

Daniel Lara - ID: 49651280
Zachary Hart – ID: 70953123
CS 132

HW 2: Wireshark Labs

Question 2: Wireshark Labs

HTTP:

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

Answer: Both the browser and the server are using version 1.1.

The image shows a Wireshark packet capture window titled "*Wi-Fi". The packet list on the left shows two packets: packet 16 (GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1) and packet 20 (HTTP/1.1 200 OK (text/html)). The packet details pane for packet 20 is expanded, showing the Hypertext Transfer Protocol section. The request method is GET, the request URI is /wireshark-labs/HTTP-wireshark-file1.html, and the request version is HTTP/1.1. The host is gaia.cs.umass.edu. The user agent is Mozilla/5.0 (Windows NT 10.0; WOW64; rv:49.0) Gecko/20100101 Firefox/49.0. The accept headers are text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8. The accept-encoding is gzip, deflate. The connection is keep-alive. The upgrade-insecure-requests header is 1. The full request URI is http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html. The HTTP request is 1/1. The response is in frame 20. The packet bytes pane at the bottom shows the raw data of the HTTP response, starting with the status line: HTTP/1.1 200 OK (text/html).

No.	Time	Source	Destination	Protocol	Length	Info
16	2.117638	169.234.99.157	128.119.245.12	HTTP	424	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
20	2.203324	128.119.245.12	169.234.99.157	HTTP	542	HTTP/1.1 200 OK (text/html)

> Frame 16: 424 bytes on wire (3392 bits), 424 bytes captured (3392 bits) on interface 0
> Ethernet II, Src: IntelCor_28:51:77 (cc:3d:82:28:51:77), Dst: CiscoInc_c0:ac:00 (00:24:f9:c0:ac:00)
> Internet Protocol Version 4, Src: 169.234.99.157, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 9458, Dst Port: 80, Seq: 1, Ack: 1, Len: 370
▼ Hypertext Transfer Protocol
 GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n
 [Expert Info (Chat/Sequence): GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n]
 [GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n]
 [Severity level: Chat]
 [Group: Sequence]
 Request Method: GET
 Request URI: /wireshark-labs/HTTP-wireshark-file1.html
 Request Version: HTTP/1.1
 Host: gaia.cs.umass.edu\r\n User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:49.0) Gecko/20100101 Firefox/49.0\r\n Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n Accept-Language: en-US,en;q=0.5\r\n Accept-Encoding: gzip, deflate\r\n DNT: 1\r\n Connection: keep-alive\r\n Upgrade-Insecure-Requests: 1\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: 20]

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.umas
0080 73 2e 65 64 75 0d 0a 55 73 65 72 2d 41 67 65 6e s.edu..U ser-Agen
0090 74 3a 20 4d 6f 7a 69 6c 6c 61 2f 35 2e 30 20 28 t: Mozil la/5.0 (
00a0 57 69 6e 64 6f 77 73 20 4e 54 20 31 30 2e 30 3b Windows NT 10.0;
00b0 20 57 4f 57 36 34 3b 20 72 76 3a 34 39 2e 30 29 WOW64; rv:49.0)
00c0 20 47 65 63 6b 6f 2f 32 30 31 30 30 31 30 31 20 Gecko/2 0100101
00d0 46 69 72 65 66 6f 78 2f 34 39 2e 30 0d 0a 41 63 Firefox/ 49.0..Ac
00e0 63 65 70 74 3a 20 74 65 78 74 2f 68 74 6d 6c 2c cept: te xt/html,

HTTP Request HTTP-Version (http.request.version), 8 bytes Packets: 40 · Displayed: 2 (5.0%) Profile: Default

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

Answer: en-US, en

The image shows a Wireshark packet capture window titled "*Wi-Fi". The packet list pane at the top shows two HTTP packets. Packet 20 is selected, showing a GET request for "/wireshark-labs/HTTP-wireshark-file1.html". The packet details pane shows the request structure, including the "Accept-Language: en-US,en;q=0.5" header, which is highlighted in pink. The packet bytes pane at the bottom shows the raw data of the request, with the "Accept-Language" header also highlighted in pink.

Wireshark packet capture showing an HTTP GET request. The packet details pane highlights the "Accept-Language: en-US,en;q=0.5" header, indicating the languages the browser can accept.

Packet 20: GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1

Request Headers:

- Host: gaia.cs.umass.edu\r\n
- User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:49.0) Gecko/20100101 Firefox/49.0\r\n
- Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n
- Accept-Language: en-US,en;q=0.5\r\n
- Accept-Encoding: gzip, deflate\r\n
- DNT: 1\r\n
- Connection: keep-alive\r\n
- Upgrade-Insecure-Requests: 1\r\n

Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html

HTTP request 1/1

Response in frame: 20

Packet bytes (hex):

```
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.umas
0080 73 2e 65 64 75 0d 0a 55 73 65 72 2d 41 67 65 6e s.edu..U ser-Agen
0090 74 3a 20 4d 6f 7a 69 6c 6c 61 2f 35 2e 30 20 28 t: Mozil la/5.0 (
00a0 57 69 6e 64 6f 77 73 20 4e 54 20 31 30 2e 30 3b Windows NT 10.0;
00b0 20 57 4f 57 36 34 3b 20 72 76 3a 34 39 2e 30 29 WOW64; rv:49.0)
00c0 20 47 65 63 6b 6f 2f 32 30 31 30 30 31 30 31 20 Gecko/2 0100101
00d0 46 69 72 65 66 6f 78 2f 34 39 2e 30 0d 0a 41 63 Firefox/ 49.0..Ac
00e0 63 65 70 74 3a 20 74 65 78 74 2f 68 74 6d 6c 2c cept: te xt/html,
```

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

Answer: My IP = 169.234.99.157 Edu IP = 128.119.245.12

The image shows a Wireshark packet capture window titled "*Wi-Fi". The packet list pane at the top shows two packets. Packet 16 is a GET request from 169.234.99.157 to 128.119.245.12. Packet 20 is the corresponding 200 OK response from 128.119.245.12 to 169.234.99.157. The packet details pane for packet 16 is expanded, showing the Hypertext Transfer Protocol section. The request method is GET, the request URI is /wireshark-labs/HTTP-wireshark-file1.html, and the request version is HTTP/1.1. The host is gaia.cs.umass.edu. The user-agent is Mozilla/5.0 (Windows NT 10.0; WOW64; rv:49.0) Gecko/20100101 Firefox/49.0. The accept headers are text/html, application/xhtml+xml, application/xml; q=0.9, */*; q=0.8. The accept-encoding is gzip, deflate. The connection is keep-alive. The upgrade-insecure-requests header is 1. The full request URI is http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html. The HTTP request is 1/1. The response is in frame 20. The packet bytes pane at the bottom shows the raw data of the request, including the host header and the user-agent string.

No.	Time	Source	Destination	Protocol	Length	Info
16	2.117638	169.234.99.157	128.119.245.12	HTTP	424	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
20	2.203324	128.119.245.12	169.234.99.157	HTTP	542	HTTP/1.1 200 OK (text/html)

> Frame 16: 424 bytes on wire (3392 bits), 424 bytes captured (3392 bits) on interface 0
> Ethernet II, Src: IntelCor_28:51:77 (cc:3d:82:28:51:77), Dst: CiscoInc_c0:ac:00 (00:24:f9:c0:ac:00)
> Internet Protocol Version 4, Src: 169.234.99.157, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 9458, Dst Port: 80, Seq: 1, Ack: 1, Len: 370
▼ Hypertext Transfer Protocol
 ▼ GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n
 ▼ [Expert Info (Chat/Sequence): GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n
 [GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n
 [Severity level: Chat]
 [Group: Sequence]
 Request Method: GET
 Request URI: /wireshark-labs/HTTP-wireshark-file1.html
 Request Version: HTTP/1.1
 Host: gaia.cs.umass.edu\r\n
 User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:49.0) Gecko/20100101 Firefox/49.0\r\n
 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n
 Accept-Language: en-US,en;q=0.5\r\n
 Accept-Encoding: gzip, deflate\r\n
 DNT: 1\r\n
 Connection: keep-alive\r\n
 Upgrade-Insecure-Requests: 1\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: 20]

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 55 73 65 72 2d 41 67 65 6e s.edu..U ser-Agen
0090 74 3a 20 4d 6f 7a 69 6c 6c 61 2f 35 2e 30 20 28 t: Mozil la/5.0 (
00a0 57 69 6e 64 6f 77 73 20 4e 54 20 31 30 2e 30 3b Windows NT 10.0;
00b0 20 57 4f 57 36 34 3b 20 72 76 3a 34 39 2e 30 29 WOW64; rv:49.0)
00c0 20 47 65 63 6b 6f 2f 32 30 31 30 30 31 30 31 20 Gecko/2 0100101
00d0 46 69 72 65 66 6f 78 2f 34 39 2e 30 0d 0a 41 63 Firefox/ 49.0..Ac
00e0 63 65 70 74 3a 20 74 65 78 74 2f 68 74 6d 6c 2c cept: te xt/html,

Bytes 110-134: Host (http.host) | Packets: 40 · Displayed: 2 (5.0%) | Profile: Default

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

Answer: HTTP/1.1 200 OK (Status Code: 200, Response Phrase: OK)

The image shows a Wireshark packet capture window titled "Wi-Fi". The packet list pane at the top shows two packets. Packet 20, at time 2.203324, is an HTTP response from 128.119.245.12 to 169.234.99.157. The status is "HTTP/1.1 200 OK (text/html)".

The packet details pane for packet 20 is expanded, showing the Hypertext Transfer Protocol section. The status code is 200 and the response phrase is OK. The pane also shows the request version (HTTP/1.1), the date (Thu, 20 Oct 2016 17:01:31 GMT), the server (Apache/2.4.6 (CentOS) OpenSSL/1.0.1e-fips PHP/5.4.16 mod_perl/2.0.9dev Perl/v5.16.3), and the content type (text/html; charset=UTF-8).

The packet bytes pane at the bottom shows the raw data of the packet, with the first few bytes being "00 ed 48 e5 00 00".

At the bottom of the window, the status bar indicates "Hypertext Transfer Protocol (http), 360 bytes", "Packets: 40 · Displayed: 2 (5.0%)", and "Profile: Default".

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

Answer: Thu, 20 Oct 2016 05:59:01 GMT

The image shows a Wireshark packet capture window titled '*Wi-Fi'. The packet list pane shows two packets. Packet 16 is a GET request to /wireshark-labs/HTTP-wireshark-file1.html. Packet 20 is the corresponding 200 OK response. The packet details pane for packet 20 shows the following information:

- Frame 20: 542 bytes on wire (4336 bits), 542 bytes captured (4336 bits) on interface 0
- Ethernet II, Src: CiscoInc_c0:ac:00 (00:24:f9:c0:ac:00), Dst: IntelCor_28:51:77 (cc:3d:82:28:51:77)
- Internet Protocol Version 4, Src: 128.119.245.12, Dst: 169.234.99.157
- Transmission Control Protocol, Src Port: 80, Dst Port: 9458, Seq: 1, Ack: 371, Len: 488
- Hypertext Transfer Protocol
 - HTTP/1.1 200 OK\r\n
 - [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
 - [HTTP/1.1 200 OK\r\n]
 - [Severity level: Chat]
 - [Group: Sequence]
 - Request Version: HTTP/1.1
 - Status Code: 200
 - Response Phrase: OK
 - Date: Thu, 20 Oct 2016 17:01:31 GMT\r\n
 - Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.1e-fips PHP/5.4.16 mod_perl/2.0.9dev Perl/v5.16.3\r\n
 - Last-Modified: Thu, 20 Oct 2016 05:59:01 GMT\r\n
 - ETag: "80-53f459f51e1c7"\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: 0.085686000 seconds]
 - [Request in frame: 16]
 - File Data: 128 bytes
- Line-based text data: text/html

The packet bytes pane shows the raw data of the response, including the status line and headers.

Packet 20: 542 bytes on wire (4336 bits), 542 bytes captured (4336 bits) on interface 0

Ethernet II, Src: CiscoInc_c0:ac:00 (00:24:f9:c0:ac:00), Dst: IntelCor_28:51:77 (cc:3d:82:28:51:77)

Internet Protocol Version 4, Src: 128.119.245.12, Dst: 169.234.99.157

Transmission Control Protocol, Src Port: 80, Dst Port: 9458, Seq: 1, Ack: 371, Len: 488

Hypertext Transfer Protocol

- HTTP/1.1 200 OK\r\n
- [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
- [HTTP/1.1 200 OK\r\n]
- [Severity level: Chat]
- [Group: Sequence]
- Request Version: HTTP/1.1
- Status Code: 200
- Response Phrase: OK
- Date: Thu, 20 Oct 2016 17:01:31 GMT\r\n
- Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.1e-fips PHP/5.4.16 mod_perl/2.0.9dev Perl/v5.16.3\r\n
- Last-Modified: Thu, 20 Oct 2016 05:59:01 GMT\r\n
- ETag: "80-53f459f51e1c7"\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: 0.085686000 seconds]
- [Request in frame: 16]
- File Data: 128 bytes

Line-based text data: text/html

0030 00 ed 48 e5 00 00 48 54 54 50 2f 31 2e 31 20 32 ..H...HT TP/1.1 2

0040 30 30 20 4f 4b 0d 0a 44 61 74 65 3a 20 54 68 75 00 OK..D ate: Thu

0050 2c 20 32 30 20 4f 63 74 20 32 30 31 36 20 31 37 , 20 Oct 2016 17

0060 3a 30 31 3a 33 31 20 47 4d 54 0d 0a 53 65 72 76 :01:31 G MT..Serv

0070 65 72 3a 20 41 70 61 63 68 65 2f 32 2e 34 2e 36 er: Apac he/2.4.6

0080 20 28 43 65 6e 74 4f 53 29 20 4f 70 65 6e 53 53 (CentOS) OpenSS

0090 4c 2f 31 2e 30 2e 31 65 2d 66 69 70 73 20 50 48 L/1.0.1e -fips PH

00a0 50 2f 35 2e 34 2e 31 36 20 6d 6f 64 5f 70 65 72 P/5.4.16 mod_per

00b0 6c 2f 32 2e 30 2e 39 64 65 76 20 50 65 72 6c 2f l/2.0.9d ev Perl/

00c0 76 35 2e 31 36 2e 33 0d 0a 4c 61 73 74 2d 4d 6f v5.16.3. .Last-Mo

00d0 64 69 66 69 65 64 3a 20 54 68 75 2c 20 32 30 20 dified: Thu, 20

Hypertext Transfer Protocol (http), 360 bytes

Packets: 40 · Displayed: 2 (5.0%)

Profile: Default

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

Answer: Content-Length: 128 (128 bytes)

The image shows a Wireshark packet capture window titled "*Wi-Fi". The packet list pane at the top shows two packets. Packet 20 is an HTTP 200 OK response from 128.119.245.12 to 169.234.99.157, with a length of 542 bytes. The packet details pane shows the structure of the HTTP response, including the status bar "HTTP/1.1 200 OK\r\n", the request version "HTTP/1.1", status code "200", and response phrase "OK". The "Content-Length" header is highlighted in pink and shows a value of "128\r\n". Other headers include "Date", "Server", "Last-Modified", "ETag", "Accept-Ranges", "Keep-Alive", "Connection", and "Content-Type". The packet bytes pane at the bottom shows the raw data of the packet, with the first few bytes highlighted in blue.

No.	Time	Source	Destination	Protocol	Length	Info
16	2.117638	169.234.99.157	128.119.245.12	HTTP	424	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
20	2.203324	128.119.245.12	169.234.99.157	HTTP	542	HTTP/1.1 200 OK (text/html)

Frame 20: 542 bytes on wire (4336 bits), 542 bytes captured (4336 bits) on interface 0
> Ethernet II, Src: CiscoInc_c0:ac:00 (00:24:f9:c0:ac:00), Dst: IntelCor_28:51:77 (cc:3d:82:28:51:77)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 169.234.99.157
> Transmission Control Protocol, Src Port: 80, Dst Port: 9458, Seq: 1, Ack: 371, Len: 488
▼ Hypertext Transfer Protocol
 ▼ HTTP/1.1 200 OK\r\n
 [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
 [HTTP/1.1 200 OK\r\n]
 [Severity level: Chat]
 [Group: Sequence]
 Request Version: HTTP/1.1
 Status Code: 200
 Response Phrase: OK
 Date: Thu, 20 Oct 2016 17:01:31 GMT\r\n Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.1e-fips PHP/5.4.16 mod_perl/2.0.9dev Perl/v5.16.3\r\n Last-Modified: Thu, 20 Oct 2016 05:59:01 GMT\r\n ETag: "80-53f459f51e1c7"\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: 0.085686000 seconds]
 [Request in frame: 16]
 File Data: 128 bytes
 > Line-based text data: text/html

0030 00 ed 48 e5 00 00 48 54 54 50 2f 31 2e 31 20 32 ..H...HT TP/1.1 2
0040 30 30 20 4f 4b 0d 0a 44 61 74 65 3a 20 54 68 75 00 OK..D ate: Thu
0050 2c 20 32 30 20 4f 63 74 20 32 30 31 36 20 31 37 , 20 Oct 2016 17
0060 3a 30 31 3a 33 31 20 47 4d 54 0d 0a 53 65 72 76 :01:31 G MT..Serv
0070 65 72 3a 20 41 70 61 63 68 65 2f 32 2e 34 2e 36 er: Apac he/2.4.6
0080 20 28 43 65 6e 74 4f 53 29 20 4f 70 65 6e 53 53 (CentOS) OpenSS
0090 4c 2f 31 2e 30 2e 31 65 2d 66 69 70 73 20 50 48 L/1.0.1e -fips PH
00a0 50 2f 35 2e 34 2e 31 36 20 6d 6f 64 5f 70 65 72 P/5.4.16 mod_per
00b0 6c 2f 32 2e 30 2e 39 64 65 76 20 50 65 72 6c 2f l/2.0.9d ev Perl/
00c0 76 35 2e 31 36 2e 33 0d 0a 4c 61 73 74 2d 4d 6f v5.16.3. .Last-Mo
00d0 64 69 66 69 65 64 3a 20 54 68 75 2c 20 32 30 20 dified: Thu, 20

Hypertext Transfer Protocol (http), 360 bytes | Packets: 40 · Displayed: 2 (5.0%) | Profile: Default

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.

Answer: No. All the headers are accounted for in the raw data.

Question 2: Wireshark Labs

DNS:

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

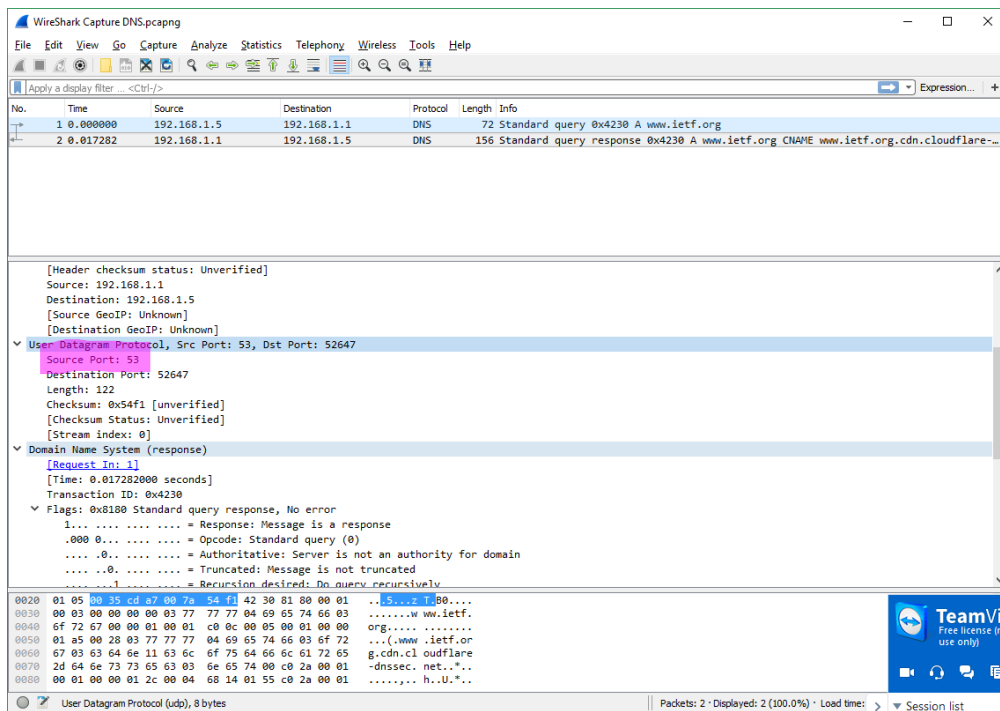
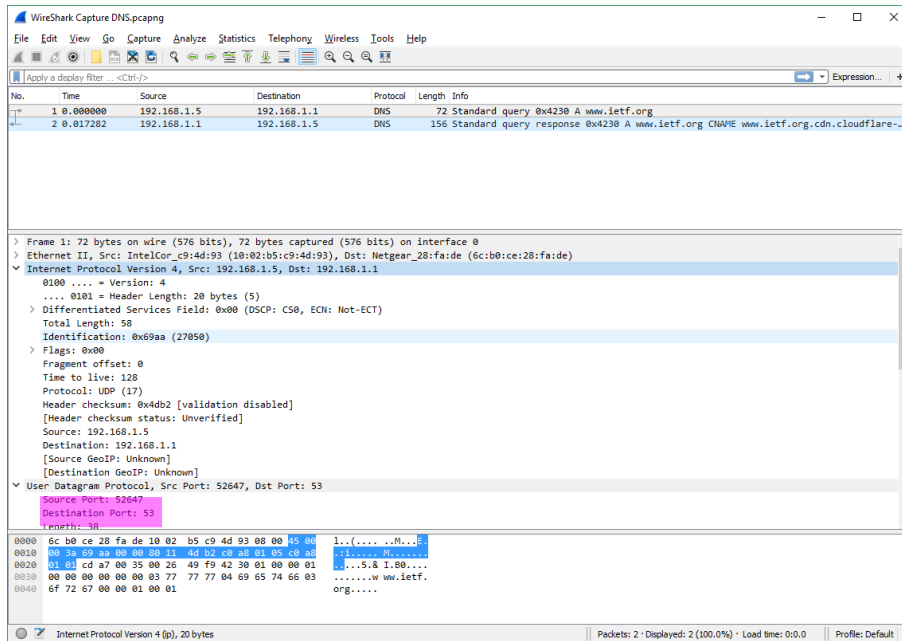
Answer: Both the query and the query response use UDP

The top screenshot shows a Wireshark capture of DNS traffic. The packet list shows two packets: a standard query (Frame 1) and a standard query response (Frame 2). The details pane for Frame 1 is expanded, showing the Internet Protocol Version 4, User Datagram Protocol, and Domain Name System (query) fields. The Domain Name System (query) field is highlighted in pink.

The bottom screenshot shows the same traffic with the response details expanded. The details pane for Frame 2 is expanded, showing the Internet Protocol Version 4, User Datagram Protocol, and Domain Name System (response) fields. The Domain Name System (response) field is highlighted in pink.

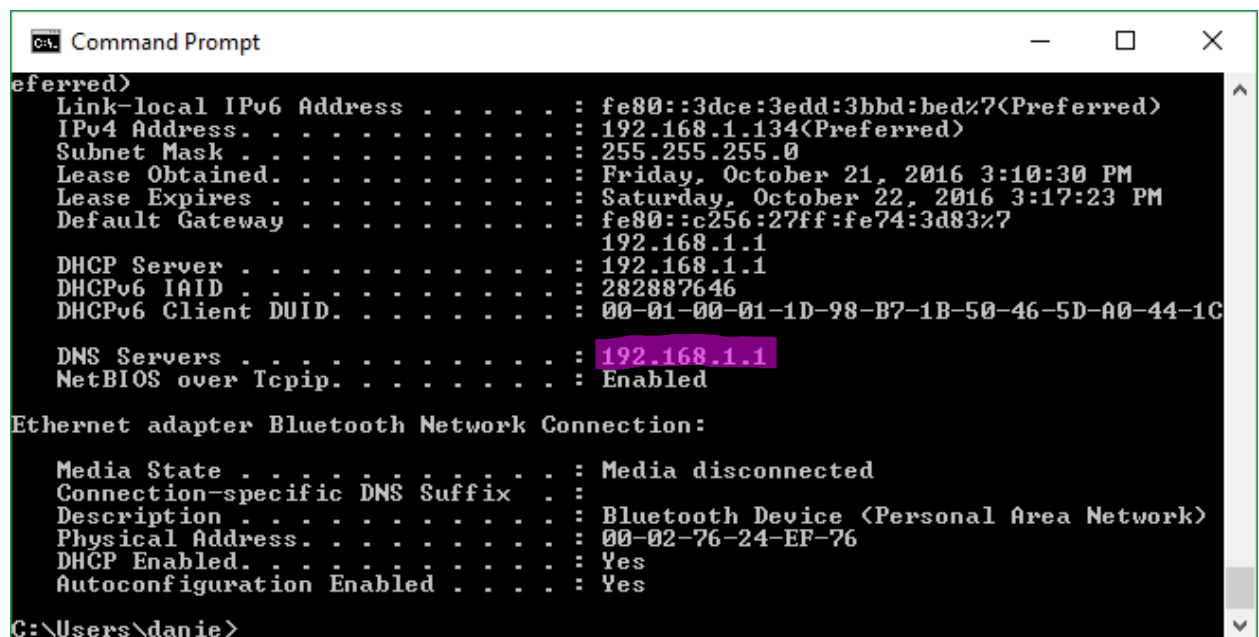
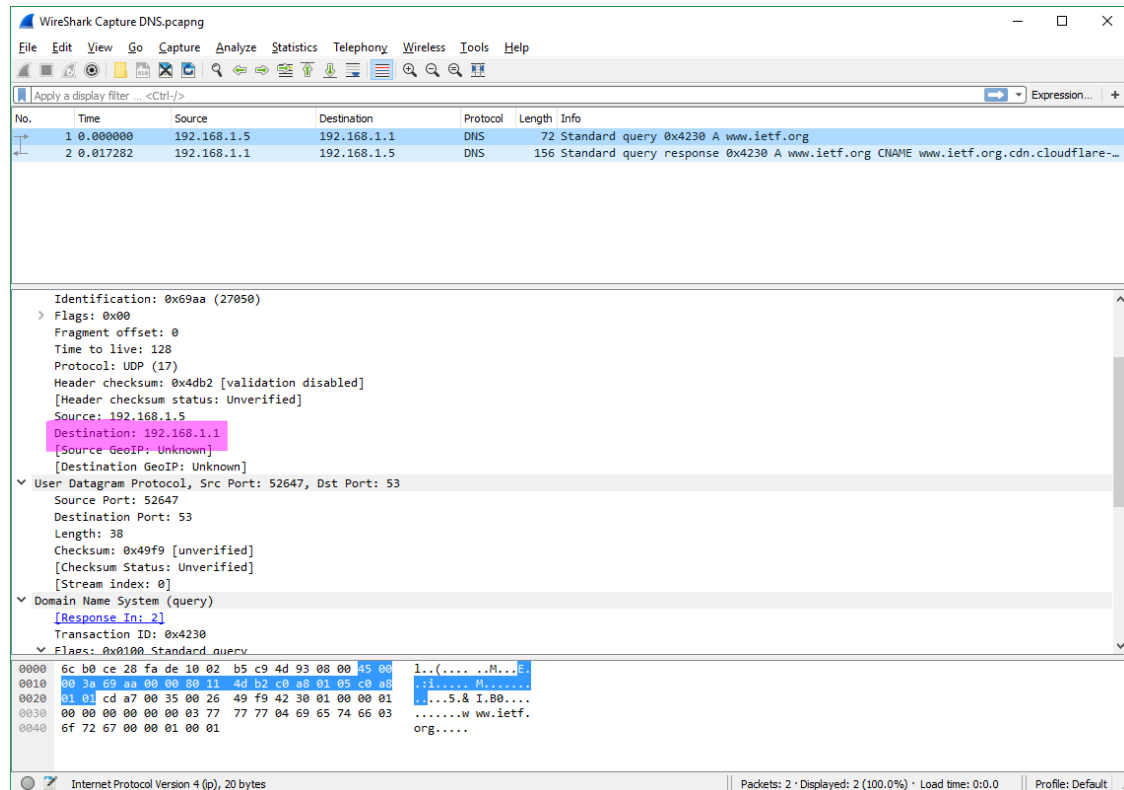
5. What is the destination port for the DNS query message? What is the source port of DNS response message?

Answer: Destination Port = 53 and Source Port = 53



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?

Answer: IP Address = 192.168.1.1 | Local DNS server IP Address = 192.168.1.1
(Local DNS was found using the command “ipconfig /all”



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

Answer: Type-A, class IN. The Query message does not have any answers associated with it.

The image shows a Wireshark capture of a DNS query message. The packet list at the top shows two packets: a standard query (packet 1) and a standard query response (packet 2). The packet details pane shows the structure of the DNS query message, including flags, questions, and queries. The query is for the domain www.ietf.org, type A, class IN. The packet bytes pane shows the raw data of the query message.

Wireshark Capture DNS.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/> Expression... +

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.1.5	192.168.1.1	DNS	72	Standard query 0x4230 A www.ietf.org
2	0.017282	192.168.1.1	192.168.1.5	DNS	156	Standard query response 0x4230 A www.ietf.org CNAME www.ietf.org.cdn.cloudflare...

Domain Name System (query)

[Response In: 2]

Transaction ID: 0x4230

Flags: 0x0100 Standard query

0... .. = Response: Message is a query

.000 0... .. = Opcode: Standard query (0)

... ..0. = Truncated: Message is not truncated

... ..1 = Recursion desired: Do query recursively

... ..0.. = Z: reserved (0)

... ..0 = Non-authenticated data: Unacceptable

Questions: 1

Answer RRs: 0

Authority RRs: 0

Additional RRs: 0

Queries

www.ietf.org: type A, class IN

Name: www.ietf.org

[Name Length: 12]

[Label Count: 3]

Type: A (Host Address) (1)

Class: IN (0x0001)

0000 6c b0 ce 28 fa de 10 02 b5 c9 4d 93 08 00 45 00 1..(.... ..M...E

0010 00 3a 69 aa 00 00 80 11 4d b2 c0 a8 01 05 c0 a8 .i.....M.....

0020 01 01 cd a7 00 35 00 26 49 f9 42 30 01 00 00 015.& I.B0....

0030 00 00 00 00 00 00 03 77 77 77 04 69 65 74 66 03w ww.ietf.

0040 6f 72 67 00 00 01 00 01 org.....

Internet Protocol Version 4 (IP), 20 bytes

Packets: 2 · Displayed: 2 (100.0%) · Load time: 0:0.0

Profile: Default

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

Answer: There were 3 answers provided. All of the answers have the following: Name, Type, Class, Time to live, and Data length. The first answer is of type “CName” and its value is www.ietf.org.cdn.cloudflare-dnssec.net. The other two responses are of type A and have addresses associated with them. (2nd: 104.20.1.85, 3rd: 104.20.0.85)

The image shows a Wireshark capture of a DNS response message. The packet list at the top shows two packets: a query (No. 1) and a response (No. 2). The response packet is selected, and the packet details pane shows the following structure:

- [Name Length: 12]
- [Label Count: 3]
- Type: A (Host Address) (1)
- Class: IN (0x0001)
- Answers
 - www.ietf.org: type CNAME, class IN, cname www.ietf.org.cdn.cloudflare-dnssec.net
 - Name: www.ietf.org
 - Type: CNAME (Canonical NAME for an alias) (5)
 - Class: IN (0x0001)
 - Time to live: 421
 - Data length: 40
 - CNAME: www.ietf.org.cdn.cloudflare-dnssec.net
 - www.ietf.org.cdn.cloudflare-dnssec.net: type A, class IN, addr 104.20.1.85
 - Name: www.ietf.org.cdn.cloudflare-dnssec.net
 - Type: A (Host Address) (1)
 - Class: IN (0x0001)
 - Time to live: 300
 - Data length: 4
 - Address: 104.20.1.85
 - www.ietf.org.cdn.cloudflare-dnssec.net: type A, class IN, addr 104.20.0.85
 - Name: www.ietf.org.cdn.cloudflare-dnssec.net
 - Type: A (Host Address) (1)
 - Class: IN (0x0001)
 - Time to live: 300
 - Data length: 4
 - Address: 104.20.0.85

The packet bytes pane at the bottom shows the raw data of the response packet, with the following text representation:

```
0010 00 8e 00 00 40 00 40 11 b7 08 c0 a8 01 01 c0 a8 ...@. ....
0020 01 05 00 35 cd a7 00 7a 54 f1 42 30 81 80 00 01 ...5...z T.80...
0030 00 03 00 00 00 00 03 77 77 77 04 69 65 74 66 03 .....w ww.ietf
0040 6f 72 67 00 00 01 00 01 c0 0c 00 05 00 01 00 00 ORG.....
0050 01 a5 00 28 03 77 77 77 04 69 65 74 66 03 6f 72 ...(.www .ietf.or
0060 67 03 63 64 6e 11 63 6c 6f 75 64 66 6c 61 72 65 g.cdn.cl oudflare
0070 2d 64 6e 73 73 65 63 03 6e 65 74 00 c0 2a 00 01 -dnssec. net.*..
0080 00 01 00 00 01 2c 00 04 68 14 01 55 c0 2a 00 01 ..... h..U.*..
0090 00 01 00 00 01 2c 00 04 68 14 00 55 ..... h..U
```

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

Answer: The destination port in the query message is 53. The source port of the response message is 53

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

Answer: The IP address is 192.168.1.1. This is the same address as the local DNS server (found by using ipconfig /all).

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

Answer: The DNS query message is type A, it does not contain any answers.

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

Answer: The response message contains 3 answers. Each answer contains a name, a type, a class, time to live, data length, and either an address (if type A) or a CNAME (if type CNAME).

15. Provide a screenshot.

The image displays two screenshots of the Wireshark network protocol analyzer interface, showing a sequence of DNS packets.

Top Screenshot: Wireshark - Packet 12

- Packet 12:** 71 bytes on wire (568 bits), 71 bytes captured (568 bits) on interface 0.
- Ethernet II:** Src: IntelCor_c9:4d:93 (10:02:b5:c9:4d:93), Dst: Netgear_28:fa:de (6c:b0:ce:28:fa:de).
- Internet Protocol Version 4:** Src: 192.168.1.5, Dst: 192.168.1.1.
- User Datagram Protocol:** Src Port: 55802, Dst Port: 53.
- Domain Name System (query):**
 - [Response In: 13]
 - Transaction ID: 0x0002
 - Flags: 0x0100 Standard query
 - Questions: 1
 - Answer RRs: 0
 - Authority RRs: 0
 - Additional RRs: 0
 - Queries:
 - www.mit.edu: type A, class IN

The packet bytes pane shows the raw data of the query, including the domain name 'www.mit.edu' in ASCII and hexadecimal.

Bottom Screenshot: Wireshark - Packet 13

- Packet 13:** 160 bytes on wire (1280 bits), 160 bytes captured (1280 bits) on interface 0.
- Ethernet II:** Src: Netgear_28:fa:de (6c:b0:ce:28:fa:de), Dst: IntelCor_c9:4d:93 (10:02:b5:c9:4d:93).
- Internet Protocol Version 4:** Src: 192.168.1.1, Dst: 192.168.1.5.
- User Datagram Protocol:** Src Port: 53, Dst Port: 55802.
- Domain Name System (response):**
 - [Request In: 12]
 - [Time: 0.008682000 seconds]
 - Transaction ID: 0x0002
 - Flags: 0x8180 Standard query response, No error
 - Questions: 1
 - Answer RRs: 3
 - Authority RRs: 0
 - Additional RRs: 0
 - Queries:
 - www.mit.edu: type A, class IN
 - Answers:
 - www.mit.edu: type CNAME, class IN, cname www.mit.edu.edgekey.net
 - www.mit.edu.edgekey.net: type CNAME, class IN, cname e9566.dscb.akamaiedge.net
 - e9566.dscb.akamaiedge.net: type A, class IN, addr 23.66.128.128

The packet bytes pane shows the raw data of the response, including the CNAME chain and the IP address '23.66.128.128'.

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

Answer: The IP address is 192.168.1.1. This is the same address as the local DNS server (found by using ipconfig /all).

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

Answer: The query is of NS and contains no 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?

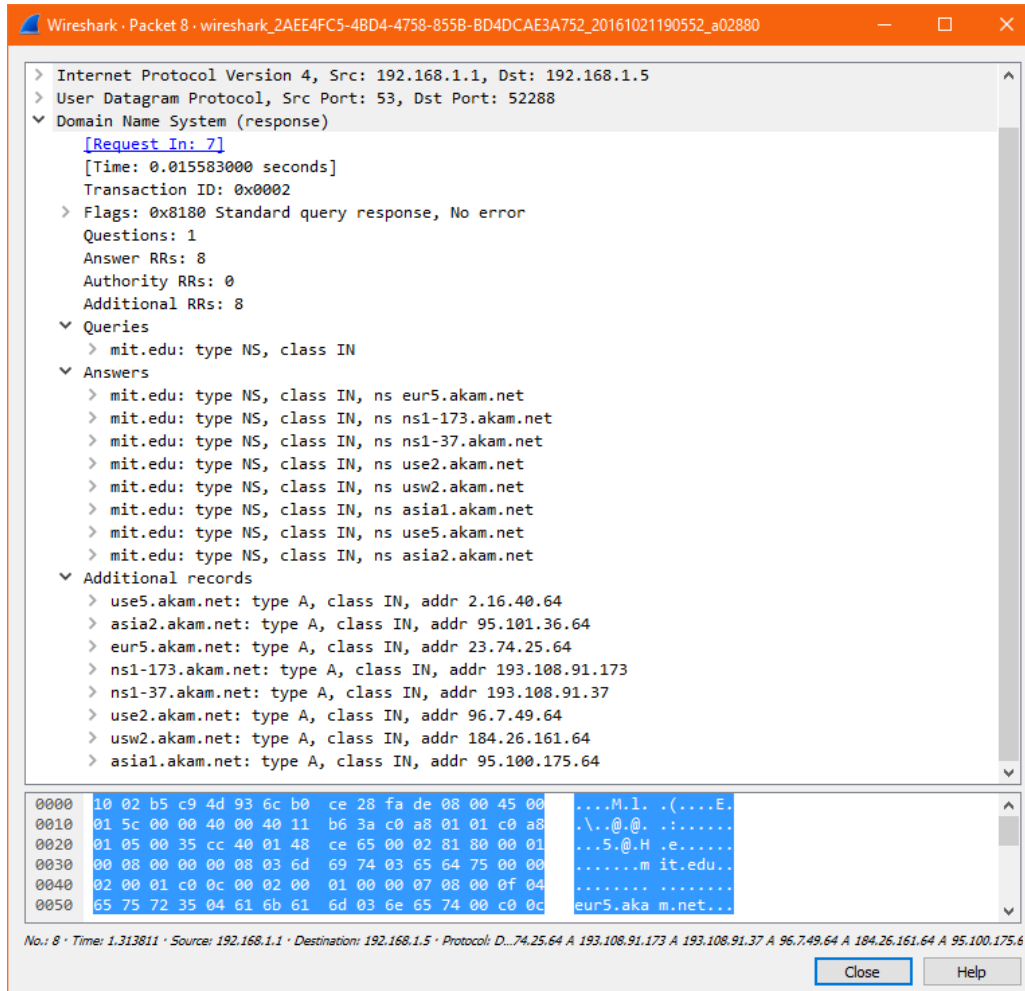
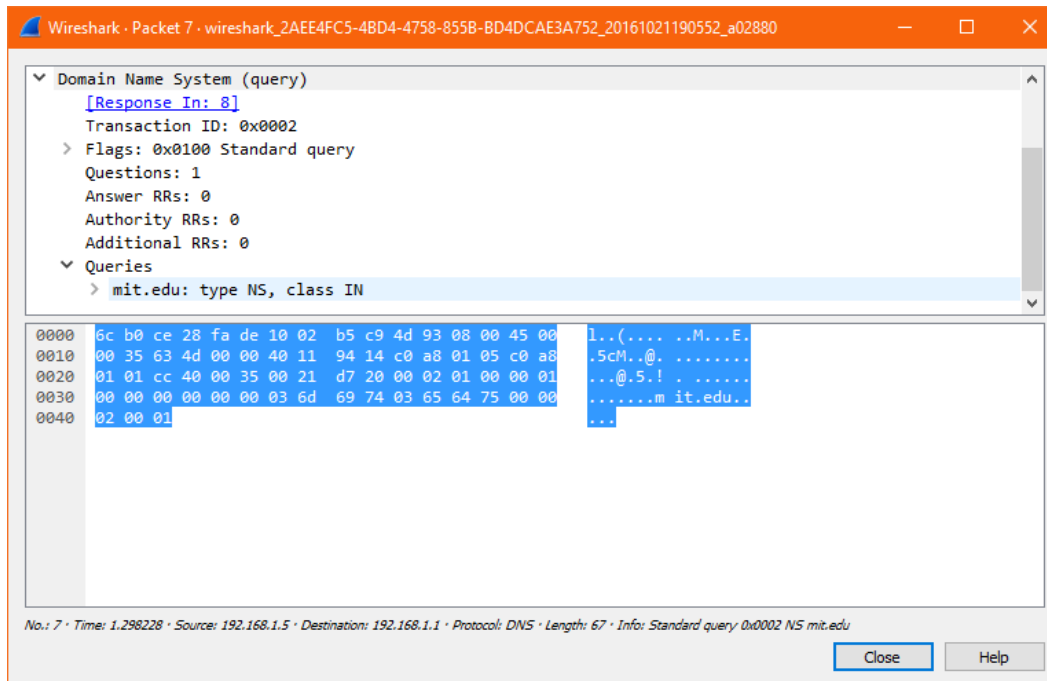
Answer: The nameservers provided are as follows:

```
mit.edu: type NS, class IN, ns eur5.akam.net
mit.edu: type NS, class IN, ns ns1-173.akam.net
mit.edu: type NS, class IN, ns ns1-37.akam.net
mit.edu: type NS, class IN, ns use2.akam.net
mit.edu: type NS, class IN, ns usw2.akam.net
mit.edu: type NS, class IN, ns asia1.akam.net
mit.edu: type NS, class IN, ns use5.akam.net
mit.edu: type NS, class IN, ns asia2.akam.net
```

In addition, the IP addresses of the nameservers are also provided:

```
▼ Additional records
  > use5.akam.net: type A, class IN, addr 2.16.40.64
  > asia2.akam.net: type A, class IN, addr 95.101.36.64
  > eur5.akam.net: type A, class IN, addr 23.74.25.64
  > ns1-173.akam.net: type A, class IN, addr 193.108.91.173
  > ns1-37.akam.net: type A, class IN, addr 193.108.91.37
  > use2.akam.net: type A, class IN, addr 96.7.49.64
  > usw2.akam.net: type A, class IN, addr 184.26.161.64
  > asia1.akam.net: type A, class IN, addr 95.100.175.64
```

19. Provide a screenshot.

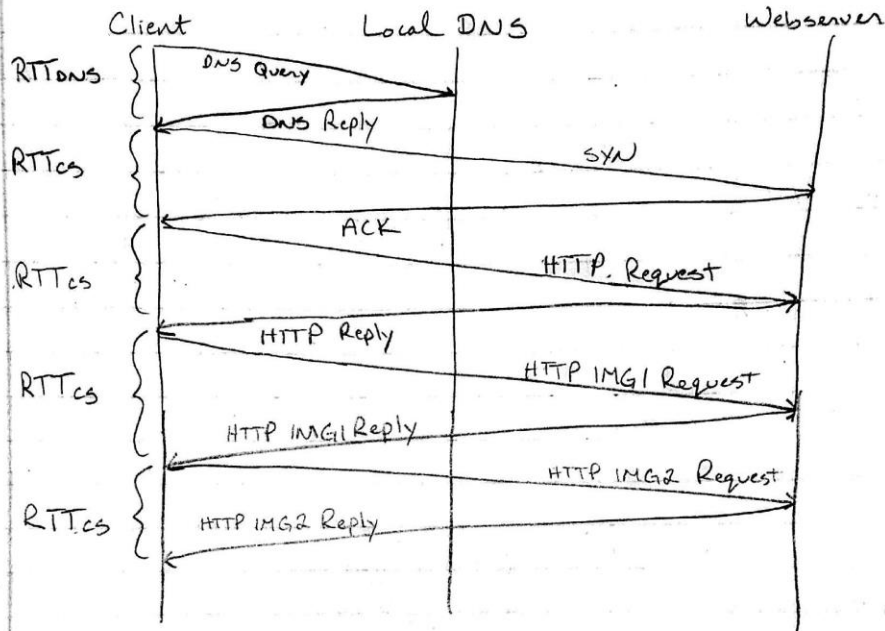


Daniel Lara
ID: 49651280
Zachary Hart
ID: 70953123
CS 132

Homework #2

Question 3

(a)



Totals $RTT_{dns} + 4 * RTT_{cs}$

