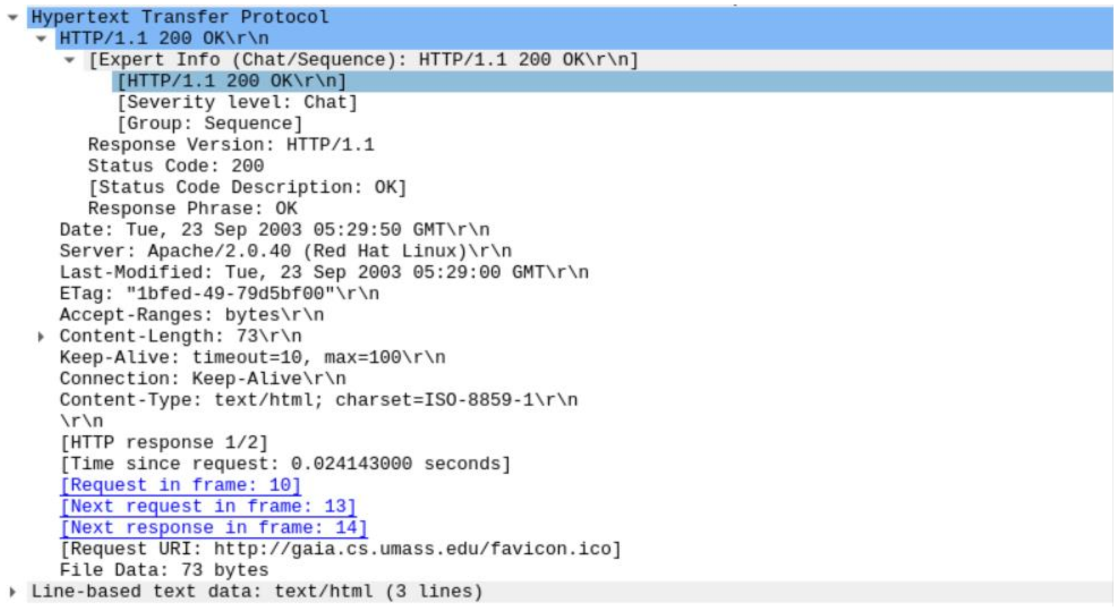
Comp9331 lab2 answer

Exercise 3: Using Wireshark to understand basic HTTP request/response messages (2.5 marks, include in your report)



```
▾ 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)
```

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

Status Code is **200** and phrase returned from the server is **ok.**

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

The time: Last-Modified: Tue, 23 Sep 2003 05:29:00 GMT\r\n.

Yes, the response also contains a DATE header, which is

Date: Tue, 23 Sep 2003 05:29:50 GMT\r\n.

Last modified time represents the time and date when the requested object was last modified. The DATE header represents the date and time when the server generated the HTTP response. They are different.

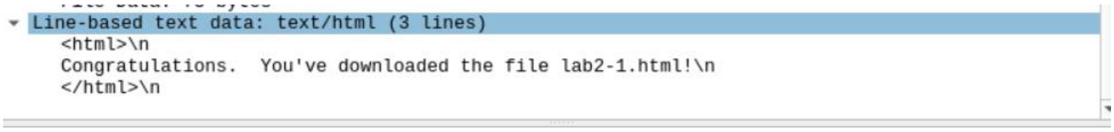
Question 3: Is the connection established between the browser and the server persistent or non-persistent? How can you infer this?

The connection established between the browser and the server is be persistent because the value in the connection field is "Keep-Alive". This indicates that the connection remains open for multiple requests and responses between the browser and the server.

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

73 bytes content according to the information “73r\n” and File Data.

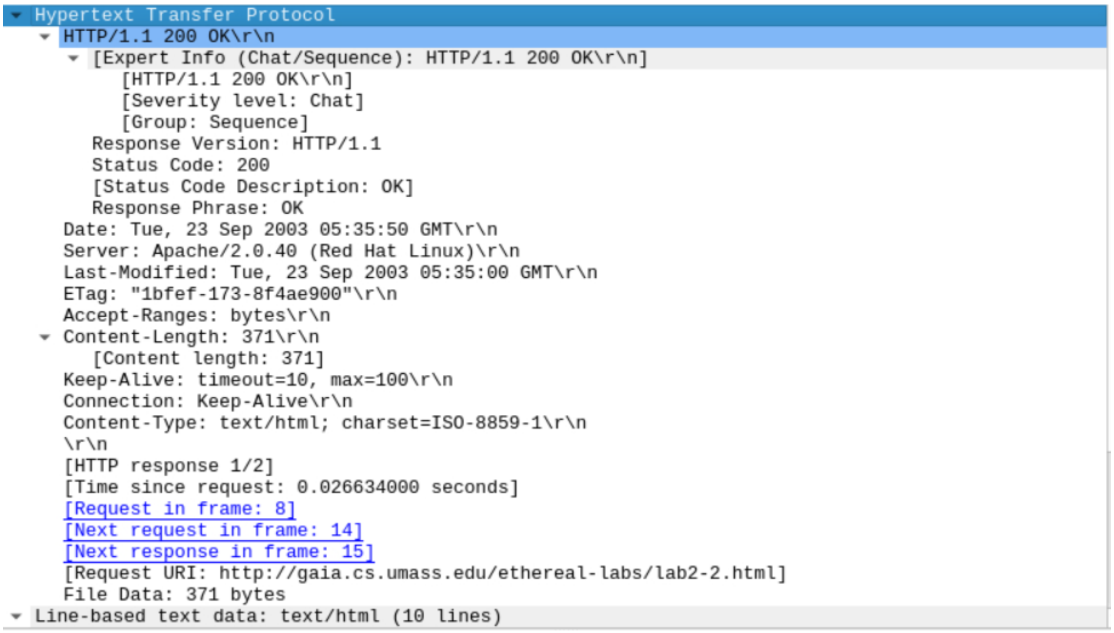
Question 5: What is the data contained inside the HTTP response packet?



```
▾ Line-based text data: text/html (3 lines)
    <html>\n
    Congratulations.  You've downloaded the file lab2-1.html!\n
    </html>\n
```

Text and html data, which is “Congratulations. You've downloaded the file lab2-1.html!”.

Exercise 4: Using Wireshark to understand the HTTP CONDITIONAL GET/response interaction (2.5 marks, include in your report)



```
▾ 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 05:35:50 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
      [Content length: 371]
    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)
```

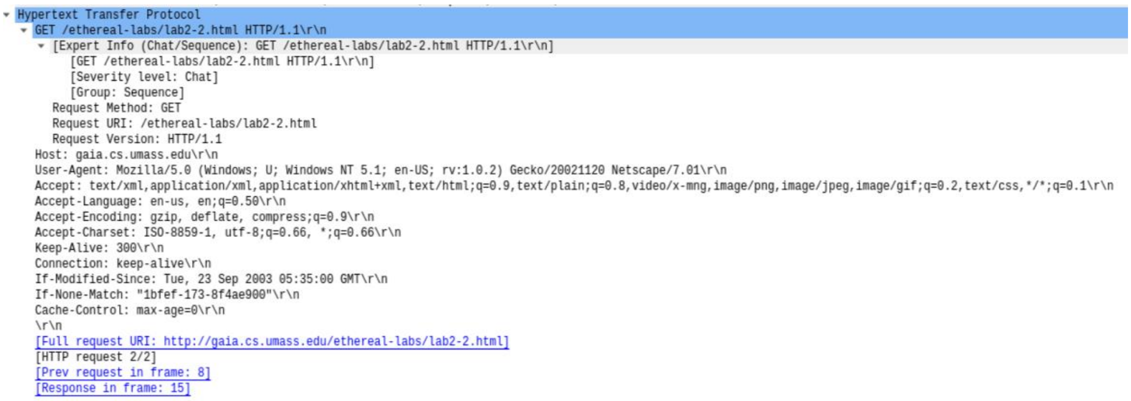
Question 1: Inspect the contents of the first HTTP GET request from the browser to the server. Do you see an “IF-MODIFIED-SINCE” line in the HTTP GET?

No, the “IF-MODIFIED-SINCE” line is not in the first HTTP GET. The "IF-MODIFIED-SINCE" header is used in conjunction with the caching mechanism

Question 2: Does the HTTP response from the server indicate the last time the requested file was modified?

Yes, Last-Modified: Tue, 23 Sep 2003 05:35:00 GMT\r\n.

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



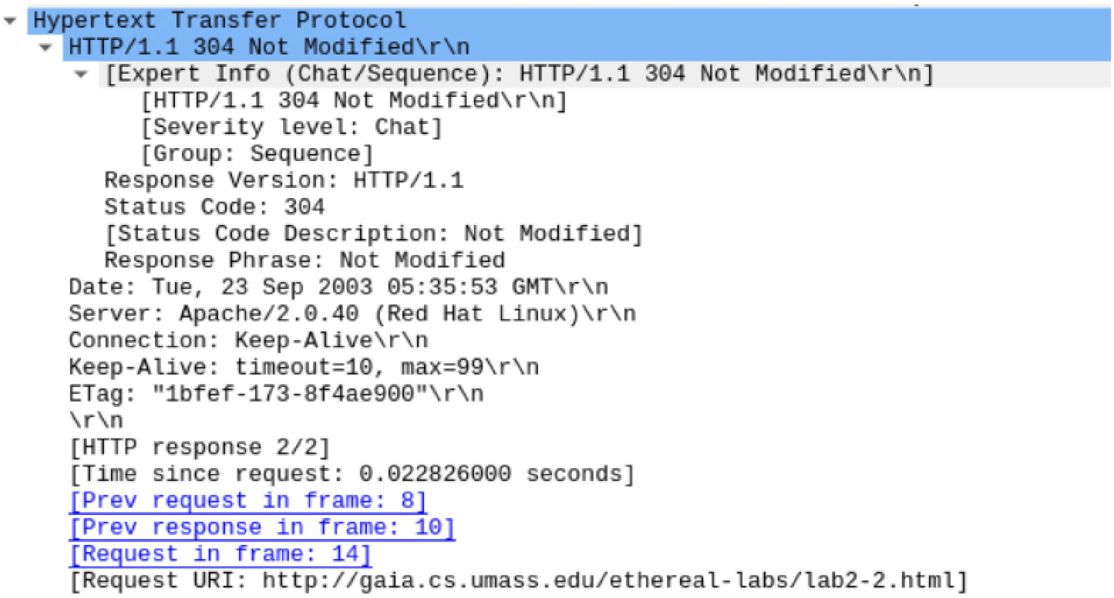
```
▾ Hypertext Transfer Protocol
  ▾ GET /ethereal-labs/lab2-2.html HTTP/1.1\r\n
    ▾ [Expert Info (Chat/Sequence): GET /ethereal-labs/lab2-2.html HTTP/1.1\r\n]
        [GET /ethereal-labs/lab2-2.html HTTP/1.1\r\n]
        [Severity level: Chat]
        [Group: Sequence]
      Request Method: GET
      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
    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, I can see the “IF-MODIFIED-SINCE:” and “IF-NONE-MATCH” lines in the HTTP GET.

The information is If-Modified-Since: Tue, 23 Sep 2003 05:35:00 GMT and

If-None-Match: "1bfef-173-8f4ae900".

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 file's contents? Explain.



```
▾ 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]
```

From the information **HTTP/1.1 304 Not Modified\r\n**,

We can know that the status code is **304** and Phrase is **Not Modified.**

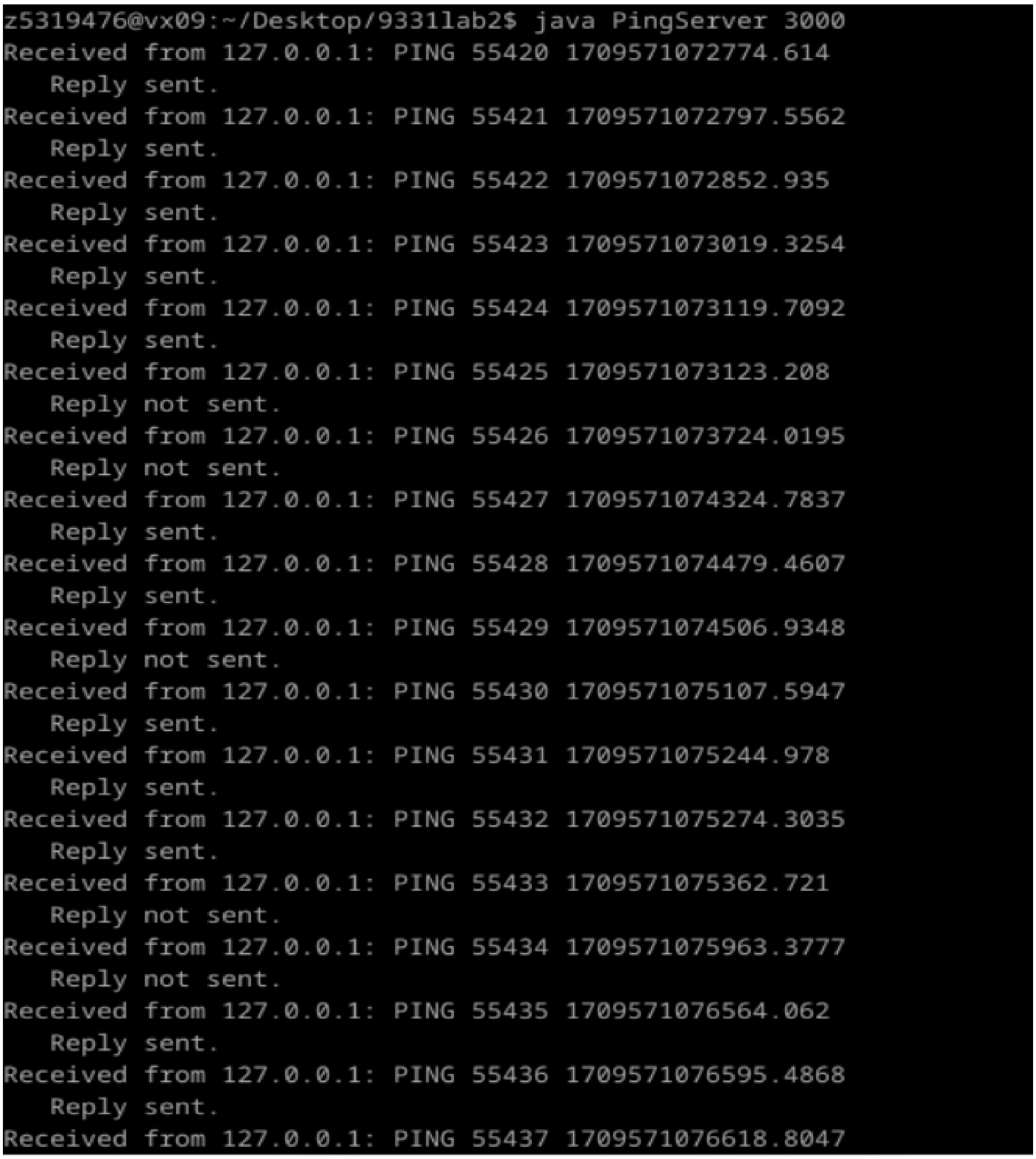
No, the server did not explicitly return the file's contents. The server has not modified the page because the value of the Etag is the same as If-None-Match value, and the locally cached version of this file can be shown by the browser.

Question 5: What is the value of the Etag field in the 2nd response message, and how is it used? Is the Etag value the same as in the 1 st response?

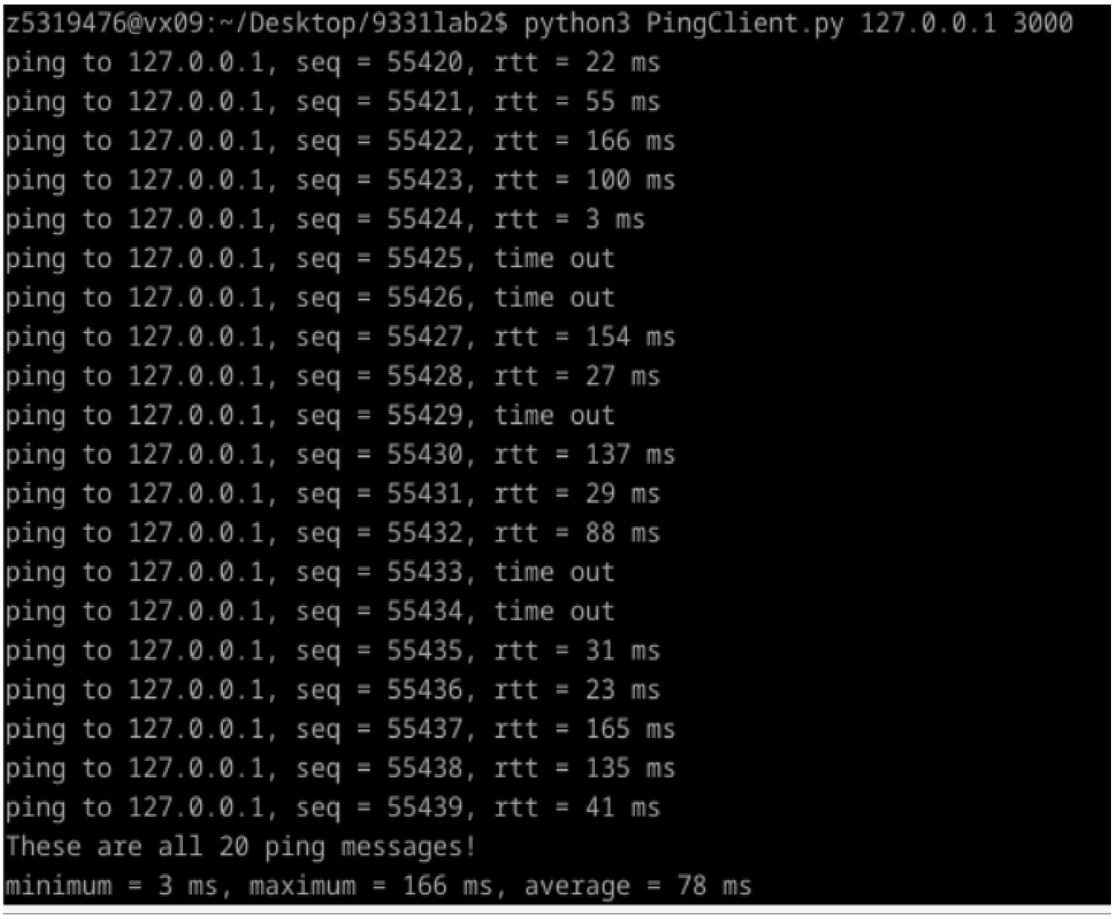
The value of the Etag field is "1bfef-173-8f4ae900"\r\n.

The ETag value is typically used for web cache validation. The server will compare the ETag value in the GET request with the ETag value on the current server resource. If they match, the server will return a status code which shows that the resource has not been modified.

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



```
z5319476@vx09:~/Desktop/9331lab2$ java PingServer 3000
Received from 127.0.0.1: PING 55420 1709571072774.614
   Reply sent.
Received from 127.0.0.1: PING 55421 1709571072797.5562
   Reply sent.
Received from 127.0.0.1: PING 55422 1709571072852.935
   Reply sent.
Received from 127.0.0.1: PING 55423 1709571073019.3254
   Reply sent.
Received from 127.0.0.1: PING 55424 1709571073119.7092
   Reply sent.
Received from 127.0.0.1: PING 55425 1709571073123.208
   Reply not sent.
Received from 127.0.0.1: PING 55426 1709571073724.0195
   Reply not sent.
Received from 127.0.0.1: PING 55427 1709571074324.7837
   Reply sent.
Received from 127.0.0.1: PING 55428 1709571074479.4607
   Reply sent.
Received from 127.0.0.1: PING 55429 1709571074506.9348
   Reply not sent.
Received from 127.0.0.1: PING 55430 1709571075107.5947
   Reply sent.
Received from 127.0.0.1: PING 55431 1709571075244.978
   Reply sent.
Received from 127.0.0.1: PING 55432 1709571075274.3035
   Reply sent.
Received from 127.0.0.1: PING 55433 1709571075362.721
   Reply not sent.
Received from 127.0.0.1: PING 55434 1709571075963.3777
   Reply not sent.
Received from 127.0.0.1: PING 55435 1709571076564.062
   Reply sent.
Received from 127.0.0.1: PING 55436 1709571076595.4868
   Reply sent.
Received from 127.0.0.1: PING 55437 1709571076618.8047
```



```
z5319476@vx09:~/Desktop/9331lab2$ python3 PingClient.py 127.0.0.1 3000
ping to 127.0.0.1, seq = 55420, rtt = 22 ms
ping to 127.0.0.1, seq = 55421, rtt = 55 ms
ping to 127.0.0.1, seq = 55422, rtt = 166 ms
ping to 127.0.0.1, seq = 55423, rtt = 100 ms
ping to 127.0.0.1, seq = 55424, rtt = 3 ms
ping to 127.0.0.1, seq = 55425, time out
ping to 127.0.0.1, seq = 55426, time out
ping to 127.0.0.1, seq = 55427, rtt = 154 ms
ping to 127.0.0.1, seq = 55428, rtt = 27 ms
ping to 127.0.0.1, seq = 55429, time out
ping to 127.0.0.1, seq = 55430, rtt = 137 ms
ping to 127.0.0.1, seq = 55431, rtt = 29 ms
ping to 127.0.0.1, seq = 55432, rtt = 88 ms
ping to 127.0.0.1, seq = 55433, time out
ping to 127.0.0.1, seq = 55434, time out
ping to 127.0.0.1, seq = 55435, rtt = 31 ms
ping to 127.0.0.1, seq = 55436, rtt = 23 ms
ping to 127.0.0.1, seq = 55437, rtt = 165 ms
ping to 127.0.0.1, seq = 55438, rtt = 135 ms
ping to 127.0.0.1, seq = 55439, rtt = 41 ms
These are all 20 ping messages!
minimum = 3 ms, maximum = 166 ms, average = 78 ms
```