Wireshark Assignment

Akshat Nambiar - 181C0204

# Question 1:

Display Filter: ip.addr = 192.168.1.23 and dns

The following sites were interacted with while we open twitter:

www.twitter.com

api.twitter.com

abs.twimg.com

pbs.twimg.com

pbs-ak.twimg.com

pbs.twimg.akadns.net

pbs.twimg.com.akamaized.net

pbs.twimg.eip.akadns.net

video.twimg.com

video-ak.twimg.com

video.twimg.akadns.net

video.twimg.com.akamaized.net

video.twimg.eip.akadns.net

ns1.p26.dynect.net

tpop-api.twitter.com

abs-zero.twimg.com

t.co

cs296.wp.edgecastcdn.net

1. Capture filter: arp src 192.168.1.23: Approx. 3 packets / minute
2. Capture filter: arp dst 192.168.1.23 :Approx. 6 packets / minute

# Question 2:

1. 192.168.1.23
2. 192.168.1.1
3. DNS
4. 23.207.75.20
5. DNS uses UDP, but can also use TCP
6. Port 53
7. Some ephemeral ports used by my PC are: 59202, 51216, 57316
8. 40:9f:38:d8:ac:bf
9. 10:50:72:24:b0:d0
10. Approximately 0.03 seconds
11. Website: http://www.goal.com/en/
12. HTTP/1.1
13. Returns UDP packets that have Port 53 as the destination. Packets pass through 192.168.1.1 Port 53 to interact with http://www.goal.com/en/.
14. Ethernet Frames = 100%, Transport Layer Protocols Present: UDP (30.3%) and TCP (68.7%)
    1. Highest number of TCP packets/sec : 424 packets/sec, around the 6sec mark.
    2. Highest number of UDP packets/sec : 168 packets/sec, around the 5sec mark.
    3. Highest number of HTTP bits/sec : 2896 bits/sec, around the 3sec mark.