

Phang Teng Fone 1003296 LAB 6

DNS basics

Question 1: Using dig, find the IP address for thyme.lcs.mit.edu. What is the IP address?

18.26.0.122

Question 2: The dig answer for the previous question includes a record of type CNAME. What does CNAME mean?

Canonical Name

Question 3: What is the expiration time for the CNAME record?

1800

Question 4: Run the following commands to find out what your computer receives when it looks up 'ai' and 'ai.' in the mit.edu domain. What are the two resulting IP addresses?

- dig +domain=mit.edu ai

No IP Address received

- dig +domain=mit.edu ai.

209.59.119.34

Question 5: Why are the results for both queries different? Look up the manual for dig to find out what the +domain parameter does. Based on the output of the two commands, what is the difference between the DNS searches being performed for 'ai' and 'ai.'?

By adding a trailing dot at the end, it signifies the DNS root (absolute address). When selecting mit.edu ai it is querying an authority server which decides to not provide an IP address, while the absolute address of ai. is being directed to a domain registrar which contains an IP address.

Question 6: Use dig to query one of the DNS root servers for the IP address of lirone.csail.mit.edu without using recursion. What is the command that you use to do this?

1st: dig . NS lirone.csail.mit.edu

2nd: dig @d.root-servers.net. lirone.csail.mit.edu +norecurs

```
;; AUTHORITY SECTION:
edu.      172800 IN      NS      a.edu-servers.net.
edu.      172800 IN      NS      b.edu-servers.net.
edu.      172800 IN      NS      c.edu-servers.net.
edu.      172800 IN      NS      d.edu-servers.net.
edu.      172800 IN      NS      e.edu-servers.net.
edu.      172800 IN      NS      f.edu-servers.net.
edu.      172800 IN      NS      g.edu-servers.net.
edu.      172800 IN      NS      h.edu-servers.net.
edu.      172800 IN      NS      i.edu-servers.net.
edu.      172800 IN      NS      j.edu-servers.net.
edu.      172800 IN      NS      k.edu-servers.net.
edu.      172800 IN      NS      l.edu-servers.net.
edu.      172800 IN      NS      m.edu-servers.net.

;; ADDITIONAL SECTION:
a.edu-servers.net. 172800 IN      A      192.5.6.30
b.edu-servers.net. 172800 IN      A      192.33.14.30
c.edu-servers.net. 172800 IN      A      192.26.92.30
d.edu-servers.net. 172800 IN      A      192.31.80.30
e.edu-servers.net. 172800 IN      A      192.12.94.30
f.edu-servers.net. 172800 IN      A      192.35.51.30
g.edu-servers.net. 172800 IN      A      192.42.92.30
h.edu-servers.net. 172800 IN      A      192.54.112.30
i.edu-servers.net. 172800 IN      A      192.43.172.30
j.edu-servers.net. 172800 IN      A      192.48.79.30
k.edu-servers.net. 172800 IN      A      192.52.178.30
l.edu-servers.net. 172800 IN      A      192.41.102.30
```

Question 7: Go through the DNS hierarchy from the root until you have found the IP address of lirone.csail.mit.edu. You should disable recursion and follow the referrals manually. Which commands did you use, and what address did you find?

1st: dig @a.edu-servers.net. lirone.csail.mit.edu +norecurs

2nd: dig @usw2.akam.net. lirone.csail.mit.edu +norecurs

3rd: dig @auth-ns0.csail.mit.edu. lirone.csail.mit.edu +norecurs

```
tengfong@Desktop:~/home$ dig @auth-ns0.csail.mit.edu. lirone.csail.mit.edu +norecurs
; <<>> DIG 9.11.3-1ubuntu1.11-Ubuntu <<>> @auth-ns0.csail.mit.edu. lirone.csail.mit.edu +norecurs
; (2 servers found)
; global options: +cmd
; Got answer:
; -->HEADER<-- opcode: QUERY, status: NOERROR, id: 17996
; flags: qr aa; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: udp: 4096
; COOKIE: 1c91b0d0f1b3dc47010000005e8caf00edc1c80d474f4806 (good)
;; QUESTION SECTION:
;lirone.csail.mit.edu.      IN      A

;; ANSWER SECTION:
;lirone.csail.mit.edu.      1800    IN      A      128.52.129.186

;; Query time: 250 msec
;; SERVER: 128.30.2.123#53(128.30.2.123)
;; WHEN: Wed Apr 08 00:49:12 +08 2020
;; MSG SIZE rcvd: 93
```

Found IP address 128.52.129.186

Understanding caching

Question 8: Without using recursion, query your default DNS server for information about www.dmoz.org and answer the following questions.

- What is the command that you used?

1st getting my DNS server: `cat /etc/resolv.conf`

2nd query: `dig @192.168.1.1 www.dmoz.org +norecurs`

- Did your default server have the answer in its cache? How did you know?

No. There was no answer section on the first run.

- How long did the query take?

4 msec

Note: If the information was cached, find another host name that was not cached and complete all the questions in this section using that host.

Question 9: Query your default DNS server for information about the host in the previous question, using the recursion option this time. How long did the query take?

`dig @192.168.1.1 www.bling.com +norecurs`

13ms

Question 10: Query your default DNS server for information about the same host without using recursion. How long did the query take? Has the cache served its purpose? Explain why.

4ms. Yes it has served its purpose as it produced an answer section (query) within a shorter time.

Part 2: Tracing DNS using Wireshark

Question 1: Locate the DNS query and response messages. Are they sent over UDP or TCP?

UDP

Question 2: What is the destination port for the DNS query message? What is the source port of the DNS response message?

Destination Port: 53

Source Port: 57763

Question 3: What is the IP address to which the DNS query message was sent? Use ifconfig to determine the IP address of your local DNS server. Are these two addresses the same?

192.168.2.11. They are not the same (mine is 192.168.1.1)

Question 4: Examine the second DNS query message. What type of DNS query is it? Does the query message contain any answers?

It is a standard recursive DNS query. The query message contains no answers.

Question 5: Examine the second DNS response message. How many answers are provided? What does each of these answers contain?

2 answers are provided. A CNAME updatekeepalive.glb.mcafee.com and a type A host address of 161.69.12.13.

```
Answers
  updatekeepalive.mcafee.com: type CNAME, class IN, cname updatekeepalive.glb.mcafee.com
    Name: updatekeepalive.mcafee.com
    Type: CNAME (Canonical NAME for an alias) (5)
    Class: IN (0x0001)
    Time to live: 209 (3 minutes, 29 seconds)
    Data length: 22
    CNAME: updatekeepalive.glb.mcafee.com
  updatekeepalive.glb.mcafee.com: type A, class IN, addr 161.69.12.13
    Name: updatekeepalive.glb.mcafee.com
    Type: A (Host Address) (1)
    Class: IN (0x0001)
    Time to live: 3 (3 seconds)
    Data length: 4
    Address: 161.69.12.13
[Request In: 11]
[Time: 0.005536000 seconds]
```

Question 6: Locate a TCP SYN packet sent by your host subsequent to the above DNS response. This packet opens a TCP connection between your host and the web server. Does the destination IP address of the SYN packet correspond to any of the IP addresses provided in the DNS response message?

I tried by sniffing my own packets to Microsoft.com and here are the responses:

962	4.340867	192.168.1.186	192.168.1.1	DNS	74	Standard query 0x90bb A login.live.com
963	4.346398	192.168.1.1	192.168.1.186	DNS	198	Standard query response 0x90bb A login.live.com CNAME login.msa.msidentity
964	4.346761	192.168.1.186	40.90.23.153	TCP	66	58543 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM=1
965	4.371476	111.221.29.254	192.168.1.186	TCP	60	443 → 58530 [ACK] Seq=8897 Ack=30190 Win=262656 Len=0
966	4.372008	111.221.29.254	192.168.1.186	TCP	60	443 → 58530 [ACK] Seq=8897 Ack=33070 Win=262656 Len=0
967	4.372008	111.221.29.254	192.168.1.186	TCP	60	443 → 58530 [ACK] Seq=8897 Ack=35317 Win=262656 Len=0
968	4.372893	111.221.29.254	192.168.1.186	TCP	60	443 → 58529 [ACK] Seq=5920 Ack=3192 Win=262656 Len=0
969	4.372894	111.221.29.254	192.168.1.186	TCP	60	443 → 58529 [ACK] Seq=5920 Ack=6072 Win=262656 Len=0
970	4.373510	111.221.29.254	192.168.1.186	TCP	60	443 → 58529 [ACK] Seq=5920 Ack=8952 Win=262656 Len=0


```
Class: IN (0x0001)
Answers
  login.live.com: type CNAME, class IN, cname login.msa.msidentity.com
    Name: login.live.com
    Type: CNAME (Canonical NAME for an alias) (5)
    Class: IN (0x0001)
    Time to live: 58 (58 seconds)
    Data length: 23
    CNAME: login.msa.msidentity.com
  login.msa.msidentity.com: type CNAME, class IN, cname login.msa.trafficmanager.net
    Name: login.msa.msidentity.com
    Type: CNAME (Canonical NAME for an alias) (5)
    Class: IN (0x0001)
    Time to live: 259 (4 minutes, 19 seconds)
    Data length: 29
    CNAME: login.msa.trafficmanager.net
  login.msa.trafficmanager.net: type A, class IN, addr 40.90.23.153
    Name: login.msa.trafficmanager.net
    Type: A (Host Address) (1)
    Class: IN (0x0001)
    Time to live: 30 (30 seconds)
```

This shows that the destination IP address of the SYN packet correspond to the DNS responses message under Answers.