LAB EXPERIMENT 10

Aim: Study of TCP and UDP packets in Wireshark.

Software Used:- WireShark

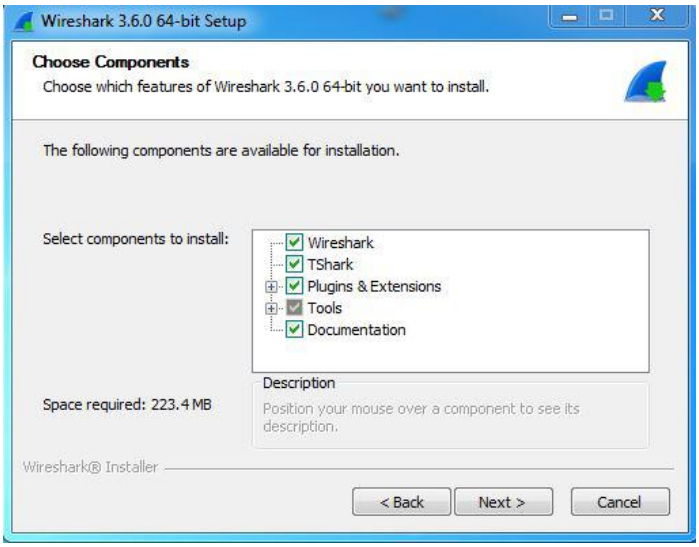
THEORY:

Wireshark is an open-source network protocol analysis software program, widely considered the industry standard. A global organization of network specialists and software developers supports Wireshark and continues to make updates for new network technologies and encryption methods.

Government agencies, corporations, non-profits, and educational institutions use Wireshark for troubleshooting and teaching purposes.

Outputs:

1. **Installation Wireshark**



2. **Pinging DGW:**

```
Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   IPv6 Address. . . . . . . . . . . : 2401:4900:1f38:4b63:9386:8cbd:3418:5562
   Temporary IPv6 Address. . . . . . : 2401:4900:1f38:4b63:ecba:3441:1073:a25f
   Link-local IPv6 Address . . . . . : fe80::b34f:1d3c:944d:b19e%18
   IPv4 Address. . . . . . . . . . . : 192.168.1.11
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : fe80::1%18
                                       192.168.1.1

Ethernet adapter Bluetooth Network Connection:

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

C:\Users\adity>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:
Reply from 192.168.1.1: bytes=32 time=41ms TTL=64
Reply from 192.168.1.1: bytes=32 time=2ms TTL=64
Reply from 192.168.1.1: bytes=32 time=3ms TTL=64
Reply from 192.168.1.1: bytes=32 time=1ms TTL=64

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 41ms, Average = 11ms
```

3. Examining ARP, ICMP packets after ping to DGW:

a. ICMP Packets Received:

icmp

No.	Time	Source	Destination	Protocol	Lengt	Info
7	1.918275	192.168.1.11	192.168.1.1	ICMP	74	Echo (ping) request id=0x0001, seq=55/14080, ttl=128 (reply in 8)
8	1.921424	192.168.1.1	192.168.1.11	ICMP	74	Echo (ping) reply id=0x0001, seq=55/14080, ttl=64 (request in 7)
15	2.924659	192.168.1.11	192.168.1.1	ICMP	74	Echo (ping) request id=0x0001, seq=56/14336, ttl=128 (reply in 16)
16	2.926542	192.168.1.1	192.168.1.11	ICMP	74	Echo (ping) reply id=0x0001, seq=56/14336, ttl=64 (request in 15)
22	3.937092	192.168.1.11	192.168.1.1	ICMP	74	Echo (ping) request id=0x0001, seq=57/14592, ttl=128 (reply in 23)
23	3.939014	192.168.1.1	192.168.1.11	ICMP	74	Echo (ping) reply id=0x0001, seq=57/14592, ttl=64 (request in 22)
24	4.950254	192.168.1.11	192.168.1.1	ICMP	74	Echo (ping) request id=0x0001, seq=58/14848, ttl=128 (reply in 25)
25	4.952379	192.168.1.1	192.168.1.11	ICMP	74	Echo (ping) reply id=0x0001, seq=58/14848, ttl=64 (request in 24)

```
  7 1.918275  192.168.1.11  192.168.1.1   ICMP     74 Echo (ping) request  id=0x0001, seq=55/14080, ttl=128 (reply
> Frame 7: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{B28D635A-0501-4672-
> Ethernet II, Src: AzureWav_e0:d1:29 (34:6f:24:e0:d1:29), Dst: TaicangT_50:d2:c0 (24:0b:88:50:d2:c0)
> Internet Protocol Version 4, Src: 192.168.1.11, Dst: 192.168.1.1
> Internet Control Message Protocol
```

```
v Frame 7: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{B28D63
    Section number: 1
  > Interface id: 0 (\Device\NPF_{B28D635A-0501-4672-81C0-1C2DBA828FCE})
    Encapsulation type: Ethernet (1)
    Arrival Time: Oct 30, 2022 21:51:20.477524000 India Standard Time
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1667146880.477524000 seconds
    [Time delta from previous captured frame: 0.335082000 seconds]
    [Time delta from previous displayed frame: 0.000000000 seconds]
    [Time since reference or first frame: 1.918275000 seconds]
    Frame Number: 7
    Frame Length: 74 bytes (592 bits)
    Capture Length: 74 bytes (592 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:icmp:data]
    [Coloring Rule Name: ICMP]
    [Coloring Rule String: icmp || icmpv6]
v Ethernet II, Src: AzureWav_e0:d1:29 (34:6f:24:e0:d1:29), Dst: TaicangT_50:d2:c0 (24:0b:88:50:d2:c0)
  > Destination: TaicangT_50:d2:c0 (24:0b:88:50:d2:c0)
  > Source: AzureWav_e0:d1:29 (34:6f:24:e0:d1:29)
    Type: IPv4 (0x0800)
v Internet Protocol Version 4, Src: 192.168.1.11, Dst: 192.168.1.1
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 60
    Identification: 0xb9f0 (47600)
  > 000. .... = Flags: 0x0
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 128
    Protocol: ICMP (1)
    Header Checksum: 0xfd73 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.1.11
    Destination Address: 192.168.1.1
```

b. Examining Address Resolution Protocol (ARP) Packet:

5	1.583170	TaicangT_50:…	AzureWav_e0:…	ARP	60	Who has 192.168.1.11? Tell 192.168.1.1
6	1.583193	AzureWav_e0:…	TaicangT_50:…	ARP	42	192.168.1.11 is at 34:6f:24:e0:d1:29
29	6.663285	TaicangT_50:…	AzureWav_e0:…	ARP	60	Who has 192.168.1.11? Tell 192.168.1.1

```
> Frame 5: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface \Device\NPF_{B28D635A-0501-4672
> Ethernet II, Src: TaicangT_50:d2:c0 (24:0b:88:50:d2:c0), Dst: AzureWav_e0:d1:29 (34:6f:24:e0:d1:29)
> Address Resolution Protocol (request)
```

```
    5 1.583170  TaicangT_50:… AzureWav_e0:… ARP      60 Who has 192.168.1.11? Tell 192.168.1.1
    6 1.583193  AzureWav_e0:… TaicangT_50:… ARP      42 192.168.1.11 is at 34:6f:24:e0:d1:29
   29 6.663285  TaicangT_50:… AzureWav_e0:… ARP      60 Who has 192.168.1.11? Tell 192.168.1.1
```

```
Frame 5: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface \Device\NPF_{B28D635A-0501-4672-
    Section number: 1
  > Interface id: 0 (\Device\NPF_{B28D635A-0501-4672-81C0-1C2DBA828FCE})
    Encapsulation type: Ethernet (1)
    Arrival Time: Oct 30, 2022 21:51:20.142419000 India Standard Time
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1667146880.142419000 seconds
    [Time delta from previous captured frame: 1.179128000 seconds]
    [Time delta from previous displayed frame: 0.000000000 seconds]
    [Time since reference or first frame: 1.583170000 seconds]
    Frame Number: 5
    Frame Length: 60 bytes (480 bits)
    Capture Length: 60 bytes (480 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:arp]
    [Coloring Rule Name: ARP]
    [Coloring Rule String: arp]
Ethernet II, Src: TaicangT_50:d2:c0 (24:0b:88:50:d2:c0), Dst: AzureWav_e0:d1:29 (34:6f:24:e0:d1:29)
  > Destination: AzureWav_e0:d1:29 (34:6f:24:e0:d1:29)
  > Source: TaicangT_50:d2:c0 (24:0b:88:50:d2:c0)
    Type: ARP (0x0806)
    Padding: 000000000000000000000000000000000000
Address Resolution Protocol (request)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: request (1)
    Sender MAC address: TaicangT_50:d2:c0 (24:0b:88:50:d2:c0)
    Sender IP address: 192.168.1.1
    Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
    Target IP address: 192.168.1.11
```

4. Examining UDP, IPv6, TCP Packets:

a. UDP:

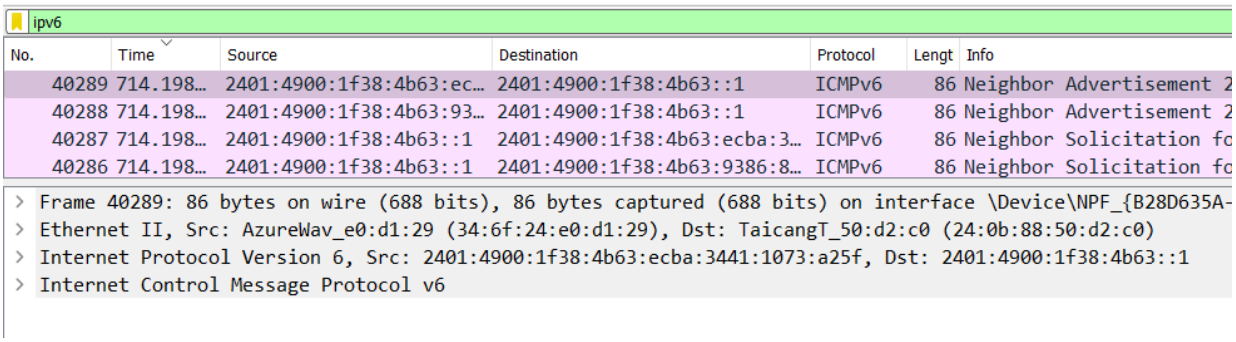
udp

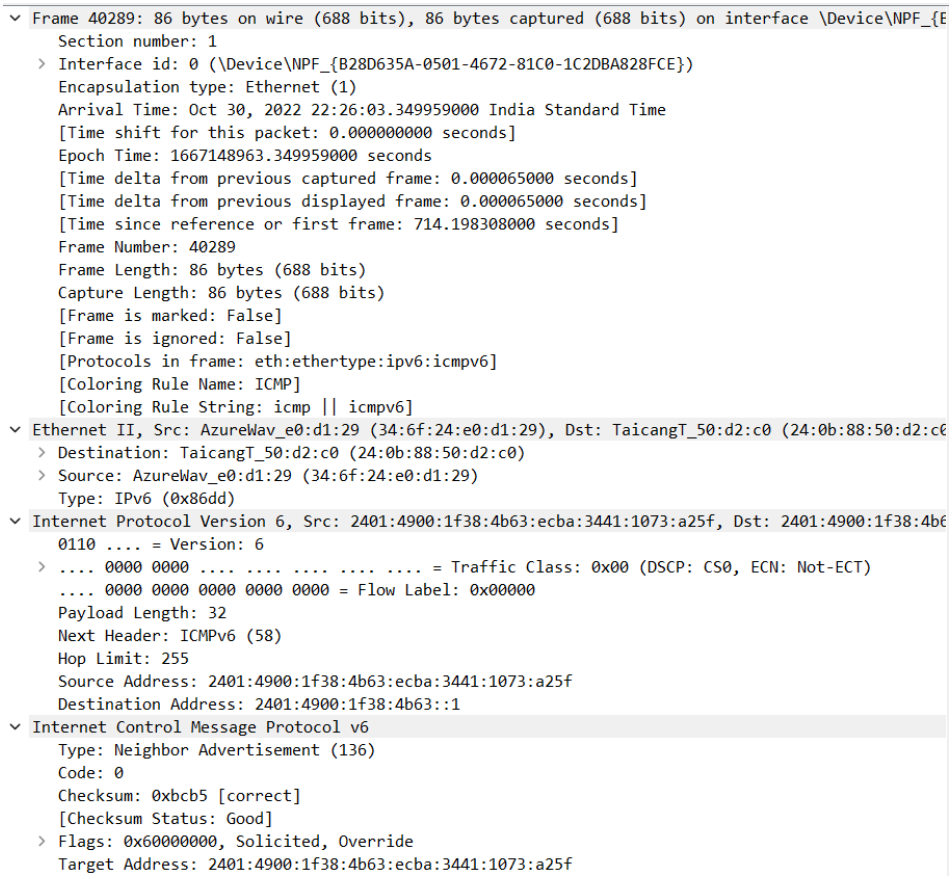
No.	Time	Source	Destination	Protocol	Lengt	Info
89	21.524898	192.168.1.13	192.168.1.11	UDP	556	58666 → 64095 Len=514

```
> Frame 89: 556 bytes on wire (4448 bits), 556 bytes captured (4448 bits) on interface \Device\NPF_{B28D635A-0501-
> Ethernet II, Src: Fn-LinkT_d1:b1:70 (ac:64:cf:d1:b1:70), Dst: AzureWav_e0:d1:29 (34:6f:24:e0:d1:29)
> Internet Protocol Version 4, Src: 192.168.1.13, Dst: 192.168.1.11
> User Datagram Protocol, Src Port: 58666, Dst Port: 64095
> Data (514 bytes)
```

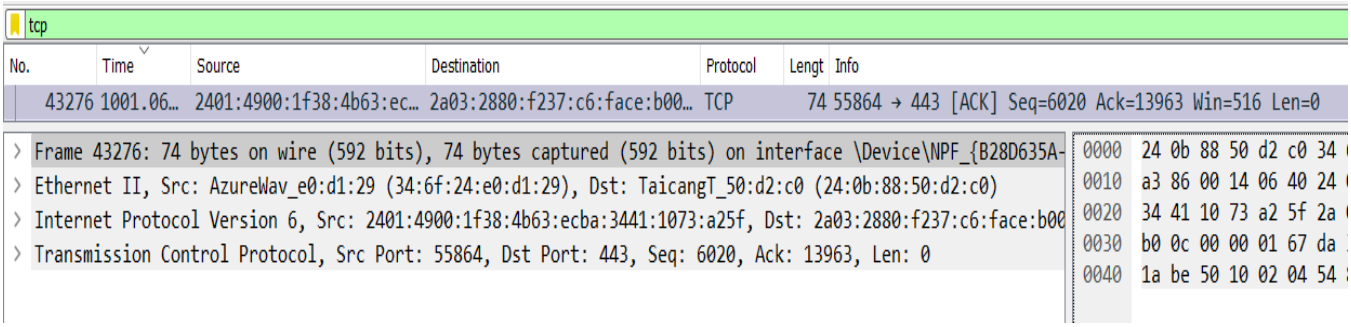
```
Frame 89: 556 bytes on wire (4448 bits), 556 bytes captured (4448 bits) on interface \Device\NPF_{B28D
    Section number: 1
  > Interface id: 0 (\Device\NPF_{B28D635A-0501-4672-81C0-1C2DBA828FCE})
    Encapsulation type: Ethernet (1)
    Arrival Time: Oct 30, 2022 22:14:30.676549000 India Standard Time
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1667148270.676549000 seconds
    [Time delta from previous captured frame: 0.026090000 seconds]
    [Time delta from previous displayed frame: 0.049952000 seconds]
    [Time since reference or first frame: 21.524898000 seconds]
    Frame Number: 89
    Frame Length: 556 bytes (4448 bits)
    Capture Length: 556 bytes (4448 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:udp:data]
    [Coloring Rule Name: UDP]
    [Coloring Rule String: udp]
Ethernet II, Src: Fn-LinkT_d1:b1:70 (ac:64:cf:d1:b1:70), Dst: AzureWav_e0:d1:29 (34:6f:24:e0:d1:29)
  > Destination: AzureWav_e0:d1:29 (34:6f:24:e0:d1:29)
  > Source: Fn-LinkT_d1:b1:70 (ac:64:cf:d1:b1:70)
    Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 192.168.1.13, Dst: 192.168.1.11
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 542
    Identification: 0x7218 (29208)
  > 010. .... = Flags: 0x2, Don't fragment
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 64
    Protocol: UDP (17)
    Header Checksum: 0x434e [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.1.13
    Destination Address: 192.168.1.11
> User Datagram Protocol, Src Port: 58666, Dst Port: 64095
Data (514 bytes)
```

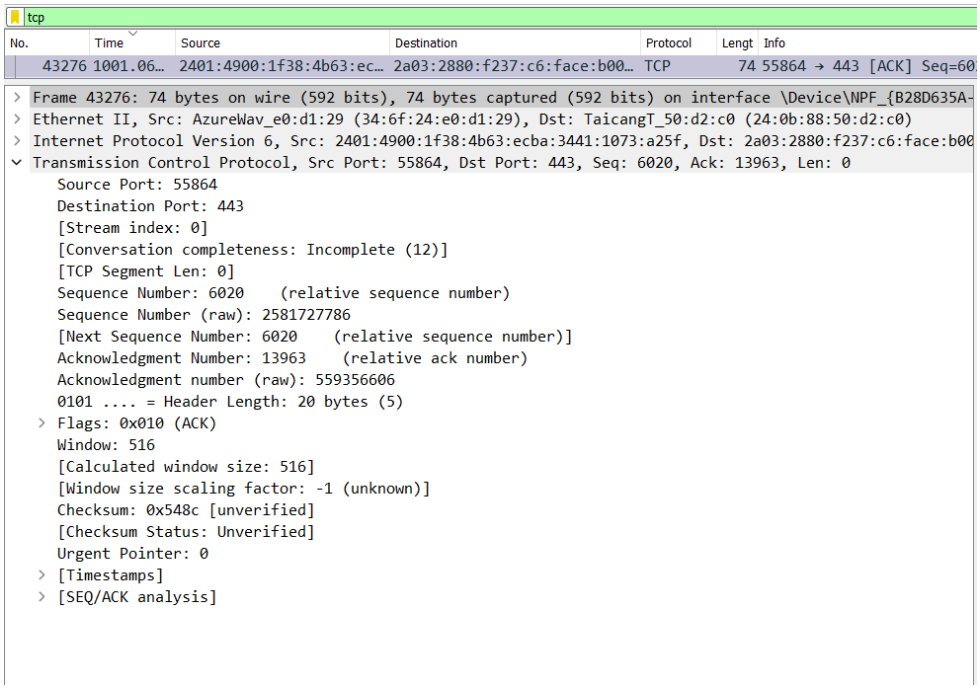
b. IPv6:


ipv6
No. Time Source Destination Protocol Lengt Info
40289 714.198… 2401:4900:1f38:4b63:ec… 2401:4900:1f38:4b63::1 ICMPv6 86 Neighbor Advertisement 2
40288 714.198… 2401:4900:1f38:4b63:93… 2401:4900:1f38:4b63::1 ICMPv6 86 Neighbor Advertisement 2
40287 714.198… 2401:4900:1f38:4b63::1 2401:4900:1f38:4b63:ecba:3… ICMPv6 86 Neighbor Solicitation fo
40286 714.198… 2401:4900:1f38:4b63::1 2401:4900:1f38:4b63:9386:8… ICMPv6 86 Neighbor Solicitation fo
Frame 40289: 86 bytes on wire (688 bits), 86 bytes captured (688 bits) on interface \Device\NPF_{B28D635A-
Ethernet II, Src: AzureWav_e0:d1:29 (34:6f:24:e0:d1:29), Dst: TaicangT_50:d2:c0 (24:0b:88:50:d2:c0)
Internet Protocol Version 6, Src: 2401:4900:1f38:4b63:ecba:3441:1073:a25f, Dst: 2401:4900:1f38:4b63::1
Internet Control Message Protocol v6


Frame 40289: 86 bytes on wire (688 bits), 86 bytes captured (688 bits) on interface \Device\NPF_{B
Section number: 1
Interface id: 0 (\Device\NPF_{B28D635A-0501-4672-81C0-1C2DBA828FCE})
Encapsulation type: Ethernet (1)
Arrival Time: Oct 30, 2022 22:26:03.349959000 India Standard Time
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1667148963.349959000 seconds
[Time delta from previous captured frame: 0.000065000 seconds]
[Time delta from previous displayed frame: 0.000065000 seconds]
[Time since reference or first frame: 714.198308000 seconds]
Frame Number: 40289
Frame Length: 86 bytes (688 bits)
Capture Length: 86 bytes (688 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:ipv6:icmpv6]
[Coloring Rule Name: ICMP]
[Coloring Rule String: icmp || icmpv6]
Ethernet II, Src: AzureWav_e0:d1:29 (34:6f:24:e0:d1:29), Dst: TaicangT_50:d2:c0 (24:0b:88:50:d2:c0
Destination: TaicangT_50:d2:c0 (24:0b:88:50:d2:c0)
Source: AzureWav_e0:d1:29 (34:6f:24:e0:d1:29)
Type: IPv6 (0x86dd)
Internet Protocol Version 6, Src: 2401:4900:1f38:4b63:ecba:3441:1073:a25f, Dst: 2401:4900:1f38:4b6
0110 .... = Version: 6
.... 0000 0000 .... = Traffic Class: 0x00 (DSCP: CS0, ECN: Not-ECT)
.... 0000 0000 0000 0000 0000 = Flow Label: 0x00000
Payload Length: 32
Next Header: ICMPv6 (58)
Hop Limit: 255
Source Address: 2401:4900:1f38:4b63:ecba:3441:1073:a25f
Destination Address: 2401:4900:1f38:4b63::1
Internet Control Message Protocol v6
Type: Neighbor Advertisement (136)
Code: 0
Checksum: 0xbcb5 [correct]
[Checksum Status: Good]
Flags: 0x60000000, Solicited, Override
Target Address: 2401:4900:1f38:4b63:ecba:3441:1073:a25f

c. TCP:


tcp
No. Time Source Destination Protocol Lengt Info
43276 1001.06… 2401:4900:1f38:4b63:ec… 2a03:2880:f237:c6:face:b00… TCP 74 55864 → 443 [ACK] Seq=6020 Ack=13963 Win=516 Len=0
Frame 43276: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{B28D635A-
Ethernet II, Src: AzureWav_e0:d1:29 (34:6f:24:e0:d1:29), Dst: TaicangT_50:d2:c0 (24:0b:88:50:d2:c0)
Internet Protocol Version 6, Src: 2401:4900:1f38:4b63:ecba:3441:1073:a25f, Dst: 2a03:2880:f237:c6:face:b00
Transmission Control Protocol, Src Port: 55864, Dst Port: 443, Seq: 6020, Ack: 13963, Len: 0
0000 24 0b 88 50 d2 c0 34
0010 a3 86 00 14 06 40 24
0020 34 41 10 73 a2 5f 2a
0030 b0 0c 00 00 01 67 da
0040 1a be 50 10 02 04 54



CONCLUSION: Study of TCP and UDP packets has been successfully done.

CRITERIA	TOTAL MARKS	MARKS OBTAINED	COMMENTS
CONCEPT	2		
IMPLEMENTATION	2		
PERFORMANCE	2		
TOTAL	6		