

ASSIGNMENT 2:

NAME: Stuti Parmar

STUDENT ID: 218516625

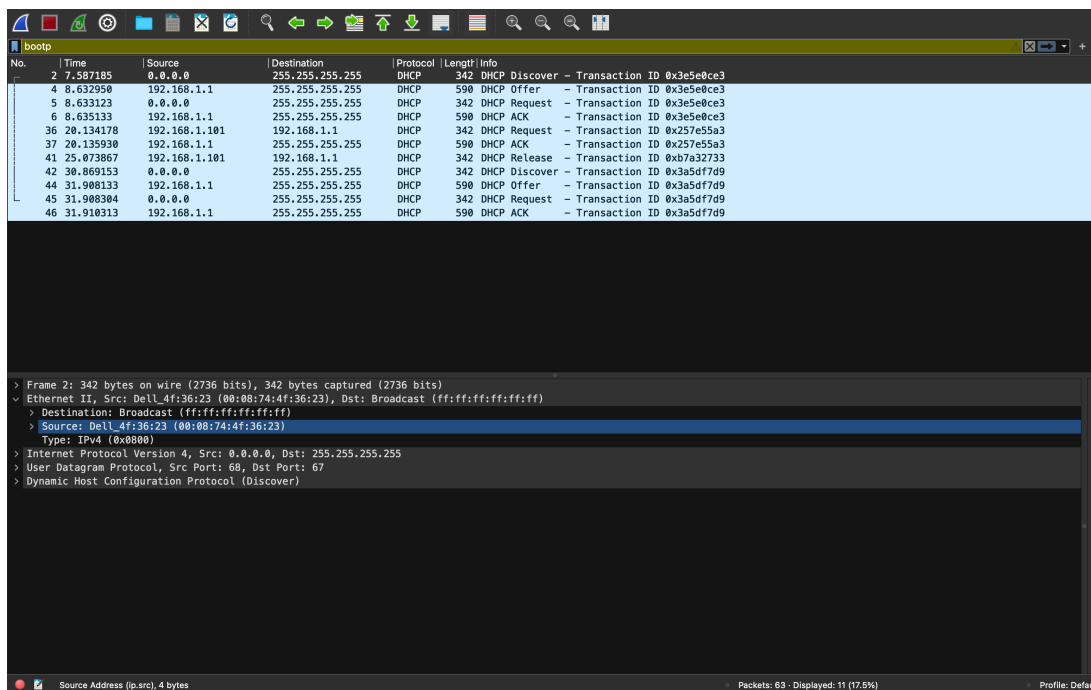
EECS 3214

Question 3: Understanding DHCP

Q.3

I used the ZIP folder and extracted the dhcp-ethereal-trace-1 and opened it in Wireshark.

- The **Source** address in the Ethernet II section is the link-layer (Ethernet) address of the sender. Therefore the link layer address of sender is: Dell_4f:36:23 (00:08:74:4f:36:23). Attaching screenshot below.



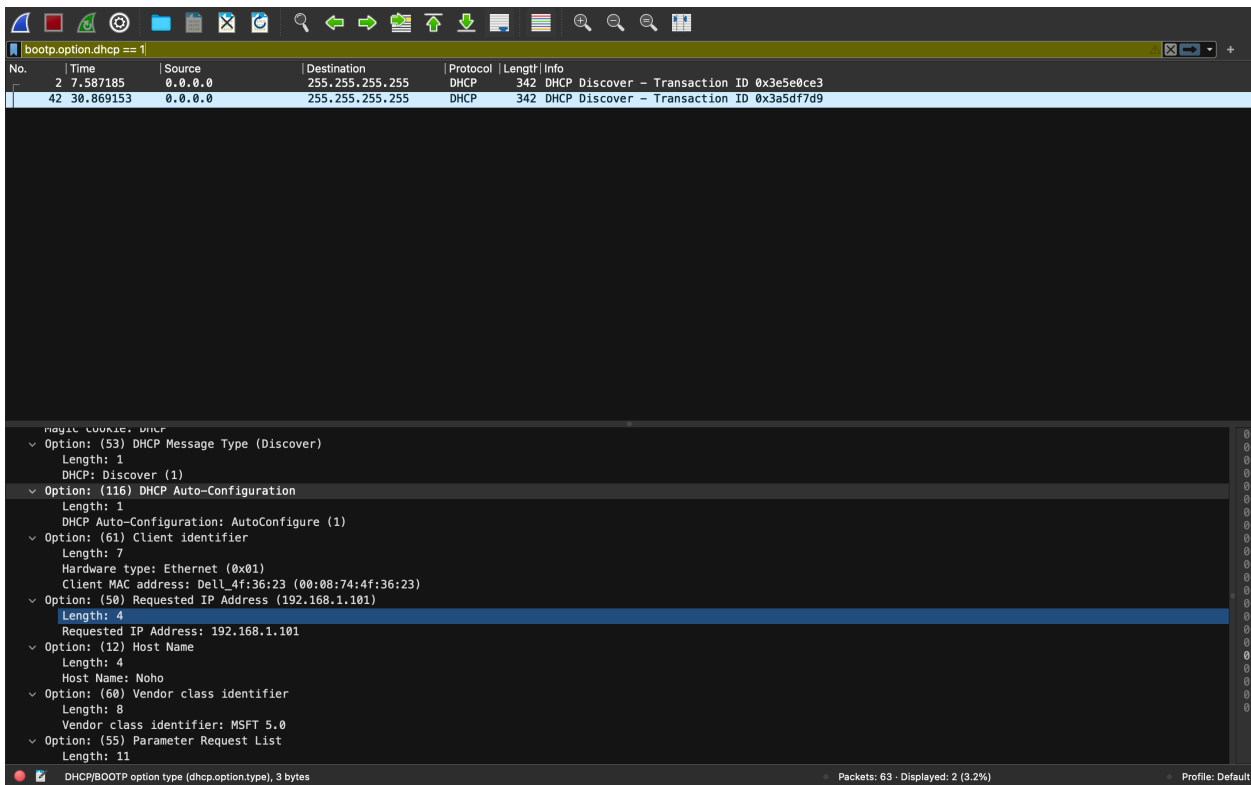
Attaching the print of packets summary below.

/Users/stuti/Desktop/dhcp-ethereal-trace-1 63 total packets, 11 shown

```
No.      Time      Source      Destination  Protocol Length Info
2 7.587185 0.0.0.0     255.255.255.255 DHCP        342    DHCP Discover - Transaction ID 0x3e5e0ce3
Frame 2: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) on interface 0
Ethernet II, Src: Dell_4f:36:23 (00:08:74:4f:36:23), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
  Destination: Broadcast (ff:ff:ff:ff:ff:ff)
  Source: Dell_4f:36:23 (00:08:74:4f:36:23)
    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 (Discover)
      0100 .... = Version: 4
      .... 0101 = Header Length: 20 bytes (5)
      Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
      Total Length: 328
      Identification: 0xb310 (45840)
      000. .... = Flags: 0x0
      ...0 0000 0000 0000 = Fragment Offset: 0
      Time to Live: 128
      Protocol: UDP (17)
      Header Checksum: 0x8695 [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)
```

Q.4

DHCP Discover message:



The image shows a Wireshark packet capture of a DHCP Discover message. The packet list at the top shows two DHCP Discover packets. The selected packet (No. 42) is expanded in the packet details pane, showing the DHCP Message Type (Discover) and various options including Client identifier, Requested IP Address, Host Name, and Vendor class identifier.

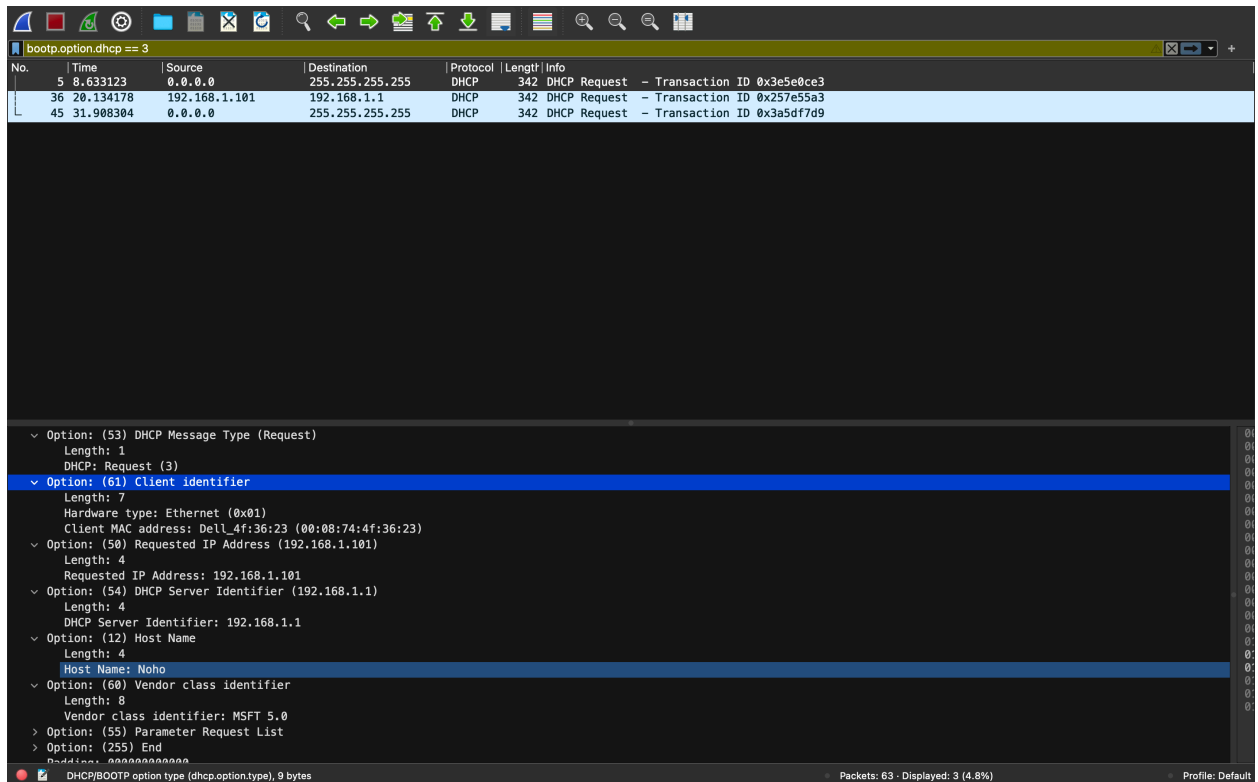
No.	Time	Source	Destination	Protocol	Length	Info
2	7.587185	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x3e5e0ce3
42	30.869153	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x3a5df7d9

Packet 42 details:

- Option: (53) DHCP Message Type (Discover)
 - Length: 1
 - DHCP: Discover (1)
- Option: (116) DHCP Auto-Configuration
 - Length: 1
 - DHCP Auto-Configuration: AutoConfigure (1)
- Option: (61) Client identifier
 - Length: 7
 - Hardware type: Ethernet (0x01)
 - Client MAC address: Dell_4f:36:23 (00:08:74:4f:36:23)
- Option: (50) Requested IP Address (192.168.1.101)
 - Length: 4
 - Requested IP Address: 192.168.1.101
- Option: (12) Host Name
 - Length: 4
 - Host Name: Noho
- Option: (60) Vendor class identifier
 - Length: 8
 - Vendor class identifier: MSFT 5.0
- Option: (55) Parameter Request List
 - Length: 11

DHCP/BOOTP option type (dhcp.option.type), 3 bytes | Packets: 63 · Displayed: 2 (3.2%) | Profile: Default

DHCP Request message:



The image shows a Wireshark packet capture of a DHCP Request message. The packet list at the top shows three DHCP Request packets. The selected packet (No. 45) is expanded in the packet details pane, showing the DHCP Message Type (Request) and various options including Client identifier, Requested IP Address, DHCP Server Identifier, Host Name, and Vendor class identifier.

No.	Time	Source	Destination	Protocol	Length	Info
5	8.633123	0.0.0.0	255.255.255.255	DHCP	342	DHCP Request - Transaction ID 0x3e5e0ce3
36	20.134178	192.168.1.101	192.168.1.1	DHCP	342	DHCP Request - Transaction ID 0x257e55a3
45	31.988384	0.0.0.0	255.255.255.255	DHCP	342	DHCP Request - Transaction ID 0x3a5df7d9

Packet 45 details:

- Option: (53) DHCP Message Type (Request)
 - Length: 1
 - DHCP: Request (3)
- Option: (61) Client identifier
 - Length: 7
 - Hardware type: Ethernet (0x01)
 - Client MAC address: Dell_4f:36:23 (00:08:74:4f:36:23)
- Option: (50) Requested IP Address (192.168.1.101)
 - Length: 4
 - Requested IP Address: 192.168.1.101
- Option: (54) DHCP Server Identifier (192.168.1.1)
 - Length: 4
 - DHCP Server Identifier: 192.168.1.1
- Option: (12) Host Name
 - Length: 4
 - Host Name: Noho
- Option: (60) Vendor class identifier
 - Length: 8
 - Vendor class identifier: MSFT 5.0
- Option: (55) Parameter Request List
- Option: (255) End

DHCP/BOOTP option type (dhcp.option.type), 9 bytes | Packets: 63 · Displayed: 3 (4.8%) | Profile: Default

Differences between discover and request message:

- **Different transaction IDs:** DHCP request Transaction ID: 0x257e55a3, DHCP discover Transaction ID: 0x3e5e0ce3
- **DHCP Discover:** The **Message Type** field will show **Discover** (code 1). **DHCP Request:** The **Message Type** field will show **Request** (code 3).

Q.8

No.	Time	Source	Destination	Protocol	Length	Info
2	7.587185	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x3e5e0ce3
4	8.632950	192.168.1.1	255.255.255.255	DHCP	590	DHCP Offer - Transaction ID 0x3e5e0ce3
5	8.633123	0.0.0.0	255.255.255.255	DHCP	342	DHCP Request - Transaction ID 0x3e5e0ce3
6	8.635133	192.168.1.1	255.255.255.255	DHCP	590	DHCP ACK - Transaction ID 0x3e5e0ce3
36	20.134178	192.168.1.101	192.168.1.1	DHCP	342	DHCP Request - Transaction ID 0x257e55a3
37	20.135930	192.168.1.1	255.255.255.255	DHCP	590	DHCP ACK - Transaction ID 0x257e55a3
41	25.073867	192.168.1.101	192.168.1.1	DHCP	342	DHCP Release - Transaction ID 0xb7a32733
42	30.869153	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x3a5df7d9
44	31.908133	192.168.1.1	255.255.255.255	DHCP	590	DHCP Offer - Transaction ID 0x3a5df7d9
45	31.908304	0.0.0.0	255.255.255.255	DHCP	342	DHCP Request - Transaction ID 0x3a5df7d9
46	31.910313	192.168.1.1	255.255.255.255	DHCP	590	DHCP ACK - Transaction ID 0x3a5df7d9

Field	Value
Ethernet II, Src: LinksysGroup_data:af:73 (00:06:25:da:af:73), Dst: Broadcast (ff:ff:ff:ff:ff:ff)	
Internet Protocol Version 4, Src: 192.168.1.1, Dst: 255.255.255.255	
User Datagram Protocol, Src Port: 67, Dst Port: 68	
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	
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:f3:36:23)	
Client hardware address padding: 00000000000000000000	
Server host name not given	
Boot file name not given	
Magic cookies: DHCP	
Option: (53) DHCP Message Type (Offer)	
Option: (1) Subnet Mask (255.255.255.0)	
Option: (3) Router	
Option: (6) Domain Name Server	
Option: (15) Domain Name	
Option: (51) IP Address Lease Time	
Option: (54) DHCP Server Identifier (192.168.1.1)	

DHCP offer message:

The IP address is the DHCP server offering to your host in the DHCP Offer is: 192.168.1.10. Your (client) address contains the offered IP address.