ENGR 3321 - Lab 2: Wireshark HTTP

October 7th 2022

Nathan Cauwet

873271826

1. *Run nslookup to obtain the IP address of a Web server in Asia. What is the IP address of that server?*
   http://global.gmarket.co.kr/

```
C:\Users\ncauw>nslookup global.gmarket.co.kr
Server:  DC13DU.du.edu
Address:  130.253.3.39

Non-authoritative answer:
Name:    global.gmarket.co.kr.gccdn.net
Address:  157.185.145.100
Aliases:  global.gmarket.co.kr
```

The ip of the server is 157.185.145.100

2. *Run nslookup* to determine the authoritative DNS servers for a university in Europe.
   https://www.ucd.ie/

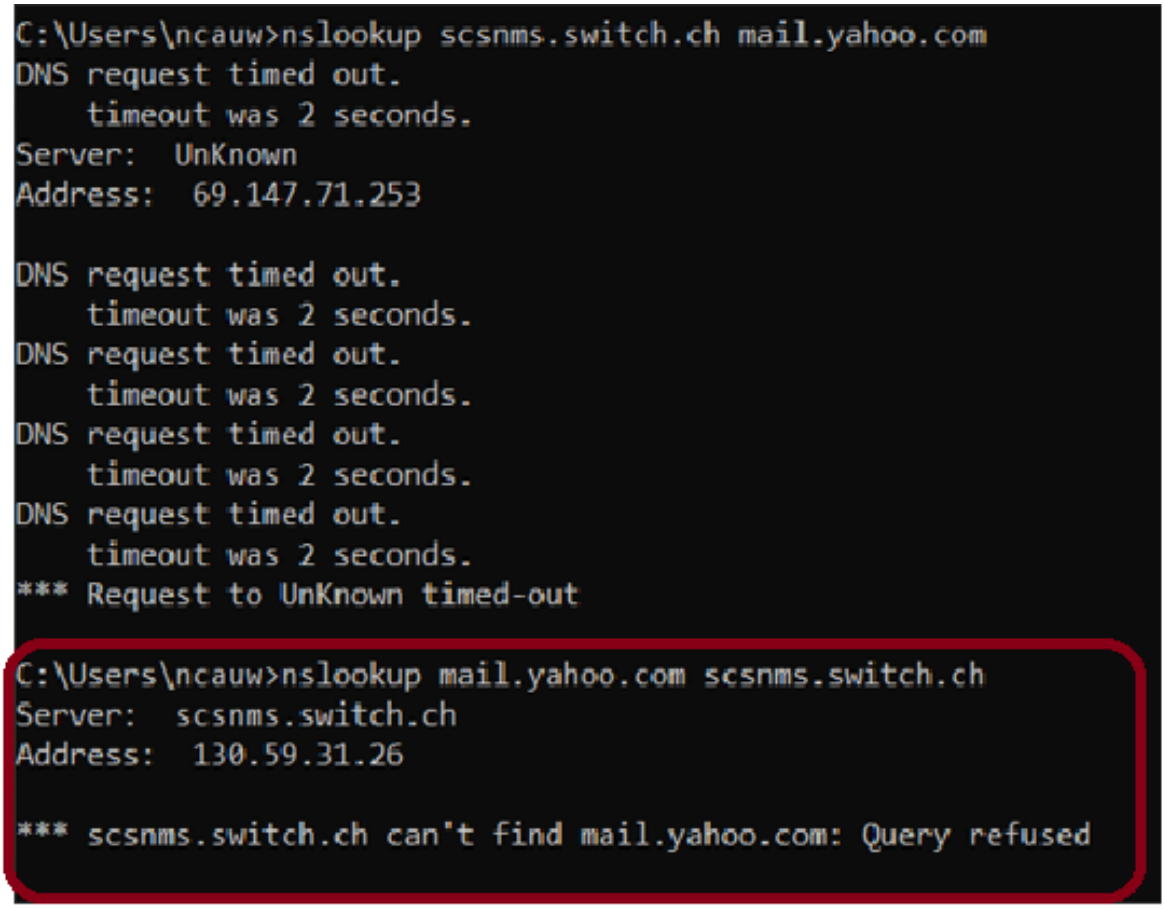
```
C:\Users\ncauw>nslookup -type=NS ucd.ie
Server:  DC13DU.du.edu
Address:  130.253.3.39

Non-authoritative answer:
ucd.ie  nameserver = scsnms.switch.ch
ucd.ie  nameserver = sec-ns.tcd.ie
ucd.ie  nameserver = auth-ns1.ucd.ie
ucd.ie  nameserver = auth-ns2.ucd.ie
ucd.ie  nameserver = uucp-gw-1.pa.dec.com
ucd.ie  nameserver = uucp-gw-2.pa.dec.com

scsnms.switch.ch        internet address = 130.59.31.26
scsnms.switch.ch        AAAA IPv6 address = 2001:620:0:ff::a7
auth-ns1.ucd.ie internet address = 137.43.132.53
auth-ns1.ucd.ie AAAA IPv6 address = 2001:770:98:200::35:1
auth-ns2.ucd.ie internet address = 137.43.132.54
auth-ns2.ucd.ie AAAA IPv6 address = 2001:770:98:200::35:2
```

The authoritative servers are the following: scsnms.switch.ch = 130.59.31.26, auth-ns1.ucd.ie = 137.43.132.53, and auth-ns2.ucd.ie = 137.43.132.54

3. *Run nslookup so that one of the DNS servers obtained in Question 2 is queried for the mail servers for Yahoo! mail. What is its IP address?*

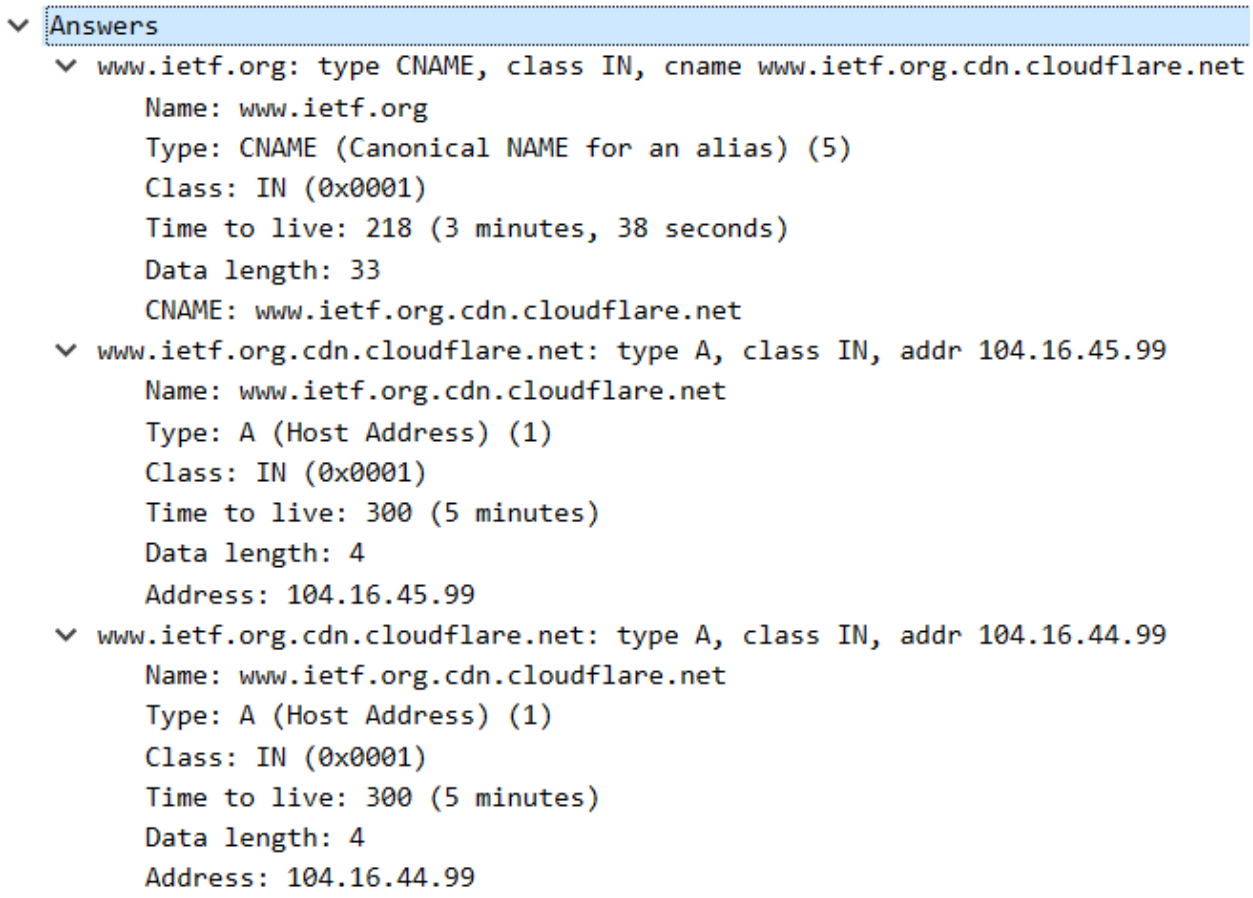


The address of the DNS server scsnms.switch.ch is 130.59.31.26. This is the same ip address that corresponded to that name server in question 2, therefore the lookup executed properly even though the query was refused.

Note: A different network was used for the rest of the tests (from question 4 to the end)

4. Both the DNS query and response are sent over UDP.
5. The destination port for the query is 53. The source port of the response message is also 53. (It is also notable that the query source port and the response destination port are the same as well)
6. The DNS query is sent to 192.168.0.1 which is the address of my router. In other words, the ip the query was sent to is the same as my local DNS server.

7. The query message is type A and class IN (additionally the flags are set to “standard query”). The query does not have any “answers”, this makes sense since the query is the request, the answers should be in the response.
8. The response message includes 3 answers containing the CNAME and Addresses (A) of the target server. The screencap below shows the full answers.



9. The destination IP of the SYN packet is 20.54.27.42. This IP does not correspond to any IP addresses in the DNS response.
10. The host does not issue new DNS queries before retrieving each image; however, an ACK must be sent to the host when each image is received.

nslookup (www.mit.edu):

11. The destination port for the query is 53. The source port of the response message is also 53.

12. The query message is sent to 192.168.0.1 which is my default DNS server (my home network's router).

13. In this capture there are 5 related query messages. The types of the queries (in order) are as follows: 1. PTR, 2. A, 3. AAAA, 4. A, 5. AAAA
(PTR = pointer, A = IPv4 address, AAAA = IPv6 address)
None of the 5 queries contain any answers.

14. There are 5 responses (one for each query). The first response contains the pointer for the domain name; the second and third do not contain answers; the fourth contains 3 answers, two CNAME values and then the ip address of the host; the fifth contains 4 answers two CNAME values and two identical IPv6 answers (which leads me to believe that due to the length of ipv6 addresses the answer had to be split into two).
15.

```
C:\Users\ncauw>nslookup www.mit.edu
Server:  modem.Home
Address:  192.168.0.1

Non-authoritative answer:
Name:    e9566.dscb.akamaiedge.net
Addresses:  2600:1405:5400:28a::255e
          2600:1405:5400:289::255e
          23.35.168.180
Aliases:  www.mit.edu
          www.mit.edu.edgekey.net
```

nslookup –type=NS mit.edu

16. The query message is sent to 192.168.0.1 which is my default DNS server (my home network's router).

17. There are 3 related query messages in this capture. The first is of type PTR, the other two are of type NS (nameserver). None of the queries contain answers.

18. The first response answers with the pointer to the domain, the second has no answers but contains the authoritative nameserver, the third response answers with 8 different nameservers. Each of the nameservers' IP addresses can be found under the "Additional records" section of the DNS response.

```
Additional records
    eur5.akam.net: type A, class IN, addr 23.74.25.64
        Name: eur5.akam.net
        Type: A (Host Address) (1)
        Class: IN (0x0001)
        Time to live: 89185 (1 day, 46 minutes, 25 seconds)
        Data length: 4
        Address: 23.74.25.64
    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: 171984 (1 day, 23 hours, 46 minutes, 2
        Data length: 4
        Address: 96.7.49.64
    use5.akam.net: type A, class IN, addr 2.16.40.64
        Name: use5.akam.net
        Type: A (Host Address) (1)
        Class: IN (0x0001)
        Time to live: 89187 (1 day, 46 minutes, 27 seconds)
        Data length: 4
        Address: 2.16.40.64
    usw2.akam.net: type A, class IN, addr 184.26.161.64
        Name: usw2.akam.net
        Type: A (Host Address) (1)
        Class: IN (0x0001)
        Time to live: 89184 (1 day, 46 minutes, 24 seconds)
        Data length: 4
        Address: 184.26.161.64
    asia1.akam.net: type A, class IN, addr 95.100.175.64
        Name: asia1.akam.net
        Type: A (Host Address) (1)
        Class: IN (0x0001)
        Time to live: 89184 (1 day, 46 minutes, 24 seconds)
        Data length: 4
        Address: 95.100.175.64
    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: 89184 (1 day, 46 minutes, 24 seconds)
        Data length: 4
        Address: 95.101.36.64
    ns1-37.akam.net: type A, class IN, addr 193.108.91.37
        Name: ns1-37.akam.net
        Type: A (Host Address) (1)
        Class: IN (0x0001)
        Time to live: 89204 (1 day, 46 minutes, 44 seconds)
        Data length: 4
        Address: 193.108.91.37
    ns1-173.akam.net: type A, class IN, addr 193.108.91.173
        Name: ns1-173.akam.net
        Type: A (Host Address) (1)
        Class: IN (0x0001)
        Time to live: 89204 (1 day, 46 minutes, 44 seconds)
        Data length: 4
        Address: 193.108.91.173
```

19.

```
C:\Users\ncauw>nslookup -type=NS mit.edu
Server:  modem.Home
Address:  192.168.0.1

Non-authoritative answer:
mit.edu nameserver = asia2.akam.net
mit.edu nameserver = usw2.akam.net
mit.edu nameserver = use2.akam.net
mit.edu nameserver = ns1-173.akam.net
mit.edu nameserver = eur5.akam.net
mit.edu nameserver = ns1-37.akam.net
mit.edu nameserver = use5.akam.net
mit.edu nameserver = asia1.akam.net

eur5.akam.net   internet address = 23.74.25.64
use2.akam.net   internet address = 96.7.49.64
use5.akam.net   internet address = 2.16.40.64
usw2.akam.net   internet address = 184.26.161.64
asia1.akam.net  internet address = 95.100.175.64
asia2.akam.net  internet address = 95.101.36.64
ns1-37.akam.net internet address = 193.108.91.37
ns1-173.akam.net        internet address = 193.108.91.173
```

nslookup www.aiit.or.kr bitsy.mit.edu

20. *To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server? If not, what does the IP address correspond to?*

    The query is sent separately to three different ip addresses. First my local DNS (192.168.0.1), then to 205.171.3.65, then to 18.0.72.3 after the first response. 205.171.3.65 corresponds to resolver.qwest.net which is used to identify the path to the target server (www.aiit.or.kr). It appears to be the top-level server for the request. I also ran the capture 2 additional times from a different computer and this address did not show up again, presumably because the cache on the resolver had not been cleared yet. 18.0.72.3 is the address of **bitsy.mit.edu** because it is being used as our DNS server.

21. *Examine the DNS query message. What "Type" of DNS query is it? Does the query message contain any "answers"?*

    The query is "type A" which corresponds to IPv4 addr. (also uses AAAA which is IPv6). None of the query messages contain any answers.

22. *Examine the DNS response message. How many "answers" are provided? What does each of these answers contain?*
    The response message provides one answer containing the IPv4 address for the server (18.0.72.3).

23.

```
C:\Users\ncauw>nslookup www.aiit.or.kr bitsy.mit.edu
DNS request timed out.
    timeout was 2 seconds.
Server:  UnKnown
Address:  18.0.72.3

DNS request timed out.
    timeout was 2 seconds.
DNS request timed out.
    timeout was 2 seconds.
DNS request timed out.
    timeout was 2 seconds.
DNS request timed out.
    timeout was 2 seconds.
*** Request to UnKnown timed-out
```

Appendices are included in the attached PDF Portfolio (named Lab3Appendix.pdf)