







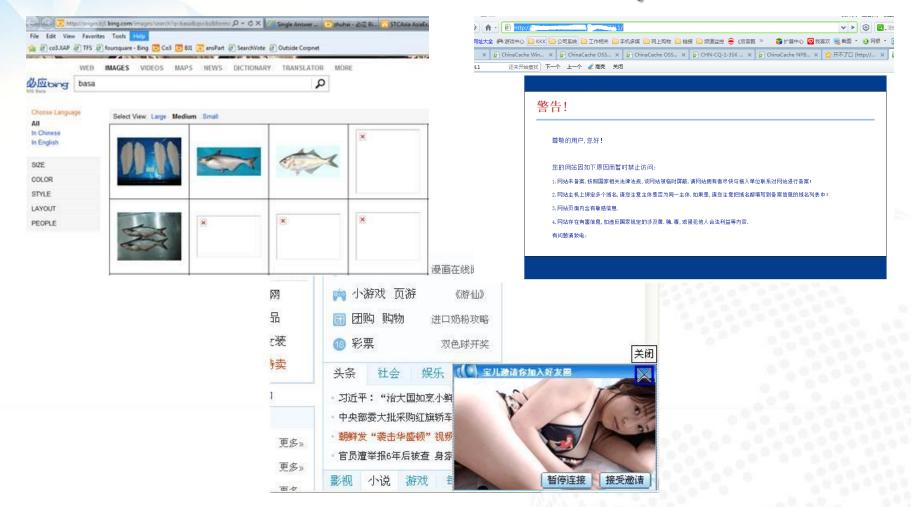
2013中国系统架构师大会 SYSTEM ARCHITECT CONFERENCE CHINA 2013

大数据下的IT架构变迁

TCP 旁路干扰技术

白金 (platinum) @ ChinaUnix weibo.com/bjpt(@白金-PT) cu.platinum@gmail.com 2013.09.05

Internet Status Quo



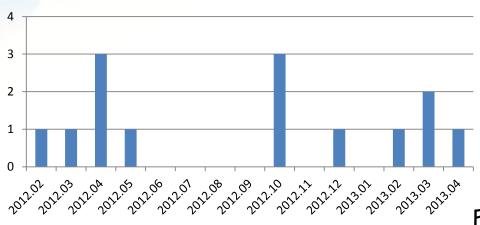






Internet Status Quo

Frequency Statistics



■干扰次数

Frequency Statistics in 2 weeks

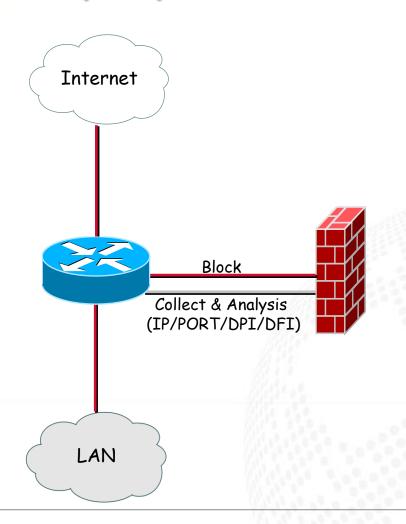








Deployment

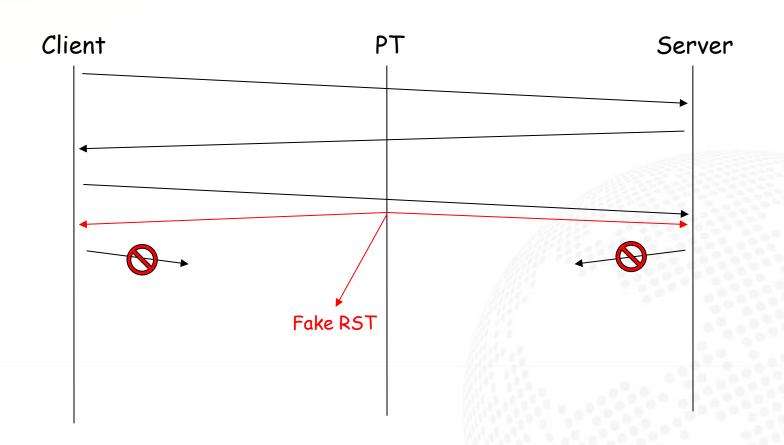








Interference Principle









RST

2 0.013 111.161. 192.168. 1TCP 66 80 > 59493 [5VN, ACK] Seq=0 Ack=1 Win=4380 Len=0 MSS=1460 30.038 192.168. 111.161. HTTP 253 GET /i/img7. 30K_D4hori6xx08gnbi46Q==/2564237037 50.091 111.161. 192.168. TCP 60 80 > 59493 [ACK] Seq=1 Ack=2 Win=4580 Len=0 60 .525 111.161. 192.168. TCP 60 80 > 59493 [ACK] Seq=1 Ack=20 Win=5504 Len=0 111.161. 192.168. TCP 290 [TCP segment of a reassembled PDU] 1		Source	Destination	Protocol Length Info
3 0.038 192.168. 111.161. TCP 54 59493 > 80 [ACK] Seq=1 ACk=1 win=4380 Len=0 4 0.078 192.168. 111.161. 192.168. TCP 60 80 > 59493 [ACK] Seq=1 Ack=200 win=5504 Len=0 6 0.525 111.161. 192.168. TCP 290 [TCP segment of a reassembled PDU] 7 0.525 111.161. 192.168. TCP 1514 [TCP segment of a reassembled PDU] 9 0.525 111.161. 192.168. TCP 1514 [TCP segment of a reassembled PDU] 10 0.526 111.161. 192.168. TCP 1514 [TCP segment of a reassembled PDU] 11.526 111.161. TCP 54 59493 > 80 [ACK] Seq=200 Ack=237 win=5452 Len=0 9 0.525 111.161. TCP 54 59493 > 80 [ACK] Seq=200 Ack=467 win=8372 Len=0 10.526 192.168. 111.161. TCP 54 59493 > 80 [ACK] Seq=200 Ack=467 win=8372 Len=0 11.527 111.161. TCP 54 59493 > 80 [ACK] Seq=200 Ack=4934 win=11292 Len=0 10.526 192.168. 111.161. TCP 54 59493 > 80 [ACK] Seq=200 Ack=4934 win=11292 Len=0 10.526 192.168. 111.161. TCP 54 59493 > 80 [ACK] Seq=200 Ack=4934 win=11292 Len=0 10.528 192.168. 111.161. TCP 54 59493 > 80 [ACK] Seq=200 Ack=4934 win=11292 Len=0 10.528 192.168. TCP 60 80 > 59493 [RST] Seq=200 Ack=4934 win=1292 Len=0 10.529 111.161. 192.168. TCP 60 80 > 59493 [RST] Seq=200 Ack=4934 win=0 Len=0 10.000 60 111.61. 192.168. TCP 60 80 > 59493 [RST] Seq=200 Ack=4934 win=0 Len=0 10.000 60 11.161. 192.168. TCP 60 80 > 59493 [RST] Seq=4394 win=0 Len=0 10.000 60 11.161. 192.168. TCP 60 80 > 59493 [RST] Seq=4394 win=0 Len=0 10.000 60 11.161. 192.168. TCP 60 80 > 59493 [RST] Seq=4394 win=0 Len=0 10.000 60 11.161. 192.168. TCP 60 80 > 59493 [RST] Seq=4394 win=0 Len=0 10.000 60 11.161. 192.168. TCP 60 80 > 59493 [RST] Seq=4394 win=0 Len=0 10.000 60 11.161. 192.168. TCP 60 80 > 59493 [RST] Seq=4394 win=0 Len=0 10.000 60 11.161. 192.168. TCP 60 80 > 59493 [RST] Seq=4394 win=0 Len=0 10.000 60 11.161. 192.168. TCP 60 80 > 59493 [RST] Seq=4394 win=0 Len=0 10.000 60 11.161. 192.168. TCP 60 80 > 59493 [RST] Seq=4394 win=0 Len=0 10.000 60 11.161. 192. 168. TCP 60 80 > 59493 [RST] Seq=4394 win=0 Len=0 10.000 60 11.161. 192. 168. TCP 60 80 > 59483 [RST] Seq=	1 0.000			
4 0.078 192.168. 111.161. 192.168. TCP 60 80 > 59493 [ACK] Seq-1 Ack-200 win-5504 Len=0 6 0.525 111.161. 192.168. TCP 290 [TCP segment of a reassembled PDU] 7 0.525 111.161. 192.168. TCP 1514 [TCP segment of a reassembled PDU] 8 0.525 192.168. 111.161. TCP 54 59493 > 80 [ACK] Seq-200 Ack-237 win-5452 Len=0 9 0.526 111.161. 192.168. TCP 1514 [TCP segment of a reassembled PDU] 9 0.526 192.168. 111.161. TCP 54 59493 > 80 [ACK] Seq-200 Ack-237 win-5452 Len=0 9 0.526 192.168. 111.161. TCP 54 59493 > 80 [ACK] Seq-200 Ack-237 win-8372 Len=0 10 0.526 192.168. 111.161. TCP 54 59493 > 80 [ACK] Seq-200 Ack-237 win-8372 Len=0 10 0.526 192.168. 111.161. TCP 54 59493 > 80 [ACK] Seq-200 Ack-234 win-1222 Len=0 10 0.528 192.168. 111.161. TCP 54 59493 > 80 [ACK] Seq-200 Ack-234 win-1222 Len=0 10 0.529 111.161. 192.168. TCP 60 80 > 59493 [RST] Seq-237 win-0 Len=0 111.161. 192.168. TCP 60 80 > 59493 [RST] Seq-237 win-0 Len=0 10 0.000 61.135. 111.161. 192.168. TCP 60 80 > 59493 [RST] Seq-2934 win-0 Len=0 10 0.000 61.135. 111.161 61.135. TCP 66 80 > 52585 > 80 [ACK] Seq-2934 win-0 Len=0 10 0.000 61.135. 111.161 61.135. TCP 66 80 > 52585 > 80 [ACK] Seq-2934 win-0 Len=0 10 0.000 61.135. 111.161 61.135. TCP 60 80 > 59493 [RST] Seq-2934 win-0 Len=0 10 0.000 61.135. 111.161 61.135. TCP 60 80 > 59493 [RST] Seq-2934 win-0 Len=0 10 0.000 61.135. 111.161 61.135. TCP 60 80 > 52585 > 80 [ACK] Seq-2934 win-0 Len=0 10 0.000 61.135. 111.161 61.135. TCP 1514 [TCP Segme No. 100 Ack 200	2 0.013	111.161.	192.168.	TCP 66 80 > 59493 [SYN, ACK] Seq=0 Ack=1 Win=4380 Len=0 MSS=1460
5 0.091 111.161. 192.168. TCP 60 80 > 59493 [ACK] Seq=1 Ack=200 win=5504 Len=0 6 0.525 111.161. 192.168. TCP 290 [TCP segment of a reassembled PDU] 8 0.525 192.168. 111.161. TCP 54 59493 > 80 [ACK] Seq=200 Ack=37 win=5452 Len=0 9 0.526 111.161. 192.168. TCP 1514 [TCP segment of a reassembled PDU] 1 0.526 192.168. 111.161. TCP 54 59493 > 80 [ACK] Seq=200 Ack=37 win=5452 Len=0 1 0.526 192.168. 111.161. TCP 54 59493 > 80 [ACK] Seq=200 Ack=37 win=372 Len=0 1 0.526 192.168. 111.161. TCP 54 59493 > 80 [ACK] Seq=200 Ack=297 win=8372 Len=0 2 0.526 192.168. 111.161. TCP 54 59493 > 80 [ACK] Seq=200 Ack=2934 win=11292 Len=0 3 0.528 192.168. 111.161. TCP 54 59493 > 80 [ACK] Seq=200 Ack=2934 win=11292 Len=0 4 0.539 111.161. 192.168. TCP 60 80 > 59493 [RST] Seq=237 win=0 Len=0 1 0.500 61.135. 111.161. 192.168. TCP 60 80 > 59493 [RST] Seq=2934 win=0 Len=0 Protocol Length Info 1 0.000 61.135. 111.161	3 0.038	192.168.	111.161.	TCP 54 59493 > 80 [ACK] Seq=1 Ack=1 Win=4380 Len=0
6 0.525 111.161. 192.168. TCP 290 [TCP segment of a reassembled PDU] 8 0.525 111.161. 192.168. TCP 54 59493 > 80 [AcK] Seq=200 Ack=237 win=5452 Len=0 0 .526 192.168. 111.161. TCP 54 59493 > 80 [AcK] Seq=200 Ack=237 win=5452 Len=0 0 .526 192.168. 111.161. TCP 54 59493 > 80 [AcK] Seq=200 Ack=237 win=5452 Len=0 10.526 192.168. 111.161. TCP 54 59493 > 80 [AcK] Seq=200 Ack=697 win=8372 Len=0 20.526 192.168. 111.161. TCP 54 59493 > 80 [AcK] Seq=200 Ack=2934 win=11292 Len=0 3 0.528 192.168. 111.161. TCP 54 59493 > 80 [AcK] Seq=200 Ack=394 win=14212 Len=0 111.161. TCP 54 59493 > 80 [AcK] Seq=200 Ack=394 win=14212 Len=0 111.161. TCP 54 59493 > 80 [AcK] Seq=200 Ack=394 win=14212 Len=0 111.161. TCP 54 59493 Seq=200 Ack=394 win=14212 Len=0 111.161. TCP 60 80 > 59493 [RST] Seq=2934 win=0 Len=0 10.000 61.135. TCP 60 80 > 59493 [RST] Seq=2934 win=0 Len=0 10.000 61.135. TCP 60 80 > 59493 [RST] Seq=2934 win=0 Len=0 111.161	4 0.078	192.168.	111.161.	HTTP 253 GET /i/img7. 50K_D4hoI6KXO8gnBi46Q==/2564237037
7 0, 525 111.161. 192.168. TCP 1514 [TCP segment of a reassembled PDU] 8 0. 525 192.168. 111.161. TCP 54 59493 > 80 [ACK] Seq=200 ACk=237 win=5452 Len=0 9 0. 525 111.161. 192.168. TCP 1291 [TCP segment of a reassembled PDU] 1 0. 526 192.168. 111.161. TCP 54 59493 > 80 [ACK] Seq=200 ACk=1697 win=8372 Len=0 1 0. 526 192.168. 111.161. TCP 54 59493 > 80 [ACK] Seq=200 ACk=2934 win=11292 Len=0 3 0. 528 192.168. 111.161. TCP 54 59493 > 80 [ACK] Seq=200 ACk=2934 win=11292 Len=0 3 0. 528 192.168. 111.161. TCP 54 59493 > 80 [ACK] Seq=200 ACk=2934 win=14292 Len=0 4 0. 539 111.161. 192.168. TCP 60 80 > 59493 [RST] Seq=200 ACk=2934 win=14212 Len=0 5 0. 540 111.161. 192.168. TCP 60 80 > 59493 [RST] Seq=2920 ACk=2934 win=0 Len=0 Time Source Destination 1 0. 000 61.135. 111.161	5 0.091	111.161.	192.168.	TCP 60 80 > 59493 [ACK] Seq=1 Ack=200 Win=5504 Len=0
8 0. 525 192. 168. 111.161. 192.168. TCP 54 \$9493 > 80 [ACK] Seq=200 Ack=237 win=5452 Len=0 90 . 525 111.161. 192.168. TCP 1114 [TCP segment of a reassembled PDU] 1 0. 526 192.168. 111.161. TCP 54 \$9493 > 80 [ACK] Seq=200 Ack=697 win=8372 Len=0 111.161. TCP 54 \$9493 > 80 [ACK] Seq=200 Ack=697 win=8372 Len=0 111.161. TCP 54 \$9493 > 80 [ACK] Seq=200 Ack=4934 win=11292 Len=0 111.161. TCP 54 \$9493 > 80 [ACK] Seq=200 Ack=4934 win=11292 Len=0 111.161. TCP 54 \$9493 > 80 [ACK] Seq=200 Ack=4934 win=11292 Len=0 111.161. TCP 54 \$9493 > 80 [ACK] Seq=200 Ack=4934 win=11292 Len=0 111.161. TCP 54 \$9493 > 80 [ACK] Seq=200 Ack=4934 win=11292 Len=0 111.161. TCP 54 \$9493 RST] Seq=1697 win=0 Len=0 111.161. TCP 54 \$9493 RST] Seq=1697 win=0 Len=0 111.161. TCP 60 80 > 59493 [RST] Seq=2934 win=0 Len=0 111.161. TCP 60 80 > 59493 [RST] Seq=2934 win=0 Len=0 111.161. TCP 60 80 > 59493 [RST] Seq=2934 win=0 Len=0 111.161. TCP 60 80 > 59493 [RST] Seq=2934 win=0 Len=0 111.161. TCP 60 80 > 59493 [RST] Seq=2934 win=0 Len=0 111.161. TCP 60 80 > 59493 [RST] Seq=2934 win=0 Len=0 111.161. TCP 60 80 > 59493 [RST] Seq=2934 win=0 Len=0 111.161. TCP 60 80 > 59493 [RST] Seq=2934 win=0 Len=0 111.161. TCP 60 80 > 59493 [RST] Seq=2934 win=0 Len=0 111.161. TCP 60 80 > 59493 [RST] Seq=2934 win=0 Len=0 111.161. TCP 60 80 > 59493 [RST] Seq=2934 win=0 Len=0 111.161. TCP 60 80 > 59493 [RST] Seq=2934 win=0 Len=0 111.161. TCP 60 80 > 59493 [RST] Seq=2934 win=0 Len=0 111.161. TCP 60 \$2585 > 80 and an analysis of the sequence of	6 0.525	111.161.	192.168.	TCP 290 [TCP segment of a reassembled PDU]
9 0.525 111.161. 192.168. TCP 1291 [TCP segment of a reassembled PDU] 1 0.526 192.168. 111.161. TCP 54 59493 > 80 [AcK] Seq=200 Ack=1697 win=8372 Len=0 2 0.526 192.168. 111.161. TCP 54 59493 > 80 [AcK] Seq=200 Ack=2934 win=11292 Len=0 3 0.528 192.168. 111.161. TCP 54 59493 > 80 [AcK] Seq=200 Ack=394 win=11292 Len=0 4 0.539 111.161. 192.168. TCP 60 80 > 59493 [RST] Seq=237 win=0 Len=0 6 0.540 111.161. 192.168. TCP 60 80 > 59493 [RST] Seq=237 win=0 Len=0 6 0.540 111.161. 192.168. TCP 60 80 > 59493 [RST] Seq=2934 win=0 Len=0 7 0.542 111.161. 192.168. TCP 60 80 > 59493 [RST] Seq=2934 win=0 Len=0 7 0.542 111.161. 192.168. TCP 60 80 > 59493 [RST] Seq=2934 win=0 Len=0 7 0.542 111.161. 192.168. TCP 60 80 > 59493 [RST] Seq=2934 win=0 Len=0 7 0.542 111.161. 192.168. TCP 60 80 > 59493 [RST] Seq=2934 win=0 Len=0 7 0.542 111.161. 192.168. TCP 60 80 > 59493 [RST] Seq=2934 win=0 Len=0 7 0.542 111.161. 192.168. TCP 60 80 > 59493 [RST] Seq=2934 win=0 Len=0 7 0.542 111.161. 192.168. TCP 60 80 > 59493 [RST] Seq=2934 win=0 Len=0 7 0.542 111.161. 192.168. TCP 60 80 > 59493 [RST] Seq=2934 win=0 Len=0 8 0.542 111.161. 192.168. TCP 60 80 > 59493 [RST] Seq=2934 win=0 Len=0 8 0.542 111.161. 192.168. TCP 60 80 > 59493 [RST] Seq=2934 win=0 Len=0 9 0.000 11.135. 111.161 11.161	7 0.525	111.161.	192.168.	TCP 1514 [TCP segment of a reassembled PDU]
0 0.526 111.161. 192.168. TCP 1514 [TCP segment of a reassembled PDU] 1 0.526 192.168. 111.161. TCP 54 59493 × 80 [AcK] Seq=200 Ack=1697 Win=8372 Len=0 2 0.526 192.168. 111.161. TCP 54 59493 × 80 [AcK] Seq=200 Ack=2934 Win=11292 Len=0 3 0.528 192.168. 111.161. TCP 54 59493 × 80 [AcK] Seq=200 Ack=394 Win=11292 Len=0 4 0.539 111.161. 192.168. TCP 60 80 × 59493 [RST] Seq=2697 Win=0 Len=0 5 0.539 111.161. 192.168. TCP 60 80 × 59493 [RST] Seq=237 Win=0 Len=0 TCP 60 80 × 59493 [RST] Seq=2394 Win=0 Len=0 TCP 60 80 × 59493 [RST] Seq=2394 Win=0 Len=0 TCP 60 80 × 59493 [RST] Seq=2394 Win=0 Len=0 TCP 60 80 × 59493 [RST] Seq=2394 Win=0 Len=0 TCP 60 80 × 59493 [RST] Seq=2394 Win=0 Len=0 TCP 60 80 × 59493 [RST] Seq=2394 Win=0 Len=0 TCP 60 80 × 59493 [RST] Seq=24394 Win=0 Len=0 TCP 74 \$2585 × 80 TCP 60 80 × 59493 [RST] Seq=24394 Win=0 Len=0 TCP 74 \$2585 × 80 TCP 60 80 × 59493 [RST] Seq=24394 Win=0 Len=0 TCP 74 \$2585 × 80 TCP 60 80 × 59493 [RST] Seq=4394 Win=0 Len=0 TCP 74 \$2585 × 80 TCP 60 80 × 59493 [RST] Seq=4394 Win=0 Len=0 TCP 74 \$2585 × 80 TCP 70 80 × 59493 [RST] Seq=4394 Win=0 Len=0 TCP 74 \$2585 × 80 TCP 70 80 × 59493 [RST] Seq=4394 Win=0 Len=0 TCP 74 \$2585 × 80 TCP 70 80 × 59493 [RST] Seq=4394 Win=0 Len=0 TCP 74 \$2585 × 80 TCP 70 80 × 59493 [RST] Seq=4394 Win=0 Len=0 TCP 74 \$2585 × 80 TCP 70 80 × 59493 [RST] Seq=4394 Win=0 Len=0 TCP 74 \$2585 × 80 TCP 70 80 × 59493 [RST] Seq=4394 Win=0 Len=0 TCP 74 \$2585 × 80 TCP 70 80 × 59493 [RST] Seq=4394 Win=0 Len=0 TCP 74 \$2585 × 80 TCP 84 80 × 52585 NOTE NOTE NOTE NOTE NOTE NOTE NOTE NOTE	8 0.525	192.168.	111.161.	TCP 54 59493 > 80 [ACK] Seq=200 Ack=237 Win=5452 Len=0
1 0.526 192.168. 111.161. TCP 54 59493 × 80 [ACK] Seq=200 Ack=1697 Win=8372 Len=0 2 0.526 192.168. 111.161. TCP 54 59493 × 80 [ACK] Seq=200 Ack=2934 Win=11292 Len=0 3 0.528 192.168. 111.161. TCP 54 59493 × 80 [ACK] Seq=200 Ack=4394 Win=14212 Len=0 4 0.539 111.161. 192.168. TCP 60 80 × 59493 [RST] Seq=237 Win=0 Len=0 5 0.539 111.161. 192.168. TCP 60 80 × 59493 [RST] Seq=237 Win=0 Len=0 6 0.540 111.161. 192.168. TCP 60 80 × 59493 [RST] Seq=237 Win=0 Len=0 7 0.542 111.161. 192.168. TCP 60 80 × 59493 [RST] Seq=237 Win=0 Len=0 Time Source Destination Protocol Length Info 1 0.000 61.135. 111.161 1 0.000	9 0.525	111.161.	192.168.	TCP 1291 [TCP segment of a reassembled PDU]
2 0.526 192.168. 111.161. TCP 54 59493 > 80 [ACK] Seq=200 Ack=2934 Win=11292 Len=0 3 0.528 192.168. 111.161. TCP 54 59493 > 80 [ACK] Seq=200 Ack=2934 Win=14212 Len=0 4 0.539 111.161. 192.168. TCP 60 80 > 59493 [RST] Seq=237 Win=0 Len=0 5 0.539 111.161. 192.168. TCP 60 80 > 59493 [RST] Seq=237 Win=0 Len=0 7 0.540 111.161. 192.168. TCP 60 80 > 59493 [RST] Seq=2934 Win=0 Len=0 7 0.540 111.161. 192.168. TCP 60 80 > 59493 [RST] Seq=2934 Win=0 Len=0 7 0.540 111.161. 192.168. TCP 60 80 > 59493 [RST] Seq=2934 Win=0 Len=0 7 0.540 111.161. 192.168. TCP 66 80 > 59493 [RST] Seq=2934 Win=0 Len=0 7 0.540 111.161. 161. 151. TCP 66 80 > 59493 [RST] Seq=2934 Win=0 Len=0 7 0.542 111.161 61.135. TCP 66 80 > 59493 [RST] Seq=2934 Win=0 Len=0 7 0.7540 111.161 61.135. TCP 66 80 > 59493 [RST] Seq=2934 Win=0 Len=0 7 0.7540 111.161 61.135. TCP 66 80 > 59493 [RST] Seq=2934 Win=0 Len=0 9 0.284 111.161 61.135. TCP 328 [TCP 60 52585 > 80	10 0.526	111.161.	192.168.	TCP 1514 [TCP segment of a reassembled PDU]
3 0.528 192.168. 4 0.539 111.161. 50.539 111.161. 192.168. TCP 60 80 > 59493 [RST] Seq=237 win=0 Len=0 111.161. 192.168. TCP 60 80 > 59493 [RST] Seq=237 win=0 Len=0 10.000 61.135. 111.161	11 0.526	192.168.	111.161.	TCP 54 59493 > 80 [ACK] Seq=200 Ack=1697 win=8372 Len=0
11.161	12 0.526	192.168.	111.161.	TCP 54 59493 > 80 [ACK] Seq=200 Ack=2934 Win=11292 Len=0
TCP 60 80 > 59493 RST Seq=1697 Win=0 Len=0	13 0.528	192.168.	111.161.	TCP 54 59493 > 80 [ACK] Seq=200 Ack=4394 Win=14212 Len=0
Time Source Destination Protocol Length Info TCP 74 52585 State St	14 0.539	111.161.	192.168.	TCP 60 80 > 59493 [RST] Seq=237 Win=0 Len=0
Time Source Destination Protocol Length Info 110.000 61.135. 2 0.000 111.161 61.135. 3 0.039 61.135. 4 0.277 61.135. 5 0.277 111.161 61.135. 6 0.282 111.161 61.135. 7 0.283 111.161 61.135. 7 0.283 111.161 61.135. 7 0.284 111.161 61.135. 8 0.284 111.161 61.135. 9 0.284 111.161 61.135. 7 0.284 111.161 61.135. 7 0.284 111.161 61.135. 7 0.284 111.161 61.135. 7 0.0000000000000000000000000000000000	15 0.539	111.161.	192.168.	TCP 60 80 > 59493 [RST] Seq=1697 Win=0 Len=0
Time Source Destination	16 0.540		192.168.	TCP 60 80 > 59493 [RST] Seq=2934 Win=0 Len=0
10.000 61.135. 2 0.000 111.161 61.135. TCP 66 80 > 52585 8C	17 0.542	111.161.	192.168.	TCP 60 80 > 59493 [RST] Seq=4394 Win=0 Len=0
10.000 61.135. 2 0.000 111.161 61.135. TCP 66 80 > 52585 File 6d View Frontes Tools File 1 File 1 Frontes Tools File 1 File	o. Time	Source	Destination	Protocol Length Info
3 0.039 61.135. 111.161 TCP 60 52585 > 80 4 0.277 61.135. 111.161 HTTP 225 GET /i/img WEB IMAGES VIDEOS MAPS NEWS DICTIONARY TRANSLATOR MORE 5 0.277 111.161 61.135. TCP 54 80 > 52585 6 0.282 111.161 61.135. TCP 328 [TCP segme Research of the	1 0.000	61.135.	111 161	TCD 74 53595 90 Interview in the property of the property of the state of the property of
3 0.039 61.135. 111.161 TCP 60 52585 > 8C 4 0.277 61.135. 111.161 HTTP 225 GET /i/img WEB IMAGES VIDEOS MAPS NEWS DICTIONARY TRANSLATOR MORE 5 0.277 111.161 61.135. TCP 54 80 > 52585 6 0.282 111.161 61.135. TCP 1514 [TCP segme 8 0.284 111.161 61.135. TCP 1514 [TCP segme 9 0.284 111.161 61.135. TCP 1514 [TCP segme 1 0.284 111.161 61.135. TCP 1514 [TCP segme 1 0.284 111.161 61.135. TCP 1514 [TCP segme 2 0.298 61.135. 111.161 TCP 60 52585 > 8C 4 0.361 61.135. 111.161 TCP 60 52585 > 8C 5 0.361 111.161 61.135. TCP 54 80 > 52585 6 0.417 61.135. 111.161 TCP 60 52585 > 8C 8 0.439 61.135. 111.161 TCP 60 52585 > 8C 9 0.439 61.135. 111.161 TCP 60 52585 > 8C 9 0.439 111.161 61.135. TCP 54 80 > 52585 9 0.439 111.161 TCP 60 52585 > 8C 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1			111.101	TCP /4 32363 > 60
5 0.277 111.161 61.135. TCP 54 80 > 52585 60.282 111.161 61.135. TCP 328 [TCP segme 10 local language 111.161 61.135. TCP 1514 [TCP segme 10 local language 111.161 61.135. TCP 1514 [TCP segme 10 local language 111.161 61.135. TCP 1514 [TCP segme 10 local language 111.161 61.135. TCP 1514 [TCP segme 10 local language 111.161 61.135. TCP 1514 [TCP segme 10 local language 111.161 61.135. TCP 1514 [TCP segme 10 local language 111.161 61.135. TCP 1514 [TCP segme 10 local language 111.161 force 111.161 forc	2 0.000			TCP 66 80 > 52585
7 0.283 111.161 61.135. TCP 1514 [TCP segme classes and continued and co	2 0.000 3 0.039	111.161	61.135.	de (a) coll YAP (a) TES (a) fournesses - Bino (a) Coll (b) Bill (c) and Part (a) Search/Vote (a) Outside Cornect
7 0.283 111.161 61.135. TCP 1514 [TCP segme classes and continued and co		111.161 61.135.	61.135. 111.161	TCP 60 52585 > 8C HTTP 225 GET /i/imc WEB IMAGES VIDEOS MAPS NEWS DICTIONARY TRANSLATOR MORE
8 0.284 111.161 61.135. TCP 1514 [TCP segme All In Chinese English Color Larguage All In 1.161 61.135. TCP 1514 [TCP segme In Chinese English In Chinese	3 0.039	111.161 61.135. 61.135.	61.135. 111.161 111.161	TCP 60 52585 > 8C HTTP 225 GET /1/img WEB IMAGES VIDEOS MAPS NEWS DICTIONARY TRANSLATOR MORE TCP 54 80 > 52585/V NUMBERS NEWS DICTIONARY TRANSLATOR MORE
9 0.284 111.161 61.135. TCP 1514 [TCP segme of the English of Chinese of Chinese of the English of Chinese of Chinese of the English of Chinese of the English of Chinese of	3 0.039 4 0.277	111.161 61.135. 61.135. 111.161	61.135. 111.161 111.161 61.135.	TCP 60 52585 > 8C HTTP 225 GET /1/img WEB IMAGES VIDEOS MAPS NEWS DICTIONARY TRANSLATOR MORE TCP 54 80 > 52585/V NUMBERS NEWS DICTIONARY TRANSLATOR MORE
0 0.284 111.161 61.135. TCP 1514 [TCP segme 1 0.284 111.161 61.135. TCP 1514 [TCP segme 1 0.298 61.135. 111.161 TCP 60 52585 > 80 30.298 61.135. 111.161 TCP 60 52585 > 80 40.361 61.135. 111.161 TCP 60 52585 > 80 50.361 111.161 61.135. TCP 54 80 > 52585 50 50 50.361 111.161 TCP 60 52585 > 80 50.361 TCP 54 80 > 52585 50.361 TCP 54 80 TC	3 0.039 4 0.277 5 0.277 6 0.282 7 0.283	111.161 61.135. 61.135. 111.161 111.161	61.135. 111.161 111.161 61.135. 61.135. 61.135.	TCP 60 52585 > 8C HTTP 225 GET /i/img WEB IMAGES VIDEOS MAPS NEWS DICTIONARY TRANSLATOR MORE TCP 54 80 > 52585 Nations basa TCP 328 [TCP segme to find the company of th
0 0.284 111.161 61.135. TCP 1514 [TCP segme 12 0.298 61.135. 111.161 TCP 60 52585 > 80 20.298 61.135. 111.161 TCP 60 52585 > 80 20.68	3 0.039 4 0.277 5 0.277 6 0.282 7 0.283 8 0.284	111.161 61.135. 61.135. 111.161 111.161 111.161 111.161	61.135. 111.161 111.161 61.135. 61.135. 61.135. 61.135.	TCP 60 52585 > 8C HTTP 225 GET /i/img
1 0.284 111.161 61.135. TCP 1514 [TCP segme 2 0.298 61.135.	3 0.039 4 0.277 5 0.277 6 0.282 7 0.283 8 0.284 9 0.284	111.161 61.135. 61.135. 111.161 111.161 111.161 111.161 111.161	61.135. 111.161 111.161 61.135. 61.135. 61.135. 61.135. 61.135.	TCP 60 52585 > 8C HTTP 225 GET /i/img WEB IMAGES VIDEOS MAPS NEWS DICTIONARY TRANSLATOR MORE TCP 54 80 > 52585 TCP 328 [TCP segme to this to the to
3 0.298 61.135.	3 0.039 4 0.277 5 0.277 6 0.282 7 0.283 8 0.284 9 0.284 10 0.284	111.161 61.135. 61.135. 111.161 111.161 111.161 111.161 111.161	61.135. 111.161 111.161 61.135. 61.135. 61.135. 61.135. 61.135. 61.135.	TCP 60 52585 > 8C
4 0.361 61.135. 111.161 TCP 60 52585 > 80 5 0.361 111.161 61.135. TCP 54 80 > 52585 6 0.417 61.135. 111.161 TCP 60 52585 > 80 7 0.417 111.161 61.135. TCP 54 80 > 52585 8 0.439 61.135. 111.161 TCP 60 52585 > 80 9 0.439 111.161 61.135. TCP 54 80 > 52585 0 0.524 61.135. 111.161 TCP 60 52585 > 80	3 0.039 4 0.277 5 0.277 6 0.282 7 0.283 8 0.284 9 0.284 10 0.284 11 0.284	111.161 61.135. 61.135. 111.161 111.161 111.161 111.161 111.161 111.161	61.135. 111.161 111.161 61.135. 61.135. 61.135. 61.135. 61.135. 61.135. 61.135.	TCP 60 52585 > 8C HTTP 225 GET /i/img TCP 54 80 > 52585 TCP 328 [TCP segme TCP 1514 [TCP segme
4 0.361 61.135. 111.161 TCP 60 52585 > 80 5 0.361 111.161 61.135. TCP 54 80 > 52585 6 0.417 61.135. 111.161 TCP 60 52585 > 80 7 0.417 111.161 61.135. TCP 54 80 > 52585 8 0.439 61.135. 111.161 TCP 60 52585 > 80 9 0.439 111.161 61.135. TCP 54 80 > 52585 0 0.524 61.135. 111.161 TCP 60 52585 > 80	3 0.039 4 0.277 5 0.277 6 0.282 7 0.283 8 0.284 9 0.284 10 0.284 11 0.284 12 0.298	111.161 61.135. 61.135. 111.161 111.161 111.161 111.161 111.161 111.161 61.135.	61.135. 111.161 111.161 61.135. 61.135. 61.135. 61.135. 61.135. 61.135. 61.135.	TCP 60 52585 > 8C HTTP 225 GET /i/img TCP 54 80 > 52585 TCP 328 [TCP segme TCP 1514 [
11.161	3 0.039 4 0.277 5 0.277 6 0.282 7 0.283 8 0.284 9 0.284 10 0.284 11 0.284 12 0.298 13 0.298	111.161 61.135. 61.135. 111.161 111.161 111.161 111.161 111.161 111.161 61.135. 61.135.	61.135. 111.161 111.161 61.135. 61.135. 61.135. 61.135. 61.135. 61.135. 111.161	TCP 60 52585 > 8C HTTP 225 GET /i/img TCP 54 80 > 52585 TCP 328 [TCP segme TCP 1514 [TCP segme TCP 1515 [TCP segme TCP 1514 [TCP segme TCP 1515 [TCP segme TCP 1515 [TCP segme TCP 1516 [TCP segme TCP 1517 [TCP segme TCP 1518 [TCP segme TCP 1518 [TCP segme TCP 1519 [TCP segme TCP 1514 [
7 0.417 111.161 61.135. TCP 54 80 > 52585 PEOPLE 8 0.439 61.135. 111.161 TCP 60 52585 > 80 9 0.439 111.161 61.135. TCP 54 80 > 52585 0 0.524 61.135. 111.161 TCP 60 52585 > 80	3 0.039 4 0.277 5 0.277 6 0.282 7 0.283 8 0.284 9 0.284 10 0.284 11 0.284 12 0.298 13 0.298 14 0.361	111.161 61.135. 61.135. 111.161 111.161 111.161 111.161 111.161 111.161 61.135. 61.135.	61.135. 111.161 111.161 61.135. 61.135. 61.135. 61.135. 61.135. 61.135. 111.161 111.161	TCP 60 52585 > 8C HTTP 225 GET /i/img TCP 54 80 > 52585 TCP 328 [TCP segme TCP 1514 [TCP segme TCP 60 52585 > 8C TC
8 0.439 61.135. 111.161 TCP 60 52585 > 80 9 0.439 111.161 61.135. TCP 54 80 > 52585 0 0.524 61.135. 111.161 TCP 60 52585 > 80	3 0.039 4 0.277 5 0.277 6 0.282 7 0.283 8 0.284 9 0.284 10 0.284 11 0.284 12 0.298 13 0.298 14 0.361 15 0.361	111.161 61.135. 61.135. 111.161 111.161 111.161 111.161 111.161 111.161 61.135. 61.135. 111.161	61.135. 111.161 111.161 61.135. 61.135. 61.135. 61.135. 61.135. 61.135. 111.161 111.161 111.161 61.135.	TCP 60 52585 > 8C HTTP 225 GET /i/imc TCP 54 80 > 52585 TCP 328 [TCP segme TCP 1514
9 0.439 111.161 61.135. TCP 54 80 > 52585 0 0.524 61.135. 111.161 TCP 60 52585 > 80	3 0.039 4 0.277 5 0.277 6 0.282 7 0.283 8 0.284 9 0.284 11 0.284 11 0.284 12 0.298 13 0.298 14 0.361 15 0.361 16 0.417	111.161 61.135. 61.135. 111.161 111.161 111.161 111.161 111.161 111.161 61.135. 61.135. 61.135.	61.135. 111.161 111.161 61.135. 61.135. 61.135. 61.135. 61.135. 61.135. 111.161 111.161 111.161 61.135.	TCP 60 52585 > 8C HTTP 225 GET /i/img TCP 54 80 > 52585 TCP 328 [TCP segme TCP 1514 [
0 0.524 61.135. 111.161 TCP 60 52585 > 80	3 0.039 4 0.277 5 0.277 6 0.282 7 0.283 8 0.284 9 0.284 11 0.284 12 0.298 13 0.298 14 0.361 15 0.361 16 0.417	111.161 61.135. 61.135. 111.161 111.161 111.161 111.161 111.161 61.135. 61.135. 61.135. 111.161 61.135.	61.135. 111.161 111.161 61.135. 61.135. 61.135. 61.135. 61.135. 61.135. 61.135. 111.161 111.161 111.161 61.135. 111.161 61.135.	TCP 60 52585 > 8C HTTP 225 GET /i/img TCP 54 80 > 52585 TCP 328 [TCP segme TCP 1514 [
	3 0.039 4 0.277 5 0.277 6 0.282 7 0.283 8 0.284 9 0.284 11 0.284 12 0.298 13 0.298 14 0.361 15 0.361 16 0.417 17 0.417 18 0.439	111.161 61.135. 61.135. 111.161 111.161 111.161 111.161 111.161 61.135. 61.135. 61.135. 111.161 61.135.	61.135. 111.161 111.161 61.135. 61.135. 61.135. 61.135. 61.135. 61.135. 61.135. 111.161 111.161 111.161 61.135. 111.161 61.135.	TCP 60 52585 > 8C HTTP 225 GET /i/img TCP 54 80 > 52585 TCP 328 [TCP segme TCP 1514 [TCP segme TCP 60 52585 > 8C TCP 60 52585 > 8C TCP 60 52585 > 8C TCP 54 80 > 52585 TCP 60 52585 > 8C TCP 54 80 > 52585 TCP 60 52585 > 8C TCP 54 80 > 52585 TCP 60 52585 > 8C TCP 54 80 > 52585 TCP 60 52585 > 8C TCP 54 80 > 52585 TCP 60 52585 > 8C TCP 54 80 > 52585 TCP 60 52585 > 8C TCP 54 80 > 52585 TCP 60 52585 > 8C TCP 54 80 > 52585 TCP 60 52585 > 8C TCP 54 80 > 52585 TCP 60 52585 > 8C
1 0.524 111.161 61.135. TCP 54 80 > 52585	3 0.039 4 0.277 5 0.277 6 0.282 7 0.283 8 0.284 10 0.284 11 0.284 12 0.298 13 0.298 14 0.361 15 0.361 16 0.417 17 0.417 18 0.439	111.161 61.135. 61.135. 111.161 111.161 111.161 111.161 111.161 111.161 61.135. 61.135. 61.135. 111.161 61.135.	61.135. 111.161 111.161 61.135. 61.135. 61.135. 61.135. 61.135. 61.135. 111.161 111.161 111.161 61.135. 111.161 61.135.	TCP 60 52585 > 8C HTTP 225 GET /i/img TCP 54 80 > 52585 TCP 328 [TCP segme TCP 1514 [TCP segme TCP 60 52585 > 8C TCP 60 52585 > 8C TCP 60 52585 > 8C TCP 54 80 > 52585 TCP 60 52585 > 8C TCP 54 80 > 52585 TCP 60 52585 > 8C TCP 54 80 > 52585
	3 0.039 4 0.277 5 0.277 6 0.282 7 0.283 8 0.284 9 0.284 11 0.284 12 0.298 13 0.298 14 0.361 15 0.361 16 0.417 17 0.417	111.161 61.135. 61.135. 111.161 111.161 111.161 111.161 111.161 111.161 61.135. 61.135. 61.135. 111.161 61.135.	61.135. 111.161 111.161 61.135. 61.135. 61.135. 61.135. 61.135. 61.135. 111.161 111.161 111.161 61.135. 111.161 61.135.	TCP 60 52585 > 80 HTTP 225 GET /i/img TCP 54 80 > 52585 TCP 328 [TCP segme TCP 1514 [TCP segme TCP 60 52585 > 80 TCP 60 52585 > 80 TCP 60 52585 > 80 TCP 54 80 > 52585 TCP 60 52585 > 80 TCP 54 80 > 52585

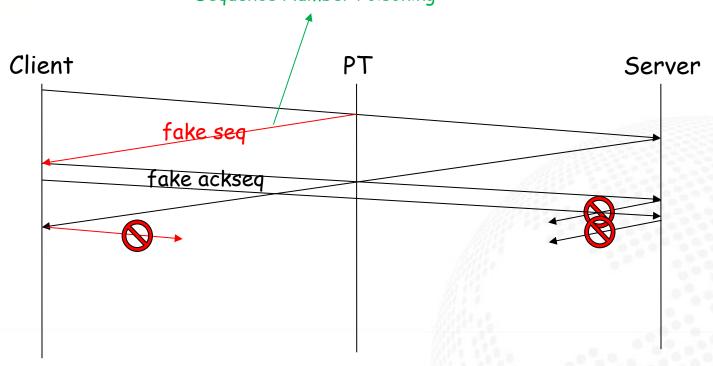






Handshake

Sequence Number Poisoning









Handshake

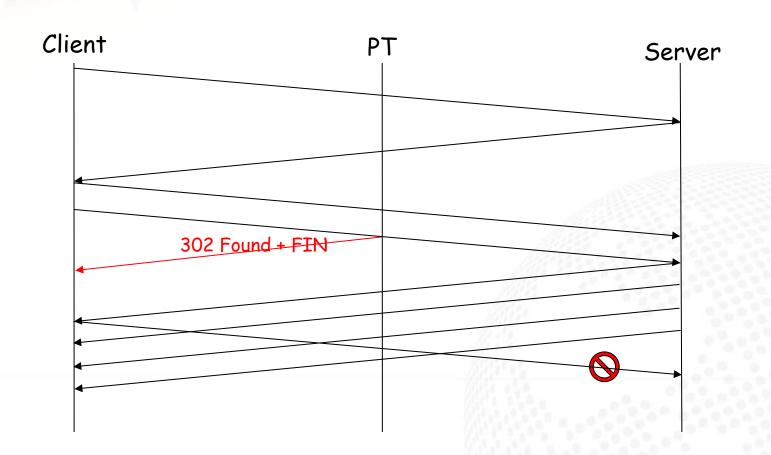
Only 53ms?!

	1	
tcp.stream eq 14		Expression Clear Apply Save
Time Source	Destination	Protocol Length Info
REF 60.5	209.1	TCP 66 49839 > 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM=1 WS=128
0.053 209.	60.5.	TCP 60 80 > 49839 [SYN, ACK] Seq=0 Ack=1 Win=579 Len=0
0.053 60.5	209.1	TCP 54 49839 > 80 [ACK] Seq=1 Ack=1 Win=65535 Len=0
0.053 60.5	209.1	HTTP 174 GET /images w.png HTTP/1.1
0.055 209.1	60.5.	TCP 60 80 > 49839 [RST, ACK] Seq=1 Ack=1 Win=580 Len=0
0.106 209.7	60.5.	TCP 60 80 > 49839 [RST] Seq=1 win=14566 Len=0
0.106 209.	60.5.	TCP 60 80 > 49839 [RST] Seq=1 Win=3703 Len=0
0.107 209.7	60.5.	TCP 60 80 > 49839 [RST, ACK] Seq=1 Ack=1 Win=581 Len=0
0.107 209.:	60.5.	TCP 60 80 > 49839 [RST, ACK] Seq=1 Ack=121 Win=583 Len=0
0.278 209.:	60.5.	TCP 66 80 > 49839 [SYN, ACK] Seq=3232500364 Ack=1 Win=65535 Len=0 MSS=1460 SACK_PERM=1 WS=12
0.279 60.5	209.1	TCP 54 49839 > 80 [RST] Seq=1 Win=0 Len=0
0.280 209.3	60.5.	TCP 60 80 > 49839 [RST, ACK] Seq=3232500365 Ack=1 Win=592 Len=0
0.329 209.	60.5.	TCP 60 80 > 49839 [RST] Seq=1 Win=0 Len=0
0.329 209.3	60.5.	TCP 60 80 > 49839 [RST] Seq=1 Win=0 Len=0
	All Control of the Co	

This is the REAL SYN/ACK sent from server! Real RTT = 278ms, not 53ms...



ISP Caching









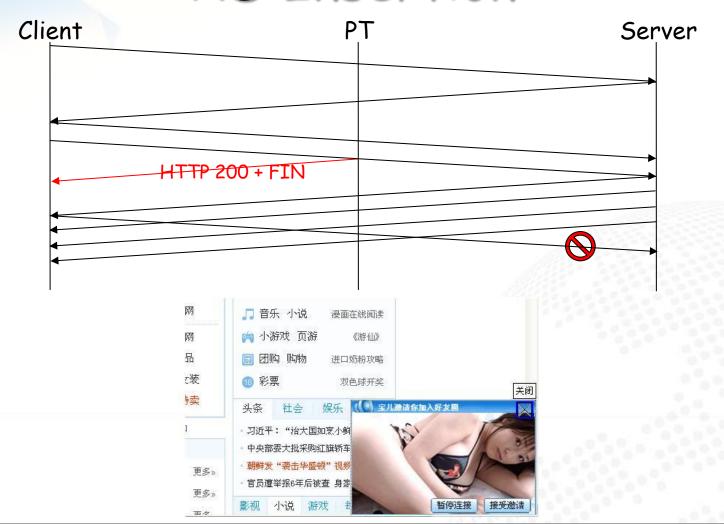
ISP Caching

```
No. Time
                             Destination
                                              Protocol Length Info
             Source
                                                         66 53455 > 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=4 SACK_PERM=1
   1 0.000
             192.168.1.100
                             123.129.214.98
                                              TCP
   2 0.049
             123.129.214.98 192.168.1.100
                                              TCP
                                                         66 80 > 53455 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1440 SACK_PERM=1 WS=128
   3 0.049
             192.168.1.100
                             123, 129, 214, 98
                                                         54 53455 > 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
                                              TCP
   4 0.050
             192.168.1.100
                                                        202 GET /gentoo/distfiles/e2fsprogs-1.42.tar.gz HTTP/1.1
                             123.129.214.98
                                              HTTP
                                              TCP
                                                        202 80 > 53455 [FIN. PSH. ACK] Seq=1 Ack=149 win=1048576 Len=148
                                                         54 53455 > 80 [ACK] Seq=149 Ack=150 Win=64092 Len=0
             192.168.1.100
                             123, 129, 214, 98
                                              TCP
   7 0.389
             123, 129, 214, 98 192, 168, 1, 100
                                              TCP
                                                         54 80 > 53455 [ACK] Seq=1 Ack=149 Win=6912 Len=0
                                             TCP
             192.168.1.100
                           123.129.214.98
                                                        54 [TCP Dup ACK 6#1] 53455 > 80 [ACK] Seq=149 Ack=150 Win=64092 Len=0
                                              TCP
                                                            [TCP Retransmission] [TCP segment of a reassembled PDU
                                              TCP
                                                      1494 [TCP segment of a reassembled PDU]
                            192,168,1,100
  11 0.537
            192.168.1.100
                           123, 129, 214, 98
                                             TCP
                                                         54 53455 > 80 [FIN, ACK] Seq=149 Ack=150 Win=64092 Len=0
            192.168.1.100
                           123.129.214.98
                                             TCP
                                                        54 [TCP Retransmission] 53455 > 80 [FIN, ACK] Seq=149 Ack=150
             123.129.214.98 192.168.1.100
                                                      1494 [TCP segment of a reassembled PDU]
                                              TCP
            123, 129, 214, 98 192, 168, 1, 100
                                                      1494 [TCP segment of a reassembled PDU]
                                              TCP
 0000
       68 5d 43 eb 30 43 e0 05
                                 c5 c0 d1 28 08 00 45 00
                                                            h]c.0c.. ...(..E.
       00 bc 66 20 00 00 37 06
                                 09 2c 7b 81 d6 62 c0 a8
                                                             ..f ..7. .,{..b..
       01 64 00 50 d0 cf 4a df
                                 2d b1 a7 7b a4 5f 50 19
 0020
       20 00 a2 70 00 00 48 54
                                 54 50 2f
                                          31 2e 31 20 33
                                                              ..p..HT TP/1.1 3
 0040
       30 32 20 46 6f 75 6e 64
                                 Od Oa 43 6f 6e 6e 65 63
                                                             02 Found ..Connec
 0050
       74 69 6f 6e 3a 20 63 6c
                                 6f 73 65 0d 0a 4c 6f 63
                                                            tion: cl ose..Loc
 0060
       61 74 69 6f 6e 3a 20 68
                                 74 74 70 3a 2f 2f 31 30
                                                            ation: h ttp://10
             30 2e 34 2e 34 2f
                                 64 6f
                                       77
                                          6e 6c 6f 61 64
                                                             .10.4.4/ download
       2f 33 30 31 31 39 39 30
 0080
                                 34 2f 33 37 38 37 34 39
                                                             <del>/3011990 4/378749</del>
       37 30 2f 33 2f 67 7a 2f
                                 31 31 33 2f 38 33 2f 31
                                                            70/3/qz/ 113/83/1
 0090
       33 34 38 39 31 30 39 30
                                 32 38 39 37 5f 35 39 35
                                                             34891090 2897_595
 00a0
 00b0
       2f 65 32 66 73 70 72 6f
                                 67 73 2d 31 2e 34 32 2e
                                                             /e2fspro qs-1.42.
 00c0
       74 61 72 2e 67 7a 0d 0a 0d 0a
                                                             tar.gz.. ..
```





AD Insertion







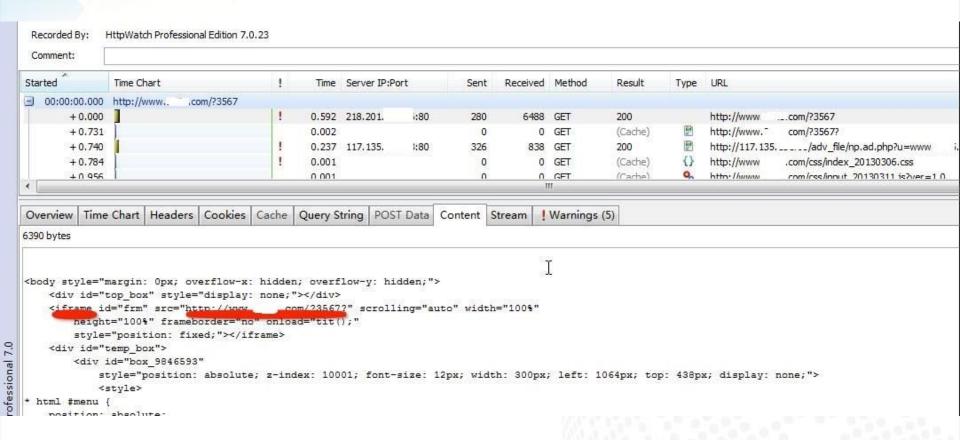
AD Insertion

No.	Time	Source	Destination	Protocol Length Info
	1 0.000	218.201.	211.151.	TCP 66 27790 > 80 [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM=1 WS=512
	2 0.062	211.151.	218.201.	TCP 60 80 > 27790 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
	3 0.062	218.201.	211.151.	TCP 54 27790 > 80 [ACK] Seq=1 Ack=1 Win=5840 Len=0
	4 0.062	218.201.	211.151.	HTTP 178 GET /?3567 HTTP/1.0
	5 0.062	211.151.	218.201.	TCP 1038 [TCP segment of a reassembled PDU]
	6 0.062	218.201.	211.151.	TCP 54 27790 > 80 [ACK] Seq=125 Ack=985 Win=6888 Len=0
	7 0.062	211.151.	218.201.	TCP 1038 [TCP segment of a reassembled PDU]
	8 0.062	218.201.	211.151.	TCP 54 27790 > 80 [ACK] Seq=125 Ack=1969 win=8856 Len=0
	9 0.063	211.151.	218.201.	TCP 1038 [TCP segment of a reassembled PDU]
1	0.063	218.201.	211.151.	TCP 54 27790 > 80 [ACK] Seq=125 Ack=2953 Win=10824 Len=0
1	1 0.063	211.151.	218.201.	TCP 1038 [TCP segment of a reassembled PDU]
1	2 0.063	218.201.	211.151.	TCP 54 27790 > 80 [ACK] Seq=125 Ack=3937 Win=12792 Len=0
1	3 0.063	211.151.	218.201.	TCP 1038 [TCP segment of a reassembled PDU]
1	4 0.063	218.201.	211.151.	TCP 54 27790 > 80 [ACK] Seq=125 Ack=4921 Win=14760 Len=0
1	5 0.063	211.151.	218.201.	TCP 1038 [TCP segment of a reassembled PDU]
1	6 0.063	218.201.	211.151.	TCP 54 27790 > 80 [ACK] Seq=125 Ack=5905 Win=16728 Len=0
1	7 0.063	211.151.	218.201.	HTTP 625 HTTP/1.0 200 OK
1	8 0.063	218.201.	211.151.	TCP 54 27790 > 80 [FIN, ACK] Seq=125 Ack=6477 Win=18696 Len=0
	9 0.124	211.151.	218.201.	TCP 60 80 > 27790 [ACK] Seq=1 Ack=125 Win=5840 Len=0
	20 0.124	218.201.	211.151.	TCP 54 [TCP Dup ACK 18#1] 27790 > 80 [ACK] Seq=126 Ack=6477 Win=18696 Len=0
	21 0.124	211.151.	218.201.	TCP 1514 [TCP Retransmission] 80 > 27790 [ACK] Seq=1 Ack=125 Win=5840 Len=1460
	22 0.124	218.201.	211.151.	TCP 54 [TCP Dup ACK 18#2] 27790 > 80 [ACK] Seq=126 Ack=6477 Win=18696 Len=0
	23 0.125	211.151.	218.201.	TCP 1514 [TCP Retransmission] 80 > 27790 [ACK] Seq=1461 Ack=125 Win=5840 Len=1460[
	24 0.125	218.201.	211.151.	TCP 54 [TCP Dup ACK 18#3] 27790 > 80 [ACK] Seq=126 Ack=6477 Win=18696 Len=0
		211.151.	218.201.	TCP 1514 [TCP Retransmission] 80 > 27790 [ACK] Seq=2921 Ack=125 Win=5840 Len=1460[
	26 0.125	218.201.	211.151.	TCP 54 [TCP Dup ACK 18#4] 27790 > 80 [ACK] Seq=126 Ack=6477 Win=18696 Len=0
	27 0.125	211.151.	218.201.	TCP 1514 [TCP Retransmission] 80 > 27790 [ACK] Seq=4381 Ack=125 Win=5840 Len=1460[
	28 0.125	218.201.	211.151.	TCP 54 [TCP Dup ACK 18#5] 27790 > 80 [ACK] Seq=126 Ack=6477 Win=18696 Len=0
	29 0.125	211.151.	218.201.	TCP 1514 [TCP Retransmission] 80 > 27790 [ACK] Seq=5841 Ack=125 Win=5840 Len=1460[
3	30 0.125	218.201.	211.151.	TCP 54 27790 > 80 [RST] Seq=125 Win=0 Len=0





AD Insertion







IP -> TTL

IPv4 Header Format

Offsets	Octet	0 1								2									3									
Oct et	Bit	0	1	2	3	4	5	6	7	8	9	11	0 11	12	13	14	15	16	17 18 19 20 21 22 23 24 25 26 27 28 29 30								30	31
0	0	Version IHL DSCP ECN Total Length																										
4	32	Identification Flags Fragment Offset																										
8	64	Time To Live Protocol Header Checksum																										
12	96		Source IP Address																									
16	128	Destination IP Address																										
20	160	Options (if IHL > 5)																										

Windows: 128 FreeBSD: 64

Linux: previous 255, now 64 Solaris: previous 255, now...?

Cisco Router: previous 255, now @#%^!~@&







IP -> TTL

```
[root@Centos-6 ~]# for ((i=79;i>0;i--)); do sysctl net.ipv4.ip default ttl=$i; sleep 1; done
net.ipv4.ip_default_ttl = 79
                                                                                                  _ D X
                             ■ 管理员: C:\Windows\system32\cmd.exe
net.ipv4.ip default ttl = 78
                             Microsoft Windows [版本 6.1.7601]
net.ipv4.ip default ttl = 77
                             版权所有(c)2009 Microsoft Corporation。保留所有权利。
net.ipv4.ip default ttl = 76
net.ipv4.ip default ttl = 75
                             C:\Users\PT>ping 192.168.80.132
net.ipv4.ip_default_ttl = 74
net.ipv4.ip default ttl = 73
                             正在 Ping 192.168.80.132 具有 32 字节的数据:
net.ipv4.ip default ttl = 72
                             来自 192.168.80.132 的回复: 字节=32 时间<1ms TTL=64
net.ipv4.ip default ttl = 71
                             |来首 192.168.80.132 的回复: 字节=32 时间<1ms TTL=63
                             来自 192.168.80.132 的回复: 字节=32 时间<1ms TTL=62
net.ipv4.ip default ttl = 70
                             来自 192.168.80.132 的回复: 字节=32 时间<1ms TTL=61
net.ipv4.ip_default_ttl = 69
net.ipv4.ip default ttl = 68
                             192.168.80.132 的 Ping 统计信息:
net.ipv4.ip default ttl = 67
                             数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 <0% 丢失>,
往返行程的估计时间<以毫秒为单位>:
最短 = 0ms, 最长 = 0ms, 平均 = 0ms
net.ipv4.ip default ttl = 66
net.ipv4.ip default ttl = 65
net.ipv4.ip default ttl = 64
net.ipv4.ip default ttl = 63
                             C: Wsers \PT>
net.ipv4.ip default ttl = 62
net.ipv4.ip default ttl = 61
net.ipv4.ip default ttl = 60
net.ipv4.ip default ttl = 59
net.ipv4.ip default ttl = 58
net.ipv4.ip default ttl = 57
net.ipv4.ip default ttl = 56
net.ipv4.ip default ttl = 55
[root@Centos-6 ~]#
```



How to resolve it?

	Protocol Length Info				
	TCP 74 52585 > 80 [SYN]		DI Length Info 74 52585 > 80 [SYN] 66 80 > 52585 [SYN, 60 52585 > 80 [ACK] 225 GET ///img3.ph.1 54 80 > 52585 [ACK] 328 [TCP segment of 1514 [TCP segment of		
	TCP 66 80 > 52585 [SYN,	_			
	TCP 60 52585 > 80 [ACK]	D			
	HTTP 225 GET /i/img3.pc-1	7 <i>F</i>			
	TCP 54 80 > 52585 [ACK]	' 1005	4.4		
	TCP 328 [TCP segment of	793			
	TCP 1514 [TCP segment of		The state of		
	TCINo. Time Source		ol Length Info	Y	
	TCI 1 0.000 61.135.	111.161 TCP	74 52585 > 80 [SYN]		
	TCI 2 0.000 111.161 TCI 3 0.039 61.135.	61.135. TCP 111.161 TCP	66 80 > 52585 [SYN, 60 52585 > 80 [ACK]		
	TCI 4 0.277 61.135.	111.161 HTTP	225 GET /i/img3.ph.1	* /	
	TCI 5 0.277 111.161	61.135. TCP	54 80 > 52585 [ACK]		
	TCI 6 0.282 111.161	61.135. TCP	328 [TCP segment of		* / 7
	TC 7 0.283 111 161 C C	61.135. TCP	1514 [TCP segment of		
	TCI 8 0.284 111 VA	61.135. TCP	No. Time Source	Destination	Protocol Length Info
17 0.417 111.161 61.135.	TCI 9 0.284 111.161	61.135. TCP	1 0.000 61.135.	111.161	TCP 74 52585 > 80 [SYN]
4	10 0.284 111.161	61.135. TCP	2 0.000 111.161	61.135.	TCP 66 80 > 52585 [SYN,
	11 0.284 111.161	61.135. TCP	3 0.039 61.135.	111.161	TCP 60 52585 > 80 [ACK]
⊕ Frame 1: 74 bytes on wire (592 bits), 74 b		111.161 TCP	4 0.277 61.135.	111.161	HTTP 225 GET /i/img3.ph.1
⊕ Ethernet II, Src: JuniperN_a5:4c:80 (84:18	13 0.298 61.135.	111.161 TCP	5 0.277 111.161	61.135.	TCP 54 80 > 52585 [ACK]
☐ Internet Protocol Version 4, Src: Version: 4	14 0.361 61.135.	111.161 TCP	6 0.282 111.161	UD 135	TCP 328 [TCP segment of
Header length: 20 bytes	15 0.361 111.161	61.135. TCP	7 0.283 111.161	(1.135.) h	TCP 1514 [TCP segment of
⊕ Differentiated Services Field: 0x00 (DSC	16 0.417 61.135.	111.161 TCP	8 0.284 111.161	61.135.	TOTAL 1514 [TCP segment of
Total Length: 60	17 0.417 111.161	61.135. TCP	9 0.284 111.161	61.135.	TCP 1514 [TCP segment of
Identification: 0x00f8 (248)	*		10 0.284 111.161	61.135.	TCP 1514 [TCP segment of
⊕ Flags: 0x02 (Don't Fragment)	⊕ Frame 4: 225 bytes on wi	re (1800 hits) 225 hyt	11 0.284 111.161	61.135.	TCP 1514 [TCP segment of
Fragment offset: 0	Ethernet II, Src: Junipe		12 0.298 01.133.	111.161	TCP 60 52585 > 80 [RST]
Time to live: 53	☐ Internet Protocol Version		13 0.298 61.135.	111.161	TCP 60 52585 > 80 [RST]
Protocol: TCP (6)	Version: 4	,	14 0.361 61.135.	111.161	TCP 60 52585 > 80 [ACK]
	Header length: 20 byte	s	15 0.361 111.161	61.135.	TCP 54 80 > 52585 [RST]
	⊕ Differentiated Services		16 0.417 61.135. 17 0.417 111.161	111.161	TCP 60 52585 > 80 [ACK] TCP 54 80 > 52585 [RST]
	Total Length: 211		1/ 0.41/ 111.161	61.135.	TCP 54 80 > 52585 [RST]
	Identification: 0x00fa		•		
	⊕ Flags: 0x02 (Don't Fra	gment)	⊕ Frame 12: 60 bytes on w	ire (480 bits), 6	00 bytes captured (480 bits)
	Fragment offset: 0				18:88:a5:4c:80), Dst: Xensourc_
	Time to live: 53		□ Internet Protocol Version		, Dst: 1
	Protocol: TCP (6)		Version: 4		
			Header length: 20 byte	es	
				es Field: 0x00 (D	SCP 0x00: Default; ECN: 0x00: N
			Total Length: 40		
A	الحاء عمر محما عصمه	امام	Identification: 0x0000		
And more a	complex met	noas	⊕ Flags: 0x02 (Don't Fra	agment)	
,			Fragment offset: 0		
			Time to live: 55		
			Protocol: TCP (6)		







Our AI

Anti-Interference Test

```
| For((i=0;i<10;i++));do wget -0 /dev/null 'http://www.goog %2F32 1.shtml&ei=yk9-UL-2JkmUiQfz8oH4Dg&usg=AFQjCNE7W-0oW9ygJlhnZ0hjeQzuzFqhyg&s 2012-10-17 15:44:14 ERROR 502: Bad Gateway. 2012-10-17 15:44:14 ERROR 502: Bad Gateway. 2012-10-17 15:44:15 ERROR 502: Bad Gateway. 2012-10-17 15:44:16 ERROR 502: Bad Gateway.
```

```
2012-10-17 15:44:16 ERROR 502: Bad Gateway.
2012-10-17 15:44:16 ERROR 502: Bad Gateway.
[root@ ~]# service AI start

Starting AI:
[root@ ~]# for((i=0;i<10;i++));do wget -0 /dev/null 'http://www.goog %2F32 1.shtml&ei=yk9-UL-2JKmUiQfz8oH4Dg&usg=AFQjCNE7W-0oW9ygJlhnZ0hjeQzuzFqhyg&s 2012-10-17 15:44:23 (108 MB/s) - `/dev/null' saved [464]
2012-10-17 15:44:25 (118 MB/s) - `/dev/null' saved [464]
2012-10-17 15:44:25 (87.4 MB/s) - `/dev/null' saved [464]
```





Reference

http://en.wikipedia.org/wiki/IPv4_header#Header

http://seclists.org/nmap-announce/1999/326

http://www.map.meteoswiss.ch/map-doc/ftp-probleme.htm

http://www.binbert.com/blog/2009/12/default-time-to-live-ttl-values/

http://en.wikipedia.org/wiki/Wireshark

http://web.eecs.umich.edu/~zhiyunq/tcp_sequence_number_inference/





Thanks!







Q&A