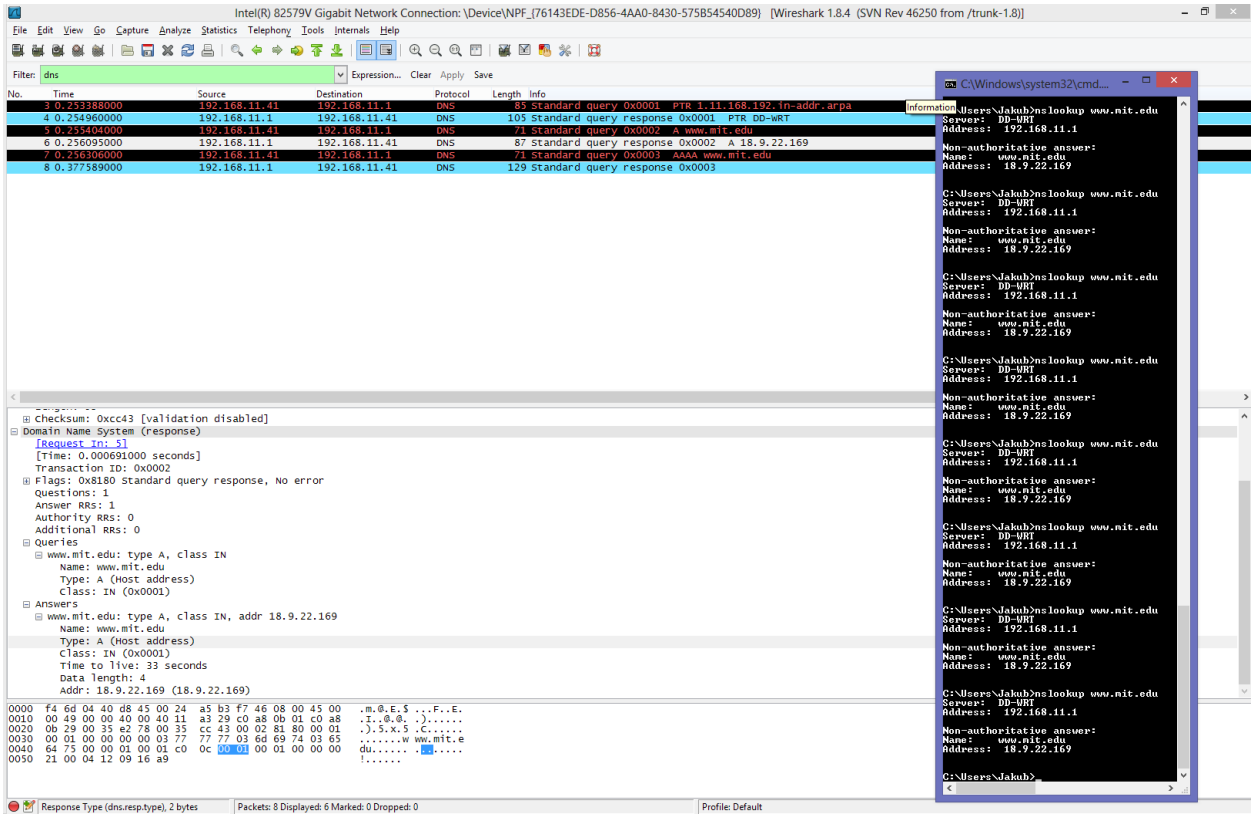
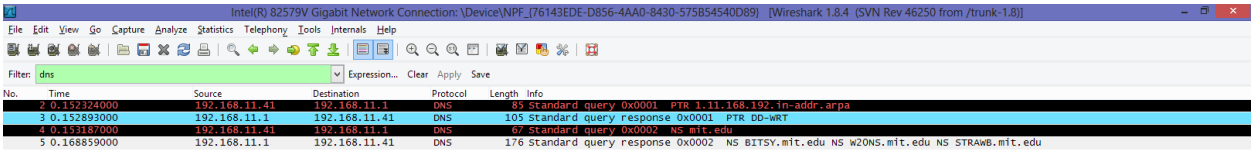
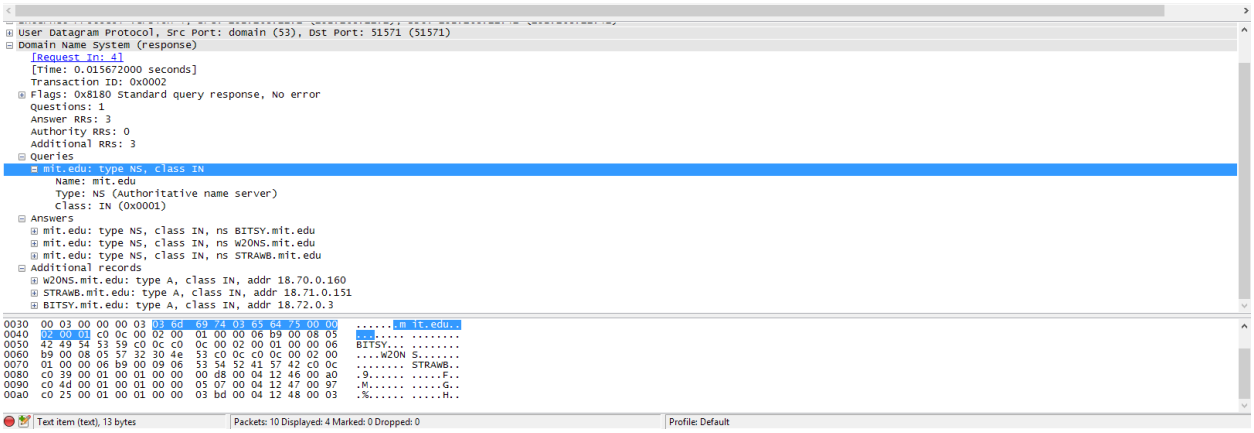
Jakub Szpunar
CS4480
WS Lab 3

1) nslookup on 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) Bothe 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 routers 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.

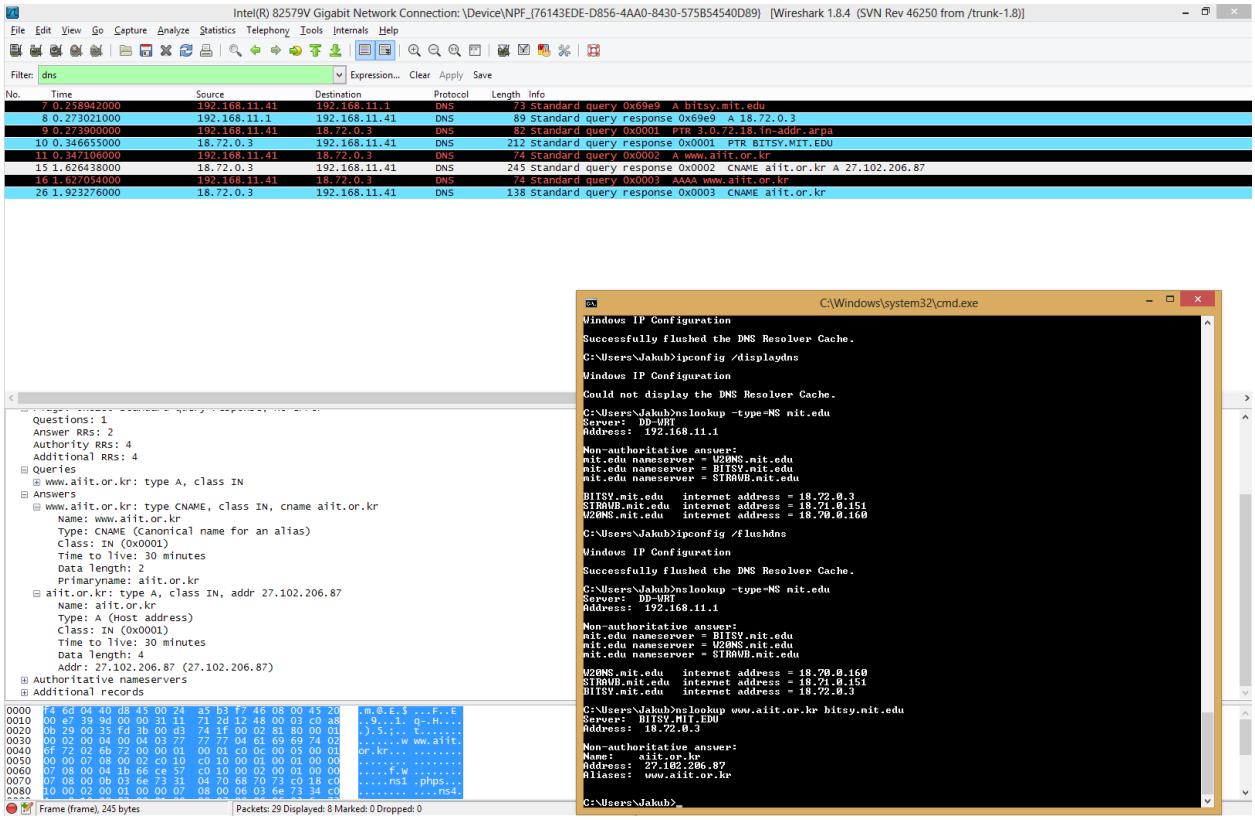


16) The query is sent to 192.168.11.1. This is my default DNS.
17) The query type is NS. The query contains no answers.
18) The response contains three nameservers. BITSY.mit.edu, W20NS.mit.edu, and STRAWB.mit.edu. In Additional records, the IP addresses of the servers are sent. 18.72.0.3, 18.70.0.160, and 18.71.0.151.
19) See next page.





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
Expression... Clear Apply Save
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 3.0.72.18.in-addr.arpa
10 0.346655000 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.aiit.or.kr
15 1.626438000 18.72.0.3 192.168.11.41 DNS 245 Standard query response 0x0002 CNAME aiit.or.kr A 27.102.206.87
16 1.627054000 192.168.11.41 18.72.0.3 DNS 74 Standard query 0x0003 AAAA www.aiit.or.kr
26 1.923276000 18.72.0.3 192.168.11.41 DNS 138 Standard query response 0x0003 CNAME aiit.or.kr
Questions: 1
Answer RRs: 2
Authority RRs: 4
Additional RRs: 4
Queries
www.aiit.or.kr: type A, class IN
Answers
www.aiit.or.kr: type CNAME, class IN, cname aiit.or.kr
Name: www.aiit.or.kr
Type: CNAME (Canonical name for an alias)
Class: IN (0x0001)
Time to live: 30 minutes
Data length: 2
Primaryname: aiit.or.kr
aiit.or.kr: type A, class IN, addr 27.102.206.87
Name: aiit.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
0000 f4 6d 04 40 d8 45 00 24 a5 b3 f7 46 08 00 45 20 .m.@.E.$ ...F..E
0010 00 e7 39 9d 00 00 31 11 71 2d 12 48 00 03 c0 a8 ..9...1. q-.H....
0020 0b 29 00 35 fd 3b 00 d3 74 1f 00 02 81 80 00 01 .).5.;.. t.......
0030 00 02 00 04 00 04 03 77 77 77 04 61 69 69 74 02 ....w ww.aiit.
0040 6f 72 02 6b 72 00 00 01 00 01 c0 0c 00 05 00 01 or.kr... ....
0050 00 00 07 08 00 02 c0 10 c0 10 00 01 00 01 00 00 ....
0060 07 08 00 04 1b 66 ce 57 c0 10 00 02 00 01 00 00 .....f.W ....
0070 07 08 00 0b 03 6e 73 31 04 70 68 70 73 c0 18 c0 .....ns1 .phps...
0080 10 00 02 00 01 00 00 07 08 00 06 03 6e 73 34 c0 ....ns4.
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 mit.edu
Server: DD-WRT
Address: 192.168.11.1
Non-authoritative answer:
mit.edu nameserver = W20NS.mit.edu
mit.edu nameserver = BITSY.mit.edu
mit.edu nameserver = STRAWB.mit.edu
BITSY.mit.edu internet address = 18.72.0.3
STRAWB.mit.edu internet address = 18.71.0.151
W20NS.mit.edu internet address = 18.70.0.160
C:\Users\Jakub>ipconfig /flushdns
Windows IP Configuration
Successfully flushed the DNS Resolver Cache.
C:\Users\Jakub>nslookup -type=NS mit.edu
Server: DD-WRT
Address: 192.168.11.1
Non-authoritative answer:
mit.edu nameserver = BITSY.mit.edu
mit.edu nameserver = W20NS.mit.edu
mit.edu nameserver = STRAWB.mit.edu
W20NS.mit.edu internet address = 18.70.0.160
STRAWB.mit.edu internet address = 18.71.0.151
BITSY.mit.edu internet address = 18.72.0.3
C:\Users\Jakub>nslookup www.aiit.or.kr bitsy.mit.edu
Server: BITSY.MIT.EDU
Address: 18.72.0.3
Non-authoritative answer:
Name: aiit.or.kr
Address: 27.102.206.87
Aliases: www.aiit.or.kr
C:\Users\Jakub>_