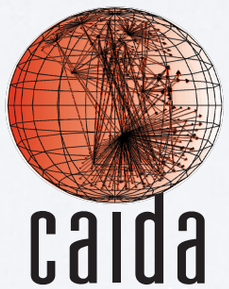
48hrs after the 1st BGP Hackathon

Alberto Dainotti
alberto@caida.org



Center for Applied Internet Data Analysis
University of California, San Diego

BGP HACKATHON 2016

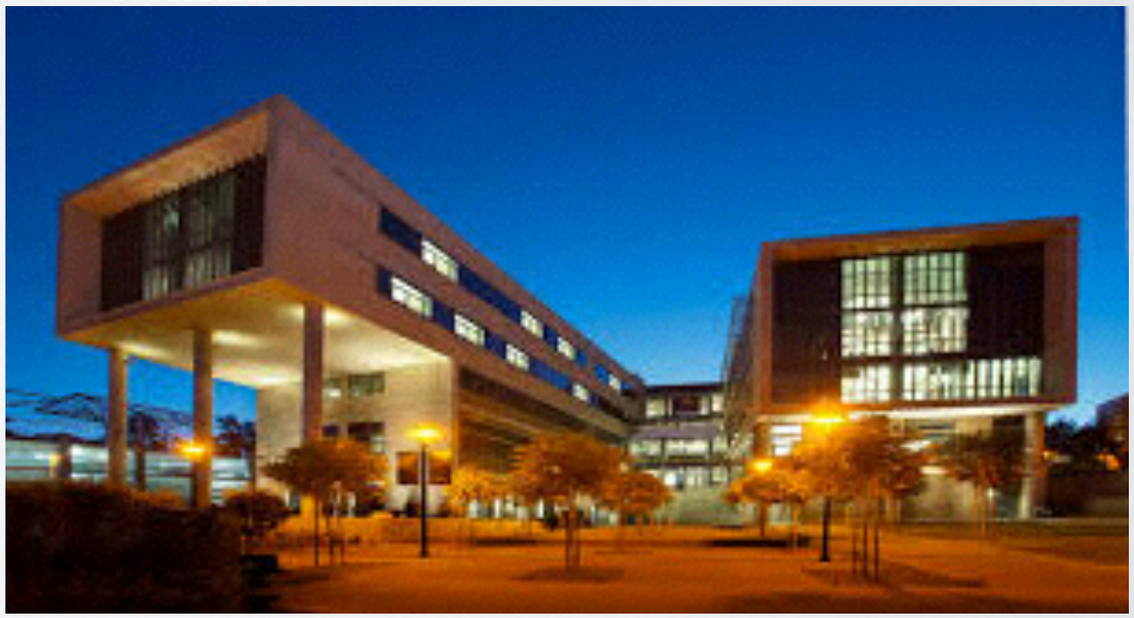
https://www.caida.org/workshops/bgp-hackathon/1602/

- **6-7 February 2016** (weekend before NANOG 66)
- San Diego Supercomputer Center, **UC San Diego**
- **Theme**: ***live BGP measurements and monitoring***
- 90 Attendees

- 50 competing participants
  - 30 graduate students
- 25 non-competing experts
- Mix of Academia, Industry, Institutions
- 15 teams!

caida

SDSC SAN DIEGO SUPERCOMPUTER CENTER



ORGANIZERS & PLATFORMS

github.com/CAIDA/bgp-hackathon/wiki/Platforms-Documentation

- Stable and experimental **data sources**
  - MRT files from *RIPE RIS*, *Route Views*
    - Also streamed through *BGPStream*
  - Cassandra Cluster - *BGPMON*
  - Kafka live feeds
    - json from new experimental *RIPE RIS*
    - BMP from *Route Views, Cisco, Randy Bush*
- **Testbed** emulating ASes on the actual Internet - *PEERING*
- **Software framework** for BGP monitoring and data analysis - *BGPStream*
- Unified Interface to **Looking Glasses** - *PERISCOPE*
- **Active Probing** infrastructure
  - *RIPE Atlas, CAIDA Ark*
- *Comet* **Supercomputer**
  - 1944 compute nodes. Each: 24 CPUs,128GB RAM

USC University of Southern California

FORTH Foundation for Research & Technology, Hellas

UC San Diego

BGPmon

UFMG Universidade Federal de Minas Gerais

Route Views 6447

caida

RIPE NCC

SDSC San Diego Supercomputer Center

SPONSORS

THANK YOU!

acm sigcomm

CISCO

COMCAST

Google

Internet Society

SDSC SAN DIEGO SUPERCOMPUTER CENTER

MANDATORY PIC OF FOLKS WITH LAPTOPS LOCKED IN A ROOM

MEASUREMENT/MONITORING…

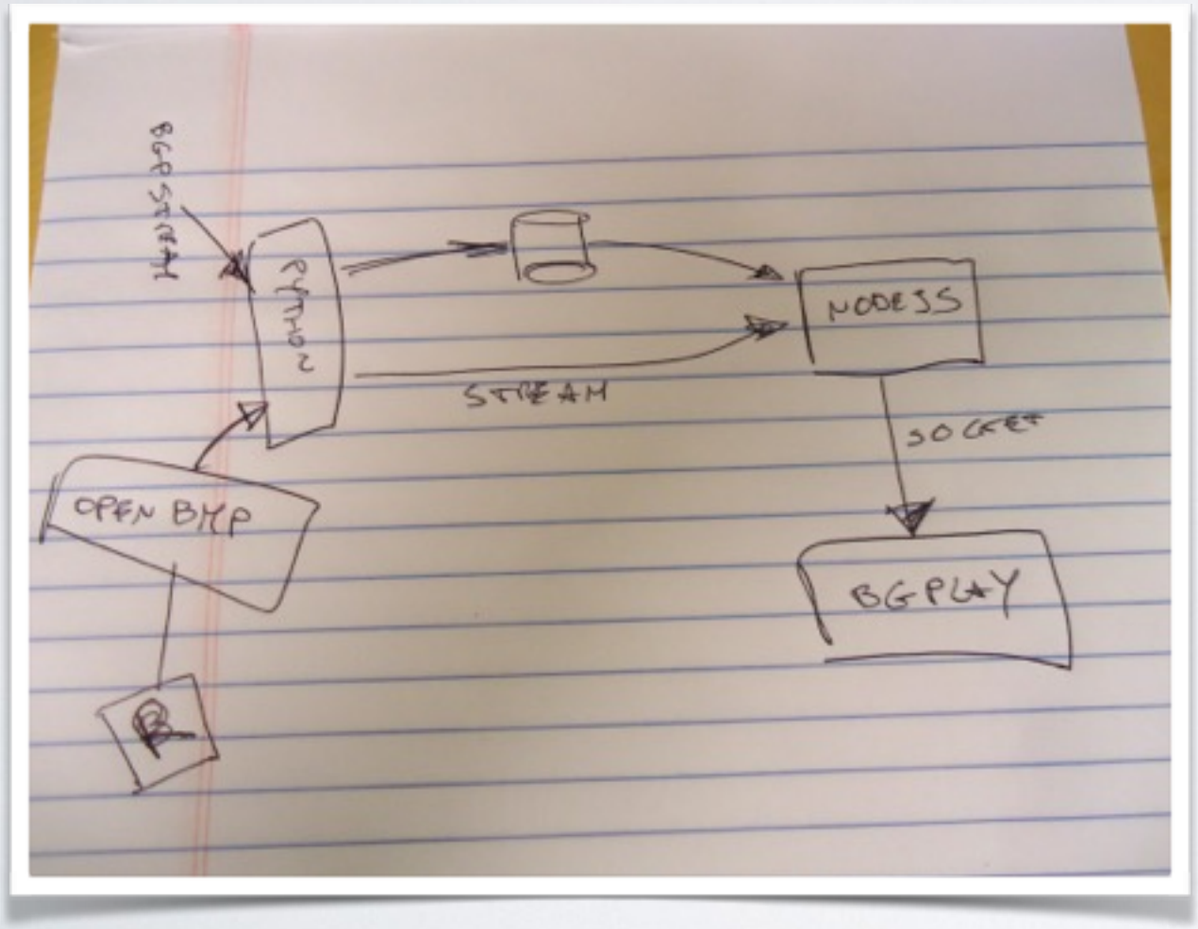
…IS CHALLENGING

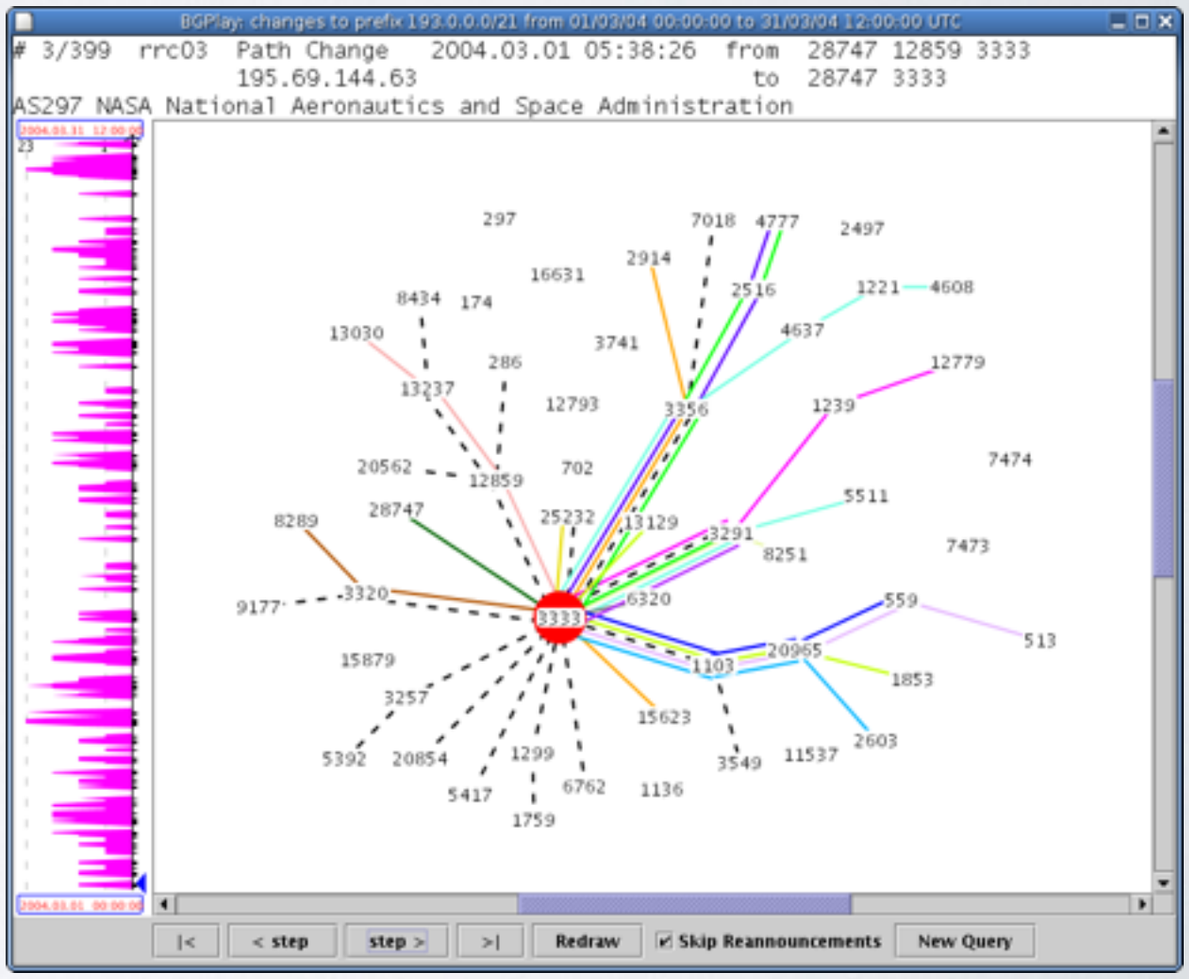
VIZ-2

TEAM

1. Massimo Candela. RIPE NCC
2. Maite Gonzalez, Universidad de Chile
3. Saif Hasan, Facebook
4. Francesco Benedetto, Roma Tre University

- Easily deployable BGPlay installation
- Data collector for ***private*** and public BGP data
- Real-time streaming and visualization



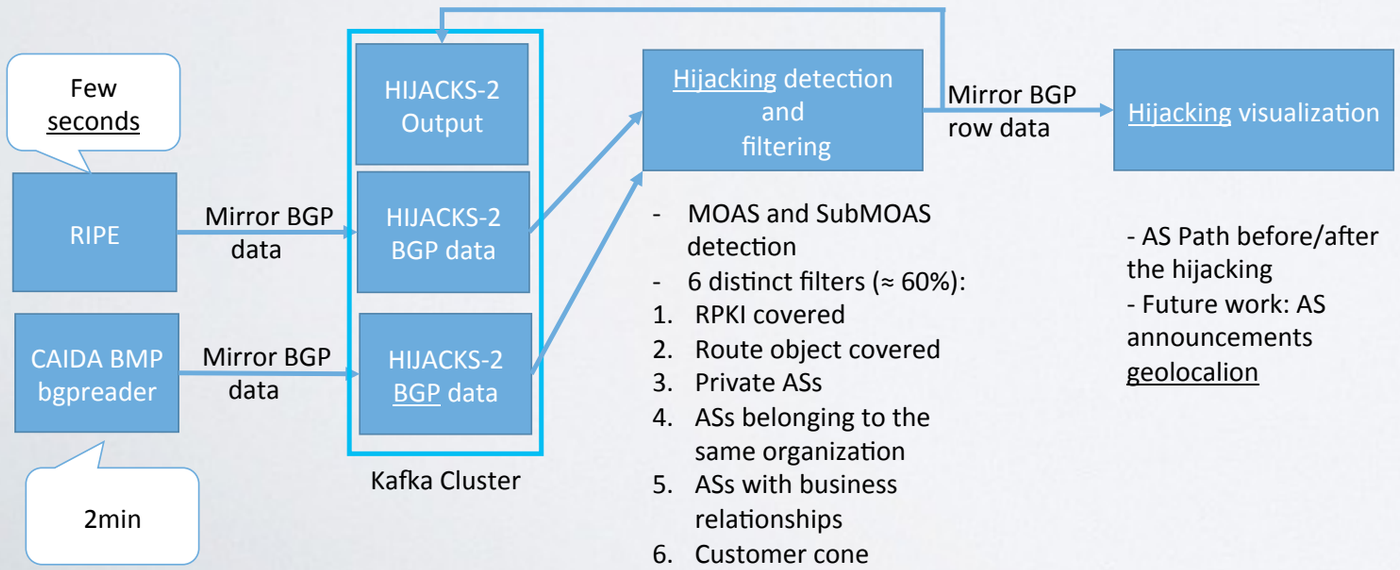


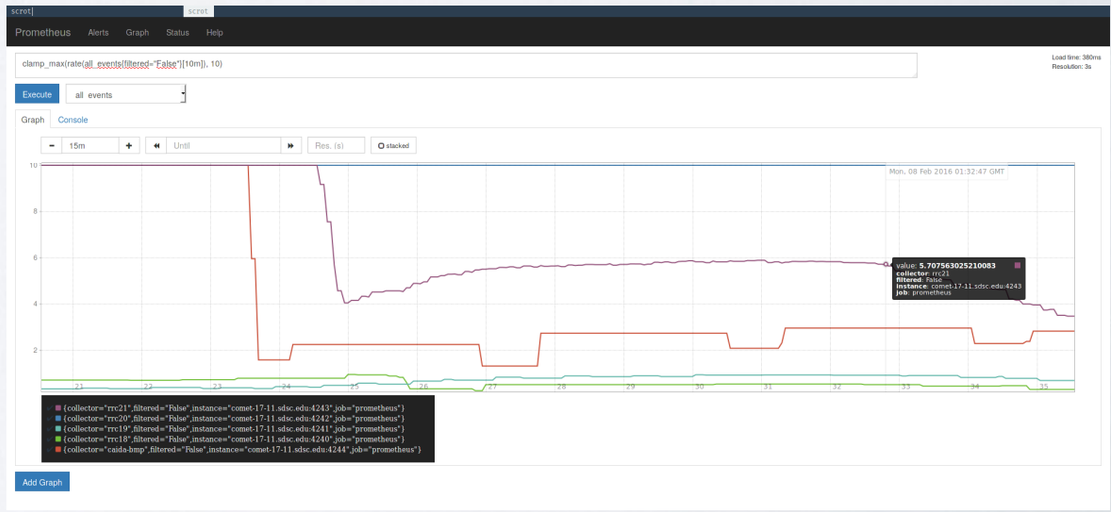
HIJACKS-2

TEAM

1 Ruwaifa Anwar, Stony Brook University, New York
2 Danilo Cicalese, Telecom ParisTech
3 Nicolas Vivet, FNISA
4 Kaname Nishizuka, NTT Communications
5 Danilo Giordano, Politecnico di Torino
6 Charles Brock, ICASA / NMT
7 Bruno Machado, Universidade Federal de Minas Gerais

- MOAS and “SubMOAS” detection
- Implemented new rules to filter out benign cases
- Used CAIDA BMP, RIPE RIS stream and PEERING
- Monitor on control plane and data plane
- **Open source** project available at github: https://github.com/CAIDA/bgp-hackaton/tree/Hijacks-2





BGPSTREAM-1

TEAM
Shane Alcock, University of Waikato

BGPStream-1

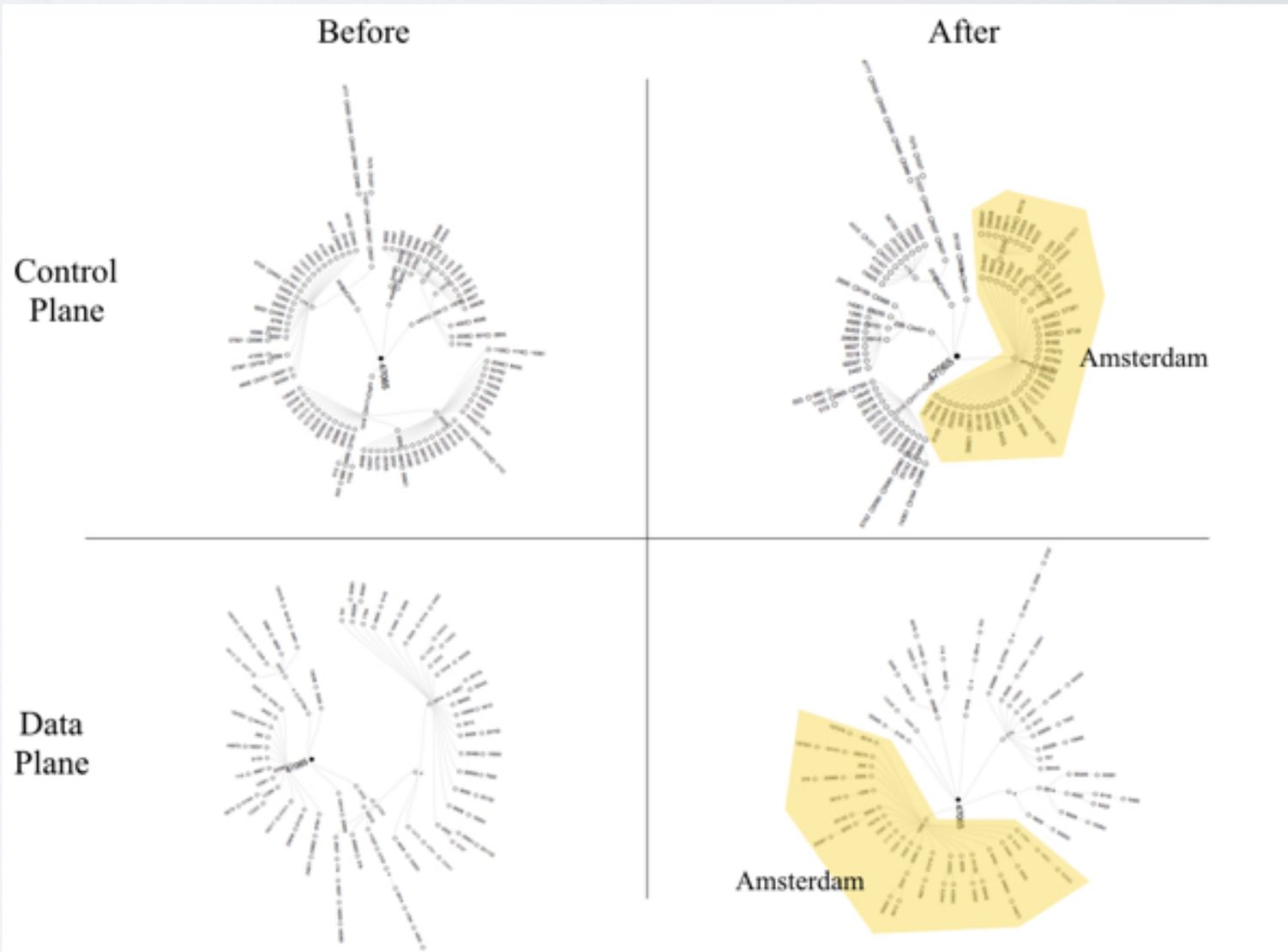
- Improved filtering / usability for BGPStream
- Created BPF-style language for describing filters
  - “project ris and collector rrc03 and prefix exact 205.107.140.0/24”
  - One CLI option, one API call
- New element properties to filter on
  - Element type, IP version, exact prefix match, less specific prefix
  - AS Path (using regular expressions)
- Add new method for specifying time period
  - “3 h” = give me the last three hours
  - “15 m” = give me the last 15 minutes

ANYCAST-1

TEAM

1 Ricardo Schmidt, University of Twente
2 Wouter de Vries, University of Twente
3 Azzam Alsudais, CU Boulder
4 Roya Ensafi, Princeton University
5 Nick Wolff, OARnet

- Used the PEERING testbed to emulate a service that uses anycast
- Set up 7 muxes for the chosen prefix
- Used RIPE atlas probes to repeatedly traceroute to the prefix from different geographic locations
- Then, announced this prefix from the muxes. Waited for a while and then after sometimes terminated the most popular mutex.
- Used both traceroutes and a BGP RIPE collectors (looking glasses) to monitor the changes.



REPORTS ETC. WILL FOLLOW

https://www.caida.org/workshops/bgp-hackathon/1602/