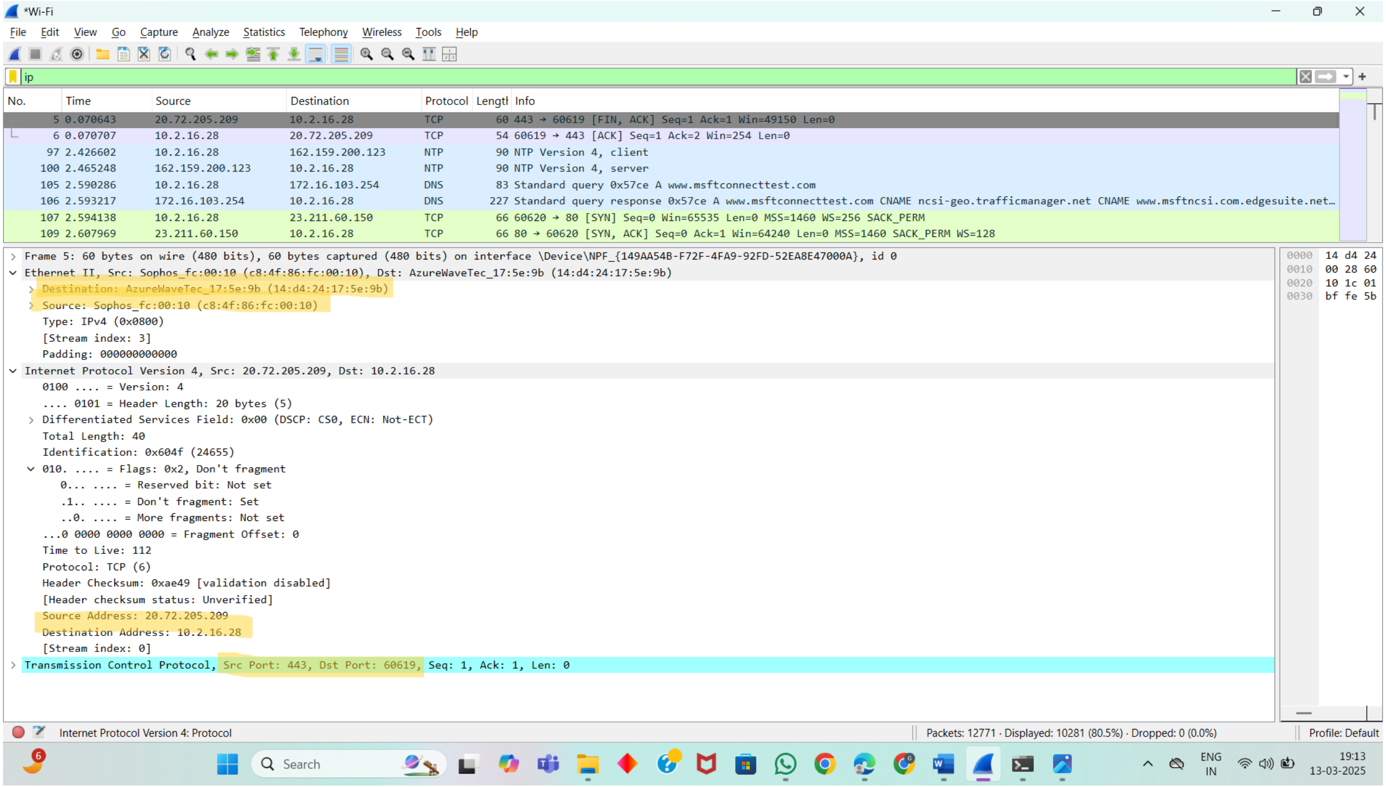
Register No:	**99220040570**
Name:	**K.Hanumaan**
Class/Section:	**8501 A/S06**
Ex.No:	**10**
Name of the Experiment	**Capture and Analyse TCP and IP packets**
Google Drive link of the packet tracer file (give view permission):	https://drive.google.com/drive/folders/1qvnsMZNaThgj8Ps7meXTnRsGRaXqe0hl?usp=drive_link

1. Visit any one website by opening a browser and fill your machine details.

Parameter	**Value**
Your Machine IP Address.	172.16.103.254
Your Machine MAC Address	14-D4-24-17-5E-9B
Default Gateway address	10.2.0.1
Website URL	https://www.slideshare.net/
Website IP Address	20.72.205.209

2. Fill the following IP packet details:

Field Name	**Field Length (no of bits)**	**Field value**
Destination MAC address	48 bits	14:d4:24:17:5e:9b
Source MAC address	48 bits	c8:4f:86:fc:00:10
Destination IP address	32 bits	10.2.16.28
Source IP Address	32 bits	20.72.205.209
Destination TCP port	16 bits	60619
Source TCP port	16 bits	443


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ip
Search
ENG
IN
19:13
13-03-2025

```
No.   Time       Source           Destination      Protocol Lengtl Info
    5 0.070643   20.72.205.209    10.2.16.28       TCP       60 443 → 60619 [FIN, ACK] Seq=1 Ack=1 Win=49150 Len=0
    6 0.070707   10.2.16.28       20.72.205.209    TCP       54 60619 → 443 [ACK] Seq=1 Ack=2 Win=254 Len=0
   97 2.426602   10.2.16.28       162.159.200.123  NTP       90 NTP Version 4, client
  100 2.465248   162.159.200.123  10.2.16.28       NTP       90 NTP Version 4, server
  105 2.590286   10.2.16.28       172.16.103.254   DNS       83 Standard query 0x57ce A www.msftconnecttest.com
  106 2.593217   172.16.103.254   10.2.16.28       DNS      227 Standard query response 0x57ce A www.msftconnecttest.com CNAME ncsi-geo.trafficmanager.net CNAME www.msftncsi.com.edgesuite.net…
  107 2.594138   10.2.16.28       23.211.60.150    TCP       66 60620 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
  109 2.607969   23.211.60.150    10.2.16.28       TCP       66 80 → 60620 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM WS=128
```

```
> Frame 5: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface \Device\NPF_{149AA54B-F72F-4FA9-92FD-52EA8E47000A}, id 0
v Ethernet II, Src: Sophos_fc:00:10 (c8:4f:86:fc:00:10), Dst: AzureWaveTec_17:5e:9b (14:d4:24:17:5e:9b)
  > Destination: AzureWaveTec_17:5e:9b (14:d4:24:17:5e:9b)
  > Source: Sophos_fc:00:10 (c8:4f:86:fc:00:10)
    Type: IPv4 (0x0800)
    [Stream index: 3]
    Padding: 000000000000
v Internet Protocol Version 4, Src: 20.72.205.209, Dst: 10.2.16.28
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 40
    Identification: 0x604f (24655)
  v 010. .... = Flags: 0x2, Don't fragment
      0... .... = Reserved bit: Not set
      .1.. .... = Don't fragment: Set
      ..0. .... = More fragments: Not set
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 112
    Protocol: TCP (6)
    Header Checksum: 0xae49 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 20.72.205.209
    Destination Address: 10.2.16.28
    [Stream index: 0]
> Transmission Control Protocol, Src Port: 443, Dst Port: 60619, Seq: 1, Ack: 1, Len: 0
```

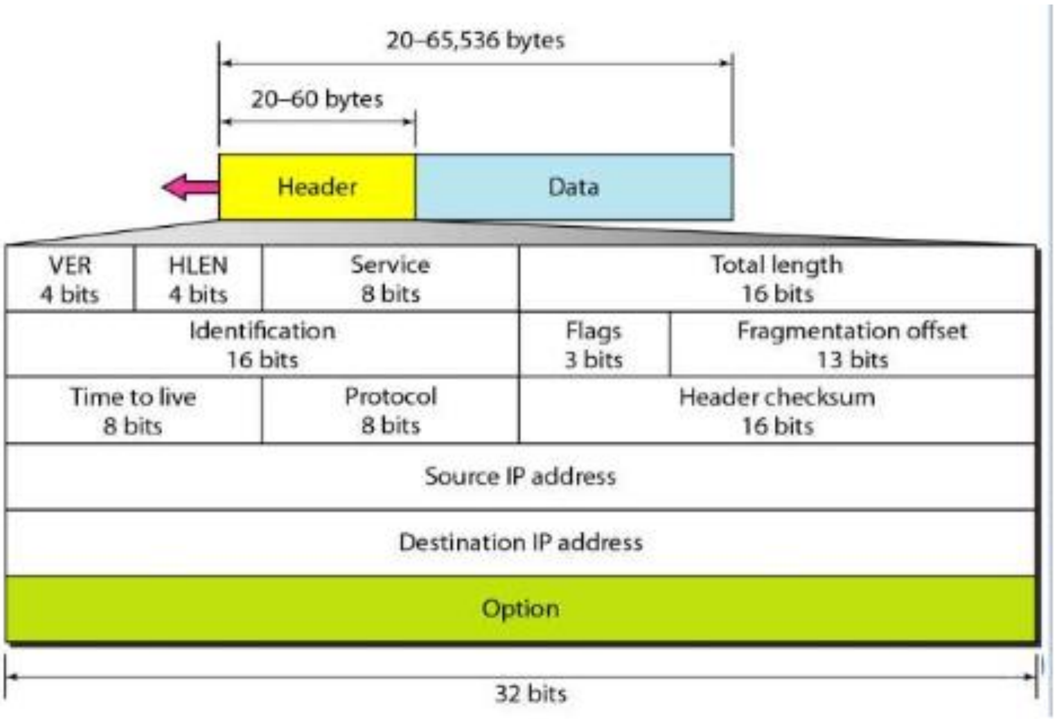
```
0000  14 d4 24
0010  00 28 60
0020  10 1c 01
0030  bf fe 5b
```

Internet Protocol Version 4: Protocol

Packets: 12771 · Displayed: 10281 (80.5%) · Dropped: 0 (0.0%)

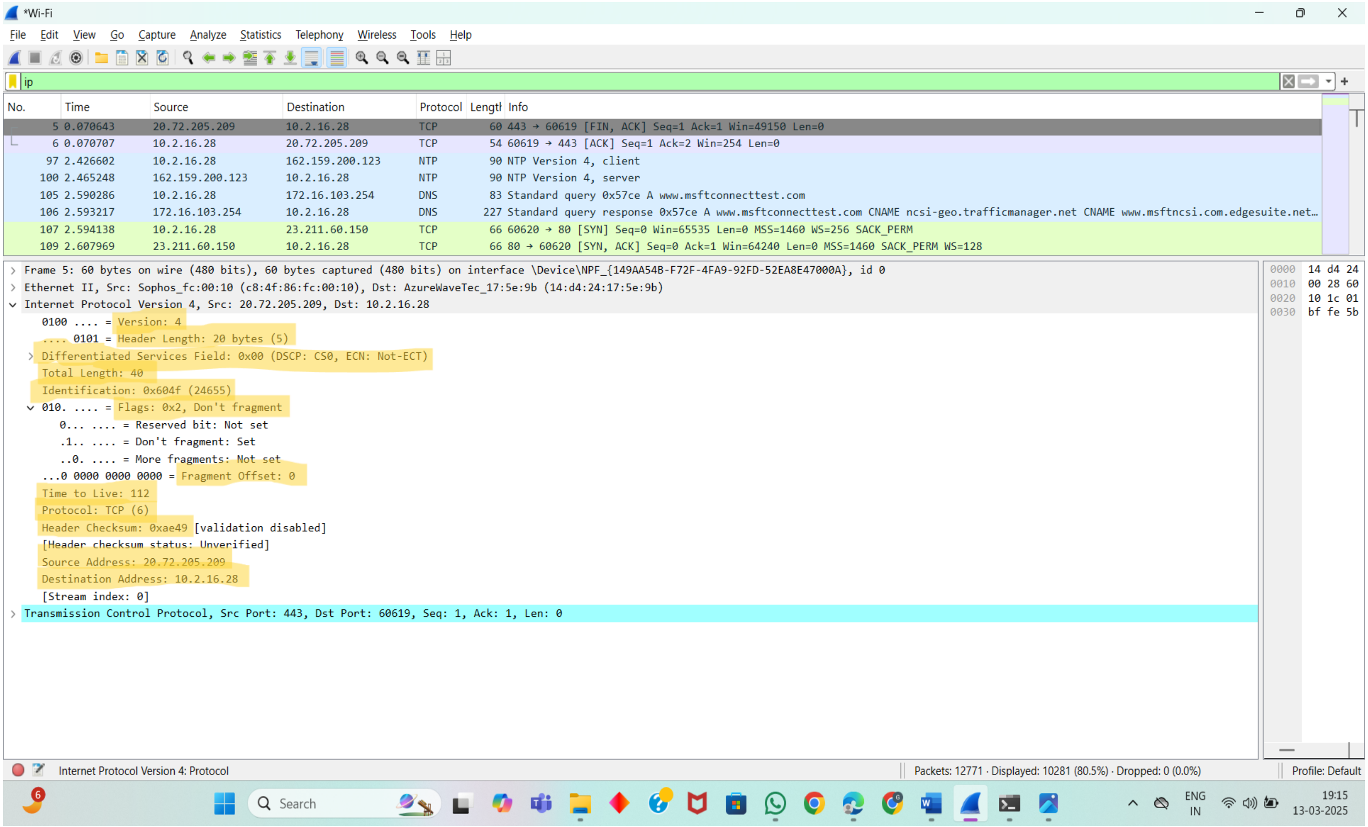
Profile: Default

3. Fill the details as per the IP frame format .(highlight the details for each of the output and paste screenshot)



Field Name	Field Value (# of bits)	Field Value (Either Binary or Hex Value)
Version	4 bits	4 (IPv4)
Header Length	4 bits	20 bytes (5 in 32 – bit words)
Type of service	8 bits	0x00
Datagram Length	16 bits	40 (0x0028 in hex)
16 bit Identifier	16 bits	0x604F (24655 in decimal)
Flags	3 bits	0x2 (Don't Fragment Set)
13-bit Fragment offset	13 bits	0 (No fragmentation)
Time-to-live	8 bits	112
Upper layer protocol	8 bits	TCP (6)
Header Checksum	16 bits	0xAE48
32 bit Source Address	32 bits	20.72.205.209
32 bit destination address	32 bits	10.2.16.28
Options (if any)	Variable	None
Date	Variable	None

Paste the screenshot and highlight the above details:



```
No.   Time      Source          Destination      Protocol Lengtl Info
    5 0.070643  20.72.205.209   10.2.16.28       TCP        60 443 → 60619 [FIN, ACK] Seq=1 Ack=1 Win=49150 Len=0
    6 0.070707  10.2.16.28      20.72.205.209    TCP        54 60619 → 443 [ACK] Seq=1 Ack=2 Win=254 Len=0
   97 2.426602  10.2.16.28      162.159.200.123  NTP        90 NTP Version 4, client
  100 2.465248  162.159.200.123 10.2.16.28       NTP        90 NTP Version 4, server
  105 2.590286  10.2.16.28      172.16.103.254   DNS        83 Standard query 0x57ce A www.msftconnecttest.com
  106 2.593217  172.16.103.254  10.2.16.28       DNS       227 Standard query response 0x57ce A www.msftconnecttest.com CNAME ncsi-geo.trafficmanager.net CNAME www.msftncsi.com.edgesuite.net…
  107 2.594138  10.2.16.28      23.211.60.150    TCP        66 60620 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
  109 2.607969  23.211.60.150   10.2.16.28       TCP        66 80 → 60620 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM WS=128
```

```
> Frame 5: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface \Device\NPF_{149AA54B-F72F-4FA9-92FD-52EA8E47000A}, id 0
> Ethernet II, Src: Sophos_fc:00:10 (c8:4f:86:fc:00:10), Dst: AzureWaveTec_17:5e:9b (14:d4:24:17:5e:9b)
v Internet Protocol Version 4, Src: 20.72.205.209, Dst: 10.2.16.28
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 40
    Identification: 0x604f (24655)
  v 010. .... = Flags: 0x2, Don't fragment
      0... .... = Reserved bit: Not set
      .1.. .... = Don't fragment: Set
      ..0. .... = More fragments: Not set
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 112
    Protocol: TCP (6)
    Header Checksum: 0xae49 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 20.72.205.209
    Destination Address: 10.2.16.28
    [Stream index: 0]
> Transmission Control Protocol, Src Port: 443, Dst Port: 60619, Seq: 1, Ack: 1, Len: 0
```

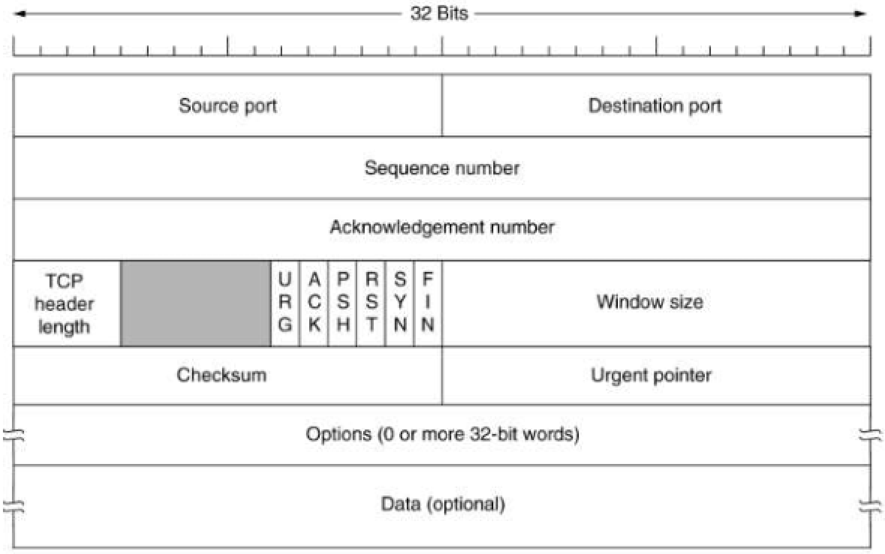
```
0000  14 d4 24
0010  00 28 60
0020  10 1c 01
0030  bf fe 5b
```

Internet Protocol Version 4: Protocol

Packets: 12771 · Displayed: 10281 (80.5%) · Dropped: 0 (0.0%)

Profile: Default

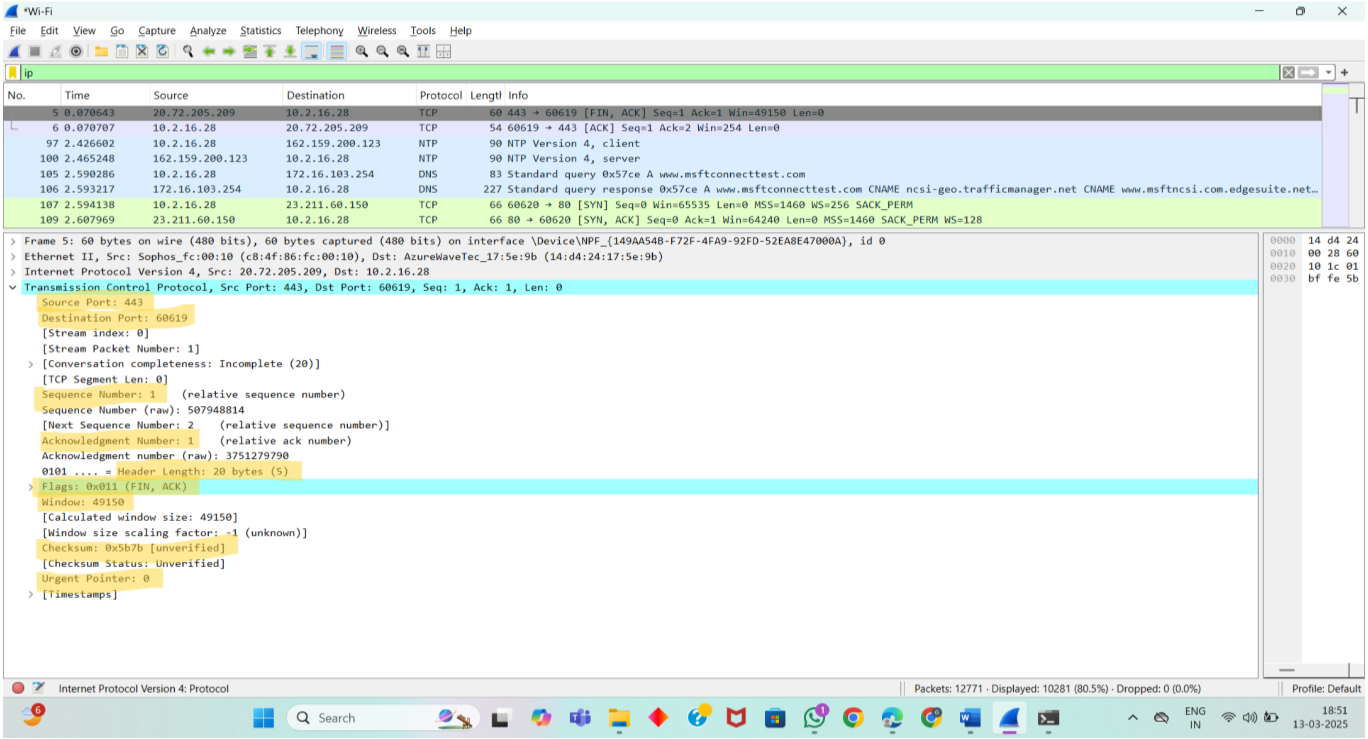
TCP Header Format:



TCP Header.

Field Name	**Field Value (# of bits)**	**Field Value (Either Binary or Hex Value)**
Source Port	16 bits	443 (0x01BB in hex)
Destination Port	16 bits	60619 (0xECDB in hex)
Sequence No.	32 bits	1 (0x00000001 in hex)
Acknowledgement No	32 bits	1 (0x00000001 in hex)
Header Length	4 bits	20 bytes (5 in 32-bit words)
FLAGS (URG,PSH,ACK,RST,SYN,FIN)	6 bits	0x011 (FIN, ACK)
Receive Window Size	16 bits	49150 (0xC01E in hex)
Checksum	16 bits	0x5B7B
Urgent Pointer	16 bits	0x0000
Options	Variable	None
Data	Variable	None

Paste the screenshot and highlight the above details:



ip

```
No.    Time      Source           Destination      Protocol Lengtl Info
     5 0.070643  20.72.205.209    10.2.16.28       TCP       60 443 → 60619 [FIN, ACK] Seq=1 Ack=1 Win=49150 Len=0
     6 0.070707  10.2.16.28       20.72.205.209    TCP       54 60619 → 443 [ACK] Seq=1 Ack=2 Win=254 Len=0
    97 2.426602  10.2.16.28       162.159.200.123  NTP       90 NTP Version 4, client
   100 2.465248  162.159.200.123  10.2.16.28       NTP       90 NTP Version 4, server
   105 2.590286  10.2.16.28       172.16.103.254   DNS       83 Standard query 0x57ce A www.msftconnecttest.com
   106 2.593217  172.16.103.254   10.2.16.28       DNS      227 Standard query response 0x57ce A www.msftconnecttest.com CNAME ncsi-geo.trafficmanager.net CNAME www.msftncsi.com.edgesuite.net…
   107 2.594138  10.2.16.28       23.211.60.150    TCP       66 60620 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
   109 2.607969  23.211.60.150    10.2.16.28       TCP       66 80 → 60620 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM WS=128
```

```
> Frame 5: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface \Device\NPF_{149AA54B-F72F-4FA9-92FD-52EA8E47000A}, id 0
> Ethernet II, Src: Sophos_fc:00:10 (c8:4f:86:fc:00:10), Dst: AzureWaveTec_17:5e:9b (14:d4:24:17:5e:9b)
> Internet Protocol Version 4, Src: 20.72.205.209, Dst: 10.2.16.28
v Transmission Control Protocol, Src Port: 443, Dst Port: 60619, Seq: 1, Ack: 1, Len: 0
    Source Port: 443
    Destination Port: 60619
    [Stream index: 0]
    [Stream Packet Number: 1]
  > [Conversation completeness: Incomplete (20)]
    [TCP Segment Len: 0]
    Sequence Number: 1    (relative sequence number)
    Sequence Number (raw): 507948814
    [Next Sequence Number: 2    (relative sequence number)]
    Acknowledgment Number: 1    (relative ack number)
    Acknowledgment number (raw): 3751279790
    0101 .... = Header Length: 20 bytes (5)
  > Flags: 0x011 (FIN, ACK)
    Window: 49150
    [Calculated window size: 49150]
    [Window size scaling factor: -1 (unknown)]
    Checksum: 0x5b7b [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
  > [Timestamps]
```

```
0000  14 d4 24
0010  00 28 60
0020  10 1c 01
0030  bf fe 5b
```

Internet Protocol Version 4: Protocol

Packets: 12771 · Displayed: 10281 (80.5%) · Dropped: 0 (0.0%)

Profile: Default

Rubrics for Wireshark labs:

Rubrics	**Excellent**	**Fair**	**Poor**	**Marks**
Understanding (2)	Understand the Concept very well. (2)	Understand the Concept (1)	Poor Understand the Concept (0)	
Usage of filters (3)	Identified and applied the filter correctly (3)	Identified the filter, but not applied correctly (2-1)	Couldn't identify and apply the filter. Just captured the packets (1)	
Attach relevant Screenshots (3)	clearly Highlighted the answers and attached the screenshots (3)	attached the screenshots, but not highlighted. (2-1)	Did not attach the screenshots (0)	
On time Submission (2)	Early or on time submission (2)	Submitted after deadline (1)	Did not Submit (0)	
			Total	

Result: Thus the Capture and analyse TCP and IP Packets has been implemented and successfully verified.