

# POLYGRAPH.io

Network Visibility as a Service

Josep Sanjuas, co-founder & CEO

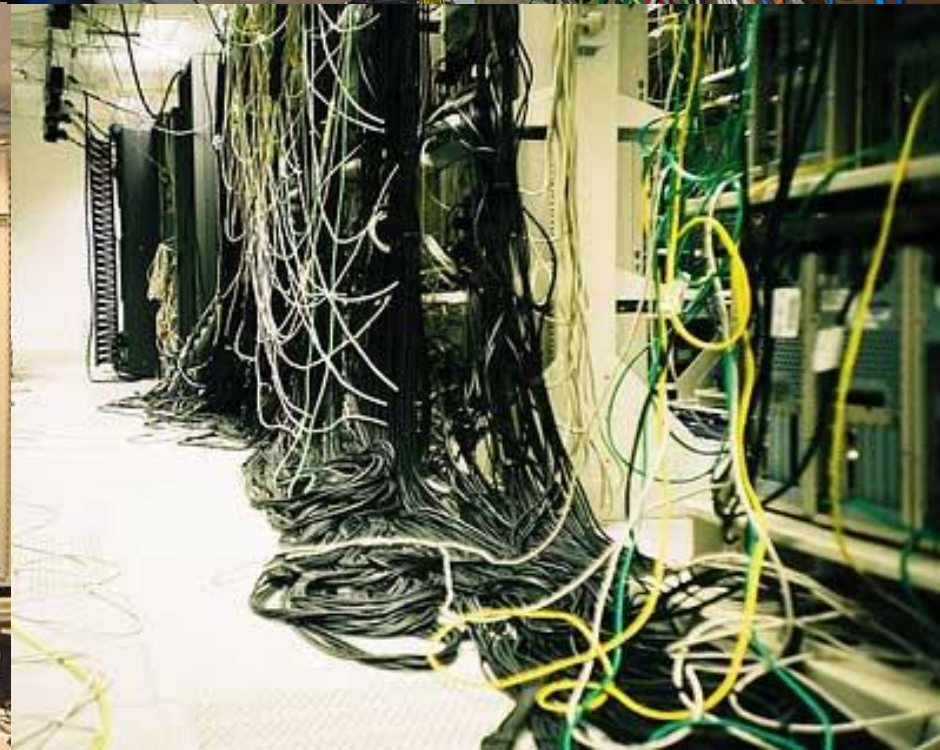
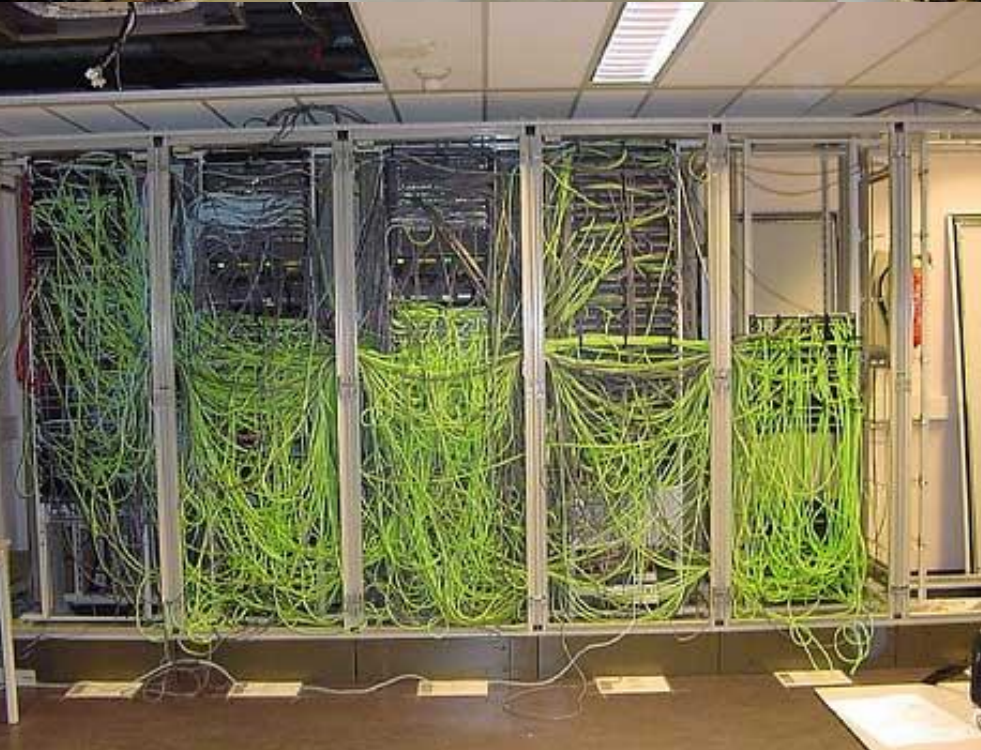
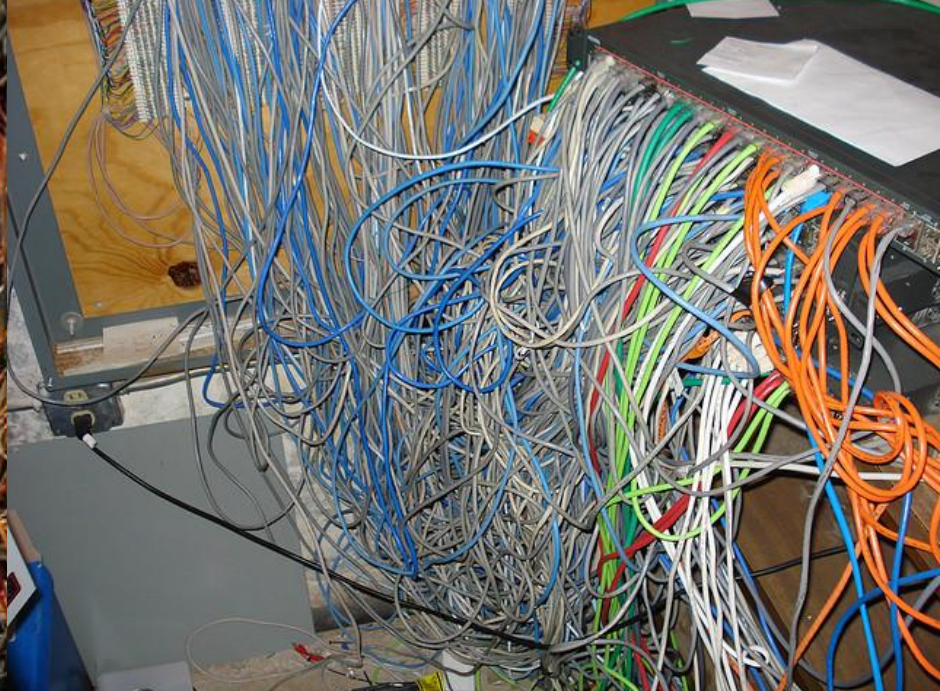
[jsanjuas@polygraph.io](mailto:jsanjuas@polygraph.io)



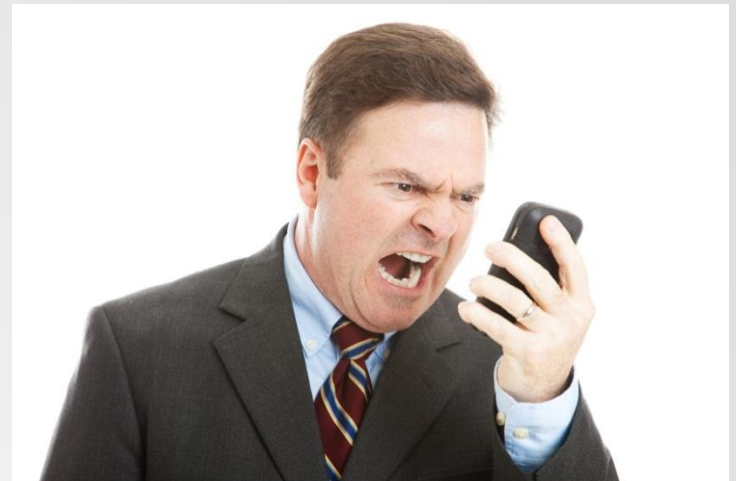
# Companies depend on Networks



e-mail, databases, shared folders, VoIP, cloud...



# Downtime



# Network Downtime equals Cost

**\$42,000/h**

avg cost of downtime

Gartner

**\$5,600/min**

avg cost of downtime  
(datacenters)

Ponemon  
INSTITUTE

“average loss per company > \$3.5M/year”

# Network Visibility

To properly manage a complex system, you need to  
**see what happens inside it**



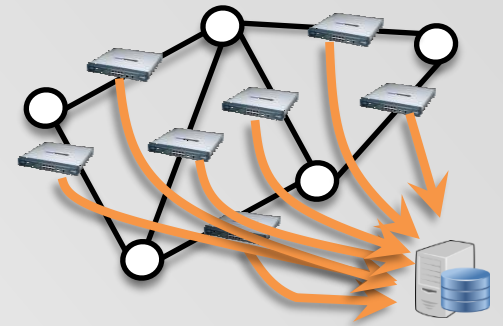
# Why Network Visibility?

- Identify congested links
- Detect unwanted applications
- Locate sources of congestion / bandwidth abuse
- Analyze performance issues
- Troubleshoot network malfunctions
- Security: detect attacks & anomalies
- Forensics: incident analysis
- Network capacity planning

# Two Families of Visibility Products

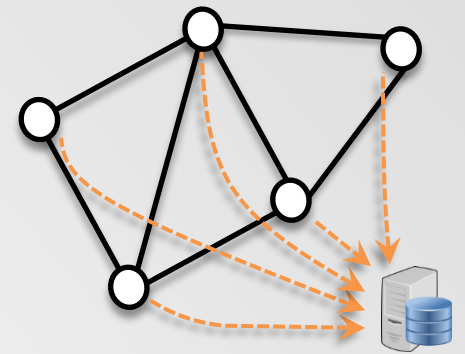
- Deep Packet Inspection

- Brute-force approach: inspect all packets
- High visibility at a **very high cost**
- Full network coverage often **cost-ineffective**



- Flow-based (NetFlow, IPFIX, sFlow..)

- Use traffic statistics exported by routers
- Lower cost but **lower visibility**



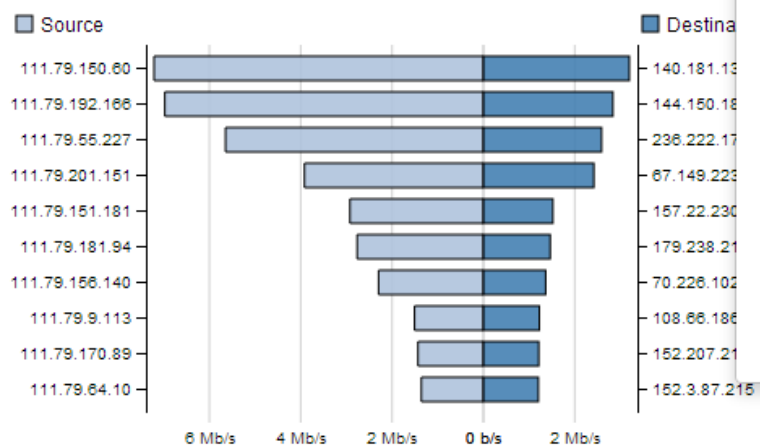


# POLYGRAPH.io - Overview

- Flow based: instant deployment (SaaS)
- Enhanced visibility: “NetFlow on steroids”
- Aims for the best user experience

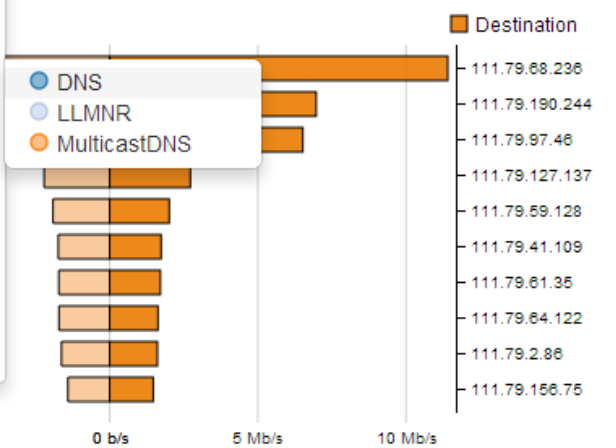
- APPLICATIONS
- PROTOCOLS
- TOP N
- AUTOZOOM
- GEOLOCATION
- ANOMALIES
- FLOWS
- REPORTS

### Top Addresses - from LAN



12-04-2014 04:20 - 12-04-2014 09:50

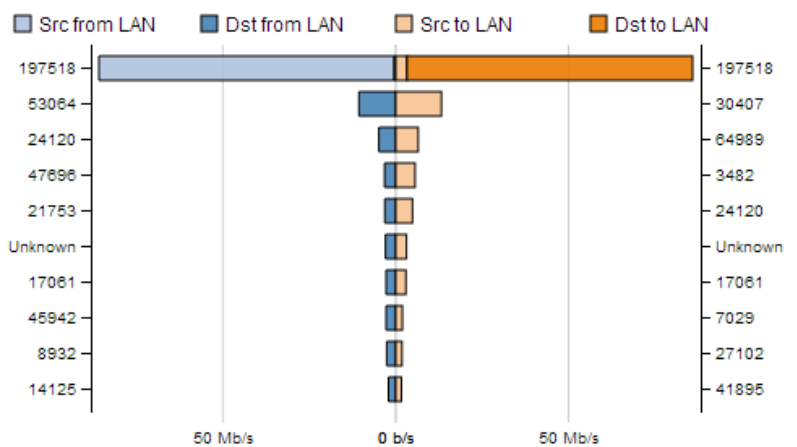
### to LAN



12-04-2014 04:20 - 12-04-2014 09:50

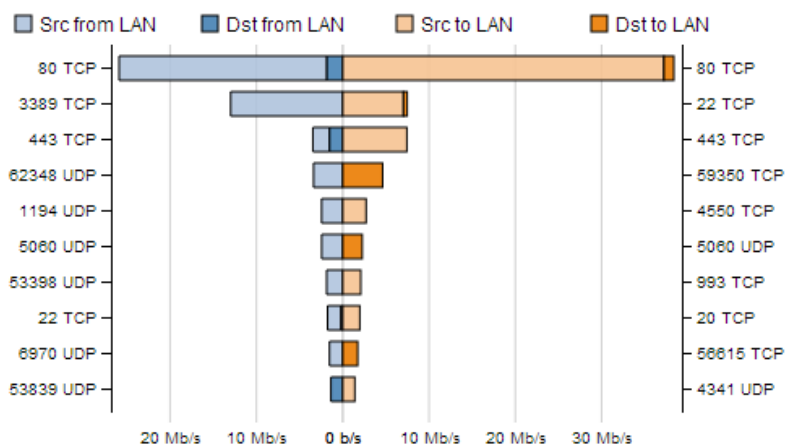
- All applications
- World wide web
- Direct Download
- Services and Others
- DNS
- Streaming and P2P TV
- File transfer
- Encrypted and Tunneling
- Games
- File Sharing P2P
- Instant Messaging
- Mail
- Voice and Video over IP

### Top Autonomous Systems



12-04-2014 04:20 - 12-04-2014 09:50

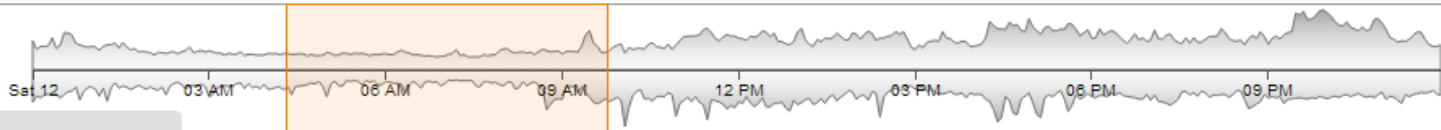
### Top Ports



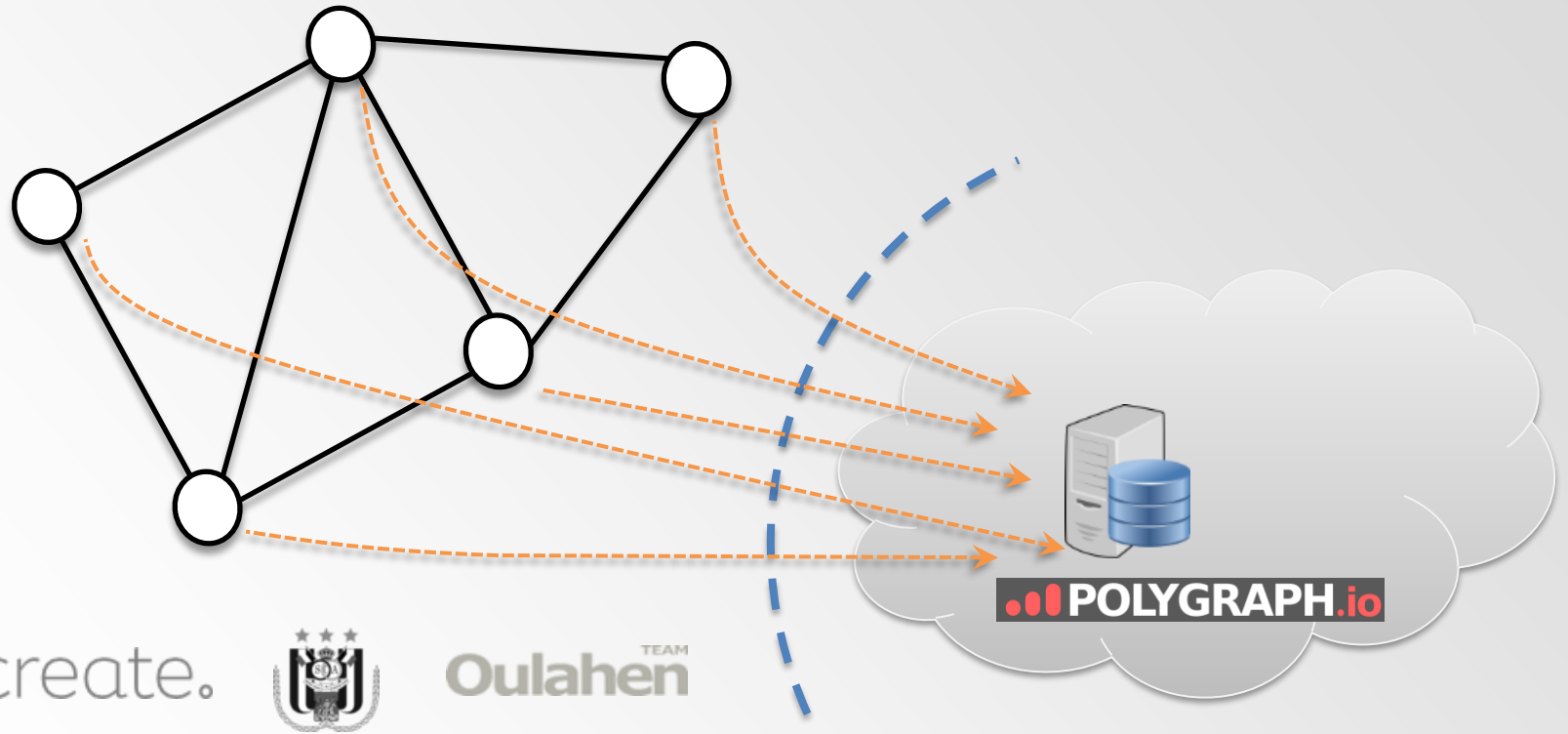
12-04-2014 04:20 - 12-04-2014 09:50

Start: 12-04-2014 04:20

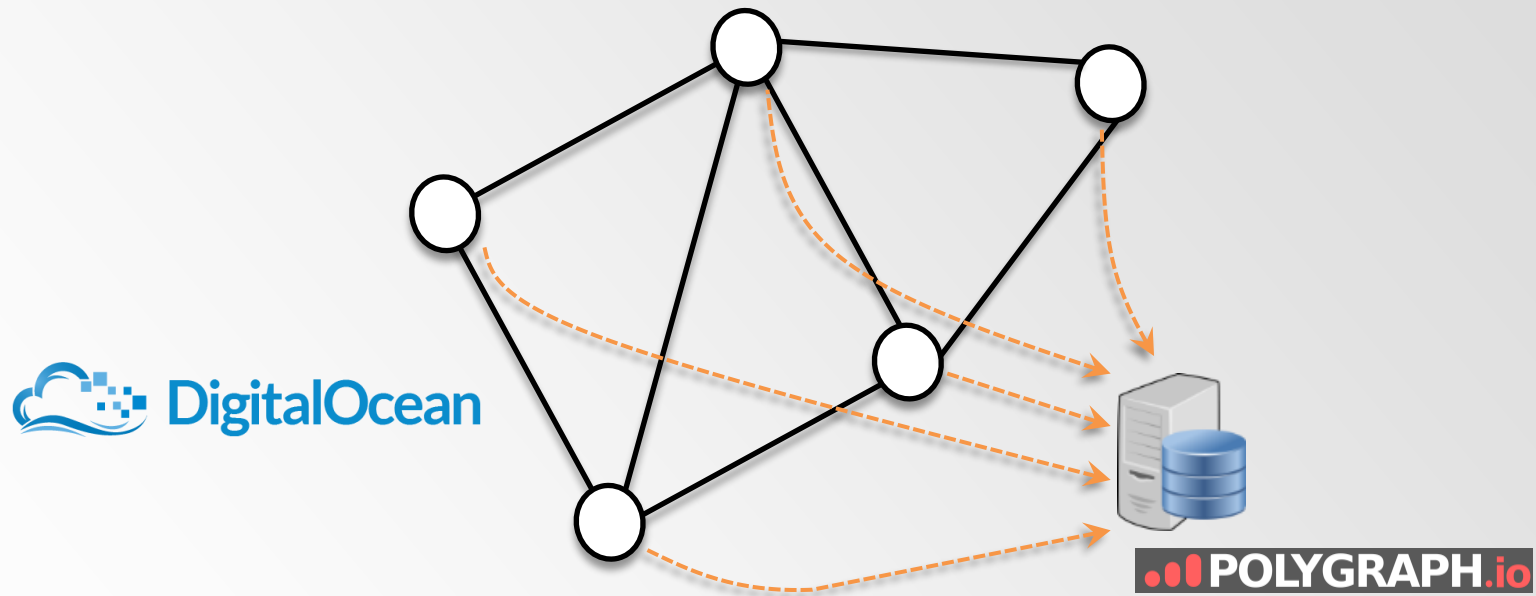
End: 12-04-2014 09:50



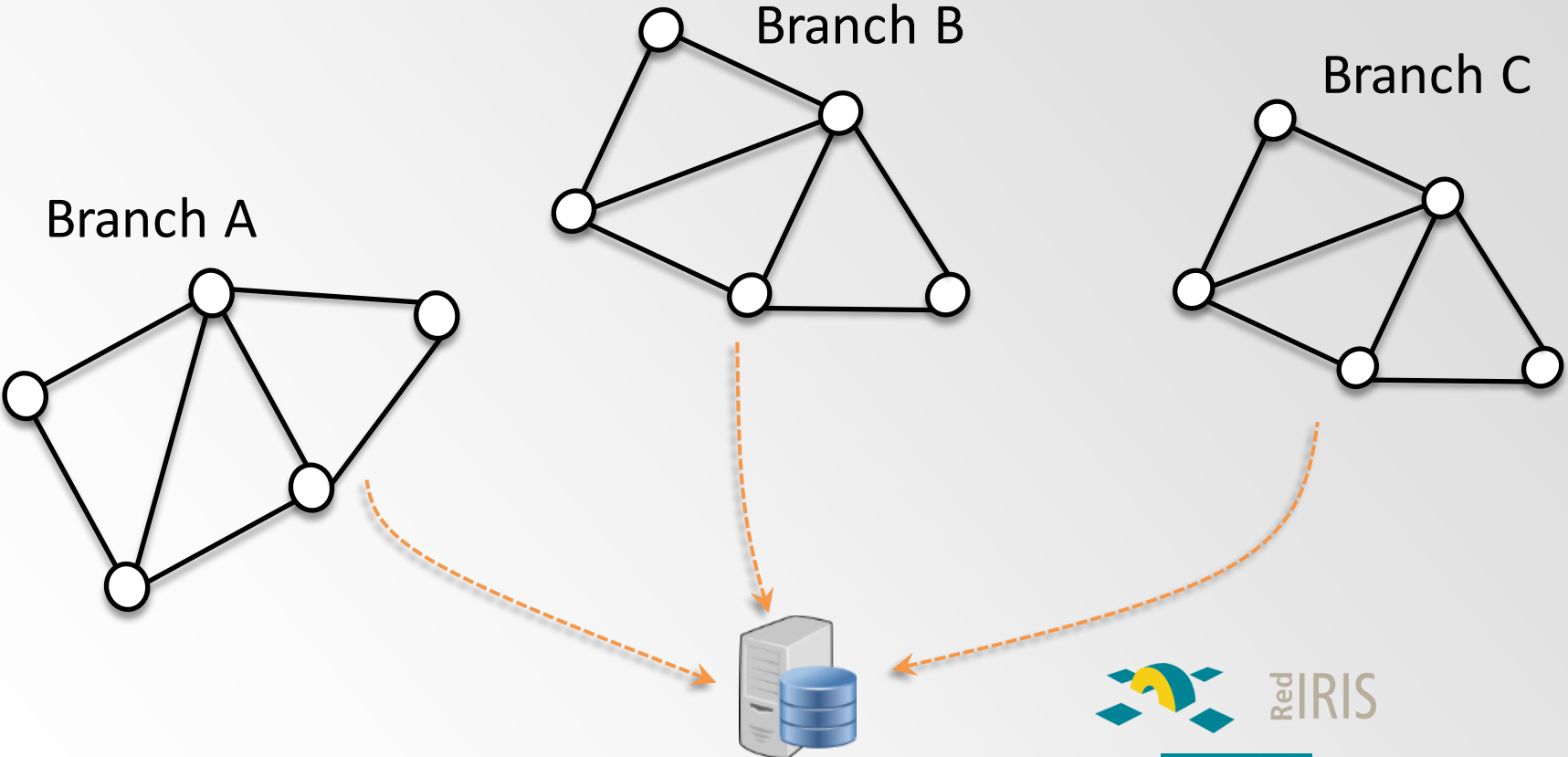
# Deployment Models: SaaS



# Deployment Models: Enterprise



# Enterprise: Multi-Tenancy



# POLYGRAPH.io - Technology

- **High visibility** at the cost of **software solutions**  
**best visibility-to-cost ratio**
- How? **NetFlow + artificial intelligence**  
**NetFlow on steroids:** application identification, SSL domain ID, attack & anomaly detection capabilities

# History

- Seed: collaboration UPC + CSUC
- Initial use case: network operation aid in a multi-tenant environment
- Draws on tech from research world
- 2 years ago: going commercial
- Spin-off of UPC-BarcelonaTech

# Application Identification

- Issue: in flow-based monitoring, it is tough to identify applications!
- Port-based identification is not accurate
  - many applications no longer use well-known ports
- Our solution: **heuristic identification via machine-learning**



# Application Identification (2)

1. Capture network traffic in high-volume links
2. Collect NetFlow
3. Combine both inputs
4. Figure out heuristics automatically:  
machine learning
5. Apply found heuristics to all customers

# Web Domain Identification

- Web domains are not included in flow-level data
  - only IP addresses, ports, protocol, bytes...
- Other products...
  - .. expect you to manually maintain mappings, e.g., 1.2.3.0/24 is Facebook
- POLYGRAPH.io:
  - does whatever it takes to figure out web services!
  - check AS numbers, DNS, even *actively connections*

# Attack Detection

- Problems of other products:
  - Attack detection often based on “patterns”
  - Often hard to tell why an alarm fired
  - Huge number of false positives
  - What flows are part of an anomaly?

# Attack Detection (2)

- Our solution:
  - Behavioral analysis + continuous learning
- Continuous learning:
  - Keep a record of what is *normal*
- Behavioral analysis:
  - Flag clusters of connections that seem related
- Combination:
  - connections from \* to 1.2.3.4:80 are normal
  - connections from \* to 4.5.6.7:80 are anomalous!

# Pre-Computing & Data Aggregation

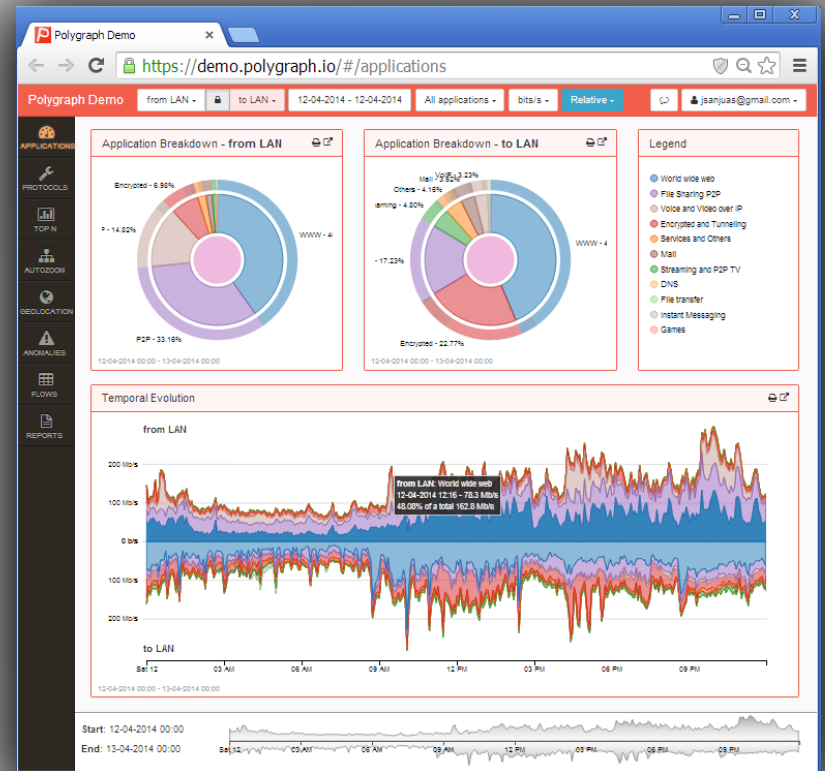
- Other products take *forever* to get results
  - e.g., “top talkers for last month”? 10 min
  - severely limits their usefulness: can’t drill down
- Our solution:
  - Pre-compute many results at various time scales
- Target outcome:
  - Be very fast for typical use cases

# Our Technology: Summary

- Identification of applications & domains
  - Heuristics figured out by machine learning
  - Automatically identify web domains
- Attack detection
  - Behavioral analysis + learning about the network
- Data pre-aggregation
  - Resolve common queries *fast*

# Website + On-Line Demo

The screenshot shows the Polygraph website homepage. The URL is <https://polygraph.io>. The navigation menu includes Product, Screenshots, Customers, Pricing, Demo, and FAQ. The main heading is "See what happens in your network." followed by "Instant deployment, no extra hardware." and "Simply export your router's stats to our cloud. All major vendors supported via NetFlow/sFlow/IPFIX/jFlow." A red button labeled "check the demo >" is prominent. Below, two steps are listed: "1. Configure your routers" with a "Click here to configure me" link and a network diagram, and "2. Enjoy network visibility" with a "Click here to find out using Polygraph." link and a laptop icon showing a warning sign.



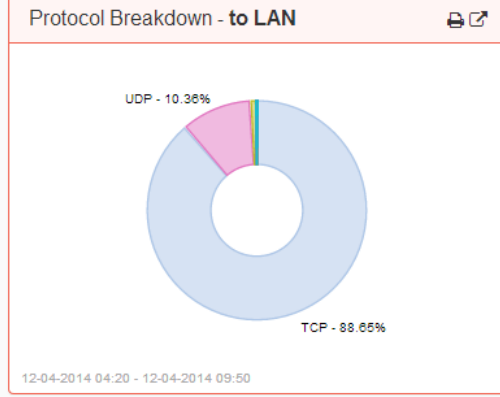
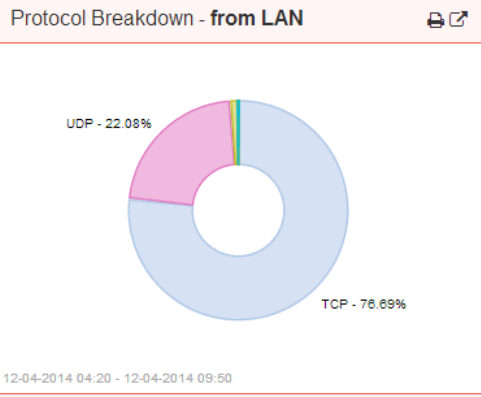
<https://polygraph.io>



traffic volume, breakdown by application



- APPLICATIONS
- PROTOCOLS
- TOP N
- AUTOZOOM
- GEOLOCATION
- ANOMALIES
- FLAWS
- REPORTS



- ### Legend
- TCP
  - UDP
  - ICMP
  - IPSEC-ESP
  - IPv6
  - GRE
  - AX.25
  - PIM



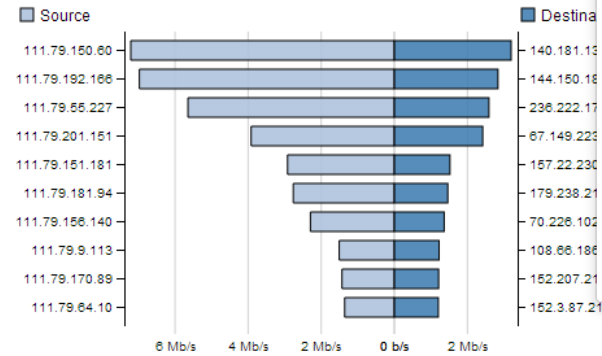
Start: 12-04-2014 04:20  
End: 12-04-2014 09:50



protocol breakdown

- APPLICATIONS
- PROTOCOLS
- TOP N
- AUTOZOOM
- GEOLOCATION
- ANOMALIES
- FLOWS
- REPORTS

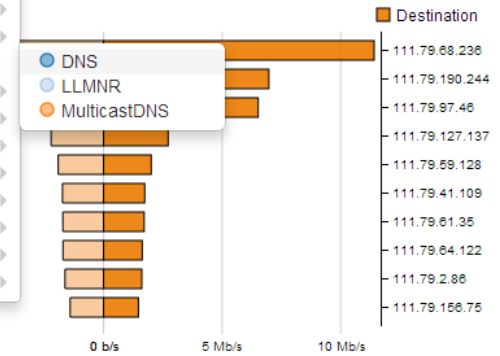
### Top Addresses - from LAN



12-04-2014 04:20 - 12-04-2014 09:50

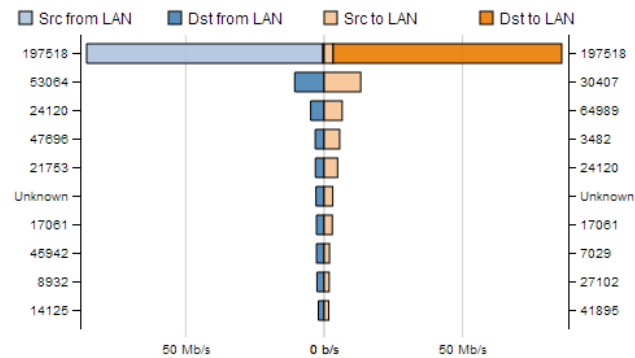
- All applications
- World wide web
- Direct Download
- Services and Others
- DNS
- Streaming and P2P TV
- File transfer
- Encrypted and Tunneling
- Games
- File Sharing P2P
- Instant Messaging
- Mail
- Voice and Video over IP

### to LAN



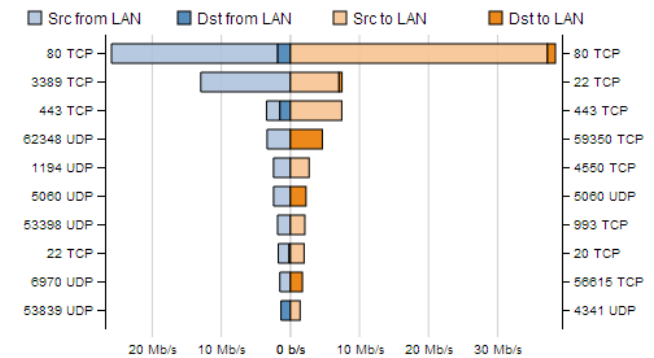
12-04-2014 04:20 - 12-04-2014 09:50

### Top Autonomous Systems



12-04-2014 04:20 - 12-04-2014 09:50

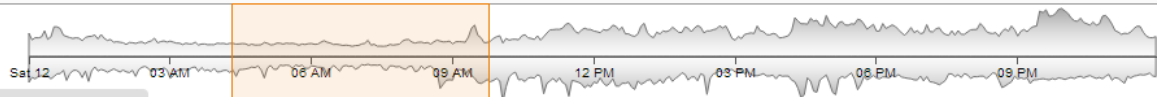
### Top Ports



12-04-2014 04:20 - 12-04-2014 09:50

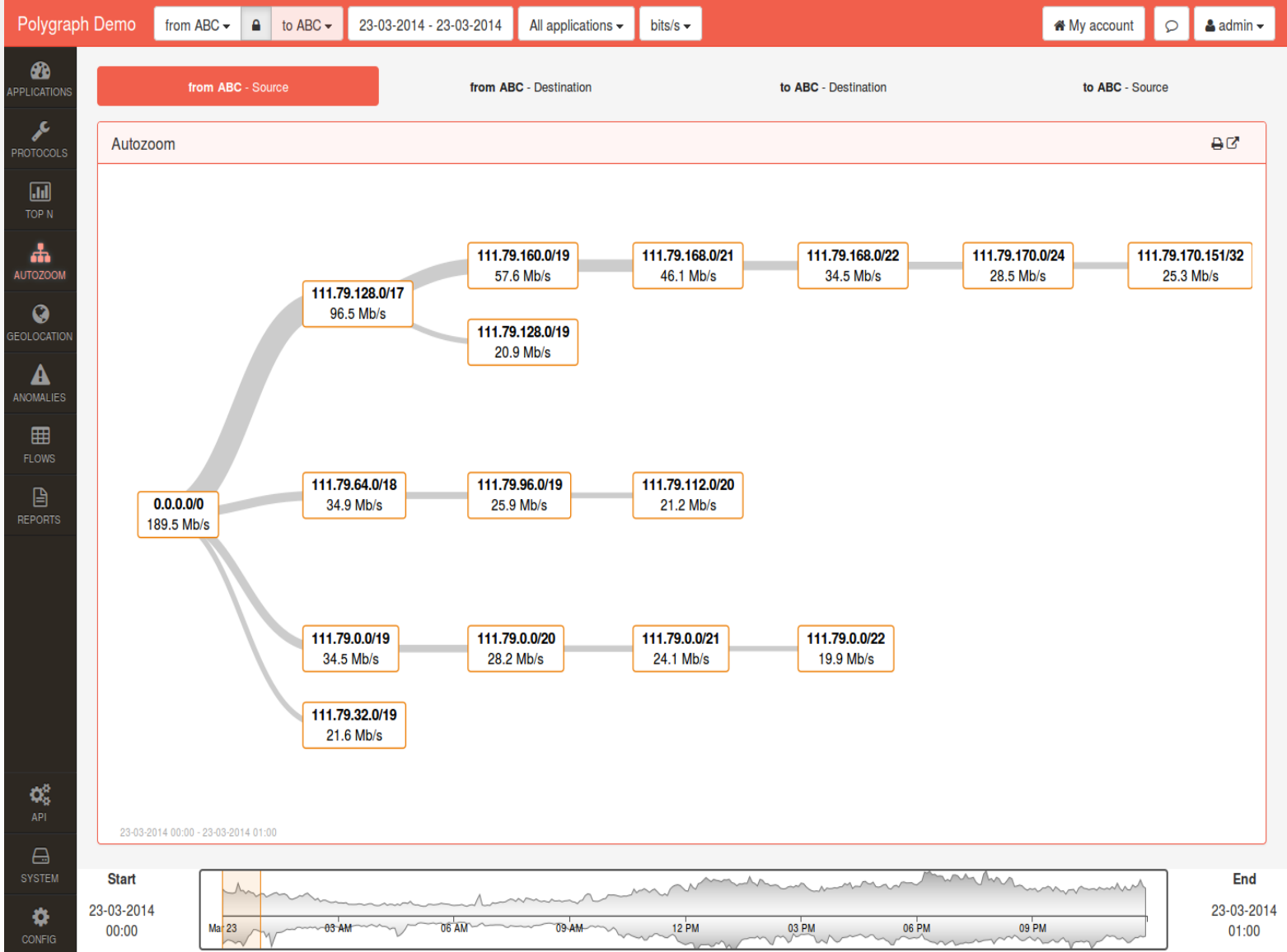
Start: 12-04-2014 04:20

End: 12-04-2014 09:50

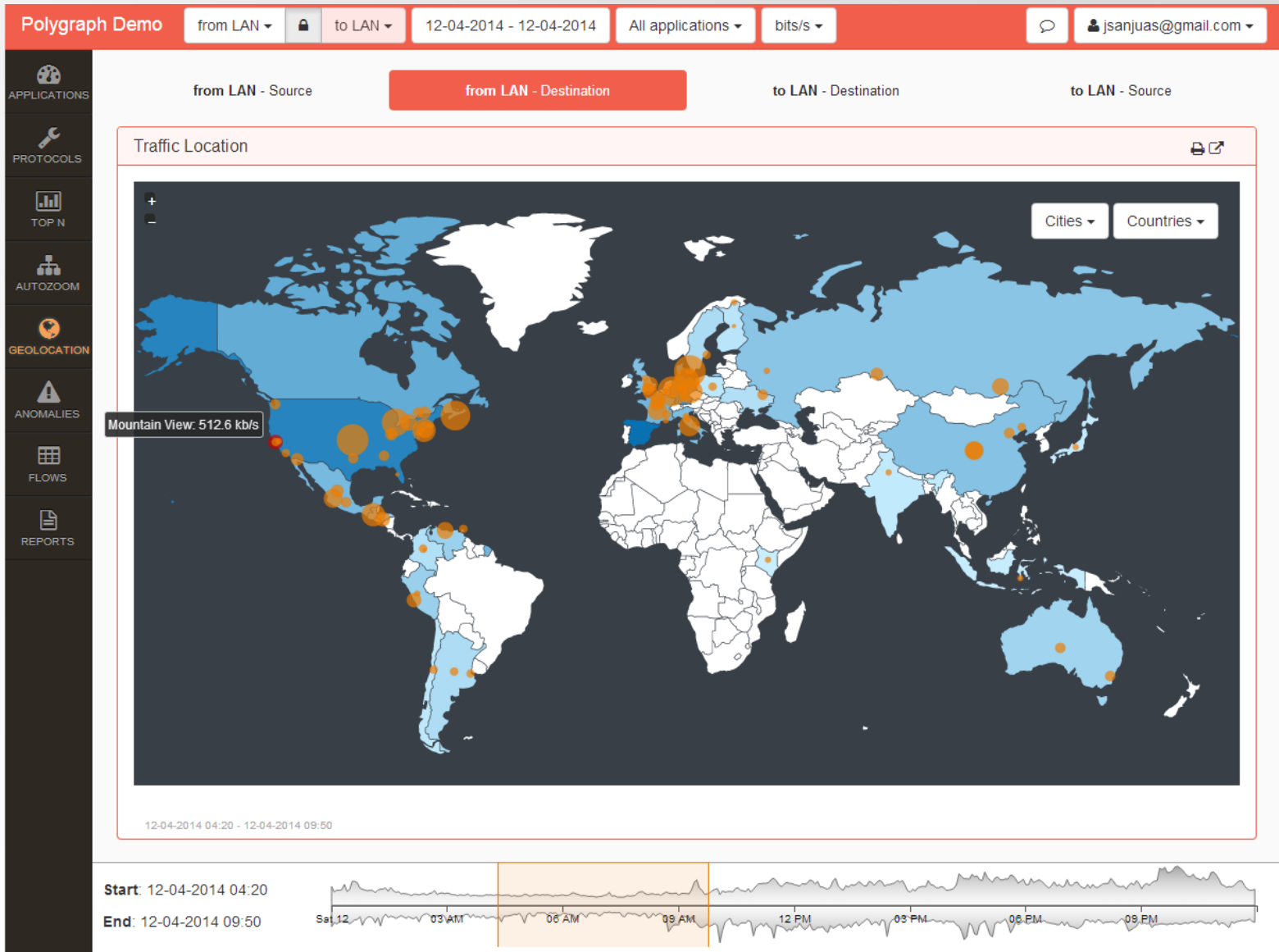


https://demo.polygraph.io/#

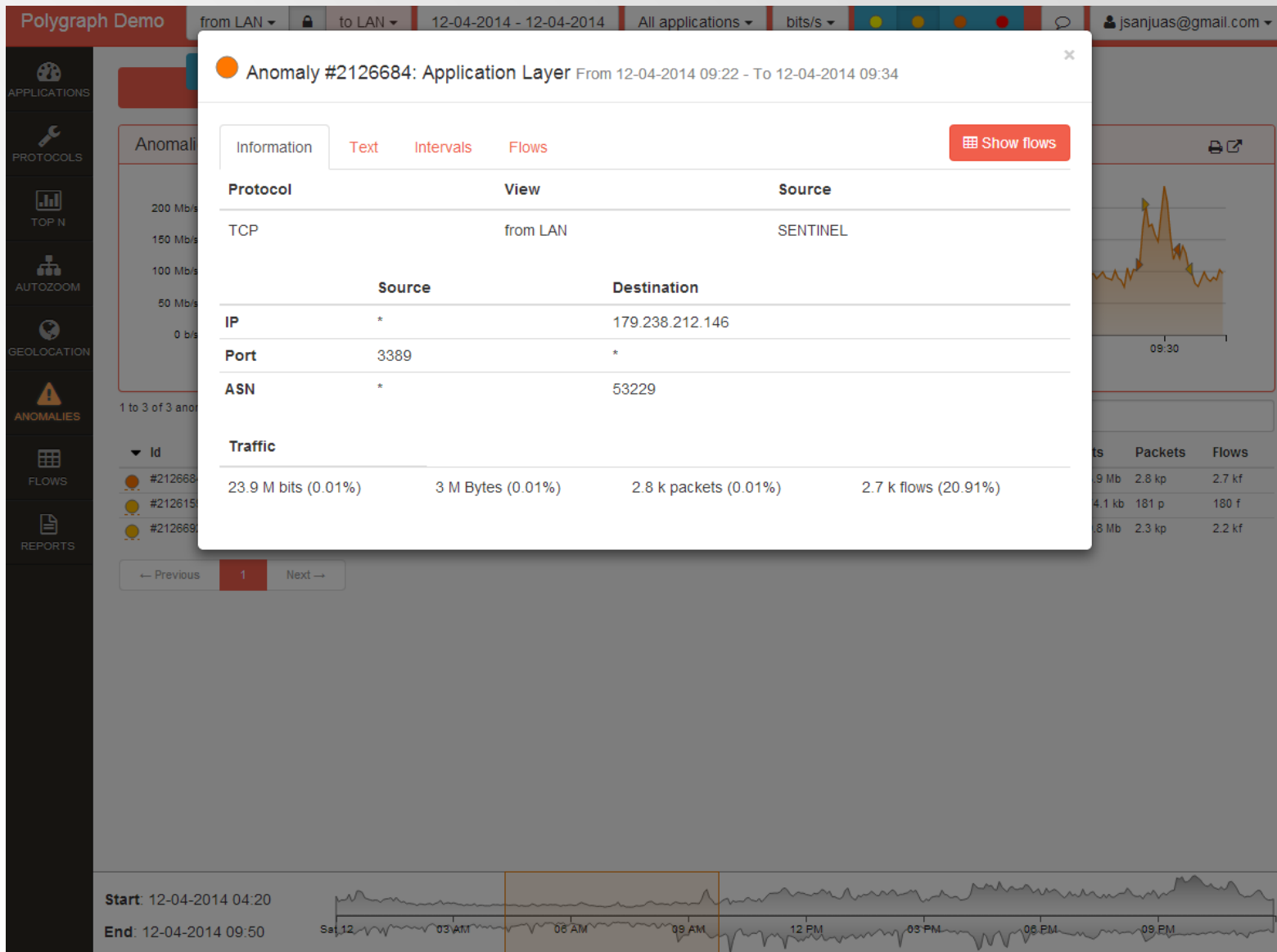
# top talkers (addresses, ports, autonomous systems)



subnetwork-level bandwidth hogs



traffic geolocation (origins & destinations)



anomaly and attack detection with automatic baselining

- APPLICATIONS
- PROTOCOLS
- TOP N
- AUTOZOOM
- GEOLOCATION
- ANOMALIES
- FLows**
- REPORTS

Search flows:

Retrieved 444 flows from 666,510 in 1.294 seconds

Showing 1 to 17 of 444 flows

Start	End	Src Addr	S. Port	Dst Addr	D. Port	Protocol	Src ASN	Dst ASN	App	Exporter
2014-04-12 04:19:36.315	2014-04-12 04:20:12.315	111.79.61.35	4499	0.193.154.164	22	TCP	197518	197169	Skype	84.8.215.18
2014-04-12 04:19:41.332	2014-04-12 04:20:31.757	111.79.61.35	3890	3.118.191.170	5900	TCP	197518	27102	BitTorrent	84.8.215.18
2014-04-12 04:21:37.207	2014-04-12 04:22:25.008	111.79.61.35	3890	3.118.191.170	5900	TCP	197518	27102	BitTorrent	84.8.215.18
2014-04-12 04:21:59.569	2014-04-12 04:22:56.089	111.79.61.35	4501	0.193.154.164	22	TCP	197518	197169	Skype	84.8.215.18
2014-04-12 04:22:41.936	2014-04-12 04:22:41.936	111.79.61.35	3890	3.118.191.170	5900	TCP	197518	27102	BitTorrent	84.8.215.18
2014-04-12 04:24:08.697	2014-04-12 04:24:08.697	111.79.61.35	4503	0.193.154.164	22	TCP	197518	197169	Skype	84.8.215.18
2014-04-12 04:24:32.957	2014-04-12 04:25:32.194	111.79.61.35	3890	3.118.191.170	5900	TCP	197518	27102	BitTorrent	84.8.215.18
2014-04-12 04:25:44.648	2014-04-12 04:26:49.184	111.79.61.35	3890	3.118.191.170	5900	TCP	197518	27102	BitTorrent	84.8.215.18
2014-04-12 04:26:59.394	2014-04-12 04:28:09.351	111.79.61.35	3890	3.118.191.170	5900	TCP	197518	27102	BitTorrent	84.8.215.18
2014-04-12 04:26:59.667	2014-04-12 04:27:27.135	111.79.61.35	4507	0.193.154.164	22	TCP	197518	197169	Skype	84.8.215.18
2014-04-12 04:28:14.392	2014-04-12 04:29:06.651	111.79.61.35	3890	3.118.191.170	5900	TCP	197518	27102	BitTorrent	84.8.215.18
2014-04-12 04:28:54.408	2014-04-12 04:29:31.625	111.79.61.35	4509	0.193.154.164	22	TCP	197518	197169	Skype	84.8.215.18
2014-04-12 04:29:28.144	2014-04-12 04:30:01.779	111.79.61.35	3890	3.118.191.170	5900	TCP	197518	27102	BitTorrent	84.8.215.18
2014-04-12 04:31:04.917	2014-04-12 04:31:57.897	111.79.61.35	3890	3.118.191.170	5900	TCP	197518	27102	BitTorrent	84.8.215.18
2014-04-12 04:31:13.986	2014-04-12 04:31:51.224	111.79.61.35	4515	0.193.154.164	22	TCP	197518	197169	Skype	84.8.215.18
2014-04-12 04:32:23.424	2014-04-12 04:32:23.424	111.79.61.35	3890	3.118.191.170	5900	TCP	197518	27102	BitTorrent	84.8.215.18
2014-04-12 04:33:40.016	2014-04-12 04:34:31.256	111.79.61.35	4529	0.193.154.164	22	TCP	197518	197169	Skype	84.8.215.18

from LAN  
 to LAN (swapped src-dst)  
 to LAN

Src:  : Port

Dst:  : Port

Protocol:

ASN:  >

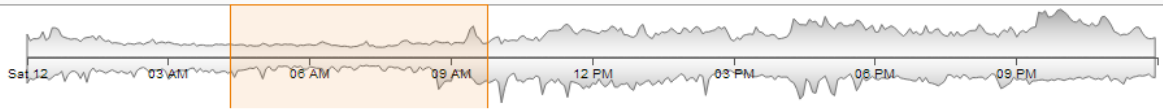
Exporter:

Bytes:  -

Packets:  -

← Previous **1** 2 3 4 5 6 7 8 9 10 11 Next →

Start: 12-04-2014 04:20  
 End: 12-04-2014 09:50



indexed traffic database for forensic analysis

Polygraph Demo from LAN to LAN 12-04-2014 - 12-04-2014 All applications bits/s jsanjuas@gmail.com

Periodic reports configuration

No periodic report configurations

Name	Periodicity	Next report	Users
No data available in table			

← Previous Next →

Reports

1 to 3 of 3 reports

Name	Download
Full daily report	Download (93.0 KB)
Weekly Top addresses report 1	Download (43.8 KB)
Weekly Top addresses report 2	Download (43.7 KB)

← Previous 1 Next →

New report

Full daily report.pdf

file:///C:/Downloads/Full%20daily%20report.pdf

Full daily report 2014-04-01 - 2014-0

### Application Breakdown

#### Application groups from ABC

#	Application group	Volume	Percent	Prev. #	Prev. vol.	Prev.
1 ▲	P2P	105.1 Mb/s +25.3 Mb/s	39.3%	+5.1%	2	79.8 Mb/s 34.2
2 ▼	WWW	90.6 Mb/s +5.0 Mb/s	33.9%	-2.8%	1	85.6 Mb/s 36.6
3 =	Encrypted	39.5 Mb/s -221.1 kb/s	14.8%	-2.2%	3	39.7 Mb/s 17.0
4 =	VoIP	17.5 Mb/s +2.2 Mb/s	6.5%	-0.0%	4	15.3 Mb/s 6.5%
5 ▲	Mail	5.4 Mb/s +1.2 Mb/s	2.0%	+0.2%	6	4.2 Mb/s 1.8%
6 ▼	Streaming	4.6 Mb/s -96.1 kb/s	1.7%	-0.3%	5	4.7 Mb/s 2.0%
7 =	Others	3.1 Mb/s +434.3 kb/s	1.2%	+0.0%	7	2.7 Mb/s 1.1%
8 =	File transfer	1.4 Mb/s +60.8 kb/s	0.5%	-0.1%	8	1.4 Mb/s 0.6%
9 =	DNS	261.6 kb/s +40.6 kb/s	0.1%	+0.0%	9	221.0 kb/s 0.1%
10 =	Instant Messaging	150.0 kb/s -8.7 kb/s	0.1%	-0.0%	10	158.6 kb/s 0.1%
11 =	Games	342.1 b/s -644.0 b/s	0.0%	-0.0%	11	986.1 b/s 0.0%

Start: 12-04-2014 04:20 End: 12-04-2014 09:50

https://demo.polygraph.io/reports/report/71/download

automated downloadable reports

<https://polygraph.io>

Talaia Networks, S.L.  
K2M – Parc UPC Campus Nord  
C/Jordi Girona, 1-3  
Barcelona (08034) Spain

 **POLYGRAPH.io**