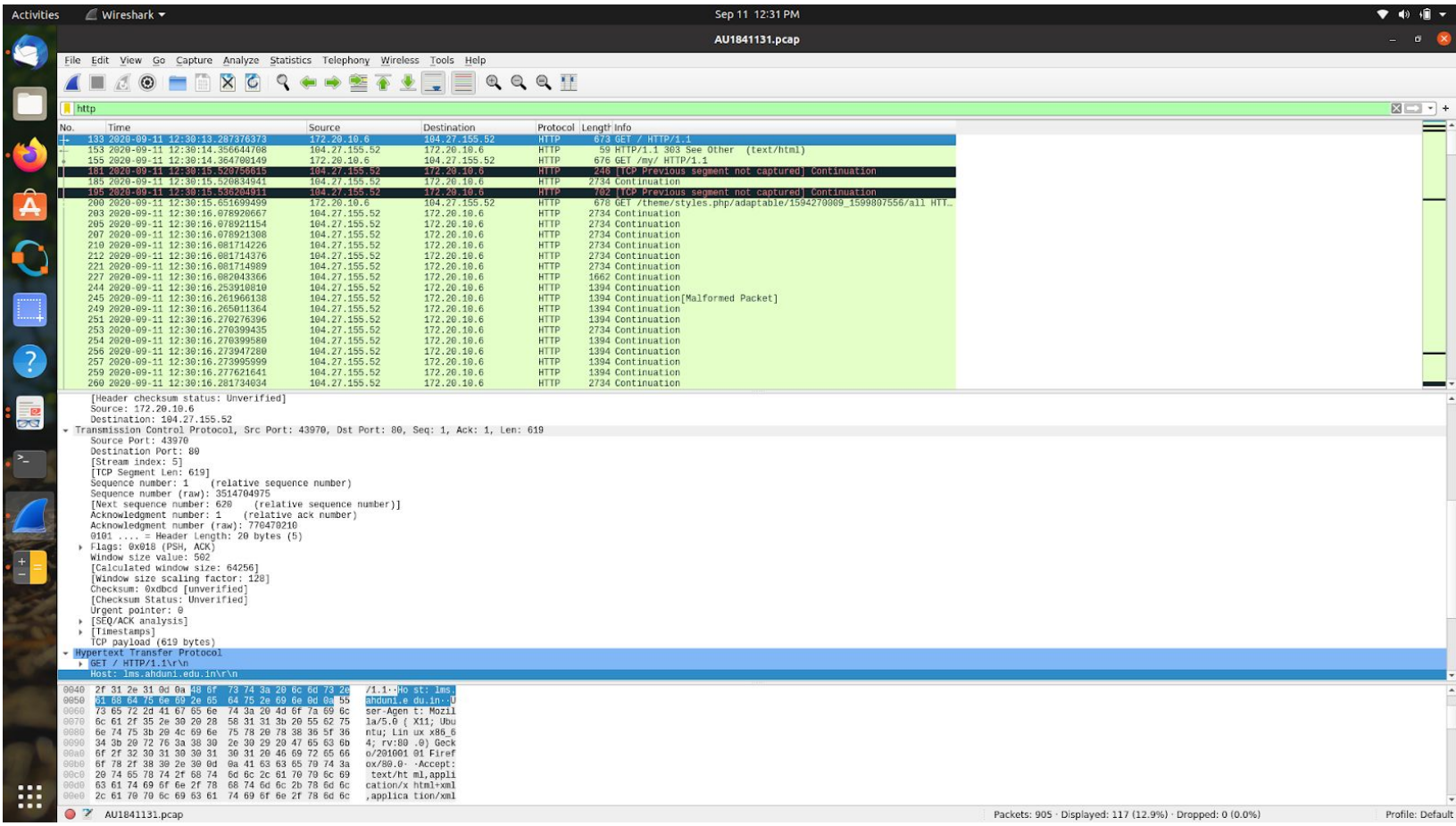
Mansi Dobariya AU1841131

CN Lab assignment 3 & 4

Wireshark Packet analyzer

1.

1.1



1.2

Hostname : lms.ahduni.edu.in

Source ip address : 172.20.10.6

Source port address : 43970

Destination ip address : 104.27.155.52

Destination port address : 80

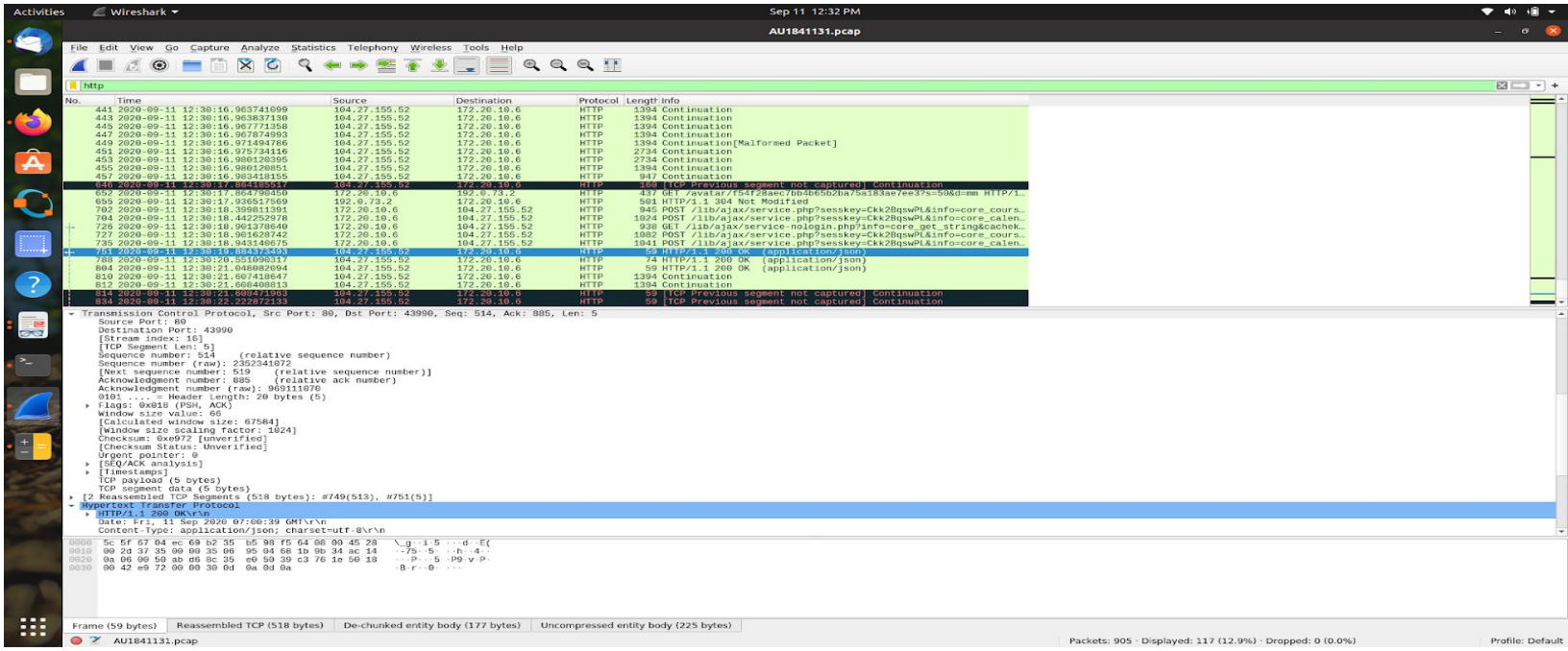
1.3

Time format := HH:MM:SS.fracodSecond

Request time = 12:30:13.28736373

Response time(ok) =12:30:19.884373493

Time taken =6.597009763 seconds



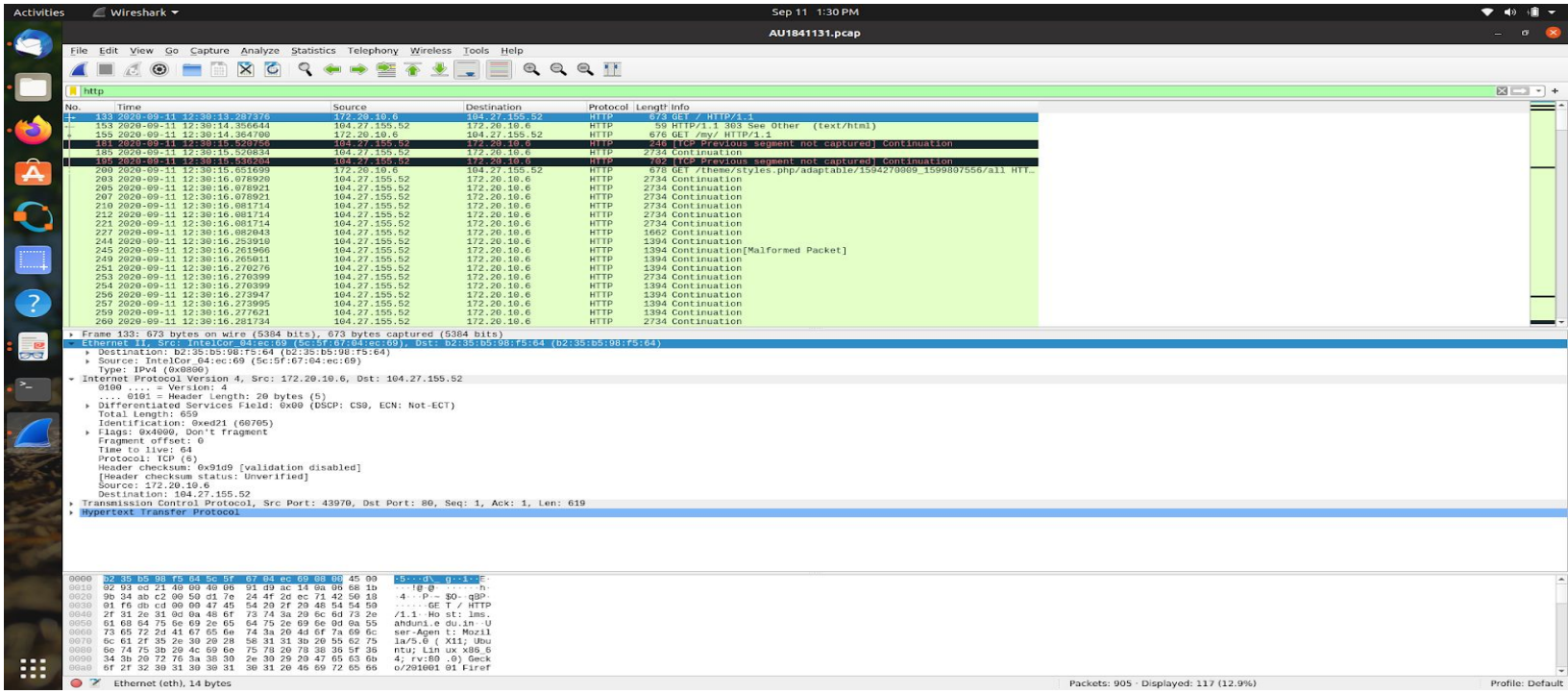
1.4

MAC address

Destination[router]: b2:35:b5:98:f5:64 (b2:35:b5:98:f5:64)

Source:[my device] IntelCor_04:ec:69 (5c:5f:67:04:ec:69)

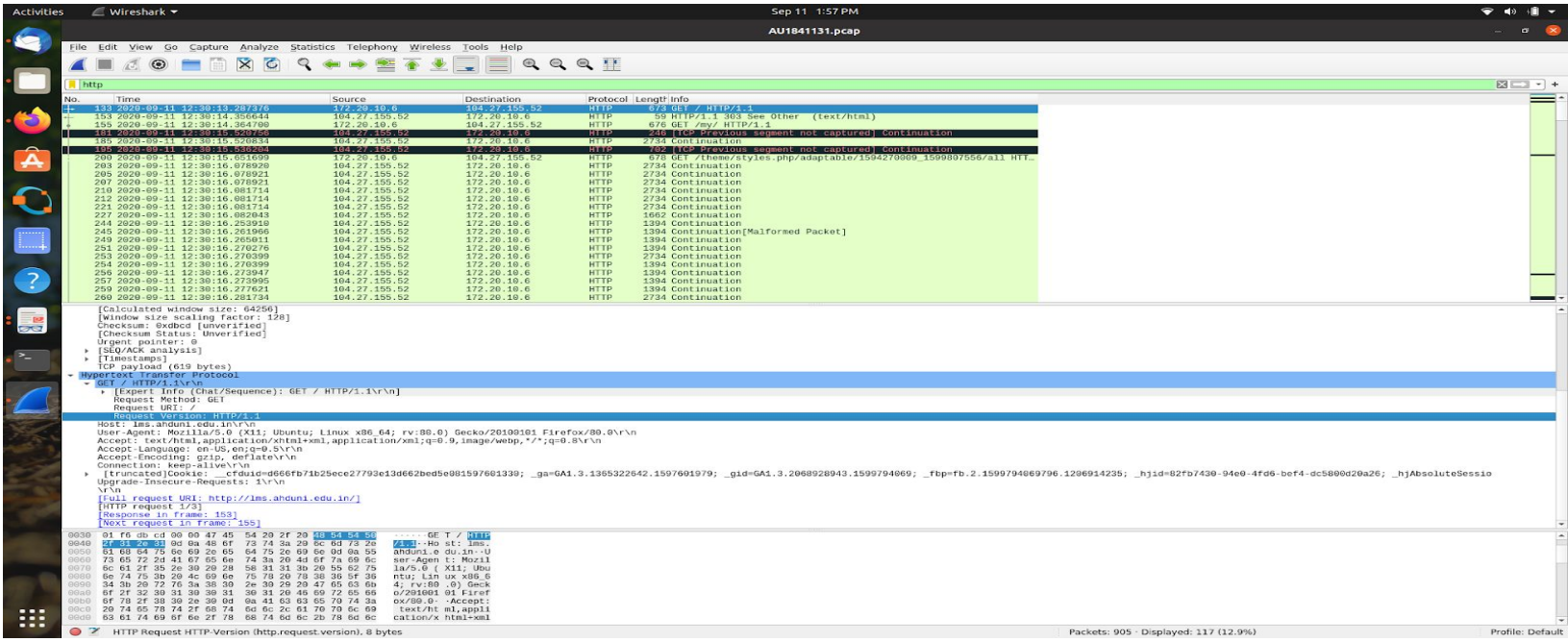
Type: IPv4 (0x0800)



2.

2.1

Http version 1.1

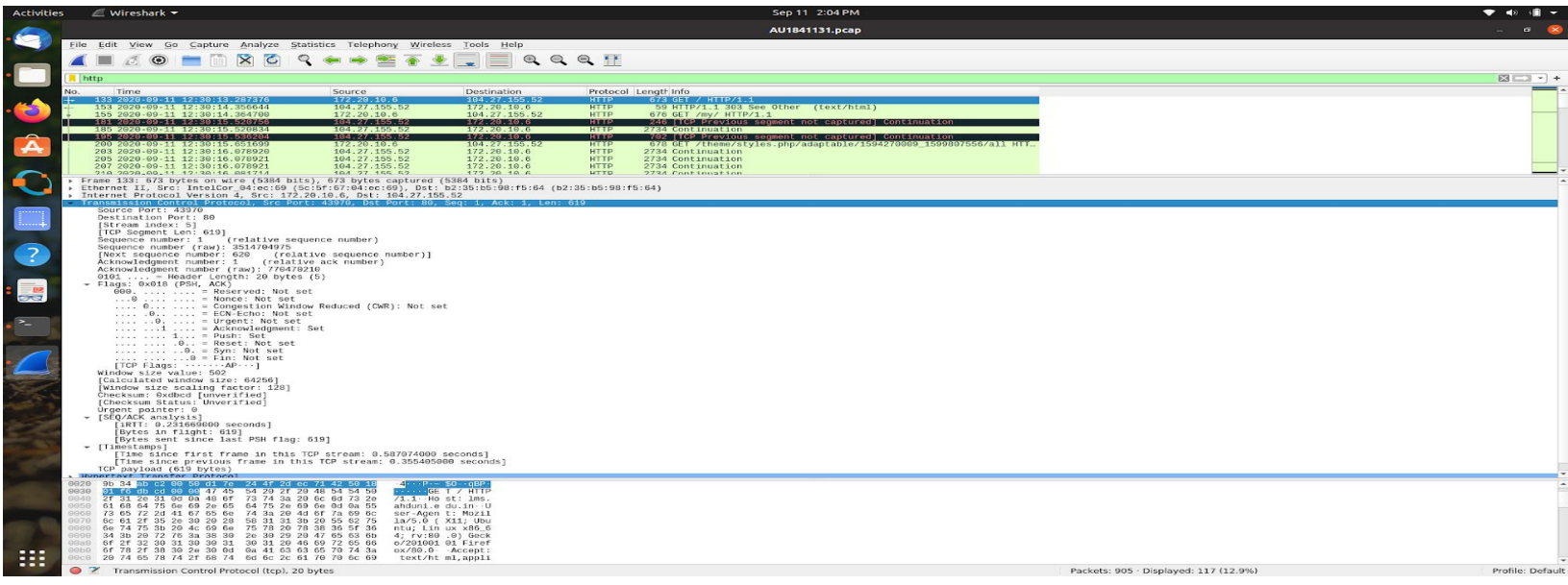


2.2

Transmission Control Protocol stream has port address of source and destination ,segment length as tcp is network layer proto

Header length , Acknowledge Flags,also window size value for sender and receiver ,TCP payload size in bytes

We’re transmitting our info source port to the destination port . This src port number is auto generated by our machine



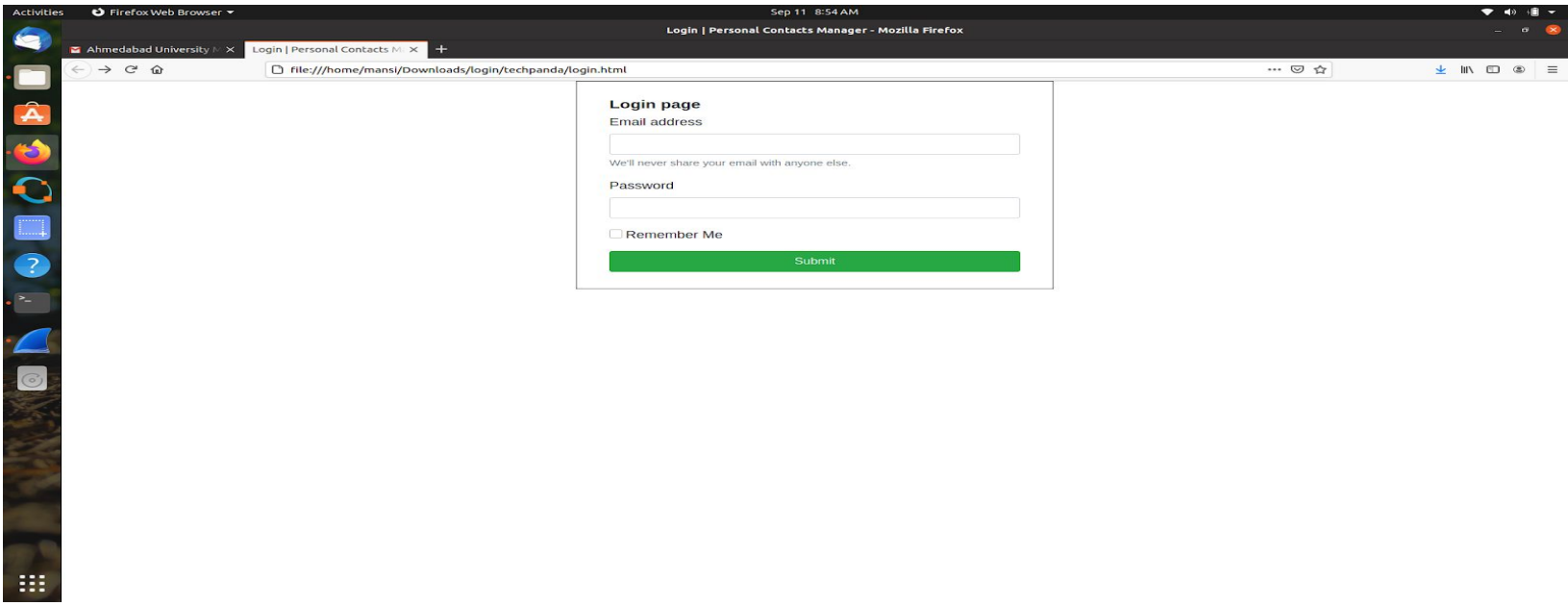
2.3

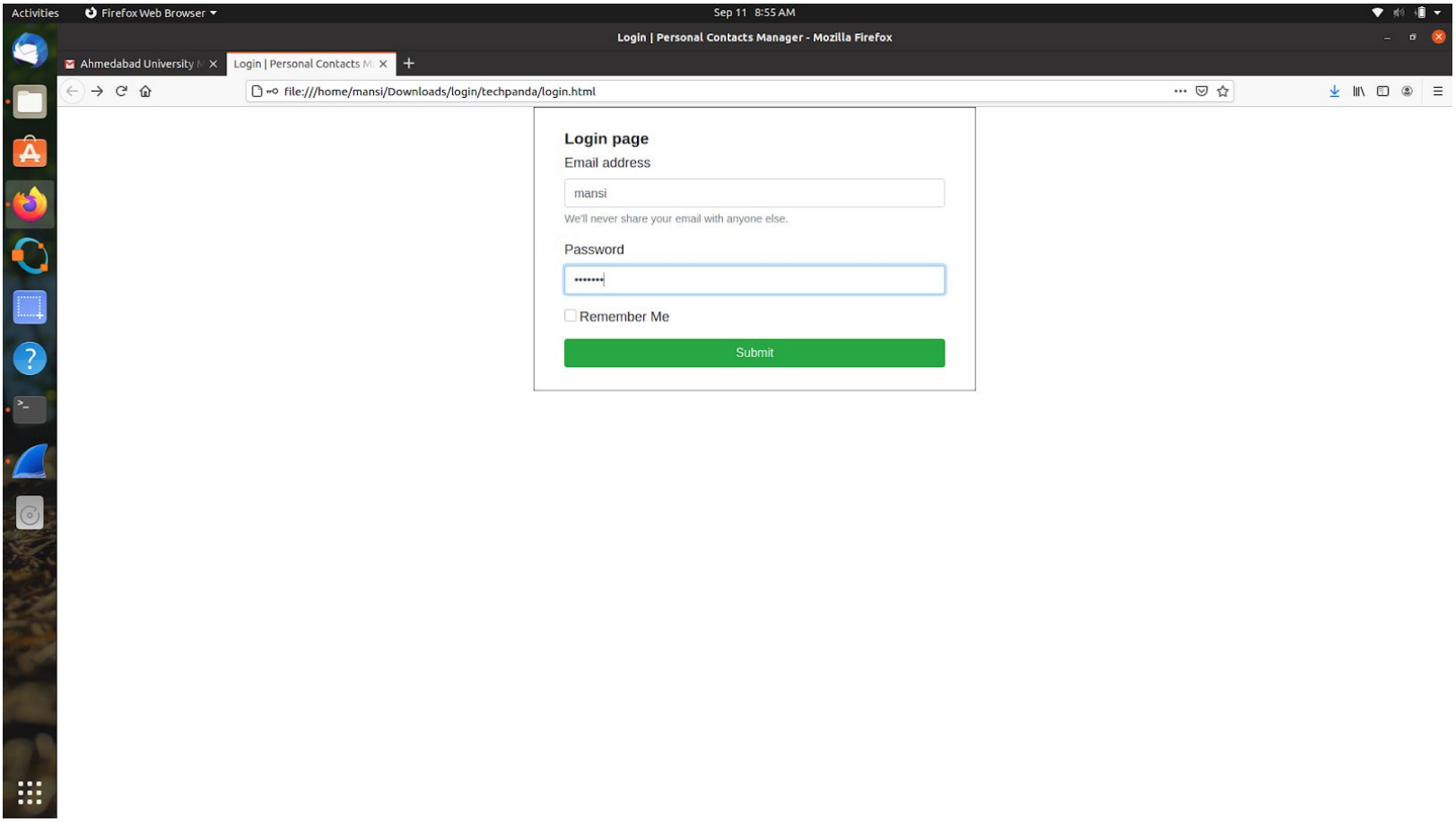
Size of Content[payload,data] = 619 bytes

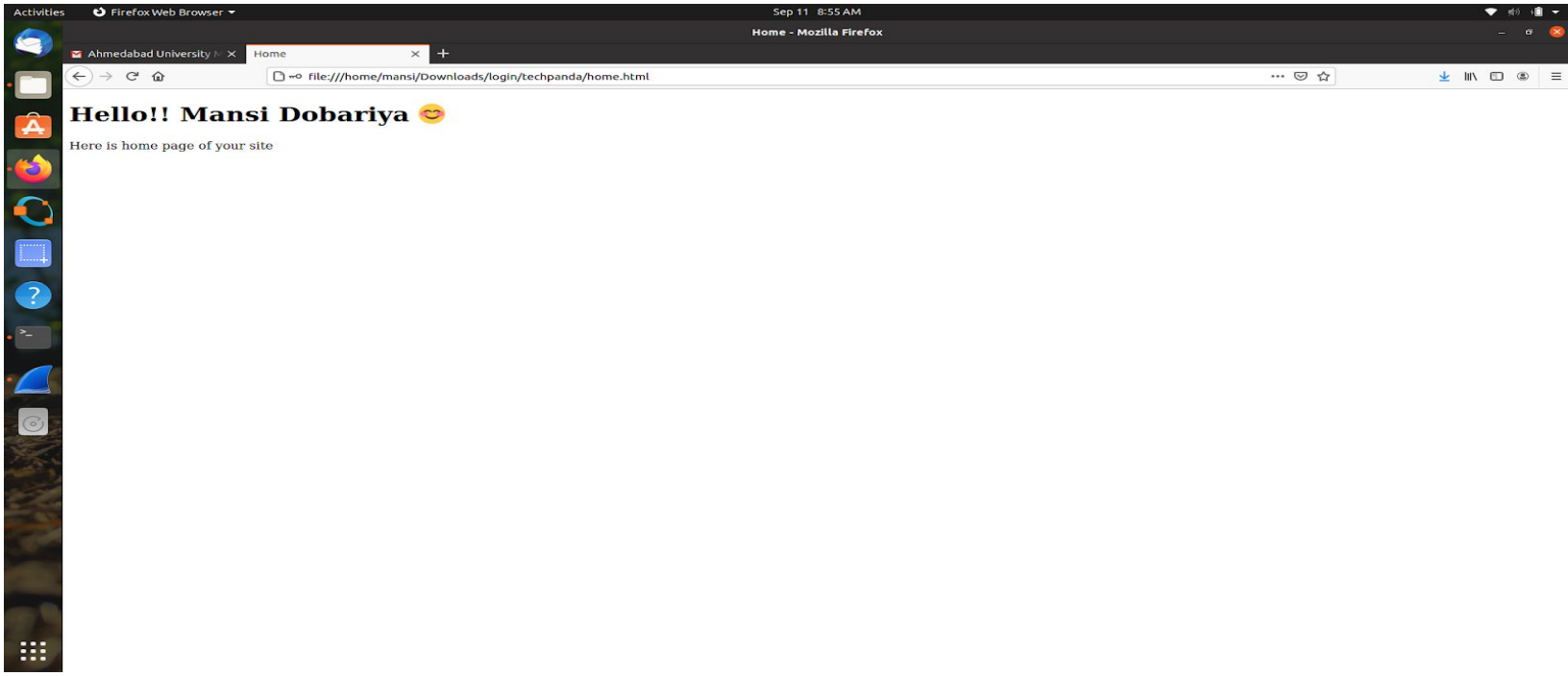
Header length = 20 bytes ,which contains where we have to send our info [details of destination]

3.

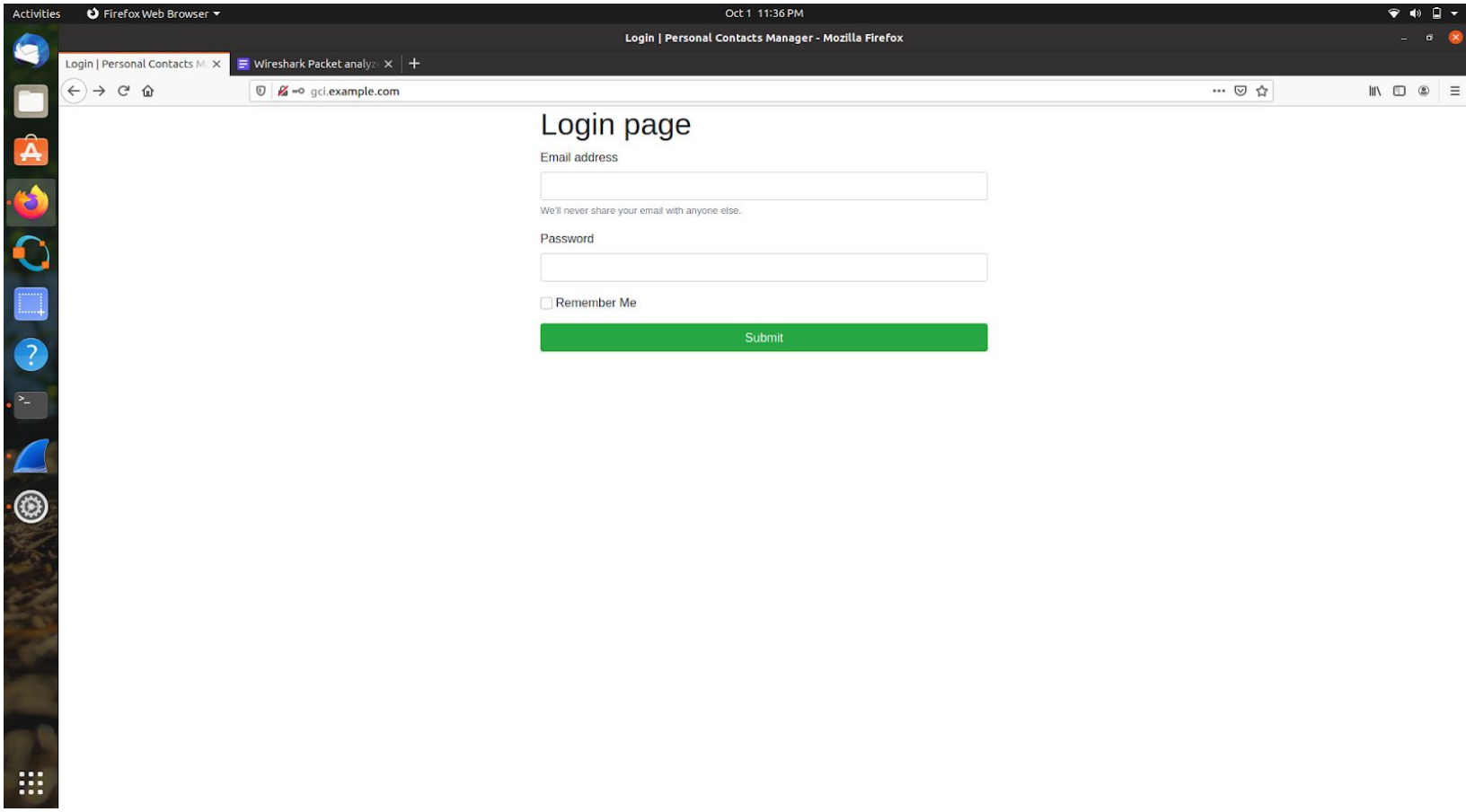
HTML pages:login and home

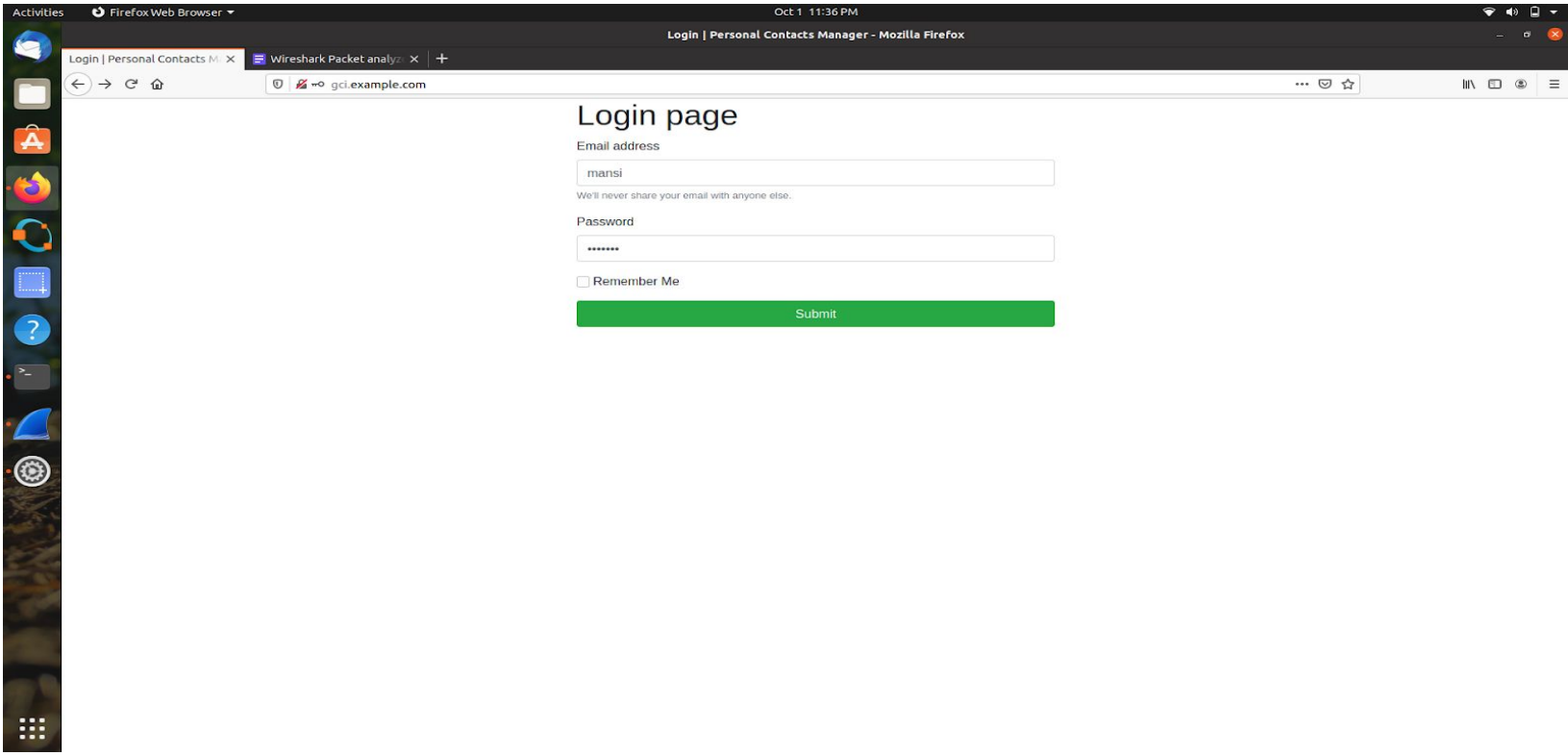


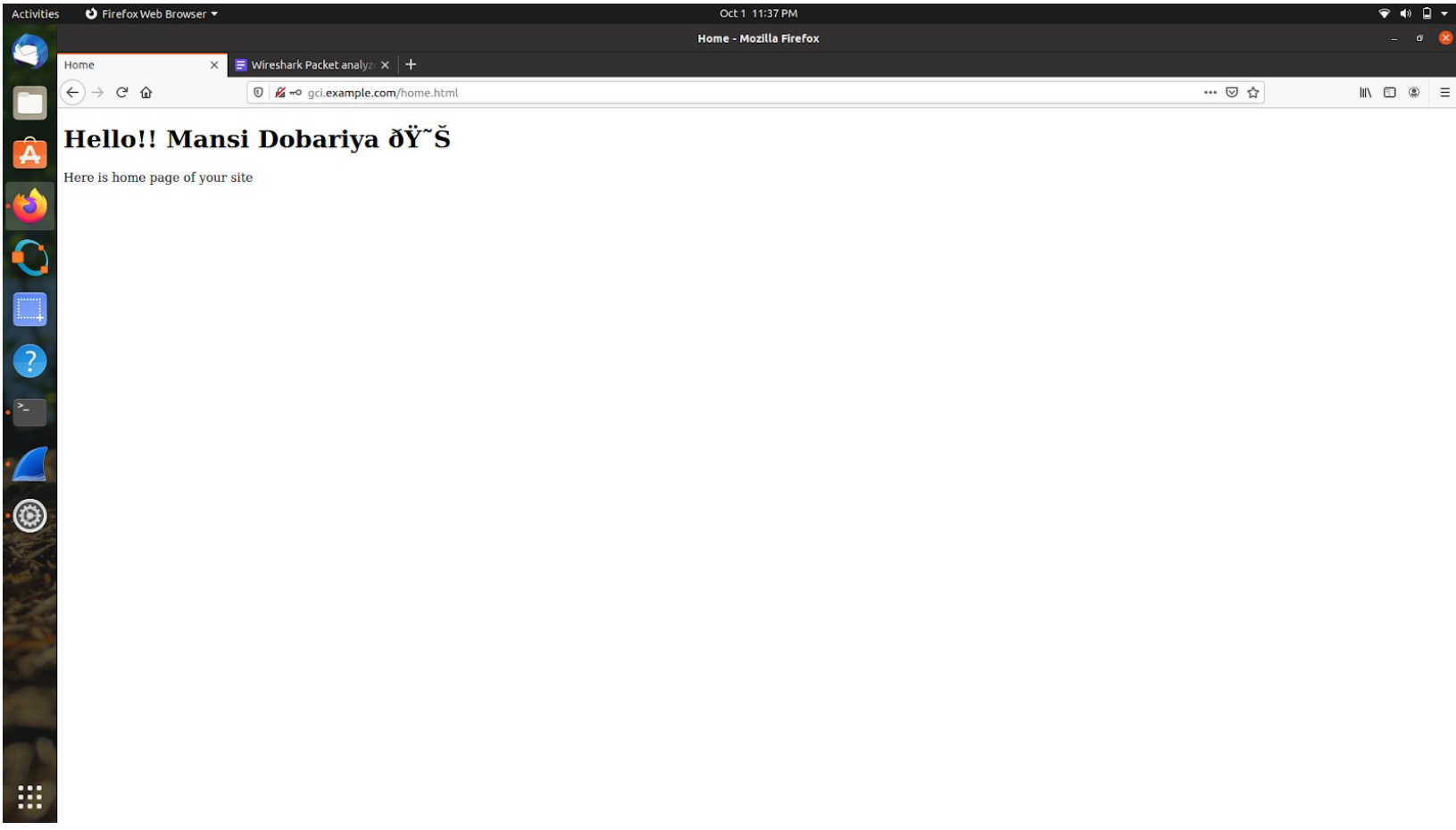


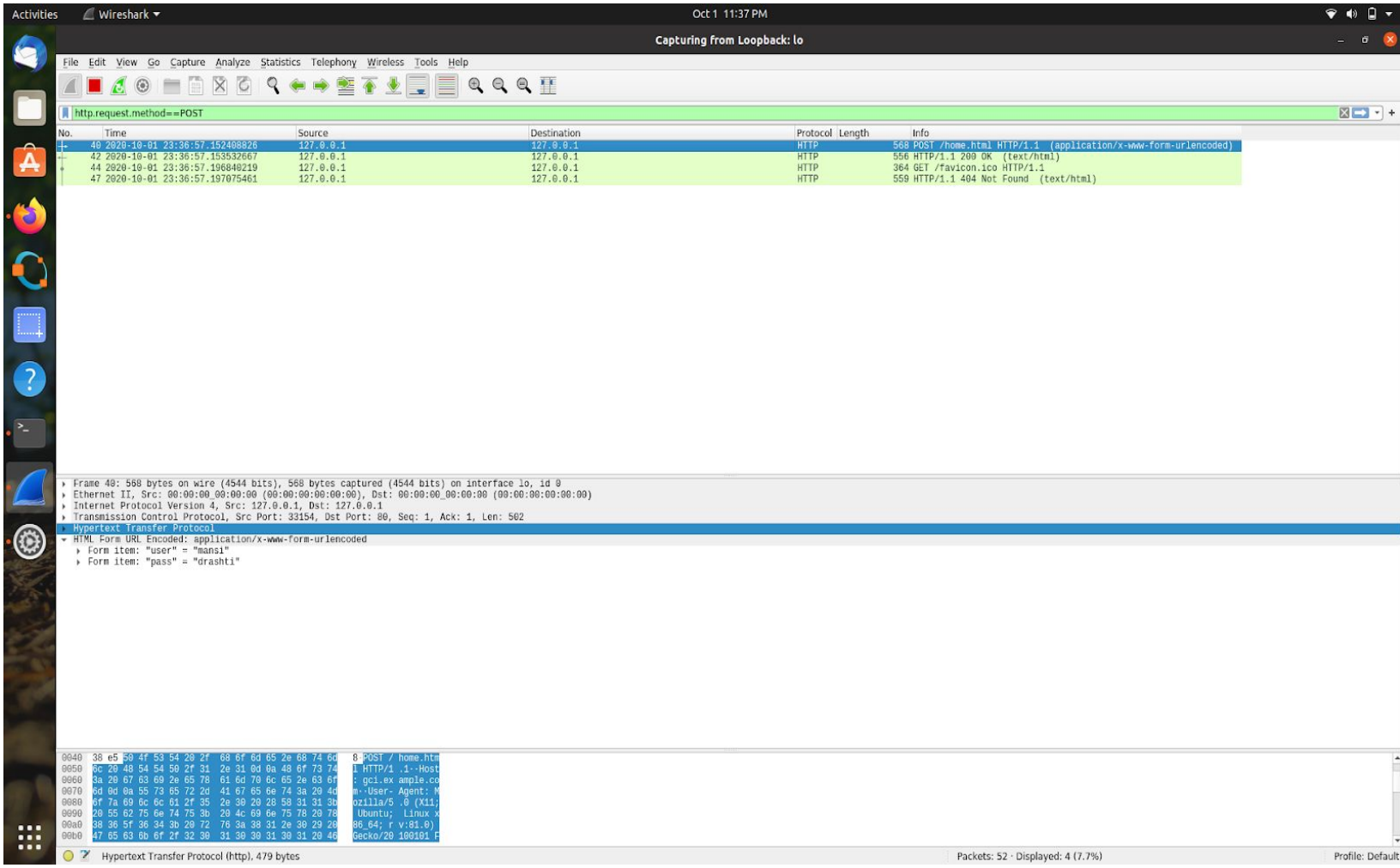


Password Username Sniffing

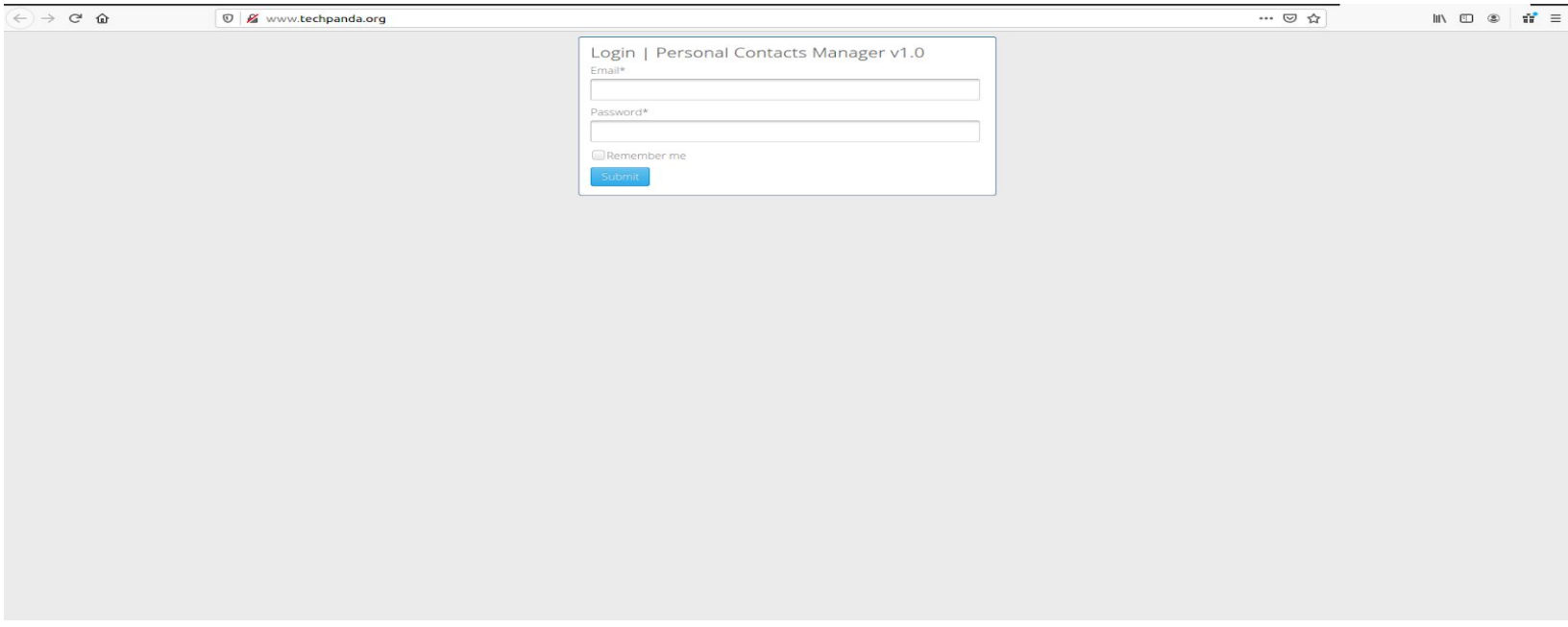


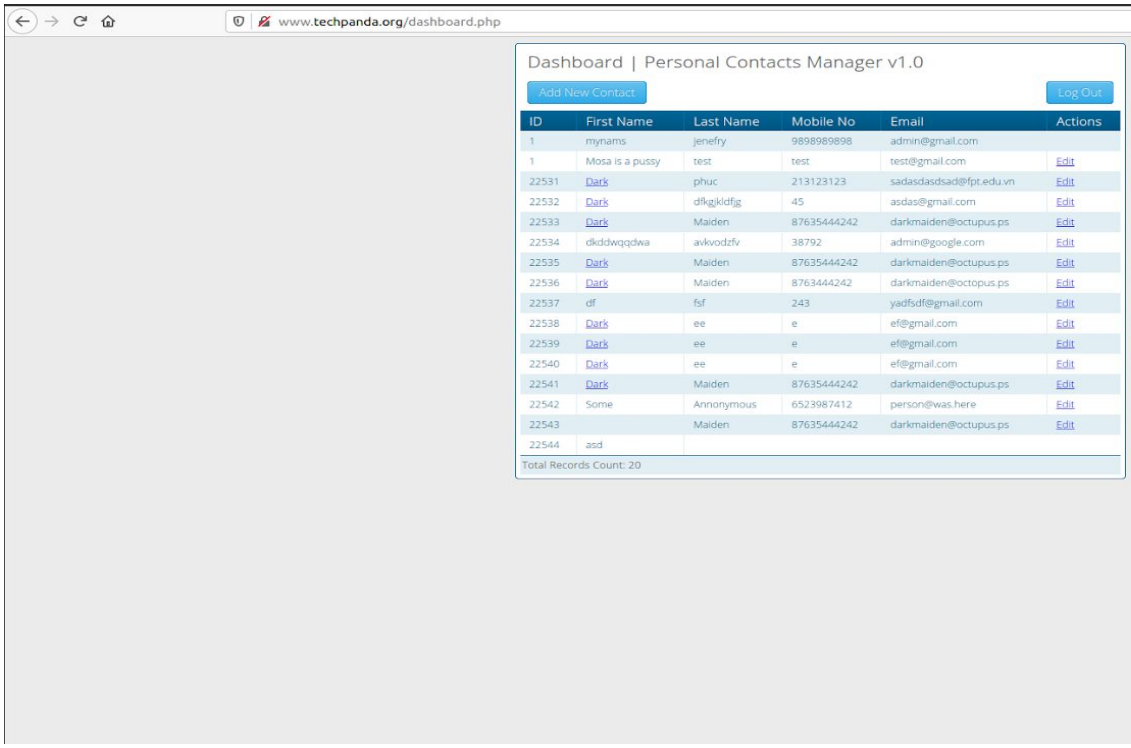

Activities
Firefox Web Browser
Oct 1 11:36 PM
Login | Personal Contacts Manager - Mozilla Firefox
Login | Personal Contacts M
Wireshark Packet analyz
gci.example.com
Login page
Email address
mansi
We'll never share your email with anyone else.
Password
Remember Me
Submit

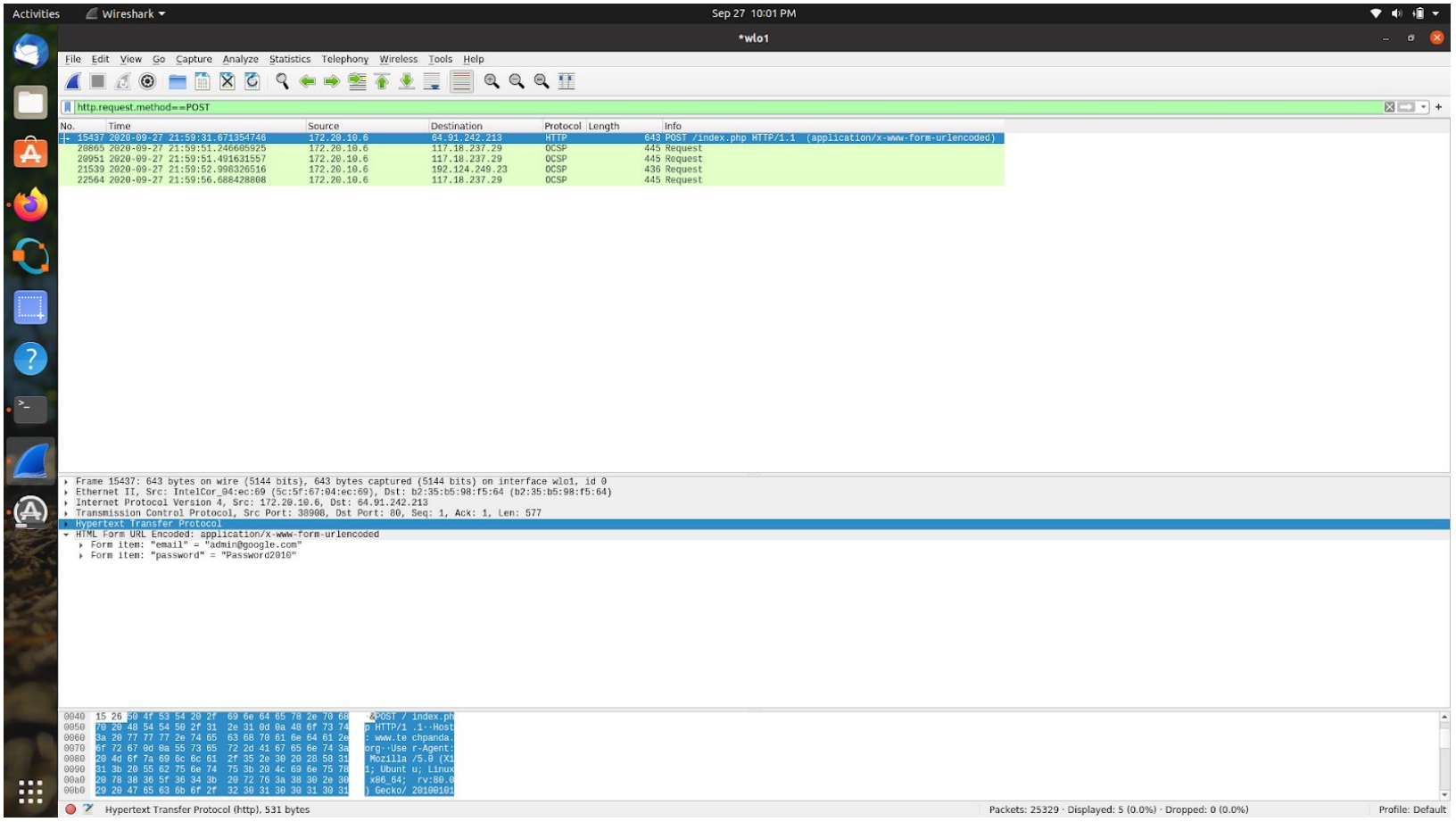

Activities
Firefox Web Browser
Oct 1 11:37 PM
Home - Mozilla Firefox
Home
Wireshark Packet analyz
gci.example.com/home.html
Hello!! Mansi Dobariya ðŸ˜Š
Here is home page of your site



Another website:




www.techpanda.org/dashboard.php
Dashboard | Personal Contacts Manager v1.0
Add New Contact
Log Out
ID First Name Last Name Mobile No Email Actions
1 mynams jenefry 9898989898 admin@gmail.com
1 Mosa is a pussy test test test@gmail.com Edit
22531 Dark phuc 213123123 sadasdasdsad@fpt.edu.vn Edit
22532 Dark dfkgjkldfjg 45 asdas@gmail.com Edit
22533 Dark Maiden 87635444242 darkmaiden@octupus.ps Edit
22534 dkddwqqdwa avkvodzfv 38792 admin@google.com Edit
22535 Dark Maiden 87635444242 darkmaiden@octupus.ps Edit
22536 Dark Maiden 8763444242 darkmaiden@octupus.ps Edit
22537 df fsf 243 yadfsdf@gmail.com Edit
22538 Dark ee e ef@gmail.com Edit
22539 Dark ee e ef@gmail.com Edit
22540 Dark ee e ef@gmail.com Edit
22541 Dark Maiden 87635444242 darkmaiden@octupus.ps Edit
22542 Some Annonymous 6523987412 person@was.here Edit
22543 Maiden 87635444242 darkmaiden@octupus.ps Edit
22544 asd
Total Records Count: 20


Activities
Wireshark
Sep 27 10:01 PM
*wlo1
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http.request.method==POST
No. Time Source Destination Protocol Length Info
15437 2020-09-27 21:59:31.671354746 172.20.10.6 64.91.242.213 HTTP 643 POST /index.php HTTP/1.1 (application/x-www-form-urlencoded)
20865 2020-09-27 21:59:51.246605925 172.20.10.6 117.18.237.29 OCSP 445 Request
20951 2020-09-27 21:59:51.491631557 172.20.10.6 117.18.237.29 OCSP 445 Request
21539 2020-09-27 21:59:52.998326516 172.20.10.6 192.124.249.23 OCSP 436 Request
22564 2020-09-27 21:59:56.688428808 172.20.10.6 117.18.237.29 OCSP 445 Request
Frame 15437: 643 bytes on wire (5144 bits), 643 bytes captured (5144 bits) on interface wlo1, id 0
Ethernet II, Src: IntelCor_04:ec:69 (5c:5f:67:04:ec:69), Dst: b2:35:b5:98:f5:64 (b2:35:b5:98:f5:64)
Internet Protocol Version 4, Src: 172.20.10.6, Dst: 64.91.242.213
Transmission Control Protocol, Src Port: 38908, Dst Port: 80, Seq: 1, Ack: 1, Len: 577
Hypertext Transfer Protocol
HTML Form URL Encoded: application/x-www-form-urlencoded
Form item: "email" = "admin@google.com"
Form item: "password" = "Password2010"
0040 15 26 50 4f 53 54 20 2f 69 6e 64 65 78 2e 70 68 &POST / index.ph
0050 70 20 48 54 54 50 2f 31 2e 31 0d 0a 48 6f 73 74 p HTTP/1 .1··Host
0060 3a 20 77 77 77 2e 74 65 63 68 70 61 6e 64 61 2e : www.te chpanda.
0070 6f 72 67 0d 0a 55 73 65 72 2d 41 67 65 6e 74 3a org··Use r-Agent:
0080 20 4d 6f 7a 69 6c 6c 61 2f 35 2e 30 20 28 58 31 Mozilla /5.0 (X1
0090 31 3b 20 55 62 75 6e 74 75 3b 20 4c 69 6e 75 78 1; Ubunt u; Linux
00a0 20 78 38 36 5f 36 34 3b 20 72 76 3a 38 30 2e 30 x86_64; rv:80.0
00b0 29 20 47 65 63 6b 6f 2f 32 30 31 30 30 31 30 31) Gecko/ 20100101
Hypertext Transfer Protocol (http), 531 bytes
Packets: 25329 · Displayed: 5 (0.0%) · Dropped: 0 (0.0%)
Profile: Default

4.decimal values expect eth

4.1 eth source 00 1e a6 83 2d a8

4.2 eth destination ac 2b 6e de fd b4

4.3 source ip 74.125.68.27 [4a 7d 44 1b in hex]

4.4 dest ip 192.168.1.104 [c0 a8 01 68]

4.5 TCP src 25 [00 19]

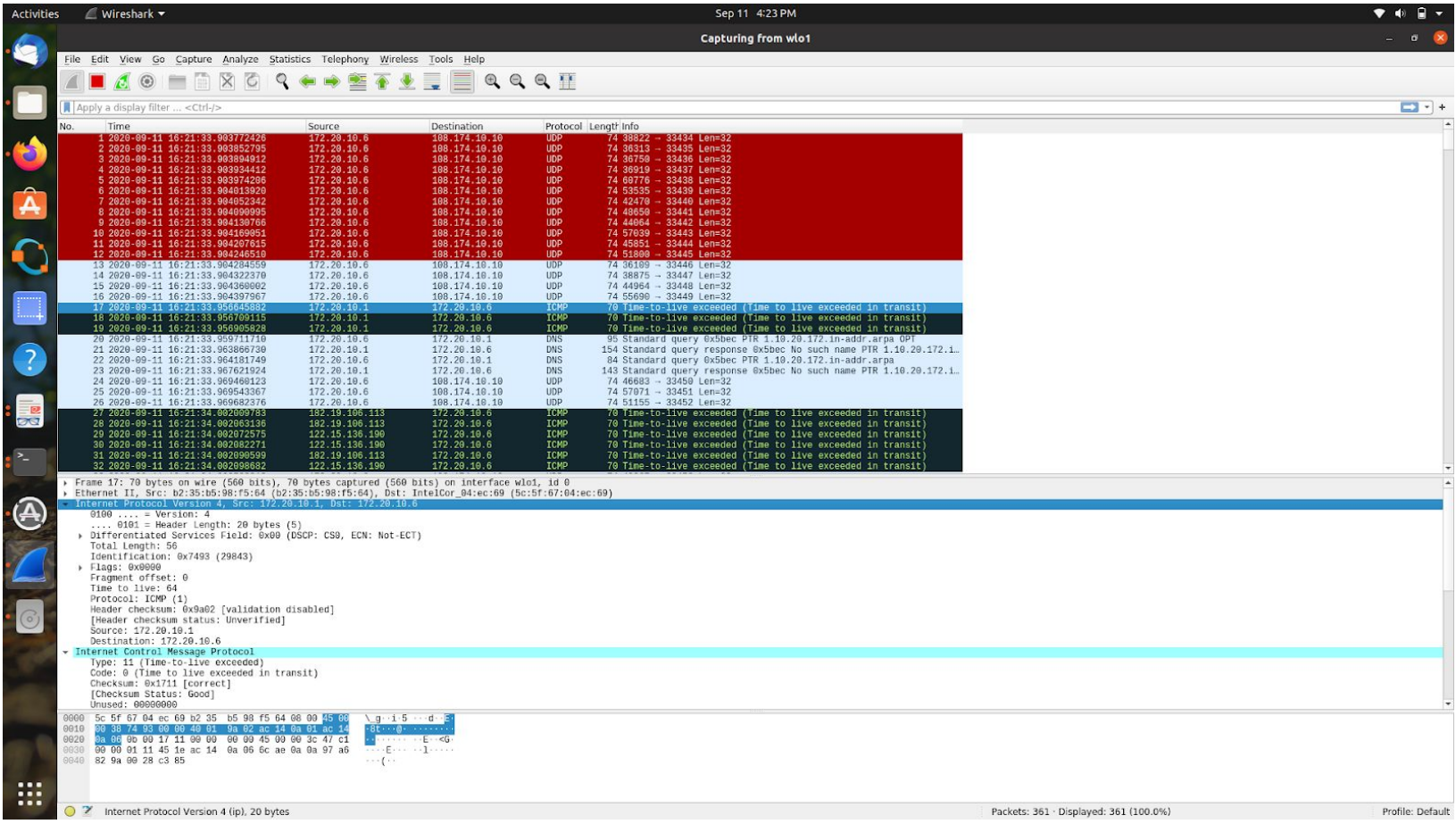
4.6 TCP dest 54656 [d5 80]

4.7 SMTP response code = 3289648 [32 32 30]

parameter = [20 6d 78 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 20 45 53 4d 54 50 20 78 33 30 73 69 34
35 33 32 38 33 34 70 67 65 2e 33 32 20 2d 20 67 73 6d 74 70]

data = [0d 0a]

5.



5.1 Internet Protocol Version = 4,

host ip address = 172.20.10.6

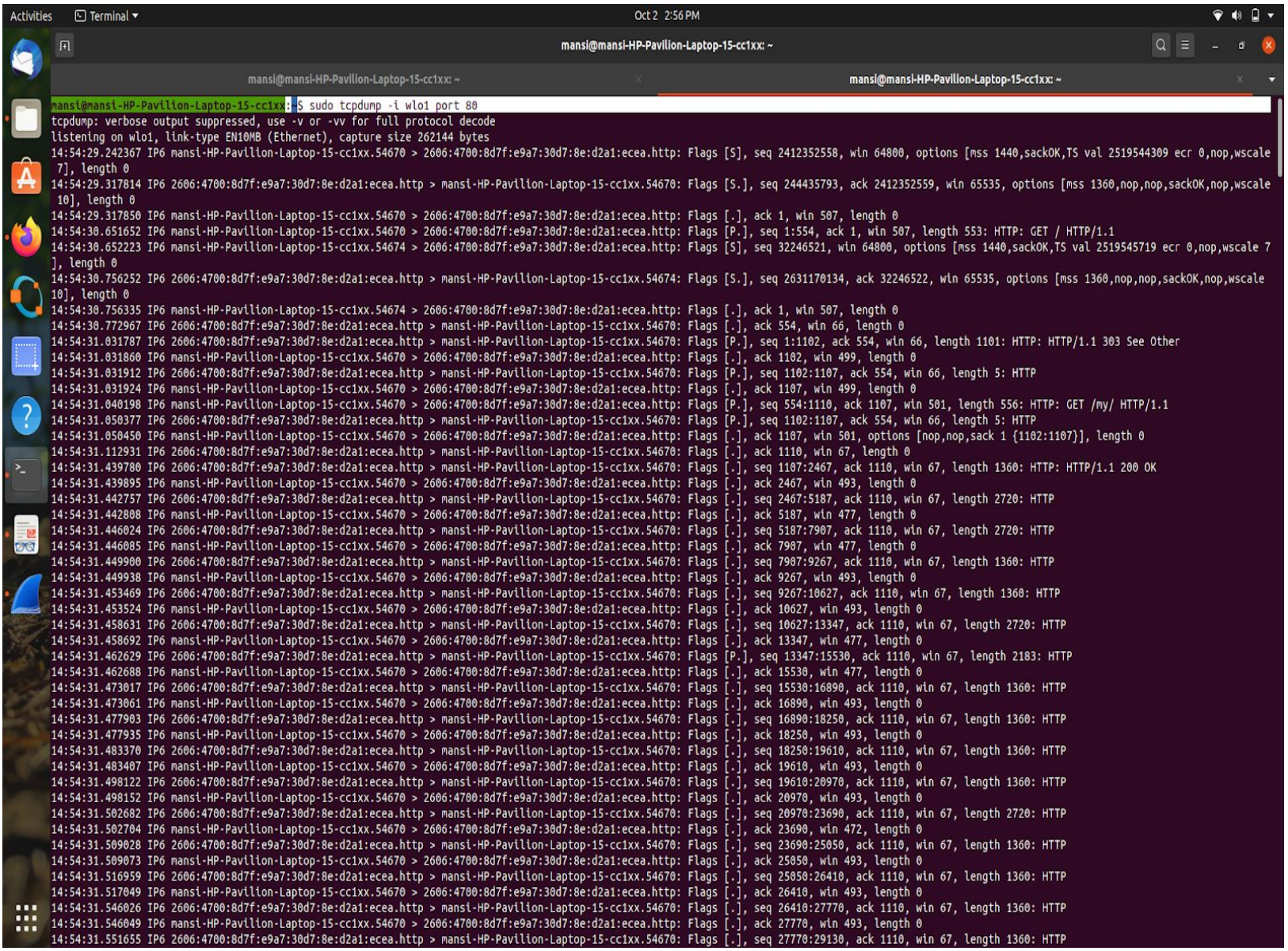
Destination ip address =108.174.10.10

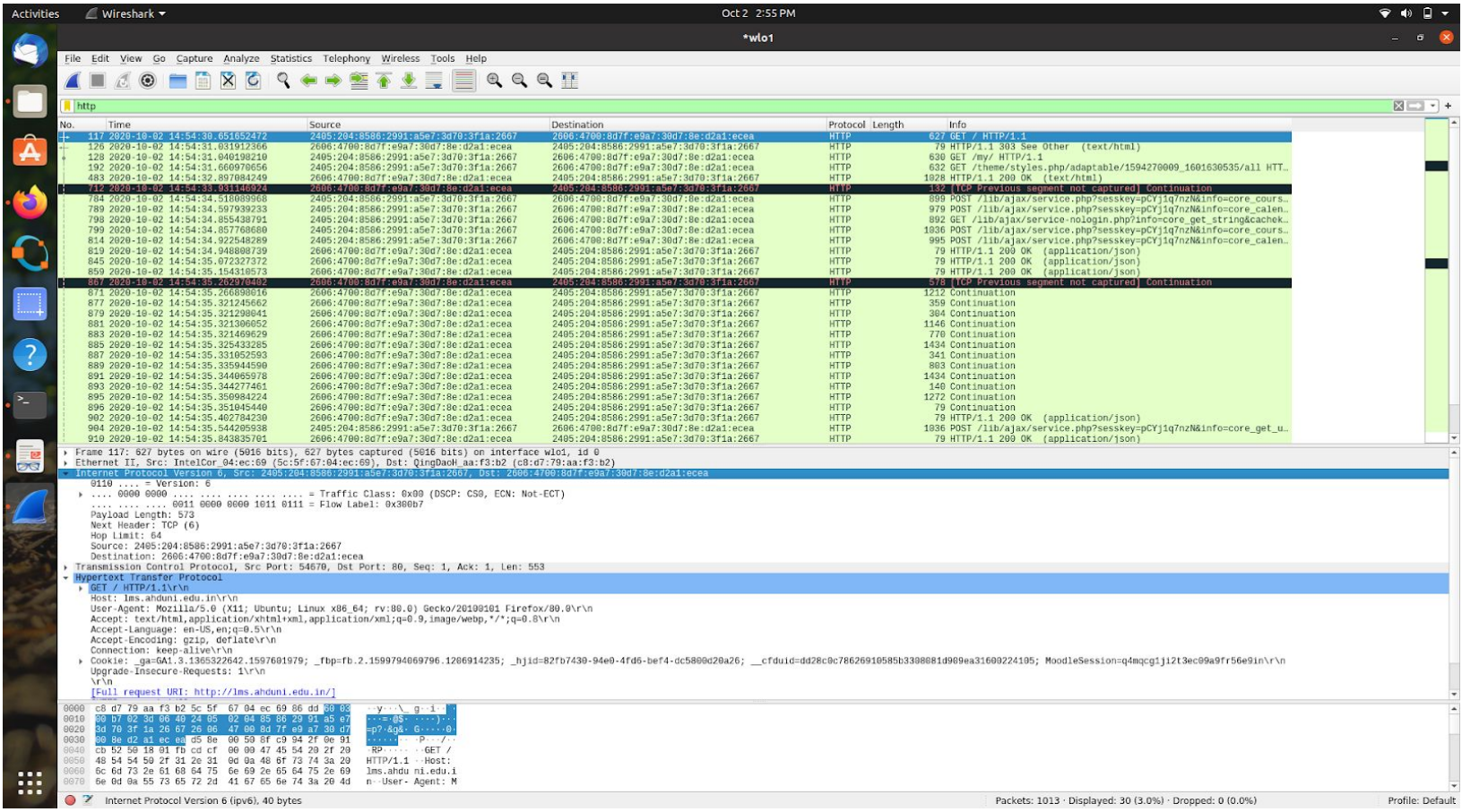
5.2 Header value = 5

5.3 Header Length = 20 bytes [4 bytes src + 4 bytes dest + 2 bytes header length in no. + 1 bytes TTL + 2 bytes checksum
payload size = 70 bytes
5.4 Yes , This IP datagram has been fragmented because of header length , flag ,TTL , source ip , destination ip address ,h
checksum,offset ,time to live ,explicit congestion notification and payload .

Using TCPDUMP Utility

1.





1.1

Using tcpdump -i wlo1 port 80 :: for capturing http packets

1.2

Hostname : lms.ahduni.edu.in

ipv6.src == 2405:204:8586:2991:a5e7:3d70:3f1a:2667

ipv6.dst == 2606:4700:8d7f:e9a7:30d7:8e:d2a1:ecea

Source Port: 54670

Destination Port: 80

1.3

Request frame.time == 2020-10-02 14:54:30.651652472 s

OK reply frame.time == 2020-10-02 14:54:32.897084249 s

Total time taken = 2.245431777 seconds

1.4

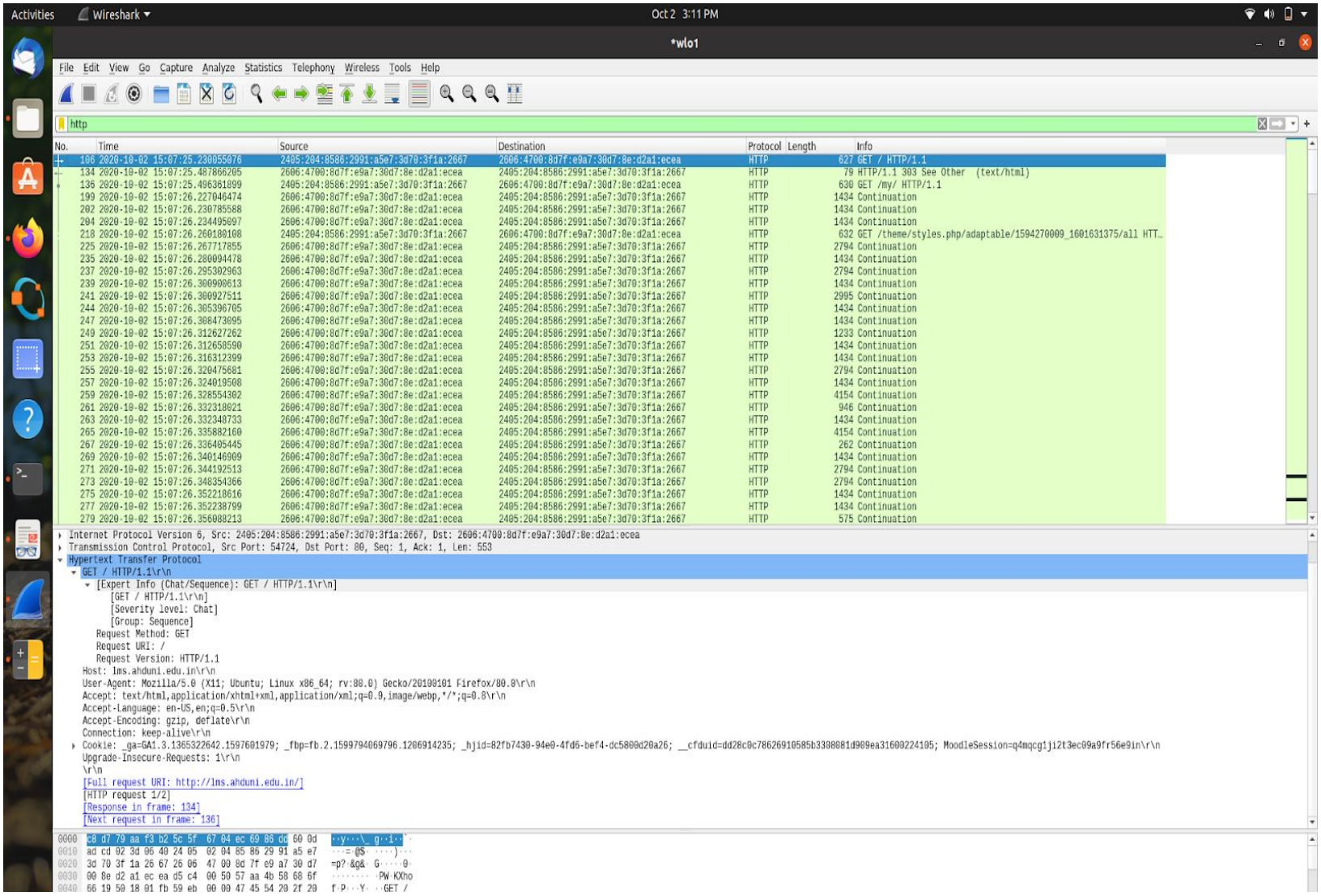
MAC address,Ethernet II

Src: IntelCor_04:ec:69 (5c:5f:67:04:ec:69)

Dst: QingDaoH_aa:f3:b2 (c8:d7:79:aa:f3:b2)

Type: IPv6 (0x86dd)

2.



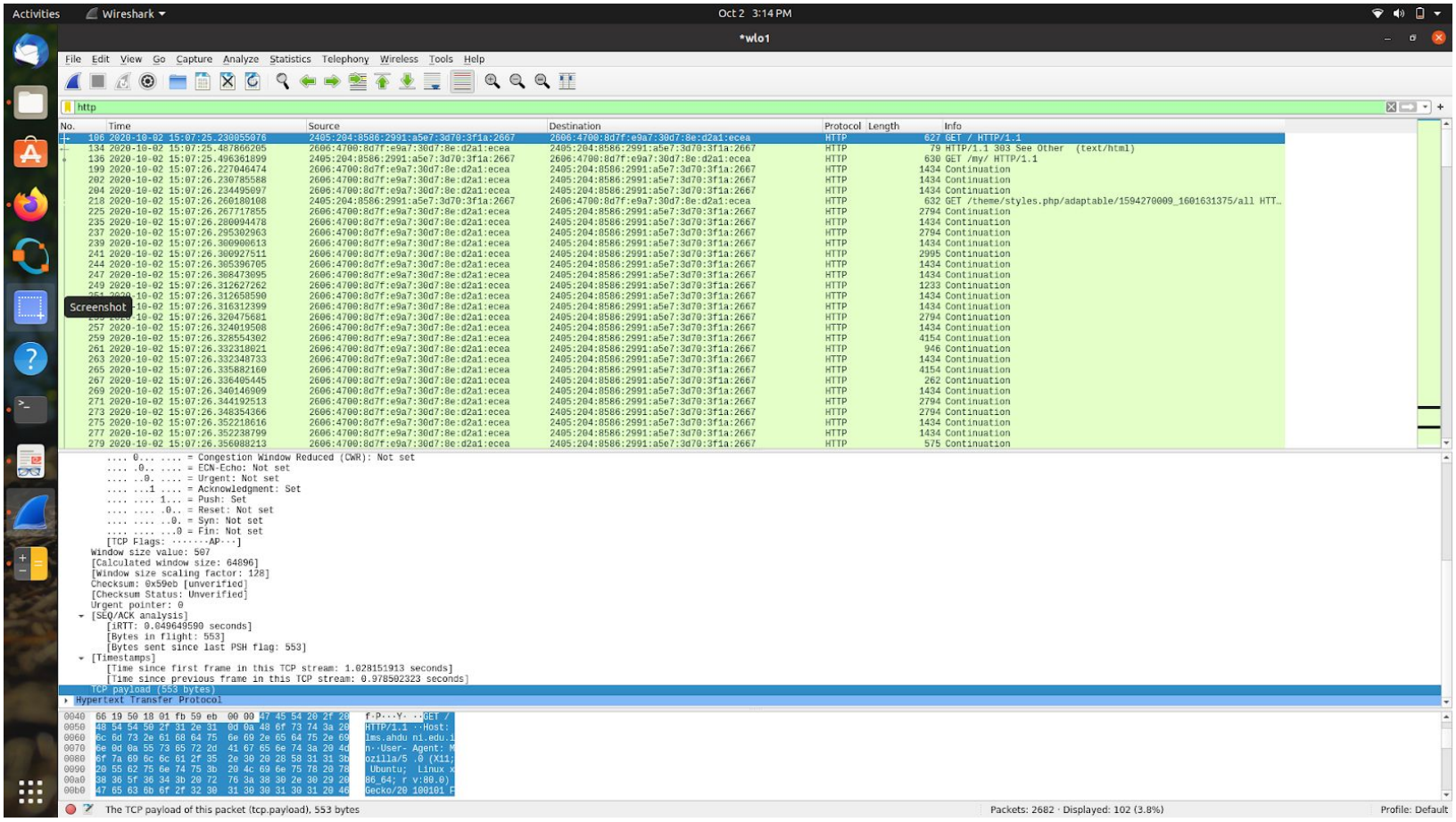
2.1

HTTP version 1.1

2.2

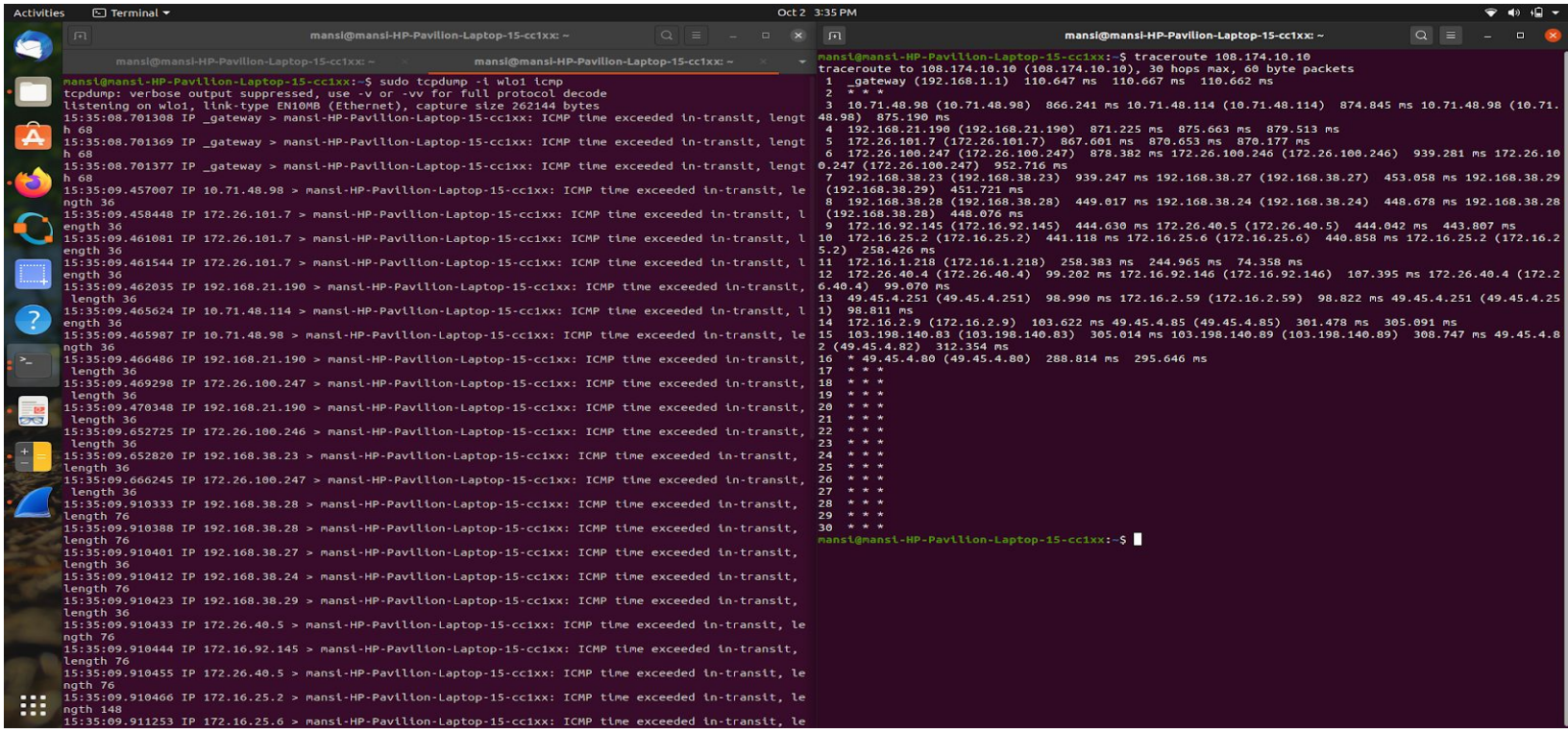
Transmission Control Protocol stream has port address of source and destination ,segment length as tcp is network layer proto
Header length , Acknowledge Flags,also window size value for sender and receiver ,TCP payload size in bytes

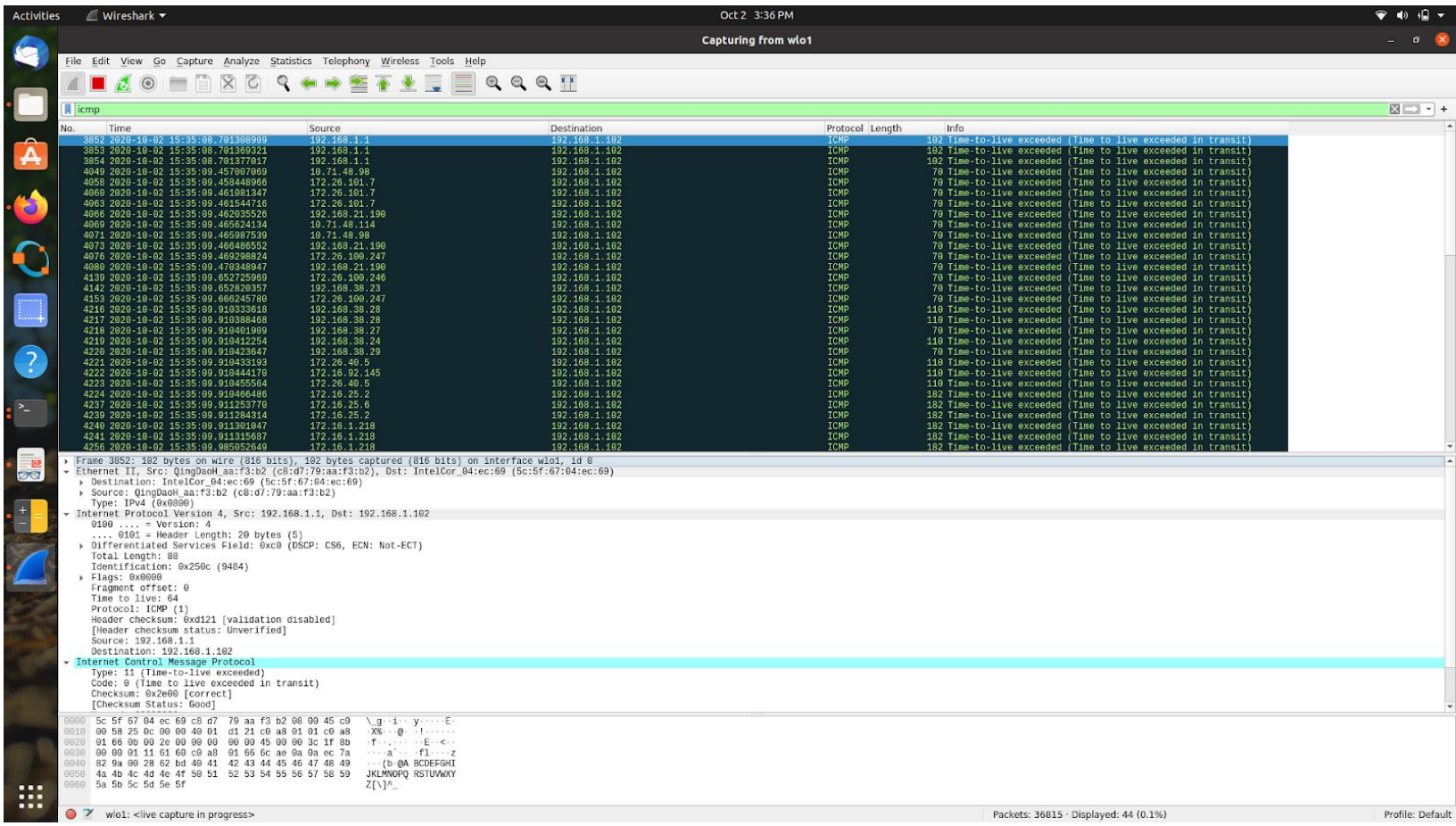
2.3

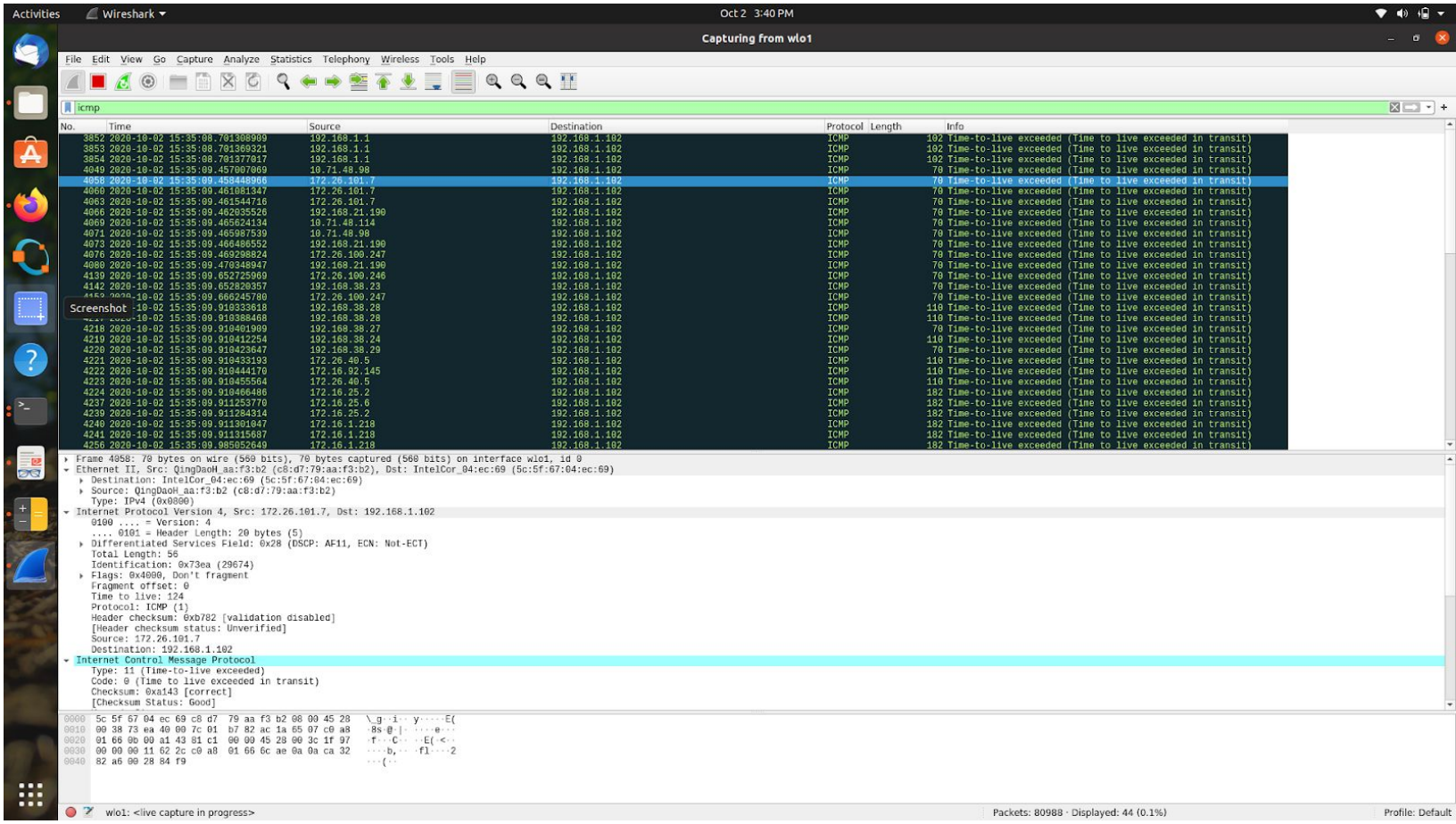


Size of Content[payload,data] = 553 bytes
Header length = 20 bytes ,which contains where we have to send our info [details of destination]

5.5.1 Internet Protocol Version = 4,
host ip address = 172.26.101.7
Destination ip address =192.168.1.102
5.2 Header value = 5
5.3 Header Length = 20 bytes [4 bytes src + 4 bytes dest + 2 bytes header length in no. + 1 bytes TTL + 2 bytes checksum
payload size = 70 bytes
5.4 Yes , This IP datagram has been fragmented because of header length , flag ,TTL , source ip , destination ip address ,header checksum,offset ,time to live ,explicit congestion notification and payload .


Activities
Terminal
Oct 2 3:35 PM
mansi@mansi-HP-Pavilion-Laptop-15-cc1xx: ~
mansi@mansi-HP-Pavilion-Laptop-15-cc1xx: ~
mansi@mansi-HP-Pavilion-Laptop-15-cc1xx:~$ sudo tcpdump -i wlo1 icmp
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on wlo1, link-type EN10MB (Ethernet), capture size 262144 bytes
15:35:08.701308 IP _gateway > mansi-HP-Pavilion-Laptop-15-cc1xx: ICMP time exceeded in-transit, length 68
15:35:08.701369 IP _gateway > mansi-HP-Pavilion-Laptop-15-cc1xx: ICMP time exceeded in-transit, length 68
15:35:08.701377 IP _gateway > mansi-HP-Pavilion-Laptop-15-cc1xx: ICMP time exceeded in-transit, length 68
15:35:09.457007 IP 10.71.48.98 > mansi-HP-Pavilion-Laptop-15-cc1xx: ICMP time exceeded in-transit, length 36
15:35:09.458448 IP 172.26.101.7 > mansi-HP-Pavilion-Laptop-15-cc1xx: ICMP time exceeded in-transit, length 36
15:35:09.461081 IP 172.26.101.7 > mansi-HP-Pavilion-Laptop-15-cc1xx: ICMP time exceeded in-transit, length 36
15:35:09.461544 IP 172.26.101.7 > mansi-HP-Pavilion-Laptop-15-cc1xx: ICMP time exceeded in-transit, length 36
15:35:09.462035 IP 192.168.21.190 > mansi-HP-Pavilion-Laptop-15-cc1xx: ICMP time exceeded in-transit, length 36
15:35:09.465624 IP 10.71.48.114 > mansi-HP-Pavilion-Laptop-15-cc1xx: ICMP time exceeded in-transit, length 36
15:35:09.465987 IP 10.71.48.98 > mansi-HP-Pavilion-Laptop-15-cc1xx: ICMP time exceeded in-transit, length 36
15:35:09.466486 IP 192.168.21.190 > mansi-HP-Pavilion-Laptop-15-cc1xx: ICMP time exceeded in-transit, length 36
15:35:09.469298 IP 172.26.100.247 > mansi-HP-Pavilion-Laptop-15-cc1xx: ICMP time exceeded in-transit, length 36
15:35:09.470348 IP 192.168.21.190 > mansi-HP-Pavilion-Laptop-15-cc1xx: ICMP time exceeded in-transit, length 36
15:35:09.652725 IP 172.26.100.246 > mansi-HP-Pavilion-Laptop-15-cc1xx: ICMP time exceeded in-transit, length 36
15:35:09.652820 IP 192.168.38.23 > mansi-HP-Pavilion-Laptop-15-cc1xx: ICMP time exceeded in-transit, length 36
15:35:09.666245 IP 172.26.100.247 > mansi-HP-Pavilion-Laptop-15-cc1xx: ICMP time exceeded in-transit, length 36
15:35:09.910333 IP 192.168.38.28 > mansi-HP-Pavilion-Laptop-15-cc1xx: ICMP time exceeded in-transit, length 76
15:35:09.910388 IP 192.168.38.28 > mansi-HP-Pavilion-Laptop-15-cc1xx: ICMP time exceeded in-transit, length 76
15:35:09.910401 IP 192.168.38.27 > mansi-HP-Pavilion-Laptop-15-cc1xx: ICMP time exceeded in-transit, length 36
15:35:09.910412 IP 192.168.38.24 > mansi-HP-Pavilion-Laptop-15-cc1xx: ICMP time exceeded in-transit, length 76
15:35:09.910423 IP 192.168.38.29 > mansi-HP-Pavilion-Laptop-15-cc1xx: ICMP time exceeded in-transit, length 36
15:35:09.910433 IP 172.26.40.5 > mansi-HP-Pavilion-Laptop-15-cc1xx: ICMP time exceeded in-transit, length 76
15:35:09.910444 IP 172.16.92.145 > mansi-HP-Pavilion-Laptop-15-cc1xx: ICMP time exceeded in-transit, length 76
15:35:09.910455 IP 172.26.40.5 > mansi-HP-Pavilion-Laptop-15-cc1xx: ICMP time exceeded in-transit, length 76
15:35:09.910466 IP 172.16.25.2 > mansi-HP-Pavilion-Laptop-15-cc1xx: ICMP time exceeded in-transit, length 148
15:35:09.911253 IP 172.16.25.6 > mansi-HP-Pavilion-Laptop-15-cc1xx: ICMP time exceeded in-transit, le
mansi@mansi-HP-Pavilion-Laptop-15-cc1xx: ~
mansi@mansi-HP-Pavilion-Laptop-15-cc1xx:~$ traceroute 108.174.10.10
traceroute to 108.174.10.10 (108.174.10.10), 30 hops max, 60 byte packets
1 _gateway (192.168.1.1) 110.647 ms 110.667 ms 110.662 ms
2 * * *
3 10.71.48.98 (10.71.48.98) 866.241 ms 10.71.48.114 (10.71.48.114) 874.845 ms 10.71.48.98 (10.71.48.98) 875.190 ms
4 192.168.21.190 (192.168.21.190) 871.225 ms 875.663 ms 879.513 ms
5 172.26.101.7 (172.26.101.7) 867.601 ms 870.653 ms 870.177 ms
6 172.26.100.247 (172.26.100.247) 878.382 ms 172.26.100.246 (172.26.100.246) 939.281 ms 172.26.100.247 (172.26.100.247) 952.716 ms
7 192.168.38.23 (192.168.38.23) 939.247 ms 192.168.38.27 (192.168.38.27) 453.058 ms 192.168.38.29 (192.168.38.29) 451.721 ms
8 192.168.38.28 (192.168.38.28) 449.017 ms 192.168.38.24 (192.168.38.24) 448.678 ms 192.168.38.28 (192.168.38.28) 448.076 ms
9 172.16.92.145 (172.16.92.145) 444.630 ms 172.26.40.5 (172.26.40.5) 444.042 ms 443.807 ms
10 172.16.25.2 (172.16.25.2) 441.118 ms 172.16.25.6 (172.16.25.6) 440.858 ms 172.16.25.2 (172.16.25.2) 258.426 ms
11 172.16.1.218 (172.16.1.218) 258.383 ms 244.965 ms 74.358 ms
12 172.26.40.4 (172.26.40.4) 99.202 ms 172.16.92.146 (172.16.92.146) 107.395 ms 172.26.40.4 (172.26.40.4) 99.070 ms
13 49.45.4.251 (49.45.4.251) 98.990 ms 172.16.2.59 (172.16.2.59) 98.822 ms 49.45.4.251 (49.45.4.251) 98.811 ms
14 172.16.2.9 (172.16.2.9) 103.622 ms 49.45.4.85 (49.45.4.85) 301.478 ms 305.091 ms
15 103.198.140.83 (103.198.140.83) 305.014 ms 103.198.140.89 (103.198.140.89) 308.747 ms 49.45.4.82 (49.45.4.82) 312.354 ms
16 * 49.45.4.80 (49.45.4.80) 288.814 ms 295.646 ms
17 * * *
18 * * *
19 * * *
20 * * *
21 * * *
22 * * *
23 * * *
24 * * *
25 * * *
26 * * *
27 * * *
28 * * *
29 * * *
30 * * *
mansi@mansi-HP-Pavilion-Laptop-15-cc1xx:~$


Activities
Wireshark
Oct 2 3:36 PM
Capturing from wlo1
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
icmp
No. Time Source Destination Protocol Length Info
3852 2020-10-02 15:35:08.701308909 192.168.1.1 192.168.1.102 ICMP 102 Time-to-live exceeded (Time to live exceeded in transit)
3853 2020-10-02 15:35:08.701369321 192.168.1.1 192.168.1.102 ICMP 102 Time-to-live exceeded (Time to live exceeded in transit)
3854 2020-10-02 15:35:08.701377017 192.168.1.1 192.168.1.102 ICMP 102 Time-to-live exceeded (Time to live exceeded in transit)
4049 2020-10-02 15:35:09.457007069 10.71.48.98 192.168.1.102 ICMP 70 Time-to-live exceeded (Time to live exceeded in transit)
4058 2020-10-02 15:35:09.458448966 172.26.101.7 192.168.1.102 ICMP 70 Time-to-live exceeded (Time to live exceeded in transit)
4060 2020-10-02 15:35:09.461081347 172.26.101.7 192.168.1.102 ICMP 70 Time-to-live exceeded (Time to live exceeded in transit)
4063 2020-10-02 15:35:09.461544716 172.26.101.7 192.168.1.102 ICMP 70 Time-to-live exceeded (Time to live exceeded in transit)
4066 2020-10-02 15:35:09.462035526 192.168.21.190 192.168.1.102 ICMP 70 Time-to-live exceeded (Time to live exceeded in transit)
4069 2020-10-02 15:35:09.465624134 10.71.48.114 192.168.1.102 ICMP 70 Time-to-live exceeded (Time to live exceeded in transit)
4071 2020-10-02 15:35:09.465987539 10.71.48.98 192.168.1.102 ICMP 70 Time-to-live exceeded (Time to live exceeded in transit)
4073 2020-10-02 15:35:09.466486552 192.168.21.190 192.168.1.102 ICMP 70 Time-to-live exceeded (Time to live exceeded in transit)
4076 2020-10-02 15:35:09.469298824 172.26.100.247 192.168.1.102 ICMP 70 Time-to-live exceeded (Time to live exceeded in transit)
4080 2020-10-02 15:35:09.470348947 192.168.21.190 192.168.1.102 ICMP 70 Time-to-live exceeded (Time to live exceeded in transit)
4139 2020-10-02 15:35:09.652725969 172.26.100.246 192.168.1.102 ICMP 70 Time-to-live exceeded (Time to live exceeded in transit)
4142 2020-10-02 15:35:09.652820357 192.168.38.23 192.168.1.102 ICMP 70 Time-to-live exceeded (Time to live exceeded in transit)
4153 2020-10-02 15:35:09.666245780 172.26.100.247 192.168.1.102 ICMP 70 Time-to-live exceeded (Time to live exceeded in transit)
4216 2020-10-02 15:35:09.910333618 192.168.38.28 192.168.1.102 ICMP 110 Time-to-live exceeded (Time to live exceeded in transit)
4217 2020-10-02 15:35:09.910388468 192.168.38.28 192.168.1.102 ICMP 110 Time-to-live exceeded (Time to live exceeded in transit)
4218 2020-10-02 15:35:09.910401909 192.168.38.27 192.168.1.102 ICMP 70 Time-to-live exceeded (Time to live exceeded in transit)
4219 2020-10-02 15:35:09.910412254 192.168.38.24 192.168.1.102 ICMP 110 Time-to-live exceeded (Time to live exceeded in transit)
4220 2020-10-02 15:35:09.910423647 192.168.38.29 192.168.1.102 ICMP 70 Time-to-live exceeded (Time to live exceeded in transit)
4221 2020-10-02 15:35:09.910433193 172.26.40.5 192.168.1.102 ICMP 110 Time-to-live exceeded (Time to live exceeded in transit)
4222 2020-10-02 15:35:09.910444170 172.16.92.145 192.168.1.102 ICMP 110 Time-to-live exceeded (Time to live exceeded in transit)
4223 2020-10-02 15:35:09.910455564 172.26.40.5 192.168.1.102 ICMP 110 Time-to-live exceeded (Time to live exceeded in transit)
4224 2020-10-02 15:35:09.910466486 172.16.25.2 192.168.1.102 ICMP 182 Time-to-live exceeded (Time to live exceeded in transit)
4237 2020-10-02 15:35:09.911253770 172.16.25.6 192.168.1.102 ICMP 182 Time-to-live exceeded (Time to live exceeded in transit)
4239 2020-10-02 15:35:09.911284314 172.16.25.2 192.168.1.102 ICMP 182 Time-to-live exceeded (Time to live exceeded in transit)
4240 2020-10-02 15:35:09.911301047 172.16.1.218 192.168.1.102 ICMP 182 Time-to-live exceeded (Time to live exceeded in transit)
4241 2020-10-02 15:35:09.911315687 172.16.1.218 192.168.1.102 ICMP 182 Time-to-live exceeded (Time to live exceeded in transit)
4256 2020-10-02 15:35:09.985052649 172.16.1.218 192.168.1.102 ICMP 182 Time-to-live exceeded (Time to live exceeded in transit)
Frame 3852: 102 bytes on wire (816 bits), 102 bytes captured (816 bits) on interface wlo1, id 0
Ethernet II, Src: QingDaoH_aa:f3:b2 (c8:d7:79:aa:f3:b2), Dst: IntelCor_04:ec:69 (5c:5f:67:04:ec:69)
Destination: IntelCor_04:ec:69 (5c:5f:67:04:ec:69)
Source: QingDaoH_aa:f3:b2 (c8:d7:79:aa:f3:b2)
Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.1.102
0100 .... = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0xc0 (DSCP: CS6, ECN: Not-ECT)
Total Length: 88
Identification: 0x250c (9484)
Flags: 0x0000
Fragment offset: 0
Time to live: 64
Protocol: ICMP (1)
Header checksum: 0xd121 [validation disabled]
[Header checksum status: Unverified]
Source: 192.168.1.1
Destination: 192.168.1.102
Internet Control Message Protocol
Type: 11 (Time-to-live exceeded)
Code: 0 (Time to live exceeded in transit)
Checksum: 0x2e00 [correct]
[Checksum Status: Good]
0000 5c 5f 67 04 ec 69 c8 d7 79 aa f3 b2 08 00 45 c0 _g··i·· y·····E·
0010 00 58 25 0c 00 00 40 01 d1 21 c0 a8 01 01 c0 a8 ·X%···@· ·!·····
0020 01 66 0b 00 2e 00 00 00 00 00 45 00 00 3c 1f 8b ·f····· ··E··<··
0030 00 00 01 11 61 60 c0 a8 01 66 6c ae 0a 0a ec 7a ····a`··· ·fl····z
0040 82 9a 00 28 62 bd 40 41 42 43 44 45 46 47 48 49 ···(b·@A BCDEFGHI
0050 4a 4b 4c 4d 4e 4f 50 51 52 53 54 55 56 57 58 59 JKLMNOPQ RSTUVWXY
0060 5a 5b 5c 5d 5e 5f Z[\]^_
wlo1: <live capture in progress>
Packets: 36815 · Displayed: 44 (0.1%)
Profile: Default


Activities
Wireshark
Oct 2 3:40 PM
Capturing from wlo1
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
icmp
No. Time Source Destination Protocol Length Info
3852 2020-10-02 15:35:08.701308909 192.168.1.1 192.168.1.102 ICMP 102 Time-to-live exceeded (Time to live exceeded in transit)
3853 2020-10-02 15:35:08.701369321 192.168.1.1 192.168.1.102 ICMP 102 Time-to-live exceeded (Time to live exceeded in transit)
3854 2020-10-02 15:35:08.701377017 192.168.1.1 192.168.1.102 ICMP 102 Time-to-live exceeded (Time to live exceeded in transit)
4049 2020-10-02 15:35:09.457007069 10.71.48.98 192.168.1.102 ICMP 70 Time-to-live exceeded (Time to live exceeded in transit)
4058 2020-10-02 15:35:09.458448966 172.26.101.7 192.168.1.102 ICMP 70 Time-to-live exceeded (Time to live exceeded in transit)
4060 2020-10-02 15:35:09.461081347 172.26.101.7 192.168.1.102 ICMP 70 Time-to-live exceeded (Time to live exceeded in transit)
4063 2020-10-02 15:35:09.461544716 172.26.101.7 192.168.1.102 ICMP 70 Time-to-live exceeded (Time to live exceeded in transit)
4066 2020-10-02 15:35:09.462035526 192.168.21.190 192.168.1.102 ICMP 70 Time-to-live exceeded (Time to live exceeded in transit)
4069 2020-10-02 15:35:09.465624134 10.71.48.114 192.168.1.102 ICMP 70 Time-to-live exceeded (Time to live exceeded in transit)
4071 2020-10-02 15:35:09.465987539 10.71.48.98 192.168.1.102 ICMP 70 Time-to-live exceeded (Time to live exceeded in transit)
4073 2020-10-02 15:35:09.466486552 192.168.21.190 192.168.1.102 ICMP 70 Time-to-live exceeded (Time to live exceeded in transit)
4076 2020-10-02 15:35:09.469298824 172.26.100.247 192.168.1.102 ICMP 70 Time-to-live exceeded (Time to live exceeded in transit)
4080 2020-10-02 15:35:09.470348947 192.168.21.190 192.168.1.102 ICMP 70 Time-to-live exceeded (Time to live exceeded in transit)
4139 2020-10-02 15:35:09.652725969 172.26.100.246 192.168.1.102 ICMP 70 Time-to-live exceeded (Time to live exceeded in transit)
4142 2020-10-02 15:35:09.652820357 192.168.38.23 192.168.1.102 ICMP 70 Time-to-live exceeded (Time to live exceeded in transit)
Screenshot
10-02 15:35:09.666245780 172.26.100.247 192.168.1.102 ICMP 70 Time-to-live exceeded (Time to live exceeded in transit)
10-02 15:35:09.910333618 192.168.38.28 192.168.1.102 ICMP 110 Time-to-live exceeded (Time to live exceeded in transit)
10-02 15:35:09.910388468 192.168.38.28 192.168.1.102 ICMP 110 Time-to-live exceeded (Time to live exceeded in transit)
4218 2020-10-02 15:35:09.910401909 192.168.38.27 192.168.1.102 ICMP 70 Time-to-live exceeded (Time to live exceeded in transit)
4219 2020-10-02 15:35:09.910412254 192.168.38.24 192.168.1.102 ICMP 110 Time-to-live exceeded (Time to live exceeded in transit)
4220 2020-10-02 15:35:09.910423647 192.168.38.29 192.168.1.102 ICMP 70 Time-to-live exceeded (Time to live exceeded in transit)
4221 2020-10-02 15:35:09.910433193 172.26.40.5 192.168.1.102 ICMP 110 Time-to-live exceeded (Time to live exceeded in transit)
4222 2020-10-02 15:35:09.910444170 172.16.92.145 192.168.1.102 ICMP 110 Time-to-live exceeded (Time to live exceeded in transit)
4223 2020-10-02 15:35:09.910455564 172.26.40.5 192.168.1.102 ICMP 110 Time-to-live exceeded (Time to live exceeded in transit)
4224 2020-10-02 15:35:09.910466486 172.16.25.2 192.168.1.102 ICMP 182 Time-to-live exceeded (Time to live exceeded in transit)
4237 2020-10-02 15:35:09.911253770 172.16.25.6 192.168.1.102 ICMP 182 Time-to-live exceeded (Time to live exceeded in transit)
4239 2020-10-02 15:35:09.911284314 172.16.25.2 192.168.1.102 ICMP 182 Time-to-live exceeded (Time to live exceeded in transit)
4240 2020-10-02 15:35:09.911301047 172.16.1.218 192.168.1.102 ICMP 182 Time-to-live exceeded (Time to live exceeded in transit)
4241 2020-10-02 15:35:09.911315687 172.16.1.218 192.168.1.102 ICMP 182 Time-to-live exceeded (Time to live exceeded in transit)
4256 2020-10-02 15:35:09.985052649 172.16.1.218 192.168.1.102 ICMP 182 Time-to-live exceeded (Time to live exceeded in transit)
Frame 4058: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface wlo1, id 0
Ethernet II, Src: QingDaoH_aa:f3:b2 (c8:d7:79:aa:f3:b2), Dst: IntelCor_04:ec:69 (5c:5f:67:04:ec:69)
Destination: IntelCor_04:ec:69 (5c:5f:67:04:ec:69)
Source: QingDaoH_aa:f3:b2 (c8:d7:79:aa:f3:b2)
Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 172.26.101.7, Dst: 192.168.1.102
0100 .... = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x28 (DSCP: AF11, ECN: Not-ECT)
Total Length: 56
Identification: 0x73ea (29674)
Flags: 0x4000, Don't fragment
Fragment offset: 0
Time to live: 124
Protocol: ICMP (1)
Header checksum: 0xb782 [validation disabled]
[Header checksum status: Unverified]
Source: 172.26.101.7
Destination: 192.168.1.102
Internet Control Message Protocol
Type: 11 (Time-to-live exceeded)
Code: 0 (Time to live exceeded in transit)
Checksum: 0xa143 [correct]
[Checksum Status: Good]
0000 5c 5f 67 04 ec 69 c8 d7 79 aa f3 b2 08 00 45 28
0010 00 38 73 ea 40 00 7c 01 b7 82 ac 1a 65 07 c0 a8
0020 01 66 0b 00 a1 43 81 c1 00 00 45 28 00 3c 1f 97
0030 00 00 00 11 62 2c c0 a8 01 66 6c ae 0a 0a ca 32
0040 82 a6 00 28 84 f9
wlo1: <live capture in progress>
Packets: 80988 · Displayed: 44 (0.1%)
Profile: Default