Exercise One

a) What is the IP address of the client that initiates the conversation?

`131.247.95.216`

b) 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.

The server is Google's. The common name is `www.l.google.com`; the addresses are `64.233.161.99`, `64.233.161.104`, and `64.233.161.147`.

c) What is happening in frames 3, 4, and 5?

The client and server are setting up a TCP connection. In frame 3, the client requests to start the connection. In frame 4, the server acknowledges the request, and in frame 5, the client acknowledges the acknowledgment.

d) What is happening in frames 6 and 7?

In frame 6, the client sends an HTTP request to GET the contents of `google.com`. In frame 7, the server acknowledges that request.

e) Ignore frame eight. However, for your information, frame eight is used to manage flow control.

f) What is happening in frames nine and ten? How are these two frames related?

In frame 9, the server assembles the requested data. In frame 10, the server sends that data via HTTP. They are related because the data sent in 10 has to be gathered and formatted beforehand; that gathering occurs in frame 9.

g) What happens in packet 11?

The client acknowledges the server's response.

h) 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.

Because the HTML page that the server sent back references a `logo.gif` file, so the client immediately requests that file to properly display the webpage.

i) What is occurring in packets 13 through 22?

On packets 13, 14, 16, 17, 18, and 20, the server sends the requested `logo.gif` file in chunks. On packets 15, 19, and 21, the client acknowledges those chunks. On packet 22, the server completes the transaction with a `HTTP 200 OK` message.

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

On packet 23, the client requests the webpage's icon (its `favicon.ico`). On packets 24 and 25, the server sends that icon and a `HTTP 200 OK` message. On packet 26, the client acknowledges the response.

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

The user was accessing `www.google.com`.

Exercise Two

a) 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.

The cname is `www.yahoo.akadns.net`. Two of its IPs are `216.109.117.106` and `216.109.117.109`.

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

Fifteen.

c) 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, it uses gzip. It also writes cookies, twice.

d) 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 looks up where `us.js2.yimg.com` is with a DNS query, and in 27 the server sends the IPs and cname where that resource is. So no, not every page component need be in the same server.

e) 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.)

No, the address requested in 26 was for `us.js2.yimg.com`, not `us.i1.yimg.com`.

f) 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.

For both packets, the host is the one that was requested in 37: `us.i1.yimg.com`.

g) 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?

Packet 143 is part of 160, yes. 141 and 142 are not part of 160; they respond to different requests.

If the packets do not arrive in order, TCP reassembles them in their order based on the sequence number, compared to the relative sequence number.

h) 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?

By looking at the stream index and packet number, and by sending it to its corresponding destination port.

Exercise Three

a) 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?

Frame 3 sends to port 80; 12 to port 443. That is, frame 3 requests via HTTP, and frame 12 via HTTPS.

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

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.

Row 'iii' is the HTTPS handshake between the client and `my.usf.com`. Since the connection to Yahoo is HTTP, no handshake is done with Yahoo, and thus no frames are listed for it either.

c) 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?

Since the connection to `my.usf.com` is HTTPS, it is encrypted, so the request's contents can't be shown. Instead, only an `Application Data` is shown.

Exercise Four

Row	Frames	Explanation
i	--	DNS request/response. Absent because DNS was likely cached in browser.

Row	Frames	Explanation
ii	1-18	HTTPS traffic. Likely from another browser tab.
iii	19-22	TCP handshake for this session.
iv	23-38	TLS handshake. Start of this HTTPS session with `os.ecci.ucr.ac.cr`.
v	39-41	HTTP request to server. Server response.
vi	42-81	HTTPS traffic with `os.ecci.ucr.ac.cr`.,

For details see `WS-Ex-04.pcap` in this directory.