

ECS 152A Programming 2

Daniel Phan
ID 914831996
Section A04

Noah Tarr
ID 917286014
Section A02

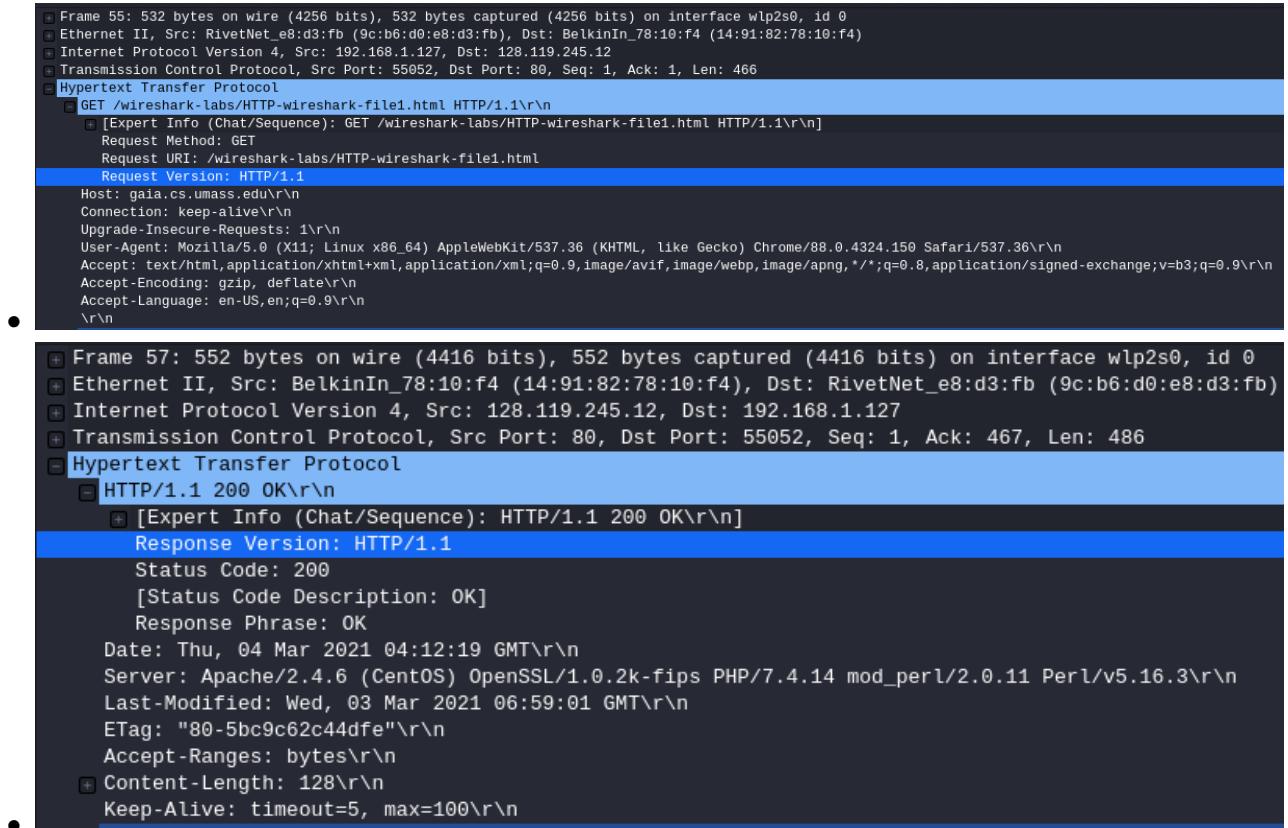
Due: 03/07/2021

1 HTTP Wireshark Lab

1.1 The Basic HTTP GET/Response Interaction

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

- Both my browser and the server are running HTTP version 1.1.



The screenshot shows two network captures in Wireshark:

- HTTP GET Request:** Frame 55 (highlighted in blue).
 - Request Method: GET
 - Request URI: /wireshark-labs/HTTP-wireshark-file1.html
 - Request Version: HTTP/1.1
 - Host: gaia.cs.umass.edu
 - Connection: keep-alive
 - Upgrade-Insecure-Requests: 1
 - User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/88.0.4324.150 Safari/537.36
 - Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
 - Accept-Encoding: gzip, deflate
 - Accept-Language: en-US,en;q=0.9
- HTTP Response:** Frame 57 (highlighted in blue).
 - Response Version: HTTP/1.1
 - Status Code: 200 [Status Code Description: OK]
 - Date: Thu, 04 Mar 2021 04:12:19 GMT
 - Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.14 mod_perl/2.0.11 Perl/v5.16.3
 - Last-Modified: Wed, 03 Mar 2021 06:59:01 GMT
 - ETag: "80-5bc9c62c44dfe"
 - Accept-Ranges: bytes
 - Content-Length: 128
 - Keep-Alive: timeout=5, max=100

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

- My browser indicates that it accepts US English.

```

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 URI: /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 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/88.0.4324.150 Safari/537.36\r\n
      Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9\r\n
      Accept-Encoding: gzip, deflate\r\n
      Accept-Language: en-US,en;q=0.9\r\n

```

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

```

  • My IP address is 192.168.1.127, while the server's IP address is 128.119.245.12.

    [+] Internet Protocol Version 4, Src: 192.168.1.127, Dst: 128.119.245.12
      0100 .... = Version: 4
      .... 0101 = Header Length: 20 bytes (5)
      [+] Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
          Total Length: 518
          Identification: 0x41f6 (16886)
      [+] Flags: 0x40, Don't fragment
          Fragment Offset: 0
          Time to Live: 64
          Protocol: TCP (6)
          Header Checksum: 0xbff50 [validation disabled]
          [Header checksum status: Unverified]
          Source Address: 192.168.1.127
          Destination Address: 128.119.245.12
    • Internet Protocol Version 4, Src: 192.168.1.127, Dst: 128.119.245.12
      0100 .... = Version: 4
      .... 0101 = Header Length: 20 bytes (5)
      [+] Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
          Total Length: 518
          Identification: 0x41f6 (16886)
      [+] Flags: 0x40, Don't fragment
          Fragment Offset: 0
          Time to Live: 64
          Protocol: TCP (6)
          Header Checksum: 0xbff50 [validation disabled]
          [Header checksum status: Unverified]
          Source Address: 192.168.1.127
          Destination Address: 128.119.245.12

```

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

- The server returned 200 for the HTML file and 404 for favico.ico.

```

[+] 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]
     Response Phrase: OK
     Date: Thu, 04 Mar 2021 04:12:19 GMT\r\n
     Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.14 mod_perl/2.0.11 Perl/v5.16.3\r\n
     Last-Modified: Wed, 03 Mar 2021 06:59:01 GMT\r\n
     ETag: "80-5bc9c62c44dfe"\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
   • Content-Type: text/html; charset=UTF-8\r\n

  •

[+] Hypertext Transfer Protocol
  [+] HTTP/1.1 404 Not Found\r\n
    [+ [Expert Info (Chat/Sequence): HTTP/1.1 404 Not Found\r\n]
     Response Version: HTTP/1.1
     Status Code: 404
     [Status Code Description: Not Found]
     Response Phrase: Not Found
     Date: Thu, 04 Mar 2021 04:12:19 GMT\r\n
     Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.14 mod_perl/2.0.11 Perl/v5.16.3\r\n
     Content-Length: 209\r\n
     Keep-Alive: timeout=5, max=99\r\n
     Connection: Keep-Alive\r\n
     Content-Type: text/html; charset=iso-8859-1\r\n
     \r\n
     [HTTP response 2/2]
   • [Time since request: 0.095551449 seconds]

```

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

- It was last modified on March 3, 2021, at 06:59:01 GMT.

```

[+] 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]
     Response Phrase: OK
     Date: Thu, 04 Mar 2021 04:12:19 GMT\r\n
     Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.14 mod_perl/2.0.11 Perl/v5.16.3\r\n
     Last-Modified: Wed, 03 Mar 2021 06:59:01 GMT\r\n
     ETag: "80-5bc9c62c44dfe"\r\n
     Accept-Ranges: bytes\r\n
   •

```

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

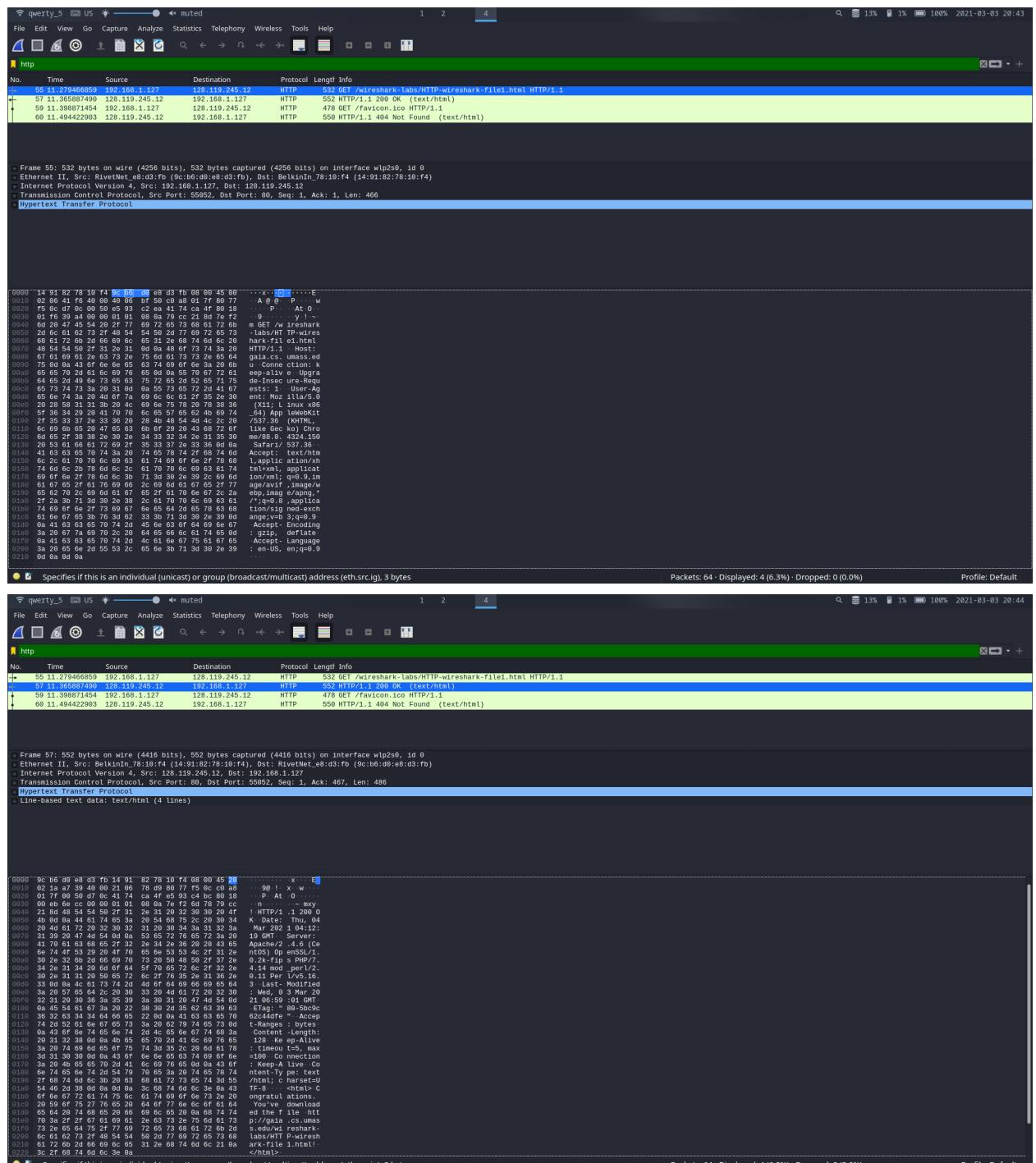
- There were 128 bytes for the HTML file, and 209 bytes for favico.ico.

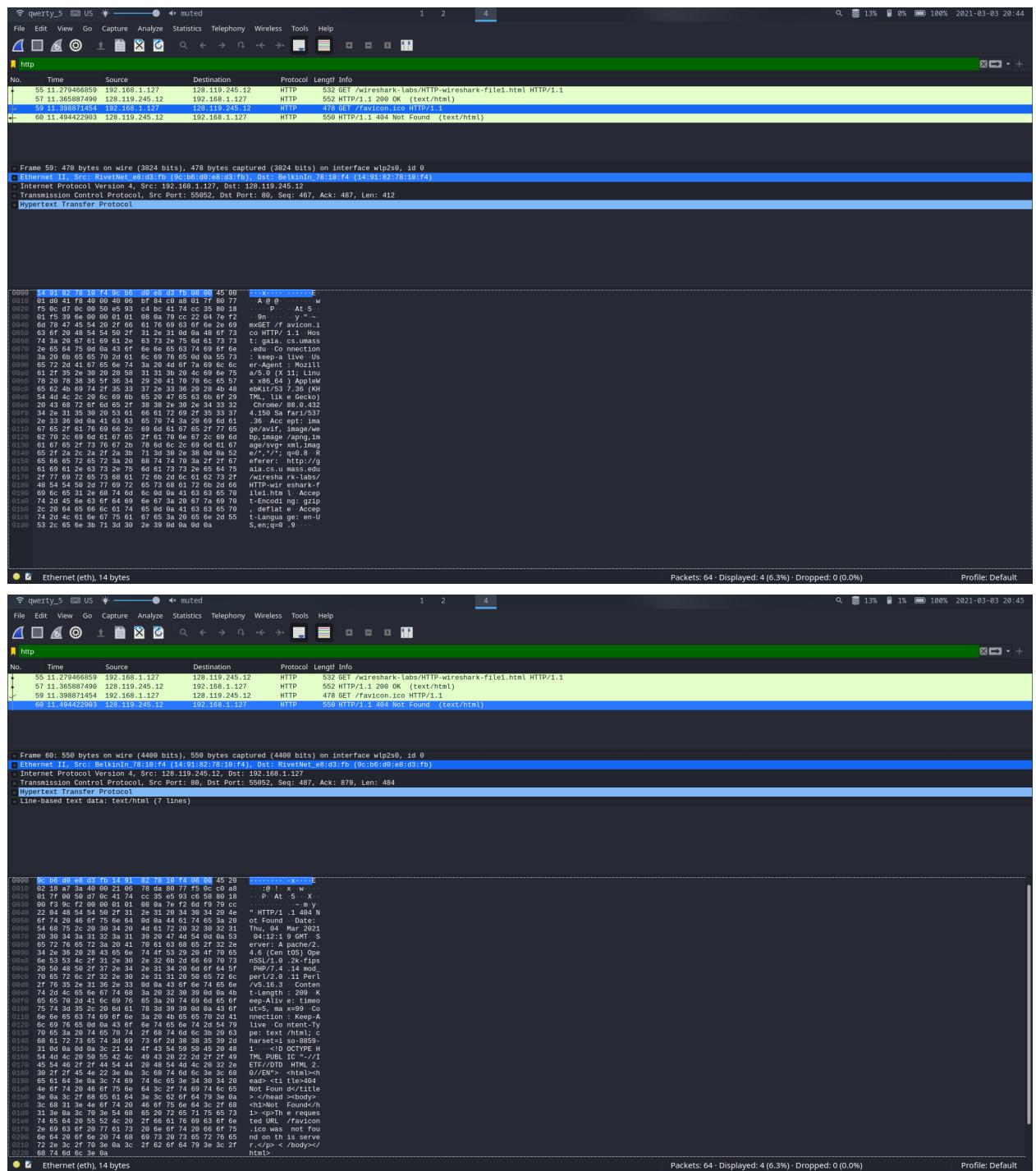
```

[+] 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]
      Response Phrase: OK
      Date: Thu, 04 Mar 2021 04:12:19 GMT\r\n
      Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.14 mod_perl/2.0.11 Perl/v5.16.3\r\n
      Last-Modified: Wed, 03 Mar 2021 06:59:01 GMT\r\n
      ETag: "80-5bc9c62c44dfe"\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 1/2]
    •
  [+] Hypertext Transfer Protocol
    [+] HTTP/1.1 404 Not Found\r\n
      [+] [Expert Info (Chat/Sequence): HTTP/1.1 404 Not Found\r\n]
        Response Version: HTTP/1.1
        Status Code: 404
        [Status Code Description: Not Found]
        Response Phrase: Not Found
        Date: Thu, 04 Mar 2021 04:12:19 GMT\r\n
        Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.14 mod_perl/2.0.11 Perl/v5.16.3\r\n
      [+ Content-Length: 209\r\n
        Keep-Alive: timeout=5, max=99\r\n
        Connection: Keep-Alive\r\n
        Content-Type: text/html; charset=iso-8859-1\r\n
        \r\n
        [HTTP response 2/2]
      •
      [Time since request: 0.095551449 seconds]
    •
  
```

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.

- I do not see any headers that are not displayed.





1.2 The HTTP CONDITIONAL GET/response interaction

- 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?

- I do not see an “IF-MODIFIED-SINCE” line in the HTTP GET.

```

Hypertext Transfer Protocol
  GET /wireshark-labs/HTTP-wireshark-file2.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 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/88.0.4324.150 Safari/537.36\r\n
  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9\r\n
  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 1/2]
[Response in frame: 85]
[Next request in frame: 86]

```

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

- The server explicitly returned the contents. I can tell because the response contains the HTML file content, and content fields like “Content-Type” and “Content Length” are set.

```

Connection: Keep-Alive\r\n
Content-Type: text/html; charset=UTF-8\r\n
\r\n
[HTTP response 1/2]
[Time since request: 0.088990448 seconds]
[Request in frame: 83]
[Next request in frame: 88]
[Next response in frame: 89]
[Request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]
File Data: 371 bytes
Line-based text data: text/html (10 lines)
\r\n
<html>\r\n
\r\n
Congratulations again! Now you've downloaded the file lab2-2.html. <br>\r\n
This file's last modification date will not change. <p>\r\n
Thus if you download this multiple times on your browser, a complete copy <br>\r\n
will only be sent once by the server due to the inclusion of the IN-MODIFIED-SINCE<br>\r\n
field in your browser's HTTP GET request to the server.\r\n
</html>\r\n

```

```

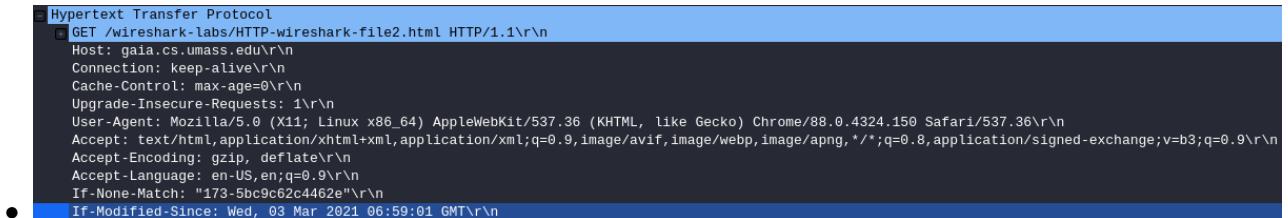
Hypertext Transfer Protocol
  HTTP/1.1 200 OK\r\n
  Date: Thu, 04 Mar 2021 04:59:38 GMT\r\n
  Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.14 mod_perl/2.0.11 Perl/v5.16.3\r\n
  Last-Modified: Wed, 03 Mar 2021 06:59:01 GMT\r\n
  ETag: "173-5bc9c62c4462e"\r\n
  Accept-Ranges: bytes\r\n
  Content-Length: 371\r\n
    [Content length: 371]
  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: 0.088990448 seconds]
[Request in frame: 83]
[Next request in frame: 88]
[Next response in frame: 89]
[Request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]
File Data: 371 bytes

```

- 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?

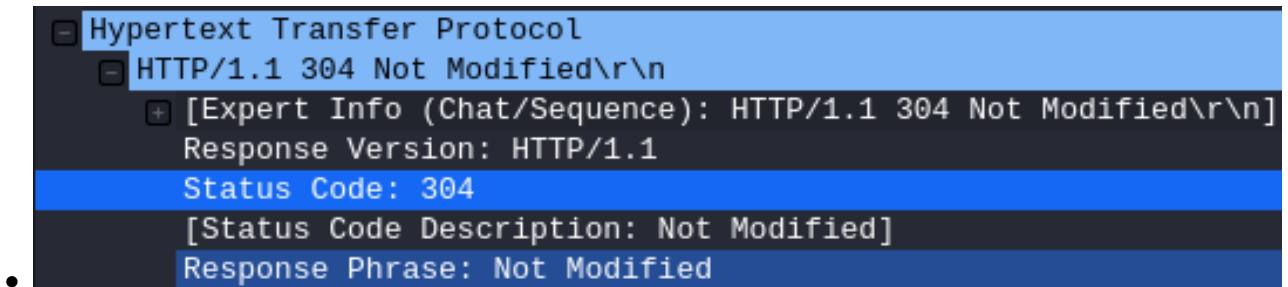
- There is an “If-Modified-Since” line, and it contains “Wed, 03 Mar 2021 06:59:01 GMT”.



```
Hypertext Transfer Protocol
  GET /wireshark-labs/HTTP-wireshark-file2.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
  Upgrade-Insecure-Requests: 1\r\n
  User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/88.0.4324.150 Safari/537.36\r\n
  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9\r\n
  Accept-Encoding: gzip, deflate\r\n
  Accept-Language: en-US,en;q=0.9\r\n
  If-None-Match: "173-5bc9c62c4462e"\r\n
  ● If-Modified-Since: Wed, 03 Mar 2021 06:59:01 GMT\r\n
```

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?

- The HTTP status code is 304 and the response phrase is “Not Modified”. The server did not explicitly return the contents of the file, as none of the signs described in the response to question 9 appeared here.

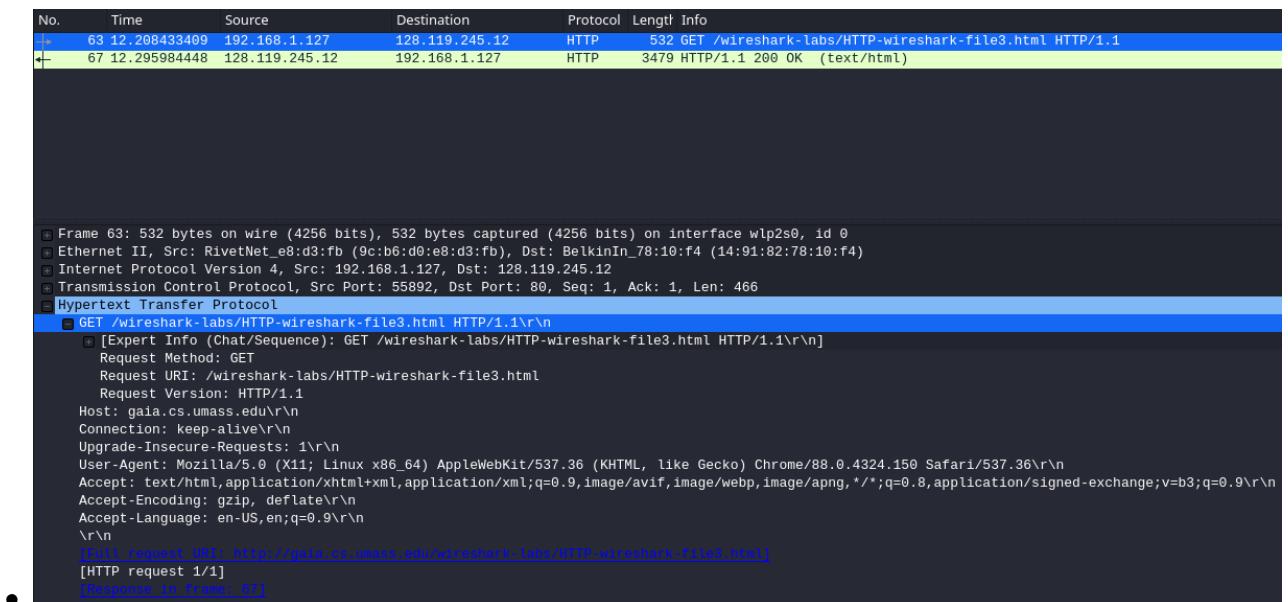


```
  ○ Hypertext Transfer Protocol
    ○ HTTP/1.1 304 Not Modified\r\n
      + [Expert Info (Chat/Sequence): HTTP/1.1 304 Not Modified\r\n]
      Response Version: HTTP/1.1
      Status Code: 304
      [Status Code Description: Not Modified]
      Response Phrase: Not Modified
  ●
```

1.3 Retrieving Long Documents

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?

- My browser sent one HTTP GET request. The packet number was 63.



No.	Time	Source	Destination	Protocol	Length	Info
63	12.209433409	192.168.1.127	128.119.245.12	HTTP	532	GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
67	12.295984448	128.119.245.12	192.168.1.127	HTTP	3479	HTTP/1.1 200 OK (text/html)

```
  + Frame 63: 532 bytes on wire (4256 bits), 532 bytes captured (4256 bits) on interface wlp2s0, id 0
  + Ethernet II, Src: RivetNet_e8:d3:fb (9c:b6:d0:e8:d3:fb), Dst: BelkinIn_78:10:f4 (14:91:82:78:10:f4)
  + Internet Protocol Version 4, Src: 192.168.1.127, Dst: 128.119.245.12
  + Transmission Control Protocol, Src Port: 80, Dst Port: 55892, Seq: 1, Ack: 1, Len: 466
  + Hypertext Transfer Protocol
    + GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1\r\n
      + [Expert Info (Chat/Sequence): GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1\r\n]
      Request Method: GET
      Request URI: /wireshark-labs/HTTP-wireshark-file3.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 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/88.0.4324.150 Safari/537.36\r\n
      Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9\r\n
      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-file3.html]
      [HTTP request 1/1]
      [Response in frame: 67]
```

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 is 65. We see that the response was broken into 2 TCP segments. The raw data of the first segment, packet 65, is highlighted in blue, and we see the HTTP status code and phrase at the top of the raw data.

[2 Reassembled TCP Segments (4861 bytes): #65(1448), #67(3413)]
[Frame: 65, payload: 0-1447 (1448 bytes)]
[Frame: 67, payload: 1448-4860 (3413 bytes)]
[Segment count: 2]
[Reassembled TCP length: 4861]
[Reassembled TCP Data: 485454502f312e3120323030204f4b0d0a446174653a205468752c2030342]

00000	48 54 54 50 2f 31 2e 31 20 32 30 30 20 4f 4b 0d	HTTP/1.1 200 OK·
00010	0a 44 61 74 65 3a 20 54 68 75 2c 20 30 34 20 4d	·Date: Thu, 04 M
00020	61 72 20 32 30 32 31 20 30 35 3a 33 34 3a 34 33	ar 2021 05:34:43
00030	20 47 4d 54 0d 0a 53 65 72 76 65 72 3a 20 41 70	GMT··Se rver: Ap
00040	61 63 68 65 2f 32 2e 34 2e 36 20 28 43 65 6e 74	ache/2.4 .6 (Cent
00050	4f 53 29 20 4f 70 65 6e 53 53 4c 2f 31 2e 30 2e	OS) Open SSL/1.0.
00060	32 6b 2d 66 69 70 73 20 50 48 50 2f 37 2e 34 2e	2k-fips PHP/7.4.
00070	31 34 20 6d 6f 64 5f 70 65 72 6c 2f 32 2e 30 2e	14 mod_p erl/2.0.
00080	31 31 20 50 65 72 6c 2f 76 35 2e 31 36 2e 33 0d	11 Perl/ v5.16.3·
00090	0a 4c 61 73 74 2d 4d 6f 64 69 66 69 65 64 3a 20	·Last-Mo dified:
000a0	57 65 64 2c 20 30 33 20 4d 61 72 20 32 30 32 31	Wed, 03 Mar 2021
000b0	20 30 36 3a 35 39 3a 30 31 20 47 4d 54 0d 0a 45	06:59:0 1 GMT··E
000c0	54 61 67 3a 20 22 31 31 39 34 2d 35 62 63 39 63	Tag: "11 94-5bc9c
000d0	36 32 63 33 66 62 66 36 22 0d 0a 41 63 63 65 70	62c3fbf6 "··Accep
000e0	74 2d 52 61 6e 67 65 73 3a 20 62 79 74 65 73 0d	t-Ranges : bytes·
000f0	0a 43 6f 6e 74 65 6e 74 2d 4c 65 6e 67 74 68 3a	·Content -Length:
01000	20 34 35 30 30 0d 0a 4b 65 65 70 2d 41 6c 69 76	4500··K eep-Aliv
01100	65 3a 20 74 69 6d 65 6f 75 74 3d 35 2c 20 6d 61	e: timeo ut=5, ma
01200	78 3d 31 30 30 0d 0a 43 6f 6e 6e 65 63 74 69 6f	x=100··C onnectio
01300	6e 3a 20 4b 65 65 70 2d 41 6c 69 76 65 0d 0a 43	n: Keep- Alive··C
01400	6f 6e 74 65 6e 74 2d 54 79 70 65 3a 20 74 65 78	ontent-T ype: tex
01500	74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d	t/html; charset=
01600	55 54 46 2d 38 0d 0a 0d 0a 3c 68 74 6d 6c 3e 3c	UTF-8·· ·<html><

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

- The status code is 200, and the phrase is “OK”.

Hypertext Transfer Protocol
HTTP/1.1 200 OK\r\nn
[Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\nn]
Response Version: HTTP/1.1
Status Code: 200
[Status Code Description: OK]
Response Phrase: OK

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

- 2 data-containing TCP segments were needed.

```

[2 Reassembled TCP Segments (4861 bytes): #65(1448), #67(3413)]
[Frame: 65, payload: 0-1447 (1448 bytes)]
[Frame: 67, payload: 1448-4860 (3413 bytes)]
[Segment count: 2]
[Reassembled TCP length: 4861]
[Reassembled TCP Data: 485454502f312e3120323030204f4b0d0a446174653a205468752c203034204d6172203...]

```

1.4 HTML Documents with Embedded Objects

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

- 3 HTTP GET requests were sent. The first two went to 128.119.245.12 (`gaia.cs.umass.edu`), while the third went to 178.79.137.164 (`kurose.cslash.net`).

89 16.301100606 192.168.1.127	128.119.245.12	HTTP	532 GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
91 16.387613418 128.119.245.12	192.168.1.127	HTTP	1367 HTTP/1.1 200 OK (text/html)
93 16.426631679 192.168.1.127	128.119.245.12	HTTP	478 GET /pearson.png HTTP/1.1
99 16.513495514 128.119.245.12	192.168.1.127	HTTP	2229 HTTP/1.1 200 OK (PNG)
104 16.684490700 192.168.1.127	178.79.137.164	HTTP	445 GET /8E_cover_small.jpg HTTP/1.1
108 16.898240272 178.79.137.164	192.168.1.127	HTTP	237 HTTP/1.1 301 Moved Permanently
Internet Protocol Version 4, Src: 192.168.1.127, Dst: 128.119.245.12			
0100 = Version: 4			
.... 0101 = Header Length: 20 bytes (5)			
+ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)			
Total Length: 518			
Identification: 0x067a (1658)			
+ Flags: 0x40, Don't fragment			
Fragment Offset: 0			
Time to Live: 64			
Protocol: TCP (6)			
Header Checksum: 0xfacc [validation disabled]			
[Header checksum status: Unverified]			
Source Address: 192.168.1.127			
Destination Address: 128.119.245.12			
Hypertext Transfer Protocol			
+ GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1\r\n			
+ [Expert Info (Chat/Sequence): GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1\r\n]			
Request Method: GET			
Request URI: /wireshark-labs/HTTP-wireshark-file4.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 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/88.0.4324.150 Safari/537.36\r\n			
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9\r\n			
Accept-Encoding: gzip, deflate\r\n			
Accept-Language: en-US,en;q=0.9\r\n			

```

[+] Internet Protocol Version 4, Src: 192.168.1.127, Dst: 128.119.245.12
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
[+] Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 464
    Identification: 0x067c (1660)
[+] Flags: 0x40, Don't fragment
    Fragment Offset: 0
    Time to Live: 64
    Protocol: TCP (6)
    Header Checksum: 0xfb00 [validation disabled]
        [Header checksum status: Unverified]
    Source Address: 192.168.1.127
    Destination Address: 128.119.245.12
● Hypertext Transfer Protocol
    GET /pearson.png HTTP/1.1\r\n
    Host: gaia.cs.umass.edu\r\n
    Connection: keep-alive\r\n
    User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/88.0.4324.150 Safari/537.36\r\n
    Accept: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8\r\n
    Referer: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file4.html\r\n
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: en-US,en;q=0.9\r\n
● Internet Protocol Version 4, Src: 192.168.1.127, Dst: 178.79.137.164
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
[+] Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 431
    Identification: 0x542e (21550)
[+] Flags: 0x40, Don't fragment
    Fragment Offset: 0
    Time to Live: 64
    Protocol: TCP (6)
    Header Checksum: 0xe6ff [validation disabled]
        [Header checksum status: Unverified]
    Source Address: 192.168.1.127
    Destination Address: 178.79.137.164
● Hypertext Transfer Protocol
    GET /8E_cover_small.jpg HTTP/1.1\r\n
    Host: kurose.cslash.net\r\n
    Connection: keep-alive\r\n
    User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/88.0.4324.150 Safari/537.36\r\n
    Accept: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8\r\n
    Referer: http://gaia.cs.umass.edu/\r\n
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: en-US,en;q=0.9\r\n

```

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 images were downloaded serially. The last packet for `pearson.png` (packet 99) arrived before the GET request for `8E_cover_small.jpg` (packet 104) was sent.

93	16.426631679	192.168.1.127	128.119.245.12	HTTP	478	GET /pearson.png	HTTP/1.1
99	16.513495514	128.119.245.12	192.168.1.127	HTTP	2229	HTTP/1.1 200 OK	(PNG)
104	16.684490700	192.168.1.127	178.79.137.164	HTTP	445	GET /8E_cover_small.jpg	HTTP/1.1
108	16.898240272	178.79.137.164	192.168.1.127	HTTP	237	HTTP/1.1 301 Moved	Permanently

1.5 HTTP Authentication

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

- The server responded with 401 and “Unauthorized”.

```

[+] Hypertext Transfer Protocol
  [+] HTTP/1.1 401 Unauthorized\r\n
    + [Expert Info (Chat/Sequence): HTTP/1.1 401 Unauthorized\r\n]
      Response Version: HTTP/1.1
      Status Code: 401
      [Status Code Description: Unauthorized]
      Response Phrase: Unauthorized
  
```

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 “Authorization” and “Cache-Control” fields are new.

```

[+] Hypertext Transfer Protocol
  [+] GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.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 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/88.0.4324.150 Safari/537.36\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9\r\n
    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-wireshark-file5.html]
  [HTTP request 1/1]
  [Response in frame 13]

[+] Hypertext Transfer Protocol
  [+] GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.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 d2lyZXNoYXJrLXN0dWlbnRz0m5ldHdvcmzs=\r\n
    Upgrade-Insecure-Requests: 1\r\n
    User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/88.0.4324.150 Safari/537.36\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9\r\n
    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-wireshark-file5.html]
  [HTTP request 1/1]
  [Response in frame 30]
  
```

2 DNS and dig

- (a) Starting with a root DNS server (from one of the root servers [a-m].root-servers.net), initiate a sequence of queries for the IP address for your department's Web server by using dig. Show the list of the names of DNS servers in the delegation chain in answering your query.
- I followed the DNS servers `a.root-servers.net` → `a.edu-servers.net` → `dns-two.ucdavis.edu`. The IP addresses are listed in the last screenshot under “ANSWER SECTION”.

```

;; WHEN: Sat Mar 06 15:56:25 PST 2021
;; MSG SIZE  rcvd: 838

panda@panda-xps ~/code/python/match (0)
> dig +norecurse @a.root-servers.net cs.ucdavis.edu

; <>> DiG 9.16.11 <>> +norecurse @a.root-servers.net cs.ucdavis.edu
; (2 servers found)
; global options: +cmd
; Got answer:
; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 23218
; flags: qr; QUERY: 1, ANSWER: 0, AUTHORITY: 13, ADDITIONAL: 27

; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1472
; QUESTION SECTION:
;cs.ucdavis.edu.           IN      A

; AUTHORITY SECTION:
edu.          172800  IN      NS      a.edu-servers.net.
edu.          172800  IN      NS      b.edu-servers.net.
edu.          172800  IN      NS      c.edu-servers.net.
edu.          172800  IN      NS      d.edu-servers.net.
edu.          172800  IN      NS      e.edu-servers.net.
edu.          172800  IN      NS      f.edu-servers.net.
edu.          172800  IN      NS      g.edu-servers.net.
edu.          172800  IN      NS      h.edu-servers.net.
edu.          172800  IN      NS      i.edu-servers.net.
edu.          172800  IN      NS      j.edu-servers.net.
edu.          172800  IN      NS      k.edu-servers.net.
edu.          172800  IN      NS      l.edu-servers.net.
edu.          172800  IN      NS      m.edu-servers.net.

; ADDITIONAL SECTION:
a.edu-servers.net. 172800  IN      A      192.5.6.30
b.edu-servers.net. 172800  IN      A      192.33.14.30
c.edu-servers.net. 172800  IN      A      192.26.92.30
d.edu-servers.net. 172800  IN      A      192.31.80.30
e.edu-servers.net. 172800  IN      A      192.12.94.30
f.edu-servers.net. 172800  IN      A      192.35.51.30
g.edu-servers.net. 172800  IN      A      192.42.93.30
h.edu-servers.net. 172800  IN      A      192.54.112.30
i.edu-servers.net. 172800  IN      A      192.43.172.30
j.edu-servers.net. 172800  IN      A      192.48.79.30
k.edu-servers.net. 172800  IN      A      192.52.178.30
l.edu-servers.net. 172800  IN      A      192.41.162.30
m.edu-servers.net. 172800  IN      A      192.55.83.30
a.edu-servers.net. 172800  IN      AAAA   2001:503:a83e::2:30
b.edu-servers.net. 172800  IN      AAAA   2001:503:231d::2:30
c.edu-servers.net. 172800  IN      AAAA   2001:503:83eb::30
d.edu-servers.net. 172800  IN      AAAA   2001:500:856e::30
e.edu-servers.net. 172800  IN      AAAA   2001:502:1ca1::30
f.edu-servers.net. 172800  IN      AAAA   2001:503:d414::30

```

```
panda@panda-xps ~/code/python/match (0)
> dig +norecurse @a.edu-servers.net cs.ucdavis.edu

; <>> DiG 9.16.11 <>> +norecurse @a.edu-servers.net cs.ucdavis.edu
; (2 servers found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 3502
;; flags: qr; QUERY: 1, ANSWER: 0, AUTHORITY: 3, ADDITIONAL: 7

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;cs.ucdavis.edu.           IN      A

;; AUTHORITY SECTION:
ucdavis.edu.          172800  IN      NS      dns-two.ucdavis.edu.
ucdavis.edu.          172800  IN      NS      dns-one.ucdavis.edu.
ucdavis.edu.          172800  IN      NS      dns-three.ucdavis.edu.

;; ADDITIONAL SECTION:
dns-two.ucdavis.edu.  172800  IN      A       128.120.252.10
dns-two.ucdavis.edu.  172800  IN      AAAA   2607:f810:3f0:2::2
dns-one.ucdavis.edu. 172800  IN      A       128.120.252.9
dns-one.ucdavis.edu. 172800  IN      AAAA   2607:f810:3f0:1::1
dns-three.ucdavis.edu. 172800  IN      A       169.237.243.171
dns-three.ucdavis.edu. 172800  IN      AAAA   2607:f810:ce0:10::2

;; Query time: 30 msec
;; SERVER: 192.5.6.30#53(192.5.6.30)
;; WHEN: Sat Mar 06 15:59:58 PST 2021
●;; MSG SIZE rcvd: 243
```

```

panda@panda-xps ~/code/python/match (0)
> dig +norecurse @dns-two.ucdavis.edu cs.ucdavis.edu

; <>> DiG 9.16.11 <>> +norecurse @dns-two.ucdavis.edu cs.ucdavis.edu
; (2 servers found)
; global options: +cmd
; Got answer:
; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 27408
; flags: qr aa; QUERY: 1, ANSWER: 4, AUTHORITY: 3, ADDITIONAL: 7

; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: e2d9f1df253b3d884b6cabfb604417a25848bead3b16ae3f (good)
; QUESTION SECTION:
;cs.ucdavis.edu.          IN      A

;; ANSWER SECTION:
cs.ucdavis.edu.    28800   IN      A      151.101.194.132
cs.ucdavis.edu.    28800   IN      A      151.101.130.132
cs.ucdavis.edu.    28800   IN      A      151.101.66.132
cs.ucdavis.edu.    28800   IN      A      151.101.2.132

;; AUTHORITY SECTION:
cs.ucdavis.edu.    28800   IN      NS     dns-two.ucdavis.edu.
cs.ucdavis.edu.    28800   IN      NS     dns-one.ucdavis.edu.
cs.ucdavis.edu.    28800   IN      NS     dns-three.ucdavis.edu.

;; ADDITIONAL SECTION:
dns-three.ucdavis.edu. 14400   IN      A      169.237.243.171
dns-one.ucdavis.edu.   14400   IN      A      128.120.252.9
dns-two.ucdavis.edu.   14400   IN      A      128.120.252.10
dns-three.ucdavis.edu. 14400   IN      AAAA   2607:f810:ce0:10::2
dns-one.ucdavis.edu.   14400   IN      AAAA   2607:f810:3f0:1::1
dns-two.ucdavis.edu.   14400   IN      AAAA   2607:f810:3f0:2::2

;; Query time: 10 msec
;; SERVER: 128.120.252.10#53(128.120.252.10)
;; WHEN: Sat Mar 06 16:00:34 PST 2021
;; MSG SIZE  rcvd: 335

```

(b) Repeat part (a) for several popular Web sites, such as google.com, yahoo.com, or amazon.com

- google.com
 - I followed the DNS servers `a.root-servers.net` → `a.gtld-servers.net` → `ns2.google.com` to get the IP address 216.58.194.174.

```

panda@panda-xps ~/code/python/match (0)
> dig +norecurse @a.root-servers.net google.com

; <>> DiG 9.16.11 <>> +norecurse @a.root-servers.net google.com
; (2 servers found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 54067
;; flags: qr; QUERY: 1, ANSWER: 0, AUTHORITY: 13, ADDITIONAL: 27

;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 1472
;; QUESTION SECTION:
;google.com.           IN      A

;; AUTHORITY SECTION:
com.          172800  IN      NS      a.gtld-servers.net.
com.          172800  IN      NS      b.gtld-servers.net.
com.          172800  IN      NS      c.gtld-servers.net.
com.          172800  IN      NS      d.gtld-servers.net.
com.          172800  IN      NS      e.gtld-servers.net.
com.          172800  IN      NS      f.gtld-servers.net.
com.          172800  IN      NS      g.gtld-servers.net.
com.          172800  IN      NS      h.gtld-servers.net.
com.          172800  IN      NS      i.gtld-servers.net.
com.          172800  IN      NS      j.gtld-servers.net.
com.          172800  IN      NS      k.gtld-servers.net.
com.          172800  IN      NS      l.gtld-servers.net.
com.          172800  IN      NS      m.gtld-servers.net.

;; ADDITIONAL SECTION:
a.gtld-servers.net. 172800  IN      A      192.5.6.30
b.gtld-servers.net. 172800  IN      A      192.33.14.30
c.gtld-servers.net. 172800  IN      A      192.26.92.30
d.gtld-servers.net. 172800  IN      A      192.31.80.30
e.gtld-servers.net. 172800  IN      A      192.12.94.30
f.gtld-servers.net. 172800  IN      A      192.35.51.30
g.gtld-servers.net. 172800  IN      A      192.42.93.30
h.gtld-servers.net. 172800  IN      A      192.54.112.30
i.gtld-servers.net. 172800  IN      A      192.43.172.30
j.gtld-servers.net. 172800  IN      A      192.48.79.30
k.gtld-servers.net. 172800  IN      A      192.52.178.30
l.gtld-servers.net. 172800  IN      A      192.41.162.30
m.gtld-servers.net. 172800  IN      A      192.55.83.30
a.gtld-servers.net. 172800  IN      AAAA   2001:503:a83e::2:30
b.gtld-servers.net. 172800  IN      AAAA   2001:503:231d::2:30
c.gtld-servers.net. 172800  IN      AAAA   2001:503:83eb::30
d.gtld-servers.net. 172800  IN      AAAA   2001:500:856e::30
e.gtld-servers.net. 172800  IN      AAAA   2001:502:1ca1::30
f.gtld-servers.net. 172800  IN      AAAA   2001:503:d414::30

```

```

panda@panda-xps ~/code/python/match (0)
> dig +norecurse @a.gtld-servers.net google.com

; <>> DiG 9.16.11 <>> +norecurse @a.gtld-servers.net google.com
; (2 servers found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 59830
;; flags: qr; QUERY: 1, ANSWER: 0, AUTHORITY: 4, ADDITIONAL: 9

;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;google.com.           IN      A

;; AUTHORITY SECTION:
google.com.          172800  IN      NS      ns2.google.com.
google.com.          172800  IN      NS      ns1.google.com.
google.com.          172800  IN      NS      ns3.google.com.
google.com.          172800  IN      NS      ns4.google.com.

;; ADDITIONAL SECTION:
ns2.google.com.      172800  IN      AAAA    2001:4860:4802:34::a
ns2.google.com.      172800  IN      A       216.239.34.10
ns1.google.com.      172800  IN      AAAA    2001:4860:4802:32::a
ns1.google.com.      172800  IN      A       216.239.32.10
ns3.google.com.      172800  IN      AAAA    2001:4860:4802:36::a
ns3.google.com.      172800  IN      A       216.239.36.10
ns4.google.com.      172800  IN      AAAA    2001:4860:4802:38::a
ns4.google.com.      172800  IN      A       216.239.38.10

;; Query time: 30 msec
;; SERVER: 192.5.6.30#53(192.5.6.30)
;; WHEN: Sat Mar 06 16:05:34 PST 2021
;; MSG SIZE rcvd: 287

```

```

panda@panda-xps ~/code/python/match (0)
> dig +norecurse @ns2.google.com google.com

; <>> DiG 9.16.11 <>> +norecurse @ns2.google.com google.com
; (2 servers found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 34927
;; flags: qr aa; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;google.com.           IN      A

;; ANSWER SECTION:
google.com.          300     IN      A       216.58.194.174

;; Query time: 30 msec
;; SERVER: 216.239.34.10#53(216.239.34.10)
;; WHEN: Sat Mar 06 16:06:05 PST 2021
;; MSG SIZE rcvd: 55

```

- yahoo.com
 - I followed the DNS servers `a.root-servers.net` → `a.gtld-servers.net` → `ns1.yahoo.com`.
The IP addresses are listed in the last screenshot under “ANSWER SECTION”.

```

panda@panda-xps ~/code/python/match (0)
> dig +norecurse @a.root-servers.net yahoo.com

; <>> DiG 9.16.11 <>> +norecurse @a.root-servers.net yahoo.com
; (2 servers found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 55548
;; flags: qr; QUERY: 1, ANSWER: 0, AUTHORITY: 13, ADDITIONAL: 27

;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 1472
;; QUESTION SECTION:
;yahoo.com.           IN      A

;; AUTHORITY SECTION:
com.          172800  IN      NS      a.gtld-servers.net.
com.          172800  IN      NS      b.gtld-servers.net.
com.          172800  IN      NS      c.gtld-servers.net.
com.          172800  IN      NS      d.gtld-servers.net.
com.          172800  IN      NS      e.gtld-servers.net.
com.          172800  IN      NS      f.gtld-servers.net.
com.          172800  IN      NS      g.gtld-servers.net.
com.          172800  IN      NS      h.gtld-servers.net.
com.          172800  IN      NS      i.gtld-servers.net.
com.          172800  IN      NS      j.gtld-servers.net.
com.          172800  IN      NS      k.gtld-servers.net.
com.          172800  IN      NS      l.gtld-servers.net.
com.          172800  IN      NS      m.gtld-servers.net.

;; ADDITIONAL SECTION:
a.gtld-servers.net. 172800  IN      A      192.5.6.30
b.gtld-servers.net. 172800  IN      A      192.33.14.30
c.gtld-servers.net. 172800  IN      A      192.26.92.30
d.gtld-servers.net. 172800  IN      A      192.31.80.30
e.gtld-servers.net. 172800  IN      A      192.12.94.30
f.gtld-servers.net. 172800  IN      A      192.35.51.30
g.gtld-servers.net. 172800  IN      A      192.42.93.30
h.gtld-servers.net. 172800  IN      A      192.54.112.30
i.gtld-servers.net. 172800  IN      A      192.43.172.30
j.gtld-servers.net. 172800  IN      A      192.48.79.30
k.gtld-servers.net. 172800  IN      A      192.52.178.30
l.gtld-servers.net. 172800  IN      A      192.41.162.30
m.gtld-servers.net. 172800  IN      A      192.55.83.30
- a.gtld-servers.net. 172800  IN      AAAA   2001:503:a83e::2:30

```

```
panda@panda-xps ~/code/python/match (0)
> dig +norecurse @a.gtld-servers.net yahoo.com

; <>> DiG 9.16.11 <>> +norecurse @a.gtld-servers.net yahoo.com
; (2 servers found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 47593
;; flags: qr; QUERY: 1, ANSWER: 0, AUTHORITY: 5, ADDITIONAL: 10

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;yahoo.com.           IN      A

;; AUTHORITY SECTION:
yahoo.com.        172800  IN      NS      ns1.yahoo.com.
yahoo.com.        172800  IN      NS      ns5.yahoo.com.
yahoo.com.        172800  IN      NS      ns2.yahoo.com.
yahoo.com.        172800  IN      NS      ns3.yahoo.com.
yahoo.com.        172800  IN      NS      ns4.yahoo.com.

;; ADDITIONAL SECTION:
ns1.yahoo.com.     172800  IN      AAAA    2001:4998:130::1001
ns1.yahoo.com.     172800  IN      A       68.180.131.16
ns5.yahoo.com.     172800  IN      A       202.165.97.53
ns5.yahoo.com.     172800  IN      AAAA    2406:2000:ff60::53
ns2.yahoo.com.     172800  IN      AAAA    2001:4998:140::1002
ns2.yahoo.com.     172800  IN      A       68.142.255.16
ns3.yahoo.com.     172800  IN      AAAA    2406:8600:f03f:1f8::1003
ns3.yahoo.com.     172800  IN      A       27.123.42.42
ns4.yahoo.com.     172800  IN      A       98.138.11.157

;; Query time: 29 msec
;; SERVER: 192.5.6.30#53(192.5.6.30)
;; WHEN: Sat Mar 06 16:10:41 PST 2021
;; MSG SIZE rcvd: 320
```

```

panda@panda-xps ~/code/python/match (0)
> dig +norecurse @ns1.yahoo.com yahoo.com

; <>> DiG 9.16.11 <>> +norecurse @ns1.yahoo.com yahoo.com
; (2 servers found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 2751
;; flags: qr aa; QUERY: 1, ANSWER: 6, AUTHORITY: 5, ADDITIONAL: 10

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1272
; COOKIE: 0c2d7ff335812872131cedb360441a1c8957825c013356f8 (good)
;; QUESTION SECTION:
;yahoo.com.           IN      A

;; ANSWER SECTION:
yahoo.com.        1800    IN      A      98.137.11.163
yahoo.com.        1800    IN      A      74.6.143.26
yahoo.com.        1800    IN      A      74.6.231.21
yahoo.com.        1800    IN      A      74.6.143.25
yahoo.com.        1800    IN      A      98.137.11.164
yahoo.com.        1800    IN      A      74.6.231.20

;; AUTHORITY SECTION:
yahoo.com.       172800   IN      NS     ns5.yahoo.com.
yahoo.com.       172800   IN      NS     ns1.yahoo.com.
yahoo.com.       172800   IN      NS     ns3.yahoo.com.
yahoo.com.       172800   IN      NS     ns4.yahoo.com.
yahoo.com.       172800   IN      NS     ns2.yahoo.com.

;; ADDITIONAL SECTION:
ns1.yahoo.com.    1209600  IN      A      68.180.131.16
ns2.yahoo.com.    1209600  IN      A      68.142.255.16
ns3.yahoo.com.    1800     IN      A      27.123.42.42
ns4.yahoo.com.    1209600  IN      A      98.138.11.157
ns5.yahoo.com.    86400    IN      A      202.165.97.53
ns1.yahoo.com.    86400    IN      AAAA   2001:4998:130::1001
ns2.yahoo.com.    86400    IN      AAAA   2001:4998:140::1002
ns3.yahoo.com.    1800     IN      AAAA   2406:8600:f03f:1f8::1003
ns5.yahoo.com.    86400    IN      AAAA   2406:2000:ff60::53

;; Query time: 19 msec
;; SERVER: 68.180.131.16#53(68.180.131.16)
;; WHEN: Sat Mar 06 16:11:08 PST 2021
;; MSG SIZE  rcvd: 444

```

- github.com

- I followed the DNS servers `a.root-servers.net` → `e.gtld-servers.net` → `ns-520.awsdns-01.net` to get the IP address 192.30.255.112.

```

panda@panda-xps ~/code/python/match (0)
> dig +norecurse @a.root-servers.net google.com

; <>> DiG 9.16.11 <>> +norecurse @a.root-servers.net google.com
; (2 servers found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 54067
;; flags: qr; QUERY: 1, ANSWER: 0, AUTHORITY: 13, ADDITIONAL: 27

;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 1472
;; QUESTION SECTION:
;google.com.           IN      A

;; AUTHORITY SECTION:
com.          172800  IN      NS      a.gtld-servers.net.
com.          172800  IN      NS      b.gtld-servers.net.
com.          172800  IN      NS      c.gtld-servers.net.
com.          172800  IN      NS      d.gtld-servers.net.
com.          172800  IN      NS      e.gtld-servers.net.
com.          172800  IN      NS      f.gtld-servers.net.
com.          172800  IN      NS      g.gtld-servers.net.
com.          172800  IN      NS      h.gtld-servers.net.
com.          172800  IN      NS      i.gtld-servers.net.
com.          172800  IN      NS      j.gtld-servers.net.
com.          172800  IN      NS      k.gtld-servers.net.
com.          172800  IN      NS      l.gtld-servers.net.
com.          172800  IN      NS      m.gtld-servers.net.

;; ADDITIONAL SECTION:
a.gtld-servers.net. 172800  IN      A      192.5.6.30
b.gtld-servers.net. 172800  IN      A      192.33.14.30
c.gtld-servers.net. 172800  IN      A      192.26.92.30
d.gtld-servers.net. 172800  IN      A      192.31.80.30
e.gtld-servers.net. 172800  IN      A      192.12.94.30
f.gtld-servers.net. 172800  IN      A      192.35.51.30
g.gtld-servers.net. 172800  IN      A      192.42.93.30
h.gtld-servers.net. 172800  IN      A      192.54.112.30
i.gtld-servers.net. 172800  IN      A      192.43.172.30
j.gtld-servers.net. 172800  IN      A      192.48.79.30
k.gtld-servers.net. 172800  IN      A      192.52.178.30
l.gtld-servers.net. 172800  IN      A      192.41.162.30
m.gtld-servers.net. 172800  IN      A      192.55.83.30
a.gtld-servers.net. 172800  IN      AAAA   2001:503:a83e::2:30
b.gtld-servers.net. 172800  IN      AAAA   2001:503:231d::2:30
c.gtld-servers.net. 172800  IN      AAAA   2001:503:83eb::30
d.gtld-servers.net. 172800  IN      AAAA   2001:500:856e::30
e.gtld-servers.net. 172800  IN      AAAA   2001:502:1ca1::30
f.gtld-servers.net. 172800  IN      AAAA   2001:503:d414::30

```

```

panda@panda-xps ~/code/python/match (0)
> dig +norecurse @a.gtld-servers.net google.com

; <>> DiG 9.16.11 <>> +norecurse @a.gtld-servers.net google.com
; (2 servers found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 59830
;; flags: qr; QUERY: 1, ANSWER: 0, AUTHORITY: 4, ADDITIONAL: 9

;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;google.com.           IN      A

;; AUTHORITY SECTION:
google.com.          172800  IN      NS      ns2.google.com.
google.com.          172800  IN      NS      ns1.google.com.
google.com.          172800  IN      NS      ns3.google.com.
google.com.          172800  IN      NS      ns4.google.com.

;; ADDITIONAL SECTION:
ns2.google.com.      172800  IN      AAAA    2001:4860:4802:34::a
ns2.google.com.      172800  IN      A       216.239.34.10
ns1.google.com.      172800  IN      AAAA    2001:4860:4802:32::a
ns1.google.com.      172800  IN      A       216.239.32.10
ns3.google.com.      172800  IN      AAAA    2001:4860:4802:36::a
ns3.google.com.      172800  IN      A       216.239.36.10
ns4.google.com.      172800  IN      AAAA    2001:4860:4802:38::a
ns4.google.com.      172800  IN      A       216.239.38.10

;; Query time: 30 msec
;; SERVER: 192.5.6.30#53(192.5.6.30)
;; WHEN: Sat Mar 06 16:05:34 PST 2021
;; MSG SIZE rcvd: 287

```

```

panda@panda-xps ~/code/python/match (0)
> dig +norecurse @ns2.google.com google.com

; <>> DiG 9.16.11 <>> +norecurse @ns2.google.com google.com
; (2 servers found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 34927
;; flags: qr aa; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;google.com.           IN      A

;; ANSWER SECTION:
google.com.          300     IN      A       216.58.194.174

;; Query time: 30 msec
;; SERVER: 216.239.34.10#53(216.239.34.10)
;; WHEN: Sat Mar 06 16:06:05 PST 2021
;; MSG SIZE rcvd: 55

```

- messenger.com
 - I followed the DNS servers `a.root-servers.net` → `e.gtld-servers.net` → `a.ns.facebook.com` to get the IP address 69.171.250.15.

```

panda@panda-xps ~/code/python/match (0)
> dig +norecurse @a.root-servers.net messenger.com

; <>> DiG 9.16.11 <>> +norecurse @a.root-servers.net messenger.com
; (2 servers found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 24881
;; flags: qr; QUERY: 1, ANSWER: 0, AUTHORITY: 13, ADDITIONAL: 27

;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;messenger.com.           IN      A

;; AUTHORITY SECTION:
com.          172800  IN      NS      e.gtld-servers.net.
com.          172800  IN      NS      b.gtld-servers.net.
com.          172800  IN      NS      j.gtld-servers.net.
com.          172800  IN      NS      m.gtld-servers.net.
com.          172800  IN      NS      i.gtld-servers.net.
com.          172800  IN      NS      f.gtld-servers.net.
com.          172800  IN      NS      a.gtld-servers.net.
com.          172800  IN      NS      g.gtld-servers.net.
com.          172800  IN      NS      h.gtld-servers.net.
com.          172800  IN      NS      l.gtld-servers.net.
com.          172800  IN      NS      k.gtld-servers.net.
com.          172800  IN      NS      c.gtld-servers.net.
com.          172800  IN      NS      d.gtld-servers.net.

;; ADDITIONAL SECTION:
e.gtld-servers.net. 172800  IN      A      192.12.94.30
e.gtld-servers.net. 172800  IN      AAAA   2001:502:1ca1::30
b.gtld-servers.net. 172800  IN      A      192.33.14.30
b.gtld-servers.net. 172800  IN      AAAA   2001:503:231d::2:30
j.gtld-servers.net. 172800  IN      A      192.48.79.30
j.gtld-servers.net. 172800  IN      AAAA   2001:502:7094::30
m.gtld-servers.net. 172800  IN      A      192.55.83.30
m.gtld-servers.net. 172800  IN      AAAA   2001:501:b1f9::30
i.gtld-servers.net. 172800  IN      A      192.43.172.30
i.gtld-servers.net. 172800  IN      AAAA   2001:503:39c1::30
f.gtld-servers.net. 172800  IN      A      192.35.51.30
f.gtld-servers.net. 172800  IN      AAAA   2001:503:d414::30
a.gtld-servers.net. 172800  IN      A      192.5.6.30
a.gtld-servers.net. 172800  IN      AAAA   2001:503:a83e::2:30
g.gtld-servers.net. 172800  IN      A      192.42.93.30
g.gtld-servers.net. 172800  IN      AAAA   2001:503:eea3::30
h.gtld-servers.net. 172800  IN      A      192.54.112.30
h.gtld-servers.net. 172800  IN      AAAA   2001:502:8cc::30
l.gtld-servers.net. 172800  IN      A      192.41.162.30

```

```

panda@panda-xps ~/code/python/matmatch (0)
> dig +norecurse @e.gtld-servers.net messenger.com

; <>> DiG 9.16.11 <>> +norecurse @e.gtld-servers.net messenger.com
; (2 servers found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<- opcode: QUERY, status: NOERROR, id: 4953
;; flags: qr; QUERY: 1, ANSWER: 0, AUTHORITY: 4, ADDITIONAL: 9

;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;messenger.com.           IN      A

;; AUTHORITY SECTION:
messenger.com.      172800  IN      NS      a.ns.facebook.com.
messenger.com.      172800  IN      NS      b.ns.facebook.com.
messenger.com.      172800  IN      NS      c.ns.facebook.com.
messenger.com.      172800  IN      NS      d.ns.facebook.com.

;; ADDITIONAL SECTION:
a.ns.facebook.com.   172800  IN      A      129.134.30.12
a.ns.facebook.com.   172800  IN      AAAA   2a03:2880:f0fc:c:face:b00c:0:35
b.ns.facebook.com.   172800  IN      A      129.134.31.12
b.ns.facebook.com.   172800  IN      AAAA   2a03:2880:f0fd:c:face:b00c:0:35
c.ns.facebook.com.   172800  IN      A      185.89.218.12
c.ns.facebook.com.   172800  IN      AAAA   2a03:2880:f1fc:c:face:b00c:0:35
d.ns.facebook.com.   172800  IN      A      185.89.219.12
d.ns.facebook.com.   172800  IN      AAAA   2a03:2880:f1fd:c:face:b00c:0:35

;; Query time: 29 msec
;; SERVER: 192.12.94.30#53(192.12.94.30)
;; WHEN: Sat Mar 06 16:20:23 PST 2021
;; MSG SIZE rcvd: 294

```

```

panda@panda-xps ~/code/python/matmatch (0)
> dig +norecurse @a.ns.facebook.com messenger.com

; <>> DiG 9.16.11 <>> +norecurse @a.ns.facebook.com messenger.com
; (2 servers found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<- opcode: QUERY, status: NOERROR, id: 23992
;; flags: qr aa; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;messenger.com.           IN      A

;; ANSWER SECTION:
messenger.com.      300     IN      A      69.171.250.15

;; Query time: 19 msec
;; SERVER: 129.134.30.12#53(129.134.30.12)
;; WHEN: Sat Mar 06 16:21:00 PST 2021
;; MSG SIZE rcvd: 71

```

- whitehouse.gov
 - I followed the DNS servers `a.root-servers.net` → `a.gov-servers.net` → `use6.akam.net` to get the IP address 23.219.242.151.

```

panda@panda-xps ~/code/python/match (0)
> dig +norecurse @a.root-servers.net whitehouse.gov

; <>> DiG 9.16.11 <>> +norecurse @a.root-servers.net whitehouse.gov
; (2 servers found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 4037
;; flags: qr; QUERY: 1, ANSWER: 0, AUTHORITY: 4, ADDITIONAL: 9

;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 1472
;; QUESTION SECTION:
;whitehouse.gov.           IN      A

;; AUTHORITY SECTION:
gov.          172800  IN      NS      a.gov-servers.net.
gov.          172800  IN      NS      b.gov-servers.net.
gov.          172800  IN      NS      c.gov-servers.net.
gov.          172800  IN      NS      d.gov-servers.net.

;; ADDITIONAL SECTION:
a.gov-servers.net. 172800  IN      A      69.36.157.30
b.gov-servers.net. 172800  IN      A      209.112.123.30
c.gov-servers.net. 172800  IN      A      69.36.153.30
d.gov-servers.net. 172800  IN      A      81.19.194.30
a.gov-servers.net. 172800  IN      AAAA   2001:500:4431::2:30
b.gov-servers.net. 172800  IN      AAAA   2620:74:27::2:30
c.gov-servers.net. 172800  IN      AAAA   2620:74:28::2:30
d.gov-servers.net. 172800  IN      AAAA   2620:74:29::2:30

;; Query time: 19 msec
;; SERVER: 198.41.0.4#53(198.41.0.4)
;; WHEN: Sat Mar 06 16:23:54 PST 2021
;; MSG SIZE  rcvd: 298

```

```
panda@panda-xps ~/code/python/match (0)
> dig +norecurse @a.gov-servers.net whitehouse.gov

; <>> DiG 9.16.11 <>> +norecurse @a.gov-servers.net whitehouse.gov
; (2 servers found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 55814
;; flags: qr; QUERY: 1, ANSWER: 0, AUTHORITY: 12, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;whitehouse.gov.           IN      A

;; AUTHORITY SECTION:
whitehouse.gov.    86400   IN      NS      use6.akam.net.
whitehouse.gov.    86400   IN      NS      a1-61.akam.net.
whitehouse.gov.    86400   IN      NS      a22-66.akam.net.
whitehouse.gov.    86400   IN      NS      ns1-176.akam.net.
whitehouse.gov.    86400   IN      NS      a12-64.akam.net.
whitehouse.gov.    86400   IN      NS      a5-64.akam.net.
whitehouse.gov.    86400   IN      NS      zc.akam.net.
whitehouse.gov.    86400   IN      NS      usw1.akam.net.
whitehouse.gov.    86400   IN      NS      a3-67.akam.net.
whitehouse.gov.    86400   IN      NS      ns1-145.akam.net.
whitehouse.gov.    86400   IN      NS      a20-65.akam.net.
whitehouse.gov.    86400   IN      NS      asia9.akam.net.

;; Query time: 49 msec
;; SERVER: 69.36.157.30#53(69.36.157.30)
;; WHEN: Sat Mar 06 16:24:29 PST 2021
;; MSG SIZE rcvd: 293
```

```
panda@panda-xps ~/code/python/match (0)
> dig +norecurse @use6.akam.net whitehouse.gov

; <>> DiG 9.16.11 <>> +norecurse @use6.akam.net whitehouse.gov
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 13567
;; flags: qr aa; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;whitehouse.gov.           IN      A

;; ANSWER SECTION:
whitehouse.gov.      20      IN      A      23.219.242.151

;; Query time: 59 msec
;; SERVER: 2.16.40.65#53(2.16.40.65)
;; WHEN: Sat Mar 06 16:25:05 PST 2021
;; MSG SIZE rcvd: 59
```