

## Roozah Khan

### Questions

- 1) What is your IP address just by looking at Wireshark? (Do the best you can)  
**My IP address is 192.168.1.153**
- 2) For the websites that you visited, what are the IP addresses of those websites?  
**The IP address for Netflix is 107.23.224.10 and for the website DSW the IP Address is 18.214.247.11. There were a lot of IP addresses, but these are the main ones that came up and the destination was my IP address.**
- 3) What protocols do you see in those web surfing sessions?  
**I see the main ones are TCP and UDP and HTTP**
- 4) Can you find the 3-way handshake for when you entered a website into your browser? (\*HINT: Look in the "Info" column for "[SYN] and [SYN ACK]" messages!!!). Once you find it, within a few messages after the handshake, you should see a "GET" message in that "Info" column...What is the text of that "GET" message?  
**I couldn't find the GET message for Netflix or DSW but for the quizlet website I did find it and it was GET**  
**//ME4wTKADAgEAMEUwQzBBMAkGBSsOAwIaBQAEFLYIDV9sa3brE%2BQ4pfhmC6hSMzROBBRAwr0njsw0gzCiM9f7bLPwtCyAzgIleoxFsh16Kyg%3D HTTP/1.1**

### Ping

- 1) What is the protocol of your ping requests? (\*HINT: Look in the protocol column)  
**It is ICMP**
- 2) For the websites that you visited, what is its corresponding IP address? (\*HINT: Think of how a website name is translated to its IP address. You may see another protocol involved in the transaction).  
  
**[www.quizlet.com](http://www.quizlet.com) IP ADDRESS: 104.16.18.221**  
**[www.youtube.com](http://www.youtube.com) IP ADDRESS: 172.217.11.14**
- 3) What messages do you see about ping requests/responses (\*HINT: Look in the "Info" column for "Echo")  
**I see "Echo (ping) request id=0xbe0f, seq=10/2560, ttl=64 (reply in 149)" and so on for the replies as well for the websites I pinged.**

### Traceroute

- 1) What is the protocol of your trace requests? (\*HINT: Look in the protocol column)  
**It is ICMP.**
- 2) For the websites that you visited, what is its corresponding IP address? (\*HINT: Think of how a website name is translated to its IP address. You may see another protocol involved in the transaction).  
  
**[www.dsw.com](http://www.dsw.com) 96.6.42.234**  
**[www.quizlet.com](http://www.quizlet.com) 104.16.16.221**