TCP Reset Attack on Video Streaming

Design Report

Abdullah Al Ishtiaq
Student Id. : 1505080
Section: B Group: 6

July 29, 2019

Department of Computer Science and Engineering
Bangladesh University of Engineering and Technology (BUET)
Dhaka - 1000

Contents

1 Introduction

The Transmission Control Protocol (TCP) is a core protocol of the Internet Protocol Suite. It is one of the 2 main transport layer protocols which sit on top of the IP layer. TCP provides reliable, ordered and error-checked host-to-host communication services for applications. It is considered a stateless protocol suite because each client connection is newly made without considering whether a previous connection had been established or not.
Although TCP is widely used in major internet applications, it introduces a few vulnerabilities too. The most common of these vulnerabilities are: Denial of Service (DOS), Connection Hijacking, TCP Veto, TCP Reset attack etc.

2 TCP Reset Attack on Video Streaming

TCP reset attack does not target the protocol's typical method of closing a connection which uses a 4-way handshake method. Rather it uses the protocol's method of immediately terminating an unwanted, unexpected or erroneous connection. From the specifications of Transmission Control Protocol (TCP) given in RFC-0793 (September 1981) we quote, "Reset (RST) must be sent whenever a segment arrives which apparently is not intended for the current connection". It is an important property of TCP for ensuring robustness, but at the same time it has opened up a scope of exploitation.
In TCP reset attack on video streaming, an attacker forges a spoofed RST packet that pretends to be the one coming from the original video streaming server. As a result the victim immediately closes the TCP connection and goes to CLOSED state. In addition to that, upon receiving additional packets from the original server, the victim itself sends RST packet to the server terminating the connection at the remote end. In this way the attacker can successfully disrupt video streaming on its victim's machine.

3 Strategy

The strategy of our attack can be described in 3 steps. Those are:

1. First we need to find out the IP address of either the victim machine or the video server. There can be quite a few machines connected to the same network and as long as we do not want to disrupt TCP connection on all of them, we need to know this information in particular prior to proceeding with our tool. Otherwise a port scanning mechanism would have sufficed.

2. Then we have to sniff packets in the network to discover the other IP address, the TCP port numbers and the correct sequence number. For this purpose, the tool will require additional feature of ARP Spoofing.

3. Finally we forge a TCP packet with correct IP addresses, TCP Port numbers and sequence number and with RST bit set and send it to the victim machine.

Here one important aspect needs to be discussed. We can also perform the attack by sending forged RST packets to the video streaming server, but chances are that it will be self harmful as the server may block the attacker's IP address. So instead of doing so, we are going to send the forged packets to the victim machine.
Another important note is that we must send the packet with haste as the sequence number in the forged RST packet must be within victim's window to be effective. Otherwise it will be discarded without any impact on the connection.

4 Timing Diagrams

Timing diagrams are really important in designing an attack tool as it gives us the insight about how the protocol actually works and how an attack can exploit its various vulnerabilities. For this reason, we have closely examined the specifications of the Transmission Control Protocol provided in RFC-0793 and accordingly drawn these timing diagrams with appropriate states.

4.1 Typical Timing Diagram

In Figure 1, the timing diagram of typical communication for video streaming between the streaming server and victim is shown. At first the connection is established through a 3-way handshake. In the "ESTABLISHED" state the two parties can start exchanging messages which are represented in the figure as "ABC", "DEF", etc. The connection can finally be closed at the end of the communication by either of the parties and in both cases another 4-way handshake will occur.

4.2 Attack Timing Diagram

We will perform the TCP reset attack by sending forged RST packet from the attacker machine. The timing diagram of the attack is shown in Figure 2. In this case the victim will assume the video server has unexpectedly

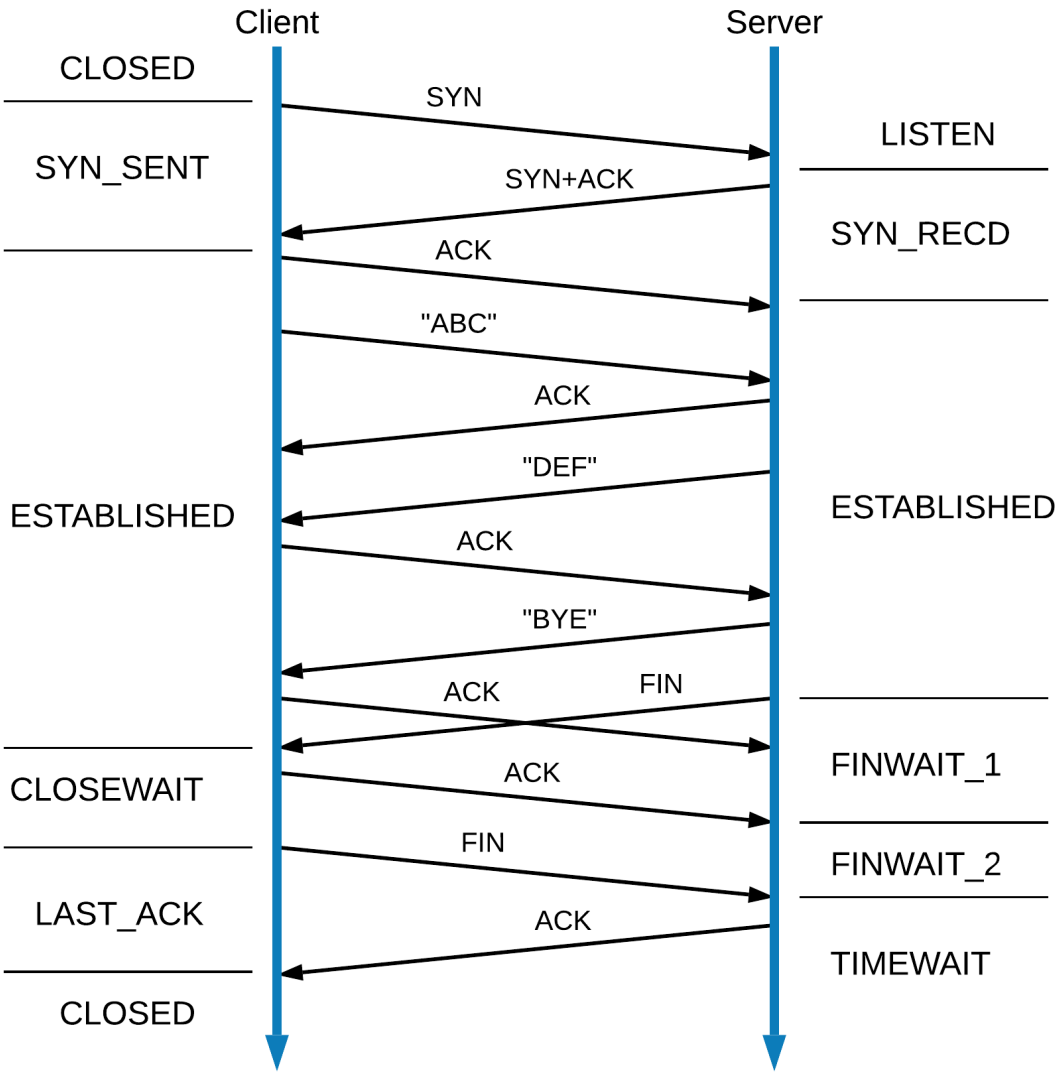

Figure 1: TCP Timing Diagram

terminated the "ESTABLISHED" TCP connection, and immediately close the connection. Upon receiving additional messages from the actual server it will send RST back and finally the server will also close the connection receiving the RST packet.

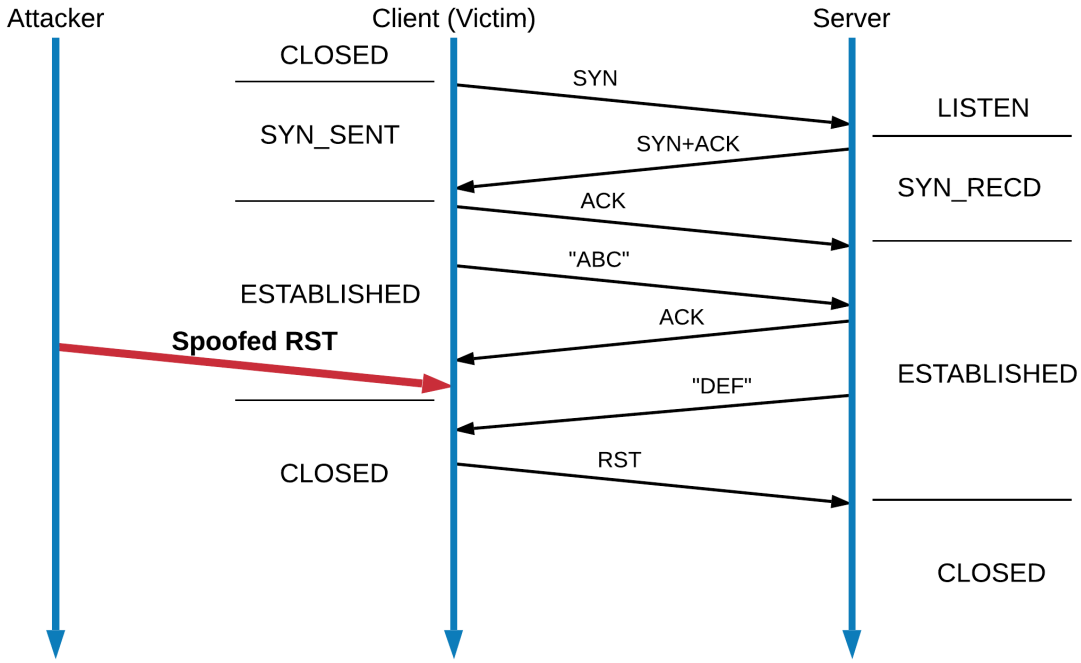

Figure 2: TCP Reset Attack Timing Diagram

5 Packet Details

In Figure 3, we show the specific fields in the TCP/IP header that need to be handled in order to perform TCP reset attack. Here source IP will be the video streaming server's IP address, Destination IP will be victim's IP address, and the port numbers will be set correspondingly. Sequence number must be correctly discovered through sniffing. Finally RST bit must be set to 1. The other fields will be changed accordingly with the help of programming language libraries. Also payload to this header is not really important in this case as it is merely an RST packet.

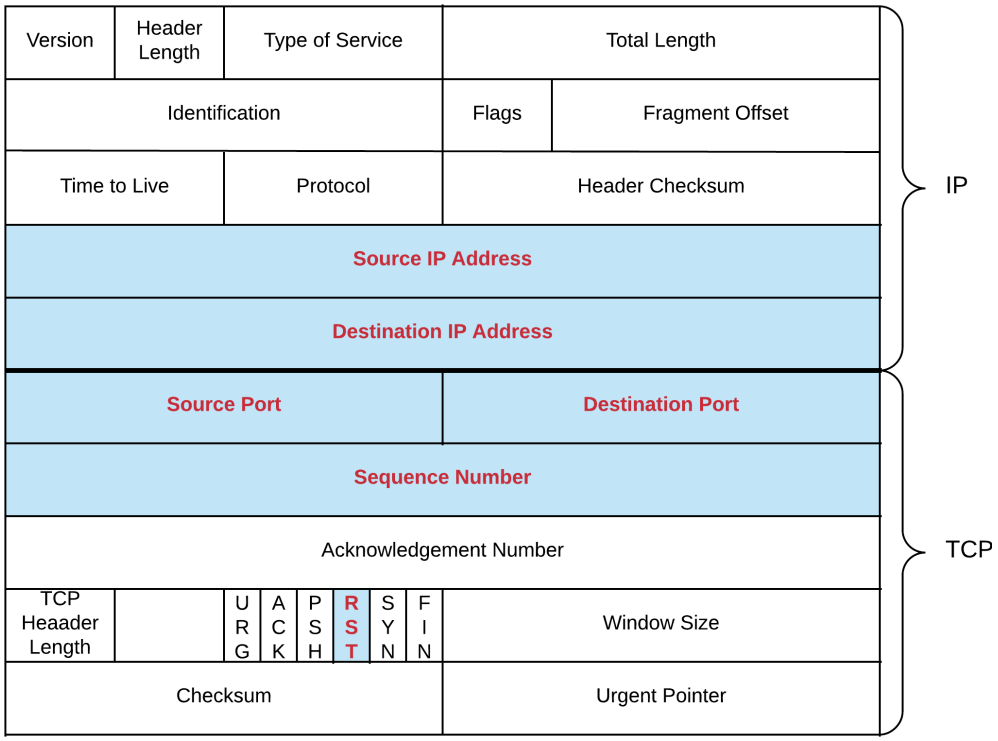

Figure 3: Attack Packet Header

6 Available Tools

There are already a few available tools for many different network attacks. Among them **Netwox** is a quite well known one. To perform TCP reset attack with Netwox from an Linux environment, the command is as follows:

```
#!/bin/bash
sudo netwox 78 --filter "src host *target's IP address*"
```

Although being readily available, there is a major drawback of this Netwox command. For working correctly, we already know from Section 3 that sequence number of the forged packet must be within the victims window. Also port numbers must be set correctly. For doing so, sniffing is a must, but it is not possible with "pcap" API for packets from other devices on the network which are connected through switch. As a result where Wireshark does not work, neither does Netwox 78 command.
Tests on Wireshark are mentioned in Section 15 where it can be seen in Figure 11 that the guest OS cannot sniff packets from the host OS. Similarly Netwox is tested in a VM environment from the guest OS where pcap API does not work attacking the host OS.
The result of the test can be seen in Figure 4 where video in the browser of the host can still load the playing video. So the attack with Netwox failed.

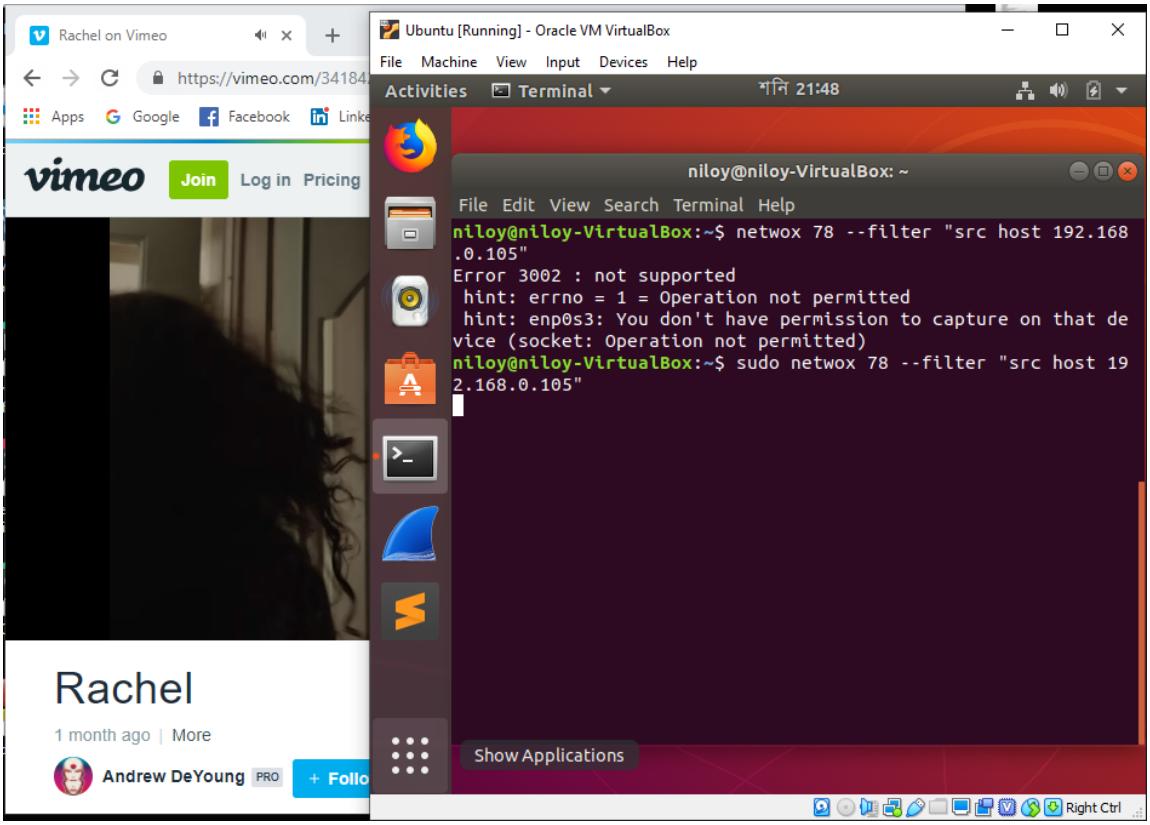

Figure 4: Netwox Test

7 Video Streaming Server

Our target is to disrupt videos from any website that uses TCP connection. For implementation purpose, we will use the website **"Vimeo.com"** as video streaming server.
Although YouTube is the most popular video streaming website, it uses UDP connection which is out of the scope of our attack tool. This choice of website is based on tests described in Section 14 where Wireshark is used to determine the transport layer protocol used by these websites.

8 Implementation Technology

Language: We are going to use **Python 3.7** for implementation purpose. One of the main reasons for choosing this language is that it has ample support for forging TCP packets and sending them to appropriate destination.

Libraries: First we need a library to sniff packets. We will use **libpcap** package for this purpose. Secondly, We will use **scapy** package for forging and sending packets. Both of these are from Python.

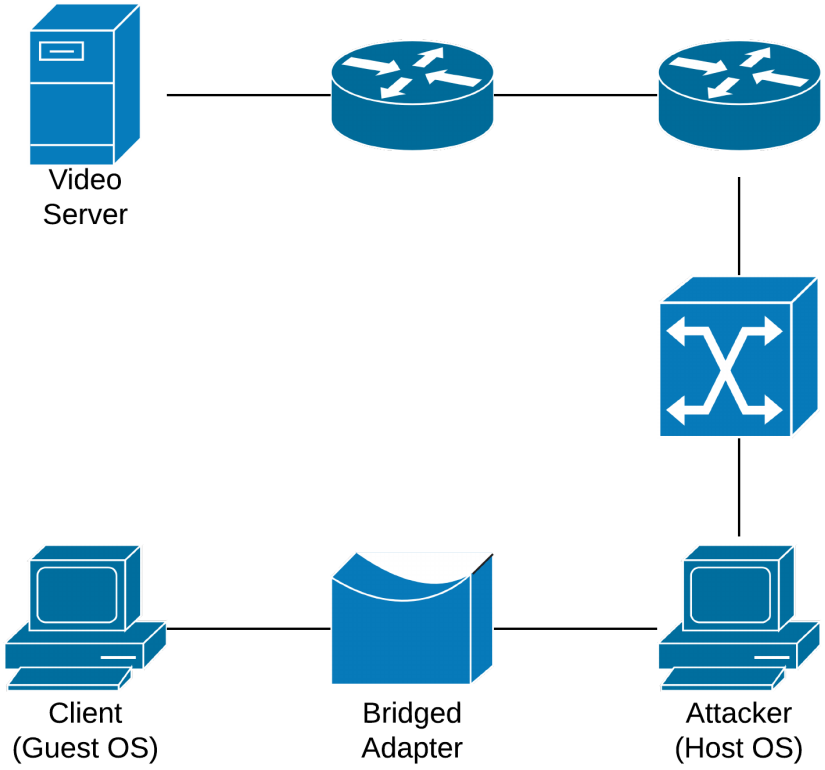

Figure 5: Implementation Topology

9 Implementation Environment

We will use **Oracle VM VirtualBox** for implementation purpose. The attack tool will be implemented in 2 phases. Those are:

1. First we will implement the TCP reset attack part assuming that we can sniff packets of victim machine. As shown in Section 15 (Figure 11), packets for guest OS can be sniffed from host OS. As TCP reset attack requires sniffing packets destined for other devices, we will use host OS as the attacker machine and guest OS of the VirtualBox as victim machine for this part. This topology is shown in Figure 5 where guest OS is connected through bridged network adapter. Video streaming server is remotely situated in the network.

2. In this phase, we will implement the part with which we can sniff packets from different machines on the network. If we can enrich the tool with additional attacking mechanisms of **ARP Spoofing** and take advantage of **ARP cache** of the network switch, the tool should be able to both sniff packets properly. As shown in Section 15 (Figure 9), normally guest OS cannot sniff host OS' packets. So for implementa-

tion of this part, we will flip the roles of attacker and victim of Figure 5 where we will try to sniff packets in the guest OS.

10 Target Environment

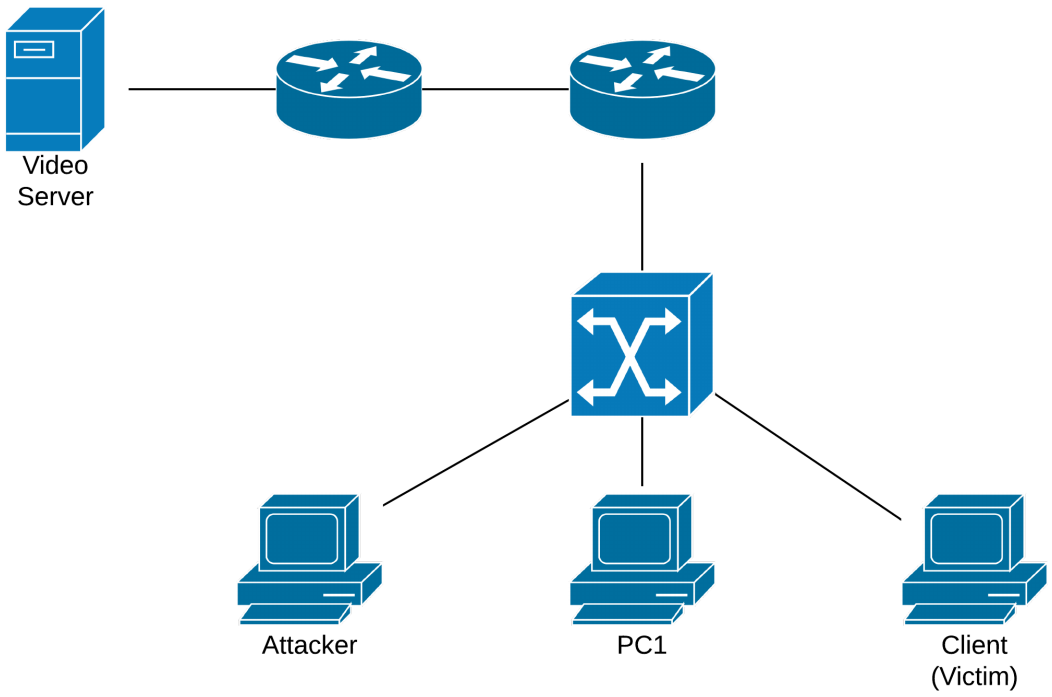

Figure 6: Target Topology

As our target environment, we have designed a topology as shown in Figure 6. Here the attacker and the victim are in the same subnet and the server is in a remote network. Without the loss of generality there can be more switches or routers in the network, and more hosts connected to the switch. This type of topology is carefully chosen as we need to sniff packets destined to the victim machine to gather information about source IP, TCP port numbers and sequence number in order to successfully perform a TCP reset attack.
Provided that the tool is a success, it will reach the state of one of a kind because currently available tools cannot work properly, as discussed in Section 6, in such a environment.

11 Justification

In our design we have included both ARP spoofing and TCP reset mechanism. It can be inferred from above discussion that if ARP spoofing can

successfully find out correct IP, port numbers and the sequence number, we can exactly mimic a RST packet from the original server.
When the victim machine receives the RST packet, it does not have any idea about the packet's actual origin. So the victim machine has no other option but to terminate its TCP connection. However the main challenge in this approach is to forge the packet and to send it in time so that it is within the victim's window. If we can do that, it can be said that our TCP reset attack will be successful.

12 Defence Mechanism

A defense mechanism for our attack tool can easily be derived from the above design. A simple time delay can effectively disable the effect of our attack. It is described below:

1. Whenever we receive an RST packet from video streaming server, we add a time delay before closing the connection rather than doing so immediately.

2. If we receive additional packets from the server within the time delay with correct sequence numbers, we can assume the RST packet was actually a spoofed one.

3. Otherwise after the time delay, we close the connection in the same way as it would normally do.

Here this defense mechanism should work propoerly because the original server is likely to retransmit the packets that were lost due too ARP spoofing and upon receiving the actual packets the victim can take appropriate measure.

13 Conclusion

We have discussed different aspects of the design of an attack tool to exploit a particular vulnerability of TCP. Nevertheless it is an inseparable part of today's internet. So as our concluding remarks, we hope that this attack tool may in turn provide us the insight about how to defend against such attacks.

14 Appendix A: Testing Video Streaming Server Connection

We have performed some tests to determine which video streaming website can be used for implementing our attack tool. If we can perform correctly for a single website using TCP connection, it can be generalized for any website using the same.

14.1 YouTube

The test failed. YouTube does not use TCP connection. Rather it uses UDP connection. It is shown in Figure 7 with the help of Wireshark. So YouTube cannot be used while implementing our attack tool

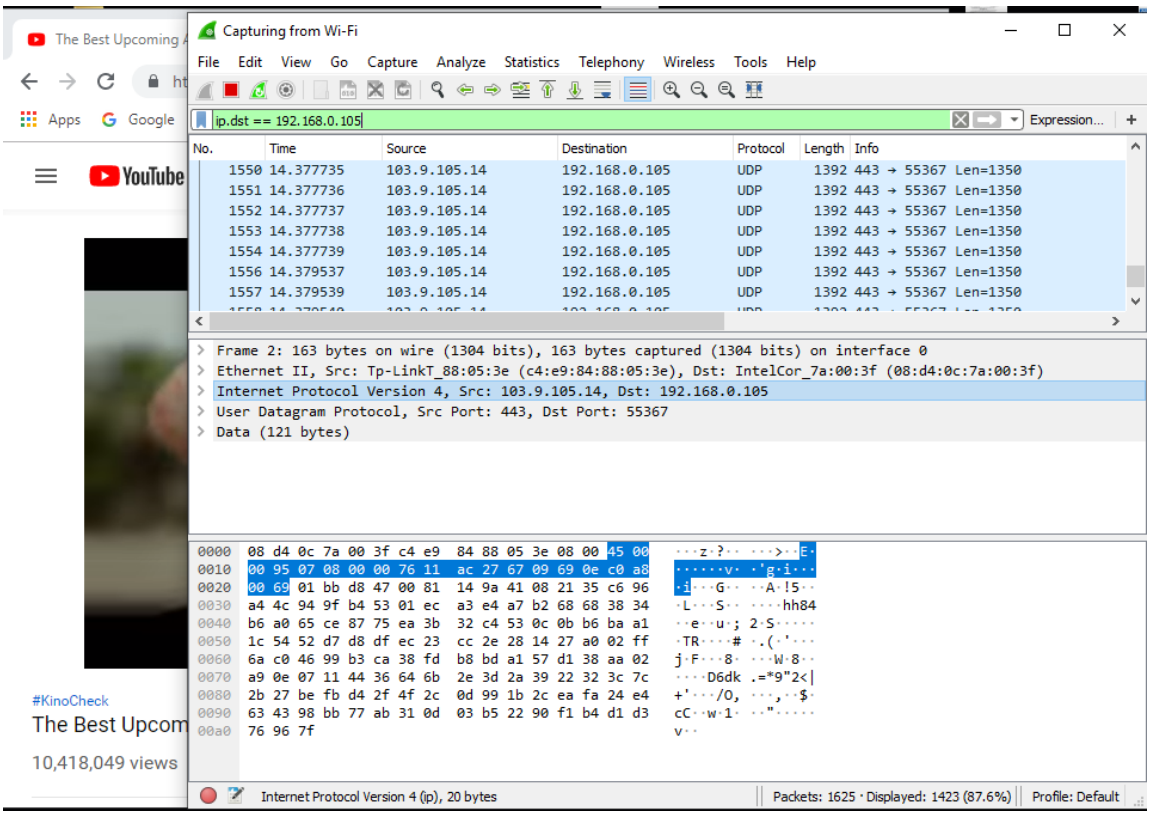

Figure 7: YouTube Connection

14.2 Vimeo

The test successful. Vimeo does indeed use TCP connection. It is shown in Figure 8 with the help of Wireshark. So it can be used in our implementation.

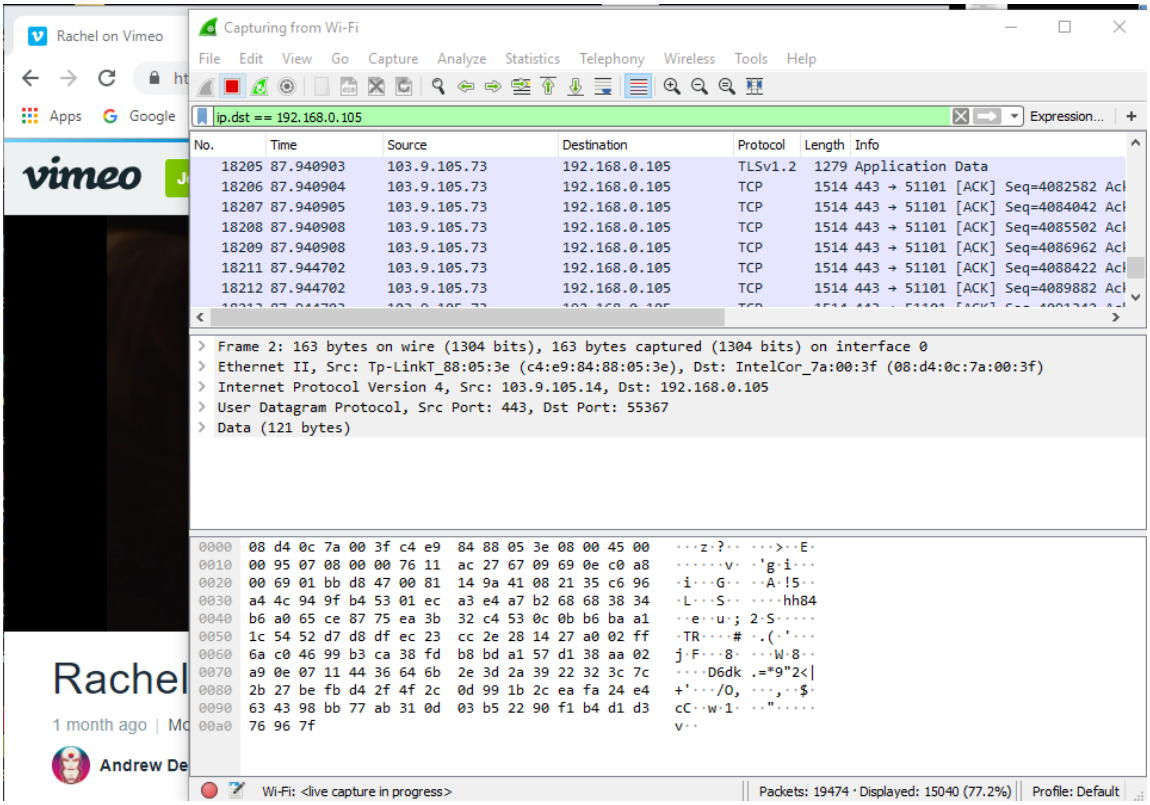

Figure 8: Vimeo Connection

15 Appendix B: Testing Sniffing with VM

We have performed test with **Oracle VM VirtualBox** to see how Wireshark behaves in this environment. Here the host OS has IP address: 172.20.56.3 and the 2 guest OS' have IP addresses: 172.20.56.50 and 172.20.56.54.

15.1 Guest Sniffing Host's Packet

The test failed. The guest OS cannot sniff packets of the host OS. It is shown in Figure 9.

15.2 Guest Sniffing Another Guest's Packet

The test failed. The guest OS cannot sniff packets of other guest's OS. It is shown in Figure 10.

15.3 Host Sniffing Guest's Packet

The test is successful. The host OS can sniff packets of the guest's OS. It is shown in Figure 11.

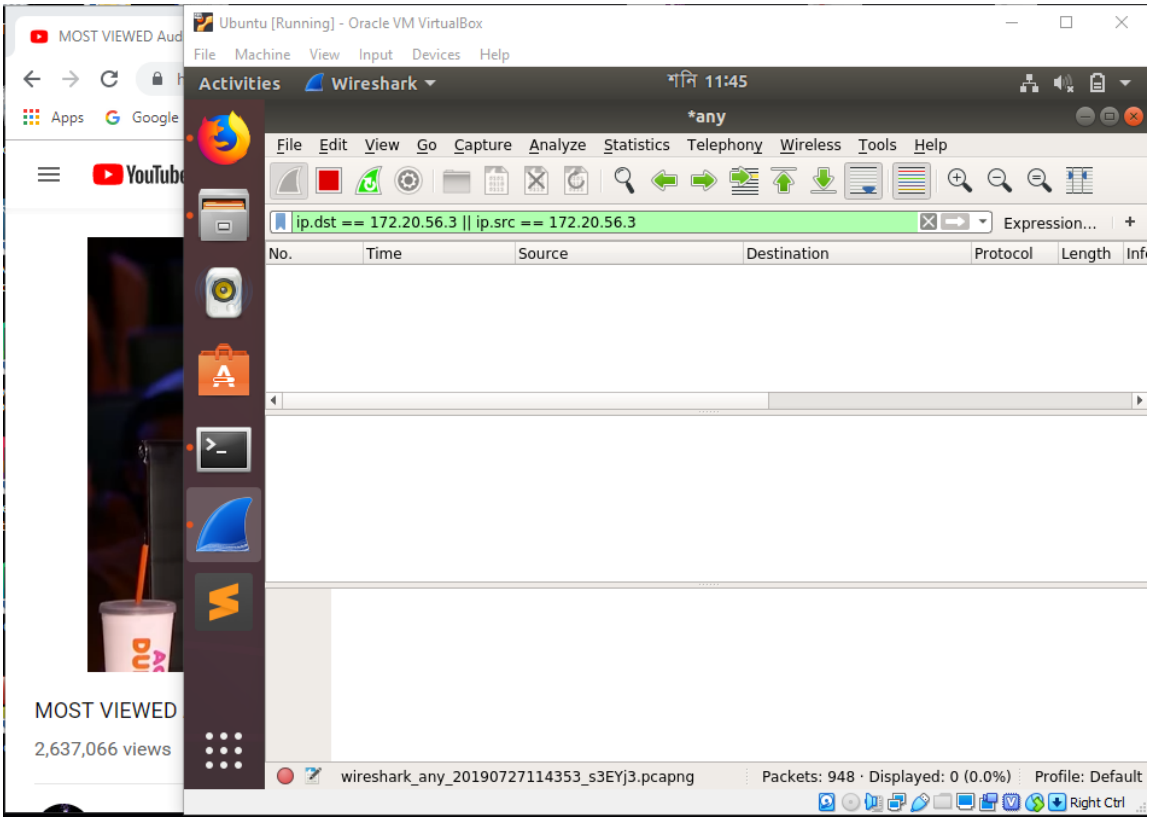

Figure 9: Guest Sniffing Host's Packet

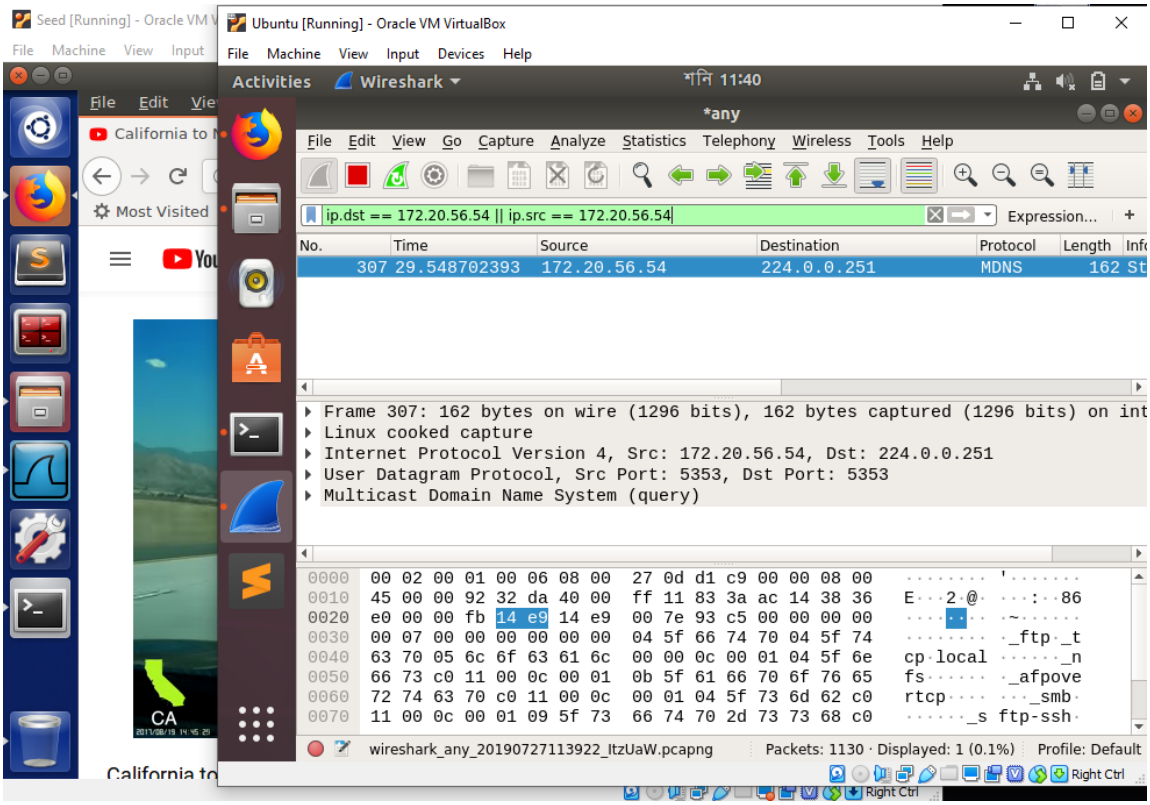

Figure 10: Guest Sniffing Another Guest's Packet

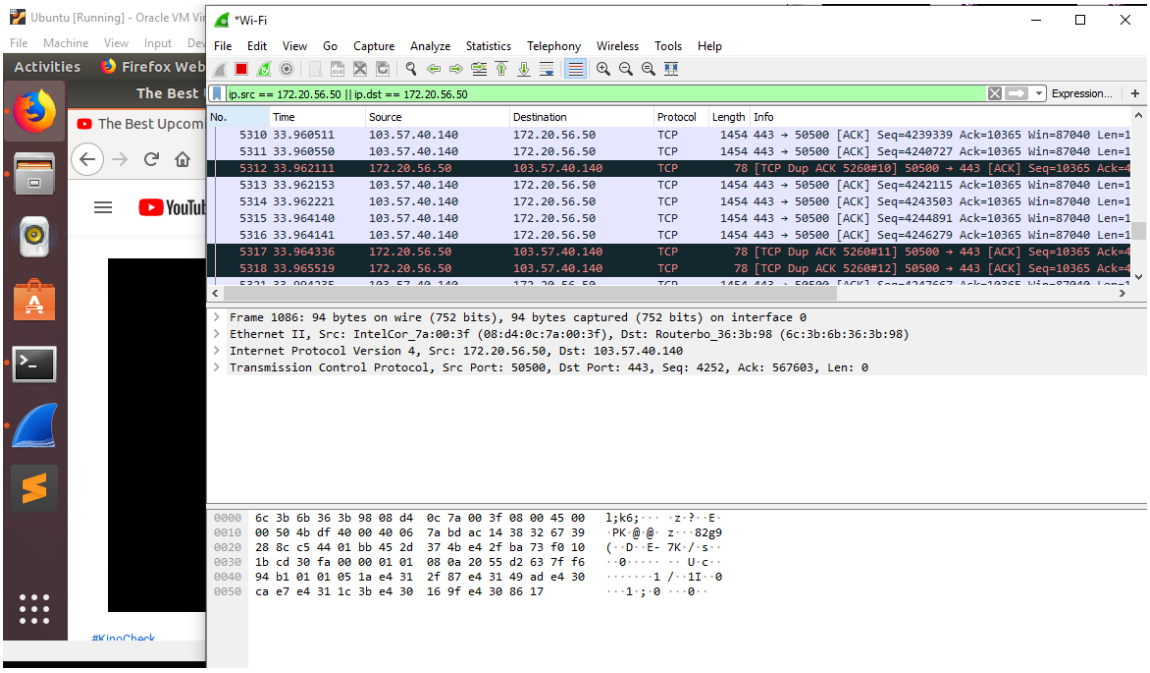

Figure 11: Host Sniffing Guest's Packet