

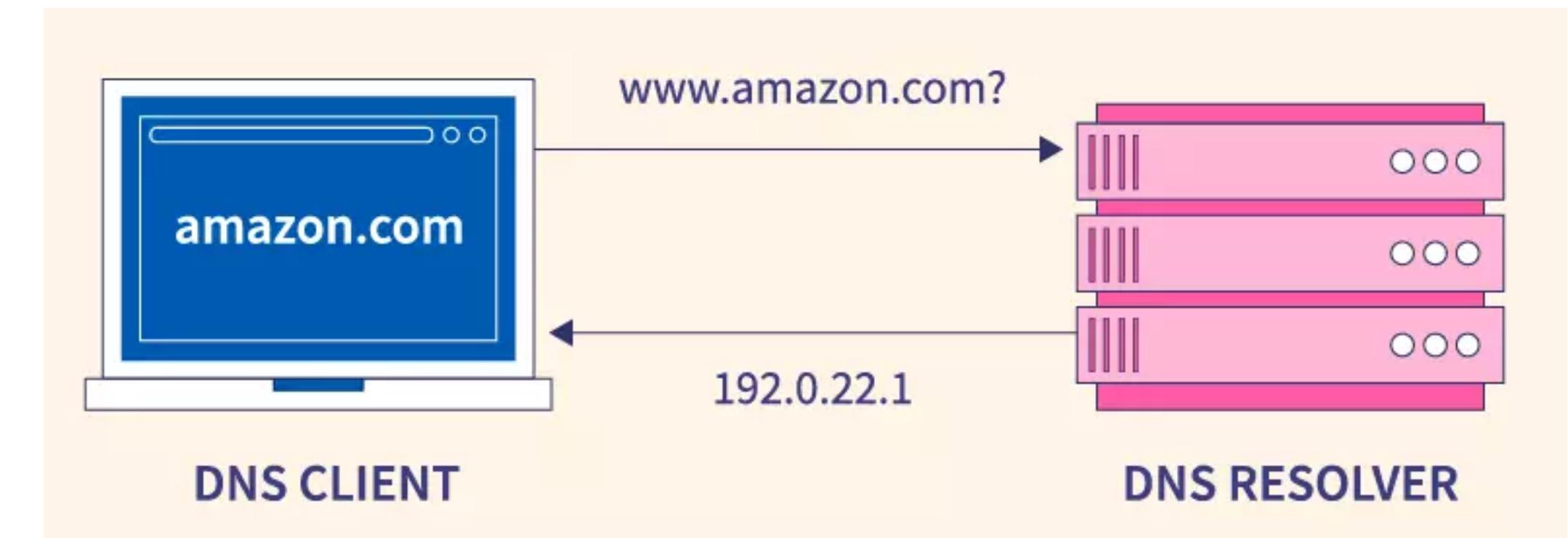
Course: CSCI 651

**Project 6: Domain
Name System**

Team Members

Khushi Mahesh
Anurag Chandra
Shreenidhi Vittala

DNS ?



Source: google.com

Working

- A system used to convert a computer's host name into an IP address on the Internet
- Its like a phonebook for our host to connect to different websites
- Example DNS server: google(8.8.8.8), cloudfare(1.1.1.1)

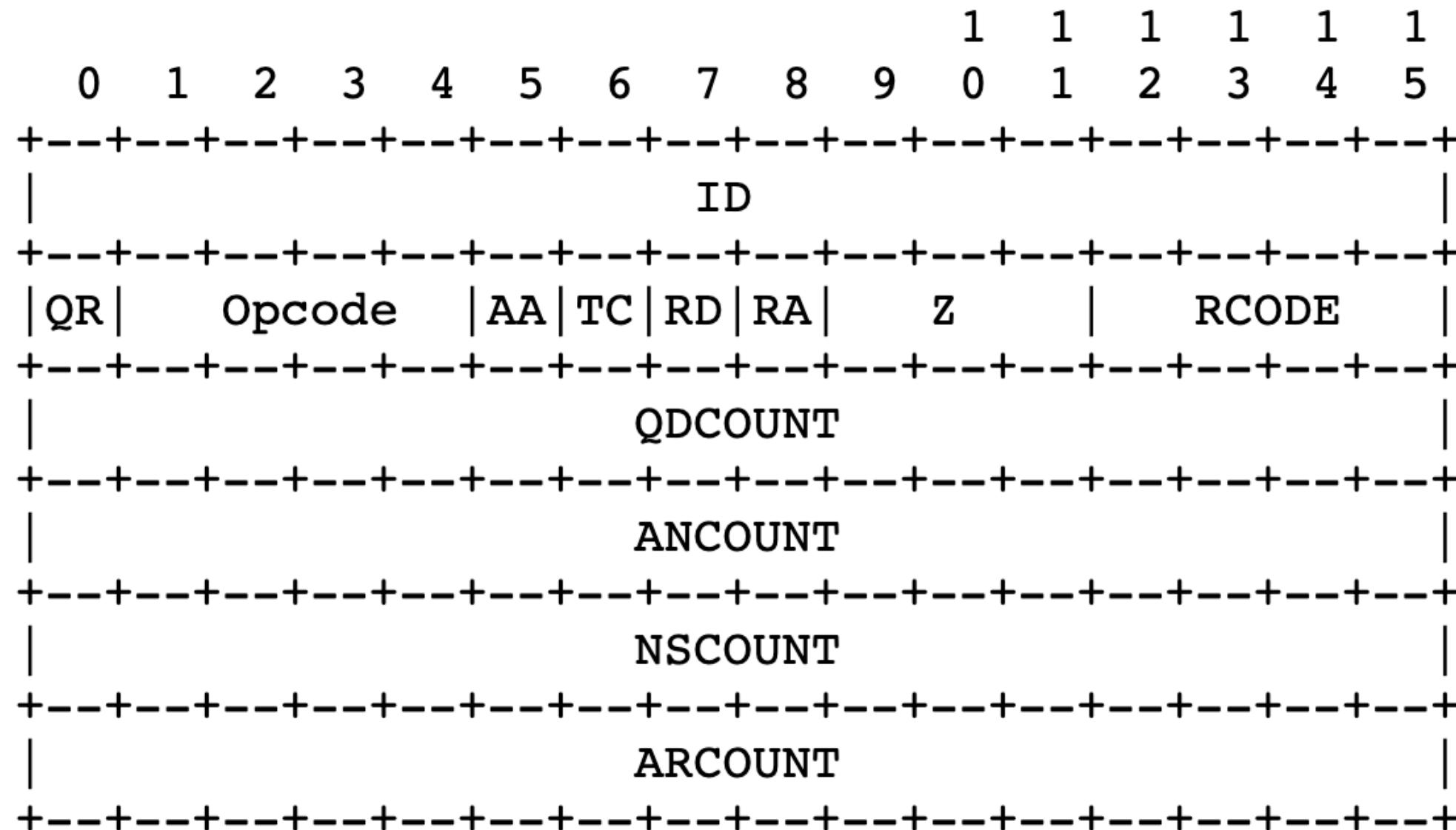
DNS Packet Structure

+-----+	
	Header
+-----+	
	Question the question for the name server
+-----+	
	Answer RRs answering the question
+-----+	
	Authority RRs pointing toward an authority
+-----+	
	Additional RRs holding additional information
+-----+	

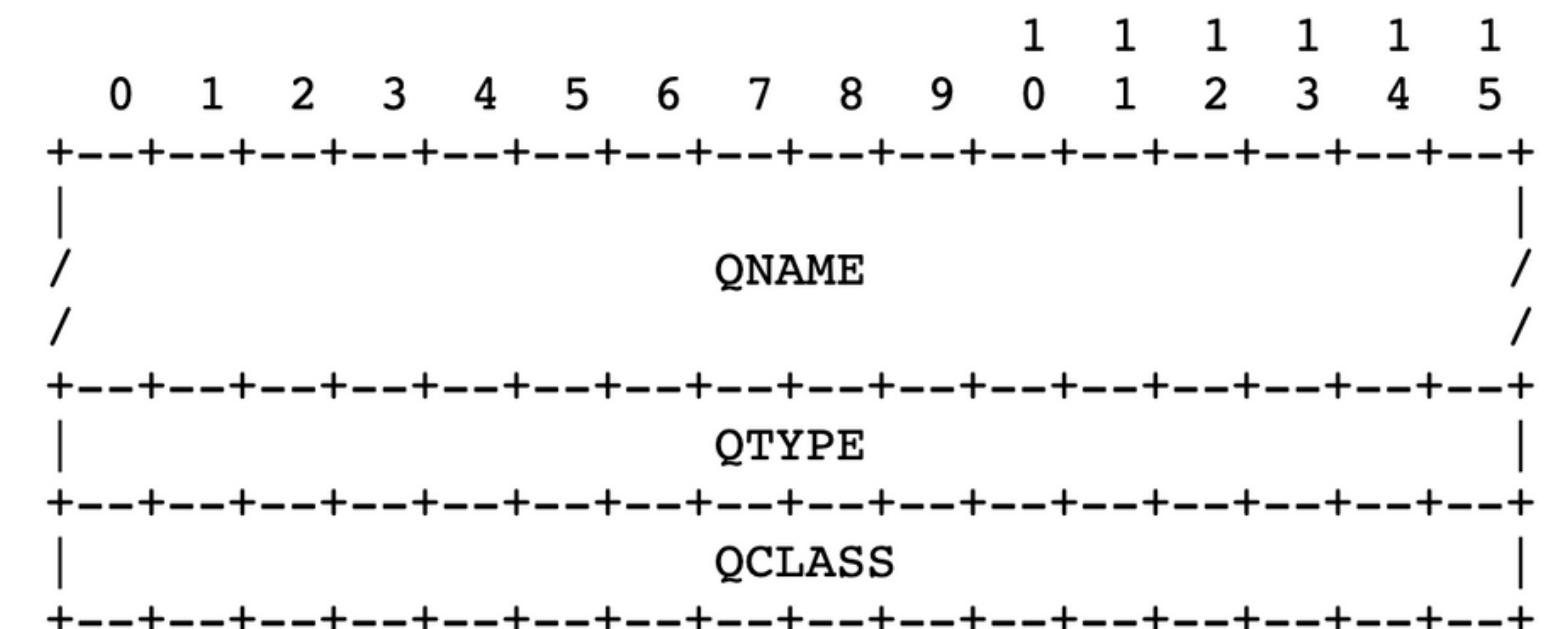
Source: RFC 1035

DNS Structure

Header Format:



Query Format:



Source: RFC 1035

DNS Structure

```
▼ Domain Name System (query)
  Transaction ID: 0x178e
  > Flags: 0x0100 Standard query
  Questions: 1
  Answer RRs: 0
  Authority RRs: 0
  Additional RRs: 0
  ▼ Queries
    ▼ image.google.com: type A, class IN
      Name: image.google.com
      [Name Length: 16]
      [Label Count: 3]
      Type: A (Host Address) (1)
      Class: IN (0x0001)
      [Response In: 7]
      0000 02 00 00 00 00 04 3c 22 fb c2 d2 51 08 00 45 00 .....<" ...Q..E.
      0010 00 3e 61 1d 00 00 40 11 ab c4 c0 a8 00 05 d0 43 .>a...@.....C
      0020 dc dc de 06 00 35 00 2a ae 19 17 8e 01 00 00 01 .....5.*.....
      0030 00 00 00 00 00 00 05 69 6d 61 67 65 06 67 6f 6f .....i mage.goo
      0040 67 6c 65 03 63 6f 6d 00 00 01 00 01 .....gle.com....
```

Source: medium.com/dns-message-how-to-read-query-and-response-message

Label Compression

Answers

- image.google.com: type CNAME, class IN, cname images.google.com
Name: image.google.com
Type: CNAME (Canonical NAME for an alias) (5)
Class: IN (0x0001)
Time to live: 60 (1 minute)
Data length: 9
CNAME: images.google.com
- images.google.com: type CNAME, class IN, cname images.l.google.com
Name: images.google.com
Type: CNAME (Canonical NAME for an alias) (5)
Class: IN (0x0001)
Time to live: 604800 (7 days)
Data length: 11

Offset	Hex	Dec	Description
0000	3c 22 fb c2 d2 51 02 00 00 00 00 04 08 00 45 00	196 34 251 194 82 81 2 0 0 0 0 0 4 8 0 71 0	<"...Q...E...
0010	00 7a 15 b0 40 00 3b 11 bb f5 d0 43 dc dc c0 a8	0 122 21 160 64 0 51 17 247 201 67 53 53 192 170z...@...;...C....
0020	00 05 00 35 de 06 00 66 e1 b0 17 8e 2 81 80 00 01 6	0 5 0 53 223 6 0 66 161 17 142 131 152 0 1 65....f.....
0030	00 03 00 00 00 00 05 69 14 6d 61 67 65 06 67 9 6f 0 22	0 3 0 0 0 0 5 105 22 109 97 96 92 94 6 109 15 102i mage.goo
0040	67 8 6c l 65 03 63 6f 0 0 0 0 00 00 01 00 01 c0 0c 00 05 38	103 8 102 101 103 100 103 105 100 100 100 100 101 100 101 100 105 56	gle.com.....
0050	00 01 00 00 00 3c 00 09 46 06 69 i 6d m 61 67 g e 73 s c0	0 1 0 0 0 0 54 0 9 72 6 105 101 109 107 101 105 101 105 101 100<... images.
0060	12 c0 2e 00 05 00 01 00 09 3a 80 00 0b 06 69 6d	18 192 34 0 5 0 1 0 9 54 80 0 111 6 109 105 101	..im.....
0070	61 67 65 73 01 6c c0 12 c0 43 00 01 00 01 00 00	97 102 101 115 1 102 112 100 109 43 0 1 100 101 100 0	ages.l... .C.....
0080	01 2c 00 04 ac d9 01 0e	1 42 0 4 172 185 1 14	,

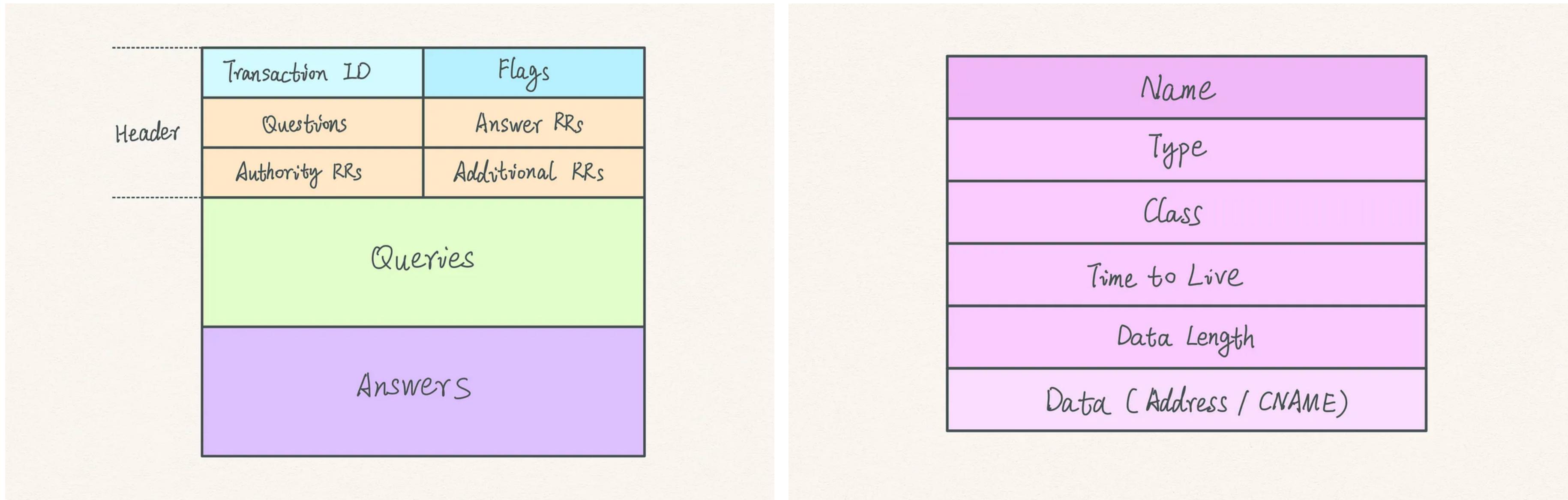
Start

offset 46 bytes

Source: medium.com/dns-message-how-to-read-query-and-response-message

DNS Structure

Response Message



Source: medium.com/dns-message-how-to-read-query-and-response-message

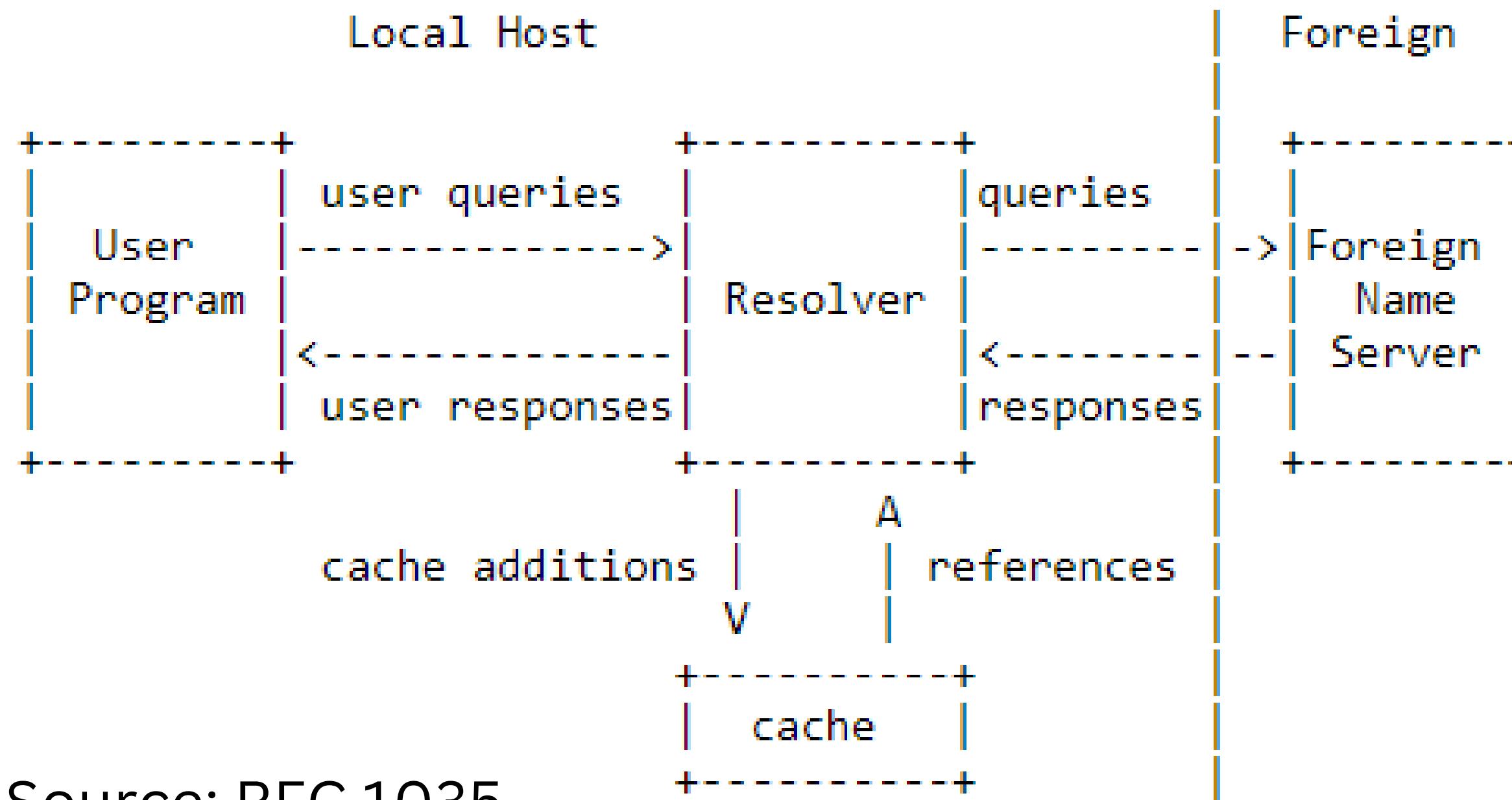
DNS Structure

```
▼ Domain Name System (response)
  Transaction ID: 0x178e
  > Flags: 0x8180 Standard query response, No error
  Questions: 1
  Answer RRs: 3
  Authority RRs: 0
  Additional RRs: 0
  > Queries
  ▼ Answers
    > image.google.com: type CNAME, class IN, cname images.google.com
    > images.google.com: type CNAME, class IN, cname images.l.google.com
    > images.l.google.com: type A, class IN, addr 172.217.1.14
  [Request In: 5]
  [Time: 0.038051000 seconds]

  0000 3c 22 fb c2 d2 51 02 00 00 00 00 04 08 00 45 00 <"....Q... ....E.
  0010 00 7a 15 b0 40 00 3b 11 bb f5 d0 43 dc dc c0 a8 ·z...@..;.. .C...
  0020 00 05 00 35 de 06 00 66 e1 b0 17 8e 81 80 00 01 ..5...f .....
  0030 00 03 00 00 00 00 05 69 6d 61 67 65 06 67 6f 6f .....i mage·goo
  0040 67 6c 65 03 63 6f 6d 00 00 01 00 01 c0 0c 00 05 gle·com. .....
  0050 00 01 00 00 00 3c 00 09 06 69 6d 61 67 65 73 c0 .....<.. .images.
  0060 12 c0 2e 00 05 00 01 00 09 3a 80 00 0b 06 69 6d .....:....im
  0070 61 67 65 73 01 6c c0 12 c0 43 00 01 00 01 00 00 ages·l.. ·C.....
  0080 01 2c 00 04 ac d9 01 0e .,.....
```

Source: medium.com/dns-message-how-to-read-query-and-response-message

Components of DNS



Source: RFC 1035

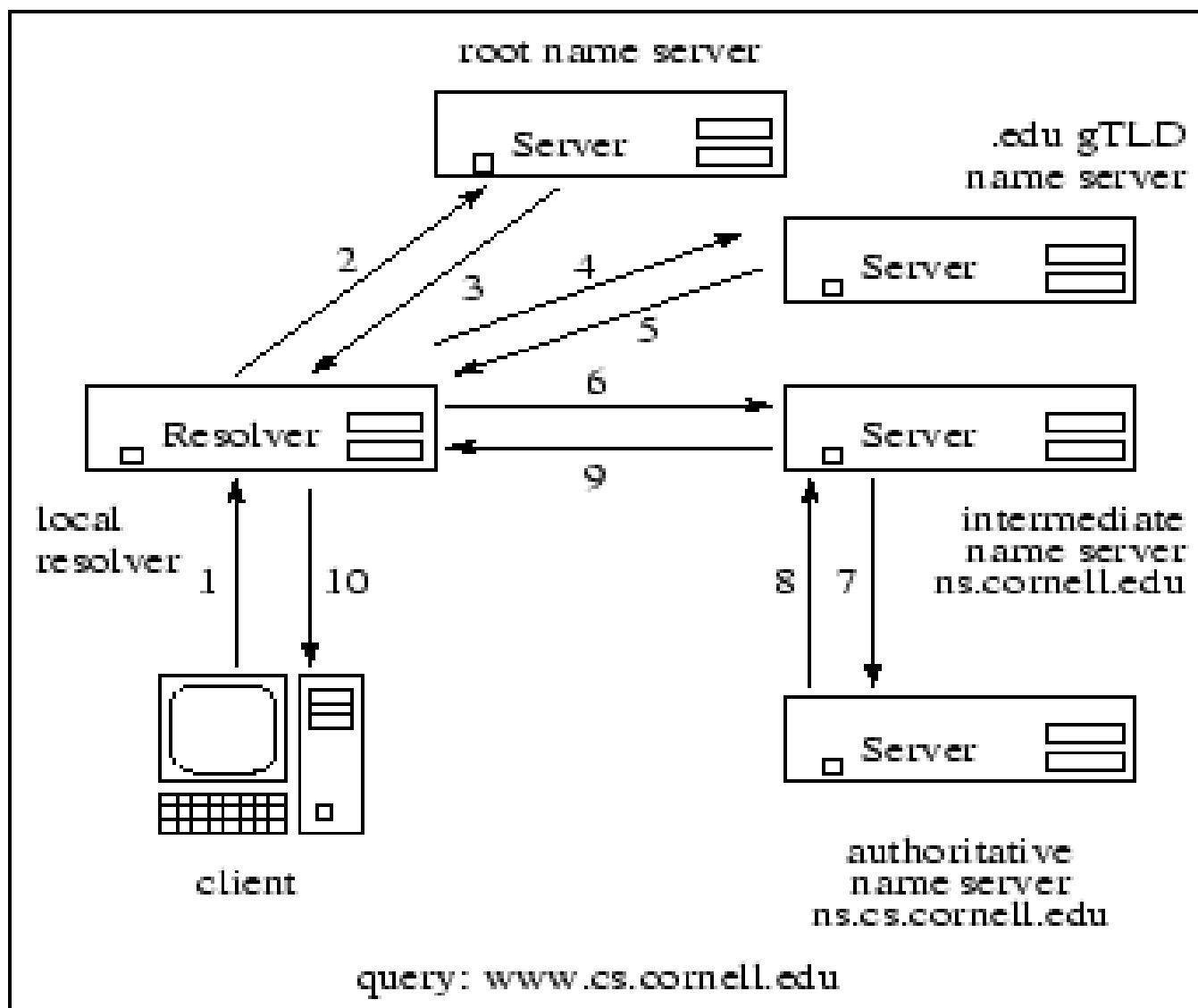
Client Implementation

- The client is an interactive terminal that can take in the input from the user for query types A and CNAME
- Recursion desired from the server can be set by the user as well
- The client then makes a function call with the domain name and query type and recursion flag to the resolver
- The return value from the resolver is then stored and displayed as output for the particular query made.

Implementation Resolver Contents

RESOLVER

Iterative DNS Query



Domain: edu
Server: k.root-servers.net

Domain: cornell.edu
Server: a.edu-servers.net

Domain: cs.cornell.edu
Server: bigred.cit.cornell.edu

Domain: www.cs.cornell.edu
Server: bigred.cit.cornell.edu

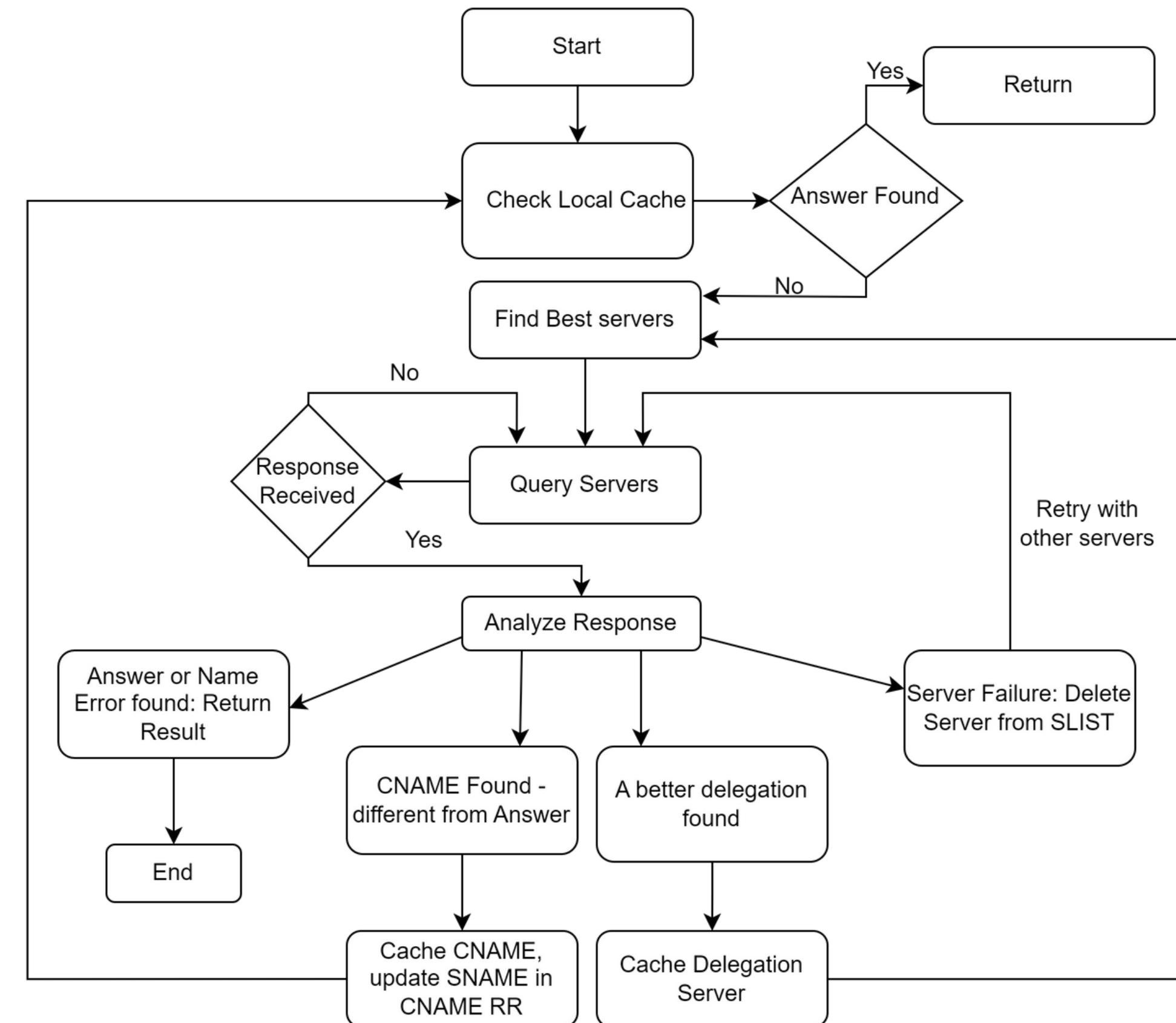
Answers:
Name: www.cs.cornell.edu
Type: CNAME
Class: 1
TTL: 86400
Server: web1.cs.cornell.edu

Name: web1.cs.cornell.edu
Type: A
Class: 1
TTL: 300
Server: 132.236.207.36

Source: cs.cornell.edu

RESOLVER ALGORITHM

Based on RFC 1034

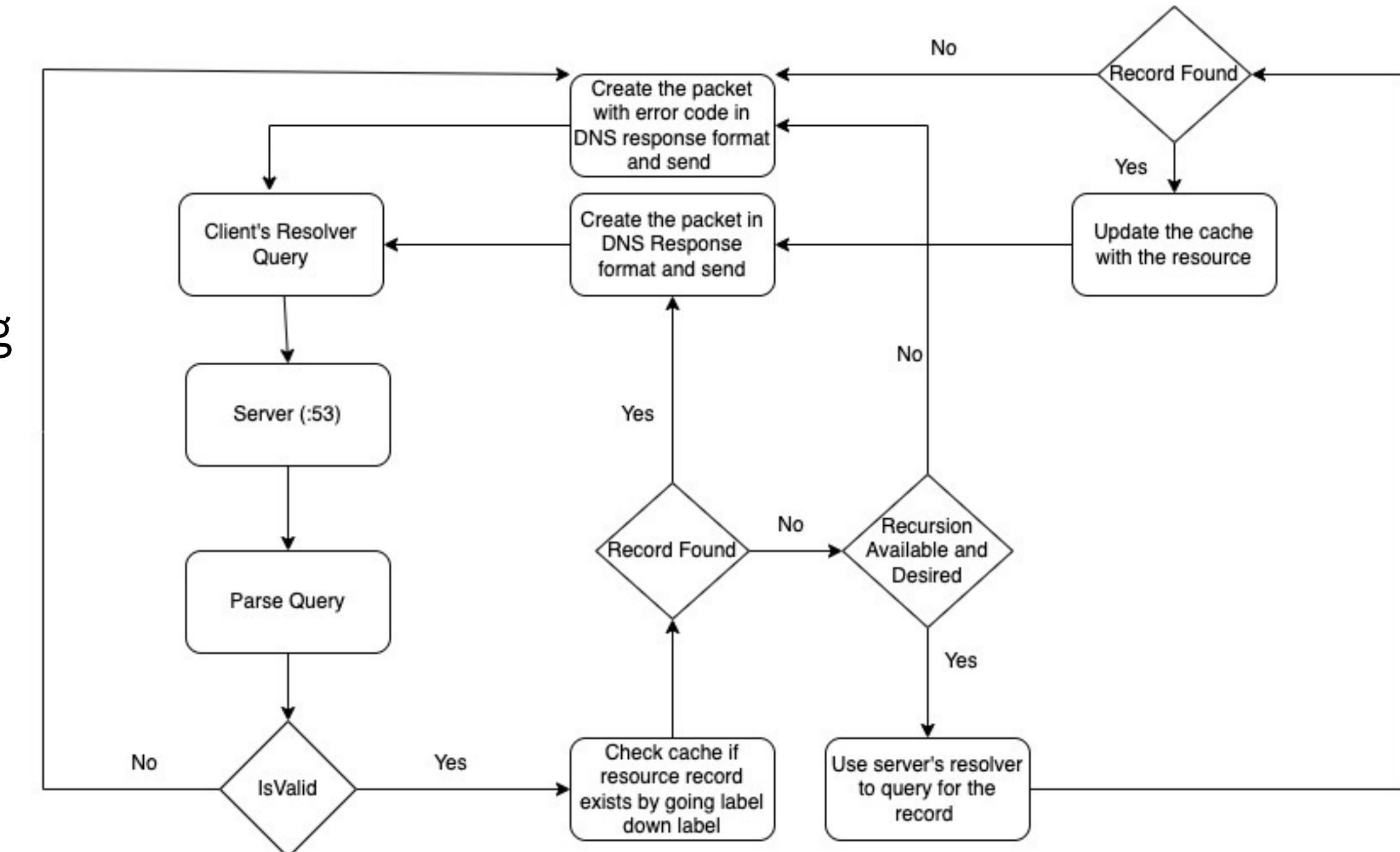


Server Implementation

Server Algorithm: RFC 1034

The DNS responses are sent as UDP packets

In case of invalid domain name, response with error code 3 indicating NXDOMAIN is set in the header and sent to the client.



DEMO

Thank you

DO YOU HAVE ANY QUESTIONS?

WE HOPE YOU LEARNT SOMETHING NEW.

