

Week 5 Lab Report

CPS 706 Computer Networks

Mitchell Mohorovich

500563037

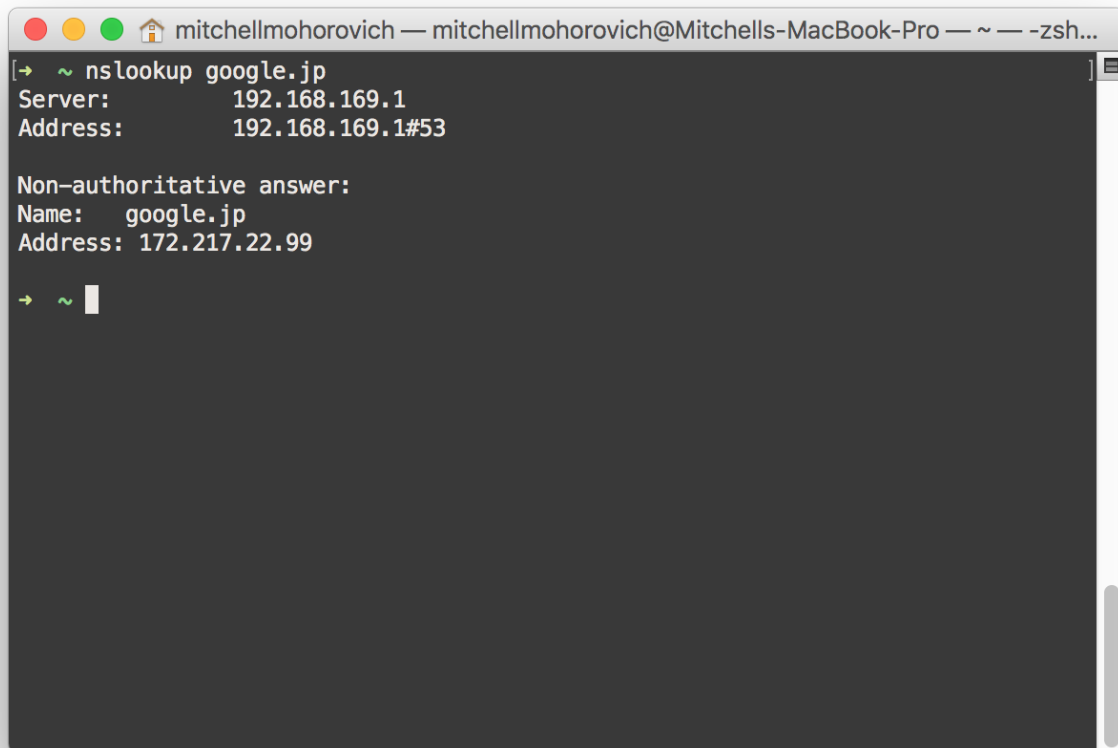
Section 5, Fridays 2-3PM

Computer Science
Ryerson University

1 nslookup

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

I used nslookup to find the IP address of `google.jp`, it returned `172.217.22.99`.

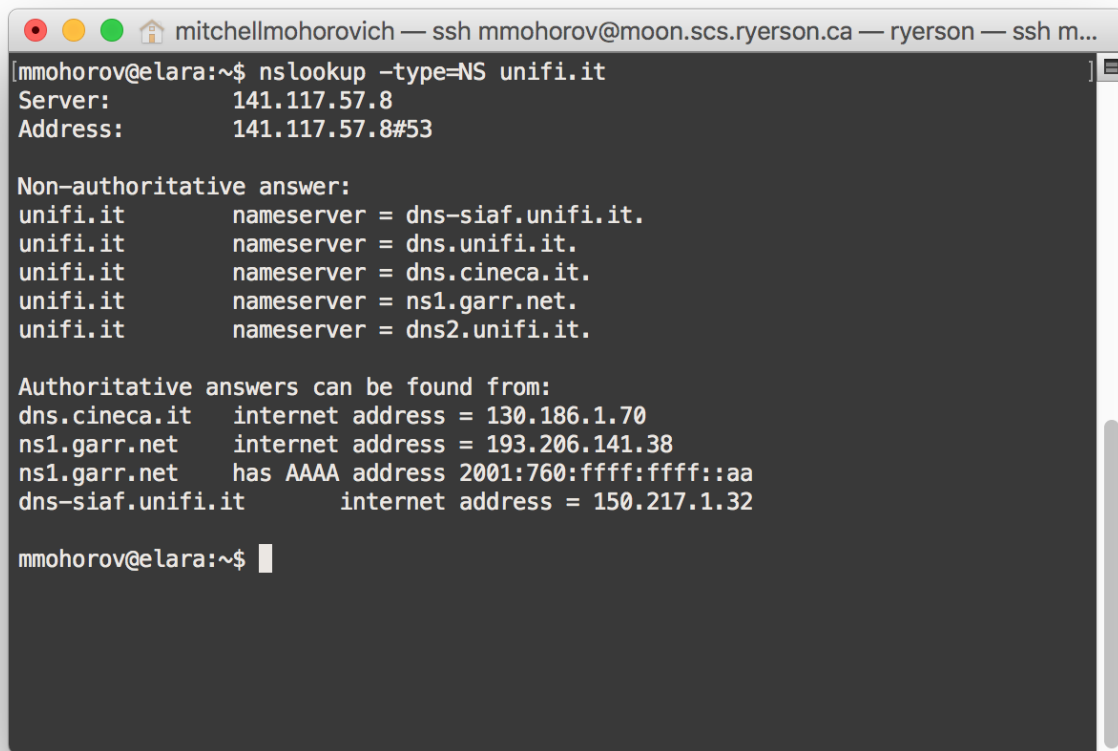
A screenshot of a macOS terminal window. The title bar shows the user 'mitchellmohorovich' on a 'Mitchells-MacBook-Pro' machine. The terminal displays the command 'nslookup google.jp' and its output. The output shows the server used (192.168.169.1) and the IP address for google.jp (172.217.22.99).

```
mitchellmohorovich — mitchellmohorovich@Mitchells-MacBook-Pro — ~ — -zsh...  
[→ ~ nslookup google.jp ]  
Server:      192.168.169.1  
Address:     192.168.169.1#53  
  
Non-authoritative answer:  
Name:   google.jp  
Address: 172.217.22.99  
  
→ ~ █
```

Figure 1: Using nslookup to find the IP of Google Japan

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

I used nslookup to find the name servers for the University of Florence. The results are shown in Figure 2 below.

A terminal window titled "mitchellmohorovich — ssh mmohorov@moon.scs.ryerson.ca — ryerson — ssh m...". The prompt is "mmohorov@elara:~\$". The command "nslookup -type=NS unifi.it" has been executed. The output shows the server and address of the DNS server, followed by a list of non-authoritative answers for the nameservers of unifi.it. The list includes dns-siaf.unifi.it, dns.unifi.it, dns.cineca.it, ns1.garr.net, and dns2.unifi.it. Below this, authoritative answers are listed for dns.cineca.it, ns1.garr.net, and dns-siaf.unifi.it, including their internet and AAAA addresses. The prompt "mmohorov@elara:~\$" is shown at the bottom.

```
mmohorov@elara:~$ nslookup -type=NS unifi.it
Server:          141.117.57.8
Address:         141.117.57.8#53

Non-authoritative answer:
unifi.it        nameserver = dns-siaf.unifi.it.
unifi.it        nameserver = dns.unifi.it.
unifi.it        nameserver = dns.cineca.it.
unifi.it        nameserver = ns1.garr.net.
unifi.it        nameserver = dns2.unifi.it.

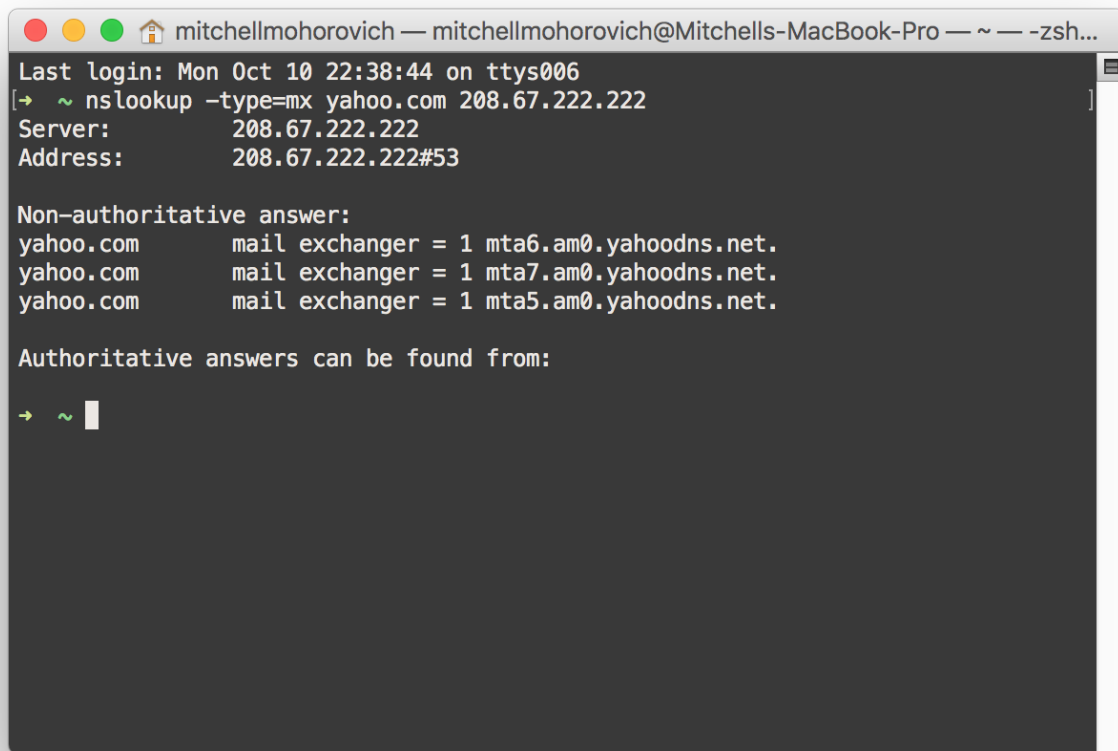
Authoritative answers can be found from:
dns.cineca.it   internet address = 130.186.1.70
ns1.garr.net    internet address = 193.206.141.38
ns1.garr.net    has AAAA address 2001:760:ffff:ffff::aa
dns-siaf.unifi.it internet address = 150.217.1.32

mmohorov@elara:~$
```

Figure 2: Using nslookup to find the name servers of the University of Florence

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

I was unable to find a DNS server run by a European university that would allow for external queries, so I used the OpenDNS public DNS server to complete this part of the lab. The screenshot of the command is shown in the screenshot below.

A terminal window titled "mitchellmohorovich — mitchellmohorovich@Mitchells-MacBook-Pro — ~ — -zsh...". The window shows the output of the command "nslookup -type=mx yahoo.com 208.67.222.222". The output includes the server address "208.67.222.222" and three non-authoritative mail exchanger records for yahoo.com: "mta6.am0.yahoodns.net.", "mta7.am0.yahoodns.net.", and "mta5.am0.yahoodns.net.". The prompt "→ ~" is visible at the bottom.

```
mitchellmohorovich — mitchellmohorovich@Mitchells-MacBook-Pro — ~ — -zsh...
Last login: Mon Oct 10 22:38:44 on ttys006
[→ ~ nslookup -type=mx yahoo.com 208.67.222.222 ]
Server:      208.67.222.222
Address:     208.67.222.222#53

Non-authoritative answer:
yahoo.com    mail exchanger = 1 mta6.am0.yahoodns.net.
yahoo.com    mail exchanger = 1 mta7.am0.yahoodns.net.
yahoo.com    mail exchanger = 1 mta5.am0.yahoodns.net.

Authoritative answers can be found from:

→ ~
```

Figure 3: Using nslookup to use OpenDNS Public DNS to return a query to find the mail servers of Yahoo!

2 Tracing DNS with Wireshark

4. *Locate the DNS query and response messages. Are they sent over UDP or TCP?*

The DNS query and response messages are sent over UDP. This is shown by the protocol flag in the packet.

5. *What is the destination port for the DNS query message? What is the source port of DNS response message?*

The destination port for the DNS query message is 53. The source port of the response message is 53 as well.

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?*

The query message is sent to 8.8.8.8. This IP is the same as my local DNS server, which is 8.8.8.8. This is because I have my DNS server manually set to Google's DNS server at 8.8.8.8.

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

Based on the DNS flags provided in the query packet, a standard DNS query was sent. The query contains three "answers".

8. *Examine the DNS response message. How many answers are provided? What do each of these answers contain?*

There are three "answers" provided, one is a CNAME DNS record, and the other two are A records. The first CNAME record says that the domain `www.ietf.orgmaps` maps to `www.ietf.org.cdn.cloudflare-dnssec.net`. The other two A records return two separate IP addresses for the URL in the CNAME record, one IP used as a primary IP address, the other as a backup (presumably) for the CDN.

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?*

The IP address subsequent TCP SYN packet sent by my host corresponds to the IP address of the first A record received.

10. *This web page contains images. Before retrieving each image, does your host issue new DNS queries?*

No, my host did not issue new DNS queries. Since the images were hosted on the same domain and the DNS records retrieved had a TTL of 244, my host used the cached records stored locally.

11. *What is the destination port for the DNS query message? What is the source port of DNS response message?*

The destination port for the DNS query message is 53, the source port is 53 as well.

12. *To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server?*

The DNS query message was sent to 8.8.8.8, this is the IP address of my default set local DNS server.

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

The DNS query sent was a “standard” DNS query.

14. *Examine the DNS response message. How many answers are provided? What do each of these answers contain?*

The DNS query provides one answer. This answer is an A record that provides the IP address of the queried URL.

15. *Provide a screenshot.*

2554	16.598446	192.168.1.70	8.8.8.8	DNS	67
2559	16.742667	8.8.8.8	192.168.1.70	DNS	87

▼ Queries

▼ mit.edu: type A, class IN

Name: mit.edu
[Name Length: 7]
[Label Count: 2]
Type: A (Host Address) (1)
Class: IN (0x0001)

▼ Answers

▼ mit.edu: type A, class IN, addr 23.40.64.128

Name: mit.edu
Type: A (Host Address) (1)
Class: IN (0x0001)
Time to live: 19
Data length: 4

Address: 23.40.64.128

0000	3c 15 c2 d9 7a de 58 98 35 ad 0e de 08 00 45 00	<...z.X. 5.....E.
0010	00 45 3d eb 00 00 2d 11 7d bf 08 08 08 08 c0 a8	.E=...-. }......
0020	01 46 00 35 e9 9e 00 31 16 7d 06 e7 81 80 00 01	.F.5...1 .}......
0030	00 01 00 00 00 00 03 6d 69 74 03 65 64 75 00 00m it.edu..
0040	01 00 01 c0 0c 00 01 00 01 00 00 00 13 00 04 17
0050	28 40 80	(@.

Figure 4: Screenshot of the answers returned from the nslookup command issued on `mit.edu`

16. *To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server?*

To DNS query message was sent to 8.8.8.8, this is the IP address of my default local DNS server.

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

The “type” of the DNS query is a standard query specified by the Flags of the DNS portion of the packet.

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 nameservers?*

The DNS response message provides the answers to the query request, which were the name-servers for the `mit.edu` domain. The response message did not provide the IP addresses, but the domains of them.

19. *Provide a screenshot.*

Net	Time	Source	Destination	Protocol	Length	Info
→ 1031	3.624286	192.168.1.70	8.8.8.8	DNS	67	Standard query 0xfb56 NS mit.edu
← 1035	3.673855	8.8.8.8	192.168.1.70	DNS	234	Standard query response 0xfb56 NS

Additional RRs: 0	
▼ Queries	
▶ mit.edu: type NS, class IN	
▼ Answers	
▶ mit.edu: type NS, class IN, ns eur5.akam.net	
▶ mit.edu: type NS, class IN, ns usw2.akam.net	
▶ mit.edu: type NS, class IN, ns ns1-37.akam.net	
▶ mit.edu: type NS, class IN, ns asia2.akam.net	
▶ mit.edu: type NS, class IN, ns asia1.akam.net	
▶ mit.edu: type NS, class IN, ns use5.akam.net	
▶ mit.edu: type NS, class IN, ns use2.akam.net	
▶ mit.edu: type NS, class IN, ns ns1-173.akam.net	

0000	3c 15 c2 d9 7a de 58 98	35 ad 0e de 08 00 45 00	<...z.X. 5.....E.
0010	00 dc 3d ce 00 00 2c 11	7e 45 08 08 08 08 c0 a8	..=...., ~E.....
0020	01 46 00 35 d3 80 00 c8	28 12 fb 56 81 80 00 01	.F.5....(..V....
0030	00 08 00 00 00 00 03 6d	69 74 03 65 64 75 00 00m it.edu..
0040	02 00 01 c0 0c 00 02 00	01 00 00 05 25 00 0f 04%...
0050	65 75 72 35 04 61 6b 61	6d 03 6e 65 74 00 c0 0c	eur5.aka m.net...
0060	00 02 00 01 00 00 05 25	00 07 04 75 73 77 32 c0% ...usw2.
0070	2a c0 0c 00 02 00 01 00	00 05 25 00 09 06 6e 73	*.....%...ns
0080	31 2d 33 37 c0 2a c0 0c	00 02 00 01 00 00 05 25	1-37.*..%

Figure 5: Screenshot of the answers returned from the `nslookup` command issued on `mit.edu`, requesting ns records

Note: For the following questions, instead of using `bitsy.mit.edu`, I used `resolver.opendns.com` as the DNS server to be queried, since `bitsy.mit.edu` was not working.

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 DNS query message was sent to 208.67.222.222, which is the IP that the URL `resolver1.opendns.com` corresponds to.

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

The DNS query message sent was a standard query.

22. *Examine the DNS response message. How many answers are provided? What does each of these answers contain?*

The DNS response message only contained one message. This one answer was an A record which maps the IP address 49.238.167.109 to the URL `www.aiit.or.kr`.

23. *Provide a screenshot.*

1590	1.235547	192.168.1.70	208.67.222.222	DNS	74	Standard query 0xb213 A www.aiit.or.kr
2388	1.907620	208.67.222.222	192.168.1.70	DNS	90	Standard query response 0xb213 A www.ai

▼ Queries
▶ www.aiit.or.kr: type A, class IN
▼ Answers
▼ www.aiit.or.kr: type A, class IN, addr 49.238.167.109
Name: www.aiit.or.kr
Type: A (Host Address) (1)
Class: IN (0x0001)
Time to live: 7200
Data length: 4
Address: 49.238.167.109

0000	3c 15 c2 d9 7a de 58 98 35 ad 0e de 08 00 45 00	<...z.X. 5.....E.
0010	00 4c 02 a5 40 00 38 11 ce eb d0 43 de de c0 a8	.L..@.8. ...C....
0020	01 46 00 35 dd 10 00 38 87 67 b2 13 81 80 00 01	.F.5...8 .g.....
0030	00 01 00 00 00 00 03 77 77 77 04 61 69 69 74 02w ww.aiit.
0040	6f 72 02 6b 72 00 00 01 00 01 c0 0c 00 01 00 01	or.kr... ..
0050	00 00 1c 20 00 04 31 ee a7 6d1. .m

Figure 6: Screenshot of the answers returned from the `nslookup` command issued on `mit.edu`, with the `-type=ns` flag set to request for nameserver records