ASSIGNMENT
INTERNET PROTOCOL LAB

NAME: Rahul Raj

REG NO: CYS22011

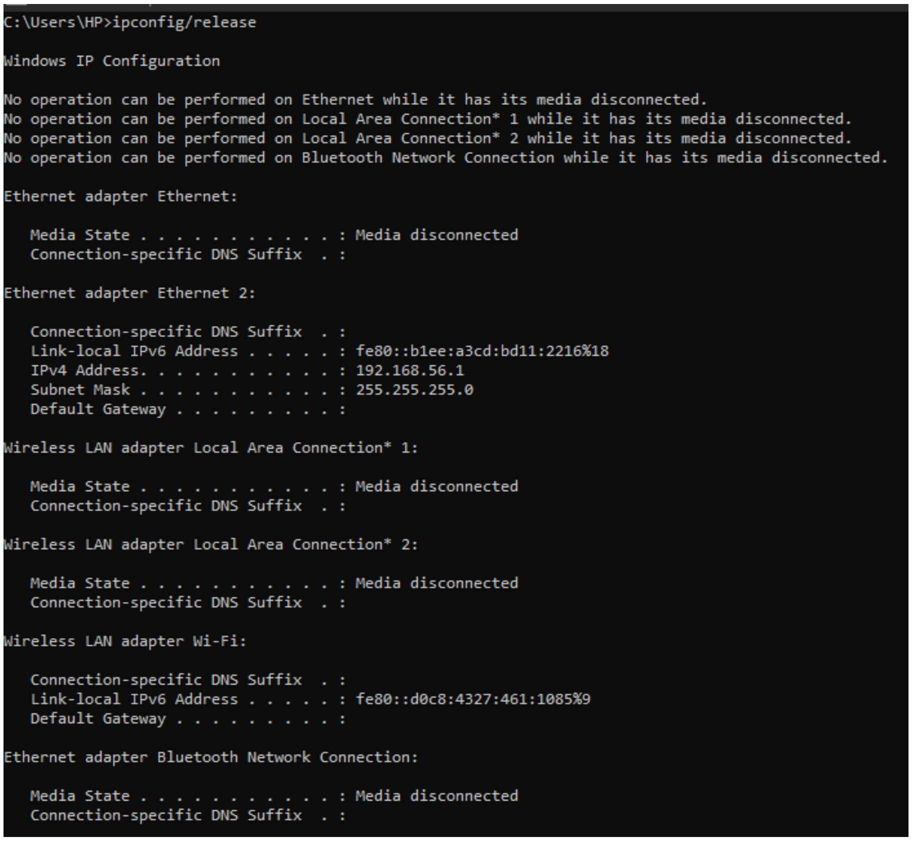
DATE OF ASSIGNMENT PROVIDED: 31/10/2022

TITLE: Analyzing DHCP using protocol analyzer

AIM: To analyze DHCP using protocol analyzer

PROCEDURE-

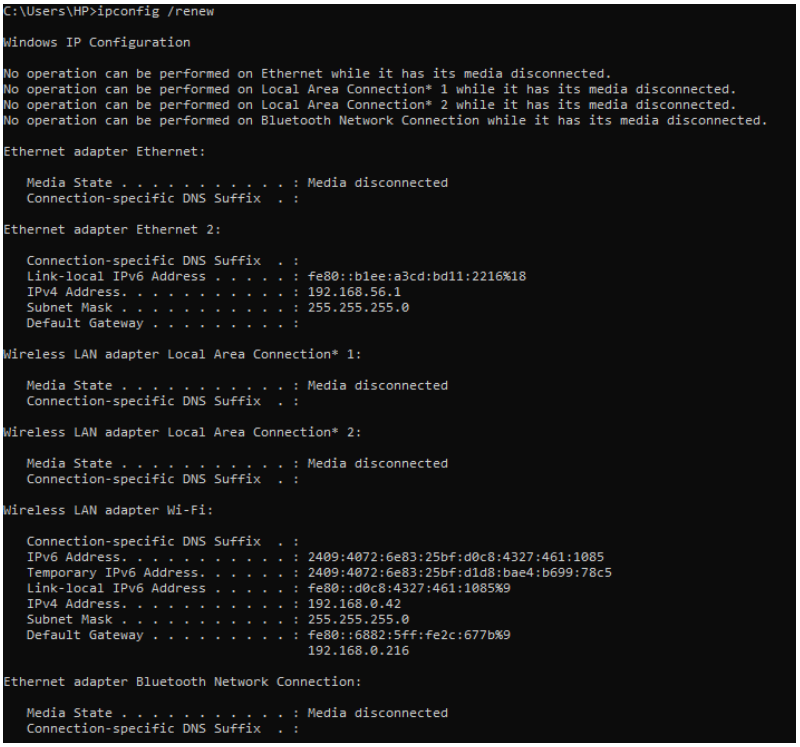
1.a) Begin by opening the Windows Command Prompt application. Type “ipconfig /release”.



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

Windows IP Configuration

No operation can be performed on Ethernet 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.
No operation can be performed on Bluetooth Network Connection while it has its media disconnected.

Ethernet adapter Ethernet:

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

Ethernet adapter Ethernet 2:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::b1ee:a3cd:bd11:2216%18
   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  . :
   Link-local IPv6 Address . . . . . : fe80::d0c8:4327:461:1085%9
   Default Gateway . . . . . . . . . :

Ethernet adapter Bluetooth Network Connection:

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

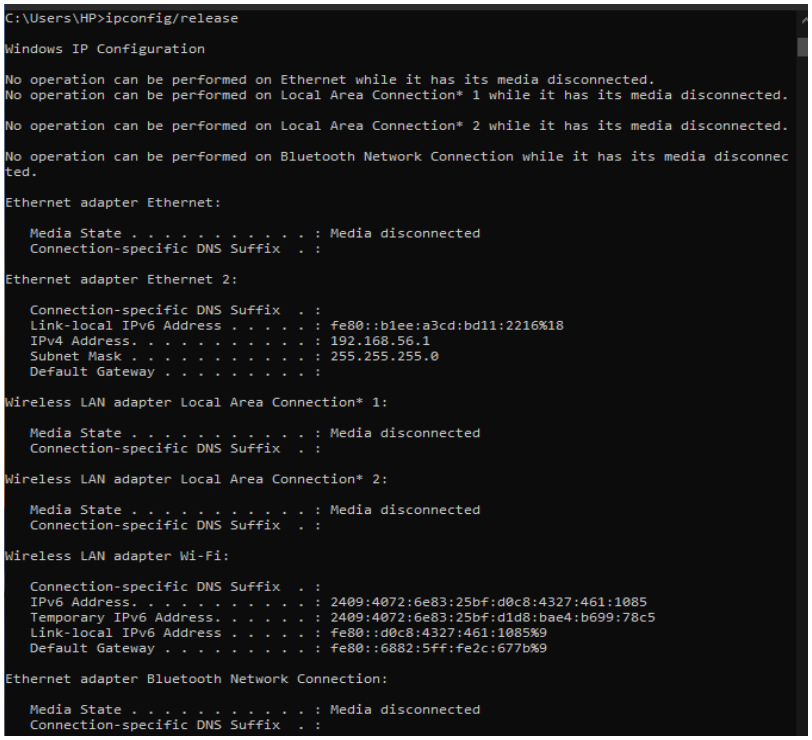
b) Start up the Wireshark packet sniffer.

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



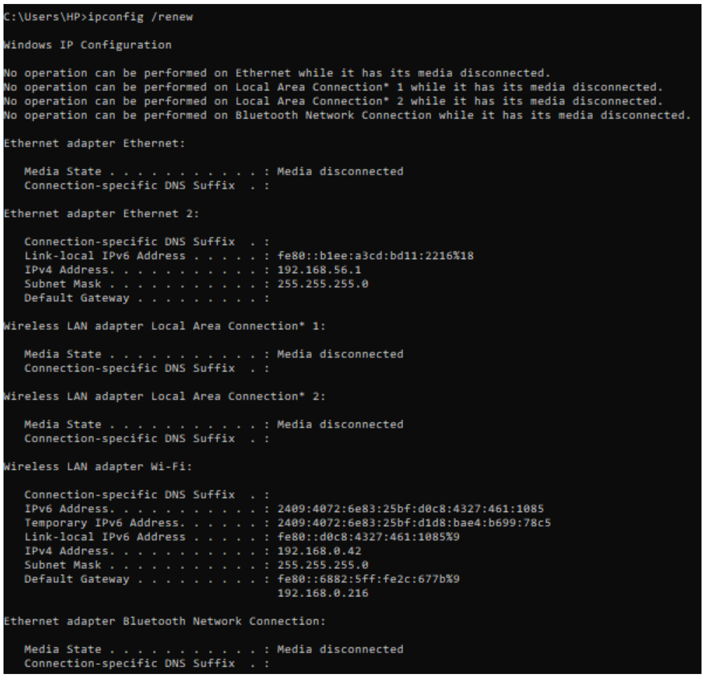
```
C:\Users\HP>ipconfig /renew

Windows IP Configuration

No operation can be performed on Ethernet 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.
No operation can be performed on Bluetooth Network Connection while it has its media disconnected.

Ethernet adapter Ethernet:

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

Ethernet adapter Ethernet 2:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::b1ee:a3cd:bd11:2216%18
   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. . . . . . . . . . . : 2409:4072:6e83:25bf:d0c8:4327:461:1085
   Temporary IPv6 Address. . . . . . : 2409:4072:6e83:25bf:d1d8:bae4:b699:78c5
   Link-local IPv6 Address . . . . . : fe80::d0c8:4327:461:1085%9
   IPv4 Address. . . . . . . . . . . : 192.168.0.42
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : fe80::6882:5ff:fe2c:677b%9
                                       192.168.0.216

Ethernet adapter Bluetooth Network Connection:

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

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



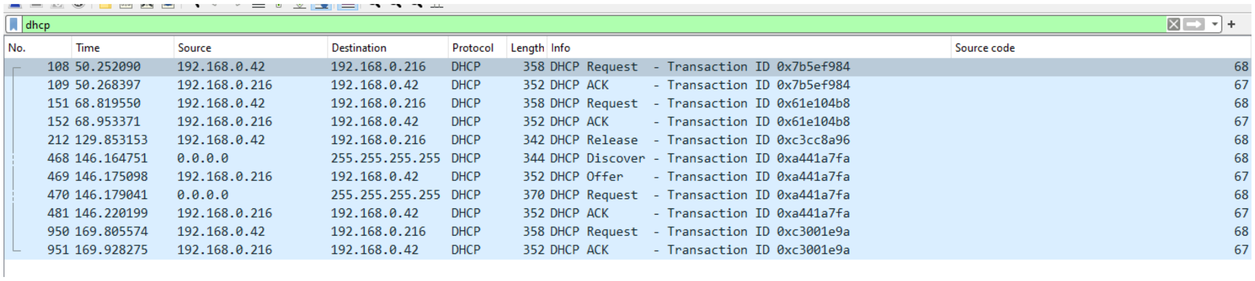
```
C:\Users\HP>ipconfig/release

Windows IP Configuration

No operation can be performed on Ethernet 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.

No operation can be performed on Bluetooth Network Connection while it has its media disconnec
ted.

Ethernet adapter Ethernet:

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

Ethernet adapter Ethernet 2:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::b1ee:a3cd:bd11:2216%18
   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. . . . . . . . . . . : 2409:4072:6e83:25bf:d0c8:4327:461:1085
   Temporary IPv6 Address. . . . . . : 2409:4072:6e83:25bf:d1d8:bae4:b699:78c5
   Link-local IPv6 Address . . . . . : fe80::d0c8:4327:461:1085%9
   Default Gateway . . . . . . . . . : fe80::6882:5ff:fe2c:677b%9

Ethernet adapter Bluetooth Network Connection:

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

e) When the second “ipconfig /renew” terminates, enter the command “ipconfig/release” to release the previously-allocated IP address to your computer.



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

Windows IP Configuration

No operation can be performed on Ethernet 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.
No operation can be performed on Bluetooth Network Connection while it has its media disconnected.

Ethernet adapter Ethernet:

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

Ethernet adapter Ethernet 2:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::b1ee:a3cd:bd11:2216%18
   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. . . . . . . . . . . : 2409:4072:6e83:25bf:d0c8:4327:461:1085
   Temporary IPv6 Address. . . . . . : 2409:4072:6e83:25bf:d1d8:bae4:b699:78c5
   Link-local IPv6 Address . . . . . : fe80::d0c8:4327:461:1085%9
   IPv4 Address. . . . . . . . . . . : 192.168.0.42
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : fe80::6882:5ff:fe2c:677b%9
                                       192.168.0.216

Ethernet adapter Bluetooth Network Connection:

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

g) Stop Wireshark packet capture.

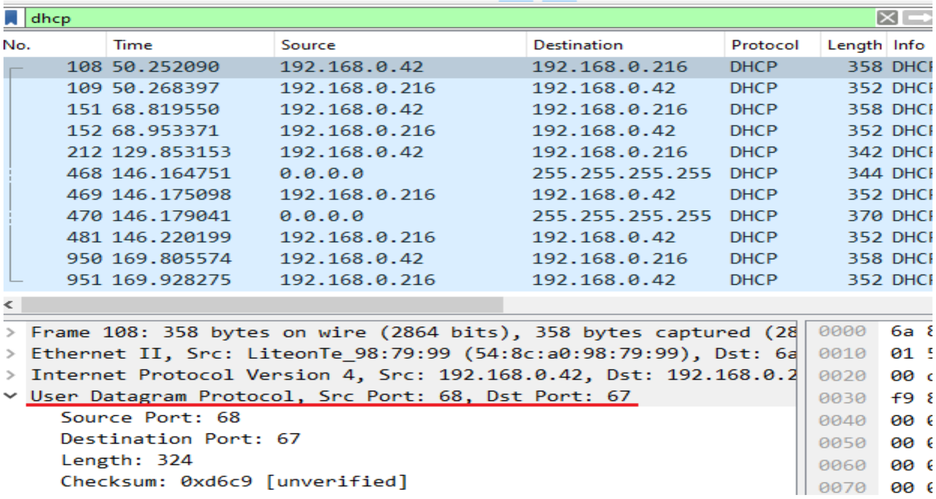


dhcp

No.	Time	Source	Destination	Protocol	Length	Info	Source code
108	50.252090	192.168.0.42	192.168.0.216	DHCP	358	DHCP Request - Transaction ID 0x7b5ef984	68
109	50.268397	192.168.0.216	192.168.0.42	DHCP	352	DHCP ACK - Transaction ID 0x7b5ef984	67
151	68.819550	192.168.0.42	192.168.0.216	DHCP	358	DHCP Request - Transaction ID 0x61e104b8	68
152	68.953371	192.168.0.216	192.168.0.42	DHCP	352	DHCP ACK - Transaction ID 0x61e104b8	67
212	129.853153	192.168.0.42	192.168.0.216	DHCP	342	DHCP Release - Transaction ID 0xc3cc8a96	68
468	146.164751	0.0.0.0	255.255.255.255	DHCP	344	DHCP Discover - Transaction ID 0xa441a7fa	68
469	146.175098	192.168.0.216	192.168.0.42	DHCP	352	DHCP Offer - Transaction ID 0xa441a7fa	67
470	146.179041	0.0.0.0	255.255.255.255	DHCP	370	DHCP Request - Transaction ID 0xa441a7fa	68
481	146.220199	192.168.0.216	192.168.0.42	DHCP	352	DHCP ACK - Transaction ID 0xa441a7fa	67
950	169.805574	192.168.0.42	192.168.0.216	DHCP	358	DHCP Request - Transaction ID 0xc3001e9a	68
951	169.928275	192.168.0.216	192.168.0.42	DHCP	352	DHCP ACK - Transaction ID 0xc3001e9a	67

After finishing capturing we get total of 11 dhcp packets.

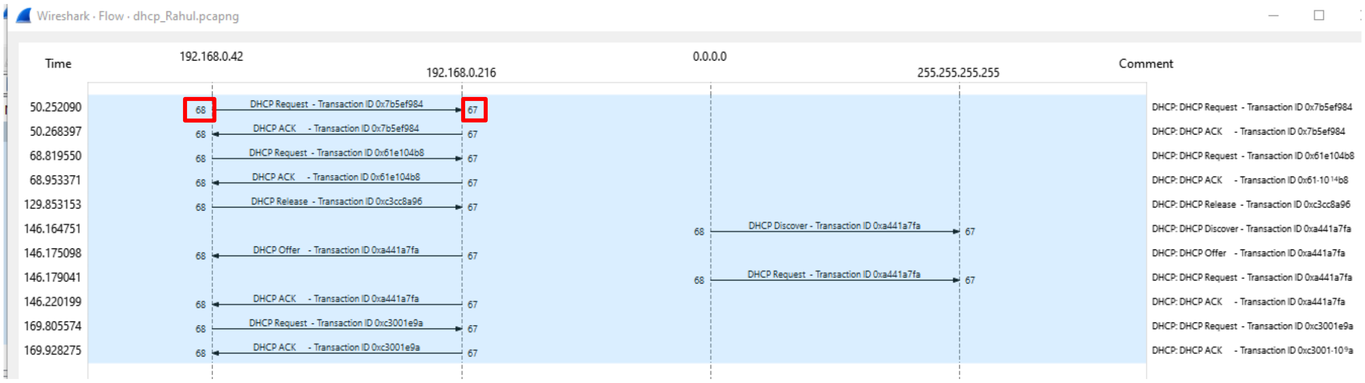
2.a) Are DHCP messages sent over UDP or TCP?



```
dhcp
No.     Time          Source          Destination      Protocol  Length Info
    108 50.252090     192.168.0.42    192.168.0.216    DHCP        358 DHCI
    109 50.268397     192.168.0.216   192.168.0.42     DHCP        352 DHCI
    151 68.819550     192.168.0.42    192.168.0.216    DHCP        358 DHCI
    152 68.953371     192.168.0.216   192.168.0.42     DHCP        352 DHCI
    212 129.853153    192.168.0.42    192.168.0.216    DHCP        342 DHCI
    468 146.164751    0.0.0.0         255.255.255.255  DHCP        344 DHCI
    469 146.175098    192.168.0.216   192.168.0.42     DHCP        352 DHCI
    470 146.179041    0.0.0.0         255.255.255.255  DHCP        370 DHCI
    481 146.220199    192.168.0.216   192.168.0.42     DHCP        352 DHCI
    950 169.805574    192.168.0.42    192.168.0.216    DHCP        358 DHCI
    951 169.928275    192.168.0.216   192.168.0.42     DHCP        352 DHCI

> Frame 108: 358 bytes on wire (2864 bits), 358 bytes captured (28   0000  6a 8
> Ethernet II, Src: LiteonTe_98:79:99 (54:8c:a0:98:79:99), Dst: 6a   0010  01 5
> Internet Protocol Version 4, Src: 192.168.0.42, Dst: 192.168.0.2   0020  00 c
v User Datagram Protocol, Src Port: 68, Dst Port: 67                 0030  f9 8
      Source Port: 68                                                0040  00 e
      Destination Port: 67                                           0050  00 e
      Length: 324                                                    0060  00 e
      Checksum: 0xd6c9 [unverified]                                  0070  00 e
```

DHCP messages are sent over UDP.

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.

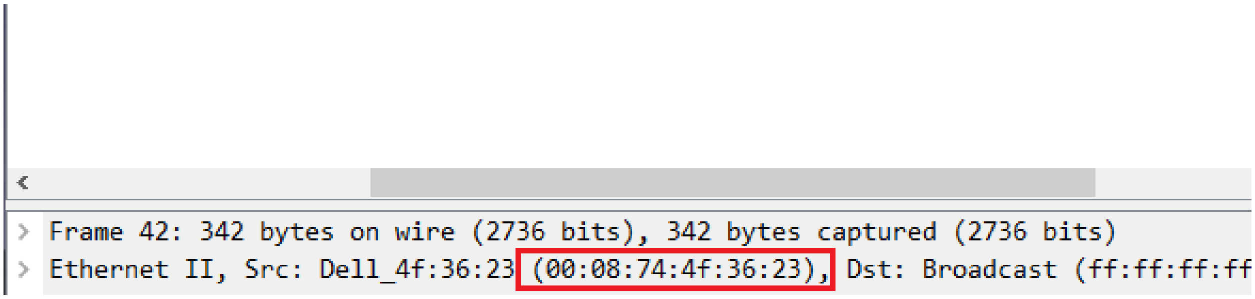


Wireshark · Flow · dhcp_Rahul.pcapng

```
Time         Comment
50.252090    DHCP: DHCP Request  - Transaction ID 0x7b5ef984
50.268397    DHCP: DHCP ACK      - Transaction ID 0x7b5ef984
68.819550    DHCP: DHCP Request  - Transaction ID 0x61e104b8
68.953371    DHCP: DHCP ACK      - Transaction ID 0x61-10¹⁴b8
129.853153   DHCP: DHCP Release  - Transaction ID 0xc3cc8a96
146.164751   DHCP: DHCP Discover - Transaction ID 0xa441a7fa
146.175098   DHCP: DHCP Offer    - Transaction ID 0xa441a7fa
146.179041   DHCP: DHCP Request  - Transaction ID 0xa441a7fa
146.220199   DHCP: DHCP ACK      - Transaction ID 0xa441a7fa
169.805574   DHCP: DHCP Request  - Transaction ID 0xc3001e9a
169.928275   DHCP: DHCP ACK      - Transaction ID 0xc3001-10⁹a
```

192.168.0.42
192.168.0.216
0.0.0.0
255.255.255.255
68 DHCP Request - Transaction ID 0x7b5ef984 67
68 DHCP ACK - Transaction ID 0x7b5ef984 67
68 DHCP Request - Transaction ID 0x61e104b8 67
68 DHCP ACK - Transaction ID 0x61e104b8 67
68 DHCP Release - Transaction ID 0xc3cc8a96 67
68 DHCP Discover - Transaction ID 0xa441a7fa 67
68 DHCP Offer - Transaction ID 0xa441a7fa 67
68 DHCP Request - Transaction ID 0xa441a7fa 67
68 DHCP ACK - Transaction ID 0xa441a7fa 67
68 DHCP Request - Transaction ID 0xc3001e9a 67
68 DHCP ACK - Transaction ID 0xc3001e9a 67

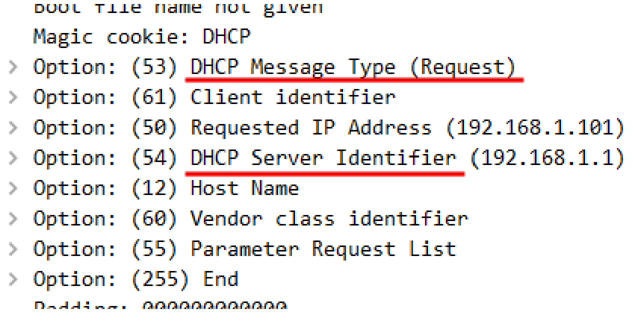
c) What is the link-layer (e.g., Ethernet) address of your host?



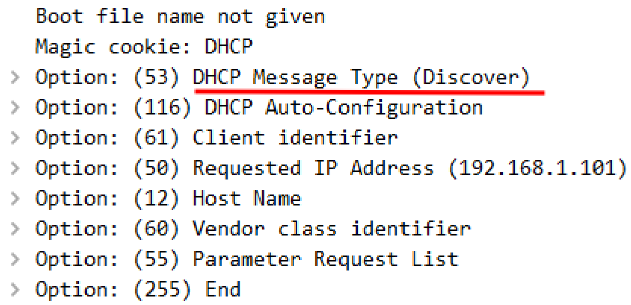
```
> Frame 42: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits)
> Ethernet II, Src: Dell_4f:36:23 (00:08:74:4f:36:23), Dst: Broadcast (ff:ff:ff:ff
```

The address of the link-layer is called MAC address.

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



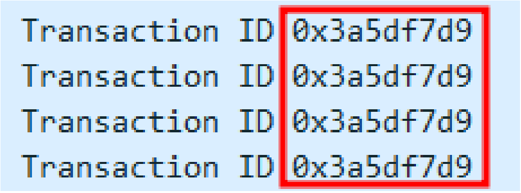
```
  Boot file name not given
  Magic cookie: DHCP
> Option: (53) DHCP Message Type (Request)
> Option: (61) Client identifier
> Option: (50) Requested IP Address (192.168.1.101)
> Option: (54) DHCP Server Identifier (192.168.1.1)
> Option: (12) Host Name
> Option: (60) Vendor class identifier
> Option: (55) Parameter Request List
> Option: (255) End
  Padding: 000000000000
```



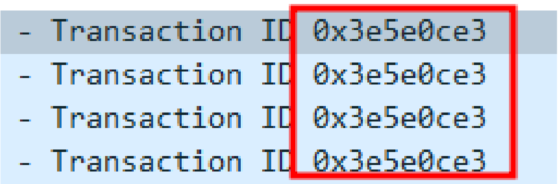
```
  Boot file name not given
  Magic cookie: DHCP
> Option: (53) DHCP Message Type (Discover)
> Option: (116) DHCP Auto-Configuration
> Option: (61) Client identifier
> Option: (50) Requested IP Address (192.168.1.101)
> Option: (12) Host Name
> Option: (60) Vendor class identifier
> Option: (55) Parameter 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 the Transaction-ID in the second set (Request/ACK) set of DHCP messages? What is the purpose of the Transaction-ID field?

The transaction ID in the first four packets is “0x3e5e0ce3”.
The transaction ID in the second set of DHCP messages is “0x3a5d7d9”.



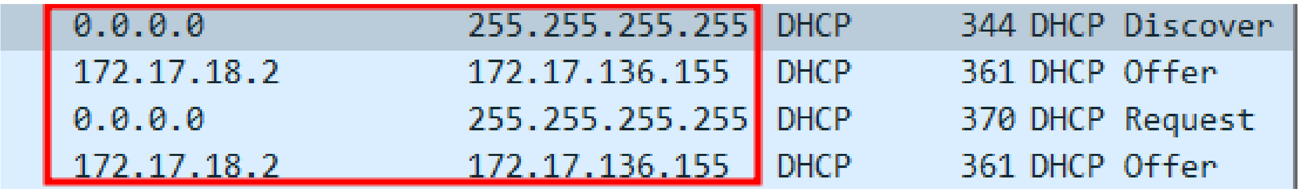
```
Transaction ID 0x3a5df7d9
Transaction ID 0x3a5df7d9
Transaction ID 0x3a5df7d9
Transaction ID 0x3a5df7d9
```



```
- Transaction ID 0x3e5e0ce3
- Transaction ID 0x3e5e0ce3
- Transaction ID 0x3e5e0ce3
- Transaction ID 0x3e5e0ce3
```

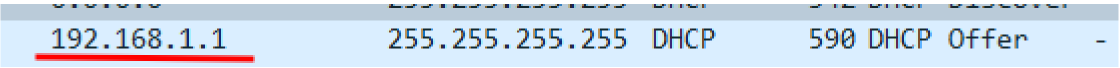
f) A host uses DHCP to obtain an IP address, among other things. But a host’s IP address is not confirmed until the end of the four-message exchange! If the IP address is not set until the end of the four-message exchange, then what values are used in the IP datagrams in the four-message exchange? For 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.

For discover and request: Source IP= 0.0.0.0 and Destination= 255.255.255.255
For offer and ACK: Source IP= 172.17.18.2 and Destination= 172.17.136.155



```
0.0.0.0         255.255.255.255  DHCP   344 DHCP Discover
172.17.18.2     172.17.136.155   DHCP   361 DHCP Offer
0.0.0.0         255.255.255.255  DHCP   370 DHCP Request
172.17.18.2     172.17.136.155   DHCP   361 DHCP Offer
```

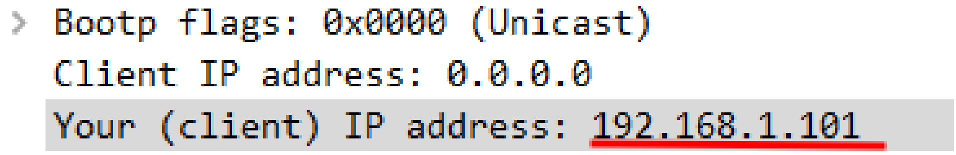
g) What is the IP address of your DHCP server?
IP=192.168.1.1



```
192.168.1.1          255.255.255.255  DHCP      590 DHCP Offer    -
```

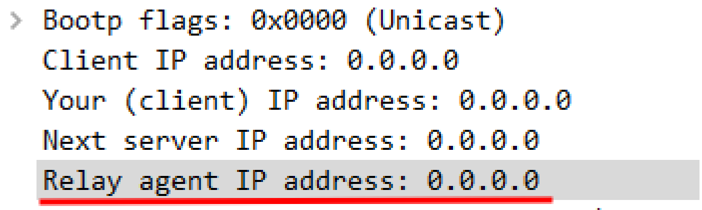
h) What IP address is the DHCP server offering to your host in the DHCP Offer message? Indicate which DHCP message contains the offered DHCP address.

IP=192.168.1.101



```
> Bootp flags: 0x0000 (Unicast)
  Client IP address: 0.0.0.0
  Your (client) IP address: 192.168.1.101
```

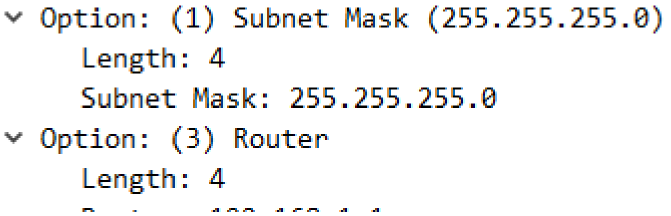
i) In the example screenshot in this assignment, there is no relay agent between the host and the DHCP server. What values in the trace indicate the absence of a relay agent? Is there a relay agent in your experiment? If so what is the IP address of the agent?



```
> 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
```

Therefore, there is no Relay agent.

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

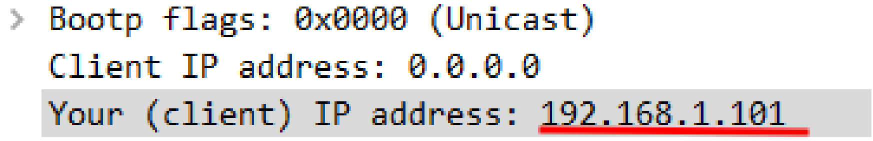


```
v Option: (1) Subnet Mask (255.255.255.0)
      Length: 4
      Subnet Mask: 255.255.255.0
v Option: (3) Router
      Length: 4
```

The router forwards the request packet to the network and it reaches the DHCP server in the other LAN network, when the DHCP server is not present in our network and if it is present in some other LAN then the DHCP DISCOVER message is sent to the router in its network.

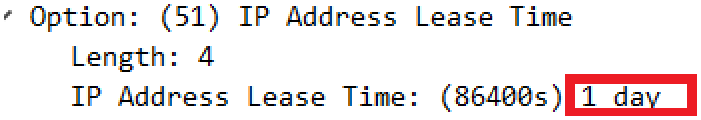
k) In the DHCP trace file, the DHCP server offers a specific IP address to the client. In the client's response to the first server OFFER message, does the client accept this IP address? Where in the client's RESPONSE is the client's requested address?

Yes, the server accepted the offered IP address.



```
> Bootp flags: 0x0000 (Unicast)
  Client IP address: 0.0.0.0
  Your (client) IP address: 192.168.1.101
```

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

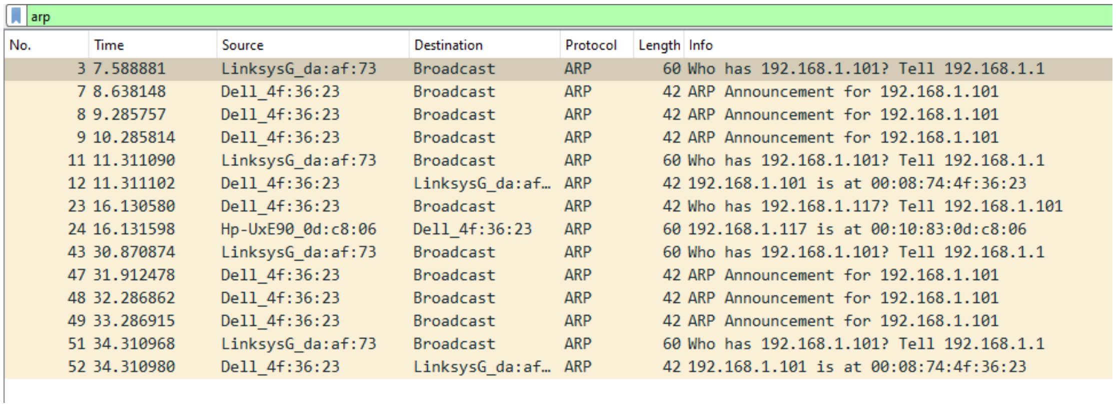


```
⌄ Option: (51) IP Address Lease Time
    Length: 4
    IP Address Lease Time: (86400s) 1 day
```

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?

The purpose of releasing messages is to release IP address to the computer.
NO, the DHCP server does not send ACK receipt of client's DHCP request.

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
Yes, it is visible that many ARP packets that were transferred in the experiment.



```
arp
No.  Time       Source             Destination        Protocol Length Info
   3 7.588881   LinksysG_da:af:73  Broadcast          ARP       60 Who has 192.168.1.101? Tell 192.168.1.1
   7 8.638148   Dell_4f:36:23      Broadcast          ARP       42 ARP Announcement for 192.168.1.101
   8 9.285757   Dell_4f:36:23      Broadcast          ARP       42 ARP Announcement for 192.168.1.101
   9 10.285814  Dell_4f:36:23      Broadcast          ARP       42 ARP Announcement for 192.168.1.101
  11 11.311090  LinksysG_da:af:73  Broadcast          ARP       60 Who has 192.168.1.101? Tell 192.168.1.1
  12 11.311102  Dell_4f:36:23      LinksysG_da:af…    ARP       42 192.168.1.101 is at 00:08:74:4f:36:23
  23 16.130580  Dell_4f:36:23      Broadcast          ARP       42 Who has 192.168.1.117? Tell 192.168.1.101
  24 16.131598  Hp-UxE90_0d:c8:06  Dell_4f:36:23      ARP       60 192.168.1.117 is at 00:10:83:0d:c8:06
  43 30.870874  LinksysG_da:af:73  Broadcast          ARP       60 Who has 192.168.1.101? Tell 192.168.1.1
  47 31.912478  Dell_4f:36:23      Broadcast          ARP       42 ARP Announcement for 192.168.1.101
  48 32.286862  Dell_4f:36:23      Broadcast          ARP       42 ARP Announcement for 192.168.1.101
  49 33.286915  Dell_4f:36:23      Broadcast          ARP       42 ARP Announcement for 192.168.1.101
  51 34.310968  LinksysG_da:af:73  Broadcast          ARP       60 Who has 192.168.1.101? Tell 192.168.1.1
  52 34.310980  Dell_4f:36:23      LinksysG_da:af…    ARP       42 192.168.1.101 is at 00:08:74:4f:36:23
```