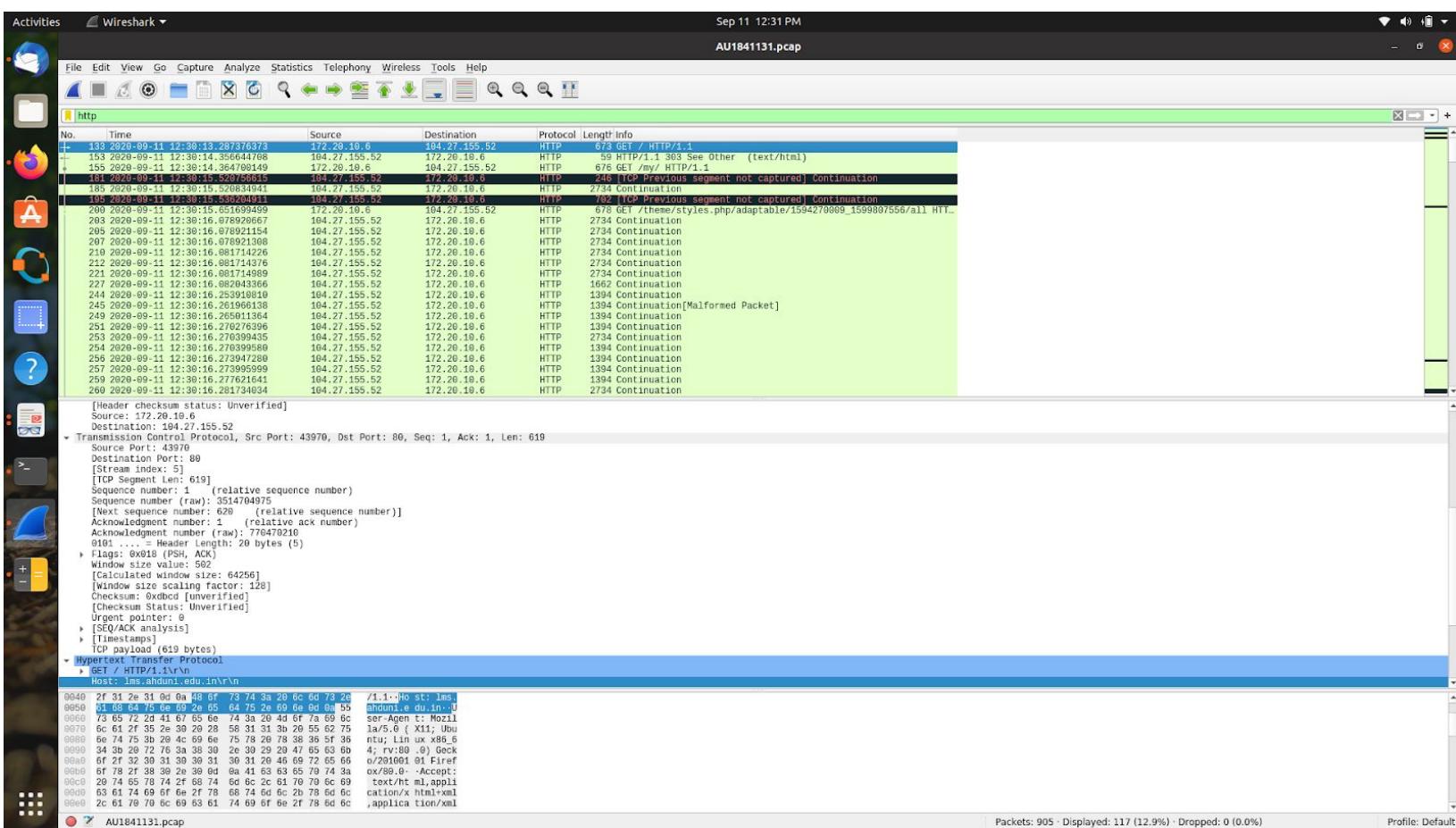


Mansi Dobariya AU1841131

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

Activities Wireshark

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

AU1841131.pcap

http

No.	Time	Source	Destination	Protocol	Length/Info
441	2020-09-11 12:30:16.963741099	104.27.155.52	172.20.10.6	HTTP	1394 Continuation
443	2020-09-11 12:30:16.963861130	104.27.155.52	172.20.10.6	HTTP	1394 Continuation
444	2020-09-11 12:30:16.963871713	104.27.155.52	172.20.10.6	HTTP	1394 Continuation
447	2020-09-11 12:30:16.967874993	104.27.155.52	172.20.10.6	HTTP	1394 Continuation
449	2020-09-11 12:30:16.971459316	104.27.155.52	172.20.10.6	HTTP	2734 Continuation[Malformed Packet]
450	2020-09-11 12:30:16.971460316	104.27.155.52	172.20.10.6	HTTP	2734 Continuation
453	2020-09-11 12:30:16.988126395	104.27.155.52	172.20.10.6	HTTP	2734 Continuation
454	2020-09-11 12:30:16.988127001	104.27.155.52	172.20.10.6	HTTP	2734 Continuation
457	2020-09-11 12:30:16.983418155	104.27.155.52	172.20.10.6	HTTP	947 Continuation
646	2020-09-11 12:30:17.001855131	104.27.155.52	172.20.10.6	HTTP	108 [TCP Previous segment not captured] Continuation
647	2020-09-11 12:30:17.001855131	104.27.155.52	172.20.10.6	HTTP	1394 Continuation
650	2020-09-11 12:30:17.001855131	104.27.155.52	172.20.10.6	HTTP	561 HTTP/1.1 304 Not Modified
700	2020-09-11 12:30:18.442252978	104.27.155.52	172.20.10.6	HTTP	1024 POST /lib/ajax/service_nologin.php?info=core_get_string&cache_k...
723	2020-09-11 12:30:18.442252978	104.27.155.52	172.20.10.6	HTTP	938 GET /lib/ajax/service_nologin.php?info=core_get_string&cache_k...
735	2020-09-11 12:30:18.943140675	104.27.155.52	172.20.10.6	HTTP	1041 POST /lib/ajax/service.php?seskey_ck2BqswPL&info=core_calen...
781	2020-09-11 12:30:20.551099317	104.27.155.52	172.20.10.6	HTTP	74 HTTP/1.1 200 OK (application/json)
800	2020-09-11 12:30:21.048082094	104.27.155.52	172.20.10.6	HTTP	59 HTTP/1.1 200 OK (application/json)
812	2020-09-11 12:30:21.668408013	104.27.155.52	172.20.10.6	HTTP	1394 Continuation
814	2020-09-11 12:30:21.668471963	104.27.155.52	172.20.10.6	HTTP	59 [TCP Previous segment not captured] Continuation
815	2020-09-11 12:30:21.668471963	104.27.155.52	172.20.10.6	HTTP	59 [TCP Previous segment not captured] Continuation

Transmission Control Protocol, Src Port: 80, Dst Port: 43990, Seq: 514, Ack: 885, Len: 5

Source Port: 80
Dest Port: 43990
Sequence number: 514
[Stream index: 16]
[TCP Segment len: 5]
Sequence number (raw): 2352341972
Acknowledge number (raw): 885 (relative ack number)
Acknowledgment number (raw): 965111070
Offset (relative sequence number): 20 bytes (5)
Flags: 0x010 (PSH, ACK)
Window size value: 65535
[Checksum Status: Unverified]
[Urgent pointer: 0]
[Timestamps]
[TCP segment data (5 bytes)]
[2 Reassembled TCP Segments (518 bytes): #749(513), #751(5)]

HTTP/1.1 200 OK\r\nContent-Type: application/json; charset=utf-8\r\nDate: Fri, 11 Sep 2020 07:00:39 GMT\r\nContent-Length: 177\r\nContent-Type: application/json; charset=utf-8\r\n

Frame (59 bytes) Reassembled TCP (518 bytes) De-chunked entity body (177 bytes) Uncompressed entity body (225 bytes)

Packets: 905 - Displayed: 117 (12.9%) - Dropped: 0 (0.0%) Profile: Default

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)

Activities Wireshark

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

AU1841131.pcap

http

No.	Time	Source	Destination	Protocol	Length/Info
153	2020-09-11 12:30:14.356644	104.27.155.52	172.20.10.6	HTTP	59 HTTP/1.1 303 See Other (text/html)
155	2020-09-11 12:30:14.364708	104.27.155.52	172.20.10.6	HTTP	674 GET /my/ HTTP/1.1
156	2020-09-11 12:30:14.364708	104.27.155.52	172.20.10.6	HTTP	59 [TCP Previous segment not captured] Continuation
158	2020-09-11 12:30:15.526834	104.27.155.52	172.20.10.6	HTTP	2734 Continuation
160	2020-09-11 12:30:15.536204	104.27.155.52	172.20.10.6	HTTP	2734 Continuation
161	2020-09-11 12:30:15.536204	104.27.155.52	172.20.10.6	HTTP	2734 Continuation
162	2020-09-11 12:30:16.078920	104.27.155.52	172.20.10.6	HTTP	2734 Continuation
203	2020-09-11 12:30:16.078921	104.27.155.52	172.20.10.6	HTTP	2734 Continuation
204	2020-09-11 12:30:16.078921	104.27.155.52	172.20.10.6	HTTP	2734 Continuation
210	2020-09-11 12:30:16.081714	104.27.155.52	172.20.10.6	HTTP	2734 Continuation
211	2020-09-11 12:30:16.081714	104.27.155.52	172.20.10.6	HTTP	2734 Continuation
212	2020-09-11 12:30:16.082244	104.27.155.52	172.20.10.6	HTTP	2734 Continuation
227	2020-09-11 12:30:16.082843	104.27.155.52	172.20.10.6	HTTP	1662 Continuation
244	2020-09-11 12:30:16.253918	104.27.155.52	172.20.10.6	HTTP	1394 Continuation
245	2020-09-11 12:30:16.253918	104.27.155.52	172.20.10.6	HTTP	1394 Continuation
246	2020-09-11 12:30:16.256511	104.27.155.52	172.20.10.6	HTTP	1394 Continuation
247	2020-09-11 12:30:16.256511	104.27.155.52	172.20.10.6	HTTP	1394 Continuation[Malformed Packet]
253	2020-09-11 12:30:16.270279	104.27.155.52	172.20.10.6	HTTP	2734 Continuation
259	2020-09-11 12:30:16.276399	104.27.155.52	172.20.10.6	HTTP	1394 Continuation
260	2020-09-11 12:30:16.276399	104.27.155.52	172.20.10.6	HTTP	1394 Continuation
267	2020-09-11 12:30:16.277621	104.27.155.52	172.20.10.6	HTTP	1394 Continuation
268	2020-09-11 12:30:16.277621	104.27.155.52	172.20.10.6	HTTP	1394 Continuation
269	2020-09-11 12:30:16.277621	104.27.155.52	172.20.10.6	HTTP	1394 Continuation
270	2020-09-11 12:30:16.281734	104.27.155.52	172.20.10.6	HTTP	2734 Continuation

Frame (480 bytes) Reassembled TCP (504 bytes) De-chunked entity body (504 bytes) Uncompressed entity body (504 bytes)

Ethernet II, Src: IntelCor_04:ec:69 (00:0c:29:04:ec:69), Dst: b2:35:b5:98:f5:64 (b2:35:b5:98:f5:64)

Destination: b2:35:b5:98:f5:64 (b2:35:b5:98:f5:64)
Source: IntelCor_04:ec:69 (00:0c:29:04:ec:69)
Type: IPv4 (0x0800)

Internet Protocol Version 4, Src: 172.20.10.6, Dst: 104.27.155.52
... 0101 = Header Length: 20 bytes (5)
... 0101 = Differentiated Services Field: 0x0 (DSCP: CS0, ECN: Not-ECT)
Total length: 504
Identification: 0x6d21 (6705)
Flags: 0x4000, Don't Fragment
Fragment offset: 0
Time to live: 64
Protocol: TCP (6)
Header checksum: 0x91d9 [validation disabled]
[Header checksum status: Unverified]
Source: 172.20.10.6
Destination: 104.27.155.52
Transmission Control Protocol, Src Port: 43970, Dst Port: 80, Seq: 1, Ack: 1, Len: 619
Hypertext Transfer Protocol

Frame (480 bytes) Reassembled TCP (504 bytes) De-chunked entity body (504 bytes) Uncompressed entity body (504 bytes)

Ethernet (eth), 14 bytes

Packets: 905 - Displayed: 117 (12.9%) - Dropped: 0 (0.0%) Profile: Default

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 protocol 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

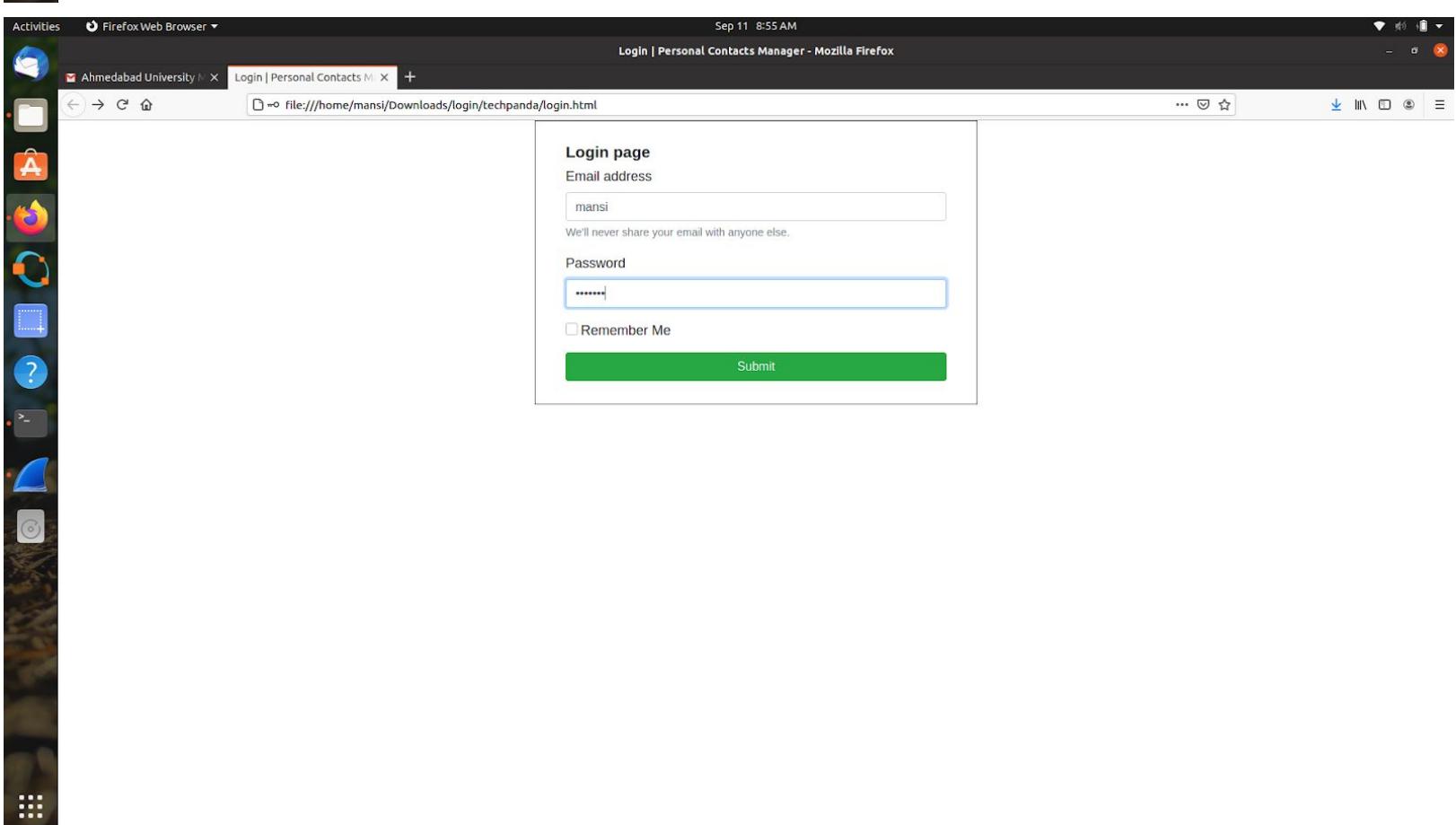
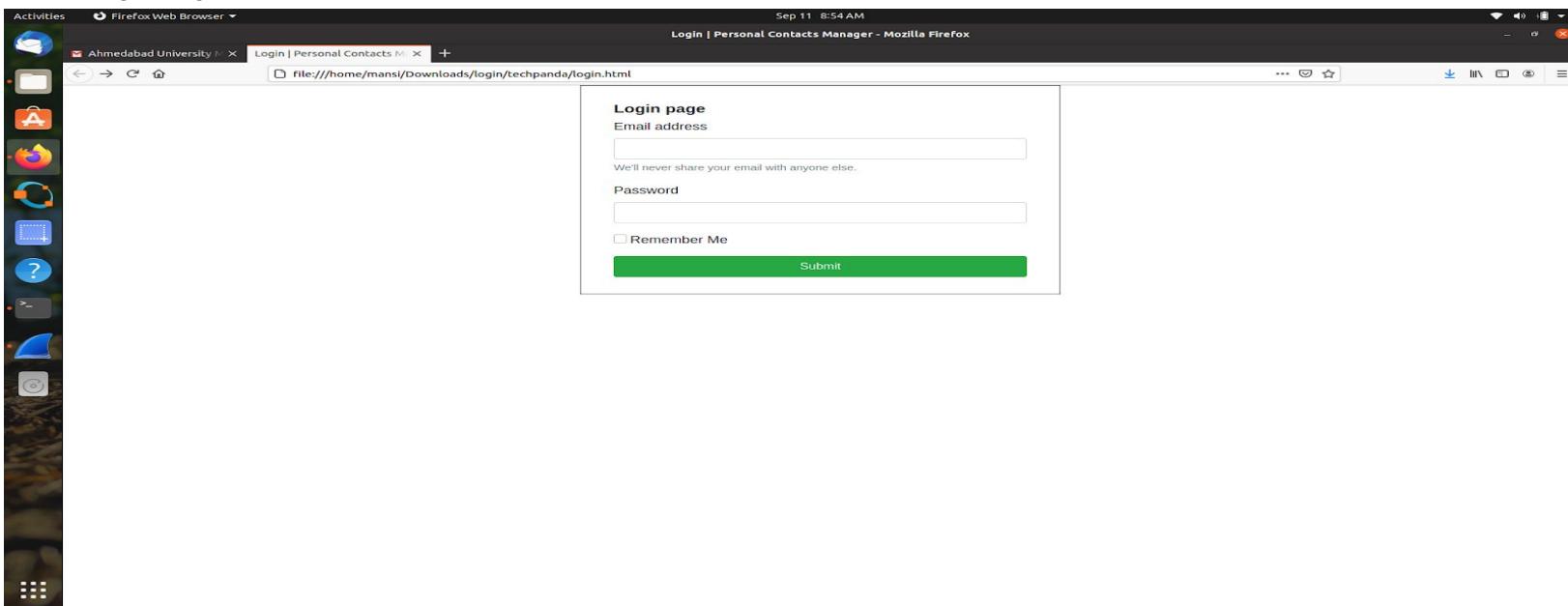
2.3

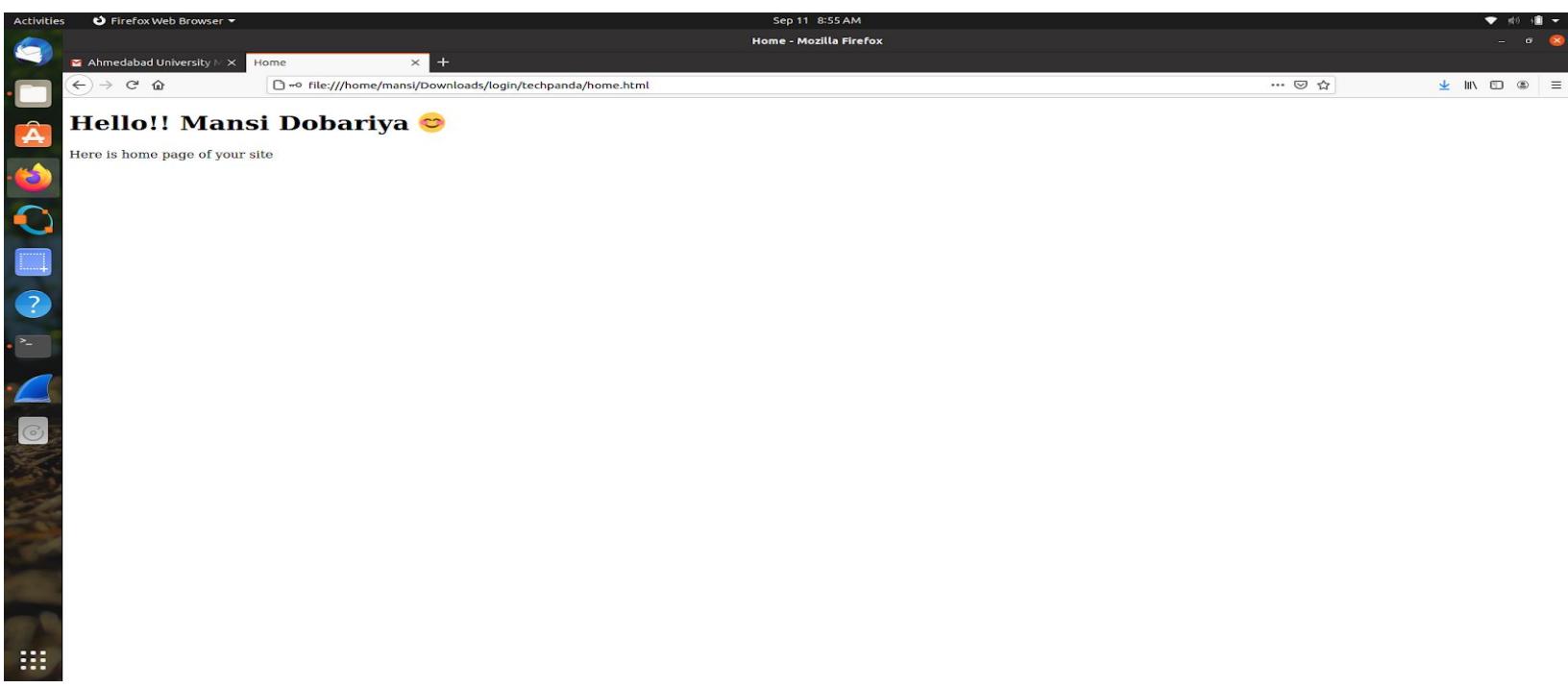
Size of Content[payload,data] = 619 bytes

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

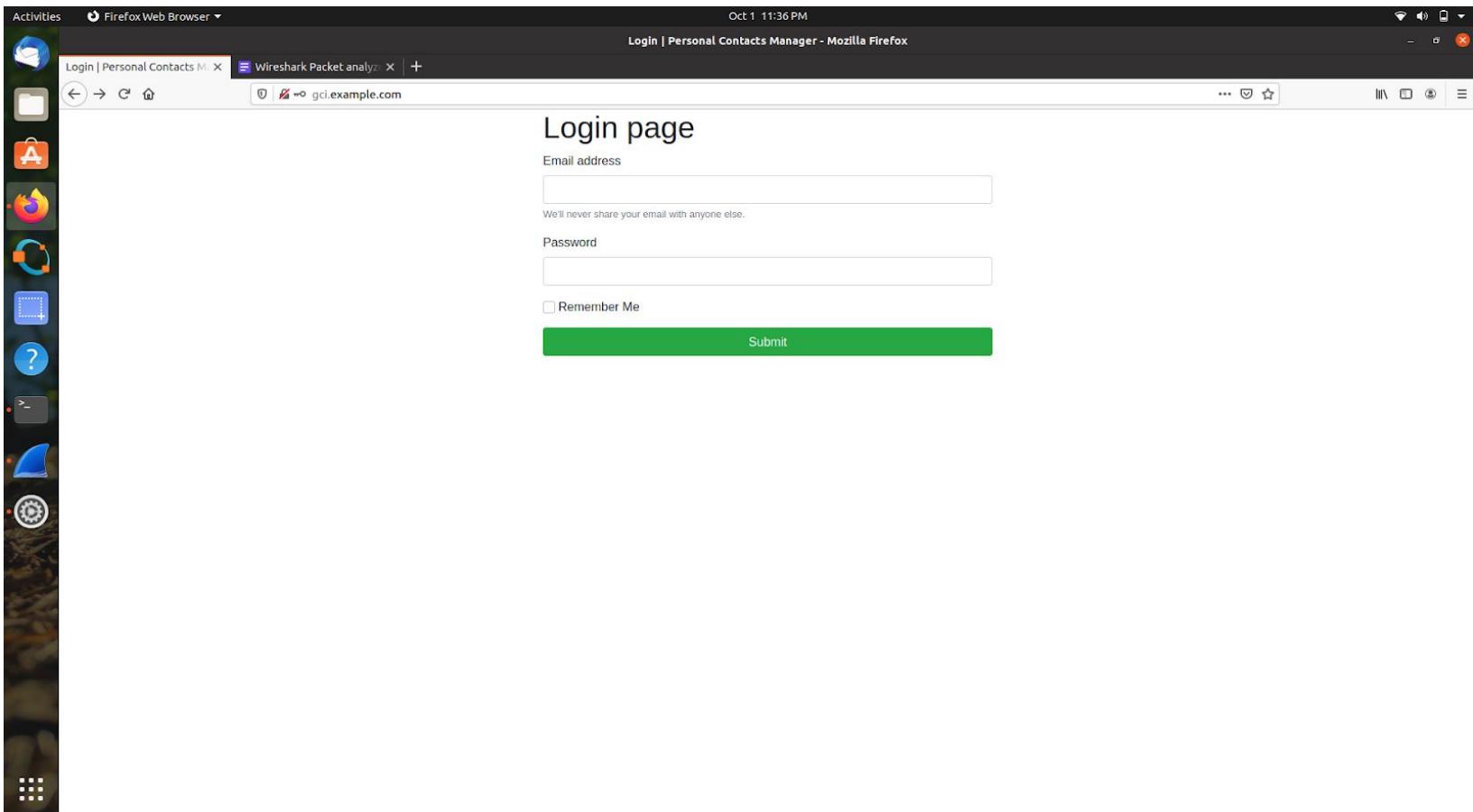
3.

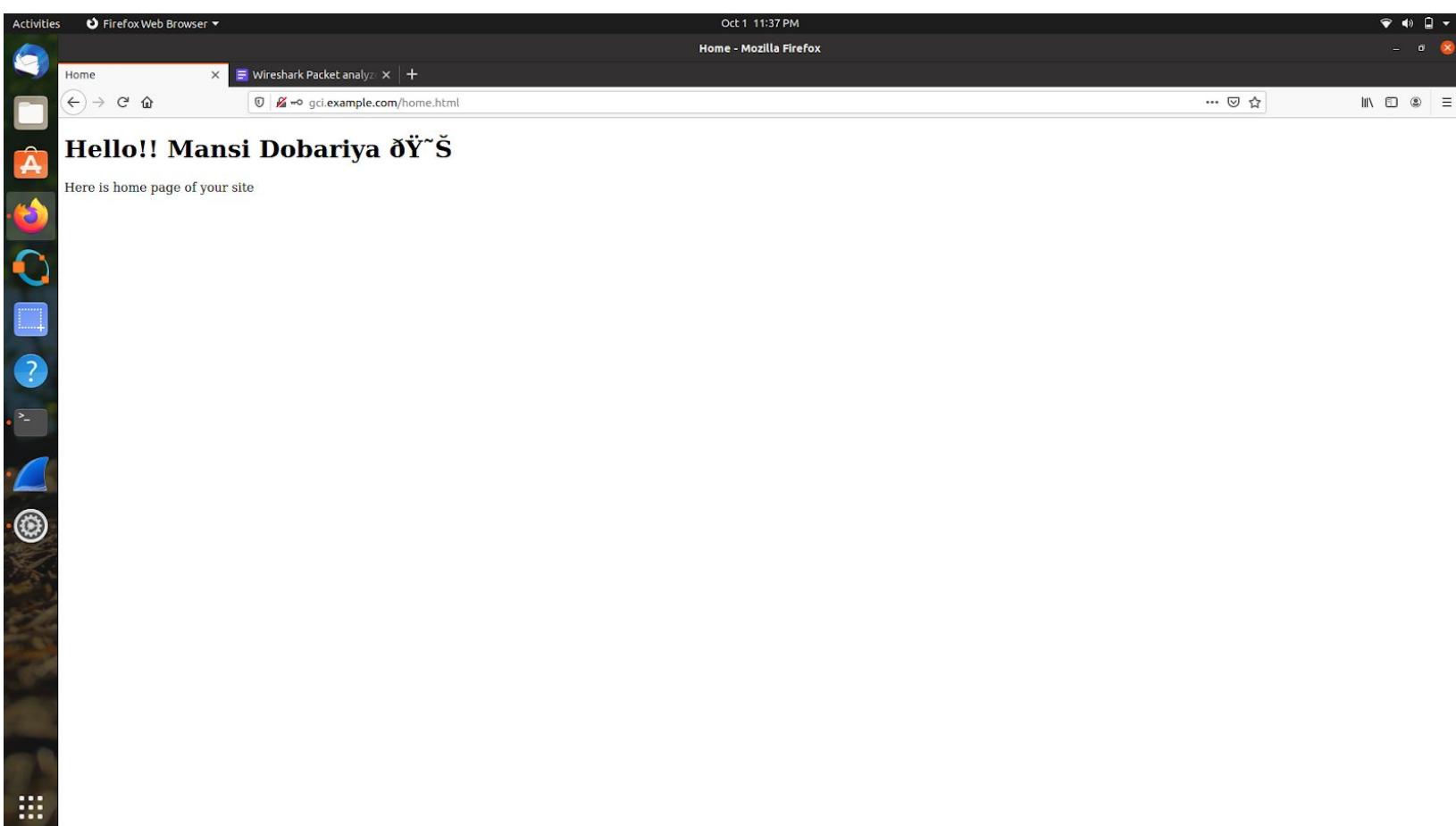
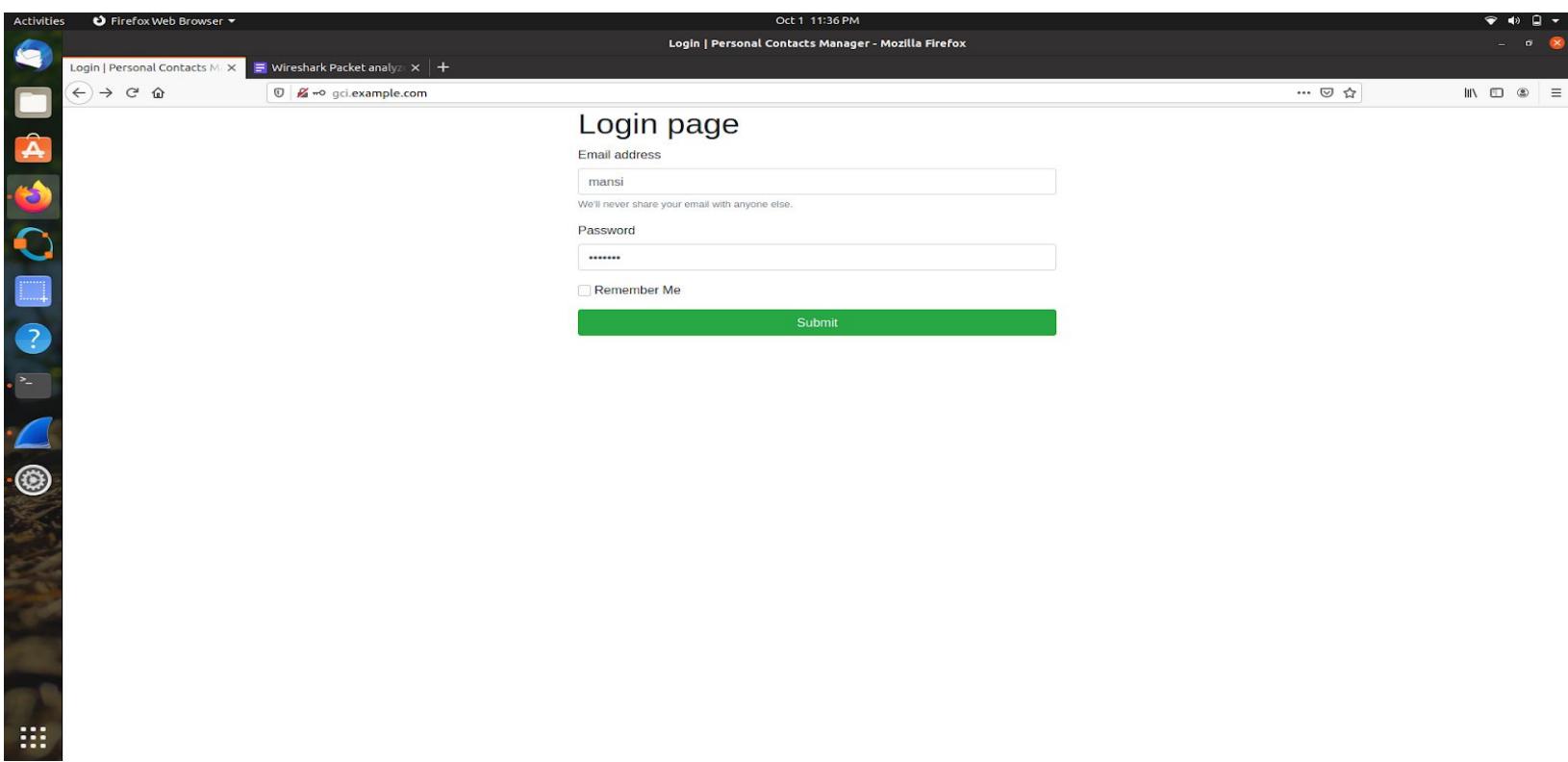
HTML pages:login and home





Password Username Sniffing





Activities Wireshark ▾ Oct 1 11:37 PM

Capturing from Loopback: lo

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http.request.method==POST

No.	Time	Source	Destination	Protocol	Length	Info
40	2020-10-01 23:36:57.152408826	127.0.0.1	127.0.0.1	HTTP	568	568 POST /home.html HTTP/1.1 (application/x-www-form-urlencoded)
42	2020-10-01 23:36:57.153532667	127.0.0.1	127.0.0.1	HTTP	558	558 HTTP/1.1 200 OK (text/html)
44	2020-10-01 23:36:57.196848219	127.0.0.1	127.0.0.1	HTTP	364	364 GET /favicon.ico HTTP/1.1
47	2020-10-01 23:36:57.197075461	127.0.0.1	127.0.0.1	HTTP	559	559 HTTP/1.1 404 Not Found (text/html)

Frame 40: 568 bytes on wire (4544 bits), 568 bytes captured (4544 bits) on interface lo, id 0

Ethernet II, Src: 00:00:00:00:00:00 (00:00:00:00:00:00), Dst: 00:00:00:00:00:00 (00:00:00:00:00:00)

Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1

Transmission Control Protocol, Src Port: 33154, Dst Port: 80, Seq: 1, Ack: 1, Len: 562

Hypertext Transfer Protocol

HTML Form URL Encoded: application/x-www-form-urlencoded

- Form item: "user" = "mansi"
- Form item: "pass" = "drashti"

```
0040 38 e5 50 4f 53 54 20 2f 68 6f 6d 65 2e 68 74 60 8 POST / home.htm
0041 3c 20 48 54 54 58 2f 31 2e 31 0d 0a 49 6f 73 74 1 HTTP/1.1 Host
0042 3a 20 67 63 69 26 65 78 61 60 78 6c 26 63 6f : gci.ex ample.co
0043 3d 9d 08 55 73 65 72 20 41 67 74 74 3a 29 4d : User Agent
0044 3a 20 67 63 69 26 65 78 61 60 78 6c 26 63 6f Mozilla/5.0 (X11/
0045 30 55 62 75 6e 74 75 3b 28 4c 69 66 75 78 26 78 Ubuntu; Linux X
0046 3a 28 36 5f 36 34 3b 26 72 78 3a 38 31 2e 38 29 20 86 64; r: v:81.0)
0047 37 65 63 6b 6f 2f 32 39 31 39 39 31 30 31 20 46 Gecko/20 100101 F
```

Packets: 52 · Displayed: 4 (7.7%) Profile: Default

Another website:

www.techpanda.org

Login | Personal Contacts Manager v1.0

Email*

Password*

Remember me

Submit

ID	First Name	Last Name	Mobile No	Email	Actions
1	myhams	jenefry	9898989898	admin@gmail.com	Edit
1	Mosa is a pussy	test	test	test@gmail.com	Edit
22531	Dark	phuc	213123123	sadasdasdsad@ftp.edu.vn	Edit
22532	Dark	dflgkldfg	45	asdas@gmail.com	Edit
22533	Dark	Maiden	87635444242	darkmaiden@octopus.ps	Edit
22534	dkddwqqdwa	avkvodzfv	38792	admin@google.com	Edit
22535	Dark	Maiden	87635444242	darkmaiden@octopus.ps	Edit
22536	Dark	Maiden	8763444242	darkmaiden@octopus.ps	Edit
22537	df	fsf	243	yadfsdf@gmail.com	Edit
22538	Dark	ee	e	ei@gmail.com	Edit
22539	Dark	ee	e	ei@gmail.com	Edit
22540	Dark	ee	e	ei@gmail.com	Edit
22541	Dark	Maiden	87635444242	darkmaiden@octopus.ps	Edit
22542	Some	Anonymous	6523987412	person@was.here	Edit
22543		Maiden	87635444242	darkmaiden@octopus.ps	Edit
22544	asd				

The screenshot shows the Wireshark interface with the following details:

- Activities**: Shows "Wireshark" as the active application.
- File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help**: The menu bar.
- *wlo1**: The selected network interface.
- http.request.method==POST**: A search filter applied to the packet list.
- Packets: 25329 - Displayed: 5 (0.0%) - Dropped: 0 (0.0%) Profile: Default**: Status bar at the bottom.

Packet List View (Selected Row):

No.	Time	Source	Destination	Protocol	Length	Info
+ 15437	2020-09-27 21:59:31.671354746	172.28.10.6	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	172.28.10.6	117.18.237.29	OCSP	445	Request
29951	2020-09-27 21:59:51.491631557	172.28.10.6	117.18.237.29	OCSP	445	Request
21539	2020-09-27 21:59:52.998326516	172.28.10.6	192.124.249.23	OCSP	436	Request
22564	2020-09-27 21:59:56.688428808	172.28.10.6	117.18.237.29	OCSP	445	Request

Details View (Selected Row):

- Frame 15437: 643 bytes on wire (5144 bits), 643 bytes captured (5144 bits) on interface wlo1, id 9
- Ethernet II, Src: IntelCor_94:ee:60 (fc:5f:87:04:ee:60), Dst: b2:38:b5:98:f5:64 (b2:38:b5:98:f5:64)
- Internet Protocol Version 4, Src: 172.28.10.6, Dst: 64.91.242.213
- Transmission Control Protocol, Src Port: 38908, Dst Port: 80, Seq: 1, Ack: 1, Len: 577
- HyperText Transfer Protocol

Http Headers:

- HTML Form URL Encoded: application/x-www-form-urlencoded
 - Form item: "email" = "admin@google.com"
 - Form item: "password" = "Password2010"

Hex View (Selected Row):

0040	15 26 50 47 53 54 29 2f 69 6e 64 65 78 2e 70 69	8POST / index.php
0050	70 28 48 54 54 59 2f 31 28 31 0d 0a 48 6f 73 74	b HTTP/1.1 -Host:
0060	5a 26 77 77 77 26 74 65 63 68 70 61 6e 64 61 26	: www.te chpanda.
0070	5f 72 67 0d 0a 55 73 65 72 2d 41 67 65 6e 74 38	org :Use r-Agent:
0080	29 4d 6f 7a 69 6c 6c 61 2f 35 7e 39 26 28 58 31	Mozilla /5.0 (X1
0090	31 3b 28 55 67 75 66 74 75 30 29 4c 69 6e 75 78	i; Ubuntu 16.04.3 X
00a0	64 69 6e 36 47 74 39 35 72 30 31 39 30 31 39 31	x86_64 AppleWebKit/537.36 (
00b0	29 28 47 62 63 6b 6f 2f 32 30 31 39 30 31 39 31) Gecko/20100101

Selected Row Description: Hypertext Transfer Protocol (http), 531 bytes

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 1
```

```
data = [0d 0a]
```

5.

The screenshot shows a Wireshark capture session titled "Capturing From wlo1". The packet list pane displays over 1000 captured packets, mostly ICMP TTL-exceeded messages. The details pane shows the structure of one such message, and the bytes pane shows the raw hex and ASCII data. The status bar at the bottom indicates the session started at Sep 11 4:23 PM.

Selected packet details:

- No. 17200-09-11 16:21:33.993772426
- Time 172.20.10.6 → 108.174.10.10
- Protocol UDP
- Length 74 bytes on wire (596 bits), 70 bytes captured (560 bits) on interface wlo1, id 0
- ICMPv4 Time-to-live exceeded (Time to live exceeded in transit)

Selected bytes details:

- 0000 5f 07 04 b6 b2 35 b5 b8 f5 f4 68 09 45 b6 ↪ g - i 5 d - e ↪
- 0010 00 30 f4 00 00 00 00 01 00 00 01 ac 14 ↪ BL+0x0000000000000000 ↪ E - ... ↪
- 0020 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ↪ E - ... ↪
- 0030 00 00 01 11 45 1e ac 14 0a 06 0c ae 0a 97 a6 ↪ E - ... ↪
- 0040 82 9a 00 28 c3 85 ↪ E - ... ↪

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

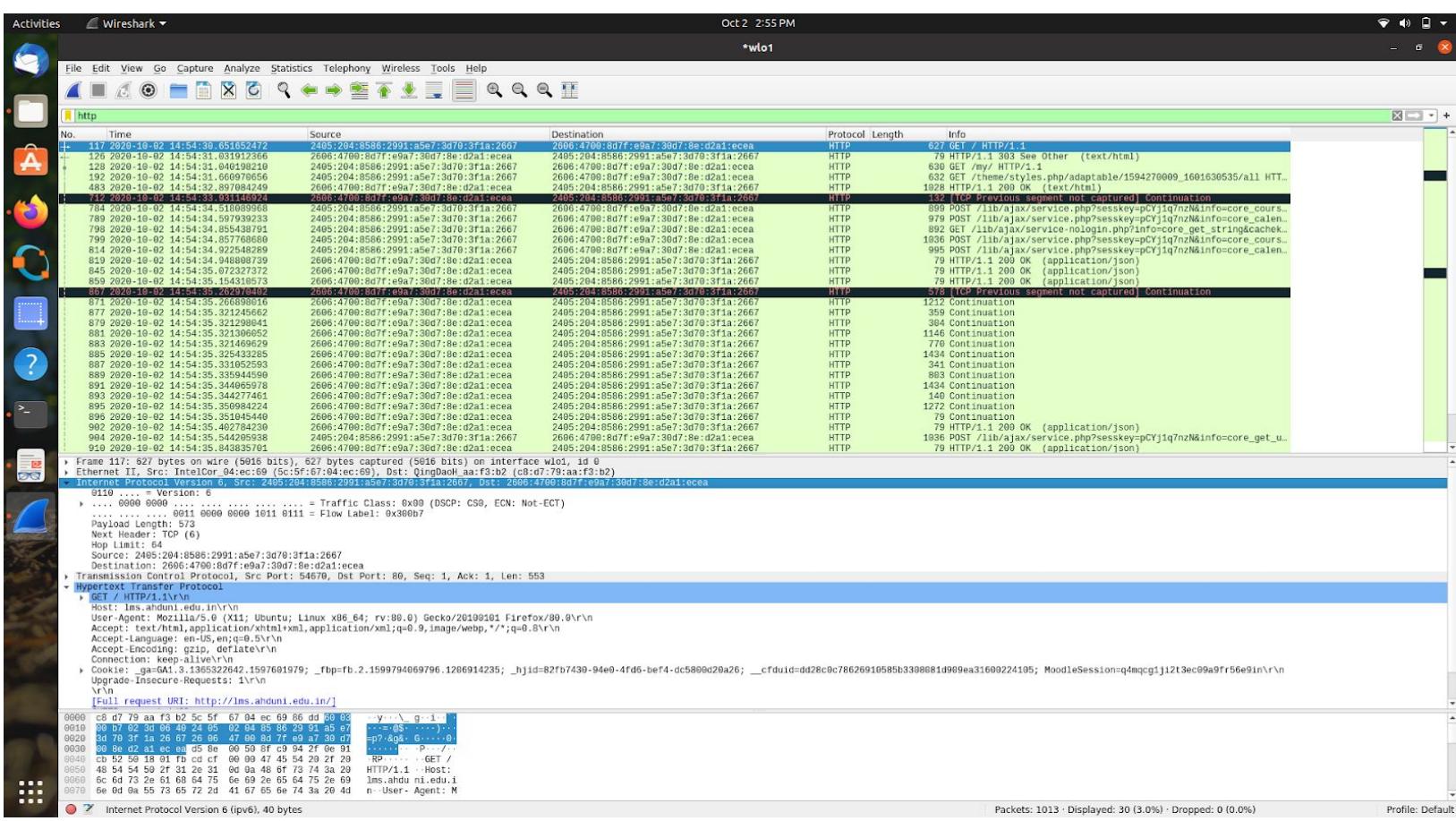
5.4 Yes , This IP datagram has been fragmented because of header length , flag ,TTL , source ip , destination ip address ,
checksum,offset ,time to live ,explicit congestion notification and payload .

Using TCPDUMP Utility

1.

```
Oct 2 2:56 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 port 80
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on wlo1, link-type EN10MB (Ethernet), capture size 262144 bytes
14:54:29.242367 IP6 mansi-HP-Pavilion-Laptop-15-cc1xx.54670 > 2606:4700:8d7f:e9a7:30d7:8e:d2a1:ecea.http: Flags [S], seq 2412352558, win 64800, options [mss 1440,sackOK,TS val 2519544309 ecr 0,nop,wscale 7], length 0
14:54:29.317814 IP6 mansi-HP-Pavilion-Laptop-15-cc1xx.54670 > 2606:4700:8d7f:e9a7:30d7:8e:d2a1:ecea.http: Flags [S.], seq 244435793, ack 2412352559, win 65535, options [mss 1360,nop,nop,sackOK,nop,wscale 10], length 0
14:54:29.317850 IP6 mansi-HP-Pavilion-Laptop-15-cc1xx.54670 > 2606:4700:8d7f:e9a7:30d7:8e:d2a1:ecea.http: Flags [.], ack 1, win 507, length 0
14:54:30.651652 IP6 mansi-HP-Pavilion-Laptop-15-cc1xx.54670 > 2606:4700:8d7f:e9a7:30d7:8e:d2a1:ecea.http: Flags [P.], seq 1:554, ack 1, win 507, length 553: HTTP: GET / HTTP/1.1
14:54:30.652223 IP6 mansi-HP-Pavilion-Laptop-15-cc1xx.54674 > 2606:4700:8d7f:e9a7:30d7:8e:d2a1:ecea.http: Flags [S.], seq 32246521, win 64800, options [mss 1440,sackOK,TS val 2519545719 ecr 0,nop,wscale 7], length 0
14:54:30.756252 IP6 2606:4700:8d7f:e9a7:30d7:8e:d2a1:ecea.http > mansi-HP-Pavilion-Laptop-15-cc1xx.54674: Flags [S.], seq 2631170134, ack 32246522, win 65535, options [mss 1360,nop,nop,sackOK,nop,wscale 10], length 0
14:54:30.756335 IP6 mansi-HP-Pavilion-Laptop-15-cc1xx.54674 > 2606:4700:8d7f:e9a7:30d7:8e:d2a1:ecea.http: Flags [.], ack 1, win 507, length 0
14:54:30.772967 IP6 2606:4700:8d7f:e9a7:30d7:8e:d2a1:ecea.http > mansi-HP-Pavilion-Laptop-15-cc1xx.54670: Flags [.], ack 554, win 66, length 0
14:54:31.031787 IP6 2606:4700:8d7f:e9a7:30d7:8e:d2a1:ecea.http > mansi-HP-Pavilion-Laptop-15-cc1xx.54670: Flags [P.], seq 1:102, ack 554, win 66, length 1101: HTTP: GET / HTTP/1.1 303 See Other
14:54:31.031860 IP6 mansi-HP-Pavilion-Laptop-15-cc1xx.54670 > 2606:4700:8d7f:e9a7:30d7:8e:d2a1:ecea.http: Flags [.], ack 1102, win 499, length 0
14:54:31.031912 IP6 2606:4700:8d7f:e9a7:30d7:8e:d2a1:ecea.http > mansi-HP-Pavilion-Laptop-15-cc1xx.54670: Flags [P.], seq 1102:1107, ack 554, win 66, length 5: HTTP
14:54:31.031924 IP6 mansi-HP-Pavilion-Laptop-15-cc1xx.54670 > 2606:4700:8d7f:e9a7:30d7:8e:d2a1:ecea.http: Flags [.], ack 1107, win 499, length 0
14:54:31.040198 IP6 mansi-HP-Pavilion-Laptop-15-cc1xx.54670 > 2606:4700:8d7f:e9a7:30d7:8e:d2a1:ecea.http: Flags [P.], seq 554:1100, ack 1107, win 501, length 556: HTTP: GET /my/ HTTP/1.1
14:54:31.050377 IP6 2606:4700:8d7f:e9a7:30d7:8e:d2a1:ecea.http > mansi-HP-Pavilion-Laptop-15-cc1xx.54670: Flags [P.], seq 1102:1107, ack 554, win 66, length 5: HTTP
14:54:31.0508450 IP6 mansi-HP-Pavilion-Laptop-15-cc1xx.54670 > 2606:4700:8d7f:e9a7:30d7:8e:d2a1:ecea.http: Flags [.], ack 1107, win 501, options [nop,nop,sack 1 {1102:1107}], length 0
14:54:31.112931 IP6 2606:4700:8d7f:e9a7:30d7:8e:d2a1:ecea.http > mansi-HP-Pavilion-Laptop-15-cc1xx.54670: Flags [.], ack 1110, win 67, length 0
14:54:31.439780 IP6 2606:4700:8d7f:e9a7:30d7:8e:d2a1:ecea.http > mansi-HP-Pavilion-Laptop-15-cc1xx.54670: Flags [.], seq 1107:2467, ack 1110, win 67, length 1360: HTTP: HTTP/1.1 200 OK
14:54:31.439895 IP6 mansi-HP-Pavilion-Laptop-15-cc1xx.54670 > 2606:4700:8d7f:e9a7:30d7:8e:d2a1:ecea.http: Flags [.], ack 2467, win 493, length 0
14:54:31.442757 IP6 2606:4700:8d7f:e9a7:30d7:8e:d2a1:ecea.http > mansi-HP-Pavilion-Laptop-15-cc1xx.54670: Flags [.], seq 2467:5187, ack 1118, win 67, length 2720: HTTP
14:54:31.442808 IP6 mansi-HP-Pavilion-Laptop-15-cc1xx.54670 > 2606:4700:8d7f:e9a7:30d7:8e:d2a1:ecea.http: Flags [.], ack 5187, win 477, length 0
14:54:31.446024 IP6 2606:4700:8d7f:e9a7:30d7:8e:d2a1:ecea.http > mansi-HP-Pavilion-Laptop-15-cc1xx.54670: Flags [.], seq 5187:5907, ack 1118, win 67, length 2720: HTTP
14:54:31.446085 IP6 mansi-HP-Pavilion-Laptop-15-cc1xx.54670 > 2606:4700:8d7f:e9a7:30d7:8e:d2a1:ecea.http: Flags [.], ack 7907, win 477, length 0
14:54:31.449900 IP6 2606:4700:8d7f:e9a7:30d7:8e:d2a1:ecea.http > mansi-HP-Pavilion-Laptop-15-cc1xx.54670: Flags [.], seq 7907:9267, ack 1116, win 67, length 1360: HTTP
14:54:31.449938 IP6 mansi-HP-Pavilion-Laptop-15-cc1xx.54670 > 2606:4700:8d7f:e9a7:30d7:8e:d2a1:ecea.http: Flags [.], ack 9267, win 493, length 0
14:54:31.453469 IP6 2606:4700:8d7f:e9a7:30d7:8e:d2a1:ecea.http > mansi-HP-Pavilion-Laptop-15-cc1xx.54670: Flags [.], seq 9267:10627, ack 1110, win 67, length 1360: HTTP
14:54:31.453524 IP6 mansi-HP-Pavilion-Laptop-15-cc1xx.54670 > 2606:4700:8d7f:e9a7:30d7:8e:d2a1:ecea.http: Flags [.], ack 10627, win 493, length 0
14:54:31.458631 IP6 2606:4700:8d7f:e9a7:30d7:8e:d2a1:ecea.http > mansi-HP-Pavilion-Laptop-15-cc1xx.54670: Flags [.], seq 10627:13347, ack 1110, win 67, length 2720: HTTP
14:54:31.458692 IP6 mansi-HP-Pavilion-Laptop-15-cc1xx.54670 > 2606:4700:8d7f:e9a7:30d7:8e:d2a1:ecea.http: Flags [.], ack 13347, win 477, length 0
14:54:31.462629 IP6 2606:4700:8d7f:e9a7:30d7:8e:d2a1:ecea.http > mansi-HP-Pavilion-Laptop-15-cc1xx.54670: Flags [P.], seq 13347:15530, ack 1110, win 67, length 2183: HTTP
14:54:31.462688 IP6 mansi-HP-Pavilion-Laptop-15-cc1xx.54670 > 2606:4700:8d7f:e9a7:30d7:8e:d2a1:ecea.http: Flags [.], ack 15530, win 477, length 0
14:54:31.473017 IP6 2606:4700:8d7f:e9a7:30d7:8e:d2a1:ecea.http > mansi-HP-Pavilion-Laptop-15-cc1xx.54670: Flags [.], seq 15530:16890, ack 1110, win 67, length 1360: HTTP
14:54:31.473061 IP6 mansi-HP-Pavilion-Laptop-15-cc1xx.54670 > 2606:4700:8d7f:e9a7:30d7:8e:d2a1:ecea.http: Flags [.], ack 16890, win 493, length 0
14:54:31.477903 IP6 2606:4700:8d7f:e9a7:30d7:8e:d2a1:ecea.http > mansi-HP-Pavilion-Laptop-15-cc1xx.54670: Flags [.], seq 16890:18250, ack 1110, win 67, length 1360: HTTP
14:54:31.477935 IP6 mansi-HP-Pavilion-Laptop-15-cc1xx.54670 > 2606:4700:8d7f:e9a7:30d7:8e:d2a1:ecea.http: Flags [.], ack 18250, win 493, length 0
14:54:31.483370 IP6 2606:4700:8d7f:e9a7:30d7:8e:d2a1:ecea.http > mansi-HP-Pavilion-Laptop-15-cc1xx.54670: Flags [.], seq 18250:19610, ack 1110, win 67, length 1360: HTTP
14:54:31.483407 IP6 mansi-HP-Pavilion-Laptop-15-cc1xx.54670 > 2606:4700:8d7f:e9a7:30d7:8e:d2a1:ecea.http: Flags [.], ack 19610, win 493, length 0
14:54:31.498122 IP6 2606:4700:8d7f:e9a7:30d7:8e:d2a1:ecea.http > mansi-HP-Pavilion-Laptop-15-cc1xx.54670: Flags [.], seq 19610:20970, ack 1110, win 67, length 1360: HTTP
14:54:31.498152 IP6 mansi-HP-Pavilion-Laptop-15-cc1xx.54670 > 2606:4700:8d7f:e9a7:30d7:8e:d2a1:ecea.http: Flags [.], ack 20970, win 493, length 0
14:54:31.502682 IP6 2606:4700:8d7f:e9a7:30d7:8e:d2a1:ecea.http > mansi-HP-Pavilion-Laptop-15-cc1xx.54670: Flags [.], seq 20970:23690, ack 1110, win 67, length 2720: HTTP
14:54:31.502704 IP6 mansi-HP-Pavilion-Laptop-15-cc1xx.54670 > 2606:4700:8d7f:e9a7:30d7:8e:d2a1:ecea.http: Flags [.], ack 23690, win 472, length 0
14:54:31.509028 IP6 2606:4700:8d7f:e9a7:30d7:8e:d2a1:ecea.http > mansi-HP-Pavilion-Laptop-15-cc1xx.54670: Flags [.], seq 23690:25058, ack 1110, win 67, length 1360: HTTP
14:54:31.509073 IP6 mansi-HP-Pavilion-Laptop-15-cc1xx.54670 > 2606:4700:8d7f:e9a7:30d7:8e:d2a1:ecea.http: Flags [.], ack 25058, win 493, length 0
14:54:31.516959 IP6 2606:4700:8d7f:e9a7:30d7:8e:d2a1:ecea.http > mansi-HP-Pavilion-Laptop-15-cc1xx.54670: Flags [.], seq 25058:26410, ack 1110, win 67, length 1360: HTTP
14:54:31.517049 IP6 mansi-HP-Pavilion-Laptop-15-cc1xx.54670 > 2606:4700:8d7f:e9a7:30d7:8e:d2a1:ecea.http: Flags [.], ack 26410, win 493, length 0
14:54:31.546026 IP6 2606:4700:8d7f:e9a7:30d7:8e:d2a1:ecea.http > mansi-HP-Pavilion-Laptop-15-cc1xx.54670: Flags [.], seq 26410:27770, ack 1110, win 67, length 1360: HTTP
14:54:31.546049 IP6 mansi-HP-Pavilion-Laptop-15-cc1xx.54670 > 2606:4700:8d7f:e9a7:30d7:8e:d2a1:ecea.http: Flags [.], ack 27770, win 493, length 0
14:54:31.551655 IP6 2606:4700:8d7f:e9a7:30d7:8e:d2a1:ecea.http > mansi-HP-Pavilion-Laptop-15-cc1xx.54670: Flags [.], seq 27770:29130, ack 1110, win 67, length 1360: HTTP
```



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.

Activities Wireshark ▾ Oct 2 3:11PM

*wlo1

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http

No.	Time	Source	Destination	Protocol	Length	Info
106	2020-10-02 15:07:25.230055976	2405:204:8586:2991:a5e7:3d70:3f1a:2667	2606:4700:8d7f:e9a7:3d07:8e:d2a1:ceea	HTTP	627	GET / HTTP/1.1.1
134	2020-10-02 15:07:25.487866205	2606:4700:8d7f:e9a7:3d07:8e:d2a1:ceea	2405:204:8586:2991:a5e7:3d70:3f1a:2667	HTTP	79	HTTP/1.1.1 303 See Other (text/html)
135	2020-10-02 15:07:25.496361899	2405:204:8586:2991:a5e7:3d70:3f1a:2667	2606:4700:8d7f:e9a7:3d07:8e:d2a1:ceea	HTTP	636	GET /my/ HTTP/1.1
199	2020-10-02 15:07:25.227046474	2606:4700:8d7f:e9a7:3d07:8e:d2a1:ceea	2405:204:8586:2991:a5e7:3d70:3f1a:2667	HTTP	1434	Continuation
202	2020-10-02 15:07:26.230785588	2606:4700:8d7f:e9a7:3d07:8e:d2a1:ceea	2405:204:8586:2991:a5e7:3d70:3f1a:2667	HTTP	1434	Continuation
204	2020-10-02 15:07:26.234495697	2606:4700:8d7f:e9a7:3d07:8e:d2a1:ceea	2405:204:8586:2991:a5e7:3d70:3f1a:2667	HTTP	1434	Continuation
218	2020-10-02 15:07:26.260188108	2405:204:8586:2991:a5e7:3d70:3f1a:2667	2606:4700:8d7f:e9a7:3d07:8e:d2a1:ceea	HTTP	632	GET /theme/styles.php/adaptable/1594270009_1601631375/all HTT...
225	2020-10-02 15:07:26.267171855	2606:4700:8d7f:e9a7:3d07:8e:d2a1:ceea	2405:204:8586:2991:a5e7:3d70:3f1a:2667	HTTP	2794	Continuation
235	2020-10-02 15:07:26.280094478	2606:4700:8d7f:e9a7:3d07:8e:d2a1:ceea	2405:204:8586:2991:a5e7:3d70:3f1a:2667	HTTP	1434	Continuation
237	2020-10-02 15:07:26.295302963	2606:4700:8d7f:e9a7:3d07:8e:d2a1:ceea	2405:204:8586:2991:a5e7:3d70:3f1a:2667	HTTP	2794	Continuation
238	2020-10-02 15:07:26.300998613	2606:4700:8d7f:e9a7:3d07:8e:d2a1:ceea	2405:204:8586:2991:a5e7:3d70:3f1a:2667	HTTP	1434	Continuation
241	2020-10-02 15:07:26.309927511	2606:4700:8d7f:e9a7:3d07:8e:d2a1:ceea	2405:204:8586:2991:a5e7:3d70:3f1a:2667	HTTP	2995	Continuation
244	2020-10-02 15:07:26.305396705	2606:4700:8d7f:e9a7:3d07:8e:d2a1:ceea	2405:204:8586:2991:a5e7:3d70:3f1a:2667	HTTP	1434	Continuation
247	2020-10-02 15:07:26.308473895	2606:4700:8d7f:e9a7:3d07:8e:d2a1:ceea	2405:204:8586:2991:a5e7:3d70:3f1a:2667	HTTP	1434	Continuation
249	2020-10-02 15:07:26.312627262	2606:4700:8d7f:e9a7:3d07:8e:d2a1:ceea	2405:204:8586:2991:a5e7:3d70:3f1a:2667	HTTP	1233	Continuation
251	2020-10-02 15:07:26.312658599	2606:4700:8d7f:e9a7:3d07:8e:d2a1:ceea	2405:204:8586:2991:a5e7:3d70:3f1a:2667	HTTP	1434	Continuation
253	2020-10-02 15:07:26.316312399	2606:4700:8d7f:e9a7:3d07:8e:d2a1:ceea	2405:204:8586:2991:a5e7:3d70:3f1a:2667	HTTP	1434	Continuation
255	2020-10-02 15:07:26.320475681	2606:4700:8d7f:e9a7:3d07:8e:d2a1:ceea	2405:204:8586:2991:a5e7:3d70:3f1a:2667	HTTP	2794	Continuation
257	2020-10-02 15:07:26.324019508	2606:4700:8d7f:e9a7:3d07:8e:d2a1:ceea	2405:204:8586:2991:a5e7:3d70:3f1a:2667	HTTP	1434	Continuation
259	2020-10-02 15:07:26.328554382	2606:4700:8d7f:e9a7:3d07:8e:d2a1:ceea	2405:204:8586:2991:a5e7:3d70:3f1a:2667	HTTP	4154	Continuation
261	2020-10-02 15:07:26.332318621	2606:4700:8d7f:e9a7:3d07:8e:d2a1:ceea	2405:204:8586:2991:a5e7:3d70:3f1a:2667	HTTP	946	Continuation
264	2020-10-02 15:07:26.332340733	2606:4700:8d7f:e9a7:3d07:8e:d2a1:ceea	2405:204:8586:2991:a5e7:3d70:3f1a:2667	HTTP	1434	Continuation
265	2020-10-02 15:07:26.335882168	2606:4700:8d7f:e9a7:3d07:8e:d2a1:ceea	2405:204:8586:2991:a5e7:3d70:3f1a:2667	HTTP	4154	Continuation
267	2020-10-02 15:07:26.336405445	2606:4700:8d7f:e9a7:3d07:8e:d2a1:ceea	2405:204:8586:2991:a5e7:3d70:3f1a:2667	HTTP	262	Continuation
269	2020-10-02 15:07:26.340146909	2606:4700:8d7f:e9a7:3d07:8e:d2a1:ceea	2405:204:8586:2991:a5e7:3d70:3f1a:2667	HTTP	1434	Continuation
271	2020-10-02 15:07:26.344192513	2606:4700:8d7f:e9a7:3d07:8e:d2a1:ceea	2405:204:8586:2991:a5e7:3d70:3f1a:2667	HTTP	2794	Continuation
273	2020-10-02 15:07:26.348354366	2606:4700:8d7f:e9a7:3d07:8e:d2a1:ceea	2405:204:8586:2991:a5e7:3d70:3f1a:2667	HTTP	2794	Continuation
275	2020-10-02 15:07:26.352210616	2606:4700:8d7f:e9a7:3d07:8e:d2a1:ceea	2405:204:8586:2991:a5e7:3d70:3f1a:2667	HTTP	1434	Continuation
277	2020-10-02 15:07:26.353228799	2606:4700:8d7f:e9a7:3d07:8e:d2a1:ceea	2405:204:8586:2991:a5e7:3d70:3f1a:2667	HTTP	1434	Continuation
279	2020-10-02 15:07:26.356988213	2606:4700:8d7f:e9a7:3d07:8e:d2a1:ceea	2405:204:8586:2991:a5e7:3d70:3f1a:2667	HTTP	575	Continuation
0000	38 d7 79 aa f3 b2 5c 5f 67 04 ec 69 86 d6 60 0d	..y...g..g..1..				
0010	ad cd 02 3d 06 49 24 05 02 04 85 86 29 91 a5 e7	...=(S.....)				
0020	3d 70 3f 1a 26 67 26 06 47 09 8d 7f e9 a7 3d 7	-p?&g G...0				
0030	00 0e d2 a1 ec ea d5 c4 00 50 57 aa 4b 58 68 6f PW Kho				
0040	66 19 50 18 01 fb 59 eb 00 09 47 45 54 29 2f 29	f..P..Y..GET /				

Internet Protocol Version 6, Src: 2405:204:8586:2991:a5e7:3d70:3f1a:2667, Dst: 2606:4700:8d7f:e9a7:3d07:8e:d2a1:ceea

Transmission Control Protocol, Src Port: 54724, Dst Port: 80, Seq: 1, Ack: 1, Len: 553

HyperText Transfer Protocol

GET / HTTP/1.1\r\n

[Expert Info (Chat/Sequence): GET / HTTP/1.1\r\n]

[GET / HTTP/1.1\r\n]

[Severity level: Chat]

[Group: Sequence]

Request Method: GET

Request URL: /

Request Version: HTTP/1.1

Host: lms.ahduni.edu.in\r\n

User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:88.0) Gecko/20100101 Firefox/88.0\r\n

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8\r\n

Accept-Language: en-US,en;q=0.5\r\n

Accept-Encoding: gzip, deflate\r\n

Connection: keep-alive\r\n

Cookie: ga=GA1.3.1385522642.1597601979; _fbp=fb.2.1599794069796.1206914235; _hjid=82fb7439-94e0-4fd6-beff-4c5800d20a26; __cfduid=dd28c0c78626910585b3398081d909ea31600224105; MoodleSession=q4mqcgij12t3ec09a9fr56e9in\r\n

Upgrade-Insecure-Requests: 1\r\n

\r\n

[Full request URI: http://lms.ahduni.edu.in/]

[HTTP request 1/2]

[Response in frame: 134]

[Next request in frame: 136]

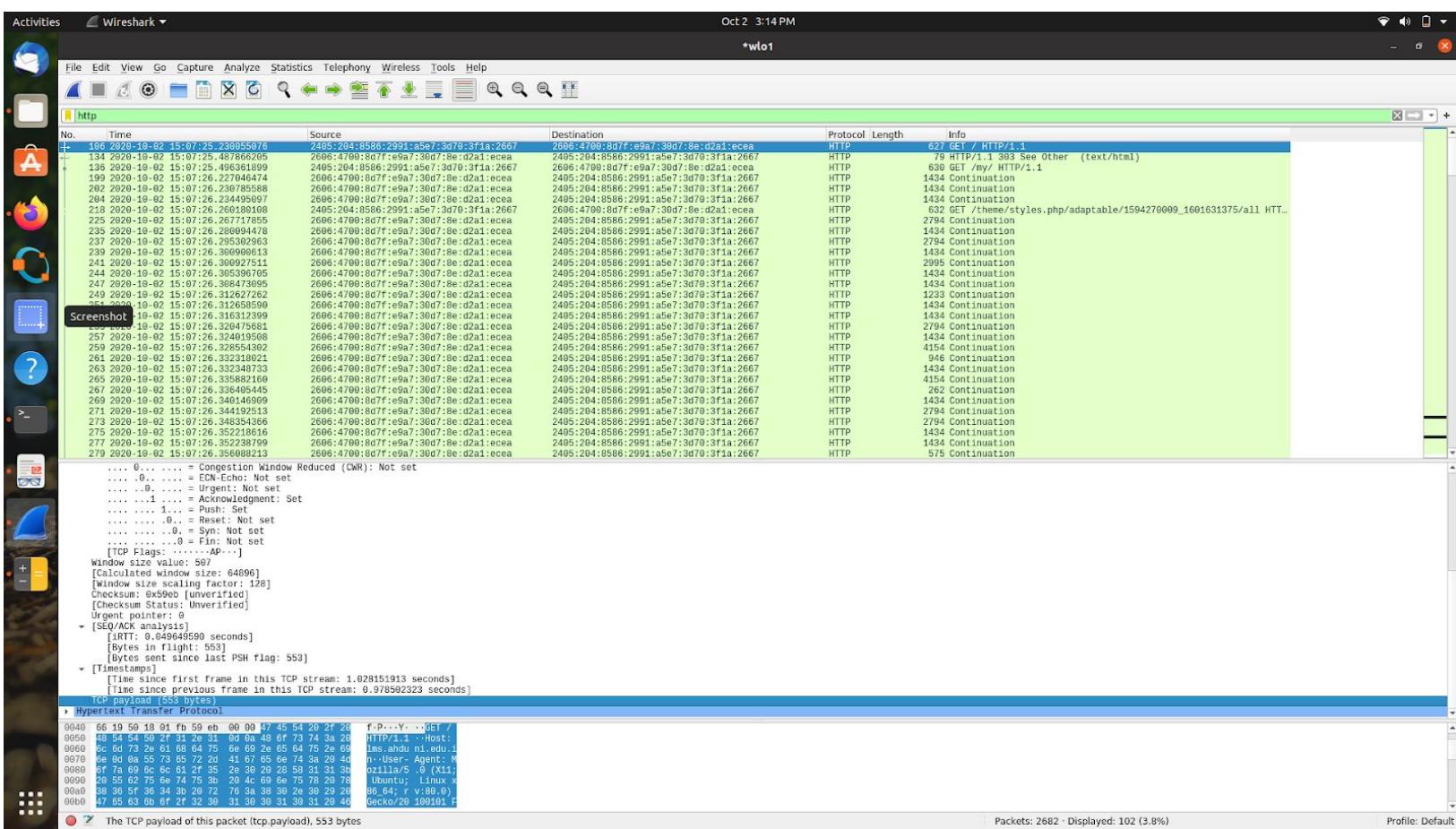
2.1

HTTP version 1.1

2.2

Transmission Control Protocol stream has port address of source and destination ,segment length as tcp is network layer protocol
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: ~
mansi@mansi-HP-Pavilion-Laptop-15-cc1xx: ~ sudo tcptrace -l wlo1 icmp
tcptrace: 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
15:35:09.470348 IP 192.168.21.190 > mansi-HP-Pavilion-Laptop-15-cc1xx: ICMP time exceeded in-transit, length 36
15:35:09.470525 IP 172.26.100.246 > mansi-HP-Pavilion-Laptop-15-cc1xx: ICMP time exceeded in-transit, length 36
15:35:09.470528 IP 192.168.38.23 > mansi-HP-Pavilion-Laptop-15-cc1xx: ICMP time exceeded in-transit, length 36
15:35:09.470545 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 36
15:35:09.910423 IP 192.168.38.29 > mansi-HP-Pavilion-Laptop-15-cc1xx: ICMP time exceeded in-transit, length 76
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, length 148
mansi@mansi-HP-Pavilion-Laptop-15-cc1xx: ~ traceroute to 108.174.10.10 (108.174.10.10), 30 hops max, 68 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)
4 192.168.21.190 (192.168.21.190) 871.225 ms 875.063 ms 879.513 ms
5 172.26.100.247 (172.26.100.247) 867.601 ms 870.653 ms 878.177 ms
6 172.26.100.247 (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
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
9 192.168.38.28 (192.168.38.28) 448.076 ms
10 192.168.38.28 (192.168.38.28) 448.076 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)
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)
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 49.45.4.85 (49.45.4.85)
16 172.16.25.2 (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)
17 192.168.38.23 (192.168.38.23) 312.354 ms
18 192.168.38.23 (192.168.38.23) 312.354 ms
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 15:35:08.701308	192.168.1.1	192.168.1.102	ICMP	68	102 Time-to-live exceeded (Time to live exceeded in transit)
3853	2020-10-02 15:35:08.701321	192.168.1.1	192.168.1.102	ICMP	68	102 Time-to-live exceeded (Time to live exceeded in transit)
3854	2020-10-02 15:35:08.701371	192.168.1.1	192.168.1.102	ICMP	68	102 Time-to-live exceeded (Time to live exceeded in transit)
4049	2020-10-02 15:35:09.457007	192.168.1.102	10.71.48.98	ICMP	68	78 Time-to-live exceeded (Time to live exceeded in transit)
4050	2020-10-02 15:35:09.458448	192.168.1.102	172.26.101.7	ICMP	68	78 Time-to-live exceeded (Time to live exceeded in transit)
4060	2020-10-02 15:35:09.461081	192.168.1.102	172.26.101.7	ICMP	68	78 Time-to-live exceeded (Time to live exceeded in transit)
4061	2020-10-02 15:35:09.461544	192.168.1.102	172.26.101.7	ICMP	68	78 Time-to-live exceeded (Time to live exceeded in transit)
4062	2020-10-02 15:35:09.462035	192.168.1.102	192.168.21.190	ICMP	68	78 Time-to-live exceeded (Time to live exceeded in transit)
4063	2020-10-02 15:35:09.465624	192.168.1.102	192.168.21.190	ICMP	68	78 Time-to-live exceeded (Time to live exceeded in transit)
4071	2020-10-02 15:35:09.465987	192.168.1.102	10.71.48.98	ICMP	68	78 Time-to-live exceeded (Time to live exceeded in transit)
4073	2020-10-02 15:35:09.466486	192.168.1.102	192.168.21.190	ICMP	68	78 Time-to-live exceeded (Time to live exceeded in transit)
4076	2020-10-02 15:35:09.469298	192.168.1.102	172.26.100.247	ICMP	68	78 Time-to-live exceeded (Time to live exceeded in transit)
4080	2020-10-02 15:35:09.470348	192.168.1.102	192.168.21.190	ICMP	68	78 Time-to-live exceeded (Time to live exceeded in transit)
4131	2020-10-02 15:35:09.470525	192.168.1.102	192.168.1.102	ICMP	68	78 Time-to-live exceeded (Time to live exceeded in transit)
4141	2020-10-02 15:35:09.470528	192.168.1.102	192.168.1.102	ICMP	68	78 Time-to-live exceeded (Time to live exceeded in transit)
4153	2020-10-02 15:35:09.466245	192.168.1.102	172.26.100.247	ICMP	68	78 Time-to-live exceeded (Time to live exceeded in transit)
4216	2020-10-02 15:35:09.910333	192.168.38.28	192.168.1.102	ICMP	68	118 Time-to-live exceeded (Time to live exceeded in transit)
4217	2020-10-02 15:35:09.910388	192.168.38.28	192.168.1.102	ICMP	68	118 Time-to-live exceeded (Time to live exceeded in transit)
4218	2020-10-02 15:35:09.910401	192.168.38.27	192.168.1.102	ICMP	68	118 Time-to-live exceeded (Time to live exceeded in transit)
4219	2020-10-02 15:35:09.910424	192.168.38.24	192.168.1.102	ICMP	68	118 Time-to-live exceeded (Time to live exceeded in transit)
4220	2020-10-02 15:35:09.910444	192.168.38.24	192.168.1.102	ICMP	68	118 Time-to-live exceeded (Time to live exceeded in transit)
4221	2020-10-02 15:35:09.910444	192.168.38.24	192.168.1.102	ICMP	68	118 Time-to-live exceeded (Time to live exceeded in transit)
4222	2020-10-02 15:35:09.910444	192.168.38.24	172.16.92.145	ICMP	68	118 Time-to-live exceeded (Time to live exceeded in transit)
4223	2020-10-02 15:35:09.910455	192.168.38.24	172.26.40.5	ICMP	68	118 Time-to-live exceeded (Time to live exceeded in transit)
4224	2020-10-02 15:35:09.910466	192.168.38.24	172.16.25.2	ICMP	68	118 Time-to-live exceeded (Time to live exceeded in transit)
4231	2020-10-02 15:35:09.911253	192.168.38.24	192.168.1.102	ICMP	68	182 Time-to-live exceeded (Time to live exceeded in transit)
4239	2020-10-02 15:35:09.911304	192.168.38.24	192.168.1.102	ICMP	68	182 Time-to-live exceeded (Time to live exceeded in transit)
4241	2020-10-02 15:35:09.911315	192.168.38.24	192.168.1.102	ICMP	68	182 Time-to-live exceeded (Time to live exceeded in transit)
4250	2020-10-02 15:35:09.911358	192.168.38.24	192.168.1.102	ICMP	68	182 Time-to-live exceeded (Time to live exceeded in transit)
4251	2020-10-02 15:35:09.911358	192.168.38.24	172.16.25.2	ICMP	68	182 Time-to-live exceeded (Time to live exceeded in transit)
4252	2020-10-02 15:35:09.911358	192.168.38.24	172.16.25.2	ICMP	68	182 Time-to-live exceeded (Time to live exceeded in transit)
Frame 3852: 192 bytes on wire (144 bits), 192 bytes captured (144 bits) on interface wlo1, id 8 Ethernet II, Src: QingBoH_aa:ff:32 (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: QingBoH_aa:ff:32 (c8:d7:79:aa:f3:b2) Type: IPv4 (0x0800) Version: 4 ... 0101 = Header Length: 20 bytes (5) ... 0101 = Header Length: 20 bytes (5) Differential Services Field: 0x0 (DSCP: CS6, ECN: Not-ECT) Total Length: 88 Identification: 0x250c (9404) Flags: FFFF 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 69 c8 d7 79 aa f3 b2 00 00 45 c0 \g-i-y-E- 0010 00 58 25 00 00 40 01 d1 21 c0 a8 01 01 c0 a8 X%-@!-!-! 0020 01 68 00 00 2e 00 00 45 00 00 9c 0f bd f-.-.-<- 0030 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 Z[\\]_ 0040 82 8a 00 28 62 bd 40 41 42 43 44 45 46 47 48 49 ... (D @A BCDEFGHI 0050 4a 4b 4c 4d 4e 4f 50 51 52 53 54 55 56 57 58 59 JKLMNOPRQ 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

icmp

No.	Time	Source	Destination	Protocol	Length	Info
3852	2020-10-02 15:35:08.791308999	192.168.1.1	192.168.1.102	ICMP	102	Time-to-live exceeded (Time to live exceeded in transit)
3853	2020-10-02 15:35:08.791369321	192.168.1.1	192.168.1.102	ICMP	102	Time-to-live exceeded (Time to live exceeded in transit)
3854	2020-10-02 15:35:08.791377817	192.168.1.1	192.168.1.102	ICMP	102	Time-to-live exceeded (Time to live exceeded in transit)
4063	2020-10-02 15:35:09.461081490	10.71.48.98	192.168.1.102	ICMP	78	Time-to-live exceeded (Time to live exceeded in transit)
4064	2020-10-02 15:35:09.461081490	10.71.48.98	192.168.1.102	ICMP	101	Time-to-live exceeded (Time to live exceeded in transit)
4065	2020-10-02 15:35:09.461081490	10.71.48.98	192.168.1.102	ICMP	78	Time-to-live exceeded (Time to live exceeded in transit)
4066	2020-10-02 15:35:09.461544716	172.26.101.7	192.168.1.102	ICMP	78	Time-to-live exceeded (Time to live exceeded in transit)
4067	2020-10-02 15:35:09.461544716	172.26.101.7	192.168.1.102	ICMP	78	Time-to-live exceeded (Time to live exceeded in transit)
4068	2020-10-02 15:35:09.462635526	192.168.21.199	192.168.1.102	ICMP	78	Time-to-live exceeded (Time to live exceeded in transit)
4069	2020-10-02 15:35:09.462635526	192.168.21.199	192.168.1.102	ICMP	78	Time-to-live exceeded (Time to live exceeded in transit)
4070	2020-10-02 15:35:09.464846552	192.168.21.199	192.168.1.102	ICMP	78	Time-to-live exceeded (Time to live exceeded in transit)
4071	2020-10-02 15:35:09.464846552	192.168.21.199	192.168.1.102	ICMP	78	Time-to-live exceeded (Time to live exceeded in transit)
4072	2020-10-02 15:35:09.469298824	172.26.100.247	192.168.1.102	ICMP	78	Time-to-live exceeded (Time to live exceeded in transit)
4080	2020-10-02 15:35:09.479348947	192.168.21.199	192.168.1.102	ICMP	78	Time-to-live exceeded (Time to live exceeded in transit)
4130	2020-10-02 15:35:09.652725969	192.168.109.246	192.168.1.102	ICMP	78	Time-to-live exceeded (Time to live exceeded in transit)
4141	2020-10-02 15:35:09.652820357	192.168.38.23	192.168.1.102	ICMP	78	Time-to-live exceeded (Time to live exceeded in transit)
4142	2020-10-02 15:35:09.669345780	172.26.100.247	192.168.1.102	ICMP	78	Time-to-live exceeded (Time to live exceeded in transit)
4218	2020-10-02 15:35:09.910388469	192.168.38.28	192.168.1.102	ICMP	119	Time-to-live exceeded (Time to live exceeded in transit)
4219	2020-10-02 15:35:09.910401998	192.168.38.27	192.168.1.102	ICMP	78	Time-to-live exceeded (Time to live exceeded in transit)
4220	2020-10-02 15:35:09.910412254	192.168.38.24	192.168.1.102	ICMP	118	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	78	Time-to-live exceeded (Time to live exceeded in transit)
4221	2020-10-02 15:35:09.910433193	192.168.38.29	192.168.1.102	ICMP	118	Time-to-live exceeded (Time to live exceeded in transit)
4222	2020-10-02 15:35:09.910433193	172.16.1.145	192.168.1.102	ICMP	100	Time-to-live exceeded (Time to live exceeded in transit)
4223	2020-10-02 15:35:09.910455504	192.168.38.40	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 15:35:09.911315887	172.16.1.218	192.168.1.102	ICMP	182	Time-to-live exceeded (Time to live exceeded in transit)
4250	2020-10-02 15:35:09.965000000	172.16.1.218	192.168.1.102	ICMP	182	Time-to-live exceeded (Time to live exceeded in transit)

Frame 4898: 78 bytes on wire (609 bits), 78 bytes captured (568 bits) on interface wlo1, id 9
 Ethernet II, Src: Qingbaoh aa:f3:b2 (c8:d7:79:aa:f3:b2), Dst: IntelCor_04:ec:69 (5c:5f:67:84:ec:69)
 Source: Qingbaoh 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
 0x0000: 00 00 ... = Version: 4
 0x0001: 00 00 ... = IHL: 5 (5)
 0x0002: 00 00 ... = Differentiated Services Field: 0x28 (DSCH: AF11, ECN: Not-ECT)
 Total Length: 58
 Identification: 0x73ea (29674)
 Flags: 0x4000, Don't fragment
 Fragment offset: 0
 Time to live: 64
 Protocol: ICMP (1)
 Header checksum: 0xb782 [validation disabled]
 [Header checksum status: Unverified]
 Source: 172.26.101.7
 Destination: 192.168.1.102
 Destination port: 53
 Internet Protocol Version 4, Src: 172.26.101.7, Dst: 192.168.1.102
 0x0000: 5c 5f 67 04 ec 69 c8 d7 79 aa f3 b2 00 00 45 28 \g-i-y-E(0x0001: 00 38 73 ea 40 00 7c 01 b7 82 ac 1a 65 07 c9 a8 8s @...-e- 0x0002: 01 66 00 00 a1 43 81 c1 00 00 45 28 00 3c if 97 f-C-:E(<- 0x0003: 00 00 00 11 62 2c c0 a8 01 66 0c ae 0a ca 32 ...b,-f1---2 0x0040: 82 a6 99 28 84 f9 ...`-

wlo1: <live capture in progress>

Packets: 80988 - Displayed: 44 (0.1%) Profile: Default