

Willis Allstead
9/23/18
CPE 400

HW1

Part 1

1.

a)

a \leftrightarrow b is 1Mb/s

b \leftrightarrow c is 2 Mb/s

transmission delay = (packet length)/(link bandwidth)

transmission delay over link A – B = $(1,000*8)/(1,000,000) = 0.008\text{s}$

transmission delay over link B – C = $(1,000*8)/(2,000,000) = 0.004\text{s}$

b)

nodal processing delay at B = 1ms = 0.001s

queuing delay at B = 3ms = 0.003s

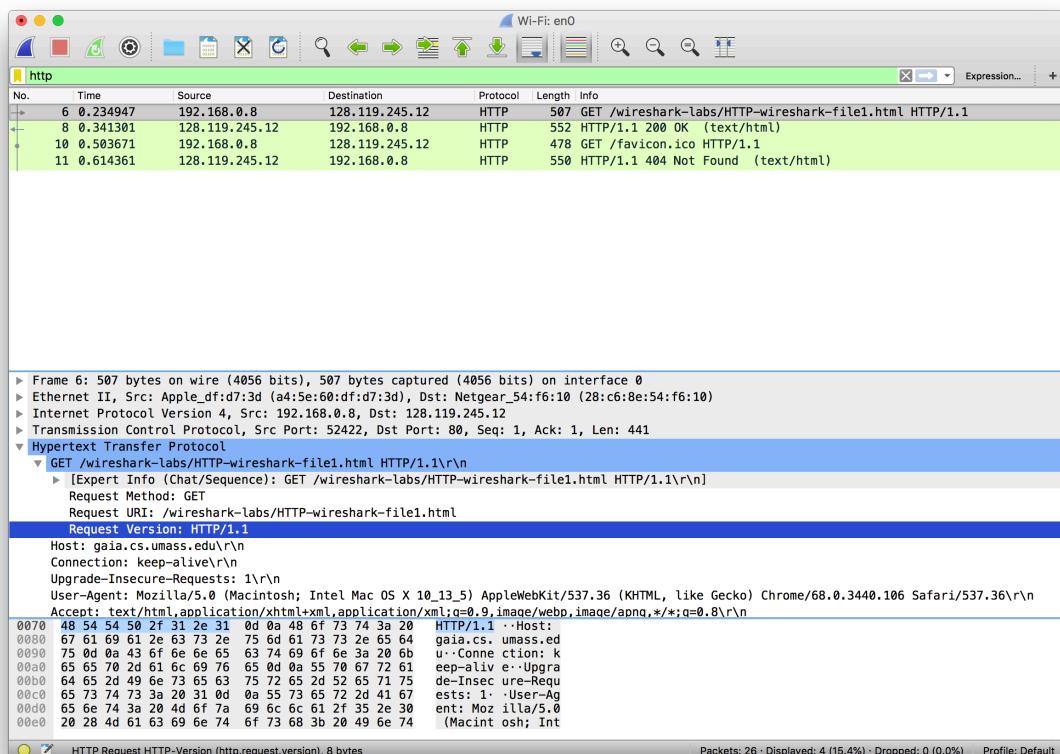
propagation delay at B = 0

Total delay from A to C = $0.008\text{s} + 0.004\text{s} + 0.003\text{s} + 0.001\text{s} = 0.016\text{s}$

Part 2

2.

a) HTTP version 1.1 is running



b) My computer's IP address: 192.168.0.8, gaia.cs.umass.edu server IP address: 128.119.245.12

The screenshot shows a Wireshark capture window with the following details:

- Protocol:** http
- Selected Frame:** 6 (0.234947)
- Source:** 192.168.0.8
- Destination:** 128.119.245.12
- Protocol:** HTTP
- Length:** 507
- Info:** GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1

The expanded frame details show the request:

```

> Transmission Control Protocol, Src Port: 52422, Dst Port: 80, Seq: 1, Ack: 1, Len: 441
  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]
        Request Method: GET
        Request URL: /wireshark-labs/HTTP-wireshark-file1.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 (Macintosh; Intel Mac OS X 10_13_5) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/68.0.3440.106 Safari/537.36\r\n
        Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8\r\n
        Accept-Encoding: gzip, deflate\r\n
        Accept-Language: en-US,en;q=0.9,fr;q=0.8\r\n
    \r\n
00a0 65 65 70 2d 61 6c 69 76 65 0d 0a 55 70 67 72 61  eep-aliv e..Upgra
00b0 64 65 2d 49 6e 73 65 63 75 72 65 2d 52 65 71 75  de-Insec ure-Requ
00c0 65 73 74 73 3a 20 31 0d 0a 55 73 65 72 2d 41 67  ests: 1 :User-Ag
00d0 65 6e 74 3a 20 4d 6f 7a 69 6c 6c 61 2f 35 2e 30  ent: Moz illa/5.0
00e0 20 28 4d 61 63 69 6e 74 f7 73 68 3b 20 49 6e 74  (Macint osh; Int
00f0 65 6c 20 4d 61 63 28 4f 53 20 58 20 31 30 5f 31 el Mac O S X 10_1
0100 33 5f 35 29 20 41 70 70 6c 65 57 65 62 4b 69 74  3.5) App leWebKit
0110 2f 35 33 37 2e 33 36 20 28 4b 48 54 4d 4c 2c 20  /537.36 (KHTML,

```

Request line (http.request.line), 30 bytes

Packets: 26 · Displayed: 4 (15.4%) · Dropped: 0 (0.0%) · Profile: Default

c) Status Code returned from the server to my browser: 200

The screenshot shows a Wireshark capture window with the following details:

- Protocol:** http
- Selected Frame:** 8 (0.341301)
- Source:** 128.119.245.12
- Destination:** 192.168.0.8
- Protocol:** HTTP
- Length:** 552
- Info:** HTTP/1.1 200 OK (text/html)

The expanded frame details show the response:

```

> Frame 8: 552 bytes on wire (4416 bits), 552 bytes captured (4416 bits) on interface 0
  Ethernet II, Src: Netgear_54:f6:10 (28:c6:8e:54:f6:10), Dst: Apple_df:d7:3d (a4:5e:60:df:d7:3d)
  Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.0.8
  Transmission Control Protocol, Src Port: 80, Dst Port: 52422, Seq: 1, Ack: 442, Len: 486
  Hypertext Transfer Protocol
    HTTP/1.1 200 OK\r\n
      [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
        Response Version: HTTP/1.1
        Status Code: 200
        [Status Code Description: OK]
    
```

d) The HTML file was last-modified on: Sun, 23 Sep 2018 05:59:01 GMT

The Wireshark interface is shown with the 'http' protocol selected. The main pane displays several network frames, with frame 11 highlighted in green. The details pane shows the following information:

```

> [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
  Response Version: HTTP/1.1
  Status Code: 200
  [Status Code Description: OK]
  Response Phrase: OK
  Date: Mon, 24 Sep 2018 03:38:40 GMT\r\n
  Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/5.4.16 mod_perl/2.0.10 Perl/v5.16.3\r\n
  Last-Modified: Sun, 23 Sep 2018 05:59:01 GMT\r\n
  ETag: "80-5768391bd6c9f"\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
00d0 33 0d 0a 4c 61 73 74 2d 4d 6f 64 69 66 69 65 64 3..Last- Modified
00e0 3a 20 53 75 6e 2c 20 32 33 20 53 65 70 20 32 30  : Sun, 2 3 Sep 20
00f0 31 38 20 30 35 3a 35 39 3a 30 31 20 47 4d 54 0d 18 05:59 :01 GMT
0100 0a 45 54 61 67 3a 20 22 38 30 2d 35 37 36 38 33 .ETag: " 80-57683
0110 39 31 62 64 36 63 39 66 22 0d 0a 41 63 63 65 70 91bd6c9f "·Accep
0120 74 2d 52 61 66 67 65 73 3a 20 62 79 74 65 73 0d t-Ranges : bytes·
0130 0a 43 6f 6e 74 65 6e 74 2d 4c 65 6e 67 74 68 3a ·Content -Length:
0140 20 31 32 38 0d 0a 4b 65 65 70 2d 41 6c 69 76 65 128 ·Ke ep-Alive
  
```

Part 3

3.

a) There is no IF-MODIFIED-SINCE header in the first request. (in first screenshot). The content is explicitly returned by the server in the first response as shown by the line-based text data in the response. (in second screenshot)

The Wireshark interface is shown with the 'http' protocol selected. The main pane displays several network frames, with frame 1018 highlighted in green. The details pane shows the following information:

```

> Frame 914: 507 bytes on wire (4056 bits), 507 bytes captured (4056 bits) on interface 0
> Ethernet II, Src: Apple_dfd:d7:3d (a4:5e:60:df:d7:3d), Dst: Netgear_54:f6:10 (28:c6:8e:54:f6:10)
> Internet Protocol Version 4, Src: 192.168.0.8, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 52536, Dst Port: 80, Seq: 1, Ack: 1, Len: 441
  ▼ 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 (Macintosh; Intel Mac OS X 10_13_5) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/68.0.3440.106 Safari/537.36
      Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8\r\n
      Accept-Encoding: gzip, deflate\r\n
      Accept-Language: en-US,en;q=0.9,gb;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: 918]
      [Next request in frame: 1017]
  
```

The bottom pane shows the raw hex and ASCII data for the selected frame:

```

0040 35 f9 47 45 54 20 2f 77 69 72 65 73 68 61 72 6b 5..GET /w ireshark
0050 2d 6c 61 62 73 2f 48 54 54 50 2d 77 69 72 65 73 -labs/HT TP-wires
0060 68 61 72 60 2d 66 69 64 65 32 2e 68 74 6d 6c 20 hark-fil e2.html
0070 48 54 50 2f 31 2e 31 0d 0a 48 6f 73 74 3a 20 HTTP/1.1 ..Host:
0080 67 61 69 61 2e 63 73 2d 75 6d 61 73 73 2e 65 64 gaia.cs. umass.ed
0090 75 0d 0a 43 6f 6e 65 63 74 69 6f 6e 3a 20 6b u..Conne ction: k
00a0 65 65 70 2d 61 6c 69 76 65 0d 0a 55 70 67 72 61 eep-aliv e..Upgra
00b0 64 65 2d 49 6e 73 65 63 75 72 65 2d 52 65 71 75 de-Insec ure-Requ
  
```

```

No. Time Source Destination Protocol Length Info
914 7.566610 192.168.0.8 128.119.245.12 HTTP 507 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
918 7.672474 128.119.245.12 192.168.0.8 HTTP 796 HTTP/1.1 200 OK (text/html)
1017 11.033448 192.168.0.8 128.119.245.12 HTTP 619 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
1018 11.135610 128.119.245.12 192.168.0.8 HTTP 305 HTTP/1.1 304 Not Modified

Last-Modified: Sun, 23 Sep 2018 05:59:01 GMT\r\n
ETag: "173-5768391bd60e7"\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: 0.105864000 seconds]
[Request in frame: 914]
[Next request in frame: 1017]
[Next response in frame: 1018]
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. <br>\n
This file's last modification date will not change. <p>\n
Thus if you download this multiple times on your browser, a complete copy <br>\n
will only be sent once by the server due to the inclusion of the IN-MODIFIED-SINCE<br>\n
field in your browser's HTTP GET request to the server.\n
\n
</html>

```

Hex dump of the file content:

```

01a0  55 54 46 2d 38 0d 0a 0d 0a 0a 3c 68 74 6d 6c 3e  UTF-8...<html>
01b0  0a 05 43 6f 6e 67 72 61 74 75 6e 61 74 69 6f 6e  <Congratulation
01c0  73 70 65 67 69 6e 21 20 20 4e 6f 77 69 70 79 6f  s again!
01d0  75 27 76 65 20 64 6f 77 6e 6c 6f 61 64 65 64 20  u've dow nloaded
01e0  74 68 65 20 66 69 6c 65 20 6c 61 62 32 2d 32 2e  the file lab2-2,
01f0  68 74 6d 6c 2e 20 3c 62 72 3c 0a 54 68 69 73 20  html.<b></b> This
0200  66 69 6c 65 27 73 20 6c 61 73 74 20 6d 6f 64 69  file's l ast modi
0210  66 69 63 61 74 69 6f 6e 20 64 61 74 65 20 77 69  fication date wi

```

b) There is an IF-MODIFIED-SINCE header in the first request. It contains “Sun, 23 Sep 2018 05:59:01 GMT\r\n” (in first screenshot). The server responds with Status Code 304: Not Modified (in second screenshot and line below selection). This is because there has been no change to the data since the last request not long ago. There is no need to respond with all of the data.

```

No. Time Source Destination Protocol Length Info
914 7.566610 192.168.0.8 128.119.245.12 HTTP 507 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
918 7.672474 128.119.245.12 192.168.0.8 HTTP 796 HTTP/1.1 200 OK (text/html)
1017 11.033448 192.168.0.8 128.119.245.12 HTTP 619 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
1018 11.135610 128.119.245.12 192.168.0.8 HTTP 305 HTTP/1.1 304 Not Modified

► Frame 1017: 619 bytes on wire (4952 bits), 619 bytes captured (4952 bits) on interface 0
► Ethernet II, Src: Apple_df:07:3d (aa:5e:60:df:d7:3d), Dst: Netgear_54:f6:10 (28:c6:8e:54:f6:10)
► Internet Protocol Version 4, Src: 192.168.0.8, Dst: 128.119.245.12
► Transmission Control Protocol, Src Port: 52536, Dst Port: 80, Seq: 442, Ack: 731, Len: 553
▼ 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
      Cache-Control: max-age=0\r\n
      Upgrade-Insecure-Requests: 1\r\n
      User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_13_5) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/68.0.3440.106 Safari/537.36\r\n
      Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8\r\n
      Accept-Encoding: gzip, deflate\r\n
      Accept-Language: en-US,en;q=0.9,nb;q=0.8\r\n
      If-None-Match: "173-5768391bd60e7"\r\n
      If-Modified-Since: Sun, 23 Sep 2018 05:59:01 GMT\r\n
    \r\n
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]
    [HTTP request 2/2]
    [Prev request in frame: 914]
    [Response in frame: 1018]

01f0  4c 61 6e 67 75 61 67 65 3a 20 65 6e 2d 55 53 2c  Language : en-US,
0200  65 6e 3b 71 3d 30 2e 39 2c 6e 62 3b 71 3d 30 2e  en;q=0.9 ,nb;q=0.
0210  38 0d 0a 49 66 2d 4e 6f 6e 65 2b 4d 61 74 63 68  8·If-No ne-Match
0220  3a 20 22 31 37 33 2d 35 37 36 38 33 39 31 62 64  : "173-5 768391bd
0230  36 30 65 37 22 0d 0a 49 66 2d 4d 6f 64 69 66 69 60e7"·I f-Modifi
0240  65 64 2d 53 69 6e 63 65 3a 20 53 75 6e 2c 20 32  ed-Since : Sun, 2
0250  33 20 53 65 70 20 32 30 31 38 20 30 35 3a 35 39  3 Sep 20 18 05:59
0260  3a 30 31 20 47 4d 54 0d 0a 0d 0a :01 GMT. ...

```

Frame 1018: 305 bytes on wire (2440 bits), 305 bytes captured (2440 bits) on interface 0

Ethernet II, Src: Netgear_54:f6:10 (28:c6:8e:54:f6:10), Dst: Apple_df:d7:3d (a4:5e:60:df:d7:3d)

Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.0.8

Transmission Control Protocol, Src Port: 80, Dst Port: 52536, Seq: 731, Ack: 995, Len: 239

Hypertext Transfer Protocol

- HTTP/1.1 304 Not Modified\r\n
- [Expert Info (Chat/Sequence): HTTP/1.1 304 Not Modified\r\n]
- Response Version: HTTP/1.1
- Status Code: 304
- [Status Code Description: Not Modified]
- Response Phrase: Not Modified
- Date: Mon, 24 Sep 2018 03:53:55 GMT\r\n
- Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/5.4.16 mod_perl/2.0.10 Perl/v5.16.3\r\n
- Connection: Keep-Alive\r\n
- Keep-Alive: timeout=5, max=99\r\n
- ETag: "173-5768391bd60e7"\r\n
- \r\n
- [HTTP response 2/2]
- [Time since request: 0.102162000 seconds]
- [Prev request in frame: 914]
- [Prev response in frame: 918]
- [Request in frame: 1017]

```

0040 d4 51 48 54 54 50 2f 31 2e 31 20 33 30 34 20 4e 0 HTTP/1.1 304 N
0050 6f 74 20 4d 6f 64 69 66 69 65 64 0d 0a 44 61 74 ot Modif ied-Dat
0060 65 3a 20 4d 6f 6e 20 32 34 20 53 65 70 20 32 e: Mon, 24 Sep 2
0070 30 31 38 20 30 33 3a 35 33 3a 35 35 20 47 4d 54 018 03:5 3:55 GMT
0080 0d 0a 53 65 72 76 65 72 3a 20 41 70 61 63 68 65 ..Server : Apache
0090 2f 32 2e 34 2e 36 20 28 43 65 6e 74 4f 53 29 20 /2.4.6 ( CentOS)
00a0 4f 70 65 6e 53 53 4c 2f 31 2e 30 2e 32 6b 2d 66 OpenSSL/ 1.0.2k-f
00b0 69 70 73 20 50 48 50 2f 35 2e 34 2e 31 36 20 6d ips PHP/ 5.4.16 m

```

Part 4

4.

- a) The IP Addresses given was: 216.58.193.174. This was achieved with command:
`nslookup google.com`.

```

1. bash
Williss-MacBook-Pro:~ willisallstead$ nslookup google.com
Server:      192.168.0.1
Address:     192.168.0.1#53

Non-authoritative answer:
Name:   google.com
Address: 216.58.193.174

Williss-MacBook-Pro:~ willisallstead$ 

```

b) As you can see above, there was no server obviously designated as the one giving the answer. But, you can see that it is a non-authoritative answer. It seems like 192.168.0.1 is the server giving the response.

c) I found that the response in wireshark listed the A-record (as was expected by not specifying the type), a TTL of 226, and an address of 172.217.4.14 (which was the address of the server it was pointing to this time).

The Wireshark interface displays a list of network frames. The first frame (3) is a standard query from 192.168.0.8 to 192.168.0.1 for 'google.com'. The second frame (4) is a standard query response from 192.168.0.1 to 192.168.0.8. Subsequent frames show TCP ACKs and unseen segments between 192.168.0.8 and 192.168.0.1. The details pane shows the DNS request and response, indicating a non-authoritative answer with TTL 226 and address 172.217.4.14. The bytes pane shows the raw hex and ASCII data of the DNS message.

No.	Time	Source	Destination	Protocol	Length	Info
3	0.425940	192.168.0.8	192.168.0.1	DNS	70	Standard query 0x638e A google.com
4	0.454458	192.168.0.1	192.168.0.8	DNS	86	Standard query response 0x638e A google.com A 172.217.4.14
1	0.000000	192.168.0.8	192.0.73.2	TCP	54	52693 → 443 [ACK] Seq=1 Ack=1 Win=8192 Len=0
2	0.016106	192.0.73.2	192.168.0.8	TCP	60	[TCP ACKed unseen segment] 443 → 52693 [ACK] Seq=1 Ack=2 Win=64 Len=0
5	0.500827	192.168.0.8	104.16.28.34	TCP	54	52673 → 443 [ACK] Seq=1 Ack=1 Win=8192 Len=0
6	0.538625	104.16.28.34	192.168.0.8	TCP	60	[TCP ACKed unseen segment] 443 → 52673 [ACK] Seq=1 Ack=2 Win=34 Len=0
7	1.001884	192.168.0.8	151.101.1.69	TCP	54	52671 → 443 [ACK] Seq=1 Ack=1 Win=7988 Len=0
8	1.040114	151.101.1.69	192.168.0.8	TCP	66	[TCP ACKed unseen segment] 443 → 52671 [ACK] Seq=1 Ack=2 Win=120 Len=0 TSval=1136

Frame 4: 86 bytes on wire (688 bits), 86 bytes captured (688 bits) on interface 0
 Ethernet II, Src: Netgear_54:f6:10 (28:c6:8e:54:f6:10), Dst: Apple_df:d7:3d (a4:5e:60:df:d7:3d)
 Internet Protocol Version 4, Src: 192.168.0.1, Dst: 192.168.0.8
 User Datagram Protocol, Src Port: 53, Dst Port: 53960
 Domain Name System (response)
 Transaction ID: 0x638e
 Flags: 0x8100 Standard query response, No error
 Questions: 1
 Answer RR: 1
 Authority RR: 0
 Additional RR: 0
 Queries
 google.com: type A, class IN
 Name: google.com
 [Name Length: 10]
 [Label Count: 2]
 Type: A (Host Address) (1)
 Class: IN (0x0001)
 Answers
 google.com: type A, class IN, addr 172.217.4.14
 Name: google.com
 Type: A (Host Address) (1)
 Class: IN (0x0001)
 Time to live: 226
 Data length: 4
 Address: 172.217.4.14
 [Request In: 3]
 [Time: 0.028518000 seconds]

```

0000 a4 5e 60 df d7 3d 28 c6 8e 54 f6 10 08 00 45 00 .^...=(. T...E.
0010 00 48 00 00 40 00 40 11 b9 4b c0 a8 00 01 c0 a8 .H-@ @- K.....
0020 00 08 00 35 d2 c8 00 34 41 89 63 8e 81 80 00 01 ..5...4 A-c.....
0030 00 01 00 00 00 00 06 67 6f 6f 67 6c 65 03 63 6f .....g oogle.co
0040 6d 00 00 01 00 01 c0 0c 00 01 00 01 00 00 00 e2 m..... .
0050 00 04 ac d9 04 0e ..... .

```

d) I ran the command shown in the screenshot below and got the following results. In wireshark I received 4 answers of type NS for my query if google.com. Each contained a name server, like ns1.google.com, ns2.google.com, etc.

```
1. bash
Williss-MacBook-Pro:~ willisallstead$ nslookup -type=NS google.com
Server:      192.168.0.1
Address:     192.168.0.1#53

Non-authoritative answer:
google.com      nameserver = ns2.google.com.
google.com      nameserver = ns1.google.com.
google.com      nameserver = ns4.google.com.
google.com      nameserver = ns3.google.com.

Authoritative answers can be found from:

Williss-MacBook-Pro:~ willisallstead$
```

The Wireshark screenshot shows the following details:

- Network Summary:** Shows two DNS requests (No. 1823 and 1839) and one DNS response (No. 1839). The requests are from 192.168.0.8 to 192.168.0.1, and the response is from 192.168.0.1 to 192.168.0.8. The response is a Standard query response (Type: 0x967b) for the query 0x967b NS google.com, containing the NS record for ns2.google.com.
- Detailed View:** The packet details for No. 1839 show the DNS response. The "Info" column displays the raw hex and ASCII data of the response message, which includes the NS record for ns2.google.com.
- Answers Section:** The "Answers" section of the DNS tab lists four NS records for google.com, each pointing to a different Google name server (ns2.google.com, ns1.google.com, ns4.google.com, ns3.google.com).

e) I ran the command shown in the screenshot below using ns1.google.com instead of the default nameserver. You can see that in the wireshark response the answer was of type A but there was no mention in either nslookup or wireshark of the response being non-authoritative.

```
Williss-MacBook-Pro:~ willisallstead$ nslookup google.com ns1.google.com
Server:      ns1.google.com
Address:     216.239.32.10#53

Name:   google.com
Address: 216.58.194.206

Williss-MacBook-Pro:~ willisallstead$ █
```

No.	Time	Source	Destination	Protocol	Length	Info
7	0.759713	192.168.0.8	216.239.32.10	DNS	70	Standard query 0x5678 A google.com
8	0.830720	216.239.32.10	192.168.0.8	DNS	86	Standard query response 0x5678 A google.com A 216.58.194.206

► Frame 8: 86 bytes on wire (688 bits), 86 bytes captured (688 bits) on interface 0
► Ethernet II, Src: Netgear_54:f6:10 (28:c6:8e:54:f6:10), Dst: Apple_df:d7:3d (a4:5e:60:df:d7:3d)
► Internet Protocol Version 4, Src: 216.239.32.10, Dst: 192.168.0.8
► User Datagram Protocol, Src Port: 53, Dst Port: 53869
▼ Domain Name System (response)
 Transaction ID: 0x5678
► Flags: 0x8500 Standard query response, No error
 Questions: 1
 Answer RRs: 1
 Authority RRs: 0
 Additional RRs: 0
▼ Queries
 ▼ google.com: type A, class IN
 Name: google.com
 [Name Length: 10]
 [Label Count: 2]
 Type: A (Host Address) (1)
 Class: IN (0x0001)
▼ Answers
 ▼ google.com: type A, class IN, addr 216.58.194.206
 Name: google.com
 Type: A (Host Address) (1)
 Class: IN (0x0001)
 Time to live: 300
 Data length: 4
 Address: 216.58.194.206
[\[Request In: 7\]](#)
[Time: 0.071007000 seconds]

```
0000 a4 5e 60 df d7 3d 28 c6 8e 54 f6 10 08 00 45 00 .^`-=··T-E·
0010 00 48 a2 af 00 00 66 11 f8 4b d8 ef 20 0a c0 a8 ·H-f-K···
0020 00 08 00 35 d2 6d 00 34 2b 56 78 85 00 00 01 ··5·m4(Vx··
0030 00 01 00 00 00 00 06 67 6f 6d 6c 65 03 63 6f .....oogle.co
0040 6d 00 00 01 00 01 c0 0c 00 01 00 01 00 00 01 2c m.....··········
0050 00 04 d8 3a c2 ce ..:::·
```