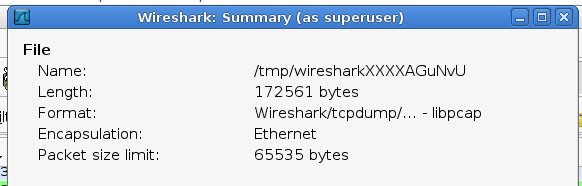
**Lab03**

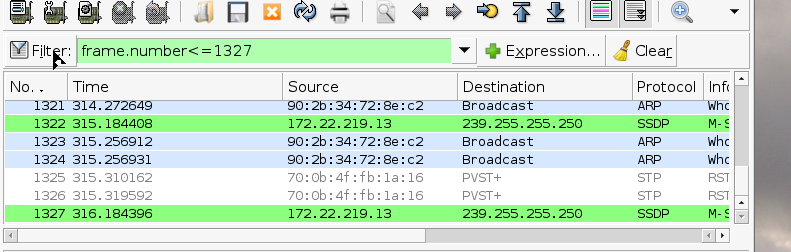
**Sayor S M Sadman Sakib (KAC25U)**

4.1

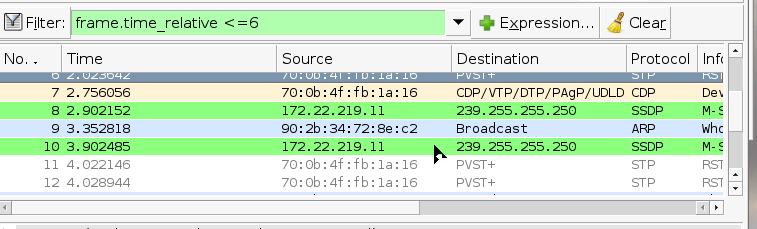
A) On the basis of the Wireshark capture justify your answer to the following questions:

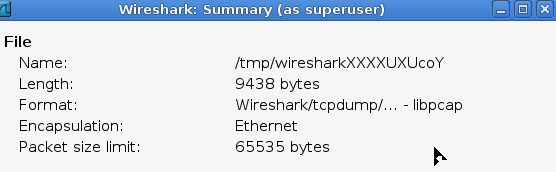
- What is the total size of 1327 pieces of captured frames?





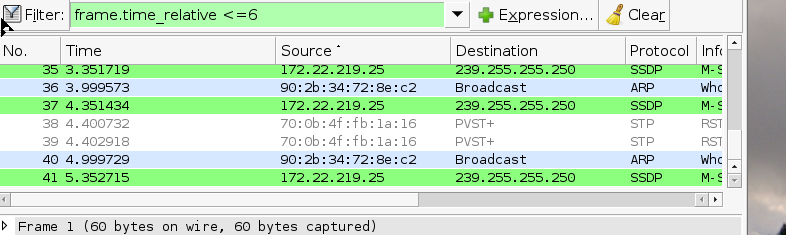
- What is the avarage bandwidth of the network traffic for 6 seconds?





Bandwith = 9438/6 Bps

- How many frames were transferred through the NIC for 6 seconds?



41

- What is the avarage frame size transferred for 6 seconds?

Average frame size = 9438/41 Bytes

B) On the basis of the Wireshark capture justify your answer to the following questions:

- What is the compression ratio in the case of pcap and txt file types?

Compression Ratio=Compressed File Size/Original File Size​

gzip -9 filename.pcap

Compression Ratio (pcap)=(10.3MB/2.4 MB)=4.292

Compression Ratio (txt)=(5.6MB/1.8 MB)=3.112

- What is the compression ratio in the case of pcap and pcapng file types?

editcap -F pcapng filename.pcap filename.pcapng

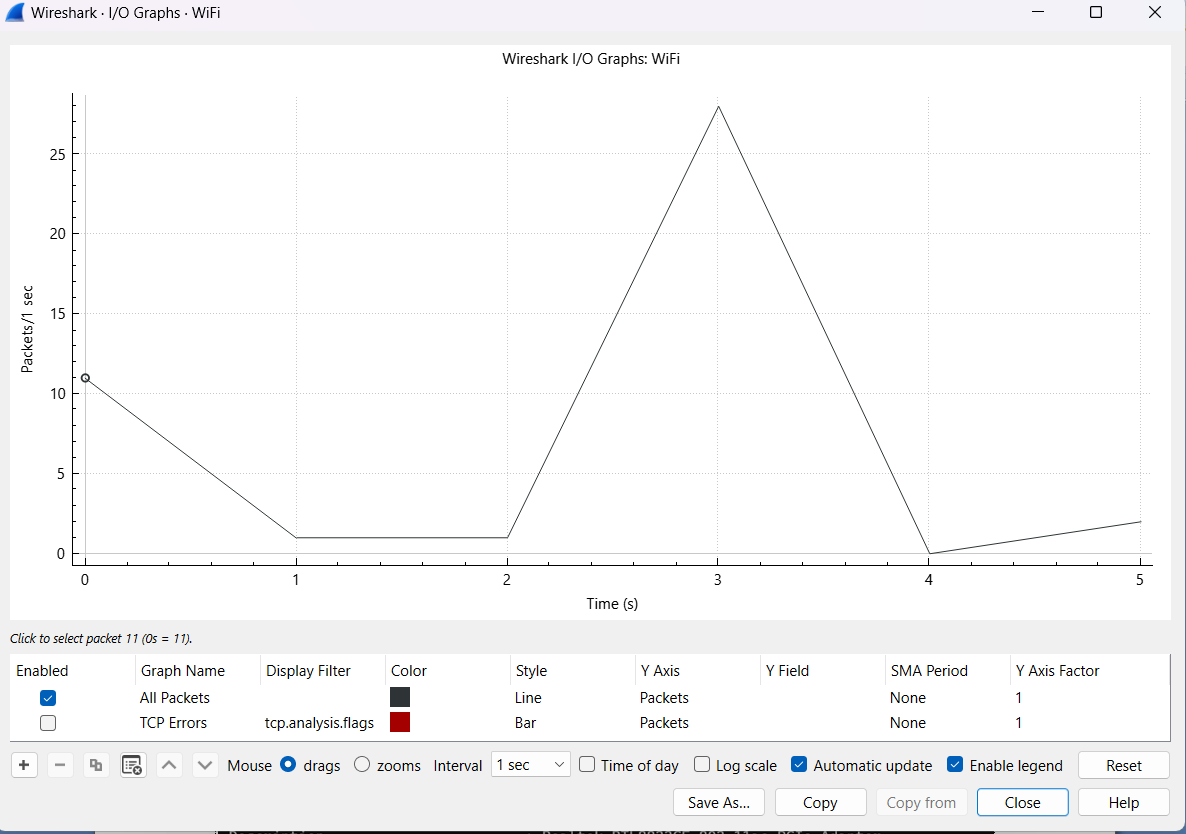
gzip -9 filename.pcapng

Compression Ratio (pcapng)=(8.2MB/2MB)​)=4.1

4.2

A) On the basis of the Wireshark capture prove your answer to the following questions:

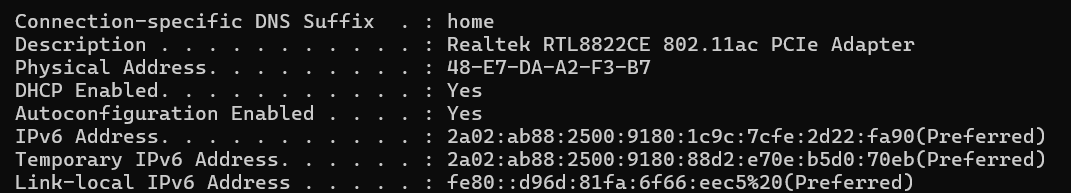
- Present the time diagram of the ARP/RARP, ICMP, ICMPv6, IPv4, IPv6, TCP, UDP and other traffics.



- What is the OUI code of the Cisco company?

The OUI for Cisco is usually **00:0a:41**

- What is the MAC address of the NIC module of your PC?



B) Identify the NIC MAC values according to the following questions:

- Where can you find the MAC OUI identifiers of NIC manufactoring companies on the Internet?

MAC OUI identifiers can be found in publicly available databases online. Websites like Wireshark's OUI Lookup Tool (https://www.wireshark.org/tools/oui-lookup.html) allow you to search for OUI codes.

- What are the MAC OUI codes of the following NIC manufacturing companies: Cisco, HP, Apple, Xiaomi, Huawei?

* Cisco: **00:0a:41**
* HP: **08:2E:5F**
* Apple: **00:17:F2**
* Xiaomi: **B4:5D:50**
* Huawei: **00:E0:FC**

4.3

A) What is the capture rule which filters the network traffic of your own PC in the case of Wireshark?

ip host 192.168.0.17(my ip)

B) What is the capture rule which filters only those frames that are sent for the broadcast address in the case of Wireshark?

This filter captures frames where the destination MAC address is the broadcast address (**ff:ff:ff:ff:ff:ff**).

eth.dst == ff:ff:ff:ff:ff:ff

4.4

A) What is the display rule which filters the network traffic of your own PC in the case of Wireshark?

ip.addr ==192.168.0.17

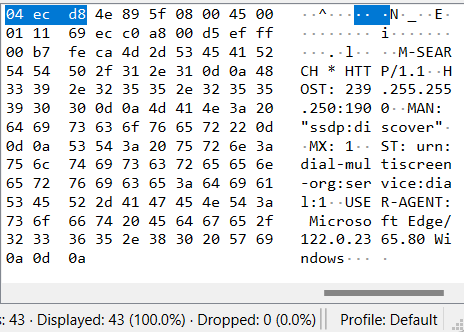
B) What is the display rule which filters only those frames that are sent for the broadcast address in the case of Wireshark?

eth.dst == ff:ff:ff:ff:ff:ff

4.5

A) In the case of Wireshark where can we find the tail of the captured frame?

* At the bottom of the Wireshark window, there is a "Packet Bytes" pane that displays the hexadecimal and ASCII representation of the selected packet.
* The ASCII representation shows the actual data, and you can scroll to the right to see the entire payload.



B) What do „.”characters indicate in the bottom field?

The "." characters in the bottom field of the "Packet Bytes" pane represent non-printable or control characters in the ASCII representation of the packet. These characters might include line feeds, carriage returns, or other control codes that don't have a visual representation.

In Wireshark's packet details, the ASCII representation is useful for quickly identifying the content of the packet payload. However, non-printable characters are represented as dots (".") to maintain readability. Printable characters (e.g., letters, numbers, symbols) will be displayed directly.