**Wireshark Assignment**

Name: **Mohammed Rushad**

Roll Number: **181CO232**

**Question 1:**

Filter: ip.addr == 192.168.144.120 and dns

We interact with the following sites when interacting with twitter

twitter.com

api.twitter.com

tpop-api.twitter.com

ns1.p26.dynect.net

abs.twimg.com

pbs.twimg.com

cs510.wpc.edgecastcdn.net

video.twimg.com

pbs-ac.twimg.com

pbs.twimg.akadns.net

pbs.twimg.com.akamaized.net

cs296.wpc.edgecastcdn.net

cs2-wpc.apr-8315.edgecastcdn.net

**a)** Capture filter: arp src 192.168.144.123

Approx. 8 packets / minute

**b)** Capture filter: arp dst 192.168.144.123

Approx. 0 packets / minute

**Question 2:**

1. 192.168.144.123
2. 192.168.144.1
3. DNS
4. 104.244.42.193
5. DNS uses UDP, can also use TCP
6. Port 53
7. Some ephemeral ports used on my pc by host initiating dns query: 62712, 56627, 60437
8. c8:58:c0:29:da:06
9. 76:83:c2:3c:b7:ee
10. Approx. time: 0.03 seconds
11. twitter.com
12. HTTP/1.1
13. udpdstport==53, filters all packets with destination port 53, using the default dns port using udp protocol.

Results have packets passing through 192.168.144.1, port 53 to access websites related to twitter.com

1. A) 100% frames are ethernet frames.

B) UDP (16.7%) and TCP (78.9%), TCP is more.

15.) A) TCP: 396 packets / second, around the 10 second mark.

B.) UDP: 36 packets / second, around the 6 second mark.

C.) HTTP: 41216 bits/ second, around the 10 second mark.

