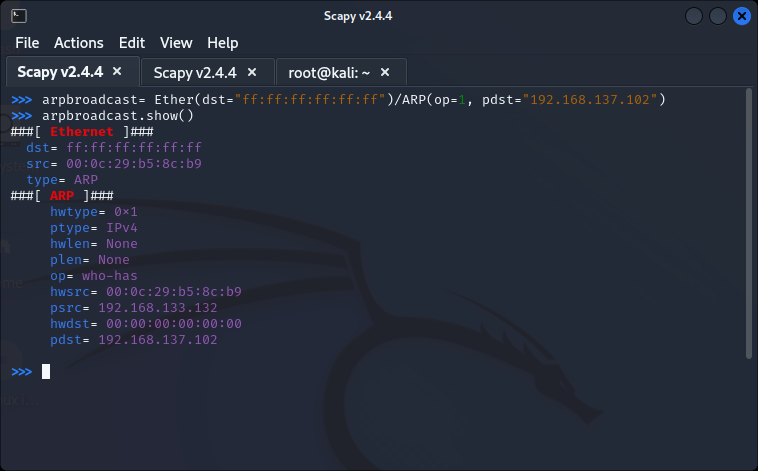
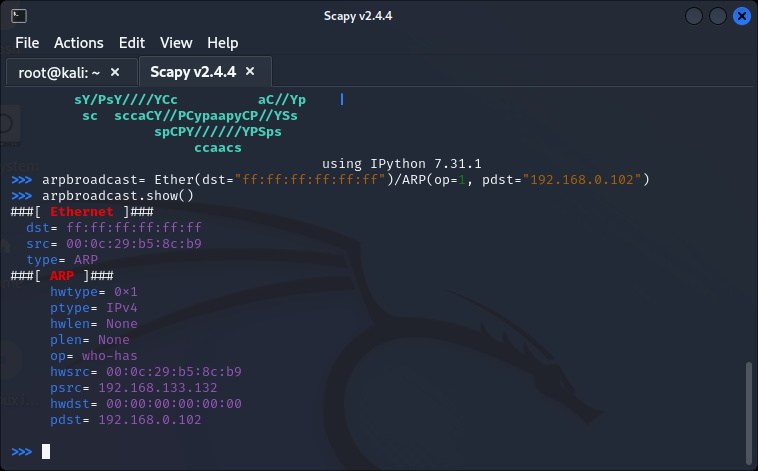
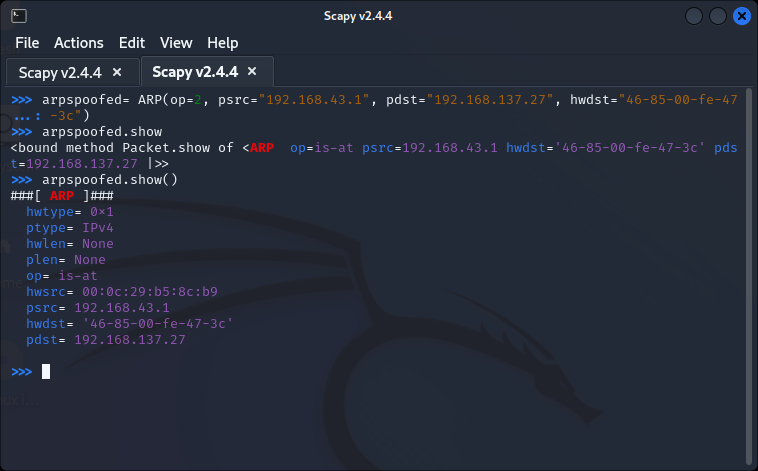


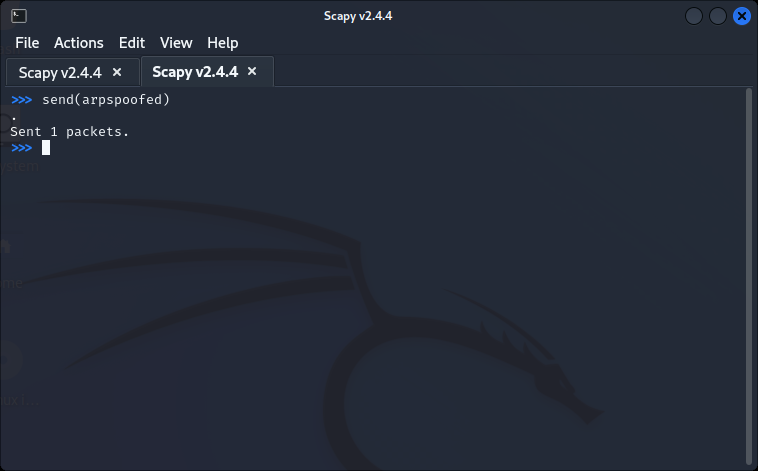
Target:

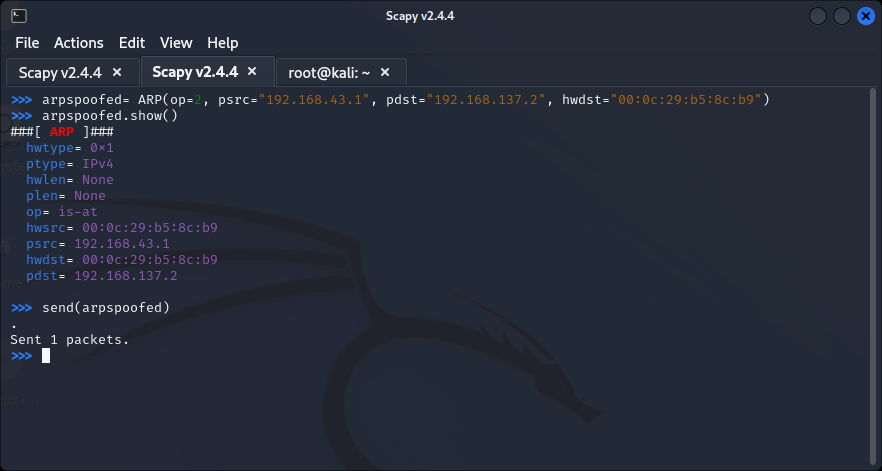




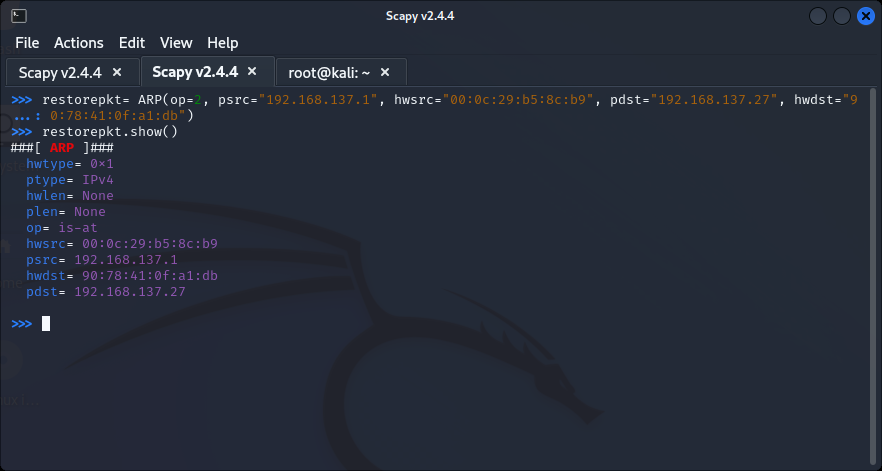
**Part III: Sending false ARP response packets to both the target and the gateway.**

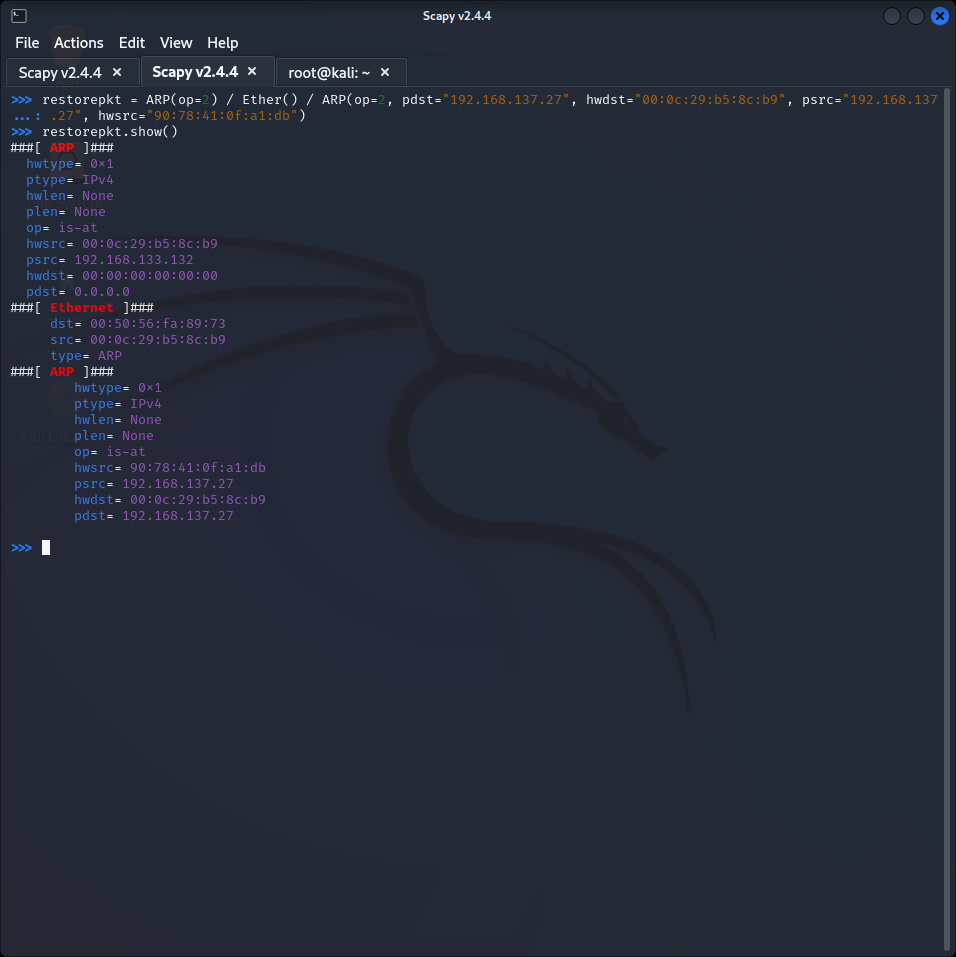






**Part III: Once the attack is done. Remember to restore the ARP tables of the machines.**

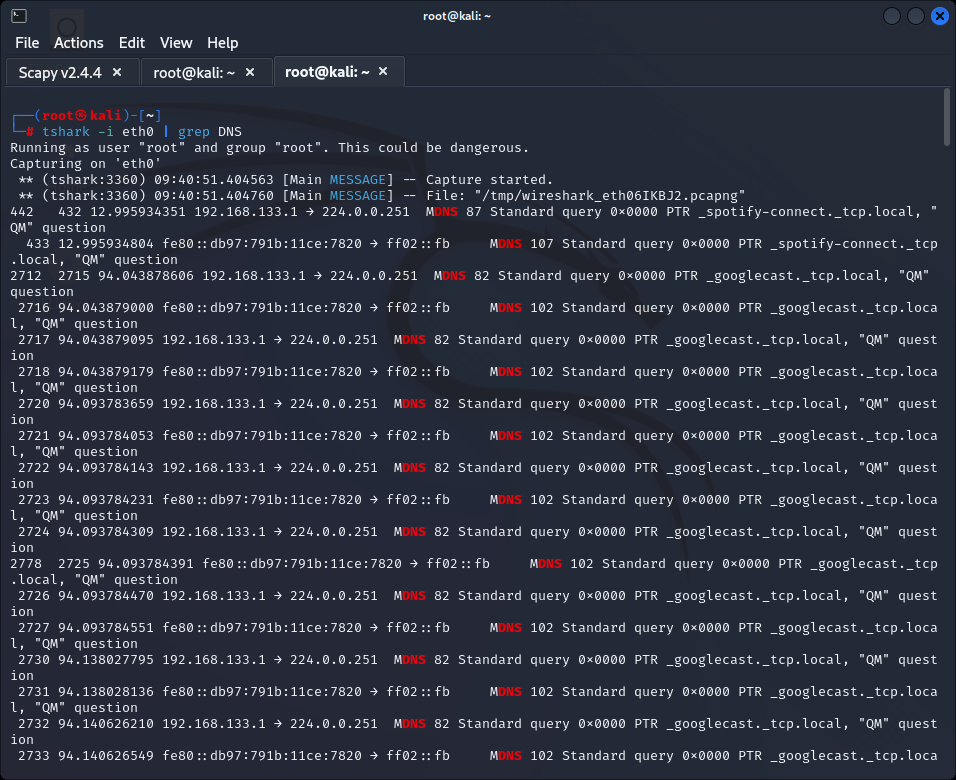




**Part IV: Automate the Whole Process Using Python Script**

**Step 1:** Create this python script:

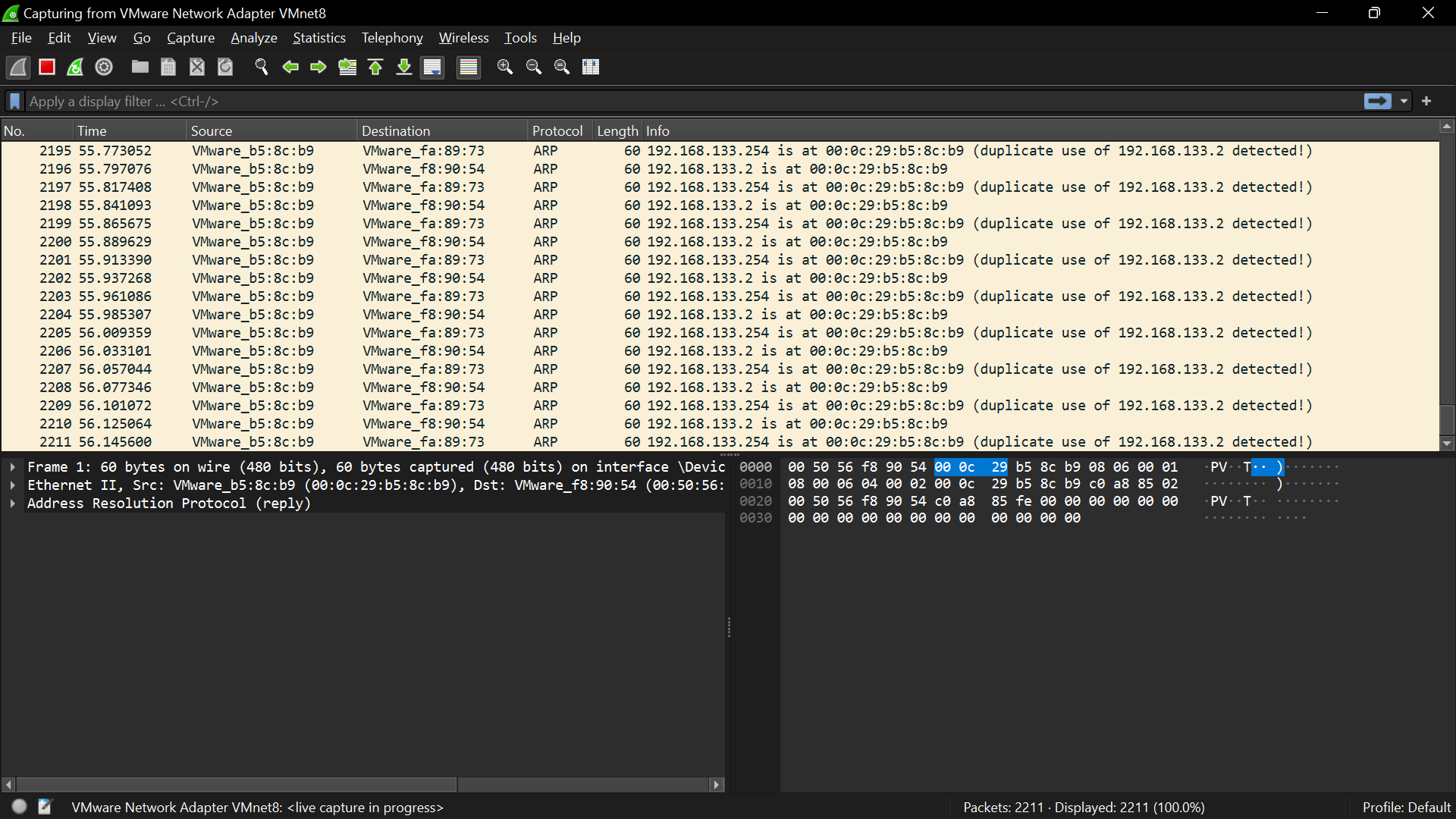
You will also notice that the MITM is also working, if you does **tshark -i <interface> | grep DNS**, on the attacker's machine, one can see the DNS requests of the target going through.



**4. Lab Task – 2: Packet sniffing with Wireshark**

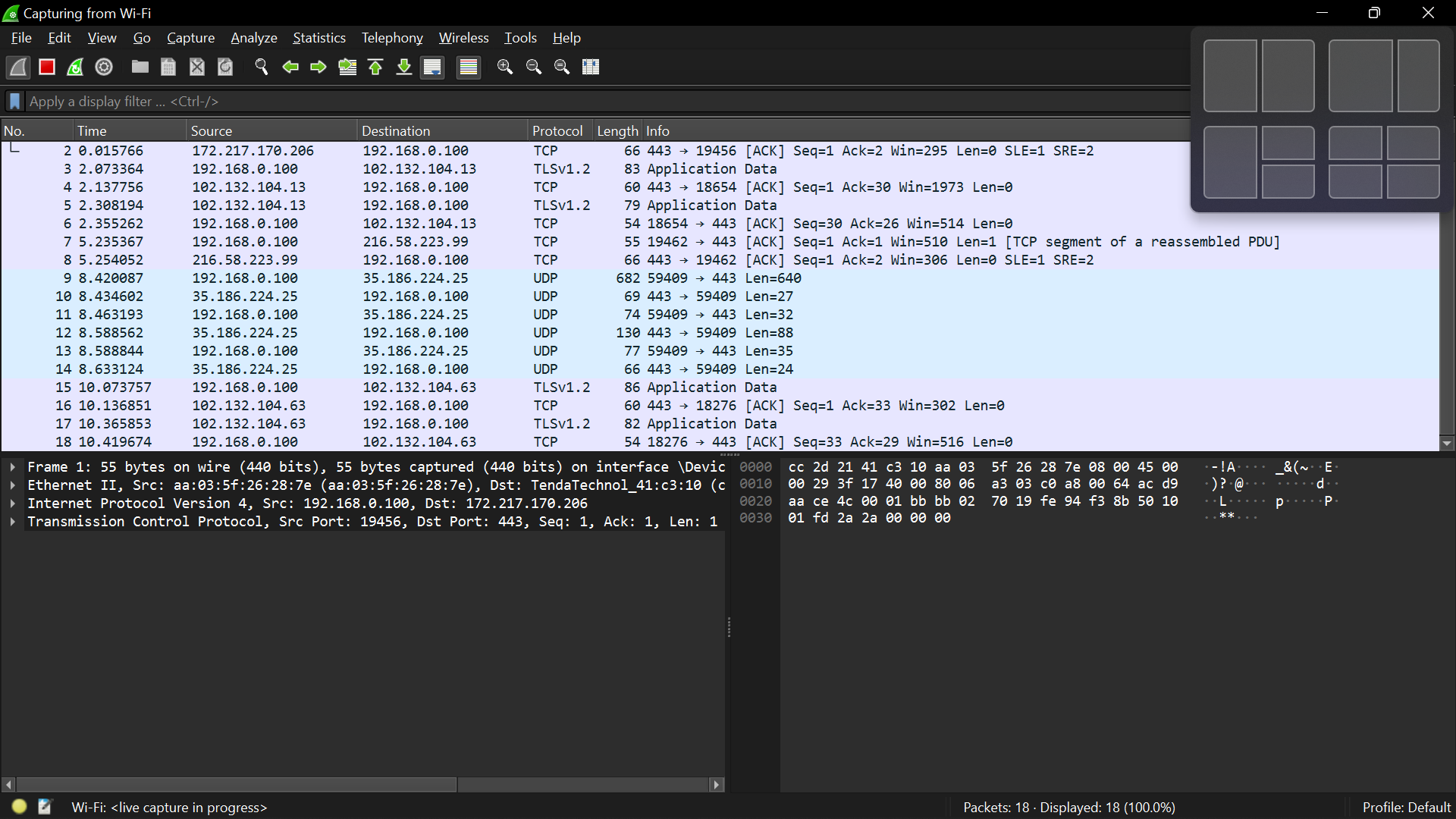
9. Click Interface List. (This will display a list of all available network interfaces on your computer. You will want to want to note the description and IP address of the interface with the most traffic. You will need to select this interface in the following steps.)

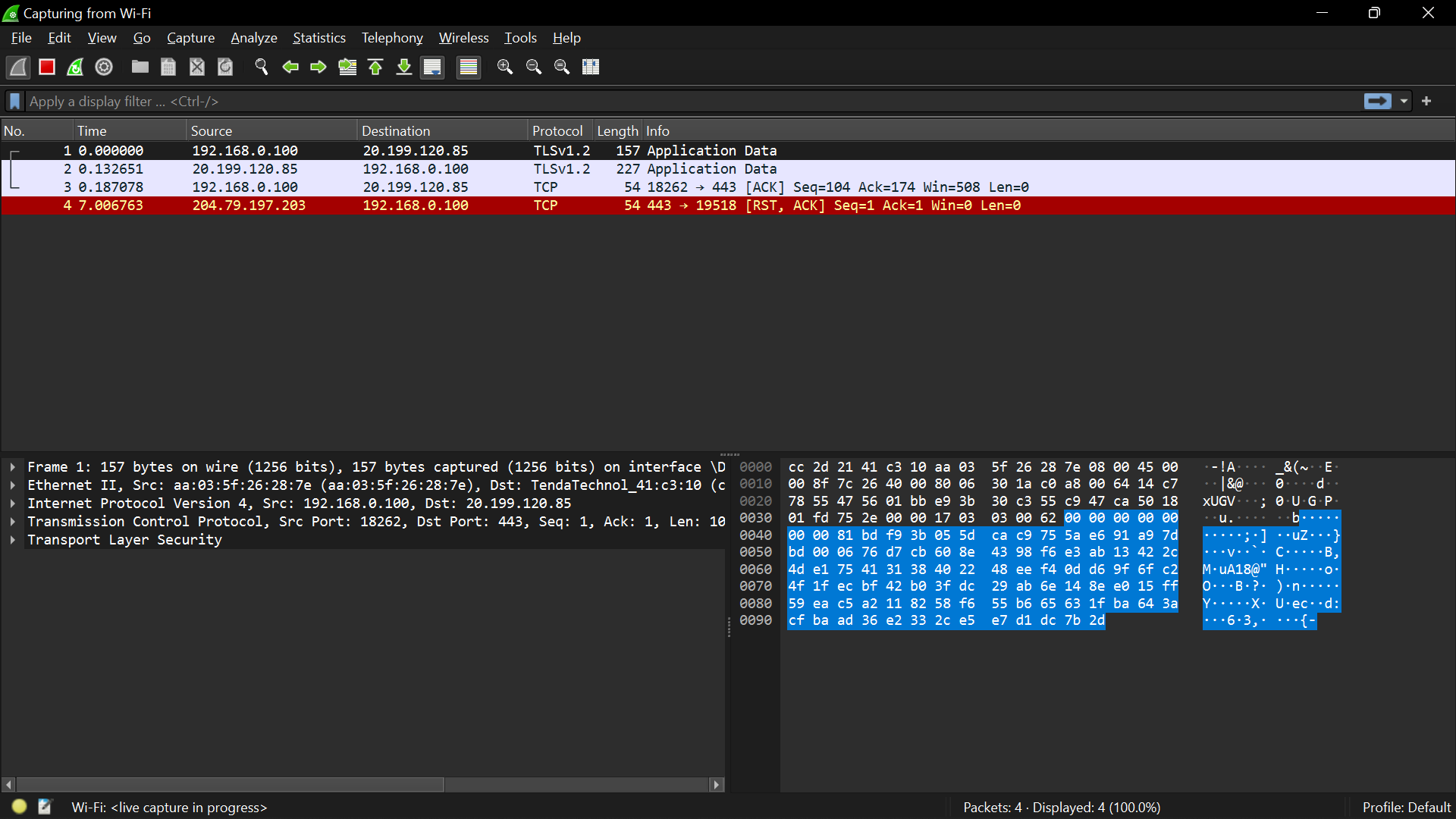
10. Note the interface with the most traffic. (You will select this interface in the following steps. If there are duplicate names for the Network Interface Card (NIC), you can use the last three or four values of the MAC address to identify the appropriate NIC.)

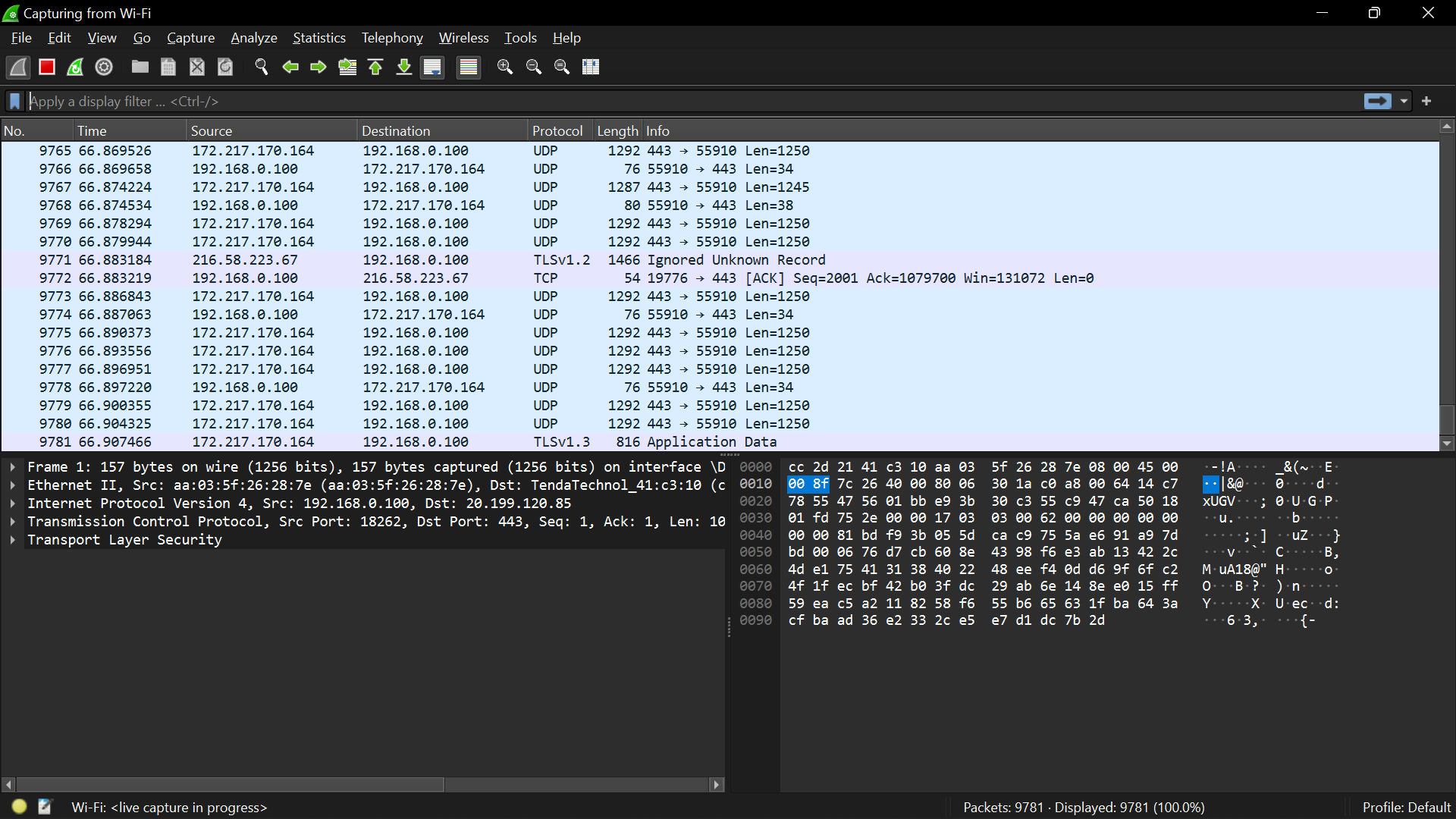


13. Select your Network Interface Card if it is not already selected.

14. Take a screenshot.







16. Click Start.

17. Let it run for 10 seconds.

18. While you are waiting open a web browser and go to www.google.com.

19. Return to your Wireshark window.

20. In the file menu click Capture and Stop (or use the keyboard shortcut—Ctrl+E).

21. Scroll up until you see a green and blue area. (These are the packets you captured when you requested Google’s main page.)

