Lab 3 Solution

EE450

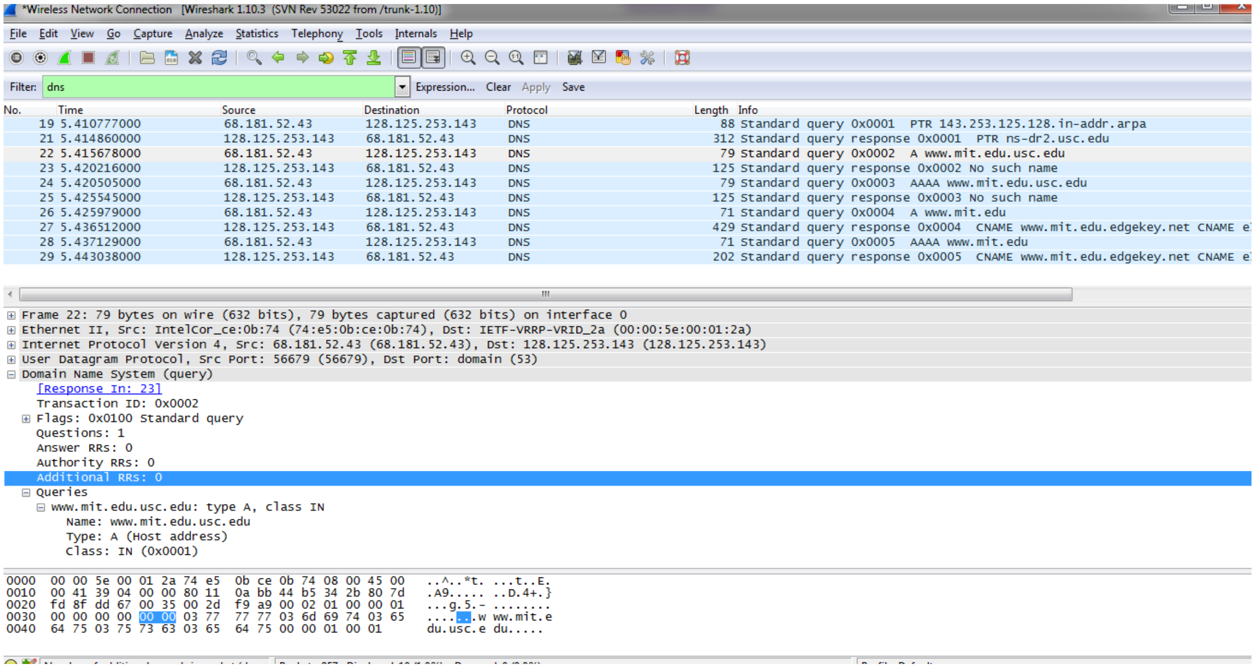
Dr. Walker

1) Using most of the websites whose severs are located in Asia the shown dns server would be you local one, for me it was the USC dns server: ns-dr2.usc.edu
   The IP address of the server: 128.125.253.143
2) I tried the website for TUDelft at Netherland. Here are the results:

ns1.tudelft.nl	130.161.180.1
ns2.tudelft.nl	130.161.180.65
ns3.tudelft.nl	131.155.0.38

3) When you do that it is probable that you get the message: *Query Refused*. In many cases the DNS servers dedicated to a university or an organization are set in a way to refuse queries from clients outside of their domain. In this way they avoid congestion.
4) There are two DNS packets, one sent and one received, both of them used UDP.
5) The destined for port for both packets is 53.
6) The DNS query is sent to a local DNS server to retrieve the destination IP. In my case it was destined for 128.125.253.143 which is the same as what obtained via ipconfig.
7) Looking at the Domain name system query part of the message you can find the the message is type A. The query massage contain no answer.
8) The response contains 4 answers which show the hierarchical structure of DNS structure and show how DNS actually resolve an IP address. You may need to go multiple layers (here 4) to get to the node which has the actual data.
9) Yes. The destination IP address of the SYN packet correspond to the last IP in the DNS response.
10) No, to retrieve the images no new DNS queries were issued.
11) The destination port of the DNS query and the source port of the DNS response is 53.
12) The DNS query message is sent to the default local DNS server. For me it was: 128.125.253.143.
13) The DNS query here is of type "AAAA" and there is no answer contained in the query.
14) The DNS response massage contains 2 answers. The answers contain the name, type, class and the canonical name in the DNS database.

15) Screen shot:


*Wireless Network Connection [Wireshark 1.10.3 (SVN Rev 53022 from /trunk-1.10)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter: dns
Expression... Clear Apply Save

```
No.   Time          Source            Destination       Protocol   Length  Info
   19 5.410777000   68.181.52.43      128.125.253.143   DNS            88 Standard query 0x0001  PTR 143.253.125.128.in-addr.arpa
   21 5.414860000   128.125.253.143   68.181.52.43      DNS           312 Standard query response 0x0001  PTR ns-dr2.usc.edu
   22 5.415678000   68.181.52.43      128.125.253.143   DNS            79 Standard query 0x0002  A www.mit.edu.usc.edu
   23 5.420216000   128.125.253.143   68.181.52.43      DNS           125 Standard query response 0x0002 No such name
   24 5.420505000   68.181.52.43      128.125.253.143   DNS            79 Standard query 0x0003  AAAA www.mit.edu.usc.edu
   25 5.425545000   128.125.253.143   68.181.52.43      DNS           125 Standard query response 0x0003 No such name
   26 5.425979000   68.181.52.43      128.125.253.143   DNS            71 Standard query 0x0004  A www.mit.edu
   27 5.436512000   128.125.253.143   68.181.52.43      DNS           429 Standard query response 0x0004  CNAME www.mit.edu.edgekey.net CNAME e
   28 5.437129000   68.181.52.43      128.125.253.143   DNS            71 Standard query 0x0005  AAAA www.mit.edu
   29 5.443038000   128.125.253.143   68.181.52.43      DNS           202 Standard query response 0x0005  CNAME www.mit.edu.edgekey.net CNAME e
```

```
⊞ Frame 22: 79 bytes on wire (632 bits), 79 bytes captured (632 bits) on interface 0
⊞ Ethernet II, Src: IntelCor_ce:0b:74 (74:e5:0b:ce:0b:74), Dst: IETF-VRRP-VRID_2a (00:00:5e:00:01:2a)
⊞ Internet Protocol Version 4, Src: 68.181.52.43 (68.181.52.43), Dst: 128.125.253.143 (128.125.253.143)
⊞ User Datagram Protocol, Src Port: 56679 (56679), Dst Port: domain (53)
⊟ Domain Name System (query)
    [Response In: 23]
    Transaction ID: 0x0002
  ⊞ Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  ⊟ Queries
    ⊟ www.mit.edu.usc.edu: type A, class IN
        Name: www.mit.edu.usc.edu
        Type: A (Host address)
        Class: IN (0x0001)
```

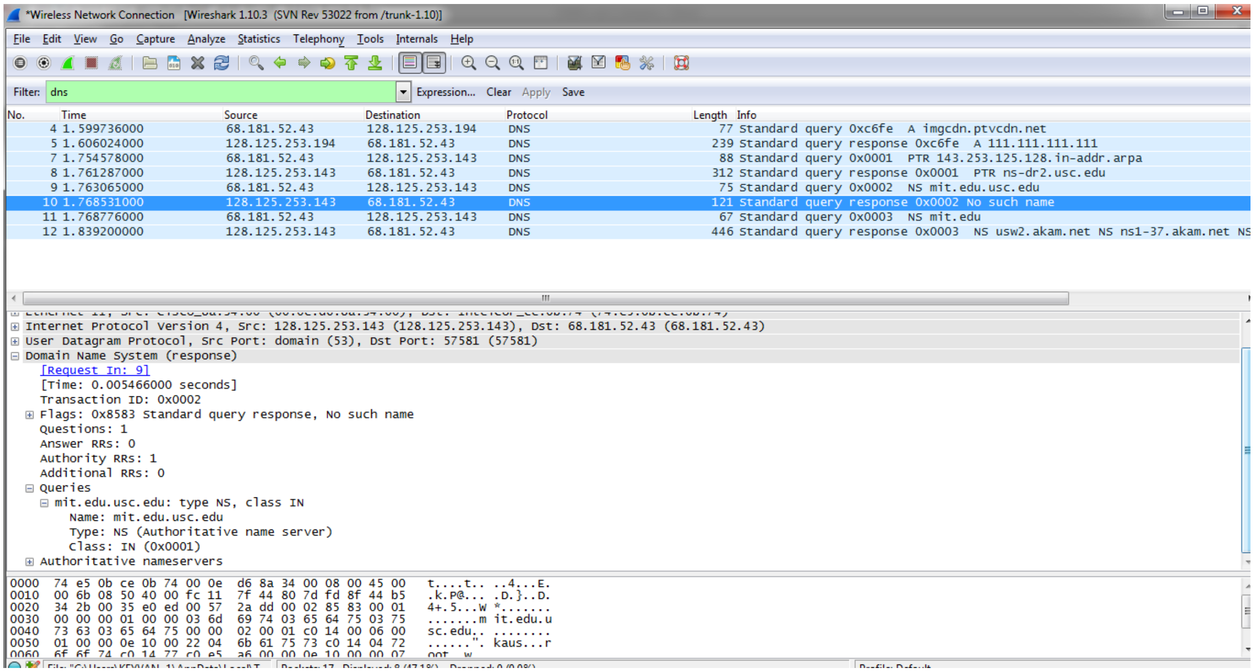
```
0000  00 00 5e 00 01 2a 74 e5  0b ce 0b 74 08 00 45 00   ..^..*t. ...t..E.
0010  00 41 39 04 00 00 80 11  0a bb 44 b5 34 2b 80 7d   .A9..... ..D.4+.}
0020  fd 8f dd 67 00 35 00 2d  f9 a9 00 02 01 00 00 01   ...g.5.- ........
0030  00 00 00 00 00 00 03 77  77 77 03 6d 69 74 03 65   .......w ww.mit.e
0040  64 75 03 75 73 63 03 65  64 75 00 00 01 00 01      du.usc.e du.....
```

16) The query is been sent to the local DNS server which is 128.125.253.143 if you try from USC campus.

17) The type of the query message was “NS”. It did not contain any answer in its body.

18) The response message provides the authoritative name servers and it does not have information of the MIT webservers IP addresses.

19) Screen shot:


*Wireless Network Connection [Wireshark 1.10.3 (SVN Rev 53022 from /trunk-1.10)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter: dns
Expression... Clear Apply Save

```
No.   Time          Source            Destination       Protocol   Length  Info
    4 1.599736000   68.181.52.43      128.125.253.194   DNS            77 Standard query 0xc6fe  A imgcdn.ptvcdn.net
    5 1.606024000   128.125.253.194   68.181.52.43      DNS           239 Standard query response 0xc6fe  A 111.111.111.111
    7 1.754578000   68.181.52.43      128.125.253.143   DNS            88 Standard query 0x0001  PTR 143.253.125.128.in-addr.arpa
    8 1.761287000   128.125.253.143   68.181.52.43      DNS           312 Standard query response 0x0001  PTR ns-dr2.usc.edu
    9 1.763065000   68.181.52.43      128.125.253.143   DNS            75 Standard query 0x0002  NS mit.edu.usc.edu
   10 1.768531000   128.125.253.143   68.181.52.43      DNS           121 Standard query response 0x0002 No such name
   11 1.768776000   68.181.52.43      128.125.253.143   DNS            67 Standard query 0x0003  NS mit.edu
   12 1.839200000   128.125.253.143   68.181.52.43      DNS           446 Standard query response 0x0003  NS usw2.akam.net NS ns1-37.akam.net NS
```

```
⊞ Internet Protocol Version 4, Src: 128.125.253.143 (128.125.253.143), Dst: 68.181.52.43 (68.181.52.43)
⊞ User Datagram Protocol, Src Port: domain (53), Dst Port: 57581 (57581)
⊟ Domain Name System (response)
    [Request In: 9]
    [Time: 0.005466000 seconds]
    Transaction ID: 0x0002
  ⊞ Flags: 0x8583 Standard query response, No such name
    Questions: 1
    Answer RRs: 0
    Authority RRs: 1
    Additional RRs: 0
  ⊟ Queries
    ⊟ mit.edu.usc.edu: type NS, class IN
        Name: mit.edu.usc.edu
        Type: NS (Authoritative name server)
        Class: IN (0x0001)
  ⊞ Authoritative nameservers
```

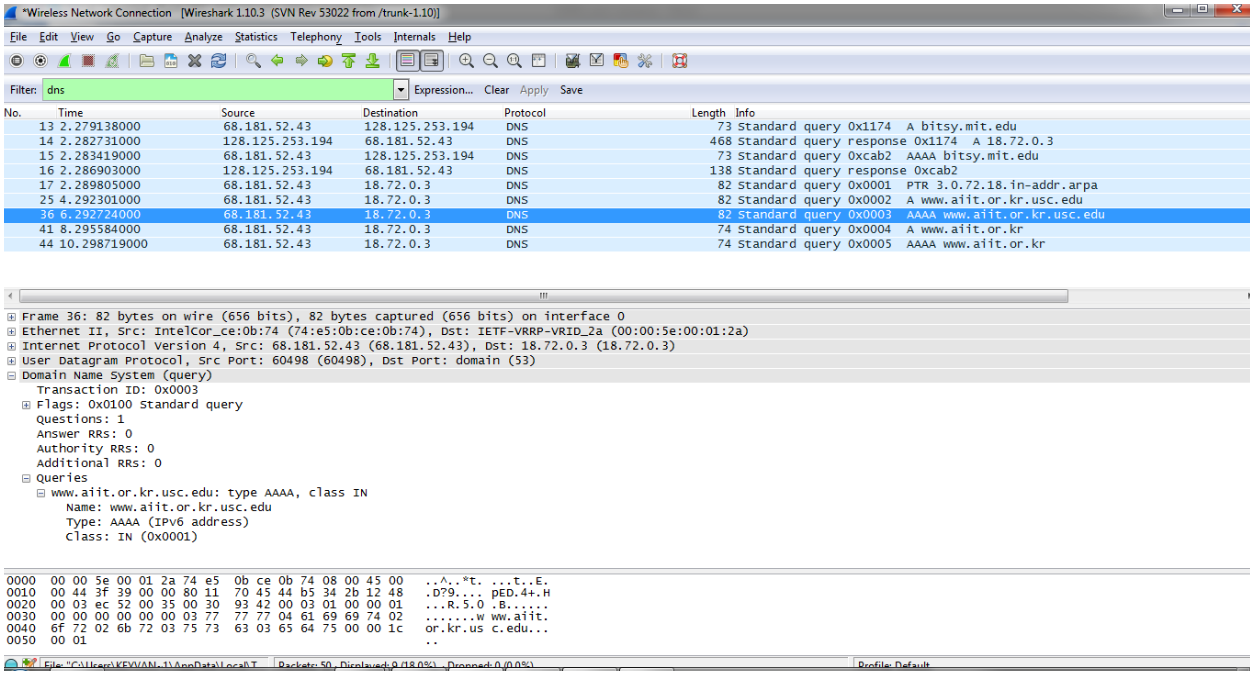
```
0000  74 e5 0b ce 0b 74 00 0e  d6 8a 34 00 08 00 45 00   t....t.. ..4...E.
0010  00 6b 08 50 40 00 fc 11  7f 44 80 7d fd 8f 44 b5   .k.P@... .D.}..D.
0020  34 2b 00 35 e0 ed 00 57  2a dd 00 02 85 83 00 01   4+.5...W *.......
0030  00 00 00 01 00 00 03 6d  69 74 03 65 64 75 03 75   .......m it.edu.u
0040  73 63 03 65 64 75 00 00  02 00 01 c0 14 00 06 00   sc.edu.. ........
0050  01 00 00 0e 10 00 22 04  6b 61 75 73 c0 14 04 72   ......". kaus...r
0060  6f 6f 74 c0 14 77 c0 e5  a6 00 00 0e 10 00 00 07   oot..w
```

20) The DNS query is sent to the address **8.8.8.8**. It is not the same as the default DNS server

21) Type: AAAA, No answer in the body

22) One answer which is the canonical name of the website.

23) Screen shot:



*Wireless Network Connection [Wireshark 1.10.3 (SVN Rev 53022 from /trunk-1.10)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Expression... Clear Apply Save

Filter: dns

```
No.     Time             Source            Destination       Protocol   Length  Info
     13 2.279138000      68.181.52.43      128.125.253.194   DNS            73 Standard query 0x1174  A bitsy.mit.edu
     14 2.282731000      128.125.253.194   68.181.52.43      DNS           468 Standard query response 0x1174  A 18.72.0.3
     15 2.283419000      68.181.52.43      128.125.253.194   DNS            73 Standard query 0xcab2  AAAA bitsy.mit.edu
     16 2.286903000      128.125.253.194   68.181.52.43      DNS           138 Standard query response 0xcab2
     17 2.289805000      68.181.52.43      18.72.0.3         DNS            82 Standard query 0x0001  PTR 3.0.72.18.in-addr.arpa
     25 4.292301000      68.181.52.43      18.72.0.3         DNS            82 Standard query 0x0002  A www.aiit.or.kr.usc.edu
     36 6.292724000      68.181.52.43      18.72.0.3         DNS            82 Standard query 0x0003  AAAA www.aiit.or.kr.usc.edu
     41 8.295584000      68.181.52.43      18.72.0.3         DNS            74 Standard query 0x0004  A www.aiit.or.kr
     44 10.298719000     68.181.52.43      18.72.0.3         DNS            74 Standard query 0x0005  AAAA www.aiit.or.kr
```

```
⊞ Frame 36: 82 bytes on wire (656 bits), 82 bytes captured (656 bits) on interface 0
⊞ Ethernet II, Src: IntelCor_ce:0b:74 (74:e5:0b:ce:0b:74), Dst: IETF-VRRP-VRID_2a (00:00:5e:00:01:2a)
⊞ Internet Protocol Version 4, Src: 68.181.52.43 (68.181.52.43), Dst: 18.72.0.3 (18.72.0.3)
⊞ User Datagram Protocol, Src Port: 60498 (60498), Dst Port: domain (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.usc.edu: type AAAA, class IN
        Name: www.aiit.or.kr.usc.edu
        Type: AAAA (IPv6 address)
        Class: IN (0x0001)
```

```
0000  00 00 5e 00 01 2a 74 e5  0b ce 0b 74 08 00 45 00   ..^..*t. ...t..E.
0010  00 44 3f 39 00 00 80 11  70 45 44 b5 34 2b 12 48   .D?9.... pED.4+.H
0020  00 03 ec 52 00 35 00 30  93 42 00 03 01 00 00 01   ...R.5.0 .B......
0030  00 00 00 00 00 00 03 77  77 77 04 61 69 69 74 02   .......w ww.aiit.
0040  6f 72 02 6b 72 03 75 73  63 03 65 64 75 00 00 1c   or.kr.us c.edu...
0050  00 01                                              ..
```

File: "C:\Users\KEYVAN~1\AppData\Local\T... Packets: 50 · Displayed: 9 (18.0%) · Dropped: 0 (0.0%) Profile: Default