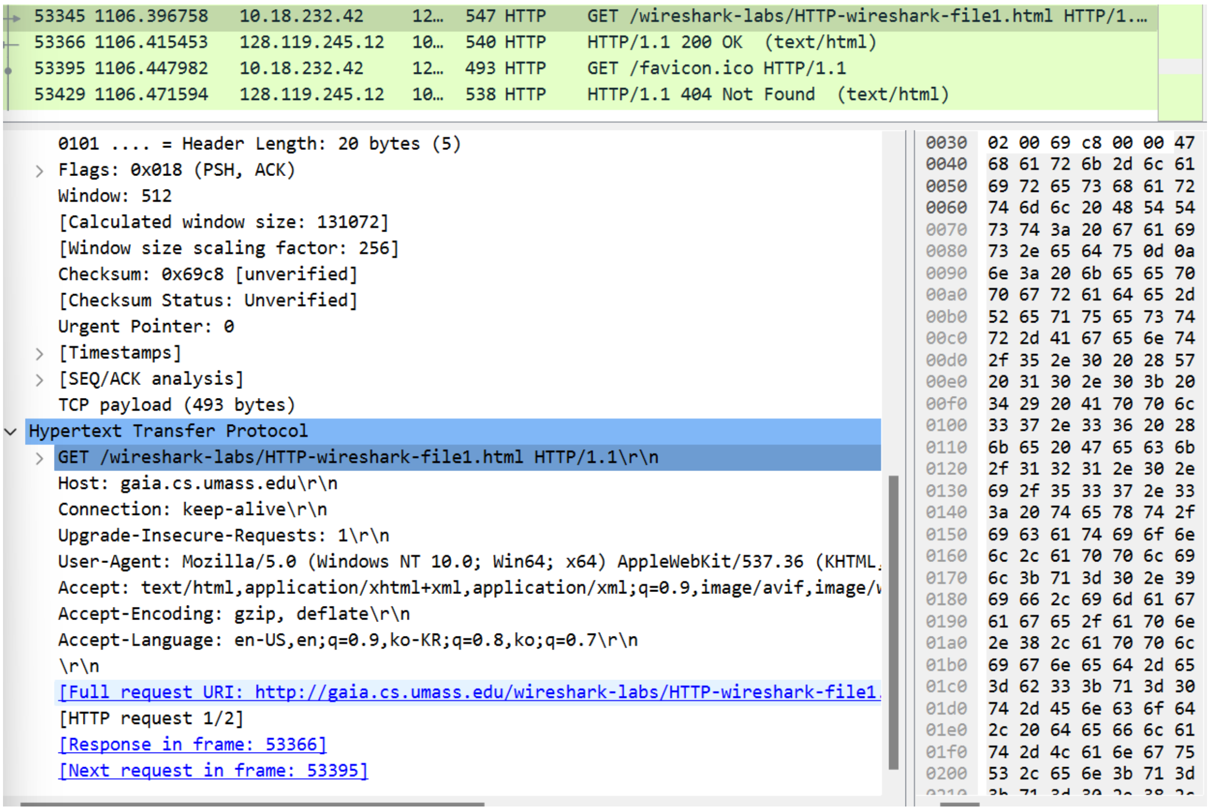
N19265157

Bomin Kim

ECE-UY 3613

LAB 2



```
53345 1106.396758   10.18.232.42     12…  547 HTTP   GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.…
53366 1106.415453   128.119.245.12   10…  540 HTTP   HTTP/1.1 200 OK  (text/html)
53395 1106.447982   10.18.232.42     12…  493 HTTP   GET /favicon.ico HTTP/1.1
53429 1106.471594   128.119.245.12   10…  538 HTTP   HTTP/1.1 404 Not Found  (text/html)
```

```
    0101 .... = Header Length: 20 bytes (5)
  > Flags: 0x018 (PSH, ACK)
    Window: 512
    [Calculated window size: 131072]
    [Window size scaling factor: 256]
    Checksum: 0x69c8 [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
  > [Timestamps]
  > [SEQ/ACK analysis]
    TCP payload (493 bytes)
v Hypertext Transfer Protocol
  > GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n
    Host: gaia.cs.umass.edu\r\n
    Connection: keep-alive\r\n
    Upgrade-Insecure-Requests: 1\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/w
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: en-US,en;q=0.9,ko-KR;q=0.8,ko;q=0.7\r\n
    \r\n
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.
    [HTTP request 1/2]
    [Response in frame: 53366]
    [Next request in frame: 53395]
```

```
0030  02 00 69 c8 00 00 47
0040  68 61 72 6b 2d 6c 61
0050  69 72 65 73 68 61 72
0060  74 6d 6c 20 48 54 54
0070  73 74 3a 20 67 61 69
0080  73 2e 65 64 75 0d 0a
0090  6e 3a 20 6b 65 65 70
00a0  70 67 72 61 64 65 2d
00b0  52 65 71 75 65 73 74
00c0  72 2d 41 67 65 6e 74
00d0  2f 35 2e 30 20 28 57
00e0  20 31 30 2e 30 3b 20
00f0  34 29 20 41 70 70 6c
0100  33 37 2e 33 36 20 28
0110  6b 65 20 47 65 63 6b
0120  2f 31 32 31 2e 30 2e
0130  69 2f 35 33 37 2e 33
0140  3a 20 74 65 78 74 2f
0150  69 63 61 74 69 6f 6e
0160  6c 2c 61 70 70 6c 69
0170  6c 3b 71 3d 30 2e 39
0180  69 66 2c 69 6d 61 67
0190  61 67 65 2f 61 70 6e
01a0  2e 38 2c 61 70 70 6c
01b0  69 67 6e 65 64 2d 65
01c0  3d 62 33 3b 71 3d 30
01d0  74 2d 45 6e 63 6f 64
01e0  2c 20 64 65 66 6c 61
01f0  74 2d 4c 61 6e 67 75
0200  53 2c 65 6e 3b 71 3d
```

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

1.1

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

En-US, ko-KR

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

10.18.232.42

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

200 OK

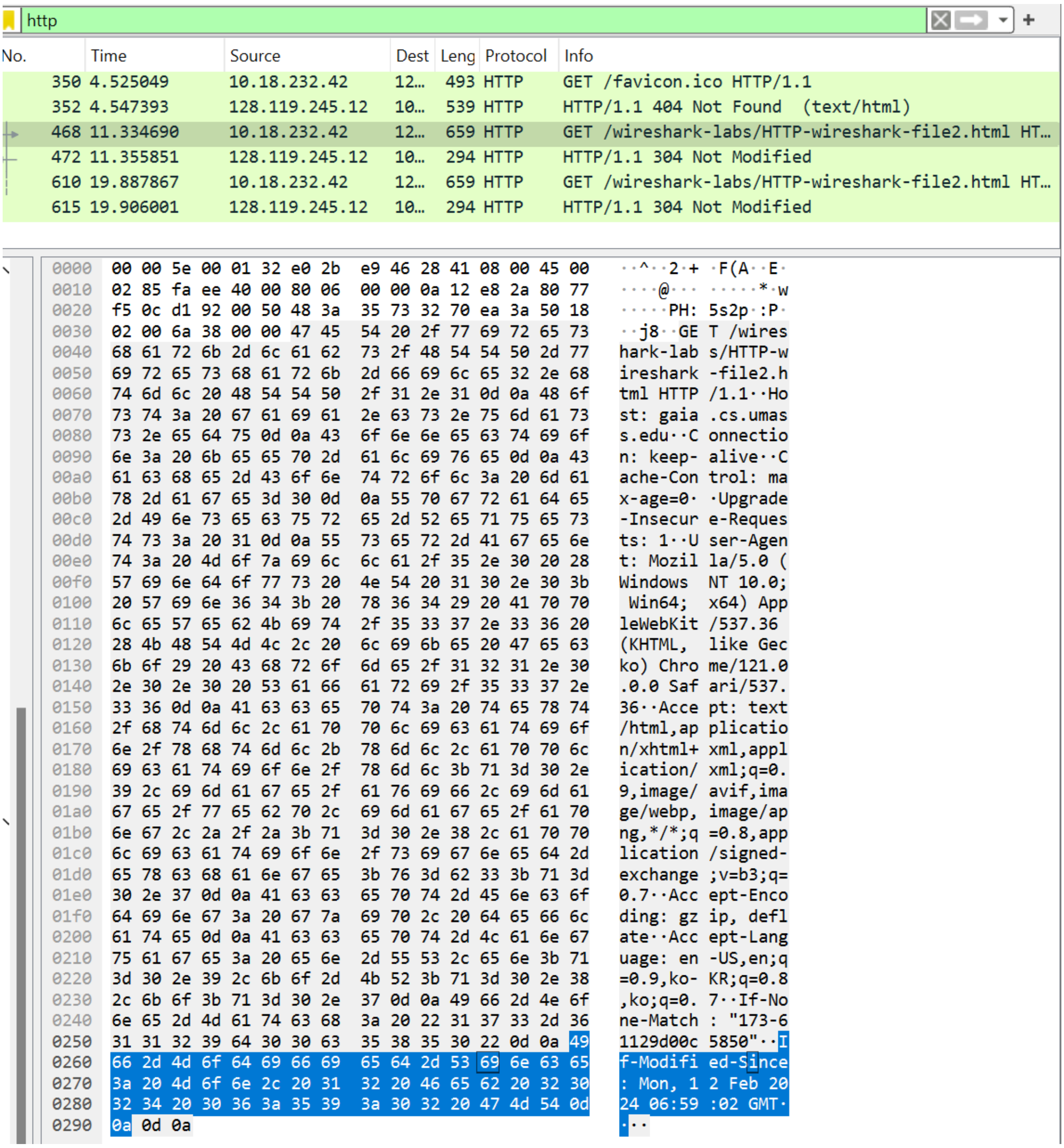
5. When was the HTML file that you are retrieving last modified at the server?

1106.415453

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

540

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.



http

```
No.   Time       Source          Dest Leng Protocol Info
  350 4.525049   10.18.232.42    12…  493 HTTP    GET /favicon.ico HTTP/1.1
  352 4.547393   128.119.245.12  10…  539 HTTP    HTTP/1.1 404 Not Found  (text/html)
  468 11.334690  10.18.232.42    12…  659 HTTP    GET /wireshark-labs/HTTP-wireshark-file2.html HT…
  472 11.355851  128.119.245.12  10…  294 HTTP    HTTP/1.1 304 Not Modified
  610 19.887867  10.18.232.42    12…  659 HTTP    GET /wireshark-labs/HTTP-wireshark-file2.html HT…
  615 19.906001  128.119.245.12  10…  294 HTTP    HTTP/1.1 304 Not Modified
```

```
0000  00 00 5e 00 01 32 e0 2b  e9 46 28 41 08 00 45 00   ··^··2·+ ·F(A··E·
0010  02 85 fa ee 40 00 80 06  00 00 0a 12 e8 2a 80 77   ····@··· ·····*·w
0020  f5 0c d1 92 00 50 48 3a  35 73 32 70 ea 3a 50 18   ·····PH: 5s2p·:P·
0030  02 00 6a 38 00 00 47 45  54 20 2f 77 69 72 65 73   ··j8··GE T /wires
0040  68 61 72 6b 2d 6c 61 62  73 2f 48 54 54 50 2d 77   hark-lab s/HTTP-w
0050  69 72 65 73 68 61 72 6b  2d 66 69 6c 65 32 2e 68   ireshark -file2.h
0060  74 6d 6c 20 48 54 54 50  2f 31 2e 31 0d 0a 48 6f   tml HTTP /1.1··Ho
0070  73 74 3a 20 67 61 69 61  2e 63 73 2e 75 6d 61 73   st: gaia .cs.umas
0080  73 2e 65 64 75 0d 0a 43  6f 6e 6e 65 63 74 69 6f   s.edu··C onnectio
0090  6e 3a 20 6b 65 65 70 2d  61 6c 69 76 65 0d 0a 43   n: keep- alive··C
00a0  61 63 68 65 2d 43 6f 6e  74 72 6f 6c 3a 20 6d 61   ache-Con trol: ma
00b0  78 2d 61 67 65 3d 30 0d  0a 55 70 67 72 61 64 65   x-age=0· ·Upgrade
00c0  2d 49 6e 73 65 63 75 72  65 2d 52 65 71 75 65 73   -Insecur e-Reques
00d0  74 73 3a 20 31 0d 0a 55  73 65 72 2d 41 67 65 6e   ts: 1··U ser-Agen
00e0  74 3a 20 4d 6f 7a 69 6c  6c 61 2f 35 2e 30 20 28   t: Mozil la/5.0 (
00f0  57 69 6e 64 6f 77 73 20  4e 54 20 31 30 2e 30 3b   Windows  NT 10.0;
0100  20 57 69 6e 36 34 3b 20  78 36 34 29 20 41 70 70    Win64;  x64) App
0110  6c 65 57 65 62 4b 69 74  2f 35 33 37 2e 33 36 20   leWebKit /537.36 
0120  28 4b 48 54 4d 4c 2c 20  6c 69 6b 65 20 47 65 63   (KHTML,  like Gec
0130  6b 6f 29 20 43 68 72 6f  6d 65 2f 31 32 31 2e 30   ko) Chro me/121.0
0140  2e 30 2e 30 20 53 61 66  61 72 69 2f 35 33 37 2e   .0.0 Saf ari/537.
0150  33 36 0d 0a 41 63 63 65  70 74 3a 20 74 65 78 74   36··Acce pt: text
0160  2f 68 74 6d 6c 2c 61 70  70 6c 69 63 61 74 69 6f   /html,ap plicatio
0170  6e 2f 78 68 74 6d 6c 2b  78 6d 6c 2c 61 70 70 6c   n/xhtml+ xml,appl
0180  69 63 61 74 69 6f 6e 2f  78 6d 6c 3b 71 3d 30 2e   ication/ xml;q=0.
0190  39 2c 69 6d 61 67 65 2f  61 76 69 66 2c 69 6d 61   9,image/ avif,ima
01a0  67 65 2f 77 65 62 70 2c  69 6d 61 67 65 2f 61 70   ge/webp, image/ap
01b0  6e 67 2c 2a 2f 2a 3b 71  3d 30 2e 38 2c 61 70 70   ng,*/*;q =0.8,app
01c0  6c 69 63 61 74 69 6f 6e  2f 73 69 67 6e 65 64 2d   lication /signed-
01d0  65 78 63 68 61 6e 67 65  3b 76 3d 62 33 3b 71 3d   exchange ;v=b3;q=
01e0  30 2e 37 0d 0a 41 63 63  65 70 74 2d 45 6e 63 6f   0.7··Acc ept-Enco
01f0  64 69 6e 67 3a 20 67 7a  69 70 2c 20 64 65 66 6c   ding: gz ip, defl
0200  61 74 65 0d 0a 41 63 63  65 70 74 2d 4c 61 6e 67   ate··Acc ept-Lang
0210  75 61 67 65 3a 20 65 6e  2d 55 53 2c 65 6e 3b 71   uage: en -US,en;q
0220  3d 30 2e 39 2c 6b 6f 2d  4b 52 3b 71 3d 30 2e 38   =0.9,ko- KR;q=0.8
0230  2c 6b 6f 3b 71 3d 30 2e  37 0d 0a 49 66 2d 4e 6f   ,ko;q=0. 7··If-No
0240  6e 65 2d 4d 61 74 63 68  3a 20 22 31 37 33 2d 36   ne-Match : "173-6
0250  31 31 32 39 64 30 30 63  35 38 35 30 22 0d 0a 49   1129d00c 5850"··I
0260  66 2d 4d 6f 64 69 66 69  65 64 2d 53 69 6e 63 65   f-Modifi ed-Since
0270  3a 20 4d 6f 6e 2c 20 31  32 20 46 65 62 20 32 30   : Mon, 1 2 Feb 20
0280  32 34 20 30 36 3a 35 39  3a 30 32 20 47 4d 54 0d   24 06:59 :02 GMT·
0290  0a 0d 0a                                           ···
```

8. Inspect the contents of the first HTTP GET request from your browser to the server. Do you see an “IF-MODIFIED-SINCE” line in the HTTP GET?

Yes, Mon,12 Feb 2024 06:59:02 GMT

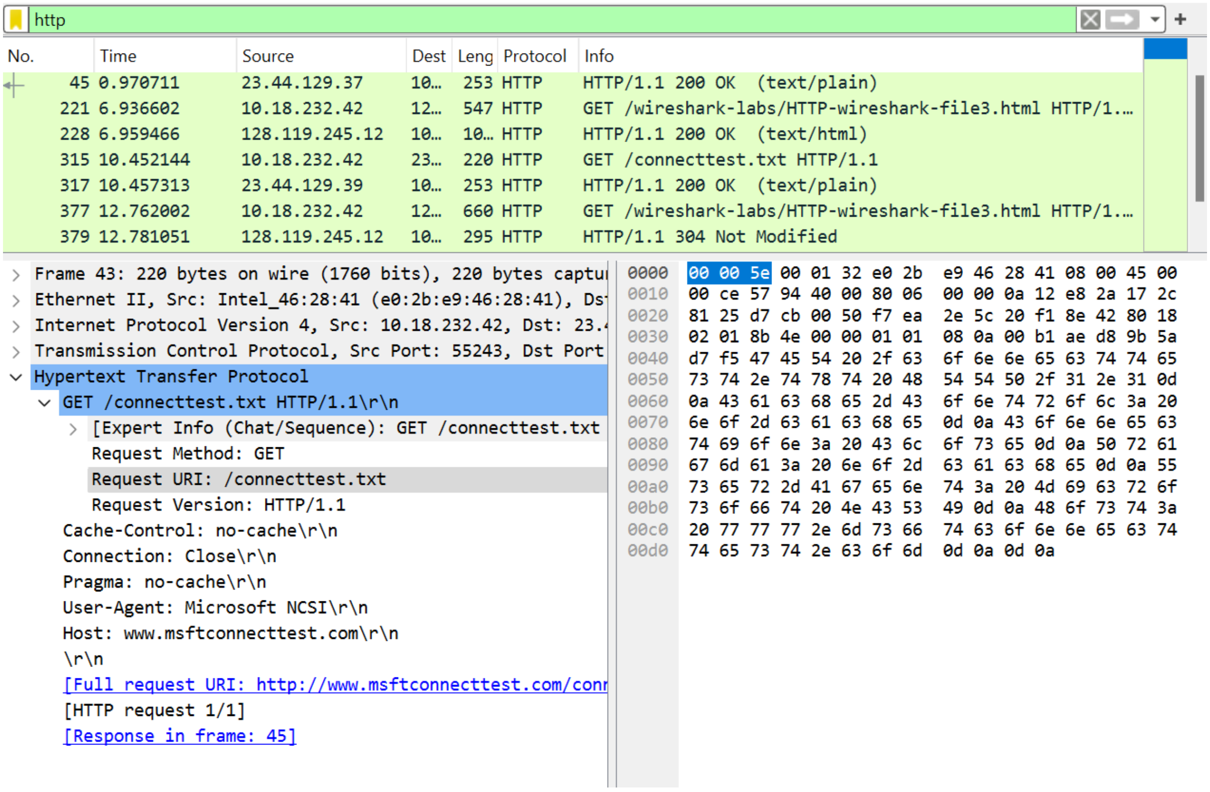
9. Inspect the contents of the server response. Did the server explicitly return the contents of the file? How can you tell?

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?

If-Modified-Since: Mon, 12 Feb 2024 06:59:02 GMT

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

304 not modified, it has not been modified since the last request. The server sent back only the headers, not the actual content of the file.



```
http

No.  Time       Source          Dest Leng Protocol Info
  45 0.970711   23.44.129.37    10…  253 HTTP     HTTP/1.1 200 OK  (text/plain)
 221 6.936602   10.18.232.42    12…  547 HTTP     GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.…
 228 6.959466   128.119.245.12  10…  10… HTTP     HTTP/1.1 200 OK  (text/html)
 315 10.452144  10.18.232.42    23…  220 HTTP     GET /connecttest.txt HTTP/1.1
 317 10.457313  23.44.129.39    10…  253 HTTP     HTTP/1.1 200 OK  (text/plain)
 377 12.762002  10.18.232.42    12…  660 HTTP     GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.…
 379 12.781051  128.119.245.12  10…  295 HTTP     HTTP/1.1 304 Not Modified
```

```
> Frame 43: 220 bytes on wire (1760 bits), 220 bytes captu
> Ethernet II, Src: Intel_46:28:41 (e0:2b:e9:46:28:41), Ds
> Internet Protocol Version 4, Src: 10.18.232.42, Dst: 23.
> Transmission Control Protocol, Src Port: 55243, Dst Port
v Hypertext Transfer Protocol
  v GET /connecttest.txt HTTP/1.1\r\n
    > [Expert Info (Chat/Sequence): GET /connecttest.txt
      Request Method: GET
      Request URI: /connecttest.txt
      Request Version: HTTP/1.1
    Cache-Control: no-cache\r\n
    Connection: Close\r\n
    Pragma: no-cache\r\n
    User-Agent: Microsoft NCSI\r\n
    Host: www.msftconnecttest.com\r\n
    \r\n
    [Full request URI: http://www.msftconnecttest.com/conn
    [HTTP request 1/1]
    [Response in frame: 45]
```

```
0000  00 00 5e 00 01 32 e0 2b  e9 46 28 41 08 00 45 00
0010  00 ce 57 94 40 00 80 06  00 00 0a 12 e8 2a 17 2c
0020  81 25 d7 cb 00 50 f7 ea  2e 5c 20 f1 8e 42 80 18
0030  02 01 8b 4e 00 00 01 01  08 0a 00 b1 ae d8 9b 5a
0040  d7 f5 47 45 54 20 2f 63  6f 6e 6e 65 63 74 74 65
0050  73 74 2e 74 78 74 20 48  54 54 50 2f 31 2e 31 0d
0060  0a 43 61 63 68 65 2d 43  6f 6e 74 72 6f 6c 3a 20
0070  6e 6f 2d 63 61 63 68 65  0d 0a 43 6f 6e 6e 65 63
0080  74 69 6f 6e 3a 20 43 6c  6f 73 65 0d 0a 50 72 61
0090  67 6d 61 3a 20 6e 6f 2d  63 61 63 68 65 0d 0a 55
00a0  73 65 72 2d 41 67 65 6e  74 3a 20 4d 69 63 72 6f
00b0  73 6f 66 74 20 4e 43 53  49 0d 0a 48 6f 73 74 3a
00c0  20 77 77 77 2e 6d 73 66  74 63 6f 6e 6e 65 63 74
00d0  74 65 73 74 2e 63 6f 6d  0d 0a 0d 0a
```

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?

221

13. Which packet number in the trace contains the status code and phrase associated with the response to the HTTP GET request? 14. What is the status code and phrase in the response? 15.

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

228 , 6 segments

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

Host: gaia.cs.umass.edu