

COMP3331 Lab 02

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

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)

```
> 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: 4127, Dst Port: 80, Seq: 1, Ack: 1, Len: 501
> 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
    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
```

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
    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
```

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

The status code and phrase returned is '200 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?

Date: Tue, 23 Sep 2003 05:29:50 GMT. Yes, the response also contains a DATE Header, and it is different to the last-modified. Since the DATE Header represents the time that when the server responds to the GET request, and the Last-Modified is the time that when the file is modified.

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

I think the connection established between the browser and the server is persistent. From the headers in the request and the response, we know the Connection is Keep-Alive: timeout=10, max=100. The timeout indicates the minimum amount of time the connection needs to be kept opened is 10s, and the max indicates the maximum number of requests that can be sent on this connection before closing is 100.

```
Keep-Alive: 300\r\n
Connection: keep-alive\r\n
\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
```

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

73 bytes.

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

Congratulations. You've downloaded the file lab2-1.html!

```
✓ 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.

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, I don't.

The screenshot shows the Wireshark interface with a packet list on the left and a packet details pane on the right. The packet list shows four packets, with the third packet (time 14.5.517390) selected. The packet details pane shows the selected packet's structure, including Ethernet II, Internet Protocol Version 4, Transmission Control Protocol, and Hypertext Transfer Protocol. The Hypertext Transfer Protocol section is expanded, showing the GET request for /ethereal-labs/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

Frame 14: 668 bytes on wire (5344 bits), 668 bytes captured (5344 bits) on interface
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: 1, Ack: 1, Len: 501
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]
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/
Accept-Language: en-us, en;q=0.50\r\n

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

Yes, it does, the last time that the requested file was modified is in Last-Modified: Tue, 23 Sep 2003 05:35:00 GMT.

The screenshot shows the Wireshark interface with a packet list on the left and a packet details pane on the right. The packet list shows four packets, with the second packet (time 10.2.357902) selected. The packet details pane shows the selected packet's structure, including Ethernet II, Internet Protocol Version 4, Transmission Control Protocol, and Hypertext Transfer Protocol. The Hypertext Transfer Protocol section is expanded, showing the 200 OK response.

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 10: 739 bytes on wire (5912 bits), 739 bytes captured (5912 bits) on interface
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: 1, Ack: 502, Len: 685
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 05:35:50 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

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, I do, the information contained in these header lines are shown below.

```
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
```

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.

'304 Not Modified' is returned from the server in response to this second http GET. And the server didn't explicitly return the contents of the file since a request is made from the browser for the same file with no new edits again. Thus, instead of returning the contents of the file, the server returned '304 Not Modified', and the browser can retrieve the content from its cache.

No.	Time	Source	Destination	Protocol	Length	Info
8	2.331268	192.168.1.102	128.119.245.12	HTTP	555	GET /etherreal-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 /etherreal-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]
      \[Prev request in frame: 8\]
      \[Prev response in frame: 10\]
      \[Request in frame: 14\]

```

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?

```
Keep-Alive: timeout=10, max=99\r\n
ETag: "1bfef-173-8f4ae900"\r\n
\r\n
```

ETag in both 1st response and 2nd response are the same:

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

Etag is an HTTP header used for Web cache validation and conditional request from browser to resources. (GeeksforGeeks) It is used for checking that if the client has the most updated version of a record, it also allow client to make conditional requests.

Exercise 5: Ping Client (*use python3)

```
rtt min/avg/max = 3.887/101.841/190.645 ms
z5261536@vx3:~/Desktop/cs3331/lab2$ python3 PingClient.py 127.0.0.1 5000
ping to 127.0.0.1, seq = 3331, rtt = 96 ms
ping to 127.0.0.1, seq = 3332, rtt = 58 ms
ping to 127.0.0.1, seq = 3333, rtt = 121 ms
ping to 127.0.0.1, seq = 3334, rtt = 156 ms
ping to 127.0.0.1, seq = 3335, rtt = 167 ms
ping to 127.0.0.1, seq = 3336, rtt = 57 ms
ping to 127.0.0.1, seq = 3337, rtt = 85 ms
ping to 127.0.0.1, seq = 3338, time out
ping to 127.0.0.1, seq = 3339, rtt = 26 ms
ping to 127.0.0.1, seq = 3340, rtt = 151 ms
ping to 127.0.0.1, seq = 3341, rtt = 92 ms
ping to 127.0.0.1, seq = 3342, rtt = 32 ms
ping to 127.0.0.1, seq = 3343, time out
ping to 127.0.0.1, seq = 3344, time out
ping to 127.0.0.1, seq = 3345, time out
rtt min/avg/max = 26.623/95.182/167.981 ms
z5261536@vx3:~/Desktop/cs3331/lab2$
```

```
z5261536@vx3:/tmp_ amd/reed/export/reed/3/z5261536/Desktop/cs3331/lab2$ java PingServer 5000
Received from 127.0.0.1: PING 3331 2021-06-22 13:00:46.327668
  Reply sent.
Received from 127.0.0.1: PING 3332 2021-06-22 13:00:46.424433
  Reply sent.
Received from 127.0.0.1: PING 3333 2021-06-22 13:00:46.483245
  Reply sent.
Received from 127.0.0.1: PING 3334 2021-06-22 13:00:46.604889
  Reply sent.
Received from 127.0.0.1: PING 3335 2021-06-22 13:00:46.761659
  Reply sent.
Received from 127.0.0.1: PING 3336 2021-06-22 13:00:46.929692
  Reply sent.
Received from 127.0.0.1: PING 3337 2021-06-22 13:00:46.986891
  Reply sent.
Received from 127.0.0.1: PING 3338 2021-06-22 13:00:47.072580
  Reply not sent.
Received from 127.0.0.1: PING 3339 2021-06-22 13:00:47.673335
  Reply sent.
Received from 127.0.0.1: PING 3340 2021-06-22 13:00:47.700007
  Reply sent.
Received from 127.0.0.1: PING 3341 2021-06-22 13:00:47.851410
  Reply sent.
Received from 127.0.0.1: PING 3342 2021-06-22 13:00:47.943960
  Reply sent.
Received from 127.0.0.1: PING 3343 2021-06-22 13:00:47.976019
  Reply not sent.
Received from 127.0.0.1: PING 3344 2021-06-22 13:00:48.576815
  Reply not sent.
Received from 127.0.0.1: PING 3345 2021-06-22 13:00:49.177619
  Reply not sent.
```