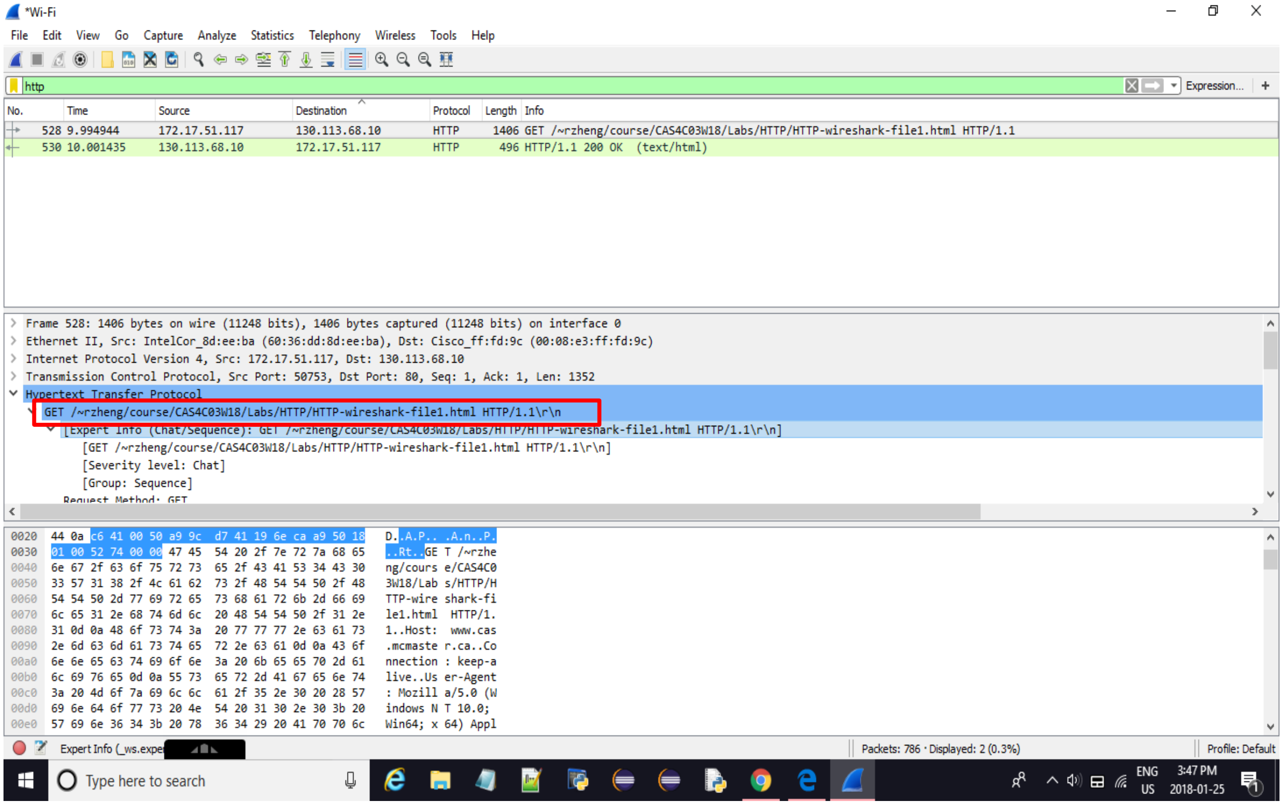
Wireshark Lab 1

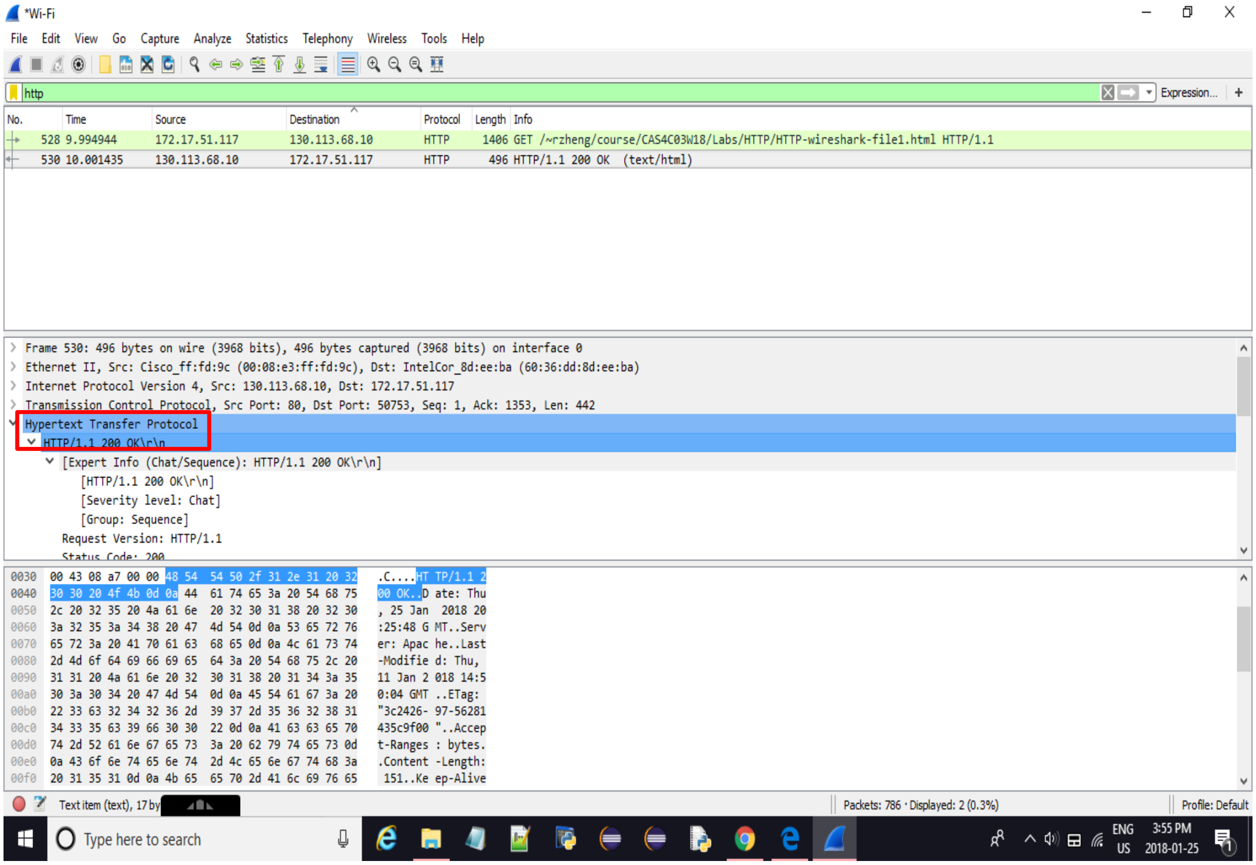
1.



*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expression...
+

```
http

No.  Time       Source         Destination    Protocol Length Info
 528 9.994944   172.17.51.117  130.113.68.10  HTTP     1406 GET /~rzheng/course/CAS4C03W18/Labs/HTTP/HTTP-wireshark-file1.html HTTP/1.1
 530 10.001435  130.113.68.10  172.17.51.117  HTTP      496 HTTP/1.1 200 OK  (text/html)

> Frame 528: 1406 bytes on wire (11248 bits), 1406 bytes captured (11248 bits) on interface 0
> Ethernet II, Src: IntelCor_8d:ee:ba (60:36:dd:8d:ee:ba), Dst: Cisco_ff:fd:9c (00:08:e3:ff:fd:9c)
> Internet Protocol Version 4, Src: 172.17.51.117, Dst: 130.113.68.10
> Transmission Control Protocol, Src Port: 50753, Dst Port: 80, Seq: 1, Ack: 1, Len: 1352
v Hypertext Transfer Protocol
  v GET /~rzheng/course/CAS4C03W18/Labs/HTTP/HTTP-wireshark-file1.html HTTP/1.1\r\n
    v [Expert Info (Chat/Sequence): GET /~rzheng/course/CAS4C03W18/Labs/HTTP/HTTP-wireshark-file1.html HTTP/1.1\r\n]
        [GET /~rzheng/course/CAS4C03W18/Labs/HTTP/HTTP-wireshark-file1.html HTTP/1.1\r\n]
        [Severity level: Chat]
        [Group: Sequence]
      Request Method: GET

0020  44 0a c6 41 00 50 a9 9c  d7 41 19 6e ca a9 50 18   D..A.P.. .A.n..P.
0030  01 00 52 74 00 00 47 45  54 20 2f 7e 72 7a 68 65   ..Rt..GE T /~rzhe
0040  6e 67 2f 63 6f 75 72 73  65 2f 43 41 53 34 43 30   ng/cours e/CAS4C0
0050  33 57 31 38 2f 4c 61 62  73 2f 48 54 54 50 2f 48   3W18/Lab s/HTTP/H
0060  54 54 50 2d 77 69 72 65  73 68 61 72 6b 2d 66 69   TTP-wire shark-fi
0070  6c 65 31 2e 68 74 6d 6c  20 48 54 54 50 2f 31 2e   le1.html  HTTP/1.
0080  31 0d 0a 48 6f 73 74 3a  20 77 77 77 2e 63 61 73   1..Host:  www.cas
0090  2e 6d 63 6d 61 73 74 65  72 2e 63 61 0d 0a 43 6f   .mcmaste r.ca..Co
00a0  6e 6e 65 63 74 69 6f 6e  3a 20 6b 65 65 70 2d 61   nnection : keep-a
00b0  6c 69 76 65 0d 0a 55 73  65 72 2d 41 67 65 6e 74   live..Us er-Agent
00c0  3a 20 4d 6f 7a 69 6c 6c  61 2f 35 2e 30 20 28 57   : Mozill a/5.0 (W
00d0  69 6e 64 6f 77 73 20 4e  54 20 31 30 2e 30 3b 20   indows N T 10.0;
00e0  57 69 6e 36 34 3b 20 78  36 34 29 20 41 70 70 6c   Win64; x 64) Appl

Expert Info (_ws.expe[redacted]          Packets: 786 · Displayed: 2 (0.3%)          Profile: Default
```

The browser is running HTTP version 1.1



*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expression... +

```
http
```

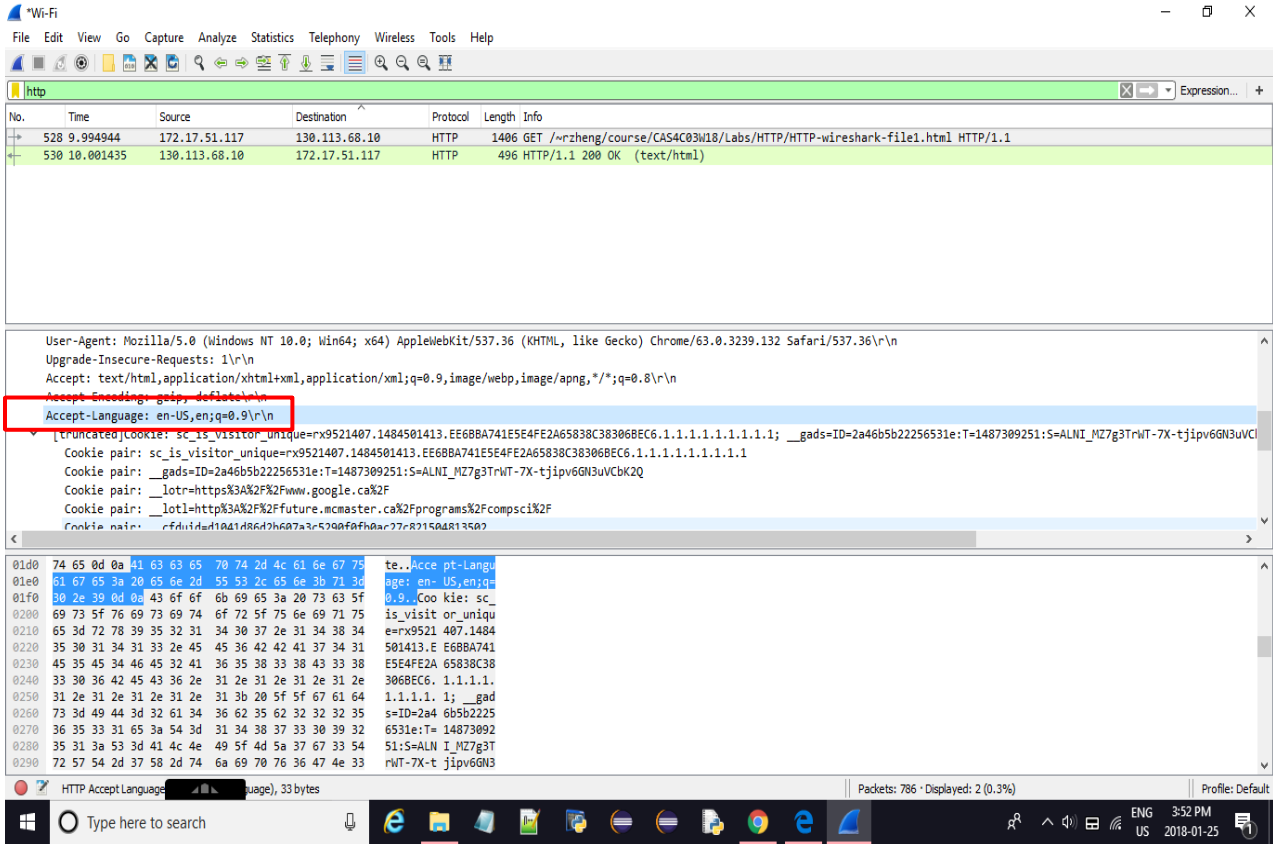
```
No.   Time        Source          Destination     Protocol  Length  Info
  528 9.994944    172.17.51.117   130.113.68.10   HTTP       1406 GET /~rzheng/course/CAS4C03W18/Labs/HTTP/HTTP-wireshark-file1.html HTTP/1.1
  530 10.001435   130.113.68.10   172.17.51.117   HTTP        496 HTTP/1.1 200 OK  (text/html)
```

```
> Frame 530: 496 bytes on wire (3968 bits), 496 bytes captured (3968 bits) on interface 0
> Ethernet II, Src: Cisco_ff:fd:9c (00:08:e3:ff:fd:9c), Dst: IntelCor_8d:ee:ba (60:36:dd:8d:ee:ba)
> Internet Protocol Version 4, Src: 130.113.68.10, Dst: 172.17.51.117
> Transmission Control Protocol, Src Port: 80, Dst Port: 50753, Seq: 1, Ack: 1353, Len: 442
v Hypertext Transfer Protocol
  v HTTP/1.1 200 OK\r\n
    v [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
        [HTTP/1.1 200 OK\r\n]
        [Severity level: Chat]
        [Group: Sequence]
      Request Version: HTTP/1.1
      Status Code: 200
```

```
0030  00 43 08 a7 00 00 48 54  54 50 2f 31 2e 31 20 32   .C....HT TP/1.1 2
0040  30 30 20 4f 4b 0d 0a 44  61 74 65 3a 20 54 68 75   00 OK..D ate: Thu
0050  2c 20 32 35 20 4a 61 6e  20 32 30 31 38 20 32 30   , 25 Jan  2018 20
0060  3a 32 35 3a 34 38 20 47  4d 54 0d 0a 53 65 72 76   :25:48 G MT..Serv
0070  65 72 3a 20 41 70 61 63  68 65 0d 0a 4c 61 73 74   er: Apac he..Last
0080  2d 4d 6f 64 69 66 69 65  64 3a 20 54 68 75 2c 20   -Modifie d: Thu,
0090  31 31 20 4a 61 6e 20 32  30 31 38 20 31 34 3a 35   11 Jan 2 018 14:5
00a0  30 3a 30 34 20 47 4d 54  0d 0a 45 54 61 67 3a 20   0:04 GMT ..ETag:
00b0  22 33 63 32 34 32 36 2d  39 37 2d 35 36 32 38 31   "3c2426- 97-56281
00c0  34 33 35 63 39 66 30 30  22 0d 0a 41 63 63 65 70   435c9f00 "..Accep
00d0  74 2d 52 61 6e 67 65 73  3a 20 62 79 74 65 73 0d   t-Ranges : bytes.
00e0  0a 43 6f 6e 74 65 6e 74  2d 4c 65 6e 67 74 68 3a   .Content -Length:
00f0  20 31 35 31 0d 0a 4b 65  65 70 2d 41 6c 69 76 65    151..Ke ep-Alive
```

The server is running HTTP version 1.1

2.



*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
Expression...

```
No.   Time       Source          Destination     Protocol  Length Info
  528 9.994944   172.17.51.117   130.113.68.10   HTTP        1406 GET /~rzheng/course/CAS4C03W18/Labs/HTTP/HTTP-wireshark-file1.html HTTP/1.1
  530 10.001435  130.113.68.10   172.17.51.117   HTTP         496 HTTP/1.1 200 OK  (text/html)
```

```
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/63.0.3239.132 Safari/537.36\r\n
    Upgrade-Insecure-Requests: 1\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8\r\n
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: en-US,en;q=0.9\r\n
  v [truncated]Cookie: sc_is_visitor_unique=rx9521407.1484501413.EE6BBA741E5E4FE2A65838C38306BEC6.1.1.1.1.1.1.1.1.1; __gads=ID=2a46b5b22256531e:T=1487309251:S=ALNI_MZ7g3TrWT-7X-tjipv6GN3uVCl
      Cookie pair: sc_is_visitor_unique=rx9521407.1484501413.EE6BBA741E5E4FE2A65838C38306BEC6.1.1.1.1.1.1.1.1.1
      Cookie pair: __gads=ID=2a46b5b22256531e:T=1487309251:S=ALNI_MZ7g3TrWT-7X-tjipv6GN3uVCbK2Q
      Cookie pair: __lotr=https%3A%2F%2Fwww.google.ca%2F
      Cookie pair: __lotl=http%3A%2F%2Ffuture.mcmaster.ca%2Fprograms%2Fcompsci%2F
      Cookie pair: __cfduid=d1041d86d2b607a3c5290f0fb0ac27c821504813502
```

```
01d0  74 65 0d 0a 41 63 63 65  70 74 2d 4c 61 6e 67 75   te..Acce pt-Langu
01e0  61 67 65 3a 20 65 6e 2d  55 53 2c 65 6e 3b 71 3d   age: en- US,en;q=
01f0  30 2e 39 0d 0a 43 6f 6f  6b 69 65 3a 20 73 63 5f   0.9..Coo kie: sc_
0200  69 73 5f 76 69 73 69 74  6f 72 5f 75 6e 69 71 75   is_visit or_uniqu
0210  65 3d 72 78 39 35 32 31  34 30 37 2e 31 34 38 34   e=rx9521 407.1484
0220  35 30 31 34 31 33 2e 45  45 36 42 42 41 37 34 31   501413.E E6BBA741
0230  45 35 45 34 46 45 32 41  36 35 38 33 38 43 33 38   E5E4FE2A 65838C38
0240  33 30 36 42 45 43 36 2e  31 2e 31 2e 31 2e 31 2e   306BEC6. 1.1.1.1.
0250  31 2e 31 2e 31 2e 31 2e  31 3b 20 5f 5f 67 61 64   1.1.1.1. 1; __gad
0260  73 3d 49 44 3d 32 61 34  36 62 35 62 32 32 32 35   s=ID=2a4 6b5b2225
0270  36 35 33 31 65 3a 54 3d  31 34 38 37 33 30 39 32   6531e:T= 14873092
0280  35 31 3a 53 3d 41 4c 4e  49 5f 4d 5a 37 67 33 54   51:S=ALN I_MZ7g3T
0290  72 57 54 2d 37 58 2d 74  6a 69 70 76 36 47 4e 33   rWT-7X-t jipv6GN3
```

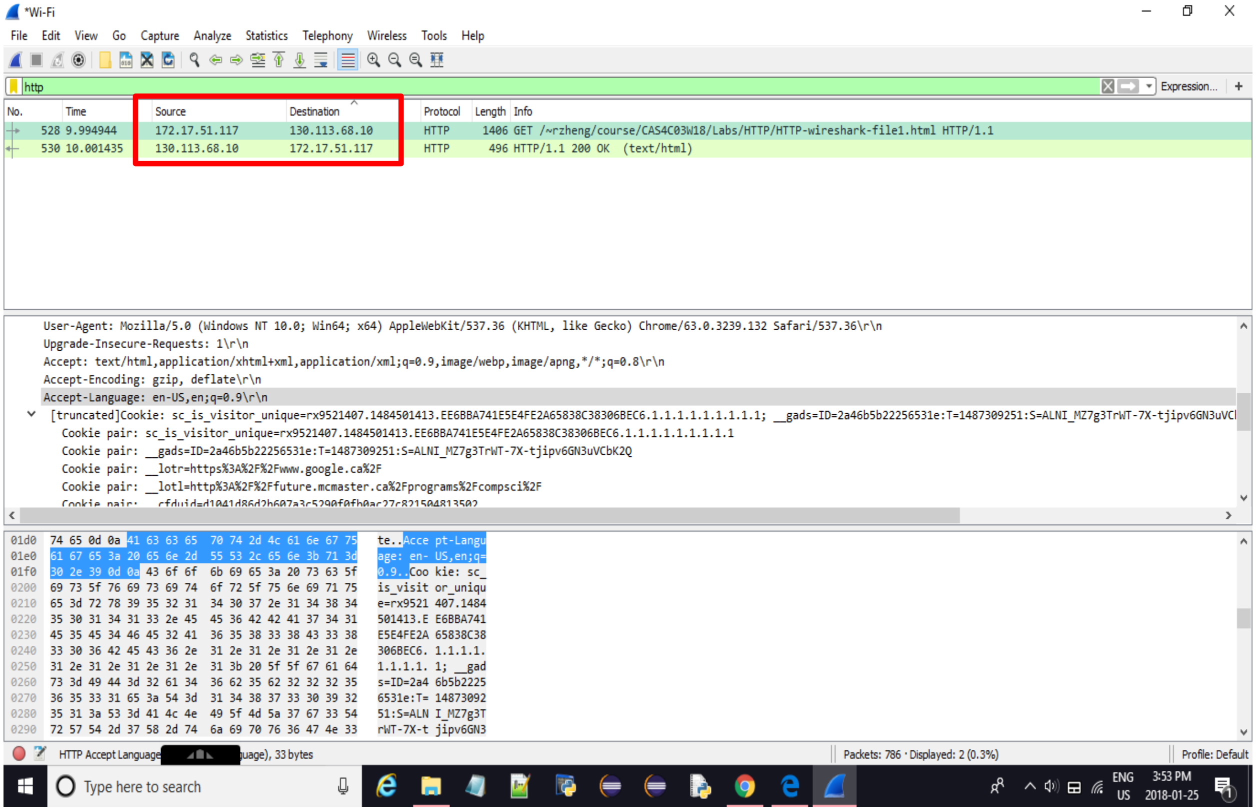
HTTP Accept Language[redacted]uage), 33 bytes

Packets: 786 · Displayed: 2 (0.3%)

Profile: Default

The language accepted: en-US, en;q=0.9\r\n

3.



*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
Expression...
+

```
No.  Time        Source         Destination    Protocol Length Info
528  9.994944    172.17.51.117  130.113.68.10  HTTP     1406   GET /~rzheng/course/CAS4C03W18/Labs/HTTP/HTTP-wireshark-file1.html HTTP/1.1
530  10.001435   130.113.68.10  172.17.51.117  HTTP      496   HTTP/1.1 200 OK  (text/html)
```

```
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/63.0.3239.132 Safari/537.36\r\n
    Upgrade-Insecure-Requests: 1\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8\r\n
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: en-US,en;q=0.9\r\n
  ˅ [truncated]Cookie: sc_is_visitor_unique=rx9521407.1484501413.EE6BBA741E5E4FE2A65838C38306BEC6.1.1.1.1.1.1.1.1.1; __gads=ID=2a46b5b22256531e:T=1487309251:S=ALNI_MZ7g3TrWT-7X-tjipv6GN3uVCl
      Cookie pair: sc_is_visitor_unique=rx9521407.1484501413.EE6BBA741E5E4FE2A65838C38306BEC6.1.1.1.1.1.1.1.1.1
      Cookie pair: __gads=ID=2a46b5b22256531e:T=1487309251:S=ALNI_MZ7g3TrWT-7X-tjipv6GN3uVCbK2Q
      Cookie pair: __lotr=https%3A%2F%2Fwww.google.ca%2F
      Cookie pair: __lotl=http%3A%2F%2Ffuture.mcmaster.ca%2Fprograms%2Fcompsci%2F
      Cookie pair: __cfduid=d1041d86d2b607a3c5290f0fb0ac27c821504813502
```

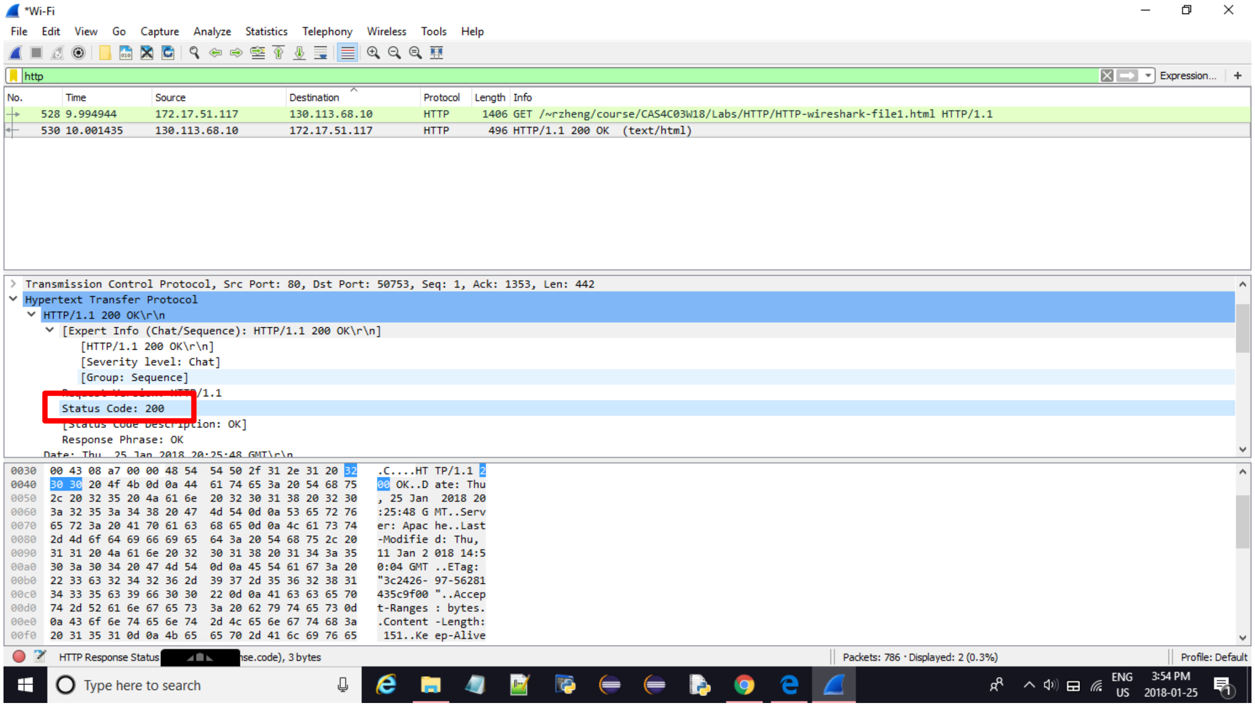
```
01d0  74 65 0d 0a 41 63 63 65  70 74 2d 4c 61 6e 67 75   te..Acce pt-Langu
01e0  61 67 65 3a 20 65 6e 2d  55 53 2c 65 6e 3b 71 3d   age: en- US,en;q=
01f0  30 2e 39 0d 0a 43 6f 6f  6b 69 65 3a 20 73 63 5f   0.9..Coo kie: sc_
0200  69 73 5f 76 69 73 69 74  6f 72 5f 75 6e 69 71 75   is_visit or_uniqu
0210  65 3d 72 78 39 35 32 31  34 30 37 2e 31 34 38 34   e=rx9521 407.1484
0220  35 30 31 34 31 33 2e 45  45 36 42 42 41 37 34 31   501413.E E6BBA741
0230  45 35 45 34 46 45 32 41  36 35 38 33 38 43 33 38   E5E4FE2A 65838C38
0240  33 30 36 42 45 43 36 2e  31 2e 31 2e 31 2e 31 2e   306BEC6. 1.1.1.1.
0250  31 2e 31 2e 31 2e 31 2e  31 3b 20 5f 5f 67 61 64   1.1.1.1. 1; __gad
0260  73 3d 49 44 3d 32 61 34  36 62 35 62 32 32 32 35   s=ID=2a4 6b5b2225
0270  36 35 33 31 65 3a 54 3d  31 34 38 37 33 30 39 32   6531e:T= 14873092
0280  35 31 3a 53 3d 41 4c 4e  49 5f 4d 5a 37 67 33 54   51:S=ALN I_MZ7g3T
0290  72 57 54 2d 37 58 2d 74  6a 69 70 76 36 47 4e 33   rWT-7X-t jipv6GN3
```

HTTP Accept Language [redacted] uage), 33 bytes | Packets: 786 · Displayed: 2 (0.3%) | Profile: Default

The IP address of my computer is 172.17.51.117

The IP address of www.cas.mcmaster.ca server is 130.113.68.10

4.



*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
Expression… +

```
No.    Time        Source         Destination    Protocol  Length Info
  528 9.994944    172.17.51.117  130.113.68.10  HTTP      1406 GET /~rzheng/course/CAS4C03W18/Labs/HTTP/HTTP-wireshark-file1.html HTTP/1.1
  530 10.001435   130.113.68.10  172.17.51.117  HTTP       496 HTTP/1.1 200 OK  (text/html)
```

```
> Transmission Control Protocol, Src Port: 80, Dst Port: 50753, Seq: 1, Ack: 1353, Len: 442
v Hypertext Transfer Protocol
  v HTTP/1.1 200 OK\r\n
    v [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
        [HTTP/1.1 200 OK\r\n]
        [Severity level: Chat]
        [Group: Sequence]
      Request Version: HTTP/1.1
      Status Code: 200
      [Status Code Description: OK]
      Response Phrase: OK
    Date: Thu, 25 Jan 2018 20:25:48 GMT\r\n
```

```
0030  00 43 08 a7 00 00 48 54  54 50 2f 31 2e 31 20 32   .C....HT TP/1.1 2
0040  30 30 20 4f 4b 0d 0a 44  61 74 65 3a 20 54 68 75   00 OK..D ate: Thu
0050  2c 20 32 35 20 4a 61 6e  20 32 30 31 38 20 32 30   , 25 Jan  2018 20
0060  3a 32 35 3a 34 38 20 47  4d 54 0d 0a 53 65 72 76   :25:48 G MT..Serv
0070  65 72 3a 20 41 70 61 63  68 65 0d 0a 4c 61 73 74   er: Apac he..Last
0080  2d 4d 6f 64 69 66 69 65  64 3a 20 54 68 75 2c 20   -Modifie d: Thu,
0090  31 31 20 4a 61 6e 20 32  30 31 38 20 31 34 3a 35   11 Jan 2 018 14:5
00a0  30 3a 30 34 20 47 4d 54  0d 0a 45 54 61 67 3a 20   0:04 GMT ..ETag:
00b0  22 33 63 32 34 32 36 2d  39 37 2d 35 36 32 38 31   "3c2426- 97-56281
00c0  34 33 35 63 39 66 30 30  22 0d 0a 41 63 63 65 70   435c9f00 "..Accep
00d0  74 2d 52 61 6e 67 65 73  3a 20 62 79 74 65 73 0d   t-Ranges : bytes.
00e0  0a 43 6f 6e 74 65 6e 74  2d 4c 65 6e 67 74 68 3a   .Content -Length:
00f0  20 31 35 31 0d 0a 4b 65  65 70 2d 41 6c 69 76 65    151..Ke ep-Alive
```

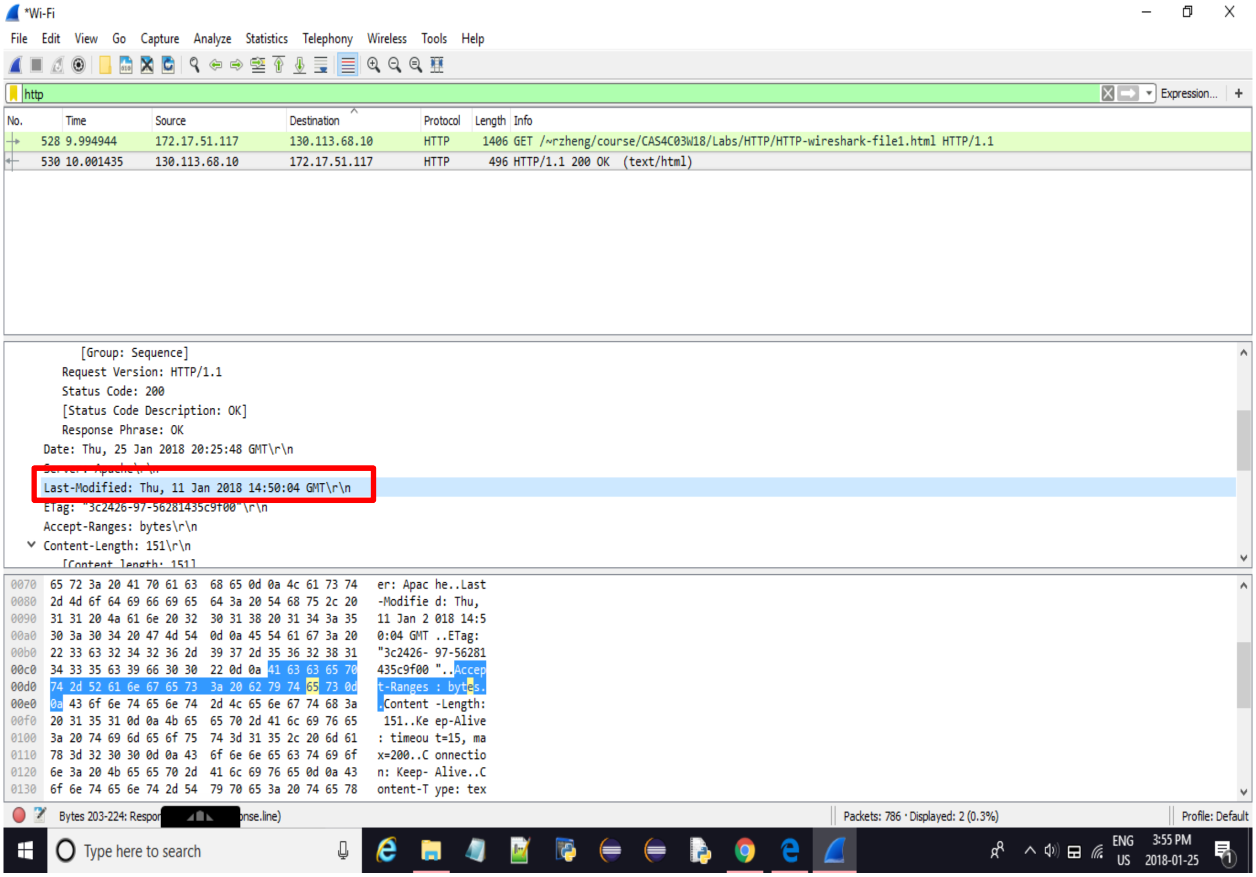
HTTP Response Status [redacted] se.code), 3 bytes

Packets: 786 · Displayed: 2 (0.3%)

Profile: Default

Status code: 200

5.


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
Expression...
+
Type here to search
ENG
US
3:55 PM
2018-01-25

```
No.  Time       Source         Destination    Protocol Length Info
 528 9.994944   172.17.51.117  130.113.68.10  HTTP     1406 GET /~rzheng/course/CAS4C03W18/Labs/HTTP/HTTP-wireshark-file1.html HTTP/1.1
 530 10.001435  130.113.68.10  172.17.51.117  HTTP      496 HTTP/1.1 200 OK  (text/html)
```

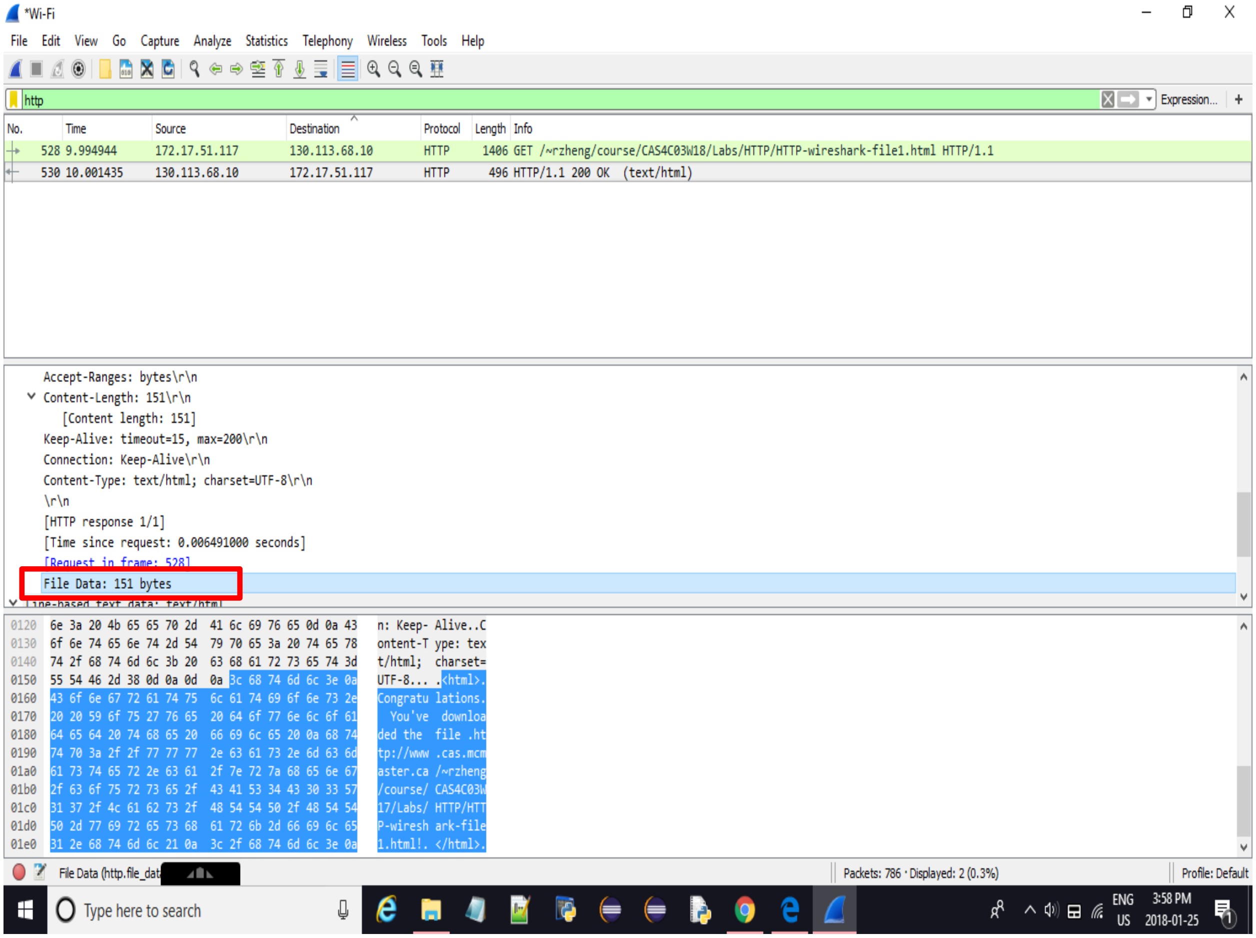
```
        [Group: Sequence]
      Request Version: HTTP/1.1
      Status Code: 200
      [Status Code Description: OK]
      Response Phrase: OK
    Date: Thu, 25 Jan 2018 20:25:48 GMT\r\n
    Server: Apache\r\n
    Last-Modified: Thu, 11 Jan 2018 14:50:04 GMT\r\n
    ETag: "3c2426-97-56281435c9f00"\r\n
    Accept-Ranges: bytes\r\n
  ˅ Content-Length: 151\r\n
      [Content length: 151]
```

```
0070  65 72 3a 20 41 70 61 63  68 65 0d 0a 4c 61 73 74   er: Apac he..Last
0080  2d 4d 6f 64 69 66 69 65  64 3a 20 54 68 75 2c 20   -Modifie d: Thu,
0090  31 31 20 4a 61 6e 20 32  30 31 38 20 31 34 3a 35   11 Jan 2 018 14:5
00a0  30 3a 30 34 20 47 4d 54  0d 0a 45 54 61 67 3a 20   0:04 GMT ..ETag:
00b0  22 33 63 32 34 32 36 2d  39 37 2d 35 36 32 38 31   "3c2426- 97-56281
00c0  34 33 35 63 39 66 30 30  22 0d 0a 41 63 63 65 70   435c9f00 "..Accep
00d0  74 2d 52 61 6e 67 65 73  3a 20 62 79 74 65 73 0d   t-Ranges : bytes.
00e0  0a 43 6f 6e 74 65 6e 74  2d 4c 65 6e 67 74 68 3a   .Content -Length:
00f0  20 31 35 31 0d 0a 4b 65  65 70 2d 41 6c 69 76 65    151..Ke ep-Alive
0100  3a 20 74 69 6d 65 6f 75  74 3d 31 35 2c 20 6d 61   : timeou t=15, ma
0110  78 3d 32 30 30 0d 0a 43  6f 6e 6e 65 63 74 69 6f   x=200..C onnectio
0120  6e 3a 20 4b 65 65 70 2d  41 6c 69 76 65 0d 0a 43   n: Keep- Alive..C
0130  6f 6e 74 65 6e 74 2d 54  79 70 65 3a 20 74 65 78   ontent-T ype: tex
```

```
Bytes 203-224: Respor[redacted]nse.line)        Packets: 786 · Displayed: 2 (0.3%)        Profile: Default
```

Last modified: Thu, 11 2018 14:50:04 GMT\r\n

6.


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expression...

```
http
```

```
No.    Time       Source         Destination    Protocol Length Info
   528 9.994944   172.17.51.117  130.113.68.10  HTTP     1406 GET /~rzheng/course/CAS4C03W18/Labs/HTTP/HTTP-wireshark-file1.html HTTP/1.1
   530 10.001435  130.113.68.10  172.17.51.117  HTTP      496 HTTP/1.1 200 OK  (text/html)
```

```
    Accept-Ranges: bytes\r\n
  ˅ Content-Length: 151\r\n
      [Content length: 151]
    Keep-Alive: timeout=15, max=200\r\n
    Connection: Keep-Alive\r\n
    Content-Type: text/html; charset=UTF-8\r\n
    \r\n
    [HTTP response 1/1]
    [Time since request: 0.006491000 seconds]
    [Request in frame: 528]
    File Data: 151 bytes
˅ Line-based text data: text/html
```

```
0120  6e 3a 20 4b 65 65 70 2d  41 6c 69 76 65 0d 0a 43   n: Keep- Alive..C
0130  6f 6e 74 65 6e 74 2d 54  79 70 65 3a 20 74 65 78   ontent-T ype: tex
0140  74 2f 68 74 6d 6c 3b 20  63 68 61 72 73 65 74 3d   t/html;  charset=
0150  55 54 46 2d 38 0d 0a 0d  0a 3c 68 74 6d 6c 3e 0a   UTF-8... .<html>.
0160  43 6f 6e 67 72 61 74 75  6c 61 74 69 6f 6e 73 2e   Congratu lations.
0170  20 20 59 6f 75 27 76 65  20 64 6f 77 6e 6c 6f 61     You've  downloa
0180  64 65 64 20 74 68 65 20  66 69 6c 65 20 0a 68 74   ded the  file .ht
0190  74 70 3a 2f 2f 77 77 77  2e 63 61 73 2e 6d 63 6d   tp://www .cas.mcm
01a0  61 73 74 65 72 2e 63 61  2f 7e 72 7a 68 65 6e 67   aster.ca /~rzheng
01b0  2f 63 6f 75 72 73 65 2f  43 41 53 34 43 30 33 57   /course/ CAS4C03W
01c0  31 37 2f 4c 61 62 73 2f  48 54 54 50 2f 48 54 54   17/Labs/ HTTP/HTT
01d0  50 2d 77 69 72 65 73 68  61 72 6b 2d 66 69 6c 65   P-wiresh ark-file
01e0  31 2e 68 74 6d 6c 21 0a  3c 2f 68 74 6d 6c 3e 0a   1.html!. </html>.
```

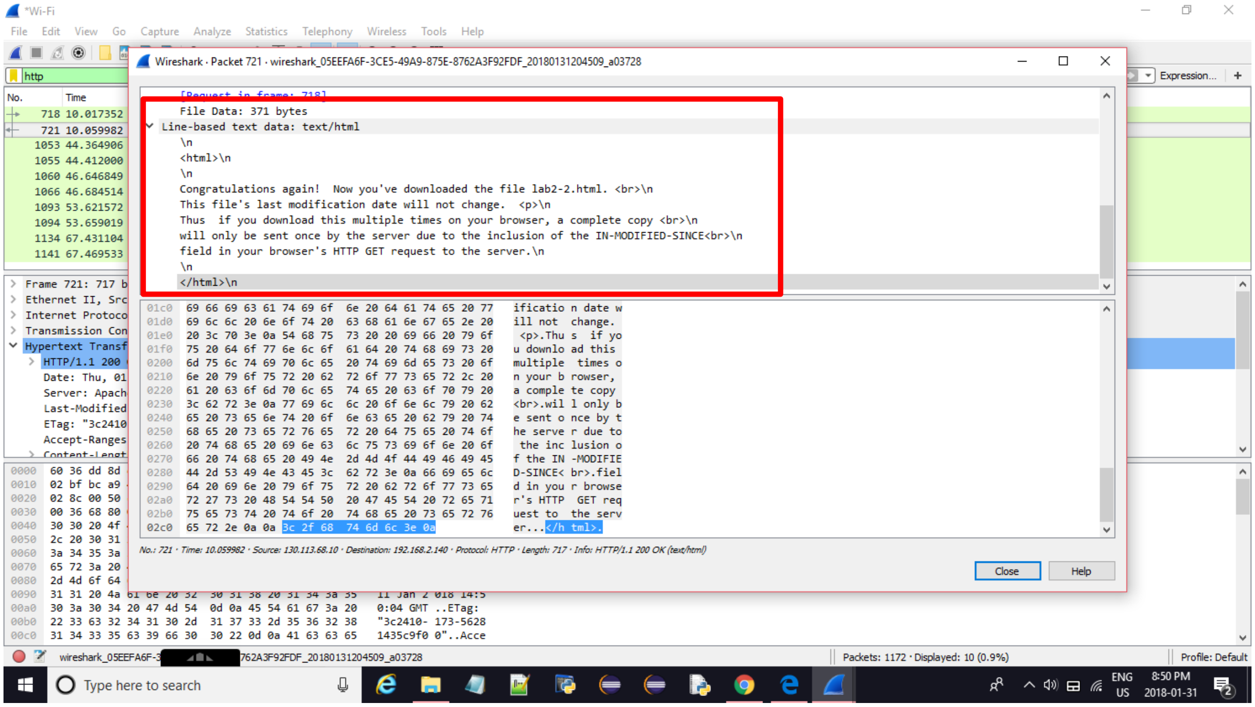
151 bytes

7. No, I do not see any headers within the data that are not displayed in the packet-listing window.

8. No, there is no IF-MODIFIED-SINCE in the first HTTP GET.

9.

Yes it did



Wireshark · Packet 721 · wireshark_05EEFA6F-3CE5-49A9-875E-8762A3F92FDF_20180131204509_a03728

```
    [Request in frame: 718]
    File Data: 371 bytes
  Line-based text data: text/html
    \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
```

```
01c0  69 66 69 63 61 74 69 6f  6e 20 64 61 74 65 20 77   ificatio n date w
01d0  69 6c 6c 20 6e 6f 74 20  63 68 61 6e 67 65 2e 20   ill not  change.
01e0  20 3c 70 3e 0a 54 68 75  73 20 20 69 66 20 79 6f    <p>.Thu s  if yo
01f0  75 20 64 6f 77 6e 6c 6f  61 64 20 74 68 69 73 20   u downlo ad this
0200  6d 75 6c 74 69 70 6c 65  20 74 69 6d 65 73 20 6f   multiple  times o
0210  6e 20 79 6f 75 72 20 62  72 6f 77 73 65 72 2c 20   n your b rowser,
0220  61 20 63 6f 6d 70 6c 65  74 65 20 63 6f 70 79 20   a comple te copy
0230  3c 62 72 3e 0a 77 69 6c  6c 20 6f 6e 6c 79 20 62   <br>.wil l only b
0240  65 20 73 65 6e 74 20 6f  6e 63 65 20 62 79 20 74   e sent o nce by t
0250  68 65 20 73 65 72 76 65  72 20 64 75 65 20 74 6f   he serve r due to
0260  20 74 68 65 20 69 6e 63  6c 75 73 69 6f 6e 20 6f    the inc lusion o
0270  66 20 74 68 65 20 49 4e  2d 4d 4f 44 49 46 49 45   f the IN -MODIFIE
0280  44 2d 53 49 4e 43 45 3c  62 72 3e 0a 66 69 65 6c   D-SINCE< br>.fiel
0290  64 20 69 6e 20 79 6f 75  72 20 62 72 6f 77 73 65   d in you r browse
02a0  72 27 73 20 48 54 54 50  20 47 45 54 20 72 65 71   r's HTTP  GET req
02b0  75 65 73 74 20 74 6f 20  74 68 65 20 73 65 72 76   uest to  the serv
02c0  65 72 2e 0a 0a 3c 2f 68  74 6d 6c 3e 0a            er...</h tml>.
```

No.: 721 · Time: 10.059982 · Source: 130.113.68.10 · Destination: 192.168.2.140 · Protocol: HTTP · Length: 717 · Info: HTTP/1.1 200 OK (text/html)

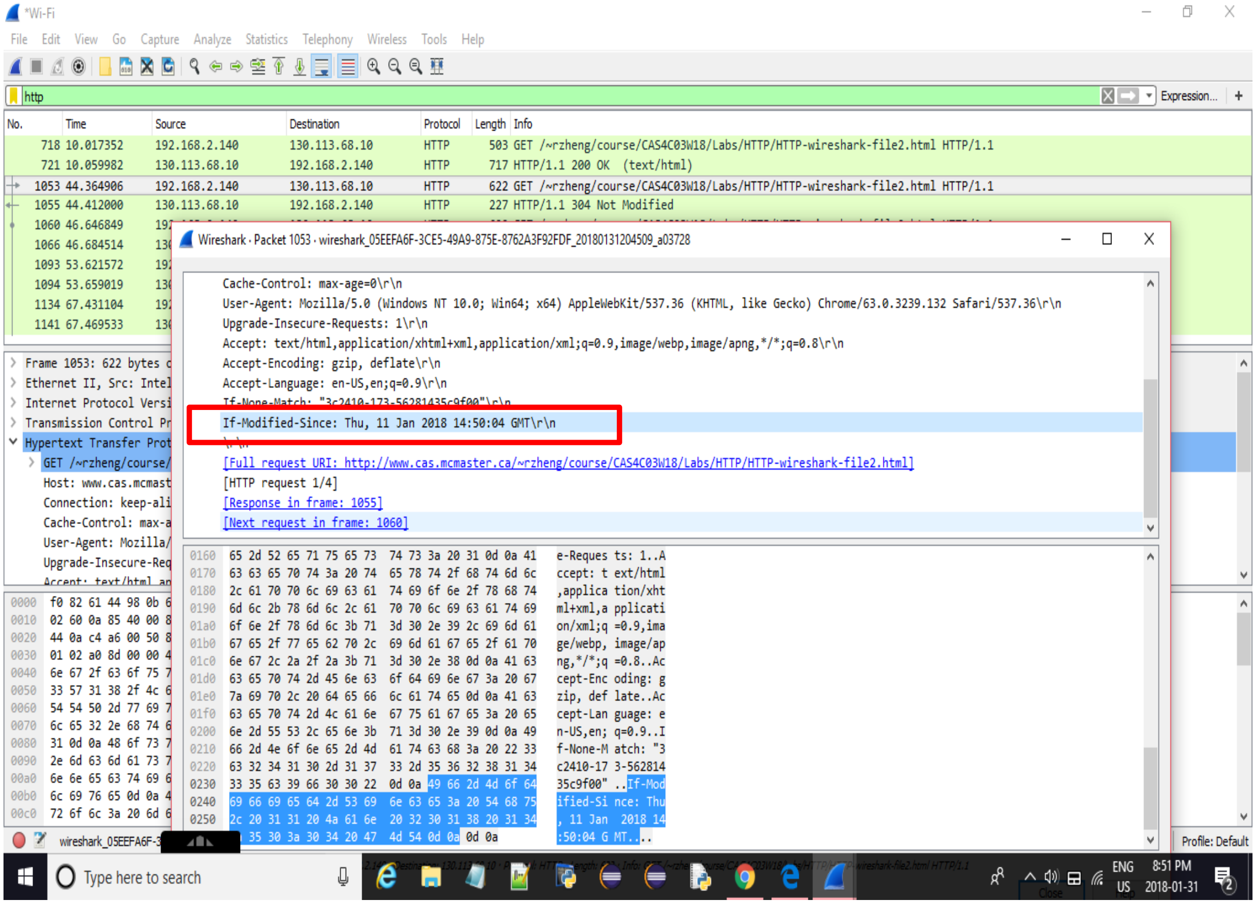
```
No.   Time
  718 10.017352
  721 10.059982
 1053 44.364906
 1055 44.412000
 1060 46.646849
 1066 46.684514
 1093 53.621572
 1094 53.659019
 1134 67.431104
 1141 67.469533
```

```
> Frame 721: 717 b
> Ethernet II, Src
> Internet Protoco
> Transmission Con
v Hypertext Transf
  > HTTP/1.1 200
    Date: Thu, 01
    Server: Apach
    Last-Modified
    ETag: "3c2410
    Accept-Ranges
  > Content-Lengt
```

```
0000  60 36 dd 8d
0010  02 bf bc a9
0020  02 8c 00 50
0030  00 36 68 80
0040  30 30 20 4f
0050  2c 20 30 31
0060  3a 34 35 3a
0070  65 72 3a 20
0080  2d 4d 6f 64
0090  31 31 20 4a 61 6e 20 32  30 31 38 20 31 34 3a 35   11 Jan 2 018 14:5
00a0  30 3a 30 34 20 47 4d 54  0d 0a 45 54 61 67 3a 20   0:04 GMT ..ETag:
00b0  22 33 63 32 34 31 30 2d  31 37 33 2d 35 36 32 38   "3c2410- 173-5628
00c0  31 34 33 35 63 39 66 30  30 22 0d 0a 41 63 63 65   1435c9f0 0"..Acce
```

wireshark_05EEFA6F-3[redacted]762A3F92FDF_20180131204509_a03728 | Packets: 1172 · Displayed: 10 (0.9%) | Profile: Default

10.



*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
Expression...

```
No.   Time       Source         Destination    Protocol Length Info
  718 10.017352  192.168.2.140  130.113.68.10  HTTP     503 GET /~rzheng/course/CAS4C03W18/Labs/HTTP/HTTP-wireshark-file2.html HTTP/1.1
  721 10.059982  130.113.68.10  192.168.2.140  HTTP     717 HTTP/1.1 200 OK  (text/html)
 1053 44.364906  192.168.2.140  130.113.68.10  HTTP     622 GET /~rzheng/course/CAS4C03W18/Labs/HTTP/HTTP-wireshark-file2.html HTTP/1.1
 1055 44.412000  130.113.68.10  192.168.2.140  HTTP     227 HTTP/1.1 304 Not Modified
 1060 46.646849  192
 1066 46.684514  130
 1093 53.621572  192
 1094 53.659019  130
 1134 67.431104  192
 1141 67.469533  130
```

```
> Frame 1053: 622 bytes c
> Ethernet II, Src: Intel
> Internet Protocol Versi
> Transmission Control Pr
v Hypertext Transfer Prot
  > GET /~rzheng/course/
    Host: www.cas.mcmast
    Connection: keep-ali
    Cache-Control: max-a
    User-Agent: Mozilla/
    Upgrade-Insecure-Req
```

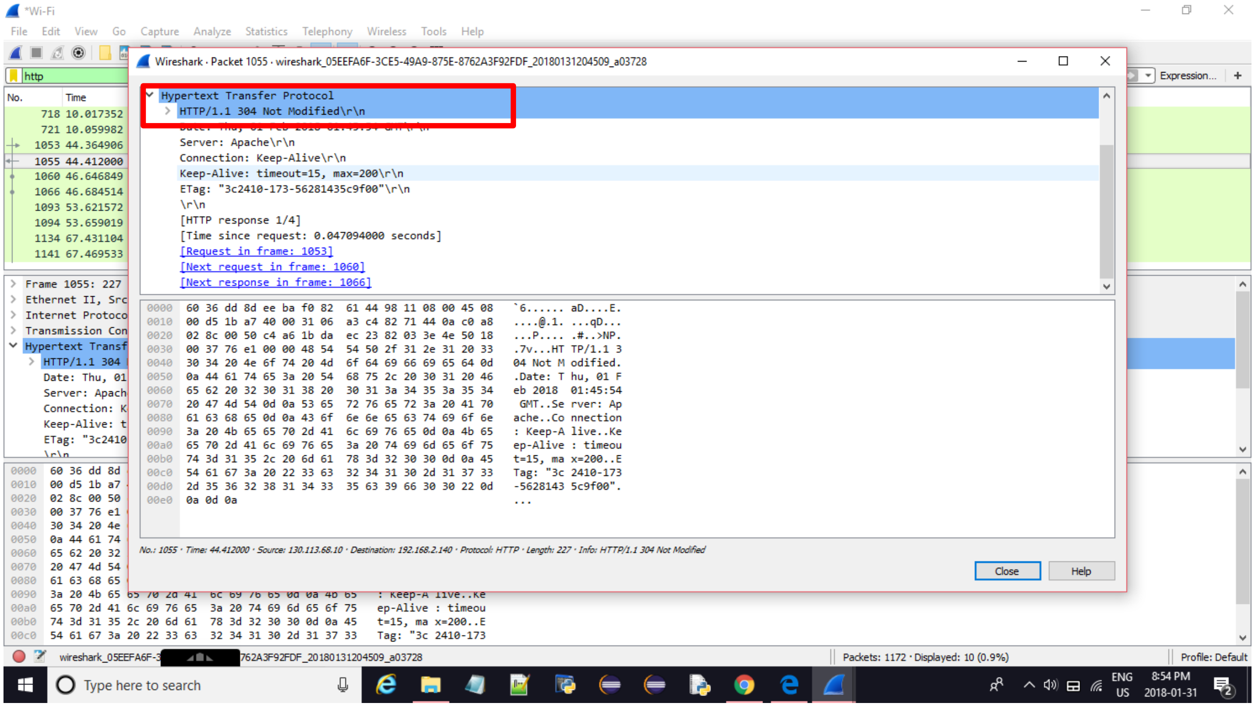
Wireshark · Packet 1053 · wireshark_05EEFA6F-3CE5-49A9-875E-8762A3F92FDF_20180131204509_a03728

```
Cache-Control: max-age=0\r\n
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/63.0.3239.132 Safari/537.36\r\n
Upgrade-Insecure-Requests: 1\r\n
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8\r\n
Accept-Encoding: gzip, deflate\r\n
Accept-Language: en-US,en;q=0.9\r\n
If-None-Match: "3c2410-173-56281435c9f00"\r\n
If-Modified-Since: Thu, 11 Jan 2018 14:50:04 GMT\r\n
\r\n
[Full request URI: http://www.cas.mcmaster.ca/~rzheng/course/CAS4C03W18/Labs/HTTP/HTTP-wireshark-file2.html]
[HTTP request 1/4]
[Response in frame: 1055]
[Next request in frame: 1060]
```

```
0160  65 2d 52 65 71 75 65 73  74 73 3a 20 31 0d 0a 41   e-Reques ts: 1..A
0170  63 63 65 70 74 3a 20 74  65 78 74 2f 68 74 6d 6c   ccept: t ext/html
0180  2c 61 70 70 6c 69 63 61  74 69 6f 6e 2f 78 68 74   ,applica tion/xht
0190  6d 6c 2b 78 6d 6c 2c 61  70 70 6c 69 63 61 74 69   ml+xml,a pplicati
01a0  6f 6e 2f 78 6d 6c 3b 71  3d 30 2e 39 2c 69 6d 61   on/xml;q =0.9,ima
01b0  67 65 2f 77 65 62 70 2c  69 6d 61 67 65 2f 61 70   ge/webp, image/ap
01c0  6e 67 2c 2a 2f 2a 3b 71  3d 30 2e 38 0d 0a 41 63   ng,*/*;q =0.8..Ac
01d0  63 65 70 74 2d 45 6e 63  6f 64 69 6e 67 3a 20 67   cept-Enc oding: g
01e0  7a 69 70 2c 20 64 65 66  6c 61 74 65 0d 0a 41 63   zip, def late..Ac
01f0  63 65 70 74 2d 4c 61 6e  67 75 61 67 65 3a 20 65   cept-Lan guage: e
0200  6e 2d 55 53 2c 65 6e 3b  71 3d 30 2e 39 0d 0a 49   n-US,en; q=0.9..I
0210  66 2d 4e 6f 6e 65 2d 4d  61 74 63 68 3a 20 22 33   f-None-M atch: "3
0220  63 32 34 31 30 2d 31 37  33 2d 35 36 32 38 31 34   c2410-17 3-562814
0230  33 35 63 39 66 30 30 22  0d 0a 49 66 2d 4d 6f 64   35c9f00" ..If-Mod
0240  69 66 69 65 64 2d 53 69  6e 63 65 3a 20 54 68 75   ified-Si nce: Thu
0250  2c 20 31 31 20 4a 61 6e  20 32 30 31 38 20 31 34   , 11 Jan  2018 14
         35 30 3a 30 34 20 47  4d 54 0d 0a 0d 0a         :50:04 G MT....
```

Yes, there is an If-Modified-Since in the second HTTP GET. The information follows are the date and time that was last accessed.

11.



Wireshark · Packet 1055 · wireshark_05EEFA6F-3CE5-49A9-875E-8762A3F92FDF_20180131204509_a03728

```
Hypertext Transfer Protocol
  HTTP/1.1 304 Not Modified\r\n
  Server: Apache\r\n
  Connection: Keep-Alive\r\n
  Keep-Alive: timeout=15, max=200\r\n
  ETag: "3c2410-173-56281435c9f00"\r\n
  \r\n
  [HTTP response 1/4]
  [Time since request: 0.047094000 seconds]
  [Request in frame: 1053]
  [Next request in frame: 1060]
  [Next response in frame: 1066]
```

```
0000  60 36 dd 8d ee ba f0 82  61 44 98 11 08 00 45 08   `6...... aD....E.
0010  00 d5 1b a7 40 00 31 06  a3 c4 82 71 44 0a c0 a8   ....@.1. ...qD...
0020  02 8c 00 50 c4 a6 1b da  ec 23 82 03 3e 4e 50 18   ...P.... .#..>NP.
0030  00 37 76 e1 00 00 48 54  54 50 2f 31 2e 31 20 33   .7v...HT TP/1.1 3
0040  30 34 20 4e 6f 74 20 4d  6f 64 69 66 69 65 64 0d   04 Not M odified.
0050  0a 44 61 74 65 3a 20 54  68 75 2c 20 30 31 20 46   .Date: T hu, 01 F
0060  65 62 20 32 30 31 38 20  30 31 3a 34 35 3a 35 34   eb 2018  01:45:54
0070  20 47 4d 54 0d 0a 53 65  72 76 65 72 3a 20 41 70    GMT..Se rver: Ap
0080  61 63 68 65 0d 0a 43 6f  6e 6e 65 63 74 69 6f 6e   ache..Co nnection
0090  3a 20 4b 65 65 70 2d 41  6c 69 76 65 0d 0a 4b 65   : Keep-A live..Ke
00a0  65 70 2d 41 6c 69 76 65  3a 20 74 69 6d 65 6f 75   ep-Alive : timeou
00b0  74 3d 31 35 2c 20 6d 61  78 3d 32 30 30 0d 0a 45   t=15, ma x=200..E
00c0  54 61 67 3a 20 22 33 63  32 34 31 30 2d 31 37 33   Tag: "3c 2410-173
00d0  2d 35 36 32 38 31 34 33  35 63 39 66 30 30 22 0d   -5628143 5c9f00".
00e0  0a 0d 0a                                           ...
```

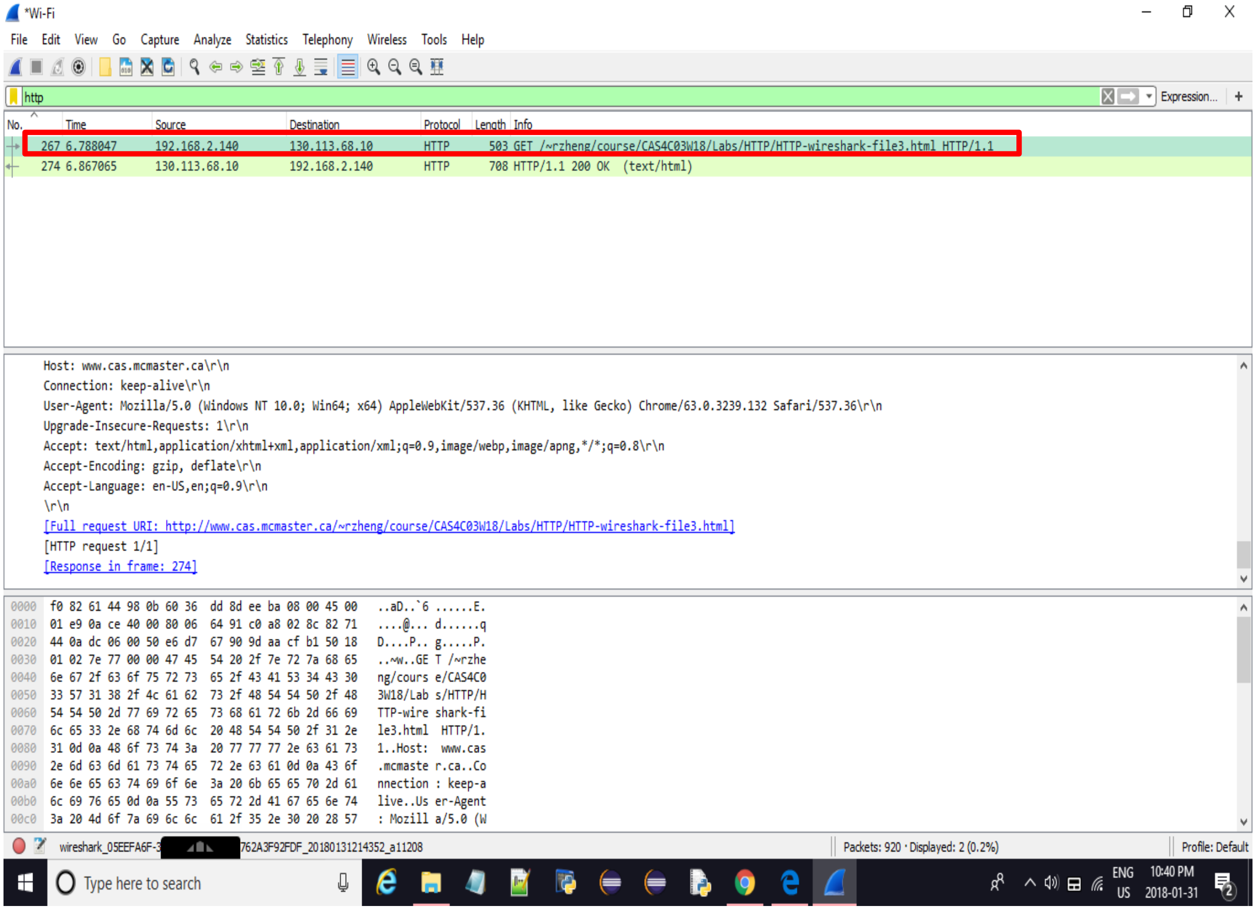
No.: 1055 · Time: 44.412000 · Source: 130.113.68.10 · Destination: 192.168.2.140 · Protocol: HTTP · Length: 227 · Info: HTTP/1.1 304 Not Modified

*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
Expression...
No. Time
Close
Help
wireshark_05EEFA6F-3[redacted]762A3F92FDF_20180131204509_a03728
Packets: 1172 · Displayed: 10 (0.9%)
Profile: Default
Type here to search
ENG US
8:54 PM 2018-01-31

The HTTP status code returned is: 304 Not Modified

No the server did not return the contents of the file this time. Since we only refreshed the page, the browser just retrieved the contents from the memory. If the file was modified since last accessed, then it would return the contents.

12.


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expression...
Type here to search
ENG
US
10:40 PM
2018-01-31

http

```
No.   Time        Source          Destination     Protocol  Length  Info
267 6.788047      192.168.2.140   130.113.68.10   HTTP      503 GET /~rzheng/course/CAS4C03W18/Labs/HTTP/HTTP-wireshark-file3.html HTTP/1.1
274 6.867065      130.113.68.10   192.168.2.140   HTTP      708 HTTP/1.1 200 OK  (text/html)
```

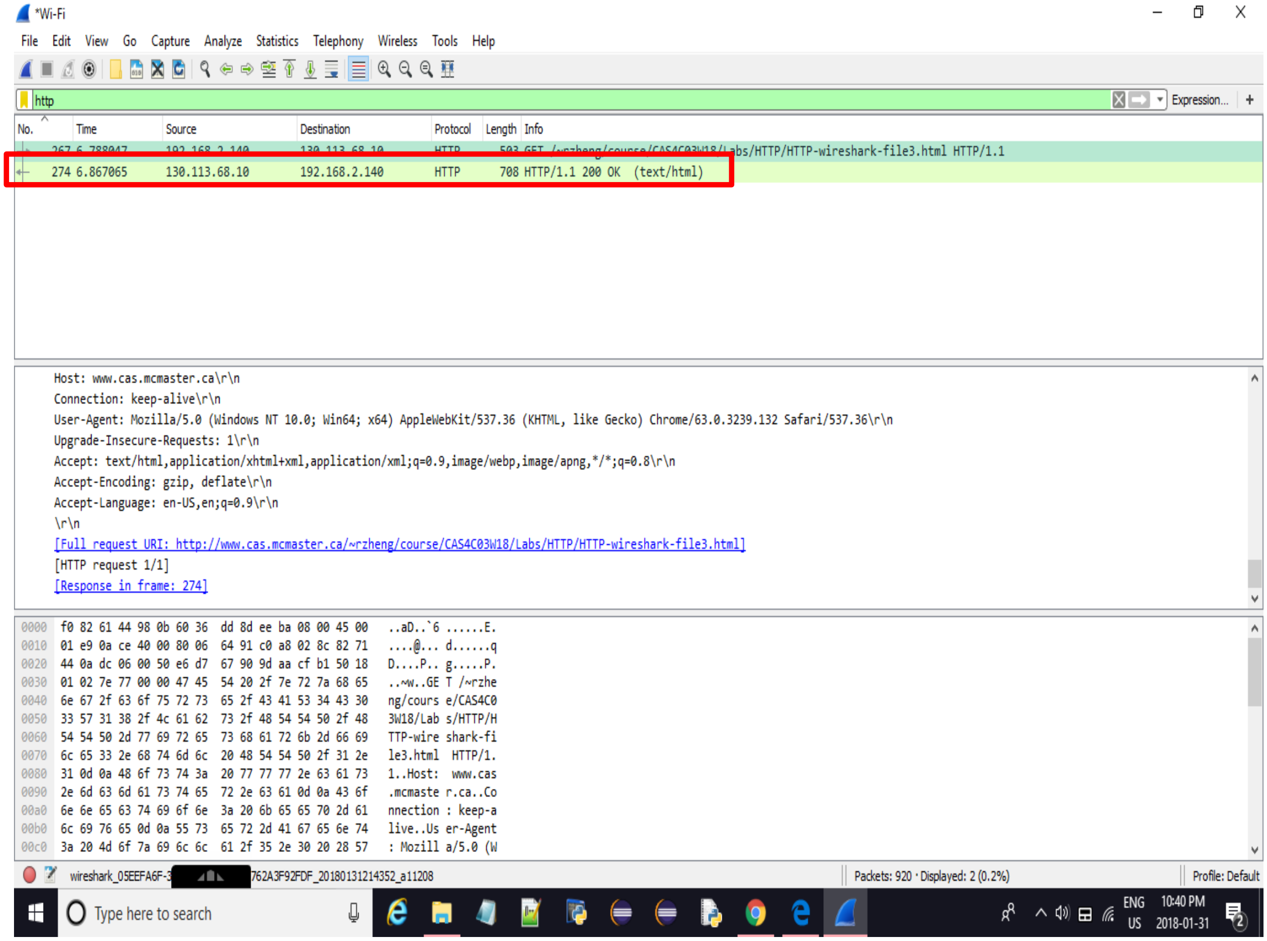
```
    Host: www.cas.mcmaster.ca\r\n
    Connection: keep-alive\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/63.0.3239.132 Safari/537.36\r\n
    Upgrade-Insecure-Requests: 1\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8\r\n
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: en-US,en;q=0.9\r\n
    \r\n
    [Full request URI: http://www.cas.mcmaster.ca/~rzheng/course/CAS4C03W18/Labs/HTTP/HTTP-wireshark-file3.html]
    [HTTP request 1/1]
    [Response in frame: 274]
```

```
0000  f0 82 61 44 98 0b 60 36  dd 8d ee ba 08 00 45 00   ..aD..`6 ......E.
0010  01 e9 0a ce 40 00 80 06  64 91 c0 a8 02 8c 82 71   ....@... d......q
0020  44 0a dc 06 00 50 e6 d7  67 90 9d aa cf b1 50 18   D....P.. g.....P.
0030  01 02 7e 77 00 00 47 45  54 20 2f 7e 72 7a 68 65   ..~w..GE T /~rzhe
0040  6e 67 2f 63 6f 75 72 73  65 2f 43 41 53 34 43 30   ng/cours e/CAS4C0
0050  33 57 31 38 2f 4c 61 62  73 2f 48 54 54 50 2f 48   3W18/Lab s/HTTP/H
0060  54 54 50 2d 77 69 72 65  73 68 61 72 6b 2d 66 69   TTP-wire shark-fi
0070  6c 65 33 2e 68 74 6d 6c  20 48 54 54 50 2f 31 2e   le3.html  HTTP/1.
0080  31 0d 0a 48 6f 73 74 3a  20 77 77 77 2e 63 61 73   1..Host:  www.cas
0090  2e 6d 63 6d 61 73 74 65  72 2e 63 61 0d 0a 43 6f   .mcmaste r.ca..Co
00a0  6e 6e 65 63 74 69 6f 6e  3a 20 6b 65 65 70 2d 61   nnection : keep-a
00b0  6c 69 76 65 0d 0a 55 73  65 72 2d 41 67 65 6e 74   live..Us er-Agent
00c0  3a 20 4d 6f 7a 69 6c 6c  61 2f 35 2e 30 20 28 57   : Mozill a/5.0 (W
```

wireshark_05EEFA6F-3[redacted]762A3F92FDF_20180131214352_a11208 | Packets: 920 · Displayed: 2 (0.2%) | Profile: Default

The browser sent one HTTP GET message, the packet number that contains the GET message is 267.

13.


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expression...
Type here to search
ENG
US
10:40 PM
2018-01-31

```
http
```

```
No.   Time        Source          Destination     Protocol Length Info
  267 6.788047    192.168.2.140   130.113.68.10   HTTP      503 GET /~rzheng/course/CAS4C03W18/Labs/HTTP/HTTP-wireshark-file3.html HTTP/1.1
  274 6.867065    130.113.68.10   192.168.2.140   HTTP      708 HTTP/1.1 200 OK  (text/html)
```

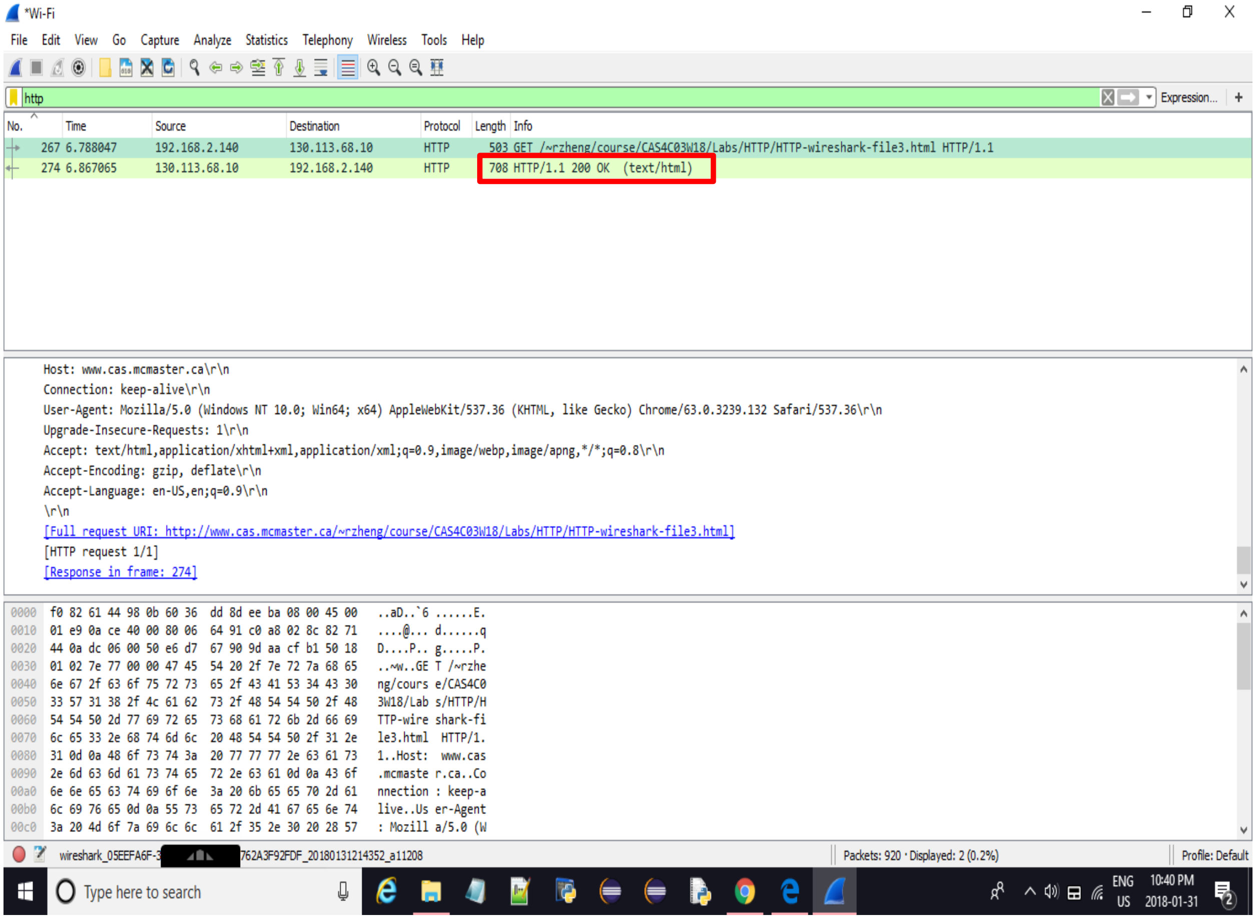
```
    Host: www.cas.mcmaster.ca\r\n
    Connection: keep-alive\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/63.0.3239.132 Safari/537.36\r\n
    Upgrade-Insecure-Requests: 1\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8\r\n
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: en-US,en;q=0.9\r\n
    \r\n
    [Full request URI: http://www.cas.mcmaster.ca/~rzheng/course/CAS4C03W18/Labs/HTTP/HTTP-wireshark-file3.html]
    [HTTP request 1/1]
    [Response in frame: 274]
```

```
0000  f0 82 61 44 98 0b 60 36  dd 8d ee ba 08 00 45 00   ..aD..`6 ......E.
0010  01 e9 0a ce 40 00 80 06  64 91 c0 a8 02 8c 82 71   ....@... d......q
0020  44 0a dc 06 00 50 e6 d7  67 90 9d aa cf b1 50 18   D....P.. g.....P.
0030  01 02 7e 77 00 00 47 45  54 20 2f 7e 72 7a 68 65   ..~w..GE T /~rzhe
0040  6e 67 2f 63 6f 75 72 73  65 2f 43 41 53 34 43 30   ng/cours e/CAS4C0
0050  33 57 31 38 2f 4c 61 62  73 2f 48 54 54 50 2f 48   3W18/Lab s/HTTP/H
0060  54 54 50 2d 77 69 72 65  73 68 61 72 6b 2d 66 69   TTP-wire shark-fi
0070  6c 65 33 2e 68 74 6d 6c  20 48 54 54 50 2f 31 2e   le3.html  HTTP/1.
0080  31 0d 0a 48 6f 73 74 3a  20 77 77 77 2e 63 61 73   1..Host:  www.cas
0090  2e 6d 63 6d 61 73 74 65  72 2e 63 61 0d 0a 43 6f   .mcmaste r.ca..Co
00a0  6e 6e 65 63 74 69 6f 6e  3a 20 6b 65 65 70 2d 61   nnection : keep-a
00b0  6c 69 76 65 0d 0a 55 73  65 72 2d 41 67 65 6e 74   live..Us er-Agent
00c0  3a 20 4d 6f 7a 69 6c 6c  61 2f 35 2e 30 20 28 57   : Mozill a/5.0 (W
```

```
wireshark_05EEFA6F-3[redacted]762A3F92FDF_20180131214352_a11208    Packets: 920 · Displayed: 2 (0.2%)    Profile: Default
```

The packet number is 274, which contains the status code and phrase in response to HTTP GET request.

14.


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expression...
+
Type here to search
ENG
US
10:40 PM
2018-01-31

```
http
```

```
No.      Time         Source           Destination      Protocol  Length  Info
    267 6.788047     192.168.2.140    130.113.68.10    HTTP         503 GET /~rzheng/course/CAS4C03W18/Labs/HTTP/HTTP-wireshark-file3.html HTTP/1.1
    274 6.867065     130.113.68.10    192.168.2.140    HTTP         708 HTTP/1.1 200 OK  (text/html)
```

```
    Host: www.cas.mcmaster.ca\r\n
    Connection: keep-alive\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/63.0.3239.132 Safari/537.36\r\n
    Upgrade-Insecure-Requests: 1\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8\r\n
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: en-US,en;q=0.9\r\n
    \r\n
    [Full request URI: http://www.cas.mcmaster.ca/~rzheng/course/CAS4C03W18/Labs/HTTP/HTTP-wireshark-file3.html]
    [HTTP request 1/1]
    [Response in frame: 274]
```

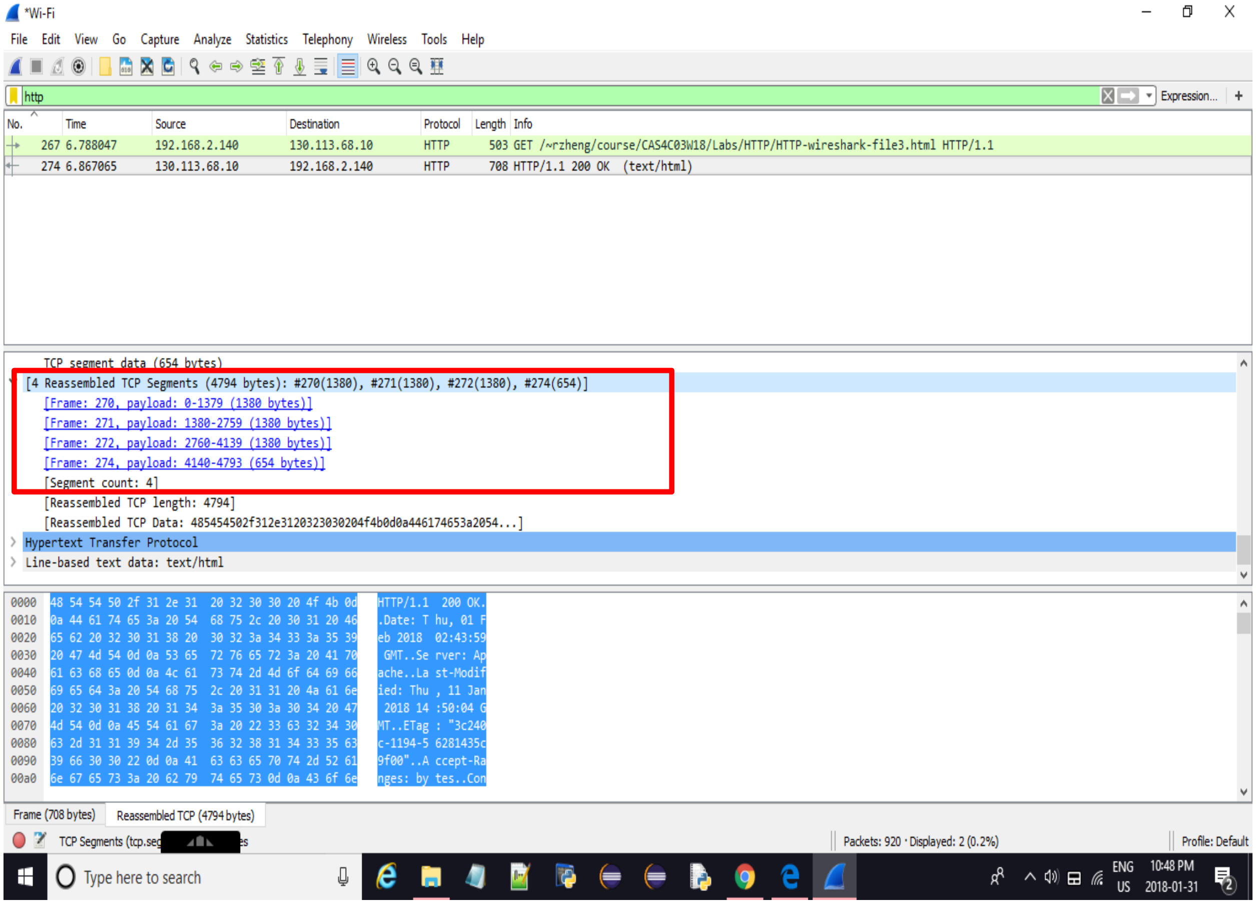
```
0000  f0 82 61 44 98 0b 60 36  dd 8d ee ba 08 00 45 00   ..aD..`6 ......E.
0010  01 e9 0a ce 40 00 80 06  64 91 c0 a8 02 8c 82 71   ....@... d......q
0020  44 0a dc 06 00 50 e6 d7  67 90 9d aa cf b1 50 18   D....P.. g.....P.
0030  01 02 7e 77 00 00 47 45  54 20 2f 7e 72 7a 68 65   ..~w..GE T /~rzhe
0040  6e 67 2f 63 6f 75 72 73  65 2f 43 41 53 34 43 30   ng/cours e/CAS4C0
0050  33 57 31 38 2f 4c 61 62  73 2f 48 54 54 50 2f 48   3W18/Lab s/HTTP/H
0060  54 54 50 2d 77 69 72 65  73 68 61 72 6b 2d 66 69   TTP-wire shark-fi
0070  6c 65 33 2e 68 74 6d 6c  20 48 54 54 50 2f 31 2e   le3.html  HTTP/1.
0080  31 0d 0a 48 6f 73 74 3a  20 77 77 77 2e 63 61 73   1..Host:  www.cas
0090  2e 6d 63 6d 61 73 74 65  72 2e 63 61 0d 0a 43 6f   .mcmaste r.ca..Co
00a0  6e 6e 65 63 74 69 6f 6e  3a 20 6b 65 65 70 2d 61   nnection : keep-a
00b0  6c 69 76 65 0d 0a 55 73  65 72 2d 41 67 65 6e 74   live..Us er-Agent
00c0  3a 20 4d 6f 7a 69 6c 6c  61 2f 35 2e 30 20 28 57   : Mozill a/5.0 (W
```

wireshark_05EEFA6F-3[redacted]762A3F92FDF_20180131214352_a11208   Packets: 920 · Displayed: 2 (0.2%)   Profile: Default

Status code: 200

Phrase: OK

15.



*Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http

```
No.   Time       Source          Destination     Protocol Length Info
  267 6.788047   192.168.2.140   130.113.68.10   HTTP       503 GET /~rzheng/course/CAS4C03W18/Labs/HTTP/HTTP-wireshark-file3.html HTTP/1.1
  274 6.867065   130.113.68.10   192.168.2.140   HTTP       708 HTTP/1.1 200 OK  (text/html)
```

```
    TCP segment data (654 bytes)
  [4 Reassembled TCP Segments (4794 bytes): #270(1380), #271(1380), #272(1380), #274(654)]
    [Frame: 270, payload: 0-1379 (1380 bytes)]
    [Frame: 271, payload: 1380-2759 (1380 bytes)]
    [Frame: 272, payload: 2760-4139 (1380 bytes)]
    [Frame: 274, payload: 4140-4793 (654 bytes)]
    [Segment count: 4]
    [Reassembled TCP length: 4794]
    [Reassembled TCP Data: 485454502f312e3120323030204f4b0d0a446174653a2054...]
> Hypertext Transfer Protocol
> Line-based text data: text/html
```

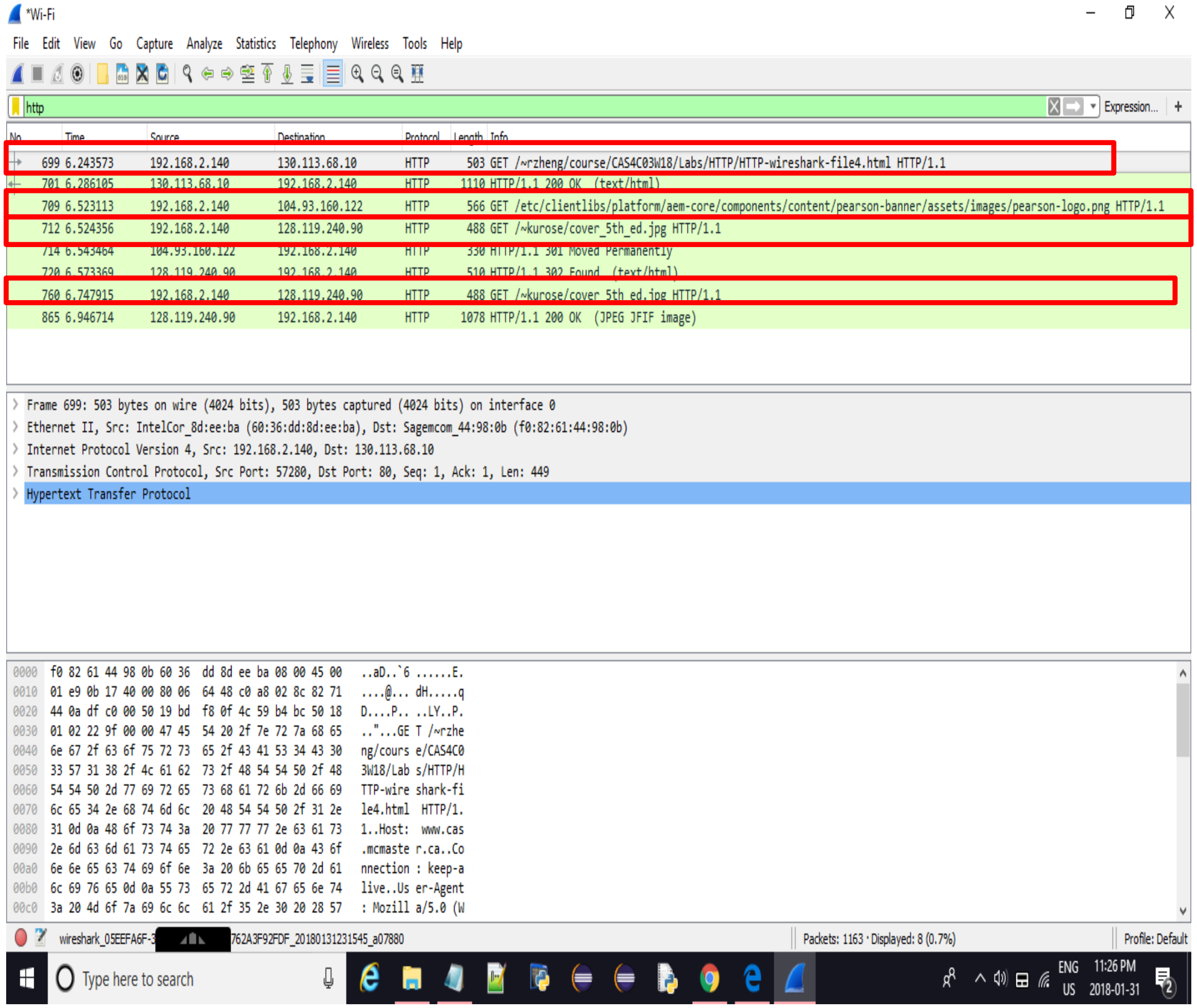
```
0000  48 54 54 50 2f 31 2e 31  20 32 30 30 20 4f 4b 0d   HTTP/1.1  200 OK.
0010  0a 44 61 74 65 3a 20 54  68 75 2c 20 30 31 20 46   .Date: T hu, 01 F
0020  65 62 20 32 30 31 38 20  30 32 3a 34 33 3a 35 39   eb 2018  02:43:59
0030  20 47 4d 54 0d 0a 53 65  72 76 65 72 3a 20 41 70    GMT..Se rver: Ap
0040  61 63 68 65 0d 0a 4c 61  73 74 2d 4d 6f 64 69 66   ache..La st-Modif
0050  69 65 64 3a 20 54 68 75  2c 20 31 31 20 4a 61 6e   ied: Thu , 11 Jan
0060  20 32 30 31 38 20 31 34  3a 35 30 3a 30 34 20 47    2018 14 :50:04 G
0070  4d 54 0d 0a 45 54 61 67  3a 20 22 33 63 32 34 30   MT..ETag : "3c240
0080  63 2d 31 31 39 34 2d 35  36 32 38 31 34 33 35 63   c-1194-5 6281435c
0090  39 66 30 30 22 0d 0a 41  63 63 65 70 74 2d 52 61   9f00"..A ccept-Ra
00a0  6e 67 65 73 3a 20 62 79  74 65 73 0d 0a 43 6f 6e   nges: by tes..Con
```

Frame (708 bytes) | Reassembled TCP (4794 bytes)

TCP Segments (tcp.seg[redacted]es | Packets: 920 · Displayed: 2 (0.2%) | Profile: Default

As shown, 4 TCP segments were needed to carry the single HTTP response and the text of the Bill of Rights.

16.


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expression...
+

```
http
```

```
No.  Time      Source         Destination     Protocol Length Info
699 6.243573   192.168.2.140  130.113.68.10   HTTP      503 GET /~rzheng/course/CAS4C03W18/Labs/HTTP/HTTP-wireshark-file4.html HTTP/1.1
701 6.286105   130.113.68.10  192.168.2.140   HTTP     1110 HTTP/1.1 200 OK  (text/html)
709 6.523113   192.168.2.140  104.93.160.122  HTTP      566 GET /etc/clientlibs/platform/aem-core/components/content/pearson-banner/assets/images/pearson-logo.png HTTP/1.1
712 6.524356   192.168.2.140  128.119.240.90  HTTP      488 GET /~kurose/cover_5th_ed.jpg HTTP/1.1
714 6.543464   104.93.160.122 192.168.2.140   HTTP      330 HTTP/1.1 301 Moved Permanently
720 6.573369   128.119.240.90 192.168.2.140   HTTP      510 HTTP/1.1 302 Found  (text/html)
760 6.747915   192.168.2.140  128.119.240.90  HTTP      488 GET /~kurose/cover_5th_ed.jpg HTTP/1.1
865 6.946714   128.119.240.90 192.168.2.140   HTTP     1078 HTTP/1.1 200 OK  (JPEG JFIF image)
```

```
> Frame 699: 503 bytes on wire (4024 bits), 503 bytes captured (4024 bits) on interface 0
> Ethernet II, Src: IntelCor_8d:ee:ba (60:36:dd:8d:ee:ba), Dst: Sagemcom_44:98:0b (f0:82:61:44:98:0b)
> Internet Protocol Version 4, Src: 192.168.2.140, Dst: 130.113.68.10
> Transmission Control Protocol, Src Port: 57280, Dst Port: 80, Seq: 1, Ack: 1, Len: 449
> Hypertext Transfer Protocol
```

```
0000  f0 82 61 44 98 0b 60 36  dd 8d ee ba 08 00 45 00   ..aD..`6 ......E.
0010  01 e9 0b 17 40 00 80 06  64 48 c0 a8 02 8c 82 71   ....@... dH.....q
0020  44 0a df c0 00 50 19 bd  f8 0f 4c 59 b4 bc 50 18   D....P.. ..LY..P.
0030  01 02 22 9f 00 00 47 45  54 20 2f 7e 72 7a 68 65   .."...GE T /~rzhe
0040  6e 67 2f 63 6f 75 72 73  65 2f 43 41 53 34 43 30   ng/cours e/CAS4C0
0050  33 57 31 38 2f 4c 61 62  73 2f 48 54 54 50 2f 48   3W18/Lab s/HTTP/H
0060  54 54 50 2d 77 69 72 65  73 68 61 72 6b 2d 66 69   TTP-wire shark-fi
0070  6c 65 34 2e 68 74 6d 6c  20 48 54 54 50 2f 31 2e   le4.html  HTTP/1.
0080  31 0d 0a 48 6f 73 74 3a  20 77 77 77 2e 63 61 73   1..Host:  www.cas
0090  2e 6d 63 6d 61 73 74 65  72 2e 63 61 0d 0a 43 6f   .mcmaste r.ca..Co
00a0  6e 6e 65 63 74 69 6f 6e  3a 20 6b 65 65 70 2d 61   nnection : keep-a
00b0  6c 69 76 65 0d 0a 55 73  65 72 2d 41 67 65 6e 74   live..Us er-Agent
00c0  3a 20 4d 6f 7a 69 6c 6c  61 2f 35 2e 30 20 28 57   : Mozill a/5.0 (W
```

wireshark_05EEFA6F-3[redacted]762A3F92FDF_20180131231545_a07880 | Packets: 1163 · Displayed: 8 (0.7%) | Profile: Default

There are 4 HTTP GET request message. Packet 699 was send to get the initial page, packet 709 was sent to get the Pearson logo, packet 712 was sent to get the cover of the 5th edition Pearson book image, packet 760 was sent to get the cover of the 5th edition Pearson book image again.

Address sent to:

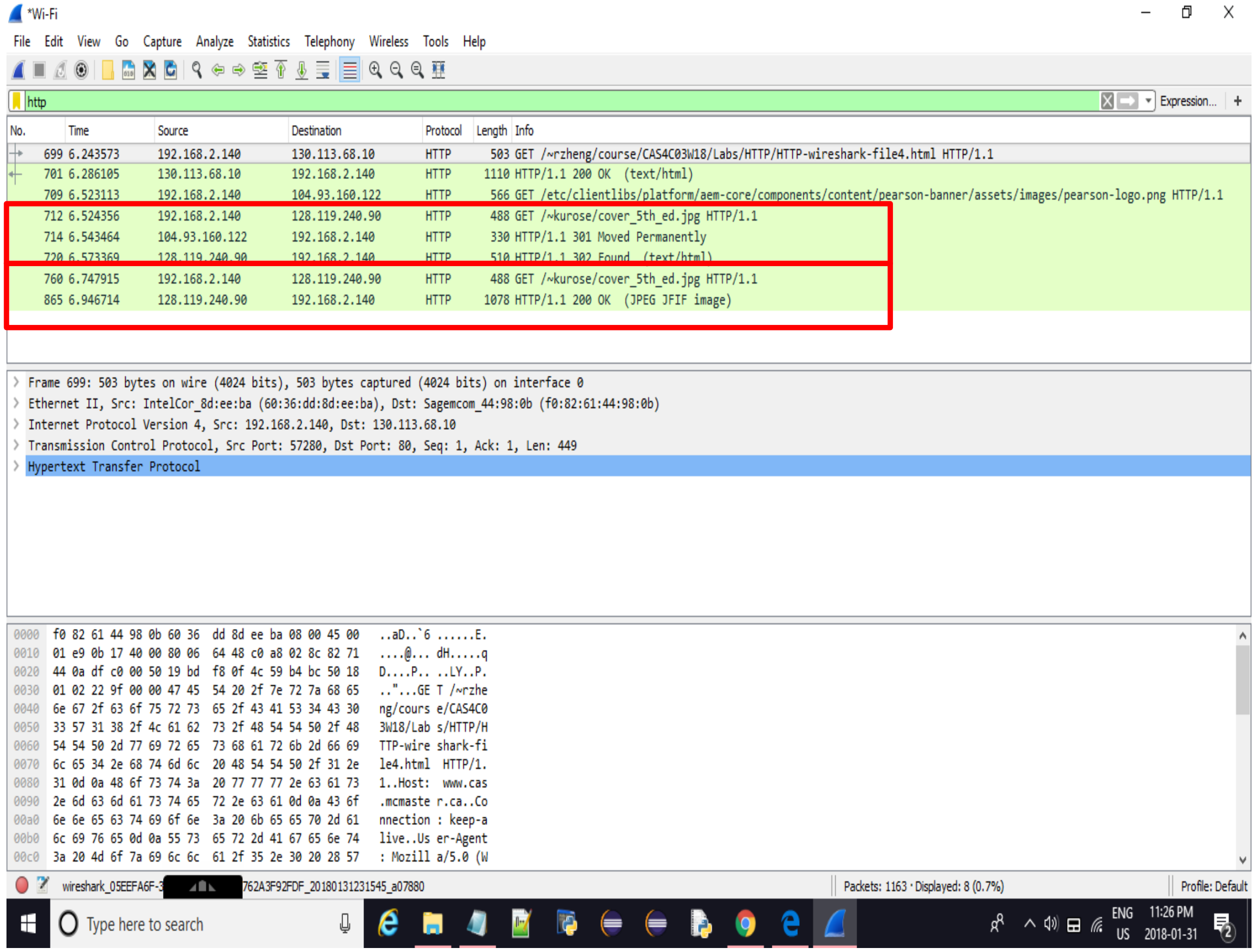
Initial page: 130.113.68.10

Pearson logo: 104.93.160.122

Pearson textbook cover: 128.119.240.90

Pearson textbook cover: 128.119.240.90

17.


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expression...
+

```
http
```

```
No.    Time        Source          Destination     Protocol Length Info
  699 6.243573    192.168.2.140   130.113.68.10   HTTP      503 GET /~rzheng/course/CAS4C03W18/Labs/HTTP/HTTP-wireshark-file4.html HTTP/1.1
  701 6.286105    130.113.68.10   192.168.2.140   HTTP     1110 HTTP/1.1 200 OK  (text/html)
  709 6.523113    192.168.2.140   104.93.160.122  HTTP      566 GET /etc/clientlibs/platform/aem-core/components/content/pearson-banner/assets/images/pearson-logo.png HTTP/1.1
  712 6.524356    192.168.2.140   128.119.240.90  HTTP      488 GET /~kurose/cover_5th_ed.jpg HTTP/1.1
  714 6.543464    104.93.160.122  192.168.2.140   HTTP      330 HTTP/1.1 301 Moved Permanently
  720 6.573369    128.119.240.90  192.168.2.140   HTTP      510 HTTP/1.1 302 Found  (text/html)
  760 6.747915    192.168.2.140   128.119.240.90  HTTP      488 GET /~kurose/cover_5th_ed.jpg HTTP/1.1
  865 6.946714    128.119.240.90  192.168.2.140   HTTP     1078 HTTP/1.1 200 OK  (JPEG JFIF image)
```

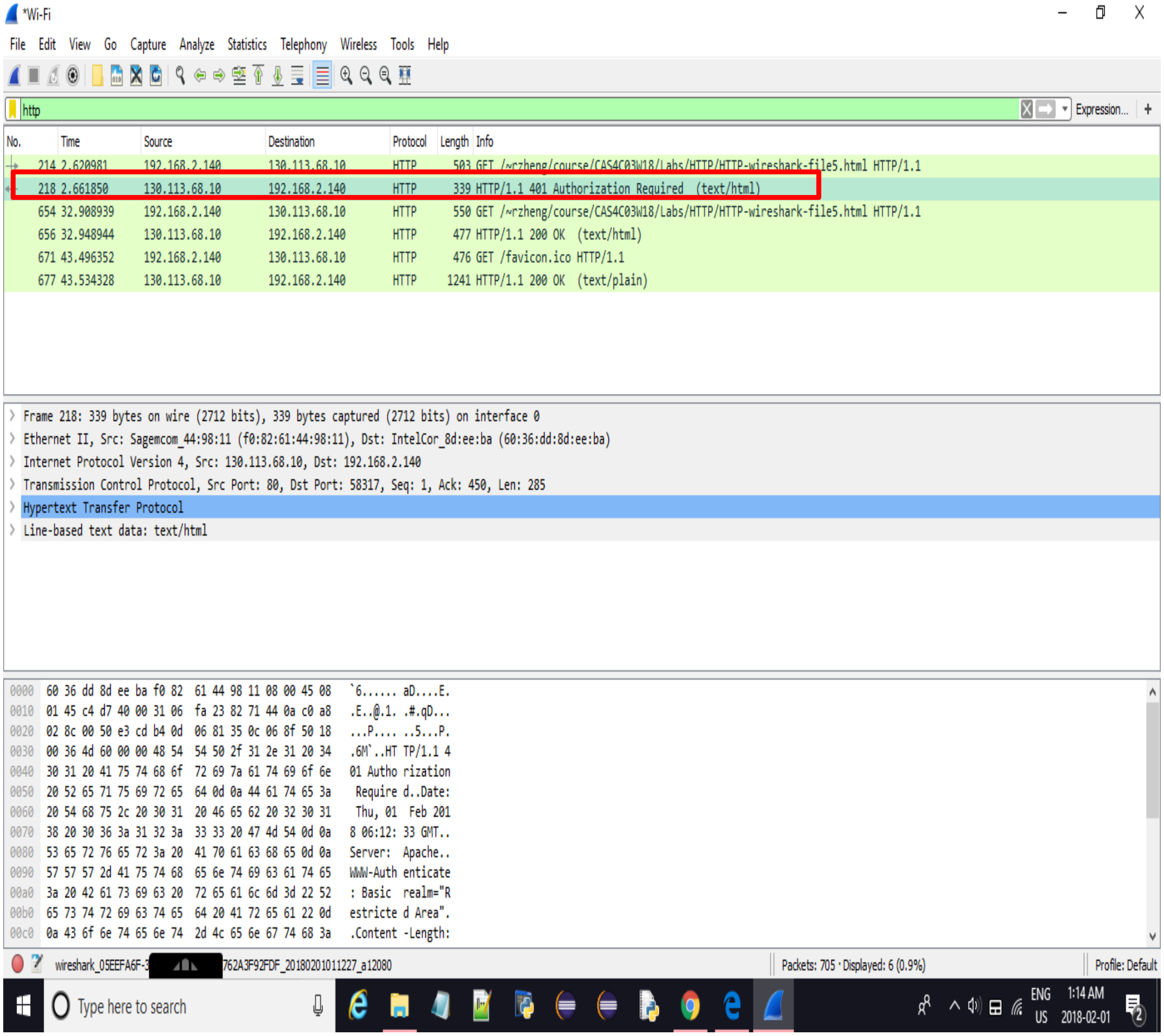
```
> Frame 699: 503 bytes on wire (4024 bits), 503 bytes captured (4024 bits) on interface 0
> Ethernet II, Src: IntelCor_8d:ee:ba (60:36:dd:8d:ee:ba), Dst: Sagemcom_44:98:0b (f0:82:61:44:98:0b)
> Internet Protocol Version 4, Src: 192.168.2.140, Dst: 130.113.68.10
> Transmission Control Protocol, Src Port: 57280, Dst Port: 80, Seq: 1, Ack: 1, Len: 449
> Hypertext Transfer Protocol
```

```
0000  f0 82 61 44 98 0b 60 36  dd 8d ee ba 08 00 45 00   ..aD..`6 ......E.
0010  01 e9 0b 17 40 00 80 06  64 48 c0 a8 02 8c 82 71   ....@... dH.....q
0020  44 0a df c0 00 50 19 bd  f8 0f 4c 59 b4 bc 50 18   D....P.. ..LY..P.
0030  01 02 22 9f 00 00 47 45  54 20 2f 7e 72 7a 68 65   .."...GE T /~rzhe
0040  6e 67 2f 63 6f 75 72 73  65 2f 43 41 53 34 43 30   ng/cours e/CAS4C0
0050  33 57 31 38 2f 4c 61 62  73 2f 48 54 54 50 2f 48   3W18/Lab s/HTTP/H
0060  54 54 50 2d 77 69 72 65  73 68 61 72 6b 2d 66 69   TTP-wire shark-fi
0070  6c 65 34 2e 68 74 6d 6c  20 48 54 54 50 2f 31 2e   le4.html  HTTP/1.
0080  31 0d 0a 48 6f 73 74 3a  20 77 77 77 2e 63 61 73   1..Host:  www.cas
0090  2e 6d 63 6d 61 73 74 65  72 2e 63 61 0d 0a 43 6f   .mcmaste r.ca..Co
00a0  6e 6e 65 63 74 69 6f 6e  3a 20 6b 65 65 70 2d 61   nnection : keep-a
00b0  6c 69 76 65 0d 0a 55 73  65 72 2d 41 67 65 6e 74   live..Us er-Agent
00c0  3a 20 4d 6f 7a 69 6c 6c  61 2f 35 2e 30 20 28 57   : Mozill a/5.0 (W
```

wireshark_05EEFA6F-3[redacted]762A3F92FDF_20180131231545_a07880 | Packets: 1163 · Displayed: 8 (0.7%) | Profile: Default

The browser downloaded the two images in serially. The first image was requested (packet 712) and got a reply (packet 720) before the second image was requested (packet 760) by the browser.

18.


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expression...
+

```
http
```

```
No.     Time        Source          Destination     Protocol  Length  Info
    214 2.620981    192.168.2.140   130.113.68.10   HTTP       503  GET /~rzheng/course/CAS4C03W18/Labs/HTTP/HTTP-wireshark-file5.html HTTP/1.1
    218 2.661850    130.113.68.10   192.168.2.140   HTTP       339  HTTP/1.1 401 Authorization Required  (text/html)
    654 32.908939   192.168.2.140   130.113.68.10   HTTP       550  GET /~rzheng/course/CAS4C03W18/Labs/HTTP/HTTP-wireshark-file5.html HTTP/1.1
    656 32.948944   130.113.68.10   192.168.2.140   HTTP       477  HTTP/1.1 200 OK  (text/html)
    671 43.496352   192.168.2.140   130.113.68.10   HTTP       476  GET /favicon.ico HTTP/1.1
    677 43.534328   130.113.68.10   192.168.2.140   HTTP      1241  HTTP/1.1 200 OK  (text/plain)
```

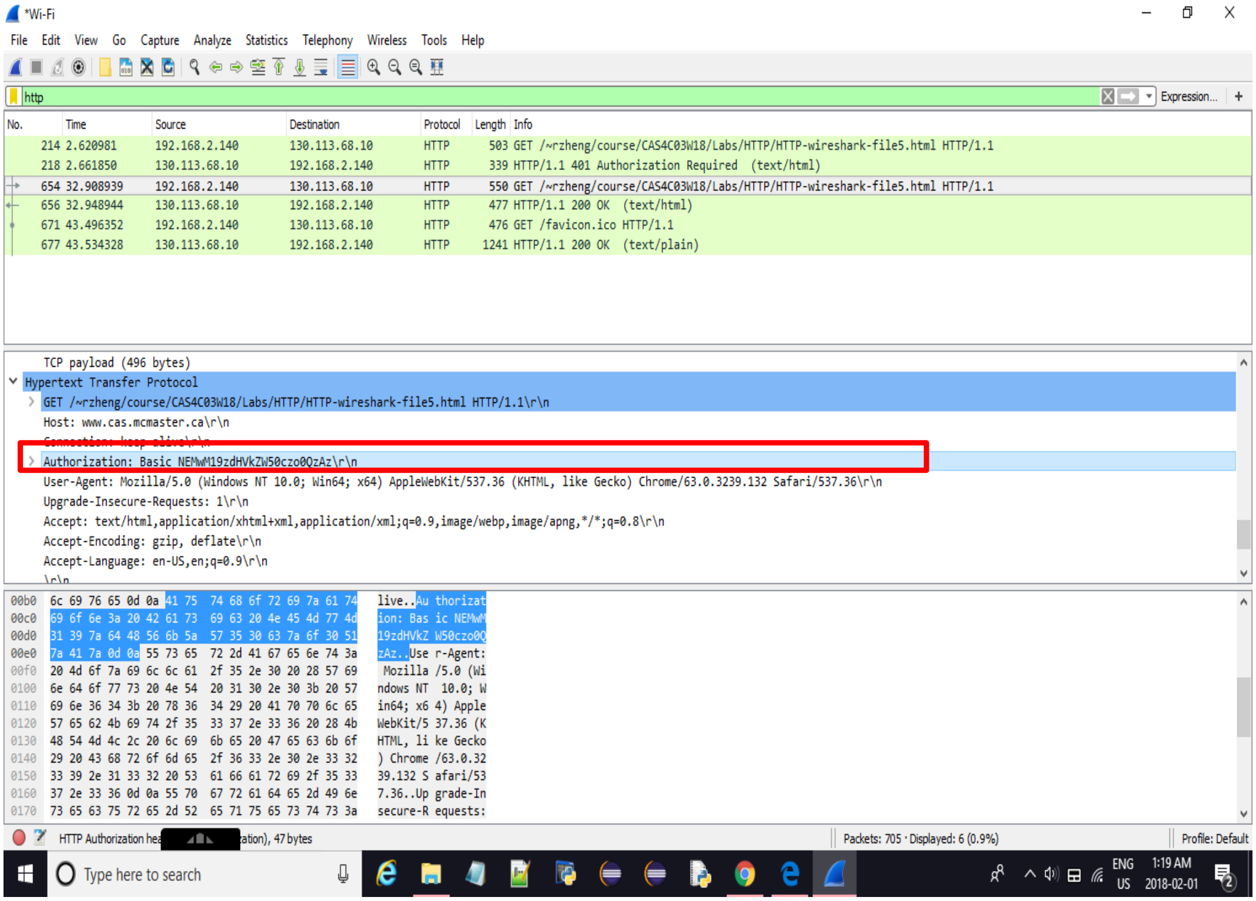
```
> Frame 218: 339 bytes on wire (2712 bits), 339 bytes captured (2712 bits) on interface 0
> Ethernet II, Src: Sagemcom_44:98:11 (f0:82:61:44:98:11), Dst: IntelCor_8d:ee:ba (60:36:dd:8d:ee:ba)
> Internet Protocol Version 4, Src: 130.113.68.10, Dst: 192.168.2.140
> Transmission Control Protocol, Src Port: 80, Dst Port: 58317, Seq: 1, Ack: 450, Len: 285
> Hypertext Transfer Protocol
> Line-based text data: text/html
```

```
0000  60 36 dd 8d ee ba f0 82  61 44 98 11 08 00 45 08   `6...... aD....E.
0010  01 45 c4 d7 40 00 31 06  fa 23 82 71 44 0a c0 a8   .E..@.1. .#.qD...
0020  02 8c 00 50 e3 cd b4 0d  06 81 35 0c 06 8f 50 18   ...P.... ..5...P.
0030  00 36 4d 60 00 00 48 54  54 50 2f 31 2e 31 20 34   .6M`..HT TP/1.1 4
0040  30 31 20 41 75 74 68 6f  72 69 7a 61 74 69 6f 6e   01 Autho rization
0050  20 52 65 71 75 69 72 65  64 0d 0a 44 61 74 65 3a    Require d..Date:
0060  20 54 68 75 2c 20 30 31  20 46 65 62 20 32 30 31    Thu, 01  Feb 201
0070  38 20 30 36 3a 31 32 3a  33 33 20 47 4d 54 0d 0a   8 06:12: 33 GMT..
0080  53 65 72 76 65 72 3a 20  41 70 61 63 68 65 0d 0a   Server:  Apache..
0090  57 57 57 2d 41 75 74 68  65 6e 74 69 63 61 74 65   WWW-Auth enticate
00a0  3a 20 42 61 73 69 63 20  72 65 61 6c 6d 3d 22 52   : Basic  realm="R
00b0  65 73 74 72 69 63 74 65  64 20 41 72 65 61 22 0d   estricte d Area".
00c0  0a 43 6f 6e 74 65 6e 74  2d 4c 65 6e 67 74 68 3a   .Content -Length:
```

wireshark_05EEFA6F-3[redacted]762A3F92FDF_20180201011227_a12080 Packets: 705 · Displayed: 6 (0.9%) Profile: Default

The server’s response: 401 Authorization required

19.



*Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http

```
No.     Time        Source          Destination     Protocol Length Info
    214 2.620981    192.168.2.140   130.113.68.10   HTTP      503 GET /~rzheng/course/CAS4C03W18/Labs/HTTP/HTTP-wireshark-file5.html HTTP/1.1
    218 2.661850    130.113.68.10   192.168.2.140   HTTP      339 HTTP/1.1 401 Authorization Required  (text/html)
    654 32.908939   192.168.2.140   130.113.68.10   HTTP      550 GET /~rzheng/course/CAS4C03W18/Labs/HTTP/HTTP-wireshark-file5.html HTTP/1.1
    656 32.948944   130.113.68.10   192.168.2.140   HTTP      477 HTTP/1.1 200 OK  (text/html)
    671 43.496352   192.168.2.140   130.113.68.10   HTTP      476 GET /favicon.ico HTTP/1.1
    677 43.534328   130.113.68.10   192.168.2.140   HTTP     1241 HTTP/1.1 200 OK  (text/plain)
```

```
    TCP payload (496 bytes)
  Hypertext Transfer Protocol
  > GET /~rzheng/course/CAS4C03W18/Labs/HTTP/HTTP-wireshark-file5.html HTTP/1.1\r\n
    Host: www.cas.mcmaster.ca\r\n
    Connection: keep-alive\r\n
  > Authorization: Basic NEMwM19zdHVkZW50czo0QzAz\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/63.0.3239.132 Safari/537.36\r\n
    Upgrade-Insecure-Requests: 1\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8\r\n
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: en-US,en;q=0.9\r\n
    \r\n
```

```
00b0  6c 69 76 65 0d 0a 41 75  74 68 6f 72 69 7a 61 74   live..Au thorizat
00c0  69 6f 6e 3a 20 42 61 73  69 63 20 4e 45 4d 77 4d   ion: Bas ic NEMwM
00d0  31 39 7a 64 48 56 6b 5a  57 35 30 63 7a 6f 30 51   19zdHVkZ W50czo0Q
00e0  7a 41 7a 0d 0a 55 73 65  72 2d 41 67 65 6e 74 3a   zAz..Use r-Agent:
00f0  20 4d 6f 7a 69 6c 6c 61  2f 35 2e 30 20 28 57 69    Mozilla /5.0 (Wi
0100  6e 64 6f 77 73 20 4e 54  20 31 30 2e 30 3b 20 57   ndows NT  10.0; W
0110  69 6e 36 34 3b 20 78 36  34 29 20 41 70 70 6c 65   in64; x6 4) Apple
0120  57 65 62 4b 69 74 2f 35  33 37 2e 33 36 20 28 4b   WebKit/5 37.36 (K
0130  48 54 4d 4c 2c 20 6c 69  6b 65 20 47 65 63 6b 6f   HTML, li ke Gecko
0140  29 20 43 68 72 6f 6d 65  2f 36 33 2e 30 2e 33 32   ) Chrome /63.0.32
0150  33 39 2e 31 33 32 20 53  61 66 61 72 69 2f 35 33   39.132 S afari/53
0160  37 2e 33 36 0d 0a 55 70  67 72 61 64 65 2d 49 6e   7.36..Up grade-In
0170  73 65 63 75 72 65 2d 52  65 71 75 65 73 74 73 3a   secure-R equests:
```

HTTP Authorization hea[redacted]ation), 47 bytes | Packets: 705 · Displayed: 6 (0.9%) | Profile: Default

The new field that is now included is the authorization field. This happened because we sent the username and password along with our request to the server to ask for the authorization of the page.