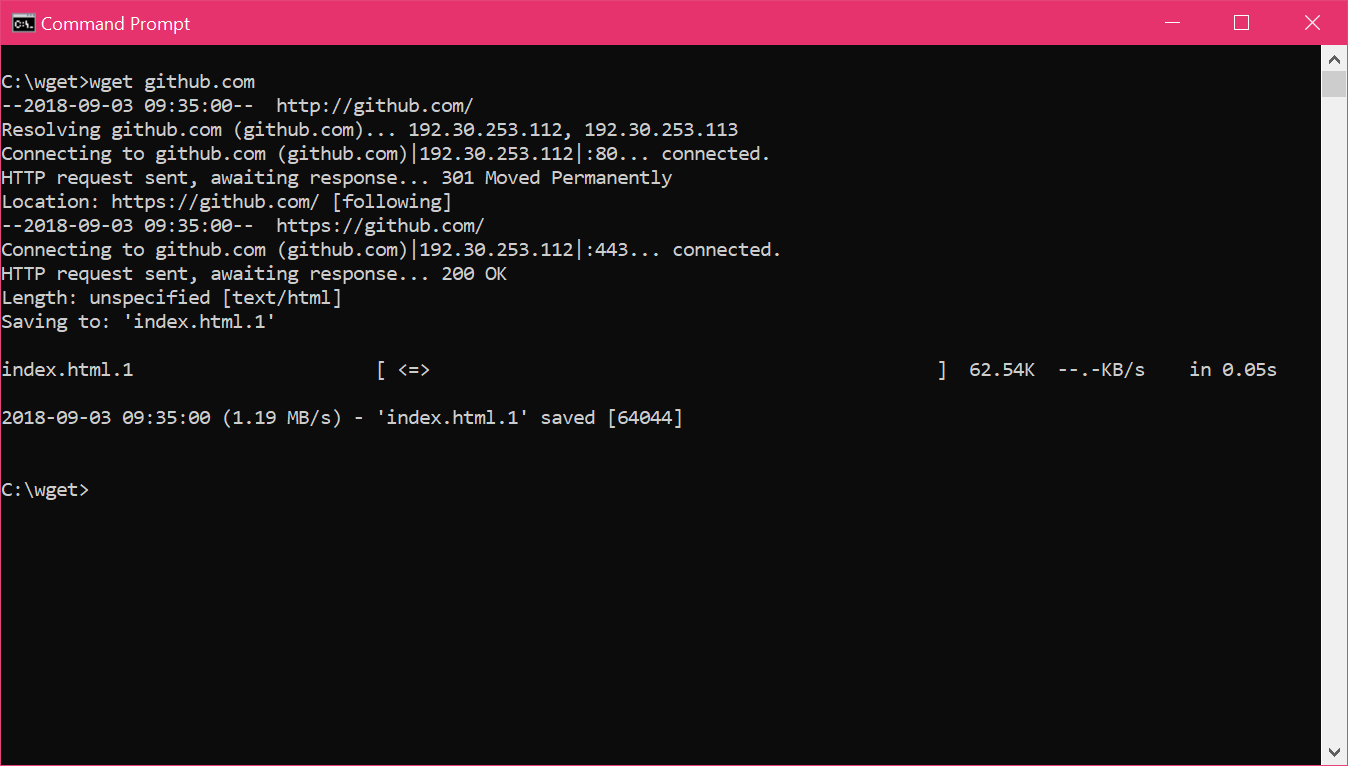
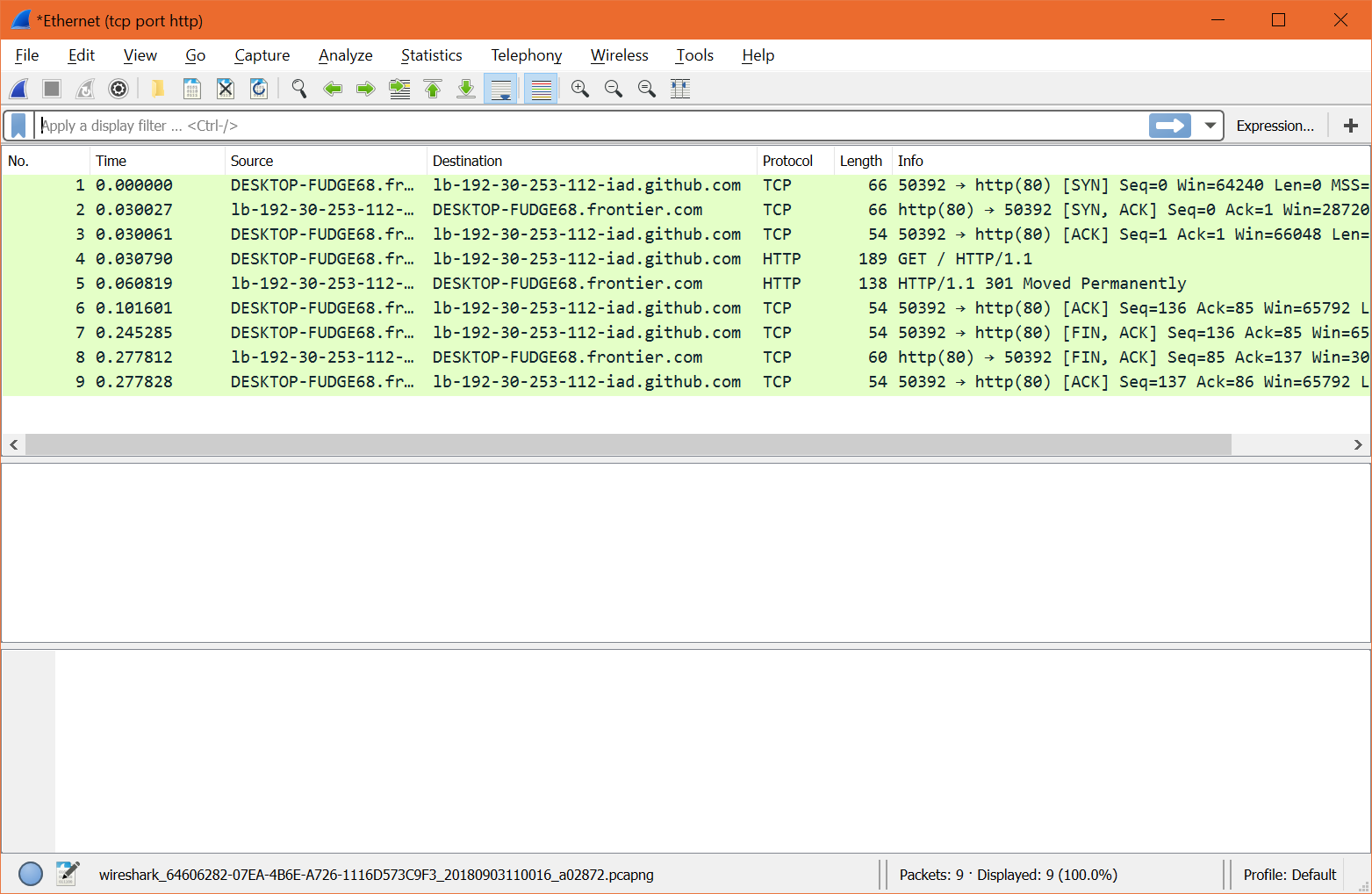
Homework-1: Wireshark

Name: Daniel Davieau

Exercise 1: Wireshark Protocol Layers

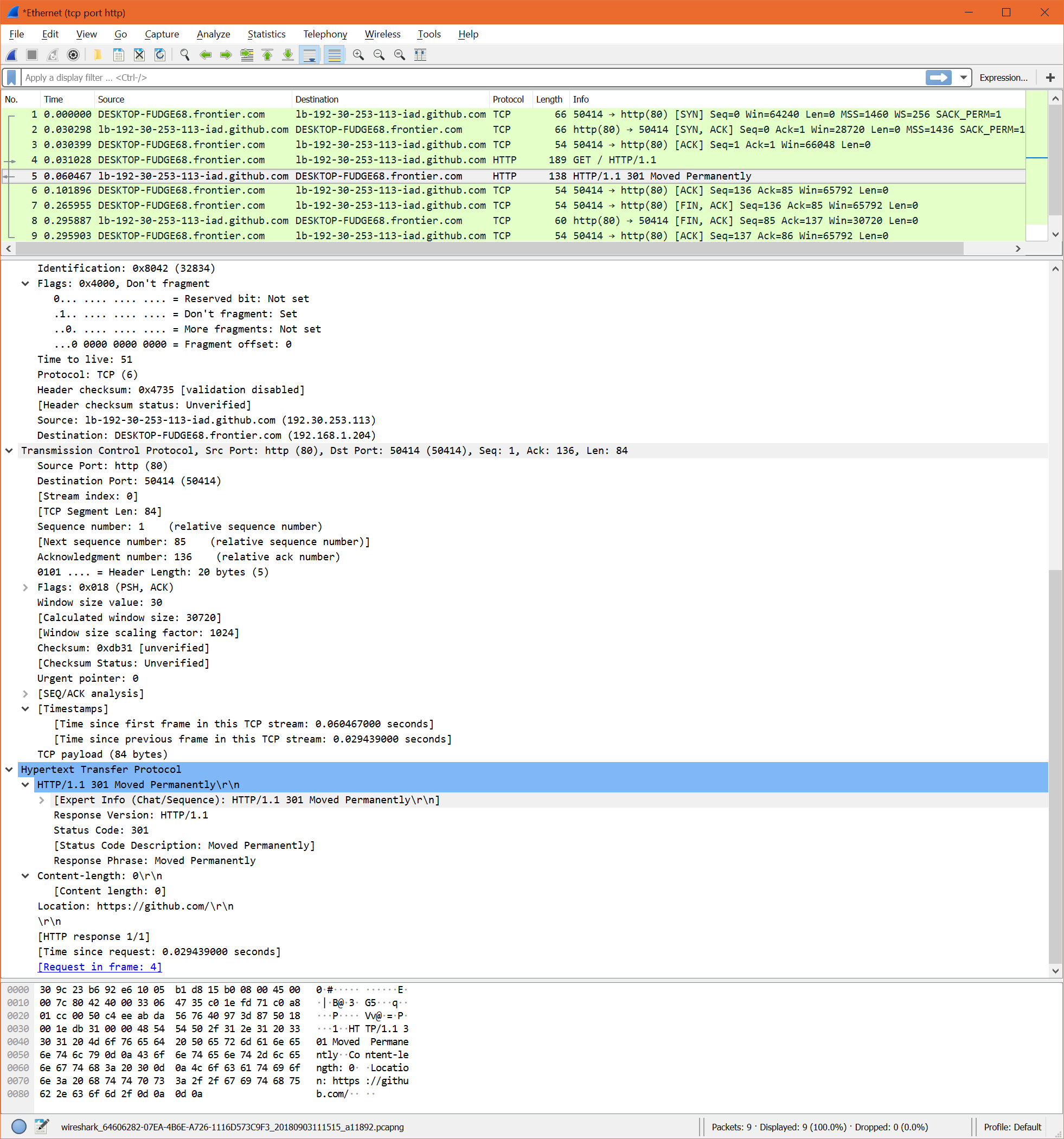
Turn In: Screen capture your Wireshark trace and turn it in (8 points)





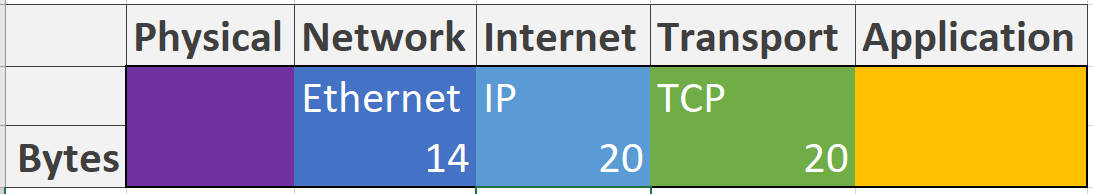
Step 2: Inspect the Trace

Turn In: Screen capture your Wireshark packet structure screen (8 points)



Step 3: Packet Structure

Turn In: Hand in your packet drawing (you can use paint program to draw) (8 points)



Step 4: Protocol Overhead

Turn In: Your estimate of download protocol overhead as defined above (4 points)

|  |  |
| --- | --- |
| SYN, ACK | 66 |
| HTTP | 138 |
| FIN,ACK | 60 |
| **Total** | **264** |
|  |  |
| Application Layer(HTTP) Breakdown |  |
| HTTP | 138 |
| Ethernet | 14 |
| IP | 20 |
| TCP | 20 |
| Http (Useful) | **84** |
| **Overhead Percentage** | **68%** |

Tell us whether you find this overhead to be significant (4 points)

***Yes! This overhead is well over 100% of the useful data.***

Step 5: Demultiplexing

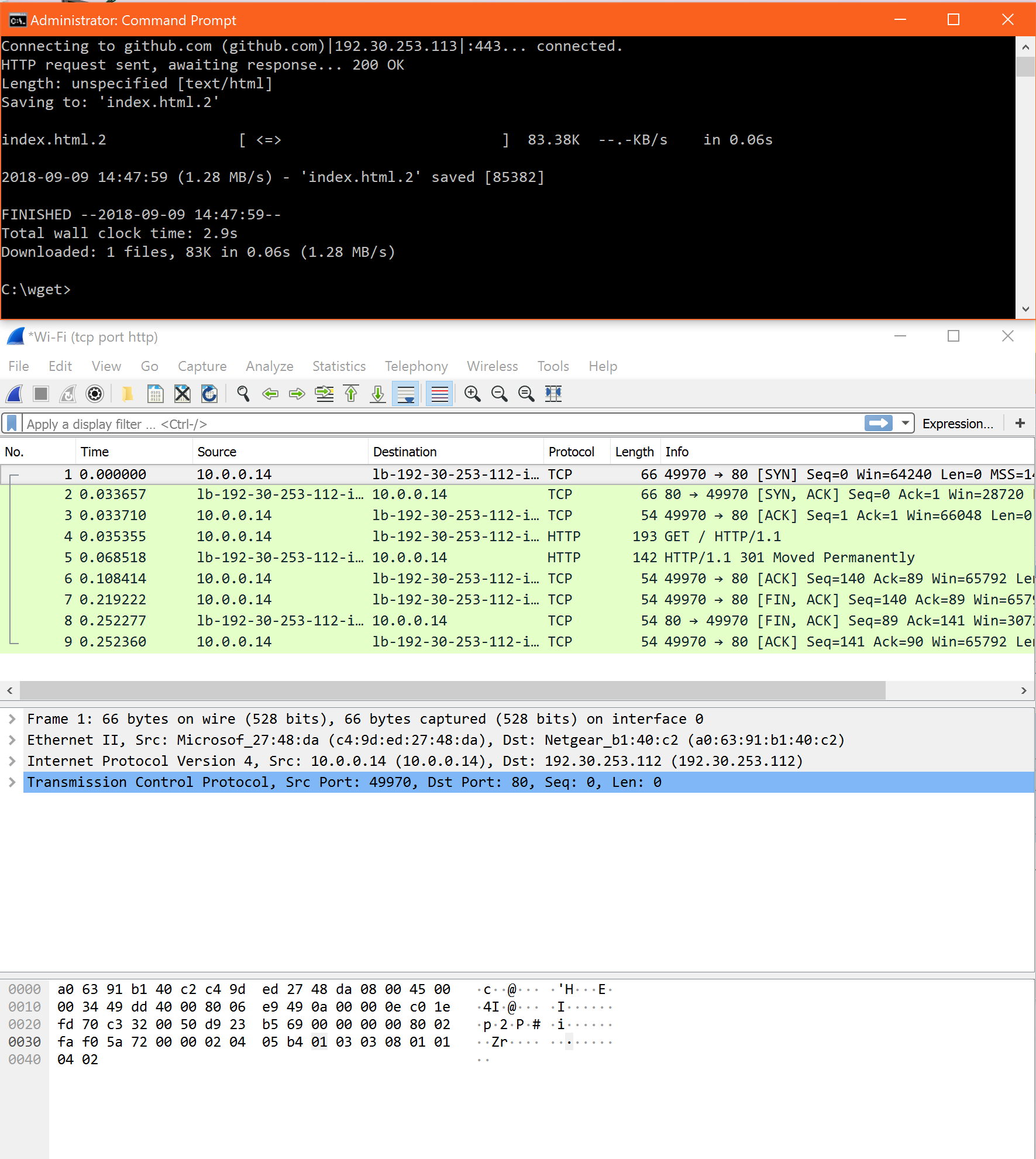
Turn In: Hand in your answers to the above questions (8 points)

1. ***In the Ethernet header the value  indicates that next layer is IP***
2. ***In the IP header the value  indicates that the next layer is TCP***

Exercise 2: Wireshark IPv4

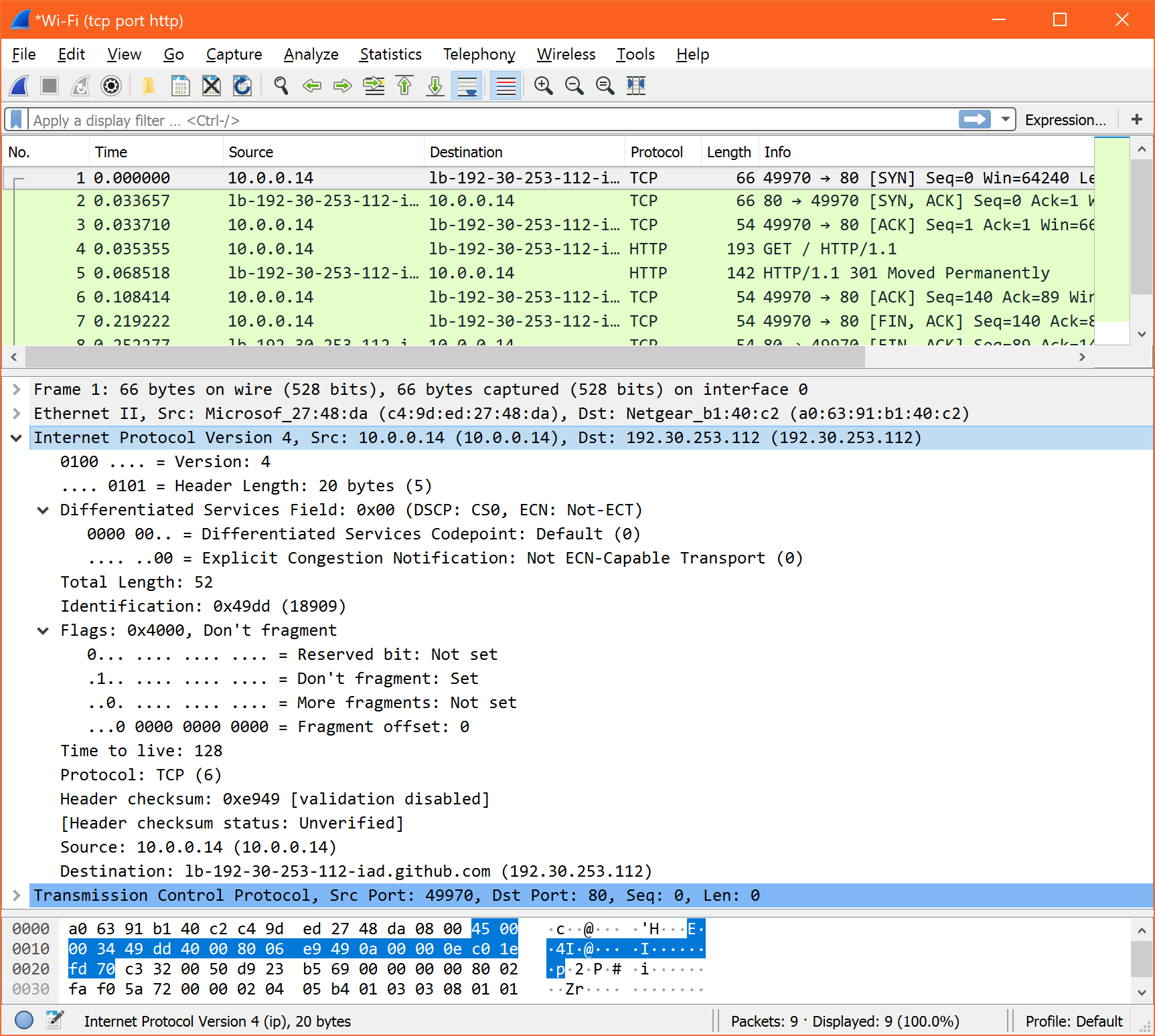
Step 1: Capture a Trace

Turn In: Screen capture your Wireshark trace and your traceroute and turn it in. (8 points)



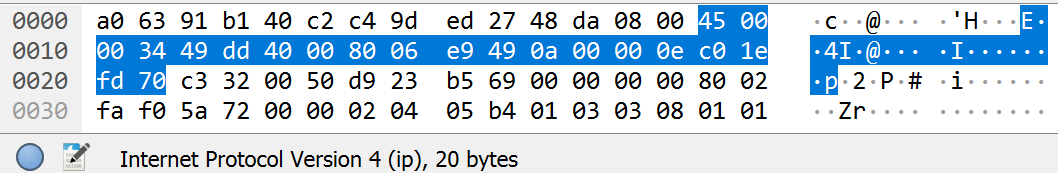
Step 2: Inspect the Trace

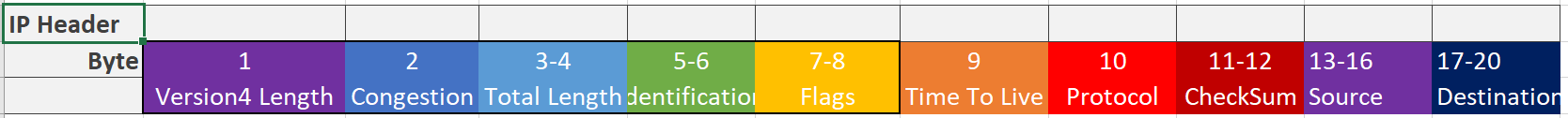
Turn In: Screen capture your Wireshark packet structure screen. Modify your screen capture to indicate each of the components of the IPv4 packet (8 points)



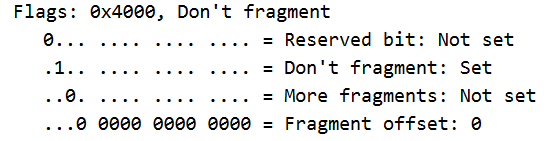
Step 3: IP Packet Structure

Turn In: Hand in your drawing of an IP packet and the answers to the questions above (8 points)



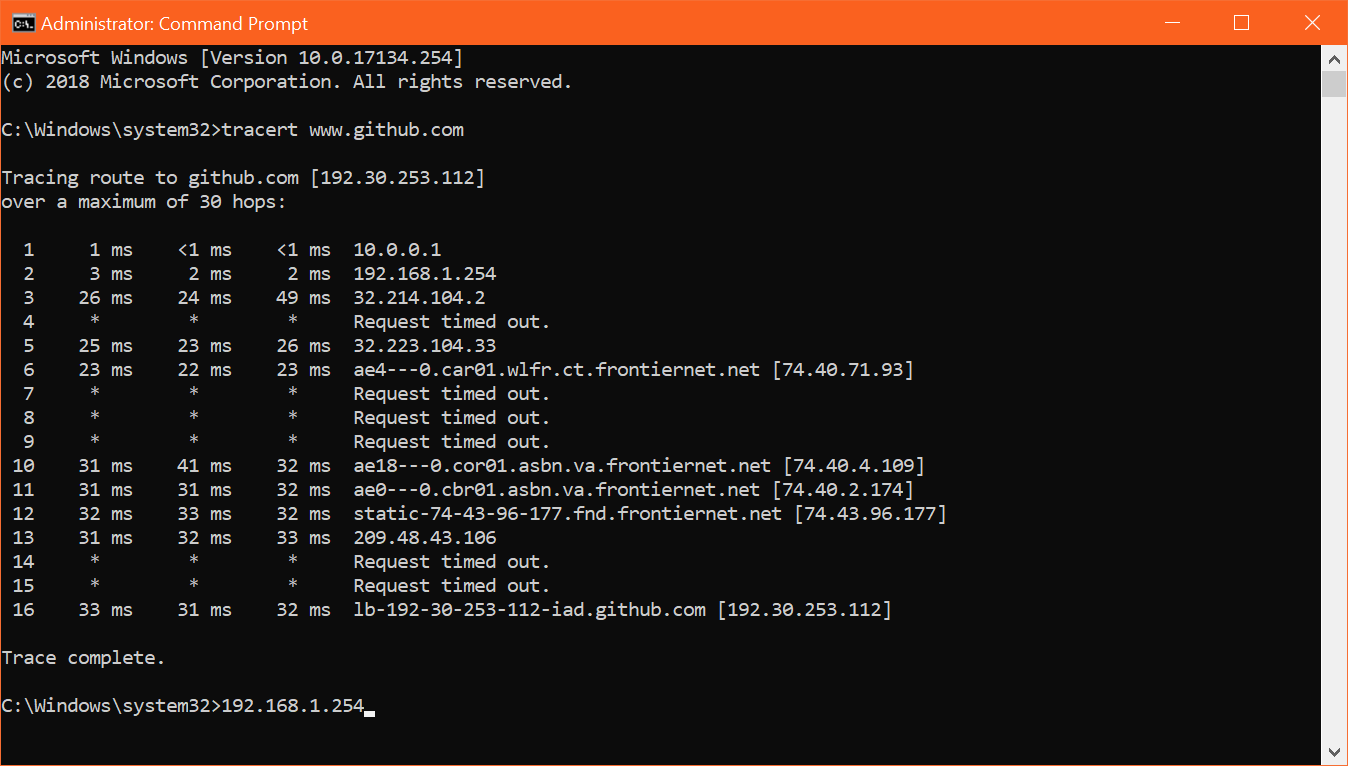


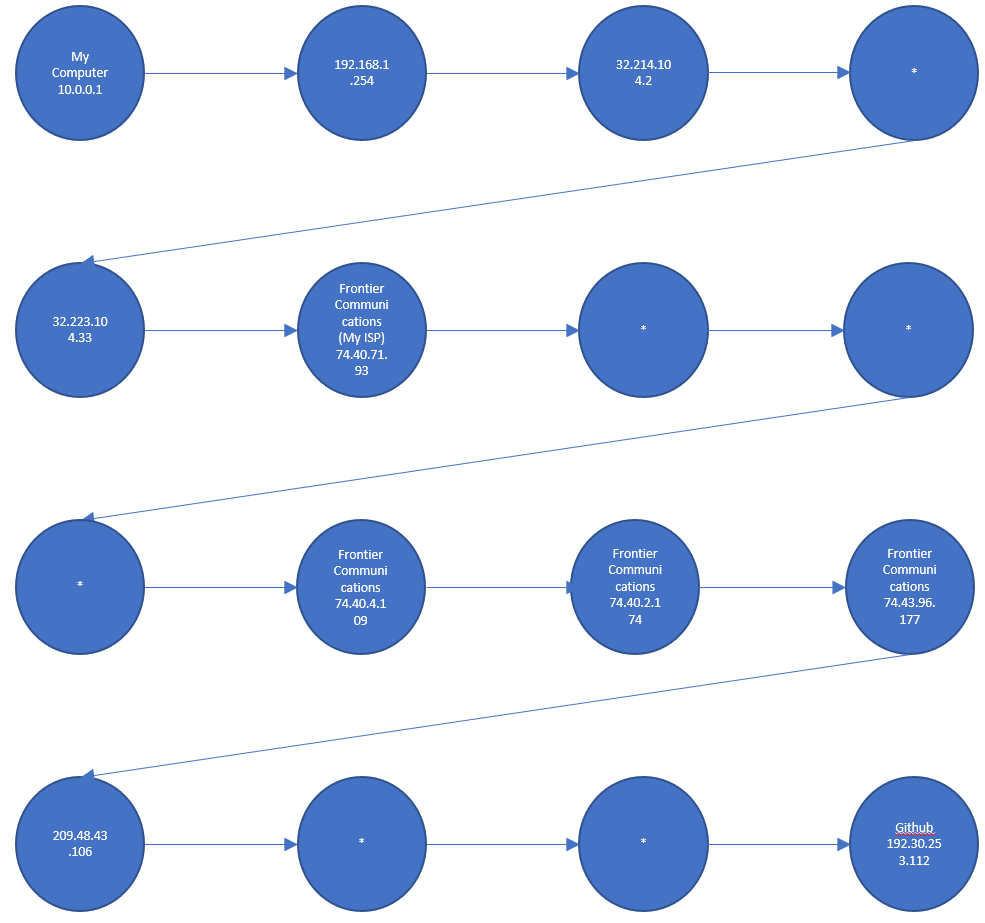
1. ***My Computer IP is 10.0.0.14 Github is 192.30.253.112***
2. ***Total Length field (20) includes the IP header and IP payload***
3. ***The identification field seems to increment for each packet per direction. I see my ip as source packets id increments 18910-18912 and remote ip 52783-52784.***
4. ***The initial TTL from my computer is 128. The maximum is 255***
5. ***We can see whether a packet is fragmented or not by looking at the Flags bits section of the IP header.***



Step 4: Internet Paths

Turn In: Hand in your drawing, and traceroute output (8 points)





Exercise 3: Wireshark DNS

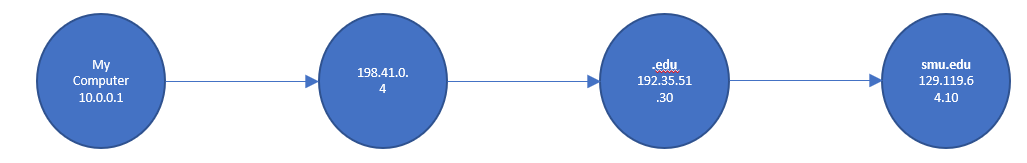
Step 1: Manual Name Resolution

Turn In: Hand in your drawing (8 points)

***dig @198.41.0.4 www.smu.edu***

***dig @192.35.51.30 www.smu.edu***

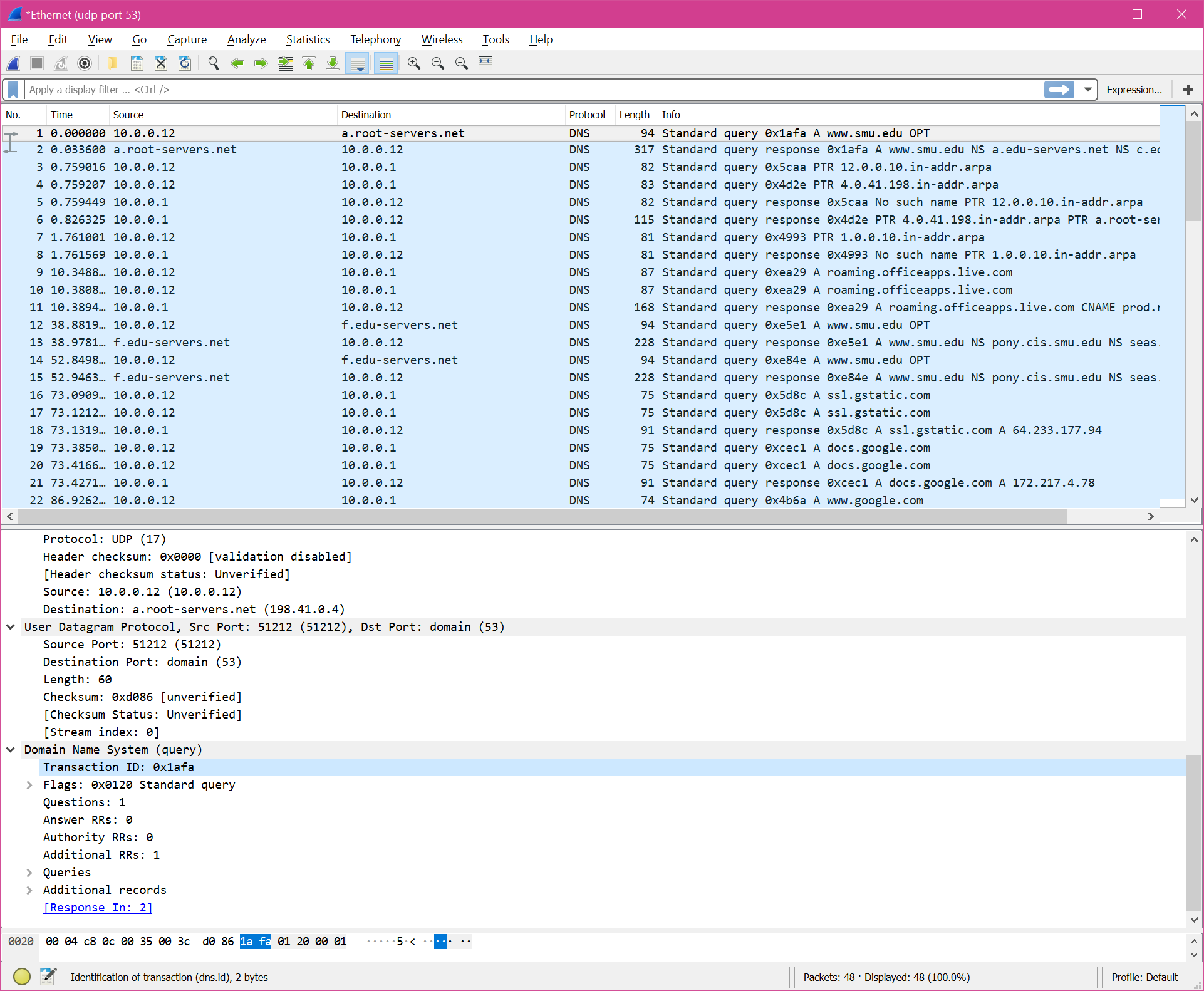
***dig @ 129.119.64.10 www.smu.edu***



Step 2: Capture a Trace

Turn In: Hand in your drawing (8 points)

***The instructions do not describe a drawing. I assume a screenshot of the capture is what is being asked for:***



Step 3: Inspect the Trace

Turn In: Hand in your answers to the above questions (12 points)

Look at the DNS header, and answer the following questions:

***1) TransactionID is 2 bytes (16 bits) long. My guess is that it is not used by other transactions.***

***2) This first bit flag indicates whether it is a query “0” or a response “1 “.***

***3) The entire DNS header is 52 bytes long.***

***4) For the initial response, in what section are the names of the nameservers carried? The section that the names of the name servers are in the “authoritative answers section” the type is “NS” name servers.***

***5)The ip addresses are in the “Additional Records” section and the type is “A” for authoritative?***

***6) The IP address of the domain name is carried in the “Answers” section***