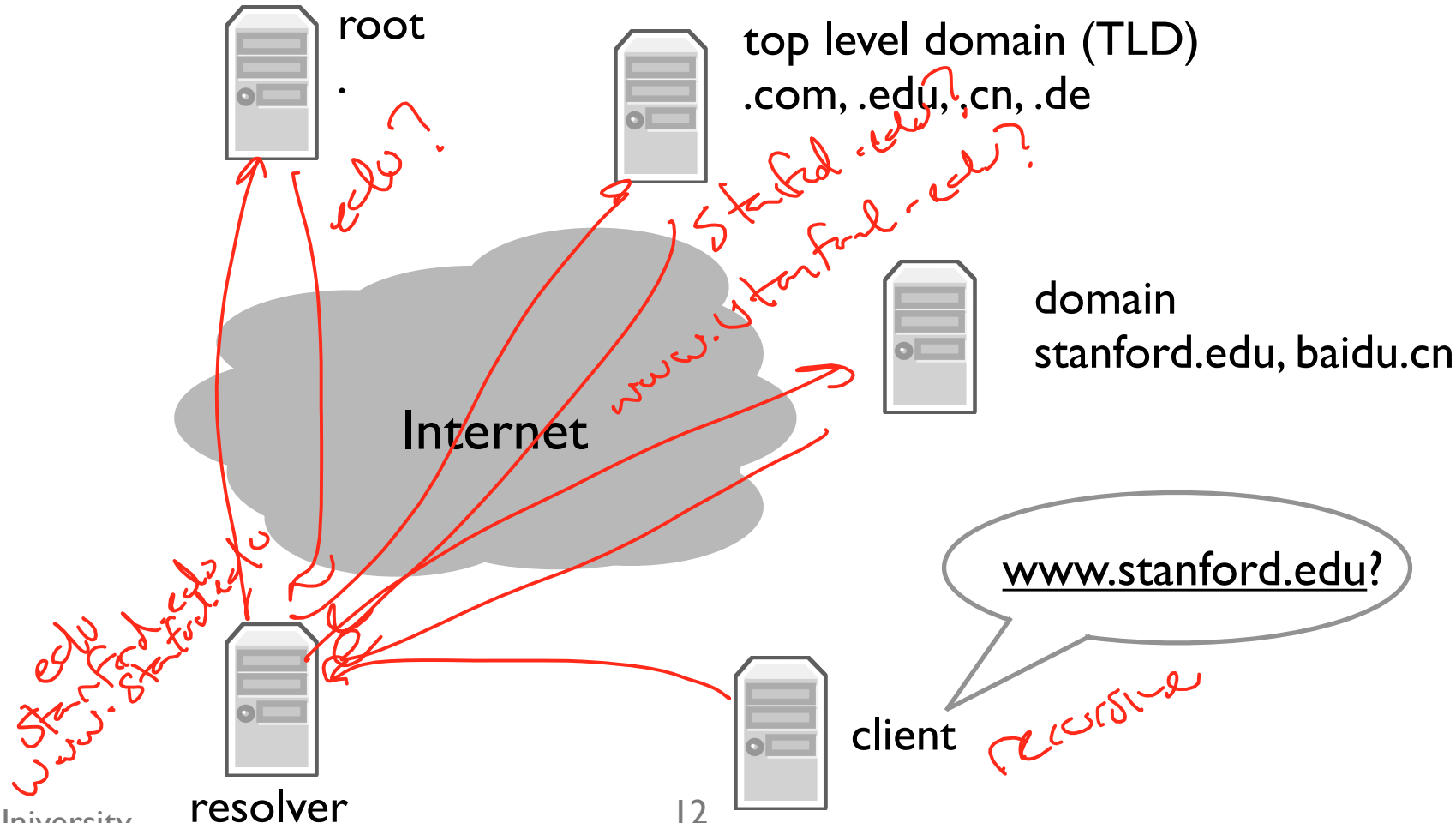
# DNS: Queries and Resource Records

# A DNS Query


root
.
top level domain (TLD)
.com, .edu, .cn, .de
domain
stanford.edu, baidu.cn
Internet
www.stanford.edu?
client
resolver
recursive

# Resource Records

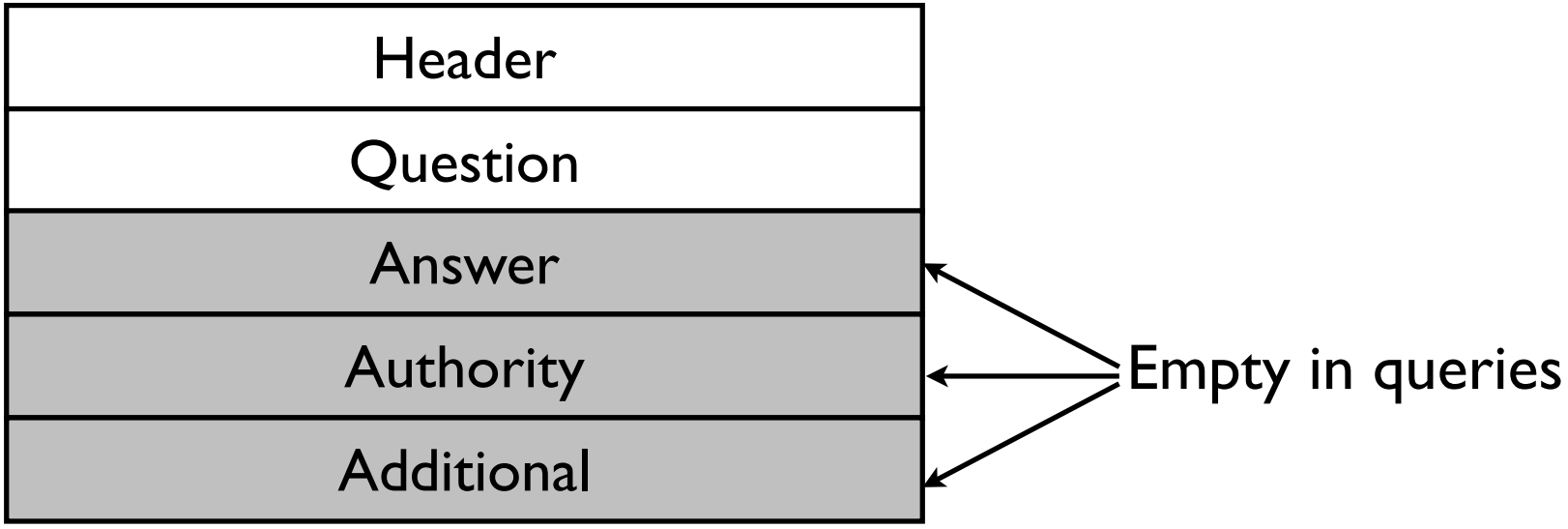
- All DNS information represented in Resource Records (RRs):

  *name [TTL] [class] type rdata*

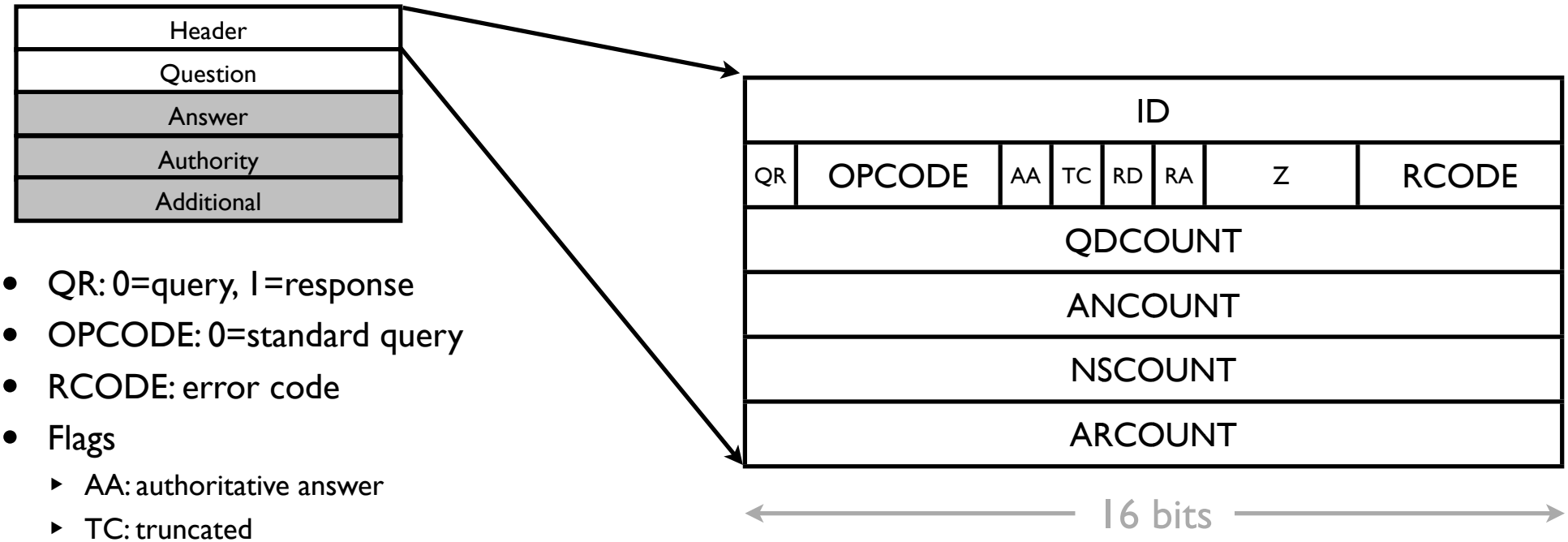
  - *name*: domain name (e.g., www.stanford.edu)
  - *TTL*: time to live (in seconds)
  - *class*: for extensibility, usually `IN 1` (Internet)
  - *type*: type of the record
  - *rdata*: resource data dependent on *type*

- Two critical RR types: A (IPv4 address) and NS (name server) records
- `dig` tool

# DNS Message Structure (RFC1035)

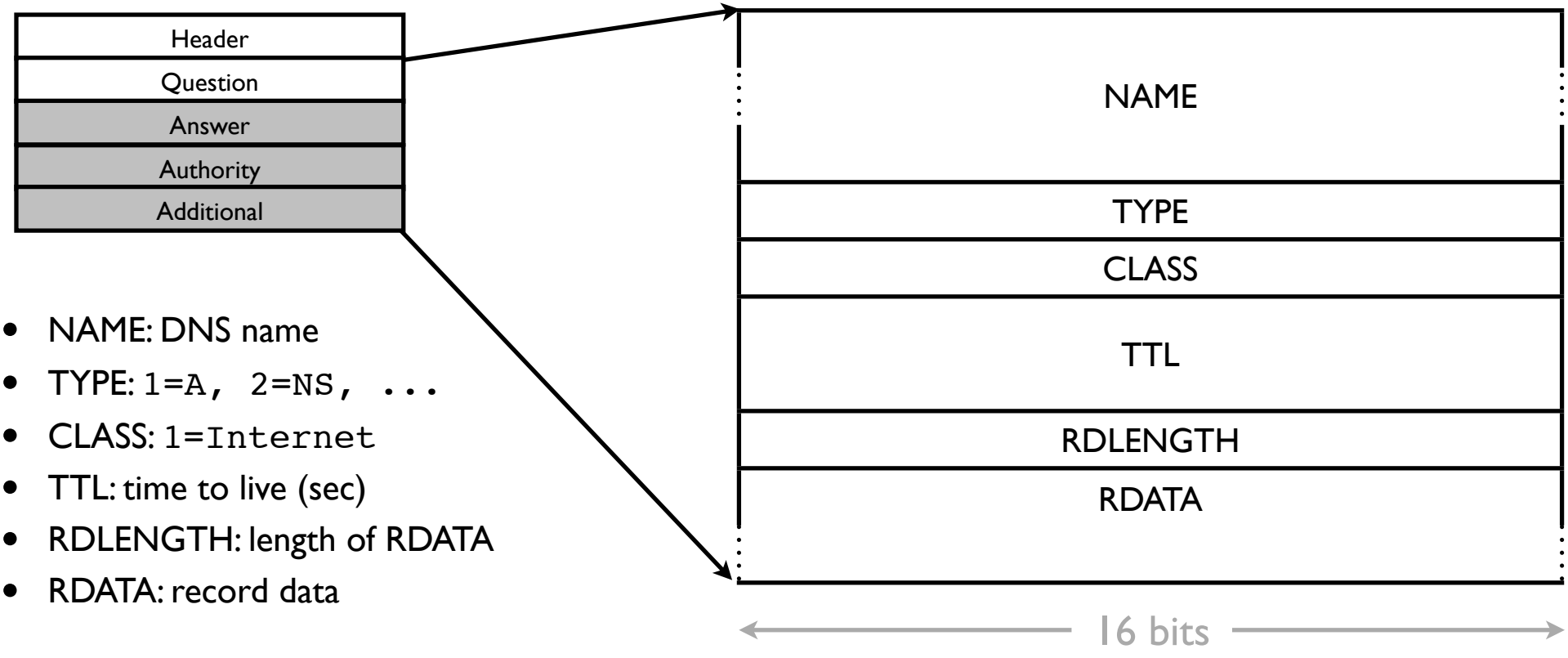


# DNS Header Structure (RFC1035)




- QR: 0=query, 1=response
- OPCODE: 0=standard query
- RCODE: error code
- Flags
  - AA: authoritative answer
  - TC: truncated
  - RD: recursion desired
  - RA: recursion available

# DNS RR Structure (RFC1035)

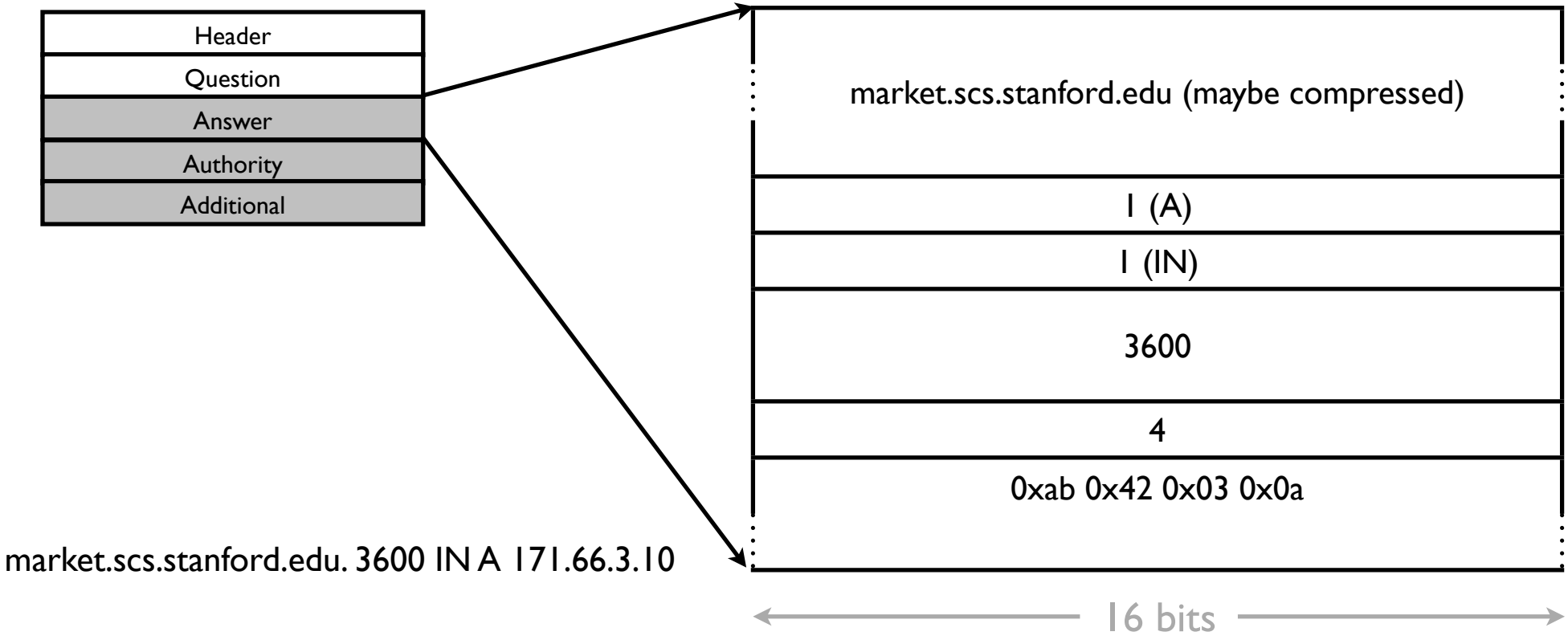



- NAME: DNS name
- TYPE: `1=A, 2=NS, ...`
- CLASS: `1=Internet`
- TTL: time to live (sec)
- RDLENGTH: length of RDATA
- RDATA: record data

# DNS Name Compression

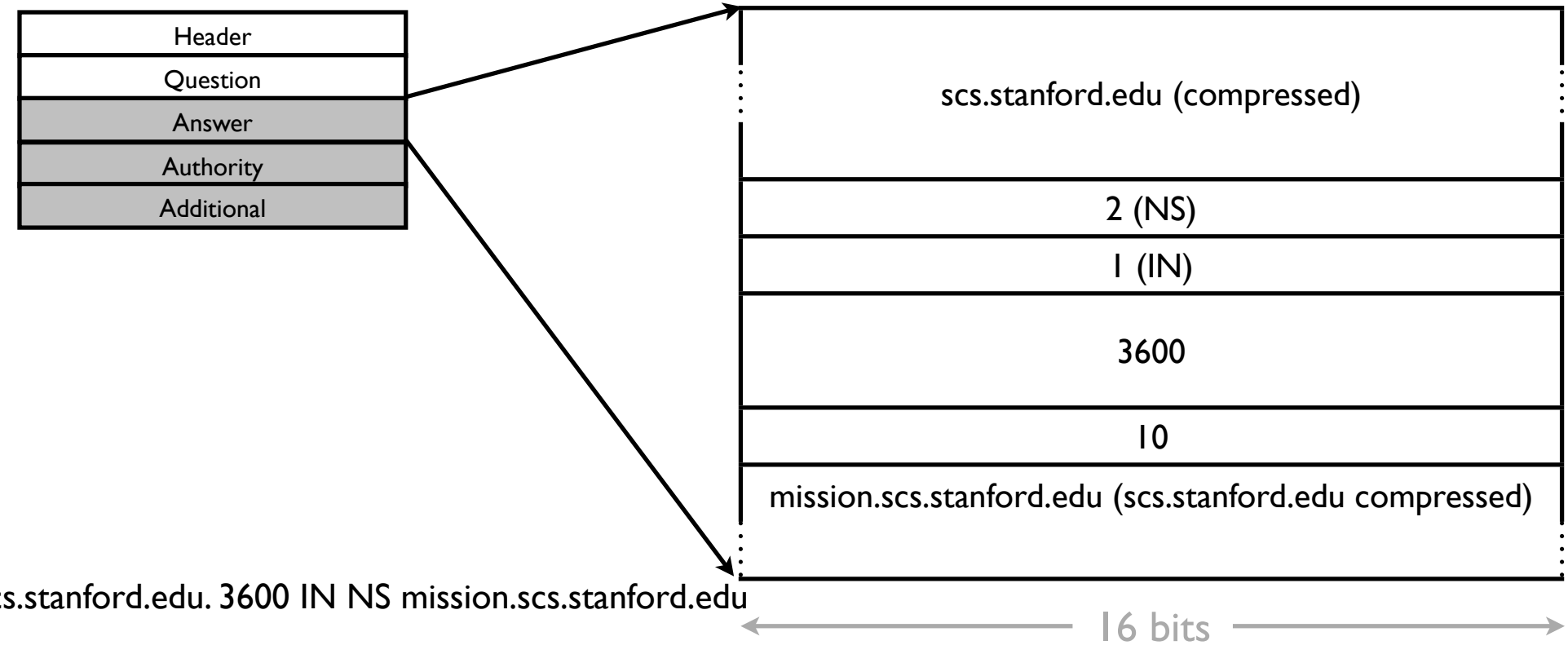
- Names can be long and repeated several times in a packet
  - Query/answer
  - NS record/A record
- Break names into labels: www.stanford.edu is www, stanford, and edu
- Each label is encoded as length, text: 3www, 8stanford, 3edu
  - Length is binary
  - Text is ASCII: 3www is 0x0377 0x7777
- If length >= 192, next 14 bits specifies offset in packet of name
  - 0xc00c means name is at offset 0xc00c-0xc000 = 0x0c = 12

# DNS A Record




market.scs.stanford.edu. 3600 IN A 171.66.3.10

# DNS NS Record



# DNS Wireshark Example