ROYAL INSTITUTE
OF TECHNOLOGY

Networked Systems Security

Domain Name System Security

Panos Papadimitratos
Networked Systems Security Group
www.ee.kth.se/nss

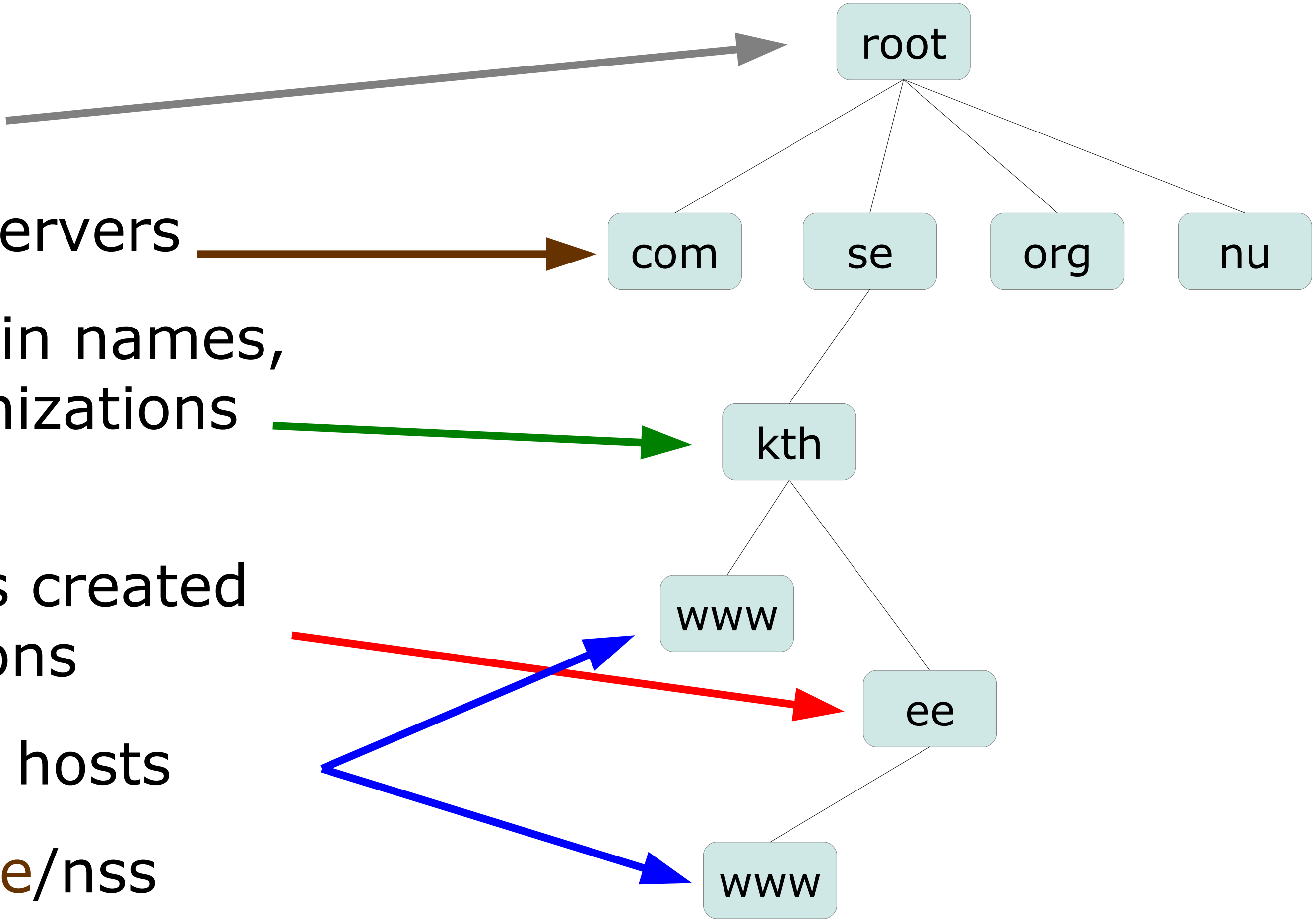
Domain Name System (DNS)

- Translate names to IP addresses
  - www.ee.kth.se q 130.237.45.45
- End-hosts query DNS servers for name-to-IP translation
- Requests are handled in a recursive manner
  - Tree-like structure

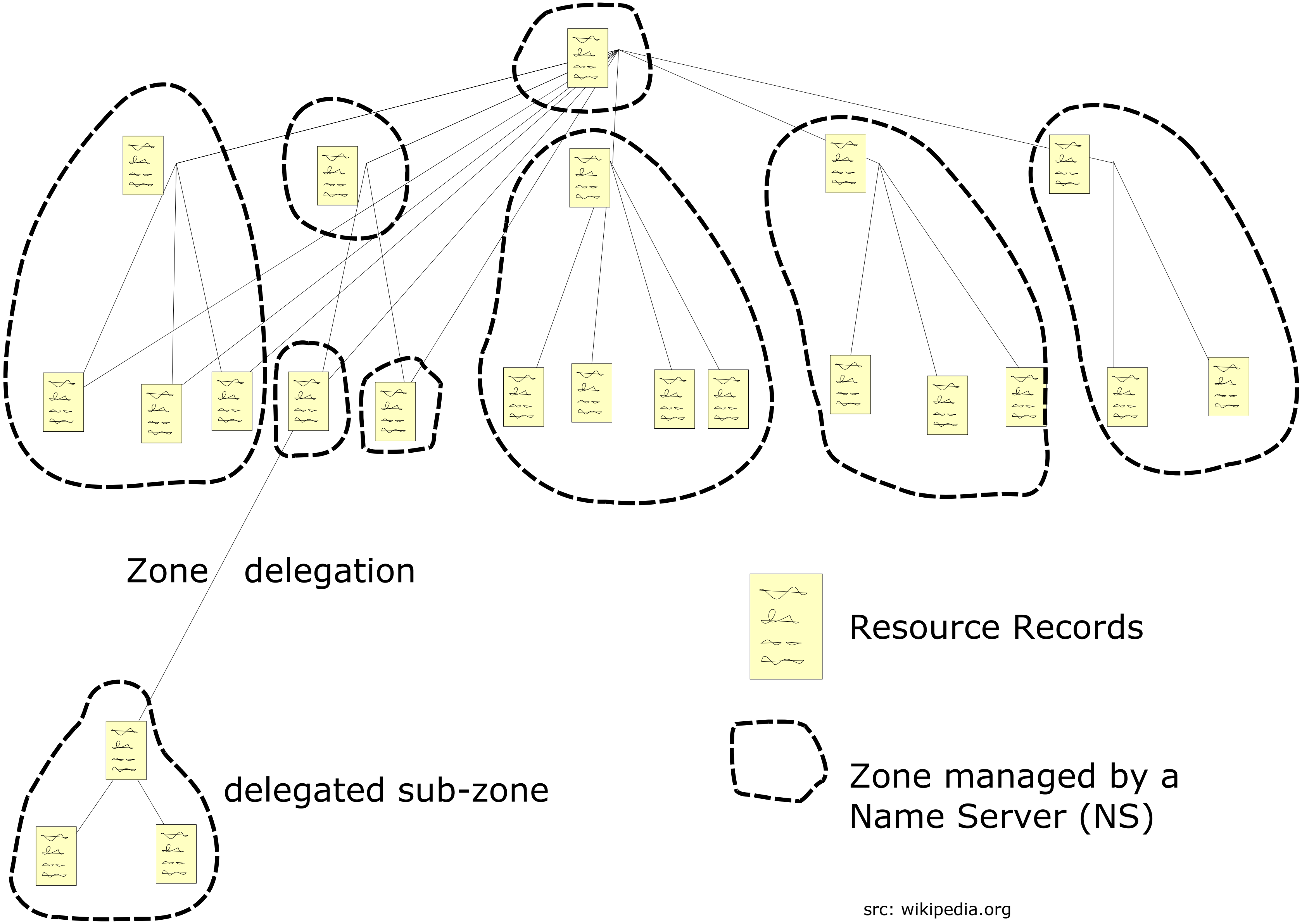
- Note: DNS was not designed with security in mind

Tree structure of domain names

- Internet root
- Top-level domain servers
- Second-level domain names, registered by organizations (or individuals)
- Sub-domain names created by such organizations
- Names assigned to hosts
- E.g., www.ee.kth.se/nss



Tree structure of authorities



Zone delegation

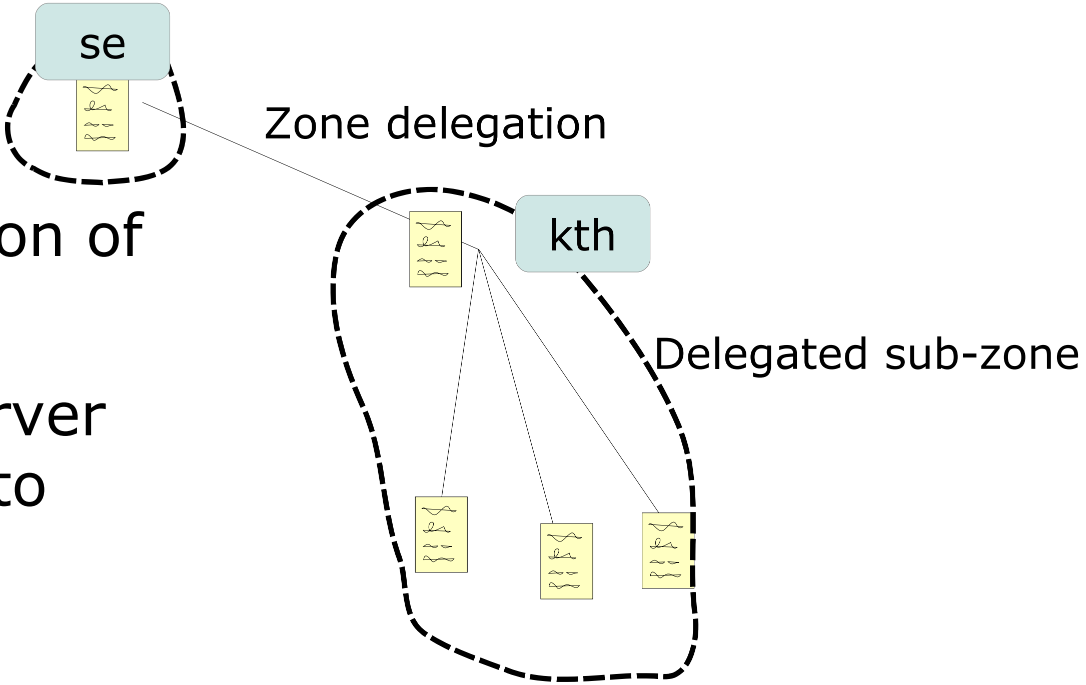
delegated sub-zone

Resource Records

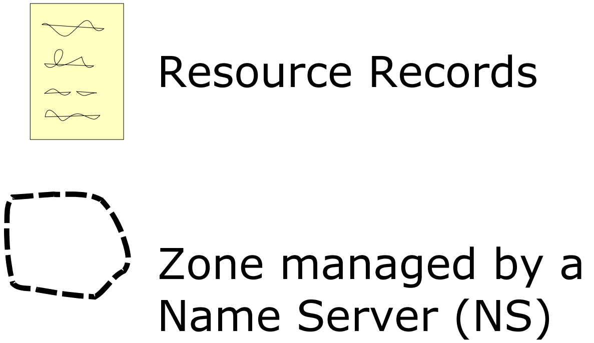
Zone managed by a
Name Server (NS)

src: wikipedia.org

Tree structure of authorities (cont'd)



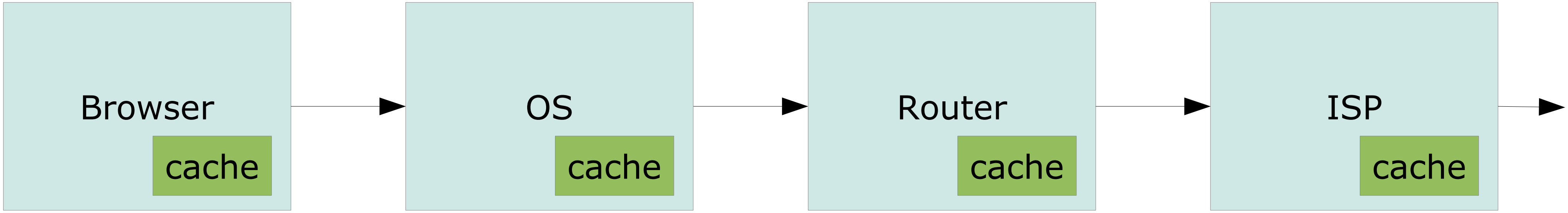
- Zone delegation is delegation of *trust*
- Example: the .se Name Server (NS) trusts the .kth.se NS to resolve *.kth.se
- .se has no say over .kth.se other than the delegation itself



src: wikipedia.org

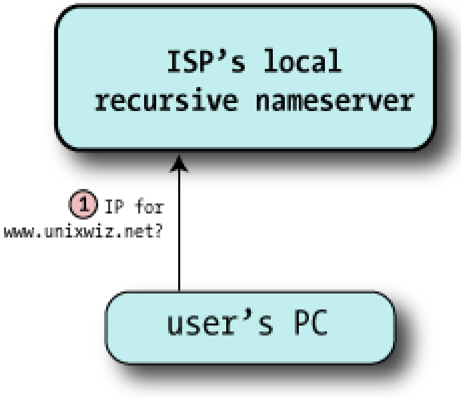
Recursive requests

- Clients/end-hosts get the answer from the nearest NS possible



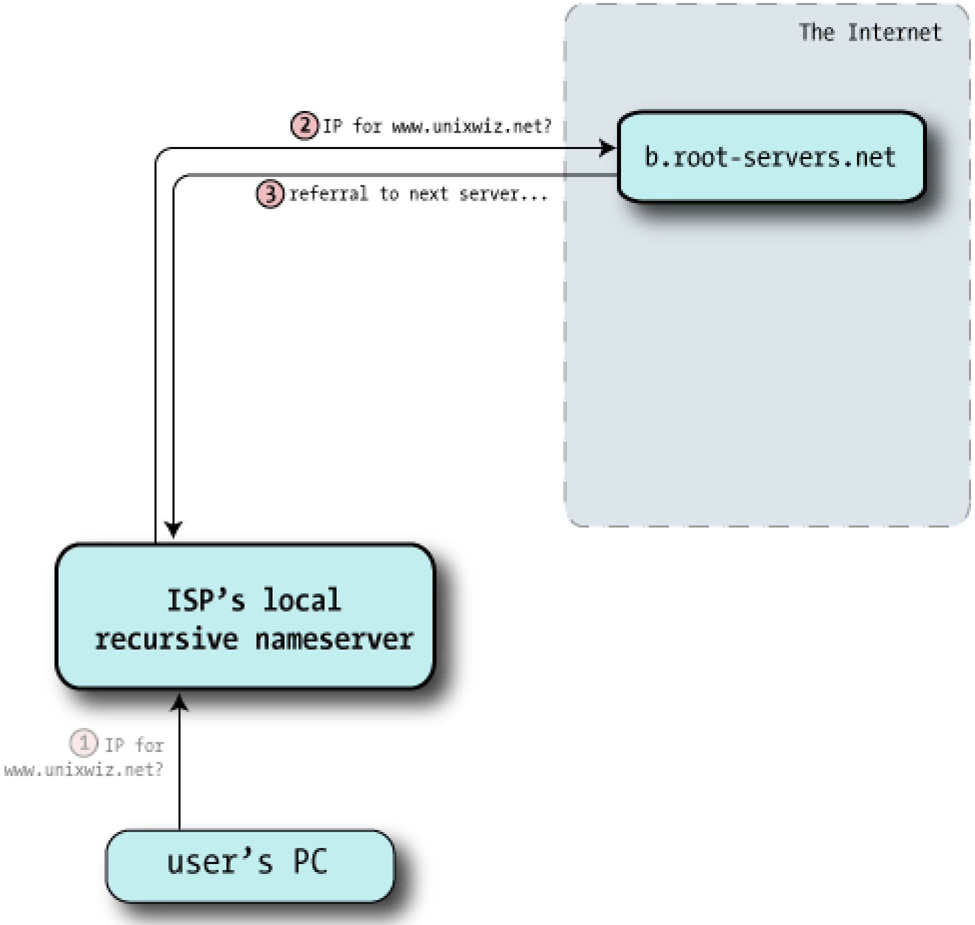
src: after wikipedia.org

Resolution example



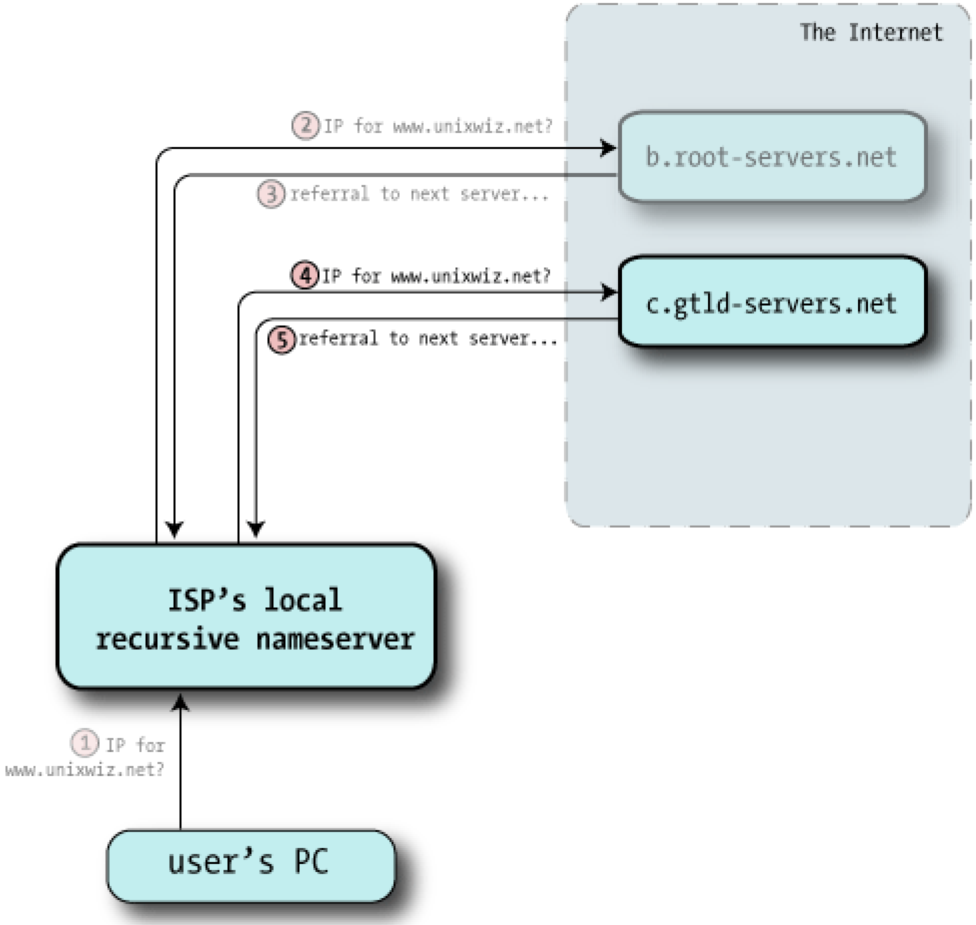
src: Steve Friedl, unixwiz.net

Resolution example (cont'd)


The Internet
2 IP for www.unixwiz.net?
b.root-servers.net
3 referral to next server...
ISP's local recursive nameserver
1 IP for www.unixwiz.net?
user's PC

src: Steve Friedl, unixwiz.net

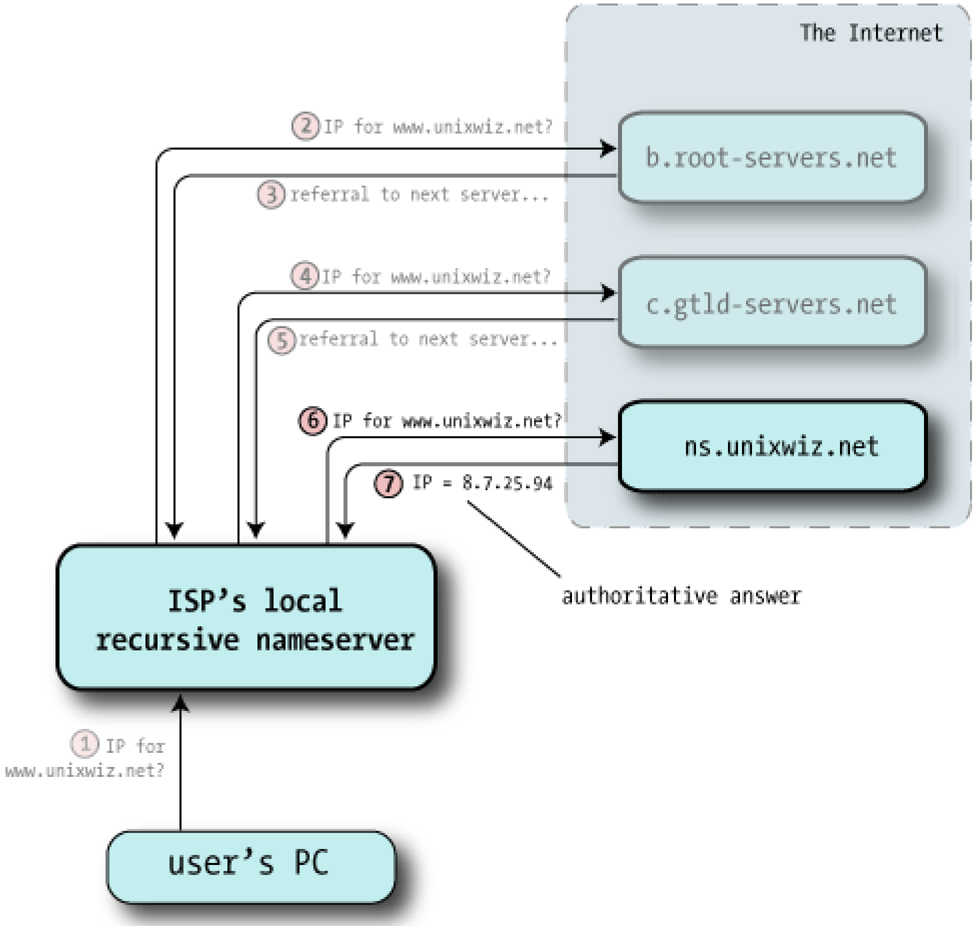
Resolution example (cont'd)


The Internet
2 IP for www.unixwiz.net?
b.root-servers.net
3 referral to next server...
4 IP for www.unixwiz.net?
c.gtld-servers.net
5 referral to next server...
ISP's local recursive nameserver
1 IP for www.unixwiz.net?
user's PC

src: Steve Friedl, unixwiz.net

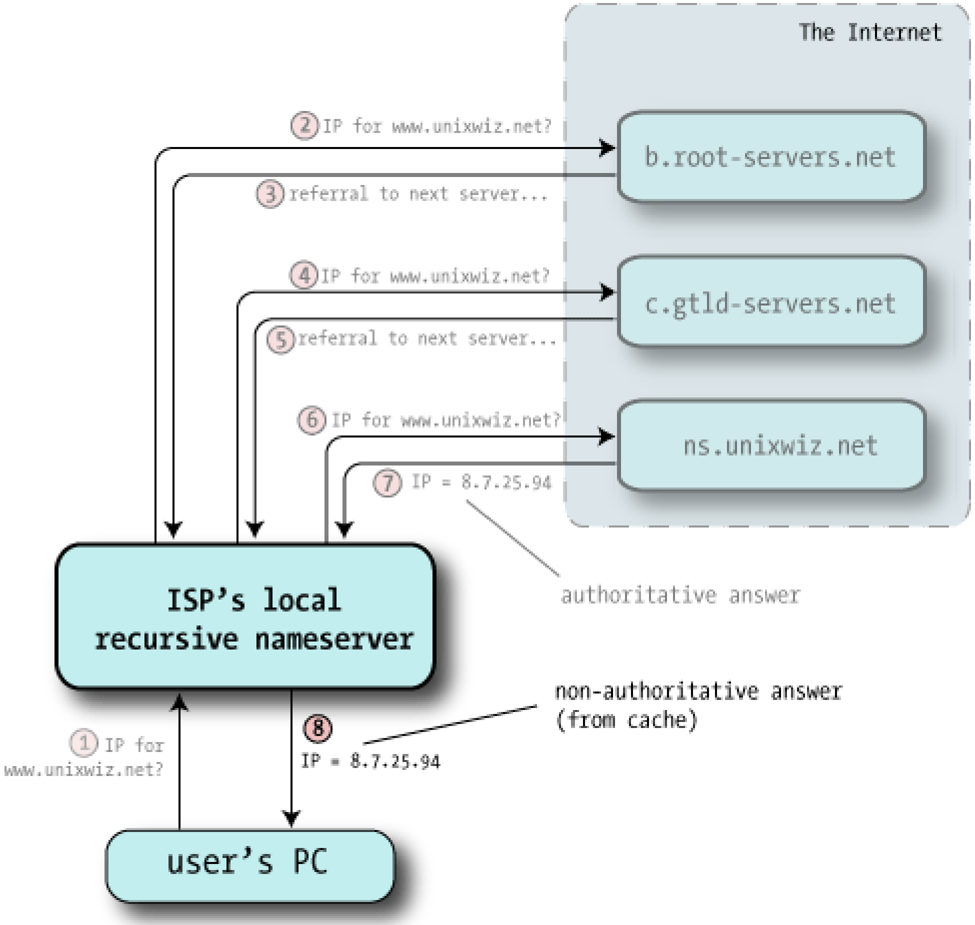
ROYAL INSTITUTE
OF TECHNOLOGY

Resolution example (cont'd)


The Internet
2 IP for www.unixwiz.net?
b.root-servers.net
3 referral to next server...
4 IP for www.unixwiz.net?
c.gtld-servers.net
5 referral to next server...
6 IP for www.unixwiz.net?
ns.unixwiz.net
7 IP = 8.7.25.94
authoritative answer
ISP's local recursive nameserver
1 IP for www.unixwiz.net?
user's PC

src: Steve Friedl, unixwiz.net

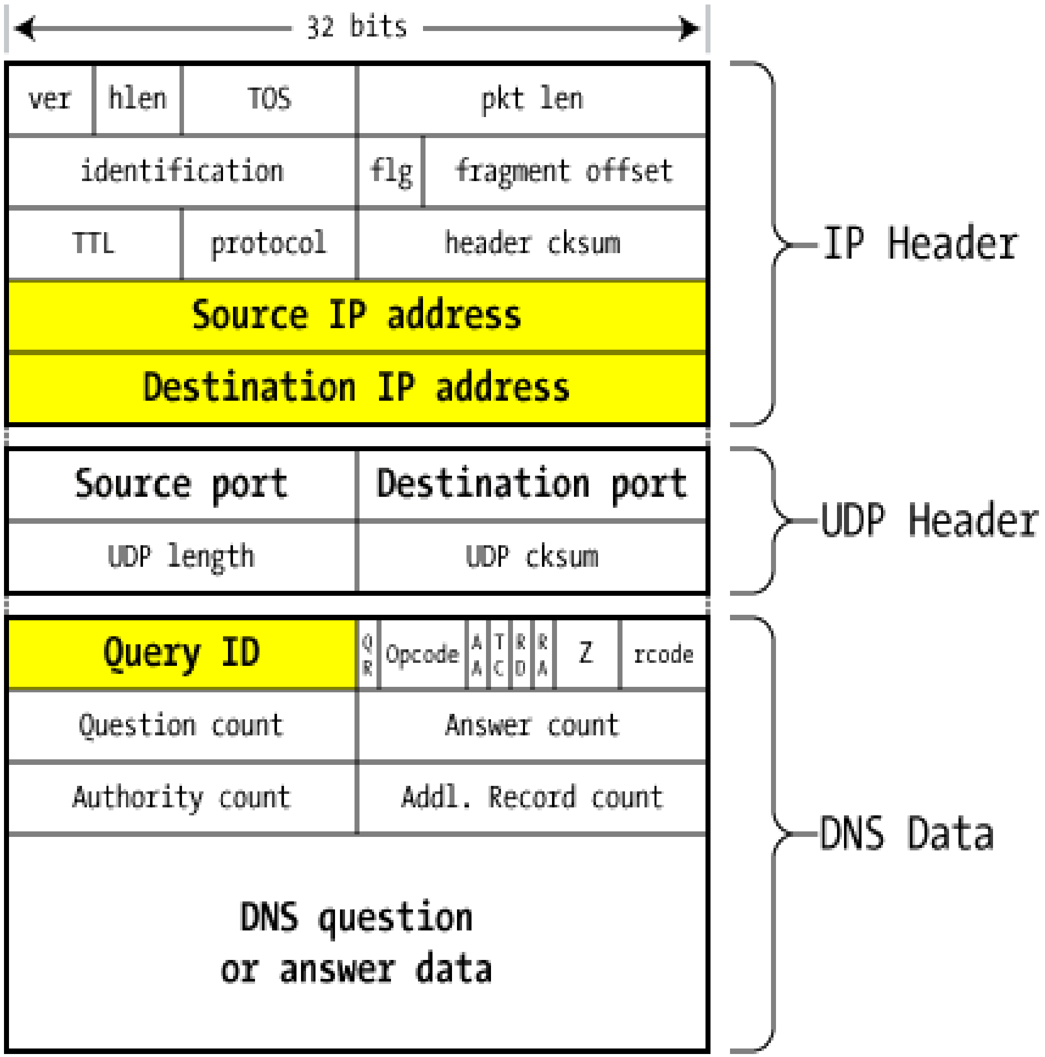
Resolution example (cont'd)


The Internet
2 IP for www.unixwiz.net?
b.root-servers.net
3 referral to next server...
4 IP for www.unixwiz.net?
c.gtld-servers.net
5 referral to next server...
6 IP for www.unixwiz.net?
ns.unixwiz.net
7 IP = 8.7.25.94
authoritative answer
ISP's local recursive nameserver
non-authoritative answer (from cache)
1 IP for www.unixwiz.net?
8 IP = 8.7.25.94
user's PC

src: Steve Friedl, unixwiz.net

DNS query

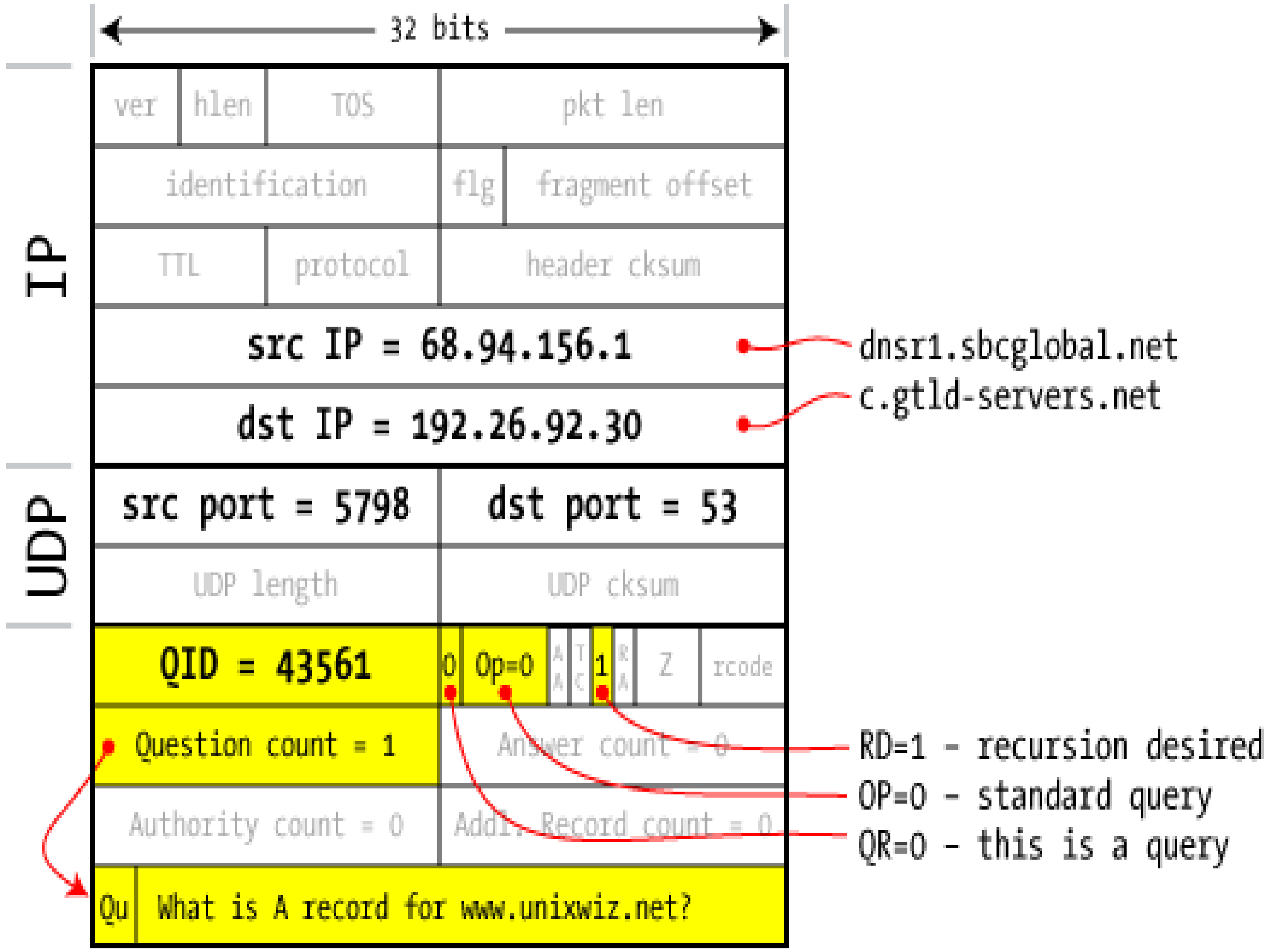
- Query ID is unique per query and links it to the response
- 16 bits of randomizable data



src: Steve Friedl, unixwiz.net

Query example

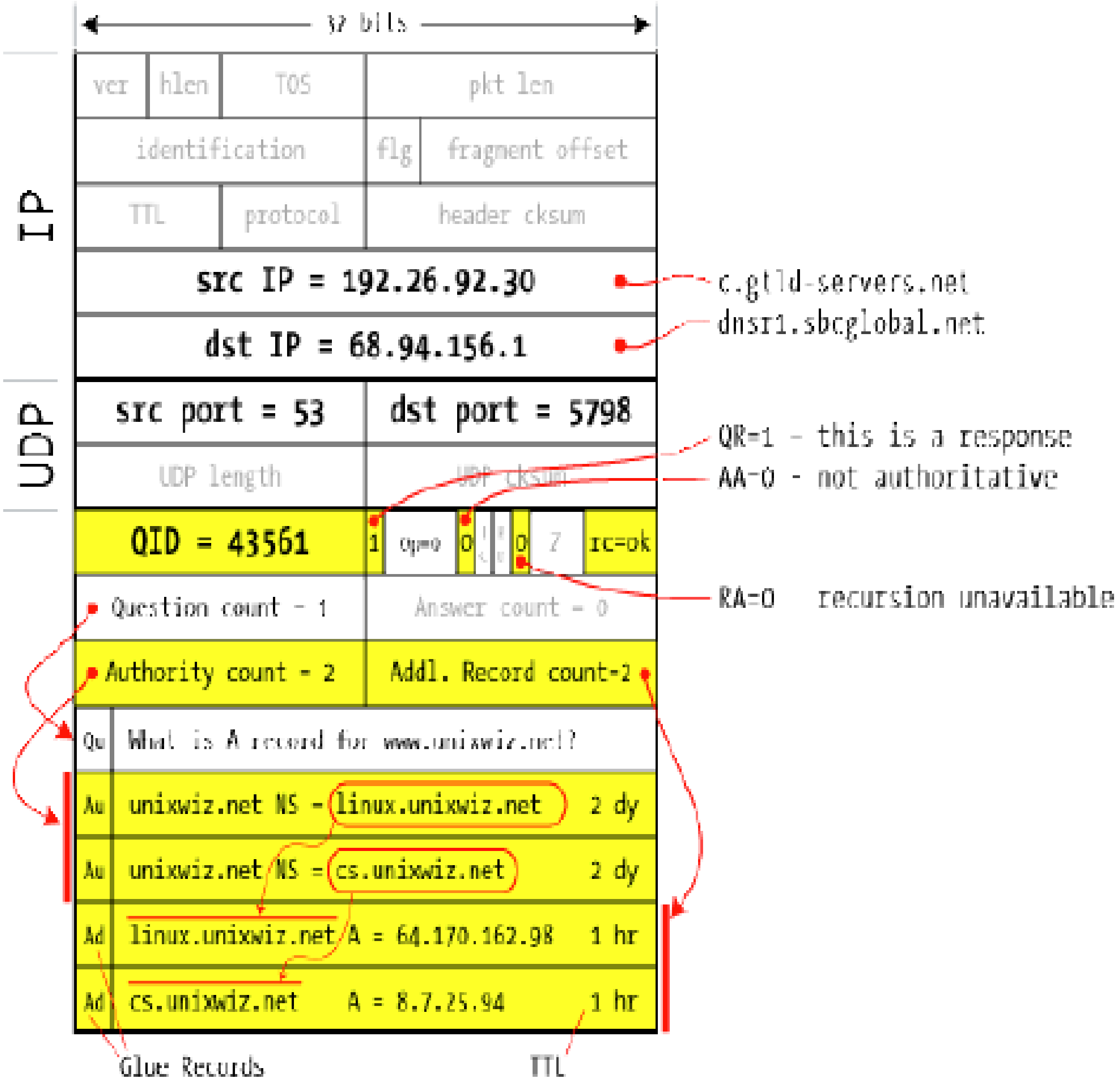
- DNS query to c.gtld-servers.net
- Gets QID 43561



src: Steve Friedl, unixwiz.net

Query example (cont'd)

- DNS response from c.gtld-servers.net
- Identified by QID
- Unknown address: Response with next NS (name and IP)
- DNS glue records
    - IP addresses of NSs within the queried domain
    - What would happen without them?



32 bits

IP

ver | hlen | TOS | pkt len

identification | flg | fragment offset

TTL | protocol | header cksum

src IP = 192.26.92.30 — c.gtld-servers.net

dst IP = 68.94.156.1 — dnsr1.sbcglobal.net

UDP

src port = 53 | dst port = 5798

UDP length | UDP cksum

QID = 43561 | 1 | Op=0 | 0 | | | 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

QR=1 - this is a response

AA=0 - not authoritative

RA=0 recursion unavailable

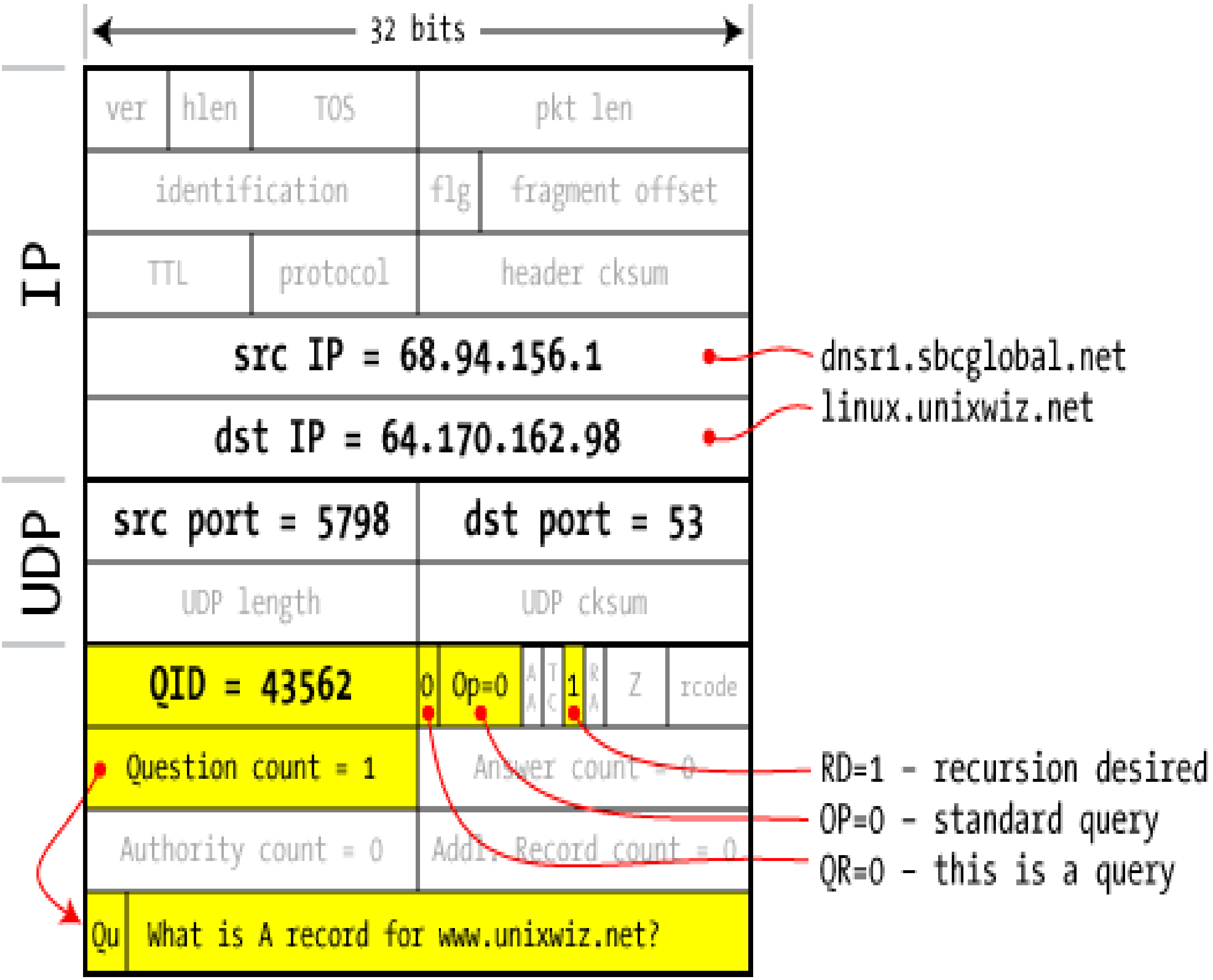
Glue Records

TTL

src: Steve Friedl, unixwiz.net

Query example (cont'd)

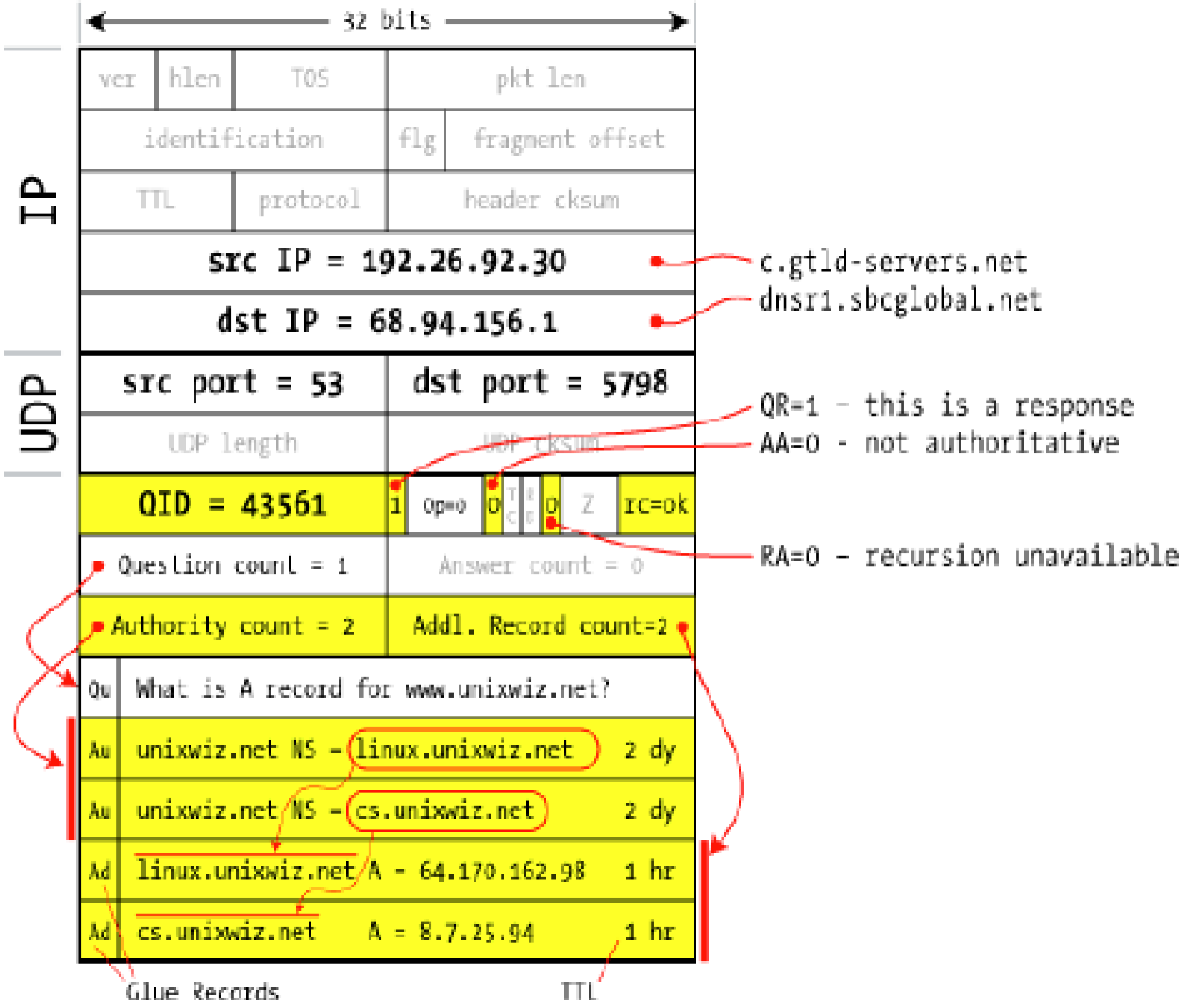
- DNS query to linux.unixwiz.net
- New QID
- Same sort of request



src: Steve Friedl, unixwiz.net

Query example (cont'd)

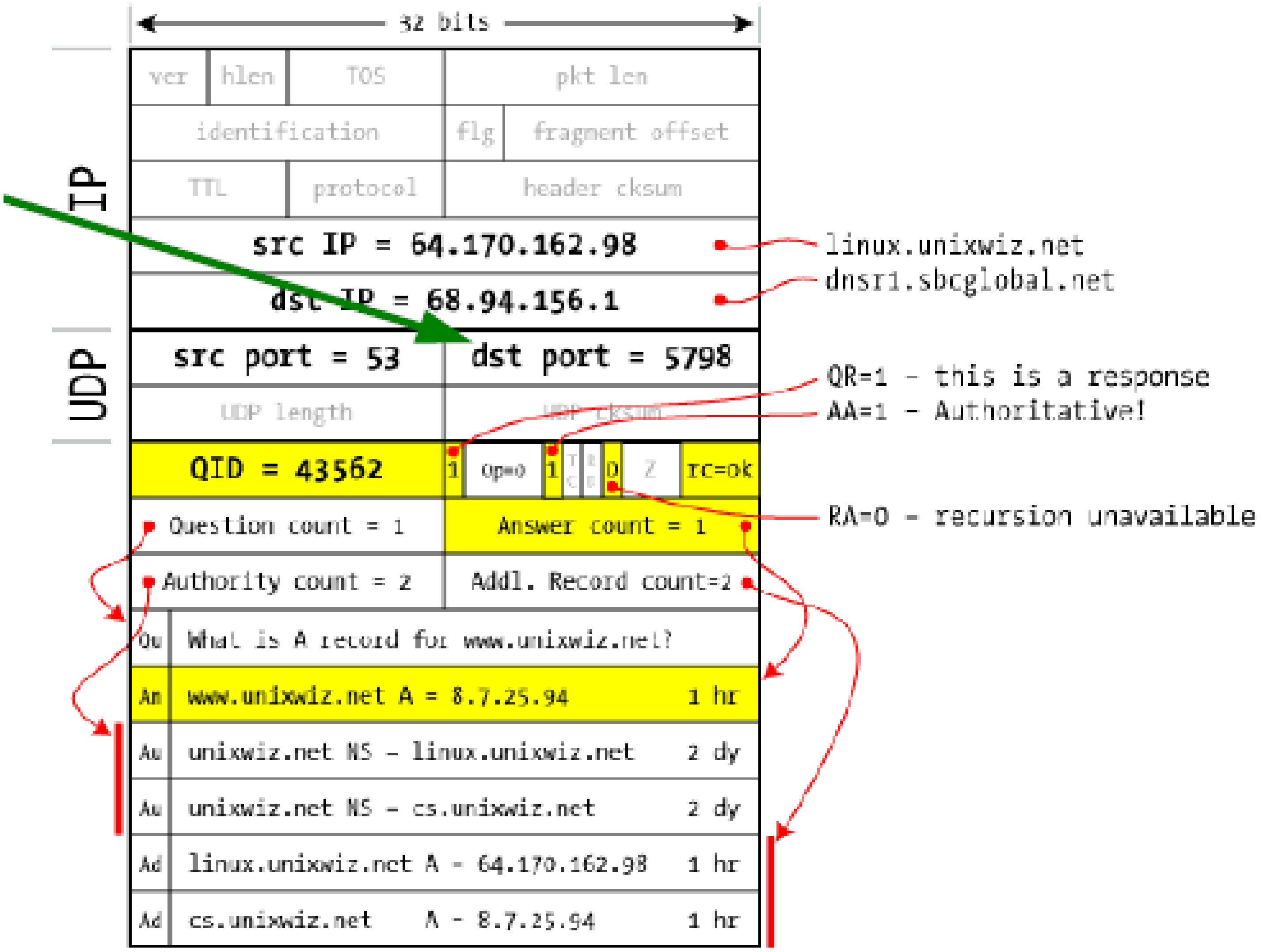
- DNS authoritative response from linux.unixwiz.net
- Linked by QID
- We got our answer



src: Steve Friedl, unixwiz.net

Checking the response

- Same UDP port we sent it from


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 | T C | R D | 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

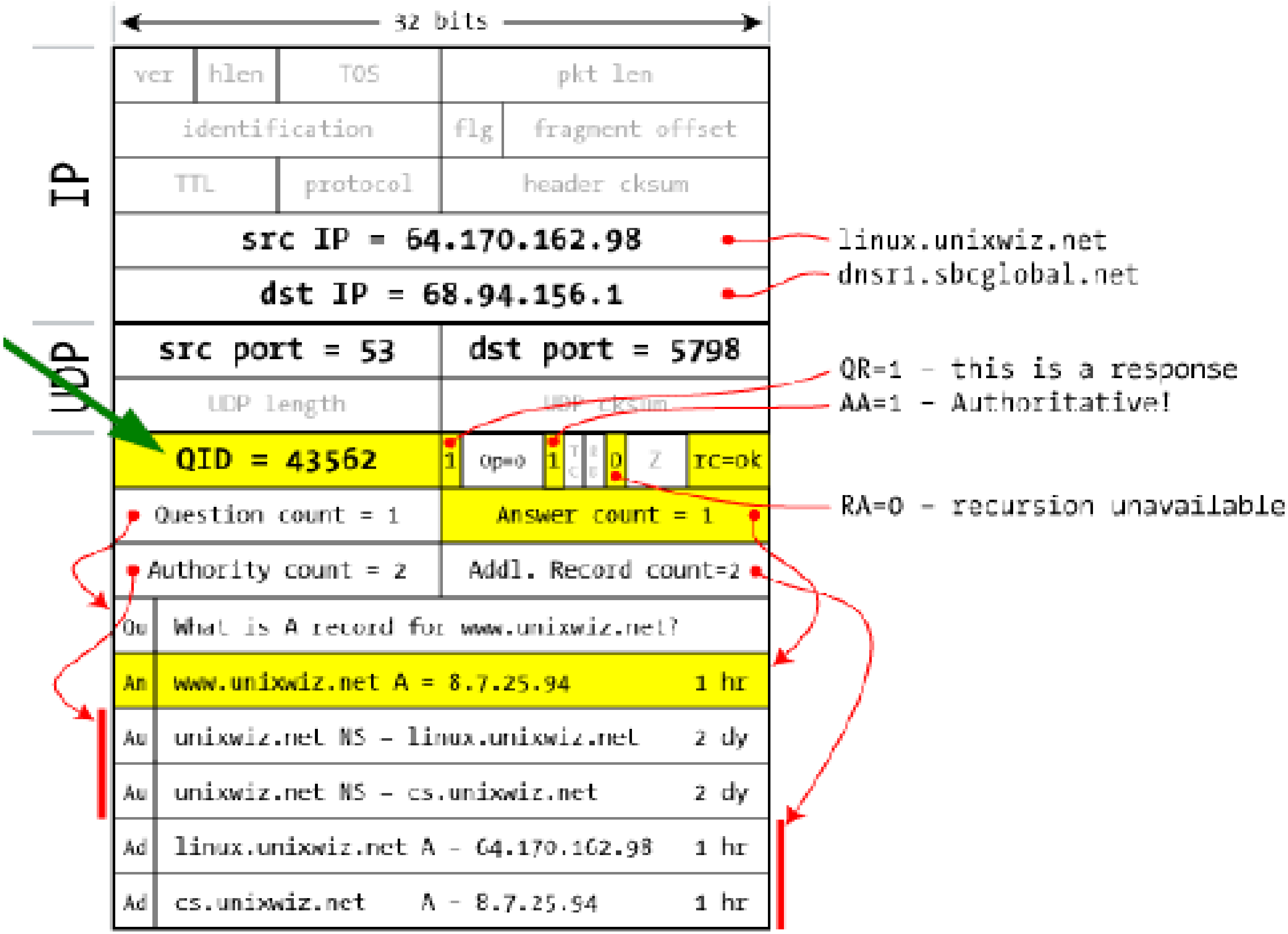
AA=1 - Authoritative!

RA=0 - recursion unavailable

src: Steve Friedl, unixwiz.net

Checking the response (cont'd)

- The Query ID matches the pending 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

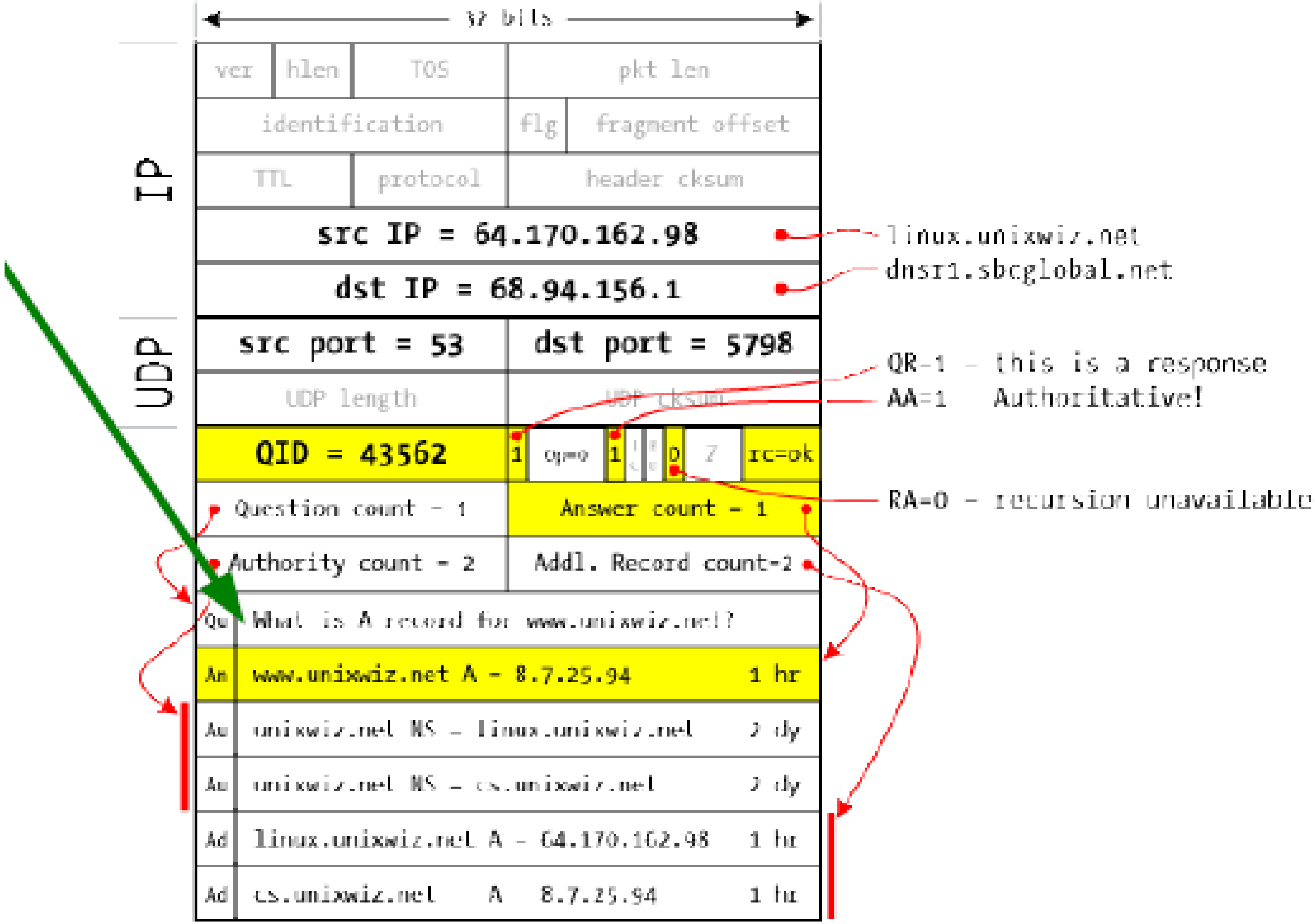
AA=1 – Authoritative!

RA=0 – recursion unavailable

src: Steve Friedl, unixwiz.net

Checking the response (cont'd)

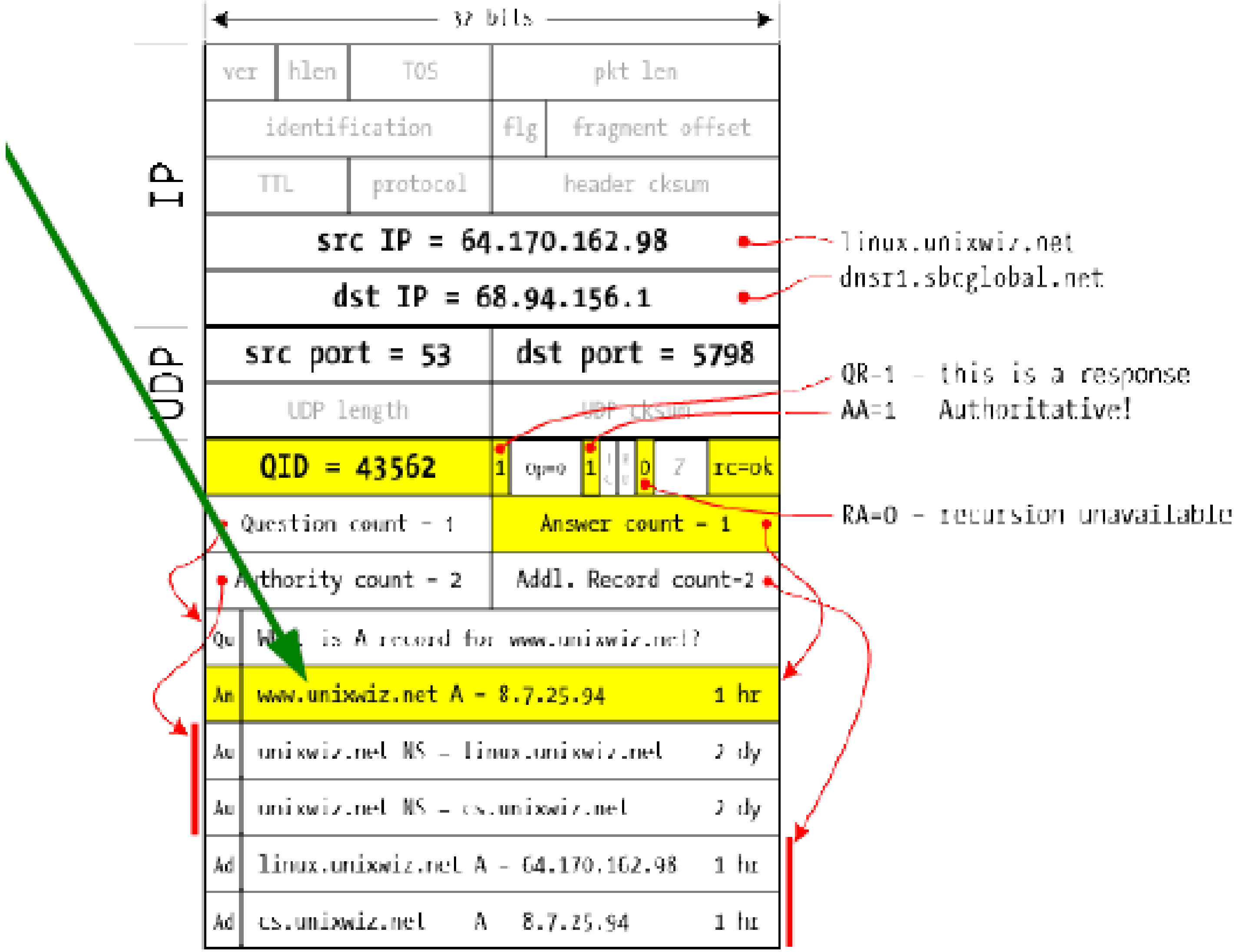
- The Question section is a duplicate



src: Steve Friedl, unixwiz.net

Checking the response (cont'd)

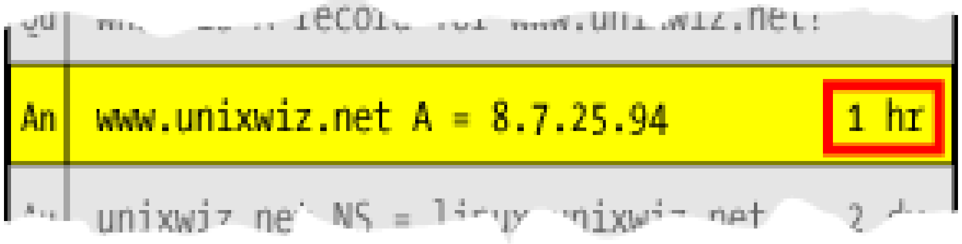
- Response is in the same domain as the query ("bailiwick checking")



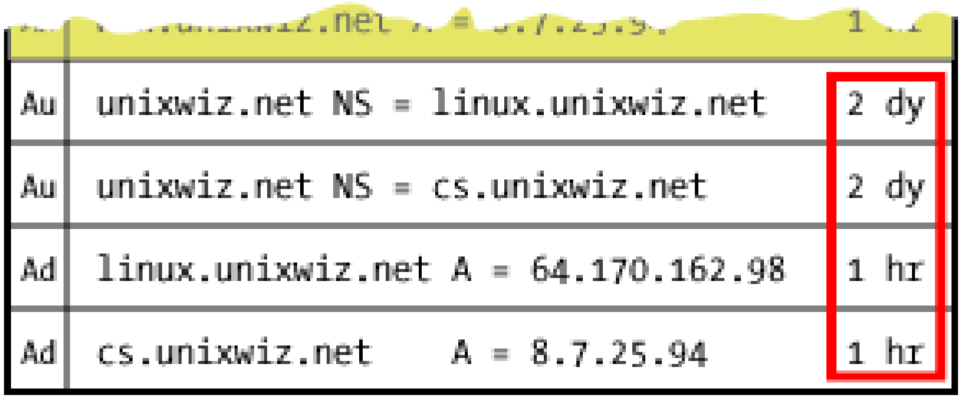
src: Steve Friedl, unixwiz.net

Time To Live (TTL)

- A DNS answer contains a TTL describing how long to keep the record
- Answers are kept in caches
- In a way, the responder manages the cache



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

How can we inject malicious data?

src: Steve Friedl, unixwiz.net

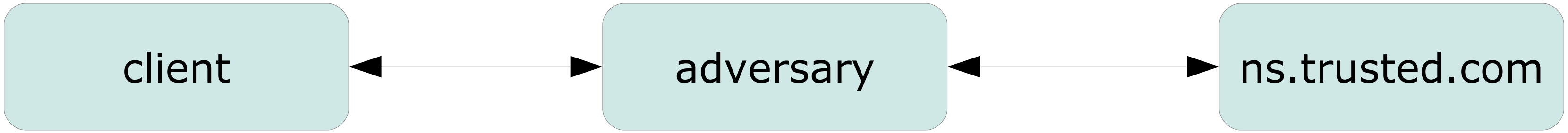
DNS Attacks

- How can we abuse DNS?
- *Examples:*
  - Man-in-the-Middle attacks
  - Kaminsky cache poisoning
  - DNS rebinding
- *Recommended reading:*
  - RFC3833: Threat Analysis of the Domain Name System (DNS)

DNS Attacks (cont'd)

- Why would we want to attack DNS?
  - To pretend to be someone else
  - To redirect users to where we want them to
  - Fun and profit

Man-in-the-Middle



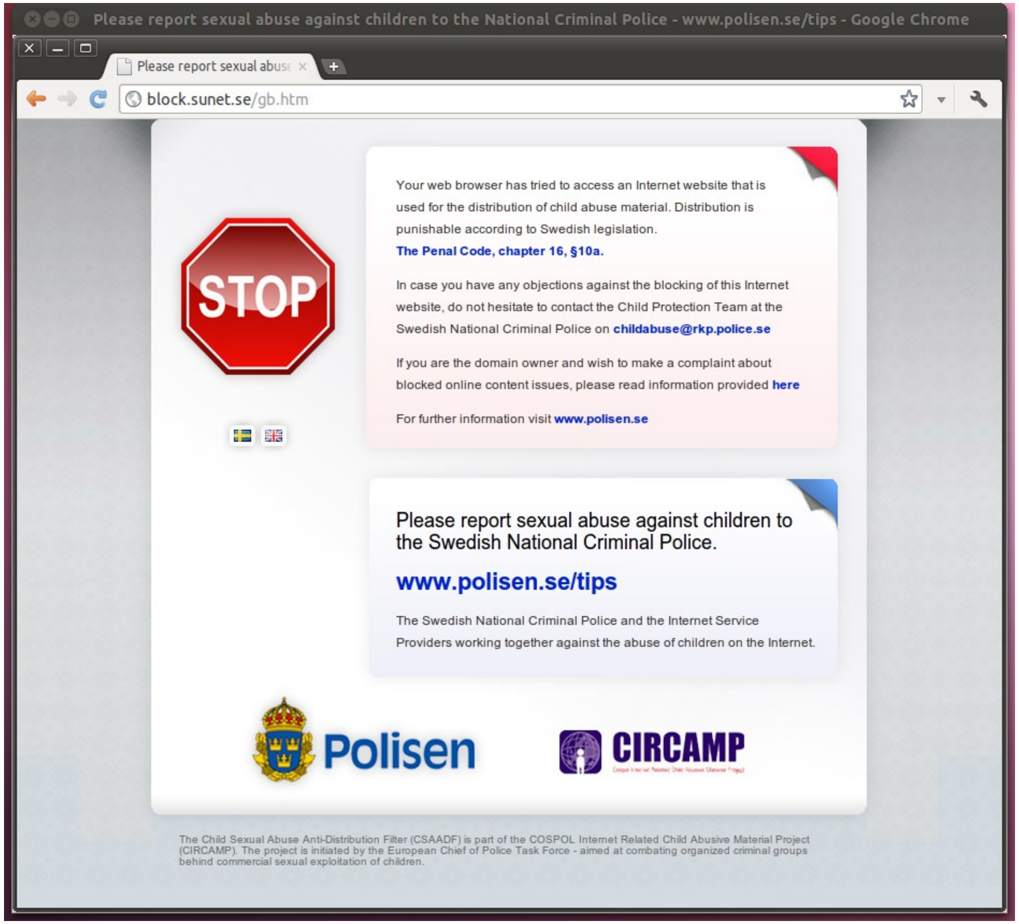
- The adversary can change the response, drop it, or create its own in an arbitrary manner
- Sometimes used by governments, asking ISPs to
  - Provide “erroneous” responses
  - Drop queries for specific sites

Government-in-the-Middle

- The Pirate Bay, along with several torrent sites, has been DNS-blocked in several countries
  - Is this how DNS was meant to be used?

Government-in-the-Middle (cont'd)

- In 2007 koreabonsai.com was blocked by Swedish ISPs, since the police listed it as child pornography
- Such lists mostly block their intended targets, but is there due process?


Please report sexual abuse against children to the National Criminal Police - www.polisen.se/tips - Google Chrome
Please report sexual abuse
block.sunet.se/gb.htm
STOP
Polisen
CIRCAMP

Your web browser has tried to access an Internet website that is used for the distribution of child abuse material. Distribution is punishable according to Swedish legislation.
The Penal Code, chapter 16, §10a.

In case you have any objections against the blocking of this Internet website, do not hesitate to contact the Child Protection Team at the Swedish National Criminal Police on **childabuse@rkp.police.se**

If you are the domain owner and wish to make a complaint about blocked online content issues, please read information provided **here**

For further information visit **www.polisen.se**

Please report sexual abuse against children to the Swedish National Criminal Police.

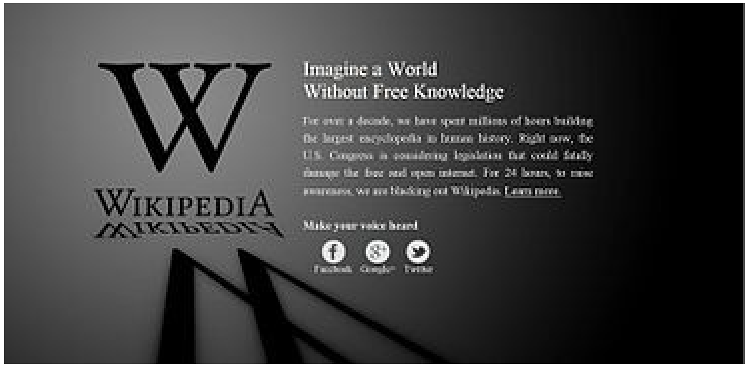
www.polisen.se/tips

The Swedish National Criminal Police and the Internet Service Providers working together against the abuse of children on the Internet.

The Child Sexual Abuse Anti-Distribution Filter (CSAADF) is part of the COSPOL Internet Related Child Abusive Material Project (CIRCAMP). The project is initiated by the European Chief of Police Task Force - aimed at combating organized criminal groups behind commercial sexual exploitation of children.

Government-in-the-Middle (cont'd)

- SOPA/PIPA in the USA contained DNS blocking sections, causing Wikipedia and others to blackout in protest

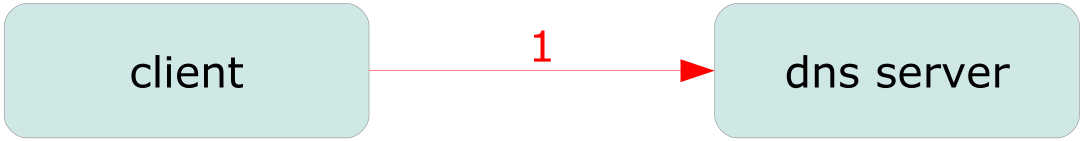


Imagine a World
Without Free Knowledge

For over a decade, we have spent millions of hours building the largest encyclopedia in human history. Right now, the U.S. Congress is considering legislation that could fatally damage the free and open internet. For 24 hours, to raise awareness, we are blacking out Wikipedia. Learn more.

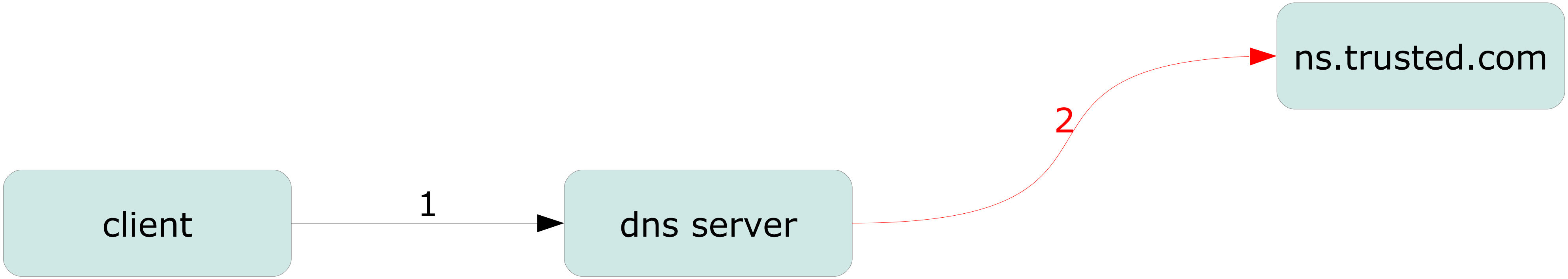
Make your voice heard

Kaminsky cache poisoning



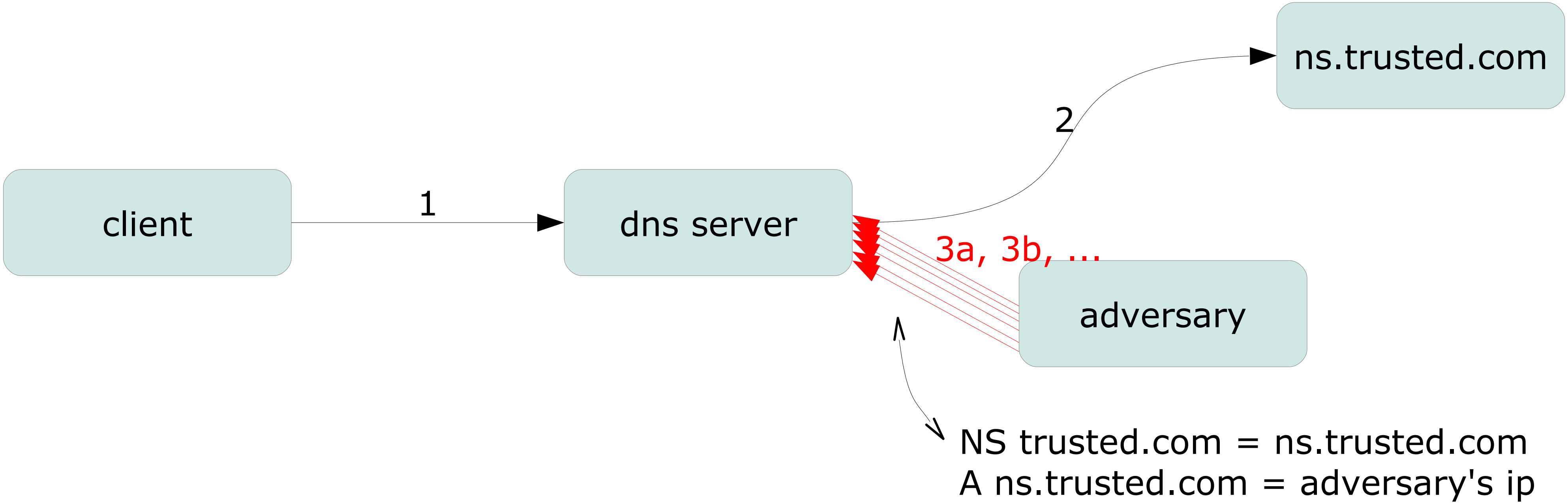
- Let client query (1) for random.trusted.com

Kaminsky cache poisoning (cont'd)



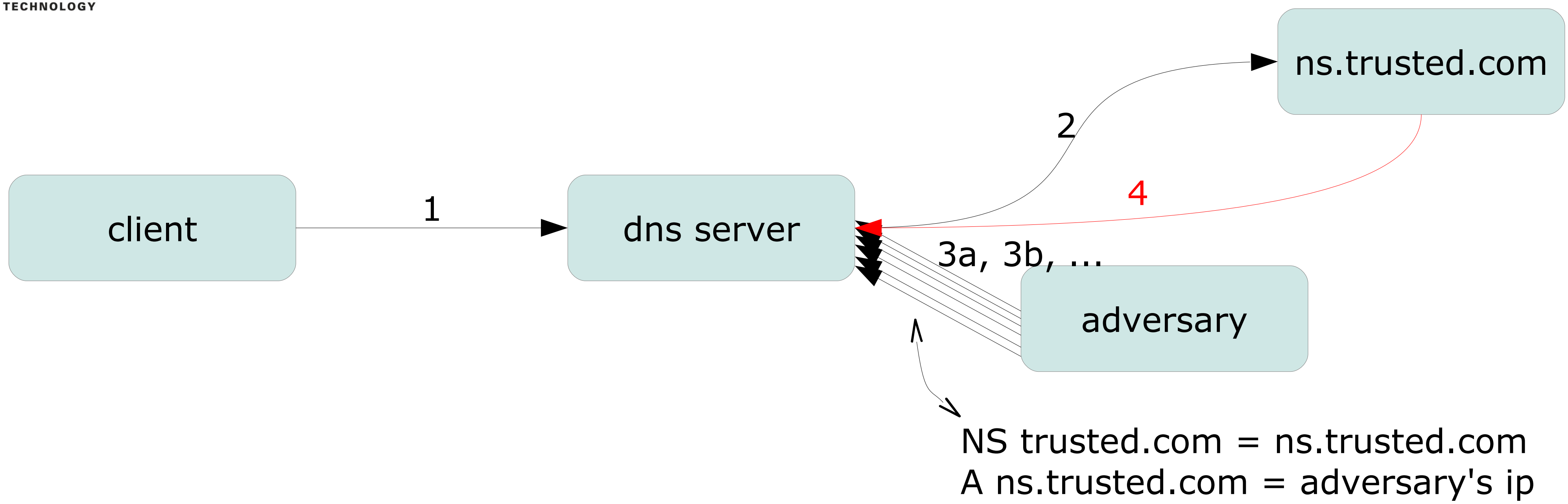
- Let client query for random.trusted.com (1)
- The local dns server will ask/look for ns.trusted.com (2)

Kaminsky cache poisoning (cont'd)


ns.trusted.com
2
client
1
dns server
3a, 3b, ...
adversary
NS trusted.com = ns.trusted.com
A ns.trusted.com = adversary's ip

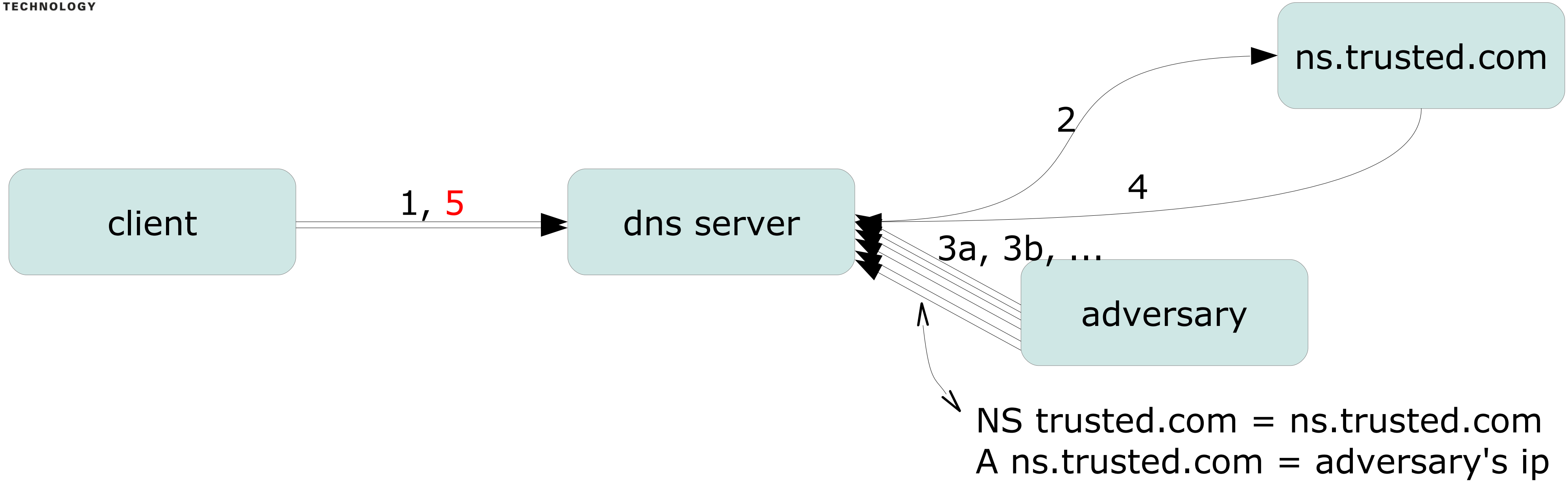
- Let client query for random.trusted.com (1)
- The local DNS server will ask/look for ns.trusted.com (2)
- The attacker sends multiple responses (3) with different QID. If any one (3) matches (2), the attacker will now “own” trusted.com

Kaminsky cache poisoning (cont'd)


ns.trusted.com
2
client
1
dns server
4
3a, 3b, ...
adversary
NS trusted.com = ns.trusted.com
A ns.trusted.com = adversary's ip

- Let client query for random.trusted.com (1)
- The local DNS server will ask/look for ns.trusted.com (2)
- The attacker sends multiple responses (3) with different QID. If any one (3) matches (2), the attacker will now “own” trusted.com
- Unless (4) arrives first

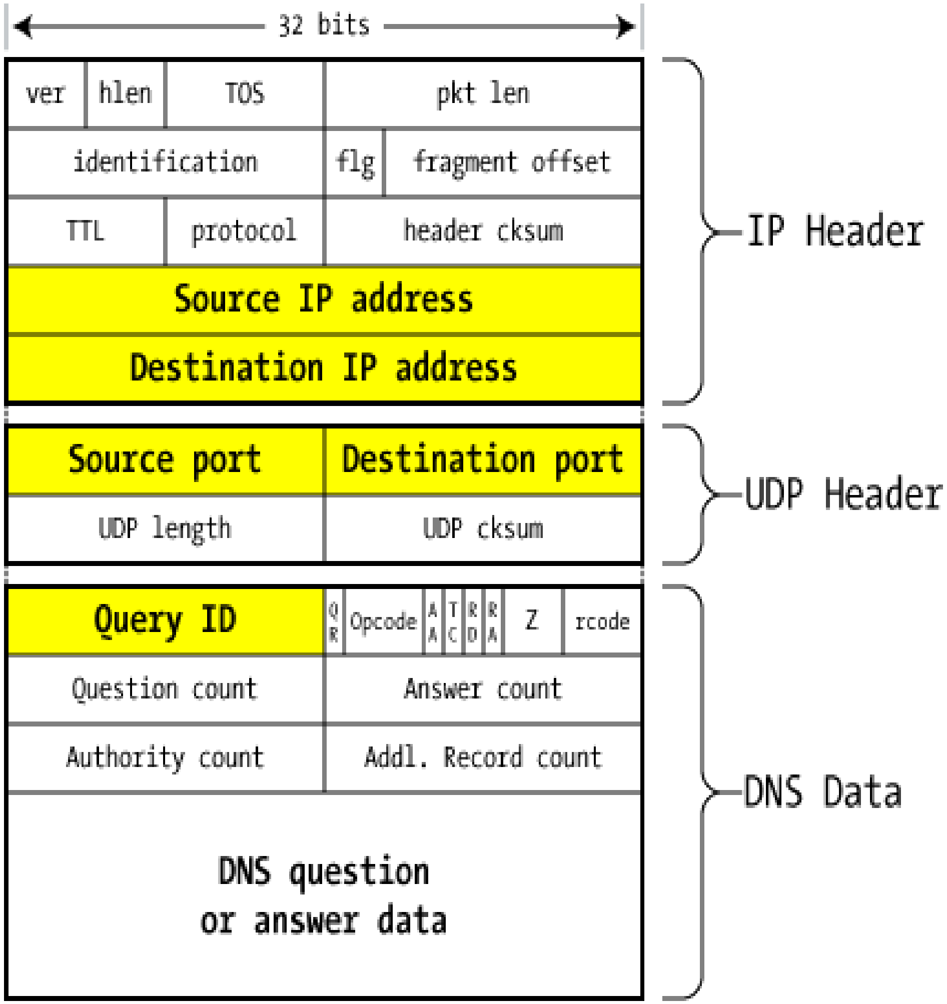
Kaminsky cache poisoning (cont'd)


ns.trusted.com
2
4
client
1, 5
dns server
3a, 3b, ...
adversary
NS trusted.com = ns.trusted.com
A ns.trusted.com = adversary's ip

- ...
- Unless (4) arrives first
- If the attack fails, let the client query (5) for random2.trusted.com

Mitigation: Increase randomization

- Query ID is 16 bits
- Source port is 16 bits, and the DNS server can allocate a range of them, e.g., 11 bits
- 2^27 is much bigger than 2^16
- DNSSEC would solve this, but still has not been fully deployed



32 bits

ver | hlen | TOS | pkt len

identification | flg | fragment offset

TTL | protocol | header cksum

Source IP address

Destination IP address

IP Header

Source port | Destination port

UDP length | UDP cksum

UDP Header

Query ID | QR | Opcode | AA | TC | RD | RA | Z | rcode

Question count | Answer count

Authority count | Addl. Record count

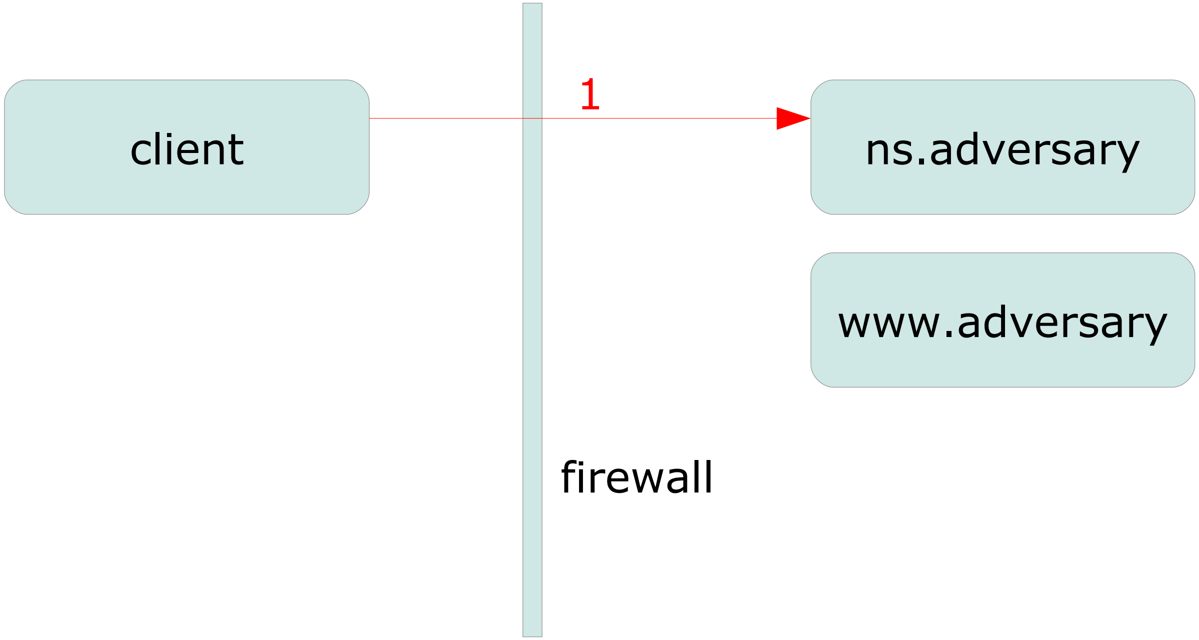
DNS question or answer data

DNS Data

src: Steve Friedl, unixwiz.net

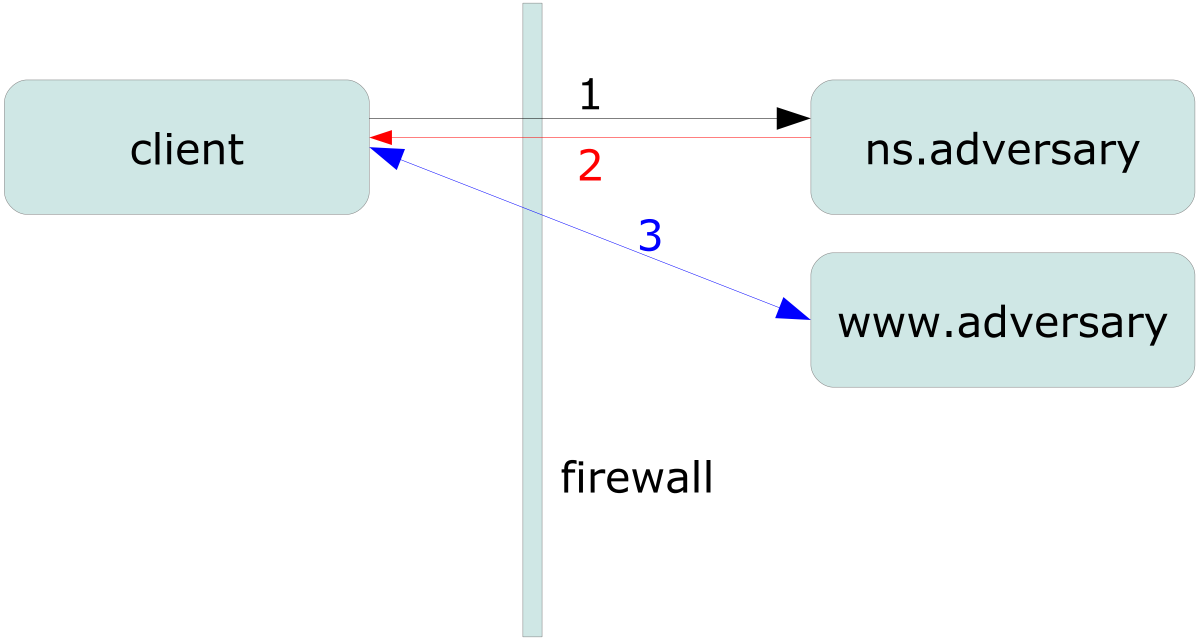
DNS Rebinding

- (1) is query for www.adversary



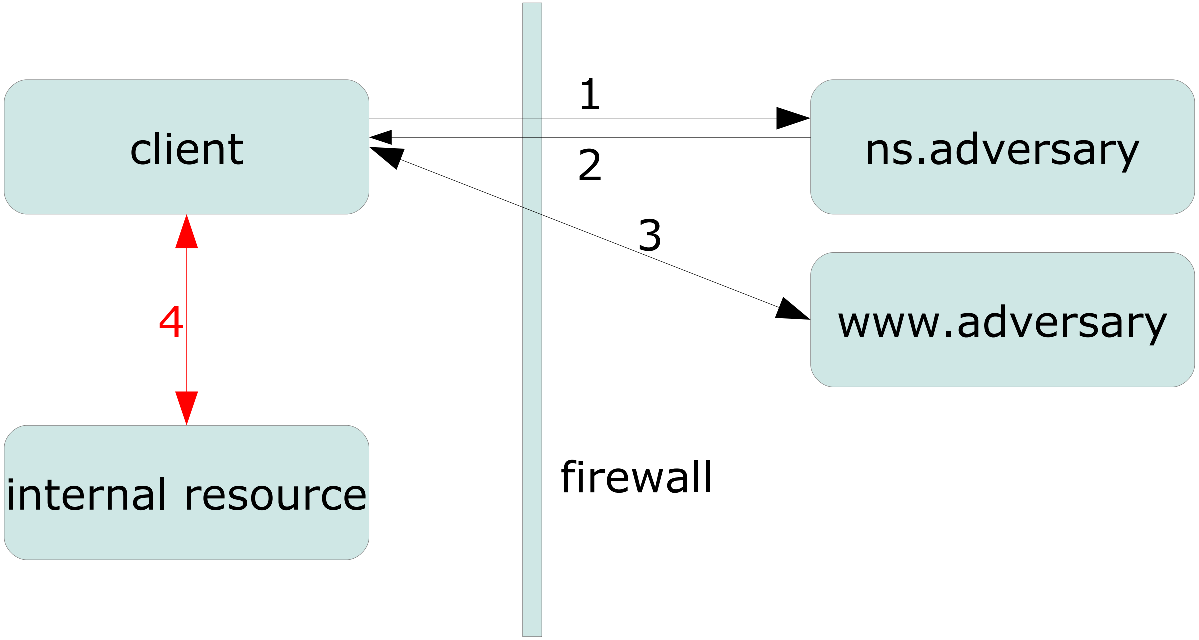
DNS Rebinding (cont'd)

- (1) is query for www.adversary
- (2) is a correct response pointing to (3), but with a short TTL



DNS Rebinding (cont'd)

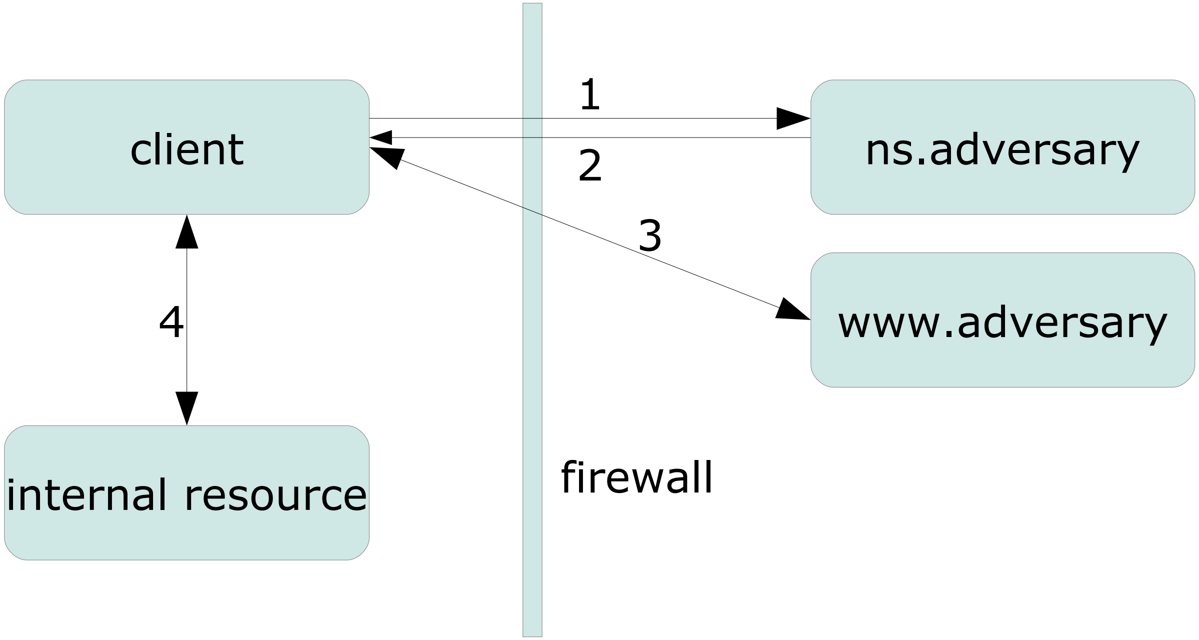
- (1) is query for www.adversary
- (2) is a correct response pointing to (3), but with a short TTL
- Client queries again, but now get an IP to (4)



DNS Rebinding (cont'd)

- (1) is query for www.adversary
- (2) is a correct response pointing to (3), but with a short TTL
- Client queries again, but now get an IP to (4)

- Circumvents the same-origin policy
  - See the lecture on web security



DNS Rebinding (cont'd)

- Browser mitigation: DNS Pinning
  - Refuse to switch to a new IP
  - But various services does this in a legitimate way
    - Proxies, VPN, dynamic DNS, ...
- Server-side defenses
  - Authenticate users with something other than IP
  - Reject HTTP requests with an unrecognized host header
- Firewall defenses
  - Check for external names resolving to internal addresses

Domain Name System Security Extensions (DNSSEC)

- Same principle as DNS
- All answers are digitally signed, to provide authentication
- New resource records (see RFC4034)
  - RRSIG DNS
    - Digital signature on the resource records in the response
  - DNSKEY
    - Public key that corresponds to the private used for the RRSIG
  - DS: Delegation Signer
    - Authenticate the DNSKEY record, i.e., a sub-domain
  - NSEC, to prove that some sub domains do not exist

DNSSEC (cont'd)

- Responses are not encrypted, i.e., no confidentiality
- Challenges as those for deploying a PKI
  - Centralized trust
  - Certificate revocation

DNSSEC NSEC

- Denial of existence records contains Next Secure (NSEC) resource records
- “NSEC RRs **assert which names do not exist** in a zone by linking from existing name to existing name along a canonical ordering of all the names within a zone.” RFC4033

DNSSEC NSEC (cont'd)

- Allows for zone walking, i.e., zone enumeration
  - 1) Query for <random>.domain.com
  - 2) If domain exits, store it and repeat 1
  - 3) Get two valid sub-domain names, say a and b, store them
  - 4) Repeat step 1 for b1.domain.com
  - 5) When the complete linked list is found, the entire domain is mapped
- Potentially exposing servers not meant for public use
  - E.g., counteract the trouble of finding IPv6 hosts in the vast number space

DNSSEC NSEC3

- Hashed Authenticated Denial of Existence (NSEC3)
- Owner names are
  - Hashed, in order to hide them
  - Chained in hash order
- Still possible to zone walk to enumerate hosts
- See a discussion of NSEC/NSEC3 (which are mutually exclusive) here: http://www.internetsociety.org/deploy360/resources/dnssec-nsec-vs-nsec3/

DNSSEC Deployment

- 2010-07-15: Distribution of possible-to-validate signed root zone; publication of root zone trust anchor
- Domain owners, ISPs, and end users have been slow to adopt
- Deployment maps:
  - http://www.internetsociety.org/deploy360/dnssec/maps/

Summary

- DNS is a tree, with delegated trust
- DNS was not designed with security in mind
- Query IDs does not provide adequate protection
- DNSSEC addresses issues, but it is not everywhere just yet

Extra reading

- Request for Comments
  - RFC3833: Threat Analysis of the Domain Name System (DNS)
  - RFC4033: DNS Security Introduction and Requirements
  - RFC4034: Resource Records for the DNS Security Extension
- *An Illustrated Guide to the Kaminsky DNS Vulnerability*
  - http://unixwiz.net/techtips/iguide-kaminsky-dns-vuln.html