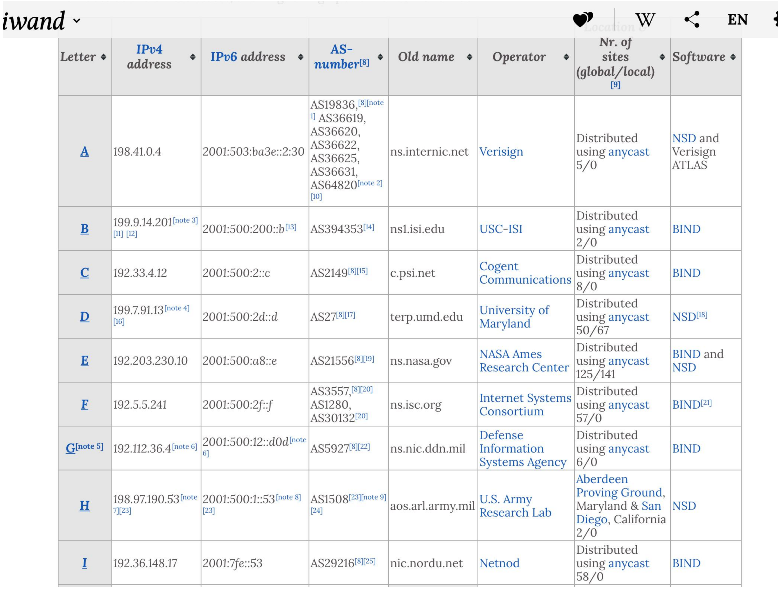
Lab2 – Yuanjie Yue 10/08/2019

Step 1. Manual Name Resolution

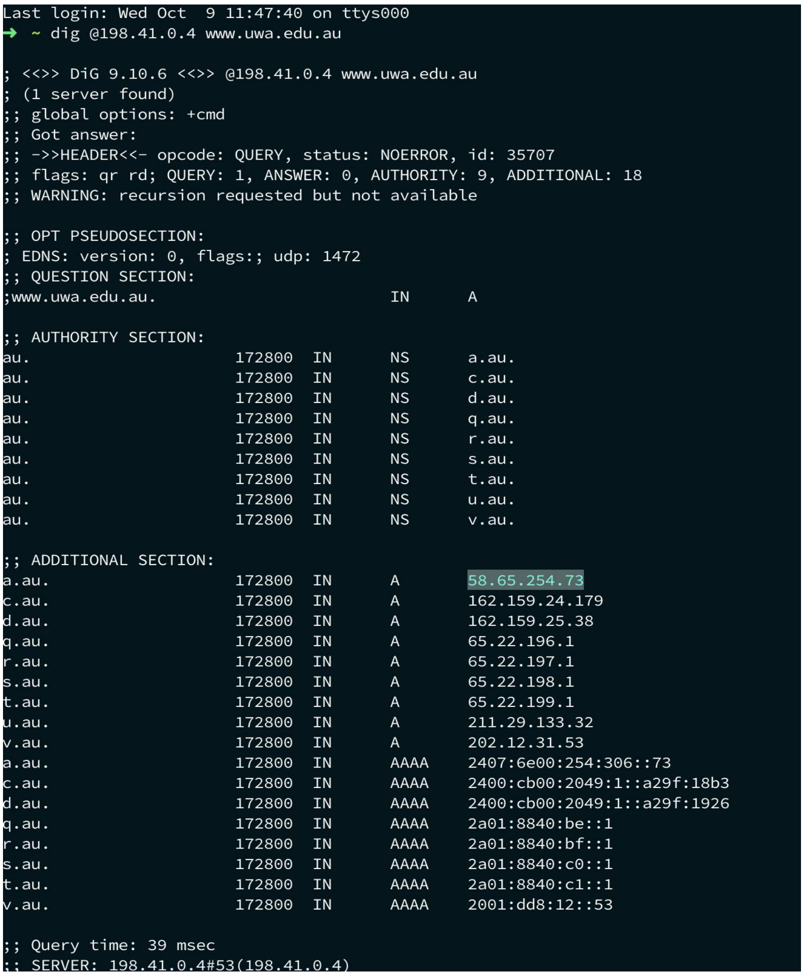
1. Send requests to the name servers following its hierarchy recursively.

1) Firstly, search the web for the name servers' IP addresses. Then use dig to ask for one of the root server, namely the a-server with IP address 198.41.0.4, for www.uwa.edu.au.



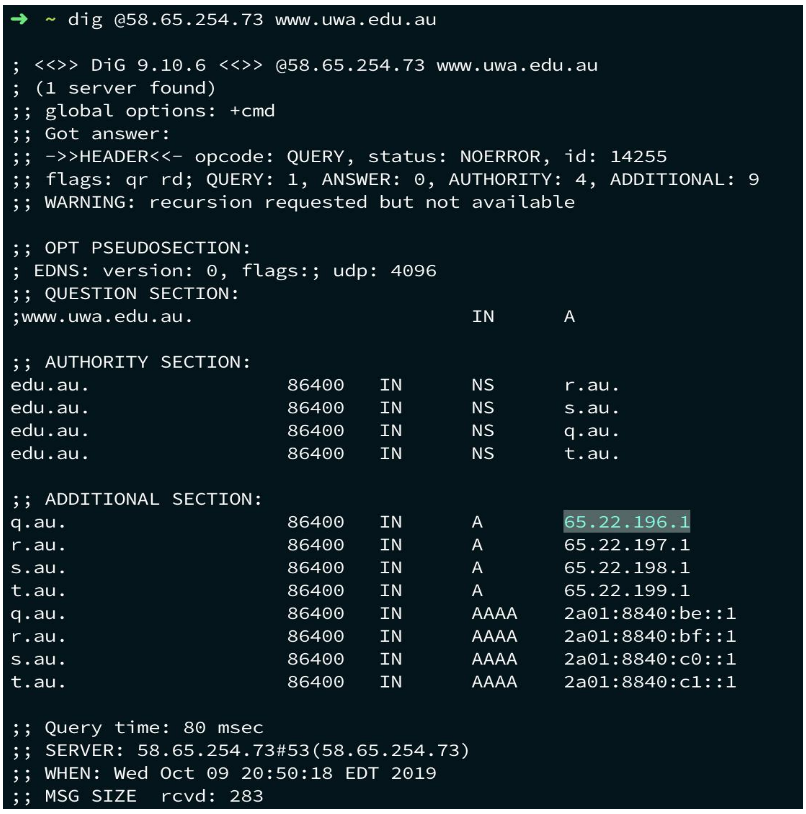
Letter	IPv4 address	IPv6 address	AS-number[8]	Old name	Operator	Location & Nr. of sites (global/local)[9]	Software
A	198.41.0.4	2001:503:ba3e::2:30	AS19836,[8][note 1] AS36619, AS36620, AS36622, AS36625, AS36631, AS64820[note 2][10]	ns.internic.net	Verisign	Distributed using anycast 5/0	NSD and Verisign ATLAS
B	199.9.14.201[note 3][11] [12]	2001:500:200::b[13]	AS394353[14]	ns1.isi.edu	USC-ISI	Distributed using anycast 2/0	BIND
C	192.33.4.12	2001:500:2::c	AS2149[8][15]	c.psi.net	Cogent Communications	Distributed using anycast 8/0	BIND
D	199.7.91.13[note 4][16]	2001:500:2d::d	AS27[8][17]	terp.umd.edu	University of Maryland	Distributed using anycast 50/67	NSD[18]
E	192.203.230.10	2001:500:a8::e	AS21556[8][19]	ns.nasa.gov	NASA Ames Research Center	Distributed using anycast 125/141	BIND and NSD
F	192.5.5.241	2001:500:2f::f	AS3557,[8][20] AS1280, AS30132[20]	ns.isc.org	Internet Systems Consortium	Distributed using anycast 57/0	BIND[21]
G[note 5]	192.112.36.4[note 6]	2001:500:12::d0d[note 6]	AS5927[8][22]	ns.nic.ddn.mil	Defense Information Systems Agency	Distributed using anycast 6/0	BIND
H	198.97.190.53[note 7][23]	2001:500:1::53[note 8][23]	AS1508[23][note 9][24]	aos.arl.army.mil	U.S. Army Research Lab	Aberdeen Proving Ground, Maryland & San Diego, California 2/0	NSD
I	192.36.148.17	2001:7fe::53	AS29216[8][25]	nic.nordu.net	Netnod	Distributed using anycast 58/0	BIND

2) Secondly, we execute the dig command 'dig @198.41.0.4 www.uwa.edu.au', which give us back a list of name servers of the top-level domain 'au', it means that the root server only knows the 'au' name servers' IP. Then will pick up the first one 58.65.254.73 for the next step.



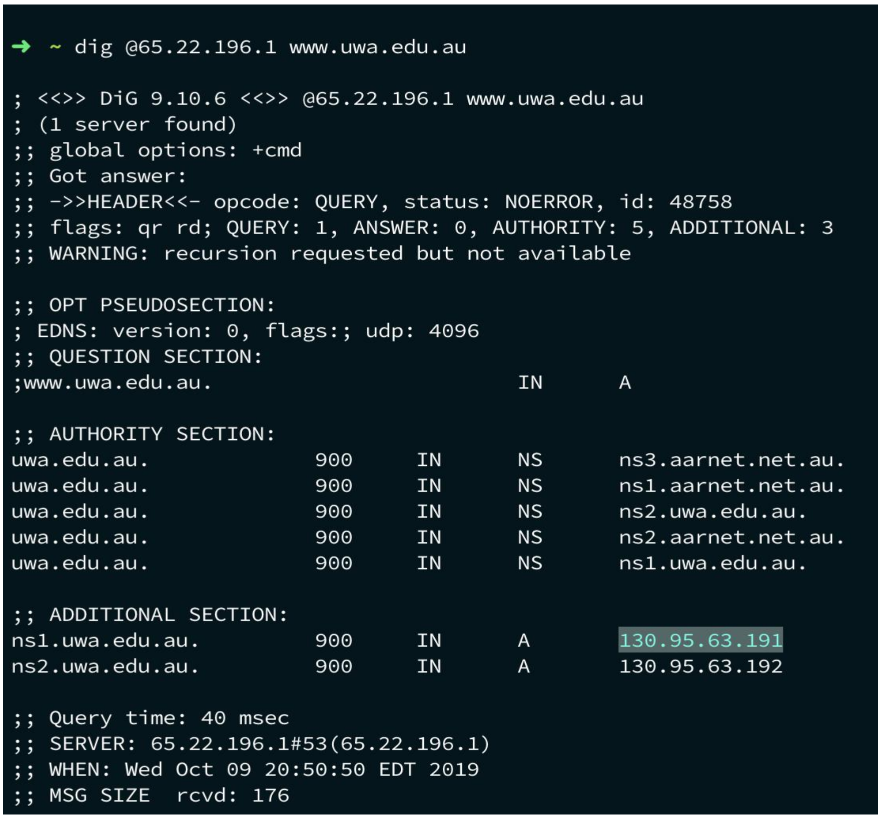
```
Last login: Wed Oct  9 11:47:40 on ttys000
➜ ~ dig @198.41.0.4 www.uwa.edu.au

; <<>> 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: 35707
;; flags: qr rd; QUERY: 1, ANSWER: 0, AUTHORITY: 9, ADDITIONAL: 18
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1472
;; QUESTION SECTION:
;www.uwa.edu.au.                        IN      A

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

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

;; Query time: 39 msec
;; SERVER: 198.41.0.4#53(198.41.0.4)
```

3) Thirdly, we will send same request using the command ‘dig @58.65.254.73 www.uwa.edu.au’. Similarly, it gives back a list of name servers on the top level domain ‘edu.au’, we will pick up the first one 65.22.196.1 for next step.



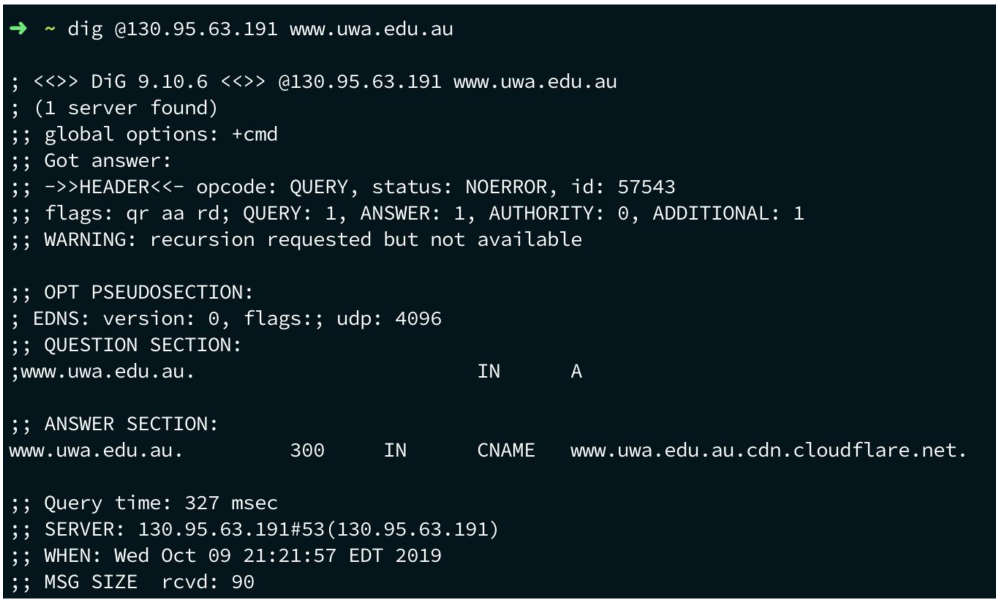
```
➜ ~ dig @58.65.254.73 www.uwa.edu.au

; <<>> DiG 9.10.6 <<>> @58.65.254.73 www.uwa.edu.au
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 14255
;; flags: qr rd; QUERY: 1, ANSWER: 0, AUTHORITY: 4, ADDITIONAL: 9
;; WARNING: recursion requested but not available

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

;; AUTHORITY SECTION:
edu.au.                 86400   IN      NS      r.au.
edu.au.                 86400   IN      NS      s.au.
edu.au.                 86400   IN      NS      q.au.
edu.au.                 86400   IN      NS      t.au.

;; ADDITIONAL SECTION:
q.au.                   86400   IN      A       65.22.196.1
r.au.                   86400   IN      A       65.22.197.1
s.au.                   86400   IN      A       65.22.198.1
t.au.                   86400   IN      A       65.22.199.1
q.au.                   86400   IN      AAAA    2a01:8840:be::1
r.au.                   86400   IN      AAAA    2a01:8840:bf::1
s.au.                   86400   IN      AAAA    2a01:8840:c0::1
t.au.                   86400   IN      AAAA    2a01:8840:c1::1

;; Query time: 80 msec
;; SERVER: 58.65.254.73#53(58.65.254.73)
;; WHEN: Wed Oct 09 20:50:18 EDT 2019
;; MSG SIZE  rcvd: 283
```

4) Fourthly, we will send same request using the command ‘dig @65.22.196.1 www.uwa.edu.au’. Similarly, it gives back a list of name servers on domain ‘uwa.edu.au’, we will pick up the first one 130.95.63.191 for next step.



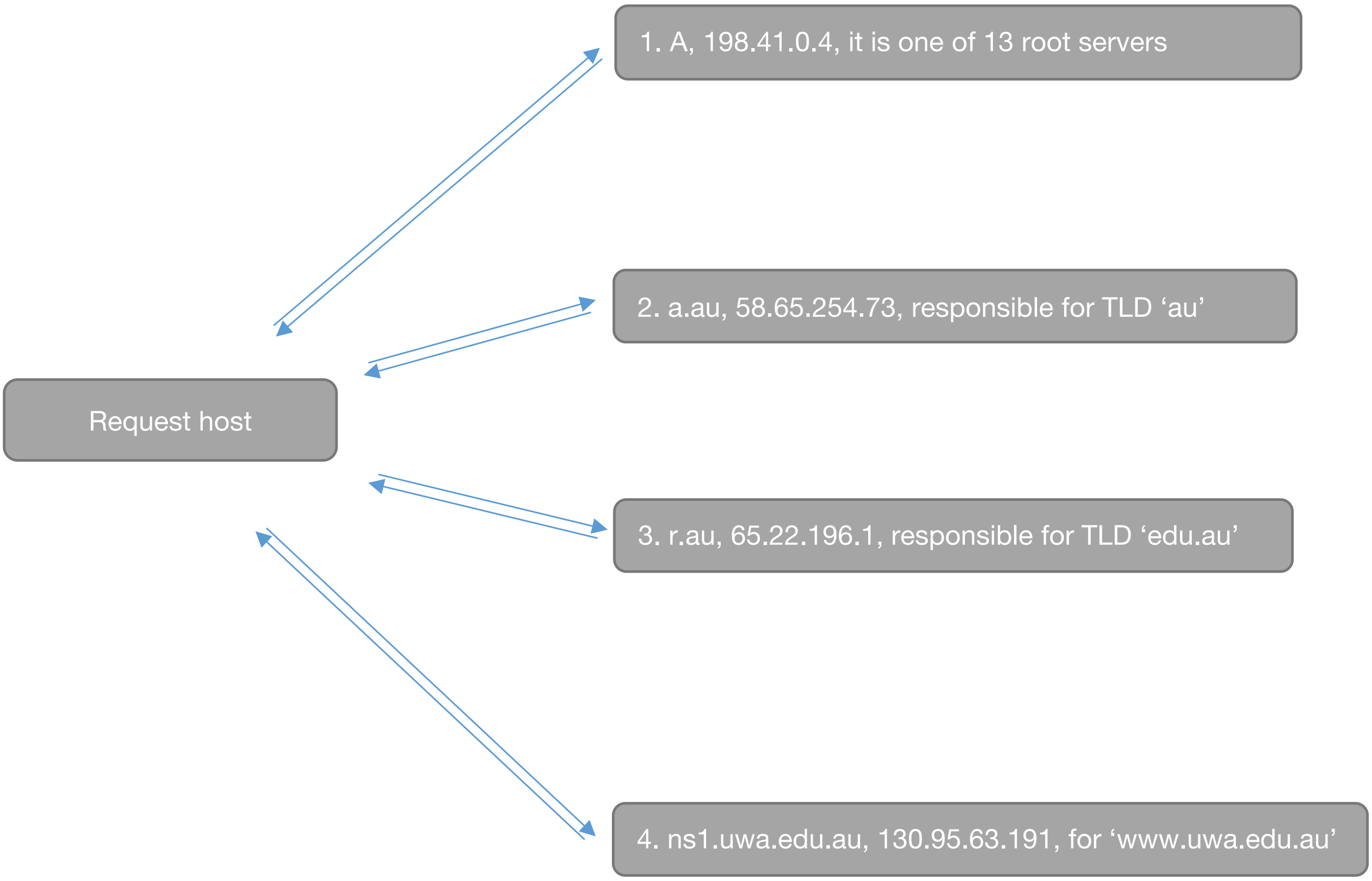
```
➜ ~ dig @65.22.196.1 www.uwa.edu.au

; <<>> DiG 9.10.6 <<>> @65.22.196.1 www.uwa.edu.au
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 48758
;; flags: qr rd; QUERY: 1, ANSWER: 0, AUTHORITY: 5, ADDITIONAL: 3
;; WARNING: recursion requested but not available

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

;; AUTHORITY SECTION:
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.uwa.edu.au.
uwa.edu.au.             900     IN      NS      ns2.aarnet.net.au.
uwa.edu.au.             900     IN      NS      ns1.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: 40 msec
;; SERVER: 65.22.196.1#53(65.22.196.1)
;; WHEN: Wed Oct 09 20:50:50 EDT 2019
;; MSG SIZE  rcvd: 176
```

5) Fifthly, we will send same request using the command 'dig @130.95.63.191 www.uwa.edu.au'. It gives back the www.uwa.edu.au and its alias. Now we know that the IP '130.95.63.191' is the one we need.



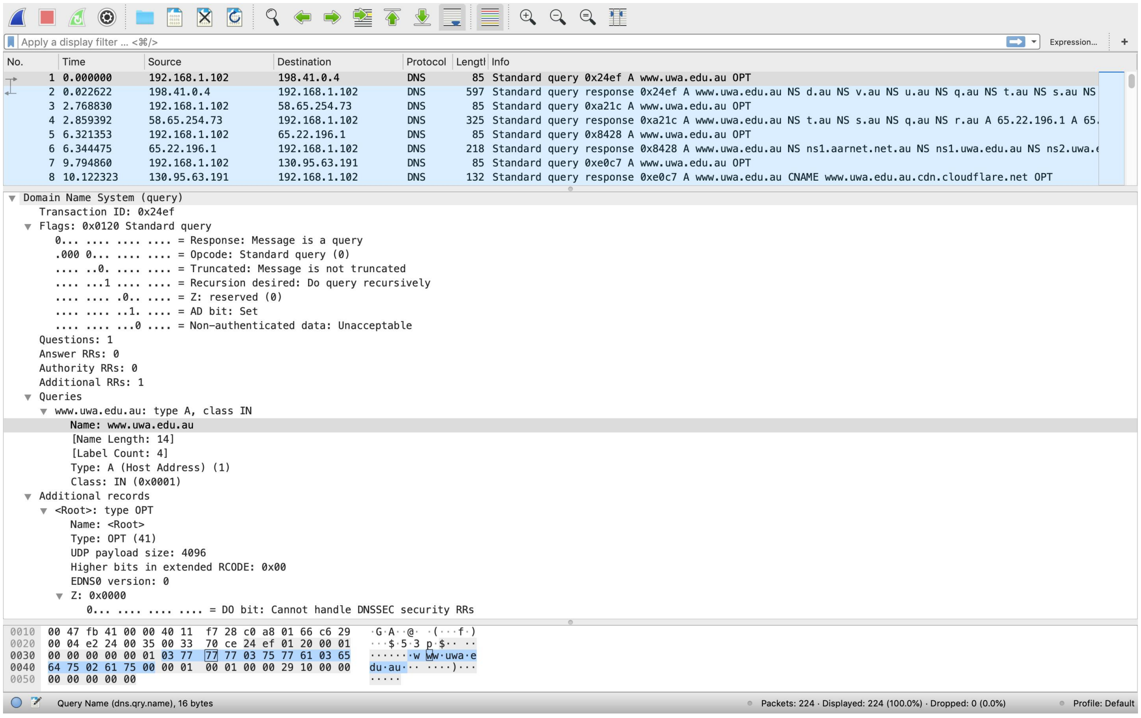
```
➜ ~ dig @130.95.63.191 www.uwa.edu.au

; <<>> 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: 57543
;; 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: 327 msec
;; SERVER: 130.95.63.191#53(130.95.63.191)
;; WHEN: Wed Oct 09 21:21:57 EDT 2019
;; MSG SIZE  rcvd: 90
```

6) Draw figure that shows the sequence of remote nameservers that you contacted and the domain for which they are responsible.


1. A, 198.41.0.4, it is one of 13 root servers
2. a.au, 58.65.254.73, responsible for TLD 'au'
Request host
3. r.au, 65.22.196.1, responsible for TLD 'edu.au'
4. ns1.uwa.edu.au, 130.95.63.191, for 'www.uwa.edu.au'

Step 2 & 3. Capture a Trace and Inspect the Trace

1. Set up the filter to be udp port 53, then repeat typing in the dig commands in Step1, which will help us get the trace.



Apply a display filter ... <⌘/>

```
No.  Time       Source          Destination     Protocol Lengtl Info
   1 0.000000   192.168.1.102   198.41.0.4      DNS        85 Standard query 0x24ef A www.uwa.edu.au OPT
   2 0.022622   198.41.0.4      192.168.1.102   DNS       597 Standard query response 0x24ef A www.uwa.edu.au NS d.au NS v.au NS u.au NS q.au NS t.au NS s.au NS
   3 2.768830   192.168.1.102   58.65.254.73    DNS        85 Standard query 0xa21c A www.uwa.edu.au OPT
   4 2.859392   58.65.254.73    192.168.1.102   DNS       325 Standard query response 0xa21c A www.uwa.edu.au NS t.au NS s.au NS q.au NS r.au A 65.22.196.1 A 65.
   5 6.321353   192.168.1.102   65.22.196.1     DNS        85 Standard query 0x8428 A www.uwa.edu.au OPT
   6 6.344475   65.22.196.1     192.168.1.102   DNS       218 Standard query response 0x8428 A www.uwa.edu.au NS ns1.aarnet.net.au NS ns1.uwa.edu.au NS ns2.uwa.e
   7 9.794860   192.168.1.102   130.95.63.191   DNS        85 Standard query 0xe0c7 A www.uwa.edu.au OPT
   8 10.122323  130.95.63.191   192.168.1.102   DNS       132 Standard query response 0xe0c7 A www.uwa.edu.au CNAME www.uwa.edu.au.cdn.cloudflare.net OPT
```

```
▼ Domain Name System (query)
    Transaction ID: 0x24ef
  ▼ 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
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 1
  ▼ Queries
    ▼ www.uwa.edu.au: type A, class IN
        Name: www.uwa.edu.au
        [Name Length: 14]
        [Label Count: 4]
        Type: A (Host Address) (1)
        Class: IN (0x0001)
  ▼ Additional records
    ▼ <Root>: type OPT
        Name: <Root>
        Type: OPT (41)
        UDP payload size: 4096
        Higher bits in extended RCODE: 0x00
        EDNS0 version: 0
      ▼ Z: 0x0000
          0... .... .... .... = DO bit: Cannot handle DNSSEC security RRs
```

```
0010  00 47 fb 41 00 00 40 11  f7 28 c0 a8 01 66 c6 29   ·G·A··@· ·(···f·)
0020  00 04 e2 24 00 35 00 33  70 ce 24 ef 01 20 00 01   ···$·5·3 p·$·· ··
0030  00 00 00 00 00 01 03 77  77 77 03 75 77 61 03 65   ·······w ww·uwa·e
0040  64 75 02 61 75 00 00 01  00 01 00 00 29 10 00 00   du·au··· ····)···
0050  00 00 00 00 00                                     ·····
```

Query Name (dns.qry.name), 16 bytes · Packets: 224 · Displayed: 224 (100.0%) · Dropped: 0 (0.0%) · Profile: Default

Step 4. Details of DNS message

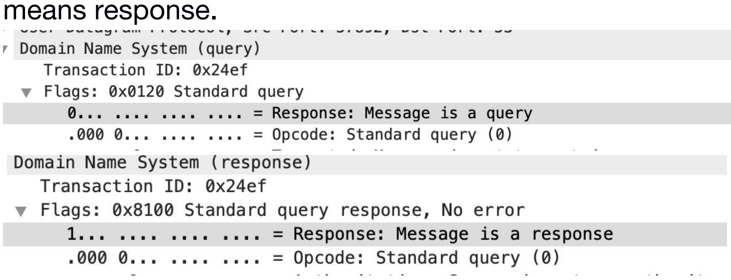
Look at the DNS header, and answer the following questions:

1. How many bits long is the Transaction ID?

As shown in the trace of the first request DNS message, we could see that the transaction ID is 0x24ef, it is four digit of hex number, which means it is of 16 bits long.

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

As is shown in the pics, the 1st flag bit marks if a DNS message is a query or response, '0' means query and '1' means response.



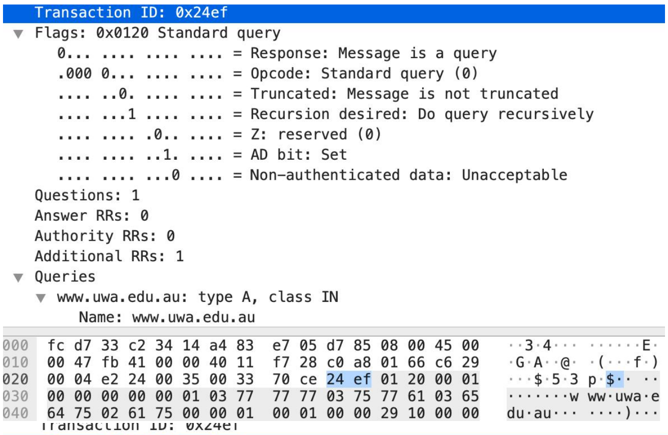
```
Domain Name System (query)
  Transaction ID: 0x24ef
▼ Flags: 0x0120 Standard query
    0... .... .... .... = Response: Message is a query
    .000 0... .... .... = Opcode: Standard query (0)
```

```
Domain Name System (response)
  Transaction ID: 0x24ef
▼ Flags: 0x8100 Standard query response, No error
    1... .... .... .... = Response: Message is a response
    .000 0... .... .... = Opcode: Standard query (0)
```

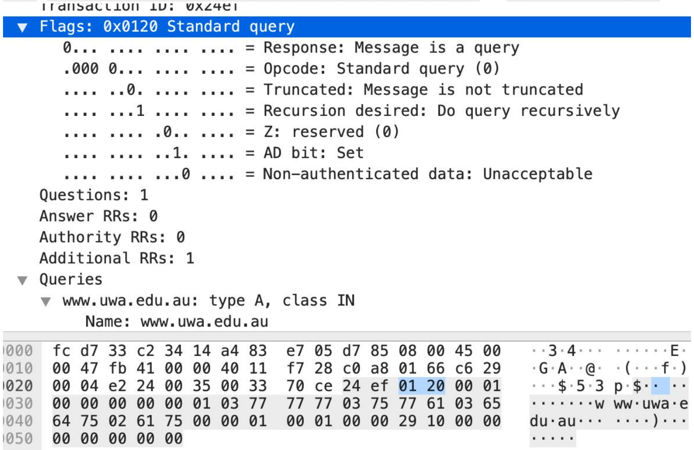
3. How many bytes long is the entire DNS header?

DNS header is 12 bytes:

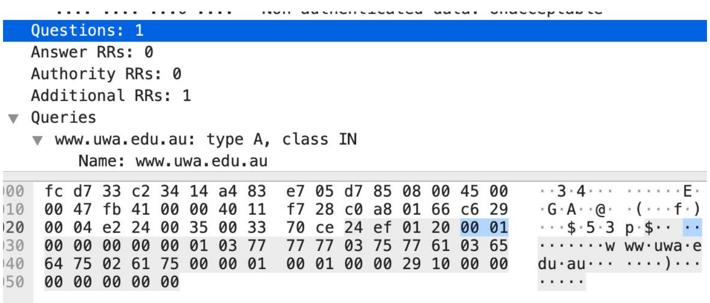
2 bytes	+	2 bytes	+	2 bytes	+	2 bytes	+	2 bytes	+	2 bytes
[Transaction ID]		[Flags]		[Questions]		[Answer RRs]		[Authority RRs]		[Additional RRs]



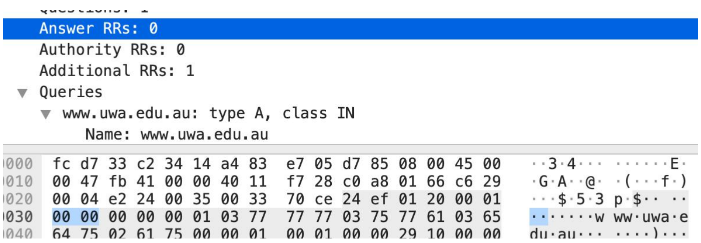
```
    Transaction ID: 0x24ef
▼ Flags: 0x0120 Standard query
      0... .... .... .... = Response: Message is a query
      .000 0... .... .... = Opcode: Standard query (0)
      .... ..0. .... .... = Truncated: Message is not truncated
      .... ...1 .... .... = Recursion desired: Do query recursively
      .... .... .0.. .... = Z: reserved (0)
      .... .... ..1. .... = AD bit: Set
      .... .... ...0 .... = Non-authenticated data: Unacceptable
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 1
▼ Queries
    ▼ www.uwa.edu.au: type A, class IN
          Name: www.uwa.edu.au

000  fc d7 33 c2 34 14 a4 83  e7 05 d7 85 08 00 45 00   ··3·4··· ······E·
010  00 47 fb 41 00 00 40 11  f7 28 c0 a8 01 66 c6 29   ·G·A··@· ·(···f·)
020  00 04 e2 24 00 35 00 33  70 ce 24 ef 01 20 00 01   ···$·5·3 p·$·· ··
030  00 00 00 00 00 01 03 77  77 77 03 75 77 61 03 65   ·······w ww·uwa·e
040  64 75 02 61 75 00 00 01  00 01 00 00 29 10 00 00   du·au··· ····)···
```



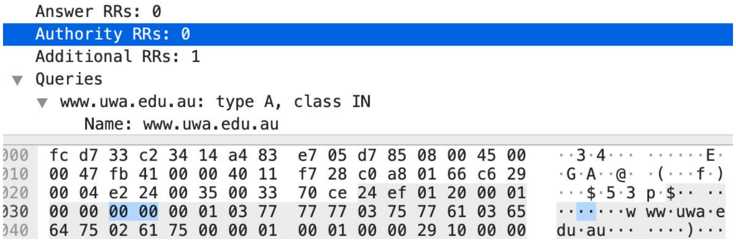
```
    Transaction ID: 0x24ef
▼ Flags: 0x0120 Standard query
      0... .... .... .... = Response: Message is a query
      .000 0... .... .... = Opcode: Standard query (0)
      .... ..0. .... .... = Truncated: Message is not truncated
      .... ...1 .... .... = Recursion desired: Do query recursively
      .... .... .0.. .... = Z: reserved (0)
      .... .... ..1. .... = AD bit: Set
      .... .... ...0 .... = Non-authenticated data: Unacceptable
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 1
▼ Queries
    ▼ www.uwa.edu.au: type A, class IN
          Name: www.uwa.edu.au

000  fc d7 33 c2 34 14 a4 83  e7 05 d7 85 08 00 45 00   ··3·4··· ······E·
010  00 47 fb 41 00 00 40 11  f7 28 c0 a8 01 66 c6 29   ·G·A··@· ·(···f·)
020  00 04 e2 24 00 35 00 33  70 ce 24 ef 01 20 00 01   ···$·5·3 p·$·· ··
030  00 00 00 00 00 01 03 77  77 77 03 75 77 61 03 65   ·······w ww·uwa·e
040  64 75 02 61 75 00 00 01  00 01 00 00 29 10 00 00   du·au··· ····)···
050  00 00 00 00 00                                     ·····
```



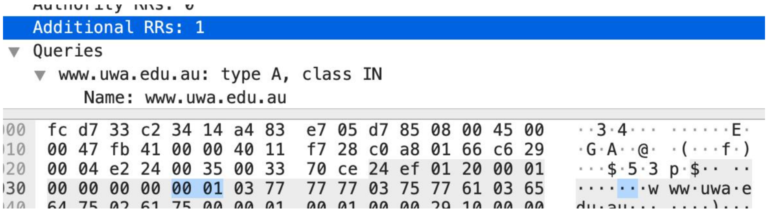
```
      .... .... ...0 .... = Non-authenticated data: Unacceptable
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 1
▼ Queries
    ▼ www.uwa.edu.au: type A, class IN
          Name: www.uwa.edu.au

000  fc d7 33 c2 34 14 a4 83  e7 05 d7 85 08 00 45 00   ··3·4··· ······E·
010  00 47 fb 41 00 00 40 11  f7 28 c0 a8 01 66 c6 29   ·G·A··@· ·(···f·)
020  00 04 e2 24 00 35 00 33  70 ce 24 ef 01 20 00 01   ···$·5·3 p·$·· ··
030  00 00 00 00 00 01 03 77  77 77 03 75 77 61 03 65   ·······w ww·uwa·e
040  64 75 02 61 75 00 00 01  00 01 00 00 29 10 00 00   du·au··· ····)···
050  00 00 00 00 00                                     ·····
```



```
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 1
▼ Queries
    ▼ www.uwa.edu.au: type A, class IN
          Name: www.uwa.edu.au

000  fc d7 33 c2 34 14 a4 83  e7 05 d7 85 08 00 45 00   ··3·4··· ······E·
010  00 47 fb 41 00 00 40 11  f7 28 c0 a8 01 66 c6 29   ·G·A··@· ·(···f·)
020  00 04 e2 24 00 35 00 33  70 ce 24 ef 01 20 00 01   ···$·5·3 p·$·· ··
030  00 00 00 00 00 01 03 77  77 77 03 75 77 61 03 65   ·······w ww·uwa·e
040  64 75 02 61 75 00 00 01  00 01 00 00 29 10 00 00   du·au··· ····)···
```



```
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 1
▼ Queries
    ▼ www.uwa.edu.au: type A, class IN
          Name: www.uwa.edu.au

000  fc d7 33 c2 34 14 a4 83  e7 05 d7 85 08 00 45 00   ··3·4··· ······E·
010  00 47 fb 41 00 00 40 11  f7 28 c0 a8 01 66 c6 29   ·G·A··@· ·(···f·)
020  00 04 e2 24 00 35 00 33  70 ce 24 ef 01 20 00 01   ···$·5·3 p·$·· ··
030  00 00 00 00 00 01 03 77  77 77 03 75 77 61 03 65   ·······w ww·uwa·e
040  64 75 02 61 75 00 00 01  00 01 00 00 29 10 00 00   du·au··· ····)···
```

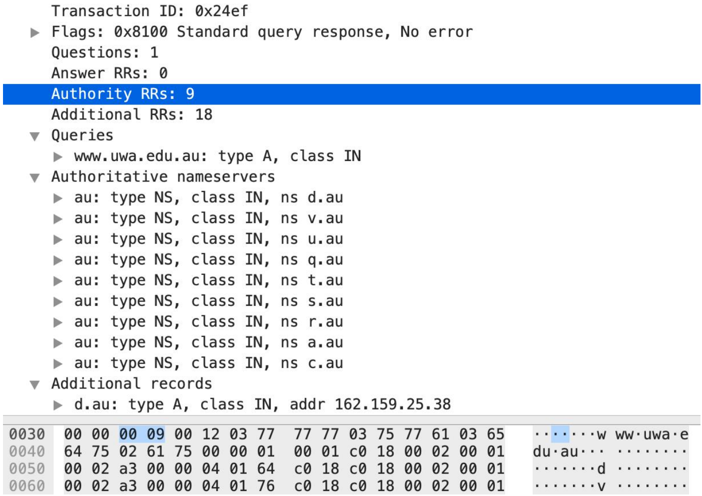


```
    Authority RRs: 0
    Additional RRs: 1
▼ Queries
    ▼ www.uwa.edu.au: type A, class IN
          Name: www.uwa.edu.au

000  fc d7 33 c2 34 14 a4 83  e7 05 d7 85 08 00 45 00   ··3·4··· ······E·
010  00 47 fb 41 00 00 40 11  f7 28 c0 a8 01 66 c6 29   ·G·A··@· ·(···f·)
020  00 04 e2 24 00 35 00 33  70 ce 24 ef 01 20 00 01   ···$·5·3 p·$·· ··
030  00 00 00 00 00 01 03 77  77 77 03 75 77 61 03 65   ·······w ww·uwa·e
040  64 75 02 61 75 00 00 01  00 01 00 00 29 10 00 00   du·au··· ····)···
```

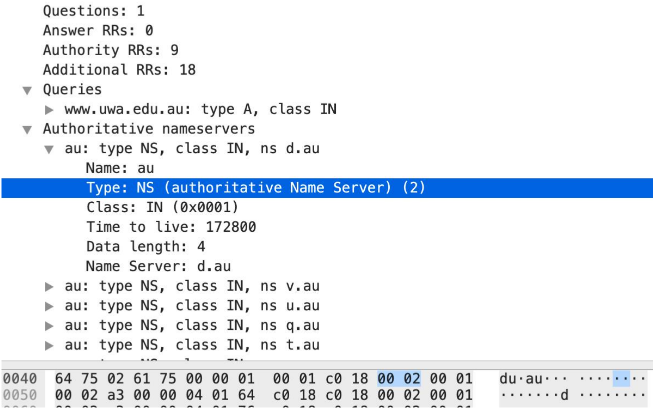
Look at the body of the DNS response messages, and answer the following questions:

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?

The Authority section carried the names of the nameservers and the NS records carry these names.



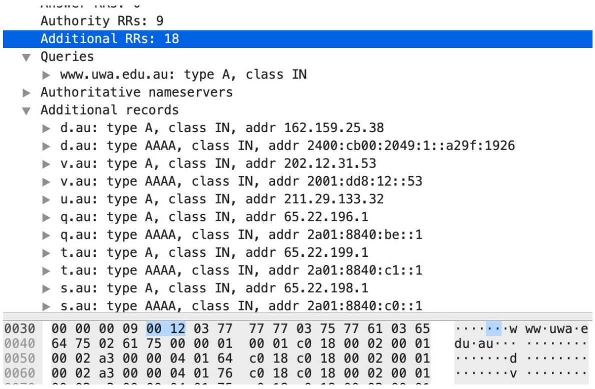
```
    Transaction ID: 0x24ef
  ▶ Flags: 0x8100 Standard query response, No error
    Questions: 1
    Answer RRs: 0
    Authority RRs: 9
    Additional RRs: 18
  ▼ Queries
      ▶ www.uwa.edu.au: type A, class IN
  ▼ Authoritative nameservers
      ▶ au: type NS, class IN, ns d.au
      ▶ au: type 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 a.au
      ▶ au: type NS, class IN, ns c.au
  ▼ Additional records
      ▶ d.au: type A, class IN, addr 162.159.25.38
0030  00 00 00 09 00 12 03 77  77 77 03 75 77 61 03 65   ·······w 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 64  c0 18 c0 18 00 02 00 01   ·······d ········
0060  00 02 a3 00 00 04 01 76  c0 18 c0 18 00 02 00 01   ·······v ········
```



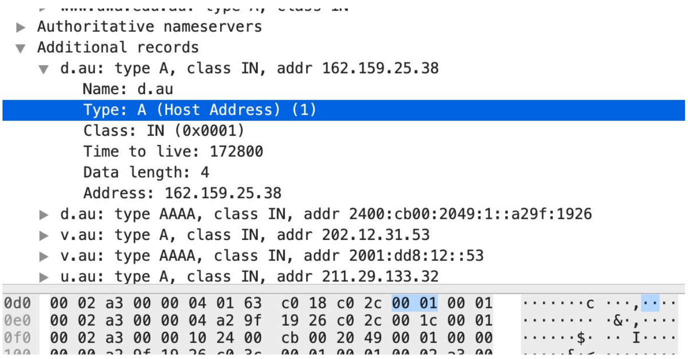
```
    Questions: 1
    Answer RRs: 0
    Authority RRs: 9
    Additional RRs: 18
  ▼ Queries
      ▶ www.uwa.edu.au: type A, class IN
  ▼ Authoritative nameservers
      ▼ au: type NS, class IN, ns d.au
            Name: au
            Type: NS (authoritative Name Server) (2)
            Class: IN (0x0001)
            Time to live: 172800
            Data length: 4
            Name Server: 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
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 64  c0 18 c0 18 00 02 00 01   ·······d ········
```

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?

The IP addresses are carried in the Additional section and the A records carry these IP addresses.



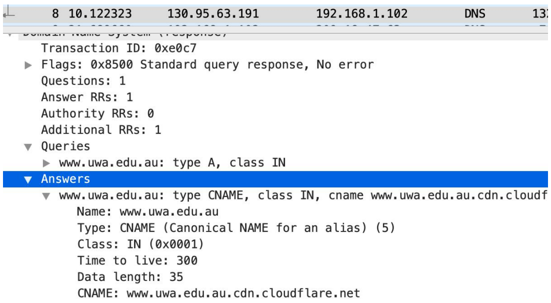
```
    Authority RRs: 9
    Additional RRs: 18
  ▼ Queries
      ▶ www.uwa.edu.au: type A, class IN
  ▶ Authoritative nameservers
  ▼ Additional records
      ▶ d.au: type A, class IN, addr 162.159.25.38
      ▶ d.au: type AAAA, class IN, addr 2400:cb00:2049:1::a29f:1926
      ▶ v.au: type A, class 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
0030  00 00 00 09 00 12 03 77  77 77 03 75 77 61 03 65   ·······w 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 64  c0 18 c0 18 00 02 00 01   ·······d ········
0060  00 02 a3 00 00 04 01 76  c0 18 c0 18 00 02 00 01   ·······v ········
```



```
▶ Authoritative nameservers
▼ Additional records
    ▼ 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
    ▶ 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
0d0  00 02 a3 00 00 04 01 63  c0 18 c0 2c 00 01 00 01   ·······c ···,····
0e0  00 02 a3 00 00 04 a2 9f  19 26 c0 2c 00 1c 00 01   ········ ·&·,····
0f0  00 02 a3 00 00 10 24 00  cb 00 20 49 00 01 00 00   ······$· ·· I····
```

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

The Answer section carries the IP address.



```
      8 10.122323     130.95.63.191       192.168.1.102       DNS      13
    Transaction ID: 0xe0c7
  ▶ Flags: 0x8500 Standard query response, No error
    Questions: 1
    Answer RRs: 1
    Authority RRs: 0
    Additional RRs: 1
  ▼ Queries
      ▶ www.uwa.edu.au: type A, class IN
  ▼ Answers
      ▼ www.uwa.edu.au: type CNAME, class IN, cname www.uwa.edu.au.cdn.cloudf
            Name: www.uwa.edu.au
            Type: CNAME (Canonical NAME for an alias) (5)
            Class: IN (0x0001)
            Time to live: 300
            Data length: 35
            CNAME: www.uwa.edu.au.cdn.cloudflare.net
```