**Computer Networks Lab Report**

**Assignment-** 5

**Class:** BCSE-III

**Semester:** 1st

**Group:**  A3

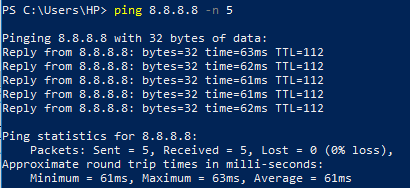
**Group Members:-**

* PARTHIV SARKAR - 002110501134
* ARKAJYOTI NASKAR - 002110501144
* SOHAM CHOWDHURY - 002110501145
* ARIYAN BHAUMIK - 002110501149

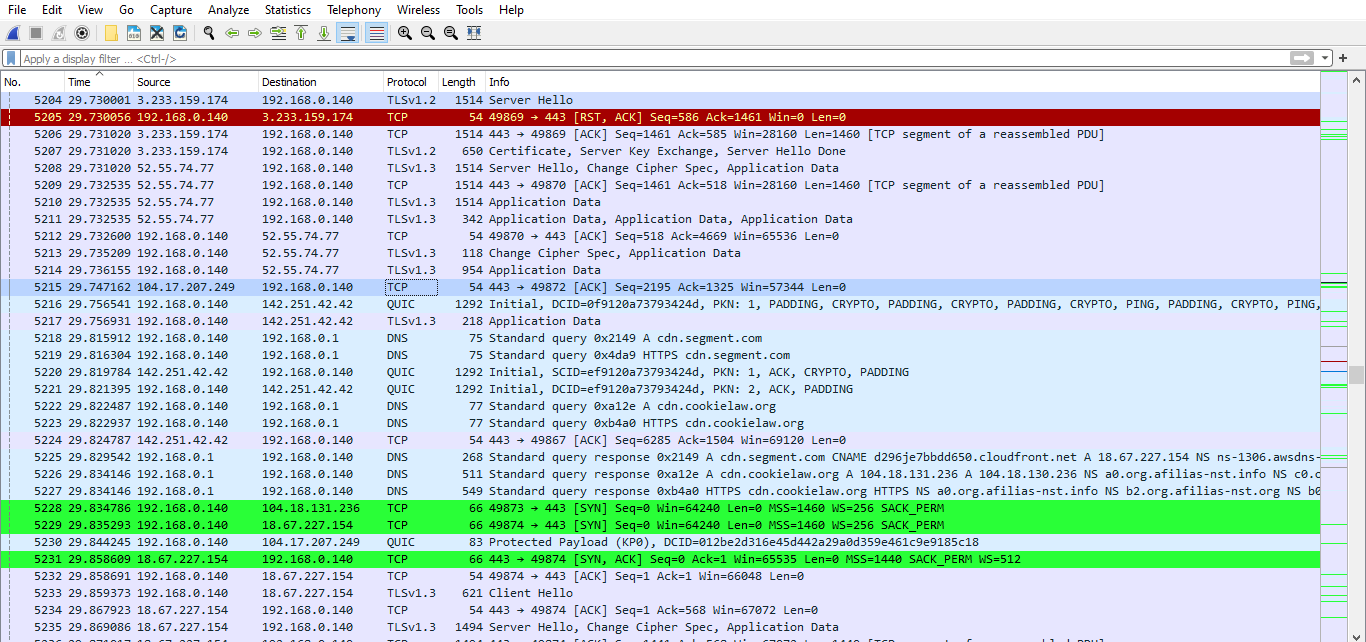
**Overview:-**

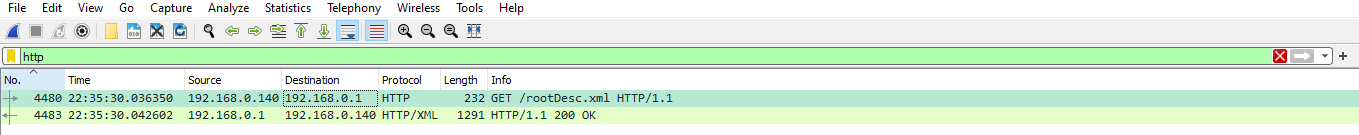
Wireshark is an open source cross-platform packet capture and analysis tool, with versions for Windows and Linux. The GUI window gives a detailed breakdown of the network protocol stack for each packet, colorizing packet details based on protocol, as well as having functionality to filter and search 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.

**Questions:-**

1. **Generate some ICMP traffic by using the Ping command line tool to check the connectivity of a neighboring 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.**



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



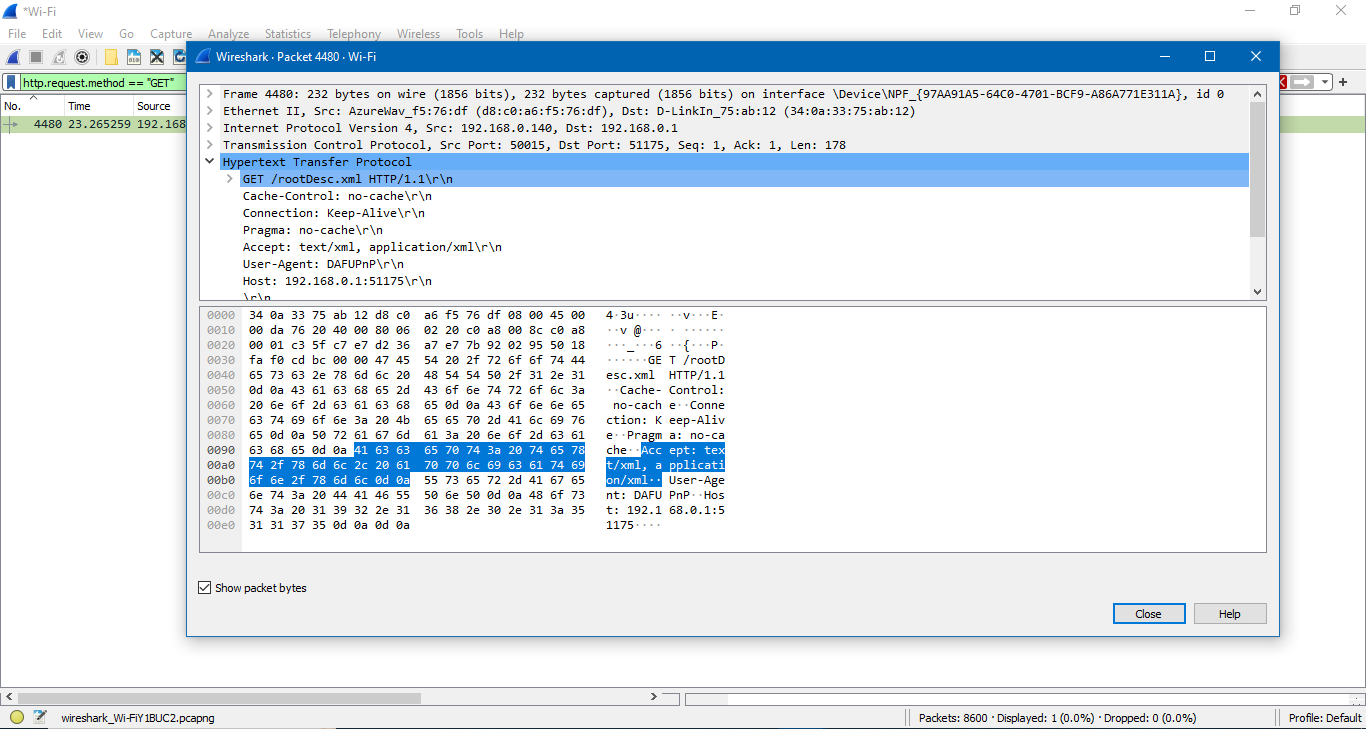
Request sent at 22:35:30.036350 and received response at 22:35:30.042602.

So, delay = 0.006252 seconds.

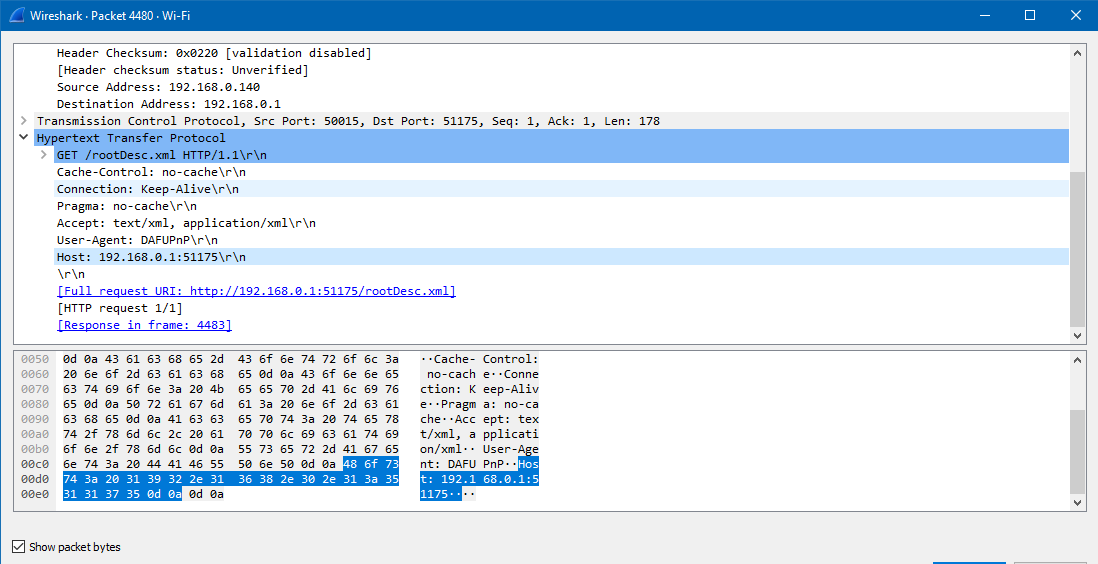
* 1. **What is the Internet address of the website? What is the Internet address of your computer?**

Internet address of website : 192.168.0.1

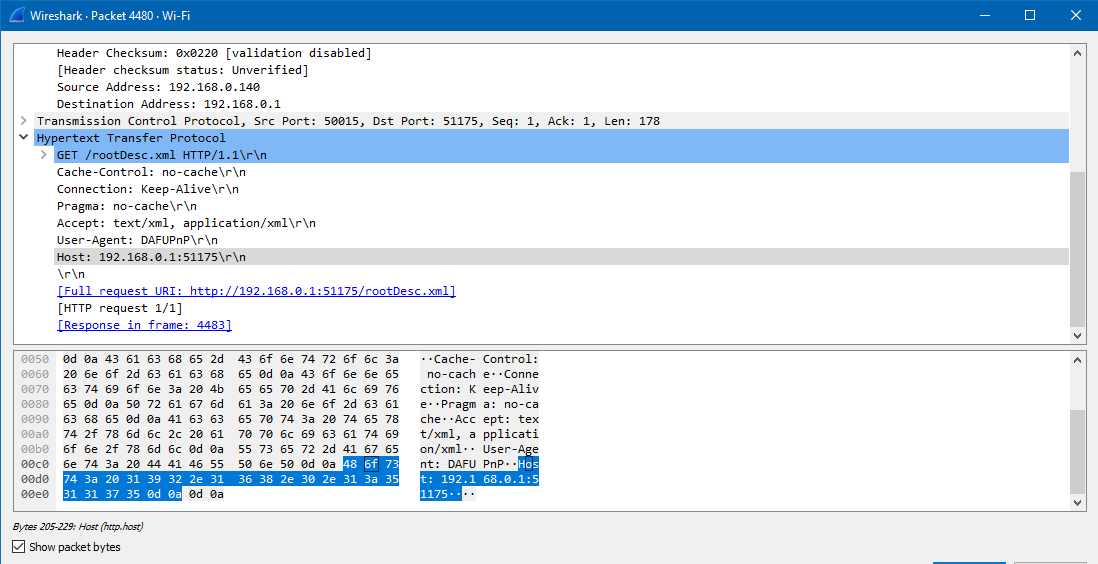
Internet address of computer : 192.168.0.140

* 1. **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.**

* 1. **Find out the value of the Host from the Packet Details Panel, within the GET command.**



Host : 192.168.0.1:51175

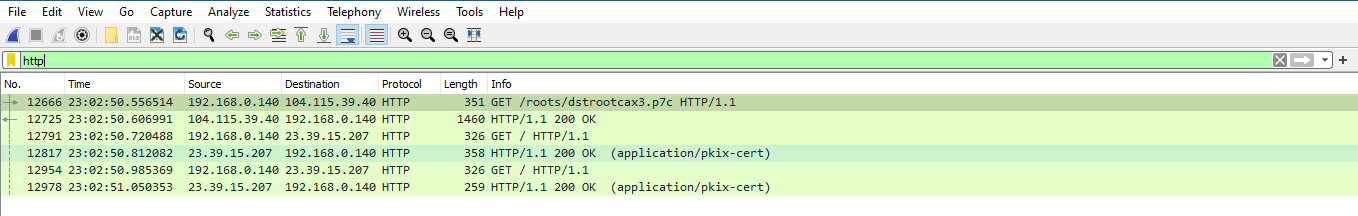
1. **Highlight the Hex and ASCII representations of the packet in the Packet Bytes Panel.**

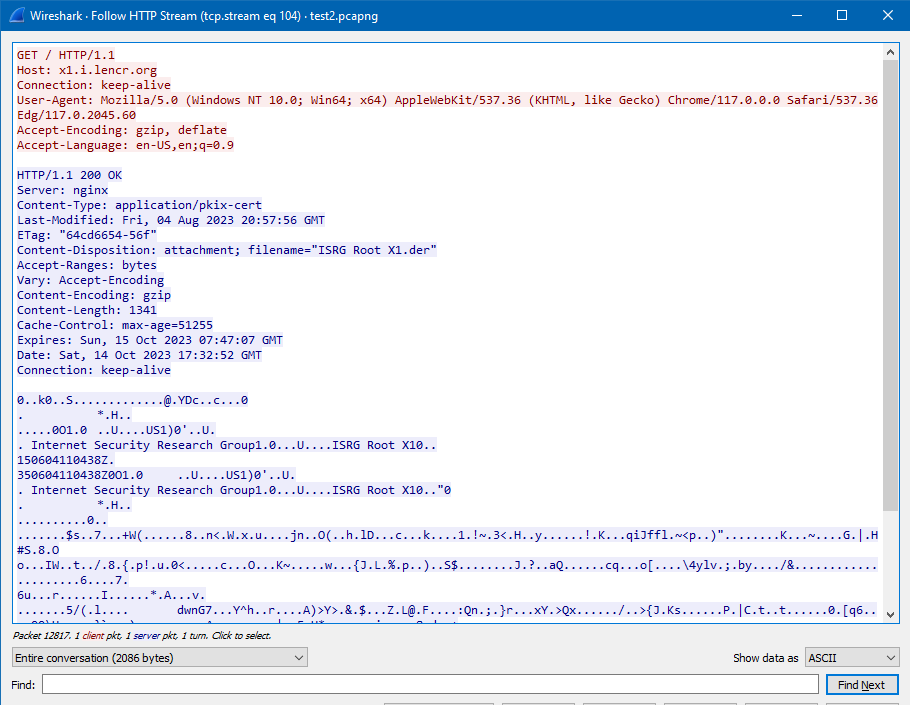
1. **Find out the first 4 bytes of the Hex value of the Host parameter from the Packet Bytes Panel.**

First 4 bytes are - 48 6f 73 74

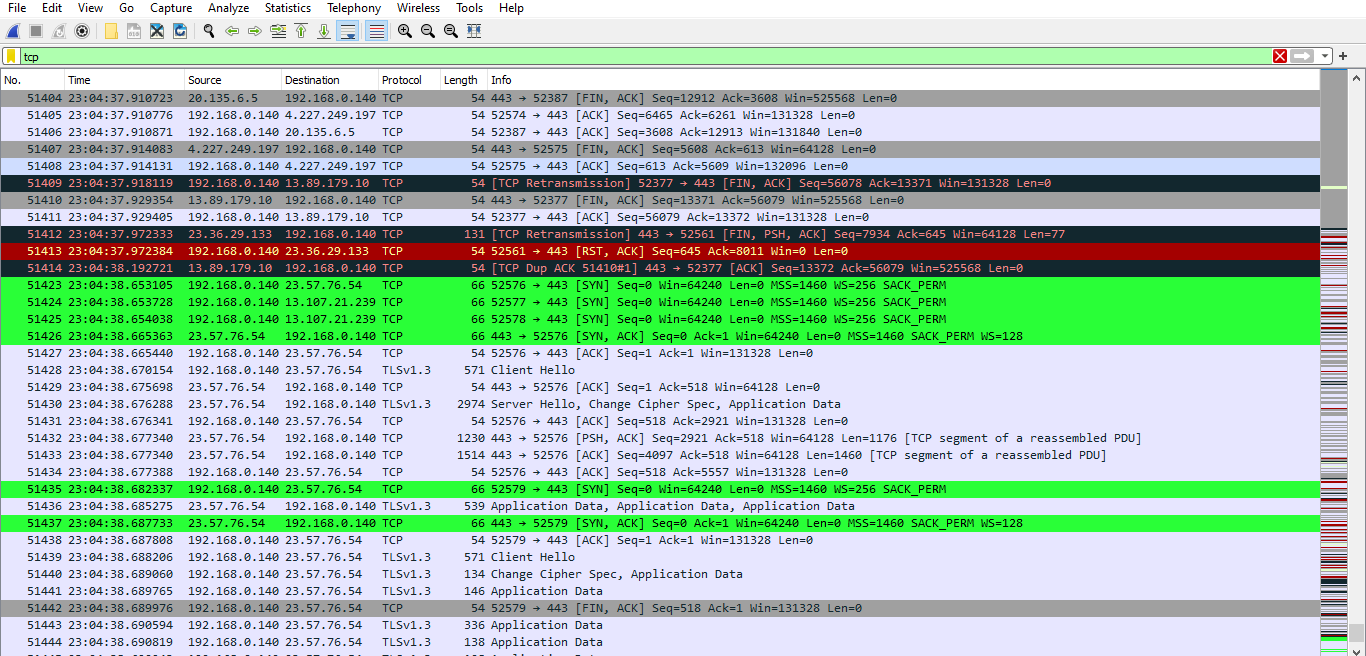
1. **Filter packets with http, TCP, DNS and other protocols. a. Find out what those packets contain by following one of the conversations (also called network flows), select one of the packets and press the right mouse button. click on follow.**

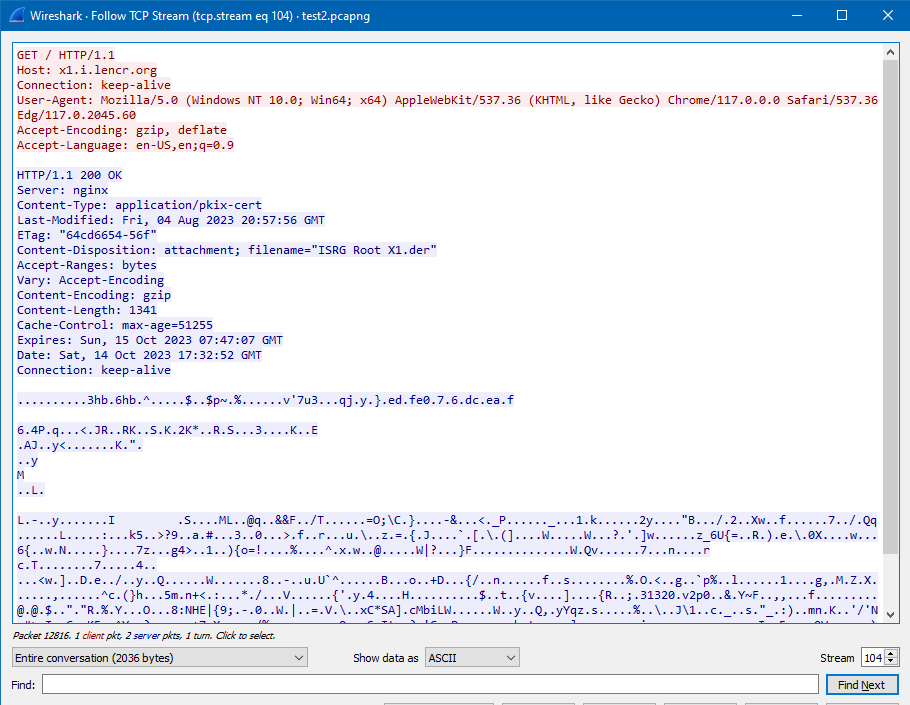
**HTTP :**



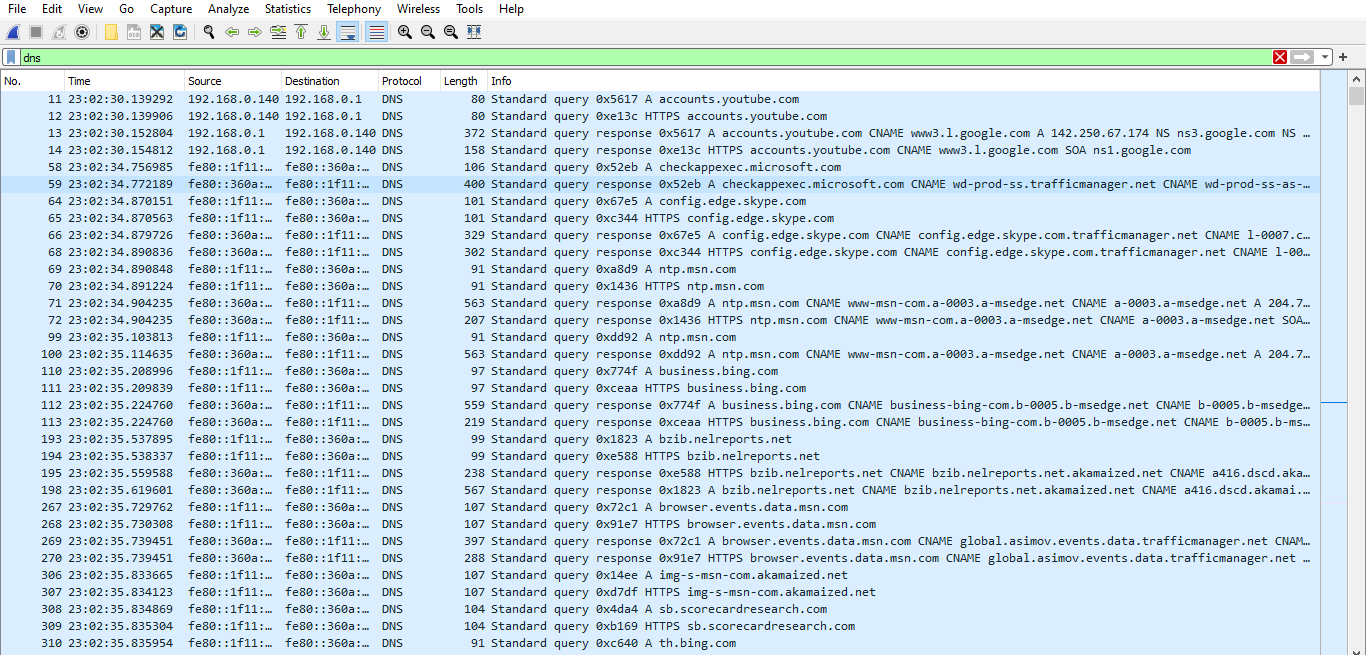


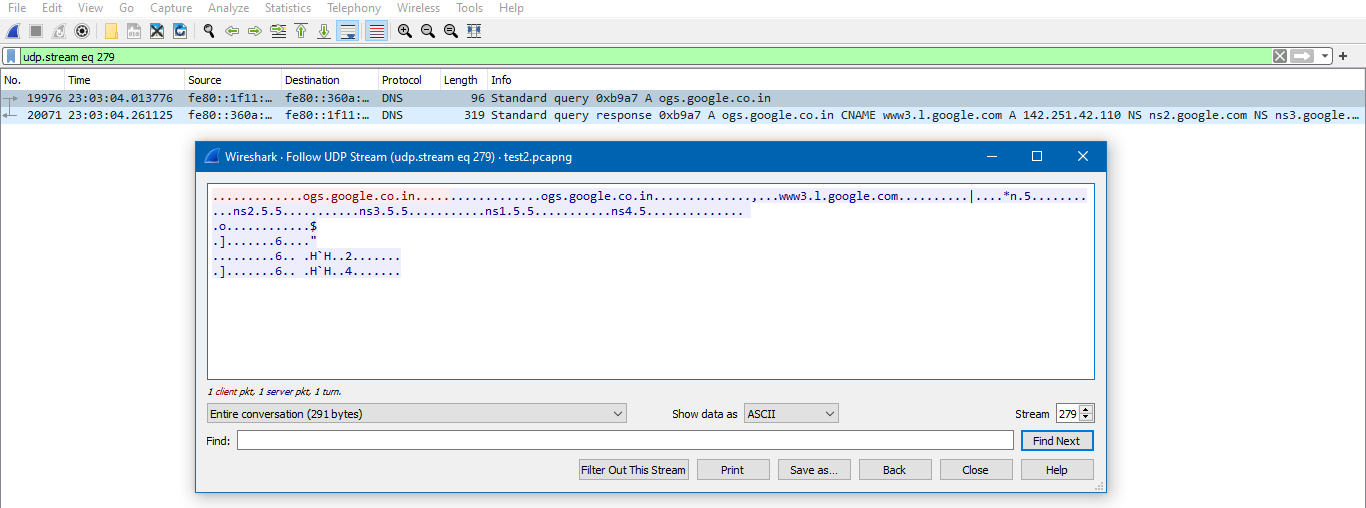
**TCP :**



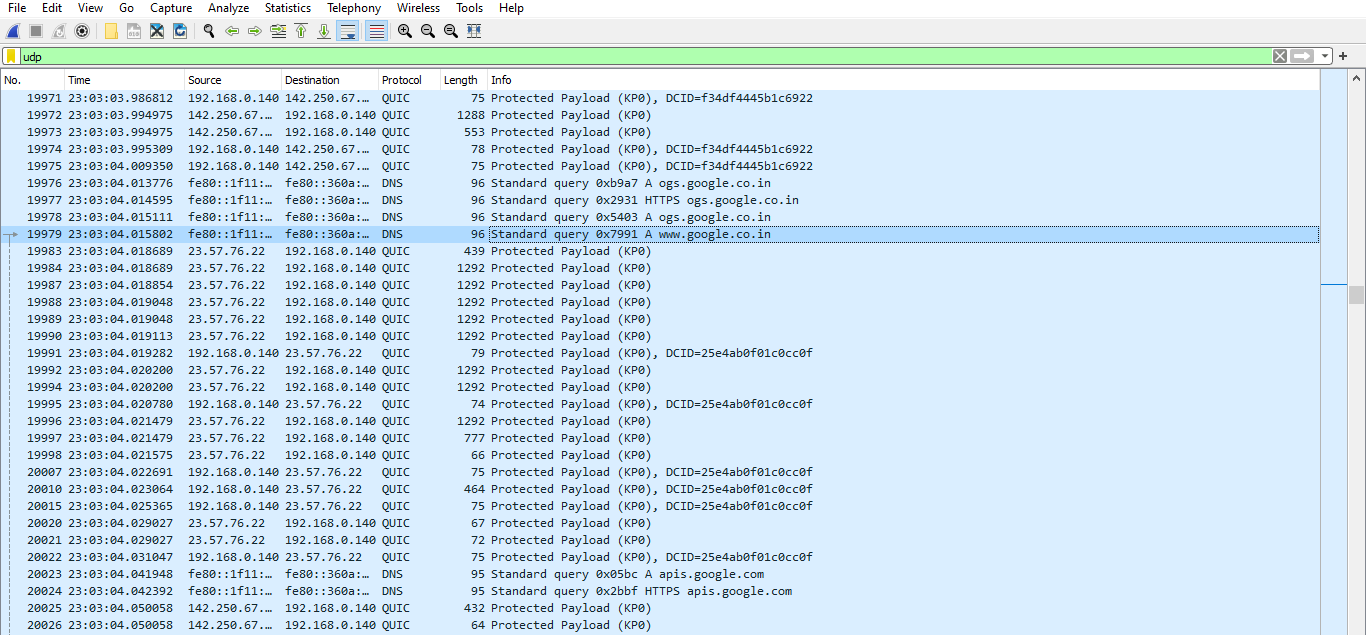


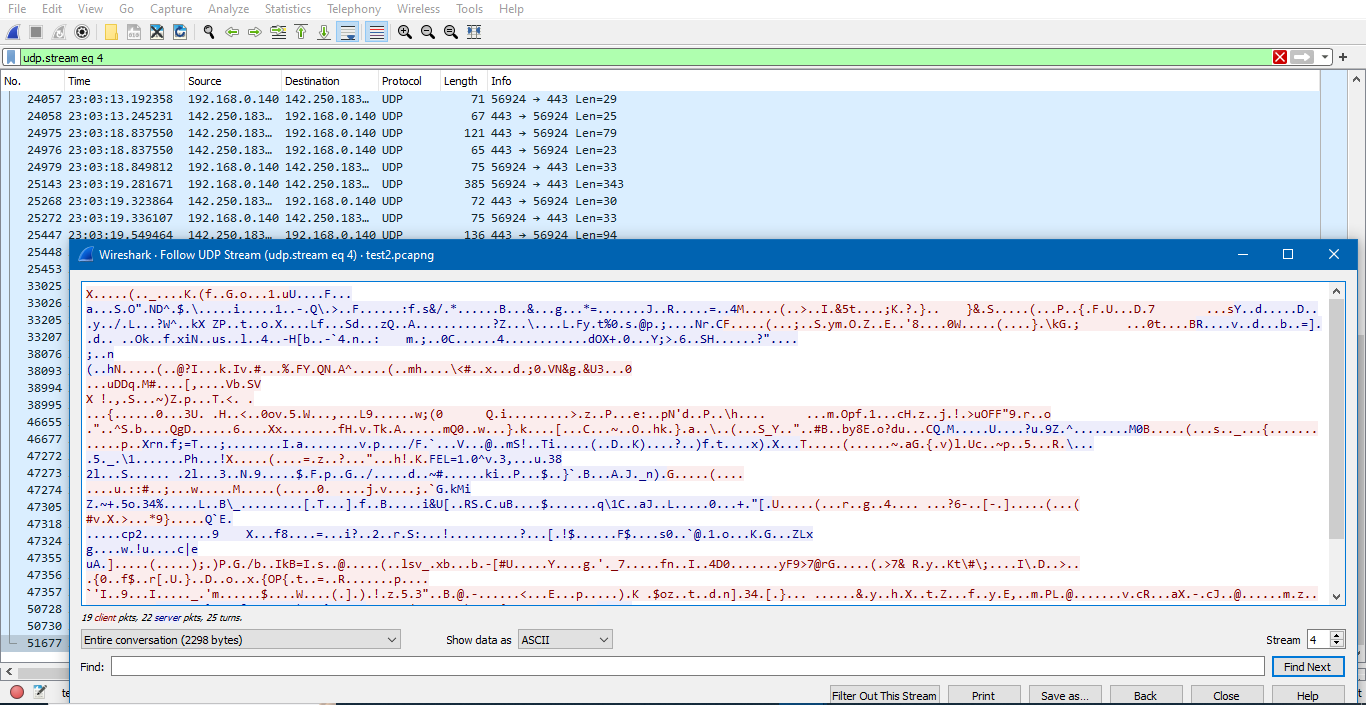
**DNS :**



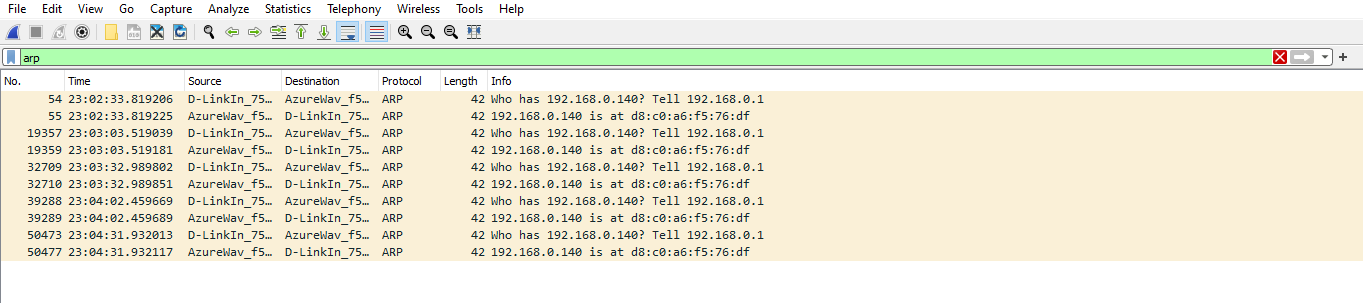


**UDP :**

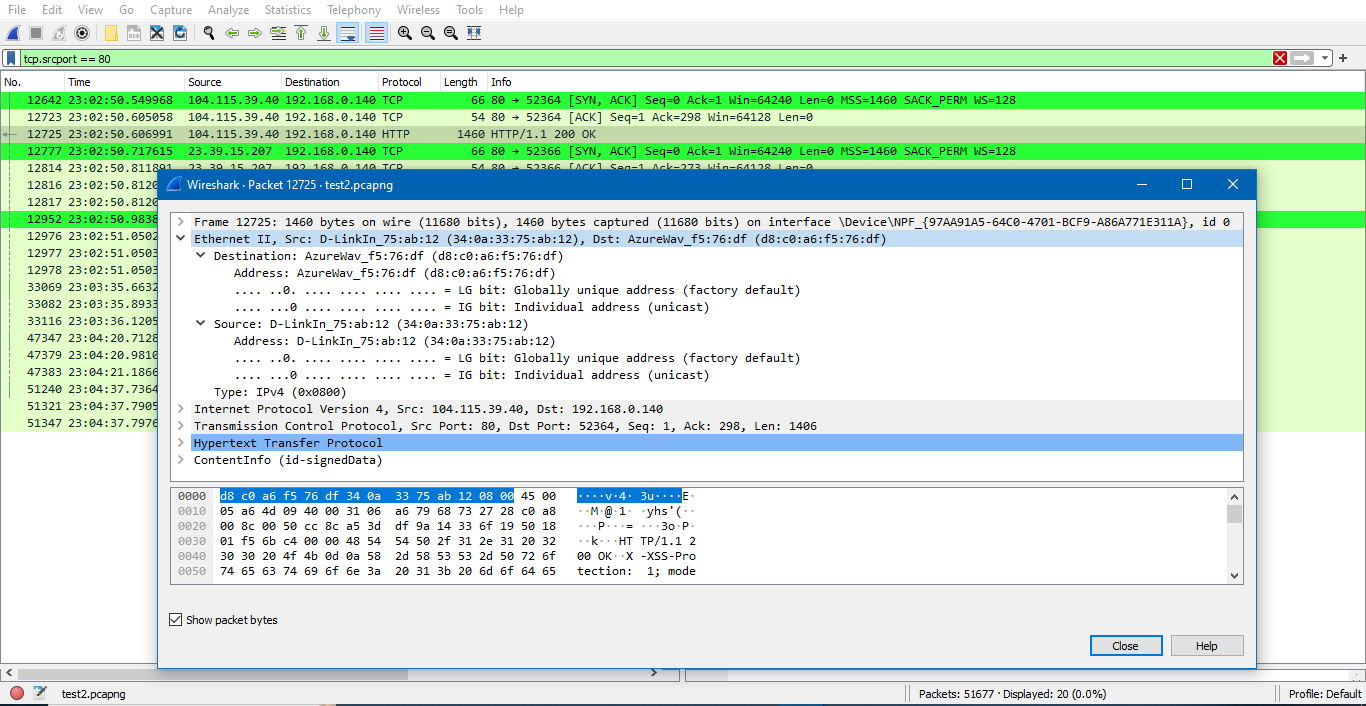




**ARP :**



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.**



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

Manufacturer of my PC’s NIC – AzureWave Technology Inc.

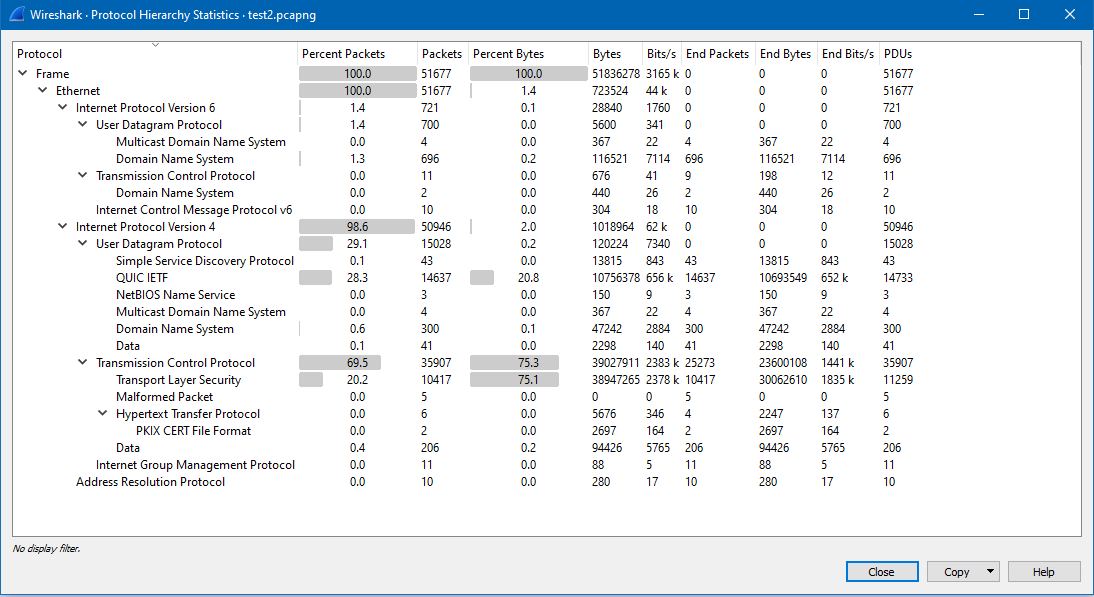
Manufacturer of server’s NIC – D-Link International

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

Hex values of my PC’s OUI - d8:c0:a6

Hex values of server’s OUI - 34:0a:33

1. **Find the following statistics:**
   1. **What percentage of packets in your capture are TCP, and give an example of the higher level protocol which uses TCP?**
      * 69.5 % of packets in the capture are TCP
      * Higher level protocols using TCP - HTTP, FTP



* 1. **What percentage of packets in your capture are UDP, and give an example of the higher level protocol which uses UDP?**
     + 29.1% packets are UDP
     + Higher level protocols using UDP- SNMP

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

