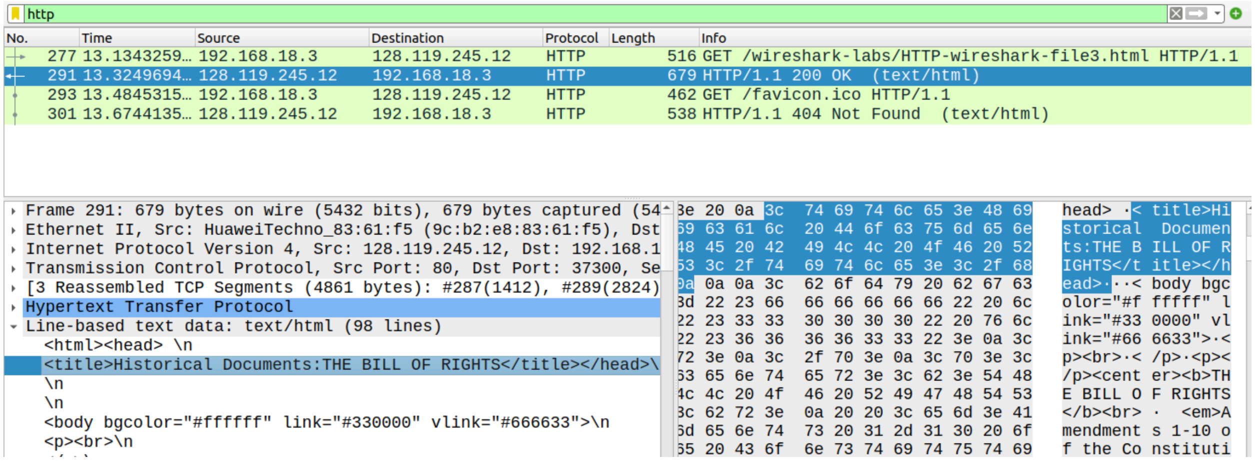
CN LAB-06 Exercises

1. **How many HTTP GET request messages did your browser send? Which packet number in the trace contains the GET message for the Bill or Rights?**
   The browser sent 2 HTTP GET requests. 1 for the html file and 1 for the favicon.ico file.

2. **Which packet number in the trace contains the status code and phrase associated with the response to the HTTP GET request?**
   Packet no. 2 contains the get message for the Bill or Rights.



```
http
No.   Time          Source          Destination     Protocol Length Info
  277 13.1343259… 192.168.18.3    128.119.245.12  HTTP        516 GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
  291 13.3249694… 128.119.245.12  192.168.18.3    HTTP        679 HTTP/1.1 200 OK  (text/html)
  293 13.4845315… 192.168.18.3    128.119.245.12  HTTP        462 GET /favicon.ico HTTP/1.1
  301 13.6744135… 128.119.245.12  192.168.18.3    HTTP        538 HTTP/1.1 404 Not Found  (text/html)
```

```
› Frame 291: 679 bytes on wire (5432 bits), 679 bytes captured (54
› Ethernet II, Src: HuaweiTechno_83:61:f5 (9c:b2:e8:83:61:f5), Dst
› Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1
› Transmission Control Protocol, Src Port: 80, Dst Port: 37300, Se
› [3 Reassembled TCP Segments (4861 bytes): #287(1412), #289(2824)
› Hypertext Transfer Protocol
⌄ Line-based text data: text/html (98 lines)
    <html><head> \n
    <title>Historical Documents:THE BILL OF RIGHTS</title></head>\
    \n
    \n
    <body bgcolor="#ffffff" link="#330000" vlink="#666633">\n
    <p><br>\n
```

```
3e 20 0a 3c  74 69 74 6c 65 3e 48 69   head> ·< title>Hi
69 63 61 6c  20 44 6f 63 75 6d 65 6e   storical  Documen
48 45 20 42  49 4c 4c 20 4f 46 20 52   ts:THE B ILL OF R
53 3c 2f 74  69 74 6c 65 3e 3c 2f 68   IGHTS</t itle></h
0a 0a 0a 3c  62 6f 64 79 20 62 67 63   ead>···< body bgc
3d 22 23 66  66 66 66 66 66 22 20 6c   olor="#f fffff" l
22 23 33 33  30 30 30 30 22 20 76 6c   ink="#33 0000" vl
22 23 36 36  36 36 33 33 22 3e 0a 3c   ink="#66 6633">·<
72 3e 0a 3c  2f 70 3e 0a 3c 70 3e 3c   p><br>·< /p>·<p><
63 65 6e 74  65 72 3e 3c 62 3e 54 48   /p><cent er><b>TH
4c 4c 20 4f  46 20 52 49 47 48 54 53   E BILL O F RIGHTS
3c 62 72 3e  0a 20 20 3c 65 6d 3e 41   </b><br> ·  <em>A
6d 65 6e 74  73 20 31 2d 31 30 20 6f   mendment s 1-10 o
65 20 43 6f  6e 73 74 69 74 75 74 69   f the Co nstituti
```

3. **What is the status code and phrase in the response?**
   Status code is **304** and the phrase is **Not Modified**.

4. **How many data-containing TCP segments were needed to carry the single HTTP response and the text of the Bill of Rights?**
   2 TCP segments were needed to carry the HTTP response of the text of the Bill of RIghts.

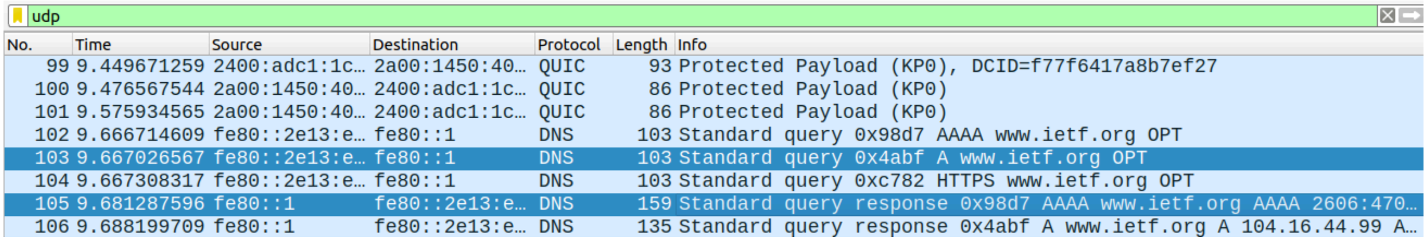
5. **How many HTTP GET request messages did your browser send? To which Internet addresses were these GET requests sent?**
   3 GET requests were sent by the browser. 1 for the HTML file and 2 for the two images respectively.
   Addresses were **128.119.245.12** and **178.79.137.164**.

6. **Can you tell whether your browser downloaded the two images serially, or whether they were downloaded from the two websites in parallel? Explain.**
   HTTP 1.1 cannot technically do parallel processing but it can perform multiple requests on the same socket with the help of pipelining. But still each response will be received in the order of its respective request. So we can say that the images were downloaded serially.

7. **What is the server's response (status code and phrase) in response to the initial HTTP GET message from your browser?**
   Status code is **401** and Phrase is **Unauthorized**.

8. **When your browser sends the HTTP GET message for the second time, what new field is included in the HTTP GET message?**
   A new authorization field is included in the HTTP request the second time.

9. **Locate the DNS query and response messages. Are they sent over UDP or TCP?**
   They are sent over UDP.

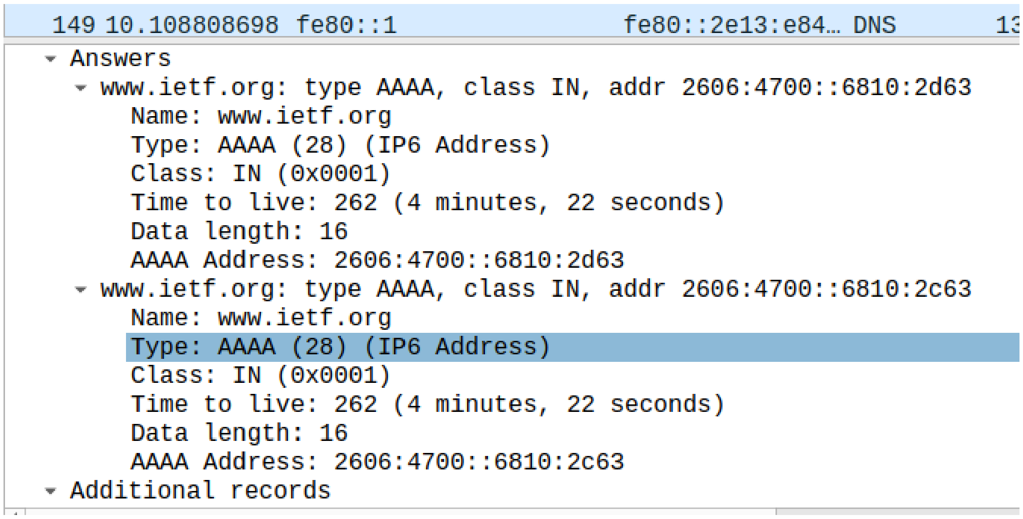


```
udp
No.  Time        Source           Destination      Protocol Length Info
 99 9.449671259 2400:adc1:1c… 2a00:1450:40… QUIC      93 Protected Payload (KP0), DCID=f77f6417a8b7ef27
100 9.476567544 2a00:1450:40… 2400:adc1:1c… QUIC      86 Protected Payload (KP0)
101 9.575934565 2a00:1450:40… 2400:adc1:1c… QUIC      86 Protected Payload (KP0)
102 9.666714609 fe80::2e13:e… fe80::1       DNS      103 Standard query 0x98d7 AAAA www.ietf.org OPT
103 9.667026567 fe80::2e13:e… fe80::1       DNS      103 Standard query 0x4abf A www.ietf.org OPT
104 9.667308317 fe80::2e13:e… fe80::1       DNS      103 Standard query 0xc782 HTTPS www.ietf.org OPT
105 9.681287596 fe80::1       fe80::2e13:e… DNS      159 Standard query response 0x98d7 AAAA www.ietf.org AAAA 2606:470…
106 9.688199709 fe80::1       fe80::2e13:e… DNS      135 Standard query response 0x4abf A www.ietf.org A 104.16.44.99 A…
```

10. **What is the destination port for the DNS query message? What is the source port of DNS response message?**
    Destination port for DNS query message is **53.**
    Source port for DN response message is **52649**.

11. **Examine the DNS query message. What "Type" of DNS query is it? Does the query message contain any "answers"?**
    It is a **standard DN query** and it contains answers.

12. **Examine the DNS response message. How many "answers" are provided? What do each of these answers contain?**
    The response contains 2 answers. Each answer contains: name. type, class, time to live, data length, AAAA address.



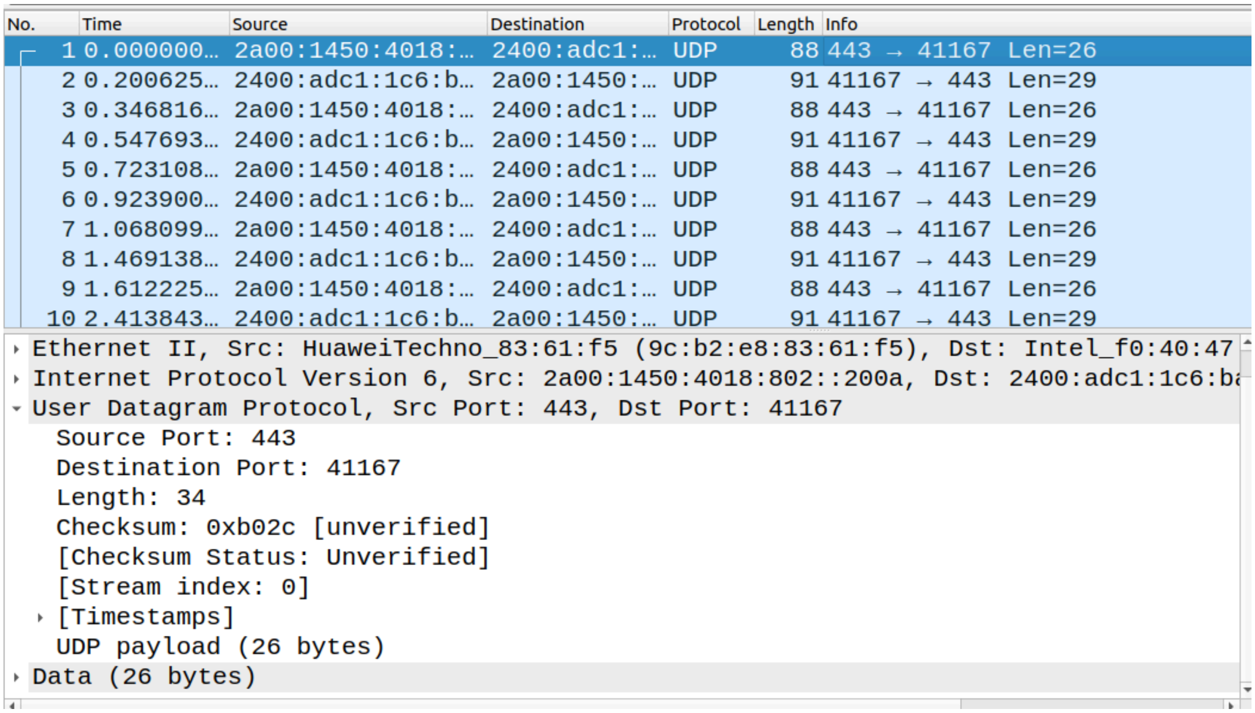
```
 149 10.108808698  fe80::1               fe80::2e13:e84… DNS       13
 Answers
    www.ietf.org: type AAAA, class IN, addr 2606:4700::6810:2d63
        Name: www.ietf.org
        Type: AAAA (28) (IP6 Address)
        Class: IN (0x0001)
        Time to live: 262 (4 minutes, 22 seconds)
        Data length: 16
        AAAA Address: 2606:4700::6810:2d63
    www.ietf.org: type AAAA, class IN, addr 2606:4700::6810:2c63
        Name: www.ietf.org
        Type: AAAA (28) (IP6 Address)
        Class: IN (0x0001)
        Time to live: 262 (4 minutes, 22 seconds)
        Data length: 16
        AAAA Address: 2606:4700::6810:2c63
 Additional records
```

13. **What is the sequence number of the TCP SYN segment that is used to initiate the TCP connection between the client computer and gaia.cs.umass.edu? What is it in the segment that identifies the segment as a SYN segment?**
Sequence number is 0
The **syn flag** is set to 1 therefore, we can tell that segment is a SYN segment.

14. **What is the sequence number of the SYNACK segment sent by gaia.cs.umass.edu to the client computer in reply to the SYN? What is the value of the Acknowledgement field in the SYNACK segment?**
Sequence number of the SYNACK segment is 0. Value of the Acknowledgement field is 1 or 49581726 (raw).

15. **What is the sequence number of the TCP segment containing the HTTP POST command?**
Sequence number of the TCP segment containing the HTTP POST command is 151782.

16. **By consulting the displayed information in Wireshark's packet content field for this packet, determine the length (in bytes) of each of the UDP header fields.**
Length of the UDP header is 26.



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000…	2a00:1450:4018:…	2400:adc1:…	UDP	88	443 → 41167 Len=26
2	0.200625…	2400:adc1:1c6:b…	2a00:1450:…	UDP	91	41167 → 443 Len=29
3	0.346816…	2a00:1450:4018:…	2400:adc1:…	UDP	88	443 → 41167 Len=26
4	0.547693…	2400:adc1:1c6:b…	2a00:1450:…	UDP	91	41167 → 443 Len=29
5	0.723108…	2a00:1450:4018:…	2400:adc1:…	UDP	88	443 → 41167 Len=26
6	0.923900…	2400:adc1:1c6:b…	2a00:1450:…	UDP	91	41167 → 443 Len=29
7	1.068099…	2a00:1450:4018:…	2400:adc1:…	UDP	88	443 → 41167 Len=26
8	1.469138…	2400:adc1:1c6:b…	2a00:1450:…	UDP	91	41167 → 443 Len=29
9	1.612225…	2a00:1450:4018:…	2400:adc1:…	UDP	88	443 → 41167 Len=26
10	2.413843…	2400:adc1:1c6:b…	2a00:1450:…	UDP	91	41167 → 443 Len=29

```
▸ Ethernet II, Src: HuaweiTechno_83:61:f5 (9c:b2:e8:83:61:f5), Dst: Intel_f0:40:47
▸ Internet Protocol Version 6, Src: 2a00:1450:4018:802::200a, Dst: 2400:adc1:1c6:ba
▾ User Datagram Protocol, Src Port: 443, Dst Port: 41167
    Source Port: 443
    Destination Port: 41167
    Length: 34
    Checksum: 0xb02c [unverified]
    [Checksum Status: Unverified]
    [Stream index: 0]
  ▸ [Timestamps]
    UDP payload (26 bytes)
▸ Data (26 bytes)
```

17. **The value in the Length field is the length of what? (You can consult the text for this answer). Verify your claim with your captured UDP packet.**
The length field is the length of the packet.

18. **What is the maximum number of bytes that can be included in a UDP payload?**
The maximum number of bytes that can be included in a UDP payload is (2^16 – 1) bytes plus the header bytes. This gives 65535 bytes – 8 bytes = 65527 bytes.

19. **What is the largest possible source port number?**
    65,535 is the largest possible port number.

20. **What is the protocol number for UDP? Give your answer in both hexadecimal and decimal notation.**
    The IP protocol number for UDP is 11 in hex, which is 17 in decimal value.

21. **Examine a pair of UDP packets in which your host sends the first UDP packet and the second UDP packet is a reply to this first UDP packet. (Hint: for a second packet to be sent in response to a first packet, the sender of the first packet should be the destination of the second packet). Describe the relationship between the port numbers in the two packets.**

    The port numbers are swapped between the request and reply packets to ensure proper delivery. The dynamically chosen source port in your first packet becomes the destination port for the reply, allowing your OS to route the incoming data to the correct application.