Now That The Root is Signed...

Wes Hardaker

SPARTA, Inc.
dba Cobham Analytic Solutions

<wes.hardaker@cobham.com>

30 Second DNSSEC Recap
(fulfilling your pre-requisite requirement)

- . (root) publishes:
  - KSK for root
  - ZSK for root
  - NS, glue records and DS for .org
- .org publishes:
  - KSK for .org
  - ZSK for .org
  - DS for nanog.org

Signs: (generates RRSIG)

Signs: (generates RRSIG)

DS = Cryptographic Hash Of

Signs: (generates RRSIG)

Signs: (generates RRSIG)

...

State of the DNSSEC World

- The root is signed!
  - Many said DNSSEC would never get deployed because the root would never be signed
  - Provides a single Trust-Anchor
- 28 TLDs signed
  - Caveat: not all are “fully operational” yet
  - 7 Generic TLDs (including .org, .biz, and .edu)
  - 7 more “announced plans” (including .com, .net)
- ~ 25k production zones signed
  - On Sept 7, according to http://secspider.cs.ucla.edu/

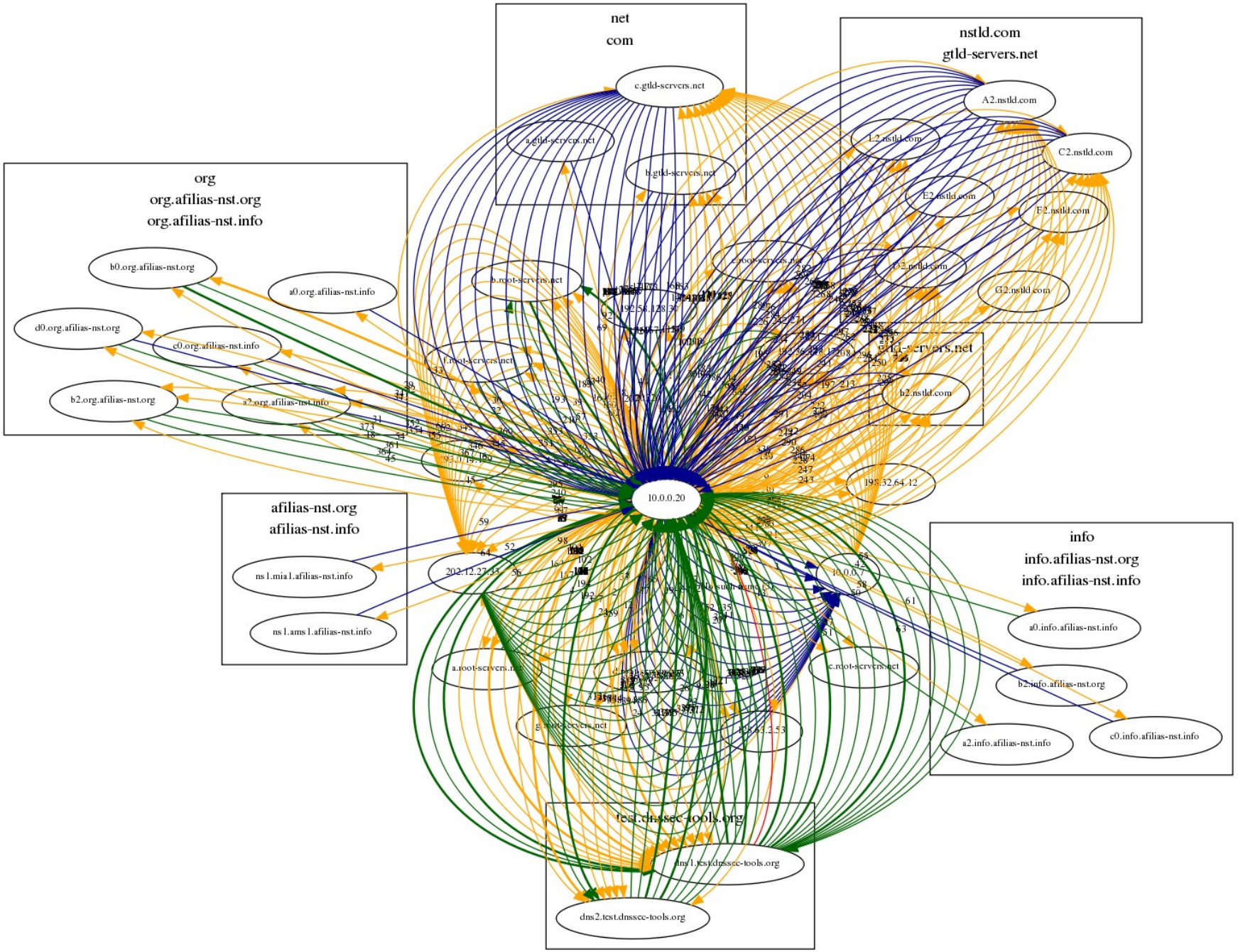
State of the DNSSEC World

- Real world DNSSEC validating resolvers:
  - Top 4 Swedish ISPs
  - US Government
  - COMCAST opt-in
  - UCBerkeley
  - ... You?

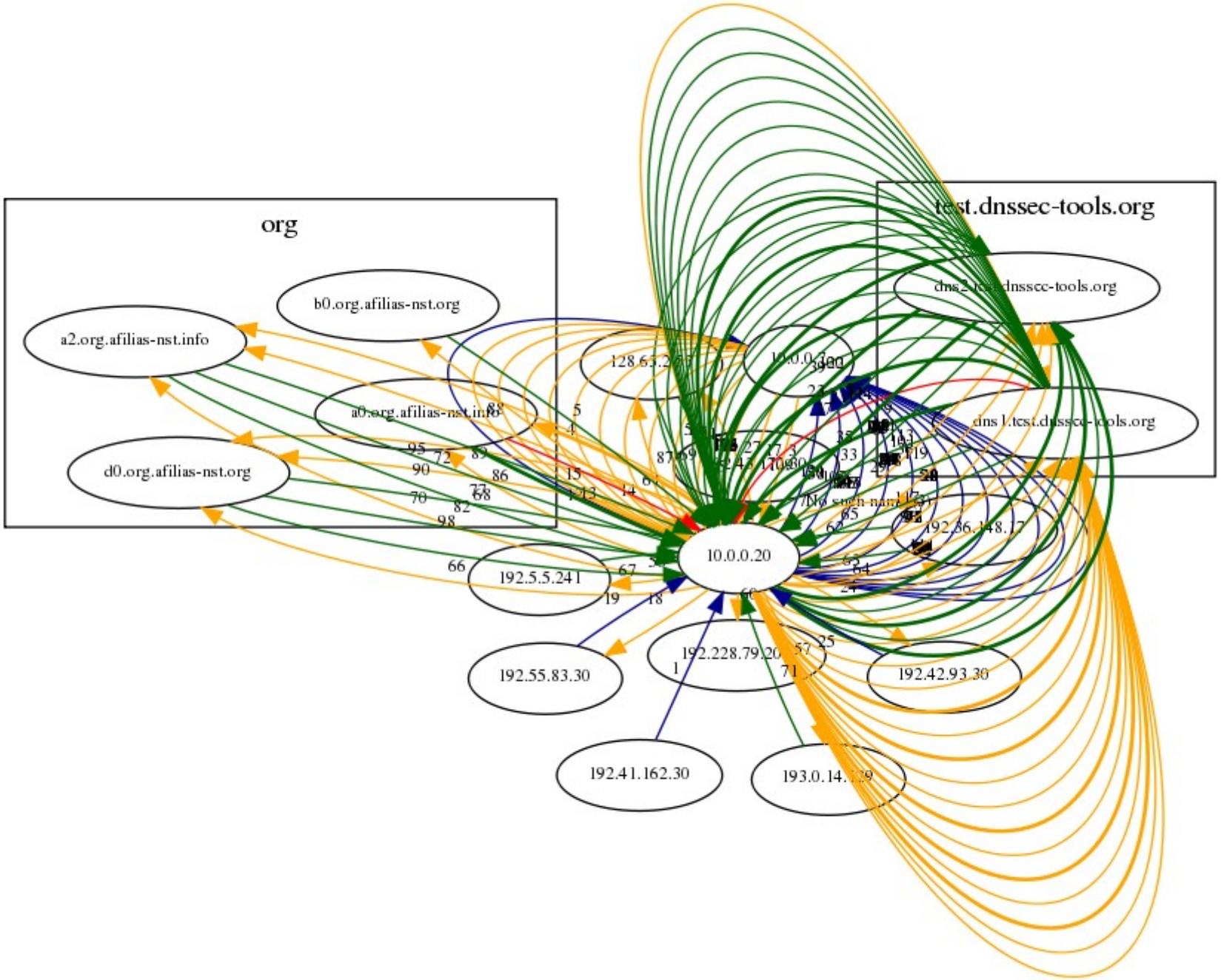
Deployment Pictures

- The following images:
  - Show one line per DNS message sent or received
  - Show the results of a browser loading a webpage
- Are color coded:
  - Orange: Query
  - Blue: Insecure Response
  - Green: Secured Response
  - Red: Truncated (switch to TCP please)

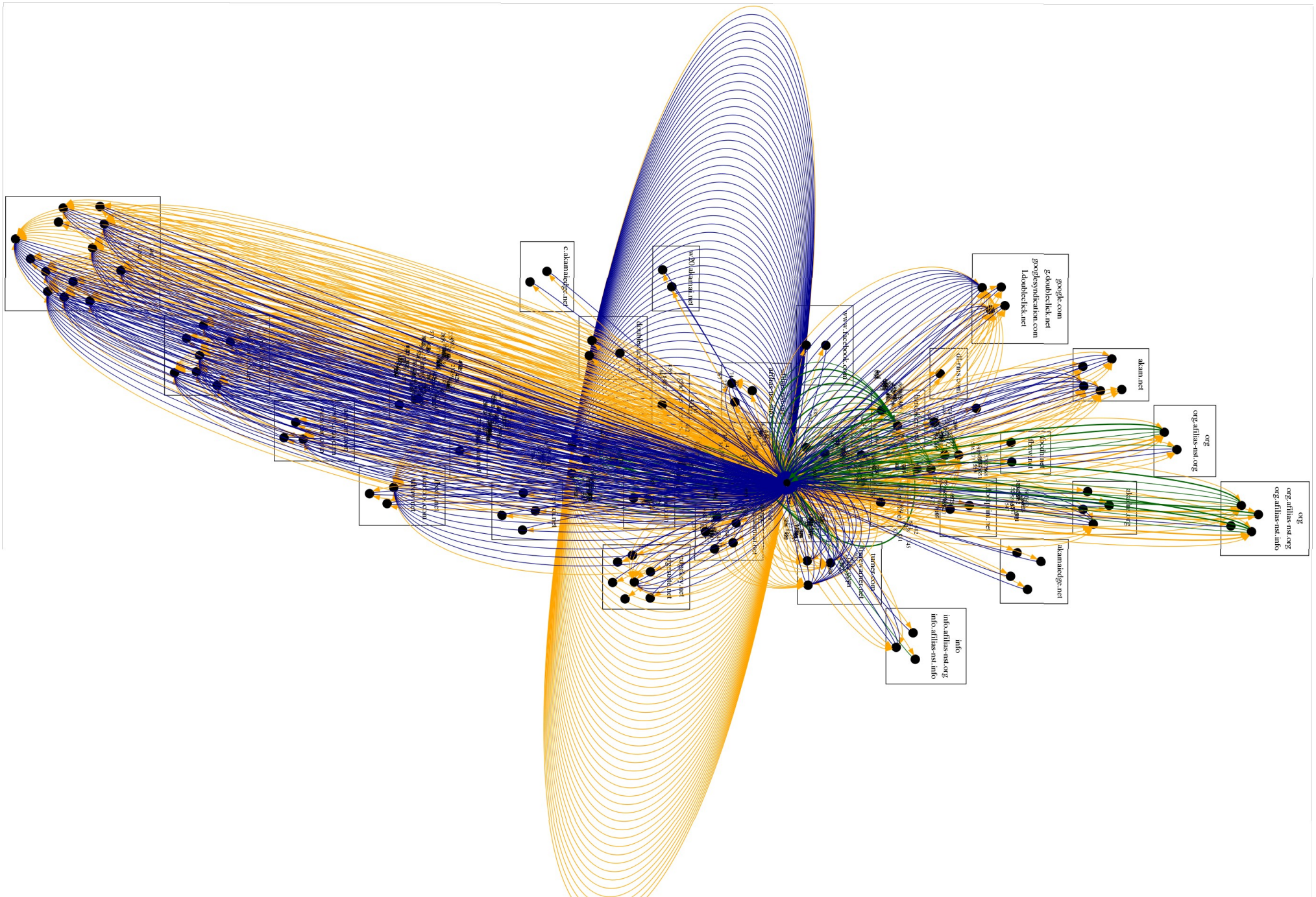
www.dnssec-tools.org



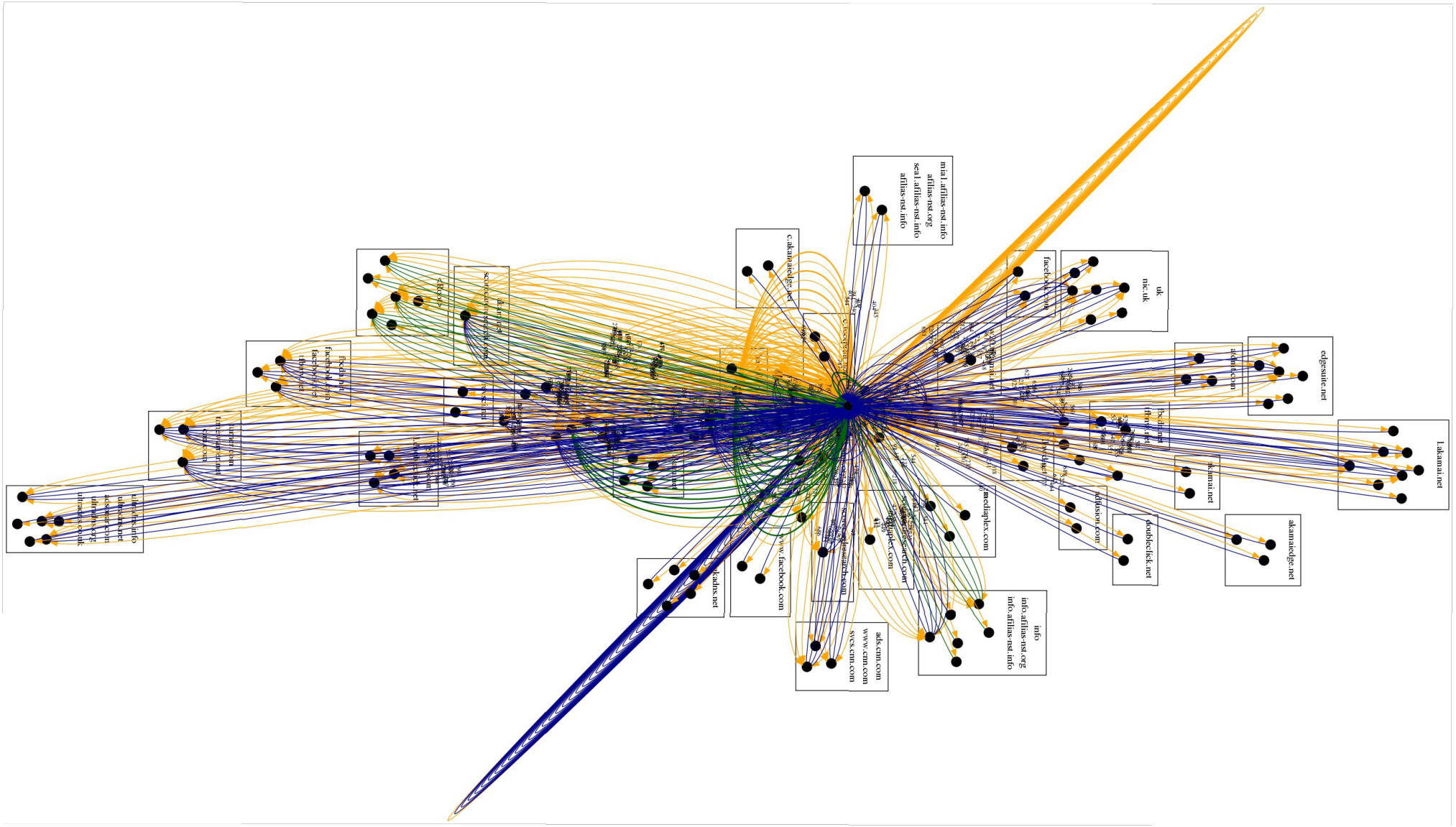
www.dnssec-tools.org w/o priming



www.cnn.com w/ priming



www.cnn.com w/o priming



Yeah... But Now What?

It Depends On Who You Are

- Zone Administrators
  - Sign your zones
  - Coordinate with your parent
- ISPs
  - Turn on validation in your resolvers
- End-Users
  - Use validating applications for improved security

Zone Administrators

Signing Your Zones

- 10 minute “live” lightning talk at NANOG44 (LA)
  - Used DNSSEC-Tools' *zonesigner* to sign a zone
  - `# zonesigner -zone example.com file file.signed`
  - https://www.dnssec-tools.org/wiki/index.php/Sign_Your_Zone
- Publish your DS record upstream
  - Now if possible
  - Later if your parent isn't yet secure
- DS record reminder:
  - Published and signed by your parent
  - Contains a fingerprint of your key

Resolver Operators
Turning on Validation

- Example named.conf settings:

```
trusted-keys {
    . 257 3 8 "AwEAAagAIKlVZrpC6Ia7gEzahOR+9W29euxhJhVVLOyQbSEW0O8gcCjF
        FVQUTf6v58fLjwBd0YI0EzrAcQqBGCzh/RStIoO8g0NfnfL2MTJRkxoX
        bfDaUeVPQuYEhg37NZWAJQ9VnMVDxP/VHL496M/QZxkjf5/Efucp2gaD
        X6RS6CXpoY68LsvPVjR0ZSwzz1apAzvN9dlzEheX7ICJBBtuA6G3LQpz
        W5hOA2hzCTMjJPJ8LbqF6dsV6DoBQzgul0sGIcGOYl7OyQdXfZ57relS
        Qageu+ipAdTTJ25AsRTAoub8ONGcLmqrAmRLKBP1dfwhYB4N7knNnulq
        QxA+Uk1ihz0=";
};
options {
    dnssec-enable yes;
    dnssec-validation yes;
};
```

- (other servers can use the shorter DS record)

Resolver Operators
Things To Think About

- Traffic will increase some
  - Requires fragmented UDP or TCP
- The root trust anchor
  - Configuration files will need to track changes
  - Automated key roll-over tracking mechanisms exist
  - Consider distributing root keys in enterprise config
- When sites are unreachable
  - Know the technology and use tools to debug it
  - Look for and learn to read DNSSEC log messages
  - Avoid disabling DNSSEC to see if it fixes things

Resolver Operators
What the Users See

- Before validation:

```
# dig +short www.dnssec-tools.org
192.94.214.6

# dig +short badsign-a.test.dnssec-tools.org
75.119.216.33
```

- After validation:

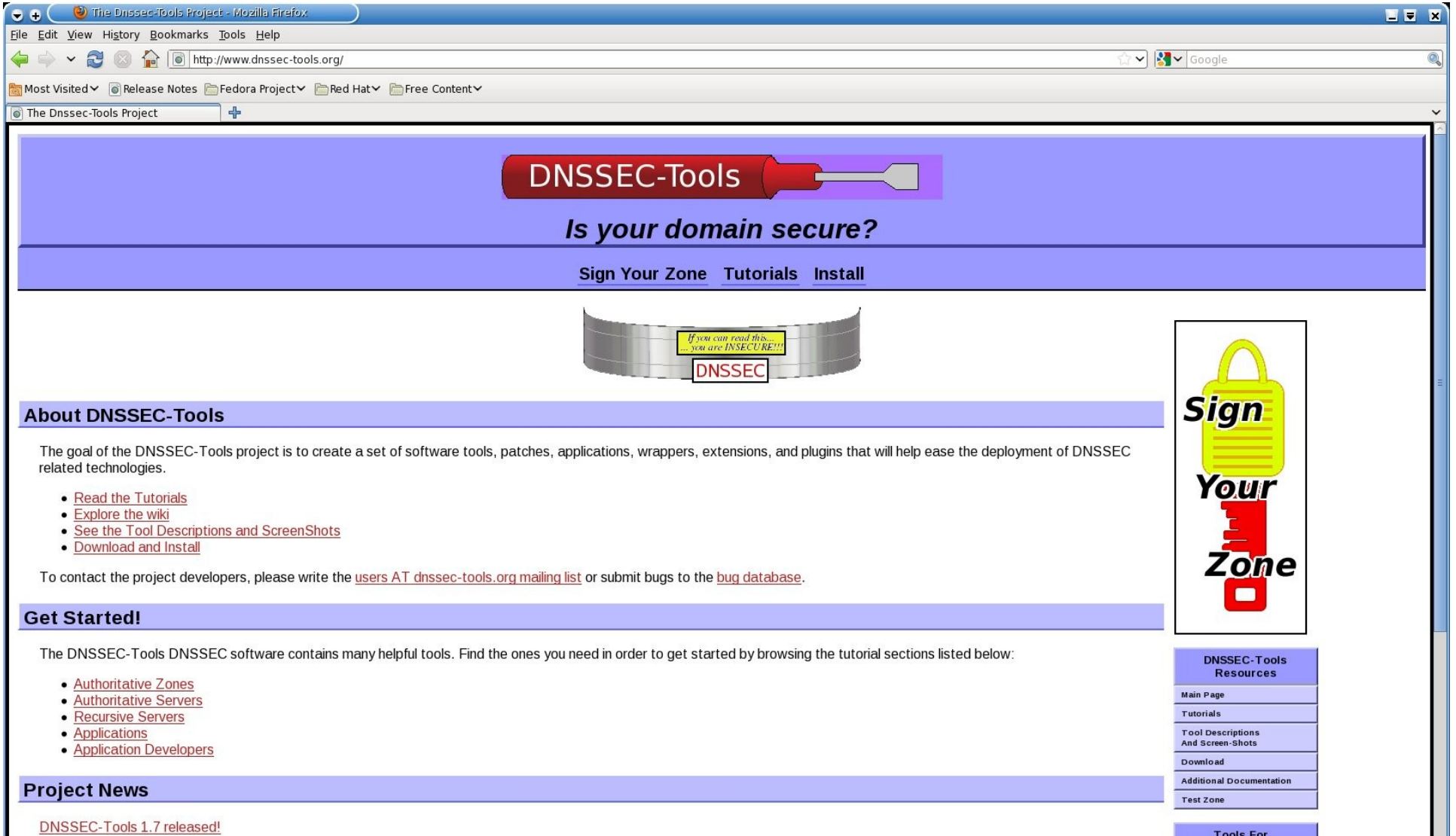
```
# dig +short www.dnssec-tools.org
192.94.214.6

# dig +short badsign-a.test.dnssec-tools.org
#
```

Resolver Operators

What the Users See

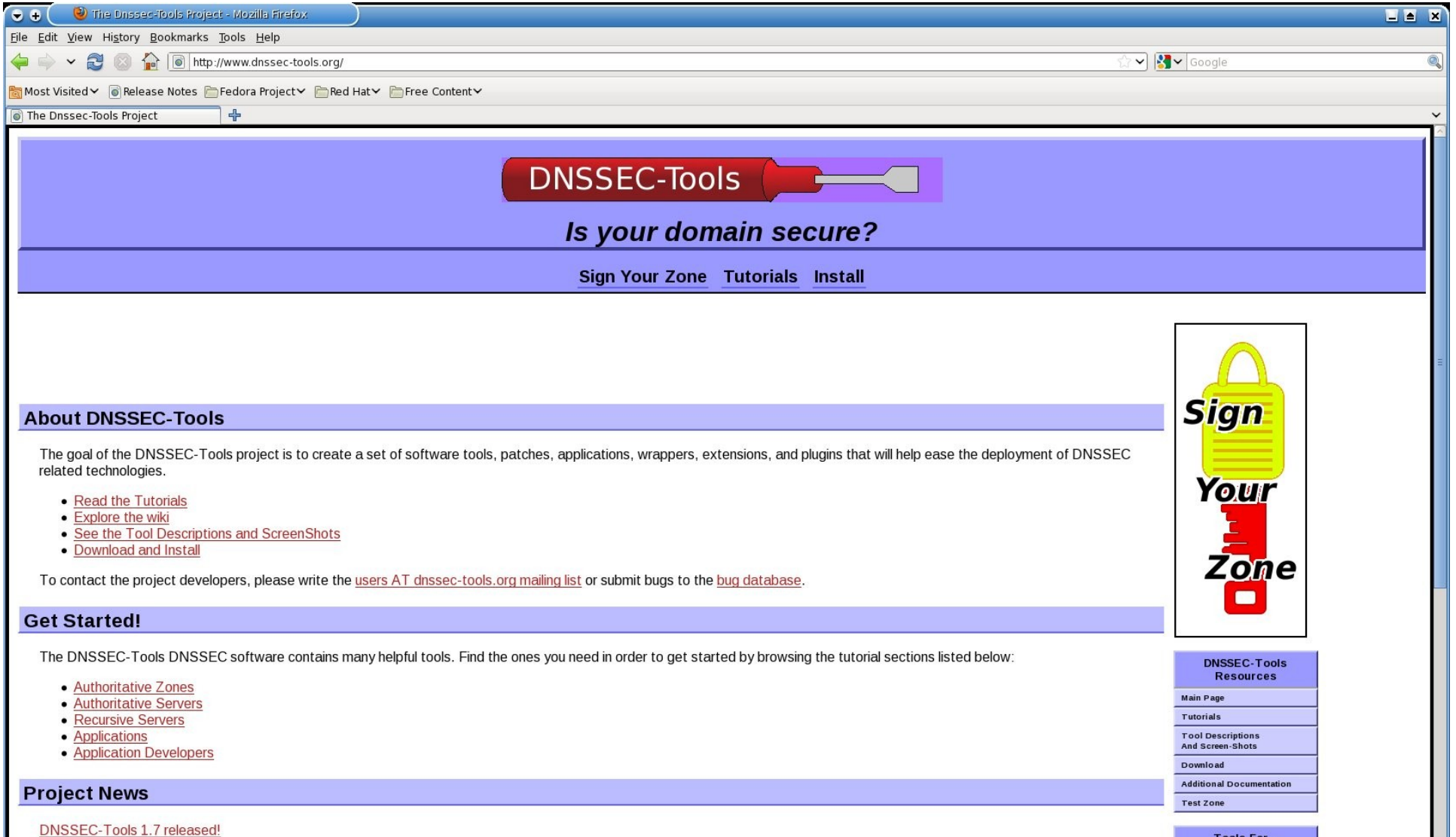
- Before Validation:



Resolver Operators

What the Users See

- After Validation:



Resolver Operators
What the Users See

- After Validation:
  - They simply don't get answers for insecure lookups
- Be it:
  - Web pages, images, javascript
  - IMAP Servers
  - The *Duke Nukem Forever* download site
- IE, whatever the client asks for
  - They get the correct answer or nothing
- But that's just the beginning...

What the Users <u>WILL</u> see

- Coming soon:
  - in-application validation
- Then things get really interesting:
  - Secure Cryptographic lookups — SSH Fingerprints, TLS Fingerprints
  - Direct to HTTPS hints
  - Verified “Server Does Not Exist” messages
  - Secured MX, SPF and DKIM lookups
  - Secured RBLs
  - Reverse lookups for location restricted content
  - *Brain storm here!*

Where Are Your Users?

AKA “the last mile problem”

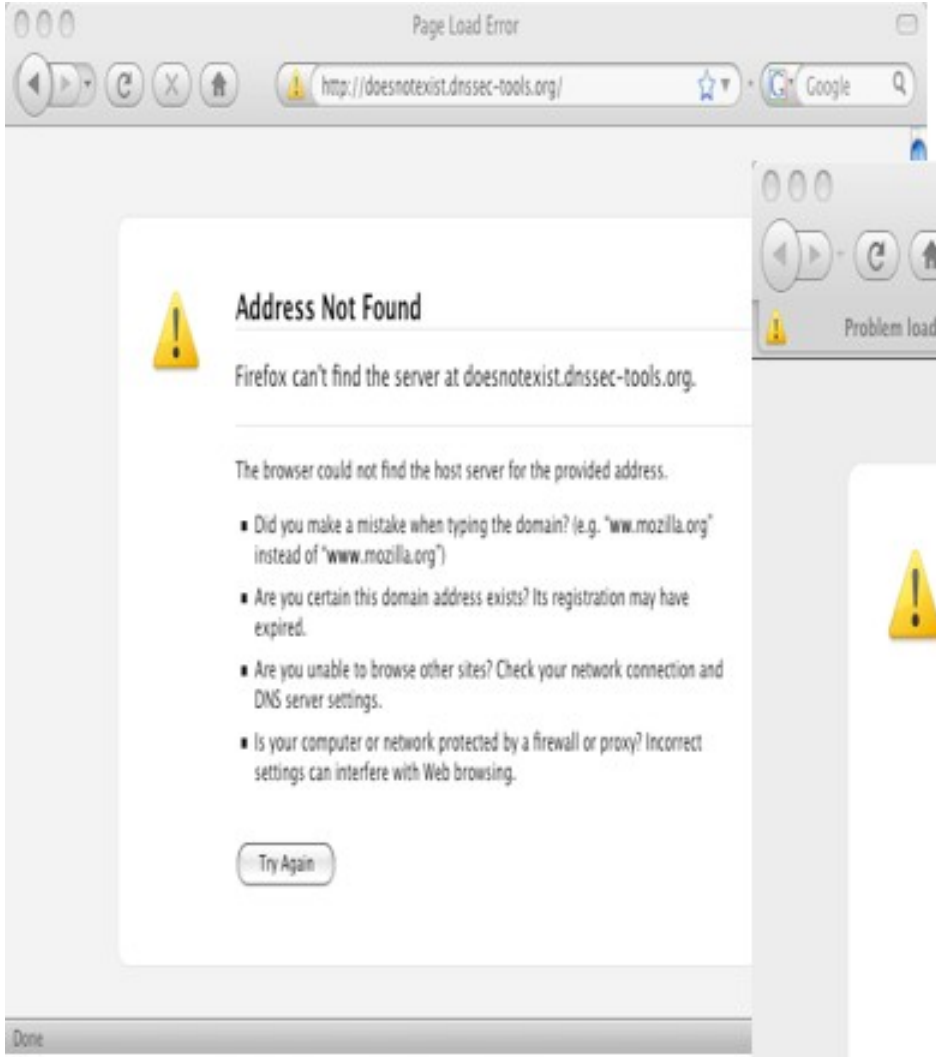
- At work:
  - Generally safe behind your secured resolver
- Until they:
  - Go home
  - Go to a coffee shop
  - Check email via their phone
  - Go to a convention without a secured resolver
    - **Cough** *NANOG* **Cough**
- Thus, the best long-term solution:
  - Validate at the end-host or end-application

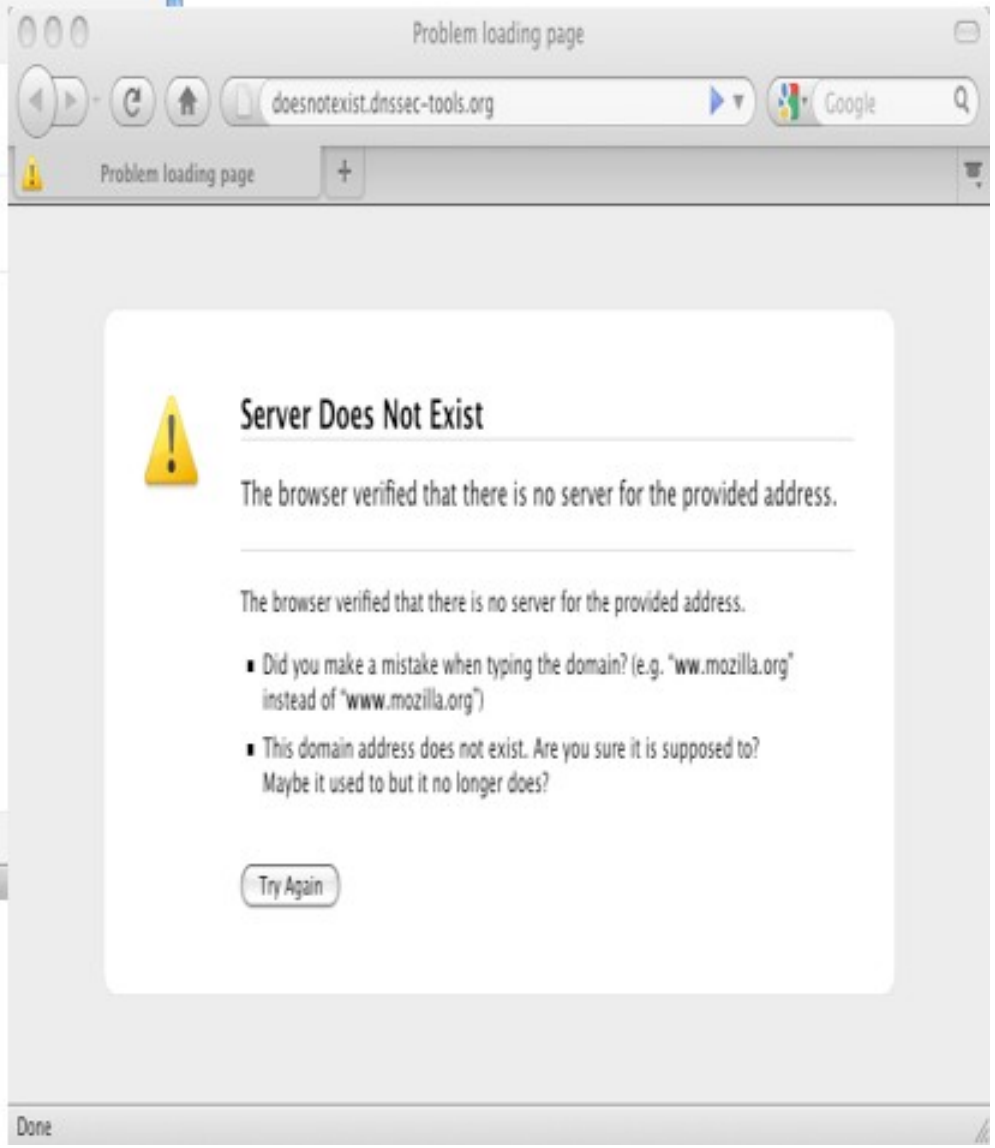
Resolver vs Application Validation

- Near by validating resolvers:
  - Refuse to relay bad/insecure answers
  - Can still be spoofed locally
  - Provide no validation results to the end-application

- End-application validation:
  - Provides security all the way to the application
    - Important for key (auto)-acceptance
  - Provides useful error codes
    - This domain doesn't exist. **At all!**

The Positive Negative





The (readable) Positive Negative

Unsecured

Address Not Found

- Did you make a mistake while typing?
- Are you certain the domain address exists?
- Are you able to browse other sites?
- Is your computer or network protected by a firewall?

Secured

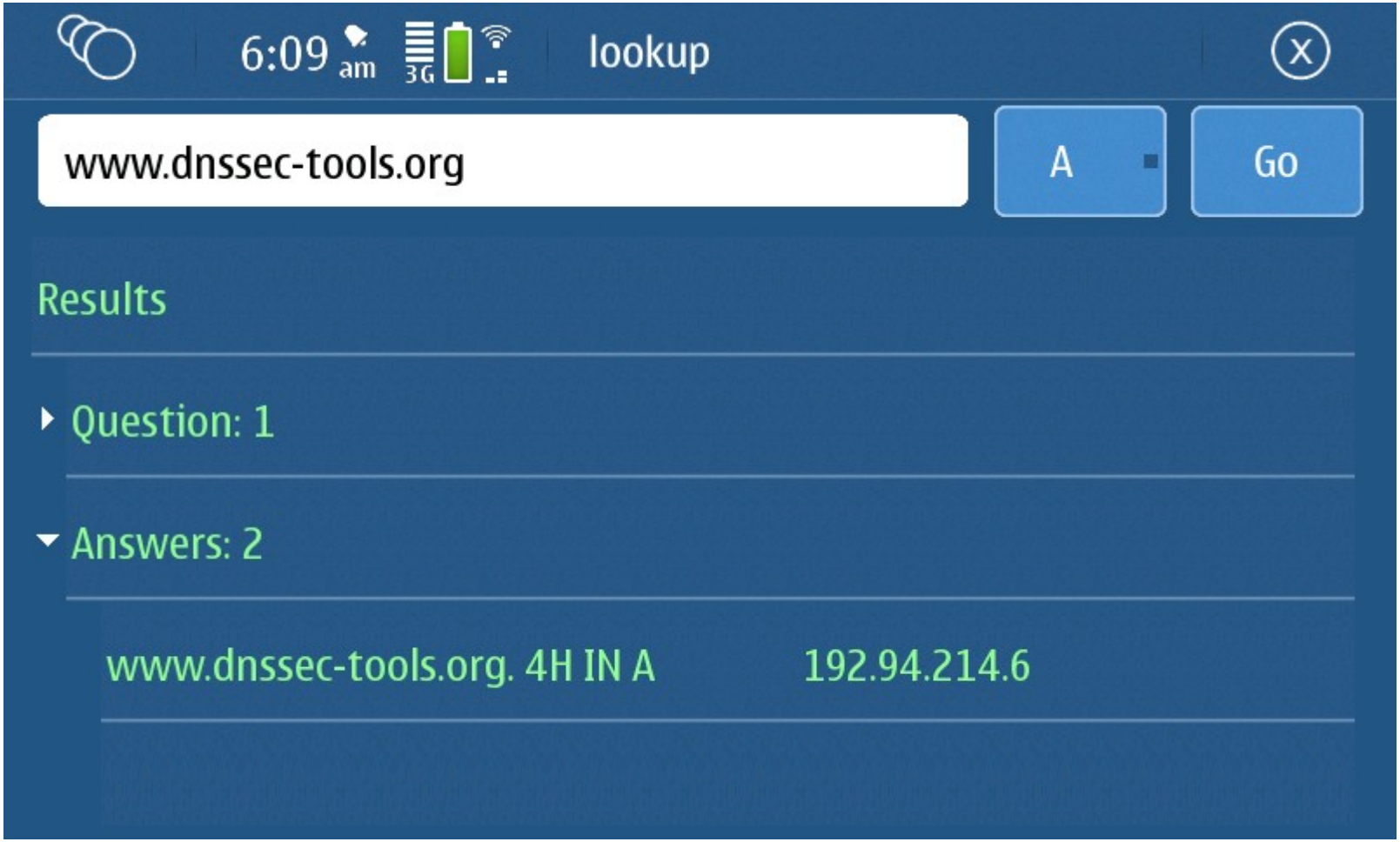
Server Does Not Exist

- Did you make a mistake typing?
- The domain address **does not exist**.

Application Demonstrations
(now or later: catch me in the hallway!)

- DNSSEC Enabled Applications
  - Firefox
  - OpenSSH
  - ThunderBird, sendmail, postfix, libspf
  - Wget, ncftp
- Zone maintance tools
  - zonesigner, rollerd, donuts, lsdnssec
- Debugging Tools
  - dnspktflow, donuts, convertar, getds, logwatch
- Validating library and perl modules

Application Screenshot
(on my phone!)



N900 Users: it's “lookup” in extras-testing

For Application Developers

- Validating resolving libraries
  - DNSSEC-Tools: “libval”
    - Designed to easily turn on DNSSEC in existing apps
    - Contains both an “easy” API and a “full details” API
  - Unbound
- Things to think about
  - Some code poorly written and don't accommodate new DNS error conditions
  - Don't fall into “DNSSEC failed, continue? Yes/No”
    - (we've beaten that dead dancing-bear enough)

DNSSEC Resources

- http://www.dnssec-deployment.org/
  - A blog entirely devoted to news about DNSSEC
- http://www.dnssec-tools.org/
  - Our tool suite, shown in these slides and demos
  - (But use any tool set that works best for you)
- https://www.iana.org/dnssec
  - Where to get the root keys
- http://www.dnssec.net/
  - Significant information repository about DNSSEC

Conclusions

- The root is signed!
- The time is right to:
  - Sign your zones
  - Turn on validation to protect your users
  - Make use of DNSSEC secured content

- Turn it on!