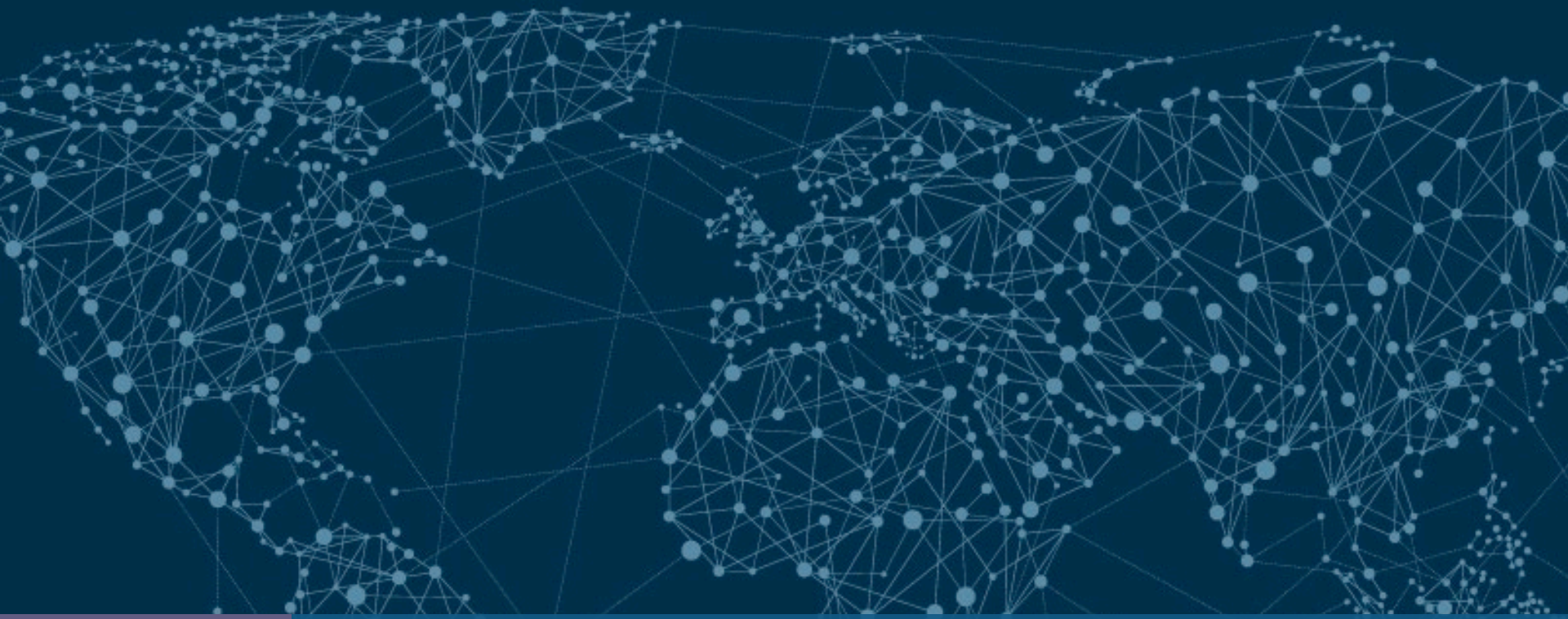
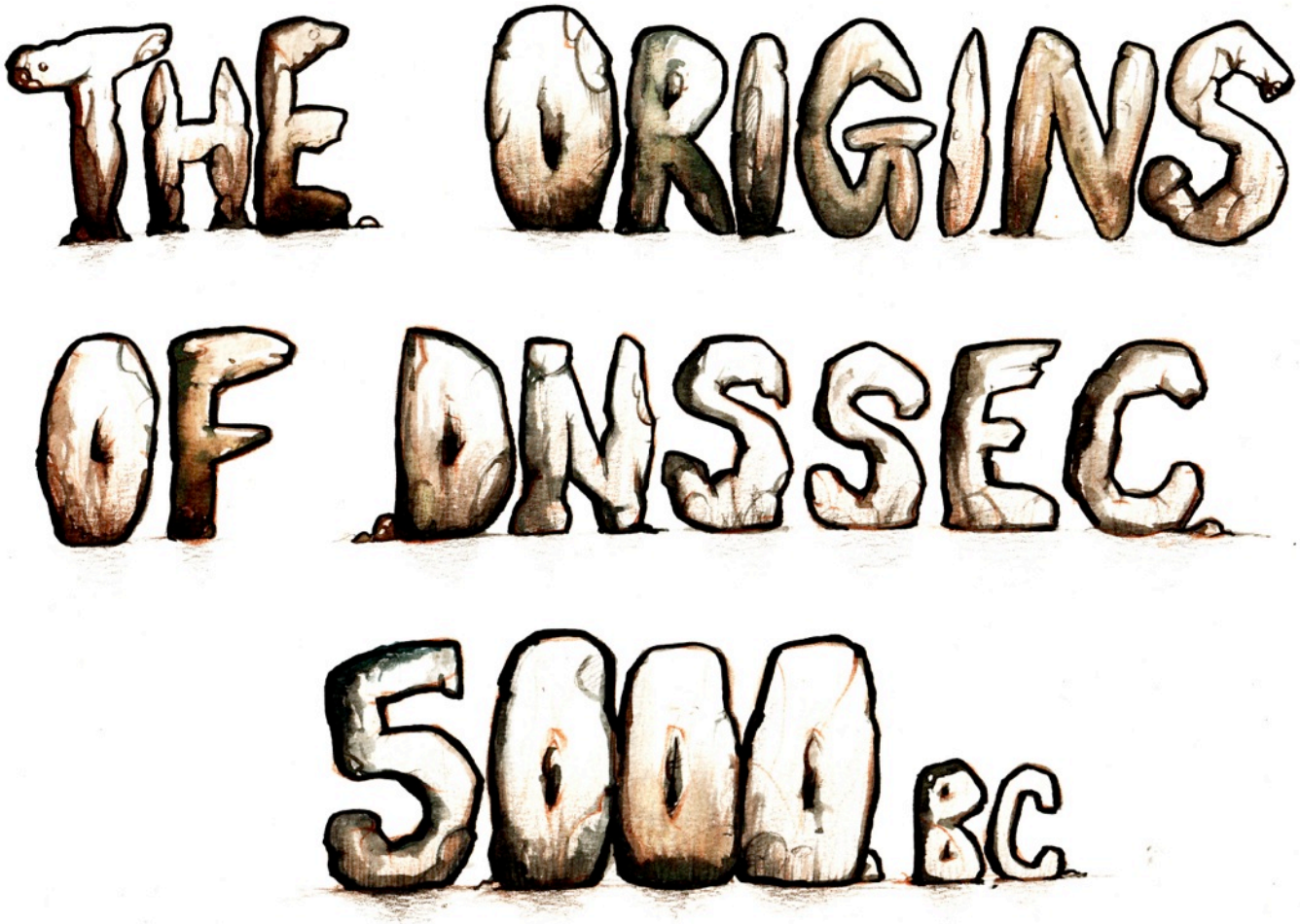


DNSSEC for Everybody: A Beginner's Guide

| ICANN 52 | February 2015

The Schedule

Outline Concept	Segment	Duration	Speaker
Welcome	Welcome and Introduction	2 mins	Dan
Basic Concepts	Caveman – DNSSEC 5000BC	3 mins	Dan
	DNS Basics	5 mins	Adam
	DNS Chain of Trust - Live	5 mins	Adam
Core Concepts	DNSSEC – How it works	10 mins	Adam
	DNSSEC – Chain of Trust Live	5 mins	Norm
Real World Examples	A sample DNSSEC implementation (what it looks like, s/w etc). A simple guide to deployment.	10 mins	Russ
	A guide to DNSSEC Deployment options: Technologies and vendors.	10 mins	Russ
Summary	Session Round up, hand out of materials, Thank you's	2 mins	Dan



nominet®

This is Ugwina. She lives in a cave on the edge of the Grand Canyon...

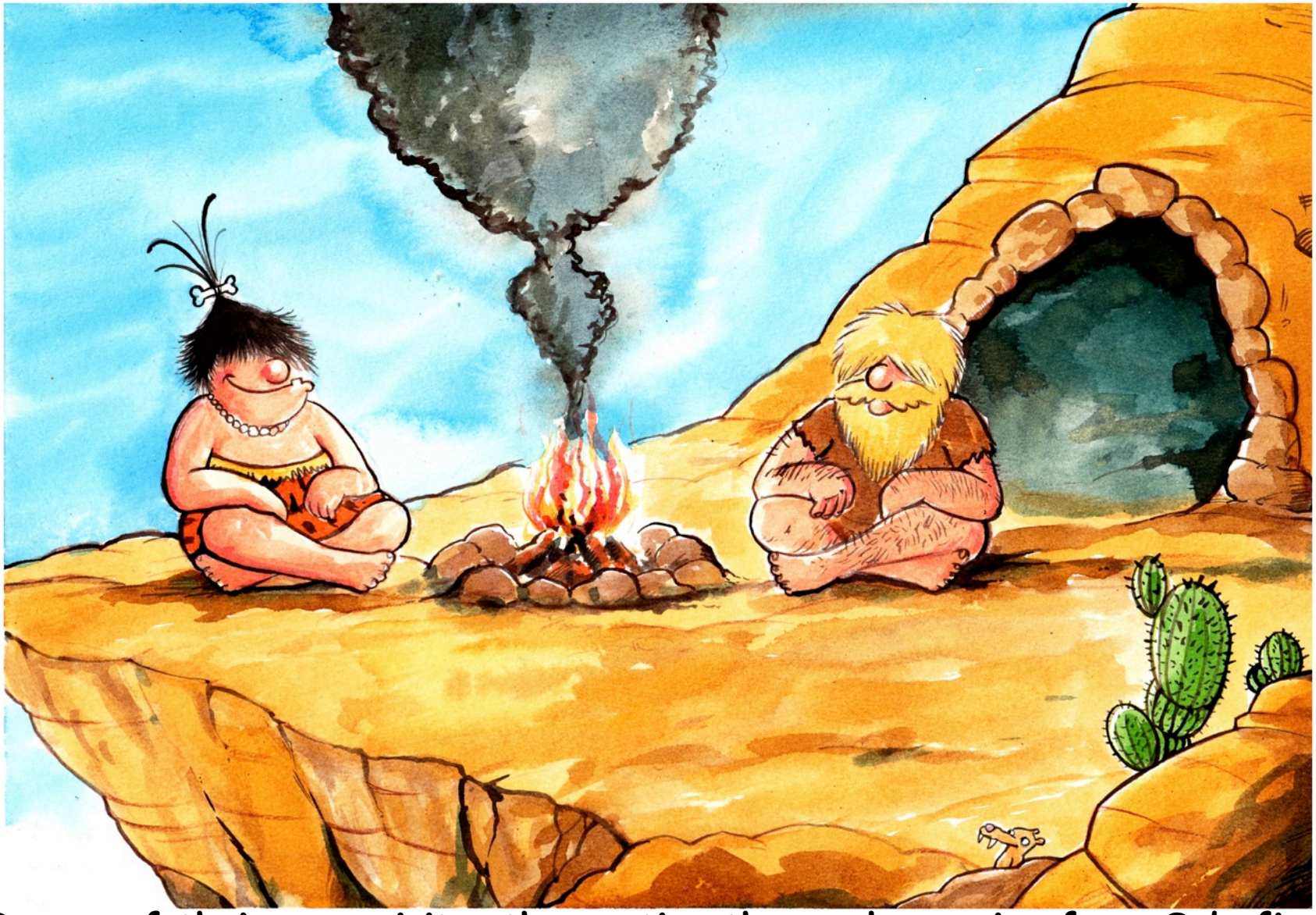
nominet®

This is Og. He lives in a cave on the other side of the Grand Canyon...

nominet®

It's a long way down and a long way round. Ugwina and Og don't get to talk much...

nominet®



On one of their rare visits, they notice the smoke coming from Og's fire

nominet®

...and soon they are chatting regularly using smoke signals

nominet®

until one day, mischievous caveman Kaminsky moves in next door to Ug and starts sending smoke signals too...

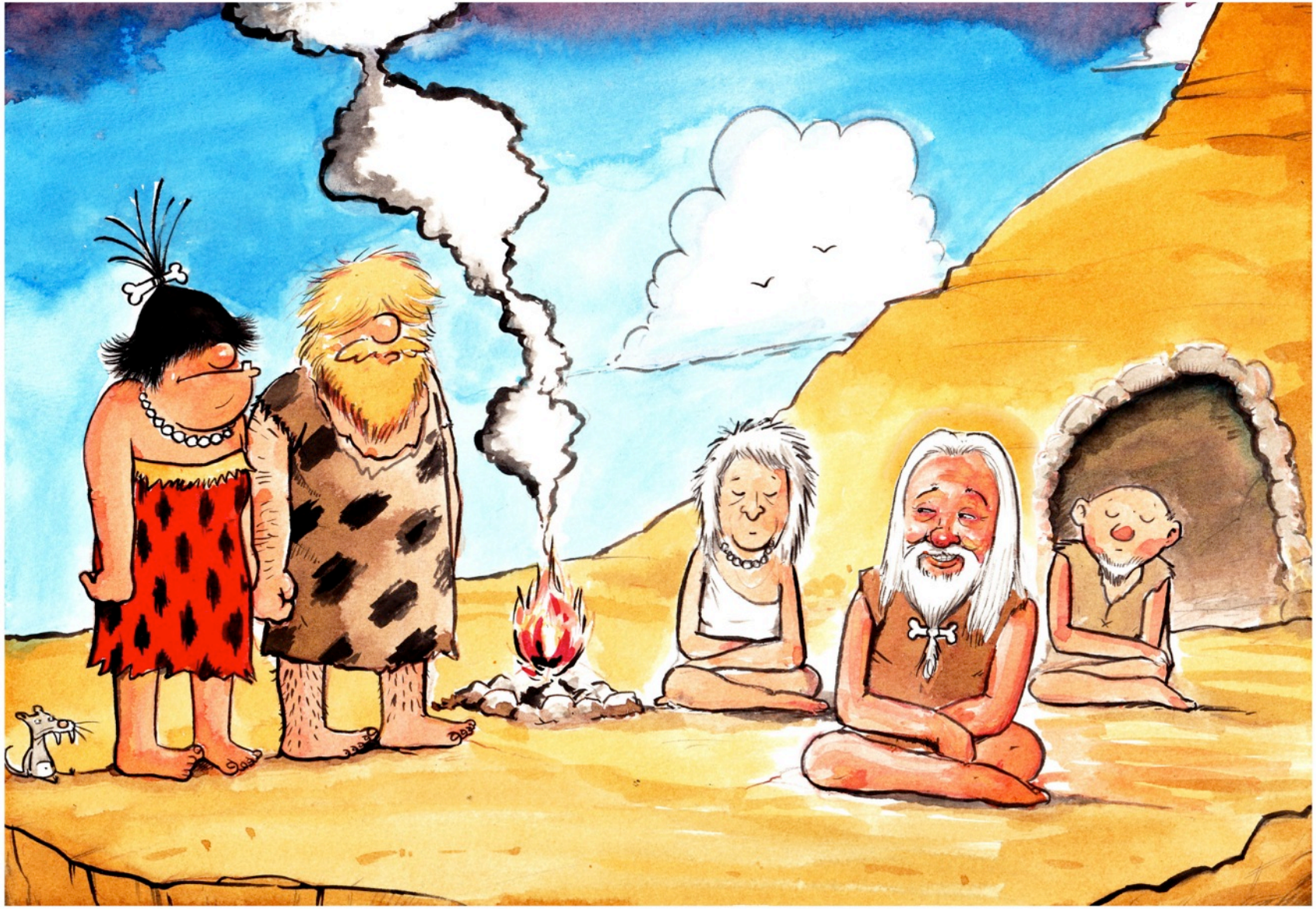
nominet®

Now Ugwina is really confused. She doesn't know which smoke to believe...

nominet®

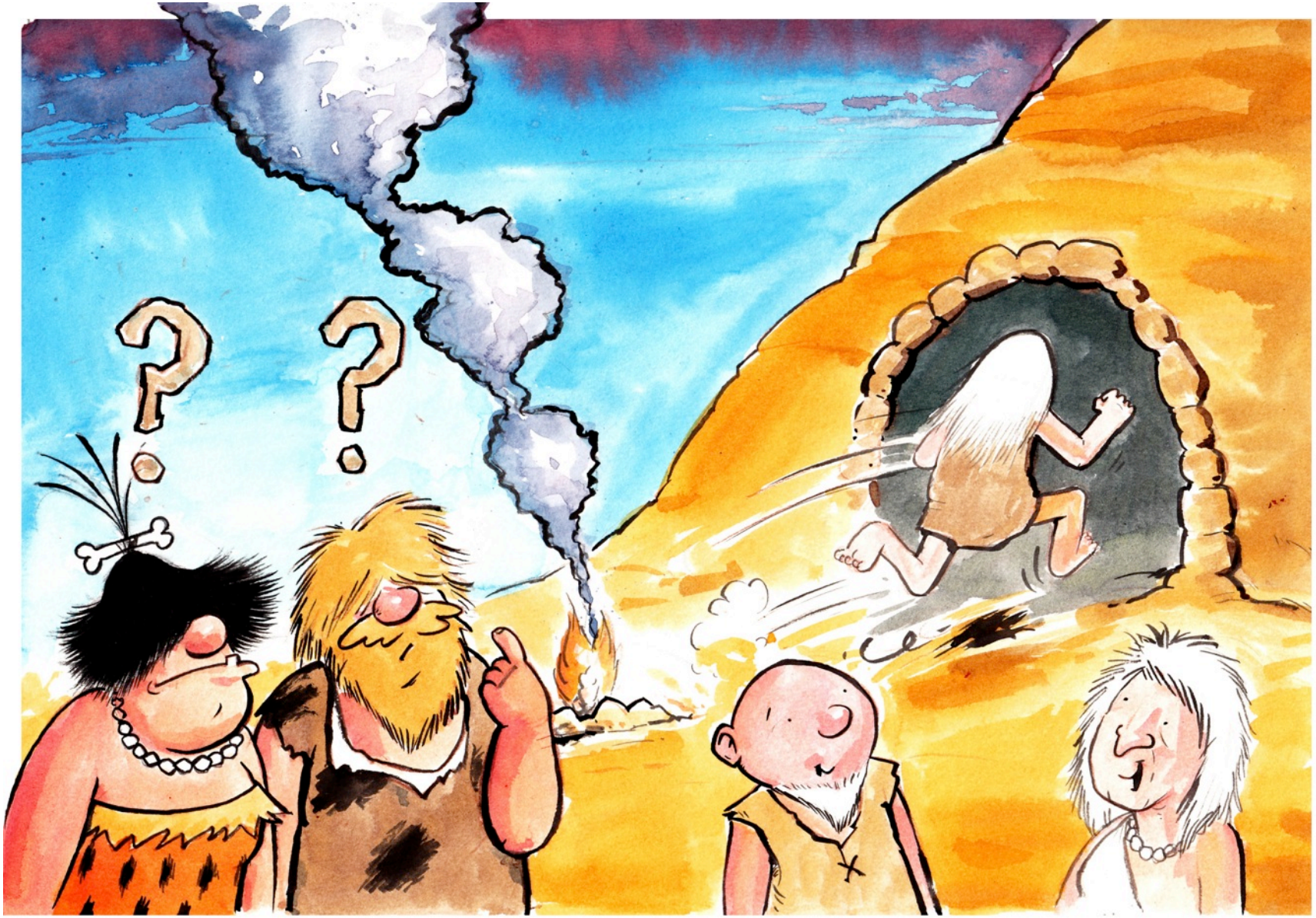
So Ugwina sets off down the canyon to try and sort out the mess...

nominet®



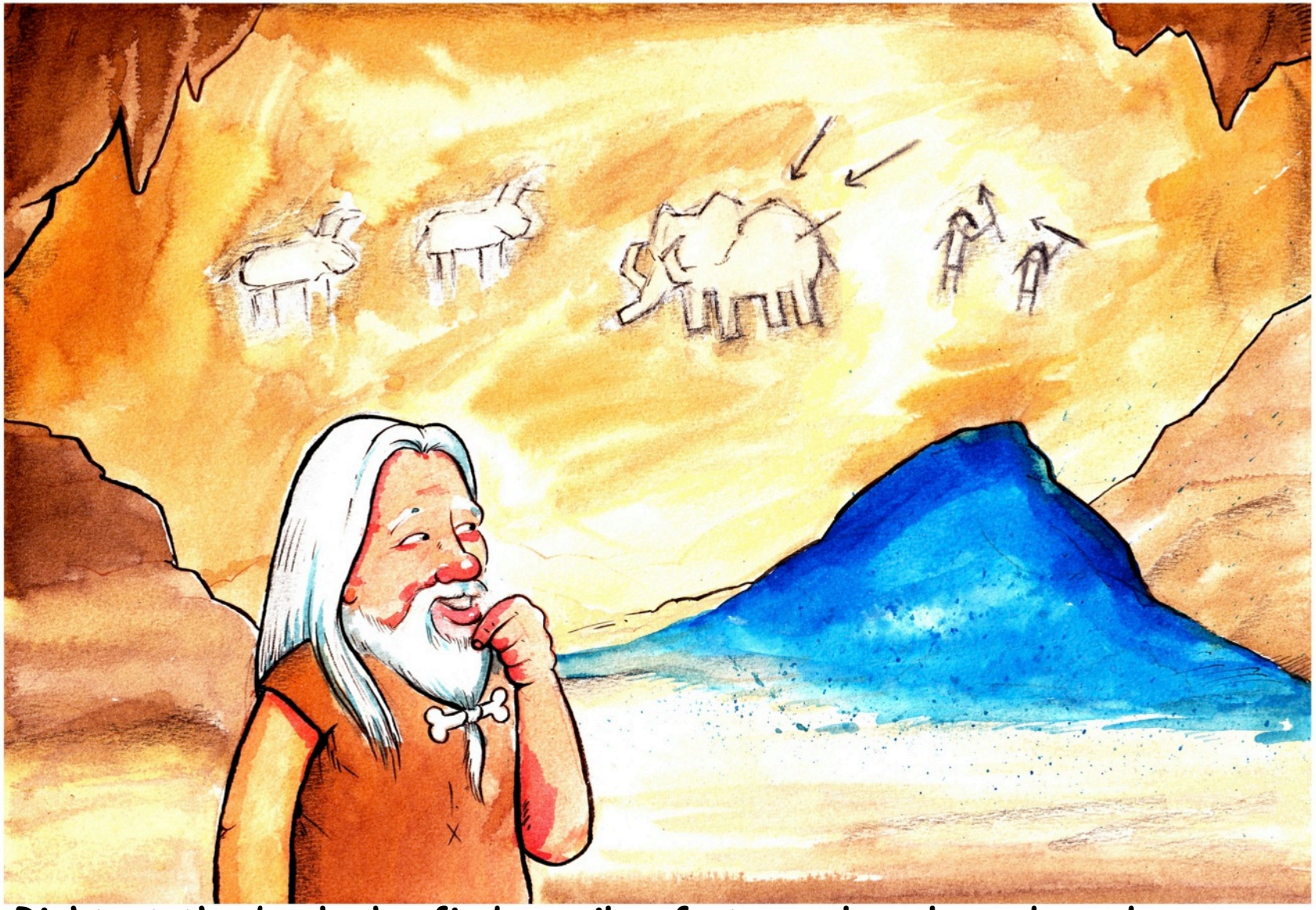
Ugwina and Og consult the wise village elders. Caveman Diffie thinks that he might have a cunning idea...

nominet®



And in a flash, jumps up and runs into Ug's cave...!

nominet®



Right at the back, he finds a pile of strangely coloured sand that has only ever been found in Ug's cave...

nominet®

And with a skip, he rushes out and throws some of the sand onto the fire. The smoke turns a magnificent blue...

nominet®

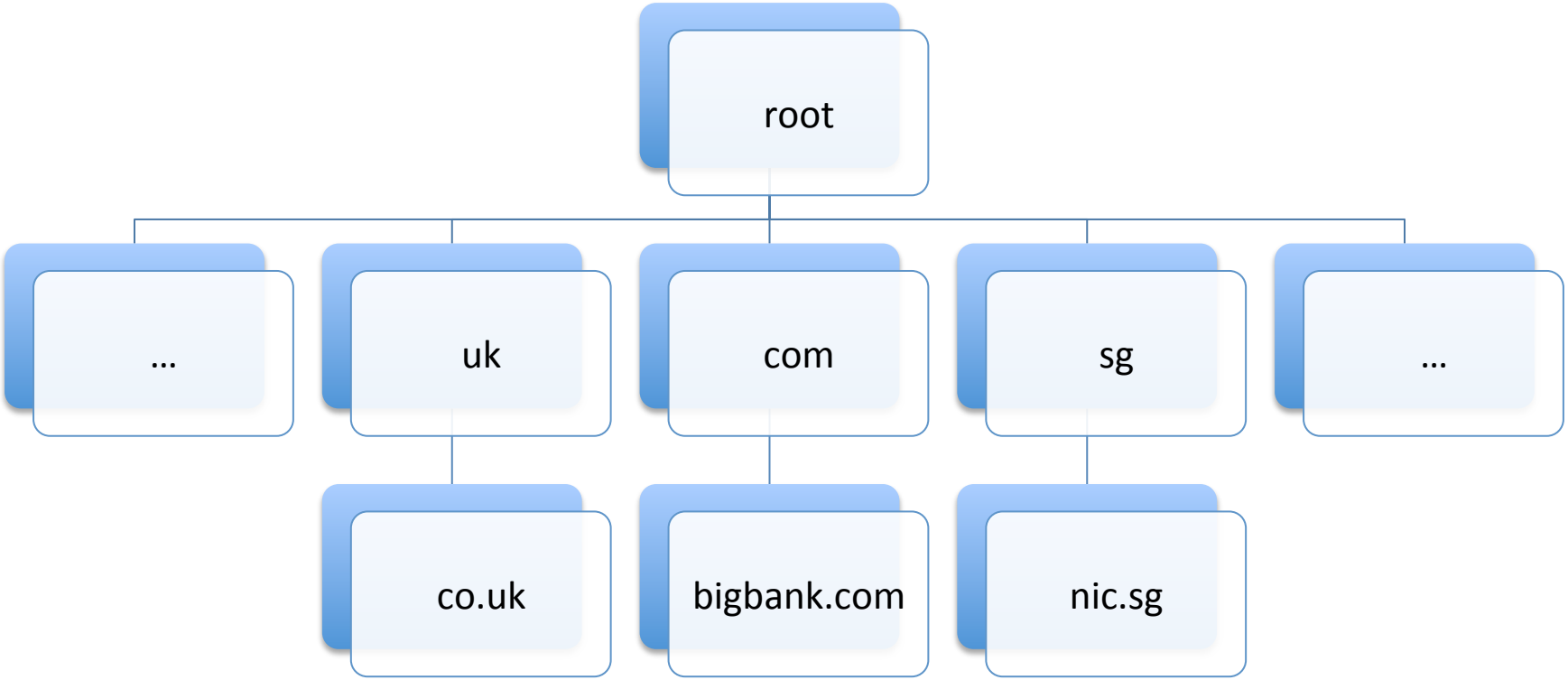
Now Ugwina and Og can chat happily again, safe in the knowledge that nobody can interfere with their conversation…

nominet®

Introduction to DNSSEC

| Adam Leach, NominetUK | ICANN 52 | February 2015

High level concept of DNS



High level concept of DNS

- A resolver knows where the root-zone is
- Traverses the DNS hierarchy
- Each level refers the resolver to the next level
- Until the question has been answered
- The resolver caches all that information for future use.

A Skit/Play

…Ugwina, the resolver, chatting with Og, the server…

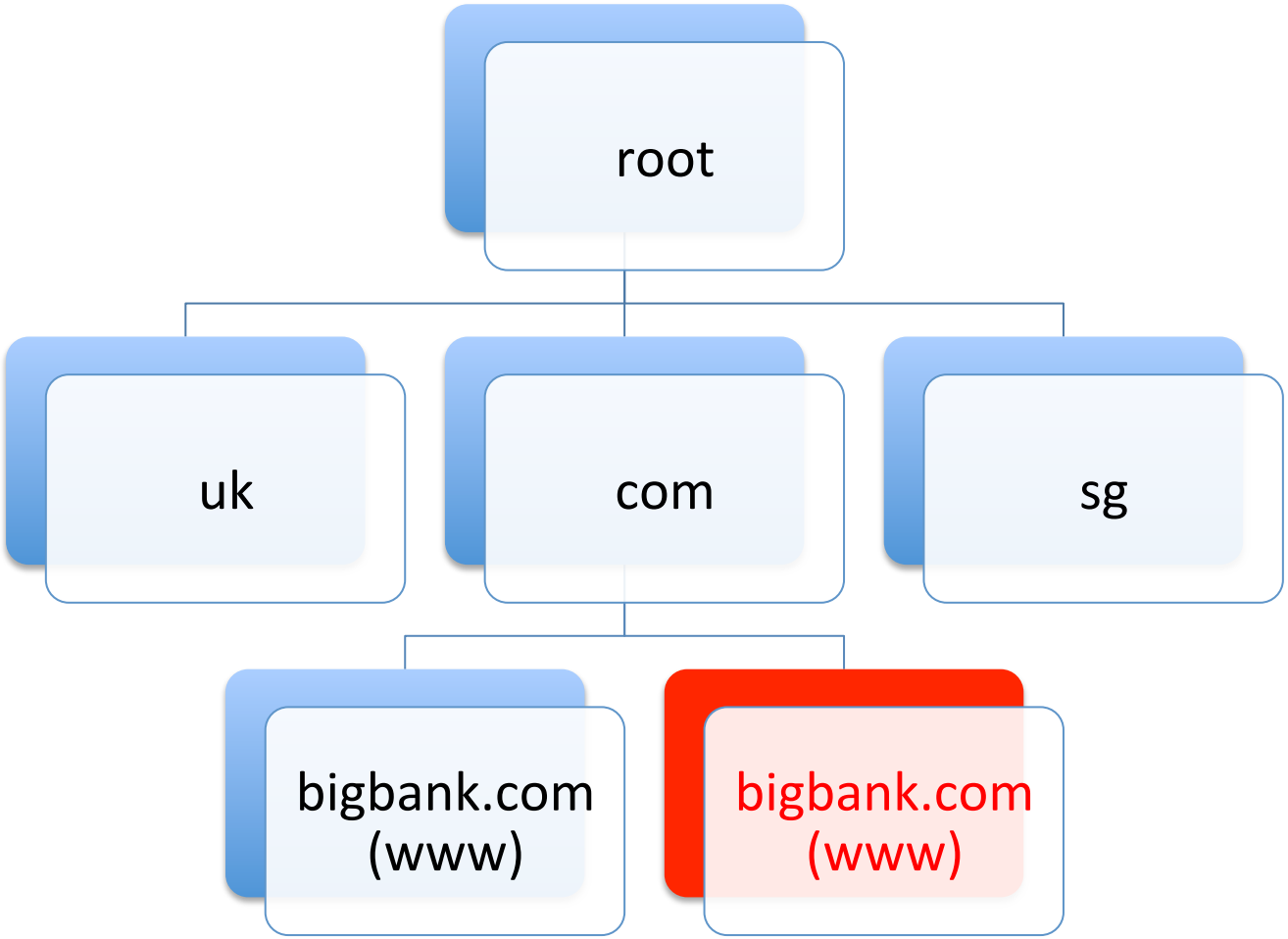
…Ugwina, the resolver is confused. She doesn't know who the real Og is…

…Ugwina, the resolver, can verify that the real Og sends the message…

High level concept of DNS

- There is no security
- Names are easily spoofed
- Caches are easily poisoned

High level concept of DNS



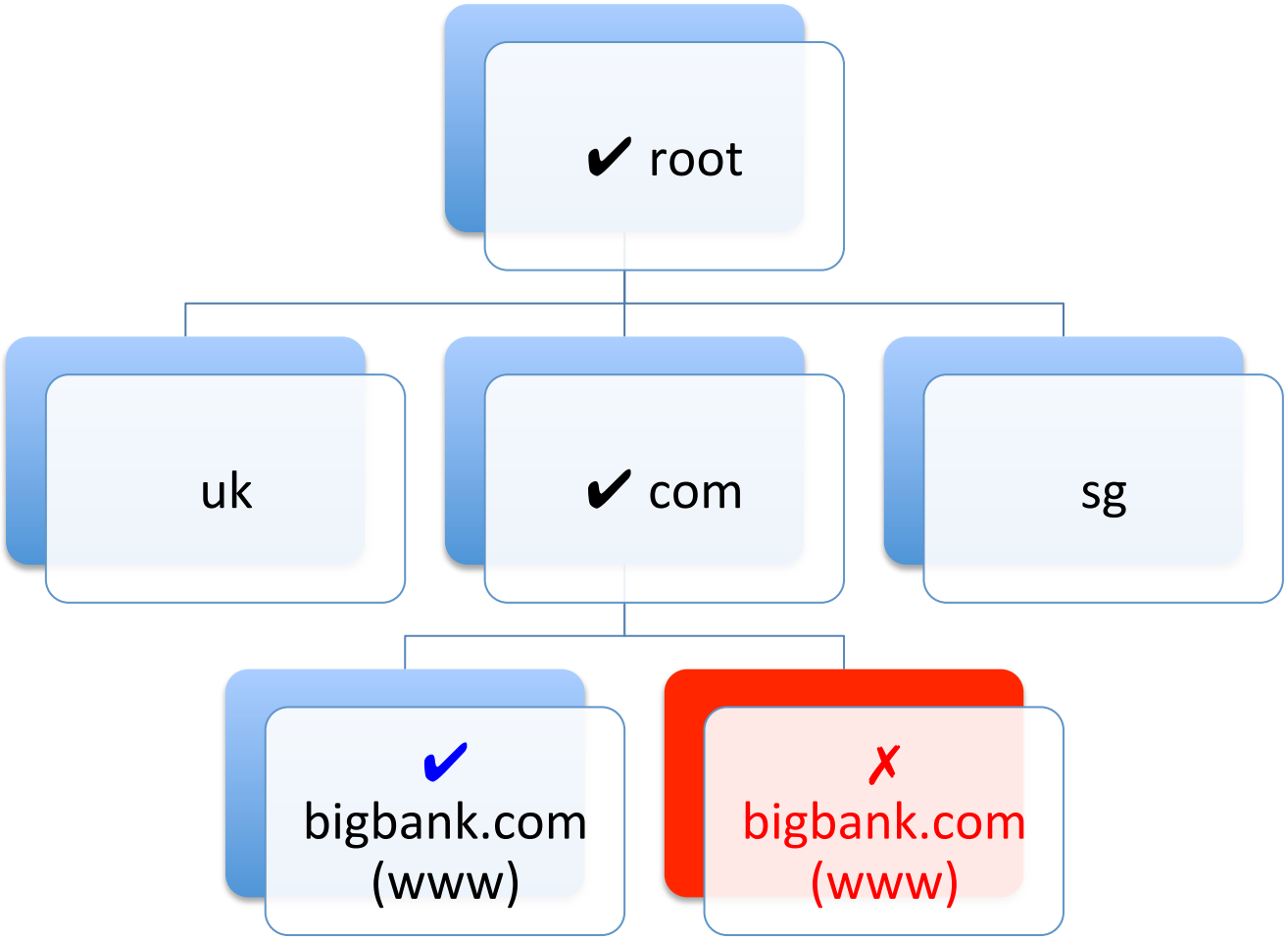
DNSSEC is the solution

- DNSSEC uses **digital signatures** to assure that information is correct and came from the right place.
- The keys and signatures to verify the information, is stored in the DNS as well
- Since DNS is a lookup system, keys can simply be looked up, like any data.

High level concept of DNSSEC

- A resolver knows what the root-key is
- It builds a Chain of Trust:
  - Each level signs the key of the next level
  - Until the chain is complete

High level concept of DNSSEC



Example of Why You Need DNSSEC and a Simple Guide to Deployment

| Russ Mundy, Parsons| ICANN 52 | February 2015

Why Worry About DNS?

- Users think in terms of names
  - Applications primarily use DNS names
  - Internet uses network addresses to connect locations
- DNS provides the translation from names to network addresses
- Proper DNS functions required by essentially all Network Applications
  - If DNS doesn't work right,

  ➔ the applications won't get to the intended locations

russ.mundy@parsons.com

DNS Hijack Threat

- DNS attacks provide a way to divert users' applications, e.g.,
  - Redirecting user applications to false locations to steal passwords or other sensitive information
  - Redirect to a man-in-the-middle location
    - See and copy an entire session: Web, email, IM, etc.
- Multiple DNS hijack tools available on the Internet
  - Some University courses have required students to write DNS hijack software as a class assignment!

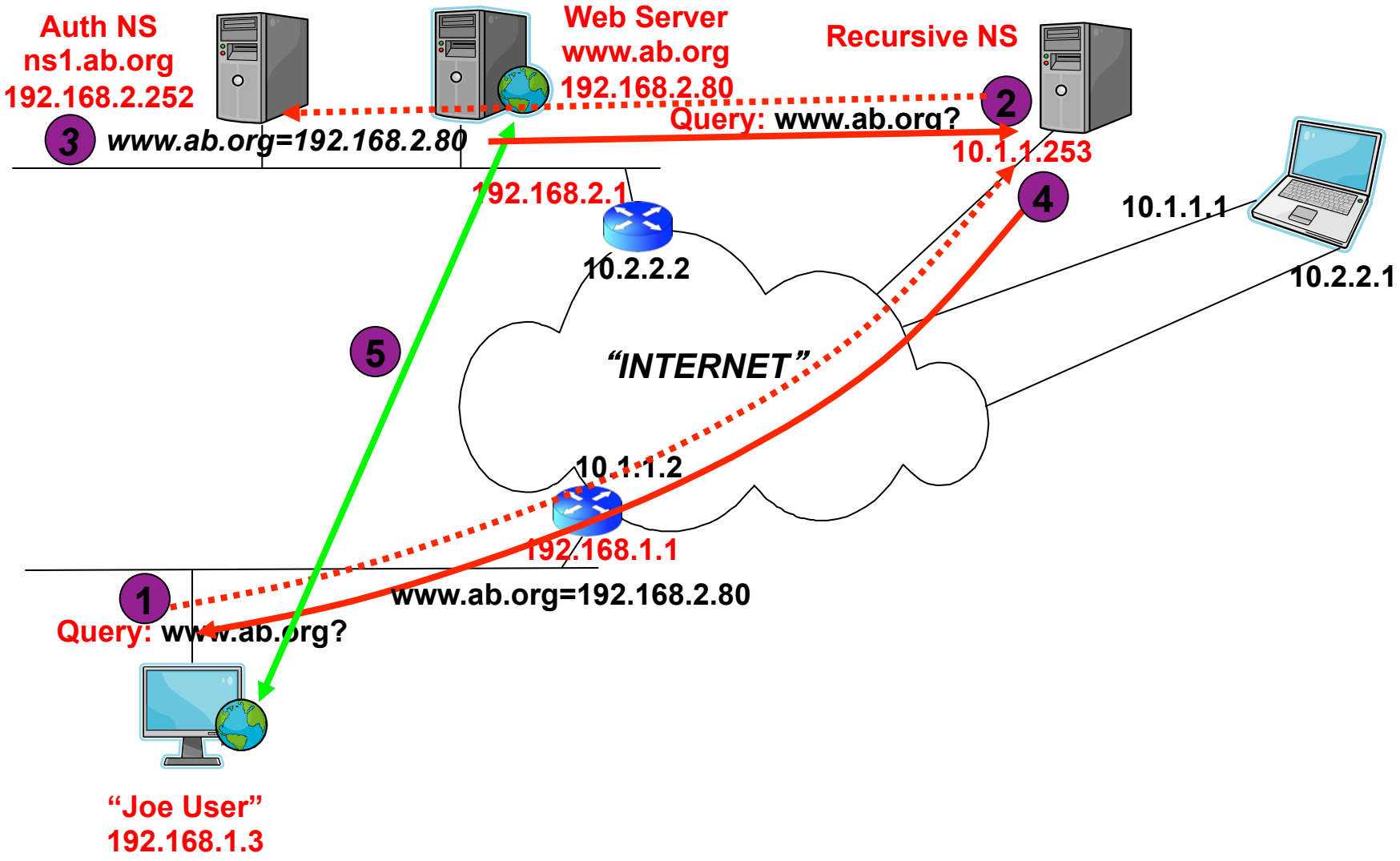
russ.mundy@parsons.com

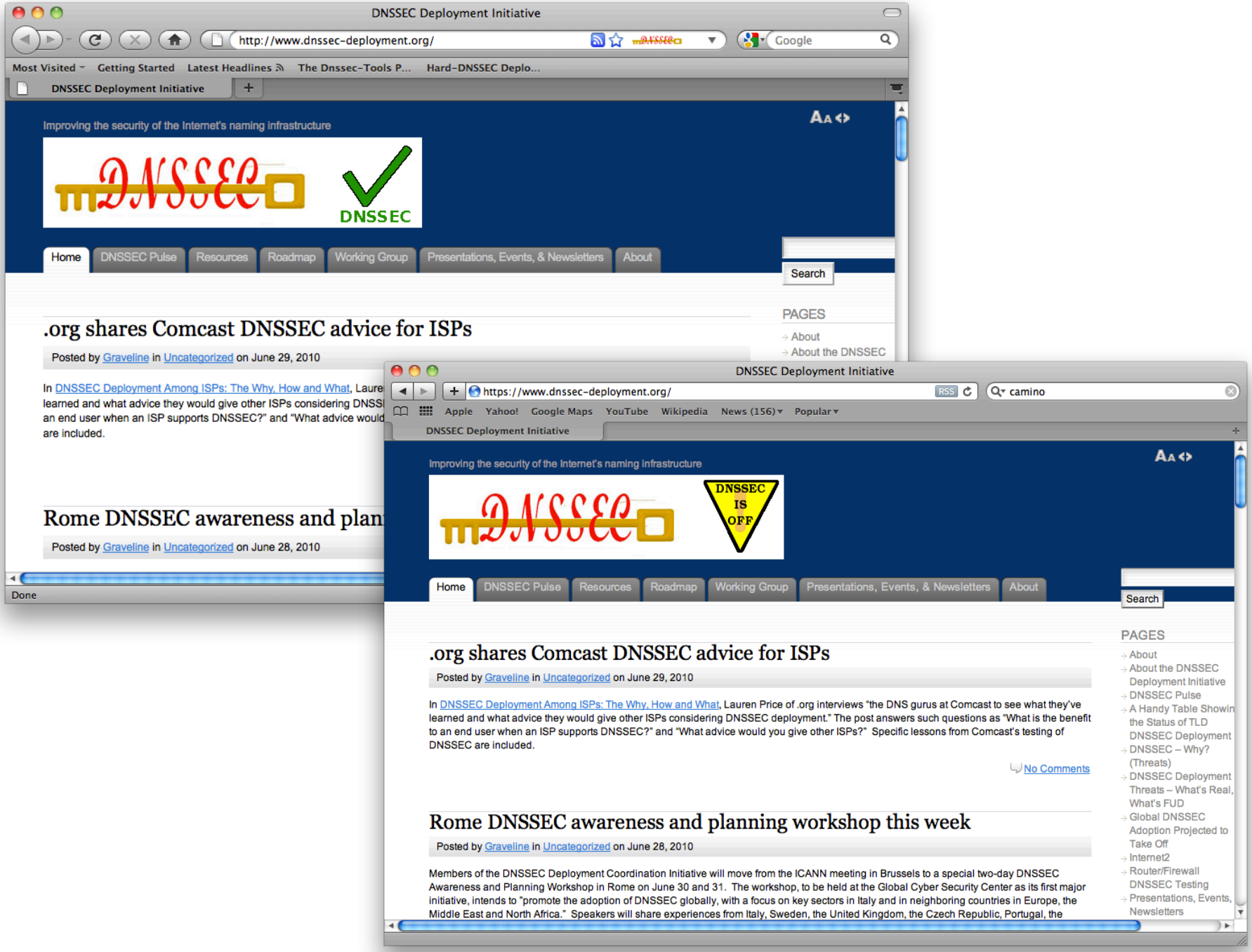
How Can DNSSEC Help?

- DNSSEC can assure users they are reaching the right location
  - DNSSEC provides cryptographic information that can be used to verify that DNS information:
    - came from the proper source and
    - it was not changed enroute
- Hijack example will show DNSSEC preventing redirection of a web application
  - Web site tailored for effective use of DNSSEC and a web browser that uses DNSSEC

russ.mundy@parsons.com

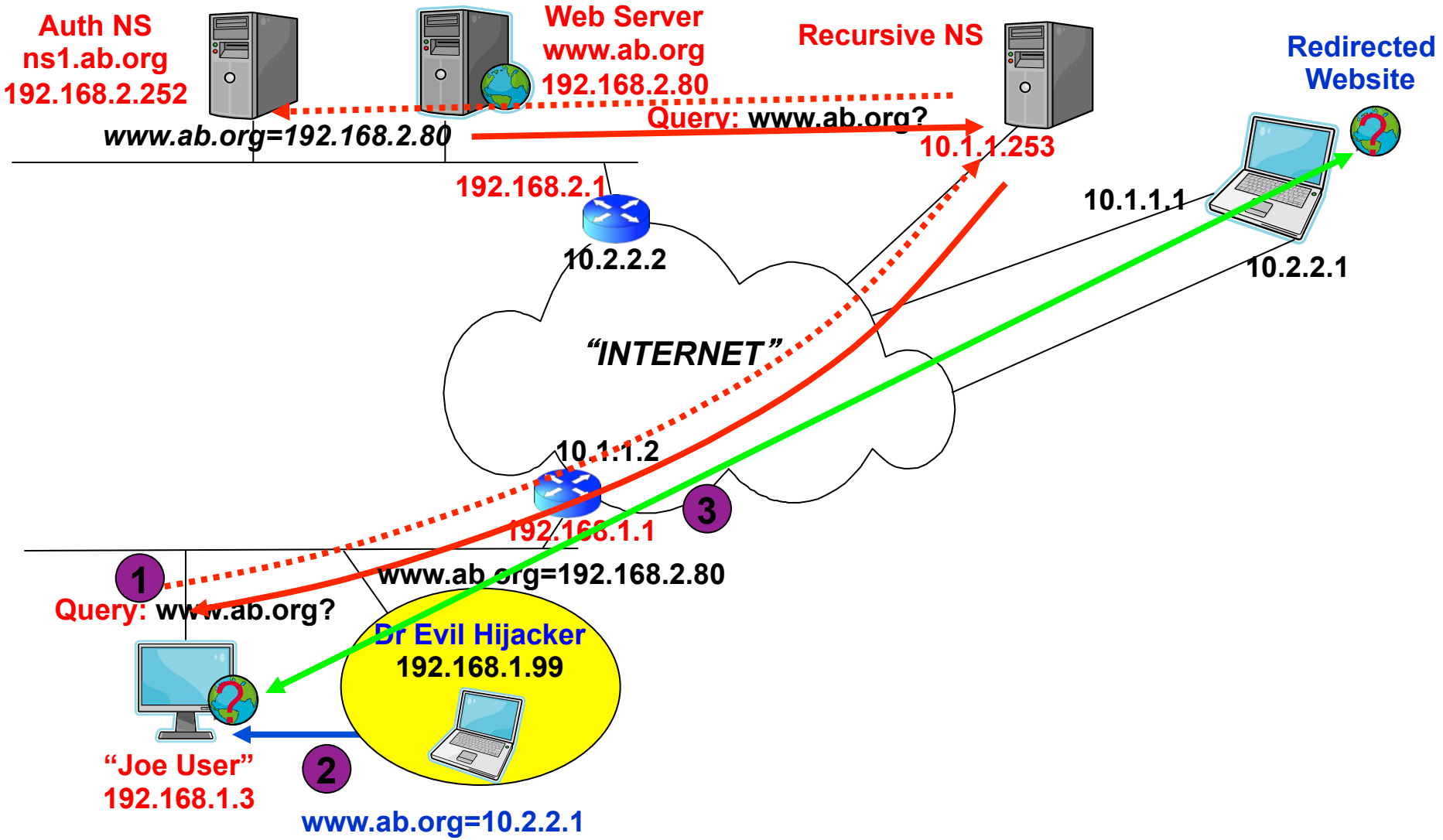
Normal DNS & Web Exchange



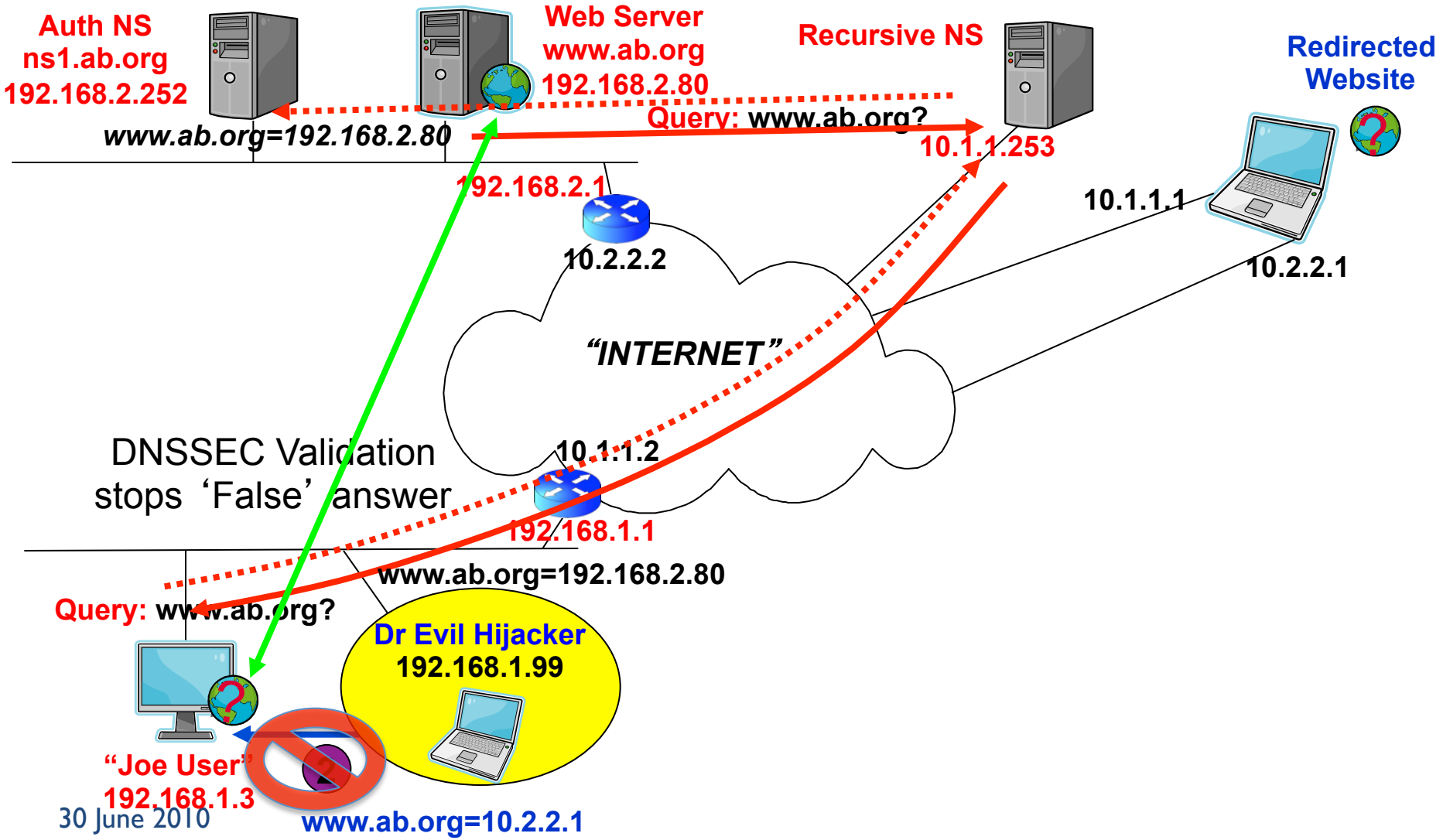


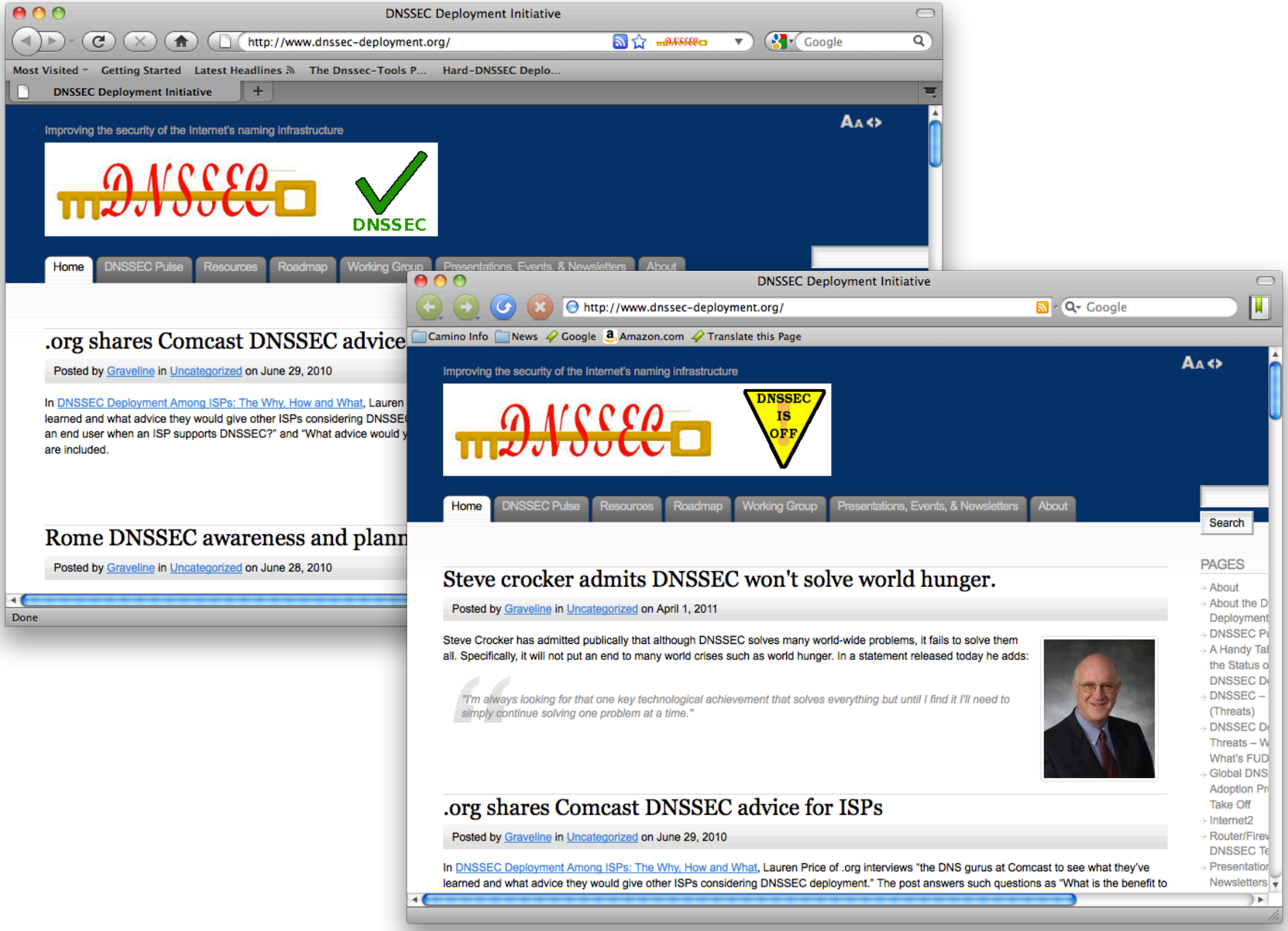
russ.mundy@parsons.com

DNS Hijacked Web Exchange



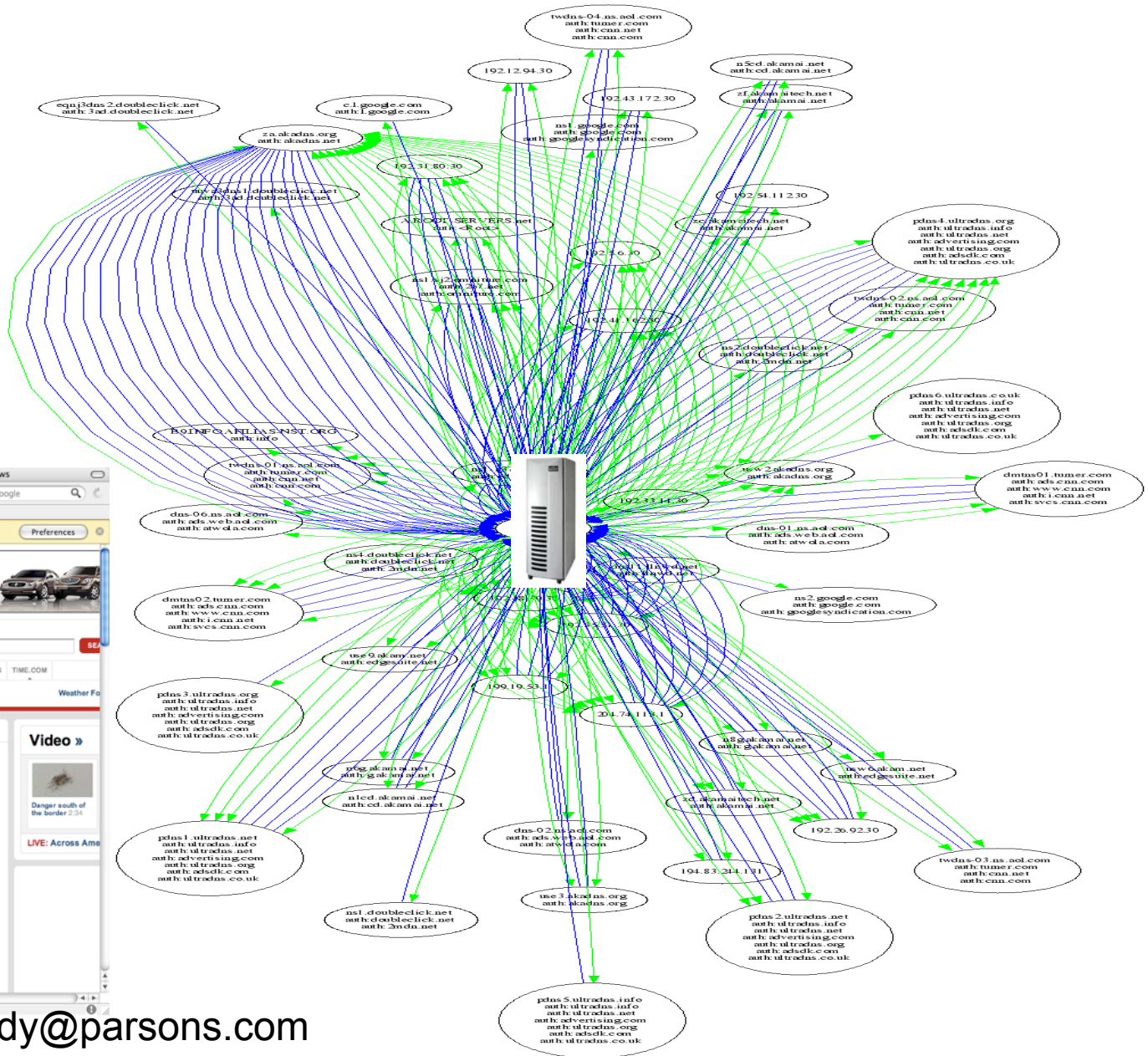
Attempted DNS Hijacked Web Exchange Stopped by DNSSEC





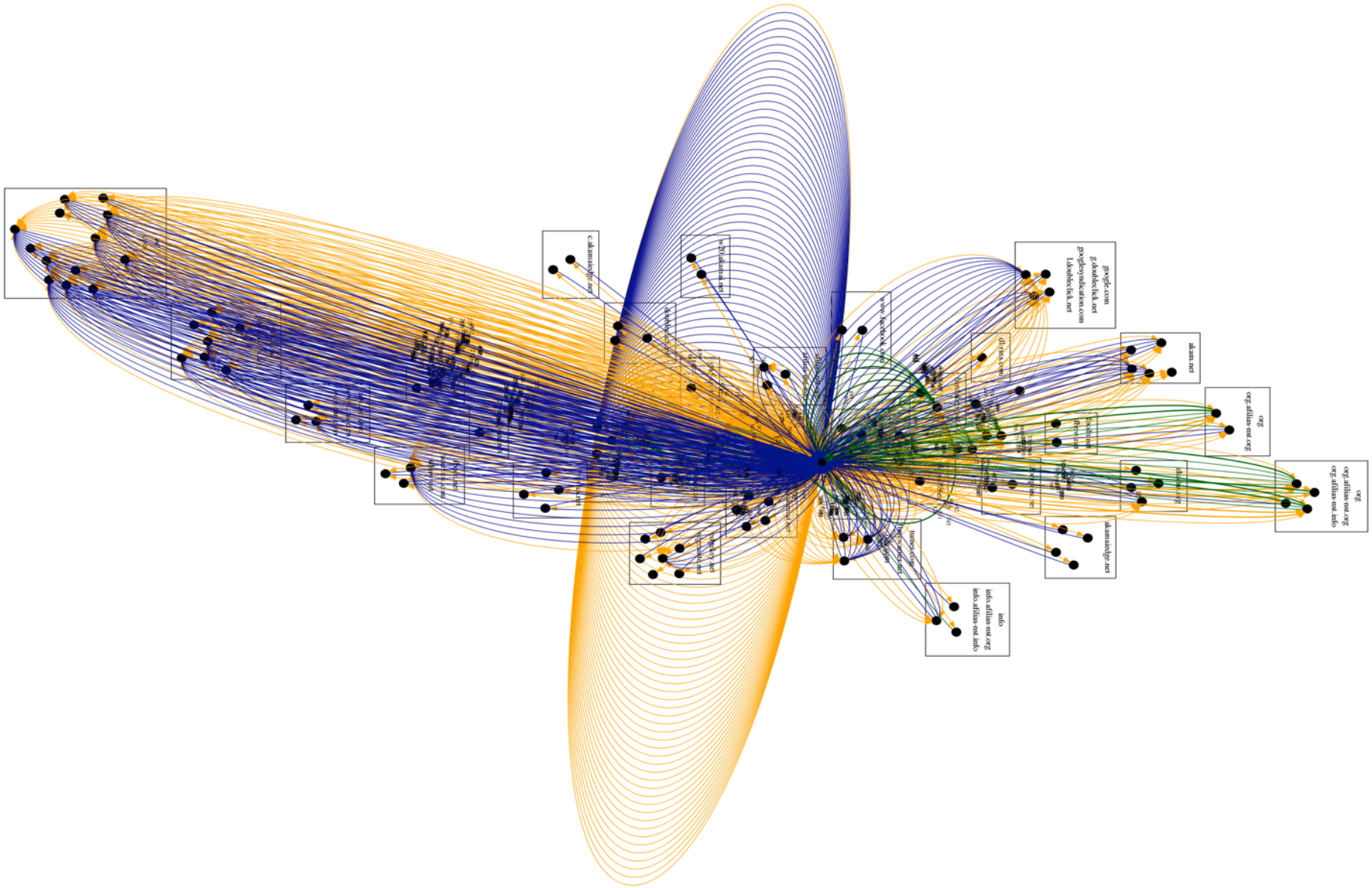
russ.mundy@parsons.com

1 Webpage = Multiple DNS Name Resolutions



russ.mundy@parsons.com

www.cnn.com



russ.mundy@parsons.com

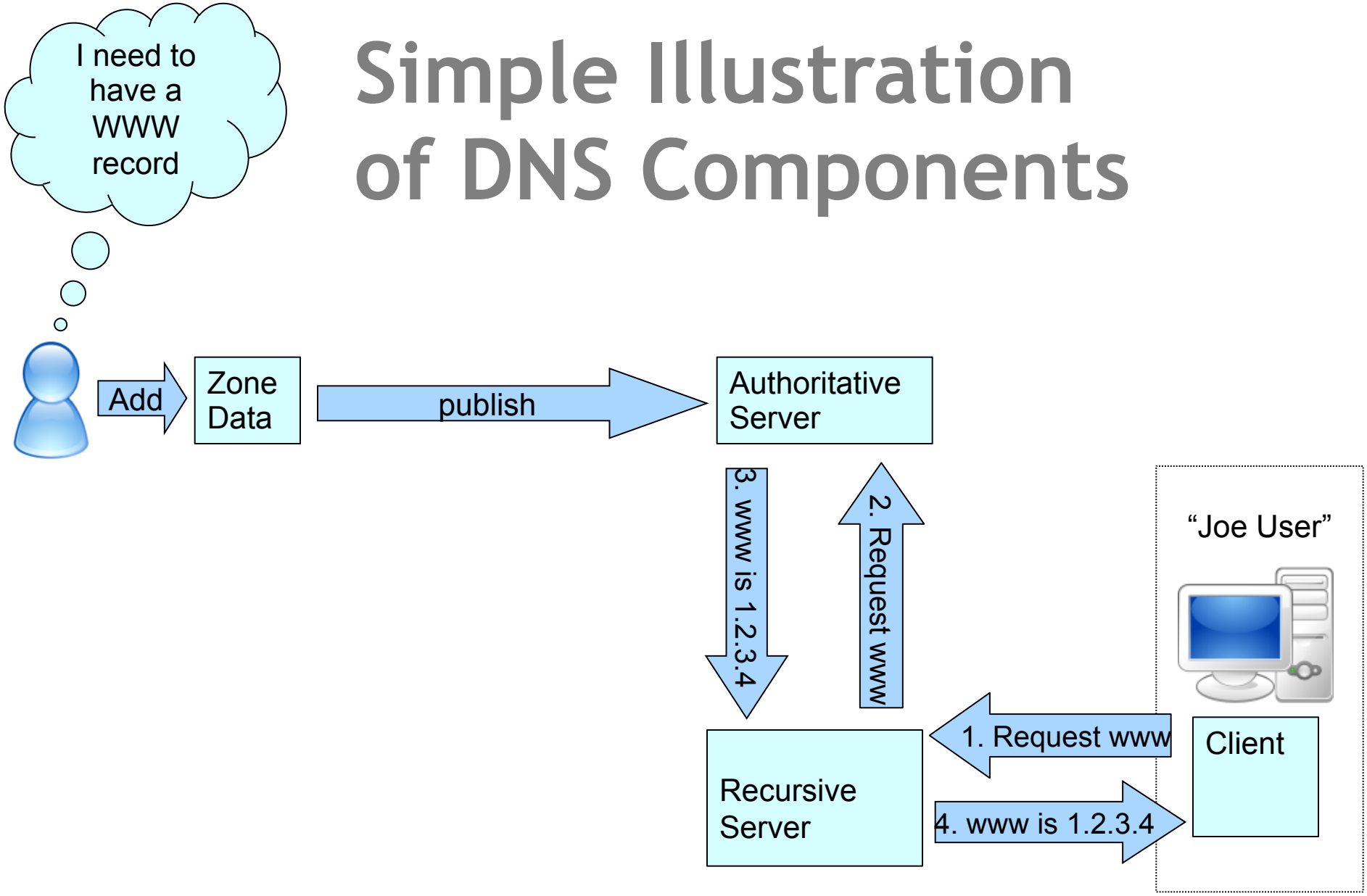
DNS Basic Functions

- DNS provides the translation from names to network addresses
- Get the right DNS content to Internet users

➢ IT'S **DNS ZONE DATA** THAT MATTERS!

russ.mundy@parsons.com

Simple Illustration of DNS Components



russ.mundy@parsons.com

DNSSEC Implementation Samples

- DNSSEC implementation depends upon & is mostly driven by an activity's DNS functions
  - DNS is made up of many parts, e.g., name server operators, applications users, name holders ("owners"), DNS provisioning
  - Activities with large, complex DNS functions are more likely to have more complex DNSSEC implementation activities
    - Also more likely to have 'DNS knowledgeable' staff

russ.mundy@parsons.com

DNSSEC Implementation Samples, Continued

- DNS size and complexity examples:
  - Registry responsible for a large TLD operation, e.g., .com
  - Substantial enterprise with many components with many geographic locations, e.g., hp.com
  - Internet-based businesses with a number of business critical zones, e.g., www.verisign.com
  - Activities with non-critical DNS zones, e.g., net-snmp.org
  - Proverbial Internet end users (all of us here)

russ.mundy@parsons.com

How Does DNSSEC Fit?

- DNSSEC required to thwart attacks on DNS CONTENT
  - DNS attacks used to attack Internet users applications

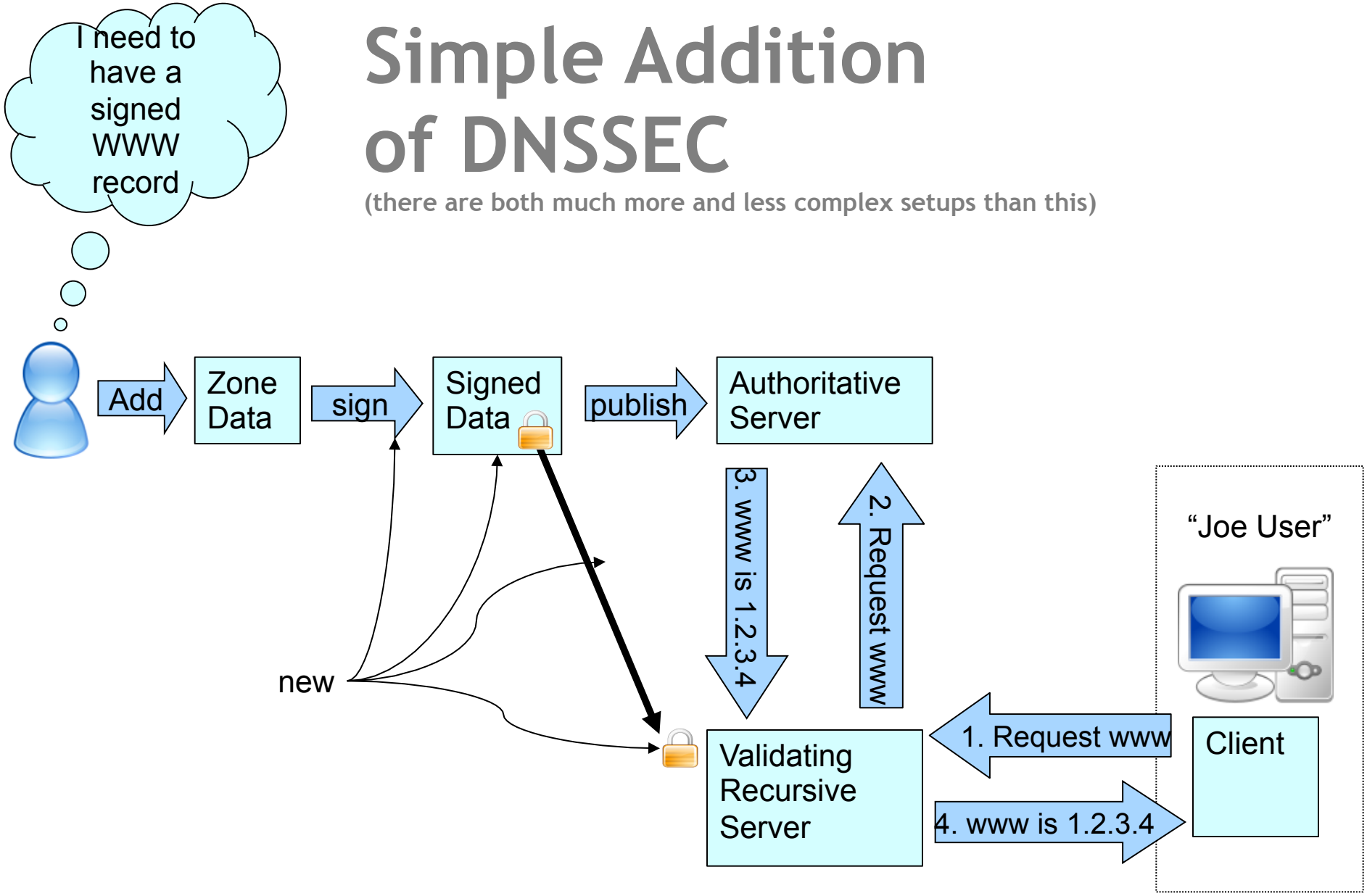
➢ Protect **DNS ZONE DATA** as much as (or more than) any DNSSEC information

  ➢ Including DNSSEC private keys!!

russ.mundy@parsons.com

Simple Addition of DNSSEC

(there are both much more and less complex setups than this)



russ.mundy@parsons.com

General Principle:

- If an activity does a lot with their DNS functions and operations then they probably will want to do a lot with the associated DNSSEC pieces;
- If an activity does little or nothing with their DNS functions and operations then they probably will do little or nothing directly with their DNSSEC elements but Require DNSSEC from their suppliers

russ.mundy@parsons.com

Thank You and Questions