Vanessa Ulloa

Daniel Kushner

CST 311

19 May 2015

Lab 3

Part I – *nslookup*

1. Run *nslookup* to obtain the IP address of a Web server in Asia. What is the IP address of that server?

```
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Windows\system32>nslookup www.asdu.ait.ac.th
Server:  dns-cac-lb-01.rr.com
Address:  209.18.47.61

Non-authoritative answer:
Name:    www.asdu.ait.ac.th.socal.rr.com
Addresses:  198.105.254.228
          198.105.244.228


C:\Windows\system32>_
```

2. Run *nslookup* to determine the authoritative DNS servers for a university in Europe.

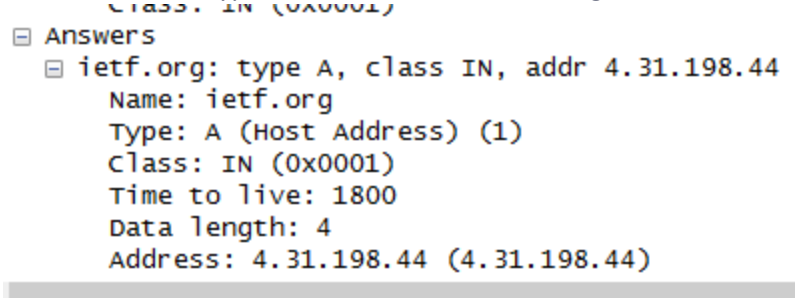
```
C:\Windows\system32>nslookup -type=NS www.cam.ac.uk
Server:  dns-cac-lb-01.rr.com
Address:  209.18.47.61

cam.ac.uk
        primary name server = ipreg.csi.cam.ac.uk
        responsible mail addr = hostmaster.cam.ac.uk
        serial  = 1432076018
        refresh = 1800 (30 mins)
        retry   = 900 (15 mins)
        expire  = 604800 (7 days)
        default TTL = 3600 (1 hour)
```

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

Part III - *Tracing DNS with Wireshark*

4. Locate the DNS query and response messages. Are then sent over UDP or TCP?
    a. UDP
5. What is the destination port for the DNS query message? What is the source port of DNS response message?
    a. Destination port: 53
    b. Source Port: 53
6. To what IP address is the DNS query message sent? Use ipconfig to determine the IP address of your local DNS server. Are these two IP addresses the same?
    a. 209.18.47.61

7. Examine the DNS query message. What "Type" of DNS query is it? Does the query message contain any "answers"?
    a. Type A Standard Query, no answers
8. Examine the DNS response message. How many "answers" are provided? What do each of these answers contain?
    a. 1 answer: name, type, class, time to live, data length, address



9. Consider the subsequent TCP SYN packet sent by your host. Does the destination IP address of the SYN packet correspond to any of the IP addresses provided in the DNS response message?
    a. 192.168.5.20
10. This web page contains images. Before retrieving each image, does your host issue new DNS queries?
    a. No
11. What is the destination port for the DNS query message? What is the source port of DNS response message?
    a. Destination port: 53
    b. Source Port: 53
12. To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server?
    a. 209.18.47.61, Yes
13. Examine the DNS query message. What "Type" of DNS query is it? Does the query message contain any "answers"?
    a. Type AAAA
    b. No answers
14. Examine the DNS response message. How many "answers" are provided? What do each of these answers
    a. 2 answers
    b. Name, Type, Class, Time to live, Data Length, AAAA address
15. Provide a screenshot.

```
Class: IN (0x0001)
Answers
  mit.edu: type AAAA, class IN, addr 2600:1406:3:286::255e
    Name: mit.edu
    Type: AAAA (IPv6 Address) (28)
    Class: IN (0x0001)
    Time to live: 20
    Data length: 16
    AAAA Address: 2600:1406:3:286::255e (2600:1406:3:286::255e)
  mit.edu: type AAAA, class IN, addr 2600:1406:3:283::255e
    Name: mit.edu
    Type: AAAA (IPv6 Address) (28)
    Class: IN (0x0001)
    Time to live: 20
    Data length: 16
    AAAA Address: 2600:1406:3:283::255e (2600:1406:3:283::255e)
```

16. To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server?
    a. 209.18.47.61, Yes
17. Examine the DNS query message. What "Type" of DNS query is it? Does the query message contain any "answers"?
    a. Type NS, yes
18. Examine the DNS response message. What MIT nameservers does the response message provide? Does this response message also provide the IP addresses of the MIT namesers?
    a. usw2.akam.net, use2.akam.net, as1a1.akam.net, ns1-173.akam.net, use5.akam.net, eur5.akam.net, ns1-37.akam.net, asia2.akam.net
19. Provide a screenshot.

```
Additional RRs: 0
Queries
  mit.edu: type NS, class IN
    Name: mit.edu
    [Name Length: 7]
    [Label Count: 2]
    Type: NS (authoritative Name Server) (2)
    Class: IN (0x0001)
Answers
  mit.edu: type NS, class IN, ns usw2.akam.net
  mit.edu: type NS, class IN, ns use2.akam.net
  mit.edu: type NS, class IN, ns asia1.akam.net
  mit.edu: type NS, class IN, ns ns1-173.akam.net
  mit.edu: type NS, class IN, ns use5.akam.net
  mit.edu: type NS, class IN, ns eur5.akam.net
  mit.edu: type NS, class IN, ns ns1-37.akam.net
  mit.edu: type NS, class IN, ns asia2.akam.net
```

Using dns-ethereal-trace-4 file for 20-23

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?
    a. 18.72.0.3
21. Examine the DNS query message. What "Type" of DNS query is it? Does the query message contain any "answers"?
    a. Type PTR

b. Yes, 1 answer

22. Examine the DNS response message. How many "answers" are provided? What does each of these answers contain?
    a. 1 answer, Name, Type, Class, Time to live, Data length, Domain Name
23. Provide a screenshot.