Generating pcap files

```
# cd tcp-packet-analysis/
# sudo tcpdump -n port 1080 -w http_1080.pcap
# sudo tcpdump -n port 1081 -w tcp_1081.pcap
# sudo tcpdump -n port 1082 -w tcp_1082.pcap
```

1 Reassembling http/1.0 packets

17 connections are established here, with each connection requesting some object in a request packet and receiving that object in the response packet.

For pipelined HTTP, reassembling request and response is not that straightforward. Pipelined HTTPs maintain session ids to map responses to the request.
However, the non-pipelined versions are fairly straightforward to reassemble. All responses belong to the latest request before them. Request and responses in non-pipelined versions of HTTP are sequential.

CONN 1

Sr.No	PACKET-TYPE	SRC	DST	SEQ-NUM	ACK-NUM
1	request	172.24.16.236:50640	34.193.77.105:1080	3964326278	479685728
2	response	34.193.77.105:1080	172.24.16.236:50640	479685728	3964326705

CONN 2

Sr.No	PACKET-TYPE	SRC	DST	SEQ-NUM	ACK-NUM
1	request	172.24.16.236:50641	34.193.77.105:1080	3710195459	1491800523
2	response	34.193.77.105:1080	172.24.16.236:50641	1491800523	3710195843

CONN 3

Sr.No	PACKET-TYPE	SRC	DST	SEQ-NUM	ACK-NUM
1	request	172.24.16.236:50642	34.193.77.105:1080	392705952	438332120
2	response	34.193.77.105:1080	172.24.16.236:50642	438332120	392706297

CONN 4

Sr.No	PACKET-TYPE	SRC	DST	SEQ-NUM	ACK-NUM
1	request	172.24.16.236:50643	34.193.77.105:1080	1683238309	2156415119
2	response	34.193.77.105:1080	172.24.16.236:50643	2156415119	1683238694

CONN 5

Sr.No	PACKET-TYPE	SRC	DST	SEQ-NUM	ACK-NUM
1	request	172.24.16.236:50644	34.193.77.105:1080	2523063669	1934081015
2	response	34.193.77.105:1080	172.24.16.236:50644	1934081015	2523064054

CONN 6

Sr.No	PACKET-TYPE	SRC	DST	SEQ-NUM	ACK-NUM
1	request	172.24.16.236:50645	34.193.77.105:1080	3886097707	1486465345
2	response	34.193.77.105:1080	172.24.16.236:50645	1486465345	3886098096

CONN 7

Sr.No	PACKET-TYPE	SRC	DST	SEQ-NUM	ACK-NUM
1	request	172.24.16.236:50646	34.193.77.105:1080	1892219783	3373545629
2	response	34.193.77.105:1080	172.24.16.236:50646	3373545629	1892220178

CONN 8

Sr.No	PACKET-TYPE	SRC	DST	SEQ-NUM	ACK-NUM
1	request	172.24.16.236:50647	34.193.77.105:1080	803109682	817422346
2	response	34.193.77.105:1080	172.24.16.236:50647	817422346	803110075

CONN 9

Sr.No	PACKET-TYPE	SRC	DST	SEQ-NUM	ACK-NUM
1	request	172.24.16.236:50648	34.193.77.105:1080	1837964181	2481599123
2	response	34.193.77.105:1080	172.24.16.236:50648	2481599123	1837964571

CONN 10

Sr.No	PACKET-TYPE	SRC	DST	SEQ-NUM	ACK-NUM
1	request	172.24.16.236:50649	34.193.77.105:1080	2365504913	3806655260
2	response	34.193.77.105:1080	172.24.16.236:50649	3806655260	2365505301

CONN 11

Sr.No	PACKET-TYPE	SRC	DST	SEQ-NUM	ACK-NUM
1	request	172.24.16.236:50650	34.193.77.105:1080	1015804995	3174536032
2	response	34.193.77.105:1080	172.24.16.236:50650	3174536032	1015805385

CONN 12

Sr.No	PACKET-TYPE	SRC	DST	SEQ-NUM	ACK-NUM
1	request	172.24.16.236:50652	34.193.77.105:1080	120788846	1270312596
2	response	34.193.77.105:1080	172.24.16.236:50652	1270312596	120789234

CONN 13

Sr.No	PACKET-TYPE	SRC	DST	SEQ-NUM	ACK-NUM
1	request	172.24.16.236:50651	34.193.77.105:1080	879721040	289605232
2	response	34.193.77.105:1080	172.24.16.236:50651	289605232	879721429

CONN 14

Sr.No	PACKET-TYPE	SRC	DST	SEQ-NUM	ACK-NUM
1	request	172.24.16.236:50653	34.193.77.105:1080	1561218073	1054187706
2	response	34.193.77.105:1080	172.24.16.236:50653	1054187706	1561218463

CONN 15					
Sr.No	PACKET-TYPE	SRC	DST	SEQ-NUM	ACK-NUM
1	request	172.24.16.236:50654	34.193.77.105:1080	277396174	4291996737
2	response	34.193.77.105:1080	172.24.16.236:50654	4291996737	277396562

CONN 16					
Sr.No	PACKET-TYPE	SRC	DST	SEQ-NUM	ACK-NUM
1	request	172.24.16.236:50655	34.193.77.105:1080	127211390	1839512486
2	response	34.193.77.105:1080	172.24.16.236:50655	1839512486	127211775

CONN 17					
Sr.No	PACKET-TYPE	SRC	DST	SEQ-NUM	ACK-NUM
1	request	172.24.16.236:50656	34.193.77.105:1080	4279052499	3087896382
2	response	34.193.77.105:1080	172.24.16.236:50656	3087896382	4279052884

2 Identifying the http version

For the first file '*http_1080.pcap*', there are 17 connections with each connection having one request and one response. Also, the program is able to parse the http content since it is not encrypted. Thus, the server uses http/1.0 on port 1080.

For the second file '*tcp_1081.pcap*', there are 6 connections, but the program is not able to parse the http content associated with each of these connections. Thus, we can conclude that http/1.1 is used by the server on port 1081.

For the third file '*tcp_1082.pcap*', there are 2 connections established and again the program is not able to parse the http content associated with each of these connections. Thus, we can conclude that http/2.0 is used by the server on port 1081.

```
# of connections in HTTP 1.1 file: 6
# of connections in HTTP 2.0 file: 2
```

3 Analysing performance between the three http versions

Fastest protocol for this pcap file – HTTP/1.0
Slowest protocol for this pcap file – HTTP/1.1

Protocol with highest number of packets sent – HTTP/1.1
Protocol with least number of packets sent – HTTP/2.0

```
# of connections in HTTP 1.1 file: 6
# of connections in HTTP 2.0 file: 2
```

HTTP VERSION ANALYSIS			
HTTP-VERSION	# CONNECTIONS	# PACKETS SENT	TIME TAKEN
HTTP 1.0	17	2566	1.2186 ms
HTTP 1.1	6	2664	1.5037 ms
HTTP 2	2	2111	1.2435 ms