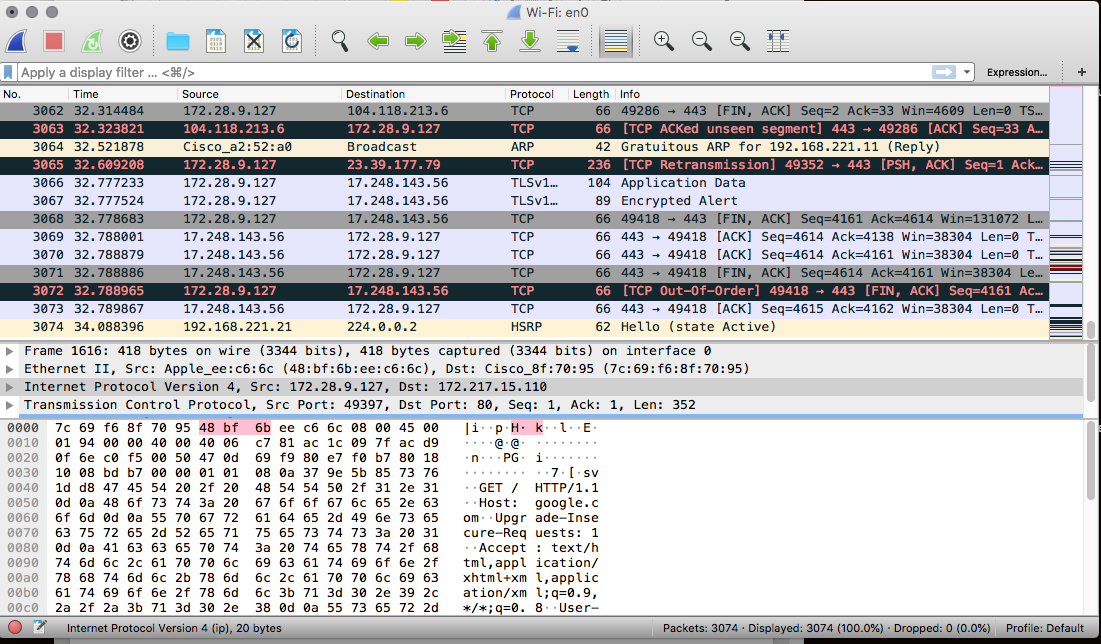
CSIS 100 – Week 4 Lab 2--Wireshark

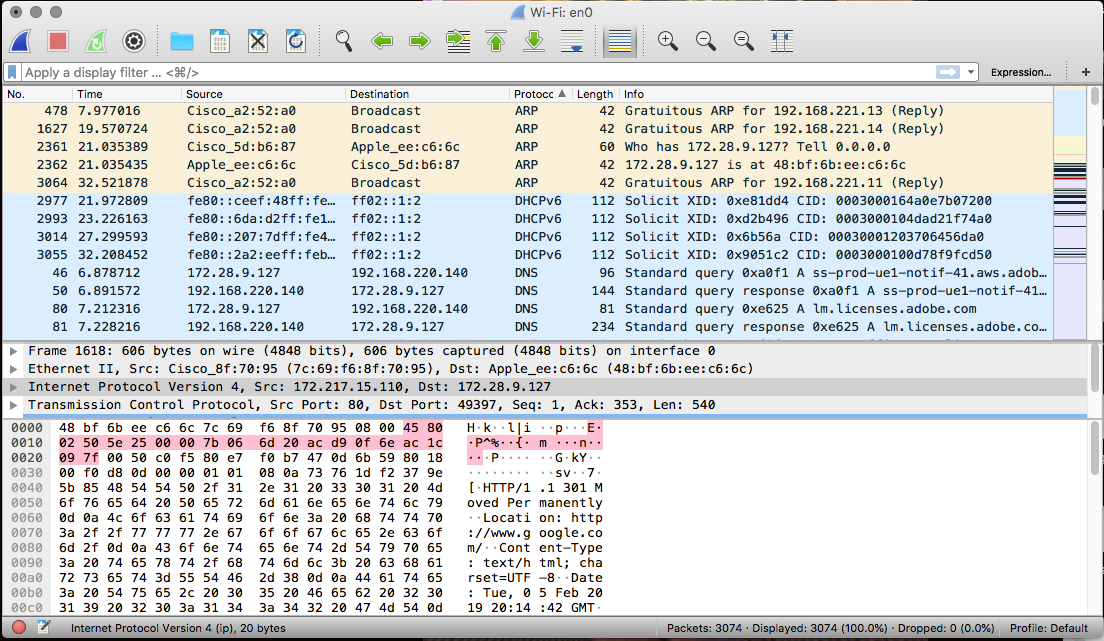
Packet Analysis Answer Template

**Screenshot #1:**

****

**Question #1 How many seconds did your capture run? 34.08**

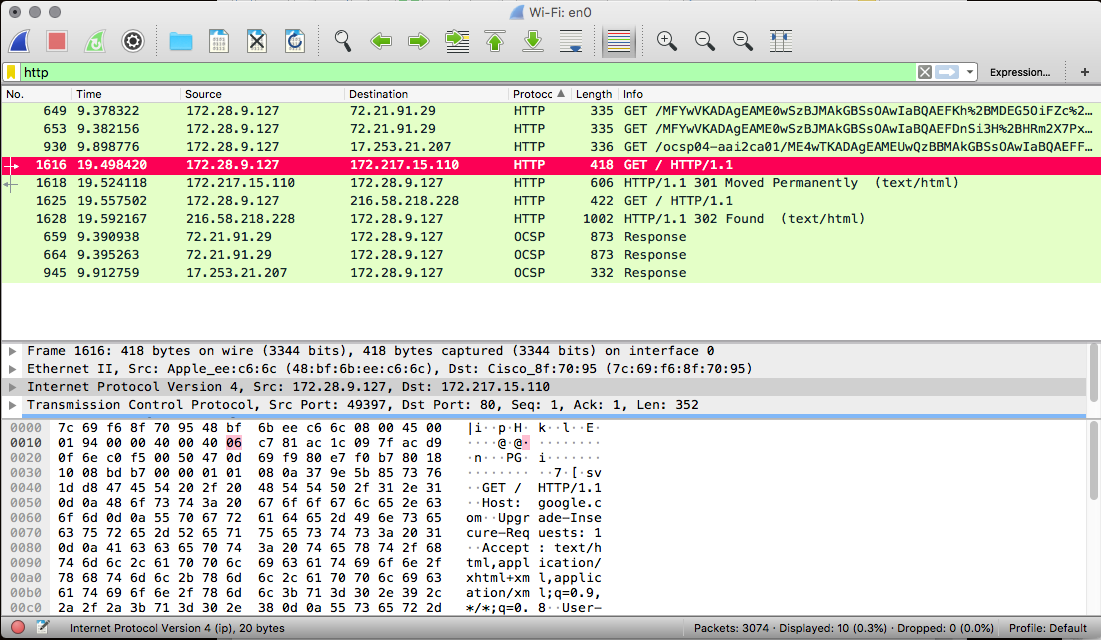
**Question 2: How many packets did you capture? 3074**

**Screenshot #2: **

**Question 3: What colors are present in your output? Yellow, blue, green, white, red, black, grey**

**Question 4: Are there any protocols that appear with more than one color? Why or why not? TCP has more than one color. It has multiple. The colors stand for bad TCP, checksum errors, TCP RST, and TPC SYN/FIN.**

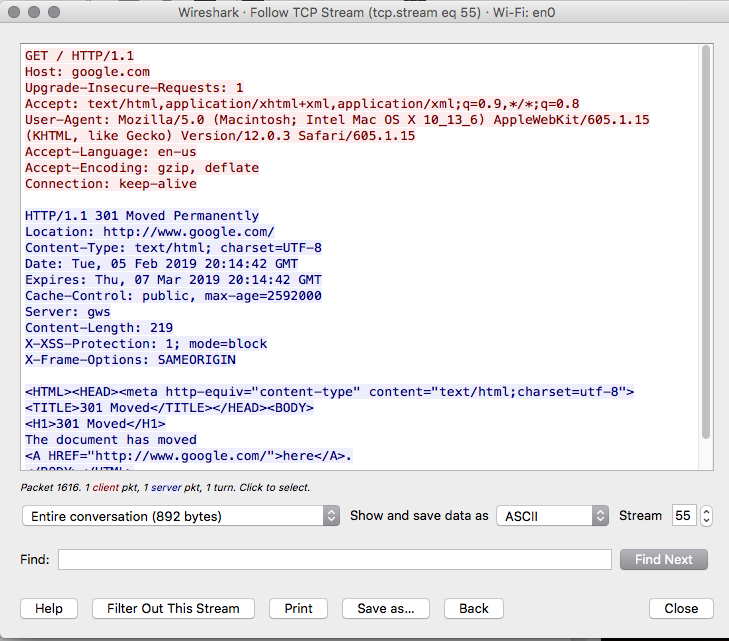
**Screenshot #3:**

****

**Question 5: How many rows are appearing in your WireShark capture with the filter in place? (Be careful with this...The “No.” column represents the packet number – not the number of rows currently visible.) 10**

**Question 6: What other protocols do you see in the “Protocol” column? OSCP**

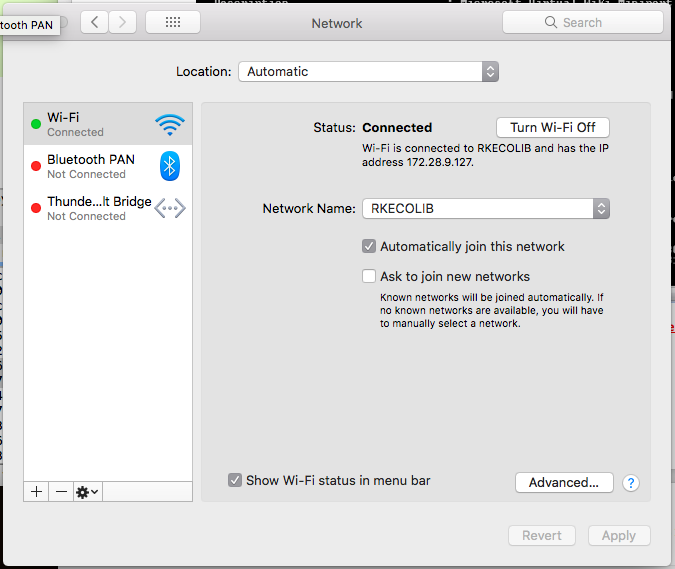
**Screenshot #4:**

****

**Question 7: What is the host listed directly below the GET / HTTP/1.1 command in your TCP Stream output? Host: google.com**

**Question 8: How many bytes is the entire conversation? 892**

**Screenshot #5:**

****

**Question 9: Compare the IPv4 address listed in your ipconfig output to the IP address that is listed under the Source column in your Wireshark capture for the first “GET / HTTP/1.1” row. Are these IP addresses the same? Why or why not? Yes. The host machine Wireshark is attached to is this network.**

**Question 10: Click on the row of the next packet in this conversation. Does your IP address appear in the Source or Destination column? Why? Destination column. Because the data flow is coming from the server, which is sending the information, to my computer.**