1.

```
madhav@ubuntu:~$ nslookup www.iith.ac.in
Server:         164.100.3.1
Address:        164.100.3.1#53

Non-authoritative answer:
Name:   www.iith.ac.in
Address: 218.248.6.135
```

2.

```
madhav@ubuntu:~$ nslookup -type=NS kent.ac.uk
Server:         164.100.17.3
Address:        164.100.17.3#53

Non-authoritative answer:
kent.ac.uk      nameserver = dns0.ukc.ac.uk.
kent.ac.uk      nameserver = cancer.ucs.ed.ac.uk.
kent.ac.uk      nameserver = dns1.ukc.ac.uk.
kent.ac.uk      nameserver = dns0.kent.ac.uk.
kent.ac.uk      nameserver = dns1.kent.ac.uk.

Authoritative answers can be found from:
dns0.ukc.ac.uk  internet address = 129.12.21.8
cancer.ucs.ed.ac.uk     internet address = 129.215.200.7
cancer.ucs.ed.ac.uk     internet address = 129.215.166.13
```

3.

```
madhav@ubuntu:~$ nslookup -type=MX yahoo.com cancer.ucs.ed.ac.uk
Server:         cancer.ucs.ed.ac.uk
Address:        129.215.200.7#53

Non-authoritative answer:
yahoo.com       mail exchanger = 1 mta6.am0.yahoodns.net.
yahoo.com       mail exchanger = 1 mta7.am0.yahoodns.net.
yahoo.com       mail exchanger = 1 mta5.am0.yahoodns.net.

Authoritative answers can be found from:
yahoo.com       nameserver = ns1.yahoo.com.
yahoo.com       nameserver = ns6.yahoo.com.
yahoo.com       nameserver = ns3.yahoo.com.
yahoo.com       nameserver = ns5.yahoo.com.
yahoo.com       nameserver = ns4.yahoo.com.
yahoo.com       nameserver = ns2.yahoo.com.
yahoo.com       nameserver = ns8.yahoo.com.
ns1.yahoo.com internet address = 68.180.131.16
ns6.yahoo.com internet address = 202.43.223.170
ns3.yahoo.com internet address = 121.101.152.99
ns5.yahoo.com internet address = 119.160.247.124
ns4.yahoo.com internet address = 68.142.196.63
ns2.yahoo.com internet address = 68.142.255.16
ns8.yahoo.com internet address = 202.165.104.22
```

```
madhav@ubuntu:~$ nslookup mta6.am0.yahoodns.net cancer.ucs.ed.ac.uk
Server:         cancer.ucs.ed.ac.uk
Address:        129.215.166.13#53

Non-authoritative answer:
Name:  mta6.am0.yahoodns.net
Address: 66.94.237.139
Name:  mta6.am0.yahoodns.net
Address: 67.195.103.232
Name:  mta6.am0.yahoodns.net
Address: 67.195.103.233
Name:  mta6.am0.yahoodns.net
Address: 67.195.168.230
Name:  mta6.am0.yahoodns.net
Address: 74.6.136.65
Name:  mta6.am0.yahoodns.net
Address: 74.6.140.64
Name:  mta6.am0.yahoodns.net
Address: 209.191.88.254
Name:  mta6.am0.yahoodns.net
Address: 66.94.237.64
```

4.

Query:

```
No.     Time            Source                Destination           Protocol Info
    506 11:22:39.127058 192.168.1.110         192.168.1.1           DNS      Standard query A
www.ietf.org

Frame 506 (72 bytes on wire, 72 bytes captured)
Ethernet II, Src: IntelCor_c9:cc:96 (00:1c:bf:c9:cc:96), Dst: Cisco-Li_1c:8e:65 (00:25:9c:1c:8e:65)
Internet Protocol, Src: 192.168.1.110 (192.168.1.110), Dst: 192.168.1.1 (192.168.1.1)
User Datagram Protocol, Src Port: 36671 (36671), Dst Port: domain (53)
Domain Name System (query)
```

Response:

```
No.     Time            Source                Destination           Protocol Info
    507 11:22:39.128218 192.168.1.1           192.168.1.110         DNS      Standard query response A
12.22.58.30

Frame 507 (88 bytes on wire, 88 bytes captured)
Ethernet II, Src: Cisco-Li_1c:8e:65 (00:25:9c:1c:8e:65), Dst: IntelCor_c9:cc:96 (00:1c:bf:c9:cc:96)
Internet Protocol, Src: 192.168.1.1 (192.168.1.1), Dst: 192.168.1.110 (192.168.1.110)
User Datagram Protocol, Src Port: domain (53), Dst Port: 36671 (36671)
Domain Name System (response)
```

UDP protocol

5.

53,53

6.
192.168.1.1 - ROUTER'S IP
192.168.1.1 - router's ip

7.
Standard query of type A
No

8.
ONE

```
Answers
    www.ietf.org: type A, class IN, addr 12.22.58.30
        Name: www.ietf.org
        Type: A (Host address)
        Class: IN (0x0001)
        Time to live: 22 minutes, 34 seconds
        Data length: 4
        Addr: 12.22.58.30
```

9.
NO.Ip addresses provided in the response message correspond to 12.22.58.30
But due to proxy, SYN packets are directed to 192.168.0.52. Without proxy they would have gone to 12.22.58.30

10.
No

11.
53,53

12.
192.168.1.1
My default ocal DNS server is my router with ip = 192.168.1.1. The DNS server for this router is again our proxy 192.168.0.4.From hostel, the default DNS server is the router. From institute, without proxy,the dafault DNS server is
164.100.3.1

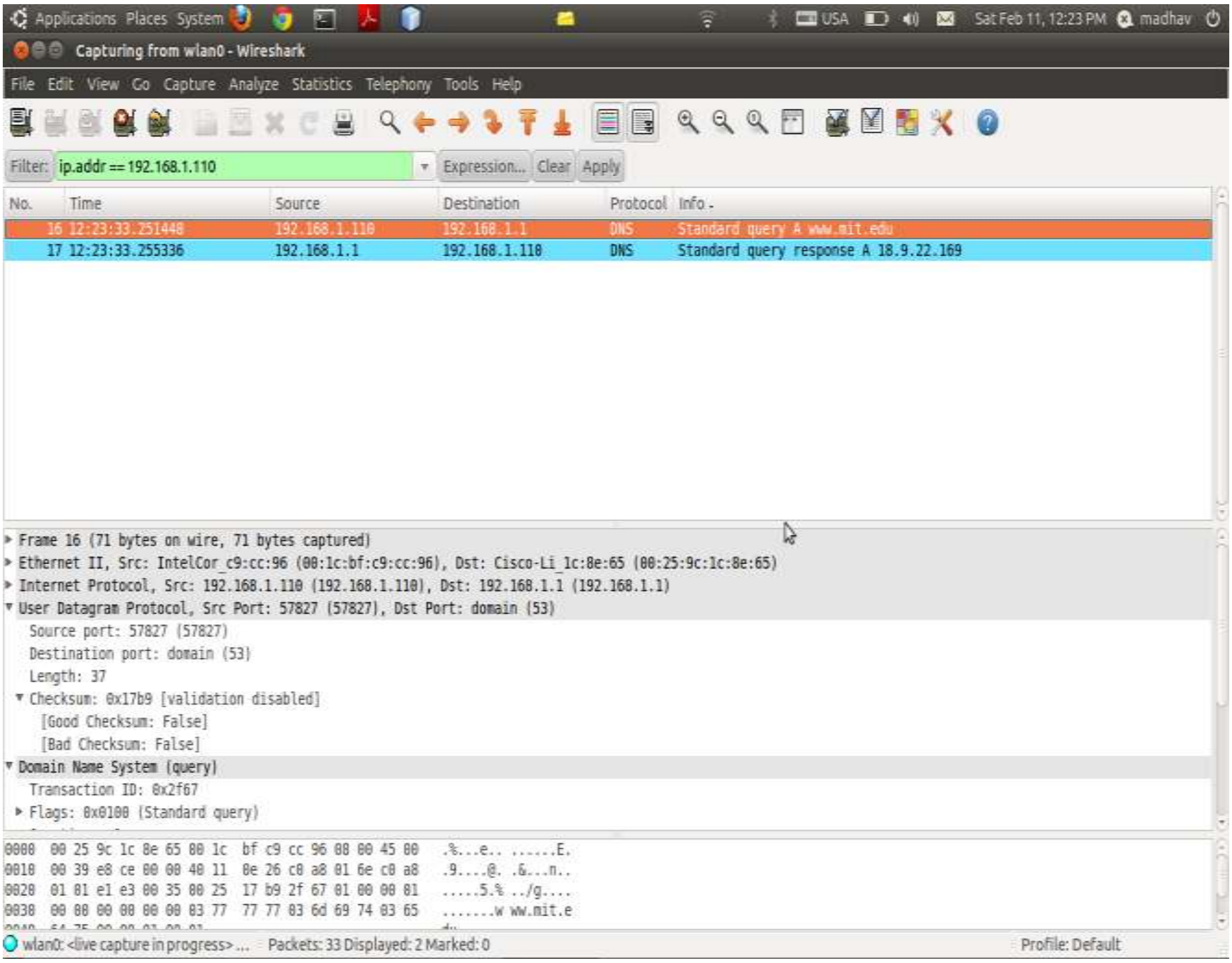
13.
Standard query of type A
No

14.
ONE

```
Answers
    www.mit.edu: type A, class IN, addr 18.9.22.169
        Name: www.mit.edu
        Type: A (Host address)
        Class: IN (0x0001)
        Time to live: 37 seconds
```

Data length: 4
Addr: 18.9.22.169

15.Screenshot


Applications Places System
USA
Sat Feb 11, 12:23 PM
madhav
Capturing from wlan0 - Wireshark
File Edit View Go Capture Analyze Statistics Telephony Tools Help
Expression...
Clear
Apply
Profile: Default

Filter: ip.addr == 192.168.1.110

```
No.   Time              Source          Destination     Protocol Info
   16 12:23:33.251448   192.168.1.110   192.168.1.1     DNS      Standard query A www.mit.edu
   17 12:23:33.255336   192.168.1.1     192.168.1.110   DNS      Standard query response A 18.9.22.169
```

```
▸ Frame 16 (71 bytes on wire, 71 bytes captured)
▸ Ethernet II, Src: IntelCor_c9:cc:96 (00:1c:bf:c9:cc:96), Dst: Cisco-Li_1c:8e:65 (00:25:9c:1c:8e:65)
▸ Internet Protocol, Src: 192.168.1.110 (192.168.1.110), Dst: 192.168.1.1 (192.168.1.1)
▾ User Datagram Protocol, Src Port: 57827 (57827), Dst Port: domain (53)
    Source port: 57827 (57827)
    Destination port: domain (53)
    Length: 37
  ▾ Checksum: 0x17b9 [validation disabled]
      [Good Checksum: False]
      [Bad Checksum: False]
▾ Domain Name System (query)
    Transaction ID: 0x2f67
  ▸ Flags: 0x0100 (Standard query)
```

```
0000  00 25 9c 1c 8e 65 00 1c  bf c9 cc 96 08 00 45 00   .%...e.. ......E.
0010  00 39 e8 ce 00 00 40 11  0e 26 c0 a8 01 6e c0 a8   .9....@. .&...n..
0020  01 01 e1 e3 00 35 00 25  17 b9 2f 67 01 00 00 01   .....5.% ../g....
0030  00 00 00 00 00 00 03 77  77 77 03 6d 69 74 03 65   .......w ww.mit.e
```

wlan0: <live capture in progress> ... Packets: 33 Displayed: 2 Marked: 0

16.
192.1681.1.1
Yes

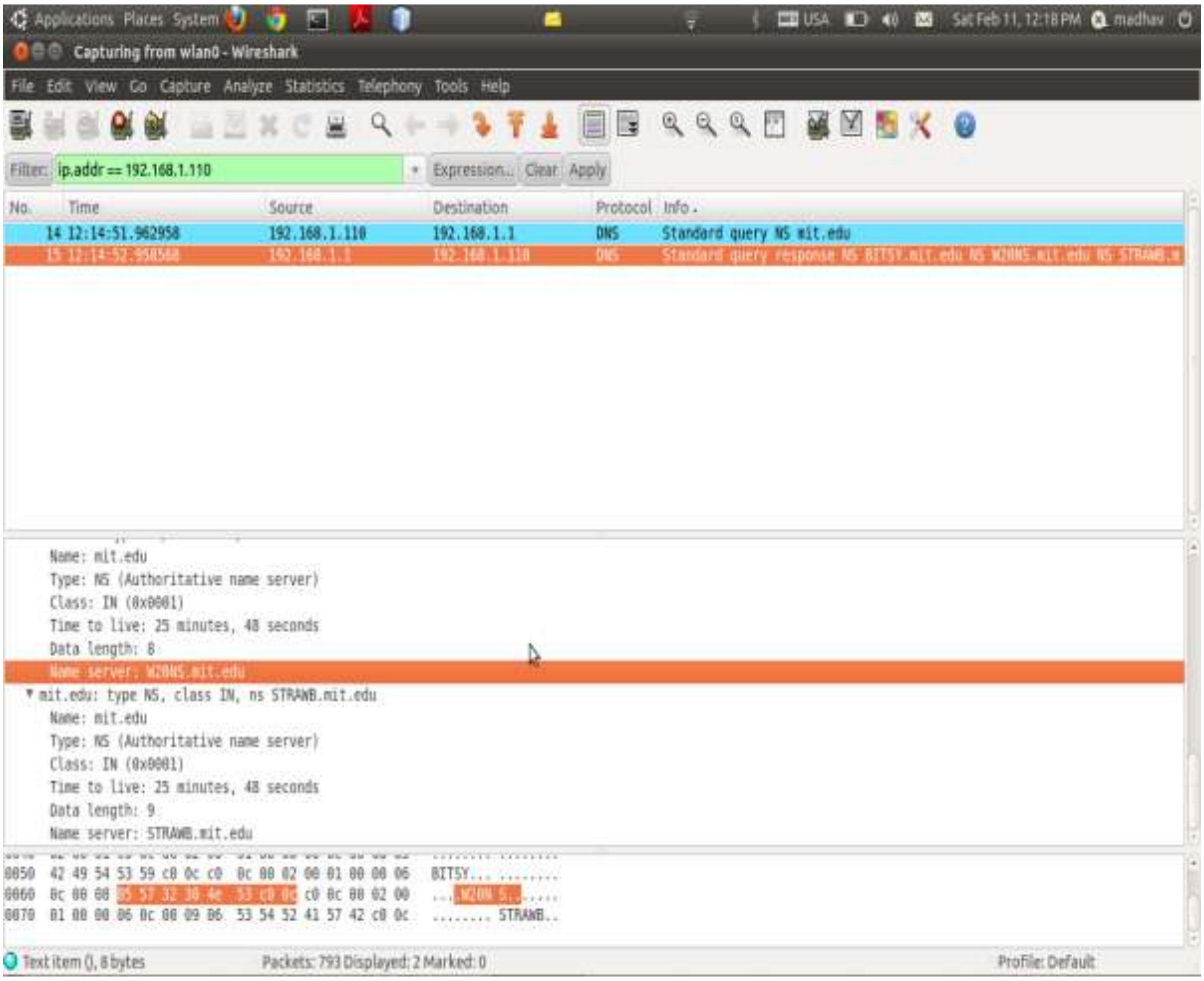
17.
Standard query of type NS
No

18.
mit.edunameserver = BITSY.mit.edu.
mit.edunameserver = W20NS.mit.edu.
mit.edunameserver = STRAWB.mit.edu.

No

19.

Screenshot


Applications Places System
Sat Feb 11, 12:18 PM madhav
Capturing from wlan0 - Wireshark
File Edit View Go Capture Analyze Statistics Telephony Tools Help
Expression... Clear Apply

Filter: ip.addr == 192.168.1.110

```
No.   Time               Source          Destination     Protocol  Info
   14 12:14:51.962958    192.168.1.110   192.168.1.1     DNS       Standard query NS mit.edu
   15 12:14:52.958568    192.168.1.1     192.168.1.110   DNS       Standard query response NS BITSY.mit.edu NS W20NS.mit.edu NS STRAWB.m
```

```
      Name: mit.edu
      Type: NS (Authoritative name server)
      Class: IN (0x0001)
      Time to live: 25 minutes, 48 seconds
      Data length: 8
      Name server: W20NS.mit.edu
  ▾ mit.edu: type NS, class IN, ns STRAWB.mit.edu
      Name: mit.edu
      Type: NS (Authoritative name server)
      Class: IN (0x0001)
      Time to live: 25 minutes, 48 seconds
      Data length: 9
      Name server: STRAWB.mit.edu
```

```
0050  42 49 54 53 59 c0 0c c0  0c 00 02 00 01 00 00 06   BITSY... ........
0060  0c 00 08 05 57 32 30 4e  53 c0 0c c0 0c 00 02 00   ....W20N S.......
0070  01 00 00 06 0c 00 09 06  53 54 52 41 57 42 c0 0c   ........ STRAWB..
```

Text item (), 8 bytes   Packets: 793 Displayed: 2 Marked: 0   Profile: Default

20.

18.72.0.3, No ,bitsy.mit.edu

21.

Standard query of type A, No

22.

1

Answers

www.aiit.or.kr: type A, class IN, addr 121.254.171.27

Name: www.aiit.or.kr

Type: A (Host address)

Class: IN (0x0001)

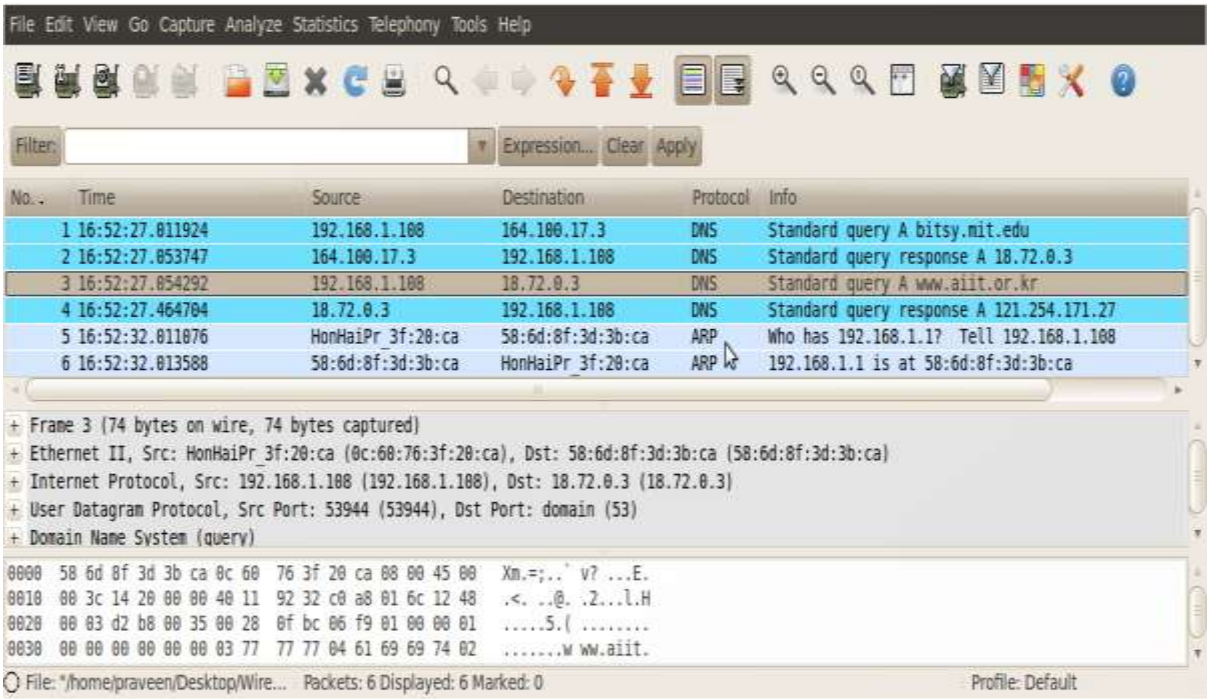
Time to live: 37 minutes, 26 seconds

Data length: 4

Addr: 121.254.171.27

23.

Screenshot



File Edit View Go Capture Analyze Statistics Telephony Tools Help
Filter:
Expression...
Clear
Apply

No.	Time	Source	Destination	Protocol	Info
1	16:52:27.011924	192.168.1.108	164.100.17.3	DNS	Standard query A bitsy.mit.edu
2	16:52:27.053747	164.100.17.3	192.168.1.108	DNS	Standard query response A 18.72.0.3
3	16:52:27.054292	192.168.1.108	18.72.0.3	DNS	Standard query A www.aiit.or.kr
4	16:52:27.464704	18.72.0.3	192.168.1.108	DNS	Standard query response A 121.254.171.27
5	16:52:32.011076	HonHaiPr_3f:20:ca	58:6d:8f:3d:3b:ca	ARP	Who has 192.168.1.1? Tell 192.168.1.108
6	16:52:32.013588	58:6d:8f:3d:3b:ca	HonHaiPr_3f:20:ca	ARP	192.168.1.1 is at 58:6d:8f:3d:3b:ca

```
+ Frame 3 (74 bytes on wire, 74 bytes captured)
+ Ethernet II, Src: HonHaiPr_3f:20:ca (0c:60:76:3f:20:ca), Dst: 58:6d:8f:3d:3b:ca (58:6d:8f:3d:3b:ca)
+ Internet Protocol, Src: 192.168.1.108 (192.168.1.108), Dst: 18.72.0.3 (18.72.0.3)
+ User Datagram Protocol, Src Port: 53944 (53944), Dst Port: domain (53)
+ Domain Name System (query)
```

```
0000  58 6d 8f 3d 3b ca 0c 60  76 3f 20 ca 08 00 45 00   Xm.=;..` v? ...E.
0010  00 3c 14 20 00 00 40 11  92 32 c0 a8 01 6c 12 48   .<. ..@. .2...l.H
0020  00 03 d2 b8 00 35 00 28  0f bc 06 f9 01 00 00 01   .....5.( ........
0030  00 00 00 00 00 00 03 77  77 77 04 61 69 69 74 02   .......w ww.aiit.
```

File: "/home/praveen/Desktop/Wire... Packets: 6 Displayed: 6 Marked: 0 Profile: Default