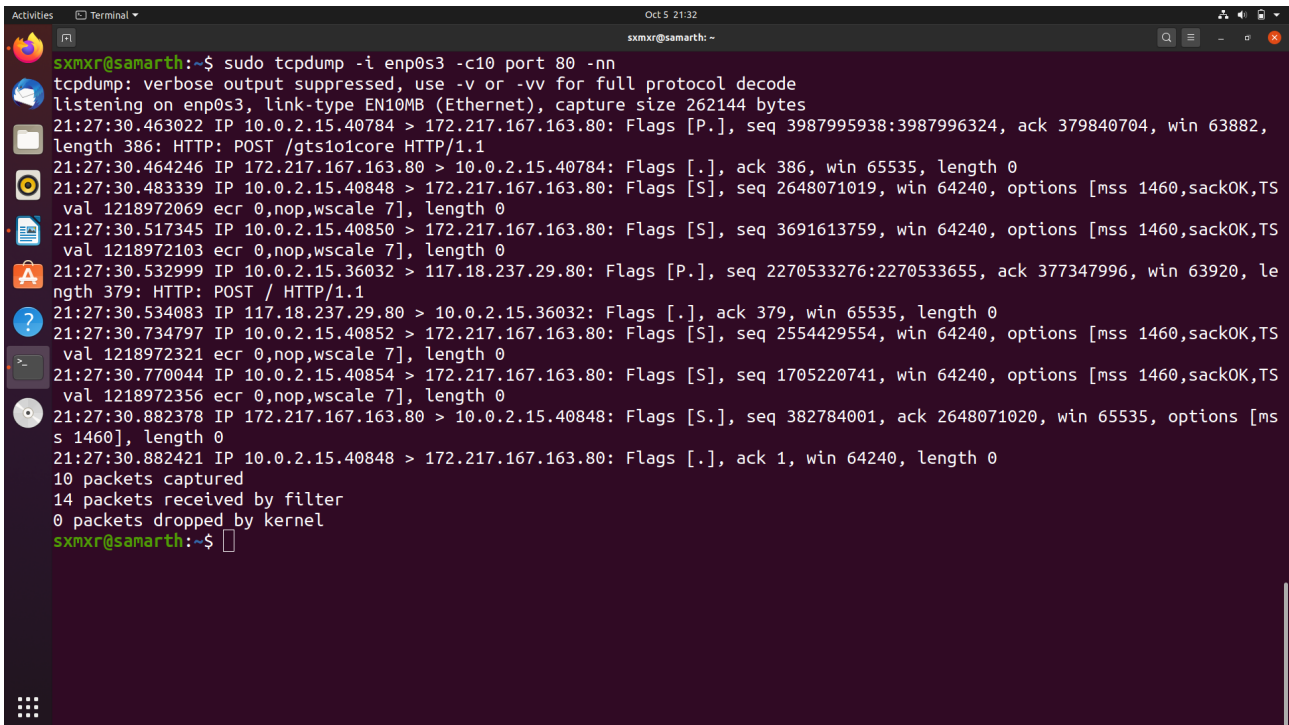


CN Assignment 3 & 4

Question 1

A)



```
Oct 5 21:32
sxmxr@samarth: ~
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 /gtsio1core 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:~$
```

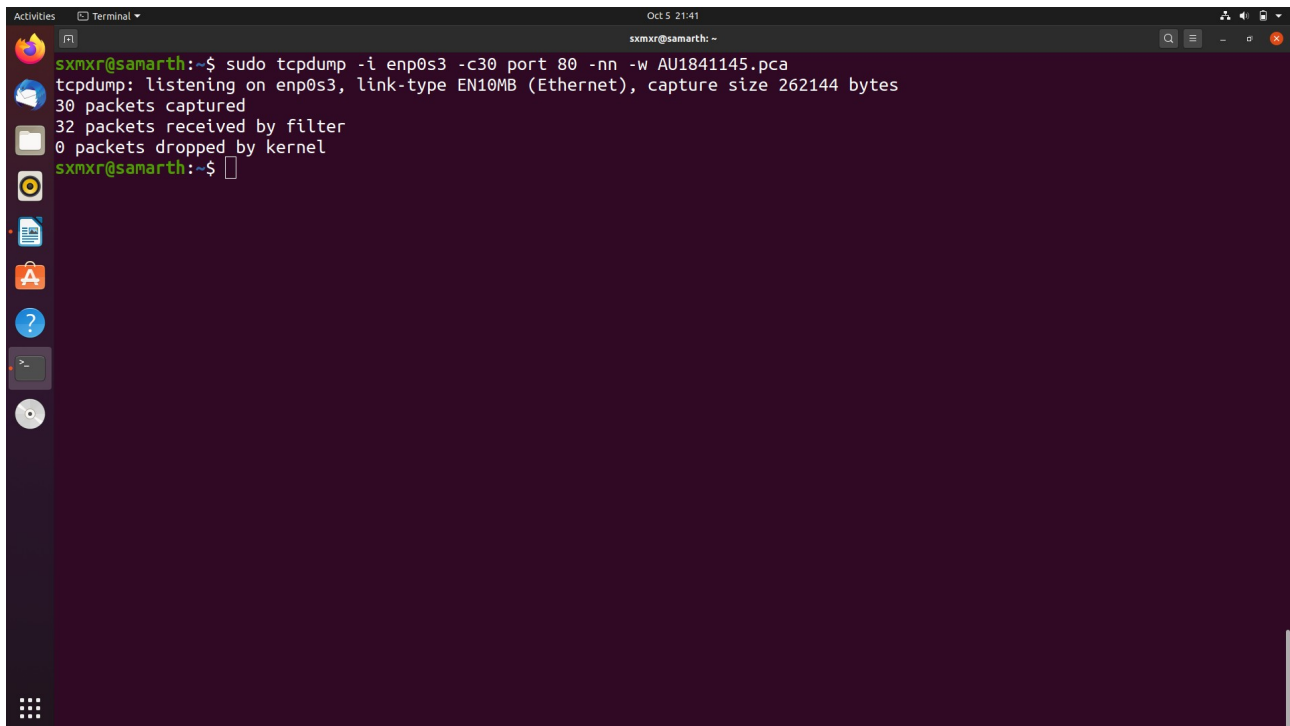
B) Source IP : 10.0.2.15
Source Packet : 40784

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 received.

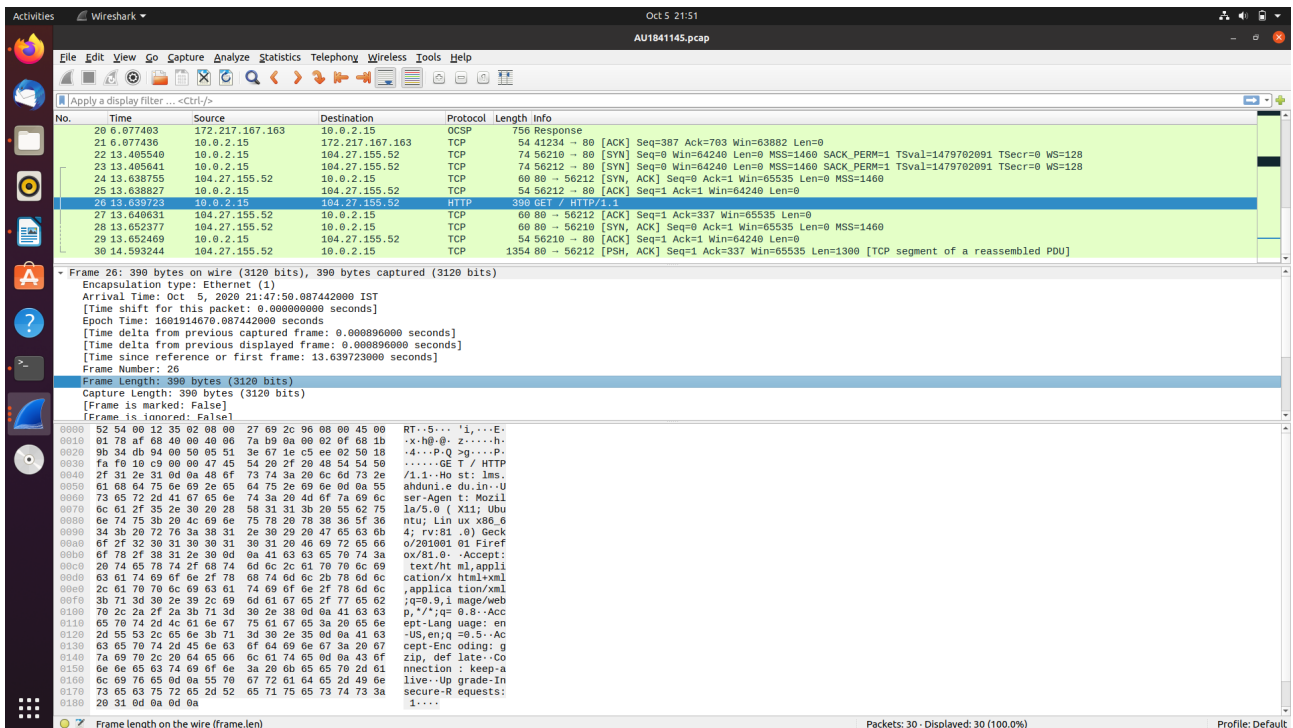
D) 10.0.2.15 is the Internet address of my computer.
172.217.167.163 is the Internet address of the URL I visited.

E)



Question 2

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



B) The content of TCP stream:

The screenshot shows a Wireshark capture of a TCP stream. The packet list on the left shows a sequence of packets, with packet 10 selected. The packet details pane on the right shows the structure of the selected packet, which is a TCP segment. The packet is a GET request for the file 'index.html'.

No.	Time	Source	Destination	Protocol	Length	Info
10	0.000000	10.0.2.15	172.217.167.195	TCP	54	48542 → 80 [ACK] Seq=1 Ack=1 Win=63882 Len=0
11	0.000000	172.217.167.195	10.0.2.15	TCP	60	[TCP ACKed unseen segment] 80 → 48542 [ACK] Seq=1 Ack=2 Win=65535 Len=0
12	0.000000	10.0.2.15	172.217.167.195	TCP	54	44774 → 80 [FIN, ACK] Seq=1 Ack=1 Win=63832 Len=0
13	0.000000	172.217.167.195	10.0.2.15	TCP	54	44772 → 80 [FIN, ACK] Seq=1 Ack=1 Win=63832 Len=0
14	0.000000	10.0.2.15	172.217.167.195	TCP	60	80 → 44774 [ACK] Seq=1 Ack=2 Win=65535 Len=0
15	0.000000	172.217.167.195	10.0.2.15	TCP	60	80 → 44774 [ACK] Seq=1 Ack=2 Win=65535 Len=0
16	0.000000	10.0.2.15	172.217.167.195	TCP	60	80 → 44774 [FIN, ACK] Seq=1 Ack=2 Win=65535 Len=0
17	0.000000	172.217.167.195	10.0.2.15	TCP	54	44772 → 80 [ACK] Seq=2 Ack=2 Win=63832 Len=0
18	0.000000	10.0.2.15	172.217.167.195	TCP	60	[TCP ACKed unseen segment] 80 → 48542 [ACK] Seq=1 Ack=3 Win=65535 Len=0

Transmission Control Protocol, Src Port: 48542, Dst Port: 80, Seq: 1, Ack: 1, Len: 0

Source Port: 48542
Destination Port: 80
[Stream index: 0]
[TCP Segment Len: 0]
Sequence number: 1 (relative sequence number)
Sequence number (raw): 589427989
[Next sequence number: 1 (relative sequence number)]
Acknowledgment number: 1 (relative ack number)
Acknowledgment number (raw): 501184704

Flags: 0x010 (ACK)
Window size value: 63882

0000 52 54 00 12 35 02 08 00 27 69 2c 96 08 00 45 00 RT=5... 'i,...E-
0010 00 28 47 ae 40 00 40 06 92 76 0a 00 02 0f ac d9 -(G@0- V-.....h-
0020 a7 c3 bd 9e 00 50 23 21 f5 15 1d df 78 c0 10P#!X-
0030 f9 8a 60 c6 00 00

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

The screenshot shows a Wireshark capture of a TCP stream. The packet list on the left shows a sequence of packets, with packet 26 selected. The packet details pane on the right shows the structure of the selected packet, which is a GET request for the file 'index.html'. The packet length is 390 bytes.

No.	Time	Source	Destination	Protocol	Length	Info
20	0.000000	172.217.167.103	10.0.2.15	DNS	756	Response
21	0.000000	10.0.2.15	172.217.167.163	TCP	54	41234 → 80 [ACK] Seq=397 Ack=793 Win=63882 Len=0
22	13.405540	10.0.2.15	194.27.155.52	TCP	74	56210 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=1479762091 TSecr=0 WS=128
23	13.405641	10.0.2.15	194.27.155.52	TCP	74	56212 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=1479762091 TSecr=0 WS=128
24	13.638755	194.27.155.52	10.0.2.15	TCP	60	80 → 56212 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460
25	13.638827	10.0.2.15	194.27.155.52	TCP	54	56212 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
26	13.639723	10.0.2.15	194.27.155.52	HTTP	390	GET / HTTP/1.1
27	13.640631	194.27.155.52	10.0.2.15	TCP	60	80 → 56212 [ACK] Seq=1 Ack=337 Win=65535 Len=0
28	13.652377	194.27.155.52	10.0.2.15	TCP	60	80 → 56210 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460
29	13.652469	10.0.2.15	194.27.155.52	TCP	54	56210 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
30	14.593244	194.27.155.52	10.0.2.15	TCP	1354	80 → 56212 [PSH, ACK] Seq=1 Ack=337 Win=65535 Len=1300 [TCP segment of a reassembled PDU]

Frame 26: 390 bytes on wire (3120 bits), 390 bytes captured (3120 bits)

Encapsulation type: Ethernet (1)
Arrival Time: Oct 5, 2020 21:47:50.087442000 IST
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1601914670.087442000 seconds
[Time delta from previous captured frame: 0.000896000 seconds]
[Time delta from previous displayed frame: 0.000896000 seconds]
[Time since reference or first frame: 13.639723000 seconds]

Frame Number: 26
Frame Length: 390 bytes (3120 bits)
Capture Length: 390 bytes (3120 bits)
[Frame is marked: False]
[Frame is loaded: False]

0000 52 54 00 12 35 02 08 00 27 69 2c 96 08 00 45 00 RT=5... 'i,...E-
0010 01 78 af 68 40 00 40 06 7a b9 0a 00 02 0f 08 1b -x.h0-0 z-....h-
0020 9b 34 bd 94 00 50 05 51 3e 67 1e c5 ee 02 50 18 -4...P.Q g-...P-
0030 fa f9 10 c9 00 00 47 45 54 28 2f 20 48 54 54 50-GE T / HTTP
0040 2f 31 2e 31 0d 0a 48 6f 73 74 3a 20 6c d3 73 2e /1.1..Ho st: lms
0050 61 68 64 75 6e 09 2e 65 64 75 2e 69 6e 0d 0a 55 ahduni.e du.in-U
0060 73 65 72 2d 41 67 65 6e 74 3a 20 4d 0f 7a 69 6c ser-Agen t: Mozill
0070 6c 61 2f 35 2e 30 20 28 5b 31 31 3b 20 55 62 75 le/5.0 (X11; Ubuntu
0080 6e 74 75 3b 20 4c 69 6e 75 78 20 78 38 36 5f 36 ntui; Lin ux x86_6
0090 34 3b 20 72 76 3a 38 31 2e 30 29 20 47 65 63 6b 4; rv:81.0) Gecko
0100 6f 2f 32 30 31 30 30 31 30 31 20 46 69 72 65 66 o/201001 01 Firef
0110 6f 78 2f 38 31 2e 30 0d 0a 41 63 63 65 70 74 3a ox/81.0 -Accept:
0120 20 74 65 78 74 2f 68 74 6d 6c 2c 61 70 70 6c 69 text/ht ml,appli
0130 63 61 74 69 6f 6e 2f 78 68 74 6d 6c 2b 78 6d 6c cation/x html+xml
0140 2c 61 78 70 6c 69 63 61 74 69 6f 6e 2f 78 6d 6c ,applicat ion/xml
0150 3b 71 30 30 2e 39 2c 69 6d 61 67 65 2f 77 65 62 ;q=0.9,i mage/web
0160 70 2c 2a 2f 2a 3b 71 3d 30 2e 38 0d 0a 41 63 63 p,/*;q=0.8-Acc
0170 65 70 74 2d 41 61 6e 67 75 61 67 65 3a 20 65 6e pt-Lang uage: en
0180 2d 53 2c 65 6e 3b 71 3d 30 2e 35 0d 0a 41 63 -US,en;q =0.5-Ac
0190 63 65 70 74 2d 45 6e 63 6f 64 69 6e 67 3a 20 67 cept-Enc oding: g
0200 7a 69 70 2c 20 64 65 66 6e 61 74 65 0d 0a 43 6f zip, def late-Co
0210 6e 65 63 74 69 6f 6e 3a 20 6b 65 65 70 2d 61 nnection : keep-a
0220 6c 69 65 6d 0a 55 70 67 72 61 64 65 2d 49 6e live-Up grade-In
0230 73 63 65 75 72 65 2d 52 65 71 75 65 73 74 73 3a secure-R equests:
0240 20 31 0d 0a 0d 0a

Question 3

UserID : samarth.s@ahduni.edu.in

Password : samarth

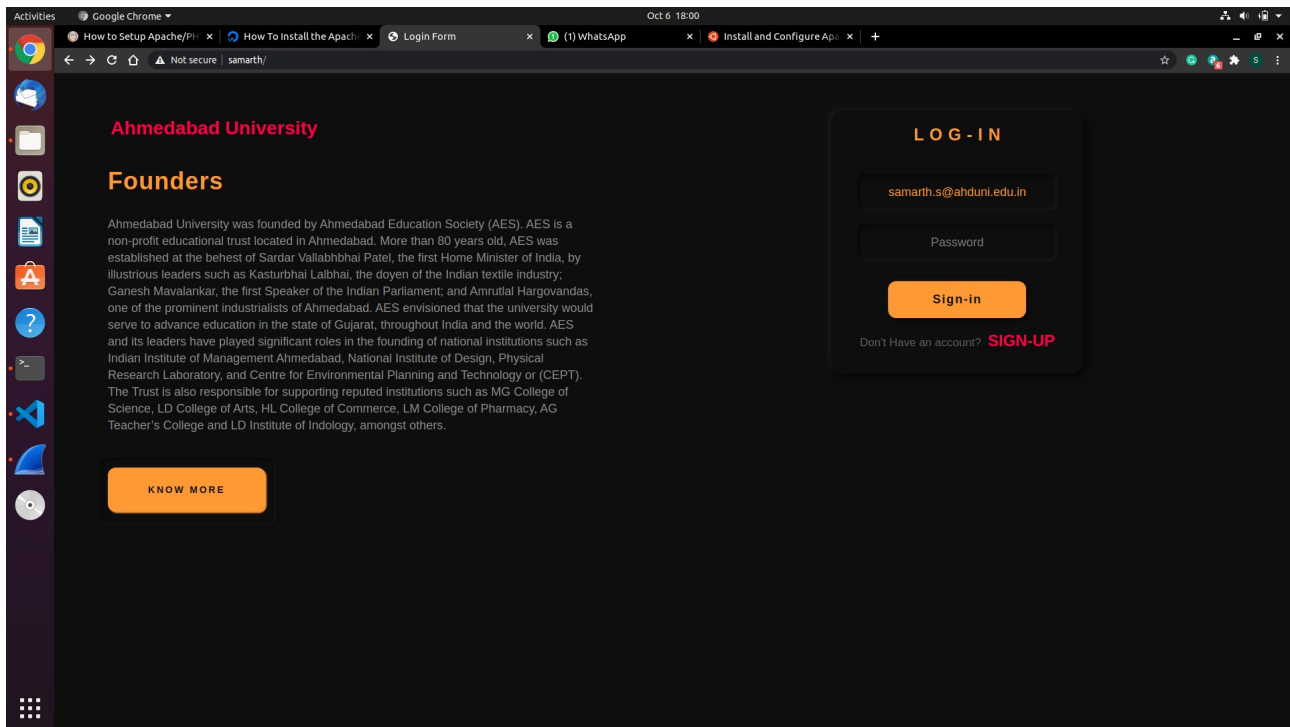
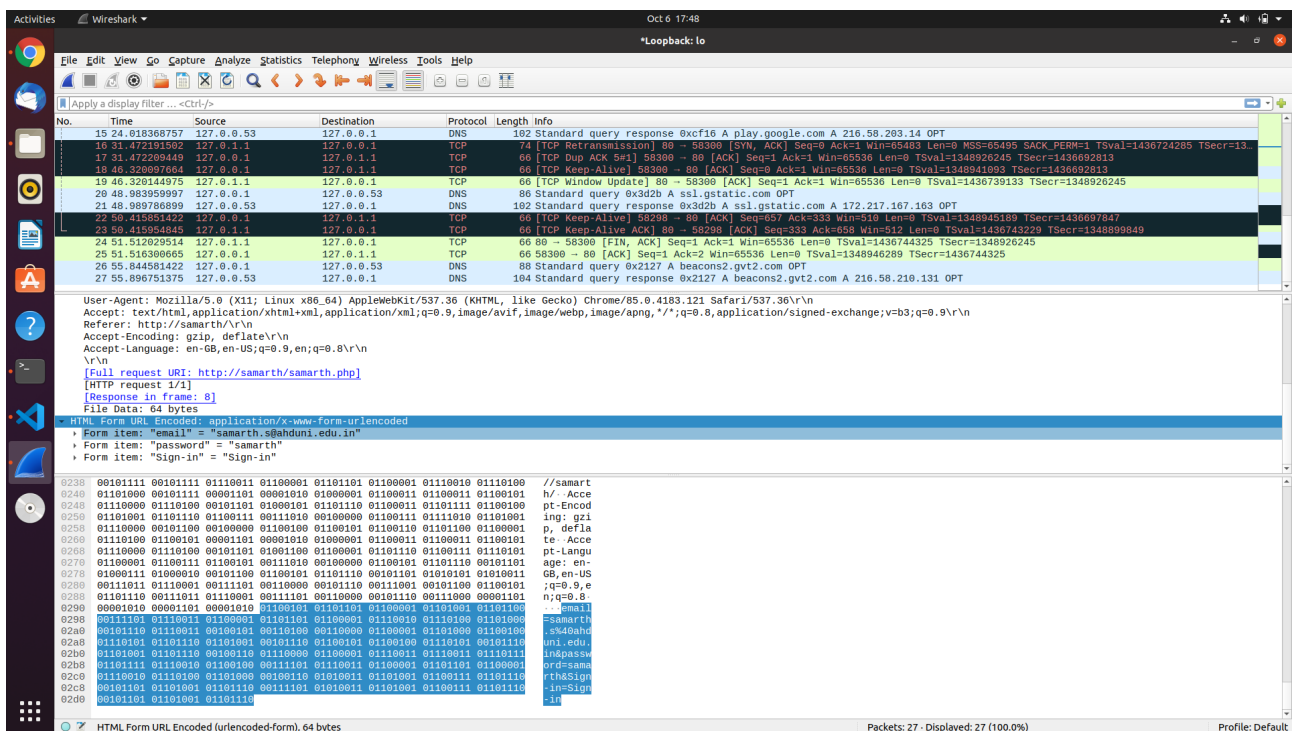


Fig: Login HTML Page



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 clicked and the HTTP packet that contained the text values was sent over the server which got captured 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

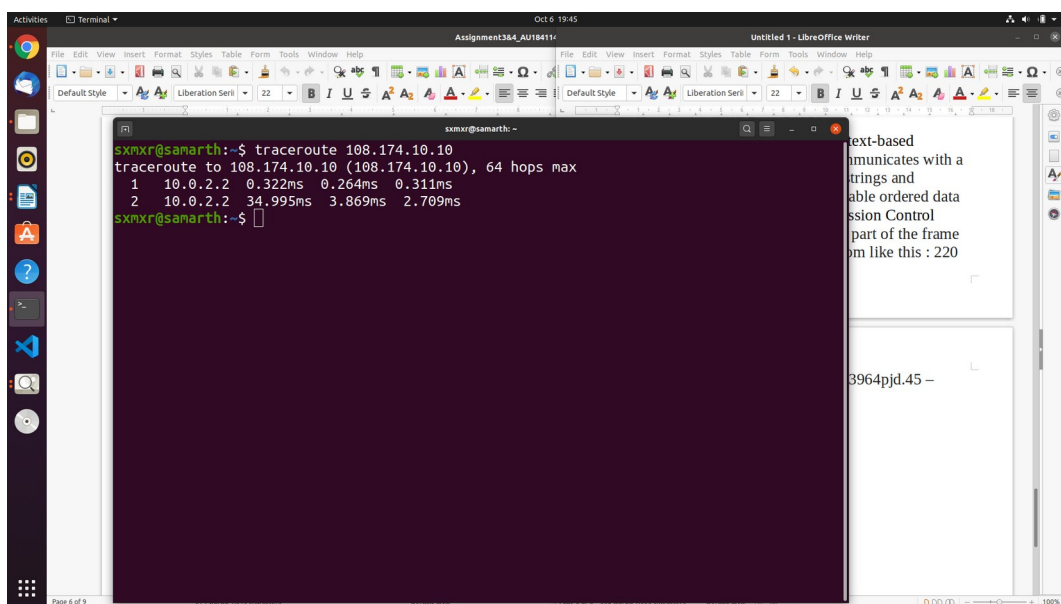
smtp.gmail.com ESMTP k14sm2303964pjd.45 –
gsmtp.

Question 5

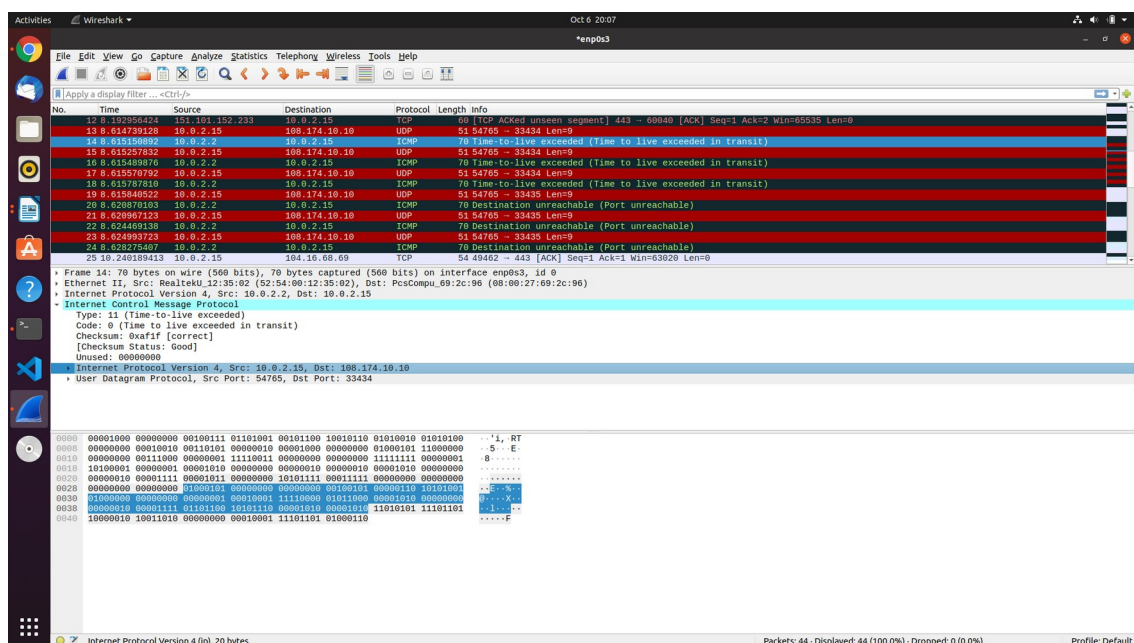
Sub-Question: A

IP version: **Ipv4**

IP address of our host: **10.0.2.15**



```
sxmrx@samarth:~$ traceroute 108.174.10.10
traceroute to 108.174.10.10 (108.174.10.10), 64 hops max
 1  10.0.2.2  0.322ms  0.264ms  0.311ms
 2  10.0.2.2  34.995ms  3.869ms  2.709ms
sxmrx@samarth:~$
```

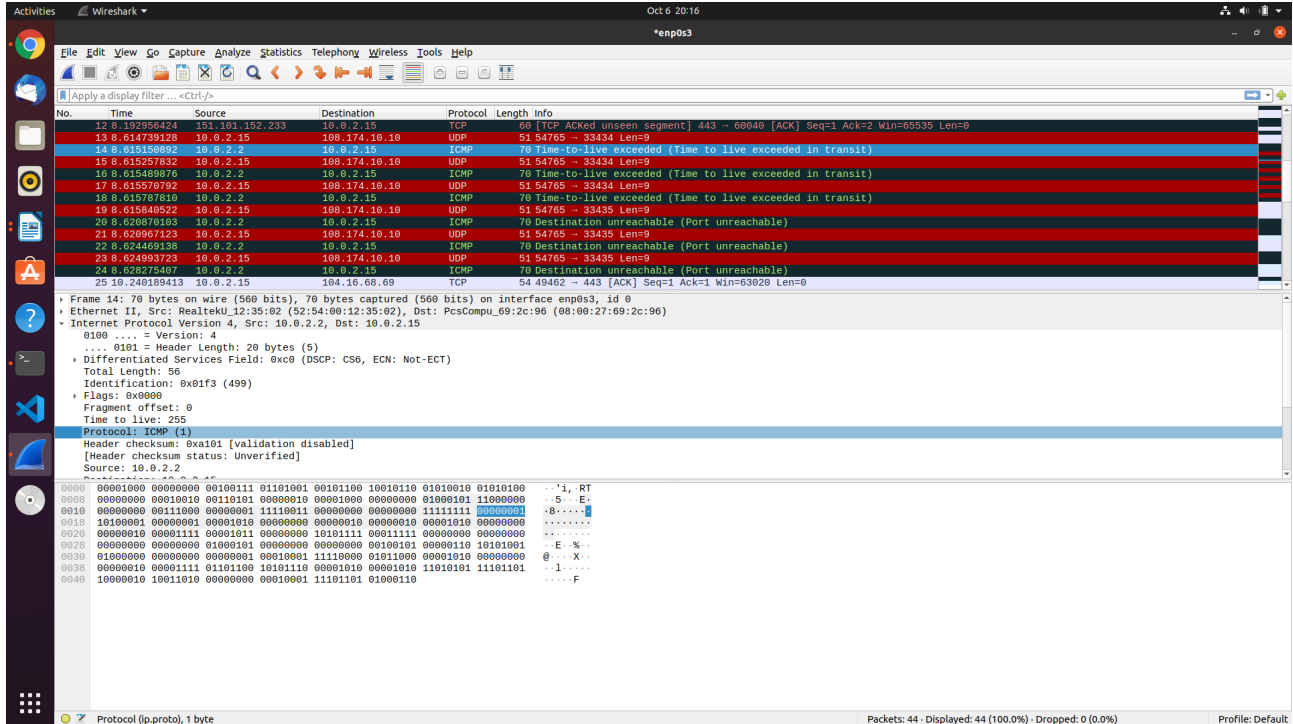


No.	Time	Source	Destination	Protocol	Length	Info
12	0.000000	10.0.2.15	10.0.2.15	ICMP	60	[TCP ACKed unseen segment] 443 -> 8080 [ACK] Seq=1 Ack=2 Win=65535 Len=0
13	0.000000	10.0.2.15	108.174.10.10	UDP	51	54765 -> 33434 Len=9
14	0.000000	10.0.2.15	108.174.10.10	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
15	0.000000	10.0.2.15	108.174.10.10	UDP	51	54765 -> 33434 Len=9
16	0.000000	10.0.2.15	108.174.10.10	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
17	0.000000	10.0.2.15	108.174.10.10	UDP	51	54765 -> 33434 Len=9
18	0.000000	10.0.2.15	108.174.10.10	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
19	0.000000	10.0.2.15	108.174.10.10	UDP	51	54765 -> 33435 Len=9
20	0.000000	10.0.2.15	108.174.10.10	ICMP	70	Destination unreachable (Port unreachable)
21	0.000000	10.0.2.15	108.174.10.10	UDP	51	54765 -> 33435 Len=9
22	0.000000	10.0.2.15	108.174.10.10	ICMP	70	Destination unreachable (Port unreachable)
23	0.000000	10.0.2.15	108.174.10.10	UDP	51	54765 -> 33435 Len=9
24	0.000000	10.0.2.15	108.174.10.10	ICMP	70	Destination unreachable (Port unreachable)
25	0.000000	10.0.2.15	108.174.10.10	TCP	54	49402 -> 443 [ACK] Seq=1 Ack=1 Win=63020 Len=0

Frame 14: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface enp0s3, id 0
Ethernet II, Src: RealtekU12:35:02 (52:54:00:12:35:02), Dst: PcsCompu, 69:2c:96 (08:00:27:09:2c:96)
Internet Protocol Version 4, Src: 10.0.2.2, Dst: 10.0.2.15
Internet Control Message Protocol
Type: 11 (Time-to-live exceeded)
Code: 0 (Time to live exceeded in transit)
Checksum: 0xaf1f [correct]
[Checksum Status: Good]
Unused: 00000000
Internet Protocol Version 4, Src: 10.0.2.15, Dst: 108.174.10.10
User Datagram Protocol, Src Port: 54765, Dst Port: 33434

Sub-Question: B

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

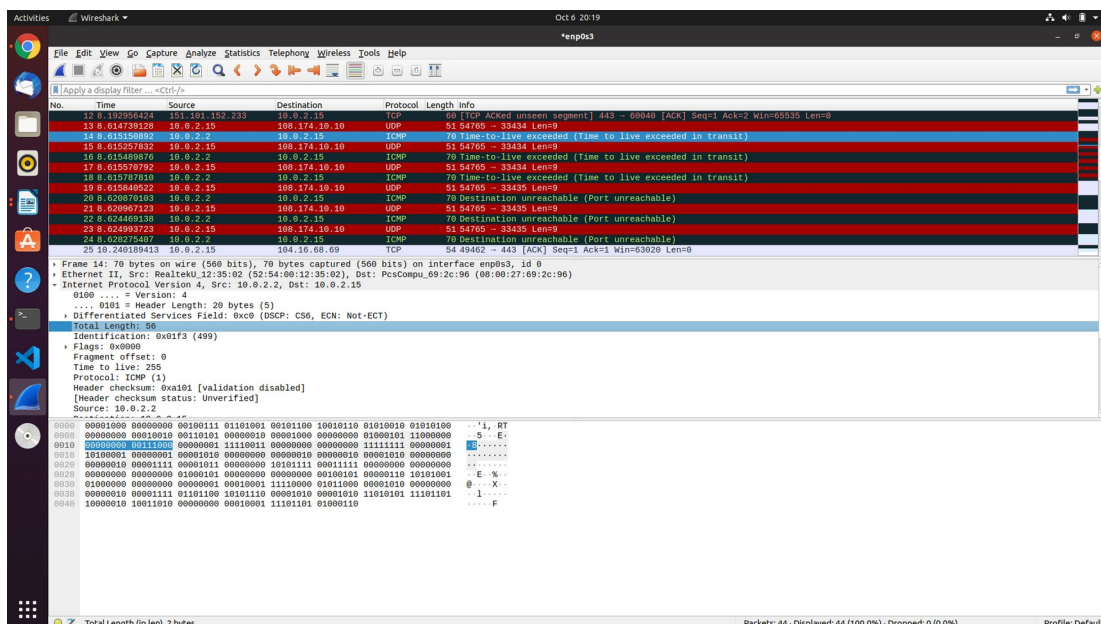


Sub-Question: C

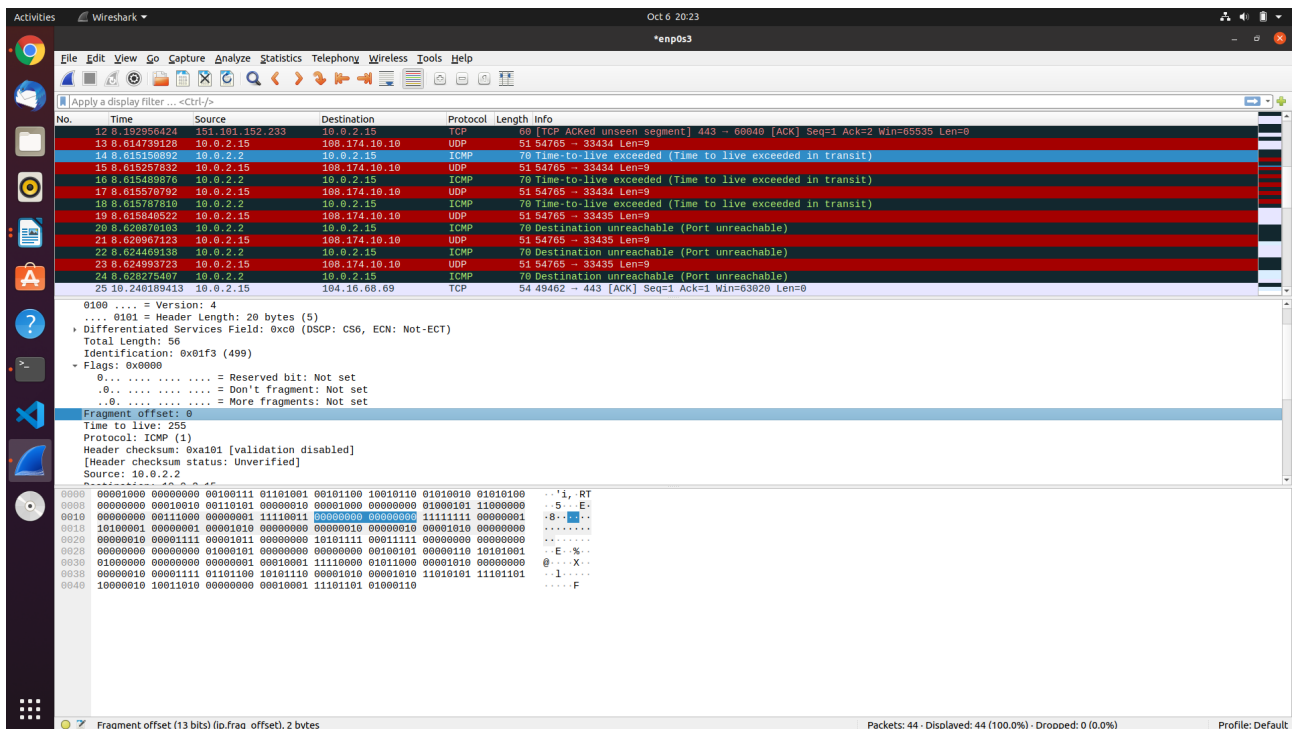
Size of IP header : 20 Bytes (It is there in the screenshot)

Total 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.