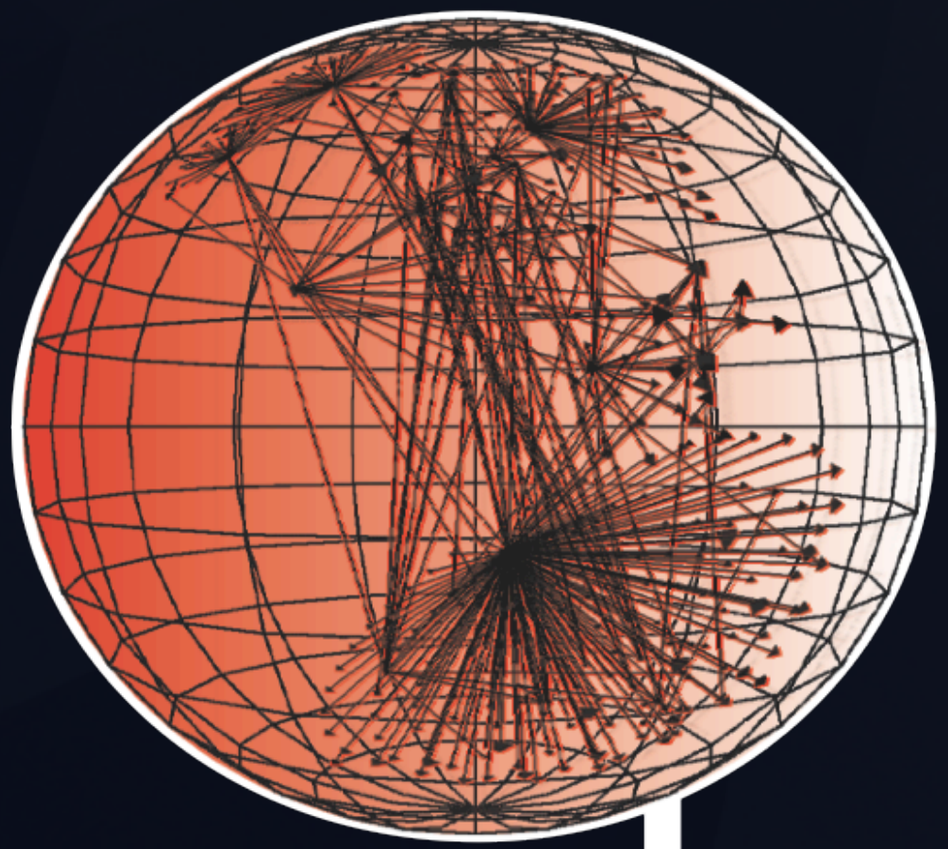
CAIDA Overview 2019

Bradley Huffaker, CAIDA

IIJ
Jan 2020



caida

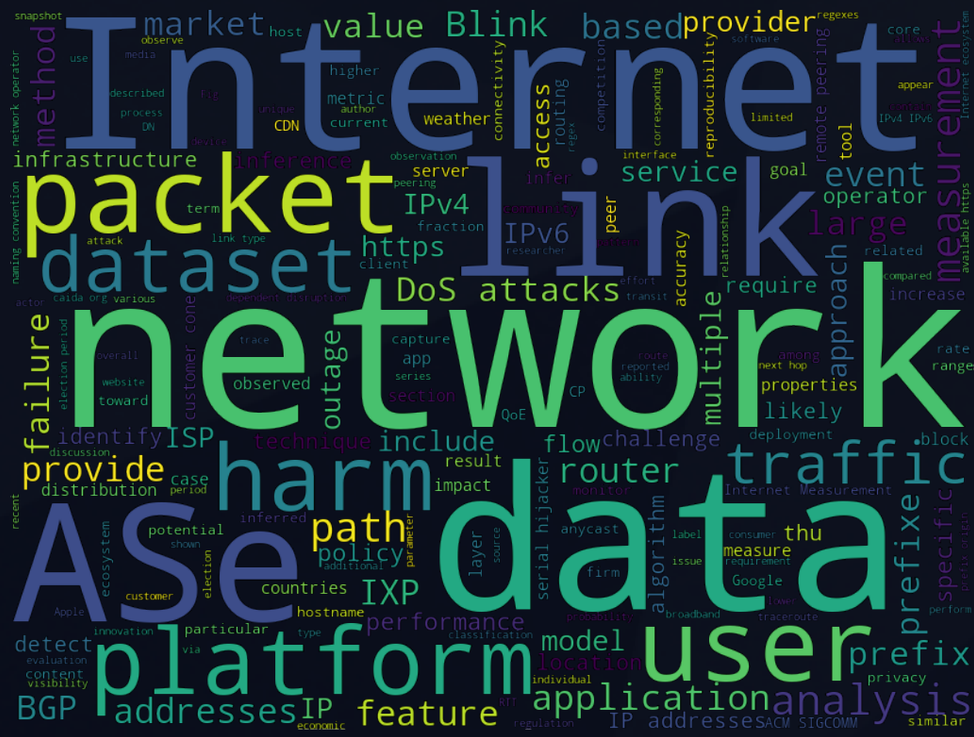
Overview

- research
  - publications 25
  - workshops 3
- infrastructure
  - measurement infrastructure
  - services (API/Web)
- datasets

Publications 2019

http://www.caida.org/publications/papers

- programmable switches (2 papers)
- traffic (2 papers)
- structural (6 papers)
- security (5 papers)
- internet outages (2 papers)
- quality of experience (2 papers)
- policy (4 papers)
- workshop reports (2 papers)



23 papers / 2 reports

Workshops 2019

http://www.caida.org/workshops/

- International Workshop on Darkspace and UnSolicited Traffic Analysis (DUST 2nd)

  http://www.caida.org/workshops/dust/1909/

- Active Internet Measurements (AIMS 11th)

  http://www.caida.org/workshops/aims/1904/

- Workshop on Internet Economics: Knowledge of Internet Structure: Measurement, Epistemology, and Technology (WIE 10: KISMET)

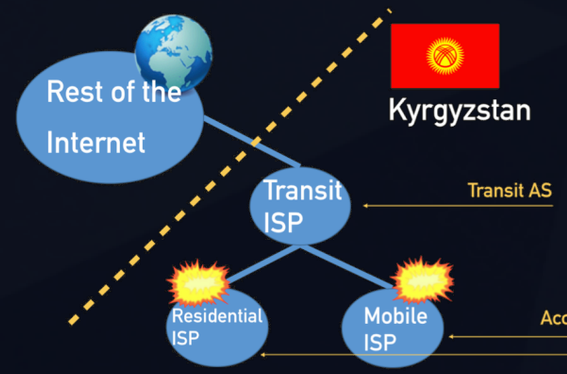
  http://www.caida.org/workshops/kismet/1912/

Mapkit

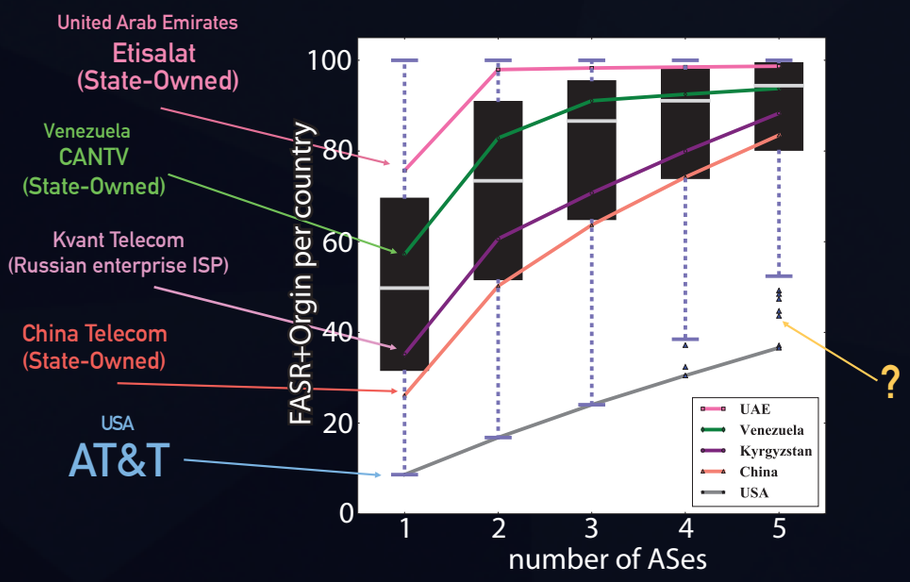
http://www.caida.org/funding/satc-mapkit/

- identify “key terrain” of a country’s cyberspace:
  - Autonomous Systems (AS), IXPs, PoPs, colocation etc

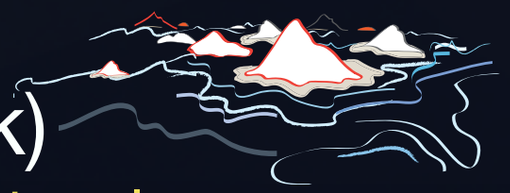
- AS-Level Transit Influence (ATI)
  - fraction of country’s addresses transiting an AS



- Country AS Topology Robustness
  - degree to which a country’s address space is dependent on a small number of ASes



Measurement Infrastructure



- Archipelago (ark)
  - supports ongoing topology measurement as well as customized experiments
- UCSD Internet Telescope (IBR)
  - packet capture to largely unused address space (one-way traffic only)
- Passive Trace Capture
  - captures packets on Tier 1 10GE backbone link (two-way traffic)
  - shared anonymized headers only

infrastructure

Archipelago

http://www.caida.org/projects/ark

caida

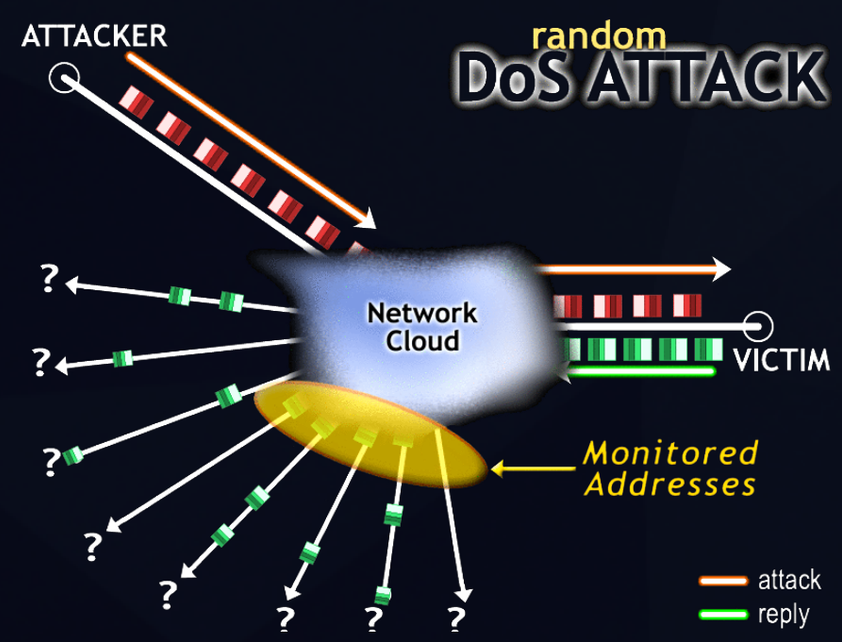
- CAIDA's active measurement infrastructure
- 188 monitors
  - 76 IPv6-enabled
  - 165 Raspberry PIs, 23 servers
  - 52 countries
- current projects
  - team-probing experiment to collect IPv4 and IPv6 topology (172)
  - MANIC (89)
  - researcher experiments, e.g., spoofer
  - Youtube QOE experiments (11)

infrastructure

Stardust

http://www.caida.org/funding/stardust/

- passive traffic monitoring of UCSD **Network Telescope**
- 0.2% of the **Internet** address space (/9+/10)
- traffic reaching the router is *unsolicited* (Internet background Radiation)
- we collect and analyze this traffic
  - malware attempting to propagate
  - backscatter from spoofed DoS attacks
  - misconfigurations
  - network scans
  - network outages



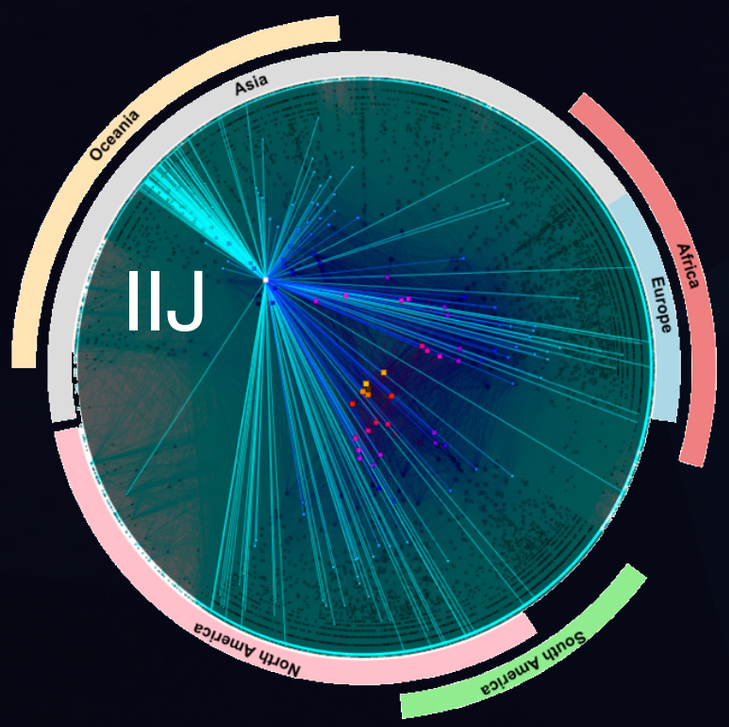
CAIDA Services http://www.caida.org/services

Services	Interfaces	Tags	Status
ASRank	Web UI / API	ASN names, org., geo, topology as-rank.caida.org	public
BGPSTREAM	API	BGP traces, AS paths, prefixes bgpstream.caida.org	public
IODA INTERNET OUTAGE DETECTION AND ANALYSIS	Web UI	outages, darknet ioda.caida.org	public
MANIC	Web UI / API	congestion, interdomain links, IP links manic.caida.org	restricted
Vela	Web UI / API	IP topology, ping, traceroute, Ark vela.caida.org	restricted
HI³	Web UI	security-related Internet time series hicube.caida.org	restricted
PANDA	Web UI /API	Internet related database / API	development
OKN-KISMET	Web UI / API	Internet identifier systems	development
FANTAIL	Web UI / API	IP and AS level trace, topology DB	development

ASRank v2

http://asrank.caida.org

- GraphQL
- JSON Output
- AS Information, Organization, Relationships, Visualization



http://api.asrank.caida.org/v2/graphql

GraphQL

```
# request ASN 3356's degree
query={
   asn(asn:"3356") {
      asnDegree {
         transit
      }
   }
}
```

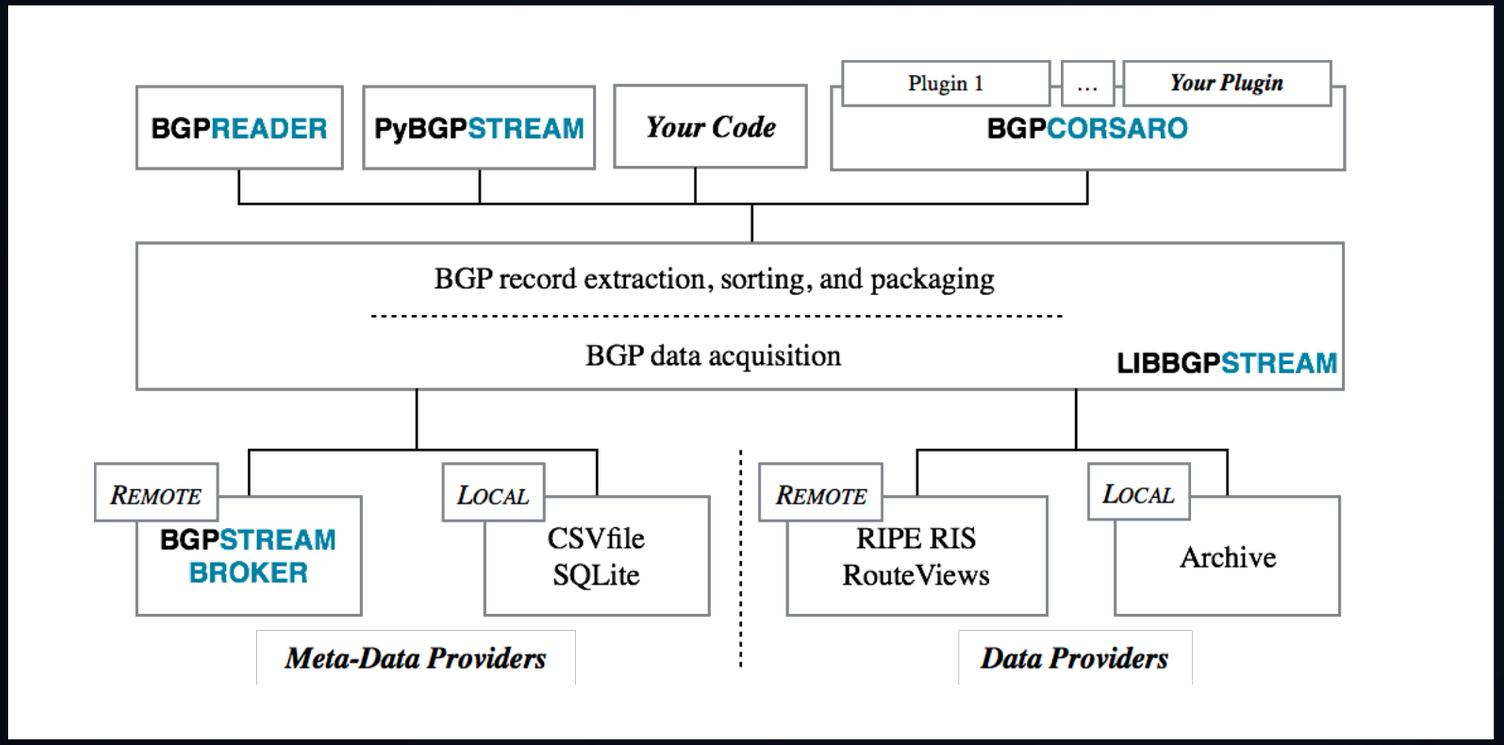
response

```
data={
    “asn": {
      "asnDegree": {
         "transit": 5255
    }
}
```

BGPSTREAM

http://bgpstream.caida.org

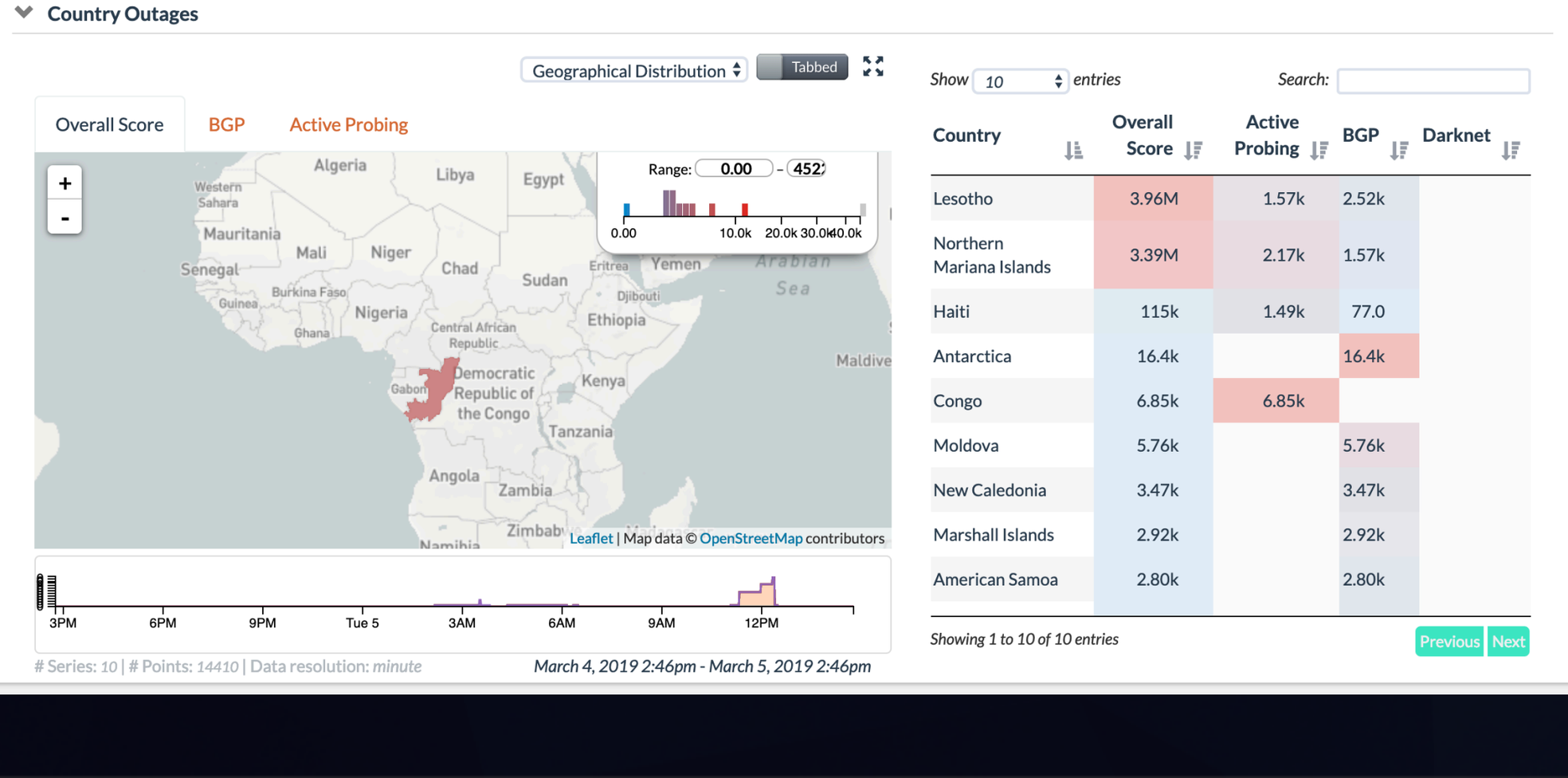
- framework for live / historical BGP data analysis
- C/C++ library , Python bindings



services

http://ioda.caida.org

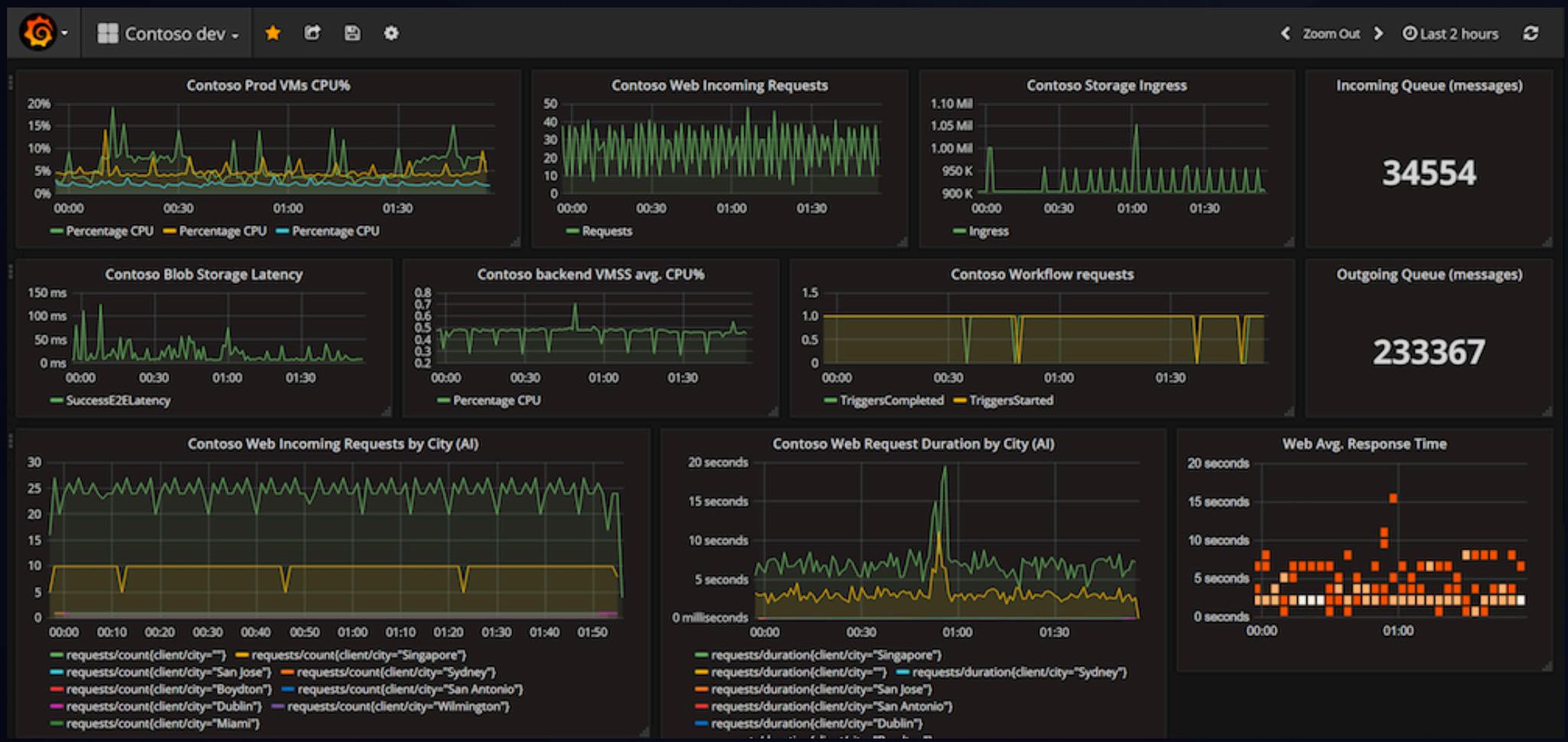
- system to detect and visualize Internet outages in near realtime
- interfaces
  - dashboard
  - alert feed



services

http://manic.caida.org

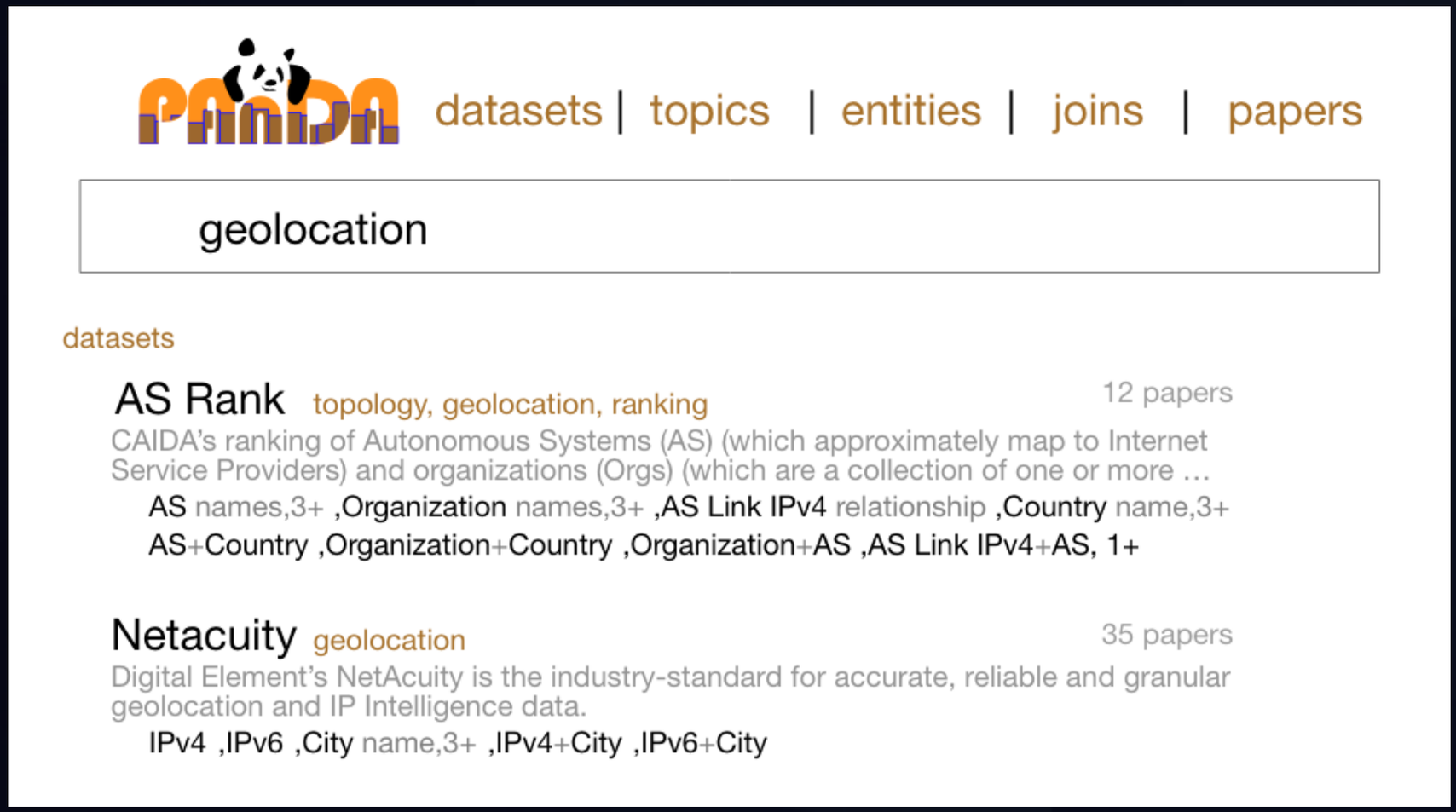
- system to infer congestion with a web interface
- API to **T**ime **S**eries **L**atency **P**rob (**TSLP**) data
  - JSON output



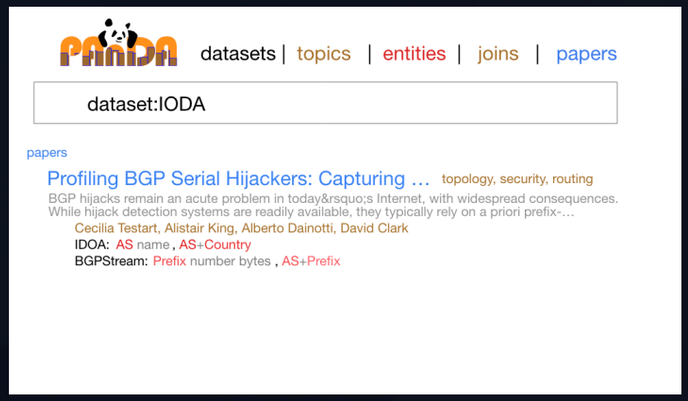
services

(under development)

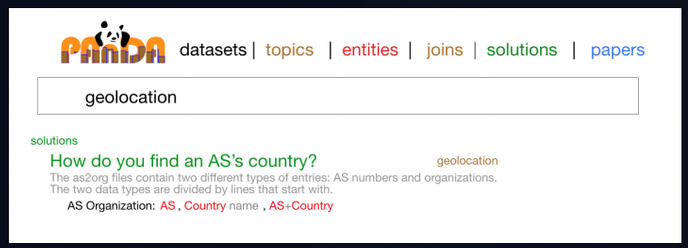
- unified interface to CAIDA datasets



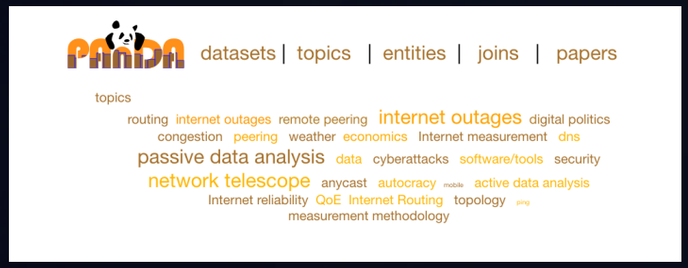
papers



solutions



topics



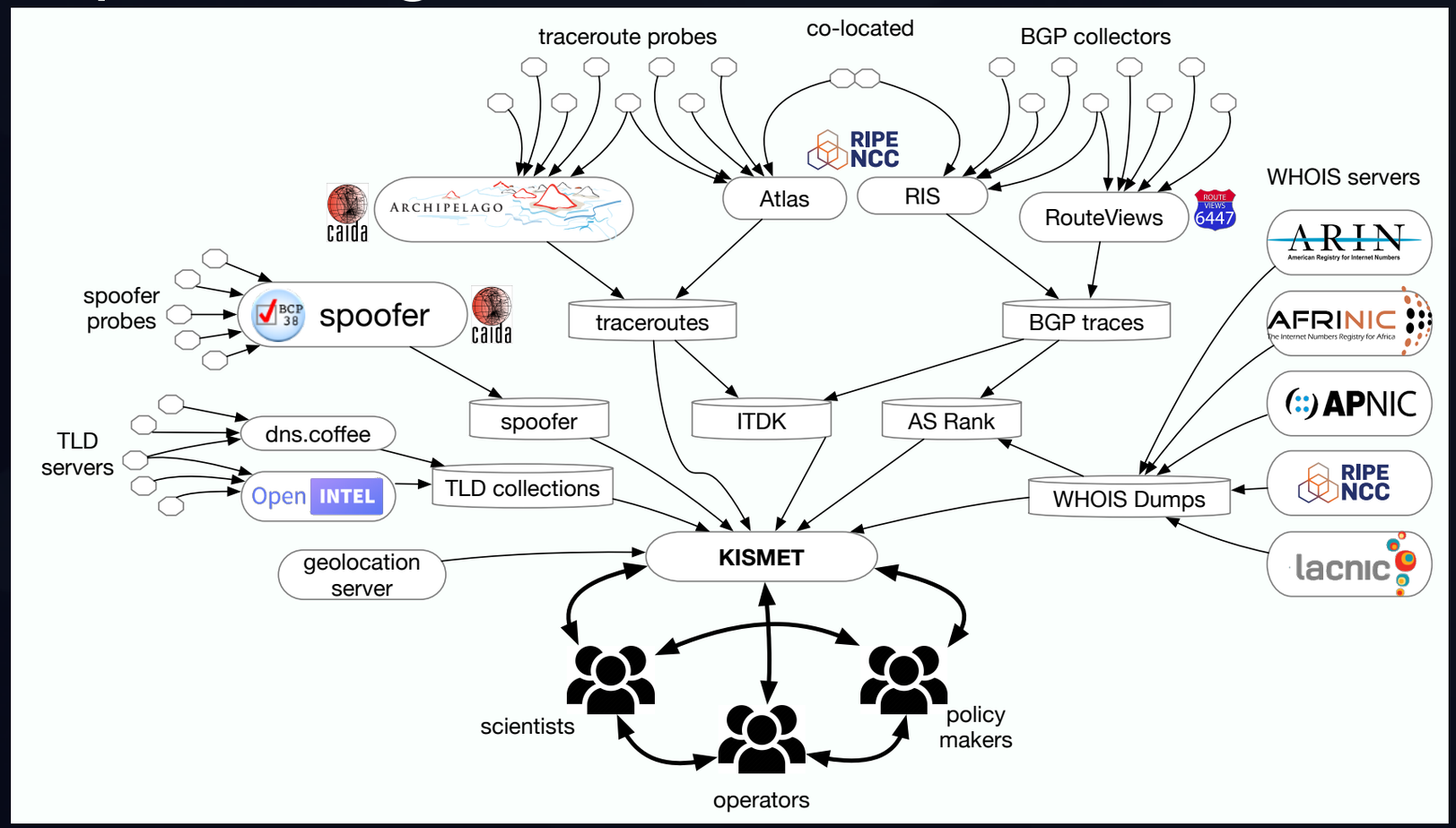
OKN-KISMET

(under development)

Open Knowledge Network:
Knowledge of Internet Structure:
Epistemology, and Technology

http://www.caida.org/funding/okn-kismet/

- phase 1: multi-stakeholder team building effort
  - academic, government, industry
- focus on Internet identifier systems
- explore rich relationships among:
  - domain names
  - Autonomous Systems
  - IP address
  - name servers



FANTAIL

(under development)

Facilitating Advances in
Network Topology Analysis

http://www.caida.org/funding/ccri-fantail/

- IP and AS level trace, topology DB
- scalable search on annotated IP traces

traceroute to 200.136.34.2 (sao2-br.ark.caida.org) from **bjc-us** of *commercial network (6)* using ICMP

Hop	Address	Prefix	AS	Location	RTT (ms)
1	**unknown.Level3.net** 209.245.28.1	209.244.0.0/14	3356	broomfield, co usa	0.3
2	**ge-5-0-48.hsa2.Denver1.Level3.net** 209.245.29.226	209.244.0.0/14	3356	denver, co usa	0.8
3	**ge-7-36.car2.Denver1.Level3.net** 4.69.200.66	4.0.0.0/9	3356	denver, co usa	1.9
4	**vlan51.ebr1.Denver1.Level3.net** 4.69.147.94	4.0.0.0/9	3356	denver, co usa	0.8
5	**ae-2-2.ebr2.Dallas1.Level3.net** 4.69.132.106	4.0.0.0/9	3356	dallas, tx usa	15.0
6	**ae-72-72.csw2.Dallas1.Level3.net** 4.69.151.141	4.0.0.0/9	3356	dallas, tx usa	15.0
7	**ae-2-70.edge2.Dallas1.Level3.net** 4.69.145.75	4.0.0.0/9	3356	dallas, tx usa	15.6
8	**DATA-RETURN.edge2.Dallas1.Level3.net** 4.71.220.70	4.0.0.0/9	3356	dallas, tx usa	15.1
9	**g1-10.br1.dfw.terremark.net** 66.165.160.249	66.165.160.0/19	23148	dallas, tx usa	47.1

CAIDA Datasets

http://www.caida.org/data/*

- **I**nternet **T**opology **D**ata **K**it (ITDK) (restricted)
  - http://www.caida.org/data/internet-topology-data-kit
  - IP topologies, routers, geolocations

- Internet eXchange Points (public)
  - http://www.caida.org/data/ixps
  - IX's geolocations, prefixex, AS members

- CYMRU Bogon Historic (public)
  - https://www.caida.org/data/bogons/
  - Historic and current CYMRU Bogon data

- Topology data (IPv4/IPv6) trace data (restricted)
  - http://www.caida.org/ipv4_routed_24_topology_dataset.xml
  - IP topologies, IP trace routes

- DNS-names (restricted)
  - http://www.caida.org/data/active/ipv4_dns_names_datasert.xml
  - DNS names for IPs in IPv4 routed /24

*selected

Questions?

- publications
  http://www.caida.org/publications/papers
- workshops
  http://www.caida.org/workshops/
- services
  http://www.caida.org/services
- datasets
  http://www.caida.org/data/overview/

Bradley Huffaker
CAIDA/UCSD
bradley@caida.org