Wireshark Lab 1

ComputerSoftware

2020001658 이유민

1. Which of the following protocols are shown as appearing (i.e., are listed in the Wireshark "protocol" column) in your trace file: TCP, QUIC, HTTP, DNS, UDP, TLSv1.2?

➔ TCP, DNS, UDP, TLSv1.2, HTTP

2. How long did it take from when the HTTP GET message was sent until the HTTP OK reply was received? (By default, the value of the Time column in the packet listing window is the amount of time, in seconds, since Wireshark tracing began. (If you want to display the Time field in time-of-day format, select the Wireshark View pull down menu, then select Time Display Format, then select Time-of-day.)

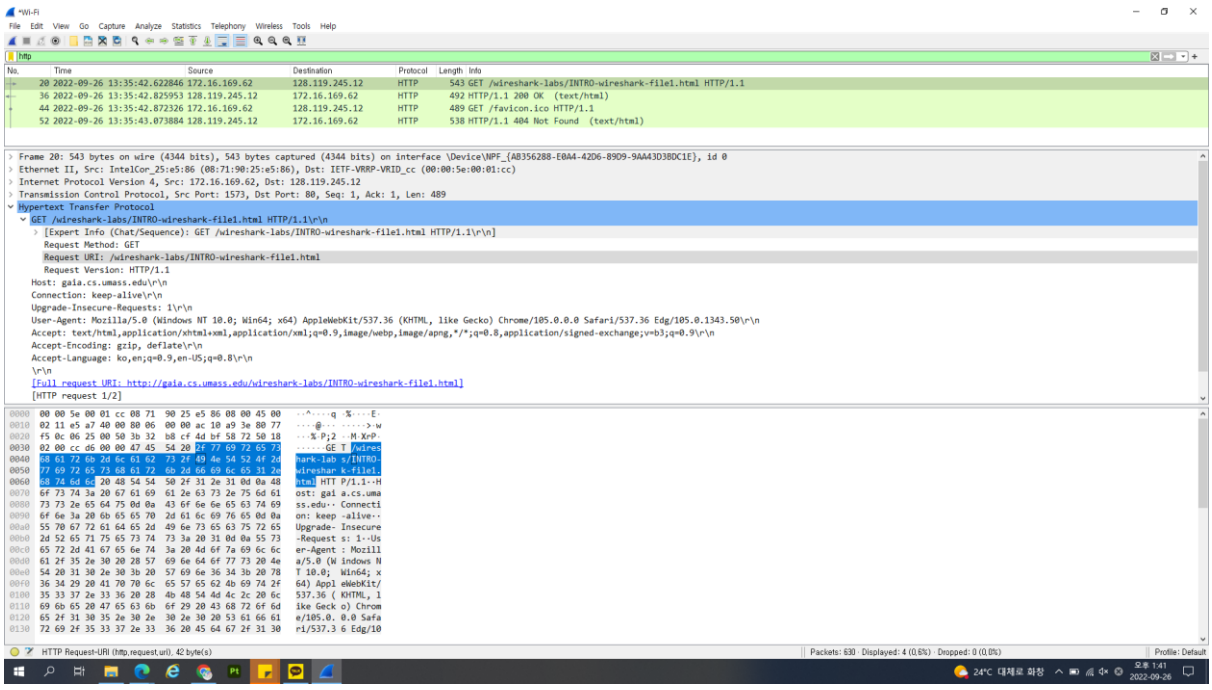
➔ 58.313738 – 58.107613 = 0.206125

3. hat is the Internet address of the gaia.cs.umass.edu (also known as www net.cs.umass.edu)? What is the Internet address of your computer or (if you are using the trace file) the computer that sent the HTTP GET message?

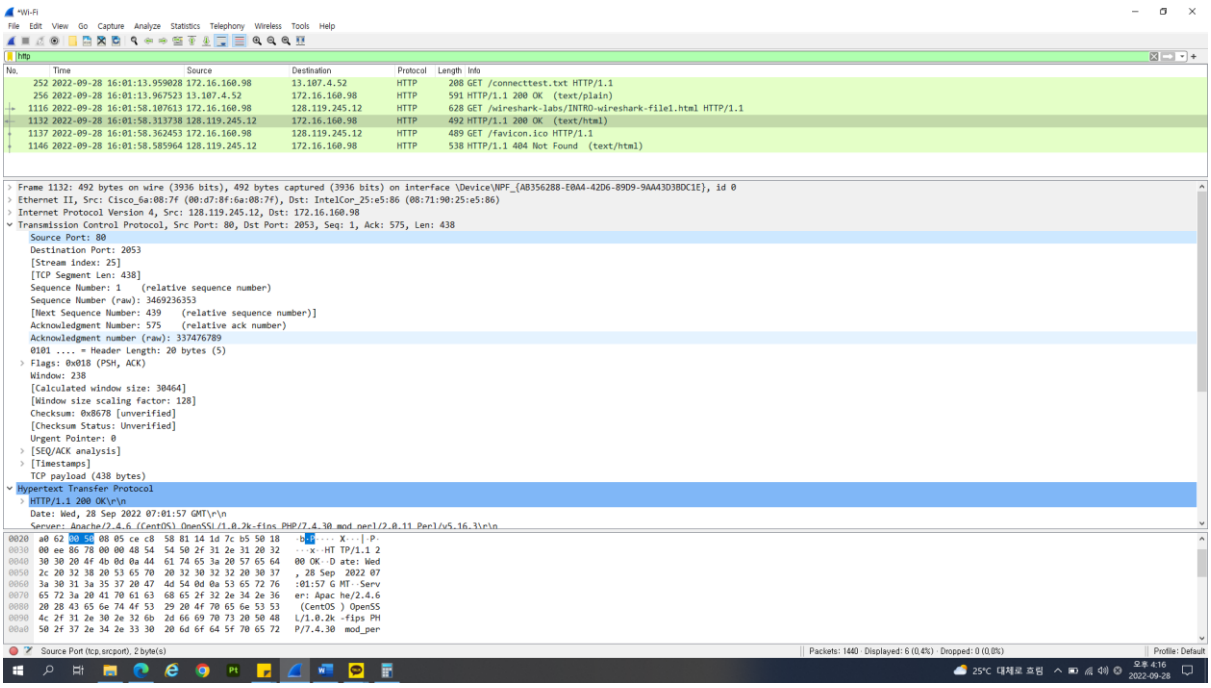
➔ 172.16.260.98

➔ 128.119.245.12

4. . Expand the information on the HTTP message in the Wireshark "Details of selected packet" window (see Figure 3 above) so you can see the fields in the HTTP GET request message. What type of Web browser issued the HTTP request? The answer is shown at the right end of the information following the "User-Agent:" field in the expanded HTTP message display. [This field value in the HTTP message is how a web server learns what type of browser you are using.]



5. Expand the information on the Transmission Control Protocol for this packet in the Wireshark "Details of selected packet" window (see Figure 3 in the lab writeup) so you can see the fields in the TCP segment carrying the HTTP message. What is the destination port number (the number following "Dest Port:" for the TCP segment containing the HTTP request) to which this HTTP request is being sent?



➔

➔ 80

6. Print the two HTTP messages (GET and OK) referred to in question 2 above. To do so, select Print from the Wireshark File command menu, and select the "Selected Packet Only" and "Print as displayed" radial buttons, and then click OK.

```
No.     Time                           Source                Destination           Protocol Length Info
   1116 2022-09-28 16:01:58.107613    172.16.160.98         128.119.245.12        HTTP     628    GET /wireshark-
labs/INTRO-wireshark-file1.html HTTP/1.1
Frame 1116: 628 bytes on wire (5024 bits), 628 bytes captured (5024 bits) on interface \Device\NPF_{AB356288-
E0A4-42D6-89D9-9AA43D3BDC1E}, id 0
Ethernet II, Src: IntelCor_25:e5:86 (08:71:90:25:e5:86), Dst: IETF-VRRP-VRID_cc (00:00:5e:00:01:cc)
Internet Protocol Version 4, Src: 172.16.160.98, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 2053, Dst Port: 80, Seq: 1, Ack: 1, Len: 574
    Source Port: 2053
    Destination Port: 80
    [Stream index: 25]
    [TCP Segment Len: 574]
    Sequence Number: 1    (relative sequence number)
    Sequence Number (raw): 337476215
    [Next Sequence Number: 575    (relative sequence number)]
    Acknowledgment Number: 1    (relative ack number)
    Acknowledgment number (raw): 3469236353
    0101 .... = Header Length: 20 bytes (5)
    Flags: 0x018 (PSH, ACK)
    Window: 512
    [Calculated window size: 131072]
    [Window size scaling factor: 256]
    Checksum: 0xc44f [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
    [SEQ/ACK analysis]
    [Timestamps]
    TCP payload (574 bytes)
Hypertext Transfer Protocol
    GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1\r\n
    Host: gaia.cs.umass.edu\r\n
    Connection: keep-alive\r\n
    Upgrade-Insecure-Requests: 1\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/105.0.0.0
Safari/537.36 Edg/105.0.1343.50\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/
signed-exchange;v=b3;q=0.9\r\n
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: ko,en;q=0.9,en-US;q=0.8\r\n
    If-None-Match: "51-5e97a1b97aa0b"\r\n
    If-Modified-Since: Sun, 25 Sep 2022 05:59:01 GMT\r\n
    \r\n
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html]
    [HTTP request 1/2]
    [Response in frame: 1132]
    [Next request in frame: 1137]
No.     Time                           Source                Destination           Protocol Length Info
   1132 2022-09-28 16:01:58.313738    128.119.245.12        172.16.160.98         HTTP     492    HTTP/1.1 200 OK
(text/html)
Frame 1132: 492 bytes on wire (3936 bits), 492 bytes captured (3936 bits) on interface \Device\NPF_{AB356288-
E0A4-42D6-89D9-9AA43D3BDC1E}, id 0
Ethernet II, Src: Cisco_6a:08:7f (00:d7:8f:6a:08:7f), Dst: IntelCor_25:e5:86 (08:71:90:25:e5:86)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 172.16.160.98
Transmission Control Protocol, Src Port: 80, Dst Port: 2053, Seq: 1, Ack: 575, Len: 438
    Source Port: 80
    Destination Port: 2053
    [Stream index: 25]
    [TCP Segment Len: 438]
    Sequence Number: 1    (relative sequence number)
    Sequence Number (raw): 3469236353
    [Next Sequence Number: 439    (relative sequence number)]
    Acknowledgment Number: 575    (relative ack number)
    Acknowledgment number (raw): 337476789
    0101 .... = Header Length: 20 bytes (5)
    Flags: 0x018 (PSH, ACK)
    Window: 238
    [Calculated window size: 30464]
    [Window size scaling factor: 128]
    Checksum: 0x8678 [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
    [SEQ/ACK analysis]
    [Timestamps]
    TCP payload (438 bytes)
Hypertext Transfer Protocol
    HTTP/1.1 200 OK\r\n
    Date: Wed, 28 Sep 2022 07:01:57 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.30 mod_perl/2.0.11 Perl/v5.16.3\r\n
    Last-Modified: Wed, 28 Sep 2022 05:59:01 GMT\r\n
```

```
    ETag: "51-5e9b6751c3fac"\r\n
    Accept-Ranges: bytes\r\n
    Content-Length: 81\r\n
    Keep-Alive: timeout=5, max=100\r\n
    Connection: Keep-Alive\r\n
    Content-Type: text/html; charset=UTF-8\r\n
    \r\n
    [HTTP response 1/2]
    [Time since request: 0.206125000 seconds]
    [Request in frame: 1116]
    [Next request in frame: 1137]
    [Next response in frame: 1146]
    [Request URI: http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html]
    File Data: 81 bytes
Line-based text data: text/html (3 lines)
```