**Computer Networks Laboratory**

**Assignment 2**

Name: Anirban Das Class: BCSE-III  Roll: 001910501077  Group: A3

**Problem Statement:**

Packet tracer and traffic analysis with Wireshark

**OVERVIEW:**

Wireshark is an open-source cross-platform packet capture and analysis tool, with versions for Windows and Linux. The GUI window gives a detailed breakdown of the network protocol stack for each packet, colorizing packet details based on protocol, as well as having functionality to filter and search the traffic, and pick out TCP streams. Wireshark can also save packet data to files for offline analysis and export/import packet captures to/from other tools. Statistics can also be generated for packet capture files.

**SYSTEM DETAILS:**

OS: 64-bit Windows 10

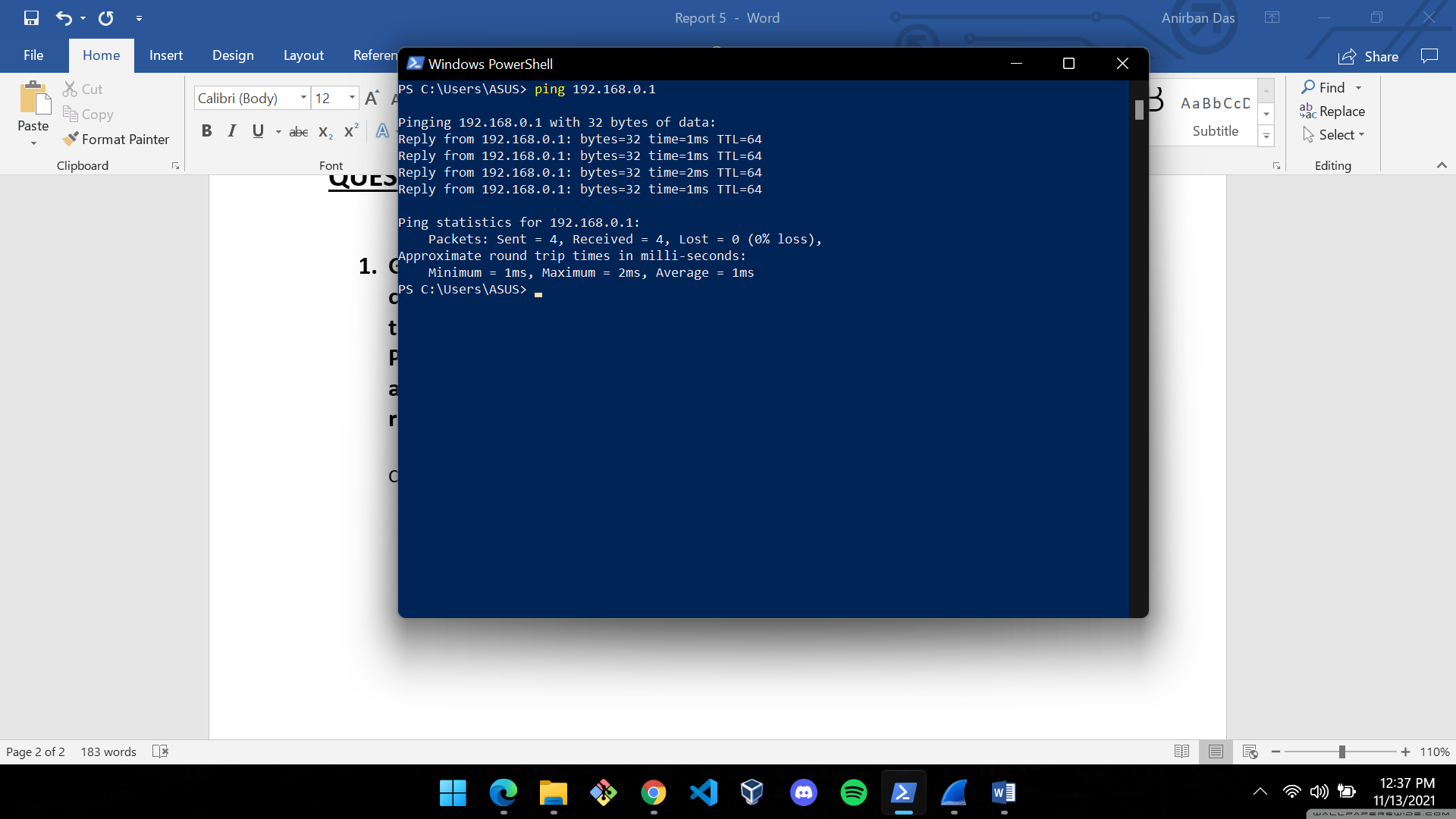
Wireshark Version: 3.4.9

**QUESTIONS:**

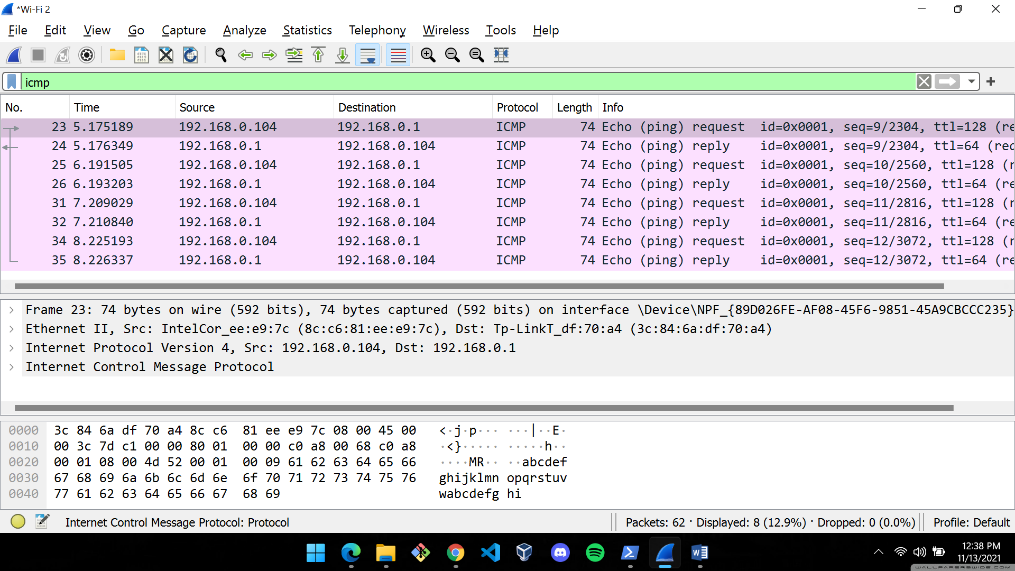
1. **Generate some ICMP traffic by using the Ping command line tool to check the connectivity of a neighbouring machine (or router). Note the results in Wireshark. The initial ARP request broadcast from your PC determines the physical MAC address of the network IP Address, and the ARP reply from the neighboring system. After the ARP**

**request, the pings (ICMP echo request and replies) can be seen.**

COMMAND PROMPT



WIRESHARK CAPTURES



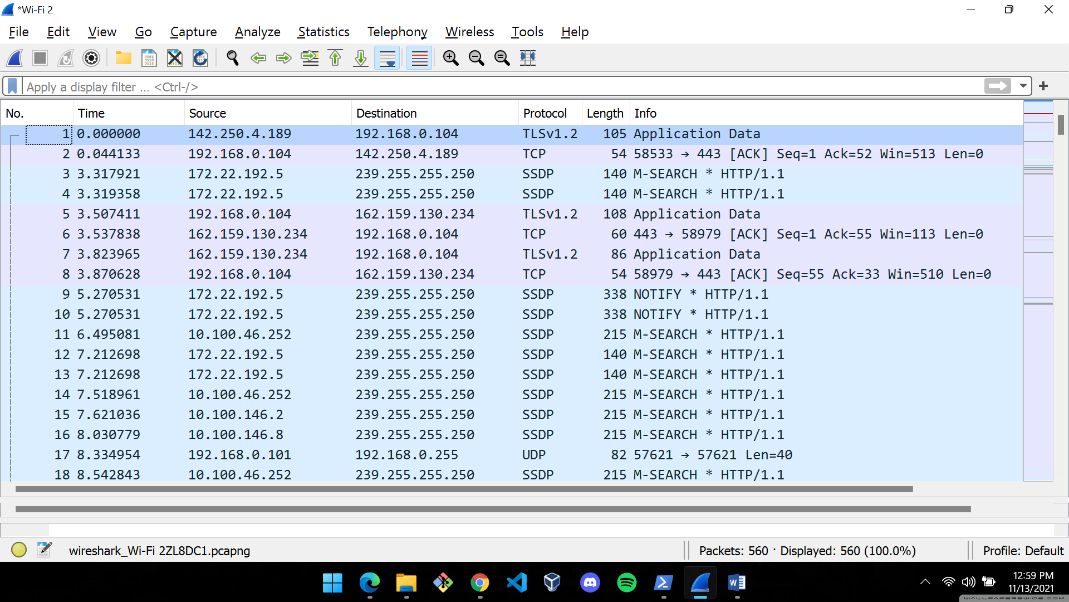
The destination (the default gateway address of my machine) is 192.168.0.1 and the source address (the router ip) is 192.168.0.104.

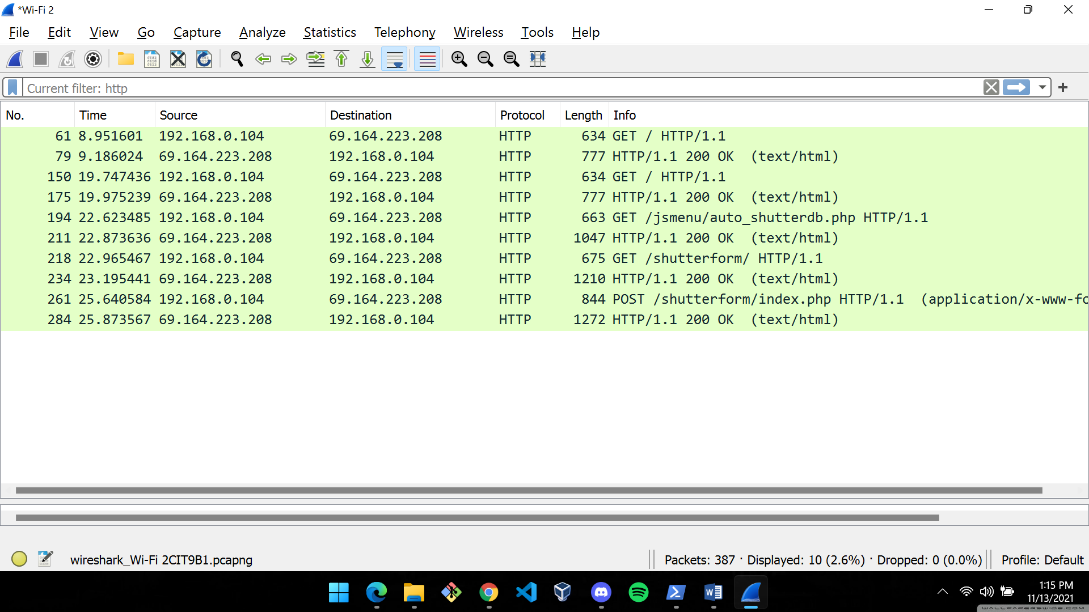
1. **Generate some web traffic and:**
2. **find the list the different protocols that appear in the protocol column in the unfiltered packetlisting window of Wireshark.**
3. **How long did it take from when the HTTP GET message was sent until the HTTP OK reply was received? (By default, the value of 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-ofday).**
4. **What is the Internet address of the website? What is the Internet address of your computer?**
5. **Search back through your capture, and find an HTTP packet containing a GET command. Click on the packet in the Packet List Panel. Then expand the HTTP layer in the Packet Details Panel, from the packet.**
6. **Find out the value of the Host from the Packet Details Panel, within the GET command.**

**ANSWERS:**

1. List of different protocols appearing in the Protocol column:
2. UDP -> User Datagram Protocol
3. TLSv1.3 -> Transport Layer Security (Version 1.3)
4. TCP -> Transmission Control Protocol
5. SSDP -> Multicast DNS
6. QUIC -> Quick UDP Internet Connection
7. DNS -> Domain Name System
8. ARP -> Address Resolution Protocol
9. ICMP -> Internet Control Message Protocol

WIRESHARK CAPTURES

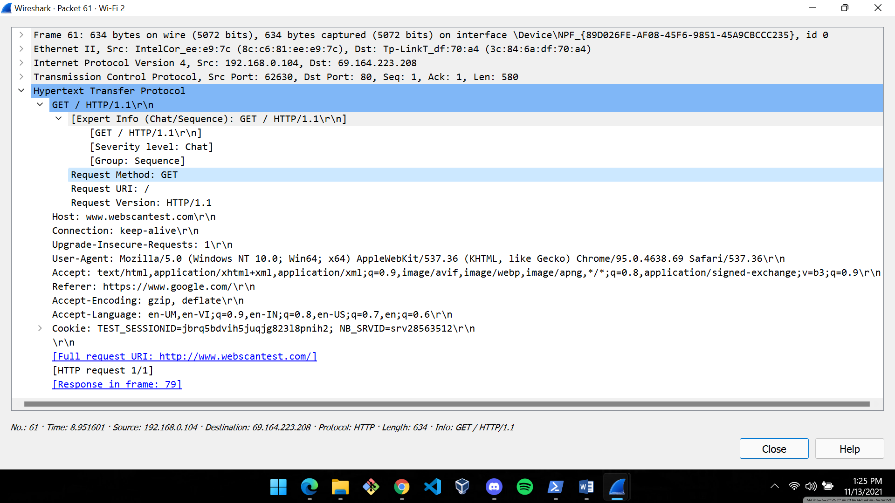




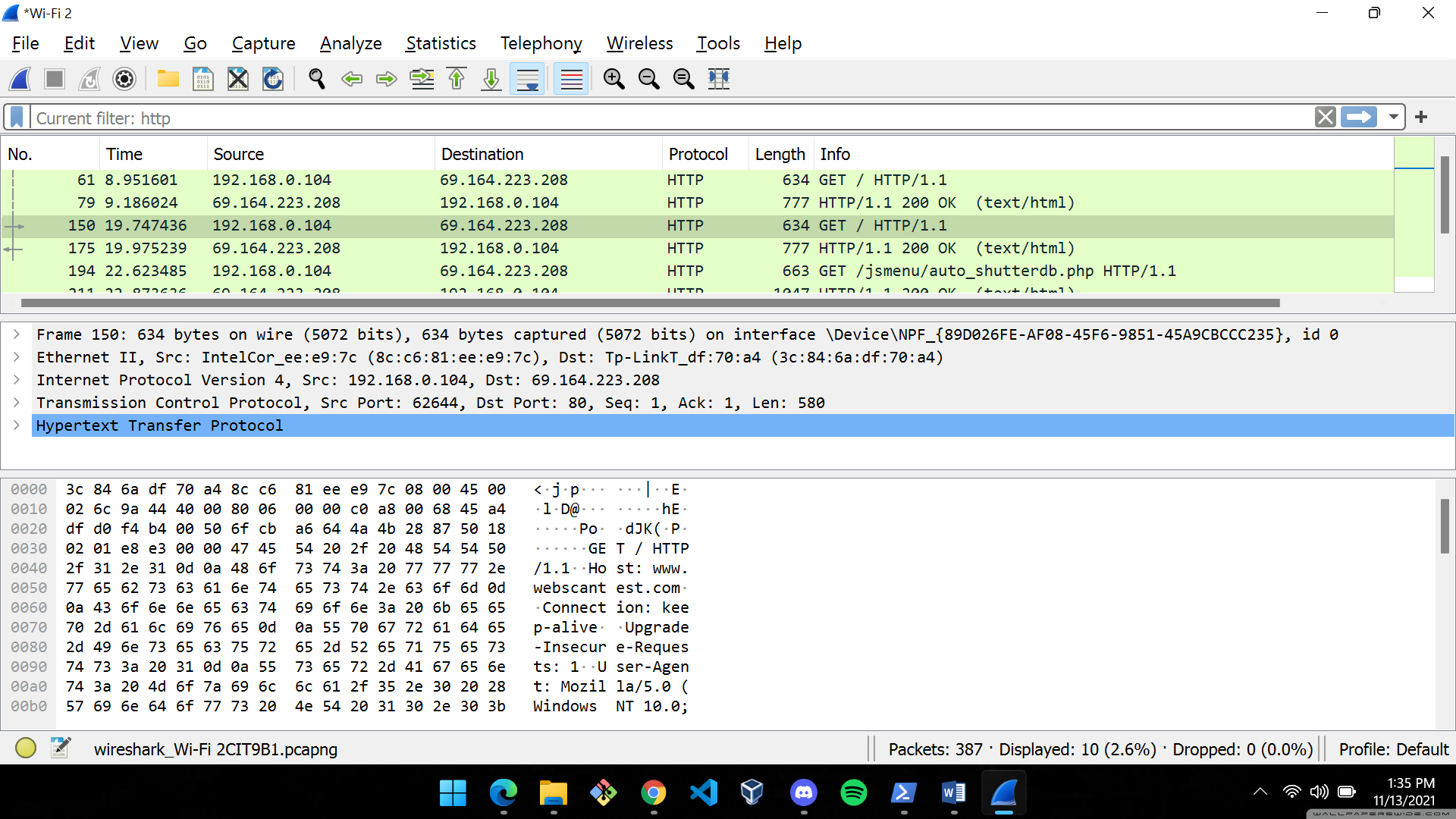
Time taken from when HTTP GET was sent until the receipt of HTTP OK message = 9.186024 – 8.951601 = 0.234423s

1. Internet address of the destination: 69.164.223.208

Internet address of my machine : 192.168.0.104

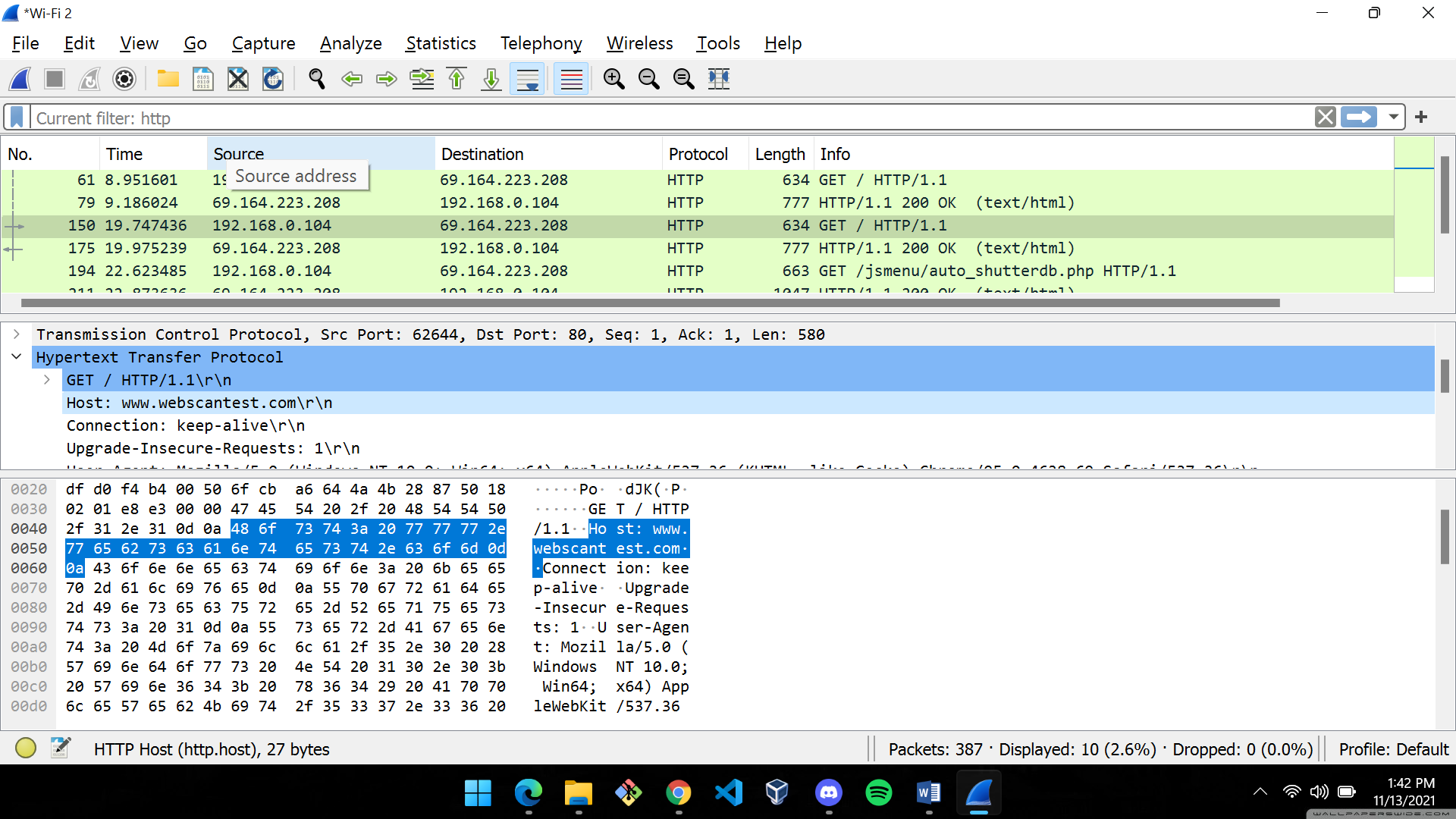


1. The value of the host is “www.webscantest.com\r\n” as seen in the above screenshot.
2. **Highlight the Hex and ASCII representations of the packet in the Packet Bytes Panel.**



**|-------HEX REPRESENTATION------| |----ASCII----|**

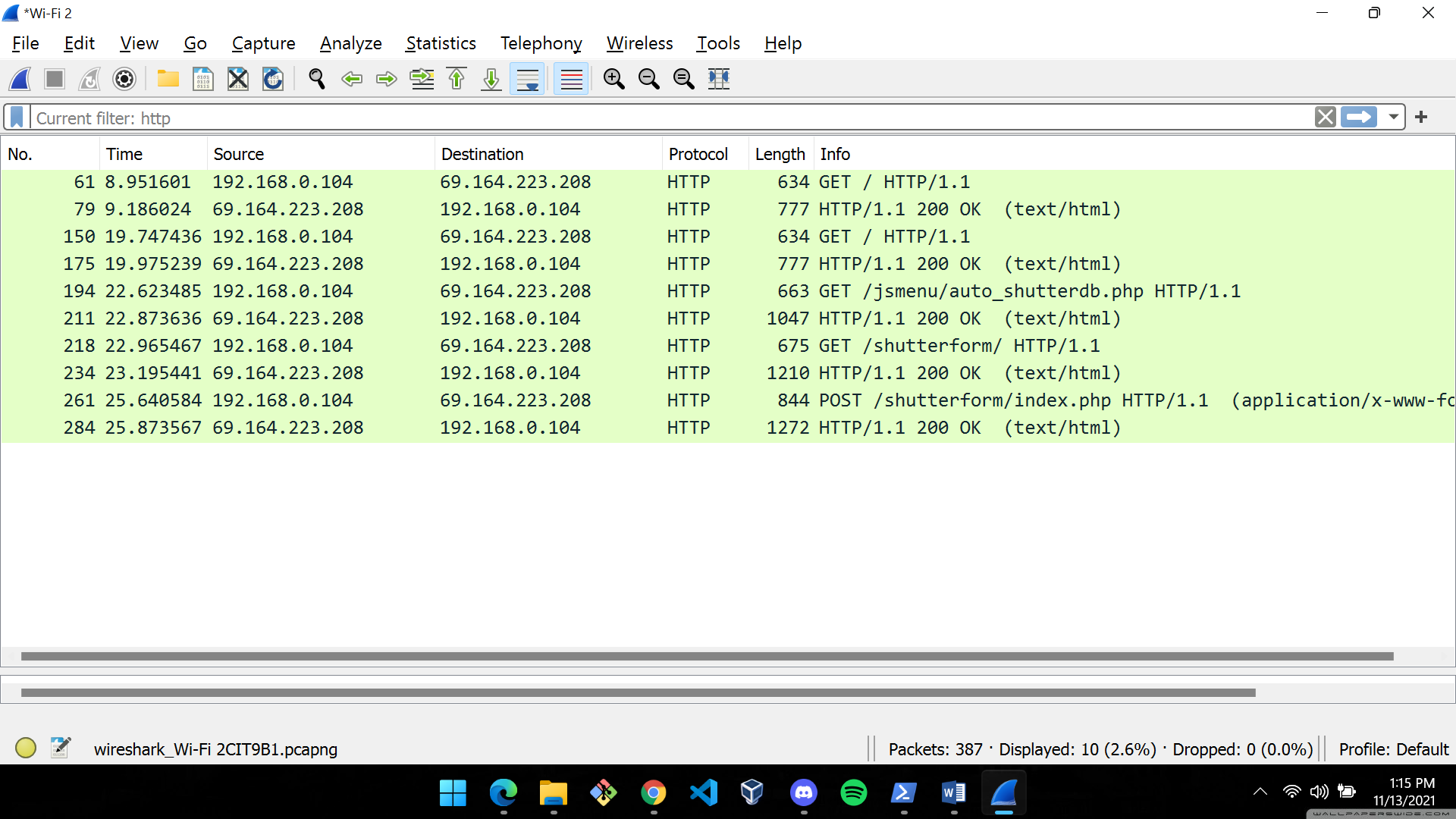
1. **Find out the first 4 bytes of the Hex value of the Host parameter from the Packet Bytes Panel.**



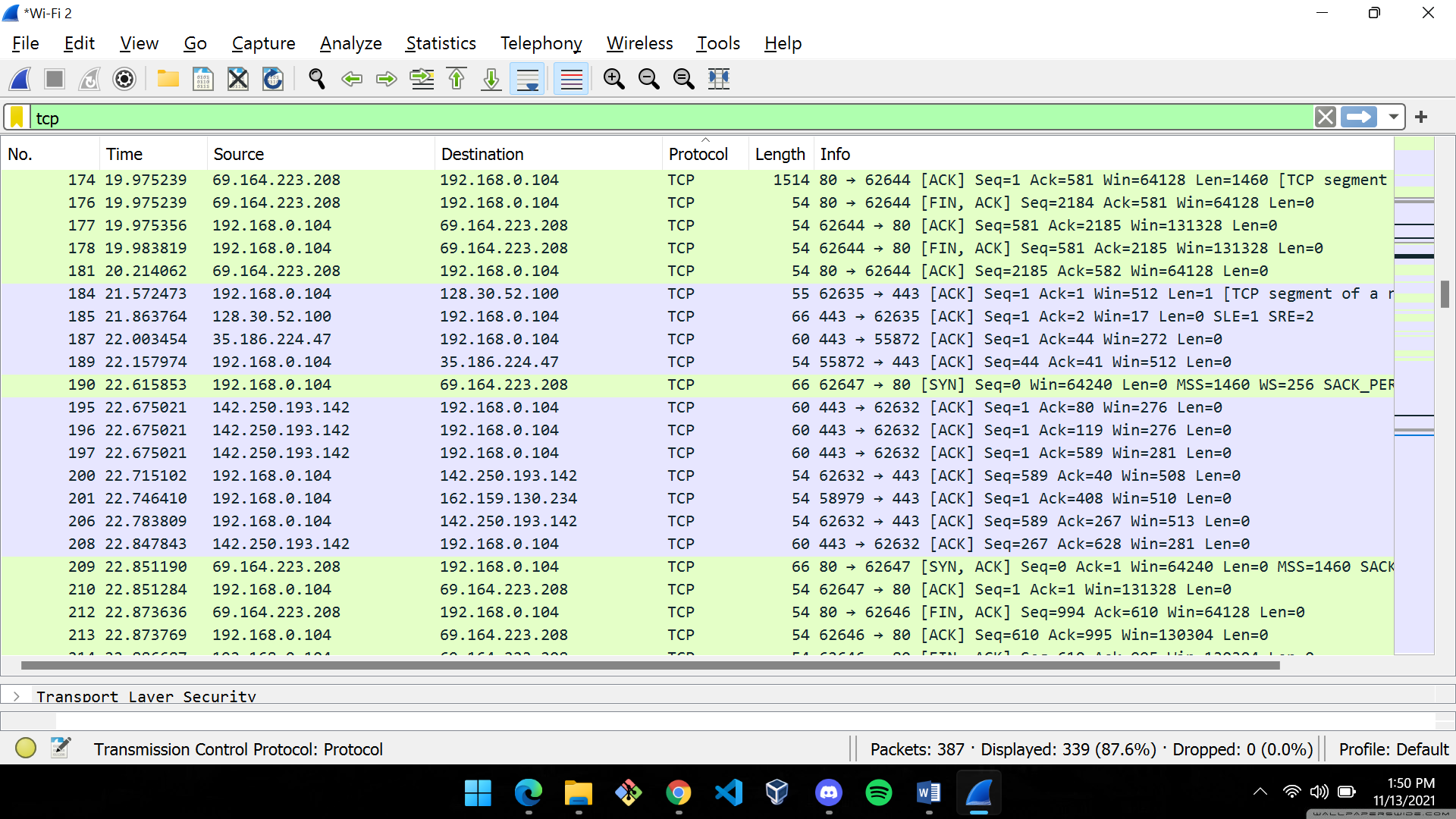
The highlighted portion of the HEX Representation of the packet is for the host parameter. The first 4 bytes are 48 6f 73 74.

1. **Filter packets with http, TCP, DNS and other protocols.**

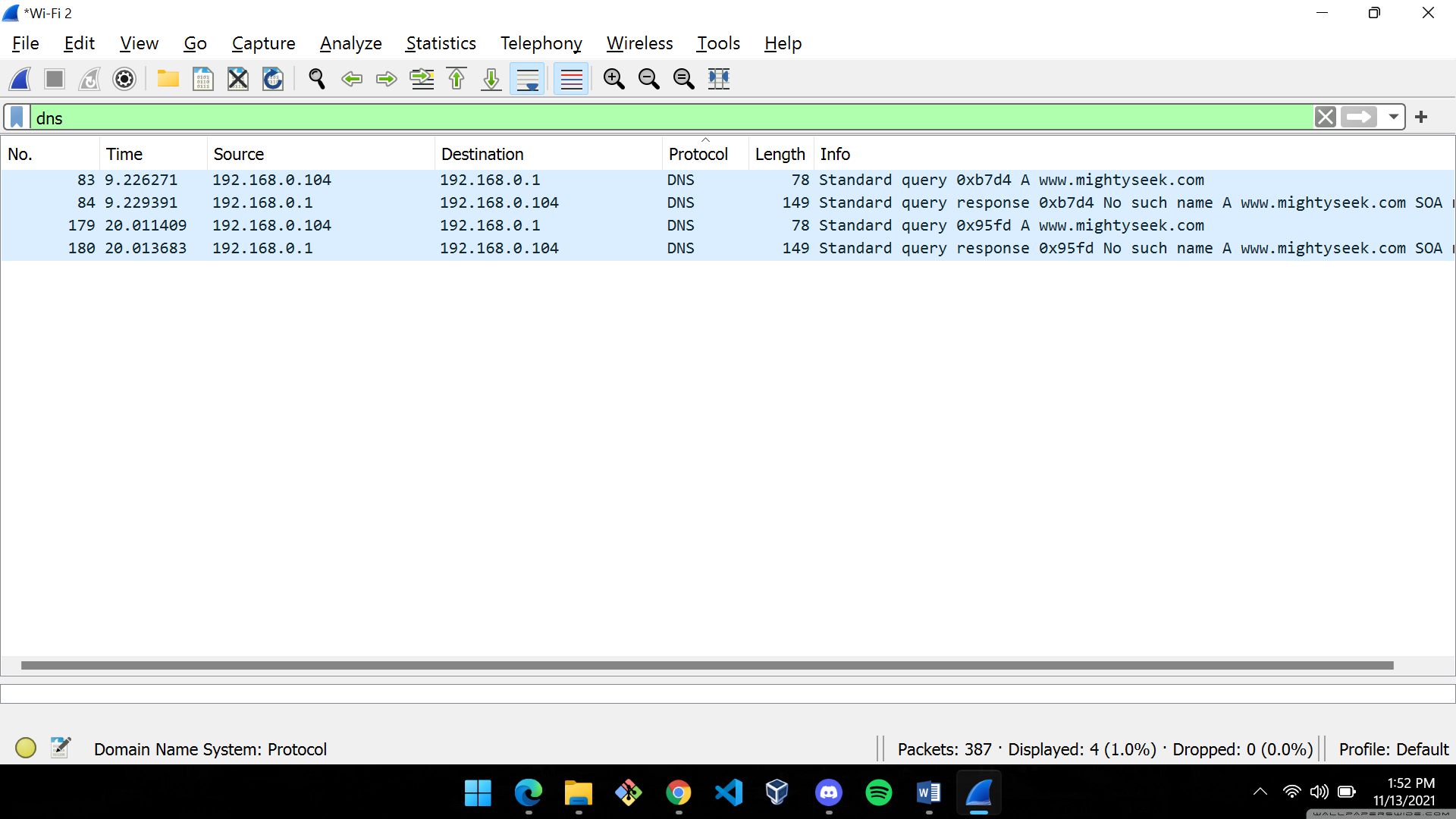
HTTP



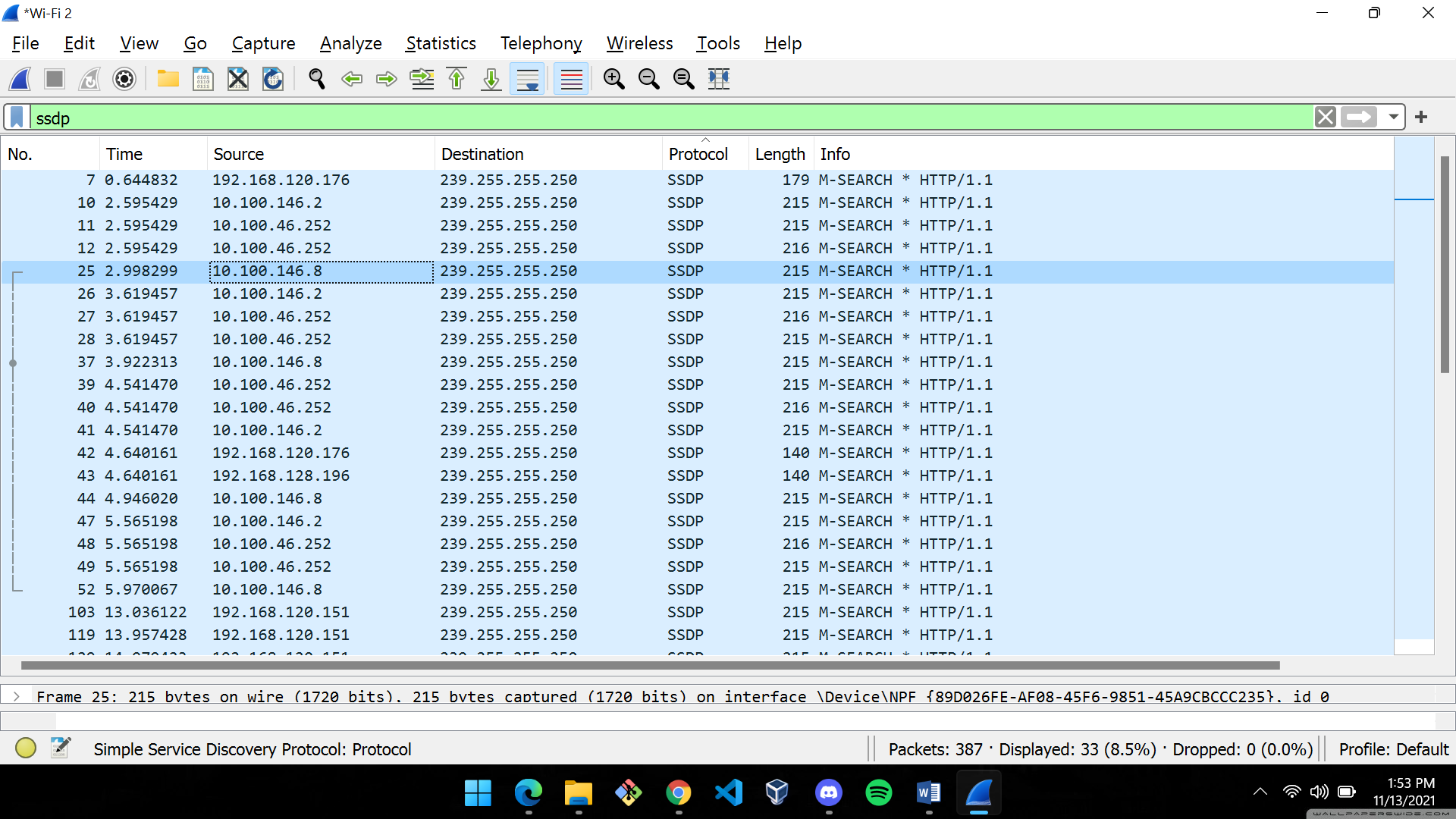
TCP



DNS

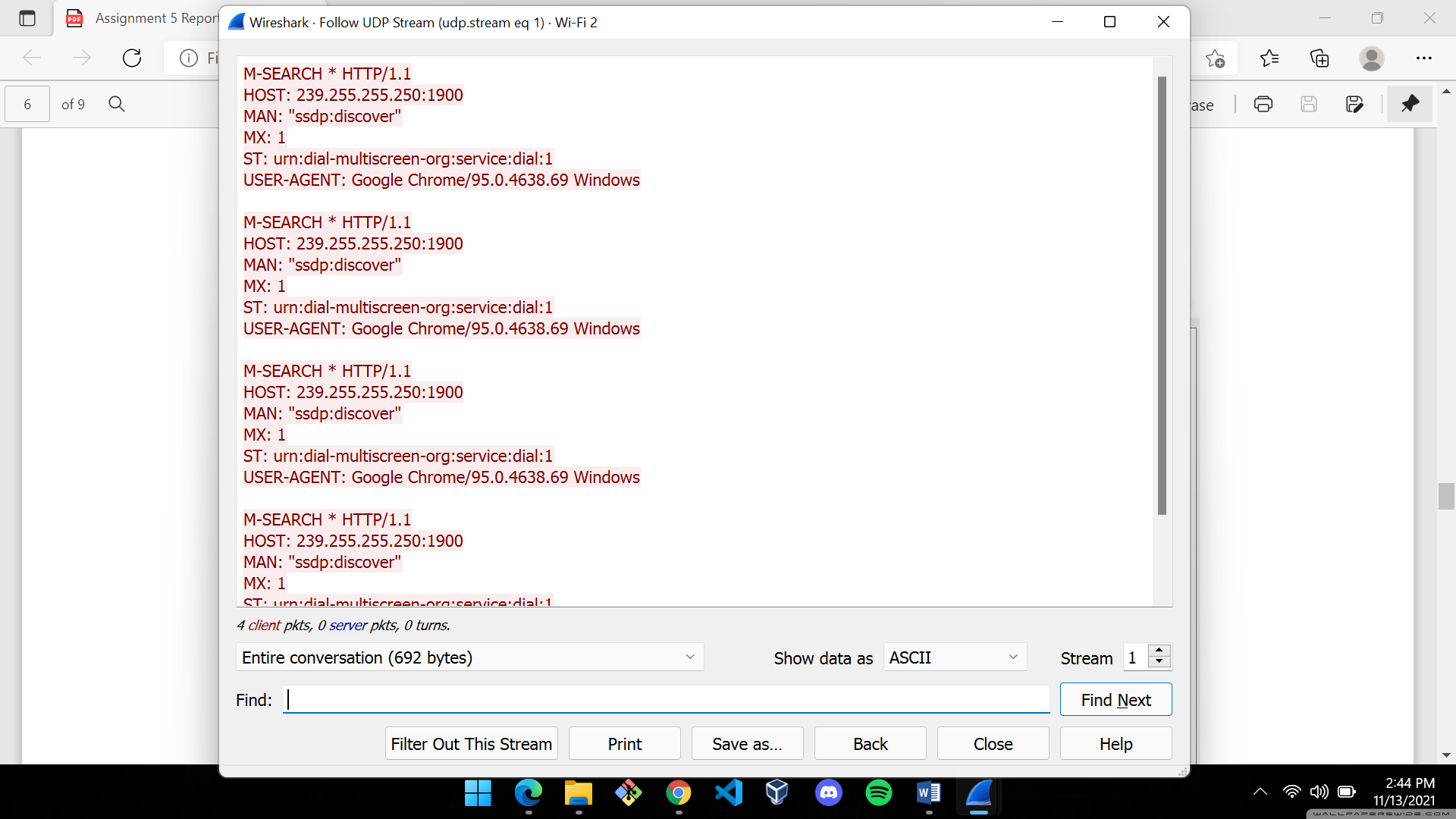


SSDP

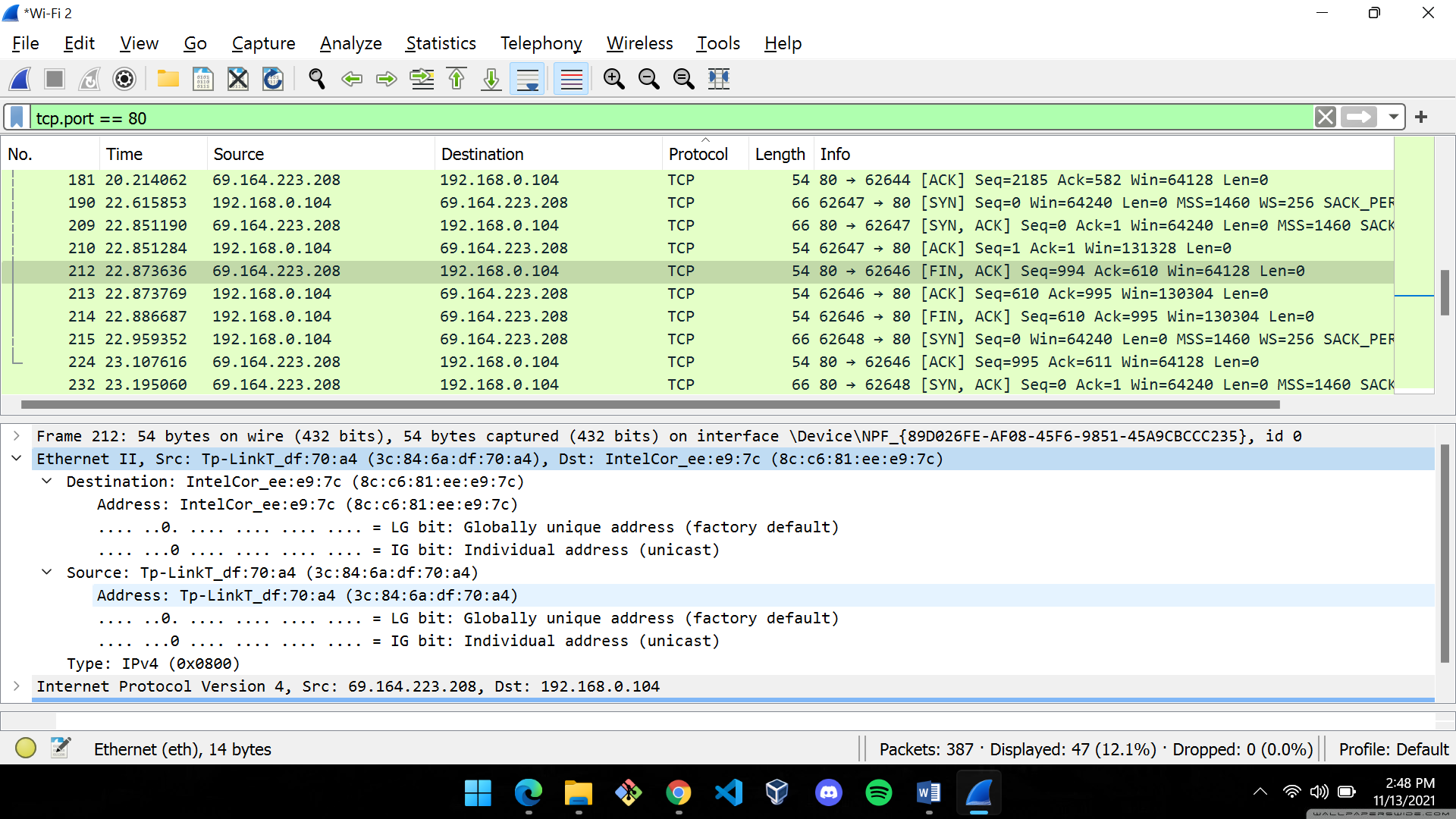


1. **Find out what are those packets contain by following one of the conversations (also called network flows), select one of the packets and press the right mouse button -> click on follow.**

Clicking on SSDP packet and following UDP stream

****

1. **Search through your capture, and find an HTTP packet coming back from the server (TCP Source Port == 80). Expand the Ethernet layer in the Packet Details Panel.**

****

Packet 212 is an HTTP packet coming back from the server (tcp source port ==80)

1. **What are the manufacturers of your PC’s Network Interface Card (NIC), and the servers NIC?**

Manufacturer of my PC’s Network Interface Card (NIC)

**IntelCor**

**MAC Address: 8c:c6:81:ee:e9:7c**

Manufacturer of my PC’s Network Interface Card (NIC)

**Tp-LinkT**

**MAC Address: 3c:84:6a:df:70:a4**

1. **What are the Hex values (shown the raw bytes panel) of the two NICS Manufacturers OUIs?**

PC: **ee:e9:7c**

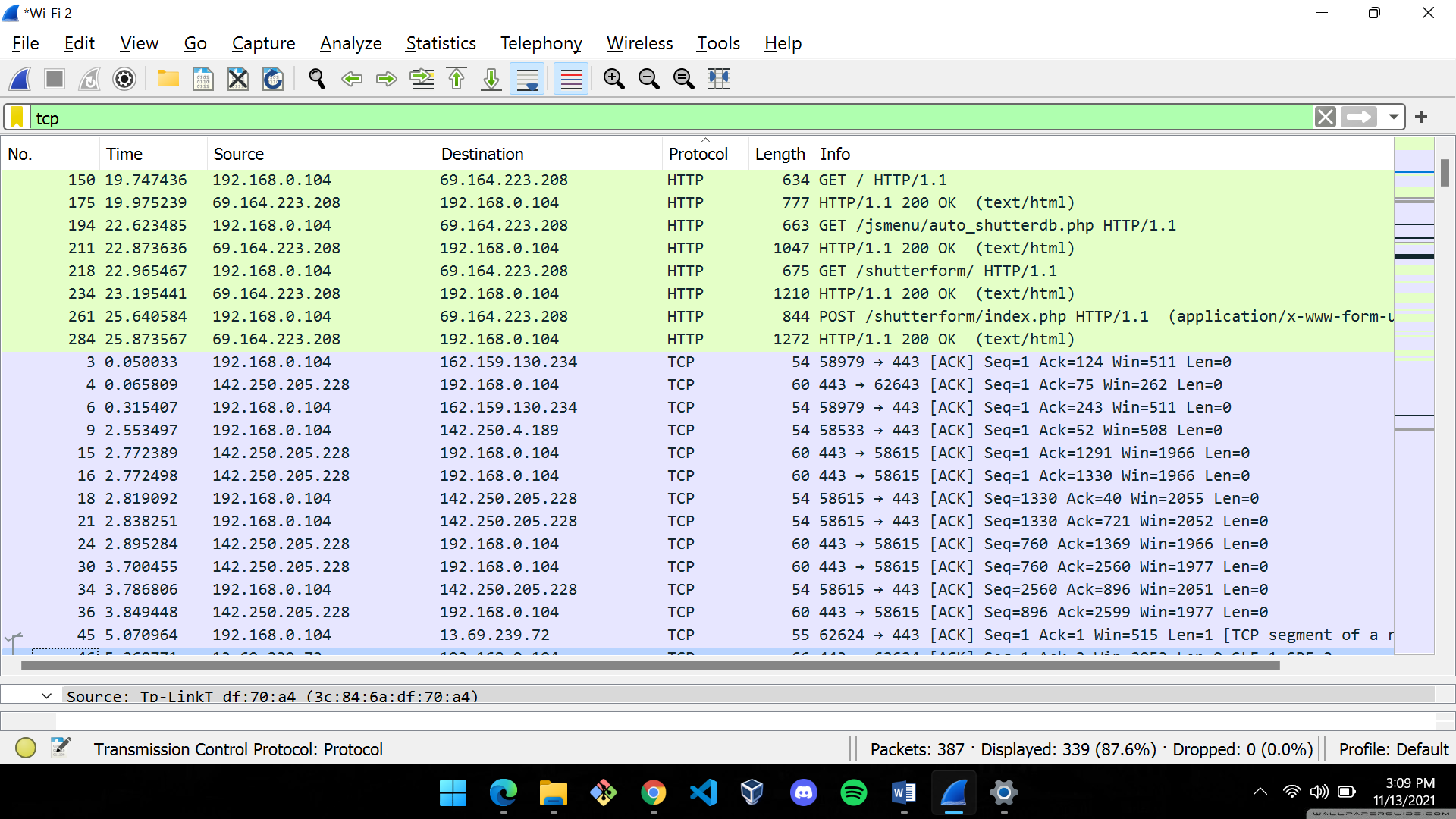
Server: **df:70:a4**

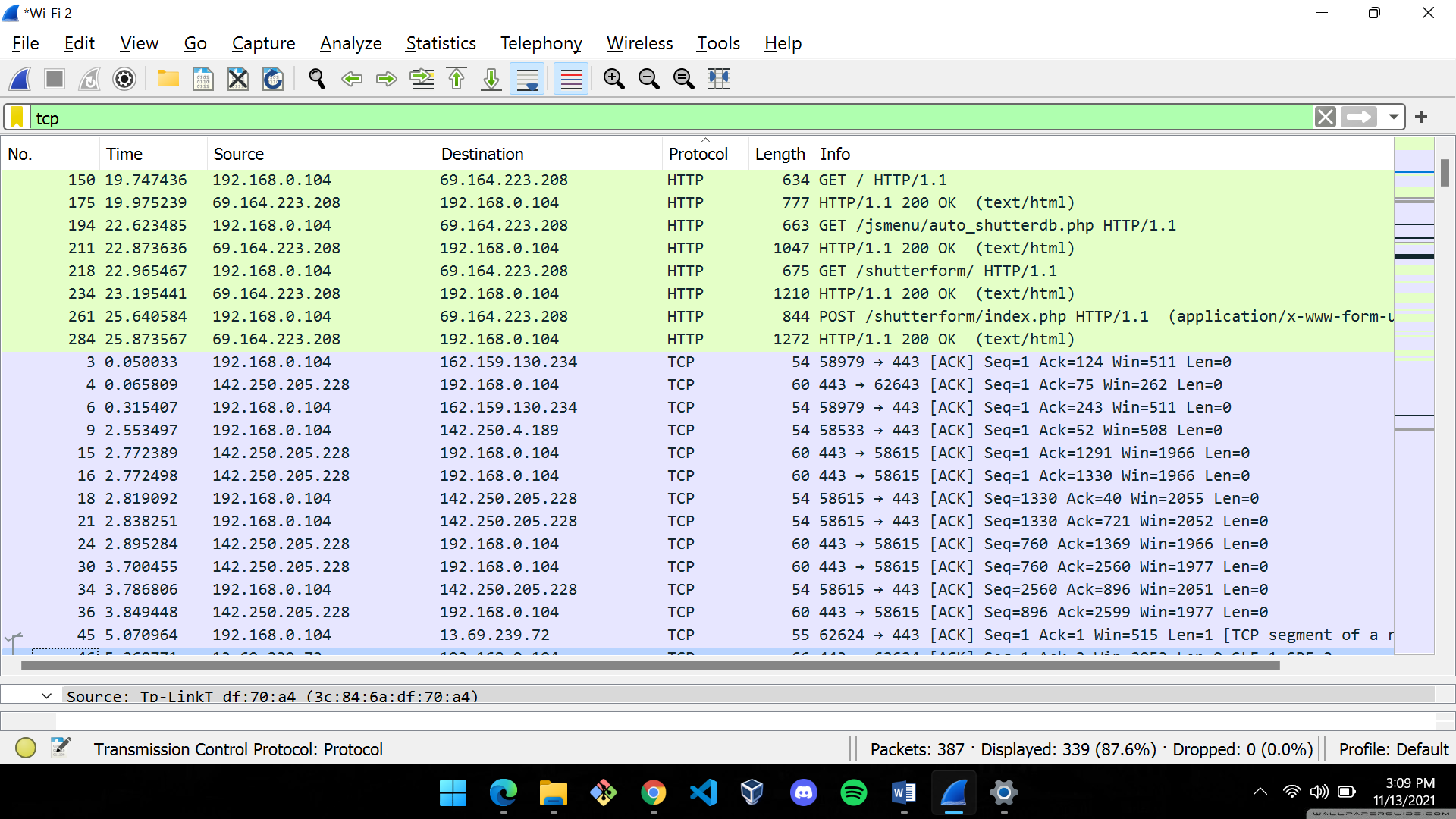
1. **Find the following statistics:**
2. **What percentage of packets in your capture are TCP, and give an example of the higher level protocol which uses TCP?**

**b. What percentage of packets in your capture are UDP, and give an example of the higher level protocol which uses UDP?**

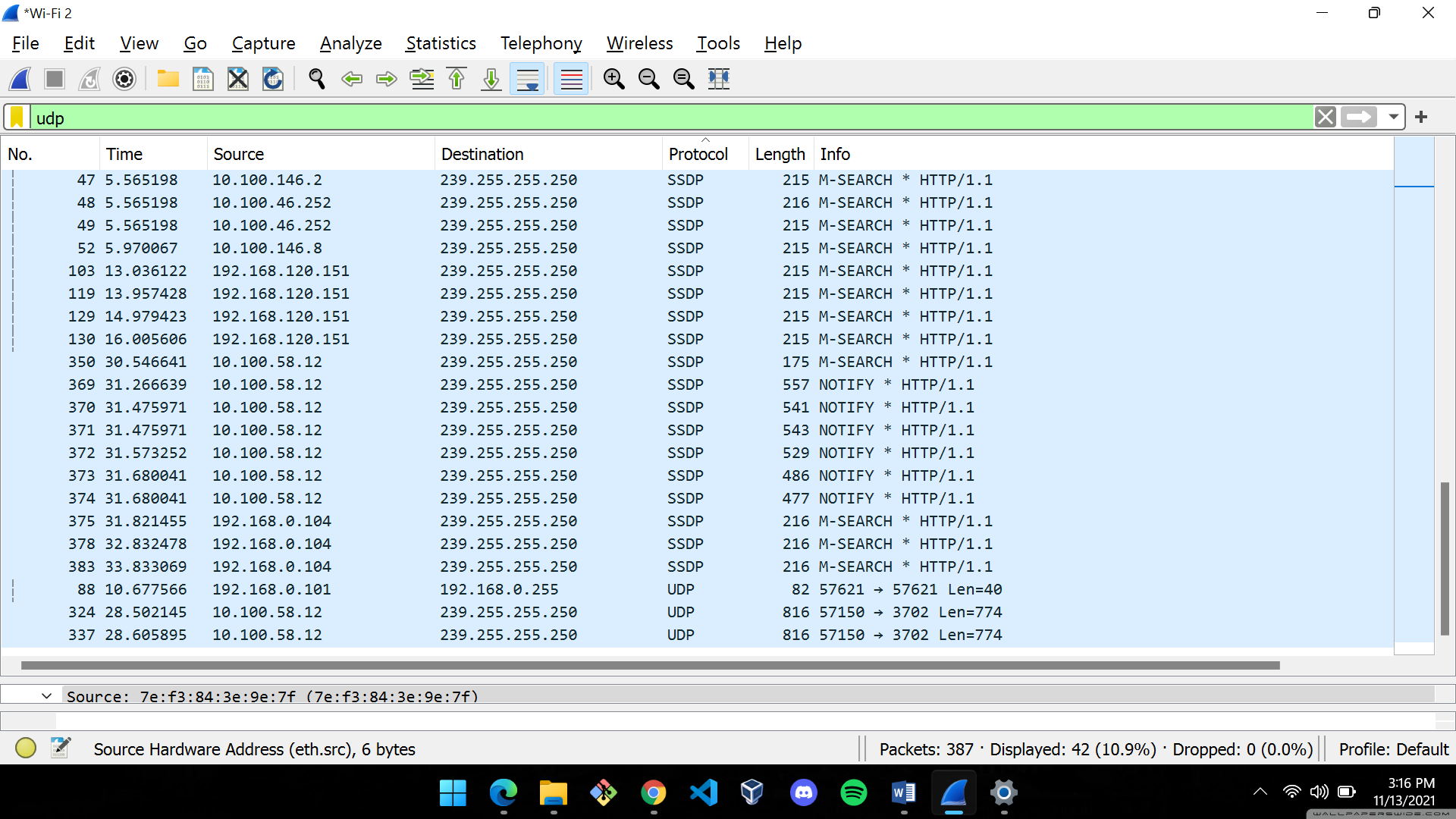
ANSWERS

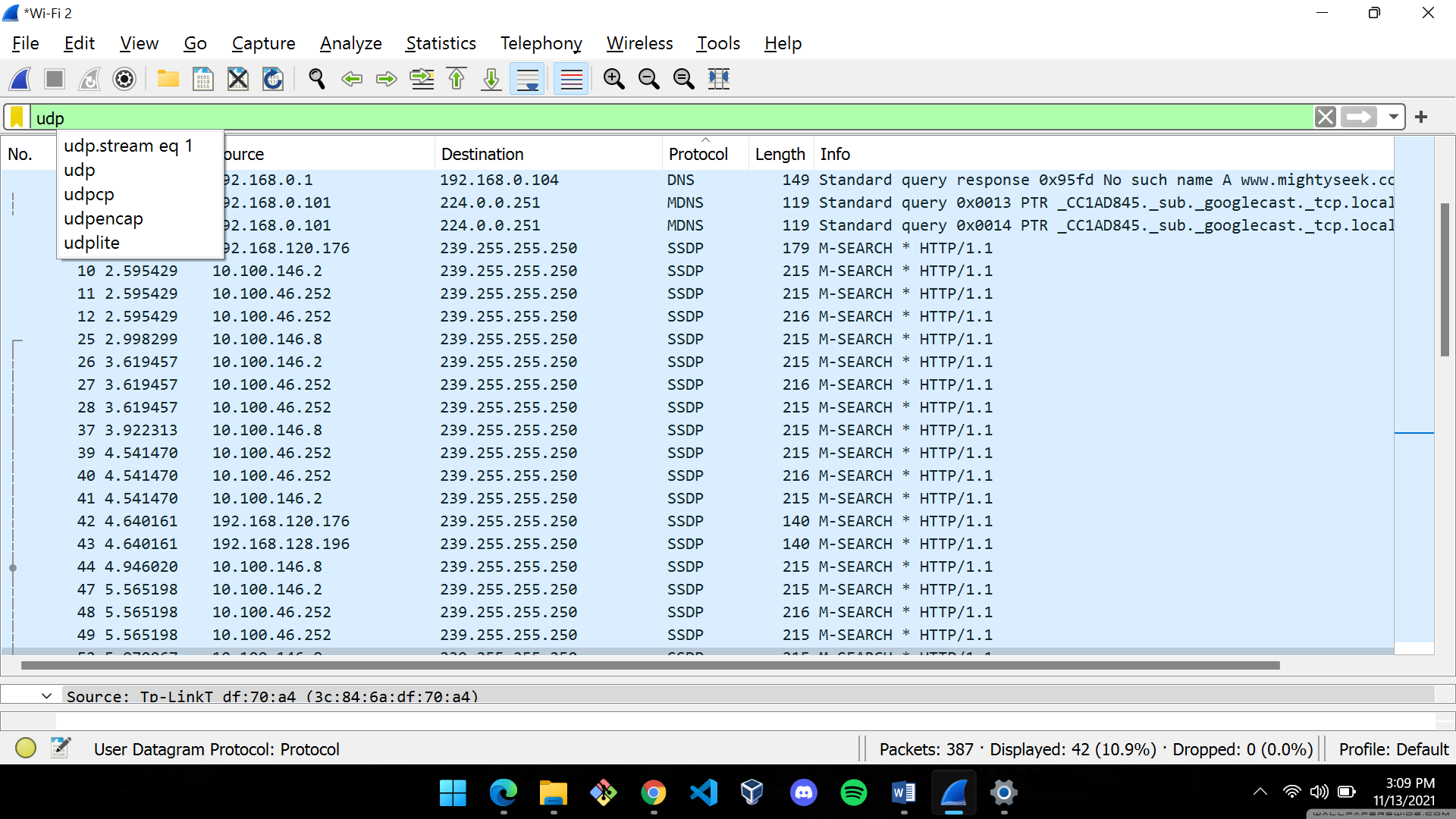
1. Out of 387 packets captured, 339 were TCP packets, i.e., TCP packets accounted for 87.6% of the total packets captured. HTTP (Hypertext Transfer Protocol) uses TCP.





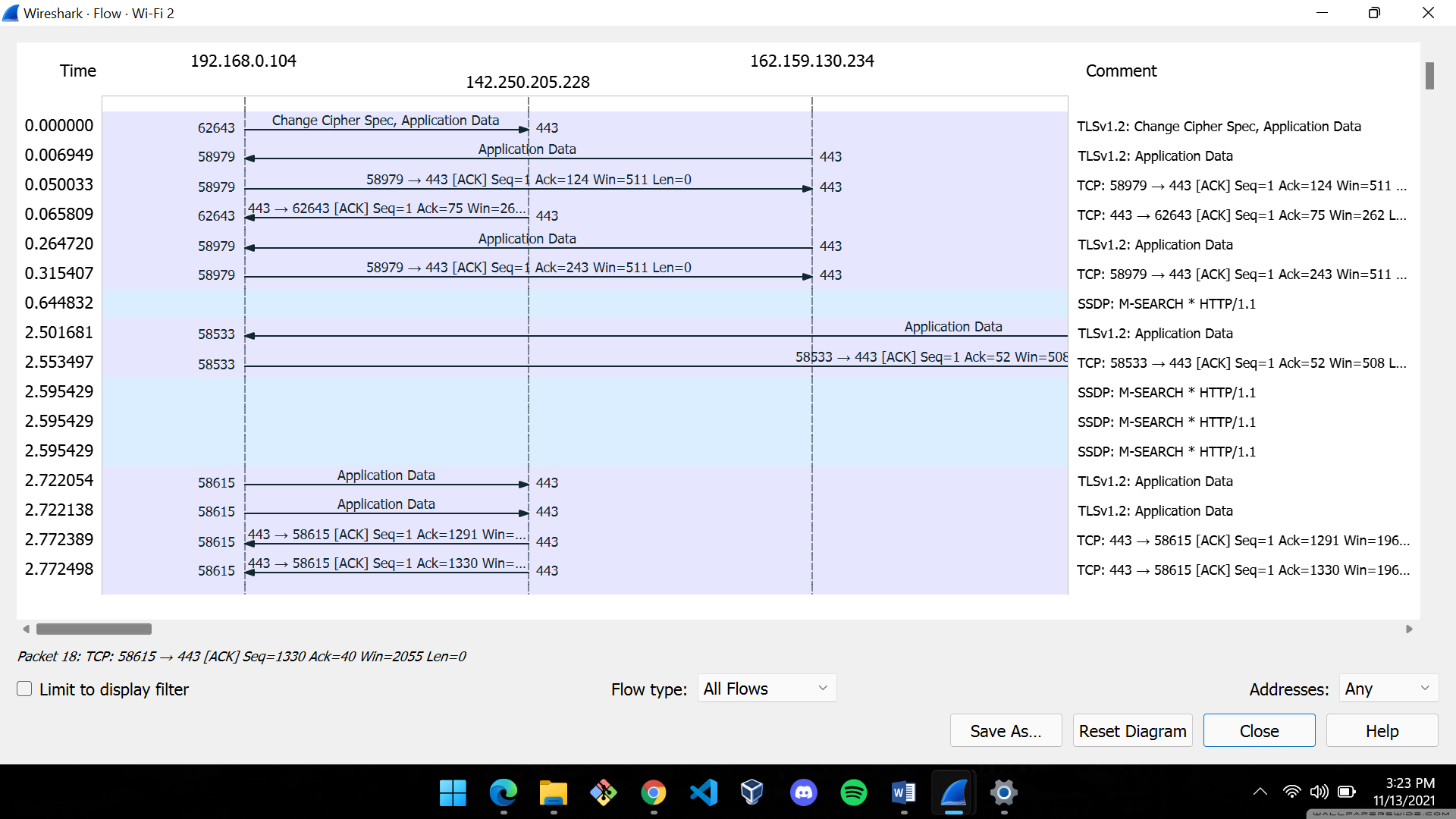
1. Out of 387 packets captured, 42 were UDP packets, i.e., UDP packets accounted for 10.9% of the total packets captured. SSDP (Simple Service Discovery Protocol) uses UDP.

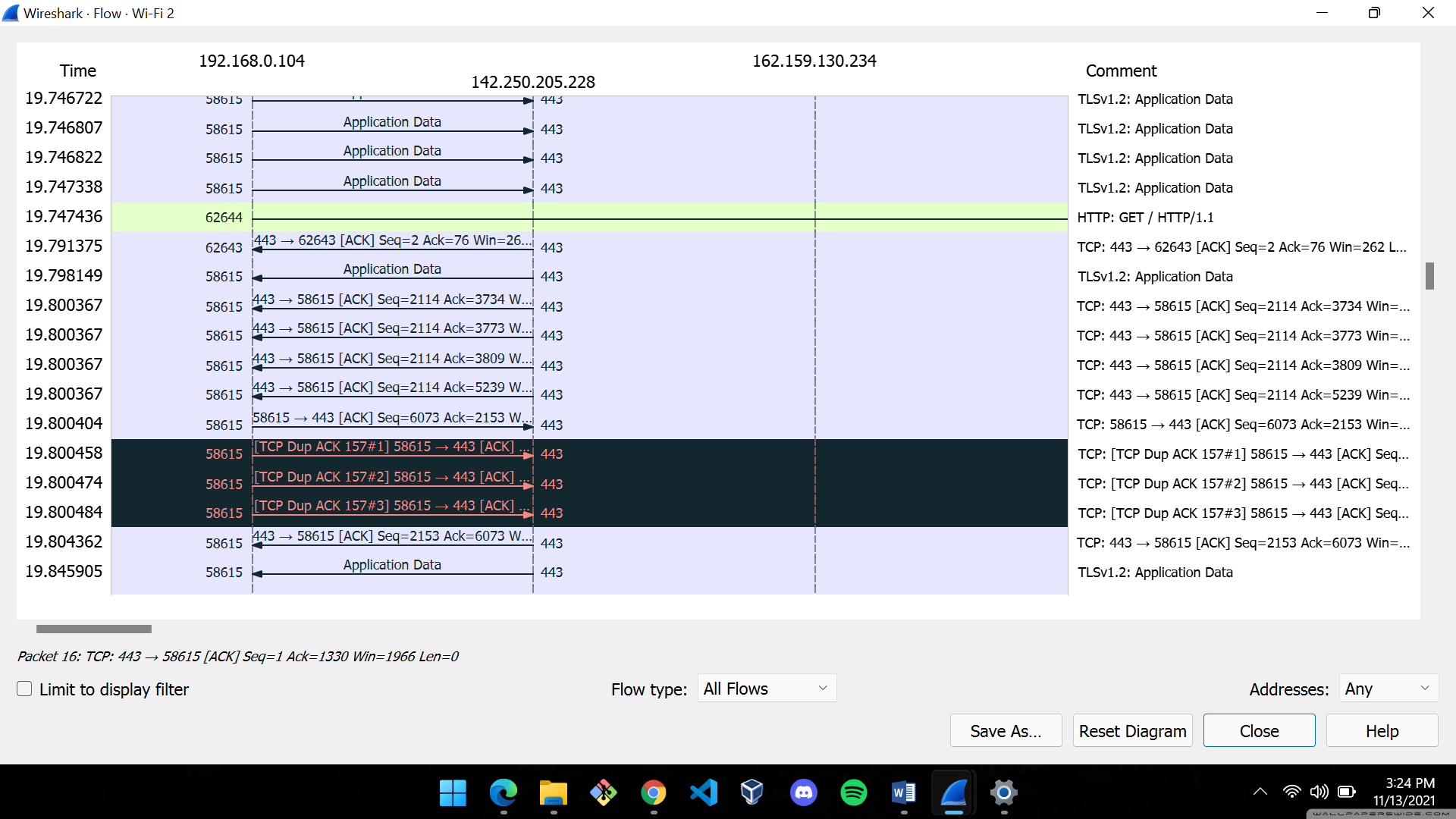




1. **Find the traffic flow. Select the Statistics->Flow Graph menu option. Choose General Flow and Network Source options, and click the OK button.**

Graph Snippets

****

****