Part I:

1. List five different protocols that appear in the protocol column in the unfiltered packet-listing window in step 7 above.

**DNS, TCP, HTTP, TLSv1.2, MPTCP**

1. How long did it take from when the HTTP GET message was sent until the HTTP OK reply was received? (By default, the value of the Time column in the packet-listing window is the amount of time, in seconds, since Wireshark tracing began. To display the Time field in time-of-day format, select the Wireshark *View* pull down menu, then select *Time* *Display Format*, then select *Time-of-day*.)

**0.033400 seconds**

1. What is the Internet (IP) address of the gaia.cs.umass.edu? What is the Internet (IP) address of your computer?

**IP address of the gaia.cs.umass.edu: 128.119.245.12**

**IP address of my computer: 128.4.212.145**

1. Save the two HTTP messages displayed in step 9 above. To do so, select *“****Export Specified Packets****”* from the Wireshark***File*** command menu, and select “***All Packets****”* and *“****Displayed****” as shown in Figure 6*, specify the location where you want to save the files, and then click Save.

Part II:

1. Is your browser running HTTP version 1.0 or 1.1? What version of HTTP is the server running?

**My browser is running HTTP version 1.1, the server is also running HTTP version 1.1**

1. What languages (if any) does your browser indicate that it can accept to the server?

**En-US**

1. What is the IP address of your computer? Of the gaia.cs.umass.edu server?

**IP address of my computer:128.4.212.145**

**IP address of the gaia.ca.umass.edu server: 128.119.245.12**

1. What is the status code returned from the server to your browser?

**200**

1. When the HTML file that you are retrieving was last modified at the server? When was it returned to your browser?

**Last modified: Thu, 02 Mar 2017 06:59:01 GMT\r\n**

**Returned to my browser: Thu, 02 Mar 2017 19:14:50 GMT\r\n**

1. How many bytes of content are being returned to your browser?

**128 bytes**

1. Save the HTTP messages displayed. To do so, select *“Export Specified Packets”* from the Wireshark *File* command menu, and select “*All Packets”* and *“Displayed”.* Specify the location where you want to save the HTTP messages, type in a name and then click Save.
2. How many HTTP GET request messages were sent by your browser?

**4**

1. To which Internet addresses were these GET requests sent?

**These GET requests were sent to 128.119.245.12**

1. How many HTTP response messages were received by your browser?

**4**

1. Save the HTTP messages displayed. To do so, select *“Export Specified Packets”* from the Wireshark *File* command menu, and select “*All Packets”* and *“Displayed”,* Specify the location where you want to save the HTTP messages, type in a name and then click Save.

Part III:

1. How many HTTP GET request messages were sent by your browser?

**1**

1. How many data-containing TCP segments were needed to carry the single HTTP response?

**4**

1. What is the length of each of these TCP segments?

**1374 bytes, 1374 bytes, 1374 bytes, 739 bytes**

1. What is the status code and phrase associated with the response to the HTTP GET request?

**200 OK**

1. What is the IP address and port number used by gaia.cs.umass.edu to send the file? What is the IP address and TCP port number used by your client computer (source) to receive the file?

**Gaia.cs.umass.edu:**

**IP address:128.119.245.12**

**Port number: 80**

**My client computer:**

**IP address:128.4.212.145**

**TCP port number:53669**

1. What are the sequence number and ACK number of the TCP segment containing the HTTP GET command?

**Sequence number:1**

**ACK number:1**

1. Save the HTTP messages displayed. To do so, select *“Export Specified Packets”* from the Wireshark *File* command menu, and select “*All Packets”* and *“Displayed”*, Specify the location where you want to save the HTTP messages, type in a name and then click Save.

Part IV:

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

**No**

1. Inspect the contents of the server response. Did the server explicitly return the contents of the file? How can you tell?

**Yes, it did, from the Line-based text data: text/html in the response.**

**It says:**

**\n**

**<html>\n**

**\n**

**Congratulations again! Now you’ve downloaded the file lab2-2.html. <br>\n**

**This file’s last modification date will not change. <p>\n**

**Thus if you download this multiple times on your browser, a complete copy <br>\n**

**Will only be sent once by the server sue to the inclusion of the IN-MODIFIED-SINCE <br>\n**

**Field in your browser’s HTTP GET request to the server.\n**

**\n**

**</html>\n**

1. Now inspect the contents of the **second** HTTP GET **request** from your browser to the server. Do you see an “IF-MODIFIED-SINCE:” line in the HTTP GET? If so, what information follows the “IF-MODIFIED-SINCE:” header?

**Yes**

**“If-Modified-Since: Thu, 02 Mar 2017 06:59:01 GMT.. If-None-Match: “173-549b9f6c21bd9”.. Cache-control: max-age=0….**

1. 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.

**HTTP status: “HTTP/1.1 304 Not Modified”, and the server does not return the contents of the file.**

1. Save the HTTP messages displayed. To do so, select *“Export Specified Packets”* from the Wireshark *File* command menu, and select “*All Packets”* and *“Displayed”*. Specify the location where you want to save the HTTP messages, type in a name and then click Save.