Name : MOHAMMED TOUSIF
Roll: CB.EN.P2CYS22008

ANALYZING DHCP USING PROTOCOL ANALYZER

Date :- 01-11-2022

Aim :- To analyze dynamic host configuration protocol (DHCP) using protocol analyzer.

Tools Required :- Windows OS , CMD with Administrator privilege , Wireshark.

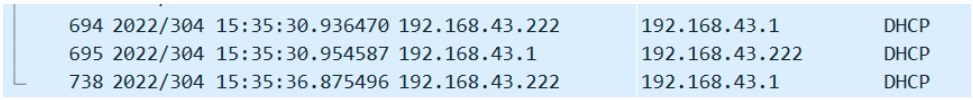
Procedure :-

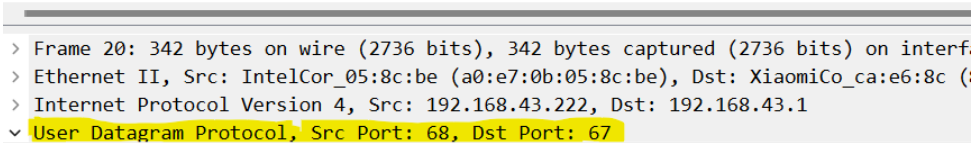
1. Perform the following steps to capture the DHCP traffic.
    - ipconfig/release
    - Capture Wireshark
    - ipconfig /renew
    - ipconfig /renew
    - ipconfig/release
    - ipconfig /renew

Protocol	Length	Info
DHCP	342	DHCP Discover - Transaction ID 0x3e5e0ce3
DHCP	590	DHCP Offer - Transaction ID 0x3e5e0ce3
DHCP	342	DHCP Request - Transaction ID 0x3e5e0ce3
DHCP	590	DHCP ACK - Transaction ID 0x3e5e0ce3
DHCP	342	DHCP Request - Transaction ID 0x257e55a3
DHCP	590	DHCP ACK - Transaction ID 0x257e55a3
DHCP	342	DHCP Release - Transaction ID 0xb7a32733
DHCP	342	DHCP Discover - Transaction ID 0x3a5df7d9
DHCP	590	DHCP Offer - Transaction ID 0x3a5df7d9
DHCP	342	DHCP Request - Transaction ID 0x3a5df7d9
DHCP	590	DHCP ACK - Transaction ID 0x3a5df7d9

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

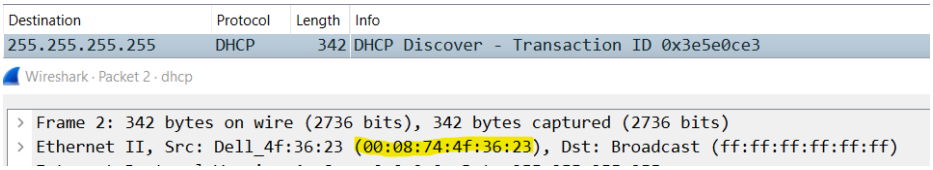
a) Are DHCP messages sent over UDP or TCP?





DHCP messages sent over UDP.

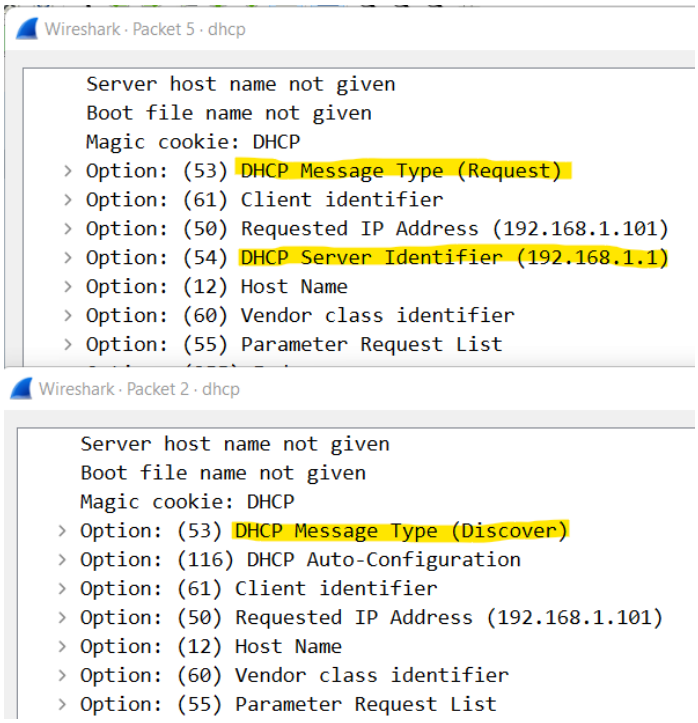
c) What is the link-layer (e.g., Ethernet) address of your host?



00:08:74:4f:36:23

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

DHCP Message Type.
DHCP Server Identifier.



e) What is the value of the Transaction-ID in each of the first four (Discover/Offer/Request/ACK) DHCP messages?

Transaction-ID of first four DHCP messages are: 0x3e5e0ce3.

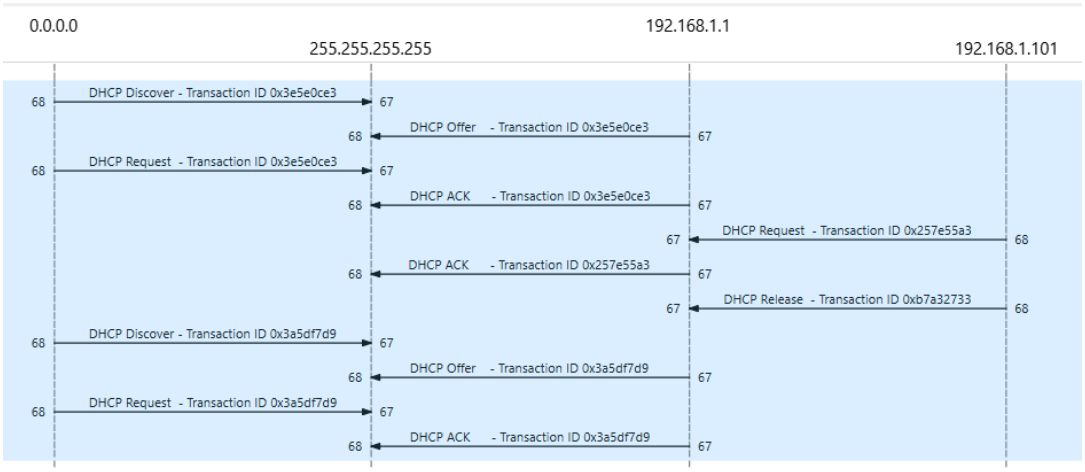
What are the values of the Transaction-ID in the second set (Request/ACK) set of DHCP messages?

Transaction-ID of first second set DHCP messages are: 0x3a5df7d9.

What is the purpose of the Transaction-ID field?

To check the flow of messages transferred between client and DHCP server. To check any inappropriate traffic and ensuring good communication.

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



0.0.0.0 - Client's Address
255.255.255.255 - Server's Address

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

192.168.1.1	255.255.255.255	DHCP	590	DHCP Offer
0.0.0.0	255.255.255.255	DHCP	342	DHCP Request
192.168.1.1	255.255.255.255	DHCP	590	DHCP ACK

192.168.1.1

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.

```
Dynamic Host Configuration Protocol (Offer)
  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
```

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?

```
Your (client) IP address: 192.168.1
Next server IP address: 0.0.0.0
Relay agent IP address: 0.0.0.0
Client MAC address: Dell 4f:36:23 (
```

As there are no relay agents between host and DHCP server. It shows Relay agent IP address as : 0.0.0.0. If there is , then it shows it's IP address.

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

```
Option: (53) DHCP Message Type (Offer)
    Length: 1
    DHCP: Offer (2)
Option: (1) Subnet Mask (255.255.255.0)
    Length: 4
    Subnet Mask: 255.255.255.0
Option: (3) Router
    Length: 4
    Router: 192.168.1.1
```

DHCP DISCOVER message is sent to router in the network of LAN to connect. The router forwards the packet to network and reaches DHCP server.

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?

```
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
```

The server accepted the offered IP address.

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

```
> Option: (53) DHCP Message Type (ACK)
> Option: (1) Subnet Mask (255.255.255.0)
> Option: (3) Router
> Option: (6) Domain Name Server
> Option: (15) Domain Name
v Option: (51) IP Address Lease Time
    Length: 4
    IP Address Lease Time: (86400s) 1 day
```

Lease Time is which the IP address available for a time period. Lease time here is 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?

DHCP Release will release the IP address of the assigned computer and it doesn't issue an acknowledgment receipt of client's DHCP request.

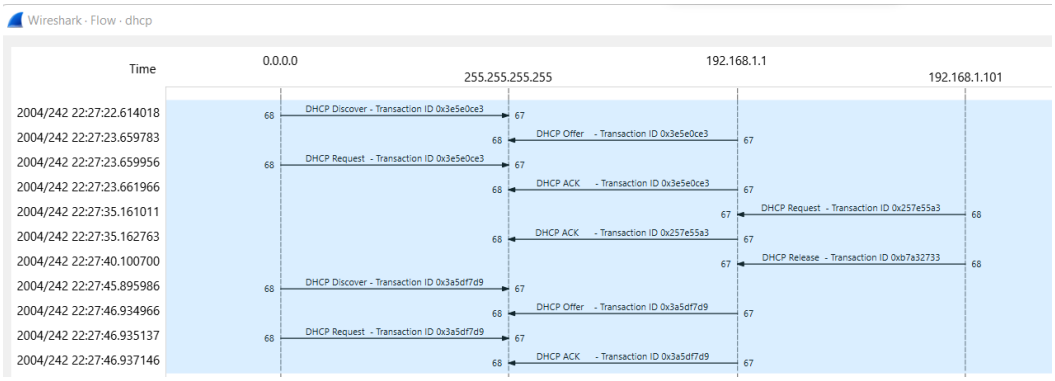
If client's DHCP release message is lost, server not know the release request and the IP remains still same.

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?

```
ARP          60 Who has 192.168.1.101? Tell 192.168.1.1
DHCP        590 DHCP Offer    - Transaction ID 0x3a5df7d9
DHCP        342 DHCP Request  - Transaction ID 0x3a5df7d9
DHCP        590 DHCP ACK      - Transaction ID 0x3a5df7d9
ARP          42 ARP Announcement for 192.168.1.101
ARP          42 ARP Announcement for 192.168.1.101
ARP          42 ARP Announcement for 192.168.1.101
IGMPv3       54 Membership Report / Join group 239.255.255.250 for any sources
ARP          60 Who has 192.168.1.101? Tell 192.168.1.1
ARP          42 192.168.1.101 is at 00:08:74:4f:36:23
```

Yes , there are some ARP packets during DHCP packet-exchange period. ARP packets are used to verify to allocate which IP address to which computer stated.

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.



For DISCOVER & OFFER requests:
Source Port :67
Destination Port : 68

For REQUEST & ACK requests:
Source Port :68
Destination Port : 67

Result : Thus , analyzing dynamic host configuration protocol (DHCP) using protocol analyzer is successfully done.