PLATINUM JUBLEE

Celebrating 75 years of WCE & 20 years of Department

20 YEARS OF EXELLENCE

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

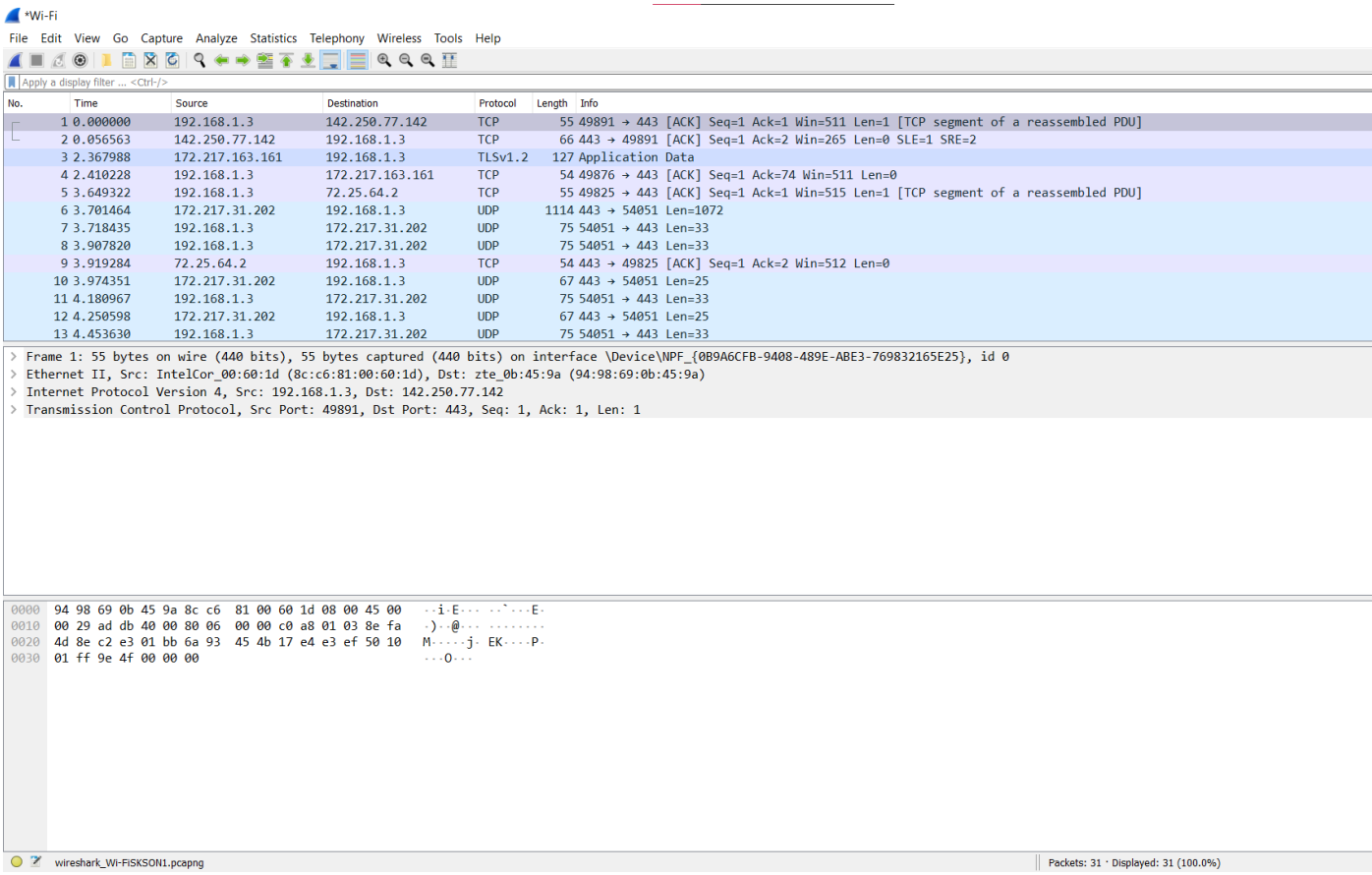
Experiment Name: Using wireshark capture live packets from LAN and analyze component of TCP header.

Contents:

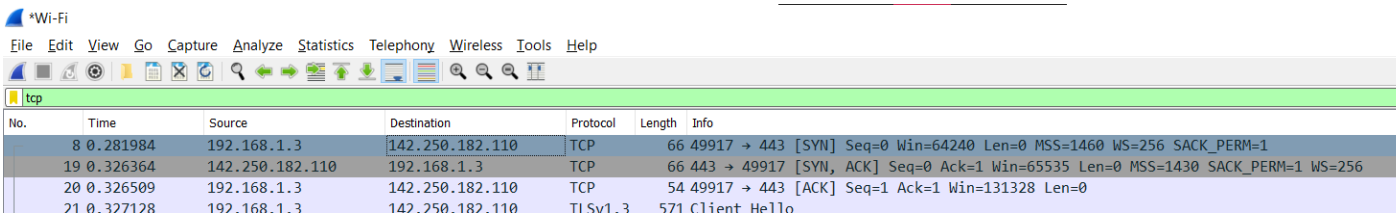
Problem Statement : Using wireshark capture live packets from LAN and analyze component of TCP header.

Platform : Wireshark

Screenshots:



Starting the connection: SYN = set



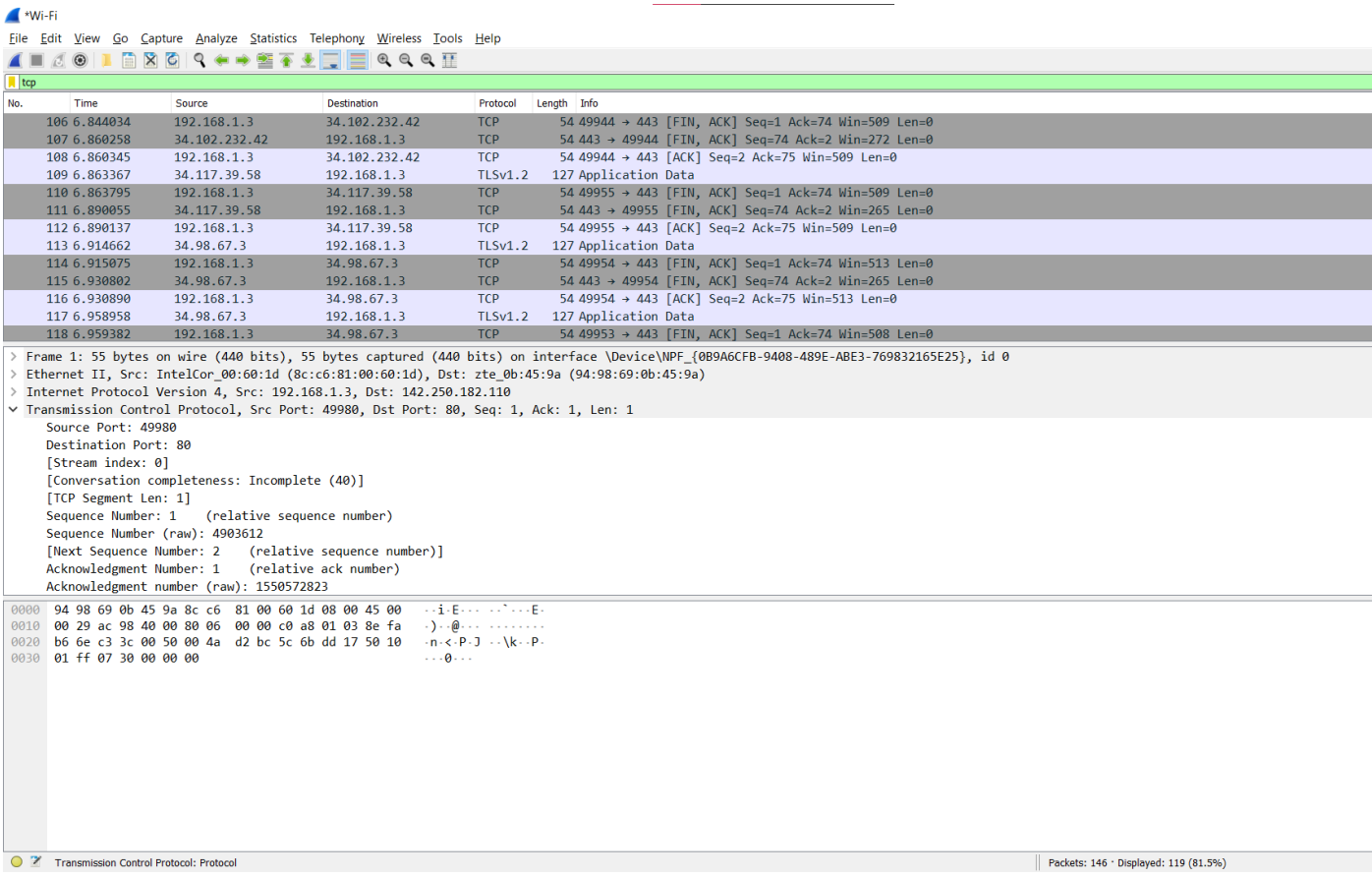
```
1000 .... = Header Length: 32 bytes (8)
Flags: 0x002 (SYN)
   000. .... .... = Reserved: Not set
   ...0 .... .... = Nonce: Not set
   .... 0... .... = Congestion Window Reduced (CWR): Not set
   .... .0.. .... = ECN-Echo: Not set
   .... ..0. .... = Urgent: Not set
   .... ...0 .... = Acknowledgment: Not set
   .... .... 0... = Push: Not set
   .... .... .0.. = Reset: Not set
   .... .... ..1. = Syn: Set
   .... .... ...0 = Fin: Not set
   [TCP Flags: ··········S·]
Window: 64240
```

TCP header components:

```
Transmission Control Protocol, Src Port: 49917, Dst Port: 443, Seq: 0, Len: 0
   Source Port: 49917
   Destination Port: 443
   [Stream index: 0]
   [Conversation completeness: Incomplete, DATA (15)]
   [TCP Segment Len: 0]
   Sequence Number: 0    (relative sequence number)
   Sequence Number (raw): 2423429267
   [Next Sequence Number: 1    (relative sequence number)]
   Acknowledgment Number: 0
   Acknowledgment number (raw): 0
   1000 .... = Header Length: 32 bytes (8)
```

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
    .... ...1 .... = Acknowledgment: Set
    .... .... 0... = Push: Not set
    .... .... .0.. = Reset: Not set
    .... .... ..0. = Syn: Not set
  > .... .... ...1 = Fin: Set
  > [TCP Flags: .......A...F]
```



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

Dr. P. K. Kharat

(Course Teacher)