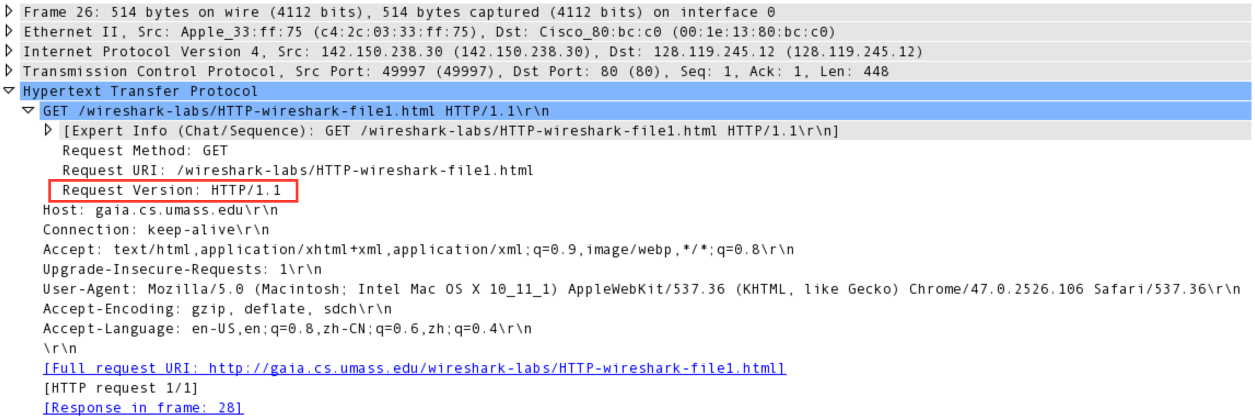
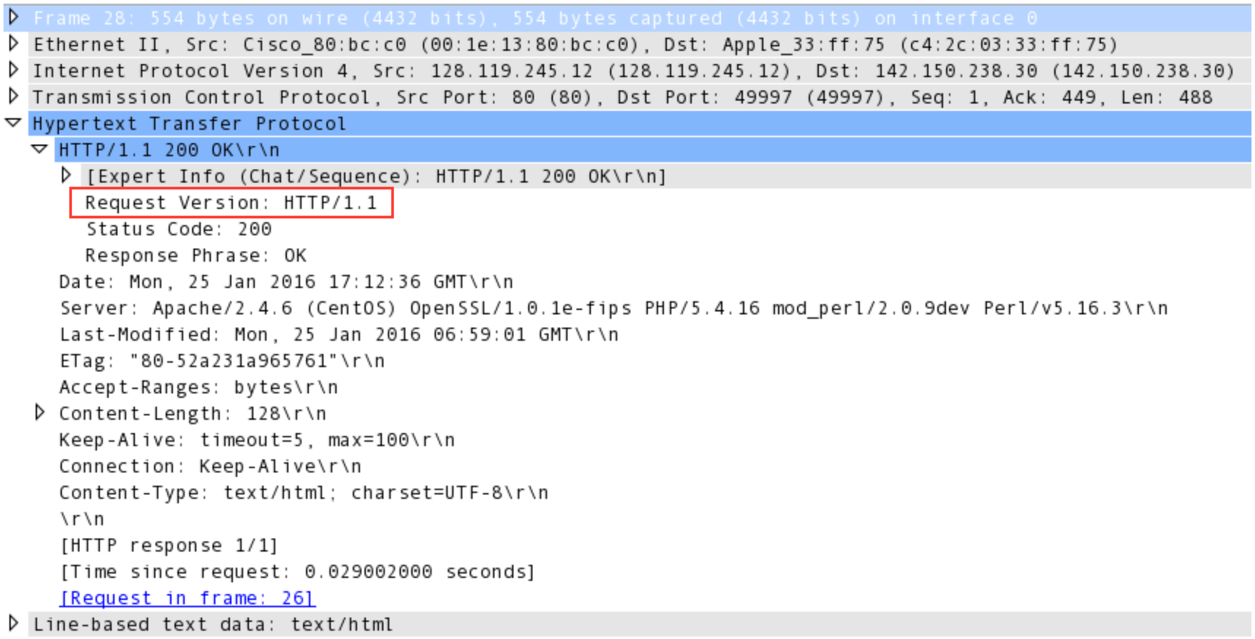
CSC358 Wireshark Assignment 2 Solution

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

Solution:
Both of them are version 1.1
(HTTP version information is listed in the item 'Request Version')



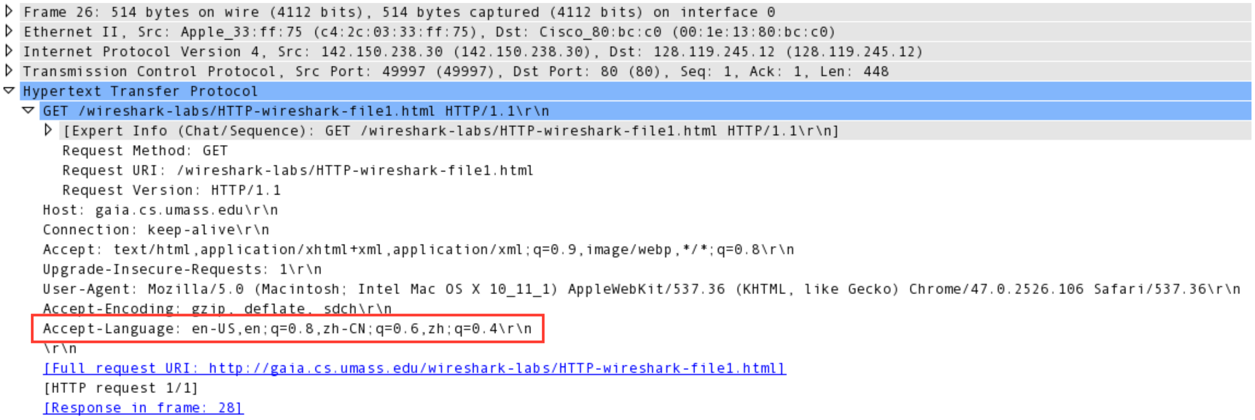
```
▷ Frame 26: 514 bytes on wire (4112 bits), 514 bytes captured (4112 bits) on interface 0
▷ Ethernet II, Src: Apple_33:ff:75 (c4:2c:03:33:ff:75), Dst: Cisco_80:bc:c0 (00:1e:13:80:bc:c0)
▷ Internet Protocol Version 4, Src: 142.150.238.30 (142.150.238.30), Dst: 128.119.245.12 (128.119.245.12)
▷ Transmission Control Protocol, Src Port: 49997 (49997), Dst Port: 80 (80), Seq: 1, Ack: 1, Len: 448
▽ Hypertext Transfer Protocol
  ▽ GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n
    ▷ [Expert Info (Chat/Sequence): GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n]
      Request Method: GET
      Request URI: /wireshark-labs/HTTP-wireshark-file1.html
      Request Version: HTTP/1.1
    Host: gaia.cs.umass.edu\r\n
    Connection: keep-alive\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8\r\n
    Upgrade-Insecure-Requests: 1\r\n
    User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/47.0.2526.106 Safari/537.36\r\n
    Accept-Encoding: gzip, deflate, sdch\r\n
    Accept-Language: en-US,en;q=0.8,zh-CN;q=0.6,zh;q=0.4\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: 28]
```



```
▷ Frame 28: 554 bytes on wire (4432 bits), 554 bytes captured (4432 bits) on interface 0
▷ Ethernet II, Src: Cisco_80:bc:c0 (00:1e:13:80:bc:c0), Dst: Apple_33:ff:75 (c4:2c:03:33:ff:75)
▷ Internet Protocol Version 4, Src: 128.119.245.12 (128.119.245.12), Dst: 142.150.238.30 (142.150.238.30)
▷ Transmission Control Protocol, Src Port: 80 (80), Dst Port: 49997 (49997), Seq: 1, Ack: 449, Len: 488
▽ Hypertext Transfer Protocol
  ▽ 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
      Response Phrase: OK
    Date: Mon, 25 Jan 2016 17:12:36 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.1e-fips PHP/5.4.16 mod_perl/2.0.9dev Perl/v5.16.3\r\n
    Last-Modified: Mon, 25 Jan 2016 06:59:01 GMT\r\n
    ETag: "80-52a231a965761"\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: 0.029002000 seconds]
    [Request in frame: 26]
▷ Line-based text data: text/html
```

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

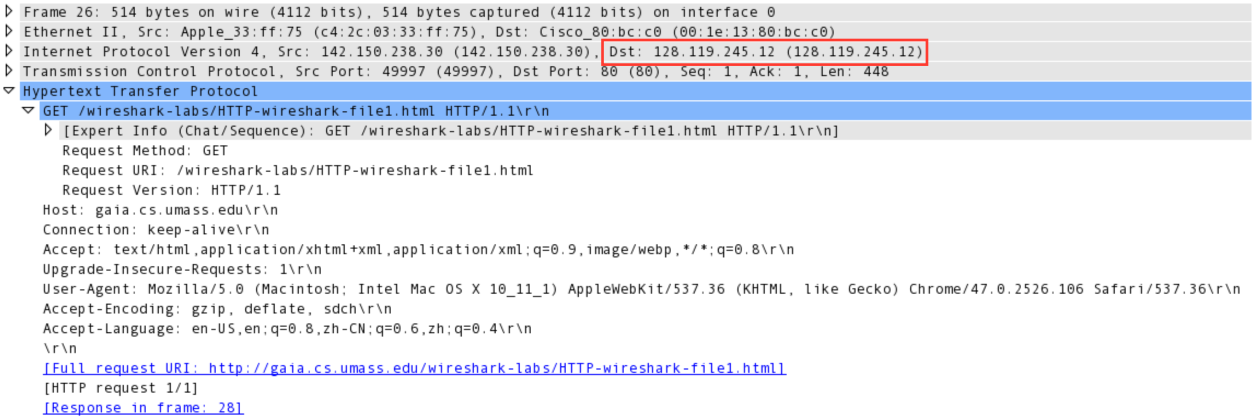
Solution:
en-US and zh-CN
(languages information is listed in the item 'Accept-Language' in the HTTP GET message)



```
▷ Frame 26: 514 bytes on wire (4112 bits), 514 bytes captured (4112 bits) on interface 0
▷ Ethernet II, Src: Apple_33:ff:75 (c4:2c:03:33:ff:75), Dst: Cisco_80:bc:c0 (00:1e:13:80:bc:c0)
▷ Internet Protocol Version 4, Src: 142.150.238.30 (142.150.238.30), Dst: 128.119.245.12 (128.119.245.12)
▷ Transmission Control Protocol, Src Port: 49997 (49997), Dst Port: 80 (80), Seq: 1, Ack: 1, Len: 448
▽ Hypertext Transfer Protocol
  ▽ GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n
    ▷ [Expert Info (Chat/Sequence): GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n]
      Request Method: GET
      Request URI: /wireshark-labs/HTTP-wireshark-file1.html
      Request Version: HTTP/1.1
    Host: gaia.cs.umass.edu\r\n
    Connection: keep-alive\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8\r\n
    Upgrade-Insecure-Requests: 1\r\n
    User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/47.0.2526.106 Safari/537.36\r\n
    Accept-Encoding: gzip, deflate, sdch\r\n
    Accept-Language: en-US,en;q=0.8,zh-CN;q=0.6,zh;q=0.4\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: 28]
```

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

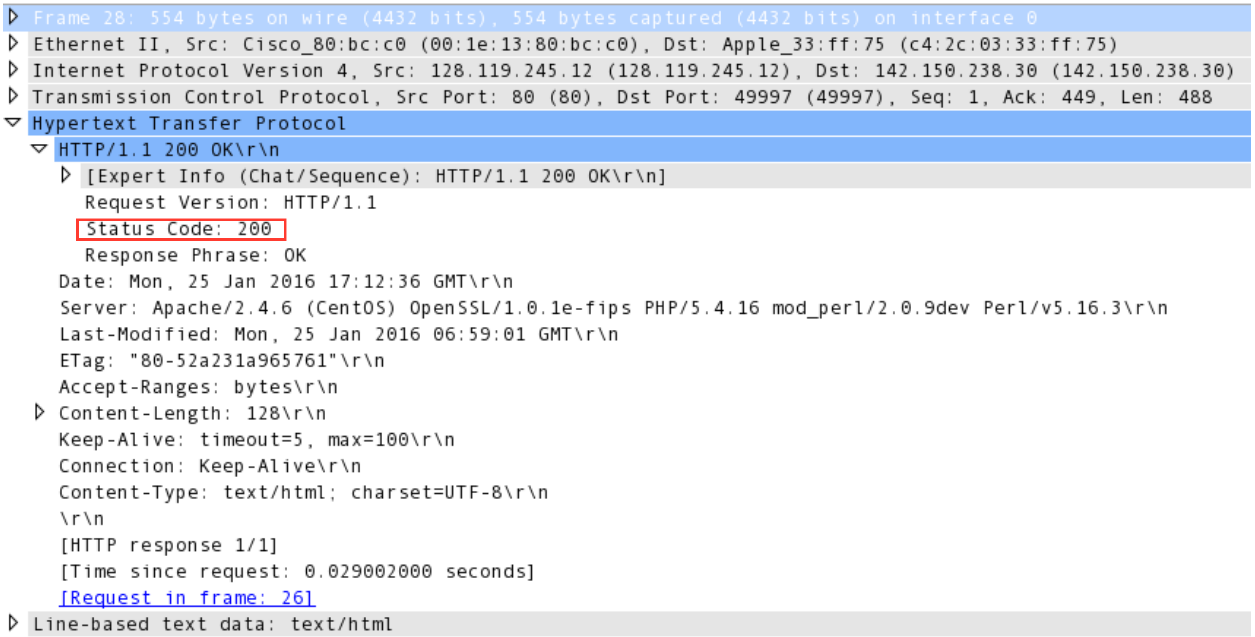
Solution:
my computer: xxx.xxx.xxx.xxx
gaia.cs.umass.edu: 128.119.245.12



```
▷ Frame 26: 514 bytes on wire (4112 bits), 514 bytes captured (4112 bits) on interface 0
▷ Ethernet II, Src: Apple_33:ff:75 (c4:2c:03:33:ff:75), Dst: Cisco_80:bc:c0 (00:1e:13:80:bc:c0)
▷ Internet Protocol Version 4, Src: 142.150.238.30 (142.150.238.30), Dst: 128.119.245.12 (128.119.245.12)
▷ Transmission Control Protocol, Src Port: 49997 (49997), Dst Port: 80 (80), Seq: 1, Ack: 1, Len: 448
▽ Hypertext Transfer Protocol
  ▽ GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n
    ▷ [Expert Info (Chat/Sequence): GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n]
      Request Method: GET
      Request URI: /wireshark-labs/HTTP-wireshark-file1.html
      Request Version: HTTP/1.1
    Host: gaia.cs.umass.edu\r\n
    Connection: keep-alive\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8\r\n
    Upgrade-Insecure-Requests: 1\r\n
    User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/47.0.2526.106 Safari/537.36\r\n
    Accept-Encoding: gzip, deflate, sdch\r\n
    Accept-Language: en-US,en;q=0.8,zh-CN;q=0.6,zh;q=0.4\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: 28]
```

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

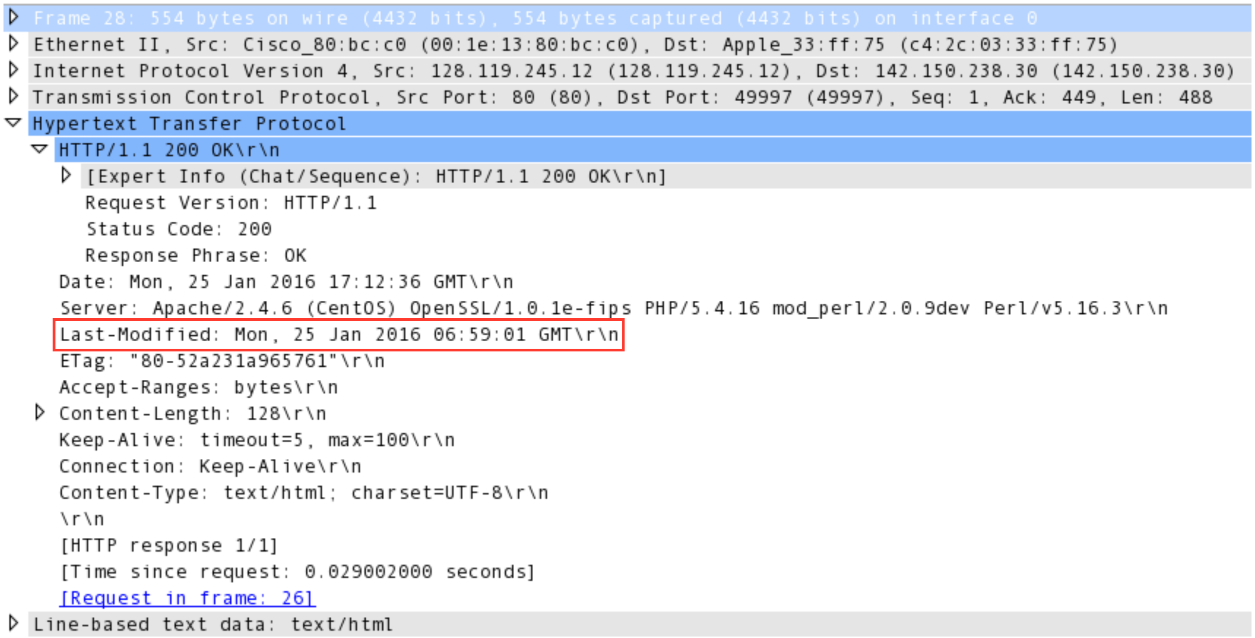
Solution:
status code:200
(status code information is listed in the HTTP OK message)



```
▷ Frame 28: 554 bytes on wire (4432 bits), 554 bytes captured (4432 bits) on interface 0
▷ Ethernet II, Src: Cisco_80:bc:c0 (00:1e:13:80:bc:c0), Dst: Apple_33:ff:75 (c4:2c:03:33:ff:75)
▷ Internet Protocol Version 4, Src: 128.119.245.12 (128.119.245.12), Dst: 142.150.238.30 (142.150.238.30)
▷ Transmission Control Protocol, Src Port: 80 (80), Dst Port: 49997 (49997), Seq: 1, Ack: 449, Len: 488
▽ Hypertext Transfer Protocol
  ▽ 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
      Response Phrase: OK
    Date: Mon, 25 Jan 2016 17:12:36 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.1e-fips PHP/5.4.16 mod_perl/2.0.9dev Perl/v5.16.3\r\n
    Last-Modified: Mon, 25 Jan 2016 06:59:01 GMT\r\n
    ETag: "80-52a231a965761"\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: 0.029002000 seconds]
    [Request in frame: 26]
▷ Line-based text data: text/html
```

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

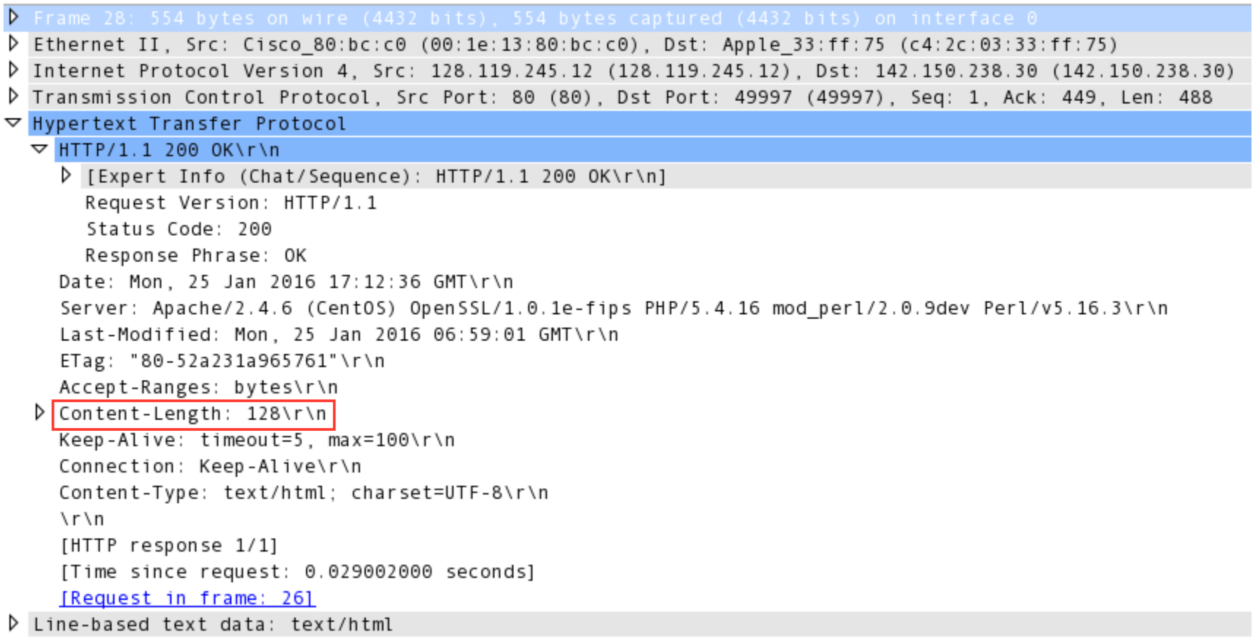
Solution:
Mon, 25 Jan 2016
(last modified information is listed in the item 'Last-Modified' in the HTTP OK message)



```
▷ Frame 28: 554 bytes on wire (4432 bits), 554 bytes captured (4432 bits) on interface 0
▷ Ethernet II, Src: Cisco_80:bc:c0 (00:1e:13:80:bc:c0), Dst: Apple_33:ff:75 (c4:2c:03:33:ff:75)
▷ Internet Protocol Version 4, Src: 128.119.245.12 (128.119.245.12), Dst: 142.150.238.30 (142.150.238.30)
▷ Transmission Control Protocol, Src Port: 80 (80), Dst Port: 49997 (49997), Seq: 1, Ack: 449, Len: 488
▽ Hypertext Transfer Protocol
  ▽ 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
      Response Phrase: OK
    Date: Mon, 25 Jan 2016 17:12:36 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.1e-fips PHP/5.4.16 mod_perl/2.0.9dev Perl/v5.16.3\r\n
    Last-Modified: Mon, 25 Jan 2016 06:59:01 GMT\r\n
    ETag: "80-52a231a965761"\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: 0.029002000 seconds]
    [Request in frame: 26]
▷ Line-based text data: text/html
```

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

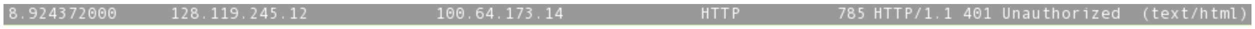
Solution:
Content length: 128
(Content length information is listed in the item ‘Content-Length’ in the HTTP OK message)



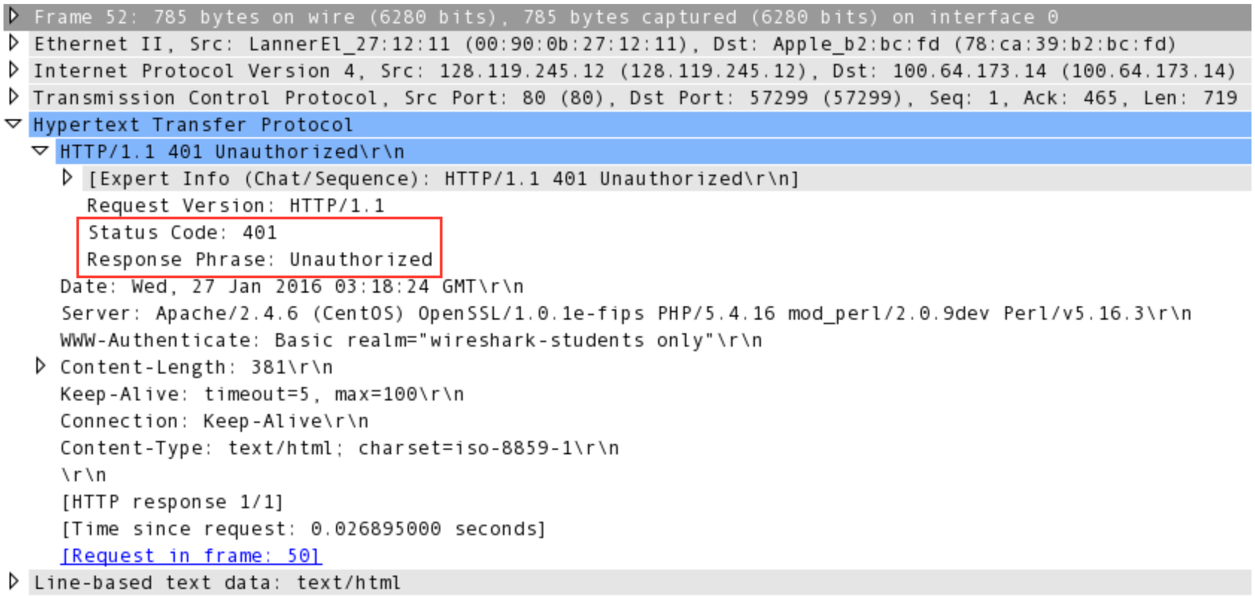
```
▷ Frame 28: 554 bytes on wire (4432 bits), 554 bytes captured (4432 bits) on interface 0
▷ Ethernet II, Src: Cisco_80:bc:c0 (00:1e:13:80:bc:c0), Dst: Apple_33:ff:75 (c4:2c:03:33:ff:75)
▷ Internet Protocol Version 4, Src: 128.119.245.12 (128.119.245.12), Dst: 142.150.238.30 (142.150.238.30)
▷ Transmission Control Protocol, Src Port: 80 (80), Dst Port: 49997 (49997), Seq: 1, Ack: 449, Len: 488
▽ Hypertext Transfer Protocol
  ▽ 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
      Response Phrase: OK
    Date: Mon, 25 Jan 2016 17:12:36 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.1e-fips PHP/5.4.16 mod_perl/2.0.9dev Perl/v5.16.3\r\n
    Last-Modified: Mon, 25 Jan 2016 06:59:01 GMT\r\n
    ETag: "80-52a231a965761"\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: 0.029002000 seconds]
    [Request in frame: 26]
▷ Line-based text data: text/html
```

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

Solution:
We got a response that said 'HTTP/1.1 401 Unauthorized'.
Status code: 401
Response phrase: Unauthorized



```
8.924372000    128.119.245.12         100.64.173.14          HTTP        785 HTTP/1.1 401 Unauthorized  (text/html)
```

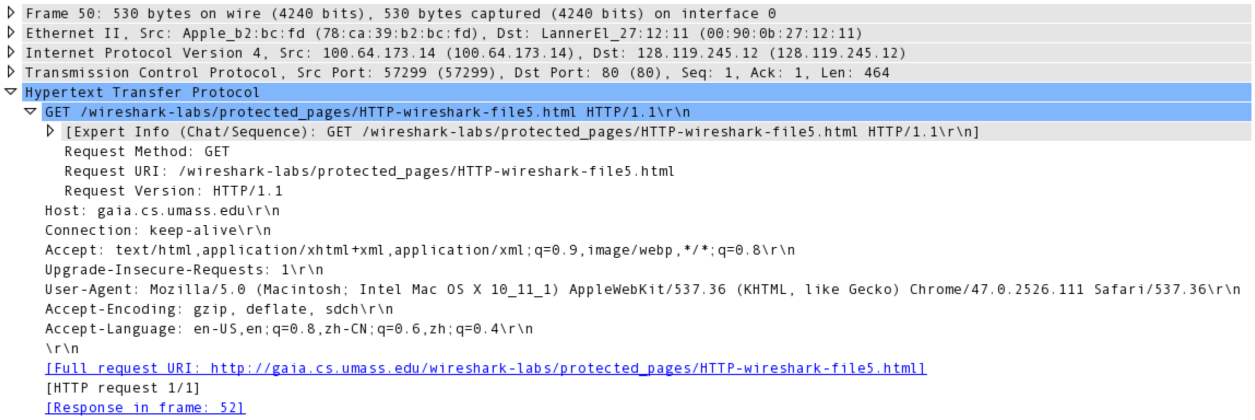


```
▷ Frame 52: 785 bytes on wire (6280 bits), 785 bytes captured (6280 bits) on interface 0
▷ Ethernet II, Src: LannerEl_27:12:11 (00:90:0b:27:12:11), Dst: Apple_b2:bc:fd (78:ca:39:b2:bc:fd)
▷ Internet Protocol Version 4, Src: 128.119.245.12 (128.119.245.12), Dst: 100.64.173.14 (100.64.173.14)
▷ Transmission Control Protocol, Src Port: 80 (80), Dst Port: 57299 (57299), Seq: 1, Ack: 465, Len: 719
▽ Hypertext Transfer Protocol
  ▽ HTTP/1.1 401 Unauthorized\r\n
    ▷ [Expert Info (Chat/Sequence): HTTP/1.1 401 Unauthorized\r\n]
      Request Version: HTTP/1.1
      Status Code: 401
      Response Phrase: Unauthorized
    Date: Wed, 27 Jan 2016 03:18:24 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.1e-fips PHP/5.4.16 mod_perl/2.0.9dev Perl/v5.16.3\r\n
    WWW-Authenticate: Basic realm="wireshark-students only"\r\n
  ▷ Content-Length: 381\r\n
    Keep-Alive: timeout=5, max=100\r\n
    Connection: Keep-Alive\r\n
    Content-Type: text/html; charset=iso-8859-1\r\n
    \r\n
    [HTTP response 1/1]
    [Time since request: 0.026895000 seconds]
    [Request in frame: 50]
▷ Line-based text data: text/html
```

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

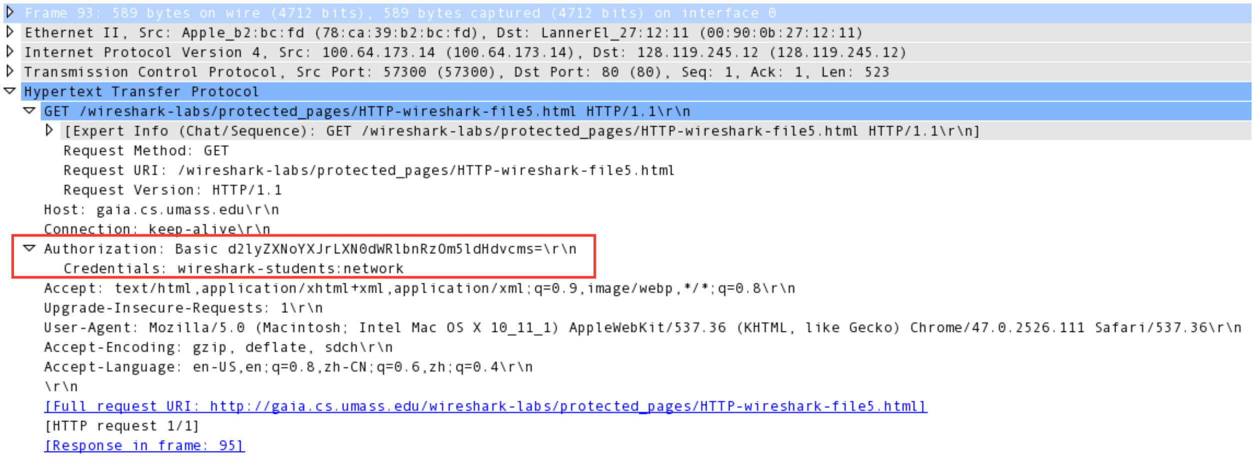
Solution:

The screenshot of first HTTP GET message:



```
▷ Frame 50: 530 bytes on wire (4240 bits), 530 bytes captured (4240 bits) on interface 0
▷ Ethernet II, Src: Apple_b2:bc:fd (78:ca:39:b2:bc:fd), Dst: LannerEl_27:12:11 (00:90:0b:27:12:11)
▷ Internet Protocol Version 4, Src: 100.64.173.14 (100.64.173.14), Dst: 128.119.245.12 (128.119.245.12)
▷ Transmission Control Protocol, Src Port: 57299 (57299), Dst Port: 80 (80), Seq: 1, Ack: 1, Len: 464
▽ 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
    Connection: keep-alive\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8\r\n
    Upgrade-Insecure-Requests: 1\r\n
    User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/47.0.2526.111 Safari/537.36\r\n
    Accept-Encoding: gzip, deflate, sdch\r\n
    Accept-Language: en-US,en;q=0.8,zh-CN;q=0.6,zh;q=0.4\r\n
    \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: 52]
```

The screenshot of second HTTP GET message:



```
▷ Frame 93: 589 bytes on wire (4712 bits), 589 bytes captured (4712 bits) on interface 0
▷ Ethernet II, Src: Apple_b2:bc:fd (78:ca:39:b2:bc:fd), Dst: LannerEl_27:12:11 (00:90:0b:27:12:11)
▷ Internet Protocol Version 4, Src: 100.64.173.14 (100.64.173.14), Dst: 128.119.245.12 (128.119.245.12)
▷ Transmission Control Protocol, Src Port: 57300 (57300), Dst Port: 80 (80), Seq: 1, Ack: 1, Len: 523
▽ 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
    Connection: keep-alive\r\n
  ▽ Authorization: Basic d2lyZXNoYXJrLXN0dWRlbnRzOm5ldHdvcms=\r\n
      Credentials: wireshark-students:network
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8\r\n
    Upgrade-Insecure-Requests: 1\r\n
    User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/47.0.2526.111 Safari/537.36\r\n
    Accept-Encoding: gzip, deflate, sdch\r\n
    Accept-Language: en-US,en;q=0.8,zh-CN;q=0.6,zh;q=0.4\r\n
    \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: 95]
```

Comparing these two HTTP GET messages, it is easy to find that the second HTTP GET message contains the 'Authorization' field.

The username (wireshark-students) and password (network) that you entered are encoded in the string of characters (d2lyZXNoYXJrLXN0dWRlbnRzOm5ldHdvcms=) following the "Authorization: Basic" header in the client's HTTP GET message. While it may appear that your username and password are encrypted, they are simply encoded in a format known as Base64 format. The username and password are *not* encrypted! To see this, go to

http://www.motobit.com/util/base64-decoder-encoder.asp and enter the base64-encoded string d2lyZXNoYXJrLXN0dWRlbnRz and decode. *Voila!* You have translated from Base64 encoding to ASCII encoding, and thus should see your username! To view the password, enter the remainder of the string Om5ldHdvcms= and press decode. Since anyone can download a tool like Wireshark and sniff packets (not just their own) passing by their network adaptor, and anyone can translate from Base64 to ASCII (you just did it!), it should be clear to you that simple passwords on WWW sites are not secure unless additional measures are taken.