IIT PALAKKAD

Indian Institute of Technology Palakkad
Department of Computer Science and Engineering
CS4010 Computer Networks
August-December 2024

Assignment – 1
Name: Neeraj Krishna N
Roll no: 112101033

Part 1

Q1

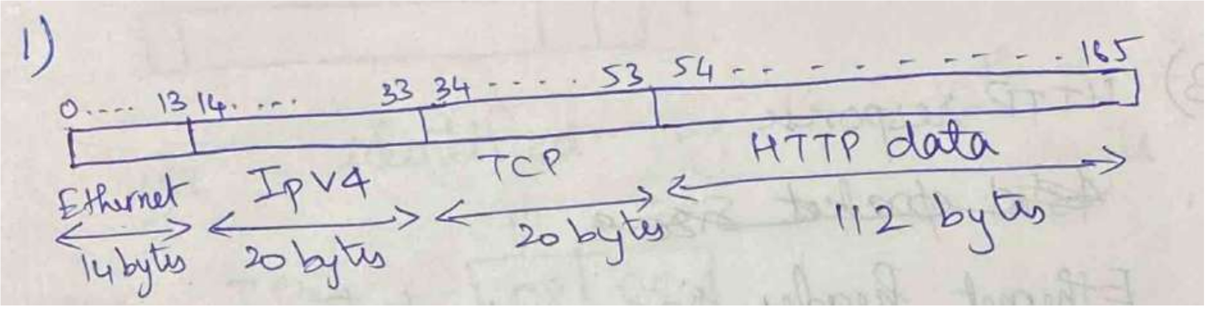


Figure 1: Packet

Q2

For packet-7, the total packet size is 1484 bytes.
Ethernet Header Size = 14 bytes
IPv4 header size = 20 bytes
TCP header size = 20 bytes

$$\begin{aligned}\text{Overhead} &= \frac{\text{Header size}}{\text{Total packet size}}\\ &= \frac{14+20+20}{1484}\\ &= 3.64\%\end{aligned}$$

Q3

HTTP response
Ethernet Header size = 14 bytes
IPv4 header size = 20 bytes
TCP header size = 20 bytes

$$\begin{aligned}
\text{HTTP headers + messages(Useful data size)} &= \text{HTTP file data size + html data size} \\
&= 736 + 14201 \text{ bytes} \\
&= 14937 \text{ bytes} \\
\text{Overhead} &= \frac{\text{Total header size}}{\text{Total Packet size}} \\
&= \frac{14 + 20 + 20}{14937 + 14 + 20 + 20} \\
&= \frac{54}{14991} \\
&\approx 0.36\%
\end{aligned}$$

Q4

Ethernet header size is 14 bytes (from 0th to 13th byte in the packet)
Type is identified by the 12th and the 13th byte. In this case the 12th and 13th byte together has the value 0x0800 which indicates that the type is IPv4. Hence 12th and 13th byte of the Ethernet header field is the demultiplexing key indicating that the next layer is IP, and the value used in this field is 0x0800 to indicate IP.

Q5

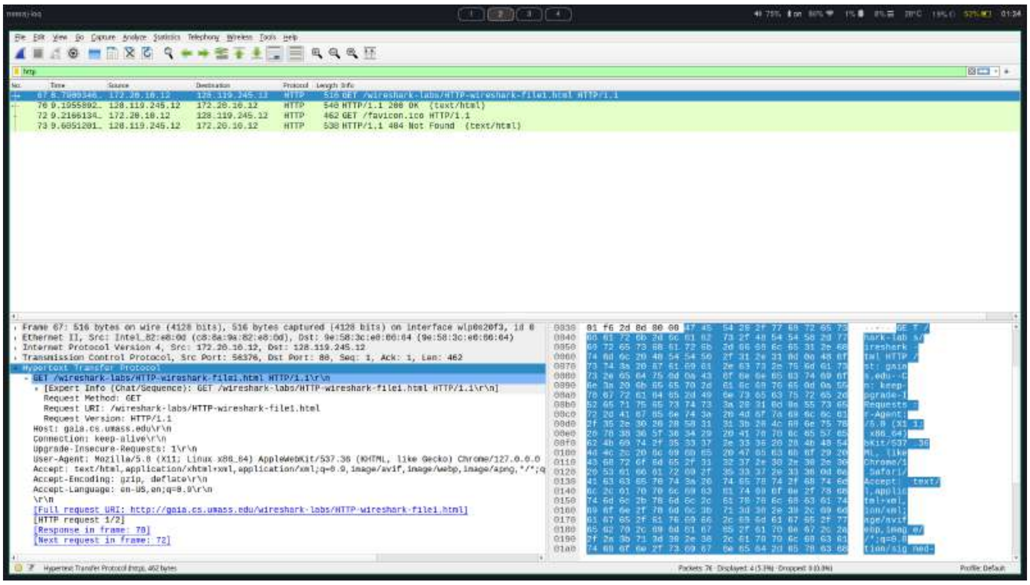
IP header size is 20 bytes. In the packet the position of IP header is from 14th to 33rd byte. 9th byte of IP header (equivalently 23rd byte in the packet (indexing starting from 0th byte)), is the demultiplexing key indicating that the next layer is TCP and the value used in this field to indicate TCP is 0x06.

Q6

TCP doesn't include a separate demultiplexing key because here the port number which is 80 acts like the demultiplexing key. If the port number is 80, then it means that HTTP is used for handling the data. TCP port is a unique number assigned to different applications

Part 2

Q1

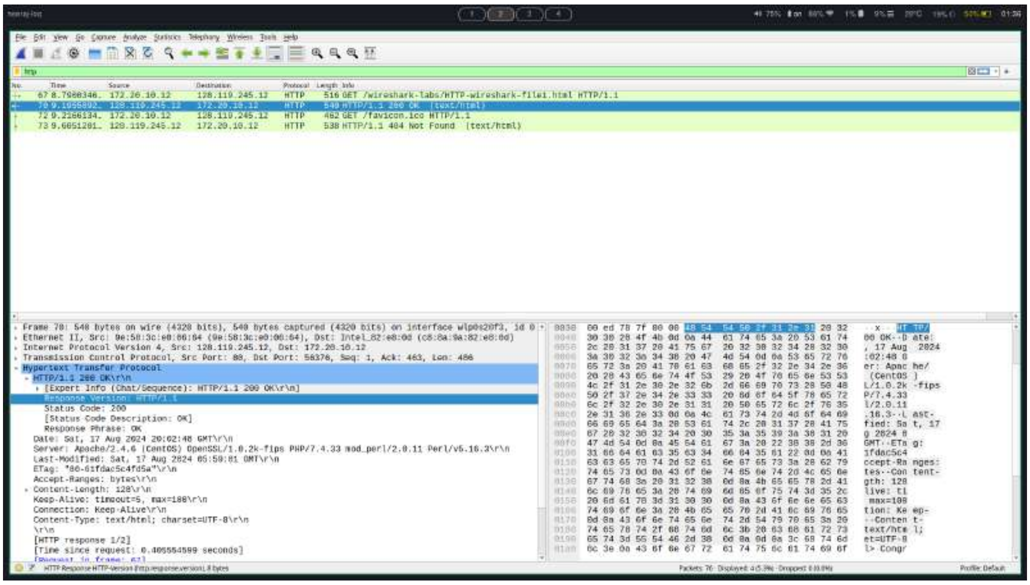


```
No.  Time         Source          Destination     Protocol Length Info
67 8.7989346…  172.20.10.12    128.119.245.12  HTTP     516 GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
76 9.1955892…  128.119.245.12  172.20.10.12    HTTP     540 HTTP/1.1 200 OK  (text/html)
72 9.2166134…  172.20.10.12    128.119.245.12  HTTP     462 GET /favicon.ico HTTP/1.1
73 9.6851201…  128.119.245.12  172.20.10.12    HTTP     538 HTTP/1.1 404 Not Found  (text/html)
```

```
Frame 67: 516 bytes on wire (4128 bits), 516 bytes captured (4128 bits) on interface wlp0s20f3, id 0
Ethernet II, Src: Intel_82:e8:0d (c8:8a:9a:82:e8:0d), Dst: 9e:58:3c:e0:06:64 (9e:58:3c:e0:06:64)
Internet Protocol Version 4, Src: 172.20.10.12, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 58376, Dst Port: 80, Seq: 1, Ack: 1, Len: 462
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/127.0.0.0
  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q
  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-file1.html]
  [HTTP request 1/2]
  [Response in frame: 70]
  [Next request in frame: 72]
```

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
Hypertext Transfer Protocol (http), 462 bytes

Figure 2: Request Version



```
No.  Time         Source          Destination     Protocol Length Info
67 8.7989346…  172.20.10.12    128.119.245.12  HTTP     516 GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
70 9.1955892…  128.119.245.12  172.20.10.12    HTTP     540 HTTP/1.1 200 OK  (text/html)
72 9.2166134…  172.20.10.12    128.119.245.12  HTTP     462 GET /favicon.ico HTTP/1.1
73 9.6851201…  128.119.245.12  172.20.10.12    HTTP     538 HTTP/1.1 404 Not Found  (text/html)
```

```
Frame 70: 540 bytes on wire (4320 bits), 540 bytes captured (4320 bits) on interface wlp0s20f3, id 0
Ethernet II, Src: 9e:58:3c:e0:06:64 (9e:58:3c:e0:06:64), Dst: Intel_82:e8:0d (c8:8a:9a:82:e8:0d)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 172.20.10.12
Transmission Control Protocol, Src Port: 80, Dst Port: 58376, Seq: 1, Ack: 463, Len: 486
Hypertext Transfer Protocol
  HTTP/1.1 200 OK\r\n
    [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
    Response Version: HTTP/1.1
    Status Code: 200
    [Status Code Description: OK]
    Response Phrase: OK
  Date: Sat, 17 Aug 2024 20:02:48 GMT\r\n
  Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.33 mod_perl/2.0.11 Perl/v5.16.3\r\n
  Last-Modified: Sat, 17 Aug 2024 05:59:01 GMT\r\n
  ETag: "80-61fdac5c4fd5a"\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]
  [Time since request: 0.405554599 seconds]
  [Request in frame: 67]
```

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
HTTP Response HTTP-Version (http.response.version), 8 bytes

Figure 3: Response Version

Browser version can be checked at the Request version in the captured packet and similarly, server version can be checked at the Response version in the packet captured.
My browser is running HTTP version 1.1 and the server is also running HTTP version 1.1

Q2

In the figure 2, we can see that there is a field named ”Accept Languages: en-US; en;q=0.9;\r\n” Browser indicates that it can accept ”en-US” (English of US)

Q3

IP address of my computer can be seen from the ”src” field of IPv4 header in figure 2, which is 172.20.10.12 and similarly IP address of ”gaia.cs.umass.edu.server” can be seen from the ”src” field of IPv4 header in figure 3 which is 128.119.245.12

Q4

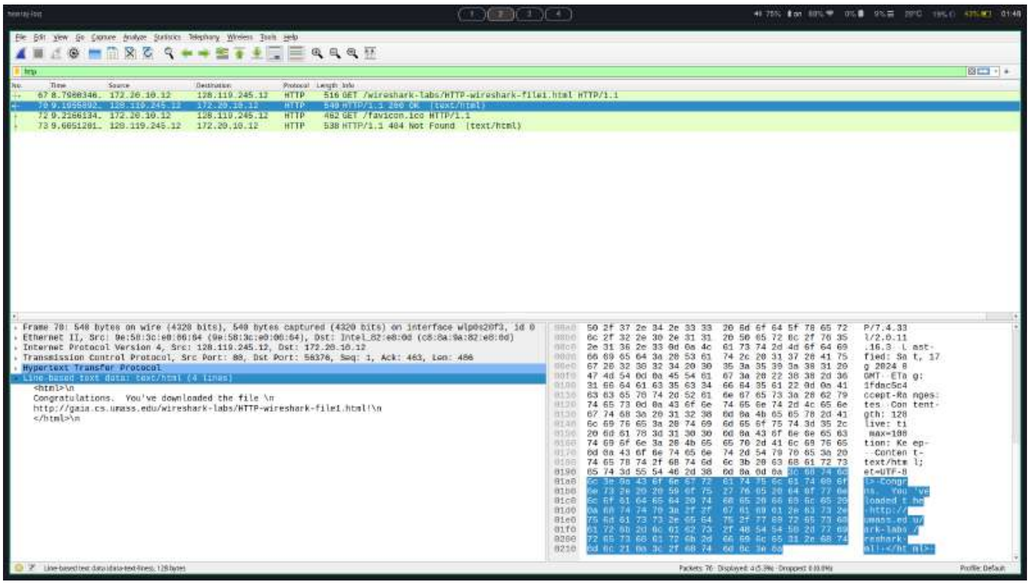
The status code can be seen from the packet listing, which is shown to be ”200 OK”

Q5

”Last modified” field can be checked in the HTTP header in the response packet of the server shown in figure 3 and the value of ”Last Modified” is ”Sat, 17 Aug 2024 05:59:01 GMT”

Q6

Content size is 128 bytes as can be seen in the bottom status bar in the figure 4


1
2
3
4
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http

```
No.  Time         Source          Destination     Protocol Length Info
  67 8.7980346…   172.20.10.12    128.119.245.12  HTTP     516 GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
  70 9.1956892…   128.119.245.12  172.20.10.12    HTTP     540 HTTP/1.1 200 OK  (text/html)
  72 9.2166134…   172.20.10.12    128.119.245.12  HTTP     462 GET /favicon.ico HTTP/1.1
  73 9.6651281…   128.119.245.12  172.20.10.12    HTTP     538 HTTP/1.1 404 Not Found  (text/html)
```

```
Frame 70: 540 bytes on wire (4320 bits), 540 bytes captured (4320 bits) on interface wlp0s20f3, id 0
Ethernet II, Src: 9e:58:3c:e0:06:64 (9e:58:3c:e0:06:64), Dst: Intel_82:e8:0d (c8:8a:9a:82:e8:0d)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 172.20.10.12
Transmission Control Protocol, Src Port: 80, Dst Port: 58376, Seq: 1, Ack: 463, Len: 486
Hypertext Transfer Protocol
Line-based text data: text/html (4 lines)
    <html>\n
    Congratulations.  You've downloaded the file \n
    http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html!\n
    </html>\n
```

```
00a0  50 2f 37 2e 34 2e 33 33  20 6d 6f 64 5f 70 65 72   P/7.4.33
00b0  6c 2f 32 2e 30 2e 31 31  20 50 65 72 6c 2f 76 35   l/2.0.11
00c0  2e 31 36 2e 33 0d 0a 4c  61 73 74 2d 4d 6f 64 69   .16.3··L ast-
00d0  66 69 65 64 3a 20 53 61  74 2c 20 31 37 20 41 75   fied: Sa t, 17
00e0  67 20 32 30 32 34 20 30  35 3a 35 39 3a 30 31 20   g 2024 0
00f0  47 4d 54 0d 0a 45 54 61  67 3a 20 22 38 30 2d 36   GMT··ETa g:
0100  31 66 64 61 63 35 63 34  66 64 35 61 22 0d 0a 41   1fdac5c4
0110  63 63 65 70 74 2d 52 61  6e 67 65 73 3a 20 62 79   ccept-Ra nges:
0120  74 65 73 0d 0a 43 6f 6e  74 65 6e 74 2d 4c 65 6e   tes··Con tent-
0130  67 74 68 3a 20 31 32 38  0d 0a 4b 65 65 70 2d 41   gth: 128
0140  6c 69 76 65 3a 20 74 69  6d 65 6f 75 74 3d 35 2c   live: ti
0150  20 6d 61 78 3d 31 30 30  0d 0a 43 6f 6e 6e 65 63    max=100
0160  74 69 6f 6e 3a 20 4b 65  65 70 2d 41 6c 69 76 65   tion: Ke ep-
0170  0d 0a 43 6f 6e 74 65 6e  74 2d 54 79 70 65 3a 20   ··Conten t-
0180  74 65 78 74 2f 68 74 6d  6c 3b 20 63 68 61 72 73   text/htm l;
0190  65 74 3d 55 54 46 2d 38  0d 0a 0d 0a 3c 68 74 6d   et=UTF-8
01a0  6c 3e 0a 43 6f 6e 67 72  61 74 75 6c 61 74 69 6f   l>·Congr
01b0  6e 73 2e 20 20 59 6f 75  27 76 65 20 64 6f 77 6e   ns.  You 've
01c0  6c 6f 61 64 65 64 20 74  68 65 20 66 69 6c 65 20   loaded t he
01d0  0a 68 74 74 70 3a 2f 2f  67 61 69 61 2e 63 73 2e   ·http://
01e0  75 6d 61 73 73 2e 65 64  75 2f 77 69 72 65 73 68   umass.ed u/
01f0  61 72 6b 2d 6c 61 62 73  2f 48 54 54 50 2d 77 69   ark-labs /
0200  72 65 73 68 61 72 6b 2d  66 69 6c 65 31 2e 68 74   reshark-
0210  6d 6c 21 0a 3c 2f 68 74  6d 6c 3e 0a               ml!·</ht ml>·
```

Line-based text data (data-text-lines), 128 bytes

Packets: 76 · Displayed: 4 (5.3%) · Dropped: 0 (0.0%)

Profile: Default

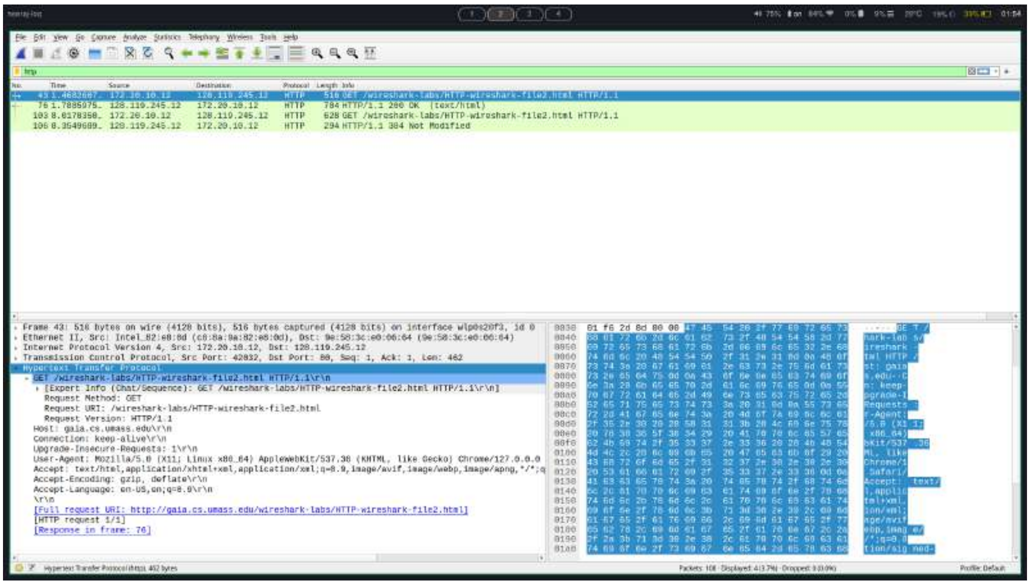
Figure 4: Content Size

Q7

No, all headers are being shown in the packet listing

Q8

No, there is no field ”If-Modified-Since” in the first HTTP Get request as shown in figure 5



File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
Hypertext Transfer Protocol (http), 462 bytes
Profile: Default

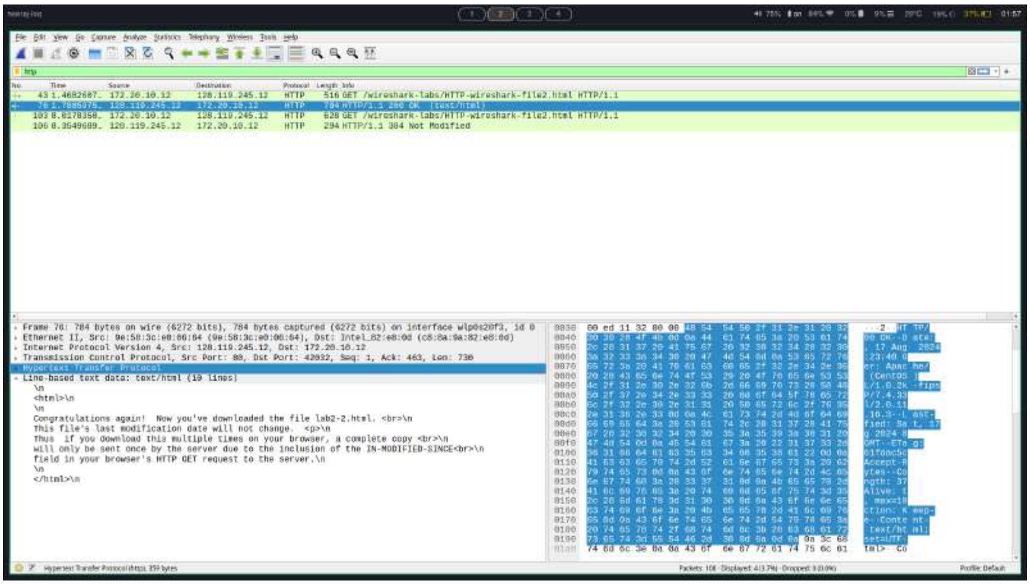
```
No.   Time          Source           Destination      Protocol Length Info
   43 1.4682687…  172.20.10.12     128.119.245.12   HTTP     516 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
   76 1.7885975…  128.119.245.12   172.20.10.12     HTTP     784 HTTP/1.1 200 OK  (text/html)
  103 8.0178358…  172.20.10.12     128.119.245.12   HTTP     628 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
  106 8.3549689…  128.119.245.12   172.20.10.12     HTTP     294 HTTP/1.1 304 Not Modified
```

```
Frame 43: 516 bytes on wire (4128 bits), 516 bytes captured (4128 bits) on interface wlp0s20f3, id 0
Ethernet II, Src: Intel_82:e8:0d (c8:8a:9a:82:e8:0d), Dst: 9e:58:3c:e0:06:64 (9e:58:3c:e0:06:64)
Internet Protocol Version 4, Src: 172.20.10.12, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 42032, Dst Port: 80, Seq: 1, Ack: 1, Len: 462
Hypertext Transfer Protocol
  GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n
    [Expert Info (Chat/Sequence): GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n]
    Request Method: GET
    Request URI: /wireshark-labs/HTTP-wireshark-file2.html
    Request Version: HTTP/1.1
  Host: gaia.cs.umass.edu\r\n
  Connection: keep-alive\r\n
  Upgrade-Insecure-Requests: 1\r\n
  User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/127.0.0.0
  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q
  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 1/1]
  [Response in frame: 76]
```

Figure 5: No field named ”If Modified” in the first GET request

Q9

Yes, the server explicitly returned the contents of the file. This can be seen from the response of the server which contains the HTML data (the section ”Line Based text data”)



File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
Hypertext Transfer Protocol (http), 359 bytes
Profile: Default

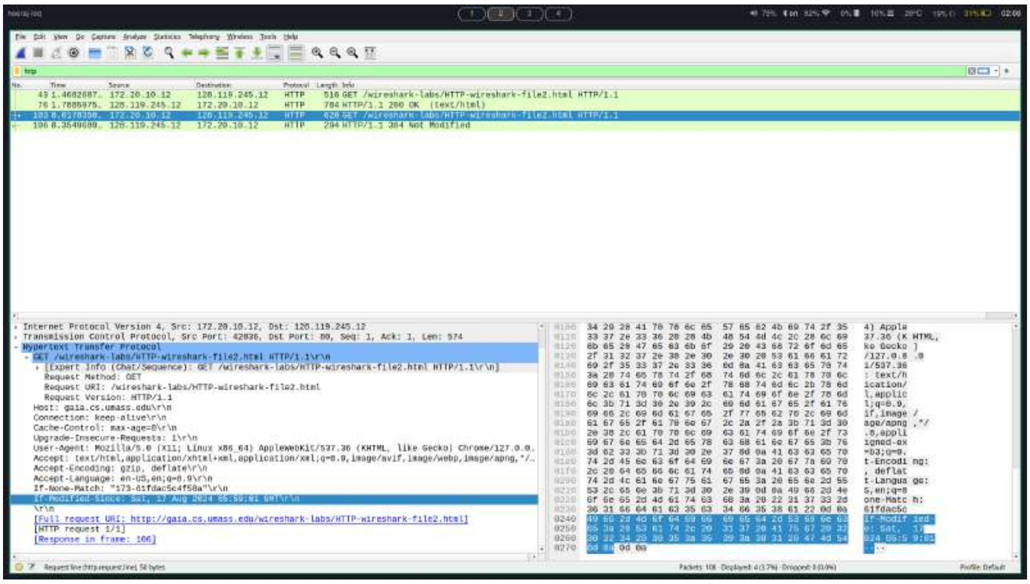
```
No.   Time          Source           Destination      Protocol Length Info
   43 1.4682687…  172.20.10.12     128.119.245.12   HTTP     516 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
   76 1.7885975…  128.119.245.12   172.20.10.12     HTTP     784 HTTP/1.1 200 OK  (text/html)
  103 8.0178358…  172.20.10.12     128.119.245.12   HTTP     628 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
  106 8.3549689…  128.119.245.12   172.20.10.12     HTTP     294 HTTP/1.1 304 Not Modified
```

```
Frame 76: 784 bytes on wire (6272 bits), 784 bytes captured (6272 bits) on interface wlp0s20f3, id 0
Ethernet II, Src: 9e:58:3c:e0:06:64 (9e:58:3c:e0:06:64), Dst: Intel_82:e8:0d (c8:8a:9a:82:e8:0d)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 172.20.10.12
Transmission Control Protocol, Src Port: 80, Dst Port: 42032, Seq: 1, Ack: 463, Len: 730
Hypertext Transfer Protocol
Line-based text data: text/html (10 lines)
  \n
  <html>\n
  \n
  Congratulations again!  Now you've downloaded the file lab2-2.html. <br>\n
  This file's last modification date will not change.  <p>\n
  Thus  if you download this multiple times on your browser, a complete copy <br>\n
  will only be sent once by the server due to the inclusion of the IN-MODIFIED-SINCE<br>\n
  field in your browser's HTTP GET request to the server.\n
  \n
  </html>\n
```

Figure 6: Server explicitly returned the contents

Q10

Yes, now IF-Modified-Since field is being shown. The information shown is ”If-Modified-Since: Sat, 17 Aug 2024 05:59:01 GMT”



```
No.  Time        Source          Destination     Protocol Length Info
  49 1.4682687…  172.20.10.12    128.119.245.12  HTTP     516 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
  76 1.7886975…  128.119.245.12  172.20.10.12    HTTP     784 HTTP/1.1 200 OK  (text/html)
 103 8.6178358…  172.20.10.12    128.119.245.12  HTTP     628 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
 106 8.3540680…  128.119.245.12  172.20.10.12    HTTP     294 HTTP/1.1 304 Not Modified
```

```
› Internet Protocol Version 4, Src: 172.20.10.12, Dst: 128.119.245.12
› Transmission Control Protocol, Src Port: 42836, Dst Port: 80, Seq: 1, Ack: 1, Len: 574
⌄ Hypertext Transfer Protocol
  ⌄ GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n
    › [Expert Info (Chat/Sequence): GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n]
      Request Method: GET
      Request URI: /wireshark-labs/HTTP-wireshark-file2.html
      Request Version: HTTP/1.1
    Host: gaia.cs.umass.edu\r\n
    Connection: keep-alive\r\n
    Cache-Control: max-age=0\r\n
    Upgrade-Insecure-Requests: 1\r\n
    User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/127.0.0.…
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/…
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: en-US,en;q=0.9\r\n
    If-None-Match: "173-61fdac5c4f58a"\r\n
    If-Modified-Since: Sat, 17 Aug 2024 05:59:01 GMT\r\n
    \r\n
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]
    [HTTP request 1/1]
    [Response in frame: 106]
```

```
0100  34 29 20 41 70 70 6c 65  57 65 62 4b 69 74 2f 35   4) Apple
0110  33 37 2e 33 36 20 28 4b  48 54 4d 4c 2c 20 6c 69   37.36 (K HTML,
0120  6b 65 20 47 65 63 6b 6f  29 20 43 68 72 6f 6d 65   ke Gecko )
0130  2f 31 32 37 2e 30 2e 30  2e 30 20 53 61 66 61 72   /127.0.0 .0
0140  69 2f 35 33 37 2e 33 36  0d 0a 41 63 63 65 70 74   i/537.36
0150  3a 20 74 65 78 74 2f 68  74 6d 6c 2c 61 70 70 6c   : text/h
0160  69 63 61 74 69 6f 6e 2f  78 68 74 6d 6c 2b 78 6d   ication/
0170  6c 2c 61 70 70 6c 69 63  61 74 69 6f 6e 2f 78 6d   l,applic
0180  6c 3b 71 3d 30 2e 39 2c  69 6d 61 67 65 2f 61 76   l;q=0.9,
0190  69 66 2c 69 6d 61 67 65  2f 77 65 62 70 2c 69 6d   if,image /
01a0  61 67 65 2f 61 70 6e 67  2c 2a 2f 2a 3b 71 3d 30   age/apng ,*/
01b0  2e 38 2c 61 70 70 6c 69  63 61 74 69 6f 6e 2f 73   .8,appli
01c0  69 67 6e 65 64 2d 65 78  63 68 61 6e 67 65 3b 76   igned-ex
01d0  3d 62 33 3b 71 3d 30 2e  37 0d 0a 41 63 63 65 70   =b3;q=0.
01e0  74 2d 45 6e 63 6f 64 69  6e 67 3a 20 67 7a 69 70   t-Encodi ng:
01f0  2c 20 64 65 66 6c 61 74  65 0d 0a 41 63 63 65 70   , deflat
0200  74 2d 4c 61 6e 67 75 61  67 65 3a 20 65 6e 2d 55   t-Langua ge:
0210  53 2c 65 6e 3b 71 3d 30  2e 39 0d 0a 49 66 2d 4e   S,en;q=0
0220  6f 6e 65 2d 4d 61 74 63  68 3a 20 22 31 37 33 2d   one-Matc h:
0230  36 31 66 64 61 63 35 63  34 66 35 38 61 22 0d 0a   61fdac5c
0240  49 66 2d 4d 6f 64 69 66  69 65 64 2d 53 69 6e 63   If-Modif ied-
0250  65 3a 20 53 61 74 2c 20  31 37 20 41 75 67 20 32   e: Sat,  17
0260  30 32 34 20 30 35 3a 35  39 3a 30 31 20 47 4d 54   024 05:5 9:01
0270  0d 0a 0d 0a                                        ····
```

Request line (http.request.line), 58 bytes
Packets: 108 · Displayed: 4 (3.7%) · Dropped: 0 (0.0%)
Profile: Default

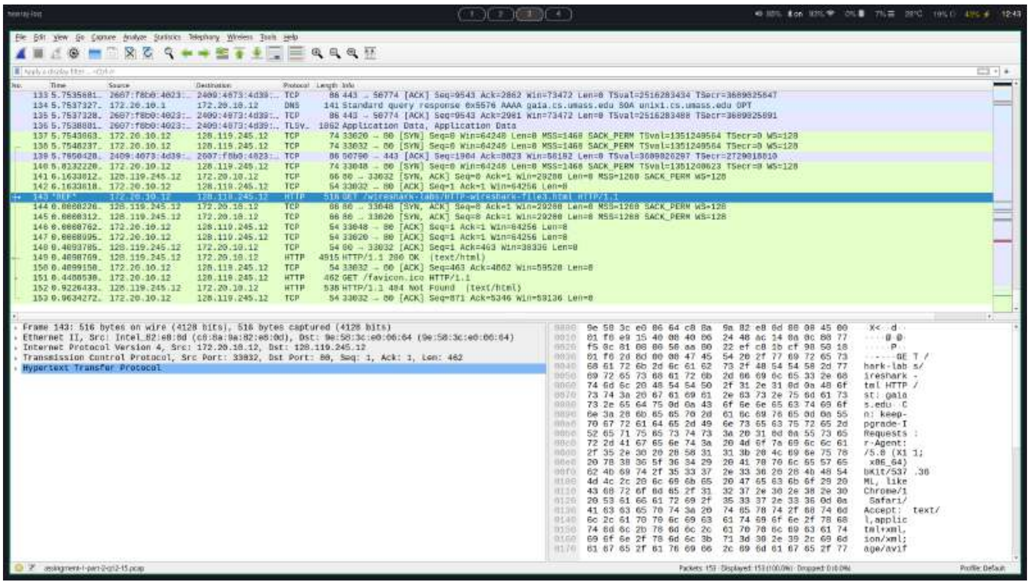
Figure 7: If-Modified-Since field present in the HTTP header

Q11

The status code and phrase is ”304 Not Modified”, which can be seen from the last response from the server in the figure 7. The server, this time did not explicitly return the contents of the file because, the browser had cached the contents of the file from the response of the previous GET request and since the file has not been modified since then (which can be identified from the ”If-Modified=Since” field in the GET request) browser renders the contents of the file from the cache

Q12

The packet whose packet number is 143 (whose timestamp is marked as REF) is the first GET request) in the figure 8. Only 1 HTTP GET request was sent by the browser which can be seen from packet number 143



```
No.  Time        Source              Destination         Protocol Length Info
 133 5.7535681…  2607:f8b0:4023:…    2409:4073:4d39:…    TCP      86 443 → 50774 [ACK] Seq=9543 Ack=2862 Win=73472 Len=0 TSval=2516283434 TSecr=3689825647
 134 5.7537327…  172.20.10.1         172.20.10.12        DNS      141 Standard query response 0x5576 AAAA gaia.cs.umass.edu SOA unix1.cs.umass.edu OPT
 135 5.7537328…  2607:f8b0:4023:…    2409:4073:4d39:…    TCP      86 443 → 50774 [ACK] Seq=9543 Ack=2981 Win=73472 Len=0 TSval=2516283488 TSecr=3689825691
 136 5.7538881…  2607:f8b0:4023:…    2409:4073:4d39:…    TLSv…    1862 Application Data, Application Data
 137 5.7543863…  172.20.10.12        128.119.245.12      TCP      74 33020 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=1351240564 TSecr=0 WS=128
 138 5.7548237…  172.20.10.12        128.119.245.12      TCP      74 33032 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=1351240564 TSecr=0 WS=128
 139 5.7850428…  2409:4073:4d39:…    2607:f8b0:4023:…    TCP      86 50790 → 443 [ACK] Seq=1904 Ack=8023 Win=58192 Len=0 TSval=3689826207 TSecr=2729018810
 140 5.8132220…  172.20.10.12        128.119.245.12      TCP      74 33048 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=1351240623 TSecr=0 WS=128
 141 6.1633812…  128.119.245.12      172.20.10.12        TCP      66 80 → 33032 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1260 SACK_PERM WS=128
 142 6.1633818…  172.20.10.12        128.119.245.12      TCP      54 33032 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0
 143 *REF*       172.20.10.12        128.119.245.12      HTTP     516 GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
 144 0.0000226…  128.119.245.12      172.20.10.12        TCP      66 80 → 33048 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1260 SACK_PERM WS=128
 145 0.0000312…  128.119.245.12      172.20.10.12        TCP      66 80 → 33020 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1260 SACK_PERM WS=128
 146 0.0000762…  172.20.10.12        128.119.245.12      TCP      54 33048 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0
 147 0.0000895…  172.20.10.12        128.119.245.12      TCP      54 33020 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0
 148 0.4093785…  128.119.245.12      172.20.10.12        TCP      54 80 → 33032 [ACK] Seq=1 Ack=463 Win=30336 Len=0
 149 0.4098769…  128.119.245.12      172.20.10.12        HTTP     4915 HTTP/1.1 200 OK  (text/html)
 150 0.4099150…  172.20.10.12        128.119.245.12      TCP      54 33032 → 80 [ACK] Seq=463 Ack=4862 Win=59520 Len=0
 151 0.4488530…  172.20.10.12        128.119.245.12      HTTP     462 GET /favicon.ico HTTP/1.1
 152 0.9226433…  128.119.245.12      172.20.10.12        HTTP     538 HTTP/1.1 404 Not Found  (text/html)
 153 0.9634272…  172.20.10.12        128.119.245.12      TCP      54 33032 → 80 [ACK] Seq=871 Ack=5346 Win=58136 Len=0
```

```
› Frame 143: 516 bytes on wire (4128 bits), 516 bytes captured (4128 bits)
› Ethernet II, Src: Intel_82:e8:0d (c8:8a:9a:82:e8:0d), Dst: 9e:58:3c:e0:06:64 (9e:58:3c:e0:06:64)
› Internet Protocol Version 4, Src: 172.20.10.12, Dst: 128.119.245.12
› Transmission Control Protocol, Src Port: 33032, Dst Port: 80, Seq: 1, Ack: 1, Len: 462
› Hypertext Transfer Protocol
```

```
0000  9e 58 3c e0 06 64 c8 8a  9a 82 e8 0d 08 00 45 00   ·X<··d··
0010  01 f6 e9 15 40 00 40 06  24 48 ac 14 0a 0c 80 77   ····@·@·
0020  f5 0c 81 08 00 50 aa 80  22 ef c8 1b cf 98 50 18   ·····P··
0030  01 f6 2d 0d 00 00 47 45  54 20 2f 77 69 72 65 73   ··-···GE T /
0040  68 61 72 6b 2d 6c 61 62  73 2f 48 54 54 50 2d 77   hark-lab s/
0050  69 72 65 73 68 61 72 6b  2d 66 69 6c 65 33 2e 68   ireshark -
0060  74 6d 6c 20 48 54 54 50  2f 31 2e 31 0d 0a 48 6f   tml HTTP /
0070  73 74 3a 20 67 61 69 61  2e 63 73 2e 75 6d 61 73   st: gaia
0080  73 2e 65 64 75 0d 0a 43  6f 6e 6e 65 63 74 69 6f   s.edu  C
0090  6e 3a 20 6b 65 65 70 2d  61 6c 69 76 65 0d 0a 55   n: keep-
00a0  70 67 72 61 64 65 2d 49  6e 73 65 63 75 72 65 2d   pgrade-I
00b0  52 65 71 75 65 73 74 73  3a 20 31 0d 0a 55 73 65   Requests :
00c0  72 2d 41 67 65 6e 74 3a  20 4d 6f 7a 69 6c 6c 61   r-Agent:
00d0  2f 35 2e 30 20 28 58 31  31 3b 20 4c 69 6e 75 78   /5.0 (X1 1;
00e0  20 78 38 36 5f 36 34 29  20 41 70 70 6c 65 57 65    x86_64)
00f0  62 4b 69 74 2f 35 33 37  2e 33 36 20 28 4b 48 54   bKit/537 .36
0100  4d 4c 2c 20 6c 69 6b 65  20 47 65 63 6b 6f 29 20   ML, like
0110  43 68 72 6f 6d 65 2f 31  32 37 2e 30 2e 30 2e 30   Chrome/1
0120  20 53 61 66 61 72 69 2f  35 33 37 2e 33 36 0d 0a    Safari/
0130  41 63 63 65 70 74 3a 20  74 65 78 74 2f 68 74 6d   Accept:  text/
0140  6c 2c 61 70 70 6c 69 63  61 74 69 6f 6e 2f 78 68   l,applic
0150  74 6d 6c 2b 78 6d 6c 2c  61 70 70 6c 69 63 61 74   tml+xml,
0160  69 6f 6e 2f 78 6d 6c 3b  71 3d 30 2e 39 2c 69 6d   ion/xml;
0170  61 67 65 2f 61 76 69 66  2c 69 6d 61 67 65 2f 77   age/avif
```

Apply a display filter … <Ctrl-/>
assignment-1-part-2-q12-15.pcap
Packets: 153 · Displayed: 153 (100.0%) · Dropped: 0 (0.0%)
Profile: Default

Figure 8: Packet trace for retrieving long document

Q13

Packet number 149 in the trace contains the status code and phrase associated with the response of the HTTP GET request (ref. figure 8)

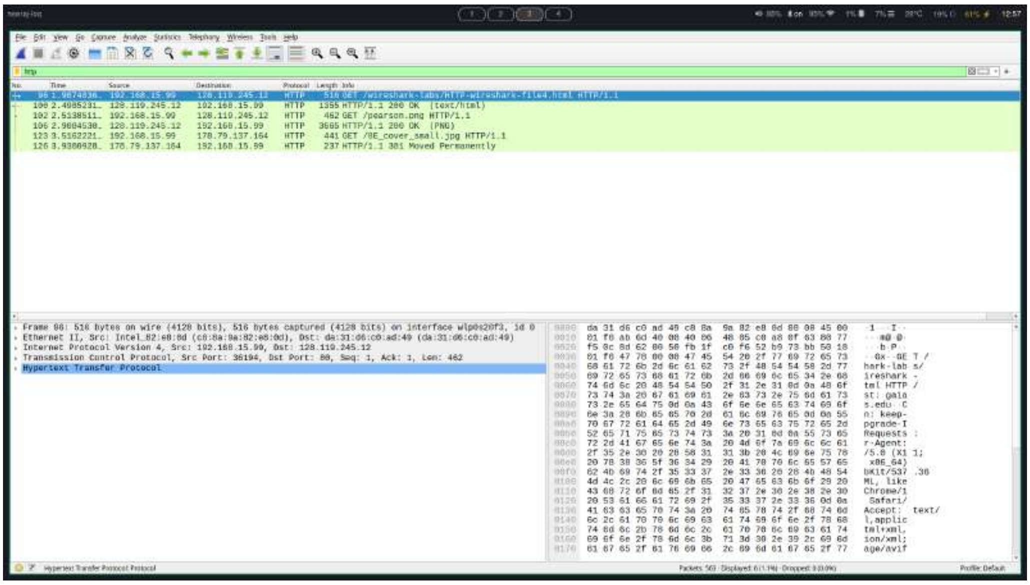
Q14

Status code and phrase is ”200 OK” as can be seen from packet number 149, from the figure 8

Q15

In total, 6 data containing TCP segments were needed to carry the single HTTP response and the text of Bill of Rights.
HTTP response is the packet number 149 in the figure 8.
The text containing the Bill of Rights is carried by 5 TCP segments, as can be seen from the packets 144 to 148 in the figure 8

Q16



```
No.    Time          Source            Destination       Protocol  Length Info
   96 1.9874836…  192.168.15.99     128.119.245.12    HTTP       516 GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
  100 2.4085231…  128.119.245.12    192.168.15.99     HTTP      1355 HTTP/1.1 200 OK  (text/html)
  102 2.5138511…  192.168.15.99     128.119.245.12    HTTP       462 GET /pearson.png HTTP/1.1
  106 2.9804530…  128.119.245.12    192.168.15.99     HTTP      3665 HTTP/1.1 200 OK  (PNG)
  123 3.5162221…  192.168.15.99     178.79.137.164    HTTP       441 GET /8E_cover_small.jpg HTTP/1.1
  126 3.9380928…  178.79.137.164    192.168.15.99     HTTP       237 HTTP/1.1 301 Moved Permanently
```

```
› Frame 96: 516 bytes on wire (4128 bits), 516 bytes captured (4128 bits) on interface wlp0s20f3, id 0
› Ethernet II, Src: Intel_82:e8:0d (c8:8a:9a:82:e8:0d), Dst: da:31:d6:c0:ad:49 (da:31:d6:c0:ad:49)
› Internet Protocol Version 4, Src: 192.168.15.99, Dst: 128.119.245.12
› Transmission Control Protocol, Src Port: 36194, Dst Port: 80, Seq: 1, Ack: 1, Len: 462
› Hypertext Transfer Protocol
```

```
0000  da 31 d6 c0 ad 49 c8 8a  9a 82 e8 0d 08 00 45 00   ·1···I··
0010  01 f6 ab 6d 40 00 40 06  48 05 c0 a8 0f 63 80 77   ···m@·@·
0020  f5 0c 8d 62 00 50 fb 1f  c0 f6 52 b9 73 bb 50 18   ···b·P··
0030  01 f6 47 78 00 00 47 45  54 20 2f 77 69 72 65 73   ··Gx··GE T /
0040  68 61 72 6b 2d 6c 61 62  73 2f 48 54 54 50 2d 77   hark-lab s/
0050  69 72 65 73 68 61 72 6b  2d 66 69 6c 65 34 2e 68   ireshark -
0060  74 6d 6c 20 48 54 54 50  2f 31 2e 31 0d 0a 48 6f   tml HTTP /
0070  73 74 3a 20 67 61 69 61  2e 63 73 2e 75 6d 61 73   st: gaia
0080  73 2e 65 64 75 0d 0a 43  6f 6e 6e 65 63 74 69 6f   s.edu··C
0090  6e 3a 20 6b 65 65 70 2d  61 6c 69 76 65 0d 0a 55   n: keep-
00a0  70 67 72 61 64 65 2d 49  6e 73 65 63 75 72 65 2d   pgrade-I
00b0  52 65 71 75 65 73 74 73  3a 20 31 0d 0a 55 73 65   Requests :
00c0  72 2d 41 67 65 6e 74 3a  20 4d 6f 7a 69 6c 6c 61   r-Agent:
00d0  2f 35 2e 30 20 28 58 31  31 3b 20 4c 69 6e 75 78   /5.0 (X1 1;
00e0  20 78 38 36 5f 36 34 29  20 41 70 70 6c 65 57 65    x86_64)
00f0  62 4b 69 74 2f 35 33 37  2e 33 36 20 28 4b 48 54   bKit/537 .36
0100  4d 4c 2c 20 6c 69 6b 65  20 47 65 63 6b 6f 29 20   ML, like
0110  43 68 72 6f 6d 65 2f 31  32 37 2e 30 2e 30 2e 30   Chrome/1
0120  20 53 61 66 61 72 69 2f  35 33 37 2e 33 36 0d 0a    Safari/
0130  41 63 63 65 70 74 3a 20  74 65 78 74 2f 68 74 6d   Accept:  text/
0140  6c 2c 61 70 70 6c 69 63  61 74 69 6f 6e 2f 78 68   l,applic
0150  74 6d 6c 2b 78 6d 6c 2c  61 70 70 6c 69 63 61 74   tml+xml,
0160  69 6f 6e 2f 78 6d 6c 3b  71 3d 30 2e 39 2c 69 6d   ion/xml;
0170  61 67 65 2f 61 76 69 66  2c 69 6d 61 67 65 2f 77   age/avif
```

Hypertext Transfer Protocol: Protocol

Packets: 563 · Displayed: 6 (1.1%) · Dropped: 0 (0.0%)

Profile: Default

Figure 9: Packet trace for HTML documents with embedded images

1. 3 HTTP GET requests were sent in total as can be seen from the packet trace in the figure 9 (Packet numbers 96, 102, 123)
2. (a) Packet number 96 is the first GET request to get the html document. Destination IP address is 128.119.245.12

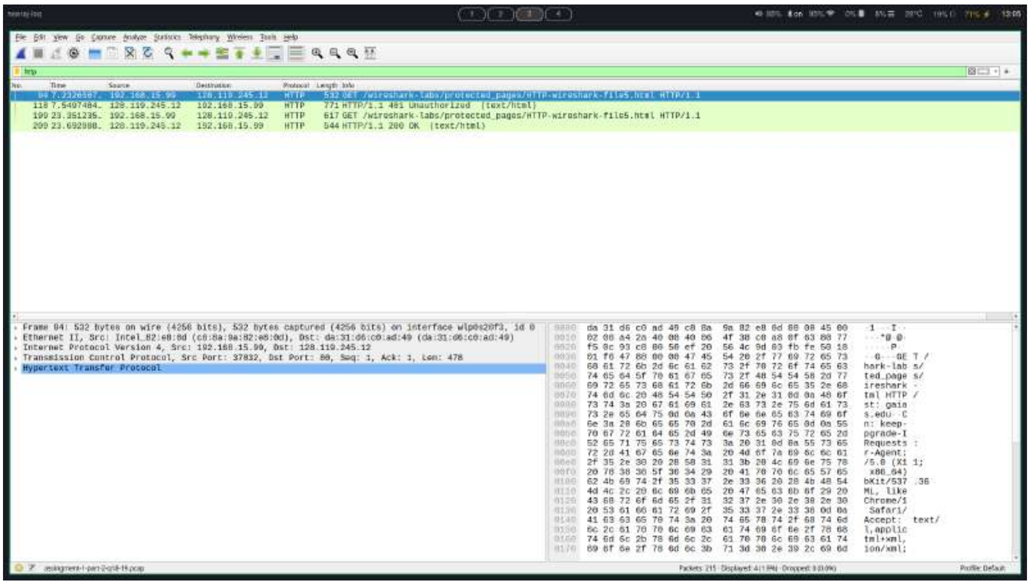
   (b) Packet number 102 is the second GET request to get the first embedded image (”pearson.png”) and the destination IP address is 128.119.145.12

   (c) Packet number 123 is the third GET request to get the second embedded image (”8E_cover_small.png”) and the destination IP address is 178.79.137.164

Q17

They were downloaded in serial becuase from the packet trace (in figure 9), we can see that after the GET request to the first image (packet number 102), the GET request for the second image (packet number 123) was sent only after the response for the first image (packet number 106).

Q18



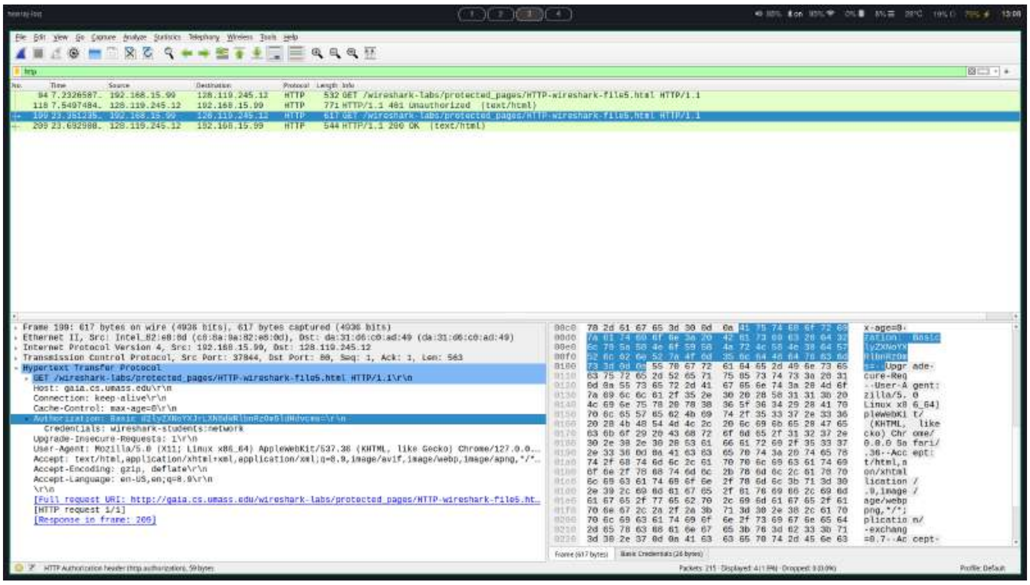
```
No.  Time         Source          Destination     Protocol Length Info
  94 7.2326587... 192.168.15.99   128.119.245.12  HTTP     532 GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
 118 7.5497484... 128.119.245.12  192.168.15.99   HTTP     771 HTTP/1.1 401 Unauthorized  (text/html)
 199 23.351235... 192.168.15.99   128.119.245.12  HTTP     617 GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
 209 23.692988... 128.119.245.12  192.168.15.99   HTTP     544 HTTP/1.1 200 OK  (text/html)
```

```
› Frame 94: 532 bytes on wire (4256 bits), 532 bytes captured (4256 bits) on interface wlp0s20f3, id 0
› Ethernet II, Src: Intel_82:e8:0d (c8:8a:9a:82:e8:0d), Dst: da:31:d6:c0:ad:49 (da:31:d6:c0:ad:49)
› Internet Protocol Version 4, Src: 192.168.15.99, Dst: 128.119.245.12
› Transmission Control Protocol, Src Port: 37832, Dst Port: 80, Seq: 1, Ack: 1, Len: 478
› Hypertext Transfer Protocol
```

Figure 10: Packet trace for HTTP Authentication

Initial GET request is packet number 94 in the packet trace shown in the figure 10, and initial response is packet number 118 in the figure 10. The status code and phrase is "401 Unauthorized" as shown in the packet listing window.

Q19



```
No.  Time         Source          Destination     Protocol Length Info
  94 7.2326587... 192.168.15.99   128.119.245.12  HTTP     532 GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
 118 7.5497484... 128.119.245.12  192.168.15.99   HTTP     771 HTTP/1.1 401 Unauthorized  (text/html)
 199 23.351235... 192.168.15.99   128.119.245.12  HTTP     617 GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
 209 23.692988... 128.119.245.12  192.168.15.99   HTTP     544 HTTP/1.1 200 OK  (text/html)
```

```
› Frame 199: 617 bytes on wire (4936 bits), 617 bytes captured (4936 bits)
› Ethernet II, Src: Intel_82:e8:0d (c8:8a:9a:82:e8:0d), Dst: da:31:d6:c0:ad:49 (da:31:d6:c0:ad:49)
› Internet Protocol Version 4, Src: 192.168.15.99, Dst: 128.119.245.12
› Transmission Control Protocol, Src Port: 37844, Dst Port: 80, Seq: 1, Ack: 1, Len: 563
⌄ 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 d2lyZXNoYXJrLXN0dWRlbnRzOm5ldHdvcms=\r\n
      Credentials: wireshark-students:network
    Upgrade-Insecure-Requests: 1\r\n
    User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/127.0.0...
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*...
    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.ht...
    [HTTP request 1/1]
    [Response in frame: 209]
```

HTTP Authorization header (http.authorization), 59 bytes

Figure 11: 2nd GET request for HTTP authentication

A new field named "Authorization" is added. as can be seen from the selected part in the figure 11.

```
Authorization: Basic d2lyZXNoYXJrLXN0dWRlbnRzOm5ldHdvcms=\r\n
    Credentials: wireshark-students:network
```