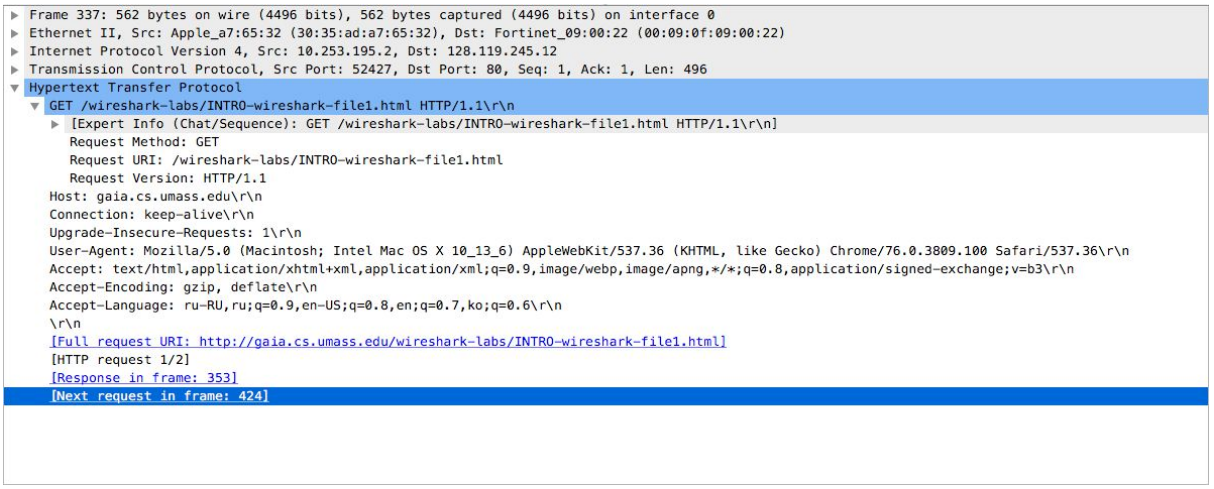
TDTS06 Computer Networks

Assignment 1: “Wireshark lab: Getting started + HTTP”

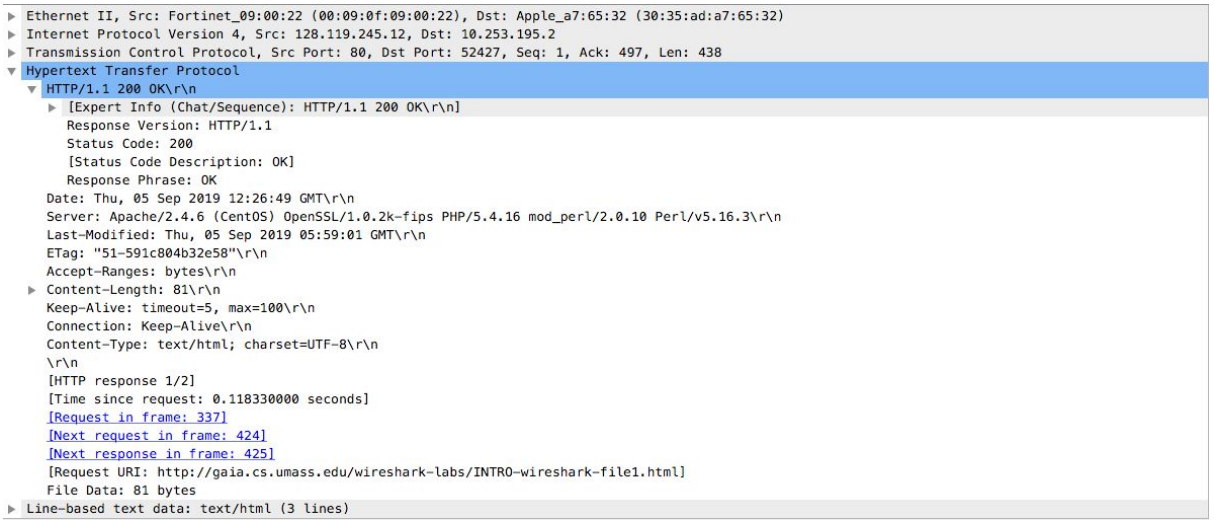
Group B12: Alim Amanzholov (aliam864), Huiwen Li (huili227)

1. Task A: The Basic HTTP GET/response interaction

The basic HTTP GET:



Response:



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

   Both client and server is running HTTP 1.1.

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 indicate its acceptable language in HEADER “Accept-Language: ru-RU,ru;q=0.9,en-US;q=0.8,en;q=0.7,ko;q=0.6.” That means the browser is expecting Russian or English content from the server.

Other information that is provided by browser include, for example, type of user-agent is Mozilla, Accept encoding type is gzip, the format of file like text and image are both acceptable.

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

   IP address of our computer: 10.253.95.2

   IP address of “gaia.cs.umass.edu” server: 128.119.245.12

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

   200 (OK), that means request succeeded, request object later in the message.

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

   The last-modified time was indicated in the header “Last-Modified”, the specific time is “Thu, 05 Sep 2019 05:59:01 GMT”.

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

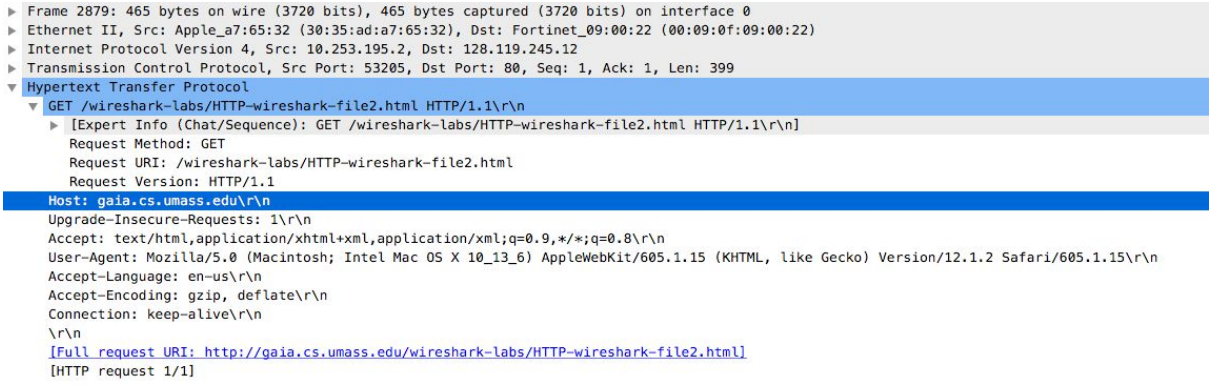
   81 bytes are being returned. That can be clarity at the Header “File Data”

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.**

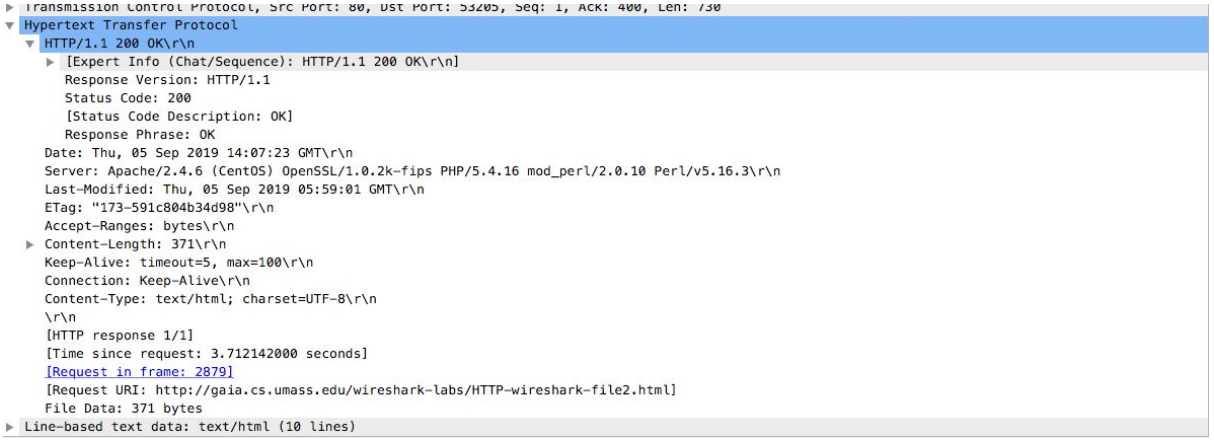
   No, all the headers are displayed in the packet-listing window according to our observation.

Task B: The HTTP CONDITIONAL GET/response interaction

First HTTP GET Request:

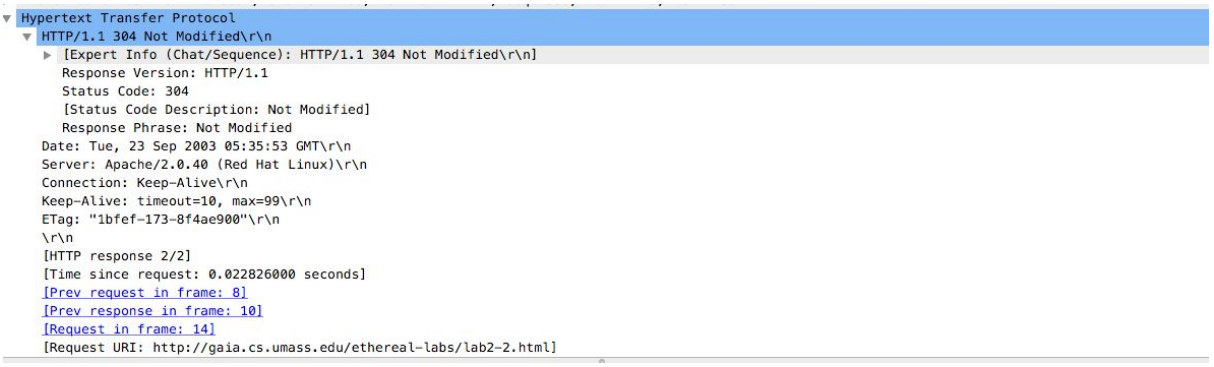


First Response:



Second HTTP GET request:

Second response:



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?**

   No, "IF-MODIFIED-SINCE" line is not observed.

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

   In the first response, the contents are returned, because the status code is 200, which means the request succeeded. And also information like content-length, content-type also give us a hint.

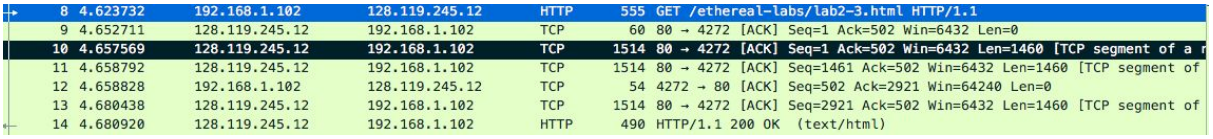
10. **Now inspect the contents of the second HTTP GET request from your browser to the server. Do you see an "IF-MODIFIED-SINCE:" line in the HTTP GET? If so, what information follows the "IF-MODIFIED-SINCE:" header?**

    Yes, and the following information is "If-Modified-Since: Tue, 23 Sep 2003 05:35:00 GMT".

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.**

    The status code of the second response is 304 (Not Modified), which means the content is not modified, therefore no content is updated and the content is served from the cache.

Task C: Retrieving Long Documents

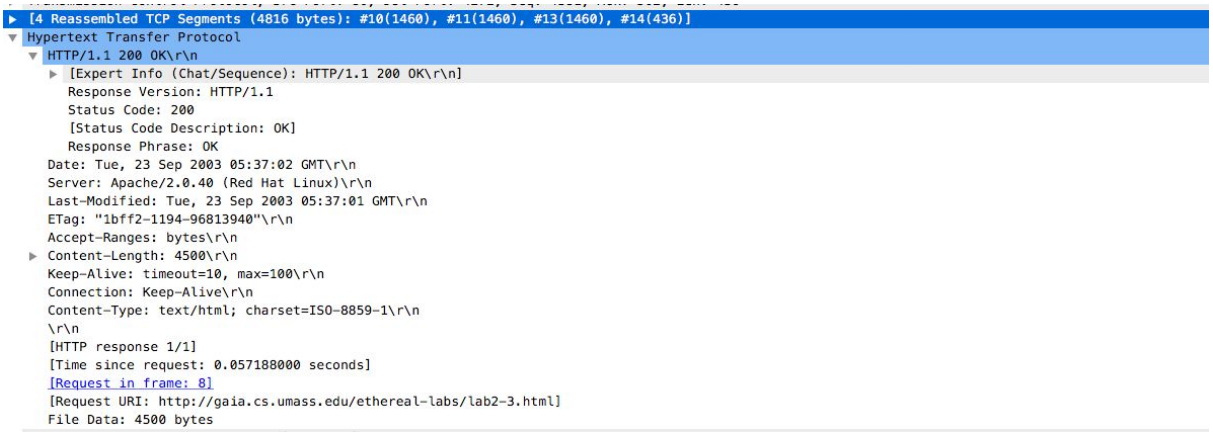


8	4.623732	192.168.1.102	128.119.245.12	HTTP	555 GET /ethereal-labs/lab2-3.html HTTP/1.1
9	4.652711	128.119.245.12	192.168.1.102	TCP	60 80 → 4272 [ACK] Seq=1 Ack=502 Win=6432 Len=0
10	4.657569	128.119.245.12	192.168.1.102	TCP	1514 80 → 4272 [ACK] Seq=1 Ack=502 Win=6432 Len=1460 [TCP segment of a r
11	4.658792	128.119.245.12	192.168.1.102	TCP	1514 80 → 4272 [ACK] Seq=1461 Ack=502 Win=6432 Len=1460 [TCP segment of
12	4.658828	192.168.1.102	128.119.245.12	TCP	54 4272 → 80 [ACK] Seq=502 Ack=2921 Win=64240 Len=0
13	4.680438	128.119.245.12	192.168.1.102	TCP	1514 80 → 4272 [ACK] Seq=2921 Ack=502 Win=6432 Len=1460 [TCP segment of
14	4.680920	128.119.245.12	192.168.1.102	HTTP	490 HTTP/1.1 200 OK (text/html)

HTTP GET request:

```
▼ Hypertext Transfer Protocol
  ▼ GET /ethereal-labs/lab2-3.html HTTP/1.1\r\n
    ▶ [Expert Info (Chat/Sequence): GET /ethereal-labs/lab2-3.html HTTP/1.1\r\n]
      Request Method: GET
      Request URI: /ethereal-labs/lab2-3.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,*
    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]
```

Response:



```
▶ [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
```

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

    Our browser sent only one HTTP GET request, The packet number in the trace that contains the GET message is 8.

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

    The packet number 14 in the trace contains the status code and phrase associated with the response to the HTTP GET request. The status code is 200 and the phrase is “OK”.

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

    4 data-containing TCP segments were needed to carry the single HTTP response and the content, which is the text of the Bill of Rights. The number of TCP segments can be seen from the following:

    [4 Reassembled TCP Segments (4816 bytes): #10(1460), #11(1460), #13(1460), #14(436)]

15. **Is there any HTTP header information in the transmitted data 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.**

    No. HTTP is contained in the TCP segment in the frame body, but HTTP doesn't have to understand the context of TCP.

Task D: HTML Documents with Embedded Objects

No.	Time	Source	Destination	Protocol	Length	Info
10	7.236929	192.168.1.102	128.119.245.12	HTTP	555	GET /ethereal-labs/lab2-4.html HTTP/1.1
12	7.260813	128.119.245.12	192.168.1.102	HTTP	1057	HTTP/1.1 200 OK (text/html)
17	7.305485	192.168.1.102	165.193.123.218	HTTP	625	GET /catalog/images/pearson-logo-footer.gif HTTP/1.1
20	7.308803	192.168.1.102	134.241.6.82	HTTP	609	GET /~kurose/cover.jpg HTTP/1.1
25	7.333054	165.193.123.218	192.168.1.102	HTTP	912	HTTP/1.1 200 OK (GIF89a)
54	7.589877	134.241.6.82	192.168.1.102	HTTP	1096	HTTP/1.0 200 Document follows (JPEG JFIF image)

1st HTTP GET Request:

```
▼ Hypertext Transfer Protocol
  ▼ GET /ethereal-labs/lab2-4.html HTTP/1.1\r\n
    ▶ [Expert Info (Chat/Sequence): GET /ethereal-labs/lab2-4.html HTTP/1.1\r\n]
      Request Method: GET
      Request URI: /ethereal-labs/lab2-4.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.
  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/lab2-4.html]
  [HTTP request 1/1]
  [Response in frame: 12]
```

1st Response:

```
▼ 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 05:38:44 GMT\r\n
  Server: Apache/2.0.40 (Red Hat Linux)\r\n
  Last-Modified: Tue, 23 Sep 2003 05:38:00 GMT\r\n
  ETag: "1bff9-2b1-9a057e00"\r\n
  Accept-Ranges: bytes\r\n
▶ Content-Length: 689\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: 0.023884000 seconds]
  [Request in frame: 10]
```

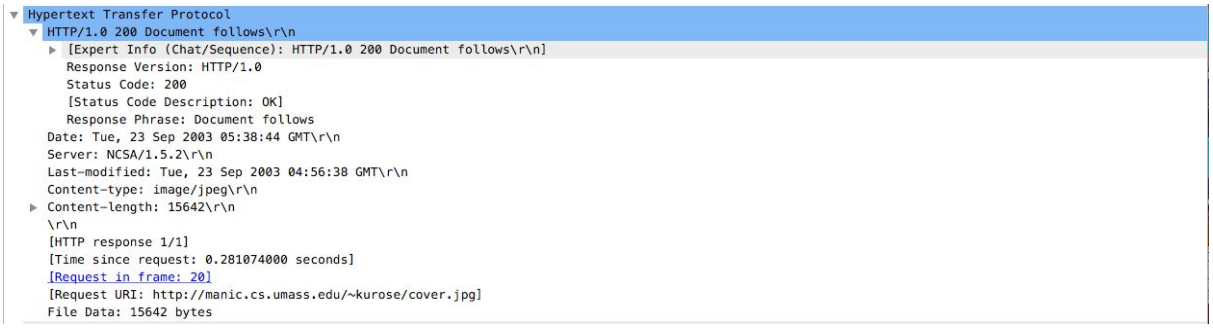
2nd HTTP GET Request:

```
▼ Hypertext Transfer Protocol
  ▼ GET /catalog/images/pearson-logo-footer.gif HTTP/1.1\r\n
    ▶ [Expert Info (Chat/Sequence): GET /catalog/images/pearson-logo-footer.gif HTTP/1.1\r\n]
      Request Method: GET
      Request URI: /catalog/images/pearson-logo-footer.gif
      Request Version: HTTP/1.1
  Host: www.aw-bc.com\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.
  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]
```

2nd Response:

3rd HTTP GET Request:

3rd Response:



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

3 GET requests are sent, and they are going to 3 different addresses:

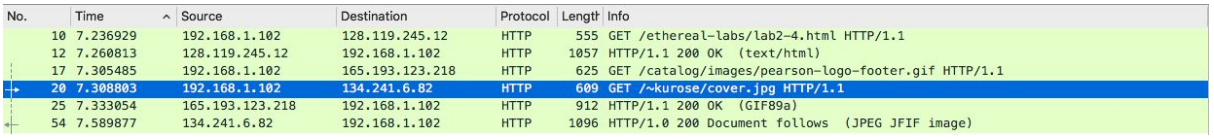
1st address: http://gaia.cs.umass.edu/ethereal-labs/lab2-4.html

2nd address: http://www.aw-bc.com/catalog/images/pearson-logo-footer.gif

3rd address: http://manic.cs.umass.edu/~kurose/cover.jpg

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

Our browser downloaded the two images from the two web sites in parallel. We can see this from when the two HTTP GET requests to the two websites were made. These two requests were made at roughly the same time as can be seen below and the browser did not wait for a response after it sent the first request to the website with an image and sent the second GET request to the other website.



No.	Time	Source	Destination	Protocol	Length	Info
10	7.236929	192.168.1.102	128.119.245.12	HTTP	555	GET /ethereal-labs/lab2-4.html HTTP/1.1
12	7.260813	128.119.245.12	192.168.1.102	HTTP	1057	HTTP/1.1 200 OK (text/html)
17	7.305485	192.168.1.102	165.193.123.218	HTTP	625	GET /catalog/images/pearson-logo-footer.gif HTTP/1.1
20	7.308803	192.168.1.102	134.241.6.82	HTTP	609	GET /~kurose/cover.jpg HTTP/1.1
25	7.333054	165.193.123.218	192.168.1.102	HTTP	912	HTTP/1.1 200 OK (GIF89a)
54	7.589877	134.241.6.82	192.168.1.102	HTTP	1096	HTTP/1.0 200 Document follows (JPEG JFIF image)

HTTP Authentication

```
  6 2.508229      192.168.1.102       128.119.245.12      HTTP      571 GET /ethereal-labs/protected_pages/lab2-5.html HTTP/1.1
  9 2.538231      128.119.245.12      192.168.1.102       HTTP      278 HTTP/1.1 401 Authorization Required  (text/html)
 65 18.516793     192.168.1.102       128.119.245.12      HTTP      622 GET /ethereal-labs/protected_pages/lab2-5.html HTTP/1.1
 68 18.541671     128.119.245.12      192.168.1.102       HTTP      499 HTTP/1.1 200 OK  (text/html)
```

First HTTP GET Request:

```
▼ 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=
    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/protected_pages/lab2-5.html]
    [HTTP request 1/1]
    [Response in frame: 9]
```

First Response:

```
▼ Hypertext Transfer Protocol
  ▼ HTTP/1.1 401 Authorization Required\r\n
    ▶ [Expert Info (Chat/Sequence): HTTP/1.1 401 Authorization Required\r\n]
      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
```

Second HTTP GET Request:

```
▼ 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=
    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]
```

Second Response:

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

The server's response is "401 Authorization Required".

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

A new field "Authorization" is included according to the server's previous response.

Task E: Preparation questions for Assignment 2*

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

    “Connection: close” and “Connection: keep-alive” imply different HTTP connections we are expecting, specifically “close” for non-persistent connections and “keep-alive” for persistent connections.

    If we only have one object to sent or download, then a non-persistent connection is enough. But when we have multiple objects to send/download, non-persistent means multiple connections are required, therefore we prefer persistent connection.