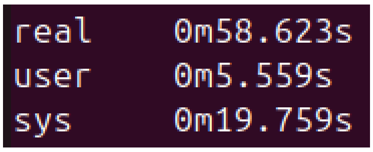
Evaluate Snort

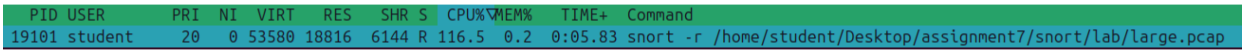
7 files were downloaded from https://share.netresec.com/s/nF5zNcaXLgwdQFZ and merged with Wireshark so that we could make large.pcap file ≃ 1GB.

time snort -r /home/student/Desktop/assignment7/snort/lab/large.pcap



```
real	0m58.623s
user	0m5.559s
sys	0m19.759s
```

using htop:



```
  PID USER       PRI  NI  VIRT   RES   SHR S  CPU%▽MEM%   TIME+  Command
19101 student     20   0 53580 18816  6144 R 116.5  0.2  0:05.83 snort -r /home/student/Desktop/assignment7/snort/lab/large.pcap
```

The command
snort -r /home/student/Desktop/assignment7/snort/lab/large.pcap
utilizes nearly 100% of the CPU (116.5% at the specific moment shown in the screenshot). This indicates that during the 20 seconds it takes for the system to process the file, the system operates at its full capacity.

Suggestions for Optimization:

- We could comment out irrelevant rules in snort.conf to reduce processing load.
- We could use Snort's multithreading feature to utilize multiple CPU cores.
- Ensure sufficient CPU and memory for better performance.