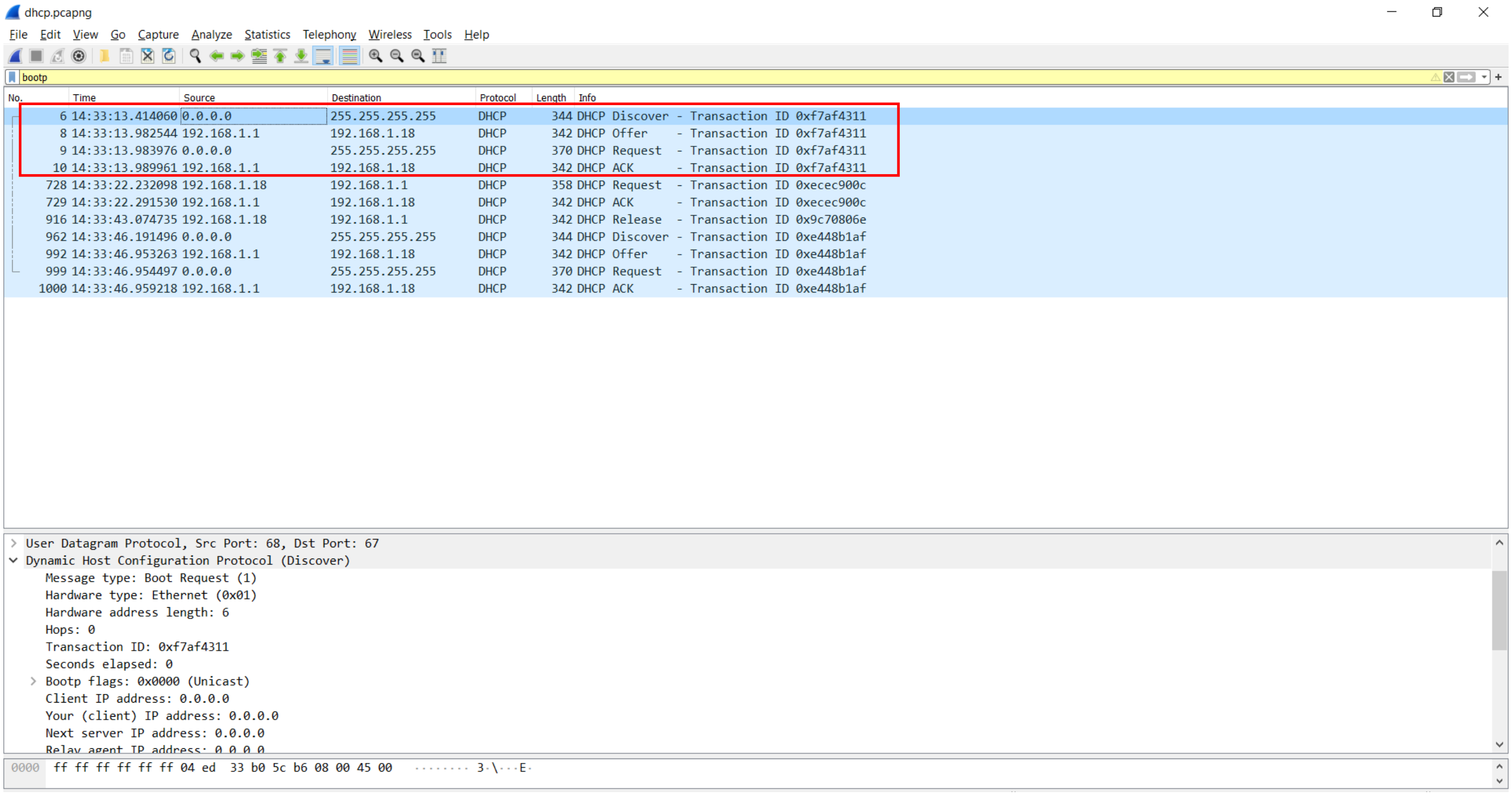
LAB 3

5. What is the value of the Transaction-ID in each of the first four (Discover/Offer/Request/ACK) DHCP messages? What are the values of the Transaction-ID in the second set (Request/ACK) set of DHCP messages? What is the purpose of the Transaction-ID field?

Solution 5:

The purpose of the Transaction-ID field is to differentiate between different requests made by the user or client. (i.e. to differentiate between multiple requests if any)

First DHCP messages	**Transaction-ID**
Discover	0xf7a4311
Offer	0xf7a4311
Request	0xf7a4311
ACK	0xf7a4311



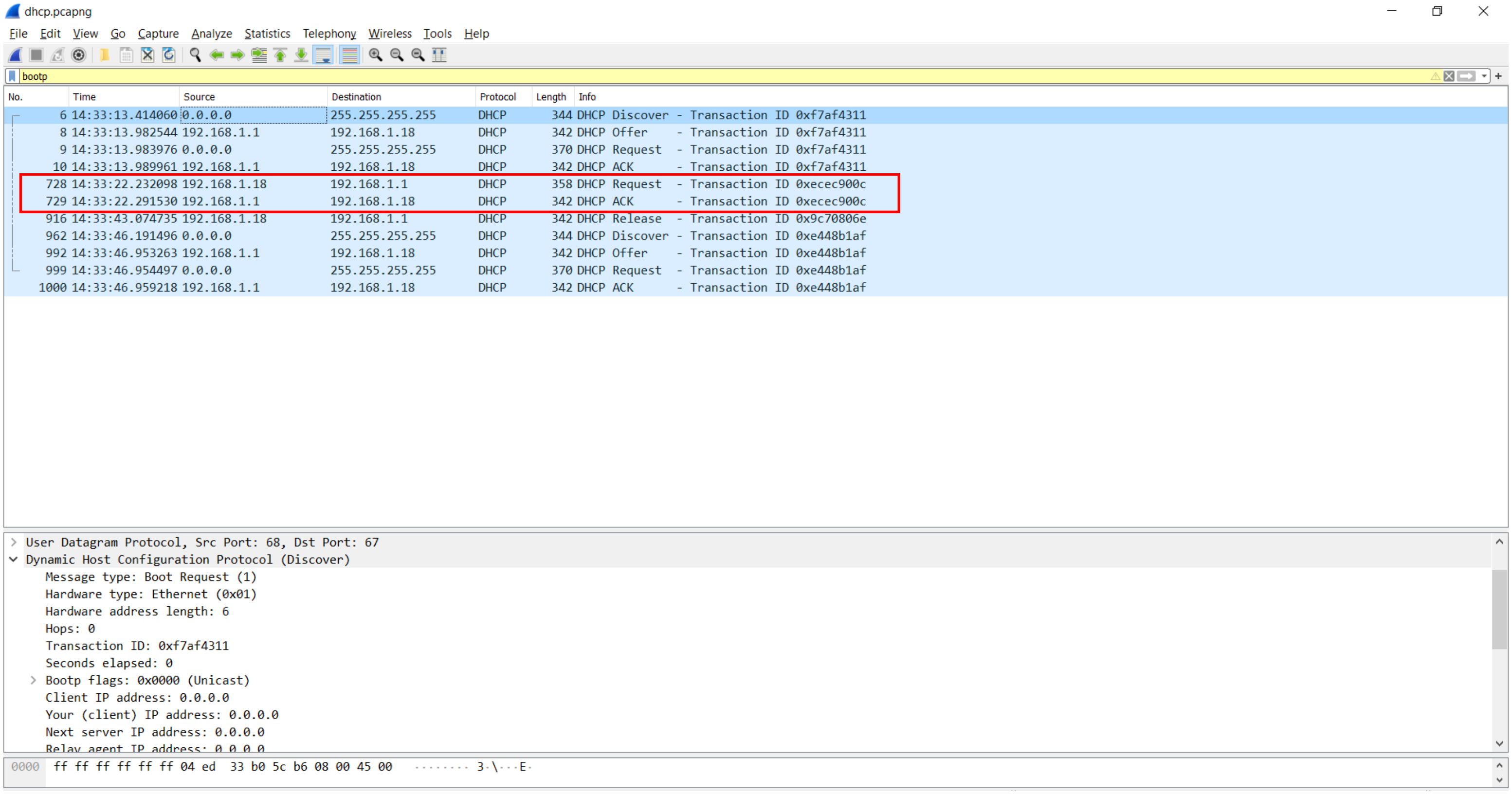
```
No.   Time            Source        Destination      Protocol Length Info
    6 14:33:13.414060 0.0.0.0       255.255.255.255  DHCP     344 DHCP Discover - Transaction ID 0xf7af4311
    8 14:33:13.982544 192.168.1.1   192.168.1.18     DHCP     342 DHCP Offer    - Transaction ID 0xf7af4311
    9 14:33:13.983976 0.0.0.0       255.255.255.255  DHCP     370 DHCP Request  - Transaction ID 0xf7af4311
   10 14:33:13.989961 192.168.1.1   192.168.1.18     DHCP     342 DHCP ACK      - Transaction ID 0xf7af4311
  728 14:33:22.232098 192.168.1.18  192.168.1.1      DHCP     358 DHCP Request  - Transaction ID 0xecec900c
  729 14:33:22.291530 192.168.1.1   192.168.1.18     DHCP     342 DHCP ACK      - Transaction ID 0xecec900c
  916 14:33:43.074735 192.168.1.18  192.168.1.1      DHCP     342 DHCP Release  - Transaction ID 0x9c70806e
  962 14:33:46.191496 0.0.0.0       255.255.255.255  DHCP     344 DHCP Discover - Transaction ID 0xe448b1af
  992 14:33:46.953263 192.168.1.1   192.168.1.18     DHCP     342 DHCP Offer    - Transaction ID 0xe448b1af
  999 14:33:46.954497 0.0.0.0       255.255.255.255  DHCP     370 DHCP Request  - Transaction ID 0xe448b1af
 1000 14:33:46.959218 192.168.1.1   192.168.1.18     DHCP     342 DHCP ACK      - Transaction ID 0xe448b1af
```

```
> User Datagram Protocol, Src Port: 68, Dst Port: 67
v Dynamic Host Configuration Protocol (Discover)
    Message type: Boot Request (1)
    Hardware type: Ethernet (0x01)
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0xf7af4311
    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
```

```
0000  ff ff ff ff ff ff 04 ed  33 b0 5c b6 08 00 45 00   ········ 3·\···E·
```

LAB 3

Second DHCP messages	Transaction-ID
Request	0xecec900c
ACK	0xecec900c



dhcp.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

bootp

```
No.  Time            Source        Destination      Protocol Length Info
   6 14:33:13.414060 0.0.0.0       255.255.255.255  DHCP     344 DHCP Discover - Transaction ID 0xf7af4311
   8 14:33:13.982544 192.168.1.1   192.168.1.18     DHCP     342 DHCP Offer    - Transaction ID 0xf7af4311
   9 14:33:13.983976 0.0.0.0       255.255.255.255  DHCP     370 DHCP Request  - Transaction ID 0xf7af4311
  10 14:33:13.989961 192.168.1.1   192.168.1.18     DHCP     342 DHCP ACK      - Transaction ID 0xf7af4311
 728 14:33:22.232098 192.168.1.18  192.168.1.1      DHCP     358 DHCP Request  - Transaction ID 0xecec900c
 729 14:33:22.291530 192.168.1.1   192.168.1.18     DHCP     342 DHCP ACK      - Transaction ID 0xecec900c
 916 14:33:43.074735 192.168.1.18  192.168.1.1      DHCP     342 DHCP Release  - Transaction ID 0x9c70806e
 962 14:33:46.191496 0.0.0.0       255.255.255.255  DHCP     344 DHCP Discover - Transaction ID 0xe448b1af
 992 14:33:46.953263 192.168.1.1   192.168.1.18     DHCP     342 DHCP Offer    - Transaction ID 0xe448b1af
 999 14:33:46.954497 0.0.0.0       255.255.255.255  DHCP     370 DHCP Request  - Transaction ID 0xe448b1af
1000 14:33:46.959218 192.168.1.1   192.168.1.18     DHCP     342 DHCP ACK      - Transaction ID 0xe448b1af
```

```
> User Datagram Protocol, Src Port: 68, Dst Port: 67
v Dynamic Host Configuration Protocol (Discover)
    Message type: Boot Request (1)
    Hardware type: Ethernet (0x01)
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0xf7af4311
    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
```

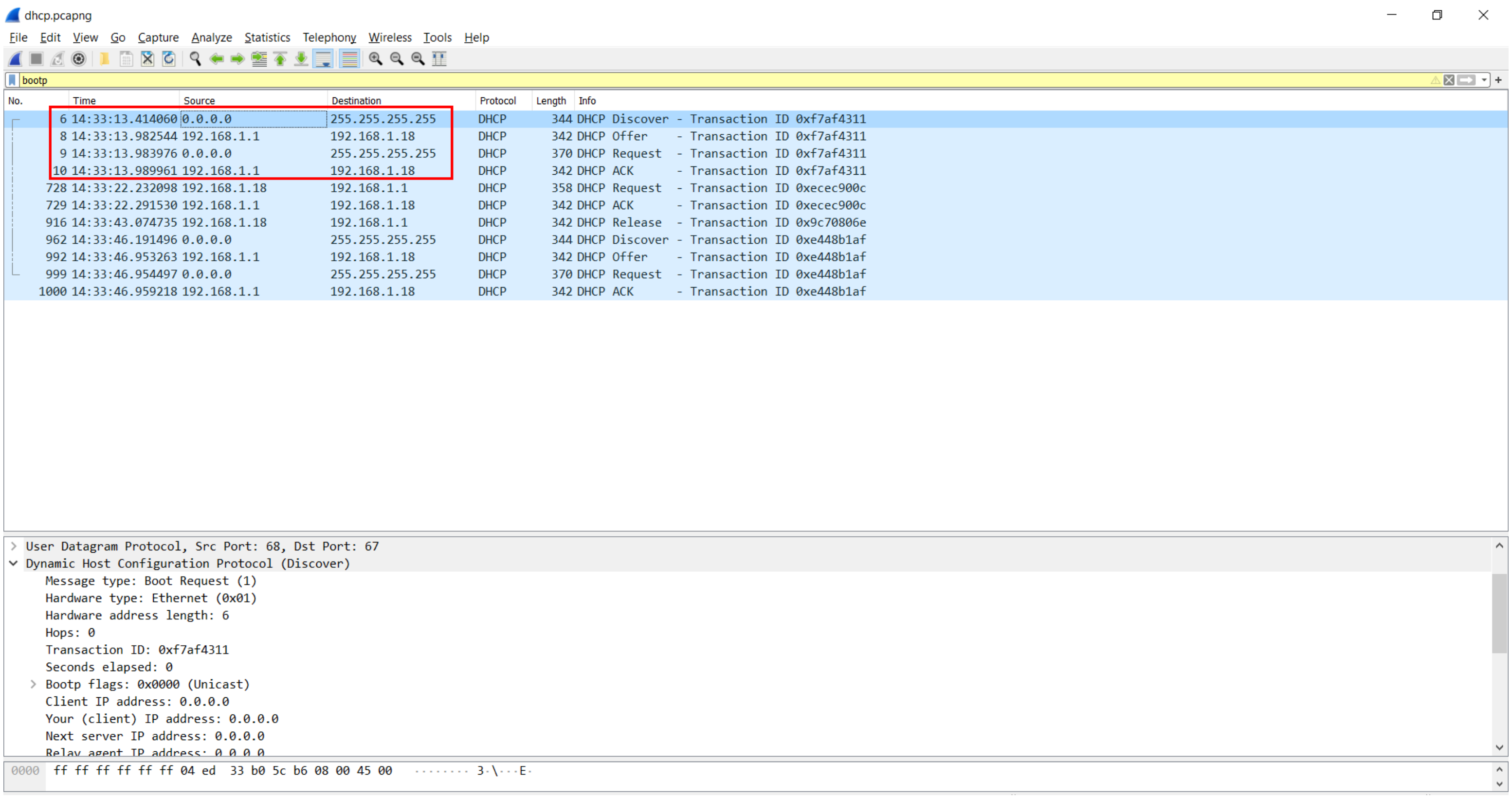
```
0000  ff ff ff ff ff ff 04 ed  33 b0 5c b6 08 00 45 00   ········ 3·\···E·
```

LAB 3

6. A host uses DHCP to obtain an IP address, among other things. But a host's IP address is not confirmed until the end of the four-message exchange! If the IP address is not set until the end of the four-message exchange, then what values are used in the IP datagrams in the four-message exchange? For each of the four DHCP messages (Discover/Offer/Request/ACK DHCP), indicate the source and destination IP addresses that are carried in the encapsulating IP datagram.

Solution 6:

	Source IP address	**Destination IP address**
Discover	0.0.0.0	255.255.255.255
Offer	192.168.1.1	192.168.1.18
Request	0.0.0.0	255.255.255.255
ACK	192.168.1.1	192.168.1.18



bootp

```
No.   Time             Source        Destination      Protocol Length Info
   6 14:33:13.414060 0.0.0.0       255.255.255.255  DHCP     344 DHCP Discover - Transaction ID 0xf7af4311
   8 14:33:13.982544 192.168.1.1   192.168.1.18     DHCP     342 DHCP Offer    - Transaction ID 0xf7af4311
   9 14:33:13.983976 0.0.0.0       255.255.255.255  DHCP     370 DHCP Request  - Transaction ID 0xf7af4311
  10 14:33:13.989961 192.168.1.1   192.168.1.18     DHCP     342 DHCP ACK      - Transaction ID 0xf7af4311
 728 14:33:22.232098 192.168.1.18  192.168.1.1      DHCP     358 DHCP Request  - Transaction ID 0xecec900c
 729 14:33:22.291530 192.168.1.1   192.168.1.18     DHCP     342 DHCP ACK      - Transaction ID 0xecec900c
 916 14:33:43.074735 192.168.1.18  192.168.1.1      DHCP     342 DHCP Release  - Transaction ID 0x9c70806e
 962 14:33:46.191496 0.0.0.0       255.255.255.255  DHCP     344 DHCP Discover - Transaction ID 0xe448b1af
 992 14:33:46.953263 192.168.1.1   192.168.1.18     DHCP     342 DHCP Offer    - Transaction ID 0xe448b1af
 999 14:33:46.954497 0.0.0.0       255.255.255.255  DHCP     370 DHCP Request  - Transaction ID 0xe448b1af
1000 14:33:46.959218 192.168.1.1   192.168.1.18     DHCP     342 DHCP ACK      - Transaction ID 0xe448b1af
```

```
> User Datagram Protocol, Src Port: 68, Dst Port: 67
v Dynamic Host Configuration Protocol (Discover)
    Message type: Boot Request (1)
    Hardware type: Ethernet (0x01)
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0xf7af4311
    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
```

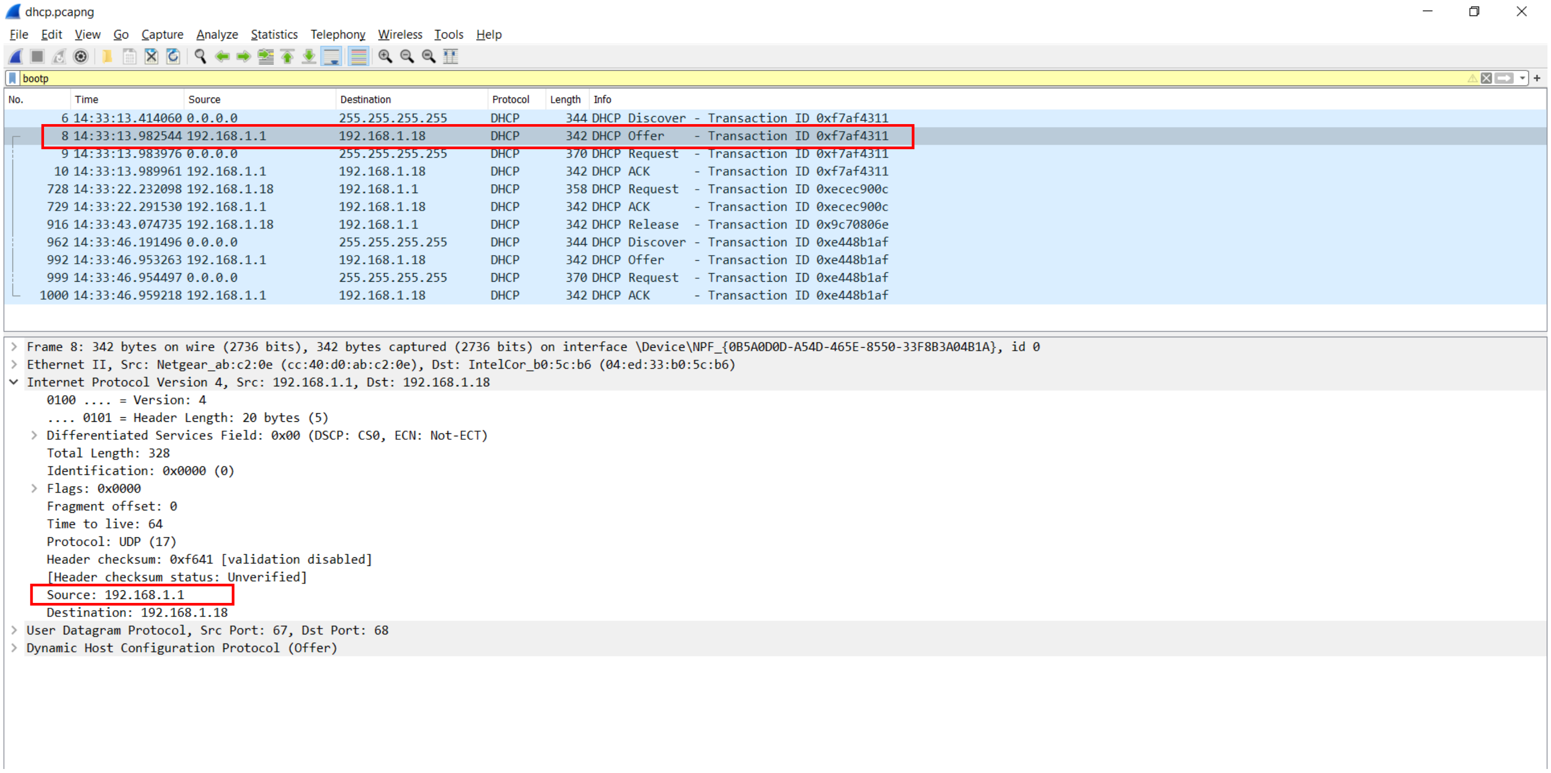
```
0000  ff ff ff ff ff ff 04 ed  33 b0 5c b6 08 00 45 00   ········ 3·\···E·
```

LAB 3

7. What is the IP address of your DHCP server?

   Solution 7:

   IP address of my DHCP Server – 192.168.1.1



dhcp.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
bootp

```
No.   Time            Source        Destination      Protocol  Length Info
    6 14:33:13.414060 0.0.0.0       255.255.255.255  DHCP      344 DHCP Discover - Transaction ID 0xf7af4311
    8 14:33:13.982544 192.168.1.1   192.168.1.18     DHCP      342 DHCP Offer    - Transaction ID 0xf7af4311
    9 14:33:13.983976 0.0.0.0       255.255.255.255  DHCP      370 DHCP Request  - Transaction ID 0xf7af4311
   10 14:33:13.989961 192.168.1.1   192.168.1.18     DHCP      342 DHCP ACK      - Transaction ID 0xf7af4311
  728 14:33:22.232098 192.168.1.18  192.168.1.1      DHCP      358 DHCP Request  - Transaction ID 0xecec900c
  729 14:33:22.291530 192.168.1.1   192.168.1.18     DHCP      342 DHCP ACK      - Transaction ID 0xecec900c
  916 14:33:43.074735 192.168.1.18  192.168.1.1      DHCP      342 DHCP Release  - Transaction ID 0x9c70806e
  962 14:33:46.191496 0.0.0.0       255.255.255.255  DHCP      344 DHCP Discover - Transaction ID 0xe448b1af
  992 14:33:46.953263 192.168.1.1   192.168.1.18     DHCP      342 DHCP Offer    - Transaction ID 0xe448b1af
  999 14:33:46.954497 0.0.0.0       255.255.255.255  DHCP      370 DHCP Request  - Transaction ID 0xe448b1af
 1000 14:33:46.959218 192.168.1.1   192.168.1.18     DHCP      342 DHCP ACK      - Transaction ID 0xe448b1af
```

```
> Frame 8: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) on interface \Device\NPF_{0B5A0D0D-A54D-465E-8550-33F8B3A04B1A}, id 0
> Ethernet II, Src: Netgear_ab:c2:0e (cc:40:d0:ab:c2:0e), Dst: IntelCor_b0:5c:b6 (04:ed:33:b0:5c:b6)
v Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.1.18
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 328
    Identification: 0x0000 (0)
  > Flags: 0x0000
    Fragment offset: 0
    Time to live: 64
    Protocol: UDP (17)
    Header checksum: 0xf641 [validation disabled]
    [Header checksum status: Unverified]
    Source: 192.168.1.1
    Destination: 192.168.1.18
> User Datagram Protocol, Src Port: 67, Dst Port: 68
> Dynamic Host Configuration Protocol (Offer)
```

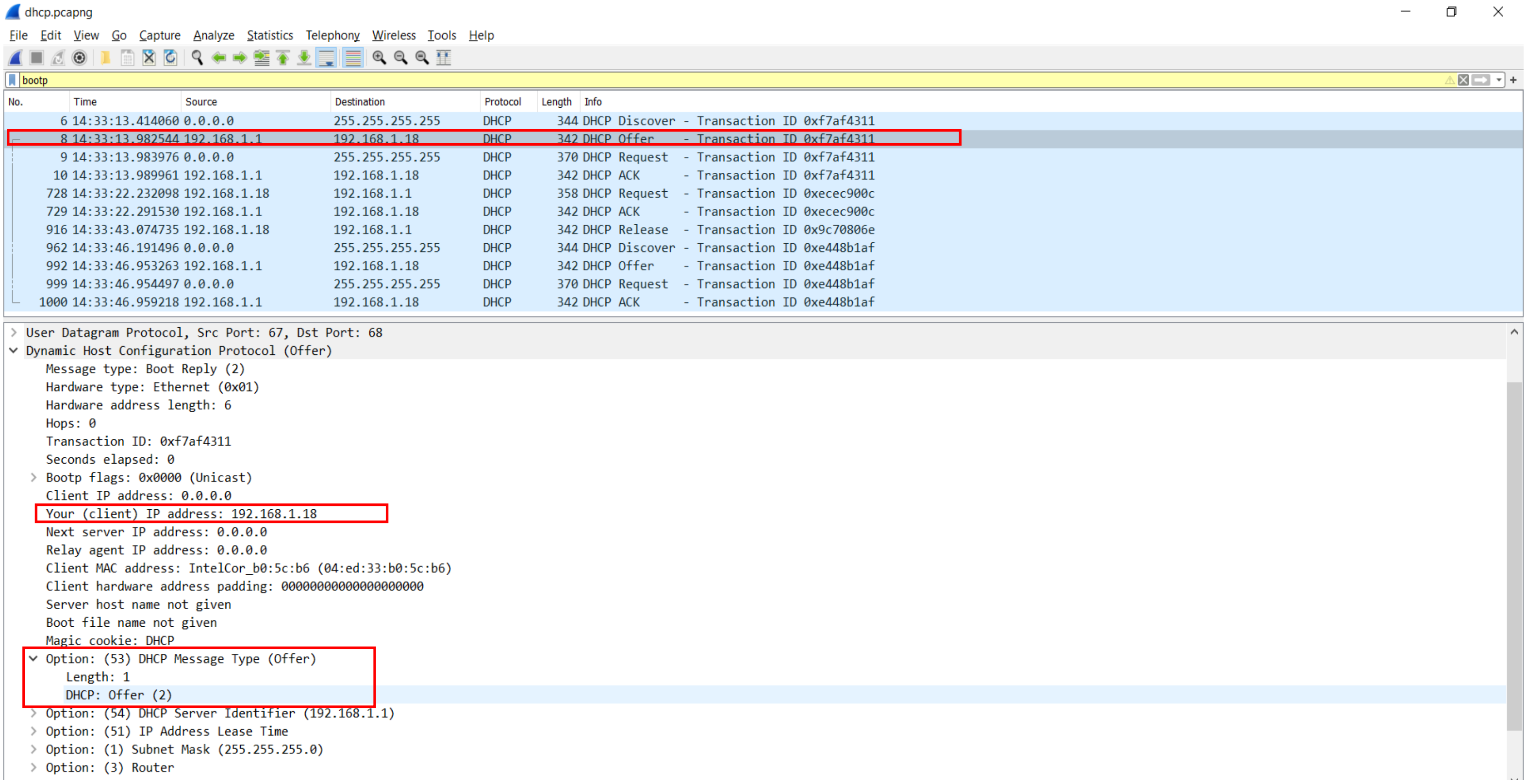
LAB 3

8. What IP address is the DHCP server offering to your host in the DHCP Offer message? Indicate which DHCP message contains the offered DHCP address.

Solution 8 :

The IP address offered by DHCP server in DHCP offer Message – 192.168.1.18

DHCP offer message contains the offered DHCP address.


dhcp.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
bootp

No.	Time	Source	Destination	Protocol	Length	Info
6	14:33:13.414060	0.0.0.0	255.255.255.255	DHCP	344	DHCP Discover - Transaction ID 0xf7af4311
8	14:33:13.982544	192.168.1.1	192.168.1.18	DHCP	342	DHCP Offer - Transaction ID 0xf7af4311
9	14:33:13.983976	0.0.0.0	255.255.255.255	DHCP	370	DHCP Request - Transaction ID 0xf7af4311
10	14:33:13.989961	192.168.1.1	192.168.1.18	DHCP	342	DHCP ACK - Transaction ID 0xf7af4311
728	14:33:22.232098	192.168.1.18	192.168.1.1	DHCP	358	DHCP Request - Transaction ID 0xecec900c
729	14:33:22.291530	192.168.1.1	192.168.1.18	DHCP	342	DHCP ACK - Transaction ID 0xecec900c
916	14:33:43.074735	192.168.1.18	192.168.1.1	DHCP	342	DHCP Release - Transaction ID 0x9c70806e
962	14:33:46.191496	0.0.0.0	255.255.255.255	DHCP	344	DHCP Discover - Transaction ID 0xe448b1af
992	14:33:46.953263	192.168.1.1	192.168.1.18	DHCP	342	DHCP Offer - Transaction ID 0xe448b1af
999	14:33:46.954497	0.0.0.0	255.255.255.255	DHCP	370	DHCP Request - Transaction ID 0xe448b1af
1000	14:33:46.959218	192.168.1.1	192.168.1.18	DHCP	342	DHCP ACK - Transaction ID 0xe448b1af

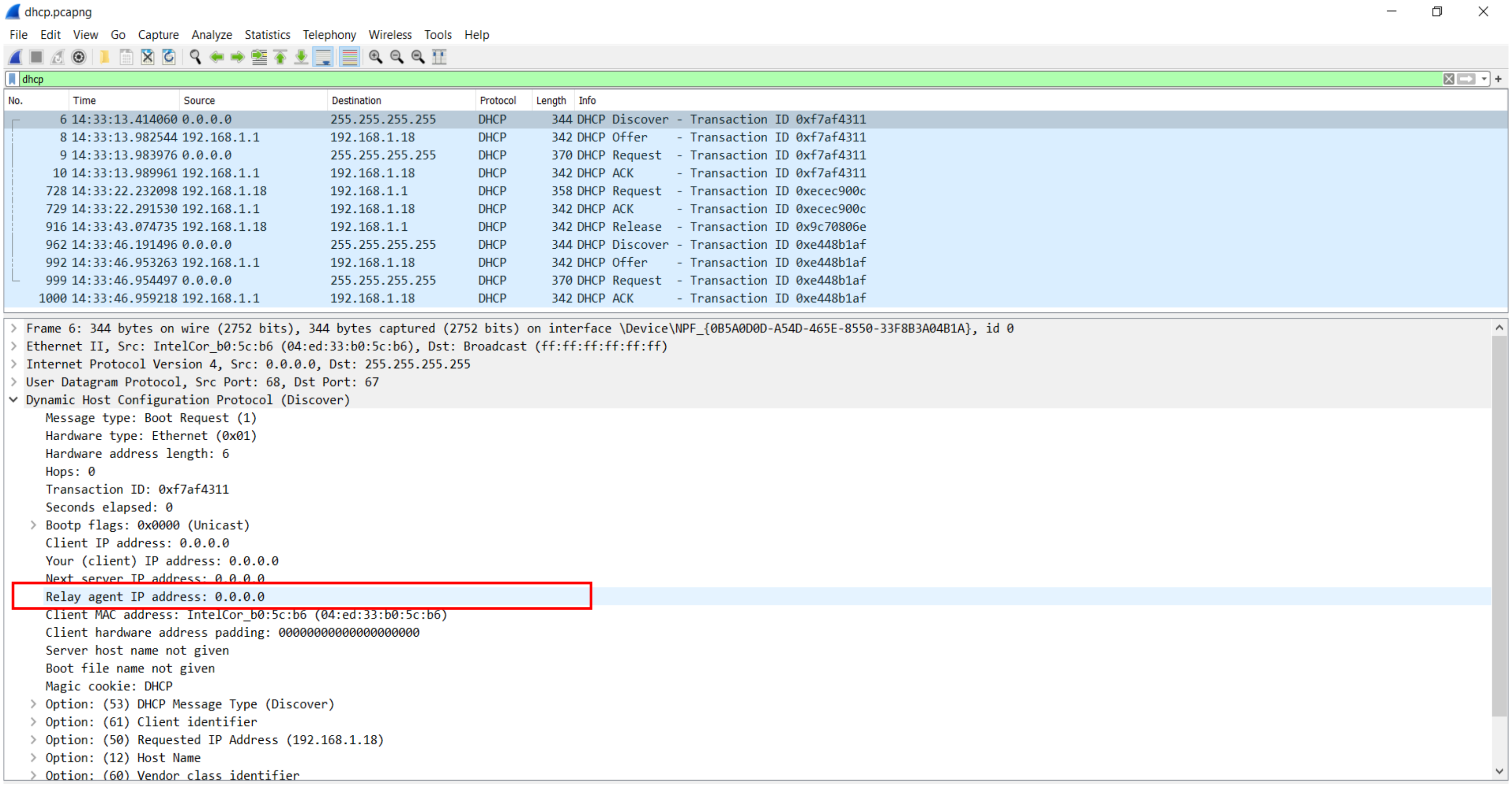
```
> User Datagram Protocol, Src Port: 67, Dst Port: 68
v Dynamic Host Configuration Protocol (Offer)
    Message type: Boot Reply (2)
    Hardware type: Ethernet (0x01)
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0xf7af4311
    Seconds elapsed: 0
  > Bootp flags: 0x0000 (Unicast)
    Client IP address: 0.0.0.0
    Your (client) IP address: 192.168.1.18
    Next server IP address: 0.0.0.0
    Relay agent IP address: 0.0.0.0
    Client MAC address: IntelCor_b0:5c:b6 (04:ed:33:b0:5c:b6)
    Client hardware address padding: 00000000000000000000
    Server host name not given
    Boot file name not given
    Magic cookie: DHCP
  v Option: (53) DHCP Message Type (Offer)
       Length: 1
       DHCP: Offer (2)
  > Option: (54) DHCP Server Identifier (192.168.1.1)
  > Option: (51) IP Address Lease Time
  > Option: (1) Subnet Mask (255.255.255.0)
  > Option: (3) Router
```

LAB 3

9. In the example screenshot in this assignment, there is no relay agent between the host and the DHCP server. What values in the trace indicate the absence of a relay agent? Is there a relay agent in your experiment? If so what is the IP address of the agent?

Solution 9 :

There is NO Relay Agent. This is indicated by the missing IP address for the Relay agent which is set to default 0.0.0.0 .



```
No.     Time            Source          Destination      Protocol Length Info
      6 14:33:13.414060 0.0.0.0         255.255.255.255  DHCP     344 DHCP Discover - Transaction ID 0xf7af4311
      8 14:33:13.982544 192.168.1.1     192.168.1.18     DHCP     342 DHCP Offer    - Transaction ID 0xf7af4311
      9 14:33:13.983976 0.0.0.0         255.255.255.255  DHCP     370 DHCP Request  - Transaction ID 0xf7af4311
     10 14:33:13.989961 192.168.1.1     192.168.1.18     DHCP     342 DHCP ACK      - Transaction ID 0xf7af4311
    728 14:33:22.232098 192.168.1.18    192.168.1.1      DHCP     358 DHCP Request  - Transaction ID 0xecec900c
    729 14:33:22.291530 192.168.1.1     192.168.1.18     DHCP     342 DHCP ACK      - Transaction ID 0xecec900c
    916 14:33:43.074735 192.168.1.18    192.168.1.1      DHCP     342 DHCP Release  - Transaction ID 0x9c70806e
    962 14:33:46.191496 0.0.0.0         255.255.255.255  DHCP     344 DHCP Discover - Transaction ID 0xe448b1af
    992 14:33:46.953263 192.168.1.1     192.168.1.18     DHCP     342 DHCP Offer    - Transaction ID 0xe448b1af
    999 14:33:46.954497 0.0.0.0         255.255.255.255  DHCP     370 DHCP Request  - Transaction ID 0xe448b1af
   1000 14:33:46.959218 192.168.1.1     192.168.1.18     DHCP     342 DHCP ACK      - Transaction ID 0xe448b1af
```

```
> Frame 6: 344 bytes on wire (2752 bits), 344 bytes captured (2752 bits) on interface \Device\NPF_{0B5A0D0D-A54D-465E-8550-33F8B3A04B1A}, id 0
> Ethernet II, Src: IntelCor_b0:5c:b6 (04:ed:33:b0:5c:b6), 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
v Dynamic Host Configuration Protocol (Discover)
    Message type: Boot Request (1)
    Hardware type: Ethernet (0x01)
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0xf7af4311
    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: IntelCor_b0:5c:b6 (04:ed:33:b0:5c:b6)
    Client hardware address padding: 00000000000000000000
    Server host name not given
    Boot file name not given
    Magic cookie: DHCP
  > Option: (53) DHCP Message Type (Discover)
  > Option: (61) Client identifier
  > Option: (50) Requested IP Address (192.168.1.18)
  > Option: (12) Host Name
  > Option: (60) Vendor class identifier
```

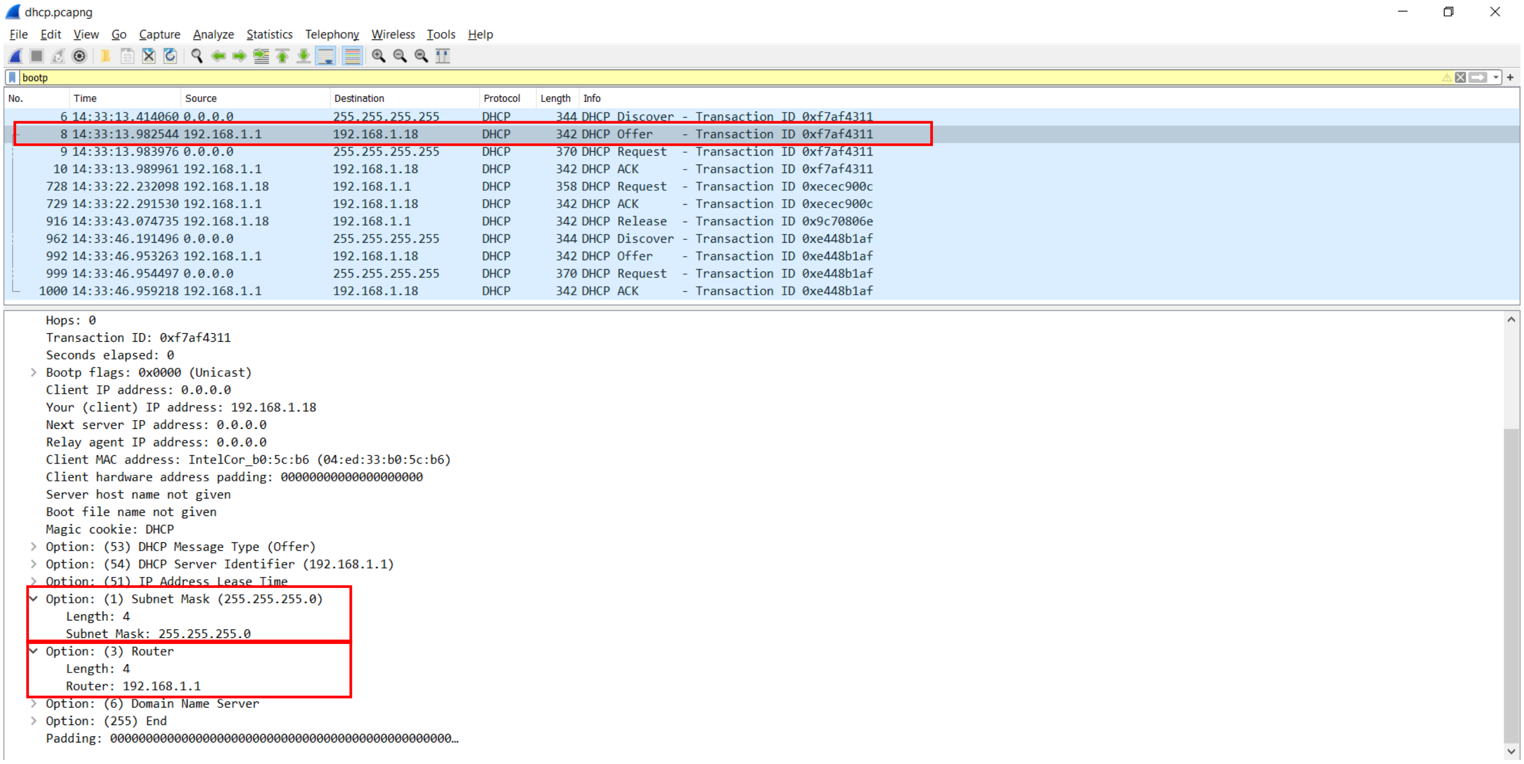
LAB 3

10. Explain the purpose of the router and subnet mask lines in the DHCP offer message

Solution 10:

The purpose of Subnet Mask is to indicate the subnet mask address – 255.255.255.0 and the broadcast domain to the client.

The purpose of the Router in the DHCP message is to indicate the Default Gateway address – 192.168.1.1 to get off the Subnet.


dhcp.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
bootp

```
No.   Time            Source        Destination      Protocol  Length Info
    6 14:33:13.414060 0.0.0.0       255.255.255.255  DHCP      344 DHCP Discover - Transaction ID 0xf7af4311
    8 14:33:13.982544 192.168.1.1   192.168.1.18     DHCP      342 DHCP Offer    - Transaction ID 0xf7af4311
    9 14:33:13.983976 0.0.0.0       255.255.255.255  DHCP      370 DHCP Request  - Transaction ID 0xf7af4311
   10 14:33:13.989961 192.168.1.1   192.168.1.18     DHCP      342 DHCP ACK      - Transaction ID 0xf7af4311
  728 14:33:22.232098 192.168.1.18  192.168.1.1      DHCP      358 DHCP Request  - Transaction ID 0xecec900c
  729 14:33:22.291530 192.168.1.1   192.168.1.18     DHCP      342 DHCP ACK      - Transaction ID 0xecec900c
  916 14:33:43.074735 192.168.1.18  192.168.1.1      DHCP      342 DHCP Release  - Transaction ID 0x9c70806e
  962 14:33:46.191496 0.0.0.0       255.255.255.255  DHCP      344 DHCP Discover - Transaction ID 0xe448b1af
  992 14:33:46.953263 192.168.1.1   192.168.1.18     DHCP      342 DHCP Offer    - Transaction ID 0xe448b1af
  999 14:33:46.954497 0.0.0.0       255.255.255.255  DHCP      370 DHCP Request  - Transaction ID 0xe448b1af
 1000 14:33:46.959218 192.168.1.1   192.168.1.18     DHCP      342 DHCP ACK      - Transaction ID 0xe448b1af
```

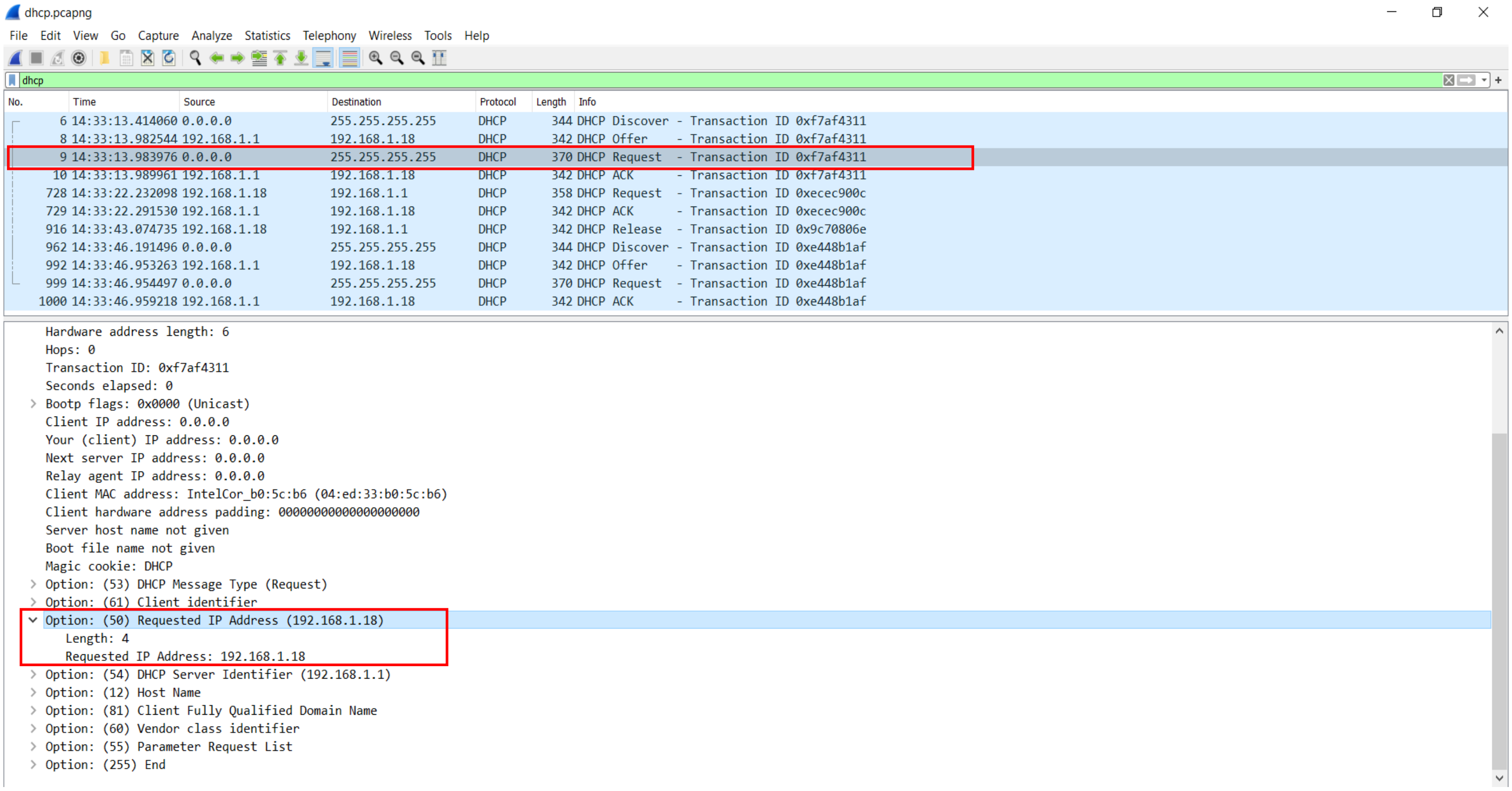
```
    Hops: 0
    Transaction ID: 0xf7af4311
    Seconds elapsed: 0
  > Bootp flags: 0x0000 (Unicast)
    Client IP address: 0.0.0.0
    Your (client) IP address: 192.168.1.18
    Next server IP address: 0.0.0.0
    Relay agent IP address: 0.0.0.0
    Client MAC address: IntelCor_b0:5c:b6 (04:ed:33:b0:5c:b6)
    Client hardware address padding: 00000000000000000000
    Server host name not given
    Boot file name not given
    Magic cookie: DHCP
  > Option: (53) DHCP Message Type (Offer)
  > Option: (54) DHCP Server Identifier (192.168.1.1)
  > Option: (51) IP Address Lease Time
  v Option: (1) Subnet Mask (255.255.255.0)
       Length: 4
       Subnet Mask: 255.255.255.0
  v Option: (3) Router
       Length: 4
       Router: 192.168.1.1
  > Option: (6) Domain Name Server
  > Option: (255) End
    Padding: 000000000000000000000000000000000000000000000000…
```

LAB 3

11. In the DHCP trace file noted in footnote 2, the DHCP server offers a specific IP address to the client (see also question 8. above). In the client's response to the first server OFFER message, does the client accept this IP address? Where in the client's RESPONSE is the client's requested address?

Solution 11:

Yes, Client accepts the IP Address – 192.168.1.18 & Request the same IP address in the DHCP Request message in the Option(50) in the Request IP Address field which has the Request IP Address that is 192.168.1.18 which is same as the offered IP Address by the DHCP server.



```
No.   Time            Source        Destination      Protocol Length Info
   6 14:33:13.414060 0.0.0.0       255.255.255.255  DHCP     344 DHCP Discover - Transaction ID 0xf7af4311
   8 14:33:13.982544 192.168.1.1   192.168.1.18     DHCP     342 DHCP Offer    - Transaction ID 0xf7af4311
   9 14:33:13.983976 0.0.0.0       255.255.255.255  DHCP     370 DHCP Request  - Transaction ID 0xf7af4311
  10 14:33:13.989961 192.168.1.1   192.168.1.18     DHCP     342 DHCP ACK      - Transaction ID 0xf7af4311
 728 14:33:22.232098 192.168.1.18  192.168.1.1      DHCP     358 DHCP Request  - Transaction ID 0xecec900c
 729 14:33:22.291530 192.168.1.1   192.168.1.18     DHCP     342 DHCP ACK      - Transaction ID 0xecec900c
 916 14:33:43.074735 192.168.1.18  192.168.1.1      DHCP     342 DHCP Release  - Transaction ID 0x9c70806e
 962 14:33:46.191496 0.0.0.0       255.255.255.255  DHCP     344 DHCP Discover - Transaction ID 0xe448b1af
 992 14:33:46.953263 192.168.1.1   192.168.1.18     DHCP     342 DHCP Offer    - Transaction ID 0xe448b1af
 999 14:33:46.954497 0.0.0.0       255.255.255.255  DHCP     370 DHCP Request  - Transaction ID 0xe448b1af
1000 14:33:46.959218 192.168.1.1   192.168.1.18     DHCP     342 DHCP ACK      - Transaction ID 0xe448b1af
```

```
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0xf7af4311
    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: IntelCor_b0:5c:b6 (04:ed:33:b0:5c:b6)
    Client hardware address padding: 00000000000000000000
    Server host name not given
    Boot file name not given
    Magic cookie: DHCP
  > Option: (53) DHCP Message Type (Request)
  > Option: (61) Client identifier
  v Option: (50) Requested IP Address (192.168.1.18)
        Length: 4
        Requested IP Address: 192.168.1.18
  > Option: (54) DHCP Server Identifier (192.168.1.1)
  > Option: (12) Host Name
  > Option: (81) Client Fully Qualified Domain Name
  > Option: (60) Vendor class identifier
  > Option: (55) Parameter Request List
  > Option: (255) End
```

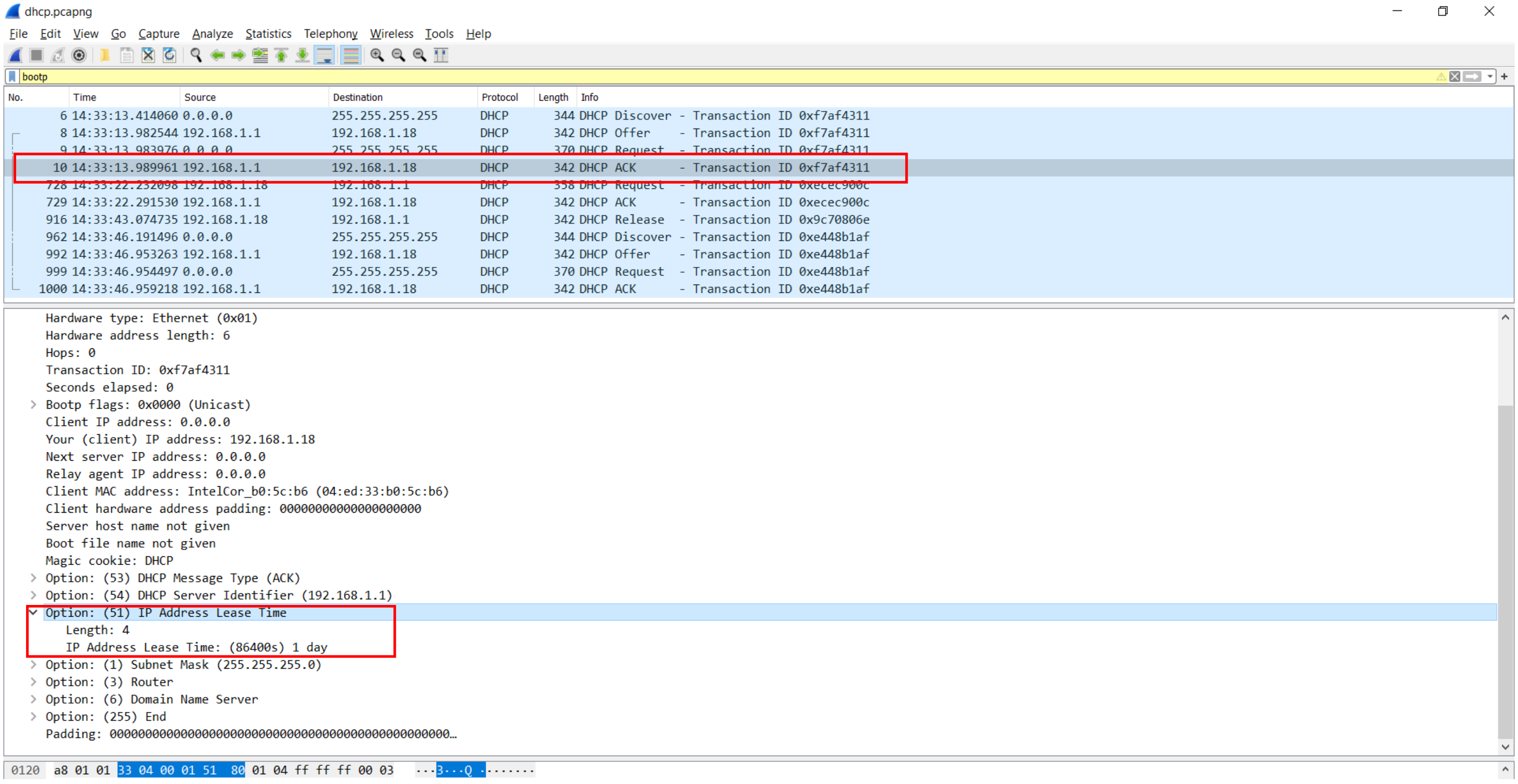
LAB 3

12. Explain the purpose of the lease time. How long is the lease time in your experiment?

Solution 12:

The purpose of the lease time is to assign & block the particular IP address for a particular client for a certain duration of time. This IP Address assigned for the client will be used by the DHCP server for any other client until the lease time expires. After the lease time expires the DHCP server can reuse the IP address for different clients.

The Lease Time in this Experiment is 86400 s which can also be written as 1 day.


dhcp.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

bootp

```
No.   Time            Source        Destination      Protocol Length Info
    6 14:33:13.414060 0.0.0.0       255.255.255.255  DHCP     344 DHCP Discover - Transaction ID 0xf7af4311
    8 14:33:13.982544 192.168.1.1   192.168.1.18     DHCP     342 DHCP Offer    - Transaction ID 0xf7af4311
    9 14:33:13.983976 0.0.0.0       255.255.255.255  DHCP     370 DHCP Request  - Transaction ID 0xf7af4311
   10 14:33:13.989961 192.168.1.1   192.168.1.18     DHCP     342 DHCP ACK      - Transaction ID 0xf7af4311
  728 14:33:22.232098 192.168.1.18  192.168.1.1      DHCP     358 DHCP Request  - Transaction ID 0xecec900c
  729 14:33:22.291530 192.168.1.1   192.168.1.18     DHCP     342 DHCP ACK      - Transaction ID 0xecec900c
  916 14:33:43.074735 192.168.1.18  192.168.1.1      DHCP     342 DHCP Release  - Transaction ID 0x9c70806e
  962 14:33:46.191496 0.0.0.0       255.255.255.255  DHCP     344 DHCP Discover - Transaction ID 0xe448b1af
  992 14:33:46.953263 192.168.1.1   192.168.1.18     DHCP     342 DHCP Offer    - Transaction ID 0xe448b1af
  999 14:33:46.954497 0.0.0.0       255.255.255.255  DHCP     370 DHCP Request  - Transaction ID 0xe448b1af
 1000 14:33:46.959218 192.168.1.1   192.168.1.18     DHCP     342 DHCP ACK      - Transaction ID 0xe448b1af
```

```
    Hardware type: Ethernet (0x01)
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0xf7af4311
    Seconds elapsed: 0
  > Bootp flags: 0x0000 (Unicast)
    Client IP address: 0.0.0.0
    Your (client) IP address: 192.168.1.18
    Next server IP address: 0.0.0.0
    Relay agent IP address: 0.0.0.0
    Client MAC address: IntelCor_b0:5c:b6 (04:ed:33:b0:5c:b6)
    Client hardware address padding: 00000000000000000000
    Server host name not given
    Boot file name not given
    Magic cookie: DHCP
  > Option: (53) DHCP Message Type (ACK)
  > Option: (54) DHCP Server Identifier (192.168.1.1)
  v Option: (51) IP Address Lease Time
      Length: 4
      IP Address Lease Time: (86400s) 1 day
  > Option: (1) Subnet Mask (255.255.255.0)
  > Option: (3) Router
  > Option: (6) Domain Name Server
  > Option: (255) End
    Padding: 000000000000000000000000000000000000000000000000…
```

```
0120  a8 01 01 33 04 00 01 51  80 01 04 ff ff ff 00 03   ···3···Q ········
```

LAB 3

13. What is the purpose of the DHCP release message? Does the DHCP server issue an acknowledgment of receipt of the client's DHCP request? What would happen if the client's DHCP release message is lost?

Solution 13:

The purpose of the DHCP release message is to terminate the lease time or period assigned for that particular IP Address (for a particular client) so that the DHCP Server can reuse the same IP Address.

No, DHCP server does not issue an acknowledgement of receipt of the client's DHCP request.

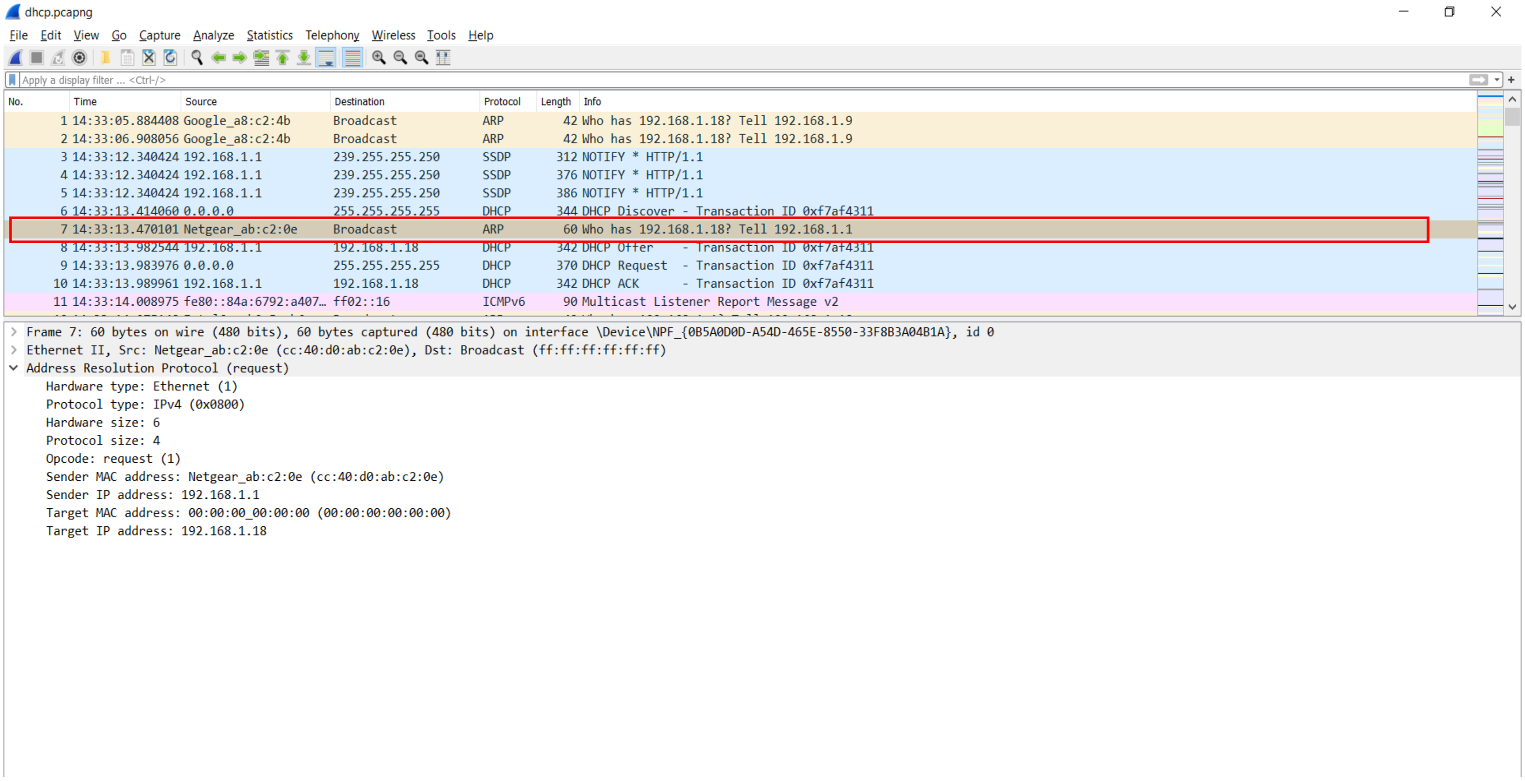
If DHCP client's release message is lost, then DHCP server has to sit back and wait for the lease period to end or another release message.

14. Clear the bootp filter from your Wireshark window. Were any ARP packets sent or received during the DHCP packet-exchange period? If so, explain the purpose of those ARP packets.

Solution 14:

Yes, there were ARP Packets sent during the DHCP packet-exchange period.

The purpose of ARP packets is to cumulate the IP addresses in use in the network and to cross verify that the IP address being offered is not being used by any other system in the network.



```
No.   Time            Source                 Destination      Protocol  Length Info
    1 14:33:05.884408 Google_a8:c2:4b        Broadcast        ARP           42 Who has 192.168.1.18? Tell 192.168.1.9
    2 14:33:06.908056 Google_a8:c2:4b        Broadcast        ARP           42 Who has 192.168.1.18? Tell 192.168.1.9
    3 14:33:12.340424 192.168.1.1            239.255.255.250  SSDP         312 NOTIFY * HTTP/1.1
    4 14:33:12.340424 192.168.1.1            239.255.255.250  SSDP         376 NOTIFY * HTTP/1.1
    5 14:33:12.340424 192.168.1.1            239.255.255.250  SSDP         386 NOTIFY * HTTP/1.1
    6 14:33:13.414060 0.0.0.0                255.255.255.255  DHCP         344 DHCP Discover - Transaction ID 0xf7af4311
    7 14:33:13.470101 Netgear_ab:c2:0e       Broadcast        ARP           60 Who has 192.168.1.18? Tell 192.168.1.1
    8 14:33:13.982544 192.168.1.1            192.168.1.18     DHCP         342 DHCP Offer    - Transaction ID 0xf7af4311
    9 14:33:13.983976 0.0.0.0                255.255.255.255  DHCP         370 DHCP Request  - Transaction ID 0xf7af4311
   10 14:33:13.989961 192.168.1.1            192.168.1.18     DHCP         342 DHCP ACK      - Transaction ID 0xf7af4311
   11 14:33:14.008975 fe80::84a:6792:a407…   ff02::16         ICMPv6        90 Multicast Listener Report Message v2

> Frame 7: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface \Device\NPF_{0B5A0D0D-A54D-465E-8550-33F8B3A04B1A}, id 0
> Ethernet II, Src: Netgear_ab:c2:0e (cc:40:d0:ab:c2:0e), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
v Address Resolution Protocol (request)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: request (1)
    Sender MAC address: Netgear_ab:c2:0e (cc:40:d0:ab:c2:0e)
    Sender IP address: 192.168.1.1
    Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
    Target IP address: 192.168.1.18
```