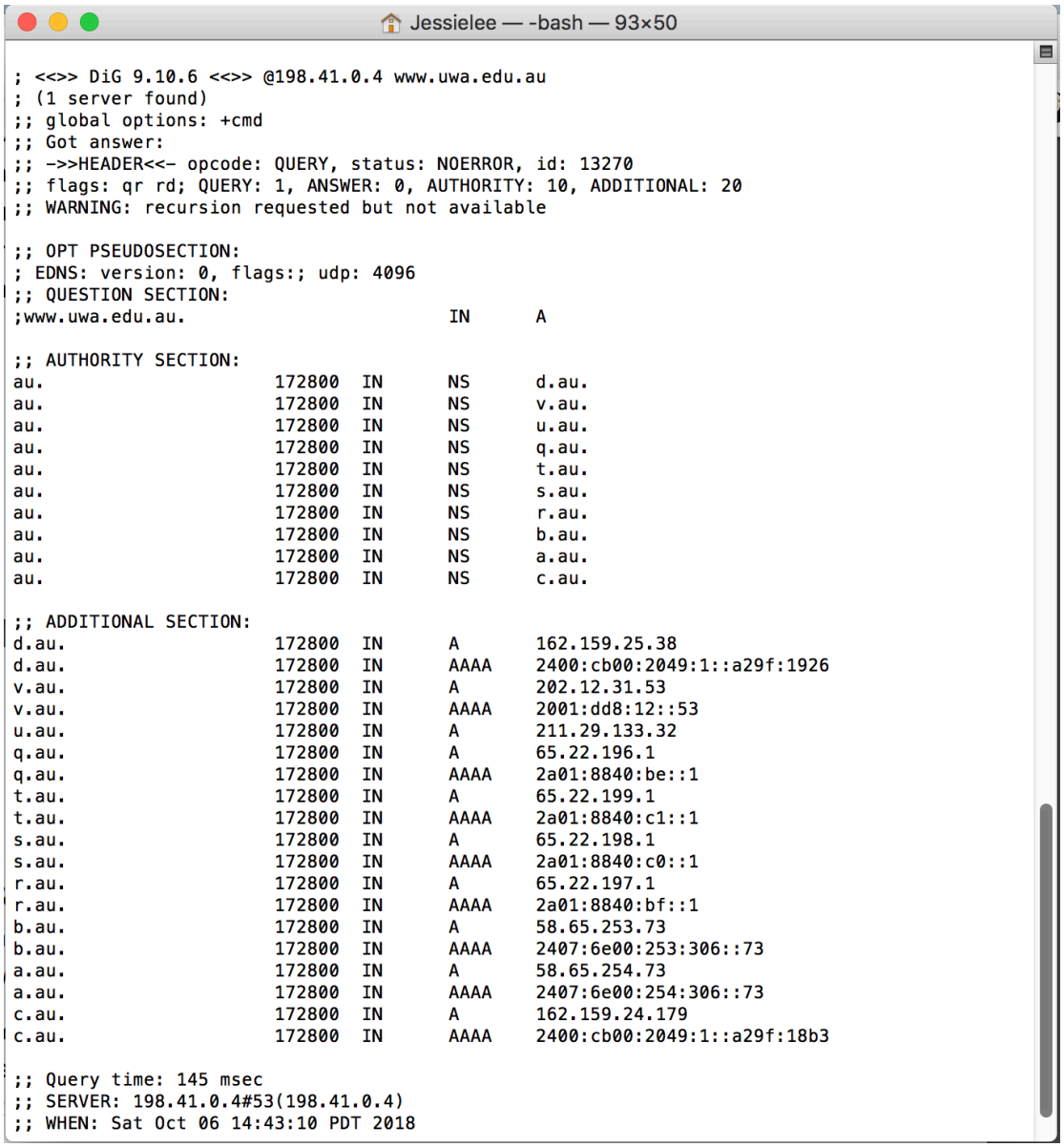
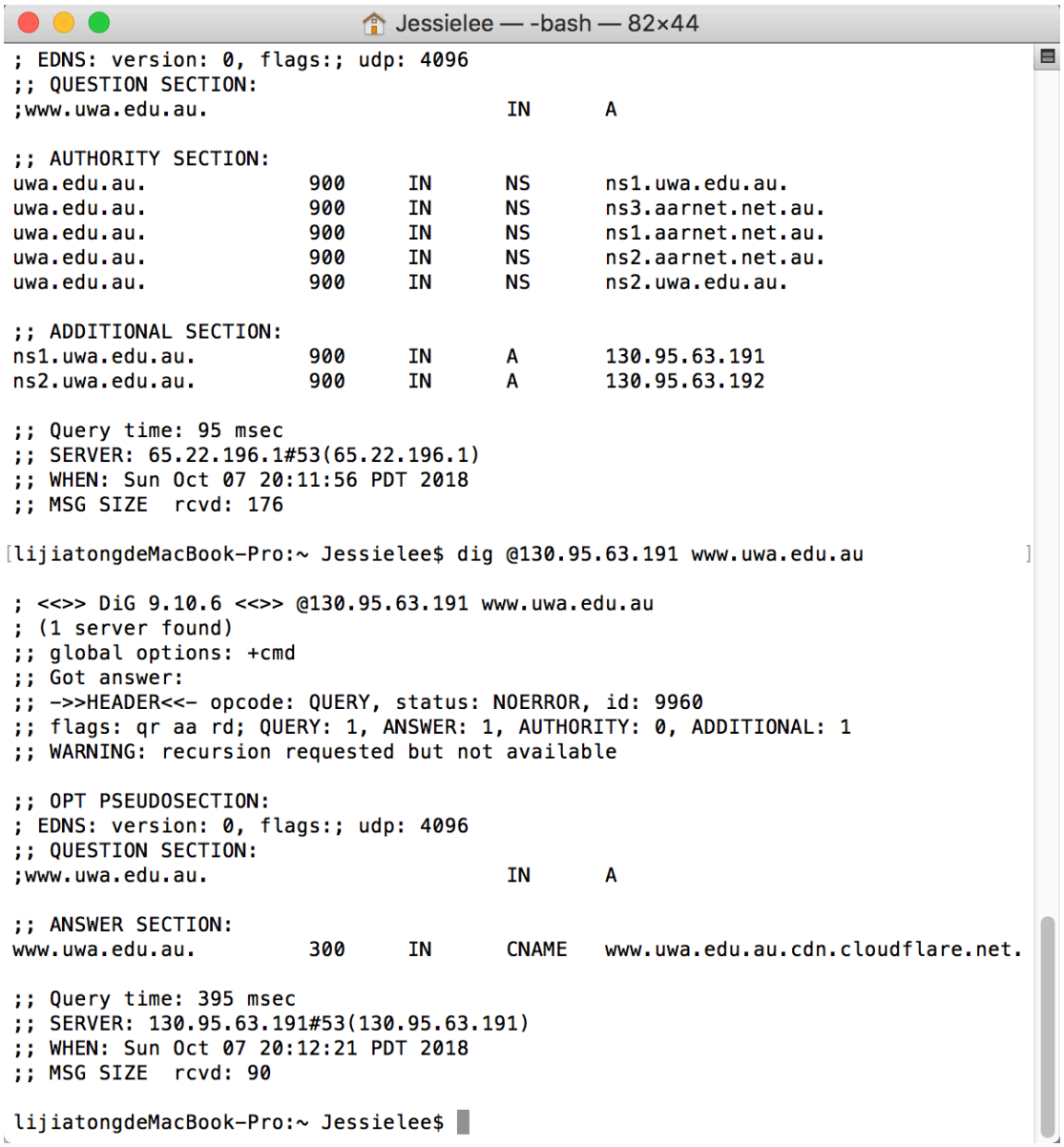
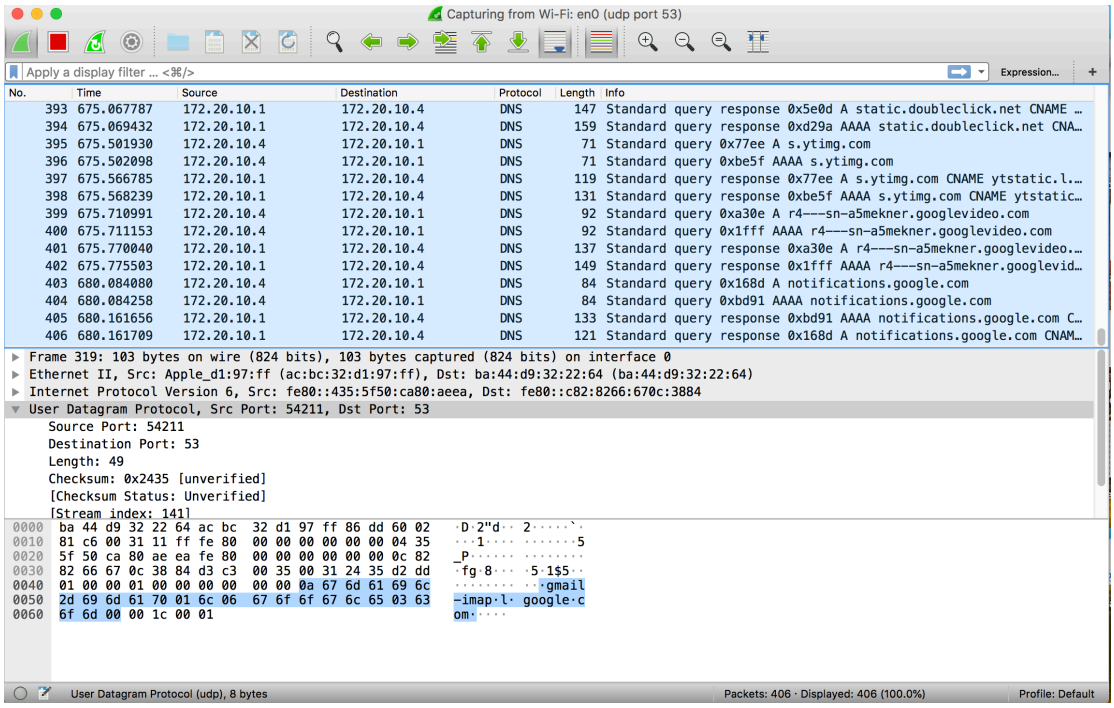

Jessielee — -bash — 93×50
; <<>> DiG 9.10.6 <<>> @198.41.0.4 www.uwa.edu.au
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 13270
;; flags: qr rd; QUERY: 1, ANSWER: 0, AUTHORITY: 10, ADDITIONAL: 20
;; WARNING: recursion requested but not available
;; 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 — 82×44
; 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:



Step4:

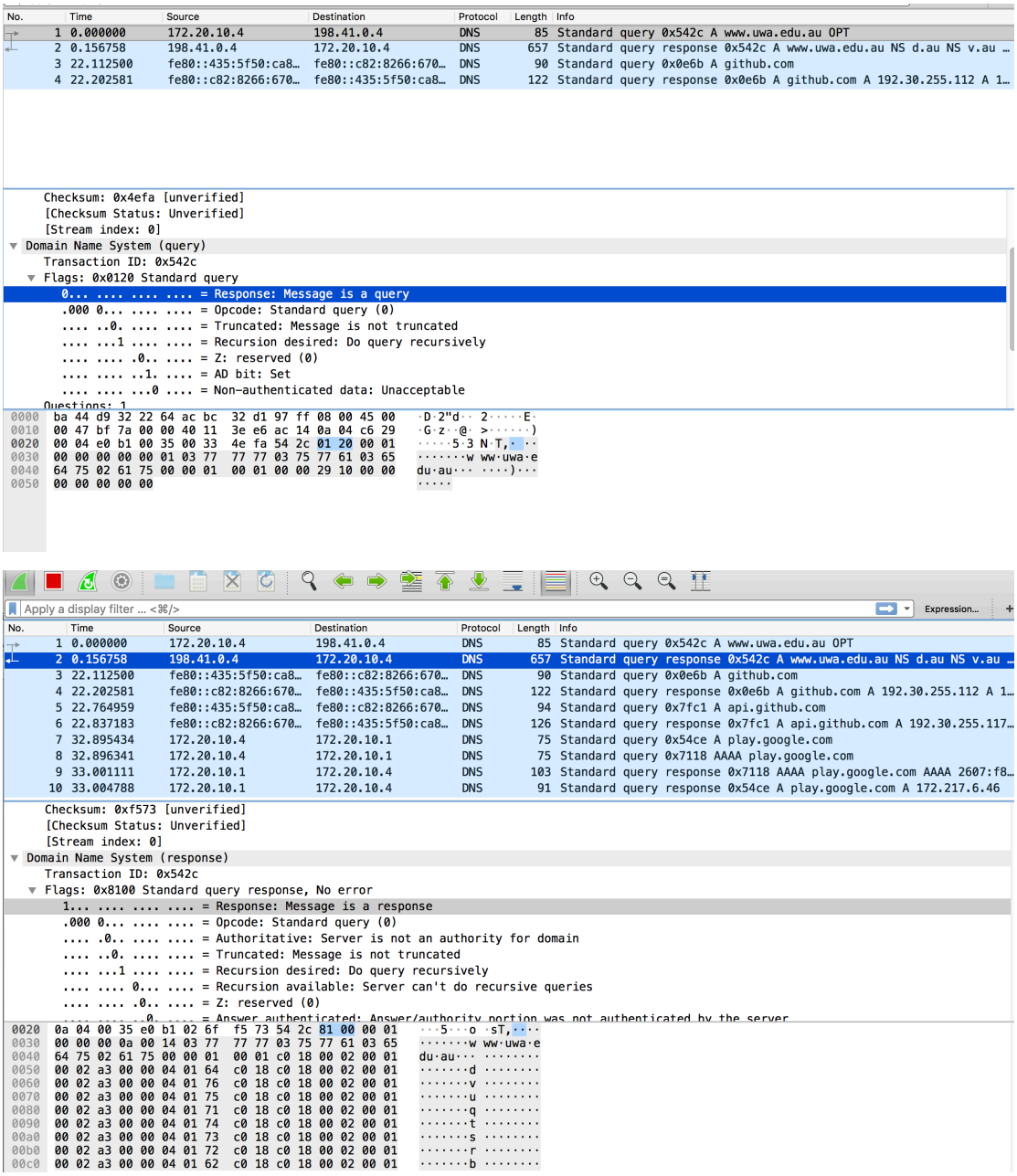
1. How many bits long is the Transaction ID? Based on this length, take your best guess as to how likely it is that concurrent transactions will use the same transaction ID.

   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.



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 Seclection

   Type is : NS(namesever)

```
▼ 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
```

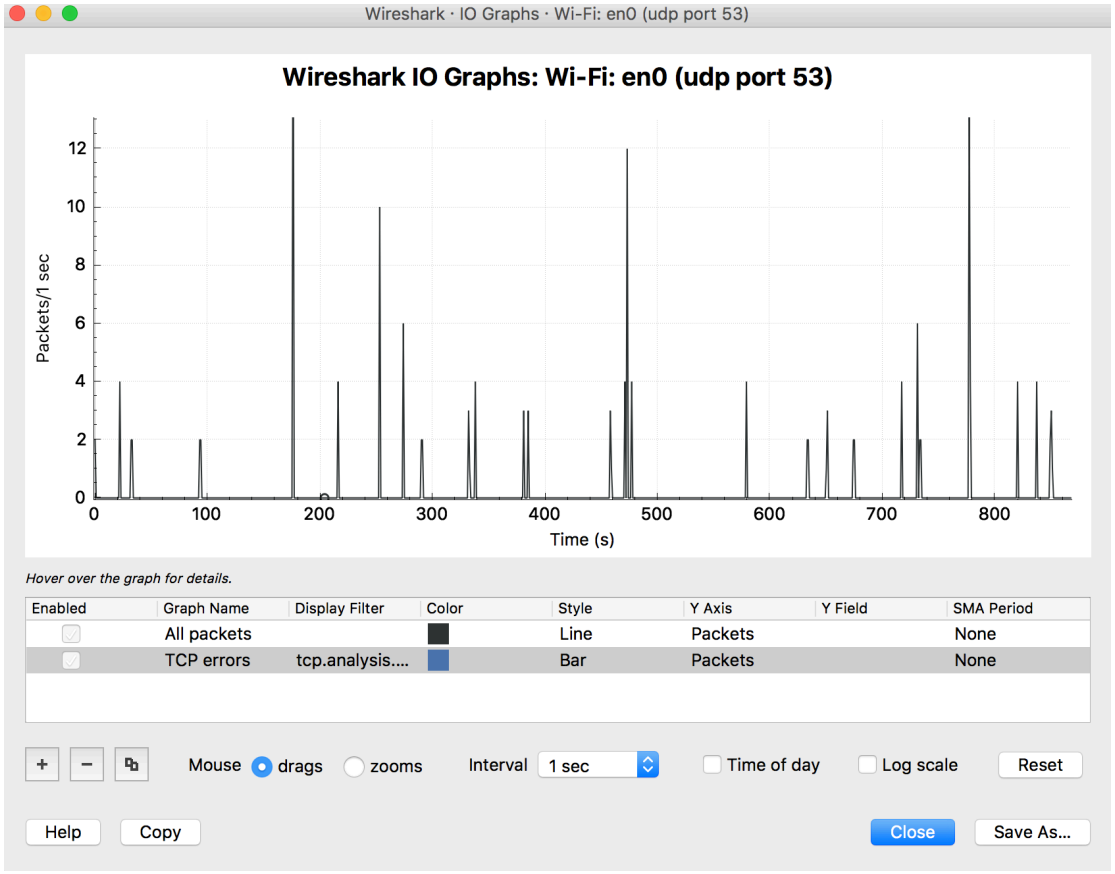
   The types are A for IPv4, AAAA for IPv6

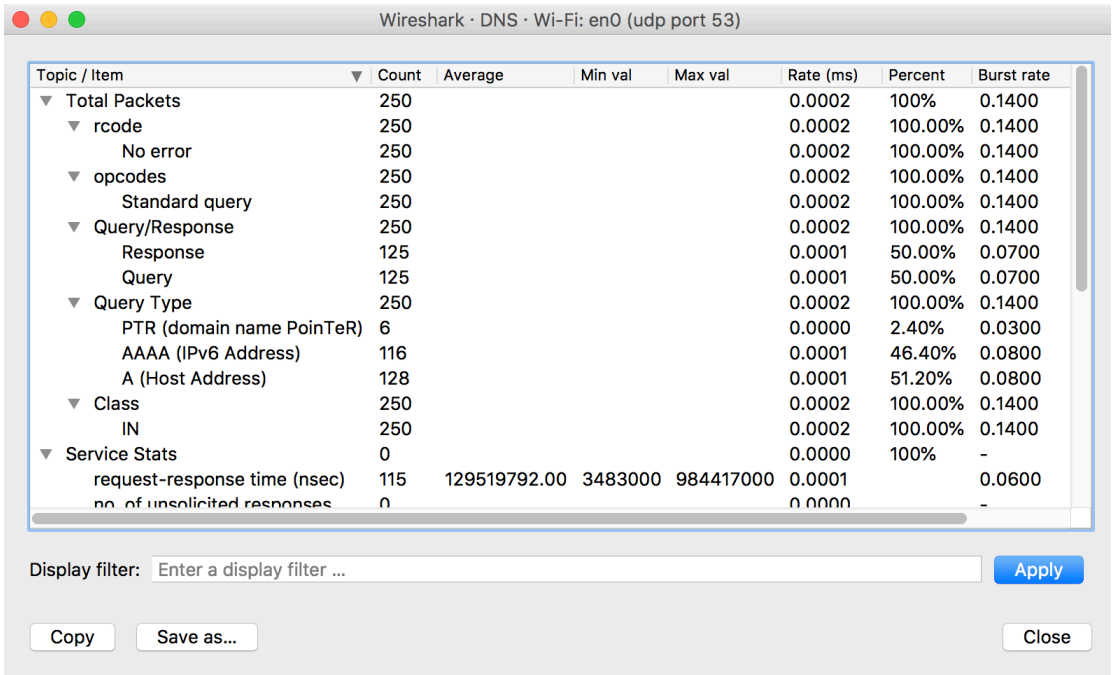
6. For the final response, in what section is the IP address of the domain name carried?

   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
```

Step 5：


Wireshark · IO Graphs · Wi-Fi: en0 (udp port 53)
Wireshark IO Graphs: Wi-Fi: en0 (udp port 53)
Packets/1 sec
Time (s)
Hover over the graph for details.
Enabled
Graph Name
Display Filter
Color
Style
Y Axis
Y Field
SMA Period
All packets
Line
Packets
None
TCP errors
tcp.analysis....
Bar
Packets
None
Mouse
drags
zooms
Interval
1 sec
Time of day
Log scale
Reset
Help
Copy
Close
Save As...


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
Display filter:
Enter a display filter ...
Apply
Copy
Save as...
Close