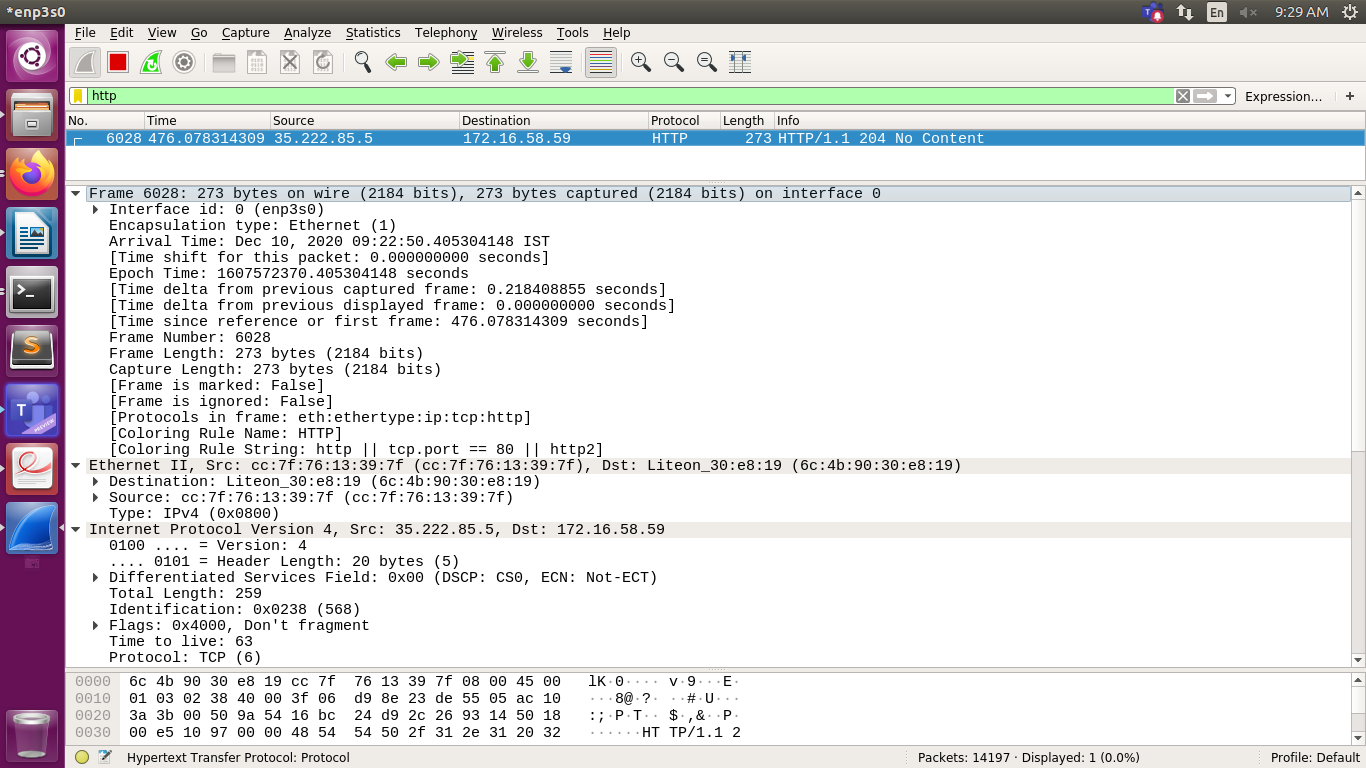
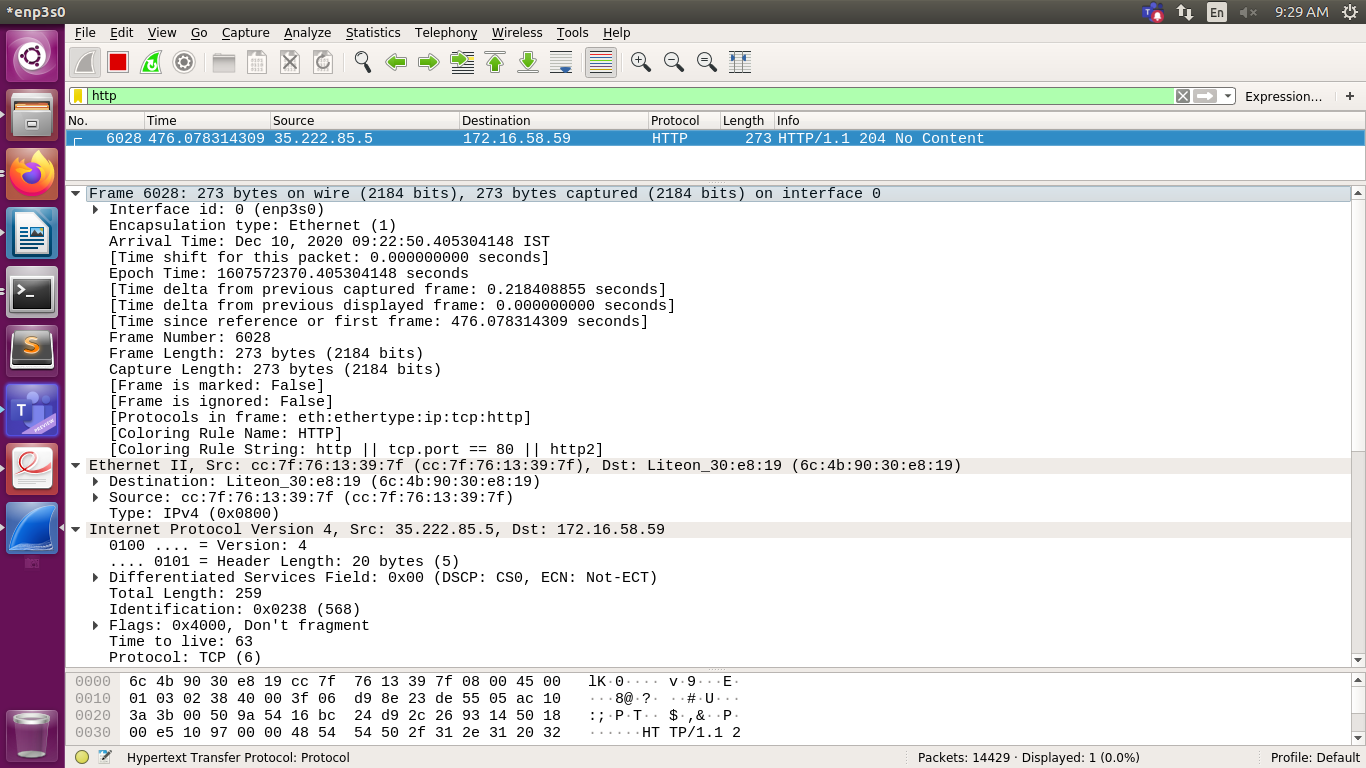
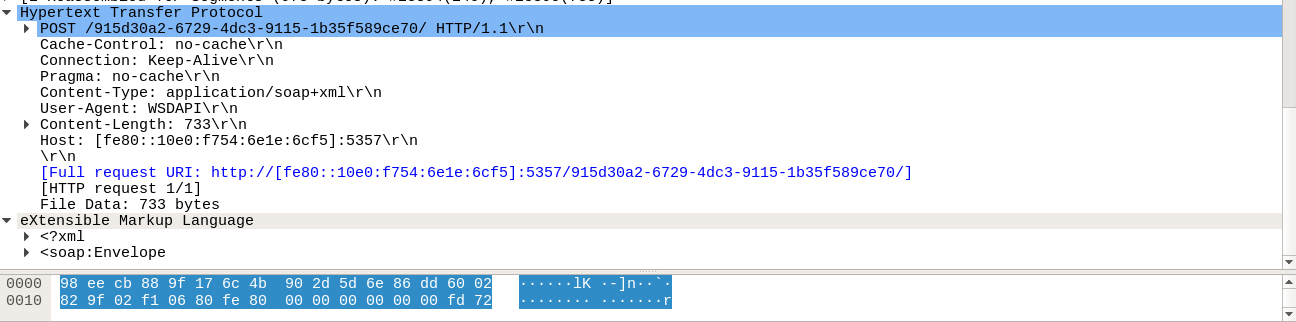
**Lab Session 2: Packet Analysis with Wireshark**

**PART-1 STUDY of Application Layer Protocols using Wireshark.**

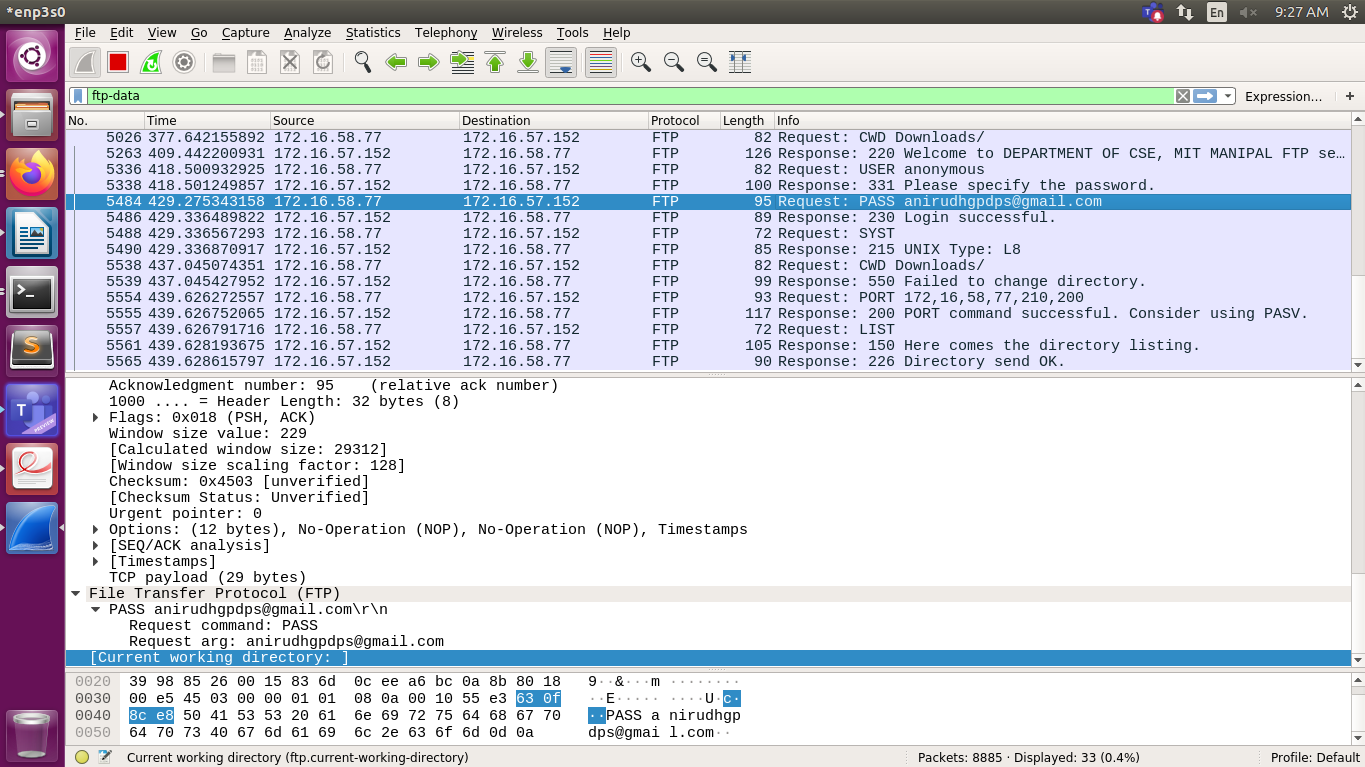
**Q 3.1.**  Retrieve web pages using HTTP. Use Wireshark to capture packets for analysis. Learn about most common HTTP messages. Also capture response messages and analyse them. During the lab session, also examine and analyse some HTTP headers.



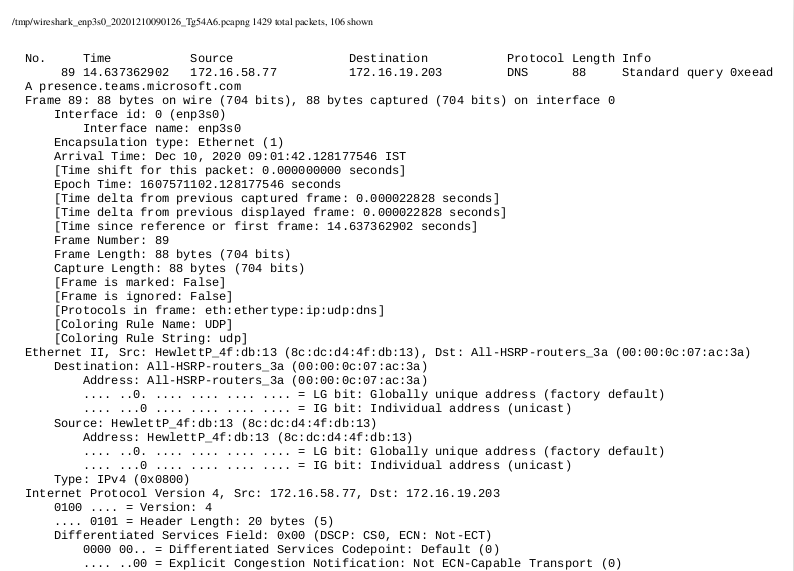


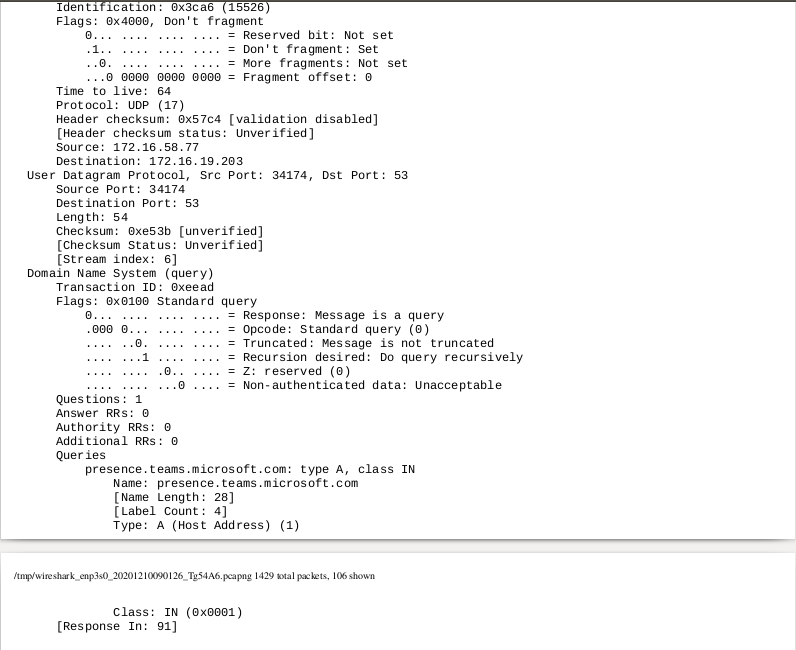


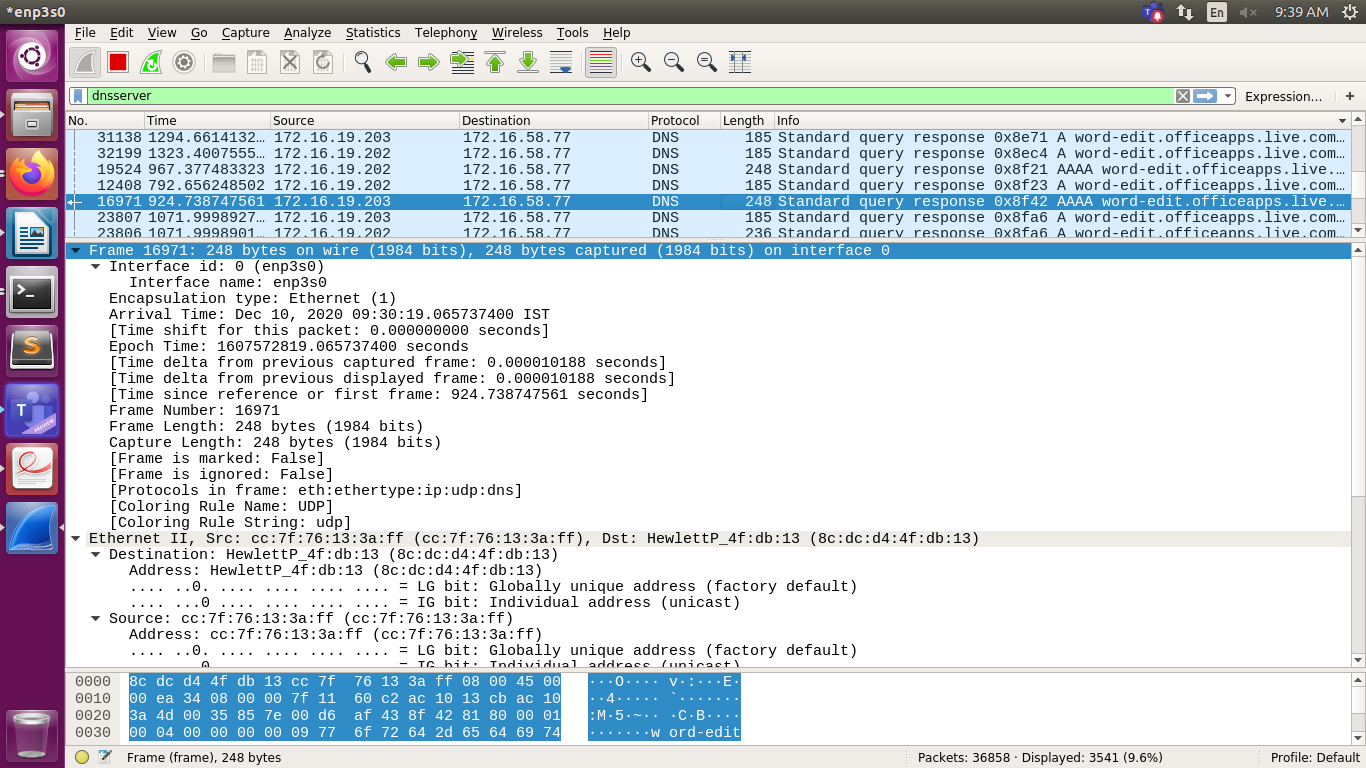
**Q 3.2**  Use FTP to transfer some files, Use Wireshark to capture some packets. Show that FTP uses two separate connections: a control connection and a data-transfer connection. The data connection is opened and closed for each file transfer activity. Also show that FTP is an insecure file transfer protocol because the transaction is done in plaintext.

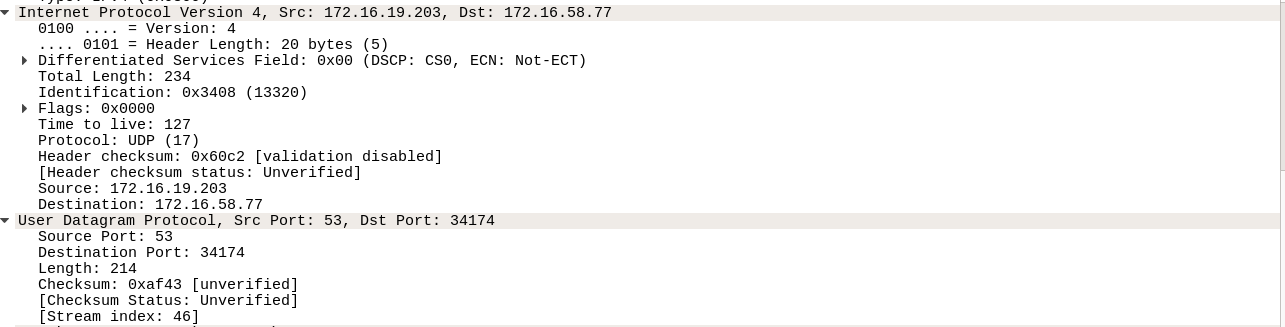


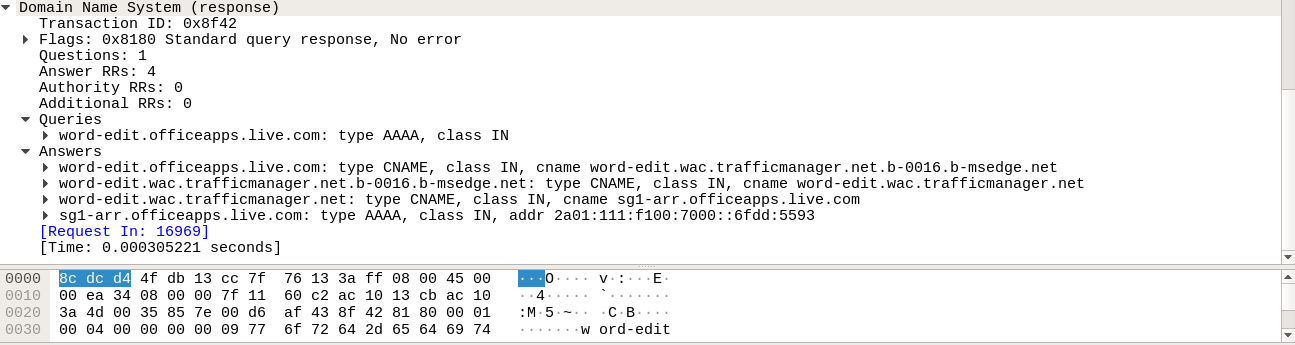
**Q 3.7**  Analyse the behaviour of the DNS protocol. In addition to Wireshark [Several network utilities are available for finding some information stored in the DNS servers. Eg. dig utilities (which has replaced nslookup). Set Wireshark to capture the packets sent by this utility.

]





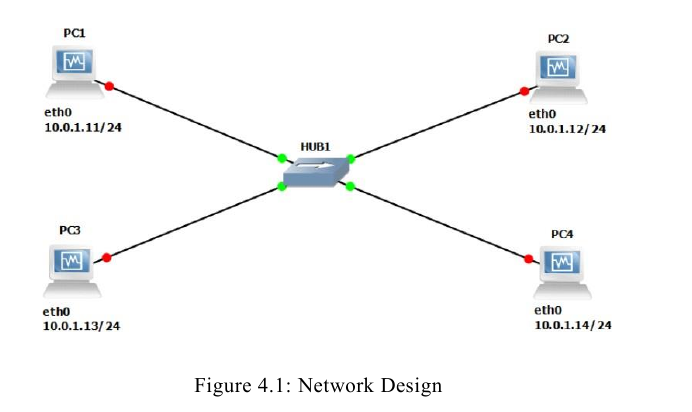


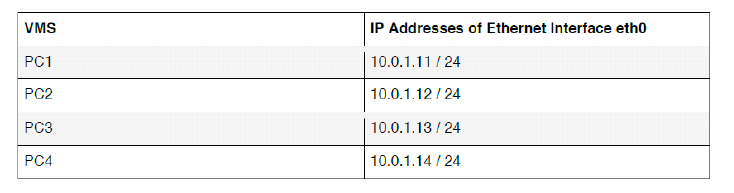


**PART-2 STUDY OF NETWORK DEVICES IN GNS3**

**Q 4.1 (a,b,c,d,e) and Q 4.3**

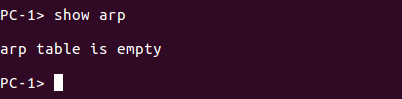
Design network configuration shown in Figure 4.1 for all parts. Connect all four VMs to a single Ethernet segment via a single hub as shown in Figure 4.1. Configure the IP addresses for the PCs as shown in Table 4.1.



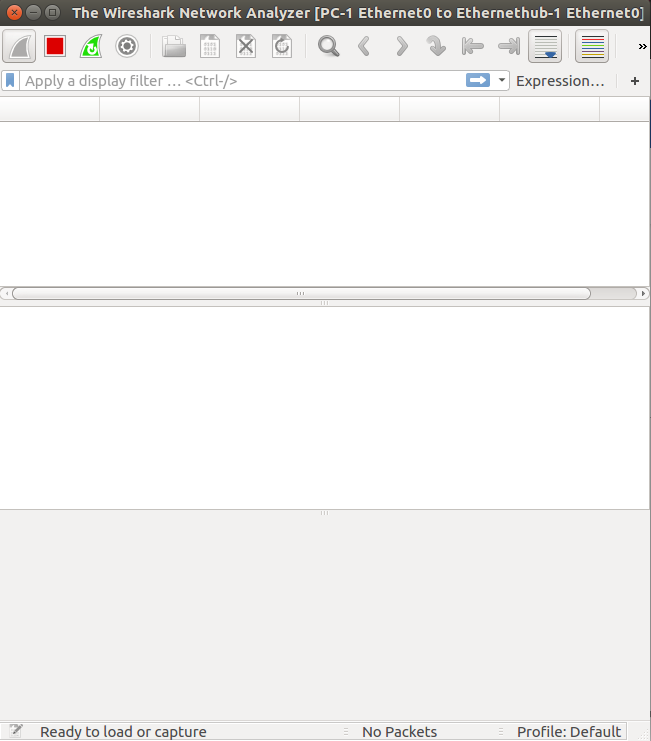


**a.** On PC1, view the ARP cache with ***show arp***

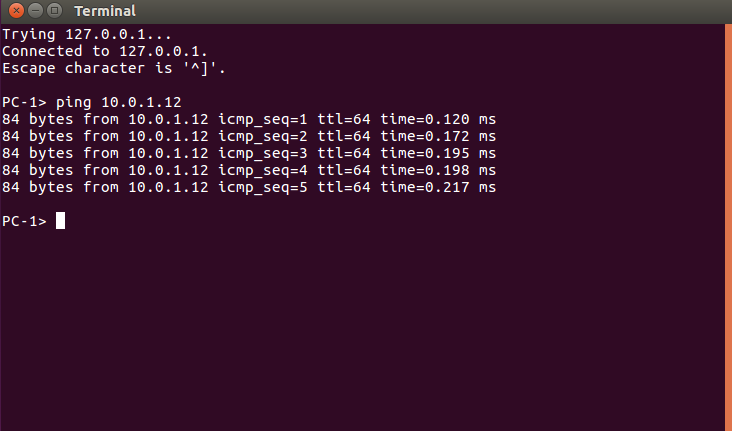




**b.** Start Wireshark on PC1-Hub1 link with a capture filter set to the IP address ofPC2.



**c.** Issue a ping command from PC1toPC2:



***PC1% ping 10.0.1.13 –c3***

Observe the ARP packets in the Wireshark window. Explore the MAC addresses in the Ethernet headers of the captured packets.

Direct our attention to the following fields:

• The destination MAC address of the ARP Request packets.

• The Type Field in the Ethernet headers of ARP packets.

d. View the ARP cache again with the command ***arp -a***. Note that ARP cache

entries can get refreshed/deleted fairly quickly (~2minutes).

***show arp***

e. Save the results of Wireshark.

**EXERCISES:**

• What is the destination MAC address of an ARP Request packet?

• What are the different Type Field values in the Ethernet headers that you observed?

• Use the captured data to analyse the process in which ARP acquires the MAC

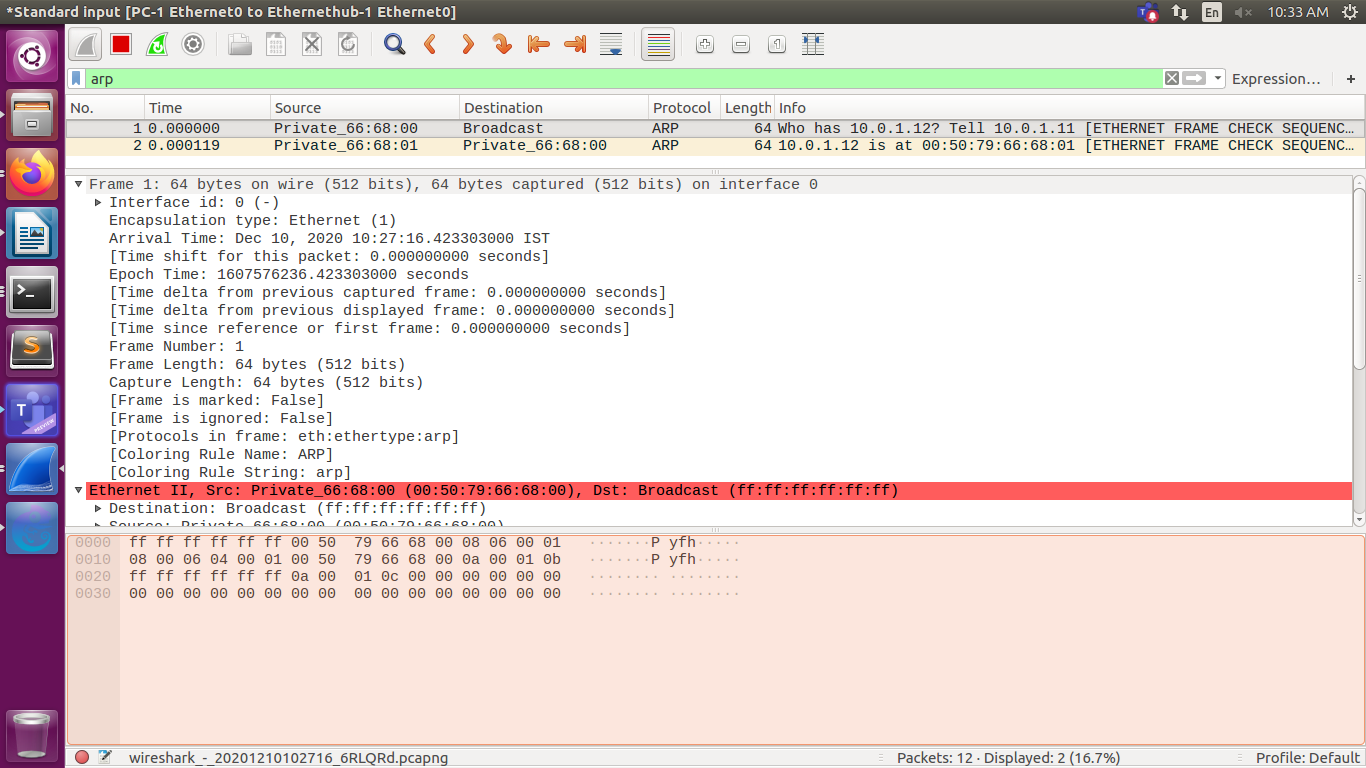
address for IP address10.0.1.12.

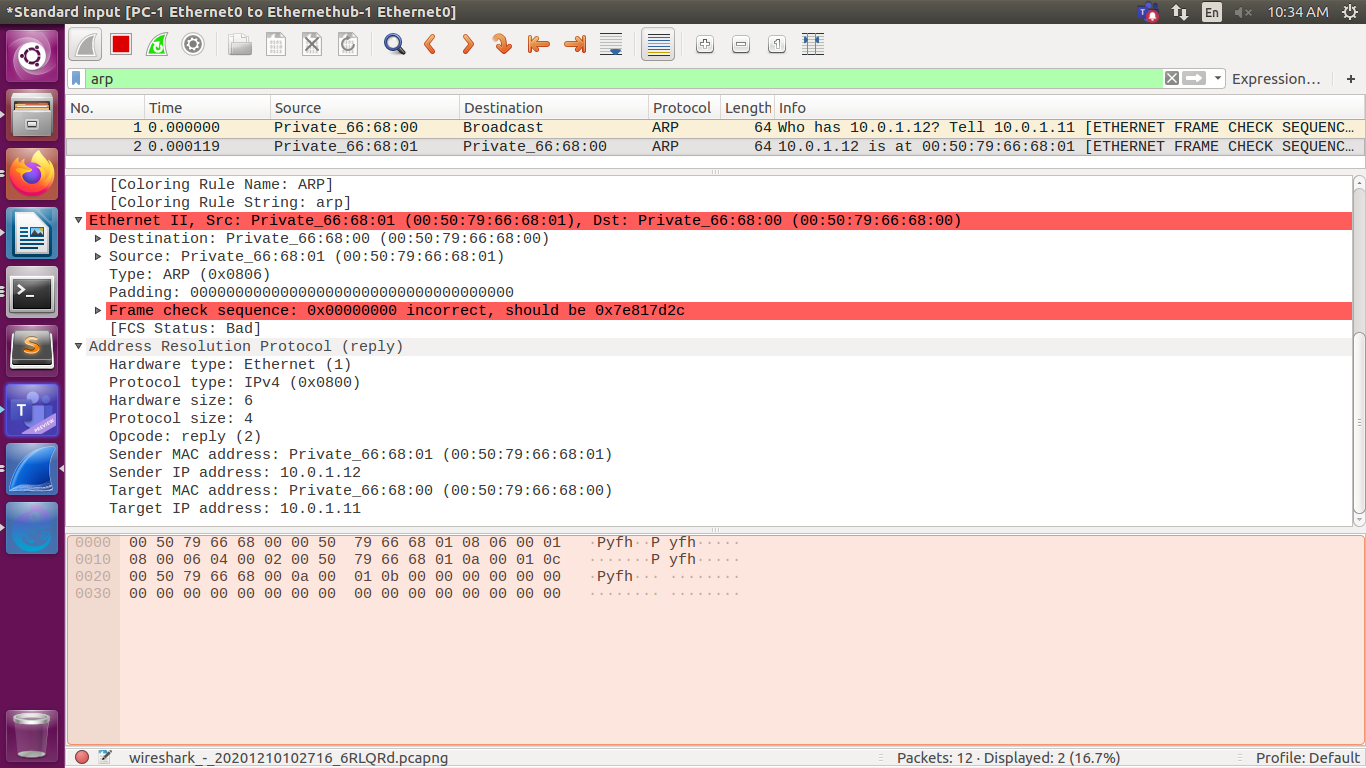
• Use your output data and ping results to explain what happened in each of the ping

commands.

• Which ping operations were successful, and which were unsuccessful? Why?

All of them were not successful.







**Q 4.2**

To test the effects of changing the netmask of a network configuration. Design the configuration as Q4.1 and replace the hub with a switch, two hosts (PC2 and PC4) have been assigned different network prefixes. Setup the interfaces of the hosts as follows:

VPCS IP Address of eth0 Network Mask

PC1 10.0.1.100/24 255.255.255.0

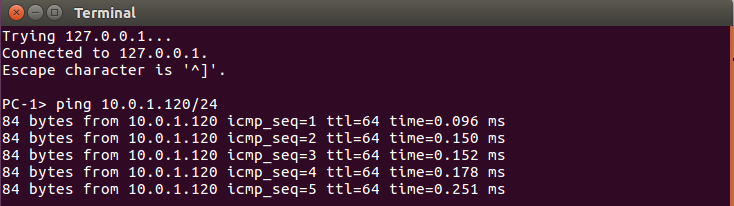
PC2 10.0.1.101/28 255.255.255.240

PC3 10.0.1.120/24 255.255.255.0

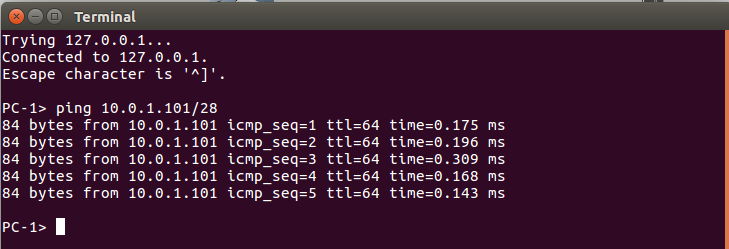
PC4 10.0.1.121/28 255.255.255.240

Run Wireshark on PC1-Switch1 link and capture the packets for the following scenarios

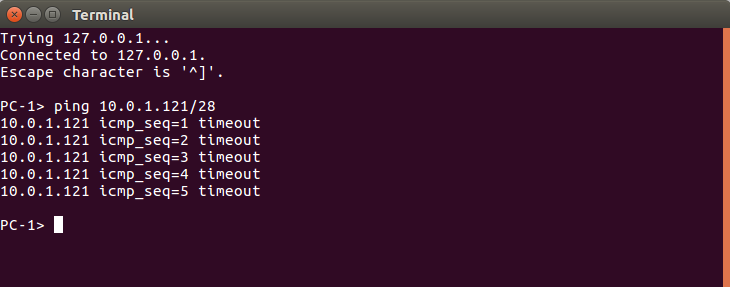
i. From PC1 ping PC3.



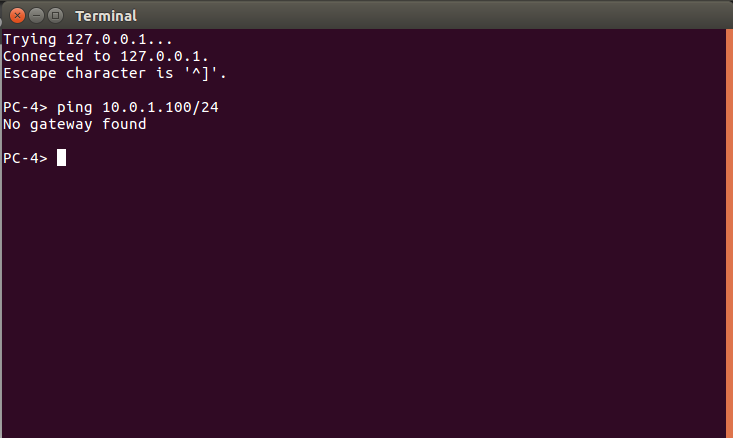
ii. From PC1 pingPC2.



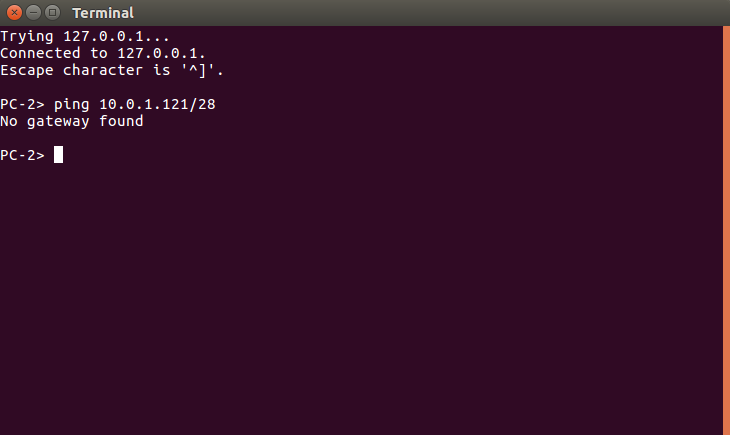
iii. From PC1 pingPC4.



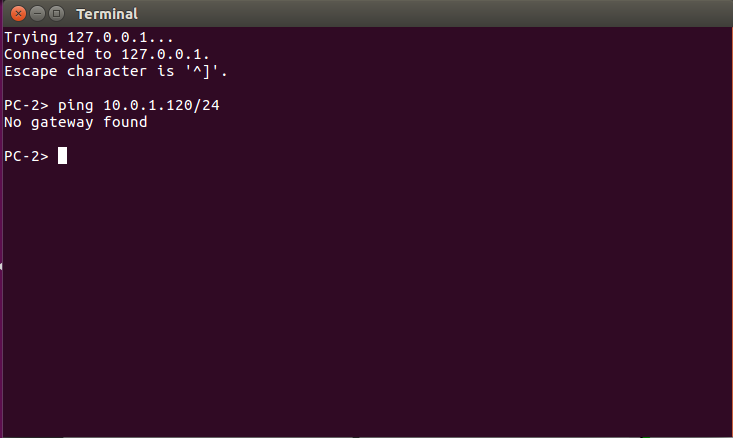
iv. From PC4 pingPC1.



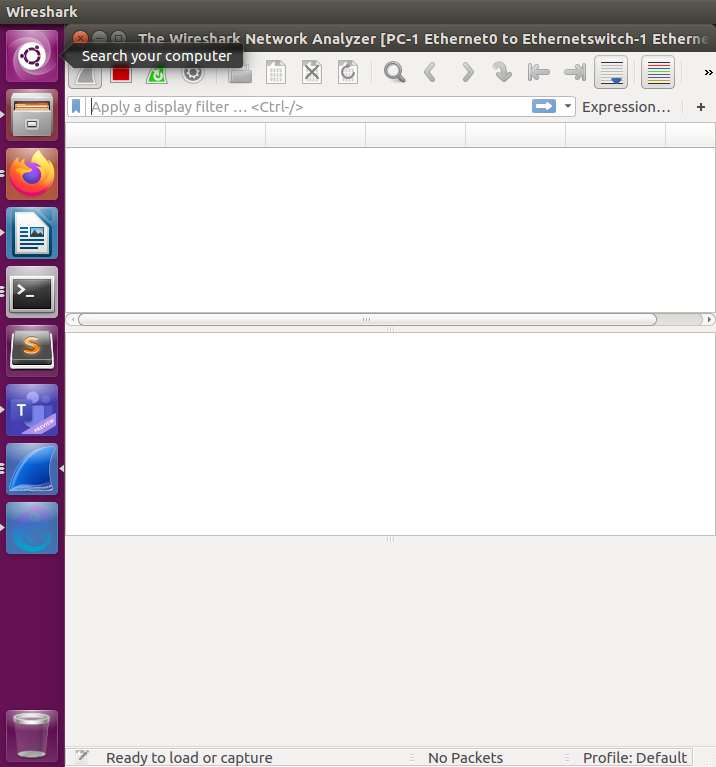
v. From PC2 ping PC4.



vi. From PC2 ping PC3.



Save the Wireshark output to a text file (using the “Packet Summary” option from “Print”) , and save the output of the ping commands. Note that not all of the above scenarios are successful. Save all the output including any error messages.



When you are done with the exercise, reset the interfaces to their original values as

Given Table4.1. (Note that /24 corresponds to network mask 255.255.255.0. and /28 to network mask 255.255.255.240).