WORKING WITH DNS

S Srinivas Saurab
CS16B039
Dept. of CSE, IIT-Madras

April 17, 2019

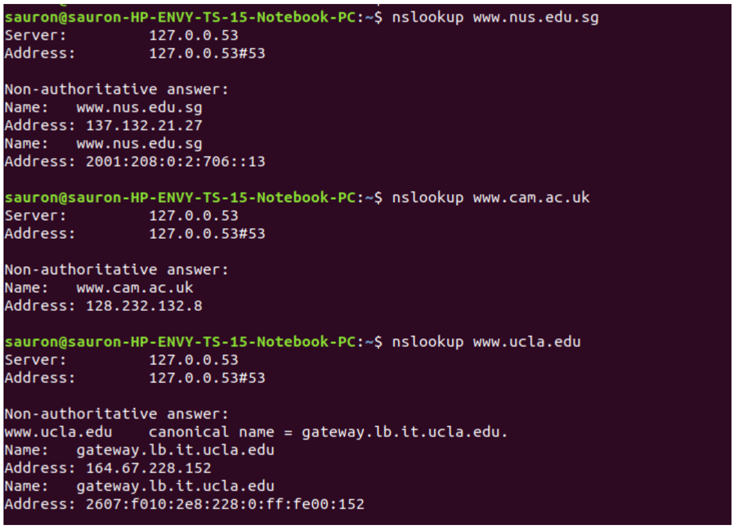
Question 1:

Favorite university in Asia : National University of Singapore
Webserver url : www.nus.edu.sg
Nslookup **IP returned** : 137.132.21.27*

Favorite university in Europe : University of Cambridge
Webserver url : www.cam.ac.uk
Nslookup **IP returned** : 128.232.132.8*

Favorite university in America : University of California, Los Angeles
Webserver url : www.ucla.edu
Canonical name : gateway.lb.it.ucla.edu
Nslookup **IP returned** :164.67.228.152(v4) & 2607:f010:2e8:228:0:ff:fe00:152(v6)

(* : Non-authoritative answer)



```
sauron@sauron-HP-ENVY-TS-15-Notebook-PC:~$ nslookup www.nus.edu.sg
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
Name:   www.nus.edu.sg
Address: 137.132.21.27
Name:   www.nus.edu.sg
Address: 2001:208:0:2:706::13

sauron@sauron-HP-ENVY-TS-15-Notebook-PC:~$ nslookup www.cam.ac.uk
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
Name:   www.cam.ac.uk
Address: 128.232.132.8

sauron@sauron-HP-ENVY-TS-15-Notebook-PC:~$ nslookup www.ucla.edu
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
www.ucla.edu    canonical name = gateway.lb.it.ucla.edu.
Name:   gateway.lb.it.ucla.edu
Address: 164.67.228.152
Name:   gateway.lb.it.ucla.edu
Address: 2607:f010:2e8:228:0:ff:fe00:152
```

Note that we see as the corresponding server because, 127.0.0.53 #53 because Ubuntu 18.04 uses “systemd-resolved” that caches DNS query responses at the local host.

Question 2:

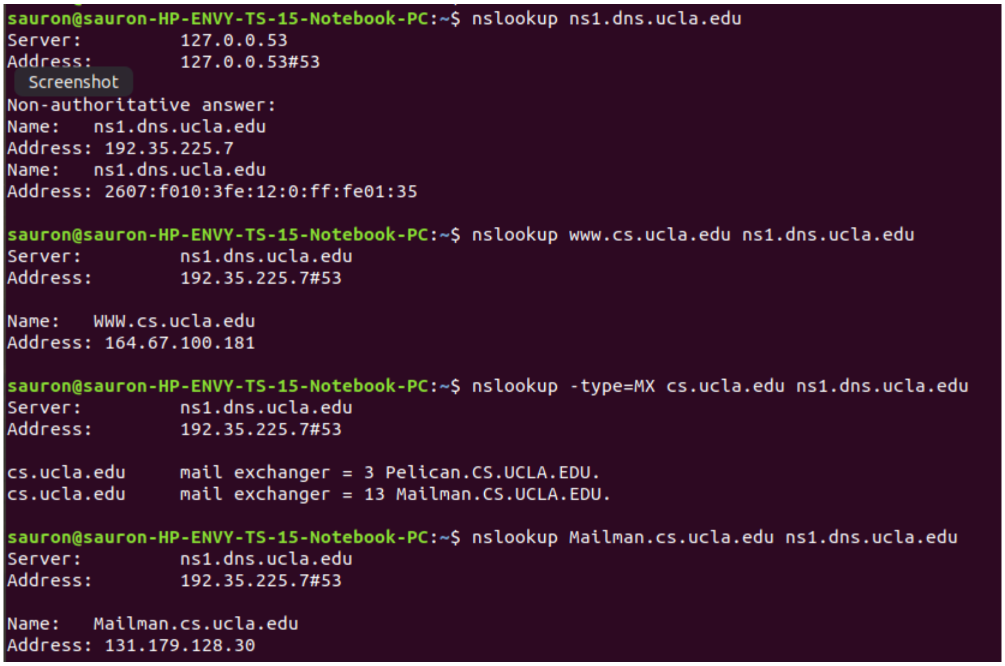
University Asia: NU-Singapore
URL : nus.edu.sg
Authoritative DNS servers:
1) ns1.nus.edu.sg
2) ns2.nus.edu.sg
3) alert.nus.edu.sg

University Europe: University of Cambridge
URL : cam.ac.uk
Authoritative DNS servers:
1) dns0.eng.cam.ac.uk
2) dns0.cl.cam.ac.uk
3) authdns0.csx.cam.ac.uk
4) ns2.ic.ac.uk
5) sns-pb.isc.org

University America: University of California, Los Angeles
URL : ucla.edu

Authoritative DNS servers:
1) ns1.dns.ucla.edu
2) ns2.dns.ucla.edu
3) ns3.dns.ucla.edu
4) ns4.dns.ucla.edu

Question 3,4:



```
sauron@sauron-HP-ENVY-TS-15-Notebook-PC:~$ nslookup ns1.dns.ucla.edu
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
Name:   ns1.dns.ucla.edu
Address: 192.35.225.7
Name:   ns1.dns.ucla.edu
Address: 2607:f010:3fe:12:0:ff:fe01:35

sauron@sauron-HP-ENVY-TS-15-Notebook-PC:~$ nslookup www.cs.ucla.edu ns1.dns.ucla.edu
Server:         ns1.dns.ucla.edu
Address:        192.35.225.7#53

Name:   WWW.cs.ucla.edu
Address: 164.67.100.181

sauron@sauron-HP-ENVY-TS-15-Notebook-PC:~$ nslookup -type=MX cs.ucla.edu ns1.dns.ucla.edu
Server:         ns1.dns.ucla.edu
Address:        192.35.225.7#53

cs.ucla.edu     mail exchanger = 3 Pelican.CS.UCLA.EDU.
cs.ucla.edu     mail exchanger = 13 Mailman.CS.UCLA.EDU.

sauron@sauron-HP-ENVY-TS-15-Notebook-PC:~$ nslookup Mailman.cs.ucla.edu ns1.dns.ucla.edu
Server:         ns1.dns.ucla.edu
Address:        192.35.225.7#53

Name:   Mailman.cs.ucla.edu
Address: 131.179.128.30
```

Figure : Example - Finding the Web, Mail and authoritative DNS IP addresses for CS Dept., UCLA.

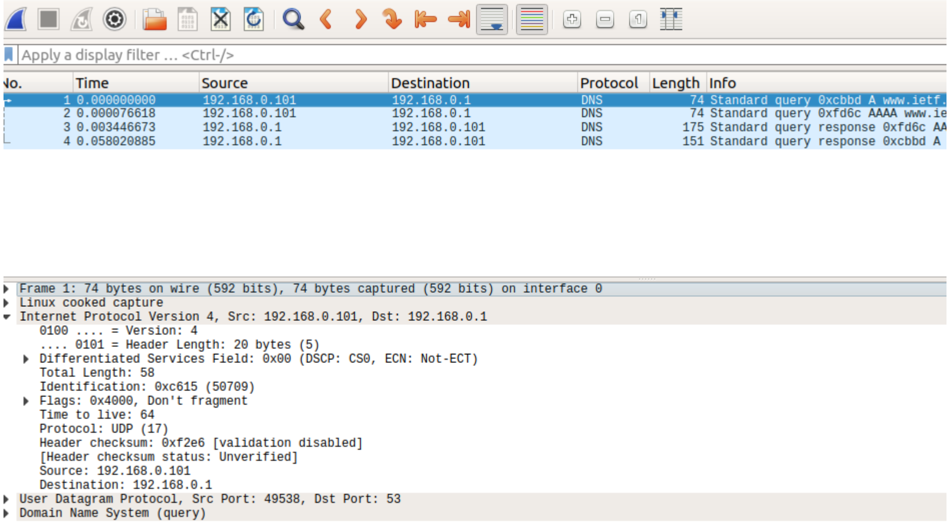
University Asia: NU-Singapore
Web server CS: www.comp.nus.edu.sg
Mail server CS: 84-101.comp.nus.edu.sg
Webserver IP : 137.132.84.218
Mailserver IP : 137.132.84.101
Auth DNS IP : 137.132.123.4

University Europe: University of Cambridge
Web server CS: www.cl.cam.ac.uk

Mail server CS: mx.cam.ac.uk
Webserver IP : 128.232.0.20(v4) & 2a05:b400:110::80:14(v6)
Mailserver IP : 131.111.8.147(/8/9*)
Auth DNS IP : 128.232.0.19(v4) & 2001:630:212:200::d:a0(v6)
(* : Using multiple server machines, round-robin scheme has been implemented here)

University America: University of California, Los Angeles
Web server CS: www.cs.ucla.edu
Mail server CS: Mailman.cs.ucla.edu
Webserver IP : 164.67.100.181
Mailserver IP : 131.179.128.30
Auth DNS IP : 192.35.225.7(v4) & 2607:f010:3fe:12:0:ff:fe01:35 (v6)

Question 5:



Apply a display filter ... <Ctrl-/>

```
No.   Time          Source           Destination      Protocol Length Info
    1 0.000000000   192.168.0.101    192.168.0.1      DNS          74 Standard query 0xcbbd A www.ietf.
    2 0.000076618   192.168.0.101    192.168.0.1      DNS          74 Standard query 0xfd6c AAAA www.ie
    3 0.003446673   192.168.0.1      192.168.0.101    DNS         175 Standard query response 0xfd6c AA
    4 0.058020885   192.168.0.1      192.168.0.101    DNS         151 Standard query response 0xcbbd A
```

```
▸ Frame 1: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0
▸ Linux cooked capture
▾ Internet Protocol Version 4, Src: 192.168.0.101, Dst: 192.168.0.1
     0100 .... = Version: 4
     .... 0101 = Header Length: 20 bytes (5)
   ▸ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
     Total Length: 58
     Identification: 0xc615 (50709)
   ▸ Flags: 0x4000, Don't fragment
     Time to live: 64
     Protocol: UDP (17)
     Header checksum: 0xf2e6 [validation disabled]
     [Header checksum status: Unverified]
     Source: 192.168.0.101
     Destination: 192.168.0.1
▸ User Datagram Protocol, Src Port: 49538, Dst Port: 53
▸ Domain Name System (query)
```

We can see the captured DNS packets in the figure above. The transport protocol can be seen in the IP-header as one of its fields. In this case, it corresponds to **UDP** with field value #17.

Question 6:

Destination port for query message : 53 (standard port on DNS server)
Source port for the query message : 54373 (an arbitrary port on our machine)

Question 7:

We can see that the DNS query has been sent to 192.168.0.1, this corresponds our default local DNS server (refer to picture in Q12).

Question 8:

There are two query messages that have been sent. Also we received two corresponding query responses. One of the queries is of 'type A' whereas the other message is of 'type AAAA' (also called : Quad A). On expanding the DNS query, we can see that there is no field or super-field named 'Answers'. Hence, as expected, the DNS query message has no answers present in it. Instead we find the super-field named 'Queries' here.

Question 9:

We know that there are two queries (A : IPv4, AAAA : IPv6). Correspondingly there are two query responses obtained.

Type A Query reponse :
In this response there are 3 answers given.

Answer 1: This is a type CNAME record. This corresponds to the canonical name of the url used (www.ietf.org) which is : www.ietf.org.cdn.cloudfare.net. This is needed because the type A records in the following answers will use the canonical alias and thus our browser needs remember this cname.

Answer 2: This answer gives the type A record. This has the fields : cname of the url, IPv4 address 1 of the domain. Note that there are two IPv4 addresses for this host and one of them, given in this answer, is : 104.20.1.85

Answer 3: This is the second type A record and corresponds to the second IPv4 address of the host queried for. This IP address is : 104.20.0.85

Type AAAA (Quad A) Query reponse :

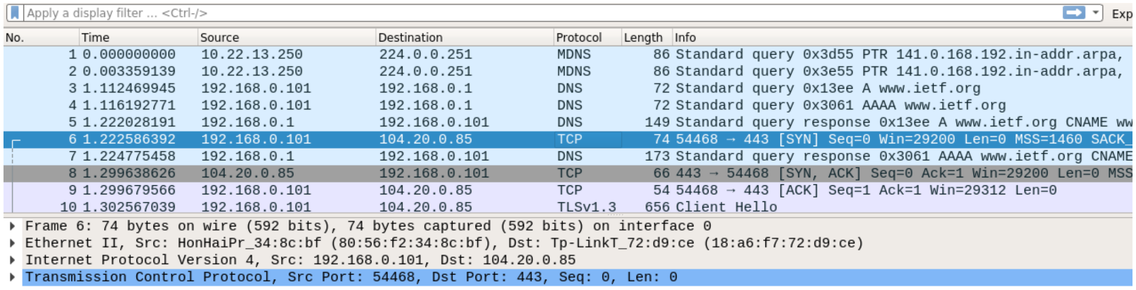
In this response there are 3 answers given.

Answer 1: This is a type CNAME record. This corresponds to the canonical name of the url used (www.ietf.org) which is : www.ietf.org.cdn.cloudfare.net. This is needed because the type AAAA records in the following answers will use the canonical alias and thus our browser needs remember this cname.

Answer 2: This answer gives the type AAAA record. This has the fields : cname of the url, IPv6 address 1 of the domain. Note that there are two IPv6 addresses for this host and one of them, given in this answer, is : 2606:4700:10::6814:155

Answer 3: This is the second type AAAA record and corresponds to the second IPv6 address of the host queried for. This IP address is : 2606:4700:10::6814:55

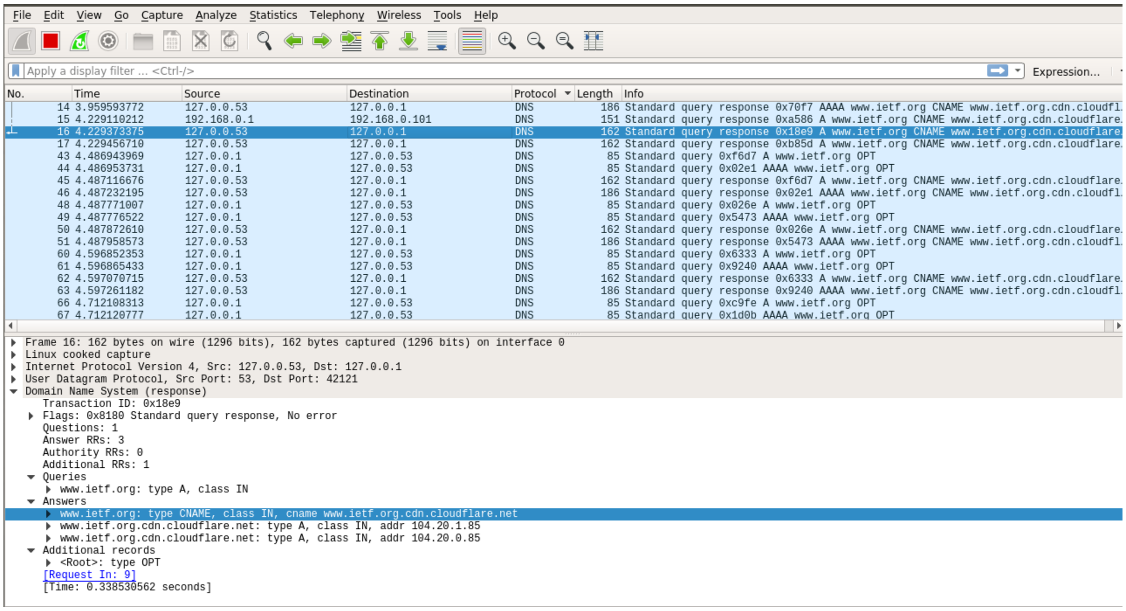
Question 10:



```
No.   Time         Source          Destination     Protocol  Length Info
    1 0.000000000  10.22.13.250    224.0.0.251     MDNS          86 Standard query 0x3d55 PTR 141.0.168.192.in-addr.arpa,
    2 0.003359139  10.22.13.250    224.0.0.251     MDNS          86 Standard query 0x3e55 PTR 141.0.168.192.in-addr.arpa,
    3 1.112469945  192.168.0.101   192.168.0.1     DNS           72 Standard query 0x13ee A www.ietf.org
    4 1.116192771  192.168.0.101   192.168.0.1     DNS           72 Standard query 0x3061 AAAA www.ietf.org
    5 1.222028191  192.168.0.1     192.168.0.101   DNS          149 Standard query response 0x13ee A www.ietf.org CNAME ww
    6 1.222586392  192.168.0.101   104.20.0.85     TCP           74 54468 → 443 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_
    7 1.224775458  192.168.0.1     192.168.0.101   DNS          173 Standard query response 0x3061 AAAA www.ietf.org CNAME
    8 1.299638626  104.20.0.85     192.168.0.101   TCP           66 443 → 54468 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS
    9 1.299679566  192.168.0.101   104.20.0.85     TCP           54 54468 → 443 [ACK] Seq=1 Ack=1 Win=29312 Len=0
   10 1.302567039  192.168.0.101   104.20.0.85     TLSv1.3      656 Client Hello
▸ Frame 6: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0
▸ Ethernet II, Src: HonHaiPr_34:8c:bf (80:56:f2:34:8c:bf), Dst: Tp-LinkT_72:d9:ce (18:a6:f7:72:d9:ce)
▸ Internet Protocol Version 4, Src: 192.168.0.101, Dst: 104.20.0.85
▸ Transmission Control Protocol, Src Port: 54468, Dst Port: 443, Seq: 0, Len: 0
```

In the figure above, we can see the first SYN message (highlighted) sent by our machine to a host whose IP address is : 104.20.0.85. From the previously seen DNS response messages, we find that this IP address is one of the IPv4 addresses corresponding to the machine hosting the server of itef.org. Hence, as expected, we find a TCP connection SYN message (perhaps as a part of HTTPs protocol) sent from our machine to one of the 'ietf' servers.

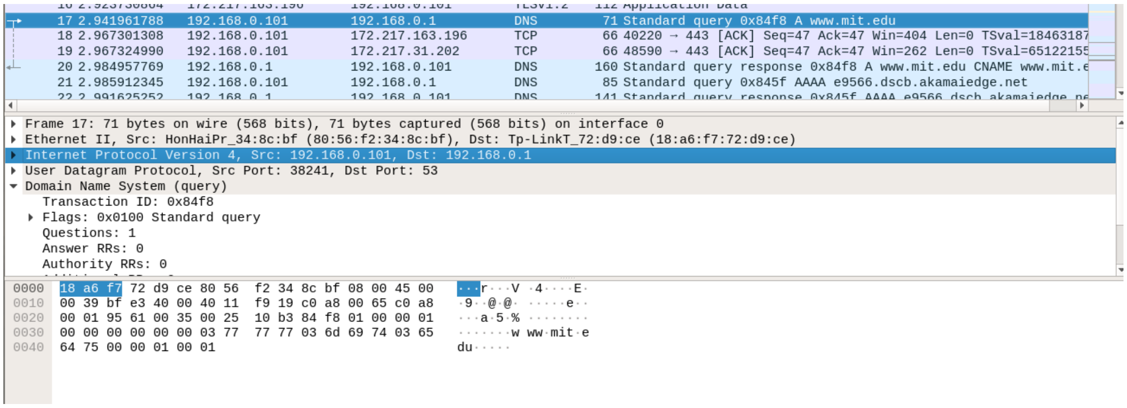
Question 10.1:


File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...

```
No.  Time         Source       Destination   Protocol  Length Info
  14 3.959593772  127.0.0.53   127.0.0.1     DNS       186 Standard query response 0x70f7 AAAA www.ietf.org CNAME www.ietf.org.cdn.cloudfl…
  15 4.229110212  192.168.0.1  192.168.0.101 DNS       151 Standard query response 0xa586 A www.ietf.org CNAME www.ietf.org.cdn.cloudflare…
  16 4.229373375  127.0.0.53   127.0.0.1     DNS       162 Standard query response 0x18e9 A www.ietf.org CNAME www.ietf.org.cdn.cloudflare…
  17 4.229456710  127.0.0.53   127.0.0.1     DNS       162 Standard query response 0xb85d A www.ietf.org CNAME www.ietf.org.cdn.cloudflare…
  43 4.486943969  127.0.0.1    127.0.0.53    DNS        85 Standard query 0xf6d7 A www.ietf.org OPT
  44 4.486953731  127.0.0.1    127.0.0.53    DNS        85 Standard query 0x02e1 AAAA www.ietf.org OPT
  45 4.487116676  127.0.0.53   127.0.0.1     DNS       162 Standard query response 0xf6d7 A www.ietf.org CNAME www.ietf.org.cdn.cloudflare…
  46 4.487232195  127.0.0.53   127.0.0.1     DNS       186 Standard query response 0x02e1 AAAA www.ietf.org CNAME www.ietf.org.cdn.cloudfl…
  48 4.487771007  127.0.0.1    127.0.0.53    DNS        85 Standard query 0x026e A www.ietf.org OPT
  49 4.487776522  127.0.0.1    127.0.0.53    DNS        85 Standard query 0x5473 AAAA www.ietf.org OPT
  50 4.487872610  127.0.0.53   127.0.0.1     DNS       162 Standard query response 0x026e A www.ietf.org CNAME www.ietf.org.cdn.cloudflare…
  51 4.487958573  127.0.0.53   127.0.0.1     DNS       186 Standard query response 0x5473 AAAA www.ietf.org CNAME www.ietf.org.cdn.cloudfl…
  60 4.596852353  127.0.0.1    127.0.0.53    DNS        85 Standard query 0x6333 A www.ietf.org OPT
  61 4.596865433  127.0.0.1    127.0.0.53    DNS        85 Standard query 0x9240 AAAA www.ietf.org OPT
  62 4.597070715  127.0.0.53   127.0.0.1     DNS       162 Standard query response 0x6333 A www.ietf.org CNAME www.ietf.org.cdn.cloudflare…
  63 4.597261182  127.0.0.53   127.0.0.1     DNS       186 Standard query response 0x9240 AAAA www.ietf.org CNAME www.ietf.org.cdn.cloudfl…
  66 4.712108313  127.0.0.1    127.0.0.53    DNS        85 Standard query 0xc9fe A www.ietf.org OPT
  67 4.712120777  127.0.0.1    127.0.0.53    DNS        85 Standard query 0x1d0b AAAA www.ietf.org OPT

Frame 16: 162 bytes on wire (1296 bits), 162 bytes captured (1296 bits) on interface 0
Linux cooked capture
Internet Protocol Version 4, Src: 127.0.0.53, Dst: 127.0.0.1
User Datagram Protocol, Src Port: 53, Dst Port: 42121
Domain Name System (response)
    Transaction ID: 0x18e9
    Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 3
    Authority RRs: 0
    Additional RRs: 1
    Queries
        www.ietf.org: type A, class IN
    Answers
        www.ietf.org: type CNAME, class IN, cname www.ietf.org.cdn.cloudflare.net
        www.ietf.org.cdn.cloudflare.net: type A, class IN, addr 104.20.1.85
        www.ietf.org.cdn.cloudflare.net: type A, class IN, addr 104.20.0.85
    Additional records
        <Root>: type OPT
    [Request In: 9]
    [Time: 0.338530562 seconds]
```

When we run the wireshark capture, we could see that there are multiple DNS requests that our host sends. However, except for the first request, all the others are handled by the cached entry within our system. This local DNS cache has the corresponding IP : 127.0.0.53. This can be seen from the wireshark capture named "Q10_1" as well as the image above.

Question 11:



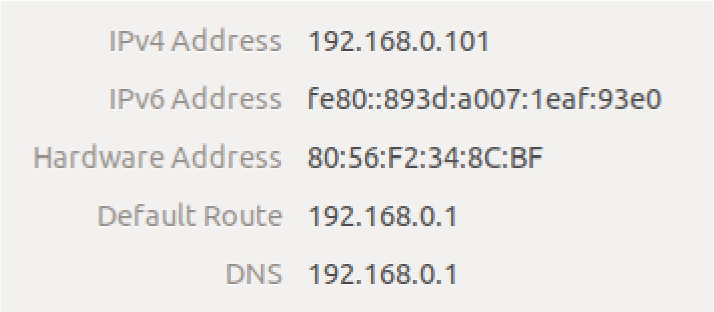
```
  16 2.923730864  172.217.163.196  192.168.0.101    TLSv1.2  112 Application Data
  17 2.941961788  192.168.0.101    192.168.0.1      DNS       71 Standard query 0x84f8 A www.mit.edu
  18 2.967301308  192.168.0.101    172.217.163.196  TCP       66 40220 → 443 [ACK] Seq=47 Ack=47 Win=404 Len=0 TSval=18463187
  19 2.967324990  192.168.0.101    172.217.31.202   TCP       66 48590 → 443 [ACK] Seq=47 Ack=47 Win=262 Len=0 TSval=65122155
  20 2.984957769  192.168.0.1      192.168.0.101    DNS      160 Standard query response 0x84f8 A www.mit.edu CNAME www.mit.e
  21 2.985912345  192.168.0.101    192.168.0.1      DNS       85 Standard query 0x845f AAAA e9566.dscb.akamaiedge.net
  22 2.991625252  192.168.0.1      192.168.0.101    DNS      141 Standard query response 0x845f AAAA e9566.dscb.akamaiedge.ne

Frame 17: 71 bytes on wire (568 bits), 71 bytes captured (568 bits) on interface 0
Ethernet II, Src: HonHaiPr_34:8c:bf (80:56:f2:34:8c:bf), Dst: Tp-LinkT_72:d9:ce (18:a6:f7:72:d9:ce)
Internet Protocol Version 4, Src: 192.168.0.101, Dst: 192.168.0.1
User Datagram Protocol, Src Port: 38241, Dst Port: 53
Domain Name System (query)
    Transaction ID: 0x84f8
    Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0

0000  18 a6 f7 72 d9 ce 80 56  f2 34 8c bf 08 00 45 00   ···r···V ·4····E·
0010  00 39 bf e3 40 00 40 11  f9 19 c0 a8 00 65 c0 a8   ·9··@·@· ·····e··
0020  00 01 95 61 00 35 00 25  10 b3 84 f8 01 00 00 01   ···a·5·% ········
0030  00 00 00 00 00 00 03 77  77 77 03 6d 69 74 03 65   ·······w ww·mit·e
0040  64 75 00 00 01 00 01                               du·····
```

From the above figure, we can find that, for DNS query:
Destination port : 53 (Standard DNS incoming UDP port)

Source port : 38241 (unassigned)

Question 12:

In the figure attached in Question 11, we can see that the query message is **sent from 192.168.0.101 to 192.168.0.1**



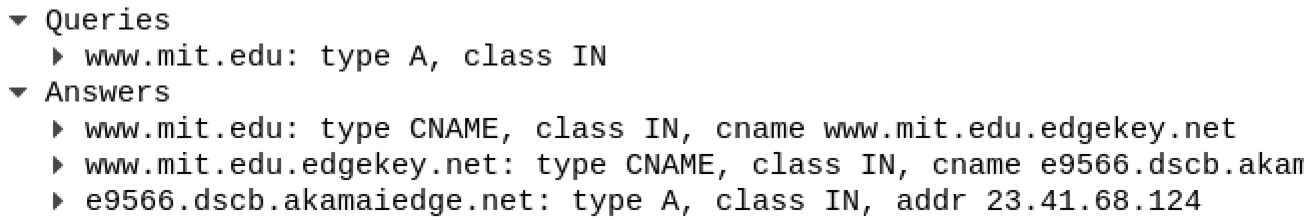
IPv4 Address	192.168.0.101
IPv6 Address	fe80::893d:a007:1eaf:93e0
Hardware Address	80:56:F2:34:8C:BF
Default Route	192.168.0.1
DNS	192.168.0.1

The source IP corresponds to our machine's private IP assigned. The destination IP **corresponds to the default DNS server** contacted by the system. This can be seen from the network specifications of our system seen in network tools.

Question 13:

In the packet selected (Figure in Question 11), on observing the body of the message (not visible in the picture, refer : Q11miteduNSLOOKUP2.pcapng)that contains the DNS query message, we can find that the type of the record bein searched for is 'A'. Thus the query is of type 'A' - indicating that it is interested to find the IPv4 address of the domain (mit.edu). Also on further inspection, we find that this query has no super-field called answers. Therefore there are no answers in the query message, as it is expected.

Question 14:



```
▾ Queries
  ▸ www.mit.edu: type A, class IN
▾ Answers
  ▸ www.mit.edu: type CNAME, class IN, cname www.mit.edu.edgekey.net
  ▸ www.mit.edu.edgekey.net: type CNAME, class IN, cname e9566.dscb.akam
  ▸ e9566.dscb.akamaiedge.net: type A, class IN, addr 23.41.68.124
```

We can find the corresponding query response message by matching the transactionID in the DNS body of the message. Here the ID takes the value : 0x84f8. On inspecting the super-field 'answers' in the response packet, we find that there are three answers present.

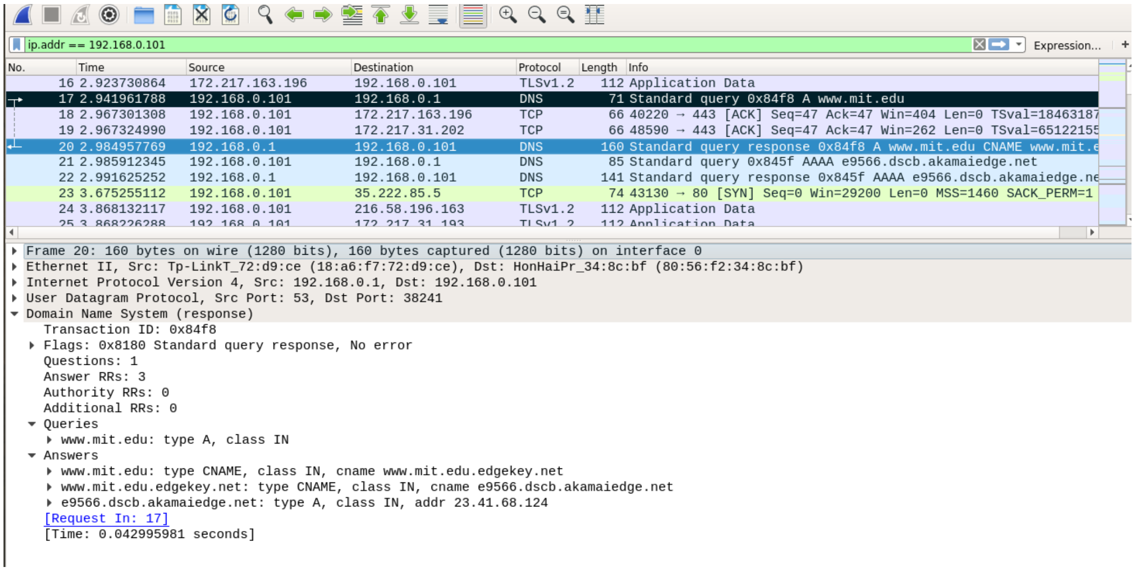
The answers are :
Answer 1 : type CNAME record <mit.edu, mit.edu.edgekey.net>

Answer 2 : type CNAME record <mit.edu.edgekey.net, e9566.dscb.akamaiedge.net>
Note that the answers 1,2 are crucial in the process of IP retrieval because the actual 'type A' record containing the IPv4 address of our interest has the canonical name of the url and not the original name 'mit.edu'.

Answer 3 : type A record <e9566.dscb.akamaiedge.net, 23.41.68.124>

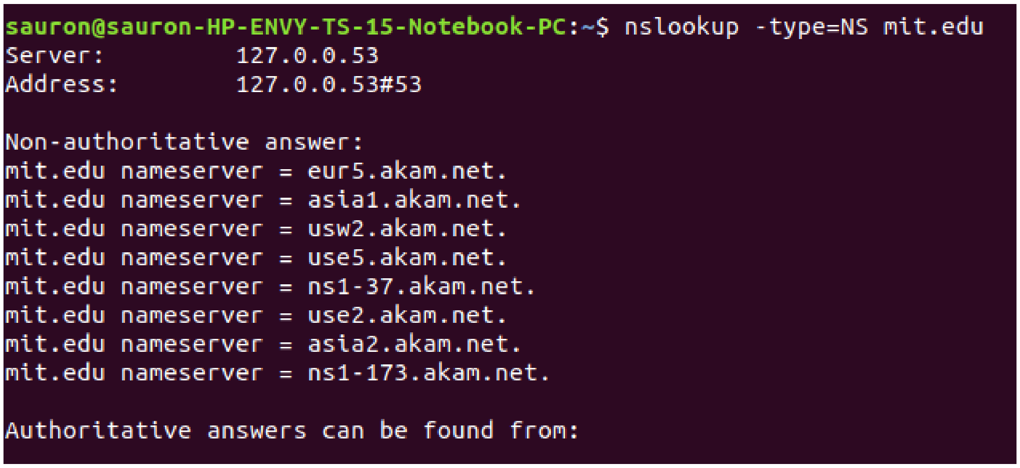
Question 15:

Showing the extended screenshot for the same. The highlighted packet is the DNS query response and the packed marked in black corresponds to our DNS query.



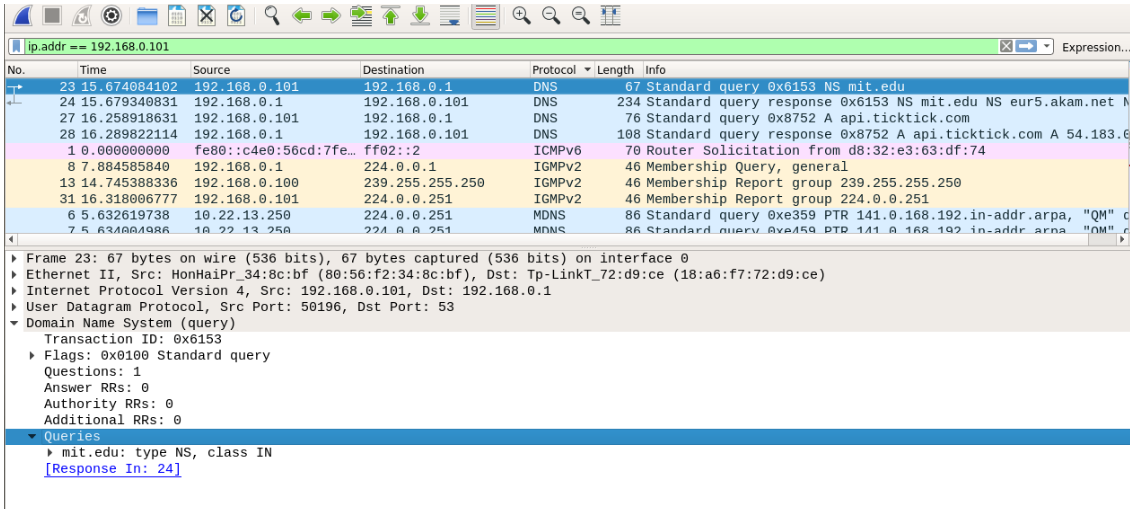
```
ip.addr == 192.168.0.101

No.     Time          Source            Destination       Protocol  Length Info
     16 2.923730864   172.217.163.196   192.168.0.101     TLSv1.2   112 Application Data
     17 2.941961788   192.168.0.101     192.168.0.1       DNS        71 Standard query 0x84f8 A www.mit.edu
     18 2.967301308   192.168.0.101     172.217.163.196   TCP        66 40220 → 443 [ACK] Seq=47 Ack=47 Win=404 Len=0 TSval=18463187
     19 2.967324990   192.168.0.101     172.217.31.202    TCP        66 48590 → 443 [ACK] Seq=47 Ack=47 Win=262 Len=0 TSval=65122155
     20 2.984957769   192.168.0.1       192.168.0.101     DNS       160 Standard query response 0x84f8 A www.mit.edu CNAME www.mit.e
     21 2.985912345   192.168.0.101     192.168.0.1       DNS        85 Standard query 0x845f AAAA e9566.dscb.akamaiedge.net
     22 2.991625252   192.168.0.1       192.168.0.101     DNS       141 Standard query response 0x845f AAAA e9566.dscb.akamaiedge.ne
     23 3.675255112   192.168.0.101     35.222.85.5       TCP        74 43130 → 80 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1
     24 3.868132117   192.168.0.101     216.58.196.163    TLSv1.2   112 Application Data
     25 3.868226288   192.168.0.101     172.217.31.193    TLSv1.2   112 Application Data

▸ Frame 20: 160 bytes on wire (1280 bits), 160 bytes captured (1280 bits) on interface 0
▸ Ethernet II, Src: Tp-LinkT_72:d9:ce (18:a6:f7:72:d9:ce), Dst: HonHaiPr_34:8c:bf (80:56:f2:34:8c:bf)
▸ Internet Protocol Version 4, Src: 192.168.0.1, Dst: 192.168.0.101
▸ User Datagram Protocol, Src Port: 53, Dst Port: 38241
▾ Domain Name System (response)
    Transaction ID: 0x84f8
  ▸ Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 3
    Authority RRs: 0
    Additional RRs: 0
  ▾ Queries
    ▸ www.mit.edu: type A, class IN
  ▾ Answers
    ▸ www.mit.edu: type CNAME, class IN, cname www.mit.edu.edgekey.net
    ▸ www.mit.edu.edgekey.net: type CNAME, class IN, cname e9566.dscb.akamaiedge.net
    ▸ e9566.dscb.akamaiedge.net: type A, class IN, addr 23.41.68.124
    [Request In: 17]
    [Time: 0.042995981 seconds]
```

Question 16:



```
sauron@sauron-HP-ENVY-TS-15-Notebook-PC:~$ nslookup -type=NS mit.edu
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
mit.edu nameserver = eur5.akam.net.
mit.edu nameserver = asia1.akam.net.
mit.edu nameserver = usw2.akam.net.
mit.edu nameserver = use5.akam.net.
mit.edu nameserver = ns1-37.akam.net.
mit.edu nameserver = use2.akam.net.
mit.edu nameserver = asia2.akam.net.
mit.edu nameserver = ns1-173.akam.net.

Authoritative answers can be found from:
```

Wireshark capture for the same :



ip.addr == 192.168.0.101

```
No.   Time          Source                   Destination      Protocol Length Info
   23 15.674084102  192.168.0.101            192.168.0.1      DNS       67 Standard query 0x6153 NS mit.edu
   24 15.679340831  192.168.0.1              192.168.0.101    DNS      234 Standard query response 0x6153 NS mit.edu NS eur5.akam.net N
   27 16.258918631  192.168.0.101            192.168.0.1      DNS       76 Standard query 0x8752 A api.ticktick.com
   28 16.289822114  192.168.0.1              192.168.0.101    DNS      108 Standard query response 0x8752 A api.ticktick.com A 54.183.0
    1 0.000000000   fe80::c4e0:56cd:7fe…     ff02::2          ICMPv6    70 Router Solicitation from d8:32:e3:63:df:74
    8 7.884585840   192.168.0.1              224.0.0.1        IGMPv2    46 Membership Query, general
   13 14.745388336  192.168.0.100            239.255.255.250  IGMPv2    46 Membership Report group 239.255.255.250
   31 16.318006777  192.168.0.101            224.0.0.251      IGMPv2    46 Membership Report group 224.0.0.251
    6 5.632619738   10.22.13.250             224.0.0.251      MDNS      86 Standard query 0xe359 PTR 141.0.168.192.in-addr.arpa, "QM" c
    7 5.634004986   10.22.13.250             224.0.0.251      MDNS      86 Standard query 0xe459 PTR 141.0.168.192.in-addr.arpa, "QM" c
```

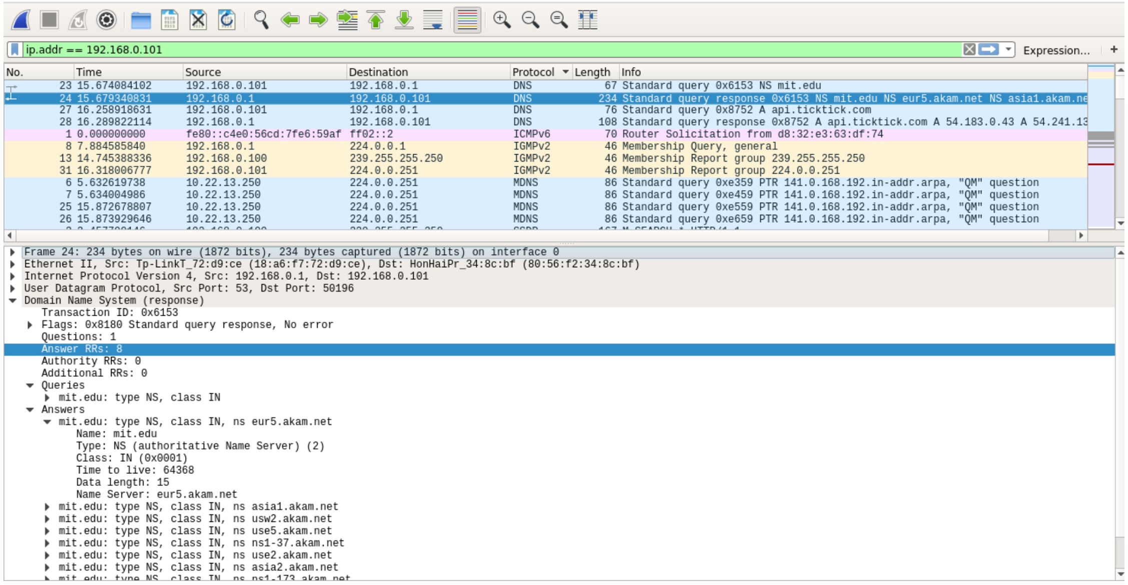
```
▸ Frame 23: 67 bytes on wire (536 bits), 67 bytes captured (536 bits) on interface 0
▸ Ethernet II, Src: HonHaiPr_34:8c:bf (80:56:f2:34:8c:bf), Dst: Tp-LinkT_72:d9:ce (18:a6:f7:72:d9:ce)
▸ Internet Protocol Version 4, Src: 192.168.0.101, Dst: 192.168.0.1
▸ User Datagram Protocol, Src Port: 50196, Dst Port: 53
▾ Domain Name System (query)
    Transaction ID: 0x6153
  ▸ Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  ▾ Queries
    ▸ mit.edu: type NS, class IN
    [Response In: 24]
```

We can see, from the figure above, corresponding to the query packet sent from our machine : 192.168.0.101 to the destination host whose IP is : **192.168.0.1.** From the figure in Q12, we can see that this **corresponds to the default local DNS server.**

Question 17:

On expanding the packet details in wireshark, we see that the query message is of the 'type NS'. This is the type of query sent when the interest is to know the authoritative DNS servers of the given domain name. On further inspection, we see that there is no super-field named 'answers' in the query message. Hence the query message has no answers, as is expected.

Question 18:



```
No.   Time          Source                     Destination        Protocol  Length  Info
   23 15.674084102  192.168.0.101              192.168.0.1        DNS           67 Standard query 0x6153 NS mit.edu
   24 15.679340831  192.168.0.1                192.168.0.101      DNS          234 Standard query response 0x6153 NS mit.edu NS eur5.akam.net NS asia1.akam.ne
   27 16.258918631  192.168.0.101              192.168.0.1        DNS           76 Standard query 0x8752 A api.ticktick.com
   28 16.289822114  192.168.0.1                192.168.0.101      DNS          108 Standard query response 0x8752 A api.ticktick.com A 54.183.0.43 A 54.241.13
    1 0.000000000   fe80::c4e0:56cd:7fe6:59af  ff02::2            ICMPv6        70 Router Solicitation from d8:32:e3:63:df:74
    8 7.884585840   192.168.0.1                224.0.0.1          IGMPv2        46 Membership Query, general
   13 14.745388336  192.168.0.100              239.255.255.250    IGMPv2        46 Membership Report group 239.255.255.250
   31 16.318006777  192.168.0.101              224.0.0.251        IGMPv2        46 Membership Report group 224.0.0.251
    6 5.632619738   10.22.13.250               224.0.0.251        MDNS          86 Standard query 0xe359 PTR 141.0.168.192.in-addr.arpa, "QM" question
    7 5.634004986   10.22.13.250               224.0.0.251        MDNS          86 Standard query 0xe459 PTR 141.0.168.192.in-addr.arpa, "QM" question
   25 15.872678807  10.22.13.250               224.0.0.251        MDNS          86 Standard query 0xe559 PTR 141.0.168.192.in-addr.arpa, "QM" question
   26 15.873929646  10.22.13.250               224.0.0.251        MDNS          86 Standard query 0xe659 PTR 141.0.168.192.in-addr.arpa, "QM" question
```

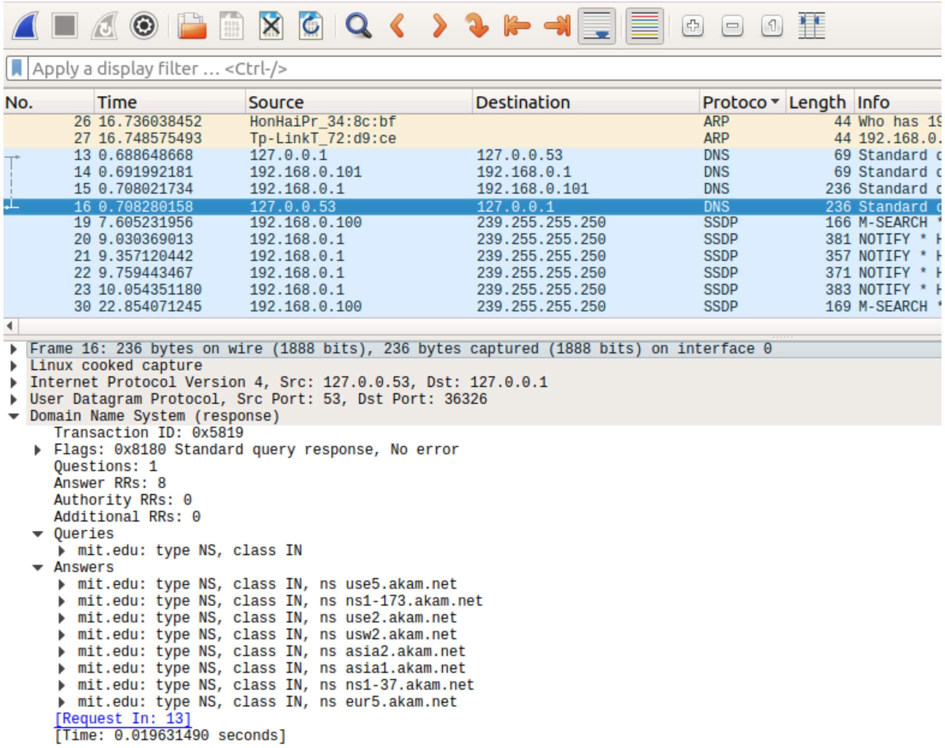
```
▸ Frame 24: 234 bytes on wire (1872 bits), 234 bytes captured (1872 bits) on interface 0
▸ Ethernet II, Src: Tp-LinkT_72:d9:ce (18:a6:f7:72:d9:ce), Dst: HonHaiPr_34:8c:bf (80:56:f2:34:8c:bf)
▸ Internet Protocol Version 4, Src: 192.168.0.1, Dst: 192.168.0.101
▸ User Datagram Protocol, Src Port: 53, Dst Port: 50196
▾ Domain Name System (response)
    Transaction ID: 0x6153
  ▸ Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 8
    Authority RRs: 0
    Additional RRs: 0
  ▾ Queries
    ▸ mit.edu: type NS, class IN
  ▾ Answers
    ▾ mit.edu: type NS, class IN, ns eur5.akam.net
         Name: mit.edu
         Type: NS (authoritative Name Server) (2)
         Class: IN (0x0001)
         Time to live: 64368
         Data length: 15
         Name Server: eur5.akam.net
    ▸ mit.edu: type NS, class IN, ns asia1.akam.net
    ▸ mit.edu: type NS, class IN, ns usw2.akam.net
    ▸ mit.edu: type NS, class IN, ns use5.akam.net
    ▸ mit.edu: type NS, class IN, ns ns1-37.akam.net
    ▸ mit.edu: type NS, class IN, ns use2.akam.net
    ▸ mit.edu: type NS, class IN, ns asia2.akam.net
    ▸ mit.edu: type NS, class IN, ns ns1-173.akam.net
```

In the response message, we can find the following **nameservers for MIT** :

1) eur5.akam.net
2) asia1.akam.net.
3) usw2.akam.net.
4) use5.akam.net.
5) ns1-37.akam.net.
6) use2.akam.net.
7) asia2.akam.net.
8) ns1-173.akam.net.

Also in each answer, we do not find a field corresponding to the IP address of the related nameserver. Therefore, **nslookup with the option : 'type=NS' does not return any IP addresses**. This is because, the NS type records that are being queried for, do not contain the field IP address in them. They only have <domain name, auth-dns server name, ttl> fields.

Question 19:



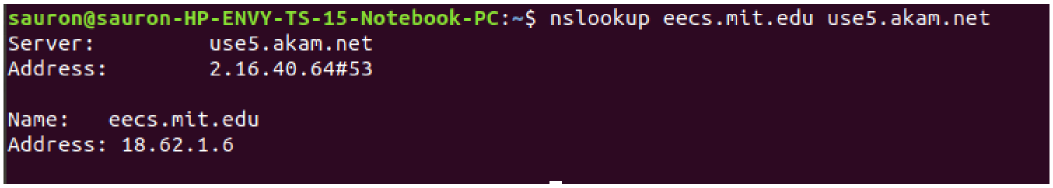
Apply a display filter … <Ctrl-/>

```
No.    Time           Source              Destination         Protoco  Length Info
    26 16.736038452   HonHaiPr_34:8c:bf                       ARP          44 Who has 19
    27 16.748575493   Tp-LinkT_72:d9:ce                       ARP          44 192.168.0.
    13 0.688648668    127.0.0.1           127.0.0.53          DNS          69 Standard c
    14 0.691992181    192.168.0.101       192.168.0.1         DNS          69 Standard c
    15 0.708021734    192.168.0.1         192.168.0.101       DNS         236 Standard c
    16 0.708280158    127.0.0.53          127.0.0.1           DNS         236 Standard c
    19 7.605231956    192.168.0.100       239.255.255.250     SSDP        166 M-SEARCH *
    20 9.030369013    192.168.0.1         239.255.255.250     SSDP        381 NOTIFY * H
    21 9.357120442    192.168.0.1         239.255.255.250     SSDP        357 NOTIFY * H
    22 9.759443467    192.168.0.1         239.255.255.250     SSDP        371 NOTIFY * H
    23 10.054351180   192.168.0.1         239.255.255.250     SSDP        383 NOTIFY * H
    30 22.854071245   192.168.0.100       239.255.255.250     SSDP        169 M-SEARCH *
```

```
▸ Frame 16: 236 bytes on wire (1888 bits), 236 bytes captured (1888 bits) on interface 0
▸ Linux cooked capture
▸ Internet Protocol Version 4, Src: 127.0.0.53, Dst: 127.0.0.1
▸ User Datagram Protocol, Src Port: 53, Dst Port: 36326
▾ Domain Name System (response)
    Transaction ID: 0x5819
  ▸ Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 8
    Authority RRs: 0
    Additional RRs: 0
  ▾ Queries
    ▸ mit.edu: type NS, class IN
  ▾ Answers
    ▸ mit.edu: type NS, class IN, ns use5.akam.net
    ▸ mit.edu: type NS, class IN, ns ns1-173.akam.net
    ▸ mit.edu: type NS, class IN, ns use2.akam.net
    ▸ mit.edu: type NS, class IN, ns usw2.akam.net
    ▸ mit.edu: type NS, class IN, ns asia2.akam.net
    ▸ mit.edu: type NS, class IN, ns asia1.akam.net
    ▸ mit.edu: type NS, class IN, ns ns1-37.akam.net
    ▸ mit.edu: type NS, class IN, ns eur5.akam.net
    [Request In: 13]
    [Time: 0.019631490 seconds]
```

The figure above shows the wireshark capture details for Questions 16 to 18.

Question 20:



```
sauron@sauron-HP-ENVY-TS-15-Notebook-PC:~$ nslookup eecs.mit.edu use5.akam.net
Server:         use5.akam.net
Address:        2.16.40.64#53

Name:   eecs.mit.edu
Address: 18.62.1.6
```

Command used : nslookup eecs.mit.edu use5.akam.net (EEnCS dept. of MIT)
On expanding the packet corresponding to the primary query of our nslookup, we can see that the source address is : 192.168.0.101 whereas the destination address is : 2.16.40.64. From our previous inspection of system network specifications, we can tell that this is not our default DNS server but is infact the **DNS server mentioned in the command**. Infact this is the meaning

of nslookup where we specify the DNS server to be contacted (if this is not mentioned, the query goes to our default server).

It is interesting to see that this IP address is obtained by DNS queries preceeding the main query. Thus the **nslookup to a specific server is a two step iterative process** of finding the IP address of DNS server (here : 2.16.40.64) and then querying into that DNS server.

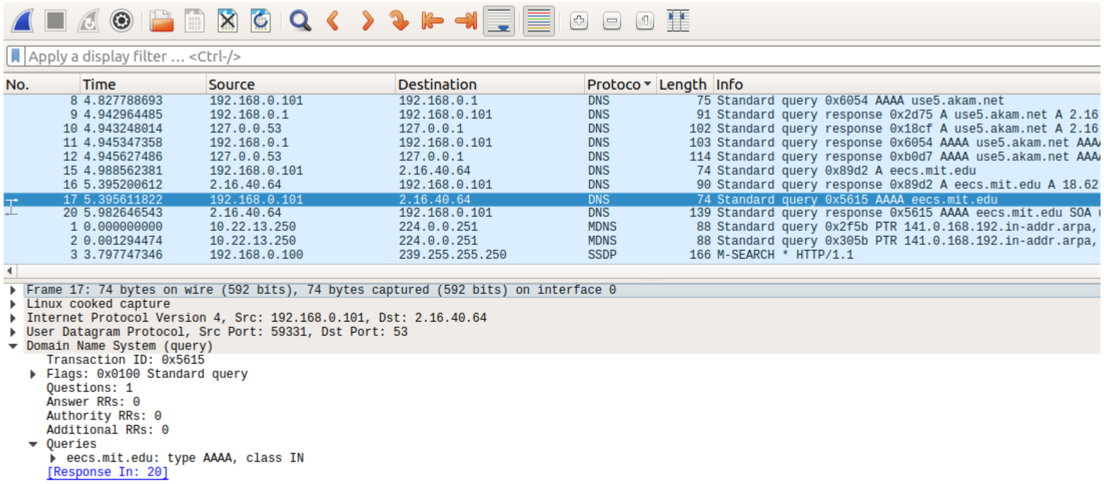
Question 21:

After expanding the query packet on wireshark, observing the body of the message that contains the DNS query message, we can find that the type of the record bein searched for is 'A'. Thus the query is of **type 'A'** - indicating that it is interested to find the IPv4 address of the domain (eecs.mit.edu). Also on further inspection, we find that this query has no super-field called answers. Therefore there are no answers in the query message, as it is expected.

Question 22:

Expanding the response message shows us that there is only one answer. This is a type A record, matching with our type A query sent previously. On insepection we find that the response IPaddress is : **18.62.1.6.** There is **only one answer** here (this means that the domain name has no aliases).

Question 23:



```
No.        Time          Source           Destination      Protoco  Length Info
         8 4.827788693   192.168.0.101    192.168.0.1      DNS          75 Standard query 0x6054 AAAA use5.akam.net
         9 4.942964485   192.168.0.1      192.168.0.101    DNS          91 Standard query response 0x2d75 A use5.akam.net A 2.16
        10 4.943248014   127.0.0.53       127.0.0.1        DNS         102 Standard query response 0x18cf A use5.akam.net A 2.16
        11 4.945347358   192.168.0.1      192.168.0.101    DNS         103 Standard query response 0x6054 AAAA use5.akam.net AAA
        12 4.945627486   127.0.0.53       127.0.0.1        DNS         114 Standard query response 0xb0d7 AAAA use5.akam.net AAA
        15 4.988562381   192.168.0.101    2.16.40.64       DNS          74 Standard query 0x89d2 A eecs.mit.edu
        16 5.395200612   2.16.40.64       192.168.0.101    DNS          90 Standard query response 0x89d2 A eecs.mit.edu A 18.62
        17 5.395611822   192.168.0.101    2.16.40.64       DNS          74 Standard query 0x5615 AAAA eecs.mit.edu
        20 5.982646543   2.16.40.64       192.168.0.101    DNS         139 Standard query response 0x5615 AAAA eecs.mit.edu SOA
         1 0.000000000   10.22.13.250     224.0.0.251      MDNS         88 Standard query 0x2f5b PTR 141.0.168.192.in-addr.arpa,
         2 0.001294474   10.22.13.250     224.0.0.251      MDNS         88 Standard query 0x305b PTR 141.0.168.192.in-addr.arpa,
         3 3.797747346   192.168.0.100    239.255.255.250  SSDP        166 M-SEARCH * HTTP/1.1
```

```
▸ Frame 17: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0
▸ Linux cooked capture
▸ Internet Protocol Version 4, Src: 192.168.0.101, Dst: 2.16.40.64
▸ User Datagram Protocol, Src Port: 59331, Dst Port: 53
▾ Domain Name System (query)
     Transaction ID: 0x5615
   ▸ Flags: 0x0100 Standard query
     Questions: 1
     Answer RRs: 0
     Authority RRs: 0
     Additional RRs: 0
   ▾ Queries
       ▸ eecs.mit.edu: type AAAA, class IN
     [Response In: 20]
```

This figure corresponds to the wireshark capture for questions 20 to 23.

Wireshark Capture filenames:

Q5-11 : ietfDNS.pcapng, Q10_1.pcapng
Q11-15 : Q11miteduNSLOOKUP2.pcapng
Q16-19 : Q16_19.pcapng
Q20-23 : Q20_23.pcapng