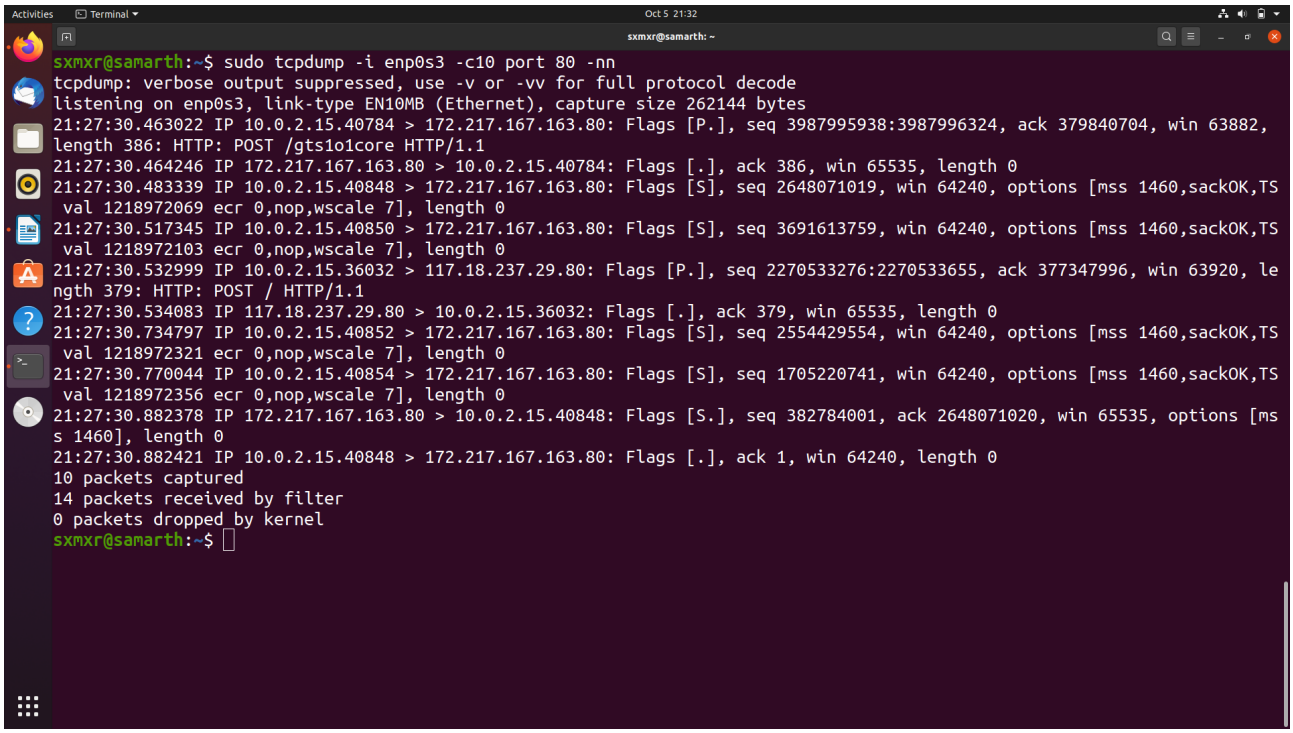
CN Assignment 3 & 4

Question 1

A)



```
sxmxr@samarth:~$ sudo tcpdump -i enp0s3 -c10 port 80 -nn
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on enp0s3, link-type EN10MB (Ethernet), capture size 262144 bytes
21:27:30.463022 IP 10.0.2.15.40784 > 172.217.167.163.80: Flags [P.], seq 3987995938:3987996324, ack 379840704, win 63882,
length 386: HTTP: POST /gts1o1core HTTP/1.1
21:27:30.464246 IP 172.217.167.163.80 > 10.0.2.15.40784: Flags [.], ack 386, win 65535, length 0
21:27:30.483339 IP 10.0.2.15.40848 > 172.217.167.163.80: Flags [S], seq 2648071019, win 64240, options [mss 1460,sackOK,TS
 val 1218972069 ecr 0,nop,wscale 7], length 0
21:27:30.517345 IP 10.0.2.15.40850 > 172.217.167.163.80: Flags [S], seq 3691613759, win 64240, options [mss 1460,sackOK,TS
 val 1218972103 ecr 0,nop,wscale 7], length 0
21:27:30.532999 IP 10.0.2.15.36032 > 117.18.237.29.80: Flags [P.], seq 2270533276:2270533655, ack 377347996, win 63920, le
ngth 379: HTTP: POST / HTTP/1.1
21:27:30.534083 IP 117.18.237.29.80 > 10.0.2.15.36032: Flags [.], ack 379, win 65535, length 0
21:27:30.734797 IP 10.0.2.15.40852 > 172.217.167.163.80: Flags [S], seq 2554429554, win 64240, options [mss 1460,sackOK,TS
 val 1218972321 ecr 0,nop,wscale 7], length 0
21:27:30.770044 IP 10.0.2.15.40854 > 172.217.167.163.80: Flags [S], seq 1705220741, win 64240, options [mss 1460,sackOK,TS
 val 1218972356 ecr 0,nop,wscale 7], length 0
21:27:30.882378 IP 172.217.167.163.80 > 10.0.2.15.40848: Flags [S.], seq 382784001, ack 2648071020, win 65535, options [ms
s 1460], length 0
21:27:30.882421 IP 10.0.2.15.40848 > 172.217.167.163.80: Flags [.], ack 1, win 64240, length 0
10 packets captured
14 packets received by filter
0 packets dropped by kernel
sxmxr@samarth:~$
```

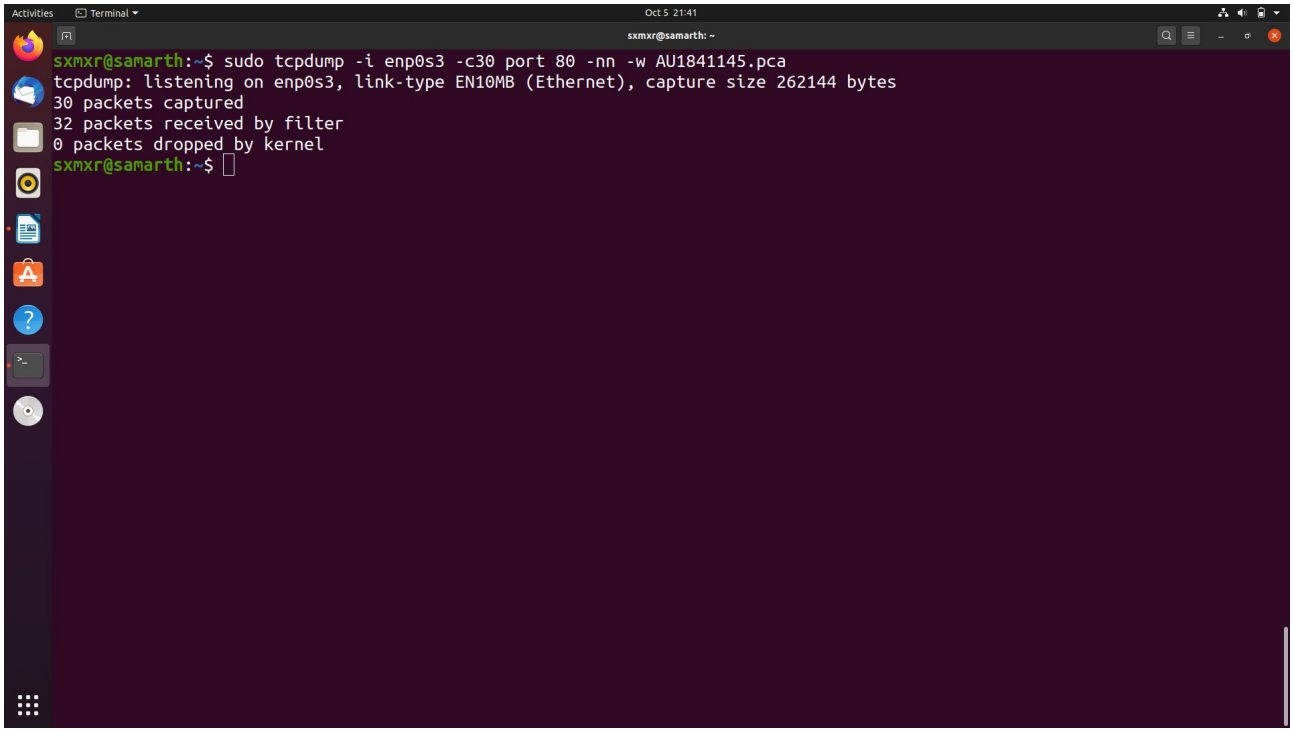
B) Source IP : 10.0.2.15
Source Packet : 40784

Destination IP : 172.217.167.163
Destination Port : 80

C) It took 0.001s from when the HTTP GET message was sent until the HTTP OK was recevied.

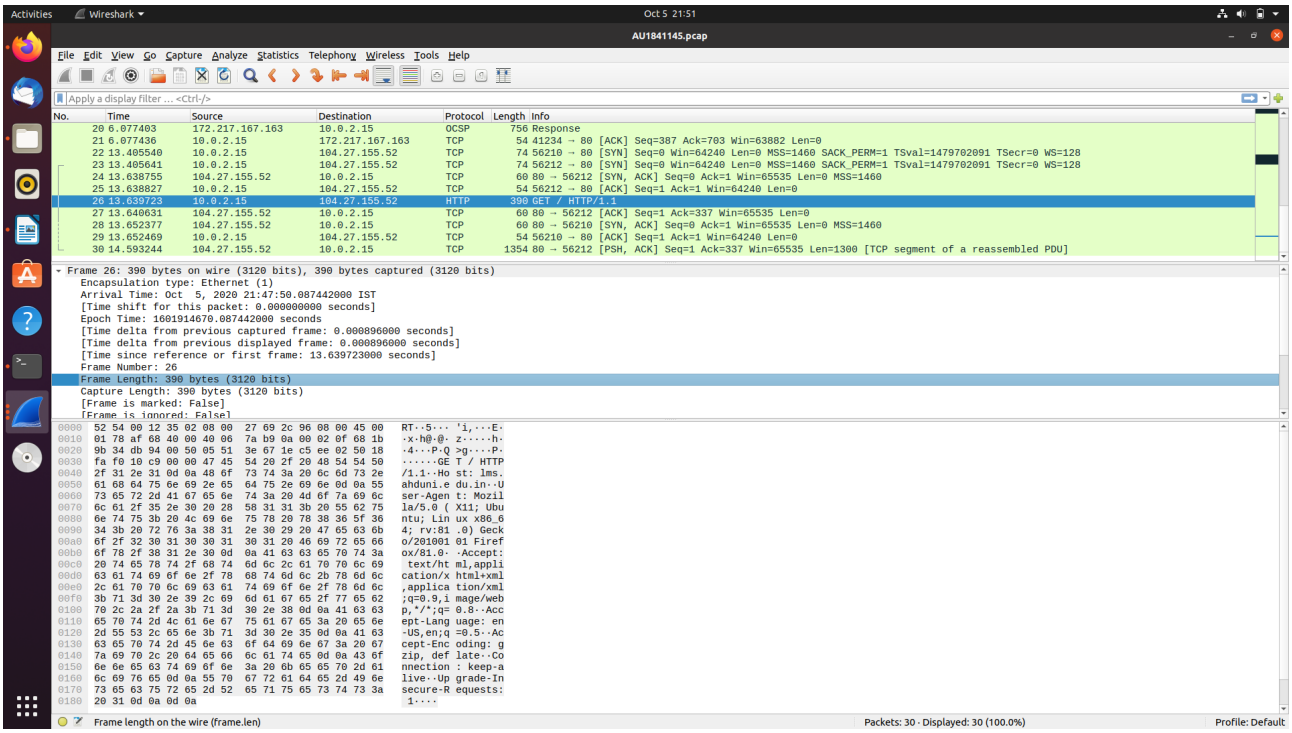
D) 10.0.2.15 is the Internet address of my computer. 172.217.167.163 is the Internet address of the URL I visited.

E)

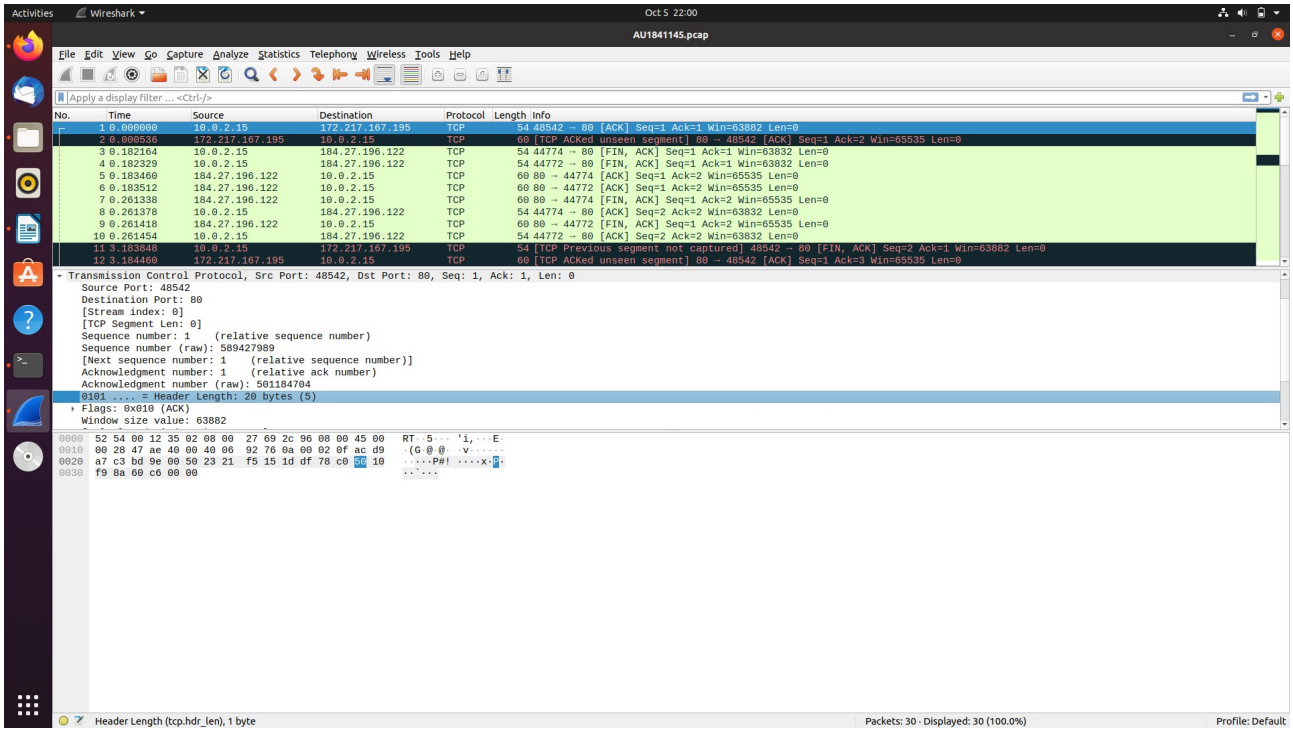


Question 2

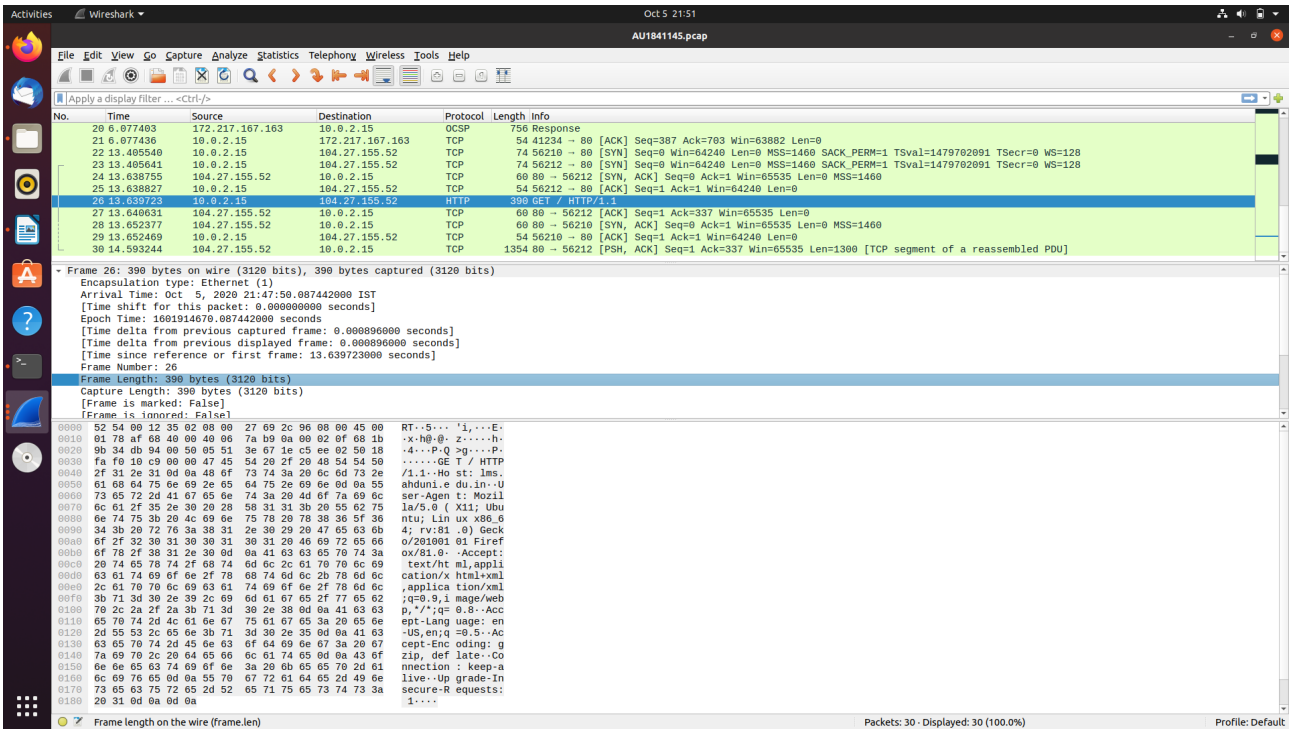
A) The browser and server are running on HTTP/1.1.



B) The content of TCP stream:



C) The size of the content is 390 Bytes in terms of bytes.



Question 3

UserID : samarth.s@ahduni.edu.in
Password : samarth

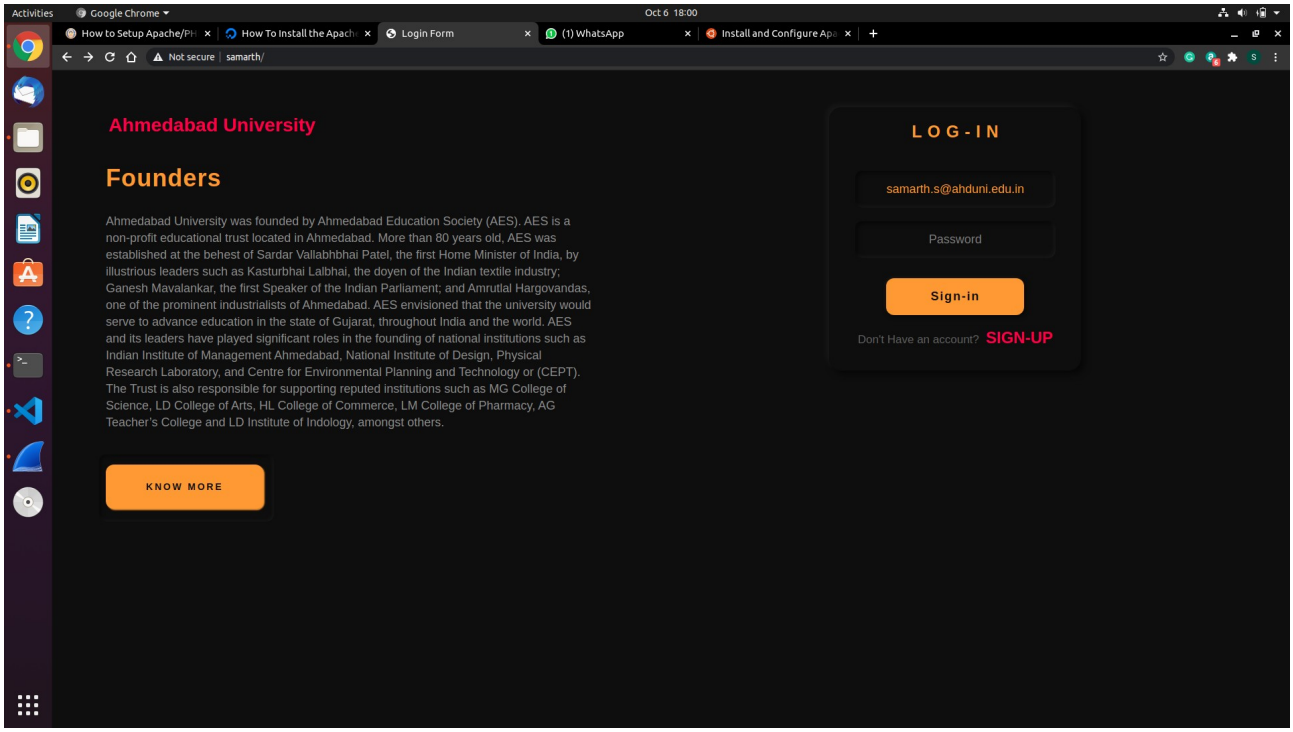
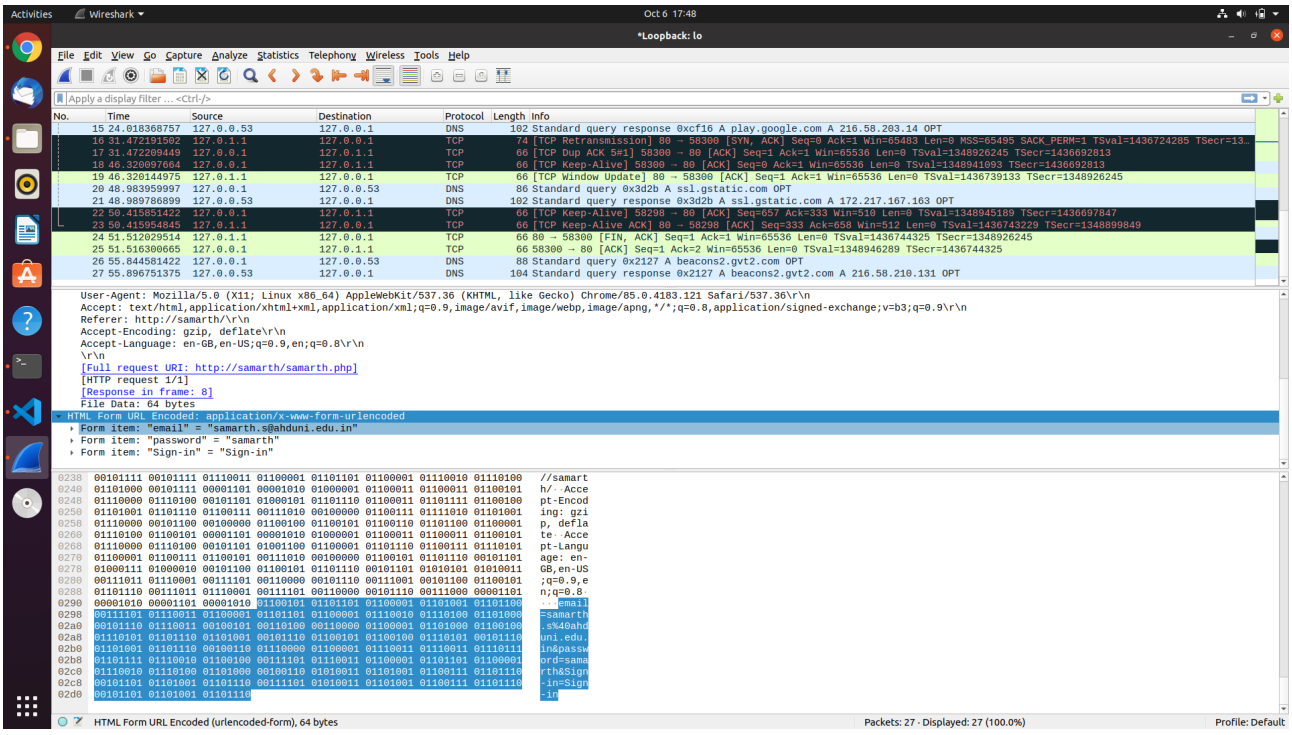


Fig: Login HTML Page



In this question, First I have created a HTML File and a PHP file. Then, with the help of Apache server, I created a virtual host named https://samarth and then deployed my html and php file on that virtual host. In the wireshark,HTTP file that was captured from the form and the input values that were fed in the form are displayed in the HTTP stream window. Here, the mode to capture HTTP file was loopback. Here, the first packets were TCP for the handshake and after the submit button was cliked and the HTTP packet that contained the text values was sent over the server which got caputured by Wireshark and it can be used to get their data i.e. Username and password.

Question 4

A) Source ethernet address: 00 1e a6 83 2d a8
B) Destination Ethernet address: ac 2b 6e de fd b4
C) Source IP Address: 74.125.68.27
D) Destination IP Address: 192.168.1.144
E) Source TCP Port: 25
F) Destination TCP Port: 54656
G) SMTP is a connection-oriented, text-based protocol in which a mail sender communicates with a mail receiver by issuing command strings and supplying necessary data over a reliable ordered data stream channel, typically a Transmission Control Protocol(TCP) connection. The last part of the frame represents a connection to google.com like this : 220

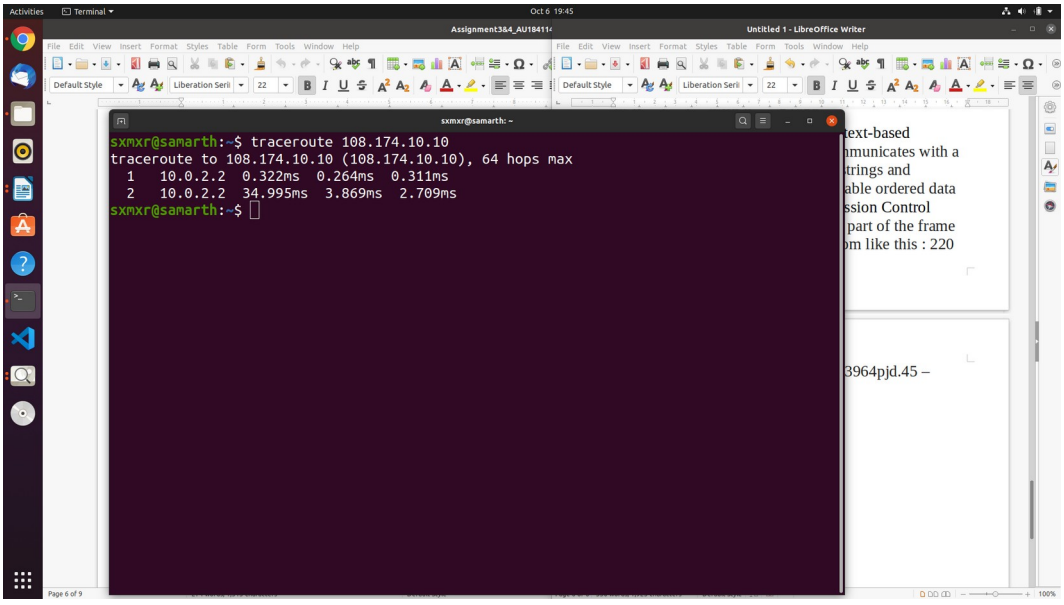
smtp.gmail.com ESMTP k14sm2303964pjd.45 – gsmtp.

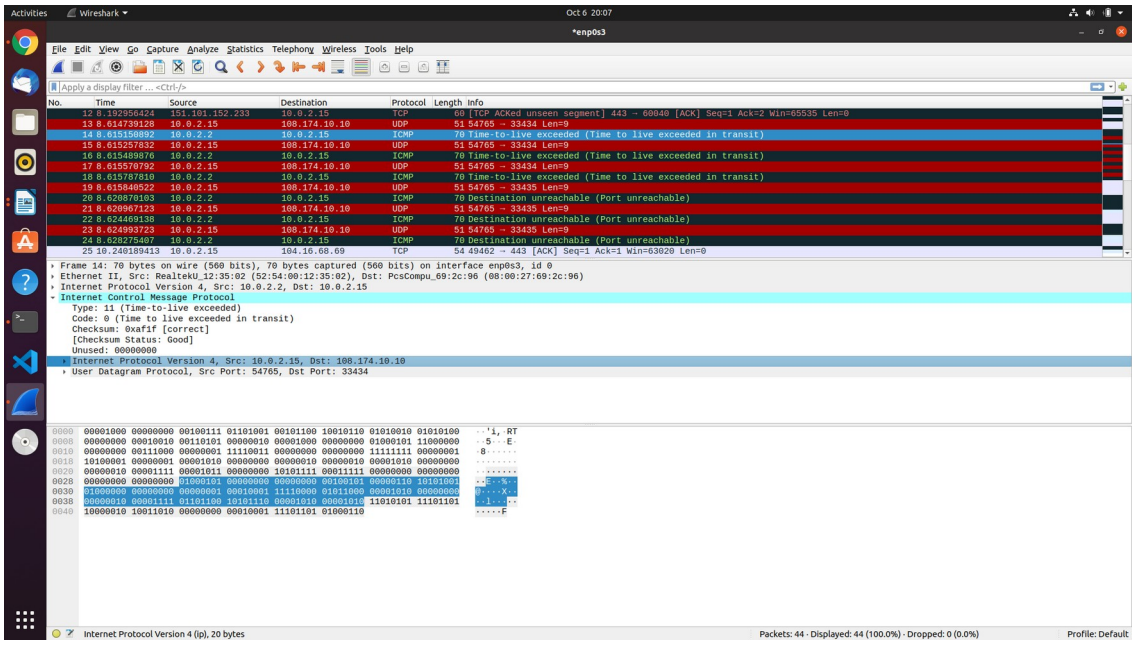
Question 5

Sub-Question: A

IP version: **Ipv4**

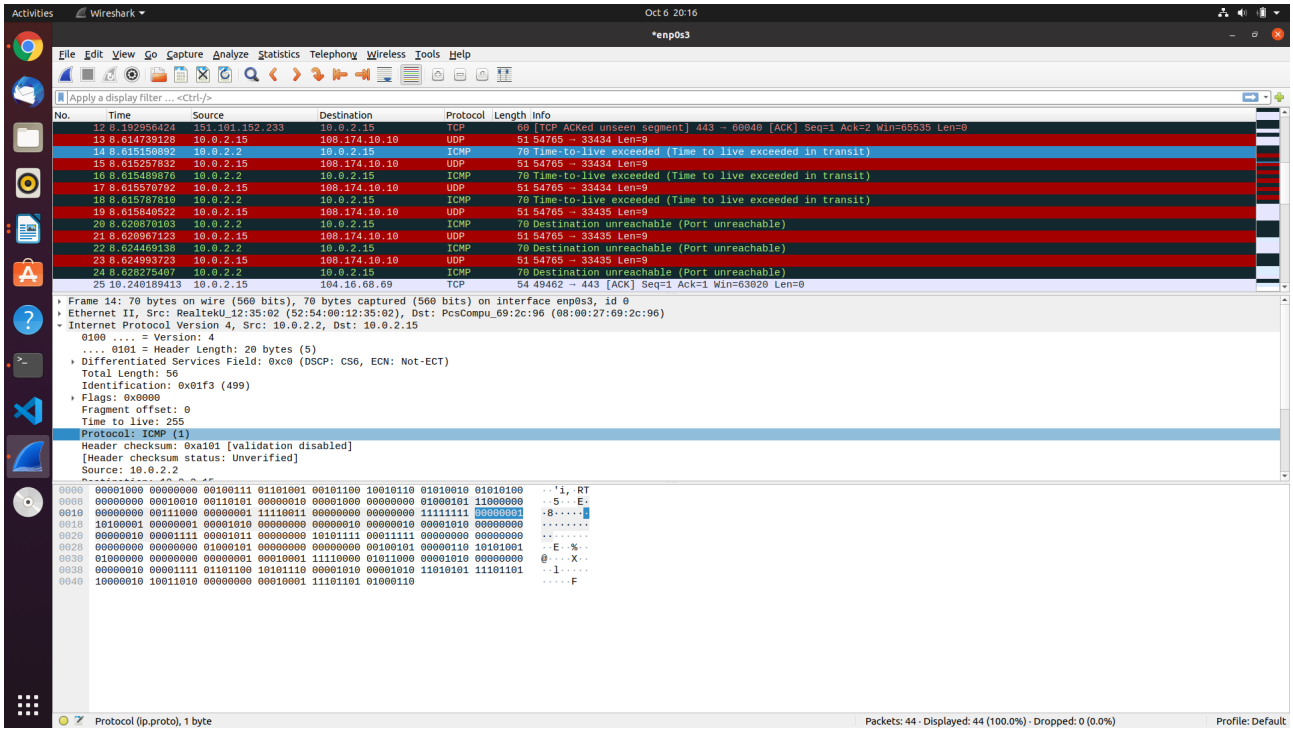
IP address of our host: **10.0.2.15**





Sub-Question: B

The value of the upper layer protocol within the IP header: ICMP(1)

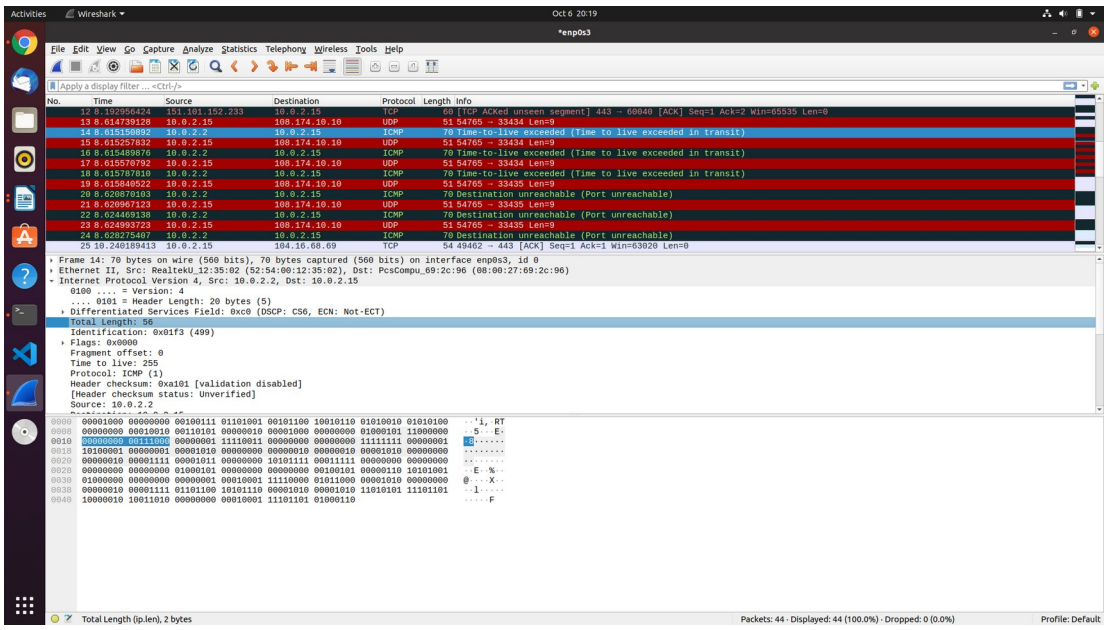


Sub-Question: C

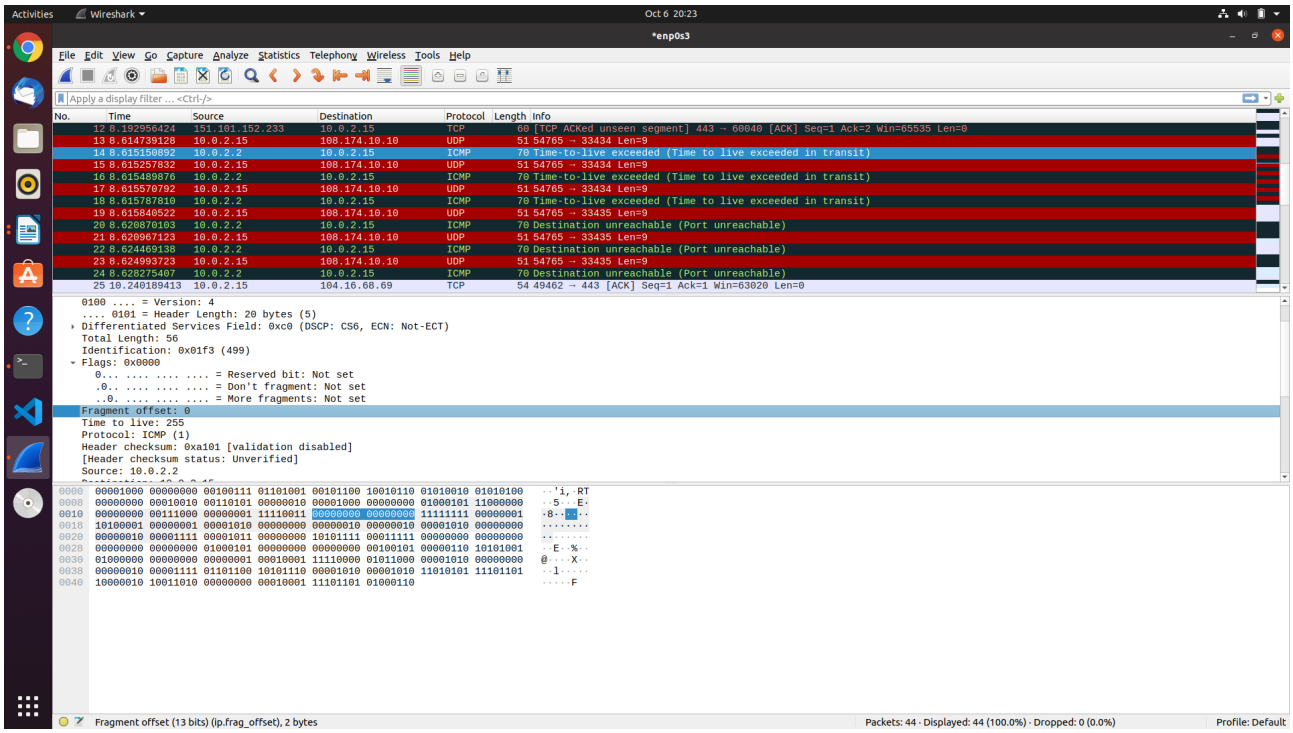
Size of IP header : 20 Bytes (It is there in the screenshot)

Total IP length : 56 Bytes (It is there in the screenshot)

Payload Size of IP Datagram : 56-20 = 36 Bytes



Sub-Question: D



The IP datagram is not fragmented as it is clearly showing more fragments = 0 in the flags of fragmentation in UDP and I can determine by Flags drop down and if more fragments are there then it will show in offset also. Therefore, this IP datagram hasn't been fragmented.