4598 Lab 1

Questions:

1. (Part 1.A.) Write the definition of a packet sniffer.

A packet sniffer is a software, like WireShark, that captures network traffic by monitoring the data packets that are sent through the network.

2. (Part 1.A) Write the definition of a packet analyzer.

A packet analyzer is a tool that takes the packets captured by the sniffer and then decodes it to a human-friendly format, allowing the user to thoroughly analyze the contents, protocols other relevant information from the packets.

3. (Part 1.A) What does the Wireshark packet capture library do?

The Wireshark packet capture library is responsible for directly capturing network traffic from the network interface card. They allow Wireshark go into "promiscuous mode" to record all traffic passing through the network adapter, even if this traffic is not directly addressed to the Wireshark host.

4. (Week 1 Lecture) What is a (data) link layer frame?

A data link layer frame is the second layer of the OSI model. It provides the transfer of frames between nodes across the physical layer. The link layer frame adds control info, synchronization, flow control and checks the bits to prevent transmission errors and ensure a reliable transmission of the data. The data link layer is divided into two parts: the Logical Link Control (LLC), which regulates error and flow management within the network layer, and the Medium Access Control (MAC), which regulates access to the transmission medium.

5. (Part 2.B.7 below) List 3 different protocols that appear in the protocol column in the unfiltered packet-listing window.

Three different protocols: HTTP, TCP, Ipv4, UPD

6. (Part 2.B.8) How long did it take from when the HTTP GET message was sent until the HTTP OK reply was received?

GET message sent: 07:40:28.277962

OK message received: 07:40:28.440560

Transmission time: 0.1626 seconds

7. Part 2.B.8) What is the Internet address of gaia.cs.umass.edu? What is the Internet address of your computer?

IP address of my computer (Source): 192.168.1.13

IP address of gaia.cs.umass.edu (Destination): 128.119.245.12

8. (Part 2.B.9) Print the two HTTP full messages (GET and OK). 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.

4598 Lab 1

Screenshots

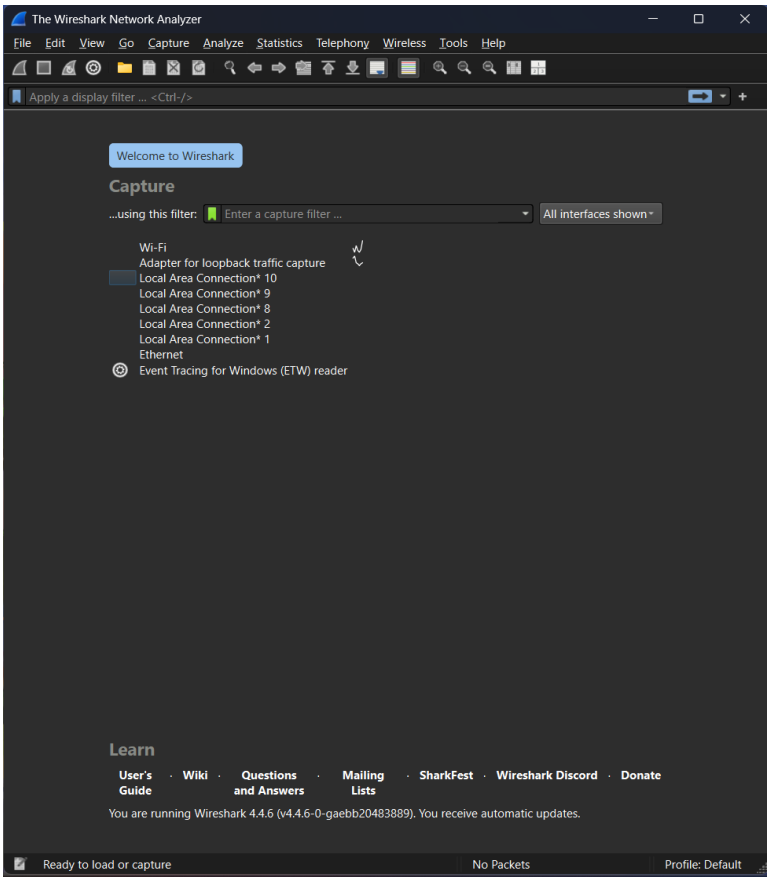

Figure 1- Wireshark startup screen

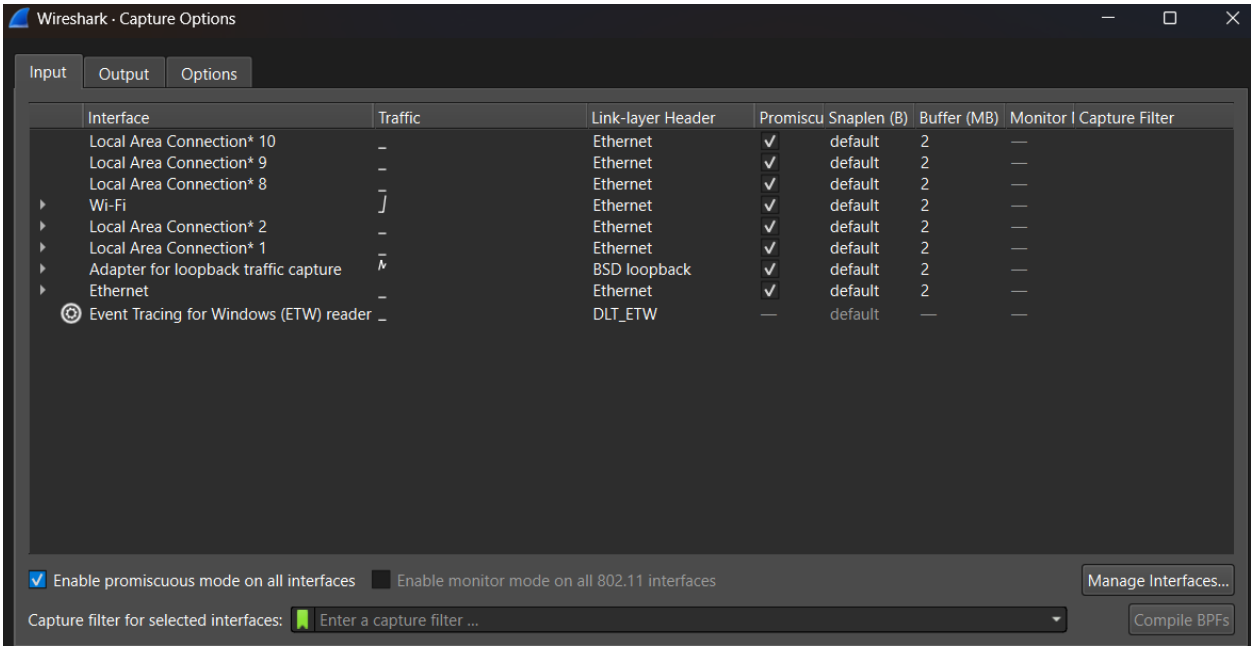

Figure 2 - Options menu

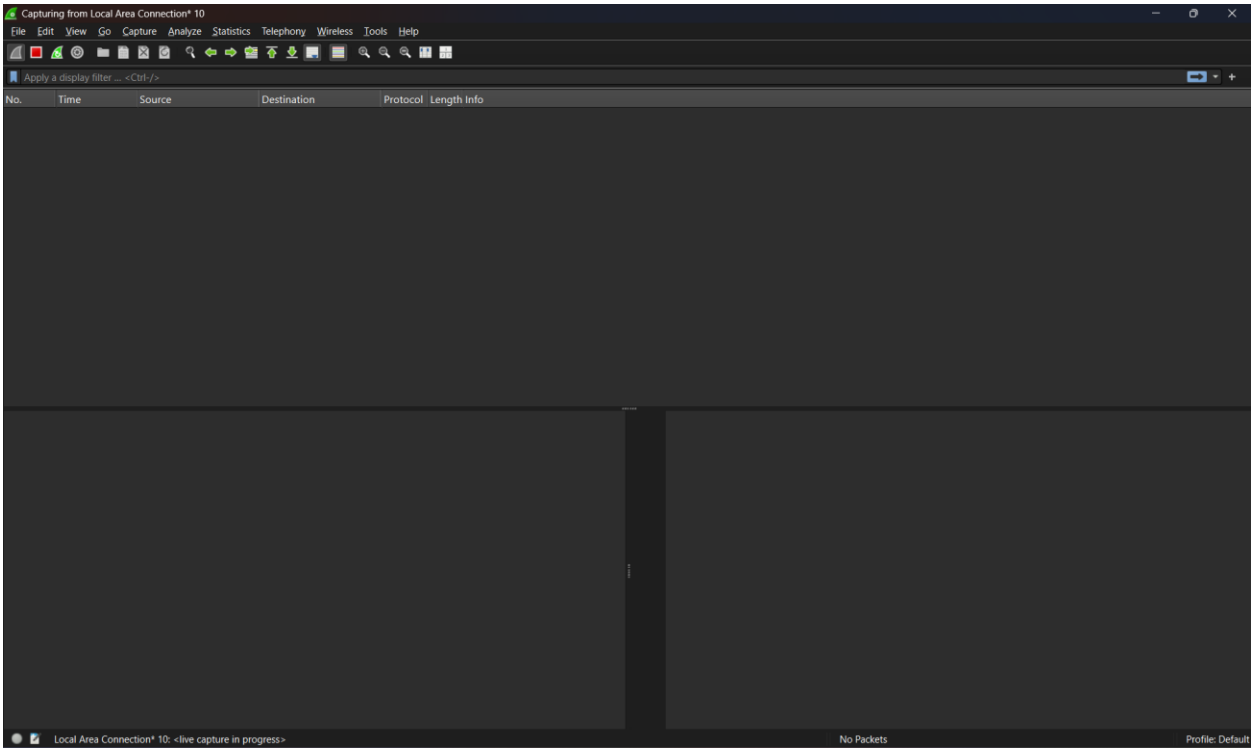

Figure 3 - Capturing screen (Stopped)

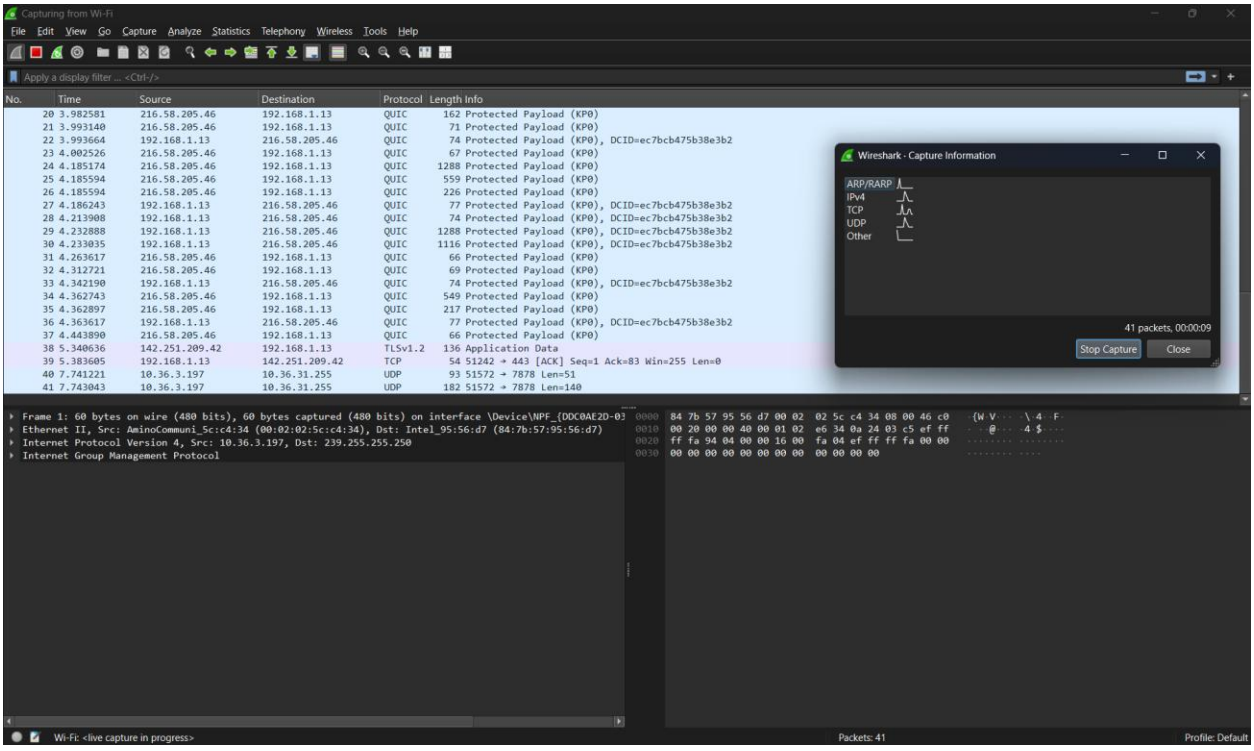

Figure 4 - Capturing screen (Running)

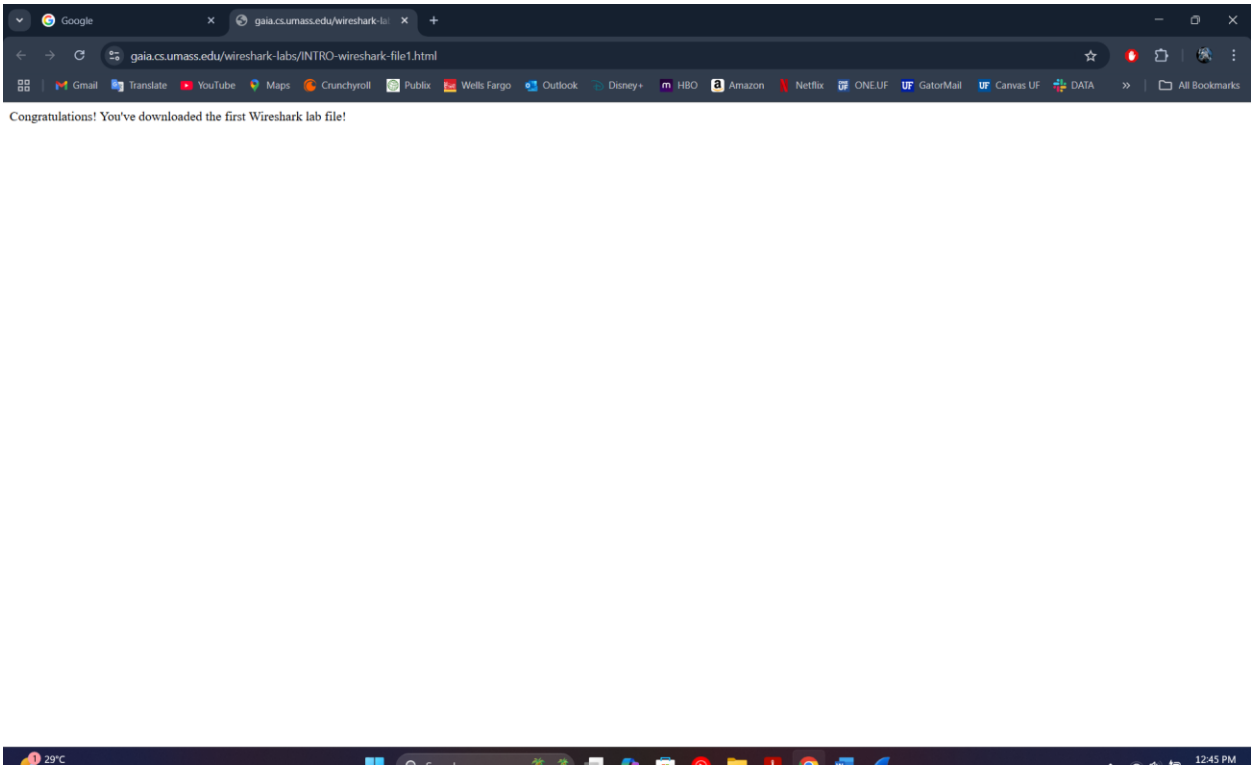

Figure 5 - Lab website message

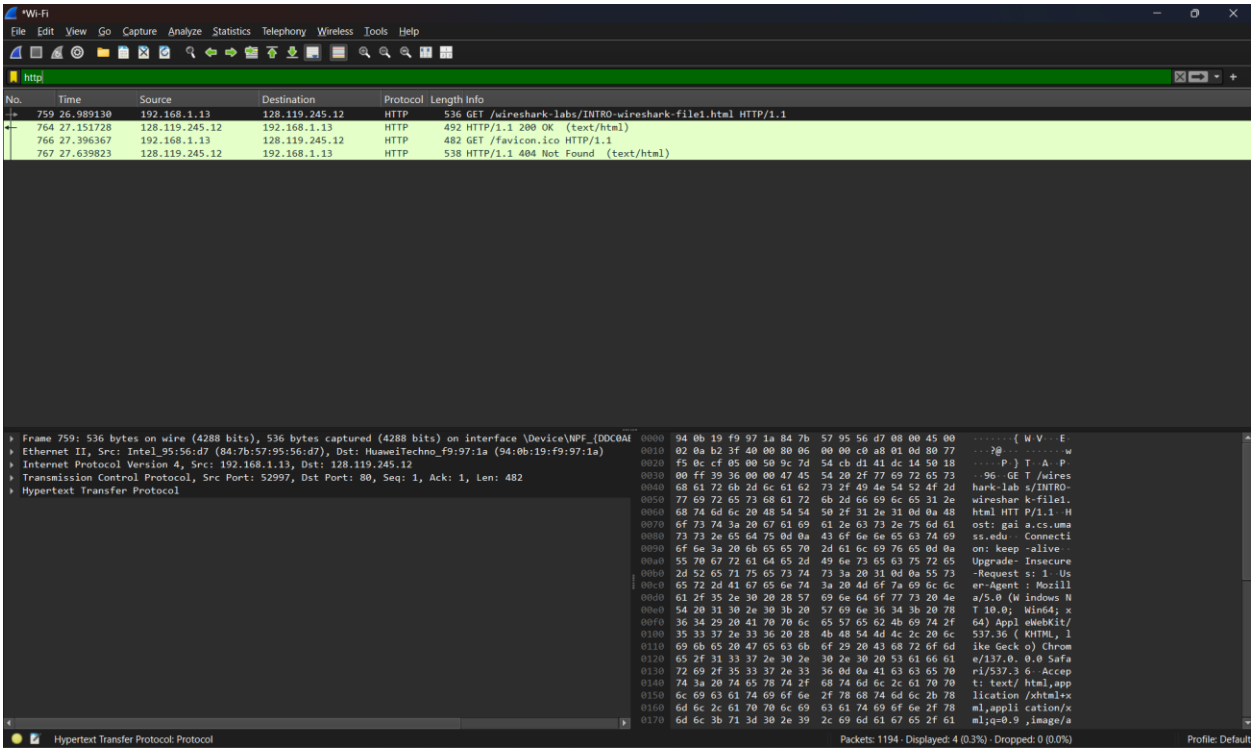

Figure 6 - HTTP protocol packets

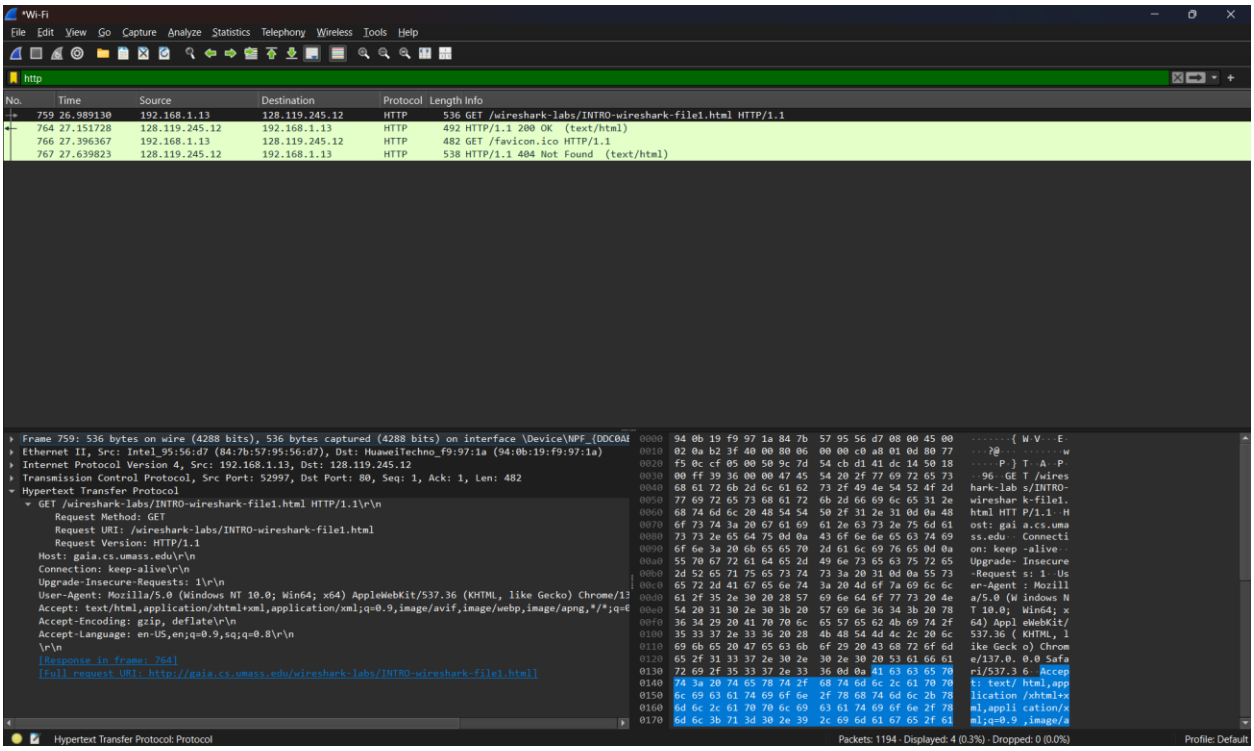

Figure 7 - GET packet expanded interface