Rob Johansen
u0531837
CS 4480 - Homework Assignment 2

---

nslookup

1. I did "nslookup www.peopledaily.com.cn" and got this IP address:

   209.177.88.10

2. I did "nslookup -type=NS ox.ac.uk" (the domain used by Oxford University) and got the following list of authoritative DNS servers:

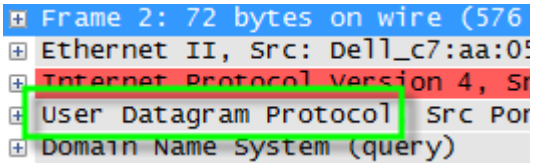
   ```
   dns2.ox.ac.uk   internet address = 163.1.2.190
   dns0.ox.ac.uk   internet address = 129.67.1.190
   ns2.ja.net      internet address = 193.63.105.17
   ns2.ja.net      AAAA IPv6 address = 2001:630:0:45::11
   ```

3. Unfortunately the Oxford DNS servers all refused my query, so I used ns.utah.edu instead. I did "nslookup mail.yahoo.com ns.utah.edu" and got this IP address for a Yahoo! mail server:

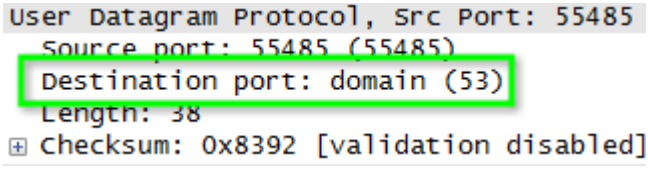
   98.138.253.138

Tracing DNS with Wireshark

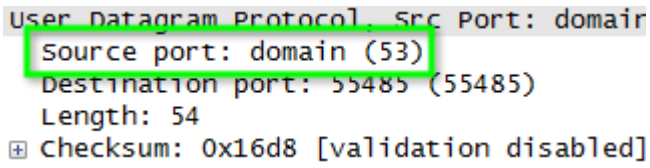
4. The DNS query and response message are sent over UDP:



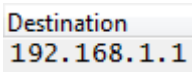
5. The destination port of the DNS query message is 53:



The source port of the DNS response message is also 53:



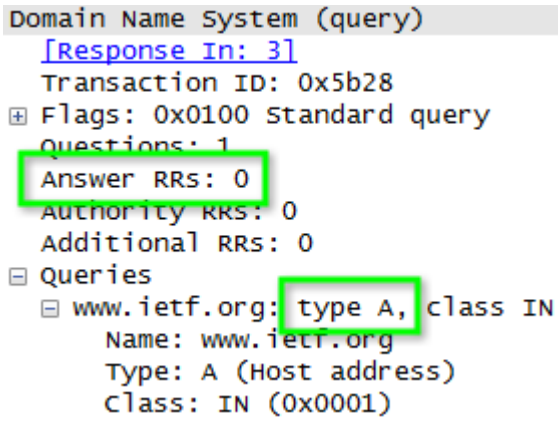
6. The DNS query message is sent to IP address 192.168.1.1, which is indeed the IP address of my local DNS server:



(Wireshark screenshot)

(ipconfig /all screenshot)

7. The type of DNS query is A, and it does not contain any answers:



8. One answer is provided. It contains the IP address of the requested host, the TTL, and other information:

```
Domain Name System (response)
  [Request In: 2]
  [Time: 0.021118000 seconds]
  Transaction ID: 0x5b28
⊞ Flags: 0x8180 Standard query response, No error
  Questions: 1
  Answer RRs: 1
  Authority RRs: 0
  Additional RRs: 0
⊞ Queries
⊟ Answers
  ⊟ www.ietf.org: type A, class IN, addr 4.31.198.44
      Name: www.ietf.org
      Type: A (Host address)
      Class: IN (0x0001)
      Time to live: 17 minutes, 19 seconds
      Data length: 4
      Addr: 4.31.198.44 (4.31.198.44)
```

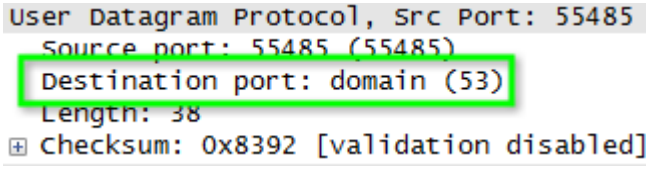
9. Yes, the IP address of the subsequent TCP SYN packet is the IP address that was provided in the DNS response message:

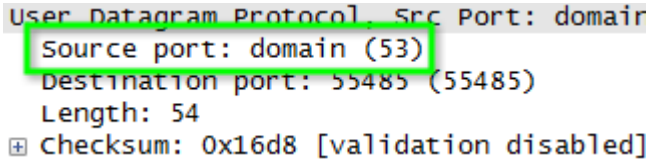
```
Source: 192.168.1.9 (192.168.1.9)
Destination: 4.31.198.44 (4.31.198.44)
[Source GeoIP: Unknown]
[Destination GeoIP: Unknown]
```

10. My host does not issue new DNS queries before requesting the images. In this screenshot, the request for an image is highlighted but as you can see there are no DNS requests before it:

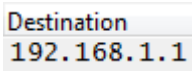
Source	Destination	Protocol	Length	Info
4.31.198.44	192.168.1.9	TCP	1514	[TCP segment of a reassembled PDU]
4.31.198.44	192.168.1.9	HTTP	342	HTTP/1.1 200 OK (text/html)
192.168.1.9	4.31.198.44	TCP	54	58015 > http [ACK] Seq=347 Ack=4669 Win=65
192.168.1.9	4.31.198.44	HTTP	371	GET /css/ietf.js HTTP/1.1
192.168.1.9	4.31.198.44	HTTP	387	GET /css/ietf.css HTTP/1.1
192.168.1.9	4.31.198.44	TCP	66	58017 > http [SYN] Seq=0 Win=8192 Len=0 MS
4.31.198.44	192.168.1.9	HTTP	1009	HTTP/1.1 200 OK (text/x-js)
192.168.1.9	4.31.198.44	HTTP	401	GET /images/ietflogotrans.gif HTTP/1.1
4.31.198.44	192.168.1.9	TCP	60	http > 58016 [ACK] Seq=1 Ack=334 Win=15744
4.31.198.44	192.168.1.9	HTTP	968	HTTP/1.1 200 OK (text/css)
192.168.1.9	4.31.198.44	HTTP	388	GET /css/ietf4.css HTTP/1.1
192.168.1.9	192.168.1.1	DNS	80	Standard query 0x943a A datatracker.ietf.
192.168.1.9	192.168.1.1	DNS	73	Standard query 0xffbc A iaoc.ietf.org
192.168.1.9	192.168.1.1	DNS	74	Standard query 0x9a4a A open-stand.org
4.31.198.44	192.168.1.9	TCP	66	http > 58017 [SYN, ACK] Seq=0 Ack=1 Win=14
192.168.1.9	4.31.198.44	TCP	54	58017 > http [ACK] Seq=1 Ack=1 Win=65700 L
192.168.1.9	4.31.198.44	HTTP	388	GET /css/ietf3.css HTTP/1.1

11. The destination port for the DNS query message is 53, as is the source port of the DNS response message:





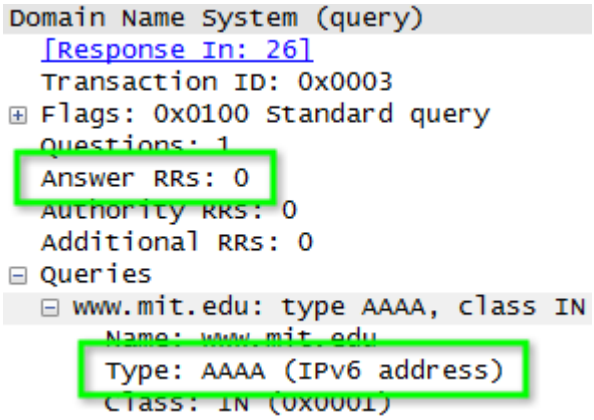
12. The DNS query message is sent to IP address 192.168.1.1, which is indeed the IP address of my local DNS server:



(Wireshark screenshot)

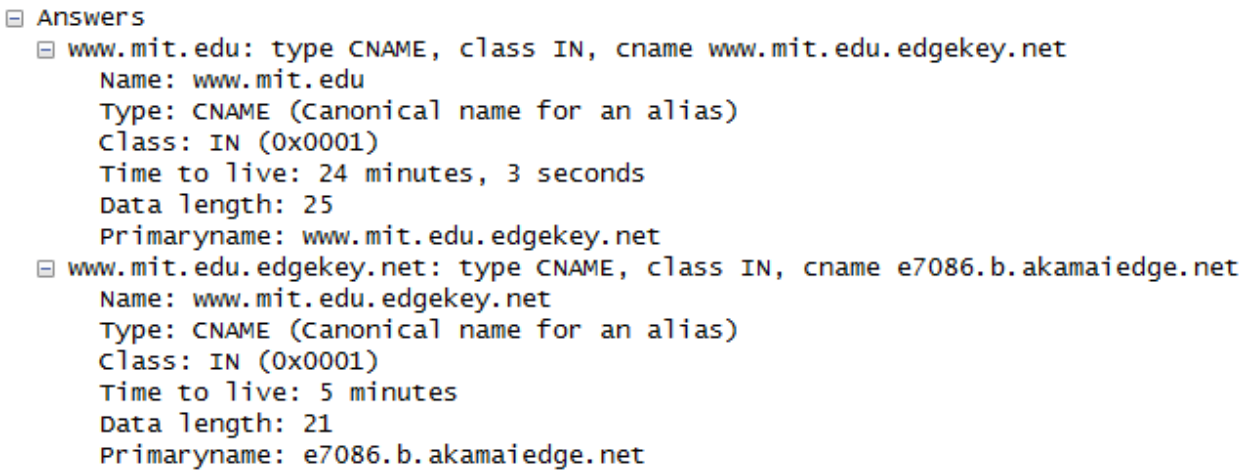
(ipconfig /all screenshot)

13. The type of the DNS query messages is AAAA (IPv6 address), and it does not contain any answers:



14. The DNS response message provides two answers, both of which contain CNAME resource records.

15. Here is a screenshot of the answers:



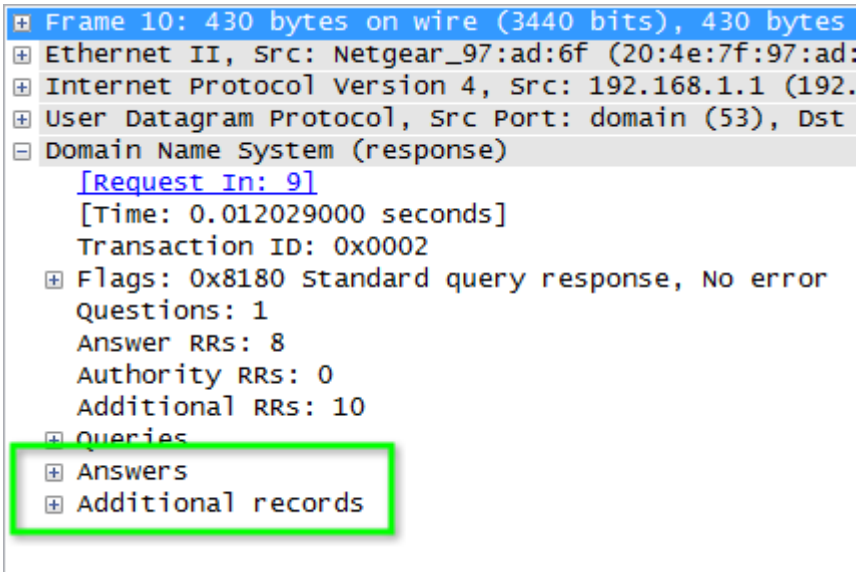
16. The DNS query message is sent to IP address 192.168.1.1, which is my default local DNS server.

17. The type of the DNS query message is NS.

18. The DNS response message provides a number of MIT nameservers as answers, and all of their IP addresses as additional records (see the screenshot for #19):

    asia2.akam.net
    ns1-173.akam.net
    use5.akam.net
    asia1.akam.net
    ns1-37.akam.net
    use2.akam.net
    usw2.akam.net
    eur5.akam.net

19. Here is a screenshot illustrating that both answers and additional records were provided in the DNS response:



20. The DNS request message is sent to IP address 89.233.43.71, which is the IP address of the ns1.censurfridns.dk nameserver.

21. The query is for an A record, and it does not contain any answers.

22. The DNS response message provides 2 answers, containing a CNAME record for www.aiit.or.kr and an A record for aiit.or.kr.

23. Here is a screenshot of the response: