ANALISI DELLA BANDA USANDO FAST.COM (NETFLIX)

Gruppo 11: Fabio Guastapaglia, Claudio Mano, Alessio Delgadillo, Marco Cifarelli, Olti Dajce

CATTURA

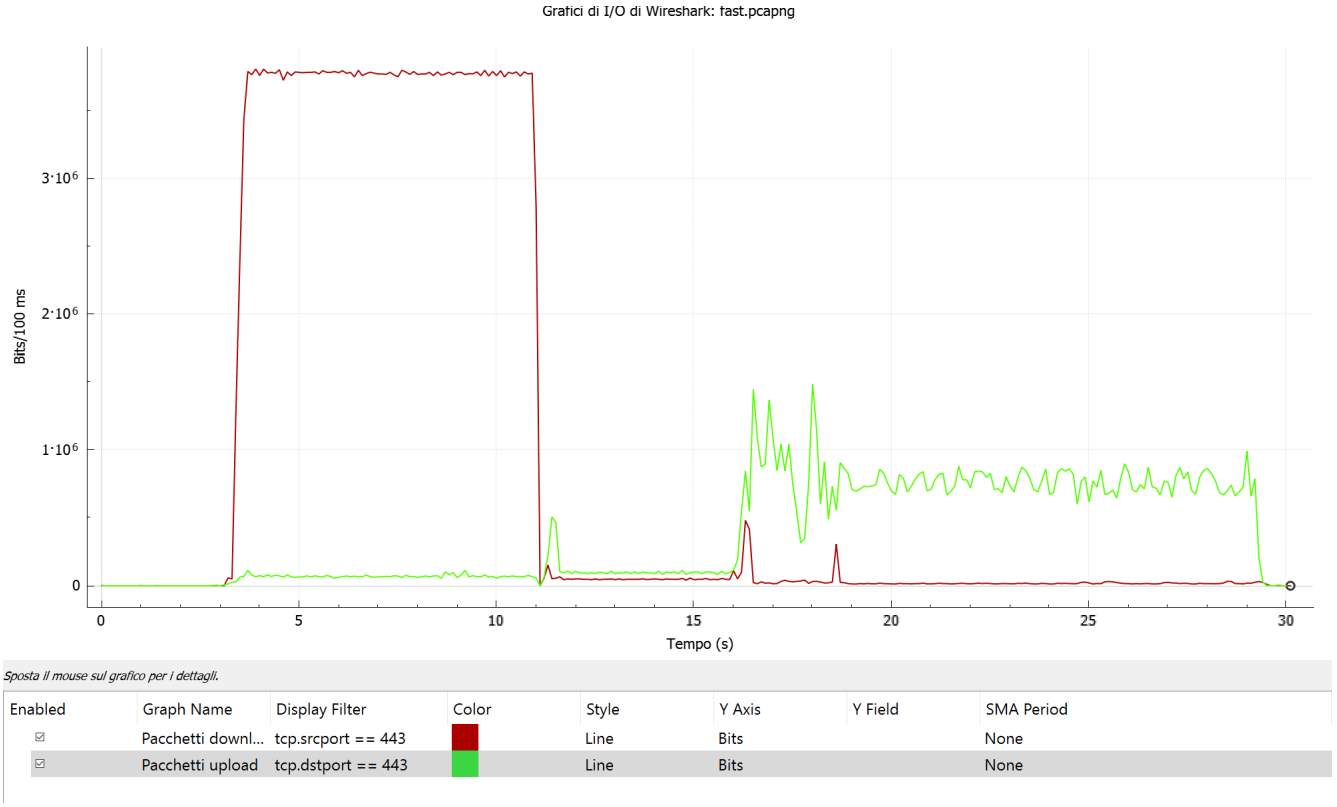
Abbiamo filtrato tutti i pacchetti TCP che utilizzano protocollo https (selezionando la porta 443 come destinazione o sorgente). Abbiamo poi avviato lo speed test ottenendo il seguente risultato:

GRAFICO DI I/O

Per analizzare il grafico di I/O abbiamo utilizzato due diversi filtri, tenendo in considerazione che la porta 443 è quella aperta dal server, mentre il nostro client comunica attraverso una porta effimera:

- **Pacchetti con porta di destinazione 443**, che ci consente di visualizzare solo quelli in upload
- **Pacchetti con porta sorgente 443**, che ci consente di visualizzare solo quelli in download

Grafico con intervallo di 100ms:



Al tempo t=3s i bit in arrivo subiscono un'impennata causata dall'apertura delle connessioni tcp fino a t=4s, dopo di che si ha una velocità costante fino al tempo t=10s per il test della velocità di download, mentre i bit in upload sono costituiti dagli ACK di risposta che vengono mandati al server. Dopodiché viene avviato il test della velocità di upload, che crea la situazione opposta, con un picco di bit in upload e una bassa quantità in download.

La velocità massima registrata da wireshark è di 37,78Mbps, leggermente superiore a quella registrata dallo speed test. Questo avviene perché lo speed test riceve solamente il payload dei pacchetti e non gli header, quindi è costretto a fare una stima non precisa della dimensione di quest'ultimi. Inoltre wireshark segnala la

ritrasmissione di 16 ACK di conferma di pacchetti ricevuti la server, ulteriore causa di una misura non precisa:

Pacchetto	Riepilogo	Gruppo	Protocollo	Conteggio
Note	This frame is a (suspected) retransmission	Sequence	TCP	16
3701	[TCP Spurious Retransmission] https(443) → 54443 [PSH, ACK] Seq=1852 Ack=518 ...	Sequence	TCP	
3793	[TCP Spurious Retransmission] https(443) → 54444 [PSH, ACK] Seq=1852 Ack=518 ...	Sequence	TCP	
3856	[TCP Spurious Retransmission] https(443) → 54443 [PSH, ACK] Seq=1852 Ack=518 ...	Sequence	TCP	
3945	[TCP Spurious Retransmission] https(443) → 54444 [PSH, ACK] Seq=1852 Ack=518 ...	Sequence	TCP	
5073	[TCP Spurious Retransmission] , Application Data	Sequence	TCP	
14849	[TCP Spurious Retransmission] , Application Data	Sequence	TCP	
19612	[TCP Spurious Retransmission] , Application Data	Sequence	TCP	
24302	[TCP Spurious Retransmission] , Application Data	Sequence	TCP	
25463	[TCP Fast Retransmission] https(443) → 54436 [ACK] Seq=4691485 Ack=1958 Win=1...	Sequence	TCP	
25544	[TCP Fast Retransmission] https(443) → 54442 [ACK] Seq=7890907 Ack=1951 Win=1...	Sequence	TCP	
27163	[TCP Fast Retransmission] https(443) → 54436 [ACK] Seq=4917997 Ack=1958 Win=1...	Sequence	TCP	
27176	[TCP Retransmission] https(443) → 54436 [ACK] Seq=4919449 Ack=1958 Win=1049...	Sequence	TCP	
27180	[TCP Retransmission] https(443) → 54436 [ACK] Seq=4920901 Ack=1958 Win=1049...	Sequence	TCP	
27192	[TCP Retransmission] https(443) → 54436 [ACK] Seq=4922353 Ack=1958 Win=1049...	Sequence	TCP	
27287	[TCP Fast Retransmission] https(443) → 54439 [ACK] Seq=8275425 Ack=1934 Win=1...	Sequence	TCP	
35740	[TCP Spurious Retransmission] , Server Hello, Change Cipher Spec, Application Data,...	Sequence	TCP	

CONNESSIONI

Tenendo traccia dei pacchetti che hanno flag SYN=1 e che partono dal client, è possibile notare che tramite il three way handshake vengono aperte 12 connessioni TCP nel momento in cui viene avviato il test di download a tempo 3 secondi

(!(tcp.flags.syn == 0)) && (ip.src == 192.168.1.12)

No.	Time	Source	Destination	Protocol	Length	Info
22	3.135001	192.168.1.12	ec2-52-31-125-224.eu-west-1.compute.amazonaws.com	TCP	66	54433 → https(443) [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
24	3.167790	192.168.1.12	ec2-52-31-125-224.eu-west-1.compute.amazonaws.com	TCP	66	54434 → https(443) [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
49	3.368463	192.168.1.12	91.81.220.13	TCP	66	54435 → https(443) [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
50	3.368520	192.168.1.12	91.81.220.13	TCP	66	54436 → https(443) [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
296	3.522729	192.168.1.12	91.81.217.23	TCP	66	54437 → https(443) [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
297	3.522801	192.168.1.12	91.81.217.23	TCP	66	54438 → https(443) [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
968	3.697658	192.168.1.12	ipv4-c051-mil001-ix.1.oca.nflxvideo.net	TCP	66	54439 → https(443) [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
969	3.697721	192.168.1.12	ipv4-c051-mil001-ix.1.oca.nflxvideo.net	TCP	66	54440 → https(443) [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
973	3.698603	192.168.1.12	ipv4-c061-mil001-ix.1.oca.nflxvideo.net	TCP	66	54441 → https(443) [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
974	3.698657	192.168.1.12	ipv4-c061-mil001-ix.1.oca.nflxvideo.net	TCP	66	54442 → https(443) [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
2311	3.974485	192.168.1.12	ipv4-c003-fra002-dev-ix.1.oca.nflxvideo.net	TCP	66	54443 → https(443) [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
2312	3.974551	192.168.1.12	ipv4-c003-fra002-dev-ix.1.oca.nflxvideo.net	TCP	66	54444 → https(443) [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
35661	11.111857	192.168.1.12	ec2-54-154-59-168.eu-west-1.compute.amazonaws.com	TCP	66	54445 → https(443) [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
35668	11.205327	192.168.1.12	91.81.220.9	TCP	66	54446 → https(443) [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
35678	11.248644	192.168.1.12	ipv4-c001-fra002-dev-ix.1.oca.nflxvideo.net	TCP	66	54447 → https(443) [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
35687	11.271829	192.168.1.12	ipv4-c007-mil001-ix.1.oca.nflxvideo.net	TCP	66	54448 → https(443) [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
35688	11.271901	192.168.1.12	ipv4-c060-fra002-ix.1.oca.nflxvideo.net	TCP	66	54449 → https(443) [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
35689	11.271958	192.168.1.12	ipv4-c046-mil001-ix.1.oca.nflxvideo.net	TCP	66	54450 → https(443) [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
37307	15.952833	192.168.1.12	40.126.31.138	TCP	66	54451 → https(443) [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
37308	15.952901	192.168.1.12	40.126.31.138	TCP	66	54452 → https(443) [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
37441	16.246953	192.168.1.12	ec2-54-154-59-168.eu-west-1.compute.amazonaws.com	TCP	66	54453 → https(443) [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
37450	16.282417	192.168.1.12	52.113.194.132	TCP	66	54454 → https(443) [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
37491	16.332098	192.168.1.12	91.81.220.11	TCP	66	54455 → https(443) [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
37492	16.332152	192.168.1.12	91.81.220.11	TCP	66	54456 → https(443) [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
37881	16.703849	192.168.1.12	91.81.217.25	TCP	66	54457 → https(443) [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
37882	16.703915	192.168.1.12	91.81.217.25	TCP	66	54458 → https(443) [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
38243	17.198296	192.168.1.12	ipv4-c061-mil001-ix.1.oca.nflxvideo.net	TCP	66	54459 → https(443) [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1

Le connessioni aperte vanno dalla porta 54433 alla 54444. Di queste 12 connessioni, quelle effettivamente usate per il test di download (nelle impostazioni di fast.com abbiamo impostato ii numero massimo ad 8) sono quelle che iniziano a tempo 3 e che sono della durata di 7-8 secondi:

Address A	Port A	Address B	Port B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s A → B	Bits/s B → A
192.168.1.12	54433	52.31.125.224	443	23	12k	11	3169	12	8999	3.135001	13.1899	1922	5458
192.168.1.12	54434	52.31.125.224	443	12	4715	6	979	6	3736	3.167790	0.2180	35k	137k
192.168.1.12	54435	91.81.220.13	443	35	12k	22	8254	13	3868	3.368463	8.1303	8121	3806
192.168.1.12	54436	91.81.220.13	443	6.071	6184k	2.034	113k	4.037	6071k	3.368520	7.7085	117k	6300k
192.168.1.12	54437	91.81.217.23	443	5.929	6048k	1.980	108k	3.949	5939k	3.522729	7.5652	115k	6281k
192.168.1.12	54438	91.81.217.23	443	39	16k	23	8162	16	8215	3.522801	8.1600	8001	8053
192.168.1.12	54439	23.246.51.153	443	10.773	11M	3.498	192k	7.275	10M	3.697658	7.3741	208k	11M
192.168.1.12	54440	23.246.51.153	443	40	15k	24	8108	16	7707	3.697721	8.1851	7924	7532

La connessione sulla porta 54434 dura pochi millisecondi, mentre le connessioni sulle porte 54433 e 54441 persistono ben oltre la durata del test, quindi probabilmente non erano coinvolte nella misurazione della velocità di download.

Per l'upload si ha una situazione analoga, con 8 connessioni che vengono aperte per l'inizio del test a tempo 15-16 secondi:

No.	Time	Source	Destination	Prot	Leng	Info
37307	15.952833	192.168.1.12	40.126.31.138	TCP	66	54451 → https(443) [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
37308	15.952901	192.168.1.12	40.126.31.138	TCP	66	54452 → https(443) [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
37441	16.246953	192.168.1.12	ec2-54-154-59-168.eu-west-1.compute.amazonaws.com	TCP	66	54453 → https(443) [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
37450	16.282417	192.168.1.12	52.113.194.132	TCP	66	54454 → https(443) [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
37491	16.332098	192.168.1.12	91.81.220.11	TCP	66	54455 → https(443) [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
37492	16.332152	192.168.1.12	91.81.220.11	TCP	66	54456 → https(443) [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
37881	16.703849	192.168.1.12	91.81.217.25	TCP	66	54457 → https(443) [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
37882	16.703915	192.168.1.12	91.81.217.25	TCP	66	54458 → https(443) [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1

Le connessioni aperte vanno dalla porta 54451 alla 54458 ed hanno una durata più variabile rispetto a quelle usate per il download:

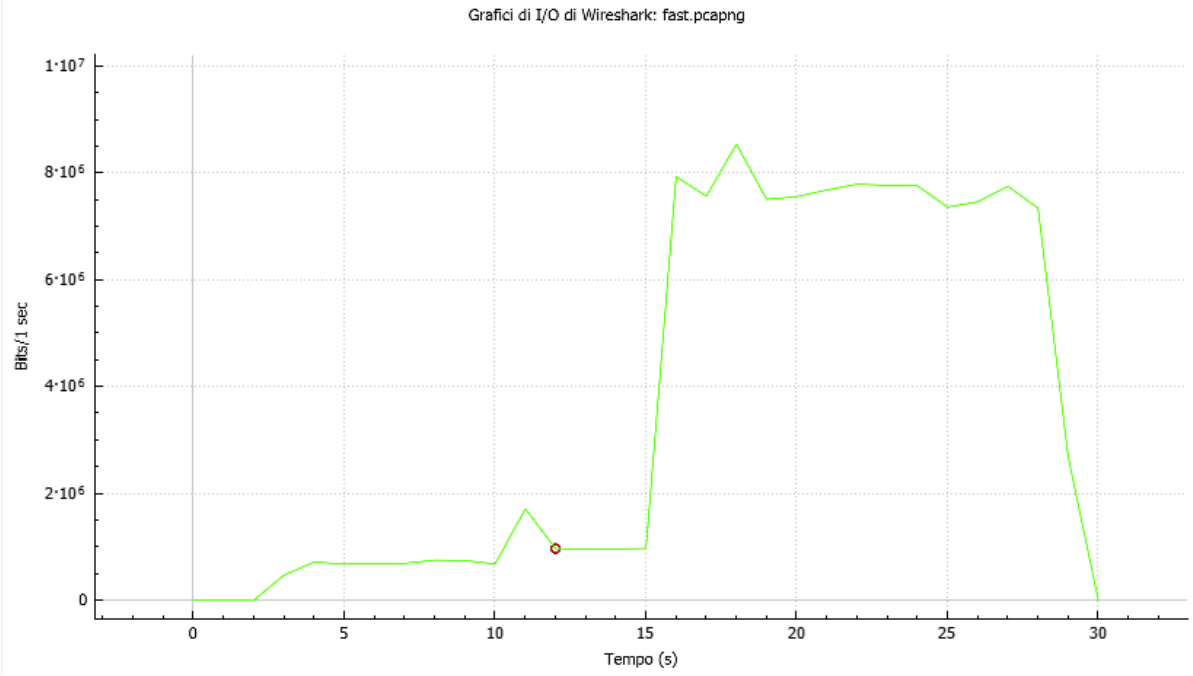
Address A	Port A	Address B	Port B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s A → B	Bits/s B → A
192.168.1.12	54451	40.126.31.138	443	23	20k	9	6630	14	13k	15.952833	0.2921	181k	366k
192.168.1.12	54452	40.126.31.138	443	24	20k	10	6673	14	13k	15.952901	0.4603	115k	234k
192.168.1.12	54453	54.154.59.168	443	13	5315	7	3751	6	1564	16.246953	0.2286	131k	54k
192.168.1.12	54454	52.113.194.132	443	157	130k	50	12k	107	118k	16.282417	2.3928	40k	395k
192.168.1.12	54455	91.81.220.11	443	3.071	4239k	1.505	4132k	1.566	106k	16.332098	13.1617	2511k	64k
192.168.1.12	54456	91.81.220.11	443	54	22k	33	12k	21	10k	16.332152	13.2081	7399	6114
192.168.1.12	54457	91.81.217.25	443	50	18k	32	12k	18	5748	16.703849	13.2119	7453	3480
192.168.1.12	54458	91.81.217.25	443	2.791	4024k	1.372	3931k	1.419	92k	16.703915	12.7963	2458k	57k

PACCHETTI RITRASMESSI IN UPLOAD

Gravità	Riepilogo	Gruppo	Protocollo	Conteggio
Note	This frame is a (suspected) retransmission	Sequence	TCP	278
38304	[TCP Retransmission] 54455 → https(443) [PSH, ACK] Seq=...	Sequence	TCP	
38307	[TCP Retransmission] 54455 → https(443) [ACK] Seq=3020...	Sequence	TCP	
38314	[TCP Retransmission] 54455 → https(443) [ACK] Seq=3035...	Sequence	TCP	
38315	[TCP Retransmission] 54455 → https(443) [ACK] Seq=3049...	Sequence	TCP	
38316	[TCP Retransmission] 54455 → https(443) [ACK] Seq=3064...	Sequence	TCP	
38322	[TCP Retransmission] 54455 → https(443) [ACK] Seq=3067...	Sequence	TCP	
38323	[TCP Retransmission] 54455 → https(443) [ACK] Seq=3081...	Sequence	TCP	
38326	[TCP Retransmission] 54455 → https(443) [ACK] Seq=3096...	Sequence	TCP	
38327	[TCP Retransmission] 54455 → https(443) [ACK] Seq=3111...	Sequence	TCP	
38333	[TCP Retransmission] 54455 → https(443) [ACK] Seq=3125...	Sequence	TCP	
38334	[TCP Retransmission] 54455 → https(443) [ACK] Seq=3140...	Sequence	TCP	
38338	[TCP Fast Retransmission] 54458 → https(443) [ACK] Seq=1...	Sequence	TCP	
38340	[TCP Retransmission] 54455 → https(443) [ACK] Seq=3154...	Sequence	TCP	
38341	[TCP Retransmission] 54455 → https(443) [PSH, ACK] Seq=...	Sequence	TCP	
38345	[TCP Retransmission] 54455 → https(443) [PSH, ACK] Seq=...	Sequence	TCP	
38346	[TCP Retransmission] 54455 → https(443) [ACK] Seq=3198...	Sequence	TCP	
38351	[TCP Retransmission] 54455 → https(443) [ACK] Seq=3212...	Sequence	TCP	
38352	[TCP Retransmission] 54455 → https(443) [ACK] Seq=3227...	Sequence	TCP	
38357	[TCP Retransmission] 54455 → https(443) [ACK] Seq=3241...	Sequence	TCP	
38358	[TCP Retransmission] 54455 → https(443) [ACK] Seq=3256...	Sequence	TCP	
38365	[TCP Retransmission] 54455 → https(443) [ACK] Seq=3270...	Sequence	TCP	
38366	[TCP Retransmission] 54455 → https(443) [ACK] Seq=3285...	Sequence	TCP	
38367	[TCP Retransmission] 54458 → https(443) [ACK] Seq=1451...	Sequence	TCP	
38368	[TCP Retransmission] 54458 → https(443) [ACK] Seq=1483...	Sequence	TCP	
38370	[TCP Retransmission] 54455 → https(443) [ACK] Seq=3299...	Sequence	TCP	
38371	[TCP Retransmission] 54455 → https(443) [ACK] Seq=3314...	Sequence	TCP	
38373	[TCP Retransmission] 54455 → https(443) [ACK] Seq=3328...	Sequence	TCP	
38374	[TCP Retransmission] 54455 → https(443) [PSH, ACK] Seq=...	Sequence	TCP	
38376	[TCP Retransmission] 54458 → https(443) [ACK] Seq=1490...	Sequence	TCP	
38377	[TCP Retransmission] 54458 → https(443) [ACK] Seq=1505...	Sequence	TCP	
38380	[TCP Retransmission] 54455 → https(443) [ACK] Seq=3424...	Sequence	TCP	
38381	[TCP Retransmission] 54455 → https(443) [ACK] Seq=3438...	Sequence	TCP	
38382	[TCP Retransmission] 54458 → https(443) [ACK] Seq=1511...	Sequence	TCP	
38383	[TCP Retransmission] 54458 → https(443) [ACK] Seq=1541...	Sequence	TCP	
38387	[TCP Retransmission] 54455 → https(443) [ACK] Seq=3453...	Sequence	TCP	
38388	[TCP Retransmission] 54455 → https(443) [ACK] Seq=3468...	Sequence	TCP	
38390	[TCP Retransmission] 54458 → https(443) [ACK] Seq=1550...	Sequence	TCP	
38392	[TCP Retransmission] 54455 → https(443) [ACK] Seq=3479...	Sequence	TCP	
38394	[TCP Retransmission] 54458 → https(443) [ACK] Seq=1560...	Sequence	TCP	
38397	[TCP Retransmission] 54455 → https(443) [ACK] Seq=3494...	Sequence	TCP	
38398	[TCP Retransmission] 54455 → https(443) [ACK] Seq=3508...	Sequence	TCP	
38399	[TCP Retransmission] 54458 → https(443) [ACK] Seq=1570...	Sequence	TCP	
38400	[TCP Retransmission] 54458 → https(443) [ACK] Seq=1585...	Sequence	TCP	
38405	[TCP Retransmission] 54455 → https(443) [PSH, ACK] Seq=...	Sequence	TCP	
38406	[TCP Retransmission] 54455 → https(443) [ACK] Seq=3524...	Sequence	TCP	
38407	[TCP Retransmission] 54458 → https(443) [ACK] Seq=1594...	Sequence	TCP	
38410	[TCP Retransmission] 54458 → https(443) [ACK] Seq=1605...	Sequence	TCP	
38414	[TCP Retransmission] 54455 → https(443) [ACK] Seq=3531...	Sequence	TCP	
38416	[TCP Retransmission] 54458 → https(443) [ACK] Seq=1615...	Sequence	TCP	
38418	[TCP Retransmission] 54455 → https(443) [ACK] Seq=3546...	Sequence	TCP	

Limitando il filtro di visualizzazione a solo i pacchetti in upload, si scopre che sono stati ritrasmessi 278 pacchetti.

Grafico upload con intervallo 1s:



I pacchetti ritrasmessi, insieme alla stima non precisa fatta dal programma di speed test, sono il motivo per cui il grafico di I/O segnala un picco massimo di 8,542mbps, quando in realtà lo speed test ha registrato una velocità di 6,6mbps.