**Instructions (Part Two)**

Based on your results from Part One, answer the following questions in your lab report.

1.  In the Wireshark filter bar, type the following and press enter:  tcp.dstport==80 and http.request.method=="GET"

a.  Explain what the filter is doing and explain the purpose of an HTTP GET packet.

The filter is finding all the packets that are going to the 80 port.

2.  Find the HTTP/1.1 packet that sends the GET request to retrieve [www.indofolio.com (Links to an external site.)](http://www.indofolio.com/).

WELL if you look at both packet traces that I did you will see that despite me opening the program multiple times, selecting the right connection device and going to the correct website there are NO HTTP GET packets. There are also no HTTP packets at all. Not sure what the problem is, ive tried many times and nothing seems to change that.

a.  What packet number is the GET packet?

b.  What is the size of the entire GET frame?

c.  What is the source's physical address?

i.  What device on your network is the source?  How do you know this?

d.  What is the destination's physical address?

i.  What device on your network is the destination?  How do you know this?

e.  What is the source's IP address?

f.  What is the destination's IP address?

g.  What transport layer protocol was used in the GET packet, TCP or UDP?  Why?

h.  What is the source's port number?  Why do you think this port number was selected?

i.  What is the destination's port number?  Why do you think this port number was selected?

j.  What flags were set on the TCP header?  Explain the purpose of each flag.

i.  Note: flags were not covered in the lecture.  You will need to research the flags.

3.  In the GET payload, Wireshark tells you which frame number the response frame is.  Double-click the frame number.  This should put you at the HTTP/1.1 OK frame.

a.  Explain the purpose of the HTTP/1.1 OK frame.  In other words, what is happening at this point in the network capture?

b.  What are the source's IP address and port?

c.  What are the destination's IP address and port?

d.  Why do you think this information is different from the previous packet?

e.  How many TCP segments were needed to deliver the entire website to your screen?

f.  How large (in bytes) is the website?

g.  What type of server is the website is hosted on?

i.  Note: you may need to do a little research here.  The server does respond with its type of web server.

4.  Attempt to use the Wireshark filter to find the FIN flag sent from the webserver.

a.  What frame number was the FIN flag sent?

b.  Explain the purpose of the FIN flag.

5.  Clear all Wireshark filters.  This allows you to see all packets captured.  Do you see any TCP Retransmission packets?

a.  Chances are high that you do have a few of these packets.  What information can you gather regarding the purpose of this packet?  In other words, why did you send or receive these packets?

6.  Develop a small list of four or five other network protocols captured by Wireshark.  Provide a brief explanation of these protocols and explain why they are important in this particular capture.