

High-Speed Network Traffic Monitoring Using ntopng

Luca Deri <deri@ntop.org>

Simone Mainardi <mainardi@ntop.org>



Introduction

- ntop develops of open source network traffic monitoring applications.
- ntop (circa 1998) is the first app we released and it is a web-based network monitoring application.
- Today our products range from traffic monitoring, high-speed packet processing (1/10/40/100 Gbit), deep-packet inspection, and IDS/IPS acceleration (snort and suricata), DDoS Mitigation.

ntop's Approach to Traffic Monitoring

- Ability to capture, process and (optionally) transmit traffic at line rate, any packet size.
- Leverage on modern multi-core/NUMA architectures in order to promote scalability.
- Use commodity hardware for producing affordable, long-living (no vendor lock), scalable (use new hardware by the time it is becoming available) monitoring solutions.
- Use open-source to spread the software, and let the community test it on unchartered places.

ntop and Open Source [1/2]

- Since day one most of the ntop tools are open source (GPLv2/3) because:
- The best way to innovate is to listen to our users, let them test our tools, learn from their feedback, integrate their code contributions.
- If open source != no cost, we can benefit from our user community and professional growth.
- When open source == no cost we receive at best bug reports/complains with limited benefits for the project.

ntop and Open Source [2/2]

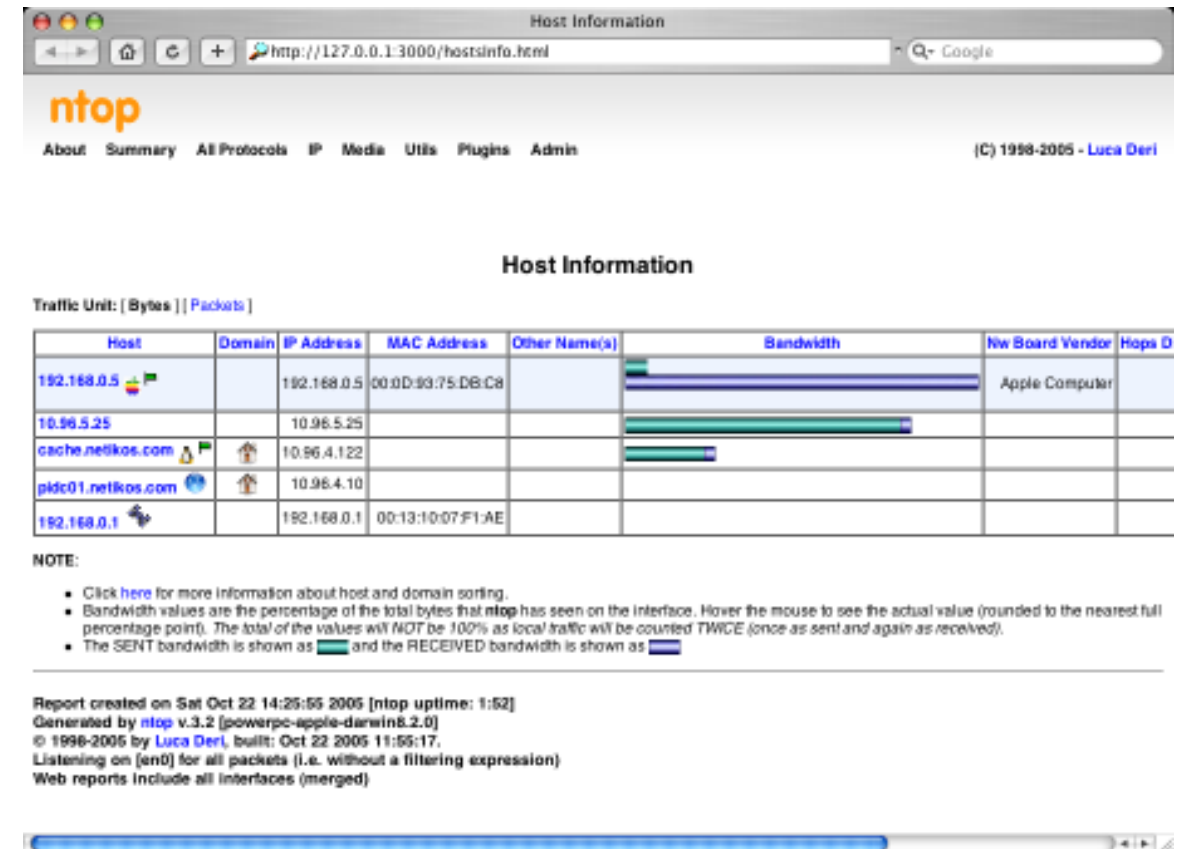
- We produce both open source tools and commercial tools (e.g. packet-to-disk) because we need income to run the project, and donations from open source are limited (< 100€ in 2015)
- Our commercial tools are free of charge for education, no-profit, research because we want to reward our community even when users cannot contribute in code, feedback or bug reports.

Coding...

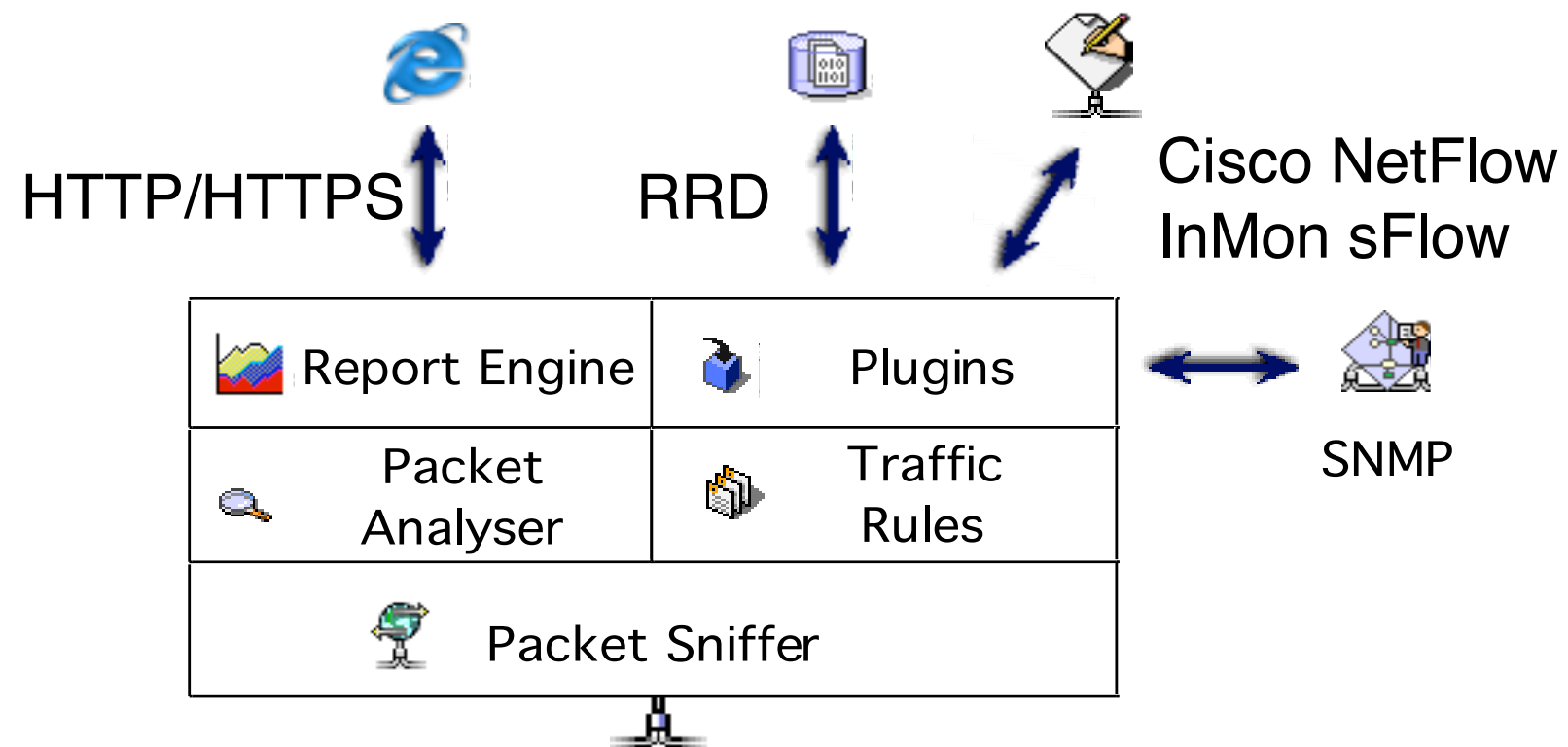
- All our open source software is stored on GitHub (after many years of a home-Ground SVN repository).
- We moved to GitHub because it is currently the best place for accepting contributions, tracking issues (not to mention that if you are not on GitHub you don't exist), and using continuous testing tools (Travis).
- In addition, we run a private ticketing system for selected users who do not want to share their issues (or data to reproduce bugs) due to privacy concerns in their company.

Some History

- In 1998, the original ntop has been created.
- It was a C-based app embedding a web server able to capture traffic and analyse it.
- Contrary to many tools available at that time, ntop used a web GUI to report traffic activities.
- It is available for Unix and Windows under GPL.



ntop Architecture



Why was ntop obsolete?

- Its original LAN-oriented design prevented ntop from handling more than a few hundred Mbit.
- The GUI was an old (no fancy HTML 5) monolithic piece written in C so changing/extending a page required a programmer.
- ntop could not be used as web-less monitoring engine to be integrated with other apps.
- Many components were designed in 1998, and it was time to start over (spaghetti code).

What Is ntopng About?

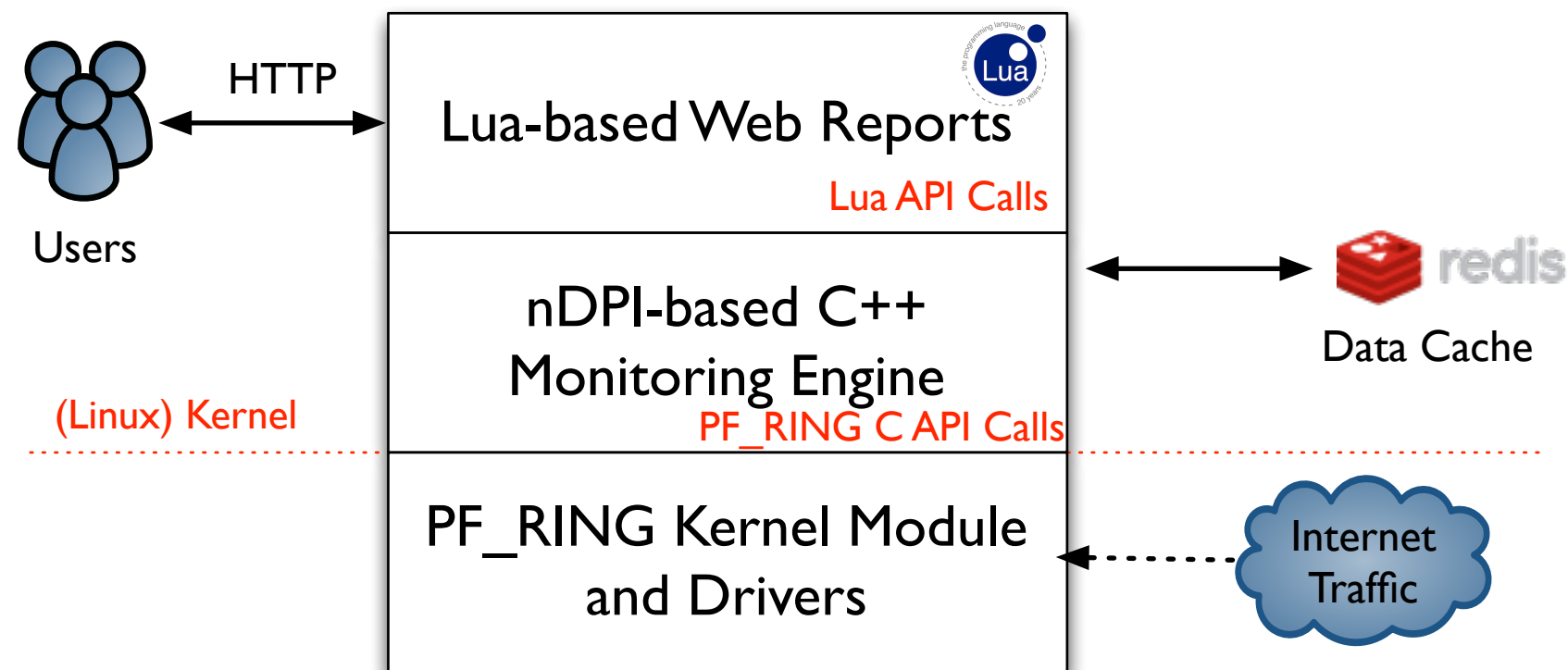
- Ntopng is a web-based, realtime traffic monitoring application able to:
- Provide permanent traffic visibility at 10Gbit+.
- Monitor QoS and QoE.
- Assist with network troubleshooting.
- Interact with external tools (e.g. Wireshark and Nagios) for reporting issues and drill down issues at packet detail.
- Collect both packets and flows (Netflow/IPFIX/sFlow).

ntopng Design Goals

- Clean separation between the monitoring engine and the reporting facilities.
- Robust, crash-free engine (ntop was not really so).
- Platform scriptability for enabling extensions or changes at runtime without restart.
- Realtime: most monitoring tools aggregate data (5 mins usually) and present it when it's too late.
- Many new features including HTML 5-based dynamic GUI, categorisation, DPI.

ntopng Architecture

- Three different and self-contained components, communicating with clean API calls.



ntopng Monitoring Engine

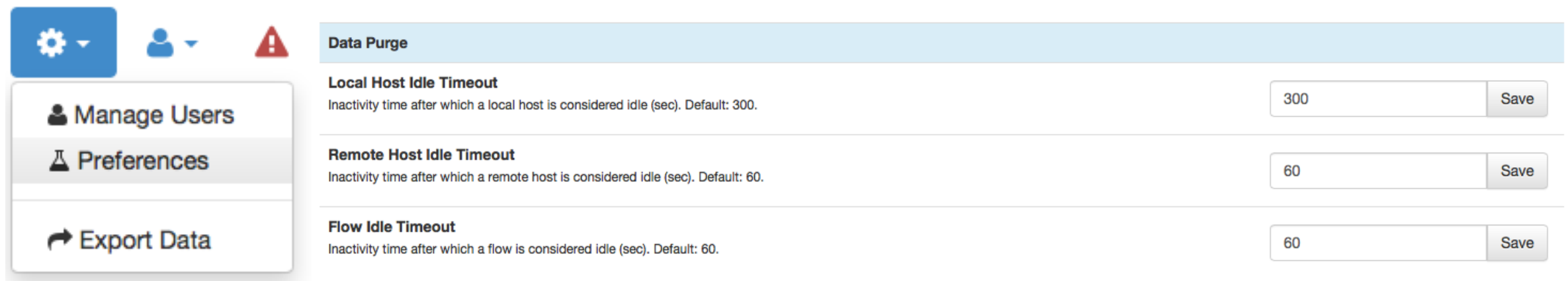
- Coded in C++ and based the concept of flow (set of packets with the same 6-tuple).
- Flows are inspected with a home-grown DPI-library named nDPI aiming to discover the “real” application protocol (no ports are used).
- Information is clustered per:
 - (Capture) Network Device
 - Flow
 - Host

Local vs Remote Hosts

- ntopng keeps information in memory at different level of accuracy in order to save resources for hosts that are not “too relevant”.
- For this reason at startup hosts are divided in:
 - Local hosts
The local host where ntopng is running as well the hosts belonging to some “privileged” IPv4/v6 networks. These hosts are very relevant and thus ntopng keep full statistics.
 - Remote hosts
Non-local hosts for which we keep a minimum level of detail.

Information Lifecycle

- ntopng keeps in memory live information such as flows and hosts statistics.
- As the memory cannot be infinite, periodically non-recent information is harvested.
- Users can specify preferences for data purge:



The screenshot shows the ntopng web interface for configuring data purge settings. On the left is a sidebar with a gear icon, a user icon, and a warning icon. Below these are three menu items: 'Manage Users' (with a person icon), 'Preferences' (with a flask icon), and 'Export Data' (with a download icon). The main content area is titled 'Data Purge' and contains three settings:

Setting	Value	Action
Local Host Idle Timeout Inactivity time after which a local host is considered idle (sec). Default: 300.	300	Save
Remote Host Idle Timeout Inactivity time after which a remote host is considered idle (sec). Default: 60.	60	Save
Flow Idle Timeout Inactivity time after which a flow is considered idle (sec). Default: 60.	60	Save

The need for DPI in Monitoring [1/2]

- Limit traffic analysis at packet header level it is no longer enough (nor cool).
- Network administrators want to know the real protocol without relying on the port being used.
- Selected protocols can be “precisely dissected” (e.g. HTTP) in order to extract information, but on the rest of the traffic it is necessary to tell network administrators what is the protocol flowing in their network.

The need for DPI in Monitoring [2/2]

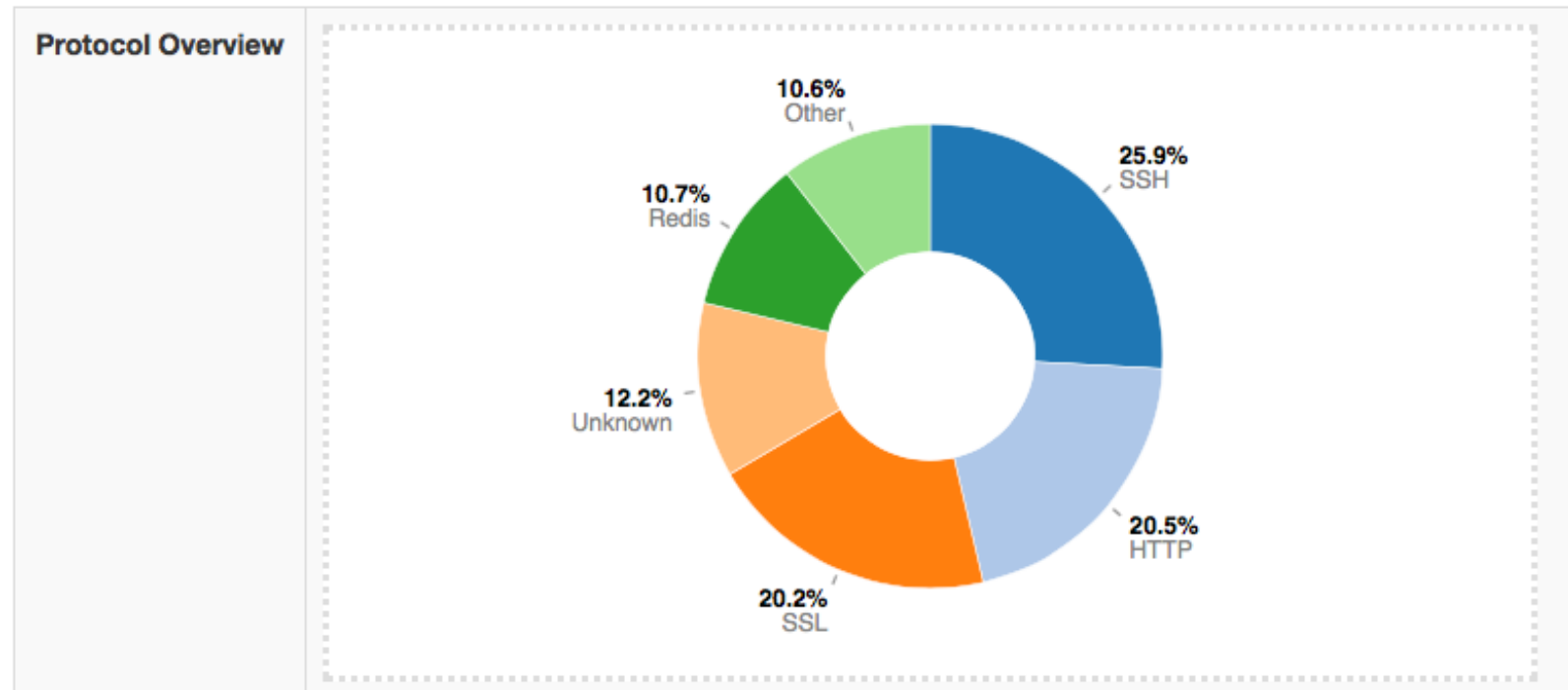
- DPI (Deep Packet Inspection) is a technique for inspecting the packet payload for the purpose of extracting metadata (e.g. protocol).
- There are many DPI toolkits available but they are not what we looked for as:
 - They are proprietary (you need to sign an NDA to use them), and costly for both purchase and maintenance.
 - Adding a new protocol requires vendor support (i.e. it has a high cost and might need time until the vendor supports it) = you're locked-in.
- On a nutshell DPI is a requirement but the market does not offer an alternative for open-source.

Say hello to nDPI

- ntop has decided to develop its own GPL DPI toolkit in order to build an open DPI layer for ntop and third party applications.
- Supported protocols (> 220) include:
 - P2P (Skype, BitTorrent)
 - Messaging (Viber, Whatsapp, MSN, The Facebook)
 - Multimedia (YouTube, Last.fm, iTunes)
 - Conferencing (Webex, CitrixOnline)
 - Streaming (Zattoo, Icecast, Shoutcast, Netflix)
 - Business (VNC, RDP, Citrix, *SQL)

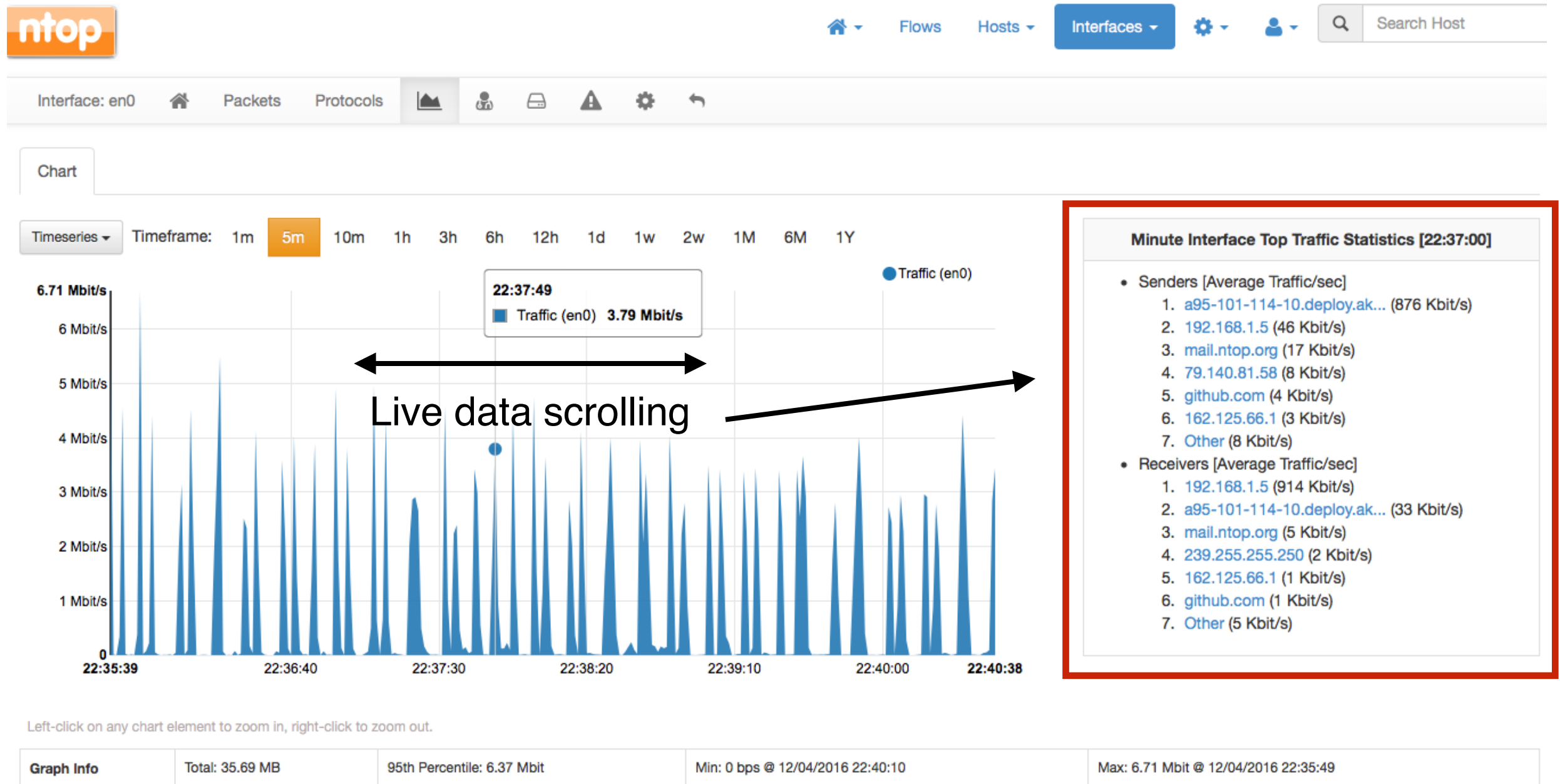


nDPI on ntopng: Interface Report [1/2]



Application Protocol	Total (Since Startup)	Percentage
Apple	17.94 KB	0 %
BitTorrent	90.59 KB	0 %
CiscoVPN	560 Bytes	0 %
DCE_RPC	2.65 KB	0 %
DHCP	1.09 MB	0 %
DHCPV6	3.38 KB	0 %

nDPI on ntopng: Interface Report [2/2]



Historical Flow Navigation

[Summary](#)[IPv4 Flows](#)[IPv6 Flows](#)[Talkers](#)[Protocols](#)

IPv6 Top Flows [11/04/2016 17:56:35 - 11/04/2016 18:56:35]

5 ▾

	Application	L4 Proto	Client	Server	Begin	End	Bytes	Avg Thpt
Info	? Unknown	UDP	simones-macbook-pro.loca...:mdns	ff02::fb:mdns	11/04/2016 18:22:02	11/04/2016 18:22:03	811 B	3.24 Kbit
Info	? Unknown	UDP	simones-macbook-pro.loca...:mdns	ff02::fb:mdns	11/04/2016 18:22:02	11/04/2016 18:22:03	811 B	3.24 Kbit
Info	? Unknown	UDP	fe80::3e15:c2ff:feb7:720...:mdns	ff02::fb:mdns	11/04/2016 18:39:30	11/04/2016 18:39:30	613 B	4.9 Kbit
Info	? Unknown	UDP	fe80::b675:eff:fe92:8917...:dhcpv6-client	ff02::1:2:dhcpv6-server	11/04/2016 18:50:40	11/04/2016 18:50:43	324 B	648 bps
Info	? Unknown	UDP	fe80::b675:eff:fe92:8917...:dhcpv6-client	ff02::1:2:dhcpv6-server	11/04/2016 18:41:55	11/04/2016 18:41:58	324 B	648 bps

Showing 1 to 5 of 65 rows

[«](#) [<](#) [1](#) [2](#) [3](#) [4](#) [5](#) [>](#) [»](#)

Download flows:

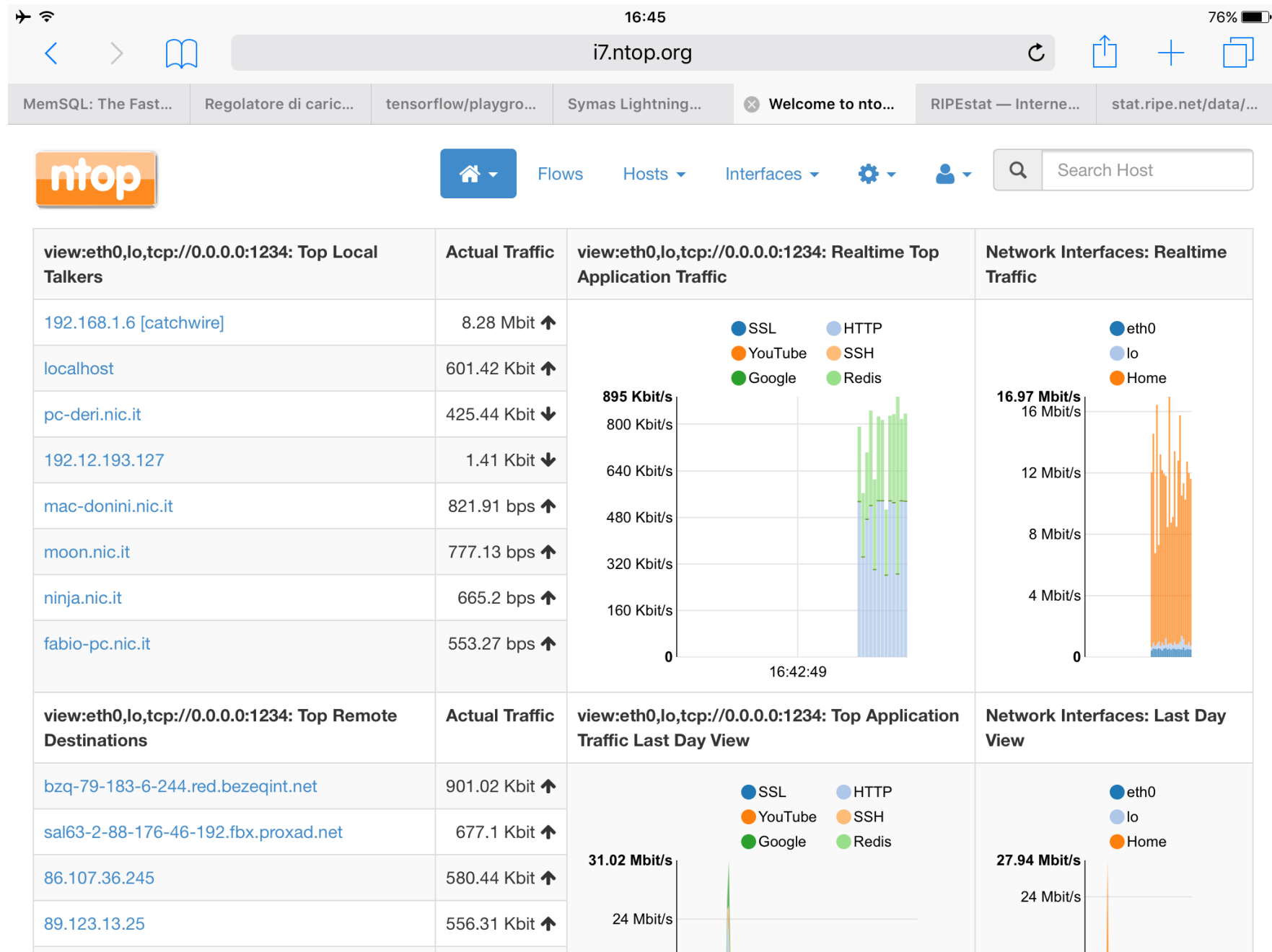
[IPv4](#)[IPv6](#)

Extract pcap:



Bulk download and full
pcap extraction options

Dashboard



Flow View

16:46

75%

i7.ntop.org

MemSQL: The Fast...

Regolatore di caric...

tensorflow/playgro...

Symas Lightning...

Welcome to nto...

RIPEstat — Interne...

stat.ripe.net/data/...

ntop

Flows

Hosts

Interfaces

Search Host

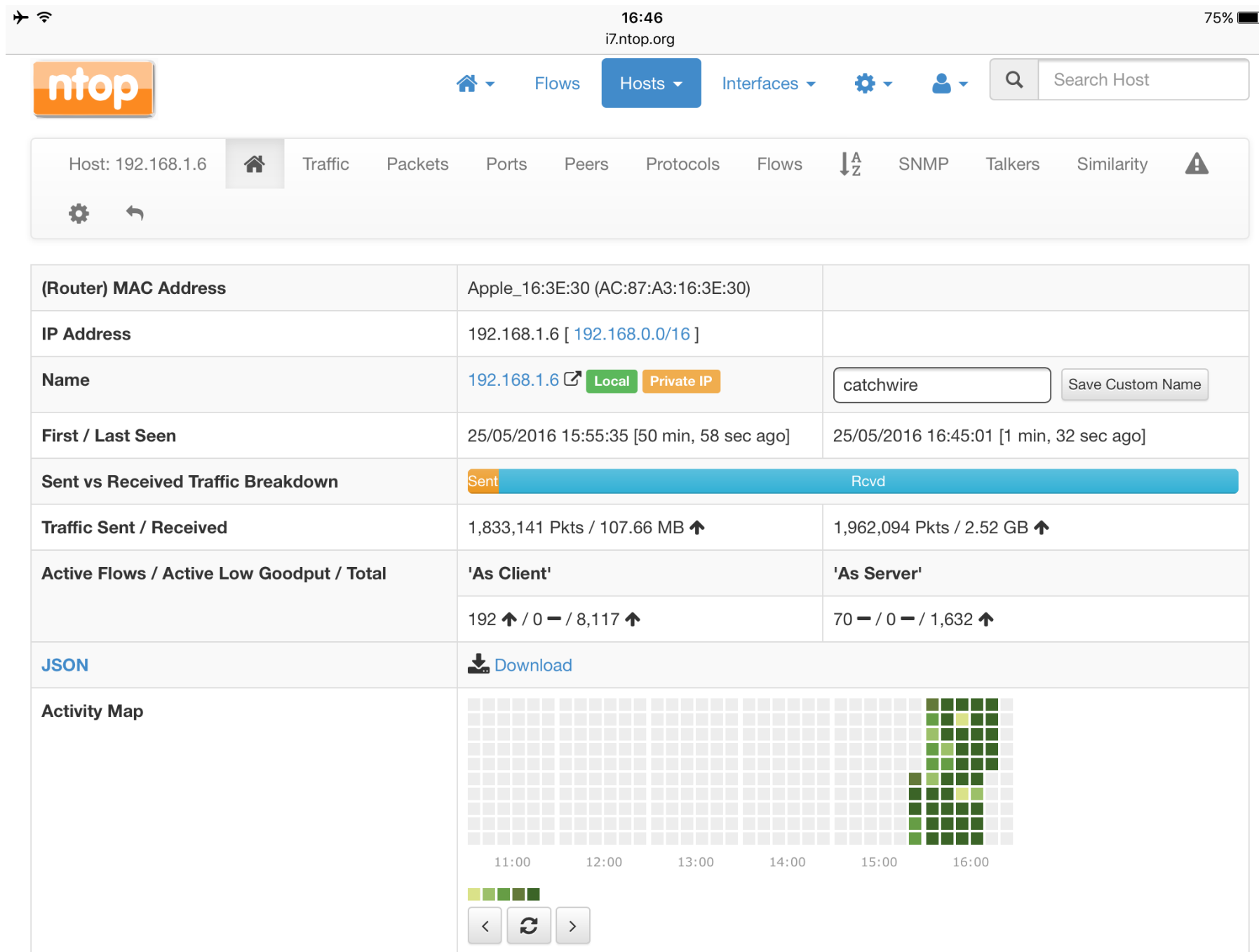
Flow: pc-deri.nic.it:59900 ⇌ 162.125.17.3:443

Overview

Flow Peers [Client / Server]	pc-deri.nic.it:59900 [00:02:CF:76:BB:1B] ⇌ 162.125.17.3:443 [F4:B5:2F:FC:AF:C2]	
Protocol	TCP / SSL.DropBox (121)	
First / Last Seen	25/05/2016 15:46:58 [57 min, 42 sec ago]	25/05/2016 16:44:00 [40 sec ago]
Total Traffic	Total: 121.08 KB —	
	Client → Server: 88 Pkts / 79.35 KB —	Client ← Server: 169 Pkts / 41.74 KB —
	<div> <div>192.12.193.11:59900</div> <div>162.125.17.3:443</div> </div>	
Network Latency Breakdown	55.031 ms (server)	
Application Latency	108.446 ms	
Packet Inter-Arrival Time [Min / Avg / Max]	Client → Server: < 1 ms / 39 sec / 54 sec	Client ← Server: 1 ms / 20 sec / 54 sec
SSL Certificate	notify.dropbox.com	
Max (Estimated) TCP Throughput	Client → Server: 12.06 Kbit	Client ← Server: 209.87 Kbit
TCP Flags	We have not seen flow begin: peer roles (client/server) might be inaccurate. This flow is active.	
Flow Status	Normal	
Actual / Peak Throughput	0 bps — / 2.3 Kbit	



Host View



Historical Talkers

Summary IPv4 Flows IPv6 Flows Talkers Protocols								
Interface en4								
50 ▾								
Host Name	IP Address	Total Traffic	Total Packets	Ingress Traffic	Ingress Packets	Egress Traffic	Egress Packets	Flows
192.168.2.130 🌐	192.168.2.130	18.27 MB	119,364	9.02 MB	86,911	9.25 MB	32,453	2,320

Summary IPv4 Flows IPv6 Flows Talkers Protocols								
Interface en4 / Talkers with 172.217.16.5 ❤️								
50 ▾								
Host Name	IP Address	Total Traffic ▾	Total Packets	Traffic Sent	Packets Sent	Traffic Received	Packets Received	Flows
192.168.2.130 ⇄	192.168.2.130	1.68 MB	3,317	0 B	0	1.68 MB	3,317	12

Summary IPv4 Flows IPv6 Flows Talkers Protocols			
Interface en4 / Talkers with 172.217.16.5 / Applications between 172.217.16.5 and 192.168.2.130 ❤️			
50 ▾			
Application	Traffic Volume	Packets	Flows
Quic	1.68 MB	3,317	12

Downloading ntopng

- ntopng has been packaged for major Linux distributions such as Debian/Ubuntu, CentOS/RedHat and also FreeBSD and OSX (brew): installation couldn't be simpler.



- ntopng is also available for for virtual envs.

- Source: <http://github.com/ntop/ntopng>

- Binary packages: <http://packages.ntop.org> including Raspberry PI and Ubiquiti.



Invitation: Thursday 3-5 PM

- Introduction to ntop network monitoring tools and policy enforcement/DDoS Mitigation
- In depth tutorial on ntopng
- Feedback on roadmap



Using ntopng



Logging into ntopng

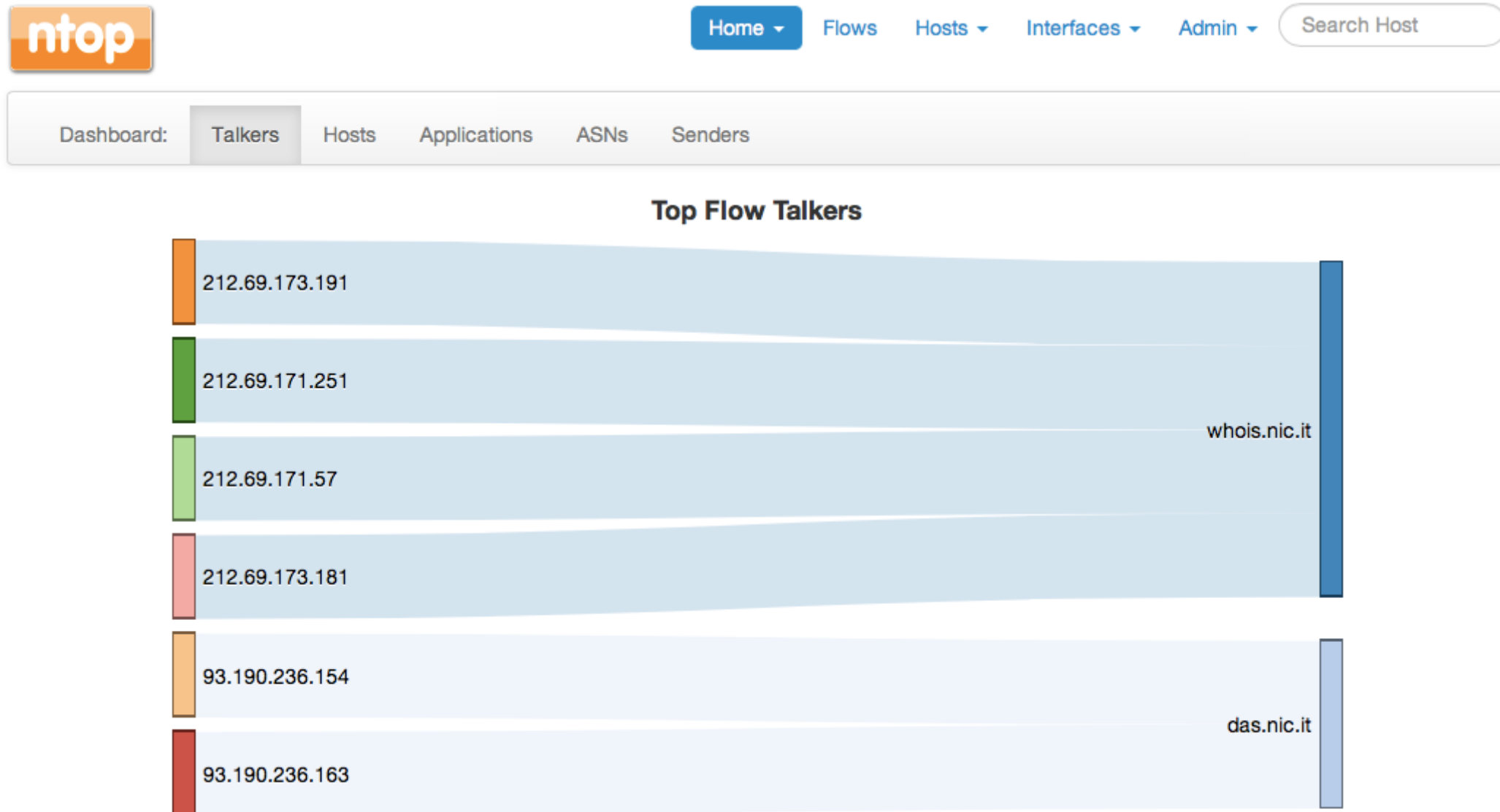
Welcome to ntopng

If you find ntopng useful, please support us by making a small [donation](#). Your funding will help to run and foster the development of this project. Thank you.

© ntop.org - ntopng is released under [GPLv3](#).

Hint: the default user and password are admin

ntopng Dashboard



© 1998-2013 - ntop.org

Generated by ntopng v.1.0.1 (r6749)
for user admin and interface eth5



26.08 Mbps [33,317 pps]

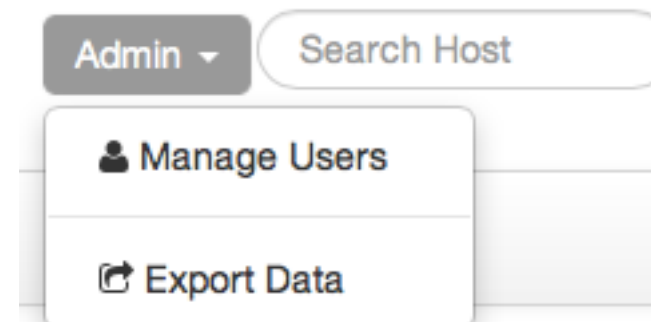
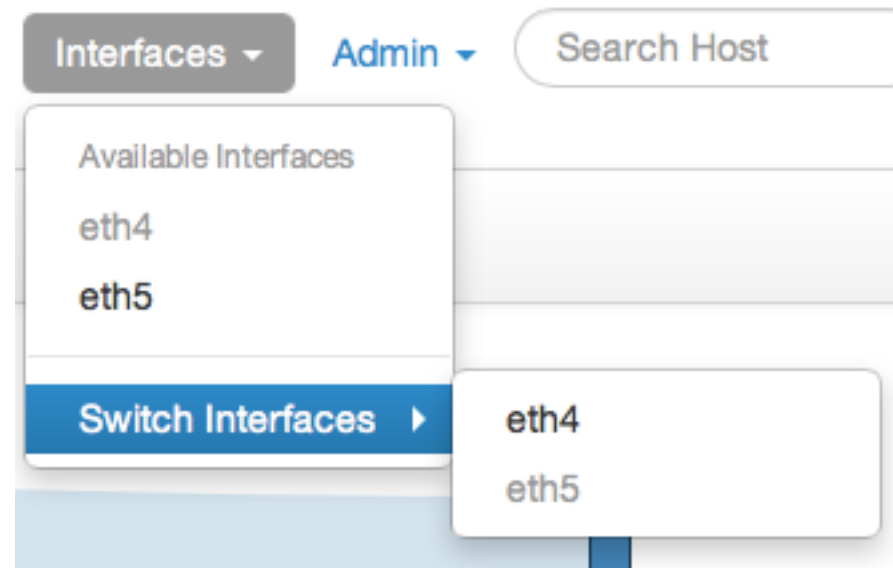
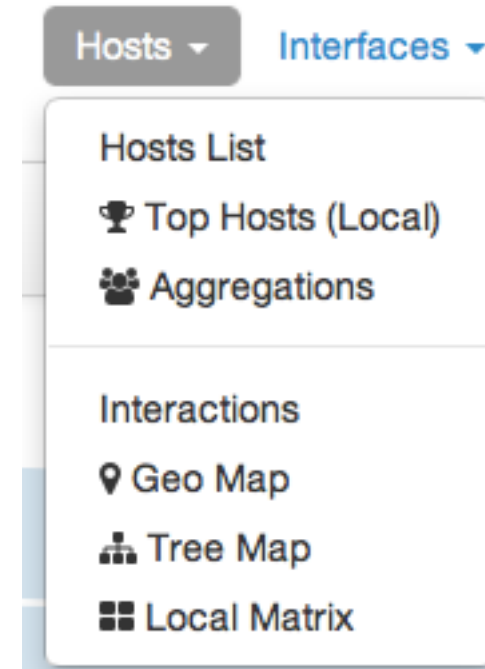
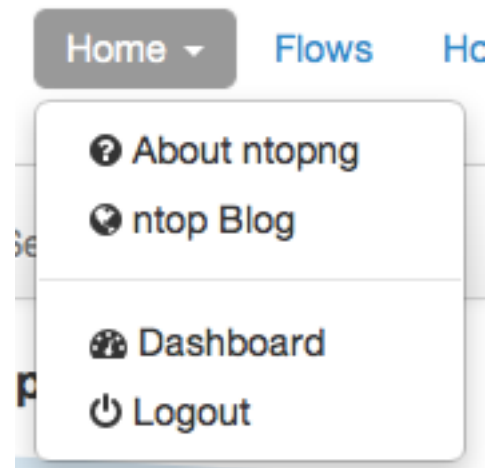
Uptime: 1 day, 2 hours, 3 min, 27
sec

1,359 hosts 155,636 flows

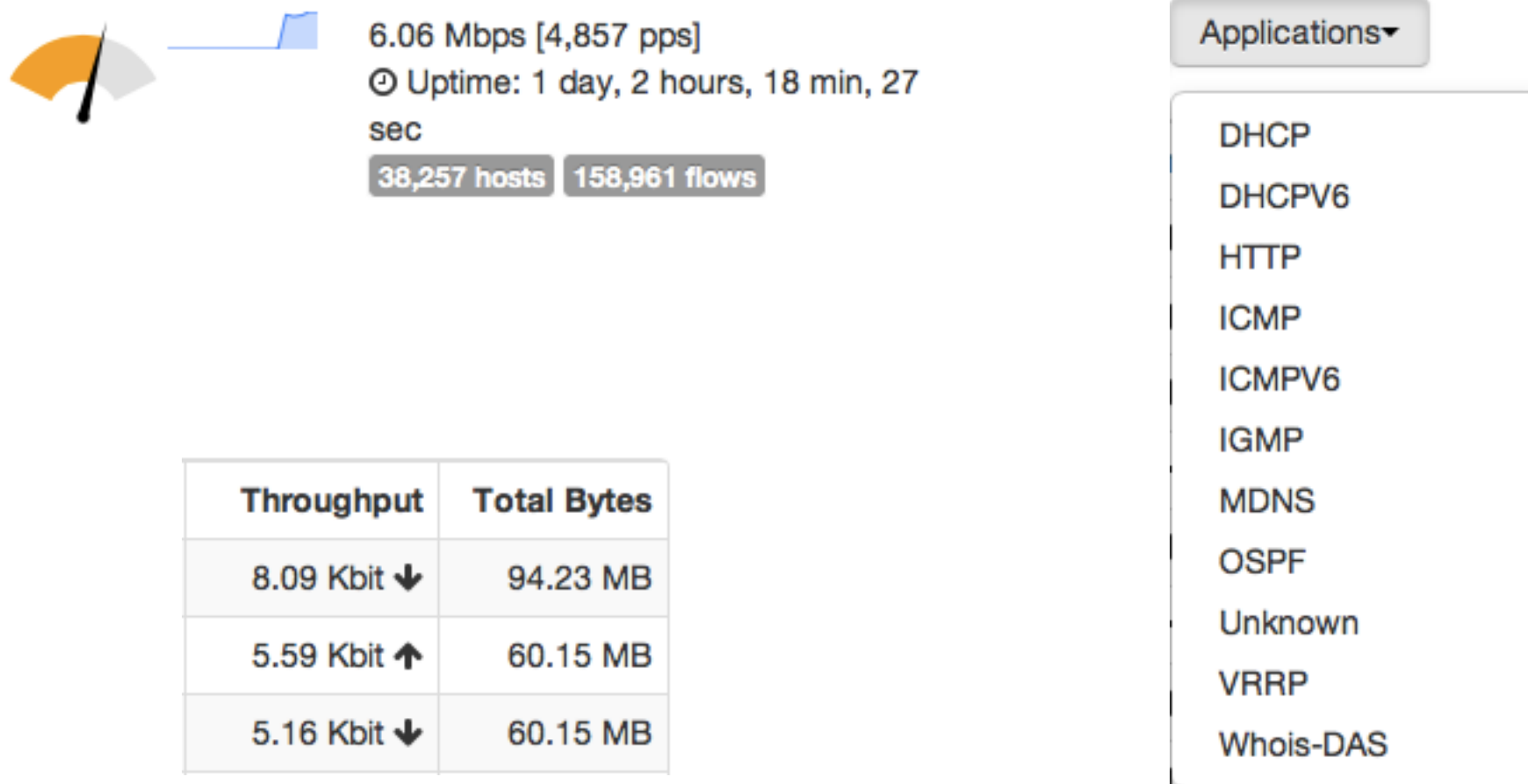


© 2016 - ntop.org

Available Menu Items



Dynamic Web Interface



Flows Monitoring [1/2]

Active Flows

⚙️ 10 ▾ ↗️ Applications ▾

Info	Application	L4 Proto	Client	Server	Duration	Breakdown	Throughput	
Info	VRRP	VRRP	fe80::192:12:192:7	ff02::12	1 day, 2 hours, 4 min, 19 sec	Client	8.09 Kbit ▾	
Info	VRRP	VRRP	192.12.192.7	224.0.0.18	1 day, 2 hours, 4 min, 19 sec	Client	5.59 Kbit ↗️	
Info	VRRP	VRRP	192.168.18.7	224.0.0.18	1 day, 2 hours, 4 min, 19 sec	Client	5.16 Kbit ▾	
Info	DHCP	UDP	0.0.0.0:68	255.255.255.255:67	1 day, 2 hours, 3 min, 57 sec	Client	0 bps ▾	
Info	OSPF	89	192.12.192.7	224.0.0.5	1 day, 2 hours, 4 min, 13 sec	Client	0 bps ▾	
Info	OSPF	89	192.168.18.7	224.0.0.5	1 day, 2 hours, 4 min, 7 sec	Client	0 bps ▾	
Info	OSPF	89	192.168.18.9	224.0.0.5	1 day, 2 hours, 4 min, 14 sec	Client	359.83 bps ↗️	
Info	OSPF	89	192.12.192.9	224.0.0.5	1 day, 2 hours, 4 min, 16 sec	Client	359.83 bps ↗️	
Info	OSPF	89	192.168.18.34	224.0.0.5	1 day, 2 hours, 4 min, 7 sec	Client	0 bps ▾	1 MB
Info	OSPF	89	192.12.192.34	224.0.0.5	1 day, 2 hours, 4 min, 7 sec	Client	0 bps —	1 MB

DHCP
 DHCPV6
 HTTP
 ICMP
 ICMPV6
 IGMP
 MDNS
 OSPF
 Unknown
 VRRP
 Whois-DAS


Showing 1 to 10 of 151325 rows

← First
Prev
1
2
3
4
5
Next
Last →

Flows Monitoring [2/2]

Flow: 192.12.192.237:53060 ⇌ whois.nic.it:5043

Overview

Client	web-r1.nic.it:53060		
Server	whois.nic.it:5043		
Application Protocol	HTTP		
First Seen	11/10/2013 13:45:26 [6 min, 54 sec ago]		
Last Seen	11/10/2013 13:52:12 [8 sec ago]		
Total Traffic Volume	7.03 KB —		
Client vs Server Traffic Breakdown	 192.12.192.237		
Client to Server Traffic	63 Pkts / 7.03 KB —		
Server to Client Traffic	0 Pkts / 0 Bytes —		
Actual Throughput	0 bps —		
TCP Flags	SYN PUSH ACK		

© 1998-2013 - [ntop.org](#)

Generated by ntopng v.1.0.1 (r6749)
for user admin and interface eth5



193.98 Kbps [260 pps]

⌚ Uptime: 1 day, 2 hours, 4 min, 49
sec

1,272 hosts 153,747 flows



© 2016 - ntop.org

Host Monitoring [1/3]

Hosts List

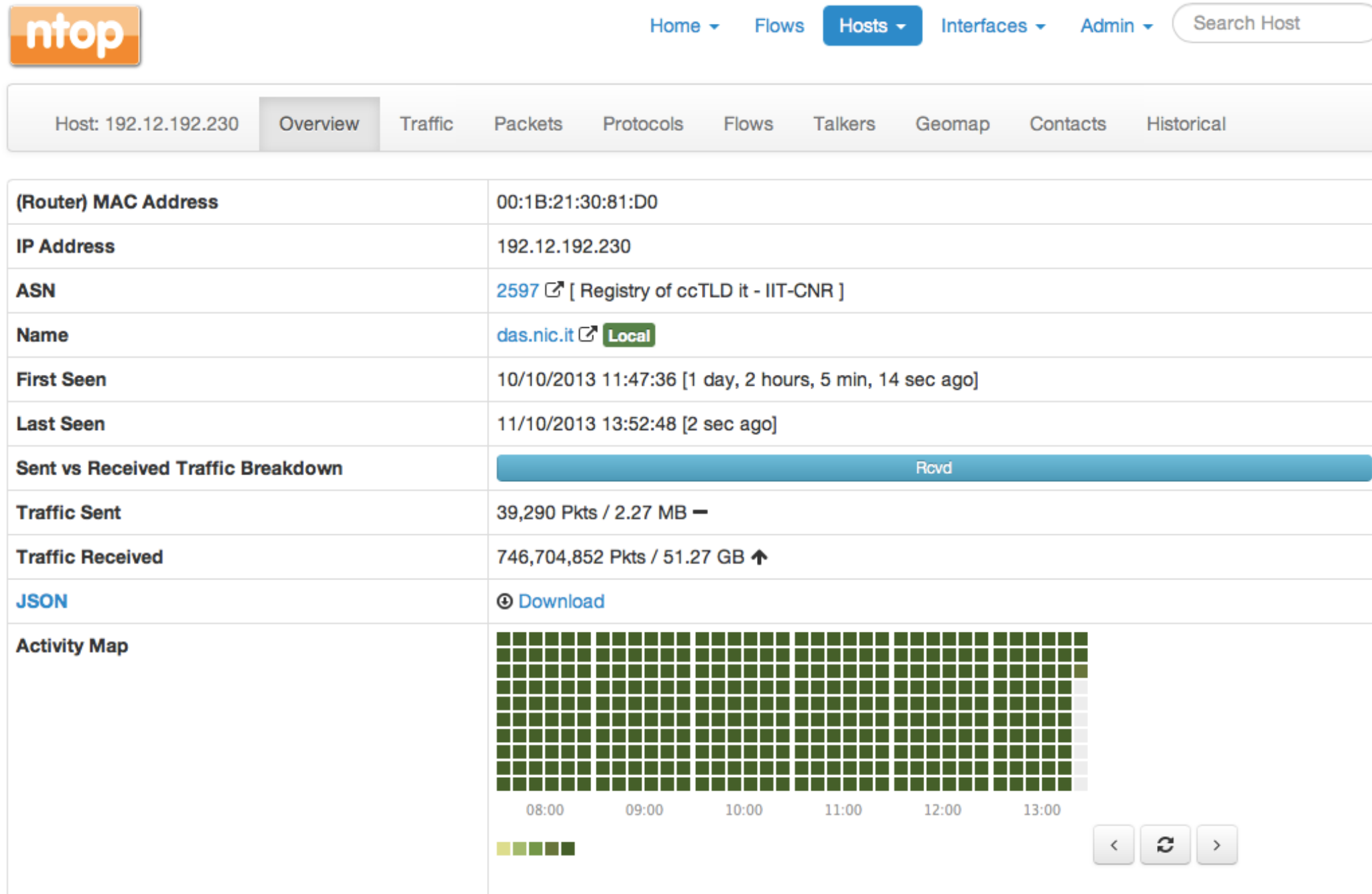
⚙️ 10 ↗️

IP Address	Location	Symbolic Name	Seen Since	ASN	Breakdown	Throughput	Traffic
192.12.192.230	Local	das.nic.it 🇮🇹	1 day, 2 hours, 4 min, 49 sec	2597 ↗️	Rcvd	13.57 Kbit	51.27 GB
192.165.67.192	Remote	192.165.67.192 🇮🇹	1 day, 2 hours, 4 min, 31 sec	34971 ↗️	Sent	0 bps	9.62 GB
192.165.67.166	Remote	192.165.67.166 🇮🇹	1 day, 2 hours, 4 min, 31 sec	34971 ↗️	Sent	659.95 bps	9.18 GB
78.46.216.98	Remote	78.46.216.98 🇩🇪	1 day, 2 hours, 4 min, 48 sec	24940 ↗️	Sent	219.98 bps	7.87 GB
192.165.67.22	Remote	192.165.67.22 🇮🇹	1 day, 2 hours, 4 min, 30 sec	34971 ↗️	Sent	0 bps	7.81 GB
78.47.50.132	Remote	78.47.50.132 🇩🇪	1 day, 2 hours, 4 min, 48 sec	24940 ↗️	Sent	879.93 bps	7.18 GB
62.149.189.11	Remote	62.149.189.11 🇮🇹	1 day, 2 hours, 4 min, 35 sec	31034 ↗️	Sent	0 bps	1.44 GB
192.12.192.242	Local	whois.nic.it 🇮🇹	1 day, 2 hours, 4 min, 49 sec	2597 ↗️	Rcvd	84.86 Kbit	964.02 MB
224.0.0.18	Remote	vrrp.mcast.net	1 day, 2 hours, 4 min, 49 sec		Rcvd	8.81 Kbit	120.35 MB
213.154.243.80	Remote	213.154.243.80 🇮🇪	18 hours, 57 min, 57 sec	12859 ↗️	Sent	4.51 Kbit	116.72 MB

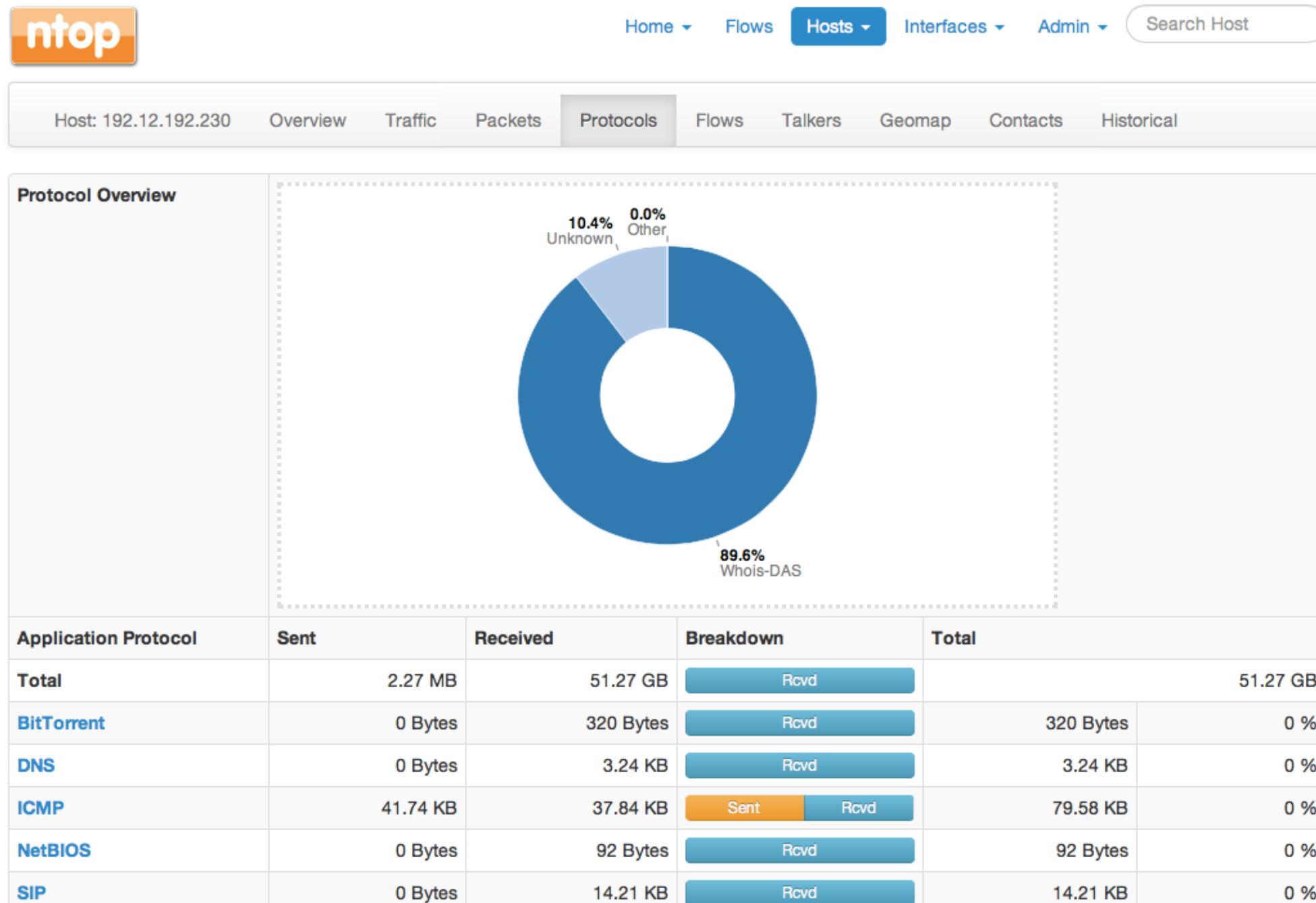
Showing 1 to 10 of 1275 rows

← First Prev 1 2 3 4 5 Next Last →

Host Monitoring [2/3]



Host Monitoring [3/3]



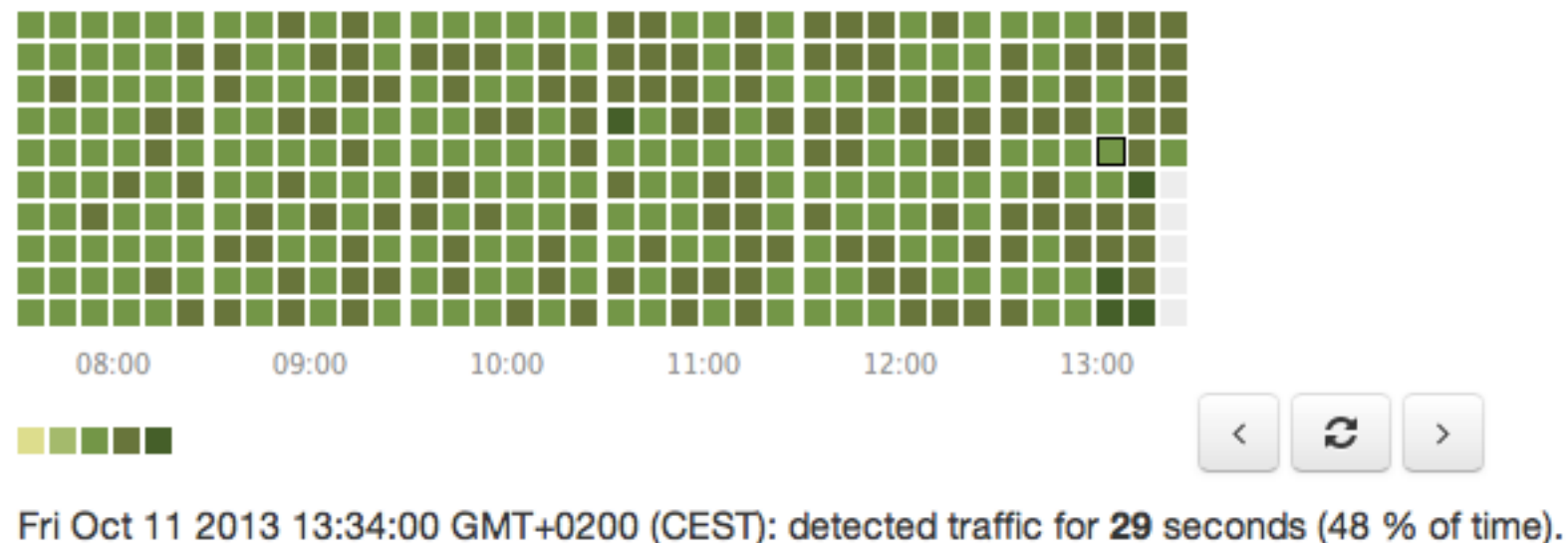
Activity Map

- 1 second resolution host and aggregation activity
- Compressed bitmap

```
> ls -l client14.dropbox.com
```

```
4 -rw-rw-rw- 1 nobody nogroup 24 Oct 11 02:31 client14.dropbox.com
```

- Saved persistently on disk (Local Hosts only)



Traffic Aggregations [1/2]

- nDPI extracts specific attributes from traffic that ntopng aggregates (if configured):
 - DNS/Whois responses
 - HTTP host names
 - Operating System (from HTTP headers)
- Aggregations can be enabled (they are off by default) and are handled just as flows and hosts.

Traffic Aggregations [2/2]

Aggregations

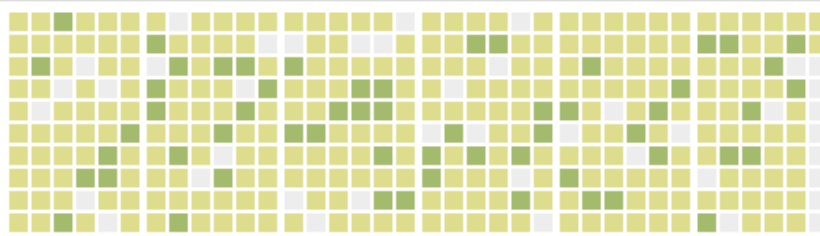
⚙️ 10 ↗️ Aggregations▼

Name	Protocol	Seen Since	Last Seen	Qu
dnsmom.nic.it	HTTP	1 day, 46 min, 20 sec	4 sec	
Linux x86_64	Operating System	1 day, 46 min, 20 sec	4 sec	
daisy.ubuntu.com	DNS	1 day, 46 min, 16 sec	28 sec	13,613 —
i7.ntop.org	HTTP	11 sec	1 sec	26 —
Intel Mac OS X 10_8_5	Operating System	11 sec	1 sec	26 —
www.google.com	DNS	1 min, 30 sec	39 sec	15 —
pnnptflomq.nic.it	DNS	39 sec	39 sec	2 —
tdkoxonu.j.nic.it	DNS	40 sec	40 sec	2 —
ilkomppxne.nic.it	DNS	39 sec	39 sec	2 —
checkip.dyndns.com	DNS	40 sec	40 sec	2 —

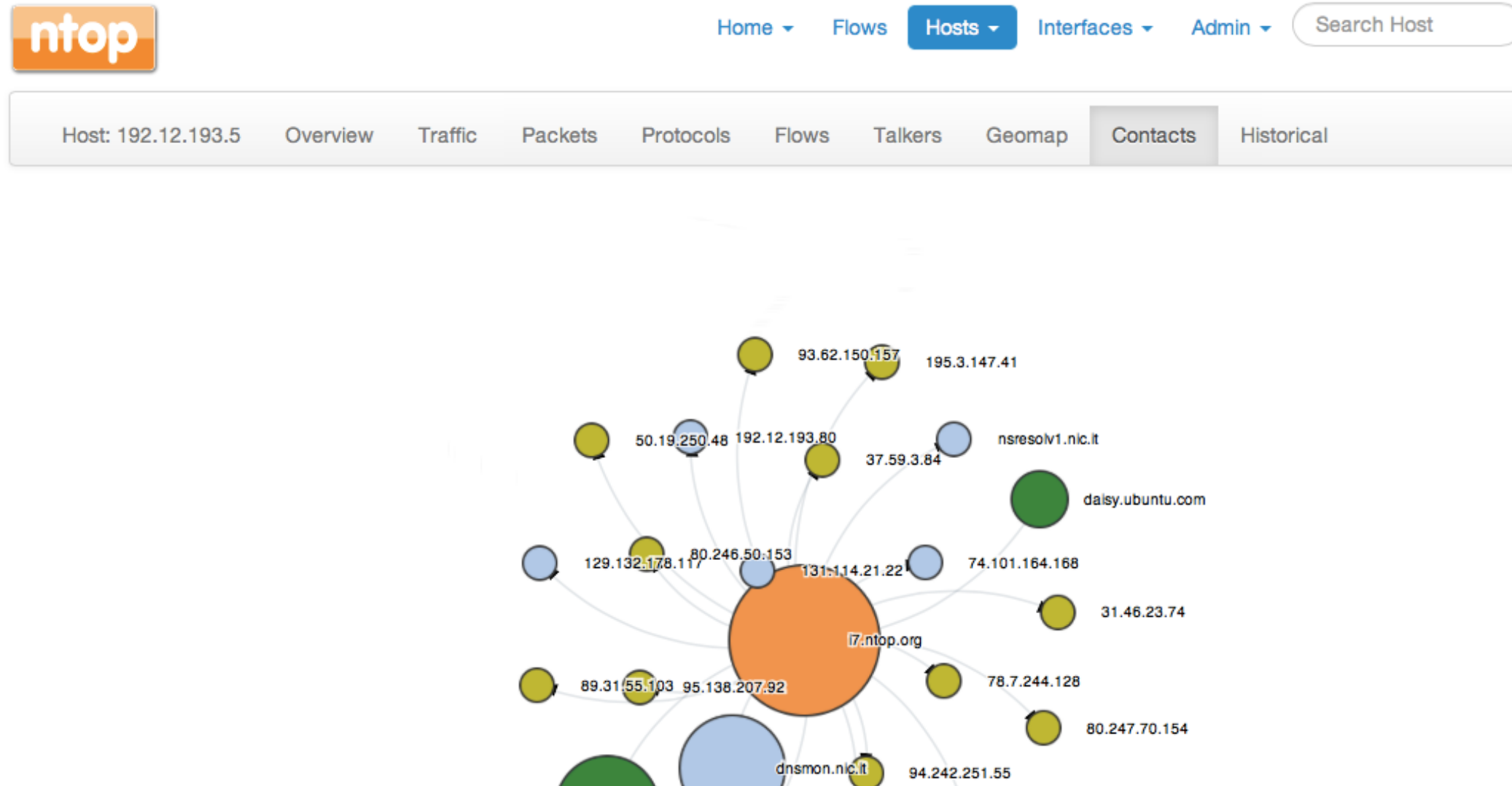
Showing 1 to 10 of 20 rows

← First Prev 1 2 Next Last →

All
DNS
Operating System
HTTP

Name	daisy.ubuntu.com ↗️
Family	DNS
First Seen	10/10/2013 15:05:05 [1 day, 46 min, 43 sec ago]
Last Seen	11/10/2013 15:51:33 [30 sec ago]
Contacts Received	13,622 —
Activity Map	 <div>10:00 11:00 12:00 13:00 14:00 15:00</div> <div>◀ ▶ ↺</div>

Hosts and Aggregations Interaction



NOTE

1. This map is centered on host **192.12.193.5**. Clicking on this host you will visualize its details.
2. Color map: **local**, **remote**, **aggregation**, **focus** host.
3. Click is enabled only for hosts that have not been purged from memory.

Geolocation

Hosts GeoMap

Host: 192.12.193.5		Overview	Traffic	Packets	Protocols	F
(Router) MAC Address		78:AC:C0:A7:0D:4C				
IP Address		192.12.193.5 [Pisa 🇮🇹]				

Maxmind GeoIP

Map Centered Using
HTML 5 Geolocation

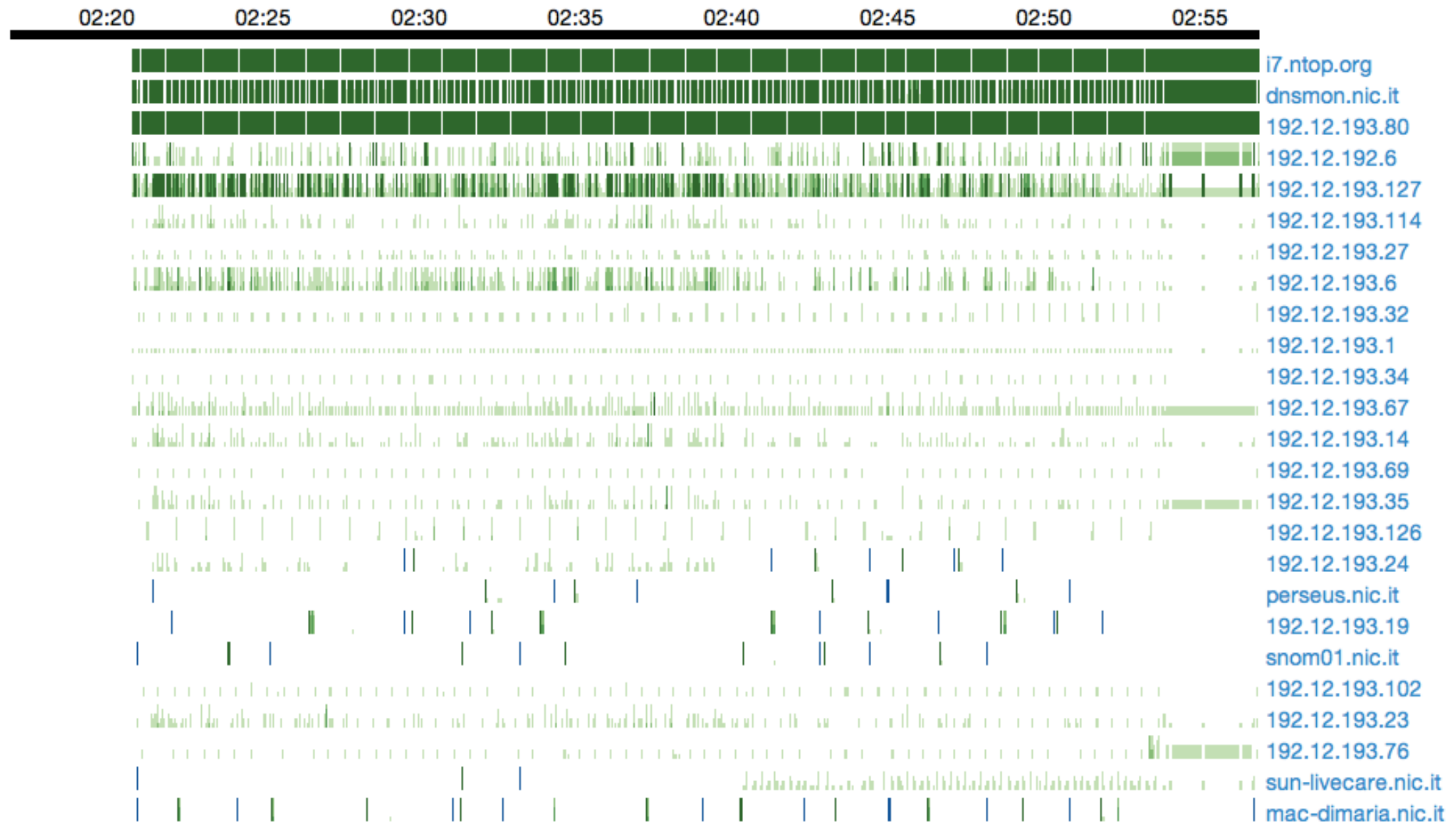


NOTE

1. 📍 Browser reported home map location [Latitude: 43.71949459086955, Longitude: 10.4219399273913]
2. In order to visualize maps you must:
 1. Have a working Internet connection.
 2. Have compiled ntopng with geolocation and started with it.
 3. Have active flows between peers with public IP addresses.
3. HTML browser geolocation is used to place on map hosts based on unknown locations.

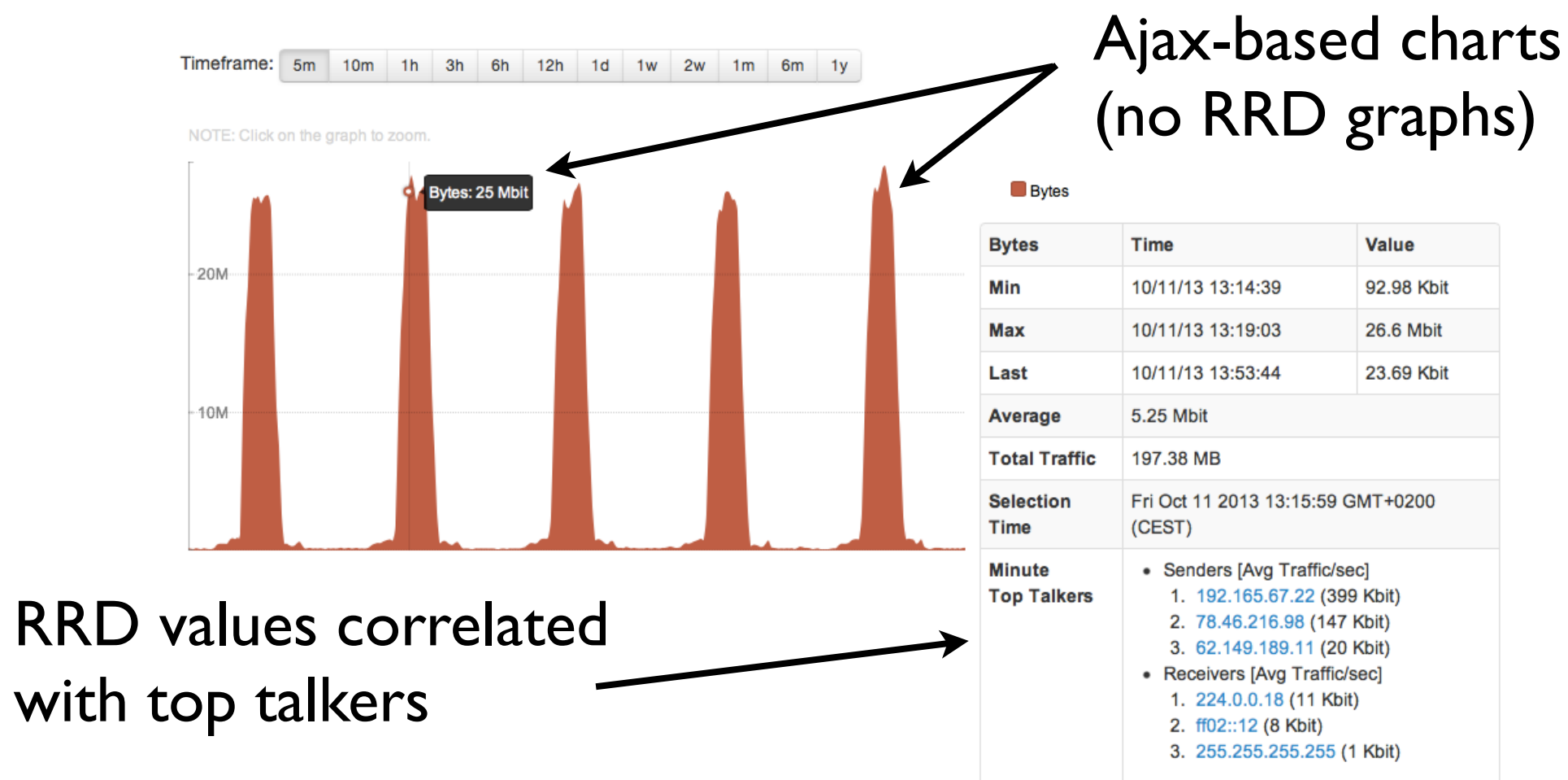
Live Host Activities

Top Hosts (Local)




Historical Activities

- All relevant counters are saved on disk in RRD.
- Interface counters are saved with 1 second resolution. Hosts counters every 5 minutes.



Using ntopng as a Live Data Source

- ntopng is a server able to serve data to third party applications via HTTP.
- Data is exported via JSON.
- This mechanism can be extended via Lua scripts.

Traffic Sent	744,856 Pkts / 97.54 MB ↑
Traffic Received	807,881 Pkts / 190.37 MB ↑
JSON	ⓓ Download
Activity Map	

Export Data

Host:

NOTE: If the field is empty all hosts will be exported

Export JSON Data

Reset Form

Using ntopng with NetFlow/sFlow

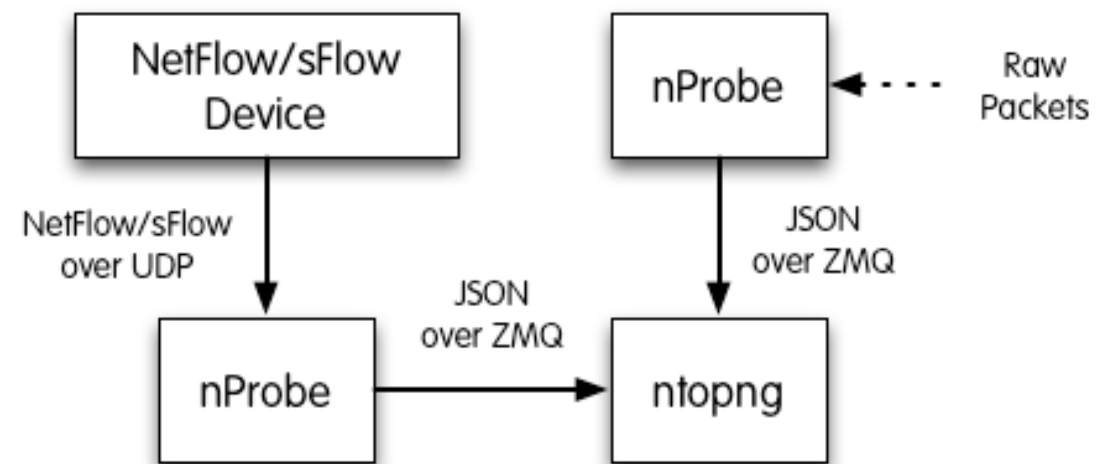
- ntopng can handle flows (Net/sFlow) via nProbe.

- **Data Collector (ntopng)**

- `ntopng -i tcp://127.0.0.1:5556`

- **Probe (nProbe)**

- `nprobe --zmq "tcp://*:5556" -i eth1 -n none` **(probe mode)**
 - `nprobe --zmq "tcp://*:5556" -i none -n none --collector-port 2055` **(sFlow/NetFlow collector mode)**



Embedding ntopng [1/2]

- Historically we have started our first embed attempt in 2003 with the Cyclades TS100.
- The nBox was used to analyse traffic then sent to ntop for representation.
- After 10 years we have tried again with ntopng.



Embedding ntopng [2/2]

- The ntopng code compiles smoothly for cheap (36 Euro) boxes such as the BeagleBone Black.
- You can now create your personal/cheap traffic analyser without having to use a PC.
- Post 1.2 release we will optimise support for these devices (cloud).



Final Remarks

- Over the past 16 years ntop created a software framework for efficiently monitoring traffic.
- “We have a story to tell you, not just hacks”.
- Commodity hardware, with adequate software, can now match the performance and flexibility that markets require. With the freedom of open source.
- ntopng is available under GNU GPLv3 from <http://www.ntop.org/>.