

- 1) nslookup on [www.asus.com.cn](http://www.asus.com.cn). The site seems to have two ip addresses: 61.244.111.116 or 210.14.136.146
- 2) Looking up uj.edu.pl, an authoritative DNS server returned is theta.uoks.uj.edu.pl
- 3) Using the DNS server from #2, a mail server returned for yahoo.com when using -type=mx is 68.142.255.16.
- 4) Both the query and responses are sent using UDP.
- 5) The destination port of the query and the source port of the response are both 53.
- 6) The DNS query is set to 192.168.11.1. Under ipconfig, the DNS server for my Ethernet connection is also 192.168.11.1. This is interesting as that is the local address of my router. In my router's configuration, it displays additional outside DNS server. It looks like my router can act as a local DNS cache/server. My router runs DD-WRT firmware.
- 7) The query type is A. The query message has no answer field.
- 8) There is only one answer sent back in response to the query. The answer is of type A, and it contains the name of the site, the type of query, the class of query, the TTL, the length of data, and the IP address of the site. The ip address is 64.170.98.30
- 9) Yes, some of the tcp syn packets are directed at 64.170.98.30
- 10) No further DNS queries are sent to get the images. All of the images appear to reside on the same server, so local DNS caching is likely used.
- 11) The destination port of the query and the source port of the response are both 53.
- 12) The DNS server is again, 192.168.11.1, this is my default DNS server.
- 13) The query is of type A, and has no answers.
- 14) Only one answer is returned. It is type A. It has the name, class, TTL, data length, and addr. The address is 18.9.22.169.
- 15) See next page.

Intel(R) 82579V Gigabit Network Connection: \Device\NPF\_{76143EDE-D856-4AA0-8430-575B54540D89} [Wireshark 1.8.4 (SVN Rev 46250 from /trunk-1.8)]

Filter: dns

| No. | Time        | Source       | Destination  | Protocol | Length | Info   |
|-----|-------------|--------------|--------------|----------|--------|--|
| 3   | 0.253368000 | 192.168.11.1 | 192.168.11.1 | DNS      | 85     | Standard query 0x0001 PTR 1.1.1.168.192.168.11.1 |
| 4   | 0.254960000 | 192.168.11.1 | 192.168.11.1 | DNS      | 105    | Standard query response 0x0001 PTR 60-wrt        |
| 5   | 0.255404000 | 192.168.11.1 | 192.168.11.1 | DNS      | 73     | Standard query 0x0002 www.mit.edu                |
| 6   | 0.256095000 | 192.168.11.1 | 192.168.11.1 | DNS      | 87     | Standard query response 0x0002 A 18.9.22.169     |
| 7   | 0.256306000 | 192.168.11.1 | 192.168.11.1 | DNS      | 71     | Standard query 0x0003 AAAA www.mit.edu           |
| 8   | 0.377589000 | 192.168.11.1 | 192.168.11.1 | DNS      | 129    | Standard query response 0x0003                   |

Checksum: 0xcc43 [validation disabled]

Domain Name System (response)

Request ID: 51

Time: 0.000691000 seconds

Transaction ID: 0x0002

Flags: 0x180 Standard query response, no error

Questions: 1

Answer RRs: 1

Authority RRs: 0

Additional RRs: 0

Queries

www.mit.edu: type A, class IN

Name: www.mit.edu

Type: A (Host address)

Class: IN (0x0001)

Answers

www.mit.edu: type A, class IN, addr 18.9.22.169

Type: A (Host address)

Class: IN (0x0001)

Time to live: 33 seconds

Data length: 4

Addr: 18.9.22.169 (18.9.22.169)

0000 f4 6d 04 40 d8 45 00 24 a5 b3 f7 46 08 00 45 00 .m.0.E.\$...F..E.

0010 00 49 00 00 40 00 40 11 a3 29 c0 a8 0b 01 c0 a8 .I..0.0..).C.....

0020 0b 29 00 35 e2 78 00 35 cc 43 00 02 81 80 00 01 .).5.X.5..C.....

0030 00 01 00 00 00 03 77 77 03 6d 69 74 03 65 .....Www.mit.e

0040 64 75 00 00 01 00 01 c0 0c 00 01 00 00 00 du.....

0050 21 00 04 12 09 16 a9 !.....

Response Type (dns.resp.type), 2 bytes | Packets: 8 Displayed: 6 Marked: 0 Dropped: 0 | Profile: Default

- 16) The query is sent to 192.168.11.1. This is my default DNS.
- 17) The query type is NS. The query contains no answers.
- 18) The response contains three nameservers. BITSY.mit.edu, W2ONS.mit.edu, and STRAWB.mit.edu. In Additional records, the IP addresses of the servers are sent. 18.72.0.3, 18.70.0.160, and 18.71.0.151.
- 19) See next page.

User Datagram Protocol, Src Port: domain (53), Dst Port: 51571 (51571)

- Domain Name System (response)**
  - [request in: 4]
    - [Time: 0.015672000 seconds]
    - Transaction ID: 0x0002
    - Flags: 0x8180 Standard query response, no error
    - Questions: 1
    - Answer RRs: 3
    - Authority RRs: 0
    - Additional RRs: 3
    - Queries
      - mit.edu: type NS, class IN**
        - Name: mit.edu
        - Type: NS (Authoritative name server)
        - Class: IN (0x0001)
    - Answers
      - mit.edu: type NS, class IN, ns BITSY.mit.edu
      - mit.edu: type NS, class IN, ns W2ONS.mit.edu
      - mit.edu: type NS, class IN, ns STRAWB.mit.edu
    - Additional records
      - w2ons.mit.edu: type A, class IN, addr 18.70.0.160
      - strawb.mit.edu: type A, class IN, addr 18.71.0.151
      - bitsy.mit.edu: type A, class IN, addr 18.72.0.1

```

0030  00 03 00 00 00 03 03 6d 69 74 03 65 64 75 00 00 .....m it.edu..
0040  02 00 01 c0 0c 00 02 00 01 00 00 06 b9 00 08 05 BITSY.....
0050  02 44 53 53 0f 0c 00 00 00 02 00 01 00 00 06 ....W2ON S.....
0060  b9 00 08 05 57 32 30 4e 53 c0 00 0c 00 00 02 00 ....STRAWB.....
0070  01 00 00 06 b9 00 09 06 53 54 52 41 57 42 c0 0c .....9.....F.....
0080  c0 19 00 01 00 01 00 00 00 08 00 04 12 46 00 a0 .....M.....G.....
0090  c0 4d 00 01 00 01 00 00 05 07 00 04 12 47 00 97 .....M.....H.....
00a0  c0 25 00 01 00 01 00 00 03 b0 04 12 48 00 03 .....%.....
  
```

Test Item (text), 13 bytes      Packets: 10 Displayed: 4 Marked: 0 Dropped: 0      Profile: Default

- 20) There are two separate type A DNS queries, for the next four questions, I am going to use the query about aiit.or.kr, and not bitsy.mit.edu. The IP address of the query is sent to 18.72.0.3, which is bitsy.mit.edu as found out in #18. This is not my default DNS server.
- 21) The DNS query is type A. The query contains no answers.
- 22) There are two answers provided. One is of type CNAME, and contains the canonical name for aiit.or.kr which is aiit.or.kr. The other answer is of type A and has the address of aiit.or.kr as 27.102.206.87
- 23) See next page:

Intel(R) 82579V Gigabit Network Connection: \Device\NPF\_{76143EDE-D856-4AA0-8430-575B54540D89} [Wireshark 1.8.4 (SVN Rev 46250 from /trunk-1.8)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: dns

| No. | Time        | Source        | Destination   | Protocol | Length | Info  |
|-----|-------------|---------------|---------------|----------|--------|---|
| 7   | 0.258942000 | 192.168.11.41 | 192.168.11.1  | DNS      | 73     | Standard query 0x69e9 A bitsy.mit.edu                           |
| 8   | 0.273021000 | 192.168.11.1  | 192.168.11.41 | DNS      | 89     | Standard query response 0x69e9 A 18.72.0.3                      |
| 9   | 0.273900000 | 192.168.11.41 | 18.72.0.3     | DNS      | 82     | Standard query 0x0001 ptr 8.0.72.18 in-addr.arpa                |
| 10  | 0.346559000 | 18.72.0.3     | 192.168.11.41 | DNS      | 212    | Standard query response 0x0001 PTR BITSY.MIT.EDU                |
| 11  | 0.347106000 | 192.168.11.41 | 18.72.0.3     | DNS      | 74     | Standard query 0x0002 A www.aift.or.kr                          |
| 15  | 1.626438000 | 18.72.0.3     | 192.168.11.41 | DNS      | 245    | Standard query response 0x0002 CNAME aift.or.kr A 27.102.206.87 |
| 16  | 1.632050000 | 192.168.11.41 | 18.72.0.3     | DNS      | 74     | Standard query 0x0003 CNAME aift.or.kr                          |
| 26  | 1.923276000 | 18.72.0.3     | 192.168.11.41 | DNS      | 138    | Standard query response 0x0003 CNAME aift.or.kr                 |

Questions: 1  
Answer RRs: 2  
Authority RRs: 4  
Additional RRs: 4

Queries

- www.aift.or.kr: type A, class IN

Answers

- www.aift.or.kr: type CNAME, class IN, cname aift.or.kr  
Name: www.aift.or.kr  
Type: CNAME (Canonical name for an alias)  
Class: IN (0x0001)  
Time to live: 30 minutes  
Data length: 2  
Primaryname: aift.or.kr
- aift.or.kr: type A, class IN, addr 27.102.206.87  
Name: aift.or.kr  
Type: A (Host address)  
Class: IN (0x0001)  
Time to live: 30 minutes  
Data length: 4  
Addr: 27.102.206.87 (27.102.206.87)

Authoritative nameservers

Additional records

Frame (Frame), 245 bytes

Packets: 29 Displayed: 8 Marked: 0 Dropped: 0

```
C:\Windows\system32\cmd.exe

Windows IP Configuration

Successfully flushed the DNS Resolver Cache.

C:\Users\Jakub>ipconfig /displaydns

Windows IP Configuration

Could not display the DNS Resolver Cache.

C:\Users\Jakub>nslookup -type=NS nit.edu
Server: DD-WRT
Address: 192.168.11.1

Non-authoritative answer:
nit.edu nameserver = U20NS.nit.edu
nit.edu nameserver = BITSY.nit.edu
nit.edu nameserver = STRAWB.nit.edu

BITSY.nit.edu internet address = 18.72.0.3
STRAWB.nit.edu internet address = 18.71.0.151
U20NS.nit.edu internet address = 18.70.0.168

C:\Users\Jakub>ipconfig /flushdns

Windows IP Configuration

Successfully flushed the DNS Resolver Cache.

C:\Users\Jakub>nslookup -type=NS nit.edu
Server: DD-WRT
Address: 192.168.11.1

Non-authoritative answer:
nit.edu nameserver = BITSY.nit.edu
nit.edu nameserver = U20NS.nit.edu
nit.edu nameserver = STRAWB.nit.edu

U20NS.nit.edu internet address = 18.70.0.168
STRAWB.nit.edu internet address = 18.71.0.151
BITSY.nit.edu internet address = 18.72.0.3

C:\Users\Jakub>nslookup www.aift.or.kr bitsy.mit.edu
Server: BITSY.MIT.EDU
Address: 18.72.0.3

Non-authoritative answer:
Name: aift.or.kr
Address: 27.102.206.87
Aliases: www.aift.or.kr

C:\Users\Jakub>
```