



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.....	3
Exercise 2: TCP/IP Encapsulation Discovery using Wireshark.....	6
References.....	11

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

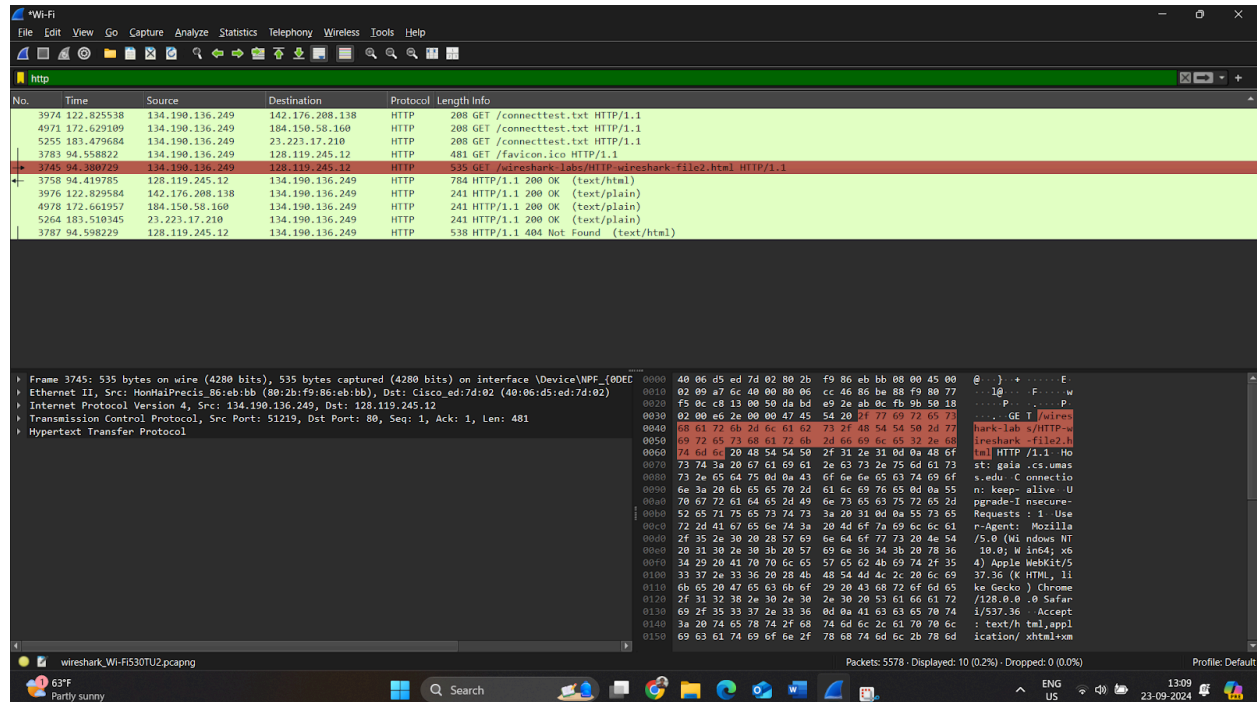


Figure 1: HTTP Message and All Headers

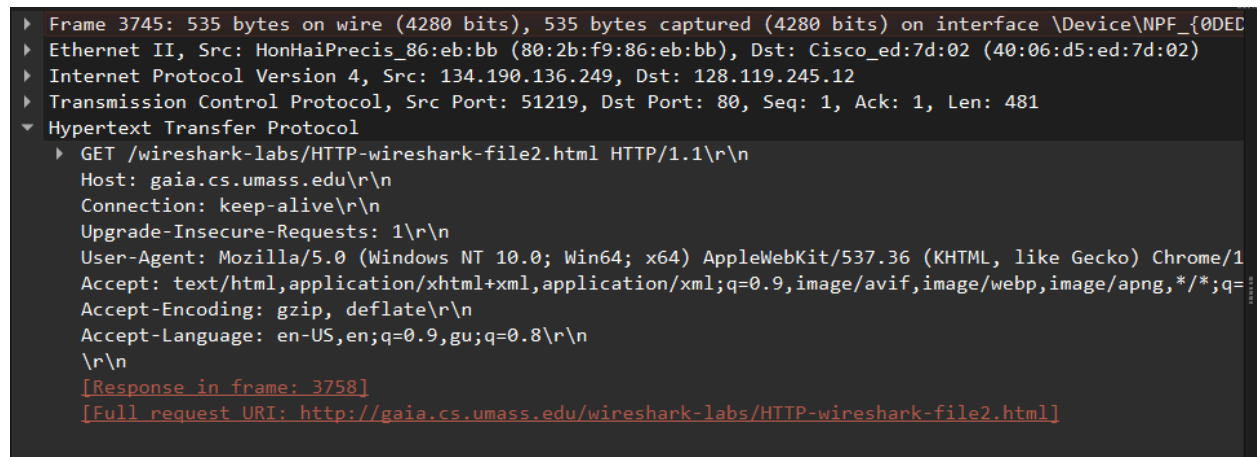


Figure 2: Application layer

```

▶ Frame 3745: 535 bytes on wire (4280 bits), 535 bytes captured (4280 bits) on interface \Device\NPF_{0DEC
▶ Ethernet II, Src: HonHaiPrecis_86:eb:bb (80:2b:f9:86:eb:bb), Dst: Cisco_ed:7d:02 (40:06:d5:ed:7d:02)
▶ Internet Protocol Version 4, Src: 134.190.136.249, Dst: 128.119.245.12
▼ Transmission Control Protocol, Src Port: 51219, Dst Port: 80, Seq: 1, Ack: 1, Len: 481
    Source Port: 51219
    Destination Port: 80
    [Stream index: 52]
    [Stream Packet Number: 4]
    ▶ [Conversation completeness: Complete, WITH_DATA (31)]
    [TCP Segment Len: 481]
    Sequence Number: 1 (relative sequence number)
    Sequence Number (raw): 3669879086
    [Next Sequence Number: 482 (relative sequence number)]
    Acknowledgment Number: 1 (relative ack number)
    Acknowledgment number (raw): 2869754779
    0101 .... = Header Length: 20 bytes (5)
    ▶ Flags: 0x018 (PSH, ACK)
    Window: 512
    [Calculated window size: 131072]
    [Window size scaling factor: 256]
    Checksum: 0xe62e [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
    ▶ [Timestamps]
    ▶ [SEQ/ACK analysis]
    TCP payload (481 bytes)
▶ Hypertext Transfer Protocol

```

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															

```

> Frame 3745: 535 bytes on wire (4280 bits), 535 bytes captured (4280 bits) on interface \Device\NPF_{0DEC
> Ethernet II, Src: HonHaiPrecis_86:eb:bb (80:2b:f9:86:eb:bb), Dst: Cisco_ed:7d:02 (40:06:d5:ed:7d:02)
> Internet Protocol Version 4, Src: 134.190.136.249, Dst: 128.119.245.12
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 521
    Identification: 0xa76c (42860)
  > 010. .... = Flags: 0x2, Don't fragment
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 128
    Protocol: TCP (6)
    Header Checksum: 0xcc46 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 134.190.136.249
    Destination Address: 128.119.245.12
    [Stream index: 45]
  > Transmission Control Protocol, Src Port: 51219, Dst Port: 80, Seq: 1, Ack: 1, Len: 481
  > Hypertext Transfer Protocol

```

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						


```

▶ Frame 3745: 535 bytes on wire (4280 bits), 535 bytes captured (4280 bits) on interface \Device\NPF_{0DEC
▼ Ethernet II, Src: HonHaiPrecis_86:eb:bb (80:2b:f9:86:eb:bb), Dst: Cisco_ed:7d:02 (40:06:d5:ed:7d:02)
  ▶ Destination: Cisco_ed:7d:02 (40:06:d5:ed:7d:02)
  ▶ Source: HonHaiPrecis_86:eb:bb (80:2b:f9:86:eb:bb)
    Type: IPv4 (0x0800)
    [Stream index: 1]
▶ Internet Protocol Version 4, Src: 134.190.136.249, Dst: 128.119.245.12
▶ Transmission Control Protocol, Src Port: 51219, Dst Port: 80, Seq: 1, Ack: 1, Len: 481
▶ Hypertext Transfer Protocol

```

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)

```

▼ Frame 3745: 535 bytes on wire (4280 bits), 535 bytes captured (4280 bits) on interface \Device\NPF_{0DEC
  Section number: 1
  ▶ Interface id: 0 (\Device\NPF_{0DEDC95-23C1-4427-90B2-2D3564478CB8})
  Encapsulation type: Ethernet (1)
  Arrival Time: Sep 23, 2024 13:04:50.669835000 Atlantic Daylight Time
  UTC Arrival Time: Sep 23, 2024 16:04:50.669835000 UTC
  Epoch Arrival Time: 1727107490.669835000
  [Time shift for this packet: 0.000000000 seconds]
  [Time delta from previous captured frame: 0.000229000 seconds]
  [Time delta from previous displayed frame: 0.000000000 seconds]
  [Time since reference or first frame: 94.380729000 seconds]
  Frame Number: 3745
  Frame Length: 535 bytes (4280 bits)
  Capture Length: 535 bytes (4280 bits)
  [Frame is marked: False]
  [Frame is ignored: False]
  [Protocols in frame: eth:ethertype:ip:tcp:http]
  [Coloring Rule Name: HTTP]
  [Coloring Rule String: http || tcp.port == 80 || http2]
  ▶ Ethernet II, Src: HonHaiPrecis_86:eb:bb (80:2b:f9:86:eb:bb), Dst: Cisco_ed:7d:02 (40:06:d5:ed:7d:02)
  ▶ Internet Protocol Version 4, Src: 134.190.136.249, Dst: 128.119.245.12
  ▶ Transmission Control Protocol, Src Port: 51219, Dst Port: 80, Seq: 1, Ack: 1, Len: 481
  ▶ Hypertext Transfer Protocol

```

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].