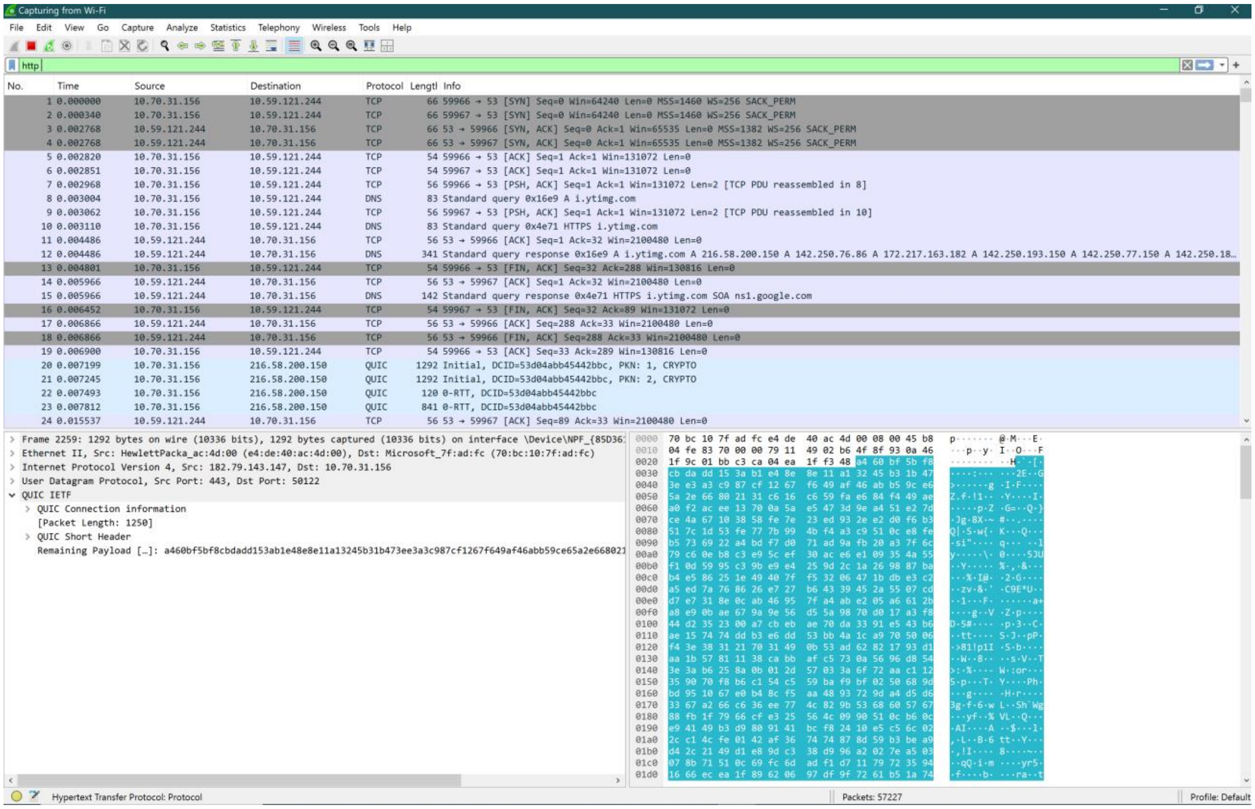
Wireshark Lab: HTTP v7.0

Submitted By: Stuti Garg (SE22UCSE263)

CSE – 4

SECTION I : The Basic HTTP GET/response interaction

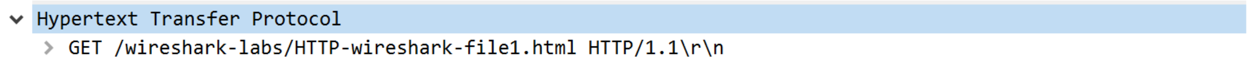

Capturing from Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

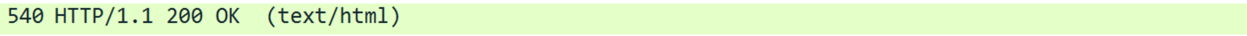
http

```
No.   Time      Source          Destination     Protocol Lengtl Info
    1 0.000000  10.70.31.156    10.59.121.244   TCP        66 59966 → 53 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
    2 0.000340  10.70.31.156    10.59.121.244   TCP        66 59967 → 53 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
    3 0.002768  10.59.121.244   10.70.31.156    TCP        66 53 → 59966 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1382 WS=256 SACK_PERM
    4 0.002768  10.59.121.244   10.70.31.156    TCP        66 53 → 59967 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1382 WS=256 SACK_PERM
    5 0.002820  10.70.31.156    10.59.121.244   TCP        54 59966 → 53 [ACK] Seq=1 Ack=1 Win=131072 Len=0
    6 0.002851  10.70.31.156    10.59.121.244   TCP        54 59967 → 53 [ACK] Seq=1 Ack=1 Win=131072 Len=0
    7 0.002968  10.70.31.156    10.59.121.244   TCP        56 59966 → 53 [PSH, ACK] Seq=1 Ack=1 Win=131072 Len=2 [TCP PDU reassembled in 8]
    8 0.003004  10.70.31.156    10.59.121.244   DNS        83 Standard query 0x16e9 A i.ytimg.com
    9 0.003062  10.70.31.156    10.59.121.244   TCP        56 59967 → 53 [PSH, ACK] Seq=1 Ack=1 Win=131072 Len=2 [TCP PDU reassembled in 10]
   10 0.003110  10.70.31.156    10.59.121.244   DNS        83 Standard query 0x4e71 HTTPS i.ytimg.com
   11 0.004486  10.59.121.244   10.70.31.156    TCP        56 53 → 59966 [ACK] Seq=1 Ack=32 Win=2100480 Len=0
   12 0.004486  10.59.121.244   10.70.31.156    DNS       341 Standard query response 0x16e9 A i.ytimg.com A 216.58.200.150 A 142.250.76.86 A 172.217.163.182 A 142.250.193.150 A 142.250.77.150 A 142.250.18…
   13 0.004801  10.70.31.156    10.59.121.244   TCP        54 59966 → 53 [FIN, ACK] Seq=32 Ack=288 Win=130816 Len=0
   14 0.005966  10.59.121.244   10.70.31.156    TCP        56 53 → 59967 [ACK] Seq=1 Ack=32 Win=2100480 Len=0
   15 0.005966  10.59.121.244   10.70.31.156    DNS       142 Standard query response 0x4e71 HTTPS i.ytimg.com SOA ns1.google.com
   16 0.006452  10.70.31.156    10.59.121.244   TCP        54 59967 → 53 [FIN, ACK] Seq=32 Ack=89 Win=131072 Len=0
   17 0.006866  10.59.121.244   10.70.31.156    TCP        56 53 → 59966 [ACK] Seq=288 Ack=33 Win=2100480 Len=0
   18 0.006866  10.59.121.244   10.70.31.156    TCP        56 53 → 59966 [FIN, ACK] Seq=288 Ack=33 Win=2100480 Len=0
   19 0.006900  10.70.31.156    10.59.121.244   TCP        54 59966 → 53 [ACK] Seq=33 Ack=289 Win=130816 Len=0
   20 0.007199  10.70.31.156    216.58.200.150  QUIC     1292 Initial, DCID=53d04abb45442bbc, PKN: 1, CRYPTO
   21 0.007245  10.70.31.156    216.58.200.150  QUIC     1292 Initial, DCID=53d04abb45442bbc, PKN: 2, CRYPTO
   22 0.007493  10.70.31.156    216.58.200.150  QUIC      120 0-RTT, DCID=53d04abb45442bbc
   23 0.007812  10.70.31.156    216.58.200.150  QUIC      841 0-RTT, DCID=53d04abb45442bbc
   24 0.015537  10.59.121.244   10.70.31.156    TCP        56 53 → 59967 [ACK] Seq=89 Ack=33 Win=2100480 Len=0
```

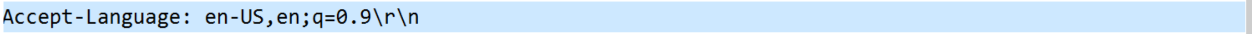
```
> Frame 2259: 1292 bytes on wire (10336 bits), 1292 bytes captured (10336 bits) on interface \Device\NPF_{85D36
> Ethernet II, Src: HewlettPacka_ac:4d:00 (e4:de:40:ac:4d:00), Dst: Microsoft_7f:ad:fc (70:bc:10:7f:ad:fc)
> Internet Protocol Version 4, Src: 182.79.143.147, Dst: 10.70.31.156
> User Datagram Protocol, Src Port: 443, Dst Port: 50122
v QUIC IETF
   > QUIC Connection information
     [Packet Length: 1250]
   > QUIC Short Header
     Remaining Payload […]: a460bf5bf8cbdadd153ab1e48e8e11a13245b31b473ee3a3c987cf1267f649af46abb59ce65a2e668021
```

```
0000  70 bc 10 7f ad fc e4 de  40 ac 4d 00 08 00 45 b8
0010  04 fe 83 70 00 00 79 11  49 02 b6 4f 8f 93 0a 46
0020  1f 9c 01 bb c3 ca 04 ea  1f f3 48 a4 60 bf 5b f8
0030  cb da dd 15 3a b1 e4 8e  8e 11 a1 32 45 b3 1b 47
0040  3e e3 a3 c9 87 cf 12 67  f6 49 af 46 ab b5 9c e6
0050  5a 2e 66 80 21 31 c6 16  c6 59 fa e6 84 f4 49 ae
0060  a0 f2 ac ee 13 70 0a 5a  e5 47 3d 9e a4 51 e2 7d
0070  ce 4a 67 10 38 58 fe 7e  23 ed 93 2e e2 d0 f6 b3
0080  51 7c 1d 53 fe 77 7b 99  4b f4 a3 c9 51 0c e8 fe
0090  b5 73 69 22 a4 bd f7 d0  71 ad 9a fb 20 a3 7f 6c
00a0  79 c6 0e b8 c3 e9 5c ef  30 ac e6 e1 09 35 4a 55
00b0  f1 0d 59 95 c3 9b e9 e4  25 9d 2c 1a 26 98 87 ba
00c0  b4 e5 86 25 1e 49 40 7f  f5 32 06 47 1b db e3 c2
00d0  a5 ed 7a 76 86 26 e7 27  b6 43 39 45 2a 55 07 cd
00e0  d7 e7 31 8e 0c ab 46 95  7f a4 ab e2 05 a6 61 2b
00f0  a8 e9 0b ae 67 9a 9e 56  d5 5a 98 70 d0 17 a3 f8
0100  44 d2 35 23 00 a7 cb eb  ae 70 da 33 91 e5 43 b6
0110  ae 15 74 74 dd b3 e6 dd  53 bb 4a 1c a9 70 50 06
0120  f4 3e 38 31 21 70 31 49  0b 53 ad 62 82 17 93 d1
0130  aa 1b 57 81 11 38 ca bb  af c5 73 0a 56 96 d8 54
0140  3e 3a b6 25 8a 0b 01 2d  57 03 3a 6f 72 aa c1 12
0150  35 90 70 f8 b6 c1 54 c5  59 ba f9 bf 02 50 68 9d
0160  bd 95 10 67 e0 b4 8c f5  aa 48 93 72 9d a4 d5 d6
0170  33 67 a2 66 c6 36 ee 77  4c 82 9b 53 68 60 57 67
0180  88 fb 1f 79 66 cf e3 25  56 4c 09 90 51 0c b6 0c
0190  e9 41 49 b3 d9 80 91 41  bc f8 24 10 e5 c5 6c 02
01a0  2c c1 4c fe 01 42 af 36  74 74 87 8d 59 b3 be a9
01b0  d4 2c 21 49 d1 e8 9d c3  38 d9 96 a2 02 7e a5 03
01c0  07 8b 71 51 0c 69 fc 6d  ad f1 d7 11 79 72 35 94
01d0  16 66 ec ea 1f 89 62 06  97 df 9f 72 61 b5 1a 74
```

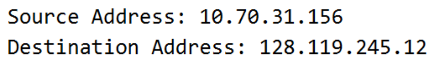
1. Is your browser running HTTP version 1.0 or 1.1? What version of HTTP is the server running?
   - Browser's running on HTTP version: HTTP/1.1
   - 

     ```
     v Hypertext Transfer Protocol
        > GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n
     ```
   - Server's HTTP version: HTTP/1.1 (It is found in the HTTP response packet).
   - 

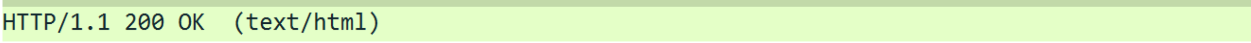
     ```
     540 HTTP/1.1 200 OK  (text/html)
     ```
   - The HTTP version is found in the GET request packet under the HTTP section.

2. What languages (if any) does your browser indicate that it can accept the server?
   - Accepted language by my server: en-US,en;q=0.9
   - 

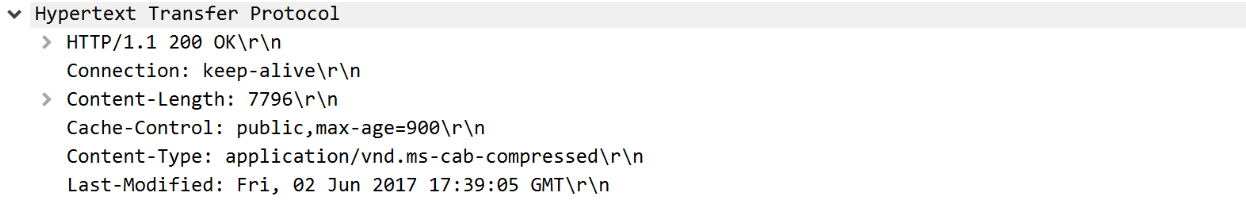
     ```
     Accept-Language: en-US,en;q=0.9\r\n
     ```
   - The accepted languages are listed in the Accept-Language header of the GET request packet under the HTTP section.

3. What is the IP address of your computer? Of the gaia.cs.umass.edu server?
   - IP address: 10.70.31.156
   - Server Address: 128.119.245.12
   - 

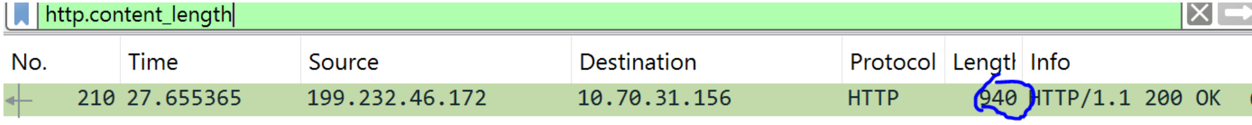
     ```
     Source Address: 10.70.31.156
     Destination Address: 128.119.245.12
     ```
   - The Source IP in the HTTP request packet represents the computer’s IP address, while the Destination IP in the HTTP response packet represents the server's IP address. Both can be found under the Internet Protocol (IP) section in the Packet Details window.

4. What is the status code returned from the server to your browser?
   - Status Code: 200 (The request was successful.)
   - 

     ```
     HTTP/1.1 200 OK  (text/html)
     ```
   - The status code is found in the HTTP response packet under the HTTP section, (200 OK).

5. When was the HTML file that you are retrieving last modified at the server?
   - It was last modified at the server: Fri, 2 Jun 2017 17:39:05 GMT\r\n
   - 

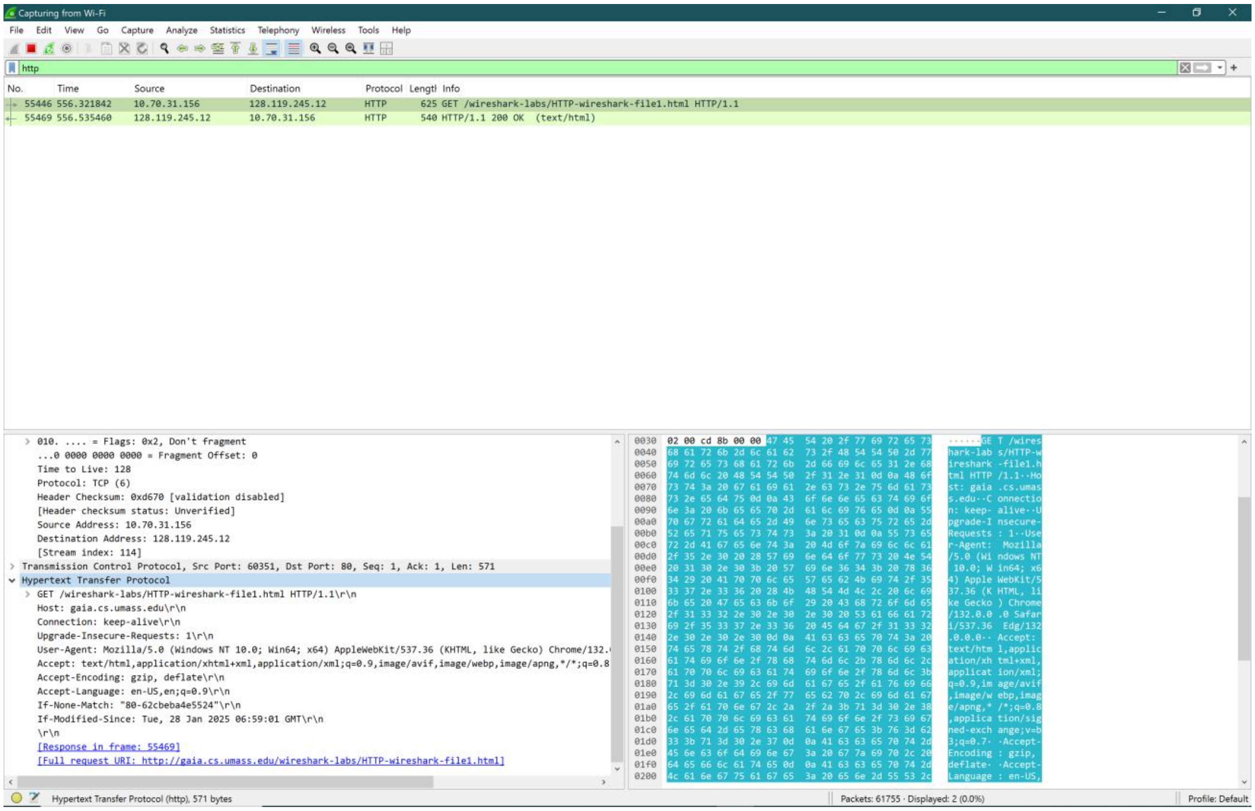
     ```
     ⌄ Hypertext Transfer Protocol
       > HTTP/1.1 200 OK\r\n
         Connection: keep-alive\r\n
       > Content-Length: 7796\r\n
         Cache-Control: public,max-age=900\r\n
         Content-Type: application/vnd.ms-cab-compressed\r\n
         Last-Modified: Fri, 02 Jun 2017 17:39:05 GMT\r\n
     ```
   - The last modified date is in the Last-Modified header of the HTTP response packet.

6. How many bytes of content are being returned to your browser?
   - Content Length: 940 bytes
   - 

     http.content_length

No.	Time	Source	Destination	Protocol	Lengtl	Info
210	27.655365	199.232.46.172	10.70.31.156	HTTP	940	HTTP/1.1 200 OK
   - Found by Wireshark filter: http.content_length

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.
   - Yes, by inspecting the raw data in the packet content window, I see some headers within the data that are not displayed in the packet-listing window.
   - Headers like Set-Cookie, Content Encoding and X-Cache are not available in the packet-listing window.

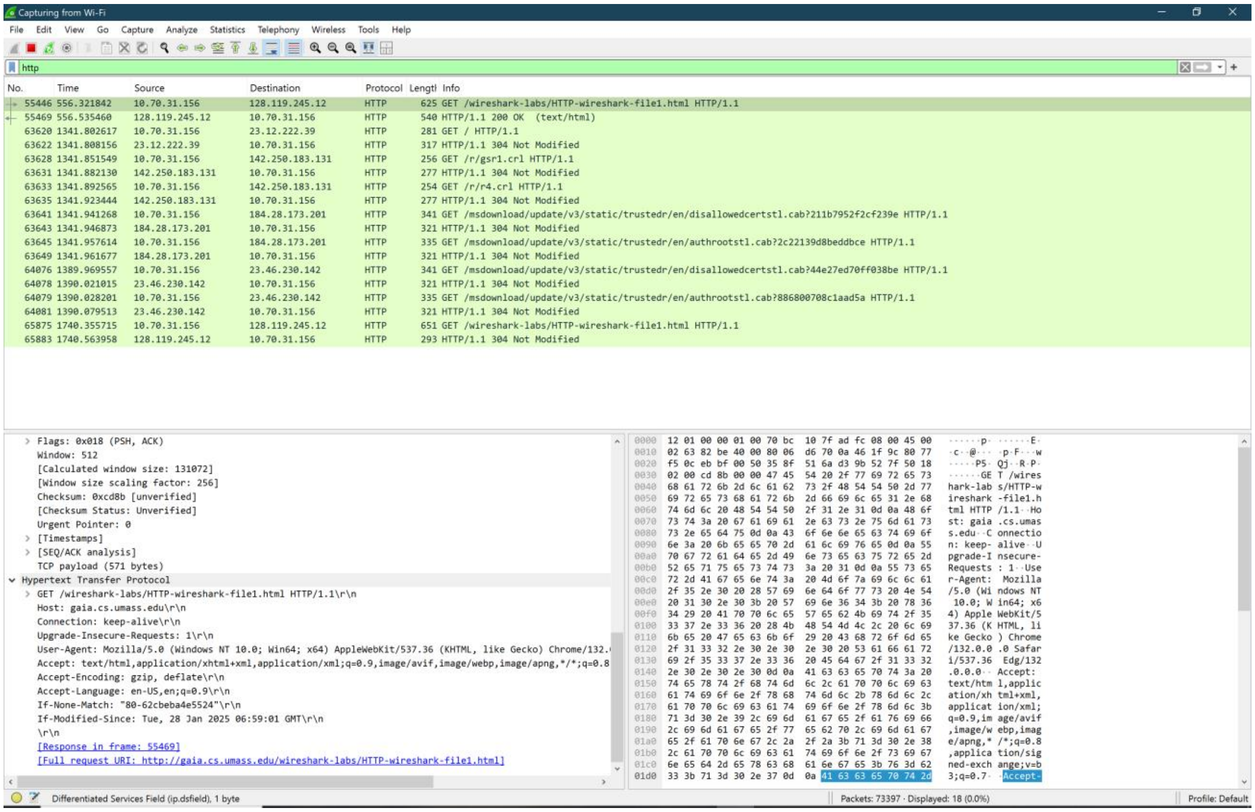


```
No.     Time        Source          Destination      Protocol Lengtl Info
  55446 556.321842  10.70.31.156    128.119.245.12   HTTP       625 GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
  55469 556.535460  128.119.245.12  10.70.31.156     HTTP       540 HTTP/1.1 200 OK  (text/html)
```

```
  > 010. .... = Flags: 0x2, Don't fragment
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 128
    Protocol: TCP (6)
    Header Checksum: 0xd670 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 10.70.31.156
    Destination Address: 128.119.245.12
    [Stream index: 114]
> Transmission Control Protocol, Src Port: 60351, Dst Port: 80, Seq: 1, Ack: 1, Len: 571
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, like Gecko) Chrome/132.
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: en-US,en;q=0.9\r\n
    If-None-Match: "80-62cbeba4e5524"\r\n
    If-Modified-Since: Tue, 28 Jan 2025 06:59:01 GMT\r\n
    \r\n
    [Response in frame: 55469]
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html]
```

```
0030  02 00 cd 8b 00 00 47 45  54 20 2f 77 69 72 65 73   ······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 31 2e 68   ireshark -file1.h
0060  74 6d 6c 20 48 54 54 50  2f 31 2e 31 0d 0a 48 6f   tml HTTP /1.1··Ho
0070  73 74 3a 20 67 61 69 61  2e 63 73 2e 75 6d 61 73   st: gaia .cs.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 55   n: keep- alive··U
00a0  70 67 72 61 64 65 2d 49  6e 73 65 63 75 72 65 2d   pgrade-I nsecure-
00b0  52 65 71 75 65 73 74 73  3a 20 31 0d 0a 55 73 65   Requests : 1··Use
00c0  72 2d 41 67 65 6e 74 3a  20 4d 6f 7a 69 6c 6c 61   r-Agent:  Mozilla
00d0  2f 35 2e 30 20 28 57 69  6e 64 6f 77 73 20 4e 54   /5.0 (Wi ndows NT
00e0  20 31 30 2e 30 3b 20 57  69 6e 36 34 3b 20 78 36    10.0; W in64; x6
00f0  34 29 20 41 70 70 6c 65  57 65 62 4b 69 74 2f 35   4) Apple WebKit/5
0100  33 37 2e 33 36 20 28 4b  48 54 4d 4c 2c 20 6c 69   37.36 (K HTML, li
0110  6b 65 20 47 65 63 6b 6f  29 20 43 68 72 6f 6d 65   ke Gecko ) Chrome
0120  2f 31 33 32 2e 30 2e 30  2e 30 20 53 61 66 61 72   /132.0.0 .0 Safar
0130  69 2f 35 33 37 2e 33 36  20 45 64 67 2f 31 33 32   i/537.36  Edg/132
0140  2e 30 2e 30 2e 30 0d 0a  41 63 63 65 70 74 3a 20   .0.0.0·· Accept: 
0150  74 65 78 74 2f 68 74 6d  6c 2c 61 70 70 6c 69 63   text/htm l,applic
0160  61 74 69 6f 6e 2f 78 68  74 6d 6c 2b 78 6d 6c 2c   ation/xh tml+xml,
0170  61 70 70 6c 69 63 61 74  69 6f 6e 2f 78 6d 6c 3b   applicat ion/xml;
0180  71 3d 30 2e 39 2c 69 6d  61 67 65 2f 61 76 69 66   q=0.9,im age/avif
0190  2c 69 6d 61 67 65 2f 77  65 62 70 2c 69 6d 61 67   ,image/w ebp,imag
01a0  65 2f 61 70 6e 67 2c 2a  2f 2a 3b 71 3d 30 2e 38   e/apng,* /*;q=0.8
01b0  2c 61 70 70 6c 69 63 61  74 69 6f 6e 2f 73 69 67   ,applica tion/sig
01c0  6e 65 64 2d 65 78 63 68  61 6e 67 65 3b 76 3d 62   ned-exch ange;v=b
01d0  33 3b 71 3d 30 2e 37 0d  0a 41 63 63 65 70 74 2d   3;q=0.7· ·Accept-
01e0  45 6e 63 6f 64 69 6e 67  3a 20 67 7a 69 70 2c 20   Encoding : gzip, 
01f0  64 65 66 6c 61 74 65 0d  0a 41 63 63 65 70 74 2d   deflate· ·Accept-
0200  4c 61 6e 67 75 61 67 65  3a 20 65 6e 2d 55 53 2c   Language : en-US,
```

Hypertext Transfer Protocol (http), 571 bytes | Packets: 61755 · Displayed: 2 (0.0%) | Profile: Default



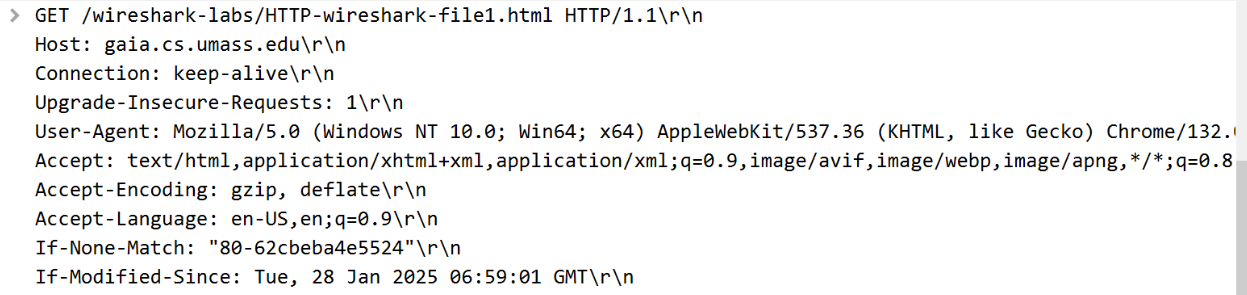
```
No.     Time         Source           Destination      Protocol Lengtl Info
  55446 556.321842   10.70.31.156     128.119.245.12   HTTP       625 GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
  55469 556.535460   128.119.245.12   10.70.31.156     HTTP       540 HTTP/1.1 200 OK  (text/html)
  63620 1341.802617  10.70.31.156     23.12.222.39     HTTP       281 GET / HTTP/1.1
  63622 1341.808156  23.12.222.39     10.70.31.156     HTTP       317 HTTP/1.1 304 Not Modified
  63628 1341.851549  10.70.31.156     142.250.183.131  HTTP       256 GET /r/gsr1.crl HTTP/1.1
  63631 1341.882130  142.250.183.131  10.70.31.156     HTTP       277 HTTP/1.1 304 Not Modified
  63633 1341.892565  10.70.31.156     142.250.183.131  HTTP       254 GET /r/r4.crl HTTP/1.1
  63635 1341.923444  142.250.183.131  10.70.31.156     HTTP       277 HTTP/1.1 304 Not Modified
  63641 1341.941268  10.70.31.156     184.28.173.201   HTTP       341 GET /msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?211b7952f2cf239e HTTP/1.1
  63643 1341.946873  184.28.173.201   10.70.31.156     HTTP       321 HTTP/1.1 304 Not Modified
  63645 1341.957614  10.70.31.156     184.28.173.201   HTTP       335 GET /msdownload/update/v3/static/trustedr/en/authrootstl.cab?2c22139d8beddbce HTTP/1.1
  63649 1341.961677  184.28.173.201   10.70.31.156     HTTP       321 HTTP/1.1 304 Not Modified
  64076 1389.969557  10.70.31.156     23.46.230.142    HTTP       341 GET /msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?44e27ed70ff038be HTTP/1.1
  64078 1390.021015  23.46.230.142    10.70.31.156     HTTP       321 HTTP/1.1 304 Not Modified
  64079 1390.028201  10.70.31.156     23.46.230.142    HTTP       335 GET /msdownload/update/v3/static/trustedr/en/authrootstl.cab?886800708c1aad5a HTTP/1.1
  64081 1390.079513  23.46.230.142    10.70.31.156     HTTP       321 HTTP/1.1 304 Not Modified
  65875 1740.355715  10.70.31.156     128.119.245.12   HTTP       651 GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
  65883 1740.563958  128.119.245.12   10.70.31.156     HTTP       293 HTTP/1.1 304 Not Modified
```

```
  > Flags: 0x018 (PSH, ACK)
    Window: 512
    [Calculated window size: 131072]
    [Window size scaling factor: 256]
    Checksum: 0xcd8b [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
  > [Timestamps]
  > [SEQ/ACK analysis]
    TCP payload (571 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, like Gecko) Chrome/132.
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: en-US,en;q=0.9\r\n
    If-None-Match: "80-62cbeba4e5524"\r\n
    If-Modified-Since: Tue, 28 Jan 2025 06:59:01 GMT\r\n
    \r\n
    [Response in frame: 55469]
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html]
```

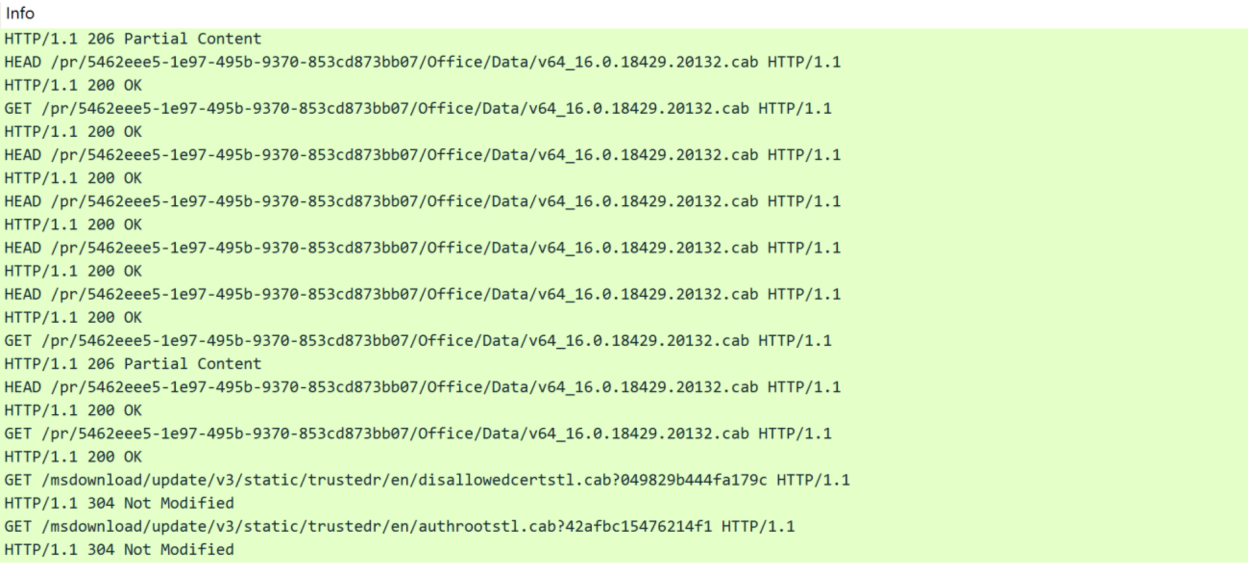
```
0000  12 01 00 00 01 00 70 bc  10 7f ad fc 08 00 45 00   ······p· ······E·
0010  02 63 82 be 40 00 80 06  d6 70 0a 46 1f 9c 80 77   ·c··@··· ·p·F···w
0020  f5 0c eb bf 00 50 35 8f  51 6a d3 9b 52 7f 50 18   ·····P5· Qj··R·P·
0030  02 00 cd 8b 00 00 47 45  54 20 2f 77 69 72 65 73   ······GE T /wires
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 31 2e 68   ireshark -file1.h
0060  74 6d 6c 20 48 54 54 50  2f 31 2e 31 0d 0a 48 6f   tml HTTP /1.1··Ho
0070  73 74 3a 20 67 61 69 61  2e 63 73 2e 75 6d 61 73   st: gaia .cs.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 55   n: keep- alive··U
00a0  70 67 72 61 64 65 2d 49  6e 73 65 63 75 72 65 2d   pgrade-I nsecure-
00b0  52 65 71 75 65 73 74 73  3a 20 31 0d 0a 55 73 65   Requests : 1··Use
00c0  72 2d 41 67 65 6e 74 3a  20 4d 6f 7a 69 6c 6c 61   r-Agent:  Mozilla
00d0  2f 35 2e 30 20 28 57 69  6e 64 6f 77 73 20 4e 54   /5.0 (Wi ndows NT
00e0  20 31 30 2e 30 3b 20 57  69 6e 36 34 3b 20 78 36    10.0; W in64; x6
00f0  34 29 20 41 70 70 6c 65  57 65 62 4b 69 74 2f 35   4) Apple WebKit/5
0100  33 37 2e 33 36 20 28 4b  48 54 4d 4c 2c 20 6c 69   37.36 (K HTML, li
0110  6b 65 20 47 65 63 6b 6f  29 20 43 68 72 6f 6d 65   ke Gecko ) Chrome
0120  2f 31 33 32 2e 30 2e 30  2e 30 20 53 61 66 61 72   /132.0.0 .0 Safar
0130  69 2f 35 33 37 2e 33 36  20 45 64 67 2f 31 33 32   i/537.36  Edg/132
0140  2e 30 2e 30 2e 30 0d 0a  41 63 63 65 70 74 3a 20   .0.0.0·· Accept: 
0150  74 65 78 74 2f 68 74 6d  6c 2c 61 70 70 6c 69 63   text/htm l,applic
0160  61 74 69 6f 6e 2f 78 68  74 6d 6c 2b 78 6d 6c 2c   ation/xh tml+xml,
0170  61 70 70 6c 69 63 61 74  69 6f 6e 2f 78 6d 6c 3b   applicat ion/xml;
0180  71 3d 30 2e 39 2c 69 6d  61 67 65 2f 61 76 69 66   q=0.9,im age/avif
0190  2c 69 6d 61 67 65 2f 77  65 62 70 2c 69 6d 61 67   ,image/w ebp,imag
01a0  65 2f 61 70 6e 67 2c 2a  2f 2a 3b 71 3d 30 2e 38   e/apng,* /*;q=0.8
01b0  2c 61 70 70 6c 69 63 61  74 69 6f 6e 2f 73 69 67   ,applica tion/sig
01c0  6e 65 64 2d 65 78 63 68  61 6e 67 65 3b 76 3d 62   ned-exch ange;v=b
01d0  33 3b 71 3d 30 2e 37 0d  0a 41 63 63 65 70 74 2d   3;q=0.7· ·Accept-
```

Differentiated Services Field (ip.dsfield), 1 byte | Packets: 73397 · Displayed: 18 (0.0%) | Profile: Default

SECTION II : The Basic HTTP GET/response interaction

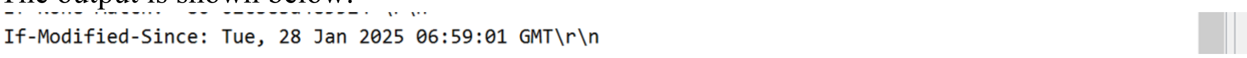
8. Inspect the contents of the first HTTP GET request from your browser to the server. Do you see an “IF-MODIFIED-SINCE” line in the HTTP GET?
   - Yes, there exists an “IF-MODIFIED-SINCE”.
   - 

     ```
     > GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n
       Host: gaia.cs.umass.edu\r\n
       Connection: keep-alive\r\n
       Upgrade-Insecure-Requests: 1\r\n
       User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/132.
       Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8
       Accept-Encoding: gzip, deflate\r\n
       Accept-Language: en-US,en;q=0.9\r\n
       If-None-Match: "80-62cbeba4e5524"\r\n
       If-Modified-Since: Tue, 28 Jan 2025 06:59:01 GMT\r\n
     ```
   - This is viewed under the HTTP GET response.

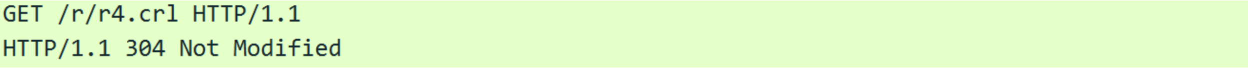
9. Inspect the contents of the server response. Did the server explicitly return the contents of the file? How can you tell?
   - Yes, the server explicitly returns the contents of the files.
   - If the server sends the file, the content of the file is viewed in the Data section of the response. If the status code is 304, it means the server did not send the file, and it was not modified.
   - 

     ```
     Info
     HTTP/1.1 206 Partial Content
     HEAD /pr/5462eee5-1e97-495b-9370-853cd873bb07/Office/Data/v64_16.0.18429.20132.cab HTTP/1.1
     HTTP/1.1 200 OK
     GET /pr/5462eee5-1e97-495b-9370-853cd873bb07/Office/Data/v64_16.0.18429.20132.cab HTTP/1.1
     HTTP/1.1 200 OK
     HEAD /pr/5462eee5-1e97-495b-9370-853cd873bb07/Office/Data/v64_16.0.18429.20132.cab HTTP/1.1
     HTTP/1.1 200 OK
     HEAD /pr/5462eee5-1e97-495b-9370-853cd873bb07/Office/Data/v64_16.0.18429.20132.cab HTTP/1.1
     HTTP/1.1 200 OK
     HEAD /pr/5462eee5-1e97-495b-9370-853cd873bb07/Office/Data/v64_16.0.18429.20132.cab HTTP/1.1
     HTTP/1.1 200 OK
     HEAD /pr/5462eee5-1e97-495b-9370-853cd873bb07/Office/Data/v64_16.0.18429.20132.cab HTTP/1.1
     HTTP/1.1 200 OK
     GET /pr/5462eee5-1e97-495b-9370-853cd873bb07/Office/Data/v64_16.0.18429.20132.cab HTTP/1.1
     HTTP/1.1 206 Partial Content
     HEAD /pr/5462eee5-1e97-495b-9370-853cd873bb07/Office/Data/v64_16.0.18429.20132.cab HTTP/1.1
     HTTP/1.1 200 OK
     GET /pr/5462eee5-1e97-495b-9370-853cd873bb07/Office/Data/v64_16.0.18429.20132.cab HTTP/1.1
     HTTP/1.1 200 OK
     GET /msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?049829b444fa179c HTTP/1.1
     HTTP/1.1 304 Not Modified
     GET /msdownload/update/v3/static/trustedr/en/authrootstl.cab?42afbc15476214f1 HTTP/1.1
     HTTP/1.1 304 Not Modified
     ```

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?
    - Yes, now I see an “IF-MODIFIED-SINCE:” line in the HTTP GET.
    - The output is shown below:

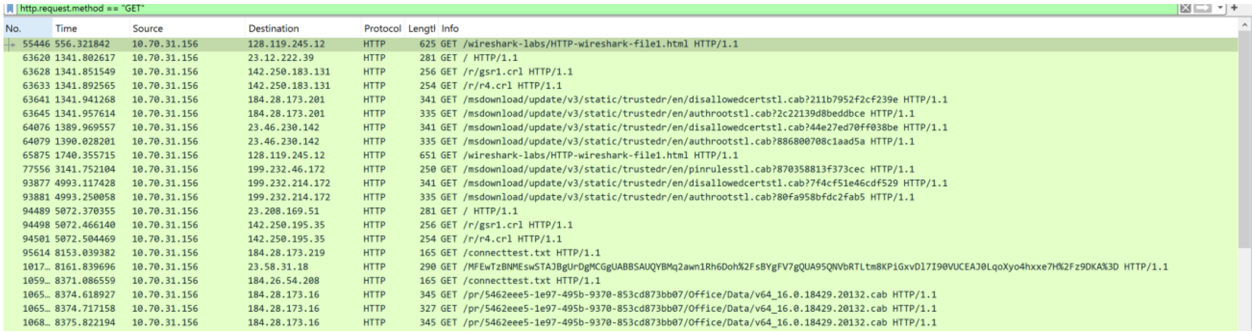


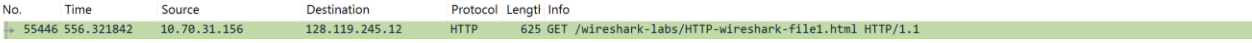
```
If-Modified-Since: Tue, 28 Jan 2025 06:59:01 GMT\r\n
```

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? Explain.
    - For the second request, the server returned 304 Not Modified, it means the server did not send the file because it hasn't changed since the last retrieval.
    - 

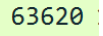
      ```
      GET /r/r4.crl HTTP/1.1
      HTTP/1.1 304 Not Modified
      ```
    - This will be shown in the HTTP Status and Phrase: 304 Not Modified.

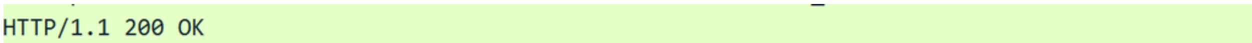
SECTION III: Retrieving Long Documents

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?
    - After filtering with http.request.method == "GET", there are 28 request messages that the browser sent.
    - 

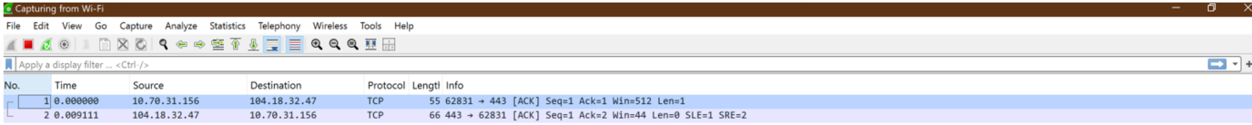
      ```
      http.request.method == "GET"
      No.   Time         Source        Destination      Protocol Lengtl Info
      55446 556.321842   10.70.31.156  128.119.245.12   HTTP     625 GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
      63620 1341.802617  10.70.31.156  23.12.222.39     HTTP     281 GET / HTTP/1.1
      63628 1341.851549  10.70.31.156  142.250.183.131  HTTP     256 GET /r/gsr1.crl HTTP/1.1
      63633 1341.892565  10.70.31.156  142.250.183.131  HTTP     254 GET /r/r4.crl HTTP/1.1
      63641 1341.941268  10.70.31.156  184.28.173.201   HTTP     341 GET /msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?211b7952f2cf239e HTTP/1.1
      63645 1341.957614  10.70.31.156  184.28.173.201   HTTP     335 GET /msdownload/update/v3/static/trustedr/en/authrootstl.cab?2c22139d8beddbce HTTP/1.1
      64076 1389.969557  10.70.31.156  23.46.230.142    HTTP     341 GET /msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?44e27ed70ff038be HTTP/1.1
      64079 1390.028201  10.70.31.156  23.46.230.142    HTTP     335 GET /msdownload/update/v3/static/trustedr/en/authrootstl.cab?886800708c1aad5a HTTP/1.1
      65875 1740.355715  10.70.31.156  128.119.245.12   HTTP     651 GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
      77556 3141.752104  10.70.31.156  199.232.46.172   HTTP     250 GET /msdownload/update/v3/static/trustedr/en/pinrulesstl.cab?870358813f373cec HTTP/1.1
      93877 4993.117428  10.70.31.156  199.232.214.172  HTTP     341 GET /msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?7f4cf51e46cdf529 HTTP/1.1
      93881 4993.250058  10.70.31.156  199.232.214.172  HTTP     335 GET /msdownload/update/v3/static/trustedr/en/authrootstl.cab?80fa958bfdc2fab5 HTTP/1.1
      94489 5072.370355  10.70.31.156  23.208.169.51    HTTP     281 GET / HTTP/1.1
      94498 5072.466140  10.70.31.156  142.250.195.35   HTTP     256 GET /r/gsr1.crl HTTP/1.1
      94501 5072.504469  10.70.31.156  142.250.195.35   HTTP     254 GET /r/r4.crl HTTP/1.1
      95614 8153.039382  10.70.31.156  184.28.173.219   HTTP     165 GET /connecttest.txt HTTP/1.1
      1017… 8161.839696  10.70.31.156  23.58.31.18      HTTP     290 GET /MFEwTzBNMEswSTAJBgUrDgMCGgUABBSAUQYBMq2awn1Rh6Doh%2FsBYgFV7gQUA95QNVbRTLtm8KPiGxvDl7I90VUCEAJ0LqoXyo4hxxe7H%2Fz9DKA%3D HTTP/1.1
      1059… 8371.086559  10.70.31.156  184.26.54.208    HTTP     165 GET /connecttest.txt HTTP/1.1
      1065… 8374.618927  10.70.31.156  184.28.173.16    HTTP     345 GET /pr/5462eee5-1e97-495b-9370-853cd873bb07/Office/Data/v64_16.0.18429.20132.cab HTTP/1.1
      1065… 8374.717158  10.70.31.156  184.28.173.16    HTTP     327 GET /pr/5462eee5-1e97-495b-9370-853cd873bb07/Office/Data/v64_16.0.18429.20132.cab HTTP/1.1
      1068… 8375.822194  10.70.31.156  184.28.173.16    HTTP     345 GET /pr/5462eee5-1e97-495b-9370-853cd873bb07/Office/Data/v64_16.0.18429.20132.cab HTTP/1.1
      ```
    - Packet number: 55446 has the trace contains the GET message for the Bill of Rights.
    - 

      ```
      No.   Time        Source        Destination     Protocol Lengtl Info
      55446 556.321842  10.70.31.156  128.119.245.12  HTTP     625 GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
      ```

13. Which packet number in the trace contains the status code and phrase associated with the response to the HTTP GET request?
    - Packet Number:  63620

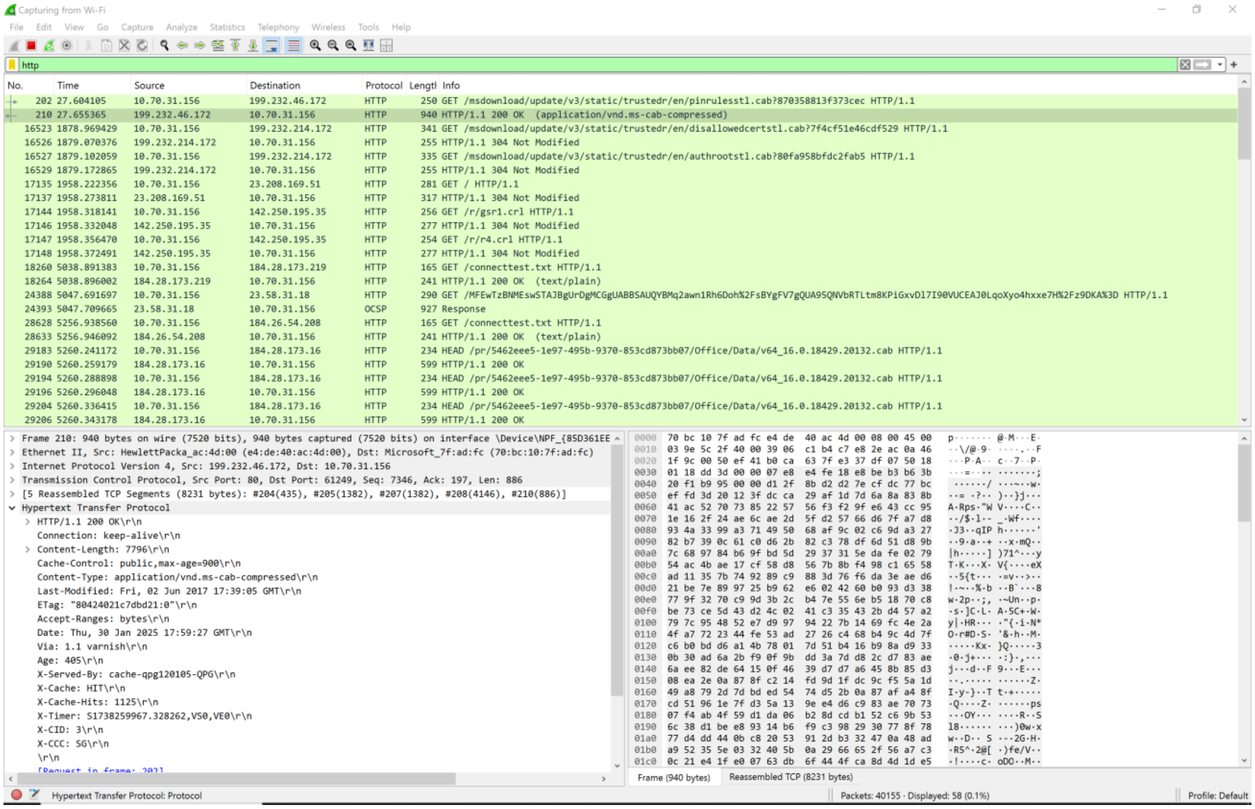
14. What is the status code and phrase in the response?
    - Status Code: 200
    - Phrase: OK
    - 

      ```
      HTTP/1.1 200 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 TCP segments carried the HTTP response and the Bill of Rights data.
    - 

      Capturing from Wi-Fi
      File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
      Apply a display filter ... <Ctrl-/>

      ```
      No. Time      Source        Destination   Protocol Lengtl Info
        1 0.000000  10.70.31.156  104.18.32.47  TCP      55 62831 → 443 [ACK] Seq=1 Ack=1 Win=512 Len=1
        2 0.009111  104.18.32.47  10.70.31.156  TCP      66 443 → 62831 [ACK] Seq=1 Ack=2 Win=44 Len=0 SLE=1 SRE=2
      ```



http

```
No.   Time         Source           Destination      Protocol Lengtl Info
  202 27.604105    10.70.31.156     199.232.46.172   HTTP      250 GET /msdownload/update/v3/static/trustedr/en/pinrulesstl.cab?870358813f373cec HTTP/1.1
  210 27.655365    199.232.46.172   10.70.31.156     HTTP      940 HTTP/1.1 200 OK  (application/vnd.ms-cab-compressed)
16523 1878.969429  10.70.31.156     199.232.214.172  HTTP      341 GET /msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?7f4cf51e46cdf529 HTTP/1.1
16526 1879.070376  199.232.214.172  10.70.31.156     HTTP      255 HTTP/1.1 304 Not Modified
16527 1879.102059  10.70.31.156     199.232.214.172  HTTP      335 GET /msdownload/update/v3/static/trustedr/en/authrootstl.cab?80fa958bfdc2fab5 HTTP/1.1
16529 1879.172865  199.232.214.172  10.70.31.156     HTTP      255 HTTP/1.1 304 Not Modified
17135 1958.222356  10.70.31.156     23.208.169.51    HTTP      281 GET / HTTP/1.1
17137 1958.273811  23.208.169.51    10.70.31.156     HTTP      317 HTTP/1.1 304 Not Modified
17144 1958.318141  10.70.31.156     142.250.195.35   HTTP      256 GET /r/gsr1.crl HTTP/1.1
17146 1958.332048  142.250.195.35   10.70.31.156     HTTP      277 HTTP/1.1 304 Not Modified
17147 1958.356470  10.70.31.156     142.250.195.35   HTTP      254 GET /r/r4.crl HTTP/1.1
17148 1958.372491  142.250.195.35   10.70.31.156     HTTP      277 HTTP/1.1 304 Not Modified
18260 5038.891383  10.70.31.156     184.28.173.219   HTTP      165 GET /connecttest.txt HTTP/1.1
18264 5038.896002  184.28.173.219   10.70.31.156     HTTP      241 HTTP/1.1 200 OK  (text/plain)
24388 5047.691697  10.70.31.156     23.58.31.18      HTTP      290 GET /MFEwTzBNMEswSTAJBgUrDgMCGgUABBSAUQYBMq2awn1Rh6Doh%2FsBYgFV7gQUA95QNVbRTLtm8KPiGxvDl7I90VUCEAJ0LqoXyo4hxxe7H%2Fz9DKA%3D HTTP/1.1
24393 5047.709665  23.58.31.18      10.70.31.156     OCSP      927 Response
28628 5256.938560  10.70.31.156     184.26.54.208    HTTP      165 GET /connecttest.txt HTTP/1.1
28633 5256.946092  184.26.54.208    10.70.31.156     HTTP      241 HTTP/1.1 200 OK  (text/plain)
29183 5260.241172  10.70.31.156     184.28.173.16    HTTP      234 HEAD /pr/5462eee5-1e97-495b-9370-853cd873bb07/Office/Data/v64_16.0.18429.20132.cab HTTP/1.1
29190 5260.259179  184.28.173.16    10.70.31.156     HTTP      599 HTTP/1.1 200 OK
29194 5260.288898  10.70.31.156     184.28.173.16    HTTP      234 HEAD /pr/5462eee5-1e97-495b-9370-853cd873bb07/Office/Data/v64_16.0.18429.20132.cab HTTP/1.1
29196 5260.296048  184.28.173.16    10.70.31.156     HTTP      599 HTTP/1.1 200 OK
29204 5260.336415  10.70.31.156     184.28.173.16    HTTP      234 HEAD /pr/5462eee5-1e97-495b-9370-853cd873bb07/Office/Data/v64_16.0.18429.20132.cab HTTP/1.1
29206 5260.343178  184.28.173.16    10.70.31.156     HTTP      599 HTTP/1.1 200 OK
```

```
> Frame 210: 940 bytes on wire (7520 bits), 940 bytes captured (7520 bits) on interface \Device\NPF_{85D361EE
> Ethernet II, Src: HewlettPacka_ac:4d:00 (e4:de:40:ac:4d:00), Dst: Microsoft_7f:ad:fc (70:bc:10:7f:ad:fc)
> Internet Protocol Version 4, Src: 199.232.46.172, Dst: 10.70.31.156
> Transmission Control Protocol, Src Port: 80, Dst Port: 61249, Seq: 7346, Ack: 197, Len: 886
> [5 Reassembled TCP Segments (8231 bytes): #204(435), #205(1382), #207(1382), #208(4146), #210(886)]
v Hypertext Transfer Protocol
  > HTTP/1.1 200 OK\r\n
    Connection: keep-alive\r\n
  > Content-Length: 7796\r\n
    Cache-Control: public,max-age=900\r\n
    Content-Type: application/vnd.ms-cab-compressed\r\n
    Last-Modified: Fri, 02 Jun 2017 17:39:05 GMT\r\n
    ETag: "80424021c7dbd21:0"\r\n
    Accept-Ranges: bytes\r\n
    Date: Thu, 30 Jan 2025 17:59:27 GMT\r\n
    Via: 1.1 varnish\r\n
    Age: 405\r\n
    X-Served-By: cache-qpg120105-QPG\r\n
    X-Cache: HIT\r\n
    X-Cache-Hits: 1125\r\n
    X-Timer: S1738259967.328262,VS0,VE0\r\n
    X-CID: 3\r\n
    X-CCC: SG\r\n
    \r\n
    [Request in frame: 202]
```

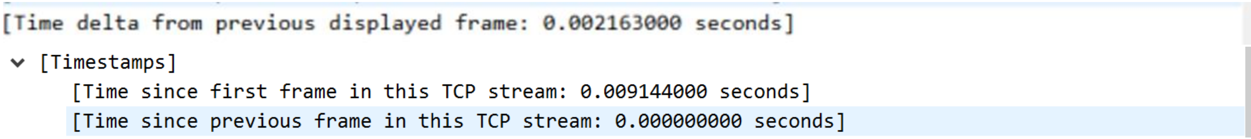
```
0000  70 bc 10 7f ad fc e4 de  40 ac 4d 00 08 00 45 00   p······· @·M···E·
0010  03 9e 5c 2f 40 00 39 06  c1 b4 c7 e8 2e ac 0a 46   ··\/@·9· ····.··F
0020  1f 9c 00 50 ef 41 b0 ca  63 7f e3 37 df 07 50 18   ···P·A·· c··7··P·
0030  01 18 dd 3d 00 00 07 e8  e4 fe 18 e8 be b3 b6 3b   ···=···· ·······;
0040  20 f1 b9 95 00 00 d1 2f  8b d2 d2 7e cf dc 77 bc    ······/ ···~··w·
0050  ef fd 3d 20 12 3f dc ca  29 af 1d 7d 6a 8a 83 8b   ··= ·?·· )··}j···
0060  41 ac 52 70 73 85 22 57  56 f3 f2 9f e6 43 cc 95   A·Rps·"W V····C··
0070  1e 16 2f 24 ae 6c ae 2d  5f d2 57 66 d6 7f a7 d8   ··/$·l·- _·Wf····
0080  93 4a 33 99 a3 71 49 50  68 af 9c 02 c6 9d a3 27   ·J3··qIP h······'
0090  82 b7 39 0c 61 c0 d6 2b  82 c3 78 df 6d 51 d8 9b   ··9·a··+ ··x·mQ··
00a0  7c 68 97 84 b6 9f bd 5d  29 37 31 5e da fe 02 79   |h·····] )71^···y
00b0  54 ac 4b ae 17 cf 58 d8  56 7b 8b f4 98 c1 65 58   T·K···X· V{····eX
00c0  ad 11 35 7b 74 92 89 c9  88 3d 76 f6 da 3e ae d6   ··5{t··· ·=v··>··
00d0  21 be 7e 89 97 25 b9 62  e6 02 42 60 b0 93 d3 38   !·~··%·b ··B`···8
00e0  77 9f 32 70 c9 9d 3b 2c  b4 7e 55 6e b5 18 70 c8   w·2p··;, ·~Un··p·
00f0  be 73 ce 5d 43 d2 4c 02  41 c3 35 43 2b d4 57 a2   ·s·]C·L· A·5C+·W·
0100  79 7c 95 48 52 e7 d9 97  94 22 7b 14 69 fc 4e 2a   y|·HR··· ·"{·i·N*
0110  4f a7 72 23 44 fe 53 ad  27 26 c4 68 b4 9c 4d 7f   O·r#D·S· '&·h··M·
0120  c6 b0 bd d6 a1 4b 78 01  7d 51 b4 16 b9 8a d9 33   ·····Kx· }Q·····3
0130  0b 30 ad 6a 2b f9 0f 9b  dd 3a 7d d8 2c d7 83 ae   ·0·j+··· ·:}·,···
0140  6a ee 82 de 64 15 0f 46  39 d7 d7 a6 45 8b 85 d3   j···d··F 9···E···
0150  08 ea 2e 0a 87 8f c2 14  fd 9d 1f dc 9c f5 5a 1d   ··.····· ······Z·
0160  49 a8 79 2d 7d bd ed 54  74 d5 2b 0a 87 af a4 8f   I·y-}··T t·+·····
0170  cd 51 96 1e 7f d3 5a 13  9e e4 d6 c9 83 ae 70 73   ·Q····Z· ······ps
0180  07 f4 ab 4f 59 d1 da 06  b2 8d cd b1 52 c6 9b 53   ···OY··· ····R··S
0190  6c 38 d1 be e8 93 14 b6  f9 c3 98 29 30 77 8f 78   l8······ ···)0w·x
01a0  77 d4 dd 44 0b c8 20 53  91 2d b3 32 47 0a 48 ad   w··D·· S ·-·2G·H·
01b0  a9 52 35 5e 03 32 40 5b  0a 29 66 65 2f 56 a7 c3   ·R5^·2@[ ·)fe/V··
01c0  0c 21 e4 1f e0 07 63 db  6f 44 4f ca 8d 4d 1d e5   ·!····c· oDO··M··
```

Frame (940 bytes)
Reassembled TCP (8231 bytes)
Hypertext Transfer Protocol: Protocol
Packets: 40155 · Displayed: 58 (0.1%)
Profile: Default

SECTION IV: HTML Documents with Embedded Objects

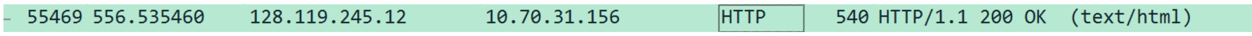
16. How many HTTP GET request messages did your browser send? To which Internet addresses were these GET requests sent?
    - The total number of HTTP GET requests my browser sent was 3.
    - First GET request to gaia.cs.umass.edu for the HTML.
    - Second GET request to gaia.cs.umass.edu for the first image.
    - Third GET request to caite.cs.umass.edu for the second image.

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.
    - My browser downloaded from the two web sites in parallel. It is usually said by observing the timestamps of the GET requests and responses for the two images.
    - Since the GET requests are sent close together, with less delay between them, the images will be downloaded in parallel.
    -

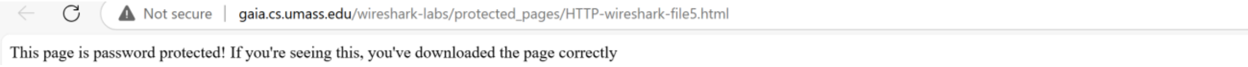


```
[Time delta from previous displayed frame: 0.002163000 seconds]
v [Timestamps]
    [Time since first frame in this TCP stream: 0.009144000 seconds]
    [Time since previous frame in this TCP stream: 0.000000000 seconds]
```

SECTION V: HTTP Authentication

18. What is the server’s response (status code and phrase) in response to the initial HTTP GET message from your browser?
    - When my browser sent the first request to the server for the HTML file, the server responded with the status code 200 OK. This means the server successfully found the file and sent it back to my browser.
    - 

```
55469 556.535460    128.119.245.12        10.70.31.156          HTTP     540 HTTP/1.1 200 OK  (text/html)
```

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

      Not secure | gaia.cs.umass.edu/wireshark-labs/protected_pages/HTTP-wireshark-file5.html

      This page is password protected! If you're seeing this, you've downloaded the page correctly
    - When my browser sent the second HTTP GET request (after receiving the 401 response), it included a new field called Authorization: Basic.
    - This field contains a base64-encoded username and password that the browser sends to the server for authentication.