

```
Jessielee — -bash — 93x50

; <<>> DiG 9.10.6 <<>> @198.41.0.4 www.uwa.edu.au
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 13270
;; flags: qr rd; QUERY: 1, ANSWER: 0, AUTHORITY: 10, ADDITIONAL: 20
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;www.uwa.edu.au.                                IN      A

;; AUTHORITY SECTION:
au.                172800 IN      NS      d.au.
au.                172800 IN      NS      v.au.
au.                172800 IN      NS      u.au.
au.                172800 IN      NS      q.au.
au.                172800 IN      NS      t.au.
au.                172800 IN      NS      s.au.
au.                172800 IN      NS      r.au.
au.                172800 IN      NS      b.au.
au.                172800 IN      NS      a.au.
au.                172800 IN      NS      c.au.

;; ADDITIONAL SECTION:
d.au.                172800 IN      A        162.159.25.38
d.au.                172800 IN      AAAA     2400:cb00:2049:1::a29f:1926
v.au.                172800 IN      A        202.12.31.53
v.au.                172800 IN      AAAA     2001:dd8:12::53
u.au.                172800 IN      A        211.29.133.32
q.au.                172800 IN      A        65.22.196.1
q.au.                172800 IN      AAAA     2a01:8840:be::1
t.au.                172800 IN      A        65.22.199.1
t.au.                172800 IN      AAAA     2a01:8840:c1::1
s.au.                172800 IN      A        65.22.198.1
s.au.                172800 IN      AAAA     2a01:8840:c0::1
r.au.                172800 IN      A        65.22.197.1
r.au.                172800 IN      AAAA     2a01:8840:bf::1
b.au.                172800 IN      A        58.65.253.73
b.au.                172800 IN      AAAA     2407:6e00:253:306::73
a.au.                172800 IN      A        58.65.254.73
a.au.                172800 IN      AAAA     2407:6e00:254:306::73
c.au.                172800 IN      A        162.159.24.179
c.au.                172800 IN      AAAA     2400:cb00:2049:1::a29f:18b3

;; Query time: 145 msec
;; SERVER: 198.41.0.4#53(198.41.0.4)
;; WHEN: Sat Oct 06 14:43:10 PDT 2018
```

```
Jessielee — -bash — 82x44
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;www.uwa.edu.au.                IN      A

;; AUTHORITY SECTION:
uwa.edu.au.                     900     IN      NS      ns1.uwa.edu.au.
uwa.edu.au.                     900     IN      NS      ns3.aarnet.net.au.
uwa.edu.au.                     900     IN      NS      ns1.aarnet.net.au.
uwa.edu.au.                     900     IN      NS      ns2.aarnet.net.au.
uwa.edu.au.                     900     IN      NS      ns2.uwa.edu.au.

;; ADDITIONAL SECTION:
ns1.uwa.edu.au.                 900     IN      A        130.95.63.191
ns2.uwa.edu.au.                 900     IN      A        130.95.63.192

;; Query time: 95 msec
;; SERVER: 65.22.196.1#53(65.22.196.1)
;; WHEN: Sun Oct 07 20:11:56 PDT 2018
;; MSG SIZE rcvd: 176

[lijiatongdeMacBook-Pro:~ Jessielee$ dig @130.95.63.191 www.uwa.edu.au ]

; <<>> DiG 9.10.6 <<>> @130.95.63.191 www.uwa.edu.au
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 9960
;; flags: qr aa rd; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;www.uwa.edu.au.                IN      A

;; ANSWER SECTION:
www.uwa.edu.au.                 300     IN      CNAME    www.uwa.edu.au.cdn.cloudflare.net.

;; Query time: 395 msec
;; SERVER: 130.95.63.191#53(130.95.63.191)
;; WHEN: Sun Oct 07 20:12:21 PDT 2018
;; MSG SIZE rcvd: 90

lijiatongdeMacBook-Pro:~ Jessielee$
```

Step2:

No.	Time	Source	Destination	Protocol	Length	Info
393	675.067787	172.20.10.1	172.20.10.4	DNS	147	Standard query response 0x5e0d A static.doubleclick.net CNAME ...
394	675.069432	172.20.10.1	172.20.10.4	DNS	159	Standard query response 0xd29a AAAA static.doubleclick.net CNA...
395	675.501930	172.20.10.4	172.20.10.1	DNS	71	Standard query 0x77ee A s.ytimg.com
396	675.502098	172.20.10.4	172.20.10.1	DNS	71	Standard query 0xbe5f AAAA s.ytimg.com
397	675.566785	172.20.10.1	172.20.10.4	DNS	119	Standard query response 0x77ee A s.ytimg.com CNAME ytstatic.l...
398	675.568239	172.20.10.1	172.20.10.4	DNS	131	Standard query response 0xbe5f AAAA s.ytimg.com CNAME ytstatic...
399	675.710991	172.20.10.4	172.20.10.1	DNS	92	Standard query 0xa30e A r4---sn-a5mekner.googlevideo.com
400	675.711153	172.20.10.4	172.20.10.1	DNS	92	Standard query 0x1fff AAAA r4---sn-a5mekner.googlevideo.com
401	675.770040	172.20.10.1	172.20.10.4	DNS	137	Standard query response 0xa30e A r4---sn-a5mekner.googlevideo...
402	675.775503	172.20.10.1	172.20.10.4	DNS	149	Standard query response 0x1fff AAAA r4---sn-a5mekner.googlevid...
403	680.084080	172.20.10.4	172.20.10.1	DNS	84	Standard query 0x168d A notifications.google.com
404	680.084258	172.20.10.4	172.20.10.1	DNS	84	Standard query 0xbd91 AAAA notifications.google.com
405	680.161656	172.20.10.1	172.20.10.4	DNS	133	Standard query response 0xbd91 AAAA notifications.google.com C...
406	680.161709	172.20.10.1	172.20.10.4	DNS	121	Standard query response 0x168d A notifications.google.com CNAM...

▶ Frame 319: 103 bytes on wire (824 bits), 103 bytes captured (824 bits) on interface 0
 ▶ Ethernet II, Src: Apple_d1:97:ff (ac:bc:32:d1:97:ff), Dst: ba:44:d9:32:22:64 (ba:44:d9:32:22:64)
 ▶ Internet Protocol Version 6, Src: fe80::435:5f50:ca80:aeea, Dst: fe80::c82:8266:670c:3884
 ▼ User Datagram Protocol, Src Port: 54211, Dst Port: 53

Source Port: 54211
 Destination Port: 53
 Length: 49
 Checksum: 0x2435 [unverified]
 [Checksum Status: Unverified]
 [Stream index: 141]

```

0000  ba 44 d9 32 22 64 ac bc 32 d1 97 ff 86 dd 60 02  .D.2"d.. 2.....
0010  81 c6 00 31 11 ff fe 80 00 00 00 00 00 04 35  ...1.....5
0020  5f 50 ca 80 ae ea fe 80 00 00 00 00 00 0c 82  _P.....
0030  82 66 67 0c 38 84 d3 c3 00 35 00 31 24 35 d2 dd  .fg.8....5 1$5..
0040  01 00 00 01 00 00 00 00 00 00 0a 67 6d 61 69 6c  .....gmail
0050  2d 69 6d 61 70 01 6c 06 67 6f 6f 67 6c 65 03 63  -imap..l. google.c
0060  6f 6d 00 00 1c 00 01  om.....
  
```

User Datagram Protocol (udp), 8 bytes
 Packets: 406 · Displayed: 406 (100.0%)
 Profile: Default

Step4:

1. How many bits long is the Transaction ID? Based on this length, take your best guess as to how likely it is that concurrent transactions will use the same transaction ID.

16 bits;

it is very unlikely to have concurrent transactions which use the same transaction ID, only if 2^{16} query/response pairs happen at the same time.

2. Which flag bit and what values signifies whether the DNS message is a query or response?

The first flag bit signifies query or response. A “0” indicates a query, and hence a “1” a response.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	172.20.10.4	198.41.0.4	DNS	85	Standard query 0x542c A www.uwa.edu.au OPT
2	0.156758	198.41.0.4	172.20.10.4	DNS	657	Standard query response 0x542c A www.uwa.edu.au NS d.au NS v.au ...
3	22.112500	fe80::435:5f50:ca8...	fe80::c82:8266:670...	DNS	90	Standard query 0x0e6b A github.com
4	22.202581	fe80::c82:8266:670...	fe80::435:5f50:ca8...	DNS	122	Standard query response 0x0e6b A github.com A 192.30.255.112 A 1...

Checksum: 0x4efa [unverified]
[Checksum Status: Unverified]
[Stream index: 0]

▼ Domain Name System (query)
Transaction ID: 0x542c
▼ Flags: 0x0120 Standard query

0... .. = Response: Message is a query
.000 0... .. = Opcode: Standard query (0)
.... 0... .. = Truncated: Message is not truncated
.... 1... .. = Recursion desired: Do query recursively
.... 0... .. = Z: reserved (0)
.... 1... .. = AD bit: Set
.... 0... .. = Non-authenticated data: Unacceptable

Questions: 1

0000ba 44 d9 32 22 64 ac bc 32 d1 97 ff 08 00 45 00 .D 2"d . 2 E .
001000 47 bf 7a 00 00 40 11 3e e6 ac 14 0a 04 c6 29 .G z . @ . >)
002000 04 e0 b1 00 35 00 33 4e fa 54 2c 01 20 00 01 5 3 N T , . . .
003000 00 00 00 00 00 01 03 77 77 77 03 75 77 61 03 65 w w w . u w a . e
004064 75 02 61 75 00 00 01 00 01 00 00 29 10 00 00 d u . a u) . . .
005000 00 00 00 00

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	172.20.10.4	198.41.0.4	DNS	85	Standard query 0x542c A www.uwa.edu.au OPT
2	0.156758	198.41.0.4	172.20.10.4	DNS	657	Standard query response 0x542c A www.uwa.edu.au NS d.au NS v.au ...
3	22.112500	fe80::435:5f50:ca8...	fe80::c82:8266:670...	DNS	90	Standard query 0x0e6b A github.com
4	22.202581	fe80::c82:8266:670...	fe80::435:5f50:ca8...	DNS	122	Standard query response 0x0e6b A github.com A 192.30.255.112 A 1...
5	22.764959	fe80::435:5f50:ca8...	fe80::c82:8266:670...	DNS	94	Standard query 0x7fc1 A api.github.com
6	22.837183	fe80::c82:8266:670...	fe80::435:5f50:ca8...	DNS	126	Standard query response 0x7fc1 A api.github.com A 192.30.255.117...
7	32.895434	172.20.10.4	172.20.10.1	DNS	75	Standard query 0x54ce A play.google.com
8	32.896341	172.20.10.4	172.20.10.1	DNS	75	Standard query 0x7118 AAAA play.google.com
9	33.001111	172.20.10.1	172.20.10.4	DNS	103	Standard query response 0x7118 AAAA play.google.com AAAA 2607:f8...
10	33.004788	172.20.10.1	172.20.10.4	DNS	91	Standard query response 0x54ce A play.google.com A 172.217.6.46

Checksum: 0xf573 [unverified]
[Checksum Status: Unverified]
[Stream index: 0]

▼ Domain Name System (response)
Transaction ID: 0x542c
▼ Flags: 0x8100 Standard query response, No error

1... .. = Response: Message is a response
.000 0... .. = Opcode: Standard query (0)
.... 0... .. = Authoritative: Server is not an authority for domain
.... 0... .. = Truncated: Message is not truncated
.... 1... .. = Recursion desired: Do query recursively
.... 0... .. = Recursion available: Server can't do recursive queries
.... 0... .. = Z: reserved (0)
.... 0... .. = Answer authenticated: Answer/authority portion was not authenticated by the server

00200a 04 00 35 e0 b1 02 6f f5 73 54 2c 81 00 00 01 . . . 5 . . o . s T , . . .
003000 00 00 0a 00 14 03 77 77 77 03 75 77 61 03 65 w w w . u w a . e
004064 75 02 61 75 00 00 01 00 01 c0 18 00 02 00 01 d u . a u
005000 02 a3 00 00 04 01 64 c0 18 c0 18 00 02 00 01 d
006000 02 a3 00 00 04 01 76 c0 18 c0 18 00 02 00 01 v
007000 02 a3 00 00 04 01 75 c0 18 c0 18 00 02 00 01 u
008000 02 a3 00 00 04 01 71 c0 18 c0 18 00 02 00 01 q
009000 02 a3 00 00 04 01 74 c0 18 c0 18 00 02 00 01 t
00a000 02 a3 00 00 04 01 73 c0 18 c0 18 00 02 00 01 s
00b000 02 a3 00 00 04 01 72 c0 18 c0 18 00 02 00 01 r
00c000 02 a3 00 00 04 01 62 c0 18 c0 18 00 02 00 01 b

3. How many bytes long is the entire DNS header? Use information in the bottom status line when you select parts of the packet and the bottom panel to help you work this out.

12 bytes long

4. For the initial response, in what section are the names of the nameservers carried? What is the Type of the records that carry nameserver names?

Authority Selection

Type is : NS(nameserver)

```

▼ Authoritative nameservers
  ▶ au: type NS, class IN, ns d.au
  ▶ au: type NS, class IN, ns v.au
  ▶ au: type NS, class IN, ns u.au
  ▶ au: type NS, class IN, ns q.au
  ▶ au: type NS, class IN, ns t.au
  ▶ au: type NS, class IN, ns s.au
  ▶ au: type NS, class IN, ns r.au
  ▶ au: type NS, class IN, ns b.au
  ▶ au: type NS, class IN, ns a.au
  ▶ au: type NS, class IN, ns c.au

```

5. Similarly, in what section are the IP addresses of the nameservers carried, and what is the Type of the records that carry the IP addresses?

Additional Section

```

▼ Additional records
  ▶ d.au: type A, class IN, addr 162.159.25.38
  ▶ d.au: type AAAA, class IN, addr 2400:cb00:2049:1::a29f:1926
  ▶ v.au: type A, class IN, addr 202.12.31.53
  ▶ v.au: type AAAA, class IN, addr 2001:dd8:12::53
  ▶ u.au: type A, class IN, addr 211.29.133.32
  ▶ q.au: type A, class IN, addr 65.22.196.1
  ▶ q.au: type AAAA, class IN, addr 2a01:8840:be::1
  ▶ t.au: type A, class IN, addr 65.22.199.1
  ▶ t.au: type AAAA, class IN, addr 2a01:8840:c1::1
  ▶ s.au: type A, class IN, addr 65.22.198.1
  ▶ s.au: type AAAA, class IN, addr 2a01:8840:c0::1

```

The types are A for IPv4, AAAA for IPv6

6. For the final response, in what section is the IP address of the domain name carried?

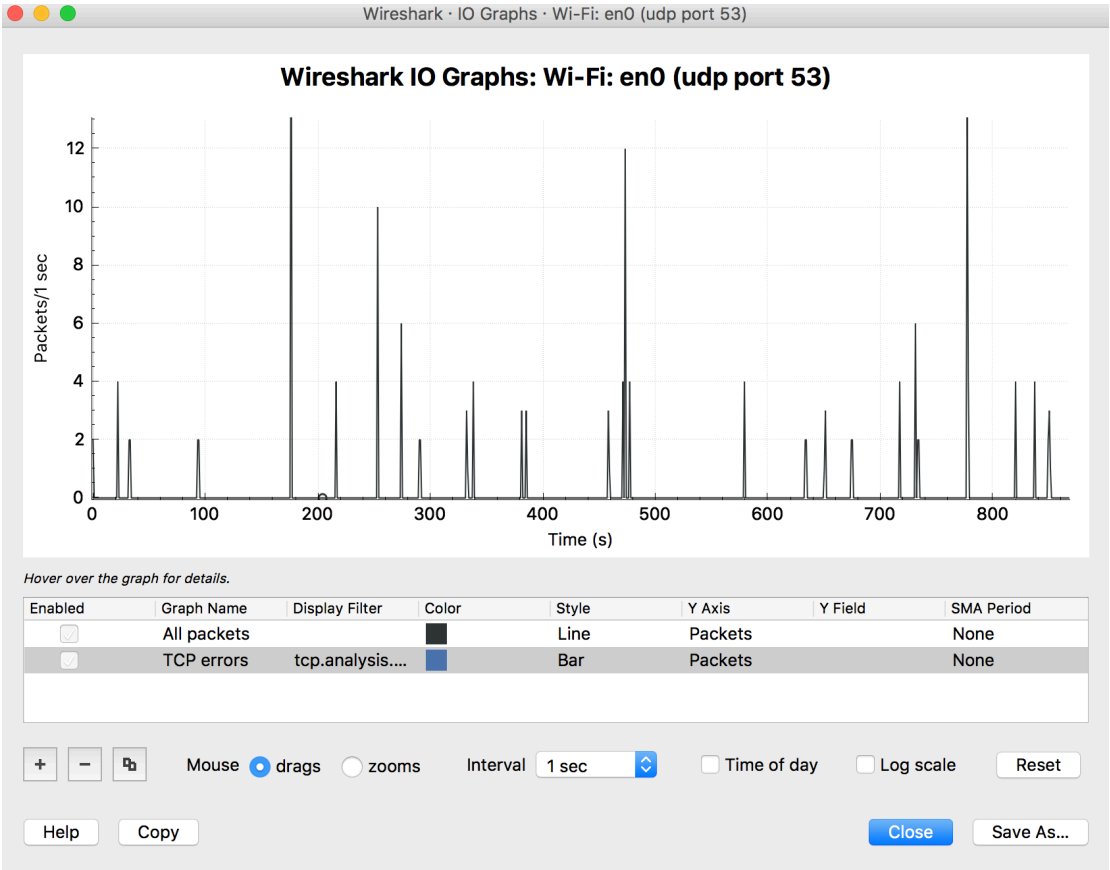
In Answer Section(A or AAAA record)

```

▼ d.au: type A, class IN, addr 162.159.25.38
  Name: d.au
  Type: A (Host Address) (1)
  Class: IN (0x0001)
  Time to live: 172800
  Data length: 4
  Address: 162.159.25.38
▼ d.au: type AAAA, class IN, addr 2400:cb00:2049:1::a29f:1926
  Name: d.au
  Type: AAAA (IPv6 Address) (28)
  Class: IN (0x0001)
  Time to live: 172800
  Data length: 16
  AAAA Address: 2400:cb00:2049:1::a29f:1926
▼ v.au: type A, class IN, addr 202.12.31.53

```

Step 5:



Wireshark · DNS · Wi-Fi: en0 (udp port 53)

Topic / Item	Count	Average	Min val	Max val	Rate (ms)	Percent	Burst rate
▼ Total Packets	250				0.0002	100%	0.1400
▼ rcode	250				0.0002	100.00%	0.1400
No error	250				0.0002	100.00%	0.1400
▼ opcodes	250				0.0002	100.00%	0.1400
Standard query	250				0.0002	100.00%	0.1400
▼ Query/Response	250				0.0002	100.00%	0.1400
Response	125				0.0001	50.00%	0.0700
Query	125				0.0001	50.00%	0.0700
▼ Query Type	250				0.0002	100.00%	0.1400
PTR (domain name PoinTeR)	6				0.0000	2.40%	0.0300
AAAA (IPv6 Address)	116				0.0001	46.40%	0.0800
A (Host Address)	128				0.0001	51.20%	0.0800
▼ Class	250				0.0002	100.00%	0.1400
IN	250				0.0002	100.00%	0.1400
▼ Service Stats	0				0.0000	100%	-
request-response time (nsec)	115	129519792.00	3483000	984417000	0.0001		0.0600
no. of unsolicited responses	0				0.0000		-

Display filter: Apply

Copy Save as... Close