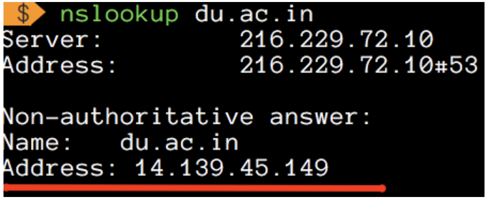
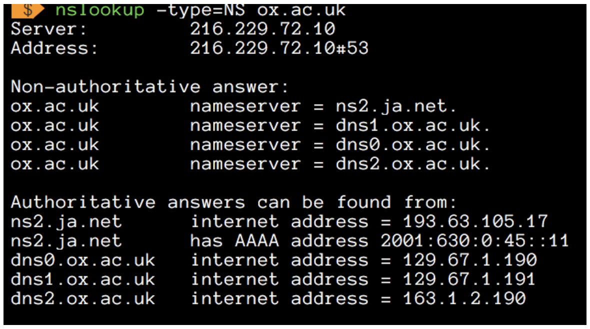
nslookup

- 1. Run nslookup to obtain the IP address of a Web Server in Asia, What is the ip address of that Server?
    - IP Address: 14.139.45.149



```
$ nslookup du.ac.in
Server:         216.229.72.10
Address:        216.229.72.10#53

Non-authoritative answer:
Name:   du.ac.in
Address: 14.139.45.149
```

  2. Run nslookup to determine the authoritative DNS servers for a university in Europe



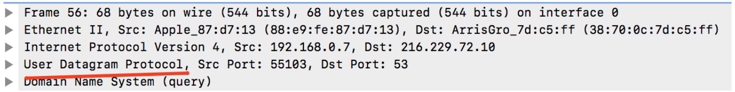
```
$ nslookup -type=NS ox.ac.uk
Server:         216.229.72.10
Address:        216.229.72.10#53

Non-authoritative answer:
ox.ac.uk        nameserver = ns2.ja.net.
ox.ac.uk        nameserver = dns1.ox.ac.uk.
ox.ac.uk        nameserver = dns0.ox.ac.uk.
ox.ac.uk        nameserver = dns2.ox.ac.uk.

Authoritative answers can be found from:
ns2.ja.net      internet address = 193.63.105.17
ns2.ja.net      has AAAA address 2001:630:0:45::11
dns0.ox.ac.uk   internet address = 129.67.1.190
dns1.ox.ac.uk   internet address = 129.67.1.191
dns2.ox.ac.uk   internet address = 163.1.2.190
```

    –

  3. Run nslookup so that one of the DNS servers obtained in question 2 is queried for the mail servers for yahoo! mail. What is its IP address?
    –

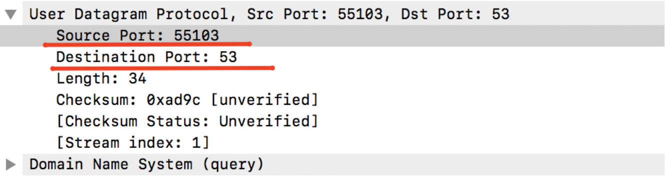
Tracing DNS with wireshark

- 1. Locate the DNS query and response messages. Are they sent over UDP or TCP?
    - The DNS query is being sent over UDP



```
▶ Frame 56: 68 bytes on wire (544 bits), 68 bytes captured (544 bits) on interface 0
▶ Ethernet II, Src: Apple_87:d7:13 (88:e9:fe:87:d7:13), Dst: ArrisGro_7d:c5:ff (38:70:0c:7d:c5:ff)
▶ Internet Protocol Version 4, Src: 192.168.0.7, Dst: 216.229.72.10
▶ User Datagram Protocol, Src Port: 55103, Dst Port: 53
▶ Domain Name System (query)
```

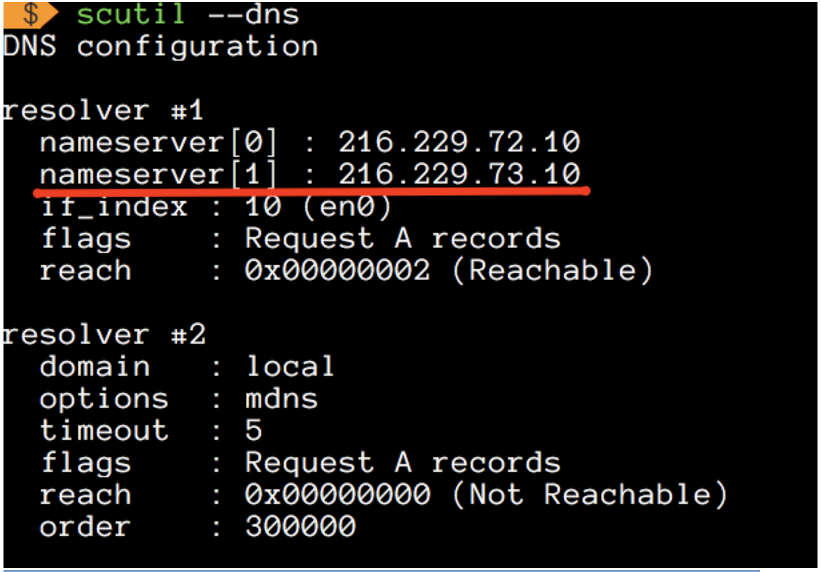
  2. What is the destination port for the DNS query message? What is the source port of DNS response message?
    - Source Port: 55103
    - Destination Port: 53



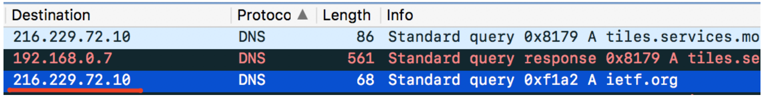
```
▼ User Datagram Protocol, Src Port: 55103, Dst Port: 53
    Source Port: 55103
    Destination Port: 53
    Length: 34
    Checksum: 0xad9c [unverified]
    [Checksum Status: Unverified]
    [Stream index: 1]
▶ Domain Name System (query)
```

3. To what ip address is the dns query message sent use ipconfig to deetermine the ip address of your local dns server. Are these two ip addresses the same?

   – The Query is sent to 226.229.72.10, the addresses are the same



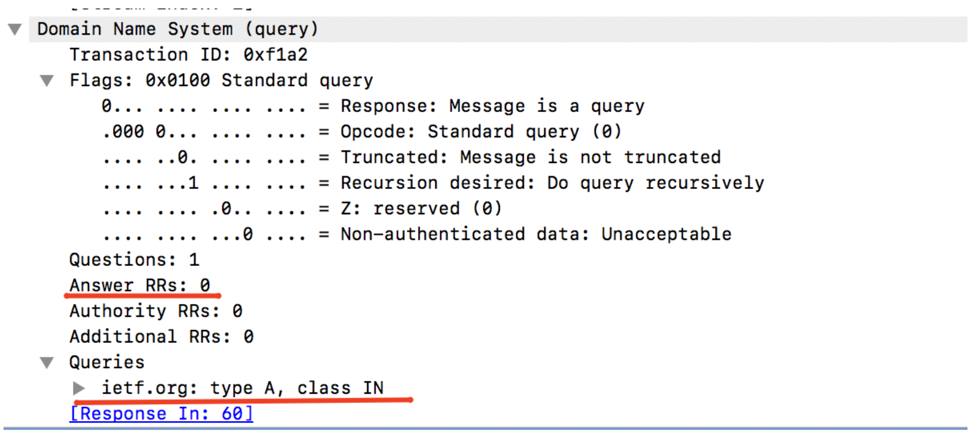
```
$ scutil --dns
DNS configuration

resolver #1
  nameserver[0] : 216.229.72.10
  nameserver[1] : 216.229.73.10
  if_index : 10 (en0)
  flags    : Request A records
  reach    : 0x00000002 (Reachable)

resolver #2
  domain   : local
  options  : mdns
  timeout  : 5
  flags    : Request A records
  reach    : 0x00000000 (Not Reachable)
  order    : 300000
```



Destination	Protoco ▲	Length	Info
216.229.72.10	DNS	86	Standard query 0x8179 A tiles.services.mo
192.168.0.7	DNS	561	Standard query response 0x8179 A tiles.se
216.229.72.10	DNS	68	Standard query 0xf1a2 A ietf.org

4. Examine the DNS query message. What ”Typee” of DNS query is it? Does the query message containy and ”answers”?

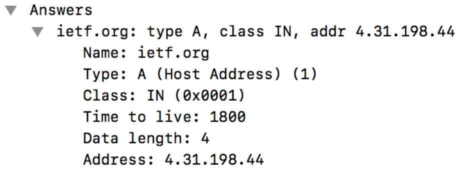
   – It is a standard Type A query and contains no ”Answers”



```
▼ Domain Name System (query)
    Transaction ID: 0xf1a2
  ▼ Flags: 0x0100 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)
      .... .... ...0 .... = Non-authenticated data: Unacceptable
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  ▼ Queries
    ▶ ietf.org: type A, class IN
    [Response In: 60]
```

5. Examine the DNS response message. How many ”answers” are provided? What do each of these answers contain?

   – The DNS response contains one ”answer” with all of the information on ietf.org that we requested, including the ip address

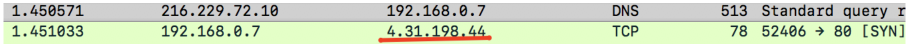


```
▼ Answers
  ▼ ietf.org: type A, class IN, addr 4.31.198.44
      Name: ietf.org
      Type: A (Host Address) (1)
      Class: IN (0x0001)
      Time to live: 1800
      Data length: 4
      Address: 4.31.198.44
```

6. Consider the subsequent TCP SYN packet sent by your host. Does the destination IP address of the SYN packet correspond to any of the IP addresses provided in the DNS response message?

   – Yes, the destination address of the TCP SYN packet matches the returned IP address of ietf.org that we requested in the previous step

   –

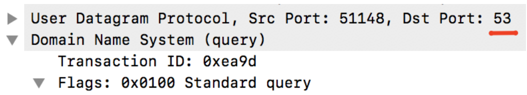


```
1.450571     216.229.72.10     192.168.0.7     DNS     513  Standard query r
1.451033     192.168.0.7       4.31.198.44     TCP      78  52406 → 80 [SYN]
```

7. What is the destination port for the DNS query message? What is the source port of the DNS response message?

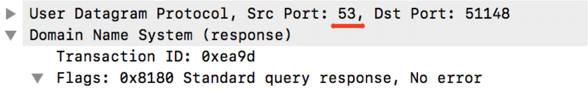
   – The Desination port for the DNS query is 53, the source port for the Response message is 53 aswell.

   –



```
▶ User Datagram Protocol, Src Port: 51148, Dst Port: 53
▼ Domain Name System (query)
    Transaction ID: 0xea9d
  ▼ Flags: 0x0100 Standard query
```

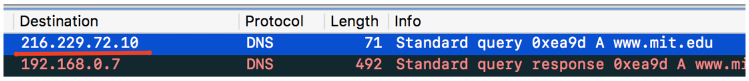
   –



```
▶ User Datagram Protocol, Src Port: 53, Dst Port: 51148
▼ Domain Name System (response)
    Transaction ID: 0xea9d
  ▼ Flags: 0x8180 Standard query response, No error
```

8. To what IP address is the DNS query meessage sent? Is this the IP address of your deefault local DNS server?

- IP Address: 216.229.72.10, This is the ip address of my local dns server.

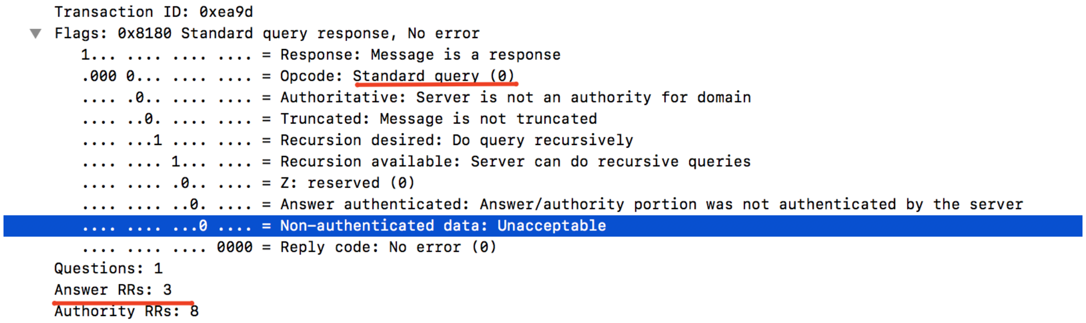


```
Destination      Protocol  Length  Info
216.229.72.10    DNS           71  Standard query 0xea9d A www.mit.edu
192.168.0.7      DNS          492  Standard query response 0xea9d A www.mi
```

-

9. Examine the DNS query mesesage. What type of DNS query is it? Dose the query message contain any ”answers”?

   - The Query is a standard Type A Query, it does not contain any answers

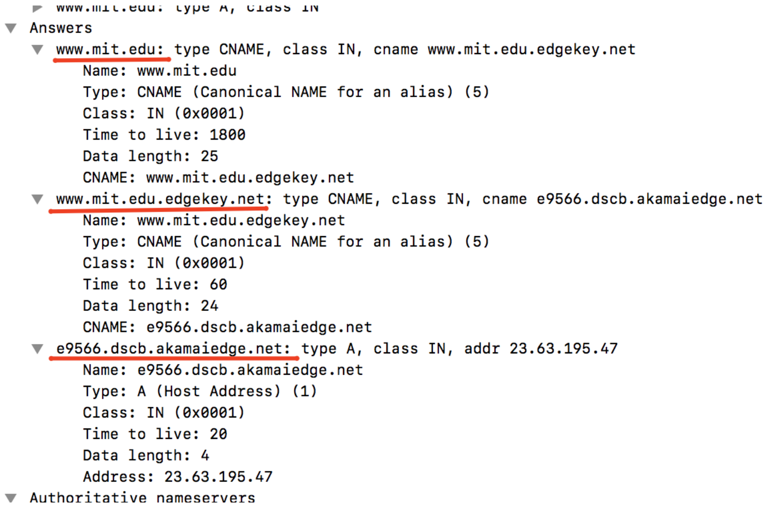


```
  Transaction ID: 0xea9d
▼ Flags: 0x8180 Standard query response, No error
    1... .... .... .... = Response: Message is a response
    .000 0... .... .... = Opcode: Standard query (0)
    .... .0.. .... .... = Authoritative: Server is not an authority for domain
    .... ..0. .... .... = Truncated: Message is not truncated
    .... ...1 .... .... = Recursion desired: Do query recursively
    .... .... 1... .... = Recursion available: Server can do recursive queries
    .... .... .0.. .... = Z: reserved (0)
    .... .... ..0. .... = Answer authenticated: Answer/authority portion was not authenticated by the server
    .... .... ...0 .... = Non-authenticated data: Unacceptable
    .... .... .... 0000 = Reply code: No error (0)
  Questions: 1
  Answer RRs: 3
  Authority RRs: 8
```

   -

10. examine the DNS response message. How many answers are provided? What do each of these answers contain?

    - There are three Answers in the DNS response message. There is one host address which corresponds to the ip address we request, and two CNAMES.



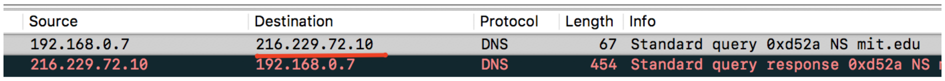
```
  ▶ www.mit.edu: type A, class IN
▼ Answers
  ▼ www.mit.edu: type CNAME, class IN, cname www.mit.edu.edgekey.net
      Name: www.mit.edu
      Type: CNAME (Canonical NAME for an alias) (5)
      Class: IN (0x0001)
      Time to live: 1800
      Data length: 25
      CNAME: www.mit.edu.edgekey.net
  ▼ www.mit.edu.edgekey.net: type CNAME, class IN, cname e9566.dscb.akamaiedge.net
      Name: www.mit.edu.edgekey.net
      Type: CNAME (Canonical NAME for an alias) (5)
      Class: IN (0x0001)
      Time to live: 60
      Data length: 24
      CNAME: e9566.dscb.akamaiedge.net
  ▼ e9566.dscb.akamaiedge.net: type A, class IN, addr 23.63.195.47
      Name: e9566.dscb.akamaiedge.net
      Type: A (Host Address) (1)
      Class: IN (0x0001)
      Time to live: 20
      Data length: 4
      Address: 23.63.195.47
▼ Authoritative nameservers
```

    -

11. To what IP address is the DNS query message sent? Is this the IP address of your default local DNS Server?

    - 216.229.72.10, this is the ip address of my local DNS server.

–

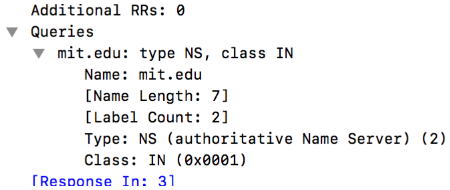


```
Source          Destination     Protocol  Length  Info
192.168.0.7     216.229.72.10   DNS           67  Standard query 0xd52a NS mit.edu
216.229.72.10   192.168.0.7     DNS          454  Standard query response 0xd52a NS
```

12. Examine the DNS query message. What ”Type” of DNS query is it? Does the query message contain any ”answers”?

    – The DNS Query is ”NS” type and contains 8 answers.

    –

    ```
        Additional RRs: 0
    ▼ Queries
      ▼ mit.edu: type NS, class IN
            Name: mit.edu
            [Name Length: 7]
            [Label Count: 2]
            Type: NS (authoritative Name Server) (2)
            Class: IN (0x0001)
        [Response In: 3]
    ```

13. Examine the DNS response message. What MIT nameservers does the response message provide? Does this reponse message also provide the IP addresses of the MIT nameservers?

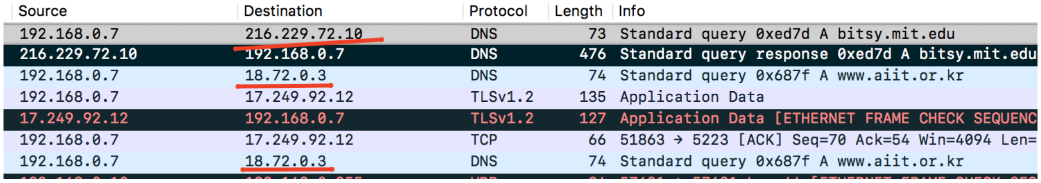
    – The response contains the Authoritative Nameservers, and does not provide IP addresses for the MIT nameservers.

14. Provide A Screenshot (Included to keep question numbers the same for easier grading)

15. To what IP address is the DNS query message sent? Is this the ip address of your default local DNS Server? If not, what does the ip address correspond to?

    – Two DNS queries are sent to 18.72.0.3, and One DNS query is sent to 216.229.72.10 which is my default dns server.

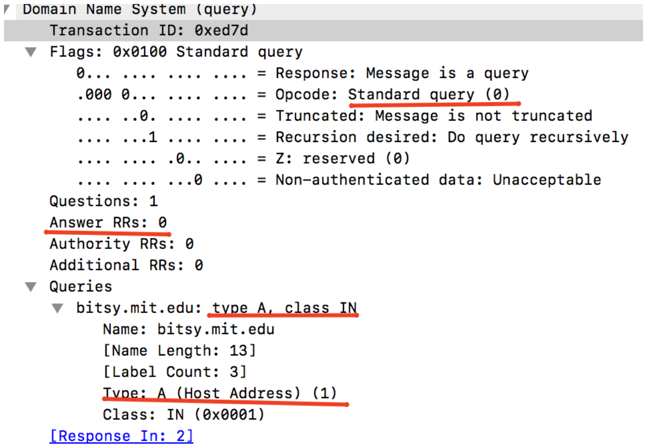
    –

    ```
    Source          Destination     Protocol  Length  Info
    192.168.0.7     216.229.72.10   DNS           73  Standard query 0xed7d A bitsy.mit.edu
    216.229.72.10   192.168.0.7     DNS          476  Standard query response 0xed7d A bitsy.mit.edu
    192.168.0.7     18.72.0.3       DNS           74  Standard query 0x687f A www.aiit.or.kr
    192.168.0.7     17.249.92.12    TLSv1.2      135  Application Data
    17.249.92.12    192.168.0.7     TLSv1.2      127  Application Data [ETHERNET FRAME CHECK SEQUENC
    192.168.0.7     17.249.92.12    TCP           66  51863 → 5223 [ACK] Seq=70 Ack=54 Win=4094 Len=
    192.168.0.7     18.72.0.3       DNS           74  Standard query 0x687f A www.aiit.or.kr
    ```

16. Examine the DNS query message. What ”Type” of DNS query is it? Does the query message contain any ”answers”?

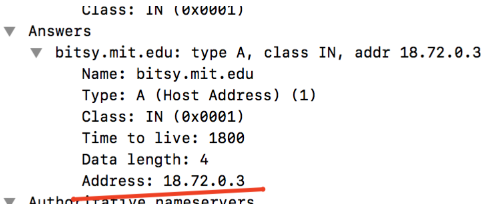
    – All three DNS queries are standard Type A queries, and all three queries do not have answers.

- 

```
▼ Domain Name System (query)
    Transaction ID: 0xed7d
  ▼ Flags: 0x0100 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)
      .... .... ...0 .... = Non-authenticated data: Unacceptable
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  ▼ Queries
    ▼ bitsy.mit.edu: type A, class IN
        Name: bitsy.mit.edu
        [Name Length: 13]
        [Label Count: 3]
        Type: A (Host Address) (1)
        Class: IN (0x0001)
    [Response In: 2]
```

17. Examine the DNs response message. How many "answers" are prio-vided? What does each of these answers contain?

    - There is one Answer which conatins the ip of bitsy.mit.edu

```
        Class: IN (0x0001)
  ▼ Answers
    ▼ bitsy.mit.edu: type A, class IN, addr 18.72.0.3
        Name: bitsy.mit.edu
        Type: A (Host Address) (1)
        Class: IN (0x0001)
        Time to live: 1800
        Data length: 4
        Address: 18.72.0.3
  ▼ Authoritative nameservers
```

18. Provide A Screenshot (Included to keep question numbers the same for easier grading)