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

1. What is the status code and phrase returned from the server to the client browser?
   Status Code – 200
   Phrase – OK

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
   Date – Tue, 23 Sep 2003 05:29:50 GMT

   Last Modified vs Date – Last-Modified response header is the date that the server thinks the resource was last modified, used to validate that the resource retrieved is the same. Whereas the date response header contains the date and time the response was originated. In this case the last modified and date response headers are the same.

3. Is the connection established between the browser and the server persistent or non-persistent? How can you infer this?
   Connection is HTTP persistent connection. Inferred by observing the header (i.e. Connection: Keep-Alive)

4. How many bytes of content are being returned to the browser?
   File Data: 73 bytes

5. What is the data contained inside the HTTP response packet?

```
<html>\n
  Congratulations.  You've downloaded the file lab2-1.html!\n
</html>\n
```

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

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?
   The first HTTP request doesn't have the If-Modified-Since header.

2. Does the response indicate the last time that the requested file was modified?
   The first response does have the last modified date in the header (i.e. Last-Modified: Tue, 23 Sep 2003 05:35:00 GMT\r\n).

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?
   The second request has the If-Modified-Since and If-None-Match header (i.e. If-Modified-Since: Tue, 23 Sep 2003 05:35:00 GMT\r\n, If-None-Match: "1bfef-173-8f4ae900"\r\n).

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.
   Status Code – 304
   Phrase – Not Modified
   The server didn't return the contents of the file back to the client because the file had not been modified since the provided if-modified-date. This essentially means the cached copy of the requested file is up to date with the server. Since the Etag of the second response is the same that of what we received in the first response, we can avoid double fetching the same content.

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 1st response message was received?
   ETag: "1bfef-173-8f4ae900"\r\n
   The Etag is essentially a fingerprint used to track responses by the server. It can be used to cache unchanged resources. For example, we obtain an Etag in the first response. On the second request we set If-None-Match to the Etag we got in the first response to avoid double fetching the resource. Both responses have the same Etag (i.e. the Etag hasn't changed).

Exercise 5 – Ping Client (sample output)

```
└─$ ./PingClient.py localhost 5000
ping to localhost, seq = 0, rtt = 49 ms
ping to localhost, seq = 1, rtt = 128 ms
ping to localhost, seq = 2, rtt = 176 ms
ping to localhost, seq = 3, rtt = time out
ping to localhost, seq = 4, rtt = 178 ms
ping to localhost, seq = 5, rtt = 133 ms
ping to localhost, seq = 6, rtt = 178 ms
ping to localhost, seq = 7, rtt = time out
ping to localhost, seq = 8, rtt = 141 ms
ping to localhost, seq = 9, rtt = 58 ms
--- localhost ping statistics ---
10 packets transmitted, 8 packets received, 20.0% packet loss
round-trip min/avg/max/stddev = 49.000/130.125/178.000/51.551 ms
```