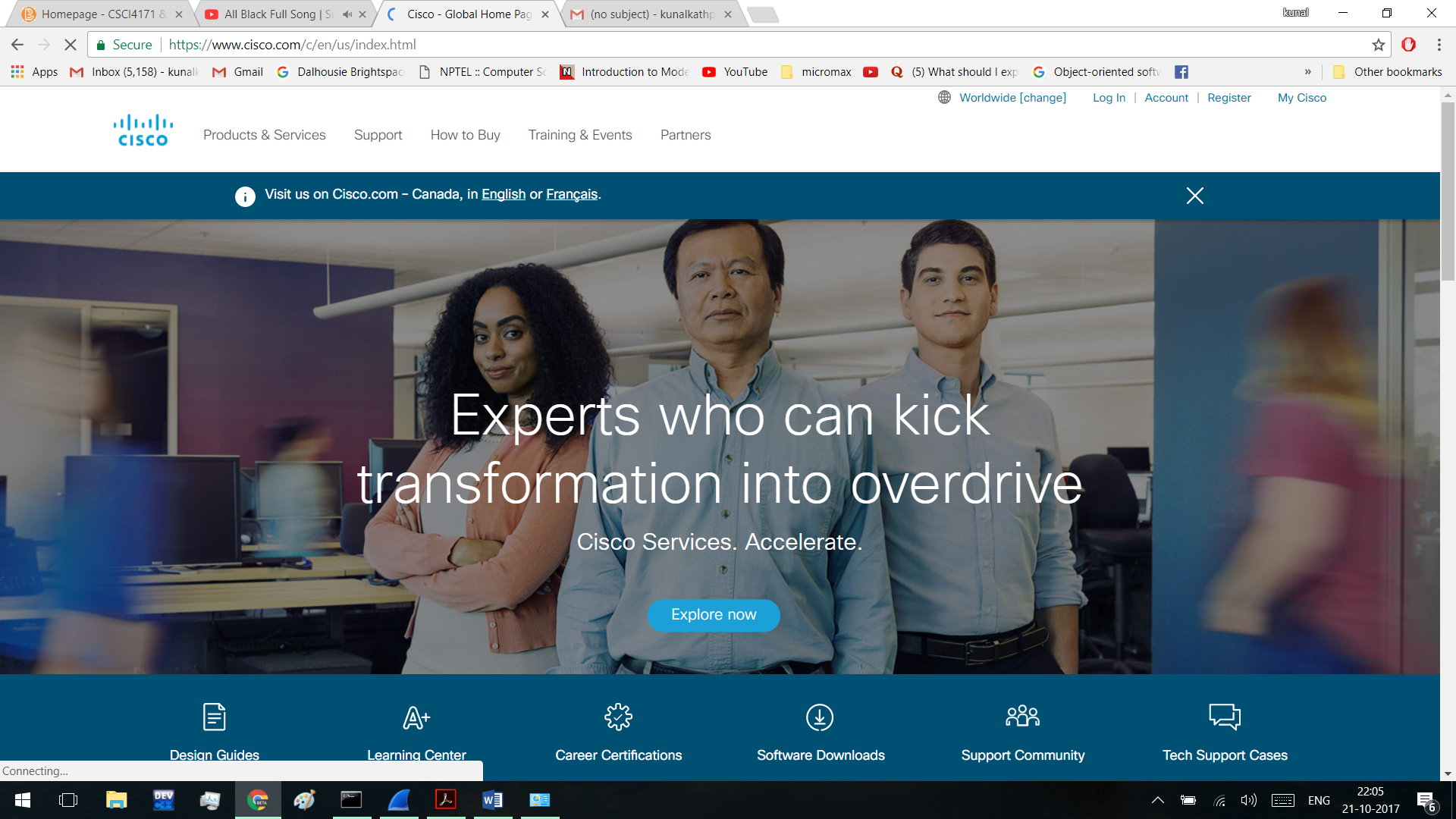
**Question 1**

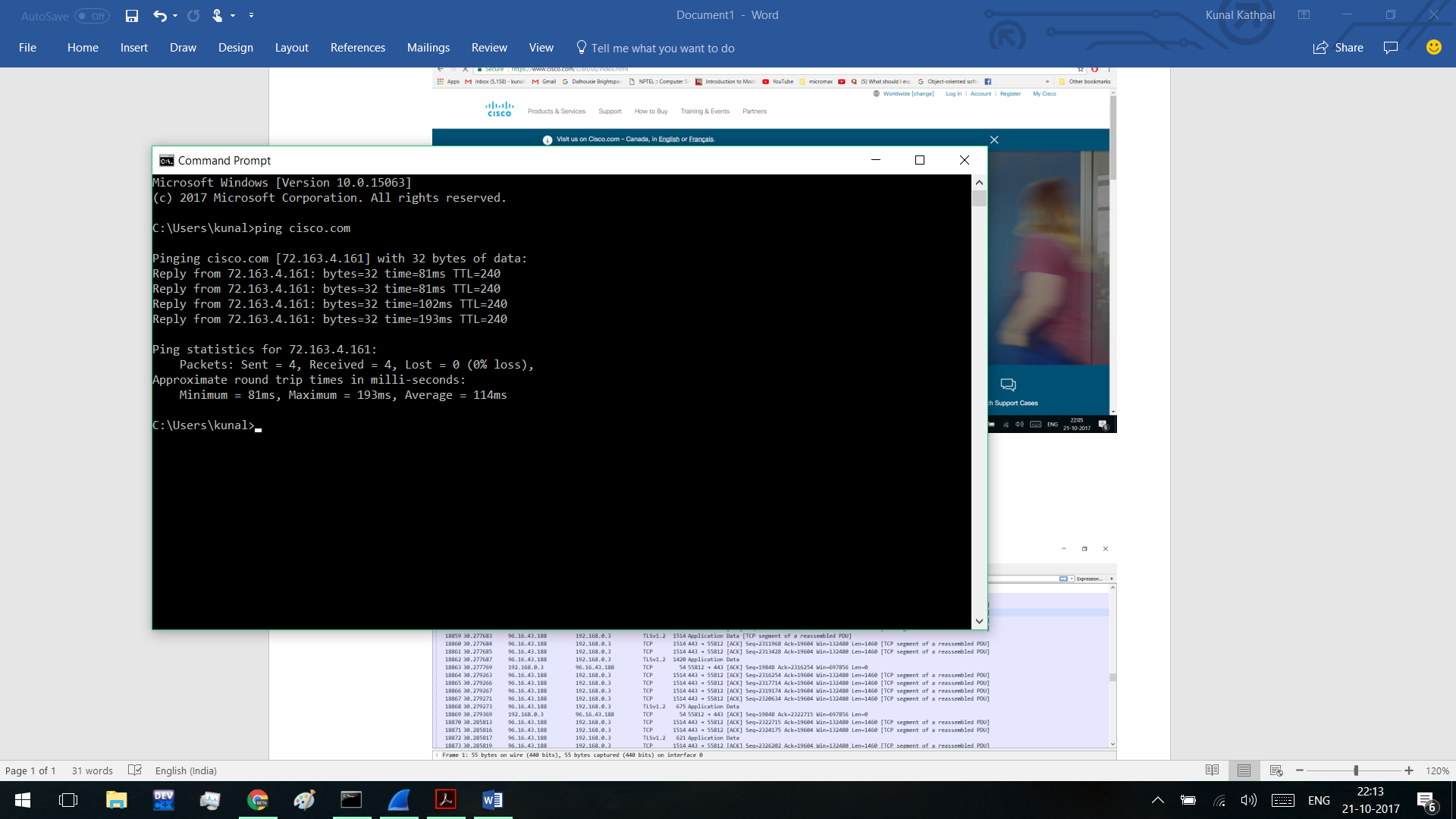
a.

* Wire shark is a open source computer network traffic monitor
* It is used to analyse and sniff packets
* Usable on multiple platforms
* Wire shark is roburst
* It’s free of cost

b. First, we will connect to a website i.e. cisco.com

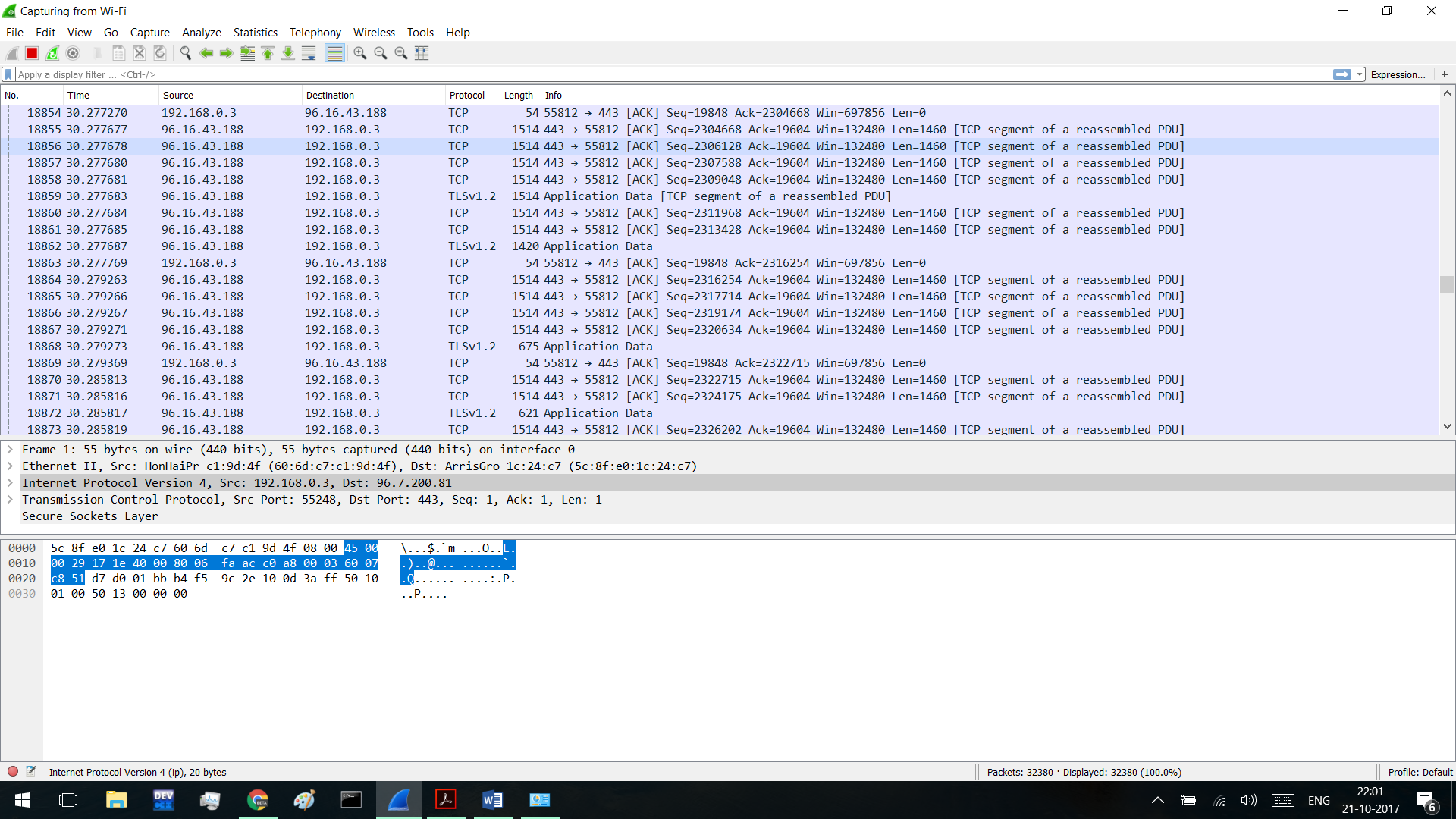


Then we will open CMD and ping cisco.com using the ping command.

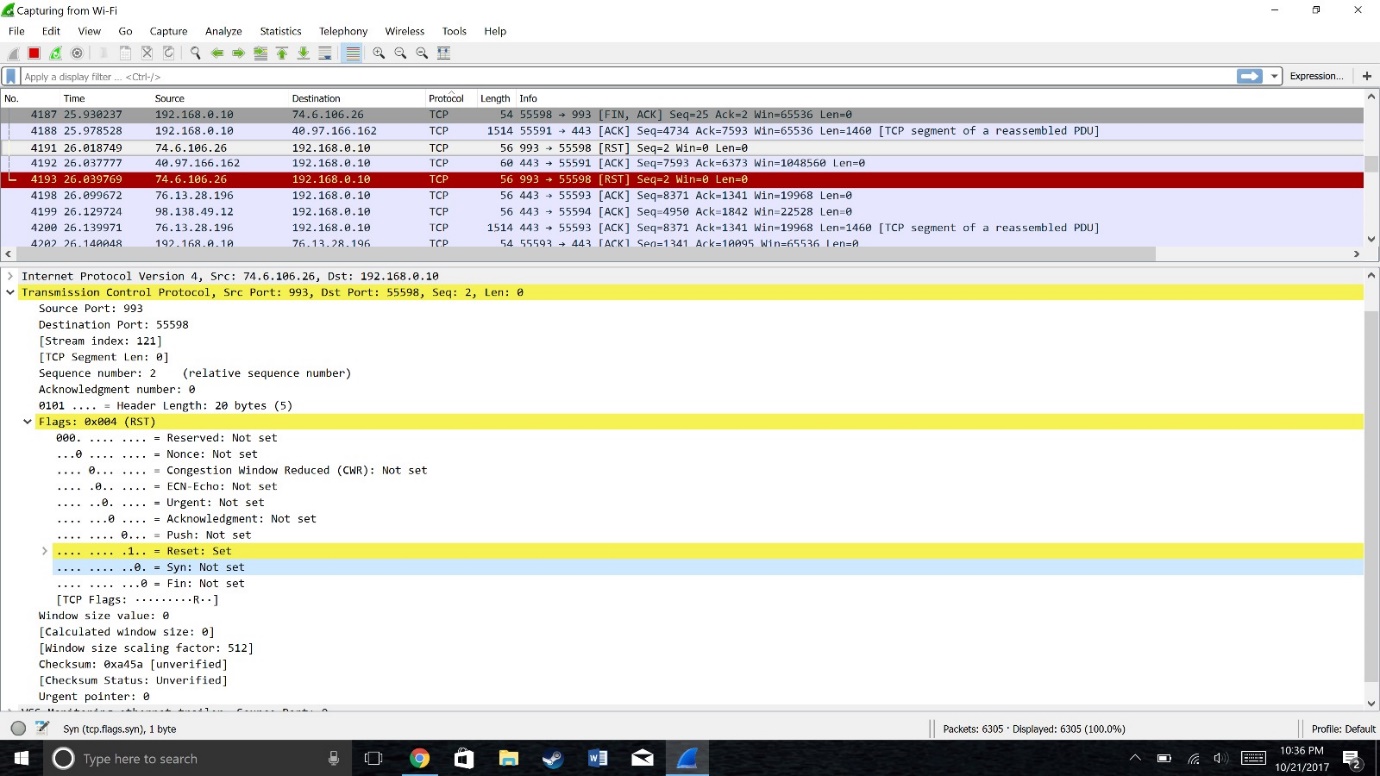


c. The figure below shoes packets being received from 96.16.43.188

The IP Address of my PC is 192.168.0.10 and the figure shows packets been received from cisco.com whose IP address is 72.163.4.161.



TCP



Source code is 993

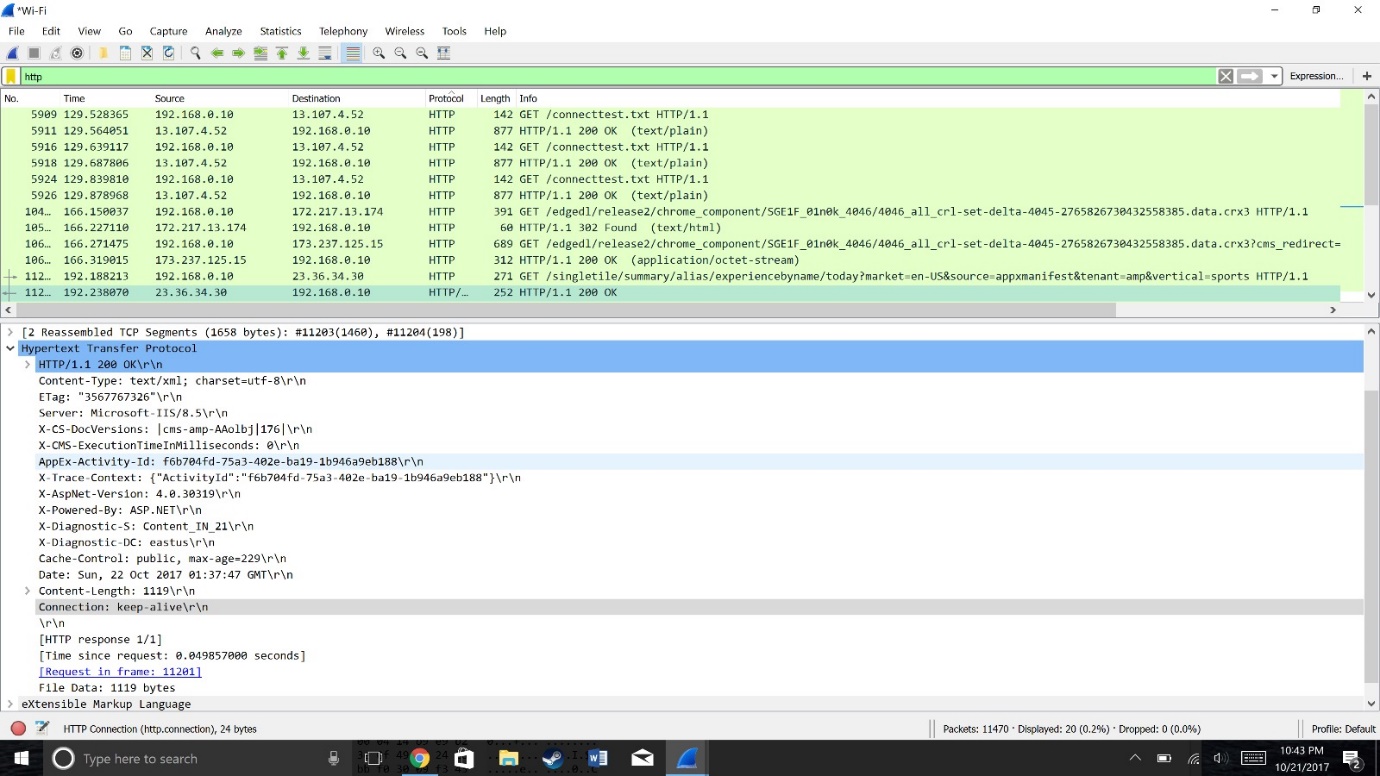
Destination port is 55598

Sequence number is 2

I observed Reset flag is SET and SYN flag NOTSET

Checksum status is verified

**HTTP**

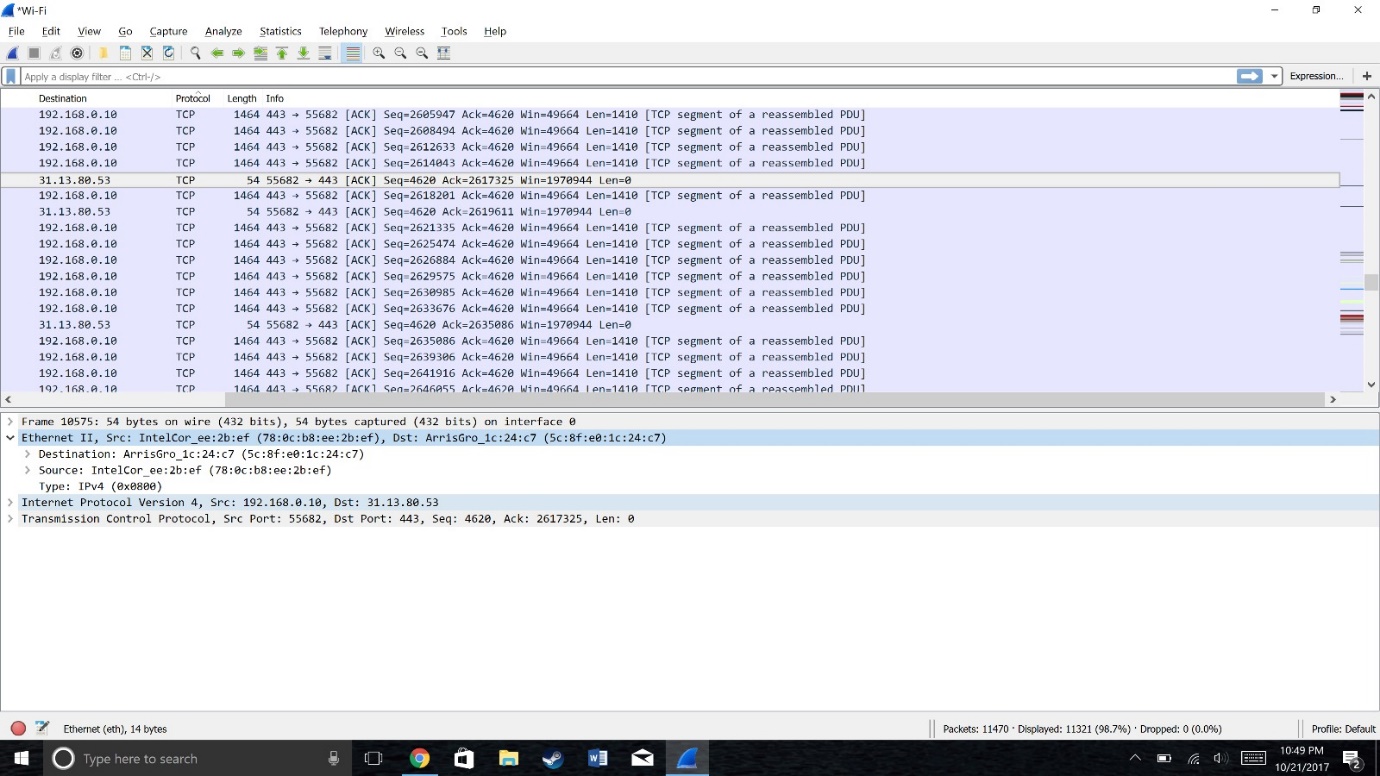


Content- type : test/xml

Charset is utf-8\r\n

Cache control is public and the length of the of content is 1119

**DATA LINK LAYER**



Moving to the Ethernet layer , we can see that it is pretty simple. It contains a destination address and a source address. The data link layer is relatively simple in that it is only concerned with getting a frame to the next adjacent node on the physical medium

d.

* First, I logged on to cisco.com
* Then I pinged cisco.com using CMD
* Then I monitored traffic on wireshark for 13 minutes
* I observed various different types of protocols such as tcp, ip, http, https, dns, arp etc..

**Question 2:**

