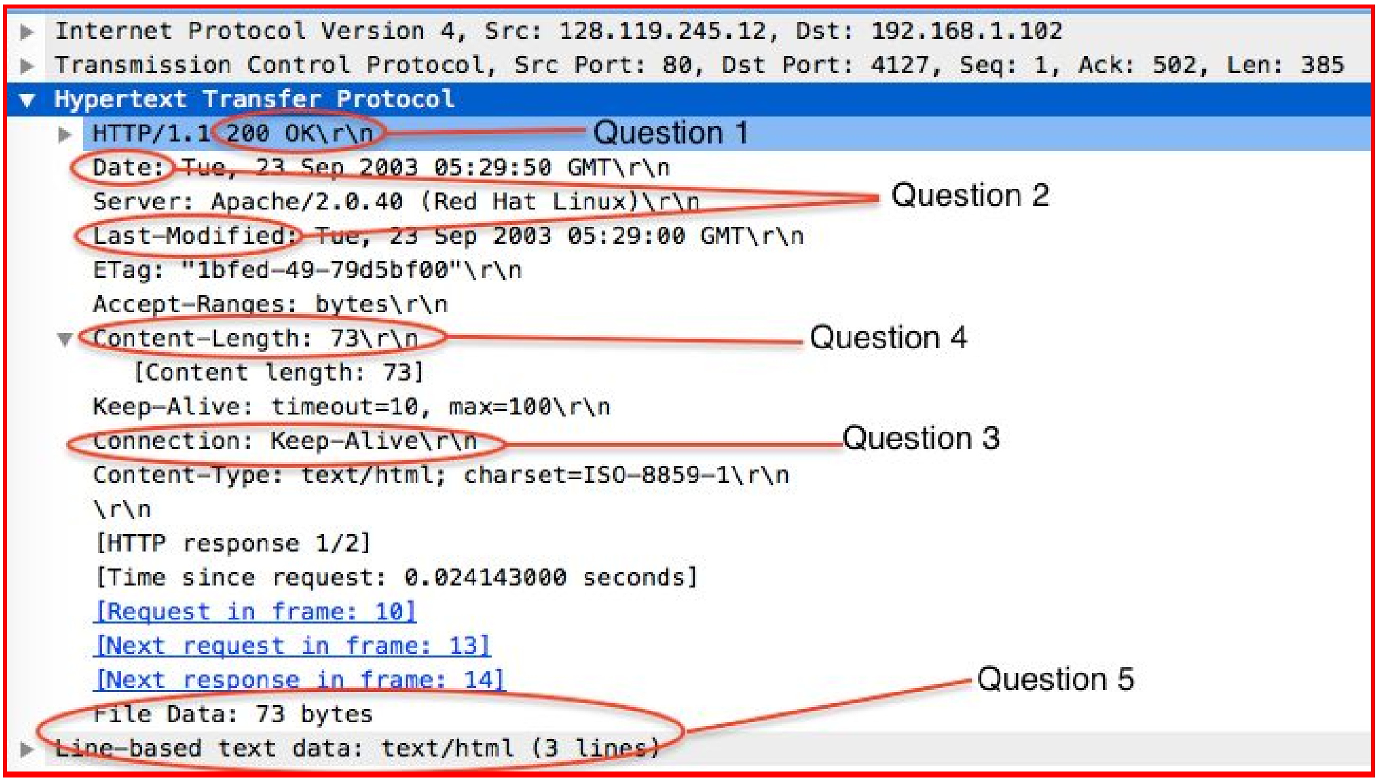
Lab03 - z5119666

Exercise 3: Using Wireshark to understand basic HTTP request/response messages



```
▶ Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.102
▶ Transmission Control Protocol, Src Port: 80, Dst Port: 4127, Seq: 1, Ack: 502, Len: 385
▼ Hypertext Transfer Protocol
  ▶ HTTP/1.1 200 OK\r\n
    Date: Tue, 23 Sep 2003 05:29:50 GMT\r\n
    Server: Apache/2.0.40 (Red Hat Linux)\r\n
    Last-Modified: Tue, 23 Sep 2003 05:29:00 GMT\r\n
    ETag: "1bfed-49-79d5bf00"\r\n
    Accept-Ranges: bytes\r\n
  ▼ Content-Length: 73\r\n
      [Content length: 73]
    Keep-Alive: timeout=10, max=100\r\n
    Connection: Keep-Alive\r\n
    Content-Type: text/html; charset=ISO-8859-1\r\n
    \r\n
    [HTTP response 1/2]
    [Time since request: 0.024143000 seconds]
    [Request in frame: 10]
    [Next request in frame: 13]
    [Next response in frame: 14]
    File Data: 73 bytes
▶ Line-based text data: text/html (3 lines)
```

Question 1: What is the status code and phrase returned from the server to the client browser?

Ans: It is “200 OK”. Standard response to successful HTTP requests. Since the response contains an entity corresponding to the GET request.

Question 2: When was the HTML file that the browser is retrieving last modified at the server? Does the response also contain a DATE header? How are these two fields different?

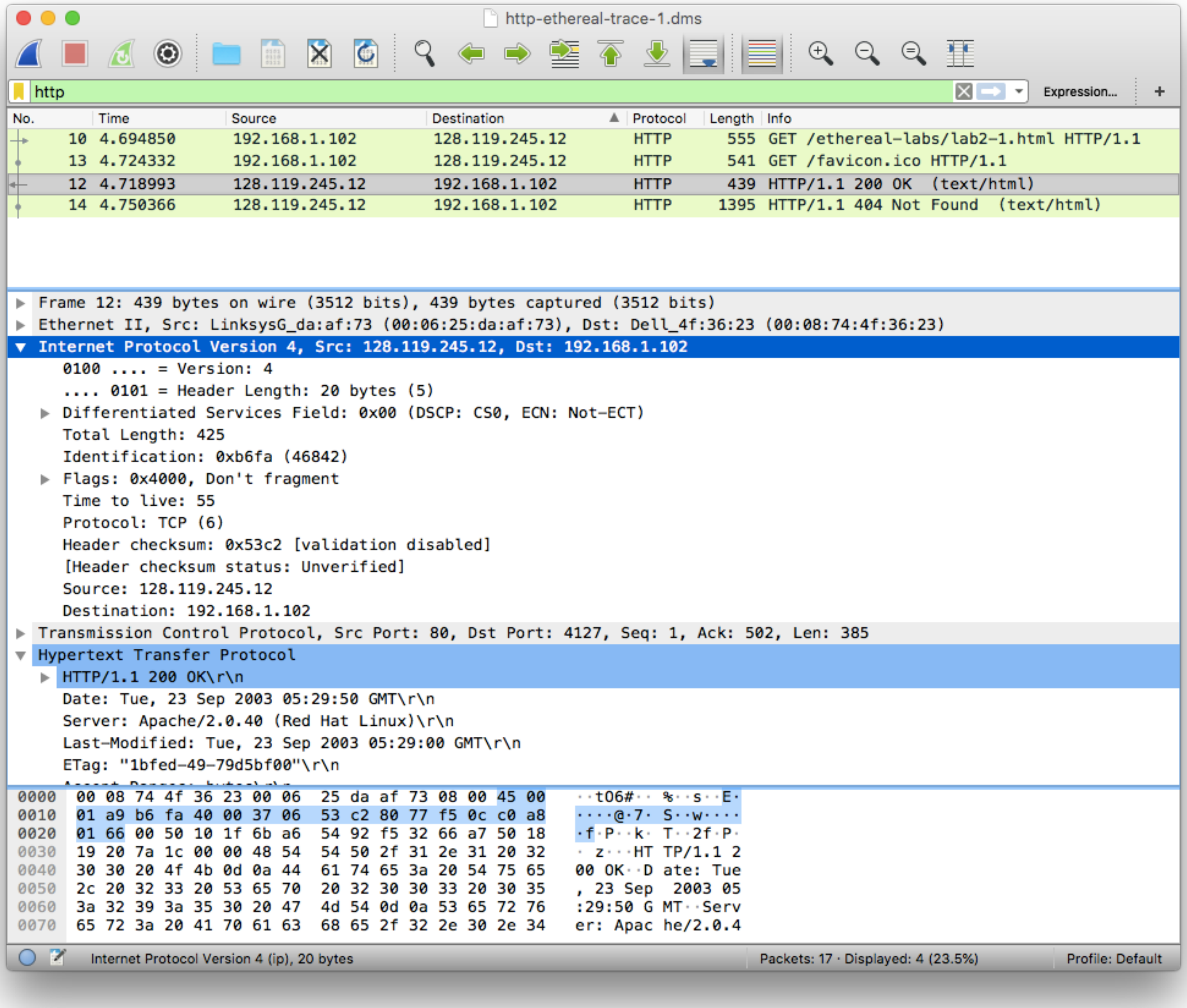
Ans: Last-Modified: Tue, 23 Sep 2003 05:29:00 GMT\r\n

The response also contains a DATE header. Date: Tue, 23 Sep 2003 05:29:50 GMT\r\n

According to the screenshots below the table:

Different	Request	Response
Frame Number	10	12
Frame Length	555 bytes	439 bytes
Total Length	541	425
Identification	0x01cd	0xb6fa

Source	192.168.1.102	128.119.245.12
Source Port	4127	80
Destination	128.119.245.12	192.168.1.102
Destination Port	80	4127
TCP Payload	501 bytes	385 bytes
Protocol	GET	HTTP/1.1

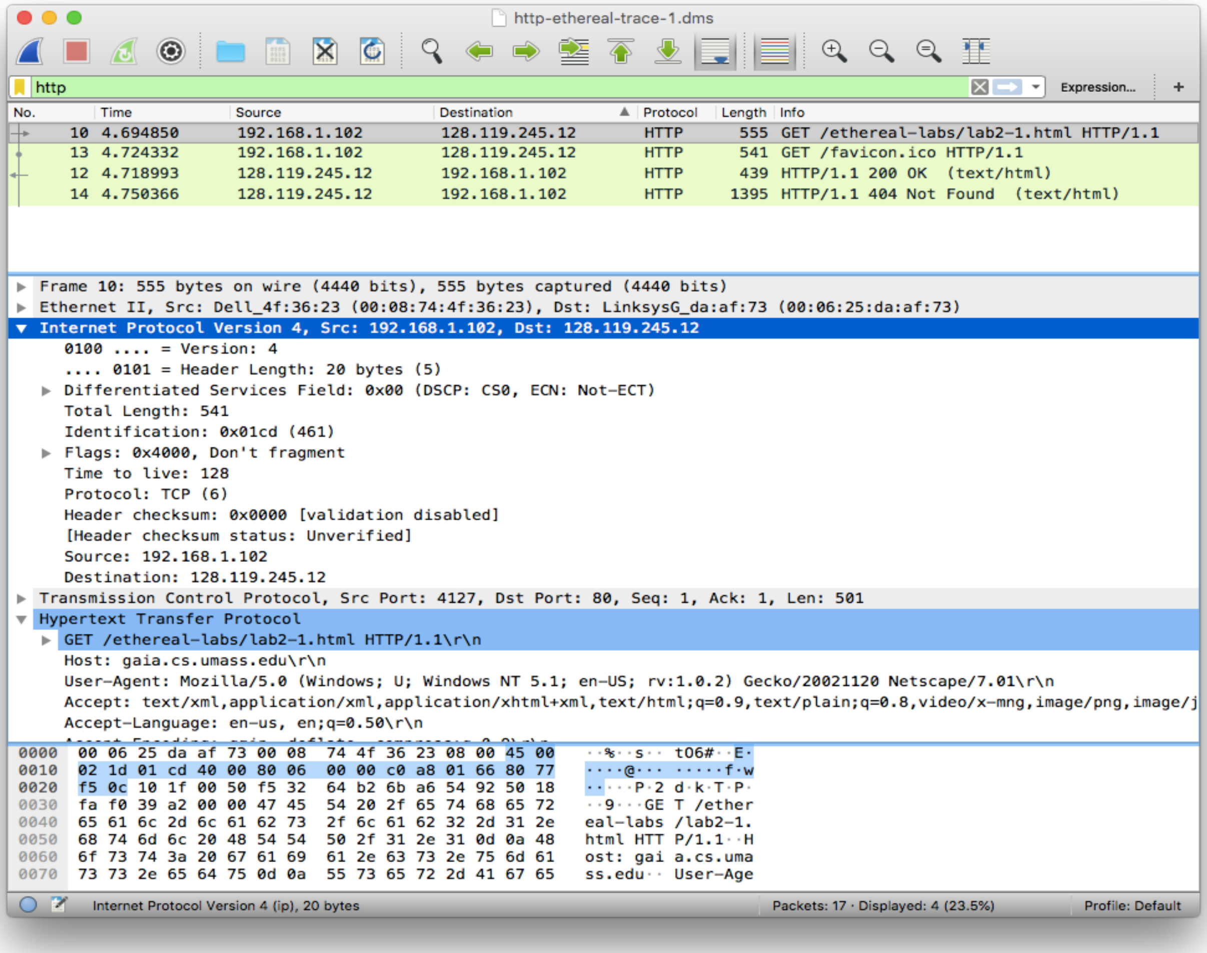


```
No.   Time      Source          Destination     Protocol Length Info
   10 4.694850  192.168.1.102   128.119.245.12  HTTP      555 GET /ethereal-labs/lab2-1.html HTTP/1.1
   13 4.724332  192.168.1.102   128.119.245.12  HTTP      541 GET /favicon.ico HTTP/1.1
   12 4.718993  128.119.245.12  192.168.1.102   HTTP      439 HTTP/1.1 200 OK  (text/html)
   14 4.750366  128.119.245.12  192.168.1.102   HTTP     1395 HTTP/1.1 404 Not Found  (text/html)
```

```
▶ Frame 12: 439 bytes on wire (3512 bits), 439 bytes captured (3512 bits)
▶ Ethernet II, Src: LinksysG_da:af:73 (00:06:25:da:af:73), Dst: Dell_4f:36:23 (00:08:74:4f:36:23)
▼ Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.102
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▶ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 425
    Identification: 0xb6fa (46842)
  ▶ Flags: 0x4000, Don't fragment
    Time to live: 55
    Protocol: TCP (6)
    Header checksum: 0x53c2 [validation disabled]
    [Header checksum status: Unverified]
    Source: 128.119.245.12
    Destination: 192.168.1.102
▶ Transmission Control Protocol, Src Port: 80, Dst Port: 4127, Seq: 1, Ack: 502, Len: 385
▼ Hypertext Transfer Protocol
  ▶ HTTP/1.1 200 OK\r\n
    Date: Tue, 23 Sep 2003 05:29:50 GMT\r\n
    Server: Apache/2.0.40 (Red Hat Linux)\r\n
    Last-Modified: Tue, 23 Sep 2003 05:29:00 GMT\r\n
    ETag: "1bfed-49-79d5bf00"\r\n
```

```
0000  00 08 74 4f 36 23 00 06  25 da af 73 08 00 45 00   ··tO6#·· %··s··E·
0010  01 a9 b6 fa 40 00 37 06  53 c2 80 77 f5 0c c0 a8   ····@·7· S··w····
0020  01 66 00 50 10 1f 6b a6  54 92 f5 32 66 a7 50 18   ·f·P··k· T··2f·P·
0030  19 20 7a 1c 00 00 48 54  54 50 2f 31 2e 31 20 32   · z···HT TP/1.1 2
0040  30 30 20 4f 4b 0d 0a 44  61 74 65 3a 20 54 75 65   00 OK··D ate: Tue
0050  2c 20 32 33 20 53 65 70  20 32 30 30 33 20 30 35   , 23 Sep  2003 05
0060  3a 32 39 3a 35 30 20 47  4d 54 0d 0a 53 65 72 76   :29:50 G MT··Serv
0070  65 72 3a 20 41 70 61 63  68 65 2f 32 2e 30 2e 34   er: Apac he/2.0.4
```

Internet Protocol Version 4 (ip), 20 bytes   Packets: 17 · Displayed: 4 (23.5%)   Profile: Default



```
No.   Time        Source          Destination     Protocol Length Info
   10 4.694850    192.168.1.102   128.119.245.12  HTTP      555  GET /ethereal-labs/lab2-1.html HTTP/1.1
   13 4.724332    192.168.1.102   128.119.245.12  HTTP      541  GET /favicon.ico HTTP/1.1
   12 4.718993    128.119.245.12  192.168.1.102   HTTP      439  HTTP/1.1 200 OK  (text/html)
   14 4.750366    128.119.245.12  192.168.1.102   HTTP     1395  HTTP/1.1 404 Not Found  (text/html)
```

```
▶ Frame 10: 555 bytes on wire (4440 bits), 555 bytes captured (4440 bits)
▶ Ethernet II, Src: Dell_4f:36:23 (00:08:74:4f:36:23), Dst: LinksysG_da:af:73 (00:06:25:da:af:73)
▼ Internet Protocol Version 4, Src: 192.168.1.102, Dst: 128.119.245.12
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▶ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 541
    Identification: 0x01cd (461)
  ▶ Flags: 0x4000, Don't fragment
    Time to live: 128
    Protocol: TCP (6)
    Header checksum: 0x0000 [validation disabled]
    [Header checksum status: Unverified]
    Source: 192.168.1.102
    Destination: 128.119.245.12
▶ Transmission Control Protocol, Src Port: 4127, Dst Port: 80, Seq: 1, Ack: 1, Len: 501
▼ Hypertext Transfer Protocol
  ▶ GET /ethereal-labs/lab2-1.html HTTP/1.1\r\n
    Host: gaia.cs.umass.edu\r\n
    User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.0.2) Gecko/20021120 Netscape/7.01\r\n
    Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,video/x-mng,image/png,image/j
    Accept-Language: en-us, en;q=0.50\r\n
```

```
0000  00 06 25 da af 73 00 08  74 4f 36 23 08 00 45 00   ··%··s·· tO6#··E·
0010  02 1d 01 cd 40 00 80 06  00 00 c0 a8 01 66 80 77   ····@··· ·····f·w
0020  f5 0c 10 1f 00 50 f5 32  64 b2 6b a6 54 92 50 18   ·····P·2 d·k·T·P·
0030  fa f0 39 a2 00 00 47 45  54 20 2f 65 74 68 65 72   ··9···GE T /ether
0040  65 61 6c 2d 6c 61 62 73  2f 6c 61 62 32 2d 31 2e   eal-labs /lab2-1.
0050  68 74 6d 6c 20 48 54 54  50 2f 31 2e 31 0d 0a 48   html HTT P/1.1··H
0060  6f 73 74 3a 20 67 61 69  61 2e 63 73 2e 75 6d 61   ost: gai a.cs.uma
0070  73 73 2e 65 64 75 0d 0a  55 73 65 72 2d 41 67 65   ss.edu·· User-Age
```

Internet Protocol Version 4 (ip), 20 bytes   Packets: 17 · Displayed: 4 (23.5%)   Profile: Default

Question 3: Is the connection established between the browser and the server persistent or non-persistent? How can you infer this?

Ans: The connection is persistent, since It contains “Connection: keep-alive” header. In HTTP/1.1 the connection is persistent by default unless we add the “Connection: close” header to the http request. In which case the server has to close the connection the requested object has been sent.

Question 4: How many bytes of content are being returned to the browser?

Ans: Content-Length: 73

Question 5: What is the data contained inside the HTTP response packet?

Ans: File Data: 73 bytes. File(html).

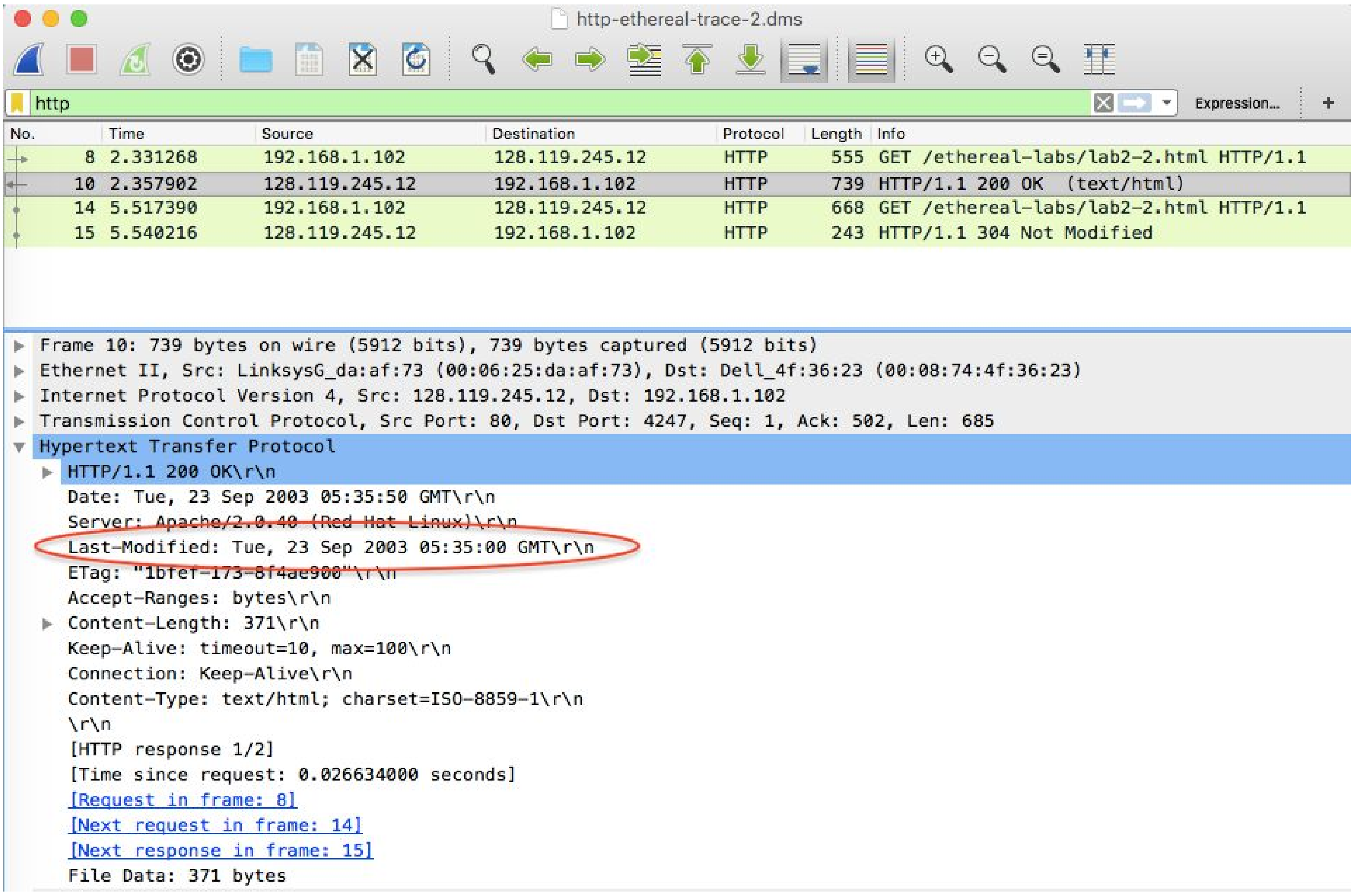
Exercise 4: Using Wireshark to understand the HTTP CONDITIONAL GET/response interaction

Question 1: Inspect the contents of the first HTTP GET request from the browser to the server. Do you see an “IF-MODIFIED-SINCE” line in the HTTP GET?

Ans: No, I do not see this line.

Question 2: Does the response indicate the last time that the requested file was modified?

Ans: Last-Modified: Tue, 23 Sep 2003 05:35:00 GMT\r\n



```
No.   Time       Source          Destination     Protocol  Length  Info
  8   2.331268   192.168.1.102   128.119.245.12  HTTP         555  GET /ethereal-labs/lab2-2.html HTTP/1.1
 10   2.357902   128.119.245.12  192.168.1.102   HTTP         739  HTTP/1.1 200 OK  (text/html)
 14   5.517390   192.168.1.102   128.119.245.12  HTTP         668  GET /ethereal-labs/lab2-2.html HTTP/1.1
 15   5.540216   128.119.245.12  192.168.1.102   HTTP         243  HTTP/1.1 304 Not Modified
```

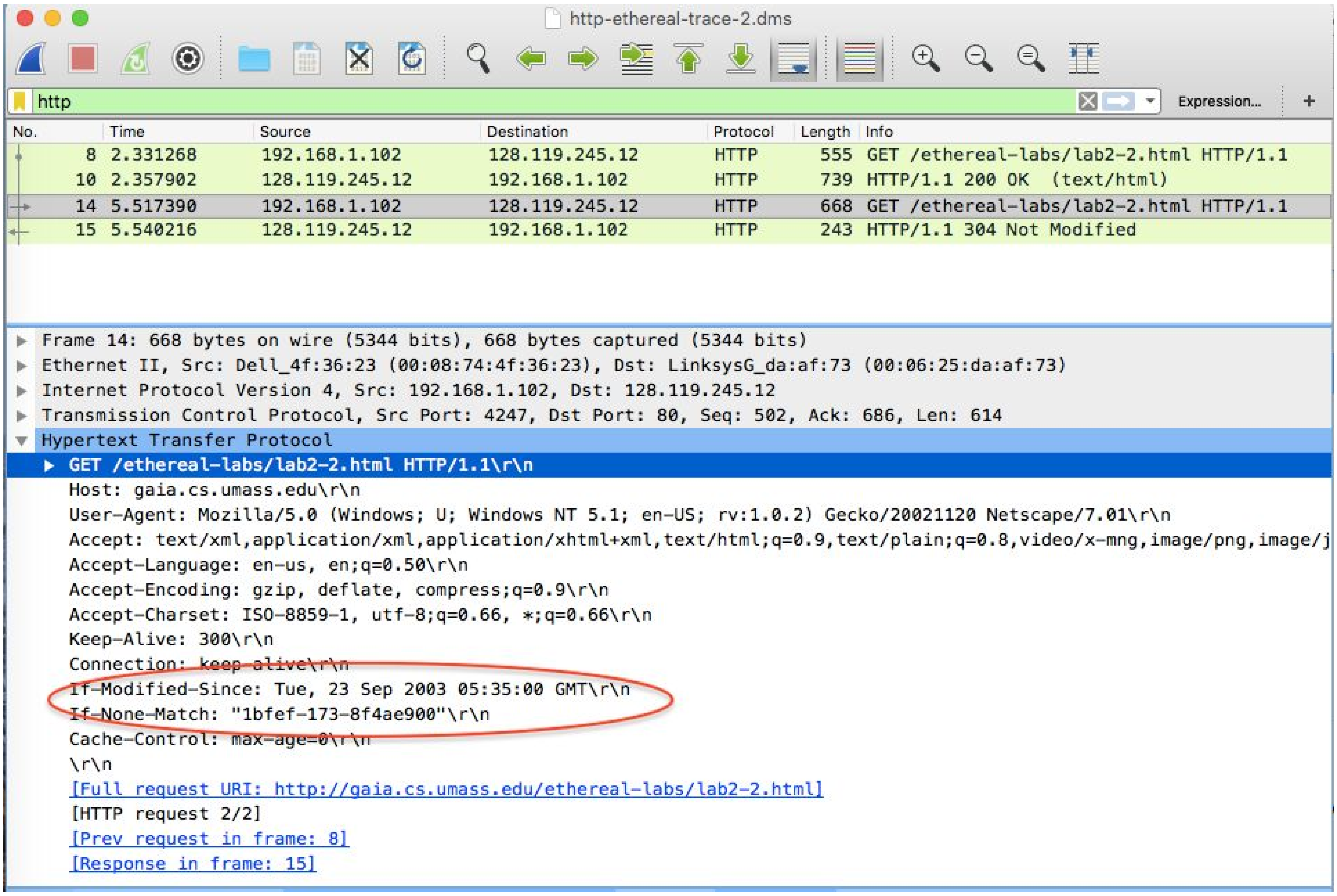
```
▶ Frame 10: 739 bytes on wire (5912 bits), 739 bytes captured (5912 bits)
▶ Ethernet II, Src: LinksysG_da:af:73 (00:06:25:da:af:73), Dst: Dell_4f:36:23 (00:08:74:4f:36:23)
▶ Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.102
▶ Transmission Control Protocol, Src Port: 80, Dst Port: 4247, Seq: 1, Ack: 502, Len: 685
▼ Hypertext Transfer Protocol
  ▶ HTTP/1.1 200 OK\r\n
    Date: Tue, 23 Sep 2003 05:35:50 GMT\r\n
    Server: Apache/2.0.40 (Red Hat Linux)\r\n
    Last-Modified: Tue, 23 Sep 2003 05:35:00 GMT\r\n
    ETag: "1bfef-173-8f4ae900"\r\n
    Accept-Ranges: bytes\r\n
  ▶ Content-Length: 371\r\n
    Keep-Alive: timeout=10, max=100\r\n
    Connection: Keep-Alive\r\n
    Content-Type: text/html; charset=ISO-8859-1\r\n
    \r\n
    [HTTP response 1/2]
    [Time since request: 0.026634000 seconds]
    [Request in frame: 8]
    [Next request in frame: 14]
    [Next response in frame: 15]
    File Data: 371 bytes
```

Question 3: Now inspect the contents of the second HTTP GET request from the browser to the server. Do you see an “IF-MODIFIED-SINCE:” and “IF-NONE-MATCH” lines in the HTTP GET? If so, what information is contained in these header lines?

Ans:

IF-MODIFIED-SINCE: Tue, 23 Sep 2003 05:35:00 GMT\r\n

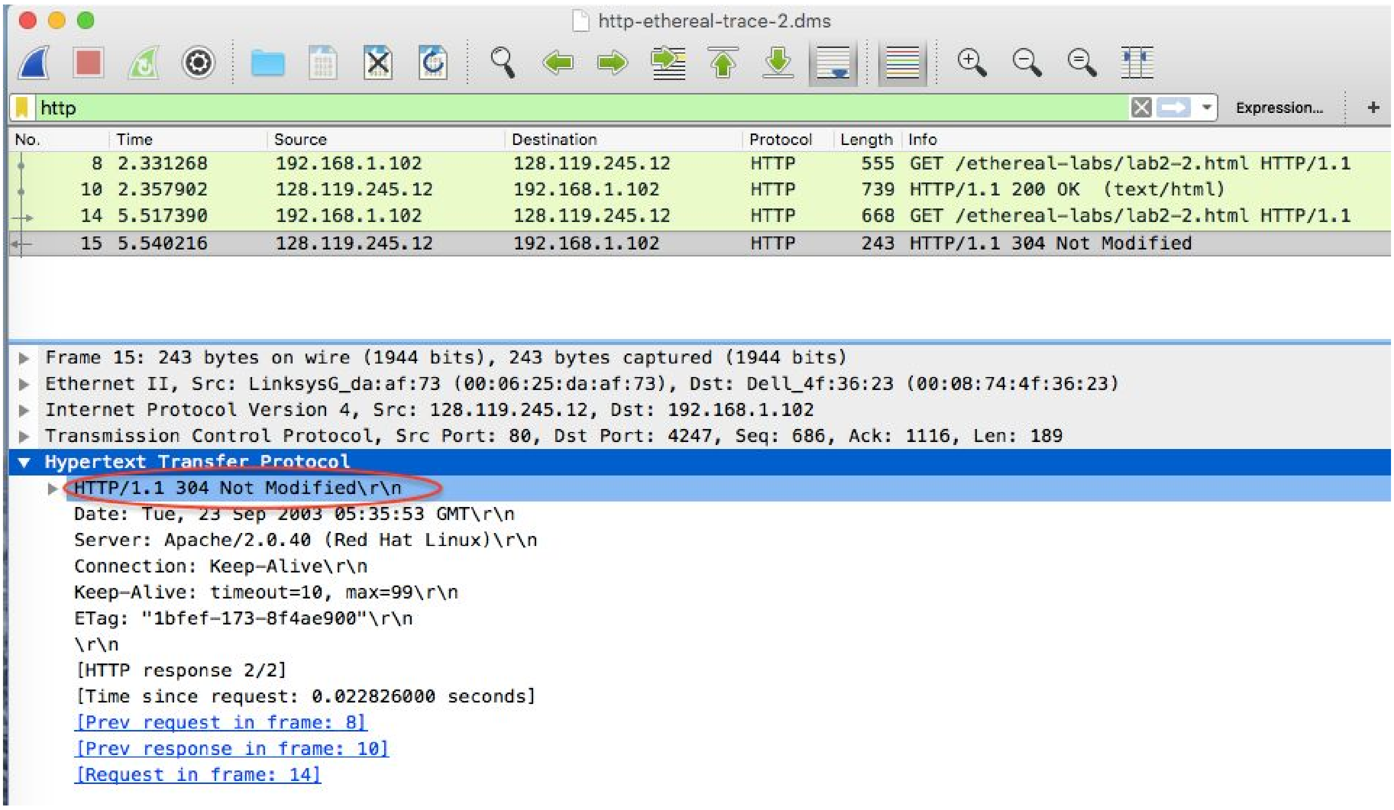
IF-NONE-MATCH: “1bfef-173-8f4ae900”\r\n



```
No.   Time      Source          Destination     Protocol Length Info
    8 2.331268  192.168.1.102   128.119.245.12  HTTP      555  GET /ethereal-labs/lab2-2.html HTTP/1.1
   10 2.357902  128.119.245.12  192.168.1.102   HTTP      739  HTTP/1.1 200 OK  (text/html)
   14 5.517390  192.168.1.102   128.119.245.12  HTTP      668  GET /ethereal-labs/lab2-2.html HTTP/1.1
   15 5.540216  128.119.245.12  192.168.1.102   HTTP      243  HTTP/1.1 304 Not Modified

▶ Frame 14: 668 bytes on wire (5344 bits), 668 bytes captured (5344 bits)
▶ Ethernet II, Src: Dell_4f:36:23 (00:08:74:4f:36:23), Dst: LinksysG_da:af:73 (00:06:25:da:af:73)
▶ Internet Protocol Version 4, Src: 192.168.1.102, Dst: 128.119.245.12
▶ Transmission Control Protocol, Src Port: 4247, Dst Port: 80, Seq: 502, Ack: 686, Len: 614
▼ Hypertext Transfer Protocol
  ▶ GET /ethereal-labs/lab2-2.html HTTP/1.1\r\n
    Host: gaia.cs.umass.edu\r\n
    User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.0.2) Gecko/20021120 Netscape/7.01\r\n
    Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,video/x-mng,image/png,image/j
    Accept-Language: en-us, en;q=0.50\r\n
    Accept-Encoding: gzip, deflate, compress;q=0.9\r\n
    Accept-Charset: ISO-8859-1, utf-8;q=0.66, *;q=0.66\r\n
    Keep-Alive: 300\r\n
    Connection: keep-alive\r\n
    If-Modified-Since: Tue, 23 Sep 2003 05:35:00 GMT\r\n
    If-None-Match: "1bfef-173-8f4ae900"\r\n
    Cache-Control: max-age=0\r\n
    \r\n
    [Full request URI: http://gaia.cs.umass.edu/ethereal-labs/lab2-2.html]
    [HTTP request 2/2]
    [Prev request in frame: 8]
    [Response in frame: 15]
```

Question 4: What is the HTTP status code and phrase returned from the server in response to this second HTTP GET? Did the server explicitly return the contents of the file? Explain.

304 Not Modified. Indicates that the resource has not been modified since the version specified by the request headers IF-MODIFIED-SINCE or IF-NONE-MATCH. In such case, there is no need to retransmit the resource since the client still has a previously-downloaded co

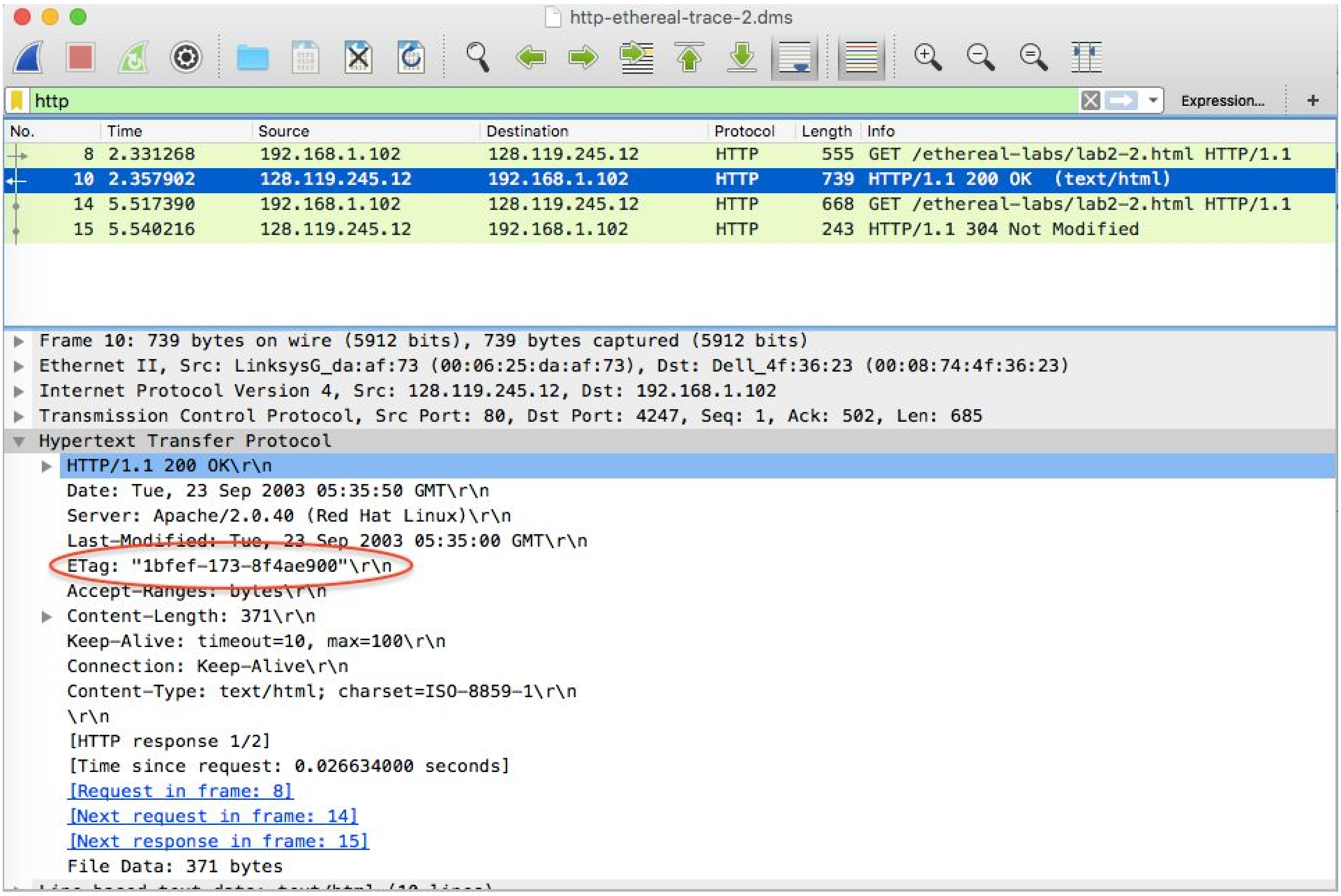


```
No.   Time      Source          Destination     Protocol Length Info
    8 2.331268  192.168.1.102   128.119.245.12  HTTP      555  GET /ethereal-labs/lab2-2.html HTTP/1.1
   10 2.357902  128.119.245.12  192.168.1.102   HTTP      739  HTTP/1.1 200 OK  (text/html)
   14 5.517390  192.168.1.102   128.119.245.12  HTTP      668  GET /ethereal-labs/lab2-2.html HTTP/1.1
   15 5.540216  128.119.245.12  192.168.1.102   HTTP      243  HTTP/1.1 304 Not Modified

▶ Frame 15: 243 bytes on wire (1944 bits), 243 bytes captured (1944 bits)
▶ Ethernet II, Src: LinksysG_da:af:73 (00:06:25:da:af:73), Dst: Dell_4f:36:23 (00:08:74:4f:36:23)
▶ Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.102
▶ Transmission Control Protocol, Src Port: 80, Dst Port: 4247, Seq: 686, Ack: 1116, Len: 189
▼ Hypertext Transfer Protocol
  ▶ HTTP/1.1 304 Not Modified\r\n
    Date: Tue, 23 Sep 2003 05:35:53 GMT\r\n
    Server: Apache/2.0.40 (Red Hat Linux)\r\n
    Connection: Keep-Alive\r\n
    Keep-Alive: timeout=10, max=99\r\n
    ETag: "1bfef-173-8f4ae900"\r\n
    \r\n
    [HTTP response 2/2]
    [Time since request: 0.022826000 seconds]
    [Prev request in frame: 8]
    [Prev response in frame: 10]
    [Request in frame: 14]
```

Question 5: What is the value of the Etag field in the 2nd response message and how it is used? Has this value changed since the 1st response message was received?

Value: 1bfef-173-8f4ae900

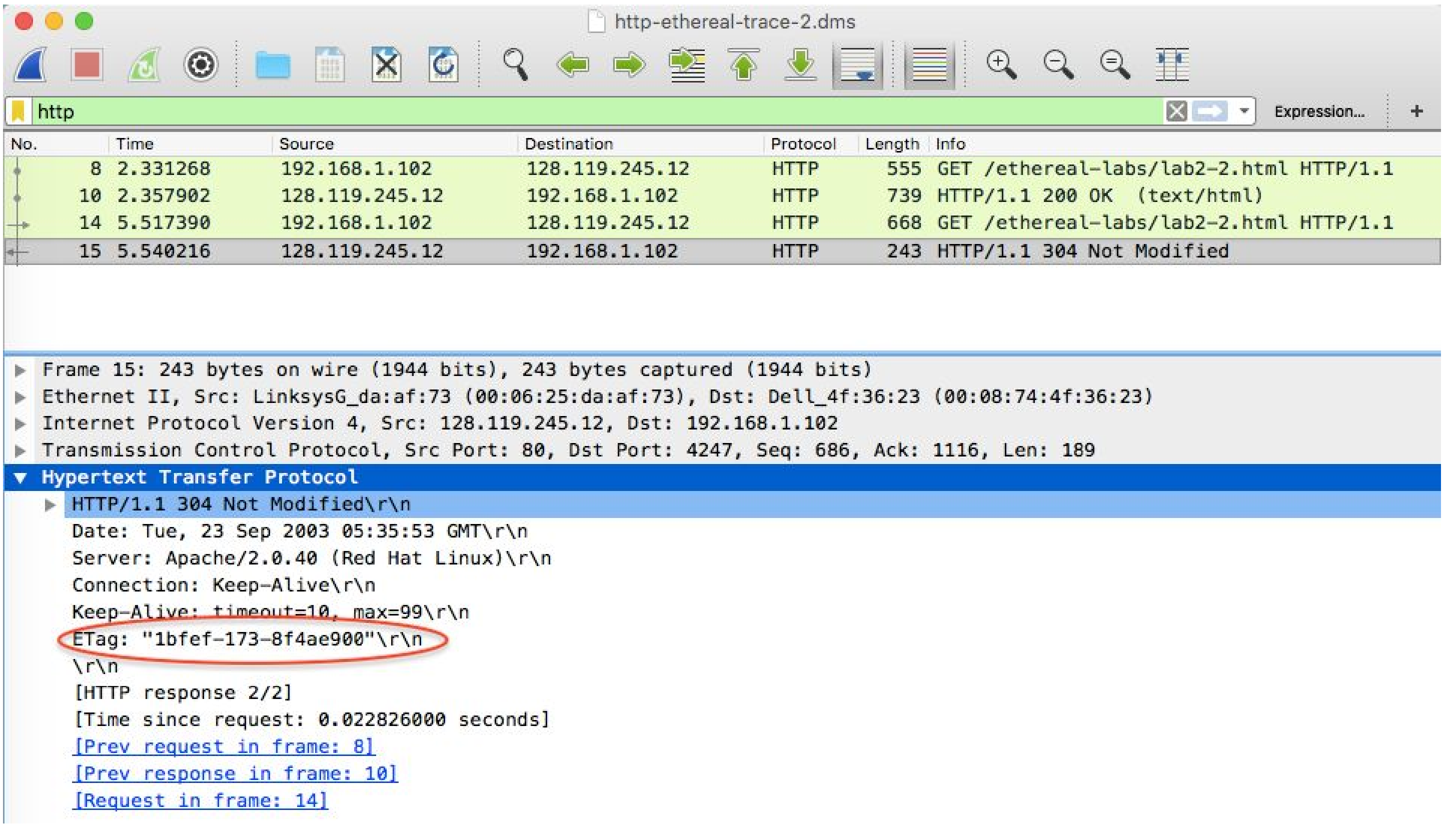
This value has not changed.



http-ethereal-trace-2.dms

```
No.  Time       Source          Destination     Protocol  Length  Info
  8  2.331268   192.168.1.102   128.119.245.12  HTTP      555     GET /ethereal-labs/lab2-2.html HTTP/1.1
 10  2.357902   128.119.245.12  192.168.1.102   HTTP      739     HTTP/1.1 200 OK  (text/html)
 14  5.517390   192.168.1.102   128.119.245.12  HTTP      668     GET /ethereal-labs/lab2-2.html HTTP/1.1
 15  5.540216   128.119.245.12  192.168.1.102   HTTP      243     HTTP/1.1 304 Not Modified
```

```
▶ Frame 10: 739 bytes on wire (5912 bits), 739 bytes captured (5912 bits)
▶ Ethernet II, Src: LinksysG_da:af:73 (00:06:25:da:af:73), Dst: Dell_4f:36:23 (00:08:74:4f:36:23)
▶ Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.102
▶ Transmission Control Protocol, Src Port: 80, Dst Port: 4247, Seq: 1, Ack: 502, Len: 685
▼ Hypertext Transfer Protocol
  ▶ HTTP/1.1 200 OK\r\n
    Date: Tue, 23 Sep 2003 05:35:50 GMT\r\n
    Server: Apache/2.0.40 (Red Hat Linux)\r\n
    Last-Modified: Tue, 23 Sep 2003 05:35:00 GMT\r\n
    ETag: "1bfef-173-8f4ae900"\r\n
    Accept-Ranges: bytes\r\n
  ▶ Content-Length: 371\r\n
    Keep-Alive: timeout=10, max=100\r\n
    Connection: Keep-Alive\r\n
    Content-Type: text/html; charset=ISO-8859-1\r\n
    \r\n
    [HTTP response 1/2]
    [Time since request: 0.026634000 seconds]
    [Request in frame: 8]
    [Next request in frame: 14]
    [Next response in frame: 15]
    File Data: 371 bytes
▶ Line-based text data: text/html (10 lines)
```



http-ethereal-trace-2.dms

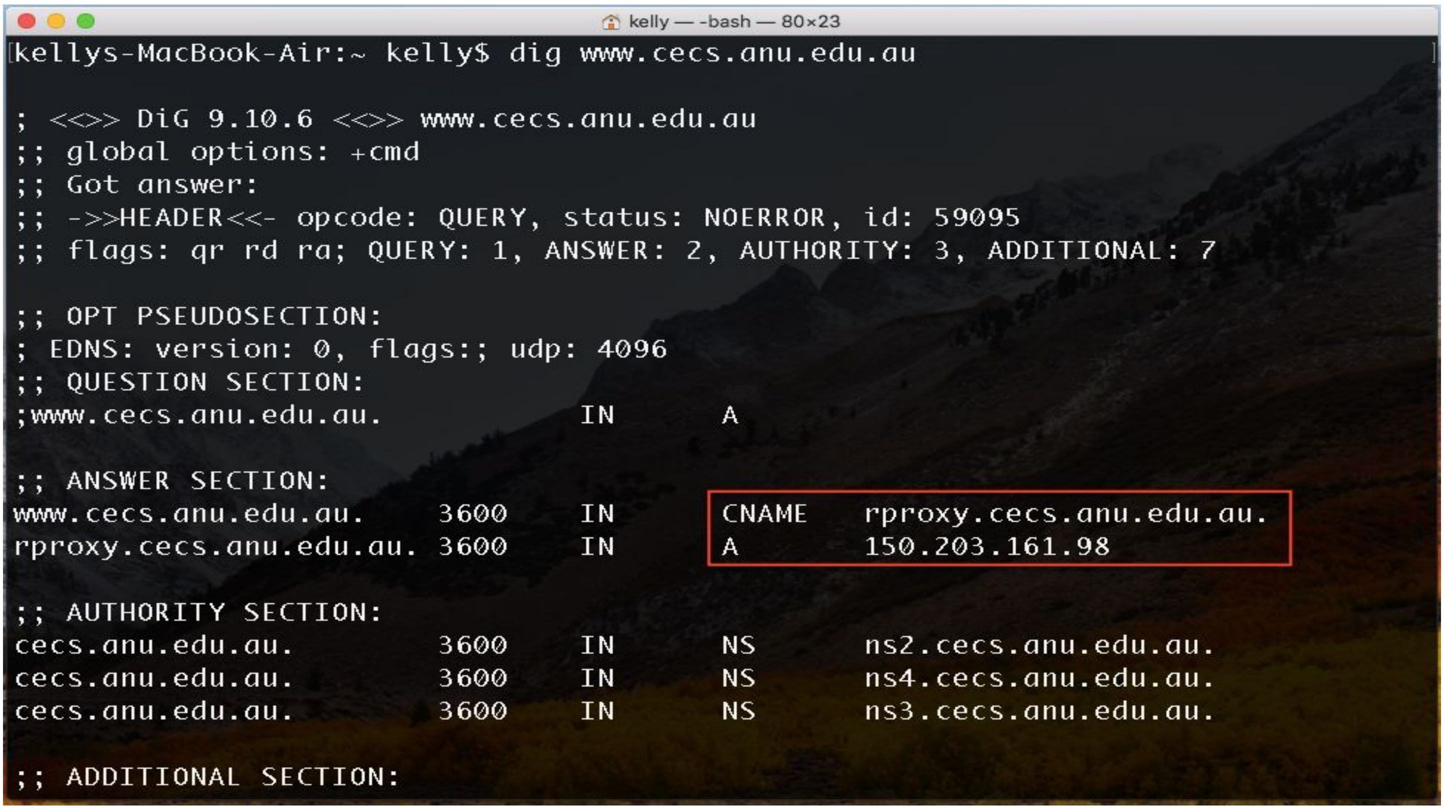
```
No.  Time       Source          Destination     Protocol  Length  Info
  8  2.331268   192.168.1.102   128.119.245.12  HTTP      555     GET /ethereal-labs/lab2-2.html HTTP/1.1
 10  2.357902   128.119.245.12  192.168.1.102   HTTP      739     HTTP/1.1 200 OK  (text/html)
 14  5.517390   192.168.1.102   128.119.245.12  HTTP      668     GET /ethereal-labs/lab2-2.html HTTP/1.1
 15  5.540216   128.119.245.12  192.168.1.102   HTTP      243     HTTP/1.1 304 Not Modified
```

```
▶ Frame 15: 243 bytes on wire (1944 bits), 243 bytes captured (1944 bits)
▶ Ethernet II, Src: LinksysG_da:af:73 (00:06:25:da:af:73), Dst: Dell_4f:36:23 (00:08:74:4f:36:23)
▶ Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.102
▶ Transmission Control Protocol, Src Port: 80, Dst Port: 4247, Seq: 686, Ack: 1116, Len: 189
▼ Hypertext Transfer Protocol
  ▶ HTTP/1.1 304 Not Modified\r\n
    Date: Tue, 23 Sep 2003 05:35:53 GMT\r\n
    Server: Apache/2.0.40 (Red Hat Linux)\r\n
    Connection: Keep-Alive\r\n
    Keep-Alive: timeout=10, max=99\r\n
    ETag: "1bfef-173-8f4ae900"\r\n
    \r\n
    [HTTP response 2/2]
    [Time since request: 0.022826000 seconds]
    [Prev request in frame: 8]
    [Prev response in frame: 10]
    [Request in frame: 14]
```

Exercise 6: Digging into DNS

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

Ans: The IP address is 150.203.161.98. The type is A.

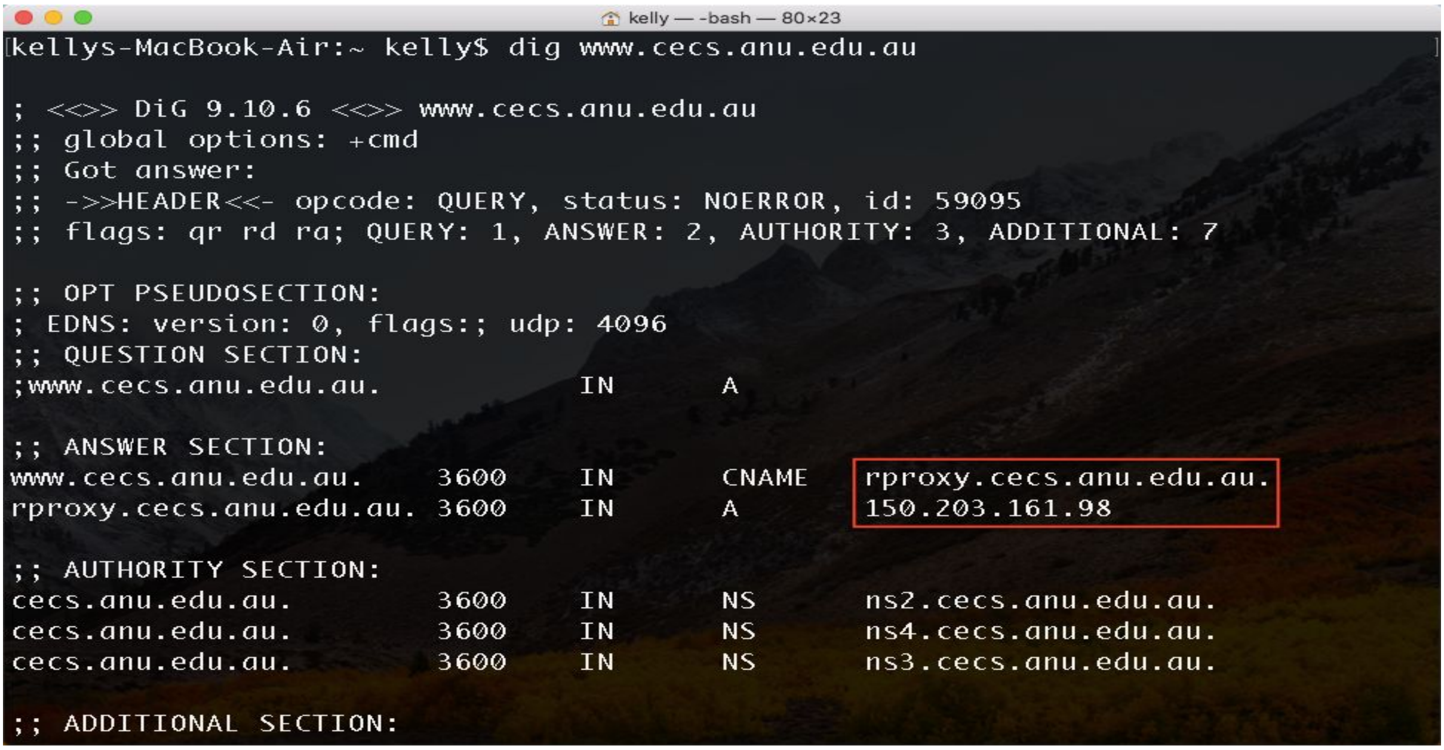


```
[kellys-MacBook-Air:~ kelly$ dig www.cecs.anu.edu.au

; <<>> DiG 9.10.6 <<>> www.cecs.anu.edu.au
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 59095
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 3, ADDITIONAL: 7

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

;; ANSWER SECTION:
www.cecs.anu.edu.au.    3600    IN      CNAME   rproxy.cecs.anu.edu.au.
rproxy.cecs.anu.edu.au. 3600    IN      A       150.203.161.98

;; AUTHORITY SECTION:
cecs.anu.edu.au.        3600    IN      NS      ns2.cecs.anu.edu.au.
cecs.anu.edu.au.        3600    IN      NS      ns4.cecs.anu.edu.au.
cecs.anu.edu.au.        3600    IN      NS      ns3.cecs.anu.edu.au.

;; ADDITIONAL SECTION:
```

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.

Ans: Canonical name: rproxy.cecs.anu.edu.au Its IP address: 150.203.161.98.

Because alias host name are more memorable than canonical hostnames.

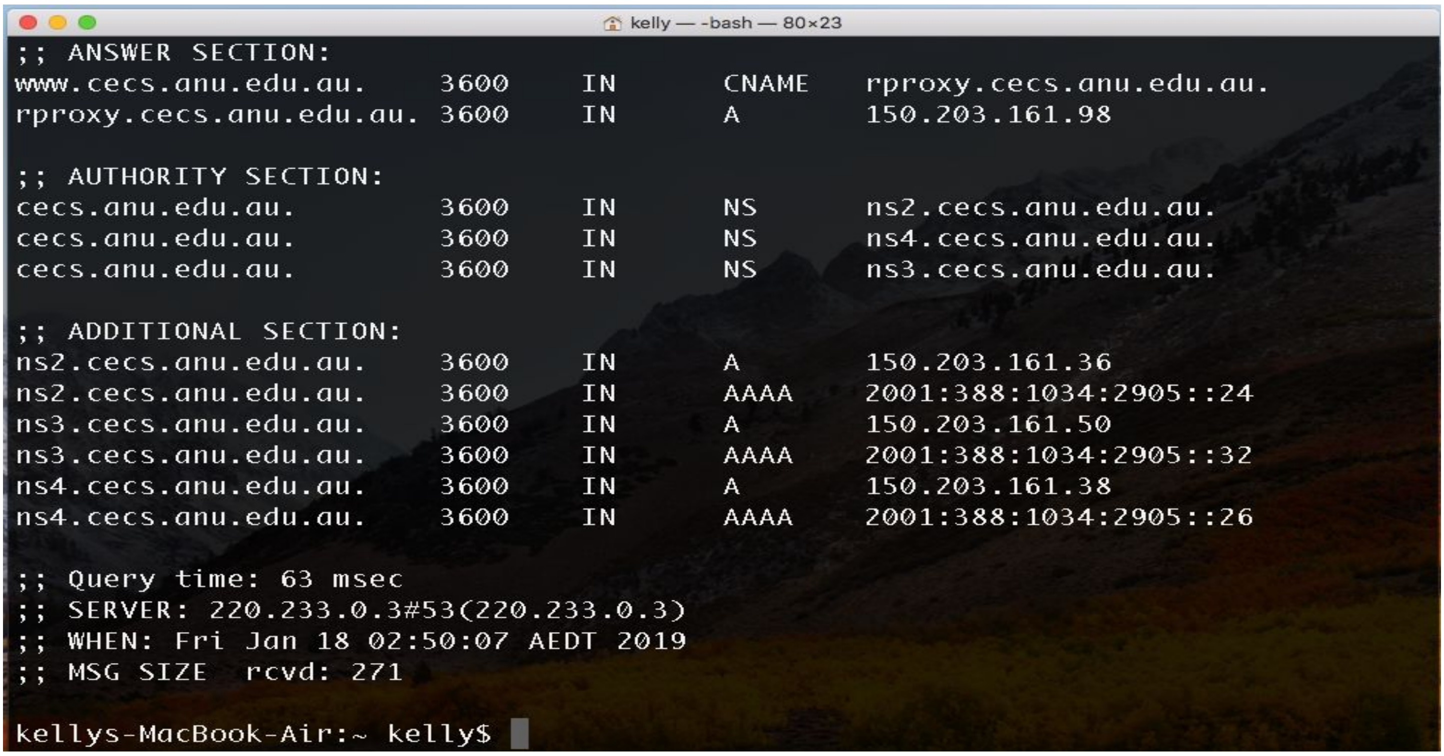


```
[kellys-MacBook-Air:~ kelly$ dig www.cecs.anu.edu.au

; <<>> DiG 9.10.6 <<>> www.cecs.anu.edu.au
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 59095
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 3, ADDITIONAL: 7

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

;; ANSWER SECTION:
www.cecs.anu.edu.au.    3600    IN      CNAME   rproxy.cecs.anu.edu.au.
rproxy.cecs.anu.edu.au. 3600    IN      A       150.203.161.98

;; AUTHORITY SECTION:
cecs.anu.edu.au.        3600    IN      NS      ns2.cecs.anu.edu.au.
cecs.anu.edu.au.        3600    IN      NS      ns4.cecs.anu.edu.au.
cecs.anu.edu.au.        3600    IN      NS      ns3.cecs.anu.edu.au.

;; ADDITIONAL SECTION:
```

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

Ans: 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 picture.

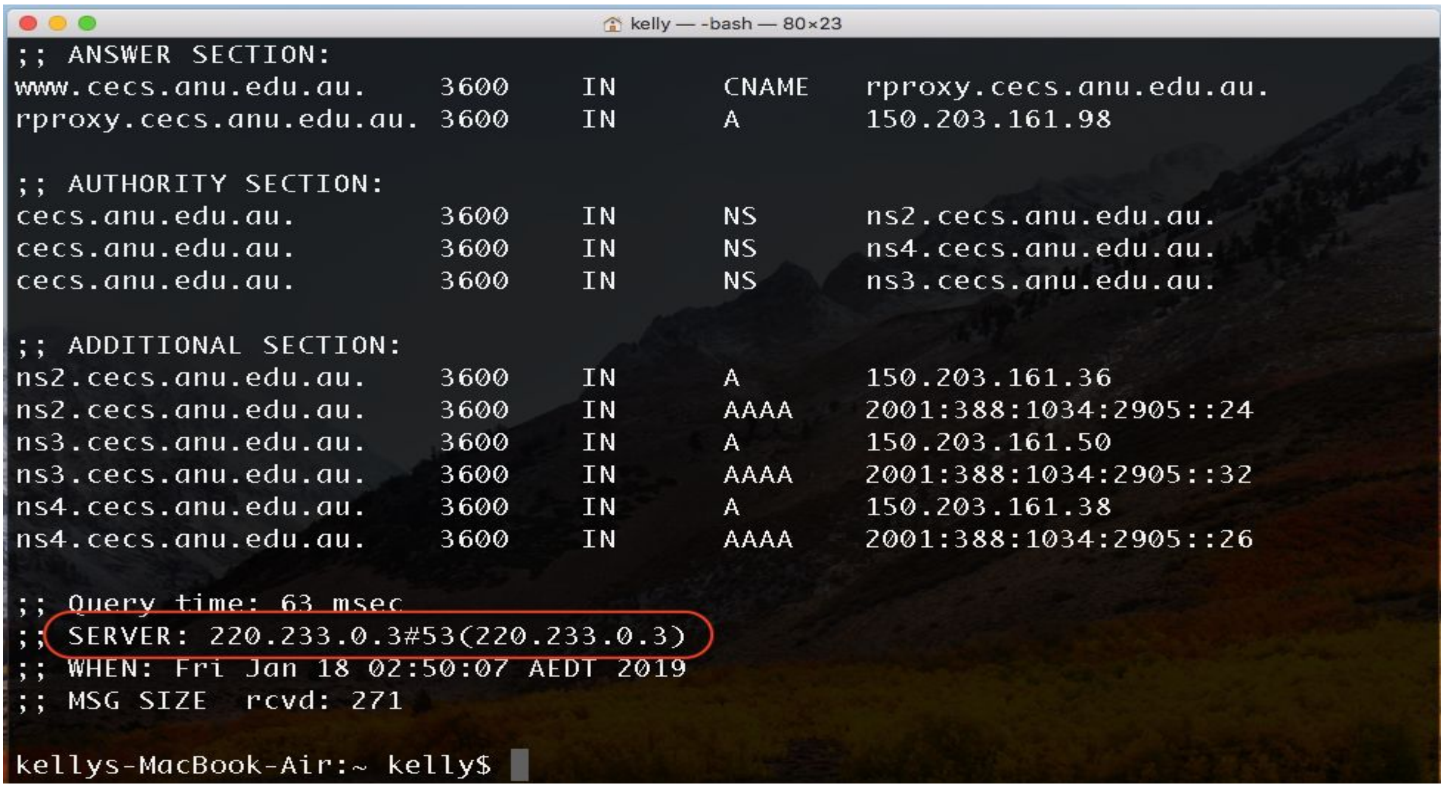
In ADDITIONAL SECTION , there are A/AAAA type RR of those Authoritative DNS Server list in AUTHORITY SECTION which showing their IPv4 or IPv6 address



```
;; ANSWER SECTION:
www.cecs.anu.edu.au.     3600    IN      CNAME    rproxy.cecs.anu.edu.au.
rproxy.cecs.anu.edu.au.  3600    IN      A        150.203.161.98

;; AUTHORITY SECTION:
cecs.anu.edu.au.         3600    IN      NS       ns2.cecs.anu.edu.au.
cecs.anu.edu.au.         3600    IN      NS       ns4.cecs.anu.edu.au.
cecs.anu.edu.au.         3600    IN      NS       ns3.cecs.anu.edu.au.

;; ADDITIONAL SECTION:
ns2.cecs.anu.edu.au.     3600    IN      A        150.203.161.36
ns2.cecs.anu.edu.au.     3600    IN      AAAA     2001:388:1034:2905::24
ns3.cecs.anu.edu.au.     3600    IN      A        150.203.161.50
ns3.cecs.anu.edu.au.     3600    IN      AAAA     2001:388:1034:2905::32
ns4.cecs.anu.edu.au.     3600    IN      A        150.203.161.38
ns4.cecs.anu.edu.au.     3600    IN      AAAA     2001:388:1034:2905::26

;; Query time: 63 msec
;; SERVER: 220.233.0.3#53(220.233.0.3)
;; WHEN: Fri Jan 18 02:50:07 AEDT 2019
;; MSG SIZE  rcvd: 271

kellys-MacBook-Air:~ kelly$
```

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

Ans: My local IP address: 220.233.0.3.



```
;; ANSWER SECTION:
www.cecs.anu.edu.au.     3600    IN      CNAME    rproxy.cecs.anu.edu.au.
rproxy.cecs.anu.edu.au.  3600    IN      A        150.203.161.98

;; AUTHORITY SECTION:
cecs.anu.edu.au.         3600    IN      NS       ns2.cecs.anu.edu.au.
cecs.anu.edu.au.         3600    IN      NS       ns4.cecs.anu.edu.au.
cecs.anu.edu.au.         3600    IN      NS       ns3.cecs.anu.edu.au.

;; ADDITIONAL SECTION:
ns2.cecs.anu.edu.au.     3600    IN      A        150.203.161.36
ns2.cecs.anu.edu.au.     3600    IN      AAAA     2001:388:1034:2905::24
ns3.cecs.anu.edu.au.     3600    IN      A        150.203.161.50
ns3.cecs.anu.edu.au.     3600    IN      AAAA     2001:388:1034:2905::32
ns4.cecs.anu.edu.au.     3600    IN      A        150.203.161.38
ns4.cecs.anu.edu.au.     3600    IN      AAAA     2001:388:1034:2905::26

;; Query time: 63 msec
;; SERVER: 220.233.0.3#53(220.233.0.3)
;; WHEN: Fri Jan 18 02:50:07 AEDT 2019
;; MSG SIZE  rcvd: 271

kellys-MacBook-Air:~ kelly$
```

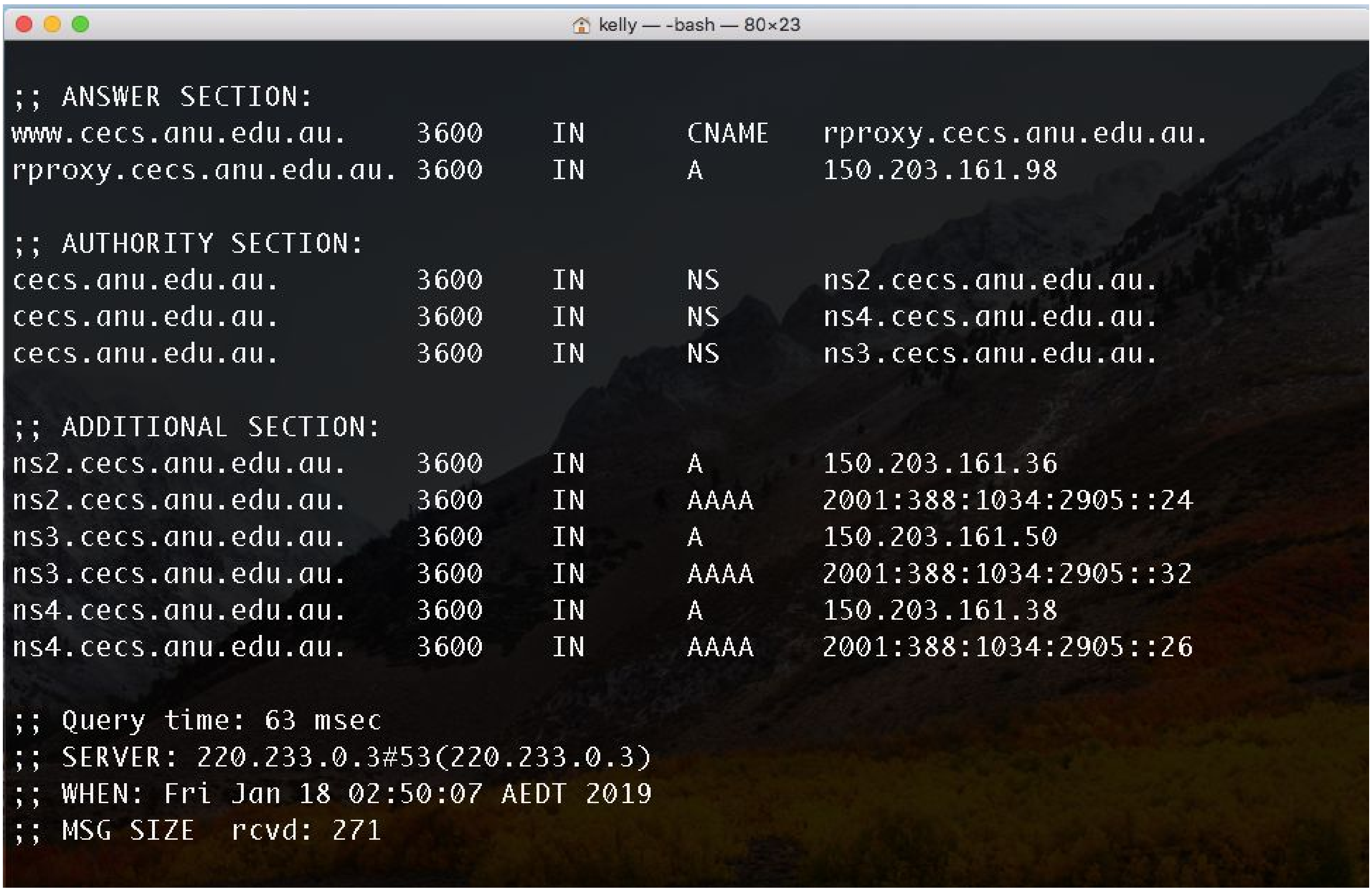
Question 5. What are the DNS nameservers for the “cecs.anu.edu.au” domain (note: the domain name is cecs.anu.edu.au and not www.cecs.anu.edu.au)? Find out their IP addresses? What type of DNS query is sent to obtain this information?

Ans: 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



```
;; ANSWER SECTION:
www.cecs.anu.edu.au.     3600    IN      CNAME   rproxy.cecs.anu.edu.au.
rproxy.cecs.anu.edu.au.  3600    IN      A       150.203.161.98

;; AUTHORITY SECTION:
cecs.anu.edu.au.         3600    IN      NS      ns2.cecs.anu.edu.au.
cecs.anu.edu.au.         3600    IN      NS      ns4.cecs.anu.edu.au.
cecs.anu.edu.au.         3600    IN      NS      ns3.cecs.anu.edu.au.

;; ADDITIONAL SECTION:
ns2.cecs.anu.edu.au.     3600    IN      A       150.203.161.36
ns2.cecs.anu.edu.au.     3600    IN      AAAA    2001:388:1034:2905::24
ns3.cecs.anu.edu.au.     3600    IN      A       150.203.161.50
ns3.cecs.anu.edu.au.     3600    IN      AAAA    2001:388:1034:2905::32
ns4.cecs.anu.edu.au.     3600    IN      A       150.203.161.38
ns4.cecs.anu.edu.au.     3600    IN      AAAA    2001:388:1034:2905::26

;; Query time: 63 msec
;; SERVER: 220.233.0.3#53(220.233.0.3)
;; WHEN: Fri Jan 18 02:50:07 AEDT 2019
;; MSG SIZE  rcvd: 271
```

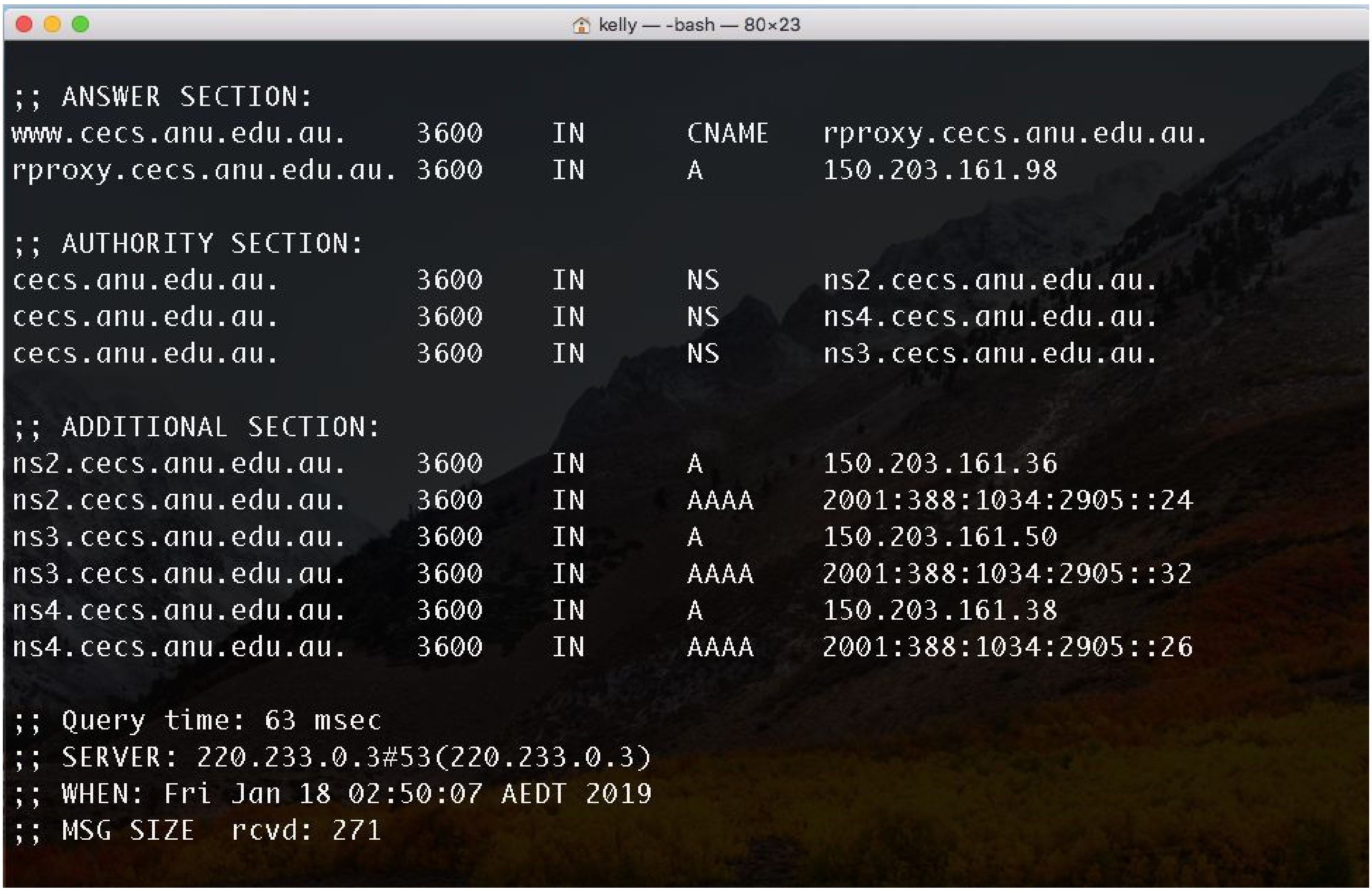
Question 6. What is the DNS name associated with the IP address 149.171.158.109? What type of DNS query is sent to obtain this information?

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

engplws008.ad.unsw.edu.au

engplws008.eng.unsw.edu.au

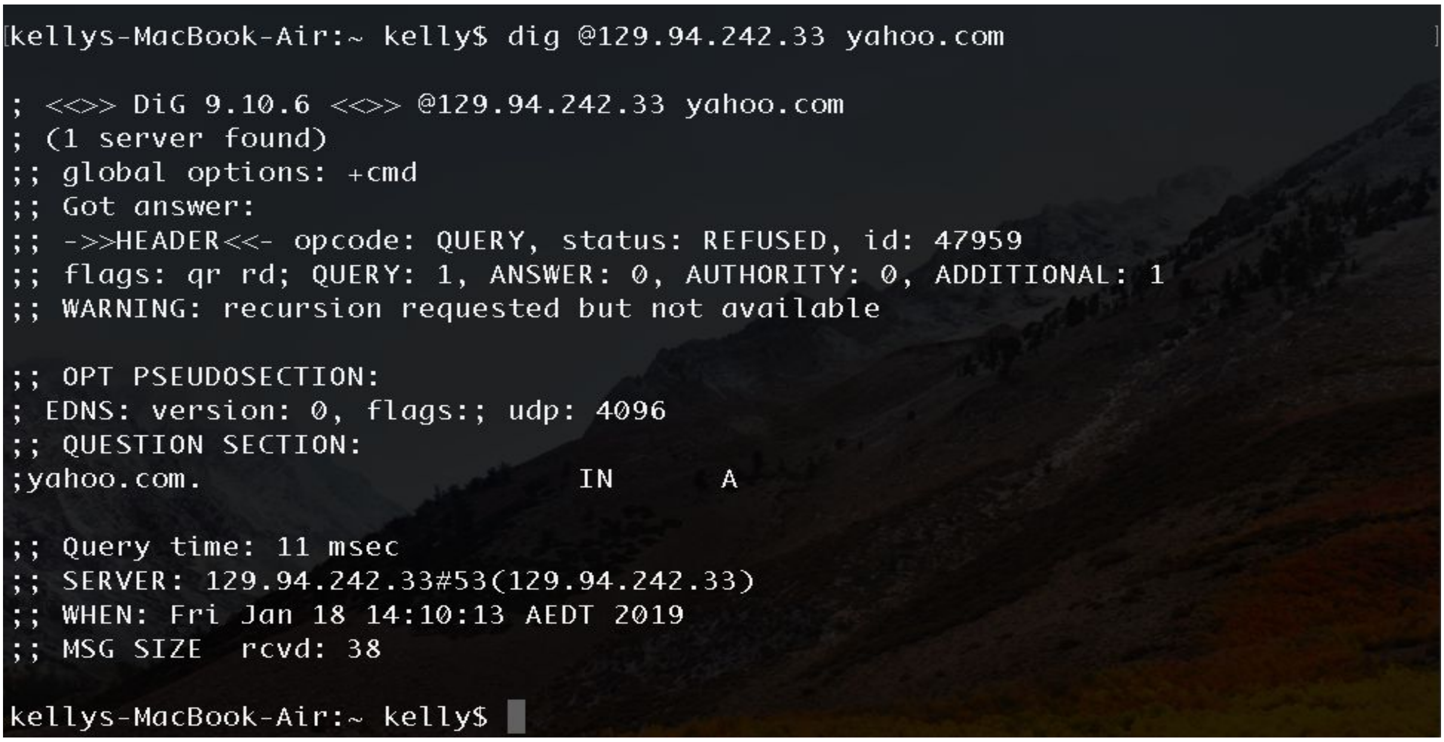
The type of DNS query is sent: PTR



```
;; ANSWER SECTION:
www.cecs.anu.edu.au.    3600    IN      CNAME   rproxy.cecs.anu.edu.au.
rproxy.cecs.anu.edu.au. 3600    IN      A       150.203.161.98

;; AUTHORITY SECTION:
cecs.anu.edu.au.        3600    IN      NS      ns2.cecs.anu.edu.au.
cecs.anu.edu.au.        3600    IN      NS      ns4.cecs.anu.edu.au.
cecs.anu.edu.au.        3600    IN      NS      ns3.cecs.anu.edu.au.

;; ADDITIONAL SECTION:
ns2.cecs.anu.edu.au.    3600    IN      A       150.203.161.36
ns2.cecs.anu.edu.au.    3600    IN      AAAA    2001:388:1034:2905::24
ns3.cecs.anu.edu.au.    3600    IN      A       150.203.161.50
ns3.cecs.anu.edu.au.    3600    IN      AAAA    2001:388:1034:2905::32
ns4.cecs.anu.edu.au.    3600    IN      A       150.203.161.38
ns4.cecs.anu.edu.au.    3600    IN      AAAA    2001:388:1034:2905::26

;; Query time: 63 msec
;; SERVER: 220.233.0.3#53(220.233.0.3)
;; WHEN: Fri Jan 18 02:50:07 AEDT 2019
;; MSG SIZE  rcvd: 271
```

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)

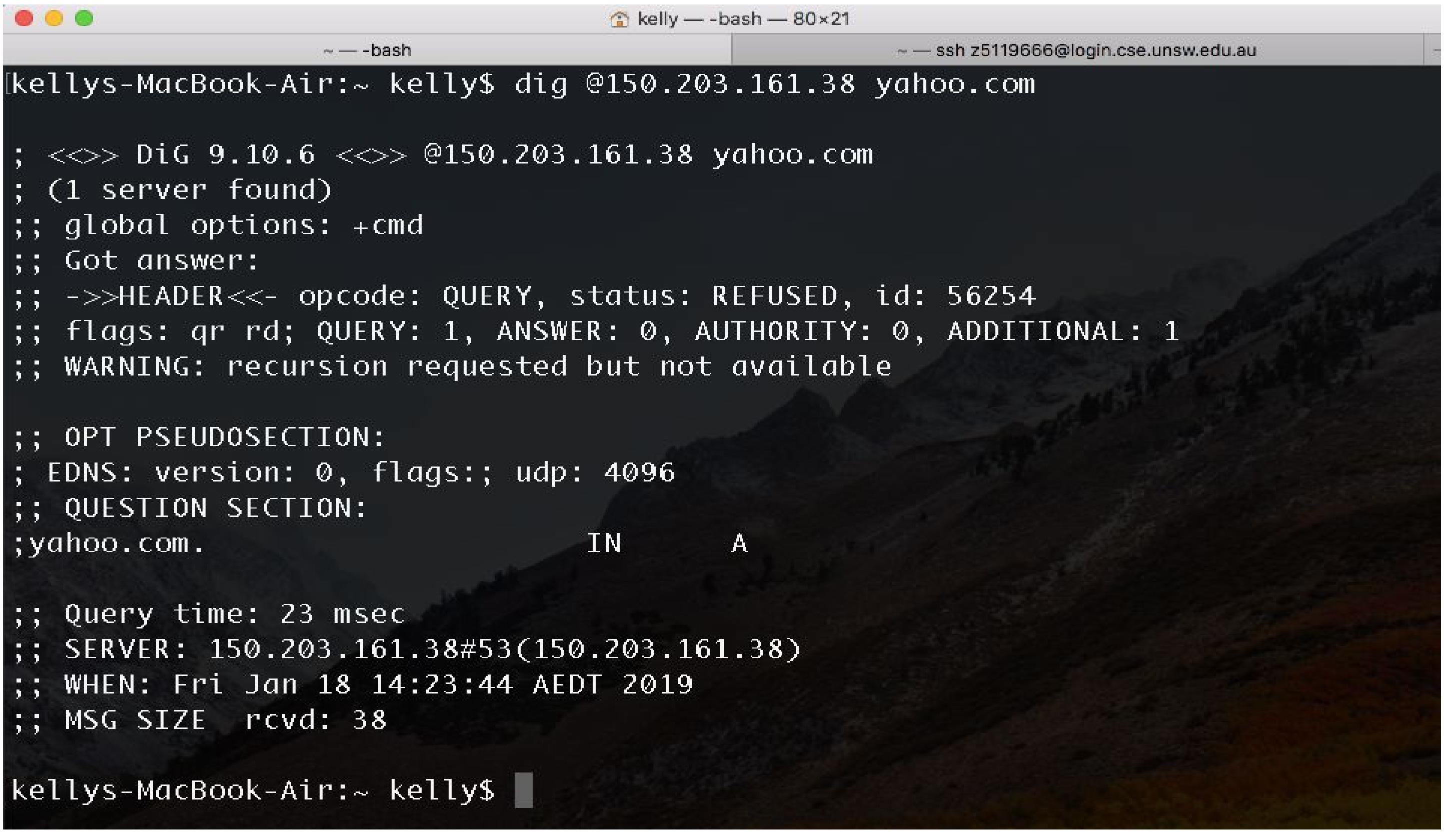
Ans: No, I didn't get an authoritative answer because there's no "aa", which means getting authoritative answer does not include in the flag. This is because it does not have authority for the CSE domain.



```
[kellys-MacBook-Air:~ kelly$ dig @129.94.242.33 yahoo.com

; <<>> DiG 9.10.6 <<>> @129.94.242.33 yahoo.com
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: REFUSED, id: 47959
;; flags: qr rd; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 1
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;yahoo.com.                     IN      A

;; Query time: 11 msec
;; SERVER: 129.94.242.33#53(129.94.242.33)
;; WHEN: Fri Jan 18 14:10:13 AEDT 2019
;; MSG SIZE  rcvd: 38

kellys-MacBook-Air:~ kelly$
```

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

Ans: Use 150.203.161.38. I no authoritative answer either.

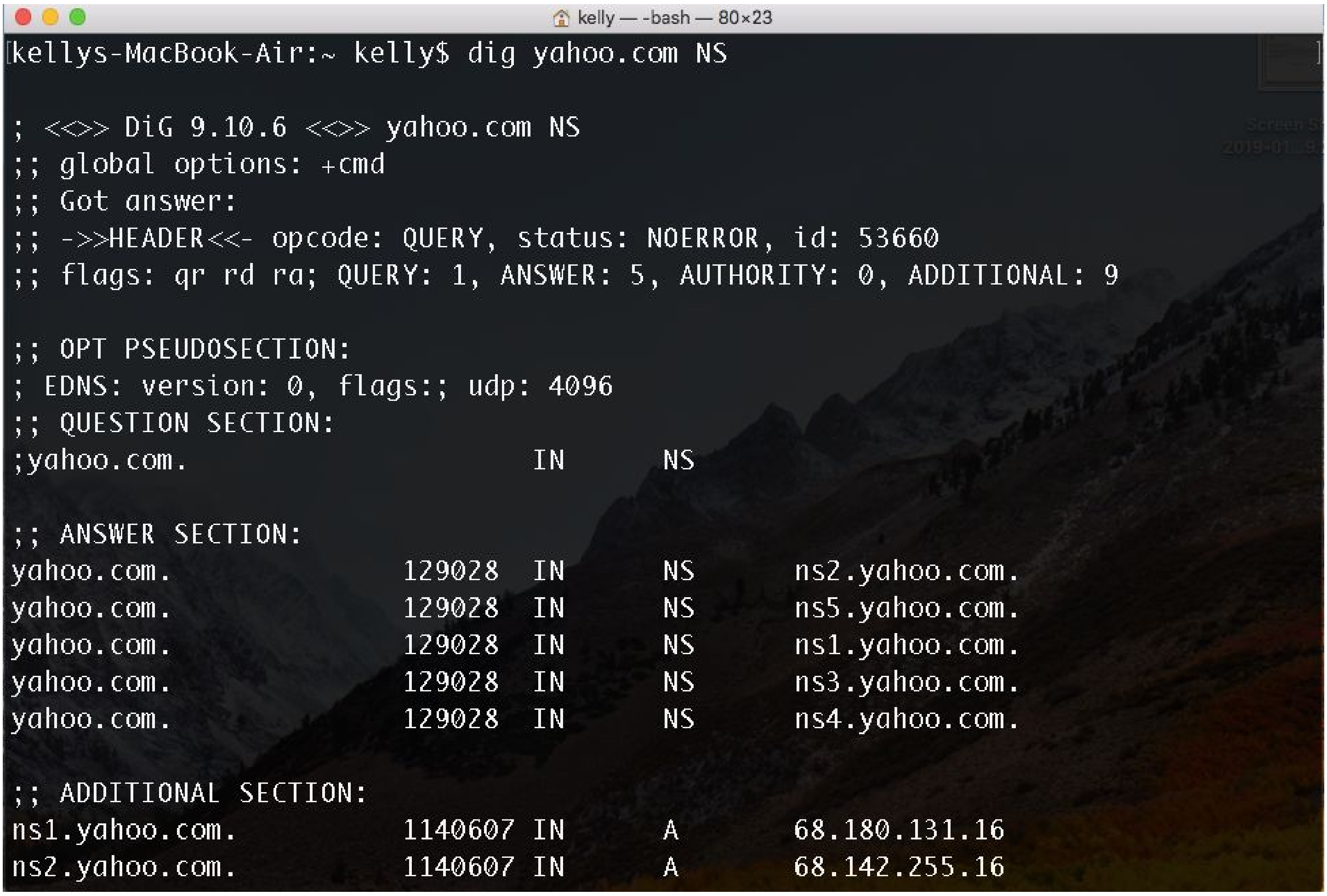


```
[kellys-MacBook-Air:~ kelly$ dig @150.203.161.38 yahoo.com

; <<>> DiG 9.10.6 <<>> @150.203.161.38 yahoo.com
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: REFUSED, id: 56254
;; flags: qr rd; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 1
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;yahoo.com.                     IN      A

;; Query time: 23 msec
;; SERVER: 150.203.161.38#53(150.203.161.38)
;; WHEN: Fri Jan 18 14:23:44 AEDT 2019
;; MSG SIZE  rcvd: 38

kellys-MacBook-Air:~ kelly$
```

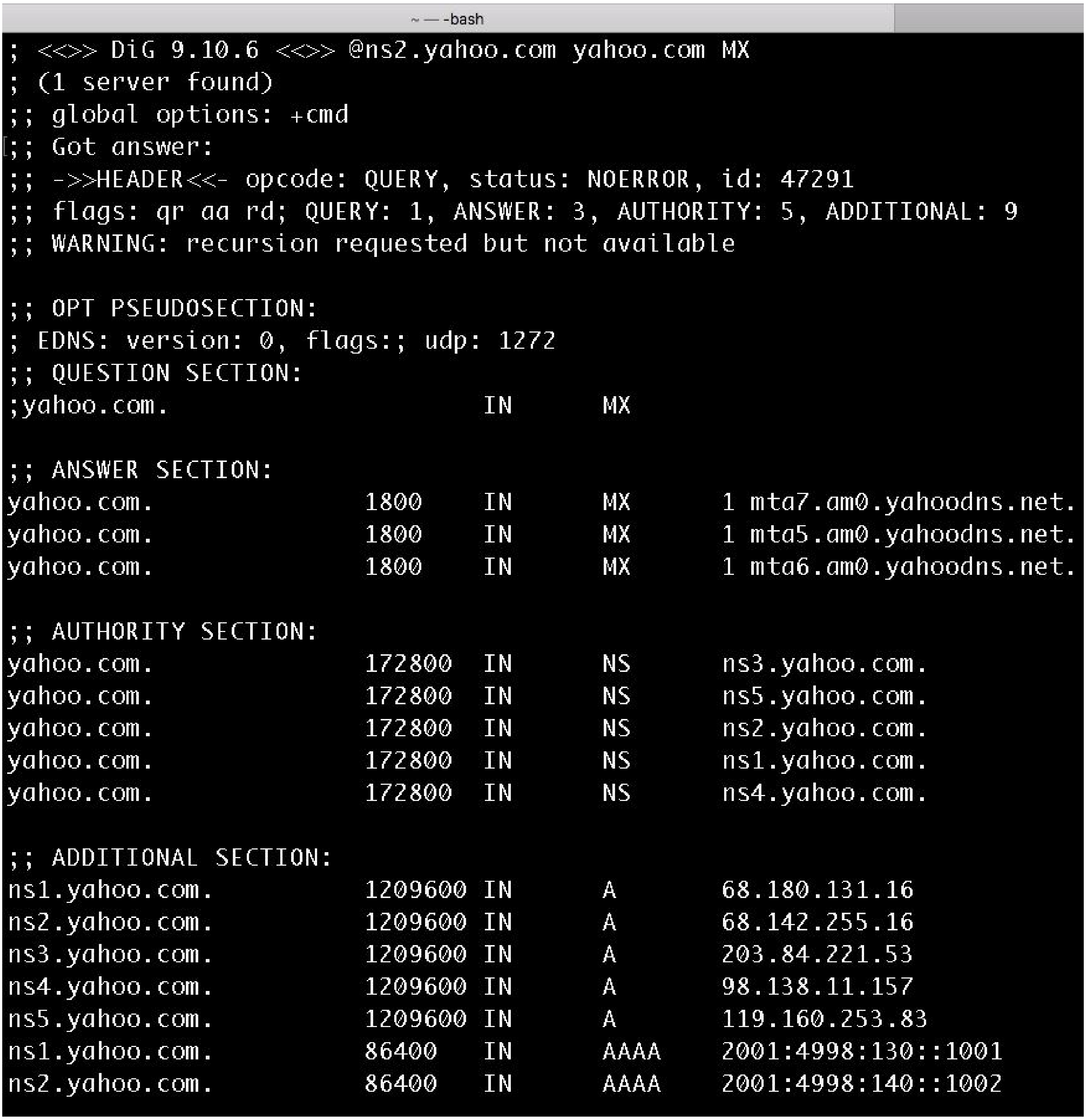
Question 9. Obtain the authoritative answer for the mail servers for Yahoo! mail. What type of DNS query is sent to obtain this information?

Ans: 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.



```
kellys-MacBook-Air:~ kelly$ dig yahoo.com NS

; <<>> DiG 9.10.6 <<>> yahoo.com NS
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 53660
;; flags: qr rd ra; QUERY: 1, ANSWER: 5, AUTHORITY: 0, ADDITIONAL: 9

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;yahoo.com.                     IN      NS

;; ANSWER SECTION:
yahoo.com.              129028  IN      NS      ns2.yahoo.com.
yahoo.com.              129028  IN      NS      ns5.yahoo.com.
yahoo.com.              129028  IN      NS      ns1.yahoo.com.
yahoo.com.              129028  IN      NS      ns3.yahoo.com.
yahoo.com.              129028  IN      NS      ns4.yahoo.com.

;; ADDITIONAL SECTION:
ns1.yahoo.com.          1140607 IN      A       68.180.131.16
ns2.yahoo.com.          1140607 IN      A       68.142.255.16
```



```
; <<>> DiG 9.10.6 <<>> @ns2.yahoo.com yahoo.com MX
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 47291
;; flags: qr aa rd; QUERY: 1, ANSWER: 3, AUTHORITY: 5, ADDITIONAL: 9
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1272
;; QUESTION SECTION:
;yahoo.com.                     IN      MX

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

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

;; ADDITIONAL SECTION:
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
ns1.yahoo.com.          86400   IN      AAAA    2001:4998:130::1001
ns2.yahoo.com.          86400   IN      AAAA    2001:4998:140::1002
```

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?

Ans: 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?

Ans: Yes, a machine may have several network interfaces. And, a network interface can have several IP address associated with it at any given time. An IP address may have associated with several names (aliases). To obtain the canonical name for the machine, use dig with query type=cname.