~~~~~~~~~~~~~~~~lab3~~~~~~~~~~~~~~~~

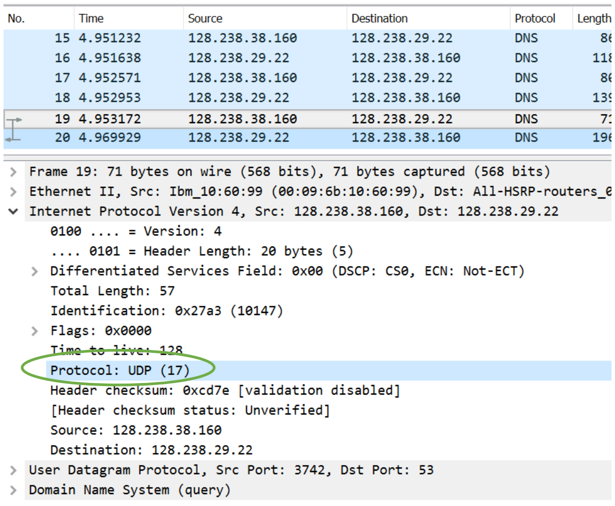
Exercise 1:

Type	description
A	Address record(32-bit IPV4)
CNAME	Canonical name record
MX	Mail exchange record
NS	Name server record
PTR	Pointer record
SOA	Start of [a zone of] authority record

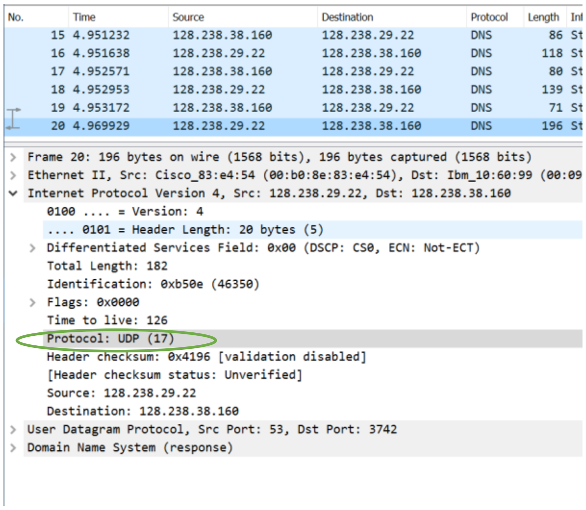
Exercise 2:

Question 1: What transport layer protocol is being used by the DNS messages?

UDP



```
No.      Time       Source           Destination      Protocol  Length
   15 4.951232   128.238.38.160   128.238.29.22    DNS        8
   16 4.951638   128.238.29.22    128.238.38.160   DNS       11
   17 4.952571   128.238.38.160   128.238.29.22    DNS        8
   18 4.952953   128.238.29.22    128.238.38.160   DNS       13
   19 4.953172   128.238.38.160   128.238.29.22    DNS        7
   20 4.969929   128.238.29.22    128.238.38.160   DNS       19

> Frame 19: 71 bytes on wire (568 bits), 71 bytes captured (568 bits)
> Ethernet II, Src: Ibm_10:60:99 (00:09:6b:10:60:99), Dst: All-HSRP-routers_0
v Internet Protocol Version 4, Src: 128.238.38.160, Dst: 128.238.29.22
     0100 .... = Version: 4
     .... 0101 = Header Length: 20 bytes (5)
   > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
     Total Length: 57
     Identification: 0x27a3 (10147)
   > Flags: 0x0000
     Time to live: 128
     Protocol: UDP (17)
     Header checksum: 0xcd7e [validation disabled]
     [Header checksum status: Unverified]
     Source: 128.238.38.160
     Destination: 128.238.29.22
> User Datagram Protocol, Src Port: 3742, Dst Port: 53
> Domain Name System (query)
```



```
No.      Time       Source           Destination      Protocol  Length  Inf
   15 4.951232   128.238.38.160   128.238.29.22    DNS         86  St
   16 4.951638   128.238.29.22    128.238.38.160   DNS        118  St
   17 4.952571   128.238.38.160   128.238.29.22    DNS         80  St
   18 4.952953   128.238.29.22    128.238.38.160   DNS        139  St
   19 4.953172   128.238.38.160   128.238.29.22    DNS         71  St
   20 4.969929   128.238.29.22    128.238.38.160   DNS        196  St

> Frame 20: 196 bytes on wire (1568 bits), 196 bytes captured (1568 bits)
> Ethernet II, Src: Cisco_83:e4:54 (00:b0:8e:83:e4:54), Dst: Ibm_10:60:99 (00:09
v Internet Protocol Version 4, Src: 128.238.29.22, Dst: 128.238.38.160
     0100 .... = Version: 4
     .... 0101 = Header Length: 20 bytes (5)
   > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
     Total Length: 182
     Identification: 0xb50e (46350)
   > Flags: 0x0000
     Time to live: 126
     Protocol: UDP (17)
     Header checksum: 0x4196 [validation disabled]
     [Header checksum status: Unverified]
     Source: 128.238.29.22
     Destination: 128.238.38.160
> User Datagram Protocol, Src Port: 53, Dst Port: 3742
> Domain Name System (response)
```

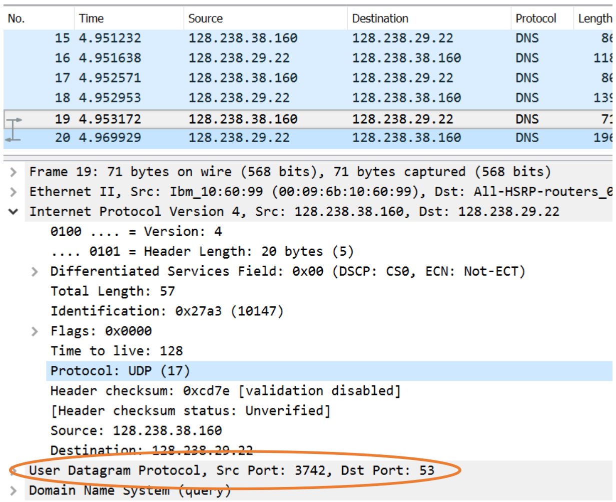
Question 2: What is the source and destination port for the DNS query message and the corresponding response?

Query: Source port: 3742

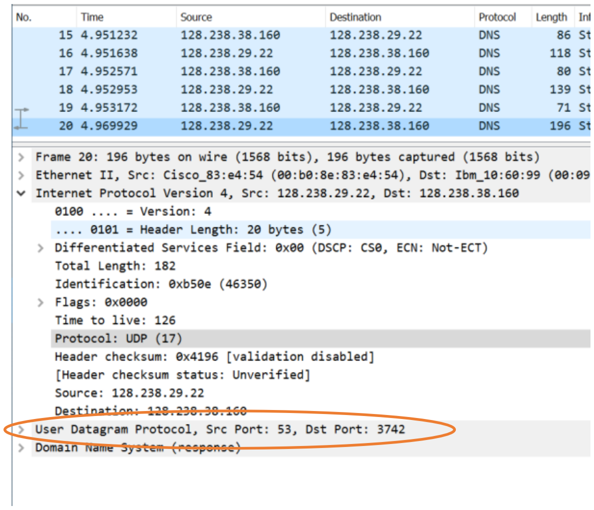
Destination port: 53

Response: Source port: 53

Destination port: 3742



```
No.    Time      Source          Destination     Protocol  Length
    15 4.951232  128.238.38.160  128.238.29.22   DNS       8
    16 4.951638  128.238.29.22   128.238.38.160  DNS       11
    17 4.952571  128.238.38.160  128.238.29.22   DNS       8
    18 4.952953  128.238.29.22   128.238.38.160  DNS       13
    19 4.953172  128.238.38.160  128.238.29.22   DNS       7
    20 4.969929  128.238.29.22   128.238.38.160  DNS       19

> Frame 19: 71 bytes on wire (568 bits), 71 bytes captured (568 bits)
> Ethernet II, Src: Ibm_10:60:99 (00:09:6b:10:60:99), Dst: All-HSRP-routers_0
v Internet Protocol Version 4, Src: 128.238.38.160, Dst: 128.238.29.22
     0100 .... = Version: 4
     .... 0101 = Header Length: 20 bytes (5)
   > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
     Total Length: 57
     Identification: 0x27a3 (10147)
   > Flags: 0x0000
     Time to live: 128
     Protocol: UDP (17)
     Header checksum: 0xcd7e [validation disabled]
     [Header checksum status: Unverified]
     Source: 128.238.38.160
     Destination: 128.238.29.22
> User Datagram Protocol, Src Port: 3742, Dst Port: 53
> Domain Name System (query)
```

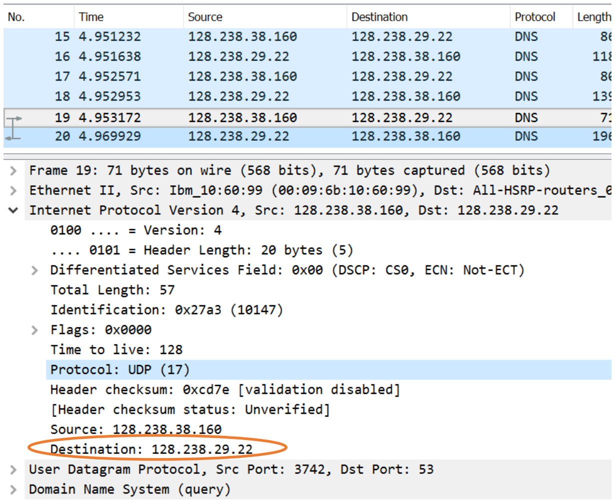


```
No.    Time      Source          Destination     Protocol  Length  Inf
    15 4.951232  128.238.38.160  128.238.29.22   DNS           86  St
    16 4.951638  128.238.29.22   128.238.38.160  DNS          118  St
    17 4.952571  128.238.38.160  128.238.29.22   DNS           80  St
    18 4.952953  128.238.29.22   128.238.38.160  DNS          139  St
    19 4.953172  128.238.38.160  128.238.29.22   DNS           71  St
    20 4.969929  128.238.29.22   128.238.38.160  DNS          196  St

> Frame 20: 196 bytes on wire (1568 bits), 196 bytes captured (1568 bits)
> Ethernet II, Src: Cisco_83:e4:54 (00:b0:8e:83:e4:54), Dst: Ibm_10:60:99 (00:09
v Internet Protocol Version 4, Src: 128.238.29.22, Dst: 128.238.38.160
     0100 .... = Version: 4
     .... 0101 = Header Length: 20 bytes (5)
   > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
     Total Length: 182
     Identification: 0xb50e (46350)
   > Flags: 0x0000
     Time to live: 126
     Protocol: UDP (17)
     Header checksum: 0x4196 [validation disabled]
     [Header checksum status: Unverified]
     Source: 128.238.29.22
     Destination: 128.238.38.160
> User Datagram Protocol, Src Port: 53, Dst Port: 3742
> Domain Name System (response)
```

Question 3: To what IP address is the DNS query message sent? Is this the same as the default local DNS server?

IP address the DNS query message sent: 128.238.29.22.

The IP address of the default DNS server for the host is 128.238.29.22. So they are the same.



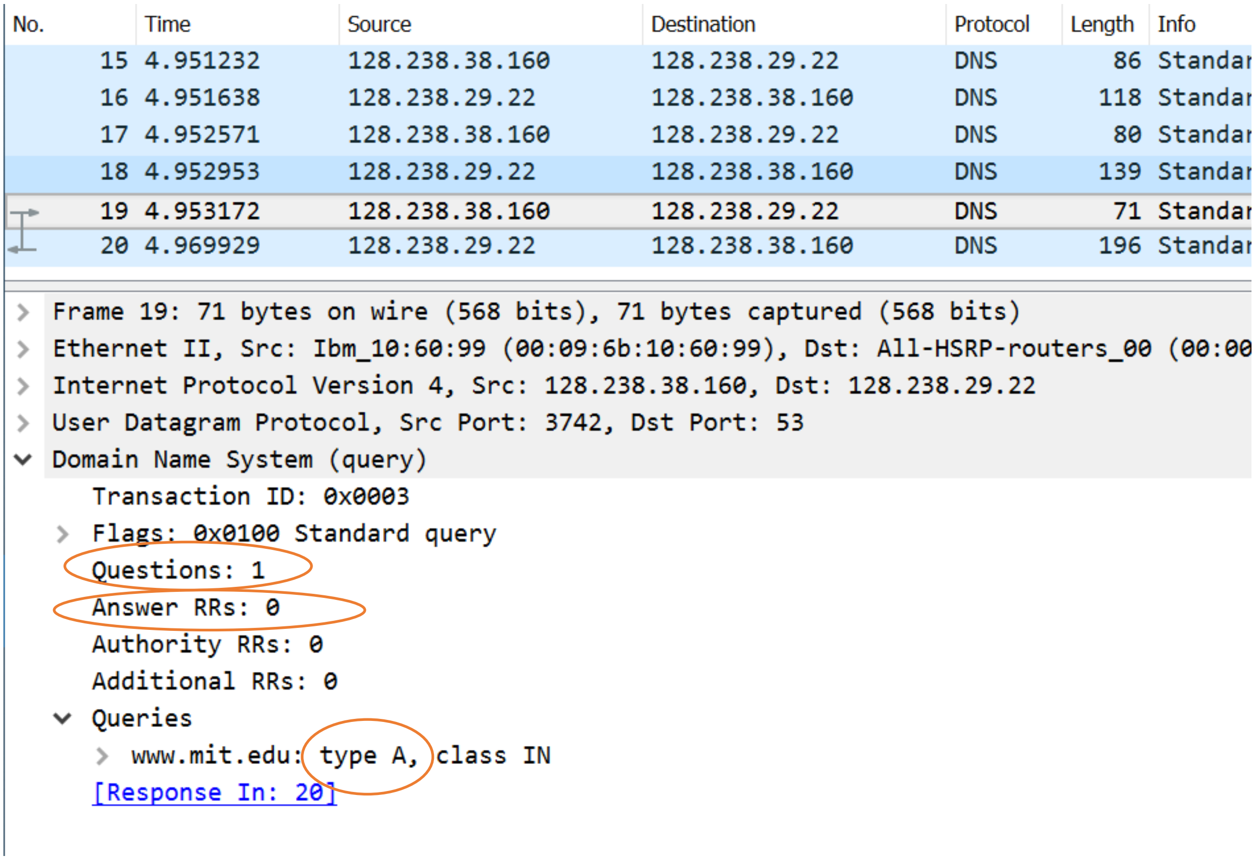
```
No.    Time      Source          Destination     Protocol  Length
    15 4.951232  128.238.38.160  128.238.29.22   DNS       8
    16 4.951638  128.238.29.22   128.238.38.160  DNS       11
    17 4.952571  128.238.38.160  128.238.29.22   DNS       8
    18 4.952953  128.238.29.22   128.238.38.160  DNS       13
    19 4.953172  128.238.38.160  128.238.29.22   DNS       7
    20 4.969929  128.238.29.22   128.238.38.160  DNS       19

> Frame 19: 71 bytes on wire (568 bits), 71 bytes captured (568 bits)
> Ethernet II, Src: Ibm_10:60:99 (00:09:6b:10:60:99), Dst: All-HSRP-routers_0
v Internet Protocol Version 4, Src: 128.238.38.160, Dst: 128.238.29.22
     0100 .... = Version: 4
     .... 0101 = Header Length: 20 bytes (5)
   > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
     Total Length: 57
     Identification: 0x27a3 (10147)
   > Flags: 0x0000
     Time to live: 128
     Protocol: UDP (17)
     Header checksum: 0xcd7e [validation disabled]
     [Header checksum status: Unverified]
     Source: 128.238.38.160
     Destination: 128.238.29.22
> User Datagram Protocol, Src Port: 3742, Dst Port: 53
> Domain Name System (query)
```

Question 4: How many “questions” are contained in the DNS query message? What “Type” of DNS queries are they? Does the query message also contain any “answers”?

One question.

Type A.

No “answer”.



```
No.    Time        Source           Destination      Protocol  Length  Info
  15 4.951232    128.238.38.160   128.238.29.22    DNS         86  Standar
  16 4.951638    128.238.29.22    128.238.38.160   DNS        118  Standar
  17 4.952571    128.238.38.160   128.238.29.22    DNS         80  Standar
  18 4.952953    128.238.29.22    128.238.38.160   DNS        139  Standar
  19 4.953172    128.238.38.160   128.238.29.22    DNS         71  Standar
  20 4.969929    128.238.29.22    128.238.38.160   DNS        196  Standar
```

```
> Frame 19: 71 bytes on wire (568 bits), 71 bytes captured (568 bits)
> Ethernet II, Src: Ibm_10:60:99 (00:09:6b:10:60:99), Dst: All-HSRP-routers_00 (00:00
> Internet Protocol Version 4, Src: 128.238.38.160, Dst: 128.238.29.22
> User Datagram Protocol, Src Port: 3742, Dst Port: 53
v Domain Name System (query)
     Transaction ID: 0x0003
   > Flags: 0x0100 Standard query
     Questions: 1
     Answer RRs: 0
     Authority RRs: 0
     Additional RRs: 0
   v Queries
      > www.mit.edu: type A, class IN
     [Response In: 20]
```

Question 5: Examine the DNS response message. Provide details of the contents of the “Answers”, “Authority” and “Additional Information” fields. What can you infer from these?

Answer: mit.edu.edu: type A, class IN, addr 18.7.22.83

Authority: mit.edu.edu: type NS, class IN, ns BITSY.mit.edu

mit.edu.edu: type NS, class IN, ns STRAWB.mit.edu

mit.edu.edu: type NS, class IN, ns W20NS.mit.edu

Additional Information: BITSY.mit.edu: type A, class IN, addr 18.72.0.3

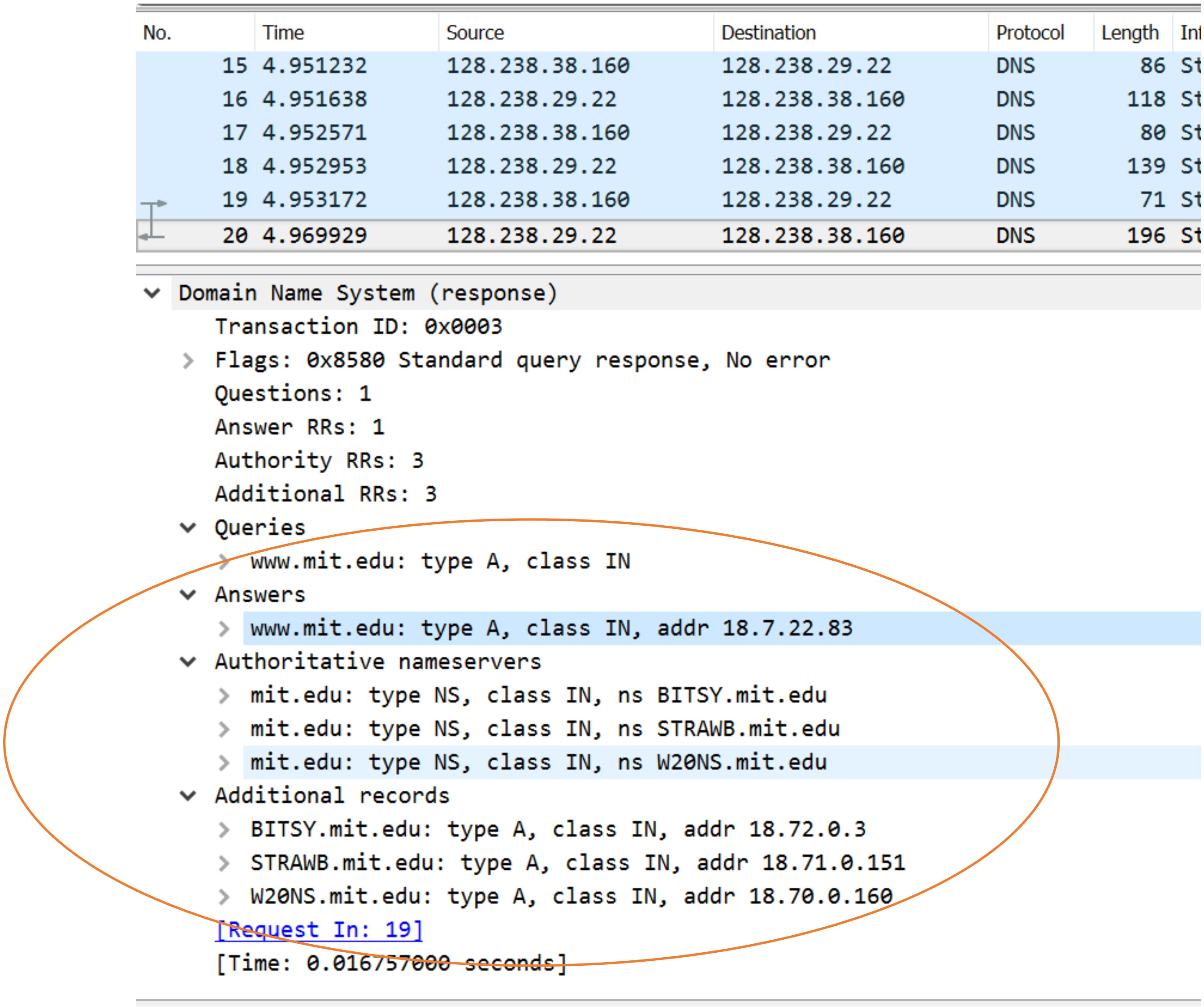
STRAWB.mit.edu: type A, class IN, addr 18.71.0.151

W20NS.mit.edu: type A, class IN, addr 18.70.0.160

Detail of “Answers”: Answers contain a A type RR which list the detail of the host name, IP address etc

“Authority” list some RR of other Authority servers in type NS

“Additional Information” giving some type A RR of Authority servers list in “Authority”



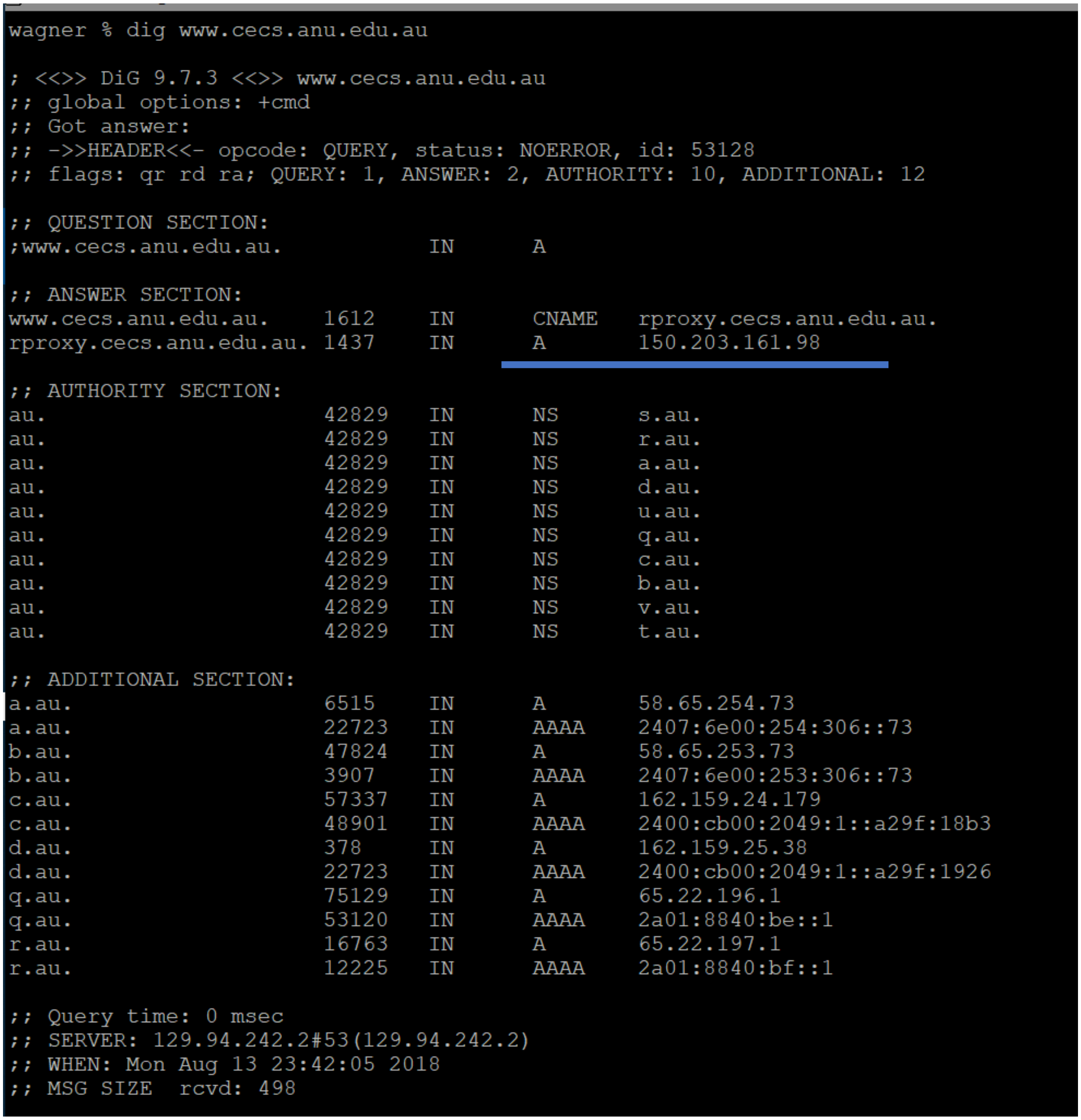
```
No.     Time        Source            Destination       Protocol  Length  Inf
     15 4.951232    128.238.38.160    128.238.29.22     DNS           86  St
     16 4.951638    128.238.29.22     128.238.38.160    DNS          118  St
     17 4.952571    128.238.38.160    128.238.29.22     DNS           80  St
     18 4.952953    128.238.29.22     128.238.38.160    DNS          139  St
     19 4.953172    128.238.38.160    128.238.29.22     DNS           71  St
     20 4.969929    128.238.29.22     128.238.38.160    DNS          196  St
```

```
v Domain Name System (response)
    Transaction ID: 0x0003
  > Flags: 0x8580 Standard query response, No error
    Questions: 1
    Answer RRs: 1
    Authority RRs: 3
    Additional RRs: 3
  v Queries
    > www.mit.edu: type A, class IN
  v Answers
    > www.mit.edu: type A, class IN, addr 18.7.22.83
  v Authoritative nameservers
    > mit.edu: type NS, class IN, ns BITSY.mit.edu
    > mit.edu: type NS, class IN, ns STRAWB.mit.edu
    > mit.edu: type NS, class IN, ns W20NS.mit.edu
  v Additional records
    > BITSY.mit.edu: type A, class IN, addr 18.72.0.3
    > STRAWB.mit.edu: type A, class IN, addr 18.71.0.151
    > W20NS.mit.edu: type A, class IN, addr 18.70.0.160
    [Request In: 19]
    [Time: 0.016757000 seconds]
```

Exercise 3:

Question 1. What is the IP address of www.cecs.anu.edu.au . What type of DNS query is sent to get this answer?

The IP address is 150.203.161.98. The type is A.



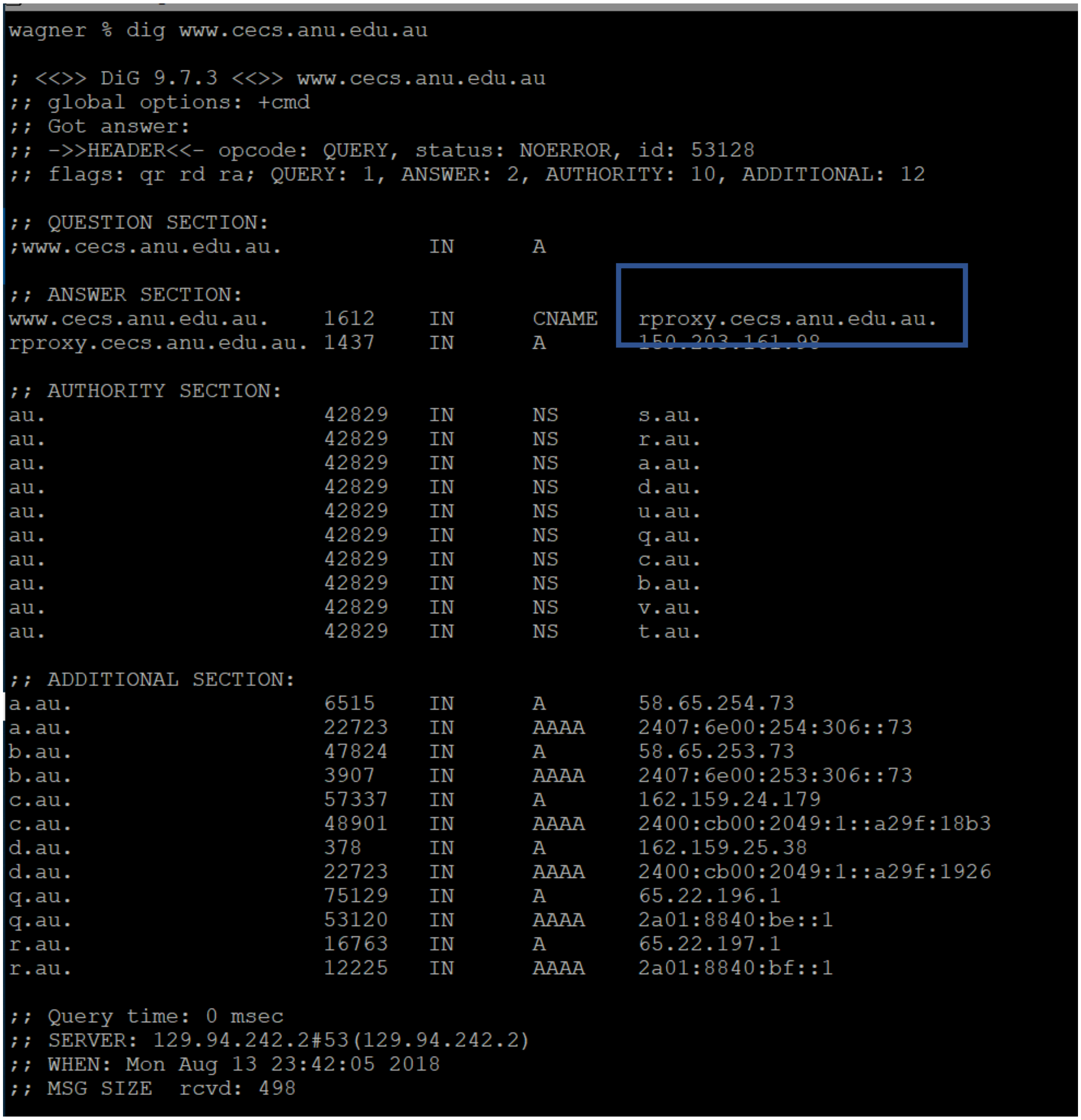
```
wagner % dig www.cecs.anu.edu.au

; <<>> DiG 9.7.3 <<>> www.cecs.anu.edu.au
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 53128
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 10, ADDITIONAL: 12

;; QUESTION SECTION:
;www.cecs.anu.edu.au.           IN      A

;; ANSWER SECTION:
www.cecs.anu.edu.au.    1612    IN      CNAME   rproxy.cecs.anu.edu.au.
rproxy.cecs.anu.edu.au. 1437    IN      A       150.203.161.98

;; AUTHORITY SECTION:
au.                     42829   IN      NS      s.au.
au.                     42829   IN      NS      r.au.
au.                     42829   IN      NS      a.au.
au.                     42829   IN      NS      d.au.
au.                     42829   IN      NS      u.au.
au.                     42829   IN      NS      q.au.
au.                     42829   IN      NS      c.au.
au.                     42829   IN      NS      b.au.
au.                     42829   IN      NS      v.au.
au.                     42829   IN      NS      t.au.

;; ADDITIONAL SECTION:
a.au.                   6515    IN      A       58.65.254.73
a.au.                   22723   IN      AAAA    2407:6e00:254:306::73
b.au.                   47824   IN      A       58.65.253.73
b.au.                   3907    IN      AAAA    2407:6e00:253:306::73
c.au.                   57337   IN      A       162.159.24.179
c.au.                   48901   IN      AAAA    2400:cb00:2049:1::a29f:18b3
d.au.                   378     IN      A       162.159.25.38
d.au.                   22723   IN      AAAA    2400:cb00:2049:1::a29f:1926
q.au.                   75129   IN      A       65.22.196.1
q.au.                   53120   IN      AAAA    2a01:8840:be::1
r.au.                   16763   IN      A       65.22.197.1
r.au.                   12225   IN      AAAA    2a01:8840:bf::1

;; Query time: 0 msec
;; SERVER: 129.94.242.2#53(129.94.242.2)
;; WHEN: Mon Aug 13 23:42:05 2018
;; MSG SIZE  rcvd: 498
```

Question 2. What is the canonical name for the CECS ANU web server? What is its IP address? Suggest a reason for having an alias for this server.

Canonical name: rproxy.cecs.anu.edu.au

Its IP address: 150.203.161.98.

Alias host name, are usually more memorable than canonical hostnames.



```
wagner % dig www.cecs.anu.edu.au

; <<>> DiG 9.7.3 <<>> www.cecs.anu.edu.au
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 53128
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 10, ADDITIONAL: 12

;; QUESTION SECTION:
;www.cecs.anu.edu.au.           IN      A

;; ANSWER SECTION:
www.cecs.anu.edu.au.    1612    IN      CNAME   rproxy.cecs.anu.edu.au.
rproxy.cecs.anu.edu.au. 1437    IN      A       150.203.161.98

;; AUTHORITY SECTION:
au.                     42829   IN      NS      s.au.
au.                     42829   IN      NS      r.au.
au.                     42829   IN      NS      a.au.
au.                     42829   IN      NS      d.au.
au.                     42829   IN      NS      u.au.
au.                     42829   IN      NS      q.au.
au.                     42829   IN      NS      c.au.
au.                     42829   IN      NS      b.au.
au.                     42829   IN      NS      v.au.
au.                     42829   IN      NS      t.au.

;; ADDITIONAL SECTION:
a.au.                   6515    IN      A       58.65.254.73
a.au.                   22723   IN      AAAA    2407:6e00:254:306::73
b.au.                   47824   IN      A       58.65.253.73
b.au.                   3907    IN      AAAA    2407:6e00:253:306::73
c.au.                   57337   IN      A       162.159.24.179
c.au.                   48901   IN      AAAA    2400:cb00:2049:1::a29f:18b3
d.au.                   378     IN      A       162.159.25.38
d.au.                   22723   IN      AAAA    2400:cb00:2049:1::a29f:1926
q.au.                   75129   IN      A       65.22.196.1
q.au.                   53120   IN      AAAA    2a01:8840:be::1
r.au.                   16763   IN      A       65.22.197.1
r.au.                   12225   IN      AAAA    2a01:8840:bf::1

;; Query time: 0 msec
;; SERVER: 129.94.242.2#53(129.94.242.2)
;; WHEN: Mon Aug 13 23:42:05 2018
;; MSG SIZE  rcvd: 498
```

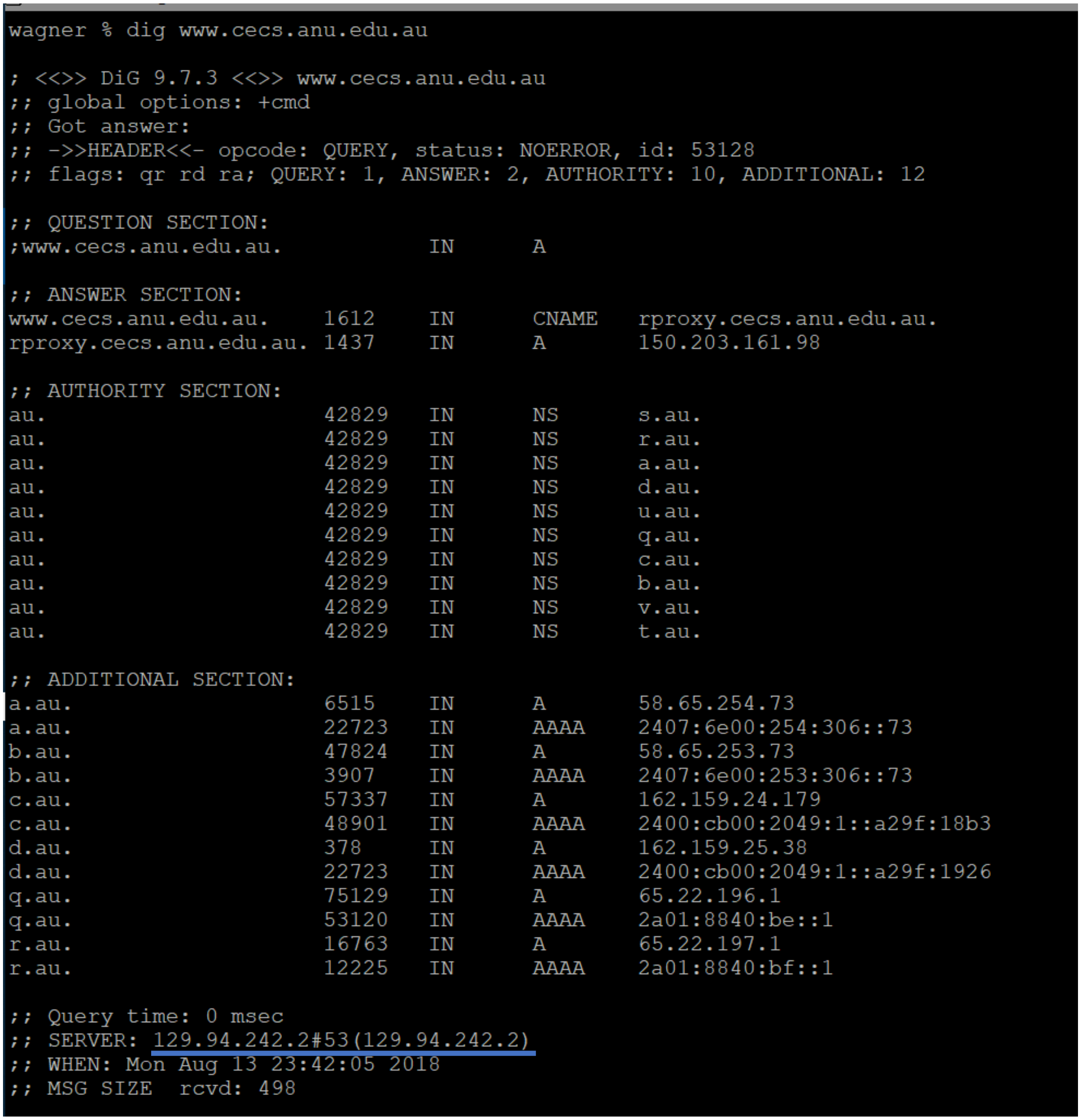
Question 3. What can you make of the rest of the response (i.e. the details available in the Authority and Additional sections)?

AUTHORITY SECTION contains some resource record in type NS. Their domain name are all “cecs.anu.edu.au.” and their authority server name were list in the above picture.

In ADDITIONAL SECTION , there are A/AAAA type RR of those Authoritative DNS Server list in AUTHORITY SECTION which showing their IPv4 or IPv6 address

Question 4. What is the IP address of the local nameserver for your machine?

My local IP address: 129.94.242.2.



```
wagner % dig www.cecs.anu.edu.au

; <<>> DiG 9.7.3 <<>> www.cecs.anu.edu.au
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 53128
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 10, ADDITIONAL: 12

;; QUESTION SECTION:
;www.cecs.anu.edu.au.           IN      A

;; ANSWER SECTION:
www.cecs.anu.edu.au.    1612    IN      CNAME   rproxy.cecs.anu.edu.au.
rproxy.cecs.anu.edu.au. 1437    IN      A       150.203.161.98

;; AUTHORITY SECTION:
au.                     42829   IN      NS      s.au.
au.                     42829   IN      NS      r.au.
au.                     42829   IN      NS      a.au.
au.                     42829   IN      NS      d.au.
au.                     42829   IN      NS      u.au.
au.                     42829   IN      NS      q.au.
au.                     42829   IN      NS      c.au.
au.                     42829   IN      NS      b.au.
au.                     42829   IN      NS      v.au.
au.                     42829   IN      NS      t.au.

;; ADDITIONAL SECTION:
a.au.                   6515    IN      A       58.65.254.73
a.au.                   22723   IN      AAAA    2407:6e00:254:306::73
b.au.                   47824   IN      A       58.65.253.73
b.au.                   3907    IN      AAAA    2407:6e00:253:306::73
c.au.                   57337   IN      A       162.159.24.179
c.au.                   48901   IN      AAAA    2400:cb00:2049:1::a29f:18b3
d.au.                   378     IN      A       162.159.25.38
d.au.                   22723   IN      AAAA    2400:cb00:2049:1::a29f:1926
q.au.                   75129   IN      A       65.22.196.1
q.au.                   53120   IN      AAAA    2a01:8840:be::1
r.au.                   16763   IN      A       65.22.197.1
r.au.                   12225   IN      AAAA    2a01:8840:bf::1

;; Query time: 0 msec
;; SERVER: 129.94.242.2#53(129.94.242.2)
;; WHEN: Mon Aug 13 23:42:05 2018
;; MSG SIZE  rcvd: 498
```

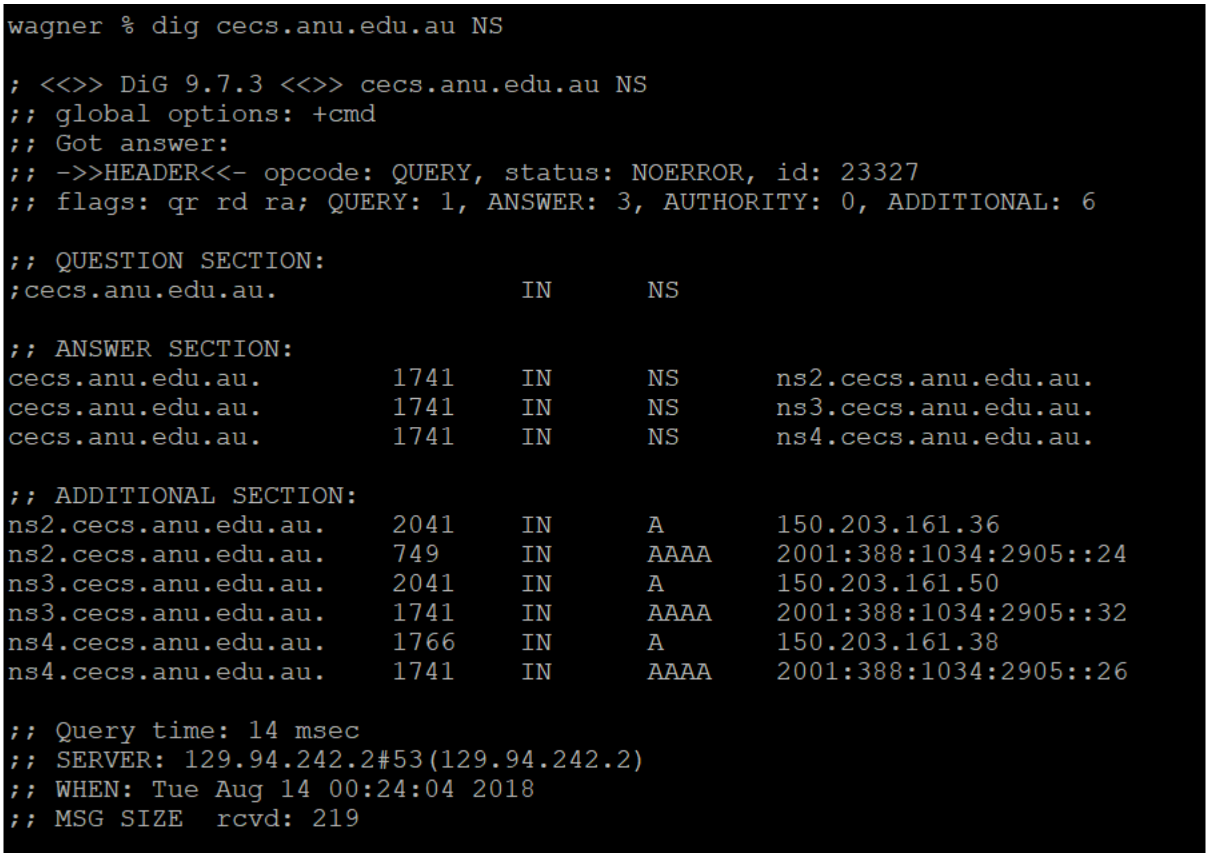
Question 5. What are the DNS nameservers for the “cecs.anu.edu.au” domain (note: the domain name is cecs.anu.edu.au and not www.cecs.anu.edu.au)? Find out their IP addresses? What type of DNS query is sent to obtain this information?

The nameservers: ns2.cecs.anu.edu.au 150.203.161.36

ns3.cecs.anu.edu.au 150.203.161.50

ns4.cecs.anu.edu.au 150.203.161.38

The type of DNS query is sent to obtain this information: NS



```
wagner % dig cecs.anu.edu.au NS

; <<>> DiG 9.7.3 <<>> cecs.anu.edu.au NS
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 23327
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 6

;; QUESTION SECTION:
;cecs.anu.edu.au.               IN      NS

;; ANSWER SECTION:
cecs.anu.edu.au.        1741    IN      NS      ns2.cecs.anu.edu.au.
cecs.anu.edu.au.        1741    IN      NS      ns3.cecs.anu.edu.au.
cecs.anu.edu.au.        1741    IN      NS      ns4.cecs.anu.edu.au.

;; ADDITIONAL SECTION:
ns2.cecs.anu.edu.au.    2041    IN      A       150.203.161.36
ns2.cecs.anu.edu.au.    749     IN      AAAA    2001:388:1034:2905::24
ns3.cecs.anu.edu.au.    2041    IN      A       150.203.161.50
ns3.cecs.anu.edu.au.    1741    IN      AAAA    2001:388:1034:2905::32
ns4.cecs.anu.edu.au.    1766    IN      A       150.203.161.38
ns4.cecs.anu.edu.au.    1741    IN      AAAA    2001:388:1034:2905::26

;; Query time: 14 msec
;; SERVER: 129.94.242.2#53(129.94.242.2)
;; WHEN: Tue Aug 14 00:24:04 2018
;; MSG SIZE  rcvd: 219
```

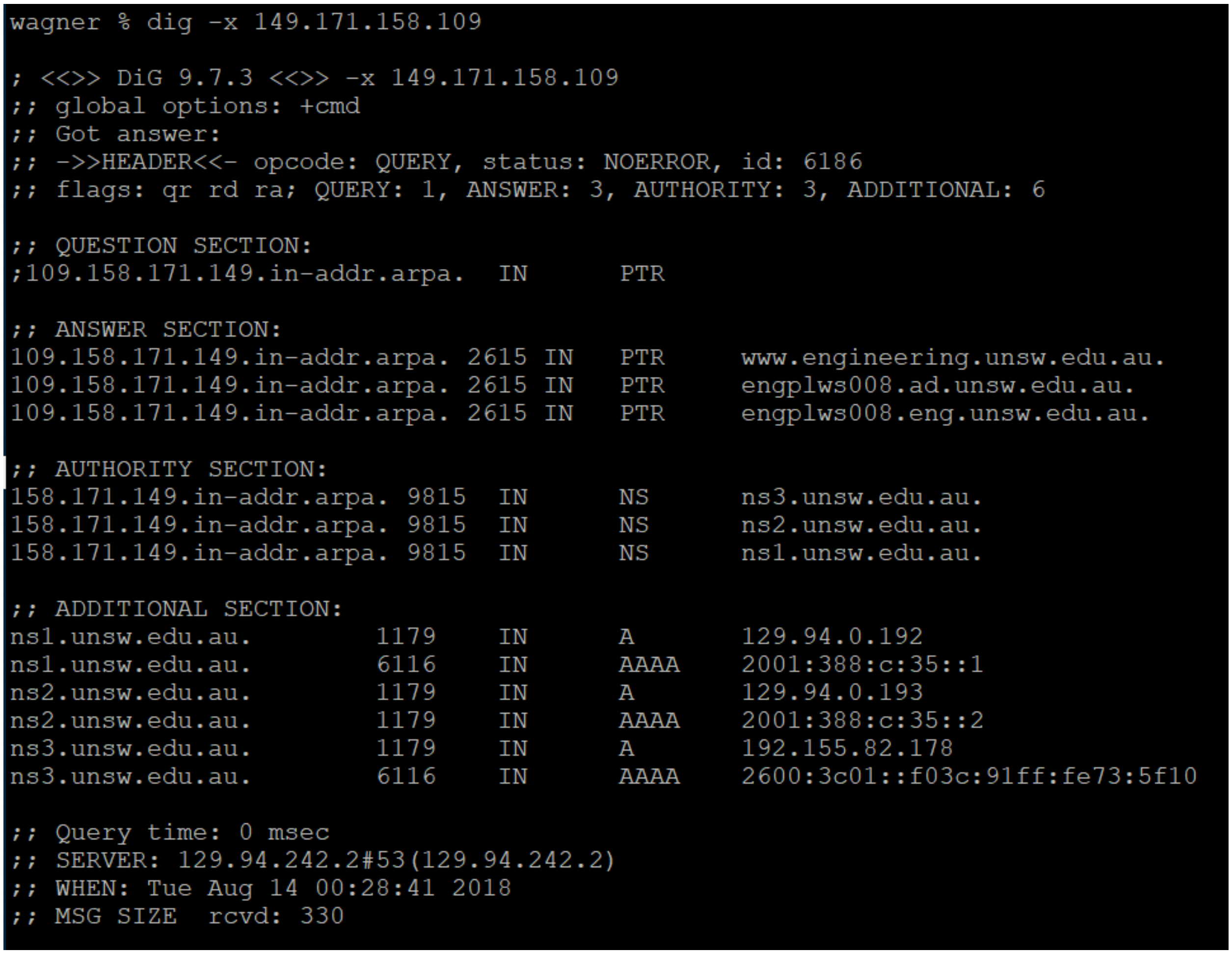
Question 6. What is the DNS name associated with the IP address 149.171.158.109? What type of DNS query is sent to obtain this information?

The DNS name: www.engineering.unsw.edu.au

engplws008.ad.unsw.edu.au

engplws008.eng.unsw.edu.au

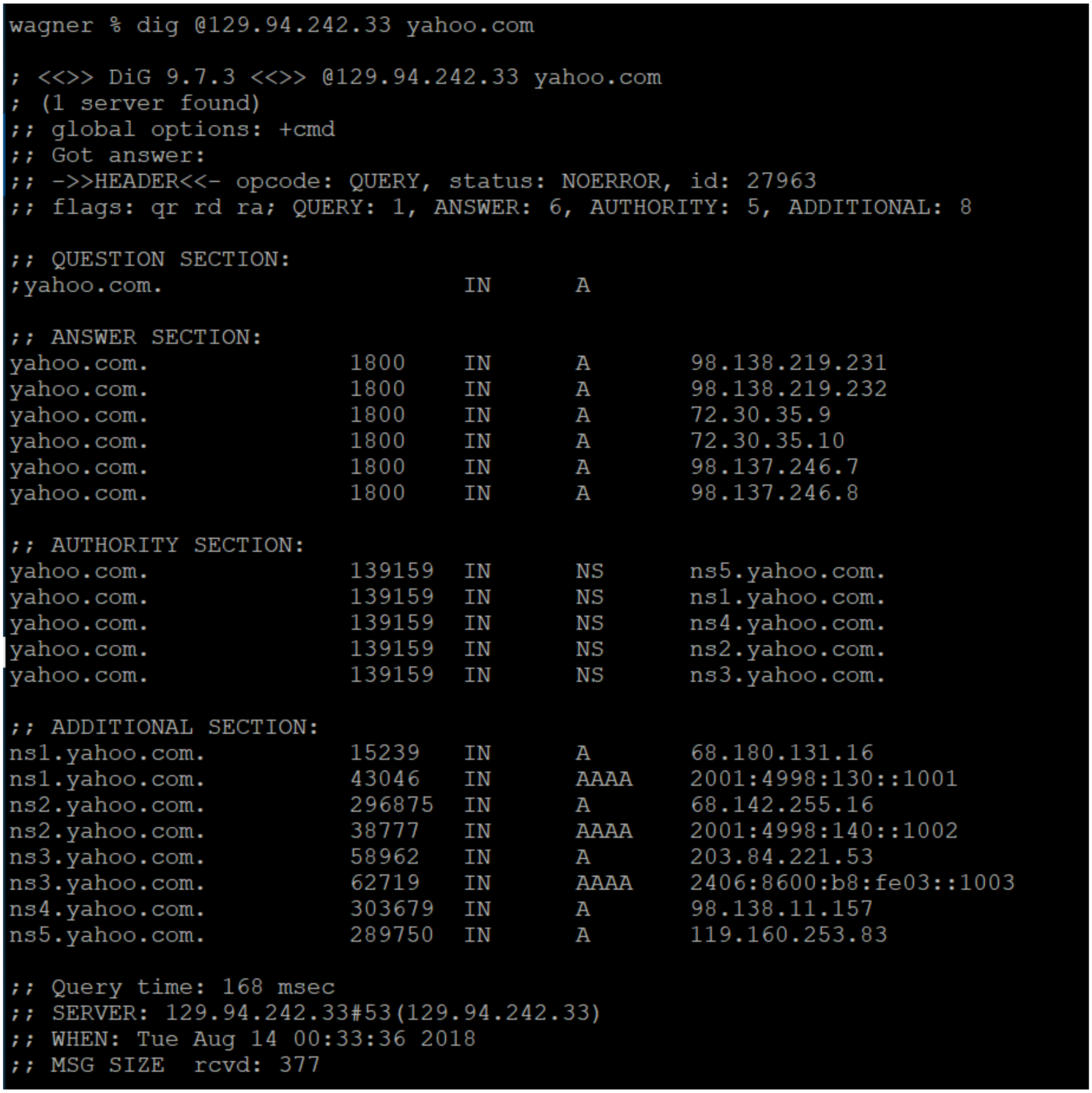
The type of DNS query is sent: PTR



```
wagner % dig -x 149.171.158.109

; <<>> DiG 9.7.3 <<>> -x 149.171.158.109
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 6186
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 3, ADDITIONAL: 6

;; QUESTION SECTION:
;109.158.171.149.in-addr.arpa.  IN      PTR

;; ANSWER SECTION:
109.158.171.149.in-addr.arpa. 2615 IN   PTR     www.engineering.unsw.edu.au.
109.158.171.149.in-addr.arpa. 2615 IN   PTR     engplws008.ad.unsw.edu.au.
109.158.171.149.in-addr.arpa. 2615 IN   PTR     engplws008.eng.unsw.edu.au.

;; AUTHORITY SECTION:
158.171.149.in-addr.arpa. 9815  IN      NS      ns3.unsw.edu.au.
158.171.149.in-addr.arpa. 9815  IN      NS      ns2.unsw.edu.au.
158.171.149.in-addr.arpa. 9815  IN      NS      ns1.unsw.edu.au.

;; ADDITIONAL SECTION:
ns1.unsw.edu.au.        1179    IN      A       129.94.0.192
ns1.unsw.edu.au.        6116    IN      AAAA    2001:388:c:35::1
ns2.unsw.edu.au.        1179    IN      A       129.94.0.193
ns2.unsw.edu.au.        1179    IN      AAAA    2001:388:c:35::2
ns3.unsw.edu.au.        1179    IN      A       192.155.82.178
ns3.unsw.edu.au.        6116    IN      AAAA    2600:3c01::f03c:91ff:fe73:5f10

;; Query time: 0 msec
;; SERVER: 129.94.242.2#53(129.94.242.2)
;; WHEN: Tue Aug 14 00:28:41 2018
;; MSG SIZE  rcvd: 330
```

Question 7. Run dig and query the CSE nameserver (129.94.242.33) for the mail servers for Yahoo! Mail (again the domain name is yahoo.com, not www.yahoo.com). Did you get an authoritative answer? Why? (HINT: Just because a response contains information in the authoritative part of the DNS response message does not mean it came from an authoritative name server. You should examine the flags in the response to determine the answer)

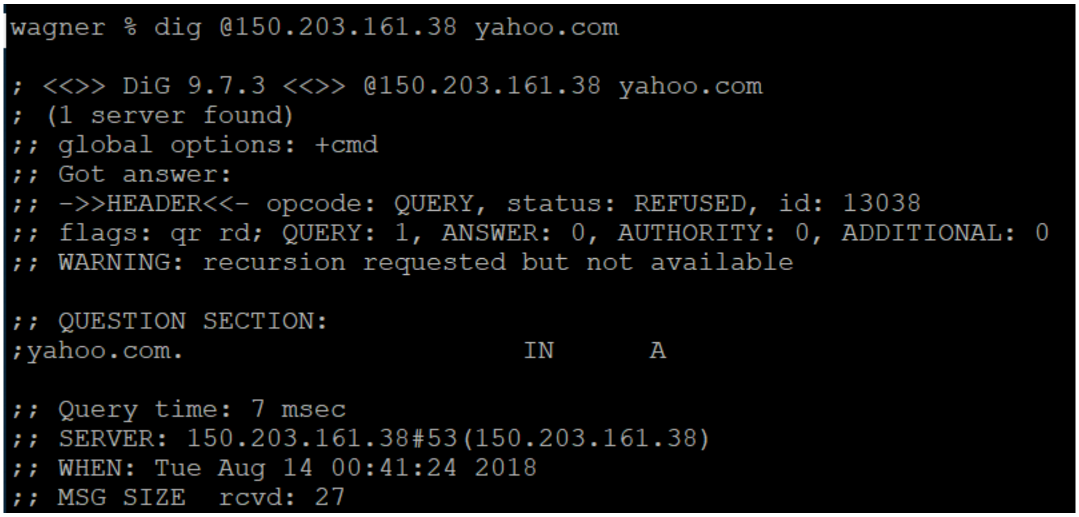
No, I didn't get an authoritative answer because "aa", which means getting authoritative answer does not include in the flag. This is because it does not have authority for the CSE domain.



```
wagner % dig @129.94.242.33 yahoo.com

; <<>> DiG 9.7.3 <<>> @129.94.242.33 yahoo.com
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 27963
;; flags: qr rd ra; QUERY: 1, ANSWER: 6, AUTHORITY: 5, ADDITIONAL: 8

;; QUESTION SECTION:
;yahoo.com.                     IN      A

;; ANSWER SECTION:
yahoo.com.              1800    IN      A       98.138.219.231
yahoo.com.              1800    IN      A       98.138.219.232
yahoo.com.              1800    IN      A       72.30.35.9
yahoo.com.              1800    IN      A       72.30.35.10
yahoo.com.              1800    IN      A       98.137.246.7
yahoo.com.              1800    IN      A       98.137.246.8

;; AUTHORITY SECTION:
yahoo.com.              139159  IN      NS      ns5.yahoo.com.
yahoo.com.              139159  IN      NS      ns1.yahoo.com.
yahoo.com.              139159  IN      NS      ns4.yahoo.com.
yahoo.com.              139159  IN      NS      ns2.yahoo.com.
yahoo.com.              139159  IN      NS      ns3.yahoo.com.

;; ADDITIONAL SECTION:
ns1.yahoo.com.          15239   IN      A       68.180.131.16
ns1.yahoo.com.          43046   IN      AAAA    2001:4998:130::1001
ns2.yahoo.com.          296875  IN      A       68.142.255.16
ns2.yahoo.com.          38777   IN      AAAA    2001:4998:140::1002
ns3.yahoo.com.          58962   IN      A       203.84.221.53
ns3.yahoo.com.          62719   IN      AAAA    2406:8600:b8:fe03::1003
ns4.yahoo.com.          303679  IN      A       98.138.11.157
ns5.yahoo.com.          289750  IN      A       119.160.253.83

;; Query time: 168 msec
;; SERVER: 129.94.242.33#53(129.94.242.33)
;; WHEN: Tue Aug 14 00:33:36 2018
;; MSG SIZE  rcvd: 377
```

Question 8. Repeat the above (i.e. Question 7) but use one of the nameservers obtained in Question 5. What is the result?

I use 150.203.161.38. I didn't get the answer either.

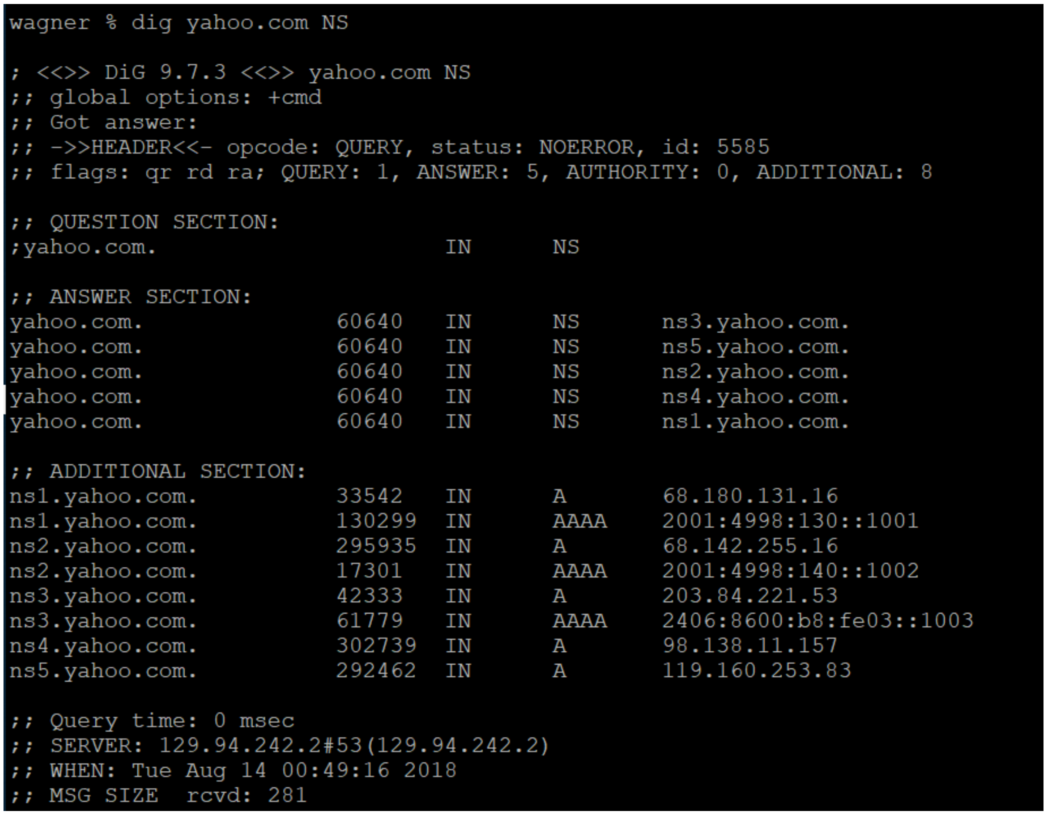


```
wagner % dig @150.203.161.38 yahoo.com

; <<>> DiG 9.7.3 <<>> @150.203.161.38 yahoo.com
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: REFUSED, id: 13038
;; flags: qr rd; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 0
;; WARNING: recursion requested but not available

;; QUESTION SECTION:
;yahoo.com.                     IN      A

;; Query time: 7 msec
;; SERVER: 150.203.161.38#53(150.203.161.38)
;; WHEN: Tue Aug 14 00:41:24 2018
;; MSG SIZE  rcvd: 27
```

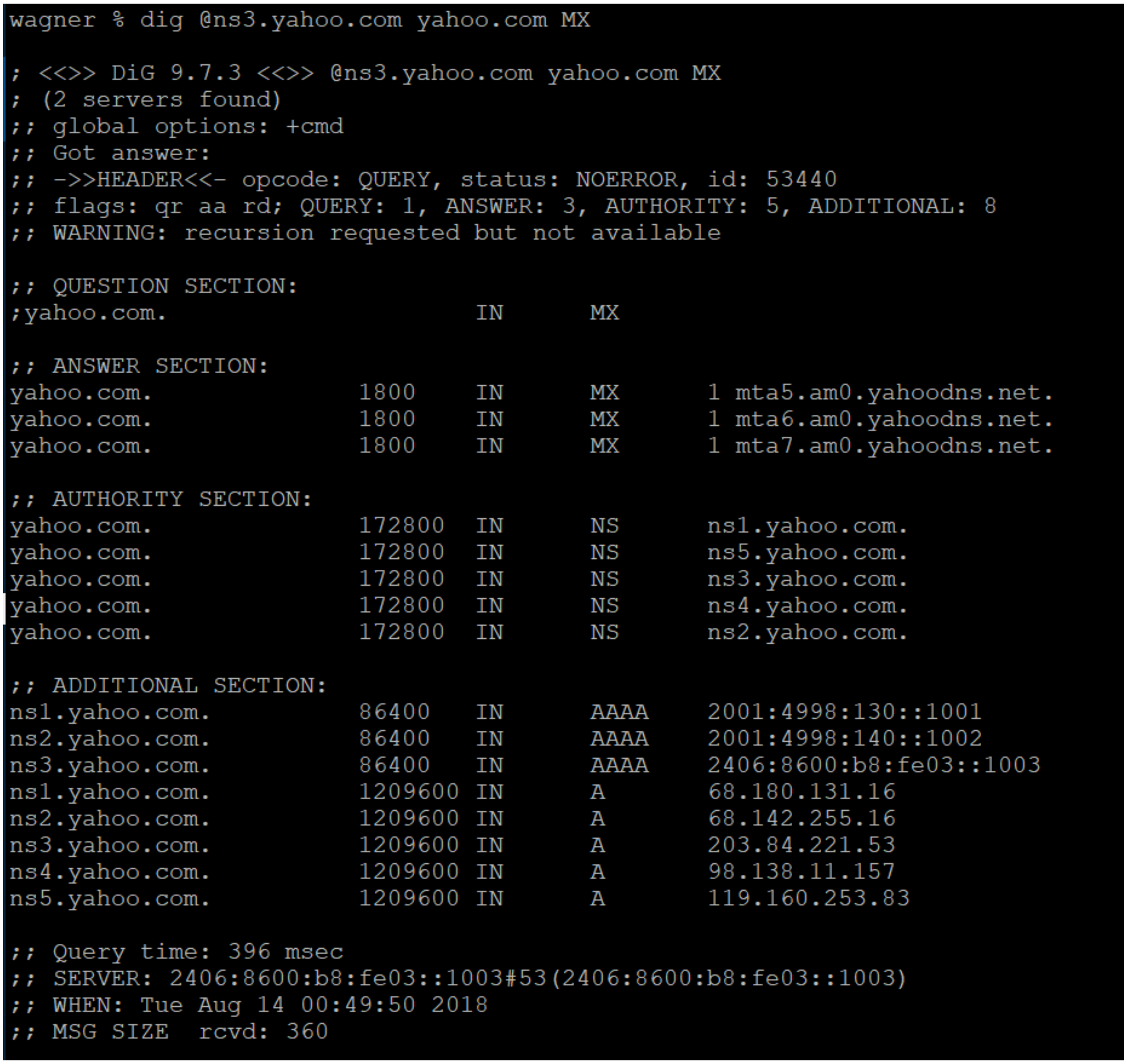
Question 9. Obtain the authoritative answer for the mail servers for Yahoo! mail. What type of DNS query is sent to obtain this information?

First, get the authoritative nameservers for the yahoo.com using NS type.

Then, query one of the authoritative nameservers for yahoo.com using MX type.



```
wagner % dig yahoo.com NS

; <<>> DiG 9.7.3 <<>> yahoo.com NS
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 5585
;; flags: qr rd ra; QUERY: 1, ANSWER: 5, AUTHORITY: 0, ADDITIONAL: 8

;; QUESTION SECTION:
;yahoo.com.                     IN      NS

;; ANSWER SECTION:
yahoo.com.              60640   IN      NS      ns3.yahoo.com.
yahoo.com.              60640   IN      NS      ns5.yahoo.com.
yahoo.com.              60640   IN      NS      ns2.yahoo.com.
yahoo.com.              60640   IN      NS      ns4.yahoo.com.
yahoo.com.              60640   IN      NS      ns1.yahoo.com.

;; ADDITIONAL SECTION:
ns1.yahoo.com.          33542   IN      A       68.180.131.16
ns1.yahoo.com.          130299  IN      AAAA    2001:4998:130::1001
ns2.yahoo.com.          295935  IN      A       68.142.255.16
ns2.yahoo.com.          17301   IN      AAAA    2001:4998:140::1002
ns3.yahoo.com.          42333   IN      A       203.84.221.53
ns3.yahoo.com.          61779   IN      AAAA    2406:8600:b8:fe03::1003
ns4.yahoo.com.          302739  IN      A       98.138.11.157
ns5.yahoo.com.          292462  IN      A       119.160.253.83

;; Query time: 0 msec
;; SERVER: 129.94.242.2#53(129.94.242.2)
;; WHEN: Tue Aug 14 00:49:16 2018
;; MSG SIZE  rcvd: 281
```



```
wagner % dig @ns3.yahoo.com yahoo.com MX

; <<>> DiG 9.7.3 <<>> @ns3.yahoo.com yahoo.com MX
; (2 servers found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 53440
;; flags: qr aa rd; QUERY: 1, ANSWER: 3, AUTHORITY: 5, ADDITIONAL: 8
;; WARNING: recursion requested but not available

;; QUESTION SECTION:
;yahoo.com.                     IN      MX

;; ANSWER SECTION:
yahoo.com.              1800    IN      MX      1 mta5.am0.yahoodns.net.
yahoo.com.              1800    IN      MX      1 mta6.am0.yahoodns.net.
yahoo.com.              1800    IN      MX      1 mta7.am0.yahoodns.net.

;; AUTHORITY SECTION:
yahoo.com.              172800  IN      NS      ns1.yahoo.com.
yahoo.com.              172800  IN      NS      ns5.yahoo.com.
yahoo.com.              172800  IN      NS      ns3.yahoo.com.
yahoo.com.              172800  IN      NS      ns4.yahoo.com.
yahoo.com.              172800  IN      NS      ns2.yahoo.com.

;; ADDITIONAL SECTION:
ns1.yahoo.com.          86400   IN      AAAA    2001:4998:130::1001
ns2.yahoo.com.          86400   IN      AAAA    2001:4998:140::1002
ns3.yahoo.com.          86400   IN      AAAA    2406:8600:b8:fe03::1003
ns1.yahoo.com.          1209600 IN      A       68.180.131.16
ns2.yahoo.com.          1209600 IN      A       68.142.255.16
ns3.yahoo.com.          1209600 IN      A       203.84.221.53
ns4.yahoo.com.          1209600 IN      A       98.138.11.157
ns5.yahoo.com.          1209600 IN      A       119.160.253.83

;; Query time: 396 msec
;; SERVER: 2406:8600:b8:fe03::1003#53(2406:8600:b8:fe03::1003)
;; WHEN: Tue Aug 14 00:49:50 2018
;; MSG SIZE  rcvd: 360
```

Question 10. In this exercise you simulate the iterative DNS query process to find the IP address of your machine (e.g. lyre00.cse.unsw.edu.au).

First, find the name server (query type NS) of the "." domain (root domain).

Query this nameserver to find the authoritative name server for the "au." domain.

Query this second server to find the authoritative nameserver for the "edu.au." domain.

Now query this nameserver to find the authoritative nameserver for "unsw.edu.au".

Next query the nameserver of unsw.edu.au to find the authoritative name server of cse.unsw.edu.au.

Now query the nameserver of cse.unsw.edu.au to find the IP address of your host.

How many DNS servers do you have to query to get the authoritative answer?

I need 6 DNS servers to query to get the authoritative answer.

Ask my local DNS server for root server: dig NS

Ask root for au. DNS server: dig NS au @f.root-servers.net

Ask au. for edu.au DNS server: dig NS edu.au @u.au

Ask edu.au for unsw.edu.au DNS server: dig NS unsw.edu.au @t.au

Ask unsw.edu.au for cse.unsw.edu.au DNS server: dig NS cse.unsw.edu.au @ns3.unsw.edu.au

Ask maestro.orchestra.cse.unsw.edu.au for lyre00.cse.unsw.edu.au: dig NS lyre00.cse.unsw.edu.au @maestro.orchestra.cse.unsw.edu.au

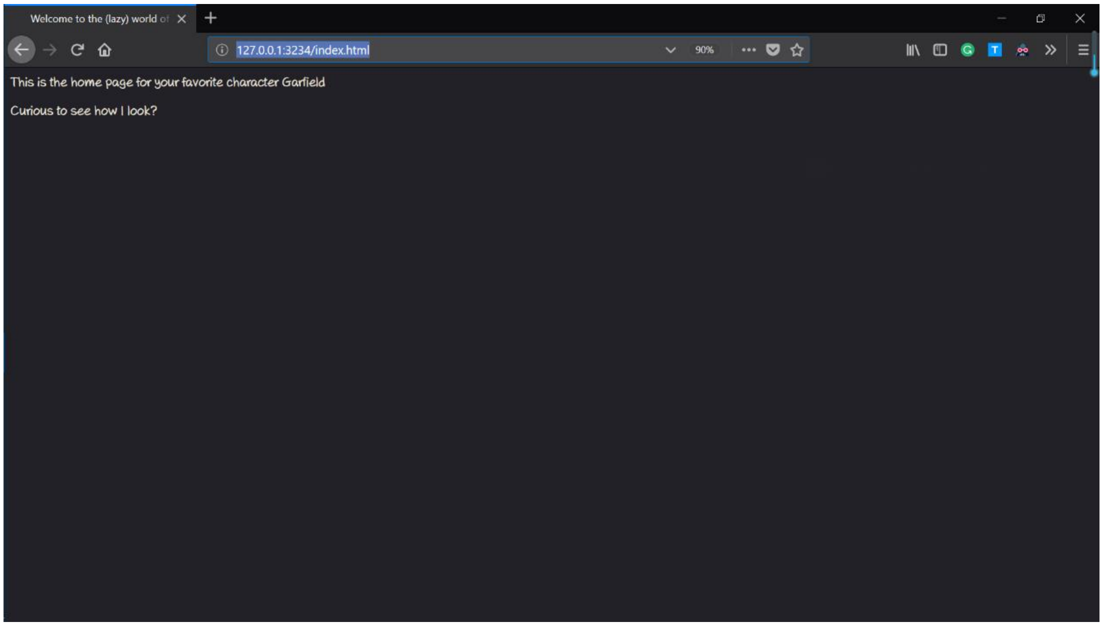
My machine IP address: 129.94.210.20

Question 11. Can one physical machine have several names and/or IP addresses associated with it?

Yes, a machine may have several network interfaces. Moreover, a network interface can have several IP address associated with it at any given time. An IP address may have associated with several names (the additional host names are known as "aliases"). To obtain the canonical name for the machine, use dig with query type=cname.

(*) Exercise 4: (port: 3234)

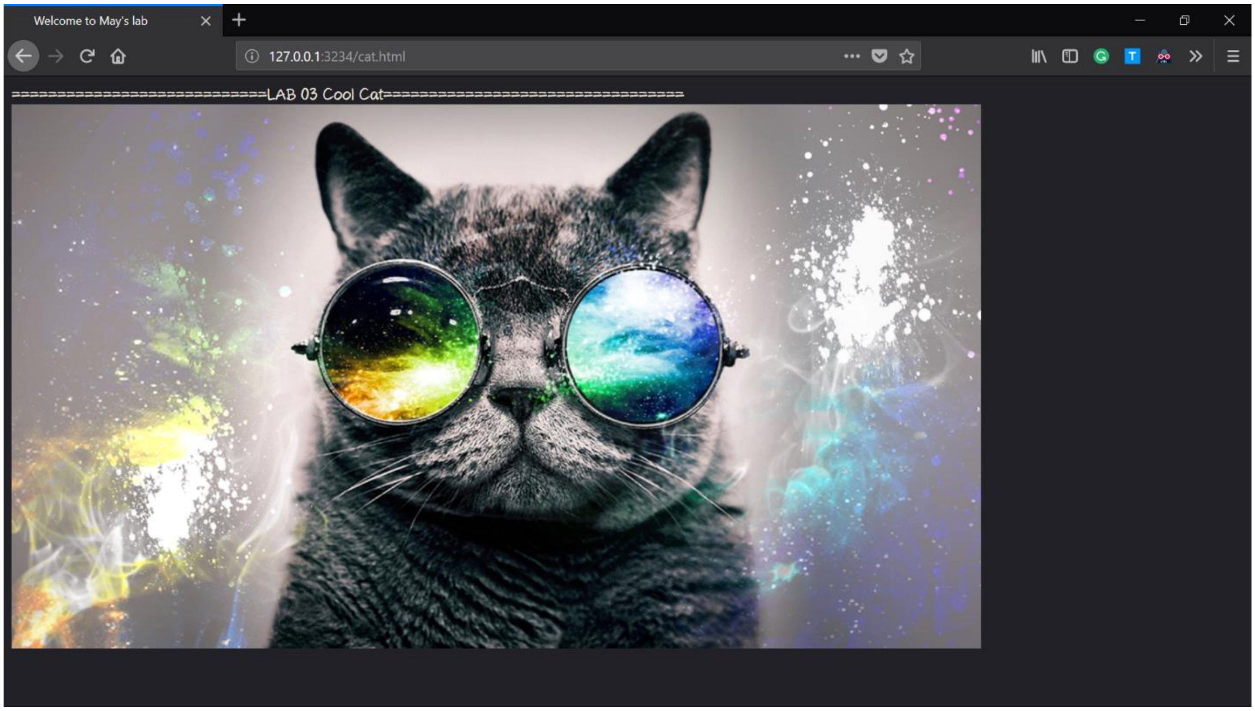
index.html



This is the home page for your favorite character Garfield

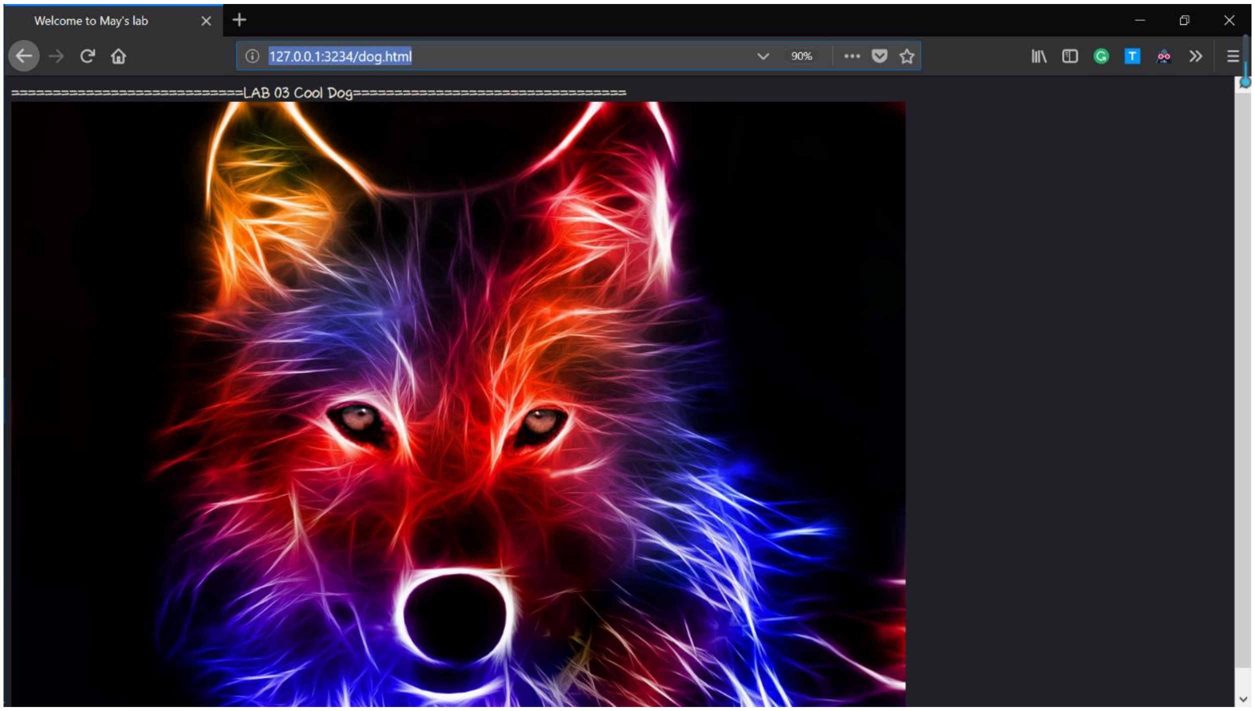
Curious to see how I look?

cat.html:



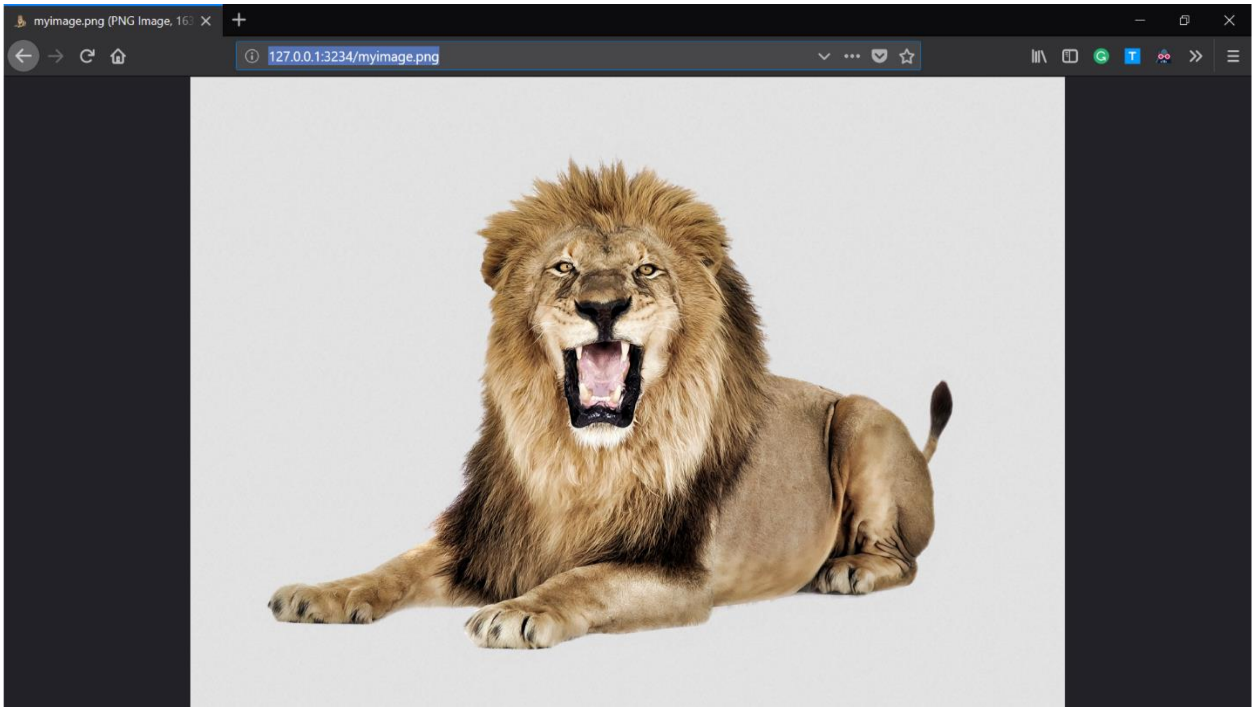
==========================LAB 03 Cool Cat===============================

dog.html:

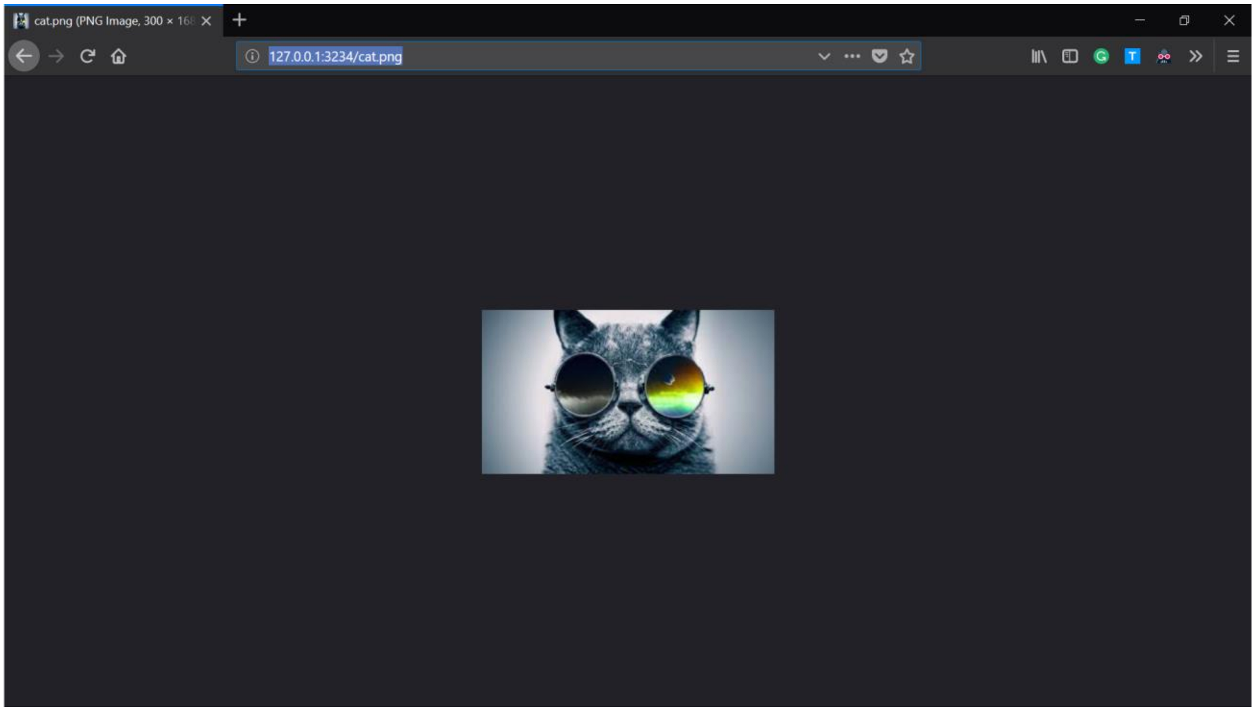


============================LAB 03 Cool Dog=================================

myimage.png:



cat.png:


cat.png (PNG Image, 300 × 16
127.0.0.1:3234/cat.png