



PLATINUM JUBILEE
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 Gcharge

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.

Screenshots:

Starting the connection: SYN = set

```

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

```

  v 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]

Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp

No.	Time	Source	Destination	Protocol	Length	Info
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
107	6.860258	34.102.232.42	192.168.1.3	TCP	54	443 → 49944 [FIN, ACK] Seq=74 Ack=2 Win=272 Len=0
108	6.860345	192.168.1.3	34.102.232.42	TCP	54	49944 → 443 [ACK] Seq=2 Ack=75 Win=509 Len=0
109	6.863367	34.117.39.58	192.168.1.3	TLSv1.2	127	Application Data
110	6.863795	192.168.1.3	34.117.39.58	TCP	54	49955 → 443 [FIN, ACK] Seq=1 Ack=74 Win=509 Len=0
111	6.890055	34.117.39.58	192.168.1.3	TCP	54	443 → 49955 [FIN, ACK] Seq=74 Ack=2 Win=265 Len=0
112	6.890137	192.168.1.3	34.117.39.58	TCP	54	49955 → 443 [ACK] Seq=2 Ack=75 Win=509 Len=0
113	6.914662	34.98.67.3	192.168.1.3	TLSv1.2	127	Application Data
114	6.915075	192.168.1.3	34.98.67.3	TCP	54	49954 → 443 [FIN, ACK] Seq=1 Ack=74 Win=513 Len=0
115	6.930802	34.98.67.3	192.168.1.3	TCP	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] Seq=2 Ack=75 Win=513 Len=0
117	6.958958	34.98.67.3	192.168.1.3	TLSv1.2	127	Application Data
118	6.959382	192.168.1.3	34.98.67.3	TCP	54	49953 → 443 [FIN, ACK] Seq=1 Ack=74 Win=508 Len=0

> 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 completeness: Incomplete (40)]

[TCP Segment Len: 1]

Sequence Number: 1 (relative sequence number)

Sequence Number (raw): 4903612

[Next Sequence Number: 2 (relative sequence number)]

Acknowledgment Number: 1 (relative ack number)

Acknowledgment number (raw): 1550572823

0000 94 98 69 0b 45 9a 8c c6 81 00 60 1d 08 00 45 00 ..i.E...^...E-

0010 00 29 ac 98 40 00 80 06 00 00 c0 a8 01 03 8e fa ..):@.....

0020 b6 6e c3 3c 00 50 00 4a d2 bc 5c 6b dd 17 50 10 ..n.<.P.J...k..P-

0030 01 ff 07 30 00 00 00 ..0...

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.