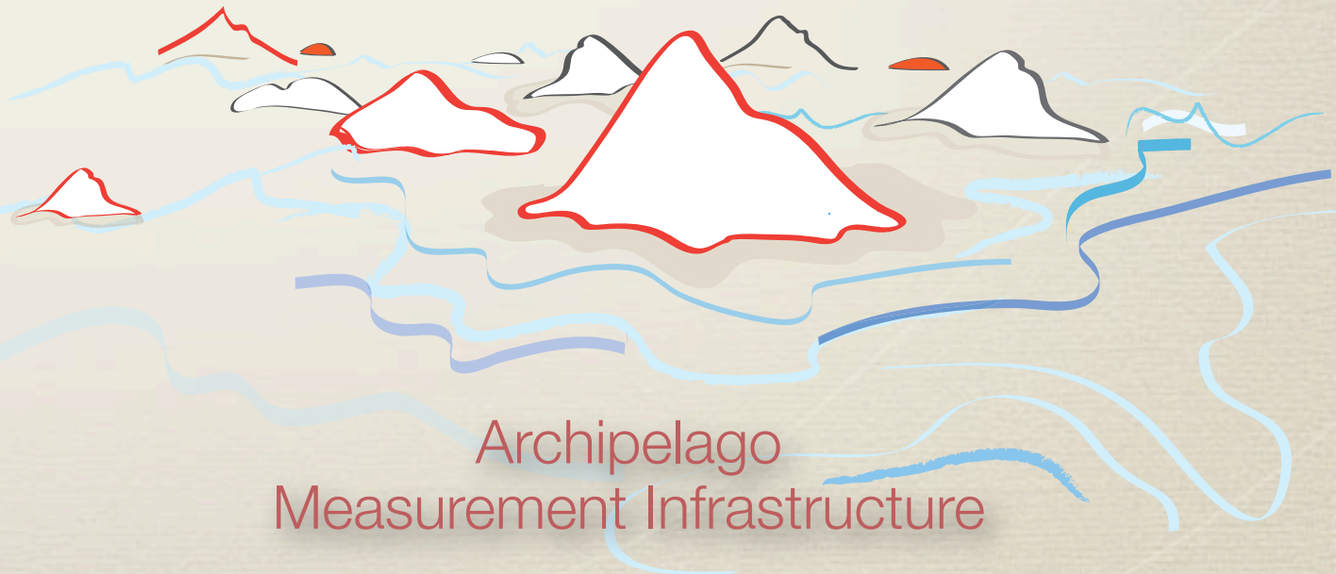
Dolphin: Bulk DNS Resolution Tool

Young Hyun
CAIDA

Jun 19, 2014

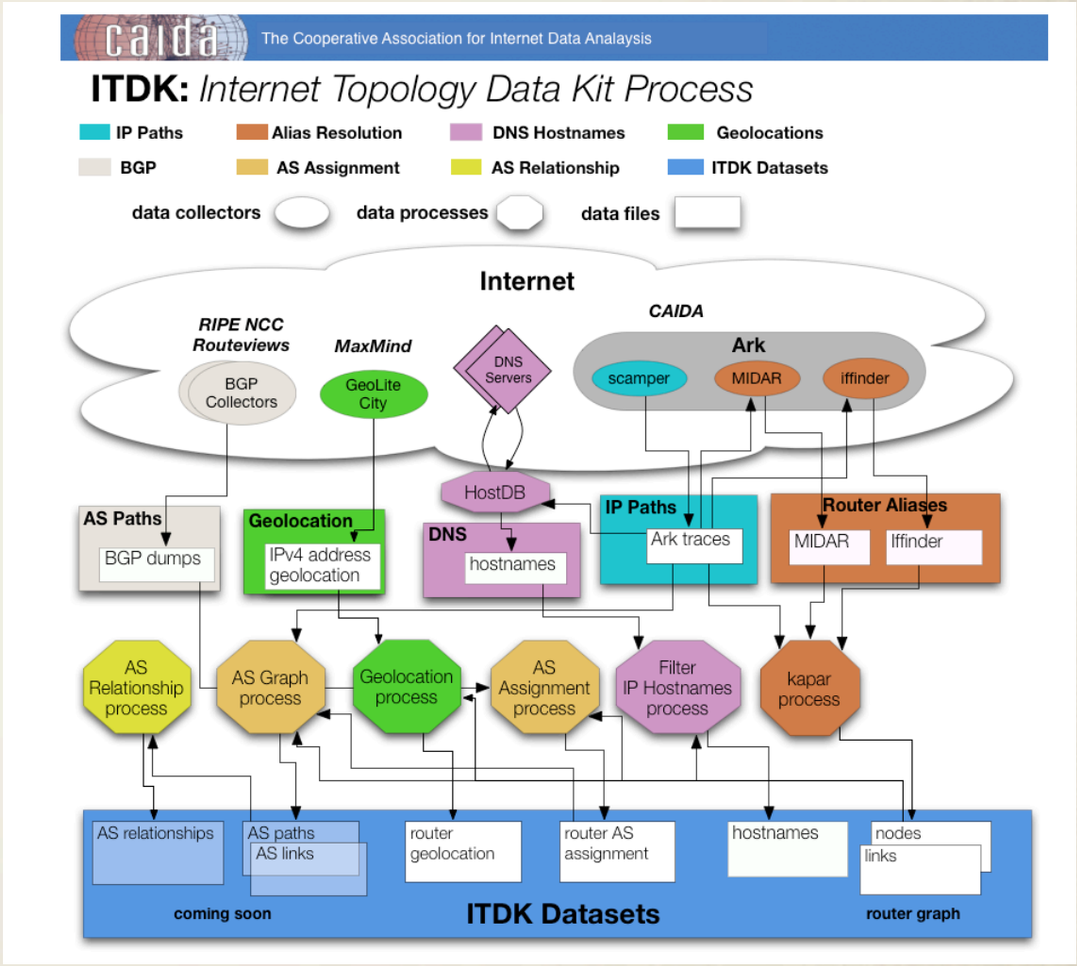


Introduction

- collecting large-scale Internet topology
  - 665 million IPv4/IPv6 traceroutes per month

Introduction

- producing Internet Topology Data Kit (ITDK)
  - two router-level graphs
    - using MIDAR, iffinder, and kapar
  - router-to-AS assignments
  - geographic location of each router
    - using MaxMind GeoLite City (free)
  - DNS names
    - using our HostDB



DNS Names

```
et-1-0-0.111.rtr.hous.net.internet2.edu

eth3530.sa.adsl.internode.on.net

ge2-13-425.psl-pe7.hel.fi.ip.tdc.net

s-br1-melb-1.bng1.sydn.nxg.net.au

gigabitethernet0-1.reg11.gdr.prosodie.net
```

DNS Names

networking
technology

et-1-0-0.111.rtr.hous.net.internet2.edu

eth3530.sa.adsl.internode.on.net

ge2-13-425.psl-pe7.hel.fi.ip.tdc.net

s-br1-melb-1.bng1.sydn.nxg.net.au

gigabitethernet0-1.reg11.gdr.prosodie.net

DNS Names

networking technology

line card position

et-1-0-0.111.rtr.hous.net.internet2.edu

eth3530.sa.adsl.internode.on.net

ge2-13-425.psl-pe7.hel.fi.ip.tdc.net

s-br1-melb-1.bng1.sydn.nxg.net.au

gigabitethernet0-1.reg11.gdr.prosodie.net

DNS Names

networking technology

line card position

PoP location / router name

```
et-1-0-0.111.rtr.hous.net.internet2.edu

eth3530.sa.adsl.internode.on.net

ge2-13-425.psl-pe7.hel.fi.ip.tdc.net

s-br1-melb-1.bng1.sydn.nxg.net.au

gigabitethernet0-1.reg11.gdr.prosodie.net
```

DNS Names

networking technology | line card position | PoP location / router name | geographic location

```
et-1-0-0.111.rtr.hous.net.internet2.edu

eth3530.sa.adsl.internode.on.net

ge2-13-425.psl-pe7.hel.fi.ip.tdc.net

s-br1-melb-1.bng1.sydn.nxg.net.au

gigabitethernet0-1.reg11.gdr.prosodie.net
```

Dolphin

Overview

- conducts parallel DNS lookups
  - millions of lookups per day from a single host
  - PTR records for IPv4 and IPv6 addresses
- retries failed lookups automatically
  - retries once per day for up to 3 days
- ensures targets only looked up once in any 7 days
  - remembers all targets queried in most recent 7 days
  - reduces load on authoritative DNS servers, independent of TTL

Implementation

- single Python source file (839 lines)
  - no installation or administration required
  - no root privileges required
- built on
  - libunbound (part of Unbound by NLnet Labs)
    - library implementing a full validating, recursive, caching resolver
    - supports IPv4/IPv6 and DNSSEC
  - LevelDB
    - library providing a persistent ordered key-value store
    - similar to Tokyo/Kyoto Cabinet, Berkeley DB, Redis, Bitcask

Possibilities

- perform DNSSEC validation
- query for A, MX, SOA, etc. records
- use ldns library for low-level structured access to raw DNS response packets
  - response header flags (e.g., AA)
  - records in authority and additional sections (e.g., glue, SOA, and DNSSEC records)

Dolphin
Usage

```
$ dolphin -v --concurrency=50 --retry-delay=4 --max-attempts=3
--root=$HOME/dolphin-state --fifo=/tmp/dolphin.queue >dolphin.out
```

--concurrency=50: do 50 concurrent DNS queries

--retry-delay=4: wait 4 hours between retries

--max-attempts=3: attempt up to 3 DNS queries per target, waiting *--retry-delay* hours between retries

--root=$HOME/dolphin-state: directory for Dolphin's working state (e.g., LevelDB database files)

--fifo=/tmp/dolphin.queue: named pipe where users can submit target addresses

>dolphin.out: DNS lookup results or errors

Dolphin

Usage

```
$ cat targets.txt >/tmp/dolphin.queue
```

targets.txt: one IPv4/IPv6 address (e.g., "1.2.3.4") per line

```
$ echo ">>EXIT" >/tmp/dolphin.queue
```

>>EXIT: request Dolphin exit after looking up all submitted targets

goal: make submission API simple to use and automate with any language

Output Format

```
<timestamp>  <address>          <hostname>
1402812960   2620:f:0:735::2     syr-7600-nyc-7600.nysernet.net
1402812960   2001:978:2:37::2:2  FAIL.NON-AUTHORITATIVE.in-addr.arpa
```

FAIL.NON-AUTHORITATIVE: no configured hostname (NXDOMAIN)

FAIL.SERVER-FAILURE: couldn't reach authoritative DNS server (SERVFAIL)

FAIL.TIMEOUT: DNS lookup timed out

Dolphin

JSON Output


```
{"timestamp": 1402965447,
 "address": "2607:da00:0:1000::9",
 "name_raw": "te0/4/1/1-ne_oma_asr9k.upnllc.com.",
 "name": "te0\\x2f4\\x2f1\\x2f1-ne\\x5foma\\x5fasr9k.upnllc.com",
 "rcode": 0,
"unbound_status": 0,
"unbound_secure": 0,
"unbound_bogus": 0}
```


goal: output complex details from raw DNS response packets

Future Work

- capture DNS query-response traffic
  - useful for tracing DNS delegation chain
- include low-level records from DNS response packets in JSON output
- possibly do DNSSEC validation
- support querying of A, MX, SOA, etc. records
- project: reverse look up of entire IPv4 address space

Thanks!

For questions: ark-info@caida.org