Assignment 1

Part A

Part 1

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

Both my browser and the server are using HTTP/1.1

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

en-us and en

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

My computer: 128.189.70.177, the umass server: 128.119.245.12

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

200 OK when requested for the first time, 304 Not Modified thereafter.

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

Last-Modified: Thu, 11 Feb 2016 06:59:01 GMT, ie. Wed, 10 Feb 10:59:01 PM PST

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

542 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.**

No couldn't find any.

Part 2

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 I don't, it looks like a pure GET.

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

Yes, after the first request I can see the HTML in the content of the response body.

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, it says "If-Modified-Since: Thu, 11 Feb 2016 06:59:01 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 response is "304 Not Modified", no, there aren't any contents in the body.

Part 3

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?

It only sent one GET request, 449.

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

Packet no. 459

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

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?

4 TCP data segments composed the entire HTTP response. I got this by filtering for tcp.port == 80

Part 4

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

It sent four requests.

a) http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file4.html
b) http://www.pearsonhighered.com/assets/hip/us/hip_us_pearsonhighered/images/pearson_logo.gif
c) http://manic.cs.umass.edu/~kurose/cover_5th_ed.jpg (Received a "302 Found" then a "200 OK")
d) http://caite.cs.umass.edu/~kurose/cover_5th_ed.jpg (Received only a "200 OK"

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.

It looks like the requests were sent in parallel because it sent two GETs one after another then received two responses.

Part 5

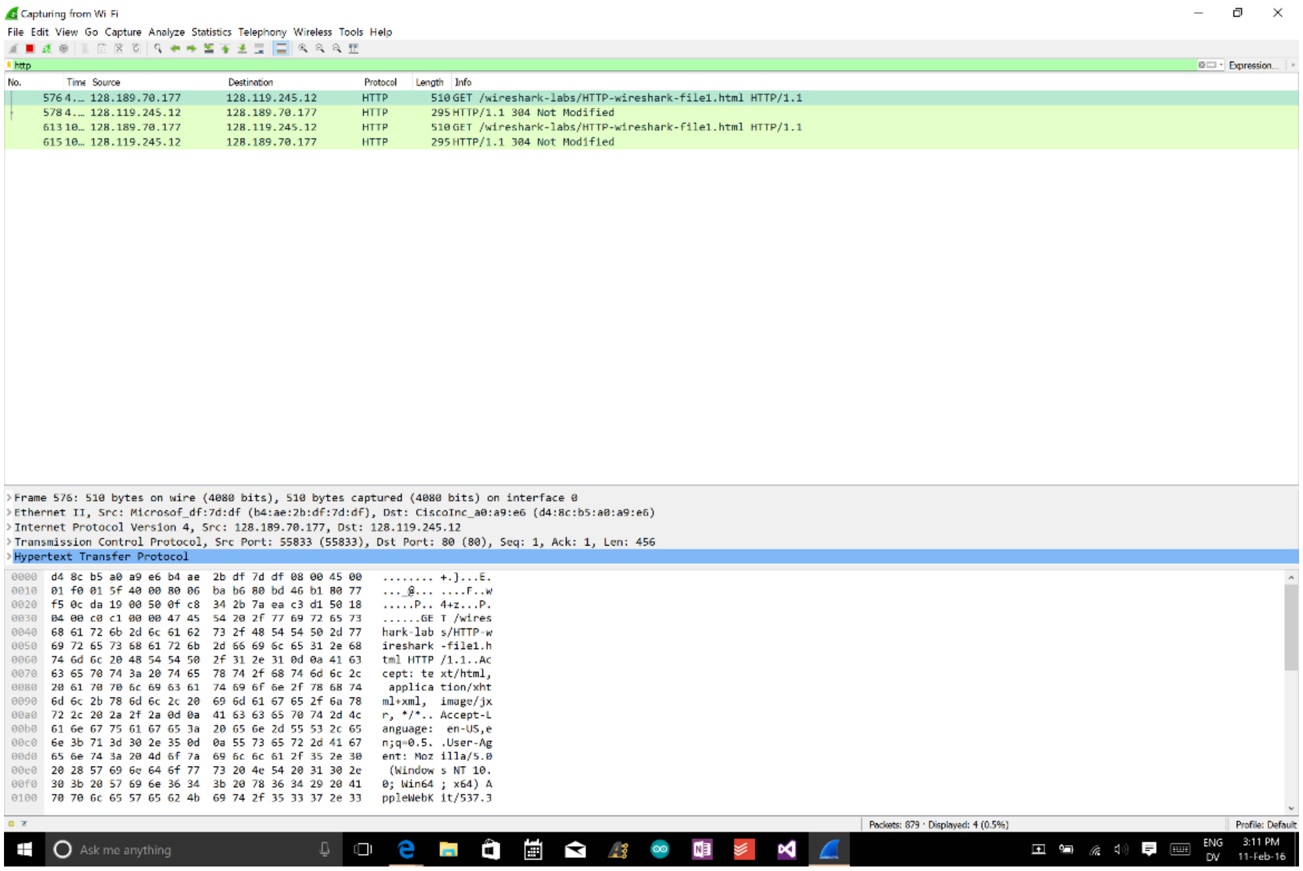
18. What is the server's response (status code and phrase) in response to the initial HTTP GET message from your browser?

401 Unauthorized

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

Authorization: Basic d2lyZXNoYXJrLXN0dWRlbnRzOm5ldHdvcms=

Credentials: wireshark-students:network (subcategory in plain text?)



```
No.   Time Source           Destination      Protocol Length Info
  576 4... 128.189.70.177   128.119.245.12   HTTP     510 GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
  578 4... 128.119.245.12   128.189.70.177   HTTP     295 HTTP/1.1 304 Not Modified
  613 10.. 128.189.70.177   128.119.245.12   HTTP     510 GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
  615 10.. 128.119.245.12   128.189.70.177   HTTP     295 HTTP/1.1 304 Not Modified
```

```
> Frame 576: 510 bytes on wire (4080 bits), 510 bytes captured (4080 bits) on interface 0
> Ethernet II, Src: Microsof_df:7d:df (b4:ae:2b:df:7d:df), Dst: CiscoInc_a0:a9:e6 (d4:8c:b5:a0:a9:e6)
> Internet Protocol Version 4, Src: 128.189.70.177, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 55833 (55833), Dst Port: 80 (80), Seq: 1, Ack: 1, Len: 456
> Hypertext Transfer Protocol
```

```
0000  d4 8c b5 a0 a9 e6 b4 ae  2b df 7d df 08 00 45 00   ........ +.}...E.
0010  01 f0 01 5f 40 00 80 06  ba b6 80 bd 46 b1 80 77   ..._@... ....F..w
0020  f5 0c da 19 00 50 0f c8  34 2b 7a ea c3 d1 50 18   .....P.. 4+z...P.
0030  04 00 c0 c1 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 31 2e 68   ireshark -file1.h
0060  74 6d 6c 20 48 54 54 50  2f 31 2e 31 0d 0a 41 63   tml HTTP /1.1..Ac
0070  63 65 70 74 3a 20 74 65  78 74 2f 68 74 6d 6c 2c   cept: te xt/html,
0080  20 61 70 70 6c 69 63 61  74 69 6f 6e 2f 78 68 74    applica tion/xht
0090  6d 6c 2b 78 6d 6c 2c 20  69 6d 61 67 65 2f 6a 78   ml+xml,  image/jx
00a0  72 2c 20 2a 2f 2a 0d 0a  41 63 63 65 70 74 2d 4c   r, */*.. Accept-L
00b0  61 6e 67 75 61 67 65 3a  20 65 6e 2d 55 53 2c 65   anguage:  en-US,e
00c0  6e 3b 71 3d 30 2e 35 0d  0a 55 73 65 72 2d 41 67   n;q=0.5. .User-Ag
00d0  65 6e 74 3a 20 4d 6f 7a  69 6c 6c 61 2f 35 2e 30   ent: Moz illa/5.0
00e0  20 28 57 69 6e 64 6f 77  73 20 4e 54 20 31 30 2e    (Window s NT 10.
00f0  30 3b 20 57 69 6e 36 34  3b 20 78 36 34 29 20 41   0; Win64 ; x64) A
0100  70 70 6c 65 57 65 62 4b  69 74 2f 35 33 37 2e 33   ppleWebK it/537.3
```

Capturing from Wi Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
Expression...
Packets: 879 · Displayed: 4 (0.5%)
Profile: Default
Ask me anything
ENG
DV
3:11 PM
11-Feb-16

Part B

client.py

```
import socket
import time
serverName = '206.87.195.168' # Mark’s computer
serverPort = 12000
clientSocket = socket.socket(socket.AF_INET, socket.SOCK_DGRAM)

# loop so I can continuously send messages
while True:

    message = raw_input('Lower case sentence: ')

    start = time.clock()

    clientSocket.sendto(message, (serverName, serverPort))
    modifiedMessage, serverAddress = clientSocket.recvfrom(2048)

    end = time.clock()
    print "%.2gs" % (end-start) # print RTT time


# should never reach here
print modifiedMessage
clientSocket.close()
```

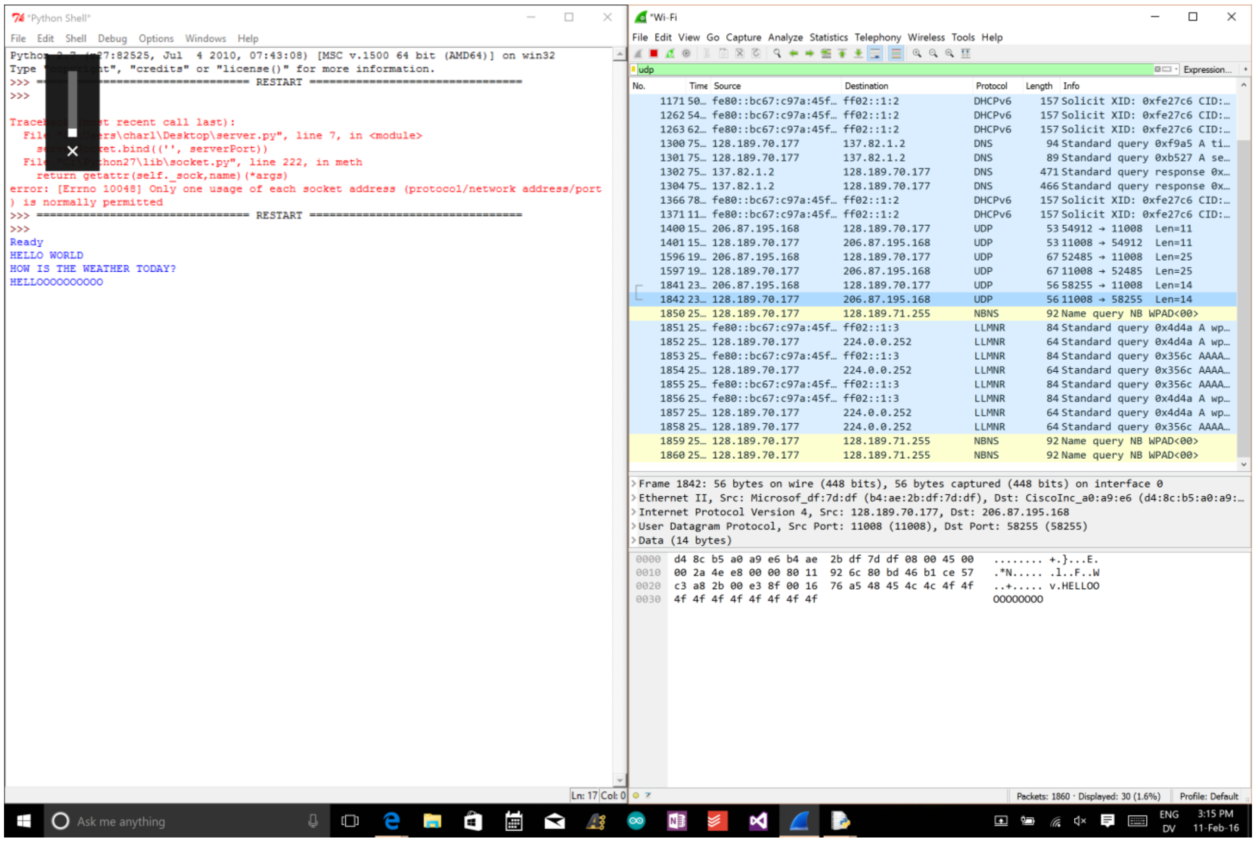
server.py

```
import socket
serverPort = 11008
serverSocket = socket.socket(socket.AF_INET, socket.SOCK_DGRAM)

try:
    serverSocket.bind(('', serverPort))
    print "Send me information!!"

    while True:
        message, clientAddress = serverSocket.recvfrom(2048)
        modifiedMessage = message.upper()
        serverSocket.sendto(modifiedMessage, clientAddress)
        print modifiedMessage
finally:
    serverSocket.close() # need to manually close on windows(!)
```

Using WireShark to read UDP messages from above code!


Python Shell
File Edit Shell Debug Options Windows Help
*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
udp
Expression...
Ln: 17 Col: 0
Packets: 1860 · Displayed: 30 (1.6%)
Profile: Default
Ask me anything
ENG
DV
3:15 PM
11-Feb-16

```
Python 2.7 (r27:82525, Jul  4 2010, 07:43:08) [MSC v.1500 64 bit (AMD64)] on win32
Type "copyright", "credits" or "license()" for more information.
>>> ================================ RESTART ================================
>>>

Traceback (most recent call last):
  File "C:\Users\charl\Desktop\server.py", line 7, in <module>
    serverSocket.bind(('', serverPort))
  File "C:\Python27\lib\socket.py", line 222, in meth
    return getattr(self._sock,name)(*args)
error: [Errno 10048] Only one usage of each socket address (protocol/network address/port
) is normally permitted
>>> ================================ RESTART ================================
>>>
Ready
HELLO WORLD
HOW IS THE WEATHER TODAY?
HELLOOOOOOOOOO
```

```
No.  Time Source                 Destination      Protocol Length Info
1171 50… fe80::bc67:c97a:45f…    ff02::1:2        DHCPv6   157 Solicit XID: 0xfe27c6 CID:…
1262 54… fe80::bc67:c97a:45f…    ff02::1:2        DHCPv6   157 Solicit XID: 0xfe27c6 CID:…
1263 62… fe80::bc67:c97a:45f…    ff02::1:2        DHCPv6   157 Solicit XID: 0xfe27c6 CID:…
1300 75… 128.189.70.177          137.82.1.2       DNS       94 Standard query 0xf9a5 A ti…
1301 75… 128.189.70.177          137.82.1.2       DNS       89 Standard query 0xb527 A se…
1302 75… 137.82.1.2              128.189.70.177   DNS      471 Standard query response 0x…
1304 75… 137.82.1.2              128.189.70.177   DNS      466 Standard query response 0x…
1366 78… fe80::bc67:c97a:45f…    ff02::1:2        DHCPv6   157 Solicit XID: 0xfe27c6 CID:…
1371 11… fe80::bc67:c97a:45f…    ff02::1:2        DHCPv6   157 Solicit XID: 0xfe27c6 CID:…
1400 15… 206.87.195.168          128.189.70.177   UDP       53 54912 → 11008  Len=11
1401 15… 128.189.70.177          206.87.195.168   UDP       53 11008 → 54912  Len=11
1596 19… 206.87.195.168          128.189.70.177   UDP       67 52485 → 11008  Len=25
1597 19… 128.189.70.177          206.87.195.168   UDP       67 11008 → 52485  Len=25
1841 23… 206.87.195.168          128.189.70.177   UDP       56 58255 → 11008  Len=14
1842 23… 128.189.70.177          206.87.195.168   UDP       56 11008 → 58255  Len=14
1850 25… 128.189.70.177          128.189.71.255   NBNS      92 Name query NB WPAD<00>
1851 25… fe80::bc67:c97a:45f…    ff02::1:3        LLMNR     84 Standard query 0x4d4a A wp…
1852 25… 128.189.70.177          224.0.0.252      LLMNR     64 Standard query 0x4d4a A wp…
1853 25… fe80::bc67:c97a:45f…    ff02::1:3        LLMNR     84 Standard query 0x356c AAAA…
1854 25… 128.189.70.177          224.0.0.252      LLMNR     64 Standard query 0x356c AAAA…
1855 25… fe80::bc67:c97a:45f…    ff02::1:3        LLMNR     84 Standard query 0x356c AAAA…
1856 25… fe80::bc67:c97a:45f…    ff02::1:3        LLMNR     84 Standard query 0x4d4a A wp…
1857 25… 128.189.70.177          224.0.0.252      LLMNR     64 Standard query 0x4d4a A wp…
1858 25… 128.189.70.177          224.0.0.252      LLMNR     64 Standard query 0x356c AAAA…
1859 25… 128.189.70.177          128.189.71.255   NBNS      92 Name query NB WPAD<00>
1860 25… 128.189.70.177          128.189.71.255   NBNS      92 Name query NB WPAD<00>

> Frame 1842: 56 bytes on wire (448 bits), 56 bytes captured (448 bits) on interface 0
> Ethernet II, Src: Microsof_df:7d:df (b4:ae:2b:df:7d:df), Dst: CiscoInc_a0:a9:e6 (d4:8c:b5:a0:a9:…
> Internet Protocol Version 4, Src: 128.189.70.177, Dst: 206.87.195.168
> User Datagram Protocol, Src Port: 11008 (11008), Dst Port: 58255 (58255)
> Data (14 bytes)

0000  d4 8c b5 a0 a9 e6 b4 ae  2b df 7d df 08 00 45 00   ........ +.}...E.
0010  00 2a 4e e8 00 00 80 11  92 6c 80 bd 46 b1 ce 57   .*N..... .l..F..W
0020  c3 a8 2b 00 e3 8f 00 16  76 a5 48 45 4c 4c 4f 4f   ..+..... v.HELLOO
0030  4f 4f 4f 4f 4f 4f 4f 4f                            OOOOOOOO
```

Python Output

Output between processes on one host

```
Lower case sentence: aoeu
0.00085s
Lower case sentence: aoe
0.0012s
Lower case sentence: oe
0.00085s
Lower case sentence: e
0.00076s
Lower case sentence: e
0.00036s
Lower case sentence: u
0.00043s
Lower case sentence: u
0.00082s
Lower case sentence: u
0.001s
Lower case sentence: u
0.00088s
Lower case sentence: u
0.0015s
Lower case sentence: u
0.0014s
Lower case sentence: u
0.0016s
Lower case sentence: u
0.0016s
Lower case sentence: u
0.00059s
Lower case sentence: u
0.0014s
Lower case sentence: u
0.0015s
Lower case sentence: u
0.0015s
Lower case sentence: u
0.0014s
Lower case sentence: u
0.0015s
Lower case sentence: u
0.0015s
Lower case sentence: u
0.0015s
Lower case sentence: u
0.0012s
Lower case sentence: u
0.0015s
Lower case sentence: u
0.0016s
Lower case sentence: u
0.0015s
Lower case sentence: u
0.0015s
Lower case sentence: e
0.0017s
```

Output when sending between hosts

```
Lower case sentence: saoeutahoseuthaoseuae
0.11s
Lower case sentence: aoeuaoeu
0.04s
Lower case sentence: aoeu
0.022s
Lower case sentence: aoeu
0.053s
Lower case sentence: aoeu
0.035s
Lower case sentence: aoeu
0.0032s
Lower case sentence: aoeu
0.069s
Lower case sentence: aoeu
0.0098s
Lower case sentence: aoeu
0.054s
Lower case sentence: aoensuthaoseuthaoesuthaoseu
0.031s
Lower case sentence: aoneusaoheu
0.074s
Lower case sentence: aoesuthaoseunth
0.1s
Lower case sentence: aosnetuhaoeu
0.045s
Lower case sentence: aoe
0.082s
Lower case sentence: aoe
0.089s
Lower case sentence: aeo
0.063s
Lower case sentence: aeo
0.11s
```