

# CS 3516 Lab 2

jppetitti

September 14, 2018

1. IP address of `www.aiit.or.kr`: 58.229.6.225
2. Authoritative DNS servers for Oxford University: `ecsu-sv26.easternct.edu`
3. The IP address of the DNS server is 209.244.0.3.
4. DNS queries and responses are sent over UDP
5. Destination port for DNS query: 53. Source port of response: 53
6. The DNS query message was sent to 192.168.1.1. This is the same as the address of my local DNS server (and is also the IP address of my router).
7. This query is Type A. The query does not contain any answers.
8. The response contains one answer, containing an IP address matched with a host name, along with a type, class, time to live, and data length.
9. Yes, this TCP SYN packet is sent from my host to the IP address returned in the DNS query response.
10. No, it doesn't need to issue a new DNS query because it already knows the IP address.
11. Destination port for the DNS query message: 53. Source port for the response: 53
12. The DNS query is sent to 192.168.1.1, which is the IP address of my default local DNS server

13. The query is of type A and does not contain any answers.
14. The response contains three answers, of type CNAME and A, and the canonical names and IP addresses they correspond to.
15. See screenshot1.png

No.	Time	Source	Destination	Protocol	Length	Info
1	0.060000000	192.168.1.222	18.207.50.150	TLSv1.2	129	Application Data
2	0.036074741	18.207.50.150	192.168.1.222	TLSv1.2	129	Application Data
3	0.036074740	192.168.1.222	18.207.50.150	TCP	66	38818 → 443 [ACK] Seq=64 Ack=64 Win=636 Len=0 TSval=2556214731 TSecr=2300993331
4	3.118375760	192.168.1.222	82.221.130.131	TCP	66	50542 → 443 [ACK] Seq=1 Ack=1 Win=324 Len=0 TSval=320155386 TSecr=892181928
5	5.316767020	82.221.130.131	192.168.1.222	TCP	64	443 → 50542 [RST] Seq=1 Win=0 Len=0
28	5.231929150	192.168.1.222	192.168.1.1	DNS	71	Standard query 0x3a75 A www.mit.edu
29	5.328205325	192.168.1.1	192.168.1.222	DNS	168	Standard query response 0x3a75 A www.mit.edu CNAME www.mit.edu.edgekey.net CNAME e9566.dscb.akamaiedge.net A 23.286.94.93
30	5.328880529	192.168.1.222	192.168.1.1	DNS	85	Standard query 0x3a75 AAAA e9566.dscb.akamaiedge.net
31	5.426458876	192.168.1.1	192.168.1.222	DNS	141	Standard query response 0x3a75 AAAA e9566.dscb.akamaiedge.net AAAA 2688:1488:28:39d::255e AAAA 2688:1488:28:39d::255e
34	5.090507771	192.168.1.222	34.195.196.96	TLSv1.2	129	Application Data
37	7.026747680	34.195.196.96	192.168.1.222	TLSv1.2	129	Application Data
38	7.026858868	192.168.1.222	34.195.196.96	TCP	66	50748 → 443 [ACK] Seq=64 Ack=64 Win=1319 Len=0 TSval=282382622 TSecr=3648330200

  

Type	Class	Time to live	Data length
CNAME (Canonical NAME for an alias) (5)	IN (Internet)	578	25
CNAME: www.mit.edu.edgekey.net			
www.mit.edu.edgekey.net: type CNAME, class IN, cname e9566.dscb.akamaiedge.net			
Name: www.mit.edu.edgekey.net			
Type: CNAME (Canonical NAME for an alias) (5)	IN (Internet)	60	24
CNAME: e9566.dscb.akamaiedge.net			
e9566.dscb.akamaiedge.net: type A, class IN, addr 23.286.94.93			
Name: e9566.dscb.akamaiedge.net			
Type: A (Host Address) (1)	IN (Internet)	20	4
Address: 23.286.94.93			

[Request in: 29]  
[Time: 0.096326171 seconds]

Number of answers in packet (dns.count.answers): 2 bytes

Packets: 38 · Displayed: 12 (31.6%) · Dropped: 0 (0.0%)

Profile: Default

16. The DNS query message is sent to 192.168.1.1. This is the address of my default local DNS server.
17. The query is of type NS, and it does not contain any answers.
18. The response provides these MIT nameservers:

- (a) asia2.akam.net
- (b) use2.akam.net
- (c) eur5.akam.net
- (d) use5.akam.net
- (e) ns1-37.akam.net
- (f) asia1.akam.net
- (g) ns1-173.akam.net
- (h) usw2.akam.net

The response also includes A records listing the IP addresses for each name server.

19. See screenshot2.png

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	192.168.1.222	192.168.1.1	DNS	67	Standard query 0x5572 NS mit.edu
2	0.021719814	192.168.1.1	192.168.1.222	DNS	374	Standard query response 0x5572 NS mit.edu NS asia2.akam.net
3	0.622809045	192.168.1.222	34.195.196.96	TLSv1.2	129	Application Data
4	0.628237273	192.168.1.222	18.207.50.150	TLSv1.2	131	Application Data
5	0.649310982	34.195.196.96	192.168.1.222	TLSv1.2	129	Application Data
6	0.649367713	192.168.1.222	34.195.196.96	TCP	66	50748 → 443 [ACK] Seq=64 Ack=64 Win=1444 Len=0 TSval=28...
7	0.711853837	18.207.50.150	192.168.1.222	TCP	66	443 → 38818 [ACK] Seq=1 Ack=66 Win=8 Len=0 TSval=230038...
8	1.426536724	192.168.1.222	239.255.255.250	SSDP	207	M-SEARCH * HTTP/1.1
9	2.427343540	192.168.1.222	239.255.255.250	SSDP	207	M-SEARCH * HTTP/1.1
10	2.457510969	192.168.1.146	192.168.1.222	SSDP	339	HTTP/1.1 200 OK
11	2.457559312	192.168.1.222	192.168.1.146	ICMP	367	Destination unreachable (Host administratively prohibit...
12	2.507666639	192.168.1.146	192.168.1.222	SSDP	348	HTTP/1.1 200 OK

Name: mit.edu  
 Type: NS (authoritative Name Server) (2)  
 Class: IN (0x0001)  
 Time to live: 1706  
 Data length: 7  
 Name Server: usw2.akam.net

Additional records  
 asia2.akam.net: type A, class IN, addr 95.101.36.64  
 Name: asia2.akam.net  
 Type: A (Host Address) (1)  
 Class: IN (0x0001)  
 Time to live: 7200  
 Data length: 4  
 Address: 95.101.36.64

use2.akam.net: type A, class IN, addr 96.7.49.64  
 Name: use2.akam.net  
 Type: A (Host Address) (1)  
 Class: IN (0x0001)  
 Time to live: 7200  
 Data length: 4

0030 00 00 00 00 00 00 00 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 aa 00 10 05 .....  
 0050 61 73 69 61 32 04 61 6b 61 6d 03 6e 65 74 00 c0 asia2.ak am-net..  
 0060 0c 00 02 00 01 00 00 95 aa 00 07 04 75 73 65 32 ..... use2..  
 0070 c0 2b c0 0c 00 02 00 01 00 00 06 aa 00 07 04 65 .....  
 0080 75 72 35 c0 2b c0 0c 00 02 00 01 00 06 aa 00 ur5+... ..  
 0090 07 04 75 73 65 35 c0 2b c0 0c 00 02 00 01 00 00 .....use5+... ..  
 00a0 06 aa 00 00 06 6e 73 31 2d 33 37 c0 2b c0 0c 00 .....ns1 -37+...  
 00b0 02 00 01 00 00 06 aa 00 08 05 61 73 69 61 31 c0 .....asia1..  
 00c0 2b c0 0c 00 02 00 01 00 00 06 aa 00 0a 07 6e 73 .....ns

Number of answers in packet (dns.count.answers), 2 bytes

Packets: 15 · Displayed: 15 (100.0%) · Dropped: 0 (0.0%) Profile: Default

20. The query message is being sent to 209.244.0.3, the DNS server I specified in the command.

21. The query message is of type A, and does not contain any answers.

22. The DNS response message is of type A, and contains one answer, specifying a hostname and IP address pair.

23. See screenshot3.png

Wireshark interface showing a packet capture with a filter: `ip.addr == 192.168.1.222`.

No.	Time	Source	Destination	Protocol	Length	Info
6	0.671511428	194.59.251.14	192.168.1.222	UDP	155	1197 → 39243 Len=113
7	0.671664013	192.168.1.222	194.59.251.14	ICMP	183	Destination unreachable (Port unreachable)
8	0.759025248	192.168.1.222	209.244.0.3	DNS	74	Standard query 0x85e4 A www.aiit.or.kr
9	1.237676403	194.59.251.14	192.168.1.222	UDP	155	1197 → 39243 Len=113
10	1.237899378	192.168.1.222	194.59.251.14	ICMP	183	Destination unreachable (Port unreachable)
11	1.237918845	209.244.0.3	192.168.1.222	DNS	90	Standard query response 0x85e4 A www.aiit.or.kr A 58.22...
12	1.239351003	192.168.1.222	209.244.0.3	DNS	74	Standard query 0xd4bc AAAA www.aiit.or.kr
13	1.542799546	194.59.251.14	192.168.1.222	UDP	155	1197 → 39243 Len=113
14	1.542861056	192.168.1.222	194.59.251.14	ICMP	183	Destination unreachable (Port unreachable)
17	1.850018999	209.244.0.3	192.168.1.222	DNS	128	Standard query response 0xd4bc AAAA www.aiit.or.kr SOA ...
18	2.766845361	194.59.251.14	192.168.1.222	UDP	155	1197 → 39243 Len=113
19	2.766953526	192.168.1.222	194.59.251.14	ICMP	183	Destination unreachable (Port unreachable)

Packet 11 details:

- Authority RRs: 0
- Additional RRs: 0
- Queries:
  - www.aiit.or.kr: type A, class IN
    - Name: www.aiit.or.kr
    - [Name Length: 14]
    - [Label Count: 4]
    - Type: A (Host Address) (1)
    - Class: IN (0x0001)
- Answers:
  - www.aiit.or.kr: type A, class IN, addr 58.229.6.225
    - Name: www.aiit.or.kr
    - Type: A (Host Address) (1)
    - Class: IN (0x0001)
    - Time to live: 7200
    - Data length: 4
    - Address: 58.229.6.225
- [Request in: 8]
- [Time: 0.478893597 seconds]

Packet 11 raw data (hex):

```

0000 e4 b3 18 45 f5 6f 60 45 cb cb 31 d0 08 00 45 00 ...E o`E --1...E
0010 00 4c 00 00 40 00 37 11 af 23 d1 f4 00 03 c0 a8 ...L-@-7- -#-....
0020 01 de 00 35 c7 8d 00 38 3d 42 85 e4 81 80 00 01 ...5...8 =B-....
0030 00 01 00 00 00 00 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 01 00 01 or-kr-...
0050 00 00 1c 20 00 04 3a e5 00 e1 .....:

```

Wireshark status: wireshark\_wlp4s0\_20180914164203\_QiD0qT.pcapng | Packets: 20 · Displayed: 14 (70.0%) · Dropped: 0 (0.0%) | Profile: Default