

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

Q1

The status code is 200, Response Phase is OK.

```
Hypertext Transfer Protocol
  ▾ HTTP/1.1 200 OK\r\n
    > [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
      Response Version: HTTP/1.1
      Status Code: 200
      [Status Code Description: OK]
      Response Phrase: OK
```

Q2

The last modified date is Tue,23 Sep 2003 05:29:00. The response also contains a DATE Header. Date is the time point that the server makes a response. Last-Modified time is the last time that the file is modified.

```
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
```

Q3

The connection is persistent because the status of connection is Keep-Alive.

```
Keep-Alive: timeout=10, max=100\r\n
Connection: Keep-Alive\r\n
Content-Type: text/html; charset=ISO-8859-1\r\n
```

Q4

The payload length is 73 and the total length of the response is 439.

```
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
555 GET /ethereal-labs/lab2-1.html HTTP/1.1
439 HTTP/1.1 200 OK (text/html)
```

Q5

The data is a sentence.

```
Line-based text data: text/html (3 lines)
<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

Q1

The first HTTP GET does not have 'IF-MODIFIED-SINCE' line.

```
Transmission Control Protocol, Src Port: 4247, Dst Port: 80, Seq: 1, ACK: 1, Len: 501
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,
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
```

Q2

Yes, the response indicates the last modified time

```
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
```

Q3

The If-Modified-Since time is the copy of Last-Modified time.

If-None-Match is the copy of E-Tag from last response.

```
If-Modified-Since: Tue, 23 Sep 2003 05:35:00 GMT\r\n
If-None-Match: "1bfef-173-8f4ae900"\r\n
```

Q4

The status code is 304, the Phase is Not Modified. The server does not return the contents of the file because the server check the Last-Modified time and it is same, so the server decides not to return any contents of the file.

```
243 HTTP/1.1 304 Not Modified
```

Q5

The E-tag value shows below, and the value is not changed.

```
Keep-Alive: timeout=10, max=99\r\n
```

```
ETag: "1bfef-173-8f4ae900"\r\n
```

Exercise 5: Ping Client

Sample output:

```
z5125710@vx6:/tmp_and/ravel/export/ravel/3/z5125710/Desktop/COMP3331/Lab2$ python3 PingClient.py 127.0.0.1 8000
3331 ping to 127.0.0.1, seq = 0, rtt = 93 ms
3332 ping to 127.0.0.1, seq = 1, rtt = 24 ms
3333 ping to 127.0.0.1, seq = 2, rtt = time out
3334 ping to 127.0.0.1, seq = 3, rtt = time out
3335 ping to 127.0.0.1, seq = 4, rtt = 40 ms
3336 ping to 127.0.0.1, seq = 5, rtt = 113 ms
3337 ping to 127.0.0.1, seq = 6, rtt = 85 ms
3338 ping to 127.0.0.1, seq = 7, rtt = time out
3339 ping to 127.0.0.1, seq = 8, rtt = 140 ms
3340 ping to 127.0.0.1, seq = 9, rtt = time out
3341 ping to 127.0.0.1, seq = 10, rtt = 46 ms
3342 ping to 127.0.0.1, seq = 11, rtt = 45 ms
3343 ping to 127.0.0.1, seq = 12, rtt = 36 ms
3344 ping to 127.0.0.1, seq = 13, rtt = 36 ms
3345 ping to 127.0.0.1, seq = 14, rtt = 9 ms

Minimum RTT = 9ms
Maximum RTT = 140ms
Average RTT = 61ms
26.666666666666668 % of packets have been lost through the network.
z5125710@vx6:/tmp_and/ravel/export/ravel/3/z5125710/Desktop/COMP3331/Lab2$
```

```
Reply not sent.
Received from 127.0.0.1: 3335 PING seq = 4, 2020-10-05 01:59:16.388
Reply sent.
Received from 127.0.0.1: 3336 PING seq = 5, 2020-10-05 01:59:16.428
Reply sent.
Received from 127.0.0.1: 3337 PING seq = 6, 2020-10-05 01:59:16.541
Reply sent.
Received from 127.0.0.1: 3338 PING seq = 7, 2020-10-05 01:59:16.626
Reply not sent.
Received from 127.0.0.1: 3339 PING seq = 8, 2020-10-05 01:59:17.226
Reply sent.
Received from 127.0.0.1: 3340 PING seq = 9, 2020-10-05 01:59:17.366
Reply not sent.
Received from 127.0.0.1: 3341 PING seq = 10, 2020-10-05 01:59:17.967
Reply sent.
Received from 127.0.0.1: 3342 PING seq = 11, 2020-10-05 01:59:18.013
Reply sent.
Received from 127.0.0.1: 3343 PING seq = 12, 2020-10-05 01:59:18.058
Reply sent.
Received from 127.0.0.1: 3344 PING seq = 13, 2020-10-05 01:59:18.094
Reply sent.
Received from 127.0.0.1: 3345 PING seq = 14, 2020-10-05 01:59:18.130
Reply sent.
```