Katie Schaumleffle

Schaumlk

CS372 Fall 2022

09/27/2022

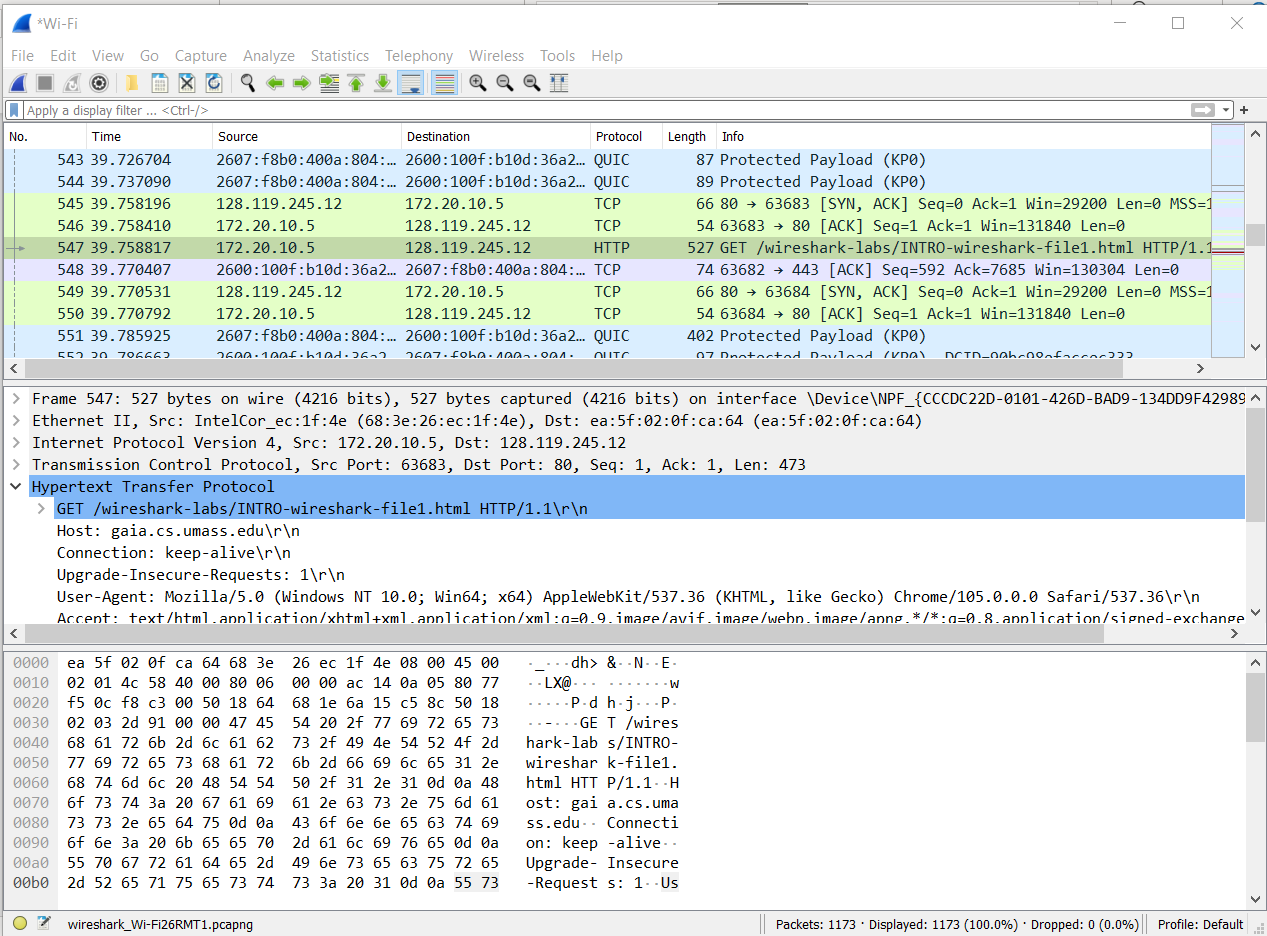
Wireshark Lab #1

The goal of this first lab was primarily to introduce you to Wireshark. The following questions will demonstrate that you’ve been able to get Wireshark up and running, and have explored some of its capabilities. Answer the following questions, based on your Wireshark experimentation and **be sure to include screenshots** showing each answer clearly, likely requiring a screenshot per question; you will be marked down on these labs if it is not immediately clear where your answer comes from:

1. List 3 different protocols that appear in the protocol column in the unfiltered packet listing pane in step 7 above.

1. HTTP

2. TCP

3. QUIC



1. How long did it take from when the HTTP GET message was sent until the HTTP OK reply was received? (By default, the value of the Time column in the packet-listing window is the amount of time, in seconds, since Wireshark tracing began. To display the Time field in time-of-day format, select the Wireshark *View* pull down menu, then select *Time* *Display Format*, then select *Time-of-day*.)

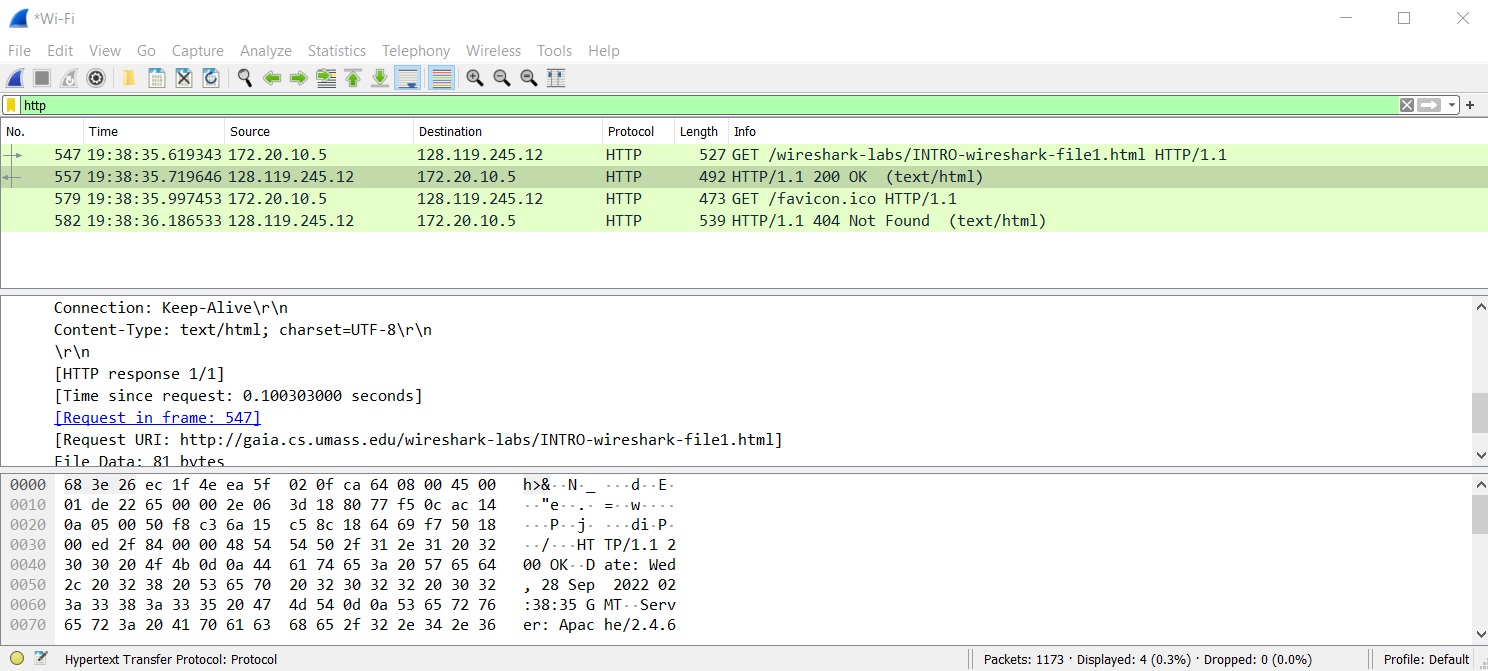
Graphical user interface, application, Word

Description automatically generated



19:38:35.719646-19:38:35.619343 = 0.100303 seconds

This is also shown in the middle section of Wireshark here:





1. What is the Internet Protocol (IP) address of the gaia.cs.umass.edu? What is the Internet Protocol (IP) address of your computer?

IP address of gaia.cs.umass.edu: 128.119.245.12

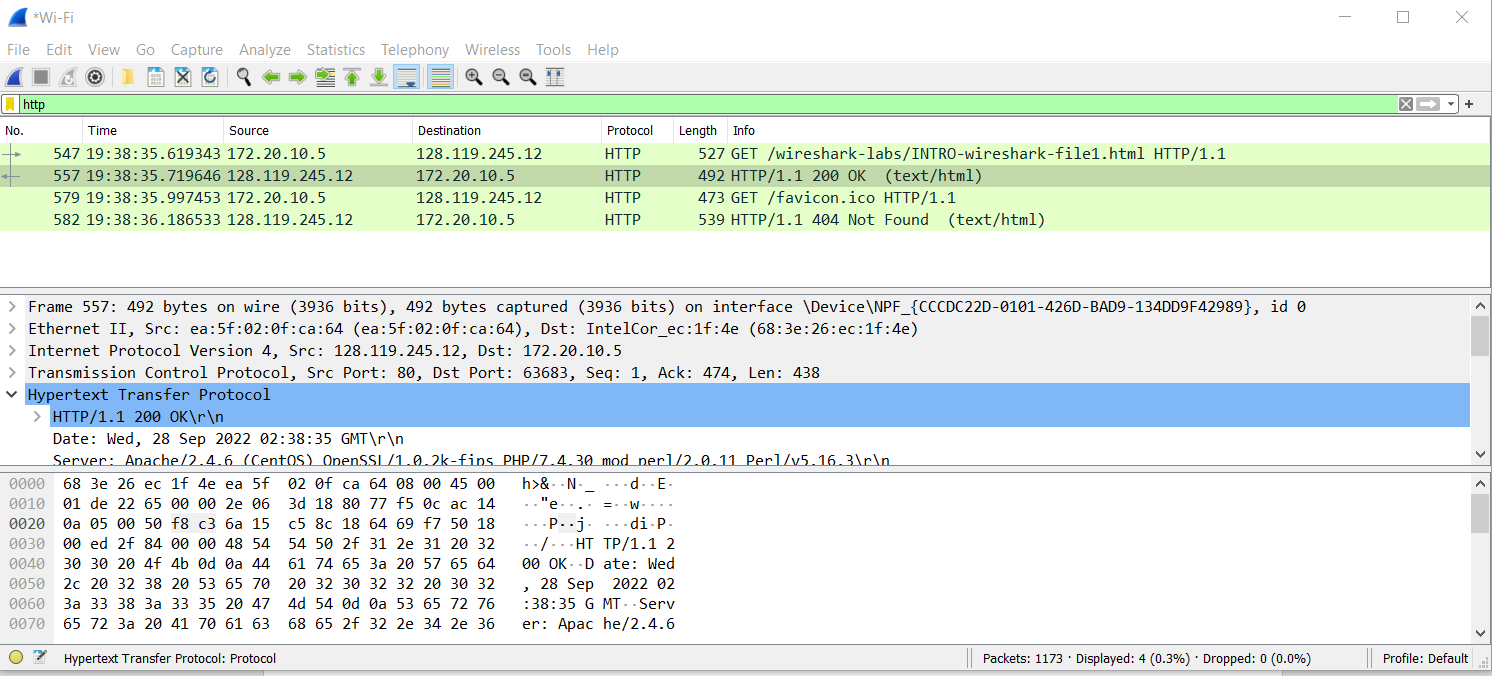
IP address of my computer: 172.20.10.5

Graphical user interface, application, Word

Description automatically generated



1. Include screenshots of the two HTTP messages (GET and OK) referred to in question 2 above. Make sure to include at least: Arrival Time, Total Length, Protocol, Source IP address, and Destination IP address.





Please note that “Arrival Time” should be labelled just as “Time” and “Total Length” is labelled as “length.”