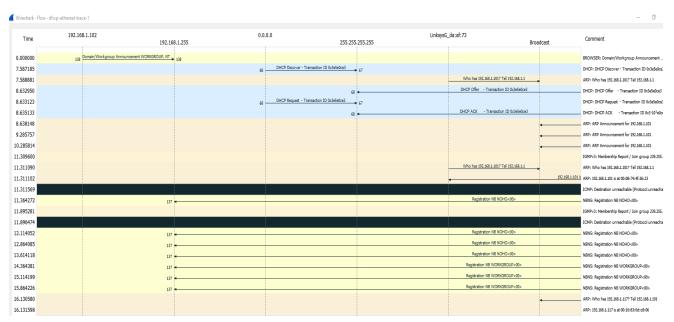
## COMP 3203 Wireshark 7

Name: Nirmith Victor D'Almeida

Number: 101160124

## They are sent over UDP

2.



Yes they are the same port number

```
3.

Ethernet II, Src: Dell_4f:36:23 (00:08:74:4f:36:23), Dst: Broadcast (ff:ff:ff:ff:ff)

Destination: Broadcast (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)
```

The link-layer address is 00:08:74:4f:36:23

```
v Option: (53) DHCP Message Type (Request)
    Length: 1
    DHCP: Request (3)
```

From the above two images we can see the difference in the DHCP Message Type.

## 5. First Set

```
2 7.587185
                                                                   DHCP
                                                                            342 DHCP Discover
                          0.0.0.0
                                              255.255.255.255
 <
    Frame 2: 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:ff:ff)
 > Internet Protocol Version 4, Src: 0.0.0.0, Dst: 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: 0x3e5e0ce3
      Seconds elapsed: 0
      4 8.632950
                        192.168.1.1
                                              255.255.255.255
                                                                  DHCP
                                                                            590 DHCP Offer
Frame 4: 590 bytes on wire (4720 bits), 590 bytes captured (4720 bits)
Ethernet II, Src: LinksysG da: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
v 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 TP address 0000
                                             255.255.255.255
      5 8.633123
                        0.0.0.0
                                                                 DHCP
                                                                           342 DHCP Request
 Frame 5: 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: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 (Request)
    Message type: Boot Request (1)
    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
```

```
6 8.635133
                         192.168.1.1
                                               255.255.255.255
                                                                    DHCP
                                                                              590 DHCP ACK
 Frame 6: 590 bytes on wire (4720 bits), 590 bytes captured (4720 bits)
Ethernet II, Src: LinksysG da: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 (ACK)
    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)
The value is 0x3e5e0ce3
SECOND SET
      36 20.134178
                         192.168.1.101
                                              192.168.1.1
                                                                  DHCP
                                                                            342 DHCP Request
      37 20.135930
                         192.168.1.1
                                              255.255.255.255
                                                                  DHCP
                                                                            590 DHCP ACK
  Frame 36: 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: LinksysG_da:af:73 (00:06:25:da:af:7
Internet Protocol Version 4, Src: 192.168.1.101, Dst: 192.168.1.1
 > 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: 0x257e55a3
     Seconds elapsed: 0
     Roots flags: Avadad (Unicast)
     37 20.135930
                        192.168.1.1
                                              255.255.255.255
                                                                    DHCP
                                                                              590 DHCP ACK
 Frame 37: 590 bytes on wire (4720 bits), 590 bytes captured (4720 bits)
 Ethernet II, Src: LinksysG_da: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 (ACK)
    Message type: Boot Reply (2)
    Hardware type: Ethernet (0x01)
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0x257e55a3
    Seconds elapsed: 0
 > Bootp flags: 0x0000 (Unicast)
    Client IP address: 192.168.1.101
    Your (client) IP address: 192.168.1.101
```

## The transcation ID of second set is 0x257e55a3

The purpose of the transaction ID is to identify if a message is part of a set of messages related to one transaction.

6.

2 7.587185 0.0.0.0 255.255.255.255 DHCP 342 DHCP Discover -Broadcast 3 7.588881 LinksysG\_da:af:73 ARP 60 Who has 192.168 4 8.632950 192.168.1.1 255.255.255.255 DHCP 590 DHCP Offer 5 8.633123 0.0.0.0 255.255.255.255 DHCP 342 DHCP Request 6 8.635133 192.168.1.1 255.255.255.255 DHCP 590 DHCP ACK 7 8.638148 Dell 4f:36:23 Broadcast ARP 42 ARP Announcemen

Discover -> Source 0.0.0.0 -> Destination 255.255.255.255

Offer -> Source 192.168.1.1 -> Destination 255.255.255.255

Request -> Source 0.0.0.0 -> Destination 255.255.255.255

ACK -> Source 192.168.1.1 -> Destination 255.255.255.255

7.

4 8.632950	192.168.1.1	255.255.255.255	DHCP	590 DHCP Offer
5 8.633123	0.0.0.0	255.255.255.255	DHCP	342 DHCP Request
6 8.635133	192.168.1.1	255.255.255.255	DHCP	590 DHCP ACK
7 8.638148	Dell_4f:36:23	Broadcast	ARP	42 ARP Announce
0 0 105757	U-11 Nt.26.33	Proodcast	ADD	40 APD Appoints

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)

The IP address is 192.168.1.1

```
8.
      Hardware type: Ethernet (ปรช1)
      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)
      Server host name not given
      Boot file name not given
      Magic cookie: DHCP
    Option: (53) DHCP Message Type (Offer)
         Length: 1
         DHCP: Offer (2)
    v 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
    V Option: (6) Domain Name Server
         Length: 8
         Domain Name Server: 63.240.76.19
         Domain Name Server: 204.127.198.19
    ∨ Option: (15) Domain Name
         Length: 22
```

Domain Name: ne2.client2.attbi.com

∨ Option: (51) IP Address Lease Time

```
2 7.587185
                           0.0.0.0
                                                255.255.255.255
                                                                      DHCP
                                                                                342 DHCP Disco
        3 7.588881
                           LinksysG_da:af:73
                                                Broadcast
                                                                      ARP
                                                                                60 Who has 19
        4 8.632950
                           192.168.1.1
                                                255.255.255.255
                                                                      DHCP
                                                                                590 DHCP Offer
                                                255.255.255.255
        5 8.633123
                           0.0.0.0
                                                                      DHCP
                                                                                342 DHCP Reque
        6 8.635133
                           192.168.1.1
                                                255.255.255.255
                                                                      DHCP
                                                                                590 DHCP ACK
                           Dell_4f:36:23
                                                                      ARP
        7 8.638148
                                                Broadcast
                                                                                42 ARP Announ
                           Dell 4f:36:23
        8 9.285757
                                                Broadcast
                                                                      ARP
                                                                                42 ARP Announ
                           No11 /f⋅36.23
        9 10 28581/
                                                Broadcast
                                                                      ΛRP
                                                                                 12 ARP Announ
   Frame 6: 590 bytes on wire (4720 bits), 590 bytes captured (4720 bits)
 > Ethernet II, Src: LinksysG_da: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 (ACK)

      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
The IP address is 0.0.0.0
```

10. IP address for router help identify default internet gateway where as subnet mask line define the subnet that is available

```
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)
  Server host name not given
  Boot file name not given
  Magic cookie: DHCP
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
V Option: (3) Router
    Length: 4
    Router: 192.168.1.1
Option: (6) Domain Name Server
    Length: 8
```

	· -			
4 8.632950	192.168.1.1	255.255.255.255	DHCP	590 DHCP Offer
5 8.633123	0.0.0.0	255.255.255.255	DHCP	342 DHCP Request
6 8.635133	192.168.1.1	255.255.255.255	DHCP	590 DHCP ACK -
7 8.638148	Dell_4f:36:23	Broadcast	ARP	42 ARP Announcemer
8 9.285757	Dell_4f:36:23	Broadcast	ARP	42 ARP Announcemer
9 10 28581/	No11 /f•36•33	Recodeset	ΛRΡ	12 ARP Announcemen

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 Magic cookie: DHCP

v Option: (53) DHCP Message Type (Offer)

Length: 1 DHCP: Offer (2)

v Option: (1) Subnet Mask (255.255.255.0)

					3
	1 0.000000	192.168.1.102	192.168.1.255	BROWSER	250 Domain/Workgroup A
	2 7.587185	0.0.0.0	255.255.255.255	DHCP	342 DHCP Discover - Tra
	3 7.588881	LinksysG_da:af:73	Broadcast	ARP	60 Who has 192.168.1.1
_	4 8.632950	192.168.1.1	255.255.255.255	DHCP	590 DHCP Offer - Tra
	5 8.633123	0.0.0.0	255.255.255.255	DHCP	342 DHCP Request - Tra
	6 8.635133	192.168.1.1	255.255.255.255	DHCP	590 DHCP ACK - Tra
	7 8.638148	Dell_4f:36:23	Broadcast	ARP	42 ARP Announcement fo
	8 9.285757	Dell_4f:36:23	Broadcast	ARP	42 ARP Announcement fo
	9 10 28581/	Noll /f⋅36⋅23	Renadcast	ΛRΡ	12 ARP Announcement for
	Length: 1				

DHCP: ACK (5)

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

Length: 8

Domain Name Server: 63.240.76.19 Domain Name Server: 204.127.198.19

v Option: (15) Domain Name

Length: 22

Domain Name: ne2.client2.attbi.com v Option: (51) IP Address Lease Time

Length: 4

IP Address Lease Time: (86400s) 1 day

v Option: (54) DHCP Server Identifier (192.168.1.1)

Length: 4

DHCP Server Identifier: 192.168.1.1

v Option: (255) End
 Option End: 255

The lease time is 1 Day.

Purpose is amount of time the DHCP server assign an IP address to a client.

- 13. The DHCP release message tells the DHCP server that it wants to cancel the ip address offered. The DHCP doesn't issue an acknowledgment of receipt of the client's DHCP request. If the message is lost it (ip address) will just be there till the lease time expires.
- 14. Yes the ARP messages where sent during the DHCP packet exchange period. It asks if any of the machines are using that particular IP address.