

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

The image shows a Wireshark packet capture of an HTTP 1.1 GET request. The packet list at the top shows two packets: packet 1521 (GET) and packet 1561 (200 OK). The packet details pane for packet 1521 is expanded, showing the Hypertext Transfer Protocol section. The 'GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n' line is highlighted with a red box. The packet bytes pane at the bottom shows the raw data of the packet.

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 0000 54
> Ethernet II, Src: Intel_4c:4a:73 (2c:6d:c1:4c:4a:73), Dst: zte_28:20:a4 (54:46:17:28:20:a4) 0010 02
> Internet Protocol Version 4, Src: 192.168.1.6, Dst: 128.119.245.12 0020 f5
> Transmission Control Protocol, Src Port: 61852, Dst Port: 80, Seq: 1, Ack: 1, Len: 498 0030 02
> Hypertext Transfer Protocol 0040 68
 > GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n 0050 69
 Host: gaia.cs.umass.edu\r\n 0060 74
 Connection: keep-alive\r\n 0070 73
 Upgrade-Insecure-Requests: 1\r\n 0080 73
 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\n 0090 6e
 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=0.0\r\n 0100 70
 Accept-Encoding: gzip, deflate\r\n 0110 52
 Accept-Language: en-US,en;q=0.9,en-IN;q=0.8\r\n 0120 72
 \r\n 0130 2f
 [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html] 0140 2e
 [HTTP request 1/1] 0150 74
 [Response in frame: 1561]

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 00000000000000000000000000000000

> Ethernet II, Src: Intel_4c:4a:73 (2c:6d:c1:4c:4a:73), Dst: zte_28:20:a4 (54:46:17:28:20:a4) 00000000000000000000000000000000

> Internet Protocol Version 4, Src: 192.168.1.6, Dst: 128.119.245.12 00000000000000000000000000000000

> Transmission Control Protocol, Src Port: 61852, Dst Port: 80, Seq: 1, Ack: 1, Len: 498 00000000000000000000000000000000

> Hypertext Transfer Protocol 00000000000000000000000000000000

> 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\n

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=0.0\r\n

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
 > 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

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

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/122.0.0.0\r\n
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\r\n
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

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						
Line-based text data: text/html (10 lines) \n <html>\n \n Congratulations again! Now you've downloaded the file lab2-2.html. \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 \n will only be sent once by the server due to the inclusion of the IN-MODIFIED-SINCE \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.

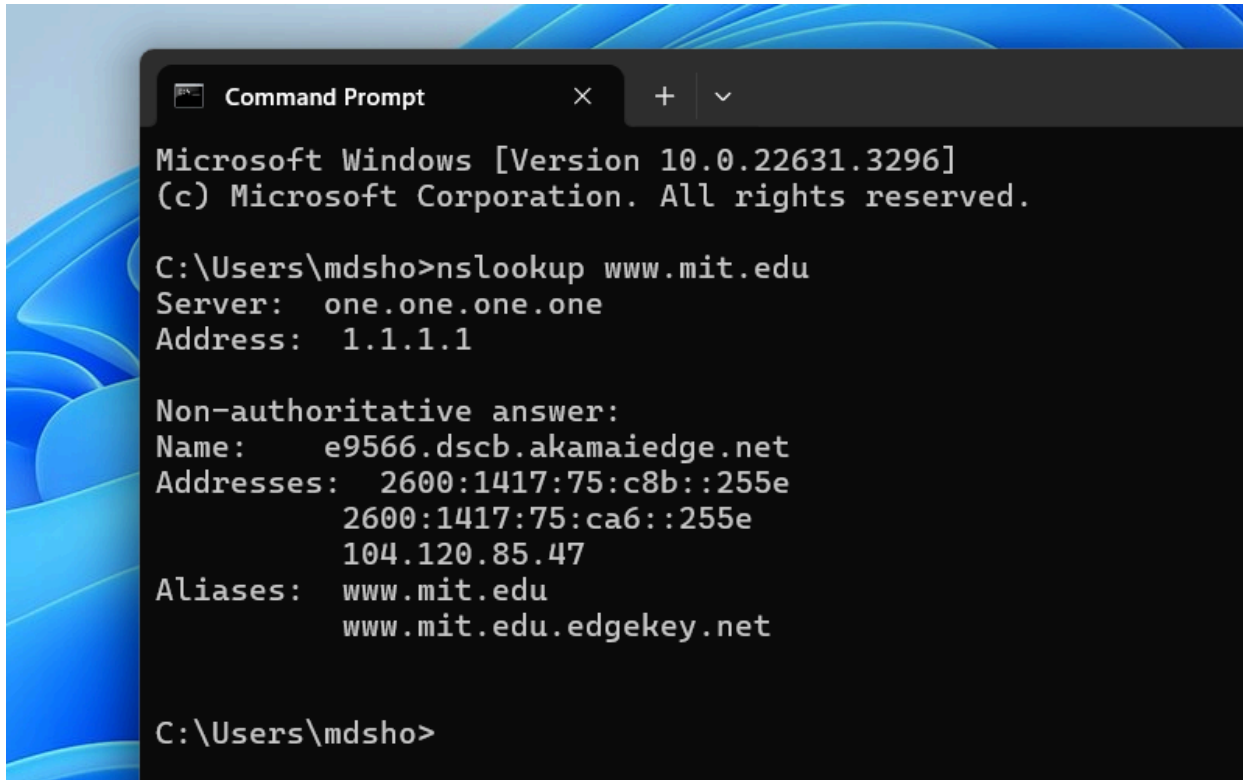
DNS ASSIGNMENT

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.

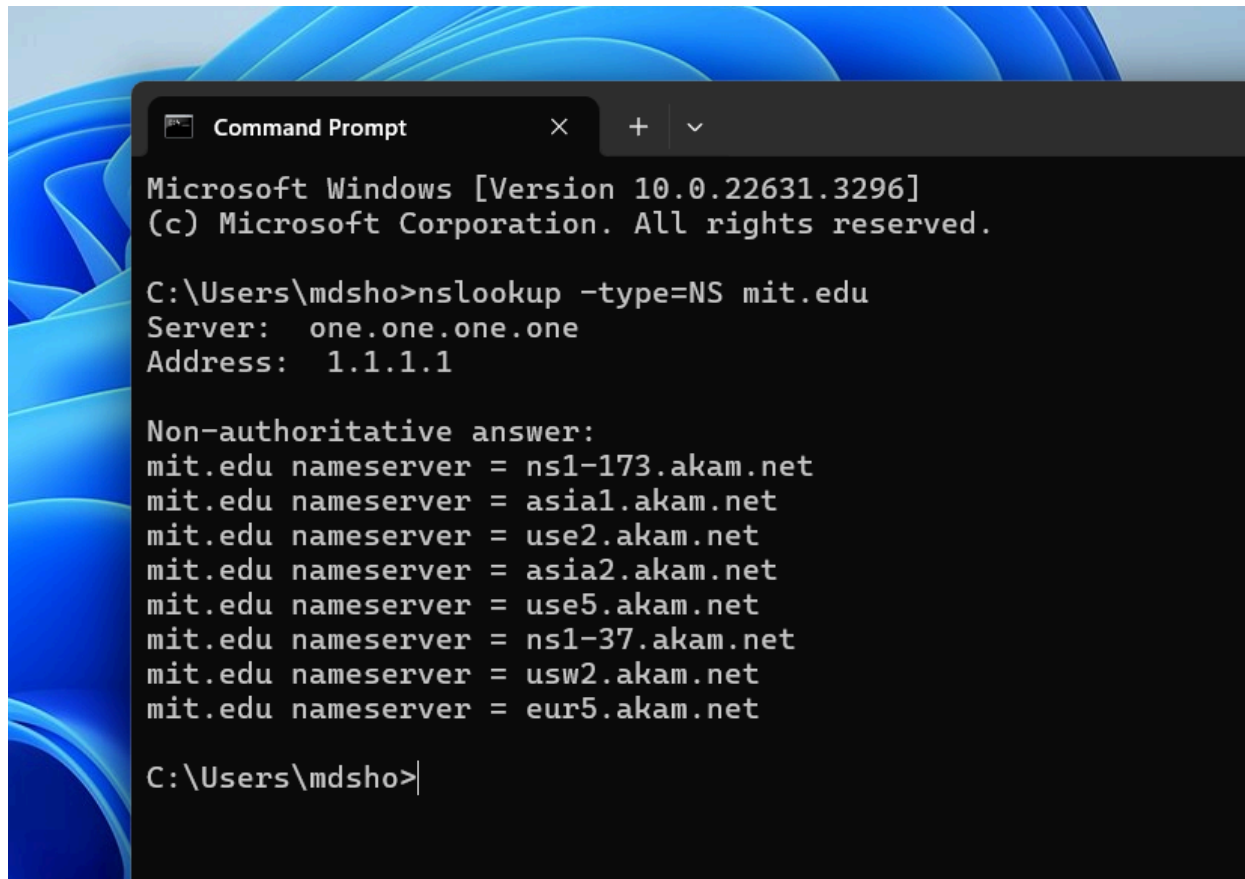
C:\Users\mdsho>nslookup www.mit.edu
Server:     one.one.one.one
Address:    1.1.1.1

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.

```

Command Prompt

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}	0000 54 46 17 28 20 a4 2c 6d c1 4c
> Ethernet II, Src: Intel_4c:4a:73 (2c:6d:c1:4c:4a:73), Dst: zte_28:20:a4 (54:46:17:28:20:a4)	0010 00 3a 1d 17 00 00 80 11 00 00
> Internet Protocol Version 4, Src: 192.168.1.6, Dst: 8.8.8.8	0020 08 08 e8 39 00 35 00 26 d1 f5
> User Datagram Protocol, Src Port: 59449, Dst Port: 53	0030 00 00 00 00 00 00 03 77 77 77
> Source Port: 59449	0040 6f 72 67 00 00 01 00 01
> Destination Port: 53	
> Length: 38	
> Checksum: 0xd1f5 [unverified]	
> [Checksum Status: Unverified]	
> [Stream index: 0]	
> [Timestamps]	
> UDP payload (30 bytes)	
> 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]	

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_{61610ABB-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

▼ 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)

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 104.16.44.99
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_{61610ABB-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

▼ 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)

```
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
```

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 [1
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	9.216605	128.119.245.12	192.168.1.6	TCP	54	80 → 52972 [ACK] Seq=1 Ack=152960 Win=260056 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

▼ 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=152060 Win=260056 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

▼ 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=40050 Win=111332 Len=0

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:

- 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.
- What is the value of the Acknowledgement field in the SYNACK segment?
 - The value of the Acknowledgement field in the SYNACK segment is 1319426792.
- 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.
- 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	52972 → 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 → 52972 [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	52972 → 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=40059 Win=111232 Len=0

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 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=111776 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)	<pre> 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-labs/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-Host: gaia 0070 2e 63 73 2e 75 6d 61 73 73 2e 65 64 75 0d 0a 43 .cs.umass.edu-CC 0080 6f 6e 6e 65 63 74 69 6f 6e 3a 20 6b 65 65 70 2d onnection: keep- 0090 61 6c 69 76 65 0d 0a 43 6f 6e 74 65 6e 74 2d 4c alive-Content-L 00a0 65 6e 67 74 68 3a 20 31 35 32 33 32 31 0d 0a 43 ength: 1 52321-CC 00b0 61 63 68 65 2d 43 6f 6e 74 72 6f 6c 3a 20 6d 61 ache-Content: 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 -Insecure-Request 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: Mozilla/5.0 (</pre>
---	---

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)

tcpstream eq 1						
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=44038 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=55359 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	8.902618	192.168.1.6	192.168.1.6	TCP	64	80 → 63077 [RST] Seq=1 Ack=60760 Win=16800 Len=0
<div> <div> <div> <div>Ethernet II, Src: Intel_Ac4a73 (2c:6d:c1:4c:4a:73), Dst: gte_2b20:a4 (08:00:2b:20:a4:00)</div> <div>Internet Protocol Version 4, Src: 192.168.1.6, Dst: 128.119.245.12</div> <div>Transmission Control Protocol, Src Port: 52972, Dst Port: 80, Seq: 1, Ack: 639, Len: 638, Window: 132352, Options: 65535, 65536, 65537, 65538, 65539, 65540, 65541, 65542, 65543, 65544, 65545, 65546, 65547, 65548, 65549, 65550, 65551, 65552, 65553, 65554, 65555, 65556, 65557, 65558, 65559, 65560, 65561, 65562, 65563, 65564, 65565, 65566, 65567, 65568, 65569, 65570, 65571, 65572, 65573, 65574, 65575, 65576, 65577, 65578, 65579, 65580, 65581, 65582, 65583, 65584, 65585, 65586, 65587, 65588, 65589, 65590, 65591, 65592, 65593, 65594, 65595, 65596, 65597, 65598, 65599, 65600, 65601, 65602, 65603, 65604, 65605, 65606, 65607, 65608, 65609, 65610, 65611, 65612, 65613, 65614, 65615, 65616, 65617, 65618, 65619, 65620, 65621, 65622, 65623, 65624, 65625, 65626, 65627, 65628, 65629, 65630, 65631, 65632, 65633, 65634, 65635, 65636, 65637, 65638, 65639, 65640, 65641, 65642, 65643, 65644, 65645, 65646, 65647, 65648, 65649, 65650, 65651, 65652, 65653, 65654, 65655, 65656, 65657, 65658, 65659, 65660, 65661, 65662, 65663, 65664, 65665, 65666, 65667, 65668, 65669, 65670, 65671, 65672, 65673, 65674, 65675, 65676, 65677, 65678, 65679, 65680, 65681, 65682, 65683, 65684, 65685, 65686, 65687, 65688, 65689, 65690, 65691, 65692, 65693, 65694, 65695, 65696, 65697, 65698, 65699, 65700, 65701, 65702, 65703, 65704, 65705, 65706, 65707, 65708, 65709, 65710, 65711, 65712, 65713, 65714, 65715, 65716, 65717, 65718, 65719, 65720, 65721, 65722, 65723, 65724, 65725, 65726, 65727, 65728, 65729, 65730, 65731, 65732, 65733, 65734, 65735, 65736, 65737, 65738, 65739, 65740, 65741, 65742, 65743, 65744, 65745, 65746, 65747, 65748, 65749, 65750, 65751, 65752, 65753, 65754, 65755, 65756, 65757, 65758, 65759, 65760, 65761, 65762, 65763, 65764, 65765, 65766, 65767, 65768, 65769, 65770, 65771, 65772, 65773, 65774, 65775, 65776, 65777, 65778, 65779, 65780, 65781, 65782, 65783, 65784, 65785, 65786, 65787, 65788, 65789, 65790, 65791, 65792, 65793, 65794, 65795, 65796, 65797, 65798, 65799, 65800, 65801, 65802, 65803, 65804, 65805, 65806, 65807, 65808, 65809, 65810, 65811, 65812, 65813, 65814, 65815, 65816, 65817, 65818, 65819, 65820, 65821, 65822, 65823, 65824, 65825, 65826, 65827, 65828, 65829, 65830, 65831, 65832, 65833, 65834, 65835, 65836, 65837, 65838, 65839, 65840, 65841, 65842, 65843, 65844, 65845, 65846, 65847, 65848, 65849, 65850, 65851, 65852, 65853, 65854, 65855, 65856, 65857, 65858, 65859, 65860, 65861, 65862, 65863, 65864, 65865, 65866, 65867, 65868, 65869, 65870, 65871, 65872, 65873, 65874, 65875, 65876, 65877, 65878, 65879, 65880, 65881, 65882, 65883, 65884, 65885, 65886, 65887, 65888, 65889, 65890, 65891, 65892, 65893, 65894, 65895, 65896, 65897, 65898, 65899, 65900, 65901, 65902, 65903, 65904, 65905, 65906, 65907, 65908, 65909, 65910, 65911, 65912, 65913, 65914, 65915, 65916, 65917, 65918, 65919, 65920, 65921, 65922, 65923, 65924, 65925, 65926, 65927, 65928, 65929, 65930, 65931, 65932, 65933, 65934, 65935, 65936, 65937, 65938, 65939, 65940, 65941, 65942, 65943, 65944, 65945, 65946, 65947, 65948, 65949, 65950, 65951, 65952, 65953, 65954, 65955, 65956, 65957, 65958, 65959, 65960, 65961, 65962, 65963, 65964, 65965, 65966, 65967, 65968, 65969, 65970, 65971, 65972, 65973, 65974, 65975, 65976, 65977, 65978, 65979, 65980, 65981, 65982, 65983, 65984, 65985, 65986, 65987, 65988, 65989, 65990, 65991, 65992, 65993, 65994, 65995, 65996, 65997, 65998, 65999, 66000, 66001, 66002, 66003, 66004, 66005, 66006, 66007, 66008, 66009, 66010, 66011, 66012, 66013, 66014, 66015, 66016, 66017, 66018, 66019, 66020, 66021, 66022, 66023, 66024, 66025, 66026, 66027, 66028, 66029, 66030, 66031, 66032, 66033, 66034, 66035, 66036, 66037, 66038, 66039, 66040, 66041, 66042, 66043, 66044, 66045, 66046, 66047, 66048, 66049, 66050, 66051, 66052, 66053, 66054, 66055, 66056, 66057, 66058, 66059, 66060, 66061, 66062, 66063, 66064, 66065, 66066, 66067, 66068, 66069, 66070, 66071, 66072, 66073, 66074, 66075, 66076, 66077, 66078, 66079, 66080, 66081, 66082, 66083, 66084, 66085, 66086, 66087, 66088, 66089, 66090, 66091, 66092, 66093, 66094, 66095, 66096, 66097, 66098, 66099, 66100, 66101, 66102, 66103, 66104, 66105, 66106, 66107, 66108, 66109, 66110, 66111, 66112, 66113, 66114, 66115, 66116, 66117, 66118, 66119, 66120, 66121, 66122, 66123, 66124, 66125, 66126, 66127, 66128, 66129, 66130, 66131, 66132, 66133, 66134, 66135, 66136, 66137, 66138, 66139, 66140, 66141, 66142, 66143, 66144, 66145, 66146, 66147, 66148, 66149, 66150, 66151, 66152, 66153, 66154, 66155, 66156, 66157, 66158, 66159, 66160, 66161, 66162, 66163, 66164, 66165, 66166, 66167, 66168, 66169, 66170, 66171, 66172, 66173, 66174, 66175, 66176, 66177, 66178, 66179, 66180, 66181, 66182, 66183, 66184, 66185, 66186, 66187, 66188, 66189, 66190, 66191, 66192, 66193, 66194, 66195, 66196, 66197, 66198, 66199, 66200, 66201, 66202, 66203, 66204, 66205, 66206, 66207, 66208, 66209, 66210, 66211, 66212, 66213, 66214, 66215, 66216, 66217, 66218, 66219, 66220, 66221, 66222, 66223, 66224, 66225, 66226, 66227, 66228, 66229, 66230, 66231, 66232, 66233, 66234, 66235, 66236, 66237, 66238, 66239, 66240, 66241, 66242, 66243, 66244, 66245, 66246, 66247, 66248, 66249, 66250, 66251, 66252, 66253, 66254, 66255, 66256, 66257, 66258, 66259, 66260, 66261, 66262, 66263, 66264, 66265, 66266, 66267, 66268, 66269, 66270, 66271, 66272, 66273, 66274, 66275, 66276, 66277, 66278, 66279, 66280, 66281, 66282, 66283, 66284, 66285, 66286, 66287, 66288, 66289, 66290, 66291, 66292, 66293, 66294, 66295, 66296, 66297, 66298, 66299, 66300, 66301, 66302, 66303, 66304, 66305, 66306, 66307, 66308, 66309, 66310, 66311, 66312, 66313, 66314, 66315, 66316, 66317, 66318, 66319, 66320, 66321, 66322, 66323, 66324, 66325, 66326, 66327, 66328, 66329, 66330, 66331, 66332, 66333, 66334, 66335, 66336, 66337, 66338, 66339, 66340, 66341, 66342, 66343, 66344, 66345, 66346, 66347, 66348, 66349, 66350, 66351, 66352, 66353, 66354, 66355, 66356, 66357, 66358, 66359, 66360, 66361, 66362, 66363, 66364, 66365, 66366, 66367, 66368, 66369, 66370, 66371, 66372, 66373, 66374, 66375, 66376, 66377, 66378, 66379, 66380, 66381, 66382, 66383, 66384, 66385, 66386, 66387, 66388, 66389, 66390, 66391, 66392, 66393, 66394, 66395, 66396, 66397, 66398, 66399, 66400, 66401, 66402, 66403, 66404, 66405, 66406, 66407, 66408, 66409, 66410, 66411, 66412, 66413, 66414, 66415, 66416, 66417, 66418, 66419, 66420, 66421, 66422, 66423, 66424, 66425, 66426, 66427, 66428, 66429, 66430, 66431, 66432, 66433, 66434, 66435, 66436, 66437, 66438, 66439, 66440, 66441, 66442, 66443, 66444, 66445, 66446, 66447, 66448, 66449, 66450, 66451, 66452, 66453, 66454, 66455, 66456, 66457, 66458, 66459, 66460, 66461, 66462, 66463, 66464, 66465, 66466, 66467, 66468, 66469, 66470, 66471, 66472, 66473, 66474, 66475, 66476, 66477, 66478, 66479, 66480, 66481, 66482, 66483, 66484, 66485, 66486, 66487, 66488, 66489, 66490, 66491, 66492, 66493, 66494, 66495, 66496, 66497, 66498, 66499, 66500, 66501, 66502, 66503, 66504, 66505, 66506, 66507, 66508, 66509, 66510, 66511, 66512, 66513, 66514, 66515, 66516, 66517, 66518, 66519, 66520, 66521, 66522, 66523, 66524, 66525, 66526, 66527, 66528, 66529, 66530, 66531, 66532, 66533, 66534, 66535, 66536, 66537, 66538, 66539, 66540, 66541, 66542, 66543, 66544, 66545, 66546, 66547, 66548, 66549, 66550, 66551, 66552, 66553, 66554, 66555, 66556, 66557, 66558, 66559, 66560, 66561, 66562, 66563, 66564, 66565, 66566, 66567, 66568, 66569, 66570, 66571, 66572, 66573, 66574, 66575, 66576, 66577, 66578, 66579, 66580, 66581, 66582, 66583, 66584, 66585, 66586, 66587, 66588, 66589, 66590, 66591, 66592, 66593, 66594, 66595, 66596, 66597, 66598, 66599, 66600, 66601, 66602, 66603, 66604, 66605, 66606, 66607, 66608, 66609, 66610, 66611, 66612, 66613, 66614, 66615, 66616, 66617, 66618, 66619, 66620, 66621, 66622, 66623, 66624, 66625, 66626, 66627, 66628, 66629, 66630, 66631, 66632, 66633, 66634, 66635, 66636, 66637, 66638, 66639, 66640, 66641, 66642, 66643, 66644, 66645, 66646, 66647, 66648, 66649, 66650, 66651, 66652, 66653, 66654, 66655, 66656, 66657, 66658, 66659, 66660, 66661, 66662, 66663, 66664, 66665, 66666, 66667, 66668, 66669, 66670, 66671, 66672, 66673, 66674, 66675, 66676, 66677, 66678, 66679, 66680, 66681, 66682, 66683, 66684, 66685, 66686, 66687, 66688, 66689, 66690, 66691, 66692, 66693, 66694, 66695, 66696, 66697, 66698, 66699, 66700, 66701, 66702, 66703, 66704, 66705, 66706, 66707, 66708, 66709, 66710, 66711, 66712, 66713, 66714, 66715, 66716, 66717, 66718, 66719, 66720, 66721, 66722, 66723, 66724, 66725, 66726, 66727, 66728, 66729, 66730, 66731, 66732, 66733, 66734, 66735, 66736, 66737, 66738, 66739, 66740, 66741, 66742, 66743, 66744, 66745, 66746, 66747, 66748, 66749, 66750, 66751, 66752, 66753, 66754, 66755, 66756, 66757, 66758, 66759, 66760, 66761, 66762, 66763, 66764, 66765, 66766, 66767, 66768, 66769, 66770, 66771, 66772, 66773, 66774, 66775, 66776, 66777, 66778, 66779, 66780, 66781, 66782, 66783, 66784, 66785, 66786, 66787, 66788, 66789, 66790, 66791, 66792, 66793, 66794, 66795, 66796, 66797, 66798, 66799, 66800, 66801, 66802, 66803, 66804, 66805, 66806, 66807, 66808, 66809, 66810, 66811, 66812, 66813, 66814, 66815, 66816, 66817, 66818, 66819, 66820, 66821, 66822, 66823, 66824, 66825, 66826, 66827, 66828, 66829, 66830, 66831, 66832, 66833, 66834, 66835, 66836, 66837, 66838, 66839, 66840, 66841, 66842, 66843, 66844, 66845, 66846, 66847, 66848, 66849, 66850, 66851, 66852, 66853, 66854, 66855, 66856, 66857, 66858, 66859, 66860, 66861, 66862, 66863, 66864, 66865, 66866, 66867, 66868, 66869, 66870, 66871, 66872, 66873, 66874, 66875, 66876, 66877, 66878, 66879, 66880, 66881, 66882, 66883, 66884, 66885, 66886, 66887, 66888, 66889, 66890, 66891, 66892, 66893, 66894, 66895, 66896, 66897, 66898, 66899, 66900, 66901, 66902, 66903, 66904, 66905, 66906, 66907, 66908, 66909, 66910, 66911, 66912, 66913, 66914, 66915, 66916, 66917, 66918, 66919, 66920, 66921, 66922, 66923, 66924, 66925, 66926, 66927, 66928, 66929, 66930, 66931, 66932, 66933, 66934, 66935, 6</div></div></div></div>						

- $\text{EstimatedRTT} = 0.875 * \text{EstimatedRTT} + 0.125 * \text{SampleRTT}$

EstimatedRTT after the receipt of the ACK of segment 1:

$\text{EstimatedRTT} = \text{RTT for Segment 1} = 0.354951 \text{ sec}$

EstimatedRTT after the receipt of the ACK of segment 2:

$\text{EstimatedRTT} = 0.875 * 0.354951 + 0.125 * 0.354668 = 0.354915$

sec

EstimatedRTT after the receipt of the ACK of segment 3:

$\text{EstimatedRTT} = 0.875 * 0.354915 + 0.125 * 0.307175 = 0.348947$

EstimatedRTT after the receipt of the ACK of segment 4:

$\text{EstimatedRTT} = 0.875 * 0.348947 + 0.125 * 0.303040 = 0.343208$

EstimatedRTT after the receipt of the ACK of segment 5:

$\text{EstimatedRTT} = 0.875 * 0.343208 + 0.125 * 0.314162 = 0.339577$

EstimatedRTT after the receipt of the ACK of segment 6:

$\text{EstimatedRTT} = 0.875 * 0.339577 + 0.125 * 0.314015 = 0.336381$

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.

- Throughput = Calculated Window Size / (Time difference between the first segment sent and the last segment sent)

$$\begin{aligned}\text{Throughput} &= 269056 / (9.216685 - 7.939672) \\ &= 210691.669 \text{ bits/sec} \\ &= 26.336 \text{ KByte / sec}\end{aligned}$$

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 many 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 reassembled data stream]
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: 2182

[Calculated window size: 269056]

[Window size scaling factor: 128]

Checksum: 0xb690 [unverified]

[Checksum Status: Unverified]

Urgent Pointer: 0

> [Timestamps]

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-...}		0000	54 46 17 28
> Ethernet II, Src: Intel_4c:4a:73 (2c:6d:c1:4c:4a:73), Dst: zte_28:20:a4 (54:46:17:28:20:a4)		0010	01 19 b5 9a
> Internet Protocol Version 4, Src: 192.168.1.6, Dst: 172.64.41.3		0020	29 03 c0 2d
✓ User Datagram Protocol, Src Port: 49197, Dst Port: 443		0030	c3 c6 6f 0e
Source Port: 49197		0040	07 b2 7b d2
Destination Port: 443		0050	08 63 f6 83
Length: 261		0060	30 54 73 a6
Checksum: 0x9808 [unverified]		0070	e2 77 3d 92
[Checksum Status: Unverified]		0080	57 c4 15 5a
[Stream index: 0]		0090	a1 1f c4 01
> [Timestamps]		00a0	89 2b ea 22
UDP payload (253 bytes)		00b0	96 a8 7d 9c
> Data (253 bytes)		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.

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) on interface eth0

> Ethernet II, Src: Intel_4c:4a:73 (2c:6d:c1:4c:4a:73), Dst: zte_2 (8c:8e:ac:4d:00:00)

> Internet Protocol Version 4, Src: 192.168.1.6, Dst: 172.64.41.3

▼ 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 05 c0 26 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  ....5W-.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 c6 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  6d 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-.-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
    
```

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		0000	54 46 17 28 20 a4 2c 6d	c1 4c 4a 73 08 00 45 00	TF (, m - L J s - - E -
> Ethernet II, Src: Intel_4c:4a:73 (2c:6d:c1:4c:4a:73), Dst: zte_2		0010	01 19 b5 9a 48 00 80 11	00 00 c0 a8 01 06 ac 40	- - - - - @ - - - - - @
> Internet Protocol Version 4, Src: 192.168.1.6, Dst: 172.64.41.3		0020	29 03 c0 2d 01 b6 91 05	98 08 54 01 42 78 c5 84	- - - - - T - B x - -
v User Datagram Protocol, Src Port: 49197, Dst Port: 443		0030	c3 c6 6f 0e 40 50 c5 dc	c3 d4 96 d4 e6 de 5d 00	- - o - @ ; - - - - -] -
Source Port: 49197		0040	07 b2 7b d2 c6 80 5c 7b	b3 46 63 f8 a9 b8 80 01	- - { - - - - } - F c - - - -
Destination Port: 443		0050	08 63 f6 83 b8 9d 7d 4e	38 62 1b b9 f1 08 fe f6	- c - - - - } N 8 b - - - -
Length: 261		0060	30 54 73 a6 6d 4d d7 a8	fa 77 66 9d 70 b3 90 10	0 T s - m M - - - w f . p - -
Checksum: 0x9808 [unverified]		0070	e2 77 3d 92 db c9 59 12	0f 42 d5 3f 23 e2 d5 aa	- w = - - - Y - - B - ? # - -
[Checksum Status: Unverified]		0080	57 c4 15 5a b8 4b b6 51	64 9e 01 81 26 e5 14 6f	W - - Z . K . Q d - - & - - o
[Stream index: 0]		0090	a1 1f c4 01 77 35 77 11	b0 47 0f d9 a9 0f f2 b7	- - - - w 5 w - - G - - - -
> [Timestamps]		00a0	89 2b ea 22 37 86 78 3e	f3 2f 84 7f c3 62 1a b7	- + - " 7 . x > - / - - - b -
UDP payload (253 bytes)		00b0	96 a8 7d 9c 90 d8 3c 75	a2 52 1a ba 09 5a 31 aa	- - } - - - < u - R - - - Z 1 -
> Data (253 bytes)		00c0	43 48 4b 76 a4 df ed 53	6c 36 2a a6 b8 37 74 46	CH K v - - - S 1 6 * - - 7 t F
		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	- ^ - - - - - Q I - - - - E]
		0110	50 53 09 a5 cb 1e d8 c1	ee e9 fe fd 8c e6 9e e4	P S - - - - - - - - - - -
		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) on interface 0

> Ethernet II, Src: Intel_4c:4a:73 (2c:6d:c1:4c:4a:73), Dst: zte_2 (88:ee:5f:ca:f7:9a)

> Internet Protocol Version 4, Src: 192.168.1.6, Dst: 172.64.41.3

> 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 .LJsE..
0010  01 19 b5 9a 40 00 80 11 00 00 c0 a8 01 06 ac 40   ...@... ..T.Bx...
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 ab 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...ZtF
00c0  43 48 4b 76 a4 df ed 53 6c 36 2a a6 b8 37 74 46   CHKV...S 16*-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...

```

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) on interface 0

> Ethernet II, Src: Intel_4c:4a:73 (2c:6d:c1:4c:4a:73), Dst: zte_2 (8c:8e:9f:3c:00:00)

> Internet Protocol Version 4, Src: 192.168.1.6, Dst: 172.64.41.3

> 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 16*-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

```

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

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.

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

> Ethernet II, Src: Intel_4c:4a:73 (2c:6d:c1:4c:4a:73), Dst: zte_28:20:a4 (54:46:17:28:20:

> Internet Protocol Version 4, Src: 192.168.1.6, Dst: 172.64.41.3

✓ 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

0010

0020

0030

0040

0050

0060

0070

0080

0090

00a0

00b0

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.

The image shows a Wireshark packet capture of a UDP packet. The top section displays a list of packets, with packet 25 selected. The packet list shows the following details:

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

The bottom section shows the details of the selected packet (25). The details pane is expanded to show the 'User Datagram Protocol' section. The protocol number is highlighted as 17 (0x11) in the 'Protocol' field. The details pane also shows the 'Internet Protocol Version 4' section, which includes the source and destination addresses (192.168.1.6 and 172.64.41.3) and the source and destination ports (49197 and 443).

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

Protocol (ip.proto), 1 byte

Packets: 68 · Displayed: