The command (for accessing the TCP client, change +notcp to +tcp):

dig @[host name] -p [port] ANY google.com. +noedns +notcp +noadflag

Deciphering:

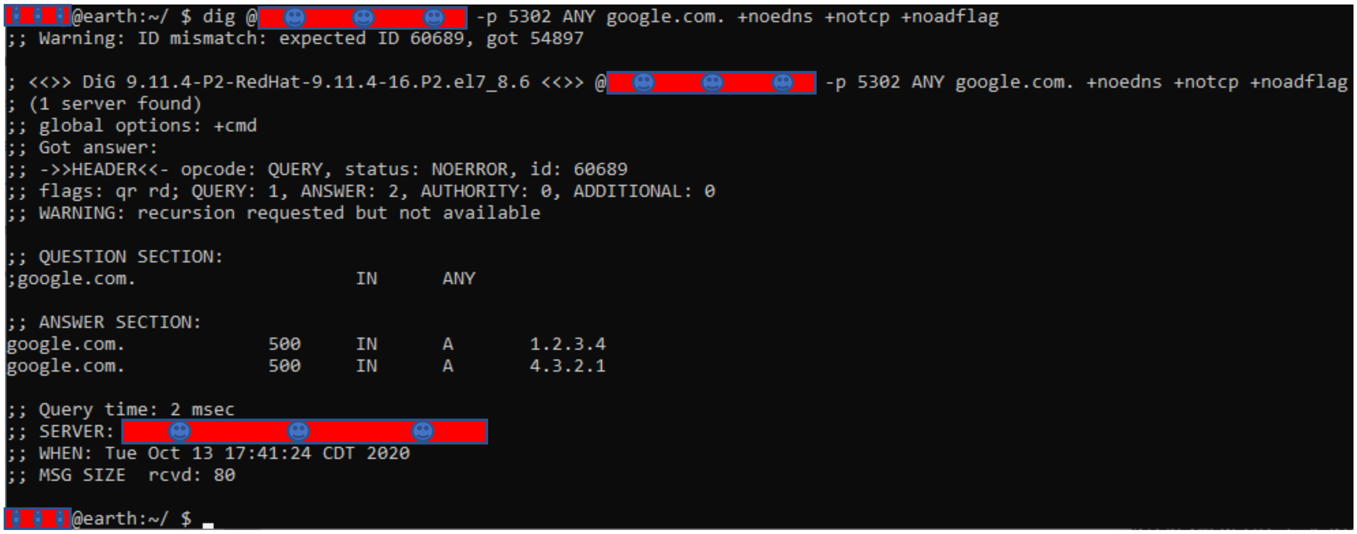
Flag	Default dig behavior	Explanation
ANY (-t ANY)	A	1
+noedns	EDNS enabled	2
+notcp	TCP when ANY	3
+noadflag	AD=1	4

Explanation:

1. The request/query type. This shows up in the QTYPE field in the DNS message header section for Question/Query (QNAME – variable length, QTYPE – 16 bits, QCLASS – 16 bits). Our specification states that it must be 0x00FF, which is the code for any class.
2. By default, dig uses extended DNS, which includes various optional fields such as Authenticated Data (AD) and Checking Disabled (CD) (DNS Security Extensions) which are bits 10 and 11 in the flags section of DNS (which we have defined in SDNS as set to 0)
3. Dig default is to use UDP, but when the ANY flag is set, dig tries to use TCP first instead.
4. As explained in (2), AD is an EDNS flag set to indicate “that all records have been validated as secure and the answer is not from a OPT-OUT range. AD=0 indicate that some part of the answer was insecure or not validated” (dig man page). In SDNS, this is in the zero area.

Additionally, the "+qr" flag is useful in determining what exactly dig is sending to the client.

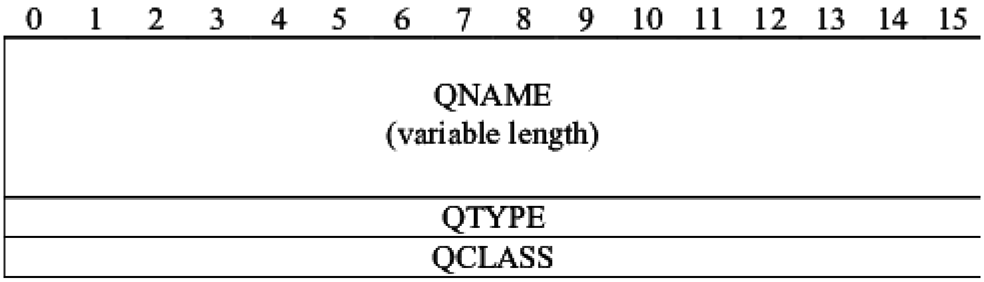
Response (this backend returns default responses instead of external DNS queries):



```
[redacted]@earth:~/ $ dig @[redacted] -p 5302 ANY google.com. +noedns +notcp +noadflag
;; Warning: ID mismatch: expected ID 60689, got 54897

; <<>> DiG 9.11.4-P2-RedHat-9.11.4-16.P2.el7_8.6 <<>> @[redacted] -p 5302 ANY google.com. +noedns +notcp +noadflag
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 60689
;; flags: qr rd; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 0
;; WARNING: recursion requested but not available

;; QUESTION SECTION:
;google.com.                    IN      ANY

;; ANSWER SECTION:
google.com.             500     IN      A       1.2.3.4
google.com.             500     IN      A       4.3.2.1

;; Query time: 2 msec
;; SERVER: [redacted]
;; WHEN: Tue Oct 13 17:41:24 CDT 2020
;; MSG SIZE  rcvd: 80

[redacted]@earth:~/ $ _
```

Resources:

- For understanding the QTYPE/Question field and specifications:
    - https://tools.ietf.org/html/rfc1035
- Visual representations of the Query/Question field



0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15

QNAME
(variable length)

QTYPE

QCLASS

- New DNS Security Extensions (and a visual representation of the newer DNS header):
    - https://unix.stackexchange.com/questions/591203/understanding-the-digs-dns-query-does-dig-set-non-zero-value-for-z-field
- for deciphering more of/more information on the DNS header:
    - https://dzone.com/articles/dissecting-dns-communications

This was in response to a class challenge to dig our servers (to discover why it didn't work). I was the only person in the entire class to get it right.

Professor's comment:

"Nice. That's the command I used. The adflag is why the tweak specification ignores the Z field. The edns is why some DNS servers are not responding fully to SDNS."