Foundation of Computer Networks - Wireshark Project
Bhavin Oza (bo2115)

1).

```
Bhavin@Ozas-MacBook-Pro ~ % nslookup www.rediff.com
Server:         66.253.214.16
Address:        66.253.214.16#53

Non-authoritative answer:
www.rediff.com  canonical name = rediff.com.edgekey.net.
rediff.com.edgekey.net  canonical name = e81366.a.akamaiedge.net.
Name:   e81366.a.akamaiedge.net
Address: 23.216.132.45
Name:   e81366.a.akamaiedge.net
Address: 23.216.132.56
```

IP: 23.216.132.45

2).

```
Bhavin@Ozas-MacBook-Pro ~ % nslookup -type=NS uoi.gr
Server:         66.253.214.16
Address:        66.253.214.16#53

Non-authoritative answer:
uoi.gr  nameserver = kouzina.noc.uoi.gr.
uoi.gr  nameserver = sns1.grnet.gr.
uoi.gr  nameserver = sns0.grnet.gr.
uoi.gr  nameserver = marina.noc.uoi.gr.

Authoritative answers can be found from:
marina.noc.uoi.gr       internet address = 195.130.120.120
kouzina.noc.uoi.gr      internet address = 195.130.120.110
```

IP: 195.130.120.110

Foundation of Computer Networks - Wireshark Project
Bhavin Oza (bo2115)

3).

```
Bhavin@Ozas-MacBook-Pro ~ % nslookup mail.yahoo.com 66.253.214.16
Server:         66.253.214.16
Address:        66.253.214.16#53

Non-authoritative answer:
mail.yahoo.com  canonical name = edge.gycpi.b.yahoodns.net.
Name:   edge.gycpi.b.yahoodns.net
Address: 69.147.82.60
Name:   edge.gycpi.b.yahoodns.net
Address: 69.147.82.61

Bhavin@Ozas-MacBook-Pro ~ %
```

Address: 69.147.82.60

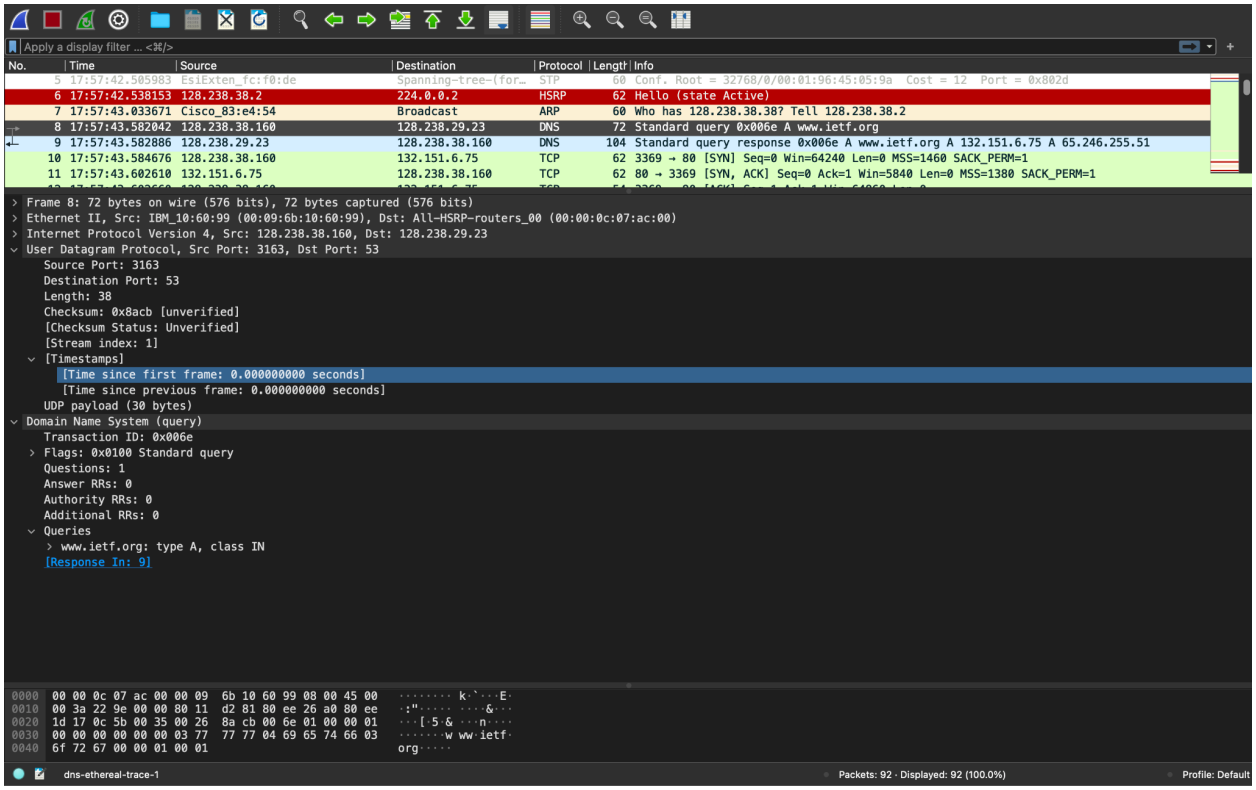
Using the dns-ethreal-trace-1 provided in zip
4). UDP

5). Destination port for DNS query: Port 53
Source port for DNS query response: Port 53

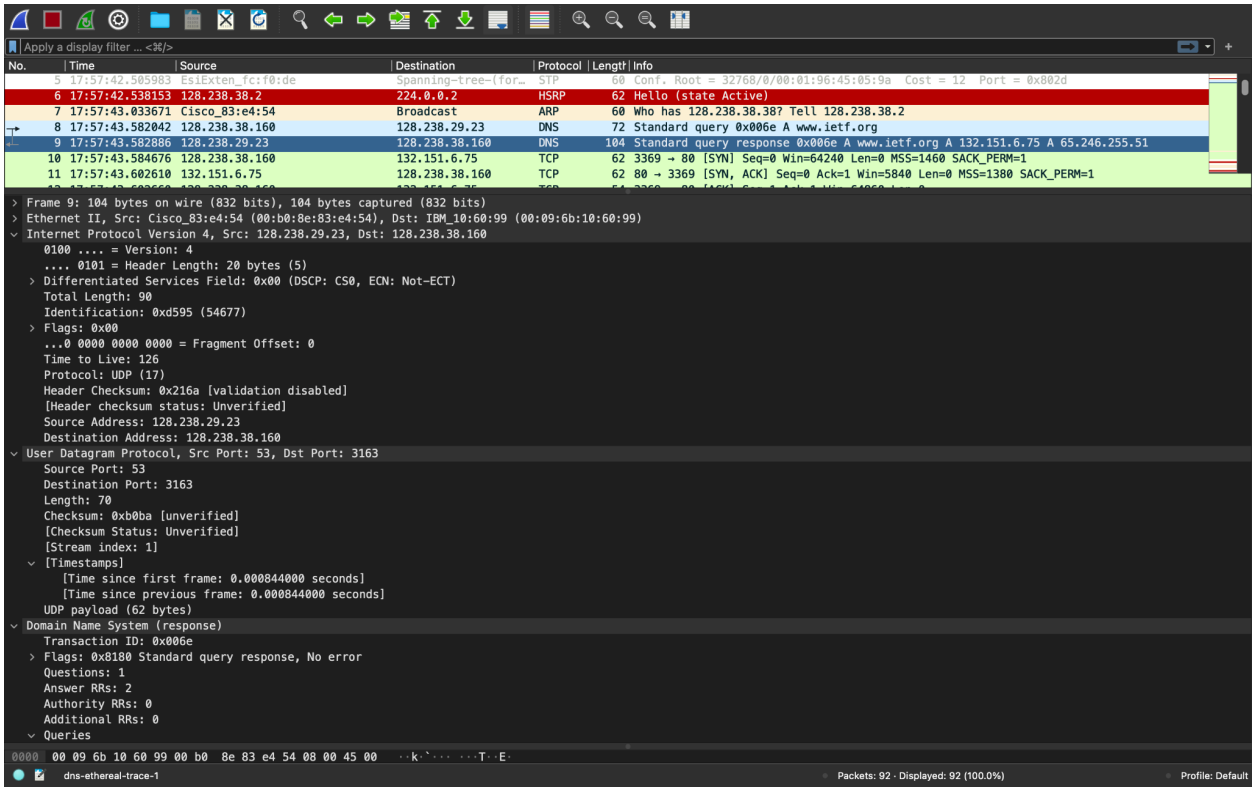
6).

```
Bhavin@Ozas-MacBook-Pro ~ % ifconfig
lo0: flags=8049<UP,LOOPBACK,RUNNING,MULTICAST> mtu 16384
        options=1203<RXCSUM,TXCSUM,TXSTATUS,SW_TIMESTAMP>
        inet 127.0.0.1 netmask 0xff000000
        inet6 ::1 prefixlen 128
        inet6 fe80::1%lo0 prefixlen 64 scopeid 0x1
        nd6 options=201<PERFORMNUD,DAD>
gif0: flags=8010<POINTOPOINT,MULTICAST> mtu 1280
stf0: flags=0<> mtu 1280
en0: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
        options=400<CHANNEL_IO>
        ether 8c:85:90:60:33:5c
        inet6 fe80::10c4:ae8f:84e0:a916%en0 prefixlen 64 secured scopeid 0x4
        inet 10.182.113.100 netmask 0xfffffe00 broadcast 10.182.113.255
        nd6 options=201<PERFORMNUD,DAD>
        media: autoselect
        status: active
en5: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
        ether ac:de:48:00:11:22
        inet6 fe80::aede:48ff:fe00:1122%en5 prefixlen 64 scopeid 0x5
        nd6 options=201<PERFORMNUD,DAD>
        media: autoselect
        status: active
en4: flags=8963<UP,BROADCAST,SMART,RUNNING,PROMISC,SIMPLEX,MULTICAST> mtu 1500
        options=460<TSO4,TSO6,CHANNEL_IO>
        ether 82:dd:82:e7:bc:04
        media: autoselect <full-duplex>
        status: inactive
en2: flags=8963<UP,BROADCAST,SMART,RUNNING,PROMISC,SIMPLEX,MULTICAST> mtu 1500
        options=460<TSO4,TSO6,CHANNEL_IO>
        ether 82:dd:82:e7:bc:00
        media: autoselect <full-duplex>
        status: inactive
en3: flags=8963<UP,BROADCAST,SMART,RUNNING,PROMISC,SIMPLEX,MULTICAST> mtu 1500
        options=460<TSO4,TSO6,CHANNEL_IO>
        ether 82:dd:82:e7:bc:05
        media: autoselect <full-duplex>
        status: inactive
en1: flags=8963<UP,BROADCAST,SMART,RUNNING,PROMISC,SIMPLEX,MULTICAST> mtu 1500
        options=460<TSO4,TSO6,CHANNEL_IO>
        ether 82:dd:82:e7:bc:01
        media: autoselect <full-duplex>
        status: inactive
bridge0: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
        options=63<RXCSUM,TXCSUM,TSO4,TSO6>
        ether 82:dd:82:e7:bc:01
        Configuration:
                id 0:0:0:0:0:0 priority 0 hellotime 0 fwddelay 0
                maxage 0 holdcnt 0 proto stp maxaddr 100 timeout 1200
                root id 0:0:0:0:0:0 priority 0 ifcost 0 port 0
                ipfilter disabled flags 0x0
        member: en1 flags=3<LEARNING,DISCOVER>
                ifmaxaddr 0 port 9 priority 0 path cost 0
        member: en2 flags=3<LEARNING,DISCOVER>
                ifmaxaddr 0 port 7 priority 0 path cost 0
        member: en3 flags=3<LEARNING,DISCOVER>
                ifmaxaddr 0 port 8 priority 0 path cost 0
        member: en4 flags=3<LEARNING,DISCOVER>
                ifmaxaddr 0 port 6 priority 0 path cost 0
        nd6 options=201<PERFORMNUD,DAD>
        media: <unknown type>
        status: inactive
p2p0: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> mtu 2304
```

Foundation of Computer Networks - Wireshark Project
Bhavin Oza (bo2115)



7). Type A Standard Query

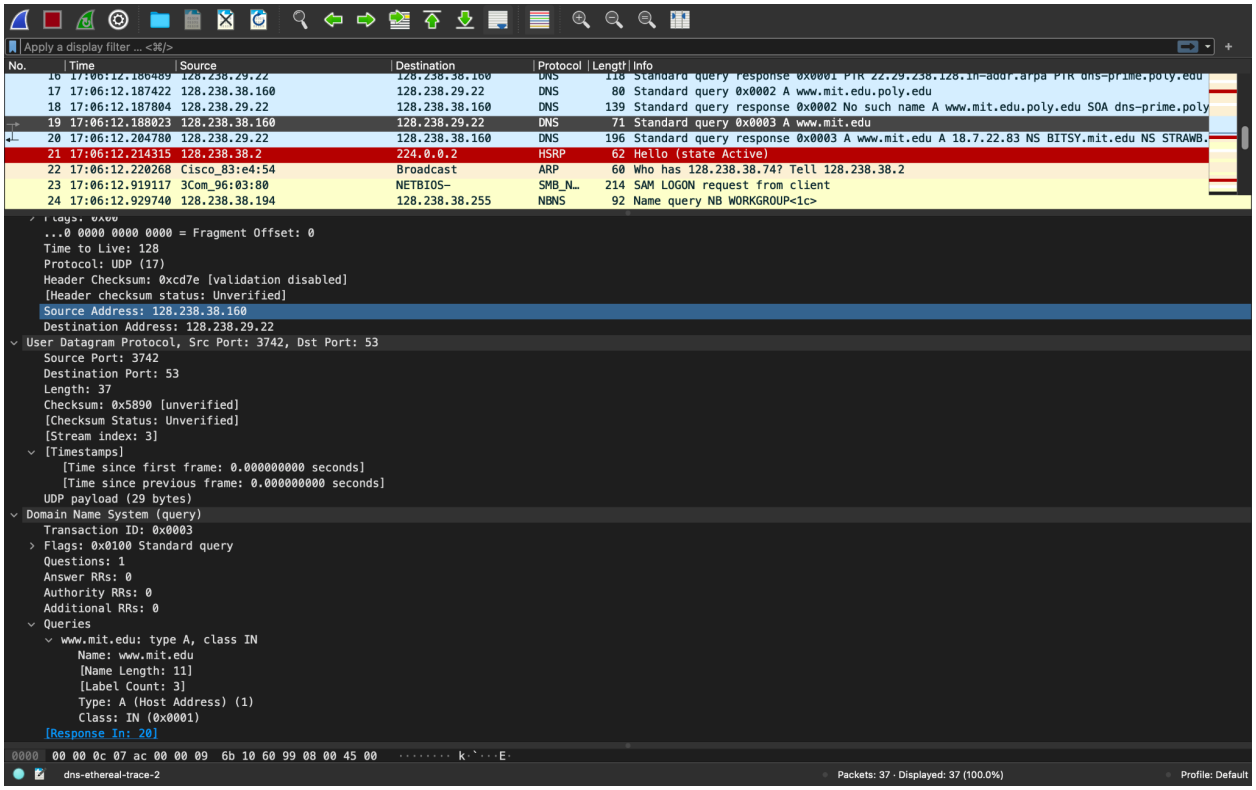


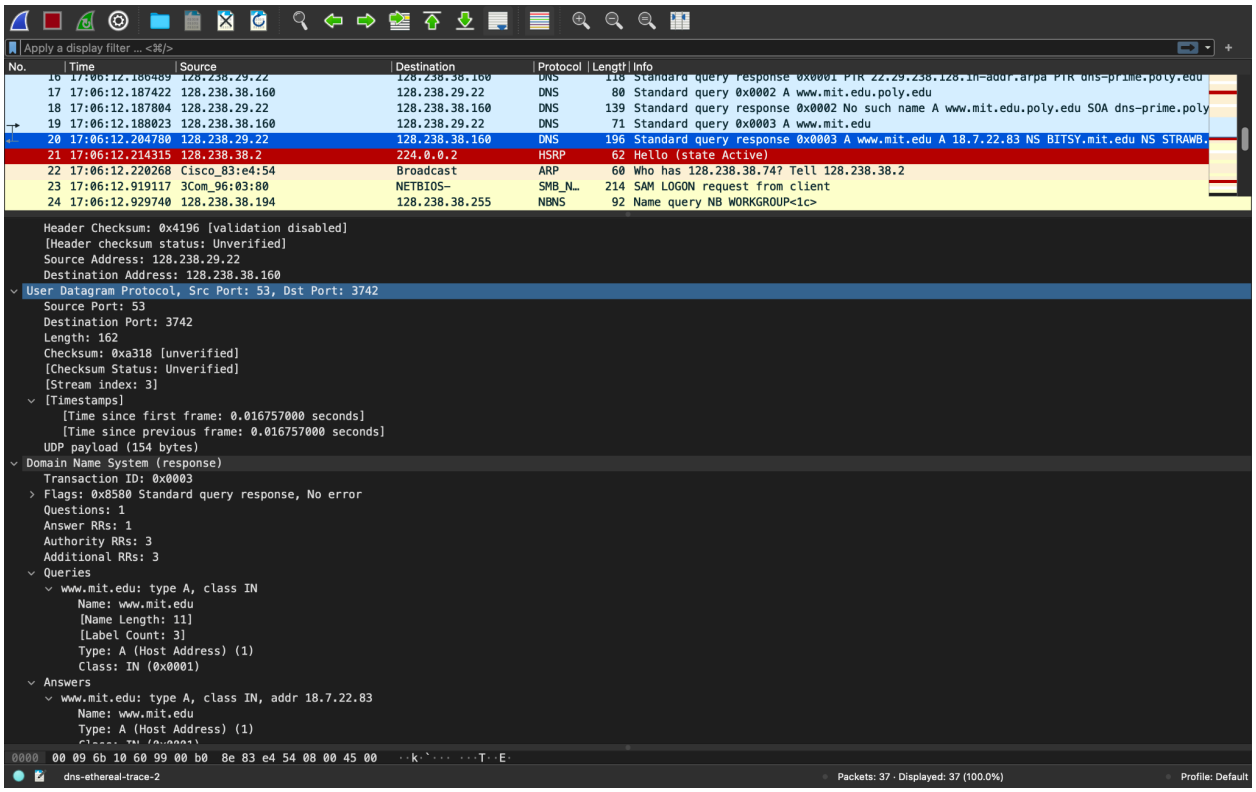
8). Two answer in DNS response message containing information about:
Name of the host, Type of the address, Class, TTL, IP address and Data Length

9). Yes, the destination IP address corresponds to the IP address provided in the DNS response message.

10). No

Foundation of Computer Networks - Wireshark Project
Bhavin Oza (bo2115)





11). Destination port for DNS query: Port 53
Source port for DNS query response: Port 53

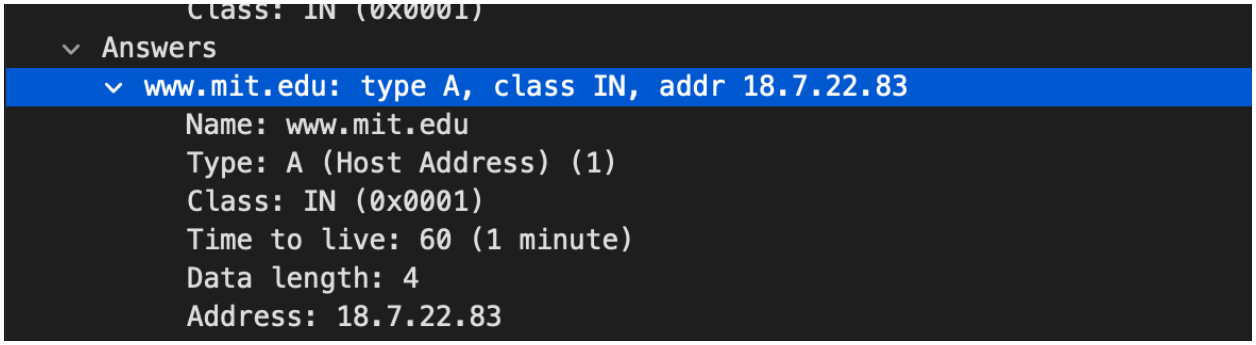
Foundation of Computer Networks - Wireshark Project
Bhavin Oza (bo2115)

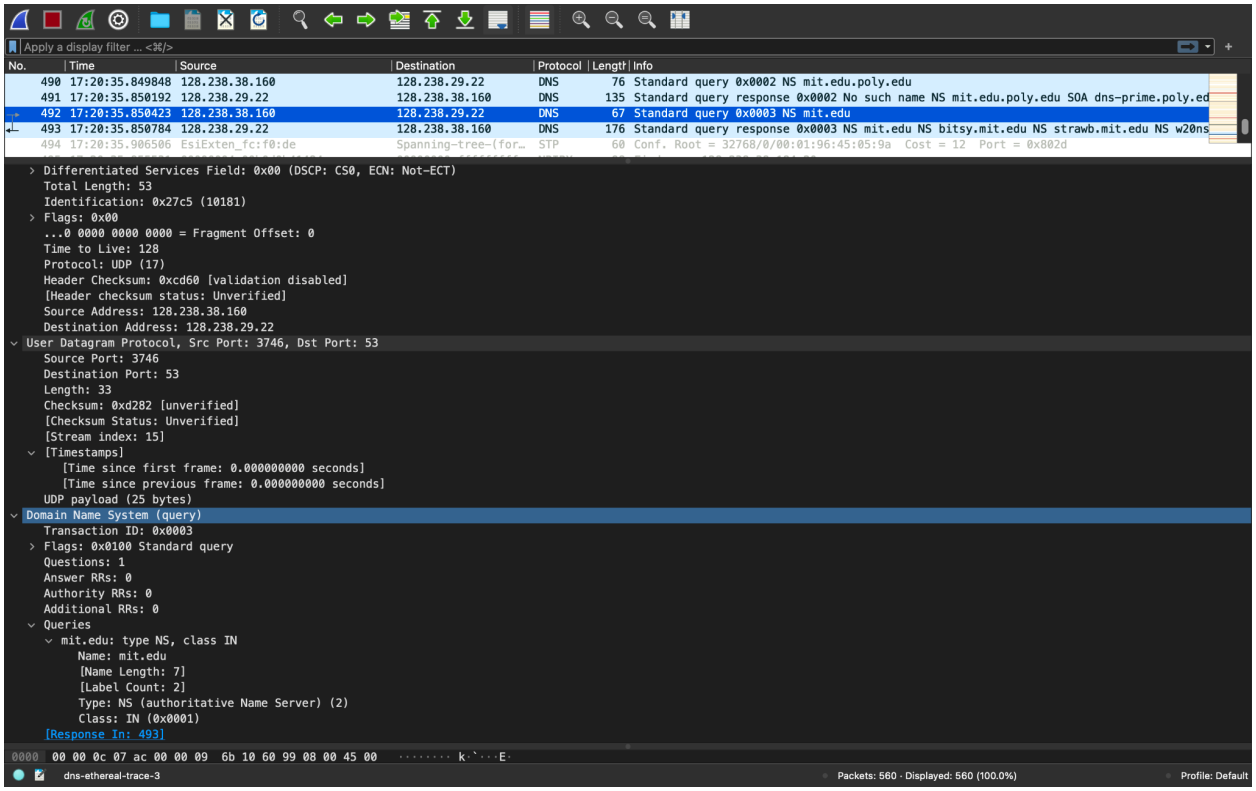
12). Yes

13). Type A Standard Query.
It does not contain any answers

14). One answer in DNS response message containing information about:
Name of the host, Type of the address, Class, TTL, IP address and Data Length

15).

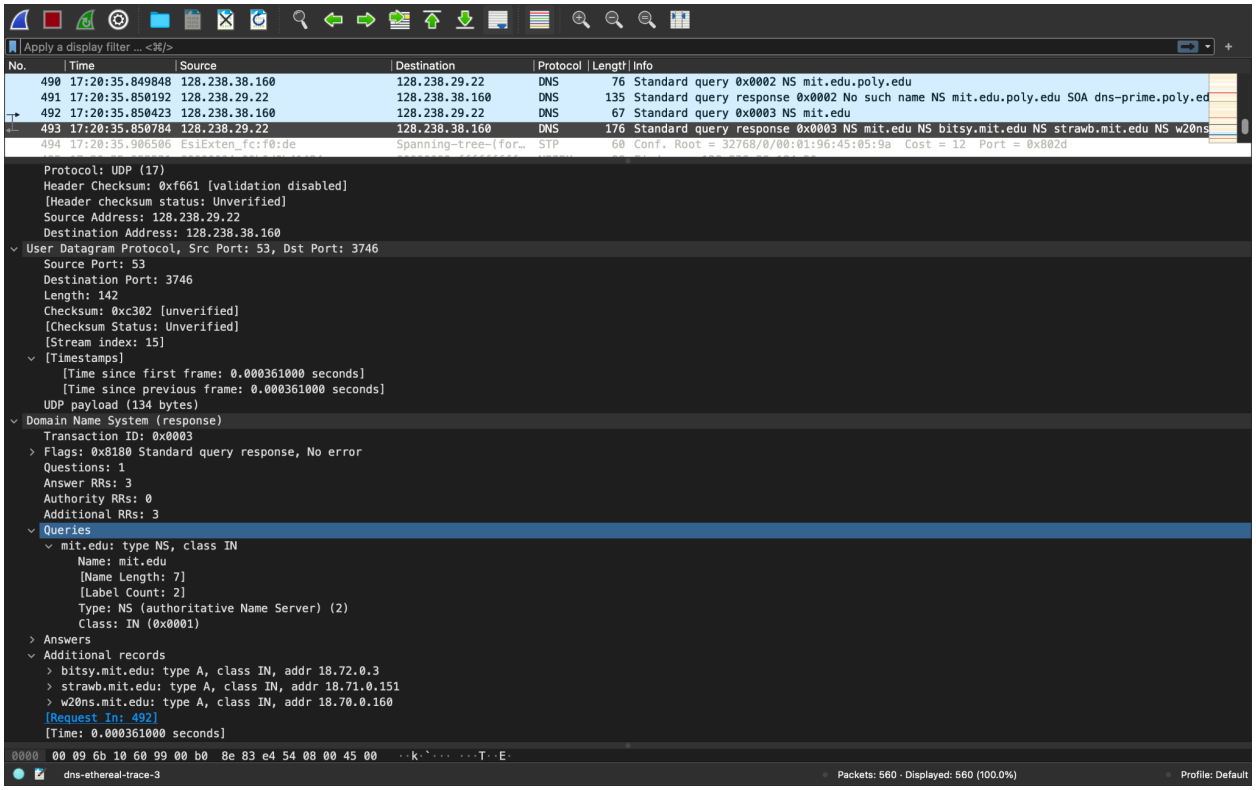




16). 128.238.29.22

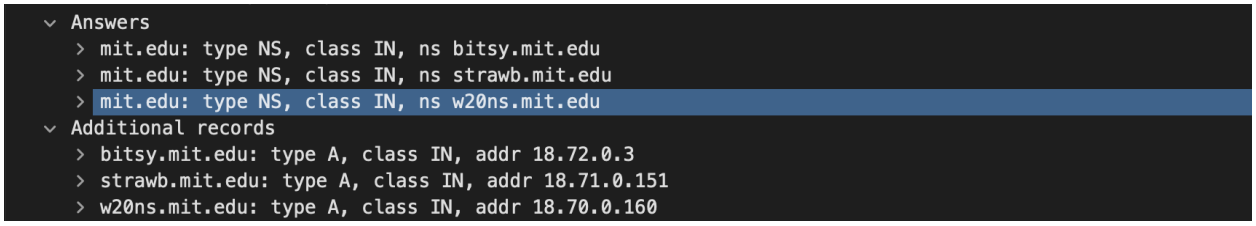
17). Type NS Standard Query.
It does not contain any answers

Foundation of Computer Networks - Wireshark Project
Bhavin Oza (bo2115)

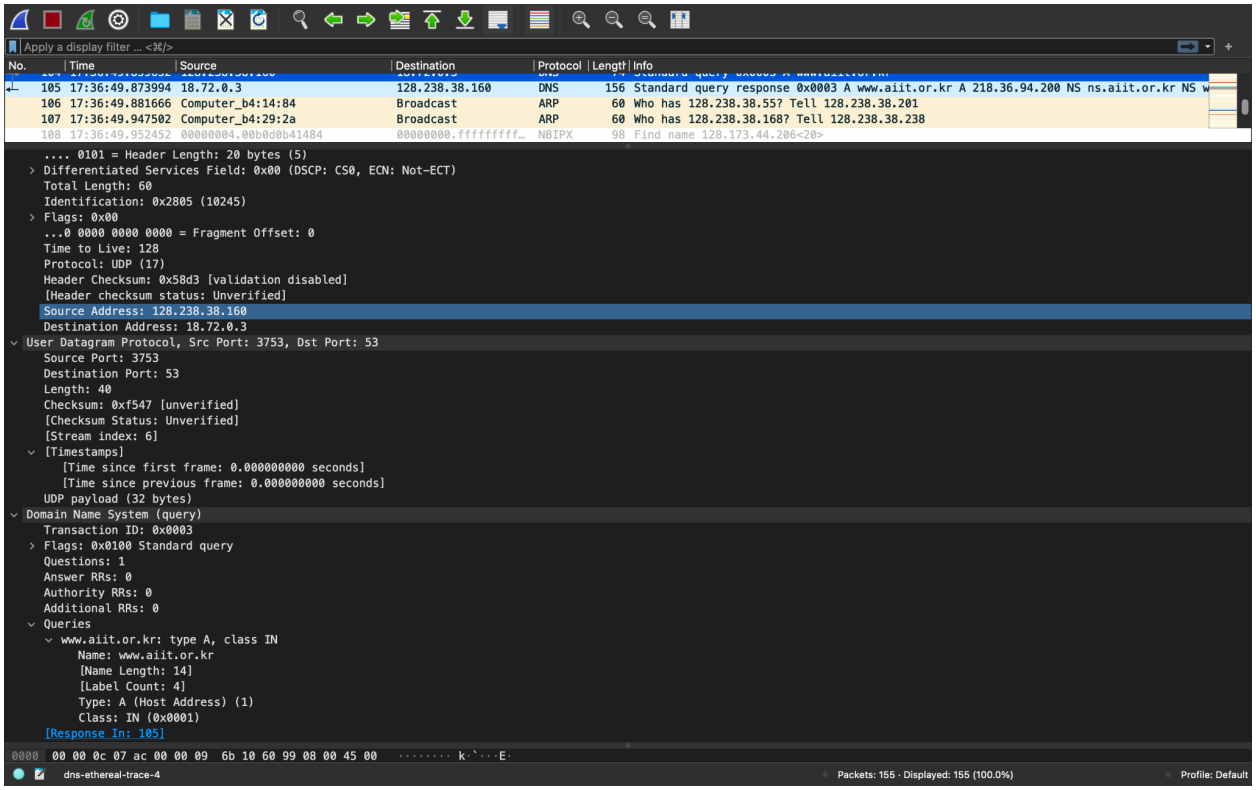


18). The nameservers are:
bitsy.mit.edu
strawb.mit.edu
w20ns.mit.edu
Yes, the response message also provides IP address for the above mentioned name servers, under additional records:
bitsy.mit.edu => 18.72.0.3
strawb.mit.edu => 18.71.0.151
w20ns.mit.edu => 18.70.0.160

19).



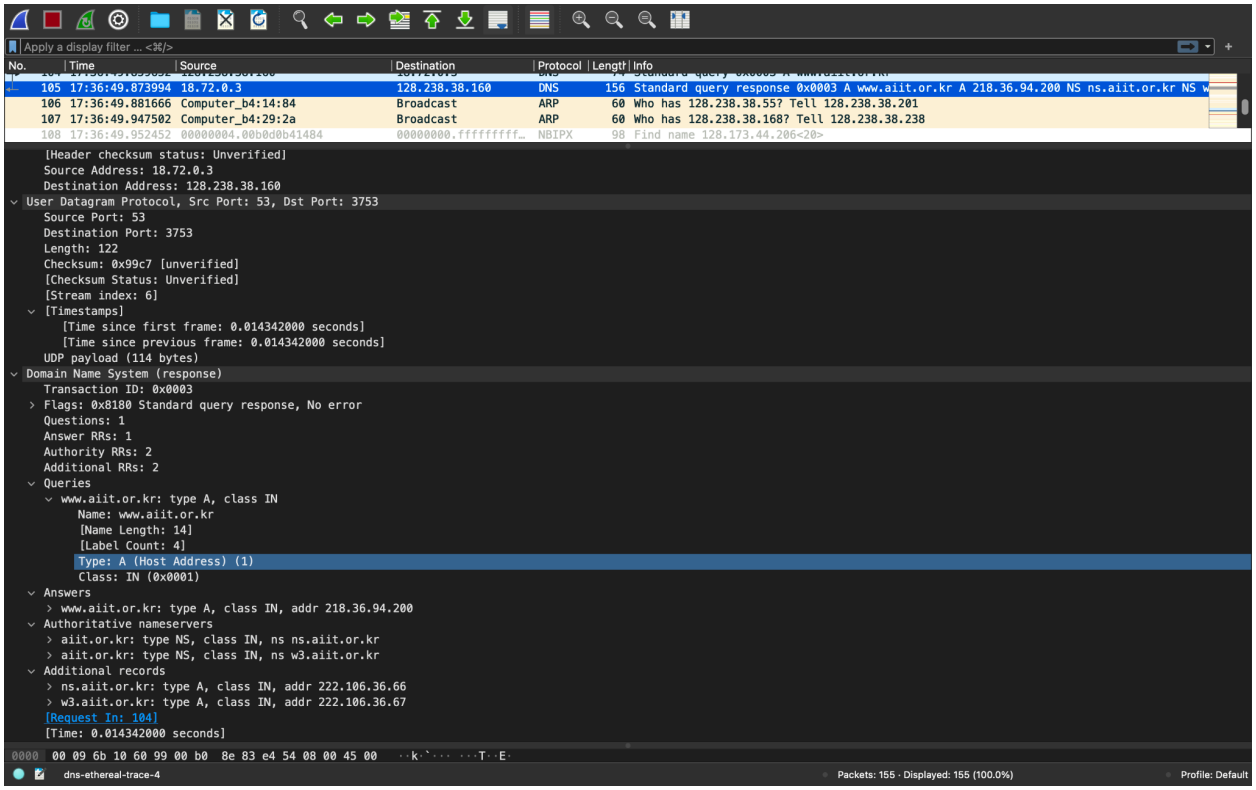
Foundation of Computer Networks - Wireshark Project
Bhavin Oza (bo2115)



20). The query is sent to IP address: 18.72.0.3, which is bitsy.mid.edu, as shown in above screenshot

21). Type A Standard Query.
It does not contain any answers

Foundation of Computer Networks - Wireshark Project
Bhavin Oza (bo2115)



22). One answer in DNS response message containing information about:
Name of the host, Type of the address, Class, TTL, IP address and Data Length

23).