Objective: To figure out high bandwidth streams initiated by a machine and mark them with a particular value if their total bytes count exceeds a threshold.

Approach:
1) Using iptables hooks and filter, we will send all SYN packets initiated by our machine to a user program, ie the target for iptable rule will be NFQUEUE.
2) The user program will then append another rule in iptables for this end host. This rule will have target set as ACCEPT and not NFQUEUE. Our program will not interfere with these packets. The rule is added to print bytes count for a connection using shell command: “iptables -nxvL”
3) Every second or so, we will be running a timer which will collect output for “iptables -nxvL” and process it.
4) If the total bytes count for a connection exceeds the threshold value:

- We append a rule in mangle table with IP DSCP field modification which signifies heavy load.
- Delete the iptable rule for this connection since we won’t need the total bytes count for this stream anymore

5) Else just ignore it for the time being.

Validation approach:
1) Using Wireshark, we can quickly check if the packets supposed to be marked are actually marked or not.
2) At any point of time, we won’t see a single connection or stream with total bytes counts exceeding the threshold in iptables output.
3) Using mangle table, we can check connections which have exceeded threshold.

Our Validation:

Mangle table :
Current mangle table rule before flushing

```
Chain PREROUTING (policy ACCEPT)
target     prot opt source               destination

Chain INPUT (policy ACCEPT)
target     prot opt source               destination

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
DSCP       tcp  --  100.80.244.31        216.58.193.206       DSCP set 0x32
DSCP       tcp  --  100.80.244.31        216.58.193.194       DSCP set 0x32
DSCP      tcp  --  100.80.244.31       216.58.193.196      DSCP set 0x32
DSCP      tcp  --  100.80.244.31       132.239.253.77      DSCP set 0x32
DSCP      tcp  --  100.80.244.31       216.58.193.193      DSCP set 0x32
DSCP      tcp  --  100.80.244.31       216.58.217.195      DSCP set 0x32
DSCP      tcp  --  100.80.244.31       216.58.193.197      DSCP set 0x32
DSCP      tcp  --  100.80.244.31       216.58.193.198      DSCP set 0x32
DSCP      tcp  --  100.80.244.31       74.125.28.189      DSCP set 0x32
DSCP      tcp  --  100.80.244.31       216.58.219.2      DSCP set 0x32
```

Iptables -nxvL (threshold set to 5KB):

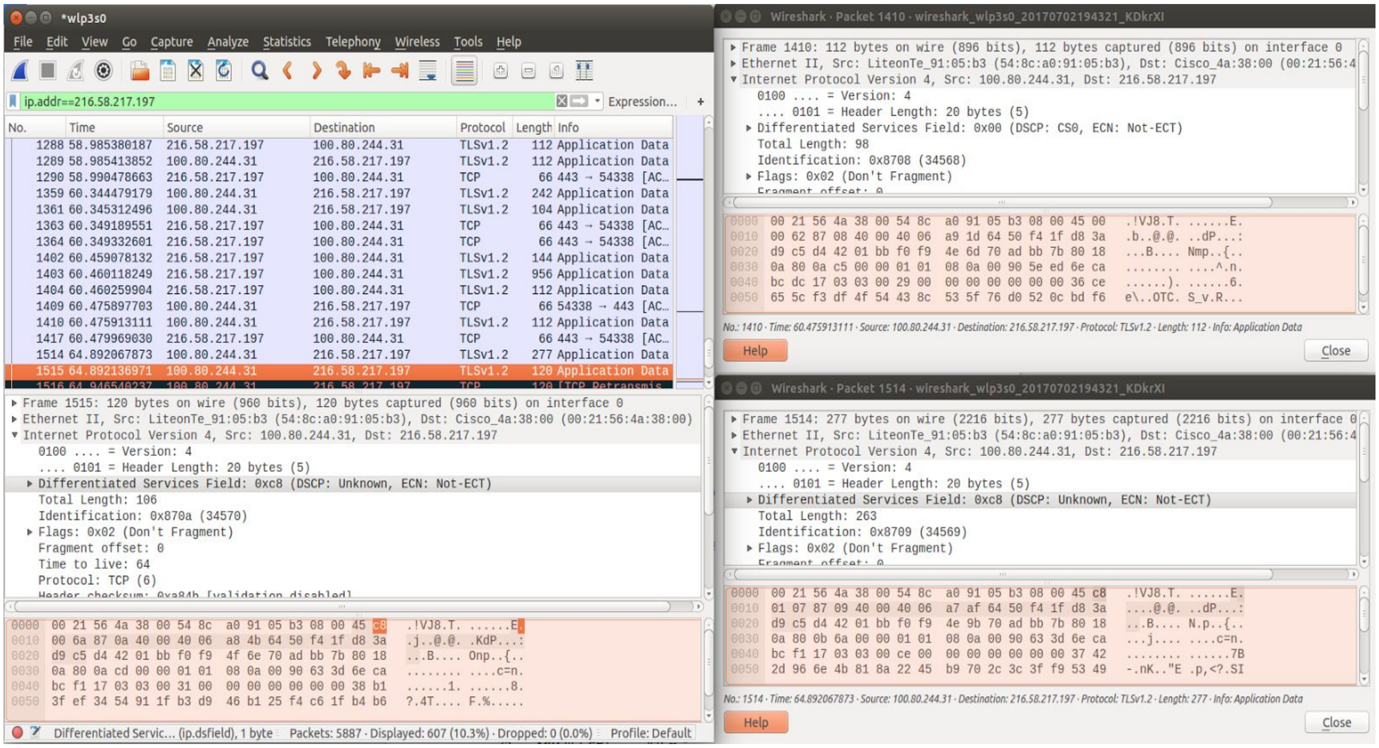
```
Chain INPUT (policy ACCEPT 70 packets, 24534 bytes)
        pkts     bytes target     prot opt in       out      source            destination

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

Chain OUTPUT (policy ACCEPT 38 packets, 9968 bytes)
        pkts     bytes target     prot opt in       out      source            destination
        34       2040 NFQUEUE          tcp  --  *          *        100.80.244.31           0.0.0.0/0
tcp flags:0x3F/0x02 NFQUEUE num 0
        9        1295 ACCEPT           tcp  --  *          *        100.80.244.31         216.58.193.195

        35       4616 ACCEPT           tcp  --  *          *        100.80.244.31          52.14.25.223
        17       2723 ACCEPT           tcp  --  *          *        100.80.244.31          31.13.71.2
        22       3257 ACCEPT           tcp  --  *          *        100.80.244.31          216.58.219.34
        24       3177 ACCEPT           tcp  --  *          *        100.80.244.31
173.194.158.75
        7        1145 ACCEPT           tcp  --  *          *        100.80.244.31
216.58.193.205
        15       4244 ACCEPT           tcp  --  *          *        100.80.244.31          172.217.5.74
        25       3202 ACCEPT           tcp  --  *          *        100.80.244.31          73.194.24.119
```

Wireshark Snippet:


*wlp3s0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expression...
+
Wireshark · Packet 1410 · wireshark_wlp3s0_20170702194321_KDkrXI
Wireshark · Packet 1514 · wireshark_wlp3s0_20170702194321_KDkrXI
Help
Close

```
ip.addr==216.58.217.197
```

```
No.   Time         Source          Destination     Protocol Length Info
 1288 58.985380187 216.58.217.197  100.80.244.31   TLSv1.2  112 Application Data
 1289 58.985413852 100.80.244.31   216.58.217.197  TLSv1.2  112 Application Data
 1290 58.990478663 216.58.217.197  100.80.244.31   TCP       66 443 → 54338 [AC…
 1359 60.344479179 100.80.244.31   216.58.217.197  TLSv1.2  242 Application Data
 1361 60.345312496 100.80.244.31   216.58.217.197  TLSv1.2  104 Application Data
 1363 60.349189551 216.58.217.197  100.80.244.31   TCP       66 443 → 54338 [AC…
 1364 60.349332601 216.58.217.197  100.80.244.31   TCP       66 443 → 54338 [AC…
 1402 60.459078132 216.58.217.197  100.80.244.31   TLSv1.2  144 Application Data
 1403 60.460118249 216.58.217.197  100.80.244.31   TLSv1.2  956 Application Data
 1404 60.460259904 216.58.217.197  100.80.244.31   TLSv1.2  112 Application Data
 1409 60.475897703 100.80.244.31   216.58.217.197  TCP       66 54338 → 443 [AC…
 1410 60.475913111 100.80.244.31   216.58.217.197  TLSv1.2  112 Application Data
 1417 60.479969030 216.58.217.197  100.80.244.31   TCP       66 443 → 54338 [AC…
 1514 64.892067873 100.80.244.31   216.58.217.197  TLSv1.2  277 Application Data
 1515 64.892136971 100.80.244.31   216.58.217.197  TLSv1.2  120 Application Data
 1516 64.946540237 100.80.244.31   216.58.217.197  TCP      120 [TCP Retransmis
```

```
▸ Frame 1515: 120 bytes on wire (960 bits), 120 bytes captured (960 bits) on interface 0
▸ Ethernet II, Src: LiteonTe_91:05:b3 (54:8c:a0:91:05:b3), Dst: Cisco_4a:38:00 (00:21:56:4a:38:00)
▾ Internet Protocol Version 4, Src: 100.80.244.31, Dst: 216.58.217.197
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▸ Differentiated Services Field: 0xc8 (DSCP: Unknown, ECN: Not-ECT)
    Total Length: 106
    Identification: 0x870a (34570)
  ▸ Flags: 0x02 (Don't Fragment)
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (6)
    Header checksum: 0xa84b [validation disabled]
```

```
0000  00 21 56 4a 38 00 54 8c  a0 91 05 b3 08 00 45 c8   .!VJ8.T. ......E.
0010  00 6a 87 0a 40 00 40 06  a8 4b 64 50 f4 1f d8 3a   .j..@.@. .KdP...:
0020  d9 c5 d4 42 01 bb f0 f9  4f 6e 70 ad bb 7b 80 18   ...B.... Onp..{..
0030  0a 80 0a cd 00 00 01 01  08 0a 00 90 63 3d 6e ca   ........ ....c=n.
0040  bc f1 17 03 03 00 31 00  00 00 00 00 00 00 38 b1   ......1. ......8.
0050  3f ef 34 54 91 1f b3 d9  46 b1 25 f4 c6 1f b4 b6   ?.4T.... F.%.....
```

```
Differentiated Servic… (ip.dsfield), 1 byte   Packets: 5887 · Displayed: 607 (10.3%) · Dropped: 0 (0.0%)   Profile: Default
```

```
▸ Frame 1410: 112 bytes on wire (896 bits), 112 bytes captured (896 bits) on interface 0
▸ Ethernet II, Src: LiteonTe_91:05:b3 (54:8c:a0:91:05:b3), Dst: Cisco_4a:38:00 (00:21:56:4
▾ Internet Protocol Version 4, Src: 100.80.244.31, Dst: 216.58.217.197
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▸ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 98
    Identification: 0x8708 (34568)
  ▸ Flags: 0x02 (Don't Fragment)
    Fragment offset: 0
```

```
0000  00 21 56 4a 38 00 54 8c  a0 91 05 b3 08 00 45 00   .!VJ8.T. ......E.
0010  00 62 87 08 40 00 40 06  a9 1d 64 50 f4 1f d8 3a   .b..@.@. ..dP...:
0020  d9 c5 d4 42 01 bb f0 f9  4e 6d 70 ad bb 7b 80 18   ...B.... Nmp..{..
0030  0a 80 0a c5 00 00 01 01  08 0a 00 90 5e ed 6e ca   ........ ....^.n.
0040  bc dc 17 03 03 00 29 00  00 00 00 00 00 00 36 ce   ......). ......6.
0050  65 5c f3 df 4f 54 43 8c  53 5f 76 d0 52 0c bd f6   e\..OTC. S_v.R...
```

No.: 1410 · Time: 60.475913111 · Source: 100.80.244.31 · Destination: 216.58.217.197 · Protocol: TLSv1.2 · Length: 112 · Info: Application Data

```
▸ Frame 1514: 277 bytes on wire (2216 bits), 277 bytes captured (2216 bits) on interface 0
▸ Ethernet II, Src: LiteonTe_91:05:b3 (54:8c:a0:91:05:b3), Dst: Cisco_4a:38:00 (00:21:56:4
▾ Internet Protocol Version 4, Src: 100.80.244.31, Dst: 216.58.217.197
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▸ Differentiated Services Field: 0xc8 (DSCP: Unknown, ECN: Not-ECT)
    Total Length: 263
    Identification: 0x8709 (34569)
  ▸ Flags: 0x02 (Don't Fragment)
    Fragment offset: 0
```

```
0000  00 21 56 4a 38 00 54 8c  a0 91 05 b3 08 00 45 c8   .!VJ8.T. ......E.
0010  01 07 87 09 40 00 40 06  a7 af 64 50 f4 1f d8 3a   ....@.@. ..dP...:
0020  d9 c5 d4 42 01 bb f0 f9  4e 9b 70 ad bb 7b 80 18   ...B.... N.p..{..
0030  0a 80 0b 6a 00 00 01 01  08 0a 00 90 63 3d 6e ca   ...j.... ....c=n.
0040  bc f1 17 03 03 00 ce 00  00 00 00 00 00 00 37 42   ........ ......7B
0050  2d 96 6e 4b 81 8a 22 45  b9 70 2c 3c 3f f9 53 49   -.nK.."E .p,<?.SI
```

No.: 1514 · Time: 64.892067873 · Source: 100.80.244.31 · Destination: 216.58.217.197 · Protocol: TLSv1.2 · Length: 277 · Info: Application Data

PS: With this approach, we are only channeling first SYN packet for any end host to the user program and no other packets. Subsequently, we are running a shell command through our script which automatically provides us the total bytes count for each connection initiated.