

COMP9331 LAB 02

YUAN GAO Z5239220

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

http						
No.	Time	Source	Destination	Protocol	Length	Info
10	4.694850	192.168.1.102	128.119.245.12	HTTP	555	GET /ethereal-labs/lab2-1.html HTTP/1.1
12	4.718993	128.119.245.12	192.168.1.102	HTTP	439	HTTP/1.1 200 OK (text/html)
13	4.724332	192.168.1.102	128.119.245.12	HTTP	541	GET /favicon.ico HTTP/1.1
14	4.750366	128.119.245.12	192.168.1.102	HTTP	1395	HTTP/1.1 404 Not Found (text/html)

▶ Frame 12: 439 bytes on wire (3512 bits), 439 bytes captured (3512 bits)
▶ Ethernet II, Src: LinksysG_da:af:73 (00:06:25:da:af:73), Dst: Dell_4f:36:23 (00:08:74:4f:36:23)
▶ Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.102
▶ Transmission Control Protocol, Src Port: 80, Dst Port: 4127, Seq: 1, Ack: 502, Len: 385
▼ 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
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]

Question 1

According to the graph:

- Status Code: 200
- Response Phrase: OK

Question 2

According to the graph:

- Last modified at the server:
Last-Modified: Tue, 23 Sep 2003 05:29:00 GMT\r\n
- Yes, the response contains a DATE header:
Date: Tue, 23 Sep 2003 05:29:50 GMT\r\n
- Data: indicates response time from server to client.
Last-Modified: indicates the last modified time of data.

Question 3

- The connection established between the browser and the server persistent is persistent. Because in `Connection:` line, the status is `Keep-Alive\r\n`

Question 4

- According to `Content-Length: 73\r\n` line, there are 73 bytes of content are being returned to the browser

Question 5

```

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

```

- According to `Line-based text data:` line, the data contained inside the HTTP response packet is `Congratulations. You've downloaded the file lab2-1.html!`

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

The image shows a Wireshark packet capture of an HTTP transaction. The packet list shows four packets: a GET request (No. 8), a 200 OK response (No. 10), a second GET request (No. 14), and a 304 Not Modified response (No. 15). The details pane for packet 10 shows the full HTTP response structure, including headers like Date, Server, Last-Modified, ETag, and Accept-Ranges, and the body content which is the HTML for lab2-2.html.

No.	Time	Source	Destination	Protocol	Length	Info
8	2.331268	192.168.1.102	128.119.245.12	HTTP	555	GET /ethereal-labs/lab2-2.html HTTP/1.1
10	2.357902	128.119.245.12	192.168.1.102	HTTP	739	HTTP/1.1 200 OK (text/html)
14	5.517390	192.168.1.102	128.119.245.12	HTTP	668	GET /ethereal-labs/lab2-2.html HTTP/1.1
15	5.540216	128.119.245.12	192.168.1.102	HTTP	243	HTTP/1.1 304 Not Modified

```

▼ 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
  ▼ Line-based text data: text/html (10 lines)
    \n
    <html>\n

```

Question 1

- No, because it is may the first request.

Question 2

- Yes, thr last modified is:

```
Tue, 23 Sep 2003 05:35:00 GMT\r\n
```

Question 3

No.	Time	Source	Destination	Protocol	Length	Info
8	2.331268	192.168.1.102	128.119.245.12	HTTP	555	GET /ethereal-labs/lab2-2.html HTTP/1.1
10	2.357902	128.119.245.12	192.168.1.102	HTTP	739	HTTP/1.1 200 OK (text/html)
14	5.517390	192.168.1.102	128.119.245.12	HTTP	668	GET /ethereal-labs/lab2-2.html HTTP/1.1
15	5.540216	128.119.245.12	192.168.1.102	HTTP	243	HTTP/1.1 304 Not Modified

▶ Frame 14: 668 bytes on wire (5344 bits), 668 bytes captured (5344 bits)
 ▶ Ethernet II, Src: Dell_4f:36:23 (00:08:74:4f:36:23), Dst: LinksysG_da:af:73 (00:06:25:da:af:73)
 ▶ Internet Protocol Version 4, Src: 192.168.1.102, Dst: 128.119.245.12
 ▶ Transmission Control Protocol, Src Port: 4247, Dst Port: 80, Seq: 502, Ack: 686, Len: 614
 ▶ 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=0.5\r\n
 Accept-Language: en-us,en;q=0.5\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, according to the graph, we can see these two line.
- The information contained in these header lines is:

If-Modified-Since: Tue, 23 Sep 2003 05:35:00 GMT\r\n

If-None-Match: "1bfef-173-8f4ae900"\r\n

Question 4

No.	Time	Source	Destination	Protocol	Length	Info
8	2.331268	192.168.1.102	128.119.245.12	HTTP	555	GET /ethereal-labs/lab2-2.html HTTP/1.1
10	2.357902	128.119.245.12	192.168.1.102	HTTP	739	HTTP/1.1 200 OK (text/html)
14	5.517390	192.168.1.102	128.119.245.12	HTTP	668	GET /ethereal-labs/lab2-2.html HTTP/1.1
15	5.540216	128.119.245.12	192.168.1.102	HTTP	243	HTTP/1.1 304 Not Modified

▶ Frame 15: 243 bytes on wire (1944 bits), 243 bytes captured (1944 bits)
 ▶ Ethernet II, Src: LinksysG_da:af:73 (00:06:25:da:af:73), Dst: Dell_4f:36:23 (00:08:74:4f:36:23)
 ▶ Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.102
 ▶ Transmission Control Protocol, Src Port: 80, Dst Port: 4247, Seq: 686, Ack: 1116, Len: 189
 ▶ Hypertext Transfer Protocol

▼ HTTP/1.1 304 Not Modified\r\n
 ▶ [Expert Info (Chat/Sequence): HTTP/1.1 304 Not Modified\r\n
 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]
 [Response in frame: 10]
 [Request in frame: 14]
 [Request URI: http://gaia.cs.umass.edu/ethereal-labs/lab2-2.html]

- According to the graph:

The HTTP status code **304**

Phrase returned from the server in response is **Not Modified**

- No, because the last request was not modified in server.

Question 5

- According to the graph, the ETag value is:

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

- This value has not changed since the 1st response message was received.

Exercise 5: Ping Client

Client message:

```
→ lab2 python3 PingClient_Yuan.py 127.0.0.1 5000
Ping to 127.0.0.1, seq = 3331, rtt = time out
Ping to 127.0.0.1, seq = 3332, rtt = 183 ms
Ping to 127.0.0.1, seq = 3333, rtt = time out
Ping to 127.0.0.1, seq = 3334, rtt = 14 ms
Ping to 127.0.0.1, seq = 3335, rtt = time out
Ping to 127.0.0.1, seq = 3336, rtt = 8 ms
Ping to 127.0.0.1, seq = 3337, rtt = time out
Ping to 127.0.0.1, seq = 3338, rtt = time out
Ping to 127.0.0.1, seq = 3339, rtt = time out
Ping to 127.0.0.1, seq = 3340, rtt = time out
Ping to 127.0.0.1, seq = 3341, rtt = 148 ms
Ping to 127.0.0.1, seq = 3342, rtt = time out
Ping to 127.0.0.1, seq = 3343, rtt = 105 ms
Ping to 127.0.0.1, seq = 3344, rtt = time out
Ping to 127.0.0.1, seq = 3345, rtt = 158 ms

In 15 packets, there are 6 packets received:
The minimum RTT is 8 ms
The maximum RTT is 183 ms
The average RTT is 103 ms
→ lab2 █
```

Server message:

```
→ lab2 java PingServer 5000
Received from 127.0.0.1: PING 3331 2020-10-01T00:48:39.649268
  Reply not sent.
Received from 127.0.0.1: PING 3332 2020-10-01T00:48:40.253324
  Reply sent.
Received from 127.0.0.1: PING 3333 2020-10-01T00:48:40.436319
  Reply not sent.
Received from 127.0.0.1: PING 3334 2020-10-01T00:48:41.039111
  Reply sent.
Received from 127.0.0.1: PING 3335 2020-10-01T00:48:41.053421
  Reply not sent.
Received from 127.0.0.1: PING 3336 2020-10-01T00:48:41.658228
  Reply sent.
Received from 127.0.0.1: PING 3337 2020-10-01T00:48:41.666066
  Reply not sent.
Received from 127.0.0.1: PING 3338 2020-10-01T00:48:42.270700
  Reply not sent.
Received from 127.0.0.1: PING 3339 2020-10-01T00:48:42.873277
  Reply not sent.
Received from 127.0.0.1: PING 3340 2020-10-01T00:48:43.476073
  Reply not sent.
Received from 127.0.0.1: PING 3341 2020-10-01T00:48:44.080307
  Reply sent.
Received from 127.0.0.1: PING 3342 2020-10-01T00:48:44.228277
  Reply not sent.
Received from 127.0.0.1: PING 3343 2020-10-01T00:48:44.832410
  Reply sent.
Received from 127.0.0.1: PING 3344 2020-10-01T00:48:44.937576
  Reply not sent.
Received from 127.0.0.1: PING 3345 2020-10-01T00:48:45.540141
  Reply sent.
```