**Wireshark Lab**

*Name: Richa Vivek Savant*

*RegNo.: BL.EN.U4CSE21171*

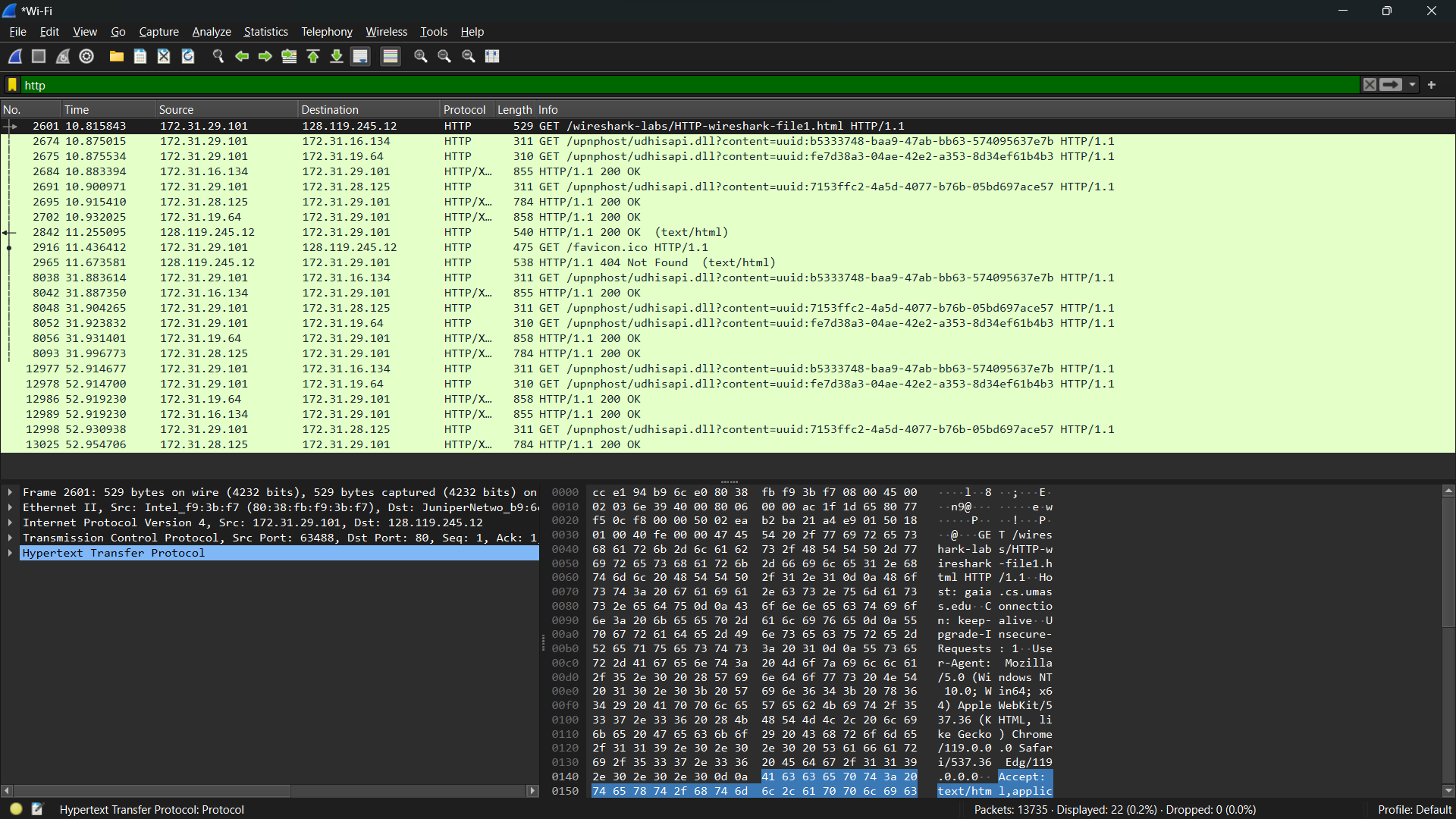
1. Experiment 1: HTTP Wireshark

The Basic HTTP GET/response interaction

Let’s begin our exploration of HTTP by downloading a very simple HTML file - one that is very short, and contains no embedded objects. Do the following:

1. Start up your web browser.
2. Start up the Wireshark packet sniffer, as described in the introductory lab (but don’t yet begin packet capture). Enter “http” (just the letters, not the quotation marks) in the display-filter-specification window, so that only captured HTTP messages will be displayed later in the packet-listing window. (We’re only interested in the HTTP protocol here, and don’t want to see the clutter of all captured packets).
3. Wait a bit more than one minute (we’ll see why shortly), and then begin Wireshark packet capture.
4. Enter the following to your browser http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html Your browser should display the very simple, one-line HTML file.
5. Stop Wireshark packet capture.

Output:



1. Experiment 2: UDP Wireshark

Start capturing packets in Wireshark and then do something that will cause your host to

send and receive several UDP packets. (One way to do this would be to use the nslookup

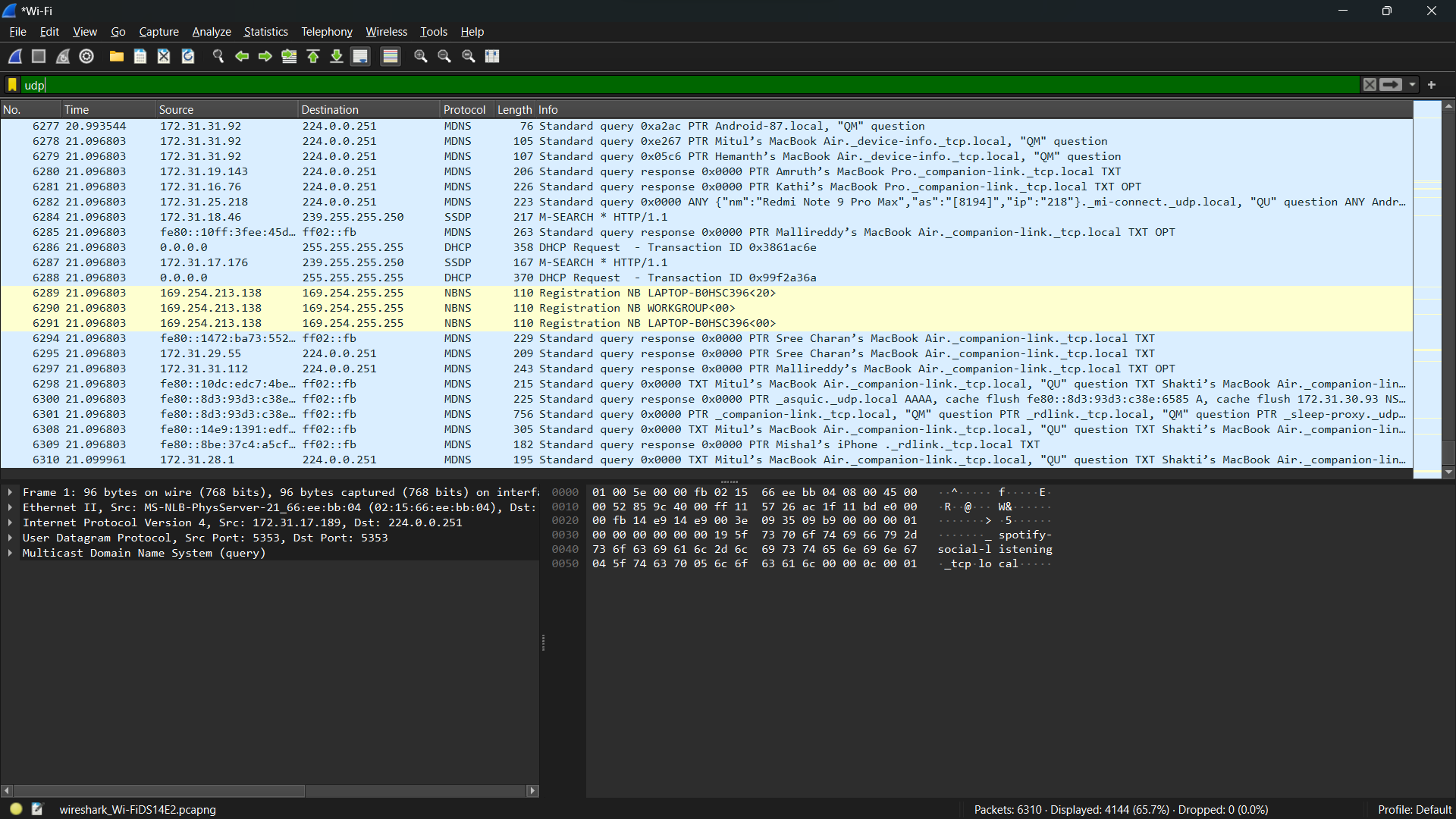
command, as we saw in the DNS Wireshark lab. If you are unable to run Wireshark on a

live network connection, you can download a packet trace file that was captured while

following the first two steps of the nslookup section of the Wireshark DNS lab on one of

the author’s computers)

Output:



1. Experiment 3: TCP Wireshark

• Start up your web browser. Go the http://gaia.cs.umass.edu/wiresharklabs/

alice.txt and retrieve an ASCII copy of *Alice in Wonderland.* Store this file

somewhere on your computer.

• Next go to <http://gaia.cs.umass.edu/wireshark-labs/TCP-wireshark-file1.html>.

Use the Browse button in this form to enter the name of the file (full path name)

on your computer containing Alice in Wonderland (or do so manually). Don’t yet

press the “Upload alice.txt file” button.

• Now start up Wireshark and begin packet capture (Capture->Options) and then

press OK on the Wireshark Packet Capture Options screen (we’ll not need to

select any options here).

• Returning to your browser, press the “Upload alice.txt file” button to upload the

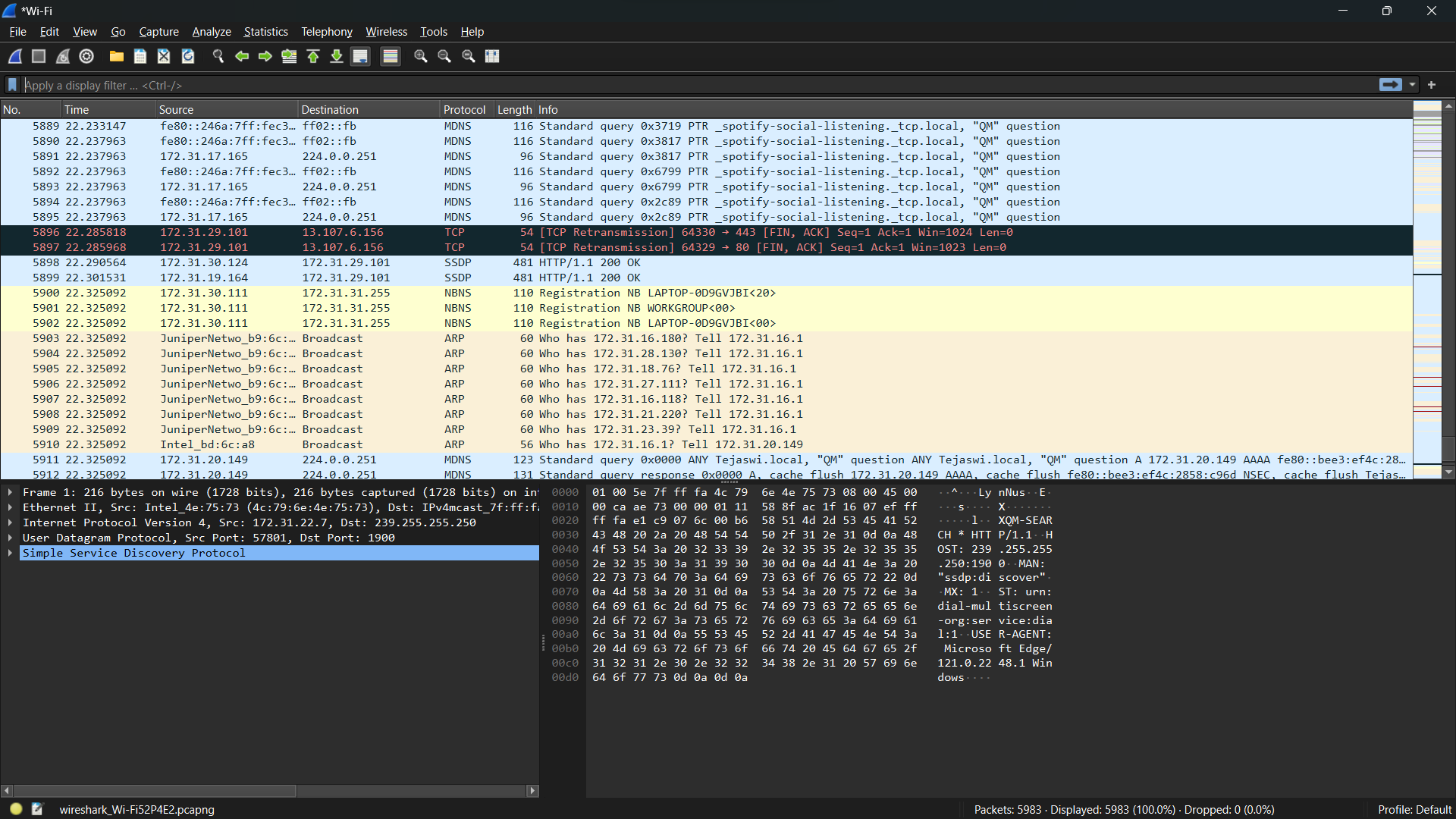
file to the gaia.cs.umass.edu server. Once the file has been uploaded, a short

congratulations message will be displayed in your browser window.

• Stop Wireshark packet capture. Your Wireshark window should look similar to

the window shown below.

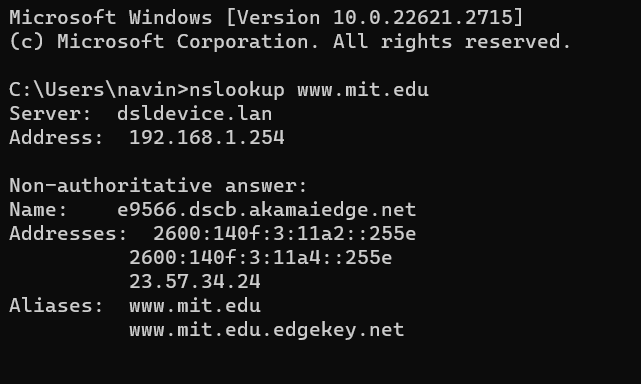
Output:



1. DNS Wireshark:

Consider the first command:

nslookup www.mit.edu



Output in wireshark:

