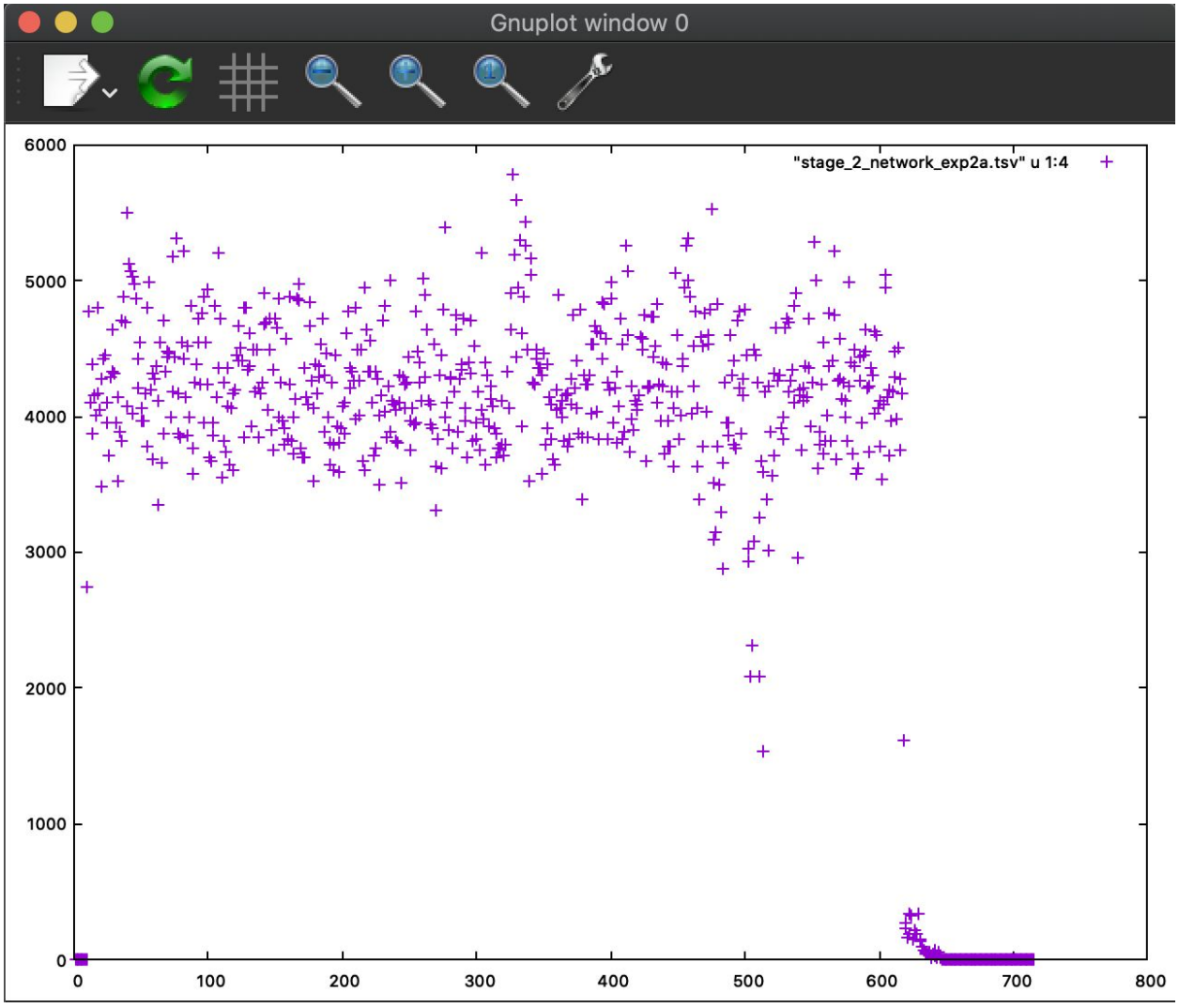
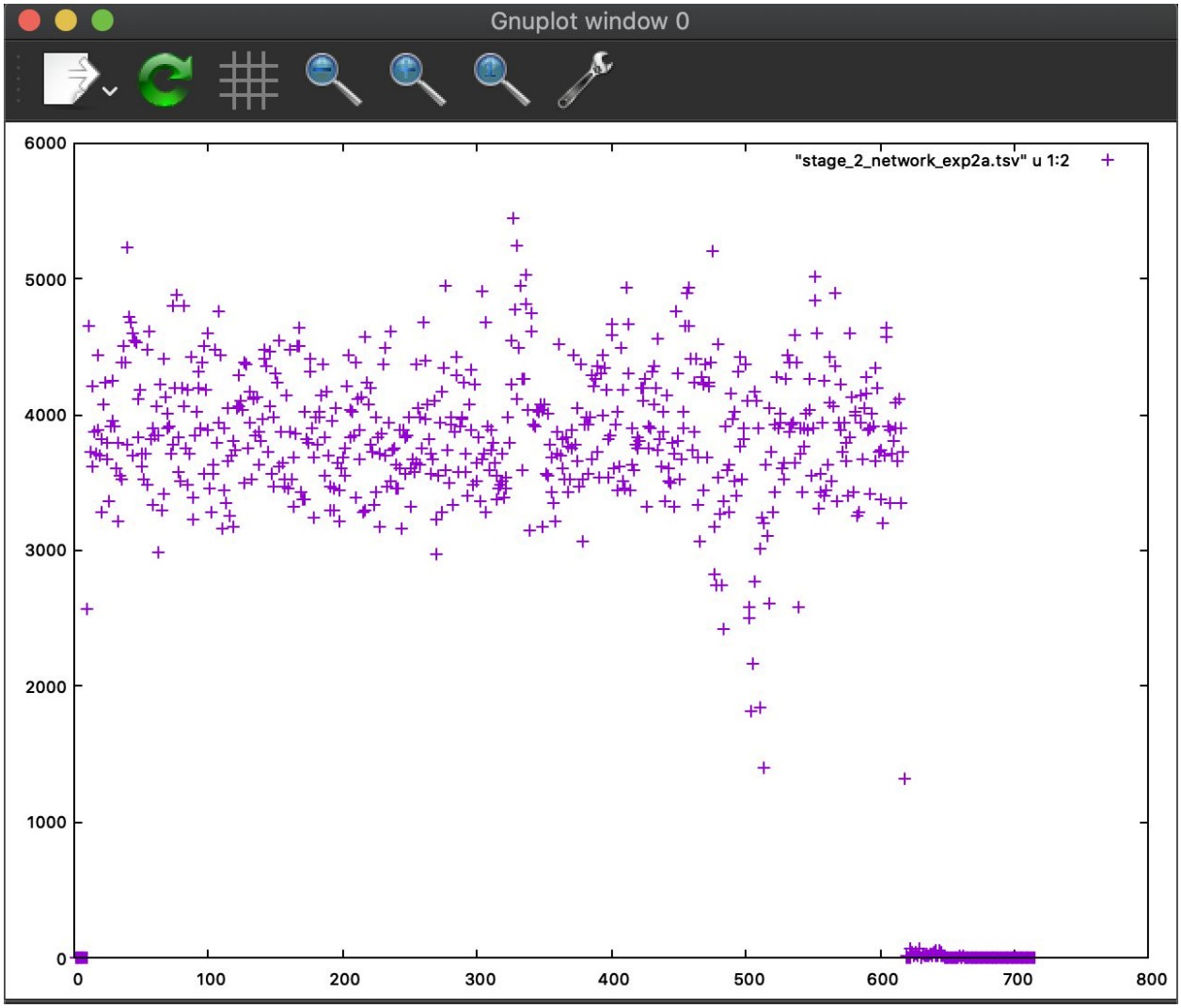
STAGE- 2 : LIVE TRAFFIC ANALYSIS

1. Graphs for incoming and outgoing traffic from server obtained from the data collected by running the network monitor utility:

    - ❏ Incoming traffic graph:



❏ Outgoing traffic graph:

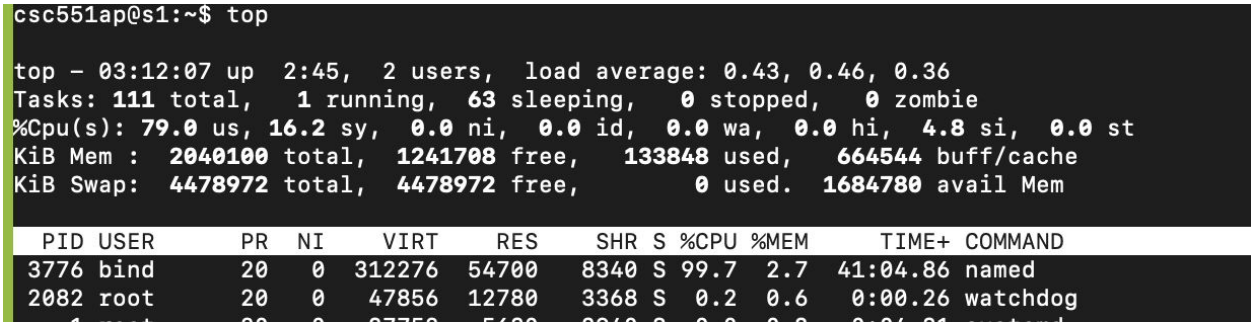


2. Observations after DoS attack on server from a client :
    - It can be seen from Fig. (6.1) that the DoS attack lasted for approximately **26sec**.
    - If we observe the tsv file for this experiment, i.e., stage_2_events_exp2b.tsv, we see that the bandwidth utilisation of the server was more than 50% during **20sec to 45sec** which is the **duration of the DoS attack**. So basically, as soon as the DoS attack was started the bandwidth utilisation of server link went above 50% and came down below 50% only after the DoS attack was over.

a) The resource being stressed here is the **server CPU** and server network bandwidth (to an extent of 50%). The output of the **top** command shows the CPU utilisation is nearly 100%.

```
csc551ap@c2:~/config/dnsperf$ ./dnsperf -d query-name-list.txt -s 10.1.3.3
DNS Performance Testing Tool
Nominum Version 2.1.0.0

[Status] Command line: dnsperf -d query-name-list.txt -s 10.1.3.3
[Status] Sending queries (to 10.1.3.3)
[Status] Started at: Fri Sep 11 01:57:47 2020
[Status] Stopping after 1 run through file
[Timeout] Query timed out: msg id 42180
[Timeout] Query timed out: msg id 42182
[Timeout] Query timed out: msg id 42185
[Timeout] Query timed out: msg id 42186
[Timeout] Query timed out: msg id 42184
[Timeout] Query timed out: msg id 42188
[Timeout] Query timed out: msg id 42187
[Timeout] Query timed out: msg id 42189
[Timeout] Query timed out: msg id 42190
[Timeout] Query timed out: msg id 42192
[Timeout] Query timed out: msg id 42191
[Timeout] Query timed out: msg id 42194
[Timeout] Query timed out: msg id 42193
[Timeout] Query timed out: msg id 42197
[Status] Testing complete (end of file)

Statistics:

  Queries sent:         499999
  Queries completed:    499985 (100.00%)
  Queries lost:         14 (0.00%)

  Response codes:       NOERROR 103072 (20.62%), NXDOMAIN 396913 (79.38%)
  Average packet size:  request 39, response 179
  Run time (s):         25.969223
  Queries per second:   19252.982656

  Average Latency (s):  0.004992 (min 0.000466, max 0.019177)
  Latency StdDev (s):   0.001316
```

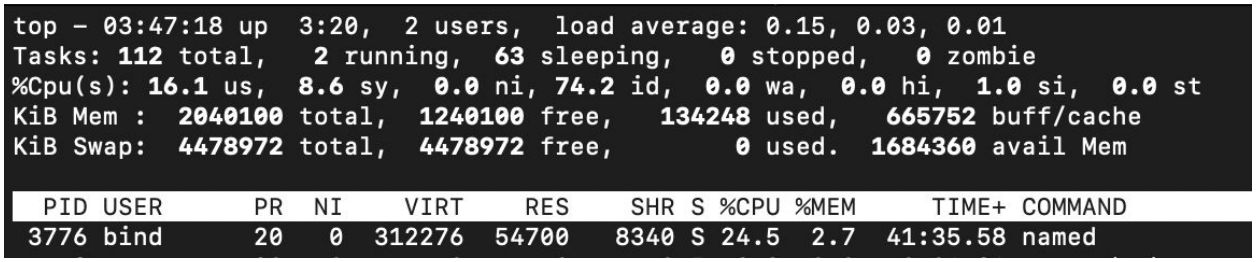
(Fig. 6.1)



(Fig. 6.2)

b) The inference is based on the tsv file collected during this experiment and Run time field in fig. (6.1) and %CPU usage in fig. (6.2).

c) Experiment 2b differs from experiment 2a in the sense that in experiment 2a the server is not overwhelmed with requests. Hence the CPU utilisation of the server is always below 25% (As evident from Fig. 6.3). On the contrary for experiment 2b, as soon as we start the DoS attack the server network bandwidth utilisation goes beyond 50% and CPU utilisation reaches 100% and stays so till the attack lasts.



(Fig. 6.3)

3. Observations after DDoS attack on the server from client:
    - It can be seen from Fig. (7.1) that the DDoS attack lasted for approximately **56sec**.
    - If we observe the tsv file for this experiment, i.e., stage_2_events_exp2c.tsv, we see that the bandwidth utilisation of the server was **more than 90%** during **19sec to 74sec**, between **80% - 90%** during **74sec - 75sec**, which is the duration of DDoS attack. So basically, as soon as the DDoS attack was started the bandwidth utilisation of server link went above 90% and came down below 50% only after the DDoS attack was over.

```
[Timeout] Query timed out: msg id 39327
[Timeout] Query timed out: msg id 39360
[Timeout] Query timed out: msg id 41315
[Timeout] Query timed out: msg id 41319
[Status] Testing complete (end of file)

Statistics:

  Queries sent:         499999
  Queries completed:    499512 (99.90%)
  Queries lost:         487 (0.10%)

  Response codes:       NOERROR 103026 (20.63%), NXDOMAIN 396486 (79.37%)
  Average packet size:  request 50, response 1009
  Run time (s):         56.683467
  Queries per second:   8812.305006

  Average Latency (s):  0.006592 (min 0.000937, max 0.017458)
  Latency StdDev (s):   0.001449

csc551ap@c2:~/config/dnsperf$
```

(Fig. 7.1)

```
top - 03:55:14 up  3:28,  2 users,  load average: 0.88, 0.52, 0.24
Tasks: 111 total,   1 running,  63 sleeping,   0 stopped,   0 zombie
%Cpu(s): 62.9 us, 18.8 sy,  0.0 ni, 14.1 id,  0.0 wa,  0.0 hi,  4.2 si,  0.0 st
KiB Mem :  2040100 total,  1237684 free,   135432 used,   666984 buff/cache
KiB Swap:  4478972 total,  4478972 free,        0 used.  1683168 avail Mem

  PID USER      PR  NI    VIRT    RES    SHR S %CPU %MEM     TIME+ COMMAND
 3776 bind      20   0  312536  54964   8340 S 81.8  2.7  46:40.54 named
```

(Fig. 7.2)

a) The resource being stressed here is the **network bandwidth of the server** and server CPU (to an extent of ~80%). It can be seen from the tsv that the network bandwidth utilisation went above 90% as soon as the DDoS attack was started from client C2. The output of the **top** command shows the CPU utilisation went up to 82% during the entire duration of experiment 2c.

b) The inference is based on the tsv file collected during this experiment and Run time field in fig. (7.1) and %CPU usage in fig. (7.2).

c) In experiment 2(b) it is the Server CPU that is getting primarily stressed while in experiment 2(c) the resource being stressed primarily is the server network bandwidth. The bandwidth utilisation is 2(b) is within 50%-80% whereas the CPU utilisation is almost 100% on the contrary, for 2(c) the network bandwidth utilization is nearly 100%, thereby restricting the number of queries and not overwhelming the server CPU to max capacity.