Experiment No. 9

Aim : Use shark to understand the operation of TCP/IP layers :

- Etherned layer : Frame header, Frame size, etc.
- Data link layer : MAC address, ARP (IP and MAC address binding)
- Network layer : IP Packed (header, Configuration), ICMP (Query and Echo)
- Transport layer : TCP Ports, TCP handshake segmends, etc.

Application layer : DHCP, FTP, HTTP header formats.

Theory :

- Wireshark, a network analysis tool mainly known as etherreal capwes packets in real time and display them in the human readable formats.
- Wireshark includes filters, colours, coding and other features that let you keep network traffic and inspect individual packet.
- Capturing Packets

⇒ After downloding and installing wireshark you can launch it and double click the capture traffic on your wireless network, click your wireless interface you can configure advanced features by clicking capture option but is not necessary for now.

- As soon as you click on interface name, you will see the packet shark appear in real time.
- Wireshark capture each packet sent to or from your server.

- **Colour Coding**

=> You will probably see packet highlighted in a variety of different colours.

- Wireshark that type of a glance uses colours to help you identify that type of glance.
- By default light purple is TCP traffic light, blue is USP traffic and black identify packets with errors.
- For e.g., they could have blue delivered out of order. To view exactly what colour mean, click view colouring rules, you can also customize and modify colouring rules.

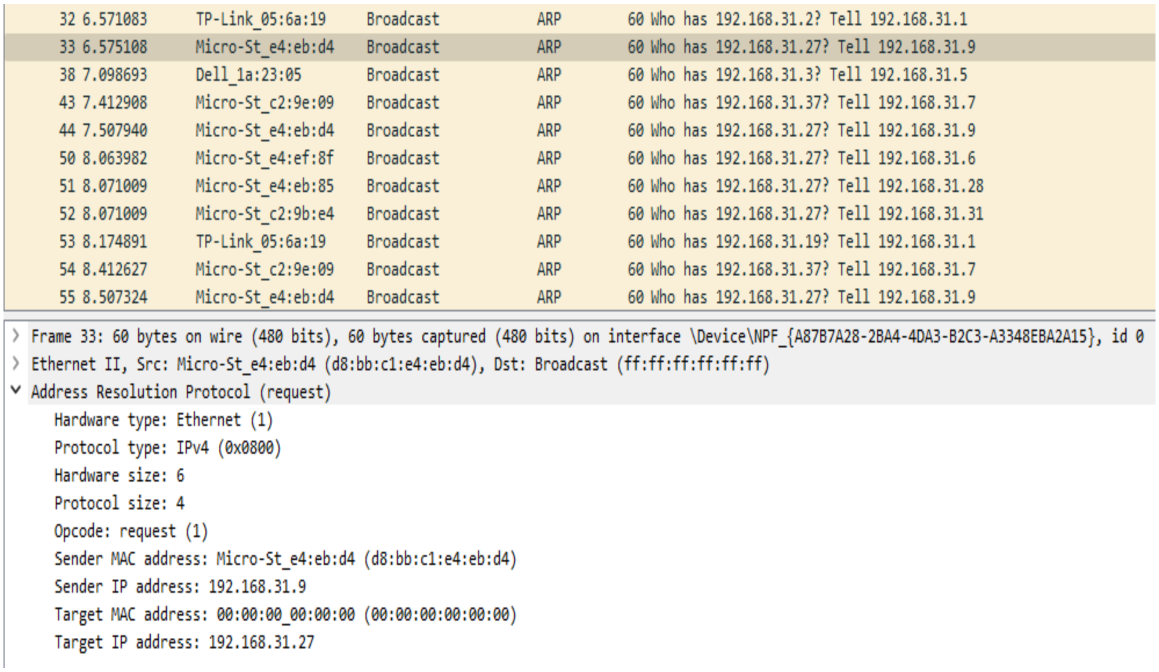
Colours in Wireshark	Packet type
1) Light purple	TCP
2) Light blue	UDP
3) Black	Packets with errors
4) light Green	HTTP traffic
5) light yellow	windows-specific traffic handling server message blocks.
6) Dark yellow	Routing
7) Dark Grey	TCP, SYN, FIN & Ack traffic

d

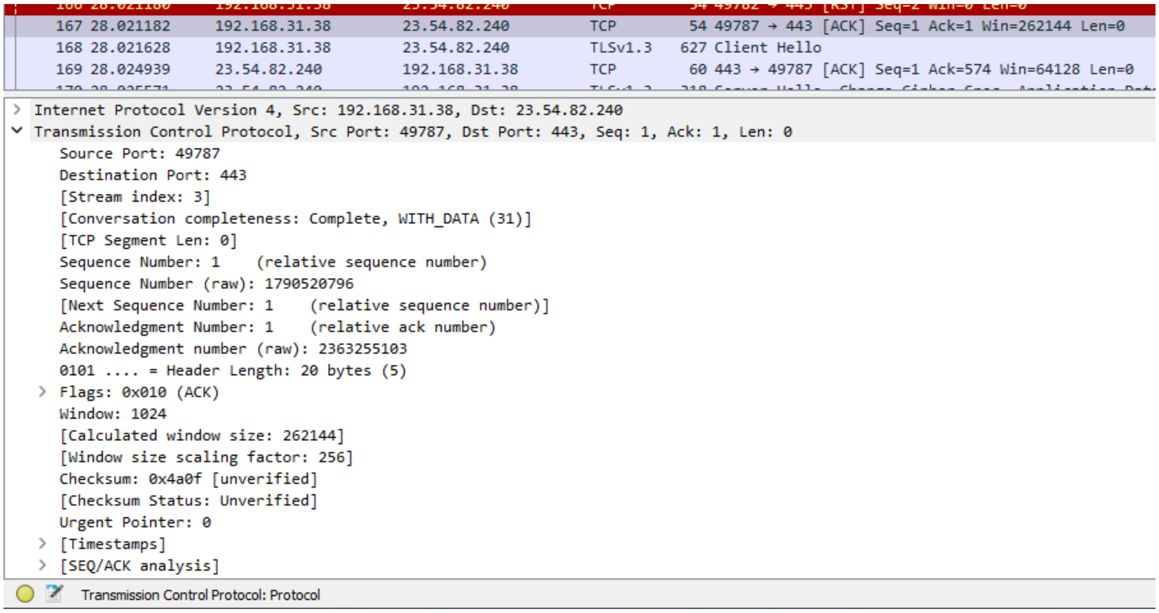
H

A

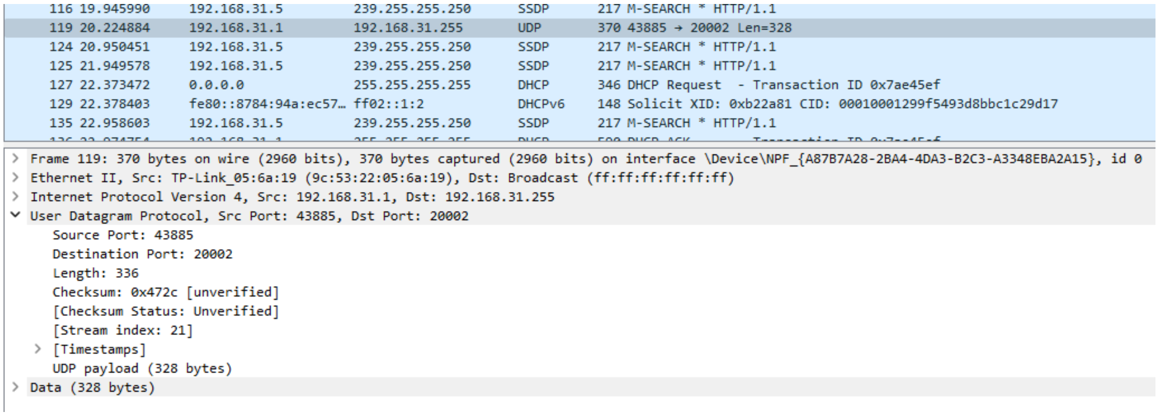
19/10/23



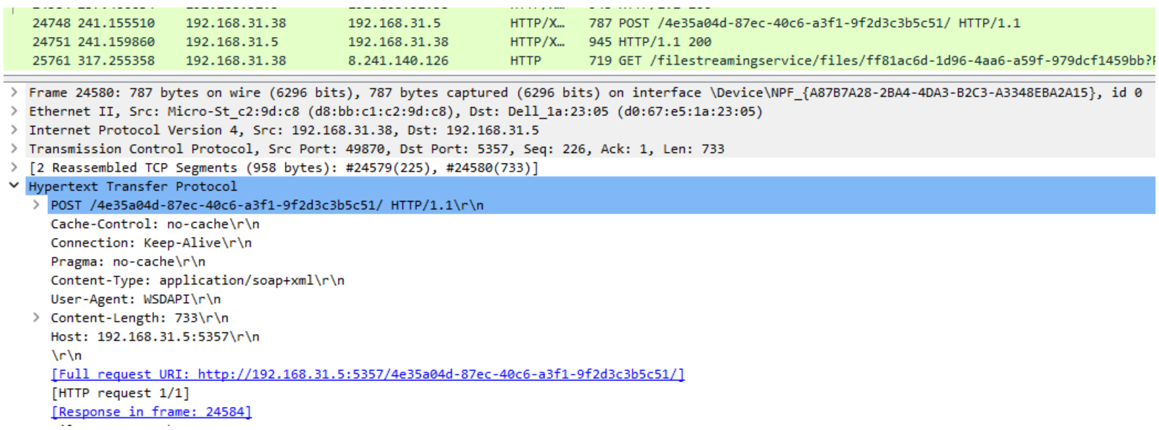
```
 32 6.571083   TP-Link_05:6a:19   Broadcast   ARP   60 Who has 192.168.31.2? Tell 192.168.31.1
 33 6.575108   Micro-St_e4:eb:d4  Broadcast   ARP   60 Who has 192.168.31.27? Tell 192.168.31.9
 38 7.098693   Dell_1a:23:05      Broadcast   ARP   60 Who has 192.168.31.3? Tell 192.168.31.5
 43 7.412908   Micro-St_c2:9e:09  Broadcast   ARP   60 Who has 192.168.31.37? Tell 192.168.31.7
 44 7.507940   Micro-St_e4:eb:d4  Broadcast   ARP   60 Who has 192.168.31.27? Tell 192.168.31.9
 50 8.063982   Micro-St_e4:ef:8f  Broadcast   ARP   60 Who has 192.168.31.27? Tell 192.168.31.6
 51 8.071009   Micro-St_e4:eb:85  Broadcast   ARP   60 Who has 192.168.31.27? Tell 192.168.31.28
 52 8.071009   Micro-St_c2:9b:e4  Broadcast   ARP   60 Who has 192.168.31.27? Tell 192.168.31.31
 53 8.174891   TP-Link_05:6a:19   Broadcast   ARP   60 Who has 192.168.31.19? Tell 192.168.31.1
 54 8.412627   Micro-St_c2:9e:09  Broadcast   ARP   60 Who has 192.168.31.37? Tell 192.168.31.7
 55 8.507324   Micro-St_e4:eb:d4  Broadcast   ARP   60 Who has 192.168.31.27? Tell 192.168.31.9

> Frame 33: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface \Device\NPF_{A87B7A28-2BA4-4DA3-B2C3-A3348EBA2A15}, id 0
> Ethernet II, Src: Micro-St_e4:eb:d4 (d8:bb:c1:e4:eb:d4), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
v Address Resolution Protocol (request)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: request (1)
    Sender MAC address: Micro-St_e4:eb:d4 (d8:bb:c1:e4:eb:d4)
    Sender IP address: 192.168.31.9
    Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
    Target IP address: 192.168.31.27
```



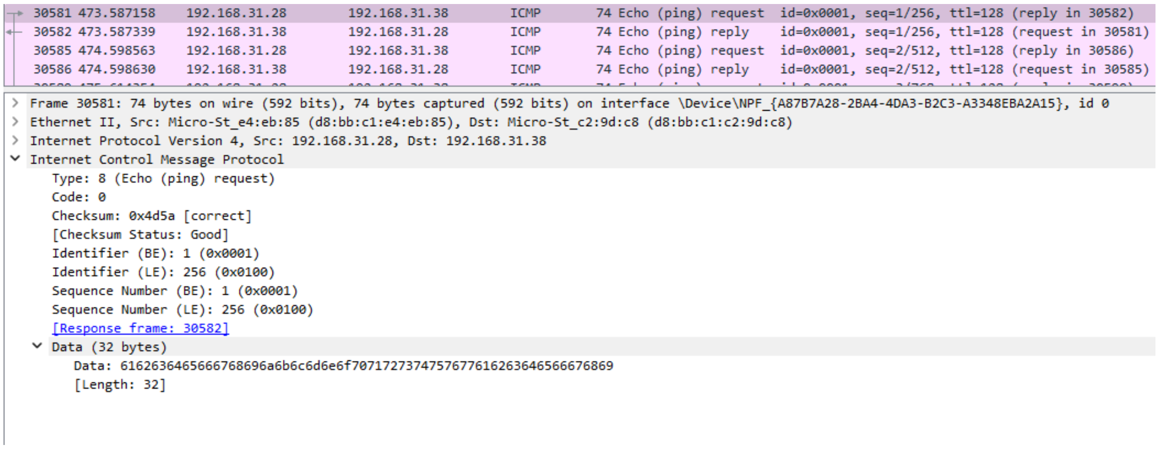
```
166 28.021180   192.168.31.38   23.54.82.240    TCP       54 49782 → 443 [RST] Seq=2 Win=0 Len=0
167 28.021182   192.168.31.38   23.54.82.240    TCP       54 49787 → 443 [ACK] Seq=1 Ack=1 Win=262144 Len=0
168 28.021628   192.168.31.38   23.54.82.240    TLSv1.3  627 Client Hello
169 28.024939   23.54.82.240    192.168.31.38   TCP       60 443 → 49787 [ACK] Seq=1 Ack=574 Win=64128 Len=0
170 28.025571   23.54.82.240    192.168.31.38   TLSv1.3  318 Server Hello, Change Cipher Spec, Application Dat

> Internet Protocol Version 4, Src: 192.168.31.38, Dst: 23.54.82.240
v Transmission Control Protocol, Src Port: 49787, Dst Port: 443, Seq: 1, Ack: 1, Len: 0
    Source Port: 49787
    Destination Port: 443
    [Stream index: 3]
    [Conversation completeness: Complete, WITH_DATA (31)]
    [TCP Segment Len: 0]
    Sequence Number: 1    (relative sequence number)
    Sequence Number (raw): 1790520796
    [Next Sequence Number: 1    (relative sequence number)]
    Acknowledgment Number: 1    (relative ack number)
    Acknowledgment number (raw): 2363255103
    0101 .... = Header Length: 20 bytes (5)
  > Flags: 0x010 (ACK)
    Window: 1024
    [Calculated window size: 262144]
    [Window size scaling factor: 256]
    Checksum: 0x4a0f [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
  > [Timestamps]
  > [SEQ/ACK analysis]

Transmission Control Protocol: Protocol
```



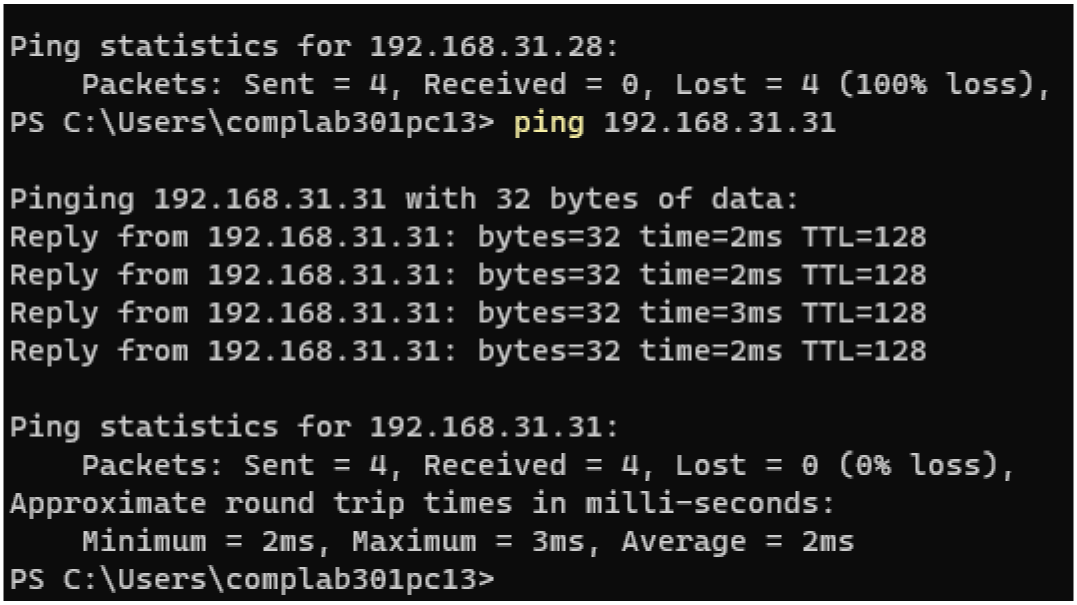
```
   116 19.945990    192.168.31.5          239.255.255.250      SSDP      217 M-SEARCH * HTTP/1.1
   119 20.224884    192.168.31.1          192.168.31.255       UDP       370 43885 → 20002 Len=328
   124 20.950451    192.168.31.5          239.255.255.250      SSDP      217 M-SEARCH * HTTP/1.1
   125 21.949578    192.168.31.5          239.255.255.250      SSDP      217 M-SEARCH * HTTP/1.1
   127 22.373472    0.0.0.0               255.255.255.255      DHCP      346 DHCP Request  - Transaction ID 0x7ae45ef
   129 22.378403    fe80::8784:94a:ec57… ff02::1:2             DHCPv6    148 Solicit XID: 0xb22a81 CID: 00010001299f5493d8bbc1c29d17
   135 22.958603    192.168.31.5          239.255.255.250      SSDP      217 M-SEARCH * HTTP/1.1

> Frame 119: 370 bytes on wire (2960 bits), 370 bytes captured (2960 bits) on interface \Device\NPF_{A87B7A28-2BA4-4DA3-B2C3-A3348EBA2A15}, id 0
> Ethernet II, Src: TP-Link_05:6a:19 (9c:53:22:05:6a:19), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
> Internet Protocol Version 4, Src: 192.168.31.1, Dst: 192.168.31.255
v User Datagram Protocol, Src Port: 43885, Dst Port: 20002
    Source Port: 43885
    Destination Port: 20002
    Length: 336
    Checksum: 0x472c [unverified]
    [Checksum Status: Unverified]
    [Stream index: 21]
  > [Timestamps]
    UDP payload (328 bytes)
> Data (328 bytes)
```



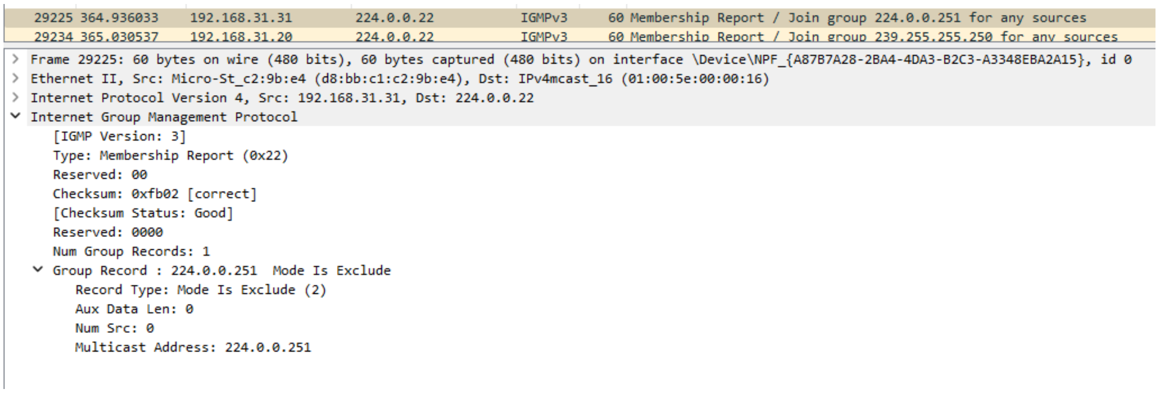
```
 24748 241.155510    192.168.31.38        192.168.31.5         HTTP/X…    787 POST /4e35a04d-87ec-40c6-a3f1-9f2d3c3b5c51/ HTTP/1.1
 24751 241.159860    192.168.31.5         192.168.31.38        HTTP/X…    945 HTTP/1.1 200
 25761 317.255358    192.168.31.38        8.241.140.126        HTTP       719 GET /filestreamingservice/files/ff81ac6d-1d96-4aa6-a59f-979dcf1459bb?

> Frame 24580: 787 bytes on wire (6296 bits), 787 bytes captured (6296 bits) on interface \Device\NPF_{A87B7A28-2BA4-4DA3-B2C3-A3348EBA2A15}, id 0
> Ethernet II, Src: Micro-St_c2:9d:c8 (d8:bb:c1:c2:9d:c8), Dst: Dell_1a:23:05 (d0:67:e5:1a:23:05)
> Internet Protocol Version 4, Src: 192.168.31.38, Dst: 192.168.31.5
> Transmission Control Protocol, Src Port: 49870, Dst Port: 5357, Seq: 226, Ack: 1, Len: 733
> [2 Reassembled TCP Segments (958 bytes): #24579(225), #24580(733)]
v Hypertext Transfer Protocol
  > POST /4e35a04d-87ec-40c6-a3f1-9f2d3c3b5c51/ HTTP/1.1\r\n
    Cache-Control: no-cache\r\n
    Connection: Keep-Alive\r\n
    Pragma: no-cache\r\n
    Content-Type: application/soap+xml\r\n
    User-Agent: WSDAPI\r\n
  > Content-Length: 733\r\n
    Host: 192.168.31.5:5357\r\n
    \r\n
    [Full request URI: http://192.168.31.5:5357/4e35a04d-87ec-40c6-a3f1-9f2d3c3b5c51/]
    [HTTP request 1/1]
    [Response in frame: 24584]
```



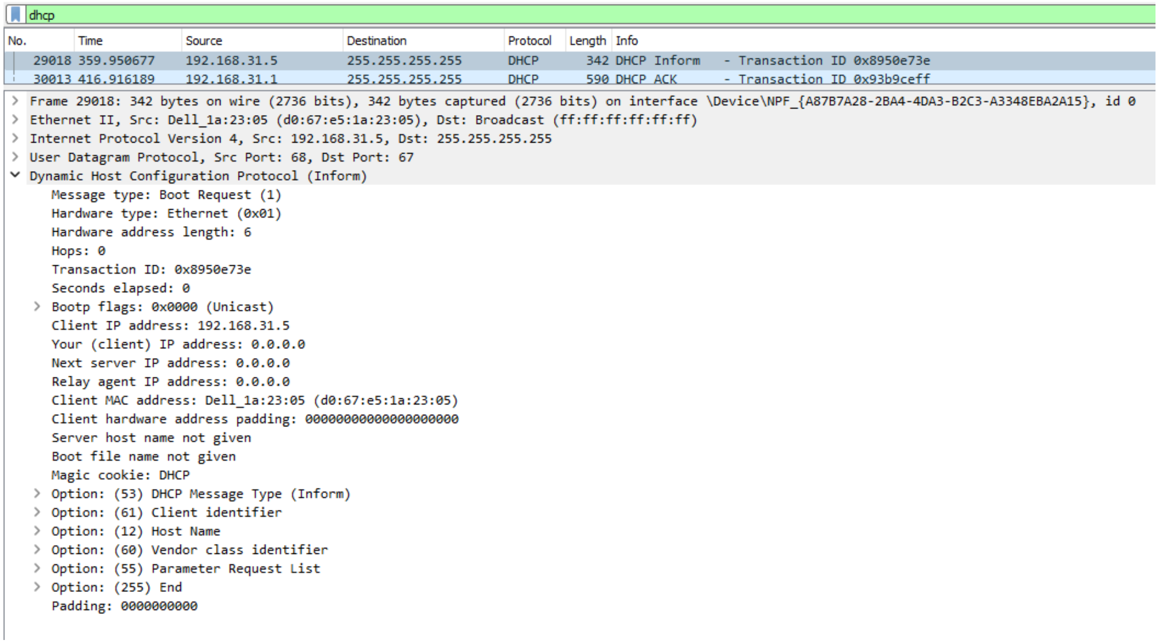
```
 30581 473.587158    192.168.31.28        192.168.31.38        ICMP       74 Echo (ping) request  id=0x0001, seq=1/256, ttl=128 (reply in 30582)
 30582 473.587339    192.168.31.38        192.168.31.28        ICMP       74 Echo (ping) reply    id=0x0001, seq=1/256, ttl=128 (request in 30581)
 30585 474.598563    192.168.31.28        192.168.31.38        ICMP       74 Echo (ping) request  id=0x0001, seq=2/512, ttl=128 (reply in 30586)
 30586 474.598630    192.168.31.38        192.168.31.28        ICMP       74 Echo (ping) reply    id=0x0001, seq=2/512, ttl=128 (request in 30585)

> Frame 30581: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{A87B7A28-2BA4-4DA3-B2C3-A3348EBA2A15}, id 0
> Ethernet II, Src: Micro-St_e4:eb:85 (d8:bb:c1:e4:eb:85), Dst: Micro-St_c2:9d:c8 (d8:bb:c1:c2:9d:c8)
> Internet Protocol Version 4, Src: 192.168.31.28, Dst: 192.168.31.38
v Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0x4d5a [correct]
    [Checksum Status: Good]
    Identifier (BE): 1 (0x0001)
    Identifier (LE): 256 (0x0100)
    Sequence Number (BE): 1 (0x0001)
    Sequence Number (LE): 256 (0x0100)
    [Response frame: 30582]
  v Data (32 bytes)
      Data: 6162636465666768696a6b6c6d6e6f7071727374757677616263646566676869
      [Length: 32]
```



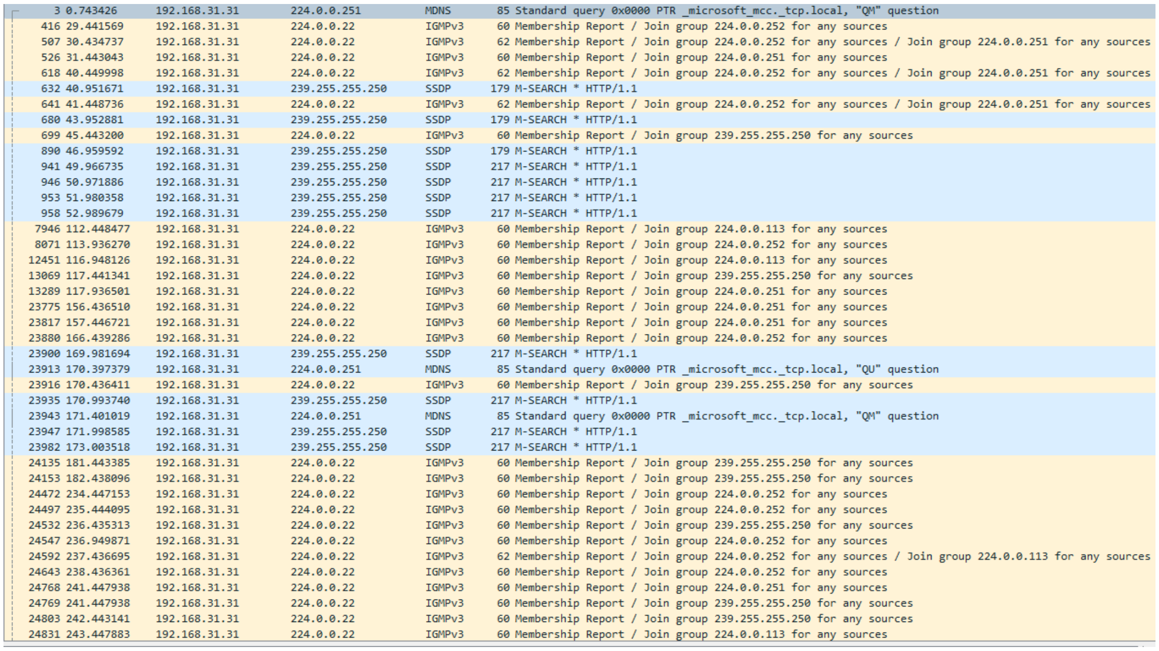
```
Ping statistics for 192.168.31.28:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
PS C:\Users\complab301pc13> ping 192.168.31.31

Pinging 192.168.31.31 with 32 bytes of data:
Reply from 192.168.31.31: bytes=32 time=2ms TTL=128
Reply from 192.168.31.31: bytes=32 time=2ms TTL=128
Reply from 192.168.31.31: bytes=32 time=3ms TTL=128
Reply from 192.168.31.31: bytes=32 time=2ms TTL=128

Ping statistics for 192.168.31.31:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 3ms, Average = 2ms
PS C:\Users\complab301pc13>
```



```
29225 364.936033    192.168.31.31     224.0.0.22        IGMPv3     60 Membership Report / Join group 224.0.0.251 for any sources
29234 365.030537    192.168.31.20     224.0.0.22        IGMPv3     60 Membership Report / Join group 239.255.255.250 for any sources

> Frame 29225: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface \Device\NPF_{A87B7A28-2BA4-4DA3-B2C3-A3348EBA2A15}, id 0
> Ethernet II, Src: Micro-St_c2:9b:e4 (d8:bb:c1:c2:9b:e4), Dst: IPv4mcast_16 (01:00:5e:00:00:16)
> Internet Protocol Version 4, Src: 192.168.31.31, Dst: 224.0.0.22
v Internet Group Management Protocol
    [IGMP Version: 3]
    Type: Membership Report (0x22)
    Reserved: 00
    Checksum: 0xfb02 [correct]
    [Checksum Status: Good]
    Reserved: 0000
    Num Group Records: 1
  v Group Record : 224.0.0.251  Mode Is Exclude
      Record Type: Mode Is Exclude (2)
      Aux Data Len: 0
      Num Src: 0
      Multicast Address: 224.0.0.251
```



```
dhcp

No.     Time          Source            Destination       Protocol  Length  Info
 29018 359.950677     192.168.31.5      255.255.255.255   DHCP       342 DHCP Inform    - Transaction ID 0x8950e73e
 30013 416.916189     192.168.31.1      255.255.255.255   DHCP       590 DHCP ACK       - Transaction ID 0x93b9ceff

> Frame 29018: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) on interface \Device\NPF_{A87B7A28-2BA4-4DA3-B2C3-A3348EBA2A15}, id 0
> Ethernet II, Src: Dell_1a:23:05 (d0:67:e5:1a:23:05), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
> Internet Protocol Version 4, Src: 192.168.31.5, Dst: 255.255.255.255
> User Datagram Protocol, Src Port: 68, Dst Port: 67
v Dynamic Host Configuration Protocol (Inform)
    Message type: Boot Request (1)
    Hardware type: Ethernet (0x01)
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0x8950e73e
    Seconds elapsed: 0
  > Bootp flags: 0x0000 (Unicast)
    Client IP address: 192.168.31.5
    Your (client) IP address: 0.0.0.0
    Next server IP address: 0.0.0.0
    Relay agent IP address: 0.0.0.0
    Client MAC address: Dell_1a:23:05 (d0:67:e5:1a:23:05)
    Client hardware address padding: 00000000000000000000
    Server host name not given
    Boot file name not given
    Magic cookie: DHCP
  > Option: (53) DHCP Message Type (Inform)
  > Option: (61) Client identifier
  > Option: (12) Host Name
  > Option: (60) Vendor class identifier
  > Option: (55) Parameter Request List
  > Option: (255) End
    Padding: 0000000000
```



```
    3 0.743426     192.168.31.31    224.0.0.251       MDNS     85 Standard query 0x0000 PTR _microsoft_mcc._tcp.local, "QM" question
  416 29.441569    192.168.31.31    224.0.0.22        IGMPv3   60 Membership Report / Join group 224.0.0.252 for any sources
  507 30.434737    192.168.31.31    224.0.0.22        IGMPv3   62 Membership Report / Join group 224.0.0.252 for any sources / Join group 224.0.0.251 for any sources
  526 31.443043    192.168.31.31    224.0.0.22        IGMPv3   60 Membership Report / Join group 224.0.0.251 for any sources
  618 40.449998    192.168.31.31    224.0.0.22        IGMPv3   62 Membership Report / Join group 224.0.0.252 for any sources / Join group 224.0.0.251 for any sources
  632 40.951671    192.168.31.31    239.255.255.250   SSDP    179 M-SEARCH * HTTP/1.1
  641 41.448736    192.168.31.31    224.0.0.22        IGMPv3   62 Membership Report / Join group 224.0.0.252 for any sources / Join group 224.0.0.251 for any sources
  680 43.952881    192.168.31.31    239.255.255.250   SSDP    179 M-SEARCH * HTTP/1.1
  699 45.443200    192.168.31.31    224.0.0.22        IGMPv3   60 Membership Report / Join group 239.255.255.250 for any sources
  890 46.959592    192.168.31.31    239.255.255.250   SSDP    179 M-SEARCH * HTTP/1.1
  941 49.966735    192.168.31.31    239.255.255.250   SSDP    217 M-SEARCH * HTTP/1.1
  946 50.971886    192.168.31.31    239.255.255.250   SSDP    217 M-SEARCH * HTTP/1.1
  953 51.980358    192.168.31.31    239.255.255.250   SSDP    217 M-SEARCH * HTTP/1.1
  958 52.989679    192.168.31.31    239.255.255.250   SSDP    217 M-SEARCH * HTTP/1.1
 7946 112.448477   192.168.31.31    224.0.0.22        IGMPv3   60 Membership Report / Join group 224.0.0.113 for any sources
 8071 113.936270   192.168.31.31    224.0.0.22        IGMPv3   60 Membership Report / Join group 224.0.0.252 for any sources
12451 116.948126   192.168.31.31    224.0.0.22        IGMPv3   60 Membership Report / Join group 224.0.0.113 for any sources
13069 117.441341   192.168.31.31    224.0.0.22        IGMPv3   60 Membership Report / Join group 239.255.255.250 for any sources
13289 117.936501   192.168.31.31    224.0.0.22        IGMPv3   60 Membership Report / Join group 224.0.0.251 for any sources
23775 156.436510   192.168.31.31    224.0.0.22        IGMPv3   60 Membership Report / Join group 224.0.0.251 for any sources
23817 157.446721   192.168.31.31    224.0.0.22        IGMPv3   60 Membership Report / Join group 224.0.0.251 for any sources
23880 166.439286   192.168.31.31    224.0.0.22        IGMPv3   60 Membership Report / Join group 224.0.0.252 for any sources
23900 169.981694   192.168.31.31    239.255.255.250   SSDP    217 M-SEARCH * HTTP/1.1
23913 170.397379   192.168.31.31    224.0.0.251       MDNS     85 Standard query 0x0000 PTR _microsoft_mcc._tcp.local, "QU" question
23916 170.436411   192.168.31.31    224.0.0.22        IGMPv3   60 Membership Report / Join group 239.255.255.250 for any sources
23935 170.993740   192.168.31.31    239.255.255.250   SSDP    217 M-SEARCH * HTTP/1.1
23943 171.401019   192.168.31.31    224.0.0.251       MDNS     85 Standard query 0x0000 PTR _microsoft_mcc._tcp.local, "QM" question
23947 171.998585   192.168.31.31    239.255.255.250   SSDP    217 M-SEARCH * HTTP/1.1
23982 173.003518   192.168.31.31    239.255.255.250   SSDP    217 M-SEARCH * HTTP/1.1
24135 181.443385   192.168.31.31    224.0.0.22        IGMPv3   60 Membership Report / Join group 239.255.255.250 for any sources
24153 182.438096   192.168.31.31    224.0.0.22        IGMPv3   60 Membership Report / Join group 239.255.255.250 for any sources
24472 234.447153   192.168.31.31    224.0.0.22        IGMPv3   60 Membership Report / Join group 224.0.0.252 for any sources
24497 235.444095   192.168.31.31    224.0.0.22        IGMPv3   60 Membership Report / Join group 224.0.0.252 for any sources
24532 236.435313   192.168.31.31    224.0.0.22        IGMPv3   60 Membership Report / Join group 239.255.255.250 for any sources
24547 236.949871   192.168.31.31    224.0.0.22        IGMPv3   60 Membership Report / Join group 224.0.0.252 for any sources
24592 237.436695   192.168.31.31    224.0.0.22        IGMPv3   62 Membership Report / Join group 224.0.0.252 for any sources / Join group 224.0.0.113 for any sources
24643 238.436361   192.168.31.31    224.0.0.22        IGMPv3   60 Membership Report / Join group 224.0.0.252 for any sources
24768 241.447938   192.168.31.31    224.0.0.22        IGMPv3   60 Membership Report / Join group 224.0.0.251 for any sources
24769 241.447938   192.168.31.31    224.0.0.22        IGMPv3   60 Membership Report / Join group 239.255.255.250 for any sources
24803 242.443141   192.168.31.31    224.0.0.22        IGMPv3   60 Membership Report / Join group 239.255.255.250 for any sources
24831 243.447883   192.168.31.31    224.0.0.22        IGMPv3   60 Membership Report / Join group 224.0.0.113 for any sources
```