B1 – LAB 4

WIRESHARK

Form groups of approximately 5 people and take a shot individually at those exercises. Communication is allowed and recommended in the groups; the more you are able to explain something, the more likely you are of having understood it.

1 – EXERCISE ONE

- Open “Exercise One.pcap”, you should see 26 packets listed
- What is the IP address of the client that initiates the conversation?
- Use the first two packets to identify the server that is going to be contacted. List the common name, and three IP addresses that can be used for the server.
- What is happening in frames 3, 4, and 5?
- What is happening in frames 6 and 7?
- Ignore frame eight. However, for your information, frame eight is used to manage flow control.
- What is happening in frames nine and ten? How are these two frames related?
- What happens in packet 11?
- After the initial set of packets is received, the client sends out a new request in packet 12. This occurs automatically without any action by the user. Why does this occur?
- What is occurring in packets 13 through 22?
- Explain what happens in packets 23 through 26.
- In one sentence describe what the user was doing

2 – EXERCISE TWO

- Open “Exercise Two.pcap”, you should see 176 packets listed
- In the first few packets, the client machine is looking up the common name (cname) of a web site to find its IP address. What is the cname of this web site? Give two IP addresses for this web site.
- How many packets/frames does it take to receive the web page (the answer to the first http get request only)?
- Does this web site use gzip to compress its data for sending? Does it write cookies? In order to answer these questions, look under the payload for the

reassembled packet that represents the web page. This will be the last packet from bullet point 3 above. Look to see if it has “Content-Encoding” set to gzip, and to see if it has a “Set-Cookie” to write a cookie.

- What is happening in packets 26 and 27? Does every component of a web page have to come from the same server?
- In packet 37 we see another DNS query, this time for us.i1.yimg.com. Why does the client need to ask for this IP address? Didn’t we just get this address in packet 26? (This is a trick question; carefully compare the two common names in packet 26 and 37.)
- In packet 42 we see a HTTP “GET”statement, and in packet 48 a new HTTP “Get” statement. Why didn’t the system need another DNS request before the second get statement? Click on packet 42 and look in the middle window. Expand the line titled “Hypertext Transfer Protocol” and read the “Host:” line. Compare that line to the “Host:” line for packet 48.
- Examine packet 139. It is one segment of a PDU that is reassembled with several other segments in packet 160.
  Look at packets 141, 142, and 143. Are these three packets also part of packet 160? What happens if a set of packets that are supposed to be reassembled do not arrive in a continuous stream or do not arrive in the proper order?
- Return to examine frames 141 and 142. Both of these are graphics (GIF files) from the same source IP address. How does the client know which graphic to match up to each get statement? Hint: Click on each and look in the middle window for the heading line that starts with “Transmission Control Protocol”. What difference do you see in the heading lines for the two files? Return to the original “GET” statements. Can you see the same difference in the “GET” statements?

3 – EXERCISE THREE

- Open “Exercise Three.pcap”, you should see 22 packets listed
- Compare the destination port in the TCP packet in frame 3 with the destination port in the TCP packet in frame 12. What difference do you see? What does this tell you about the difference in the two requests?

Row	www.yahoo.com frames	my.usf.com frames	Brief explanation
i	1-2	8-9	DNS Request to find the IP Address for common name & DNS Response
ii	3-5	10-12	Three-way handshake
iii	--	13-20	
iv	6	21	GET Request for web page
v	7	22	First packet from web server with web page content

- Explain what is happening in row “iii” above. Why are there no frames listed for yahoo in row “iii"?
- Look at the “Info” column on frame 6. It says: “GET / HTTP / 1.1. What is the corresponding Info field for the my.usf.com web request (frame 21)? Why doesn’t it read the same as in frame 6?