Vanessa Ulloa

Daniel Kushner

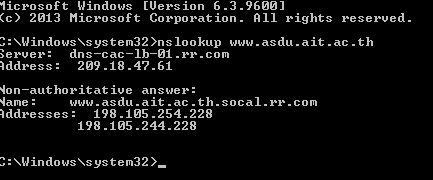
CST 311

19 May 2015

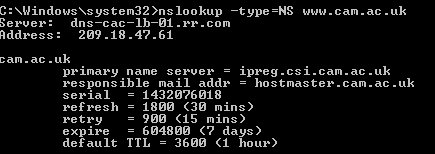
Lab 3

## 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?



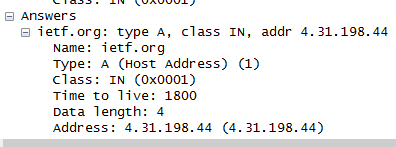
1. Run *nslookup* to determine the authoritative DNS servers for a university in Europe.



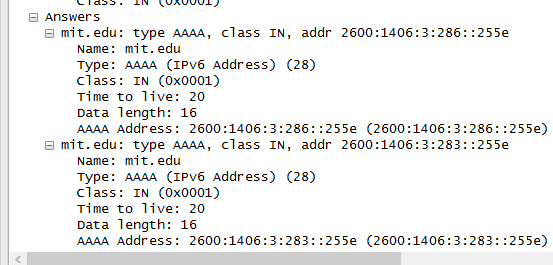
1. Run *nslookup* so that one of the DNS severs obtained in Question 2 is queried for the mail servers for Yahoo! Mail. What is its IP address?

## Part III - *Tracing DNS with Wireshark*

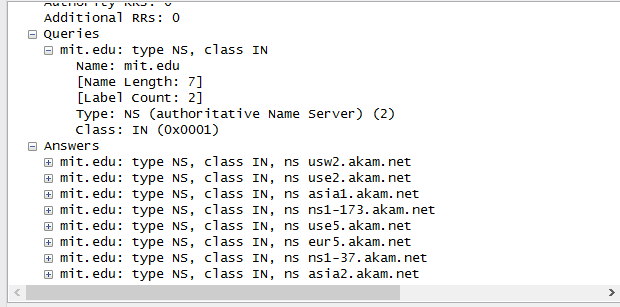
1. Locate the DNS query and response messages. Are then sent over UDP or TCP?
   1. UDP
2. What is the destination port for the DNS query message? What is the source port of DNS response message?
   1. Destination port: 53
   2. Source Port: 53
3. To what IP address is the DNS query message sent? Use ipconfig to determine the IP address of your local DNS server. Are these two IP addresses the same?
   1. 209.18.47.61
4. Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”?
   1. Type A Standard Query, no answers
5. Examine the DNS response message. How many “answers” are provided? What do each of these answers contain?
   1. 1 answer: name, type, class, time to live, data length, address



1. 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?
   1. 192.168.5.20
2. This web page contains images. Before retrieving each image, does your host issue new DNS queries?
   1. No
3. What is the destination port for the DNS query message? What is the source port of DNS response message?
   1. Destination port: 53
   2. Source Port: 53
4. To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server?
   1. 209.18.47.61, Yes
5. Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”?
   1. Type AAAA
   2. No answers
6. Examine the DNS response message. How many “answers” are provided? What do each of these answers
   1. 2 answers
   2. Name, Type, Class, Time to live, Data Length, AAAA address
7. Provide a screenshot.



1. To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server?
   1. 209.18.47.61, Yes
2. Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”?
   1. Type NS, yes
3. 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?
   1. 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
4. Provide a screenshot.



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

1. 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?
   1. 18.72.0.3
2. Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”?
   1. Type PTR
   2. Yes, 1 answer
3. Examine the DNS response message. How many “answers” are provided? What does each of these answers contain?
   1. 1 answer, Name, Type, Class, Time to live, Data length, Domain Name
4. Provide a screenshot.

