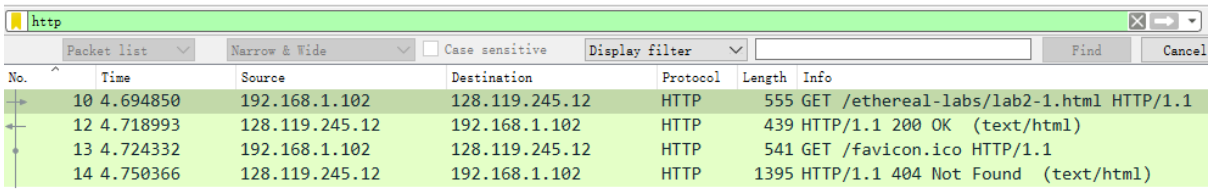
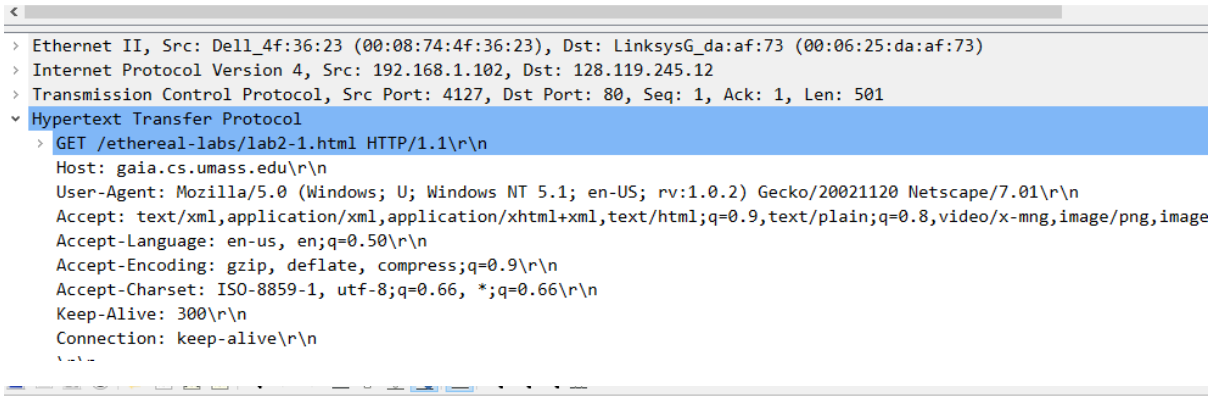
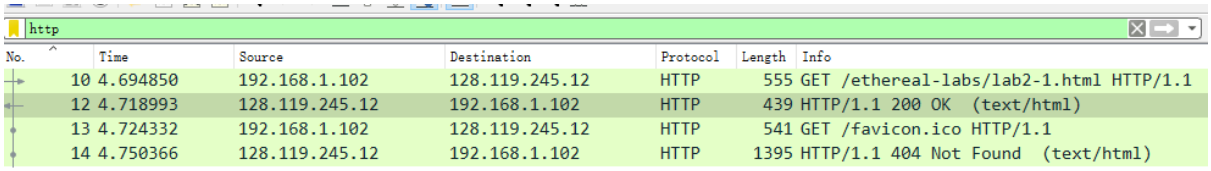
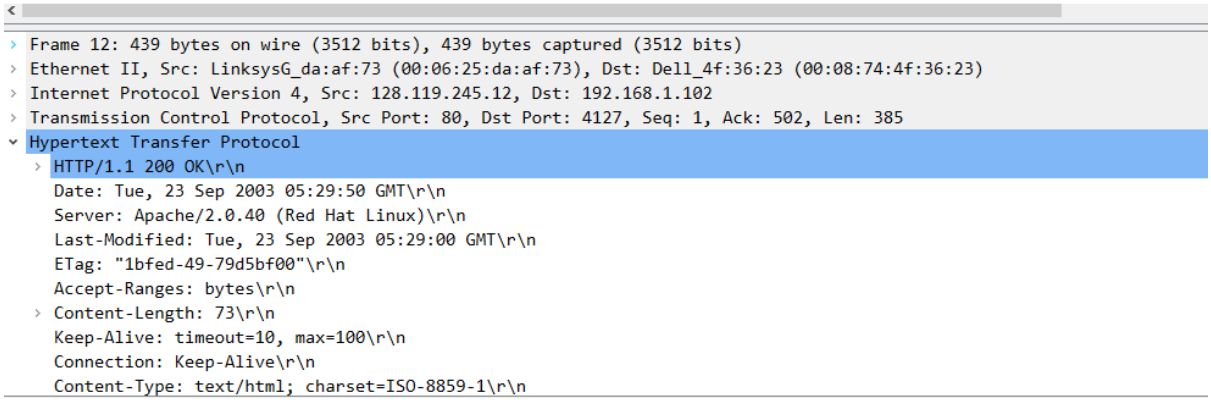
COMP3331 Lab 02

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?

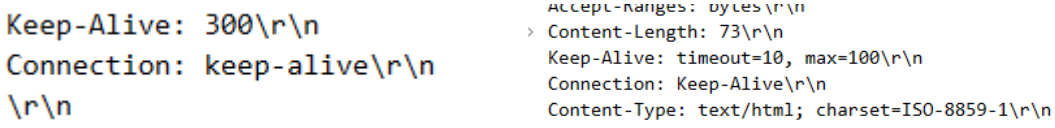
The status code and phrase returned is ‘200 OK’.

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.

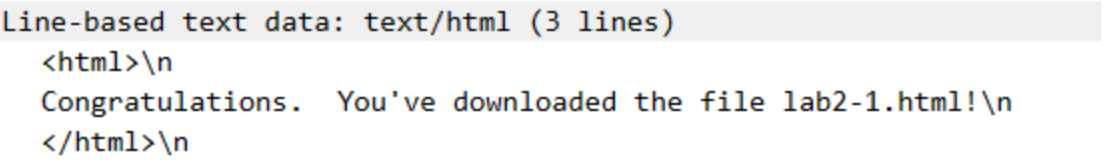


4: How many bytes of content are being returned to the browser?

73 bytes.

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

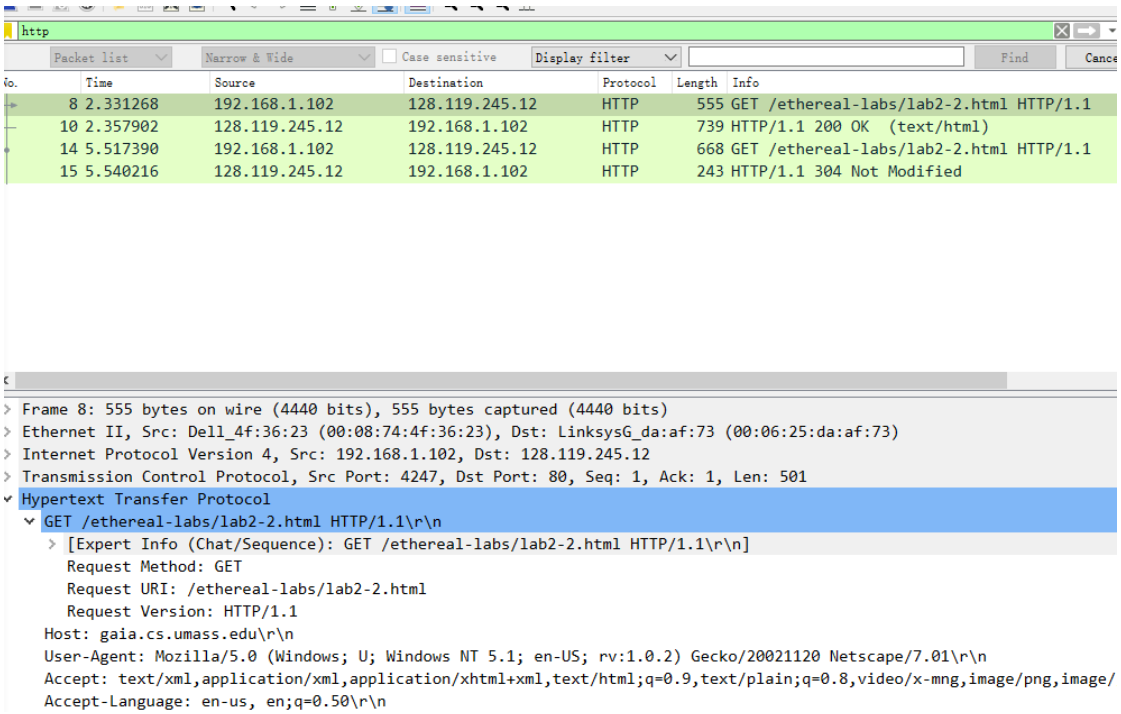
Congratulations. You’ve downloaded the file lab2-1.html!



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

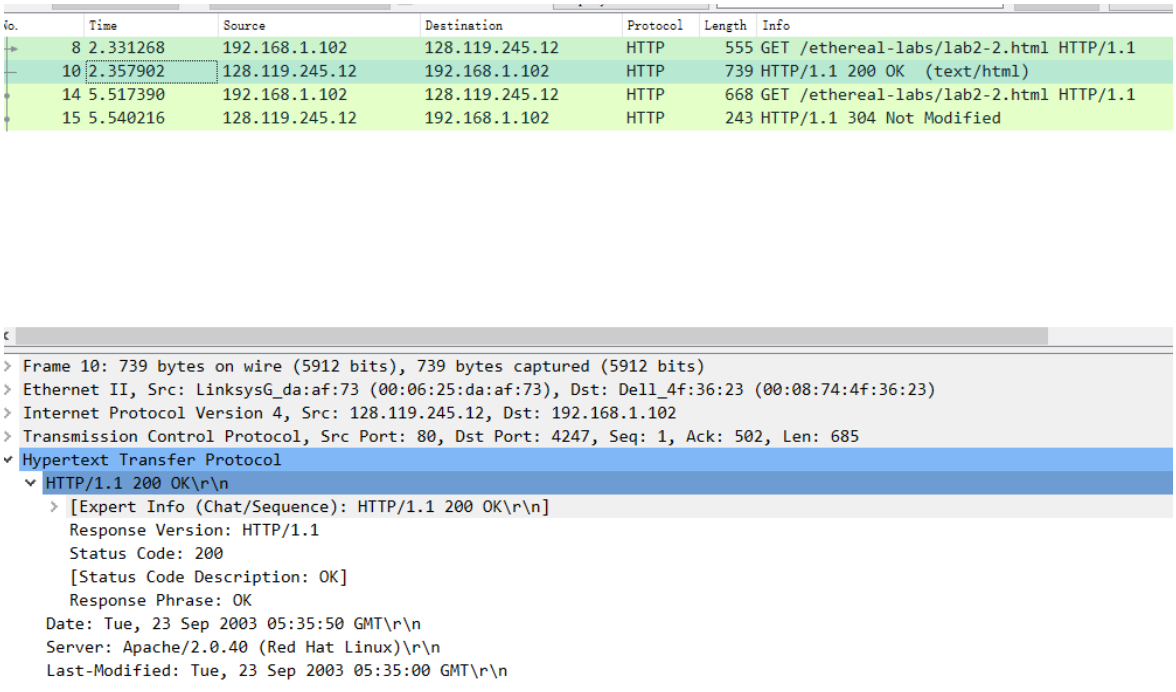
1: Inspect the contents of the first HTTP GET request from the browser to the server. Do you see an “IF-MODIFIED-SINCE” line in the HTTP GET?

No, I don’t.



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.



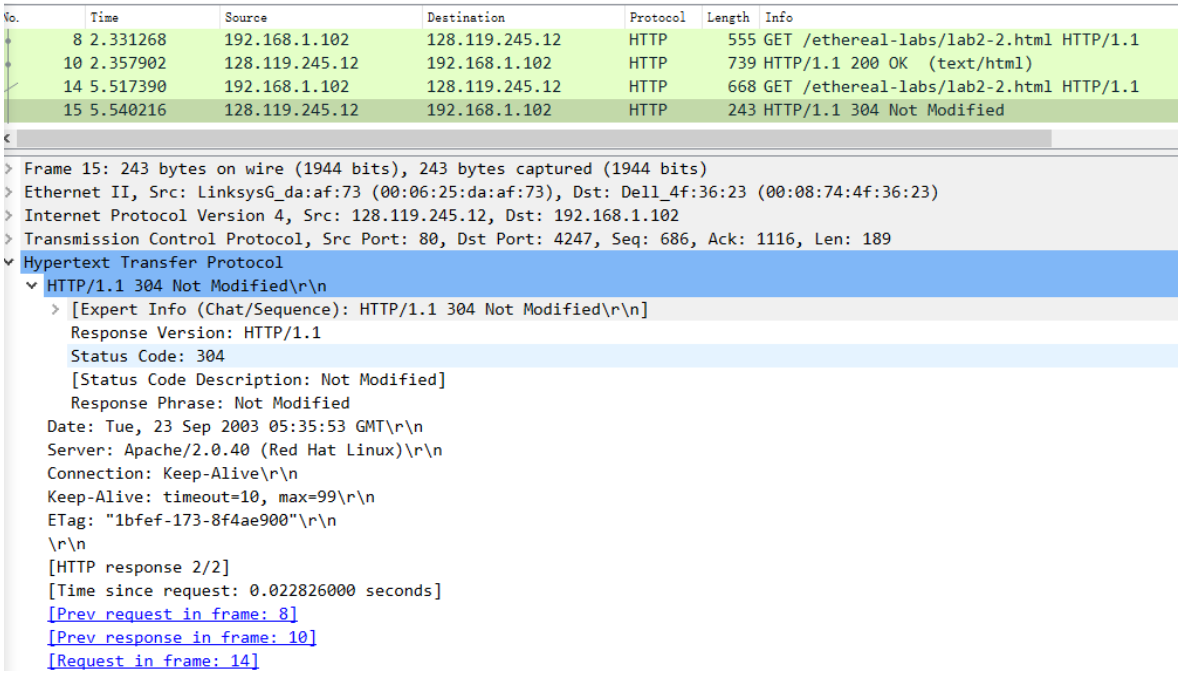
3: Now inspect the contents of the second HTTP GET request from the browser to the server. Do you see an "IF-MODIFIED-SINCE:" and "IF-NONE-MATCH" lines in the HTTP GET? If so, what information is contained in these header lines?

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.



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 1 st 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)