DALHOUSIE UNIVERSITY

CSCI 6704

Advanced Topics in Networks

Assignment 1

Name: Jay Sanjaybhai Patel
Banner ID: B00982253

Table of Contents

Exercise 1: Virtual Circuit Packet Switching

Switch 1

VCin	In port	VCout	Out port
10	1	10	3
10	2	20	3
10	3	10	4
20	3	10	2
10	4	30	3
30	3	10	1

Switch 2

VCin	In port	VCout	Out port
10	2	10	4
20	2	20	4
10	1	10	2
10	3	30	4
10	4	20	2
20	4	10	3
30	2	10	1
30	4	30	2

Switch 3

VCin	In port	VCout	Out port
10	1	10	2
10	4	10	3
10	2	20	3
10	3	10	1
20	3	10	4

Switch 4

VCin	In port	VCout	Out port
10	3	10	4
20	3	20	4
10	1	10	3
20	1	20	3
10	2	30	3
10	4	10	1
30	3	20	1

Switch 5

VCin	In port	VCout	Out port
10	1	10	4
20	1	10	2
30	1	20	2

10	2	10	3
20	2	10	1
30	2	20	1
10	3	30	2
10	4	30	1

Exercise 2: TCP/IP Encapsulation Discovery using Wireshark

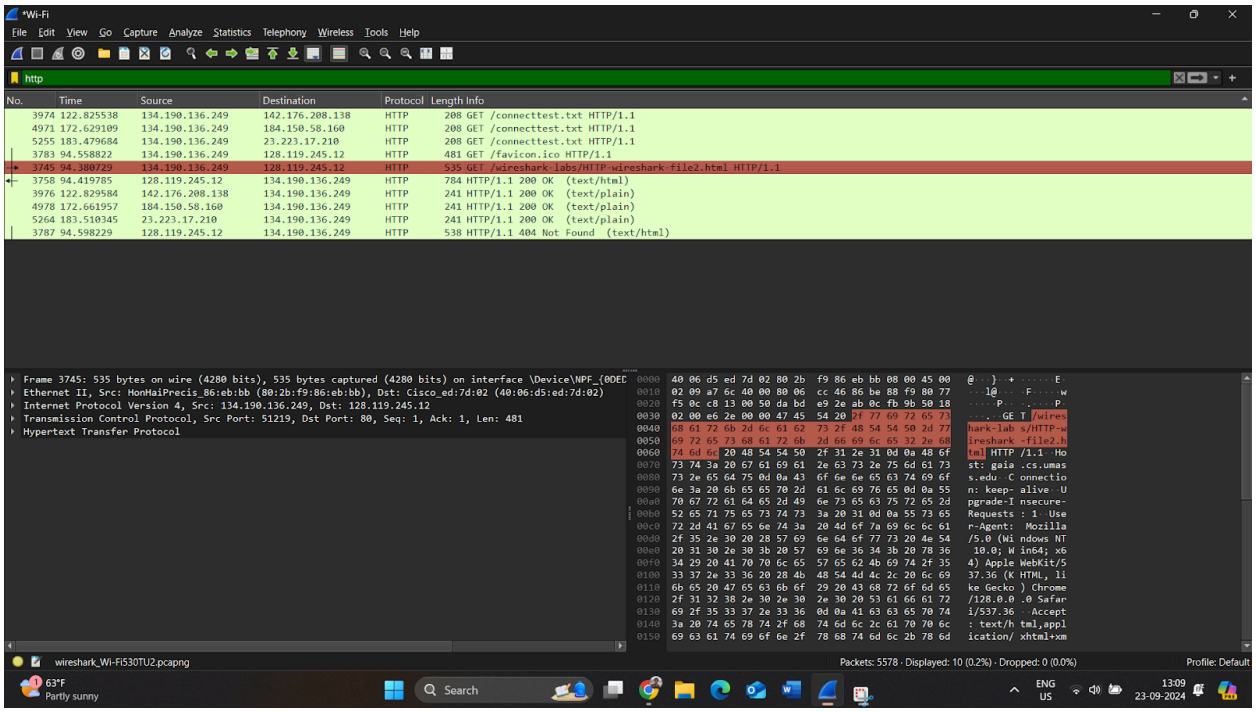

Figure 1: HTTP Message and All Headers

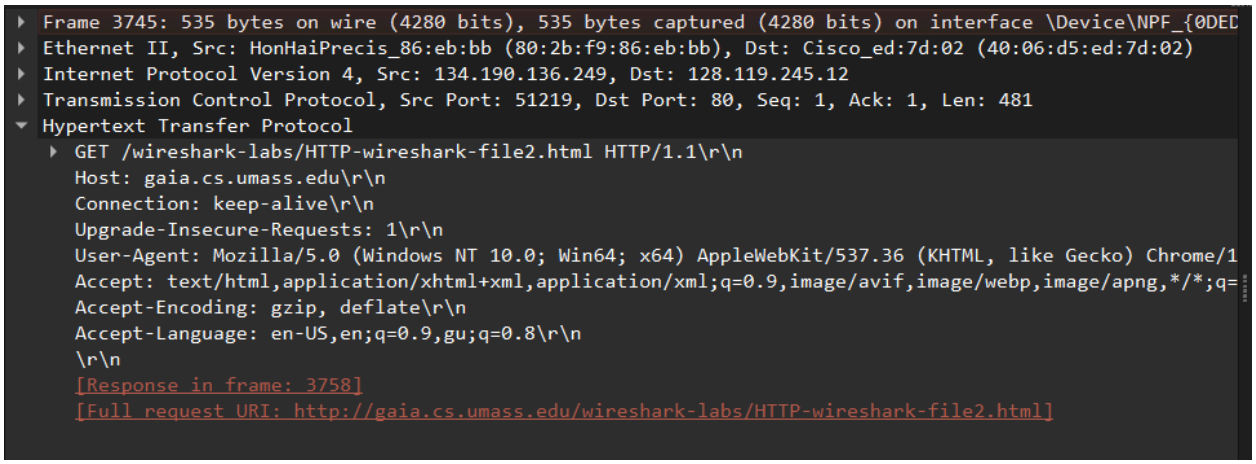

Figure 2: Application layer

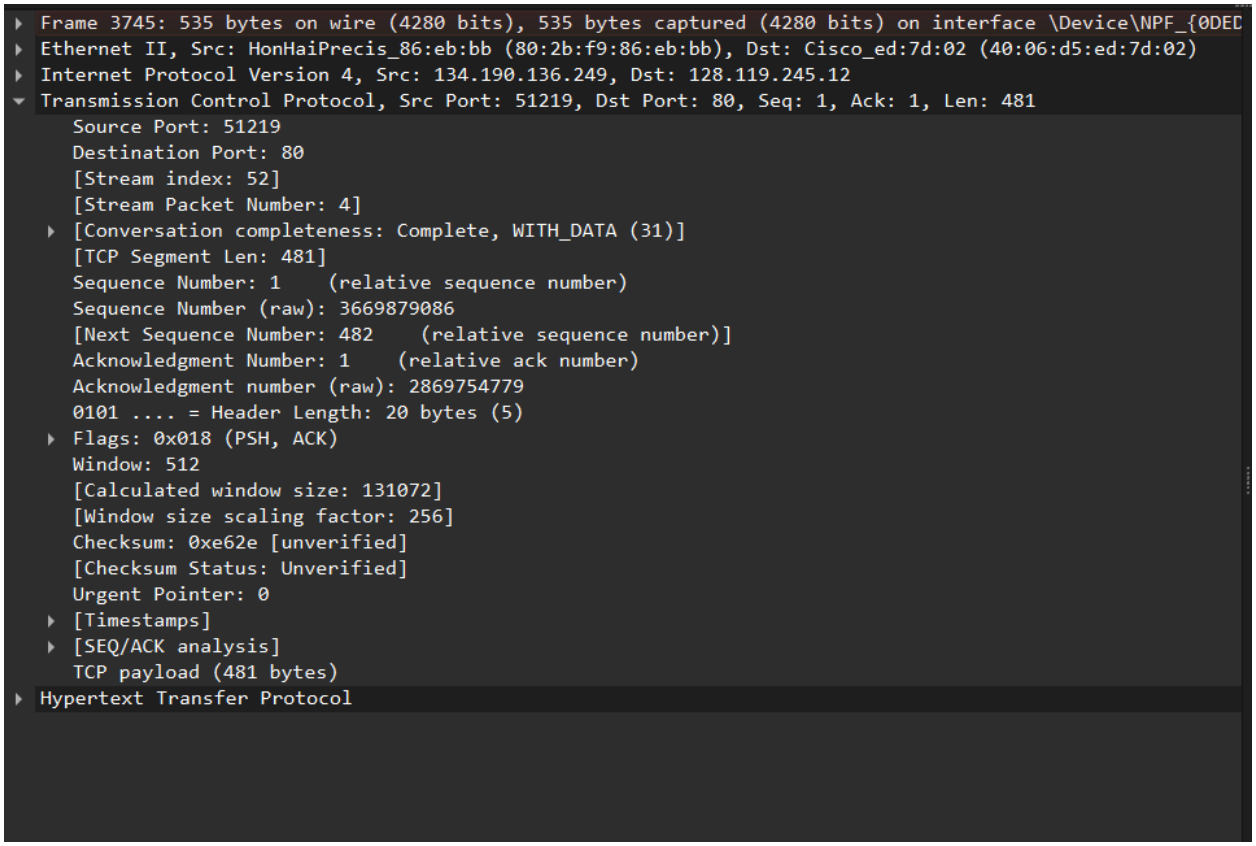

Figure 3: Transport layer

Table 1: TCP Header Values

51219								80
3669879086 (raw)								
2869754779 (raw)								
5 (20 Bytes - 0101)	0	0	1	1	0	0	0	512
0xe62e								0
None								
None								

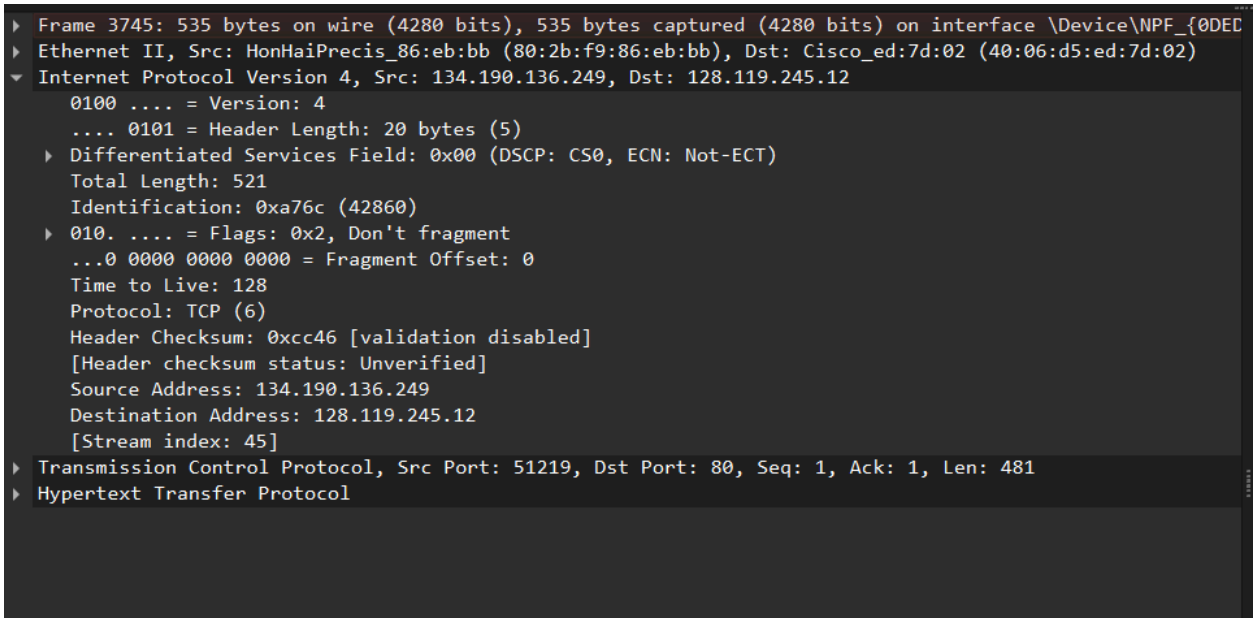

Figure 4: Network layer

Table 2: IP Header Values

4 (0100)	5 (0101)	0x00 (CS0)	521			
0xa76c (42860)			0	1	0	0
128	6 (TCP)		0xcc46			
134.190.136.249						
128.119.245.12						
None						
None						

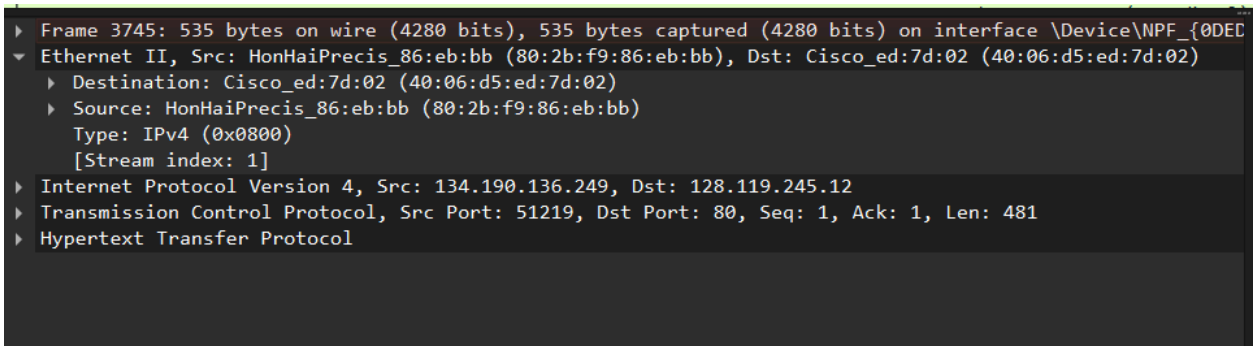

Figure 5: Data link layer

For Data link layer, values are identified as below :

- Destination MAC Address : Cisco_ed:7d:02 (40:06:d5:ed:7d:02)
- Source MAC Address : HonHaiPrecis_86:eb:bb (80:2b:f9:86:eb:bb)
- Type : IPV4 (0x08000)

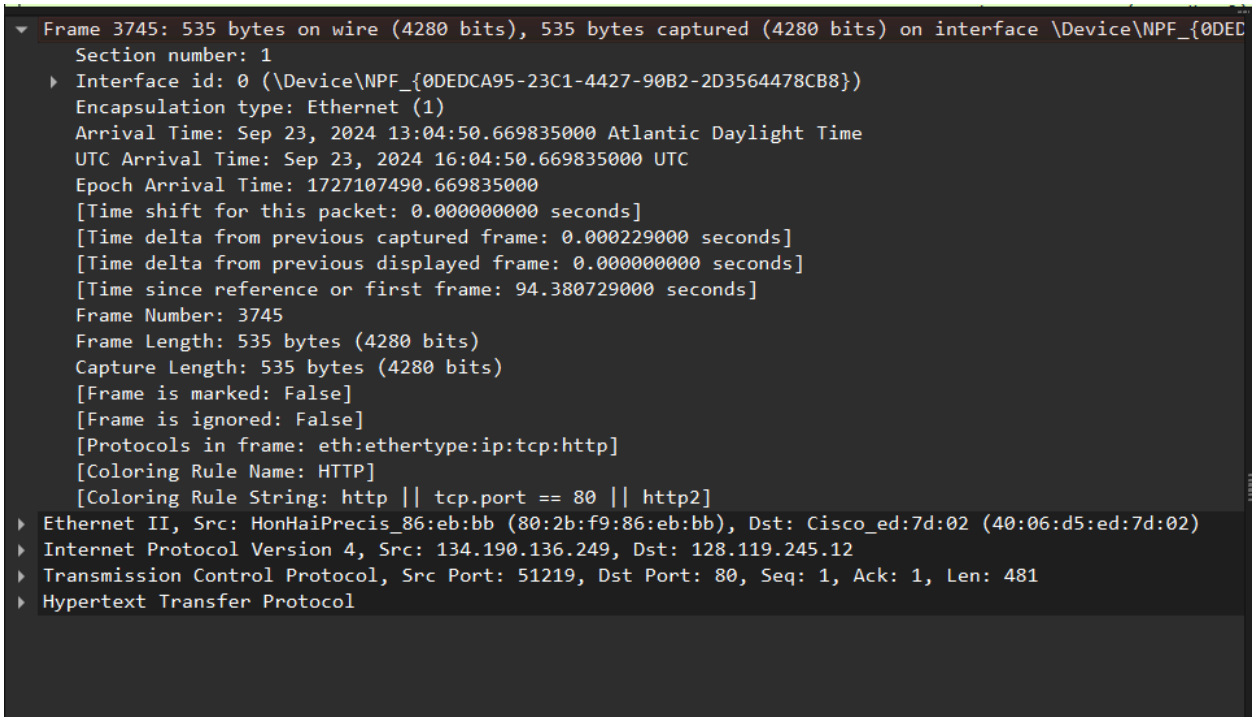

Figure 6: Physical layer

Are you able to find the Data Link Trailer in the Ethernet frame capture in Wireshark? Why or why not?

No, you cannot find the Data Link Trailer in an Ethernet frame capture using Wireshark because the Frame Check Sequence (FCS) which is responsible for error checking is not typically captured in Wireshark. This happens as the FCS is typically removed by network interface cards (NICs) before sending the frame to the OS for capture.

References

[1] "Wireshark.Go Deep", *wireshark.org* [Online]. Available: https://www.wireshark.org/. [Accessed: Sep 23rd, 2024].