Wireshark Laboratory - Introduction to Software

Figure 1 - Demonstration of the steps with filter HTTP.

Figure 2 - Demonstration of the steps without filters.
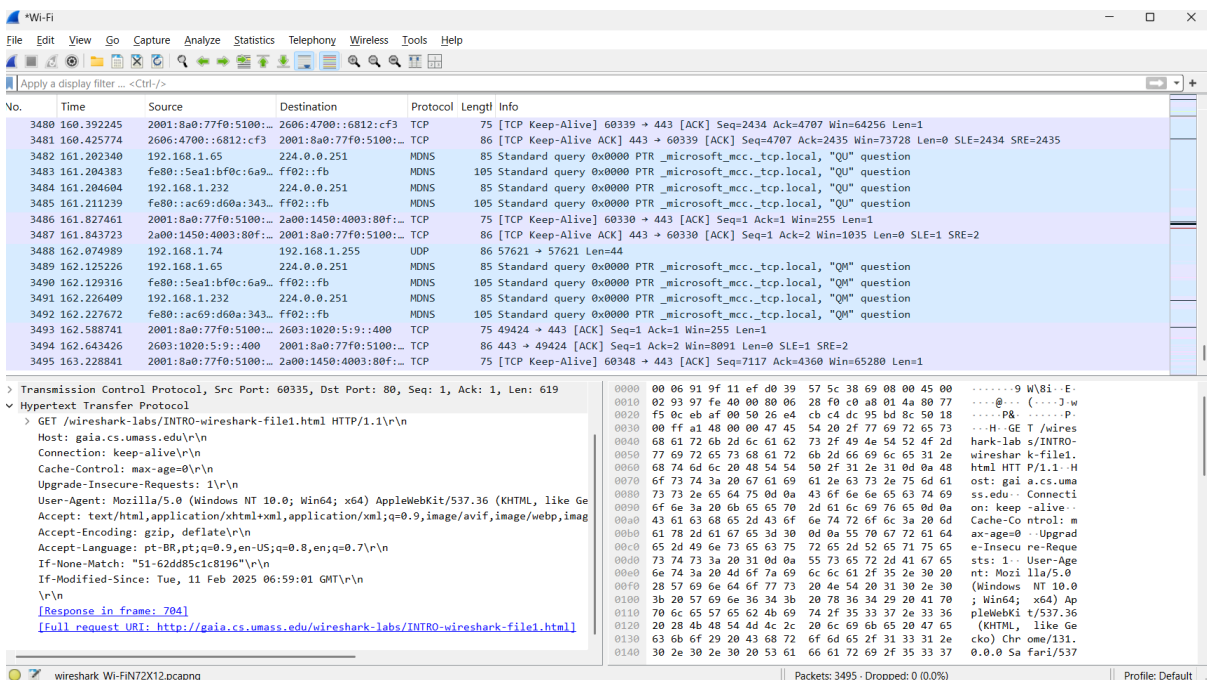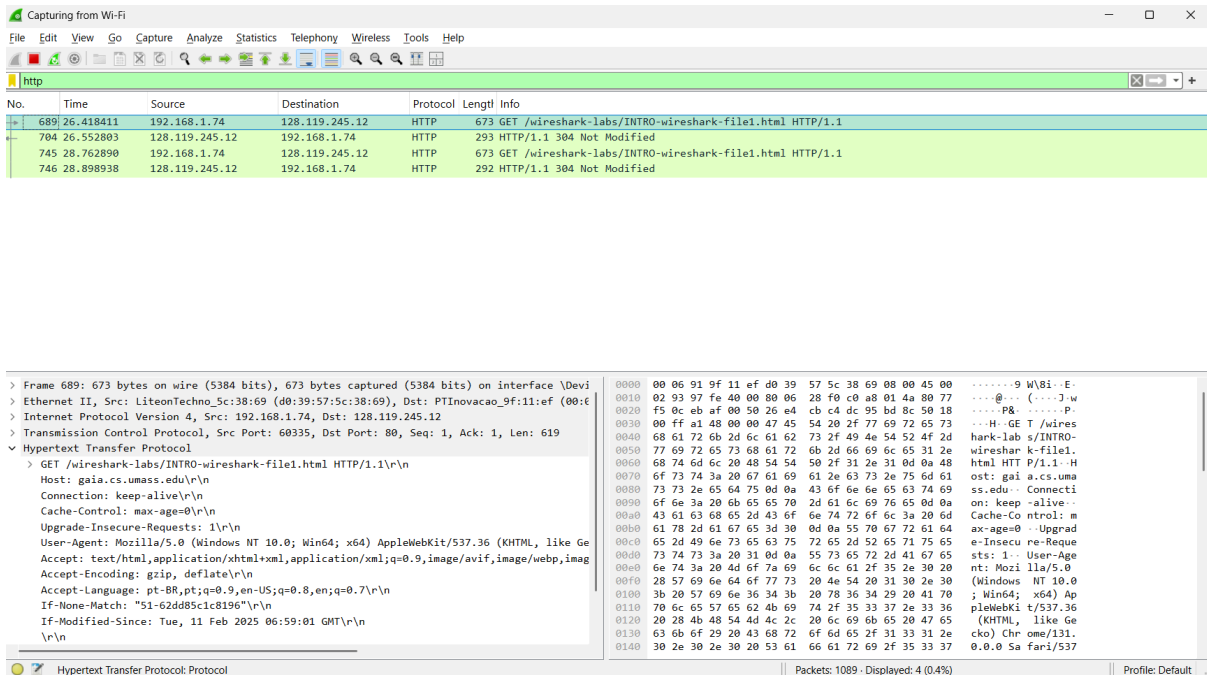
What to hand in (Page 10 of PDF)

1. List 3 different protocols that appear in the protocol column in the unfiltered packet-listing window in step 7 above.
With reference to figure 2, we can list 3 different protocols: HTTP, MDNS, TLSv1.2.

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 packetlisting 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.)

The total time was: 26.552803 (GET sent) - 26.418411(Received) = 0.134392 seconds (approximately 134 milliseconds). The "304 Not Modified" response is valid, as the HTTP server is working correctly.

3. What is the Internet address of the gaia.cs.umass.edu (also known as wwwnet.cs.umass.edu)? What is the Internet address of your computer?
gaia.cs.umass.edu: 128.119.245.12; My computer: 192.168.1.74.

4. Print 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.
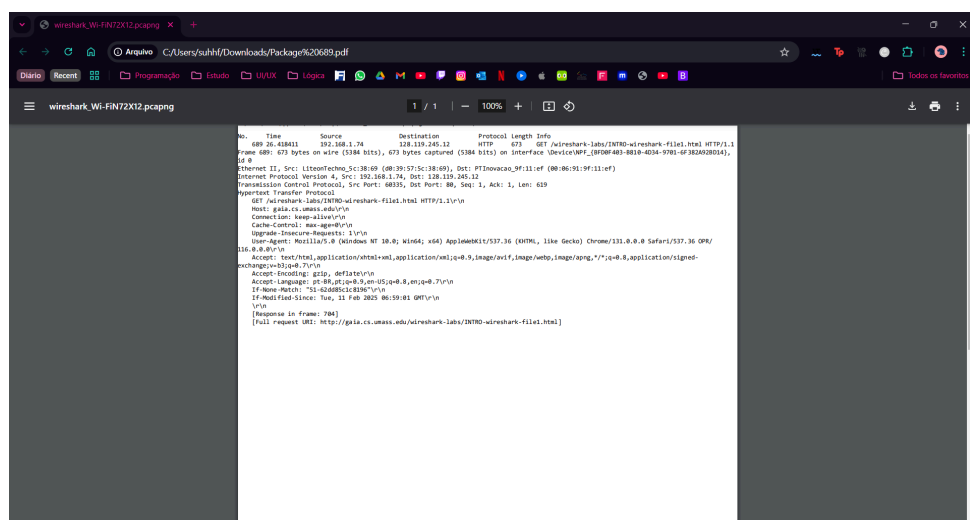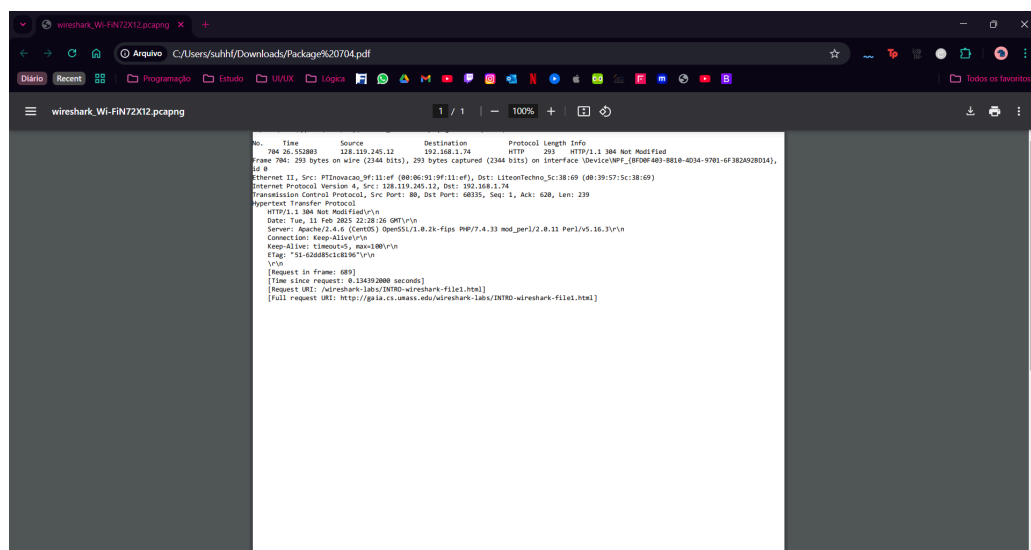*The following images are of the specific packages 689 and 704.*

Figure 3 - Package 689.

Figura 4 - Package 704.