DNS Review Quiz

Match the term to the description:

Level:

C Domain name

B DNS zone

A Delegation

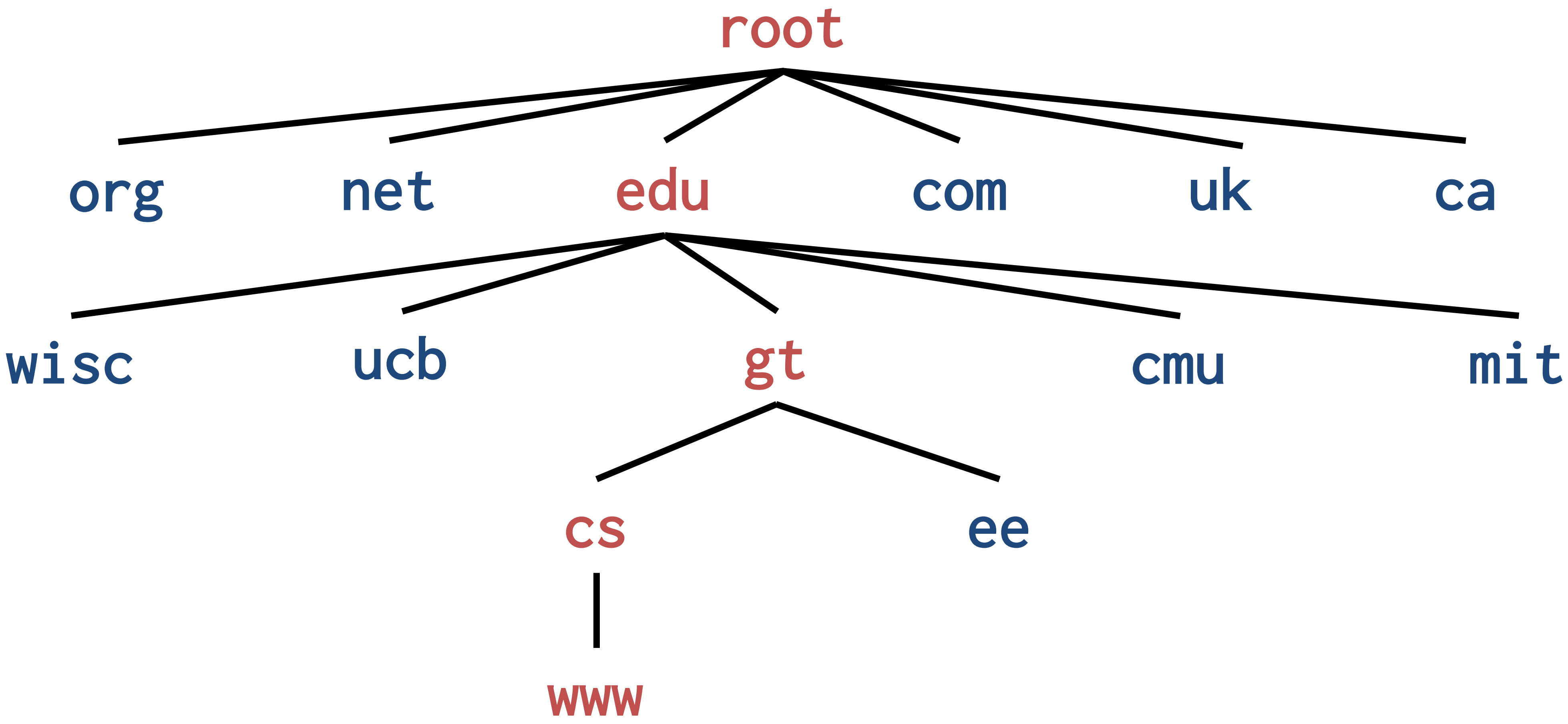
Descriptions:

A. Transfer of authority for/to a sub-domain

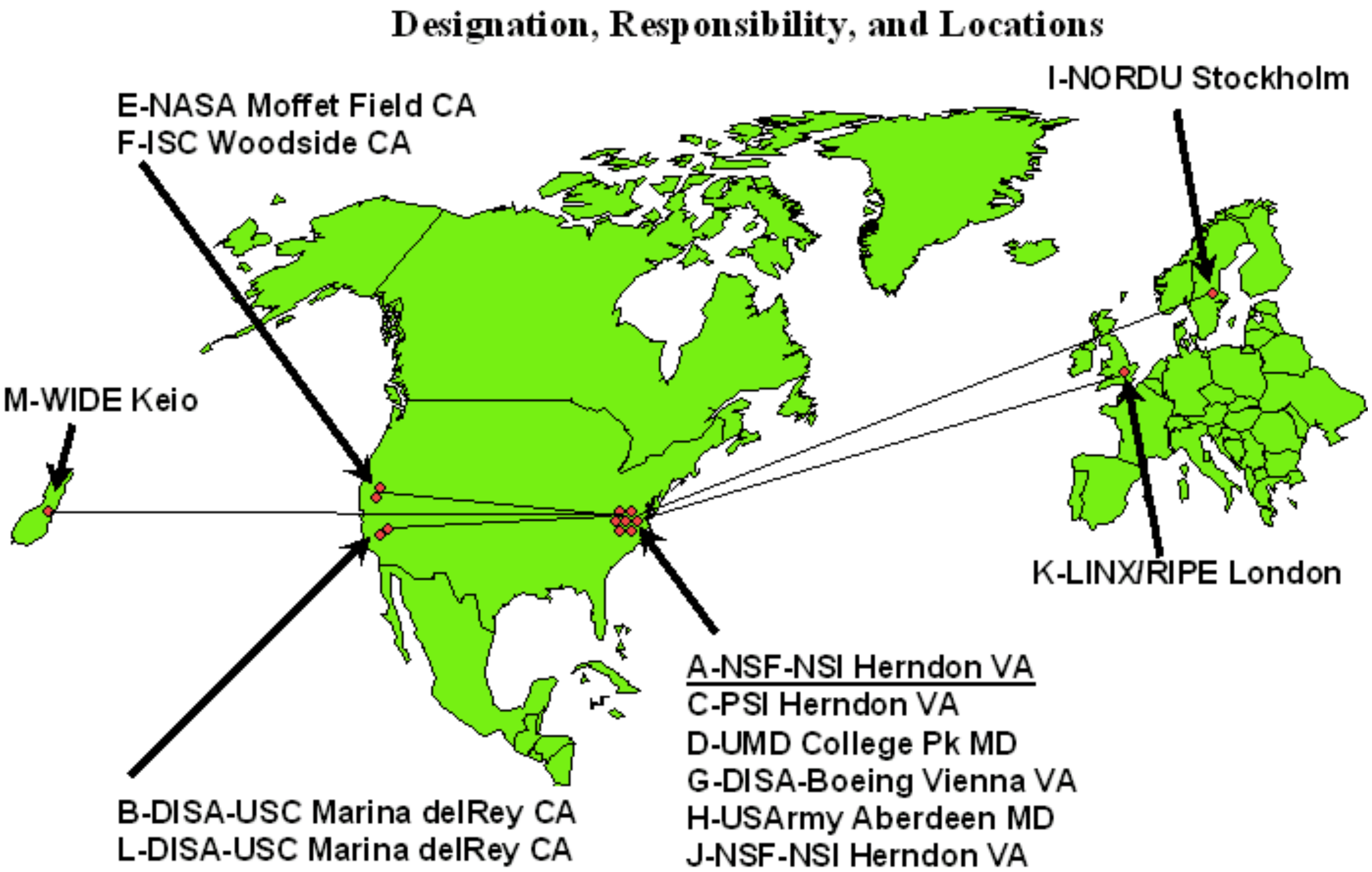
B. A set of names under the same authority (ie ".com")

C. A name in the DNS format

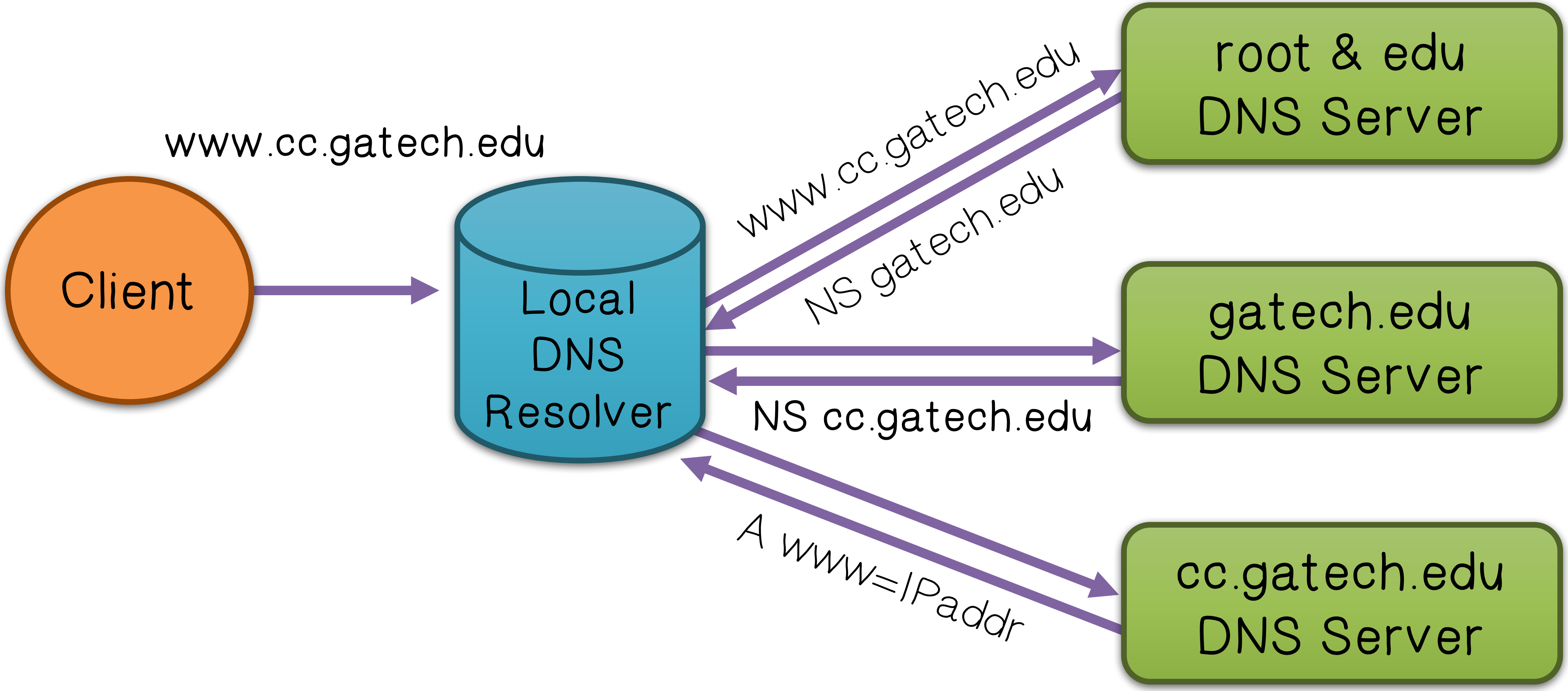
DNS: Hierarchical Name Space



DNS: DNS Root Name Servers



DNS: DNS Lookup Example



DNS: DNS Lookup Example

DNS record types (partial list):

- NS: name server (points to other server)
- A: address record (contains IP address)
- MX: address in charge of handling email
- TXT: generic text (e.g. used to distribute site public keys (DKIM)

DNS Caching Quiz

Fill in the blanks:

Changing a domain name into an IP address involves a large number of steps. To save time, the records are cached on a local server for reuse later.

Each record has a TTL that states how long a record can be kept for future use.

Caching

DNS responses are cached

- Quick response for repeated translations
- Note: NS records for domains also cached

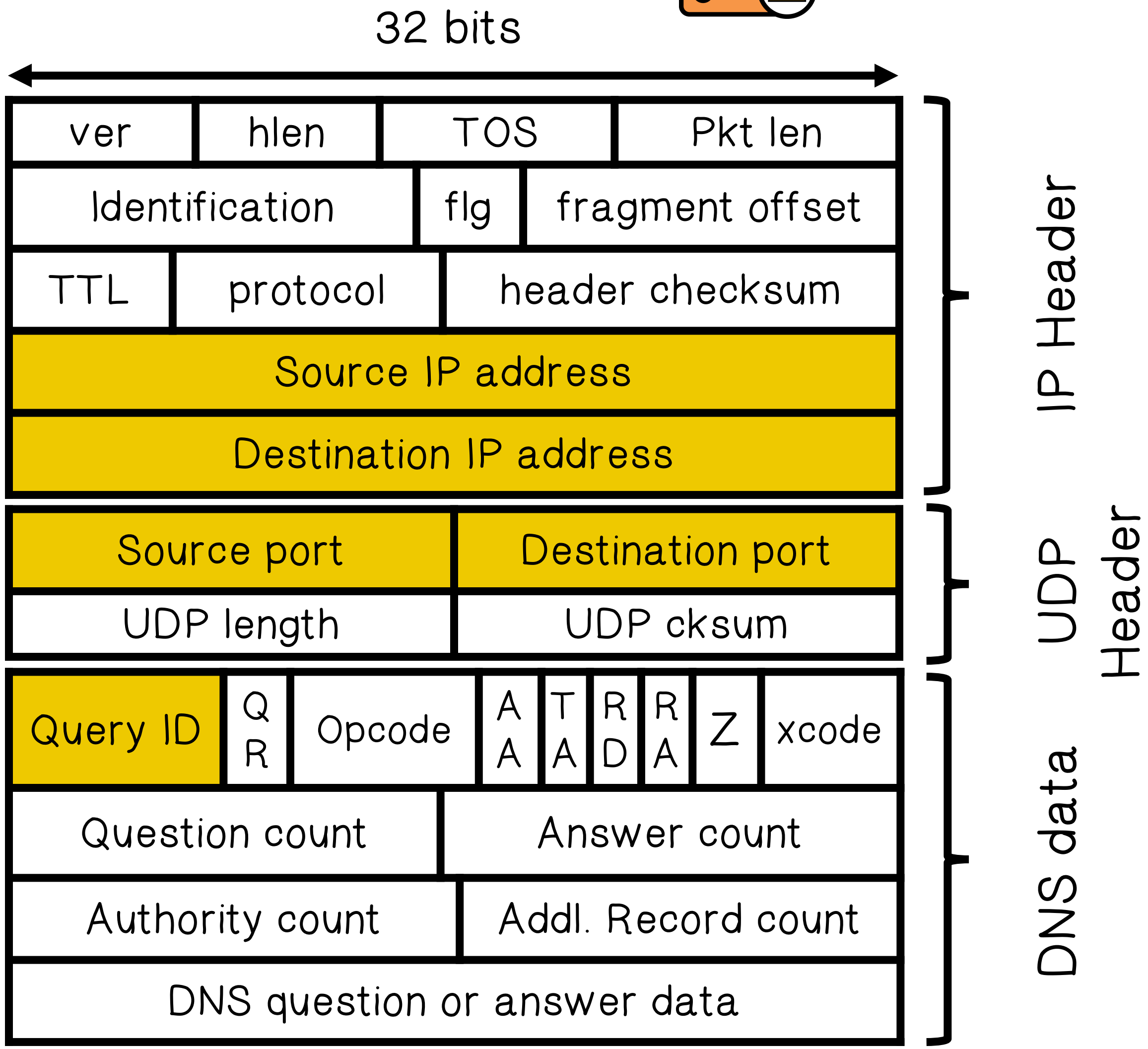
DNS negative queries are cached

- Save time for nonexistent sites, e.g. misspelling

Cached data periodically times out

- Lifetime (TTL) of data controlled by owner of data
- TTL passed with every record

DNS Packet



32 bits

ver | hlen | TOS | Pkt len

Identification | flg | fragment offset

TTL | protocol | header checksum

Source IP address

Destination IP address

Source port | Destination port

UDP length | UDP cksum

Query ID | QR | Opcode | AA | TA | RD | RA | Z | xcode

Question count | Answer count

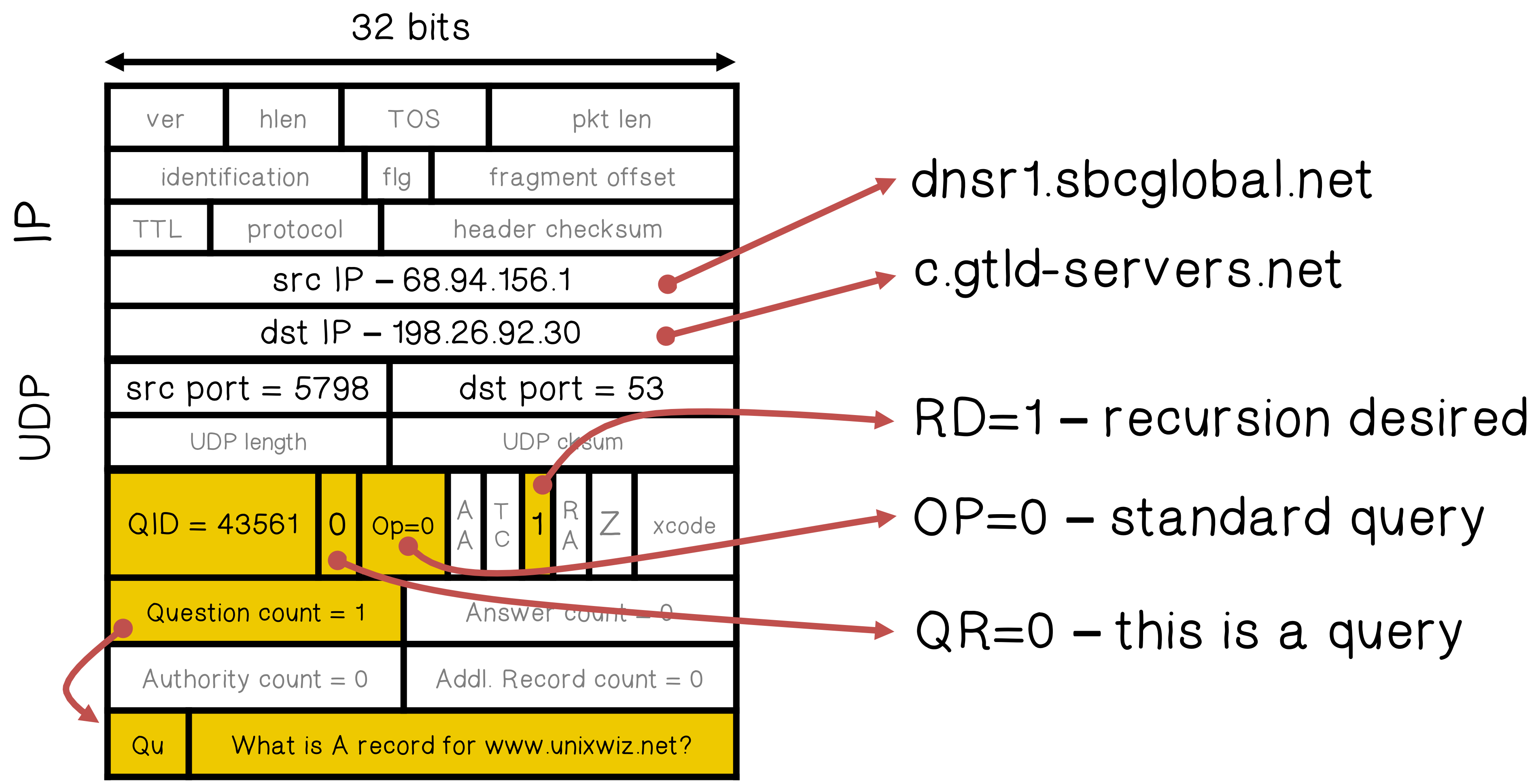
Authority count | Addl. Record count

DNS question or answer data

Query ID:

- 16 bit random value
- Links response to query

DNS Packet: Resolver to NS request



32 bits

IP

ver	hlen	TOS	pkt len
identification	flg	fragment offset	
TTL	protocol	header checksum	
src IP – 68.94.156.1			
dst IP – 198.26.92.30			

UDP

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

QID = 43561	0	Op=0	AA	TC	1	RA	Z	xcode

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

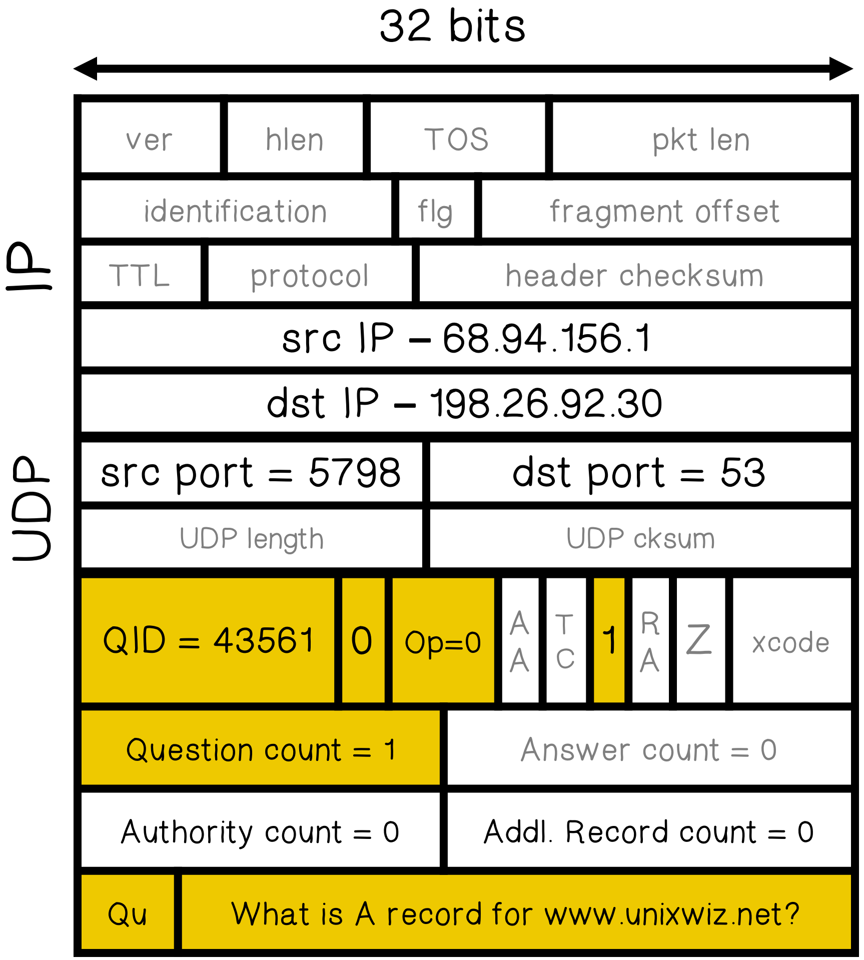
c.gtld-servers.net

RD=1 – recursion desired

OP=0 – standard query

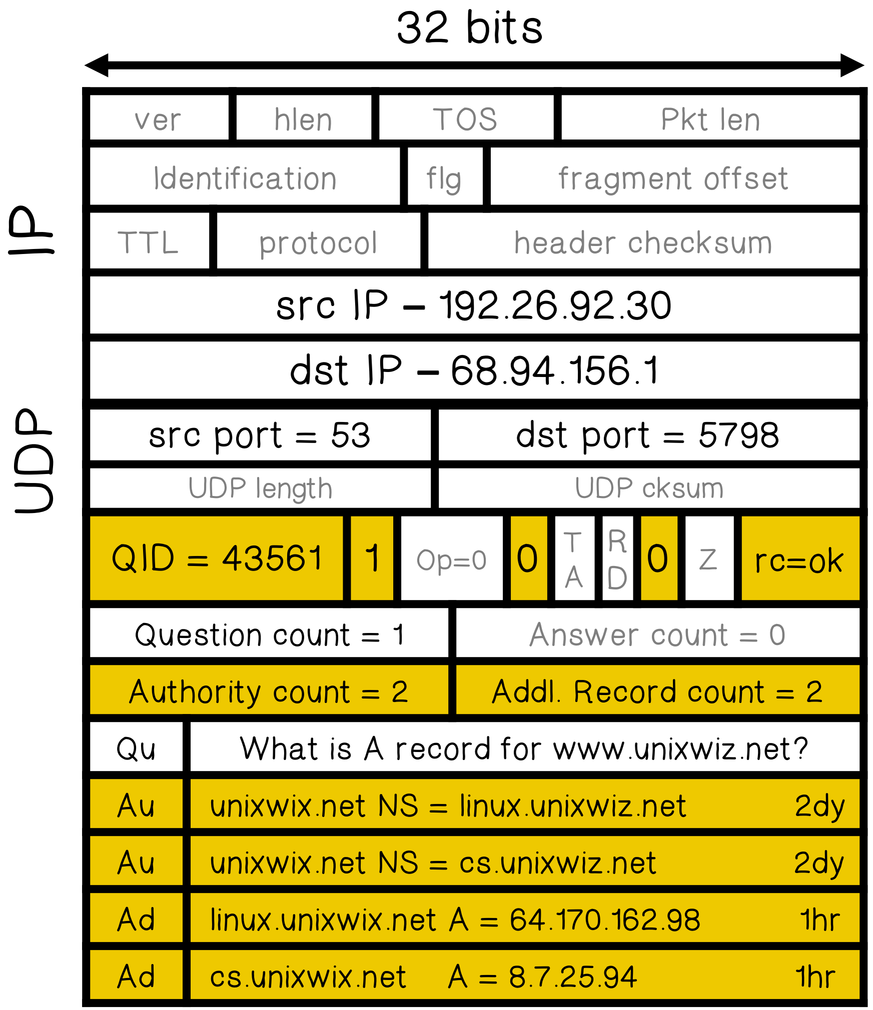
QR=0 – this is a query

DNS Packet: Response to Resolver



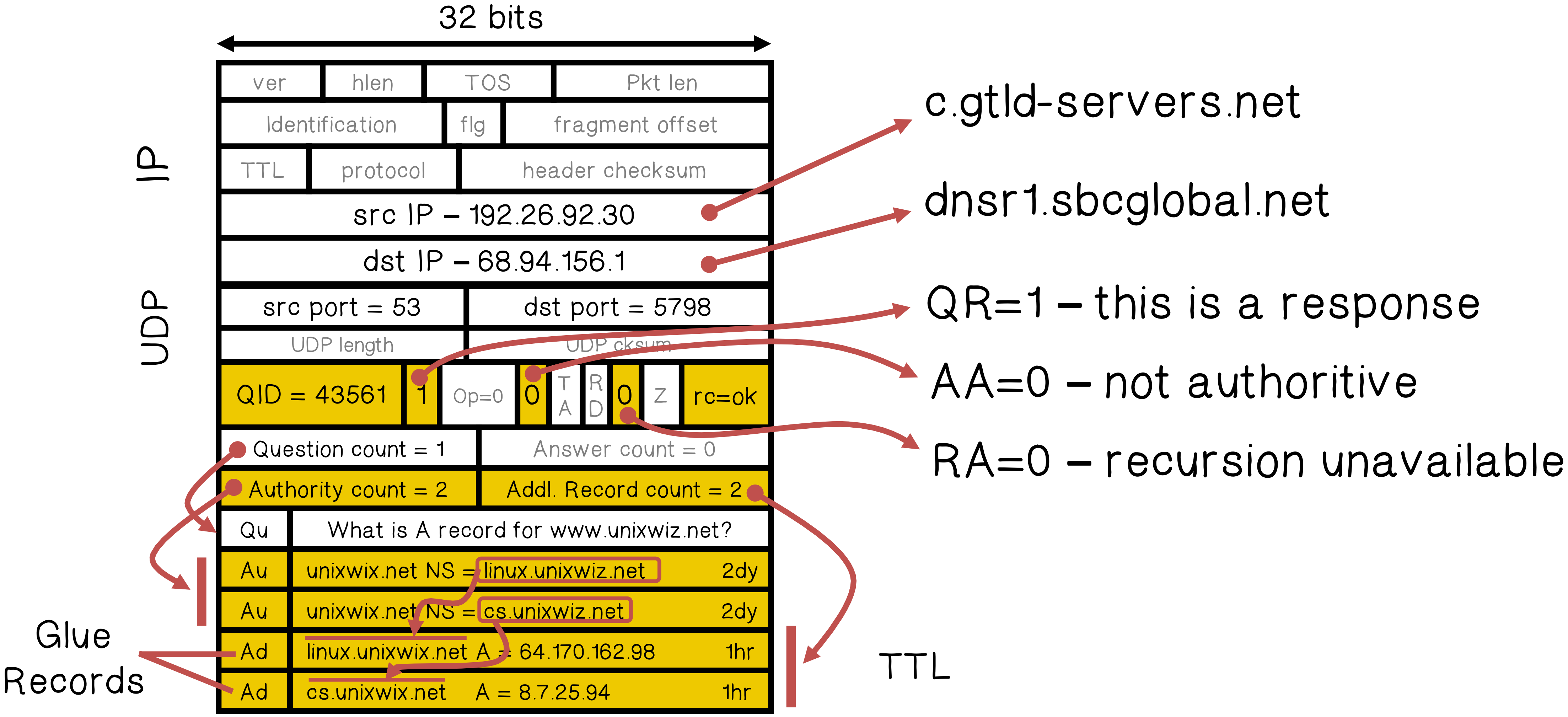
ver	hlen	TOS	pkt len					
identification	flg	fragment offset						
TTL	protocol	header checksum						
src IP – 68.94.156.1								
dst IP – 198.26.92.30								
src port = 5798	dst port = 53							
UDP length	UDP ckisum							
QID = 43561	0	Op=0	AA	TC	1	RA	Z	xcode
Question count = 1	Answer count = 0							
Authority count = 0	Addl. Record count = 0							
Qu	What is A record for www.unixwiz.net?							

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



ver	hlen	TOS	Pkt len					
Identification	flg	fragment offset						
TTL	protocol	header checksum						
src IP – 192.26.92.30								
dst IP – 68.94.156.1								
src port = 53	dst port = 5798							
UDP length	UDP cksum							
QID = 43561	1	Op=0	0	TA	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	unixwix.net NS = linux.unixwiz.net	2dy						
Au	unixwix.net NS = cs.unixwiz.net	2dy						
Ad	linux.unixwix.net A = 64.170.162.98	1hr						
Ad	cs.unixwix.net A = 8.7.25.94	1hr						

DNS Packet: Response to Resolver



32 bits

IP

ver | hlen | TOS | Pkt len

Identification | flg | fragment offset

TTL | protocol | header checksum

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 | TA | 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 | unixwix.net NS = linux.unixwiz.net | 2dy

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

Ad | linux.unixwix.net A = 64.170.162.98 | 1hr

Ad | cs.unixwix.net A = 8.7.25.94 | 1hr

c.gtld-servers.net

dnsr1.sbcglobal.net

QR=1 – this is a response

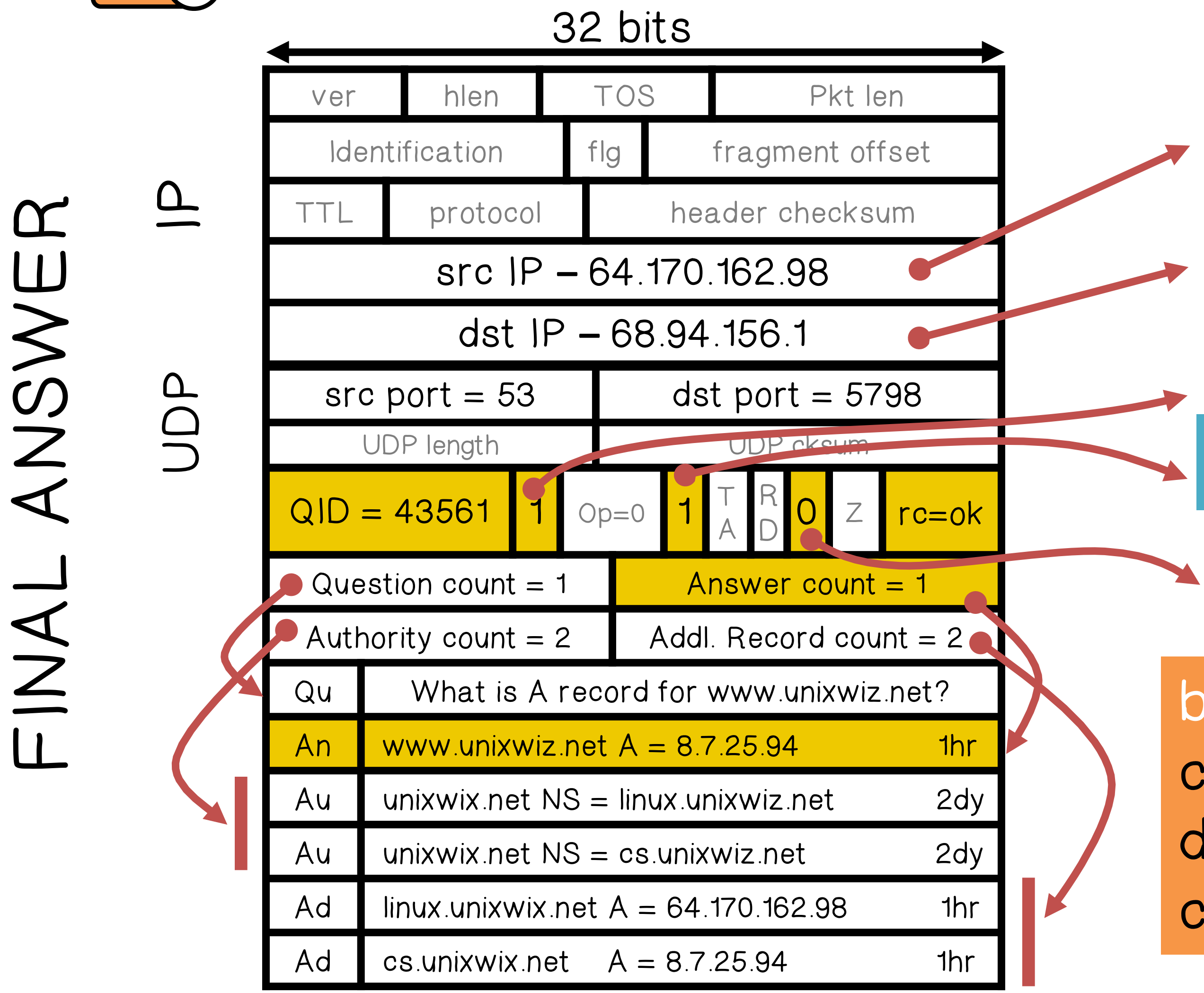
AA=0 – not authoritive

RA=0 – recursion unavailable

Glue Records

TTL

DNS Packet: Authoritative Response



ver | hlen | TOS | Pkt len

Identification | flg | fragment offset

TTL | protocol | header checksum

src IP – 64.170.162.98

dst IP – 68.94.156.1

src port = 53 | dst port = 5798

UDP length | UDP cksum

QID = 43561 | 1 | Op=0 | 1 | TA | 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 | 1hr

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

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

Ad | linux.unixwix.net A = 64.170.162.98 | 1hr

Ad | cs.unixwix.net A = 8.7.25.94 | 1hr

linux.unixwiz.net

dnsr1.sbcglobal.net

QR=1 – this is a response

AA=1 – Authoritative!

RA=0 – recursion unavailable

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

DNS Quiz

Select the true statements about DNS:

□ DNS stores the IP address. For security reasons the domain name is stored somewhere else.

☑ All domain names and IP addresses are stored at the Central Registry.

☑ It can take several days for information to propagate to all DNS servers.

Basic DNS Vulnerabilities

Users/hosts trust the host-address mapping provided by DNS:

- Used as basis for many security policies:
  - Browser same origin policy, URL address

Obvious problems

- Interception of requests or compromise of DNS servers can result in incorrect or malicious responses
  - e.g.: malicious access point in a Cafe

Solution

- authenticated requests/responses
  - Provided by DNSsec ... but few use DNSsec (yet)

Basic DNS Vulnerabilities: Cache Poisoning

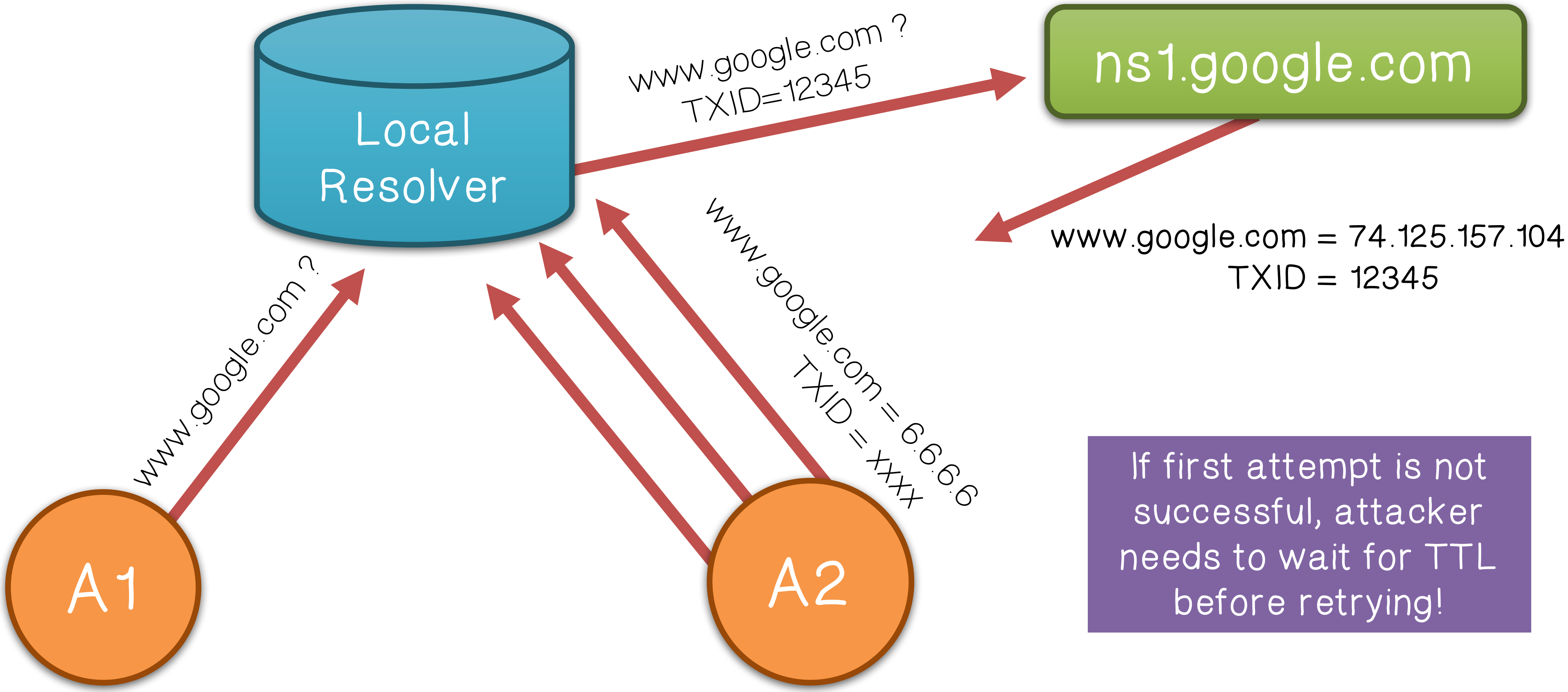
Basic idea: give DNS servers false records and get it cached

DNS uses a 16-bit request identifier to pair queries with answers

☠ Cache may be poisoned when a name server:

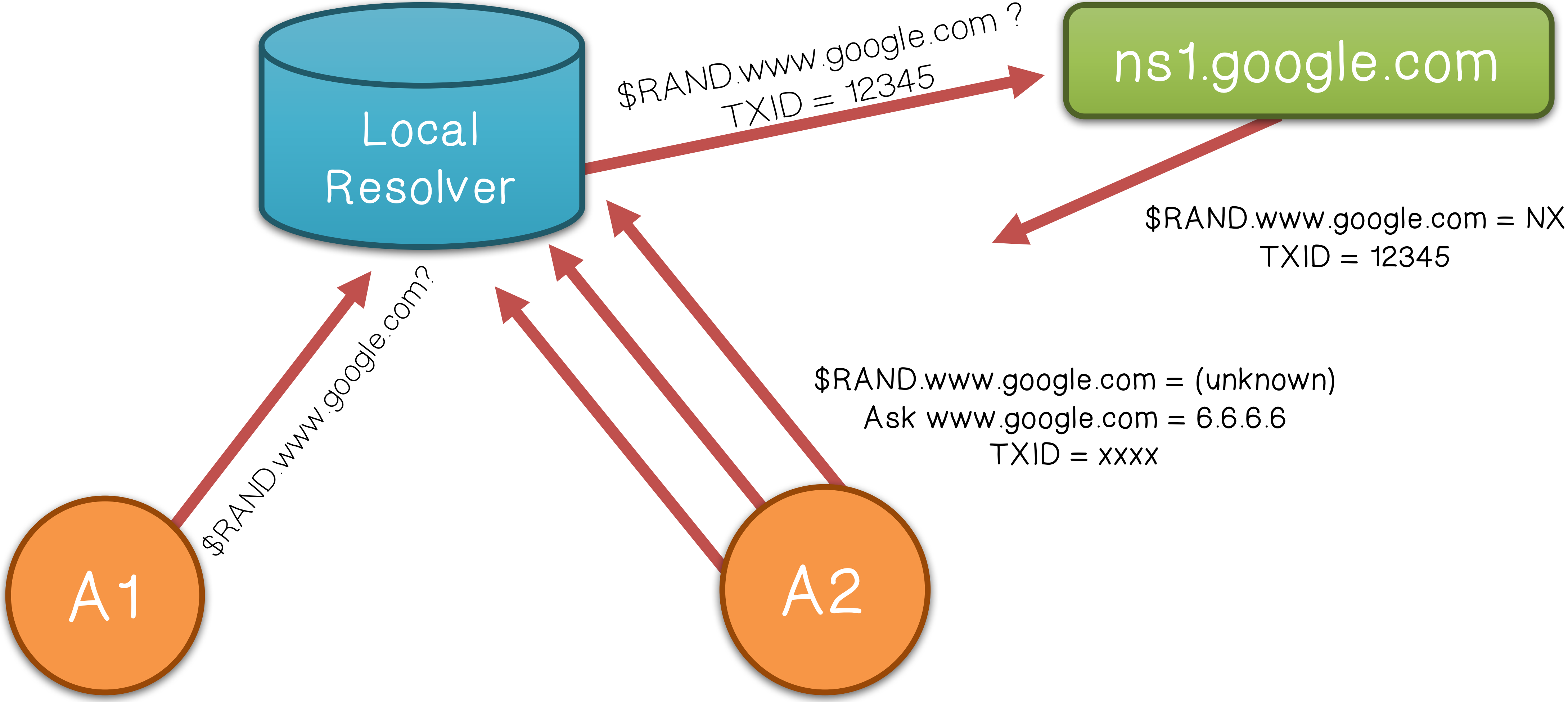
- Disregards identifiers
- Has predictable ids
- Accepts unsolicited DNS records

Traditional Poisoning Attack



If first attempt is not successful, attacker needs to wait for TTL before retrying!

Kaminsky's Poisoning Attack



Local Resolver

ns1.google.com

A1

A2

$RAND.www.google.com?

$RAND.www.google.com ?
TXID = 12345

$RAND.www.google.com = NX
TXID = 12345

$RAND.www.google.com = (unknown)
Ask www.google.com = 6.6.6.6
TXID = xxxx

DNS Defenses

- Increase Query ID size
- Randomize src port, additional 11 bits
  - Now attack takes several hours
- Ask every DNS query twice:
  - Attacker has to guess QueryID correctly twice (32 bits)
  - But DNS system cannot handle the load
- Deploy DNSSEC (eventually)

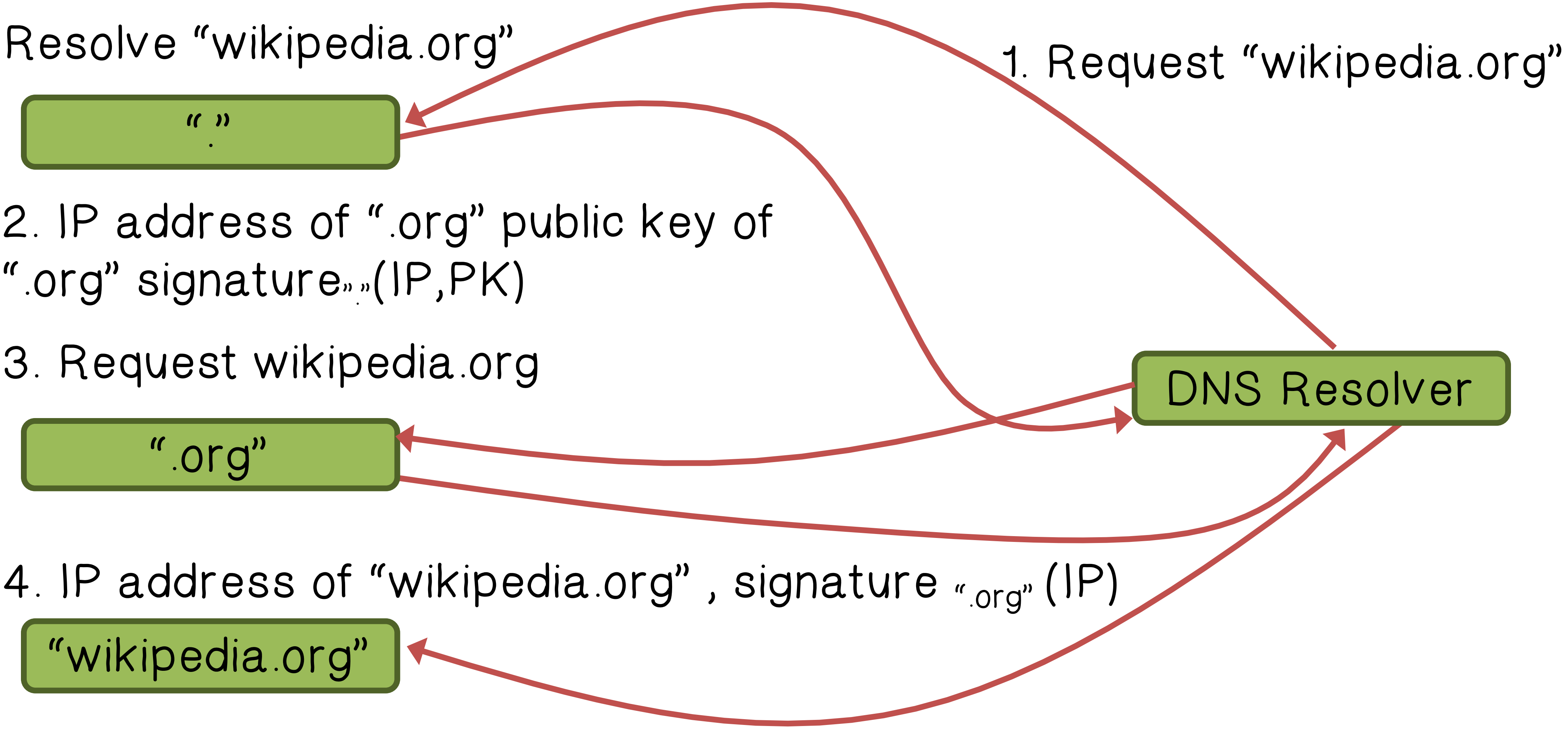
DNSSEC

Guarantees:

- Authenticity of DNS answer origin
- Integrity of reply
- Authenticity of denial of existence

- Accomplishes this guarantee by signing DNS replies at each step of the way
- Uses public-key cryptography to sign responses
- Typically use trust anchors, entries in the operating system to bootstrap the process

DNSSEC: DNS Signing



Resolve “wikipedia.org”

“.”

1. Request “wikipedia.org”

2. IP address of “.org” public key of “.org” signature$_{\text{“.”}}$(IP,PK)

3. Request wikipedia.org

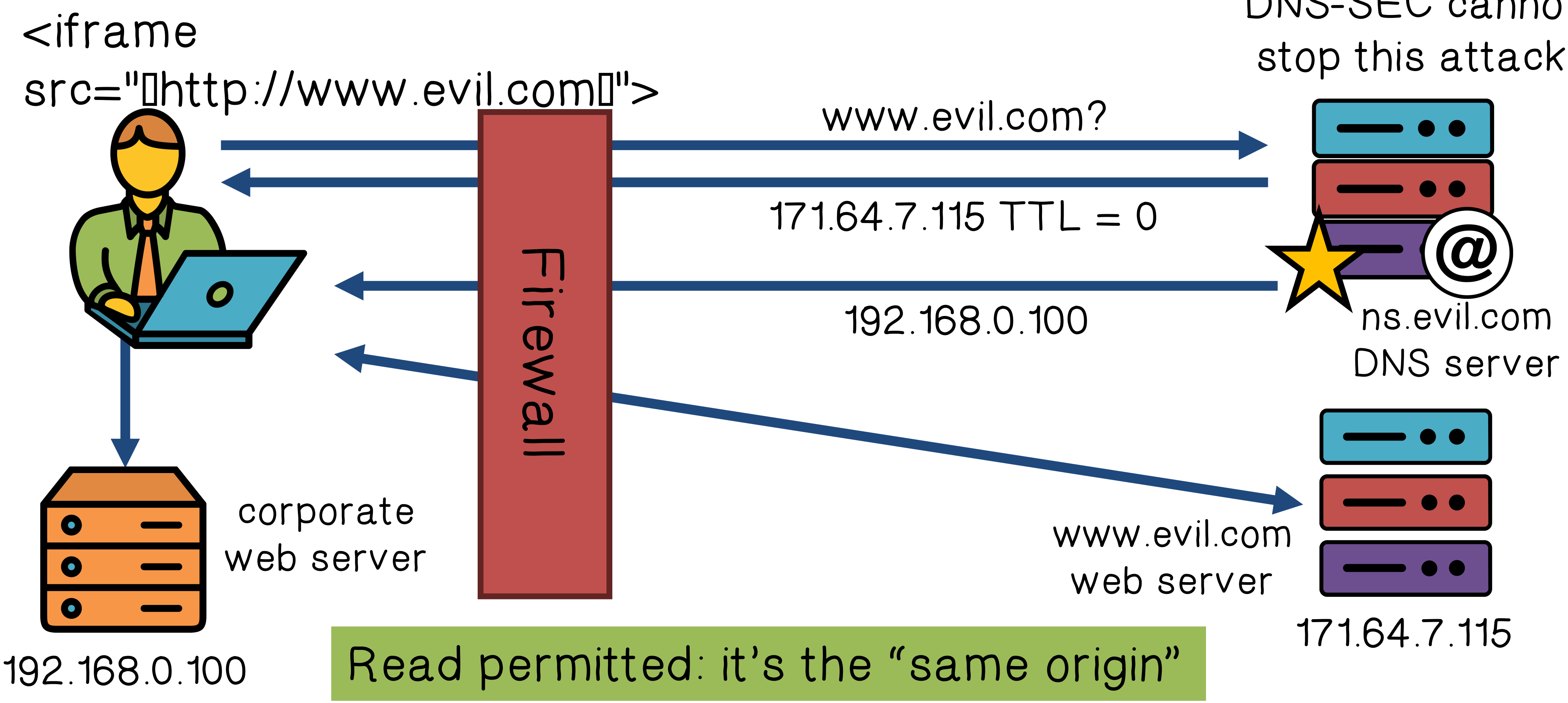
“.org”

DNS Resolver

4. IP address of “wikipedia.org” , signature $_{\text{“.org”}}$ (IP)

“wikipedia.org”

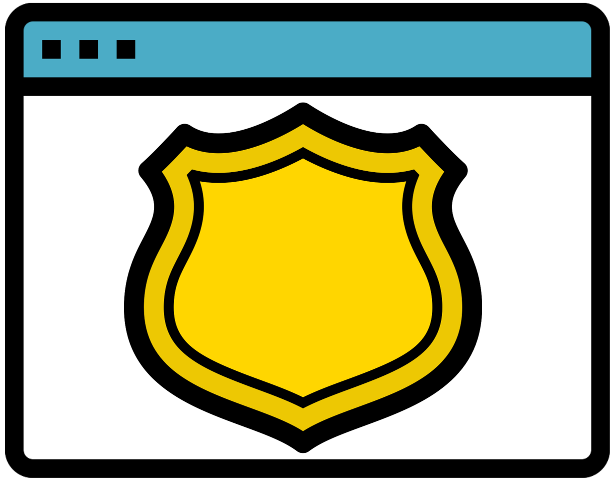
DNS Rebinding Attack



DNS-SEC cannot stop this attack

Read permitted: it’s the “same origin”

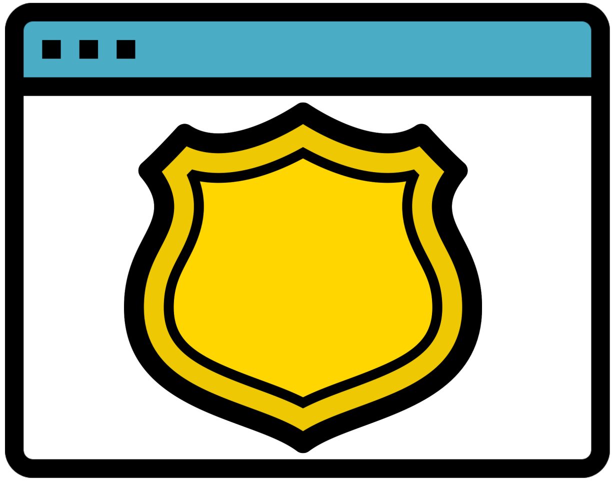
DNS Rebinding Attack: Defenses



Browser mitigation: DNS Pinning

- Refuse to switch to a new IP
- Interacts poorly with proxies, VPN, dynamic DNS, ...
- Not consistently implemented in any browser

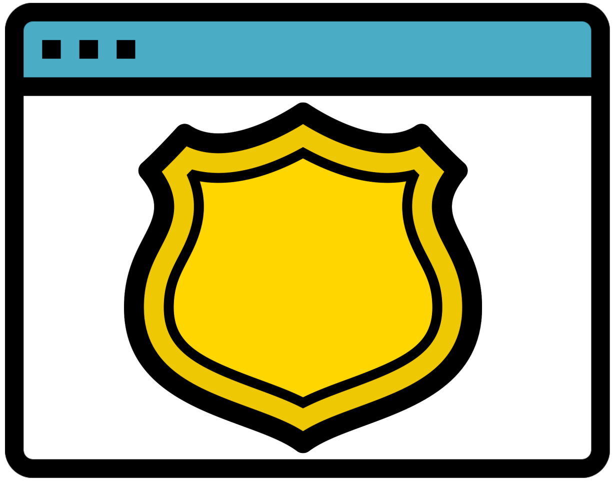
DNS Rebinding Attack: Defenses



Server-side defenses

- Check Host header for unrecognized domains
- Authenticate users with something other than IP

DNS Rebinding Attack: Defenses



Firewall defenses

- External names can't resolve to internal addresses
- Protects browsers inside the organization

DNS Rebinding Quiz

Select all the true statements about rebinding attacks:

☑ The attacker needs to register a domain and delegate it to a server under his control.

☑ The attacker's server responds with a short TTL record.

□ A short TTL means the page will be quickly cached.

☑ The attacker exploits the same origin policy.