The first thing I did was to export all the objects, but nothing. Then, I looked through the strings :

strings -n 7 mule.pcapng > file.txt

And at some point, I found this list of processes :

```
USER        PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root          1  0.0  0.0  24876 14384 ?        Ss   10:08   0:06 /sbin/init splash
root          2  0.0  0.0      0     0 ?        S    10:08   0:00 [kthreadd]
root          3  0.0  0.0      0     0 ?        S    10:08   0:00 [pool_workqueue_release]
root          4  0.0  0.0      0     0 ?        I<   10:08   0:00 [kworker/R-rcu_gp]
root          5  0.0  0.0      0     0 ?        I<   10:08   0:00 [kworker/R-sync_wq]
.
.
.
```

And it was huge! The first thing I reminded of was Q3 : Ce comanda a fost executata pe serverul de C2, pentru a exfiltra date? (Points: 48) **Formatul raspunsului este: xx.** It was **ps,** the command used to list the processes on Linux.

Now, we have to look after the malware. I filtered the strings because I wanted to see all the processes from **darius**, the used found in the packets :

strings file.txt | grep darius > darius.txt

For the malware, it was pretty hard to find. I got an idea : I searched for the malware file thanks to the title of the challenge. After multiple failed tries, I used :

strings darius.txt | grep lue

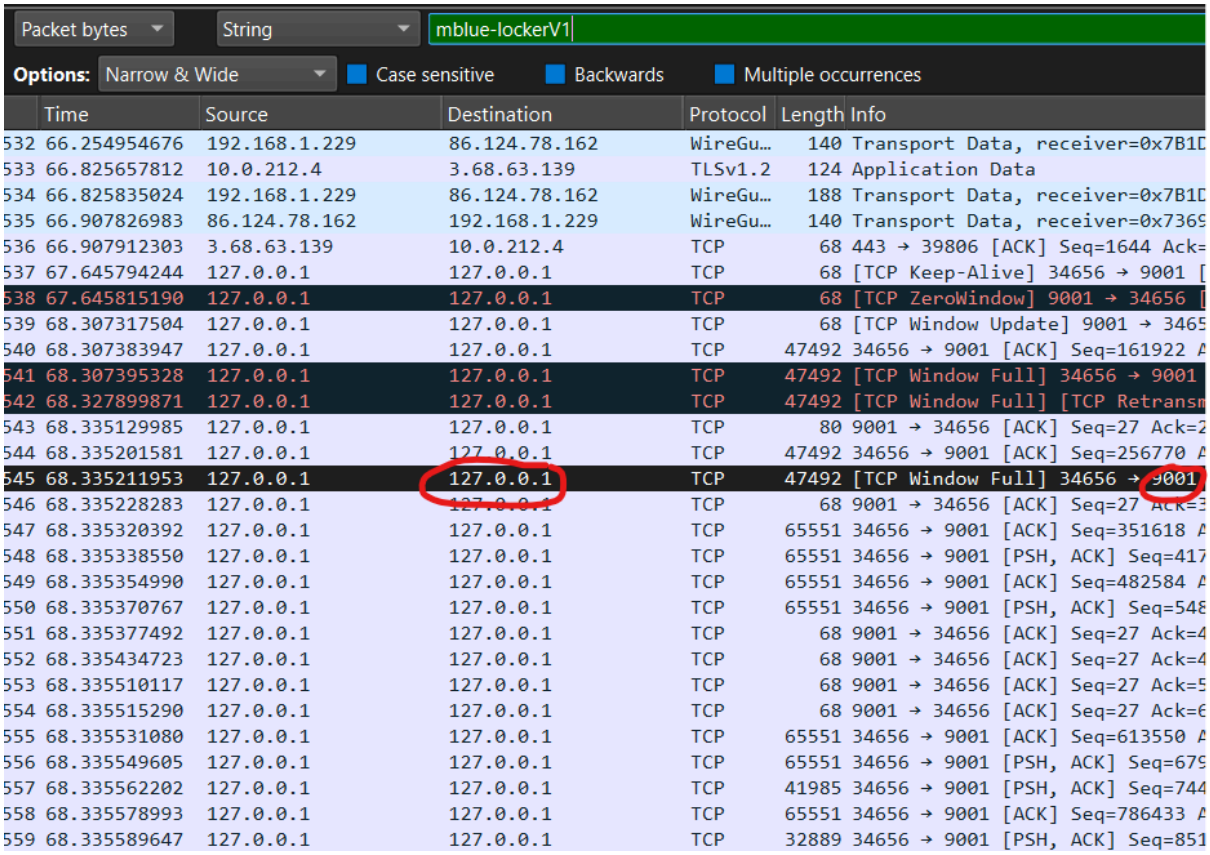
And the output was :

```
darius    177717  0.0  0.0   2684  1384 pts/2    S+   12:55   0:00 ./mblue-lockerV1
darius    177717  0.0  0.0   2684  1384 pts/2    S+   12:55   0:00 ./mblue-lockerV1
darius    177717  0.0  0.0   2684  1384 pts/2    S+   12:55   0:00 ./mblue-lockerV1
darius    177717  0.0  0.0   2684  1384 pts/2    S+   12:55   0:00 ./mblue-lockerV1
.
.
.
```

In the title, you can get hits about the challenge

Q1. Sa se identifice numele malware-ului care ruleaza pe statia compromisa. (Points: 100)Formatul raspunsului este de forma: cuvant-cuvant. : **mblue-lockerV1**

For the rest second question, I searched **mblue-lockerV1** with Wireshark and I found the IP and the Port :



Q2. Identifică IP si port pentru serverul de C2. (Points: 60) Formatul raspunsului este: IP:PORT : **127.0.0.1:9001**