Name: Ammaar Ahmad
Roll no :1801CS08
CS-359 Assignment-1

Problem1: Capture Filters:

1.) To Capture TCP traffic to/from Facebook, during the time when you log in to your Facebook account

First we will try to find www.facebook.com 's IP address
>Run dig www.facebook.com in terminal
After doing that I got IP address as 31.13.79.35

Capture Filter : tcp and host 31.13.79.35

Total number of packets captured : 1933

2.)To Capture all HTTP traffic to/from Facebook, when you log in to your Facebook account.

We will apply display filter to the previously captured packets to capture all HTTP traffic Display filter : ssl
No of packets captured : 1025 (53.0%)

Or

Display filter : tcp.port==443

No of packets captured : 1933 (100%)

3.)To capture all traffic from youtube while playing a popular video in it

First we will try to find www.youtube.com 's IP address
>Run ping www.youtube.com in terminal
After doing that I got IP address as 142.250.67.238

Capture Filter : host 142.250.67.238

Total no of packets capture : 237

After you run Wireshark with the above capture filters and collect the data, do the following:

1.)To capture TCP packets When the flags SYN, PSH, and RST set.While logging into my facebook account

Display Filter	No of packets	Fraction in %
tcp.flags.syn==1	2	0.1%
tcp.flags.push==1	910	47.1%
tcp.flags.reset==1	0	0.0%

2.) To capture Facebook's HTTPS packets which are sent vs received in machine

To get Machine IP address: ifconfig

My machine IP address as 192.168.0.105

	sent	received
Display filter	tcp.port==443 and ip.src==192.168.0.105	tcp.port==443 and ip.dst==192.168.0.105
No of packets	955	978
Fraction	49.4%	50.6%

Now we will capture Youtube's packets (sent vs received)

	sent	received
Display filter	ip.src==192.168.0.105	ip.dst==192.168.0.105
No of packets	89	148
Fraction	37.55%	62.45%

Problem2:- Captured Data Analysis

a. Count how many TCP packets you received from / sent to Facebook or YouTube, and how many of each were also HTTP packets.

b. Determine if any TCP packets with SYN or PSH flags set were sent from your host or received from Facebook/Youtube.

c. Go flag-by-flag and count how many packets have tcp.flags.push set, then how many have tcp.flags.syn set, and finally, how many have tcp.flags.reset set.

To capture tcp : Display filter is tcp

To capture https : Display filter is tcp.port==443

Protocol	facebook	Youtube
TCP	1933	237
HTTPS	1933	237

Display filter to capture when SYN flag is set : tcp.flags.syn==1
Display filter to capture when PUSH flag is set : tcp.flags.push==1
Display filter to capture when RESET flag is set : tcp.flags.reset==1

Flag which is being set	Facebook	Youtube
SYN	2(0.1%)	0 (0%)
PUSH	910(47.1%)	136 (57.38%)
RESET	0(0.0%)	0(0%)