Wireshark Exercise 1

Submitted by : K Krishna Swaroop 181CO125

Answer for Qn1)

Required filter is: “ip.addr ==192.168.1.12”

1a) Required filter is: “eth.src == 06:03:67:3c:a5:29 and arp”

On an average, ARP packets sent by my machine is 1 packet per 41.4 seconds.

1b) Required filter is: “eth.dst == 06:03:67:3c:a5:29 and arp”

On an average, ARP packets received by my machine is 1 packet per 41.4 seconds and is received from 192.168.1.12

Answer for Qn2)

Disclaimer : As no capture file named ‘http.cap’ was provided, the questions have been answered w.r.t capture file ‘Ans 2.pcapng’ or any other general case scenario.

2.1) User IP address : 192.168.1.12

2.2) N/A - Router not specified.

2.3) DNS protocol

2.4) IP Address : 142.250.76.78 (use http as filter in wireshark)

2.5) UDP is used by DNS

2.6) Port 53

2.7) Source port : 62210,, Destination port : 53 (use udp as filter)

2.8) 00:1f:e6:21:a0:98

2.9) N/A

2.10) 5 seconds //Find from tcp data

2.11) website – ‘twitter.com’

2.12) Version 1.1

2.13) Query means : UDP packet with destination port being 53. Result included all DNS packets sent and received.

2.14 A) 100%

2.14 B) UDP and TCP were used. TCP made most of the traffic. UDP made 31.9% and TCP made 68%

2.15 A) 1750 packets/s at t = 24s

2.15 B) 270 packets/s at t = 3s

2.15 C) 2500 HTTP Bits/s at t = 10s