Experiment-2: Basic Hands-on Experience on Wireshark with Practice Exercise.

1. Run the Wireshark and start capturing packets from WiFi interface.

2. While Wireshark is running, enter the URL:
   http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html
   and have that page displayed in your browser. In order to display this page, yourbrowser will contact the HTTP server at gaia.cs.umass.edu and exchange HTTPmessages with the server in order to download this page. The WiFi frames containing these HTTP messages aswell as all other frames passing through your WiFi will be captured by Wireshark.

3. After your browser has displayed the line: “Congratulations! You've downloaded the first Wireshark lab file!”, **STOP the Wireshark packet capture by selecting stop in the Wireshark capture window**. You now have live packet data that contains all protocol messages exchanged between your computer and other network entities! The HTTP message exchanges with the gaia.cs.umass.edu web server should appear somewhere in the listing of packets captured. But there will be many other types of packets displayed as well (due to many different protocol types).

4. Type in “http” (without the quotes, and *in lower case*) into the display filter specification window at the top. Then select *Apply* or just hit return. This will cause only HTTP message to be displayed in the packet-listing window. Figure 1 below shows a screenshot after the http filter has been applied to the packet capture window.

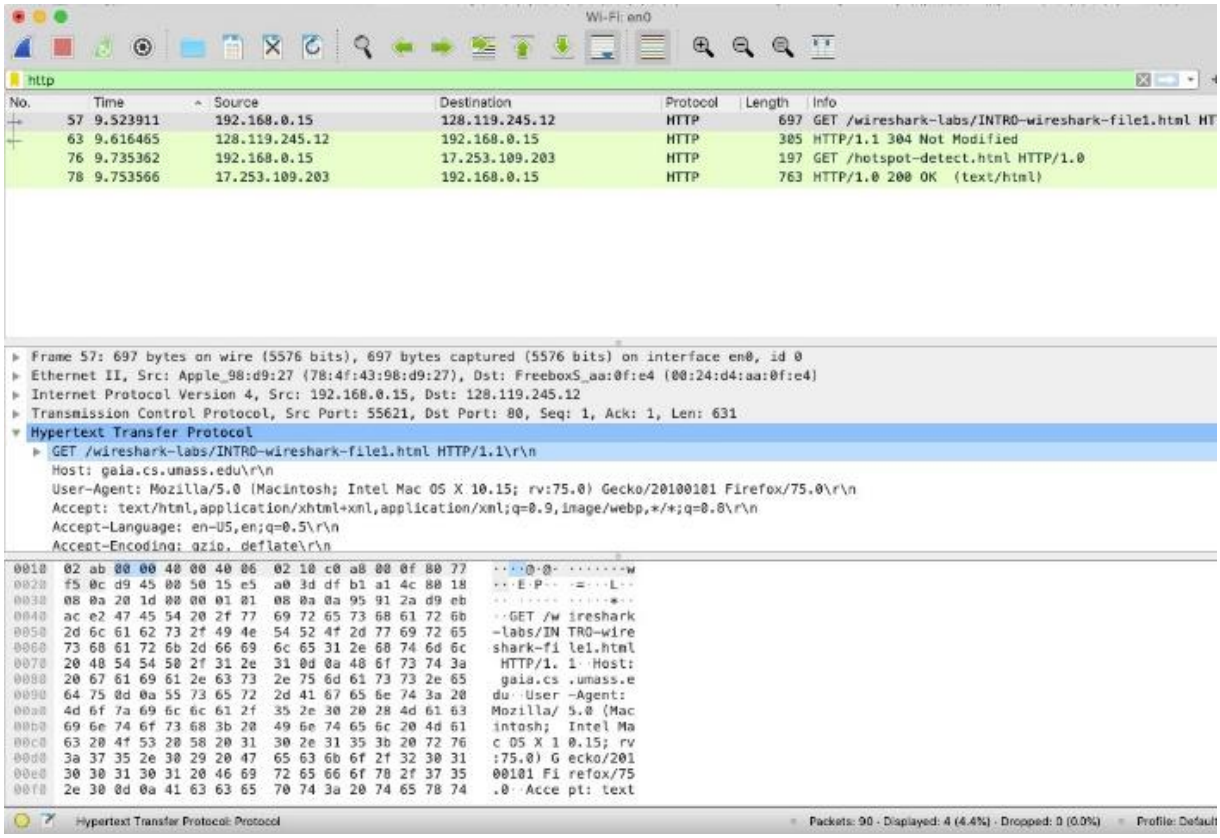

Figure-1: looking at the details of the HTTP message that contained a GET ofhttp://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html

5. Find the HTTP GET message that was sent from your computer to the gaia.cs.umass.edu HTTP server. (Look for an HTTP GET message in the "**Packets Listing Window**" that shows "GET" followed by the **gaia.cs.umass.edu** URL that you entered.)
   When you select that HTTP GET message in **Packets Listing Window**, *the Ethernet frame, IP datagram, TCP segment, and HTTP message header information will be displayed in the* ***packet- header window***. In this window, *maximize* the amount information displayed about the HTTP protocol. Your Wireshark display should look as shown in Figure-1 above.

Practice Exercise

Write the answers the following questions in a word-document with snapshots. Name this document as *YOUR NAME_ROLL NO_EXP-2* and upload in the Google drive folder with link:

https://docs.google.com/forms/d/e/1FAIpQLSfSoSNgOfJF_EVGchPs0IoUg-pdXgPs50P0QO4G9EivW2JrgQ/viewform?usp=sf_link

1. **List 3 different protocols that appear in the protocol column in the unfiltered packet listing window.**

2. **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*.)

3. **What is the Internet address of the gaia.cs.umass.edu** (also known as www-net.cs.umass.edu)?

4. **What is the Internet address of your computer?**

5. **Print (as pdf) the two HTTP messages (GET and OK) referred to in question 2 above.** To do so, select *Print* from the Wireshark *File* command menu, and select the "*Selected Packet Only"* and *"Print as displayed"* radial buttons, and then click OK.