

Home Page: <http://www.public.asu.edu/~bhao2>

Lab 2

All datagrams related to favicon.ico had been ignored.

```
No.      Time          Source           Destination      Protocol Length Info
 178  8.000224000  192.168.1.11    128.119.245.12  HTTP      430      GET /wireshark-1

Frame 178: 430 bytes on wire (3440 bits), 430 bytes captured (3440 bits) on interface 0
Ethernet II, Src: Vmware_b4:cb:20 (00:0c:29:b4:cb:20), Dst: Tp-LinkT_f8:6d:f9 (a0:f3:c1:f8:6d:f9)
Internet Protocol Version 4, Src: 192.168.1.11 (192.168.1.11), Dst: 128.119.245.12 (128.119.245.12)
Transmission Control Protocol, Src Port: 52147 (52147), Dst Port: http (80), Seq: 1, Ack: 1, Len: 3
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
  User-Agent: Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.170
  Accept-Encoding: gzip,deflate,sdch\r\n
  Accept-Language: en-US,en;q=0.8\r\n
  \r\n
  [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html]
  [HTTP request 1/4]
  [Next request in frame: 179]
```

Diagram 1

```
No.      Time          Source           Destination      Protocol Length Info
 185  8.096226000  128.119.245.12  192.168.1.11    HTTP      482      HTTP/1.1 200 OK

Frame 185: 482 bytes on wire (3856 bits), 482 bytes captured (3856 bits) on interface 0
Ethernet II, Src: Tp-LinkT_f8:6d:f9 (a0:f3:c1:f8:6d:f9), Dst: Vmware_b4:cb:20 (00:0c:29:b4:cb:20)
Internet Protocol Version 4, Src: 128.119.245.12 (128.119.245.12), Dst: 192.168.1.11 (192.168.1.11)
Transmission Control Protocol, Src Port: http (80), Dst Port: 52147 (52147), Seq: 1, Ack: 377, Len:
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, 10 Feb 2014 07:19:01 GMT\r\n
  Server: Apache/2.2.3 (CentOS)\r\n
  Last-Modified: Mon, 10 Feb 2014 07:18:01 GMT\r\n
  ETag: "8734d-80-23cadc40"\r\n
  Accept-Ranges: bytes\r\n
  Content-Length: 128\r\n
  Keep-Alive: timeout=10, max=100\r\n
  Connection: Keep-Alive\r\n
  Content-Type: text/html; charset=UTF-8\r\n
  \r\n
  [HTTP response 2/4]
  [Time since request: 0.095898000 seconds]
  [Prev request in frame: 178]
  [Request in frame: 179]
  [Next request in frame: 190]
Line-based text data: text/html
<html>\n
  Congratulations. You've downloaded the file \n
  http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html!\n
</html>\n
```

Diagram 2

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

Home Page: <http://www.public.asu.edu/~bhao2>

Answer

According to the diagram 1, the browser is running HTTP 1.1. According to the diagram 2, the server is also running HTTP 1.1.

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

Answer

According to the diagram 1, the accepting languages are en-US,en.

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

Answer

According to Diagram 1, my computer's IP address is 192.168.1.11 and the IP address of gaia.cs.umass.edu is 128.119.245.12.

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

Answer

According to the diagram 2, the status code returned from the server to my browser is 200.

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

Answer

According to the diagram 2, the last modified time is Mon, 10 Feb 2014 07:18:01 GMT.

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

Answer

According to the diagram 2, Content-Length: 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.

Answer

No, there is no more headers below.

Home Page: <http://www.public.asu.edu/~bhao2>

No.	Time	Source	Destination	Protocol	Length	Info
293	6.372538000	192.168.1.11	128.119.245.12	HTTP	430	GET /wireshark-1

Frame 293: 430 bytes on wire (3440 bits), 430 bytes captured (3440 bits) on interface 0
 Ethernet II, Src: Vmware_b4:cb:20 (00:0c:29:b4:cb:20), Dst: Tp-LinkT_f8:6d:f9 (a0:f3:c1:f8:6d:f9)
 Internet Protocol Version 4, Src: 192.168.1.11 (192.168.1.11), Dst: 128.119.245.12 (128.119.245.12)
 Transmission Control Protocol, Src Port: 52200 (52200), Dst Port: http (80), Seq: 1, Ack: 1, Len: 3
 Hypertext Transfer Protocol

```
GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n
[Expert Info (Chat/Sequence): GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n]
Request Method: GET
Request URI: /wireshark-labs/HTTP-wireshark-file2.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
User-Agent: Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.170
Accept-Encoding: gzip,deflate,sdch\r\n
Accept-Language: en-US,en;q=0.8\r\n
\r\n
[Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]
[HTTP request 1/4]
[Next request in frame: 294]
```

Diagram 3

No.	Time	Source	Destination	Protocol	Length	Info
598	22.740632000	192.168.1.11	128.119.245.12	HTTP	543	GET /wireshark-1

Frame 598: 543 bytes on wire (4344 bits), 543 bytes captured (4344 bits) on interface 0
 Ethernet II, Src: Vmware_b4:cb:20 (00:0c:29:b4:cb:20), Dst: Tp-LinkT_f8:6d:f9 (a0:f3:c1:f8:6d:f9)
 Internet Protocol Version 4, Src: 192.168.1.11 (192.168.1.11), Dst: 128.119.245.12 (128.119.245.12)
 Transmission Control Protocol, Src Port: 52199 (52199), Dst Port: http (80), Seq: 1, Ack: 1, Len: 4
 Hypertext Transfer Protocol

```
GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n
[Expert Info (Chat/Sequence): GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n]
Request Method: GET
Request URI: /wireshark-labs/HTTP-wireshark-file2.html
Request Version: HTTP/1.1
Host: gaia.cs.umass.edu\r\n
Connection: keep-alive\r\n
Cache-Control: max-age=0\r\n
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8\r\n
User-Agent: Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.170
Accept-Encoding: gzip,deflate,sdch\r\n
Accept-Language: en-US,en;q=0.8\r\n
If-None-Match: "d6c96-173-cf742c40"\r\n
If-Modified-Since: Mon, 10 Feb 2014 08:06:01 GMT\r\n
\r\n
[Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]
[HTTP request 1/2]
[Next request in frame: 599]
```

Diagram 4

Home Page: <http://www.public.asu.edu/~bhao2>

No.	Time	Source	Destination	Protocol	Length	Info
296	6.468901000	128.119.245.12	192.168.1.11	HTTP	726	HTTP/1.1 200 OK

Frame 296: 726 bytes on wire (5808 bits), 726 bytes captured (5808 bits) on interface 0
 Ethernet II, Src: Tp-LinkT_f8:6d:f9 (a0:f3:c1:f8:6d:f9), Dst: Vmware_b4:cb:20 (00:0c:29:b4:cb:20)
 Internet Protocol Version 4, Src: 128.119.245.12 (128.119.245.12), Dst: 192.168.1.11 (192.168.1.11)
 Transmission Control Protocol, Src Port: http (80), Dst Port: 52200 (52200), Seq: 1, Ack: 377, Len:
 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, 10 Feb 2014 08:06:07 GMT\r\n
  Server: Apache/2.2.3 (CentOS)\r\n
  Last-Modified: Mon, 10 Feb 2014 08:06:01 GMT\r\n
  ETag: "d6c96-173-cf742c40"\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=UTF-8\r\n
\r\n
[HTTP response 2/4]
[Time since request: 0.096127000 seconds]
[Prev request in frame: 293]
[Request in frame: 294]
[Next request in frame: 301]
```

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
```

Diagram 5

No.	Time	Source	Destination	Protocol	Length	Info
604	22.837714000	128.119.245.12	192.168.1.11	HTTP	236	HTTP/1.1 304 Not

Frame 604: 236 bytes on wire (1888 bits), 236 bytes captured (1888 bits) on interface 0
 Ethernet II, Src: Tp-LinkT_f8:6d:f9 (a0:f3:c1:f8:6d:f9), Dst: Vmware_b4:cb:20 (00:0c:29:b4:cb:20)
 Internet Protocol Version 4, Src: 128.119.245.12 (128.119.245.12), Dst: 192.168.1.11 (192.168.1.11)
 Transmission Control Protocol, Src Port: http (80), Dst Port: 52199 (52199), Seq: 1, Ack: 490, Len:
 Hypertext Transfer Protocol

```
HTTP/1.1 304 Not Modified\r\n
  [Expert Info (Chat/Sequence): HTTP/1.1 304 Not Modified\r\n]
  Request Version: HTTP/1.1
  Status Code: 304
  Response Phrase: Not Modified
  Date: Mon, 10 Feb 2014 08:06:23 GMT\r\n
  Server: Apache/2.2.3 (CentOS)\r\n
  Connection: Keep-Alive\r\n
  Keep-Alive: timeout=10, max=100\r\n
  ETag: "d6c96-173-cf742c40"\r\n
\r\n
[HTTP response 2/2]
[Time since request: 0.096972000 seconds]
[Prev request in frame: 598]
[Request in frame: 599]
```

Diagram 6

Home Page: <http://www.public.asu.edu/~bhao2>

- 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?**

Answer

According to the Diagram 3, there is no IF-MODIFIED-SINCE line in the first HTTP GET, but according to the Diagram 4, IF-MODIFIED-SINCE is found in the second HTTP GET (the web page cached locally, asking the server side, the local cache need to be updated or not).

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

Answer

According to Diagram 5, the server explicitly return the contents of the file, but according to the Diagram 6, the server did not explicitly return the contents of the file since the file had not been modified.

- 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?**

Answer

According to the Diagram 4, IF-MODIFIED-SINCE is found in the second HTTP GET (the web page cached locally, asking the server side, the local cache need to be updated or not).

According to the Diagram 6, the server returning a 304 not modified follows the "IF-MODIFIED-SINCE:" header.

- 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.**

Answer

According to the Diagram 6. The HTTP status code is 304 Not Modified and the server did not explicitly return the contents of the file since the file was cached locally.

Home Page: <http://www.public.asu.edu/~bhao2>

For Question 12-19, the answers are based on the author's trace file.

The screenshot shows a network trace with the following key details:

- Packet 8:** 555 GET /etherreal-labs/lab2-3.html HTTP/1.1
- Packet 10:** 1514 [TCP segment of a reassembled PDU]
- Packet 14:** 490 HTTP/1.1 200 OK (text/html)
- Packet 15:** 54 4272 > http [ACK] Seq=502 Ack=4817 win=64240 Len=0

The expanded view of packet 10 shows the following details:

- Host:** gaia.cs.umass.edu
- User-Agent:** Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.0.2) Gecko/20021120 Netscape/7.01
- 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
- Accept-Language:** en-us, en;q=0.50
- Accept-Encoding:** gzip, deflate, compress;q=0.9
- Accept-Charset:** ISO-8859-1, utf-8;q=0.66, *;q=0.66
- Keep-Alive:** 300
- Connection:** keep-alive
- Status:** 200 OK
- Phrase:** OK
- Date:** Tue, 23 Sep 2003 05:37:02 GMT
- Server:** Apache/2.0.40 (Red Hat Linux)
- ETag:** "1bff2-1194-96813 940"

Diagram 7

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?

Answer

According to the Diagram 7, only 1 HTTP GET request was sent by my browser and the packet 8 in the trace contains the GET message for the Bill of Rights.

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

Answer

```

0000 00 08 74 4f 36 23 00 06 25 da af 73 08 00 45 00 ..t06#.. %.s..E.
0010 05 dc 21 6e 40 00 37 06 e5 1b 80 77 f5 0c c0 a8 ..!n@.7. ...w...
0020 01 66 00 50 10 b0 85 b2 aa 64 fb 98 e0 df 50 10 .f.P.... .d....P.
0030 19 20 e5 fc 00 00 48 54 54 50 2f 31 2e 31 20 32 . ....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 32 33 20 53 65 70 20 32 30 30 33 20 30 35 , 23 Sep 2003 05
0060 3a 33 37 3a 30 32 20 47 4d 54 0d 0a 53 65 72 76 :37:02 G MT..serv
0070 65 72 3a 20 41 70 61 63 68 65 2f 32 2e 30 2e 34 er: Apac he/2.0.4
0080 30 20 28 52 65 64 20 48 61 74 20 4c 69 6e 75 78 0 (Red H at Linux
0090 29 0d 0a 4c 61 73 74 2d 4d 6f 64 69 66 69 65 64 )..Last- Modified
00a0 3a 20 54 75 65 2c 20 32 33 20 53 65 70 20 32 30 : Tue, 2 3 sep 20
00b0 30 33 20 30 35 3a 33 37 3a 30 31 20 47 4d 54 0d 03 05:37 :01 GMT.
00c0 0a 45 54 61 67 3a 20 22 31 62 66 66 32 2d 31 31 .ETag: " 1bff2-11
00d0 39 34 2d 39 36 38 31 33 39 34 30 22 0d 0a 41 63 94-96813 940"..Ac
00e0 63 65 70 74 2d 52 61 6a 67 65 73 3a 20 62 70 74 cent-Pan nes: hvt
    
```

Connects in packet 10

Home Page: <http://www.public.asu.edu/~bhao2>

The first response packet (PDU) from the server, packet 10 contains the status code and phrase.

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

Answer

200 OK

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

Answer

According to the diagram 7, 3 TCP segments (10, 11 and 13) were needed to carry the single HTTP response and the text of the Bill of Rights.

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)	

Diagram 8

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

Answer

According to the Diagram 8, the browser sent 3 HTTP GET request messages. Packet 10 was sent to 128.119.245.12, packet 17 was sent to 165.193.123.218, and packet 20 was sent to 134.241.6.82.

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

Answer

Two images were downloaded in parallel. According to diagram 8, the HTTP GET requests for two images were sent using packet 17 and 20, and the response packets were 25 and 54 which means the request for the second image was made before the first image was received.

Home Page: <http://www.public.asu.edu/~bhao2>

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)

```

Frame 65: 622 bytes on wire (4976 bits), 622 bytes captured (4976 bits)
Ethernet II, Src: DellComp_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 (192.168.1.102), Dst: 128.119.245.12 (128.119.245.12)
Transmission Control Protocol, Src Port: lisp-cons (4342), Dst Port: http (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,im
      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
      Credentials: eth-students:networks
\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]

```

Diagram 9

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

Answer

According to the diagram 9, the initial HTTP GET message should be packet 6 and the packet 9 is the response to the packet 6. Thus the server's response is 401 Authorization Required.

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

Answer

The new field of the HTTP GET message is the Authorization: Basic.