

Step1:

```
~$ dig @198.41.0.4 www.uwa.edu.au

; <<> 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: 51242
;; flags: qr rd; QUERY: 1, ANSWER: 0, AUTHORITY: 9, ADDITIONAL: 18
;; 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      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
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: 10 msec
;; SERVER: 198.41.0.4#53(198.41.0.4)
;; WHEN: Thu Oct 10 20:56:39 PDT 2019
;; MSG SIZE rcvd: 555

~$ █
```

Root Name Server

A

TLD

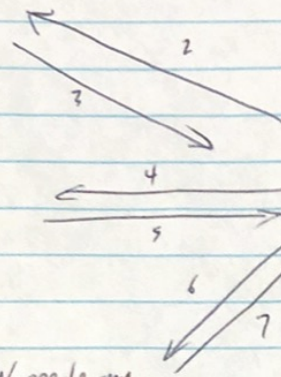
.com

Authority Name Server

www.google.com

local name server

request machine



Step4:

Wi-Fi: en0 (udp port 53)

Apply a display filter ... <#>/>

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.0.10	192.168.0.4	DNS	85	Standard query 0xdb4c A www.uwa.edu.au OPT
2	0.011362	192.168.0.4	192.168.0.10	DNS	597	Standard query response 0xdb4c A www.uwa.edu.au NS a.au NS c.au NS d.au NS
3	19.080946	192.168.0.10	75.75.75.75	DNS	74	Standard query 0x202f A www.google.com
4	19.093305	75.75.75.75	192.168.0.10	DNS	90	Standard query response 0x202f A www.google.com A 172.217.3.196
5	19.793161	192.168.0.10	75.75.75.75	DNS	80	Standard query 0x4468 A api.momentumdash.com
6	19.805436	75.75.75.75	192.168.0.10	DNS	129	Standard query response 0x4468 A api.momentumdash.com CNAME ingress-westu
7	20.717736	192.168.0.10	75.75.75.75	DNS	70	Standard query 0x46a8 A google.com

Frame 2: 597 bytes on wire (4776 bits), 597 bytes captured (4776 bits)

- Ethernet II, Src: Motorola_ff:d7:40 (88:b4:a6:ff:d7:40), Dst: Apple_9a:80:a3 (f4:5c:89:9a:80:a3)
- Internet Protocol Version 4, Src: 192.168.0.4, Dst: 192.168.0.10
- User Datagram Protocol, Src Port: domain (53), Dst Port: 56452 (56452)
- Domain Name System (response)
 - Transaction ID: 0xdb4c
 - Flags: 0x8100 Standard query response, No error
 - Questions: 1
 - Answer RRs: 0
 - Authority RRs: 9
 - Additional RRs: 18
 - Queries
 - Authoritative nameservers
 - Additional records
 - [Request In: 1]
 - [Time: 0.011362000 seconds]

0020 00 0a 00 35 dc 84 02 33 64 69 db 4c 81 00 00 01 ...5...3 di...L...

0030 00 00 00 00 00 12 03 77 77 77 03 75 77 61 03 65w ww-uwa-e

0040 64 75 02 61 75 00 00 01 00 01 c0 18 00 02 00 01 du-au-...

0050 00 02 a3 00 00 04 01 61 c0 18 c0 18 00 02 00 01a

0060 00 02 a3 00 00 04 01 63 c0 18 c0 18 00 02 00 01c

0070 00 02 a3 00 00 04 01 64 c0 18 c0 18 00 02 00 01d

0080 00 02 a3 00 00 04 01 71 c0 18 c0 18 00 02 00 01q

0090 00 02 a3 00 00 04 01 72 c0 18 c0 18 00 02 00 01r

Identification of transaction (dns.id), 2 bytes

Packets: 20 - Displayed: 20 (100.0%) - Dropped: 0 (0.0%) Profile: Default

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.

Transaction ID is 0xdb4c, so its length is 16 bits.

2^{16} concurrent transactions may cause collisions.

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

The first bit .

Domain Name System (response)

- Transaction ID: 0xdb4c
- Flags: 0x8100 Standard query response, No error
 - 1... .. = Response: Message is a response
 - .000 0... .. = Opcode: Standard query (0)

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.

DNS header is 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?

▼ Authoritative nameservers

```
▶ au: type NS, class IN, ns a.au
▶ au: type NS, class IN, ns c.au
▶ au: type NS, class IN, ns d.au
▶ au: type NS, class IN, ns q.au
▶ au: type NS, class IN, ns r.au
▶ au: type NS, class IN, ns s.au
▶ au: type NS, class IN, ns t.au
▶ au: type NS, class IN, ns u.au
▶ au: type NS, class IN, ns v.au
```

Names of the nameservers carried in Authoritative nameservers section.

Type is NS.

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 records

```
▶ a.au: type A, class IN, addr 58.65.254.73
▶ c.au: type A, class IN, addr 162.159.24.179
▶ d.au: type A, class IN, addr 162.159.25.38
▶ q.au: type A, class IN, addr 65.22.196.1
▶ r.au: type A, class IN, addr 65.22.197.1
▶ s.au: type A, class IN, addr 65.22.198.1
▶ t.au: type A, class IN, addr 65.22.199.1
▶ u.au: type A, class IN, addr 211.29.133.32
▶ v.au: type A, class IN, addr 202.12.31.53
▶ a.au: type AAAA, class IN, addr 2407:6e00:254:306::73
```

In the Additional records section.

IPv4 type is A, IPv6 type is AAAA.

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

The image shows a Wireshark packet capture of a DNS response. The top pane displays a list of packets, with packet 20 selected. The middle pane shows the details of packet 20, which is a DNS response from 192.168.0.10 to 75.75.75.75. The bottom pane shows the raw packet data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
14	22.201346	75.75.75.75	192.168.0.10	DNS	187	Standard query response 0xd5d8 A bl.ecbsn.com CNAME ev.ecbsn.com CNAME ev
15	22.267639	192.168.0.10	75.75.75.75	DNS	82	Standard query 0xfd60 A e4201.b.akamaiedge.net
16	22.374446	75.75.75.75	192.168.0.10	DNS	98	Standard query response 0xfd60 A e4201.b.akamaiedge.net A 104.115.149.141
17	22.374853	192.168.0.10	75.75.75.75	DNS	75	Standard query 0x0be0 A www.gstatic.com
18	22.396124	75.75.75.75	192.168.0.10	DNS	91	Standard query response 0x0be0 A www.gstatic.com A 172.217.14.195
19	22.807532	192.168.0.10	75.75.75.75	DNS	79	Standard query 0x1aca A clients5.google.com
20	23.021083	75.75.75.75	192.168.0.10	DNS	119	Standard query response 0x1aca A clients5.google.com CNAME clients.l.google.com

Frame 20: 119 bytes on wire (952 bits), 119 bytes captured (952 bits)
Ethernet II, Src: Motorola_ff:d7:40 (88:b4:a6:ff:d7:40), Dst: Apple_9a:80:a3 (f4:5c:89:9a:80:a3)
Internet Protocol Version 4, Src: 75.75.75.75, Dst: 192.168.0.10
User Datagram Protocol, Src Port: domain (53), Dst Port: 63375 (63375)
▼ Domain Name System (response)
Transaction ID: 0x1aca
Flags: 0x8180 Standard query response, No error
Questions: 1
Answer RRs: 2
Authority RRs: 0
Additional RRs: 0
Queries
▼ Answers
▶ clients5.google.com: type CNAME, class IN, cname clients.l.google.com
▶ clients.l.google.com: type A, class IN, addr 172.217.14.206
[\[Request In: 19\]](#)
[Time: 0.213551000 seconds]

```
0000  f4 5c 89 9a 80 a3 88 b4 a6 ff d7 40 08 00 45 40  .\.....@..E@
0010  00 69 00 00 40 00 3a 11 e8 fb 4b 4b 4b 4b c0 a8  .i.@:..-KKKK..
0020  00 0a 00 35 f7 8f 00 55 de db 1a ca 81 80 00 01  ..S..U.....
0030  00 02 00 00 00 00 08 63 6c 69 65 6e 74 73 35 06  .....clients5
0040  67 6f 6f 67 6c 65 03 63 6f 6d 00 00 01 00 01 c0  google.c om.....
0050  0c 00 05 00 01 00 00 00 83 00 0c 07 63 6c 69 65  .....clie
0060  6e 74 73 01 6c c0 15 c0 31 00 01 00 01 00 00 00  nts.l..1.....
0070  48 00 04 ac d9 0e ce H.....
```

In the Answers section.