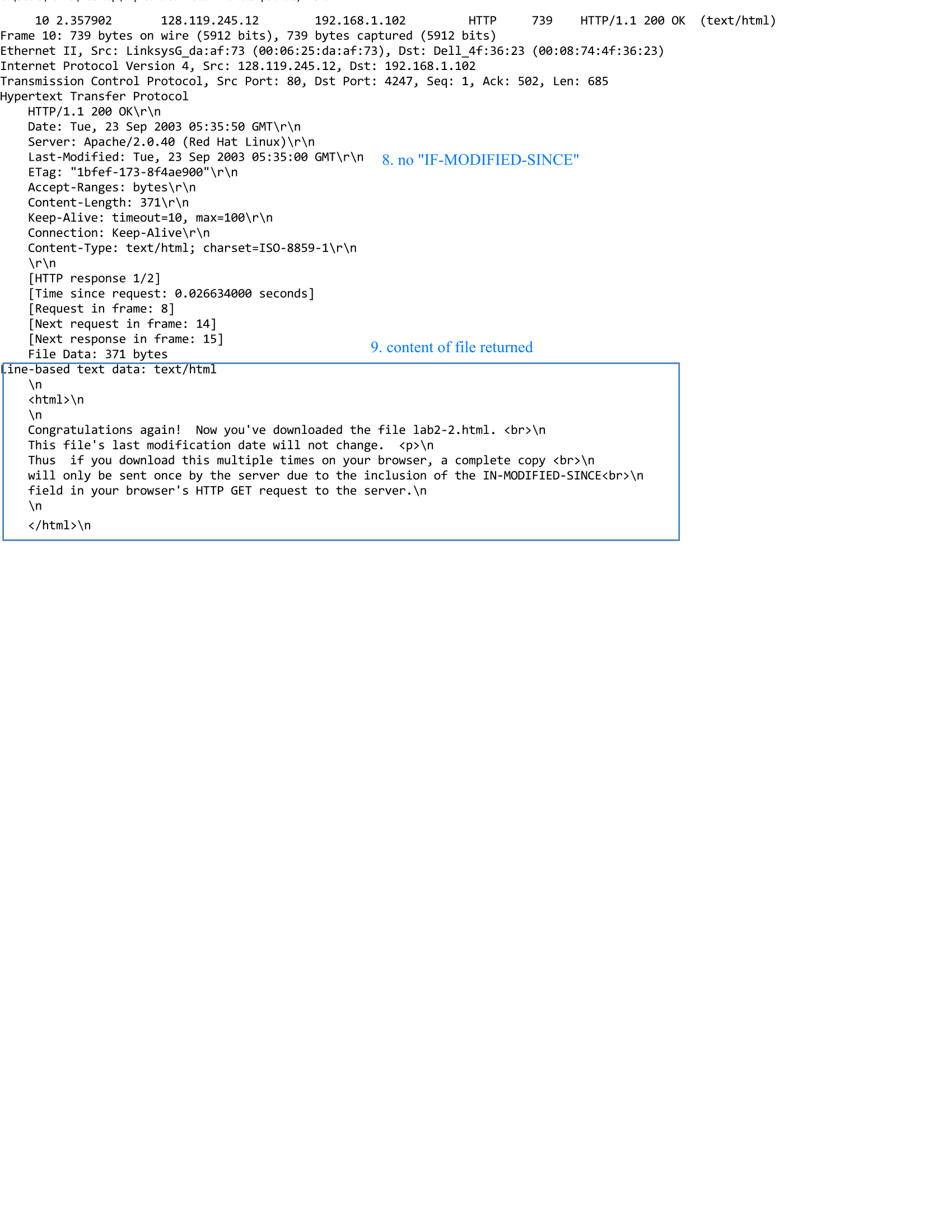
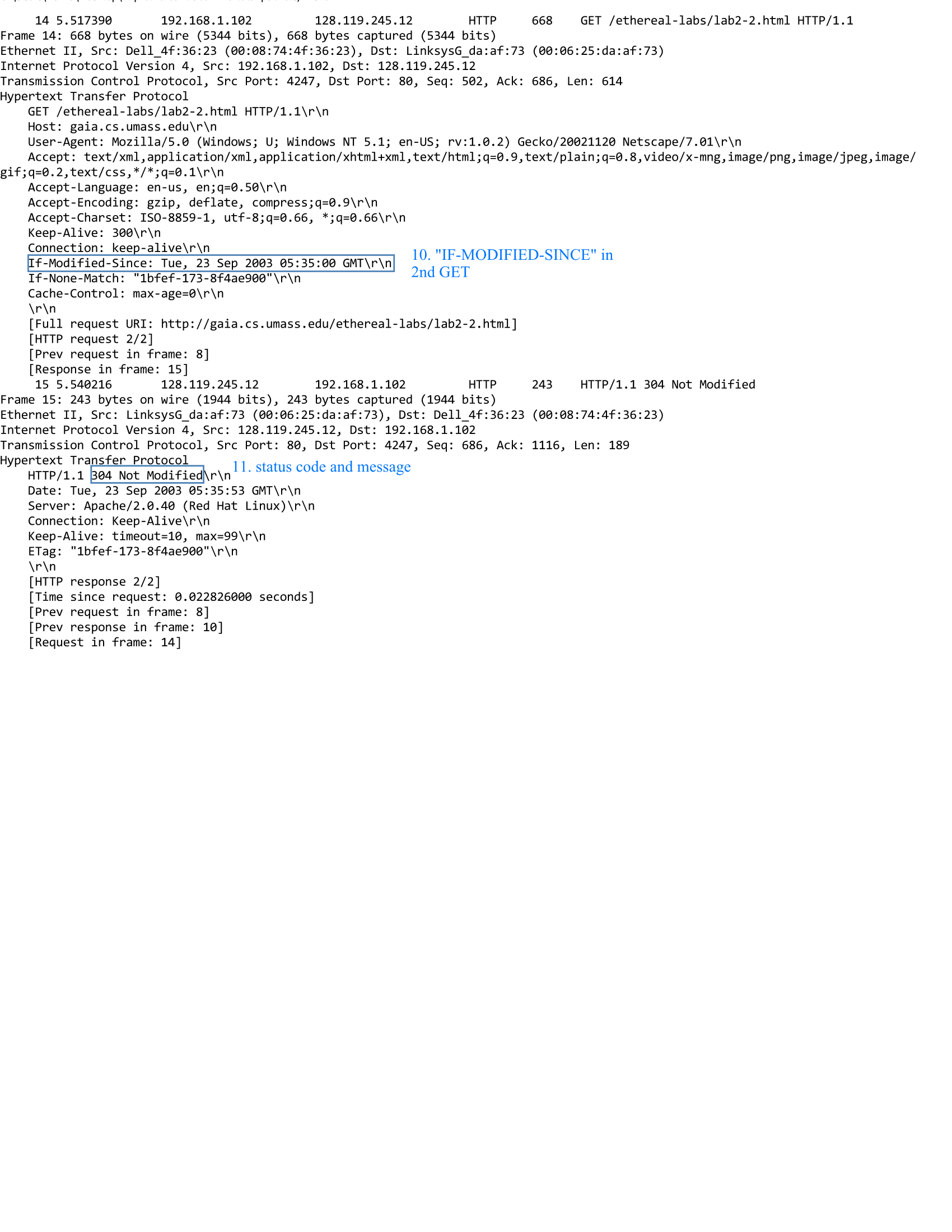
Wireshark Lab

1. **The Basic HTTP GET/response interaction**
2. The browser is running HTTP version 1.1. The server is also running HTTP version 1.1.
3. The browser can accept these versions of the English language: en-CA, en-GB, en-US or en.
4. The computer IP address is 192.168.1.10. The server IP address is 128.119.245.12.
5. The status code returned from the server to my browser is 200.
6. The document was last modified on Tue, 30 Jan 2018 06:59:01 GMT\r\n.
7. 128 bytes of content are being returned to my browser.
8. I do not see any headers within the data that are not displayed in the packet-listing window.

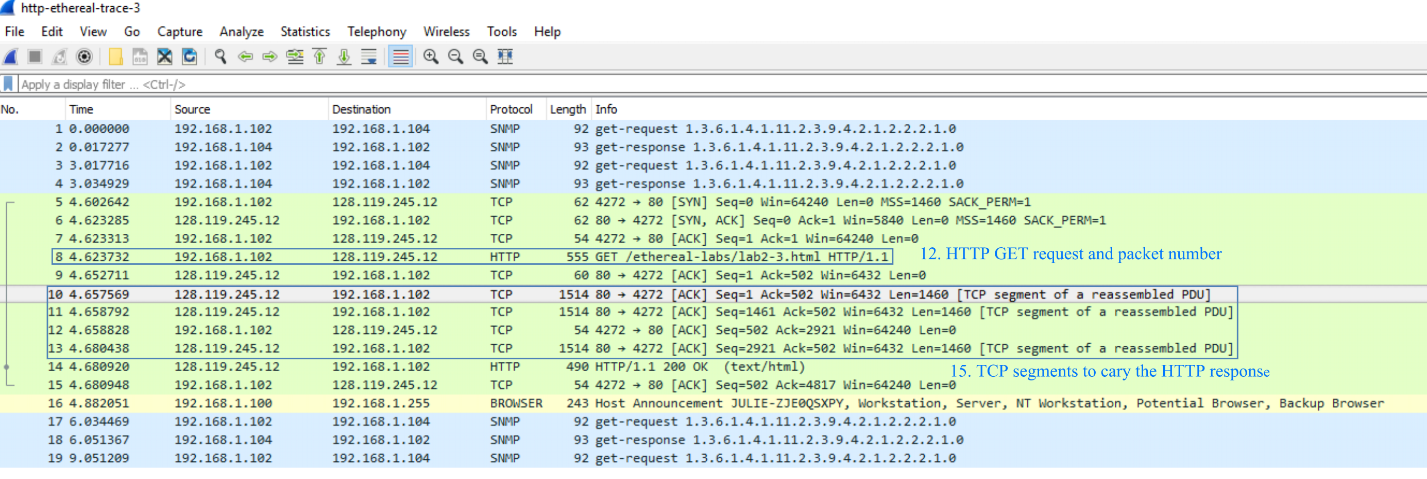


1. **The HTTP CONDITIONAL GET/response interaction**
2. No, I do not see an “IF-MODIFIED-SINCE” line in the first HTTP GET.
3. Yes, the server returned the contents of the file in the “Line-based text data” tab. I can tell because it is the exact same data as the content on the website.
4. Yes, the 2nd GET has the “IF-MODIFIED-SINCE” line. The date follows the header of when it should be updated.
5. The status code and phrase returned from the server in response to the second HTTP GET is 304 Not Modified. The content of the file did not change from before.





1. **Retrieving Long Documents**
2. The browser sent 1 HTTP GET request message. The packet number in the trace that contains the GET message for the Bill of Rights is packet 8.
3. The packet number that contains the status code and phrase associated with the response to HTTP GET request is packet 14.
4. The status code and phrase in the response is 200 OK.
5. There were 3 data-containing TCP segments needed to carry the single HTTP response and text of the Bill of Rights. These packets are 10, 11 and 13.





1. **HTML Documents with Embedded Objects**
2. There were 3 HTTP GET messages sent by the browser. These messages were sent to different IP addresses. Packet 10 was sent to 128.119.245.12, packet 17 was sent to 165.193.123.218 and packet 20 was sent to 134.241.6.82.
3. According to the time stamps and TCP source ports, it appears as though the images were downloaded serially over separate TCP connections.

