Part C Report:

The analysis_pcap_http program is used for finding the http versions, printing the requests and comparing the various HTTP versions from a pcapfile. I created a packet from existing TCP packet using only the data that is required for the analysis. The packet format cr3eated by me includes source port, destination port, syn, ack, fin flags, source ip address, destination ip address, sequence number, acknowledgement number windows size. The program creates three separate lists based on number of flows which makes the analysis easier. After that I check for the handshakes done and calculate number of flows. The program also prints the sequence number, acknowledgement numbers and window size for each flow. The program calculates the Http version depending on number of connections and compares the different metrices required to load a site for different HTTP versions. The filters used in wireshark are the as follows: http.request.method == GET and http.request.method == GET and tcp.port==63478. The code to answer the questions below is attached in the folder.

```
HTTP flow for: 50520

GET Requests ('GET ', '130.245.70.215', '34.193.77.105', '847d7fda', 'bfb9ee43')

Http Responses

('HTTP', '34.193.77.105', '130.245.70.215', 'bfb9ee43', '847d8171')

('34.193.77.105', '130.245.70.215', 'bfb9f17c', '847d8171')

('34.193.77.105', '130.245.70.215', 'bfb9f17d', '847d8172')

('HTTP', '34.193.77.105', '130.245.70.215', 'bfb9ee43', '847d8171')

('34.193.77.105', '130.245.70.215', 'bfb9f17c', '847d8171')

('34.193.77.105', '130.245.70.215', 'bfb9f17d', '847d8172')

('34.193.77.105', '130.245.70.215', 'bfb9f17c', '847d8171')

('34.193.77.105', '130.245.70.215', 'bfb9f17d', '847d8172')

('34.193.77.105', '130.245.70.215', 'bfb9f17d', '847d8172')
```

2.

Since the payload is encoded in both the files we need to think to of other methods to calculate the versions. For this we calculate the number of flows. The number of flows in HTTP version 2.0 is 1 and other the other file will then be that of HTTP 1.1

for File http_1081

HTTP version 1.1

for File http_1082

HTTP version 2.0

3.

Time Required to load Site: 0.518024921417 packets 2015 raw bytes 2193708

Time Required to load Site: 0.398512840271 packets 1835 raw bytes 2183805

Time Required to load Site: 0.428415060043 packets 1767 raw bytes 2173955

Depending on the above results we conclude the following:

1. Site took less time to load under HTTP version 1.1 due to fast due to due to compressed packet format.
2. It took most time to load under HTTP version 1.0 due to huge packet and lack of pipelining and multiplexing.
3. The HTTP 1.0 sent the most number of packets due to multiple connections having bulkier packets whereas HTTP 2.0 sent less number of packets due single connection and compressed packets.