21CY681 - INTERNET PROTOCOL LAB - V

Name: Surya S Nair

Register Number: CB.EN.P2CYS22007

Date: 31st October 2022

Assignment Topic: Analyzing DHCP using protocol Analyser

AIM: Analyzing DHCP using protocol Analyser

PROCEDURE:

1. Perform the following steps to capture the DHCP traffic.

a) Begin by opening the Windows Command Prompt application. Type “ipconfig /release”.

b) Start up the Wireshark packet sniffer.

c) Now go back to the Windows Command Prompt and enter “ipconfig /renew”.

d) Wait until the “ipconfig /renew” has terminated. Then enter the same command “ipconfig /renew” again.

e) When the second “ipconfig /renew” terminates, enter the command

“ipconfig/release” to release the previously-allocated IP address to your

computer.

f) Finally, enter “ipconfig /renew” to again be allocated an IP address for your computer.

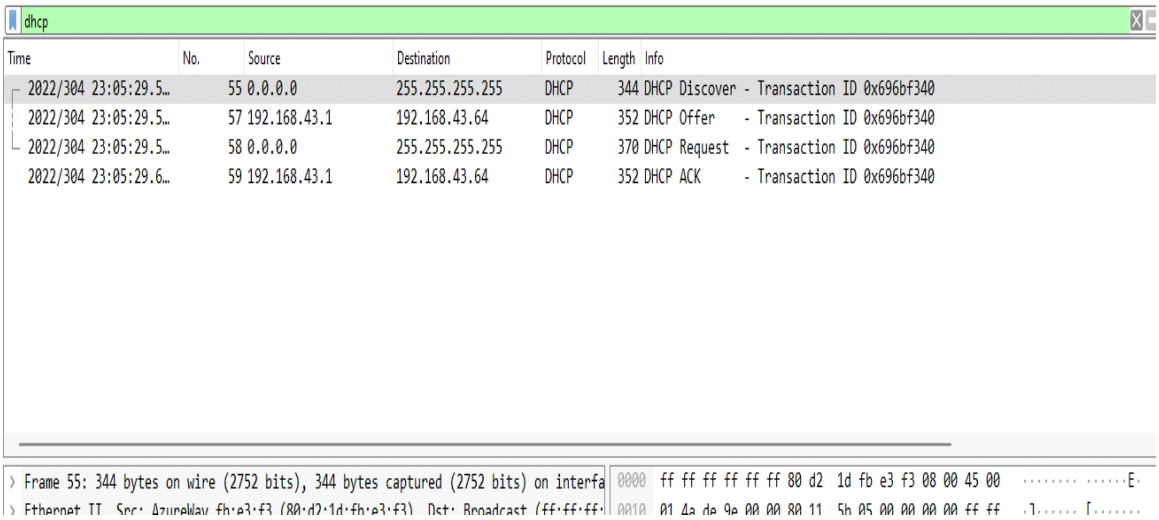
g) Stop Wireshark packet capture.

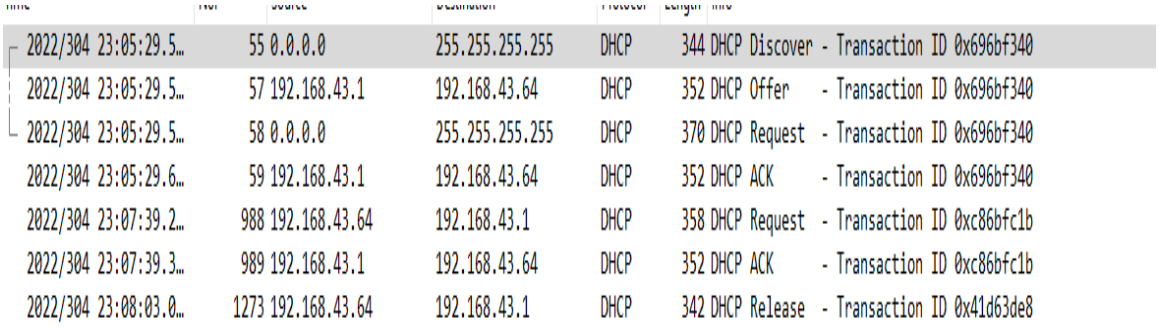
Ans:

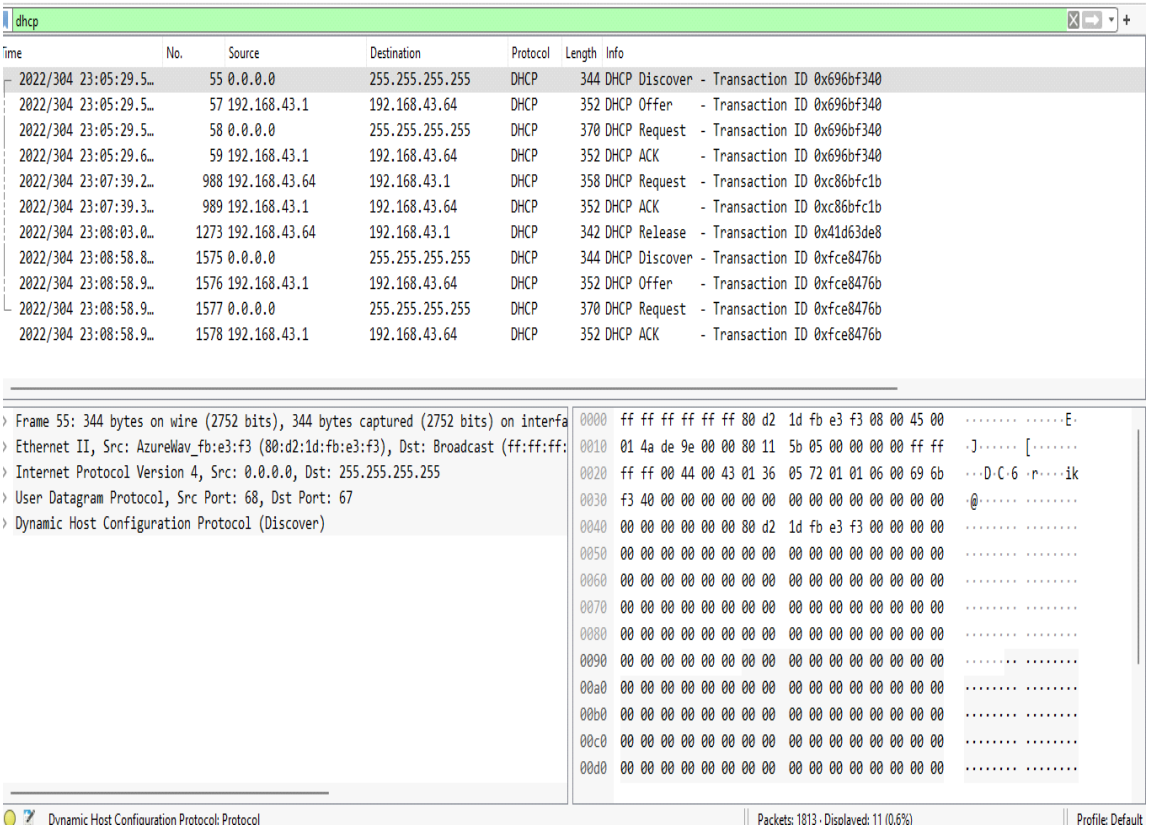
ipconfig /release will release the IP address

ipconfig /renew will renew the IP address

DHCP message sequences are DHCP Discover,DHCP Offer,DHCP Request and DHCP Ack.






dhcp
Time No. Source Destination Protocol Length Info
2022/304 23:05:29.5… 55 0.0.0.0 255.255.255.255 DHCP 344 DHCP Discover - Transaction ID 0x696bf340
2022/304 23:05:29.5… 57 192.168.43.1 192.168.43.64 DHCP 352 DHCP Offer - Transaction ID 0x696bf340
2022/304 23:05:29.5… 58 0.0.0.0 255.255.255.255 DHCP 370 DHCP Request - Transaction ID 0x696bf340
2022/304 23:05:29.6… 59 192.168.43.1 192.168.43.64 DHCP 352 DHCP ACK - Transaction ID 0x696bf340
2022/304 23:07:39.2… 988 192.168.43.64 192.168.43.1 DHCP 358 DHCP Request - Transaction ID 0xc86bfc1b
2022/304 23:07:39.3… 989 192.168.43.1 192.168.43.64 DHCP 352 DHCP ACK - Transaction ID 0xc86bfc1b
2022/304 23:08:03.0… 1273 192.168.43.64 192.168.43.1 DHCP 342 DHCP Release - Transaction ID 0x41d63de8
2022/304 23:08:58.8… 1575 0.0.0.0 255.255.255.255 DHCP 344 DHCP Discover - Transaction ID 0xfce8476b
2022/304 23:08:58.9… 1576 192.168.43.1 192.168.43.64 DHCP 352 DHCP Offer - Transaction ID 0xfce8476b
2022/304 23:08:58.9… 1577 0.0.0.0 255.255.255.255 DHCP 370 DHCP Request - Transaction ID 0xfce8476b
2022/304 23:08:58.9… 1578 192.168.43.1 192.168.43.64 DHCP 352 DHCP ACK - Transaction ID 0xfce8476b
Frame 55: 344 bytes on wire (2752 bits), 344 bytes captured (2752 bits) on interfa
Ethernet II, Src: AzureWav_fb:e3:f3 (80:d2:1d:fb:e3:f3), Dst: Broadcast (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)
0000 ff ff ff ff ff ff 80 d2 1d fb e3 f3 08 00 45 00
0010 01 4a de 9e 00 00 80 11 5b 05 00 00 00 00 ff ff
0020 ff ff 00 44 00 43 01 36 05 72 01 01 06 00 69 6b
0030 f3 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0040 00 00 00 00 00 00 80 d2 1d fb e3 f3 00 00 00 00
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
Dynamic Host Configuration Protocol: Protocol
Packets: 1813 · Displayed: 11 (0.6%)
Profile: Default

```
C:\WINDOWS\system32>ipconfig /release

Windows IP Configuration

No operation can be performed on Ethernet 2 while it has its media disconnected.
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.

Ethernet adapter Ethernet 2:

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

Ethernet adapter VirtualBox Host-Only Network:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::5890:9542:683:4d7d%11
   IPv4 Address. . . . . . . . . . . : 192.168.56.1
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

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  . :
   IPv6 Address. . . . . . . . . . . : 2409:4072:6d04:7bc:8181:96a9:19f3:33c4
   Temporary IPv6 Address. . . . . . : 2409:4072:6d04:7bc:1ca1:780c:8f9f:68ca
   Link-local IPv6 Address . . . . . : fe80::8181:96a9:19f3:33c4%10
   Default Gateway . . . . . . . . . : fe80::dc66:42ff:fef5:ed89%10
```

```
C:\WINDOWS\system32>ipconfig /renew

Windows IP Configuration

No operation can be performed on Ethernet 2 while it has its media disconnected.
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.

Ethernet adapter Ethernet 2:

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

Ethernet adapter VirtualBox Host-Only Network:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::5890:9542:683:4d7d%11
   IPv4 Address. . . . . . . . . . . : 192.168.56.1
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

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  . :
   IPv6 Address. . . . . . . . . . . : 2409:4072:6d04:7bc:8181:96a9:19f3:33c4
   Temporary IPv6 Address. . . . . . : 2409:4072:6d04:7bc:1ca1:780c:8f9f:68ca
   Link-local IPv6 Address . . . . . : fe80::8181:96a9:19f3:33c4%10
   IPv4 Address. . . . . . . . . . . : 192.168.43.64
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : fe80::dc66:42ff:fef5:ed89%10
                                       192.168.43.1
```

```
C:\WINDOWS\system32>ipconfig /renew

Windows IP Configuration

No operation can be performed on Ethernet 2 while it has its media disconnected.
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.

Ethernet adapter Ethernet 2:

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

Ethernet adapter VirtualBox Host-Only Network:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::5890:9542:683:4d7d%11
   IPv4 Address. . . . . . . . . . . : 192.168.56.1
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

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  . :
   IPv6 Address. . . . . . . . . . . : 2409:4072:6d04:7bc:8181:96a9:19f3:33c4
   Temporary IPv6 Address. . . . . . : 2409:4072:6d04:7bc:1ca1:780c:8f9f:68ca
   Link-local IPv6 Address . . . . . : fe80::8181:96a9:19f3:33c4%10
   IPv4 Address. . . . . . . . . . . : 192.168.43.64
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : fe80::dc66:42ff:fef5:ed89%10
                                       192.168.43.1
```

```
C:\WINDOWS\system32>ipconfig /release

Windows IP Configuration

No operation can be performed on Ethernet 2 while it has its media disconnected.
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.

Ethernet adapter Ethernet 2:

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

Ethernet adapter VirtualBox Host-Only Network:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::5890:9542:683:4d7d%11
   IPv4 Address. . . . . . . . . . . : 192.168.56.1
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

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  . :
   IPv6 Address. . . . . . . . . . . : 2409:4072:6d04:7bc:8181:96a9:19f3:33c4
   Temporary IPv6 Address. . . . . . : 2409:4072:6d04:7bc:1ca1:780c:8f9f:68ca
   Link-local IPv6 Address . . . . . : fe80::8181:96a9:19f3:33c4%10
   Default Gateway . . . . . . . . . : fe80::dc66:42ff:fef5:ed89%10
```

```
C:\WINDOWS\system32>ipconfig /renew

Windows IP Configuration

No operation can be performed on Ethernet 2 while it has its media disconnected.
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.

Ethernet adapter Ethernet 2:

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

Ethernet adapter VirtualBox Host-Only Network:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::5890:9542:683:4d7d%11
   IPv4 Address. . . . . . . . . . . : 192.168.56.1
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

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  . :
   IPv6 Address. . . . . . . . . . . : 2409:4072:6d04:7bc:8181:96a9:19f3:33c4
   Temporary IPv6 Address. . . . . . : 2409:4072:6d04:7bc:1ca1:780c:8f9f:68ca
   Link-local IPv6 Address . . . . . : fe80::8181:96a9:19f3:33c4%10
   IPv4 Address. . . . . . . . . . . : 192.168.43.64
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : fe80::dc66:42ff:fef5:ed89%10
                                       192.168.43.1
```

2.Open the captured traffic file and given pcap file “dhcp” in Wireshark to answer the following questions.

a) Are DHCP messages sent over UDP or TCP?

Ans: DHCP messages are sent over UDP .The DHCP employs a connectionless service model, using the User Datagram Protocol (UDP). It is implemented with two UDP port numbers for its operations. UDP port number 67 is the port used by the server, and UDP port number 68 is used by the client.

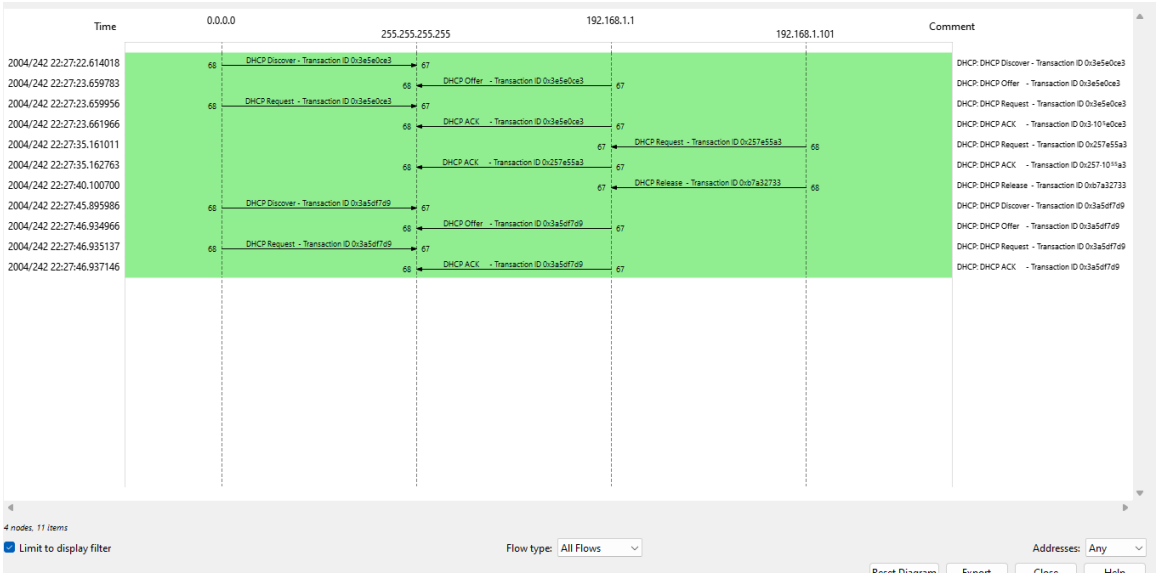
dhcp

Time	No.	Source	Destination	Protocol	Length	Info
2004/242 22:27:46.9…	46	192.168.1.1	255.255.255.255	DHCP	590	DHCP ACK - Transaction ID 0x3a5df7d9
2004/242 22:27:46.9…	44	192.168.1.1	255.255.255.255	DHCP	590	DHCP Offer - Transaction ID 0x3a5df7d9
2004/242 22:27:35.1…	37	192.168.1.1	255.255.255.255	DHCP	590	DHCP ACK - Transaction ID 0x257e55a3
2004/242 22:27:23.6…	6	192.168.1.1	255.255.255.255	DHCP	590	DHCP ACK - Transaction ID 0x3e5e0ce3
2004/242 22:27:23.6…	4	192.168.1.1	255.255.255.255	DHCP	590	DHCP Offer - Transaction ID 0x3e5e0ce3
2004/242 22:27:46.9…	45	0.0.0.0	255.255.255.255	DHCP	342	DHCP Request - Transaction ID 0x3a5df7d9
2004/242 22:27:45.8…	42	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x3a5df7d9
2004/242 22:27:40.1…	41	192.168.1.101	192.168.1.1	DHCP	342	DHCP Release - Transaction ID 0xb7a32733
2004/242 22:27:35.1…	36	192.168.1.101	192.168.1.1	DHCP	342	DHCP Request - Transaction ID 0x257e55a3
2004/242 22:27:23.6…	5	0.0.0.0	255.255.255.255	DHCP	342	DHCP Request - Transaction ID 0x3e5e0ce3
2004/242 22:27:22.6…	2	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x3e5e0ce3

```
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 328
    Identification: 0xb32f (45871)
  > 000. .... = Flags: 0x0
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 128
    Protocol: UDP (17)
    Header Checksum: 0x8676 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 0.0.0.0
    Destination Address: 255.255.255.255
  User Datagram Protocol, Src Port: 68, Dst Port: 67
  Dynamic Host Configuration Protocol (Discover)
```

b) 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.

Ans:



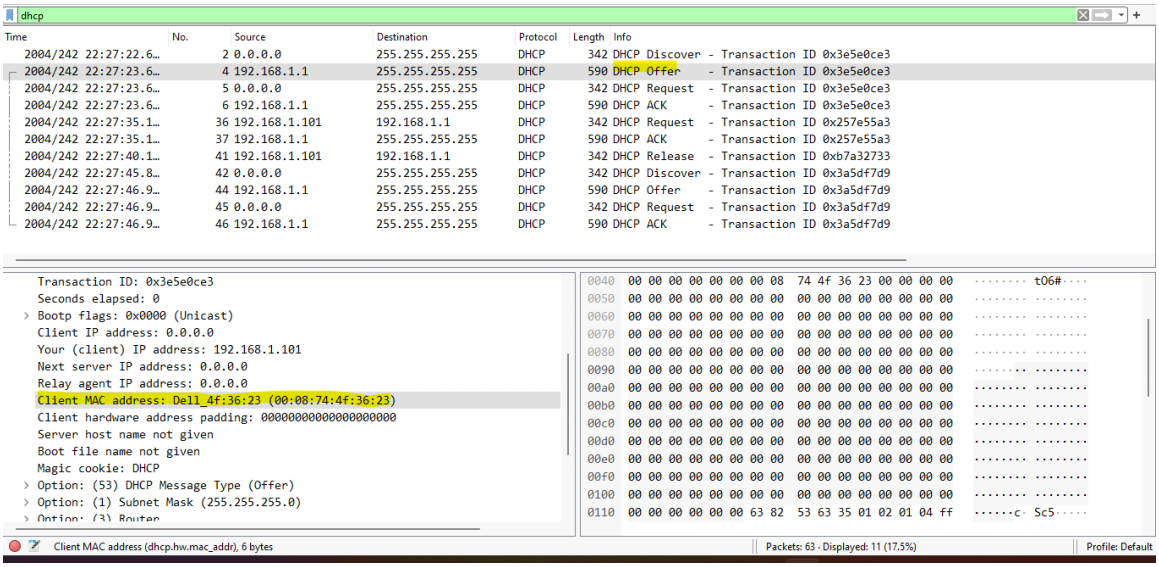

```
DHCP ACK      - Transaction ID 0x3a5df7d9                67    68 255.255.255.255
DHCP Offer    - Transaction ID 0x3a5df7d9                67    68 255.255.255.255
DHCP ACK      - Transaction ID 0x257e55a3                67    68 255.255.255.255
DHCP ACK      - Transaction ID 0x3e5e0ce3                67    68 255.255.255.255
DHCP Offer    - Transaction ID 0x3e5e0ce3                67    68 255.255.255.255
DHCP Request  - Transaction ID 0x3a5df7d9                68    67 255.255.255.255
DHCP Discover - Transaction ID 0x3a5df7d9                68    67 255.255.255.255
DHCP Release  - Transaction ID 0xb7a32733                68    67 192.168.1.1
DHCP Request  - Transaction ID 0x257e55a3                68    67 192.168.1.1
DHCP Request  - Transaction ID 0x3e5e0ce3                68    67 255.255.255.255
DHCP Discover - Transaction ID 0x3e5e0ce3                68    67 255.255.255.255
```

67-source port number

68-destination port number

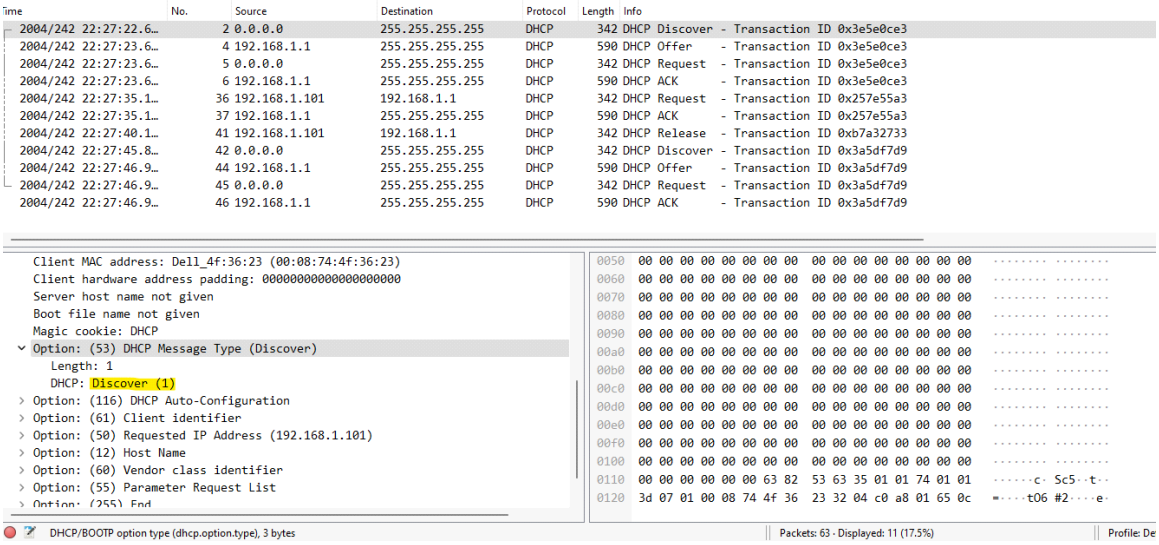
c) What is the link-layer (e.g., Ethernet) address of your host?

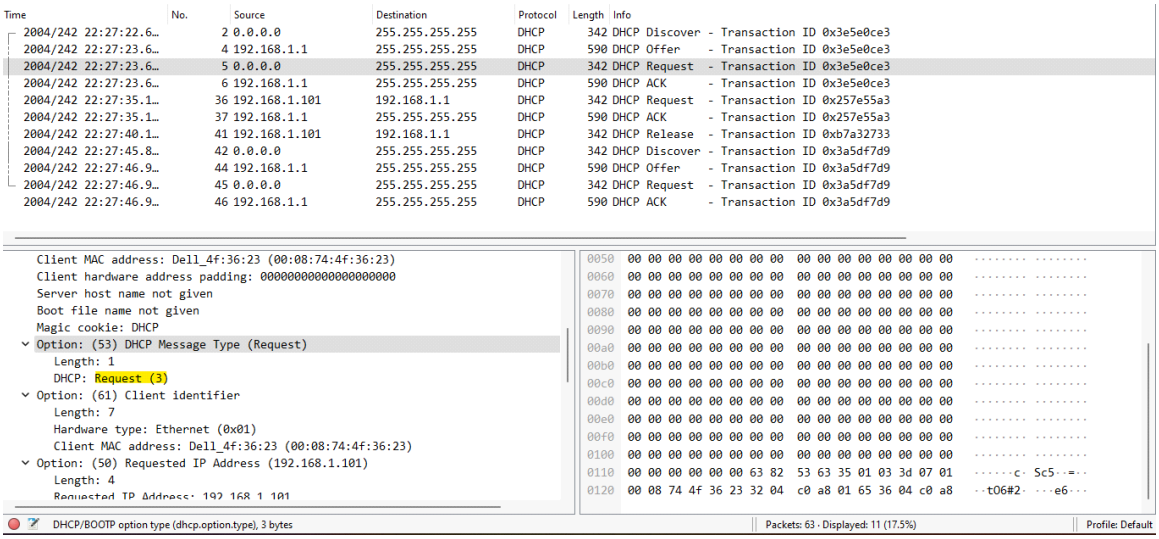
Ans:



d) What values in the DHCP discover message differentiate this message from the DHCP request message?

Ans :DHCP Message Type and DHCP Server Identifier





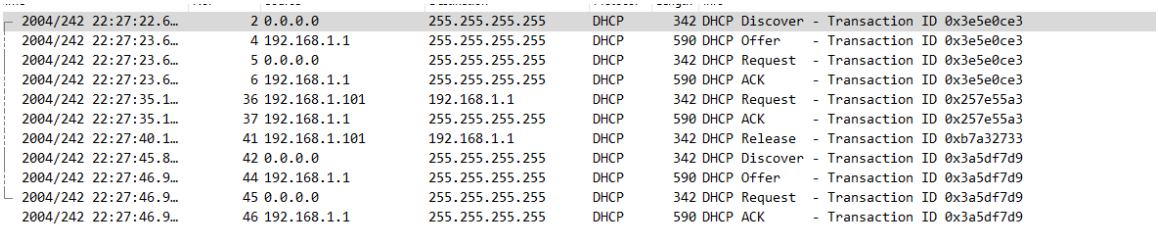
Server host name not given
Boot file name not given
Magic cookie: DHCP
> Option: (53) DHCP Message Type (Request)
> Option: (61) Client identifier
> Option: (50) Requested IP Address (192.168.1.101)
> Option: (54) DHCP Server Identifier (192.168.1.1)
> Option: (12) Host Name
> Option: (60) Vendor class identifier
> Option: (55) Parameter Request List
> Option: (255) End

Server host name not given
Boot file name not given
Magic cookie: DHCP
> Option: (53) DHCP Message Type (Discover)
> Option: (116) DHCP Auto-Configuration
> Option: (61) Client identifier
> Option: (50) Requested IP Address (192.168.1.101)
> Option: (12) Host Name
> Option: (60) Vendor class identifier
> Option: (55) Parameter Request List
> Option: (255) End

e) 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

theTransaction-ID in the second set (Request/ACK) set of DHCP messages?What is the purpose of the Transaction-ID field?

Ans:



2004/242 22:27:22.6…	2	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x3e5e0ce3
2004/242 22:27:23.6…	4	192.168.1.1	255.255.255.255	DHCP	590	DHCP Offer - Transaction ID 0x3e5e0ce3
2004/242 22:27:23.6…	5	0.0.0.0	255.255.255.255	DHCP	342	DHCP Request - Transaction ID 0x3e5e0ce3
2004/242 22:27:23.6…	6	192.168.1.1	255.255.255.255	DHCP	590	DHCP ACK - Transaction ID 0x3e5e0ce3
2004/242 22:27:35.1…	36	192.168.1.101	192.168.1.1	DHCP	342	DHCP Request - Transaction ID 0x257e55a3
2004/242 22:27:35.1…	37	192.168.1.1	255.255.255.255	DHCP	590	DHCP ACK - Transaction ID 0x257e55a3
2004/242 22:27:40.1…	41	192.168.1.101	192.168.1.1	DHCP	342	DHCP Release - Transaction ID 0xb7a32733
2004/242 22:27:45.8…	42	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x3a5df7d9
2004/242 22:27:46.9…	44	192.168.1.1	255.255.255.255	DHCP	590	DHCP Offer - Transaction ID 0x3a5df7d9
2004/242 22:27:46.9…	45	0.0.0.0	255.255.255.255	DHCP	342	DHCP Request - Transaction ID 0x3a5df7d9
2004/242 22:27:46.9…	46	192.168.1.1	255.255.255.255	DHCP	590	DHCP ACK - Transaction ID 0x3a5df7d9

The transaction ID in the first four packets is 0x3e5e0ce3

The transaction ID in the second set of DHCP messages is 0x3a5d7d9

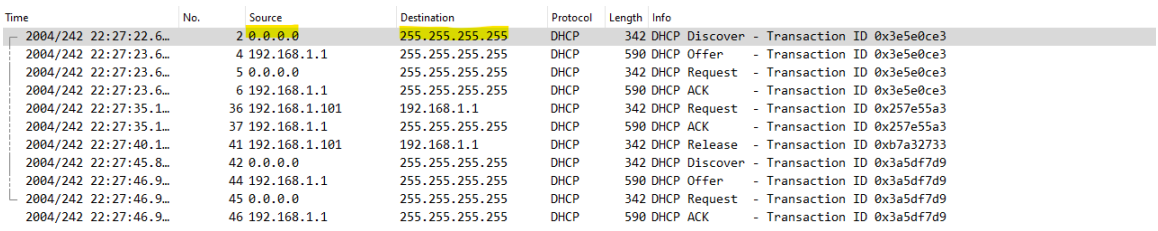
To keep a track of message that are coming or is used by the server to identify or take a note of which message was sent by which computer.If the process is new the Id will be new.

f) 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.

Ans : If IP address is not set until the end of the four message exchange , then 0.0.0.0 is used as the IP in the DHCP exchange.

For Discover and Request , the source IP is 0.0.0.0 and dst IP is 255.255.255.255

For Offer and ACK , the source IP is 172.17.18.2 and dst IP is 172.17.136.155



Time	No.	Source	Destination	Protocol	Length	Info
2004/242 22:27:22.6…	2	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x3e5e0ce3
2004/242 22:27:23.6…	4	192.168.1.1	255.255.255.255	DHCP	590	DHCP Offer - Transaction ID 0x3e5e0ce3
2004/242 22:27:23.6…	5	0.0.0.0	255.255.255.255	DHCP	342	DHCP Request - Transaction ID 0x3e5e0ce3
2004/242 22:27:23.6…	6	192.168.1.1	255.255.255.255	DHCP	590	DHCP ACK - Transaction ID 0x3e5e0ce3
2004/242 22:27:35.1…	36	192.168.1.101	192.168.1.1	DHCP	342	DHCP Request - Transaction ID 0x257e55a3
2004/242 22:27:35.1…	37	192.168.1.1	255.255.255.255	DHCP	590	DHCP ACK - Transaction ID 0x257e55a3
2004/242 22:27:40.1…	41	192.168.1.101	192.168.1.1	DHCP	342	DHCP Release - Transaction ID 0xb7a32733
2004/242 22:27:45.8…	42	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x3a5df7d9
2004/242 22:27:46.9…	44	192.168.1.1	255.255.255.255	DHCP	590	DHCP Offer - Transaction ID 0x3a5df7d9
2004/242 22:27:46.9…	45	0.0.0.0	255.255.255.255	DHCP	342	DHCP Request - Transaction ID 0x3a5df7d9
2004/242 22:27:46.9…	46	192.168.1.1	255.255.255.255	DHCP	590	DHCP ACK - Transaction ID 0x3a5df7d9

```
DHCP ACK      - Transaction ID 0x3a5df7d9                    67    68 255.255.255.255
DHCP Offer    - Transaction ID 0x3a5df7d9                    67    68 255.255.255.255
DHCP ACK      - Transaction ID 0x257e55a3                    67    68 255.255.255.255
DHCP ACK      - Transaction ID 0x3e5e0ce3                    67    68 255.255.255.255
DHCP Offer    - Transaction ID 0x3e5e0ce3                    67    68 255.255.255.255
DHCP Request  - Transaction ID 0x3a5df7d9                    68    67 255.255.255.255
DHCP Discover - Transaction ID 0x3a5df7d9                    68    67 255.255.255.255
DHCP Release  - Transaction ID 0xb7a32733                    68    67 192.168.1.1
DHCP Request  - Transaction ID 0x257e55a3                    68    67 192.168.1.1
DHCP Request  - Transaction ID 0x3e5e0ce3                    68    67 255.255.255.255
DHCP Discover - Transaction ID 0x3e5e0ce3                    68    67 255.255.255.255
```

g) What is the IP address of your DHCP server?

Ans:The IP address of the DHCP server is 192.168.1.1

```
2004/242 22:27:23.6…   4 192.168.1.1   255.255.255.255   DHCP   590 DHCP Offer   - Transaction ID 0x3e5e0ce3
```

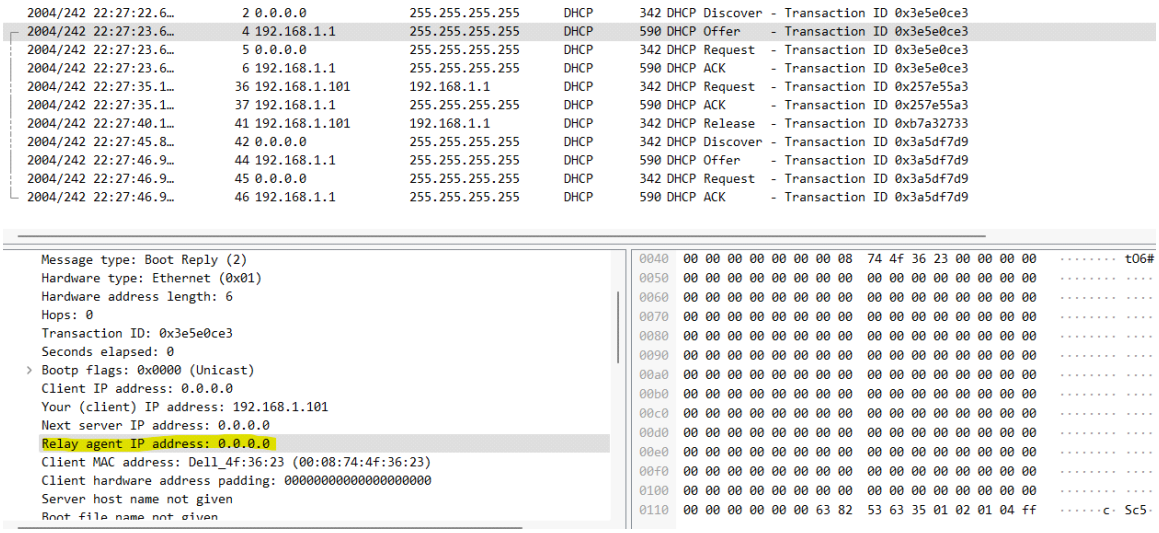
h) What IP address is the DHCP server offering to your host in the DHCP Offermessage? Indicate which DHCP message contains the offered DHCP address.

Ans:The DHCP offered address is 192.168.1.101

```
Message type: Boot Reply (2)
Hardware type: Ethernet (0x01)
Hardware address length: 6
Hops: 0
Transaction ID: 0x3e5e0ce3
Seconds elapsed: 0
> Bootp flags: 0x0000 (Unicast)
Client IP address: 0.0.0.0
Your (client) IP address: 192.168.1.101
Next server IP address: 0.0.0.0
Relay agent IP address: 0.0.0.0
Client MAC address: Dell_4f:36:23 (00:08:74:4f:36:23)
Client hardware address padding: 00000000000000000000
Server host name not given
Boot file name not given
```

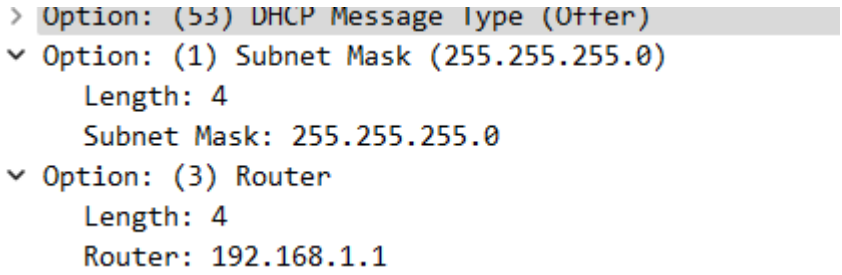
i) In the example screenshot in this assignment, there is no relay agent between the host and the DHCP server. What values in the trace indicate the absence of a relay agent? Is there a relay agent in your experiment? If so what is the IP address of the agent?

Ans: There is no relay agent ,so the value for relay agent is 0.0.0.0



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

Ans:For connecting with internet we need router.If IP address is not set until the end of the four message exchange , then 0.0.0.0 is used as the IP in the DHCP exchange.For Discover and Request , the source IP is 0.0.0.0 and dst IP is 255.255.255.255 .For Offer and ACK , the source IP is 172.17.18.2 and dst IP is 172.17.136.155



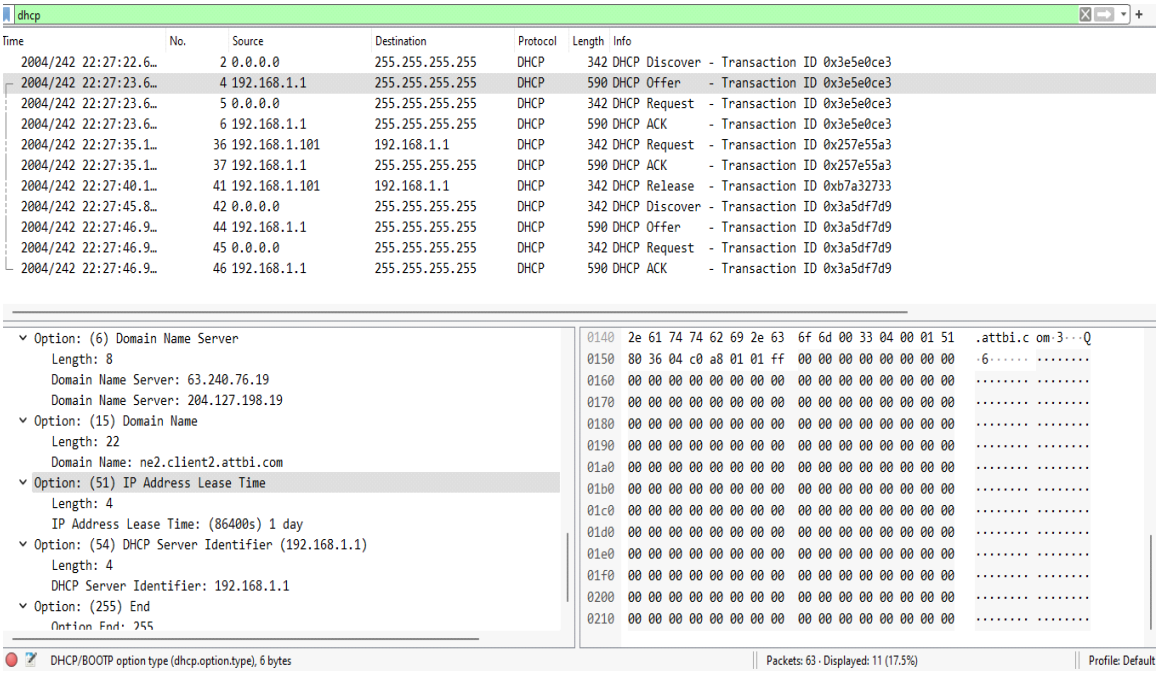
k) In the DHCP trace file, the DHCP server offers a specific IP address to the client. In the client's response to the first server OFFER message, does the client accept this IP address? Where in the client's RESPONSE is the client's requested address?

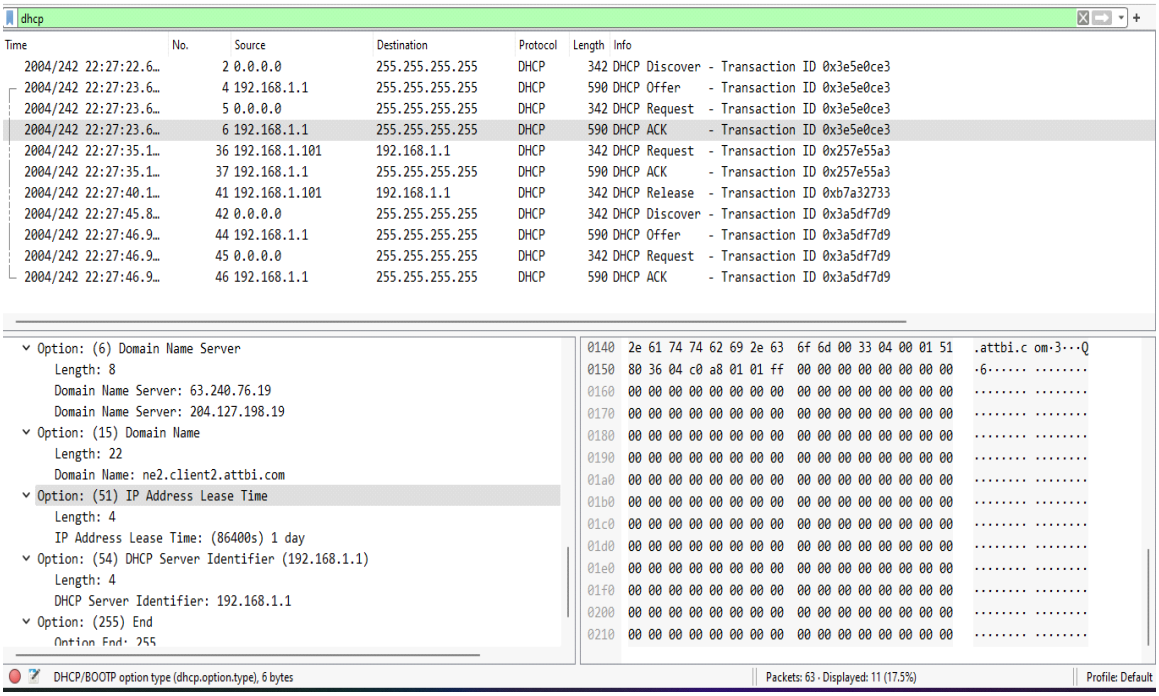
Ans:Yes,in the client's response to the first server OFFER message,the client accept this IP address.The client IP requested address is mentioned in the packet is shown below:

```
> Bootp flags: 0x0000 (Unicast)
  Client IP address: 0.0.0.0
  Your (client) IP address: 192.168.1.101
  Next server IP address: 0.0.0.0
  Relay agent IP address: 0.0.0.0
  Client MAC address: Dell_4f:36:23 (00:08:74:4f:36:23)
  Client hardware address padding: 00000000000000000000
  Server host name not given
  Boot file name not given
  Magic cookie: DHCP
```

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

Ans:





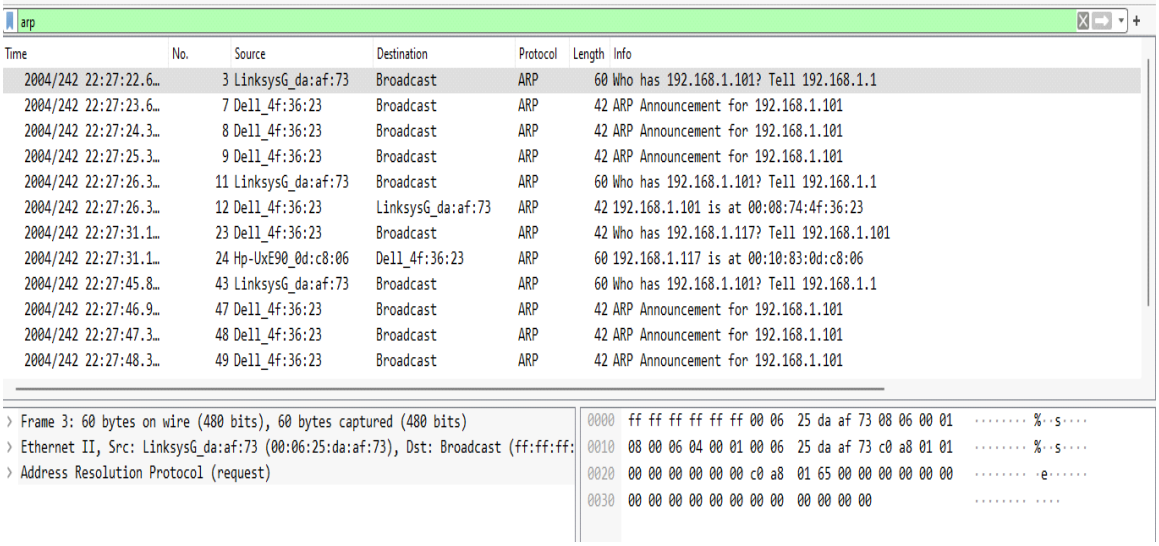
The lease time of the IP for an computer is 1day.

m) 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?

Ans:The purpose of release message is to release the IP address assigned to the computer. The DHCP server doesn't send an ACK receipt of client's DHCP request.If the client's DHCP message is lost then the server might not know whether the client issued an release request or not . So the IP assigned to the computer previously still remains the same.

n) Clear the DHCP 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.

Ans:Yes.We can see many ARP packets that were transferred in the experiment since the server verifies whether the IP which is to be allocated to the requested computer is used already by any other computer.



RESULT: Analyzed DHCP using protocol Analyser.