Network Traffic Analysis

Antonio Scapellato – Massimo Valle

About our work

To analyze the traffic, the first thing to do is to sniff the network, after that it is possible to handle the sniffed traffic as a dataset.

We have dived our work (code) in the following steps:

1. Loading the capture (e.g: 'network_traffic.pcap')
2. Creating a structure (e.g: dataframe in Pandas)
3. Manage the dataframe in order to achieve a goal (e.g: TOP IPs, amount of traffic and so on…)

Creativity tasks

1. We decided to extend the second task finding the top 50 IPs and using the file 'ips_location.csv' and in order to visualize theme we produced a graph and plotted them in a map ('map.html').
2. For the second creativity task we decided to answer a personal question.
   How the internet works? Or after the results ... How bad the internet works?
   We decided to analyze the 'tos' of each packet and we have found out that the 98% of the traffic is 'type 0' (best effort) and just a small amount of the packets are they are treated in a discriminatory manner! (Also if there are hundreds of different 'type of service' codes)