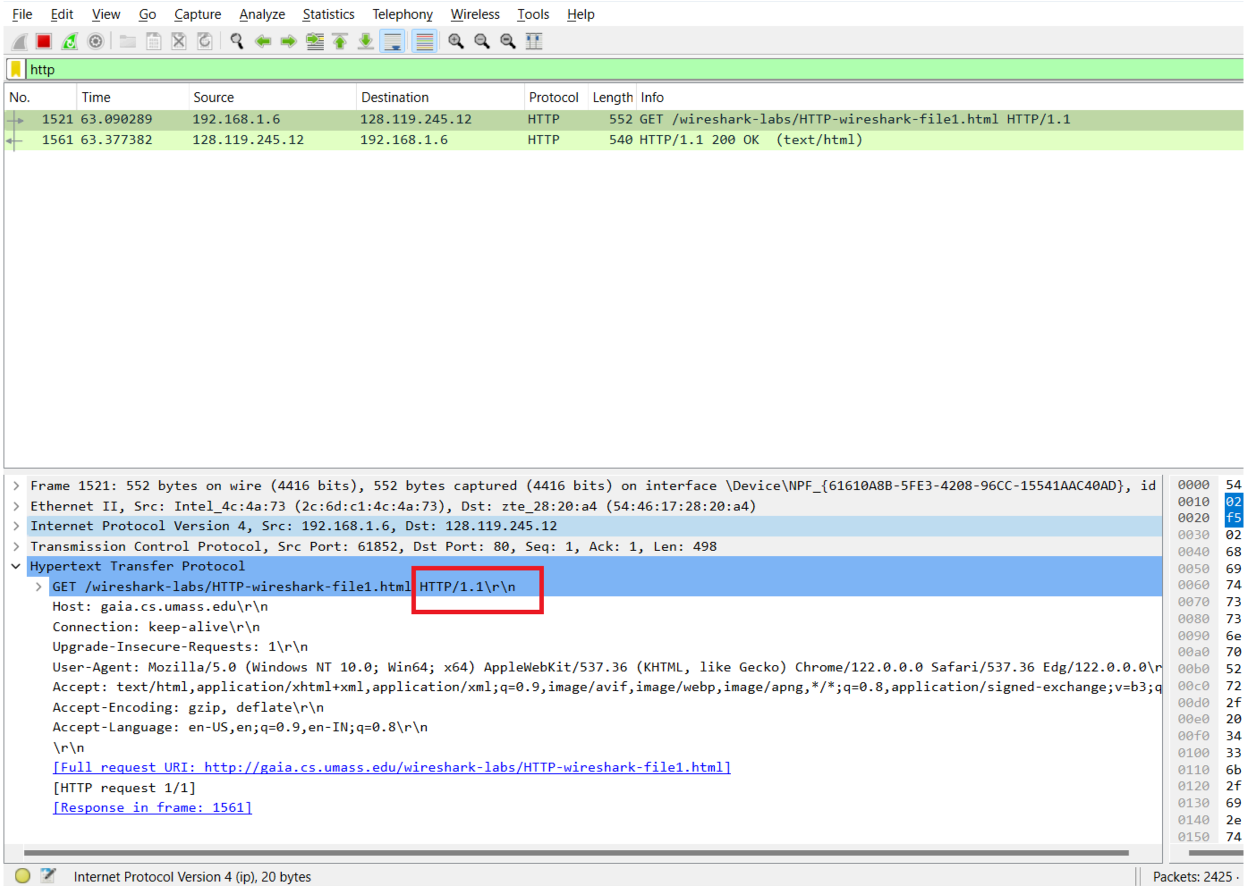
CN ASSIGNMENT 2

MOHAMMAD SHOAIB ANSARI
BT21CSE063
COMPUTER NETWORKS

HTTP: ASSIGNMENT

1. Is your browser running HTTP version 1.0 or 1.1?

- It is running HTTP 1.1



http

No.	Time	Source	Destination	Protocol	Length	Info
1521	63.090289	192.168.1.6	128.119.245.12	HTTP	552	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
1561	63.377382	128.119.245.12	192.168.1.6	HTTP	540	HTTP/1.1 200 OK (text/html)

```
> Frame 1521: 552 bytes on wire (4416 bits), 552 bytes captured (4416 bits) on interface \Device\NPF_{61610A8B-5FE3-4208-96CC-15541AAC40AD}, id
> Ethernet II, Src: Intel_4c:4a:73 (2c:6d:c1:4c:4a:73), Dst: zte_28:20:a4 (54:46:17:28:20:a4)
> Internet Protocol Version 4, Src: 192.168.1.6, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 61852, Dst Port: 80, Seq: 1, Ack: 1, Len: 498
v Hypertext Transfer Protocol
  > GET /wireshark-labs/HTTP-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/122.0.0.0 Safari/537.36 Edg/122.0.0.0\r
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: en-US,en;q=0.9,en-IN;q=0.8\r\n
    \r\n
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html]
    [HTTP request 1/1]
    [Response in frame: 1561]
```

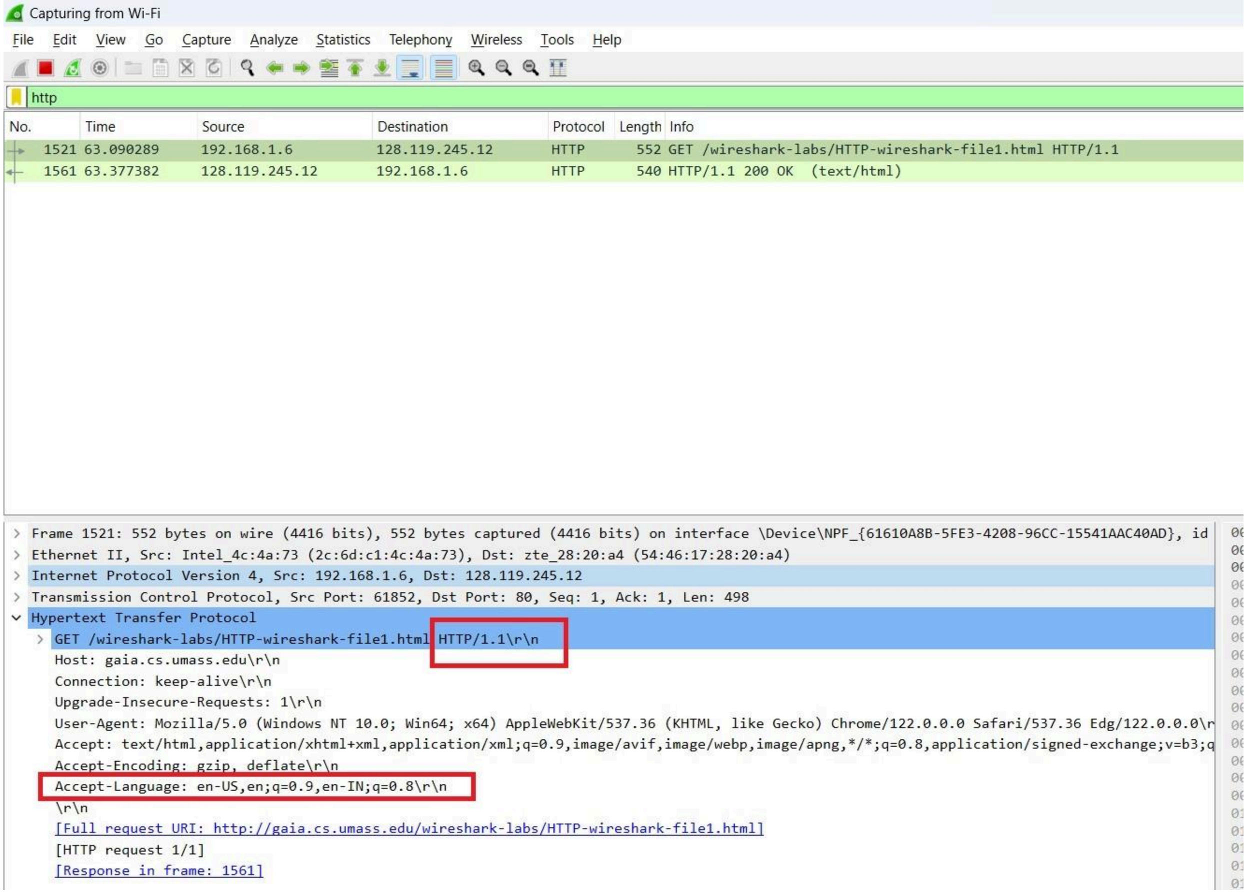
```
0000  54
0010  02
0020  f5
0030  02
0040  68
0050  69
0060  74
0070  73
0080  73
0090  6e
00a0  70
00b0  52
00c0  72
00d0  2f
00e0  20
00f0  34
0100  33
0110  6b
0120  2f
0130  69
0140  2e
0150  74
```

Internet Protocol Version 4 (ip), 20 bytes

Packets: 2425 ·

2. What languages (if any) does your browser indicate that it can accept to the server?

- "en-US,en;q=0.9,en-IN;q=0.8". This indicates that the preferred language is English (United States), with English (unspecified) as a secondary preference with a slightly lower weight, and English (India) as a third preference with an even lower weight.


Capturing from Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

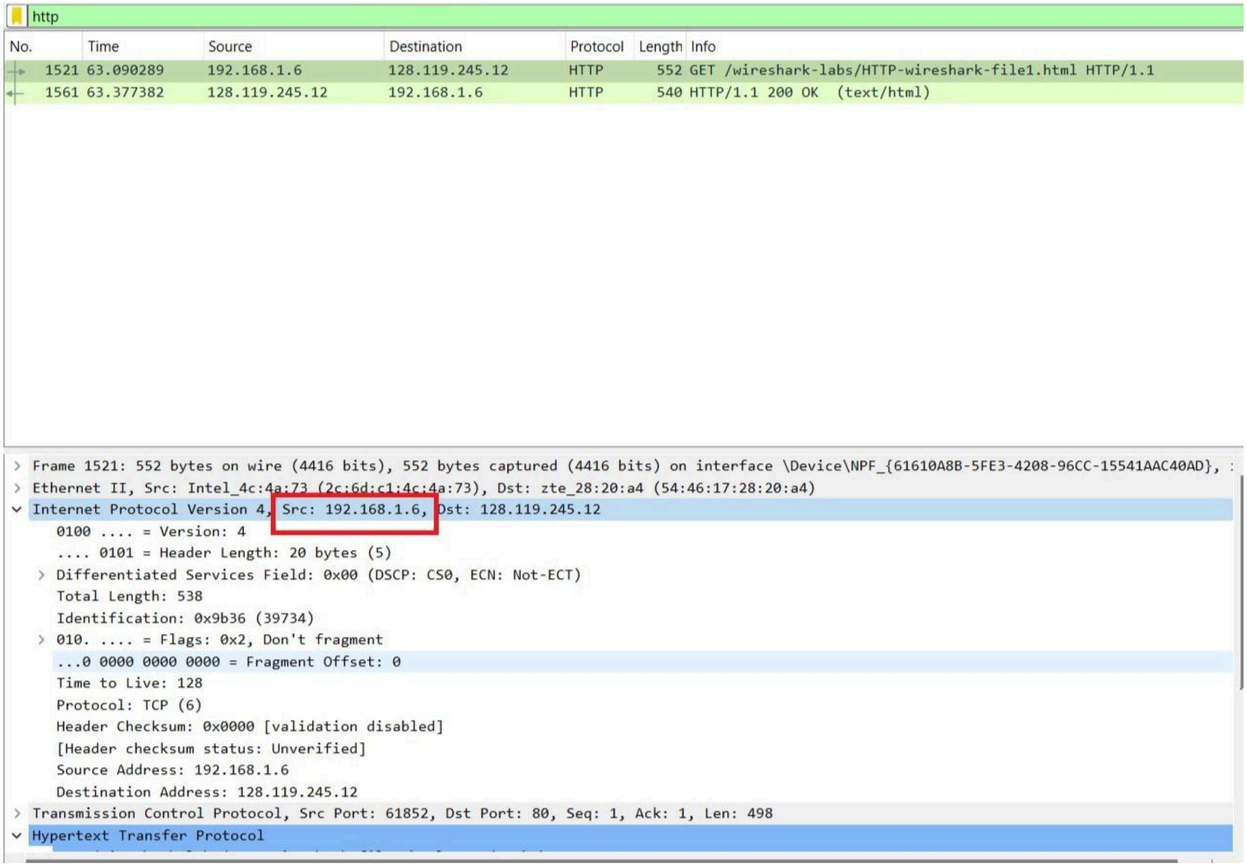
http

```
No.     Time        Source          Destination     Protocol  Length Info
  1521  63.090289   192.168.1.6     128.119.245.12  HTTP       552 GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
  1561  63.377382   128.119.245.12  192.168.1.6     HTTP       540 HTTP/1.1 200 OK  (text/html)
```

```
> Frame 1521: 552 bytes on wire (4416 bits), 552 bytes captured (4416 bits) on interface \Device\NPF_{61610A8B-5FE3-4208-96CC-15541AAC40AD}, id
> Ethernet II, Src: Intel_4c:4a:73 (2c:6d:c1:4c:4a:73), Dst: zte_28:20:a4 (54:46:17:28:20:a4)
> Internet Protocol Version 4, Src: 192.168.1.6, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 61852, Dst Port: 80, Seq: 1, Ack: 1, Len: 498
v Hypertext Transfer Protocol
  > GET /wireshark-labs/HTTP-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/122.0.0.0 Safari/537.36 Edg/122.0.0.0\r
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: en-US,en;q=0.9,en-IN;q=0.8\r\n
    \r\n
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html]
    [HTTP request 1/1]
    [Response in frame: 1561]
```

3. What is the IP address of your computer?

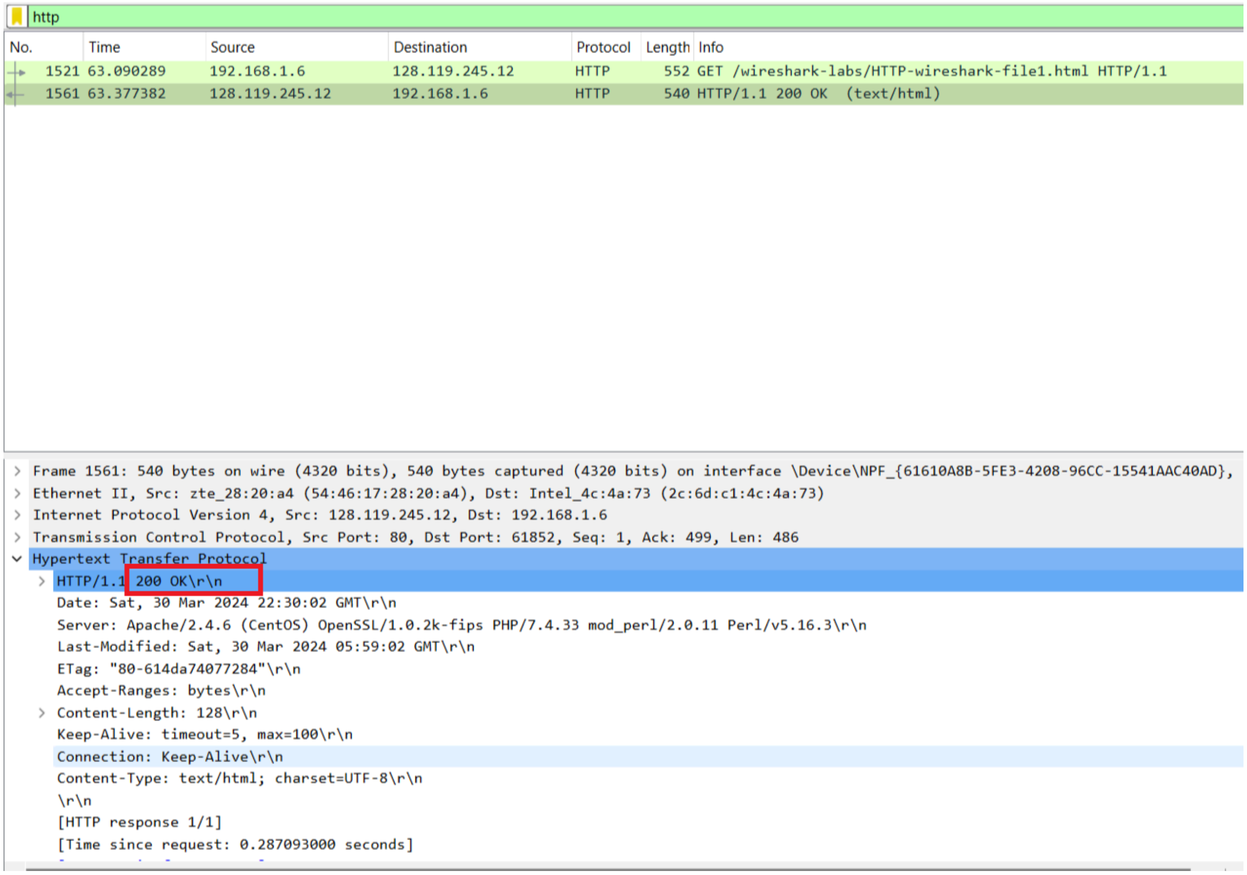
- 192.168.1.6



```
http
No.      Time          Source          Destination      Protocol  Length Info
   1521 63.090289    192.168.1.6     128.119.245.12   HTTP       552 GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
   1561 63.377382    128.119.245.12  192.168.1.6      HTTP       540 HTTP/1.1 200 OK  (text/html)
```

```
> Frame 1521: 552 bytes on wire (4416 bits), 552 bytes captured (4416 bits) on interface \Device\NPF_{61610A8B-5FE3-4208-96CC-15541AAC40AD}, :
> Ethernet II, Src: Intel_4c:4a:73 (2c:6d:c1:4c:4a:73), Dst: zte_28:20:a4 (54:46:17:28:20:a4)
v Internet Protocol Version 4, Src: 192.168.1.6, 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: 538
    Identification: 0x9b36 (39734)
  > 010. .... = Flags: 0x2, Don't fragment
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 128
    Protocol: TCP (6)
    Header Checksum: 0x0000 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.1.6
    Destination Address: 128.119.245.12
> Transmission Control Protocol, Src Port: 61852, Dst Port: 80, Seq: 1, Ack: 1, Len: 498
v Hypertext Transfer Protocol
```

4. What is the status code returned from the server to your browser?
- 200



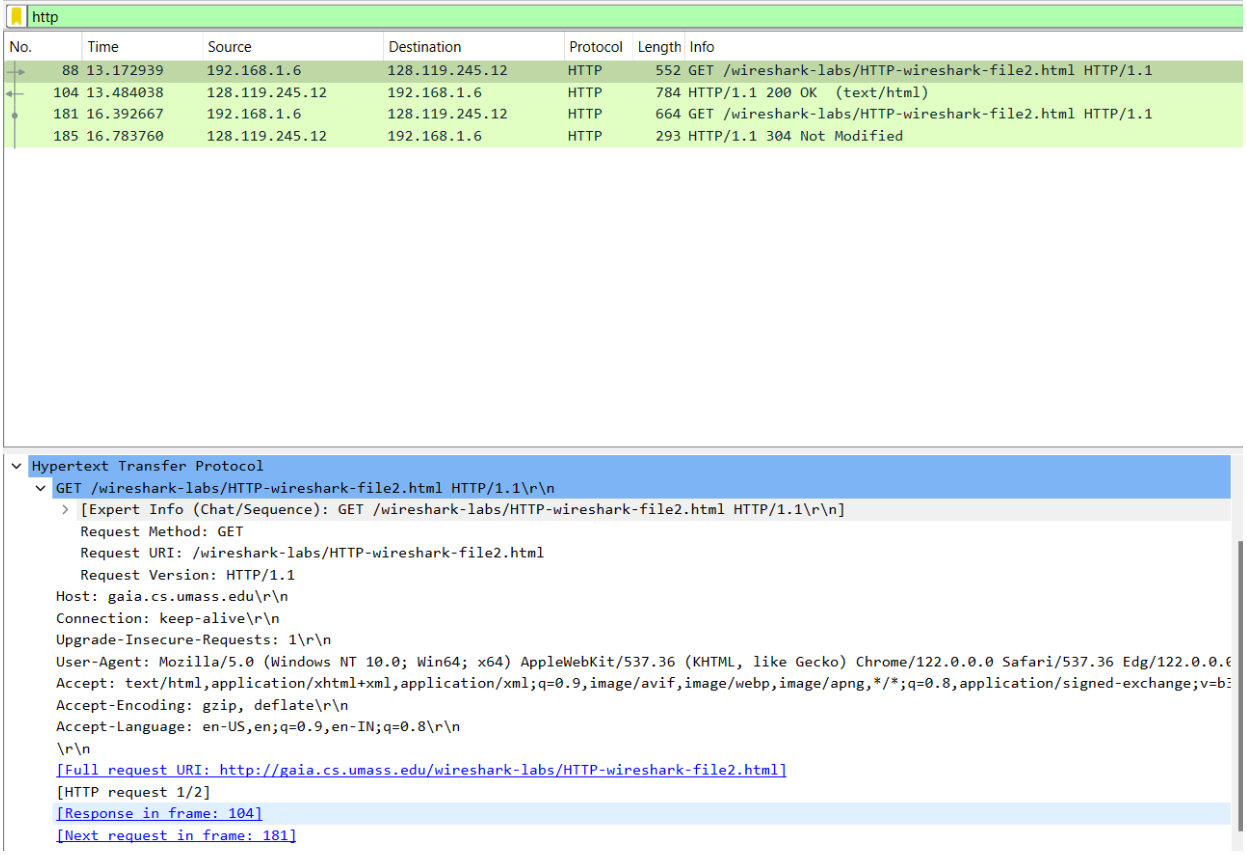
http

```
No.     Time        Source          Destination     Protocol Length Info
   1521 63.090289   192.168.1.6     128.119.245.12  HTTP        552 GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
   1561 63.377382   128.119.245.12  192.168.1.6     HTTP        540 HTTP/1.1 200 OK  (text/html)
```

```
> Frame 1561: 540 bytes on wire (4320 bits), 540 bytes captured (4320 bits) on interface \Device\NPF_{61610A8B-5FE3-4208-96CC-15541AAC40AD},
> Ethernet II, Src: zte_28:20:a4 (54:46:17:28:20:a4), Dst: Intel_4c:4a:73 (2c:6d:c1:4c:4a:73)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.6
> Transmission Control Protocol, Src Port: 80, Dst Port: 61852, Seq: 1, Ack: 499, Len: 486
v Hypertext Transfer Protocol
  > HTTP/1.1 200 OK\r\n
    Date: Sat, 30 Mar 2024 22:30:02 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.33 mod_perl/2.0.11 Perl/v5.16.3\r\n
    Last-Modified: Sat, 30 Mar 2024 05:59:02 GMT\r\n
    ETag: "80-614da74077284"\r\n
    Accept-Ranges: bytes\r\n
  > Content-Length: 128\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 1/1]
    [Time since request: 0.287093000 seconds]
```

5. Inspect the contents of the first HTTP GET request from your browser to the server. Do you see an “IF-MODIFIED-SINCE” line in the HTTP GET?

- There is no IF-MODIFIED-SINCE in the first HTTP GET

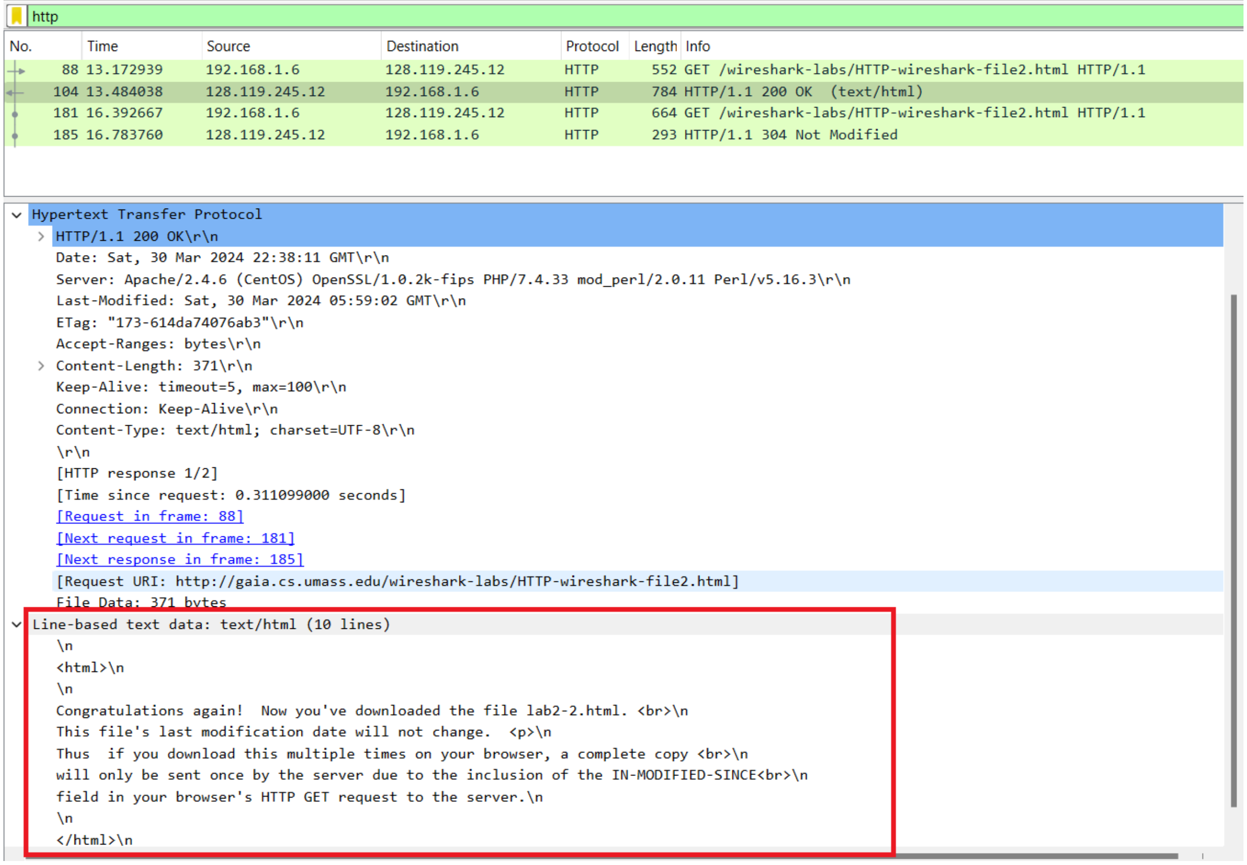


```
No.     Time        Source          Destination     Protocol Length Info
    88 13.172939   192.168.1.6     128.119.245.12  HTTP     552 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
   104 13.484038   128.119.245.12  192.168.1.6     HTTP     784 HTTP/1.1 200 OK  (text/html)
   181 16.392667   192.168.1.6     128.119.245.12  HTTP     664 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
   185 16.783760   128.119.245.12  192.168.1.6     HTTP     293 HTTP/1.1 304 Not Modified
```

```
Hypertext Transfer Protocol
  GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n
    [Expert Info (Chat/Sequence): GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n]
    Request Method: GET
    Request URI: /wireshark-labs/HTTP-wireshark-file2.html
    Request Version: HTTP/1.1
  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/122.0.0.0 Safari/537.36 Edg/122.0.0.
  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b
  Accept-Encoding: gzip, deflate\r\n
  Accept-Language: en-US,en;q=0.9,en-IN;q=0.8\r\n
  \r\n
  [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]
  [HTTP request 1/2]
  [Response in frame: 104]
  [Next request in frame: 181]
```

6. Inspect the contents of the server response. Did the server explicitly return the contents of the file? How can you tell?

- Yes, the server explicitly returns the contents of the file. It is captured in the packet details.

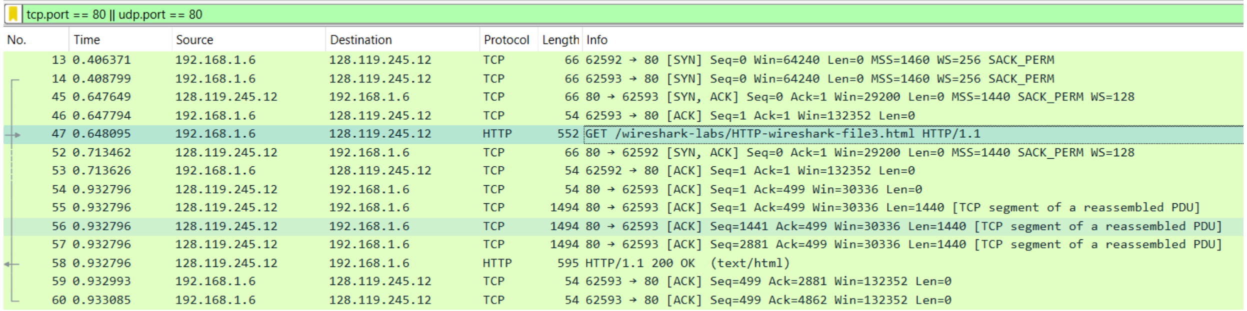


```
http
No.    Time        Source           Destination      Protocol Length Info
   88 13.172939   192.168.1.6      128.119.245.12   HTTP      552 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
  104 13.484038   128.119.245.12   192.168.1.6      HTTP      784 HTTP/1.1 200 OK  (text/html)
  181 16.392667   192.168.1.6      128.119.245.12   HTTP      664 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
  185 16.783760   128.119.245.12   192.168.1.6      HTTP      293 HTTP/1.1 304 Not Modified
```

```
v Hypertext Transfer Protocol
  > HTTP/1.1 200 OK\r\n
    Date: Sat, 30 Mar 2024 22:38:11 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.33 mod_perl/2.0.11 Perl/v5.16.3\r\n
    Last-Modified: Sat, 30 Mar 2024 05:59:02 GMT\r\n
    ETag: "173-614da74076ab3"\r\n
    Accept-Ranges: bytes\r\n
  > Content-Length: 371\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: 0.311099000 seconds]
    [Request in frame: 88]
    [Next request in frame: 181]
    [Next response in frame: 185]
    [Request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]
    File Data: 371 bytes
v Line-based text data: text/html (10 lines)
    \n
    <html>\n
    \n
    Congratulations again!  Now you've downloaded the file lab2-2.html. <br>\n
    This file's last modification date will not change.  <p>\n
    Thus  if you download this multiple times on your browser, a complete copy <br>\n
    will only be sent once by the server due to the inclusion of the IN-MODIFIED-SINCE<br>\n
    field in your browser's HTTP GET request to the server.\n
    \n
    </html>\n
```

7. 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?

- My browser sent 1 HTTP GET request. Packet number 47 contains the GET message.



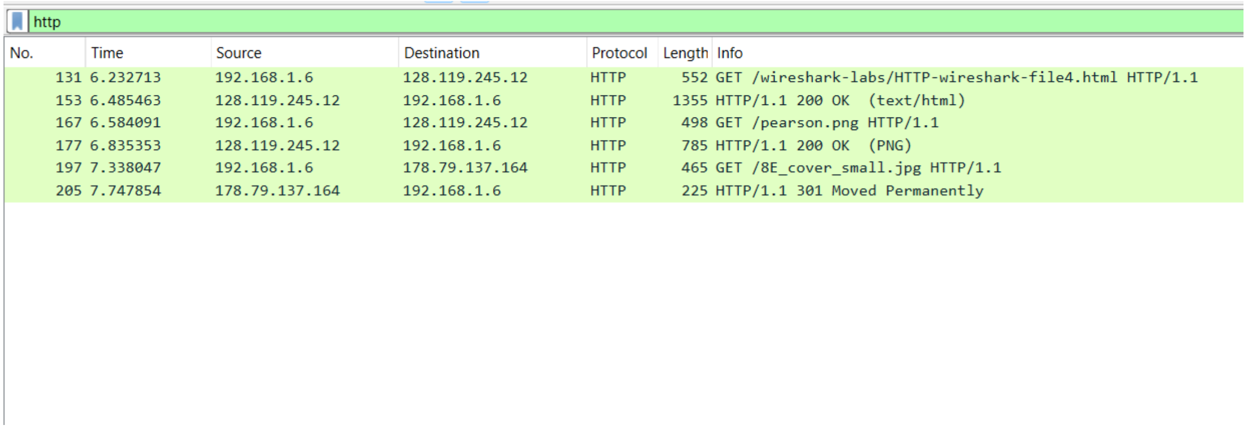
```
tcp.port == 80 || udp.port == 80
No.   Time       Source           Destination      Protocol Length Info
   13 0.406371   192.168.1.6      128.119.245.12   TCP        66 62592 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
   14 0.408799   192.168.1.6      128.119.245.12   TCP        66 62593 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
   45 0.647649   128.119.245.12   192.168.1.6      TCP        66 80 → 62593 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1440 SACK_PERM WS=128
   46 0.647794   192.168.1.6      128.119.245.12   TCP        54 62593 → 80 [ACK] Seq=1 Ack=1 Win=132352 Len=0
   47 0.648095   192.168.1.6      128.119.245.12   HTTP      552 GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
   52 0.713462   128.119.245.12   192.168.1.6      TCP        66 80 → 62592 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1440 SACK_PERM WS=128
   53 0.713626   192.168.1.6      128.119.245.12   TCP        54 62592 → 80 [ACK] Seq=1 Ack=1 Win=132352 Len=0
   54 0.932796   128.119.245.12   192.168.1.6      TCP        54 80 → 62593 [ACK] Seq=1 Ack=499 Win=30336 Len=0
   55 0.932796   128.119.245.12   192.168.1.6      TCP      1494 80 → 62593 [ACK] Seq=1 Ack=499 Win=30336 Len=1440 [TCP segment of a reassembled PDU]
   56 0.932796   128.119.245.12   192.168.1.6      TCP      1494 80 → 62593 [ACK] Seq=1441 Ack=499 Win=30336 Len=1440 [TCP segment of a reassembled PDU]
   57 0.932796   128.119.245.12   192.168.1.6      TCP      1494 80 → 62593 [ACK] Seq=2881 Ack=499 Win=30336 Len=1440 [TCP segment of a reassembled PDU]
   58 0.932796   128.119.245.12   192.168.1.6      HTTP      595 HTTP/1.1 200 OK  (text/html)
   59 0.932993   192.168.1.6      128.119.245.12   TCP        54 62593 → 80 [ACK] Seq=499 Ack=2881 Win=132352 Len=0
   60 0.933085   192.168.1.6      128.119.245.12   TCP        54 62593 → 80 [ACK] Seq=499 Ack=4862 Win=132352 Len=0
```

8. Which packet number in the trace contains the status code and phrase associated with the response to the HTTP GET request?

- Packet number **58** in the trace contains the status code and phrase associated with the response to the HTTP GET request

9. How many HTTP GET request messages did your browser send? To which Internet addresses were these GET requests sent?

- My browser sent three HTTP GET messages. Packet 131 was sent to 128.119.245.12. Packet 167 was sent to 128.119.245.12. Packet 197 was sent to 178.79.137.164.



http

No.	Time	Source	Destination	Protocol	Length	Info
131	6.232713	192.168.1.6	128.119.245.12	HTTP	552	GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
153	6.485463	128.119.245.12	192.168.1.6	HTTP	1355	HTTP/1.1 200 OK (text/html)
167	6.584091	192.168.1.6	128.119.245.12	HTTP	498	GET /pearson.png HTTP/1.1
177	6.835353	128.119.245.12	192.168.1.6	HTTP	785	HTTP/1.1 200 OK (PNG)
197	7.338047	192.168.1.6	178.79.137.164	HTTP	465	GET /8E_cover_small.jpg HTTP/1.1
205	7.747854	178.79.137.164	192.168.1.6	HTTP	225	HTTP/1.1 301 Moved Permanently

10. Can you tell whether your browser downloaded the two images serially, or whether they were downloaded from the two websites in parallel? Explain.

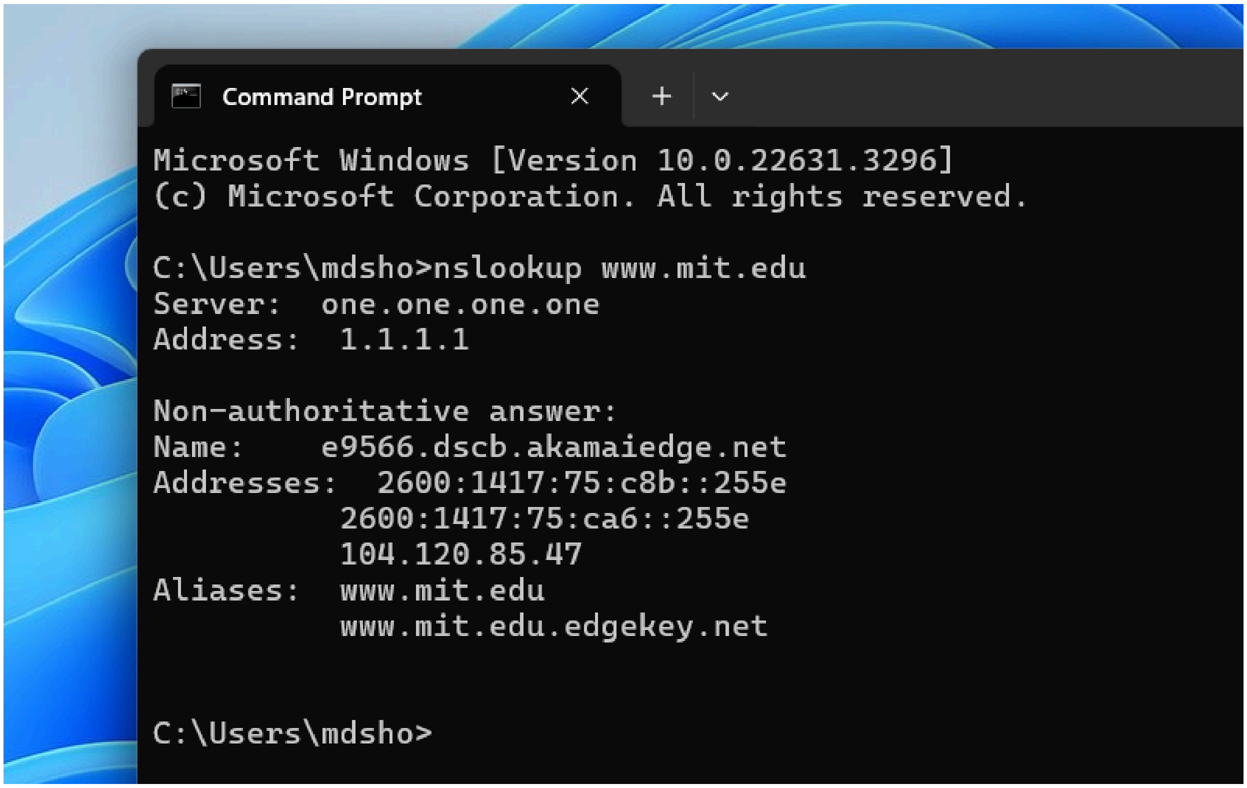
- The two images were downloaded serially because the first image was requested and sent before the second image was requested by the browser. The second image was only requested after the first image came back. The 2 images were transmitted over 2 TCP connections therefore they were downloaded serially.

DNS ASSIGNMENT

1. Run ‘nslookup www.mit.edu’ on your command prompt and what will be the name and IP address of the DNS server that provides the answer?

- The DNS server that provided the answer for the nslookup of www.mit.edu is:

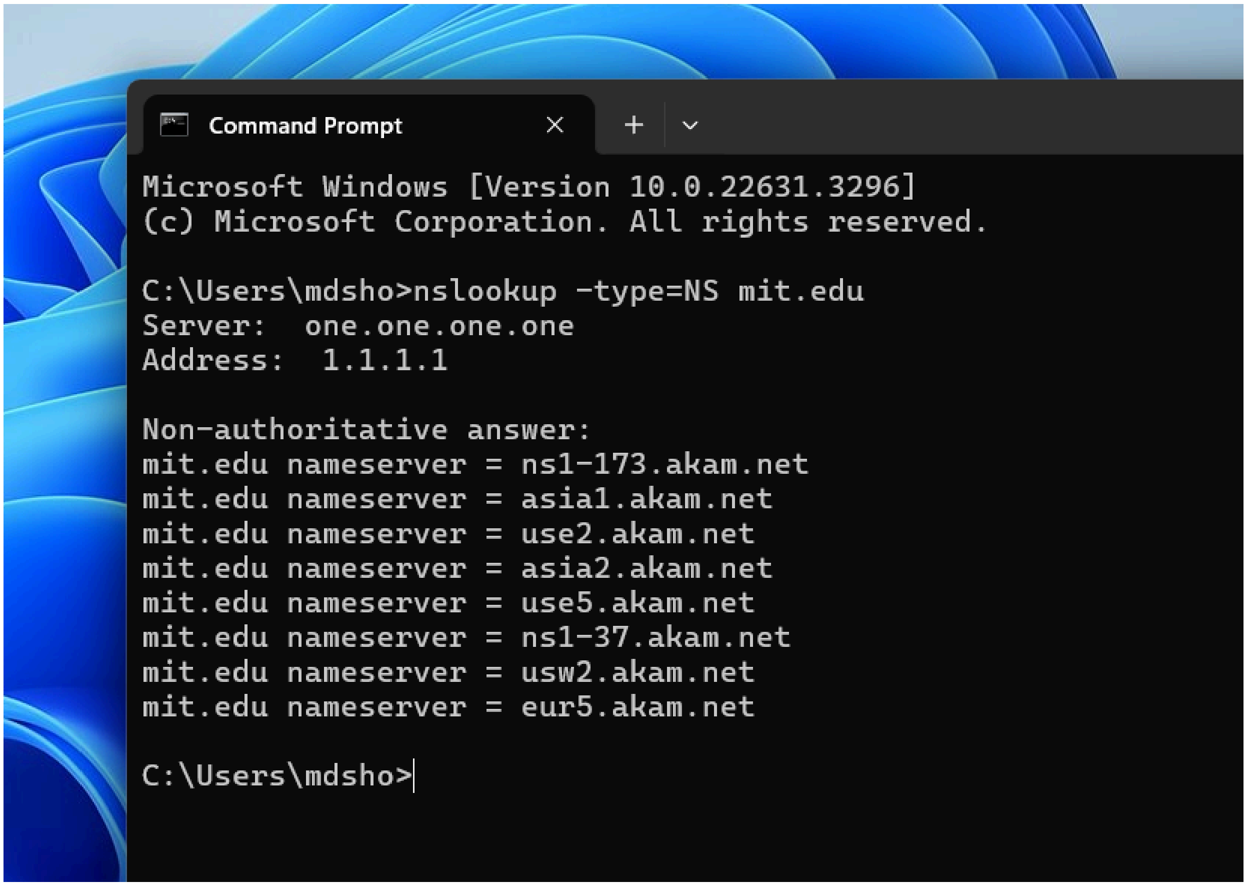
Name: one.one.one.one
Address: 1.1.1.1
It is a public DNS server operated by Cloudflare (1.1.1.1).



```
Microsoft Windows [Version 10.0.22631.3296]
(c) Microsoft Corporation. All rights reserved.

C:\Users\mdsho>nslookup www.mit.edu
Server:  one.one.one.one
Address:  1.1.1.1

Non-authoritative answer:
Name:    e9566.dscb.akamaiedge.net
Addresses:  2600:1417:75:c8b::255e
          2600:1417:75:ca6::255e
          104.120.85.47
Aliases:  www.mit.edu
          www.mit.edu.edgekey.net


C:\Users\mdsho>
```

2. Run ‘nslookup –type=NS mit.edu’ on your command prompt and what will be the host names of the authoritative DNS for mit.edu.

- The hostnames of the authoritative DNS servers for mit.edu are
  ns1-173.akam.net
  asia1.akam.net
  use2.akam.net
  asia2.akam.net
  use5.akam.net
  ns1-37.akam.net
  usw2.akam.net
  eur5.akam.net

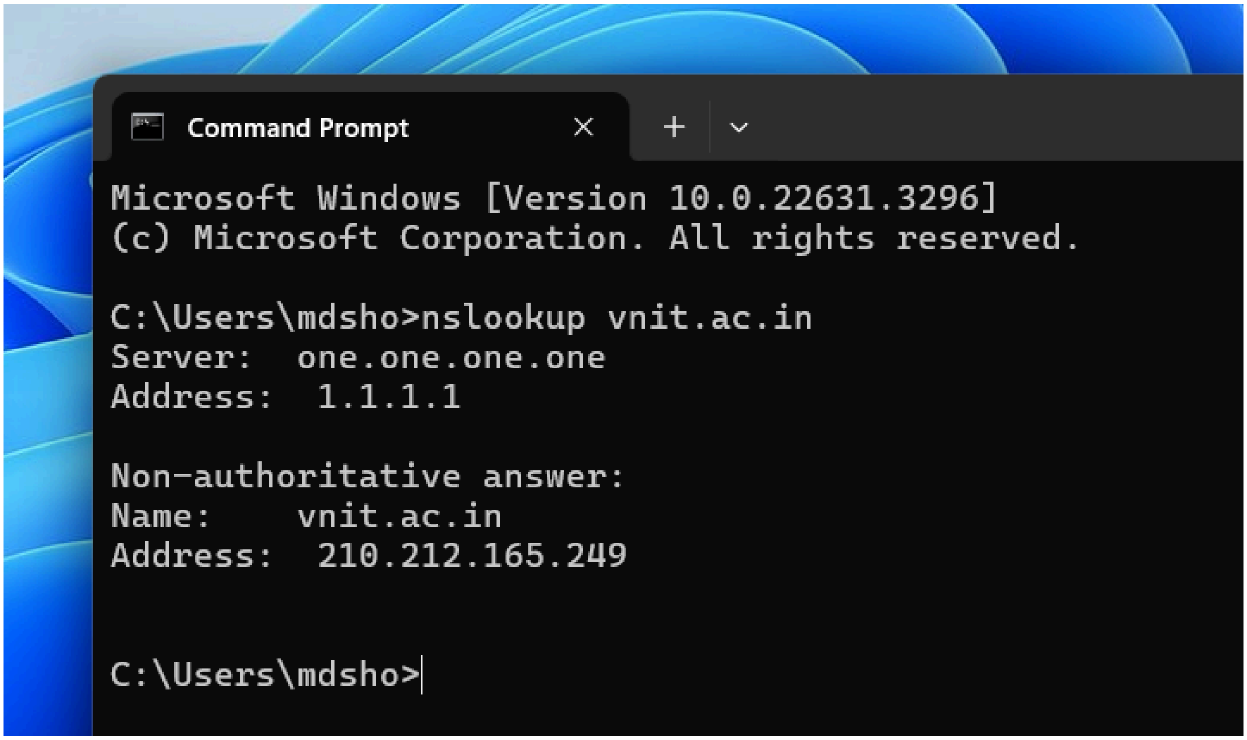


```
Microsoft Windows [Version 10.0.22631.3296]
(c) Microsoft Corporation. All rights reserved.

C:\Users\mdsho>nslookup -type=NS mit.edu
Server:  one.one.one.one
Address:  1.1.1.1

Non-authoritative answer:
mit.edu nameserver = ns1-173.akam.net
mit.edu nameserver = asia1.akam.net
mit.edu nameserver = use2.akam.net
mit.edu nameserver = asia2.akam.net
mit.edu nameserver = use5.akam.net
mit.edu nameserver = ns1-37.akam.net
mit.edu nameserver = usw2.akam.net
mit.edu nameserver = eur5.akam.net

C:\Users\mdsho>
```

.

3. Run nslookup to obtain the IP address of a Web server in Asia. What is the IP address of that server?

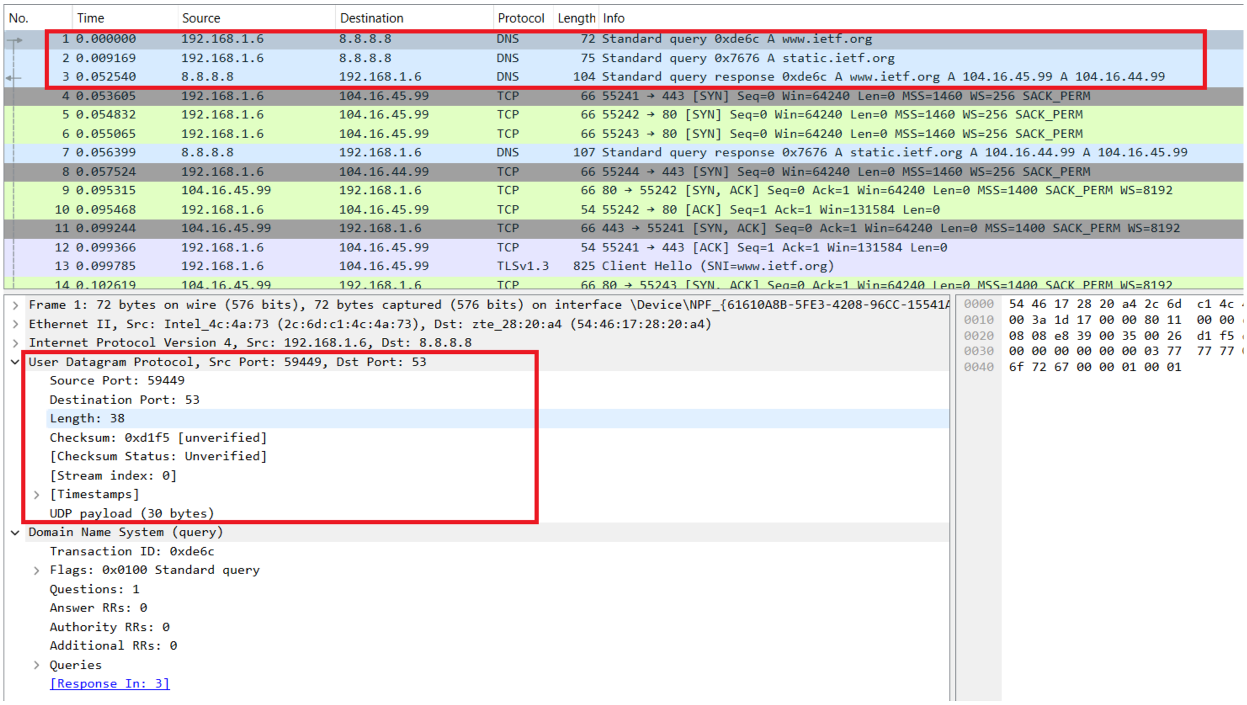
- I queried the webpage for the VNIT Nagpur. The IP address of the server is 210.212.165.249.



```
Microsoft Windows [Version 10.0.22631.3296]
(c) Microsoft Corporation. All rights reserved.

C:\Users\mdsho>nslookup vnit.ac.in
Server:  one.one.one.one
Address:  1.1.1.1

Non-authoritative answer:
Name:    vnit.ac.in
Address:  210.212.165.249


C:\Users\mdsho>
```

4. Locate the DNS query and response messages. Are they sent over UDP or TCP?

- The DNS query and response messages are sent over UDP.



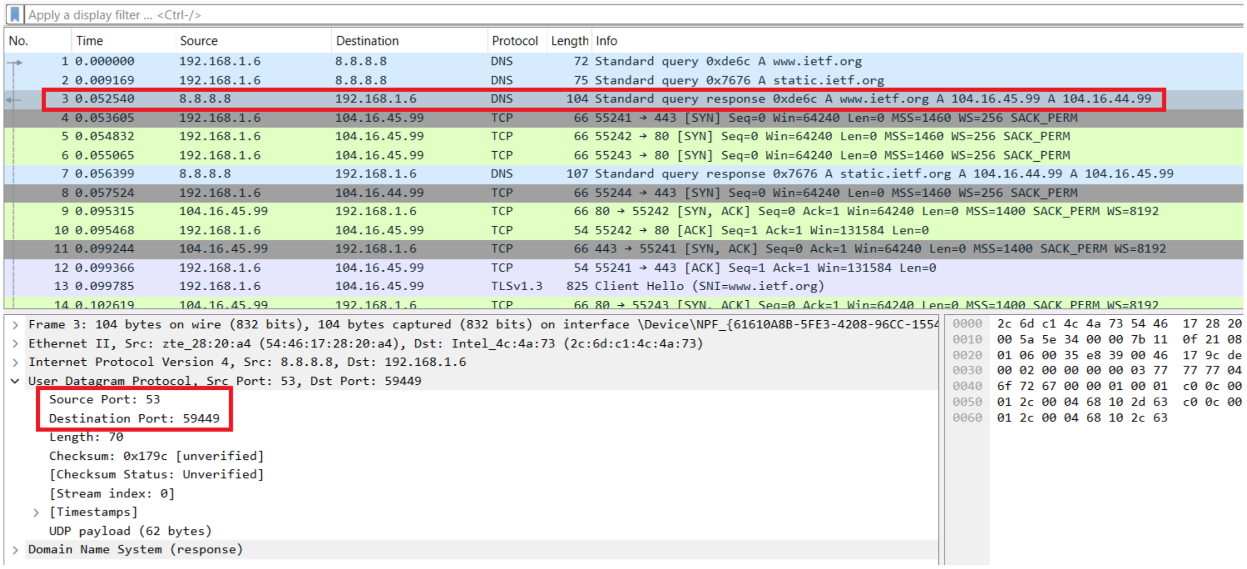
No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.1.6	8.8.8.8	DNS	72	Standard query 0xde6c A www.ietf.org
2	0.009169	192.168.1.6	8.8.8.8	DNS	75	Standard query 0x7676 A static.ietf.org
3	0.052540	8.8.8.8	192.168.1.6	DNS	104	Standard query response 0xde6c A www.ietf.org A 104.16.45.99 A 104.16.44.99
4	0.053605	192.168.1.6	104.16.45.99	TCP	66	55241 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
5	0.054832	192.168.1.6	104.16.45.99	TCP	66	55242 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
6	0.055065	192.168.1.6	104.16.45.99	TCP	66	55243 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
7	0.056399	8.8.8.8	192.168.1.6	DNS	107	Standard query response 0x7676 A static.ietf.org A 104.16.44.99 A 104.16.45.99
8	0.057524	192.168.1.6	104.16.44.99	TCP	66	55244 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
9	0.095315	104.16.45.99	192.168.1.6	TCP	66	80 → 55242 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1400 SACK_PERM WS=8192
10	0.095468	192.168.1.6	104.16.45.99	TCP	54	55242 → 80 [ACK] Seq=1 Ack=1 Win=131584 Len=0
11	0.099244	104.16.45.99	192.168.1.6	TCP	66	443 → 55241 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1400 SACK_PERM WS=8192
12	0.099366	192.168.1.6	104.16.45.99	TCP	54	55241 → 443 [ACK] Seq=1 Ack=1 Win=131584 Len=0
13	0.099785	192.168.1.6	104.16.45.99	TLSv1.3	825	Client Hello (SNI=www.ietf.org)
14	0.102619	104.16.45.99	192.168.1.6	TCP	66	80 → 55243 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1400 SACK_PERM WS=8192

```
> Frame 1: 72 bytes on wire (576 bits), 72 bytes captured (576 bits) on interface \Device\NPF_{61610A8B-5FE3-4208-96CC-15541A
> Ethernet II, Src: Intel_4c:4a:73 (2c:6d:c1:4c:4a:73), Dst: zte_28:20:a4 (54:46:17:28:20:a4)
> Internet Protocol Version 4, Src: 192.168.1.6, Dst: 8.8.8.8
v User Datagram Protocol, Src Port: 59449, Dst Port: 53
    Source Port: 59449
    Destination Port: 53
    Length: 38
    Checksum: 0xd1f5 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 0]
  > [Timestamps]
    UDP payload (30 bytes)
v Domain Name System (query)
    Transaction ID: 0xde6c
  > Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  > Queries
    [Response In: 3]
```

```
0000  54 46 17 28 20 a4 2c 6d  c1 4c
0010  00 3a 1d 17 00 00 80 11  00 00
0020  08 08 e8 39 00 35 00 26  d1 f5
0030  00 00 00 00 00 00 03 77  77 77
0040  6f 72 67 00 00 01 00 01
```

5. What is the destination port for the DNS query message? What is the source port
   of the DNS response message?

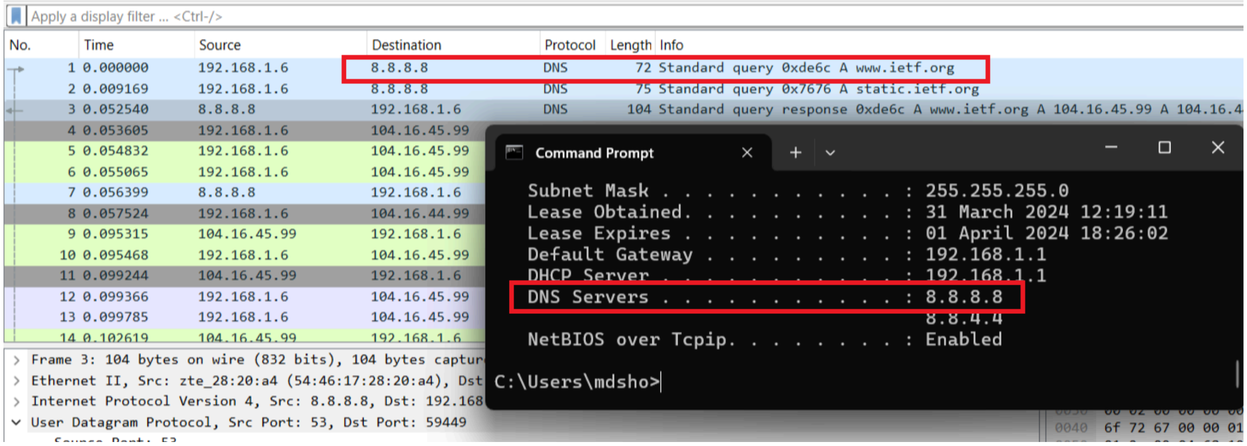
- The destination port for the DNS query message is 53
  The source port of the DNS response message is 53.



```
Apply a display filter ... <Ctrl-/>

No.     Time        Source          Destination     Protocol  Length Info
      1 0.000000    192.168.1.6     8.8.8.8         DNS          72 Standard query 0xde6c A www.ietf.org
      2 0.009169    192.168.1.6     8.8.8.8         DNS          75 Standard query 0x7676 A static.ietf.org
      3 0.052540    8.8.8.8         192.168.1.6     DNS         104 Standard query response 0xde6c A www.ietf.org A 104.16.45.99 A 104.16.44.99
      4 0.053605    192.168.1.6     104.16.45.99    TCP          66 55241 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
      5 0.054832    192.168.1.6     104.16.45.99    TCP          66 55242 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
      6 0.055065    192.168.1.6     104.16.45.99    TCP          66 55243 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
      7 0.056399    8.8.8.8         192.168.1.6     DNS         107 Standard query response 0x7676 A static.ietf.org A 104.16.44.99 A 104.16.45.99
      8 0.057524    192.168.1.6     104.16.44.99    TCP          66 55244 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
      9 0.095315    104.16.45.99    192.168.1.6     TCP          66 80 → 55242 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1400 SACK_PERM WS=8192
     10 0.095468    192.168.1.6     104.16.45.99    TCP          54 55242 → 80 [ACK] Seq=1 Ack=1 Win=131584 Len=0
     11 0.099244    104.16.45.99    192.168.1.6     TCP          66 443 → 55241 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1400 SACK_PERM WS=8192
     12 0.099366    192.168.1.6     104.16.45.99    TCP          54 55241 → 443 [ACK] Seq=1 Ack=1 Win=131584 Len=0
     13 0.099785    192.168.1.6     104.16.45.99    TLSv1.3     825 Client Hello (SNI=www.ietf.org)
     14 0.102619    104.16.45.99    192.168.1.6     TCP          66 80 → 55243 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1400 SACK_PERM WS=8192

> Frame 3: 104 bytes on wire (832 bits), 104 bytes captured (832 bits) on interface \Device\NPF_{61610A8B-5FE3-4208-96CC-1554
> Ethernet II, Src: zte_28:20:a4 (54:46:17:28:20:a4), Dst: Intel_4c:4a:73 (2c:6d:c1:4c:4a:73)
> Internet Protocol Version 4, Src: 8.8.8.8, Dst: 192.168.1.6
v User Datagram Protocol, Src Port: 53, Dst Port: 59449
    Source Port: 53
    Destination Port: 59449
    Length: 70
    Checksum: 0x179c [unverified]
    [Checksum Status: Unverified]
    [Stream index: 0]
  > [Timestamps]
    UDP payload (62 bytes)
> Domain Name System (response)

0000  2c 6d c1 4c 4a 73 54 46  17 28 20
0010  00 5a 5e 34 00 00 7b 11  0f 21 08
0020  01 06 00 35 e8 39 00 46  17 9c de
0030  00 02 00 00 00 00 03 77  77 77 04
0040  6f 72 67 00 00 01 00 01  c0 0c 00
0050  01 2c 00 04 68 10 2d 63  c0 0c 00
0060  01 2c 00 04 68 10 2c 63
```

6. To what IP address is the DNS query message sent? Use ipconfig to determine
   the IP address of your local DNS server. Are these two IP addresses the same?

- The DNS query was sent to IP address 8.8.8.8. Yes it is the same IP address as that of my local DNS server.



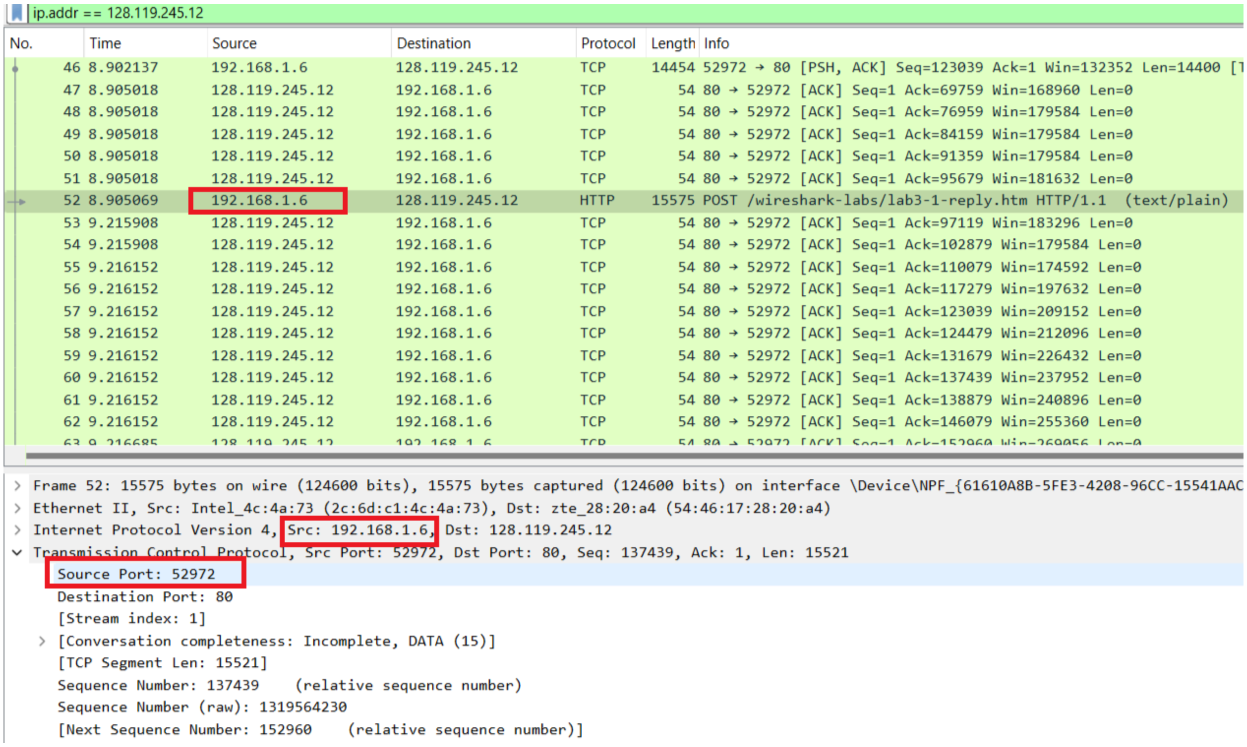
```
Apply a display filter ... <Ctrl-/>

No.     Time        Source          Destination     Protocol  Length Info
      1 0.000000    192.168.1.6     8.8.8.8         DNS          72 Standard query 0xde6c A www.ietf.org
      2 0.009169    192.168.1.6     8.8.8.8         DNS          75 Standard query 0x7676 A static.ietf.org
      3 0.052540    8.8.8.8         192.168.1.6     DNS         104 Standard query response 0xde6c A www.ietf.org A 104.16.45.99 A 104.16.4
      4 0.053605    192.168.1.6     104.16.45.99
      5 0.054832    192.168.1.6     104.16.45.99
      6 0.055065    192.168.1.6     104.16.45.99
      7 0.056399    8.8.8.8         192.168.1.6
      8 0.057524    192.168.1.6     104.16.44.99
      9 0.095315    104.16.45.99    192.168.1.6
     10 0.095468    192.168.1.6     104.16.45.99
     11 0.099244    104.16.45.99    192.168.1.6
     12 0.099366    192.168.1.6     104.16.45.99
     13 0.099785    192.168.1.6     104.16.45.99
     14 0.102619    104.16.45.99    192.168.1.6

> Frame 3: 104 bytes on wire (832 bits), 104 bytes captur
> Ethernet II, Src: zte_28:20:a4 (54:46:17:28:20:a4), Dst
> Internet Protocol Version 4, Src: 8.8.8.8, Dst: 192.168
v User Datagram Protocol, Src Port: 53, Dst Port: 59449

0040  6f 72 67 00 00 01
```

```
   Subnet Mask . . . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . . . : 31 March 2024 12:19:11
   Lease Expires . . . . . . . . . . . . : 01 April 2024 18:26:02
   Default Gateway . . . . . . . . . . . : 192.168.1.1
   DHCP Server . . . . . . . . . . . . . : 192.168.1.1
   DNS Servers . . . . . . . . . . . . . : 8.8.8.8
                                           8.8.4.4
   NetBIOS over Tcpip. . . . . . . . . . : Enabled

C:\Users\mdsho>
```

TCP ASSIGNMENT

1. What is the IP address and TCP port number used by the client computer (source) that is transferring the file to gaia.cs.umass.edu?

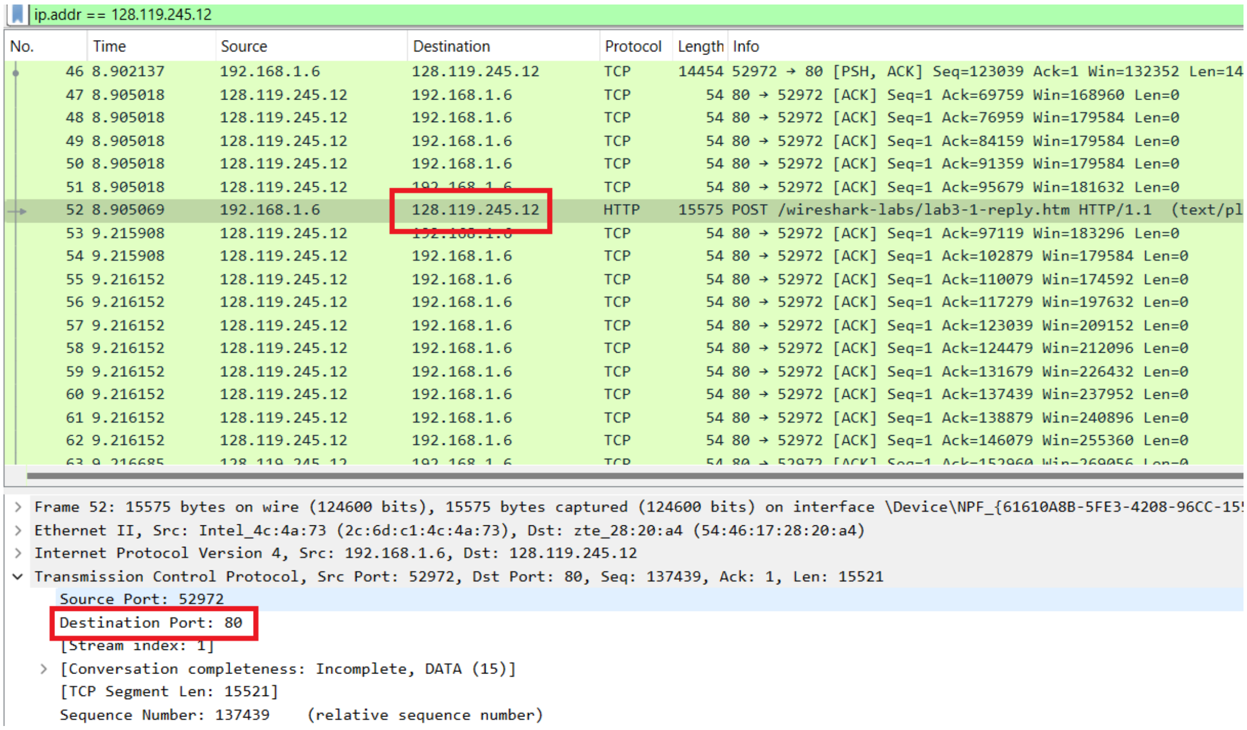
- The IP address is 192.168.1.6 and the TCP port number is 52972.



```
ip.addr == 128.119.245.12

No.  Time        Source           Destination      Protocol  Length  Info
  46 8.902137    192.168.1.6      128.119.245.12   TCP       14454 52972 → 80 [PSH, ACK] Seq=123039 Ack=1 Win=132352 Len=14400 [T
  47 8.905018    128.119.245.12   192.168.1.6      TCP          54 80 → 52972 [ACK] Seq=1 Ack=69759 Win=168960 Len=0
  48 8.905018    128.119.245.12   192.168.1.6      TCP          54 80 → 52972 [ACK] Seq=1 Ack=76959 Win=179584 Len=0
  49 8.905018    128.119.245.12   192.168.1.6      TCP          54 80 → 52972 [ACK] Seq=1 Ack=84159 Win=179584 Len=0
  50 8.905018    128.119.245.12   192.168.1.6      TCP          54 80 → 52972 [ACK] Seq=1 Ack=91359 Win=179584 Len=0
  51 8.905018    128.119.245.12   192.168.1.6      TCP          54 80 → 52972 [ACK] Seq=1 Ack=95679 Win=181632 Len=0
  52 8.905069    192.168.1.6      128.119.245.12   HTTP      15575 POST /wireshark-labs/lab3-1-reply.htm HTTP/1.1  (text/plain)
  53 9.215908    128.119.245.12   192.168.1.6      TCP          54 80 → 52972 [ACK] Seq=1 Ack=97119 Win=183296 Len=0
  54 9.215908    128.119.245.12   192.168.1.6      TCP          54 80 → 52972 [ACK] Seq=1 Ack=102879 Win=179584 Len=0
  55 9.216152    128.119.245.12   192.168.1.6      TCP          54 80 → 52972 [ACK] Seq=1 Ack=110079 Win=174592 Len=0
  56 9.216152    128.119.245.12   192.168.1.6      TCP          54 80 → 52972 [ACK] Seq=1 Ack=117279 Win=197632 Len=0
  57 9.216152    128.119.245.12   192.168.1.6      TCP          54 80 → 52972 [ACK] Seq=1 Ack=123039 Win=209152 Len=0
  58 9.216152    128.119.245.12   192.168.1.6      TCP          54 80 → 52972 [ACK] Seq=1 Ack=124479 Win=212096 Len=0
  59 9.216152    128.119.245.12   192.168.1.6      TCP          54 80 → 52972 [ACK] Seq=1 Ack=131679 Win=226432 Len=0
  60 9.216152    128.119.245.12   192.168.1.6      TCP          54 80 → 52972 [ACK] Seq=1 Ack=137439 Win=237952 Len=0
  61 9.216152    128.119.245.12   192.168.1.6      TCP          54 80 → 52972 [ACK] Seq=1 Ack=138879 Win=240896 Len=0
  62 9.216152    128.119.245.12   192.168.1.6      TCP          54 80 → 52972 [ACK] Seq=1 Ack=146079 Win=255360 Len=0
  63 9.216685    128.119.245.12   192.168.1.6      TCP          54 80 → 52972 [ACK] Seq=1 Ack=152960 Win=269056 Len=0

> Frame 52: 15575 bytes on wire (124600 bits), 15575 bytes captured (124600 bits) on interface \Device\NPF_{61610A8B-5FE3-4208-96CC-15541AAC
> Ethernet II, Src: Intel_4c:4a:73 (2c:6d:c1:4c:4a:73), Dst: zte_28:20:a4 (54:46:17:28:20:a4)
> Internet Protocol Version 4, Src: 192.168.1.6, Dst: 128.119.245.12
v Transmission Control Protocol, Src Port: 52972, Dst Port: 80, Seq: 137439, Ack: 1, Len: 15521
    Source Port: 52972
    Destination Port: 80
    [Stream index: 1]
  > [Conversation completeness: Incomplete, DATA (15)]
    [TCP Segment Len: 15521]
    Sequence Number: 137439    (relative sequence number)
    Sequence Number (raw): 1319564230
    [Next Sequence Number: 152960    (relative sequence number)]
```

2. What is the IP address of gaia.cs.umass.edu? On what port number is it sending and receiving TCP segments for this connection?

- The IP address of gaia.cs.umass.edu is 128.119.245.12. It is sending and receiving TCP segments on port number 80.



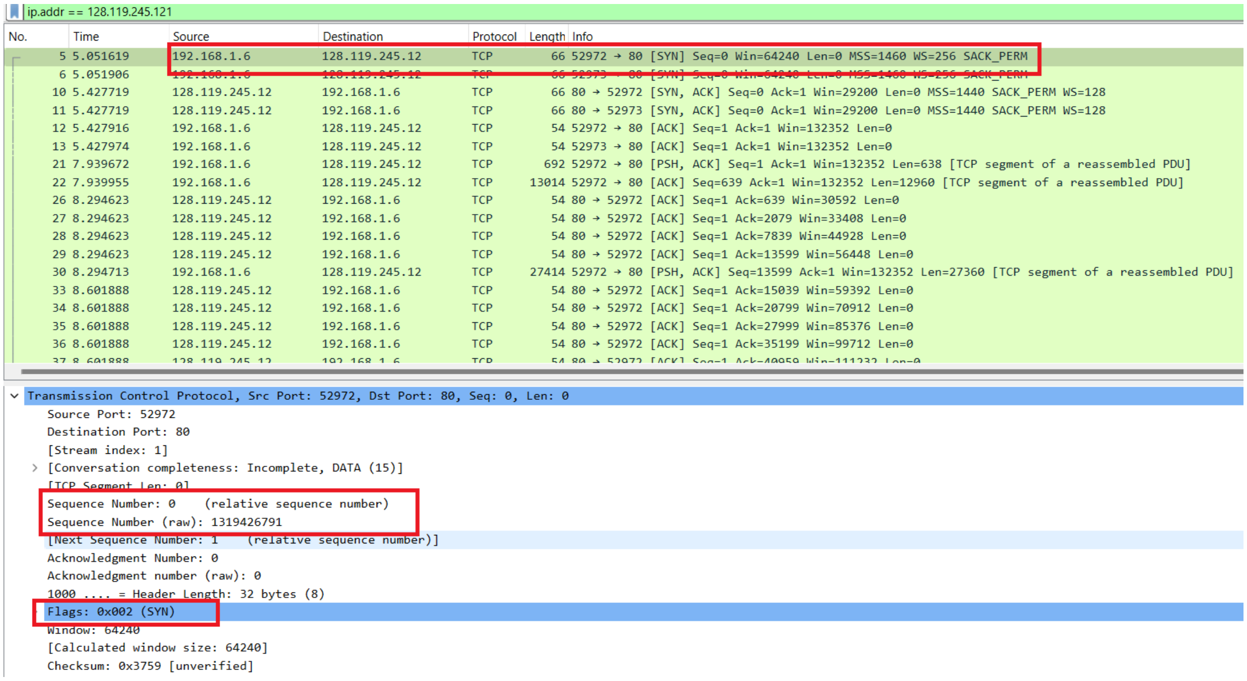
ip.addr == 128.119.245.12

```
No.  Time       Source          Destination     Protocol Length Info
  46 8.902137   192.168.1.6     128.119.245.12  TCP      14454 52972 → 80 [PSH, ACK] Seq=123039 Ack=1 Win=132352 Len=14
  47 8.905018   128.119.245.12  192.168.1.6     TCP         54 80 → 52972 [ACK] Seq=1 Ack=69759 Win=168960 Len=0
  48 8.905018   128.119.245.12  192.168.1.6     TCP         54 80 → 52972 [ACK] Seq=1 Ack=76959 Win=179584 Len=0
  49 8.905018   128.119.245.12  192.168.1.6     TCP         54 80 → 52972 [ACK] Seq=1 Ack=84159 Win=179584 Len=0
  50 8.905018   128.119.245.12  192.168.1.6     TCP         54 80 → 52972 [ACK] Seq=1 Ack=91359 Win=179584 Len=0
  51 8.905018   128.119.245.12  192.168.1.6     TCP         54 80 → 52972 [ACK] Seq=1 Ack=95679 Win=181632 Len=0
  52 8.905069   192.168.1.6     128.119.245.12  HTTP     15575 POST /wireshark-labs/lab3-1-reply.htm HTTP/1.1  (text/pl
  53 9.215908   128.119.245.12  192.168.1.6     TCP         54 80 → 52972 [ACK] Seq=1 Ack=97119 Win=183296 Len=0
  54 9.215908   128.119.245.12  192.168.1.6     TCP         54 80 → 52972 [ACK] Seq=1 Ack=102879 Win=179584 Len=0
  55 9.216152   128.119.245.12  192.168.1.6     TCP         54 80 → 52972 [ACK] Seq=1 Ack=110079 Win=174592 Len=0
  56 9.216152   128.119.245.12  192.168.1.6     TCP         54 80 → 52972 [ACK] Seq=1 Ack=117279 Win=197632 Len=0
  57 9.216152   128.119.245.12  192.168.1.6     TCP         54 80 → 52972 [ACK] Seq=1 Ack=123039 Win=209152 Len=0
  58 9.216152   128.119.245.12  192.168.1.6     TCP         54 80 → 52972 [ACK] Seq=1 Ack=124479 Win=212096 Len=0
  59 9.216152   128.119.245.12  192.168.1.6     TCP         54 80 → 52972 [ACK] Seq=1 Ack=131679 Win=226432 Len=0
  60 9.216152   128.119.245.12  192.168.1.6     TCP         54 80 → 52972 [ACK] Seq=1 Ack=137439 Win=237952 Len=0
  61 9.216152   128.119.245.12  192.168.1.6     TCP         54 80 → 52972 [ACK] Seq=1 Ack=138879 Win=240896 Len=0
  62 9.216152   128.119.245.12  192.168.1.6     TCP         54 80 → 52972 [ACK] Seq=1 Ack=146079 Win=255360 Len=0
  63 9.216685   128.119.245.12  192.168.1.6     TCP         54 80 → 52972 [ACK] Seq=1 Ack=152960 Win=269056 Len=0
```

```
> Frame 52: 15575 bytes on wire (124600 bits), 15575 bytes captured (124600 bits) on interface \Device\NPF_{61610A8B-5FE3-4208-96CC-15
> Ethernet II, Src: Intel_4c:4a:73 (2c:6d:c1:4c:4a:73), Dst: zte_28:20:a4 (54:46:17:28:20:a4)
> Internet Protocol Version 4, Src: 192.168.1.6, Dst: 128.119.245.12
v Transmission Control Protocol, Src Port: 52972, Dst Port: 80, Seq: 137439, Ack: 1, Len: 15521
    Source Port: 52972
    Destination Port: 80
    [Stream index: 1]
  > [Conversation completeness: Incomplete, DATA (15)]
    [TCP Segment Len: 15521]
    Sequence Number: 137439    (relative sequence number)
```

3. 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?

- The sequence number of the TCP SYN segment that is used to initiate the TCP connection is 1319426791.
  In this segment, the SYN flag is set to 1 and it indicates that this segment is a SYN segment.



```
ip.addr == 128.119.245.121

No.   Time        Source           Destination      Protocol  Length Info
    5 5.051619    192.168.1.6      128.119.245.12   TCP         66 52972 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
    6 5.051906    192.168.1.6      128.119.245.12   TCP         66 52973 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
   10 5.427719    128.119.245.12   192.168.1.6      TCP         66 80 → 52972 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1440 SACK_PERM WS=128
   11 5.427719    128.119.245.12   192.168.1.6      TCP         66 80 → 52973 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1440 SACK_PERM WS=128
   12 5.427916    192.168.1.6      128.119.245.12   TCP         54 52972 → 80 [ACK] Seq=1 Ack=1 Win=132352 Len=0
   13 5.427974    192.168.1.6      128.119.245.12   TCP         54 52973 → 80 [ACK] Seq=1 Ack=1 Win=132352 Len=0
   21 7.939672    192.168.1.6      128.119.245.12   TCP        692 52972 → 80 [PSH, ACK] Seq=1 Ack=1 Win=132352 Len=638 [TCP segment of a reassembled PDU]
   22 7.939955    192.168.1.6      128.119.245.12   TCP      13014 52972 → 80 [ACK] Seq=639 Ack=1 Win=132352 Len=12960 [TCP segment of a reassembled PDU]
   26 8.294623    128.119.245.12   192.168.1.6      TCP         54 80 → 52972 [ACK] Seq=1 Ack=639 Win=30592 Len=0
   27 8.294623    128.119.245.12   192.168.1.6      TCP         54 80 → 52972 [ACK] Seq=1 Ack=2079 Win=33408 Len=0
   28 8.294623    128.119.245.12   192.168.1.6      TCP         54 80 → 52972 [ACK] Seq=1 Ack=7839 Win=44928 Len=0
   29 8.294623    128.119.245.12   192.168.1.6      TCP         54 80 → 52972 [ACK] Seq=1 Ack=13599 Win=56448 Len=0
   30 8.294713    192.168.1.6      128.119.245.12   TCP      27414 52972 → 80 [PSH, ACK] Seq=13599 Ack=1 Win=132352 Len=27360 [TCP segment of a reassembled PDU]
   33 8.601888    128.119.245.12   192.168.1.6      TCP         54 80 → 52972 [ACK] Seq=1 Ack=15039 Win=59392 Len=0
   34 8.601888    128.119.245.12   192.168.1.6      TCP         54 80 → 52972 [ACK] Seq=1 Ack=20799 Win=70912 Len=0
   35 8.601888    128.119.245.12   192.168.1.6      TCP         54 80 → 52972 [ACK] Seq=1 Ack=27999 Win=85376 Len=0
   36 8.601888    128.119.245.12   192.168.1.6      TCP         54 80 → 52972 [ACK] Seq=1 Ack=35199 Win=99712 Len=0
   37 8.601888    128.119.245.12   192.168.1.6      TCP         54 80 → 52972 [ACK] Seq=1 Ack=40959 Win=111232 Len=0

v Transmission Control Protocol, Src Port: 52972, Dst Port: 80, Seq: 0, Len: 0
    Source Port: 52972
    Destination Port: 80
    [Stream index: 1]
  > [Conversation completeness: Incomplete, DATA (15)]
    [TCP Segment Len: 0]
    Sequence Number: 0    (relative sequence number)
    Sequence Number (raw): 1319426791
    [Next Sequence Number: 1    (relative sequence number)]
    Acknowledgment Number: 0
    Acknowledgment number (raw): 0
    1000 .... = Header Length: 32 bytes (8)
    Flags: 0x002 (SYN)
    Window: 64240
    [Calculated window size: 64240]
    Checksum: 0x3759 [unverified]
```

4. Answer the following:
    a. What is the sequence number of the SYNACK segment sent by gaia.cs.umass.edu to the client computer in reply to the SYN?

    - The sequence number of the SYNACK segment sent by gaia.cs.umass.edu to the client computer is 4231772314.

    b. What is the value of the Acknowledgement field in the SYNACK segment?

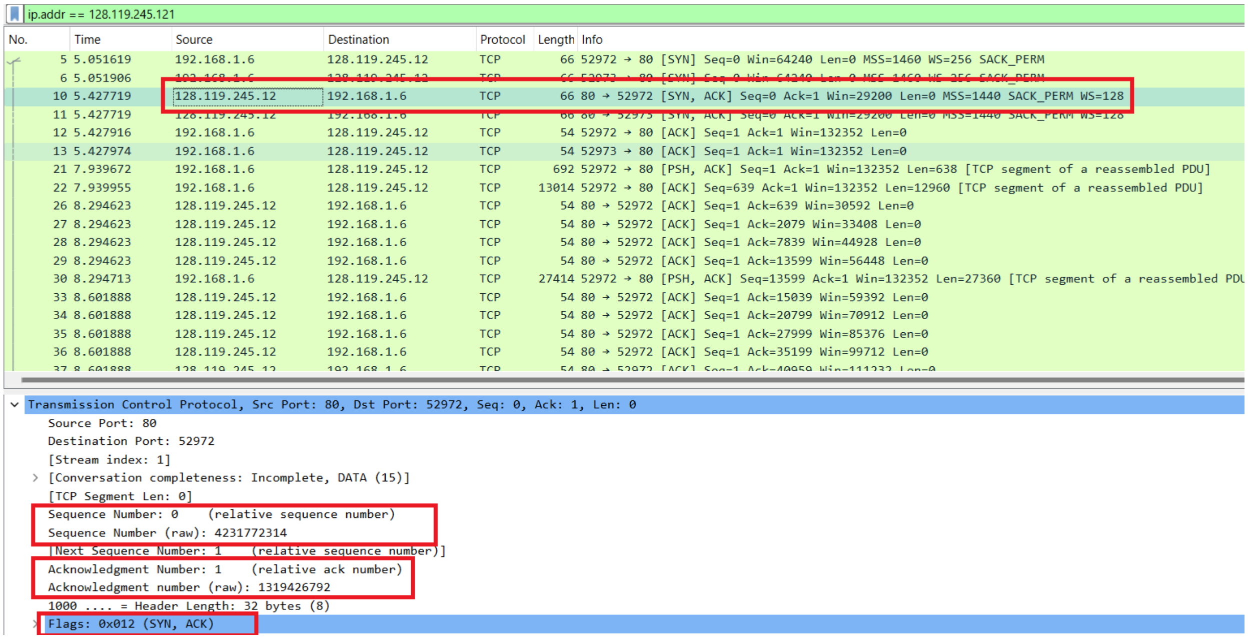
    - The value of the Acknowledgement field in the SYNACK segment is 1319426792.

    c. How did gaia.cs.umass.edu determine that value?

    - The value of the ACKnowledgement field in the SYNACK segment is determined by gaia.cs.umass.edu by adding 1 to the initial sequence number of SYN segment from the client computer.

    d. What is it in the segment that identifies the segment as a SYNACK segment?

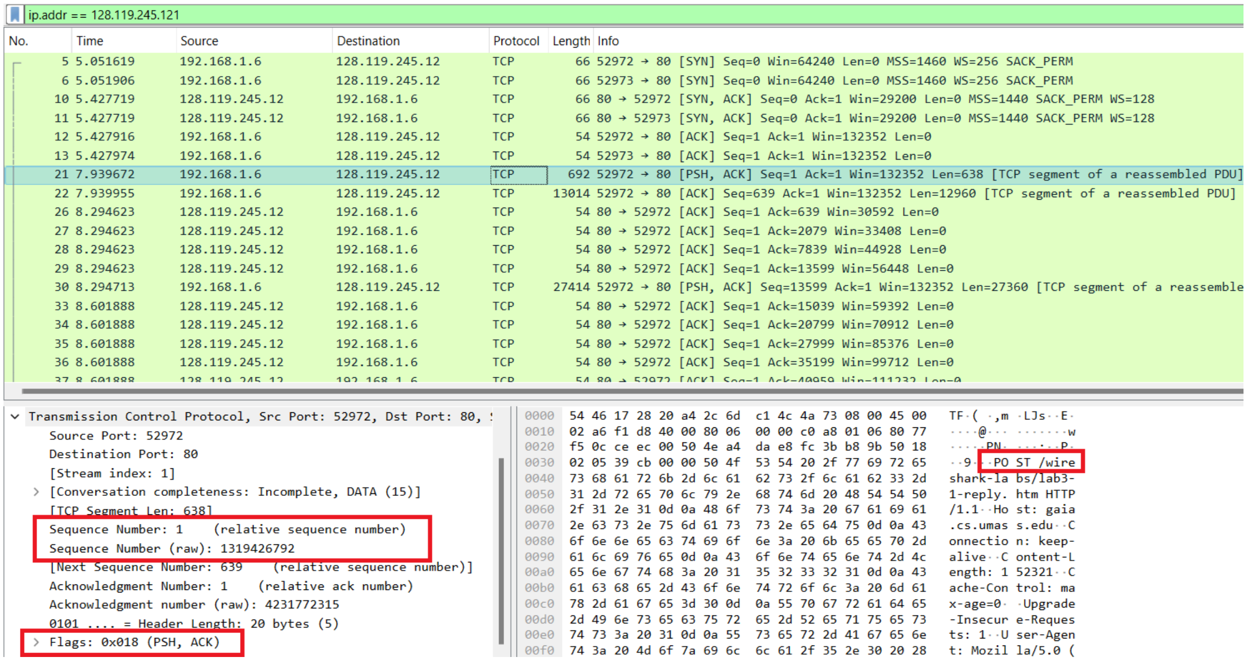
- The SYN flag and Acknowledgement flag in the segment are set to 1 and they indicate that this segment is a SYNACK segment.



```
ip.addr == 128.119.245.121

No.  Time      Source          Destination     Protocol Length Info
   5 5.051619  192.168.1.6     128.119.245.12  TCP        66 52972 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
   6 5.051906  192.168.1.6     128.119.245.12  TCP        66 52973 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
  10 5.427719  128.119.245.12  192.168.1.6     TCP        66 80 → 52972 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1440 SACK_PERM WS=128
  11 5.427719  128.119.245.12  192.168.1.6     TCP        66 80 → 52973 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1440 SACK_PERM WS=128
  12 5.427916  192.168.1.6     128.119.245.12  TCP        54 52972 → 80 [ACK] Seq=1 Ack=1 Win=132352 Len=0
  13 5.427974  192.168.1.6     128.119.245.12  TCP        54 52973 → 80 [ACK] Seq=1 Ack=1 Win=132352 Len=0
  21 7.939672  192.168.1.6     128.119.245.12  TCP       692 52972 → 80 [PSH, ACK] Seq=1 Ack=1 Win=132352 Len=638 [TCP segment of a reassembled PDU]
  22 7.939955  192.168.1.6     128.119.245.12  TCP     13014 52972 → 80 [ACK] Seq=639 Ack=1 Win=132352 Len=12960 [TCP segment of a reassembled PDU]
  26 8.294623  128.119.245.12  192.168.1.6     TCP        54 80 → 52972 [ACK] Seq=1 Ack=639 Win=30592 Len=0
  27 8.294623  128.119.245.12  192.168.1.6     TCP        54 80 → 52972 [ACK] Seq=1 Ack=2079 Win=33408 Len=0
  28 8.294623  128.119.245.12  192.168.1.6     TCP        54 80 → 52972 [ACK] Seq=1 Ack=7839 Win=44928 Len=0
  29 8.294623  128.119.245.12  192.168.1.6     TCP        54 80 → 52972 [ACK] Seq=1 Ack=13599 Win=56448 Len=0
  30 8.294713  192.168.1.6     128.119.245.12  TCP     27414 52972 → 80 [PSH, ACK] Seq=13599 Ack=1 Win=132352 Len=27360 [TCP segment of a reassembled PDU
  33 8.601888  128.119.245.12  192.168.1.6     TCP        54 80 → 52972 [ACK] Seq=1 Ack=15039 Win=59392 Len=0
  34 8.601888  128.119.245.12  192.168.1.6     TCP        54 80 → 52972 [ACK] Seq=1 Ack=20799 Win=70912 Len=0
  35 8.601888  128.119.245.12  192.168.1.6     TCP        54 80 → 52972 [ACK] Seq=1 Ack=27999 Win=85376 Len=0
  36 8.601888  128.119.245.12  192.168.1.6     TCP        54 80 → 52972 [ACK] Seq=1 Ack=35199 Win=99712 Len=0
  37 8.601888  128.119.245.12  192.168.1.6     TCP        54 80 → 52972 [ACK] Seq=1 Ack=40959 Win=111232 Len=0

v Transmission Control Protocol, Src Port: 80, Dst Port: 52972, Seq: 0, Ack: 1, Len: 0
    Source Port: 80
    Destination Port: 52972
    [Stream index: 1]
  > [Conversation completeness: Incomplete, DATA (15)]
    [TCP Segment Len: 0]
    Sequence Number: 0    (relative sequence number)
    Sequence Number (raw): 4231772314
    [Next Sequence Number: 1    (relative sequence number)]
    Acknowledgment Number: 1    (relative ack number)
    Acknowledgment number (raw): 1319426792
    1000 .... = Header Length: 32 bytes (8)
  > Flags: 0x012 (SYN, ACK)
```

5. What is the sequence number of the TCP segment containing the HTTP POST command? Note that in order to find the POST command; you'll need to dig into the packet content field at the bottom of the Wireshark window, looking for a segment with a "POST" within its DATA field.

- The sequence number of the TCP segment containing the HTTP POSTCommand is 1319426792..



ip.addr == 128.119.245.121

```
No.   Time       Source          Destination     Protocol Length Info
   5 5.051619    192.168.1.6     128.119.245.12  TCP         66 52972 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
   6 5.051906    192.168.1.6     128.119.245.12  TCP         66 52973 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
  10 5.427719    128.119.245.12  192.168.1.6     TCP         66 80 → 52972 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1440 SACK_PERM WS=128
  11 5.427719    128.119.245.12  192.168.1.6     TCP         66 80 → 52973 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1440 SACK_PERM WS=128
  12 5.427916    192.168.1.6     128.119.245.12  TCP         54 52972 → 80 [ACK] Seq=1 Ack=1 Win=132352 Len=0
  13 5.427974    192.168.1.6     128.119.245.12  TCP         54 52973 → 80 [ACK] Seq=1 Ack=1 Win=132352 Len=0
  21 7.939672    192.168.1.6     128.119.245.12  TCP        692 52972 → 80 [PSH, ACK] Seq=1 Ack=1 Win=132352 Len=638 [TCP segment of a reassembled PDU]
  22 7.939955    192.168.1.6     128.119.245.12  TCP      13014 52972 → 80 [ACK] Seq=639 Ack=1 Win=132352 Len=12960 [TCP segment of a reassembled PDU]
  26 8.294623    128.119.245.12  192.168.1.6     TCP         54 80 → 52972 [ACK] Seq=1 Ack=639 Win=30592 Len=0
  27 8.294623    128.119.245.12  192.168.1.6     TCP         54 80 → 52972 [ACK] Seq=1 Ack=2079 Win=33408 Len=0
  28 8.294623    128.119.245.12  192.168.1.6     TCP         54 80 → 52972 [ACK] Seq=1 Ack=7839 Win=44928 Len=0
  29 8.294623    128.119.245.12  192.168.1.6     TCP         54 80 → 52972 [ACK] Seq=1 Ack=13599 Win=56448 Len=0
  30 8.294713    192.168.1.6     128.119.245.12  TCP      27414 52972 → 80 [PSH, ACK] Seq=13599 Ack=1 Win=132352 Len=27360 [TCP segment of a reassemble
  33 8.601888    128.119.245.12  192.168.1.6     TCP         54 80 → 52972 [ACK] Seq=1 Ack=15039 Win=59392 Len=0
  34 8.601888    128.119.245.12  192.168.1.6     TCP         54 80 → 52972 [ACK] Seq=1 Ack=20799 Win=70912 Len=0
  35 8.601888    128.119.245.12  192.168.1.6     TCP         54 80 → 52972 [ACK] Seq=1 Ack=27999 Win=85376 Len=0
  36 8.601888    128.119.245.12  192.168.1.6     TCP         54 80 → 52972 [ACK] Seq=1 Ack=35199 Win=99712 Len=0
  37 8.601888    128.119.245.12  192.168.1.6     TCP         54 80 → 52972 [ACK] Seq=1 Ack=40959 Win=111232 Len=0
```

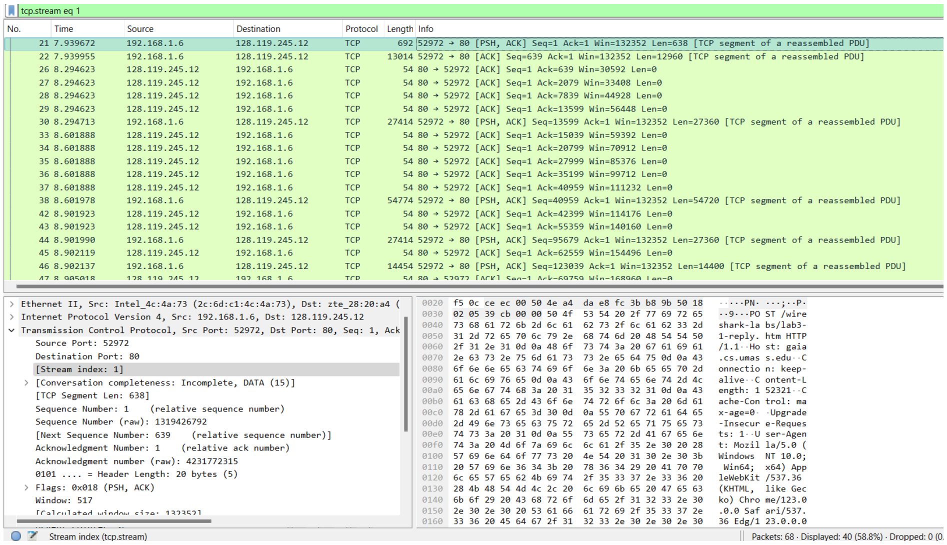
```
˅ Transmission Control Protocol, Src Port: 52972, Dst Port: 80,
    Source Port: 52972
    Destination Port: 80
    [Stream index: 1]
  › [Conversation completeness: Incomplete, DATA (15)]
    [TCP Segment Len: 638]
    Sequence Number: 1    (relative sequence number)
    Sequence Number (raw): 1319426792
    [Next Sequence Number: 639    (relative sequence number)]
    Acknowledgment Number: 1    (relative ack number)
    Acknowledgment number (raw): 4231772315
    0101 .... = Header Length: 20 bytes (5)
  › Flags: 0x018 (PSH, ACK)
```

```
0000  54 46 17 28 20 a4 2c 6d  c1 4c 4a 73 08 00 45 00   TF·( ·,m ·LJs··E·
0010  02 a6 f1 d8 40 00 80 06  00 00 c0 a8 01 06 80 77   ····@··· ·······w
0020  f5 0c ce ec 00 50 4e a4  da e8 fc 3b b8 9b 50 18   ·····PN· ··:···P·
0030  02 05 39 cb 00 00 50 4f  53 54 20 2f 77 69 72 65   ··9···PO ST /wire
0040  73 68 61 72 6b 2d 6c 61  62 73 2f 6c 61 62 33 2d   shark-la bs/lab3-
0050  31 2d 72 65 70 6c 79 2e  68 74 6d 20 48 54 54 50   1-reply. htm HTTP
0060  2f 31 2e 31 0d 0a 48 6f  73 74 3a 20 67 61 69 61   /1.1··Ho st: gaia
0070  2e 63 73 2e 75 6d 61 73  73 2e 65 64 75 0d 0a 43   .cs.umas s.edu··C
0080  6f 6e 6e 65 63 74 69 6f  6e 3a 20 6b 65 65 70 2d   onnectio n: keep-
0090  61 6c 69 76 65 0d 0a 43  6f 6e 74 65 6e 74 2d 4c   alive··C ontent-L
00a0  65 6e 67 74 68 3a 20 31  35 32 33 32 31 0d 0a 43   ength: 1 52321··C
00b0  61 63 68 65 2d 43 6f 6e  74 72 6f 6c 3a 20 6d 61   ache-Con trol: ma
00c0  78 2d 61 67 65 3d 30 0d  0a 55 70 67 72 61 64 65   x-age=0· ·Upgrade
00d0  2d 49 6e 73 65 63 75 72  65 2d 52 65 71 75 65 73   -Insecur e-Reques
00e0  74 73 3a 20 31 0d 0a 55  73 65 72 2d 41 67 65 6e   ts: 1··U ser-Agen
00f0  74 3a 20 4d 6f 7a 69 6c  6c 61 2f 35 2e 30 20 28   t: Mozil la/5.0 (
```

6. Consider the TCP segment containing the HTTP POST as the first segment in the TCP connection:

   a. What are the sequence numbers of the first six segments in the TCP connection (including the segment containing the HTTP POST)?

   - The first 6 segments in the TCP connection are No. 21, 22, 30, 38, 44, 46.
     The ACK of these segments are No. 26, 29, 37, 51, 57, 60.
     Segment 1 sequence number: 1319426792 (Relative - 1)
     Segment 2 sequence number: 1319427430 (Relative - 639)
     Segment 3 sequence number: 1319440390 (Relative - 13599)
     Segment 4 sequence number: 1319467750 (Relative - 40959)
     Segment 5 sequence number: 1319522470 (Relative - 95679)
     Segment 6 sequence number: 1319549830 (Relative - 123039)



```
No.    Time        Source            Destination       Protocol  Length Info
    21 7.939672    192.168.1.6       128.119.245.12    TCP          692 52972 → 80 [PSH, ACK] Seq=1 Ack=1 Win=132352 Len=638 [TCP segment of a reassembled PDU]
    22 7.939955    192.168.1.6       128.119.245.12    TCP        13014 52972 → 80 [ACK] Seq=639 Ack=1 Win=132352 Len=12960 [TCP segment of a reassembled PDU]
    26 8.294623    128.119.245.12    192.168.1.6       TCP           54 80 → 52972 [ACK] Seq=1 Ack=639 Win=30592 Len=0
    27 8.294623    128.119.245.12    192.168.1.6       TCP           54 80 → 52972 [ACK] Seq=1 Ack=2079 Win=33408 Len=0
    28 8.294623    128.119.245.12    192.168.1.6       TCP           54 80 → 52972 [ACK] Seq=1 Ack=7839 Win=44928 Len=0
    29 8.294623    128.119.245.12    192.168.1.6       TCP           54 80 → 52972 [ACK] Seq=1 Ack=13599 Win=56448 Len=0
    30 8.294713    192.168.1.6       128.119.245.12    TCP        27414 52972 → 80 [PSH, ACK] Seq=13599 Ack=1 Win=132352 Len=27360 [TCP segment of a reassembled PDU]
    33 8.601888    128.119.245.12    192.168.1.6       TCP           54 80 → 52972 [ACK] Seq=1 Ack=15039 Win=59392 Len=0
    34 8.601888    128.119.245.12    192.168.1.6       TCP           54 80 → 52972 [ACK] Seq=1 Ack=20799 Win=70912 Len=0
    35 8.601888    128.119.245.12    192.168.1.6       TCP           54 80 → 52972 [ACK] Seq=1 Ack=27999 Win=85376 Len=0
    36 8.601888    128.119.245.12    192.168.1.6       TCP           54 80 → 52972 [ACK] Seq=1 Ack=35199 Win=99712 Len=0
    37 8.601888    128.119.245.12    192.168.1.6       TCP           54 80 → 52972 [ACK] Seq=1 Ack=40959 Win=111232 Len=0
    38 8.601978    192.168.1.6       128.119.245.12    TCP        54774 52972 → 80 [PSH, ACK] Seq=40959 Ack=1 Win=132352 Len=54720 [TCP segment of a reassembled PDU]
    42 8.901923    128.119.245.12    192.168.1.6       TCP           54 80 → 52972 [ACK] Seq=1 Ack=42399 Win=114176 Len=0
    43 8.901923    128.119.245.12    192.168.1.6       TCP           54 80 → 52972 [ACK] Seq=1 Ack=55359 Win=140160 Len=0
    44 8.901990    192.168.1.6       128.119.245.12    TCP        27414 52972 → 80 [PSH, ACK] Seq=95679 Ack=1 Win=132352 Len=27360 [TCP segment of a reassembled PDU]
    45 8.902119    128.119.245.12    192.168.1.6       TCP           54 80 → 52972 [ACK] Seq=1 Ack=62559 Win=154496 Len=0
    46 8.902137    192.168.1.6       128.119.245.12    TCP        14454 52972 → 80 [PSH, ACK] Seq=123039 Ack=1 Win=132352 Len=14400 [TCP segment of a reassembled PDU]
    47 8.905018    128.119.245.12    192.168.1.6       TCP           54 80 → 52972 [ACK] Seq=1 Ack=69759 Win=168960 Len=0
```

```
> Ethernet II, Src: Intel_4c:4a:73 (2c:6d:c1:4c:4a:73), Dst: zte_28:20:a4 (
> Internet Protocol Version 4, Src: 192.168.1.6, Dst: 128.119.245.12
v Transmission Control Protocol, Src Port: 52972, Dst Port: 80, Seq: 1, Ack
    Source Port: 52972
    Destination Port: 80
    [Stream index: 1]
  > [Conversation completeness: Incomplete, DATA (15)]
    [TCP Segment Len: 638]
    Sequence Number: 1    (relative sequence number)
    Sequence Number (raw): 1319426792
    [Next Sequence Number: 639    (relative sequence number)]
    Acknowledgment Number: 1    (relative ack number)
    Acknowledgment number (raw): 4231772315
    0101 .... = Header Length: 20 bytes (5)
  > Flags: 0x018 (PSH, ACK)
    Window: 517
    [Calculated window size: 132352]
```

```
0020  f5 0c ce ec 00 50 4e a4  da e8 fc 3b b8 9b 50 18   ·····PN· ···;··P·
0030  02 05 39 cb 00 00 50 4f  53 54 20 2f 77 69 72 65   ··9···PO ST /wire
0040  73 68 61 72 6b 2d 6c 61  62 73 2f 6c 61 62 33 2d   shark-la bs/lab3-
0050  31 2d 72 65 70 6c 79 2e  68 74 6d 20 48 54 54 50   1-reply. htm HTTP
0060  2f 31 2e 31 0d 0a 48 6f  73 74 3a 20 67 61 69 61   /1.1··Ho st: gaia
0070  2e 63 73 2e 75 6d 61 73  73 2e 65 64 75 0d 0a 43   .cs.umas s.edu··C
0080  6f 6e 6e 65 63 74 69 6f  6e 3a 20 6b 65 65 70 2d   onnectio n: keep-
0090  61 6c 69 76 65 0d 0a 43  6f 6e 74 65 6e 74 2d 4c   alive··C ontent-L
00a0  65 6e 67 74 68 3a 20 31  35 32 33 32 31 0d 0a 43   ength: 1 52321··C
00b0  61 63 68 65 2d 43 6f 6e  74 72 6f 6c 3a 20 6d 61   ache-Con trol: ma
00c0  78 2d 61 67 65 3d 30 0d  0a 55 70 67 72 61 64 65   x-age=0· ·Upgrade
00d0  2d 49 6e 73 65 63 75 72  65 2d 52 65 71 75 65 73   -Insecur e-Reques
00e0  74 73 3a 20 31 0d 0a 55  73 65 72 2d 41 67 65 6e   ts: 1··U ser-Agen
00f0  74 3a 20 4d 6f 7a 69 6c  6c 61 2f 35 2e 30 20 28   t: Mozil la/5.0 (
0100  57 69 6e 64 6f 77 73 20  4e 54 20 31 30 2e 30 3b   Windows  NT 10.0;
0110  20 57 69 6e 36 34 3b 20  78 36 34 29 20 41 70 70    Win64;  x64) App
0120  6c 65 57 65 62 4b 69 74  2f 35 33 37 2e 33 36 20   leWebKit /537.36 
0130  28 4b 48 54 4d 4c 2c 20  6c 69 6b 65 20 47 65 63   (KHTML,  like Gec
0140  6b 6f 29 20 43 68 72 6f  6d 65 2f 31 32 33 2e 30   ko) Chro me/123.0
0150  2e 30 2e 30 20 53 61 66  61 72 69 2f 35 33 37 2e   .0.0 Saf ari/537.
0160  33 36 20 45 64 67 2f 31  32 33 2e 30 2e 30 2e 30   36 Edg/1 23.0.0.0
```

Stream index (tcp.stream)
Packets: 68 · Displayed: 40 (58.8%) · Dropped: 0 (0.

b. At what time was each segment sent? And when was the ACK for each segment received?

-

	Sent time	ACK received time	RTT
Segment 1	7.939672	8.294623	0.354951
Segment 2	7.939955	8.294623	0.354668
Segment 3	8.294713	8.601888	0.307175
Segment 4	8.601978	8.905018	0.303040
Segment 5	8.901990	9.216152	0.314162
Segment 6	8.902137	9.216152	0.314015

-

c. What is the EstimatedRTT value after the receipt of each ACK? (*Use the EstimatedRTT equation. Assume that the value of the EstimatedRTT is equal to the measured RTT for the first segment, and then is computed using the EstimatedRTT equation).

- EstimatedRTT = 0.875 * EstimatedRTT + 0.125 * SampleRTT

  EstimatedRTT after the receipt of the ACK of segment 1:
  EstimatedRTT = RTT for Segment 1 = 0.354951 sec

  EstimatedRTT after the receipt of the ACK of segment 2:
  EstimatedRTT = 0.875 * 0.354951 + 0.125 * 0.354668 = 0.354915 sec

  EstimatedRTT after the receipt of the ACK of segment 3:
  EstimatedRTT = 0.875 * 0.354915 + 0.125 * 0.307175 = 0.348947

  EstimatedRTT after the receipt of the ACK of segment 4:
  EstimatedRTT = 0.875 * 0.348947 + 0.125 * 0.303040 = 0.343208

  EstimatedRTT after the receipt of the ACK of segment 5:
  EstimatedRTT = 0.875 * 0.343208 + 0.125 * 0.314162 = 0.339577

  EstimatedRTT after the receipt of the ACK of segment 6:
  EstimatedRTT = 0.875 * 0.339577 + 0.125 * 0.314015 = 0.336381

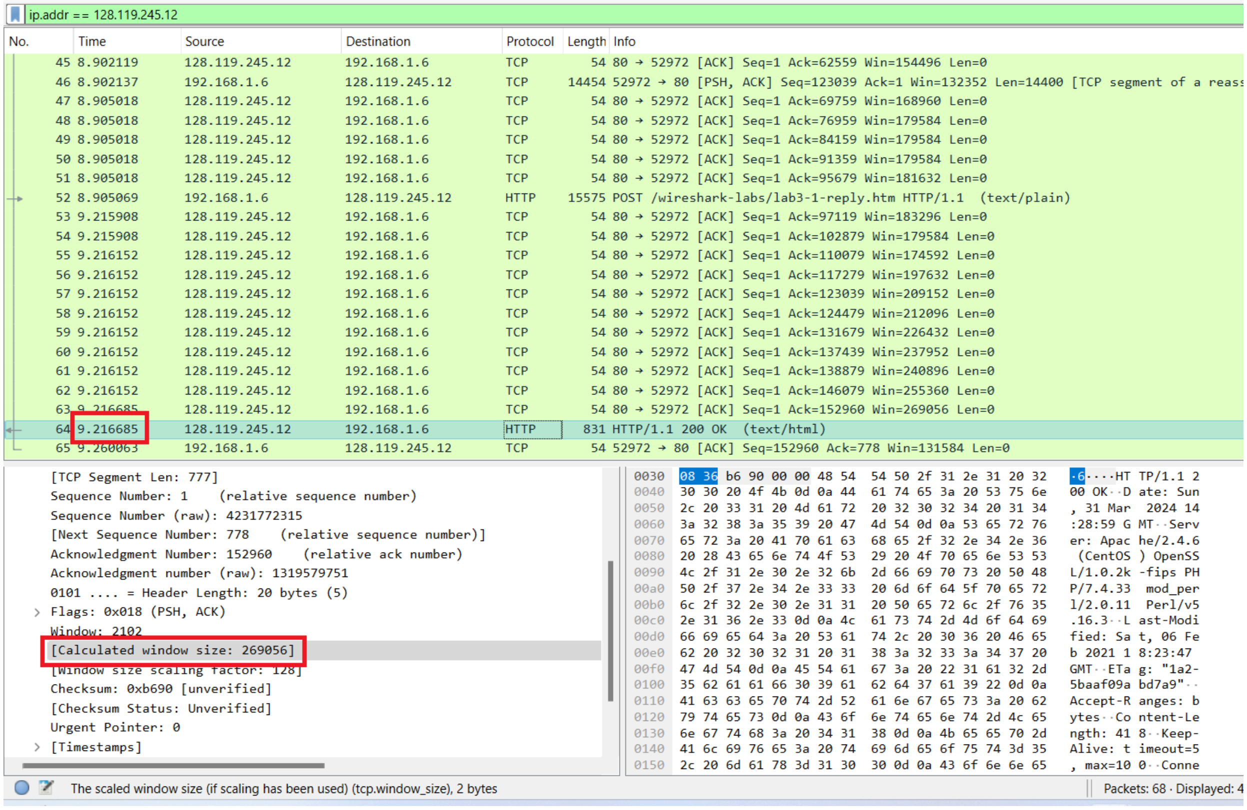
d. What is the length of each of the first six TCP segments?

Segment	Length
1	692
2	13014
3	27414
4	55774
5	27414
6	14454

e. What is the throughput (bytes transferred per unit time) for the TCP connection? Explain how you calculated this value.

- Throughout = Calculated Window Size / (Time difference between the first segment sent and the last segment sent)
  Throughput = 269056 / (9.216685 - 7.939672)
  = 210691.669 bits/sec
  = 26.336 KByte / sec

  The average throughput for this TCP connection is computed as the ratio between the total amount data and the total transmission time. I figured out how may bytes were transferred during the amount of time between when the client sent the 1st segment containing the 1st bytes of data in and alice.txt and when the last segment in the connection containing the last bytes of data in alice.txt was sent



```
ip.addr == 128.119.245.12

No.  Time      Source          Destination     Protocol Length Info
  45 8.902119  128.119.245.12  192.168.1.6     TCP        54 80 → 52972 [ACK] Seq=1 Ack=62559 Win=154496 Len=0
  46 8.902137  192.168.1.6     128.119.245.12  TCP     14454 52972 → 80 [PSH, ACK] Seq=123039 Ack=1 Win=132352 Len=14400 [TCP segment of a reass
  47 8.905018  128.119.245.12  192.168.1.6     TCP        54 80 → 52972 [ACK] Seq=1 Ack=69759 Win=168960 Len=0
  48 8.905018  128.119.245.12  192.168.1.6     TCP        54 80 → 52972 [ACK] Seq=1 Ack=76959 Win=179584 Len=0
  49 8.905018  128.119.245.12  192.168.1.6     TCP        54 80 → 52972 [ACK] Seq=1 Ack=84159 Win=179584 Len=0
  50 8.905018  128.119.245.12  192.168.1.6     TCP        54 80 → 52972 [ACK] Seq=1 Ack=91359 Win=179584 Len=0
  51 8.905018  128.119.245.12  192.168.1.6     TCP        54 80 → 52972 [ACK] Seq=1 Ack=95679 Win=181632 Len=0
  52 8.905069  192.168.1.6     128.119.245.12  HTTP    15575 POST /wireshark-labs/lab3-1-reply.htm HTTP/1.1  (text/plain)
  53 9.215908  128.119.245.12  192.168.1.6     TCP        54 80 → 52972 [ACK] Seq=1 Ack=97119 Win=183296 Len=0
  54 9.215908  128.119.245.12  192.168.1.6     TCP        54 80 → 52972 [ACK] Seq=1 Ack=102879 Win=179584 Len=0
  55 9.216152  128.119.245.12  192.168.1.6     TCP        54 80 → 52972 [ACK] Seq=1 Ack=110079 Win=174592 Len=0
  56 9.216152  128.119.245.12  192.168.1.6     TCP        54 80 → 52972 [ACK] Seq=1 Ack=117279 Win=197632 Len=0
  57 9.216152  128.119.245.12  192.168.1.6     TCP        54 80 → 52972 [ACK] Seq=1 Ack=123039 Win=209152 Len=0
  58 9.216152  128.119.245.12  192.168.1.6     TCP        54 80 → 52972 [ACK] Seq=1 Ack=124479 Win=212096 Len=0
  59 9.216152  128.119.245.12  192.168.1.6     TCP        54 80 → 52972 [ACK] Seq=1 Ack=131679 Win=226432 Len=0
  60 9.216152  128.119.245.12  192.168.1.6     TCP        54 80 → 52972 [ACK] Seq=1 Ack=137439 Win=237952 Len=0
  61 9.216152  128.119.245.12  192.168.1.6     TCP        54 80 → 52972 [ACK] Seq=1 Ack=138879 Win=240896 Len=0
  62 9.216152  128.119.245.12  192.168.1.6     TCP        54 80 → 52972 [ACK] Seq=1 Ack=146079 Win=255360 Len=0
  63 9.216685  128.119.245.12  192.168.1.6     TCP        54 80 → 52972 [ACK] Seq=1 Ack=152960 Win=269056 Len=0
  64 9.216685  128.119.245.12  192.168.1.6     HTTP      831 HTTP/1.1 200 OK  (text/html)
  65 9.260063  192.168.1.6     128.119.245.12  TCP        54 52972 → 80 [ACK] Seq=152960 Ack=778 Win=131584 Len=0
```

```
    [TCP Segment Len: 777]
    Sequence Number: 1    (relative sequence number)
    Sequence Number (raw): 4231772315
    [Next Sequence Number: 778    (relative sequence number)]
    Acknowledgment Number: 152960    (relative ack number)
    Acknowledgment number (raw): 1319579751
    0101 .... = Header Length: 20 bytes (5)
  > Flags: 0x018 (PSH, ACK)
    Window: 2102
    [Calculated window size: 269056]
    [Window size scaling factor: 128]
    Checksum: 0xb690 [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
  > [Timestamps]
```

```
0030  08 36 b6 90 00 00 48 54  54 50 2f 31 2e 31 20 32   ·6····HT TP/1.1 2
0040  30 30 20 4f 4b 0d 0a 44  61 74 65 3a 20 53 75 6e   00 OK··D ate: Sun
0050  2c 20 33 31 20 4d 61 72  20 32 30 32 34 20 31 34   , 31 Mar  2024 14
0060  3a 32 38 3a 35 39 20 47  4d 54 0d 0a 53 65 72 76   :28:59 G MT··Serv
0070  65 72 3a 20 41 70 61 63  68 65 2f 32 2e 34 2e 36   er: Apac he/2.4.6
0080  20 28 43 65 6e 74 4f 53  29 20 4f 70 65 6e 53 53    (CentOS ) OpenSS
0090  4c 2f 31 2e 30 2e 32 6b  2d 66 69 70 73 20 50 48   L/1.0.2k -fips PH
00a0  50 2f 37 2e 34 2e 33 33  20 6d 6f 64 5f 70 65 72   P/7.4.33  mod_per
00b0  6c 2f 32 2e 30 2e 31 31  20 50 65 72 6c 2f 76 35   l/2.0.11  Perl/v5
00c0  2e 31 36 2e 33 0d 0a 4c  61 73 74 2d 4d 6f 64 69   .16.3··L ast-Modi
00d0  66 69 65 64 3a 20 53 61  74 2c 20 30 36 20 46 65   fied: Sa t, 06 Fe
00e0  62 20 32 30 32 31 20 31  38 3a 32 33 3a 34 37 20   b 2021 1 8:23:47
00f0  47 4d 54 0d 0a 45 54 61  67 3a 20 22 31 61 32 2d   GMT··ETa g: "1a2-
0100  35 62 61 61 66 30 39 61  62 64 37 61 39 22 0d 0a   5baaf09a bd7a9"··
0110  41 63 63 65 70 74 2d 52  61 6e 67 65 73 3a 20 62   Accept-R anges: b
0120  79 74 65 73 0d 0a 43 6f  6e 74 65 6e 74 2d 4c 65   ytes··Co ntent-Le
0130  6e 67 74 68 3a 20 34 31  38 0d 0a 4b 65 65 70 2d   ngth: 41 8··Keep-
0140  41 6c 69 76 65 3a 20 74  69 6d 65 6f 75 74 3d 35   Alive: t imeout=5
0150  2c 20 6d 61 78 3d 31 30  30 0d 0a 43 6f 6e 6e 65   , max=10 0··Conne
```

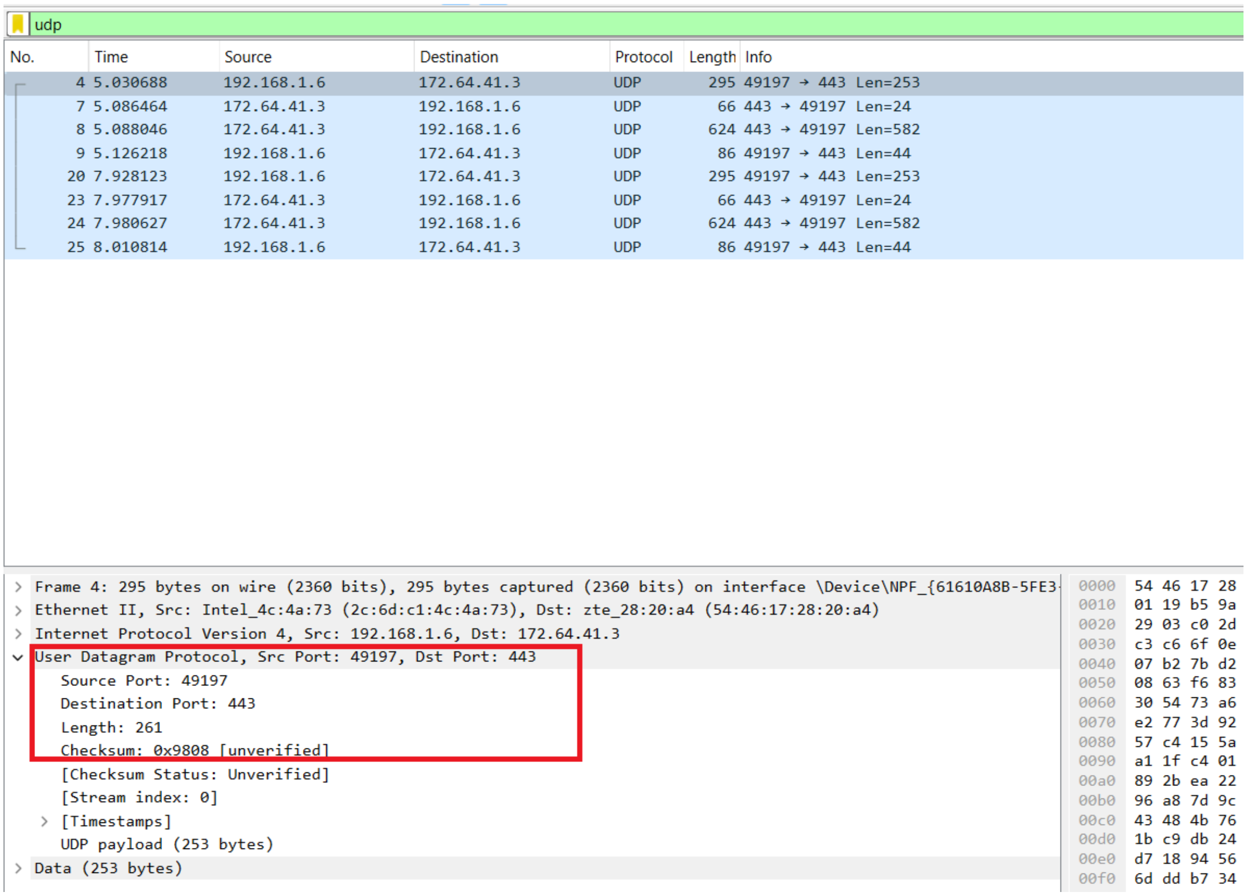
```
The scaled window size (if scaling has been used) (tcp.window_size), 2 bytes        Packets: 68 · Displayed: 4
```

UDP ASSIGNMENT

1. Select one UDP packet from your trace. From this packet, determine how

many fields there are in the UDP header. Name these fields. (Answer these questions directly from what you observe in the packet trace.)

- There are 4 fields in the UDP header. They are
    1. Source Port
    2. Destination Port
    3. Length
    4. Checksum



```
udp
```

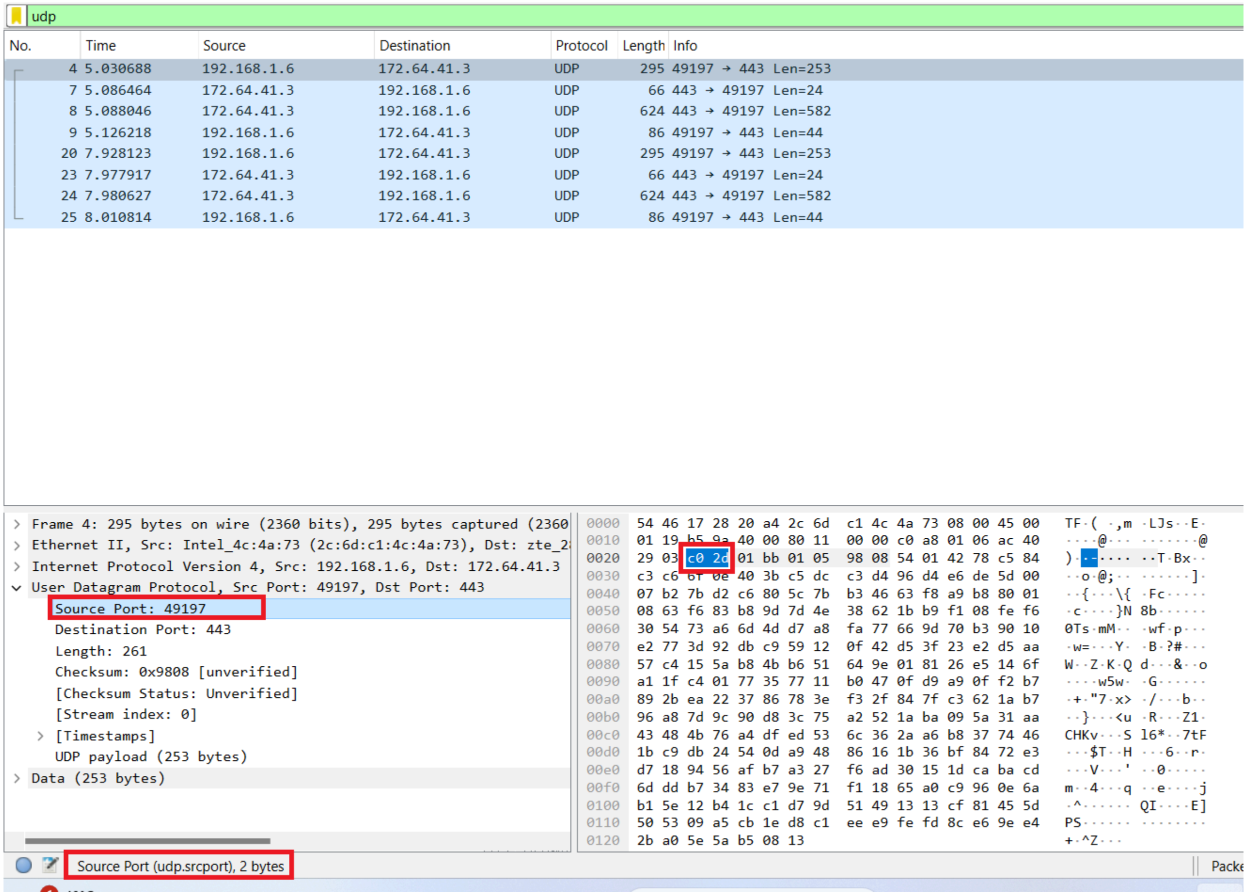
```
No.   Time       Source         Destination    Protocol  Length  Info
    4 5.030688   192.168.1.6    172.64.41.3    UDP          295  49197 → 443 Len=253
    7 5.086464   172.64.41.3    192.168.1.6    UDP           66  443 → 49197 Len=24
    8 5.088046   172.64.41.3    192.168.1.6    UDP          624  443 → 49197 Len=582
    9 5.126218   192.168.1.6    172.64.41.3    UDP           86  49197 → 443 Len=44
   20 7.928123   192.168.1.6    172.64.41.3    UDP          295  49197 → 443 Len=253
   23 7.977917   172.64.41.3    192.168.1.6    UDP           66  443 → 49197 Len=24
   24 7.980627   172.64.41.3    192.168.1.6    UDP          624  443 → 49197 Len=582
   25 8.010814   192.168.1.6    172.64.41.3    UDP           86  49197 → 443 Len=44
```

```
> Frame 4: 295 bytes on wire (2360 bits), 295 bytes captured (2360 bits) on interface \Device\NPF_{61610A8B-5FE3
> Ethernet II, Src: Intel_4c:4a:73 (2c:6d:c1:4c:4a:73), Dst: zte_28:20:a4 (54:46:17:28:20:a4)
> Internet Protocol Version 4, Src: 192.168.1.6, Dst: 172.64.41.3
v User Datagram Protocol, Src Port: 49197, Dst Port: 443
    Source Port: 49197
    Destination Port: 443
    Length: 261
    Checksum: 0x9808 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 0]
  > [Timestamps]
    UDP payload (253 bytes)
> Data (253 bytes)
```

```
0000  54 46 17 28
0010  01 19 b5 9a
0020  29 03 c0 2d
0030  c3 c6 6f 0e
0040  07 b2 7b d2
0050  08 63 f6 83
0060  30 54 73 a6
0070  e2 77 3d 92
0080  57 c4 15 5a
0090  a1 1f c4 01
00a0  89 2b ea 22
00b0  96 a8 7d 9c
00c0  43 48 4b 76
00d0  1b c9 db 24
00e0  d7 18 94 56
00f0  6d dd b7 34
```

2. 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.

- Source Port - 2 bytes
  Destination Port - 2 bytes
  Length - 2 bytes
  Checksum - 2 bytes
  Therefore, the length of the UDP header is 8 bytes.

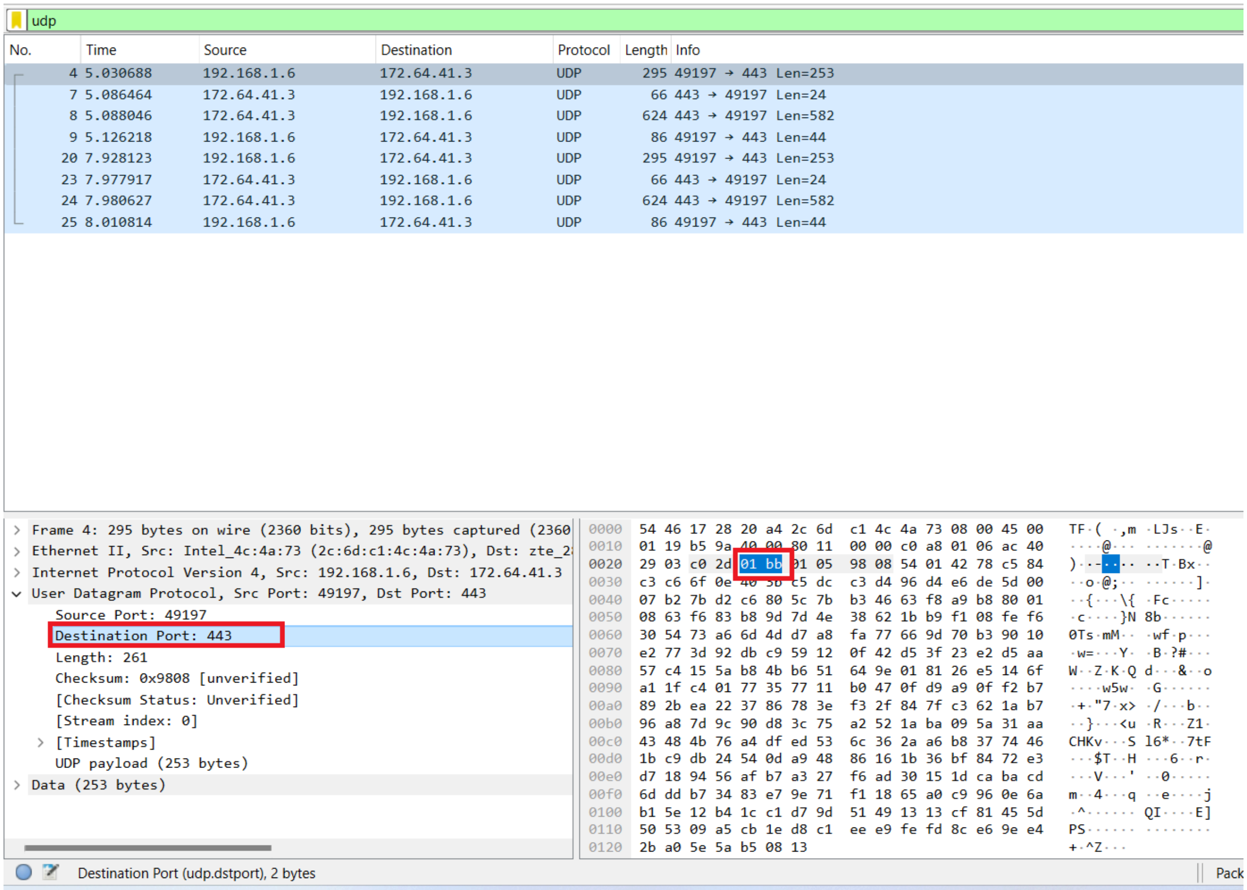


```
udp

No.   Time       Source        Destination   Protocol  Length Info
    4 5.030688   192.168.1.6   172.64.41.3   UDP        295 49197 → 443 Len=253
    7 5.086464   172.64.41.3   192.168.1.6   UDP         66 443 → 49197 Len=24
    8 5.088046   172.64.41.3   192.168.1.6   UDP        624 443 → 49197 Len=582
    9 5.126218   192.168.1.6   172.64.41.3   UDP         86 49197 → 443 Len=44
   20 7.928123   192.168.1.6   172.64.41.3   UDP        295 49197 → 443 Len=253
   23 7.977917   172.64.41.3   192.168.1.6   UDP         66 443 → 49197 Len=24
   24 7.980627   172.64.41.3   192.168.1.6   UDP        624 443 → 49197 Len=582
   25 8.010814   192.168.1.6   172.64.41.3   UDP         86 49197 → 443 Len=44
```

```
> Frame 4: 295 bytes on wire (2360 bits), 295 bytes captured (2360
> Ethernet II, Src: Intel_4c:4a:73 (2c:6d:c1:4c:4a:73), Dst: zte_2
> Internet Protocol Version 4, Src: 192.168.1.6, Dst: 172.64.41.3
v User Datagram Protocol, Src Port: 49197, Dst Port: 443
    Source Port: 49197
    Destination Port: 443
    Length: 261
    Checksum: 0x9808 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 0]
  > [Timestamps]
    UDP payload (253 bytes)
> Data (253 bytes)
```

```
0000  54 46 17 28 20 a4 2c 6d  c1 4c 4a 73 08 00 45 00   TF·( ·,m ·LJs··E·
0010  01 19 b5 9a 40 00 80 11  00 00 c0 a8 01 06 ac 40   ····@··· ·······@
0020  29 03 c0 2d 01 bb 01 05  98 08 54 01 42 78 c5 84   )··-···· ··T·Bx··
0030  c3 c6 6f 0e 40 3b c5 dc  c3 d4 96 d4 e6 de 5d 00   ··o·@;·· ······]·
0040  07 b2 7b d2 c6 80 5c 7b  b3 46 63 f8 a9 b8 80 01   ··{···\{ ·Fc·····
0050  08 63 f6 83 b8 9d 7d 4e  38 62 1b b9 f1 08 fe f6   ·c····}N 8b······
0060  30 54 73 a6 6d 4d d7 a8  fa 77 66 9d 70 b3 90 10   0Ts·mM·· ·wf·p···
0070  e2 77 3d 92 db c9 59 12  0f 42 d5 3f 23 e2 d5 aa   ·w=···Y· ·B·?#···
0080  57 c4 15 5a b8 4b b6 51  64 9e 01 81 26 e5 14 6f   W··Z·K·Q d···&··o
0090  a1 1f c4 01 77 35 77 11  b0 47 0f d9 a9 0f f2 b7   ····w5w· ·G······
00a0  89 2b ea 22 37 86 78 3e  f3 2f 84 7f c3 62 1a b7   ·+·"7·x> ·/···b··
00b0  96 a8 7d 9c 90 d8 3c 75  a2 52 1a ba 09 5a 31 aa   ··}···<u ·R···Z1·
00c0  43 48 4b 76 a4 df ed 53  6c 36 2a a6 b8 37 74 46   CHKv···S l6*··7tF
00d0  1b c9 db 24 54 0d a9 48  86 16 1b 36 bf 84 72 e3   ···$T··H ···6··r·
00e0  d7 18 94 56 af b7 a3 27  f6 ad 30 15 1d ca ba cd   ···V···' ··0·····
00f0  6d dd b7 34 83 e7 9e 71  f1 18 65 a0 c9 96 0e 6a   m··4···q ··e····j
0100  b1 5e 12 b4 1c c1 d7 9d  51 49 13 13 cf 81 45 5d   ·^······ QI····E]
0110  50 53 09 a5 cb 1e d8 c1  ee e9 fe fd 8c e6 9e e4   PS······ ········
0120  2b a0 5e 5a b5 08 13                               +·^Z···
```

Source Port (udp.srcport), 2 bytes



udp

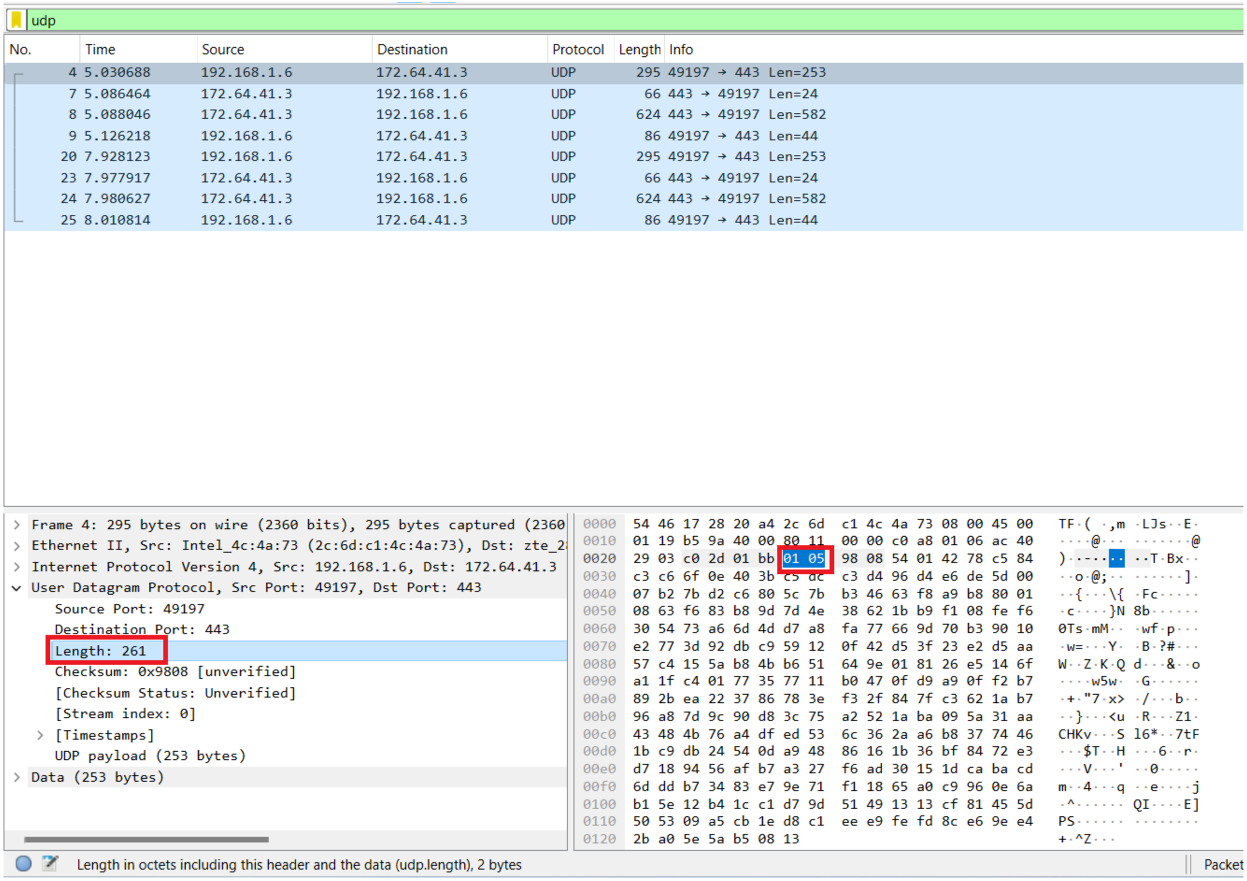
```
No.   Time        Source         Destination    Protocol  Length Info
    4 5.030688    192.168.1.6    172.64.41.3    UDP         295 49197 → 443 Len=253
    7 5.086464    172.64.41.3    192.168.1.6    UDP          66 443 → 49197 Len=24
    8 5.088046    172.64.41.3    192.168.1.6    UDP         624 443 → 49197 Len=582
    9 5.126218    192.168.1.6    172.64.41.3    UDP          86 49197 → 443 Len=44
   20 7.928123    192.168.1.6    172.64.41.3    UDP         295 49197 → 443 Len=253
   23 7.977917    172.64.41.3    192.168.1.6    UDP          66 443 → 49197 Len=24
   24 7.980627    172.64.41.3    192.168.1.6    UDP         624 443 → 49197 Len=582
   25 8.010814    192.168.1.6    172.64.41.3    UDP          86 49197 → 443 Len=44
```

```
> Frame 4: 295 bytes on wire (2360 bits), 295 bytes captured (2360
> Ethernet II, Src: Intel_4c:4a:73 (2c:6d:c1:4c:4a:73), Dst: zte_2
> Internet Protocol Version 4, Src: 192.168.1.6, Dst: 172.64.41.3
v User Datagram Protocol, Src Port: 49197, Dst Port: 443
    Source Port: 49197
    Destination Port: 443
    Length: 261
    Checksum: 0x9808 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 0]
  > [Timestamps]
    UDP payload (253 bytes)
> Data (253 bytes)
```

```
0000  54 46 17 28 20 a4 2c 6d  c1 4c 4a 73 08 00 45 00   TF·( ·,m ·LJs··E·
0010  01 19 b5 9a 40 00 80 11  00 00 c0 a8 01 06 ac 40   ····@··· ·······@
0020  29 03 c0 2d 01 bb 01 05  98 08 54 01 42 78 c5 84   )··-···· ··T·Bx··
0030  c3 c6 6f 0e 40 3b c5 dc  c3 d4 96 d4 e6 de 5d 00   ··o·@;·· ······]·
0040  07 b2 7b d2 c6 80 5c 7b  b3 46 63 f8 a9 b8 80 01   ··{···\{ ·Fc·····
0050  08 63 f6 83 b8 9d 7d 4e  38 62 1b b9 f1 08 fe f6   ·c····}N 8b······
0060  30 54 73 a6 6d 4d d7 a8  fa 77 66 9d 70 b3 90 10   0Ts·mM·· ·wf·p···
0070  e2 77 3d 92 db c9 59 12  0f 42 d5 3f 23 e2 d5 aa   ·w=···Y· ·B·?#···
0080  57 c4 15 5a b8 4b b6 51  64 9e 01 81 26 e5 14 6f   W··Z·K·Q d···&··o
0090  a1 1f c4 01 77 35 77 11  b0 47 0f d9 a9 0f f2 b7   ····w5w· ·G······
00a0  89 2b ea 22 37 86 78 3e  f3 2f 84 7f c3 62 1a b7   ·+·"7·x> ·/···b··
00b0  96 a8 7d 9c 90 d8 3c 75  a2 52 1a ba 09 5a 31 aa   ··}···<u ·R···Z1·
00c0  43 48 4b 76 a4 df ed 53  6c 36 2a a6 b8 37 74 46   CHKv···S l6*··7tF
00d0  1b c9 db 24 54 0d a9 48  86 16 1b 36 bf 84 72 e3   ···$T··H ···6··r·
00e0  d7 18 94 56 af b7 a3 27  f6 ad 30 15 1d ca ba cd   ···V···' ··0·····
00f0  6d dd b7 34 83 e7 9e 71  f1 18 65 a0 c9 96 0e 6a   m··4···q ··e····j
0100  b1 5e 12 b4 1c c1 d7 9d  51 49 13 13 cf 81 45 5d   ·^······ QI····E]
0110  50 53 09 a5 cb 1e d8 c1  ee e9 fe fd 8c e6 9e e4   PS······ ········
0120  2b a0 5e 5a b5 08 13                               +·^Z···
```

Destination Port (udp.dstport), 2 bytes

Pack

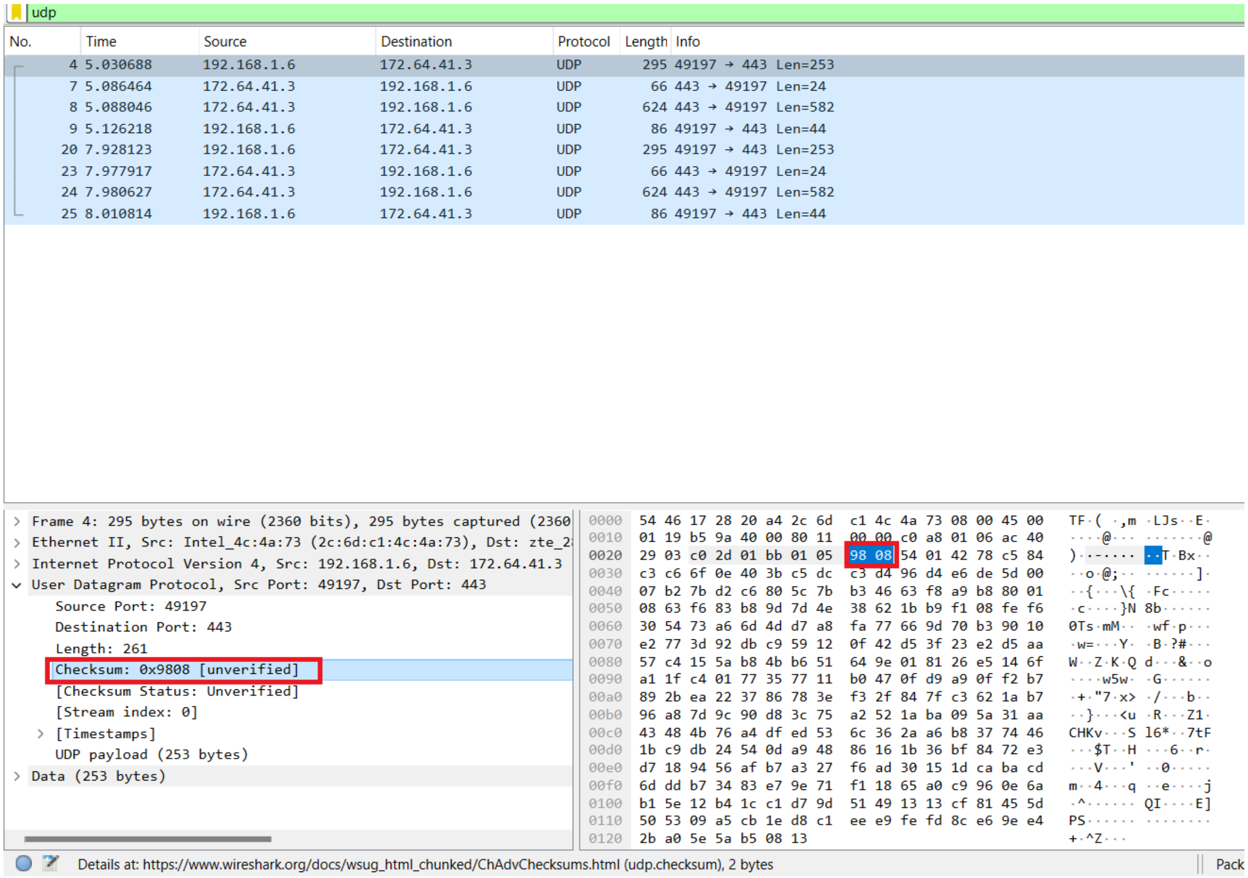


```
No.   Time      Source        Destination   Protocol Length Info
    4 5.030688  192.168.1.6   172.64.41.3   UDP       295 49197 → 443 Len=253
    7 5.086464  172.64.41.3   192.168.1.6   UDP        66 443 → 49197 Len=24
    8 5.088046  172.64.41.3   192.168.1.6   UDP       624 443 → 49197 Len=582
    9 5.126218  192.168.1.6   172.64.41.3   UDP        86 49197 → 443 Len=44
   20 7.928123  192.168.1.6   172.64.41.3   UDP       295 49197 → 443 Len=253
   23 7.977917  172.64.41.3   192.168.1.6   UDP        66 443 → 49197 Len=24
   24 7.980627  172.64.41.3   192.168.1.6   UDP       624 443 → 49197 Len=582
   25 8.010814  192.168.1.6   172.64.41.3   UDP        86 49197 → 443 Len=44
```

```
> Frame 4: 295 bytes on wire (2360 bits), 295 bytes captured (2360
> Ethernet II, Src: Intel_4c:4a:73 (2c:6d:c1:4c:4a:73), Dst: zte_2
> Internet Protocol Version 4, Src: 192.168.1.6, Dst: 172.64.41.3
v User Datagram Protocol, Src Port: 49197, Dst Port: 443
    Source Port: 49197
    Destination Port: 443
    Length: 261
    Checksum: 0x9808 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 0]
  > [Timestamps]
    UDP payload (253 bytes)
> Data (253 bytes)
```

```
0000  54 46 17 28 20 a4 2c 6d  c1 4c 4a 73 08 00 45 00   TF·( ·,m ·LJs··E·
0010  01 19 b5 9a 40 00 80 11  00 00 c0 a8 01 06 ac 40   ····@··· ·······@
0020  29 03 c0 2d 01 bb 01 05  98 08 54 01 42 78 c5 84   )··-···· ··T·Bx··
0030  c3 c6 6f 0e 40 3b c5 dc  c3 d4 96 d4 e6 de 5d 00   ··o·@;·· ······]·
0040  07 b2 7b d2 c6 80 5c 7b  b3 46 63 f8 a9 b8 80 01   ··{···\{ ·Fc·····
0050  08 63 f6 83 b8 9d 7d 4e  38 62 1b b9 f1 08 fe f6   ·c····}N 8b······
0060  30 54 73 a6 6d 4d d7 a8  fa 77 66 9d 70 b3 90 10   0Ts·mM·· ·wf·p···
0070  e2 77 3d 92 db c9 59 12  0f 42 d5 3f 23 e2 d5 aa   ·w=···Y· ·B·?#···
0080  57 c4 15 5a b8 4b b6 51  64 9e 01 81 26 e5 14 6f   W··Z·K·Q d···&··o
0090  a1 1f c4 01 77 35 77 11  b0 47 0f d9 a9 0f f2 b7   ····w5w· ·G······
00a0  89 2b ea 22 37 86 78 3e  f3 2f 84 7f c3 62 1a b7   ·+·"7·x> ·/···b··
00b0  96 a8 7d 9c 90 d8 3c 75  a2 52 1a ba 09 5a 31 aa   ··}···<u ·R···Z1·
00c0  43 48 4b 76 a4 df ed 53  6c 36 2a a6 b8 37 74 46   CHKv···S l6*··7tF
00d0  1b c9 db 24 54 0d a9 48  86 16 1b 36 bf 84 72 e3   ···$T··H ···6··r·
00e0  d7 18 94 56 af b7 a3 27  f6 ad 30 15 1d ca ba cd   ···V···' ··0·····
00f0  6d dd b7 34 83 e7 9e 71  f1 18 65 a0 c9 96 0e 6a   m··4···q ··e····j
0100  b1 5e 12 b4 1c c1 d7 9d  51 49 13 13 cf 81 45 5d   ·^······ QI····E]
0110  50 53 09 a5 cb 1e d8 c1  ee e9 fe fd 8c e6 9e e4   PS······ ········
0120  2b a0 5e 5a b5 08 13                               +·^Z···
```

Length in octets including this header and the data (udp.length), 2 bytes



```
udp

No.   Time        Source         Destination    Protocol  Length Info
    4 5.030688    192.168.1.6    172.64.41.3    UDP          295 49197 → 443 Len=253
    7 5.086464    172.64.41.3    192.168.1.6    UDP           66 443 → 49197 Len=24
    8 5.088046    172.64.41.3    192.168.1.6    UDP          624 443 → 49197 Len=582
    9 5.126218    192.168.1.6    172.64.41.3    UDP           86 49197 → 443 Len=44
   20 7.928123    192.168.1.6    172.64.41.3    UDP          295 49197 → 443 Len=253
   23 7.977917    172.64.41.3    192.168.1.6    UDP           66 443 → 49197 Len=24
   24 7.980627    172.64.41.3    192.168.1.6    UDP          624 443 → 49197 Len=582
   25 8.010814    192.168.1.6    172.64.41.3    UDP           86 49197 → 443 Len=44
```

```
> Frame 4: 295 bytes on wire (2360 bits), 295 bytes captured (2360
> Ethernet II, Src: Intel_4c:4a:73 (2c:6d:c1:4c:4a:73), Dst: zte_2
> Internet Protocol Version 4, Src: 192.168.1.6, Dst: 172.64.41.3
v User Datagram Protocol, Src Port: 49197, Dst Port: 443
    Source Port: 49197
    Destination Port: 443
    Length: 261
    Checksum: 0x9808 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 0]
  > [Timestamps]
    UDP payload (253 bytes)
> Data (253 bytes)
```

```
0000  54 46 17 28 20 a4 2c 6d  c1 4c 4a 73 08 00 45 00   TF·( ·,m ·LJs··E·
0010  01 19 b5 9a 40 00 80 11  00 00 c0 a8 01 06 ac 40   ····@··· ·······@
0020  29 03 c0 2d 01 bb 01 05  98 08 54 01 42 78 c5 84   )··-···· ··T·Bx··
0030  c3 c6 6f 0e 40 3b c5 dc  c3 d4 96 d4 e6 de 5d 00   ··o·@;·· ······]·
0040  07 b2 7b d2 c6 80 5c 7b  b3 46 63 f8 a9 b8 80 01   ··{···\{ ·Fc·····
0050  08 63 f6 83 b8 9d 7d 4e  38 62 1b b9 f1 08 fe f6   ·c····}N 8b······
0060  30 54 73 a6 6d 4d d7 a8  fa 77 66 9d 70 b3 90 10   0Ts·mM·· ·wf·p···
0070  e2 77 3d 92 db c9 59 12  0f 42 d5 3f 23 e2 d5 aa   ·w=···Y· ·B·?#···
0080  57 c4 15 5a b8 4b b6 51  64 9e 01 81 26 e5 14 6f   W··Z·K·Q d···&··o
0090  a1 1f c4 01 77 35 77 11  b0 47 0f d9 a9 0f f2 b7   ····w5w· ·G······
00a0  89 2b ea 22 37 86 78 3e  f3 2f 84 7f c3 62 1a b7   ·+·"7·x> ·/···b··
00b0  96 a8 7d 9c 90 d8 3c 75  a2 52 1a ba 09 5a 31 aa   ··}···<u ·R···Z1·
00c0  43 48 4b 76 a4 df ed 53  6c 36 2a a6 b8 37 74 46   CHKv···S l6*··7tF
00d0  1b c9 db 24 54 0d a9 48  86 16 1b 36 bf 84 72 e3   ···$T··H ···6··r·
00e0  d7 18 94 56 af b7 a3 27  f6 ad 30 15 1d ca ba cd   ···V···' ··0·····
00f0  6d dd b7 34 83 e7 9e 71  f1 18 65 a0 c9 96 0e 6a   m··4···q ··e····j
0100  b1 5e 12 b4 1c c1 d7 9d  51 49 13 13 cf 81 45 5d   ·^······ QI····E]
0110  50 53 09 a5 cb 1e d8 c1  ee e9 fe fd 8c e6 9e e4   PS······ ········
0120  2b a0 5e 5a b5 08 13                               +·^Z···
```

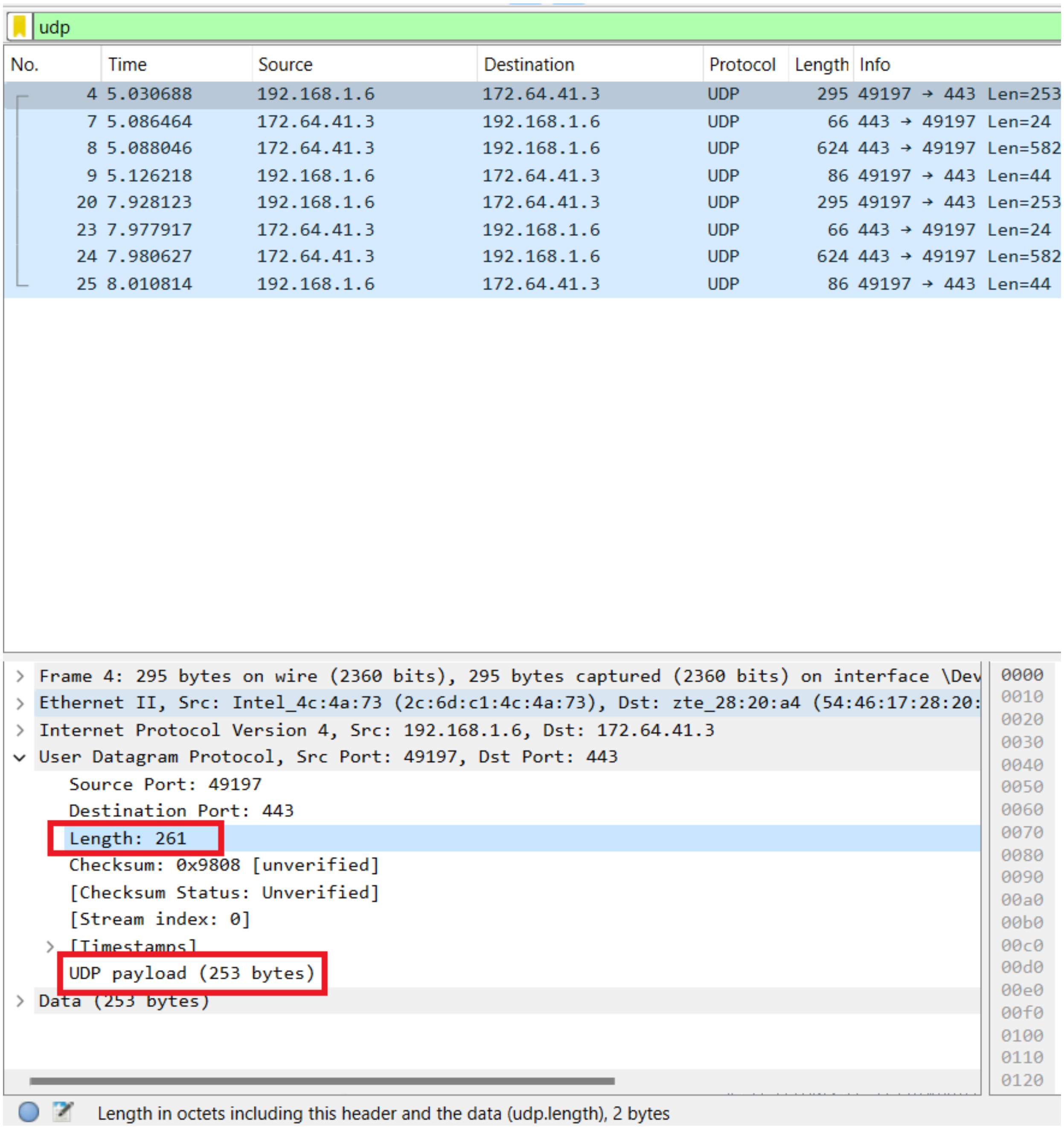
Details at: https://www.wireshark.org/docs/wsug_html_chunked/ChAdvChecksums.html (udp.checksum), 2 bytes

Pack

3. 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 value of the Length field specifies the length in bytes of the entire UDP datagram (including the header and the data).
  Therefore, the length of the UDP payload = Value of Length field - 8

  In the captured UDP packet the value of the Length field is 261. Therefore the length of UDP payload will be 261 - 8 = 253 bytes which is also written in the packet details.



```
udp

No.   Time      Source        Destination   Protocol  Length Info
    4 5.030688  192.168.1.6   172.64.41.3   UDP        295 49197 → 443 Len=253
    7 5.086464  172.64.41.3   192.168.1.6   UDP         66 443 → 49197 Len=24
    8 5.088046  172.64.41.3   192.168.1.6   UDP        624 443 → 49197 Len=582
    9 5.126218  192.168.1.6   172.64.41.3   UDP         86 49197 → 443 Len=44
   20 7.928123  192.168.1.6   172.64.41.3   UDP        295 49197 → 443 Len=253
   23 7.977917  172.64.41.3   192.168.1.6   UDP         66 443 → 49197 Len=24
   24 7.980627  172.64.41.3   192.168.1.6   UDP        624 443 → 49197 Len=582
   25 8.010814  192.168.1.6   172.64.41.3   UDP         86 49197 → 443 Len=44
```

```
> Frame 4: 295 bytes on wire (2360 bits), 295 bytes captured (2360 bits) on interface \Dev    0000
> Ethernet II, Src: Intel_4c:4a:73 (2c:6d:c1:4c:4a:73), Dst: zte_28:20:a4 (54:46:17:28:20:    0010
> Internet Protocol Version 4, Src: 192.168.1.6, Dst: 172.64.41.3                            0020
v User Datagram Protocol, Src Port: 49197, Dst Port: 443                                    0030
     Source Port: 49197                                                                      0040
     Destination Port: 443                                                                   0050
     Length: 261                                                                             0060
     Checksum: 0x9808 [unverified]                                                           0070
     [Checksum Status: Unverified]                                                           0080
     [Stream index: 0]                                                                       0090
   > [Timestamps]                                                                            00a0
     UDP payload (253 bytes)                                                                 00b0
> Data (253 bytes)                                                                           00c0
                                                                                             00d0
                                                                                             00e0
                                                                                             00f0
                                                                                             0100
                                                                                             0110
                                                                                             0120
```

Length in octets including this header and the data (udp.length), 2 bytes

4. What is the maximum number of bytes that can be included in a UDP payload?

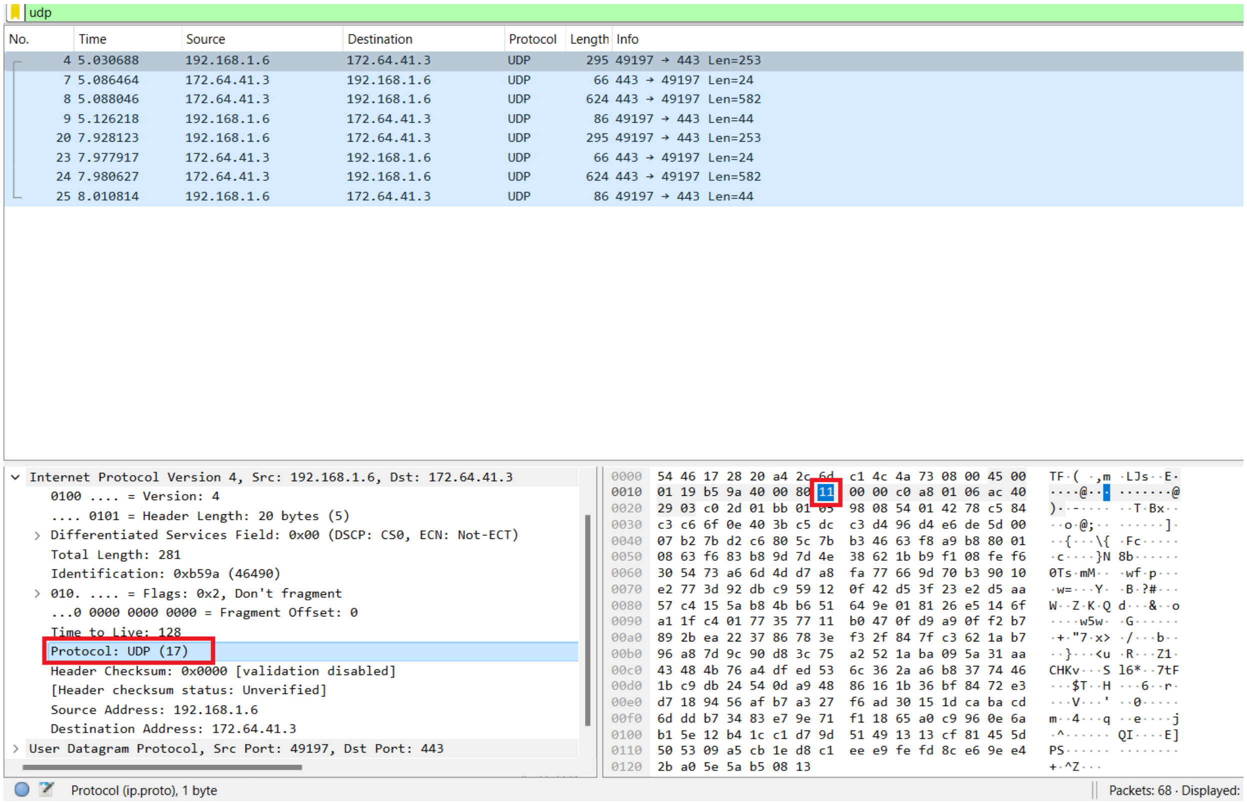
- As the length field has 16 bits, its maximum value is (2^16 - 1) i.e., 65535. The maximum number of bytes that can be included in a UDP payload = 65535 - 8 (UDP headers) - 20 (IP headers) = 65507 bytes.

5. What is the largest possible source port number?

- As the source port number header field in UDP has 16 bits, the largest possible source port number is (2^16 - 1) i.e., 65535.

6. What is the protocol number for UDP?

- The protocol number for UDP is 17 in decimal which in hexadecimal notation is 0x11.



udp

```
No.   Time      Source        Destination   Protocol Length Info
    4 5.030688  192.168.1.6   172.64.41.3   UDP      295 49197 → 443 Len=253
    7 5.086464  172.64.41.3   192.168.1.6   UDP       66 443 → 49197 Len=24
    8 5.088046  172.64.41.3   192.168.1.6   UDP      624 443 → 49197 Len=582
    9 5.126218  192.168.1.6   172.64.41.3   UDP       86 49197 → 443 Len=44
   20 7.928123  192.168.1.6   172.64.41.3   UDP      295 49197 → 443 Len=253
   23 7.977917  172.64.41.3   192.168.1.6   UDP       66 443 → 49197 Len=24
   24 7.980627  172.64.41.3   192.168.1.6   UDP      624 443 → 49197 Len=582
   25 8.010814  192.168.1.6   172.64.41.3   UDP       86 49197 → 443 Len=44
```

```
v Internet Protocol Version 4, Src: 192.168.1.6, Dst: 172.64.41.3
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 281
    Identification: 0xb59a (46490)
  > 010. .... = Flags: 0x2, Don't fragment
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 128
    Protocol: UDP (17)
    Header Checksum: 0x0000 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.1.6
    Destination Address: 172.64.41.3
> User Datagram Protocol, Src Port: 49197, Dst Port: 443
```

```
0000  54 46 17 28 20 a4 2c 6d  c1 4c 4a 73 08 00 45 00   TF·( ·,m ·LJs··E·
0010  01 19 b5 9a 40 00 80 11  00 00 c0 a8 01 06 ac 40   ····@··· ·······@
0020  29 03 c0 2d 01 bb 01 05  98 08 54 01 42 78 c5 84   )·-····· ··T·Bx··
0030  c3 c6 6f 0e 40 3b c5 dc  c3 d4 96 d4 e6 de 5d 00   ··o·@;·· ······]·
0040  07 b2 7b d2 c6 80 5c 7b  b3 46 63 f8 a9 b8 80 01   ··{···\{ ·Fc·····
0050  08 63 f6 83 b8 9d 7d 4e  38 62 1b b9 f1 08 fe f6   ·c····}N 8b······
0060  30 54 73 a6 6d 4d d7 a8  fa 77 66 9d 70 b3 90 10   0Ts·mM·· ·wf·p···
0070  e2 77 3d 92 db c9 59 12  0f 42 d5 3f 23 e2 d5 aa   ·w=···Y· ·B·?#···
0080  57 c4 15 5a b8 4b b6 51  64 9e 01 81 26 e5 14 6f   W··Z·K·Q d···&··o
0090  a1 1f c4 01 77 35 77 11  b0 47 0f d9 a9 0f f2 b7   ····w5w· ·G······
00a0  89 2b ea 22 37 86 78 3e  f3 2f 84 7f c3 62 1a b7   ·+·"7·x> ·/···b··
00b0  96 a8 7d 9c 90 d8 3c 75  a2 52 1a ba 09 5a 31 aa   ··}···<u ·R···Z1·
00c0  43 48 4b 76 a4 df ed 53  6c 36 2a a6 b8 37 74 46   CHKv···S l6*··7tF
00d0  1b c9 db 24 54 0d a9 48  86 16 1b 36 bf 84 72 e3   ···$T··H ···6··r·
00e0  d7 18 94 56 af b7 a3 27  f6 ad 30 15 1d ca ba cd   ···V···' ··0·····
00f0  6d dd b7 34 83 e7 9e 71  f1 18 65 a0 c9 96 0e 6a   m··4···q ··e····j
0100  b1 5e 12 b4 1c c1 d7 9d  51 49 13 13 cf 81 45 5d   ·^······ QI····E]
0110  50 53 09 a5 cb 1e d8 c1  ee e9 fe fd 8c e6 9e e4   PS······ ········
0120  2b a0 5e 5a b5 08 13                               +·^Z···
```

Protocol (ip.proto), 1 byte

Packets: 68 · Displayed: