LAB 9

LAB REPORT

Draw the format of the packet you saved, including the link, IP, and TCP headers, and identify the value of each field in these headers.

Express the values in the decimal format. What is the value of the protocol field in the IP header of the packet you saved? What is the use of the protocol field?

Internet Protocol Version 4, Src: 172.16.59.46 (172.16.59.46), Dst: 31.170.160.169 (31.170.160.169)
- Version: 4
- Header length: 20 bytes
- Differentiated Services Field: 0x10 (DSCP 0x04: Unknown DSCP; ECN: 0x00: Not-ECT (Not ECN-Capable Transport))
  - 0001 00.. = Differentiated Services Codepoint: Unknown (0x04)
  - .... ..00 = Explicit Congestion Notification: Not-ECT (Not ECN-Capable Transport) (0x00)
- Total Length: 60
- Identification: 0x3290 (12944)
- Flags: 0x02 (Don't Fragment)
  - 0... .... = Reserved bit: Not set
  - .1.. .... = Don't fragment: Set
  - ..0. .... = More fragments: Not set
- Fragment offset: 0
- Time to live: 64
- Protocol: TCP (6)
- Header checksum: 0x608a [validation disabled]
  - [Good: False]
  - [Bad: False]
- Source: 172.16.59.46 (172.16.59.46)
- Destination: 31.170.160.169 (31.170.160.169)
- [Source GeoIP: Unknown]
- [Destination GeoIP: Unknown]

Version : 4 bits. The version of IP used, which is four for IPv4.
Header Length : 4 bits. The header length in 32-bit words.
Differentiated Services : 8 bits. Specifies how the upper layer protocol wants the current datagram to be handled. Six bits of this field areused as a differential service code point (DSCP) and a two-bit currently unused (CU) field is reserved.
Total Length : 16 bits. The IP datagram length in bytes, including the
IP header.
Identification : 16 bits. Contains an integer that identifies the current
datagram.
Flags : 3 bits. Consists of a 3-bit field of which the lower two bits control fragmentation. The highest order bit is not used.
Fragment Offset : 13 bits. Indicates the position of the fragment's datarelative to the beginning of the data in the original datagram. It allows the destination IP process to properly reconstruct the original datagram.Time to Live : 8 bits. A counter that is decremented by one each time the datagram is forwarded. A datagram with 0 in this field is discarded.
Protocol : 8 bits. The upper layer protocol that is the source or destination of the data. The protocol field values for several higherlayer protocols are: 1 for ICMP, 2 for IGMP, 6 for TCP, and 17 for UDP.
Header Checksum : 16 bits. Calculated over the IP header to verify itscorrectness.
Source IP Address : 32 bits. The IP address of the sending host.
Destination IP Address : 32 bits. The IP address of the receivinghost.

Transmission Control Protocol, Src Port: 45195 (45195), Dst Port: telnet (23), Seq: 0, Len: 0
- Source port: 45195 (45195)
- Destination port: telnet (23)
- [Stream index: 0]
- Sequence number: 0 (relative sequence number)
- Header length: 40 bytes
- Flags: 0x002 (SYN)
  - 000. .... = Reserved: Not set

```
        ...0 .... .... = Nonce: Not set
        .... 0... .... = Congestion Window Reduced (CWR): Not set
        .... .0.. .... = ECN-Echo: Not set
        .... ..0. .... = Urgent: Not set
        .... ...0 .... = Acknowledgment: Not set
        .... .... 0... = Push: Not set
        .... .... .0.. = Reset: Not set
        .... .... ..1. = Syn: Set
        .... .... ...0 = Fin: Not set
    Window size value: 29200
    [Calculated window size: 29200]
    Checksum: 0x103d [validation disabled]
        [Good Checksum: False]
        [Bad Checksum: False]
    Options: (20 bytes), Maximum segment size, SACK permitted, Timestamps, No-Operation (NOP), Window
scale
        Maximum segment size: 1460 bytes
            Kind: MSS size (2)
            Length: 4
            MSS Value: 1460
        TCP SACK Permitted Option: True
            Kind: SACK Permission (4)
            Length: 2
        Timestamps: TSval 346084, TSecr 0
            Kind: Timestamp (8)
            Length: 10
            Timestamp value: 346084
            Timestamp echo reply: 0
        No-Operation (NOP)
            Type: 1
        Window scale: 7 (multiply by 128)
            Kind: Window Scale (3)
            Length: 3
            Shift count: 7
            [Multiplier: 128]
```

Source Port Number : 16 bits. The port number of the source process.
Destination Port Number : 16 bits. The port number of the process running in the destination host.
Sequence Number : 32 bits. Identifies the byte in the stream of data fromthe sending TCP to the receiving TCP. It is the sequence number of thefirst byte of data in this segment represents.
Acknowledgement Number : 32 bits. Contains the next sequence numberthat the destination host wants to receive.
Header Length : 4 bits. The length of the header in 32-bit words.
Reserved : 6 bits. Reserved for future use.
Flags : There are 6 bits for flags in the TCP header, each is used asfollows.
URG : If the first bit is set, an urgent message is being carried.
ACK : If the second bit is set, the acknowledgement number is valid.
PSH : If the third bit is set, it is a notification from the sender to the receiver that the receiver should pass all the data received to the application as soon as possible.
RST : If the fourth bit is set, it signals a request to reset the TCP connection.
SYN : The fifth bit of the flag field of the packet is set when initiating a
connection.
FIN : The sixth bit is set to terminate a connection.
Window Size : 16 bits. The maximum number of bytes that a receiver
can accept.
TCP Checksum : 16 bits. Covers both the TCP header and TCP data.
Urgent Pointer : 16 bits. If the URG flag is set, the pointer points to the last byte of the urgent message in the TCP payload. More specifically, thelast byte of the urgent message is identified by adding the urgent pointer value to the sequence number in the TCP header.

No.	Time	Source	Destination	Protocol	Length	Info
23	95.060709	Giga-Byt_90:4d:fe		ARP	44	Who has 31.170.160.169? Tell 172.. .

Frame 23: 44 bytes on wire (352 bits), 44 bytes captured (352 bits)
Linux cooked capture

Address Resolution Protocol (request)

No.	Time	Source	Destination	Protocol	Length	Info
24	95.083660	Cisco_d8:42:3f		ARP	62	31.170.160.169 is at 00:00:0c:07:ac:3b

Frame 24: 62 bytes on wire (496 bits), 62 bytes captured (496 bits)
Linux cooked capture
Address Resolution Protocol (reply)
VSS-Monitoring ethernet trailer, Source Port: 0