Wireshark Assignment

1. Exercise 1
   1. What is the IP address of the client that initiates the conversation?

**The IP address of the client is 131.247.95.216.**

* 1. 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.

**In packet 1 the server common name is www.lgoogle.com, and three IP address listed for this common name are 64.233.161.99, 64.233.161.104, 64.233.161.147.**

* 1. What is happening in frames 3, 4, and 5?

**In frame 3 and 4 the client is requesting a connection with the server, and in frame 5 the server is sending back an acknowledgment stating that the connection was successful.**

* 1. What is happening in frames 6 and 7?

**In frame 6 the client is requesting a webpage from the server. In frame 7 the server is sending an acknowledgement to the client.**

* 1. Ignore frame eight. However, for your information, frame eight is used to manage flow control.
  2. What is happening in frames nine and ten? How are these two frames related?

**In frame 9 the server is sending another acknowledgement to the client. In frame 10 the server is sending an HTML page to the client.**

* 1. What happens in packet 11?

**In packet 11 the client sends an acknowledgement to the server stating that the information exchanged was received.**

* 1. 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? See the first “hint” to the left.

**The server failed to send part of the previous packet to the client to the client automatically resent the request.**

* 1. What is occurring in packets 13 through 22?

**The client is sending an image for a logo to the client and they are both sending acknowledgements back and forth to make sure the entire image was transferred without any errors.**

* 1. Explain what happens in packets 23 through 26. See the second “hint” to the left.

**The client requests the logo for the webpage and the server sends an ACK. Then the server sends the logo to the client. When the client receives the file, it sends an ACK back to the server.**

* 1. In one sentence describe what the user was doing (Reading email? Accessing a web page? FTP? Other?).

**The client is accessing a webpage because they are requesting a logo that is seen in your browser's tabs.**

1. Exercise 2
   1. 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.

**CNAME = www.yahoo.com.akadns.com IP Addresses = 216.109.117.109, 216.109.117.110.**

* 1. How many packets/frames does it take to receive the web page (the answer to the first http get request only)?

**17 Packets.**

* 1. 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 question b 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.

**Yes, the website uses gzip to compress the data. The website also writes cookies. Both items are seen in the payload of the packet.**

* 1. What is happening in packets 26 and 27? Does every component of a web page have to come from the same server? See the Hint to the left.

**The client is making a query to the domain name service to make find out the correct IP address for the information being requested.**

* 1. 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.)

**The servers being looked up are using different common names. So even if they used the same IP address, the client would still need to see what the IP address of the server is.**

* 1. 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.

**The host has already been looked up previously for both packets. So, the client used the same IP that was used before.**

* 1. 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?

**Only packet 143 is part of packet 140. If the packets do not arrive in order, then the main packet is not affected.**

* 1. 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?

**Both files in frames 141 and 142 are similar and from the same source IP address. The client matches each statement from their “Stream Index”. Each of them has a different steam index.**

1. Exercise 3
   1. 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?

**The destination on frame 3 is sent to port 3, while the destination in frame 12 is port 443. Port 80 is generally used for non-secure transfers for webpages and such. Port 443 is used for secure transfers using SSL or TLS.**

The following table compares the two requests for web pages. For example, row i) shows that frames 1-2 and frames 8-9 represent the DNS lookups for each of the web requests.

|  |  |  |  |
| --- | --- | --- | --- |
| Row | www.yahoo.com  frames | my.usf.com  frames | Brief Explanation of Activity |
| i) | 1-2 | 8-9 | DNS Request to find 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. |

* 1. Explain what is happening in row “iii” above. Why are there no frames listed for yahoo in row “iii"?

**The DNS lookup has already taken place, so when the client makes another request to the same IP address there is no need for yahoo to lookup the address again.**

* 1. 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?

**Frame 21 is encrypted so the info section shows less information.**

1. Exercise 4
   1. Examine packet 228. With this packet, a new client is joining the network. What is the Layer 2 address of that client?

**MAC Address: 00:15:00:34:18:52**

* 1. Examine packet 228. What layer 2 flag fields are set?

**DS status, More Fragments, Retry, PWR MGT, More Data, Protected Flag, Protected flag, Order flag.**

* 1. Examine packet 728. What security protocol is requested for use after authentication takes place: WPA or TKIP?

**WPA**

* 1. Go back and examine packet 228. What is the purpose of including TKIP parameters in that frame?

**So that the receiver knows what protocol is being used.**