**Rob Johansen**

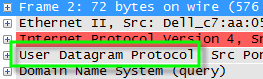
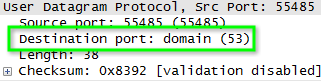
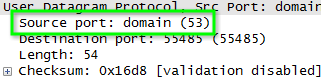
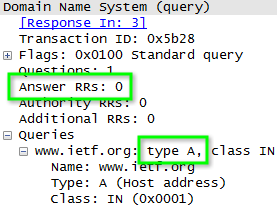
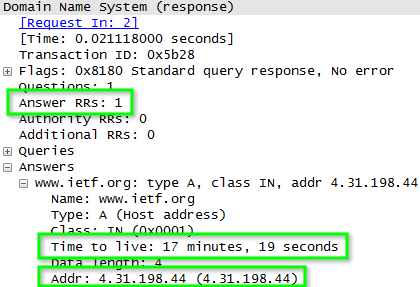
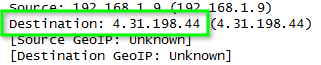
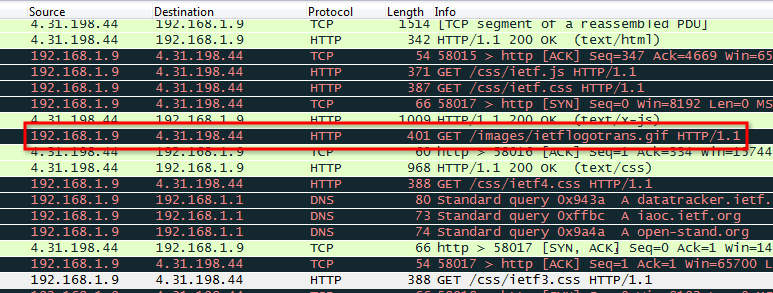
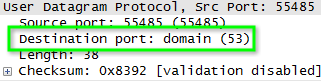
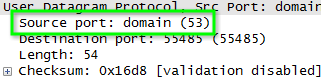
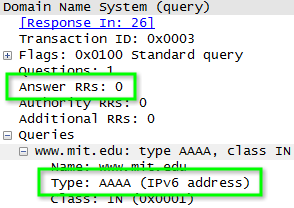
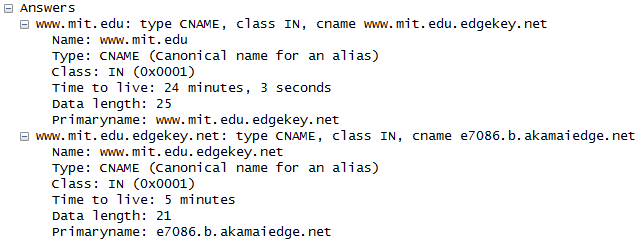
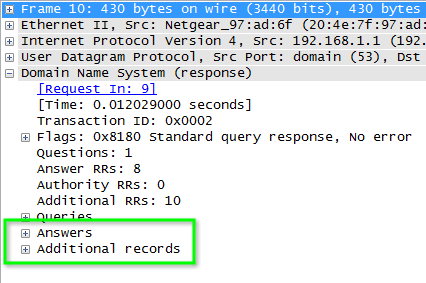
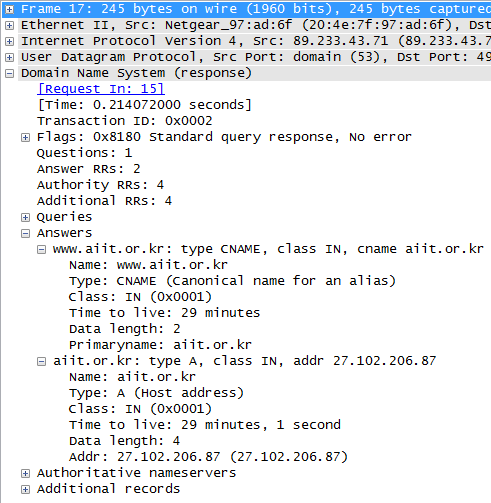
**u0531837**

**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**

1. The DNS query and response message are sent over UDP:  
     
    
2. The destination port of the DNS query message is 53:  
     
      
     
     
   The source port of the DNS response message is also 53:  
     
    
3. The DNS query message is sent to IP address 192.168.1.1, which is indeed the IP address of my local DNS server:  
     
    C:\Rob\UofU\Classes\CS 4480\HA 2\4.png  
    (Wireshark screenshot)  
     
    C:\Rob\UofU\Classes\CS 4480\HA 2\5.png  
    (ipconfig /all screenshot)
4. The type of DNS query is A, and it does not contain any answers:  
     
    
5. One answer is provided. It contains the IP address of the requested host, the TTL, and other information:  
     
    
6. Yes, the IP address of the subsequent TCP SYN packet is the IP address that was provided in the DNS response message:  
     
    
7. 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:  
     
   
8. The destination port for the DNS query message is 53, as is the source port of the DNS response message:  
     
      
     
     
    
9. The DNS query message is sent to IP address 192.168.1.1, which is indeed the IP address of my local DNS server:  
     
    C:\Rob\UofU\Classes\CS 4480\HA 2\4.png  
    (Wireshark screenshot)  
     
    C:\Rob\UofU\Classes\CS 4480\HA 2\5.png  
    (ipconfig /all screenshot)
10. The type of the DNS query messages is AAAA (IPv6 address), and it does not contain any answers:  
      
     
11. The DNS response message provides two answers, both of which contain CNAME resource records.
12. Here is a screenshot of the answers:  
      
    
13. The DNS query message is sent to IP address 192.168.1.1, which is my default local DNS server.
14. The type of the DNS query message is NS.
15. 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
16. Here is a screenshot illustrating that both answers and additional records were provided in the DNS response:  
      
     
17. The DNS request message is sent to IP address 89.233.43.71, which is the IP address of the ns1.censurfridns.dk nameserver.
18. The query is for an A record, and it does not contain any answers.
19. The DNS response message provides 2 answers, containing a CNAME record for www.aiit.or.kr and an A record for aiit.or.kr.
20. Here is a screenshot of the response: