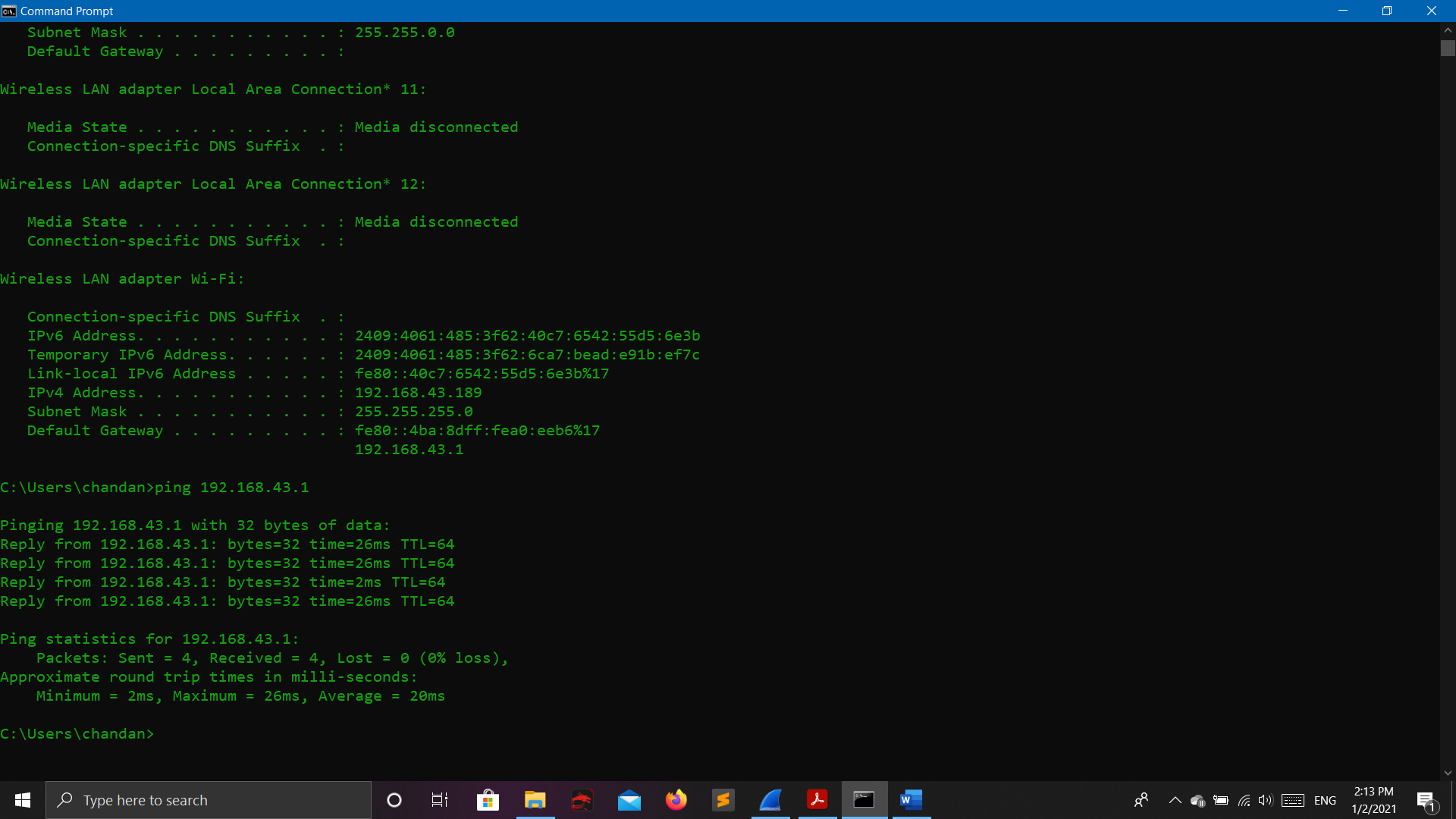


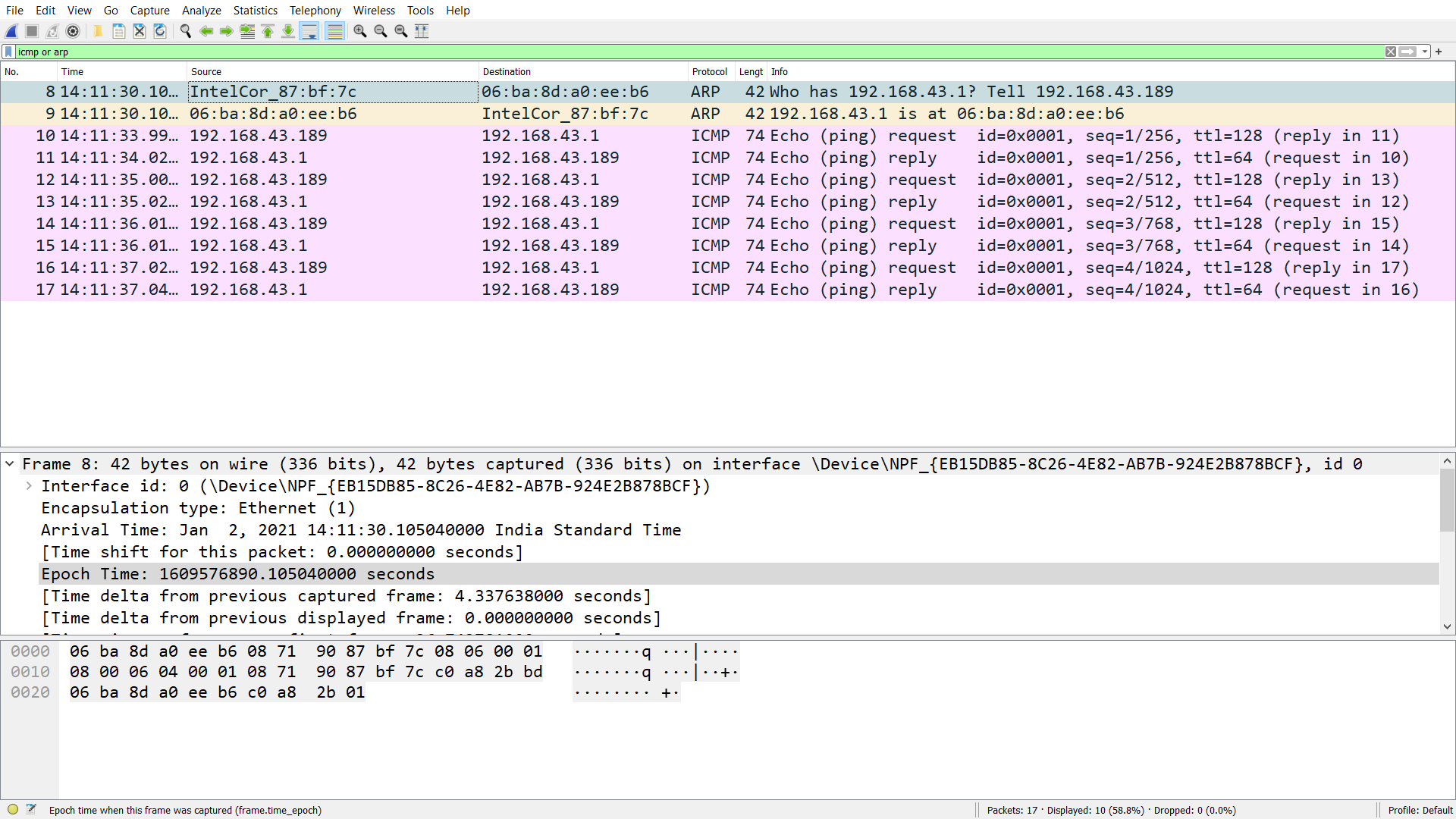
Computer Network assignment 5



* **Name: -** CHANDAN JANA
* **Roll: -** 301910501006
* **Class: -** BCSE-III
* **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.
* **Submission date: -** 01/02/2021
* **Q 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 neighbouring system. After the ARP request, the pings (ICMP echo request and replies) can be seen.**
* Ping to Gateway router ---

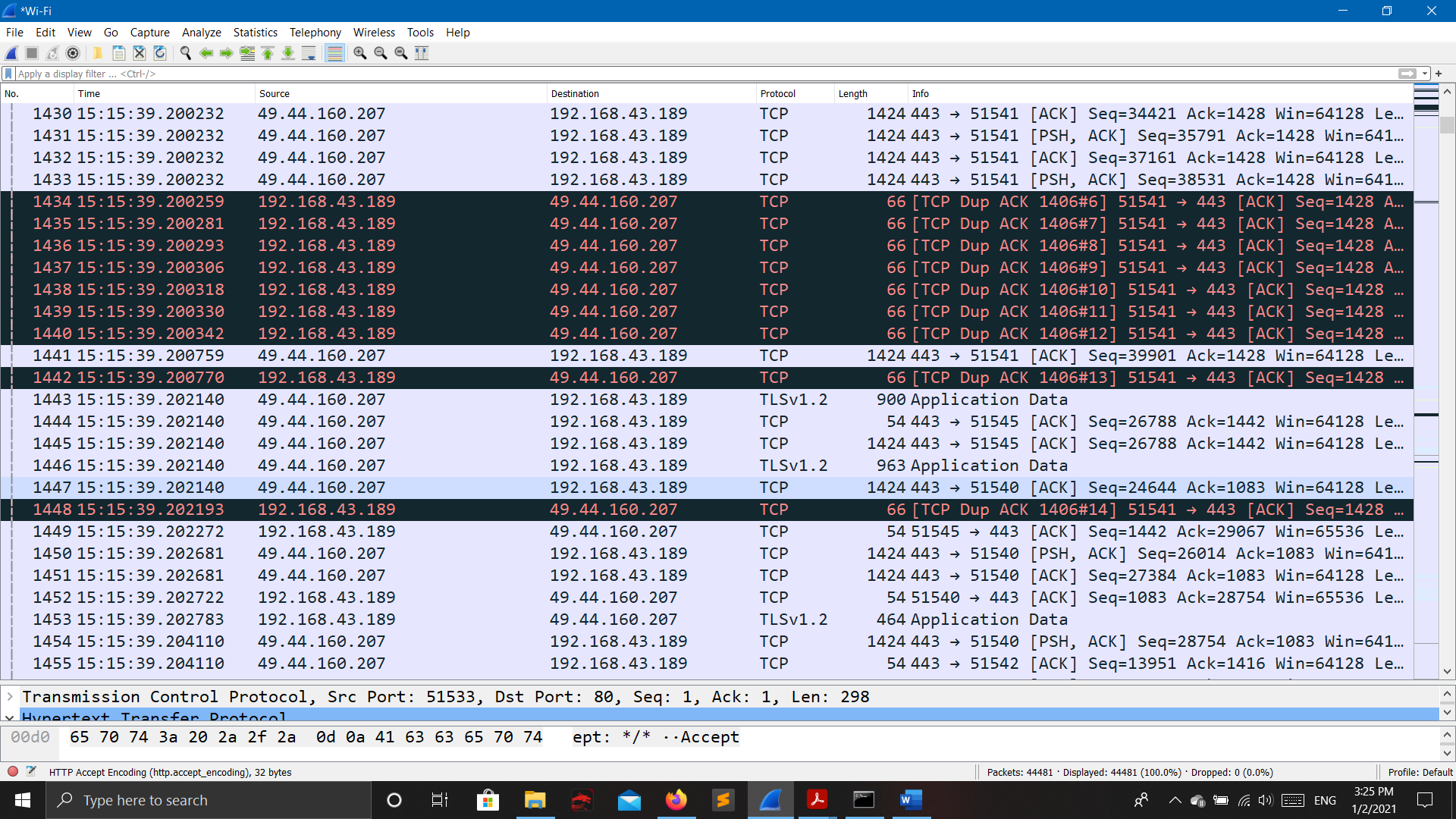


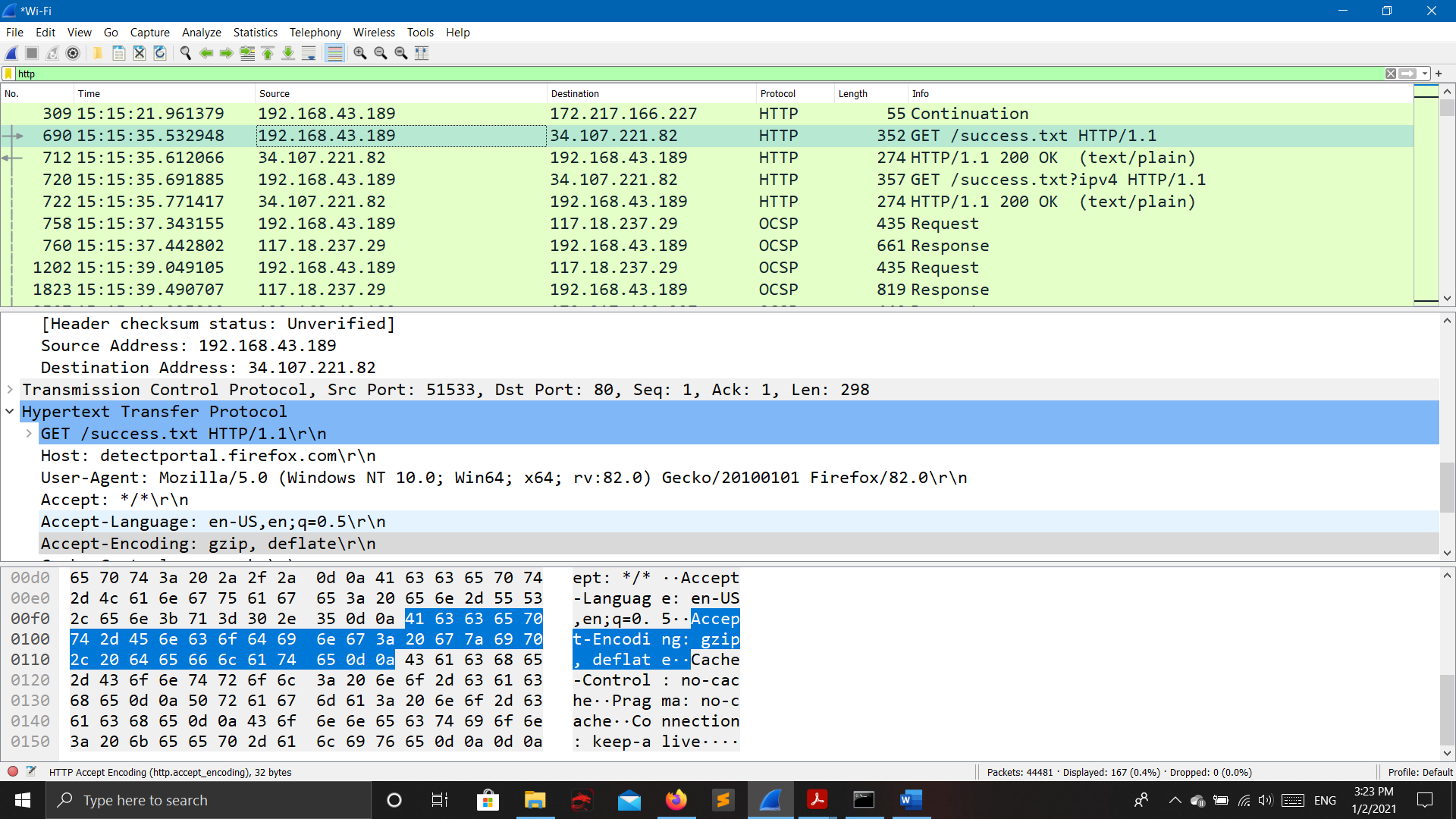
* Output on Wireshark ---



***Note: - Following frame 8 and 9 is type of ARP and frame number 10 to 17 are type of ICMP protocol.***

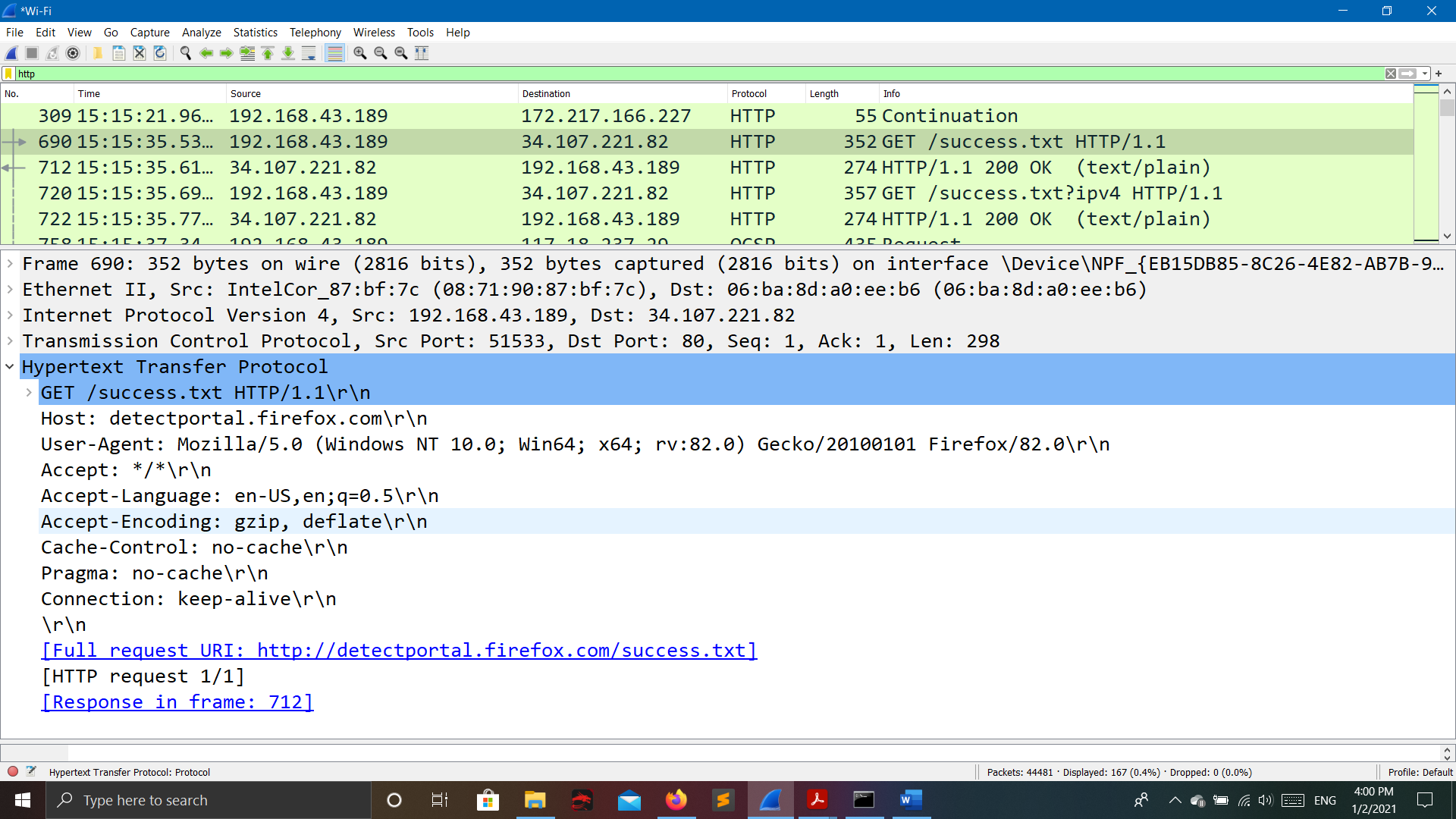
* **Q2.a: - Generate some web traffic and find the list the different protocols that appear in the protocol column in the unfiltered packet-listing window of Wireshark.**

****

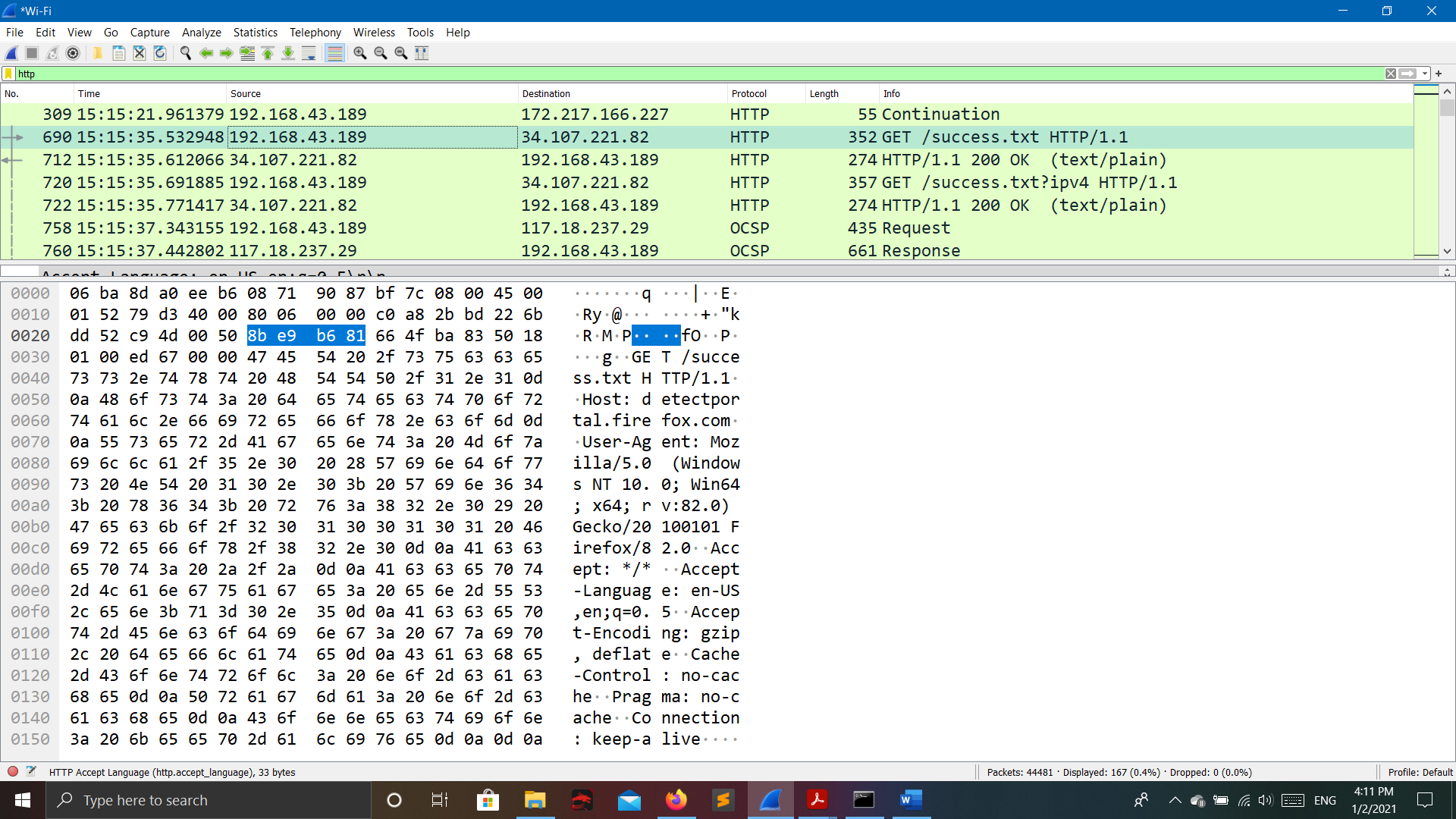
* **Q2.b: - How long did it take from when the HTTP GET message was sent until the HTTP OK reply was received? **

Following Packet number 690 is sending HTTP GET request to the address 34.107.221.82 at time 15:15:35.532948 and receive reply ok from 34.107.221.82 at 15:15:35.612066 on packet number 712 so the total time taken to receive ok is 79118 micro seconds.

* **Q2.c: - What is the Internet address of the website? What is the Internet address of your computer?**
* The Internet address of the website is: 34.1070221.82
* The Internet address of my computer is: 192.168.43.189
* **Q2.d: - 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.**

****

* **Q2.e: - Find out the value of the Host from the Packet Details Panel, within the GET command.**
* The value of host is: detectportal.firefox.com\r\n
* **Q 3: - Highlight the Hex and ASCII representations of the packet in the Packet Bytes Panel.**

****

**The Hex and ASCII representations of the packet in the Packet Bytes Panel are:**

0000 06 ba 8d a0 ee b6 08 71 90 87 bf 7c 08 00 45 00 .......q...|..E.

0010 01 52 79 d3 40 00 80 06 00 00 c0 a8 2b bd 22 6b .Ry.@.......+."k

0020 dd 52 c9 4d 00 50 8b e9 b6 81 66 4f ba 83 50 18 .R.M.P....fO..P.

0030 01 00 ed 67 00 00 47 45 54 20 2f 73 75 63 63 65 ...g..GET /succe

0040 73 73 2e 74 78 74 20 48 54 54 50 2f 31 2e 31 0d ss.txt HTTP/1.1.

0050 0a 48 6f 73 74 3a 20 64 65 74 65 63 74 70 6f 72 .Host: detectpor

0060 74 61 6c 2e 66 69 72 65 66 6f 78 2e 63 6f 6d 0d tal.firefox.com.

0070 0a 55 73 65 72 2d 41 67 65 6e 74 3a 20 4d 6f 7a .User-Agent: Moz

0080 69 6c 6c 61 2f 35 2e 30 20 28 57 69 6e 64 6f 77 illa/5.0 (Window

0090 73 20 4e 54 20 31 30 2e 30 3b 20 57 69 6e 36 34 s NT 10.0; Win64

00a0 3b 20 78 36 34 3b 20 72 76 3a 38 32 2e 30 29 20 ; x64; rv:82.0)

00b0 47 65 63 6b 6f 2f 32 30 31 30 30 31 30 31 20 46 Gecko/20100101 F

00c0 69 72 65 66 6f 78 2f 38 32 2e 30 0d 0a 41 63 63 irefox/82.0..Acc

00d0 65 70 74 3a 20 2a 2f 2a 0d 0a 41 63 63 65 70 74 ept: \*/\*..Accept

00e0 2d 4c 61 6e 67 75 61 67 65 3a 20 65 6e 2d 55 53 -Language: en-US

00f0 2c 65 6e 3b 71 3d 30 2e 35 0d 0a 41 63 63 65 70 ,en;q=0.5..Accep

0100 74 2d 45 6e 63 6f 64 69 6e 67 3a 20 67 7a 69 70 t-Encoding: gzip

0110 2c 20 64 65 66 6c 61 74 65 0d 0a 43 61 63 68 65 , deflate..Cache

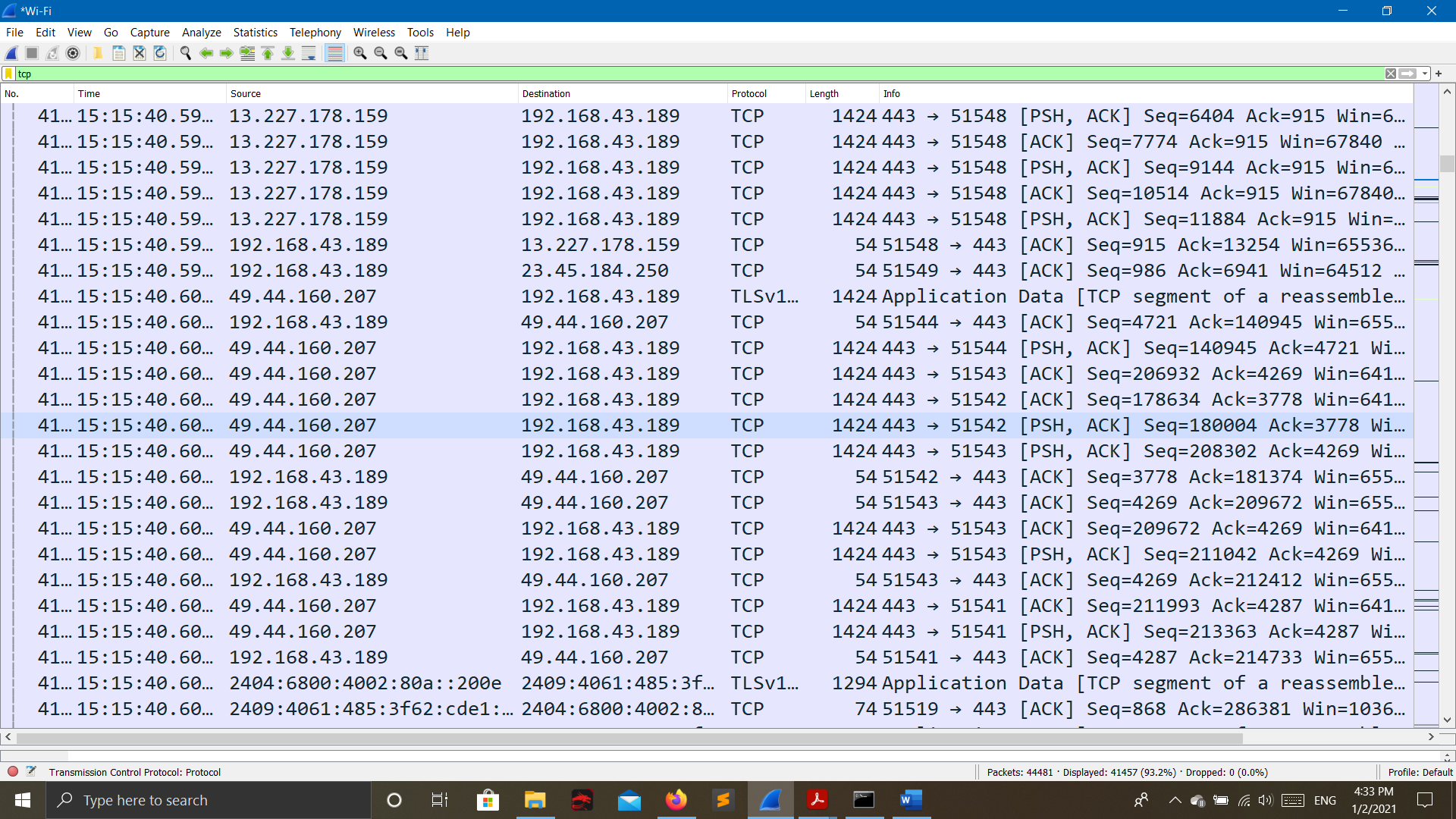
0120 2d 43 6f 6e 74 72 6f 6c 3a 20 6e 6f 2d 63 61 63 -Control: no-cac

0130 68 65 0d 0a 50 72 61 67 6d 61 3a 20 6e 6f 2d 63 he..Pragma: no-c

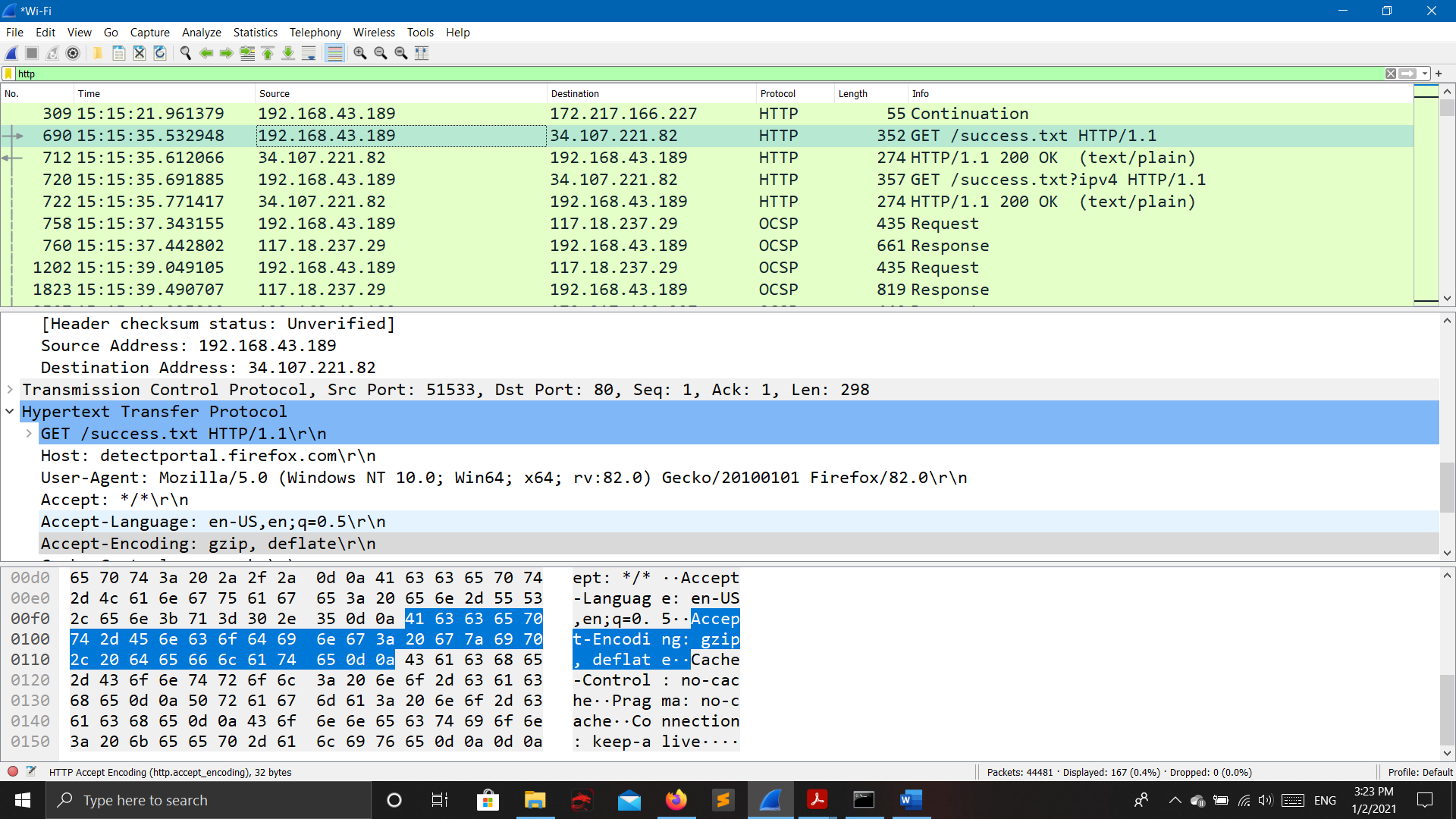
0140 61 63 68 65 0d 0a 43 6f 6e 6e 65 63 74 69 6f 6e ache..Connection

0150 3a 20 6b 65 65 70 2d 61 6c 69 76 65 0d 0a 0d 0a : keep-alive....

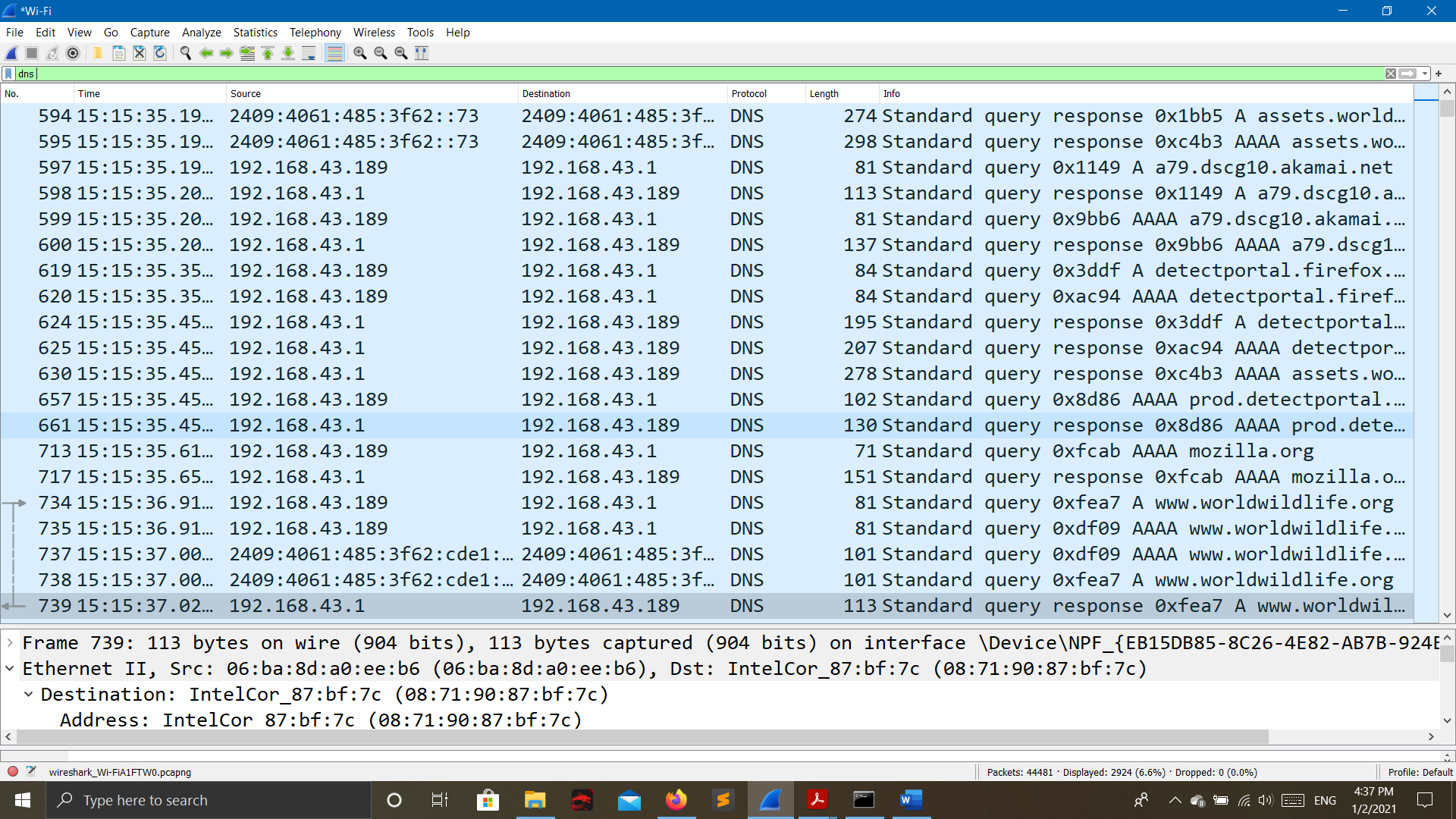
* **Q 4: - Find out the first 4 bytes of the Hex value of the Host parameter from the Packet Bytes Panel.**
* **The first 4 bytes of the Hex value is : 48 6f 73 74**
* **Q 5: - Filter packets with http, TCP, DNS and other protocols.**
* **TCP**

****

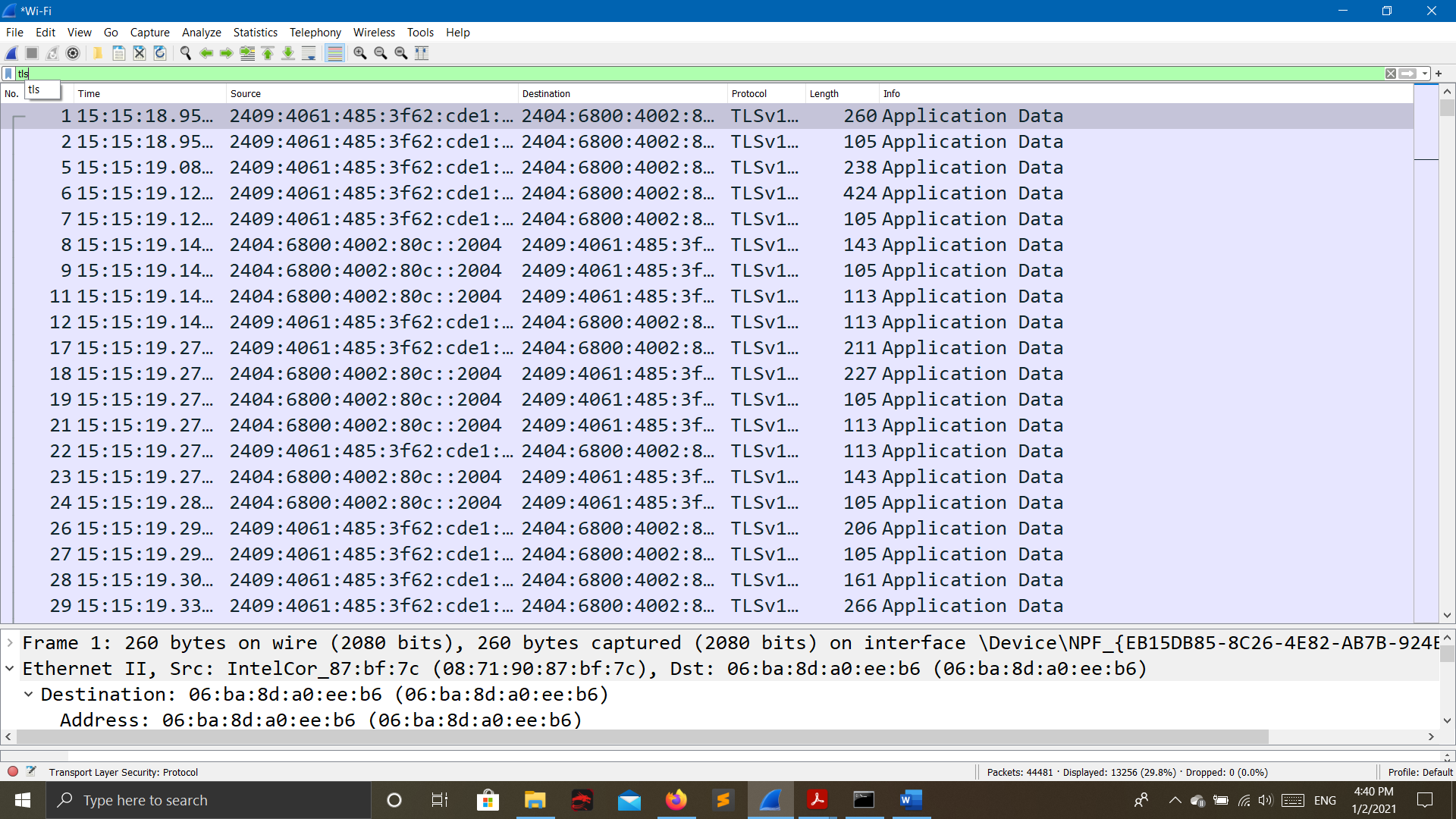
**HTTP**

****

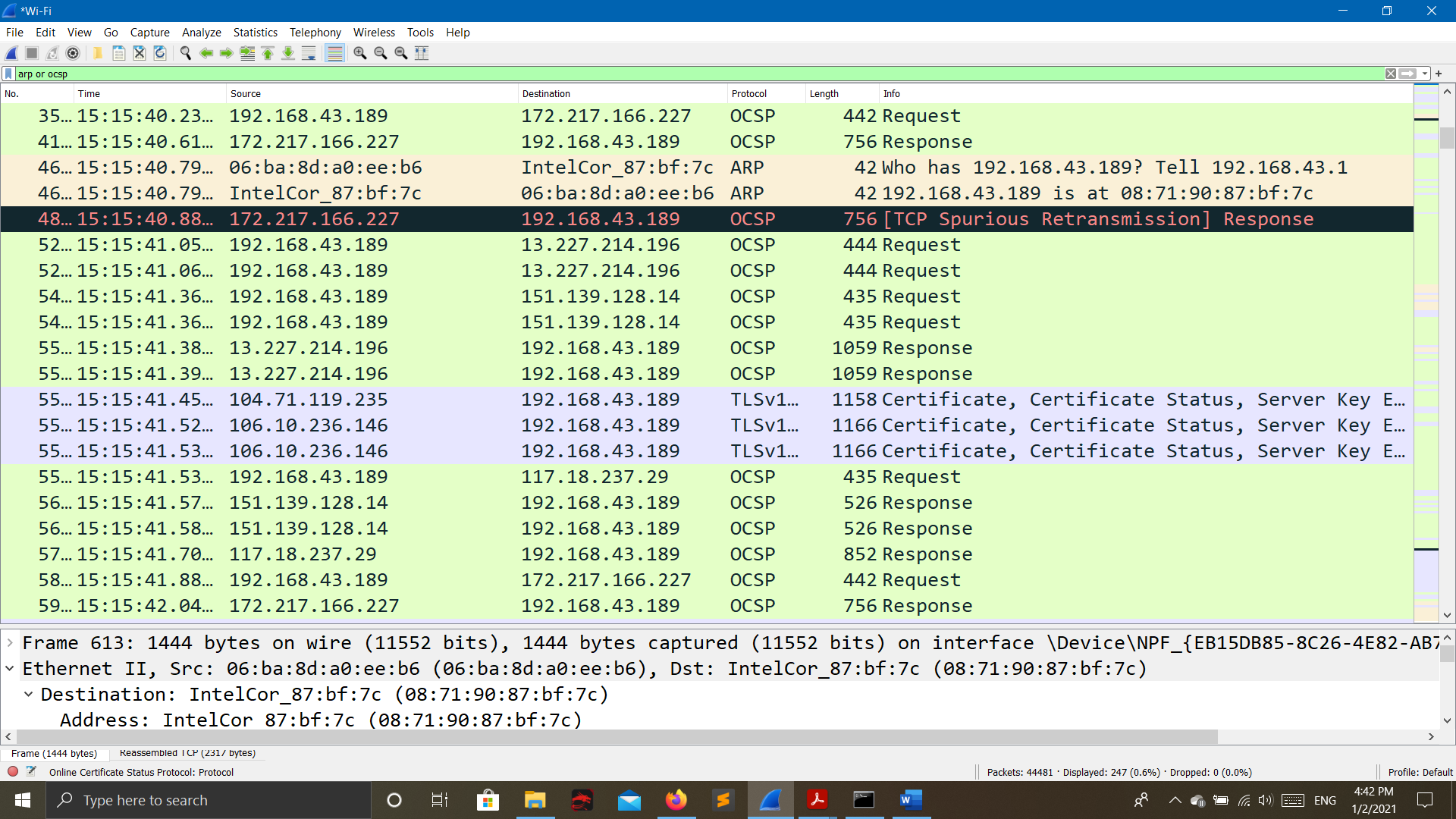
**DNS**

****

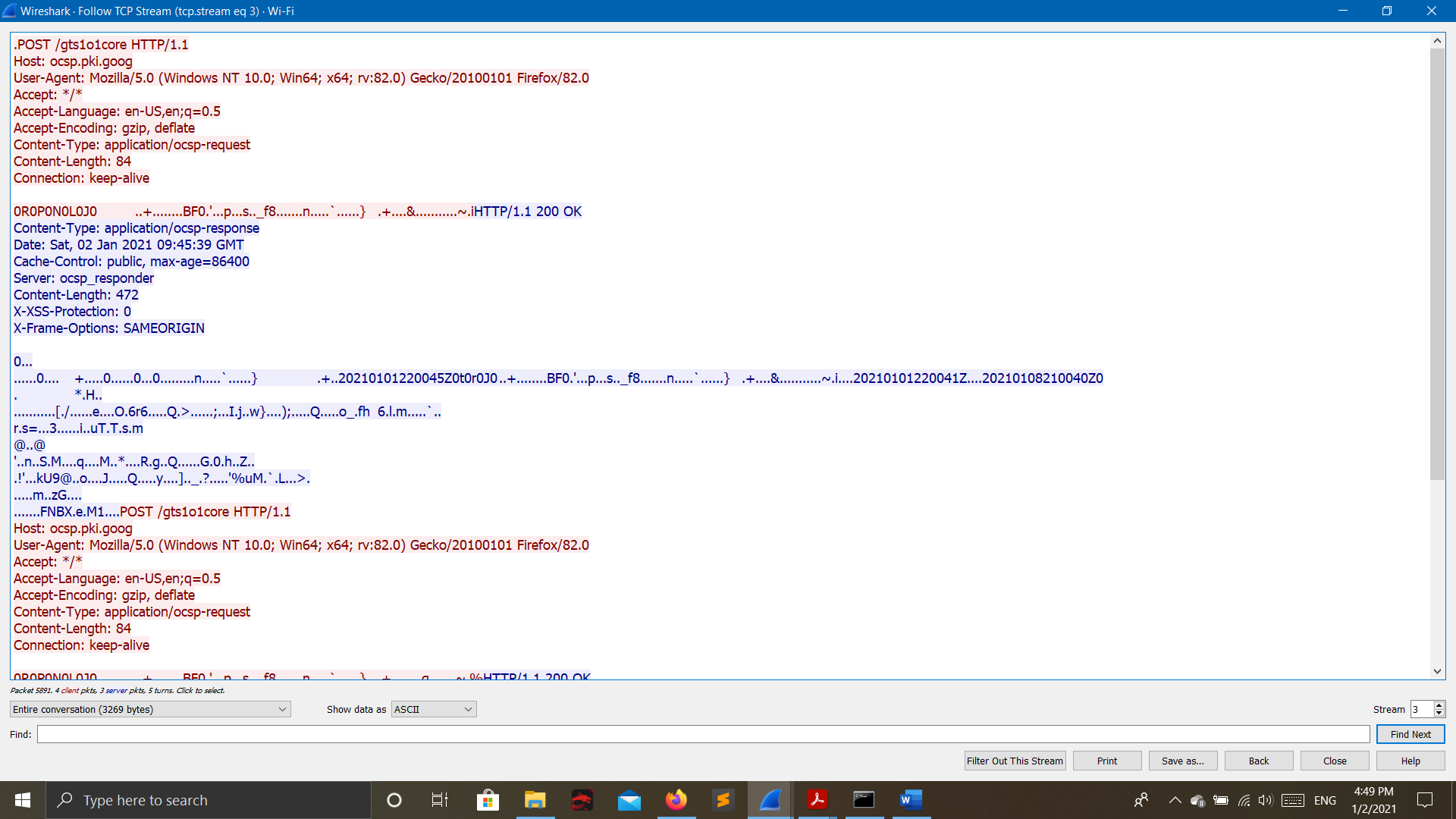
**TLS v1**

****

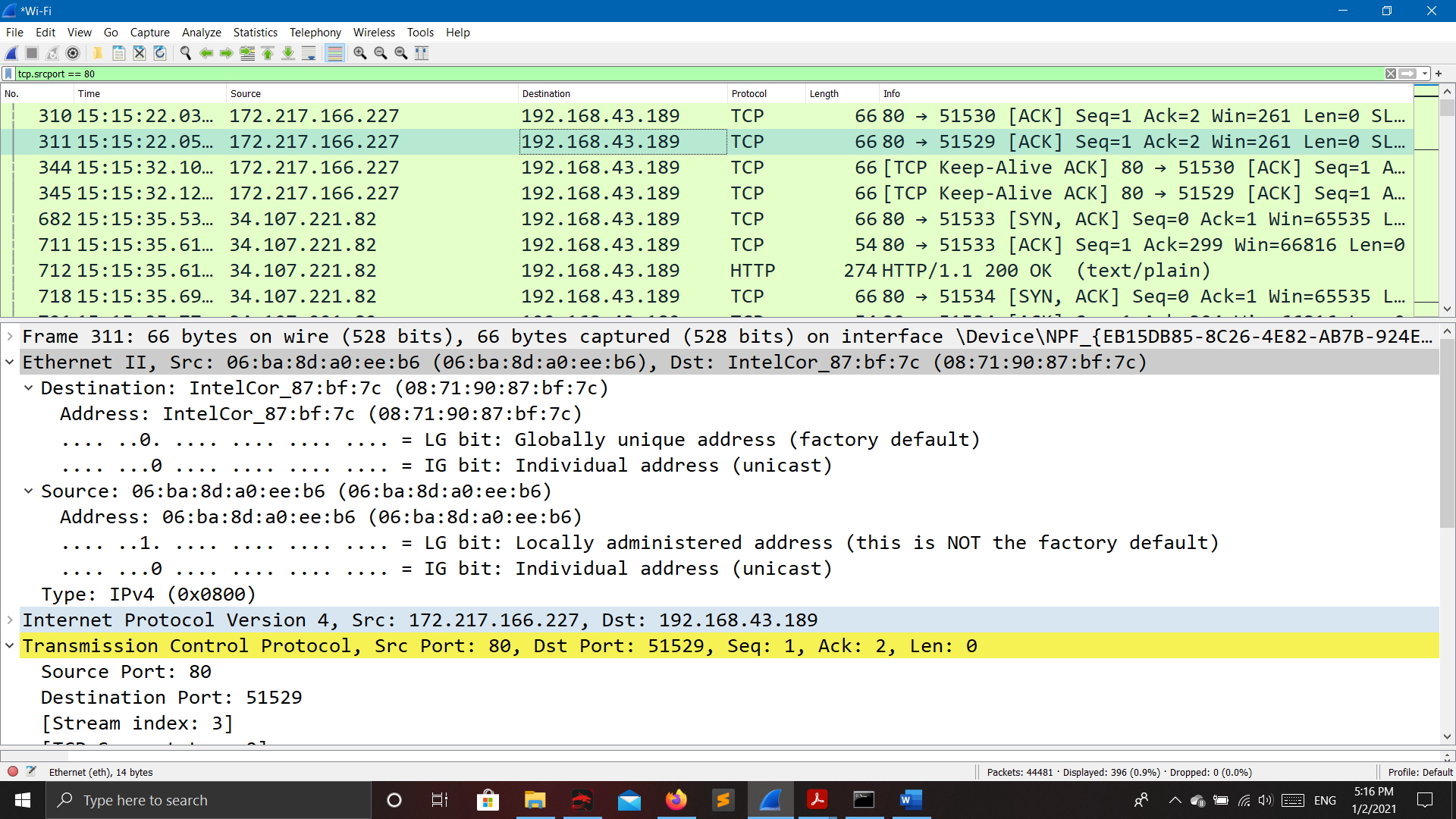
**ARP and OCSP**

****

* **Q5.a: Find out what are those packets contain by following one of the conversations.**
* Selecting packets having protocol type is HTTP then selecting conversion of TCP stream.

****

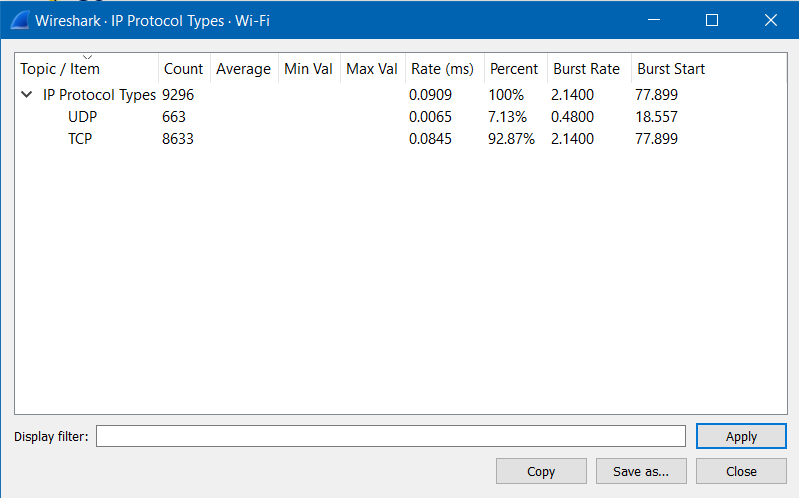
* **Q6: -** Search through your capture, and find an HTTP packet coming back from the server (TCP Source Port == 80). Expand the Ethernet layer in the Packet Details Panel.



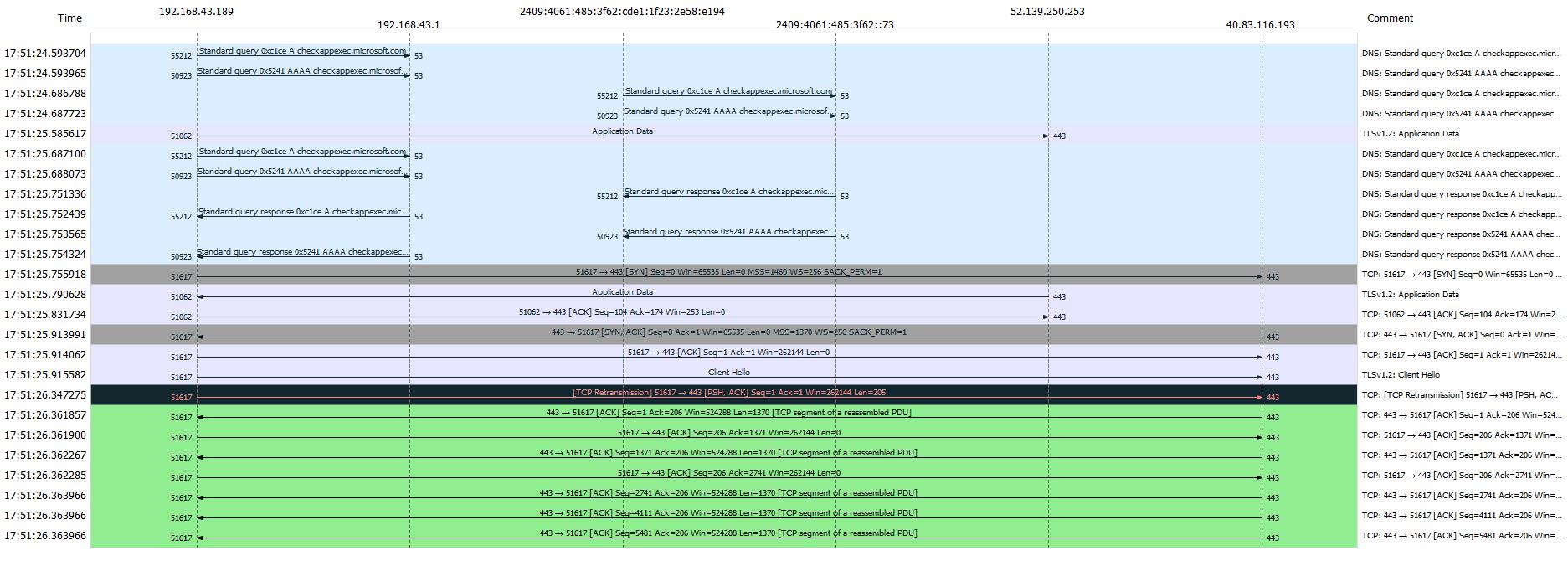
* **Q7: - What are the manufacturers of your PC’s Network Interface Card (NIC), and the servers NIC?**
* My PC’s NIC: Intelcor\_87:bf:7c
* Server’s NIC: 06:ba:8d:a0:ee:b6
* **Q8: - What are the Hex values (shown the raw bytes panel) of the two NICS Manufacturers OUIs?**
* My PC’s NIC: 08:71:90:87:bf:7c
* Server’s NIC: 06:ba:8d:a0:ee:b6
* **Q9: - Find the following statistics:**

**A:** 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?

****

* **Q10: Find the traffic flow Select the Statistics->Flow Graph menu option. Choose General Flow and Network Source options, and click the OK button.**
* **General Flow:**

****

* **TCP Flow:**

****