DNS: Records and Messages

Let's now get into what DNS records and messages look like.

WE'LL COVER THE FOLLOWING

Resource Records

The DNS distributed database consists of entities called **RR**s, or **Resource Records**.

Format

RRs are 4-tuples with the following entries:

```
(name, value, type, ttl)
```

Every resource record has a `type` and a `TTL` along with a `name-value` pair. The TTL specifies **how long an RR entry can be cached by the client**. The remaining fields are described for each RR type below.

Types of RRs

- **Address**
  - Type `A` addresses are used to map IPv4 addresses to hostnames.
  - `name` is the hostname in question.
  - `value` is the IP address of the hostname.
  - **Example:** `educative.io. 299 IN A 104.20.7.183` where 299 is the TTL, educative.io is the name, `A` is the type, and `104.20.7.183` is the

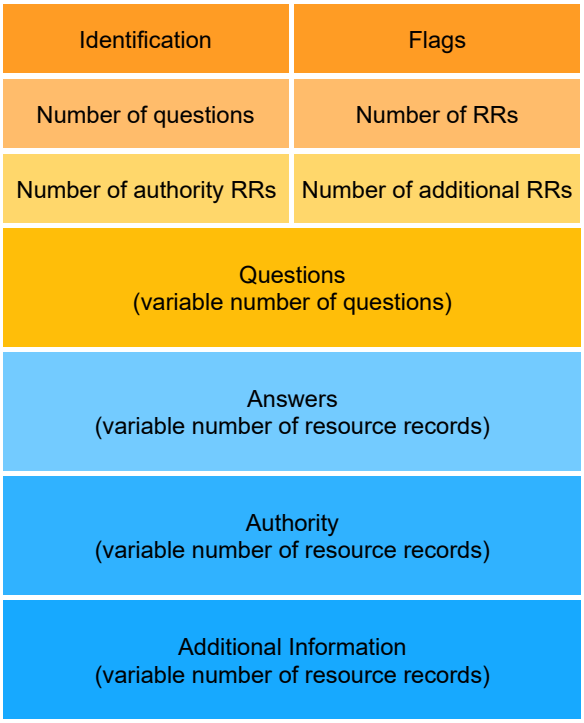
value.

- **Canonical name**
  - Type `CNAME` records are records of alias hostnames against actual hostnames. For example if, `ibm.com` is really `servereast.backup2.com`, then the latter is the canonical name of `ibm.com`.
  - `name` is the alias name for the real or 'canonical' name of the server.
  - `value` is the canonical name of the server.
  - **Example:** `bar.example.com. CNAME foo.example.com.`
- **Mail Exchanger**
  - We have seen this one before! Type `MX` records are records of the server that accepts email on behalf of a certain domain.
  - The `name` is the name of the host.
  - `value` is the name of the mail server associated with the host.
  - **Example:** `educative.io mail exchanger = 10 aspmx2.googlemail.com.`

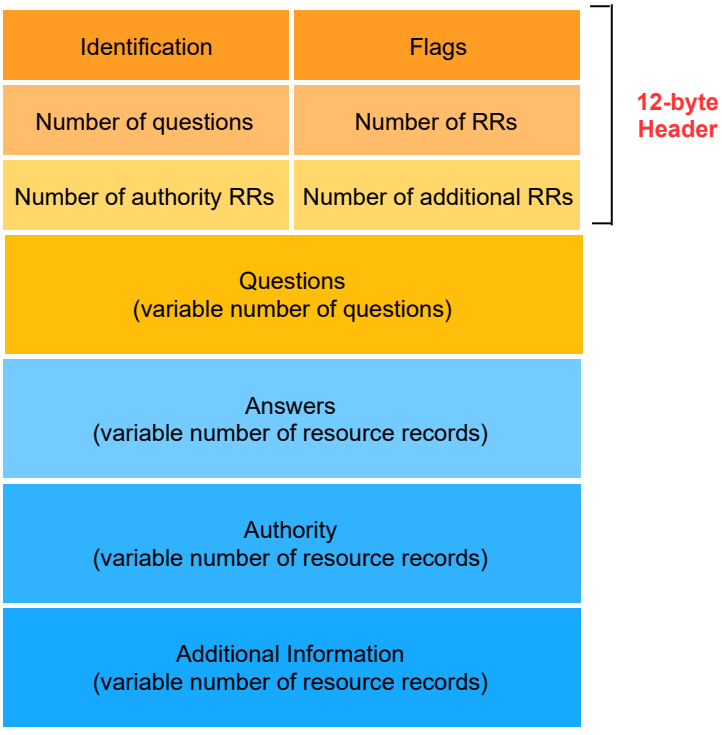
These resource records are stored in text form in special files called **zone files**.

DNS Messages

There are a few kinds of DNS messages, out of which the most common are **query** and **reply**, and both have the same format. Study the following slides for a detailed overview of a DNS message.

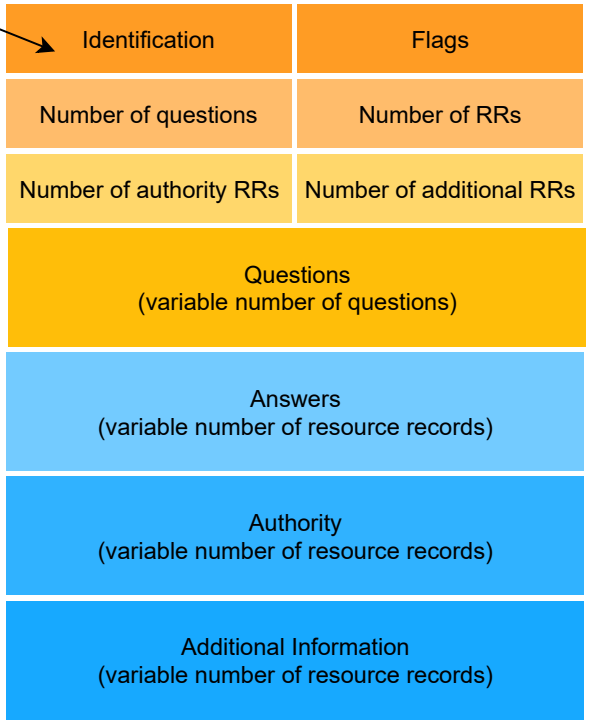


Here is a generic DNS message

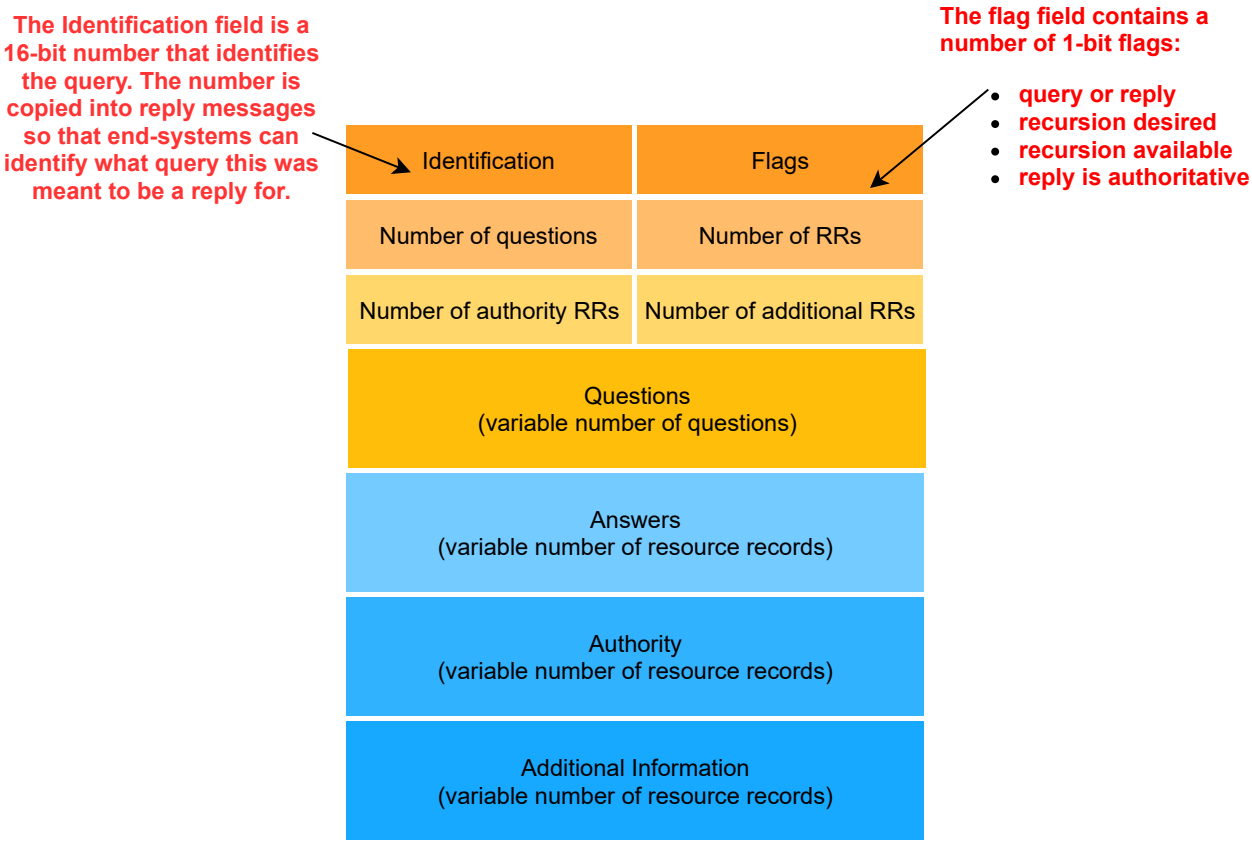


Let's discuss the header first. It is 12-bytes long and contains a number of fields.

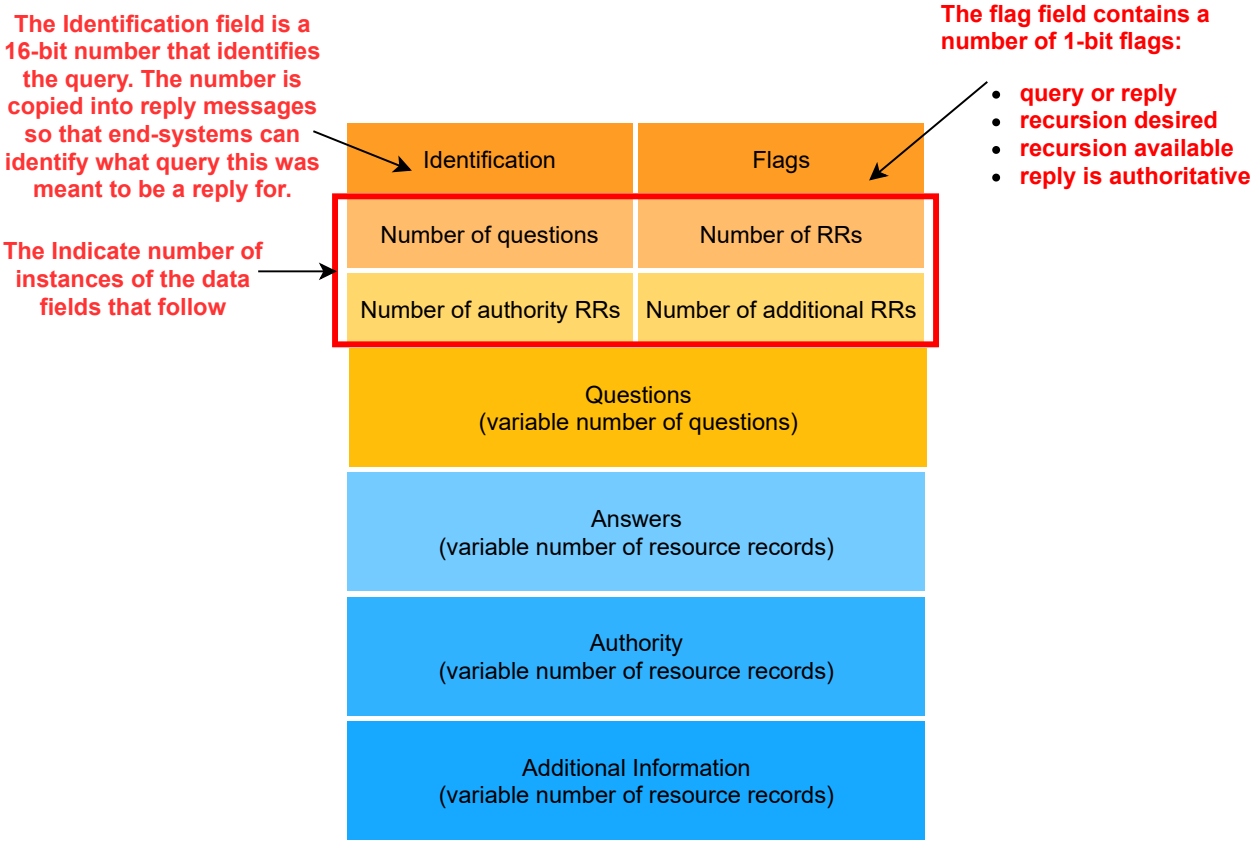
The Identification field is a 16-bit number that identifies the query. The number is copied into reply messages so that end-systems can identify what query this was meant to be a reply for.



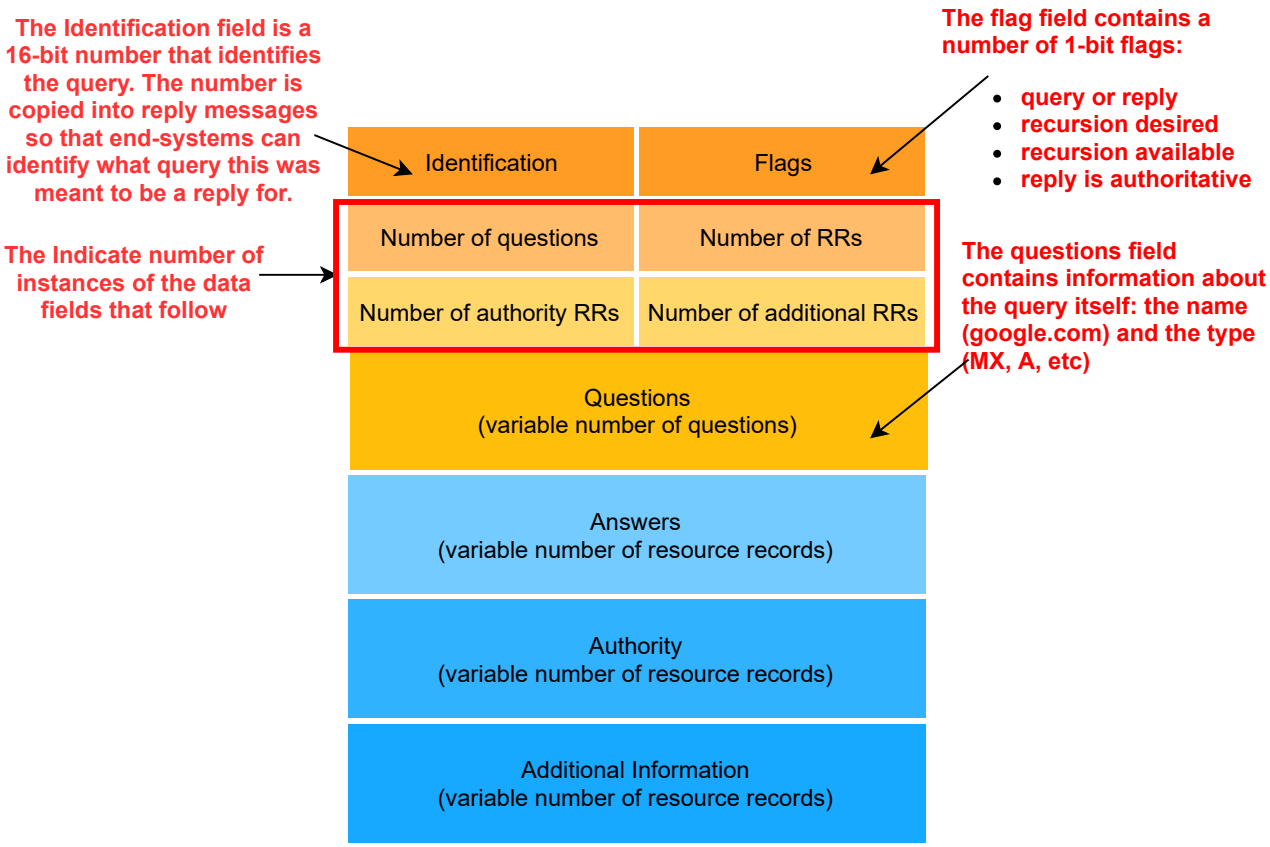
The identification field.



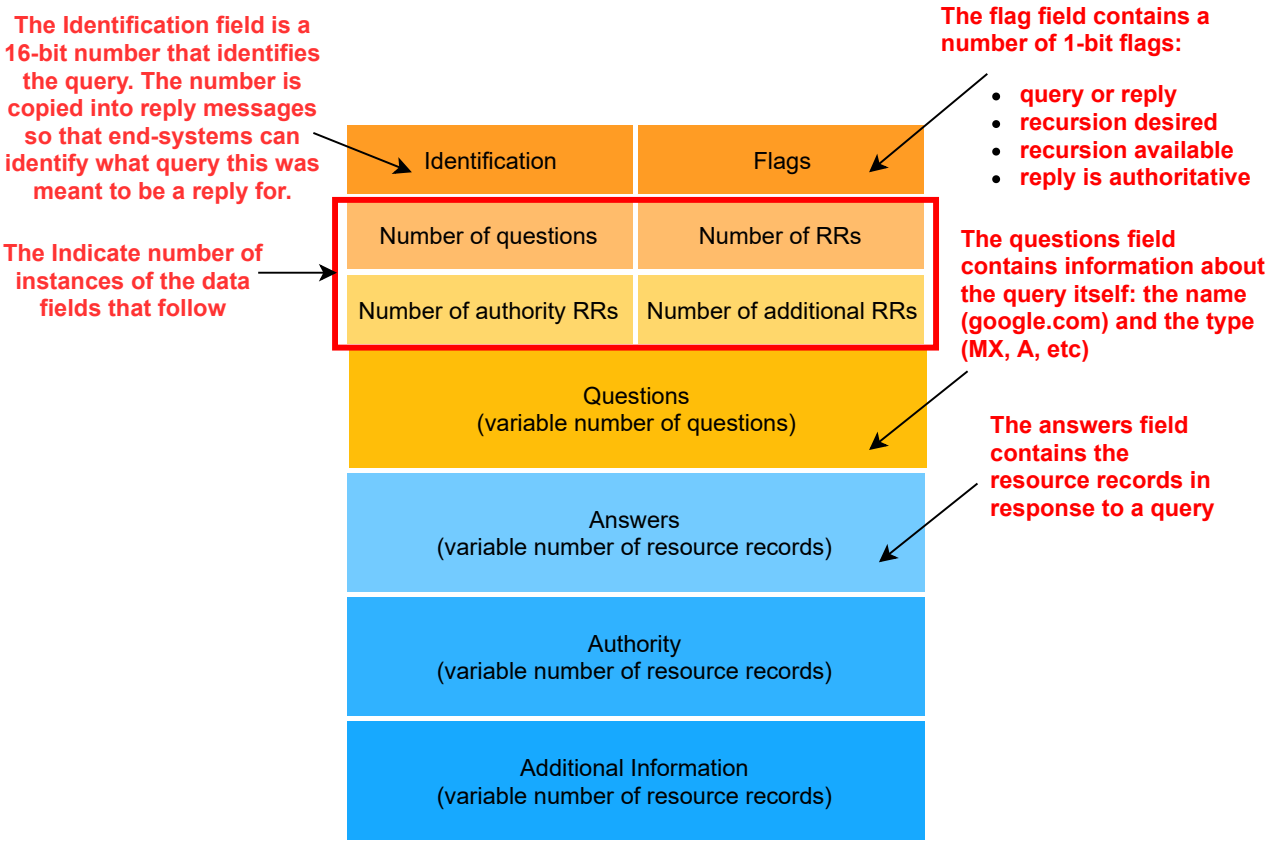
The flags field.



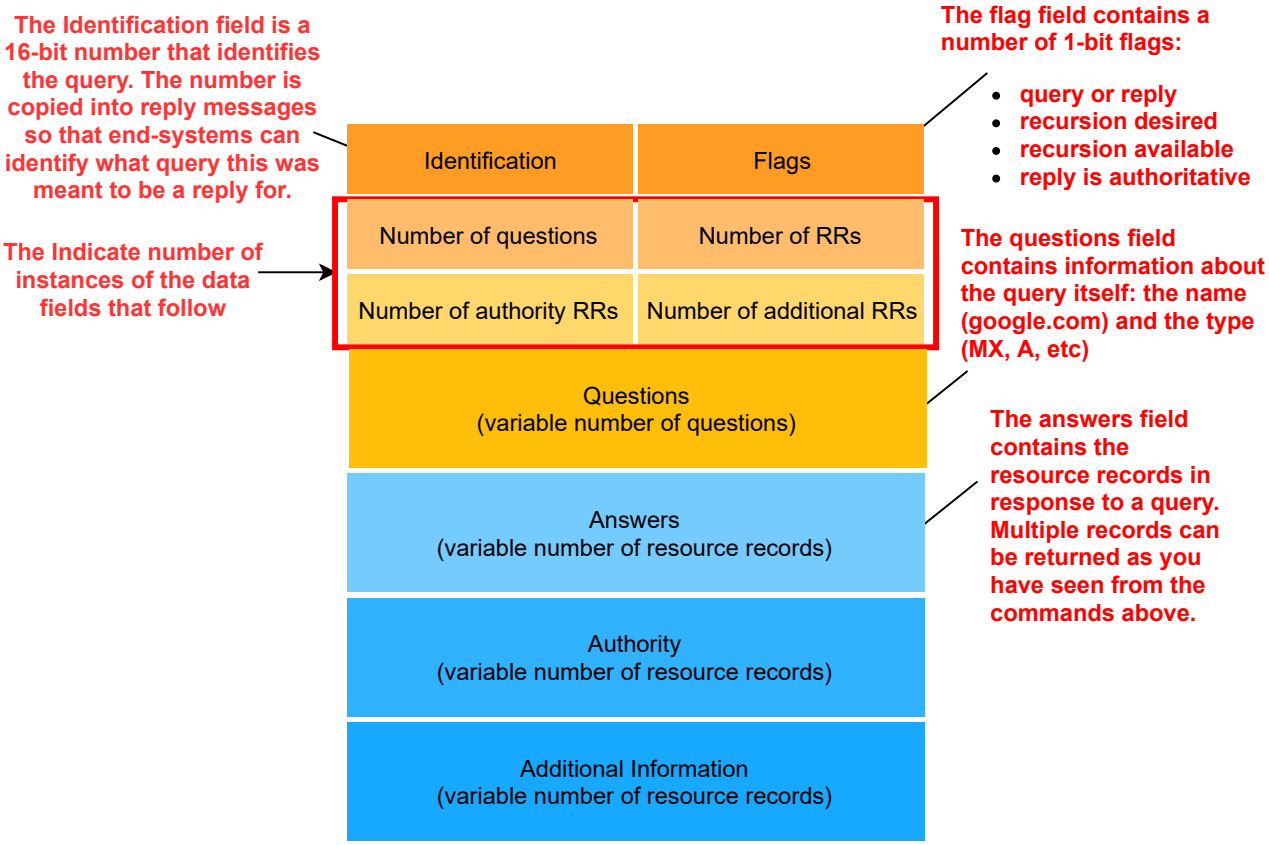
Number-of fields. These indicate the number of instances of the 4 data sections that follow.



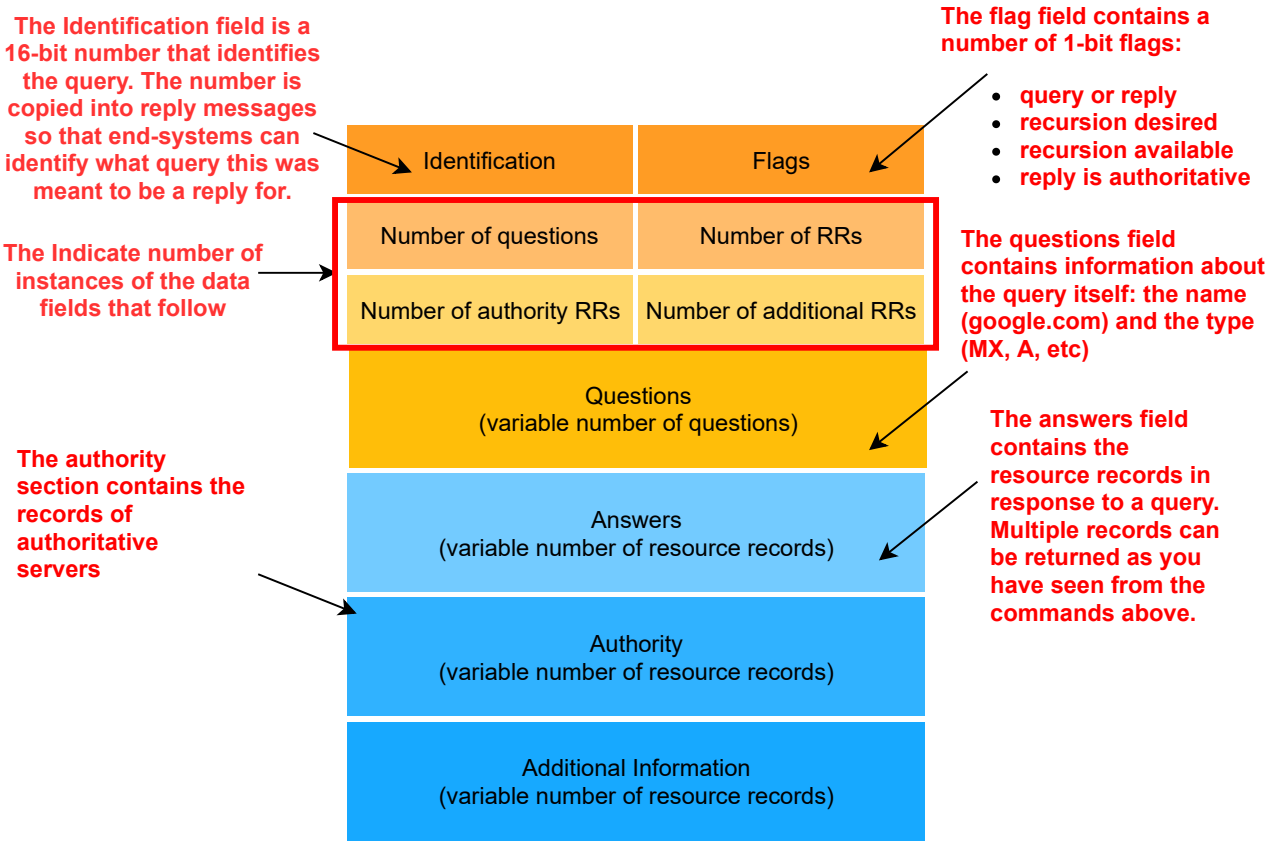
The questions field.



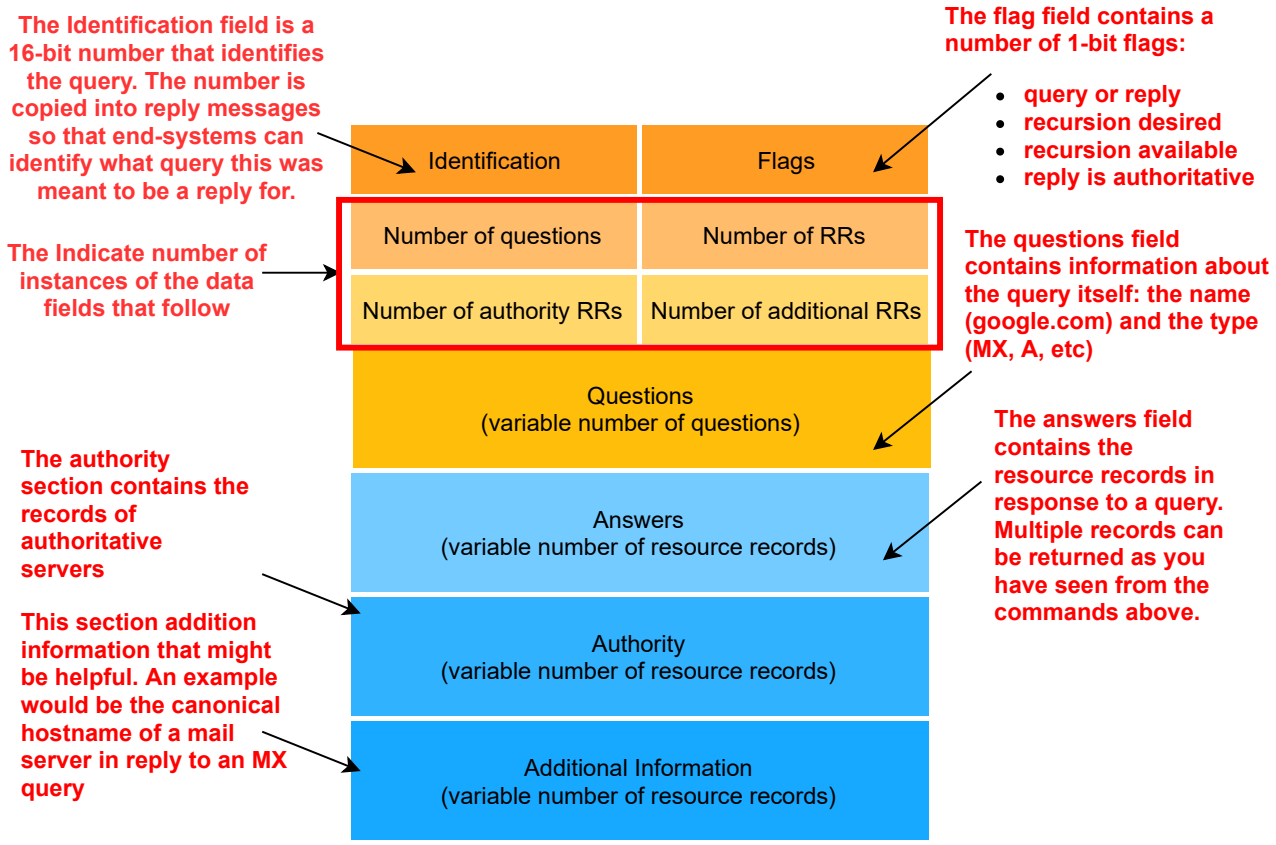
The Answers field.



The Answers field.



The Authority field.



The Additional Information field.

10 of 10

There are also **zone transfer request and response**. But, those are not used by common clients. Backup or secondary DNS servers use them for **zone transfers**, which are when zone files are copied from one server to another. This takes place over TCP.

1 Which of the following are valid DNS record entry types?

In the next lesson, we'll use command-line tools to look at DNS response messages and resource records!