# Speedtest Analysis with wireshark (Group 1)

Since make an analysis into a local machine could lead to a bad evaluation of results due to other applications' network traffic noise, we made the analysis into a isolated environment like a virtual machine. For a further accuracy in the capture we set the `tcp` filter option in wireshark and after we run the speedtest.

Fast.com result
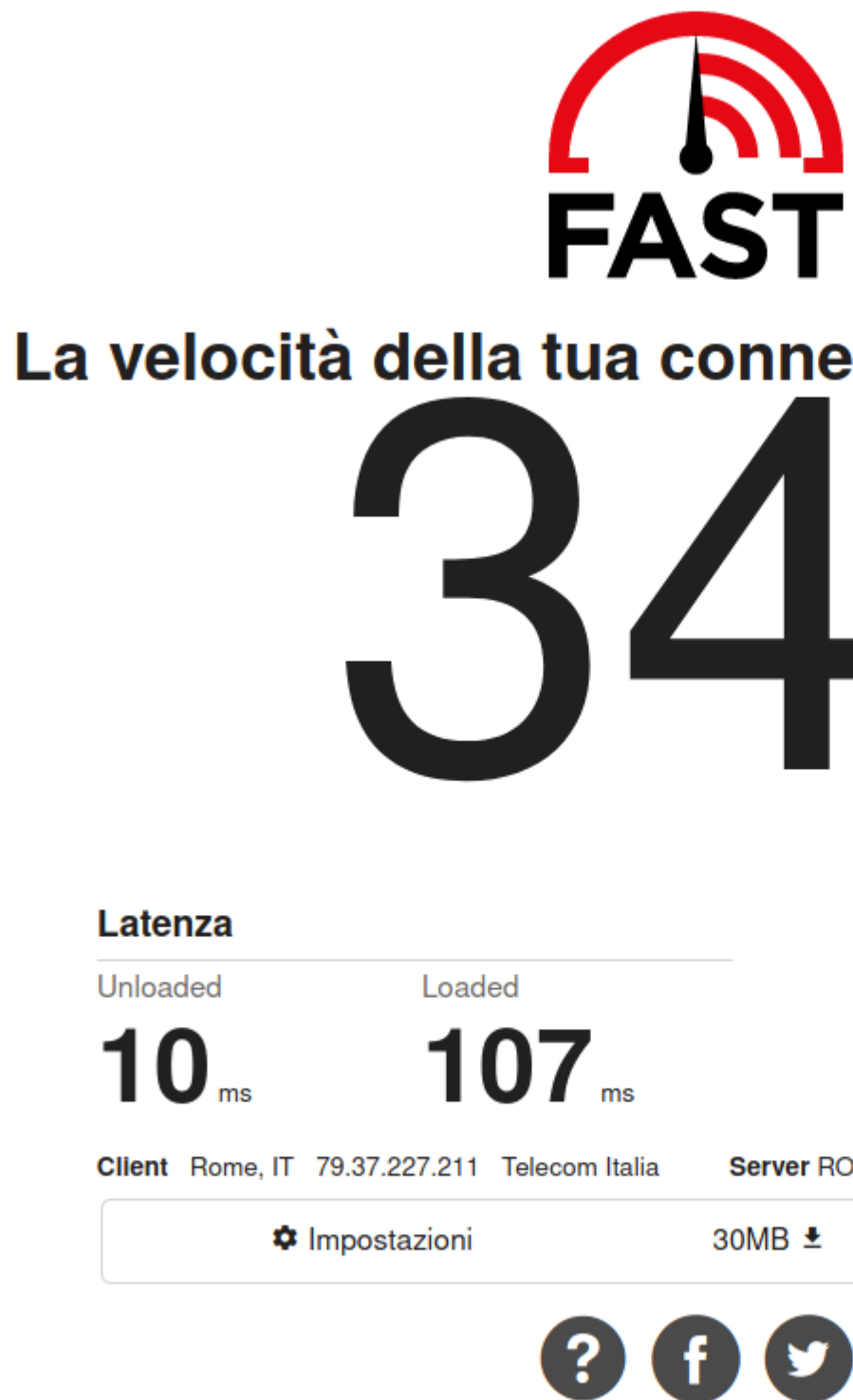
From this speedtest we focused into 2 informations: the download speed (34 Mbps) and the upload speed (8.1 Mbps).

Wireshark analysis

During the speedtest we captured all traffic outgoing and ingoing from and to our machine including the one created by fast.com and it can be found in [this pcap file](#).

Conversations:

We report below the conversations extracted from wireshark capture of fast.com speedtest:

|	Ethernet · 5	IPv4 · 14	IPv6	TCP · 26	UDP · 264	
Address A ▾	Address B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A
2.23.20.150	192.168.1.26	99	68 k	50	62 k	49
18.203.130.218	192.168.1.26	199	237 k	90	16 k	109
23.246.50.154	192.168.1.26	3.455	7.125 k	1.773	6.270 k	1.682
23.246.51.156	192.168.1.26	6.935	15 M	3.743	13 M	3.192
45.57.72.140	192.168.1.26	11.830	17 M	5.780	2.471 k	6.050
45.57.73.144	192.168.1.26	10.827	16 M	5.415	3.349 k	5.412
52.18.232.179	192.168.1.26	27	4.584	12	2.553	15
93.184.220.29	192.168.1.26	73	12 k	30	6.784	43
151.99.109.9	192.168.1.26	14.793	24 M	7.546	8.650 k	7.247
192.168.1.1	192.168.1.26	568	62 k	286	32 k	282
192.168.1.1	224.0.0.1	1	60	1	60	0
192.168.1.9	255.255.255.255	2	376	2	376	0
192.168.1.9	192.168.1.255	2	376	2	376	0
192.168.1.26	224.0.0.251	1	46	1	46	0

☐ Risoluzione dei nomi   ☐ Limita al filtro di visualizzazione   ☐ Ora iniziale assoluta

From this table we see that our machine exchange an high number of packets with these 5 endpoints: 23.246.50.154, 23.246.51.156, 45.57.72.140, 45.57.73.144, 151.99.109.9. We suppose that fast.com opens 5 connections with these machines on the internet for the speedtest, in particular, analyzing the number of bytes exchanged in both directions between the local machine and these remote machines, the first two hosts (23.246.50.154, 23.246.51.156) are used to test the download speed, and the other three hosts (45.57.72.140, 45.57.73.144, 151.99.109.9) are used to test the upload speed. Making a whois request on the address 52.18.232.179 (seventh row first column) the result is that it belongs to amazon and since netflix relies on AWS for its services we suppose also that the 5 hosts used for the speedtest were sent by the host with ip 52.18.232.179.

I/O Graph analysis

To analyze the speedtest we opened the I/O Graph window from statistics
menu and we added two filters: one for filtering the download traffic
`tcp.srcport == 443` (the pink curve) and one for filtering the upload traffic
`tcp.dstport == 443` (the blue curve).
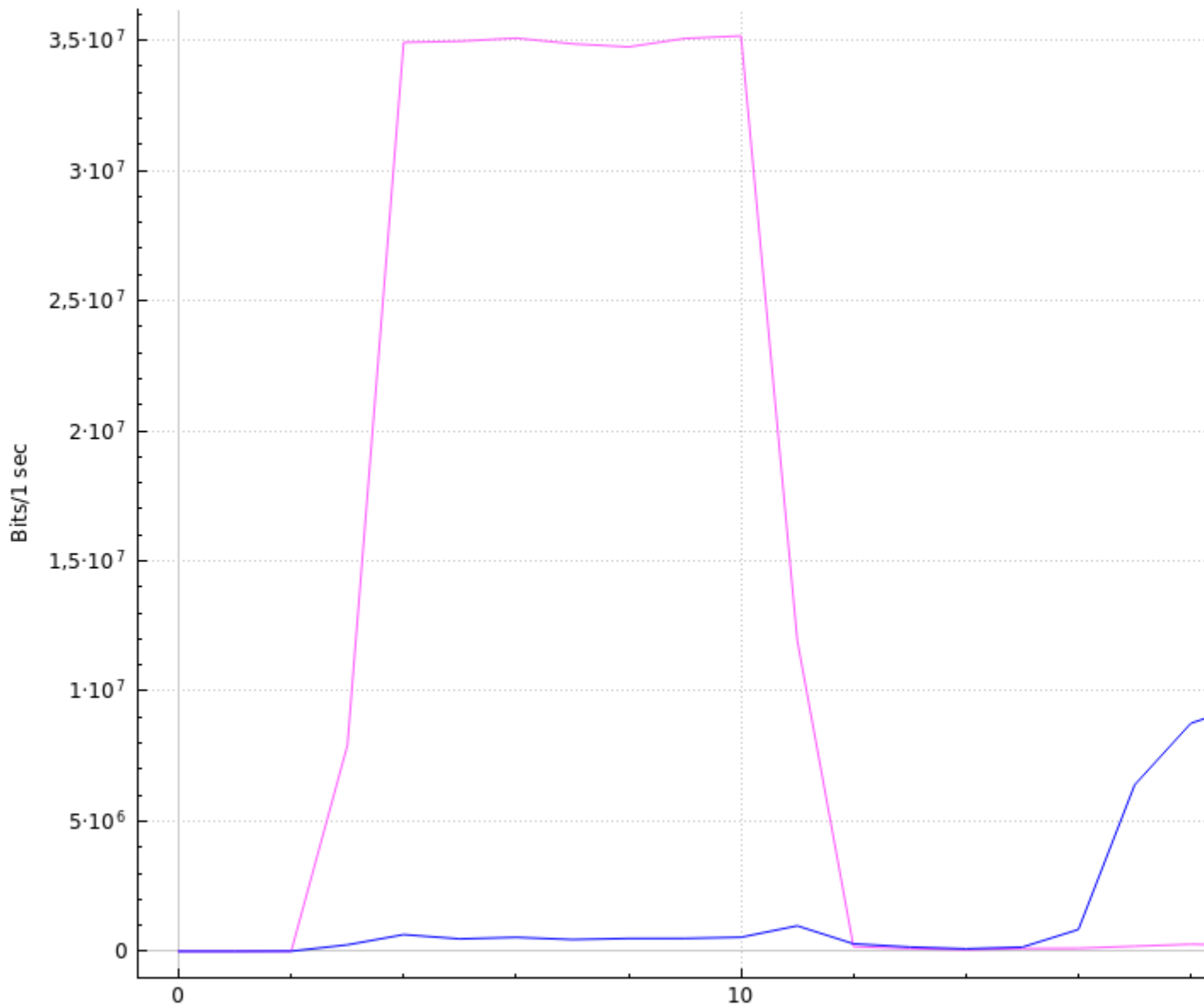
Results

From the wireshark analysis the curves describes with a good accuracy what
fast.com says, in fact the upload curve in the chart oscillates around 35 Mbsp
and the download around 9 Mbps. In conclusion the wireshark estimation is
very close to the fast.com speedtest result.