

PLATINUM JUBLEE

Celebrating 75 years of WCE & 20 years of Department





Walchand College of Engineering, Sangli

(Government Aided Autonomous Institute)

Department of Information Technology

Computer Networks Lab

EVEN SEMESTER AY 2021-22

Submitted by

Name: Om Vivek Gharge

PRN: 2020BTEIT00041

Batch: S2

Course Code: 5IT272

Date: 14/06/2022

Contact Number: 9730369761

Department of Information Technology

2021-22

Experiment Number: 10

Experiment Name: Using wireshark capture live packets from LAN and analyze

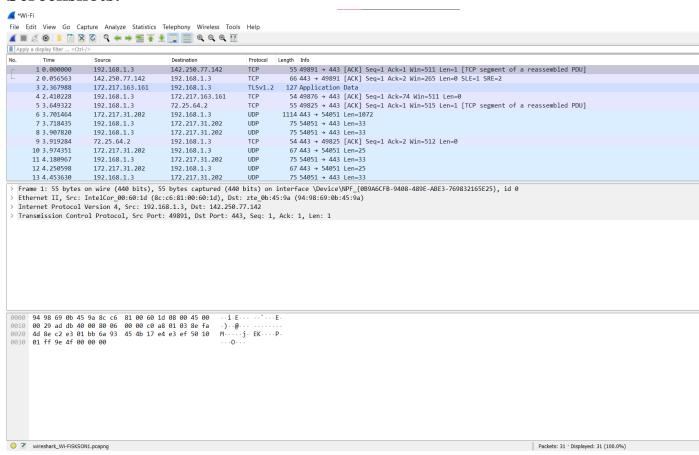
component of TCP header.

Contents:

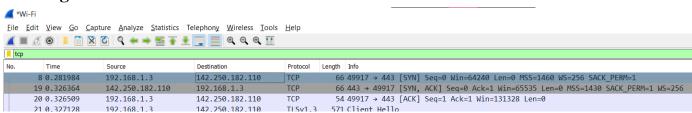
Problem Statement: Using wireshark capture live packets from LAN and analyze component of TCP header.

Platform: Wireshark

Screenshots:



Starting the connection: SYN = set



```
1000 .... = Header Length: 32 bytes (8)

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
...0 ... = Reset: Not set
...0 ... = Reset: Not set
...0 ... = Fin: Not set
...0 = Fin: Not set
...0 = Fin: Not set
...0 = Fin: Not set
```

TCP header components:

Termination: FIN = set

```
Flags: 0x011 (FIN, ACK)
       000. .... = Reserved: Not set
       ...0 .... = Nonce: Not set
       .... 0... = Congestion Window Reduced (CWR): Not set
       .... .0.. .... = ECN-Echo: Not set
       .... ..0. .... = Urgent: Not set
       .... = Acknowledgment: Set
       .... 0... = Push: Not set
       .... .... .0.. = Reset: Not set
       .... .... ..0. = Syn: Not set
      .... .... 1 = Fin: Set
  > [TCP Flags: .....A...F]

✓ *Wi-Fi

<u>F</u>ile <u>E</u>dit <u>V</u>iew <u>G</u>o <u>C</u>apture <u>A</u>nalyze <u>S</u>tatistics Telephon<u>y</u> <u>W</u>ireless <u>T</u>ools <u>H</u>elp
tcp
                                       Destination
                                                         Protocol
                                                                Length Info
                    Source
     106 6.844034
                    192.168.1.3
                                       34.102.232.42
                                                         TCP
                                                                   54 49944 → 443 [FIN, ACK] Seq=1 Ack=74 Win=509 Len=0
                    34.102.232.42
192.168.1.3
    107 6.860258
                                      192.168.1.3
34.102.232.42
                                                         TCP
                                                                  54 443 → 49944 [FIN, ACK] Seq=74 Ack=2 Win=272 Len=0
54 49944 → 443 [ACK] Seq=2 Ack=75 Win=509 Len=0
     108 6.860345
     109 6.863367
                    34.117.39.58
                                       192.168.1.3
                                                         TLSv1.2
                                                                  127 Application Data
                                                                  54 49955 → 443 [FIN, ACK] Seq=1 Ack=74 Win=509 Len=0
54 443 + 49955 [FIN, ACK] Seq=74 Ack=2 Win=265 Len=0
54 49955 → 443 [ACK] Seq=2 Ack=75 Win=509 Len=0
     110 6.863795
                                       34.117.39.58
                    192.168.1.3
     111 6.890055
                    34.117.39.58
                                      192.168.1.3
                                                         TCP
                                       34.117.39.58
     112 6.890137
                    192.168.1.3
                                                         TCP 54 49953 → 4443 [FIN, ACK] Seq=1 Ack=74 Win=513 Len=0

TCP 54 49954 → 443 [FIN, ACK] Seq=1 Ack=74 Win=565 Len=0
                                                         TCP
     113 6.914662
                    34.98.67.3
                                       192.168.1.3
     114 6.915075
                    192.168.1.3
                                       34.98.67.3
                                       192.168.1.3
                                                                  54 443 → 49954 [FIN, ACK] Seq=74 Ack=2 Win=265 Len=0
    116 6.930890
                    192.168.1.3
                                      34.98.67.3
                                                         TCP
                                                                  54 49954 → 443 [ACK] Seg=2 Ack=75 Win=513 Len=0
                                                         TLSv1.2 127 Application Data
                                                                 54 49953 → 443 [FIN, ACK] Seq=1 Ack=74 Win=508 Len=0
    118 6.959382 192.168.1.3
                                      34.98.67.3
                                                        TCP
  Frame 1: 55 bytes on wire (440 bits), 55 bytes captured (440 bits) on interface \Device\NPF_{0B9A6CFB-9408-489E-ABE3-769832165E25}, id 0
  Ethernet II. Src: IntelCor 00:60:1d (8c:c6:81:00:60:1d). Dst: zte 0b:45:9a (94:98:69:0b:45:9a)
  Internet Protocol Version 4, Src: 192.168.1.3, Dst: 142.250.182.110
Transmission Control Protocol, Src Port: 49980, Dst Port: 80, Seq: 1, Ack: 1, Len: 1
     Source Port: 49980
    Destination Port: 80
     [Stream index: 0]
     [Conversation compacting [TCP Segment Len: 1] [TCP Segment Len: 1] (relative sequence number)
     [Conversation completeness: Incomplete (40)]
     [Next Sequence Number: 2 (relative sequence number)]
Acknowledgment Number: 1 (relative ack number)
     Acknowledgment number (raw): 1550572823
O Z Transmission Control Protocol: Protocol
                                                                                                                          Packets: 146 · Displayed: 119 (81.5%)
```

Conclusion: As seen in the above images, Live packets from LAN are captured using Wireshark and various components of TCP header are analyzed.