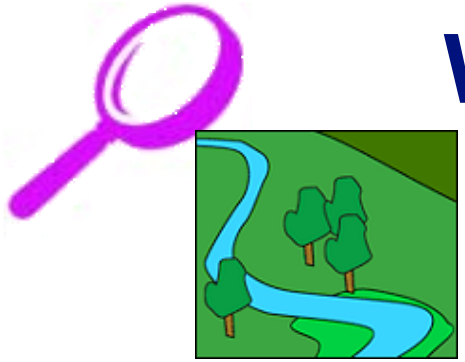
SWITCH

The Swiss Education & Research Network



Watch your Flows with NfSen and NFDUMP

50th RIPE Meeting
May 3, 2005 Stockholm
Peter Haag

SWITCH cert

NfSen/nfdump

SWITCH
The Swiss Education & Research Network

What I am going to present:

- **The Motivation.**
- **What are NfSen and nfdump?**
- **The Tools in Action.**
- **Outlook - what's next.**

NfSen/nfdump

SWITCH
The Swiss Education & Research Network

The Motivation:

NfSen and nfdump came out of operational needs.

When discussing with other teams:

- **"Watch your flows for …"**
- **"I've seen a lot of … in our flows …"**

Netflow turnes out to be "The Data Source" although not the only one - for all kind of information and/or events to look at a network.

But …

```
Router# show ip cache flow
```

… seems not to be the solution for every task.

NfSen/nfdump

SWITCH
The Swiss Education & Research Network

Wish list:

- Must be fast!
- Must be really fast! ~ 25GB data/day
- Easy to use.
- Keep netflow data for a certain period of time.
- Easy navigation when searching stored netflow data.
- Flexible and powerful filtering.
- Flexible aggregation of netflow data.
- Top N statistics for packets, bytes, IP addresses, ports …
- Profiling hosts in case of an incident.
- A tool, which supports us in our daily work.

Many tools available, but either too slow, too cumbersome or not what we wanted.

→ *nfdump*

SWITCH cert

nfdump

SWITCH
The Swiss Education & Research Network

nfdump:

- **Stores netflow data in time sliced files.**
- **CMD line based tool comparable to tcpdump.**
- **Written in C ⇒ fast.**
- **Supports netflow format v5 and v7.**
- **Powerful pcap like filter syntax:**
  '(tcp and dst net 172.16/16 and src port > 1024 and bytes < 600) or (…'
- **Flexible aggregation.**
- **Efficient filter engine: > 4 Mio flows/s on 3GHz Intel.**
- **Fast Statistics (Top N) 2.5 s for 1.5Mio flows.**
  Top N flows, packets, (src/dst) IP addresses.
- **…**

The wish list became true

nfdump

SWITCH
The Swiss Education & Research Network

List Flows:

```
nfsrv% nfdump -r nfcapd.200504131500 -c 10
Date flow start         Len Proto    Src IP Addr:Port          Dst IP Addr:Port  Packets     Bytes
Apr 13 2005 14:59:56      0 TCP   213.161.64.210:80     ->    211.99.1.218:34156        5    828  B
Apr 13 2005 14:59:56      0 TCP      64.62.154.4:80     -> 162.139.189.158:4527        3    140  B
Apr 13 2005 14:59:56      2 TCP   131.132.112.21:1138   ->    64.18.47.234:80          5    637  B
Apr 13 2005 14:59:56      1 TCP     64.62.191.95:80     ->   172.212.81.18:4390        5    493  B
Apr 13 2005 14:59:56      0 TCP  216.109.117.206:80     -> 211.223.204.230:1132        3    266  B
Apr 13 2005 14:59:56      1 TCP     83.141.49.51:80     ->     211.92.9.56:37157      42  57.0 KB
Apr 13 2005 14:59:48      5 TCP   191.210.93.172:80     ->    149.194.8.73:3530       20  16.6 KB
Apr 13 2005 14:59:56      0 TCP   191.101.94.201:80     ->  199.53.250.100:30267       5    633  B
Apr 13 2005 14:59:56      0 TCP    199.81.104.90:60553 ->  213.161.61.209:80          6    803  B
Apr 13 2005 14:59:48     10 TCP      9.4.223.185:1433   ->  168.150.251.37:22520       3    140  B
Flows analysed: 29 matched: 10, Bytes read: 1416
Time window: Apr 13 2005 14:59:16 - Apr 13 2005 14:59:58

nfsrv% nfdump -r nfcapd.200504131500 -c 10 -o long 'not (flags 0 or tos 0)'
Date flow start         Len Proto    Src IP Addr:Port          Dst IP Addr:Port   Flags Tos Packets    Bytes
Apr 13 2005 14:59:42      9 TCP     194.42.48.56:4586  ->    194.42.48.11:179   .AP... 192       4   319  B
Apr 13 2005 14:59:53      0 TCP      194.42.48.4:57627 ->    194.42.48.11:179   .A.... 192       1    60  B
Apr 13 2005 14:59:48      5 TCP     194.42.48.15:11013 ->    194.42.48.11:179   .AP... 192       2    99  B
Apr 13 2005 14:59:57      0 TCP     83.238.131.3:4438  ->   192.41.222.35:135   ....S.  32       1    48  B
Apr 13 2005 14:59:41     16 TCP     211.21.32.28:14502 ->    211.21.32.30:639   .AP... 192       5   621  B
Apr 13 2005 14:59:50      8 TCP     194.42.48.79:179   ->    194.42.48.11:11029 .AP... 192       2    99  B
Apr 13 2005 14:59:58      0 UDP    194.42.48.120:123   ->    194.42.48.11:123   .A....  16       1    76  B
Apr 13 2005 14:59:59      1 TCP     194.42.48.69:179   ->    194.42.48.11:20994 .AP... 192       2   139  B
Apr 13 2005 14:59:56     11 TCP     194.42.48.82:11002 ->    194.42.48.11:179   .AP... 192       2   139  B
Apr 13 2005 15:00:05      3 TCP   213.17.198.139:3942  ->   192.41.230.52:445   ....S.  32       2    96  B
Flows analysed: 262471 matched: 10, Bytes read: 12815808
Time window: Apr 13 2005 14:44:50 - Apr 13 2005 15:00:22
```

(IP addresses anonymised)

Create TopN Statistics Packets/Bytes:

```
nfsrv% nfdump -r nfcapd.200504131500 -S -n 10
Flows analysed: 3136914 matched: 3136914, Bytes read: 153167712
Aggregated flows 2452160
Time window: Apr 13 2005 14:44:50 - Apr 13 2005 15:04:59
Top 10 flows packet count:
Date flow start        Len Proto    Src IP Addr:Port          Dst IP Addr:Port  Packets    Bytes
Apr 13 2005 14:53:35   630 TCP     211.21.10.35:20     ->    196.3.50.254:55260  886934   1.2 GB   2
Apr 13 2005 14:49:39   866 TCP        62.2.16.4:44890 ->     211.21.1.10:119    840504   1.2 GB   2
Apr 13 2005 14:45:59   846 TCP    62.53.226.182:44671 ->     211.21.1.10:119    701456 991.3 MB   1
Apr 13 2005 14:58:45   320 TCP     211.21.10.21:40398 ->   212.31.34.212:435    435334 619.0 MB   2
Apr 13 2005 14:47:05   872 TCP     211.21.10.35:57348 ->  80.218.156.106:61749  329811 181.2 MB   1
Apr 13 2005 14:53:35   630 TCP     196.3.50.254:55260 ->    211.21.10.35:20     323622  16.3 MB   2
Apr 13 2005 14:45:26  1121 TCP     211.21.10.35:58992 ->    80.24.26.102:28266  319523 457.1 MB   4
Apr 13 2005 14:50:03   842 TCP      211.21.1.10:43979 ->   164.172.36.58:119    270816 381.1 MB   2
Apr 13 2005 14:49:39   868 TCP      211.21.1.10:119   ->       62.2.16.4:44890  262789  13.7 MB   3
Apr 13 2005 14:45:26  1120 TCP     80.24.26.102:28266 ->    211.21.10.35:58992  208535   9.2 MB   3

Top 10 flows byte count:
Date flow start        Len Proto    Src IP Addr:Port          Dst IP Addr:Port  Packets    Bytes
Apr 13 2005 14:53:35   630 TCP     211.21.10.35:20     ->    196.3.50.254:55260  886934   1.2 GB   2
Apr 13 2005 14:49:39   866 TCP        62.2.16.4:44890 ->     211.21.1.10:119    840504   1.2 GB   2
Apr 13 2005 14:45:59   846 TCP    62.53.226.182:44671 ->     211.21.1.10:119    701456 991.3 MB   1
Apr 13 2005 14:58:45   320 TCP     211.21.10.21:40398 ->   212.31.34.212:435    435334 619.0 MB   2
Apr 13 2005 14:45:26  1121 TCP     211.21.10.35:58992 ->    80.24.26.102:28266  319523 457.1 MB   4
Apr 13 2005 14:50:03   842 TCP      211.21.1.10:43979 ->   164.172.36.58:119    270816 381.1 MB   2
Apr 13 2005 14:49:20   888 TCP     211.21.10.21:40572 -> 162.162.153.116:433    205729 288.7 MB   3
Apr 13 2005 14:53:01   667 TCP     211.21.10.35:80    ->   81.56.217.164:33732  204589 283.3 MB   3
Apr 13 2005 14:47:29   997 TCP     211.21.10.35:55866 ->   83.173.244.45:17079  205958 254.8 MB   3
Apr 13 2005 14:48:50   915 TCP     211.21.10.21:40485 -> 162.162.153.116:433    200618 281.5 MB   2
```

(IP addresses anonymised)

SWITCH
The Swiss Education & Research Network

Create TopN statistics IP addresses, Ports:

```
nfsrv% nfdump -r nfcapd.200504131500 -n 10 -s dstport
Flows analysed: 3136914 matched: 3136914, Bytes read: 153167712
Number of IP addr 65208
Time window: Apr 13 2005 14:44:50 - Apr 13 2005 15:04:59
Top 10    Dst Port counts:
Date first seen           Len        Dst Port  Packets     Bytes   Flows
Apr 13 2005 14:44:53     1206              80  8551963  829.3 MB  351633
Apr 13 2005 14:44:53     1198              53  1062287   81.8 MB  304564
Apr 13 2005 14:44:51     1200             123   316006   22.9 MB  222275
Apr 13 2005 14:58:24      393            1433   189067    9.6 MB  158998
Apr 13 2005 14:48:54      962             445   219088   11.9 MB  116296
Apr 13 2005 14:44:54     1197               0   717472  310.2 MB  107595
Apr 13 2005 14:50:38      859             135   135711    6.7 MB   97032
Apr 13 2005 14:46:14     1117            4672   107272   10.3 MB   77803
Apr 13 2005 14:44:53     1206            4662  2479351    1.7 GB   51231
Apr 13 2005 14:52:58      713            3306    72365    4.3 MB   46010


nfsrv% nfdump -r nfcapd.200504131500 -n 10 -s srcip
Flows analysed: 3136914 matched: 3136914, Bytes read: 153167712
Number of IP addr 373382
Time window: Apr 13 2005 14:44:50 - Apr 13 2005 15:04:59
Top 10 Src IP Addr counts:
Date first seen           Len     Src IP Addr  Packets     Bytes   Flows
Apr 13 2005 14:44:51     1207    149.166.2.21   220281   11.2 MB  143596
Apr 13 2005 15:02:30       88    81.208.28.50   129377    1.9 MB  129375
Apr 13 2005 14:44:54     1197   199.81.104.52   341597   40.4 MB   77627
Apr 13 2005 14:59:47      304   200.48.111.64    63820    2.9 MB   43089
Apr 13 2005 14:44:53     1198     211.21.1.80   110847   11.0 MB   33535
Apr 13 2005 14:59:50      301  213.180.210.35    29765    1.3 MB   29641
Apr 13 2005 14:59:22      335   141.249.141.4   148644   84.3 MB   20252
Apr 13 2005 14:45:02     1189  191.176.20.204    34824    6.0 MB   14684
Apr 13 2005 15:01:53       85    54.57.93.182    14565  654.3 KB   14561
Apr 13 2005 14:59:19      332  54.211.161.192    21615    1.1 MB   14039
```

NfSen/nfdump

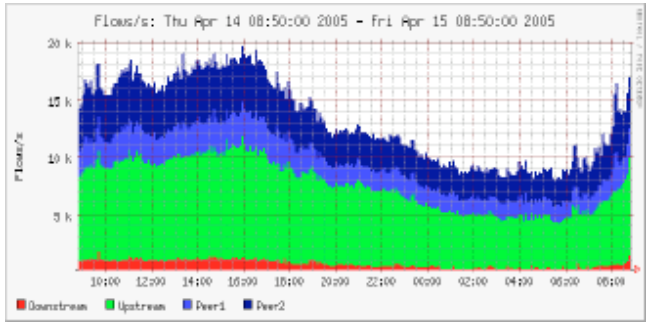
SWITCH
The Swiss Education & Research Network

Command line based tool:

- Flexible
- Easy to use
- Fast
- …

but …

… don't we all like pictures?



NfSen

SWITCH
The Swiss Education & Research Network

Wish list:

- Use nfdump as backend tool. ⇒ modular design.
- Pictures!
- Graph current network situation.
- Graph specific profiles.
  - Track hosts, ports etc. from live data.
  - Profile hosts involved in incidents from history data.
- Drill down from overview to the details down to the specific flows.
- Analyse a specific time window.
- Web based.
- Automatic alerting.
- Flexible extensions using plugins.
- Easy to use.
- Auto - Cleanup. Aging data files: max space, max lifetime.

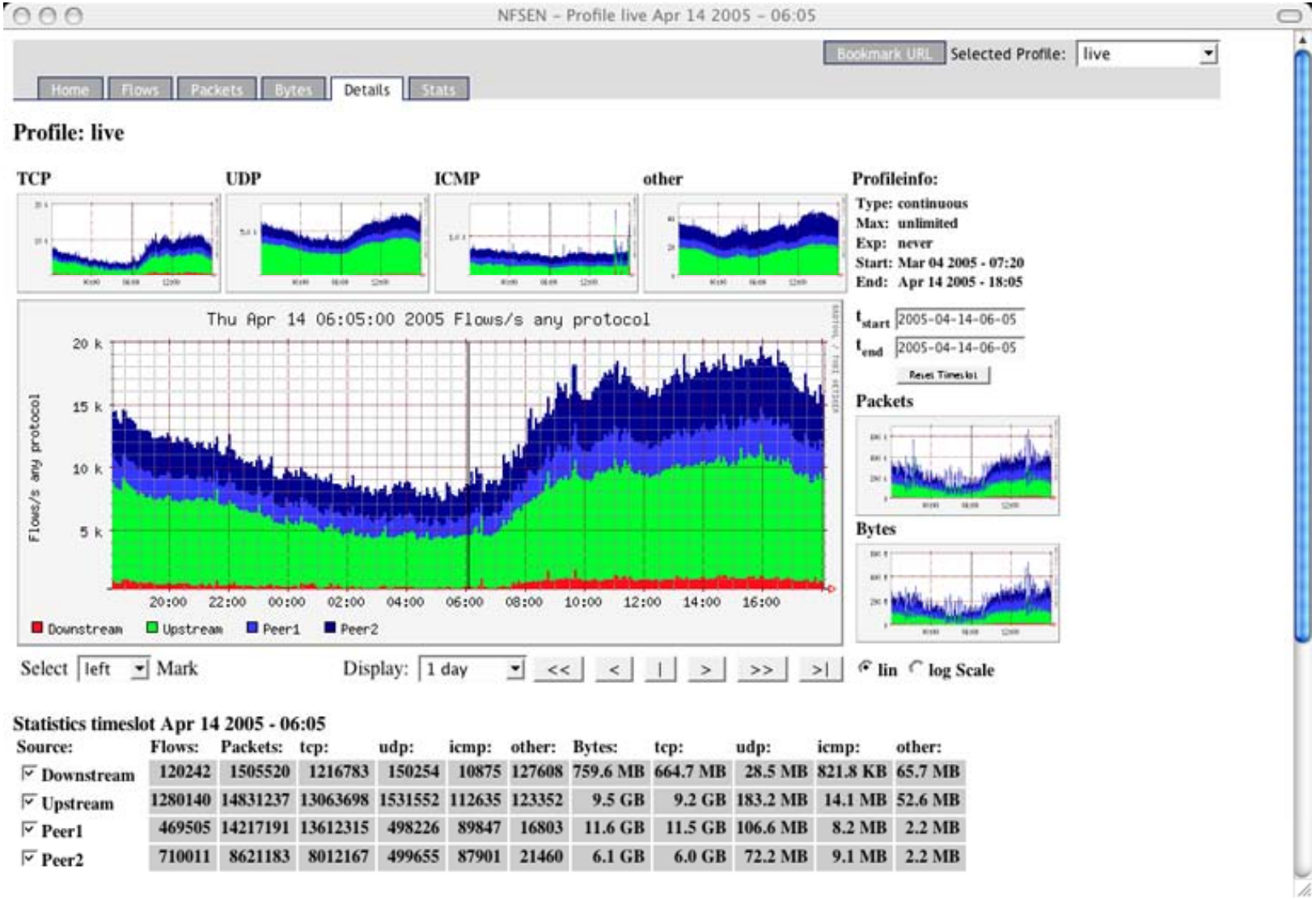
NfSen

SWITCH cert

NfSen


NFSEN – Profile live Overview
Bookmark URL
Selected Profile: live
Home
Flows
Packets
Bytes
Details
Stats
Type: Continuous
Overview Profile: live

NfSen

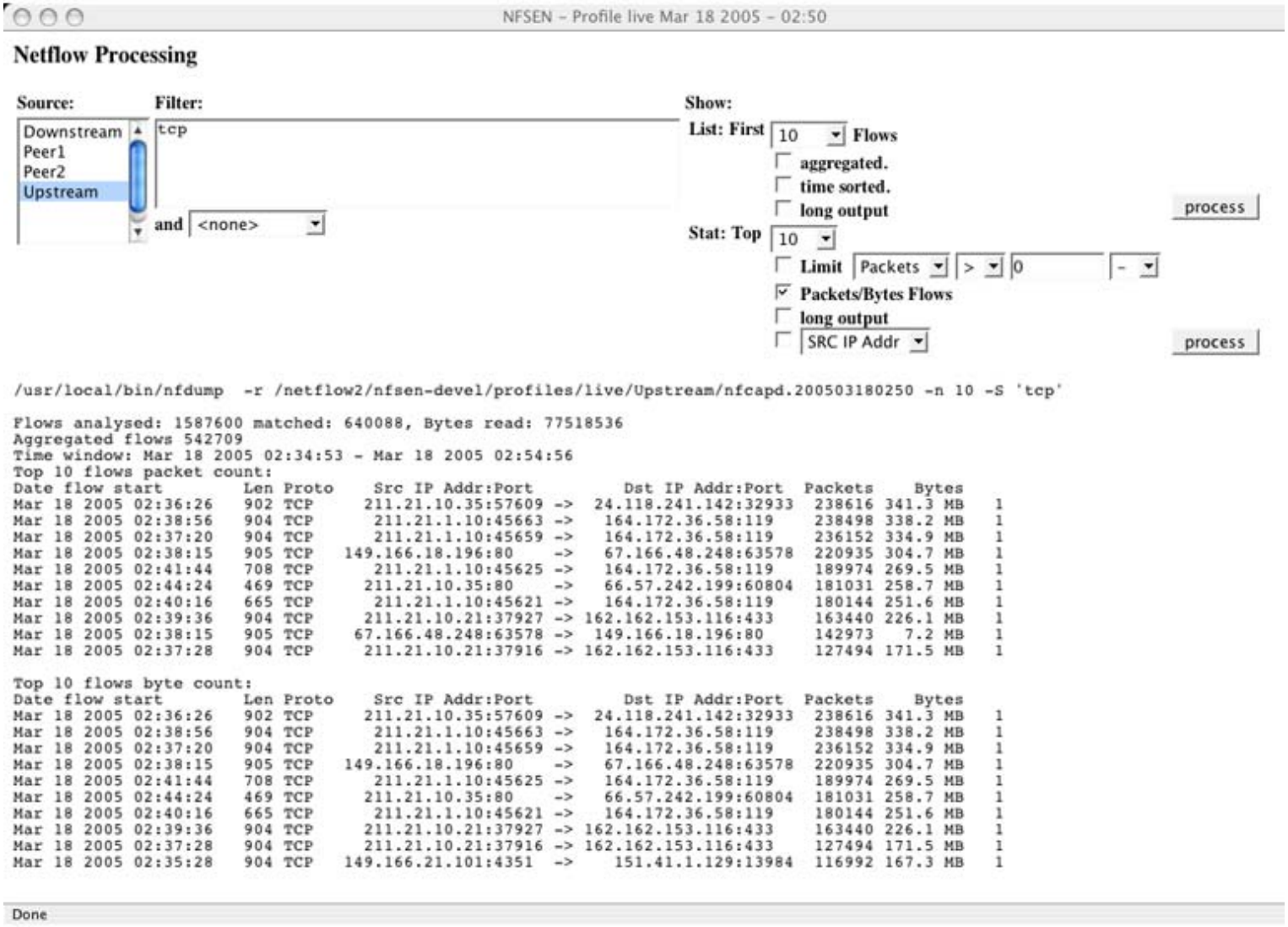


Statistics timeslot Apr 14 2005 - 06:05

Source:	Flows:	Packets:	tcp:	udp:	icmp:	other:	Bytes:	tcp:	udp:	icmp:	other:
Downstream	120242	1505520	1216783	150254	10875	127608	759.6 MB	664.7 MB	28.5 MB	821.8 KB	65.7 MB
Upstream	1280140	14831237	13063698	1531552	112635	123352	9.5 GB	9.2 GB	183.2 MB	14.1 MB	52.6 MB
Peer1	469505	14217191	13612315	498226	89847	16803	11.6 GB	11.5 GB	106.6 MB	8.2 MB	2.2 MB
Peer2	710011	8621183	8012167	499655	87901	21460	6.1 GB	6.0 GB	72.2 MB	9.1 MB	2.2 MB

NfSen

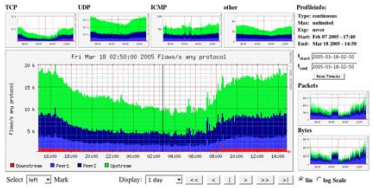
SWITCH
The Swiss Education & Research Network



(IP addresses anonymised)

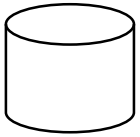
NfSen/nfdump

Putting all together:

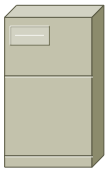


From:
To:

Summary:
monitored:
...
..



```
cobol% nfflt -r /netflow0/nfsen/spool/swiix1/nfcapd.200405170940 -c 10
May 17 2004 09:39:42      0 TCP    192.33.107.206:0     ->    80.142.112.36:0       1    40  8
May 17 2004 09:39:42      0 TCP    195.174.131.65:3880  ->   192.33.227.81:15000    1    48  8
May 17 2004 09:39:43      0 TCP    80.196.222.194:31910 ->   192.33.223.236:135     1    48  8
May 17 2004 09:39:43      0 TCP  193.189.164.241:41478  ->    192.33.120.24:5000    1    48  8
May 17 2004 09:39:43      0 TCP  212.238.236.208:2493   ->   192.33.120.96:2745     1    48  8
May 17 2004 09:39:43      0 TCP  212.238.236.208:2494   ->    192.33.120.96:135     1    48  8
May 17 2004 09:39:43      0 TCP  212.238.236.208:2495   ->    192.33.120.96:135     1    48  8
May 17 2004 09:39:34      9 TCP      68.93.60.50:2580   ->   192.33.216.177:2745     3   144  8
May 17 2004 09:39:34      9 TCP      68.93.60.50:2581   ->   192.33.216.177:135      3   144  8
May 17 2004 09:39:34      9 TCP    154.20.99.176:2108   ->   192.33.228.187:445      3   144  8
cobol%
```



softflowd
pfflowd

Input

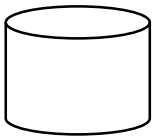
netflow v5, v7

Web Front-end

Post Processing

CLI

Periodic Update Tasks & Plugins



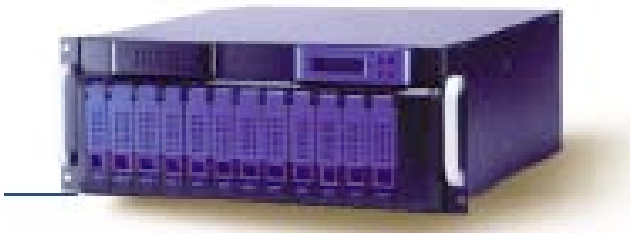
nfdump Backend

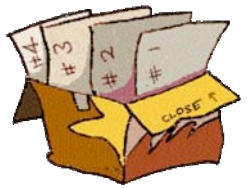
NfSen/nfdump

SWITCH
The Swiss Education & Research Network

Figures @ SWITCH:

- Server: 2 x 3GHz 2GB Ram. Debian Linux Kernel 2.6.10
- 3TB (2TB + 1TB) AXUS Disk Raid
- XFS file system.
- Gigabit Ethernet interfaces.
- 5min workload avg. ca. 5%.
- 25GB Netflow data / day.
- About 41 days of netflow data available.

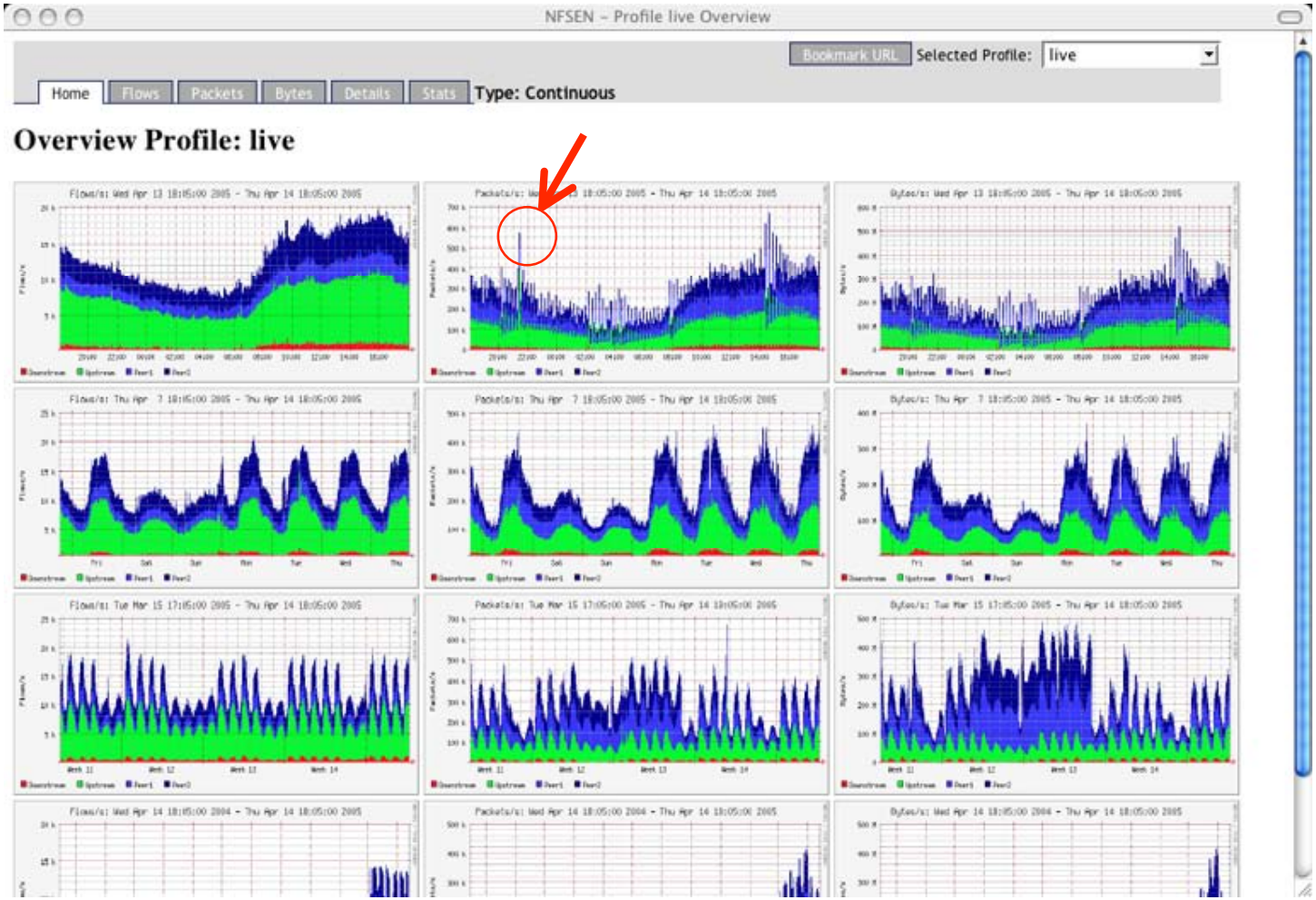




NfSen/nfdump in Action

SWITCH
The Swiss Education & Research Network

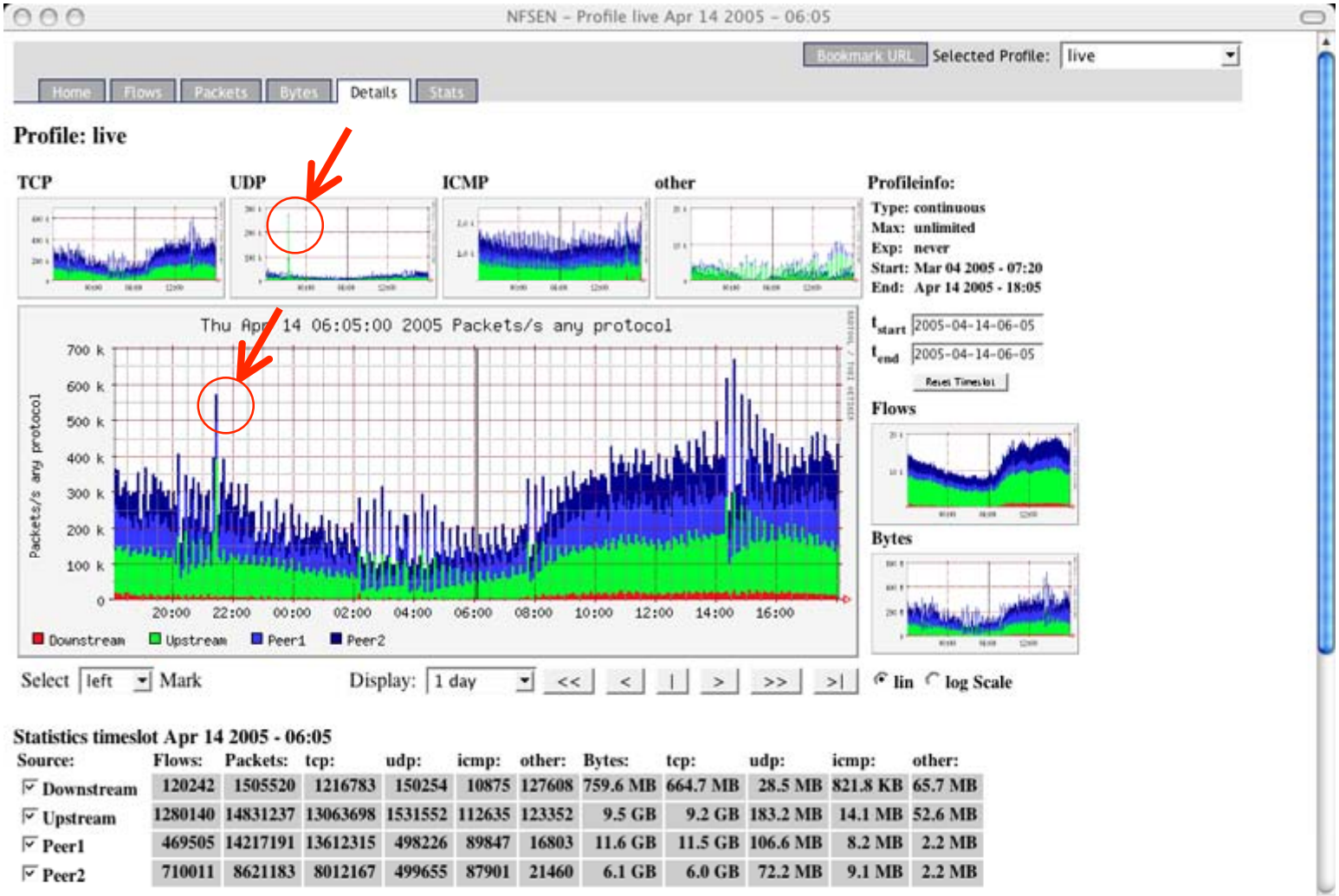
Overview - Details - Flows



NfSen/nfdump in Action

SWITCH
The Swiss Education & Research Network

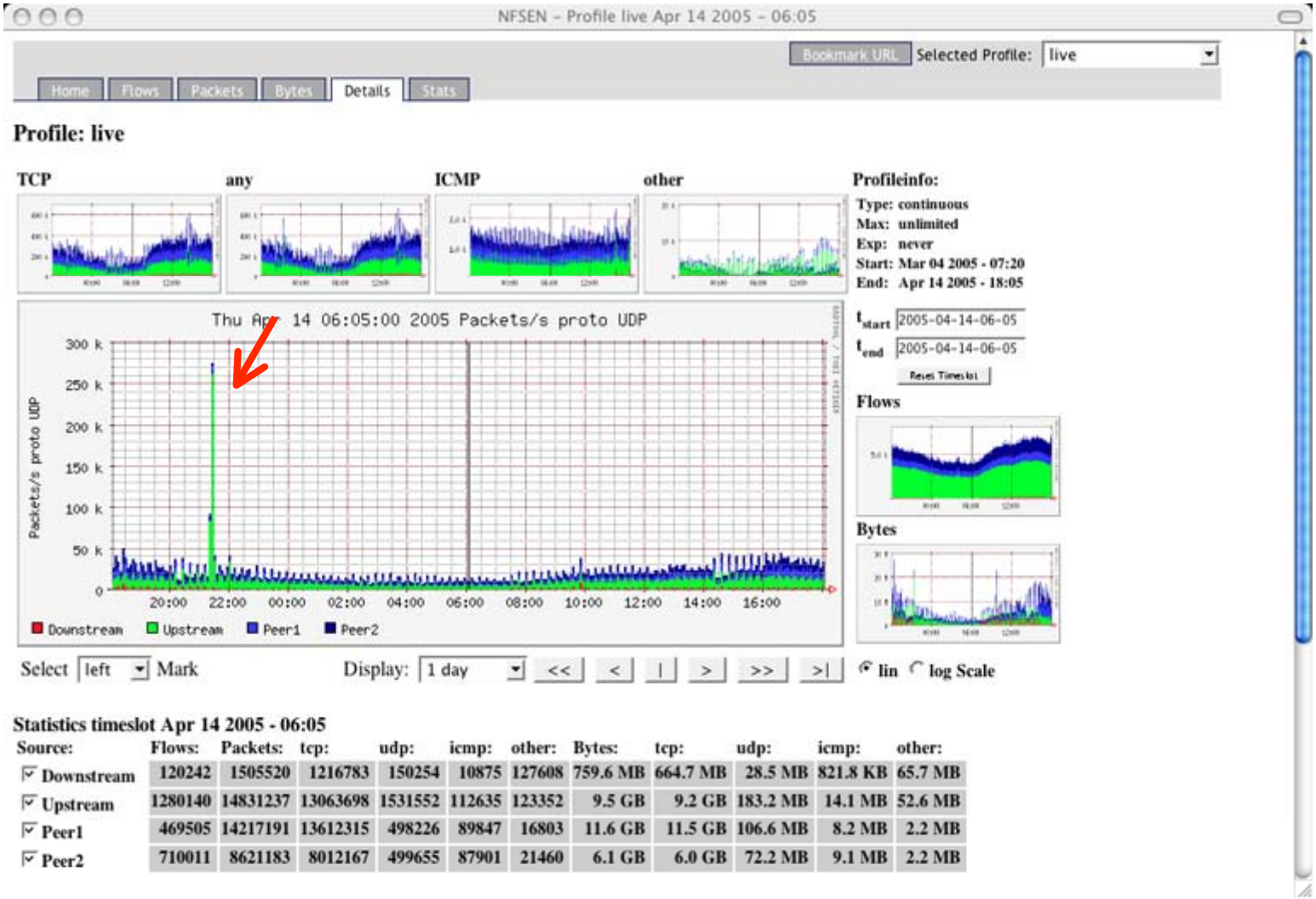
Overview - **Details** - Flows



NfSen/nfdump

SWITCH
The Swiss Education & Research Network

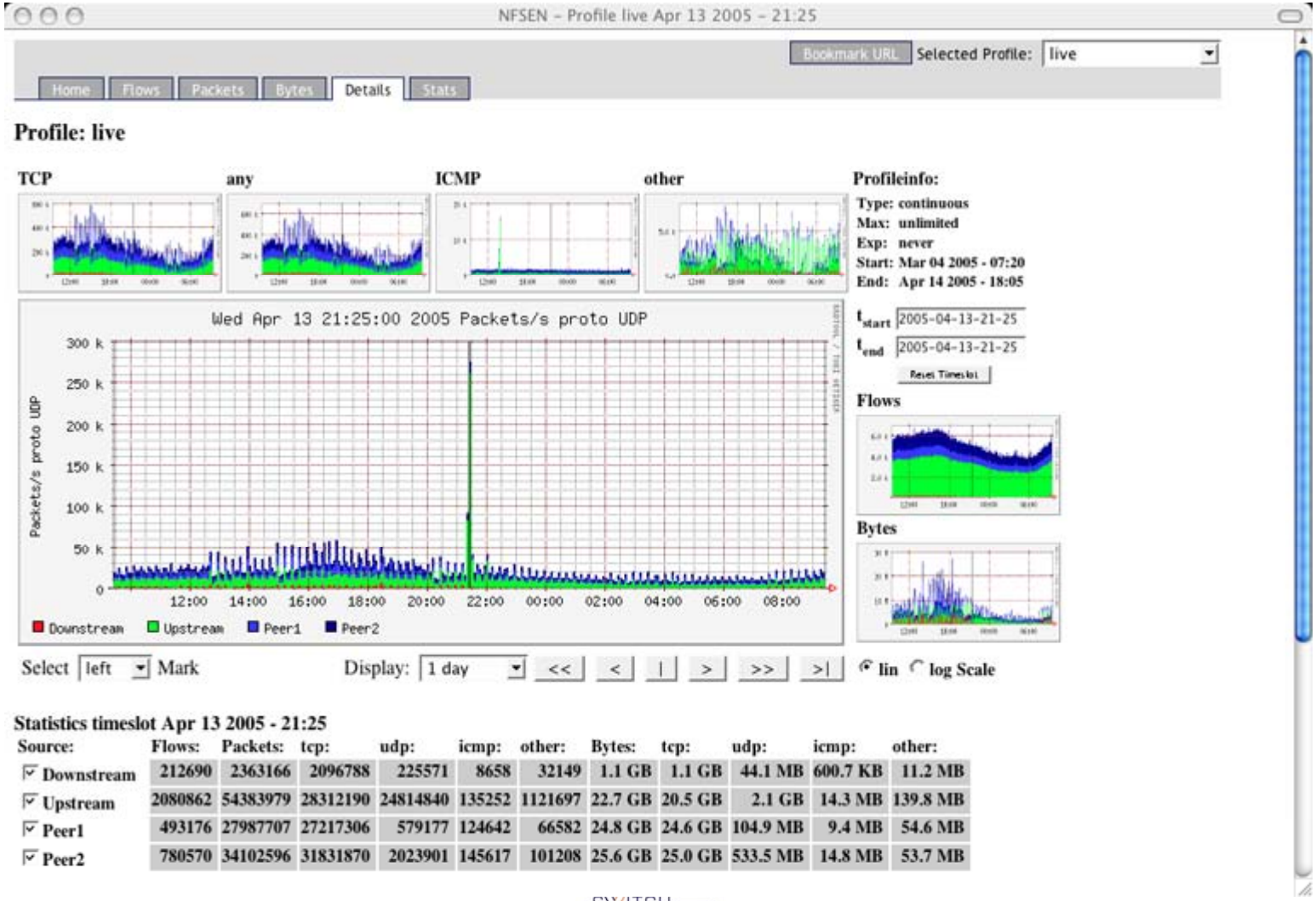
Overview - **Details** - Flows



Source:	Flows:	Packets:	tcp:	udp:	icmp:	other:	Bytes:	tcp:	udp:	icmp:	other:
Downstream	120242	1505520	1216783	150254	10875	127608	759.6 MB	664.7 MB	28.5 MB	821.8 KB	65.7 MB
Upstream	1280140	14831237	13063698	1531552	112635	123352	9.5 GB	9.2 GB	183.2 MB	14.1 MB	52.6 MB
Peer1	469505	14217191	13612315	498226	89847	16803	11.6 GB	11.5 GB	106.6 MB	8.2 MB	2.2 MB
Peer2	710011	8621183	8012167	499655	87901	21460	6.1 GB	6.0 GB	72.2 MB	9.1 MB	2.2 MB

NfSen/nfdump

Overview - **Details** - Flows

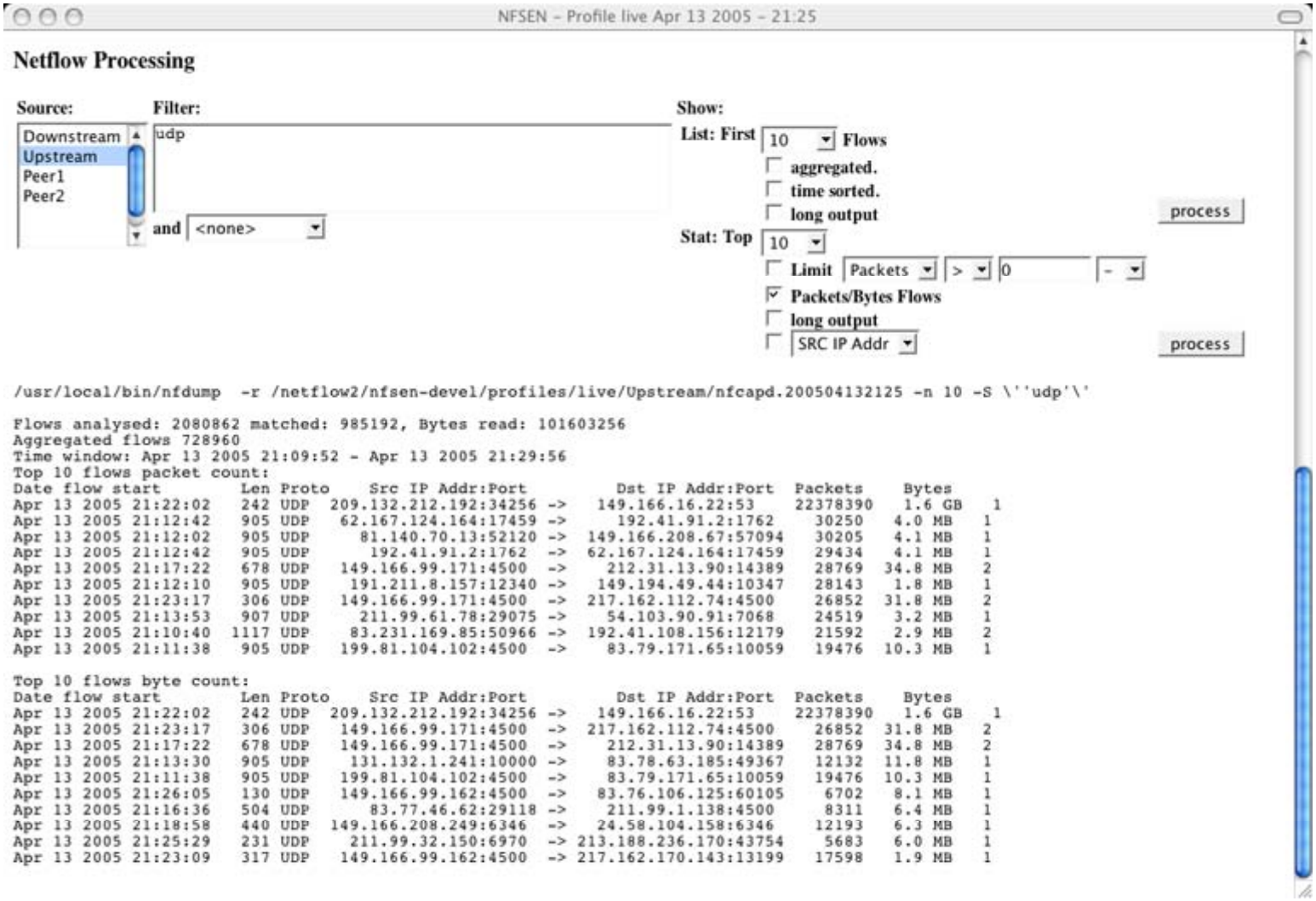


Source:	Flows:	Packets:	tcp:	udp:	icmp:	other:	Bytes:	tcp:	udp:	icmp:	other:
Downstream	212690	2363166	2096788	225571	8658	32149	1.1 GB	1.1 GB	44.1 MB	600.7 KB	11.2 MB
Upstream	2080862	54383979	28312190	24814840	135252	1121697	22.7 GB	20.5 GB	2.1 GB	14.3 MB	139.8 MB
Peer1	493176	27987707	27217306	579177	124642	66582	24.8 GB	24.6 GB	104.9 MB	9.4 MB	54.6 MB
Peer2	780570	34102596	31831870	2023901	145617	101208	25.6 GB	25.0 GB	533.5 MB	14.8 MB	53.7 MB

NfSen/nfdump in action

SWITCH
The Swiss Education & Research Network

Overview - Details - **Flows**

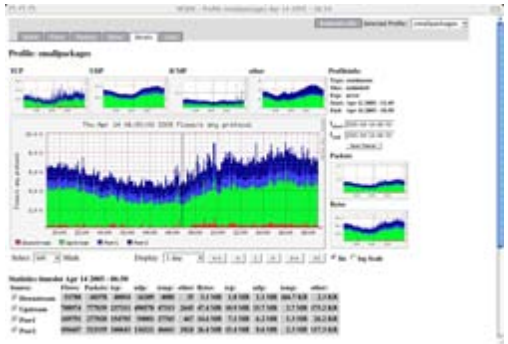


NfSen/nfdump

SWITCH
The Swiss Education & Research Network

Profiles:

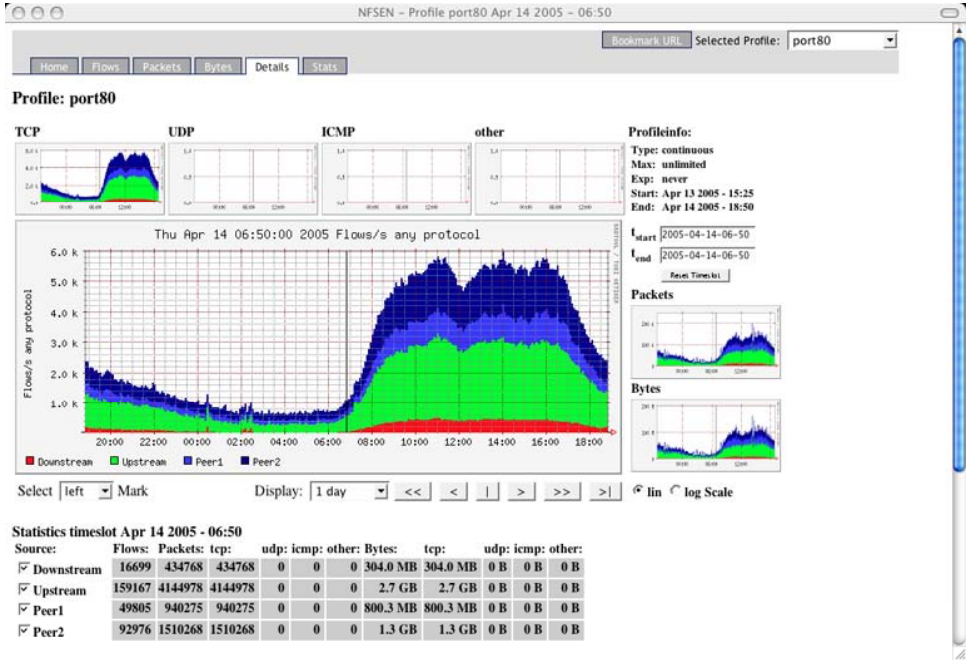
- A profile is a specific view on the netflow data with nfdump filters applied.
- The profile applies to the graphical as well as to the numerical view.
- Profiles can be created from data in the past. (static)
- Profiles can be created from incoming data (continuous)
- Any views or processing options are available.



NfSen/nfdump

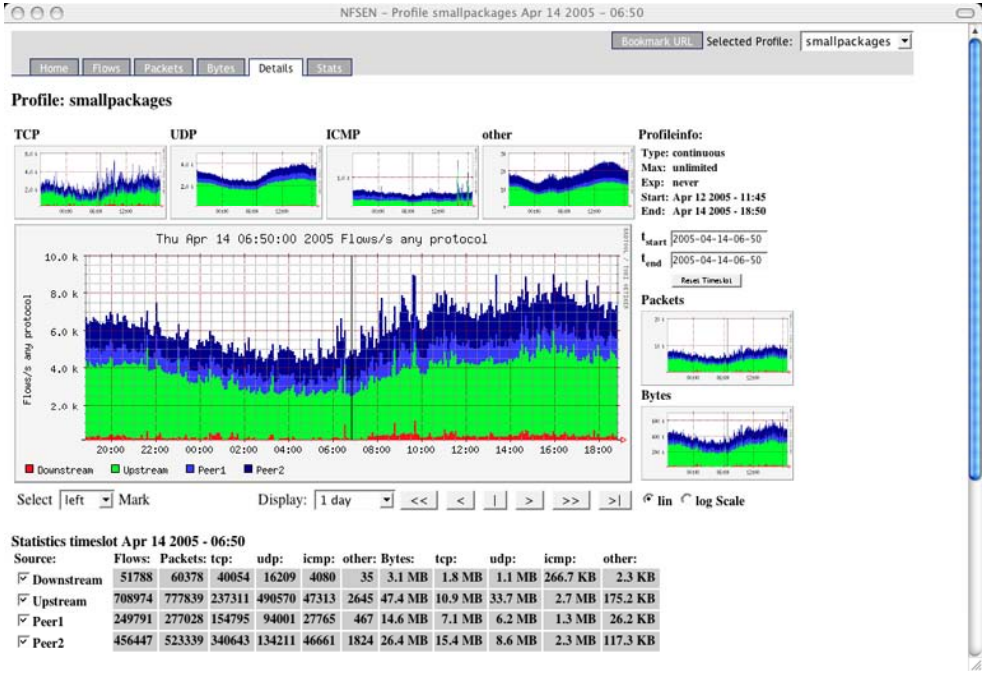
Example Profiles:

Filter: ‘tcp and port 80’



Source:	Flows:	Packets:	tcp:	udp:	icmp:	other:	Bytes:	tcp:	udp:	icmp:	other:
Downstream	16699	434768	434768	0	0	0	304.0 MB	304.0 MB	0 B	0 B	0 B
Upstream	159167	4144978	4144978	0	0	0	2.7 GB	2.7 GB	0 B	0 B	0 B
Peer1	49805	940275	940275	0	0	0	800.3 MB	800.3 MB	0 B	0 B	0 B
Peer2	92976	1510268	1510268	0	0	0	1.3 GB	1.3 GB	0 B	0 B	0 B

Filter: ‘bytes < 100’



Source:	Flows:	Packets:	tcp:	udp:	icmp:	other:	Bytes:	tcp:	udp:	icmp:	other:
Downstream	51788	60378	40054	16209	4080	35	3.1 MB	1.8 MB	1.1 MB	266.7 KB	2.3 KB
Upstream	708974	777839	237311	490570	47313	2645	47.4 MB	10.9 MB	33.7 MB	2.7 MB	175.2 KB
Peer1	249791	277028	154795	94001	27765	467	14.6 MB	7.1 MB	6.2 MB	1.3 MB	26.2 KB
Peer2	456447	523339	340643	134211	46661	1824	26.4 MB	15.4 MB	8.6 MB	2.3 MB	117.3 KB

Filters may be as complex as the the filter syntax of nfdump allows.
Example: ‘src net 172.16/16 and src port > 1024 and dst host 192.168.16.17 and dst port 80 and packets > 1000’

NfSen/nfdump

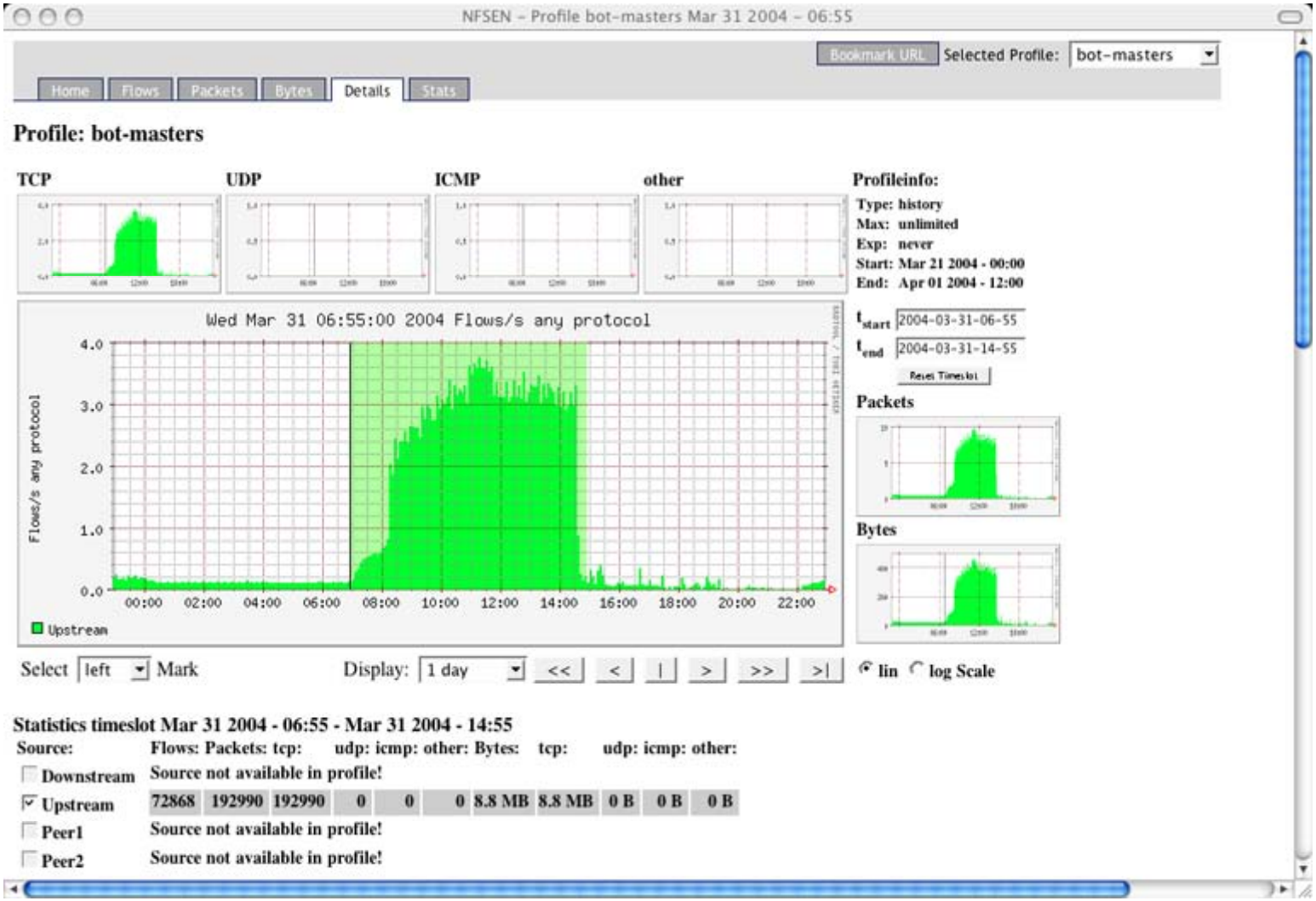
SWITCH
The Swiss Education & Research Network

Incident Handling:

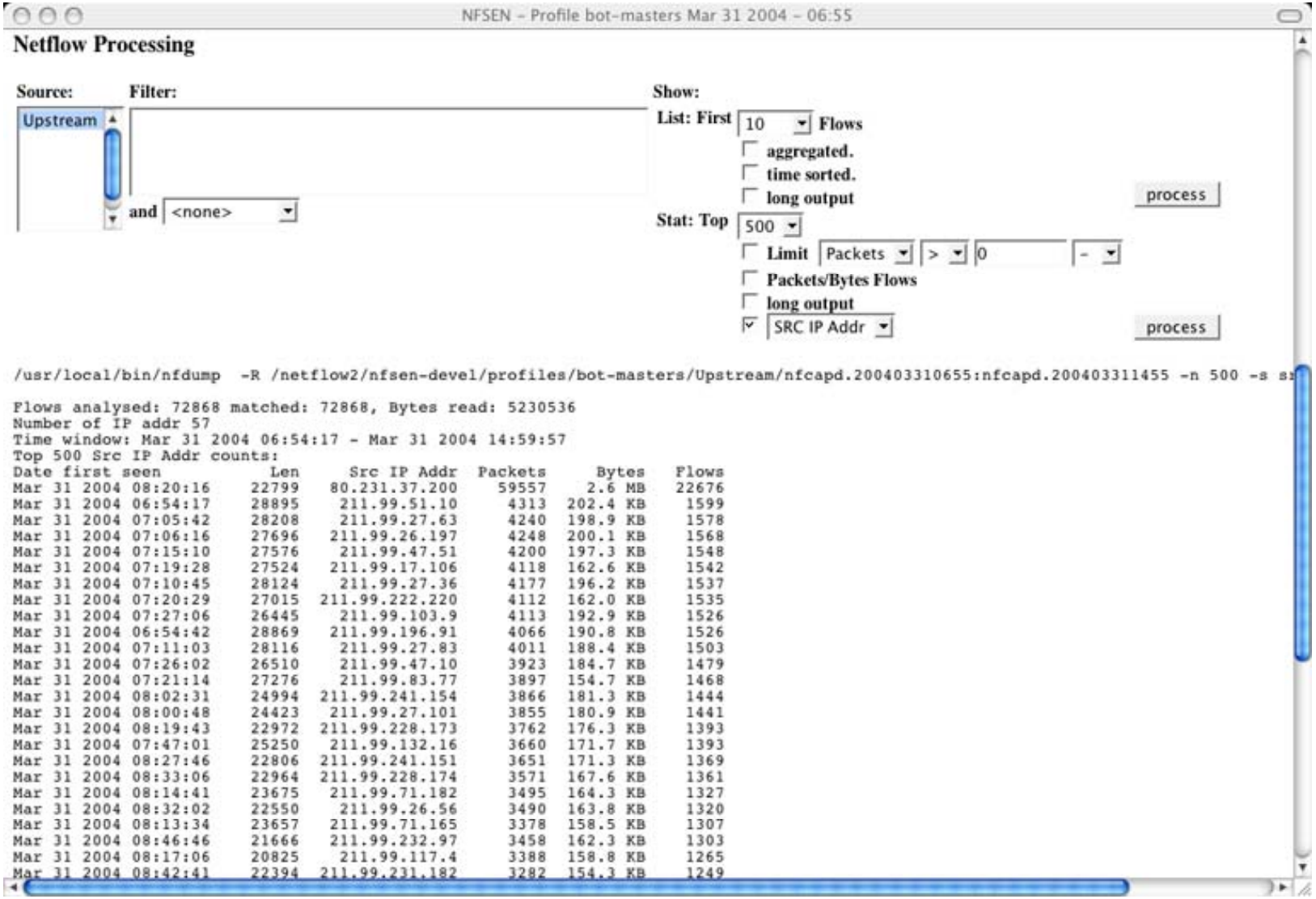
1. Customer calls and reports a hacked system:
2. Customer reports IRC connection on hacked host.
3. In agreement with the customer to find other infected hosts ⇒ Create history profile of botnet master.

NfSen/nfdump

Analyse Incident:



NfSen/nfdump

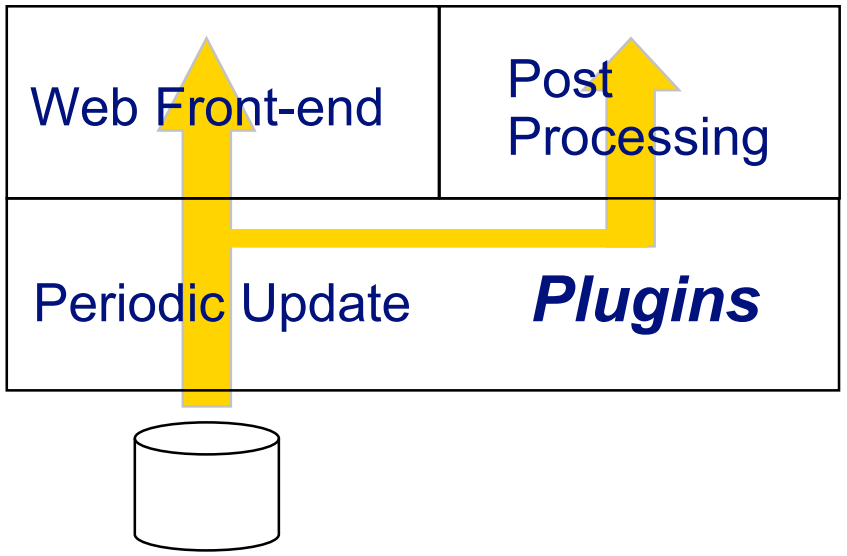


(IP addresses anonymised)

SWITCH
The Swiss Education & Research Network

NfSen Plugins:

NfSen and nfdump are very flexible for a lot of tasks. However, some automated background tasks would be nice!



NfSen/nfdump

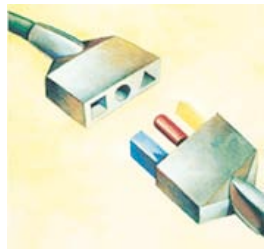
SWITCH
The Swiss Education & Research Network

Plugins - what for?

- Monitoring and alerting.
- Track for known botnet masters and send notifications.
- Track for scanners or DDoS attacks, not necessarily visible in the graph.
- Track for any special pattern you like …

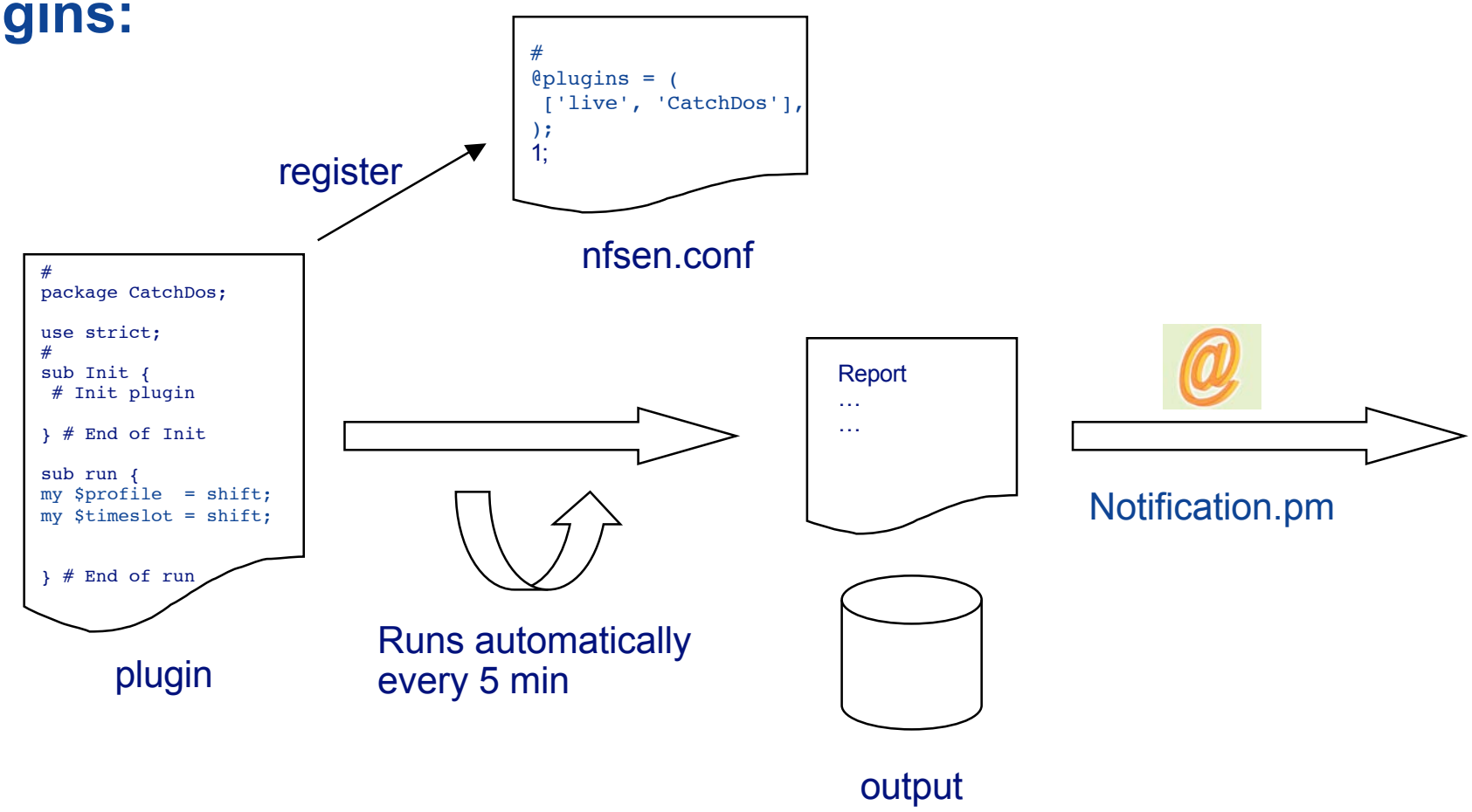
Plugins are:

- Simple Perl modules hooked into NfSen.
- Called at regular 5 Min intervals.



NfSen/nfdump

Plugins:



NfSen/nfdump

SWITCH
The Swiss Education & Research Network

Example:

The plugin processes data with nfdump arguments and filter: -A srcip,dstport -S 'bytes < 70'

Candidates for scanning activities appear:

```
From: nfsen@switch.ch
To: cert@switch.ch
Subject: Scanners

Flows analysed: 2602435 matched: 491818, Bytes read: 127070496
Aggregated flows 176217
Time window: Apr 15 2005 10:44:52 - Apr 15 2005 11:04:54
Top 10 flows packet count:
Date flow start        Len Proto    Src IP Addr:Port          Dst IP Addr:Port  Packets    Bytes  Aggr
Apr 15 2005 10:59:52   298 TCP  149.166.208.111:0     ->         0.0.0.0:135     19154 897.8 KB 19154
Apr 15 2005 10:59:51   115 TCP    221.219.74.59:0     ->         0.0.0.0:4899    14262 668.5 KB 14262
Apr 15 2005 10:59:52   286 TCP     67.67.180.42:0     ->         0.0.0.0:1433    11356 532.3 KB 11356
Apr 15 2005 11:00:55   237 TCP  194.149.144.241:0     ->         0.0.0.0:2100     8654 401.7 KB  8654
Apr 15 2005 11:00:28   250 ICMP   211.144.194.2:0     ->         0.0.0.0:0        6995 437.2 KB  6995
Apr 15 2005 10:59:52   214 ICMP  54.101.213.162:0     ->         0.0.0.0:0        4330 219.9 KB  4330
Apr 15 2005 10:59:52   299 TCP     62.206.4.112:0     ->         0.0.0.0:135      3317 151.5 KB  3317
Apr 15 2005 10:59:52   299 TCP    151.99.143.20:0     ->         0.0.0.0:135      3298 154.6 KB  3298
Apr 15 2005 10:59:52   290 TCP   191.171.226.94:0     ->         0.0.0.0:135      3246 132.2 KB  3246
Apr 15 2005 10:59:53   299 TCP   219.91.168.232:0     ->         0.0.0.0:135      3157 154.0 KB  3157
```

(IP addresses anonymised)

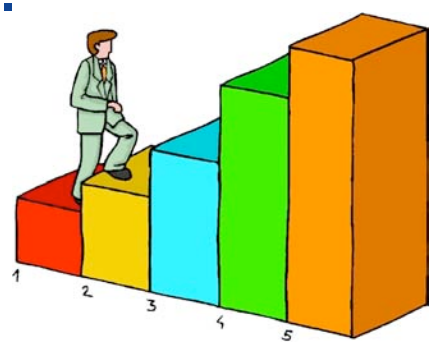
NfSen/nfdump

SWITCH
The Swiss Education & Research Network

Next Steps - Todo list:

NfSen:

- Protocol and TCP/UDP Port Tracking.
- Link Plugins to Web Interface.
- Optional MySQL based logging and reporting extension.
- Anomaly detection.



nfdump:

- Integrate Crypto - PAn:
  Cryptography-based Prefix-preserving Anonymization
- Related filters: 'Worm Footprint Tracking'

```
first { dst ip <A> dst port 445 bytes > 600 }
then { src ip <A> and dst ip 172.16.17.18 and dst port 80 }
```

- Integrate wm.edu Packeteer's PacketShaper patch into nfdump.
- Netflow v9 IPv6
- More - and more flexible statistics.

NfSen/nfdump

SWITCH
The Swiss Education & Research Network

Summary:

- Good and flexible tools for all sort of netflow tasks.
  - Network monitoring.
  - Incident Handling.
  - All sort of tracking …
- Open Source Tools under BSD License.
- Cmd line tool: nfdump
  - Written in C. Runs on most *nix.
    Tested on Linux Kernel 2.4.* and 2.6.*,
    FreeBSD, OpenBSD, Solaris.
  - Available at http://nfdump.sourceforge.net
- Web based frontend: NfSen
  - Written in PHP and Perl.
  - Extendable using plugins.
  - Available at http://nfsen.sourceforge.net
- Possible candidate for the toolset in GN2/JRA2

Questions?