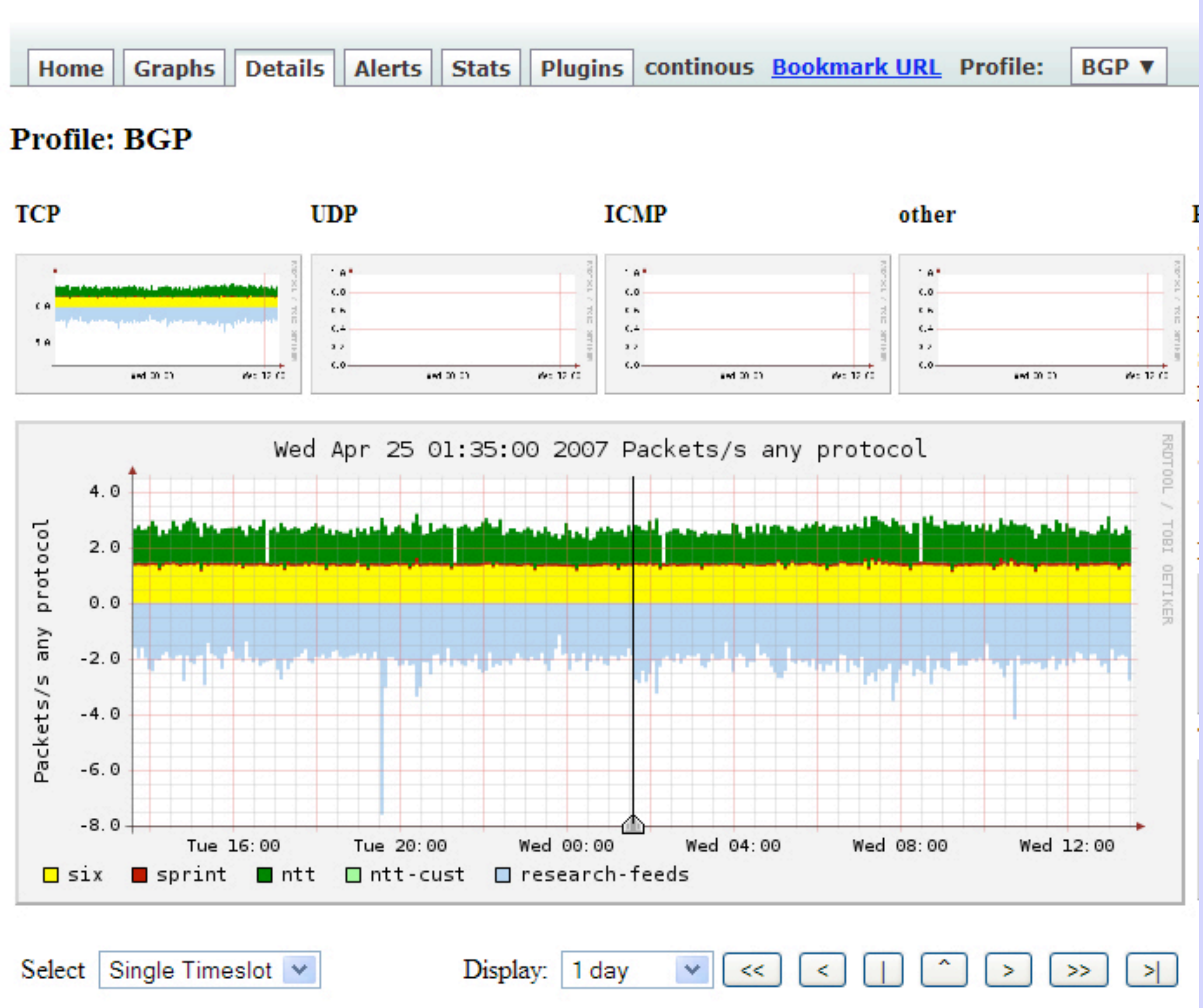
NFSEN: How is My Network Being Used (Apps)?

AfNOG / Abuja

2007.04.27

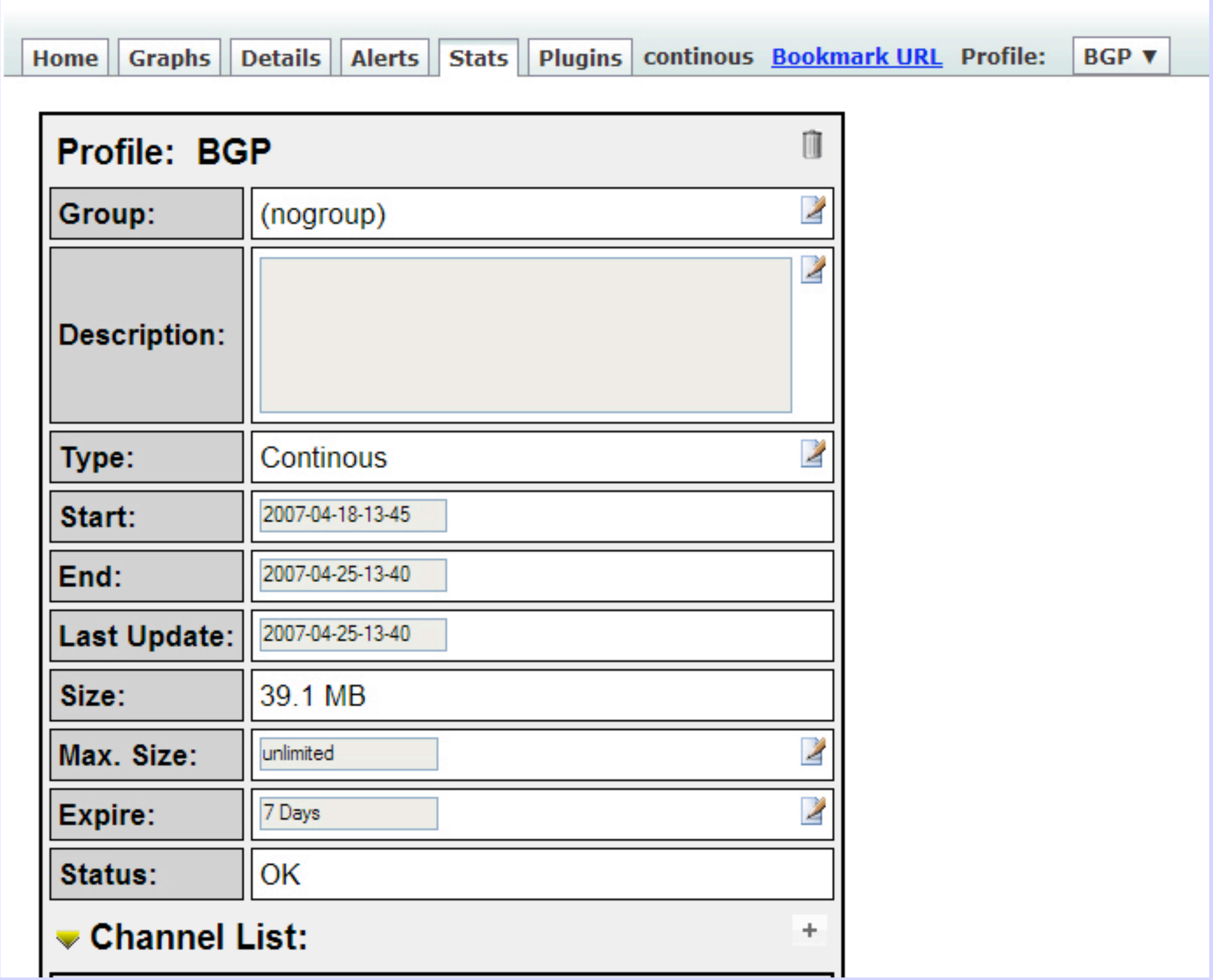
Randy Bush <randy@psg.com>
Mark Tinka <mtinka@psg.com>

I Use to Look at BGP Peers!



Profile: BGP

Here is Profile for BGP

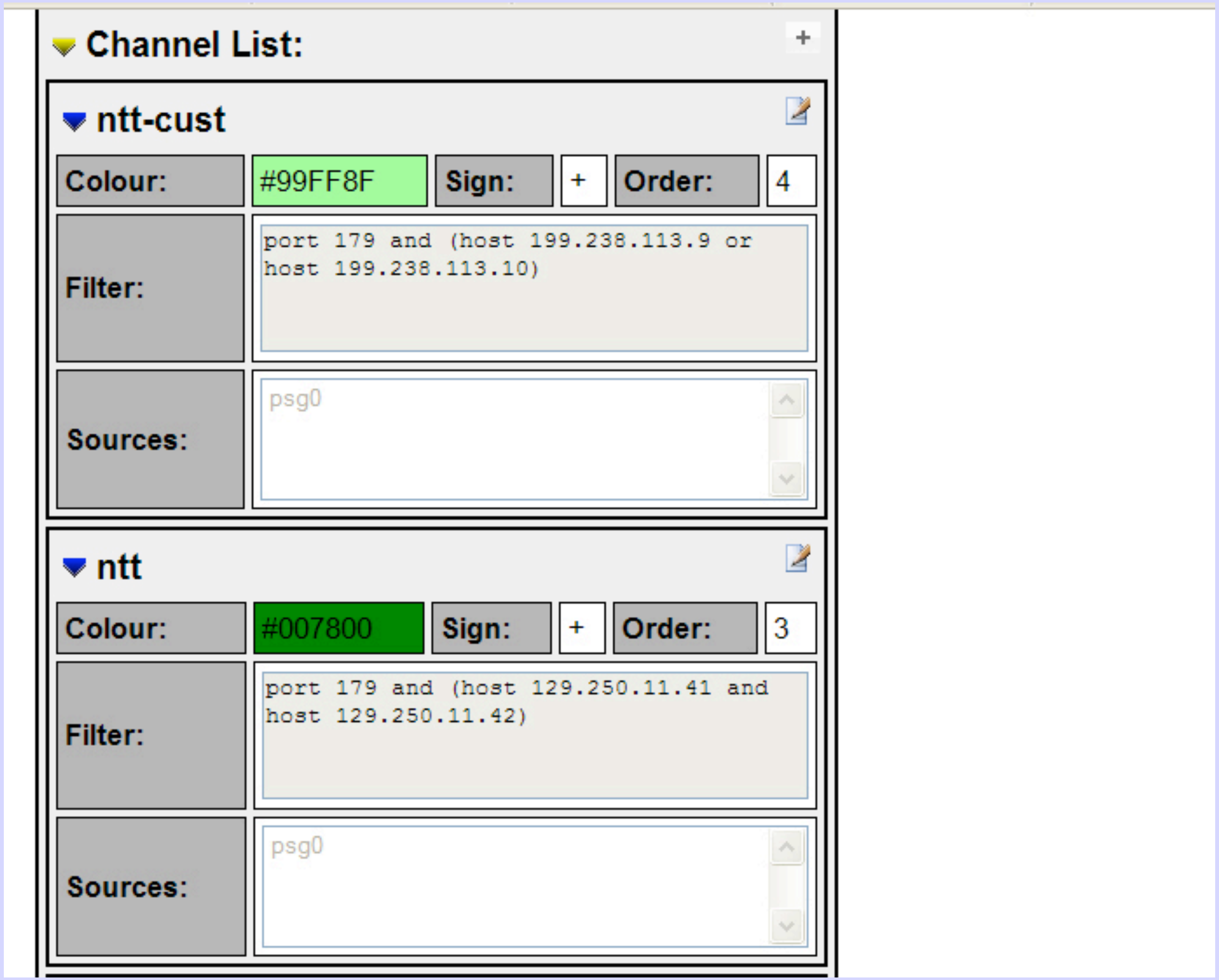


Profile: BGP

Group:	(nogroup)
Description:	
Type:	Continous
Start:	2007-04-18-13-45
End:	2007-04-25-13-40
Last Update:	2007-04-25-13-40
Size:	39.1 MB
Max. Size:	unlimited
Expire:	7 Days
Status:	OK

Channel List:

Entries for Two Peers



Channel List:

ntt-cust

Colour:	#99FF8F	Sign:	+	Order:	4

Filter:

```
port 179 and (host 199.238.113.9 or
host 199.238.113.10)
```

Sources: psg0

ntt

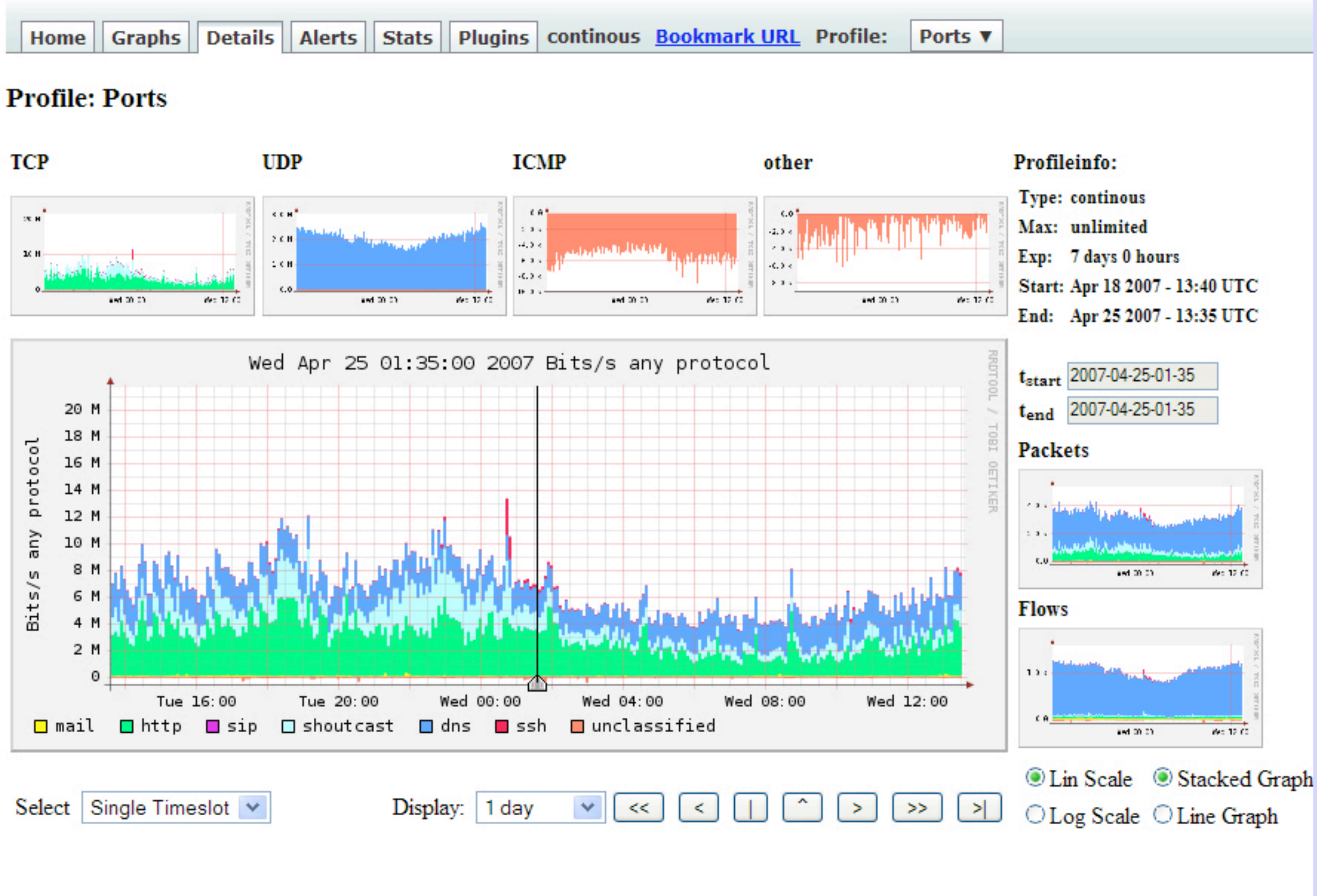
Colour:	#007800	Sign:	+	Order:	3

Filter:

```
port 179 and (host 129.250.11.41 and
host 129.250.11.42)
```

Sources: psg0

Application Ports



Profile: Ports

Profileinfo:

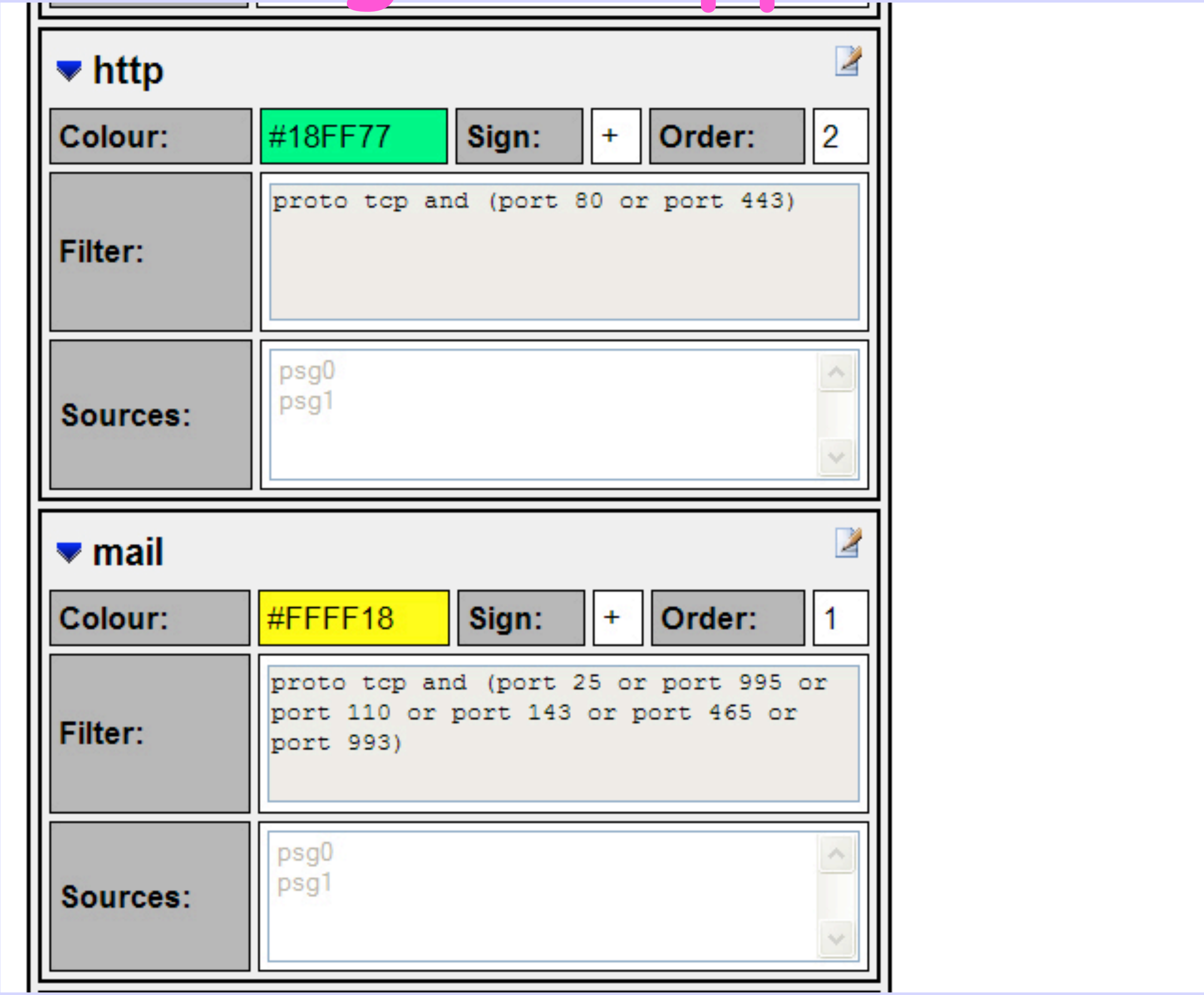
Type: continous
Max: unlimited
Exp: 7 days 0 hours
Start: Apr 18 2007 - 13:40 UTC
End: Apr 25 2007 - 13:35 UTC

t_{start} 2007-04-25-01-35
t_{end} 2007-04-25-01-35

● Lin Scale ● Stacked Graph
○ Log Scale ○ Line Graph

Select: Single Timeslot
Display: 1 day

Focusing on Applications



http

Colour: #18FF77 Sign: + Order: 2

Filter:

```
proto tcp and (port 80 or port 443)
```

Sources:

psg0
psg1

mail

Colour: #FFFF18 Sign: + Order: 1

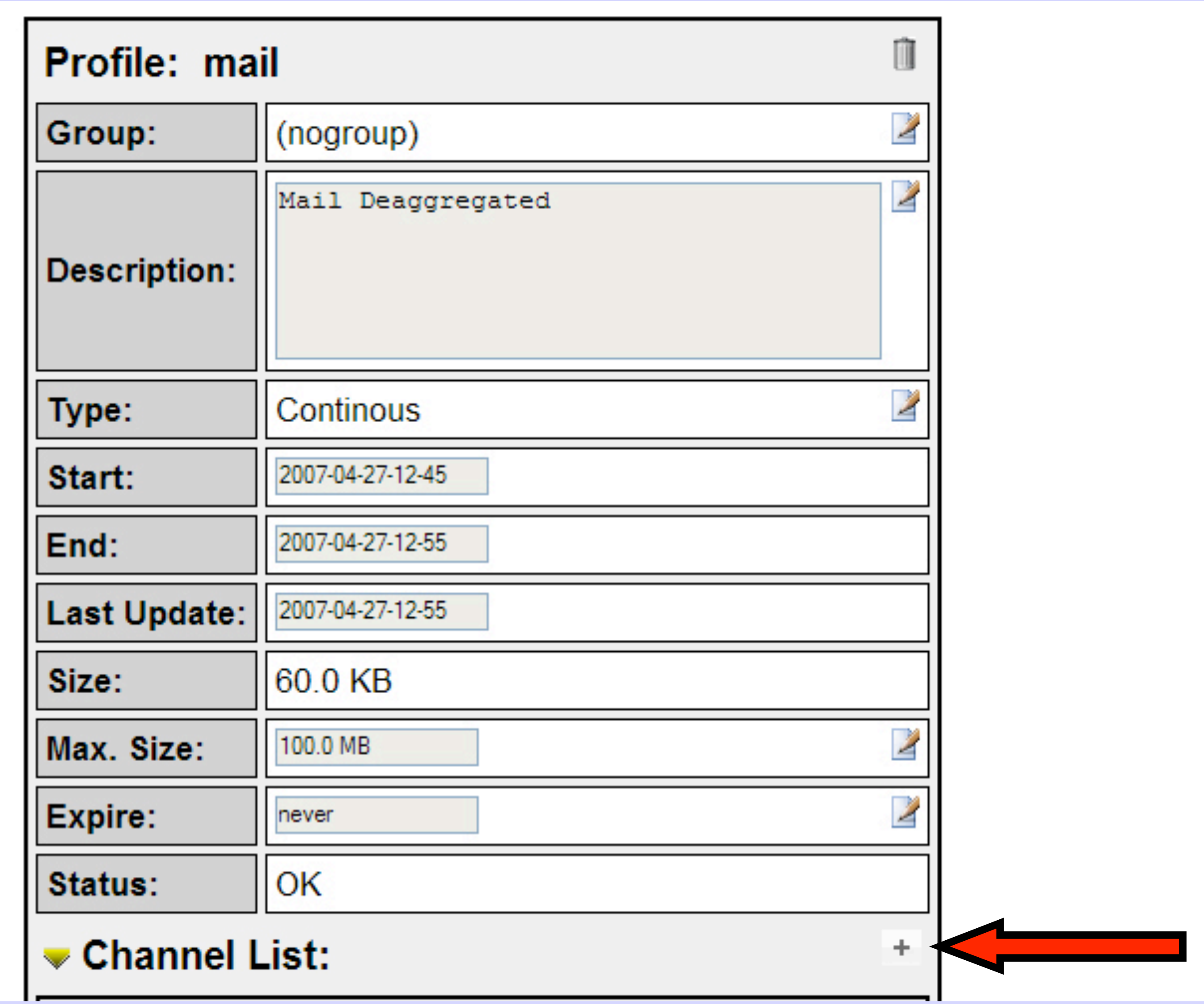
Filter:

```
proto tcp and (port 25 or port 995 or
port 110 or port 143 or port 465 or
port 993)
```

Sources:

psg0
psg1

Making a New Channel

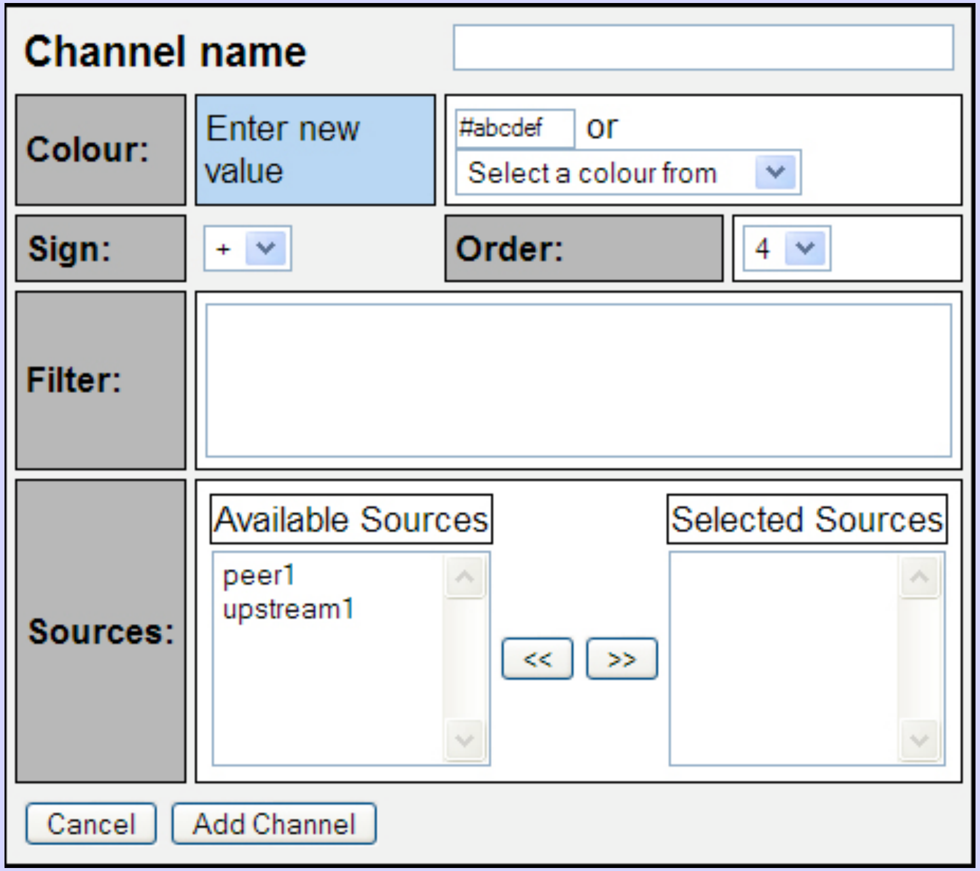


Profile: mail

Group:	(nogroup)
Description:	Mail Deaggregated
Type:	Continous
Start:	2007-04-27-12-45
End:	2007-04-27-12-55
Last Update:	2007-04-27-12-55
Size:	60.0 KB
Max. Size:	100.0 MB
Expire:	never
Status:	OK

Channel List:

New Channel Form



Channel name

Colour: Enter new value #abcdef or Select a colour from

Sign: +

Order: 4

Filter:

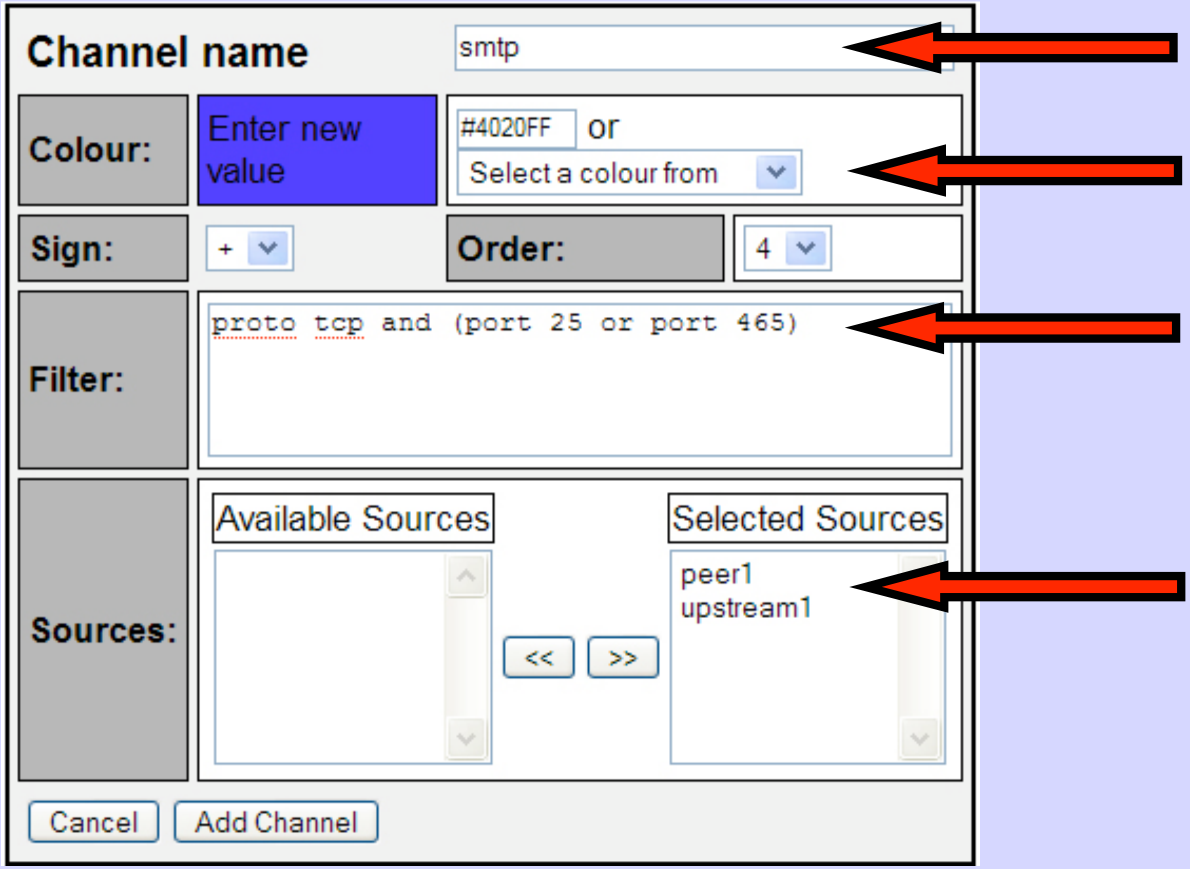
Sources:

Available Sources

peer1
upstream1

Selected Sources

SMTP Channel



Channel name: smtp

Colour: Enter new value #4020FF or Select a colour from

Sign: +

Order: 4

Filter:

```
proto tcp and (port 25 or port 465)
```

Sources:

Available Sources

Selected Sources: peer1, upstream1

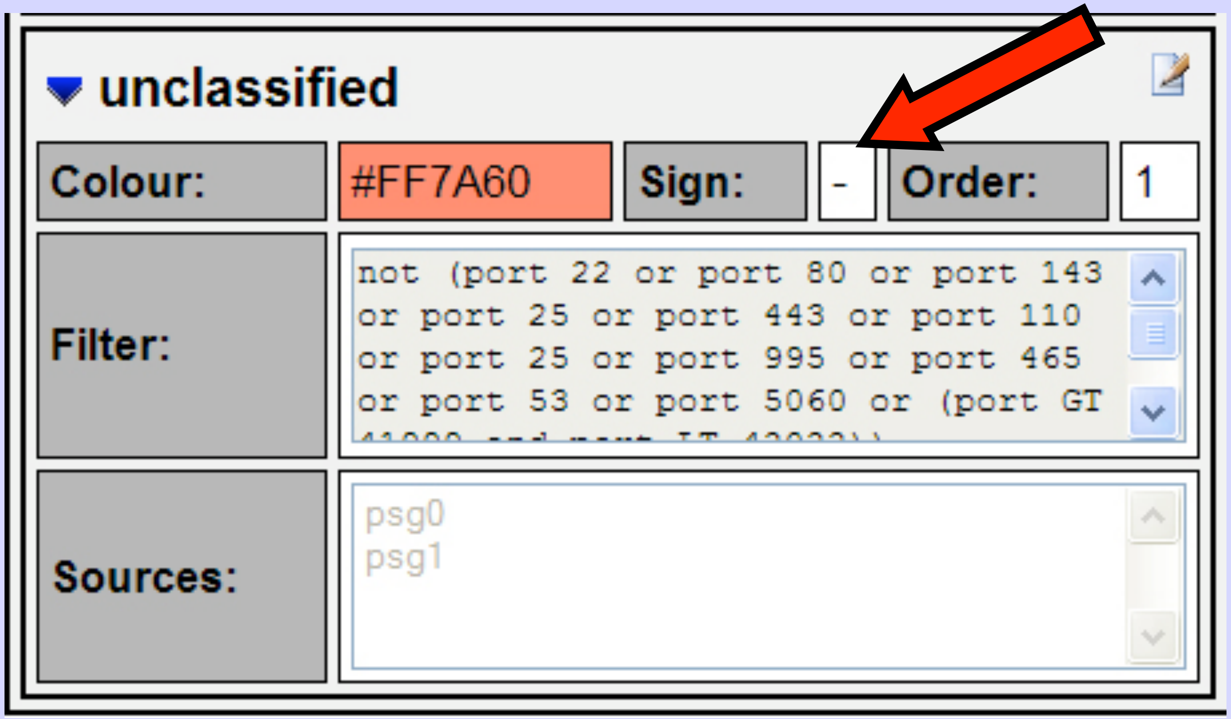
Name for Legend

Pick Contrasting Colors

Get Secure and Insecure

Which Interfaces

Unclassified



unclassified

Colour:	#FF7A60	Sign:	-	Order:	1

Filter:

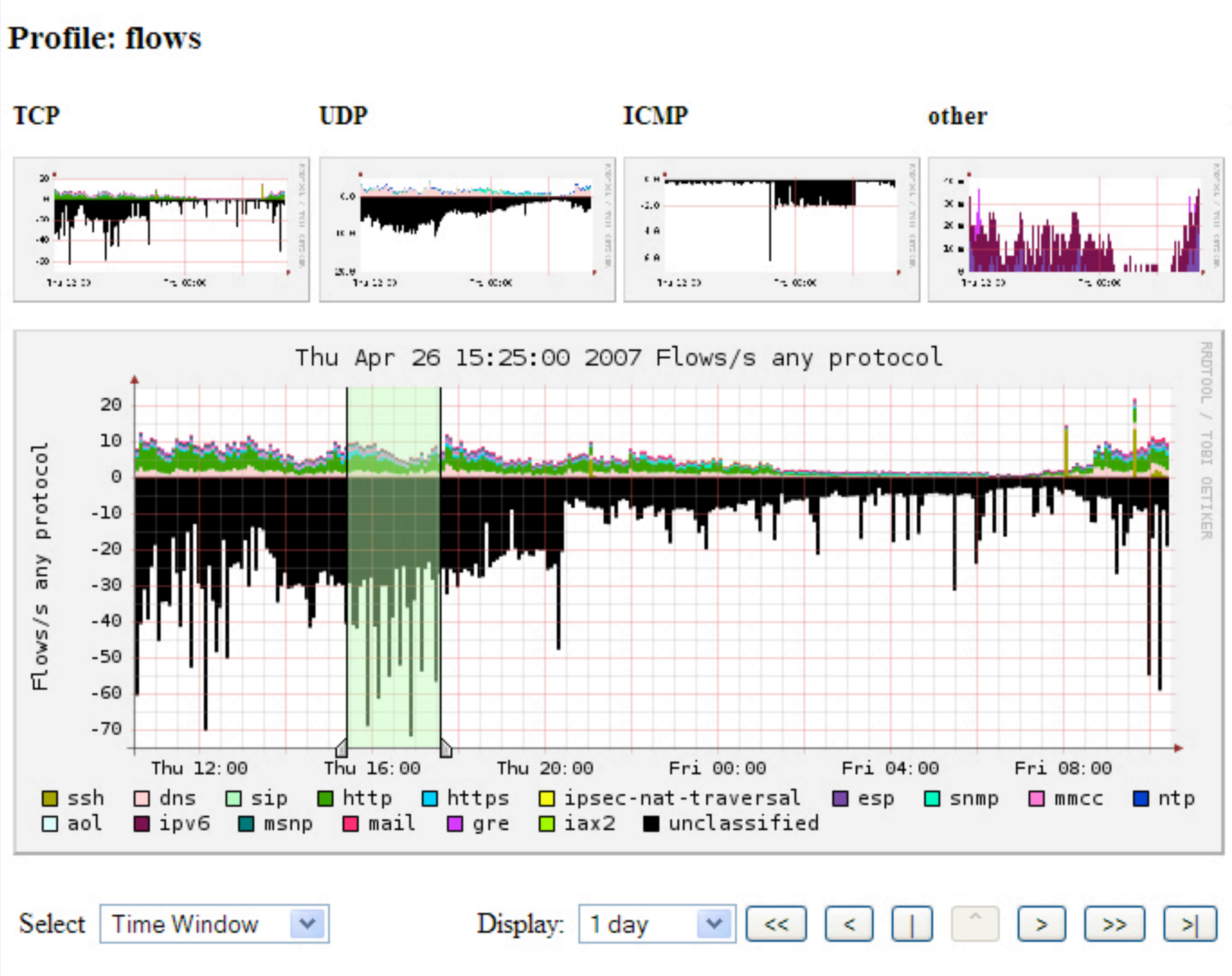
```
not (port 22 or port 80 or port 143
or port 25 or port 443 or port 110
or port 25 or port 995 or port 465
or port 53 or port 5060 or (port GT
41000 and port LT 42000))
```

Sources:

psg0
psg1

Good Habit to Show What We Missed

Unclassified?

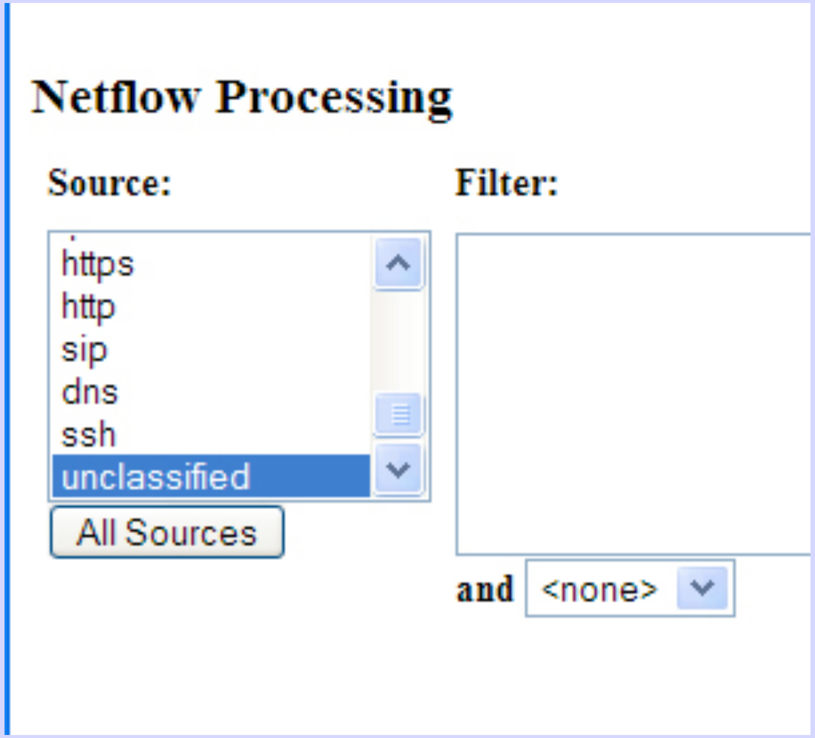


Profile: flows

Select: Time Window

Display: 1 day

Select only Unclassified

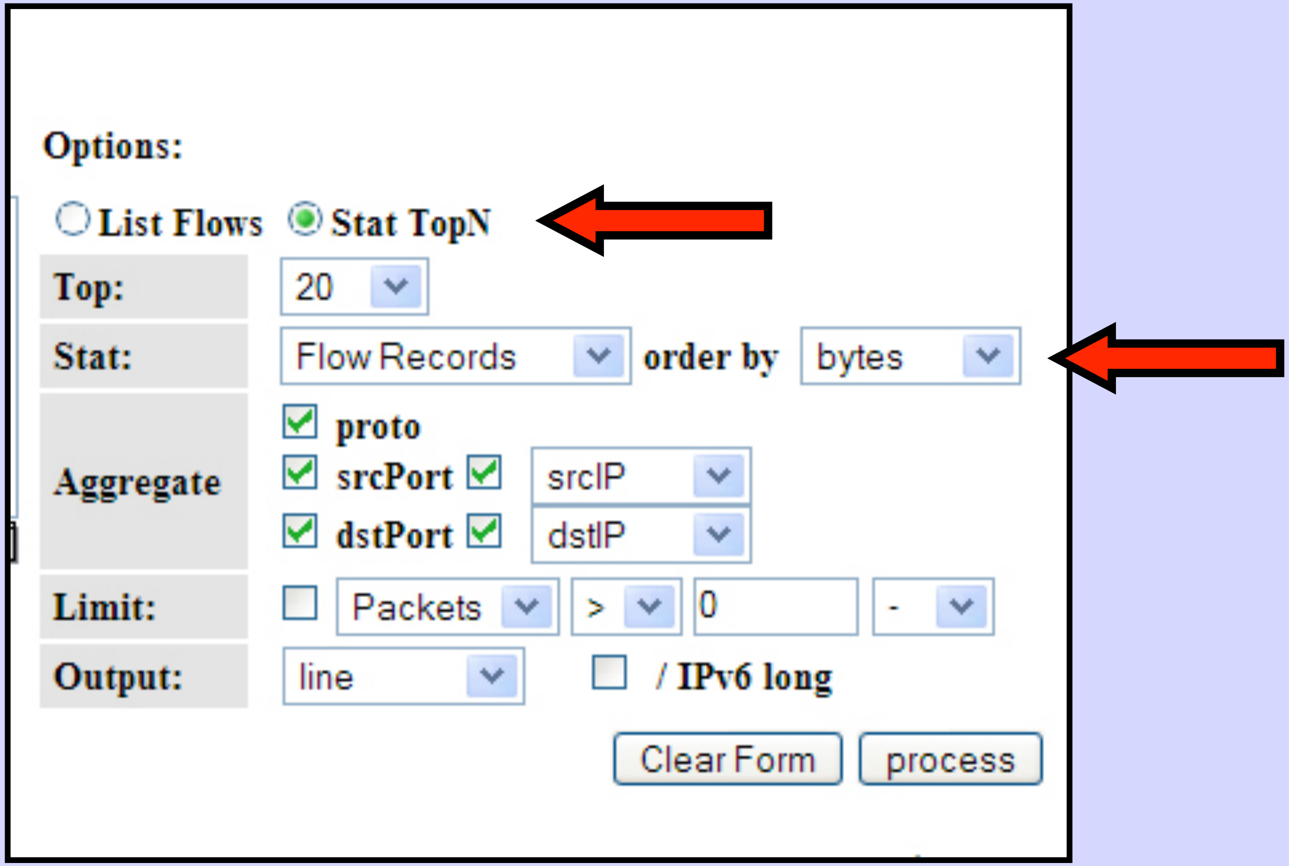


Netflow Processing

Source:

Filter:

What we Want to See

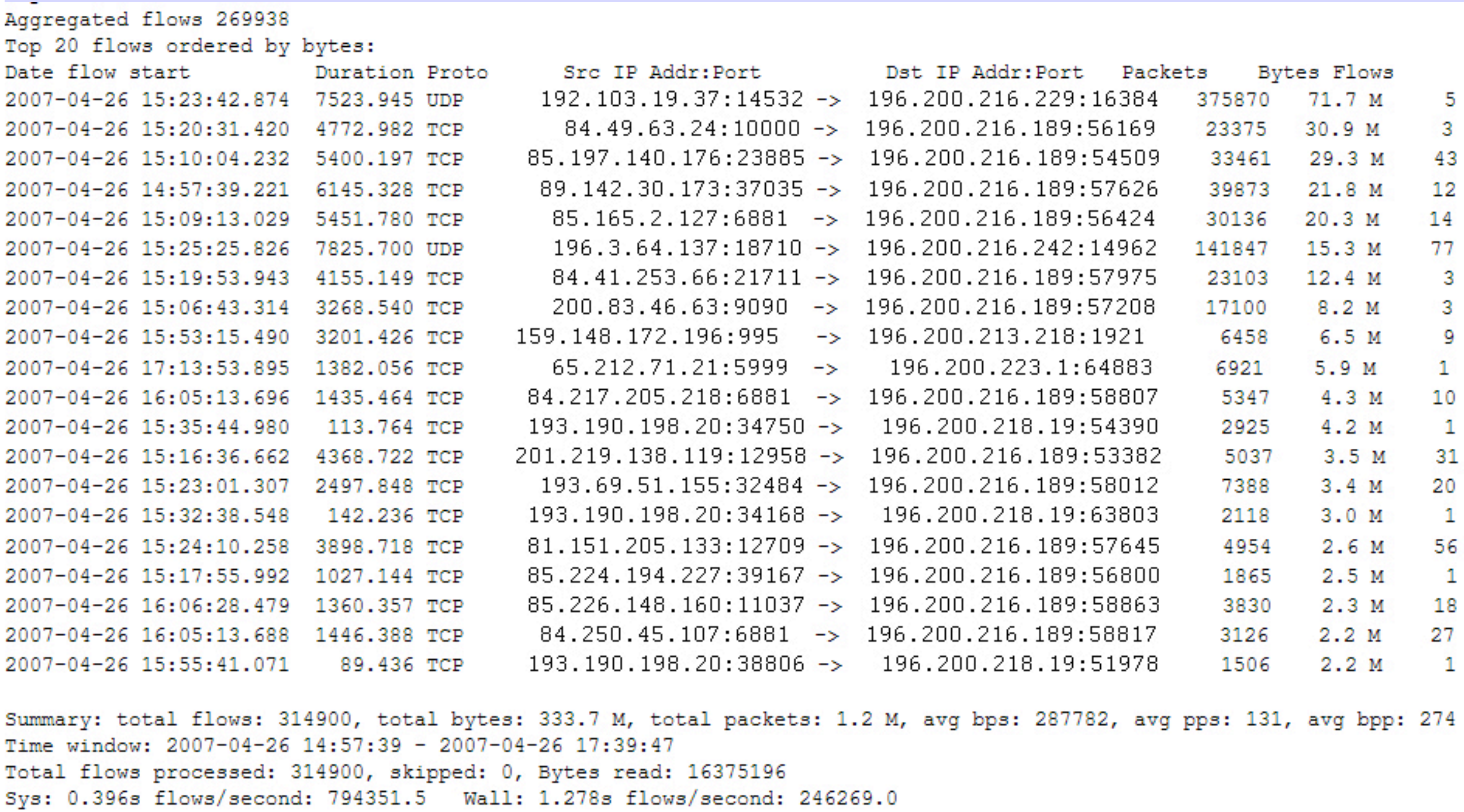


Options:

○ List Flows ● Stat TopN

Top:	20
Stat:	Flow Records order by bytes
Aggregate	☑ proto ☑ srcPort ☑ srcIP ☑ dstPort ☑ dstIP
Limit:	□ Packets > 0 -
Output:	line □ / IPv6 long

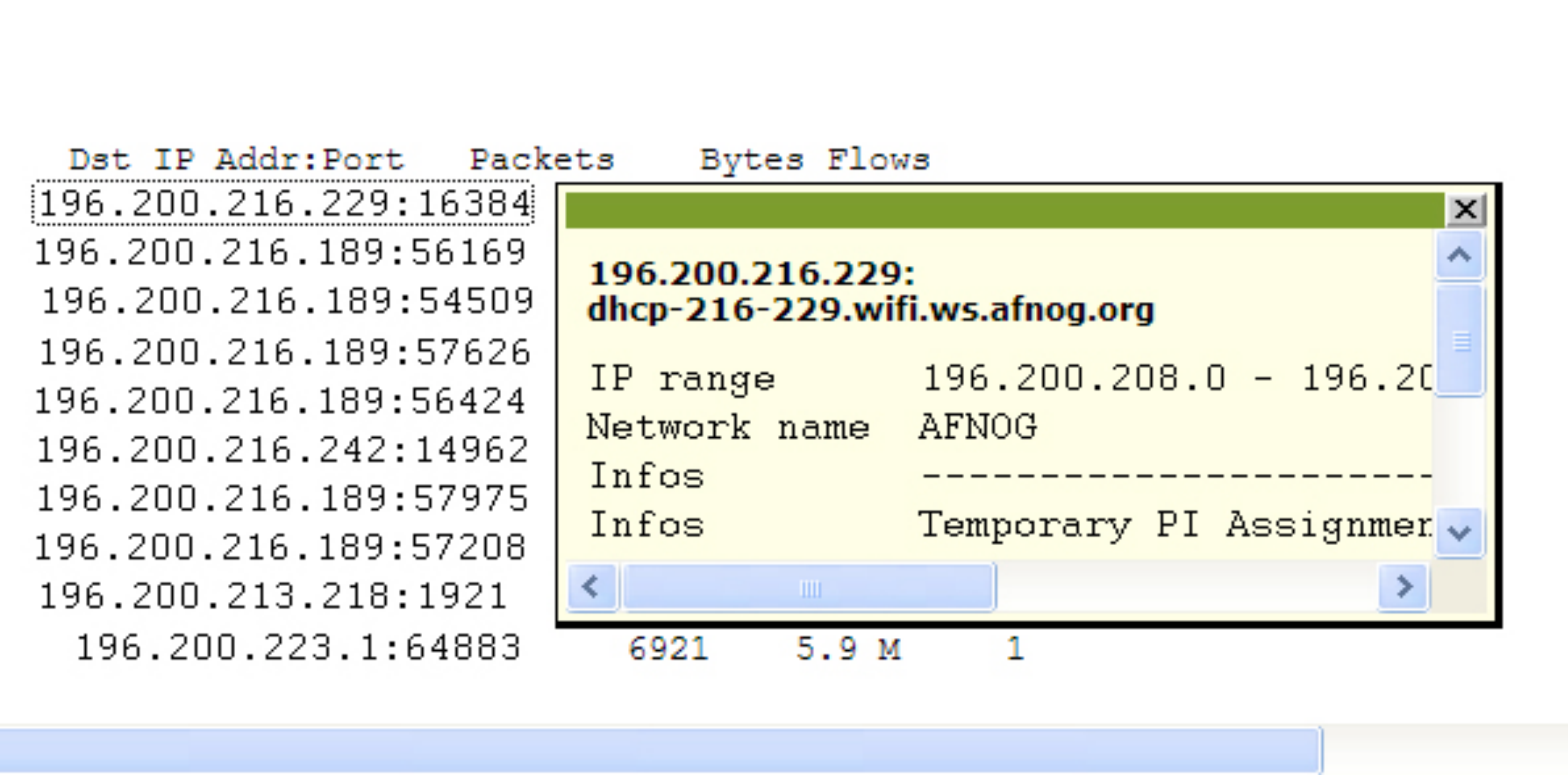
And we Get Stats!



```
Aggregated flows 269938
Top 20 flows ordered by bytes:
Date flow start          Duration Proto      Src IP Addr:Port          Dst IP Addr:Port   Packets    Bytes Flows
2007-04-26 15:23:42.874  7523.945 UDP     192.103.19.37:14532 ->  196.200.216.229:16384  375870   71.7 M     5
2007-04-26 15:20:31.420  4772.982 TCP       84.49.63.24:10000 ->  196.200.216.189:56169   23375   30.9 M     3
2007-04-26 15:10:04.232  5400.197 TCP    85.197.140.176:23885 ->  196.200.216.189:54509   33461   29.3 M    43
2007-04-26 14:57:39.221  6145.328 TCP     89.142.30.173:37035 ->  196.200.216.189:57626   39873   21.8 M    12
2007-04-26 15:09:13.029  5451.780 TCP      85.165.2.127:6881  ->  196.200.216.189:56424   30136   20.3 M    14
2007-04-26 15:25:25.826  7825.700 UDP      196.3.64.137:18710 ->  196.200.216.242:14962  141847   15.3 M    77
2007-04-26 15:19:53.943  4155.149 TCP      84.41.253.66:21711 ->  196.200.216.189:57975   23103   12.4 M     3
2007-04-26 15:06:43.314  3268.540 TCP      200.83.46.63:9090  ->  196.200.216.189:57208   17100    8.2 M     3
2007-04-26 15:53:15.490  3201.426 TCP   159.148.172.196:995   ->  196.200.213.218:1921     6458    6.5 M     9
2007-04-26 17:13:53.895  1382.056 TCP      65.212.71.21:5999  ->    196.200.223.1:64883    6921    5.9 M     1
2007-04-26 16:05:13.696  1435.464 TCP    84.217.205.218:6881  ->  196.200.216.189:58807    5347    4.3 M    10
2007-04-26 15:35:44.980   113.764 TCP    193.190.198.20:34750 ->   196.200.218.19:54390    2925    4.2 M     1
2007-04-26 15:16:36.662  4368.722 TCP   201.219.138.119:12958 ->  196.200.216.189:53382    5037    3.5 M    31
2007-04-26 15:23:01.307  2497.848 TCP     193.69.51.155:32484 ->  196.200.216.189:58012    7388    3.4 M    20
2007-04-26 15:32:38.548   142.236 TCP    193.190.198.20:34168 ->   196.200.218.19:63803    2118    3.0 M     1
2007-04-26 15:24:10.258  3898.718 TCP    81.151.205.133:12709 ->  196.200.216.189:57645    4954    2.6 M    56
2007-04-26 15:17:55.992  1027.144 TCP    85.224.194.227:39167 ->  196.200.216.189:56800    1865    2.5 M     1
2007-04-26 16:06:28.479  1360.357 TCP    85.226.148.160:11037 ->  196.200.216.189:58863    3830    2.3 M    18
2007-04-26 16:05:13.688  1446.388 TCP     84.250.45.107:6881  ->  196.200.216.189:58817    3126    2.2 M    27
2007-04-26 15:55:41.071    89.436 TCP    193.190.198.20:38806 ->   196.200.218.19:51978    1506    2.2 M     1

Summary: total flows: 314900, total bytes: 333.7 M, total packets: 1.2 M, avg bps: 287782, avg pps: 131, avg bpp: 274
Time window: 2007-04-26 14:57:39 - 2007-04-26 17:39:47
Total flows processed: 314900, skipped: 0, Bytes read: 16375196
Sys: 0.396s flows/second: 794351.5   Wall: 1.278s flows/second: 246269.0
```

Who Was It?



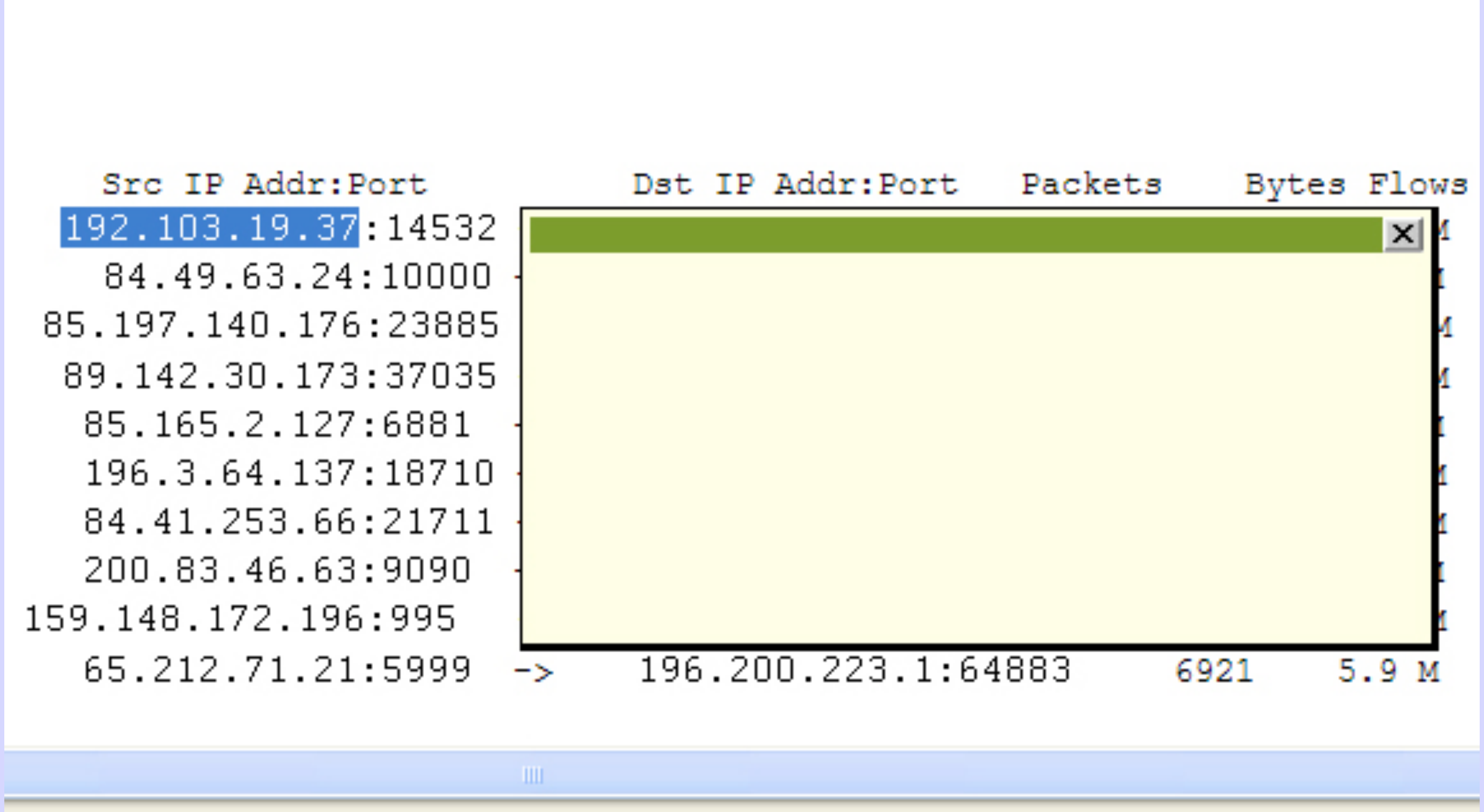
```
 Dst IP Addr:Port    Packets     Bytes Flows
196.200.216.229:16384
196.200.216.189:56169
196.200.216.189:54509
196.200.216.189:57626
196.200.216.189:56424
196.200.216.242:14962
196.200.216.189:57975
196.200.216.189:57208
196.200.213.218:1921
  196.200.223.1:64883       6921     5.9 M     1
```

196.200.216.229:
dhcp-216-229.wifi.ws.afnog.org

```
IP range        196.200.208.0 - 196.20
Network name    AFNOG
Infos           ----------------------
Infos           Temporary PI Assignmer
```

At your site, you would use better names ☺

To Whom Were They Talking?



```
     Src IP Addr:Port              Dst IP Addr:Port     Packets      Bytes Flows
  192.103.19.37:14532
    84.49.63.24:10000
 85.197.140.176:23885
  89.142.30.173:37035
    85.165.2.127:6881
   196.3.64.137:18710
   84.41.253.66:21711
    200.83.46.63:9090
159.148.172.196:995
    65.212.71.21:5999  ->     196.200.223.1:64883      6921      5.9 M
```

Broken in-addr.arpa ☹

Yep, in-addr.arpa ☹

```
% host 192.103.19.37
;; connection timed out; no servers could be
reached
```

Try Whois

```
% whois -h whois.arin.net 192.103.19.37

OrgName:     Nokia Data Communications
Corporation
OrgID:       NDCC-2
Address:     2300 Tall Pines Drive, Suite 100
City:        Largo
StateProv:   FL
PostalCode:  34641
Country:     US
```

Hi Joel ☺