



VERISIGN®

DNSViz – Powerful DNS Analysis

Casey Deccio

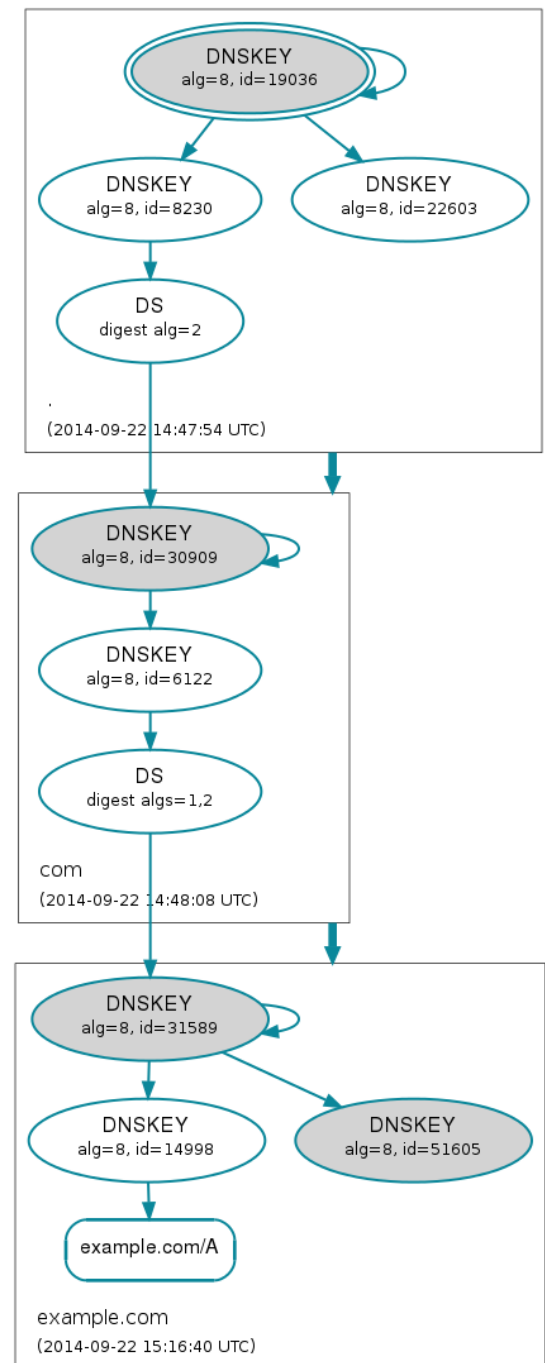
Verisign Labs

NANOG 63

Feb 3, 2015

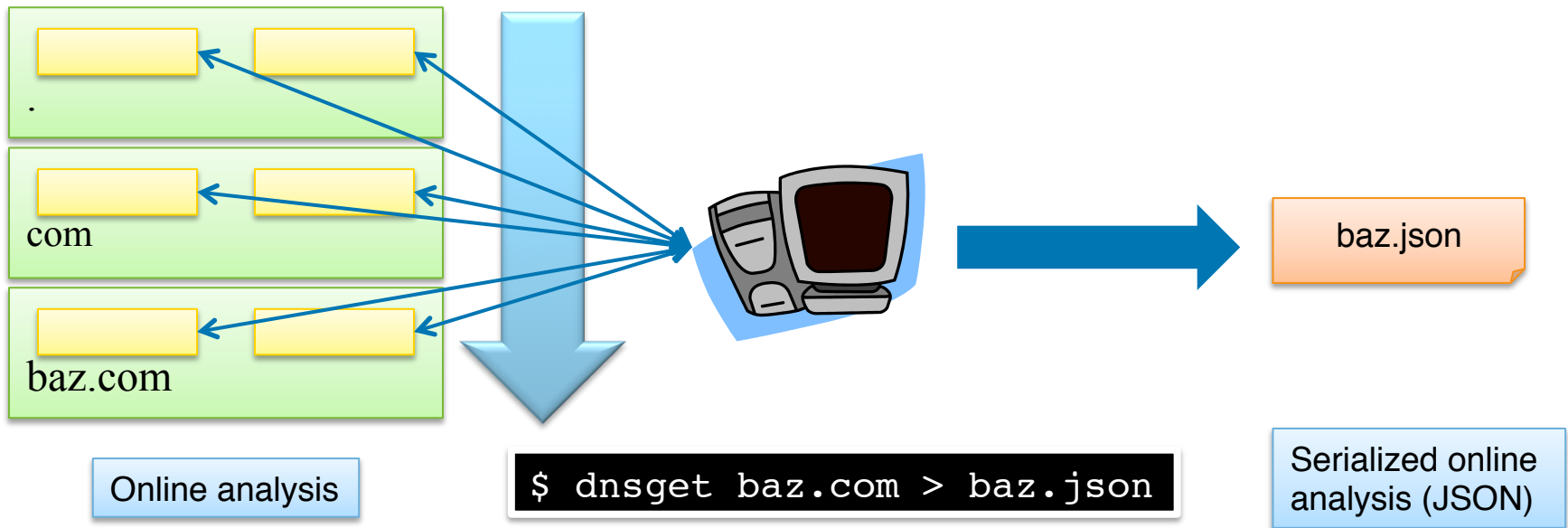
DNSViz History

- **2010** – dnsviz.net launched by Sandia National Labs to help with DNSSEC analysis
- **2011** – archive of DNS monitoring began
- **2013** – database backend rewritten
- **2014/2015** – adopted by Verisign Labs
 - Analysis engine rewritten
 - Decoupled from graph and database
 - Made suitable for local installation/ invocation
 - Hosting migrated to Verisign Labs
 - 0.2.0 release under GPLv2



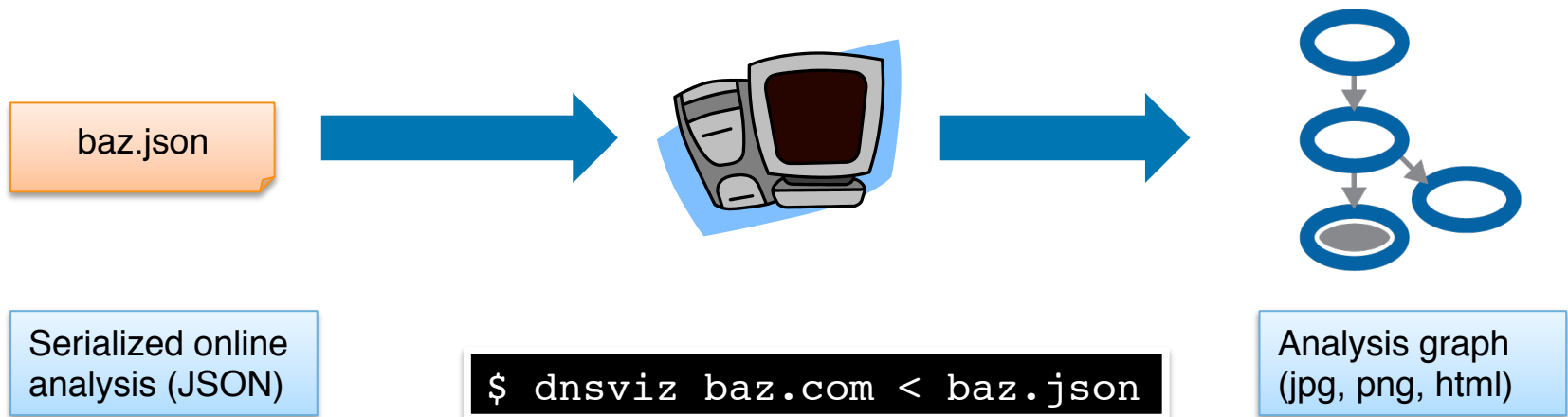
Local DNS Analysis Using DNSViz Command Line

- `dnsget`
 - **Description:** Online analysis (query/response) of DNS name, servers, and dependencies, following referrals
 - **Input:** One or more domain names
 - **Output:** Serialized (JSON) DNS analysis, including query/response diagnostics



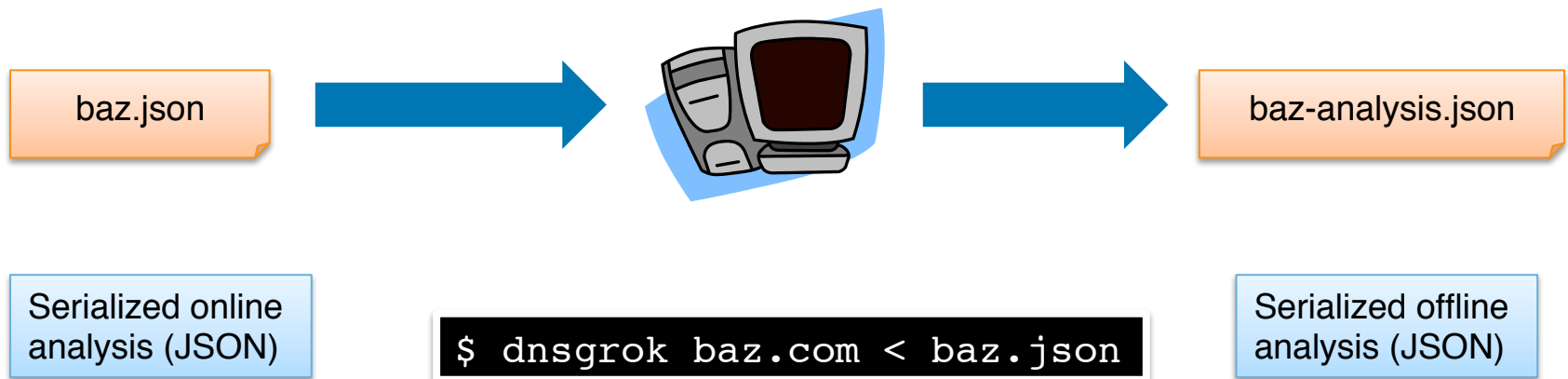
Local DNS Analysis Using DNSViz Command Line

- `dnsviz`
 - **Description:** Offline analysis (correctness/validation/consistency) of DNS name, servers, and dependencies
 - **Input:** One or more domain names and serialized (JSON) analysis (output from `dnsget`)
 - **Output:** Graph of DNS analysis, as an image - png, jpg, html (interactive) format



Local DNS Analysis Using DNSViz Command Line

- **dnsgrok**
 - **Description:** Offline analysis (correctness/validation/consistency) of DNS name, servers, and dependencies
 - **Input:** One or more domain names and serialized (JSON) analysis (output from dnsgrok)
 - **Output:** Serialized (JSON) DNS analysis, including error-level filtering



Features

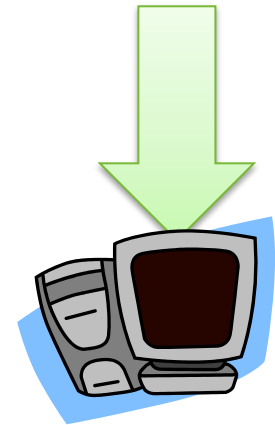
- Automatically detects IPv6 connectivity for related tests
- Works on arbitrary names – not just zones
- Follows CNAME dependencies
- Checks negative responses – both of names and zones
 - NXDOMAIN
 - No data
 - NSEC/NSEC3
- Other
 - DNAME
 - Wildcard

Features

- Stub/full analysis
 - **Default:** Analyze just the name itself (stub)
 - **Optional:** Analyze to the height of any ancestor, including root (full)
- Explicit delegation
 - **Default:** Infer name servers from delegation from IANA root
 - **Optional:** Specify arbitrary name servers for a domain
 - (This also allows for analysis with an alternate (non-IANA) root)
- DLV
 - **Default:** No DLV
 - **Optional:** Specify a DLV server (e.g., dlv.isc.org)
 - (Yes, there is still quite a presence of DLV users out there)
- Multiple names analyzed serially or in parallel (work-in-progress)

0.2.0 Release – download and install

- Dependencies
 - dnspython \geq 1.12
 - pygraphviz \geq 1.1
 - M2Crypto \geq 0.21.0 (patches for DSA, ECDSA, GOST)
- Download location
 - <https://github.com/dnsviz/dnsviz>
- Install
 - Commands:
 - `python setup.py build`
 - `sudo python setup.py install`
 - Location:
 - Supporting python modules: PREFIX/lib/python\$VER/
 - Scripts: PREFIX/bin
- License: GPLv2



Example – verisignlabs.com

```
$ dnsget verisignlabs.com > v.json
```

```
Analyzing com (stub)
```

```
Analyzing verisignlabs.com
```

```
$ dnsgrok -l error verisignlabs.com < v.json
```

```
$ dnsgrok -l info verisignlabs.com < v.json
```

```
{
```

```
  "verisignlabs.com.": {
```

```
    "status": "NOERROR",
```

```
    "answer": {
```

```
      "verisignlabs.com./IN/A": [
```

```
        {
```

```
          "description": "RRset for verisignlabs.com./A",
```

```
          "rrsig": [
```

```
            {
```

```
              "description": "RRSIG covering
```

```
verisignlabs.com./A",
```

```
              "status": "VALID"
```

```
            }
```

```
          ]
```

```
        }
```

```
      ],
```

```
...
```



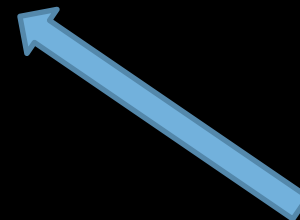
Online analysis



Offline analysis



Name status



RRSIG status

Example – verisignlabs.com

```
...  
  "nxdomain": {  
    "c1vw9md205.verisignlabs.com./IN/A": {  
      "proof": [  
        {  
          "description": "NSEC3 record(s) proving the  
non-existence (NXDOMAIN) of c1vw9md205.verisignlabs.com.",  
          "nsec3": [  
            {  
              "description": "RRset for  
1p82sf5a4tdaeigps7d10gvp3lunl6io.verisignlabs.com./NSEC3",  
              "rrsig": [  
                {  
                  "description": "RRSIG covering  
1p82sf5a4tdaeigps7d10gvp3lunl6io.verisignlabs.com./NSEC3",  
                  "status": "VALID"  
                }  
              ]  
            }  
          ]  
        },  
      ]  
    },  
  },
```

NXDOMAIN/
NSEC3 status

NSEC3 RRSIG
status

Example – verisignlabs.com

```
...
  "dnskeys": [
    {
      "description": "DNSKEY for verisignlabs.com.
(algorithm 8 (RSA/SHA-256), key tag 63023)"
    },
    {
      "description": "DNSKEY for verisignlabs.com.
(algorithm 8 (RSA/SHA-256), key tag 19773)"
    }
  ],
  "delegation": {
    "ds": [
      {
        "description": "DS record(s) corresponding to
DNSKEY for verisignlabs.com. (algorithm 8 (RSA/SHA-256), key tag
19773)",
        "status": "VALID"
      }
    ],
    "status": "SECURE"
  },
}
```

← DNSKEY status/errors

← DS status/delegation status

DNSViz Library – Lower Level Functionality

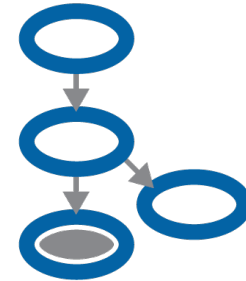
- Query engine
- Query/response handlers
- Subclass-able DNS Query
 - Define flags, types, response handling, etc.

Testing and Feedback

- Help requested!
- Usability Feedback
 - Command line
 - Serialized online analysis schema (`dnsget` output)
 - Offline analysis schema (`dnsgrok` and `dnsviz` output)
 - Error code and description
 - Low-level primitives
- Feature requests
- Bug reports

Future Work

- Regression tests
- Web front-end
 - General design
 - URL schema
- Recursive implementation and testing
- Arbitrary record types queried
- Community help welcome!
- Google Groups mailing list:
<https://groups.google.com/d/forum/dnsviz-users>



powered by



VERISIGN™