1) Exercise One

a) The IP address of the client that initiates the conversation is *131.247.95.216*

b) The common name is: *www.l.google.com* , and three IP addresses that can be used for the server are: *64.233.161.99* , *64.233.161.104* , *64.233.161.147*

c) In frames 3, 4, and 5, there are a *Three-way Handshake*

d) In frames 6 and 7, the client is sending a HTTP request to the server and it got an ACK from the server.

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

f) In frames nine and ten, the HTTP response with a lot of data split to another TCP segment, which is in frame nine. And the HTTP response itself is in frame ten.

g) In packet 11, the client sends an ACK to response the HTTP request from the server.

h) The reason why this occur without any action is the previous web page which is received by the client tell it to receive an image from the server (which is /intl/en/images/logo.gif).

i) In packets 13 through 22, the server sends the image to the client by separate segments and the client tells the server that it got these segments by some ACKs.

j) Like it is in packet 12 to 22, the server sends the favicon.ico to the client, and the client tells the server that it got the file successfully by ACK.

2) Exercise Two

a) The common name of this web site is: *www.yahoo.akadns.net* , here are 2 IP address for this web site: *216.109.117.106* , *216.198.117.109*

b) It takes 17 packets/frames to receive the web page.

c) This web site use gzip to compress its data for sending. Yes, it does write cookies.

d) In packets 26 and 27, client gets connect to another server calls *us.js2.yimg.com*. Not every component of a web page have to come from the same server.

e) The reason why the client need to ask for this IP address is it needs another JavaScript file. We did not get this address in packet 26, the common names are different. And the A record domains they specify are different as well.

f) The reason why the system does not need another DNS request before the second get statement is the 2 files (dsf_1.1.js and y3.gif) are all from the same server (or Host).

g) Packet 141,142 are not part of packet 160. 143 is a part of packet 160. It will not get an ACK from the client.

h) On one hand, the 2 packets have their own “Request in Frame” statement. On the other hand, they got different “Src Port”.

3) Exercise Three

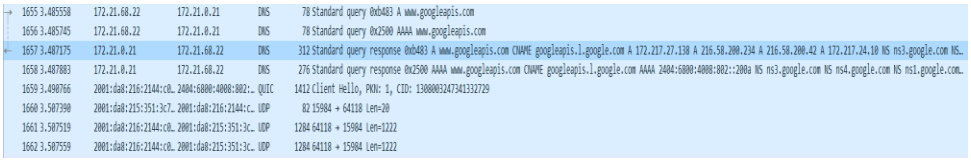
a) In frame 3, the destination port is 80. In frame 12, the destination port is 443. The first one is a HTTP request, the second one is a HTTPS request.

b) In row “iii”, the SSL/TLS is built on the TCP connection, but for yahoo, it does not use HTTPS. So no Security Layer.

c) The Secure Sockets Layer. The reason it does not read the same as in frame 6 is because it is based on a secure socket layer. So the information should be save.

4) Exercise Four

a) Question4_1.pcapng is an example by visiting google. The environment here is using ipv4+ipv6. So there are 2 kinds of IP address.



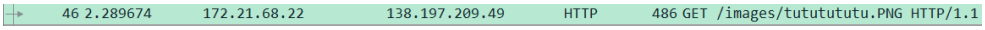
What is the IP address of the client that initiates the conversation?

The IP address of the client that initiates the conversation is 172.21.68.22.

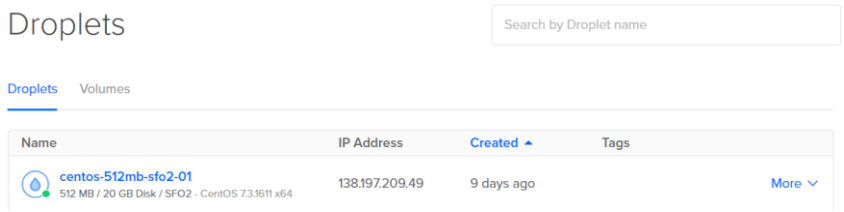
Use the first two packets to identify the server that is going to be contacted. List the common name, and three IP addresses that can be used for the server.

The common name is: googleapis.l.google.com , and three IP addresses that can be used for the server are: 172.217.27.138 , 172.217.24.10 , 216.58.200.234 .

b) Question4_2.pcapng is an example by visiting my own website zhangqinyuan.xzy

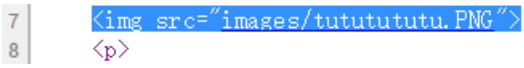


The destination here is my VPS:



After the initial set of packets is received, the client sends out a new request in packet 46. This occurs automatically without any action by the user. Why does this occur?

That is because in my file index.html, there is a line says:



So, the client will automatically ask the server to send the image.