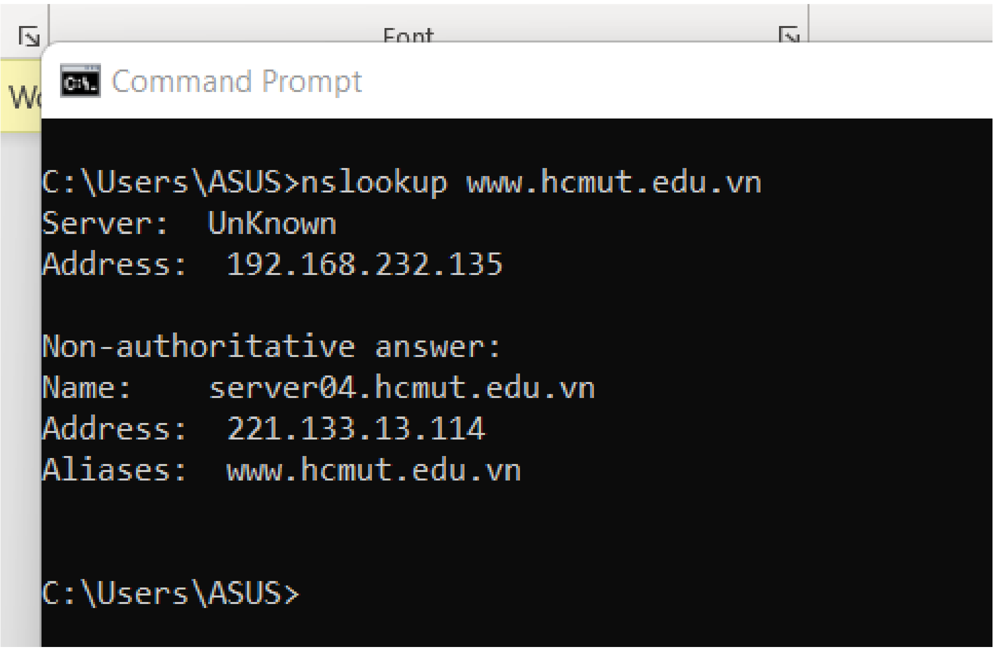
1/

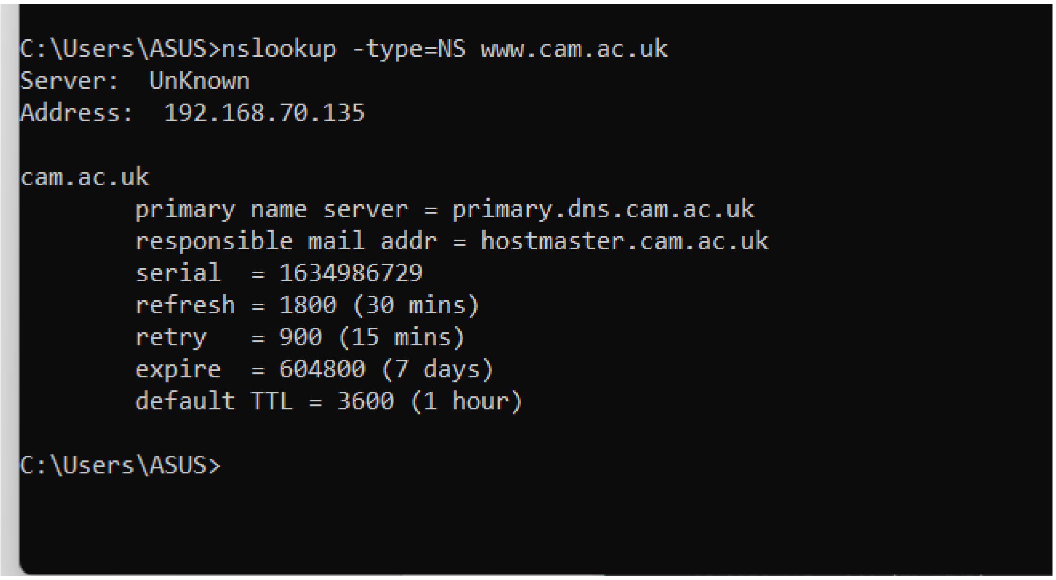
Access to the website “Trường Đại Học Bách Khoa TP. HCM”. (www.hcmut.edu.vn)



```
C:\Users\ASUS>nslookup www.hcmut.edu.vn
Server:  UnKnown
Address:  192.168.232.135

Non-authoritative answer:
Name:    server04.hcmut.edu.vn
Address:  221.133.13.114
Aliases:  www.hcmut.edu.vn


C:\Users\ASUS>
```

Address of Server: 192.168.232.135

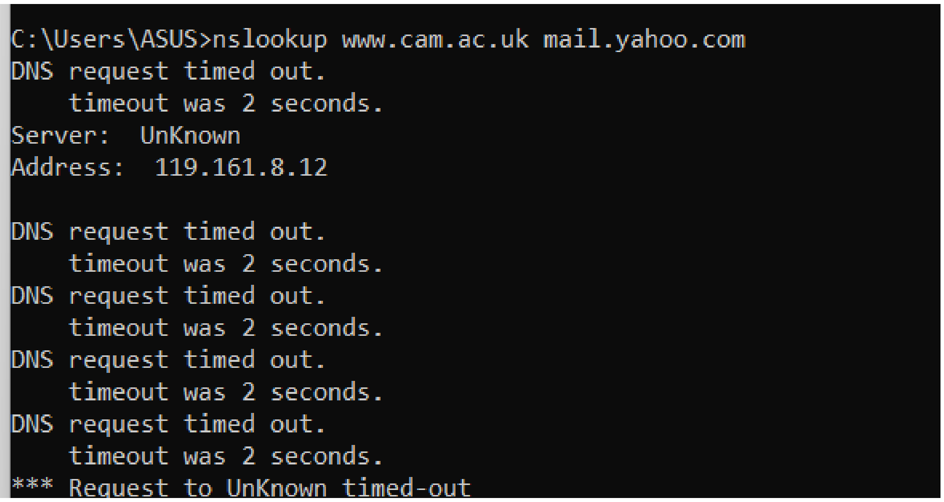
2/ Cambridge University: https://www.cam.ac.uk/



```
C:\Users\ASUS>nslookup -type=NS www.cam.ac.uk
Server:  UnKnown
Address:  192.168.70.135

cam.ac.uk
        primary name server = primary.dns.cam.ac.uk
        responsible mail addr = hostmaster.cam.ac.uk
        serial  = 1634986729
        refresh = 1800 (30 mins)
        retry   = 900 (15 mins)
        expire  = 604800 (7 days)
        default TTL = 3600 (1 hour)

C:\Users\ASUS>
```

Primary name server: primary.dns.cam.ac.uk

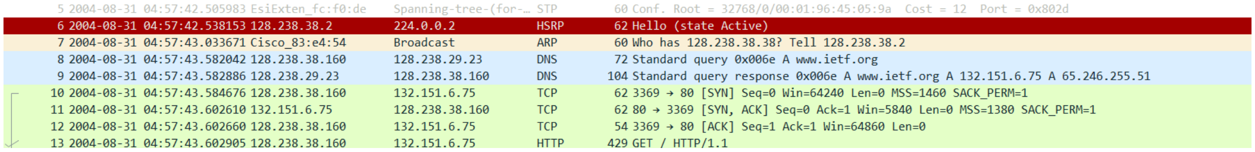
3/



```
C:\Users\ASUS>nslookup www.cam.ac.uk mail.yahoo.com
DNS request timed out.
    timeout was 2 seconds.
Server:  UnKnown
Address:  119.161.8.12

DNS request timed out.
    timeout was 2 seconds.
DNS request timed out.
    timeout was 2 seconds.
DNS request timed out.
    timeout was 2 seconds.
DNS request timed out.
    timeout was 2 seconds.
*** Request to UnKnown timed-out
```

DNS servers obtained in Question 2 is queried for the mail servers for Yahoo! Mail: 119.161.8.12

4/



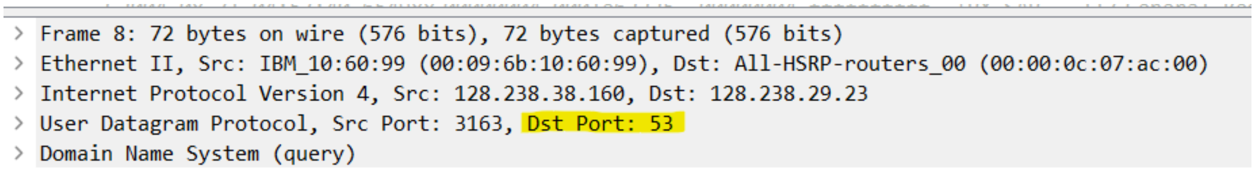
```
 5 2004-08-31 04:57:42.505983 EsiExten_fc:f0:de   Spanning-tree-(for-… STP    60 Conf. Root = 32768/0/00:01:96:45:05:9a  Cost = 12  Port = 0x802d
 6 2004-08-31 04:57:42.538153 128.238.38.2        224.0.0.2            HSRP   62 Hello (state Active)
 7 2004-08-31 04:57:43.033671 Cisco_83:e4:54      Broadcast            ARP    60 Who has 128.238.38.38? Tell 128.238.38.2
 8 2004-08-31 04:57:43.582042 128.238.38.160      128.238.29.23        DNS    72 Standard query 0x006e A www.ietf.org
 9 2004-08-31 04:57:43.582886 128.238.29.23       128.238.38.160       DNS   104 Standard query response 0x006e A www.ietf.org A 132.151.6.75 A 65.246.255.51
10 2004-08-31 04:57:43.584676 128.238.38.160      132.151.6.75         TCP    62 3369 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
11 2004-08-31 04:57:43.602610 132.151.6.75        128.238.38.160       TCP    62 80 → 3369 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1380 SACK_PERM=1
12 2004-08-31 04:57:43.602660 128.238.38.160      132.151.6.75         TCP    54 3369 → 80 [ACK] Seq=1 Ack=1 Win=64860 Len=0
13 2004-08-31 04:57:43.602905 128.238.38.160      132.151.6.75         HTTP  429 GET / HTTP/1.1
```

The DNS query and response messages are sent over UDP.

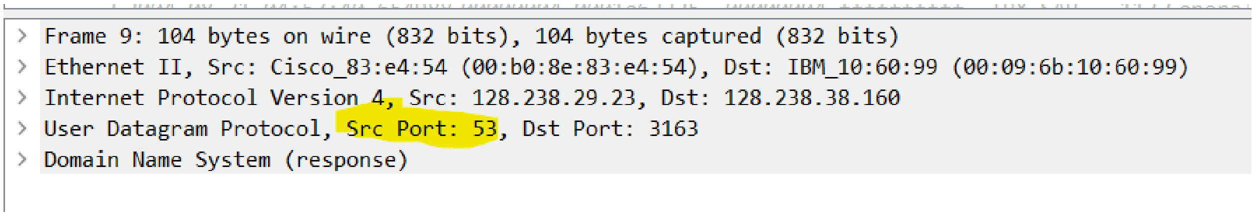
5/

The destination port of DNS query message is 53.

The source port of DNS response message is 53.



```
> Frame 8: 72 bytes on wire (576 bits), 72 bytes captured (576 bits)
> Ethernet II, Src: IBM_10:60:99 (00:09:6b:10:60:99), Dst: All-HSRP-routers_00 (00:00:0c:07:ac:00)
> Internet Protocol Version 4, Src: 128.238.38.160, Dst: 128.238.29.23
> User Datagram Protocol, Src Port: 3163, Dst Port: 53
> Domain Name System (query)
```

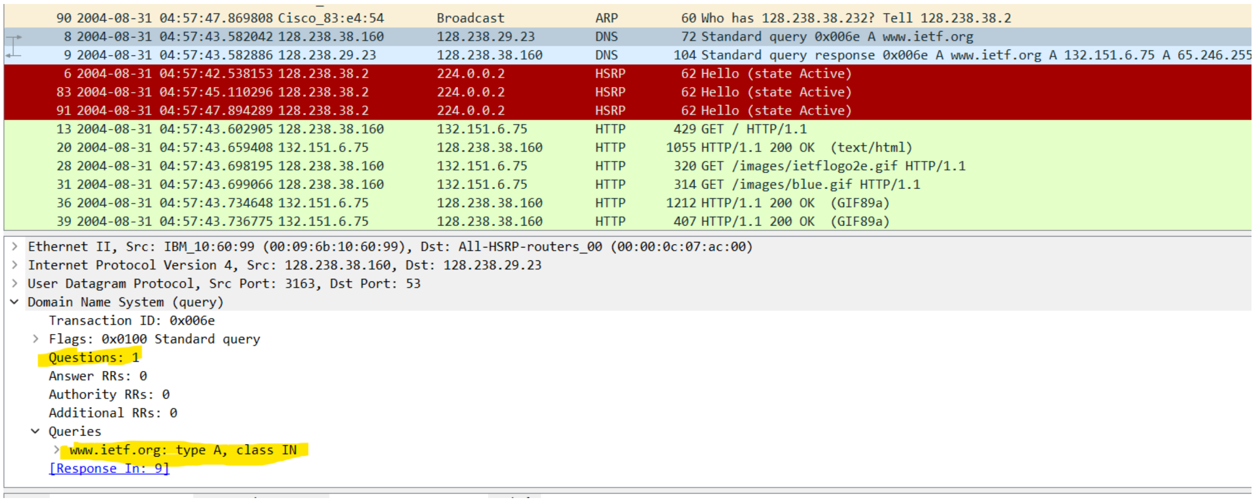


```
> Frame 9: 104 bytes on wire (832 bits), 104 bytes captured (832 bits)
> Ethernet II, Src: Cisco_83:e4:54 (00:b0:8e:83:e4:54), Dst: IBM_10:60:99 (00:09:6b:10:60:99)
> Internet Protocol Version 4, Src: 128.238.29.23, Dst: 128.238.38.160
> User Datagram Protocol, Src Port: 53, Dst Port: 3163
> Domain Name System (response)
```

6/

The DNS query was sent to IP address 128.238.29.23. Yes it is the same IP address as that of my local DNS server.

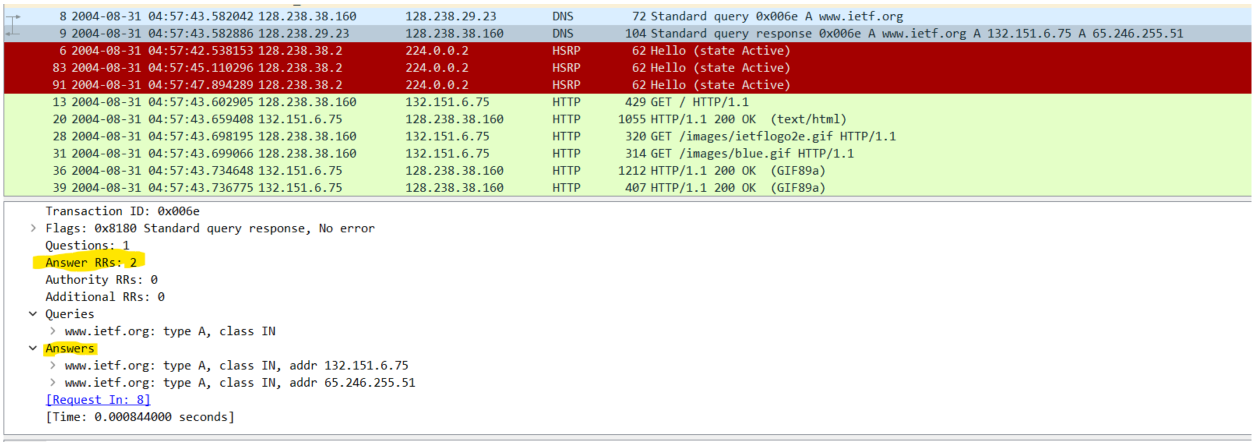
7/



```
   90 2004-08-31 04:57:47.869808 Cisco_83:e4:54    Broadcast        ARP      60 Who has 128.238.38.232? Tell 128.238.38.2
    8 2004-08-31 04:57:43.582042 128.238.38.160    128.238.29.23    DNS      72 Standard query 0x006e A www.ietf.org
    9 2004-08-31 04:57:43.582886 128.238.29.23     128.238.38.160   DNS     104 Standard query response 0x006e A www.ietf.org A 132.151.6.75 A 65.246.255
    6 2004-08-31 04:57:42.538153 128.238.38.2      224.0.0.2        HSRP     62 Hello (state Active)
   83 2004-08-31 04:57:45.110296 128.238.38.2      224.0.0.2        HSRP     62 Hello (state Active)
   91 2004-08-31 04:57:47.894289 128.238.38.2      224.0.0.2        HSRP     62 Hello (state Active)
   13 2004-08-31 04:57:43.602905 128.238.38.160    132.151.6.75     HTTP    429 GET / HTTP/1.1
   20 2004-08-31 04:57:43.659408 132.151.6.75      128.238.38.160   HTTP   1055 HTTP/1.1 200 OK  (text/html)
   28 2004-08-31 04:57:43.698195 128.238.38.160    132.151.6.75     HTTP    320 GET /images/ietflogo2e.gif HTTP/1.1
   31 2004-08-31 04:57:43.699066 128.238.38.160    132.151.6.75     HTTP    314 GET /images/blue.gif HTTP/1.1
   36 2004-08-31 04:57:43.734648 132.151.6.75      128.238.38.160   HTTP   1212 HTTP/1.1 200 OK  (GIF89a)
   39 2004-08-31 04:57:43.736775 132.151.6.75      128.238.38.160   HTTP    407 HTTP/1.1 200 OK  (GIF89a)

> Ethernet II, Src: IBM_10:60:99 (00:09:6b:10:60:99), Dst: All-HSRP-routers_00 (00:00:0c:07:ac:00)
> Internet Protocol Version 4, Src: 128.238.38.160, Dst: 128.238.29.23
> User Datagram Protocol, Src Port: 3163, Dst Port: 53
v Domain Name System (query)
    Transaction ID: 0x006e
  > Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  v Queries
    > www.ietf.org: type A, class IN
    [Response In: 9]
```

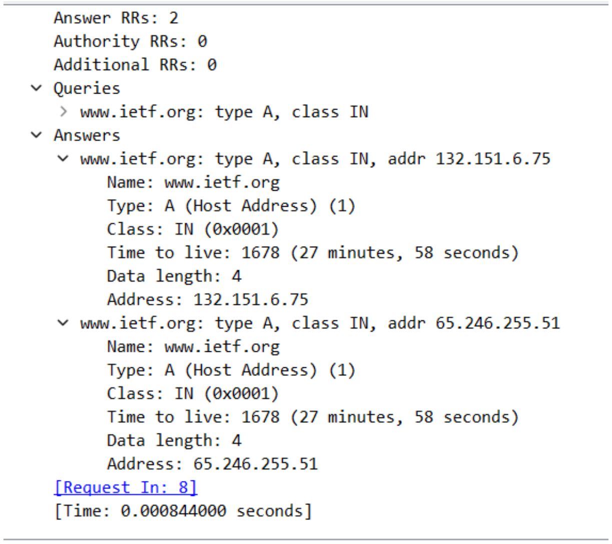
The query message was a type “A” query, but the message did not contain any “answers.”

8/



```
    8 2004-08-31 04:57:43.582042 128.238.38.160    128.238.29.23    DNS      72 Standard query 0x006e A www.ietf.org
    9 2004-08-31 04:57:43.582886 128.238.29.23     128.238.38.160   DNS     104 Standard query response 0x006e A www.ietf.org A 132.151.6.75 A 65.246.255.51
    6 2004-08-31 04:57:42.538153 128.238.38.2      224.0.0.2        HSRP     62 Hello (state Active)
   83 2004-08-31 04:57:45.110296 128.238.38.2      224.0.0.2        HSRP     62 Hello (state Active)
   91 2004-08-31 04:57:47.894289 128.238.38.2      224.0.0.2        HSRP     62 Hello (state Active)
   13 2004-08-31 04:57:43.602905 128.238.38.160    132.151.6.75     HTTP    429 GET / HTTP/1.1
   20 2004-08-31 04:57:43.659408 132.151.6.75      128.238.38.160   HTTP   1055 HTTP/1.1 200 OK  (text/html)
   28 2004-08-31 04:57:43.698195 128.238.38.160    132.151.6.75     HTTP    320 GET /images/ietflogo2e.gif HTTP/1.1
   31 2004-08-31 04:57:43.699066 128.238.38.160    132.151.6.75     HTTP    314 GET /images/blue.gif HTTP/1.1
   36 2004-08-31 04:57:43.734648 132.151.6.75      128.238.38.160   HTTP   1212 HTTP/1.1 200 OK  (GIF89a)
   39 2004-08-31 04:57:43.736775 132.151.6.75      128.238.38.160   HTTP    407 HTTP/1.1 200 OK  (GIF89a)

    Transaction ID: 0x006e
  > Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 2
    Authority RRs: 0
    Additional RRs: 0
  v Queries
    > www.ietf.org: type A, class IN
  v Answers
    > www.ietf.org: type A, class IN, addr 132.151.6.75
    > www.ietf.org: type A, class IN, addr 65.246.255.51
    [Request In: 8]
    [Time: 0.000844000 seconds]
```

The response message contained 2 answers to the query which was the sites address [132.151.6.75] and [65.246.255.51]. These contains some following information:



```
    Answer RRs: 2
    Authority RRs: 0
    Additional RRs: 0
  ˅ Queries
    > www.ietf.org: type A, class IN
  ˅ Answers
    ˅ www.ietf.org: type A, class IN, addr 132.151.6.75
        Name: www.ietf.org
        Type: A (Host Address) (1)
        Class: IN (0x0001)
        Time to live: 1678 (27 minutes, 58 seconds)
        Data length: 4
        Address: 132.151.6.75
    ˅ www.ietf.org: type A, class IN, addr 65.246.255.51
        Name: www.ietf.org
        Type: A (Host Address) (1)
        Class: IN (0x0001)
        Time to live: 1678 (27 minutes, 58 seconds)
        Data length: 4
        Address: 65.246.255.51
    [Request In: 8]
    [Time: 0.000844000 seconds]
```

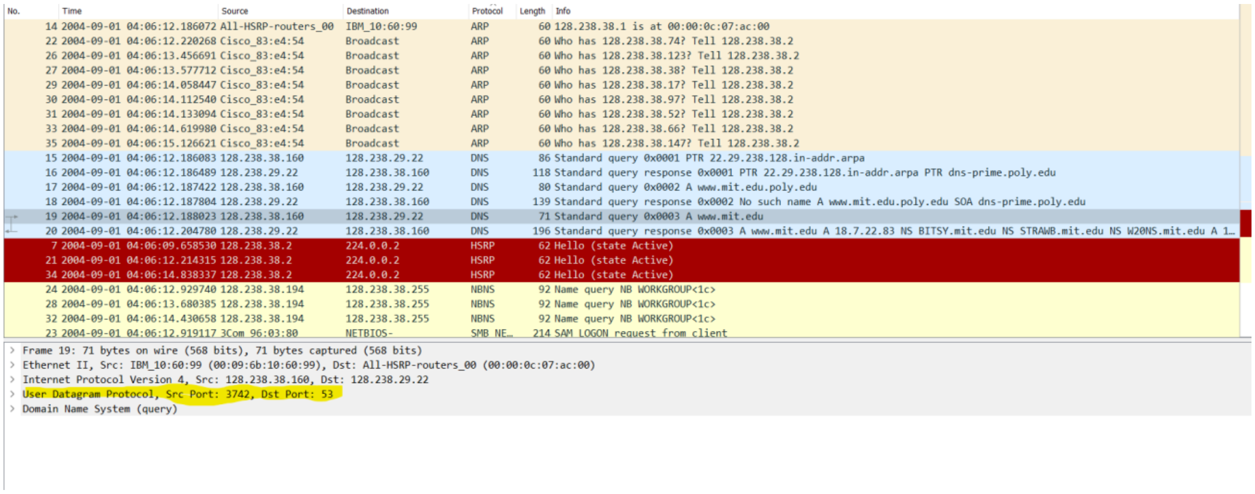
9/

The destination of the SYN packet is 132.151.6.75, the same address that was provided in the DNS response message as the type "A" address of the webpage.

10/

No, my host didn't issue new DNS queries before the images were retrieved.

11/



```
No.  Time                       Source                Destination     Protocol  Length Info
  14 2004-09-01 04:06:12.186072 All-HSRP-routers_00   IBM_10:60:99    ARP       60 128.238.38.1 is at 00:00:0c:07:ac:00
  22 2004-09-01 04:06:12.220268 Cisco_83:e4:54        Broadcast       ARP       60 Who has 128.238.38.74? Tell 128.238.38.2
  26 2004-09-01 04:06:13.456691 Cisco_83:e4:54        Broadcast       ARP       60 Who has 128.238.38.123? Tell 128.238.38.2
  27 2004-09-01 04:06:13.577712 Cisco_83:e4:54        Broadcast       ARP       60 Who has 128.238.38.38? Tell 128.238.38.2
  29 2004-09-01 04:06:14.058447 Cisco_83:e4:54        Broadcast       ARP       60 Who has 128.238.38.17? Tell 128.238.38.2
  30 2004-09-01 04:06:14.112540 Cisco_83:e4:54        Broadcast       ARP       60 Who has 128.238.38.97? Tell 128.238.38.2
  31 2004-09-01 04:06:14.133094 Cisco_83:e4:54        Broadcast       ARP       60 Who has 128.238.38.52? Tell 128.238.38.2
  33 2004-09-01 04:06:14.619980 Cisco_83:e4:54        Broadcast       ARP       60 Who has 128.238.38.66? Tell 128.238.38.2
  35 2004-09-01 04:06:15.126621 Cisco_83:e4:54        Broadcast       ARP       60 Who has 128.238.38.147? Tell 128.238.38.2
  15 2004-09-01 04:06:12.186083 128.238.38.160        128.238.29.22   DNS       86 Standard query 0x0001 PTR 22.29.238.128.in-addr.arpa
  16 2004-09-01 04:06:12.186489 128.238.29.22         128.238.38.160  DNS      118 Standard query response 0x0001 PTR 22.29.238.128.in-addr.arpa PTR dns-prime.poly.edu
  17 2004-09-01 04:06:12.187422 128.238.38.160        128.238.29.22   DNS       80 Standard query 0x0002 A www.mit.edu.poly.edu
  18 2004-09-01 04:06:12.187804 128.238.29.22         128.238.38.160  DNS      139 Standard query response 0x0002 No such name A www.mit.edu.poly.edu SOA dns-prime.poly.edu
  19 2004-09-01 04:06:12.188023 128.238.38.160        128.238.29.22   DNS       71 Standard query 0x0003 A www.mit.edu
  20 2004-09-01 04:06:12.204780 128.238.29.22         128.238.38.160  DNS      196 Standard query response 0x0003 A www.mit.edu A 18.7.22.83 NS BITSY.mit.edu NS STRAWB.mit.edu NS W20NS.mit.edu A 1…
   7 2004-09-01 04:06:09.658530 128.238.38.2          224.0.0.2       HSRP      62 Hello (state Active)
  21 2004-09-01 04:06:12.214315 128.238.38.2          224.0.0.2       HSRP      62 Hello (state Active)
  34 2004-09-01 04:06:14.838337 128.238.38.2          224.0.0.2       HSRP      62 Hello (state Active)
  24 2004-09-01 04:06:12.929740 128.238.38.194        128.238.38.255  NBNS      92 Name query NB WORKGROUP<1c>
  28 2004-09-01 04:06:13.680385 128.238.38.194        128.238.38.255  NBNS      92 Name query NB WORKGROUP<1c>
  32 2004-09-01 04:06:14.430658 128.238.38.194        128.238.38.255  NBNS      92 Name query NB WORKGROUP<1c>
  23 2004-09-01 04:06:12.919117 3Com_96:03:80         NETBIOS-        SMB NE…  214 SAM LOGON request from client

> Frame 19: 71 bytes on wire (568 bits), 71 bytes captured (568 bits)
> Ethernet II, Src: IBM_10:60:99 (00:09:6b:10:60:99), Dst: All-HSRP-routers_00 (00:00:0c:07:ac:00)
> Internet Protocol Version 4, Src: 128.238.38.160, Dst: 128.238.29.22
> User Datagram Protocol, Src Port: 3742, Dst Port: 53
> Domain Name System (query)
```

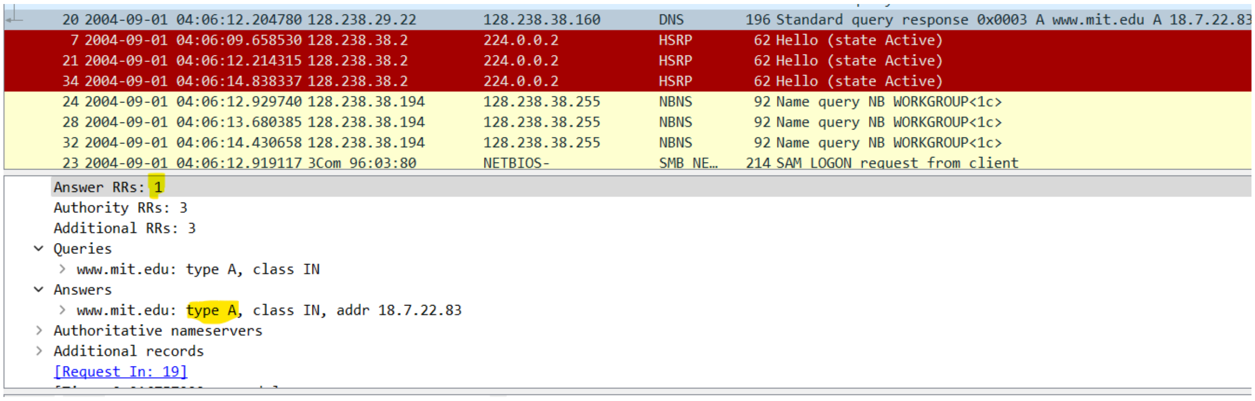
Src port: 3742, dst port: 53

12/ The DNS query message is sent to IP address 128.238.29.22, the same address as my default local DNS server.

13/

The DNS query message is a type “A” query, containing only one question and not containing any answers.

14/

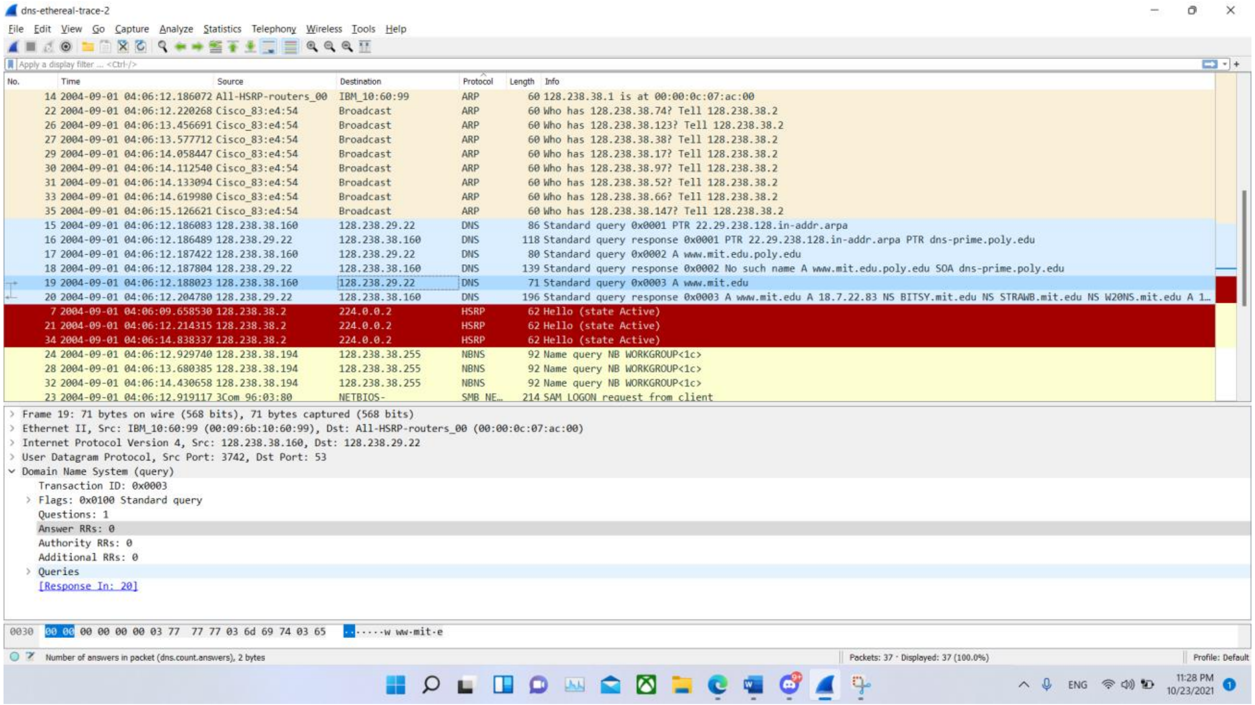


```
   20 2004-09-01 04:06:12.204780 128.238.29.22      128.238.38.160     DNS       196 Standard query response 0x0003 A www.mit.edu A 18.7.22.83
    7 2004-09-01 04:06:09.658530 128.238.38.2       224.0.0.2          HSRP       62 Hello (state Active)
   21 2004-09-01 04:06:12.214315 128.238.38.2       224.0.0.2          HSRP       62 Hello (state Active)
   34 2004-09-01 04:06:14.838337 128.238.38.2       224.0.0.2          HSRP       62 Hello (state Active)
   24 2004-09-01 04:06:12.929740 128.238.38.194     128.238.38.255     NBNS       92 Name query NB WORKGROUP<1c>
   28 2004-09-01 04:06:13.680385 128.238.38.194     128.238.38.255     NBNS       92 Name query NB WORKGROUP<1c>
   32 2004-09-01 04:06:14.430658 128.238.38.194     128.238.38.255     NBNS       92 Name query NB WORKGROUP<1c>
   23 2004-09-01 04:06:12.919117 3Com_96:03:80      NETBIOS-           SMB NE…   214 SAM LOGON request from client
```

```
    Answer RRs: 1
    Authority RRs: 3
    Additional RRs: 3
  ⌄ Queries
    > www.mit.edu: type A, class IN
  ⌄ Answers
    > www.mit.edu: type A, class IN, addr 18.7.22.83
  > Authoritative nameservers
  > Additional records
    [Request In: 19]
```

The response message contains one answer to the aforementioned query which is the type “A” address of http://www.mit.edu or 18.7.22.83. It also contained information on 3 authoritative nameservers and 3 additional records.

15/



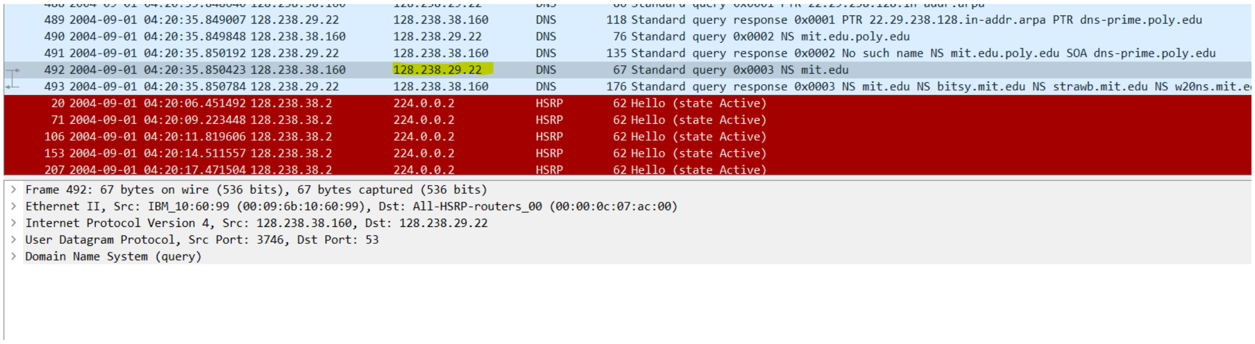
dns-ethereal-trace-2
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>

```
No.   Time                       Source                 Destination      Protocol  Length Info
   14 2004-09-01 04:06:12.186072 All-HSRP-routers_00    IBM_10:60:99     ARP        60 128.238.38.1 is at 00:00:0c:07:ac:00
   22 2004-09-01 04:06:12.220268 Cisco_83:e4:54         Broadcast        ARP        60 Who has 128.238.38.74? Tell 128.238.38.2
   26 2004-09-01 04:06:13.456691 Cisco_83:e4:54         Broadcast        ARP        60 Who has 128.238.38.123? Tell 128.238.38.2
   27 2004-09-01 04:06:13.577712 Cisco_83:e4:54         Broadcast        ARP        60 Who has 128.238.38.38? Tell 128.238.38.2
   29 2004-09-01 04:06:14.058447 Cisco_83:e4:54         Broadcast        ARP        60 Who has 128.238.38.17? Tell 128.238.38.2
   30 2004-09-01 04:06:14.112540 Cisco_83:e4:54         Broadcast        ARP        60 Who has 128.238.38.97? Tell 128.238.38.2
   31 2004-09-01 04:06:14.133094 Cisco_83:e4:54         Broadcast        ARP        60 Who has 128.238.38.52? Tell 128.238.38.2
   33 2004-09-01 04:06:14.619980 Cisco_83:e4:54         Broadcast        ARP        60 Who has 128.238.38.66? Tell 128.238.38.2
   35 2004-09-01 04:06:15.126621 Cisco_83:e4:54         Broadcast        ARP        60 Who has 128.238.38.147? Tell 128.238.38.2
   15 2004-09-01 04:06:12.186083 128.238.38.160         128.238.29.22    DNS        86 Standard query 0x0001 PTR 22.29.238.128.in-addr.arpa
   16 2004-09-01 04:06:12.186489 128.238.29.22          128.238.38.160   DNS       118 Standard query response 0x0001 PTR 22.29.238.128.in-addr.arpa PTR dns-prime.poly.edu
   17 2004-09-01 04:06:12.187422 128.238.38.160         128.238.29.22    DNS        80 Standard query 0x0002 A www.mit.edu.poly.edu
   18 2004-09-01 04:06:12.187804 128.238.29.22          128.238.38.160   DNS       139 Standard query response 0x0002 No such name A www.mit.edu.poly.edu SOA dns-prime.poly.edu
   19 2004-09-01 04:06:12.188023 128.238.38.160         128.238.29.22    DNS        71 Standard query 0x0003 A www.mit.edu
   20 2004-09-01 04:06:12.204780 128.238.29.22          128.238.38.160   DNS       196 Standard query response 0x0003 A www.mit.edu A 18.7.22.83 NS BITSY.mit.edu NS STRAWB.mit.edu NS W20NS.mit.edu A 1…
    7 2004-09-01 04:06:09.658530 128.238.38.2           224.0.0.2        HSRP       62 Hello (state Active)
   21 2004-09-01 04:06:12.214315 128.238.38.2           224.0.0.2        HSRP       62 Hello (state Active)
   34 2004-09-01 04:06:14.838337 128.238.38.2           224.0.0.2        HSRP       62 Hello (state Active)
   24 2004-09-01 04:06:12.929740 128.238.38.194         128.238.38.255   NBNS       92 Name query NB WORKGROUP<1c>
   28 2004-09-01 04:06:13.680385 128.238.38.194         128.238.38.255   NBNS       92 Name query NB WORKGROUP<1c>
   32 2004-09-01 04:06:14.430658 128.238.38.194         128.238.38.255   NBNS       92 Name query NB WORKGROUP<1c>
   23 2004-09-01 04:06:12.919117 3Com_96:03:80          NETBIOS-         SMB NE…   214 SAM LOGON request from client
```

```
> Frame 19: 71 bytes on wire (568 bits), 71 bytes captured (568 bits)
> Ethernet II, Src: IBM_10:60:99 (00:09:6b:10:60:99), Dst: All-HSRP-routers_00 (00:00:0c:07:ac:00)
> Internet Protocol Version 4, Src: 128.238.38.160, Dst: 128.238.29.22
> User Datagram Protocol, Src Port: 3742, Dst Port: 53
⌄ Domain Name System (query)
    Transaction ID: 0x0003
  > Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  > Queries
    [Response In: 20]

0030  00 00 00 00 00 00 03 77  77 77 03 6d 69 74 03 65   ·······w ww·mit·e
```

Number of answers in packet (dns.count.answers), 2 bytes
Packets: 37 · Displayed: 37 (100.0%)
Profile: Default
ENG
11:28 PM
10/23/2021

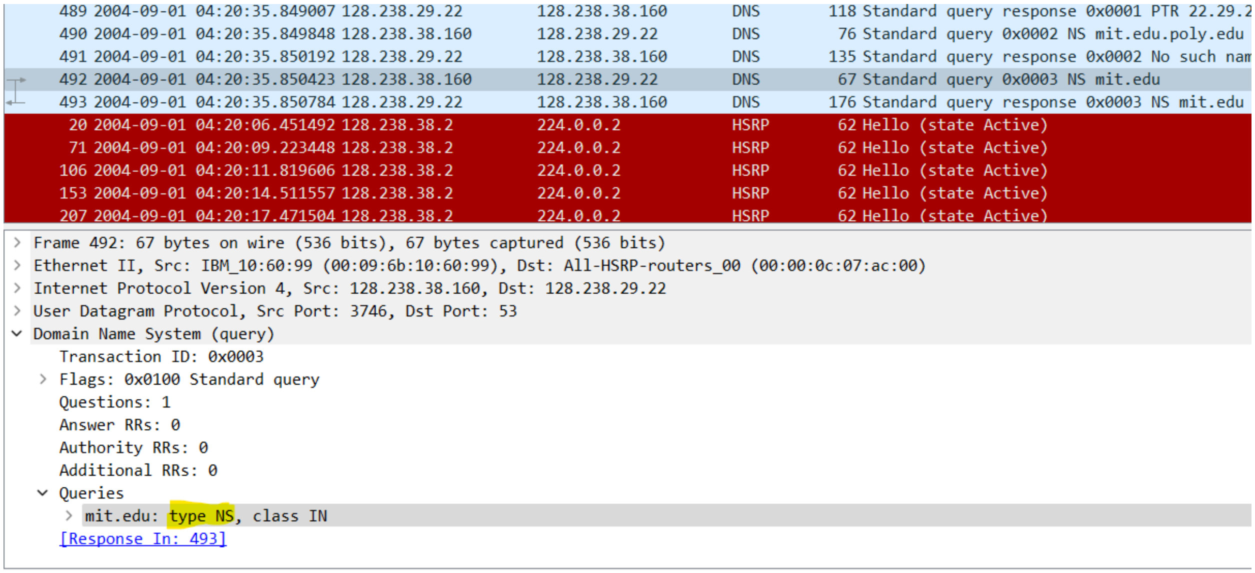
16/



```
489 2004-09-01 04:20:35.849007 128.238.29.22   128.238.38.160  DNS   118 Standard query response 0x0001 PTR 22.29.238.128.in-addr.arpa PTR dns-prime.poly.edu
490 2004-09-01 04:20:35.849848 128.238.38.160  128.238.29.22   DNS    76 Standard query 0x0002 NS mit.edu.poly.edu
491 2004-09-01 04:20:35.850192 128.238.29.22   128.238.38.160  DNS   135 Standard query response 0x0002 No such name NS mit.edu.poly.edu SOA dns-prime.poly.edu
492 2004-09-01 04:20:35.850423 128.238.38.160  128.238.29.22   DNS    67 Standard query 0x0003 NS mit.edu
493 2004-09-01 04:20:35.850784 128.238.29.22   128.238.38.160  DNS   176 Standard query response 0x0003 NS mit.edu NS bitsy.mit.edu NS strawb.mit.edu NS w20ns.mit.e
 20 2004-09-01 04:20:06.451492 128.238.38.2    224.0.0.2       HSRP   62 Hello (state Active)
 71 2004-09-01 04:20:09.223448 128.238.38.2    224.0.0.2       HSRP   62 Hello (state Active)
106 2004-09-01 04:20:11.819606 128.238.38.2    224.0.0.2       HSRP   62 Hello (state Active)
153 2004-09-01 04:20:14.511557 128.238.38.2    224.0.0.2       HSRP   62 Hello (state Active)
207 2004-09-01 04:20:17.471504 128.238.38.2    224.0.0.2       HSRP   62 Hello (state Active)

> Frame 492: 67 bytes on wire (536 bits), 67 bytes captured (536 bits)
> Ethernet II, Src: IBM_10:60:99 (00:09:6b:10:60:99), Dst: All-HSRP-routers_00 (00:00:0c:07:ac:00)
> Internet Protocol Version 4, Src: 128.238.38.160, Dst: 128.238.29.22
> User Datagram Protocol, Src Port: 3746, Dst Port: 53
> Domain Name System (query)
```

The query is sent to 128.238.29.22, the same IP address as that of my default local DNS server.

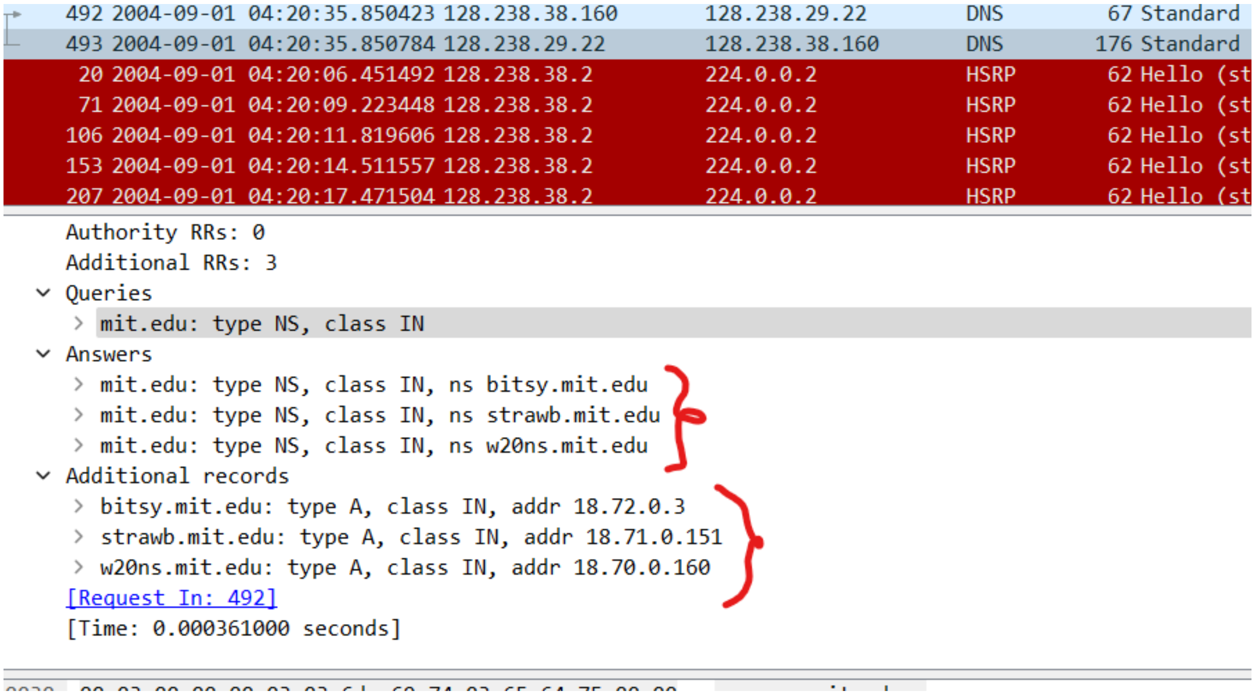
17/



```
489 2004-09-01 04:20:35.849007 128.238.29.22   128.238.38.160  DNS   118 Standard query response 0x0001 PTR 22.29.2
490 2004-09-01 04:20:35.849848 128.238.38.160  128.238.29.22   DNS    76 Standard query 0x0002 NS mit.edu.poly.edu
491 2004-09-01 04:20:35.850192 128.238.29.22   128.238.38.160  DNS   135 Standard query response 0x0002 No such nam
492 2004-09-01 04:20:35.850423 128.238.38.160  128.238.29.22   DNS    67 Standard query 0x0003 NS mit.edu
493 2004-09-01 04:20:35.850784 128.238.29.22   128.238.38.160  DNS   176 Standard query response 0x0003 NS mit.edu
 20 2004-09-01 04:20:06.451492 128.238.38.2    224.0.0.2       HSRP   62 Hello (state Active)
 71 2004-09-01 04:20:09.223448 128.238.38.2    224.0.0.2       HSRP   62 Hello (state Active)
106 2004-09-01 04:20:11.819606 128.238.38.2    224.0.0.2       HSRP   62 Hello (state Active)
153 2004-09-01 04:20:14.511557 128.238.38.2    224.0.0.2       HSRP   62 Hello (state Active)
207 2004-09-01 04:20:17.471504 128.238.38.2    224.0.0.2       HSRP   62 Hello (state Active)

> Frame 492: 67 bytes on wire (536 bits), 67 bytes captured (536 bits)
> Ethernet II, Src: IBM_10:60:99 (00:09:6b:10:60:99), Dst: All-HSRP-routers_00 (00:00:0c:07:ac:00)
> Internet Protocol Version 4, Src: 128.238.38.160, Dst: 128.238.29.22
> User Datagram Protocol, Src Port: 3746, Dst Port: 53
v Domain Name System (query)
    Transaction ID: 0x0003
  > Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  v Queries
    > mit.edu: type NS, class IN
    [Response In: 493]
```

The DNS query is a type "NS" message including one question. The query message did not contain any answers.

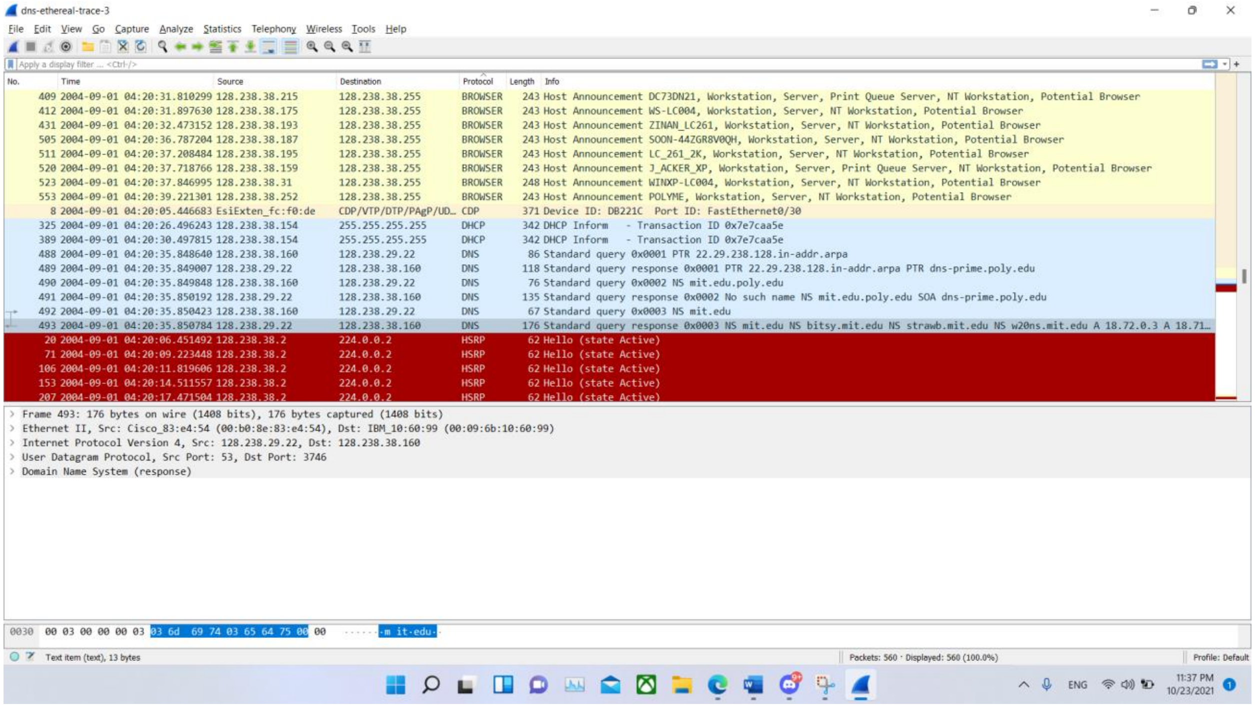
18/



```
492 2004-09-01 04:20:35.850423 128.238.38.160   128.238.29.22   DNS    67 Standard
493 2004-09-01 04:20:35.850784 128.238.29.22    128.238.38.160  DNS   176 Standard
 20 2004-09-01 04:20:06.451492 128.238.38.2     224.0.0.2       HSRP   62 Hello (st
 71 2004-09-01 04:20:09.223448 128.238.38.2     224.0.0.2       HSRP   62 Hello (st
106 2004-09-01 04:20:11.819606 128.238.38.2     224.0.0.2       HSRP   62 Hello (st
153 2004-09-01 04:20:14.511557 128.238.38.2     224.0.0.2       HSRP   62 Hello (st
207 2004-09-01 04:20:17.471504 128.238.38.2     224.0.0.2       HSRP   62 Hello (st

    Authority RRs: 0
    Additional RRs: 3
  ∨ Queries
    > mit.edu: type NS, class IN
  ∨ Answers
    > mit.edu: type NS, class IN, ns bitsy.mit.edu
    > mit.edu: type NS, class IN, ns strawb.mit.edu
    > mit.edu: type NS, class IN, ns w20ns.mit.edu
  ∨ Additional records
    > bitsy.mit.edu: type A, class IN, addr 18.72.0.3
    > strawb.mit.edu: type A, class IN, addr 18.71.0.151
    > w20ns.mit.edu: type A, class IN, addr 18.70.0.160
    [Request In: 492]
    [Time: 0.000361000 seconds]
```

The response message provides 3 MIT nameservers: w20ns.mit.edu[18.70.0.160], strawb.mit.edu[18.71.0.150], and bitsy.mit.edu[18.72.0.3]. The IP addresses for the nameservers was included under the additional records category sent back as part of the response message.

19/

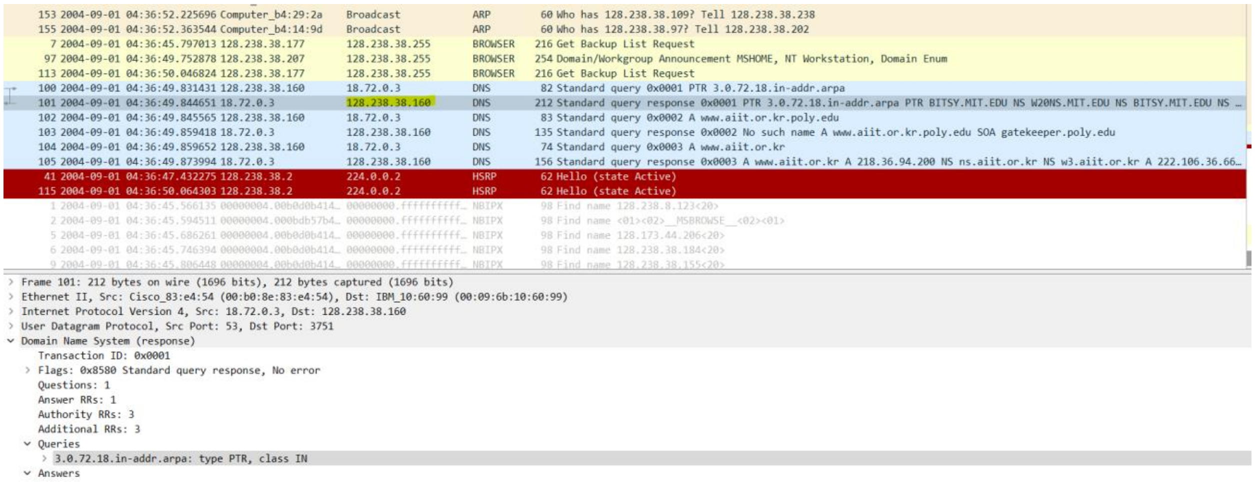


dns-ethereal-trace-3
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

```
No.  Time                       Source           Destination          Protocol Length Info
409 2004-09-01 04:20:31.810299 128.238.38.215   128.238.38.255       BROWSER  243 Host Announcement DC73DN21, Workstation, Server, Print Queue Server, NT Workstation, Potential Browser
412 2004-09-01 04:20:31.897630 128.238.38.175   128.238.38.255       BROWSER  243 Host Announcement WS-LC004, Workstation, Server, NT Workstation, Potential Browser
431 2004-09-01 04:20:32.473152 128.238.38.193   128.238.38.255       BROWSER  243 Host Announcement ZINAN_LC261, Workstation, Server, NT Workstation, Potential Browser
505 2004-09-01 04:20:36.787204 128.238.38.187   128.238.38.255       BROWSER  243 Host Announcement SOON-44ZGR8V0QH, Workstation, Server, NT Workstation, Potential Browser
511 2004-09-01 04:20:37.208484 128.238.38.195   128.238.38.255       BROWSER  243 Host Announcement LC_261_2K, Workstation, Server, NT Workstation, Potential Browser
520 2004-09-01 04:20:37.718766 128.238.38.159   128.238.38.255       BROWSER  243 Host Announcement J_ACKER_XP, Workstation, Server, Print Queue Server, NT Workstation, Potential Browser
523 2004-09-01 04:20:37.846995 128.238.38.31    128.238.38.255       BROWSER  248 Host Announcement WINXP-LC004, Workstation, Server, NT Workstation, Potential Browser
553 2004-09-01 04:20:39.221301 128.238.38.252   128.238.38.255       BROWSER  243 Host Announcement POLYME, Workstation, Server, NT Workstation, Potential Browser
  8 2004-09-01 04:20:05.446683 EsiExten_fc:f0:de CDP/VTP/DTP/PAgP/UD… CDP      371 Device ID: DB221C  Port ID: FastEthernet0/30
325 2004-09-01 04:20:26.496243 128.238.38.154   255.255.255.255      DHCP     342 DHCP Inform   - Transaction ID 0x7e7caa5e
389 2004-09-01 04:20:30.497815 128.238.38.154   255.255.255.255      DHCP     342 DHCP Inform   - Transaction ID 0x7e7caa5e
488 2004-09-01 04:20:35.848640 128.238.38.160   128.238.29.22        DNS       86 Standard query 0x0001 PTR 22.29.238.128.in-addr.arpa
489 2004-09-01 04:20:35.849007 128.238.29.22    128.238.38.160       DNS      118 Standard query response 0x0001 PTR 22.29.238.128.in-addr.arpa PTR dns-prime.poly.edu
490 2004-09-01 04:20:35.849848 128.238.38.160   128.238.29.22        DNS       76 Standard query 0x0002 NS mit.edu.poly.edu
491 2004-09-01 04:20:35.850192 128.238.29.22    128.238.38.160       DNS      135 Standard query response 0x0002 No such name NS mit.edu.poly.edu SOA dns-prime.poly.edu
492 2004-09-01 04:20:35.850423 128.238.38.160   128.238.29.22        DNS       67 Standard query 0x0003 NS mit.edu
493 2004-09-01 04:20:35.850784 128.238.29.22    128.238.38.160       DNS      176 Standard query response 0x0003 NS mit.edu NS bitsy.mit.edu NS strawb.mit.edu NS w20ns.mit.edu A 18.72.0.3 A 18.71…
 20 2004-09-01 04:20:06.451492 128.238.38.2     224.0.0.2            HSRP      62 Hello (state Active)
 71 2004-09-01 04:20:09.223448 128.238.38.2     224.0.0.2            HSRP      62 Hello (state Active)
106 2004-09-01 04:20:11.819606 128.238.38.2     224.0.0.2            HSRP      62 Hello (state Active)
153 2004-09-01 04:20:14.511557 128.238.38.2     224.0.0.2            HSRP      62 Hello (state Active)
207 2004-09-01 04:20:17.471504 128.238.38.2     224.0.0.2            HSRP      62 Hello (state Active)

> Frame 493: 176 bytes on wire (1408 bits), 176 bytes captured (1408 bits)
> Ethernet II, Src: Cisco_83:e4:54 (00:b0:8e:83:e4:54), Dst: IBM_10:60:99 (00:09:6b:10:60:99)
> Internet Protocol Version 4, Src: 128.238.29.22, Dst: 128.238.38.160
> User Datagram Protocol, Src Port: 53, Dst Port: 3746
> Domain Name System (response)

0030  00 03 00 00 00 03 03 6d  69 74 03 65 64 75 00 00   ······m it·edu··

Text item (text), 13 bytes          Packets: 560 · Displayed: 560 (100.0%)          Profile: Default
```

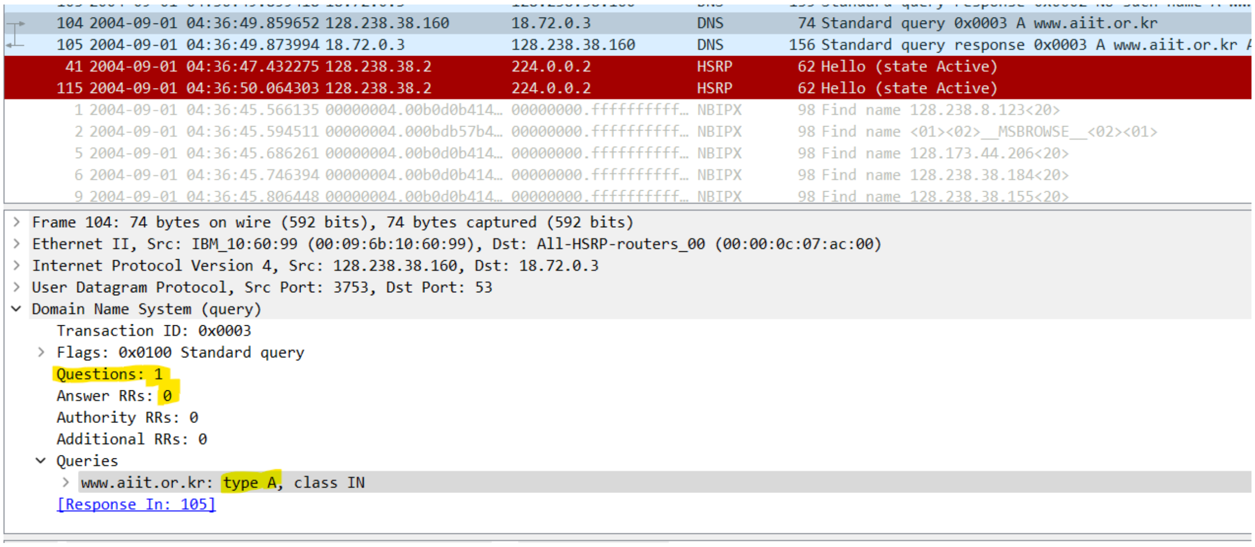
20/

This DNS query message is sent to 128.238.38.160 which is the IP address of the MIT DNS response sender.



```
153 2004-09-01 04:36:52.225696 Computer_b4:29:2a  Broadcast          ARP       60 Who has 128.238.38.109? Tell 128.238.38.238
155 2004-09-01 04:36:52.363544 Computer_b4:14:9d  Broadcast          ARP       60 Who has 128.238.38.97? Tell 128.238.38.202
  7 2004-09-01 04:36:45.797013 128.238.38.177     128.238.38.255     BROWSER  216 Get Backup List Request
 97 2004-09-01 04:36:49.752878 128.238.38.207     128.238.38.255     BROWSER  254 Domain/Workgroup Announcement MSHOME, NT Workstation, Domain Enum
113 2004-09-01 04:36:50.046824 128.238.38.177     128.238.38.255     BROWSER  216 Get Backup List Request
100 2004-09-01 04:36:49.831431 128.238.38.160     18.72.0.3          DNS       82 Standard query 0x0001 PTR 3.0.72.18.in-addr.arpa
101 2004-09-01 04:36:49.844651 18.72.0.3          128.238.38.160     DNS      212 Standard query response 0x0001 PTR 3.0.72.18.in-addr.arpa PTR BITSY.MIT.EDU NS W20NS.MIT.EDU NS BITSY.MIT.EDU NS …
102 2004-09-01 04:36:49.845565 128.238.38.160     18.72.0.3          DNS       83 Standard query 0x0002 A www.aiit.or.kr.poly.edu
103 2004-09-01 04:36:49.859418 18.72.0.3          128.238.38.160     DNS      135 Standard query response 0x0002 No such name A www.aiit.or.kr.poly.edu SOA gatekeeper.poly.edu
104 2004-09-01 04:36:49.859652 128.238.38.160     18.72.0.3          DNS       74 Standard query 0x0003 A www.aiit.or.kr
105 2004-09-01 04:36:49.873994 18.72.0.3          128.238.38.160     DNS      156 Standard query response 0x0003 A www.aiit.or.kr A 218.36.94.200 NS ns.aiit.or.kr NS w3.aiit.or.kr A 222.106.36.66…
 41 2004-09-01 04:36:47.432275 128.238.38.2       224.0.0.2          HSRP      62 Hello (state Active)
115 2004-09-01 04:36:50.064303 128.238.38.2       224.0.0.2          HSRP      62 Hello (state Active)
  1 2004-09-01 04:36:45.566135 00000004.00b0d0b414… 00000000.ffffffffff… NBIPX  98 Find name 128.238.8.123<20>
  2 2004-09-01 04:36:45.594511 00000004.000bdb57b4… 00000000.ffffffffff… NBIPX  98 Find name <01><02>__MSBROWSE__<02><01>
  5 2004-09-01 04:36:45.686261 00000004.00b0d0b414… 00000000.ffffffffff… NBIPX  98 Find name 128.173.44.206<20>
  6 2004-09-01 04:36:45.746394 00000004.00b0d0b414… 00000000.ffffffffff… NBIPX  98 Find name 128.238.38.184<20>
  9 2004-09-01 04:36:45.806448 00000004.00b0d0b414… 00000000.ffffffffff… NBIPX  98 Find name 128.238.38.155<20>

> Frame 101: 212 bytes on wire (1696 bits), 212 bytes captured (1696 bits)
> Ethernet II, Src: Cisco_83:e4:54 (00:b0:8e:83:e4:54), Dst: IBM_10:60:99 (00:09:6b:10:60:99)
> Internet Protocol Version 4, Src: 18.72.0.3, Dst: 128.238.38.160
> User Datagram Protocol, Src Port: 53, Dst Port: 3751
v Domain Name System (response)
    Transaction ID: 0x0001
  > Flags: 0x8580 Standard query response, No error
    Questions: 1
    Answer RRs: 1
    Authority RRs: 3
    Additional RRs: 3
  v Queries
    > 3.0.72.18.in-addr.arpa: type PTR, class IN
  v Answers
```

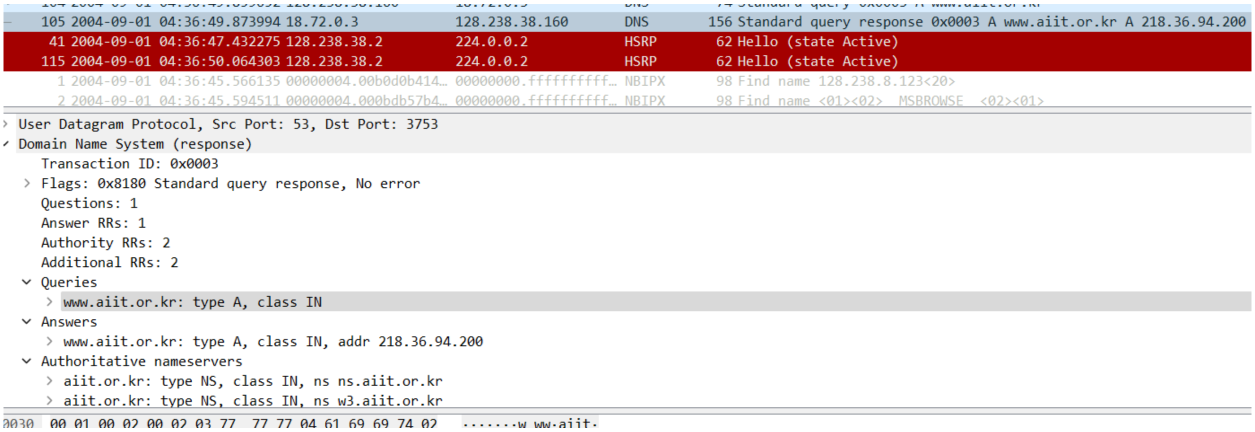
21/



```
104 2004-09-01 04:36:49.859652 128.238.38.160     18.72.0.3          DNS       74 Standard query 0x0003 A www.aiit.or.kr
105 2004-09-01 04:36:49.873994 18.72.0.3          128.238.38.160     DNS      156 Standard query response 0x0003 A www.aiit.or.kr A
 41 2004-09-01 04:36:47.432275 128.238.38.2       224.0.0.2          HSRP      62 Hello (state Active)
115 2004-09-01 04:36:50.064303 128.238.38.2       224.0.0.2          HSRP      62 Hello (state Active)
  1 2004-09-01 04:36:45.566135 00000004.00b0d0b414… 00000000.ffffffffff… NBIPX  98 Find name 128.238.8.123<20>
  2 2004-09-01 04:36:45.594511 00000004.000bdb57b4… 00000000.ffffffffff… NBIPX  98 Find name <01><02>__MSBROWSE__<02><01>
  5 2004-09-01 04:36:45.686261 00000004.00b0d0b414… 00000000.ffffffffff… NBIPX  98 Find name 128.173.44.206<20>
  6 2004-09-01 04:36:45.746394 00000004.00b0d0b414… 00000000.ffffffffff… NBIPX  98 Find name 128.238.38.184<20>
  9 2004-09-01 04:36:45.806448 00000004.00b0d0b414… 00000000.ffffffffff… NBIPX  98 Find name 128.238.38.155<20>

> Frame 104: 74 bytes on wire (592 bits), 74 bytes captured (592 bits)
> Ethernet II, Src: IBM_10:60:99 (00:09:6b:10:60:99), Dst: All-HSRP-routers_00 (00:00:0c:07:ac:00)
> Internet Protocol Version 4, Src: 128.238.38.160, Dst: 18.72.0.3
> User Datagram Protocol, Src Port: 3753, Dst Port: 53
v Domain Name System (query)
    Transaction ID: 0x0003
  > Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  v Queries
    > www.aiit.or.kr: type A, class IN
    [Response In: 105]
```

This DNS query is a type “A” query. The message does not contain any answers.

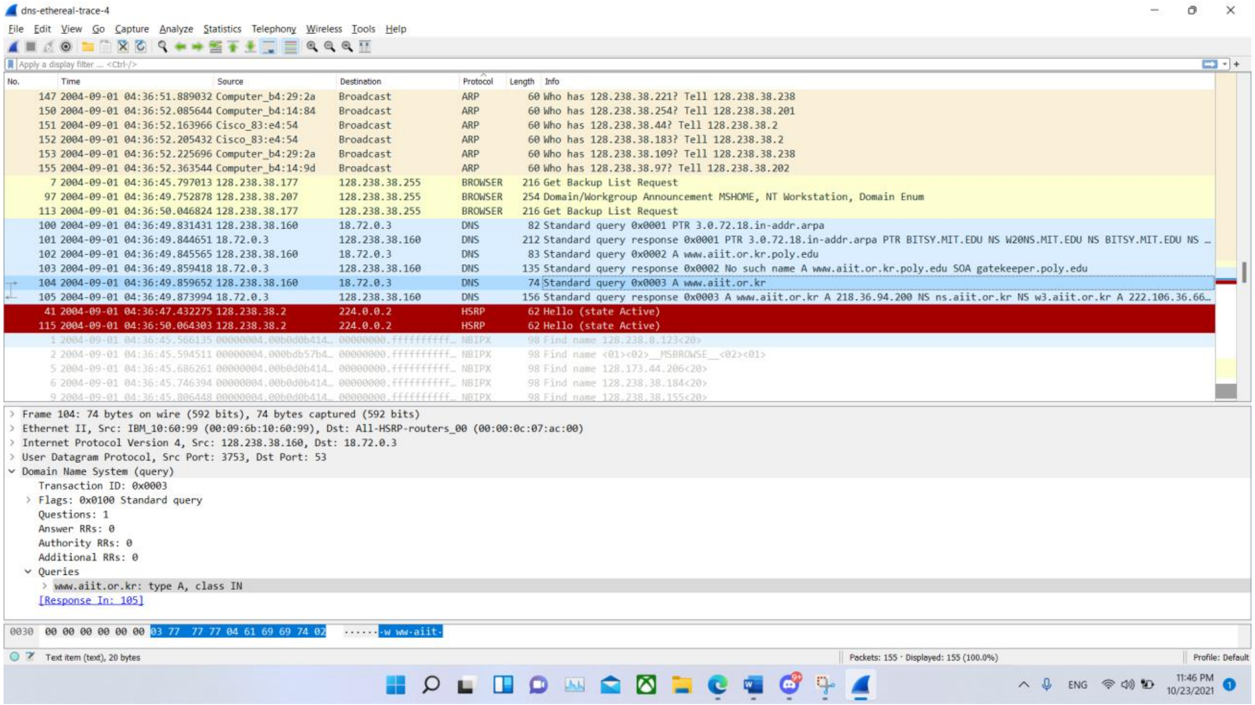
22/



```
105 2004-09-01 04:36:49.873994 18.72.0.3      128.238.38.160  DNS    156 Standard query response 0x0003 A www.aiit.or.kr A 218.36.94.200
 41 2004-09-01 04:36:47.432275 128.238.38.2   224.0.0.2       HSRP    62 Hello (state Active)
115 2004-09-01 04:36:50.064303 128.238.38.2   224.0.0.2       HSRP    62 Hello (state Active)
  1 2004-09-01 04:36:45.566135 00000004.00b0d0b414… 00000000.ffffffffff… NBIPX  98 Find name 128.238.8.123<20>
  2 2004-09-01 04:36:45.594511 00000004.000bdb57b4… 00000000.ffffffffff… NBIPX  98 Find name <01><02>__MSBROWSE__<02><01>
> User Datagram Protocol, Src Port: 53, Dst Port: 3753
⌄ Domain Name System (response)
    Transaction ID: 0x0003
  > Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 1
    Authority RRs: 2
    Additional RRs: 2
  ⌄ Queries
    > www.aiit.or.kr: type A, class IN
  ⌄ Answers
    > www.aiit.or.kr: type A, class IN, addr 218.36.94.200
  ⌄ Authoritative nameservers
    > aiit.or.kr: type NS, class IN, ns ns.aiit.or.kr
    > aiit.or.kr: type NS, class IN, ns w3.aiit.or.kr
0030  00 01 00 02 00 02 03 77  77 77 04 61 69 69 74 02   .......w ww.aiit.
```

It only provided one “answer” containing the servers IP address.

23/



dns-ethereal-trace-4
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>

```
No.  Time                       Source             Destination      Protocol Length Info
147 2004-09-01 04:36:51.889032 Computer_b4:29:2a Broadcast        ARP       60 Who has 128.238.38.221? Tell 128.238.38.238
150 2004-09-01 04:36:52.085644 Computer_b4:14:84 Broadcast        ARP       60 Who has 128.238.38.254? Tell 128.238.38.201
151 2004-09-01 04:36:52.163966 Cisco_83:e4:54    Broadcast        ARP       60 Who has 128.238.38.44? Tell 128.238.38.2
152 2004-09-01 04:36:52.205432 Cisco_83:e4:54    Broadcast        ARP       60 Who has 128.238.38.183? Tell 128.238.38.2
153 2004-09-01 04:36:52.225696 Computer_b4:29:2a Broadcast        ARP       60 Who has 128.238.38.109? Tell 128.238.38.238
155 2004-09-01 04:36:52.363544 Computer_b4:14:9d Broadcast        ARP       60 Who has 128.238.38.97? Tell 128.238.38.202
  7 2004-09-01 04:36:45.797013 128.238.38.177    128.238.38.255   BROWSER  216 Get Backup List Request
 97 2004-09-01 04:36:49.752878 128.238.38.207    128.238.38.255   BROWSER  254 Domain/Workgroup Announcement MSHOME, NT Workstation, Domain Enum
113 2004-09-01 04:36:50.046824 128.238.38.177    128.238.38.255   BROWSER  216 Get Backup List Request
100 2004-09-01 04:36:49.831431 128.238.38.160    18.72.0.3        DNS       82 Standard query 0x0001 PTR 3.0.72.18.in-addr.arpa
101 2004-09-01 04:36:49.844651 18.72.0.3         128.238.38.160   DNS      212 Standard query response 0x0001 PTR 3.0.72.18.in-addr.arpa PTR BITSY.MIT.EDU NS W20NS.MIT.EDU NS BITSY.MIT.EDU NS …
102 2004-09-01 04:36:49.845565 128.238.38.160    18.72.0.3        DNS       83 Standard query 0x0002 A www.aiit.or.kr.poly.edu
103 2004-09-01 04:36:49.859418 18.72.0.3         128.238.38.160   DNS      135 Standard query response 0x0002 No such name A www.aiit.or.kr.poly.edu SOA gatekeeper.poly.edu
104 2004-09-01 04:36:49.859652 128.238.38.160    18.72.0.3        DNS       74 Standard query 0x0003 A www.aiit.or.kr
105 2004-09-01 04:36:49.873994 18.72.0.3         128.238.38.160   DNS      156 Standard query response 0x0003 A www.aiit.or.kr A 218.36.94.200 NS ns.aiit.or.kr NS w3.aiit.or.kr A 222.106.36.66…
 41 2004-09-01 04:36:47.432275 128.238.38.2      224.0.0.2        HSRP      62 Hello (state Active)
115 2004-09-01 04:36:50.064303 128.238.38.2      224.0.0.2        HSRP      62 Hello (state Active)
  1 2004-09-01 04:36:45.566135 00000004.00b0d0b414… 00000000.ffffffffff… NBIPX  98 Find name 128.238.8.123<20>
  2 2004-09-01 04:36:45.594511 00000004.000bdb57b4… 00000000.ffffffffff… NBIPX  98 Find name <01><02>__MSBROWSE__<02><01>
  5 2004-09-01 04:36:45.686261 00000004.00b0d0b414… 00000000.ffffffffff… NBIPX  98 Find name 128.173.44.206<20>
  6 2004-09-01 04:36:45.746394 00000004.00b0d0b414… 00000000.ffffffffff… NBIPX  98 Find name 128.238.38.184<20>
  9 2004-09-01 04:36:45.806448 00000004.00b0d0b414… 00000000.ffffffffff… NBIPX  98 Find name 128.238.38.155<20>

> Frame 104: 74 bytes on wire (592 bits), 74 bytes captured (592 bits)
> Ethernet II, Src: IBM_10:60:99 (00:09:6b:10:60:99), Dst: All-HSRP-routers_00 (00:00:0c:07:ac:00)
> Internet Protocol Version 4, Src: 128.238.38.160, Dst: 18.72.0.3
> User Datagram Protocol, Src Port: 3753, Dst Port: 53
⌄ Domain Name System (query)
    Transaction ID: 0x0003
  > Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  ⌄ Queries
    > www.aiit.or.kr: type A, class IN
    [Response In: 105]

0030  00 00 00 00 00 00 03 77  77 77 04 61 69 69 74 02   ......·w ww·aiit·

Text item (text), 20 bytes          Packets: 155 · Displayed: 155 (100.0%)          Profile: Default
```