

## Report for Lab 1-1: Testing Wireshark

Name: 전현승	Student ID: 2018112749	Date: 2020/03/22
-----------	------------------------	------------------

Part I	
1	Is the frame an outgoing or an incoming frame?
2	Source IP address of the network-layer header in the frame:
3	Destination IP address of the network-layer header in the frame:
4	Total number of bytes in the whole frame:
5	Number of bytes in the Ethernet (data-link layer) header:
6	Number of bytes in the IP header:
7	Number of bytes in the TCP header:
8	Total bytes in the message (at the application layer):

1. Is the frame an outgoing or an incoming frame?

The image shows a Wireshark packet capture window. The top pane displays a list of captured packets. Packet 228 is selected, showing an outgoing HTTP GET request from source IP 192.168.0.11 to destination IP 93.184.216.34. The middle pane shows the details of the selected packet, including the Ethernet II header, Internet Protocol Version 4 header, and Hypertext Transfer Protocol header. The bottom pane shows the raw packet data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
228	4.814888	192.168.0.11	93.184.216.34	HTTP	473	GET / HTTP/1.1
231	4.973307	93.184.216.34	192.168.0.11	HTTP	1076	HTTP/1.1 200 OK (text/html)
249	5.197131	192.168.0.11	93.184.216.34	HTTP	388	GET /favicon.ico HTTP/1.1
254	5.323703	93.184.216.34	192.168.0.11	HTTP	1067	HTTP/1.1 404 Not Found (text/html)

Frame 228: 473 bytes on wire (3784 bits), 473 bytes captured (3784 bits) on interface \Device\NPF\_{D136CB4F-CDA7-4A36-8BF9-CFDC17C41F29}

Interface id: 0 (\Device\NPF\_{D136CB4F-CDA7-4A36-8BF9-CFDC17C41F29})

Encapsulation type: Ethernet (1)

Arrival Time: Mar 22, 2020 14:02:40.788330000 대한민국 표준시

[Time shift for this packet: 0.00000000 seconds]

Epoch Time: 1584853360.788330000 seconds

[Time delta from previous captured frame: 0.000046000 seconds]

[Time delta from previous displayed frame: 0.000000000 seconds]

[Time since reference or first frame: 4.814888000 seconds]

Frame Number: 228

Frame Length: 473 bytes (3784 bits)

0000 88 36 6c e8 4a dc dc fb 48 5e bc 03 08 00 45 00 -61.J... H^...E-

0010 01 cb d6 5b 40 00 80 06 00 00 c0 a8 00 0b 5d b8 ...[@... ..].

0020 d8 22 25 2e 00 50 2e 80 3d 19 53 e4 f9 9e 50 18 .%.P..=.S...P.

0030 02 01 57 f9 00 00 65 78 61 6d 70 6c 65 2e 63 6f ..W...ex ample.co

0040 6d 0d 0a 43 6f 6e 6e 65 63 74 69 6f 6e 3a 20 6b m..Conne ction: k

0050 65 65 70 2d 61 6c 69 76 65 0d 0a 55 70 67 72 61 eep-aliv e..Upgra

0060 64 65 2d 49 6e 73 65 63 75 72 65 2d 52 65 71 75 de-Insec ure-Requ

0070 65 73 74 73 3a 20 31 0d 0a 55 73 65 72 2d 41 67 ests: 1. ·User-Ag

0080 65 6e 74 3a 20 4d 6f 7a 69 6c 6c 61 2f 35 2e 30 ent: Moz illa/5.0

0090 20 28 57 69 6e 64 6f 77 73 20 4e 54 20 31 30 2e (Window s NT 10.

00a0 30 3b 20 57 69 6e 36 34 3b 20 78 36 34 29 20 41 0; Win64 ; x64) A

Frame (473 bytes) Reassembled TCP (440 bytes)

Interface id (frame.interface\_id) | Packets: 266 · Displayed: 4 (1.5%) · Dropped: 0 (0.0%) | Profile: Default

Outgoing frame (GET request)

2. Source IP address of the network-layer header in the frame:
3. Destination IP address of the network-layer header in the frame:

The image shows the details pane of the selected packet (Frame 228) in Wireshark. The 'Internet Protocol Version 4' header is expanded, showing the source IP address as 192.168.0.11 and the destination IP address as 93.184.216.34. The 'Transmission Control Protocol' header is also expanded, showing the source port as 9518 and the destination port as 80.

[Header checksum status: Unverified]

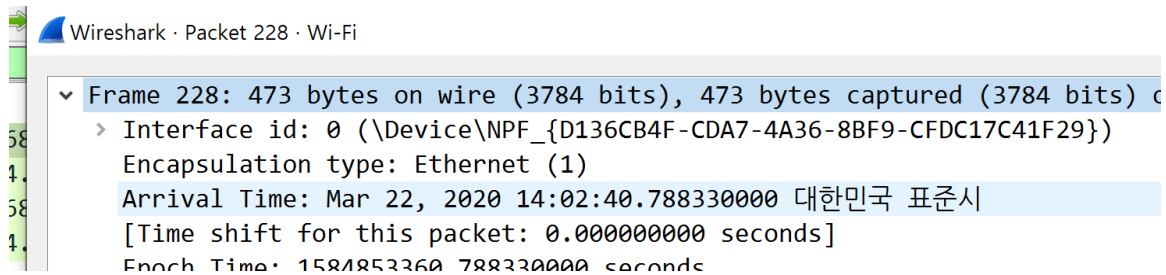
Source: 192.168.0.11

Destination: 93.184.216.34

Transmission Control Protocol, Src Port: 9518, Dst Port: 80, S

Source IP address : 192.168.0.11  
Destination IP address : 93.184.216.34

4. Total number of bytes in the whole frame:

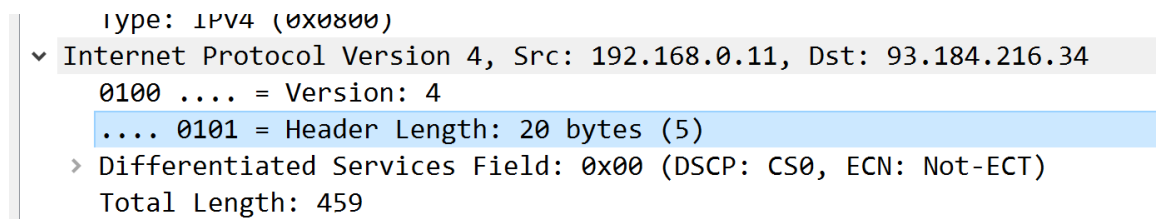


473 bytes

5. Number of bytes in the Ethernet (data-link layer) header:

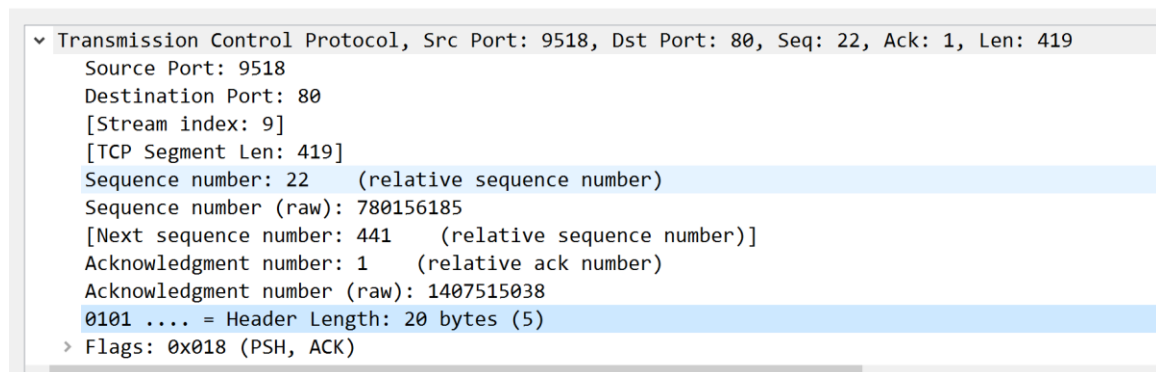
473 bytes (Whole frame) – 459 bytes (IPv4) = 14 bytes

6. Number of bytes in the IP header:



20 bytes

7. Number of bytes in the TCP header:



20 bytes

8. Total bytes in the message (at the application layer):

459 bytes (IPv4) – 20 bytes (IP header) – 20 bytes (TCP header) = 419 bytes