Competition in network traffic analisys

Elisabetta Fedele & Emilio Corigliano

Why we decided to join

- To understand the practical aspects of what we studied
- To learn how to work paired up
- To enrich our python coding skills

python

WIRESHARK

Creative Task 1

- In the first cretive task we wanted to show the structure of all the networks (based on the natural netmask) found in the capture
- To do that we have created a tree structure based on an increasing order, which make it easy to analyze the results
- We saved the output on the file creative_task_1.csv

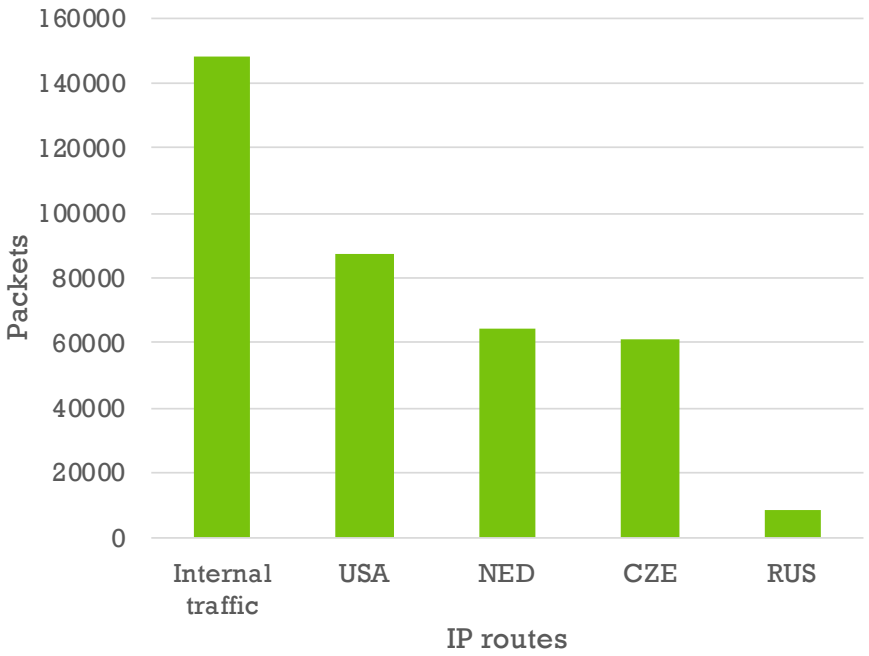
```
129.6.0.0
|- 129.6.15.28
129.6.255.255

129.7.0.0
|- 129.7.53.72
129.7.255.255

129.8.0.0
|- 129.8.31.161
|- 129.8.39.17
129.8.255.255

129.11.0.0
|- 129.11.57.158
129.11.255.255

129.16.0.0
|- 129.16.15.155
|- 129.16.37.36
|- 129.16.55.109
|- 129.16.113.228
|- 129.16.137.106
129.16.255.255
```

Creative Task 2

- For the second creative task we wanted to underline the top 15 links (the most used connections between different IP addresses)
- Our initial idea was to use Basemap or cartopy to see our result printed on a map, but we had some technical issues with the installation of the libraries, so we worked manually, making a map on GoogleMaps
- Even if it is not what the competition asked us, we found interesting to share our final results, achieved using GoogleMaps and dbip, a website which for every IP address have its coordinates

Click here to see our map!

Creative Task 2



Creative task 3

- For the third creative task we wanted to analyze for a parcticular link the traffic and the amount of packet lost
- So, in order to do that, we filtered the interested packets and we counted the retransmitted packets (thanks to the ACK number and the SEQ number of the packets).
- We gave in output the packets lost on the total amount of packets transmitted, the rate of it (in the file creative_task_3.csv) and a plot that shows the loss (y-axis) in function of the time (x-axis)

Creative Task 3