Wireshark Experiment

Sravani Tangeda

AP20110010174

CSE-C

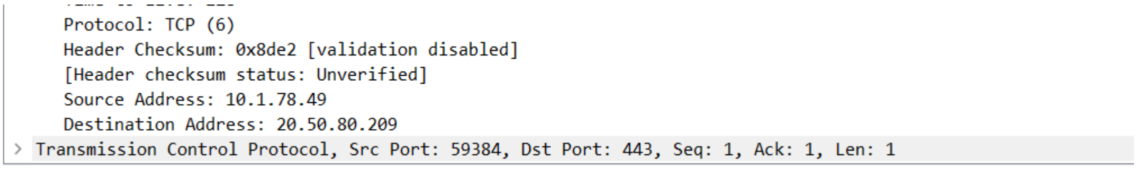
Aim:

Wireshark is open-source software designed for network traffic analysis. Wireshark is supported and updated for new network technologies and encryption techniques by a multinational organization of network specialists and software developers. When a communication problem happens, this software is used to understand how communication occurs across a network.

In this experiment, we have to find the details of the packet in the packet details pane. The details of protocols of the chosen packet are shown in the pane and these details are written in the report.

1. For which protocol (HTTP/TCP/UDP/HTTS) are you giving the answer?

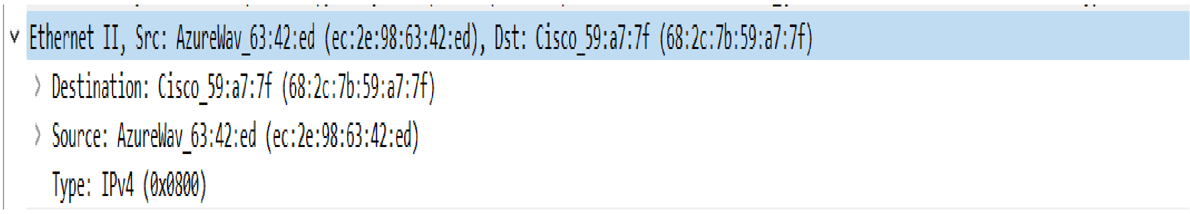
TCP (Transmission Control Protocol)



```
    Protocol: TCP (6)
    Header Checksum: 0x8de2 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 10.1.78.49
    Destination Address: 20.50.80.209
> Transmission Control Protocol, Src Port: 59384, Dst Port: 443, Seq: 1, Ack: 1, Len: 1
```

2. Is the frame an outgoing or an incoming frame?

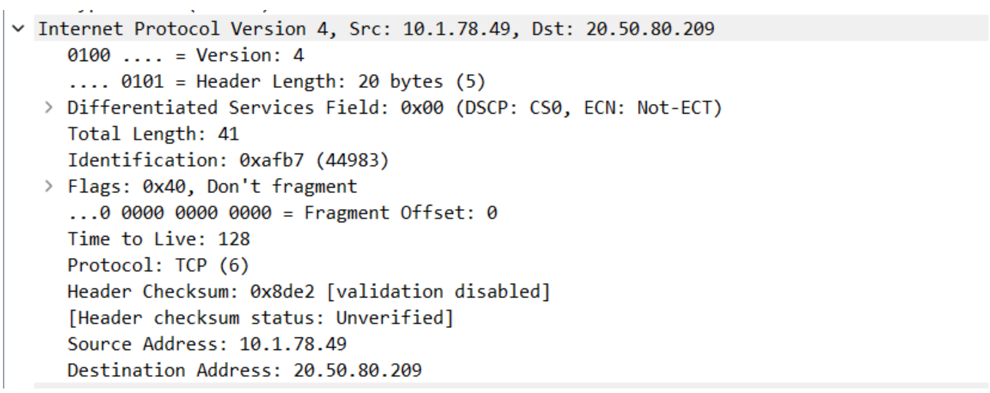
Outgoing frame



```
v Ethernet II, Src: AzureWav_63:42:ed (ec:2e:98:63:42:ed), Dst: Cisco_59:a7:7f (68:2c:7b:59:a7:7f)
  > Destination: Cisco_59:a7:7f (68:2c:7b:59:a7:7f)
  > Source: AzureWav_63:42:ed (ec:2e:98:63:42:ed)
    Type: IPv4 (0x0800)
```

3. What is the source IP address of the network-layer header in the frame?

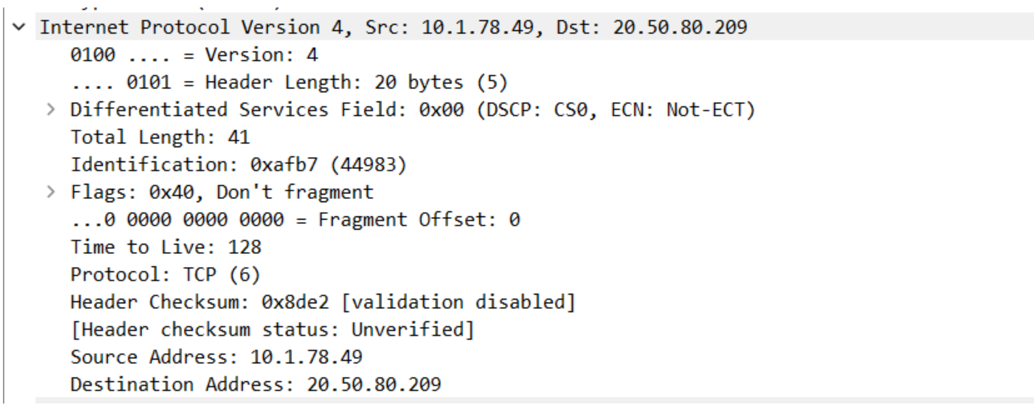
10.1.78.49



```
v Internet Protocol Version 4, Src: 10.1.78.49, Dst: 20.50.80.209
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 41
    Identification: 0xafb7 (44983)
  > Flags: 0x40, Don't fragment
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 128
    Protocol: TCP (6)
    Header Checksum: 0x8de2 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 10.1.78.49
    Destination Address: 20.50.80.209
```

4. What is the destination IP address of the network-layer header in the frame?

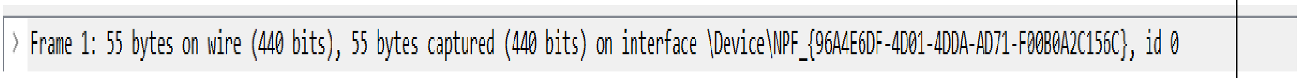
20.50.80.209



```
v Internet Protocol Version 4, Src: 10.1.78.49, Dst: 20.50.80.209
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 41
    Identification: 0xafb7 (44983)
  > Flags: 0x40, Don't fragment
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 128
    Protocol: TCP (6)
    Header Checksum: 0x8de2 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 10.1.78.49
    Destination Address: 20.50.80.209
```

5. What is the total number of bytes in the whole frame?

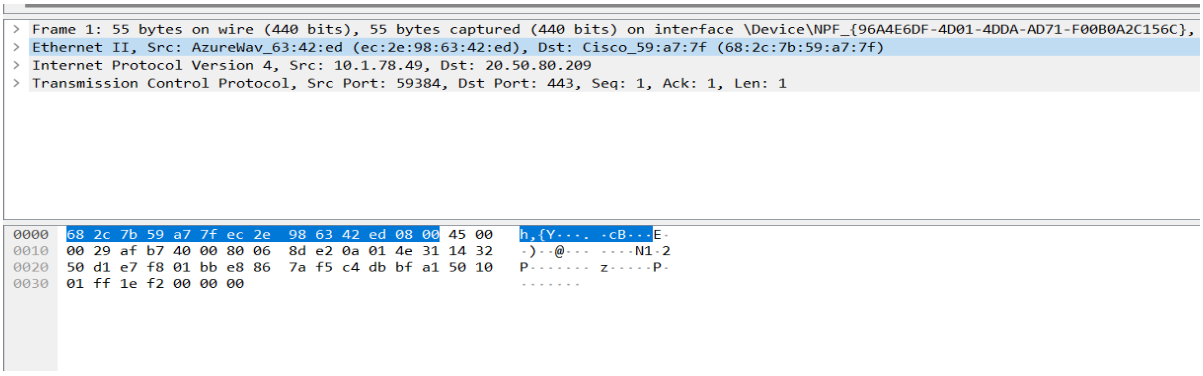
55 Bytes



```
> Frame 1: 55 bytes on wire (440 bits), 55 bytes captured (440 bits) on interface \Device\NPF_{96A4E6DF-4D01-4DDA-AD71-F00B0A2C156C}, id 0
```

6. What is the number of bytes in the Ethernet (data-link layer) header?

14 Bytes

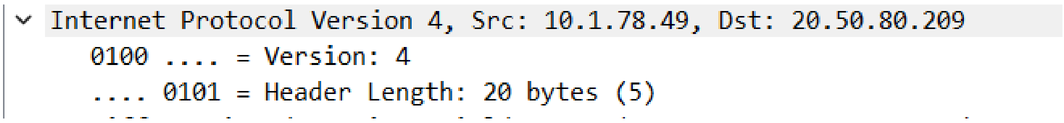


```
> Frame 1: 55 bytes on wire (440 bits), 55 bytes captured (440 bits) on interface \Device\NPF_{96A4E6DF-4D01-4DDA-AD71-F00B0A2C156C},
> Ethernet II, Src: AzureWav_63:42:ed (ec:2e:98:63:42:ed), Dst: Cisco_59:a7:7f (68:2c:7b:59:a7:7f)
> Internet Protocol Version 4, Src: 10.1.78.49, Dst: 20.50.80.209
> Transmission Control Protocol, Src Port: 59384, Dst Port: 443, Seq: 1, Ack: 1, Len: 1

0000  68 2c 7b 59 a7 7f ec 2e  98 63 42 ed 08 00 45 00   h,{Y···. ·cB···E·
0010  00 29 af b7 40 00 80 06  8d e2 0a 01 4e 31 14 32   ·)··@··· ····N1·2
0020  50 d1 e7 f8 01 bb e8 86  7a f5 c4 db bf a1 50 10   P······· z·····P·
0030  01 ff 1e f2 00 00 00                               ·······
```

7. What is the number of bytes in the IP header?

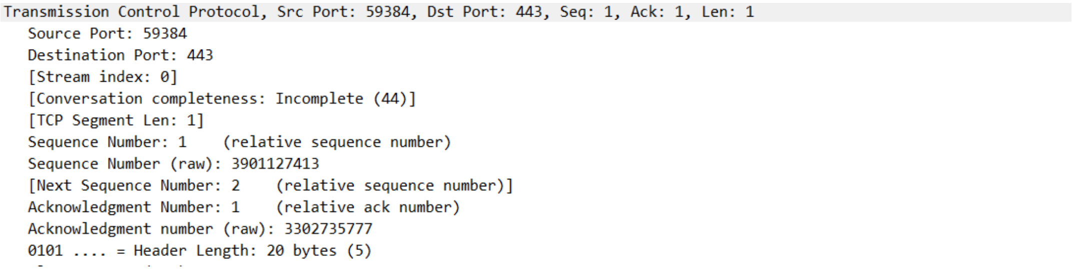
20 Bytes



```
v Internet Protocol Version 4, Src: 10.1.78.49, Dst: 20.50.80.209
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
```

8. What is the number of bytes in the TCP header?

20 Bytes

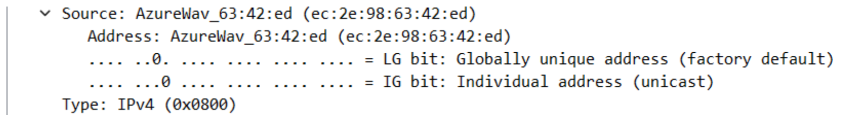


```
Transmission Control Protocol, Src Port: 59384, Dst Port: 443, Seq: 1, Ack: 1, Len: 1
   Source Port: 59384
   Destination Port: 443
   [Stream index: 0]
   [Conversation completeness: Incomplete (44)]
   [TCP Segment Len: 1]
   Sequence Number: 1    (relative sequence number)
   Sequence Number (raw): 3901127413
   [Next Sequence Number: 2    (relative sequence number)]
   Acknowledgment Number: 1    (relative ack number)
   Acknowledgment number (raw): 3302735777
   0101 .... = Header Length: 20 bytes (5)
```

9. What is the source MAC address? Is it a unicast address or broadcast or multicast address?

ec:2e:98:63:42:ed

Unicast address

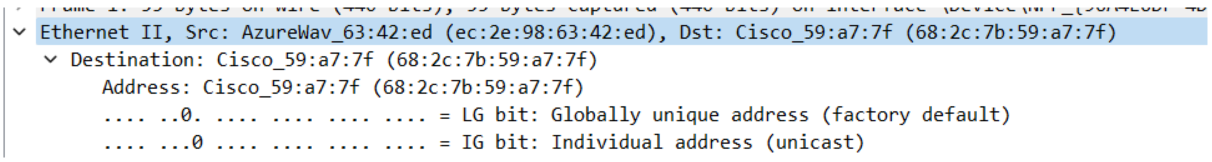


```
v Source: AzureWav_63:42:ed (ec:2e:98:63:42:ed)
    Address: AzureWav_63:42:ed (ec:2e:98:63:42:ed)
    .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
    .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  Type: IPv4 (0x0800)
```

10. What is the destination MAC address? Is it unicast address or broadcast or multicast address?

68:2c:7b:59:a7:7f

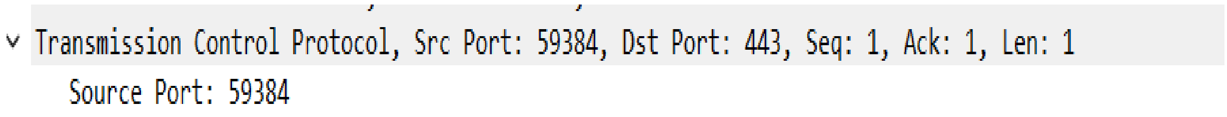
Unicast address



```
v Ethernet II, Src: AzureWav_63:42:ed (ec:2e:98:63:42:ed), Dst: Cisco_59:a7:7f (68:2c:7b:59:a7:7f)
  v Destination: Cisco_59:a7:7f (68:2c:7b:59:a7:7f)
      Address: Cisco_59:a7:7f (68:2c:7b:59:a7:7f)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
```

11. What is the source port number

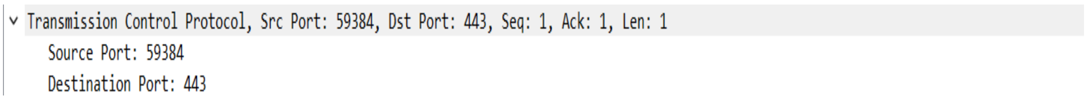
59384



```
v Transmission Control Protocol, Src Port: 59384, Dst Port: 443, Seq: 1, Ack: 1, Len: 1
    Source Port: 59384
```

12 . What is the destination port number

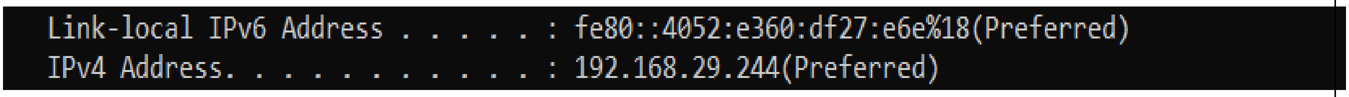
443



```
v Transmission Control Protocol, Src Port: 59384, Dst Port: 443, Seq: 1, Ack: 1, Len: 1
    Source Port: 59384
    Destination Port: 443
```

13. Write the IPv6 address

fe80::4052:e360:df27:e6e%18



```
   Link-local IPv6 Address . . . . . : fe80::4052:e360:df27:e6e%18(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.29.244(Preferred)
```

14. Write pseudocode (or a program) to decide the type of MAC address (unicast or multicast or broadcast) given the input from the keyboard.

- Consider 8-bits [a7, a6, a5, a4, a3, a2, a1, a0] of the MAC address, a7 is the MSB (Most Significant Bit), and a0 is the LSB (Least Significant Bit).
- If a0 is 0 then it is the Unicast MAC address.
- If a0 is 1, then it is the Multicast MAC address.
- If all bits are 1’s, then it is the broadcast address.

Problems Faced:

Initially, I found difficulty in understanding the working of Wireshark software and how to capture the packet details.

Conclusion:

With the help of this experiment, I learned how Wireshark software is used to know the details of a particular packet and its protocol details including source and destination mac addresses, IP addresses etc.