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

The browser is running HTTP 1.1 as it is requesting it.

```
/home/viles222/Documents/wireshark/http-ethereal-trace-1 17 total packets, 4 shown

No.     Time           Source                Destination           Protocol Length Info
     10 4.694850       192.168.1.102         128.119.245.12        HTTP     555    GET /ethereal-labs/lab2-1.html
HTTP/1.1
Frame 10: 555 bytes on wire (4440 bits), 555 bytes captured (4440 bits)
Ethernet II, Src: Dell_4f:36:23 (00:08:74:4f:36:23), Dst: LinksysG_da:af:73 (00:06:25:da:af:73)
Internet Protocol Version 4, Src: 192.168.1.102, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 4127, Dst Port: 80, Seq: 1, Ack: 1, Len: 501
Hypertext Transfer Protocol
    GET /ethereal-labs/lab2-1.html HTTP/1.1\r\n
        [Expert Info (Chat/Sequence): GET /ethereal-labs/lab2-1.html HTTP/1.1\r\n]
            [GET /ethereal-labs/lab2-1.html HTTP/1.1\r\n]
            [Severity level: Chat]
            [Group: Sequence]
        Request Method: GET
        Request URI: /ethereal-labs/lab2-1.html
        Request Version: HTTP/1.1
    Host: gaia.cs.umass.edu\r\n
    User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.0.2) Gecko/20021120 Netscape/7.01\r\n
    Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,video/x-mng,image/
png,image/jpeg,image/gif;q=0.2,text/css,*/*;q=0.1\r\n
    Accept-Language: en-us, en;q=0.50\r\n
    Accept-Encoding: gzip, deflate, compress;q=0.9\r\n
    Accept-Charset: ISO-8859-1, utf-8;q=0.66, *;q=0.66\r\n
    Keep-Alive: 300\r\n
    Connection: keep-alive\r\n
    \r\n
    [Full request URI: http://gaia.cs.umass.edu/ethereal-labs/lab2-1.html]
    [HTTP request 1/2]
    [Response in frame: 12]
    [Next request in frame: 13]
```

The server is running HTTP 1.1 aswell.

```
/home/viles222/Documents/wireshark/http-ethereal-trace-1 17 total packets, 4 shown

No.     Time           Source                Destination           Protocol Length Info
     12 4.718993       128.119.245.12        192.168.1.102         HTTP     439    HTTP/1.1 200 OK  (text/html)
Frame 12: 439 bytes on wire (3512 bits), 439 bytes captured (3512 bits)
Ethernet II, Src: LinksysG_da:af:73 (00:06:25:da:af:73), Dst: Dell_4f:36:23 (00:08:74:4f:36:23)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.102
Transmission Control Protocol, Src Port: 80, Dst Port: 4127, Seq: 1, Ack: 502, Len: 385
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]
        Response Version: HTTP/1.1
        Status Code: 200
        [Status Code Description: OK]
        Response Phrase: OK
    Date: Tue, 23 Sep 2003 05:29:50 GMT\r\n
    Server: Apache/2.0.40 (Red Hat Linux)\r\n
    Last-Modified: Tue, 23 Sep 2003 05:29:00 GMT\r\n
    ETag: "1bfed-49-79d5bf00"\r\n
    Accept-Ranges: bytes\r\n
    Content-Length: 73\r\n
    Keep-Alive: timeout=10, max=100\r\n
    Connection: Keep-Alive\r\n
    Content-Type: text/html; charset=ISO-8859-1\r\n
    \r\n
    [HTTP response 1/2]
    [Time since request: 0.024143000 seconds]
    [Request in frame: 10]
    [Next request in frame: 13]
    [Next response in frame: 14]
    [Request URI: http://gaia.cs.umass.edu/favicon.ico]
    File Data: 73 bytes
Line-based text data: text/html (3 lines)
```

2. What languages (if any) does your browser indicate that it can accept to the server? In the captured session, what other information (if any) does the browser provide the server with regarding the user/browser?

The browser accepts american - english language as seen at the blue line.
It also provides information on the users browser, browser version and operating system.

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

The computer has the ip adress of 192.168.1.102 as seen in green which is its private ip adress provided by its router, unless set manually, probably not. The server has the ip adress of 128.119.245.12 as seen in black.

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

Status code 200, meaning OK, as seen in purple.

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

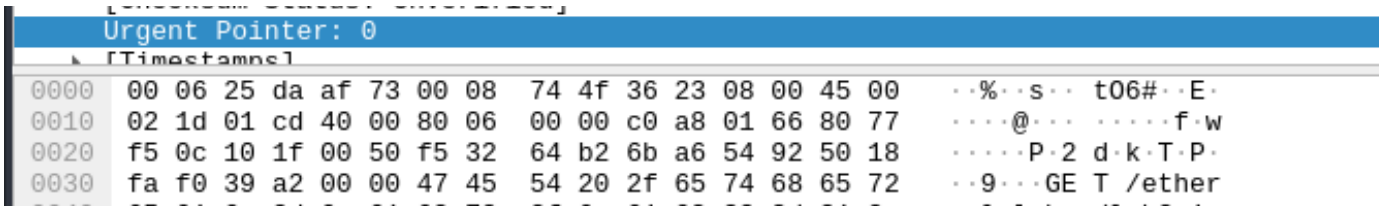
From the downloaded trace the last modification is from 05:29:00 23 september 2003.

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

73 bytes of content are sent from the server to the user.

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

There is tcp data included in the HTTP header ass well.



Task A: For questions 1-7, first write a brief but precise answer for each of the above questions, then write a (combined) paragraph explaining and discussing your observations from the above practice questions. Note that your answer may benefit from explaining and/or referring to some of your observations explicitly.

Both the browser and server seems to be running HTTP 1.1 with the browser acceptring only english language. With the user running windows with netscape as browser. The user has the local ip address of 192.168.1.102 and the server having the public ip of 128.119.245.12.
We also observed information about the http return code 200 and the size of the returned file.

```
No.     Time           Source                Destination           Protocol Length Info
      8 2.331268       192.168.1.102         128.119.245.12        HTTP     555    GET /ethereal-labs/lab2-2.html
HTTP/1.1
Frame 8: 555 bytes on wire (4440 bits), 555 bytes captured (4440 bits)
Ethernet II, Src: Dell_4f:36:23 (00:08:74:4f:36:23), Dst: LinksysG_da:af:73 (00:06:25:da:af:73)
Internet Protocol Version 4, Src: 192.168.1.102, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 4247, Dst Port: 80, Seq: 1, Ack: 1, Len: 501
Hypertext Transfer Protocol
    GET /ethereal-labs/lab2-2.html HTTP/1.1\r\n
        [Expert Info (Chat/Sequence): GET /ethereal-labs/lab2-2.html HTTP/1.1\r\n]
        Request Method: GET
        Request URI: /ethereal-labs/lab2-2.html
        Request Version: HTTP/1.1
    Host: gaia.cs.umass.edu\r\n
    User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.0.2) Gecko/20021120 Netscape/7.01\r\n
    Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,video/x-mng,image/
png,image/jpeg,image/gif;q=0.2,text/css,*/*;q=0.1\r\n
    Accept-Language: en-us, en;q=0.50\r\n
    Accept-Encoding: gzip, deflate, compress;q=0.9\r\n
    Accept-Charset: ISO-8859-1, utf-8;q=0.66, *;q=0.66\r\n
    Keep-Alive: 300\r\n
    Connection: keep-alive\r\n
    \r\n
    [Full request URI: http://gaia.cs.umass.edu/ethereal-labs/lab2-2.html]
    [HTTP request 1/2]
    [Response in frame: 10]
    [Next request in frame: 14]
```

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?

There is no if-modified line in the first request to the server.

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

```
No.     Time           Source                Destination           Protocol Length Info
     10 2.357902       128.119.245.12        192.168.1.102         HTTP     739    HTTP/1.1 200 OK  (text/html)
Frame 10: 739 bytes on wire (5912 bits), 739 bytes captured (5912 bits)
Ethernet II, Src: LinksysG_da:af:73 (00:06:25:da:af:73), Dst: Dell_4f:36:23 (00:08:74:4f:36:23)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.102
Transmission Control Protocol, Src Port: 80, Dst Port: 4247, Seq: 1, Ack: 502, Len: 685
Hypertext Transfer Protocol
    HTTP/1.1 200 OK\r\n
    Date: Tue, 23 Sep 2003 05:35:50 GMT\r\n
    Server: Apache/2.0.40 (Red Hat Linux)\r\n
    Last-Modified: Tue, 23 Sep 2003 05:35:00 GMT\r\n
    ETag: "1bfef-173-8f4ae900"\r\n
    Accept-Ranges: bytes\r\n
    Content-Length: 371\r\n
    Keep-Alive: timeout=10, max=100\r\n
    Connection: Keep-Alive\r\n
    Content-Type: text/html; charset=ISO-8859-1\r\n
    \r\n
    [HTTP response 1/2]
    [Time since request: 0.026634000 seconds]
    [Request in frame: 8]
    [Next request in frame: 14]
    [Next response in frame: 15]
    [Request URI: http://gaia.cs.umass.edu/ethereal-labs/lab2-2.html]
    File Data: 371 bytes
Line-based text data: text/html (10 lines)
```

Yes, this can be seen in the http header of ”Line-based text data” of 10 lines as seen in blue.

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?

```
No.     Time           Source                Destination           Protocol Length Info
     14 5.517390       192.168.1.102         128.119.245.12        HTTP     668    GET /ethereal-labs/lab2-2.html
HTTP/1.1
Frame 14: 668 bytes on wire (5344 bits), 668 bytes captured (5344 bits)
Ethernet II, Src: Dell_4f:36:23 (00:08:74:4f:36:23), Dst: LinksysG_da:af:73 (00:06:25:da:af:73)
Internet Protocol Version 4, Src: 192.168.1.102, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 4247, Dst Port: 80, Seq: 502, Ack: 686, Len: 614
Hypertext Transfer Protocol
    GET /ethereal-labs/lab2-2.html HTTP/1.1\r\n
    Host: gaia.cs.umass.edu\r\n
    User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.0.2) Gecko/20021120 Netscape/7.01\r\n
    Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,video/x-mng,image/
png,image/jpeg,image/gif;q=0.2,text/css,*/*;q=0.1\r\n
    Accept-Language: en-us, en;q=0.50\r\n
    Accept-Encoding: gzip, deflate, compress;q=0.9\r\n
    Accept-Charset: ISO-8859-1, utf-8;q=0.66, *;q=0.66\r\n
    Keep-Alive: 300\r\n
    Connection: keep-alive\r\n
    If-Modified-Since: Tue, 23 Sep 2003 05:35:00 GMT\r\n
    If-None-Match: "1bfef-173-8f4ae900"\r\n
    Cache-Control: max-age=0\r\n
    \r\n
    [Full request URI: http://gaia.cs.umass.edu/ethereal-labs/lab2-2.html]
    [HTTP request 2/2]
    [Prev request in frame: 8]
    [Response in frame: 15]
```

Yes, the information that follows is the last time the website was modified as seen in black.

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.

```
No.     Time           Source                Destination           Protocol Length Info
     15 5.540216       128.119.245.12        192.168.1.102         HTTP     243    HTTP/1.1 304 Not Modified
Frame 15: 243 bytes on wire (1944 bits), 243 bytes captured (1944 bits)
Ethernet II, Src: LinksysG_da:af:73 (00:06:25:da:af:73), Dst: Dell_4f:36:23 (00:08:74:4f:36:23)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.102
Transmission Control Protocol, Src Port: 80, Dst Port: 4247, Seq: 686, Ack: 1116, Len: 189
Hypertext Transfer Protocol
    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]
        Response Version: HTTP/1.1
        Status Code: 304
        [Status Code Description: Not Modified]
        Response Phrase: Not Modified
    Date: Tue, 23 Sep 2003 05:35:53 GMT\r\n
    Server: Apache/2.0.40 (Red Hat Linux)\r\n
    Connection: Keep-Alive\r\n
    Keep-Alive: timeout=10, max=99\r\n
    ETag: "1bfef-173-8f4ae900"\r\n
    \r\n
    [HTTP response 2/2]
    [Time since request: 0.022826000 seconds]
    [Prev request in frame: 8]
    [Prev response in frame: 10]
    [Request in frame: 14]
    [Request URI: http://gaia.cs.umass.edu/ethereal-labs/lab2-2.html]
```

It gave return code of 304 meaning that the file requested has not been modified since last time. It did not return the contents of the file since it has been locally cached on the computer and it hasn't been modified since the last time requesting the file.

Task B: For questions 8-11, first write a brief but precise answer for each of the above questions, then write a (combined) paragraph explaining and discussing your observations from the above practice questions. Note that your answer may benefit from explaining and/or referring to some of your observations explicitly.

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?

```
No.     Time           Source                Destination           Protocol Length Info
      8 4.623732       192.168.1.102         128.119.245.12        HTTP     555    GET /ethereal-labs/lab2-3.html
HTTP/1.1
Frame 8: 555 bytes on wire (4440 bits), 555 bytes captured (4440 bits)
Ethernet II, Src: Dell_4f:36:23 (00:08:74:4f:36:23), Dst: LinksysG_da:af:73 (00:06:25:da:af:73)
Internet Protocol Version 4, Src: 192.168.1.102, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 4272, Dst Port: 80, Seq: 1, Ack: 1, Len: 501
Hypertext Transfer Protocol
    GET /ethereal-labs/lab2-3.html HTTP/1.1\r\n
    Host: gaia.cs.umass.edu\r\n
    User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.0.2) Gecko/20021120 Netscape/7.01\r\n
    Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,video/x-mng,image/
png,image/jpeg,image/gif;q=0.2,text/css,*/*;q=0.1\r\n
    Accept-Language: en-us, en;q=0.50\r\n
    Accept-Encoding: gzip, deflate, compress;q=0.9\r\n
    Accept-Charset: ISO-8859-1, utf-8;q=0.66, *;q=0.66\r\n
    Keep-Alive: 300\r\n
    Connection: keep-alive\r\n
    \r\n
    [Full request URI: http://gaia.cs.umass.edu/ethereal-labs/lab2-3.html]
    [HTTP request 1/1]
    [Response in frame: 14]
```

The browser sent one HTTP get request seen in blue. Packet number 8 contains the get message as seen in blue.

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

```
No.     Time           Source                Destination           Protocol Length Info
     14 4.680920       128.119.245.12        192.168.1.102         HTTP     490    HTTP/1.1 200 OK  (text/html)
Frame 14: 490 bytes on wire (3920 bits), 490 bytes captured (3920 bits)
Ethernet II, Src: LinksysG_da:af:73 (00:06:25:da:af:73), Dst: Dell_4f:36:23 (00:08:74:4f:36:23)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.102
Transmission Control Protocol, Src Port: 80, Dst Port: 4272, Seq: 4381, Ack: 502, Len: 436
[4 Reassembled TCP Segments (4816 bytes): #10(1460), #11(1460), #13(1460), #14(436)]
Hypertext Transfer Protocol
    HTTP/1.1 200 OK\r\n
        [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
        Response Version: HTTP/1.1
        Status Code: 200
        [Status Code Description: OK]
        Response Phrase: OK
    Date: Tue, 23 Sep 2003 05:37:02 GMT\r\n
    Server: Apache/2.0.40 (Red Hat Linux)\r\n
    Last-Modified: Tue, 23 Sep 2003 05:37:01 GMT\r\n
    ETag: "1bff2-1194-96813940"\r\n
    Accept-Ranges: bytes\r\n
    Content-Length: 4500\r\n
    Keep-Alive: timeout=10, 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: 0.057188000 seconds]
    [Request in frame: 8]
    [Request URI: http://gaia.cs.umass.edu/ethereal-labs/lab2-3.html]
    File Data: 4500 bytes
Line-based text data: text/html (98 lines)
```

Packet number 14 seen in blue contains the status code of 200 meaning OK seen in red.

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

There were 4 TCP segments needed to carry the response as seen in green in the previous question.

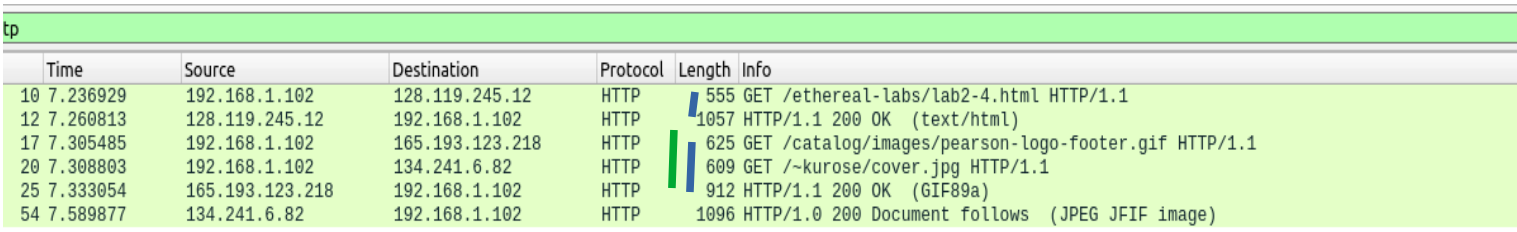
15. Is there any HTTP header information in any of the transmitted data packets associated with TCP segmentation? For this question you may want to think about at what layer each protocol operates, and how the protocols at the different layers interoperate.

Tcp operates on the transport layer while http operates on the application layer. As such the tcp message encapsulates the http message. As such, during the tcp-segmentation there is encapsulated http information to be found.

Task C: For questions 12-15, first write a brief but precise answer for each of the above questions, then write a (combined) paragraph explaining and discussing your observations from the above practice questions. Note that your answer may benefit from explaining and/or referring to some of your observations explicitly.

For the 12 to 15 question we observed that the browser send one http get and one http response. For the request the server answers here with a status code of 200 “OK”. We also observed that when the requested file is too large for one http messeage it will be split into multiple tcp-segments. At last we observed how tcp interacts with http during encapsulation sent during the tcp segments.

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



The browser sent three HTTP GET to gaia.cs.umass.edu , www.aw-bc.com and manic.cs.umass.edu.

```
Accept-Language: en-us, en;q=0.50\r\n
Accept-Encoding: gzip, deflate, compress;q=0.9\r\n
Accept-Charset: ISO-8859-1, utf-8;q=0.66, *;q=0.66\r\n
Keep-Alive: 300\r\n
Connection: keep-alive\r\n
Referer: http://gaia.cs.umass.edu/ethereal-labs/lab2-4.html\r\n
\r\n
[Full request URI: http://www.aw-bc.com/catalog/images/pearson-logo-footer.gif]
[HTTP request 1/1]
[Response in frame: 25]
```

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.

The two images where downloaded in parallel as there where two http get for the images in order, as seen in green, and if it would have been a serial download the browser would download one picture and wait for it to be complete until downloading the other one.

Task D: For questions 16-17, first write a brief but precise answer for each of the above questions, then write a paragraph explaining and discussing your observations from the above practice questions. Note that your answer may benefit from explaining and/or referring to some of your observations explicitly.

We observed in question 16 that when the browser sends a http get to a website with images, the browser then will send subsequent http gets for each of the images. We observed then that the browser does downloads the images in parallel and doesn't wait for the http get response for the first image image.

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

```
No.     Time           Source                Destination           Protocol Length Info
      9 2.538231       128.119.245.12        192.168.1.102         HTTP     278    HTTP/1.1 401 Authorization
Required  (text/html)
Frame 9: 278 bytes on wire (2224 bits), 278 bytes captured (2224 bits)
Ethernet II, Src: LinksysG_da:af:73 (00:06:25:da:af:73), Dst: Dell_4f:36:23 (00:08:74:4f:36:23)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.102
Transmission Control Protocol, Src Port: 80, Dst Port: 4335, Seq: 1461, Ack: 518, Len: 224
[2 Reassembled TCP Segments (1684 bytes): #8(1460), #9(224)]
Hypertext Transfer Protocol
    HTTP/1.1 401 Authorization Required\r\n
        [Expert Info (Chat/Sequence): HTTP/1.1 401 Authorization Required\r\n]
            [HTTP/1.1 401 Authorization Required\r\n]
            [Severity level: Chat]
            [Group: Sequence]
        Response Version: HTTP/1.1
        Status Code: 401
        [Status Code Description: Unauthorized]
        Response Phrase: Authorization Required
    Date: Tue, 23 Sep 2003 05:39:58 GMT\r\n
    Server: Apache/2.0.40 (Red Hat Linux)\r\n
    WWW-Authenticate: Basic realm="eth-students only"\r\n
    Vary: accept-language\r\n
    Accept-Ranges: bytes\r\n
    Content-Length: 1349\r\n
    Keep-Alive: timeout=10, 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: 0.030002000 seconds]
    [Request in frame: 6]
    [Request URI: http://gaia.cs.umass.edu/ethereal-labs/protected_pages/lab2-5.html]
    File Data: 1349 bytes
Line-based text data: text/html (56 lines)
```

The server returned the status code 401 "authorization required" with the response of Authorization required as seen in blue.

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

/home/vilgot/Hämtningar/wireshark-traces(1)/http-ethereal-trace-5 73 total packets, 4 shown

```
No.     Time           Source                Destination           Protocol Length Info
     65 18.516793      192.168.1.102         128.119.245.12        HTTP     622    GET /ethereal-labs/
protected_pages/lab2-5.html HTTP/1.1
Frame 65: 622 bytes on wire (4976 bits), 622 bytes captured (4976 bits)
Ethernet II, Src: Dell_4f:36:23 (00:08:74:4f:36:23), Dst: LinksysG_da:af:73 (00:06:25:da:af:73)
Internet Protocol Version 4, Src: 192.168.1.102, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 4342, Dst Port: 80, Seq: 1, Ack: 1, Len: 568
Hypertext Transfer Protocol
    GET /ethereal-labs/protected_pages/lab2-5.html HTTP/1.1\r\n
        [Expert Info (Chat/Sequence): GET /ethereal-labs/protected_pages/lab2-5.html HTTP/1.1\r\n]
        Request Method: GET
        Request URI: /ethereal-labs/protected_pages/lab2-5.html
        Request Version: HTTP/1.1
    Host: gaia.cs.umass.edu\r\n
    User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.0.2) Gecko/20021120 Netscape/7.01\r\n
    Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,video/x-mng,image/
png,image/jpeg,image/gif;q=0.2,text/css,*/*;q=0.1\r\n
    Accept-Language: en-us, en;q=0.50\r\n
    Accept-Encoding: gzip, deflate, compress;q=0.9\r\n
    Accept-Charset: ISO-8859-1, utf-8;q=0.66, *;q=0.66\r\n
    Keep-Alive: 300\r\n
    Connection: keep-alive\r\n
    Authorization: Basic ZXRoLXN0dWRlbnRzOm5ldHdvcmtz\r\n
    \r\n
    [Full request URI: http://gaia.cs.umass.edu/ethereal-labs/protected_pages/lab2-5.html]
    [HTTP request 1/1]
    [Response in frame: 68]
```

There was an authorization field included included of a hashed password value in the second HTTP get message as seen in red.

Task E: For questions 18-19, first write a brief but precise answer for each of the above questions, then write a paragraph explaining and discussing your observations from the above practice questions. Note that your answer may benefit from explaining and/or referring to some of your observations explicitly.

Our observation in question 18 is that when a website needs authorization to be downloaded the HTTP response will be 401. In the second HTTP get we observed an additional field containing a hashed value of the login credentials, to which after the server response was response code 200.

HTTP Persistent connection

20. What does the "Connection: close" and "Connection: keep-alive" header field imply in HTTP protocol? When should one be used over the other?

“HTTP Connection: “ header field hints the web server about the wanted connection behavior server. The “connection: close” hits the server that it doesn’t want persistent tcp connection, that it will close the connection after each http get response. If more http gets are sent a new tcp connection have to be established and closed for each http get.

“Connection: keep-alive” tells the server that the browser want to have an open tcp connection, which means that there can be multiple HTTP get and responses without having to close the tcp connection for each. This also does means that it it up to the client to figure out when the get and responses are completed and then close the connection.

“Connection: close” should be used when the client or server does not expect to send further HTTP get or responses over the same tcp connection. This is mostly used for short-lived interactions or simple HTTP requests.

“Connection: keep-alive” should be used when the server or client expects to send multiple HTTP GETs or responses over the same connection such as loading multiple images or large files from the same connection.