Hands on 1

Question 1

In my word, the role that Domain Name Service plays is providing a mapping between the domain name and IP address, with which we could access the remote servers via simple semantic domain names rather than meaningless number tuples.

Question 2

The "dig" command returns as following in my environment:

```
; <<>> DiG 9.8.3-P1 <<>> www.sina.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 12851
;; flags: qr rd ra; QUERY: 1, ANSWER: 4, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;www.sina.com.                  IN      A

;; ANSWER SECTION:
www.sina.com.           59      IN      CNAME   us.sina.com.cn.
us.sina.com.cn.         59      IN      CNAME   spool.grid.sinaedge.com.
spool.grid.sinaedge.com. 59     IN      A       58.205.212.26
spool.grid.sinaedge.com. 59     IN      A       58.205.212.27

;; Query time: 482 msec
;; SERVER: 8.8.4.4#53(8.8.4.4)
;; WHEN: Sat Oct 19 15:15:47 2019
;; MSG SIZE  rcvd: 124
```

According to the manual, the fourth line in the ANSWER SECTION indicates the type of the DNS record.

"A" refers to the most plain address record: a domain name matched with an IPv4 address.

"AAAA" is also plain, but matched with an IPv6 address.

"CNAME" isn't so direct as "A" and "AAAA" type; it means this domain isn't mapped with an IP address directly. It is mapped with another domain name and the actual IP address should be obtained via that indirect domain name, though. So you can see those records with "A" type have specific IP addresses on the right, however those with "CNAME" type have other domain names on the right side.

There are also some unnatural types of records, like "MX", "NS", "SOA", and "TXT". Omit them to reduce the size of this PDF document.

Question 3

The "dig" command displays which Domain Name Server it is using on the third last line. For example, I'm currently using Google's DNS at 8.8.4.4#53, because of my earlier system configuration. But if we want to explicitly declare the DNS that "dig" command uses, we could run the following command:

```
dig @4.2.2.1 google.com.hk
```

And here's the result:

```
; <<>> DiG 9.8.3-P1 <<>> @4.2.2.1 google.com.hk
; (1 server found)

......

;; ANSWER SECTION:
google.com.hk.          247     IN      A       31.13.86.1

;; Query time: 43 msec
;; SERVER: 4.2.2.1#53(4.2.2.1)
;; WHEN: Sat Oct 19 15:50:01 2019
;; MSG SIZE  rcvd: 47
```

Question 4

Interesting question. First let's see if we can get 13 root domain name servers:

```
; <<>> DiG 9.8.3-P1 <<>> . ns
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 33807
;; flags: qr rd ra; QUERY: 1, ANSWER: 13, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;.                              IN      NS

;; ANSWER SECTION:
.                       60407   IN      NS      a.root-servers.net.
.                       60407   IN      NS      b.root-servers.net.
.                       60407   IN      NS      c.root-servers.net.
.                       60407   IN      NS      d.root-servers.net.
.                       60407   IN      NS      e.root-servers.net.
.                       60407   IN      NS      f.root-servers.net.
.                       60407   IN      NS      g.root-servers.net.
.                       60407   IN      NS      h.root-servers.net.
.                       60407   IN      NS      i.root-servers.net.
.                       60407   IN      NS      j.root-servers.net.
.                       60407   IN      NS      k.root-servers.net.
.                       60407   IN      NS      l.root-servers.net.
.                       60407   IN      NS      m.root-servers.net.

;; Query time: 264 msec
;; SERVER: 8.8.8.8#53(8.8.8.8)
;; WHEN: Sat Oct 19 15:52:22 2019
;; MSG SIZE  rcvd: 228
```

So when we are digging information about the librone.csail.mit.edu(.), we would get the following:

```
; <<>> DiG 9.8.3-P1 <<>> lirone.csail.mit.edu
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 22227
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;lirone.csail.mit.edu.          IN      A

;; ANSWER SECTION:
lirone.csail.mit.edu.   1799    IN      A       128.52.129.186

;; Query time: 476 msec
;; SERVER: 8.8.8.8#53(8.8.8.8)
;; WHEN: Sat Oct 19 15:51:56 2019
;; MSG SIZE  rcvd: 54
```

Under the current circumstance, lirone.csail.mit.edu. are mapped directly to 128.52.129.186. But when we see it with +trace command, here's what we've gotten:

```
; <<>> DiG 9.8.3-P1 <<>> lirone.csail.mit.edu. +trace
;; global options: +cmd
.                       60099   IN      NS      m.root-servers.net.
.                       60099   IN      NS      b.root-servers.net.
.                       60099   IN      NS      c.root-servers.net.
.                       60099   IN      NS      d.root-servers.net.
.                       60099   IN      NS      e.root-servers.net.
.                       60099   IN      NS      f.root-servers.net.
.                       60099   IN      NS      g.root-servers.net.
.                       60099   IN      NS      h.root-servers.net.
.                       60099   IN      NS      a.root-servers.net.
```

```
.                       60099   IN      NS      i.root-servers.net.
.                       60099   IN      NS      j.root-servers.net.
.                       60099   IN      NS      k.root-servers.net.
.                       60099   IN      NS      l.root-servers.net.
;; Received 228 bytes from 8.8.8.8#53(8.8.8.8) in 3759 ms

edu.                    172800  IN      NS      e.edu-servers.net.
edu.                    172800  IN      NS      i.edu-servers.net.
edu.                    172800  IN      NS      l.edu-servers.net.
edu.                    172800  IN      NS      k.edu-servers.net.
edu.                    172800  IN      NS      j.edu-servers.net.
edu.                    172800  IN      NS      b.edu-servers.net.
edu.                    172800  IN      NS      d.edu-servers.net.
edu.                    172800  IN      NS      a.edu-servers.net.
edu.                    172800  IN      NS      m.edu-servers.net.
edu.                    172800  IN      NS      f.edu-servers.net.
edu.                    172800  IN      NS      c.edu-servers.net.
edu.                    172800  IN      NS      g.edu-servers.net.
edu.                    172800  IN      NS      h.edu-servers.net.
;; Received 497 bytes from 199.7.83.42#53(199.7.83.42) in 4095 ms

mit.edu.                172800  IN      NS      usw2.akam.net.
mit.edu.                172800  IN      NS      asia1.akam.net.
mit.edu.                172800  IN      NS      asia2.akam.net.
mit.edu.                172800  IN      NS      use2.akam.net.
mit.edu.                172800  IN      NS      ns1-37.akam.net.
mit.edu.                172800  IN      NS      ns1-173.akam.net.
mit.edu.                172800  IN      NS      eur5.akam.net.
mit.edu.                172800  IN      NS      use5.akam.net.
;; Received 205 bytes from 192.12.94.30#53(192.12.94.30) in 2969 ms

csail.mit.edu.          1800    IN      NS      auth-ns2.csail.mit.edu.
csail.mit.edu.          1800    IN      NS      auth-ns0.csail.mit.edu.
```

```
csail.mit.edu.          1800    IN      NS      auth-ns3.csail.mit.edu.
csail.mit.edu.          1800    IN      NS      auth-ns1.csail.mit.edu.
;; Received 222 bytes from 184.26.161.64#53(184.26.161.64) in 1842 ms

lirone.csail.mit.edu.   1800    IN      A       128.52.129.186
;; Received 54 bytes from 128.30.2.123#53(128.30.2.123) in 394 ms
```

That's a perfect hierarchy! It starts from 13 root DNSs, and then the edu. (ruled by the MoE or something), mit.edu. (ruled by the MIT), csail.mit.edu. (ruled by the MIT Computer Science & Artificial Intelligence Lab), and finally the domain lirone.csail.mit.edu. (ruled by The Programming Methodology Group, CSAIL, MIT.)

Question 5 & 6

Differences between Twitter and Baidu's treatment?

Twitter

dig www.twitter.com +trace

```
; <<>> DiG 9.8.3-P1 <<>> www.twitter.com +trace
;; global options: +cmd
.                       59784   IN      NS      i.root-servers.net.
.                       59784   IN      NS      k.root-servers.net.
.                       59784   IN      NS      e.root-servers.net.
.                       59784   IN      NS      g.root-servers.net.
.                       59784   IN      NS      d.root-servers.net.
.                       59784   IN      NS      c.root-servers.net.
.                       59784   IN      NS      h.root-servers.net.
.                       59784   IN      NS      l.root-servers.net.
.                       59784   IN      NS      a.root-servers.net.
.                       59784   IN      NS      m.root-servers.net.
.                       59784   IN      NS      b.root-servers.net.
.                       59784   IN      NS      j.root-servers.net.
```

```
.                       59784   IN      NS      f.root-servers.net.
;; Received 228 bytes from 8.8.8.8#53(8.8.8.8) in 317 ms

com.                    172800  IN      NS      d.gtld-servers.net.
com.                    172800  IN      NS      k.gtld-servers.net.
com.                    172800  IN      NS      h.gtld-servers.net.
com.                    172800  IN      NS      g.gtld-servers.net.
com.                    172800  IN      NS      c.gtld-servers.net.
com.                    172800  IN      NS      b.gtld-servers.net.
com.                    172800  IN      NS      a.gtld-servers.net.
com.                    172800  IN      NS      m.gtld-servers.net.
com.                    172800  IN      NS      f.gtld-servers.net.
com.                    172800  IN      NS      i.gtld-servers.net.
com.                    172800  IN      NS      j.gtld-servers.net.
com.                    172800  IN      NS      l.gtld-servers.net.
com.                    172800  IN      NS      e.gtld-servers.net.
;; Received 493 bytes from 192.33.4.12#53(192.33.4.12) in 26 ms

www.twitter.com.        190     IN      A       69.171.232.21
;; Received 49 bytes from 192.54.112.30#53(192.54.112.30) in 28 ms
```

Baidu

dig www.baidu.com +trace

```
; <<>> DiG 9.8.3-P1 <<>> www.baidu.com +trace
;; global options: +cmd
.                       59782   IN      NS      a.root-servers.net.
.                       59782   IN      NS      b.root-servers.net.
.                       59782   IN      NS      c.root-servers.net.
.                       59782   IN      NS      d.root-servers.net.
.                       59782   IN      NS      e.root-servers.net.
.                       59782   IN      NS      f.root-servers.net.
.                       59782   IN      NS      g.root-servers.net.
```

```
.                       59782   IN      NS      h.root-servers.net.
.                       59782   IN      NS      i.root-servers.net.
.                       59782   IN      NS      j.root-servers.net.
.                       59782   IN      NS      k.root-servers.net.
.                       59782   IN      NS      l.root-servers.net.
.                       59782   IN      NS      m.root-servers.net.
;; Received 228 bytes from 8.8.8.8#53(8.8.8.8) in 248 ms

com.                    172800  IN      NS      c.gtld-servers.net.
com.                    172800  IN      NS      f.gtld-servers.net.
com.                    172800  IN      NS      i.gtld-servers.net.
com.                    172800  IN      NS      j.gtld-servers.net.
com.                    172800  IN      NS      b.gtld-servers.net.
com.                    172800  IN      NS      g.gtld-servers.net.
com.                    172800  IN      NS      d.gtld-servers.net.
com.                    172800  IN      NS      l.gtld-servers.net.
com.                    172800  IN      NS      k.gtld-servers.net.
com.                    172800  IN      NS      a.gtld-servers.net.
com.                    172800  IN      NS      h.gtld-servers.net.
com.                    172800  IN      NS      m.gtld-servers.net.
com.                    172800  IN      NS      e.gtld-servers.net.
;; Received 491 bytes from 192.5.5.241#53(192.5.5.241) in 24 ms

baidu.com.              172800  IN      NS      ns2.baidu.com.
baidu.com.              172800  IN      NS      ns3.baidu.com.
baidu.com.              172800  IN      NS      ns4.baidu.com.
baidu.com.              172800  IN      NS      ns1.baidu.com.
baidu.com.              172800  IN      NS      ns7.baidu.com.
;; Received 201 bytes from 192.5.6.30#53(192.5.6.30) in 399 ms

www.baidu.com.          1200    IN      CNAME   www.a.shifen.com.
a.shifen.com.           1200    IN      NS      ns5.a.shifen.com.
a.shifen.com.           1200    IN      NS      ns2.a.shifen.com.
```

```
a.shifen.com.           1200    IN      NS      ns3.a.shifen.com.
a.shifen.com.           1200    IN      NS      ns4.a.shifen.com.
a.shifen.com.           1200    IN      NS      ns1.a.shifen.com.
;; Received 228 bytes from 180.76.76.92#53(180.76.76.92) in 41 ms
```

Baidu has a quite normal hierarchy: The domain name resolve process starts from 13 root DNSs, and then some Generic Top Level Domains (those gtld-servers.net.), and then Baidu's internal DNSs; finally, the shifen.com is Baidu's advertisement managements system. Finally we got a normal IP as 180.76.76.92.

What about Twitter? we may see that after the DNSs and GTLDs, no requests were posted to Twitter's internal network. And the IP we got is also very weird: 69.171.232.21 seems belonging to facebook.com! Why?

Well, it's a very practical technique that resolve domain names to wrong IPs could make some domain "unreachable". And what if we resolve those requests to those IP that I want to ban too, we can shoot two birds down in one fell swoop! Great.

Here's the full list that normal requests to the DNS would be incorrectly resolves to, most of them belongs to FaceBook and Google:

```
8.7.198.45
31.13.64.1
31.13.64.33
31.13.64.49
31.13.65.1
31.13.65.17
31.13.65.18
31.13.66.1
31.13.66.6
31.13.66.23
31.13.68.1
31.13.68.22
31.13.69.33
```

31.13.69.86
31.13.69.129
31.13.69.160
31.13.70.1
31.13.70.20
31.13.71.7
31.13.71.23
31.13.72.1
31.13.72.17
31.13.72.23
31.13.72.34
31.13.72.54
31.13.73.1
31.13.73.17
31.13.73.23
31.13.74.1
31.13.74.17
31.13.75.17
31.13.75.18
31.13.76.8
31.13.76.16
31.13.77.33
31.13.77.55
31.13.78.65
31.13.78.66
31.13.79.1
31.13.79.17
31.13.80.1
31.13.80.17
31.13.81.1
31.13.81.17
31.13.82.1
31.13.82.17

31.13.82.23
31.13.83.1
31.13.83.8
31.13.83.16
31.13.84.1
31.13.84.8
31.13.84.16
31.13.85.1
31.13.85.8
31.13.85.16
31.13.86.1
31.13.86.8
31.13.86.16
31.13.97.245
31.13.97.248
46.82.174.68
59.24.3.173
64.13.192.74
64.13.192.76
64.13.232.149
66.220.146.94
66.220.147.11
66.220.147.44
66.220.147.47
66.220.149.18
66.220.149.32
66.220.149.99
66.220.151.20
66.220.152.17
66.220.152.28
66.220.155.12
66.220.155.14
66.220.158.32

67.15.100.252
67.15.129.210
67.228.37.26
67.228.74.123
67.228.102.32
67.228.126.62
67.228.221.221
67.228.235.91
67.228.235.93
69.63.176.15
69.63.176.59
69.63.176.143
69.63.178.13
69.63.180.173
69.63.181.11
69.63.181.12
69.63.184.14
69.63.184.30
69.63.184.142
69.63.186.30
69.63.186.31
69.63.187.12
69.63.189.16
69.63.190.26
69.171.224.12
69.171.224.40
69.171.224.85
69.171.225.13
69.171.227.37
69.171.228.20
69.171.228.74
69.171.229.11
69.171.229.28

69.171.229.73
69.171.230.18
69.171.232.21
69.171.233.24
69.171.233.33
69.171.233.37
69.171.234.18
69.171.234.29
69.171.234.48
69.171.235.16
69.171.235.64
69.171.235.101
69.171.237.16
69.171.237.26
69.171.239.11
69.171.240.27
69.171.242.11
69.171.242.30
69.171.244.11
69.171.244.12
69.171.244.15
69.171.245.49
69.171.245.53
69.171.245.84
69.171.246.9
69.171.247.20
69.171.247.32
69.171.247.71
69.171.248.65
69.171.248.112
69.171.248.128
74.86.3.208
74.86.12.172

74.86.12.173
74.86.17.48
74.86.118.24
74.86.142.55
74.86.151.162
74.86.151.167
74.86.226.234
74.86.228.110
74.86.235.236
75.126.2.43
75.126.33.156
75.126.115.192
75.126.124.162
75.126.135.131
75.126.150.210
75.126.164.178
75.126.215.88
78.16.49.15
88.191.249.182
88.191.249.183
88.191.253.157
93.46.8.89
173.252.73.48
173.252.100.21
173.252.100.32
173.252.102.16
173.252.102.241
173.252.103.64
173.252.110.21
174.36.196.242
174.36.228.136
174.37.54.20
174.37.154.236

```
174.37.175.229
199.16.156.7
199.16.156.40
199.16.158.190
199.59.148.14
199.59.148.97
199.59.148.140
199.59.148.209
199.59.149.136
199.59.149.244
199.59.150.11
199.59.150.49
205.186.152.122
208.43.170.231
208.43.237.140
208.101.21.43
208.101.48.171
208.101.60.87
243.185.187.39
```

May you rest in peace.