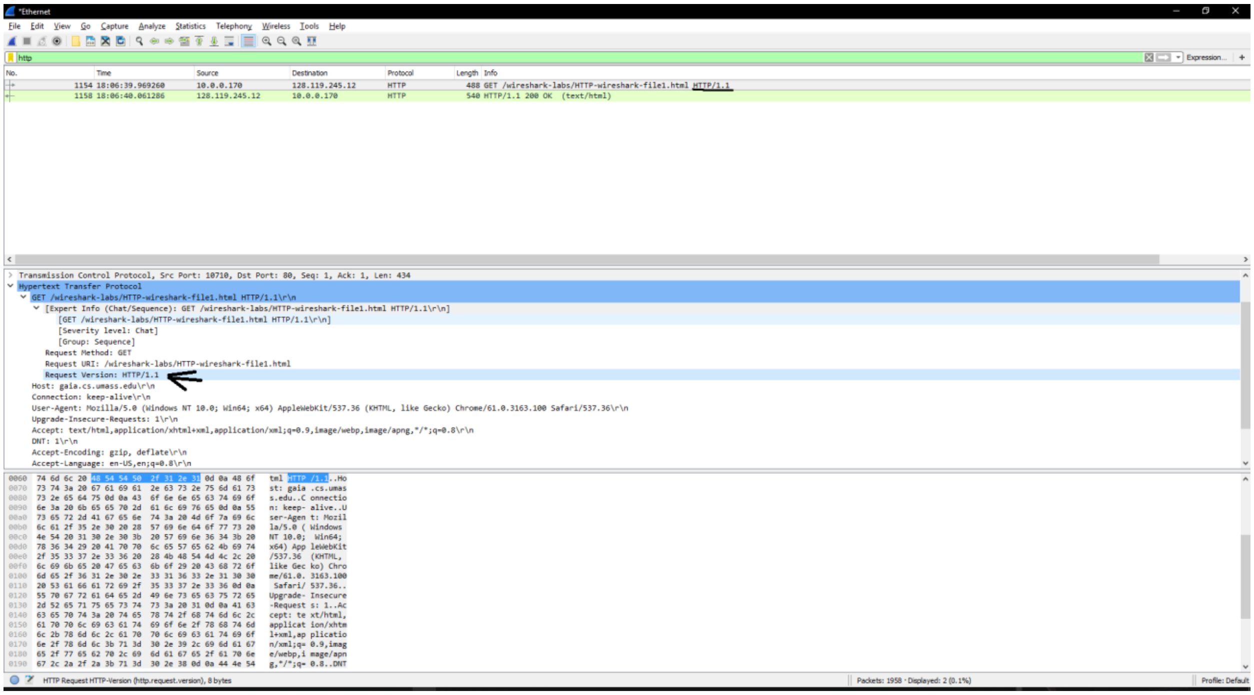
Brandon Lo

CS372 Lab 2

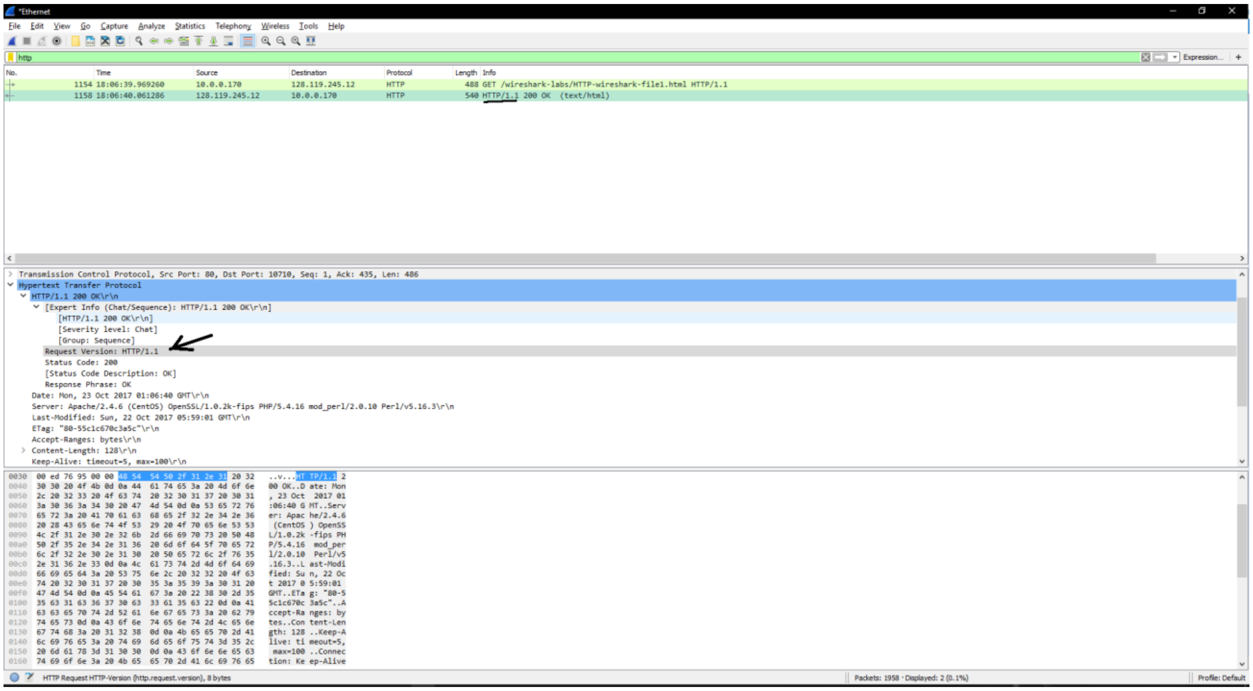
1. My browser is running HTTP version 1.1
   The server is also shown running HTTP version 1.1


*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
Expression...
HTTP Request HTTP-Version (http.request.version), 8 bytes
Packets: 1958 · Displayed: 2 (0.1%)
Profile: Default

```
No.        Time              Source          Destination      Protocol   Length Info
     1154 18:06:39.969260   10.0.0.170      128.119.245.12   HTTP         488 GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
     1158 18:06:40.061286   128.119.245.12  10.0.0.170       HTTP         540 HTTP/1.1 200 OK  (text/html)
```

```
> Transmission Control Protocol, Src Port: 10710, Dst Port: 80, Seq: 1, Ack: 1, Len: 434
v Hypertext Transfer Protocol
  v GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n
    v [Expert Info (Chat/Sequence): GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n]
        [GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n]
        [Severity level: Chat]
        [Group: Sequence]
      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
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/61.0.3163.100 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
    DNT: 1\r\n
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: en-US,en;q=0.8\r\n
```

```
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  73 65 72 2d 41 67 65 6e  74 3a 20 4d 6f 7a 69 6c   ser-Agen t: Mozil
00b0  6c 61 2f 35 2e 30 20 28  57 69 6e 64 6f 77 73 20   la/5.0 ( Windows 
00c0  4e 54 20 31 30 2e 30 3b  20 57 69 6e 36 34 3b 20   NT 10.0;  Win64; 
00d0  78 36 34 29 20 41 70 70  6c 65 57 65 62 4b 69 74   x64) App leWebKit
00e0  2f 35 33 37 2e 33 36 20  28 4b 48 54 4d 4c 2c 20   /537.36  (KHTML, 
00f0  6c 69 6b 65 20 47 65 63  6b 6f 29 20 43 68 72 6f   like Gec ko) Chro
0100  6d 65 2f 36 31 2e 30 2e  33 31 36 33 2e 31 30 30   me/61.0. 3163.100
0110  20 53 61 66 61 72 69 2f  35 33 37 2e 33 36 0d 0a    Safari/ 537.36..
0120  55 70 67 72 61 64 65 2d  49 6e 73 65 63 75 72 65   Upgrade- Insecure
0130  2d 52 65 71 75 65 73 74  73 3a 20 31 0d 0a 41 63   -Request s: 1..Ac
0140  63 65 70 74 3a 20 74 65  78 74 2f 68 74 6d 6c 2c   cept: te xt/html,
0150  61 70 70 6c 69 63 61 74  69 6f 6e 2f 78 68 74 6d   applicat ion/xhtm
0160  6c 2b 78 6d 6c 2c 61 70  70 6c 69 63 61 74 69 6f   l+xml,ap plicatio
0170  6e 2f 78 6d 6c 3b 71 3d  30 2e 39 2c 69 6d 61 67   n/xml;q= 0.9,imag
0180  65 2f 77 65 62 70 2c 69  6d 61 67 65 2f 61 70 6e   e/webp,i mage/apn
0190  67 2c 2a 2f 2a 3b 71 3d  30 2e 38 0d 0a 44 4e 54   g,*/*;q= 0.8..DNT
```

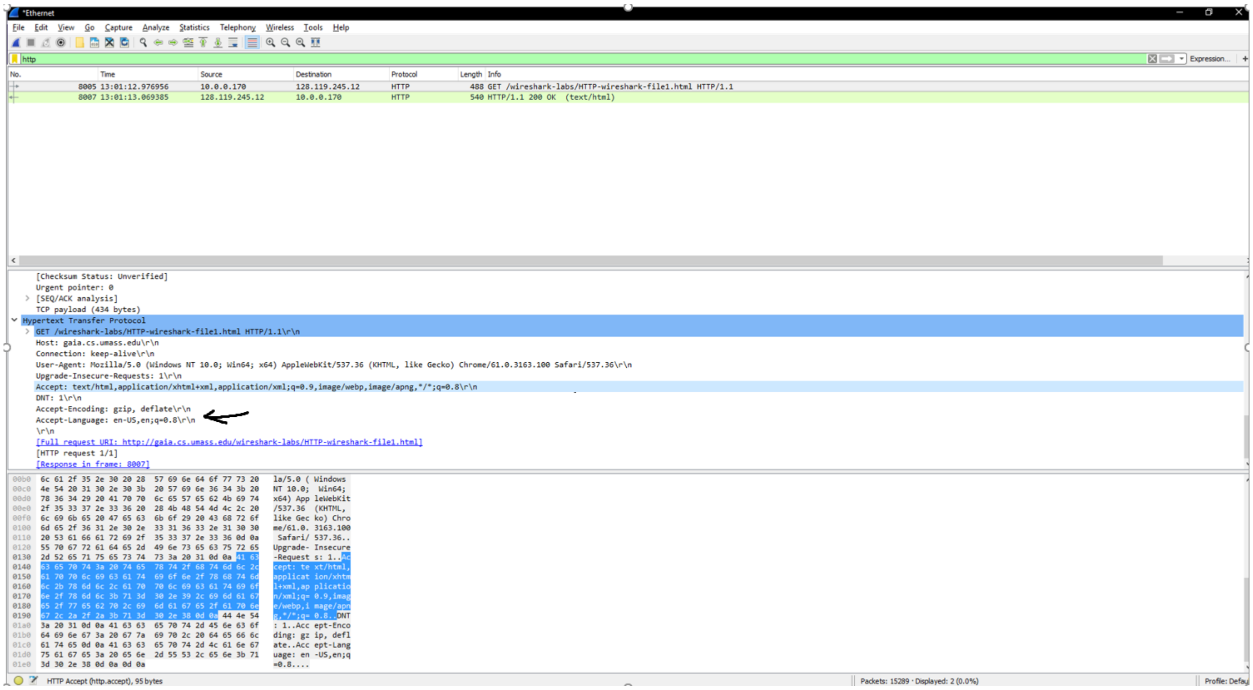

*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
Expression...
HTTP Request HTTP-Version (http.request.version), 8 bytes
Packets: 1958 · Displayed: 2 (0.1%)
Profile: Default

```
No.        Time              Source          Destination      Protocol   Length Info
     1154 18:06:39.969260   10.0.0.170      128.119.245.12   HTTP         488 GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
     1158 18:06:40.061286   128.119.245.12  10.0.0.170       HTTP         540 HTTP/1.1 200 OK  (text/html)
```

```
> Transmission Control Protocol, Src Port: 80, Dst Port: 10710, Seq: 1, Ack: 435, Len: 486
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: Mon, 23 Oct 2017 01:06:40 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/5.4.16 mod_perl/2.0.10 Perl/v5.16.3\r\n
    Last-Modified: Sun, 22 Oct 2017 05:59:01 GMT\r\n
    ETag: "80-55c1c670c3a5c"\r\n
    Accept-Ranges: bytes\r\n
  > Content-Length: 128\r\n
    Keep-Alive: timeout=5, max=100\r\n
```

```
0030  00 ed 76 95 00 00 48 54  54 50 2f 31 2e 31 20 32   ..v...HT TP/1.1 2
0040  30 30 20 4f 4b 0d 0a 44  61 74 65 3a 20 4d 6f 6e   00 OK..D ate: Mon
0050  2c 20 32 33 20 4f 63 74  20 32 30 31 37 20 30 31   , 23 Oct  2017 01
0060  3a 30 36 3a 34 30 20 47  4d 54 0d 0a 53 65 72 76   :06:40 G MT..Serv
0070  65 72 3a 20 41 70 61 63  68 65 2f 32 2e 34 2e 36   er: Apac he/2.4.6
0080  20 28 43 65 6e 74 4f 53  29 20 4f 70 65 6e 53 53    (CentOS ) OpenSS
0090  4c 2f 31 2e 30 2e 32 6b  2d 66 69 70 73 20 50 48   L/1.0.2k -fips PH
00a0  50 2f 35 2e 34 2e 31 36  20 6d 6f 64 5f 70 65 72   P/5.4.16  mod_per
00b0  6c 2f 32 2e 30 2e 31 30  20 50 65 72 6c 2f 76 35   l/2.0.10  Perl/v5
00c0  2e 31 36 2e 33 0d 0a 4c  61 73 74 2d 4d 6f 64 69   .16.3..L ast-Modi
00d0  66 69 65 64 3a 20 53 75  6e 2c 20 32 32 20 4f 63   fied: Su n, 22 Oc
00e0  74 20 32 30 31 37 20 30  35 3a 35 39 3a 30 31 20   t 2017 0 5:59:01 
00f0  47 4d 54 0d 0a 45 54 61  67 3a 20 22 38 30 2d 35   GMT..ETa g: "80-5
0100  35 63 31 63 36 37 30 63  33 61 35 63 22 0d 0a 41   5c1c670c 3a5c"..A
0110  63 63 65 70 74 2d 52 61  6e 67 65 73 3a 20 62 79   ccept-Ra nges: by
0120  74 65 73 0d 0a 43 6f 6e  74 65 6e 74 2d 4c 65 6e   tes..Con tent-Len
0130  67 74 68 3a 20 31 32 38  0d 0a 4b 65 65 70 2d 41   gth: 128 ..Keep-A
0140  6c 69 76 65 3a 20 74 69  6d 65 6f 75 74 3d 35 2c   live: ti meout=5,
0150  20 6d 61 78 3d 31 30 30  0d 0a 43 6f 6e 6e 65 63    max=100 ..Connec
0160  74 69 6f 6e 3a 20 4b 65  65 70 2d 41 6c 69 76 65   tion: Ke ep-Alive
```

2. The languages that the server can accept is en-US (US English).



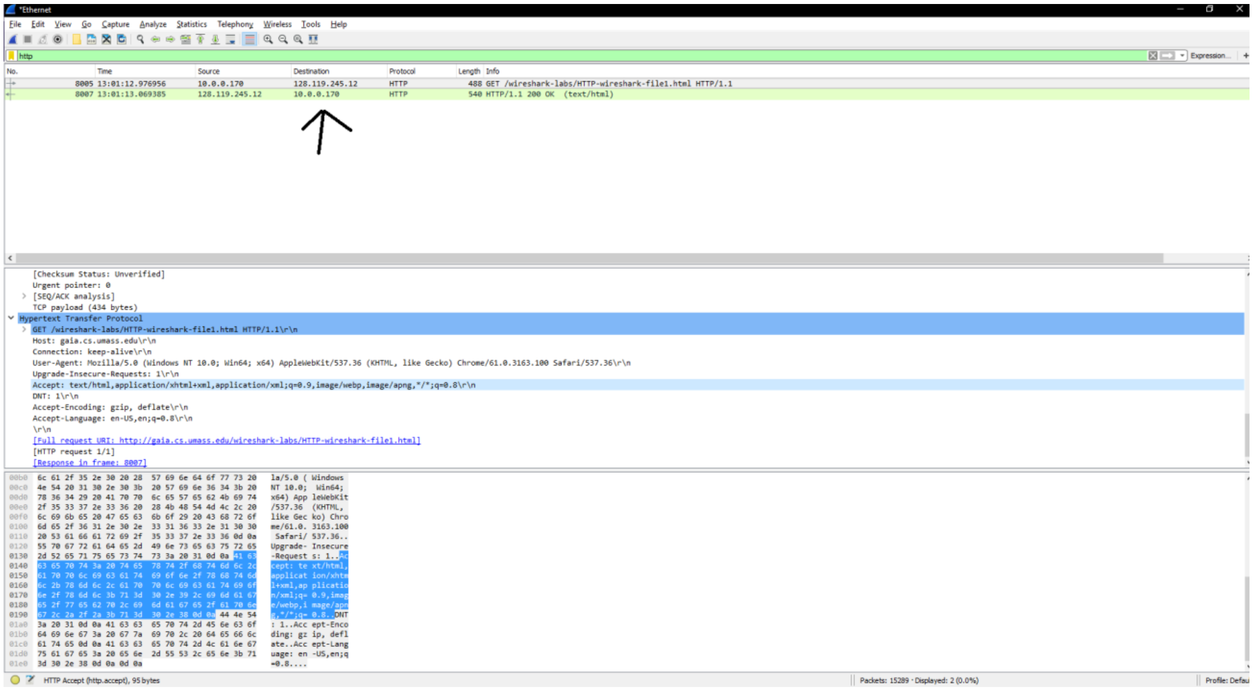
```
http

No.   Time              Source          Destination     Protocol  Length Info
 8005 13:01:12.976956   10.0.0.170      128.119.245.12  HTTP      488 GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
 8007 13:01:13.069385   128.119.245.12  10.0.0.170      HTTP      540 HTTP/1.1 200 OK  (text/html)
```

```
    [Checksum Status: Unverified]
    Urgent pointer: 0
  > [SEQ/ACK analysis]
    TCP payload (434 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
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/61.0.3163.100 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
    DNT: 1\r\n
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: en-US,en;q=0.8\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: 8007]
```

```
00b0  6c 61 2f 35 2e 30 20 28  57 69 6e 64 6f 77 73 20   la/5.0 ( Windows
00c0  4e 54 20 31 30 2e 30 3b  20 57 69 6e 36 34 3b 20   NT 10.0;  Win64;
00d0  78 36 34 29 20 41 70 70  6c 65 57 65 62 4b 69 74   x64) App leWebKit
00e0  2f 35 33 37 2e 33 36 20  28 4b 48 54 4d 4c 2c 20   /537.36  (KHTML,
00f0  6c 69 6b 65 20 47 65 63  6b 6f 29 20 43 68 72 6f   like Gec ko) Chro
0100  6d 65 2f 36 31 2e 30 2e  33 31 36 33 2e 31 30 30   me/61.0. 3163.100
0110  20 53 61 66 61 72 69 2f  35 33 37 2e 33 36 0d 0a    Safari/ 537.36..
0120  55 70 67 72 61 64 65 2d  49 6e 73 65 63 75 72 65   Upgrade- Insecure
0130  2d 52 65 71 75 65 73 74  73 3a 20 31 0d 0a 41 63   -Request s: 1..Ac
0140  63 65 70 74 3a 20 74 65  78 74 2f 68 74 6d 6c 2c   cept: te xt/html,
0150  61 70 70 6c 69 63 61 74  69 6f 6e 2f 78 68 74 6d   applicat ion/xhtm
0160  6c 2b 78 6d 6c 2c 61 70  70 6c 69 63 61 74 69 6f   l+xml,ap plicatio
0170  6e 2f 78 6d 6c 3b 71 3d  30 2e 39 2c 69 6d 61 67   n/xml;q= 0.9,imag
0180  65 2f 77 65 62 70 2c 69  6d 61 67 65 2f 61 70 6e   e/webp,i mage/apn
0190  67 2c 2a 2f 2a 3b 71 3d  30 2e 38 0d 0a 44 4e 54   g,*/*;q= 0.8..DNT
01a0  3a 20 31 0d 0a 41 63 63  65 70 74 2d 45 6e 63 6f   : 1..Acc ept-Enco
01b0  64 69 6e 67 3a 20 67 7a  69 70 2c 20 64 65 66 6c   ding: gz ip, defl
01c0  61 74 65 0d 0a 41 63 63  65 70 74 2d 4c 61 6e 67   ate..Acc ept-Lang
01d0  75 61 67 65 3a 20 65 6e  2d 55 53 2c 65 6e 3b 71   uage: en -US,en;q
01e0  3d 30 2e 38 0d 0a 0d 0a                            =0.8....
```

```
HTTP Accept (http.accept), 95 bytes        Packets: 15289 · Displayed: 2 (0.0%)        Profile: Defau
```

3. The IP address of my computer is 10.0.0.170
The IP address of the gaia.cs.umass.edu server is 128.119.245.12



*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expression…

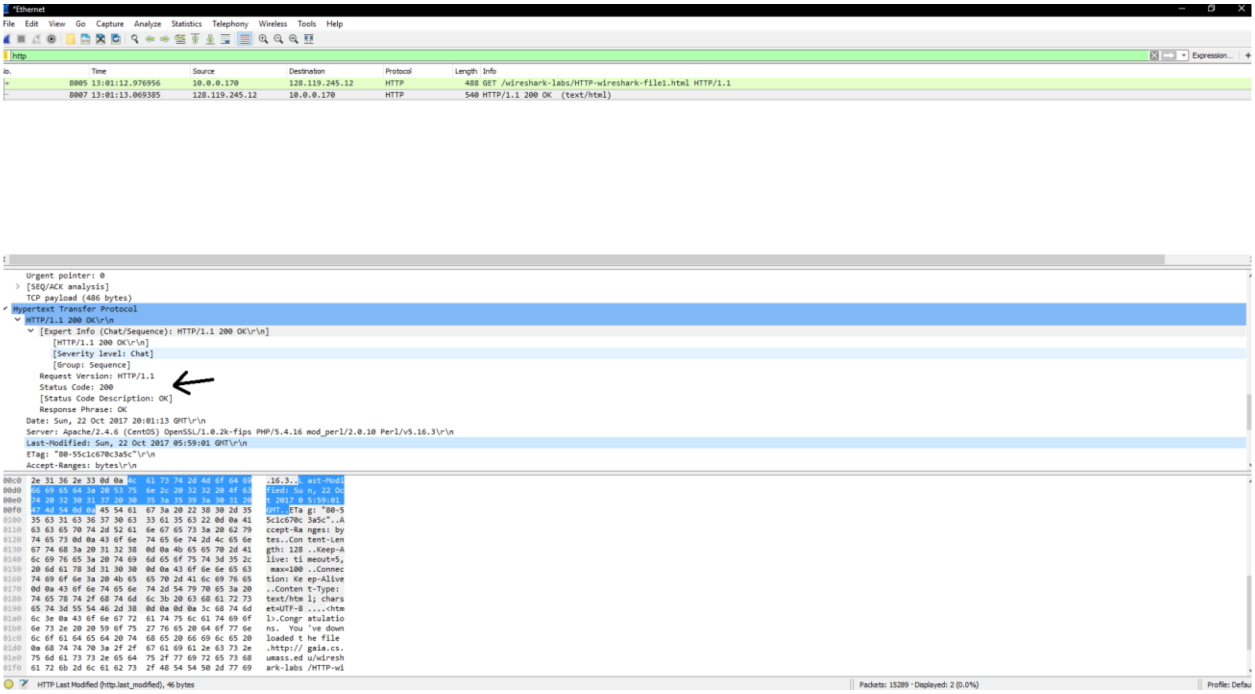
```
http

No.   Time              Source          Destination     Protocol  Length Info
 8005 13:01:12.976956   10.0.0.170      128.119.245.12  HTTP      488 GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
 8007 13:01:13.069385   128.119.245.12  10.0.0.170      HTTP      540 HTTP/1.1 200 OK  (text/html)
```

```
    [Checksum Status: Unverified]
    Urgent pointer: 0
  > [SEQ/ACK analysis]
    TCP payload (434 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
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/61.0.3163.100 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
    DNT: 1\r\n
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: en-US,en;q=0.8\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: 8007]
```

```
00b0  6c 61 2f 35 2e 30 20 28  57 69 6e 64 6f 77 73 20   la/5.0 ( Windows
00c0  4e 54 20 31 30 2e 30 3b  20 57 69 6e 36 34 3b 20   NT 10.0;  Win64;
00d0  78 36 34 29 20 41 70 70  6c 65 57 65 62 4b 69 74   x64) App leWebKit
00e0  2f 35 33 37 2e 33 36 20  28 4b 48 54 4d 4c 2c 20   /537.36  (KHTML,
00f0  6c 69 6b 65 20 47 65 63  6b 6f 29 20 43 68 72 6f   like Gec ko) Chro
0100  6d 65 2f 36 31 2e 30 2e  33 31 36 33 2e 31 30 30   me/61.0. 3163.100
0110  20 53 61 66 61 72 69 2f  35 33 37 2e 33 36 0d 0a    Safari/ 537.36..
0120  55 70 67 72 61 64 65 2d  49 6e 73 65 63 75 72 65   Upgrade- Insecure
0130  2d 52 65 71 75 65 73 74  73 3a 20 31 0d 0a 41 63   -Request s: 1..Ac
0140  63 65 70 74 3a 20 74 65  78 74 2f 68 74 6d 6c 2c   cept: te xt/html,
0150  61 70 70 6c 69 63 61 74  69 6f 6e 2f 78 68 74 6d   applicat ion/xhtm
0160  6c 2b 78 6d 6c 2c 61 70  70 6c 69 63 61 74 69 6f   l+xml,ap plicatio
0170  6e 2f 78 6d 6c 3b 71 3d  30 2e 39 2c 69 6d 61 67   n/xml;q= 0.9,imag
0180  65 2f 77 65 62 70 2c 69  6d 61 67 65 2f 61 70 6e   e/webp,i mage/apn
0190  67 2c 2a 2f 2a 3b 71 3d  30 2e 38 0d 0a 44 4e 54   g,*/*;q= 0.8..DNT
01a0  3a 20 31 0d 0a 41 63 63  65 70 74 2d 45 6e 63 6f   : 1..Acc ept-Enco
01b0  64 69 6e 67 3a 20 67 7a  69 70 2c 20 64 65 66 6c   ding: gz ip, defl
01c0  61 74 65 0d 0a 41 63 63  65 70 74 2d 4c 61 6e 67   ate..Acc ept-Lang
01d0  75 61 67 65 3a 20 65 6e  2d 55 53 2c 65 6e 3b 71   uage: en -US,en;q
01e0  3d 30 2e 38 0d 0a 0d 0a                            =0.8....
```

```
HTTP Accept (http.accept), 95 bytes        Packets: 15289 · Displayed: 2 (0.0%)        Profile: Defau
```

4. The status code returned from the server to my browser is 200.


*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
Expression…

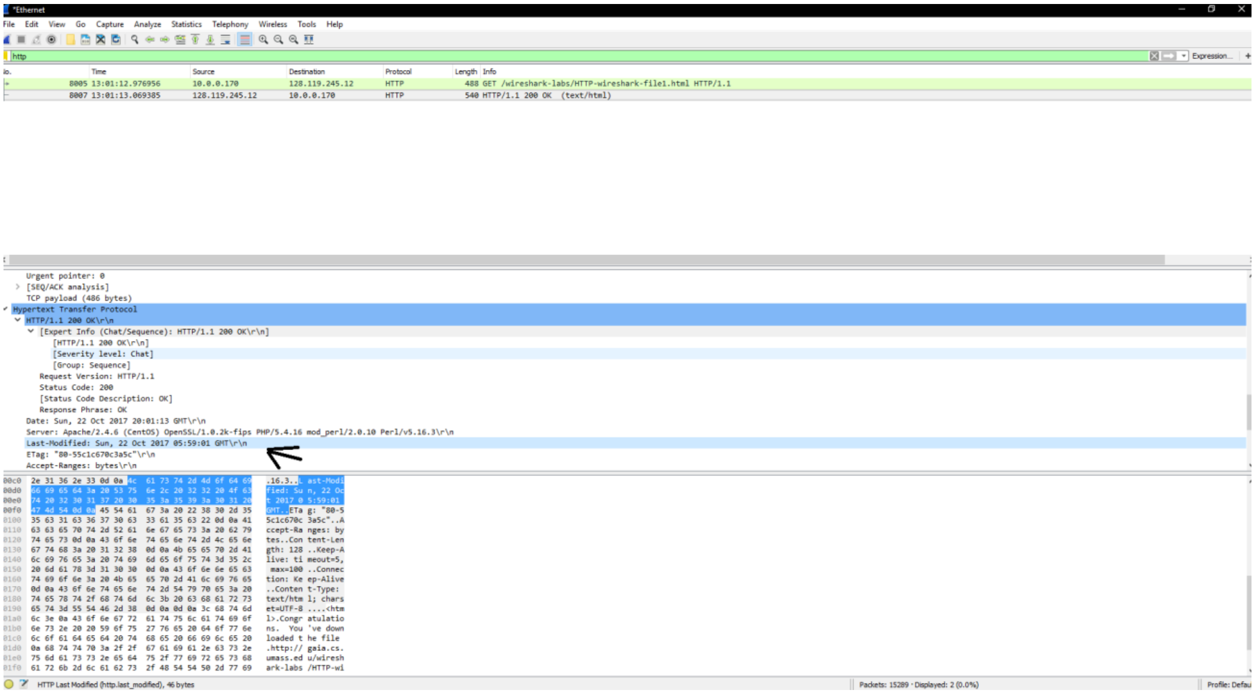
```
No.      Time              Source          Destination     Protocol  Length Info
   8005 13:01:12.976956   10.0.0.170      128.119.245.12  HTTP         488 GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
   8007 13:01:13.069385   128.119.245.12  10.0.0.170      HTTP         540 HTTP/1.1 200 OK  (text/html)
```

```
    Urgent pointer: 0
  > [SEQ/ACK analysis]
    TCP payload (486 bytes)
✓ Hypertext Transfer Protocol
  ✓ HTTP/1.1 200 OK\r\n
    ✓ [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: Sun, 22 Oct 2017 20:01:13 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/5.4.16 mod_perl/2.0.10 Perl/v5.16.3\r\n
    Last-Modified: Sun, 22 Oct 2017 05:59:01 GMT\r\n
    ETag: "80-55c1c670c3a5c"\r\n
    Accept-Ranges: bytes\r\n
```

```
00c0  2e 31 36 2e 33 0d 0a 4c  61 73 74 2d 4d 6f 64 69   .16.3..L ast-Modi
00d0  66 69 65 64 3a 20 53 75  6e 2c 20 32 32 20 4f 63   fied: Su n, 22 Oc
00e0  74 20 32 30 31 37 20 30  35 3a 35 39 3a 30 31 20   t 2017 0 5:59:01 
00f0  47 4d 54 0d 0a 45 54 61  67 3a 20 22 38 30 2d 35   GMT..ETa g: "80-5
0100  35 63 31 63 36 37 30 63  33 61 35 63 22 0d 0a 41   5c1c670c 3a5c"..A
0110  63 63 65 70 74 2d 52 61  6e 67 65 73 3a 20 62 79   ccept-Ra nges: by
0120  74 65 73 0d 0a 43 6f 6e  74 65 6e 74 2d 4c 65 6e   tes..Con tent-Len
0130  67 74 68 3a 20 31 32 38  0d 0a 4b 65 65 70 2d 41   gth: 128 ..Keep-A
0140  6c 69 76 65 3a 20 74 69  6d 65 6f 75 74 3d 35 2c   live: ti meout=5,
0150  20 6d 61 78 3d 31 30 30  0d 0a 43 6f 6e 6e 65 63    max=100 ..Connec
0160  74 69 6f 6e 3a 20 4b 65  65 70 2d 41 6c 69 76 65   tion: Ke ep-Alive
0170  0d 0a 43 6f 6e 74 65 6e  74 2d 54 79 70 65 3a 20   ..Conten t-Type: 
0180  74 65 78 74 2f 68 74 6d  6c 3b 20 63 68 61 72 73   text/htm l; chars
0190  65 74 3d 55 54 46 2d 38  0d 0a 0d 0a 3c 68 74 6d   et=UTF-8 ....<htm
01a0  6c 3e 0a 43 6f 6e 67 72  61 74 75 6c 61 74 69 6f   l>.Congr atulatio
01b0  6e 73 2e 20 20 59 6f 75  27 76 65 20 64 6f 77 6e   ns.  You 've down
01c0  6c 6f 61 64 65 64 20 74  68 65 20 66 69 6c 65 20   loaded t he file 
01d0  0a 68 74 74 70 3a 2f 2f  67 61 69 61 2e 63 73 2e   .http:// gaia.cs.
01e0  75 6d 61 73 73 2e 65 64  75 2f 77 69 72 65 73 68   umass.ed u/wiresh
01f0  61 72 6b 2d 6c 61 62 73  2f 48 54 54 50 2d 77 69   ark-labs /HTTP-wi
```

HTTP Last Modified (http.last_modified), 46 bytes | Packets: 15289 · Displayed: 2 (0.0%) | Profile: Defau

5. The HTML file was last modified Sunday, 22 October 2017 05:59:01 GMT


*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
Expression…

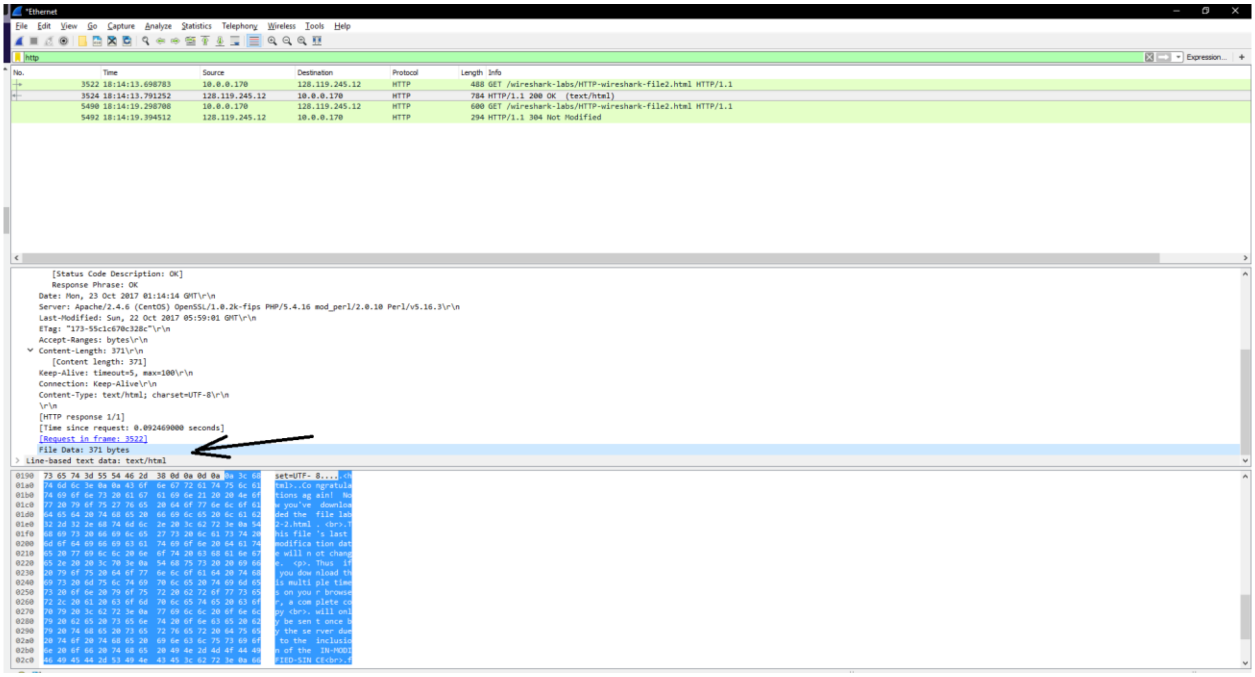
```
No.      Time              Source          Destination     Protocol  Length Info
   8005 13:01:12.976956   10.0.0.170      128.119.245.12  HTTP         488 GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
   8007 13:01:13.069385   128.119.245.12  10.0.0.170      HTTP         540 HTTP/1.1 200 OK  (text/html)
```

```
    Urgent pointer: 0
  > [SEQ/ACK analysis]
    TCP payload (486 bytes)
✓ Hypertext Transfer Protocol
  ✓ HTTP/1.1 200 OK\r\n
    ✓ [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: Sun, 22 Oct 2017 20:01:13 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/5.4.16 mod_perl/2.0.10 Perl/v5.16.3\r\n
    Last-Modified: Sun, 22 Oct 2017 05:59:01 GMT\r\n
    ETag: "80-55c1c670c3a5c"\r\n
    Accept-Ranges: bytes\r\n
```

```
00c0  2e 31 36 2e 33 0d 0a 4c  61 73 74 2d 4d 6f 64 69   .16.3..L ast-Modi
00d0  66 69 65 64 3a 20 53 75  6e 2c 20 32 32 20 4f 63   fied: Su n, 22 Oc
00e0  74 20 32 30 31 37 20 30  35 3a 35 39 3a 30 31 20   t 2017 0 5:59:01 
00f0  47 4d 54 0d 0a 45 54 61  67 3a 20 22 38 30 2d 35   GMT..ETa g: "80-5
0100  35 63 31 63 36 37 30 63  33 61 35 63 22 0d 0a 41   5c1c670c 3a5c"..A
0110  63 63 65 70 74 2d 52 61  6e 67 65 73 3a 20 62 79   ccept-Ra nges: by
0120  74 65 73 0d 0a 43 6f 6e  74 65 6e 74 2d 4c 65 6e   tes..Con tent-Len
0130  67 74 68 3a 20 31 32 38  0d 0a 4b 65 65 70 2d 41   gth: 128 ..Keep-A
0140  6c 69 76 65 3a 20 74 69  6d 65 6f 75 74 3d 35 2c   live: ti meout=5,
0150  20 6d 61 78 3d 31 30 30  0d 0a 43 6f 6e 6e 65 63    max=100 ..Connec
0160  74 69 6f 6e 3a 20 4b 65  65 70 2d 41 6c 69 76 65   tion: Ke ep-Alive
0170  0d 0a 43 6f 6e 74 65 6e  74 2d 54 79 70 65 3a 20   ..Conten t-Type: 
0180  74 65 78 74 2f 68 74 6d  6c 3b 20 63 68 61 72 73   text/htm l; chars
0190  65 74 3d 55 54 46 2d 38  0d 0a 0d 0a 3c 68 74 6d   et=UTF-8 ....<htm
01a0  6c 3e 0a 43 6f 6e 67 72  61 74 75 6c 61 74 69 6f   l>.Congr atulatio
01b0  6e 73 2e 20 20 59 6f 75  27 76 65 20 64 6f 77 6e   ns.  You 've down
01c0  6c 6f 61 64 65 64 20 74  68 65 20 66 69 6c 65 20   loaded t he file 
01d0  0a 68 74 74 70 3a 2f 2f  67 61 69 61 2e 63 73 2e   .http:// gaia.cs.
01e0  75 6d 61 73 73 2e 65 64  75 2f 77 69 72 65 73 68   umass.ed u/wiresh
01f0  61 72 6b 2d 6c 61 62 73  2f 48 54 54 50 2d 77 69   ark-labs /HTTP-wi
```

HTTP Last Modified (http.last_modified), 46 bytes | Packets: 15289 · Displayed: 2 (0.0%) | Profile: Defau

6. The file data size is 371 bytes.



*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expression...

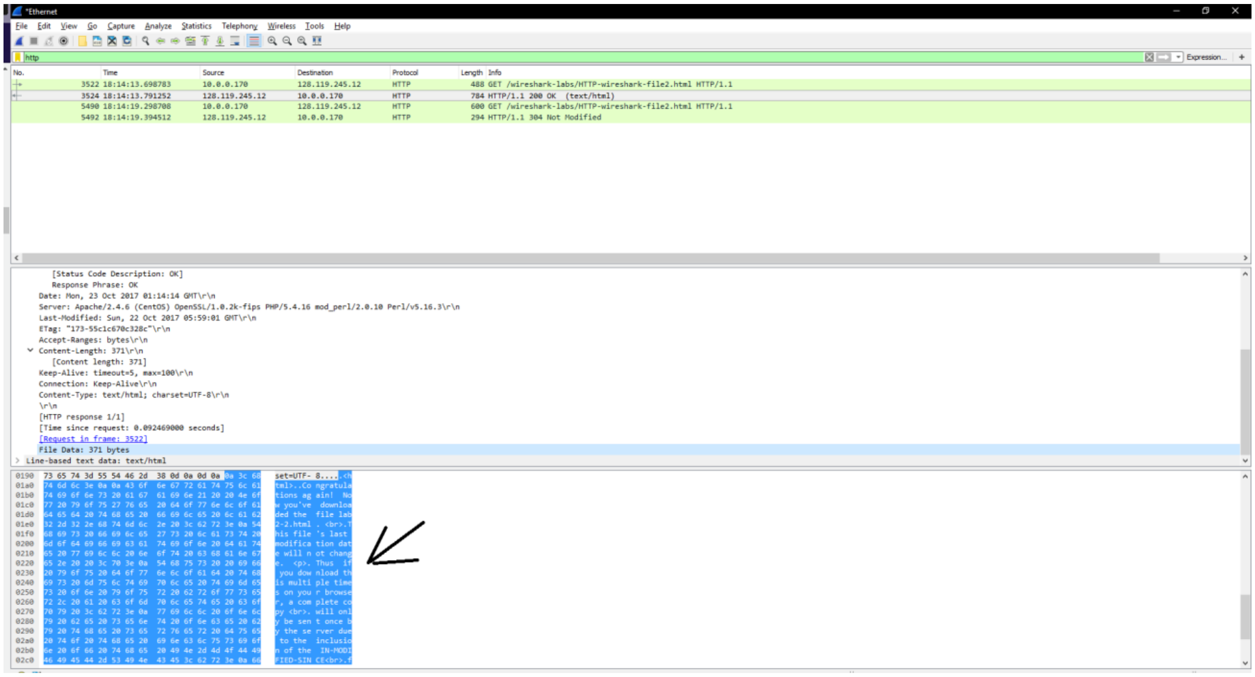
http

```
No.   Time             Source          Destination     Protocol Length Info
 3522 18:14:13.698783  10.0.0.170      128.119.245.12  HTTP      488 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
 3524 18:14:13.791252  128.119.245.12  10.0.0.170      HTTP      784 HTTP/1.1 200 OK  (text/html)
 5490 18:14:19.298708  10.0.0.170      128.119.245.12  HTTP      600 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
 5492 18:14:19.394512  128.119.245.12  10.0.0.170      HTTP      294 HTTP/1.1 304 Not Modified
```

```
      [Status Code Description: OK]
      Response Phrase: OK
    Date: Mon, 23 Oct 2017 01:14:14 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/5.4.16 mod_perl/2.0.10 Perl/v5.16.3\r\n
    Last-Modified: Sun, 22 Oct 2017 05:59:01 GMT\r\n
    ETag: "173-55c1c670c328c"\r\n
    Accept-Ranges: bytes\r\n
  ˅ Content-Length: 371\r\n
      [Content length: 371]
    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 1/1]
    [Time since request: 0.092469000 seconds]
    [Request in frame: 3522]
    File Data: 371 bytes
> Line-based text data: text/html
```

```
0190  73 65 74 3d 55 54 46 2d  38 0d 0a 0d 0a 0a 3c 68   set=UTF- 8.....<h
01a0  74 6d 6c 3e 0a 0a 43 6f  6e 67 72 61 74 75 6c 61   tml>..Co ngratula
01b0  74 69 6f 6e 73 20 61 67  61 69 6e 21 20 20 4e 6f   tions ag ain!  No
01c0  77 20 79 6f 75 27 76 65  20 64 6f 77 6e 6c 6f 61   w you've  downloa
01d0  64 65 64 20 74 68 65 20  66 69 6c 65 20 6c 61 62   ded the  file lab
01e0  32 2d 32 2e 68 74 6d 6c  2e 20 3c 62 72 3e 0a 54   2-2.html . <br>.T
01f0  68 69 73 20 66 69 6c 65  27 73 20 6c 61 73 74 20   his file 's last 
0200  6d 6f 64 69 66 69 63 61  74 69 6f 6e 20 64 61 74   modifica tion dat
0210  65 20 77 69 6c 6c 20 6e  6f 74 20 63 68 61 6e 67   e will n ot chang
0220  65 2e 20 20 3c 70 3e 0a  54 68 75 73 20 20 69 66   e.  <p>. Thus  if
0230  20 79 6f 75 20 64 6f 77  6e 6c 6f 61 64 20 74 68    you dow nload th
0240  69 73 20 6d 75 6c 74 69  70 6c 65 20 74 69 6d 65   is multi ple time
0250  73 20 6f 6e 20 79 6f 75  72 20 62 72 6f 77 73 65   s on you r browse
0260  72 2c 20 61 20 63 6f 6d  70 6c 65 74 65 20 63 6f   r, a com plete co
0270  70 79 20 3c 62 72 3e 0a  77 69 6c 6c 20 6f 6e 6c   py <br>. will onl
0280  79 20 62 65 20 73 65 6e  74 20 6f 6e 63 65 20 62   y be sen t once b
0290  79 20 74 68 65 20 73 65  72 76 65 72 20 64 75 65   y the se rver due
02a0  20 74 6f 20 74 68 65 20  69 6e 63 6c 75 73 69 6f    to the  inclusio
02b0  6e 20 6f 66 20 74 68 65  20 49 4e 2d 4d 4f 44 49   n of the  IN-MODI
02c0  46 49 45 44 2d 53 49 4e  43 45 3c 62 72 3e 0a 66   FIED-SIN CE<br>.f
```

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



*Ethernet

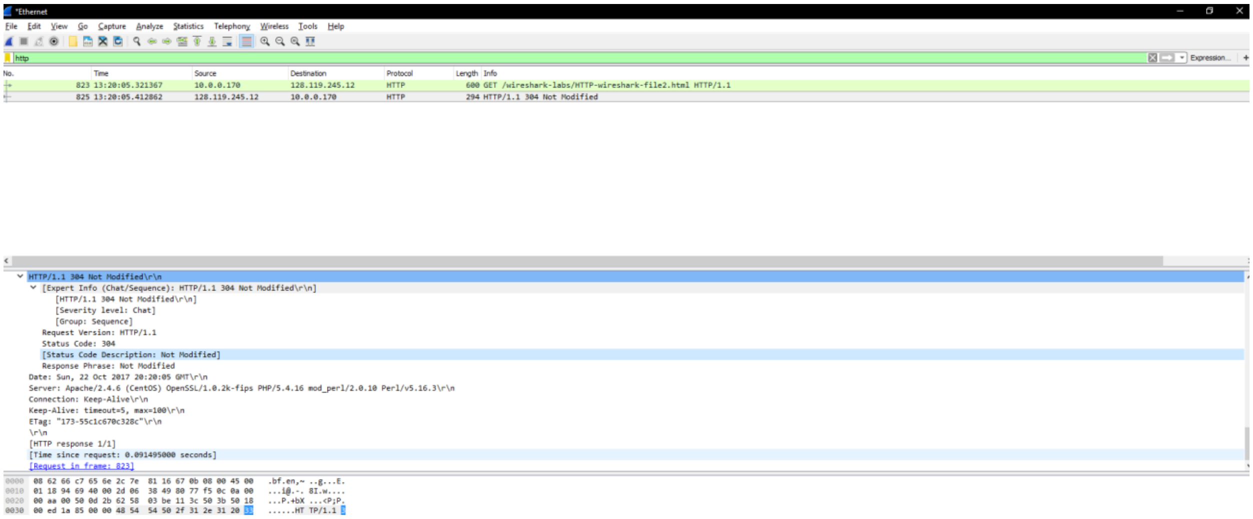
http

```
No.   Time             Source          Destination     Protocol Length Info
 3522 18:14:13.698783  10.0.0.170      128.119.245.12  HTTP      488 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
 3524 18:14:13.791252  128.119.245.12  10.0.0.170      HTTP      784 HTTP/1.1 200 OK  (text/html)
 5490 18:14:19.298708  10.0.0.170      128.119.245.12  HTTP      600 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
 5492 18:14:19.394512  128.119.245.12  10.0.0.170      HTTP      294 HTTP/1.1 304 Not Modified
```

```
      [Status Code Description: OK]
      Response Phrase: OK
    Date: Mon, 23 Oct 2017 01:14:14 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/5.4.16 mod_perl/2.0.10 Perl/v5.16.3\r\n
    Last-Modified: Sun, 22 Oct 2017 05:59:01 GMT\r\n
    ETag: "173-55c1c670c328c"\r\n
    Accept-Ranges: bytes\r\n
  ˅ Content-Length: 371\r\n
      [Content length: 371]
    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 1/1]
    [Time since request: 0.092469000 seconds]
    [Request in frame: 3522]
    File Data: 371 bytes
> Line-based text data: text/html
```

```
0190  73 65 74 3d 55 54 46 2d  38 0d 0a 0d 0a 0a 3c 68   set=UTF- 8.....<h
01a0  74 6d 6c 3e 0a 0a 43 6f  6e 67 72 61 74 75 6c 61   tml>..Co ngratula
01b0  74 69 6f 6e 73 20 61 67  61 69 6e 21 20 20 4e 6f   tions ag ain!  No
01c0  77 20 79 6f 75 27 76 65  20 64 6f 77 6e 6c 6f 61   w you've  downloa
01d0  64 65 64 20 74 68 65 20  66 69 6c 65 20 6c 61 62   ded the  file lab
01e0  32 2d 32 2e 68 74 6d 6c  2e 20 3c 62 72 3e 0a 54   2-2.html . <br>.T
01f0  68 69 73 20 66 69 6c 65  27 73 20 6c 61 73 74 20   his file 's last 
0200  6d 6f 64 69 66 69 63 61  74 69 6f 6e 20 64 61 74   modifica tion dat
0210  65 20 77 69 6c 6c 20 6e  6f 74 20 63 68 61 6e 67   e will n ot chang
0220  65 2e 20 20 3c 70 3e 0a  54 68 75 73 20 20 69 66   e.  <p>. Thus  if
0230  20 79 6f 75 20 64 6f 77  6e 6c 6f 61 64 20 74 68    you dow nload th
0240  69 73 20 6d 75 6c 74 69  70 6c 65 20 74 69 6d 65   is multi ple time
0250  73 20 6f 6e 20 79 6f 75  72 20 62 72 6f 77 73 65   s on you r browse
0260  72 2c 20 61 20 63 6f 6d  70 6c 65 74 65 20 63 6f   r, a com plete co
0270  70 79 20 3c 62 72 3e 0a  77 69 6c 6c 20 6f 6e 6c   py <br>. will onl
0280  79 20 62 65 20 73 65 6e  74 20 6f 6e 63 65 20 62   y be sen t once b
0290  79 20 74 68 65 20 73 65  72 76 65 72 20 64 75 65   y the se rver due
02a0  20 74 6f 20 74 68 65 20  69 6e 63 6c 75 73 69 6f    to the  inclusio
02b0  6e 20 6f 66 20 74 68 65  20 49 4e 2d 4d 4f 44 49   n of the  IN-MODI
02c0  46 49 45 44 2d 53 49 4e  43 45 3c 62 72 3e 0a 66   FIED-SIN CE<br>.f
```

8. No, I do not see an IF-MODIFIED-SINCE

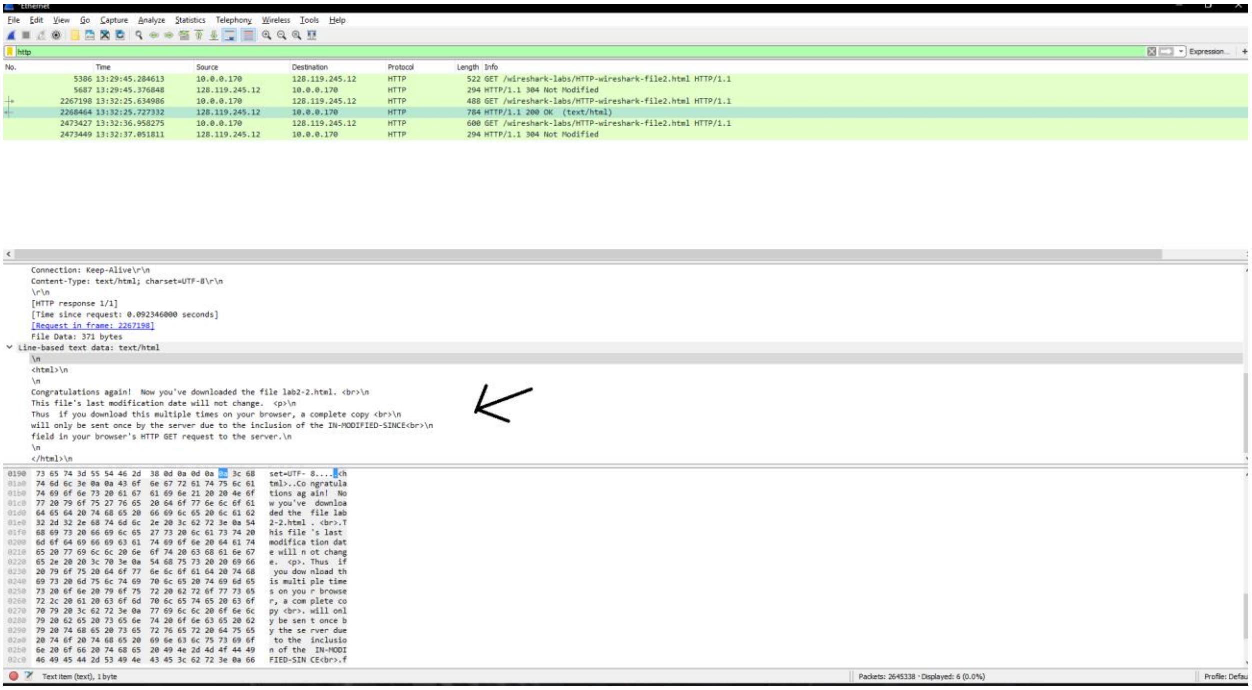

*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expression…

```
http
No.     Time                Source           Destination      Protocol  Length Info
    823 13:20:05.321367     10.0.0.170       128.119.245.12   HTTP         600 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
    825 13:20:05.412862     128.119.245.12   10.0.0.170       HTTP         294 HTTP/1.1 304 Not Modified
```

```
HTTP/1.1 304 Not Modified\r\n
    [Expert Info (Chat/Sequence): HTTP/1.1 304 Not Modified\r\n]
        [HTTP/1.1 304 Not Modified\r\n]
        [Severity level: Chat]
        [Group: Sequence]
    Request Version: HTTP/1.1
    Status Code: 304
    [Status Code Description: Not Modified]
    Response Phrase: Not Modified
Date: Sun, 22 Oct 2017 20:20:05 GMT\r\n
Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/5.4.16 mod_perl/2.0.10 Perl/v5.16.3\r\n
Connection: Keep-Alive\r\n
Keep-Alive: timeout=5, max=100\r\n
ETag: "173-55c1c670c328c"\r\n
\r\n
[HTTP response 1/1]
[Time since request: 0.091495000 seconds]
[Request in frame: 823]
```

```
0000  08 62 66 c7 65 6e 2c 7e  81 16 67 0b 08 00 45 00   .bf.en,~ ..g...E.
0010  01 18 94 69 40 00 2d 06  38 49 80 77 f5 0c 0a 00   ...i@.-. 8I.w....
0020  00 aa 00 50 0d 2b 62 58  03 be 11 3c 50 3b 50 18   ...P.+bX ...<P;P.
0030  00 ed 1a 85 00 00 48 54  54 50 2f 31 2e 31 20 33   ......HT TP/1.1 3
```

9. Yes the server returned the contents of the file since it is returned under the Line-based text data: text/html.

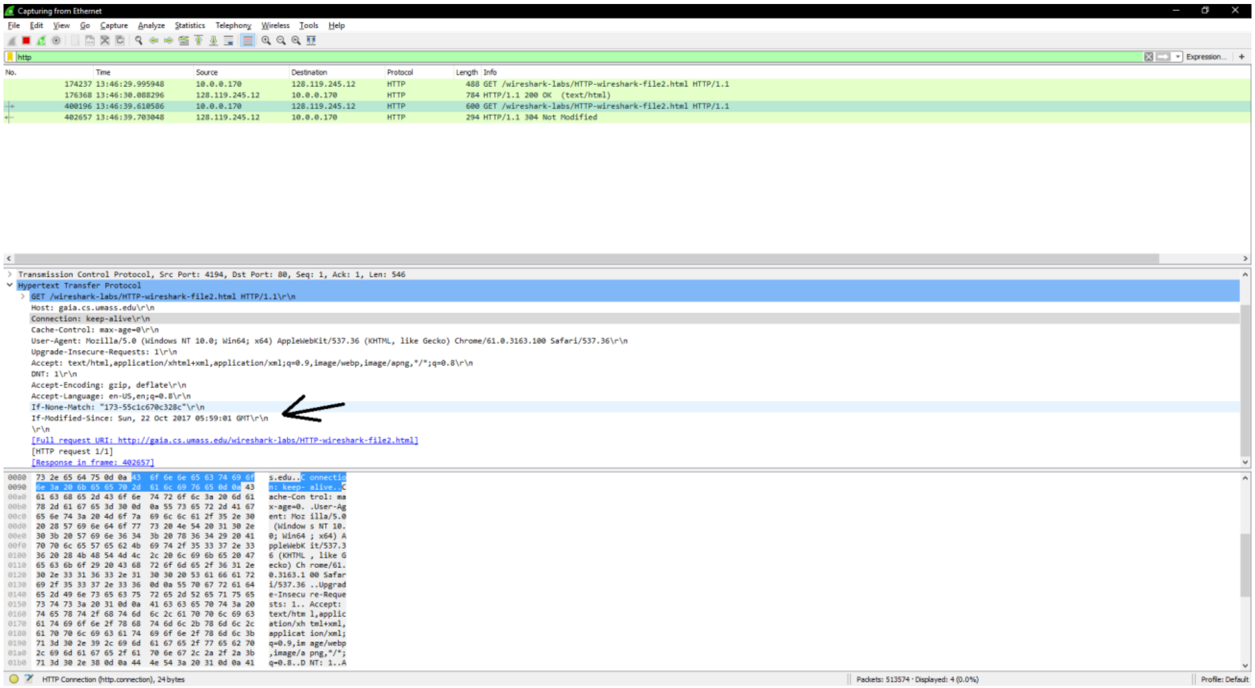

*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expression…

```
http
No.     Time                Source           Destination      Protocol  Length Info
   5386 13:29:45.284613     10.0.0.170       128.119.245.12   HTTP         522 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
   5687 13:29:45.376848     128.119.245.12   10.0.0.170       HTTP         294 HTTP/1.1 304 Not Modified
2267198 13:32:25.634986     10.0.0.170       128.119.245.12   HTTP         488 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
2268464 13:32:25.727332     128.119.245.12   10.0.0.170       HTTP         784 HTTP/1.1 200 OK  (text/html)
2473427 13:32:36.958275     10.0.0.170       128.119.245.12   HTTP         600 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
2473449 13:32:37.051811     128.119.245.12   10.0.0.170       HTTP         294 HTTP/1.1 304 Not Modified
```

```
    Connection: Keep-Alive\r\n
    Content-Type: text/html; charset=UTF-8\r\n
    \r\n
    [HTTP response 1/1]
    [Time since request: 0.092346000 seconds]
    [Request in frame: 2267198]
    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
```

```
0190  73 65 74 3d 55 54 46 2d  38 0d 0a 0d 0a 0a 3c 68   set=UTF- 8.....<h
01a0  74 6d 6c 3e 0a 0a 43 6f  6e 67 72 61 74 75 6c 61   tml>..Co ngratula
01b0  74 69 6f 6e 73 20 61 67  61 69 6e 21 20 20 4e 6f   tions ag ain!  No
01c0  77 20 79 6f 75 27 76 65  20 64 6f 77 6e 6c 6f 61   w you've  downloa
01d0  64 65 64 20 74 68 65 20  66 69 6c 65 20 6c 61 62   ded the  file lab
01e0  32 2d 32 2e 68 74 6d 6c  2e 20 3c 62 72 3e 0a 54   2-2.html . <br>.T
01f0  68 69 73 20 66 69 6c 65  27 73 20 6c 61 73 74 20   his file 's last 
0200  6d 6f 64 69 66 69 63 61  74 69 6f 6e 20 64 61 74   modifica tion dat
0210  65 20 77 69 6c 6c 20 6e  6f 74 20 63 68 61 6e 67   e will n ot chang
0220  65 2e 20 20 3c 70 3e 0a  54 68 75 73 20 20 69 66   e.  <p>. Thus  if
0230  20 79 6f 75 20 64 6f 77  6e 6c 6f 61 64 20 74 68    you dow nload th
0240  69 73 20 6d 75 6c 74 69  70 6c 65 20 74 69 6d 65   is multi ple time
0250  73 20 6f 6e 20 79 6f 75  72 20 62 72 6f 77 73 65   s on you r browse
0260  72 2c 20 61 20 63 6f 6d  70 6c 65 74 65 20 63 6f   r, a com plete co
0270  70 79 20 3c 62 72 3e 0a  77 69 6c 6c 20 6f 6e 6c   py <br>. will onl
0280  79 20 62 65 20 73 65 6e  74 20 6f 6e 63 65 20 62   y be sen t once b
0290  79 20 74 68 65 20 73 65  72 76 65 72 20 64 75 65   y the se rver due
02a0  20 74 6f 20 74 68 65 20  69 6e 63 6c 75 73 69 6f    to the  inclusio
02b0  6e 20 6f 66 20 74 68 65  20 49 4e 2d 4d 4f 44 49   n of the  IN-MODI
02c0  46 49 45 44 2d 53 49 4e  43 45 3c 62 72 3e 0a 66   FIED-SIN CE<br>.f
```

10. Yes, the IF-MODIFIED-SINCE header in the HTTP GET return the modified date as Sunday, 22 October 2017 05:59:01 GMT.


Capturing from Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
Expression...

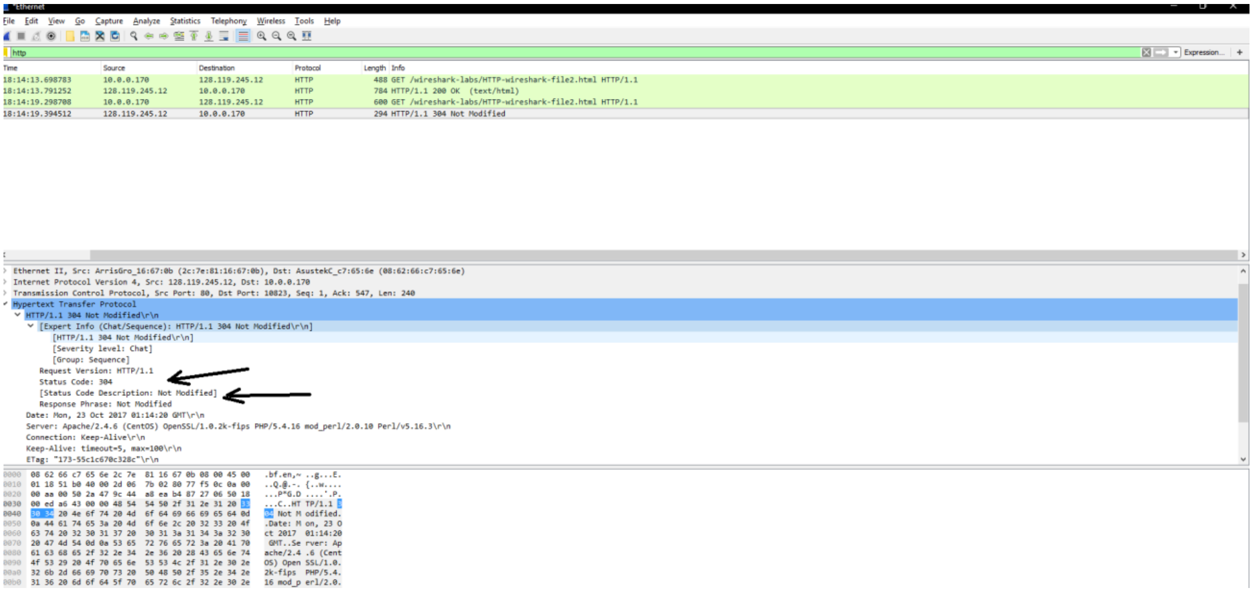
```
No.     Time             Source          Destination     Protocol Length Info
 174237 13:46:29.995948  10.0.0.170      128.119.245.12  HTTP     488 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
 176368 13:46:30.088296  128.119.245.12  10.0.0.170      HTTP     784 HTTP/1.1 200 OK  (text/html)
 400196 13:46:39.610586  10.0.0.170      128.119.245.12  HTTP     600 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
 402657 13:46:39.703048  128.119.245.12  10.0.0.170      HTTP     294 HTTP/1.1 304 Not Modified
```

```
> Transmission Control Protocol, Src Port: 4194, Dst Port: 80, Seq: 1, Ack: 1, Len: 546
v 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
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/61.0.3163.100 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
    DNT: 1\r\n
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: en-US,en;q=0.8\r\n
    If-None-Match: "173-55c1c670c328c"\r\n
    If-Modified-Since: Sun, 22 Oct 2017 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: 402657]
```

```
0080  73 2e 65 64 75 0d 0a 43  6f 6e 6e 65 63 74 69 6f   s.edu..C onnectio
0090  6e 3a 20 6b 65 65 70 2d  61 6c 69 76 65 0d 0a 43   n: keep- alive..C
00a0  61 63 68 65 2d 43 6f 6e  74 72 6f 6c 3a 20 6d 61   ache-Con trol: ma
00b0  78 2d 61 67 65 3d 30 0d  0a 55 73 65 72 2d 41 67   x-age=0. .User-Ag
00c0  65 6e 74 3a 20 4d 6f 7a  69 6c 6c 61 2f 35 2e 30   ent: Moz illa/5.0
00d0  20 28 57 69 6e 64 6f 77  73 20 4e 54 20 31 30 2e    (Window s NT 10.
00e0  30 3b 20 57 69 6e 36 34  3b 20 78 36 34 29 20 41   0; Win64 ; x64) A
00f0  70 70 6c 65 57 65 62 4b  69 74 2f 35 33 37 2e 33   ppleWebK it/537.3
0100  36 20 28 4b 48 54 4d 4c  2c 20 6c 69 6b 65 20 47   6 (KHTML , like G
0110  65 63 6b 6f 29 20 43 68  72 6f 6d 65 2f 36 31 2e   ecko) Ch rome/61.
0120  30 2e 33 31 36 33 2e 31  30 30 20 53 61 66 61 72   0.3163.1 00 Safar
0130  69 2f 35 33 37 2e 33 36  0d 0a 55 70 67 72 61 64   i/537.36 ..Upgrad
0140  65 2d 49 6e 73 65 63 75  72 65 2d 52 65 71 75 65   e-Insecu re-Reque
0150  73 74 73 3a 20 31 0d 0a  41 63 63 65 70 74 3a 20   sts: 1.. Accept: 
0160  74 65 78 74 2f 68 74 6d  6c 2c 61 70 70 6c 69 63   text/htm l,applic
0170  61 74 69 6f 6e 2f 78 68  74 6d 6c 2b 78 6d 6c 2c   ation/xh tml+xml,
0180  61 70 70 6c 69 63 61 74  69 6f 6e 2f 78 6d 6c 3b   applicat ion/xml;
0190  71 3d 30 2e 39 2c 69 6d  61 67 65 2f 77 65 62 70   q=0.9,im age/webp
01a0  2c 69 6d 61 67 65 2f 61  70 6e 67 2c 2a 2f 2a 3b   ,image/a png,*/*;
01b0  71 3d 30 2e 38 0d 0a 44  4e 54 3a 20 31 0d 0a 41   q=0.8..D NT: 1..A
```

HTTP Connection (http.connection), 24 bytes   Packets: 513574 · Displayed: 4 (0.0%)   Profile: Default

11. The HTTP status code and phrase response from the server is HTTP/1.1 304 Not Modified. The server did not return the contents of the file because the page was not modified, so it was loaded from the cache.

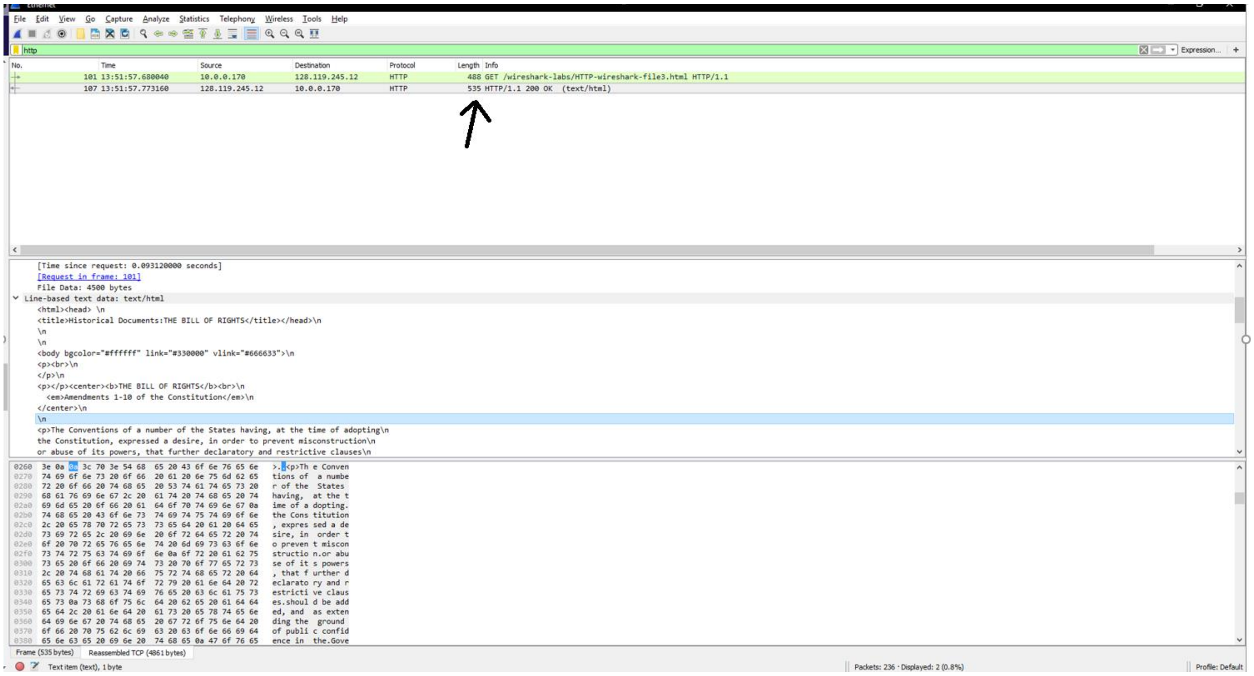

*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
Expression...

```
Time             Source          Destination     Protocol Length Info
18:14:13.698783  10.0.0.170      128.119.245.12  HTTP     488 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
18:14:13.791252  128.119.245.12  10.0.0.170      HTTP     784 HTTP/1.1 200 OK  (text/html)
18:14:19.298708  10.0.0.170      128.119.245.12  HTTP     600 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
18:14:19.394512  128.119.245.12  10.0.0.170      HTTP     294 HTTP/1.1 304 Not Modified
```

```
> Ethernet II, Src: ArrisGro_16:67:0b (2c:7e:81:16:67:0b), Dst: AsustekC_c7:65:6e (08:62:66:c7:65:6e)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 10.0.0.170
> Transmission Control Protocol, Src Port: 80, Dst Port: 10823, Seq: 1, Ack: 547, Len: 240
v Hypertext Transfer Protocol
  v HTTP/1.1 304 Not Modified\r\n
    v [Expert Info (Chat/Sequence): HTTP/1.1 304 Not Modified\r\n]
        [HTTP/1.1 304 Not Modified\r\n]
        [Severity level: Chat]
        [Group: Sequence]
      Request Version: HTTP/1.1
      Status Code: 304
      [Status Code Description: Not Modified]
      Response Phrase: Not Modified
    Date: Mon, 23 Oct 2017 01:14:20 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/5.4.16 mod_perl/2.0.10 Perl/v5.16.3\r\n
    Connection: Keep-Alive\r\n
    Keep-Alive: timeout=5, max=100\r\n
    ETag: "173-55c1c670c328c"\r\n
```

```
0000  08 62 66 c7 65 6e 2c 7e  81 16 67 0b 08 00 45 00   .bf.en,~ ..g...E.
0010  01 18 51 b0 40 00 2d 06  7b 02 80 77 f5 0c 0a 00   ..Q.@.-. {..w....
0020  00 aa 00 50 2a 47 9c 44  a8 ea b4 87 27 06 50 18   ...P*G.D ....'.P.
0030  00 ed a6 43 00 00 48 54  54 50 2f 31 2e 31 20 33   ...C..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 4d  6f 6e 2c 20 32 33 20 4f   .Date: M on, 23 O
0060  63 74 20 32 30 31 37 20  30 31 3a 31 34 3a 32 30   ct 2017  01:14:20
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 2f 32 2e 34  2e 36 20 28 43 65 6e 74   ache/2.4 .6 (Cent
0090  4f 53 29 20 4f 70 65 6e  53 53 4c 2f 31 2e 30 2e   OS) Open SSL/1.0.
00a0  32 6b 2d 66 69 70 73 20  50 48 50 2f 35 2e 34 2e   2k-fips  PHP/5.4.
00b0  31 36 20 6d 6f 64 5f 70  65 72 6c 2f 32 2e 30 2e   16 mod_p erl/2.0.
```

12. 1 Get request


Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expression...
+

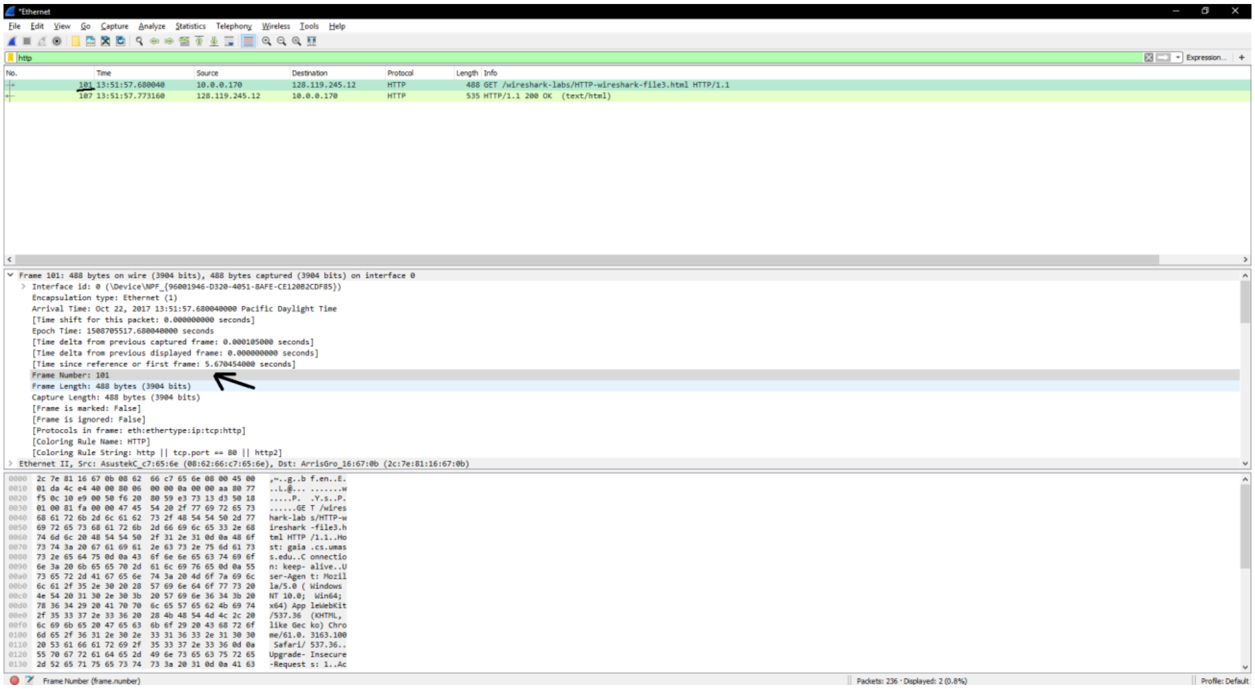
```
http

No.   Time              Source          Destination     Protocol  Length Info
  101 13:51:57.680040   10.0.0.170      128.119.245.12  HTTP         488 GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
  107 13:51:57.773160   128.119.245.12  10.0.0.170      HTTP         535 HTTP/1.1 200 OK  (text/html)
```

```
    [Time since request: 0.093120000 seconds]
    [Request in frame: 101]
    File Data: 4500 bytes
v Line-based text data: text/html
    <html><head> \n
    <title>Historical Documents:THE BILL OF RIGHTS</title></head>\n
    \n
    \n
    <body bgcolor="#ffffff" link="#330000" vlink="#666633">\n
    <p><br>\n
    </p>\n
    <p></p><center><b>THE BILL OF RIGHTS</b><br>\n
      <em>Amendments 1-10 of the Constitution</em>\n
    </center>\n
    \n
    <p>The Conventions of a number of the States having, at the time of adopting\n
    the Constitution, expressed a desire, in order to prevent misconstruction\n
    or abuse of its powers, that further declaratory and restrictive clauses\n
```

```
0260  3e 0a 0a 3c 70 3e 54 68  65 20 43 6f 6e 76 65 6e   >..<p>Th e Conven
0270  74 69 6f 6e 73 20 6f 66  20 61 20 6e 75 6d 62 65   tions of  a numbe
0280  72 20 6f 66 20 74 68 65  20 53 74 61 74 65 73 20   r of the  States 
0290  68 61 76 69 6e 67 2c 20  61 74 20 74 68 65 20 74   having,  at the t
02a0  69 6d 65 20 6f 66 20 61  64 6f 70 74 69 6e 67 0a   ime of a dopting.
02b0  74 68 65 20 43 6f 6e 73  74 69 74 75 74 69 6f 6e   the Cons titution
02c0  2c 20 65 78 70 72 65 73  73 65 64 20 61 20 64 65   , expres sed a de
02d0  73 69 72 65 2c 20 69 6e  20 6f 72 64 65 72 20 74   sire, in  order t
02e0  6f 20 70 72 65 76 65 6e  74 20 6d 69 73 63 6f 6e   o preven t miscon
02f0  73 74 72 75 63 74 69 6f  6e 0a 6f 72 20 61 62 75   structio n.or abu
0300  73 65 20 6f 66 20 69 74  73 20 70 6f 77 65 72 73   se of it s powers
0310  2c 20 74 68 61 74 20 66  75 72 74 68 65 72 20 64   , that f urther d
0320  65 63 6c 61 72 61 74 6f  72 79 20 61 6e 64 20 72   eclarato ry and r
0330  65 73 74 72 69 63 74 69  76 65 20 63 6c 61 75 73   estricti ve claus
0340  65 73 0a 73 68 6f 75 6c  64 20 62 65 20 61 64 64   es.shoul d be add
0350  65 64 2c 20 61 6e 64 20  61 73 20 65 78 74 65 6e   ed, and  as exten
0360  64 69 6e 67 20 74 68 65  20 67 72 6f 75 6e 64 20   ding the  ground 
0370  6f 66 20 70 75 62 6c 69  63 20 63 6f 6e 66 69 64   of publi c confid
0380  65 6e 63 65 20 69 6e 20  74 68 65 0a 47 6f 76 65   ence in  the.Gove
```

```
Frame (535 bytes)   Reassembled TCP (4861 bytes)
Text item (text), 1 byte          Packets: 236 · Displayed: 2 (0.8%)          Profile: Default
```

13. The packet number is 101.


*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expression...
+

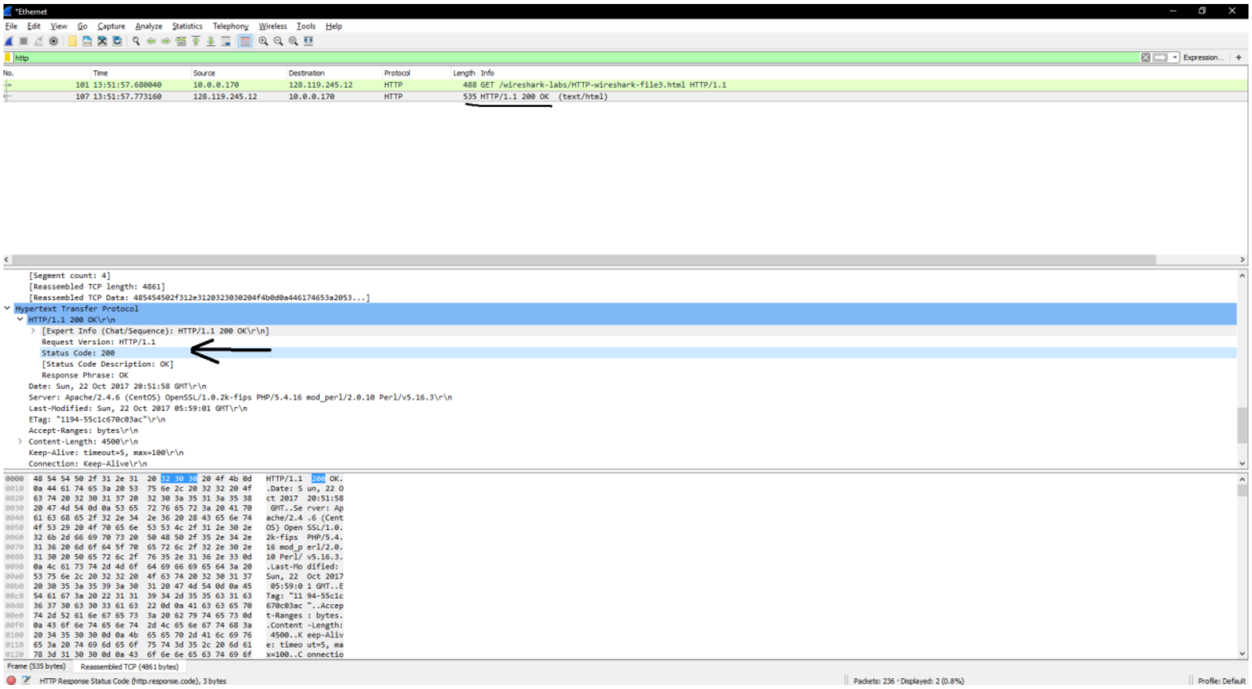
```
http

No.   Time              Source          Destination     Protocol  Length Info
  101 13:51:57.680040   10.0.0.170      128.119.245.12  HTTP         488 GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
  107 13:51:57.773160   128.119.245.12  10.0.0.170      HTTP         535 HTTP/1.1 200 OK  (text/html)
```

```
v Frame 101: 488 bytes on wire (3904 bits), 488 bytes captured (3904 bits) on interface 0
  > Interface id: 0 (\Device\NPF_{96001946-D320-4051-8AFE-CE120B2CDF85})
    Encapsulation type: Ethernet (1)
    Arrival Time: Oct 22, 2017 13:51:57.680040000 Pacific Daylight Time
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1508705517.680040000 seconds
    [Time delta from previous captured frame: 0.000105000 seconds]
    [Time delta from previous displayed frame: 0.000000000 seconds]
    [Time since reference or first frame: 5.670454000 seconds]
    Frame Number: 101
    Frame Length: 488 bytes (3904 bits)
    Capture Length: 488 bytes (3904 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:tcp:http]
    [Coloring Rule Name: HTTP]
    [Coloring Rule String: http || tcp.port == 80 || http2]
> Ethernet II, Src: AsustekC_c7:65:6e (08:62:66:c7:65:6e), Dst: ArrisGro_16:67:0b (2c:7e:81:16:67:0b)
```

```
0000  2c 7e 81 16 67 0b 08 62  66 c7 65 6e 08 00 45 00   ,~..g..b f.en..E.
0010  01 da 4c e4 40 00 80 06  00 00 0a 00 00 aa 80 77   ..L.@... .......w
0020  f5 0c 10 e9 00 50 f6 20  80 59 e3 73 13 d3 50 18   .....P.  .Y.s..P.
0030  01 00 81 fa 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 33 2e 68   ireshark -file3.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  73 65 72 2d 41 67 65 6e  74 3a 20 4d 6f 7a 69 6c   ser-Agen t: Mozil
00b0  6c 61 2f 35 2e 30 20 28  57 69 6e 64 6f 77 73 20   la/5.0 ( Windows 
00c0  4e 54 20 31 30 2e 30 3b  20 57 69 6e 36 34 3b 20   NT 10.0;  Win64; 
00d0  78 36 34 29 20 41 70 70  6c 65 57 65 62 4b 69 74   x64) App leWebKit
00e0  2f 35 33 37 2e 33 36 20  28 4b 48 54 4d 4c 2c 20   /537.36  (KHTML, 
00f0  6c 69 6b 65 20 47 65 63  6b 6f 29 20 43 68 72 6f   like Gec ko) Chro
0100  6d 65 2f 36 31 2e 30 2e  33 31 36 33 2e 31 30 30   me/61.0. 3163.100
0110  20 53 61 66 61 72 69 2f  35 33 37 2e 33 36 0d 0a    Safari/ 537.36..
0120  55 70 67 72 61 64 65 2d  49 6e 73 65 63 75 72 65   Upgrade- Insecure
0130  2d 52 65 71 75 65 73 74  73 3a 20 31 0d 0a 41 63   -Request s: 1..Ac
```

```
Frame Number (frame.number)          Packets: 236 · Displayed: 2 (0.8%)          Profile: Default
```

14. The status code and phrase is “200 OK”.

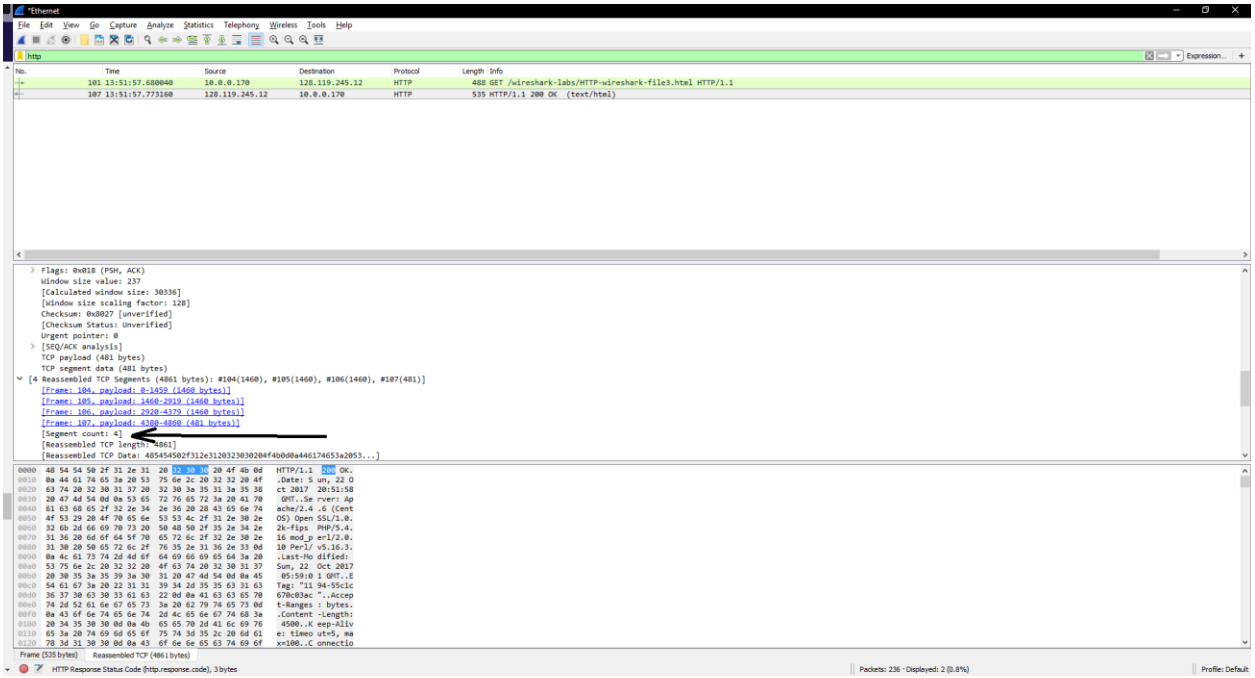

*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
Expression…
Frame (535 bytes)
Reassembled TCP (4861 bytes)
HTTP Response Status Code (http.response.code), 3 bytes
Packets: 236 · Displayed: 2 (0.8%)
Profile: Default

```
No.      Time              Source          Destination     Protocol  Length  Info
    101 13:51:57.680040   10.0.0.170      128.119.245.12  HTTP         488  GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
    107 13:51:57.773160   128.119.245.12  10.0.0.170      HTTP         535  HTTP/1.1 200 OK  (text/html)
```

```
    [Segment count: 4]
    [Reassembled TCP length: 4861]
    [Reassembled TCP Data: 485454502f312e3120323030204f4b0d0a446174653a2053...]
v Hypertext Transfer Protocol
  v HTTP/1.1 200 OK\r\n
    > [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
      Request Version: HTTP/1.1
      Status Code: 200
      [Status Code Description: OK]
      Response Phrase: OK
    Date: Sun, 22 Oct 2017 20:51:58 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/5.4.16 mod_perl/2.0.10 Perl/v5.16.3\r\n
    Last-Modified: Sun, 22 Oct 2017 05:59:01 GMT\r\n
    ETag: "1194-55c1c670c03ac"\r\n
    Accept-Ranges: bytes\r\n
  > Content-Length: 4500\r\n
    Keep-Alive: timeout=5, max=100\r\n
    Connection: Keep-Alive\r\n
```

```
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 53  75 6e 2c 20 32 32 20 4f   .Date: S un, 22 O
0020  63 74 20 32 30 31 37 20  32 30 3a 35 31 3a 35 38   ct 2017  20:51:58
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 2f 32 2e 34  2e 36 20 28 43 65 6e 74   ache/2.4 .6 (Cent
0050  4f 53 29 20 4f 70 65 6e  53 53 4c 2f 31 2e 30 2e   OS) Open SSL/1.0.
0060  32 6b 2d 66 69 70 73 20  50 48 50 2f 35 2e 34 2e   2k-fips  PHP/5.4.
0070  31 36 20 6d 6f 64 5f 70  65 72 6c 2f 32 2e 30 2e   16 mod_p erl/2.0.
0080  31 30 20 50 65 72 6c 2f  76 35 2e 31 36 2e 33 0d   10 Perl/ v5.16.3.
0090  0a 4c 61 73 74 2d 4d 6f  64 69 66 69 65 64 3a 20   .Last-Mo dified: 
00a0  53 75 6e 2c 20 32 32 20  4f 63 74 20 32 30 31 37   Sun, 22  Oct 2017
00b0  20 30 35 3a 35 39 3a 30  31 20 47 4d 54 0d 0a 45    05:59:0 1 GMT..E
00c0  54 61 67 3a 20 22 31 31  39 34 2d 35 35 63 31 63   Tag: "11 94-55c1c
00d0  36 37 30 63 30 33 61 63  22 0d 0a 41 63 63 65 70   670c03ac "..Accep
00e0  74 2d 52 61 6e 67 65 73  3a 20 62 79 74 65 73 0d   t-Ranges : bytes.
00f0  0a 43 6f 6e 74 65 6e 74  2d 4c 65 6e 67 74 68 3a   .Content -Length:
0100  20 34 35 30 30 0d 0a 4b  65 65 70 2d 41 6c 69 76    4500..K eep-Aliv
0110  65 3a 20 74 69 6d 65 6f  75 74 3d 35 2c 20 6d 61   e: timeo ut=5, ma
0120  78 3d 31 30 30 0d 0a 43  6f 6e 6e 65 63 74 69 6f   x=100..C onnectio
```

15. There are 4 data-containing TCP segments that are needed to carry the single HTTP response.

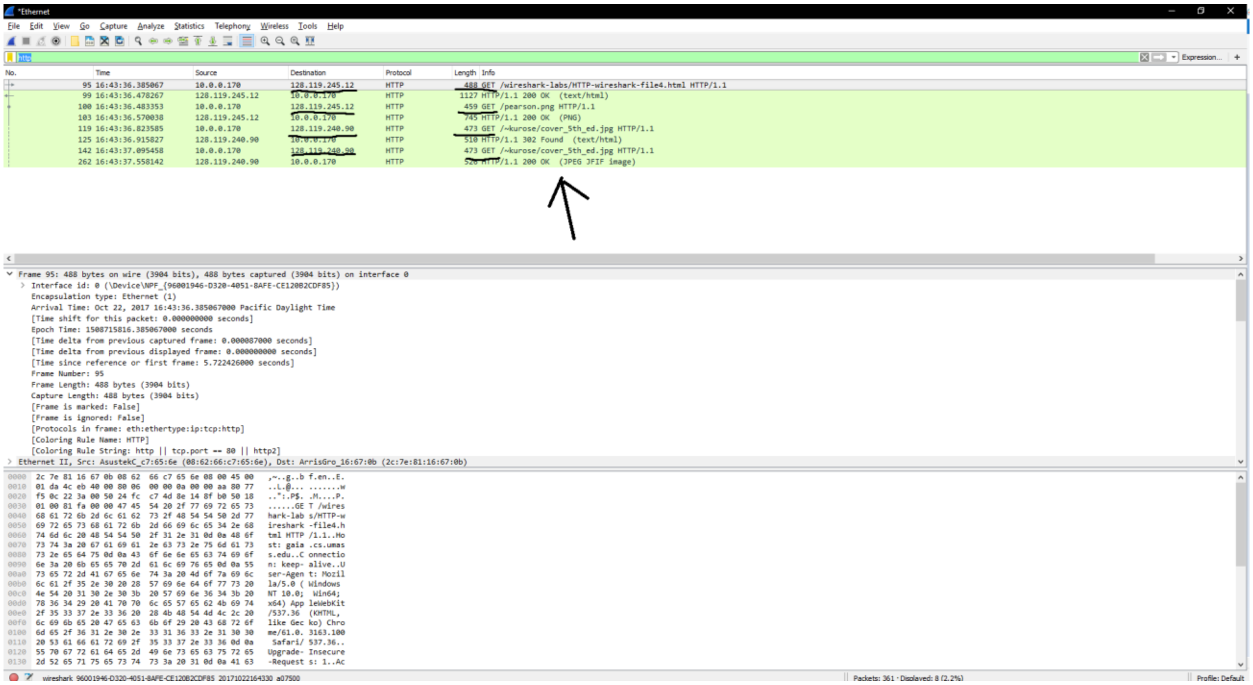

*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
Expression…
Frame (535 bytes)
Reassembled TCP (4861 bytes)
HTTP Response Status Code (http.response.code), 3 bytes
Packets: 236 · Displayed: 2 (0.8%)
Profile: Default

```
No.      Time              Source          Destination     Protocol  Length  Info
    101 13:51:57.680040   10.0.0.170      128.119.245.12  HTTP         488  GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
    107 13:51:57.773160   128.119.245.12  10.0.0.170      HTTP         535  HTTP/1.1 200 OK  (text/html)
```

```
  > Flags: 0x018 (PSH, ACK)
    Window size value: 237
    [Calculated window size: 30336]
    [Window size scaling factor: 128]
    Checksum: 0x8027 [unverified]
    [Checksum Status: Unverified]
    Urgent pointer: 0
  > [SEQ/ACK analysis]
    TCP payload (481 bytes)
    TCP segment data (481 bytes)
v [4 Reassembled TCP Segments (4861 bytes): #104(1460), #105(1460), #106(1460), #107(481)]
    [Frame: 104, payload: 0-1459 (1460 bytes)]
    [Frame: 105, payload: 1460-2919 (1460 bytes)]
    [Frame: 106, payload: 2920-4379 (1460 bytes)]
    [Frame: 107, payload: 4380-4860 (481 bytes)]
    [Segment count: 4]
    [Reassembled TCP length: 4861]
    [Reassembled TCP Data: 485454502f312e3120323030204f4b0d0a446174653a2053...]
```

```
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 53  75 6e 2c 20 32 32 20 4f   .Date: S un, 22 O
0020  63 74 20 32 30 31 37 20  32 30 3a 35 31 3a 35 38   ct 2017  20:51:58
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 2f 32 2e 34  2e 36 20 28 43 65 6e 74   ache/2.4 .6 (Cent
0050  4f 53 29 20 4f 70 65 6e  53 53 4c 2f 31 2e 30 2e   OS) Open SSL/1.0.
0060  32 6b 2d 66 69 70 73 20  50 48 50 2f 35 2e 34 2e   2k-fips  PHP/5.4.
0070  31 36 20 6d 6f 64 5f 70  65 72 6c 2f 32 2e 30 2e   16 mod_p erl/2.0.
0080  31 30 20 50 65 72 6c 2f  76 35 2e 31 36 2e 33 0d   10 Perl/ v5.16.3.
0090  0a 4c 61 73 74 2d 4d 6f  64 69 66 69 65 64 3a 20   .Last-Mo dified: 
00a0  53 75 6e 2c 20 32 32 20  4f 63 74 20 32 30 31 37   Sun, 22  Oct 2017
00b0  20 30 35 3a 35 39 3a 30  31 20 47 4d 54 0d 0a 45    05:59:0 1 GMT..E
00c0  54 61 67 3a 20 22 31 31  39 34 2d 35 35 63 31 63   Tag: "11 94-55c1c
00d0  36 37 30 63 30 33 61 63  22 0d 0a 41 63 63 65 70   670c03ac "..Accep
00e0  74 2d 52 61 6e 67 65 73  3a 20 62 79 74 65 73 0d   t-Ranges : bytes.
00f0  0a 43 6f 6e 74 65 6e 74  2d 4c 65 6e 67 74 68 3a   .Content -Length:
0100  20 34 35 30 30 0d 0a 4b  65 65 70 2d 41 6c 69 76    4500..K eep-Aliv
0110  65 3a 20 74 69 6d 65 6f  75 74 3d 35 2c 20 6d 61   e: timeo ut=5, ma
0120  78 3d 31 30 30 0d 0a 43  6f 6e 6e 65 63 74 69 6f   x=100..C onnectio
```

16. There were 4 HTTP GET messages send from the browser to 128.119.245.12, 128.119.245.12, 128.119.240.90, and 128.119.240.90


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

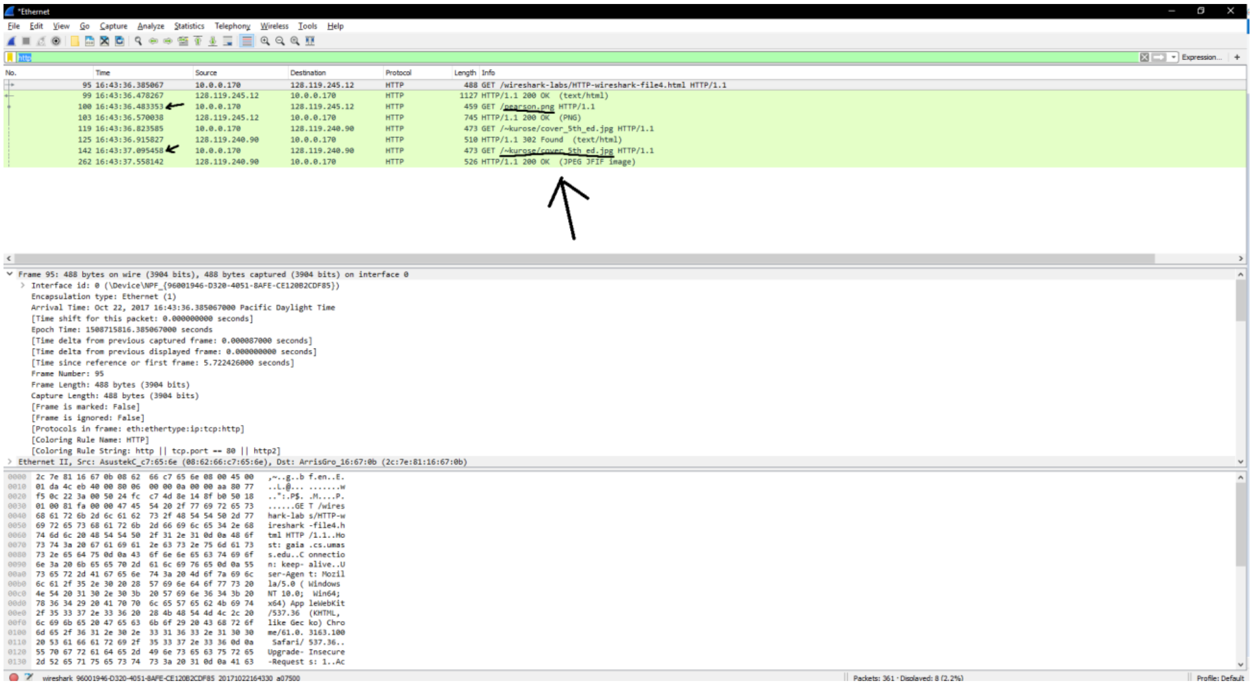
```
No.    Time             Source           Destination      Protocol  Length Info
    95 16:43:36.385067  10.0.0.170       128.119.245.12   HTTP       488 GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
    99 16:43:36.478267  128.119.245.12   10.0.0.170       HTTP      1127 HTTP/1.1 200 OK  (text/html)
   100 16:43:36.483353  10.0.0.170       128.119.245.12   HTTP       459 GET /pearson.png HTTP/1.1
   103 16:43:36.570038  128.119.245.12   10.0.0.170       HTTP       745 HTTP/1.1 200 OK  (PNG)
   119 16:43:36.823585  10.0.0.170       128.119.240.90   HTTP       473 GET /~kurose/cover_5th_ed.jpg HTTP/1.1
   125 16:43:36.915827  128.119.240.90   10.0.0.170       HTTP       510 HTTP/1.1 302 Found  (text/html)
   142 16:43:37.095458  10.0.0.170       128.119.240.90   HTTP       473 GET /~kurose/cover_5th_ed.jpg HTTP/1.1
   262 16:43:37.558142  128.119.240.90   10.0.0.170       HTTP       526 HTTP/1.1 200 OK  (JPEG JFIF image)
```

```
v Frame 95: 488 bytes on wire (3904 bits), 488 bytes captured (3904 bits) on interface 0
    > Interface id: 0 (\Device\NPF_{96001946-D320-4051-8AFE-CE120B2CDF85})
      Encapsulation type: Ethernet (1)
      Arrival Time: Oct 22, 2017 16:43:36.385067000 Pacific Daylight Time
      [Time shift for this packet: 0.000000000 seconds]
      Epoch Time: 1508715816.385067000 seconds
      [Time delta from previous captured frame: 0.000087000 seconds]
      [Time delta from previous displayed frame: 0.000000000 seconds]
      [Time since reference or first frame: 5.722426000 seconds]
      Frame Number: 95
      Frame Length: 488 bytes (3904 bits)
      Capture Length: 488 bytes (3904 bits)
      [Frame is marked: False]
      [Frame is ignored: False]
      [Protocols in frame: eth:ethertype:ip:tcp:http]
      [Coloring Rule Name: HTTP]
      [Coloring Rule String: http || tcp.port == 80 || http2]
> Ethernet II, Src: AsustekC_c7:65:6e (08:62:66:c7:65:6e), Dst: ArrisGro_16:67:0b (2c:7e:81:16:67:0b)
```

```
0000  2c 7e 81 16 67 0b 08 62  66 c7 65 6e 08 00 45 00   ,~..g..b f.en..E.
0010  01 da 4c eb 40 00 80 06  00 00 0a 00 00 aa 80 77   ..L.@... .......w
0020  f5 0c 22 3a 00 50 24 fc  c7 4d 8e 14 8f b0 50 18   ..":.P$. .M....P.
0030  01 00 81 fa 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 34 2e 68   ireshark -file4.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  73 65 72 2d 41 67 65 6e  74 3a 20 4d 6f 7a 69 6c   ser-Agen t: Mozil
00b0  6c 61 2f 35 2e 30 20 28  57 69 6e 64 6f 77 73 20   la/5.0 ( Windows
00c0  4e 54 20 31 30 2e 30 3b  20 57 69 6e 36 34 3b 20   NT 10.0;  Win64;
00d0  78 36 34 29 20 41 70 70  6c 65 57 65 62 4b 69 74   x64) App leWebKit
00e0  2f 35 33 37 2e 33 36 20  28 4b 48 54 4d 4c 2c 20   /537.36  (KHTML,
00f0  6c 69 6b 65 20 47 65 63  6b 6f 29 20 43 68 72 6f   like Gec ko) Chro
0100  6d 65 2f 36 31 2e 30 2e  33 31 36 33 2e 31 30 30   me/61.0. 3163.100
0110  20 53 61 66 61 72 69 2f  35 33 37 2e 33 36 0d 0a    Safari/ 537.36..
0120  55 70 67 72 61 64 65 2d  49 6e 73 65 63 75 72 65   Upgrade- Insecure
0130  2d 52 65 71 75 65 73 74  73 3a 20 31 0d 0a 41 63   -Request s: 1..Ac
```

```
wireshark_96001946-D320-4051-8AFE-CE120B2CDF85_20171022164330_a07500    Packets: 361 · Displayed: 8 (2.2%)    Profile: Default
```

17. The browser downloaded the two images serially because they have differing GET request times. If the images were downloaded in parallel, then the GET requests would be the same.


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

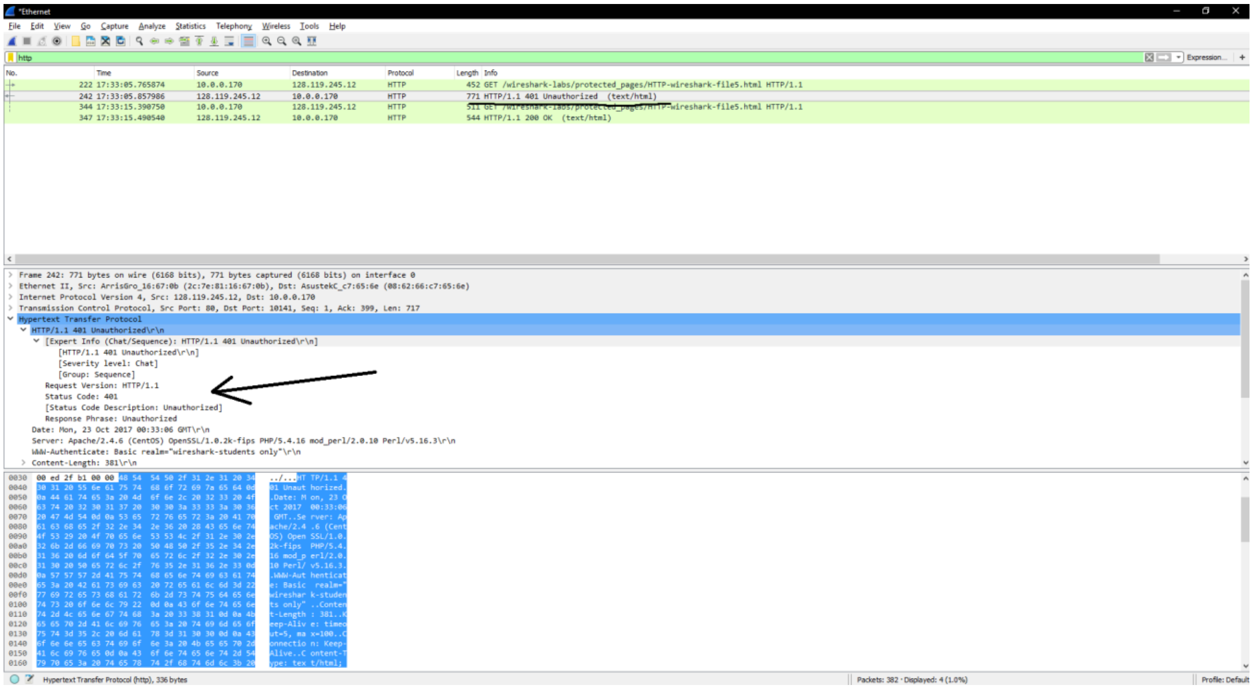
```
No.    Time             Source           Destination      Protocol  Length Info
    95 16:43:36.385067  10.0.0.170       128.119.245.12   HTTP       488 GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
    99 16:43:36.478267  128.119.245.12   10.0.0.170       HTTP      1127 HTTP/1.1 200 OK  (text/html)
   100 16:43:36.483353  10.0.0.170       128.119.245.12   HTTP       459 GET /pearson.png HTTP/1.1
   103 16:43:36.570038  128.119.245.12   10.0.0.170       HTTP       745 HTTP/1.1 200 OK  (PNG)
   119 16:43:36.823585  10.0.0.170       128.119.240.90   HTTP       473 GET /~kurose/cover_5th_ed.jpg HTTP/1.1
   125 16:43:36.915827  128.119.240.90   10.0.0.170       HTTP       510 HTTP/1.1 302 Found  (text/html)
   142 16:43:37.095458  10.0.0.170       128.119.240.90   HTTP       473 GET /~kurose/cover_5th_ed.jpg HTTP/1.1
   262 16:43:37.558142  128.119.240.90   10.0.0.170       HTTP       526 HTTP/1.1 200 OK  (JPEG JFIF image)
```

```
v Frame 95: 488 bytes on wire (3904 bits), 488 bytes captured (3904 bits) on interface 0
    > Interface id: 0 (\Device\NPF_{96001946-D320-4051-8AFE-CE120B2CDF85})
      Encapsulation type: Ethernet (1)
      Arrival Time: Oct 22, 2017 16:43:36.385067000 Pacific Daylight Time
      [Time shift for this packet: 0.000000000 seconds]
      Epoch Time: 1508715816.385067000 seconds
      [Time delta from previous captured frame: 0.000087000 seconds]
      [Time delta from previous displayed frame: 0.000000000 seconds]
      [Time since reference or first frame: 5.722426000 seconds]
      Frame Number: 95
      Frame Length: 488 bytes (3904 bits)
      Capture Length: 488 bytes (3904 bits)
      [Frame is marked: False]
      [Frame is ignored: False]
      [Protocols in frame: eth:ethertype:ip:tcp:http]
      [Coloring Rule Name: HTTP]
      [Coloring Rule String: http || tcp.port == 80 || http2]
> Ethernet II, Src: AsustekC_c7:65:6e (08:62:66:c7:65:6e), Dst: ArrisGro_16:67:0b (2c:7e:81:16:67:0b)
```

```
0000  2c 7e 81 16 67 0b 08 62  66 c7 65 6e 08 00 45 00   ,~..g..b f.en..E.
0010  01 da 4c eb 40 00 80 06  00 00 0a 00 00 aa 80 77   ..L.@... .......w
0020  f5 0c 22 3a 00 50 24 fc  c7 4d 8e 14 8f b0 50 18   ..":.P$. .M....P.
0030  01 00 81 fa 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 34 2e 68   ireshark -file4.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  73 65 72 2d 41 67 65 6e  74 3a 20 4d 6f 7a 69 6c   ser-Agen t: Mozil
00b0  6c 61 2f 35 2e 30 20 28  57 69 6e 64 6f 77 73 20   la/5.0 ( Windows
00c0  4e 54 20 31 30 2e 30 3b  20 57 69 6e 36 34 3b 20   NT 10.0;  Win64;
00d0  78 36 34 29 20 41 70 70  6c 65 57 65 62 4b 69 74   x64) App leWebKit
00e0  2f 35 33 37 2e 33 36 20  28 4b 48 54 4d 4c 2c 20   /537.36  (KHTML,
00f0  6c 69 6b 65 20 47 65 63  6b 6f 29 20 43 68 72 6f   like Gec ko) Chro
0100  6d 65 2f 36 31 2e 30 2e  33 31 36 33 2e 31 30 30   me/61.0. 3163.100
0110  20 53 61 66 61 72 69 2f  35 33 37 2e 33 36 0d 0a    Safari/ 537.36..
0120  55 70 67 72 61 64 65 2d  49 6e 73 65 63 75 72 65   Upgrade- Insecure
0130  2d 52 65 71 75 65 73 74  73 3a 20 31 0d 0a 41 63   -Request s: 1..Ac
```

```
wireshark_96001946-D320-4051-8AFE-CE120B2CDF85_20171022164330_a07500    Packets: 361 · Displayed: 8 (2.2%)    Profile: Default
```

18. The server response in response to the initial HTTP GET message from my browser is HTTP/1.1 401 Unauthorized.


*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
Expression...

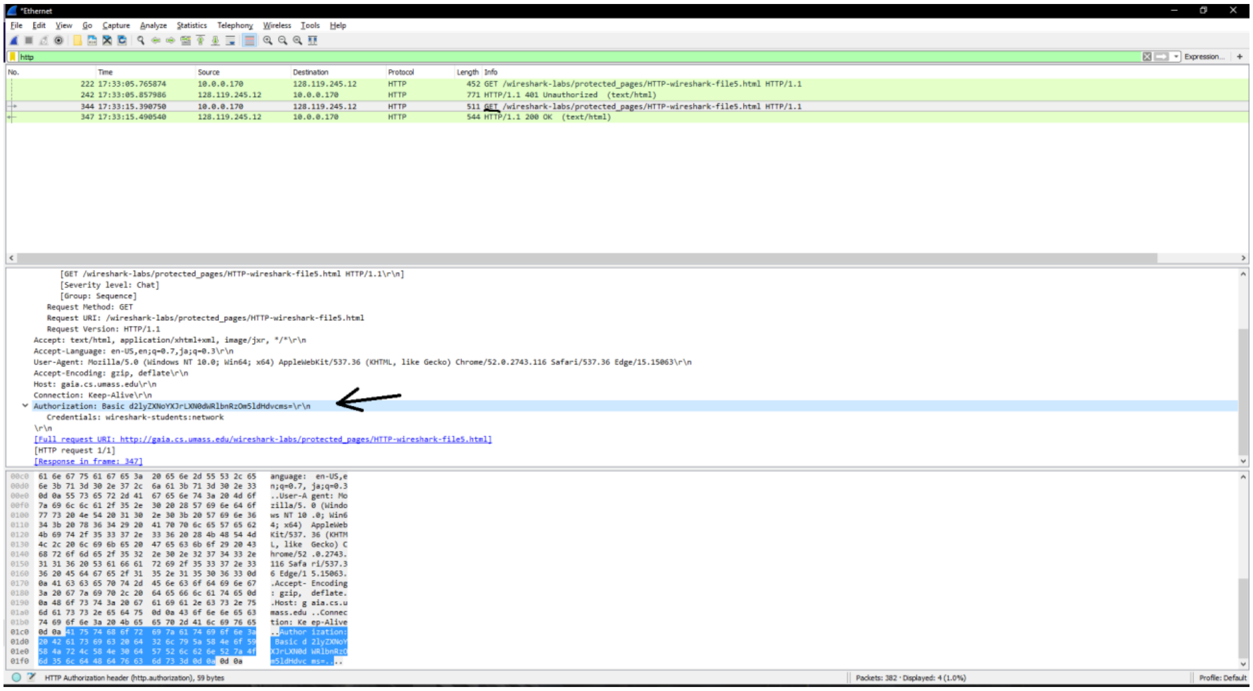
```
No.   Time               Source          Destination     Protocol  Length Info
  222 17:33:05.765874    10.0.0.170      128.119.245.12  HTTP      452 GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
  242 17:33:05.857986    128.119.245.12  10.0.0.170      HTTP      771 HTTP/1.1 401 Unauthorized  (text/html)
  344 17:33:15.390750    10.0.0.170      128.119.245.12  HTTP      511 GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
  347 17:33:15.490540    128.119.245.12  10.0.0.170      HTTP      544 HTTP/1.1 200 OK  (text/html)
```

```
> Frame 242: 771 bytes on wire (6168 bits), 771 bytes captured (6168 bits) on interface 0
> Ethernet II, Src: ArrisGro_16:67:0b (2c:7e:81:16:67:0b), Dst: AsustekC_c7:65:6e (08:62:66:c7:65:6e)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 10.0.0.170
> Transmission Control Protocol, Src Port: 80, Dst Port: 10141, Seq: 1, Ack: 399, Len: 717
v Hypertext Transfer Protocol
  v HTTP/1.1 401 Unauthorized\r\n
    v [Expert Info (Chat/Sequence): HTTP/1.1 401 Unauthorized\r\n]
        [HTTP/1.1 401 Unauthorized\r\n]
        [Severity level: Chat]
        [Group: Sequence]
      Request Version: HTTP/1.1
      Status Code: 401
      [Status Code Description: Unauthorized]
      Response Phrase: Unauthorized
    Date: Mon, 23 Oct 2017 00:33:06 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/5.4.16 mod_perl/2.0.10 Perl/v5.16.3\r\n
    WWW-Authenticate: Basic realm="wireshark-students only"\r\n
  > Content-Length: 381\r\n
```

```
0030  00 ed 2f b1 00 00 48 54  54 50 2f 31 2e 31 20 34   ../...HT TP/1.1 4
0040  30 31 20 55 6e 61 75 74  68 6f 72 69 7a 65 64 0d   01 Unaut horized.
0050  0a 44 61 74 65 3a 20 4d  6f 6e 2c 20 32 33 20 4f   .Date: M on, 23 O
0060  63 74 20 32 30 31 37 20  30 30 3a 33 33 3a 30 36   ct 2017  00:33:06
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 2f 32 2e 34  2e 36 20 28 43 65 6e 74   ache/2.4 .6 (Cent
0090  4f 53 29 20 4f 70 65 6e  53 53 4c 2f 31 2e 30 2e   OS) Open SSL/1.0.
00a0  32 6b 2d 66 69 70 73 20  50 48 50 2f 35 2e 34 2e   2k-fips  PHP/5.4.
00b0  31 36 20 6d 6f 64 5f 70  65 72 6c 2f 32 2e 30 2e   16 mod_p erl/2.0.
00c0  31 30 20 50 65 72 6c 2f  76 35 2e 31 36 2e 33 0d   10 Perl/ v5.16.3.
00d0  0a 57 57 57 2d 41 75 74  68 65 6e 74 69 63 61 74   .WWW-Aut henticat
00e0  65 3a 20 42 61 73 69 63  20 72 65 61 6c 6d 3d 22   e: Basic  realm="
00f0  77 69 72 65 73 68 61 72  6b 2d 73 74 75 64 65 6e   wireshar k-studen
0100  74 73 20 6f 6e 6c 79 22  0d 0a 43 6f 6e 74 65 6e   ts only" ..Conten
0110  74 2d 4c 65 6e 67 74 68  3a 20 33 38 31 0d 0a 4b   t-Length : 381..K
0120  65 65 70 2d 41 6c 69 76  65 3a 20 74 69 6d 65 6f   eep-Aliv e: timeo
0130  75 74 3d 35 2c 20 6d 61  78 3d 31 30 30 0d 0a 43   ut=5, ma x=100..C
0140  6f 6e 6e 65 63 74 69 6f  6e 3a 20 4b 65 65 70 2d   onnectio n: Keep-
0150  41 6c 69 76 65 0d 0a 43  6f 6e 74 65 6e 74 2d 54   Alive..C ontent-T
0160  79 70 65 3a 20 74 65 78  74 2f 68 74 6d 6c 3b 20   ype: tex t/html; 
```

```
Hypertext Transfer Protocol (http), 336 bytes      Packets: 382 · Displayed: 4 (1.0%)      Profile: Default
```

19. When the browser sends the HTTP get message for the second time, the new field included is the Authentication: Basic d2lyZXNoYXJrLXN0dWRlbnRzOm5ldHdvcms


*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
Expression...

```
No.   Time               Source          Destination     Protocol  Length Info
  222 17:33:05.765874    10.0.0.170      128.119.245.12  HTTP      452 GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
  242 17:33:05.857986    128.119.245.12  10.0.0.170      HTTP      771 HTTP/1.1 401 Unauthorized  (text/html)
  344 17:33:15.390750    10.0.0.170      128.119.245.12  HTTP      511 GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
  347 17:33:15.490540    128.119.245.12  10.0.0.170      HTTP      544 HTTP/1.1 200 OK  (text/html)
```

```
        [GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1\r\n]
        [Severity level: Chat]
        [Group: Sequence]
      Request Method: GET
      Request URI: /wireshark-labs/protected_pages/HTTP-wireshark-file5.html
      Request Version: HTTP/1.1
    Accept: text/html, application/xhtml+xml, image/jxr, */*\r\n
    Accept-Language: en-US,en;q=0.7,ja;q=0.3\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/52.0.2743.116 Safari/537.36 Edge/15.15063\r\n
    Accept-Encoding: gzip, deflate\r\n
    Host: gaia.cs.umass.edu\r\n
    Connection: Keep-Alive\r\n
  v Authorization: Basic d2lyZXNoYXJrLXN0dWRlbnRzOm5ldHdvcms=\r\n
      Credentials: wireshark-students:network
    \r\n
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/protected_pages/HTTP-wireshark-file5.html]
    [HTTP request 1/1]
    [Response in frame: 347]
```

```
00c0  61 6e 67 75 61 67 65 3a  20 65 6e 2d 55 53 2c 65   anguage:  en-US,e
00d0  6e 3b 71 3d 30 2e 37 2c  6a 61 3b 71 3d 30 2e 33   n;q=0.7, ja;q=0.3
00e0  0d 0a 55 73 65 72 2d 41  67 65 6e 74 3a 20 4d 6f   ..User-A gent: Mo
00f0  7a 69 6c 6c 61 2f 35 2e  30 20 28 57 69 6e 64 6f   zilla/5. 0 (Windo
0100  77 73 20 4e 54 20 31 30  2e 30 3b 20 57 69 6e 36   ws NT 10 .0; Win6
0110  34 3b 20 78 36 34 29 20  41 70 70 6c 65 57 65 62   4; x64)  AppleWeb
0120  4b 69 74 2f 35 33 37 2e  33 36 20 28 4b 48 54 4d   Kit/537. 36 (KHTM
0130  4c 2c 20 6c 69 6b 65 20  47 65 63 6b 6f 29 20 43   L, like  Gecko) C
0140  68 72 6f 6d 65 2f 35 32  2e 30 2e 32 37 34 33 2e   hrome/52 .0.2743.
0150  31 31 36 20 53 61 66 61  72 69 2f 35 33 37 2e 33   116 Safa ri/537.3
0160  36 20 45 64 67 65 2f 31  35 2e 31 35 30 36 33 0d   6 Edge/1 5.15063.
0170  0a 41 63 63 65 70 74 2d  45 6e 63 6f 64 69 6e 67   .Accept- Encoding
0180  3a 20 67 7a 69 70 2c 20  64 65 66 6c 61 74 65 0d   : gzip,  deflate.
0190  0a 48 6f 73 74 3a 20 67  61 69 61 2e 63 73 2e 75   .Host: g aia.cs.u
01a0  6d 61 73 73 2e 65 64 75  0d 0a 43 6f 6e 6e 65 63   mass.edu ..Connec
01b0  74 69 6f 6e 3a 20 4b 65  65 70 2d 41 6c 69 76 65   tion: Ke ep-Alive
01c0  0d 0a 41 75 74 68 6f 72  69 7a 61 74 69 6f 6e 3a   ..Author ization:
01d0  20 42 61 73 69 63 20 64  32 6c 79 5a 58 4e 6f 59    Basic d 2lyZXNoY
01e0  58 4a 72 4c 58 4e 30 64  57 52 6c 62 6e 52 7a 4f   XJrLXN0d WRlbnRzO
01f0  6d 35 6c 64 48 64 76 63  6d 73 3d 0d 0a 0d 0a      m5ldHdvc ms=....
```

```
HTTP Authorization header (http.authorization), 59 bytes      Packets: 382 · Displayed: 4 (1.0%)      Profile: Default
```