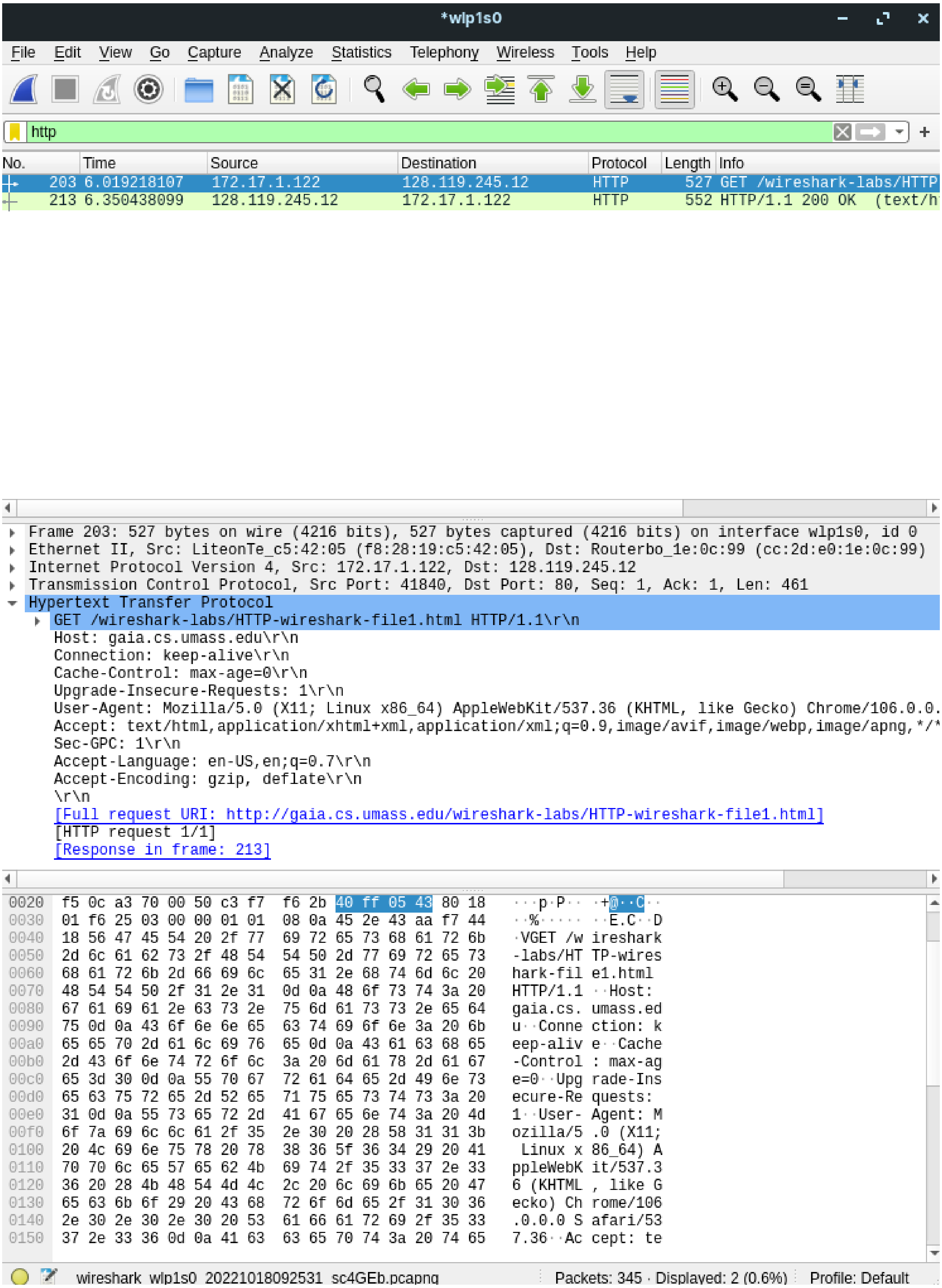
Lab Task 1:

The Basic HTTP GET/response interaction.


*wlp1s0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http

```
No.    Time         Source          Destination      Protocol  Length Info
203 6.019218107    172.17.1.122    128.119.245.12   HTTP       527 GET /wireshark-labs/HTTP
213 6.350438099    128.119.245.12  172.17.1.122     HTTP       552 HTTP/1.1 200 OK  (text/h
```

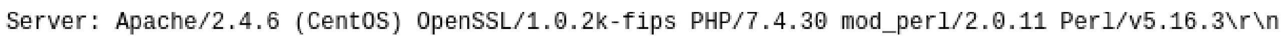
```
▸ Frame 203: 527 bytes on wire (4216 bits), 527 bytes captured (4216 bits) on interface wlp1s0, id 0
▸ Ethernet II, Src: LiteonTe_c5:42:05 (f8:28:19:c5:42:05), Dst: Routerbo_1e:0c:99 (cc:2d:e0:1e:0c:99)
▸ Internet Protocol Version 4, Src: 172.17.1.122, Dst: 128.119.245.12
▸ Transmission Control Protocol, Src Port: 41840, Dst Port: 80, Seq: 1, Ack: 1, Len: 461
▾ 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
     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/106.0.0.
     Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*
     Sec-GPC: 1\r\n
     Accept-Language: en-US,en;q=0.7\r\n
     Accept-Encoding: gzip, deflate\r\n
     \r\n
     [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html]
     [HTTP request 1/1]
     [Response in frame: 213]
```

```
0020  f5 0c a3 70 00 50 c3 f7  f6 2b 40 ff 05 43 80 18   ···p·P·· ·+@··C··
0030  01 f6 25 03 00 00 01 01  08 0a 45 2e 43 aa f7 44   ··%····· ··E.C··D
0040  18 56 47 45 54 20 2f 77  69 72 65 73 68 61 72 6b   ·VGET /w ireshark
0050  2d 6c 61 62 73 2f 48 54  54 50 2d 77 69 72 65 73   -labs/HT TP-wires
0060  68 61 72 6b 2d 66 69 6c  65 31 2e 68 74 6d 6c 20   hark-fil e1.html
0070  48 54 54 50 2f 31 2e 31  0d 0a 48 6f 73 74 3a 20   HTTP/1.1 ··Host:
0080  67 61 69 61 2e 63 73 2e  75 6d 61 73 73 2e 65 64   gaia.cs. umass.ed
0090  75 0d 0a 43 6f 6e 6e 65  63 74 69 6f 6e 3a 20 6b   u··Conne ction: k
00a0  65 65 70 2d 61 6c 69 76  65 0d 0a 43 61 63 68 65   eep-aliv e··Cache
00b0  2d 43 6f 6e 74 72 6f 6c  3a 20 6d 61 78 2d 61 67   -Control : max-ag
00c0  65 3d 30 0d 0a 55 70 67  72 61 64 65 2d 49 6e 73   e=0··Upg rade-Ins
00d0  65 63 75 72 65 2d 52 65  71 75 65 73 74 73 3a 20   ecure-Re quests:
00e0  31 0d 0a 55 73 65 72 2d  41 67 65 6e 74 3a 20 4d   1··User- Agent: M
00f0  6f 7a 69 6c 6c 61 2f 35  2e 30 20 28 58 31 31 3b   ozilla/5 .0 (X11;
0100  20 4c 69 6e 75 78 20 78  38 36 5f 36 34 29 20 41    Linux x 86_64) A
0110  70 70 6c 65 57 65 62 4b  69 74 2f 35 33 37 2e 33   ppleWebK it/537.3
0120  36 20 28 4b 48 54 4d 4c  2c 20 6c 69 6b 65 20 47   6 (KHTML , like G
0130  65 63 6b 6f 29 20 43 68  72 6f 6d 65 2f 31 30 36   ecko) Ch rome/106
0140  2e 30 2e 30 2e 30 20 53  61 66 61 72 69 2f 35 33   .0.0.0 S afari/53
0150  37 2e 33 36 0d 0a 41 63  63 65 70 74 3a 20 74 65   7.36··Ac cept: te
```

wireshark wlp1s0 20221018092531 sc4GEb.pcapng · Packets: 345 · Displayed: 2 (0.6%) · Profile: Default

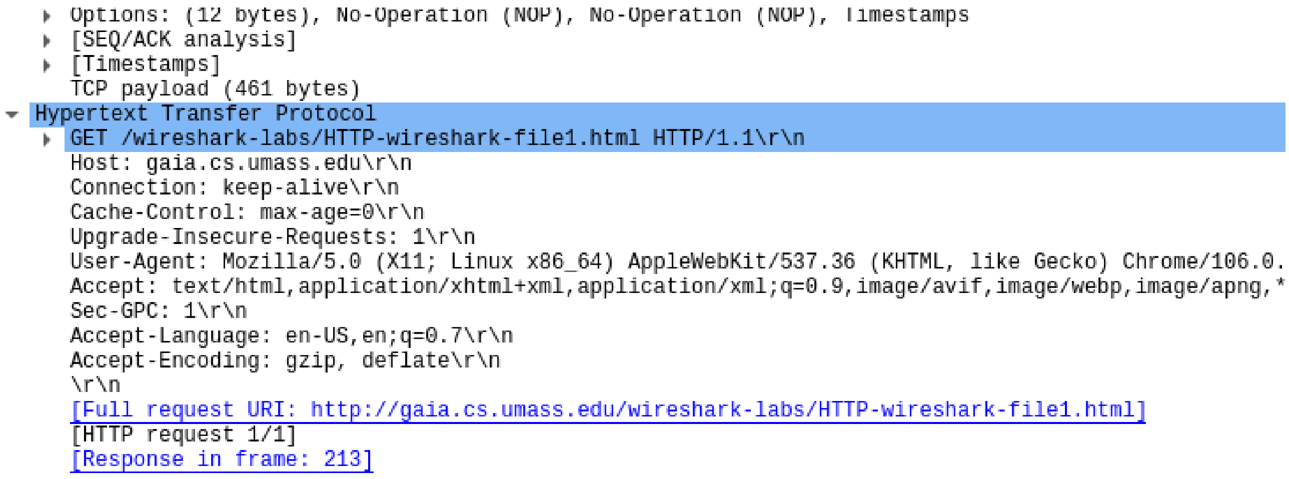
Answers:

1. Browser running HTTP version 1.1.
2. The server version is:



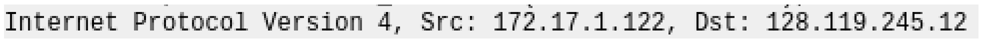
```
Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.30 mod_perl/2.0.11 Perl/v5.16.3\r\n
```

3. Accept Language is: “en-US, en;1=0.7\r\n”



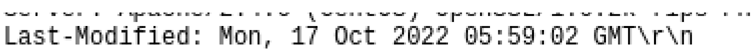
```
  ▸ Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
  ▸ [SEQ/ACK analysis]
  ▸ [Timestamps]
    TCP payload (461 bytes)
▾ Hypertext Transfer Protocol
  ▸ GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n
    Host: gaia.cs.umass.edu\r\n
    Connection: keep-alive\r\n
    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/106.0.
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*
    Sec-GPC: 1\r\n
    Accept-Language: en-US,en;q=0.7\r\n
    Accept-Encoding: gzip, deflate\r\n
    \r\n
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html]
    [HTTP request 1/1]
    [Response in frame: 213]
```

4. My machine IP is: 172.17.1.122
   The server’s IP address is: 127.119.245.12



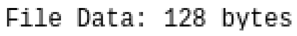
```
Internet Protocol Version 4, Src: 172.17.1.122, Dst: 128.119.245.12
```

5. Status code is: 200
6. Last modified time is:



```
Last-Modified: Mon, 17 Oct 2022 05:59:02 GMT\r\n
```

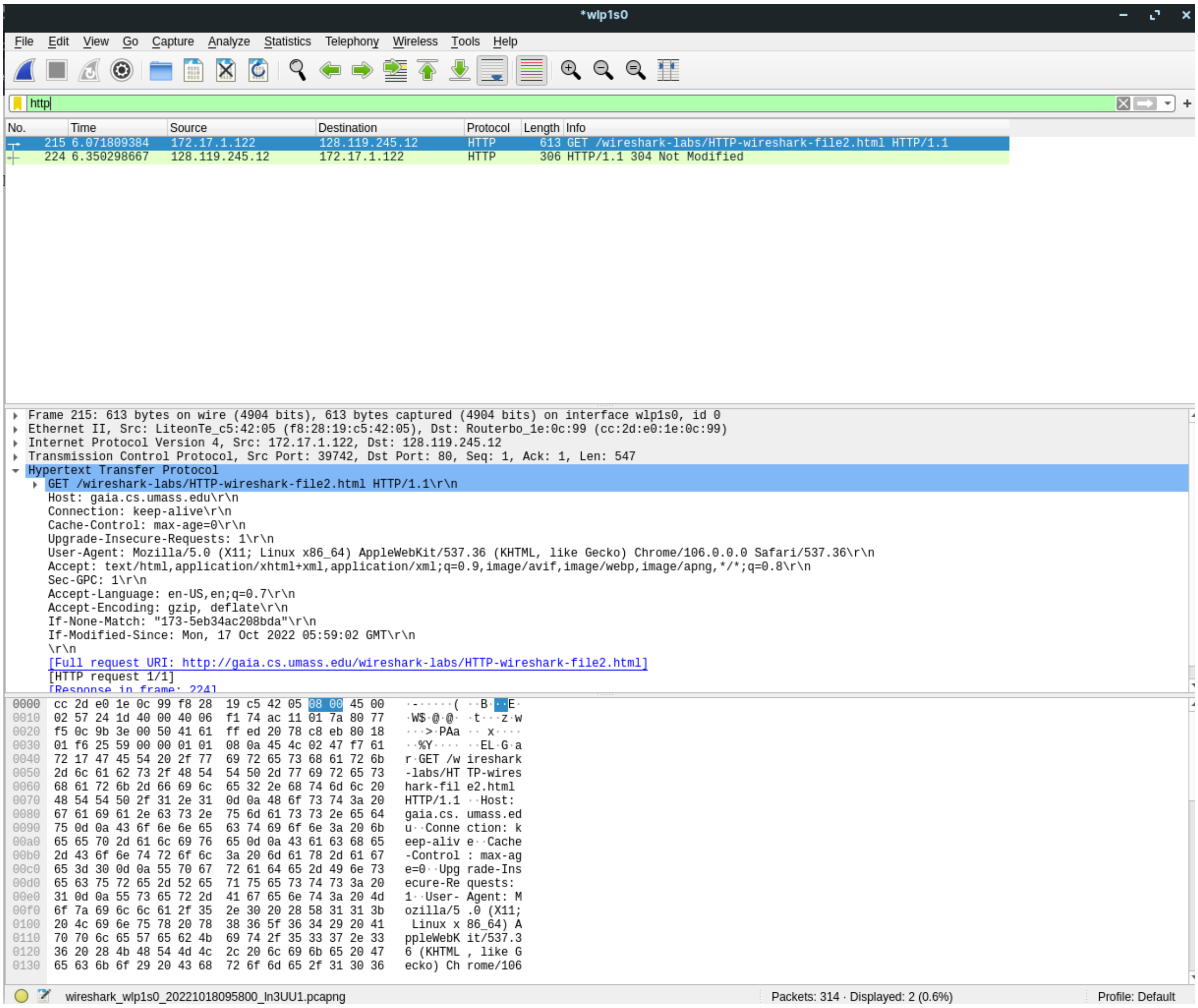
7. Bytes size is:



```
File Data: 128 bytes
```

8. No all of the headers can be found in the raw data.

Task 02:



*wlp1s0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
http
```

```
No.   Time          Source           Destination      Protocol  Length Info
  215 6.071809384   172.17.1.122     128.119.245.12   HTTP         613 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
  224 6.350298667   128.119.245.12   172.17.1.122     HTTP         306 HTTP/1.1 304 Not Modified
```

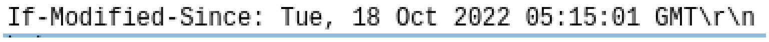
```
▸ Frame 215: 613 bytes on wire (4904 bits), 613 bytes captured (4904 bits) on interface wlp1s0, id 0
▸ Ethernet II, Src: LiteonTe_c5:42:05 (f8:28:19:c5:42:05), Dst: Routerbo_1e:0c:99 (cc:2d:e0:1e:0c:99)
▸ Internet Protocol Version 4, Src: 172.17.1.122, Dst: 128.119.245.12
▸ Transmission Control Protocol, Src Port: 39742, Dst Port: 80, Seq: 1, Ack: 1, Len: 547
▾ 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/106.0.0.0 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\r\n
    Sec-GPC: 1\r\n
    Accept-Language: en-US,en;q=0.7\r\n
    Accept-Encoding: gzip, deflate\r\n
    If-None-Match: "173-5eb34ac208bda"\r\n
    If-Modified-Since: Mon, 17 Oct 2022 05:59:02 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: 224]
```

```
0000  cc 2d e0 1e 0c 99 f8 28  19 c5 42 05 08 00 45 00   ·-·····( ··B···E·
0010  02 57 24 1d 40 00 40 06  f1 74 ac 11 01 7a 80 77   ·W$·@·@· ·t···z·w
0020  f5 0c 9b 3e 00 50 41 61  ff ed 20 78 c8 eb 80 18   ···>·PAa ·· x····
0030  01 f6 25 59 00 00 01 01  08 0a 45 4c 02 47 f7 61   ··%Y···· ··EL·G·a
0040  72 17 47 45 54 20 2f 77  69 72 65 73 68 61 72 6b   r·GET /w ireshark
0050  2d 6c 61 62 73 2f 48 54  54 50 2d 77 69 72 65 73   -labs/HT TP-wires
0060  68 61 72 6b 2d 66 69 6c  65 32 2e 68 74 6d 6c 20   hark-fil e2.html
0070  48 54 54 50 2f 31 2e 31  0d 0a 48 6f 73 74 3a 20   HTTP/1.1 ··Host:
0080  67 61 69 61 2e 63 73 2e  75 6d 61 73 73 2e 65 64   gaia.cs. umass.ed
0090  75 0d 0a 43 6f 6e 6e 65  63 74 69 6f 6e 3a 20 6b   u··Conne ction: k
00a0  65 65 70 2d 61 6c 69 76  65 0d 0a 43 61 63 68 65   eep-aliv e··Cache
00b0  2d 43 6f 6e 74 72 6f 6c  3a 20 6d 61 78 2d 61 67   -Control : max-ag
00c0  65 3d 30 0d 0a 55 70 67  72 61 64 65 2d 49 6e 73   e=0··Upg rade-Ins
00d0  65 63 75 72 65 2d 52 65  71 75 65 73 74 73 3a 20   ecure-Re quests:
00e0  31 0d 0a 55 73 65 72 2d  41 67 65 6e 74 3a 20 4d   1··User- Agent: M
00f0  6f 7a 69 6c 6c 61 2f 35  2e 30 20 28 58 31 31 3b   ozilla/5 .0 (X11;
0100  20 4c 69 6e 75 78 20 78  38 36 5f 36 34 29 20 41    Linux x 86_64) A
0110  70 70 6c 65 57 65 62 4b  69 74 2f 35 33 37 2e 33   ppleWebK it/537.3
0120  36 20 28 4b 48 54 4d 4c  2c 20 6c 69 6b 65 20 47   6 (KHTML , like G
0130  65 63 6b 6f 29 20 43 68  72 6f 6d 65 2f 31 30 36   ecko) Ch rome/106
```

```
wireshark_wlp1s0_20221018095800_ln3UU1.pcapng     Packets: 314 · Displayed: 2 (0.6%)     Profile: Default
```

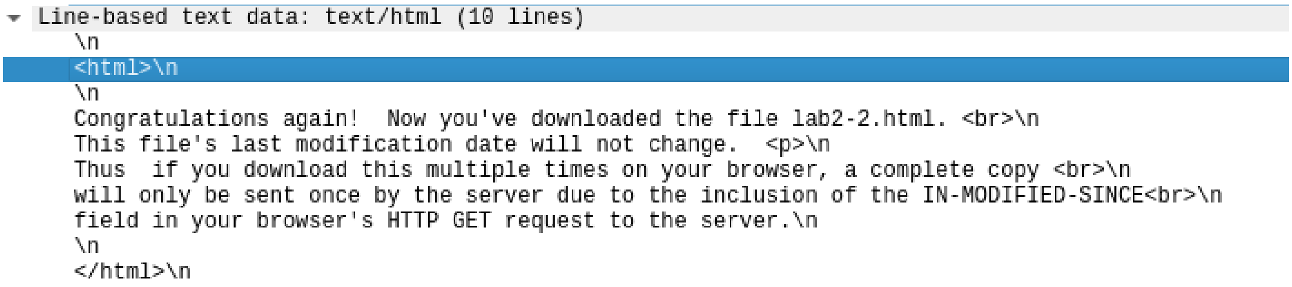
Answers:

1. No, it’s not showing in 200,OK response.



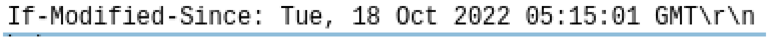
```
If-Modified-Since: Tue, 18 Oct 2022 05:15:01 GMT\r\n
```

2. Yes, the server explicitly returns the contents of the file.



```
▾ 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
```

3. Yess, it’s showing:



```
If-Modified-Since: Tue, 18 Oct 2022 05:15:01 GMT\r\n
```

4. 304 Not modified is the code and it does not explicitly returns the content of the file.