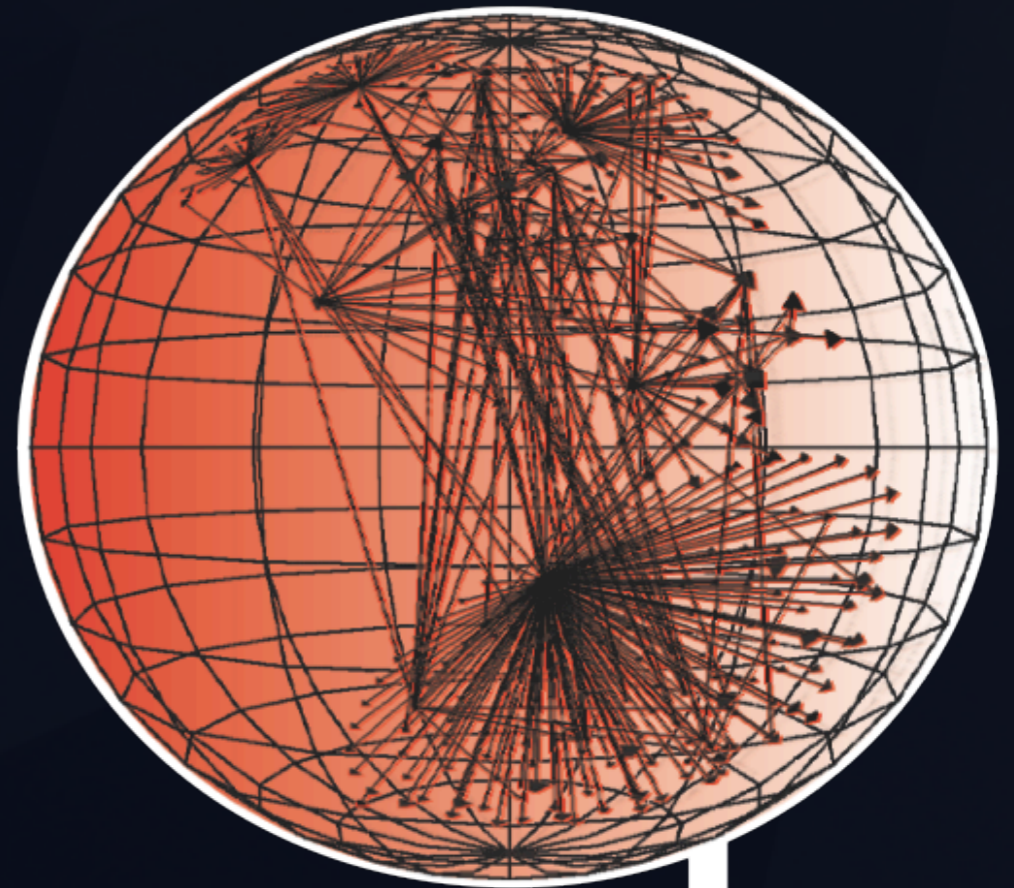


CAIDA Overview 2019

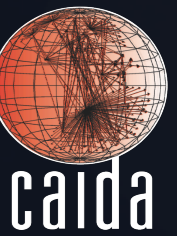
Bradley Huffaker, CAIDA

*IIJ
Jan 2019*



caida

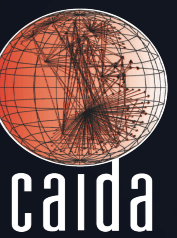
Overview



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

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 (AIM 11th)

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

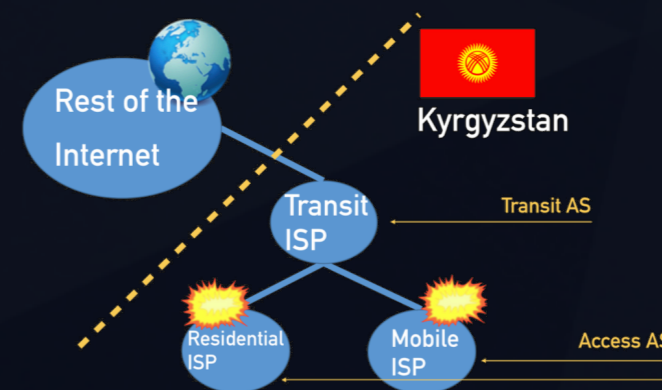
- Workshop on Internet Economics: Knowledge of Internet Structure: Measurement, Epistemology, and Technology (WIE 10: KISMET)

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

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

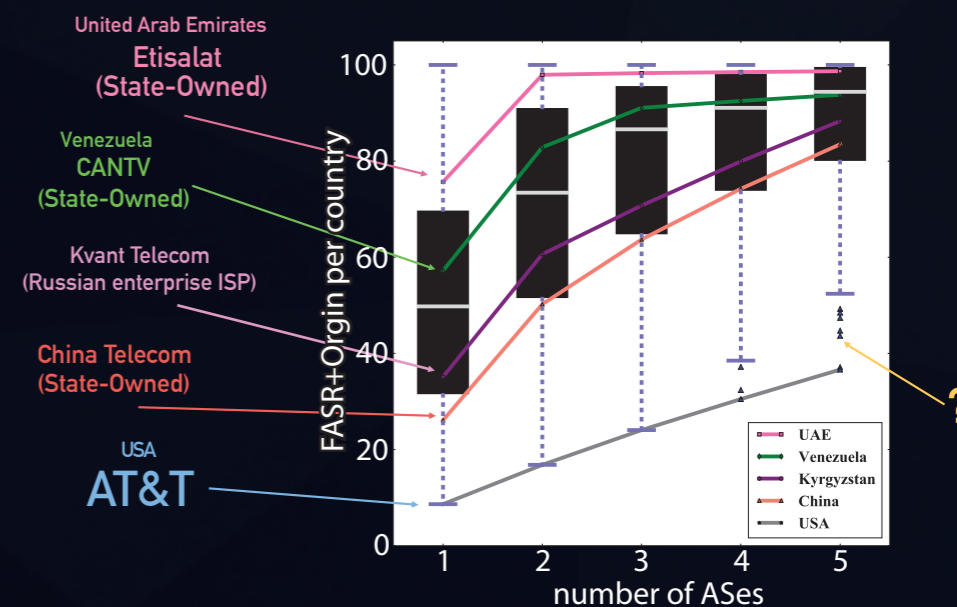
- AS-Level Transit Influence (ATI)

- fraction of country’s addresses transiting an AS

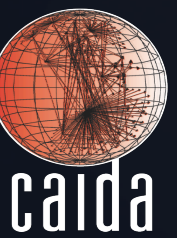


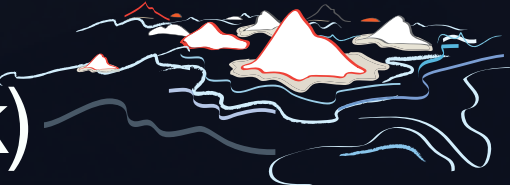
- Country AS Topology Robustness

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



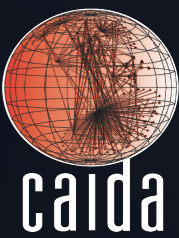
Measurement Infrastructure



- 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

Archipelago

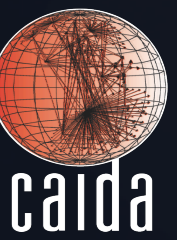
<http://www.caida.org/projects/ark>



- 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)

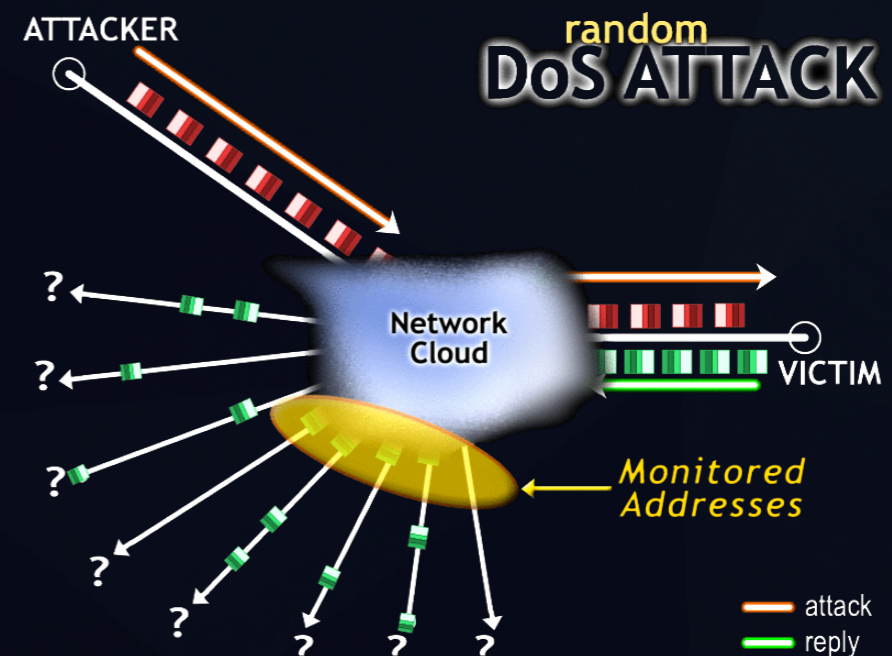


infrastructure Stardust

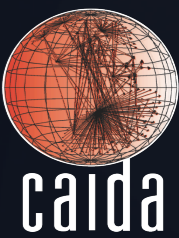








<http://www.caida.org/funding/stardust/>







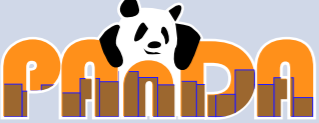


- passive traffic monitoring of UCSD **Network Telescope**
- 0.2% of the **Internet** address space (/9+/10)
- traffic reaching the router is *unsolicited* (Internet background Radiation)
- we collect and analyze this traffic
 - malware attempting to propagate
 - backscatter from spoofed DoS attacks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



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



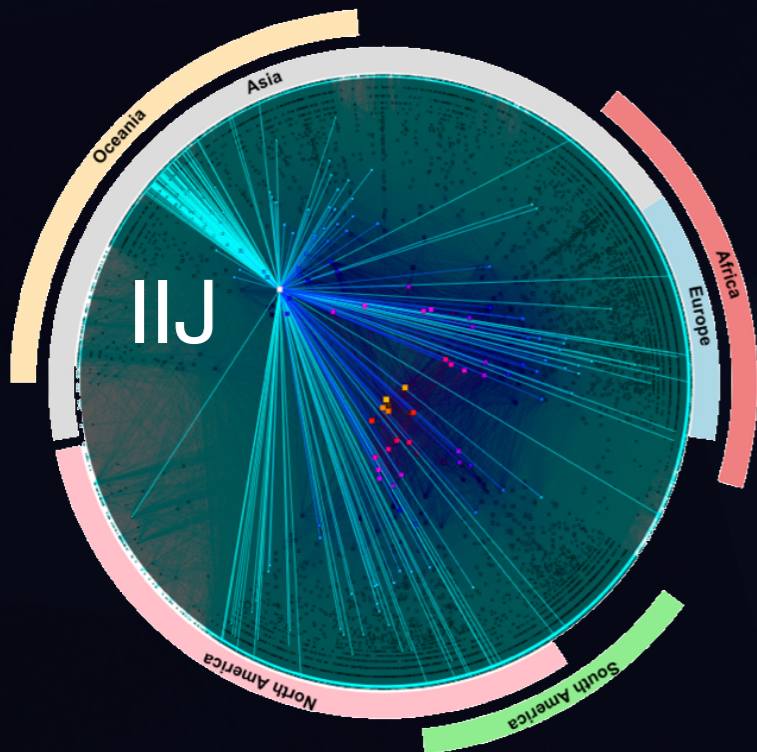
Services	Interfaces	Tags	Status
	Web UI / API	ASN names, org., geo, topology as-rank.caida.org	public
	API	BGP traces, AS paths, prefixes bgpstream.caida.org	public
 <small>INTERNET OUTAGE DETECTION AND ANALYSIS</small>	Web UI	outages, darknet ioda.caida.org	public
	Web UI / API	congestion, interdomain links, IP links manic.caida.org	restricted
Vela	Web UI / API	IP topology, ping, traceroute, Ark vela.caida.org	restricted
	Web UI	security-related Internet time series hicube.caida.org	restricted
	Web UI /API	Internet related database / API	development

Services	Interfaces	Tags	Status
	Web UI / API	ASN names, org., geo, topology as-rank.caida.org	public
	API	BGP traces, AS paths, prefixes bgpstream.caida.org	public
	Web UI	outages, darknet ioda.caida.org	public
	Web UI / API	congestion, interdomain links, IP links manic.caida.org	restricted
	Web UI / API	IP topology, ping, traceroute, Ark vela.caida.org	restricted
	Web UI	security-related Internet time series hicube.caida.org	restricted
	Web UI / API	Internet related database / API	development
	Web UI / API	Internet identifier systems	development
	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
    }
  }
}
```



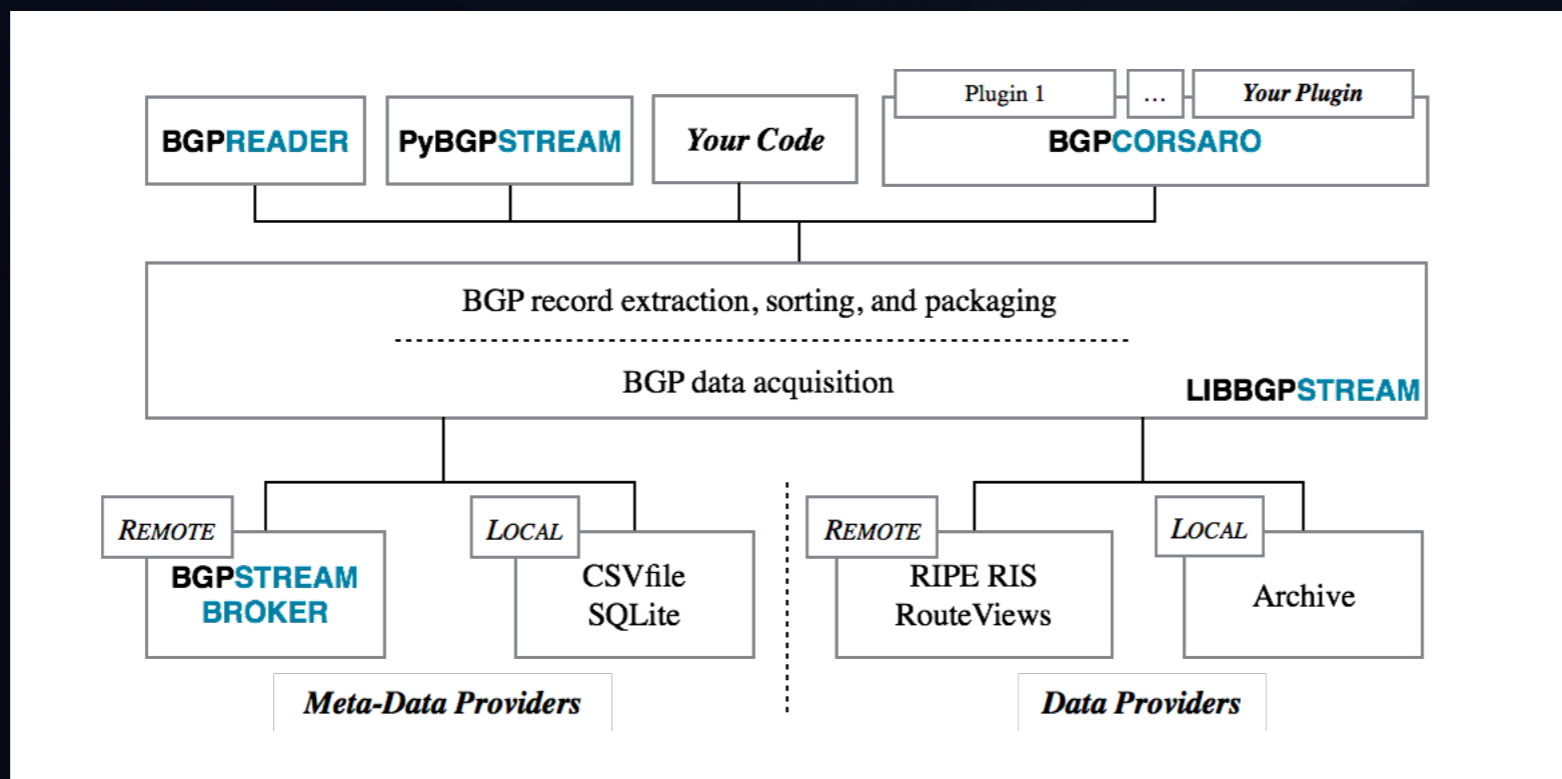
response

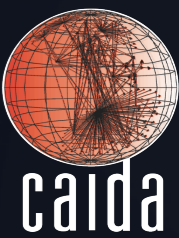
```
data={
  "asn": {
    "asnDegree": {
      "transit": 5255
    }
  }
}
```



<http://bgpstream.caida.org>

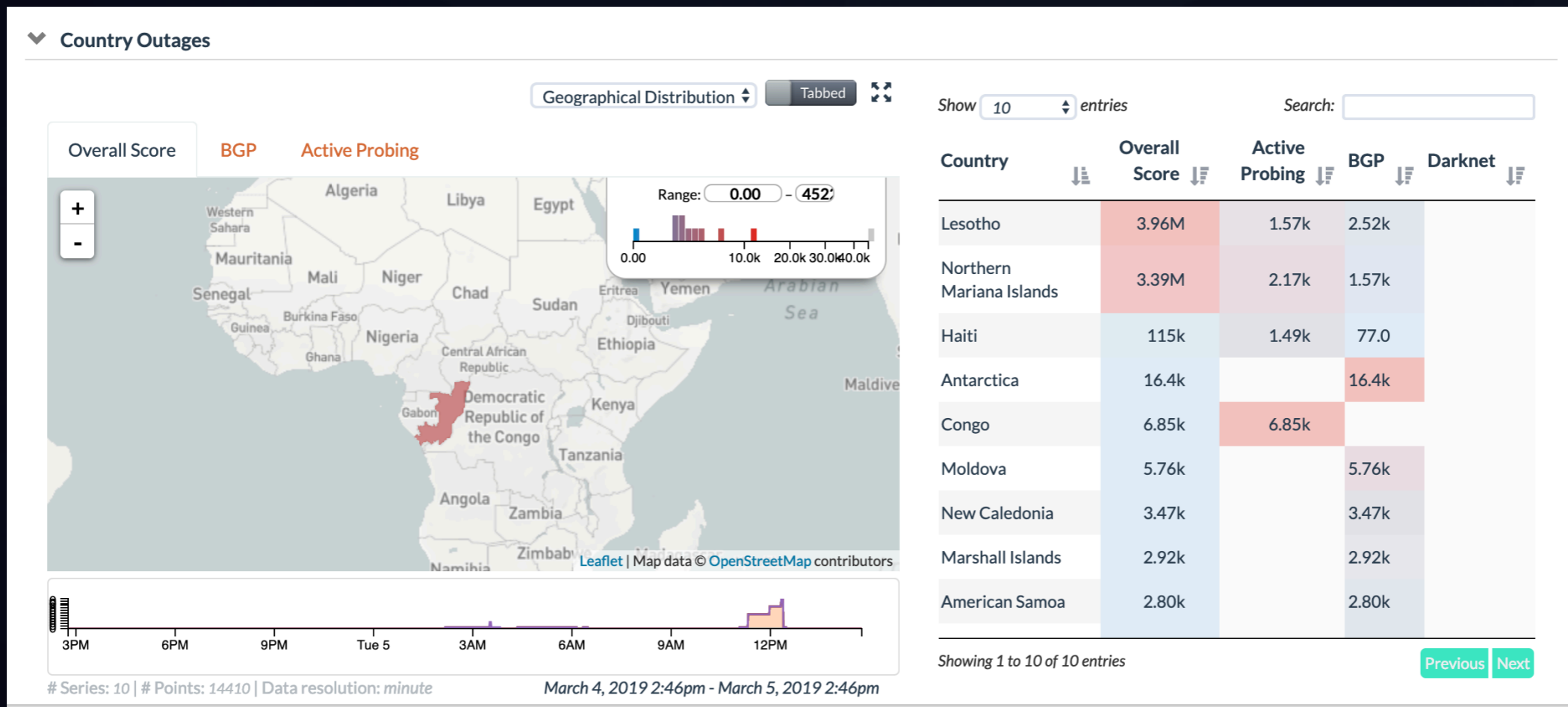
- framework for live / historical BGP data analysis
- C/C++ library , Python bindings

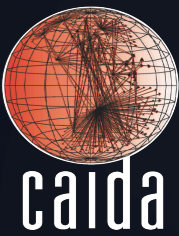




<http://ioda.caida.org>

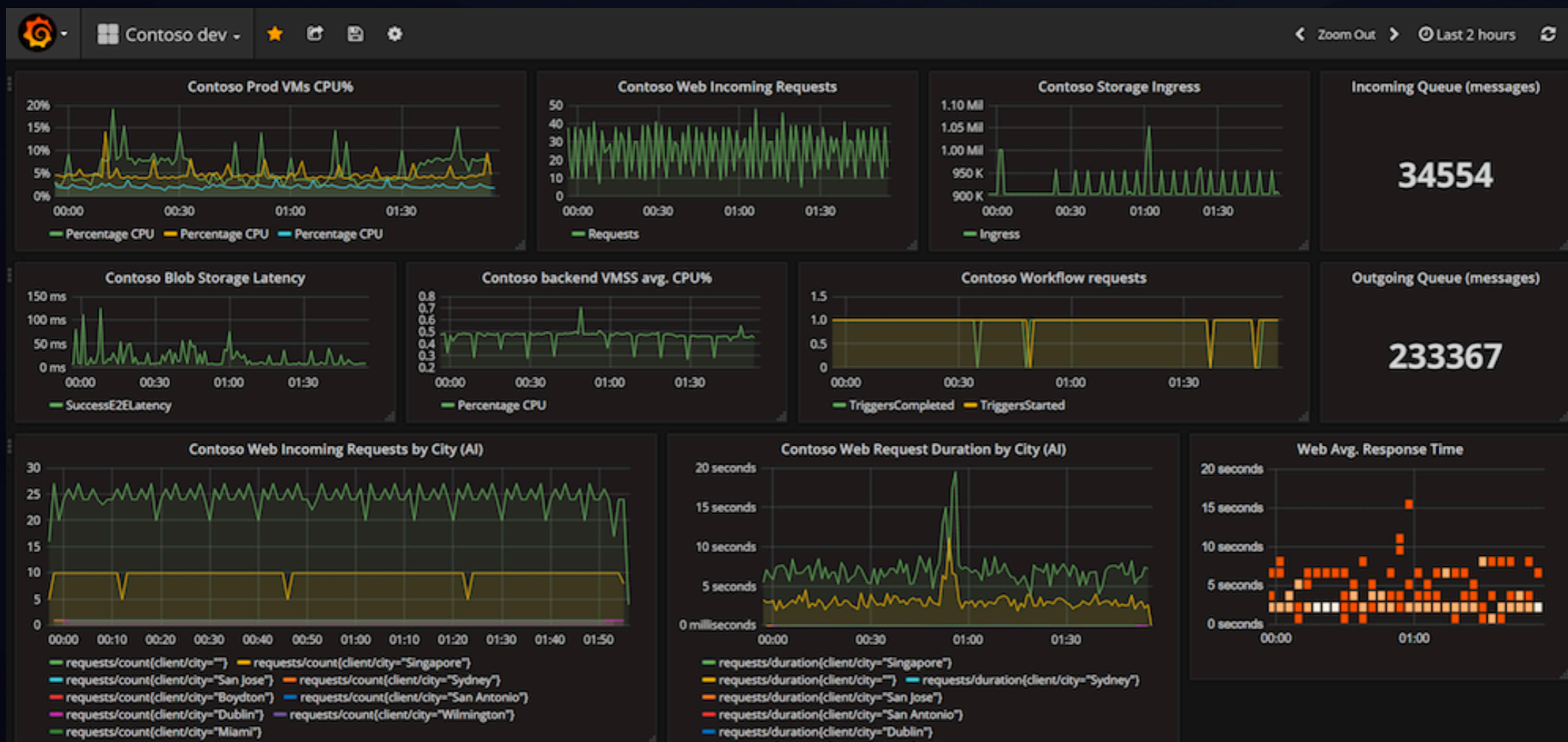
- system to detect and visualize Internet outages in near realtime
- interfaces
 - dashboard
 - alert feed

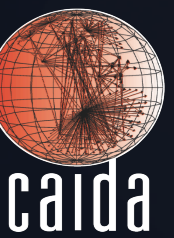




<http://manic.caida.org>

- system to infer congestion with a web interface
- API to Time Series Latency Prob (TSLP) data
 - JSON output





- unified interface to CAIDA datasets

papers

geolocation

datasets

AS Rank *topology, geolocation, ranking* 12 papers
 CAIDA's ranking of Autonomous Systems (AS) (which approximately map to Internet Service Providers) and organizations (Orgs) (which are a collection of one or more ...
 AS names,3+ ,Organization names,3+ ,AS Link IPv4 relationship ,Country name,3+ AS+Country ,Organization+Country ,Organization+AS ,AS Link IPv4+AS, 1+

Netacuity *geolocation* 35 papers
 Digital Element's NetAcuity is the industry-standard for accurate, reliable and granular geolocation and IP Intelligence data.
 IPv4 ,IPv6 ,City name,3+ ,IPv4+City ,IPv6+City

dataset:IODA

papers

Profiling BGP Serial Hijackers: Capturing ... *topology, security, routing*
 BGP hijacks remain an acute problem in today's Internet, with widespread consequences. While hijack detection systems are readily available, they typically rely on a priori prefix-...
 Cecilia Testart, Alistair King, Alberto Dainotti, David Clark
 IDOA: AS name , AS+Country
 BGPStream: Prefix number bytes , AS+Prefix

solutions

geolocation

solutions

How do you find an AS's country? *geolocation*
 The as2org files contain two different types of entries: AS numbers and organizations. The two data types are divided by lines that start with.
 AS Organization: AS , Country name , AS+Country

topics

topics

routing internet outages remote peering internet outages digital politics congestion peering weather economics Internet measurement dns passive data analysis data cyberattacks software/tools security network telescope anycast autocracy mode active data analysis Internet reliability QoE Internet Routing topology measurement methodology

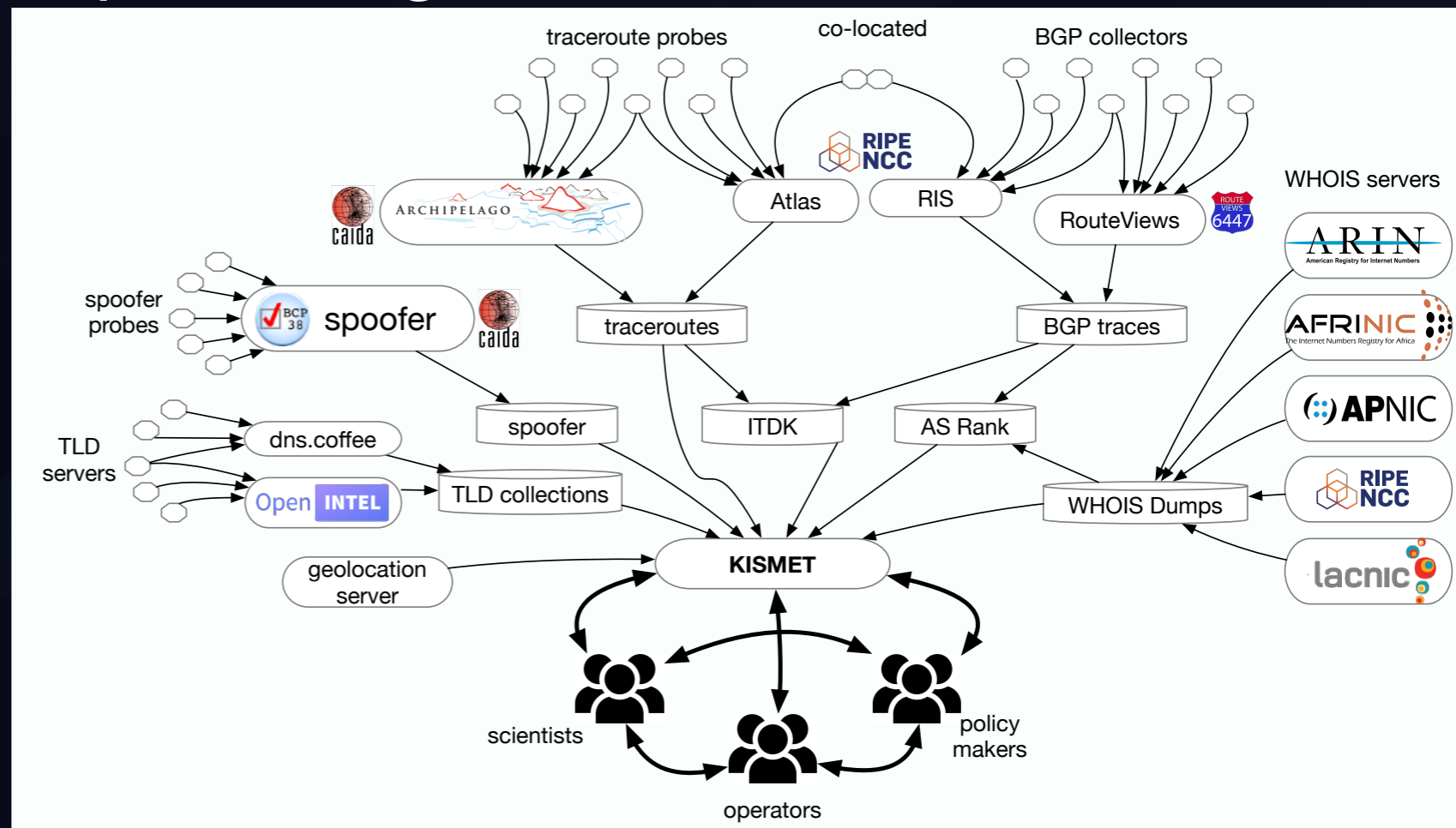
OKN-KISMET

(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

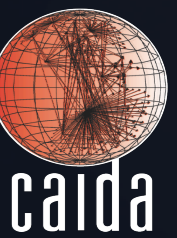
<http://www.caida.org/funding/ccri-fantail/>

- 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 ■■

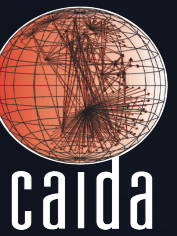
CAIDA Datasets



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

- **Internet Topology Data Kit (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

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

