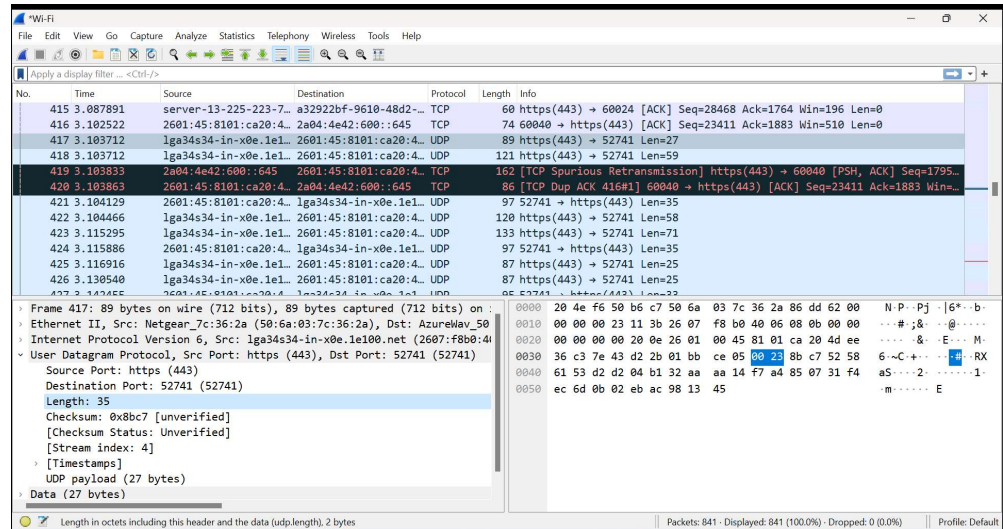


CSC535 Homework#1

1. Wireshark:

a. UDP:

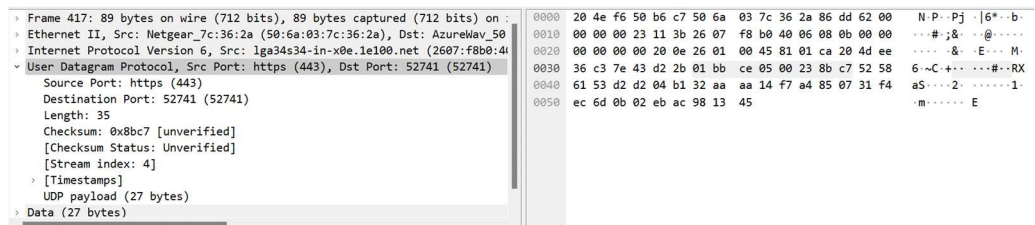
i. Length = 89



ii.

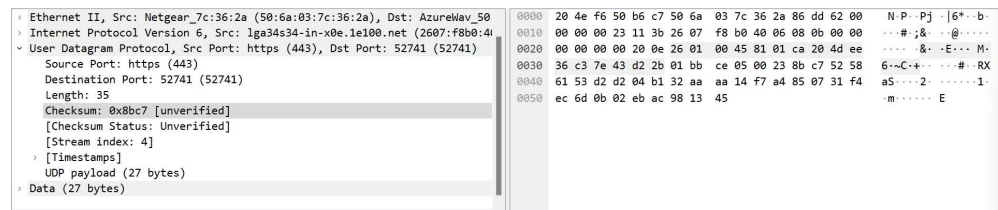
iii. Hexadecimal value:

1. 01 bb ce 05 00 23 8b c7



2.

b. CheckSum : 0x8bc7 =



i.

c. bb ce 05 00 23 8b c7 = 303

i. 303 = 0000 0011

ii. FF = 1111 1111

iii. = 1111 1100 = FC

iv. FC != 8BC7

d. This is because the pseudo-header is created to calculate the checksum and then not use it, so the client/user will create a pseudo header again and then creates another checksum at the destination.

```

Wireshark - Packet 142 - popeys.pcapng
> Frame 142: 72 bytes on wire (576 bits), 72 bytes captured (576 bits) on interface \Device\NPF_{D389F893-8539-4C93-BB04-A2E8E6D3D2CD}, id 0
> Ethernet II, Src: Netgear_7c:36:2a (50:6a:03:7c:36:2a), Dst: AzureWav_50:b6:c7 (20:4e:f6:50:b6:c7)
> Internet Protocol Version 4, Src: 179.190.102.34.bc.googleusercontent.com (34.102.190.179), Dst: a32922bf-9610-48d2-8e2f-6ea3d957f698.local (192.168.0.26)
0100 ..... = Version: 4
..... 0101 = Header Length: 20 bytes (5)
> Differentiated Services Field: 0x20 (DSCP: CS1, ECN: Not-ECT)
Total Length: 58
Identification: 0x0000 (0)
> 010. .... = Flags: 0x2, Don't fragment
...0 0000 0000 0000 = Fragment Offset: 0
Time to Live: 59
Protocol: UDP (17)
Header Checksum: 0x9dh7 [validation disabled]
[Header checksum status: Unverified]
Source Address: 179.190.102.34.bc.googleusercontent.com (34.102.190.179)
Destination Address: a32922bf-9610-48d2-8e2f-6ea3d957f698.local (192.168.0.26)
> User Datagram Protocol, Src Port: https (443), Dst Port: 63532 (63532)
> Data (30 bytes)

0000 20 4e f6 50 b6 c7 50 6a 03 7c 36 2a 08 00 45 20 N-P-Pj |6*..E
0010 00 3a 00 00 00 3b 11 9d b7 22 66 be b3 c0 a8 :..@:;..f....
0020 00 1a 01 bb f8 2c 00 26 c6 c0 49 a6 92 29 ce f6 :.., & ..I..)
0030 c2 b0 ab 3b 11 04 66 a4 aa b9 01 9d ae 85 18 ff :..f: .....
0040 f3 2d f3 92 ca af e7 75 :.....u

```

- e.
 - i. Source IP = 22 66 be b3
 - ii. Destination IP = c0 a8 00 1a
 - iii. UDP length = 89
- f. $1F9+182+89 = 404+1f9 = 5FD$
 - i. $5FD = 1111\ 1101$
 - ii. $FF = 1111\ 1111$
 - iii. $\quad = 0000\ 0010 = 2$

2. With GBN, is it possible for the sender to receive an ACK for a packet that falls outside of its current sending window? Please describe your assumption clearly.
 - a. Yes it is possible, because Go Back N it uses a process where the receiver sends a single acknowledgment in response to a certain number (n) of frames received, this is called cumulative acknowledgement. An example is when a sender has a window size of 3 and sends packets 1, 2, 3 at T0 and at T1 the receiver ACKS 1, 2, 3. Then at T2 the sender will be timed out and resends 1, 2, 3. Then at T3 the receiver will receive the copies and re acknowledges 1,2,4,