

Computer Networks Assignment - 1

Submitted By: N V H Sowndarya
Email ID: sowndaryanookala.vh@uga.edu

Submission Date: 24th February,23
UGA ID: 811594990

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

The IP address of a server in Asia (www.iiit.ac.in) is 196.12.53.50



```
Windows PowerShell

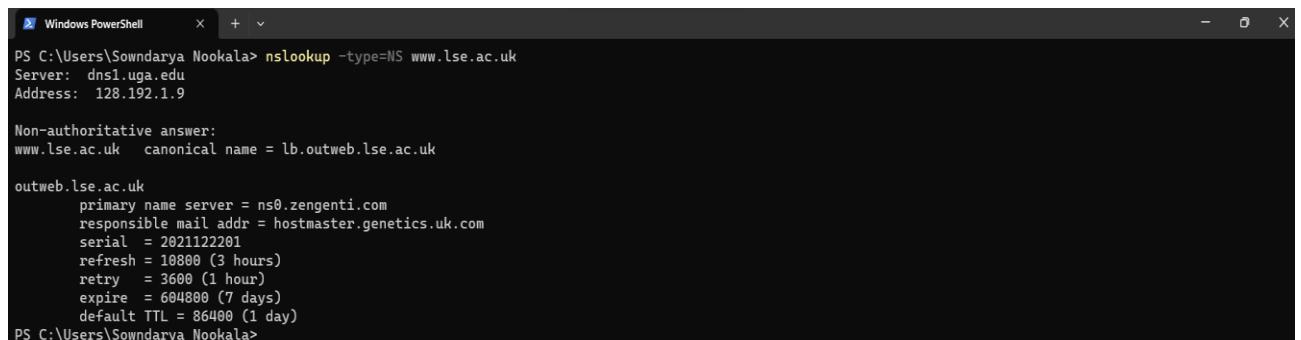
PS C:\Users\Sowndarya Nookala> nslookup www.iiit.ac.in
Server: dns1.uga.edu
Address: 128.192.1.9

Non-authoritative answer:
Name: www.iiit.ac.in
Address: 196.12.53.50

PS C:\Users\Sowndarya Nookala>
```

2. Run *nslookup* to determine the authoritative DNS servers for a university in Europe.

The authoritative DNS servers for London School of Economics and Political Science in United Kingdom, Europe with (<https://www.lse.ac.uk/>) is ns0.zengenti.com



```
Windows PowerShell

PS C:\Users\Sowndarya Nookala> nslookup -type=NS www.lse.ac.uk
Server: dns1.uga.edu
Address: 128.192.1.9

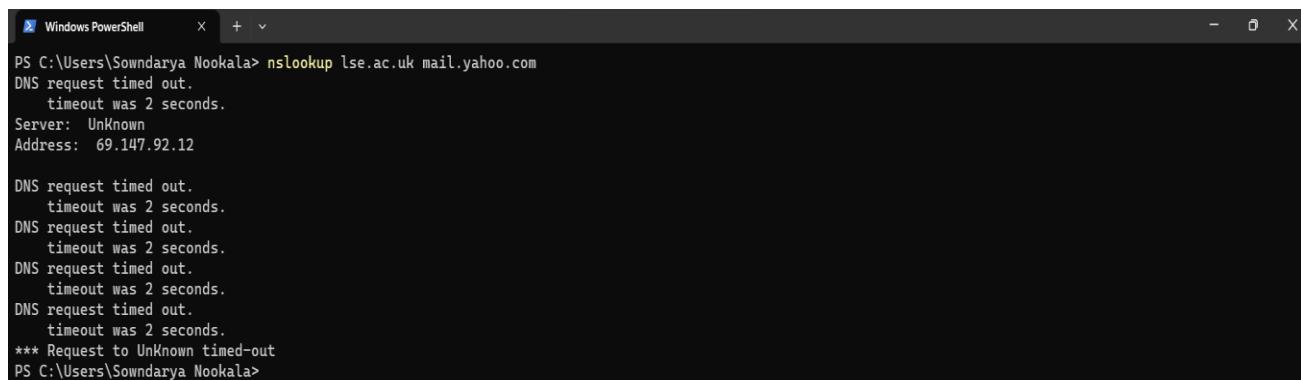
Non-authoritative answer:
www.lse.ac.uk canonical name = lb.outweb.lse.ac.uk

outweb.lse.ac.uk
    primary name server = ns0.zengenti.com
    responsible mail addr = hostmaster.genetics.uk.com
    serial = 2021122201
    refresh = 10800 (3 hours)
    retry = 3600 (1 hour)
    expire = 604800 (7 days)
    default TTL = 86400 (1 day)

PS C:\Users\Sowndarya Nookala>
```

3. Run *nslookup* so that one of the DNS servers obtained in Question 2 is queried for the mail servers for Yahoo! mail. What is its IP address?

The IP address after querying lse.ac.uk with yahoo mail server using the nslookup is 69.147.92.12



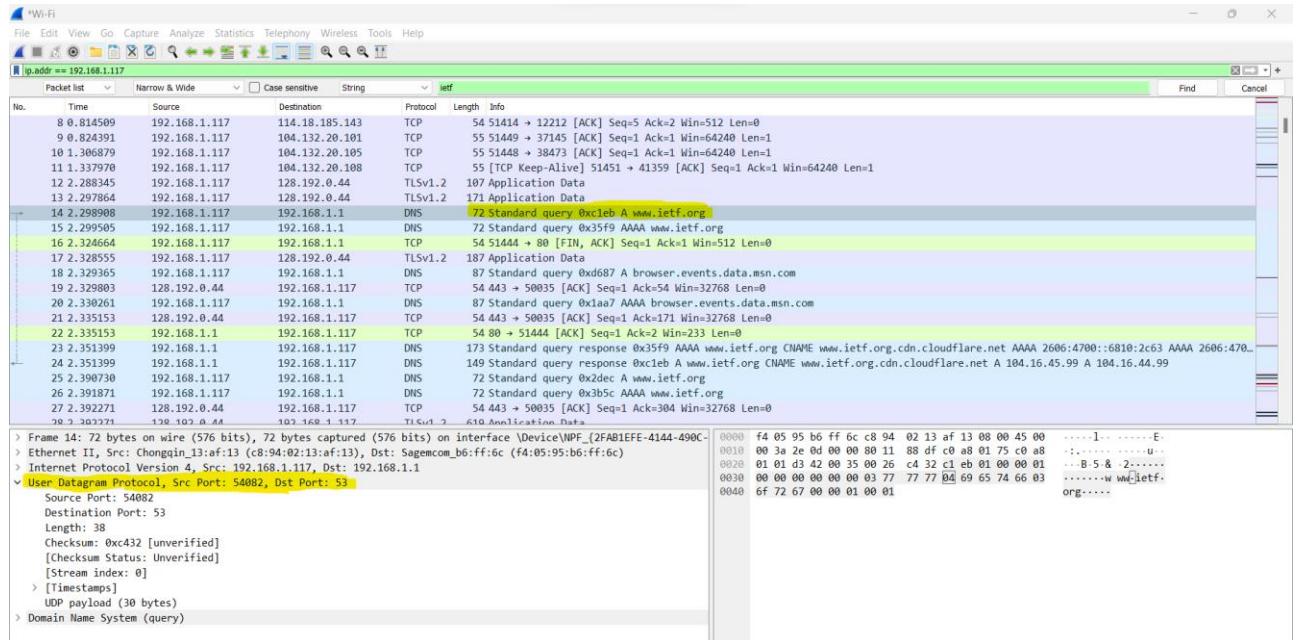
```
Windows PowerShell

PS C:\Users\Sowndarya Nookala> nslookup lse.ac.uk mail.yahoo.com
DNS request timed out.
    timeout was 2 seconds.
Server: Unknown
Address: 69.147.92.12

DNS request timed out.
    timeout was 2 seconds.
*** Request to Unknown timed-out
PS C:\Users\Sowndarya Nookala>
```

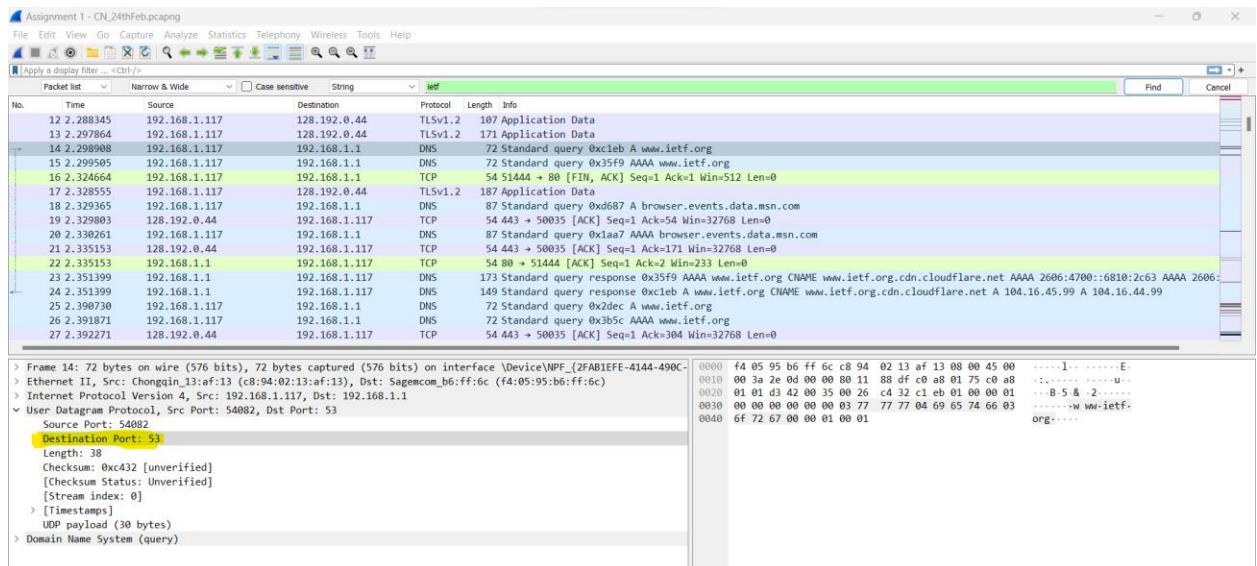
4. Locate the DNS query and response messages. Are they sent over UDP or TCP?

The DNS query and response messages are sent over User Datagram Protocol (UDP).

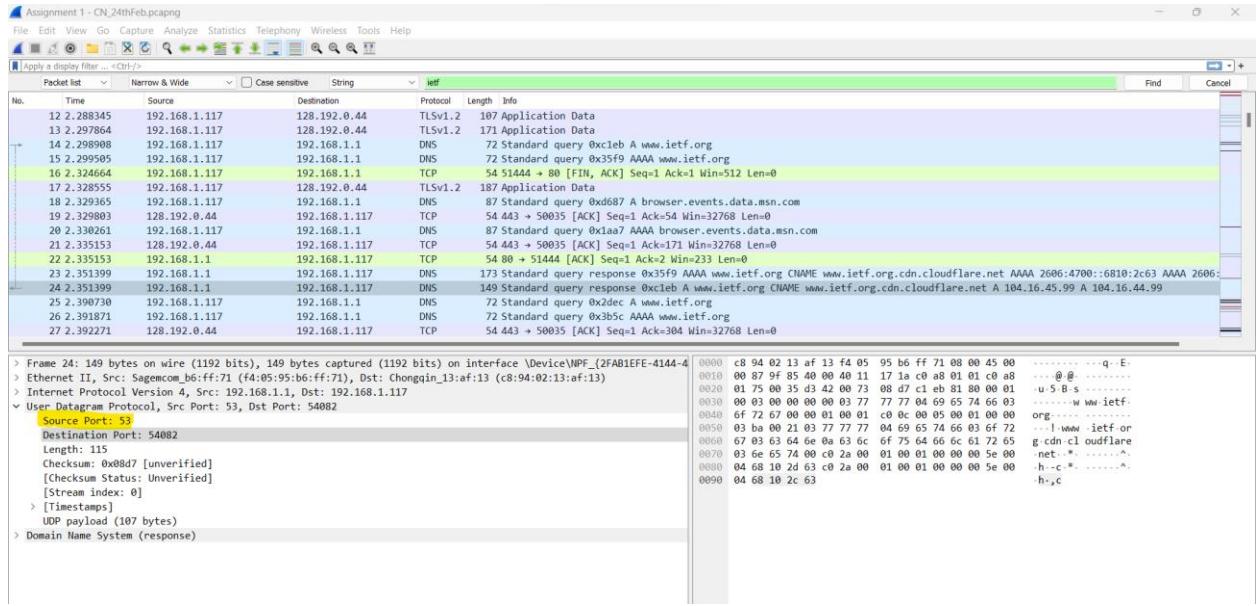


5. What is the destination port for the DNS query message? What is the source port of DNS response message?

The Source port is 54082 and the Destination port is 53 for the DNS query message.

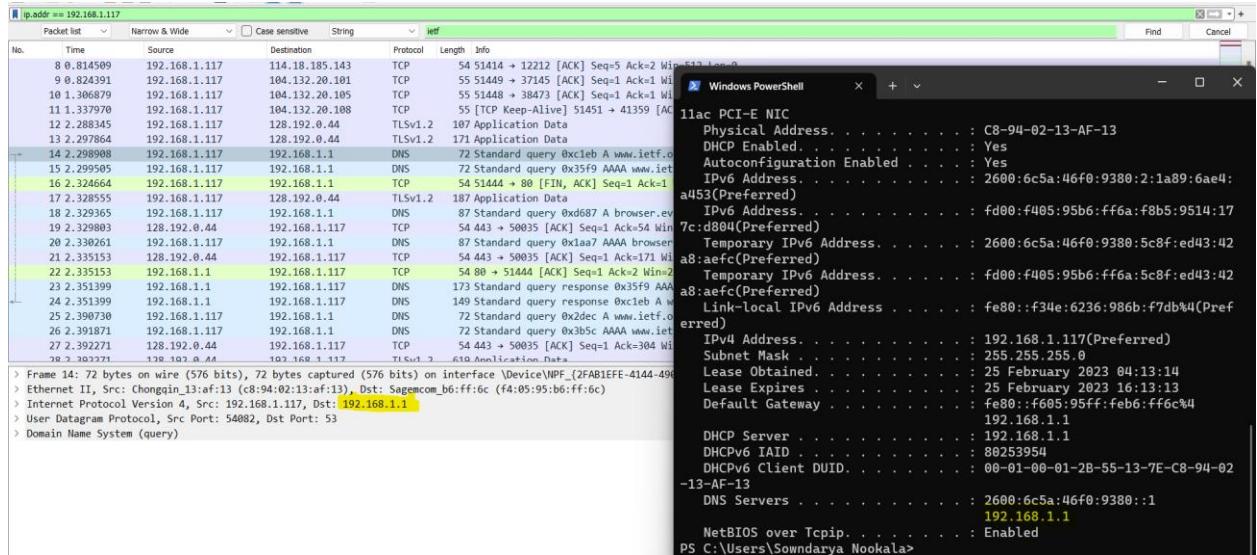


The Source port is 53 and the Destination port is 54082 for the DNS response message.



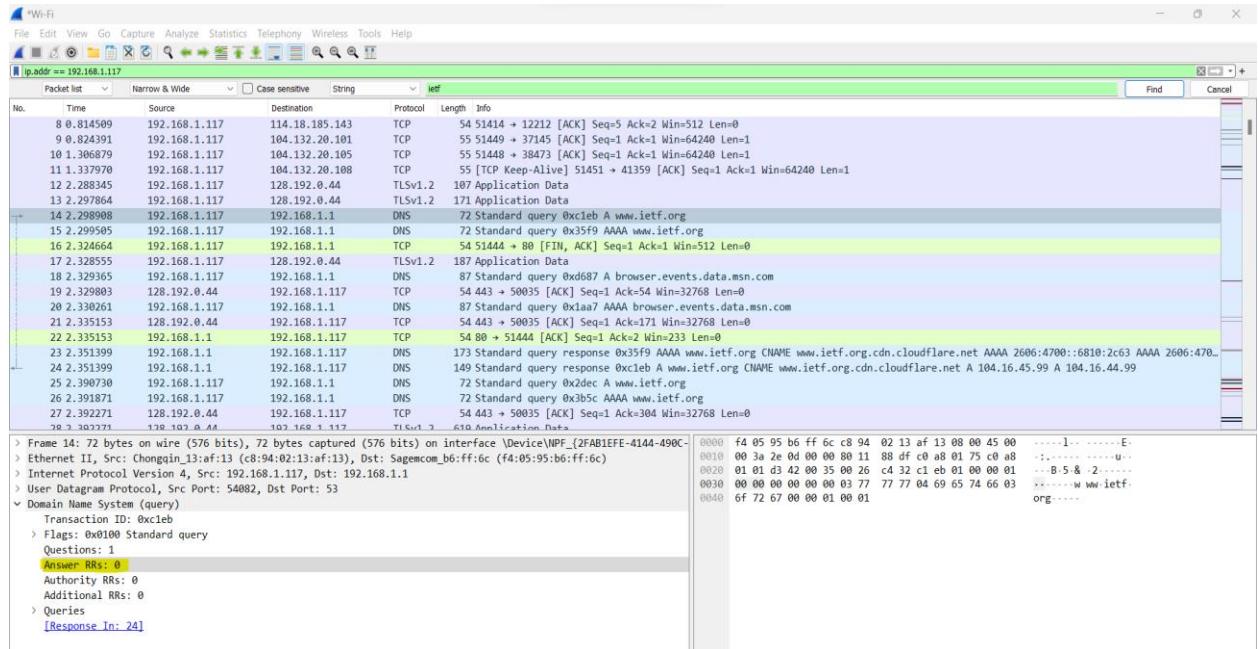
6. To what IP address is the DNS query message sent? Use ipconfig to determine the IP address of your local DNS server. Are these two IP addresses the same?

The DNS query messages are sent to 192.168.1.1 which is same as local address.



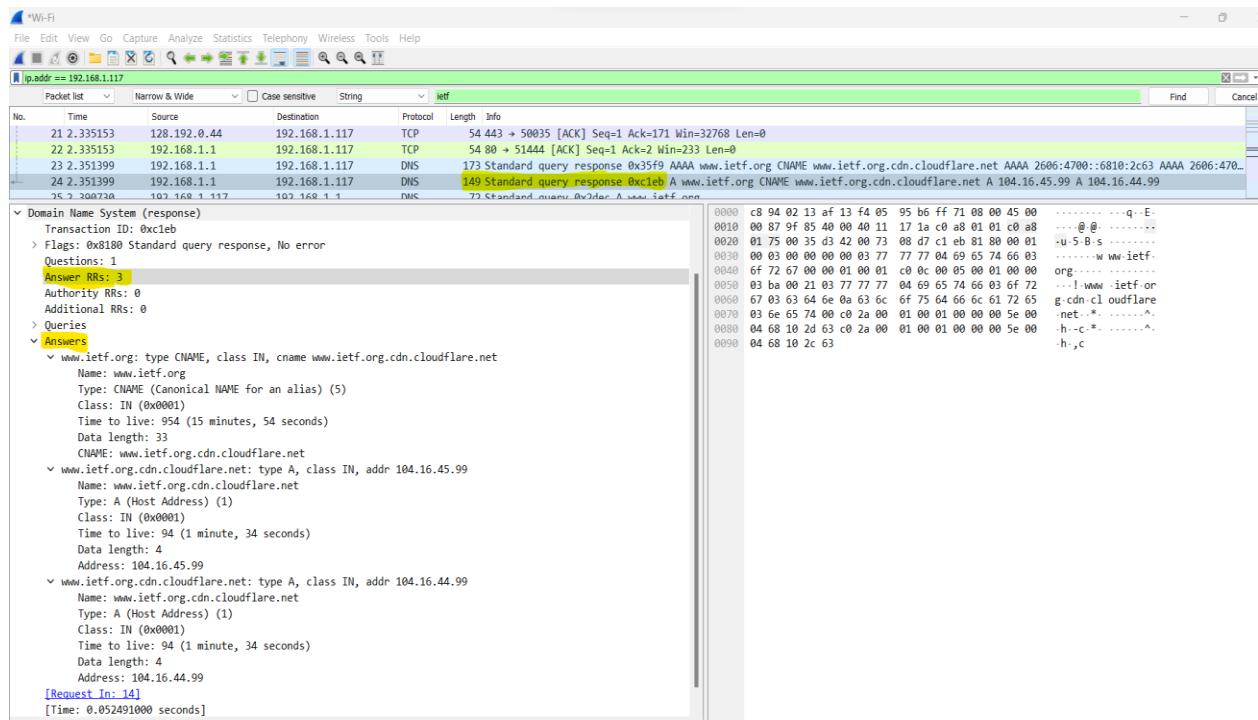
7. Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”?

The Type of DNS query is of Type A. The query does not contain any answers.



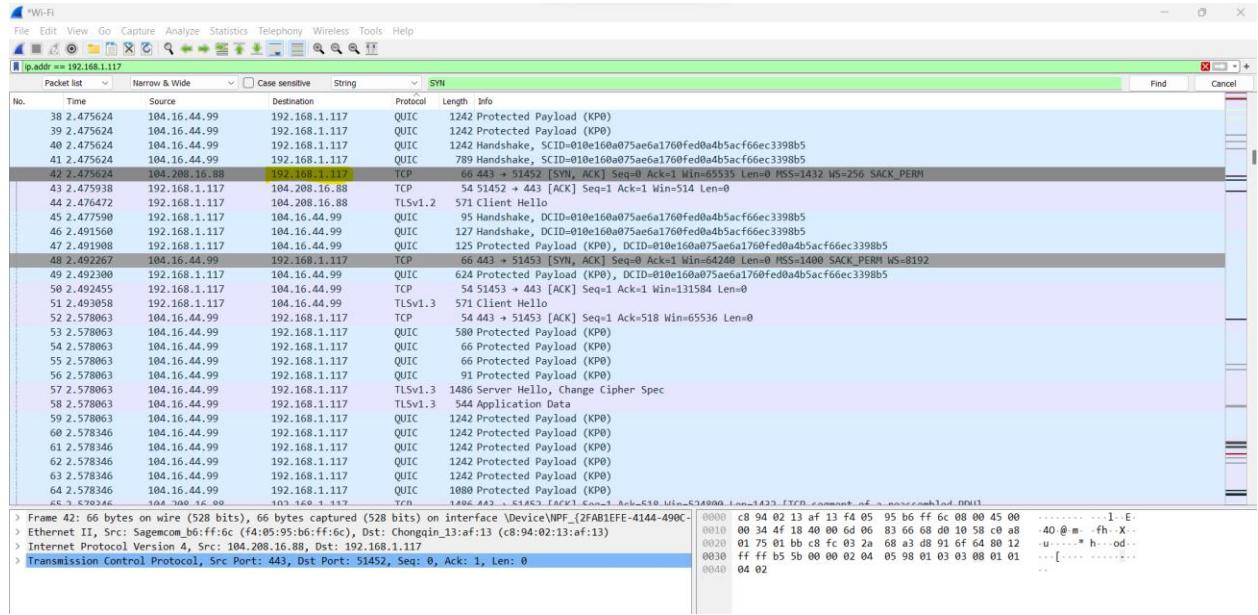
8. Examine the DNS response message. How many “answers” are provided? What do each of these answers contain?

For DNS response messages, three answers are retrieved. The answer contains namespace, type, class and address of that web address.



- 9. Consider the subsequent TCP SYN packet sent by your host. Does the destination IP address of the SYN packet correspond to any of the IP addresses provided in the DNS response message?**

The SYN packet's destination IP address matches the IP addresses provided in the DNS response message that is 192.168.1.117



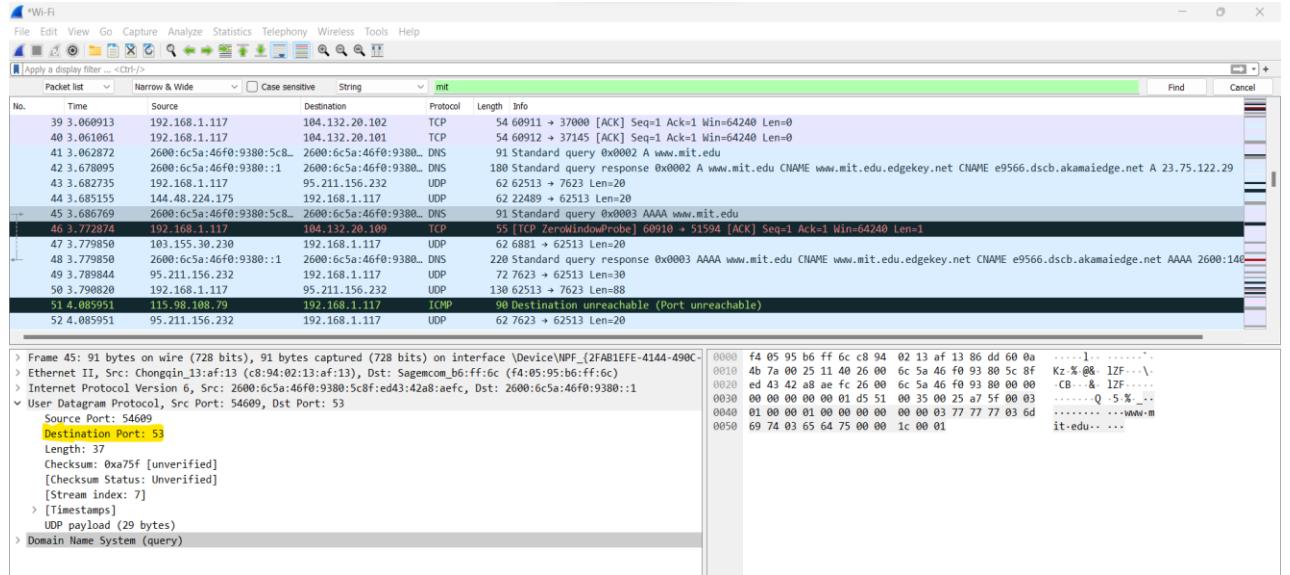
- 10. This web page contains images. Before retrieving each image, does your host issue new DNS queries?**

No, the host is not issuing new DNS queries before retrieving images.

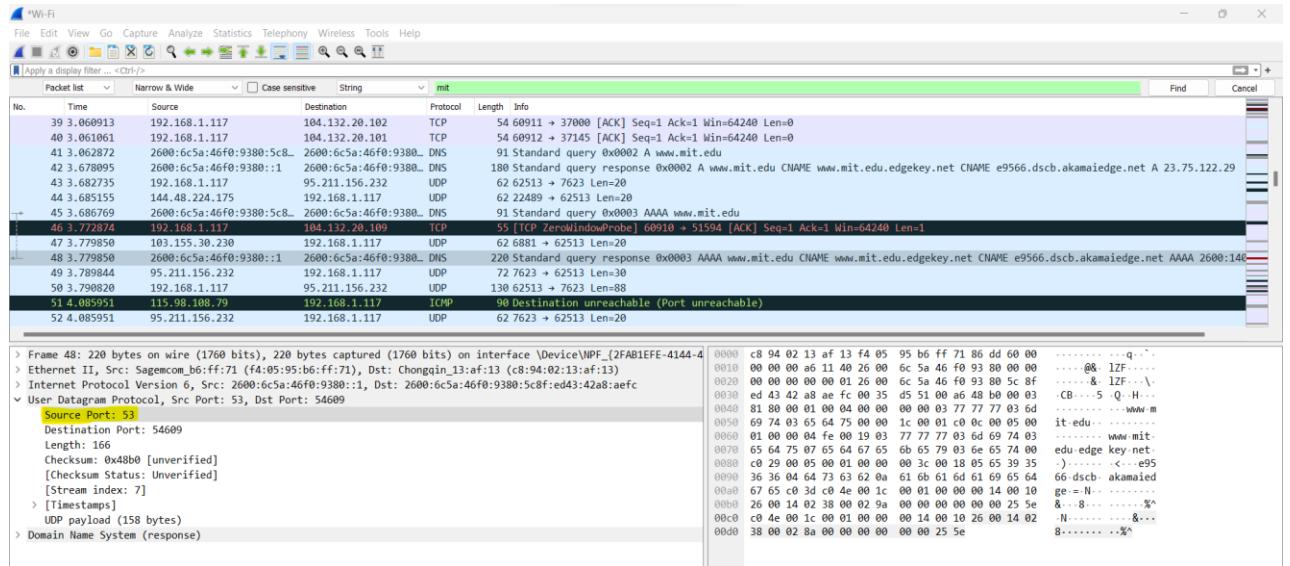
- 11. What is the destination port for the DNS query message? What is the source port of DNS response message?**

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

For Query Message - Source Port: 54609 Destination Port: 53

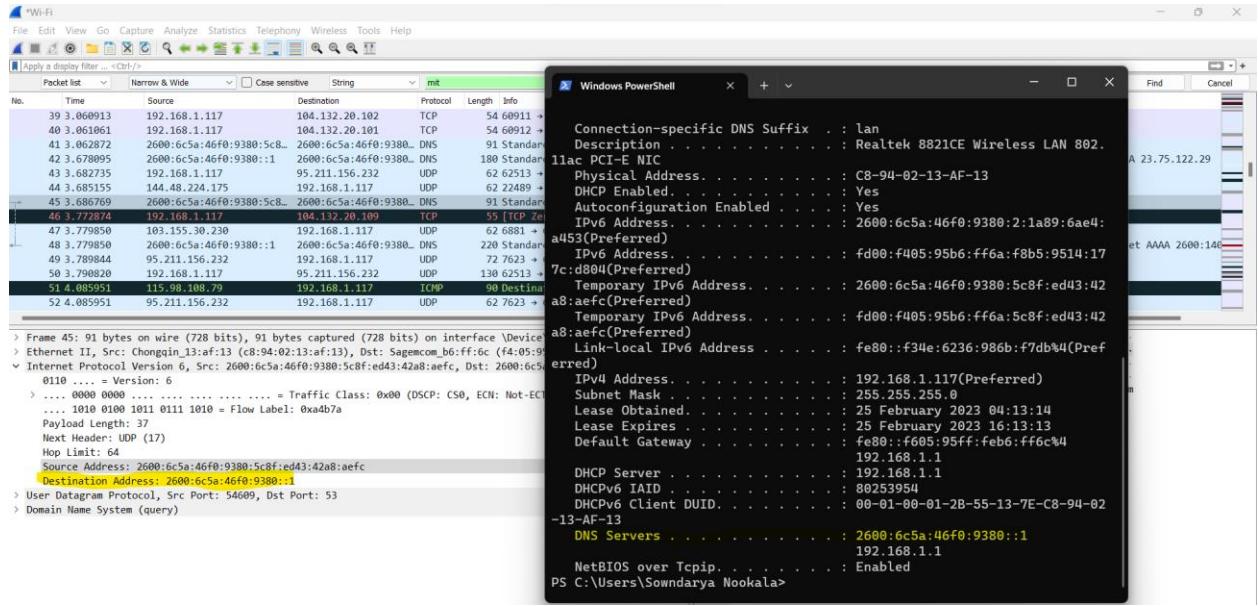


For Response Message - Source Port: 53 Destination Port: 54609



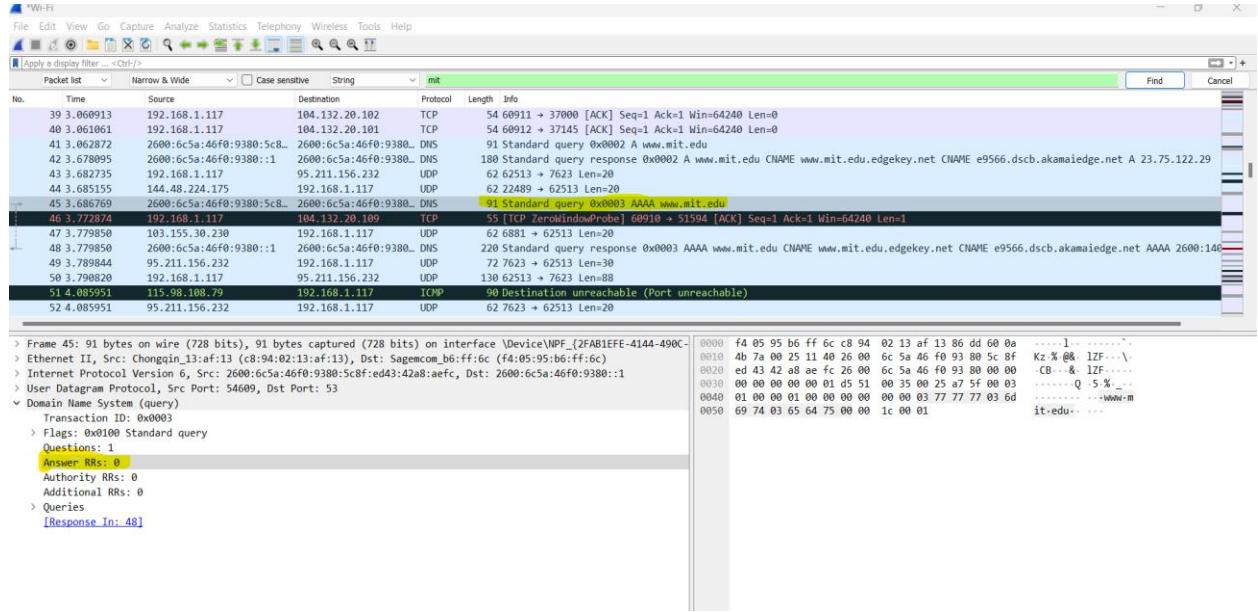
12. To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server?

The DNS query message is sent to the IP address(v6) 2600:6c5a:46f0:9380::1
Yes, this is same as my local DNS server.



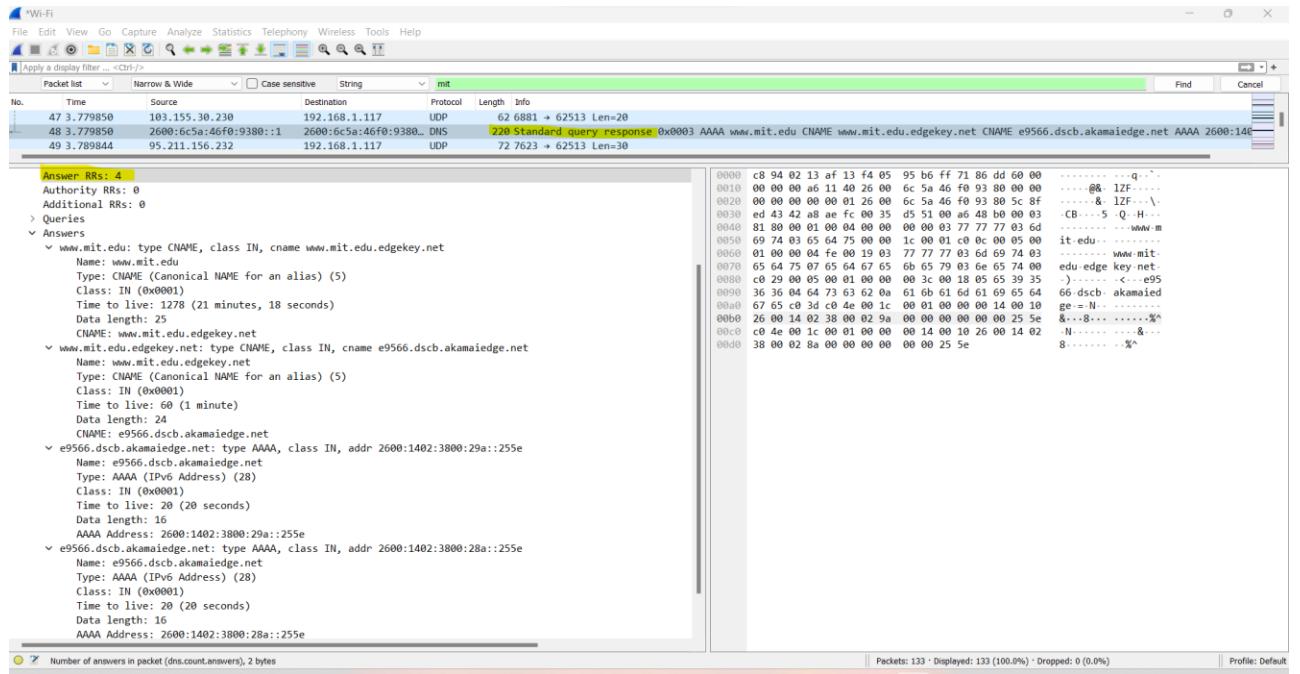
13. Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”?

This is DNS query is of TYPE AAAA and it doesn't contain any answers.

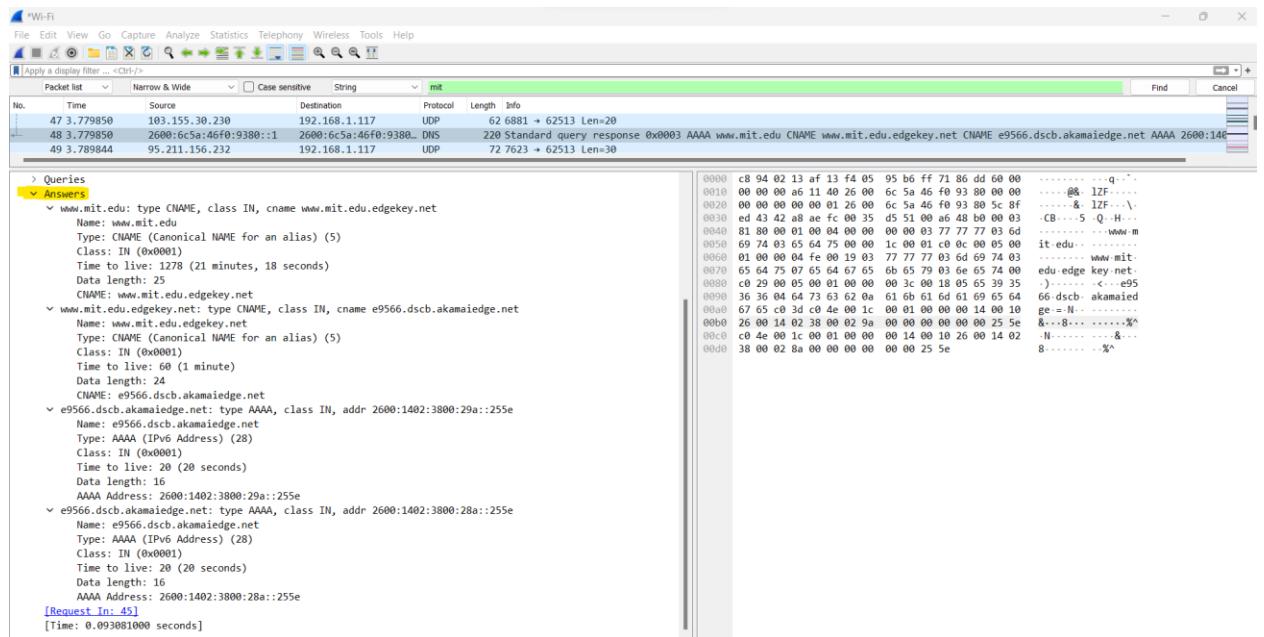


14. Examine the DNS response message. How many “answers” are provided? What do each of these answers contain?

Four answers are provided in the DNS response message.

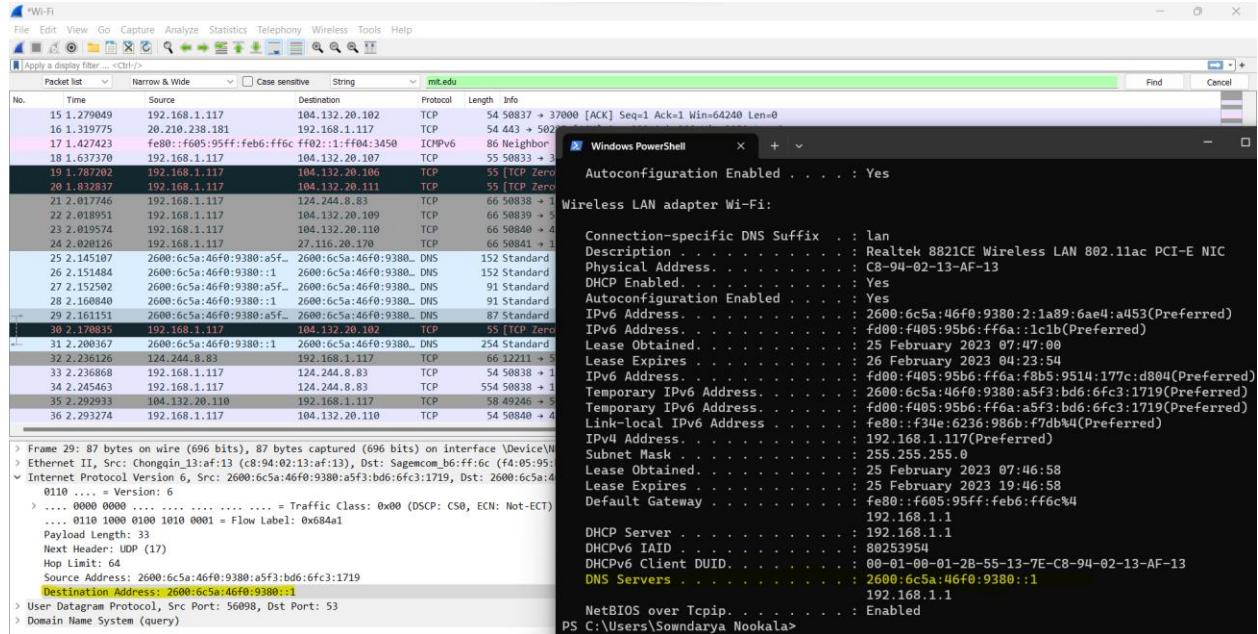


15. Provide a screenshot.



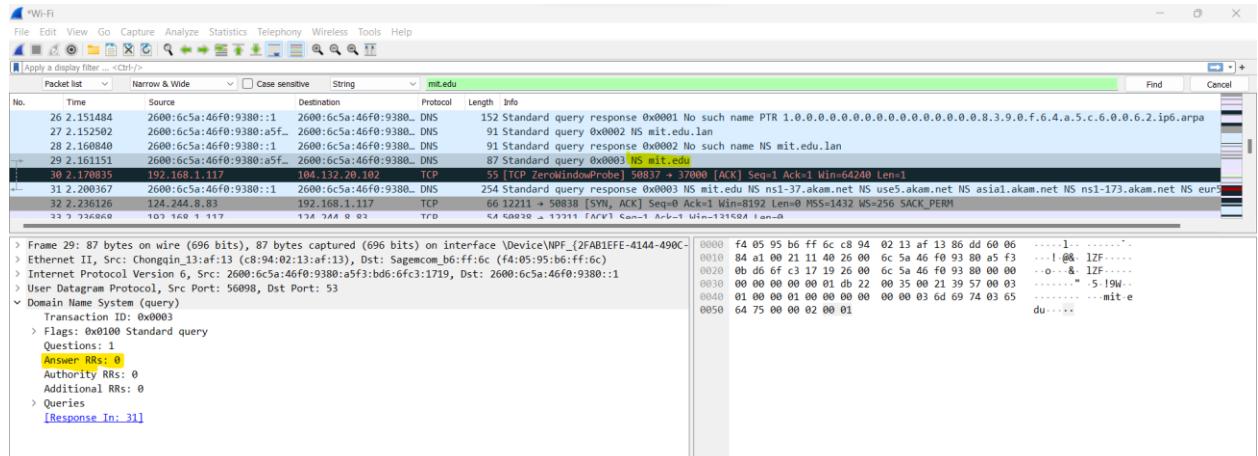
16. To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server?

The DNS query message is sent to the IP address 2600:6c5a:46f0:9380::1
Yes, this is same as my local DNS server.



17. Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”?

The DNS query message is of Type: NS, this doesn't contain any answers.



18. Examine the DNS response message. What MIT nameservers does the response message provide? Does this response message also provide the IP addresses of the MIT nameservers?

There are 8 nameservers in the DNS response message. No, the response message does not include IP addresses of the nameservers.

+ 29 2.161151	2600:6c5a:46f0:9380:a5f..	2600:6c5a:46f0:9380.. DNS	87 Standard query 0x0003 NS mit.edu
30 2.170835	192.168.1.117	104.132.20.102 TCP	55 [TCP ZeroWindowProbe] 50837 → 37000 [ACK] Seq=1 Ack=1 Win=64240 Len=1
+ 31 2.200367	2600:6c5a:46f0:9380::1	2600:6c5a:46f0:9380.. DNS	254 Standard query response 0x0003 NS mit.edu NS ns1-37.akam.net NS use5.akam.net NS asia1.akam.net NS ns1-173.akam.net NS eur5.akam.net
+ 32 2.236126	124.244.8.83	192.168.1.117 TCP	66 12211 → 50838 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1432 WS=256 SACK_PERM
+ 33 2.236469	102.160.1.117	194.74.8.93 TPD	CA 60039 → 17711 [ARV1] Seq=1 Arv=1 Win=131404 Len=8

> Frame 31: 254 bytes on wire (2032 bits), 254 bytes captured (2032 bits) on interface \Device\NPF_{2FAB1EFE-4144-4

- > Ethernet II, Src: Sagemcom_b6:ff:6c (f4:05:95:b6:ff:6c), Dst: Chongain_13:af:13 (c8:94:02:13:af:13)
- > Internet Protocol Version 6, Src: 2600:6c5a:46f0:9380::1, Dst: 2600:6c5a:46f0:9380:a5f3:bd6:6fc3:1719
- > User Datagram Protocol, Src Port: 53, Dst Port: 56098
- > Domain Name System (response)
 - Transaction ID: 0x0003
 - Flags: 0x0100
 - Questions: 1
 - Answer RRs: 8**
 - Authority RRs: 0
 - Additional RRs: 0
 - Queries

19. Provide a screenshot.

<pre>> Queries < Answers > mit.edu: type NS, class IN, ns ns1-37.akam.net > mit.edu: type NS, class IN, ns use5.akam.net > mit.edu: type NS, class IN, ns asia1.akam.net > mit.edu: type NS, class IN, ns ns1-173.akam.net > mit.edu: type NS, class IN, ns eur5.akam.net > mit.edu: type NS, class IN, ns asia2.akam.net > mit.edu: type NS, class IN, ns use2.akam.net > mit.edu: type NS, class IN, ns usw2.akam.net [Request In: 29] [Time: 0.039210000 seconds]</pre>	<pre>0000 c8 94 02 13 af 13 f4 05 95 b6 ff 6c 86 dd 60 00 1.- 0010 00 00 00 c8 94 02 13 af 13 f4 05 95 b6 ff 6c 86 dd 60 00@. 12f.- 0020 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00&. 12f.- 0030 00 d6 ff c3 17 19 00 35 db 22 00 c6 61 58 00o. 5. ah.- 0040 81 00 00 01 00 00 00 00 00 00 03 fd 69 74 03 65 mit-e 0050 64 75 00 00 02 00 01 c9 0c 00 02 00 01 00 00 06 du.- 0060 35 08 11 06 6e 73 31 2d 33 37 04 61 60 61 62 03 5...ns1- 37. 0070 6e 65 74 00 c9 0c 00 02 00 01 00 00 06 35 00 07 net.- 0080 04 75 73 65 35 c9 2c c0 0c 00 02 00 01 00 00 06 use5.- 0090 35 00 08 05 61 73 69 61 31 c9 2c c0 0c 00 02 00 5...asia 1.- 00a0 01 00 00 06 35 00 08 07 6e 73 31 2d 31 37 33 c05... ns1-173 00b0 2c c0 0c 00 02 00 01 00 00 06 35 00 07 04 65 75 ,.....5...eu 00c0 72 35 c9 2c c0 0c 00 02 00 01 00 00 06 35 00 08 r5.- 00d0 05 61 73 69 61 32 c0 2c c0 0c 00 02 00 01 00 00 r5...asia2.- 00e0 06 35 00 07 04 75 73 65 32 c0 2c c0 0c 00 02 00 5...use 2.- 00f0 01 00 00 06 35 00 07 04 75 73 77 32 c0 2c5...usw2.- </pre>
--	---

20. To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server? If not, what does the IP address correspond to?

The query was sent to a two different IP addresses which are 192.168.1.1 and 18.0.72.3 and one of the IP addresses is same as my local.

<p>File Edit View Go Capture Analyze Statistics Telephone Wireless Tools Help</p> <p>dns</p> <table border="1"> <thead> <tr> <th>No.</th><th>Time</th><th>Source</th><th>Destination</th><th>Protocol</th><th>Length</th><th>Info</th></tr> </thead> <tbody> <tr> <td>22 2.103816</td><td>192.168.1.117</td><td>192.168.1.1</td><td>DNS</td><td>73</td><td>Standard query 0xa0f3 A bitsy.mit.edu</td></tr> <tr> <td>23 2.104235</td><td>192.168.1.117</td><td>192.168.1.1</td><td>DNS</td><td>73</td><td>Standard query 0x6e2d AAAA bitsy.mit.edu</td></tr> <tr> <td>24 2.110363</td><td>192.168.1.1</td><td>192.168.1.117</td><td>DNS</td><td>89</td><td>Standard query response 0xa0f3 A bitsy.mit.edu A 18.0.72.3</td></tr> <tr> <td>25 2.110363</td><td>192.168.1.1</td><td>192.168.1.117</td><td>DNS</td><td>73</td><td>Standard query response 0x6e2d AAAA bitsy.mit.edu</td></tr> <tr> <td>30 2.149628</td><td>192.168.1.117</td><td>18.0.72.3</td><td>DNS</td><td>82</td><td>Standard query 0x0001 PTR 3.72.0.18.in-addr.arpa</td></tr> <tr> <td>54 4.163132</td><td>192.168.1.117</td><td>18.0.72.3</td><td>DNS</td><td>82</td><td>Standard query 0x0002 A www.aiit.or.kr.uga.edu</td></tr> <tr> <td>81 6.176601</td><td>192.168.1.117</td><td>18.0.72.3</td><td>DNS</td><td>82</td><td>Standard query 0x0003 AAAA www.aiit.or.kr.uga.edu</td></tr> <tr> <td>124 8.192031</td><td>192.168.1.117</td><td>18.0.72.3</td><td>DNS</td><td>74</td><td>Standard query 0x0004 A www.aiit.or.kr</td></tr> <tr> <td>129 10.195596</td><td>192.168.1.117</td><td>18.0.72.3</td><td>DNS</td><td>74</td><td>Standard query 0x0005 AAAA www.aiit.or.kr</td></tr> </tbody> </table>	No.	Time	Source	Destination	Protocol	Length	Info	22 2.103816	192.168.1.117	192.168.1.1	DNS	73	Standard query 0xa0f3 A bitsy.mit.edu	23 2.104235	192.168.1.117	192.168.1.1	DNS	73	Standard query 0x6e2d AAAA bitsy.mit.edu	24 2.110363	192.168.1.1	192.168.1.117	DNS	89	Standard query response 0xa0f3 A bitsy.mit.edu A 18.0.72.3	25 2.110363	192.168.1.1	192.168.1.117	DNS	73	Standard query response 0x6e2d AAAA bitsy.mit.edu	30 2.149628	192.168.1.117	18.0.72.3	DNS	82	Standard query 0x0001 PTR 3.72.0.18.in-addr.arpa	54 4.163132	192.168.1.117	18.0.72.3	DNS	82	Standard query 0x0002 A www.aiit.or.kr.uga.edu	81 6.176601	192.168.1.117	18.0.72.3	DNS	82	Standard query 0x0003 AAAA www.aiit.or.kr.uga.edu	124 8.192031	192.168.1.117	18.0.72.3	DNS	74	Standard query 0x0004 A www.aiit.or.kr	129 10.195596	192.168.1.117	18.0.72.3	DNS	74	Standard query 0x0005 AAAA www.aiit.or.kr	<pre>0000 f4 05 95 b6 ff 6c c8 94 02 13 af 13 f4 05 95 b6 ff 6c 86 dd 60 00 1.- 0010 00 3b 73 ec 00 00 80 11 42 ff c0 a8 01 75 c0 a8 ;s... B...u... 0020 01 01 c9 e8 00 35 00 27 48 ab f3 03 01 00 00 015... H..... 0030 00 00 00 00 00 00 05 62 69 74 73 79 03 6d 69 74b itsy-mit 0040 03 05 64 75 00 00 01 00edu....</pre>
No.	Time	Source	Destination	Protocol	Length	Info																																																								
22 2.103816	192.168.1.117	192.168.1.1	DNS	73	Standard query 0xa0f3 A bitsy.mit.edu																																																									
23 2.104235	192.168.1.117	192.168.1.1	DNS	73	Standard query 0x6e2d AAAA bitsy.mit.edu																																																									
24 2.110363	192.168.1.1	192.168.1.117	DNS	89	Standard query response 0xa0f3 A bitsy.mit.edu A 18.0.72.3																																																									
25 2.110363	192.168.1.1	192.168.1.117	DNS	73	Standard query response 0x6e2d AAAA bitsy.mit.edu																																																									
30 2.149628	192.168.1.117	18.0.72.3	DNS	82	Standard query 0x0001 PTR 3.72.0.18.in-addr.arpa																																																									
54 4.163132	192.168.1.117	18.0.72.3	DNS	82	Standard query 0x0002 A www.aiit.or.kr.uga.edu																																																									
81 6.176601	192.168.1.117	18.0.72.3	DNS	82	Standard query 0x0003 AAAA www.aiit.or.kr.uga.edu																																																									
124 8.192031	192.168.1.117	18.0.72.3	DNS	74	Standard query 0x0004 A www.aiit.or.kr																																																									
129 10.195596	192.168.1.117	18.0.72.3	DNS	74	Standard query 0x0005 AAAA www.aiit.or.kr																																																									

21. Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”?

The DNS query message of my request is of Type: A and the message this doesn't contain any answers.

Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

dns

No.	Time	Source	Destination	Protocol	Length	Info
22	2.103816	192.168.1.117	192.168.1.1	DNS	73	Standard query 0xaf03 A bitsy.mit.edu
23	2.104235	192.168.1.117	192.168.1.1	DNS	73	Standard query 0x6e2d AAAA bitsy.mit.edu
24	2.110363	192.168.1.1	192.168.1.117	DNS	89	Standard query response 0xaf03 A bitsy.mit.edu A 18.0.72.3
25	2.110363	192.168.1.1	192.168.1.117	DNS	73	Standard query response 0x6e2d AAAA bitsy.mit.edu
30	2.149628	192.168.1.117	18.0.72.3	DNS	82	Standard query 0x0001 PTR 3.72.0.18.in-addr.arpa
54	4.163132	192.168.1.117	18.0.72.3	DNS	82	Standard query 0x0002 A www.aiit.or.kr.uga.edu
81	6.176601	192.168.1.117	18.0.72.3	DNS	82	Standard query 0x0003 AAAA www.aiit.or.kr.uga.edu
124	8.192031	192.168.1.117	18.0.72.3	DNS	74	Standard query 0x0004 A www.aiit.or.kr
129	10.195596	192.168.1.117	18.0.72.3	DNS	74	Standard query 0x0005 AAAA www.aiit.or.kr


```
> Frame 22: 73 bytes on wire (584 bits), 73 bytes captured (584 bits) on interface \Device\NPF_{2FAB1EFF-4144-490C-0000-000000000000
> Ethernet II, Src: Chongqin_13:af:13 (c8:94:02:13:af:13), Dst: Sagemcom_b6:ff:6c (f4:05:95:b6:ff:6c)
  > Destination: Sagemcom_b6:ff:6c (f4:05:95:b6:ff:6c)
  > Source: Chongqin_13:af:13 (c8:94:02:13:af:13)
  > Type: IPv4 (0x0800)
> Internet Protocol Version 4, Src: 192.168.1.117, Dst: 192.168.1.1
> User Datagram Protocol, Src Port: 51688, Dst Port: 53
  > Domain Name System (query)
    Transaction ID: 0xaf03
    Flags: 0x0100 Standard query
    Questions: 1
      <--> www.aiit.or.kr.
    Authority RRs: 0
    Additional RRs: 0
  > Queries
    [Response In: 24]
```

22. Examine the DNS response message. How many “answers” are provided? What does each of these answers contain?

For my DNS response message, one answer is provided. The answer contains type class and the address of the answer received.

Wi-Fi

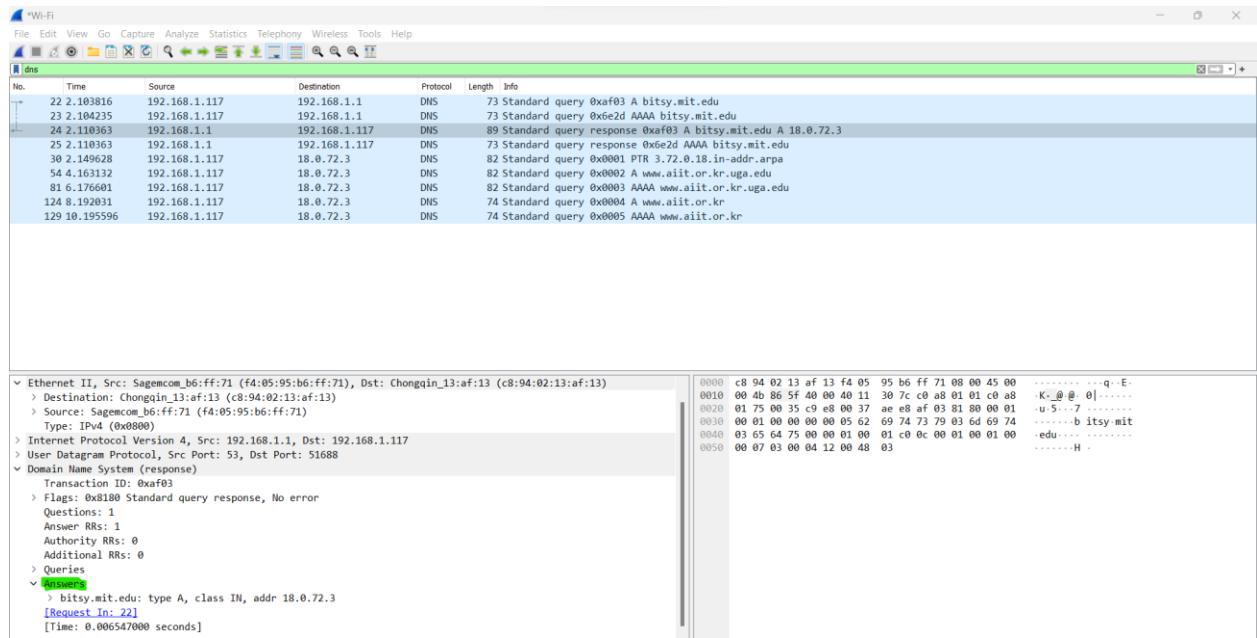
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

dns

No.	Time	Source	Destination	Protocol	Length	Info
22	2.103816	192.168.1.117	192.168.1.1	DNS	73	Standard query 0xaf03 A bitsy.mit.edu
23	2.104235	192.168.1.117	192.168.1.1	DNS	73	Standard query 0x6e2d AAAA bitsy.mit.edu
24	2.110363	192.168.1.1	192.168.1.117	DNS	89	Standard query response 0xaf03 A bitsy.mit.edu A 18.0.72.3
25	2.110363	192.168.1.1	192.168.1.117	DNS	73	Standard query response 0x6e2d AAAA bitsy.mit.edu
30	2.149628	192.168.1.117	18.0.72.3	DNS	82	Standard query 0x0001 PTR 3.72.0.18.in-addr.arpa
54	4.163132	192.168.1.117	18.0.72.3	DNS	82	Standard query 0x0002 A www.aiit.or.kr.uga.edu
81	6.176601	192.168.1.117	18.0.72.3	DNS	82	Standard query 0x0003 AAAA www.aiit.or.kr.uga.edu
124	8.192031	192.168.1.117	18.0.72.3	DNS	74	Standard query 0x0004 A www.aiit.or.kr
129	10.195596	192.168.1.117	18.0.72.3	DNS	74	Standard query 0x0005 AAAA www.aiit.or.kr

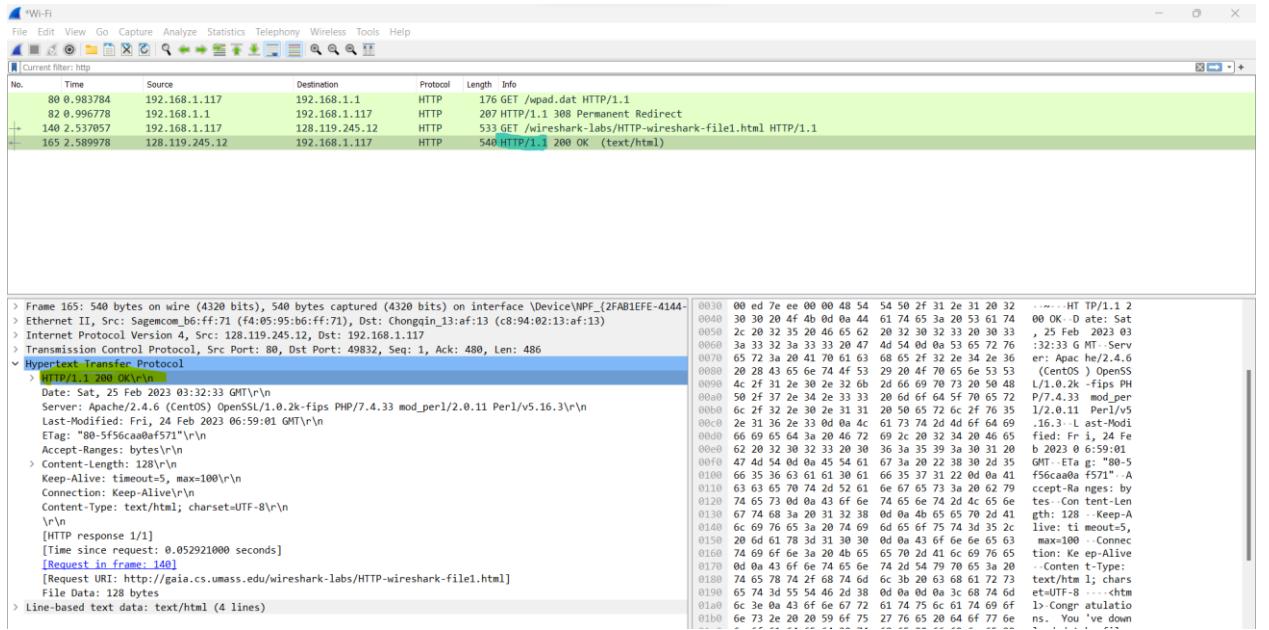
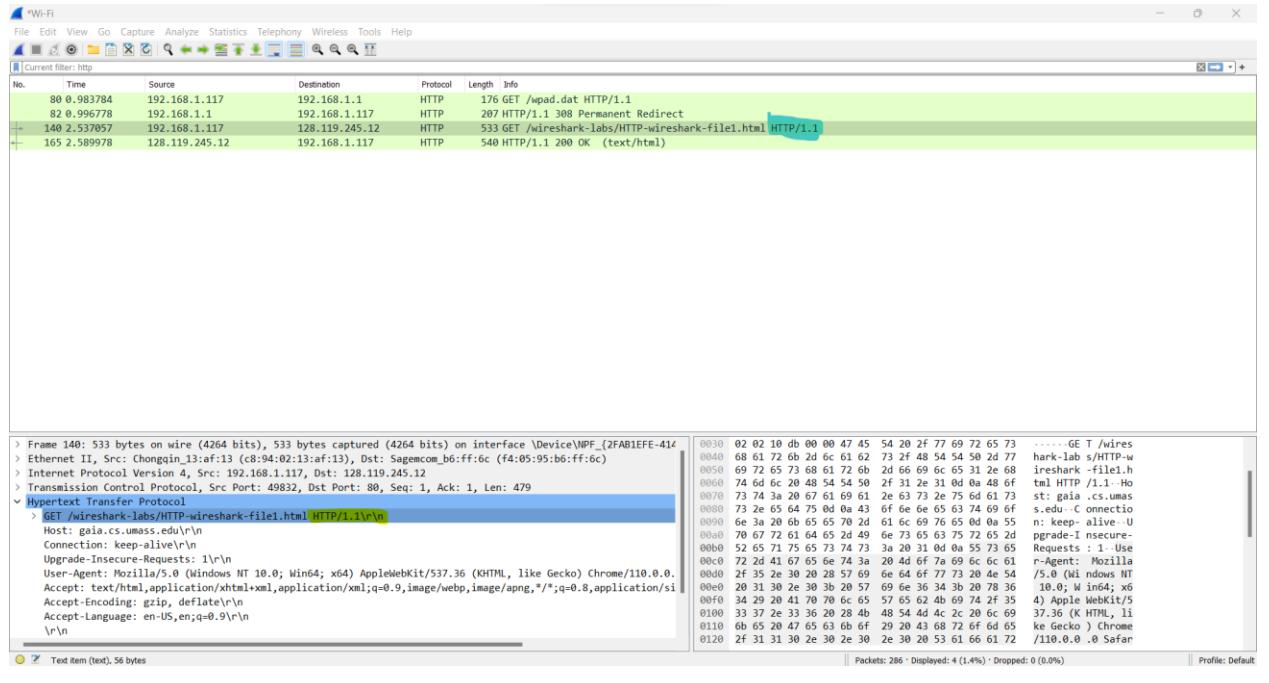

```
> Frame 24: 89 bytes on wire (712 bits), 89 bytes captured (712 bits) on interface \Device\NPF_{2FAB1EFF-4144-490C-0000-000000000000
> Ethernet II, Src: Sagemcom_b6:ff:71 (f4:05:95:b6:ff:71), Dst: Chongqin_13:af:13 (c8:94:02:13:af:13)
  > Destination: Chongqin_13:af:13 (c8:94:02:13:af:13)
  > Source: Sagemcom_b6:ff:71 (f4:05:95:b6:ff:71)
  > Type: IPv4 (0x0800)
> Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.1.117
> User Datagram Protocol, Src Port: 53, Dst Port: 51688
  > Domain Name System (response)
    Transaction ID: 0xaf03
    Flags: 0x0100 Standard query response, No error
    Questions: 1
      www.aiit.or.kr.
    Authority RRs: 0
    Additional RRs: 0
  > Queries
    [Request In: 22]
    [Time: 0.006547000 seconds]
```

23. Provide a screenshot.



1. Is your browser running HTTP version 1.0 or 1.1? What version of HTTP is the server running?

The browser is running HTTP version 1.1. The HTTP version of the server is also 1.1.



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

The accepted language that is listed by browser is US English.

```

No. Time Source Destination Protocol Length Info
80 0.983784 192.168.1.117 192.168.1.1 HTTP 176 GET /wpad.dat HTTP/1.1
82 0.996778 192.168.1.1 192.168.1.117 HTTP 207 HTTP/1.1 308 Permanent Redirect
+- 140 2.537057 192.168.1.117 128.119.245.12 HTTP 533 GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
+- 165 2.589978 128.119.245.12 192.168.1.117 HTTP 540 HTTP/1.1 200 OK (text/html)

> Frame 140: 533 bytes on wire (4264 bits), 533 bytes captured (4264 bits) on interface \Device\NPF_{2FAB1EFE-4144-4D3B-B6A8-000000000000
> Ethernet II, Src: Chongqin_13:af:13 (c8:94:02:13:af:13), Dst: Sagemcom_b6:ff:6c (f4:05:95:b6:ff:6c)
> Internet Protocol Version 4, Src: 192.168.1.117, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 49832, Dst Port: 80, Seq: 1, Ack: 1, Len: 479
  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/110.0.0.0
      Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=1
      Accept-Encoding: gzip, deflate\r\n
      Accept-Language: en-US,en;q=0.9\r\n
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html]
    [HTTP request 1/1]
    [Response in frame: 165]

0030 02 02 10 db 00 00 47 45 54 20 2f 77 69 72 65 73 ... GE T /wires
0040 68 61 72 6b 2d 0e 61 62 73 2f 48 54 54 50 2d 77 hark-lab s/HTTP-w
0050 69 72 65 73 68 61 72 6b 2d 66 69 6c 65 31 2e 68 ireshark -file1.h
0060 74 6d 6c 20 48 54 54 50 2f 31 2e 31 0d 0a 48 6f tml HTTP /1.1 Ho
0070 73 74 3a 20 67 61 69 61 2e 63 73 2e 75 6d 61 73 st: gaia .cs.umass
0080 73 2e 65 64 75 0d 0a 43 6f 6e 66 65 63 74 69 6f s.edu C connectio
0090 06 3a 2b 6b 65 65 70 2d 61 6c 69 76 65 0d 0a 55 n: keep- alive..U
00a0 70 67 72 61 64 65 2d 49 6e 73 65 63 75 72 65 2d pgrade-I nsecure-
00b0 52 65 72 75 65 73 74 3a 20 31 0d 0a 55 73 65 Requests : 1- Use
00c0 72 2d 41 67 65 6e 74 3a 20 4d 6f 7a 69 6c 61 r-Agent: Mozilla
00d0 2f 35 2e 30 20 28 57 69 6e 64 69 77 73 28 4e 54 /5.0 (Wi ndows NT
00e0 34 29 20 41 70 60 6c 65 57 65 62 4b 69 74 2f 35 10.0; W ind64; x6
00f0 34 29 20 41 70 60 6c 65 57 65 62 4b 69 74 2f 35 3 Apple WebKit/5
0100 33 37 2e 33 36 20 28 4b 48 54 4d 4c 2c 20 6c 69 37.36 (K HTML, li
0110 6b 65 20 47 65 63 6b 6f 20 29 43 68 72 6f 6d 65 ke Gecko ) Chrome
0120 2f 31 31 30 2e 30 2e 30 2e 30 2e 30 20 53 61 66 61 72 /110.0 .0 Safar
0130 69 2f 35 33 37 2e 33 36 20 45 64 67 2f 31 31 30 1/537.36 Edg/110
0140 2e 30 2e 31 35 38 37 2e 35 63 0d 0a 41 63 63 65 .0.1587. 50 Acce
0150 70 74 3a 2a 20 74 65 78 74 2f 68 74 6d 6c 2c 1d 70 pt: text /html,ap

```

3. What is the IP address of your computer? Of the gaia.cs.umass.edu server?

The IP address of my computer is 192.168.1.117 and the IP address of gaia.cs.umass.edu server is 128.119.245.12

```

No. Time Source Destination Protocol Length Info
80 0.983784 192.168.1.117 192.168.1.1 HTTP 176 GET /wpad.dat HTTP/1.1
82 0.996778 192.168.1.1 192.168.1.117 HTTP 207 HTTP/1.1 308 Permanent Redirect
+- 140 2.537057 192.168.1.117 128.119.245.12 HTTP 533 GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
+- 165 2.589978 128.119.245.12 192.168.1.117 HTTP 540 HTTP/1.1 200 OK (text/html)

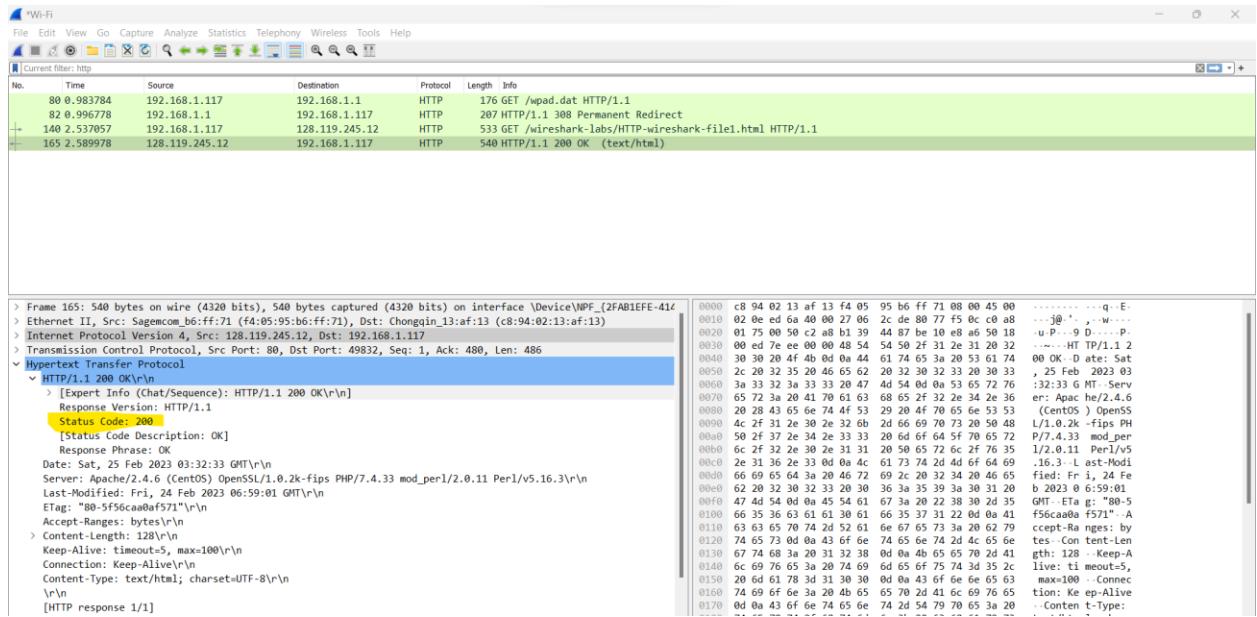
> Frame 140: 533 bytes on wire (4264 bits), 533 bytes captured (4264 bits) on interface \Device\NPF_{2FAB1EFE-4144-4D3B-B6A8-000000000000
> Ethernet II, Src: Chongqin_13:af:13 (c8:94:02:13:af:13), Dst: Sagemcom_b6:ff:6c (f4:05:95:b6:ff:6c)
> Internet Protocol Version 4, Src: 192.168.1.117, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 49832, Dst Port: 80, Seq: 1, Ack: 1, Len: 479
  Hypertext Transfer Protocol
    GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
      Host: gaia.cs.umass.edu
      Connection: keep-alive
      Upgrade-Insecure-Requests: 1
      User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/110.0.0.0
      Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=1
      Accept-Encoding: gzip, deflate
      Accept-Language: en-US,en;q=0.9
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html]
    [HTTP request 1/1]
    [Response in frame: 165]

0000 f4 05 b6 ff 6c 94 02 13 af 13 08 00 45 00 ... l... .... E-
0010 02 07 ae 9a 40 00 80 06 12 b5 c0 a8 01 75 80 77 ...@... .... u-w
0020 f5 0c c2 a8 00 50 b0 1e c7 b1 39 44 87 50 18 ...P... .... 9D-P-
0030 02 02 10 db 00 00 47 45 54 20 2f 77 69 72 65 73 ... GE T /wires
0040 68 61 72 6b 2d 0e 61 62 73 2f 48 54 54 50 2d 77 hark-lab s/HTTP-w
0050 69 72 65 73 68 61 72 6b 2d 66 69 6c 65 31 2e 68 ireshark -file1.h
0060 74 6d 6c 20 48 54 54 50 2f 31 2e 31 0d 0a 48 6f tml HTTP /1.1 Ho
0070 73 74 3a 20 67 61 69 61 2e 63 73 2e 75 6d 61 73 st: gaia .cs.umass
0080 73 2e 65 64 75 0d 0a 43 6f 6e 66 65 63 74 69 6f s.edu C connectio
0090 06 3a 2b 6b 65 65 70 2d 61 6c 69 76 65 0d 0a 55 n: keep- alive..U
00a0 70 67 72 61 64 65 2d 49 6e 73 65 63 75 72 65 2d pgrade-I nsecure-
00b0 52 65 71 75 65 73 74 3a 20 31 0d 0a 55 73 65 Requests : 1- Use
00c0 72 2d 41 67 65 6e 74 3a 20 4d 6f 7a 69 6c 61 r-Agent: Mozilla
00d0 2f 35 2e 30 20 28 57 69 6e 64 69 77 73 28 4e 54 /5.0 (Wi ndows NT
00e0 34 29 20 41 70 60 6c 65 57 65 62 4b 69 74 2f 35 10.0; W ind64; x6
00f0 34 29 20 41 70 60 6c 65 57 65 62 4b 69 74 2f 35 3 Apple WebKit/5
0100 33 37 2e 33 36 20 28 4b 48 54 4d 4c 2c 20 6c 69 37.36 (K HTML, li
0110 6b 65 20 47 65 63 6b 6f 29 20 43 68 72 6f 6d 65 ke Gecko ) Chrome
0120 2f 31 31 30 2e 30 2e 30 2e 30 2e 30 20 53 61 66 61 72 /110.0 .0 Safar
0130 69 2f 35 33 37 2e 33 36 20 45 64 67 2f 31 31 30 1/537.36 Edg/110
0140 2e 30 2e 31 35 38 37 2e 35 63 0d 0a 41 63 63 65 .0.1587. 50 Acce

```

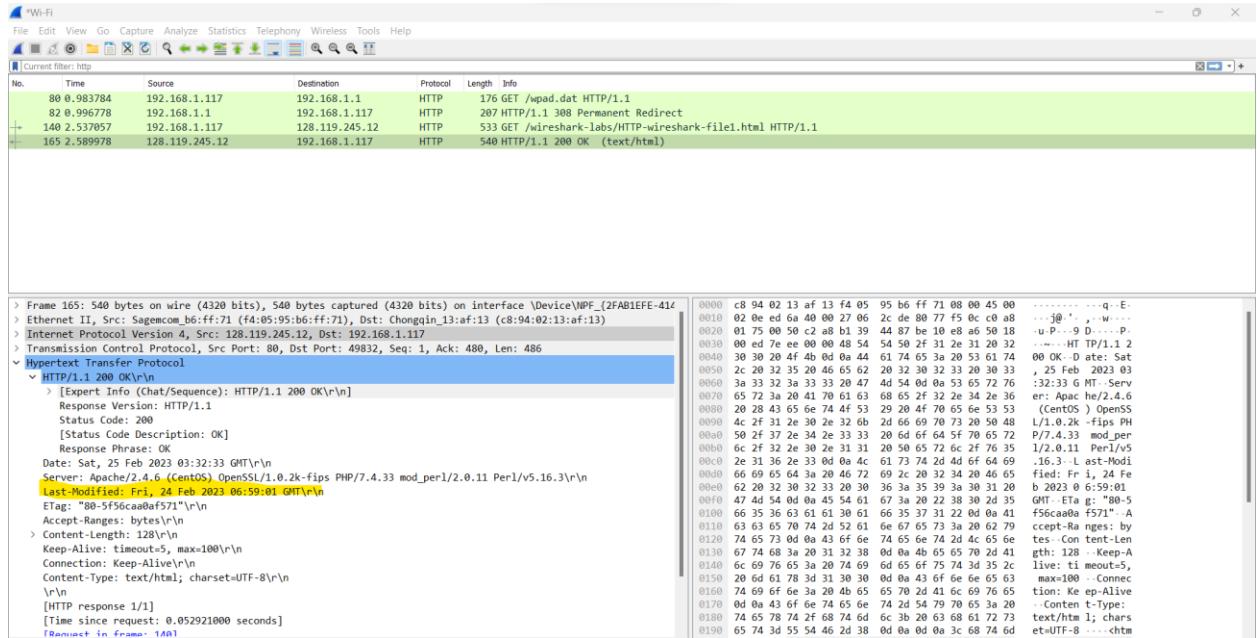
4. What is the status code returned from the server to your browser?

The status code returned from the server is 200 OK.



5. When was the HTML file that you are retrieving last modified at the server?

The last modified date of the HTML file is 24th February,2023 at 06:59:01 GMT\r\n



6. How many bytes of content are being returned to your browser?

The frame is returning 540 bytes of data out of which the HTTP request to the server is returning 128 bytes to my browser.

```

Frame 165: 128 bytes on wire (4320 bits), 540 bytes captured (4320 bits) on interface \Device\NPF_{2FAB1EFE-4144-409C-BB4D-000000000000
> Ethernet II, Src: Sagecom_b6:ff:71 (f4:05:95:b6:ff:71), Dst: Chongan1_3:af:13 (c8:94:02:13:af:13)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.117
> Transmission Control Protocol, Src Port: 80, Dst Port: 49832, Seq: 1, Ack: 480, Len: 486
    Hypertext Transfer Protocol
        > HTTP/1.1 200 OK\r\n
            Date: Sat, 25 Feb 2023 03:32:33 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: Fri, 24 Feb 2023 06:59:01 GMT\r\n
            ETag: "80-5f56ca0a0f571"\r\n
            Accept-Ranges: bytes\r\n
            Content-Length: 128\r\n
                [Content length: 128]
            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: 0.052921000 seconds]
        [Request in frame: 146]
        [Request URL: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html]
        [File Data: 128 bytes]
    Line-based text data: text/html (4 lines)

```

7. By inspecting the raw data in the packet content window, do you see any headers within the data that are not displayed in the packet-listing window? If so, name one.

There aren't any headers that are not displayed in the packet window.

8. 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?

In the HTTP GET request there is no “IF-MODIFIED-SINCE”.

```

Frame 75: 533 bytes on wire (4264 bits), 533 bytes captured (4264 bits) on interface \Device\NPF_{2FAB1EFE-4144-409C-BB4D-000000000000
> Ethernet II, Src: Chongan1_3:af:13 (c8:94:02:13:af:13), Dst: Sagecom_b6:ff:71 (f4:05:95:b6:ff:71)
> Internet Protocol Version 4, Src: 192.168.1.117, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 49788, Dst Port: 80, Seq: 1, Ack: 1, Len: 479
    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]
            [GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n]
            [Severity level: Chat]
            [Group: Sequence]
            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/110.0.0.0
            Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=1.0
            Accept-Encoding: gzip, deflate\r\n
            Accept-Language: en-US,en;q=0.9\r\n
        \r\n
        [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]
        [HTTP request 1/1]
        [Response in frame: 82]

```

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

The browser returned the contents of the file which are displayed under Line-based text data.

```

Frame 82: 784 bytes on wire (6272 bits), 784 bytes captured (6272 bits) on interface \Device\NPF_{2FA81EFE-4144-4
> Ethernet II, Src: Sagemon_b6:ff:71 (f4:05:95:b6:ff:71), Dst: Chongmin_13:a:f1:13 (c8:94:02:13:a:f1:13)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.117
> Transmission Control Protocol, Src Port: 80, Dst Port: 49788, Seq: 1, Ack: 480, Len: 730
  Hypertext Transfer Protocol
    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. <br><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.<br><n>
      </html><n>

```

```

Frame 82: 784 bytes on wire (6272 bits), 784 bytes captured (6272 bits) on interface \Device\NPF_{2FA81EFE-4144-4
> Ethernet II, Src: Sagemon_b6:ff:71 (f4:05:95:b6:ff:71), Dst: Chongmin_13:a:f1:13 (c8:94:02:13:a:f1:13)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.117
> Transmission Control Protocol, Src Port: 80, Dst Port: 49788, Seq: 1, Ack: 480, Len: 730
  Hypertext Transfer Protocol
    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. <br><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.<br><n>
      </html><n>

```

10. Now inspect the contents of the second HTTP GET request from your browser to the server. Do you see an “IF-MODIFIED-SINCE:” line in the HTTP GET? If so, what information follows the “IF-MODIFIED-SINCE:” header?

The second HTTP Get request contains the if-modified since line and it has the information about the date it was modified.

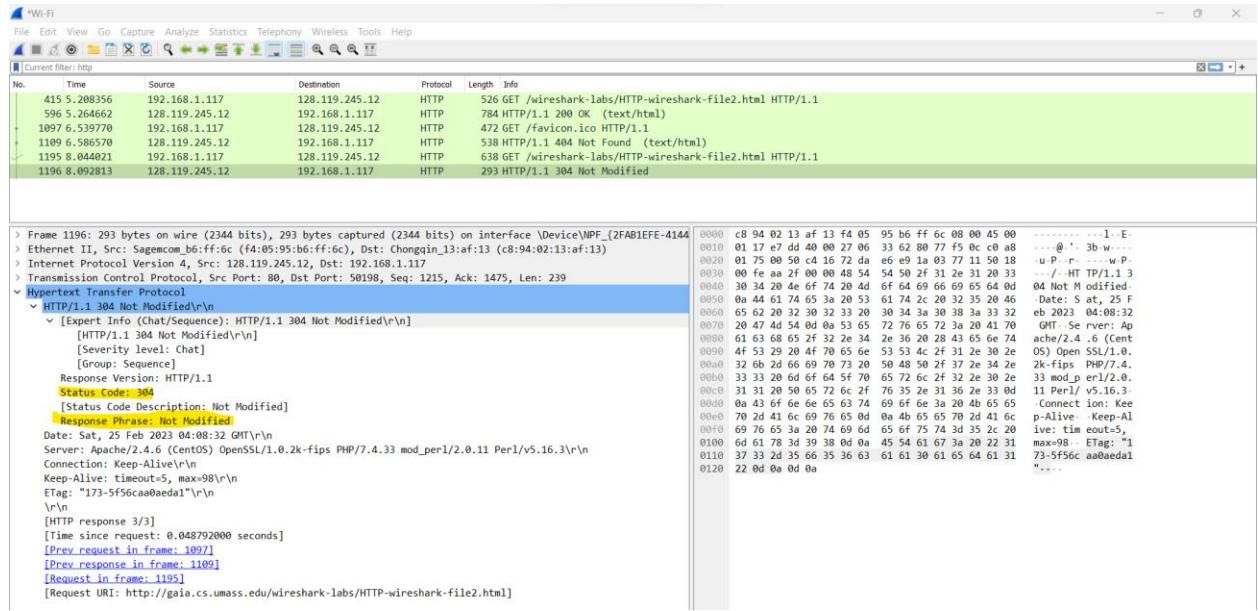
```

Frame 1195: 638 bytes on wire (5104 bits), 638 bytes captured (5104 bits) on interface \Device\NPF_{2FA81EFE-4144-4
> Ethernet II, Src: Chongmin_13:a:f1:13 (c8:94:02:13:a:f1:13), Dst: Sagemon_b6:ff:6c (f4:05:95:b6:ff:6c)
> Internet Protocol Version 4, Src: 192.168.1.117, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 50198, Dst Port: 80, Seq: 891, Ack: 1215, Len: 584
  Hypertext Transfer Protocol
    > [Expert Info (Chat/Sequence): GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n]
      [GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n]
      [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
    Cache-Control: max-age=0\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/110.0.0.0
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=1.0
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: en-US,en;q=0.9\r\n
    If-None-Match: "73-5f6ca0a6da1"\r\n
    If-Modified-Since: Fri, 24 Feb 2023 06:59:01 GMT\r\n
    Vary: *
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]
    [HTTP request 3/3]
    [Prev request_in frame: 1097]
    [Response_in frame: 1196]

```

11. What is the HTTP status code and phrase returned from the server in response to this second HTTP GET? Did the server explicitly return the contents of the file? Explain.

The HTTP status code that the server responded with was a 304 Not Modified. This means that the server explicitly returned the contents of the file with no modifications made to the file that was returned.



12. How many HTTP GET request messages did your browser send? Which packet number in the trace contains the GET message for the Bill or Rights?

The browser sent only one HTTP GET request to the server. The packet number of the GET message in the trace is at 1318.

```

Frame 1318: 533 bytes on wire (4264 bits), 533 bytes captured (4264 bits) on interface \Device\NPF_{2FAB1EFF-E414-490C-BA36-6C3BB690F749}
No. Time Source Destination Protocol Length Info
+- 1318 2.029646 192.168.1.117 128.119.245.12 HTTP 533 GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
+- 1353 2.083054 128.119.245.12 192.168.1.117 HTTP 619 HTTP/1.1 200 OK (text/html)

Frame 1318: 533 bytes on wire (4264 bits), 533 bytes captured (4264 bits) on interface \Device\NPF_{2FAB1EFF-E414-490C-BA36-6C3BB690F749}
Section number: 1
> Interface id: 0 (\Device\NPF_{2FAB1EFF-E414-490C-BA36-6C3BB690F749})
Encapsulation type: Ethernet (1)
Arrival Time: Feb 25, 2023 09:50:40.830344000 India Standard Time
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1677298840.830344000 seconds
[Time delta from previous captured frame: 0.000422000 seconds]
[Time delta from previous displayed frame: 0.000000000 seconds]
[Time since reference or first frame: 2.029640000 seconds]
[Frame Number: 1318]
Frame Length: 533 bytes (4264 bits)
Capture Length: 533 bytes (4264 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:ip:tcp:http]
[Coloring Rule Name: HTTP]
[Coloring Rule String: http || tcp.port == 80 || http2]

Frame 1353: 619 bytes on wire (4952 bits), 619 bytes captured (4952 bits) on interface \Device\NPF_{2FAB1EFF-E414-490C-BA36-6C3BB690F749}
No. Time Source Destination Protocol Length Info
+- 1318 2.029646 192.168.1.117 128.119.245.12 HTTP 533 GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
+- 1353 2.083054 128.119.245.12 192.168.1.117 HTTP 619 HTTP/1.1 200 OK (text/html)

Frame 1353: 619 bytes on wire (4952 bits), 619 bytes captured (4952 bits) on interface \Device\NPF_{2FAB1EFF-E414-490C-BA36-6C3BB690F749}
Section number: 1
> Interface id: 0 (\Device\NPF_{2FAB1EFF-E414-490C-BA36-6C3BB690F749})
Encapsulation type: Ethernet (1)
Arrival Time: Feb 25, 2023 09:50:40.883752000 India Standard Time
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1677298840.883752000 seconds
[Time delta from previous captured frame: 0.000000000 seconds]
[Time delta from previous displayed frame: 0.053408000 seconds]
[Time since reference or first frame: 2.083054000 seconds]
[Frame Number: 1353]
Frame Length: 619 bytes (4952 bits)
Capture Length: 619 bytes (4952 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:ip:tcp:http:data-text-lines]
[Coloring Rule Name: HTTP]
[Coloring Rule String: http || tcp.port == 80 || http2]

```

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

The packet number which contains the status code and phrase associated with the HTTP GET response is 1353.

```

Frame 1318: 533 bytes on wire (4264 bits), 533 bytes captured (4264 bits) on interface \Device\NPF_{2FAB1EFF-E414-490C-BA36-6C3BB690F749}
No. Time Source Destination Protocol Length Info
+- 1318 2.029646 192.168.1.117 128.119.245.12 HTTP 533 GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
+- 1353 2.083054 128.119.245.12 192.168.1.117 HTTP 619 HTTP/1.1 200 OK (text/html)

Frame 1353: 619 bytes on wire (4952 bits), 619 bytes captured (4952 bits) on interface \Device\NPF_{2FAB1EFF-E414-490C-BA36-6C3BB690F749}
No. Time Source Destination Protocol Length Info
+- 1318 2.029646 192.168.1.117 128.119.245.12 HTTP 533 GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
+- 1353 2.083054 128.119.245.12 192.168.1.117 HTTP 619 HTTP/1.1 200 OK (text/html)

Frame 1353: 619 bytes on wire (4952 bits), 619 bytes captured (4952 bits) on interface \Device\NPF_{2FAB1EFF-E414-490C-BA36-6C3BB690F749}
No. Time Source Destination Protocol Length Info
+- 1318 2.029646 192.168.1.117 128.119.245.12 HTTP 533 GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
+- 1353 2.083054 128.119.245.12 192.168.1.117 HTTP 619 HTTP/1.1 200 OK (text/html)

Frame 1353: 619 bytes on wire (4952 bits), 619 bytes captured (4952 bits) on interface \Device\NPF_{2FAB1EFF-E414-490C-BA36-6C3BB690F749}
Section number: 1
> Interface id: 0 (\Device\NPF_{2FAB1EFF-E414-490C-BA36-6C3BB690F749})
Encapsulation type: Ethernet (1)
Arrival Time: Feb 25, 2023 09:50:40.883752000 India Standard Time
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1677298840.883752000 seconds
[Time delta from previous captured frame: 0.000000000 seconds]
[Time delta from previous displayed frame: 0.053408000 seconds]
[Time since reference or first frame: 2.083054000 seconds]
[Frame Number: 1353]
Frame Length: 619 bytes (4952 bits)
Capture Length: 619 bytes (4952 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:ip:tcp:http:data-text-lines]
[Coloring Rule Name: HTTP]
[Coloring Rule String: http || tcp.port == 80 || http2]

```

14. What is the status code and phrase in the response?

The status code of the response packet is 200, and the response phrase was “OK”.

```

No. Time Source Destination Protocol Length Info
1318 2.029646 192.168.1.117 128.119.245.12 HTTP 533 GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
1353 2.083054 128.119.245.12 192.168.1.117 HTTP 619 HTTP/1.1 200 OK (text/html)

> Transmission Control Protocol, Src Port: 80, Dst Port: 59799, Seq: 4297, Ack: 480, Len: 565
> [4 Reassembled TCP Segments (4861 bytes): #1349(1432), #1350(1432), #1352(1432), #1353(565)]
  Hypertext Transfer Protocol
    HTTP/1.1 200 OK\r\n
      [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
        [Severity level: Chat]
        [Group: Sequence]
        Response Version: HTTP/1.1
          Status Code: 200
          [Status Code Description: OK]
          Response Phrase: OK
        Date: Sat, 25 Feb 2023 04:20:40 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: Fri, 24 Feb 2023 06:59:01 GMT\r\n
        ETag: "1194-5f56ca0aaaf21"\r\n
        Accept-Ranges: bytes\r\n
      Content-Length: 4500\r\n

```

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

The HTTP response and the text of the Bill of Rights takes 4 data-containing TCP segments.

```

No. Time Source Destination Protocol Length Info
1318 2.029646 192.168.1.117 128.119.245.12 HTTP 533 GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
1353 2.083054 128.119.245.12 192.168.1.117 HTTP 619 HTTP/1.1 200 OK (text/html)

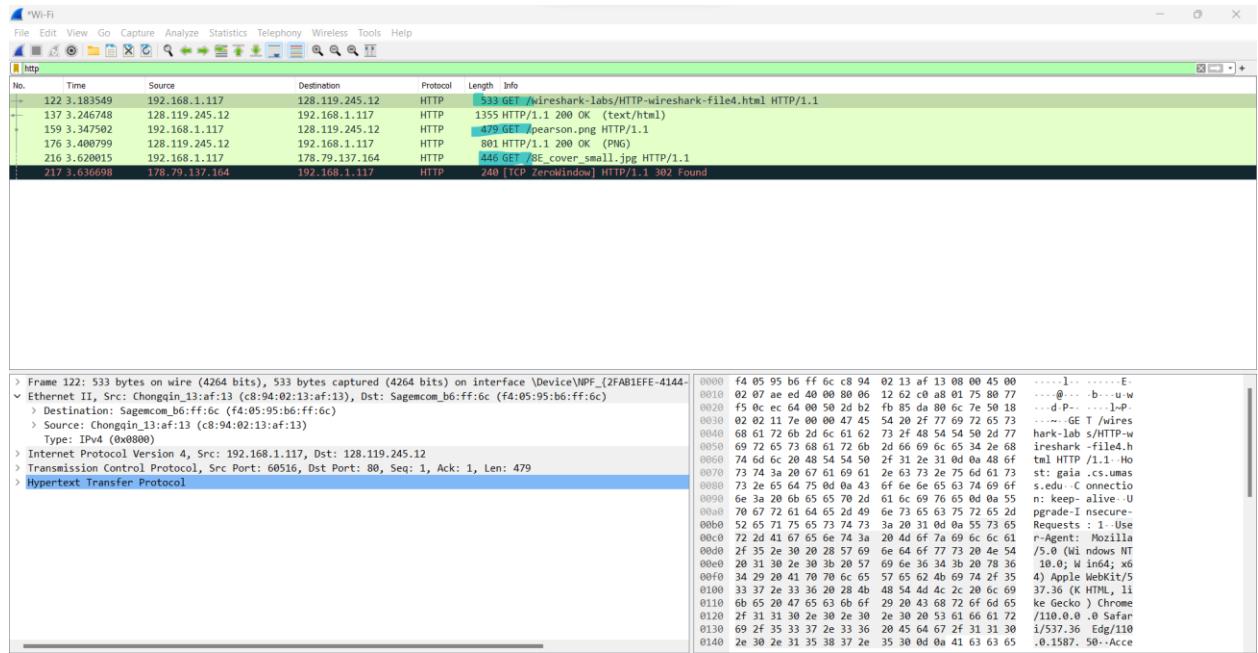
> Frame 1353: 619 bytes on wire (4952 bits), 619 bytes captured (4952 bits) on interface \Device\NPF_{2FAB1EFE-4144
  Ethernet II, Src: Sagemcom_b6:ff:71 (f4:05:95:b6:ff:71), Dst: Chongqin_13:af:13 (c8:94:02:13:af:13)
  > Destination: Chongqin_13:af:13 (c8:94:02:13:af:13)
  > Source: Sagemcom_b6:ff:71 (f4:05:95:b6:ff:71)
  > Type: IPv4 (0x0800)
  > Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.117
  > Transmission Control Protocol, Src Port: 80, Dst Port: 59799, Seq: 4297, Ack: 480, Len: 565
  > [4 Reassembled TCP Segments (4861 bytes): #1349(1432), #1350(1432), #1352(1432), #1353(565)]
    [Frame: 1349, payload: 0-1431 (1432 bytes)]
    [Frame: 1350, payload: 1432-2863 (1432 bytes)]
    [Frame: 1352, payload: 2864-4295 (1432 bytes)]
    [Frame: 1353, payload: 4296-4860 (565 bytes)]
    [Segment count: 4]
    [Reassembled TCP Length: 4861]
    [Reassembled TCP Data: 485454502f312e3120323030204f4b0d0a446174653a205361742c203235204665622032...]
  Hypertext Transfer Protocol
  Line-based text data: text/html (98 lines)

0000 48 54 54 50 2f 31 2e 31 20 32 30 30 20 4f 4b 0d HTTP/1.1 200 OK-
0010 0a 44 61 74 65 3a 20 53 61 74 2c 20 32 35 20 46 Date: S at, 25 F
0020 65 62 20 32 30 32 33 20 30 34 3a 32 30 3a 34 30 eb 2023 04:20:40
0030 20 47 4d 54 0d 0a 53 65 72 65 72 3a 20 41 70 GHT-.Se rver: Ap
0040 63 60 65 3a 32 2e 34 2e 30 3a 32 30 3a 34 30 che/2.4 .6 .(Cent
0050 74 72 72 65 72 20 65 78 63 65 73 73 69 76 65 20 , mon ex cessive
0060 69 66 65 73 73 0a 69 6d 70 6f 73 65 64 2c 20 6e fines-im posed, n
0070 6f 72 20 63 72 75 65 6c 20 61 6a 64 20 75 6e 75 or cruel and unu
0080 73 75 61 6c 20 70 75 66 69 73 68 6d 65 6e 74 73 sual pun ishments
0090 20 69 66 66 6c 69 63 74 65 64 2e 0a 0a 0a 3c 2f 70 inflict ed.../p
00a0 3a 3c 70 3e 3c 61 20 6e 61 6d 65 3d 22 39 22 3e >x>n a name="9">
00b0 3a 73 74 72 6f 6e 67 3e 3c 68 33 3e 41 6d 65 <strong><3>Amen
00c0 64 6d 65 6e 74 20 49 58 3c 2f 68 33 3e 3c 2f 73 dment IX </h>/s
00d0 74 72 72 65 6e 67 3e 0a 69 63 65 64 2c 20 41 6f 66 tron>a>->x>
00e0 6f 72 72 65 6e 67 3e 0a 69 63 65 64 2c 20 41 6f 66 /p>Th e con
00f0 61 74 69 6f 6e 20 69 6e 20 74 68 65 20 41 6f 66 stitutio n, of ce
0100 73 74 69 74 75 74 69 6f 6e 2c 20 6f 66 20 63 65 6f 6e 2c 20 6f 66
0110 72 74 61 69 6e 20 72 69 67 68 74 73 2c 20 73 68 rtain ri ghts, sh
0120 61 6c 6c 0a 6e 6f 74 20 62 65 20 63 6f 6e 73 74 all-not be const
0130 72 75 65 64 20 74 6f 20 64 65 6e 79 20 6f 72 20 rued to deny or

```

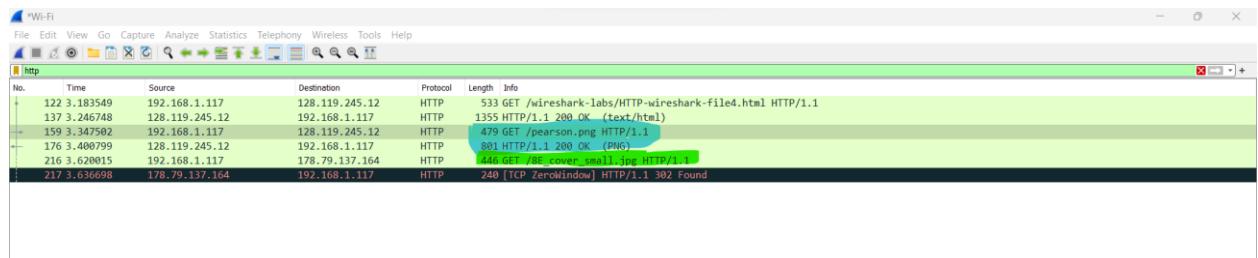
16. How many HTTP GET request messages did your browser send? To which Internet addresses were these GET requests sent.

The browser sent 3 HTTP GET request messages to the server. The address to which the first two GET requests were sent are 128.119.245.12. The last GET request was sent 178.79.137.164



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

The browser downloaded the two images *serially* which is evident from the request and response messages received in the trace. For the first image a http get and response was done after which the next request for second image was sent.



18. What is the server's response (status code and phrase) in response to the initial HTTP GET message from your browser?

The server's response to my HTTP GET message is a 401 with "Unauthorized phrase".

This Wireshark capture shows the initial interaction between a client and a server. The client (Sagemcom_b6:ff:71) sends an HTTP GET request to the server (Chongqin_13:af:13) for the URL /wireshark-labs/protected_pages/HTTP-wiresharkfile5.html. The server responds with a 401 Unauthorized status code, indicating that the user is not authenticated.

```

Frame 60: 771 bytes on wire (6168 bits), 771 bytes captured (6168 bits) on interface \Device\NPF_{2FAB1EFE-4144-4
Ethernet II, Src: Sagemcom_b6:ff:71 (f4:05:95:b6:ff:71), Dst: Chongqin_13:af:13 (c8:94:02:13:af:13)
> Destination: Chongqin_13:af:13 (c8:94:02:13:af:13)
> Source: Sagemcom_b6:ff:71 (f4:05:95:b6:ff:71)
Type: IPv4 (0x0800)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.117
> Transmission Control Protocol, Src Port: 80, Dst Port: 51863, Seq: 1, Ack: 488, Len: 717
> Hypertext Transfer Protocol
>   HTTP/1.1 401 Unauthorized\r\n
Date: Sat, 25 Feb 2023 05:16:57 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
WWW-Authenticate: Basic realm="wireshark-students only"\r\n
Content-Length: 381\r\n
Keep-Alive: timeout=5, max=100\r\n
Connection: Keep-Alive\r\n
Content-Type: text/html; charset=iso-8859-1\r\n
\r\n
[HTTP response 1/1]
[Time since request: 0.053156000 seconds]
[Request in frame: 56]
[Request URI: http://gaia.cs.umass.edu/wireshark-labs/protected_pages/HTTP-wiresharkfile5.html]
File Data: 381 bytes
> Line-based text data: text/html (12 lines)

```

The captured data shows the raw hex and ASCII representations of the 401 Unauthorized response, which includes the HTTP headers and the challenge for basic authentication.

19. When your browser's sends the HTTP GET message for the second time, what new field is included in the HTTP GET message?

The new field that is included in the HTTP GET message is the Authorization field as Authorization: Basic ZHE6YWZzYWE

This Wireshark capture shows the second HTTP GET request from the client (Sagemcom_b6:ff:71) to the server (Chongqin_13:af:13). The client has added an Authorization header with the value Basic ZHE6YWZzYWE, indicating that it has provided the required authentication credentials.

```

Frame 145: 602 bytes on wire (4816 bits), 602 bytes captured (4816 bits) on interface \Device\NPF_{2FAB1EFE-4144-4
Ethernet II, Src: Chongqin_13:af:13 (c8:94:02:13:af:13), Dst: Sagemcom_b6:ff:6c (f4:05:95:b6:ff:6c)
> Destination: Sagemcom_b6:ff:6c (f4:05:95:b6:ff:6c)
> Source: Chongqin_13:af:13 (c8:94:02:13:af:13)
Type: IPv4 (0x0800)
> Internet Protocol Version 4, Src: 192.168.1.117, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 52107, Dst Port: 80, Seq: 1, Ack: 548
> Hypertext Transfer Protocol
>   GET /wireshark-labs/protected_pages/HTTP-wiresharkfile5.html HTTP/1.1\r\n
Host: gaia.cs.umass.edu\r\n
Connection: keep-alive\r\n
Cache-Control: max-age=0\r\n
Authorization: Basic ZHE6YWZzYWE\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/110.0.0.0\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=1\r
Accept-Encoding: gzip, deflate\r\n
Accept-Language: en-US,en;q=0.9\r\n
\r\n
[Full request URI: http://gaia.cs.umass.edu/wireshark-labs/protected_pages/HTTP-wiresharkfile5.html]
[HTTP request 1/1]
[Response in frame: 149]

```

The captured data shows the raw hex and ASCII representations of the second HTTP GET request, highlighting the addition of the Authorization header.