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/).

What packet number is the GET packet?

134

What is the size of the entire GET frame?

494

What is the source's physical address?

192.168.0.18

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

That is my computer, well I know my address already but you can just do ipconfig on command prompt and it’s a local address.

What is the destination's physical address?

72.18.132.134

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

That’s the router address.

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?

TCP. Because a connection has to be established before sending data.

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

80

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

60792

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

Ack, is to acknowledge that there was a successful packet transferred. FIN, is to show that there is no more data from the sender.

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?

The http/1.1 fram is a connection that can be used multiple times to download image, scripts, etc. after the page has been delivered.

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

192.168.0.18 60792

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

72.18.132.134 80

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

Uh, its not different?

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

Lets say around 140

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

440

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

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?

557

b.  Explain the purpose of the FIN flag.

FIN, is to show that there is no more data from the sender.

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?

No idea, but there all between my computer and local connections. Im guessing they were dropped because of network congestion?

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.

IGMP: this is a communications protocol used to manage the membership of Internet Protocol multicast groups

UDP: uses a best-effort delivery system, similar to how first class and lower postal services of

ARP: is an Internet layer protocol that helps TCP/IP network components find other devices in the same broadcast domain.

DNS: makes it easier to identify a host by a domain name. A domain name uses words rather than numbers to identify Internet hosts.