

CS 352 Project 2

Mark Malysa (mbm206), Jared Hynes (jlh484)

October 24, 2025

Part A: Recursive Resolver

Question 1

What is the value of domain name found in the question section of the DNS query?

```
05 69 6c 61 62 31 02 63 73 07 72 75 74 67 65 72 73 03 65 64 75 00
```

This encodes "ilab1.cs.rutgers.edu" in DNS wire format where each label is prefixed by its length.

Question 2

What is the value of domain name found in the answer section of DNS response? Explain.

```
c0 0c
```

This is a DNS compression pointer. The bytes c0 0c point to offset 12 (0x0C) in the DNS message where "ilab1.cs.rutgers.edu" was previously encoded in the question section. DNS uses compression to save space by avoiding repetition of domain names.

Question 3

What is the value of the rdlength field in the DNS response message?

```
00 04
```

This is 4 bytes in decimal, which is correct for an IPv4 address (A record).

Question 4

What is the value of the address received in the DNS response message?

```
80 06 0d 02
```

This converts to IP address: 128.6.13.2

Part B: NS Records

Question 5

What is the value of QDCOUNT, ANCOUNT, NSCOUNT, ARCOUNT in the DNS response message?

```
QDCOUNT: 00 01 (1 question)
ANCOUNT: 00 02 (2 answer records)
NSCOUNT: 00 00 (0 authority records)
ARCOUNT: 00 00 (0 additional records)
```

Question 6

What is the value of the rdlength field in the DNS response message?

```
Answer Record 1 (ns1.rutgers.edu): 00 06 (6 bytes)
Answer Record 2 (runs2.rutgers.edu): 00 08 (8 bytes)
```

Question 7

What are the name server names received in the response?

NS Record 1: ns1.rutgers.edu

```
03 6e 73 31 c0 0f
```

NS Record 2: runs2.rutgers.edu

```
05 72 75 6e 73 32 c0 0f
```

Both use compression pointers (c0 0f) to reference "rutgers.edu".

Part C: Iterative Resolver

Question 8

What is the value of the type field in the first DNS query among the iterative messages?

```
00 01
```

This is TYPE A (IPv4 address query) to the root server 198.41.0.4.

Question 9

What is the value of the type field value in resource records in first DNS response message among the iterative messages?

Authority Section:

```
All 13 records have TYPE: 00 02 (NS records)
```

These are the .edu TLD name servers (d.edu-servers.net, b.edu-servers.net, etc.)

Additional Section:

```
TYPE: 00 01 (A records - IPv4 addresses)
TYPE: 00 1c (AAAA records - IPv6 addresses)
```

These are glue records providing the IP addresses of the .edu name servers.

Question 10

What is the destination IP of second DNS query sent? Where is this IP found from?

Destination IP:

```
c0 1f 50 1e
```

This converts to: 192.31.80.30

This IP came from the Additional Records section (glue record) of the first DNS response from the root server. Specifically, it is the IPv4 address (A record) for d.edu-servers.net, which was listed in the Authority section. The resolver used this glue record to know where to send the second query.

Without glue records, there would be a circular dependency - you'd need to query .edu servers to find their IP addresses, but you need their IP addresses to query them!