tcpdump commands used:

(1) tcpdump -n -i en0 tcp and host sbunetsyslabs.com -w http_1080.pcap
(2) tcpdump -n -i en0 tcp and host sbunetsyslabs.com -w http_1081.pcap
(3) tcpdump -n -i en0 tcp and host sbunetsyslabs.com -w http_1082.pcap

Code high level view:

The methods used in 'analysis_pcap_http.py' are similar as in the previous 'analysis_pcap_tcp.py'. Some methods are redesigned for answering the questions. In most of the new methods, server port number is added as argument. The main idea is as flows. Firstly, for each pcap file, store packet and their timestamp pairs in a 'bufList'. Secondly, identify client port connections with each server port, store each connection's packets as a flow in a directory. Client port is the key, value is a packet list. Lastly, take required information from the directories of specific client/server ports to calculate answers. Code and detailed comments are included in part C folder.