Hands-on-3

Domain Name Service (DNS)

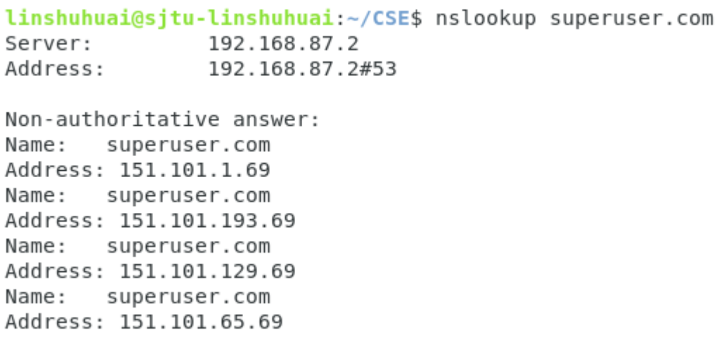
This hands-on would help you learn more about the Internet's Domain Name System (DNS).

Q1: What's the role of DNS? Please describe it using your own words.

域名系统是将域名和IP地址相互映射的一个分布式数据库，主要功能是提供域名解析服务，并将域名解析为IP地址，实现用户访问网站时只用输入域名即可访问的功能，能够使人更方便地访问互联网。

Answer Section: five fields of this section are name, expiration time, class, type, data

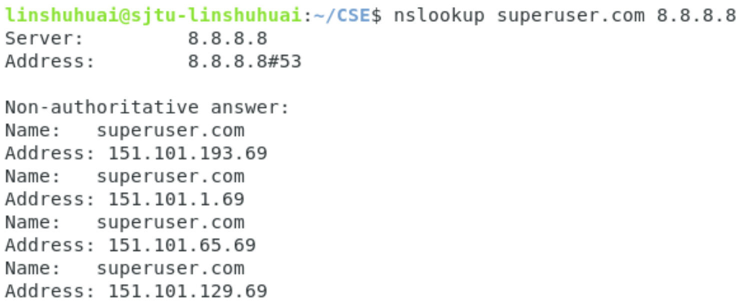
Q2: How can you ask a specific DNS server (instead of the default) for information about a domain name? For example, once the default server crashes and you wish to ask the other server 8.8.8.8, what command should you use?



```
linshuhuai@sjtu-linshuhuai:~/CSE$ nslookup superuser.com
Server:         192.168.87.2
Address:        192.168.87.2#53

Non-authoritative answer:
Name:   superuser.com
Address: 151.101.1.69
Name:   superuser.com
Address: 151.101.193.69
Name:   superuser.com
Address: 151.101.129.69
Name:   superuser.com
Address: 151.101.65.69
```

`nslookup superuser.com` 会向自己的DNS server发送域名解析请求来找到superuser.com的IP地址

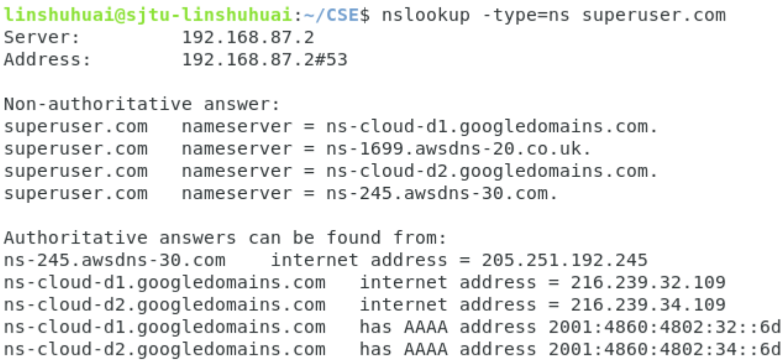


```
linshuhuai@sjtu-linshuhuai:~/CSE$ nslookup superuser.com 8.8.8.8
Server:         8.8.8.8
Address:        8.8.8.8#53

Non-authoritative answer:
Name:   superuser.com
Address: 151.101.193.69
Name:   superuser.com
Address: 151.101.1.69
Name:   superuser.com
Address: 151.101.65.69
Name:   superuser.com
Address: 151.101.129.69
```

如果在命令里面对加一个ip地址，可以将域名解析请求发给指定的DNS server。比如 `nslookup superuser.com 8.8.8.8`

另外，这里出现“Non-authoritative answe”表明这次查询并没有到网络外去查询（即没有去找到superuser.com的权威服务器），而是在local DNS的缓存区中查找并找到数据。如果想找权威服务器，可以如下操作：



```
linshuhuai@sjtu-linshuhuai:~/CSE$ nslookup -type=ns superuser.com
Server:         192.168.87.2
Address:        192.168.87.2#53

Non-authoritative answer:
superuser.com   nameserver = ns-cloud-d1.googledomains.com.
superuser.com   nameserver = ns-1699.awsdns-20.co.uk.
superuser.com   nameserver = ns-cloud-d2.googledomains.com.
superuser.com   nameserver = ns-245.awsdns-30.com.

Authoritative answers can be found from:
ns-245.awsdns-30.com    internet address = 205.251.192.245
ns-cloud-d1.googledomains.com   internet address = 216.239.32.109
ns-cloud-d2.googledomains.com   internet address = 216.239.34.109
ns-cloud-d1.googledomains.com   has AAAA address 2001:4860:4802:32::6d
ns-cloud-d2.googledomains.com   has AAAA address 2001:4860:4802:34::6d
```

指令加 -type=ns

最下面的几个是superuser.com的权威服务器

Q3: Do you know the process of solving the domain name of "ipads.se.sjtu.edu.cn"? How many queries did it take to find the IP address for ipads? Include the sequence of commands that you used.

Hint: you should start from "cn".

查询过程：

dig . dn

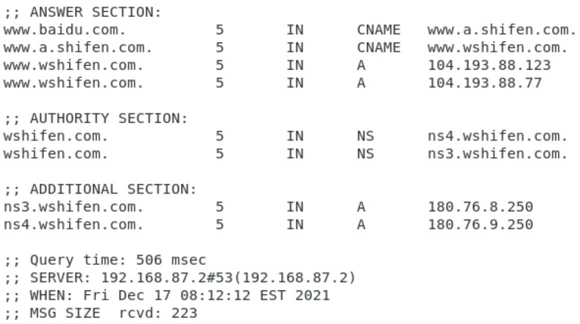
dig . cn
dig @k.root-servers.net ipads.se.sjtu.edu.cn +norecurse
dig @a.dns.cn ipads.se.sjtu.edu.cn +norecurse
dig @dns.edu.cn ipads.se.sjtu.edu.cn +norecurse
dig @dns.sjtu.edu.cn ipads.se.sjtu.edu.cn +norecurse
dig @202.120.40.2 ipads.se.sjtu.edu.cn +norecurse

一共需要6步

Q4: Did the default server have the answer in its cache? How do you know?

Hint: For each query that you run, please keep track of how long it took to get a response. If this information was cached, please find another host name that is not cached and *do differential testing*.

`dig www.baidu.com`



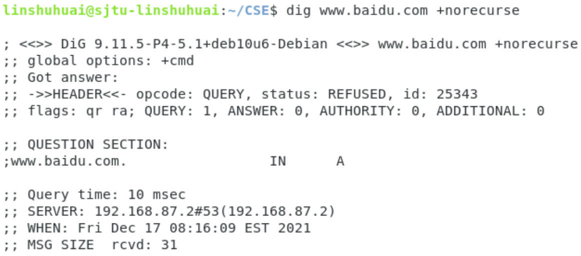
```
;; ANSWER SECTION:
www.baidu.com.          5       IN      CNAME   www.a.shifen.com.
www.a.shifen.com.       5       IN      CNAME   www.wshifen.com.
www.wshifen.com.        5       IN      A       104.193.88.123
www.wshifen.com.        5       IN      A       104.193.88.77

;; AUTHORITY SECTION:
wshifen.com.            5       IN      NS      ns4.wshifen.com.
wshifen.com.            5       IN      NS      ns3.wshifen.com.

;; ADDITIONAL SECTION:
ns3.wshifen.com.        5       IN      A       180.76.8.250
ns4.wshifen.com.        5       IN      A       180.76.9.250

;; Query time: 506 msec
;; SERVER: 192.168.87.2#53(192.168.87.2)
;; WHEN: Fri Dec 17 08:12:12 EST 2021
;; MSG SIZE  rcvd: 223
```

`dig www.baidu.com +norecurse`



```
linshuhuai@sjtu-linshuhuai:~/CSE$ dig www.baidu.com +norecurse

; <<>> DiG 9.11.5-P4-5.1+deb10u6-Debian <<>> www.baidu.com +norecurse
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: REFUSED, id: 25343
;; flags: qr ra; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 0

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

;; Query time: 10 msec
;; SERVER: 192.168.87.2#53(192.168.87.2)
;; WHEN: Fri Dec 17 08:16:09 EST 2021
;; MSG SIZE  rcvd: 31
```

可以看出默认服务器在第一次解析域名时耗时比较大，而在第二次解析同一个域名时由于cache已经存了hostname所以快了很多。