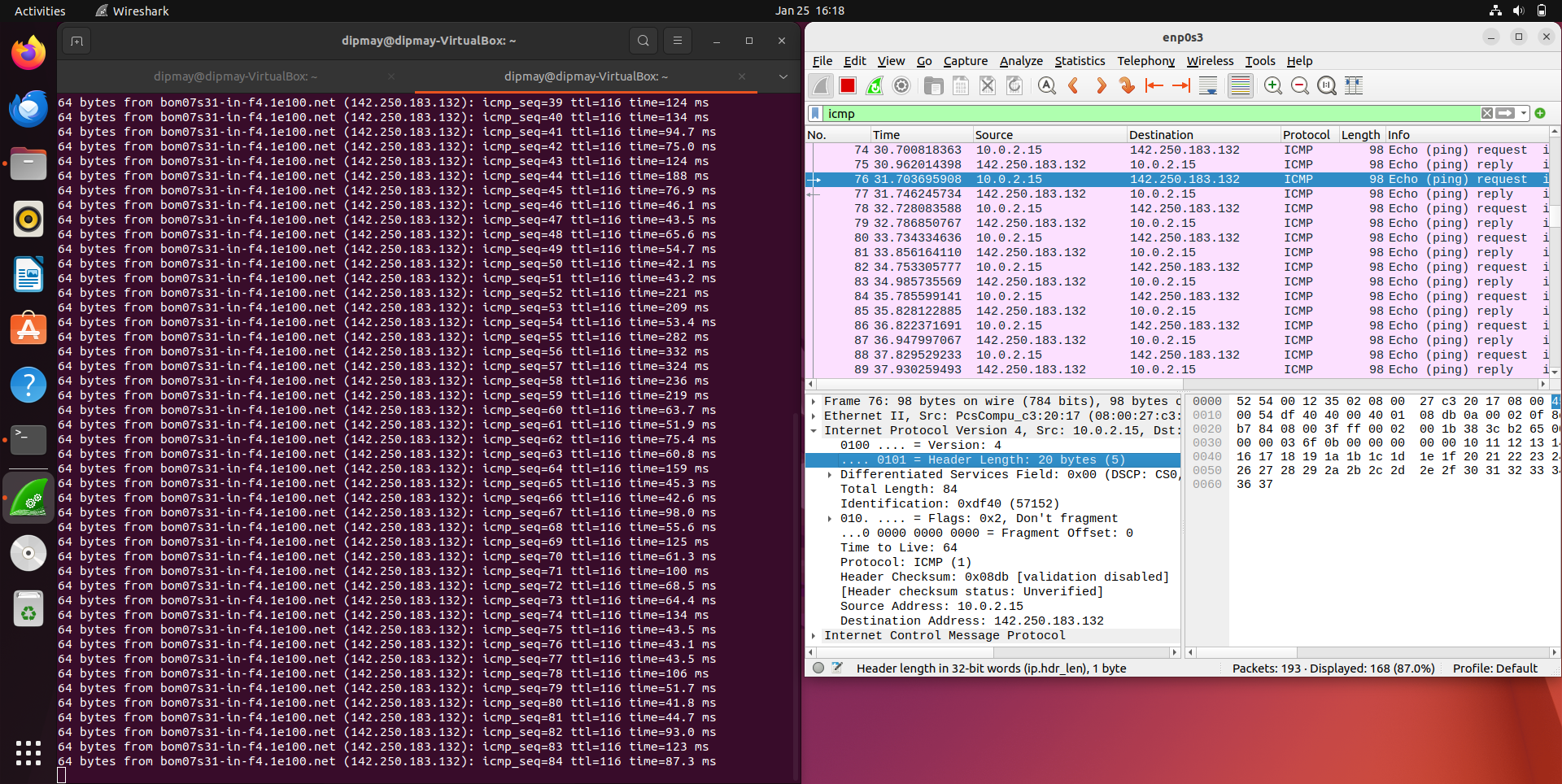
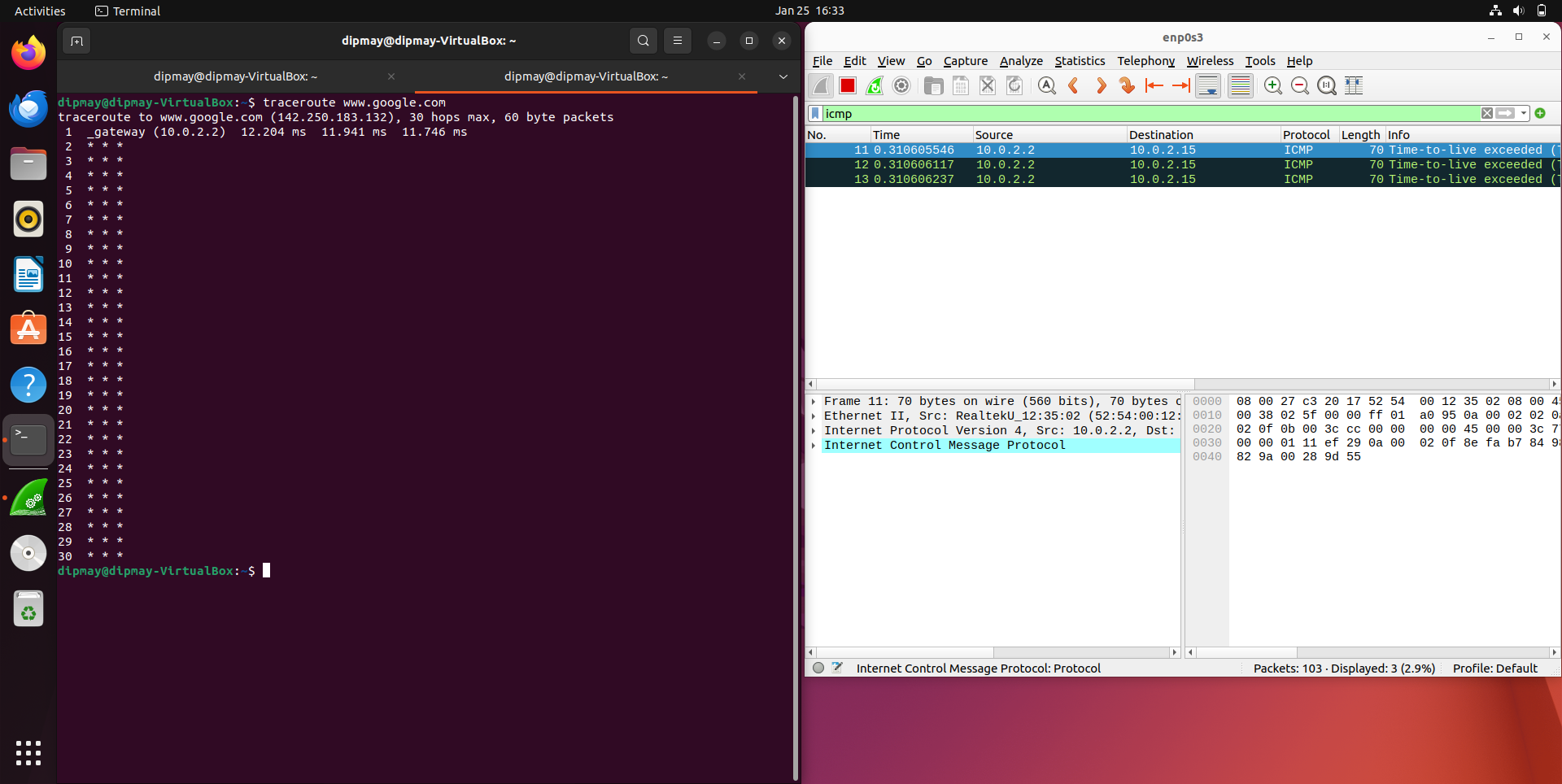
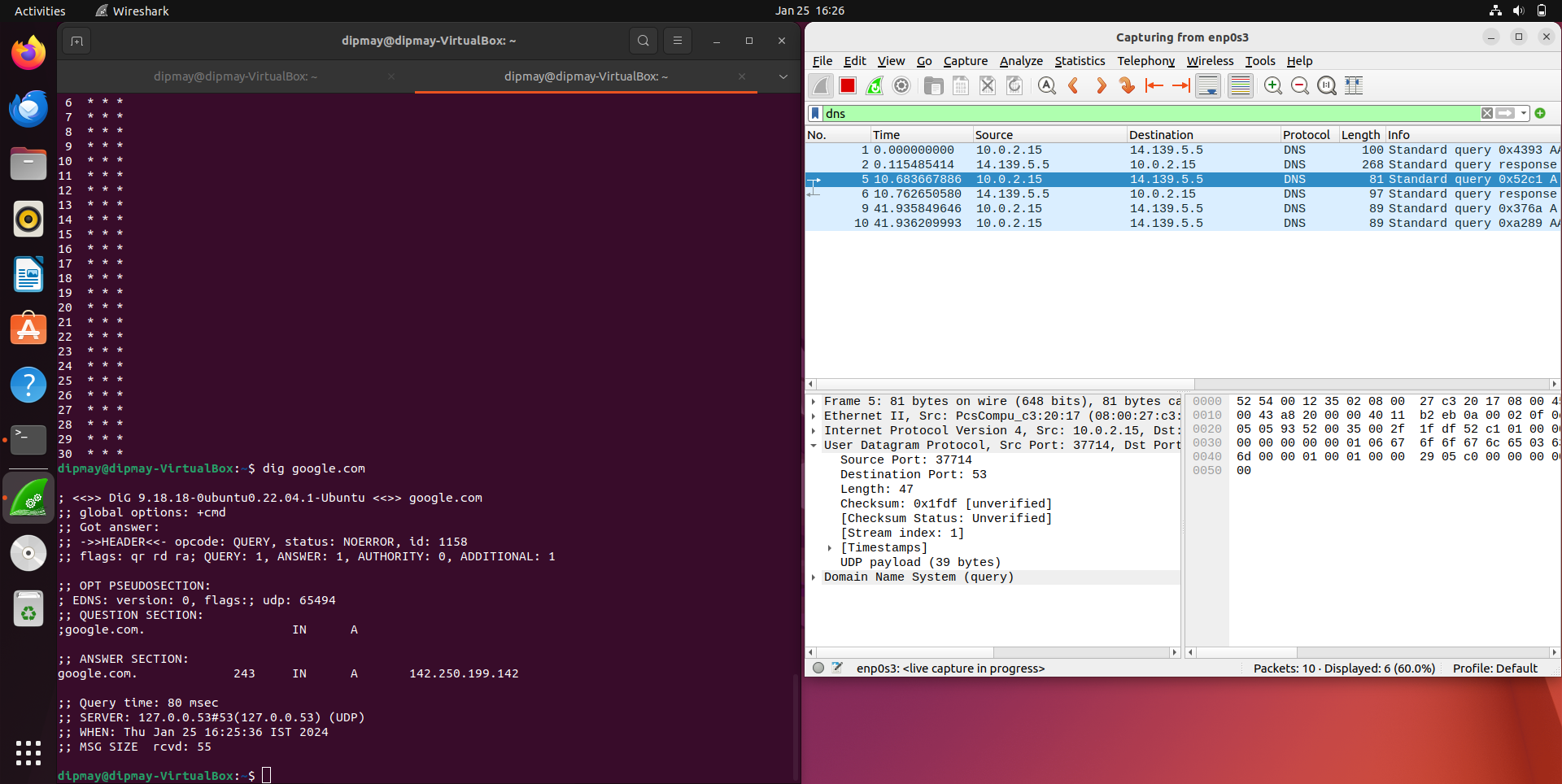
***EXPLORING WIRESHARK TOOL***

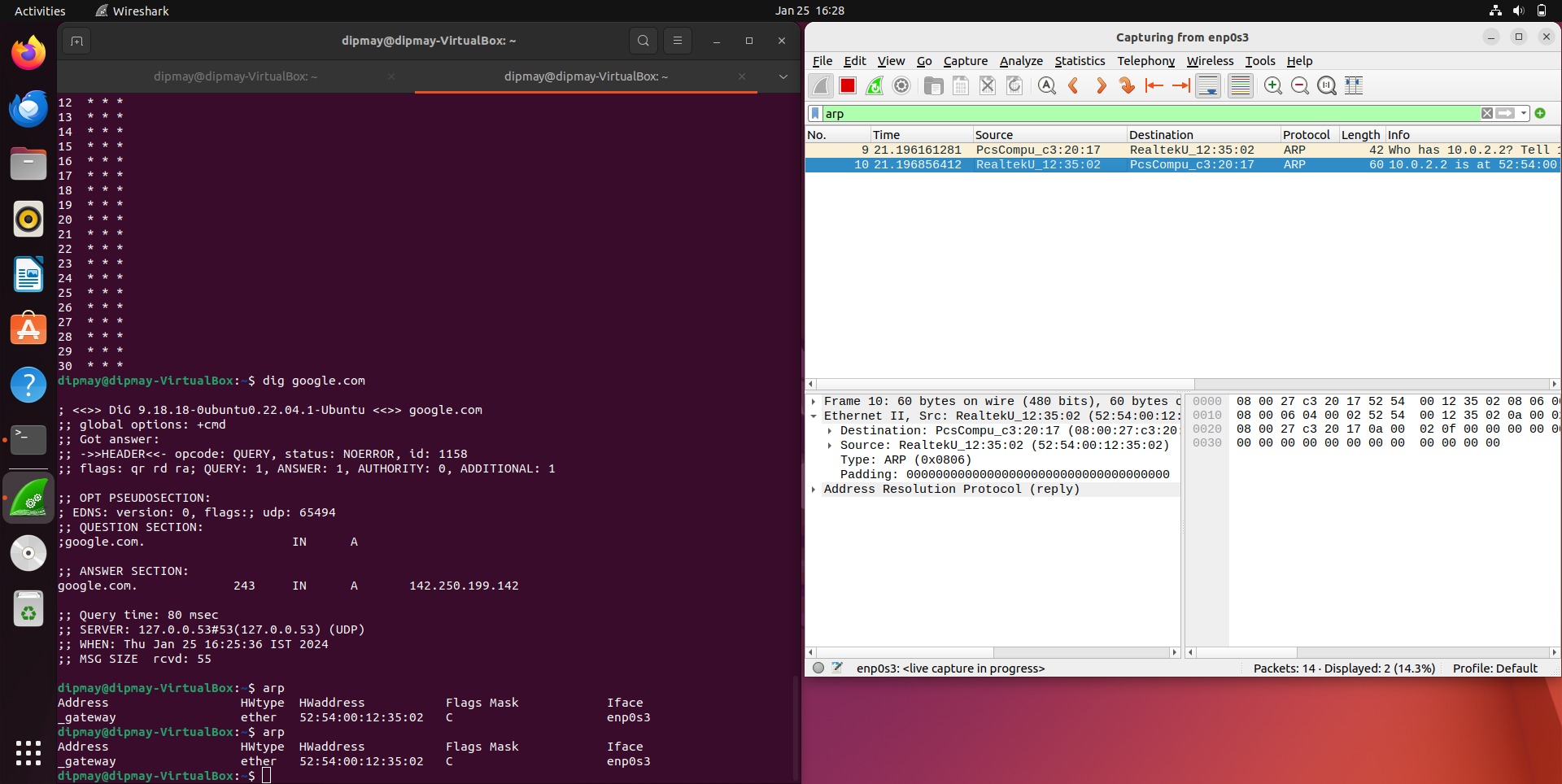
**Dipmay Biswas (2021CSB043)**

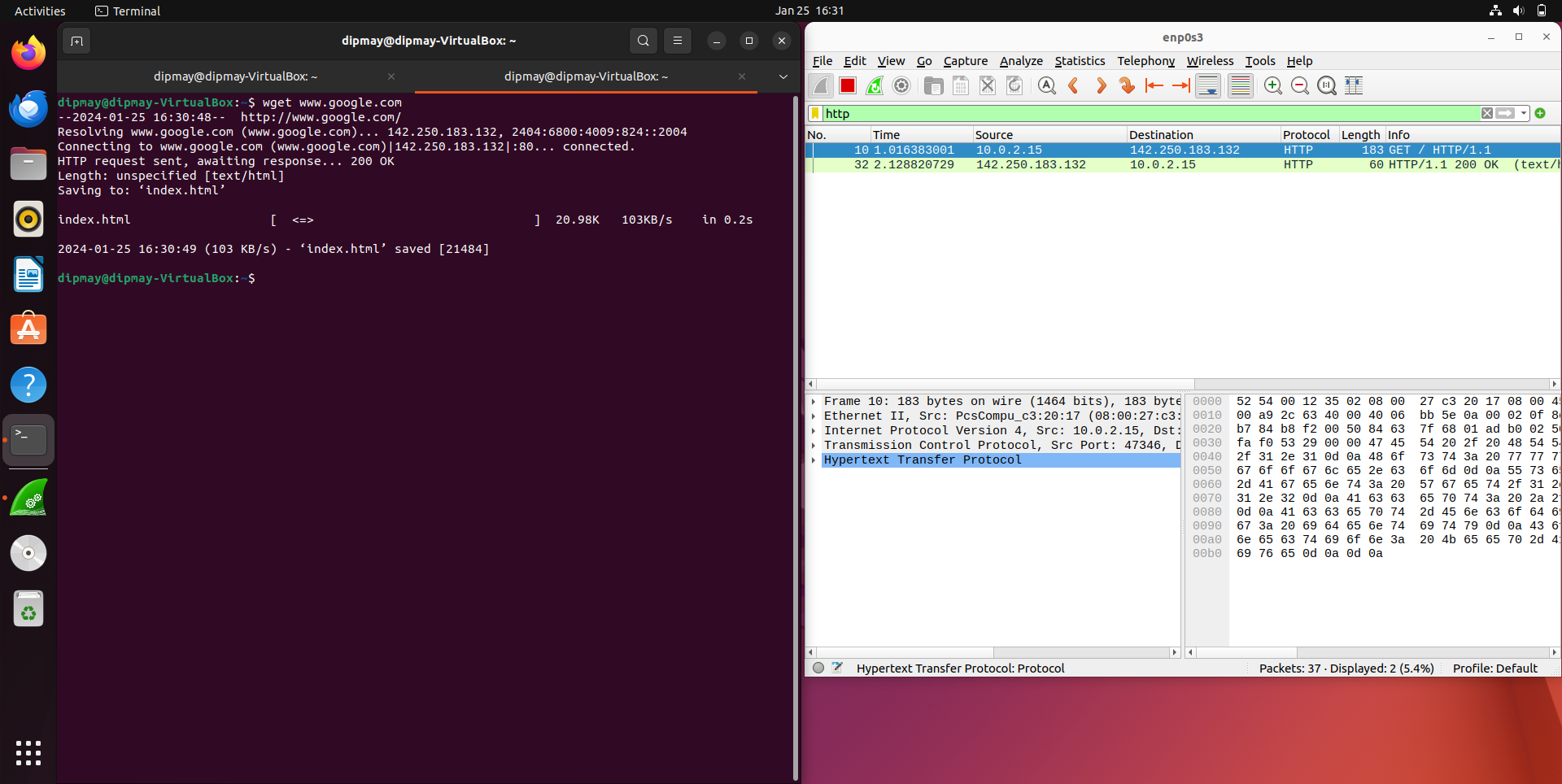
Q1) Analyse the packets (across all layers)exchanged with your computer while executing the following commands ∶ (i) 𝐩𝐢𝐧𝐠



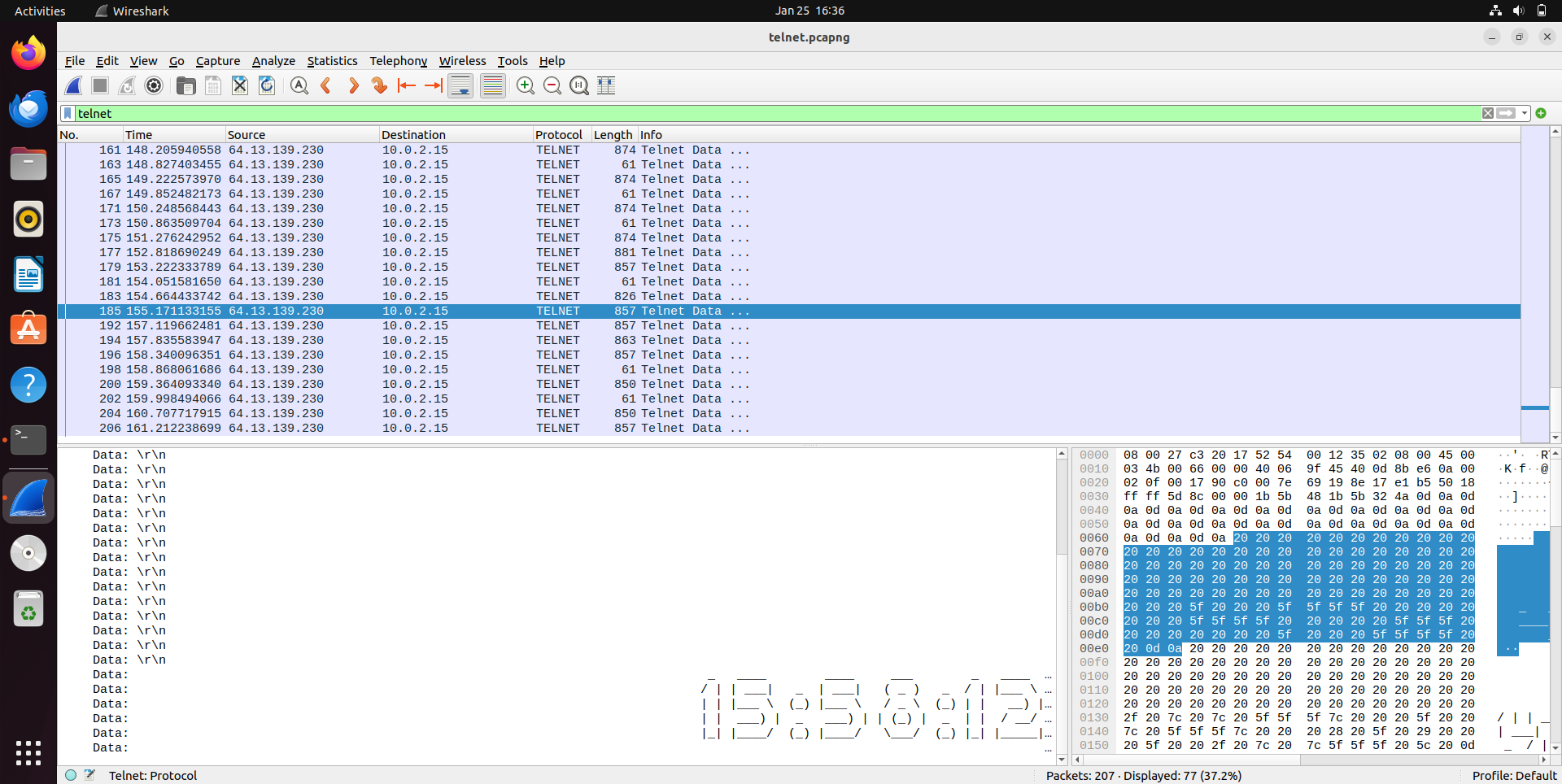
Q1) Analyse the packets (across all layers)exchanged with your computer while executing the following commands ∶ (ii) 𝐭𝐫𝐚𝐜𝐞𝐫𝐨𝐮𝐭𝐞 

Q1) Analyse the packets (across all layers)exchanged with your computer while executing the following commands ∶ (iii) **dig**

Q1) Analyse the packets (across all layers)exchanged with your computer while executing the following commands ∶ (iv) **arp**

Q1) Analyse the packets (across all layers)exchanged with your computer while executing the following commands∶ (v) 𝐰𝐠𝐞𝐭

Q2) Capture the packets while sending/receiving telnet requests/responses between your computer and a custom server running the telnet daemon. What is your observation while analyzing the application layer data?

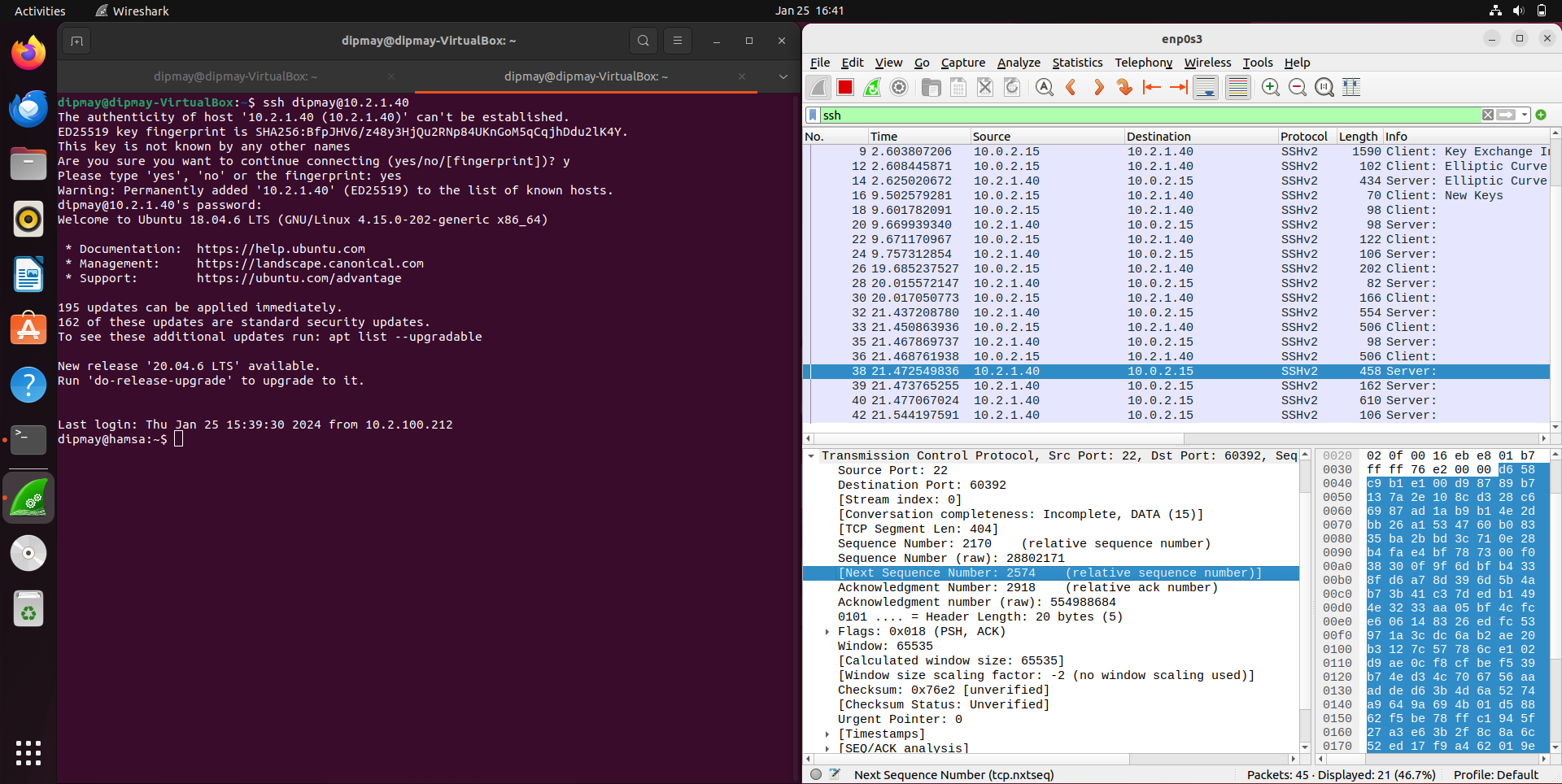


TCP protocols follow 3-way handshaking.

Port Number for Telnet ∶ 23

The application layer is **unsecured** as no key exchange mechanism is present like ssh.

Q3) Capture the packets while sending/receiving ssh requests/responses between your computer and one of the department servers. What is your observation while analyzing the application layer data?



Port Number for ssh ∶ 22

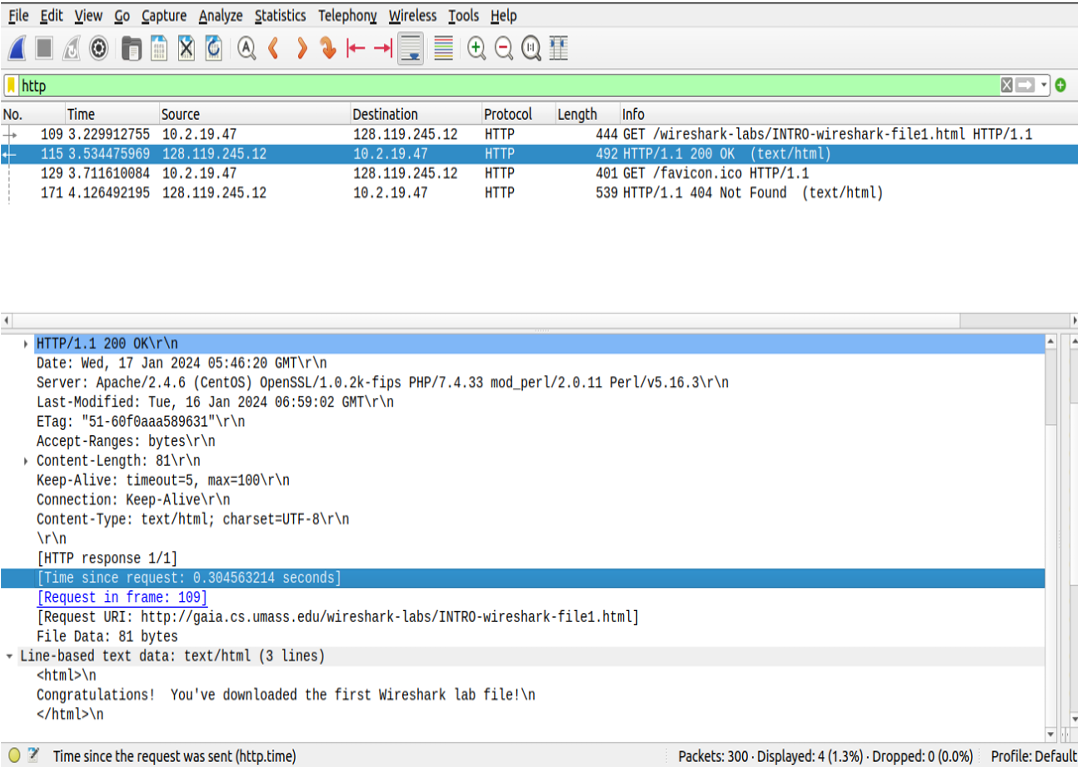
It is used for remote login.

It is much more **secure** in comparison to telnet.

Key exchange occurs and then proceeds.

Elliptic Curve Diffie − HellmanKey Exchange

.Q4) Enter the URL ∶ ℎ𝑡𝑡𝑝://𝑔𝑎𝑖𝑎.𝑐𝑠.𝑢𝑚𝑎𝑠𝑠.𝑒𝑑𝑢/𝑤𝑖𝑟𝑒𝑠ℎ𝑎𝑟𝑘 − 𝑙𝑎𝑏𝑠/𝐼𝑁𝑇𝑅𝑂 − 𝑤𝑖𝑟𝑒𝑠ℎ𝑎𝑟𝑘 − 𝑓𝑖𝑙𝑒1.ℎ𝑡𝑚𝑙 and capture packets using Wireshark. After your browser has displayed the INTRO−wireshark−file1.html page (it is a simple one-line of congratulations), stop Wireshark packet capture.



Answer the following from the captured packets ∶

(a) How long did it take from when the HTTP GET message was sent until the HTTP OK reply was received?

Ans) **0**.**304563214 sec.**

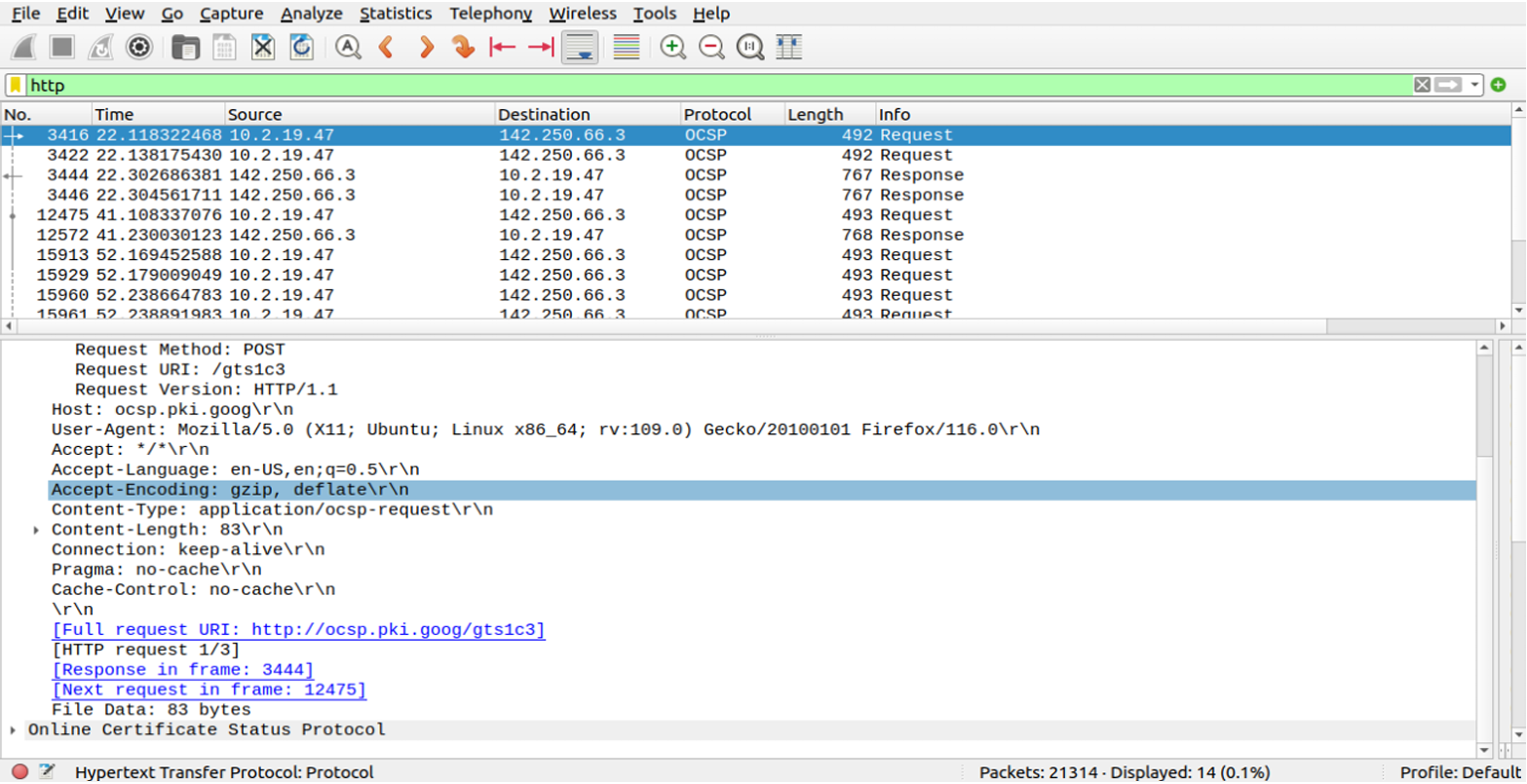
(b) What is the Internet address of the gaia.cs.umass.edu? What is the Internet address of your computer? Support your answer with an appropriate screenshot from your computer.

Ans) **128.119.245.12** & **10.2.19.47**

Q5) Start the Wireshark packet capturing service. Enter the URL ∶

https://www.gmail.com on your browser and sign− in to your gmail account by providing credentials (Username/Password).

Answer the following from the captured packets ∶



(a) Is there any difference in the application layer protocol?

Ans) **Yes!!**(b) How is it different from the HTTP data you analyzed in the above problem?  
  
Ans) **It is much more secure than HTTP protocol as it uses OCSP.**