SACC

卓越 5周年 变迁

2013中国系统架构师大会

SYSTEM ARCHITECT CONFERENCE CHINA 2013

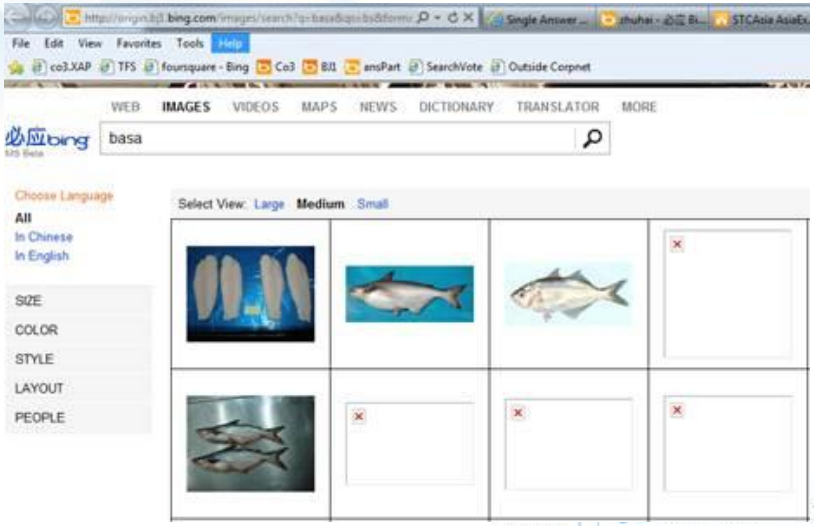
大数据下的IT架构变迁

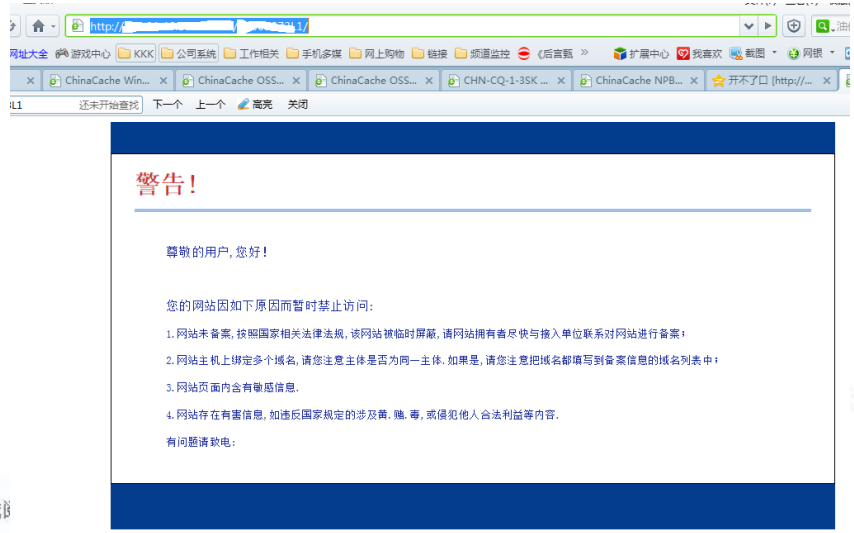
TCP 旁路干扰技术

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

2013.09.05

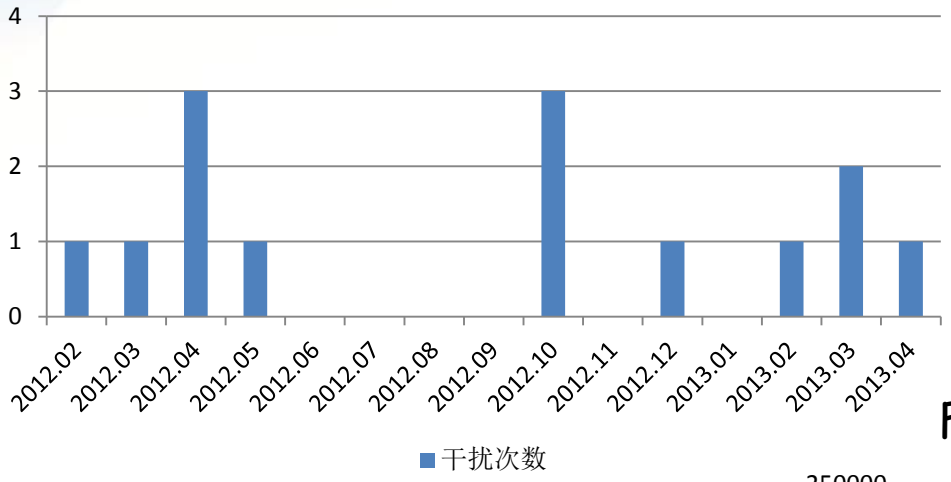
Internet Status Quo



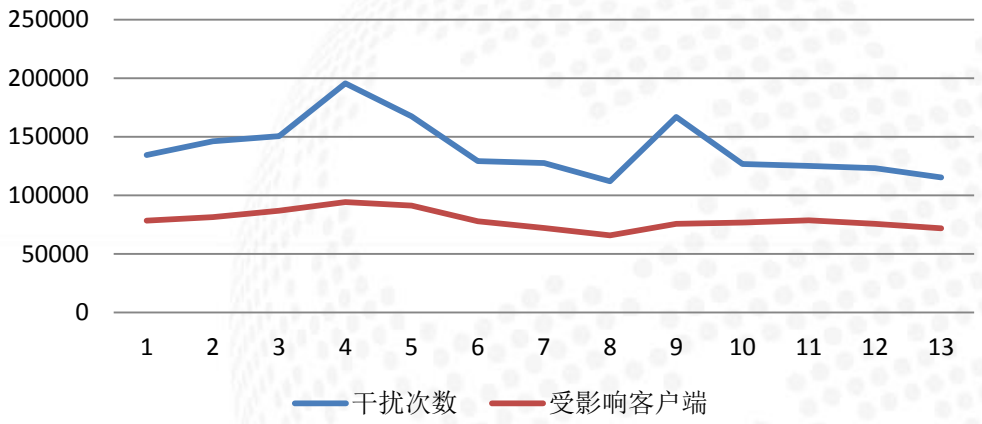


Internet Status Quo

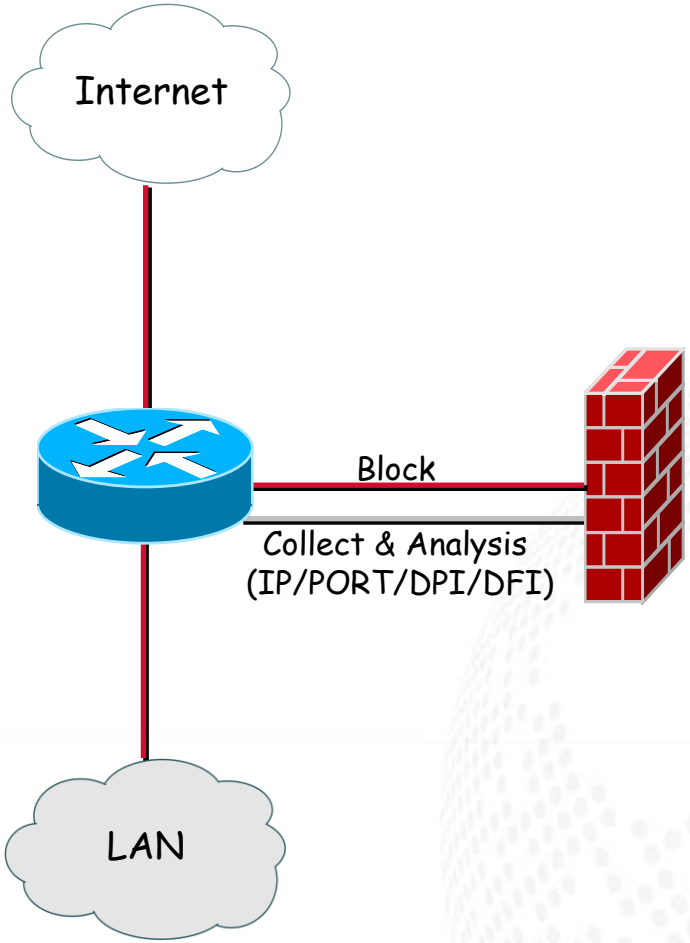
Frequency Statistics



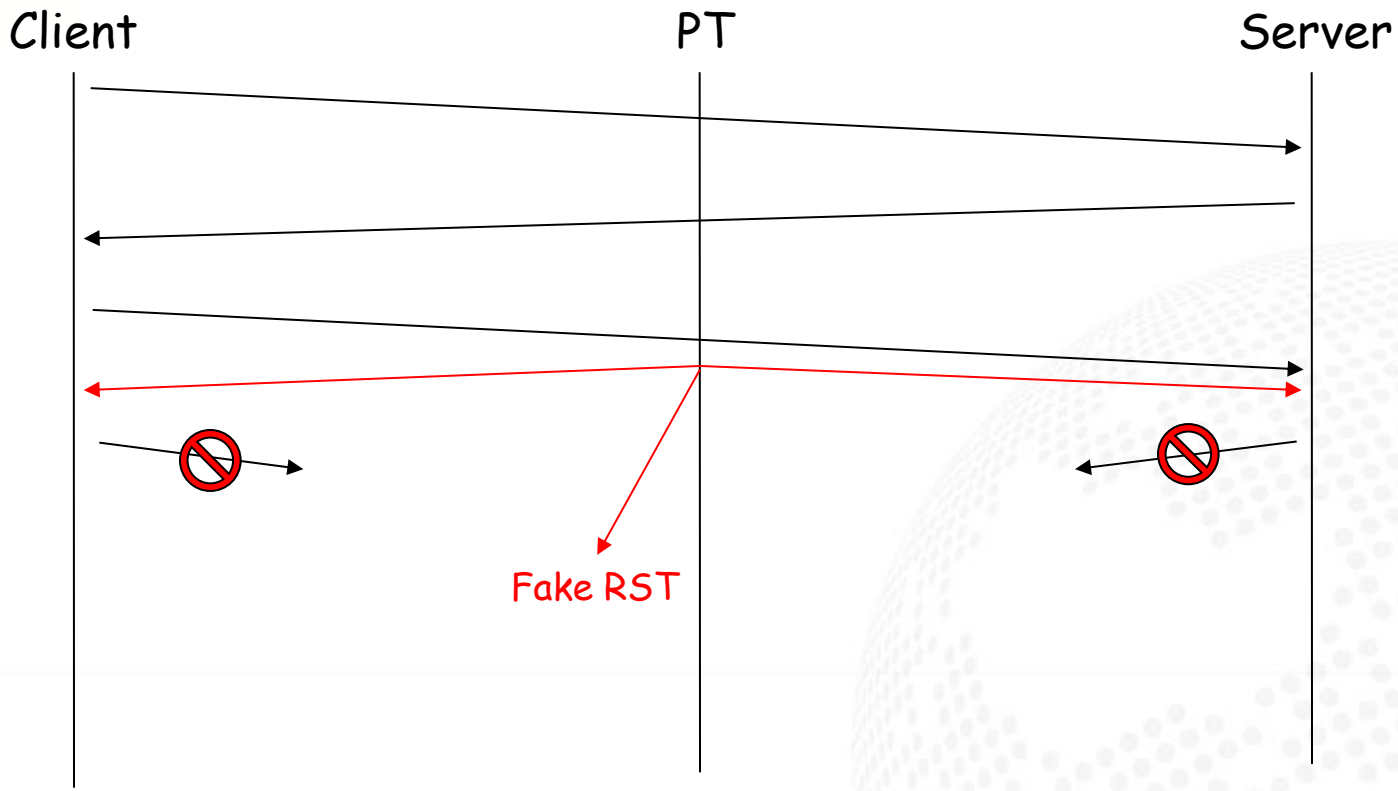
Frequency Statistics in 2 weeks



Deployment



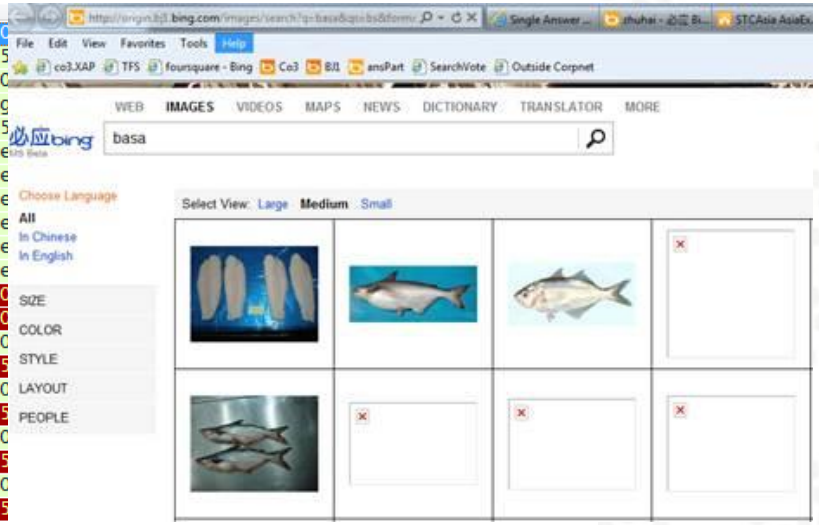
Interference Principle



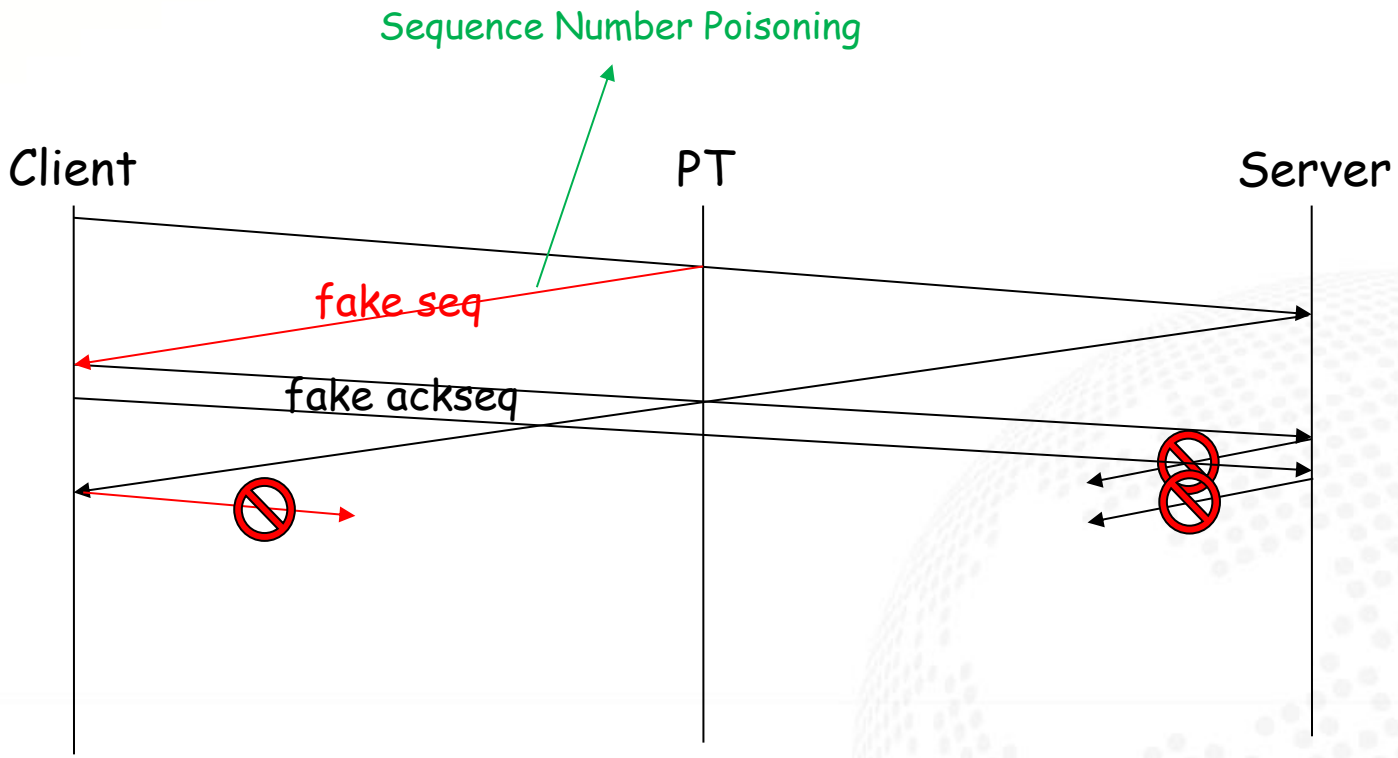
RST

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000	192.168.	111.161.	TCP	74	59493 > 80 [SYN] Seq=0 Win=4380 Len=0 MSS=1460 SACK_PERM=1
2	0.013	111.161.	192.168.	TCP	66	80 > 59493 [SYN, ACK] Seq=0 Ack=1 Win=4380 Len=0 MSS=1460
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.	HTTP	253	GET /i/img7. 50K_D4hoI6KXO8gnBi46Q==/2564237037
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]
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]
10	0.526	111.161.	192.168.	TCP	1514	[TCP segment of a reassembled PDU]
11	0.526	192.168.	111.161.	TCP	54	59493 > 80 [ACK] Seq=200 Ack=1697 Win=8372 Len=0
12	0.526	192.168.	111.161.	TCP	54	59493 > 80 [ACK] Seq=200 Ack=2934 Win=11292 Len=0
13	0.528	192.168.	111.161.	TCP	54	59493 > 80 [ACK] Seq=200 Ack=4394 Win=14212 Len=0
14	0.539	111.161.	192.168.	TCP	60	80 > 59493 [RST] Seq=237 Win=0 Len=0
15	0.539	111.161.	192.168.	TCP	60	80 > 59493 [RST] Seq=1697 Win=0 Len=0
16	0.540	111.161.	192.168.	TCP	60	80 > 59493 [RST] Seq=2934 Win=0 Len=0
17	0.542	111.161.	192.168.	TCP	60	80 > 59493 [RST] Seq=4394 Win=0 Len=0

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000	61.135.	111.161	TCP	74	52585 > 80
2	0.000	111.161	61.135.	TCP	66	80 > 52585
3	0.039	61.135.	111.161	TCP	60	52585 > 80
4	0.277	61.135.	111.161	HTTP	225	GET /i/img
5	0.277	111.161	61.135.	TCP	54	80 > 52585
6	0.282	111.161	61.135.	TCP	328	[TCP segme
7	0.283	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
10	0.284	111.161	61.135.	TCP	1514	[TCP segme
11	0.284	111.161	61.135.	TCP	1514	[TCP segme
12	0.298	61.135.	111.161	TCP	60	52585 > 80
13	0.298	61.135.	111.161	TCP	60	52585 > 80
14	0.361	61.135.	111.161	TCP	60	52585 > 80
15	0.361	111.161	61.135.	TCP	54	80 > 52585
16	0.417	61.135.	111.161	TCP	60	52585 > 80
17	0.417	111.161	61.135.	TCP	54	80 > 52585
18	0.439	61.135.	111.161	TCP	60	52585 > 80
19	0.439	111.161	61.135.	TCP	54	80 > 52585
20	0.524	61.135.	111.161	TCP	60	52585 > 80
21	0.524	111.161	61.135.	TCP	54	80 > 52585

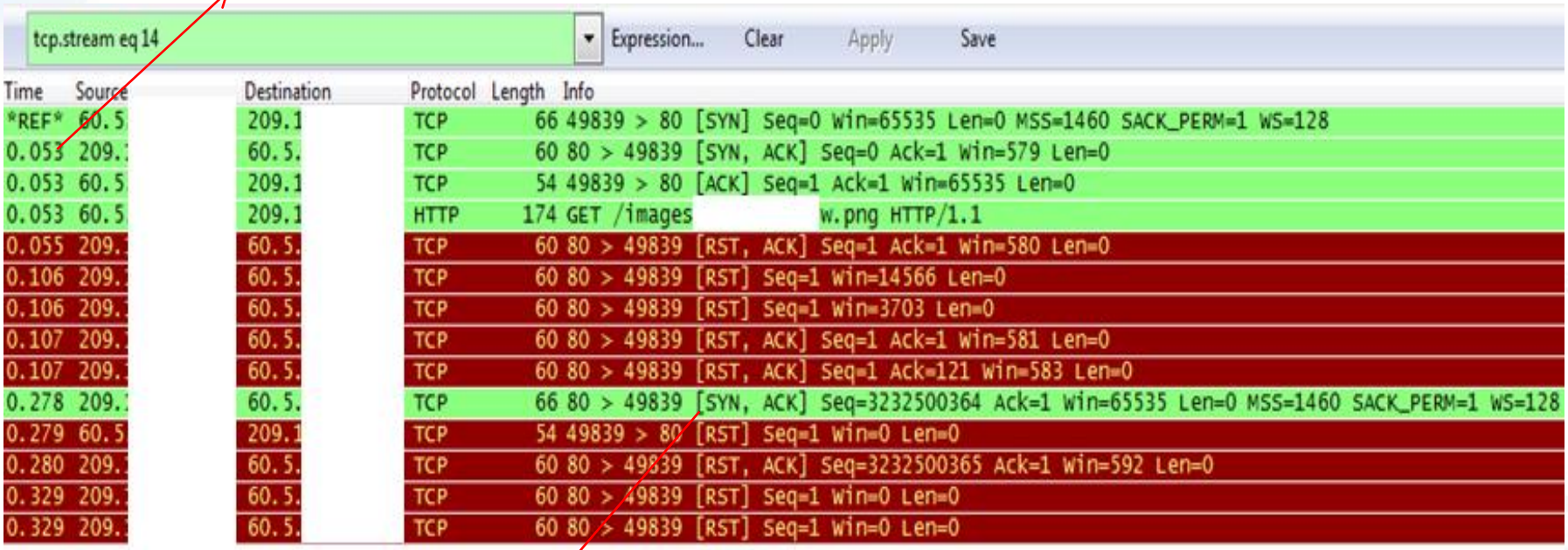


Handshake


Sequence Number Poisoning
Client
PT
Server
fake seq
fake ackseq

Handshake

Only 53ms?!

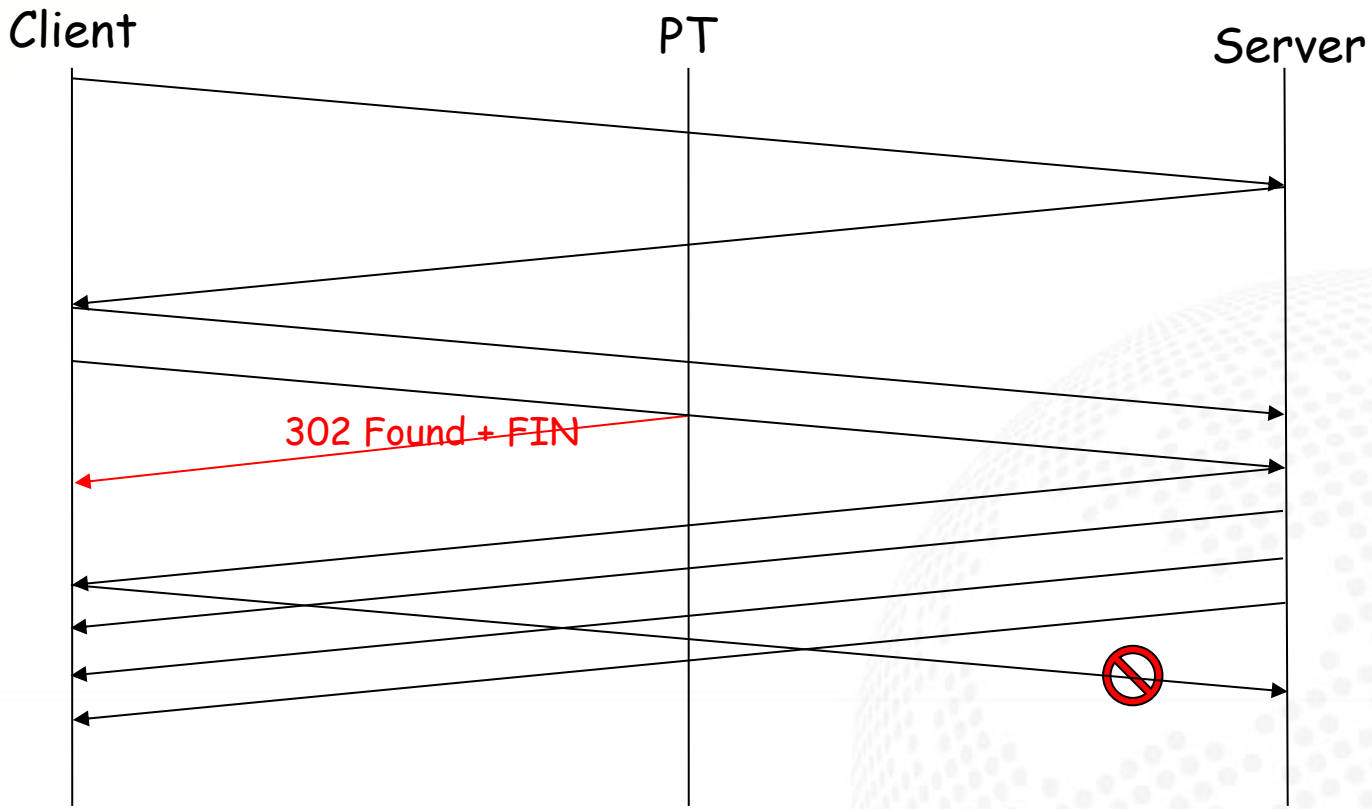


tcp.stream eq 14 | Expression... | Clear | Apply | Save

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.	60.5.	TCP	60	80 > 49839 [RST, ACK] Seq=1 Ack=1 Win=580 Len=0
0.106	209.	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.	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=128
0.279	60.5	209.1	TCP	54	49839 > 80 [RST] Seq=1 Win=0 Len=0
0.280	209.	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.	60.5.	TCP	60	80 > 49839 [RST] Seq=1 Win=0 Len=0

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

ISP Caching

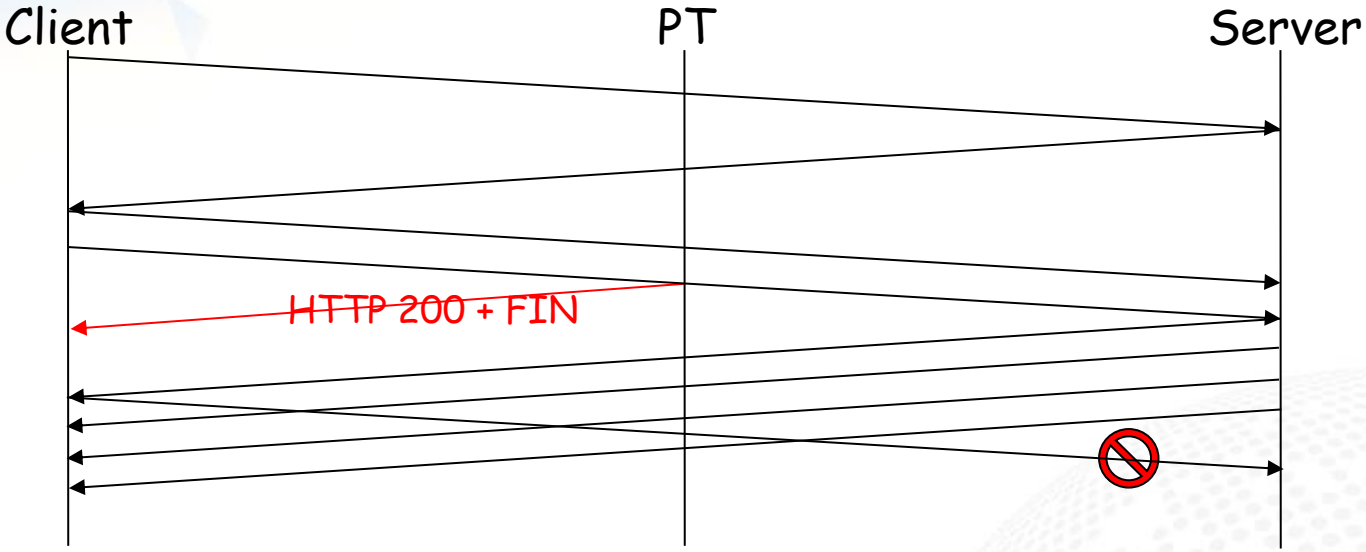


ISP Caching

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000	192.168.1.100	123.129.214.98	TCP	66	53455 > 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=4 SACK_PERM=1
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	TCP	54	53455 > 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
4	0.050	192.168.1.100	123.129.214.98	HTTP	202	GET /gentoo/distfiles/e2fsprogs-1.42.tar.gz HTTP/1.1
5	0.056	123.129.214.98	192.168.1.100	TCP	202	80 > 53455 [FIN, PSH, ACK] Seq=1 Ack=149 Win=1048576 Len=148
6	0.056	192.168.1.100	123.129.214.98	TCP	54	53455 > 80 [ACK] Seq=149 Ack=150 Win=64092 Len=0
7	0.389	123.129.214.98	192.168.1.100	TCP	54	80 > 53455 [ACK] Seq=1 Ack=149 Win=6912 Len=0
8	0.389	192.168.1.100	123.129.214.98	TCP	54	[TCP Dup ACK 6#1] 53455 > 80 [ACK] Seq=149 Ack=150 Win=64092 Len=0
9	0.392	123.129.214.98	192.168.1.100	TCP	289	[TCP Retransmission] [TCP segment of a reassembled PDU]
10	0.407	123.129.214.98	192.168.1.100	TCP	1494	[TCP segment of a reassembled PDU]
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
12	0.839	192.168.1.100	123.129.214.98	TCP	54	[TCP Retransmission] 53455 > 80 [FIN, ACK] Seq=149 Ack=150 Win=64092 Len=0
13	1.430	123.129.214.98	192.168.1.100	TCP	1494	[TCP segment of a reassembled PDU]
14	1.560	123.129.214.98	192.168.1.100	TCP	1494	[TCP segment of a reassembled PDU]

```
0000  68 5d 43 eb 30 43 e0 05  c5 c0 d1 28 08 00 45 00   h]C.0C.. ...(..E.
0010  00 bc 66 20 00 00 37 06  09 2c 7b 81 d6 62 c0 a8   ..f ..7. .,{..b..
0020  01 64 00 50 d0 cf 4a df  2d b1 a7 7b a4 5f 50 19   .d.P..J. -..{._P.
0030  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  0d 0a 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
0070  2e 31 30 2e 34 2e 34 2f  64 6f 77 6e 6c 6f 61 64   .10.4.4/ download
0080  2f 33 30 31 31 39 39 30  34 2f 33 37 38 37 34 39   /3011990 4/378749
0090  37 30 2f 33 2f 67 7a 2f  31 31 33 2f 38 33 2f 31   70/3/gz/ 113/83/1
00a0  33 34 38 39 31 30 39 30  32 38 39 37 5f 35 39 35   34891090 2897_595
00b0  2f 65 32 66 73 70 72 6f  67 73 2d 31 2e 34 32 2e   /e2fspro gs-1.42.
00c0  74 61 72 2e 67 7a 0d 0a  0d 0a                     tar.gz.. ..
```

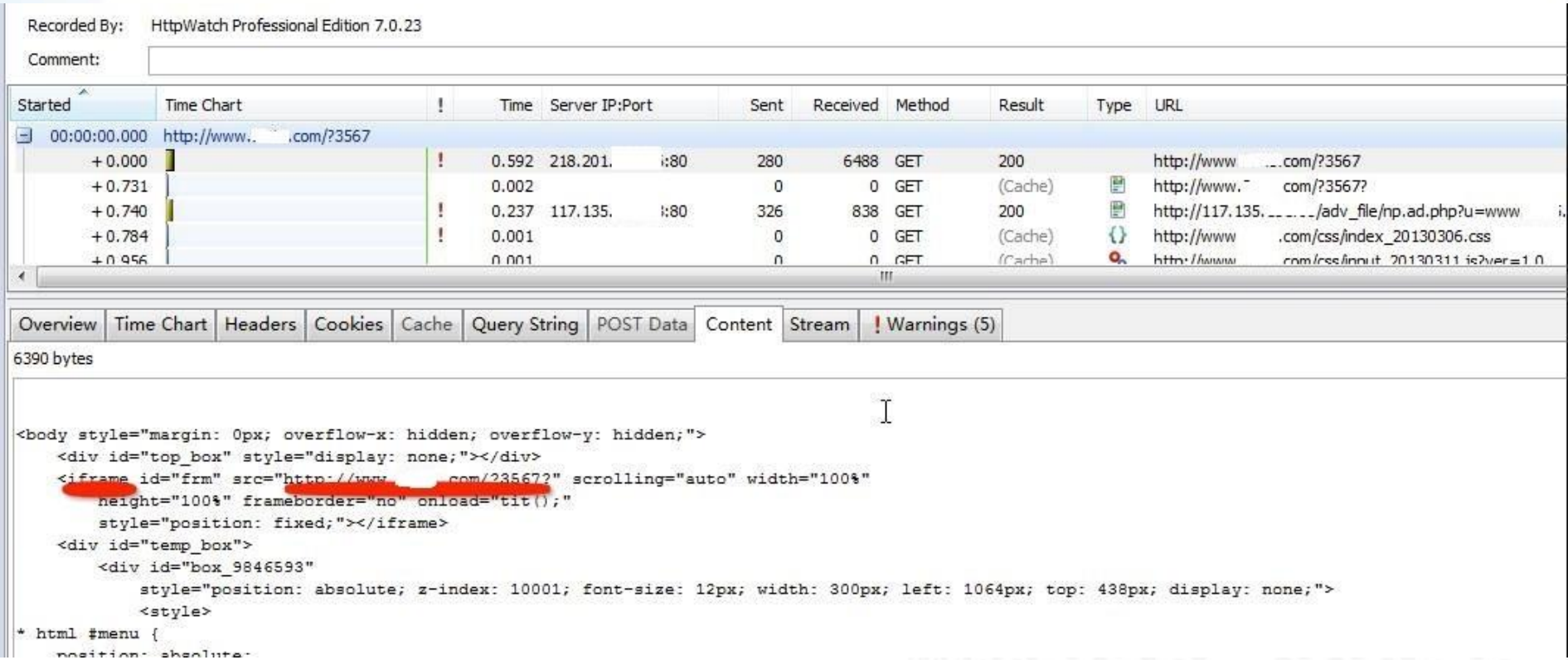
AD Insertion



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]
10	0.063	218.201.	211.151.	TCP	54	27790 > 80 [ACK] Seq=125 Ack=2953 Win=10824 Len=0
11	0.063	211.151.	218.201.	TCP	1038	[TCP segment of a reassembled PDU]
12	0.063	218.201.	211.151.	TCP	54	27790 > 80 [ACK] Seq=125 Ack=3937 Win=12792 Len=0
13	0.063	211.151.	218.201.	TCP	1038	[TCP segment of a reassembled PDU]
14	0.063	218.201.	211.151.	TCP	54	27790 > 80 [ACK] Seq=125 Ack=4921 Win=14760 Len=0
15	0.063	211.151.	218.201.	TCP	1038	[TCP segment of a reassembled PDU]
16	0.063	218.201.	211.151.	TCP	54	27790 > 80 [ACK] Seq=125 Ack=5905 Win=16728 Len=0
17	0.063	211.151.	218.201.	HTTP	625	HTTP/1.0 200 OK
18	0.063	218.201.	211.151.	TCP	54	27790 > 80 [FIN, ACK] Seq=125 Ack=6477 Win=18696 Len=0
19	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
25	0.125	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[
30	0.125	218.201.	211.151.	TCP	54	27790 > 80 [RST] Seq=125 Win=0 Len=0

AD Insertion



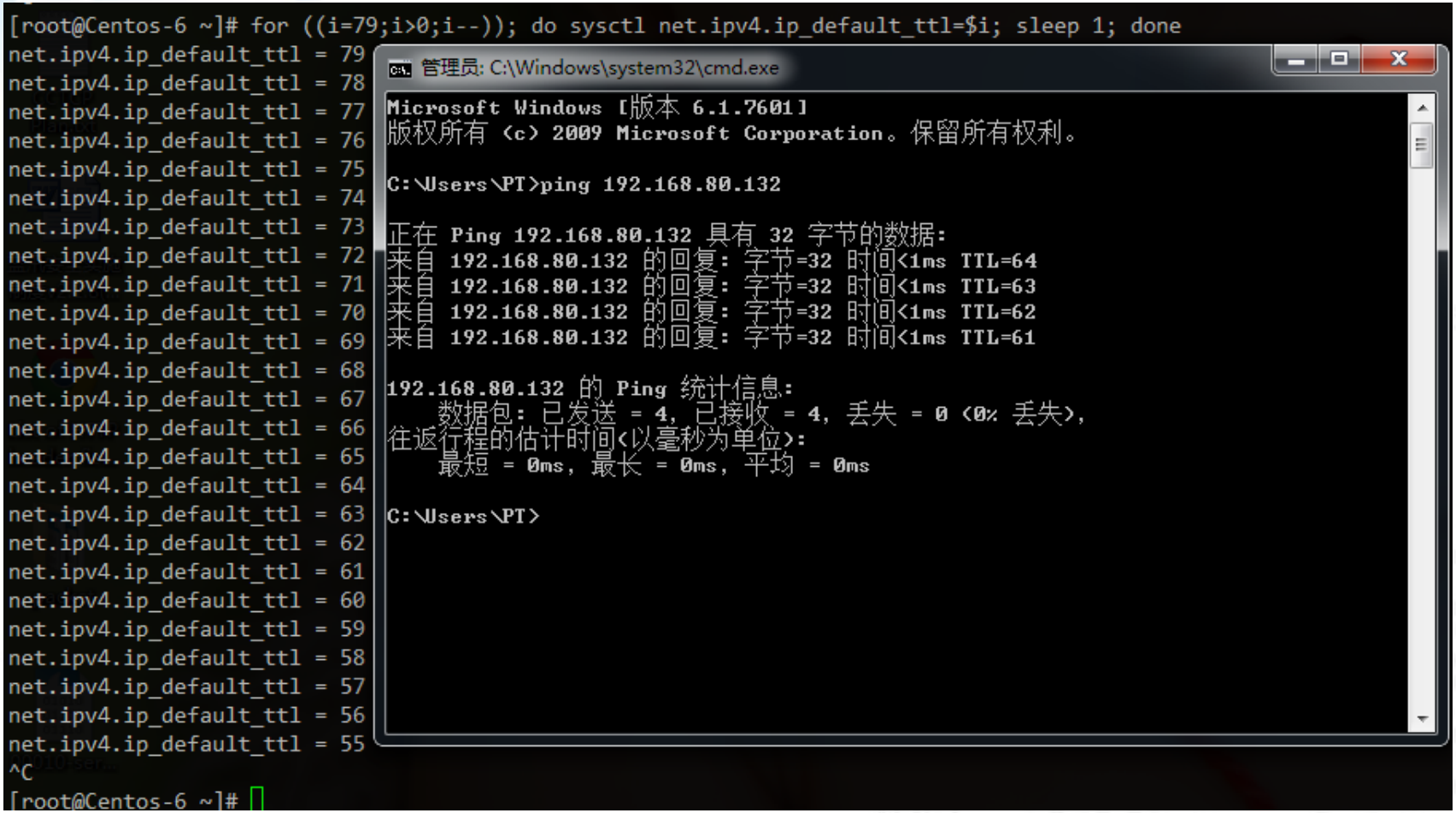
IP -> TTL

IPv4 Header Format

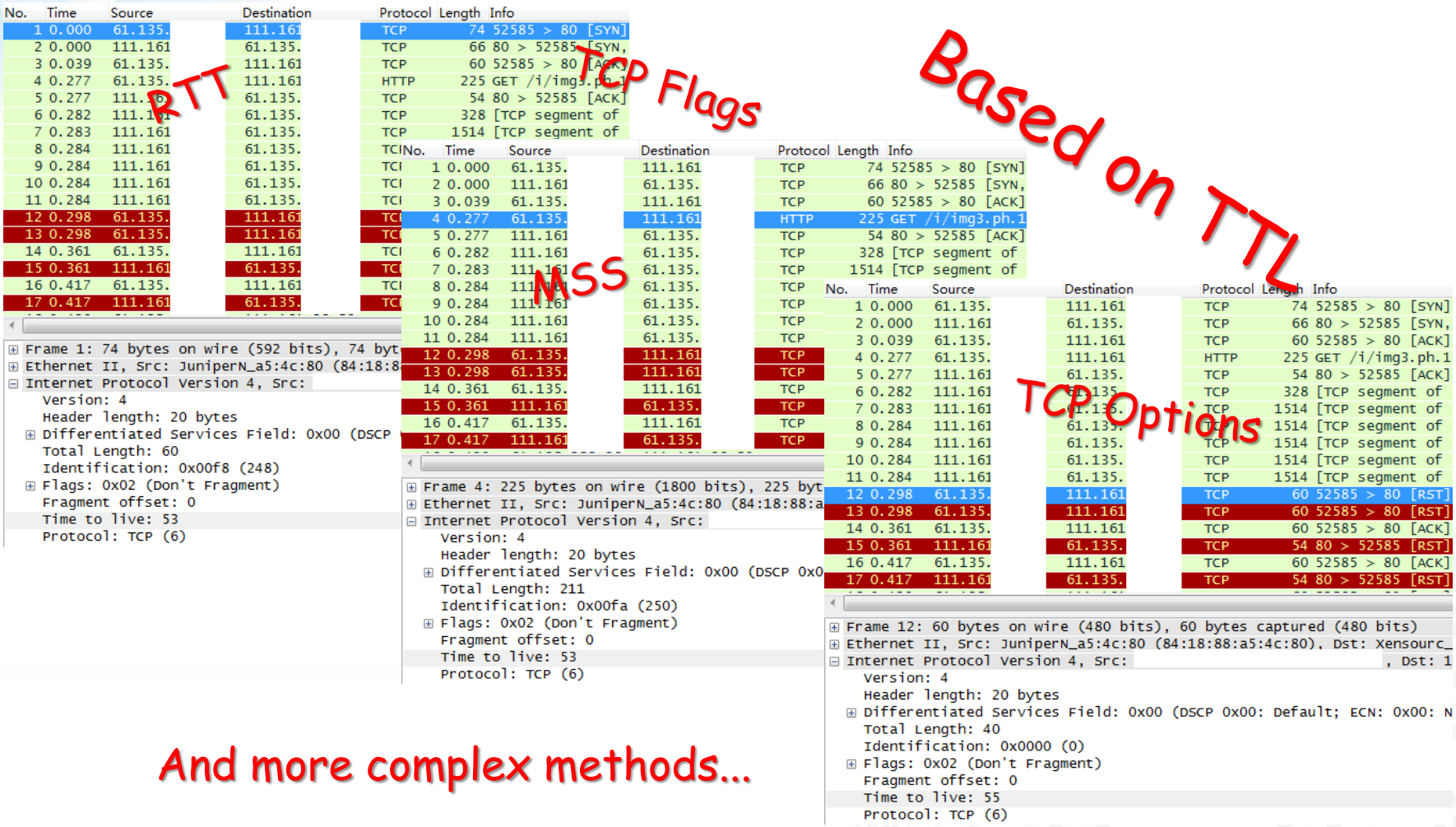
Offsets	Octet	0								1								2								3							
Octet	Bit	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
0	0	Version				IHL				DSCP						ECN		Total Length															
4	32	Identification																Flags			Fragment Offset											
8	64	Time To Live								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
net.ipv4.ip_default_ttl = 78
net.ipv4.ip_default_ttl = 77
net.ipv4.ip_default_ttl = 76
net.ipv4.ip_default_ttl = 75
net.ipv4.ip_default_ttl = 74
net.ipv4.ip_default_ttl = 73
net.ipv4.ip_default_ttl = 72
net.ipv4.ip_default_ttl = 71
net.ipv4.ip_default_ttl = 70
net.ipv4.ip_default_ttl = 69
net.ipv4.ip_default_ttl = 68
net.ipv4.ip_default_ttl = 67
net.ipv4.ip_default_ttl = 66
net.ipv4.ip_default_ttl = 65
net.ipv4.ip_default_ttl = 64
net.ipv4.ip_default_ttl = 63
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
^C
[root@Centos-6 ~]#
管理员: C:\Windows\system32\cmd.exe
Microsoft Windows [版本 6.1.7601]
版权所有 (c) 2009 Microsoft Corporation。保留所有权利。
C:\Users\PT>ping 192.168.80.132
正在 Ping 192.168.80.132 具有 32 字节的数据:
来自 192.168.80.132 的回复: 字节=32 时间<1ms TTL=64
来自 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
来自 192.168.80.132 的回复: 字节=32 时间<1ms TTL=61
192.168.80.132 的 Ping 统计信息:
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
C:\Users\PT>

How to resolve it?



And more complex methods...

Our AI

Anti-Interference Test

```
[root@[redacted] ~]# for((i=0;i<10;i++));do wget -O /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 15:44:15 ERROR 502: Bad Gateway.
2012-10-17 15:44:15 ERROR 502: Bad Gateway.
2012-10-17 15:44:15 ERROR 502: Bad Gateway.
2012-10-17 15:44:16 ERROR 502: Bad Gateway.
```

访问 10 次敏感 URL
遭到干扰，下载无法正常进行

```
2012-10-17 15:44:16 ERROR 502: Bad Gateway.
2012-10-17 15:44:16 ERROR 502: Bad Gateway.
[root@[redacted] ~]# service AI start
Starting AI:                                               [  OK  ]
[root@[redacted] ~]# for((i=0;i<10;i++));do wget -O /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 15:44:24 (81.2 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]
```

同时在上下层启动 AI
上下层之间配合，一起拦截中间干扰

再次访问敏感 URL
均可成功访问

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!


SequeMedia
盛拓传媒
IT168.com
www.it168.com
ChinaUnix.net
ITPUB

Q & A