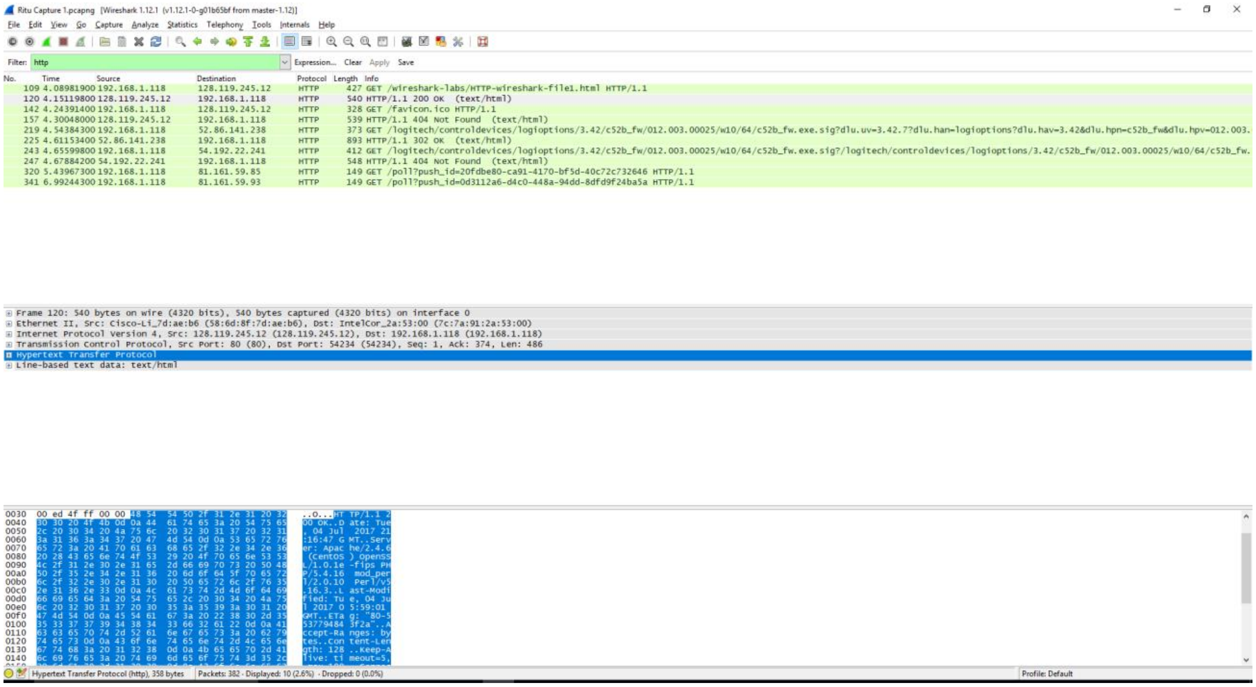
Ritu Bidyut Bhawal

1001387294

Part 1


Ritu Capture 1.pcapng [Wireshark 1.12.1 (v1.12.1-0-g01b65bf from master-1.12)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter: http
Expression... Clear Apply Save

```
No.   Time        Source          Destination     Protocol Length Info
  109 4.08981900 192.168.1.118   128.119.245.12  HTTP     427 GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
  120 4.15119800 128.119.245.12  192.168.1.118   HTTP     540 HTTP/1.1 200 OK  (text/html)
  142 4.24391400 192.168.1.118   128.119.245.12  HTTP     328 GET /favicon.ico HTTP/1.1
  157 4.30048000 128.119.245.12  192.168.1.118   HTTP     539 HTTP/1.1 404 Not Found  (text/html)
  219 4.54384300 192.168.1.118   52.86.141.238   HTTP     373 GET /logitech/controldevices/logioptions/3.42/c52b_fw/012.003.00025/w10/64/c52b_fw.exe.sig?dlu.uv=3.42.7?dlu.han=logioptions?dlu.hav=3.42&dlu.hpn=c52b_fw&dlu.hpv=012.003.
  225 4.61153400 52.86.141.238   192.168.1.118   HTTP     893 HTTP/1.1 302 OK  (text/html)
  243 4.65599800 192.168.1.118   54.192.22.241   HTTP     412 GET /logitech/controldevices/logioptions/3.42/c52b_fw/012.003.00025/w10/64/c52b_fw.exe.sig?/logitech/controldevices/logioptions/3.42/c52b_fw/012.003.00025/w10/64/c52b_fw.
  247 4.67884200 54.192.22.241   192.168.1.118   HTTP     548 HTTP/1.1 404 Not Found  (text/html)
  320 5.43967300 192.168.1.118   81.161.59.85    HTTP     149 GET /poll?push_id=20fdbe80-ca91-4170-bf5d-40c72c732646 HTTP/1.1
  341 6.99244300 192.168.1.118   81.161.59.93    HTTP     149 GET /poll?push_id=0d3112a6-d4c0-448a-94dd-8dfd9f24ba5a HTTP/1.1
```

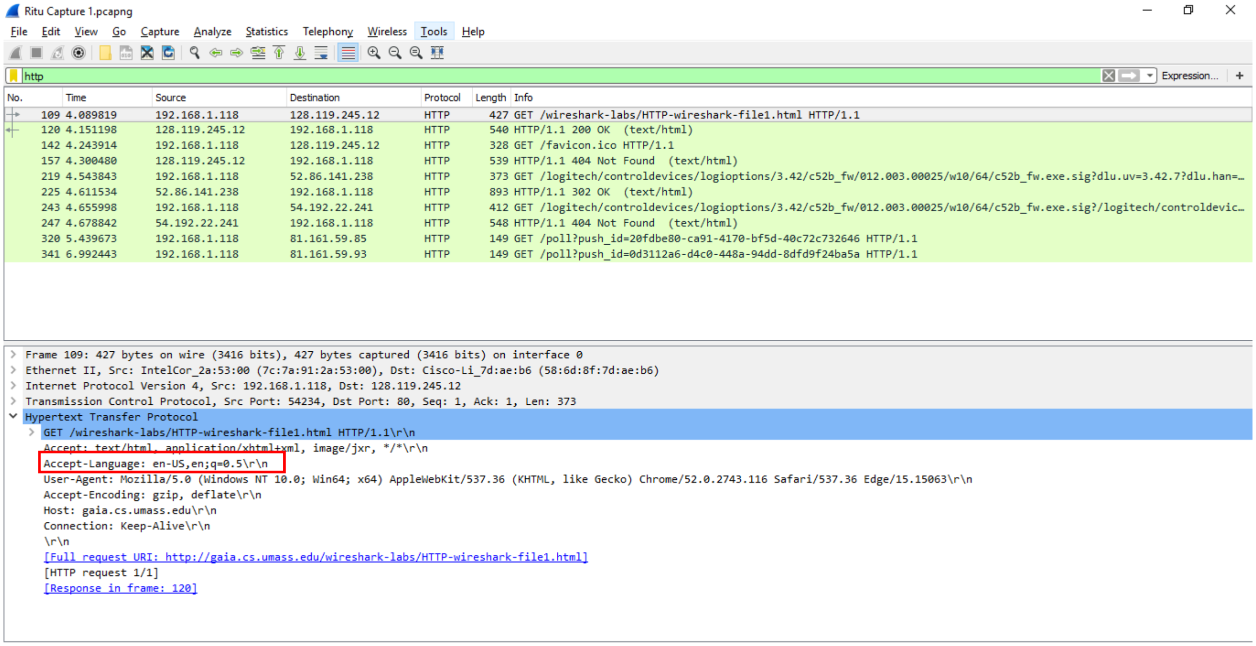
```
⊞ Frame 120: 540 bytes on wire (4320 bits), 540 bytes captured (4320 bits) on interface 0
⊞ Ethernet II, Src: Cisco-Li_7d:ae:b6 (58:6d:8f:7d:ae:b6), Dst: IntelCor_2a:53:00 (7c:7a:91:2a:53:00)
⊞ Internet Protocol Version 4, Src: 128.119.245.12 (128.119.245.12), Dst: 192.168.1.118 (192.168.1.118)
⊞ Transmission Control Protocol, Src Port: 80 (80), Dst Port: 54234 (54234), Seq: 1, Ack: 374, Len: 486
⊞ Hypertext Transfer Protocol
⊞ Line-based text data: text/html
```

```
0030  00 ed 4f ff 00 00 48 54  54 50 2f 31 2e 31 20 32   ..o...HT TP/1.1 2
0040  30 30 20 4f 4b 0d 0a 44  61 74 65 3a 20 54 75 65   00 OK..D ate: Tue
0050  2c 20 30 34 20 4a 75 6c  20 32 30 31 37 20 32 31   , 04 Jul  2017 21
0060  3a 31 36 3a 34 37 20 47  4d 54 0d 0a 53 65 72 76   :16:47 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 31 65  2d 66 69 70 73 20 50 48   L/1.0.1e -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 54 75  65 2c 20 30 34 20 4a 75   fied: Tu e, 04 Ju
00e0  6c 20 32 30 31 37 20 30  35 3a 35 39 3a 30 31 20   l 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 33 37 37 39 34 38 34  33 66 32 61 22 0d 0a 41   53779484 3f2a"..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,
```

Hypertext Transfer Protocol (http), 358 bytes | Packets: 382 · Displayed: 10 (2.6%) · Dropped: 0 (0.0%) | Profile: Default

1. Is your browser running HTTP version 1.0 or 1.1? What version of HTTP is the server running?

A. Browser is running HTTP 1.1, The server is running HTTP 1.1 as well


Ritu Capture 1.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
Expression...
+

```
No.   Time      Source          Destination     Protocol Length Info
  109 4.089819  192.168.1.118   128.119.245.12  HTTP     427 GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
  120 4.151198  128.119.245.12  192.168.1.118   HTTP     540 HTTP/1.1 200 OK  (text/html)
  142 4.243914  192.168.1.118   128.119.245.12  HTTP     328 GET /favicon.ico HTTP/1.1
  157 4.300480  128.119.245.12  192.168.1.118   HTTP     539 HTTP/1.1 404 Not Found  (text/html)
  219 4.543843  192.168.1.118   52.86.141.238   HTTP     373 GET /logitech/controldevices/logioptions/3.42/c52b_fw/012.003.00025/w10/64/c52b_fw.exe.sig?dlu.uv=3.42.7?dlu.han=…
  225 4.611534  52.86.141.238   192.168.1.118   HTTP     893 HTTP/1.1 302 OK  (text/html)
  243 4.655998  192.168.1.118   54.192.22.241   HTTP     412 GET /logitech/controldevices/logioptions/3.42/c52b_fw/012.003.00025/w10/64/c52b_fw.exe.sig?/logitech/controldevic…
  247 4.678842  54.192.22.241   192.168.1.118   HTTP     548 HTTP/1.1 404 Not Found  (text/html)
  320 5.439673  192.168.1.118   81.161.59.85    HTTP     149 GET /poll?push_id=20fdbe80-ca91-4170-bf5d-40c72c732646 HTTP/1.1
  341 6.992443  192.168.1.118   81.161.59.93    HTTP     149 GET /poll?push_id=0d3112a6-d4c0-448a-94dd-8dfd9f24ba5a HTTP/1.1
```

```
> Frame 109: 427 bytes on wire (3416 bits), 427 bytes captured (3416 bits) on interface 0
> Ethernet II, Src: IntelCor_2a:53:00 (7c:7a:91:2a:53:00), Dst: Cisco-Li_7d:ae:b6 (58:6d:8f:7d:ae:b6)
> Internet Protocol Version 4, Src: 192.168.1.118, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 54234, Dst Port: 80, Seq: 1, Ack: 1, Len: 373
v Hypertext Transfer Protocol
  > GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n
    Accept: text/html, application/xhtml+xml, image/jxr, */*\r\n
    Accept-Language: en-US,en;q=0.5\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
    \r\n
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html]
    [HTTP request 1/1]
    [Response in frame: 120]
```

2. What languages (if any) does your browser indicate that it can accept to the server?

A. English US.

3. What is the IP address of your computer? Of the gaia.cs.umass.edu server?

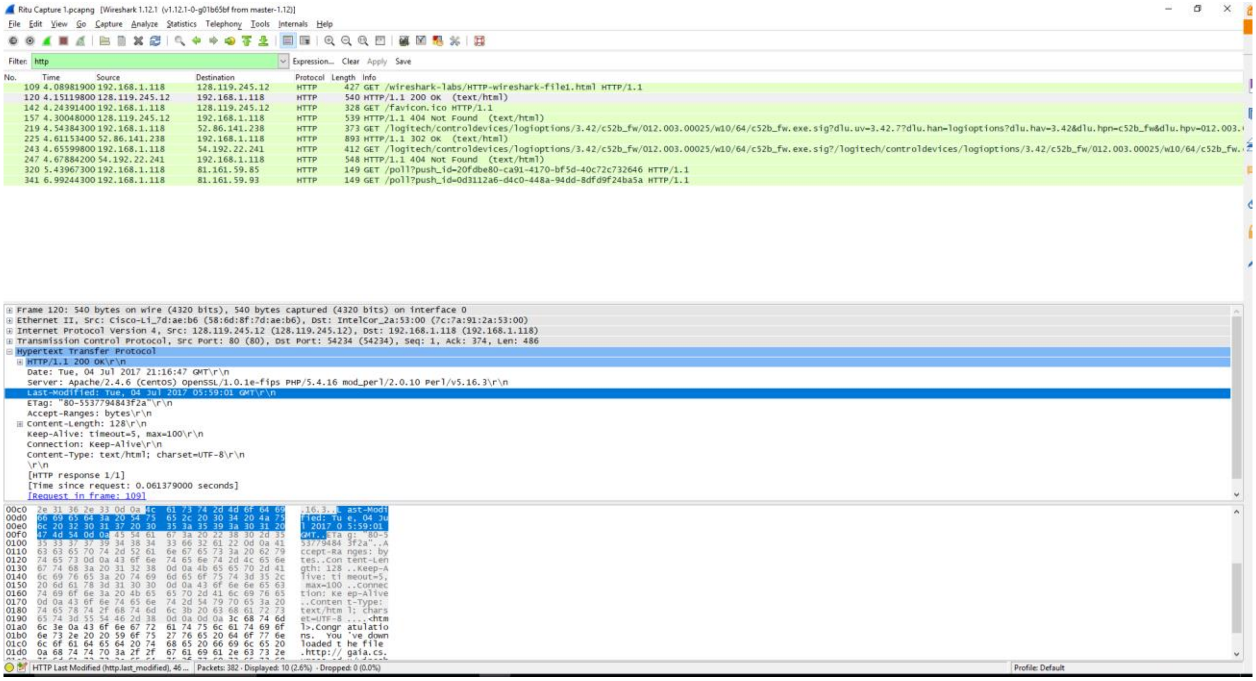
A. IP address of Computer : 192.168.1.118
   IP address of Server: 128.119.245.12

4. What is the status code returned from the server to your browser?

A. 200

5. When was the HTML file that you are retrieving last modified at the server?

A. Last Modified : Tue, 04 Jul 2017 05:59:01 GMT\r\n



Ritu Capture 1.pcapng [Wireshark 1.12.1 (v1.12.1-0-g01b65bf from master-1.12)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter:
Expression... Clear Apply Save

Filter: http

```
No.     Time        Source          Destination     Protocol Length Info
    109 4.08981900  192.168.1.118   128.119.245.12  HTTP       427 GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
    120 4.15119800  128.119.245.12  192.168.1.118   HTTP       540 HTTP/1.1 200 OK  (text/html)
    142 4.24391400  192.168.1.118   128.119.245.12  HTTP       328 GET /favicon.ico HTTP/1.1
    157 4.30048000  128.119.245.12  192.168.1.118   HTTP       539 HTTP/1.1 404 Not Found  (text/html)
    219 4.54384300  192.168.1.118   52.86.141.238   HTTP       373 GET /logitech/controldevices/logioptions/3.42/c52b_fw/012.003.00025/w10/64/c52b_fw.exe.sig?dlu.uv=3.42.7?dlu.han=logioptions?dlu.hav=3.42&dlu.hpn=c52b_fw&dlu.hpv=012.003.
    225 4.61153400  52.86.141.238   192.168.1.118   HTTP       893 HTTP/1.1 302 OK  (text/html)
    243 4.65599800  192.168.1.118   54.192.22.241   HTTP       412 GET /logitech/controldevices/logioptions/3.42/c52b_fw/012.003.00025/w10/64/c52b_fw.exe.sig?/logitech/controldevices/logioptions/3.42/c52b_fw/012.003.00025/w10/64/c52b_fw.
    247 4.67884200  54.192.22.241   192.168.1.118   HTTP       548 HTTP/1.1 404 Not Found  (text/html)
    320 5.43967300  192.168.1.118   81.161.59.85    HTTP       149 GET /poll?push_id=20fdbe80-ca91-4170-bf5d-40c72c732646 HTTP/1.1
    341 6.99244300  192.168.1.118   81.161.59.93    HTTP       149 GET /poll?push_id=0d3112a6-d4c0-448a-94dd-8dfd9f24ba5a HTTP/1.1
```

```
⊞ Frame 120: 540 bytes on wire (4320 bits), 540 bytes captured (4320 bits) on interface 0
⊞ Ethernet II, Src: Cisco-Li_7d:ae:b6 (58:6d:8f:7d:ae:b6), Dst: IntelCor_2a:53:00 (7c:7a:91:2a:53:00)
⊞ Internet Protocol Version 4, Src: 128.119.245.12 (128.119.245.12), Dst: 192.168.1.118 (192.168.1.118)
⊞ Transmission Control Protocol, Src Port: 80 (80), Dst Port: 54234 (54234), Seq: 1, Ack: 374, Len: 486
⊟ Hypertext Transfer Protocol
  ⊞ HTTP/1.1 200 OK\r\n
    Date: Tue, 04 Jul 2017 21:16:47 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.1e-fips PHP/5.4.16 mod_perl/2.0.10 Perl/v5.16.3\r\n
    Last-Modified: Tue, 04 Jul 2017 05:59:01 GMT\r\n
    ETag: "80-5537794843f2a"\r\n
    Accept-Ranges: bytes\r\n
  ⊞ Content-Length: 128\r\n
    Keep-Alive: timeout=5, max=100\r\n
    Connection: Keep-Alive\r\n
    Content-Type: text/html; charset=UTF-8\r\n
    \r\n
    [HTTP response 1/1]
    [Time since request: 0.061379000 seconds]
    [Request in frame: 109]
```

```
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 54 75  65 2c 20 30 34 20 4a 75   fied: Tu e, 04 Ju
00e0  6c 20 32 30 31 37 20 30  35 3a 35 39 3a 30 31 20   l 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 33 37 37 39 34 38 34  33 66 32 61 22 0d 0a 41   53779484 3f2a"..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.
```

HTTP Last Modified (http.last_modified), 46 ... | Packets: 382 · Displayed: 10 (2.6%) · Dropped: 0 (0.0%) | Profile: Default

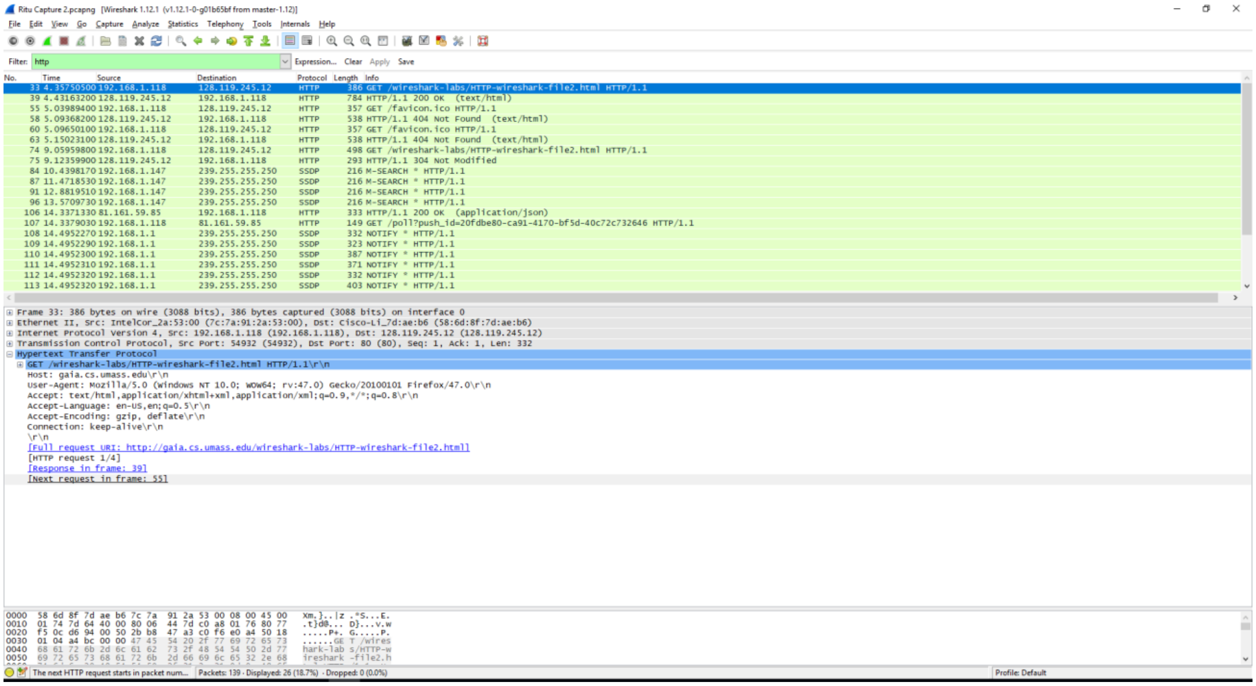
6. How many bytes of content are being returned to your browser?

A. 128 Bytes

7. By inspecting the raw data in the packet content window, do you see any headers within the data that are not displayed in the packet-listing window? If so, name one.

A. IP header

Part 2


Ritu Capture 2.pcapng [Wireshark 1.12.1 (v1.12.1-0-g01b65bf from master-1.12)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter: http
Expression... Clear Apply Save

```
No.   Time       Source          Destination      Protocol Length Info
   33 4.35750500 192.168.1.118   128.119.245.12   HTTP     386 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
   39 4.43163200 128.119.245.12  192.168.1.118    HTTP     784 HTTP/1.1 200 OK  (text/html)
   55 5.03989400 192.168.1.118   128.119.245.12   HTTP     357 GET /favicon.ico HTTP/1.1
   58 5.09368200 128.119.245.12  192.168.1.118    HTTP     538 HTTP/1.1 404 Not Found  (text/html)
   60 5.09650100 192.168.1.118   128.119.245.12   HTTP     357 GET /favicon.ico HTTP/1.1
   63 5.15023100 128.119.245.12  192.168.1.118    HTTP     538 HTTP/1.1 404 Not Found  (text/html)
   74 9.05959800 192.168.1.118   128.119.245.12   HTTP     498 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
   75 9.12359900 128.119.245.12  192.168.1.118    HTTP     293 HTTP/1.1 304 Not Modified
   84 10.4398170 192.168.1.147   239.255.255.250  SSDP     216 M-SEARCH * HTTP/1.1
   87 11.4718530 192.168.1.147   239.255.255.250  SSDP     216 M-SEARCH * HTTP/1.1
   91 12.8819510 192.168.1.147   239.255.255.250  SSDP     216 M-SEARCH * HTTP/1.1
   96 13.5709730 192.168.1.147   239.255.255.250  SSDP     216 M-SEARCH * HTTP/1.1
  106 14.3371330 81.161.59.85    192.168.1.118    HTTP     333 HTTP/1.1 200 OK  (application/json)
  107 14.3379030 192.168.1.118   81.161.59.85     HTTP     149 GET /poll?push_id=20fdbe80-ca91-4170-bf5d-40c72c732646 HTTP/1.1
  108 14.4952270 192.168.1.1     239.255.255.250  SSDP     332 NOTIFY * HTTP/1.1
  109 14.4952290 192.168.1.1     239.255.255.250  SSDP     323 NOTIFY * HTTP/1.1
  110 14.4952300 192.168.1.1     239.255.255.250  SSDP     387 NOTIFY * HTTP/1.1
  111 14.4952310 192.168.1.1     239.255.255.250  SSDP     371 NOTIFY * HTTP/1.1
  112 14.4952320 192.168.1.1     239.255.255.250  SSDP     332 NOTIFY * HTTP/1.1
  113 14.4952320 192.168.1.1     239.255.255.250  SSDP     403 NOTIFY * HTTP/1.1
```

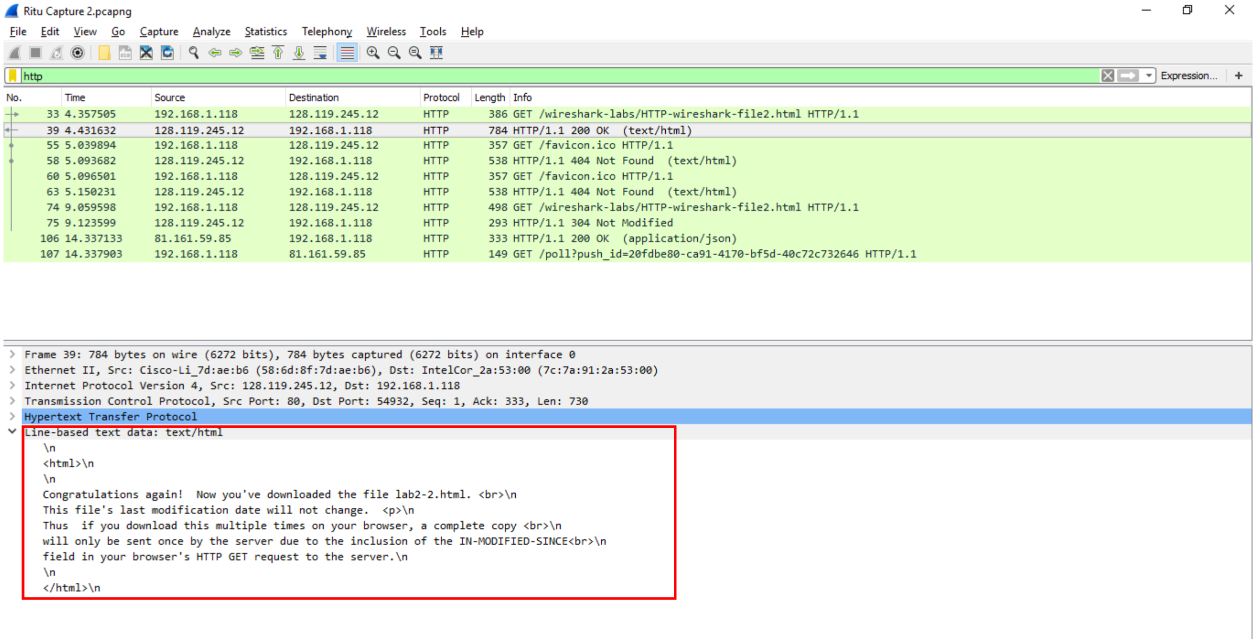
```
⊞ Frame 33: 386 bytes on wire (3088 bits), 386 bytes captured (3088 bits) on interface 0
⊞ Ethernet II, Src: IntelCor_2a:53:00 (7c:7a:91:2a:53:00), Dst: Cisco-Li_7d:ae:b6 (58:6d:8f:7d:ae:b6)
⊞ Internet Protocol Version 4, Src: 192.168.1.118 (192.168.1.118), Dst: 128.119.245.12 (128.119.245.12)
⊞ Transmission Control Protocol, Src Port: 54932 (54932), Dst Port: 80 (80), Seq: 1, Ack: 1, Len: 332
⊟ Hypertext Transfer Protocol
  ⊞ GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n
    Host: gaia.cs.umass.edu\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:47.0) Gecko/20100101 Firefox/47.0\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n
    Accept-Language: en-US,en;q=0.5\r\n
    Accept-Encoding: gzip, deflate\r\n
    Connection: keep-alive\r\n
    \r\n
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]
    [HTTP request 1/4]
    [Response in frame: 39]
    [Next request in frame: 55]
```

```
0000  58 6d 8f 7d ae b6 7c 7a  91 2a 53 00 08 00 45 00   Xm.}..|z .*S...E.
0010  01 74 7d 64 40 00 80 06  44 7d c0 a8 01 76 80 77   .t}d@... D}...v.w
0020  f5 0c d6 94 00 50 2b b8  47 a3 c0 f6 e0 a4 50 18   .....P+. G.....P.
0030  01 04 a4 bc 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 32 2e 68   ireshark -file2.h
```

The next HTTP request starts in packet num...
Packets: 139 · Displayed: 26 (18.7%) · Dropped: 0 (0.0%)
Profile: Default

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

A. NO

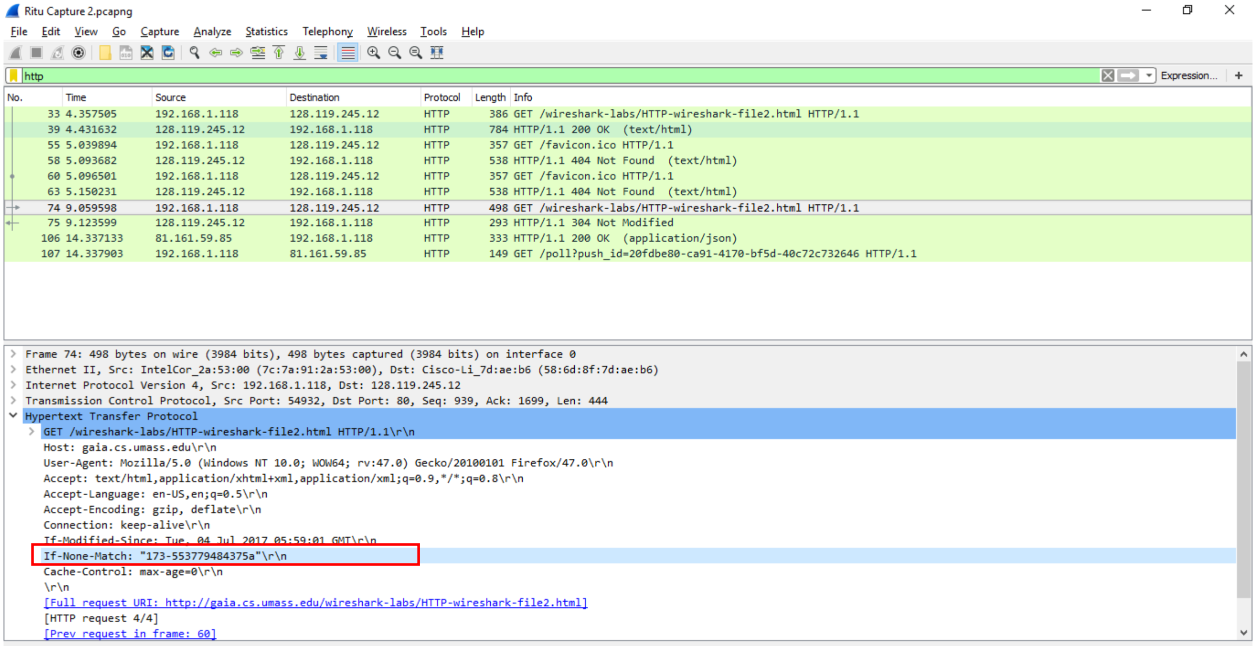

Ritu Capture 2.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
Expression...

```
No.   Time       Source          Destination     Protocol Length Info
   33 4.357505   192.168.1.118   128.119.245.12  HTTP     386 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
   39 4.431632   128.119.245.12  192.168.1.118   HTTP     784 HTTP/1.1 200 OK  (text/html)
   55 5.039894   192.168.1.118   128.119.245.12  HTTP     357 GET /favicon.ico HTTP/1.1
   58 5.093682   128.119.245.12  192.168.1.118   HTTP     538 HTTP/1.1 404 Not Found  (text/html)
   60 5.096501   192.168.1.118   128.119.245.12  HTTP     357 GET /favicon.ico HTTP/1.1
   63 5.150231   128.119.245.12  192.168.1.118   HTTP     538 HTTP/1.1 404 Not Found  (text/html)
   74 9.059598   192.168.1.118   128.119.245.12  HTTP     498 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
   75 9.123599   128.119.245.12  192.168.1.118   HTTP     293 HTTP/1.1 304 Not Modified
  106 14.337133  81.161.59.85    192.168.1.118   HTTP     333 HTTP/1.1 200 OK  (application/json)
  107 14.337903  192.168.1.118   81.161.59.85    HTTP     149 GET /poll?push_id=20fdbe80-ca91-4170-bf5d-40c72c732646 HTTP/1.1
```

```
> Frame 39: 784 bytes on wire (6272 bits), 784 bytes captured (6272 bits) on interface 0
> Ethernet II, Src: Cisco-Li_7d:ae:b6 (58:6d:8f:7d:ae:b6), Dst: IntelCor_2a:53:00 (7c:7a:91:2a:53:00)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.118
> Transmission Control Protocol, Src Port: 80, Dst Port: 54932, Seq: 1, Ack: 333, Len: 730
> Hypertext Transfer Protocol
v 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
```

9. Inspect the contents of the server response. Did the server explicitly return the contents of the file? How can you tell?

A. The server returns the entire contents of the file (as seen in above screenshot).


Ritu Capture 2.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expression…
+

```
http
```

```
No.    Time       Source          Destination     Protocol Length Info
    33 4.357505   192.168.1.118   128.119.245.12  HTTP      386 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
    39 4.431632   128.119.245.12  192.168.1.118   HTTP      784 HTTP/1.1 200 OK  (text/html)
    55 5.039894   192.168.1.118   128.119.245.12  HTTP      357 GET /favicon.ico HTTP/1.1
    58 5.093682   128.119.245.12  192.168.1.118   HTTP      538 HTTP/1.1 404 Not Found  (text/html)
    60 5.096501   192.168.1.118   128.119.245.12  HTTP      357 GET /favicon.ico HTTP/1.1
    63 5.150231   128.119.245.12  192.168.1.118   HTTP      538 HTTP/1.1 404 Not Found  (text/html)
    74 9.059598   192.168.1.118   128.119.245.12  HTTP      498 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
    75 9.123599   128.119.245.12  192.168.1.118   HTTP      293 HTTP/1.1 304 Not Modified
   106 14.337133  81.161.59.85    192.168.1.118   HTTP      333 HTTP/1.1 200 OK  (application/json)
   107 14.337903  192.168.1.118   81.161.59.85    HTTP      149 GET /poll?push_id=20fdbe80-ca91-4170-bf5d-40c72c732646 HTTP/1.1
```

```
> Frame 74: 498 bytes on wire (3984 bits), 498 bytes captured (3984 bits) on interface 0
> Ethernet II, Src: IntelCor_2a:53:00 (7c:7a:91:2a:53:00), Dst: Cisco-Li_7d:ae:b6 (58:6d:8f:7d:ae:b6)
> Internet Protocol Version 4, Src: 192.168.1.118, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 54932, Dst Port: 80, Seq: 939, Ack: 1699, Len: 444
v Hypertext Transfer Protocol
  > GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n
    Host: gaia.cs.umass.edu\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:47.0) Gecko/20100101 Firefox/47.0\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n
    Accept-Language: en-US,en;q=0.5\r\n
    Accept-Encoding: gzip, deflate\r\n
    Connection: keep-alive\r\n
    If-Modified-Since: Tue, 04 Jul 2017 05:59:01 GMT\r\n
    If-None-Match: "173-553779484375a"\r\n
    Cache-Control: max-age=0\r\n
    \r\n
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]
    [HTTP request 4/4]
    [Prev request in frame: 60]
```

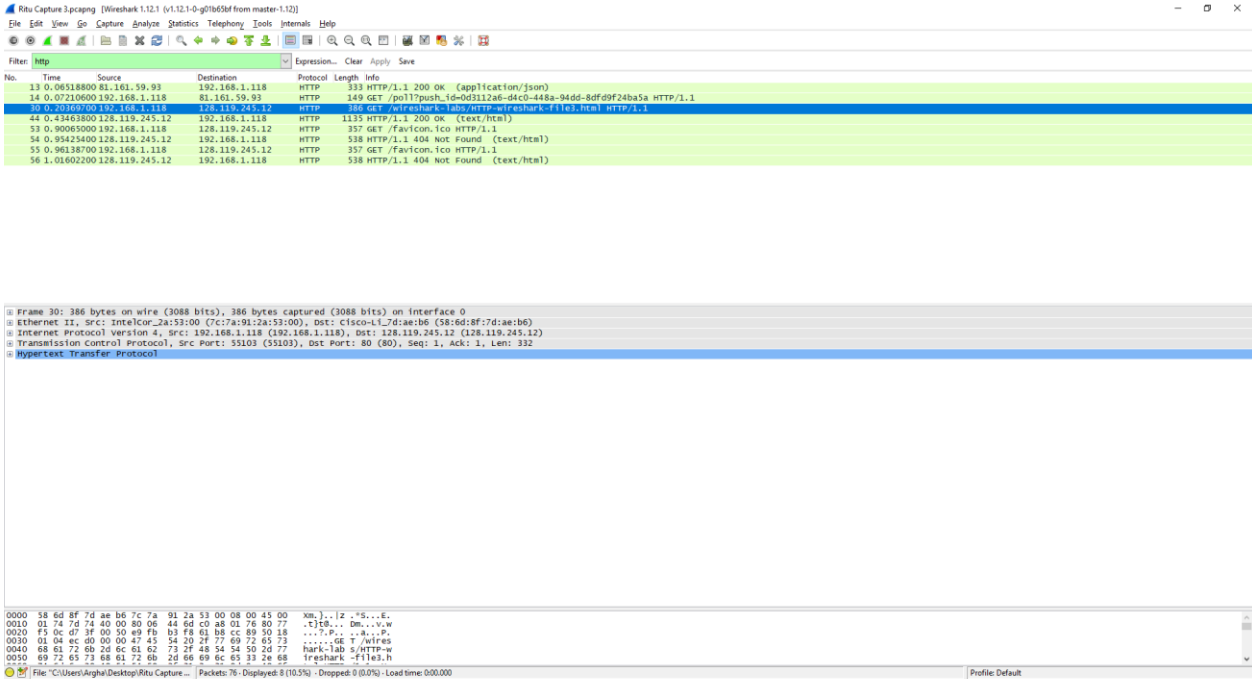
10. Now inspect the contents of the second HTTP GET request from your browser to the server. Do you see an “IF-MODIFIED-SINCE:” line in the HTTP GET? If so, what information follows the “IF-MODIFIED-SINCE:” header?

A. Yes we can see the “IF-MODIFIED-SINCE:” in the second GET request.
It is followed by the information “**If-None-Match: “173-553779484375a”\r\n** (as seen in above screenshot).

11. What is the HTTP status code and phrase returned from the server in response to this second HTTP GET? Did the server explicitly return the contents of the file? Explain.

A. We get a 304 Not Modified. The server doesn’t explicitly return the content of the file since it had already sent it earlier response. (and it would be a wastage of bandwidth).

Part 3


Ritu Capture 3.pcapng [Wireshark 1.12.1 (v1.12.1-0-g01b65bf from master-1.12)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Expression... Clear Apply Save

Filter: http

```
No.  Time         Source          Destination     Protocol Length Info
  13 0.06518800   81.161.59.93    192.168.1.118   HTTP      333 HTTP/1.1 200 OK  (application/json)
  14 0.07210600   192.168.1.118   81.161.59.93    HTTP      149 GET /poll?push_id=0d3112a6-d4c0-448a-94dd-8dfd9f24ba5a HTTP/1.1
  30 0.20369700   192.168.1.118   128.119.245.12  HTTP      386 GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
  44 0.43463800   128.119.245.12  192.168.1.118   HTTP     1135 HTTP/1.1 200 OK  (text/html)
  53 0.90065000   192.168.1.118   128.119.245.12  HTTP      357 GET /favicon.ico HTTP/1.1
  54 0.95425400   128.119.245.12  192.168.1.118   HTTP      538 HTTP/1.1 404 Not Found  (text/html)
  55 0.96138700   192.168.1.118   128.119.245.12  HTTP      357 GET /favicon.ico HTTP/1.1
  56 1.01602200   128.119.245.12  192.168.1.118   HTTP      538 HTTP/1.1 404 Not Found  (text/html)
```

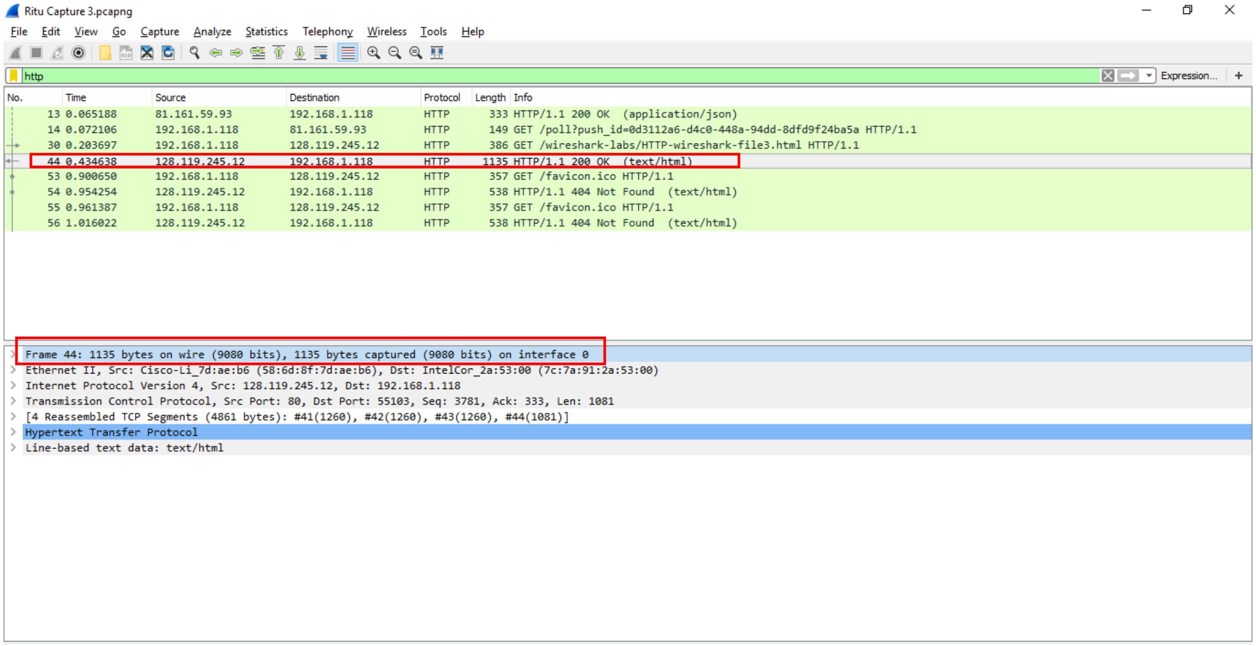
```
⊞ Frame 30: 386 bytes on wire (3088 bits), 386 bytes captured (3088 bits) on interface 0
⊞ Ethernet II, Src: IntelCor_2a:53:00 (7c:7a:91:2a:53:00), Dst: Cisco-Li_7d:ae:b6 (58:6d:8f:7d:ae:b6)
⊞ Internet Protocol Version 4, Src: 192.168.1.118 (192.168.1.118), Dst: 128.119.245.12 (128.119.245.12)
⊞ Transmission Control Protocol, Src Port: 55103 (55103), Dst Port: 80 (80), Seq: 1, Ack: 1, Len: 332
⊞ Hypertext Transfer Protocol
```

```
0000  58 6d 8f 7d ae b6 7c 7a  91 2a 53 00 08 00 45 00   Xm.}..|z .*S...E.
0010  01 74 7d 74 40 00 80 06  44 6d c0 a8 01 76 80 77   .t}t@... Dm...v.w
0020  f5 0c d7 3f 00 50 e9 fb  b3 f8 61 b8 cc 89 50 18   ...?.P.. ..a...P.
0030  01 04 ec d0 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
```

File: "C:\Users\Argha\Desktop\Ritu Capture ... | Packets: 76 · Displayed: 8 (10.5%) · Dropped: 0 (0.0%) · Load time: 0:00.000 | Profile: Default

12. How many HTTP GET request messages did your browser send? Which packet number in the trace contains the GET message for the Bill or Rights?

A. Our Brower sent only 1 HTTP GET request.
   Packet number 30 contains the GET message for the Bill of Rights.


Ritu Capture 3.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expression... +

http

```
No.  Time      Source          Destination     Protocol Length Info
  13 0.065188  81.161.59.93    192.168.1.118   HTTP      333 HTTP/1.1 200 OK  (application/json)
  14 0.072106  192.168.1.118   81.161.59.93    HTTP      149 GET /poll?push_id=0d3112a6-d4c0-448a-94dd-8dfd9f24ba5a HTTP/1.1
  30 0.203697  192.168.1.118   128.119.245.12  HTTP      386 GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
  44 0.434638  128.119.245.12  192.168.1.118   HTTP     1135 HTTP/1.1 200 OK  (text/html)
  53 0.900650  192.168.1.118   128.119.245.12  HTTP      357 GET /favicon.ico HTTP/1.1
  54 0.954254  128.119.245.12  192.168.1.118   HTTP      538 HTTP/1.1 404 Not Found  (text/html)
  55 0.961387  192.168.1.118   128.119.245.12  HTTP      357 GET /favicon.ico HTTP/1.1
  56 1.016022  128.119.245.12  192.168.1.118   HTTP      538 HTTP/1.1 404 Not Found  (text/html)
```

```
> Frame 44: 1135 bytes on wire (9080 bits), 1135 bytes captured (9080 bits) on interface 0
> Ethernet II, Src: Cisco-Li_7d:ae:b6 (58:6d:8f:7d:ae:b6), Dst: IntelCor_2a:53:00 (7c:7a:91:2a:53:00)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.118
> Transmission Control Protocol, Src Port: 80, Dst Port: 55103, Seq: 3781, Ack: 333, Len: 1081
> [4 Reassembled TCP Segments (4861 bytes): #41(1260), #42(1260), #43(1260), #44(1081)]
> Hypertext Transfer Protocol
> Line-based text data: text/html
```

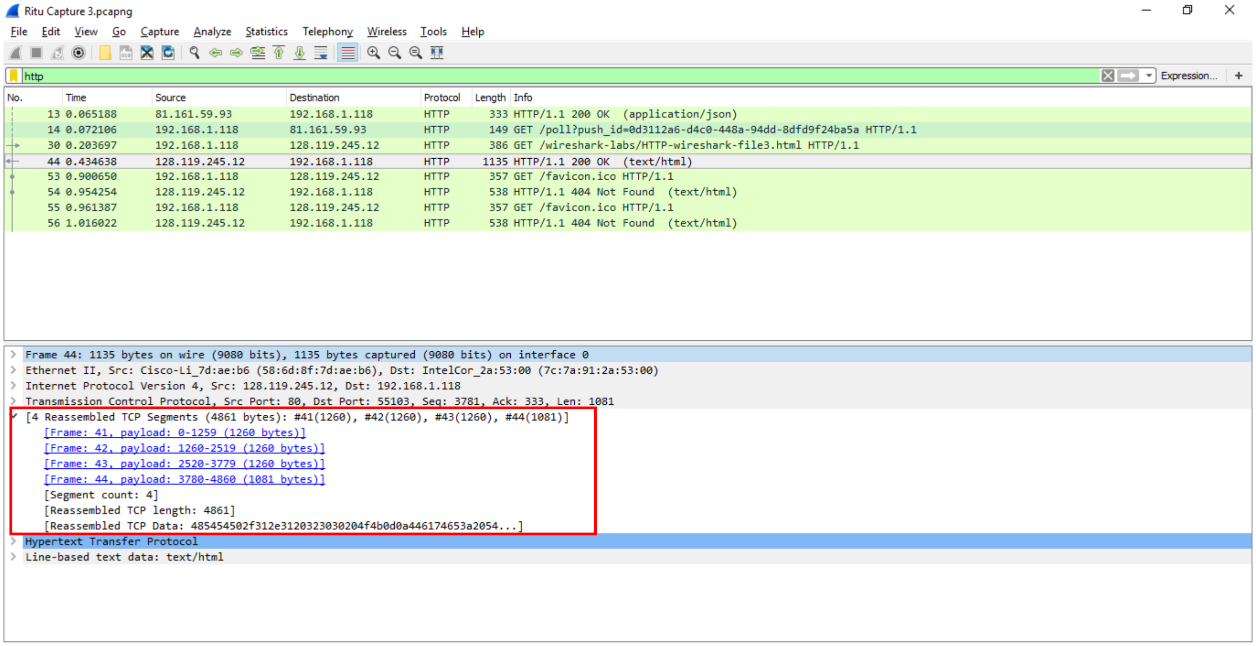
13. Which packet number in the trace contains the status code and phrase associated with the response to the HTTP GET request?

A. The response is in packet number 44 (as seen in above screenshot).

14. What is the status code and phrase in the response?

A. Status Code : 200

Phrase response is: OK


Ritu Capture 3.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
Expression...
+

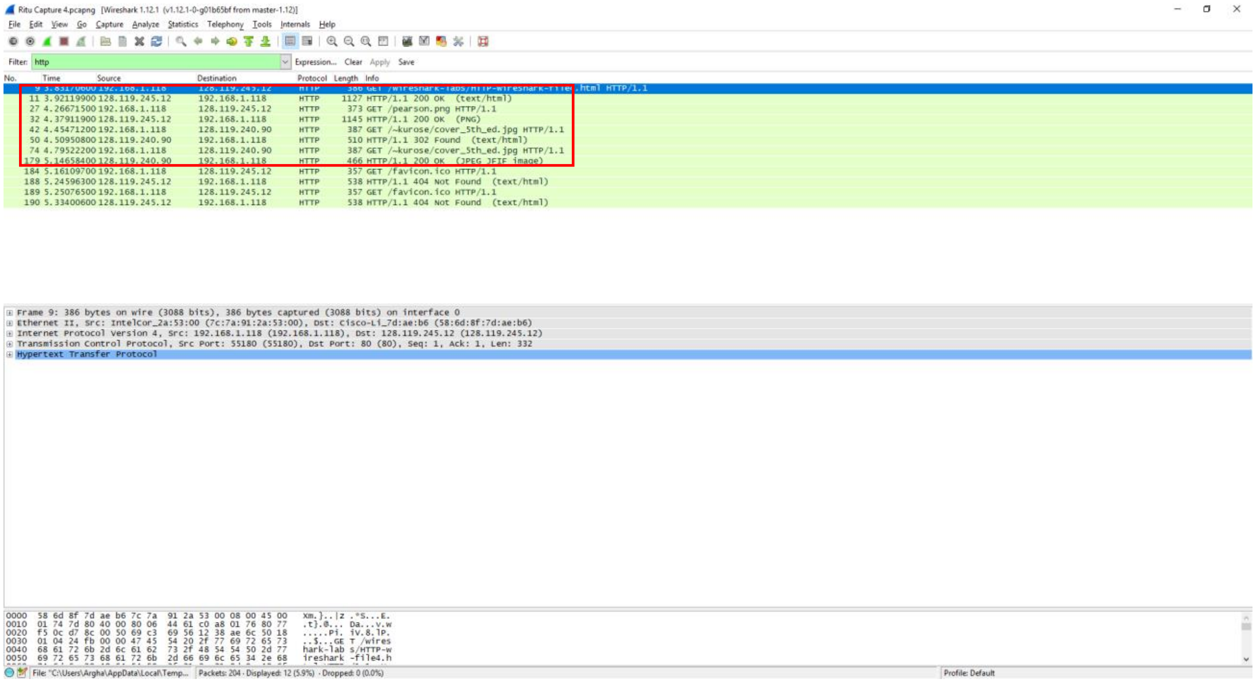
```
No.  Time       Source          Destination     Protocol Length Info
  13 0.065188   81.161.59.93    192.168.1.118   HTTP      333 HTTP/1.1 200 OK  (application/json)
  14 0.072106   192.168.1.118   81.161.59.93    HTTP      149 GET /poll?push_id=0d3112a6-d4c0-448a-94dd-8dfd9f24ba5a HTTP/1.1
  30 0.203697   192.168.1.118   128.119.245.12  HTTP      386 GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
  44 0.434638   128.119.245.12  192.168.1.118   HTTP     1135 HTTP/1.1 200 OK  (text/html)
  53 0.900650   192.168.1.118   128.119.245.12  HTTP      357 GET /favicon.ico HTTP/1.1
  54 0.954254   128.119.245.12  192.168.1.118   HTTP      538 HTTP/1.1 404 Not Found  (text/html)
  55 0.961387   192.168.1.118   128.119.245.12  HTTP      357 GET /favicon.ico HTTP/1.1
  56 1.016022   128.119.245.12  192.168.1.118   HTTP      538 HTTP/1.1 404 Not Found  (text/html)
```

```
> Frame 44: 1135 bytes on wire (9080 bits), 1135 bytes captured (9080 bits) on interface 0
> Ethernet II, Src: Cisco-Li_7d:ae:b6 (58:6d:8f:7d:ae:b6), Dst: IntelCor_2a:53:00 (7c:7a:91:2a:53:00)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.118
> Transmission Control Protocol, Src Port: 80, Dst Port: 55103, Seq: 3781, Ack: 333, Len: 1081
✓ [4 Reassembled TCP Segments (4861 bytes): #41(1260), #42(1260), #43(1260), #44(1081)]
     [Frame: 41, payload: 0-1259 (1260 bytes)]
     [Frame: 42, payload: 1260-2519 (1260 bytes)]
     [Frame: 43, payload: 2520-3779 (1260 bytes)]
     [Frame: 44, payload: 3780-4860 (1081 bytes)]
     [Segment count: 4]
     [Reassembled TCP length: 4861]
     [Reassembled TCP Data: 485454502f312e3120323030204f4b0d0a446174653a2054...]
> Hypertext Transfer Protocol
> Line-based text data: text/html
```

15. How many data-containing TCP segments were needed to carry the single HTTP response and the text of the Bill of Rights?

A. 4 TCP Segments

Part 4


Ritu Capture 4.pcapng [Wireshark 1.12.1 (v1.12.1-0-g01b65bf from master-1.12)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter: http
Expression... Clear Apply Save

```
No.    Time       Source           Destination      Protocol Length Info
     9 3.83170600 192.168.1.118    128.119.245.12   HTTP      386 GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
    11 3.92119900 128.119.245.12   192.168.1.118    HTTP     1127 HTTP/1.1 200 OK  (text/html)
    27 4.26671500 192.168.1.118    128.119.245.12   HTTP      373 GET /pearson.png HTTP/1.1
    32 4.37911900 128.119.245.12   192.168.1.118    HTTP     1145 HTTP/1.1 200 OK  (PNG)
    42 4.45471200 192.168.1.118    128.119.240.90   HTTP      387 GET /~kurose/cover_5th_ed.jpg HTTP/1.1
    50 4.50950800 128.119.240.90   192.168.1.118    HTTP      510 HTTP/1.1 302 Found  (text/html)
    74 4.79522200 192.168.1.118    128.119.240.90   HTTP      387 GET /~kurose/cover_5th_ed.jpg HTTP/1.1
   179 5.14658400 128.119.240.90   192.168.1.118    HTTP      466 HTTP/1.1 200 OK  (JPEG JFIF image)
   184 5.16109700 192.168.1.118    128.119.245.12   HTTP      357 GET /favicon.ico HTTP/1.1
   188 5.24596300 128.119.245.12   192.168.1.118    HTTP      538 HTTP/1.1 404 Not Found  (text/html)
   189 5.25076500 192.168.1.118    128.119.245.12   HTTP      357 GET /favicon.ico HTTP/1.1
   190 5.33400600 128.119.245.12   192.168.1.118    HTTP      538 HTTP/1.1 404 Not Found  (text/html)
```

```
⊞ Frame 9: 386 bytes on wire (3088 bits), 386 bytes captured (3088 bits) on interface 0
⊞ Ethernet II, Src: IntelCor_2a:53:00 (7c:7a:91:2a:53:00), Dst: Cisco-Li_7d:ae:b6 (58:6d:8f:7d:ae:b6)
⊞ Internet Protocol Version 4, Src: 192.168.1.118 (192.168.1.118), Dst: 128.119.245.12 (128.119.245.12)
⊞ Transmission Control Protocol, Src Port: 55180 (55180), Dst Port: 80 (80), Seq: 1, Ack: 1, Len: 332
⊞ Hypertext Transfer Protocol
```

```
0000  58 6d 8f 7d ae b6 7c 7a  91 2a 53 00 08 00 45 00   Xm.}..|z .*S...E.
0010  01 74 7d 80 40 00 80 06  44 61 c0 a8 01 76 80 77   .t}.@... Da...v.w
0020  f5 0c d7 8c 00 50 69 c3  69 56 12 38 ae 6c 50 18   .....Pi. iV.8.lP.
0030  01 04 24 fb 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
```

File: "C:\Users\Argha\AppData\Local\Temp... | Packets: 204 · Displayed: 12 (5.9%) · Dropped: 0 (0.0%) | Profile: Default

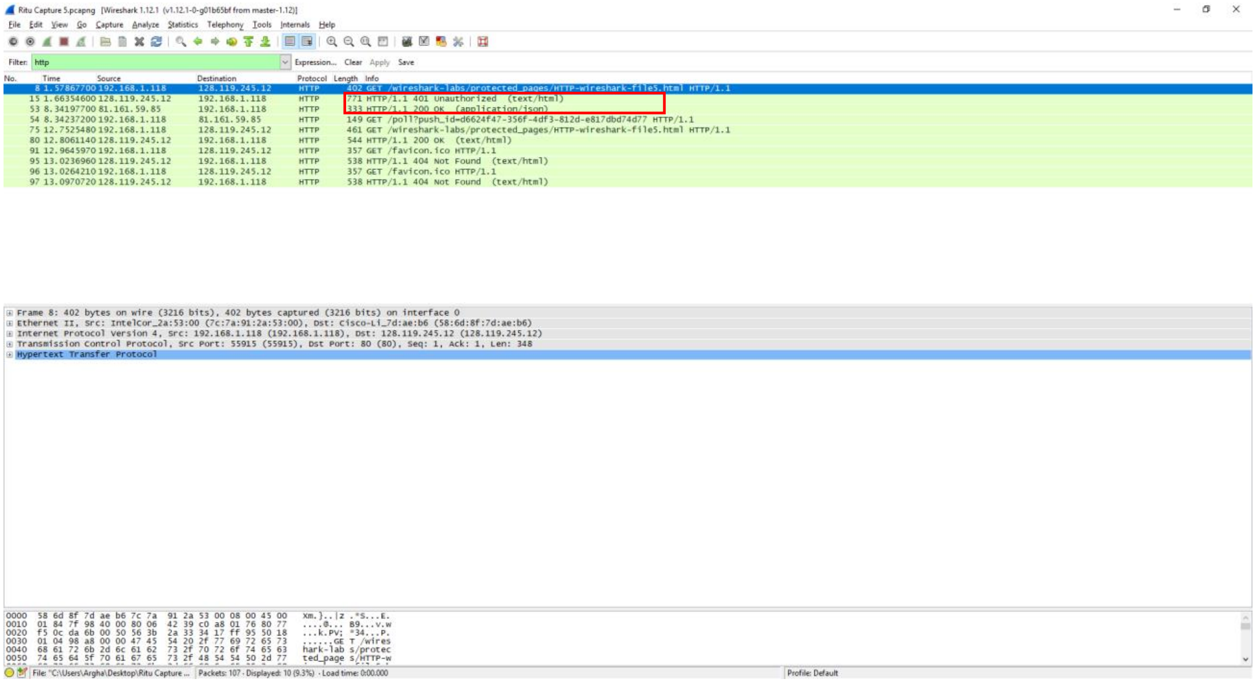
16. How many HTTP GET request messages did your browser send? To which Internet addresses were these GET requests sent?

A. 4
The GET requested were sent to the following Internet address
128.119.245.12
128.119.240.90

17. Can you tell whether your browser downloaded the two images serially, or whether they were downloaded from the two web sites in parallel? Explain.

A. The two images were downloaded serially because it looks like the 1st image was downloaded from the same IP address and for the 2nd image, it had to fetch it from another IP address.

Part 5


Ritu Capture 5.pcapng [Wireshark 1.12.1 (v1.12.1-0-g01b65bf from master-1.12)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Expression... Clear Apply Save

Filter: http

```
No.    Time        Source           Destination      Protocol Length Info
     8 1.57867700  192.168.1.118    128.119.245.12   HTTP     402 GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
    15 1.66354600  128.119.245.12   192.168.1.118    HTTP     771 HTTP/1.1 401 Unauthorized  (text/html)
    53 8.34197700  81.161.59.85     192.168.1.118    HTTP     333 HTTP/1.1 200 OK  (application/json)
    54 8.34237200  192.168.1.118    81.161.59.85     HTTP     149 GET /poll?push_id=d6624f47-356f-4df3-812d-e817dbd74d77 HTTP/1.1
    75 12.7525480  192.168.1.118    128.119.245.12   HTTP     461 GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
    80 12.8061140  128.119.245.12   192.168.1.118    HTTP     544 HTTP/1.1 200 OK  (text/html)
    91 12.9645970  192.168.1.118    128.119.245.12   HTTP     357 GET /favicon.ico HTTP/1.1
    95 13.0236960  128.119.245.12   192.168.1.118    HTTP     538 HTTP/1.1 404 Not Found  (text/html)
    96 13.0264210  192.168.1.118    128.119.245.12   HTTP     357 GET /favicon.ico HTTP/1.1
    97 13.0970720  128.119.245.12   192.168.1.118    HTTP     538 HTTP/1.1 404 Not Found  (text/html)
```

```
⊞ Frame 8: 402 bytes on wire (3216 bits), 402 bytes captured (3216 bits) on interface 0
⊞ Ethernet II, Src: IntelCor_2a:53:00 (7c:7a:91:2a:53:00), Dst: Cisco-Li_7d:ae:b6 (58:6d:8f:7d:ae:b6)
⊞ Internet Protocol Version 4, Src: 192.168.1.118 (192.168.1.118), Dst: 128.119.245.12 (128.119.245.12)
⊞ Transmission Control Protocol, Src Port: 55915 (55915), Dst Port: 80 (80), Seq: 1, Ack: 1, Len: 348
⊞ Hypertext Transfer Protocol
```

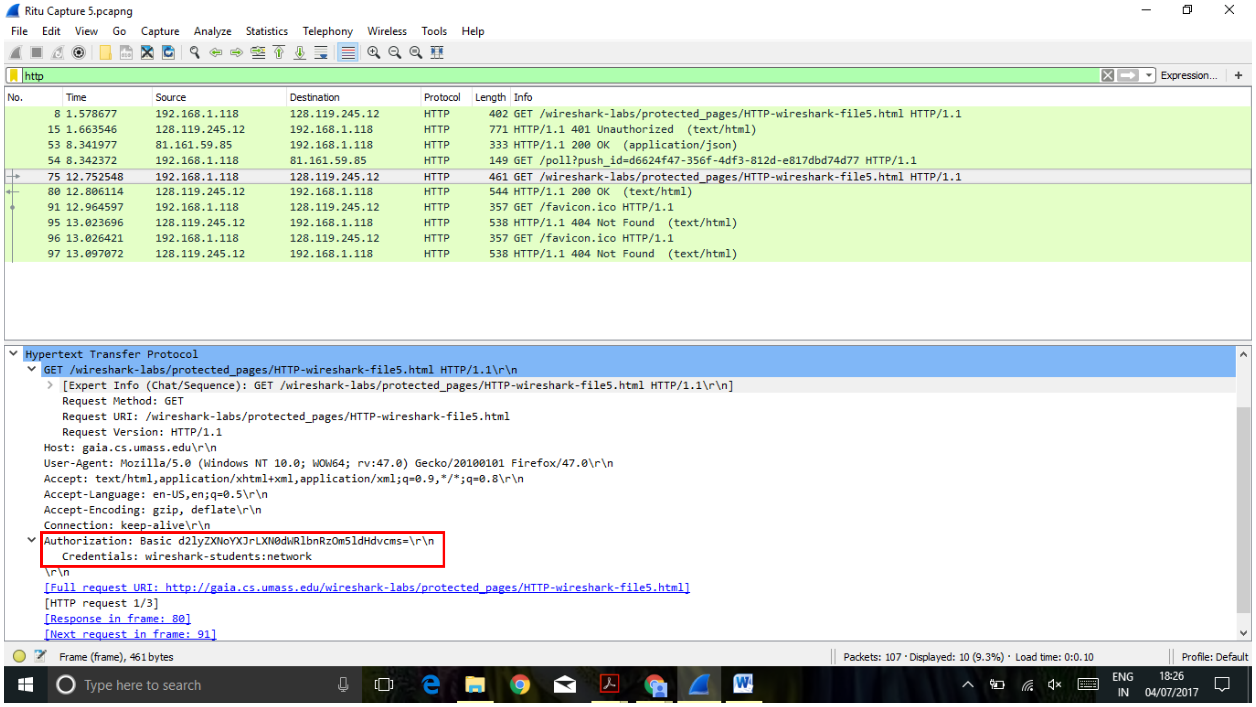
```
0000  58 6d 8f 7d ae b6 7c 7a  91 2a 53 00 08 00 45 00   Xm.}..|z .*S...E.
0010  01 84 7f 98 40 00 80 06  42 39 c0 a8 01 76 80 77   ....@... B9...v.w
0020  f5 0c da 6b 00 50 56 3b  2a 33 34 17 ff 95 50 18   ...k.PV; *34...P.
0030  01 04 98 a8 00 00 47 45  54 20 2f 77 69 72 65 73   ......GE T /wires
0040  68 61 72 6b 2d 6c 61 62  73 2f 70 72 6f 74 65 63   hark-lab s/protec
0050  74 65 64 5f 70 61 67 65  73 2f 48 54 54 50 2d 77   ted_page s/HTTP-w
```

File: "C:\Users\Argha\Desktop\Ritu Capture ... | Packets: 107 · Displayed: 10 (9.3%) · Load time: 0:00.000 | Profile: Default

18. What is the server’s response (status code and phrase) in response to the initial HTTP GET message from your browser?

A. Status Code : 401

   Phrase: Unauthorized


Ritu Capture 5.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
Expression…
+

```
No.     Time        Source           Destination      Protocol  Length  Info
      8 1.578677    192.168.1.118    128.119.245.12   HTTP       402 GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
     15 1.663546    128.119.245.12   192.168.1.118    HTTP       771 HTTP/1.1 401 Unauthorized  (text/html)
     53 8.341977    81.161.59.85     192.168.1.118    HTTP       333 HTTP/1.1 200 OK  (application/json)
     54 8.342372    192.168.1.118    81.161.59.85     HTTP       149 GET /poll?push_id=d6624f47-356f-4df3-812d-e817dbd74d77 HTTP/1.1
     75 12.752548   192.168.1.118    128.119.245.12   HTTP       461 GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
     80 12.806114   128.119.245.12   192.168.1.118    HTTP       544 HTTP/1.1 200 OK  (text/html)
     91 12.964597   192.168.1.118    128.119.245.12   HTTP       357 GET /favicon.ico HTTP/1.1
     95 13.023696   128.119.245.12   192.168.1.118    HTTP       538 HTTP/1.1 404 Not Found  (text/html)
     96 13.026421   192.168.1.118    128.119.245.12   HTTP       357 GET /favicon.ico HTTP/1.1
     97 13.097072   128.119.245.12   192.168.1.118    HTTP       538 HTTP/1.1 404 Not Found  (text/html)
```

```
Hypertext Transfer Protocol
  GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1\r\n
    [Expert Info (Chat/Sequence): GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1\r\n]
    Request Method: GET
    Request URI: /wireshark-labs/protected_pages/HTTP-wireshark-file5.html
    Request Version: HTTP/1.1
  Host: gaia.cs.umass.edu\r\n
  User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:47.0) Gecko/20100101 Firefox/47.0\r\n
  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n
  Accept-Language: en-US,en;q=0.5\r\n
  Accept-Encoding: gzip, deflate\r\n
  Connection: keep-alive\r\n
  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 1/3]
  [Response in frame: 80]
  [Next request in frame: 91]
```

```
Frame (frame), 461 bytes        Packets: 107 · Displayed: 10 (9.3%) · Load time: 0:0.10        Profile: Default
```

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

A. A new field of Authorization and Credentials are added in the 2nd GET message. (as seen in above screenshot)