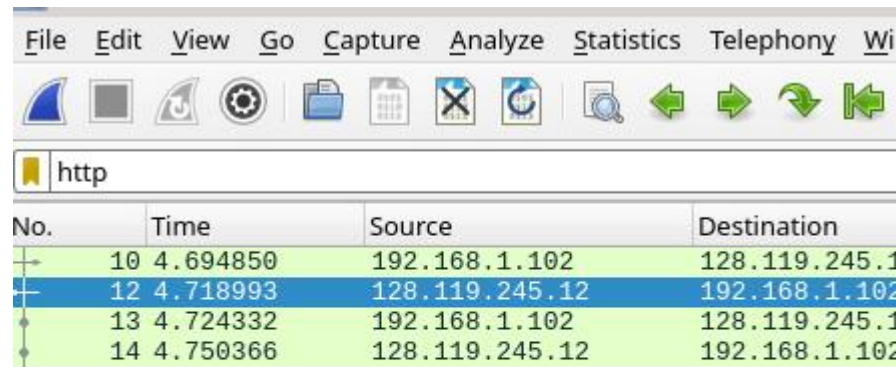
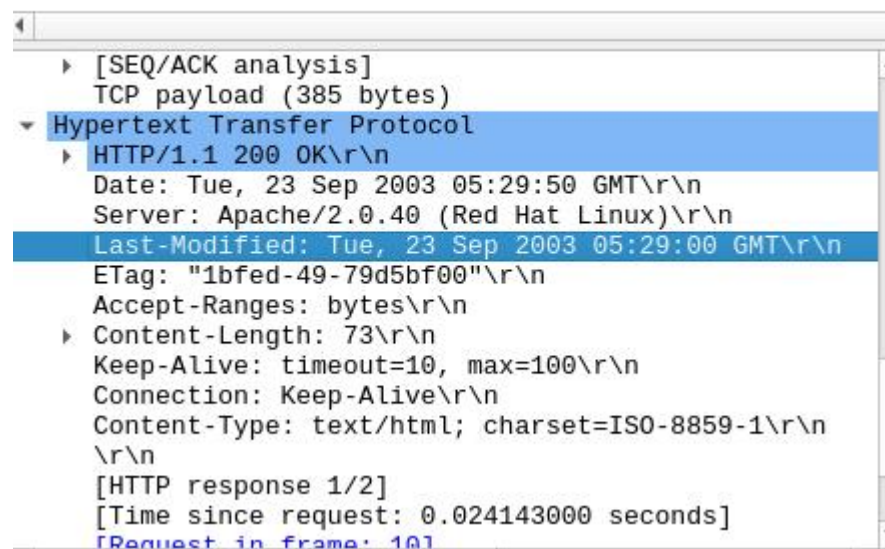


### Exercise 3: Using Wireshark to understand basic HTTP request/response messages (2.5 marks, include in your report)



No.	Time	Source	Destination
10	4.694850	192.168.1.102	128.119.245.12
12	4.718993	128.119.245.12	192.168.1.102
13	4.724332	192.168.1.102	128.119.245.12
14	4.750366	128.119.245.12	192.168.1.102



```
[SEQ/ACK analysis]
  TCP payload (385 bytes)
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
[HTTP response 1/2]
[Time since request: 0.024143000 seconds]
[Request in frame: 10]
```

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

Status Code: 200, Phrase Returned: 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?

Last modified: Tue, 23 Sep 2003 05:29:00 GMT

Response contains a date header: Tue, 23 Sep 2003 05:29:50 GMT\r\n

The Last-Modified field indicates the time when the requested resource was last modified on the server.

Date field indicates the time when the server generated the response.

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

Persistent.

The Keep-Alive head and Connection: Keep-Alive shows the server is willing to keep the connection open for a certain amount of time and can handle a maximum number of requests.

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

73 bytes

```
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/ethereal-ls]
File Data: 73 bytes
Line-based text data: text/html (3 lines)
```

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

Text/html

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

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. I didn't see "IF-MODIFIED-SINCE" line

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

Tue, 23 Sep 2003 05:35:50 GMT

The screenshot shows the Wireshark network protocol analyzer interface. The top menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, and Wire. Below the menu is a toolbar with various icons. A filter bar at the top shows 'http'. Below the filter bar are fields for 'Filter Buttons Preferences...', 'Label: Enter a description for the filter ...', and 'Comment: Enter a comment for the filter ...'. The main packet list displays four packets:

No.	Time	Source	Destination
8	2.331268	192.168.1.102	128.119.245.12
10	2.357902	128.119.245.12	192.168.1.102
14	5.517390	192.168.1.102	128.119.245.12
15	5.540216	128.119.245.12	192.168.1.102

The details pane at the bottom shows the selected packet (No. 10) as an 'Hypertext Transfer Protocol' response. The status is 'HTTP/1.1 200 OK\r\n'. The response headers are:

- 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

The details pane also shows the following information:

- [HTTP response 1/2]
- [Time since request: 0.026634000 seconds]
- [Request in frame: 8]
- [Next request in frame: 14]
- [Next response in frame: 15]

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?

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

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

No.	Time	Source	Destination
8	2.331268	192.168.1.102	128.119.245.12
10	2.357902	128.119.245.12	192.168.1.102
14	5.517390	192.168.1.102	128.119.245.12
15	5.540216	128.119.245.12	192.168.1.102

▶ [SEQ/ACK analysis]
TCP payload (614 bytes)
▼ 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 5.0; en-us; rv:1.0.2) Gecko/20030917 Firefox/1.0.2\r\n
Accept: text/xml,application/xml,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\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]

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?

Status code: 304.

Phrase returned: Not Modified.

The server didn't explicitly return the file's contents. This is because the 304 status code indicates that the client already has the latest version of the resource and can continue to use the cached version it holds, so the server does not need to transfer the same resource content again. Therefore, when the client receives a 304 response, it continues to use the resource content it has cached without triggering a re-fetch of the resource, thus improving efficiency and reducing network load.

No.	Time	Source	Destination
8	2.331268	192.168.1.102	128.119.245.12
10	2.357902	128.119.245.12	192.168.1.102
14	5.517390	192.168.1.102	128.119.245.12
15	5.540216	128.119.245.12	192.168.1.102

▶ [Timestamps]  
▶ [SEQ/ACK analysis]  
TCP payload (189 bytes)

▼ Hypertext Transfer Protocol

▶ HTTP/1.1 304 Not Modified\r\n
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-lal]

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<sup>st</sup> response?

Etag: "1bfef-173-8f4ae900"

An ETag (entity tag) is a unique identifier assigned by the server to each resource to identify a specific version of the resource.

When the resource content changes, the value of ETag will also change.

Same.



File Edit View Go Capture Analyze Statistics Telephony Wi

http

Filter Buttons Preferences... Label: Enter a description for the filter ..

Comment: Enter a comment for the filter

No.	Time	Source	Destination
8	2.331268	192.168.1.102	128.119.245.12
10	2.357902	128.119.245.12	192.168.1.102
14	5.517390	192.168.1.102	128.119.245.12
15	5.540216	128.119.245.12	192.168.1.102

[Timestamps]  
 [SEQ/ACK analysis]  
 TCP payload (189 bytes)  
 ▾ Hypertext Transfer Protocol  
   ▸ HTTP/1.1 304 Not Modified\r\n
     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-lab/

Exercise 5

```
z5369144@vx12:~/Downloads/comp3331/week2$ ./PingClient 127.0.0.1 8080
```

```
Ping to 127.0.0.1:8080, seq = 52606, rtt = 118 ms  
Ping to 127.0.0.1:8080, seq = 52607, rtt = 103 ms  
Ping to 127.0.0.1:8080, seq = 52608, rtt = 158 ms  
Ping to 127.0.0.1:8080, seq = 52609, rtt = 13 ms  
Ping to 127.0.0.1:8080, seq = 52610, rtt = 182 ms  
Ping to 127.0.0.1:8080, seq = 52611, rtt = 196 ms  
Ping to 127.0.0.1:8080, seq = 52612, timeout  
Ping to 127.0.0.1:8080, seq = 52613, rtt = 120 ms  
Ping to 127.0.0.1:8080, seq = 52614, timeout  
Ping to 127.0.0.1:8080, seq = 52615, rtt = 83 ms  
Ping to 127.0.0.1:8080, seq = 52616, timeout  
Ping to 127.0.0.1:8080, seq = 52617, rtt = 97 ms  
Ping to 127.0.0.1:8080, seq = 52618, timeout  
Ping to 127.0.0.1:8080, seq = 52619, rtt = 133 ms  
Ping to 127.0.0.1:8080, seq = 52620, rtt = 115 ms  
Ping to 127.0.0.1:8080, seq = 52621, rtt = 119 ms  
Ping to 127.0.0.1:8080, seq = 52622, rtt = 58 ms  
Ping to 127.0.0.1:8080, seq = 52623, timeout  
Ping to 127.0.0.1:8080, seq = 52624, rtt = 194 ms  
Ping to 127.0.0.1:8080, seq = 52625, rtt = 45 ms  
minimum = 13 ms , maximum = 196 ms, average = 116 ms
```