CS 3516 Lab 2

jppetitti

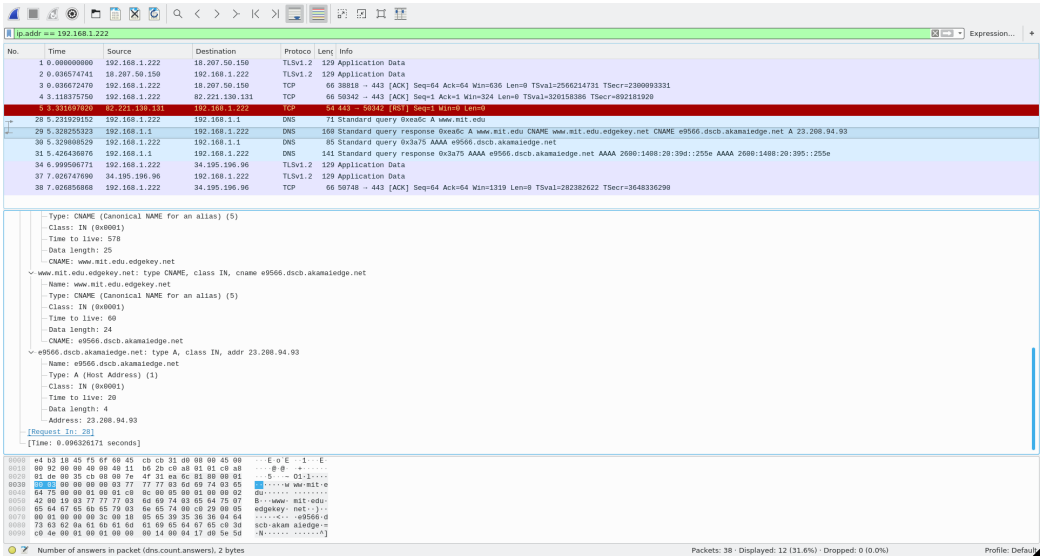
September 14, 2018

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



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

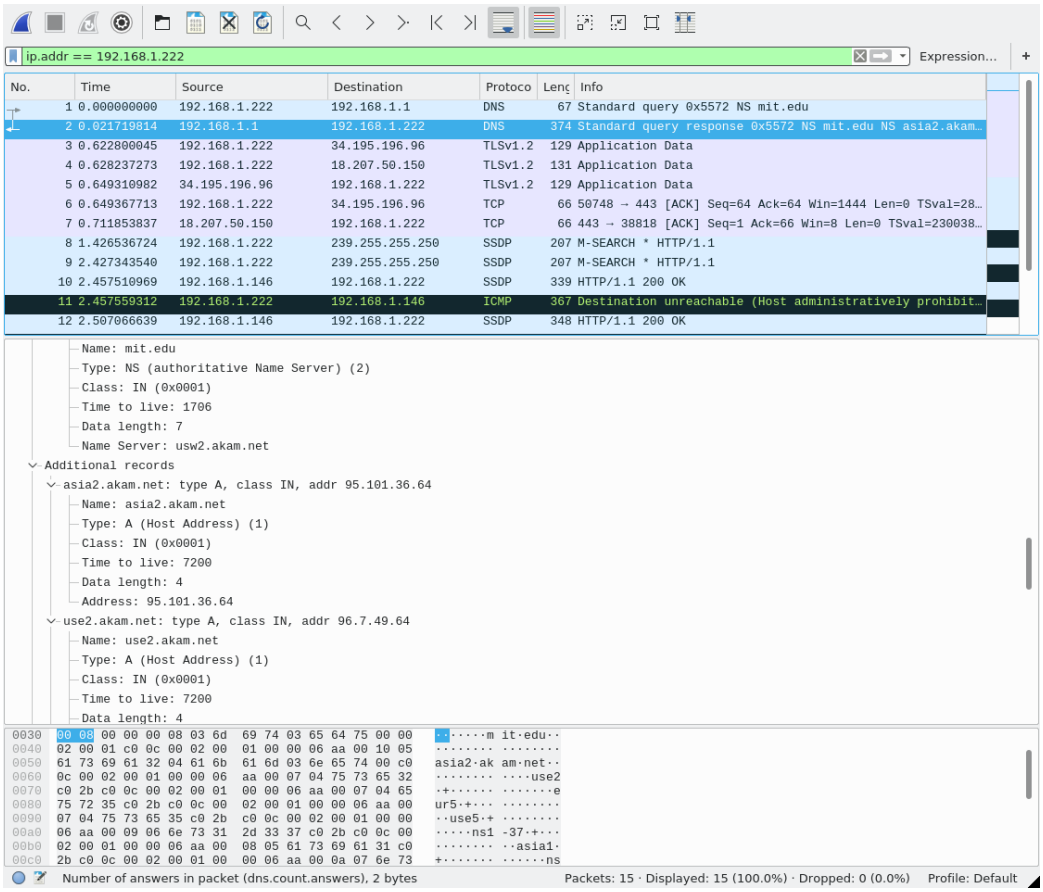
    (f) asia1.akam.net

    (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

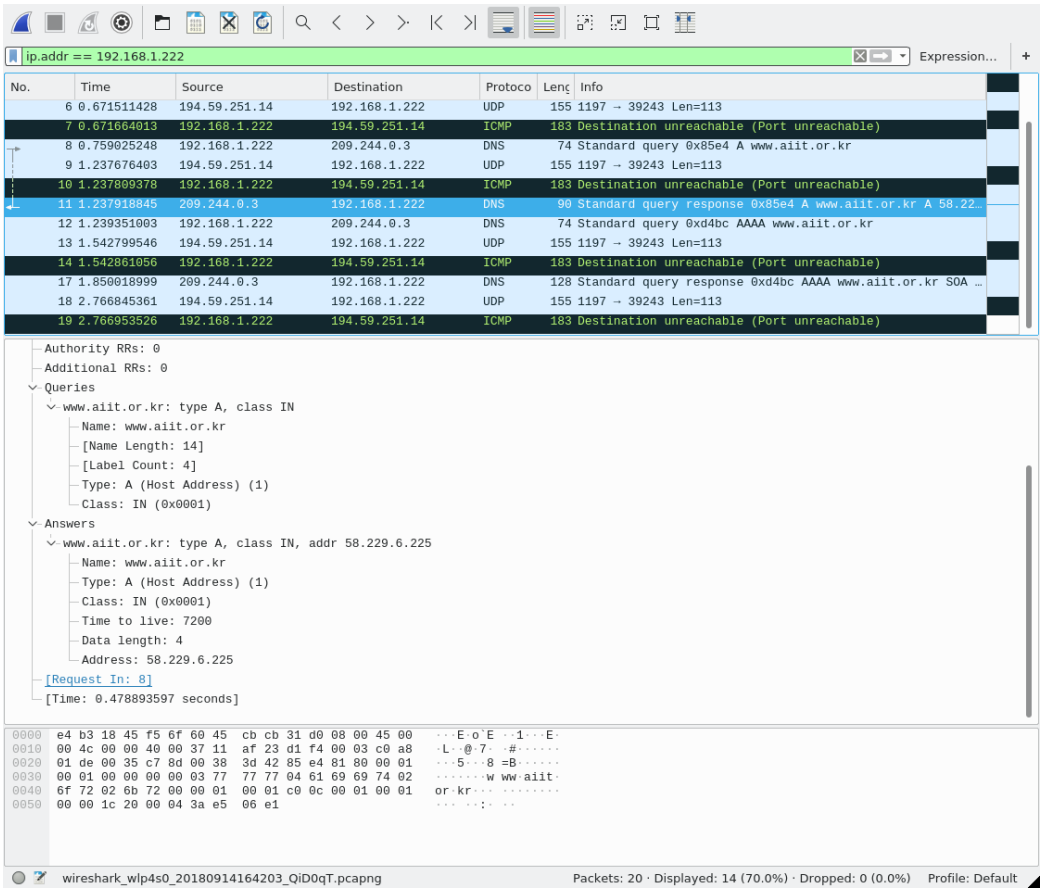


20. The query message is being sent to 209.244.0.3, the DNS server I specified in the command.

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


ip.addr == 192.168.1.222
Expression...
No. Time Source Destination Protoco Lenç 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 1.237809378 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)
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]
0000 e4 b3 18 45 f5 6f 60 45 cb cb 31 d0 08 00 45 00
0010 00 4c 00 00 40 00 37 11 af 23 d1 f4 00 03 c0 a8
0020 01 de 00 35 c7 8d 00 38 3d 42 85 e4 81 80 00 01
0030 00 01 00 00 00 00 03 77 77 77 04 61 69 69 74 02
0040 6f 72 02 6b 72 00 00 01 00 01 c0 0c 00 01 00 01
0050 00 00 1c 20 00 04 3a e5 06 e1
wireshark_wlp4s0_20180914164203_QiD0qT.pcapng
Packets: 20 · Displayed: 14 (70.0%) · Dropped: 0 (0.0%)
Profile: Default