Networks Lab
Lab 3 Report

Roll No : CS14B051

Part 2

1) After physically setting up the systems, we have to manually configure the IP addresses of A and B's ethernet interfaces to belong to a subnet.

   This can be done using the command-

   sudo ifconfig eno0 192.168.123.23 netmask 255.255.255.0

   This has to be done on both A and B.

2) To verify , use **ping --new ip of B--** .
3) The using sudo **echo 1 > /proc/sys/net/ipv4/ip_forward** we enable ip forwarding between A and B.
4) Using **route add default gw 192.168.1.23 eno0** , we add A as the default gateway in B's routeing tables.
5) Then we configure NAT using

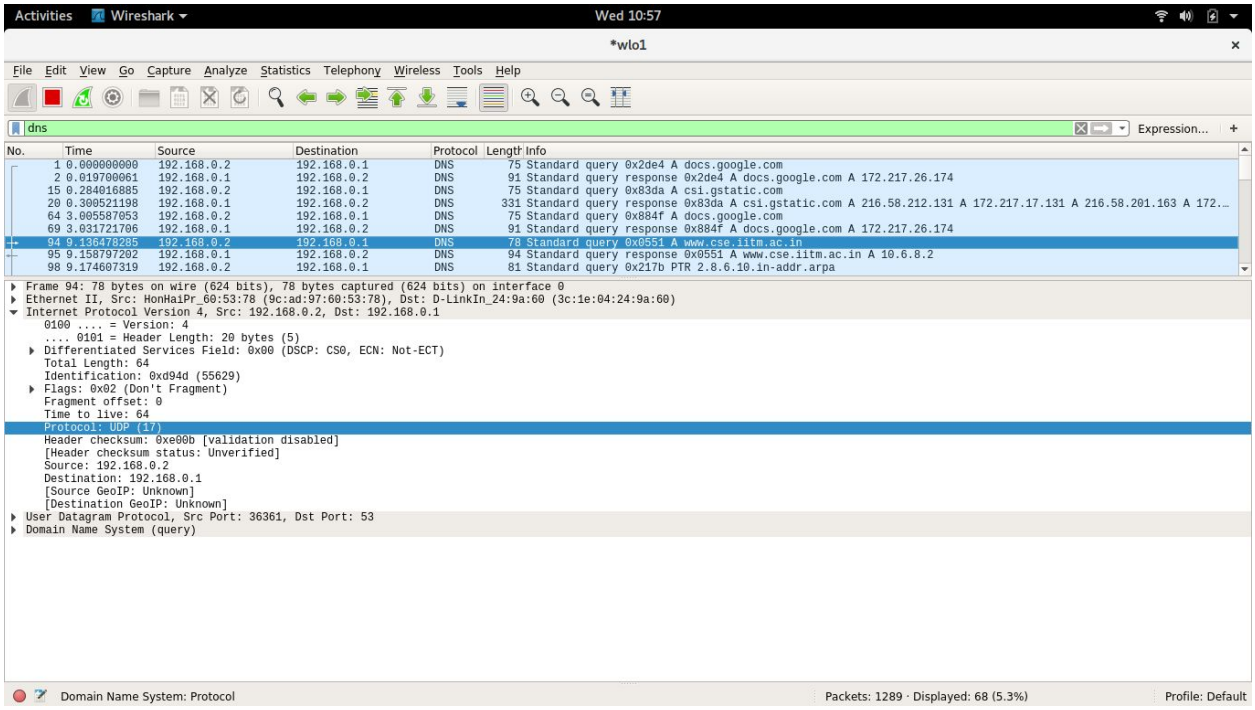
   ```
   # /sbin/iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE
   # /sbin/iptables -A FORWARD -i eth0 -o eth1 -m state
           --state RELATED,ESTABLISHED -j ACCEPT
   # /sbin/iptables -A FORWARD -i eth1 -o eth0 -j ACCEPT
   ```

6) We then set DNS server in B to institute server.

We are now able to use A's wireless internet connection in B.

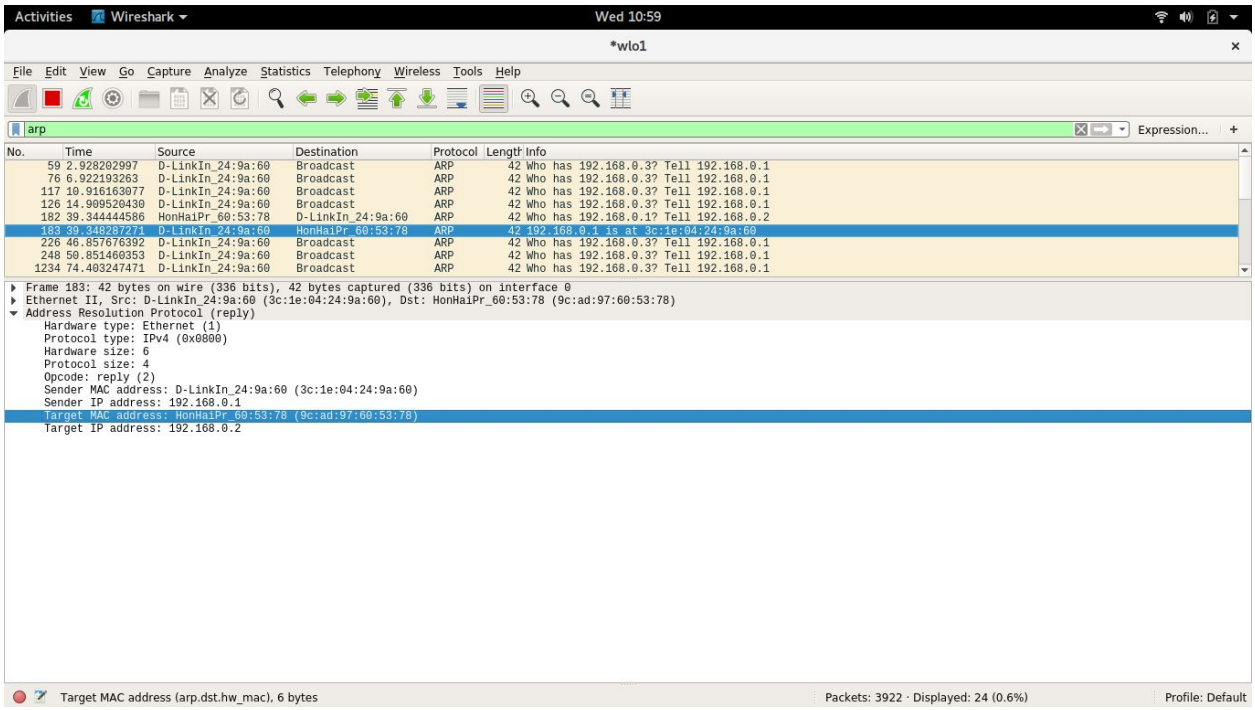
Part 3.1

1) DNS Reply and transport packets for cse.iitm.ac.in .Upon capturing DNS information in Wireshark using filter **DNS** we obtain the following packet.



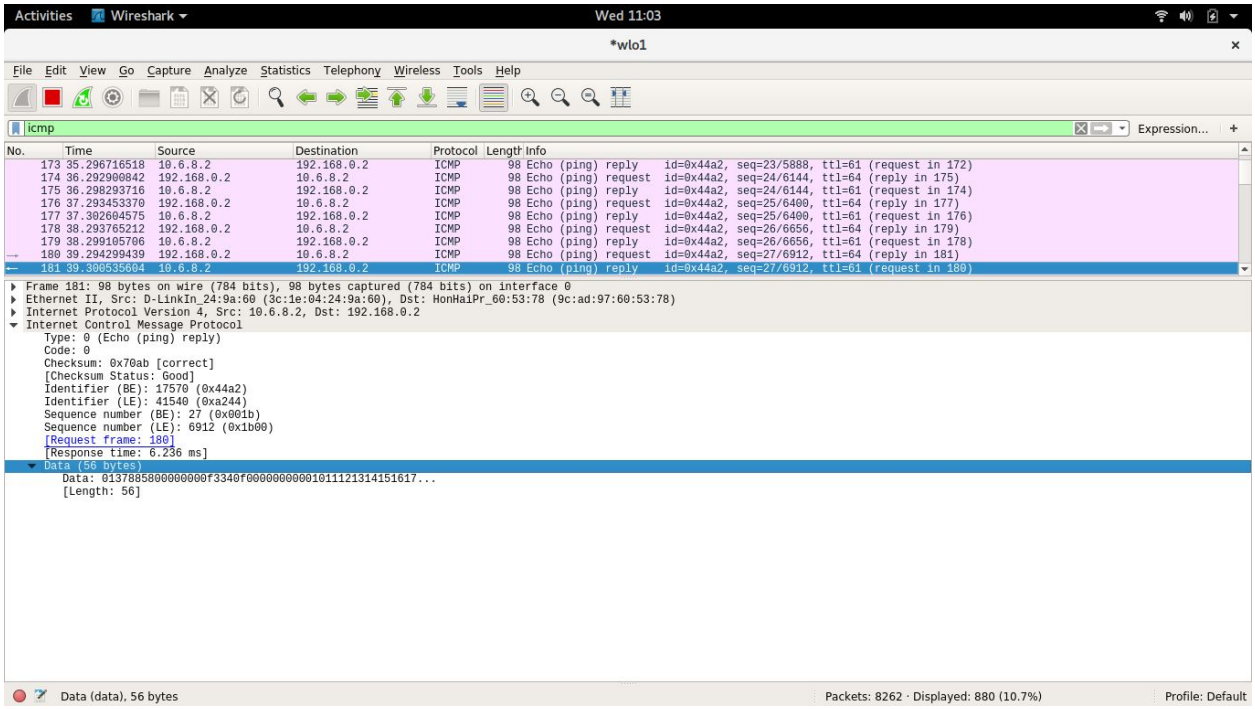
From above we see that the protocol used is **UDP.**

2) ARP Request and response. On using the filter **ARP** we get below. From this we conclude that the target MAC address is **00:00:00:00:00:00** for response**.F**



3) ICMP Echo and reply packets. Upon using the filter **ICMP** we obtain below. From below we conclude Type: 0,Data Size: 56 bytes,Data: 01:37:88:58:00:00:00:00:f3:34:0f:00:00:00:00:00:10:11:12:13:14:15:16:17:18:19:1a:1b:1c:1d:1e:1f:20:21:22:23:24:25:26:27:28:29:2a:2b:2c:2d:2e:2f:30:31:32:33:34:35:36:

37.

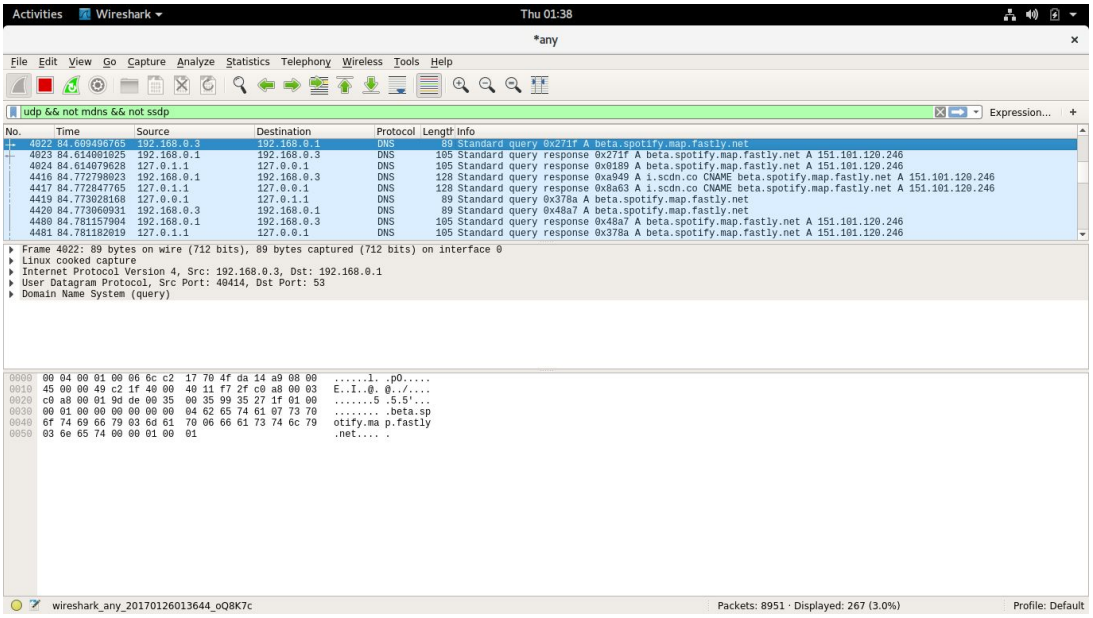


4) Wireshark wasn't able to capture HTTP requests.

5) Different filters i used were:

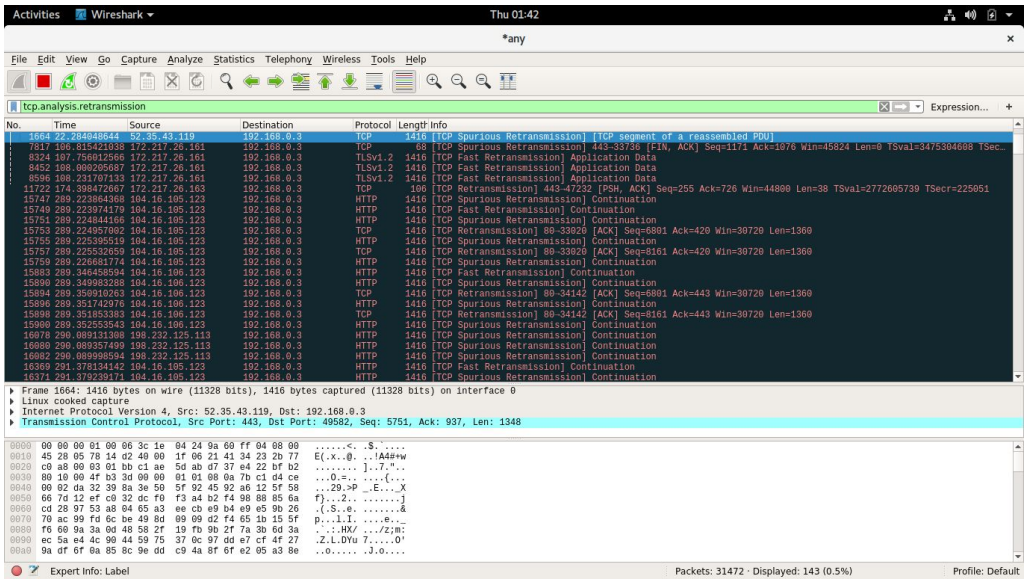
Udp && not mdns && ssdp

The only queries on my system using udp was the spotify application i was running.



tcp.analysis.retransmission

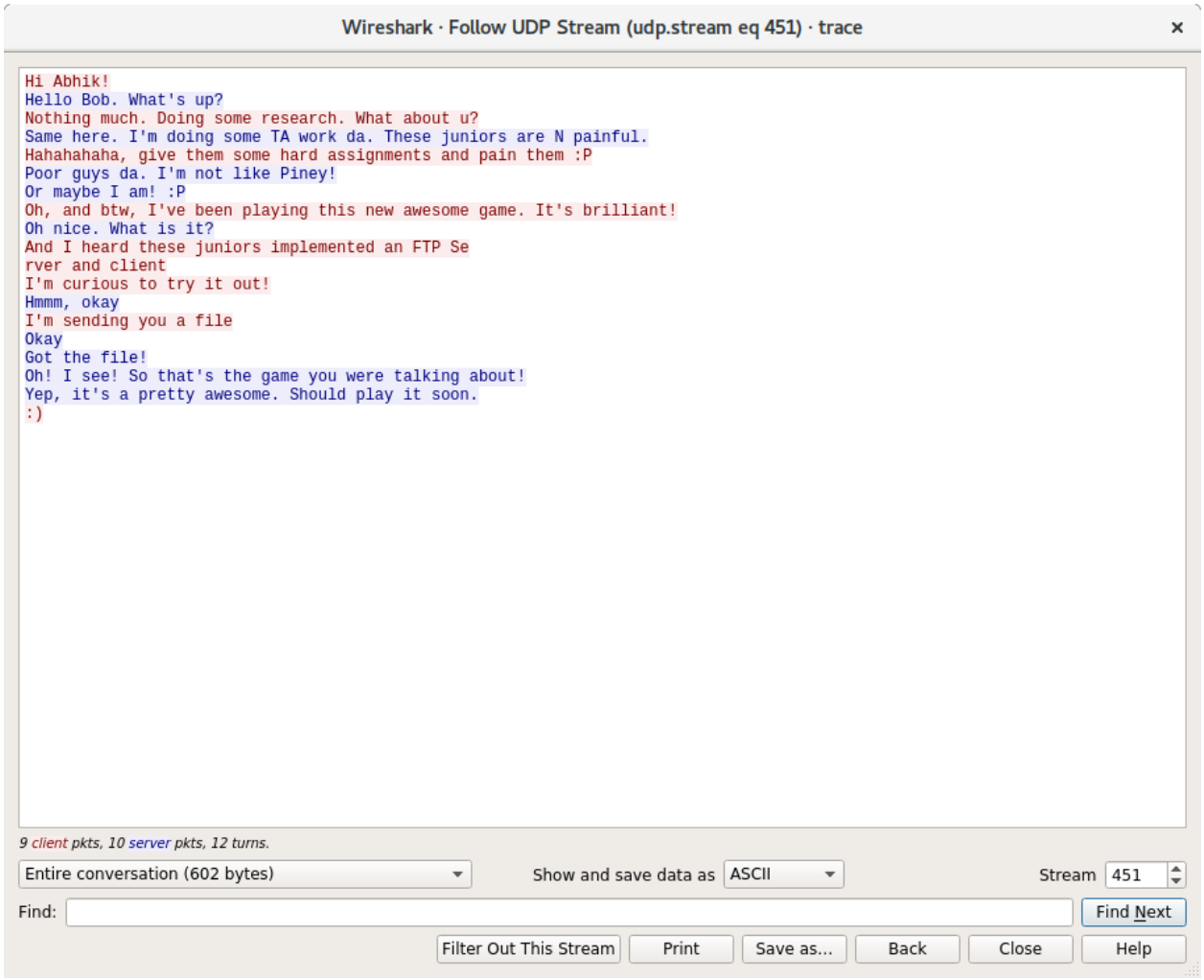
Helps analyze slow performance



Part 3.2

Method Followed

1) I first used the filter **UDP** to get all udp messages.
2) Then i started going through all the messages until i came across one.
3) Then using **Follow->UDP Stream** i was able to get the entire conversation.



4) Then realizing that there was a file transfer, using filter **tcp && ip.src == 10.6.15.92 && ip.dest==10.22.21.249** i was able to find a packet of the file.

5) Then using **Follow->TCP Stream,** I got the entire file.

6) Saving the file as raw data and running external terminal command **foremost** on it, I was able to obtain the image

Answers to questions

1) BOB - 10.22.21.249

   ABHIK - 10.6.15.92

2) 10 packets. The type of the file is Raw Data. The final image is jpg.
3) WatchDogs.