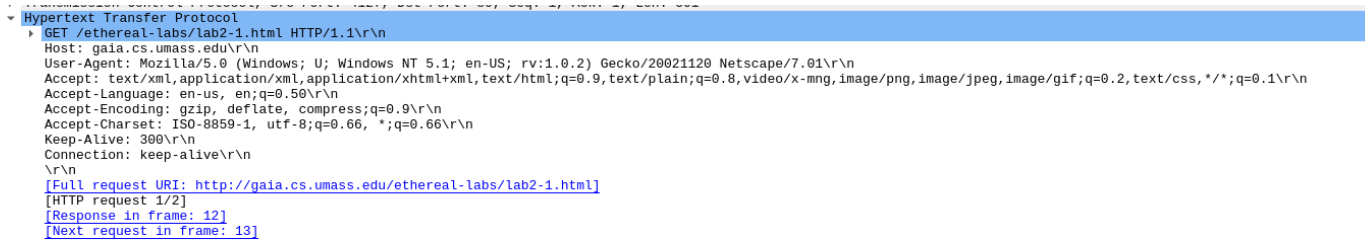
Lab02 - Week 3

Exercise 3: Using Wireshark to understand basic HTTP request/response messages

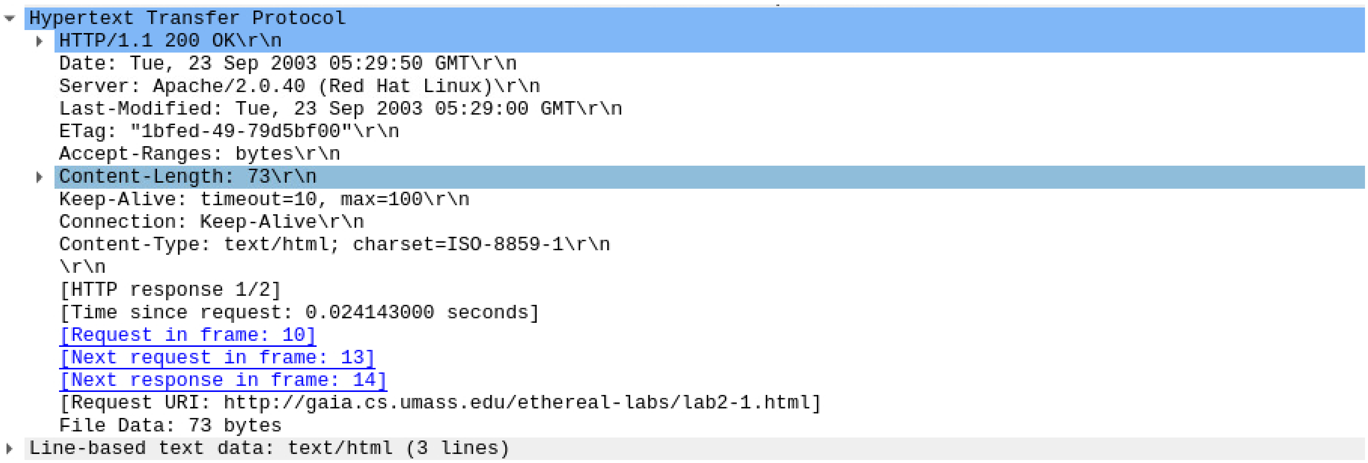
Output from http-wireshark-trace-1

HTTP Get Request



```
▾ Hypertext Transfer Protocol
  ▸ GET /ethereal-labs/lab2-1.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/lab2-1.html]
    [HTTP request 1/2]
    [Response in frame: 12]
    [Next request in frame: 13]
```

HTTP Response



```
▾ Hypertext Transfer Protocol
  ▸ HTTP/1.1 200 OK\r\n
    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/ethereal-labs/lab2-1.html]
    File Data: 73 bytes
▸ Line-based text data: text/html (3 lines)
```

Question 1: What is the status code and phrase returned from the server to the client browser?

- The server returned a 200 status code to the client browser, indicating a successful request and response.

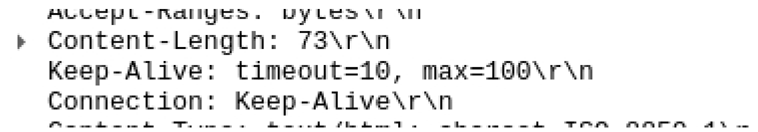
Question 2: When was the HTML file that the browser is retrieving last modified at the server? Does the response also contain a DATE header? How are these two fields different?

- Last-Modified: Tue, 23 Sep 2003 05:29:00 GMT\r\n
- Date: Tue, 23 Sep 2003 05:29:50 GMT\r\n

In this example, the date and last modified differ by 00:00:50. The last modified header should contain the date and time the origin server believes the resource was last modified, whilst the Date header should contain the date and time which the response was generated. Thus we see the response was modified just before it was sent.

Question 3: Is the connection established between the browser and the server persistent or non-persistent? How can you infer this?

The connection is persistent. This can be inferred by the Keep-Alive header in both the request and response, with the Connection header in the response also indicating it is a ‘Keep-Alive’ connection.

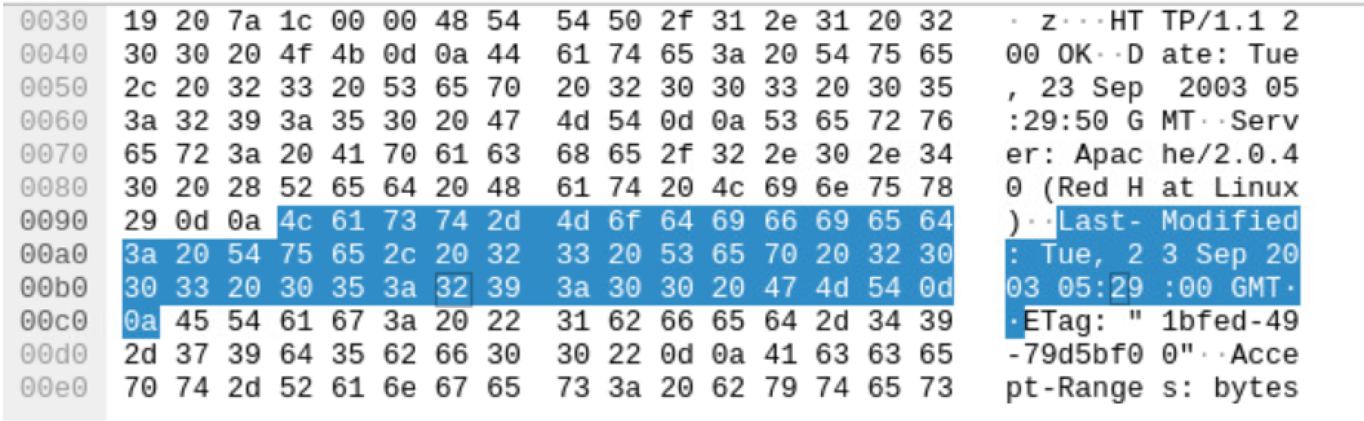


```
    Accept-Ranges: bytes\r\n
  ▸ Content-Length: 73\r\n
    Keep-Alive: timeout=10, max=100\r\n
    Connection: Keep-Alive\r\n
```

Question 4: How many bytes of content are being returned to the browser?

The HTTP response contained 73 bytes of file data.

Question 5: What is the data contained inside the HTTP response packet?

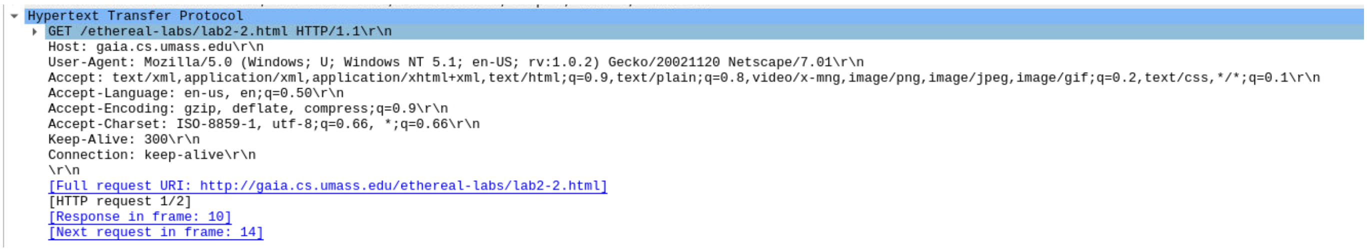


```
0030  19 20 7a 1c 00 00 48 54  54 50 2f 31 2e 31 20 32   · z···HT TP/1.1 2
0040  30 30 20 4f 4b 0d 0a 44  61 74 65 3a 20 54 75 65   00 OK··D ate: Tue
0050  2c 20 32 33 20 53 65 70  20 32 30 30 33 20 30 35   , 23 Sep  2003 05
0060  3a 32 39 3a 35 30 20 47  4d 54 0d 0a 53 65 72 76   :29:50 G MT··Serv
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 32 39  3a 30 30 20 47 4d 54 0d   03 05:29 :00 GMT·
00c0  0a 45 54 61 67 3a 20 22  31 62 66 65 64 2d 34 39   ·ETag: " 1bfed-49
00d0  2d 37 39 64 35 62 66 30  30 22 0d 0a 41 63 63 65   -79d5bf0 0"··Acce
00e0  70 74 2d 52 61 6e 67 65  73 3a 20 62 79 74 65 73   pt-Range s: bytes
```

Exercise 4: Using Wireshark to understand the HTTP CONDITIONAL GET/response interaction

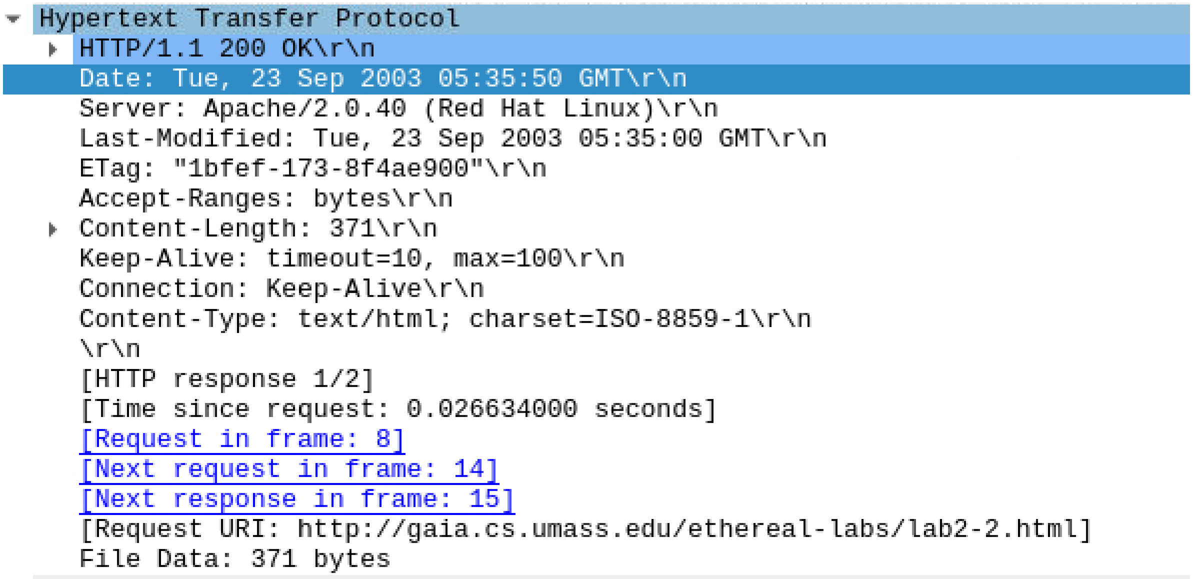
Output from http-wireshark-trace-2

HTTP Get Request 1



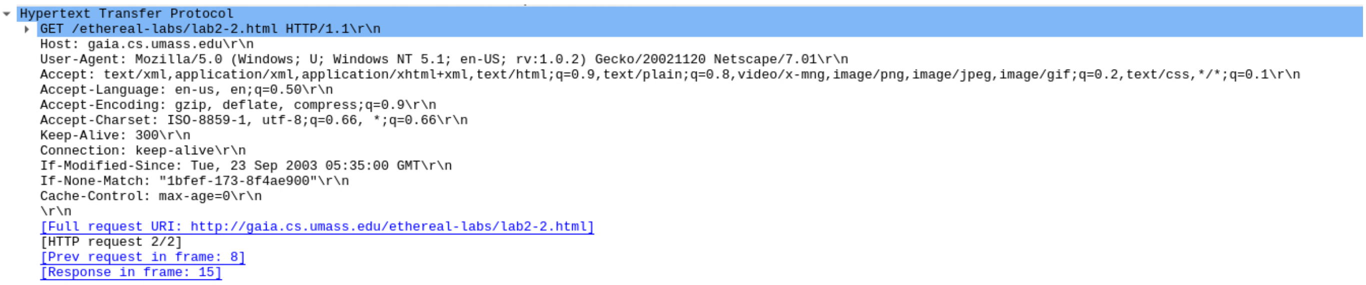
```
▾ Hypertext Transfer Protocol
  ▸ GET /ethereal-labs/lab2-2.html HTTP/1.1\r\n
    Host: gaia.cs.umass.edu\r\n
    User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.0.2) Gecko/20021120 Netscape/7.01\r\n
    Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,video/x-mng,image/png,image/jpeg,image/gif;q=0.2,text/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
    \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]
```

HTTP Response 1



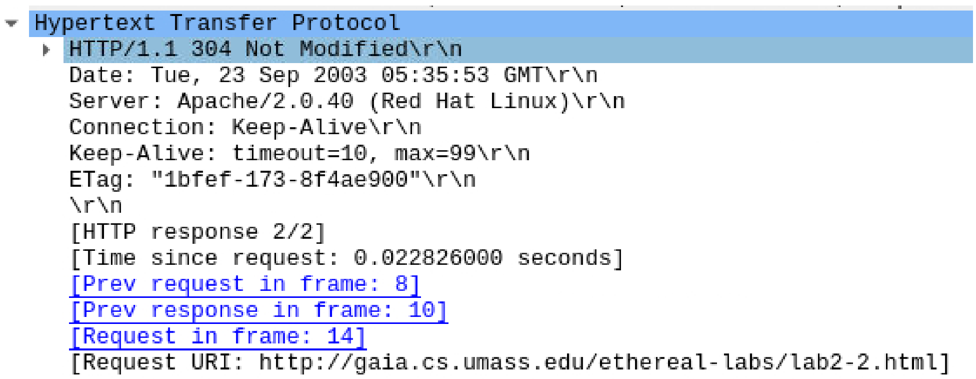
```
▾ Hypertext Transfer Protocol
  ▸ HTTP/1.1 200 OK\r\n
    Date: Tue, 23 Sep 2003 05:35:50 GMT\r\n
    Server: Apache/2.0.40 (Red Hat Linux)\r\n
    Last-Modified: Tue, 23 Sep 2003 05:35:00 GMT\r\n
    ETag: "1bfef-173-8f4ae900"\r\n
    Accept-Ranges: bytes\r\n
  ▸ Content-Length: 371\r\n
    Keep-Alive: 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
```

HTTP Get Request 2



```
▾ 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]
```

HTTP Response 2



```
▾ Hypertext Transfer Protocol
  ▸ HTTP/1.1 304 Not Modified\r\n
    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]
```

Question 1: Inspect the contents of the first HTTP GET request from the browser to the server. Do you see an “IF-MODIFIED-SINCE” line in the HTTP GET?

No?

Question 2: Does the response indicate the last time that the requested file was modified?

Yes, the requested file was last modified Tue, 23 Sep 2003 05:35:00 GMT.

Question 3: Now inspect the contents of the second HTTP GET request from the browser to the server. Do you see an “IF-MODIFIED-SINCE:” and “IF-NONE-MATCH” lines in the HTTP GET? If so, what information is contained in these header lines?

Yes. The ‘IF-MODIFIED-SINCE’ header contains a specified date time, in this case Tue, 23 Sep 2003 05:35:00 GMT\r\n, and the ‘IF-NONE-MATCH’’ header contains "1bfef-173-8f4ae900"\r\n.

The former can be inferred to mean a conditional get request where we only receive the file if the file’s last modified date is greater than the specified date. The latter, on the other hand, after some googling seems to contain an entity tag, or etag_value. In this case, the server should only return the file with status code 200 if the resource doesn’t contain the specified entity tags.

Question 4: 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.

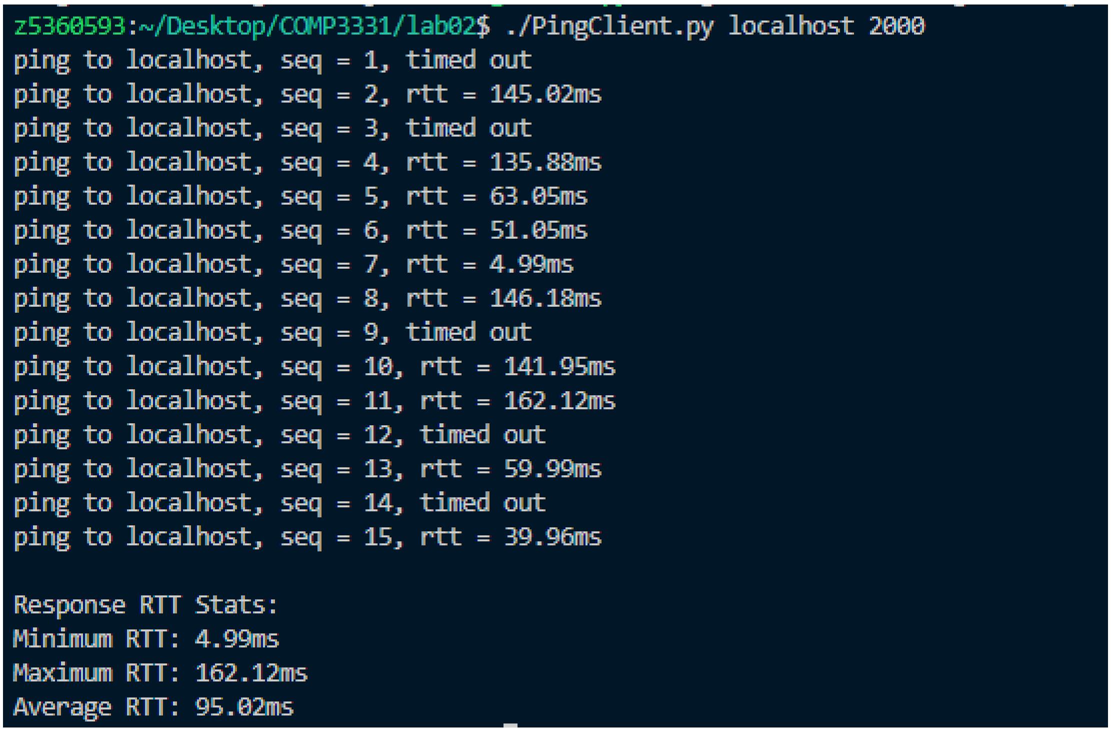
In this case, the server returned a 304 Not Modified response. We can infer that this means the requested file did not have a last-modified datetime greater than the specified time, and as such no actually file body was returned.

Question 5: What is the value of the Etag field in the 2nd response message and how it is used? Has this value changed since the 1 st response message was received?

The Etag field in the second response message contains ETag: "1bfef-173-8f4ae900"\r\n. ETags, or entity tags, identify the specific version of the requested resource, and can be used in web caches sort of like a version number, saving bandwidth by allowing resources to be resent only when they have been modified. Once a file has been modified, a new Etag value will be generated.

Since in our case our file has not been modified, the etag contained in the first http response is the same as the etag in the second http response.

Exercise 5: Ping Client (marked, submit source code as a separate file, include sample output in the report)



```
z5360593:~/Desktop/COMP3331/lab02$ ./PingClient.py localhost 2000
ping to localhost, seq = 1, timed out
ping to localhost, seq = 2, rtt = 145.02ms
ping to localhost, seq = 3, timed out
ping to localhost, seq = 4, rtt = 135.88ms
ping to localhost, seq = 5, rtt = 63.05ms
ping to localhost, seq = 6, rtt = 51.05ms
ping to localhost, seq = 7, rtt = 4.99ms
ping to localhost, seq = 8, rtt = 146.18ms
ping to localhost, seq = 9, timed out
ping to localhost, seq = 10, rtt = 141.95ms
ping to localhost, seq = 11, rtt = 162.12ms
ping to localhost, seq = 12, timed out
ping to localhost, seq = 13, rtt = 59.99ms
ping to localhost, seq = 14, timed out
ping to localhost, seq = 15, rtt = 39.96ms

Response RTT Stats:
Minimum RTT: 4.99ms
Maximum RTT: 162.12ms
Average RTT: 95.02ms
```