**Homework 2: HTTP, TCP, and Wireshark**

**Part C HTTP Analysis task:**

1. Filter used in Wireshark: host [www.sbunetsyslabs.com](http://www.sbunetsyslabs.com)
2. **High level view of the analysis\_pcap\_http code:**

Like TCP, we maintain a class object for IP headers, TCP headers, and HTTP headers. We read each of the .pcap files and store data in these header objects. Then we followed the below steps:

Reassemble packets in http\_1080.pcap file.

Got the protocol for each of the .pcap files.

Then the total time, total sent bytes, and count of packets for each HTTP protocol.

1. **Reassemble each unique HTTP Request/Response for http\_1080.pcap:** We check for each socks packet, whether it is request packet or response packet by checking 4 bytes at index (dataoffset + 34) value. If it is either a GET or POST request, we mark it as request packet. If it is HTTP, we mark it as response packet. We reassemble for each port in this way. We pick the source port, destination port, source IP address, destination IP address, sequence number, and acknowledgement number from each packet into the header objects.

HTTP REQ/RESP 1 <Packet Type, Source, Destination, Seq Number, Ack Number>

REQUEST 172.24.20.24:37213 34.193.77.105:1080 1016332660 2652609954

RESPONSE 172.24.20.24:37213 34.193.77.105:1080 2652609954 1016333044

RESPONSE 172.24.20.24:37213 34.193.77.105:1080 2652611340 1016333044

RESPONSE 172.24.20.24:37213 34.193.77.105:1080 2652612726 1016333044

RESPONSE 172.24.20.24:37213 34.193.77.105:1080 2652614112 1016333044

RESPONSE 172.24.20.24:37213 34.193.77.105:1080 2652615498 1016333044

RESPONSE 172.24.20.24:37213 34.193.77.105:1080 2652616884 1016333044

RESPONSE 172.24.20.24:37213 34.193.77.105:1080 2652618270 1016333044

1. **Identify HTTP Protocol:** If there is only one TCP flow/ connection, then it is HTTPS 2. If there are more than one TCP connections but less than 6, and each TCP connection suffice more than one requests, it is HTTPS 1.1. If there a TCP connection for every request, it is HTTP 1.

For http\_1080.pcap: Protocol is HTTP 1

For tcp\_1081.pcap: Protocol is HTTP 1.1

For tcp\_1082.pcap: Protocol is HTTP 2

1. Load Time:

HTTP 1: 0.78 sec

HTTP 1.1: 5.87 sec

HTTP 2: 5.76 sec

Observation is, HTTPS 1.1 and HTTPS 2 in contrast to expectation took more time. The reason being in these protocol, there is a delay or wait time at sender end for FIN packet. Fastest is HTTP 1 and slowest is HTTP 1.1.

HTTP 1

Total number of packets: 429

Total number of bytes: 29922 bytes

HTTPS 1.1

Total number of packets: 458

Total number of bytes: 35444 bytes

HTTPS 2

Total number of packets: 362

Total number of bytes: 22818 bytes

The total bytes sent and number of packets sent in case of HTTPS 2is least. While HTTPS 1.1 allowed us to send multiple requests in single TCP connection, the total bytes sent and total packets sent is highest. There are total 6 connections made in this protocol. In case of HTTP 1, there are total 18 TCP connections made and almost same number of packets are sent as in HTTP 1.1, but number of bytes sent is less.