

# Now That The Root is Signed...

Wes Hardaker

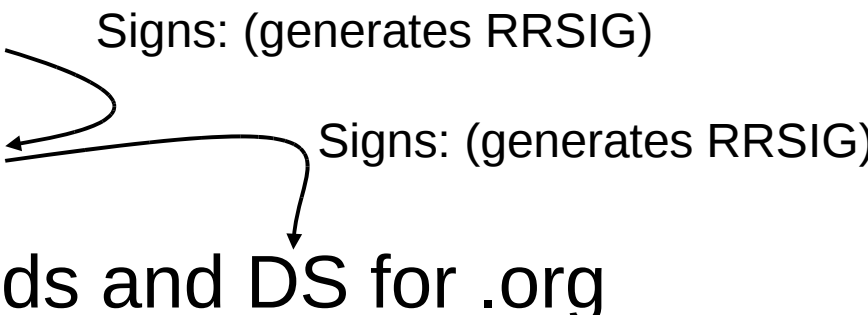
SPARTA, Inc.  
dba Cobham Analytic Solutions

<wes.hardaker@cobham.com>

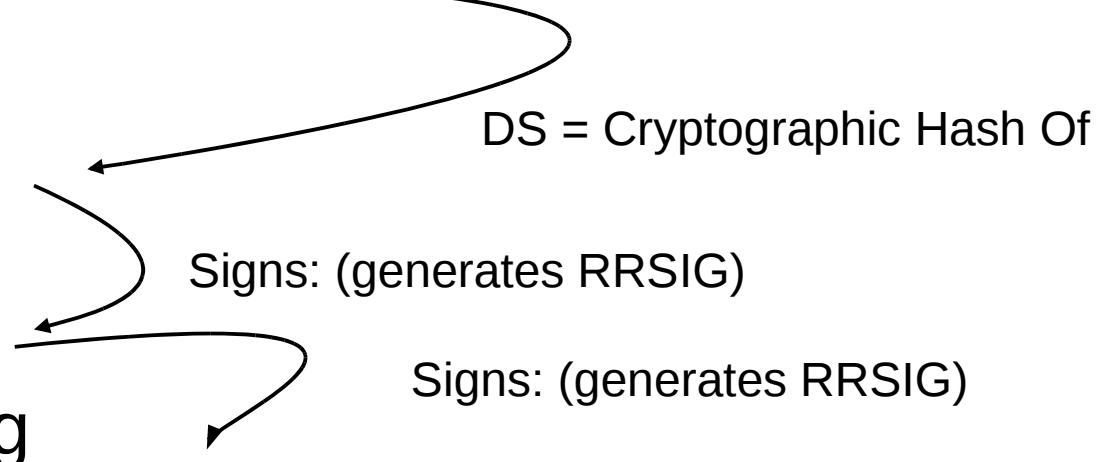
# 30 Second DNSSEC Recap

(fulfilling your pre-requisite requirement)

- . (root) publishes:

- KSK for root
  - ZSK for root
  - NS, glue records and DS for .org
- 
- Signs: (generates RRSIG)
- Signs: (generates RRSIG)

- .org publishes:

- KSK for .org
  - ZSK for .org
  - DS for nanog.org
- 
- 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/>

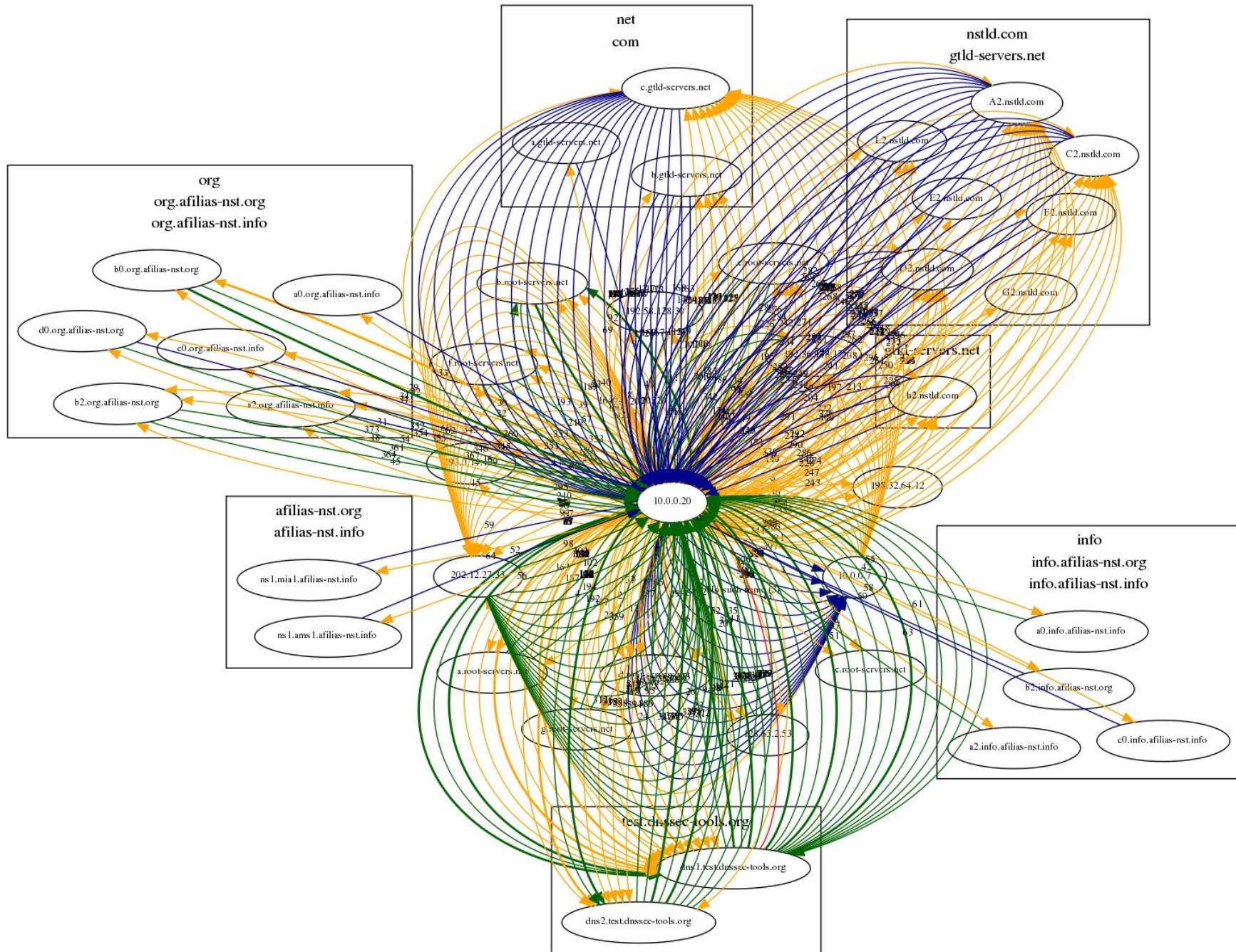
# State of the DNSSEC World

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

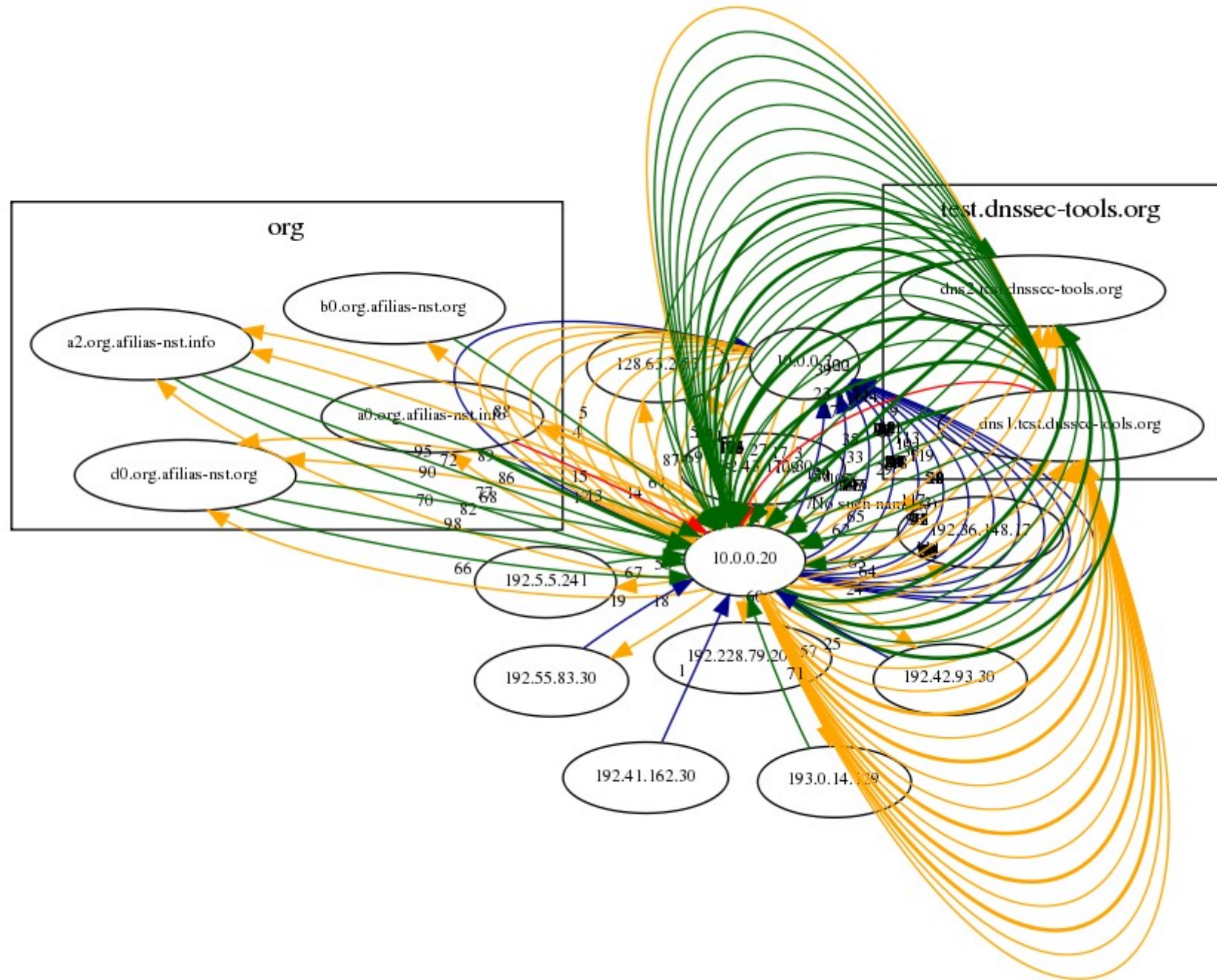
# Deployment Pictures

- 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)

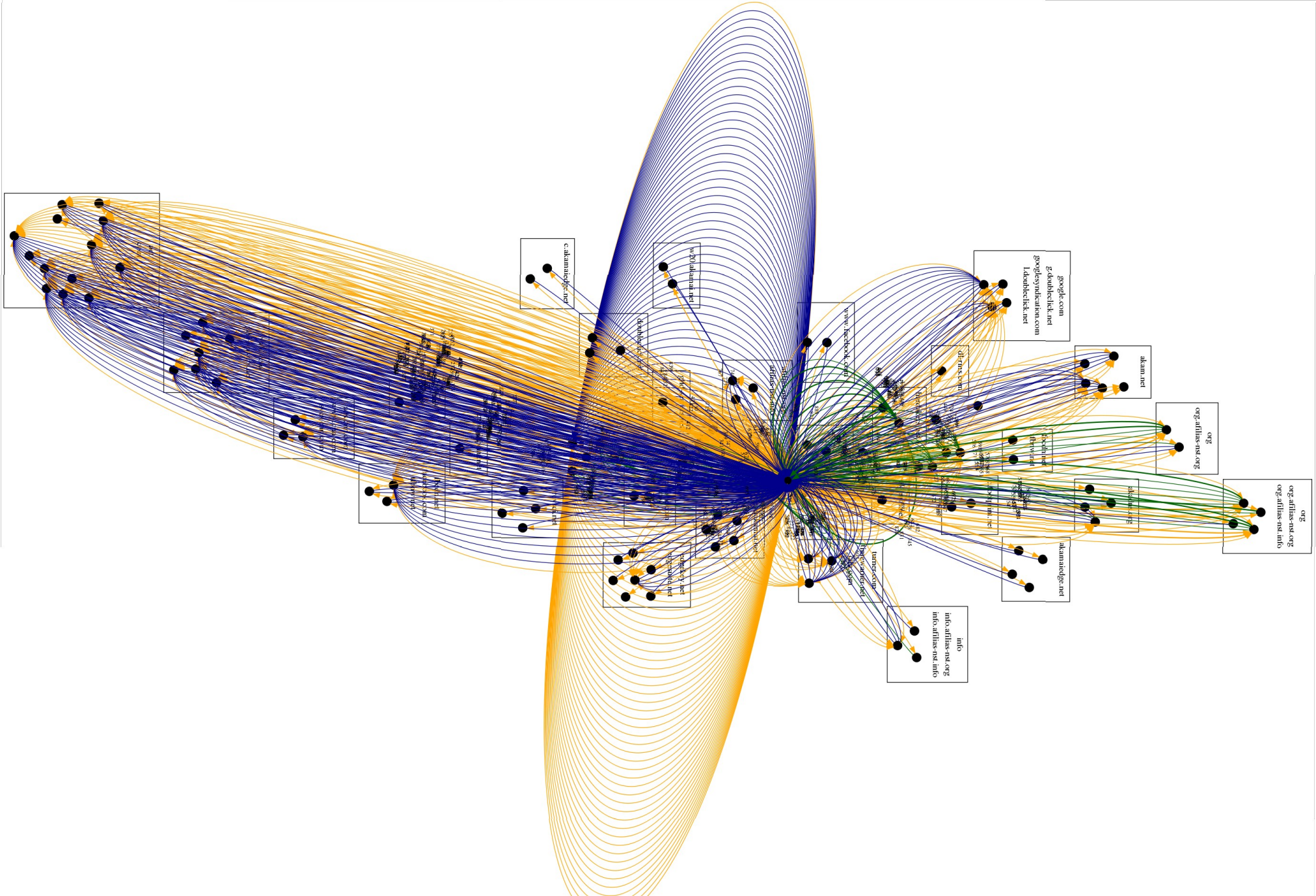
# www.dnssec-tools.org



# www.dnssec-tools.org w/o priming



# www.cnn.com w/ priming







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](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 "AwEAAagAIKlVZrpC6Ia7gEzah0R+9W29euxhJhVVL0yQbSEW008gcCjF
        FVQUTf6v58fLjwBd0YI0EzrAcQqBGCzh/RStIo08g0NfnfL2MTJRkxoX
        bfDaUeVPQuYEHg37NZWAJQ9VnMVDxP/VHL496M/QZxkjf5/Efucp2gaD
        X6RS6CXpoY68LsvPVjR0ZSwzz1apAzvN9dlzEheX7ICJBBtuA6G3LQpz
        W5h0A2hzCTMjJPJ8LbqF6dsV6DoBQzgu10sGIcG0Y170yQdXfZ57re1S
        Qageu+ipAdTTJ25AsRTAoub80NGcLmqrAmRLKBP1dfwhYB4N7knNnulq
        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:

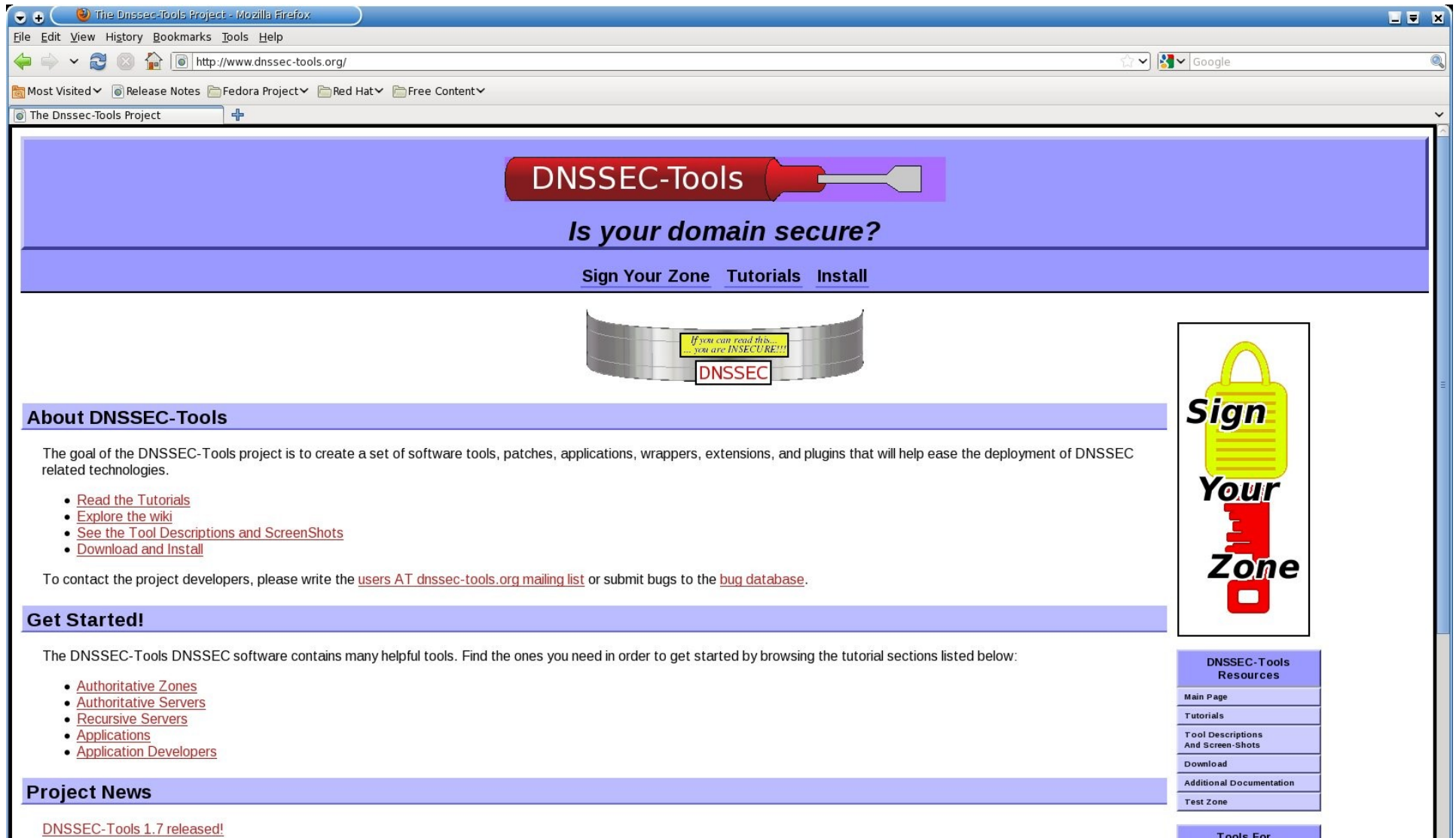
```
# dig +short www.dnssec-tools.org  
192.94.214.6
```

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

# Resolver Operators

## What the Users See

- Before Validation:



The screenshot shows a Mozilla Firefox browser window displaying the website <http://www.dnssec-tools.org/>. The browser's address bar shows the URL, and the page title is "The Dnssec-Tools Project". The website has a blue header with the text "DNSSEC-Tools" and a red screwdriver icon. Below the header, it asks "Is your domain secure?" and provides links for "Sign Your Zone", "Tutorials", and "Install".

The main content area features a central graphic of a silver metal band with a yellow label that reads "If you can read this... you are INSECURE!!!" and a red box labeled "DNSSEC". To the right of this graphic is a vertical banner with a yellow padlock icon and the text "Sign Your Zone".

The website is organized into several sections:

- About DNSSEC-Tools**: A section with a blue header containing a paragraph about the project's goal and a list of links: "Read the Tutorials", "Explore the wiki", "See the Tool Descriptions and ScreenShots", and "Download and Install".
- Get Started!**: A section with a blue header containing a paragraph about the software's helpful tools and a list of links: "Authoritative Zones", "Authoritative Servers", "Recursive Servers", "Applications", and "Application Developers".
- Project News**: A section with a blue header containing a link: "DNSSEC-Tools 1.7 released!".

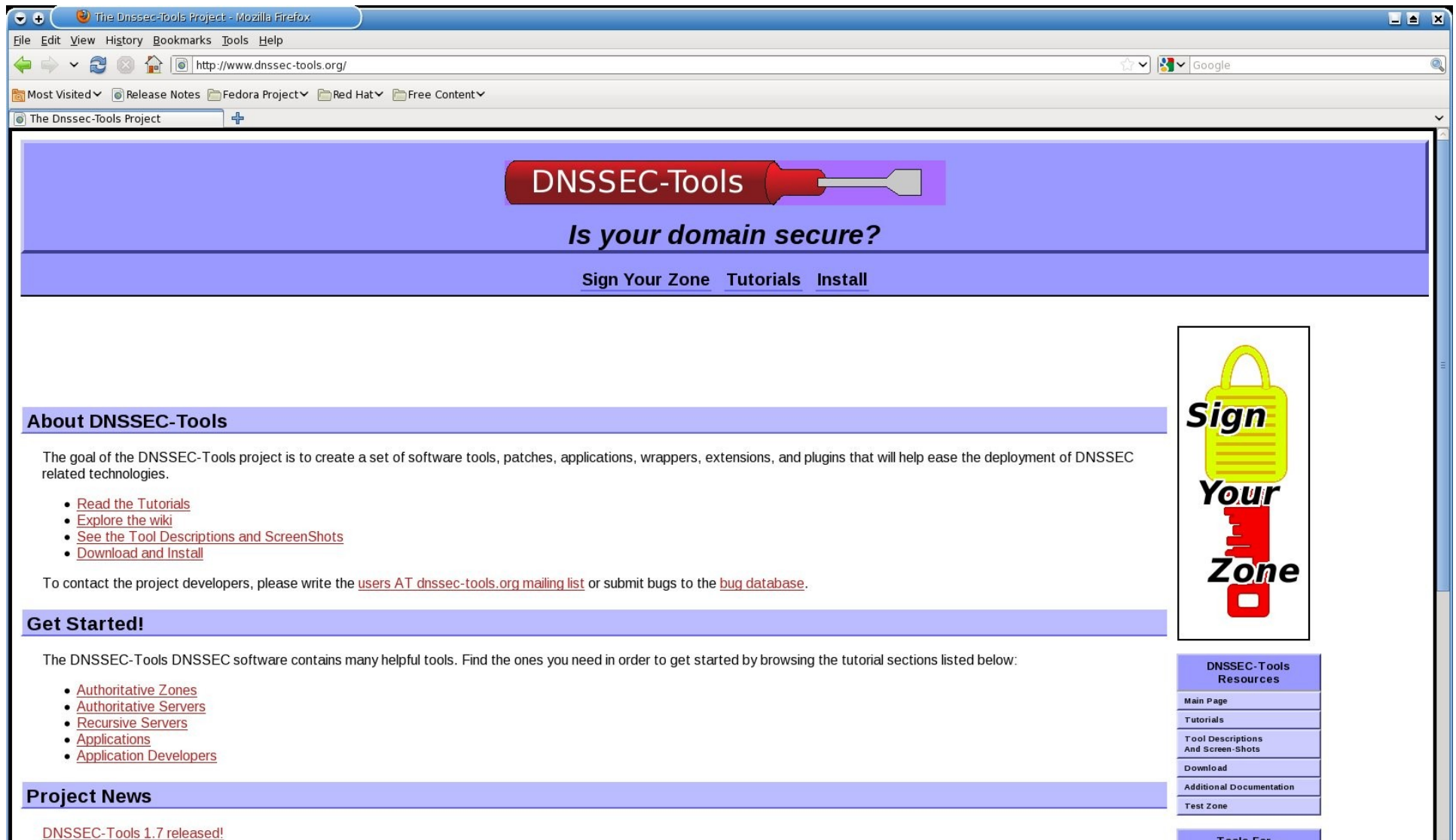
On the right side of the page, there is a sidebar with a blue header "DNSSEC-Tools Resources" and a list of links: "Main Page", "Tutorials", "Tool Descriptions And Screen-Shots", "Download", "Additional Documentation", and "Test Zone".



# Resolver Operators

## What the Users See

- After Validation:



The screenshot shows a Mozilla Firefox browser window displaying the website <http://www.dnssec-tools.org/>. The browser's address bar shows the URL, and the page title is "The Dnssec-Tools Project - Mozilla Firefox". The website's main header features a red wrench icon with the text "DNSSEC-Tools" and the question "Is your domain secure?". Below this, there are links for "Sign Your Zone", "Tutorials", and "Install".

The main content area is divided into several sections:

- About DNSSEC-Tools**: A section with a blue header. The text states: "The goal of the DNSSEC-Tools project is to create a set of software tools, patches, applications, wrappers, extensions, and plugins that will help ease the deployment of DNSSEC related technologies." Below this is a list of links: [Read the Tutorials](#), [Explore the wiki](#), [See the Tool Descriptions and ScreenShots](#), and [Download and Install](#). A note at the bottom of this section says: "To contact the project developers, please write the [users AT dnssec-tools.org mailing list](mailto:users@dnssec-tools.org) or submit bugs to the [bug database](#)."
- Get Started!**: A section with a blue header. The text says: "The DNSSEC-Tools DNSSEC software contains many helpful tools. Find the ones you need in order to get started by browsing the tutorial sections listed below:" followed by a list of links: [Authoritative Zones](#), [Authoritative Servers](#), [Recursive Servers](#), [Applications](#), and [Application Developers](#).
- Project News**: A section with a blue header. The text says: "DNSSEC-Tools 1.7 released!"

On the right side of the page, there is a vertical banner with a yellow padlock icon and the text "Sign Your Zone". Below this banner is a sidebar titled "DNSSEC-Tools Resources" with a list of links: [Main Page](#), [Tutorials](#), [Tool Descriptions And Screen-Shots](#), [Download](#), [Additional Documentation](#), and [Test Zone](#).

# 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 WILL 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?

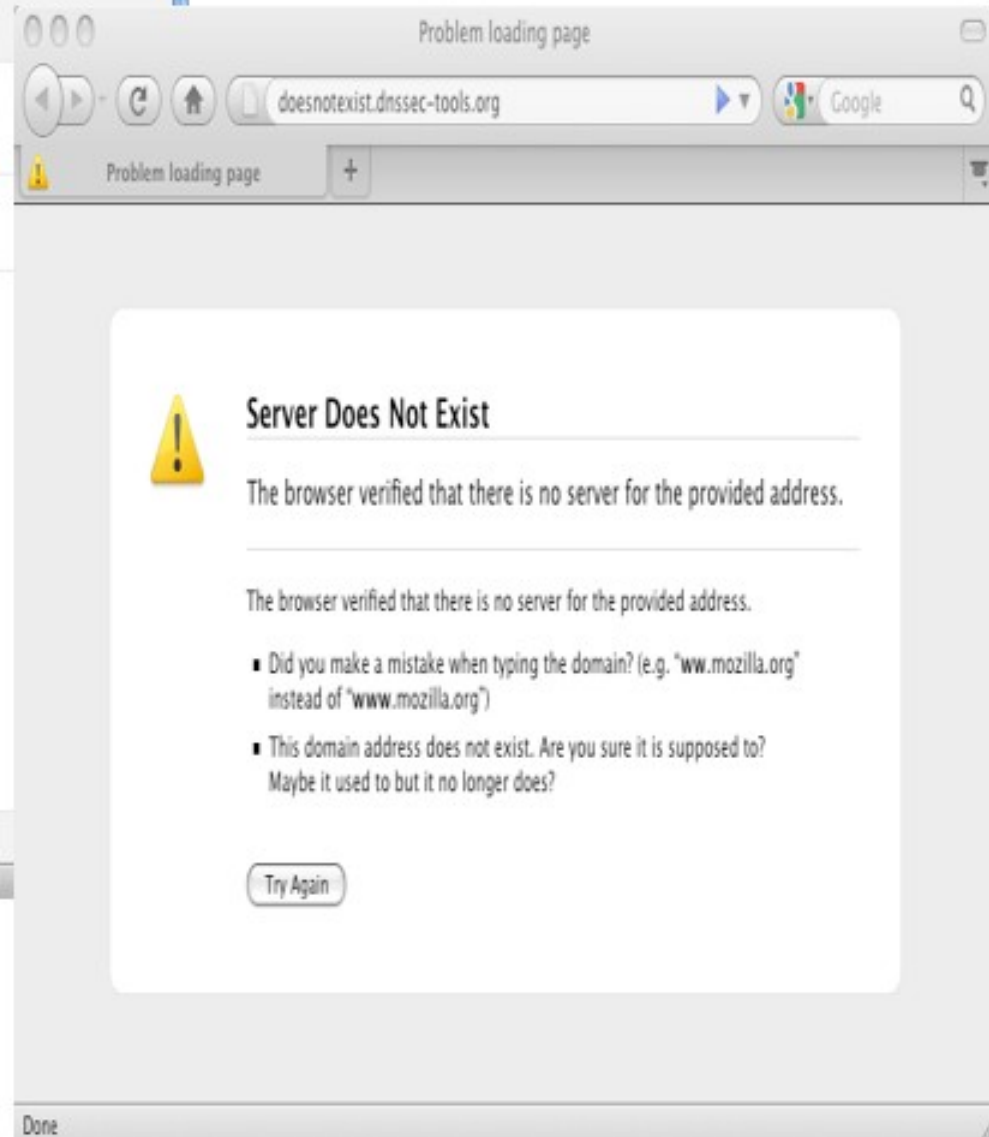
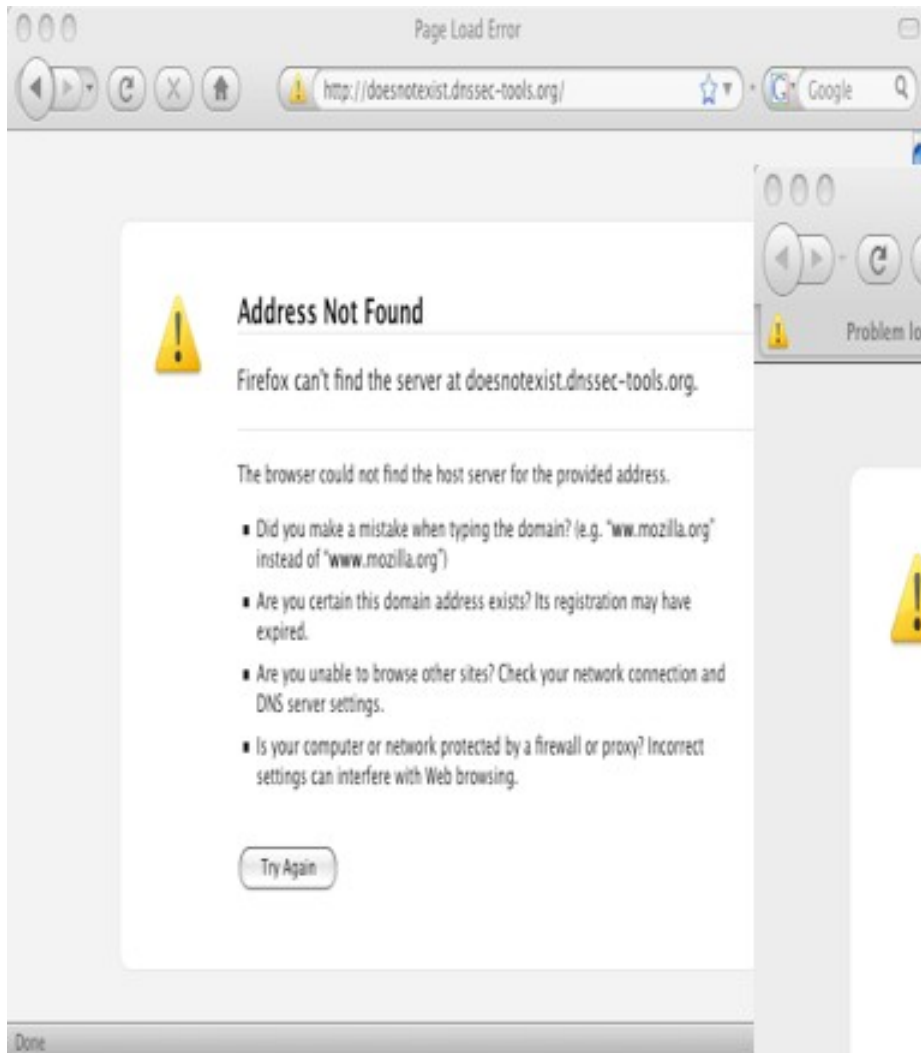
## AKA “the last mile problem”

- 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.**

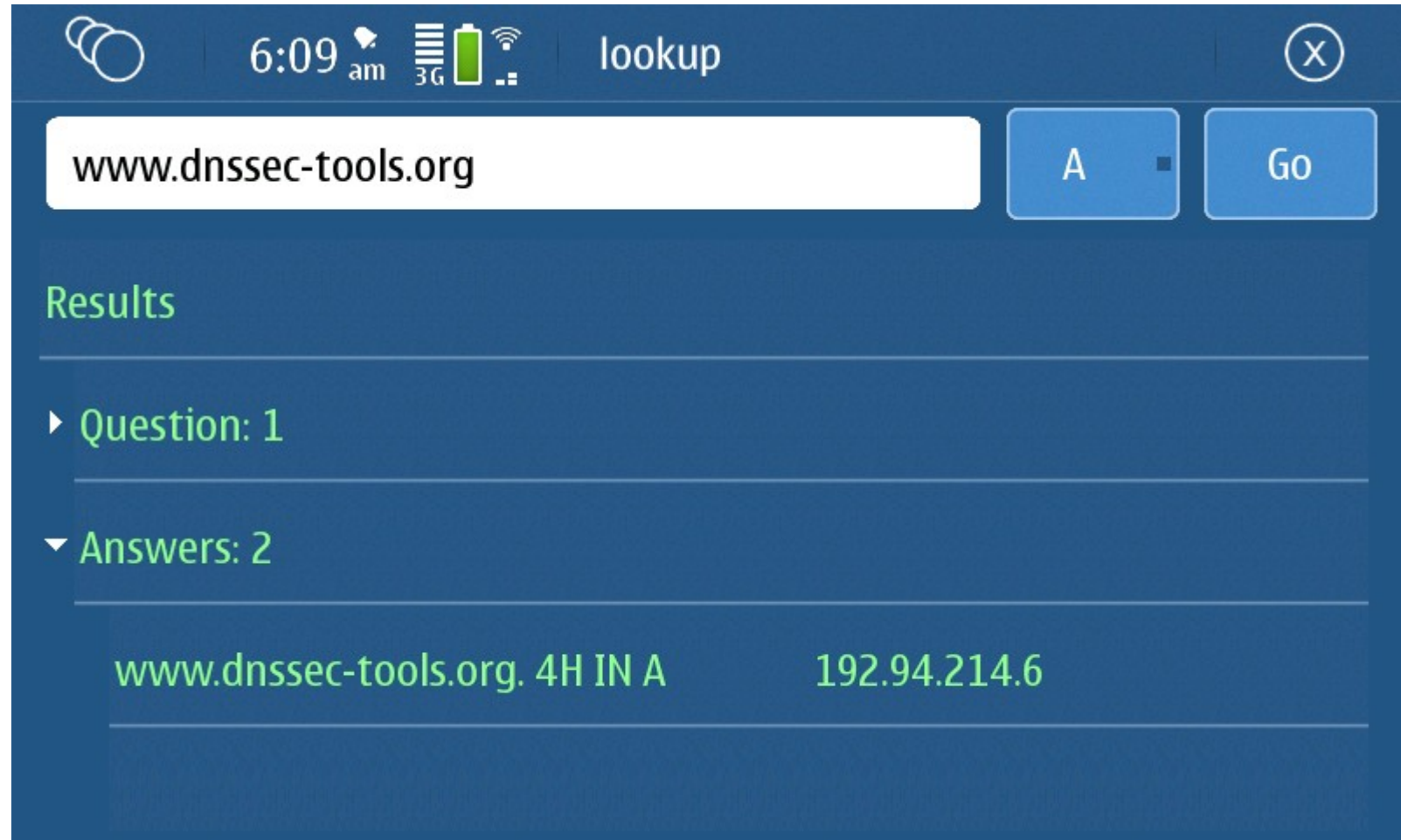
# Application Demonstrations

(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, Isdnssec
- 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!