TRAFFIC ANALYSIS COMPETITION

GIORGIO N. BUTTIGLIERI

SIMONE BASELICE

SUMMARY

1. IP locations distribution analysis

2. Connections quality analysis

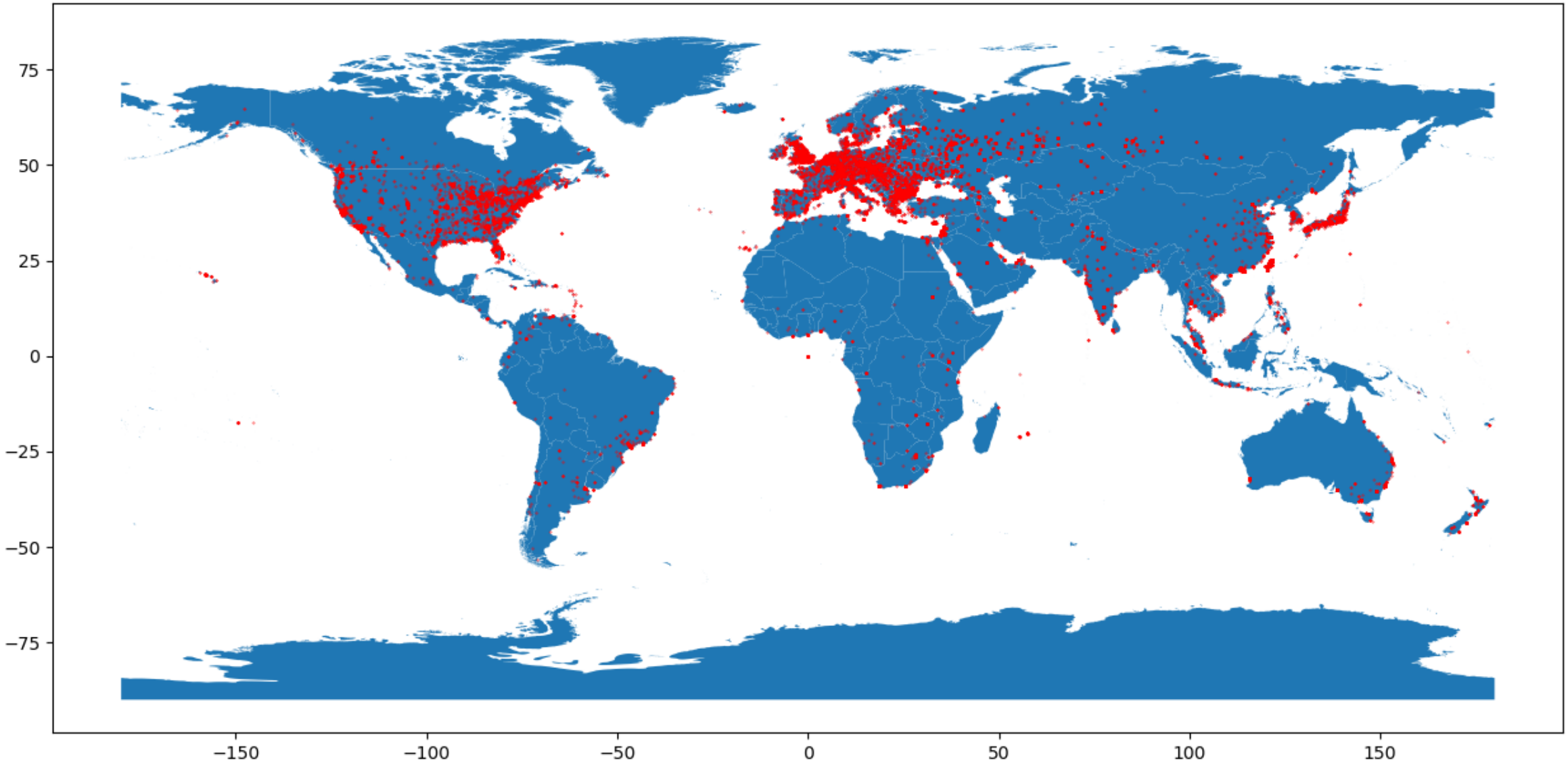
3. Subnets analysis

IP DISTRIBUTION

- Real locations of the IP addresses have been gathered using the service offered by extreme-ip-lookup.com. We made a python script called "*locate_ip.py*" that works by sending a GET request for every IP at the URL https://extreme-ip-lookup.com/json/{IP}

- We plotted the results in a world map and analyzed the locations distribution

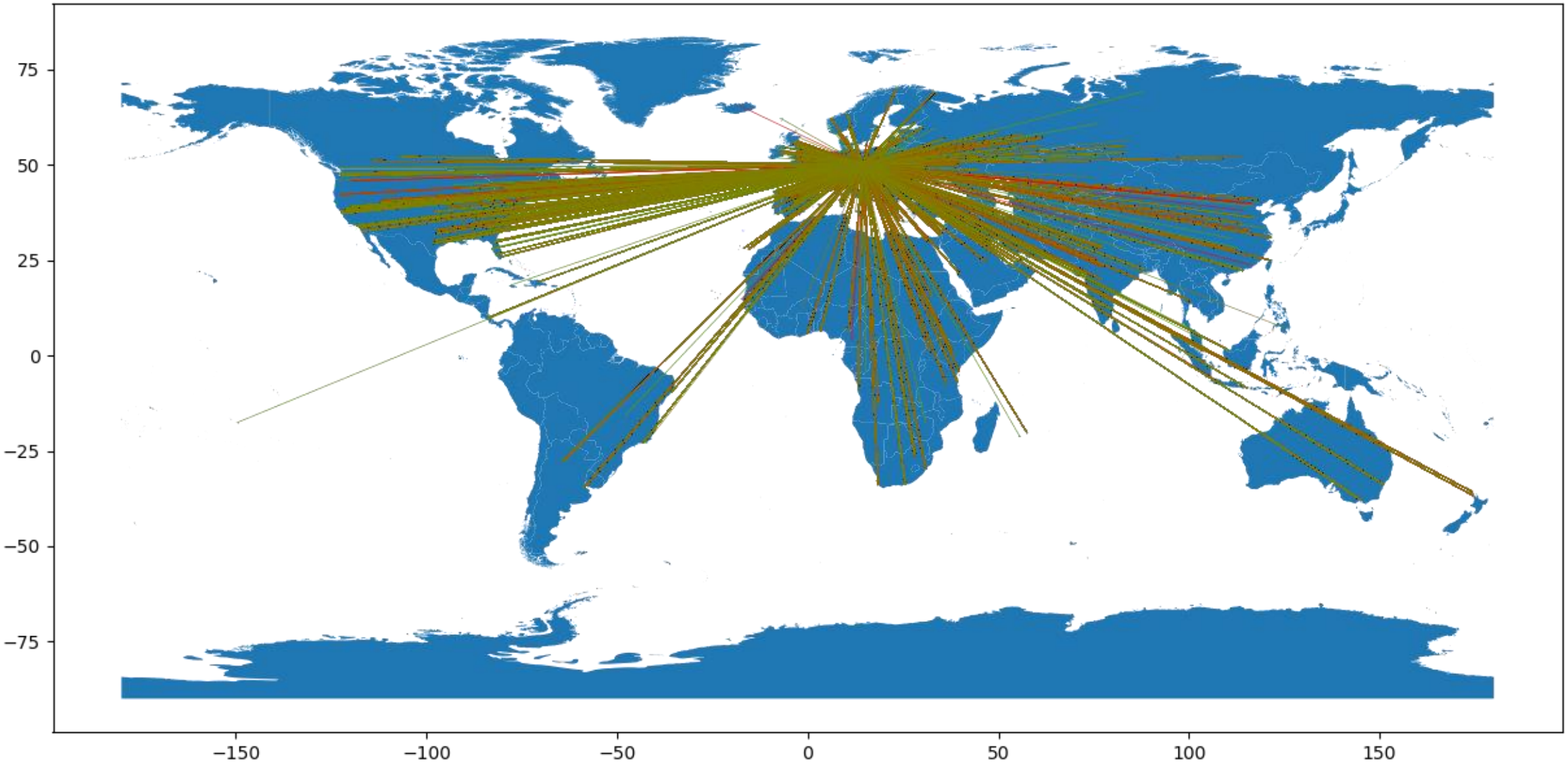
ACTUAL DISTRIBUTION



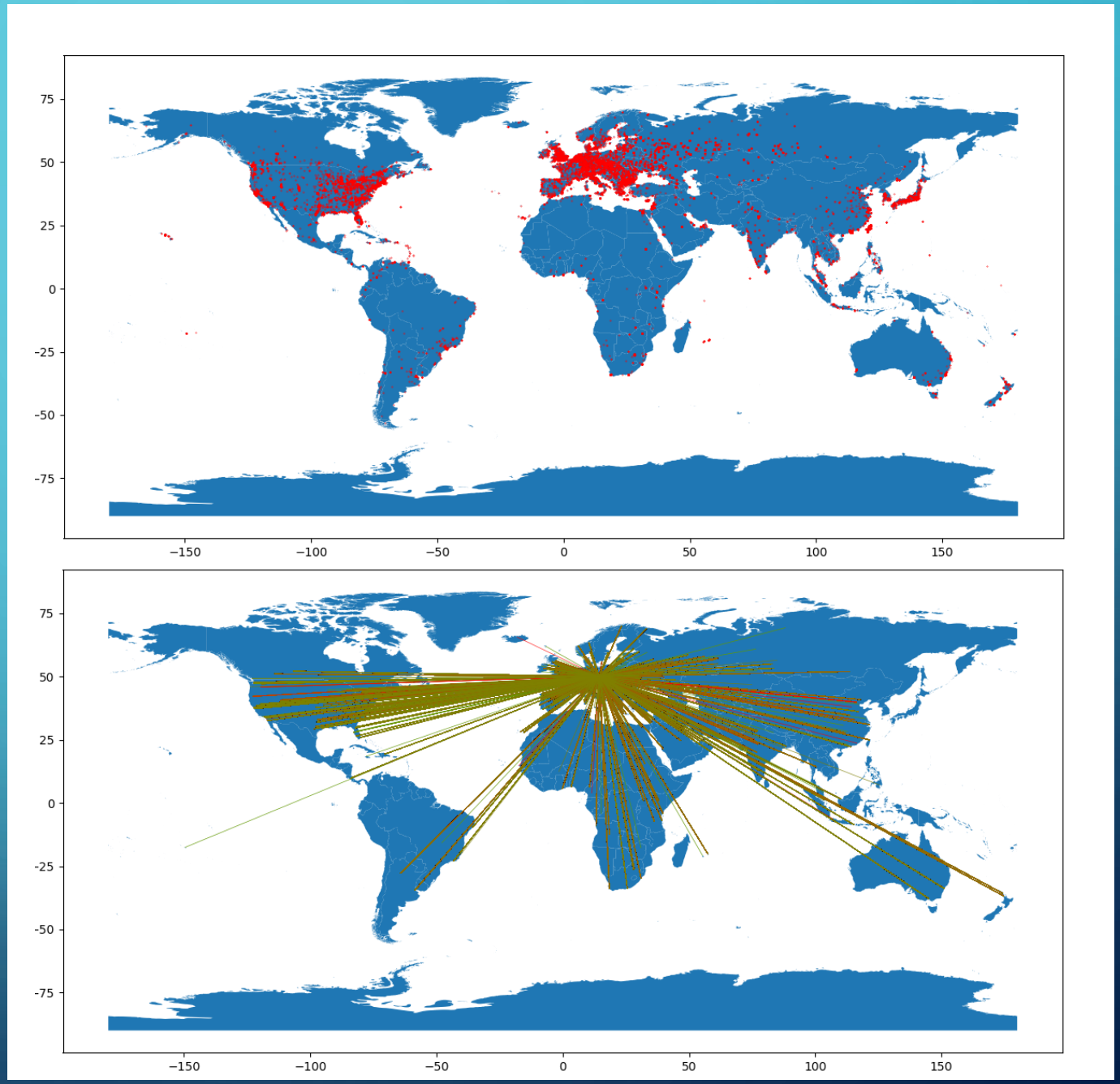
CONNECTION QUALITY ANALYSIS

- We tracked TCP bidirectional connections
- For every connection it counts the number of times there are 3 or more repeated ACK (NACK) so to estimate the number of errors occurred for that specific connection
- We plotted the connections as lines where the line color indicates the connection quality

TCP CONNECTIONS



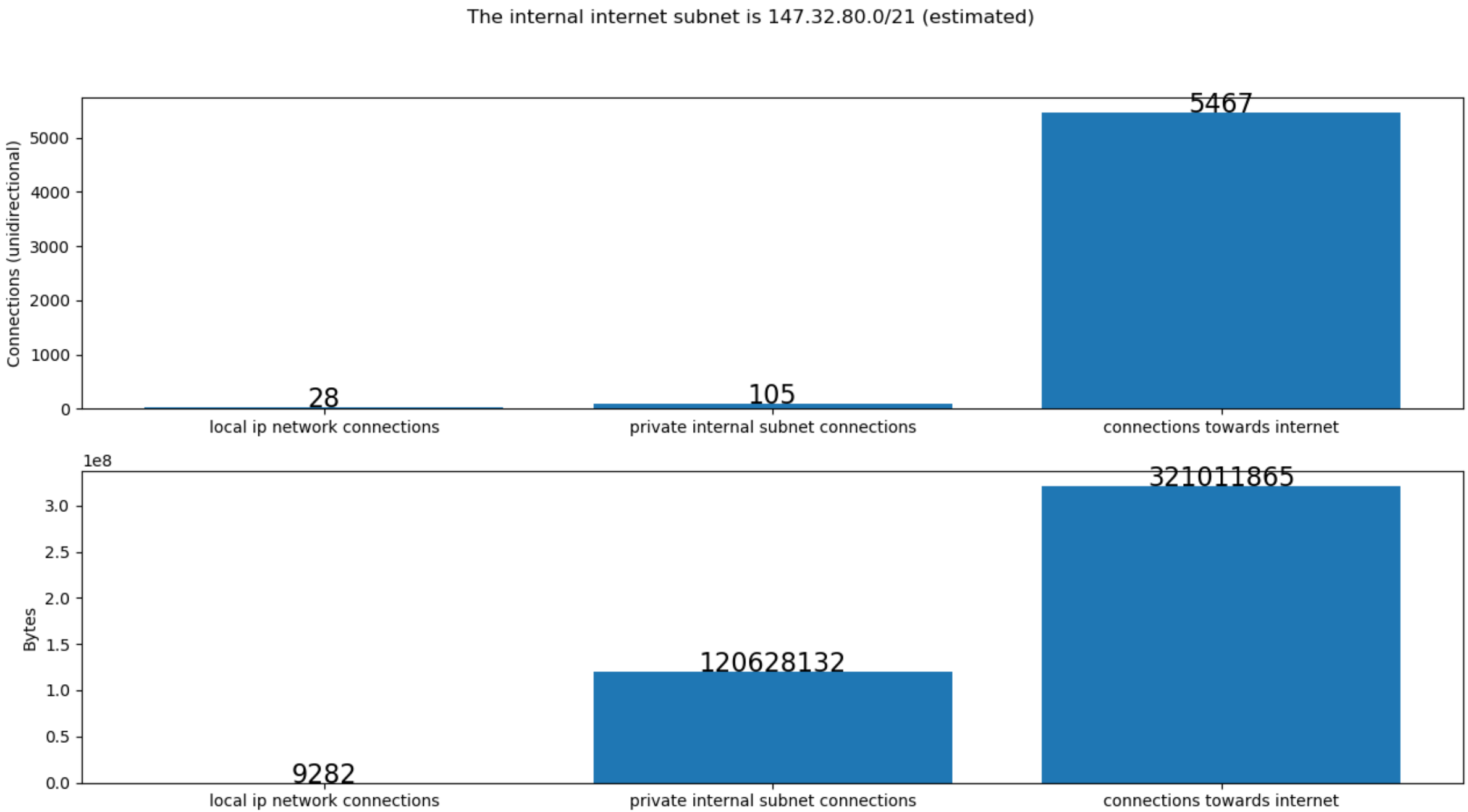
IP LOCATIONS



TCP STREAMS

SUBNET ANALYSIS

- We divided the traffic in three networks
  - 1) Local IP network (192.168.0.0/16)
  - 2) Biggest local area network. Biggest subnet connected to the internet by the router
  - 3) World-wide internet


The internal internet subnet is 147.32.80.0/21 (estimated)
Connections (unidirectional)
0
1000
2000
3000
4000
5000
28
105
5467
local ip network connections
private internal subnet connections
connections towards internet
1e8
Bytes
0.0
0.5
1.0
1.5
2.0
2.5
3.0
9282
120628132
321011865
local ip network connections
private internal subnet connections
connections towards internet