***Lab report “1.Wireshark\_Introduction.docx”***

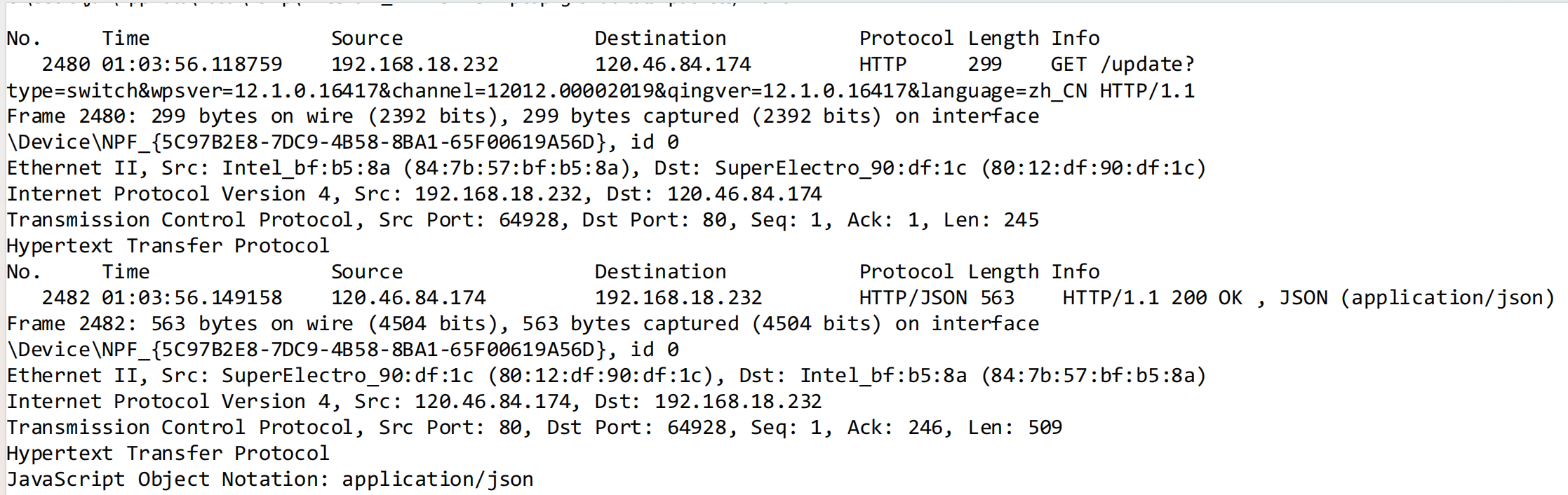
1. Three different protocols that appear in the protocol column in the unfiltered packet-listing window are:

a. TCP (Transmission Control Protocol)

b. DNS(Domain Name System)

c. HTTP (Hypertext Transfer Protocol)

1. It took 01:03:56.118759 time from when the HTTP GET message was sent until the HTTP OK reply was received.
2. The Internet address of the cs.whu.edu.cn is 120.46.84.174. The Internet address of my computer is 192.168.18.232.

4. 

***Lab report “2.Wireshark\_HTTP.docx”***

***1. The Basic HTTP GET/response interaction***

1. My browser is running HTTP version 1.1. The server is also running HTTP version 1.1, as indicated by the "HTTP/1.1" in the GET request.
2. The languages that my browser indicates it can accept to the server are Chinese (zh-CN) and English (en).
3. The IP address of my computer is 192.168.18.232. The IP address of the gaia.cs.umass.edu server is 128.119.245.12.
4. The status code returned from the server to my browser is not provided in the excerpt.
5. The information regarding when the HTML file was last modified at the server is Wed, 27 Mar 2024 05:59:02 GMT
6. The number of bytes of content being returned to my browser is 128 bytes.
7. By inspecting the raw data in the packet content window, it's possible to see additional headers within the data that are not displayed in the packet-listing window. One such header might be "Content-Type," which specifies the media type of the resource being returned.

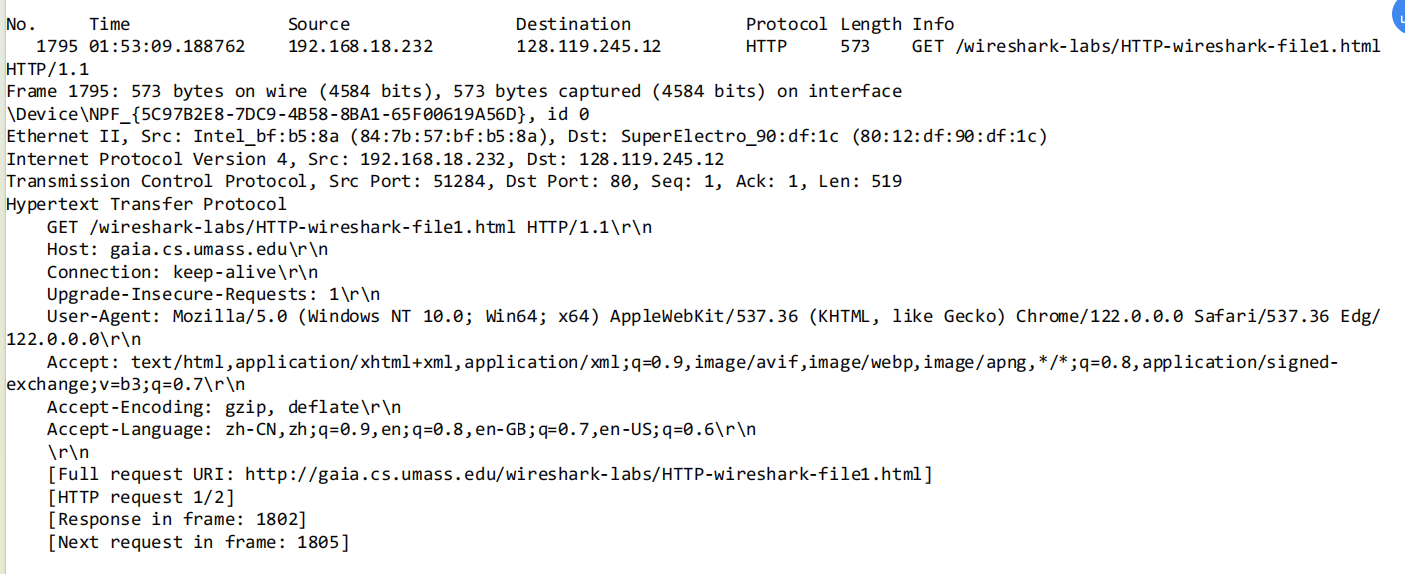


Figure of the exercise

***2. The HTTP CONDITIONAL GET/response interaction***

8. Inspecting the contents of the first HTTP GET request from the browser to the server, there is no "IF-MODIFIED-SINCE" line in the HTTP GET.

9. Inspecting the contents of the server response, the server did explicitly return the contents of the file. This can be inferred from the presence of the "HTTP/1.1 200 OK" status line in the response, which indicates that the request was successful and the server is returning the requested resource.

10. Inspecting the contents of the second HTTP GET request from the browser to the server, there is an "IF-MODIFIED-SINCE" line in the HTTP GET. Following the "IF-MODIFIED-SINCE" header is the timestamp "Fri, 29 Mar 2024 05:59:01 GMT," indicating the last modification time of the file that the browser is querying about.

11. The HTTP status code returned from the server in response to the second HTTP GET is "HTTP/1.1 304 Not Modified." This status code indicates that the requested resource has not been modified since the time specified in the "IF-MODIFIED-SINCE" header of the request. Therefore, the server did not explicitly return the contents of the file; instead, it informed the browser that the cached version is still valid, and there is no need to resend the content.

***3. Retrieving Long Documents***

12.My browser sent one HTTP GET request message. The packet number in the trace containing the GET message for the Bill of Rights is 95.

13.The packet number in the trace containing the status code and phrase associated with the response to the HTTP GET request is 131.

14.The status code and phrase in the response are "HTTP/1.1 200 OK."

15.To carry the single HTTP response and the text of the Bill of Rights, four reassembled TCP segments were needed. These segments are shown in the trace as packets #128, #129, #130, and #131.

***4. HTML Documents with Embedded Objects***

16.My browser sent three HTTP GET request messages. These GET requests were sent to the following Internet addresses:

First GET request for /wireshark-labs/HTTP-wireshark-file4.html was sent to 128.119.245.12.

Second GET request for /pearson.png was sent to 128.119.245.12.

Third GET request for /8E\_cover\_small.jpg was sent to 178.79.137.164.

17.It appears that the browser downloaded the two images in parallel rather than serially. This can be proved from the fact that there are two distinct destination IP addresses in the HTTP GET requests:

The first GET request for /pearson.png was sent to 128.119.245.12.

The second GET request for /8E\_cover\_small.jpg was sent to 178.79.137.164.

Since the destination IP addresses are different, it suggests that the browser initiated separate connections to retrieve the images concurrently from different servers

***5 HTTP Authentication***

18.The server's response to the initial HTTP GET message from the browser is:

- Status code: 401 Unauthorized

- Status phrase: Unauthorized

19.When the browser sends the HTTP GET message for the second time, the new field included in the HTTP GET message is the Authorization field. This field contains the basic authentication credentials required for accessing the protected resource.

Authorization: Basic d2lyZXNoYXJrLXN0dWRlbnRzOm5ldHdvcms=

This is a Base64-encoded representation of the username and password needed for authentication.