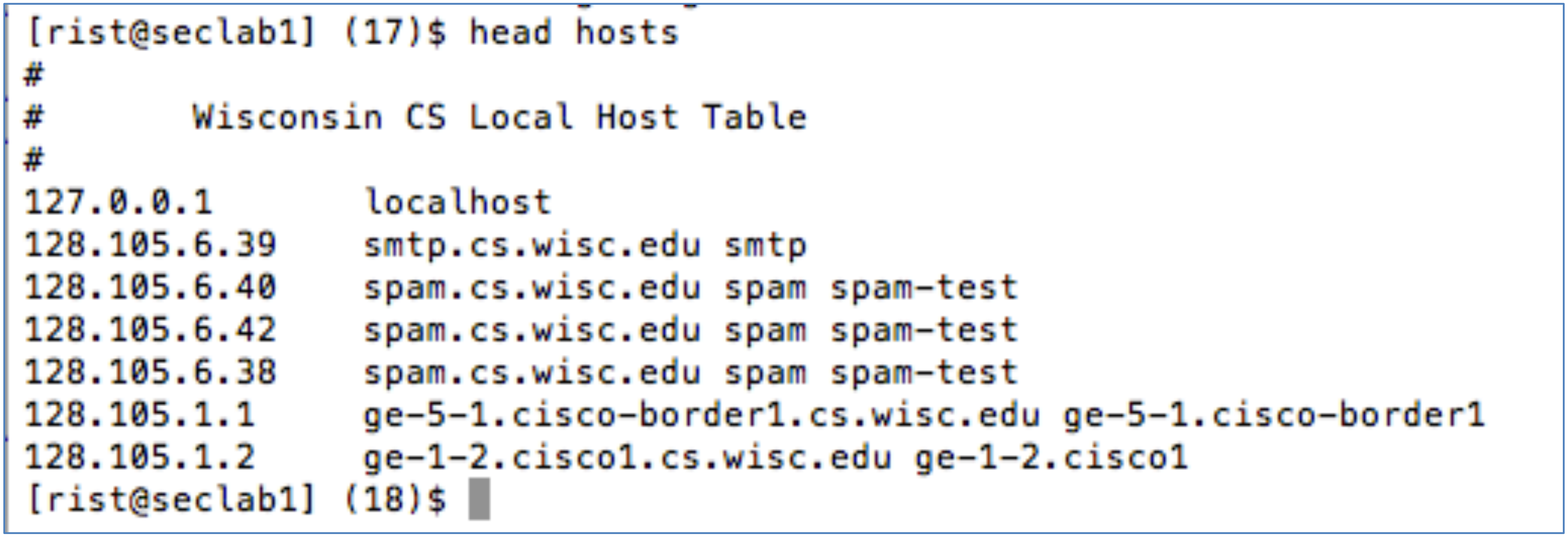
DNS

CS642: Computer Security

128.105.5.31

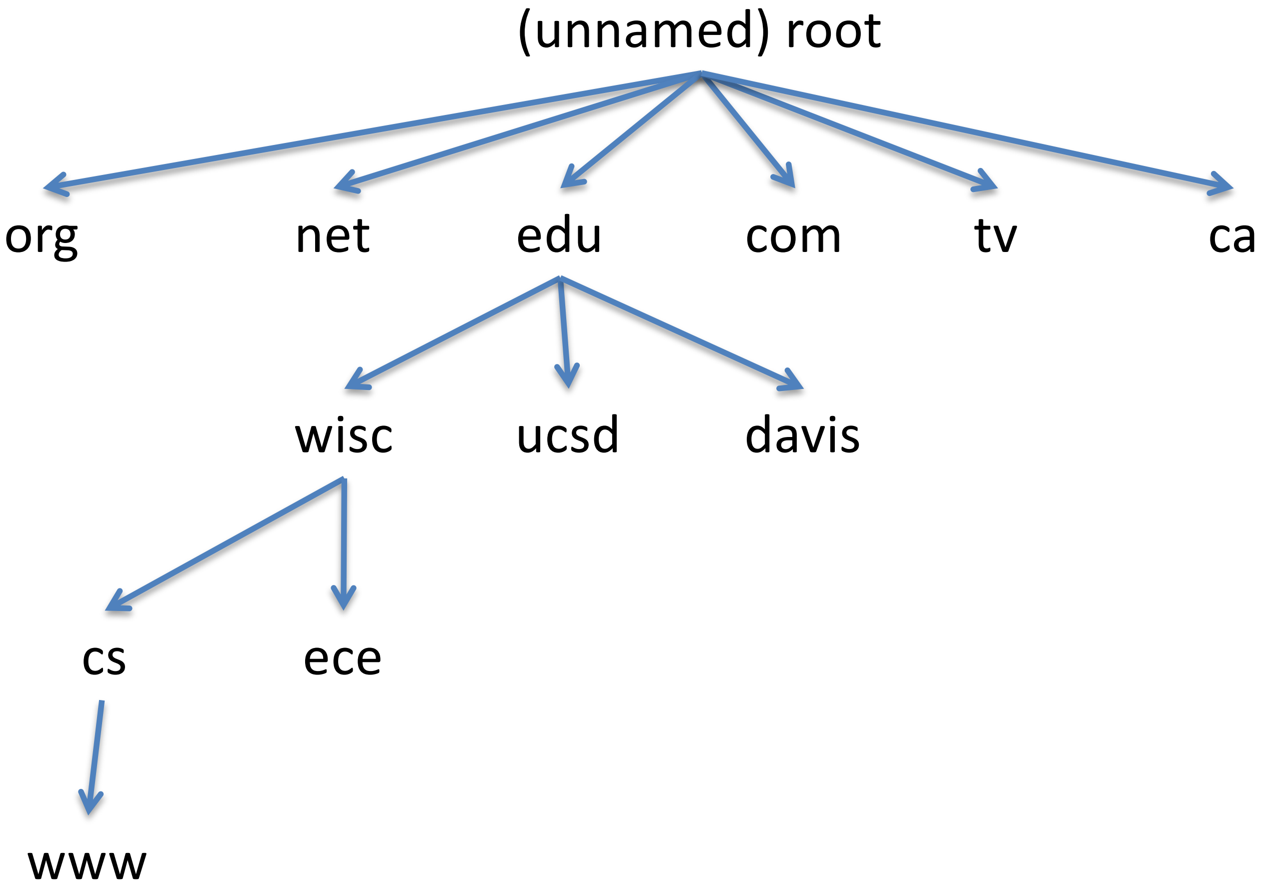
We don’t want to have to remember IP addresses



```
[rist@seclab1] (17)$ head hosts
#
#       Wisconsin CS Local Host Table
#
127.0.0.1       localhost
128.105.6.39    smtp.cs.wisc.edu smtp
128.105.6.40    spam.cs.wisc.edu spam spam-test
128.105.6.42    spam.cs.wisc.edu spam spam-test
128.105.6.38    spam.cs.wisc.edu spam spam-test
128.105.1.1     ge-5-1.cisco-border1.cs.wisc.edu ge-5-1.cisco-border1
128.105.1.2     ge-1-2.cisco1.cs.wisc.edu ge-1-2.cisco1
[rist@seclab1] (18)$ █
```

Early days of ARPANET: manually managed hosts.txt served from single computer at SRI

Heirarchical domain name space



(unnamed) root

org net edu com tv ca

wisc ucsd davis

cs ece

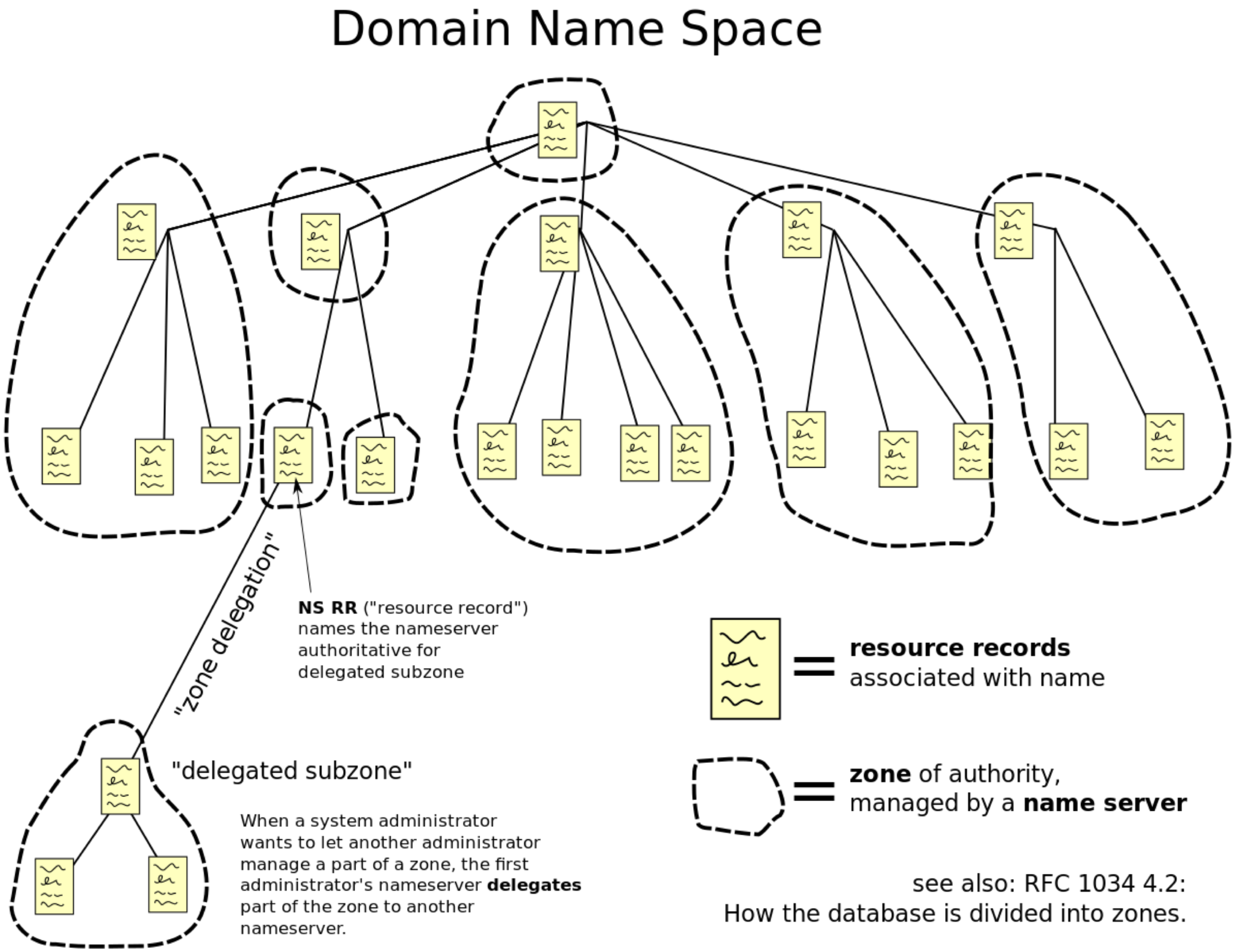
www

Top Level domains (TLD)

Second Level domains

max 63 per element

Zones



NS RR ("resource record") names the nameserver authoritative for delegated subzone

When a system administrator wants to let another administrator manage a part of a zone, the first administrator's nameserver **delegates** part of the zone to another nameserver.

= **resource records** associated with name

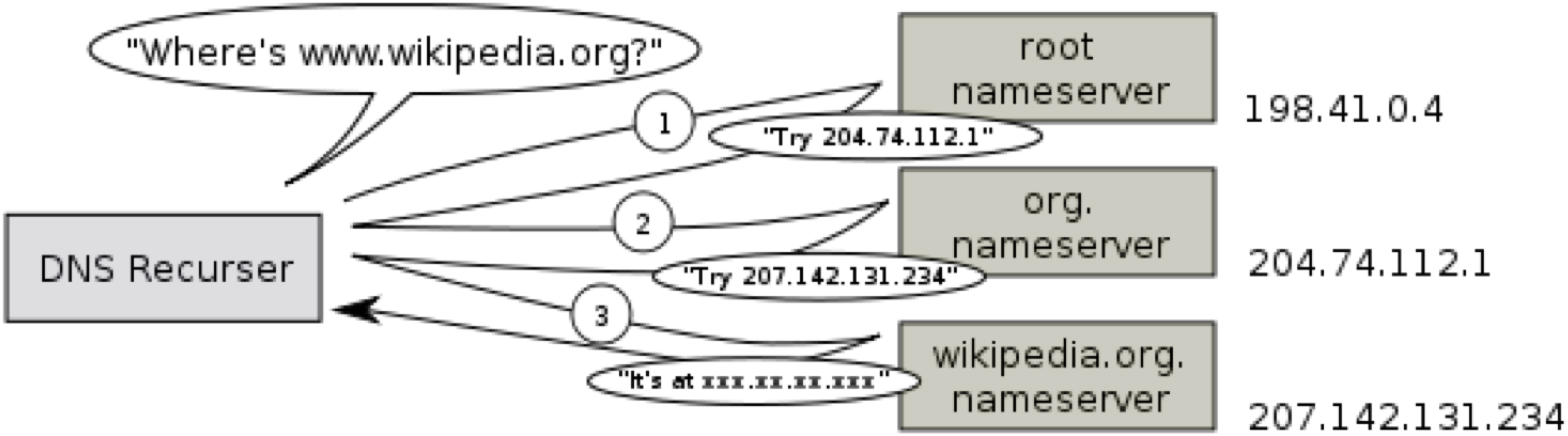
= **zone** of authority, managed by a **name server**

see also: RFC 1034 4.2:
How the database is divided into zones.

From
https://en.wikipedia.org/wiki/Domain_Name_System

Resolving names

- Clients configured with initial name servers
- Iterative: clients follow referrals to lookup name at next server
- Recrsive: NS does lookup on behalf of client, caches results



From http://en.wikipedia.org/wiki/File:An_example_of_theoretical_DNS_recursion.svg

Example DNS query types

A	address (get me an IPv4 address)
AAAA	IPv6 address
NS	name server
TXT	human readable text, has been used for some encryption mechanisms
MX	mail exchange

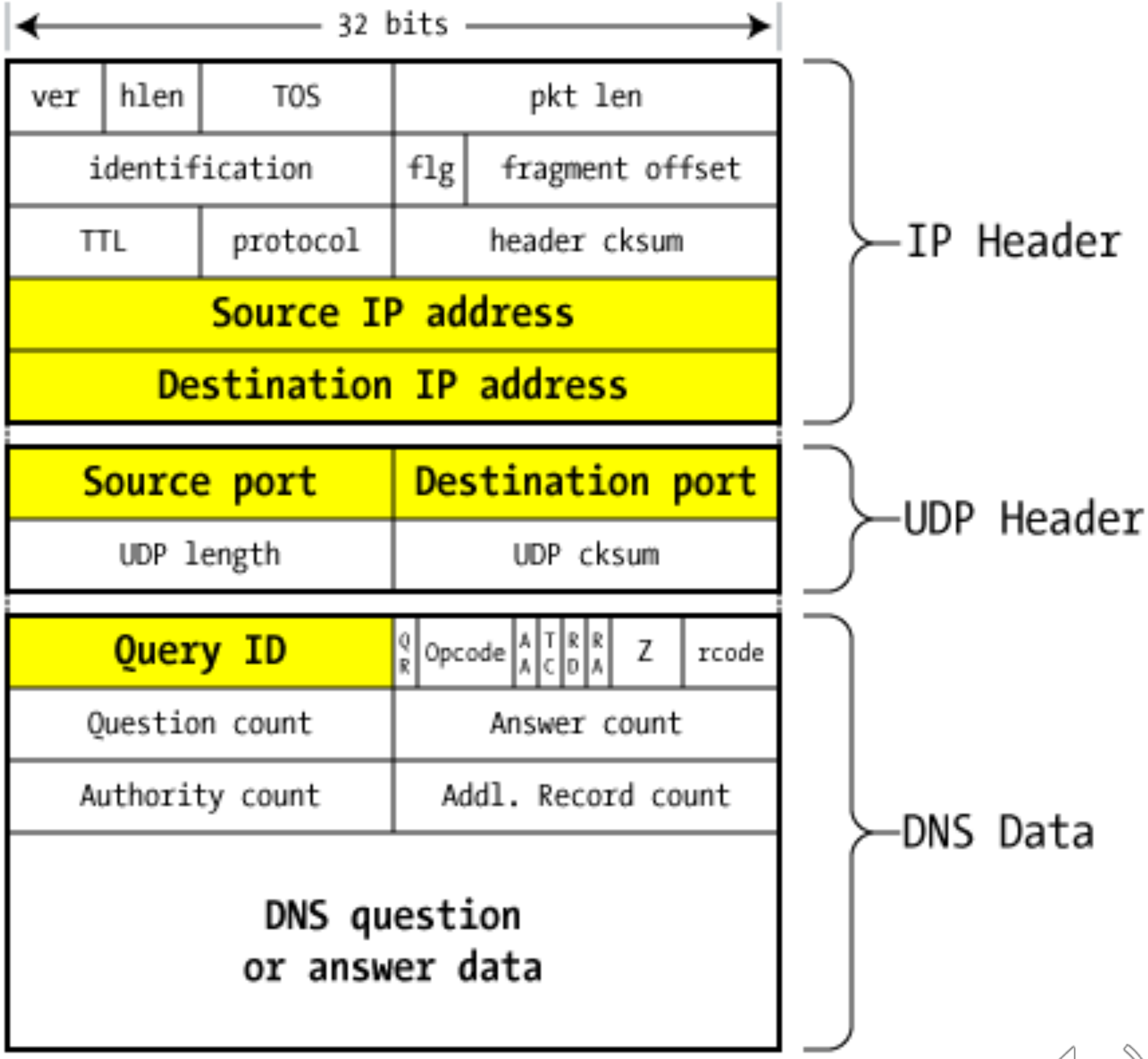
Authoritative vs Caching Name Servers

- Authoritative name server only returns names configured by an original source (e.g. admin)
  - Sets AA (authoritative answer) bit in response
- Caching name server may do lookups to other servers, return indirect/cached results
  - Speeds up queries
  - Both negative and positive responses
  - periodically times out. TTL set by data owner

DNS packet on wire

Query ID is 16-bit random value

We'll walk through the example from Friedl's document

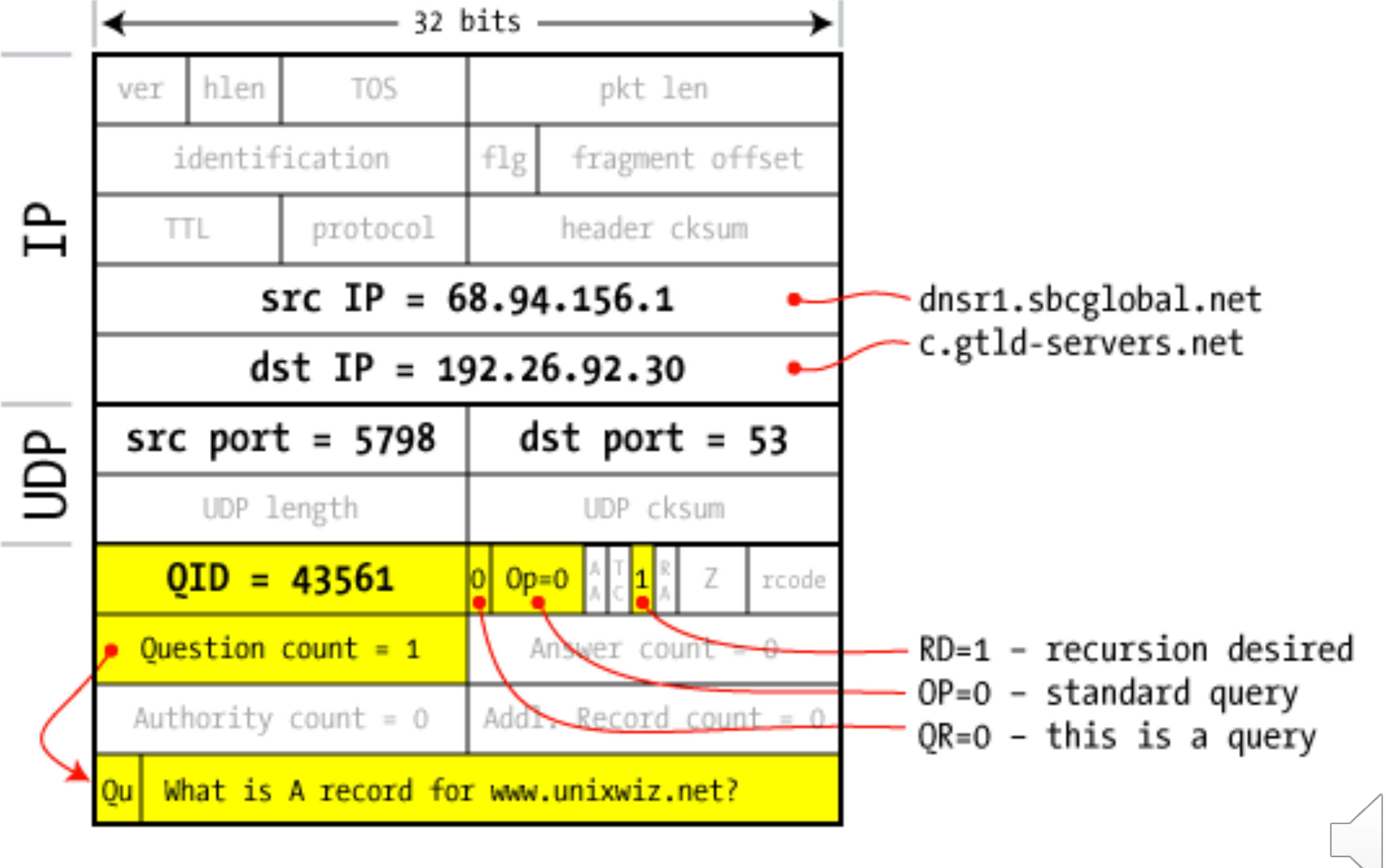


32 bits

ver	hlen	TOS	pkt len						
identification			flg	fragment offset					
TTL	protocol		header cksum						
Source IP address									
Destination IP address									
Source port			Destination port						
UDP length			UDP cksum						
Query ID			QR	Opcode	AA	TC	RD	RA	Z / rcode
Question count			Answer count						
Authority count			Addl. Record count						
DNS question or answer data									

From Friedl explanation of DNS cache poisoning, as are following diagrams

Query from resolver to NS



32 bits

IP

ver | hlen | TOS | pkt len

identification | flg | fragment offset

TTL | protocol | header cksum

src IP = 68.94.156.1

dst IP = 192.26.92.30

UDP

src port = 5798 | dst port = 53

UDP length | UDP cksum

QID = 43561 | 0 | Op=0 | AA | TC | 1 | RA | Z | rcode

Question count = 1 | Answer count = 0

Authority count = 0 | Add'l Record count = 0

Qu | What is A record for www.unixwiz.net?

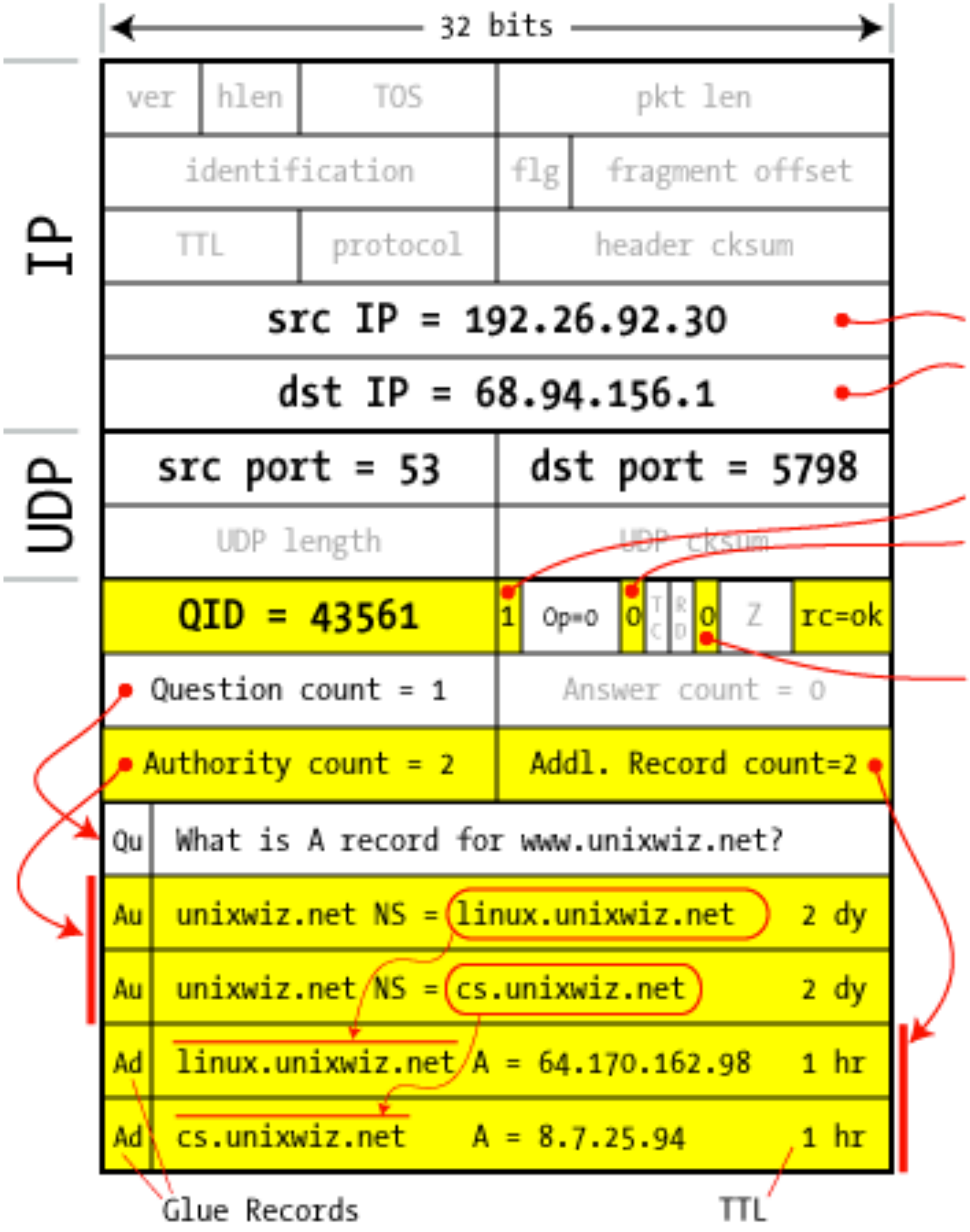
dnsr1.sbcglobal.net

c.gtld-servers.net

RD=1 - recursion desired

OP=0 - standard query

QR=0 - this is a query



32 bits

IP

ver | hlen | TOS | pkt len

identification | flg | fragment offset

TTL | protocol | header cksum

src IP = 192.26.92.30

dst IP = 68.94.156.1

UDP

src port = 53 | dst port = 5798

UDP length | UDP cksum

QID = 43561 | 1 | Op=0 | 0 | TC | RD | 0 | Z | rc=ok

Question count = 1 | Answer count = 0

Authority count = 2 | Addl. Record count=2

Qu What is A record for www.unixwiz.net?

Au unixwiz.net NS = linux.unixwiz.net 2 dy

Au unixwiz.net NS = cs.unixwiz.net 2 dy

Ad linux.unixwiz.net A = 64.170.162.98 1 hr

Ad cs.unixwiz.net A = 8.7.25.94 1 hr

Glue Records

TTL

c.gtld-servers.net

dnsr1.sbcglobal.net

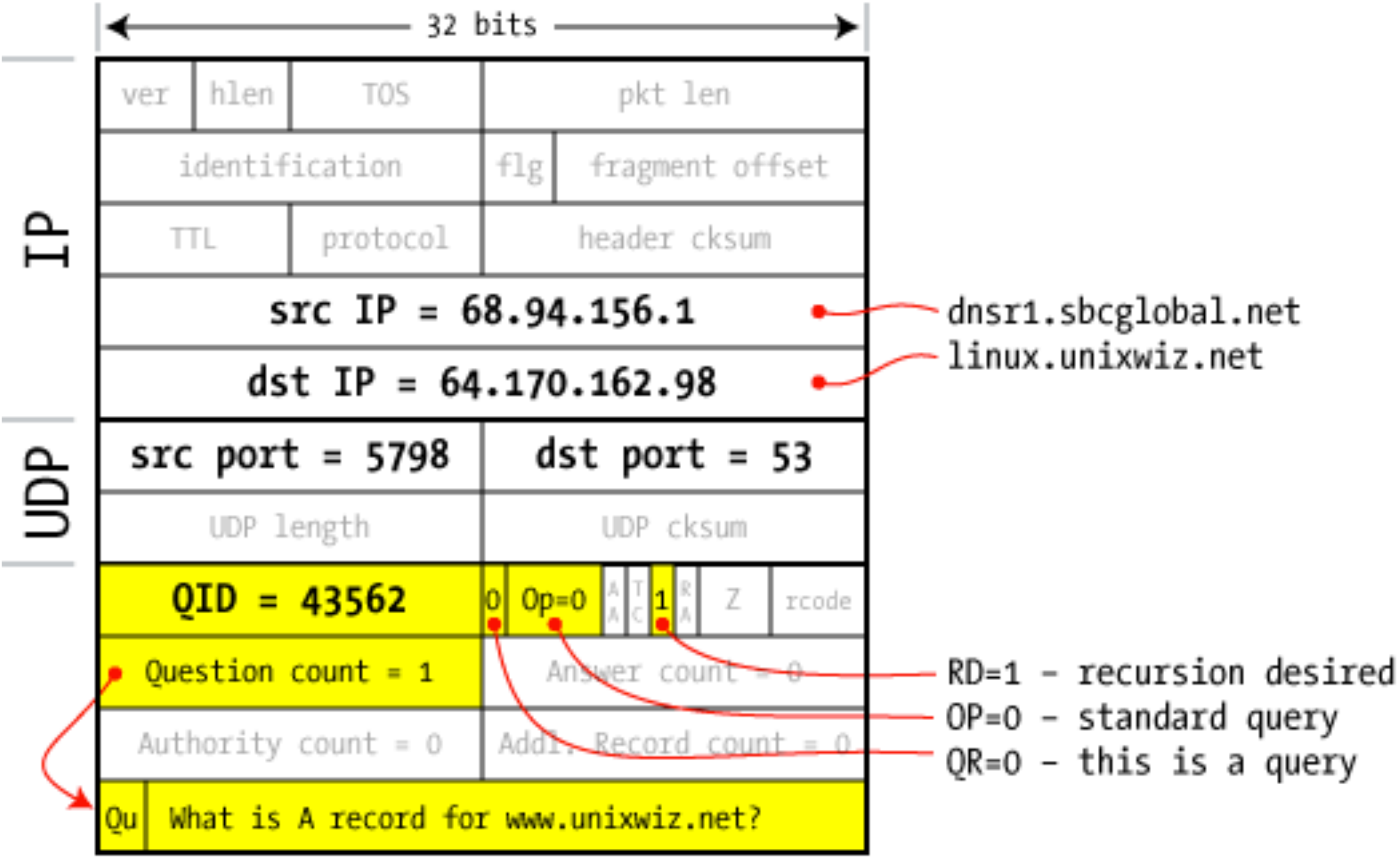
QR=1 - this is a response

AA=0 - not authoritative

RA=0 - recursion unavailable

Response contains IP addr of next NS server (called “glue”)

Response ignored if unrecognized QueryID



32 bits

IP

ver | hlen | TOS | pkt len

identification | flg | fragment offset

TTL | protocol | header cksum

src IP = 68.94.156.1

dst IP = 64.170.162.98

UDP

src port = 5798 | dst port = 53

UDP length | UDP cksum

QID = 43562 | 0 | Op=0 | AA | TC | 1 | RA | Z | rcode

Question count = 1 | Answer count = 0

Authority count = 0 | Addl. Record count = 0

Qu | What is A record for www.unixwiz.net?

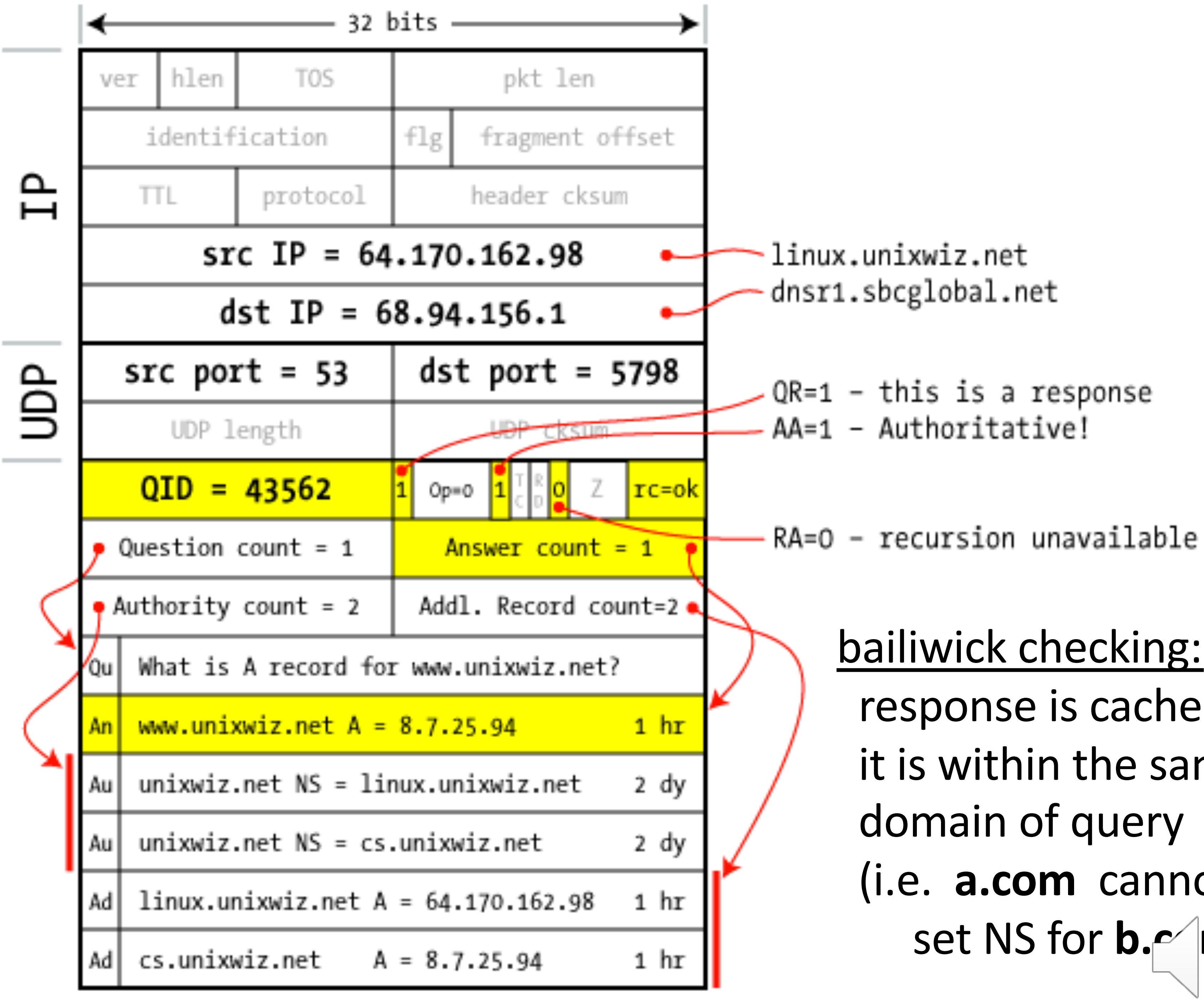
dnsr1.sbcglobal.net

linux.unixwiz.net

RD=1 - recursion desired

OP=0 - standard query

QR=0 - this is a query



32 bits

IP

ver	hlen	TOS	pkt len
identification		flg	fragment offset
TTL	protocol	header cksum	
src IP = 64.170.162.98			
dst IP = 68.94.156.1			

UDP

src port = 53	dst port = 5798
UDP length	UDP cksum

QID = 43562	1	Op=0	1	TC	RD	0	Z	rc=ok

Question count = 1	Answer count = 1
Authority count = 2	Addl. Record count=2

Qu	What is A record for www.unixwiz.net?	
An	www.unixwiz.net A = 8.7.25.94	1 hr
Au	unixwiz.net NS = linux.unixwiz.net	2 dy
Au	unixwiz.net NS = cs.unixwiz.net	2 dy
Ad	linux.unixwiz.net A = 64.170.162.98	1 hr
Ad	cs.unixwiz.net A = 8.7.25.94	1 hr

linux.unixwiz.net

dnsr1.sbcglobal.net

QR=1 - this is a response

AA=1 - Authoritative!

RA=0 - recursion unavailable

<u>bailiwick checking:</u>

response is cached if it is within the same domain of query (i.e. **a.com** cannot set NS for **b.com**)

Here we go again…

- What security checks are in place?
  - Random query ID’s to link responses to queries
  - Bailiwick checking (sanity check on response)
- No authentication
  - DNSsec is supposed to fix this but no one uses it yet
- Many things trust hostname to IP mapping
  - Browser same-origin policy
  - URL address bar

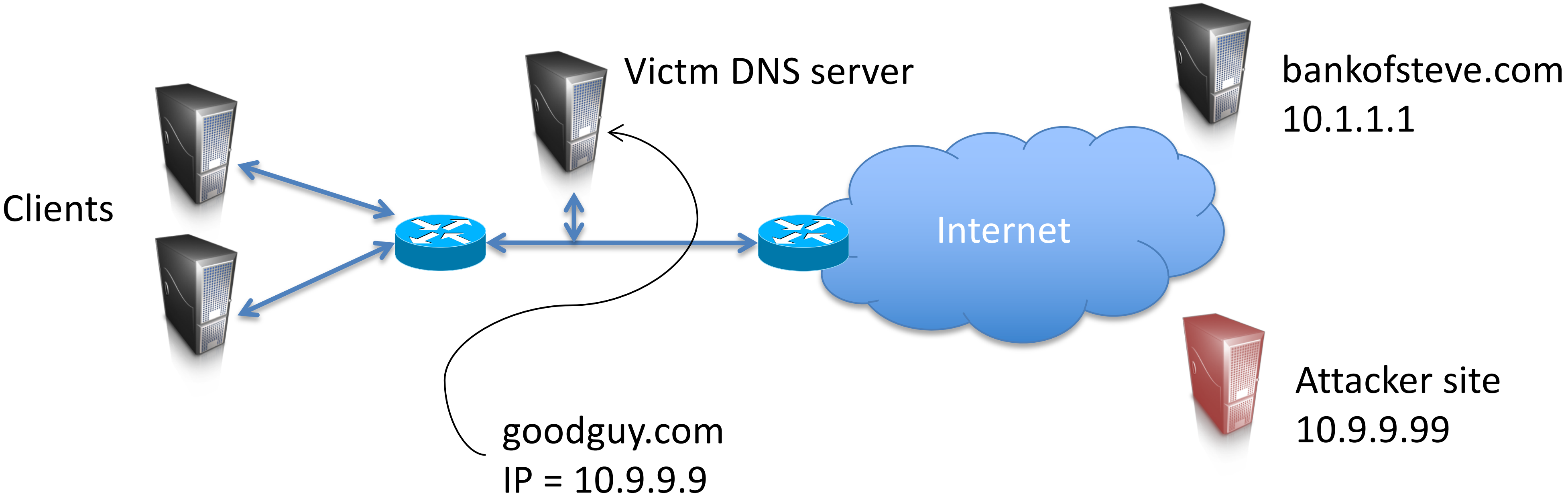
What are clear problems?

- Corrupted nameservers
- Intercept & manipulate requests
- Other obvious issues?

DDoS against DNS

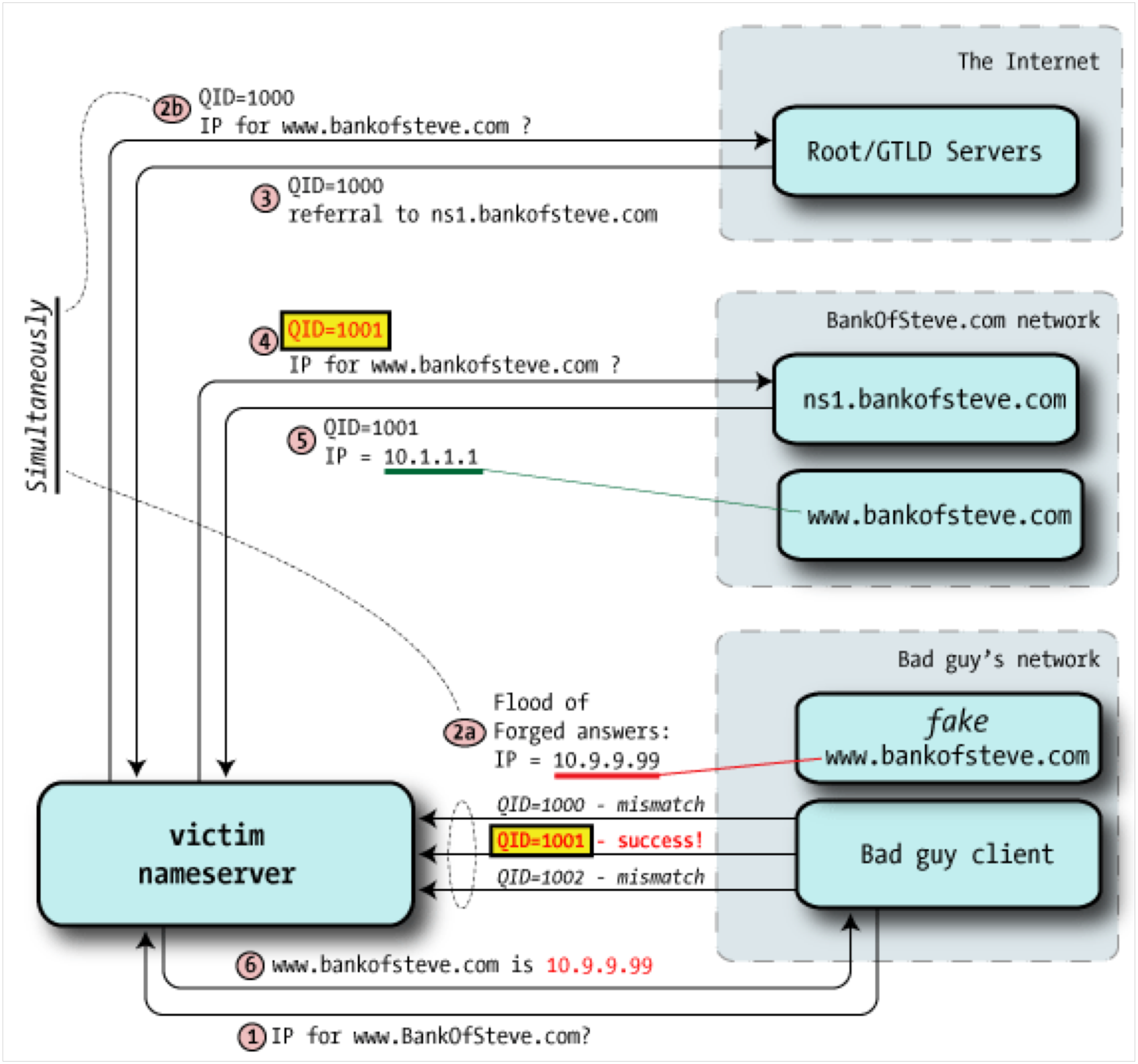
- Denial of Service
  - take down DNS server, clients can’t use Internet
  - Feb 6, 2007 attack against 6 of 13 root servers:
    - 2 suffered very badly
    - Others experienced heavy traffic
- DoD purportedly has interesting response:
  - “In the event of a massive cyberattack against the country that was perceived as originating from a foreign source, the United States would consider launching a counterattack or bombing the source of the cyberattack, Hall said. But he noted the preferred route would be warning the source to shut down the attack before a military response.”
  - http://www.computerworld.com/s/article/9010921/RSA_U.S._cyber_counterattack_Bomb_one_way_or_the_other

DNS cache poisoning



How might an attacker do this?

Assume DNS server uses predictable UDP port



The Internet

Root/GTLD Servers

2b QID=1000
IP for www.bankofsteve.com ?

3 QID=1000
referral to ns1.bankofsteve.com

Simultaneously

BankOfSteve.com network

ns1.bankofsteve.com

www.bankofsteve.com

4 QID=1001
IP for www.bankofsteve.com ?

5 QID=1001
IP = 10.1.1.1

Bad guy's network

fake
www.bankofsteve.com

Bad guy client

2a Flood of
Forged answers:
IP = 10.9.9.99

QID=1000 - mismatch

QID=1001 - success!

QID=1002 - mismatch

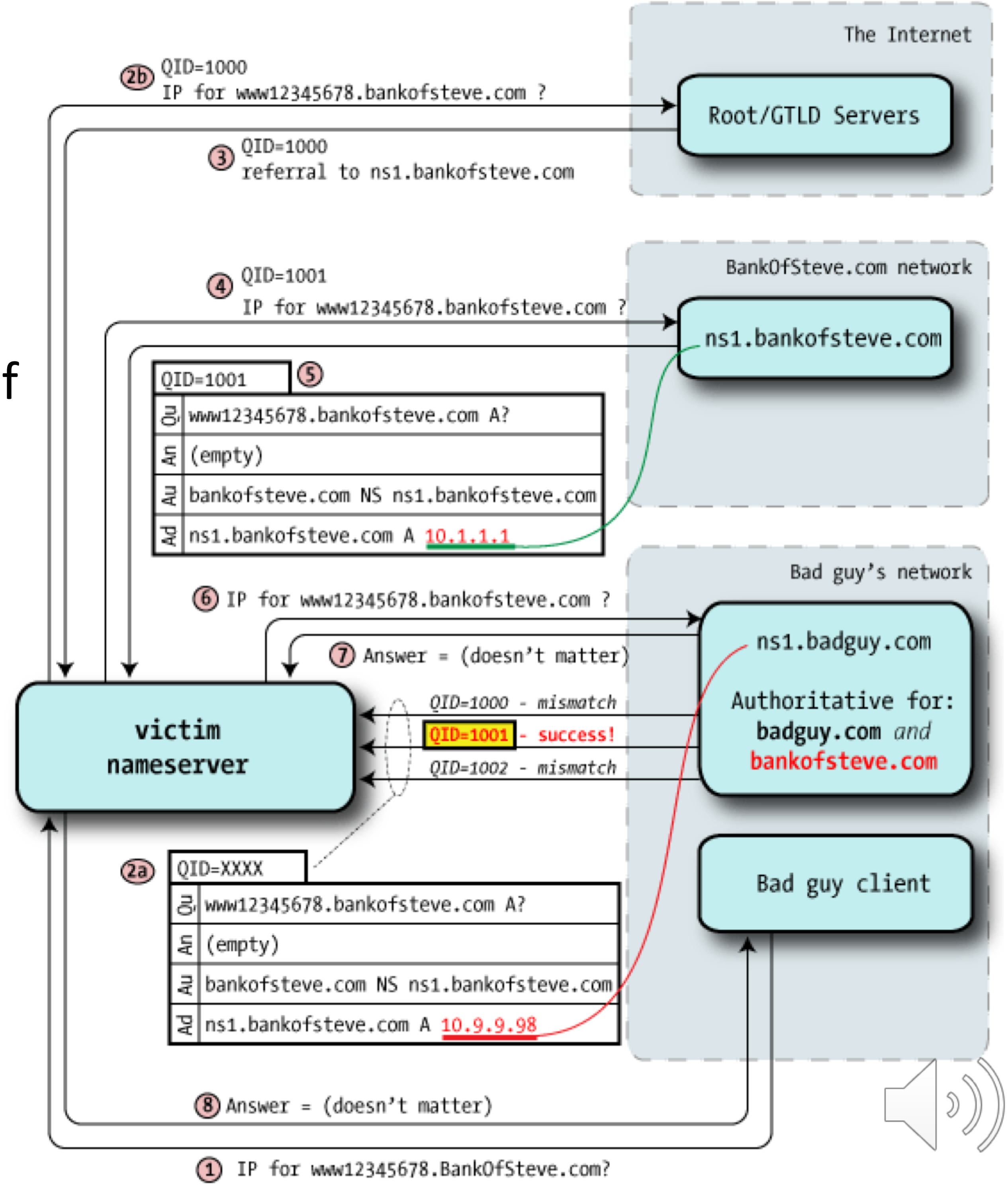
victim
nameserver

6 www.bankofsteve.com is 10.9.9.99

1 IP for www.BankOfSteve.com?

Another idea:

- Poison cache for NS record instead
- Now can take over all of second level domain


The Internet
Root/GTLD Servers
2b QID=1000
IP for www12345678.bankofsteve.com ?
3 QID=1000
referral to ns1.bankofsteve.com
BankOfSteve.com network
ns1.bankofsteve.com
4 QID=1001
IP for www12345678.bankofsteve.com ?
5 QID=1001
Qu www12345678.bankofsteve.com A?
An (empty)
Au bankofsteve.com NS ns1.bankofsteve.com
Ad ns1.bankofsteve.com A 10.1.1.1
Bad guy's network
6 IP for www12345678.bankofsteve.com ?
7 Answer = (doesn't matter)
ns1.badguy.com
Authoritative for:
badguy.com and
bankofsteve.com
victim
nameserver
QID=1000 - mismatch
QID=1001 - success!
QID=1002 - mismatch
2a QID=XXXX
Qu www12345678.bankofsteve.com A?
An (empty)
Au bankofsteve.com NS ns1.bankofsteve.com
Ad ns1.bankofsteve.com A 10.9.9.98
Bad guy client
8 Answer = (doesn't matter)
1 IP for www12345678.BankOfSteve.com?

How many tries does this require?

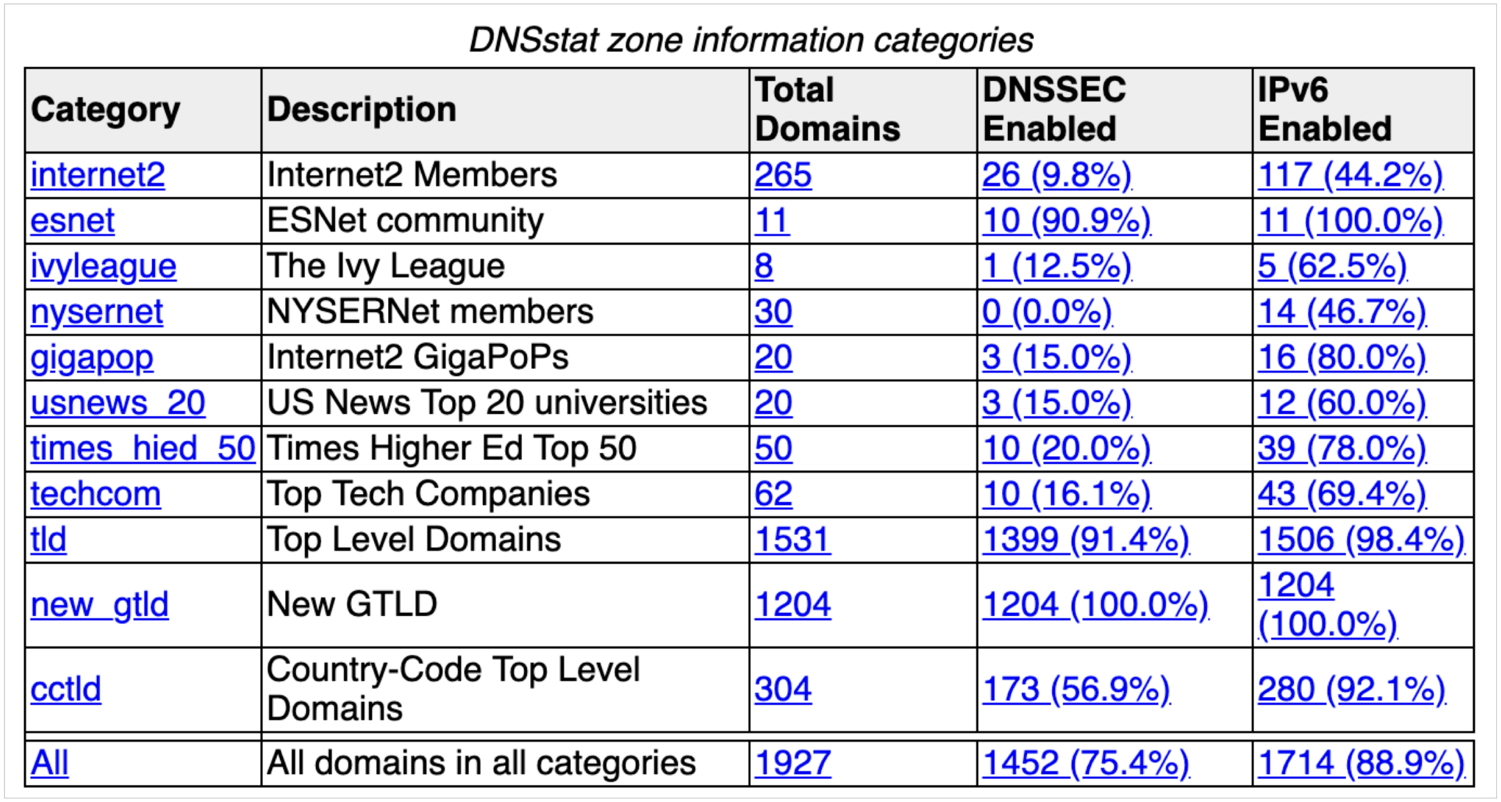
- Send flood
- Good chance of success in 10 seconds

Defenses

- Query ID size is fixed at 16 bits
- Repeat each query with fresh Query ID
  - Doubles the space
- Randomize UDP source port ports
  - Dan Bernstein's DJBDNS did this already
  - Now other implementations do, too
- DNSsec
  - Cryptographically sign DNS responses, verify via chain of trust from roots on down

DNSsec

- Authenticated DNS protocol
- Used by TLDs :)
- But no one else :(



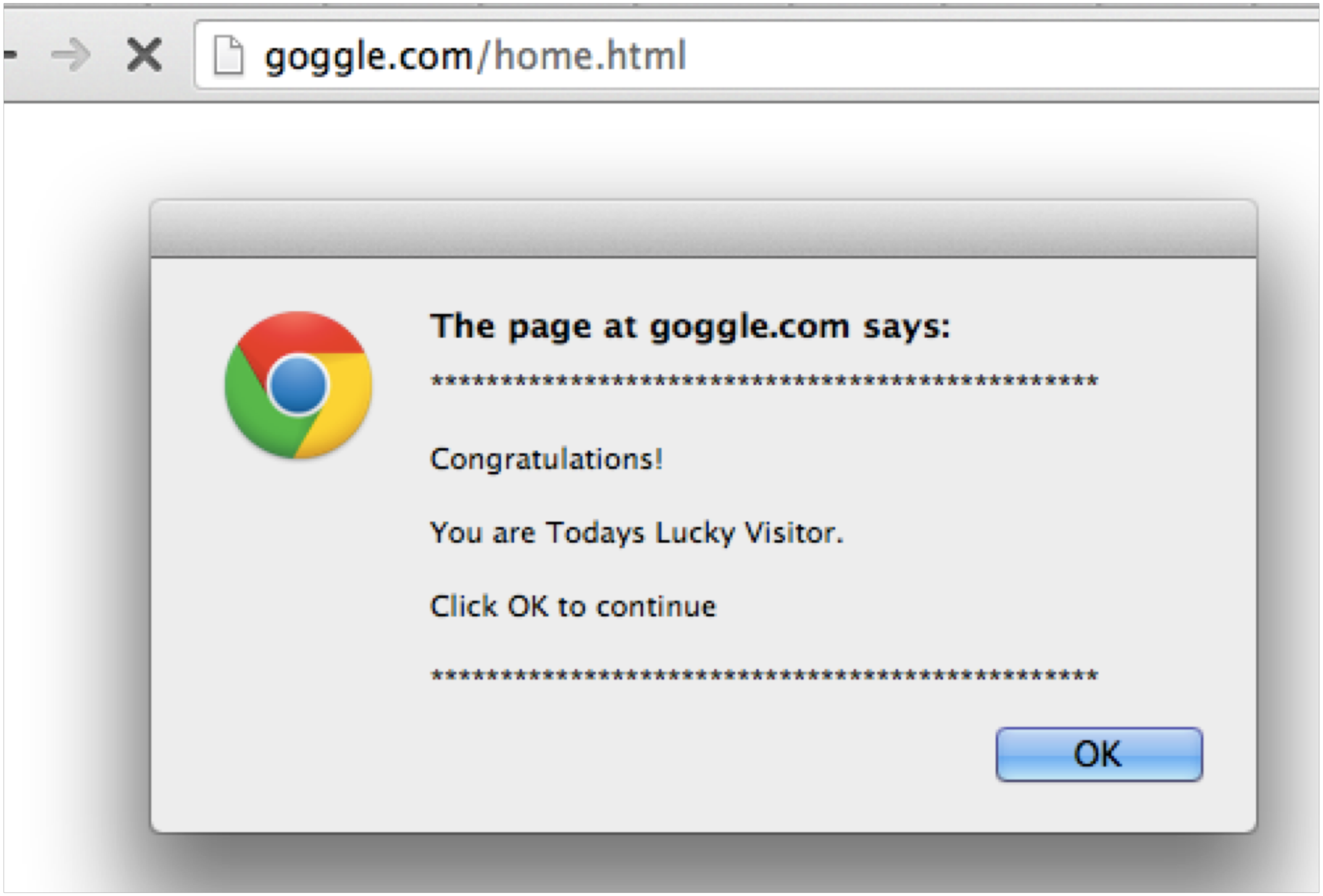
DNSstat zone information categories

Category	Description	Total Domains	DNSSEC Enabled	IPv6 Enabled
internet2	Internet2 Members	265	26 (9.8%)	117 (44.2%)
esnet	ESNet community	11	10 (90.9%)	11 (100.0%)
ivyleague	The Ivy League	8	1 (12.5%)	5 (62.5%)
nysernet	NYSERNet members	30	0 (0.0%)	14 (46.7%)
gigapop	Internet2 GigaPoPs	20	3 (15.0%)	16 (80.0%)
usnews_20	US News Top 20 universities	20	3 (15.0%)	12 (60.0%)
times_hied_50	Times Higher Ed Top 50	50	10 (20.0%)	39 (78.0%)
techcom	Top Tech Companies	62	10 (16.1%)	43 (69.4%)
tld	Top Level Domains	1531	1399 (91.4%)	1506 (98.4%)
new_gtld	New GTLD	1204	1204 (100.0%)	1204 (100.0%)
cctld	Country-Code Top Level Domains	304	173 (56.9%)	280 (92.1%)
All	All domains in all categories	1927	1452 (75.4%)	1714 (88.9%)

[https://www.huque.com/app/dnsstat/] retrieved: March 21, 2019

Phishing is common problem

- Typo squatting:
  - www.ca.wisc.edu
  - www.goggle.com
- Other shenanigans:
  - www.badguy.com/(256 characters of filler)/www.google.com
- Phishing attacks
  - These just trick users into thinking a malicious domain name is the real one



The page at goggle.com says:

****

Congratulations!

You are Todays Lucky Visitor.

Click OK to continue

****