关于 DNS 逆向查询的答疑

谢瑞桃

同学提问：为啥 nslookup 转 IP 域名时，虽然学校的 IP 地址转不了域名，但是谷歌的可以。见下图：

```
PS C:\Windows\system32> nslookup
默认服务器:  ns.szptt.net.cn
Address:  202.96.134.133

> www.szu.edu.cn
服务器:  ns.szptt.net.cn
Address:  202.96.134.133

非权威应答:
名称:    www.szu.edu.cn
Addresses:  2001:250:3c00:212::166
          210.39.12.247

> 210.39.12.247
服务器:  ns.szptt.net.cn
Address:  202.96.134.133

*** ns.szptt.net.cn 找不到 210.39.12.247: Server failed
```

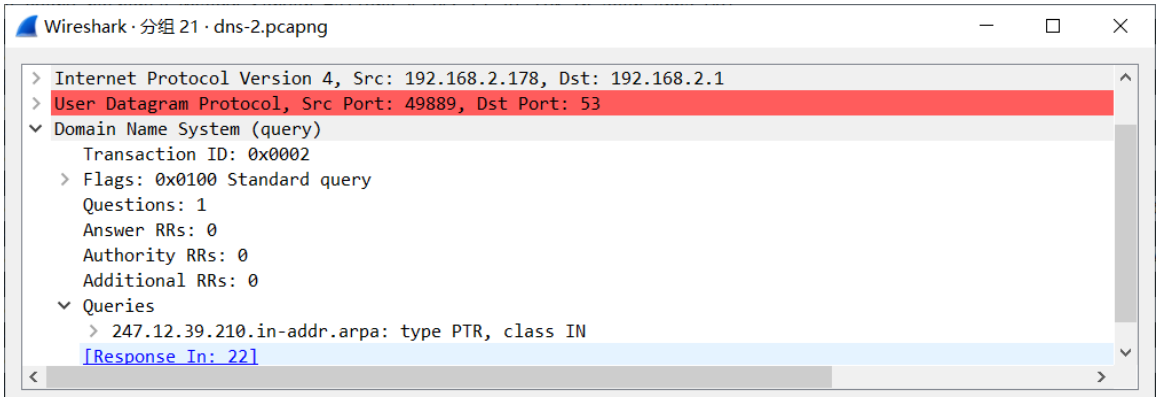
```
> google-public-dns-a.google.com
服务器:  ns.szptt.net.cn
Address:  202.96.134.133

非权威应答:
名称:    google-public-dns-a.google.com
Addresses:  2001:4860:4860::8888
          8.8.8.8

> 8.8.8.8
服务器:  ns.szptt.net.cn
Address:  202.96.134.133

名称:    dns.google
Address:  8.8.8.8
```

同学提问：老师，为什么我输入域名可以找到 IP 地址，但是输入 ip 地址却找不到对应的域名？见下图：

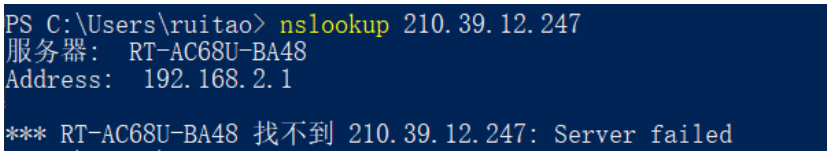
```
C:\Users\Administrator>nslookup
默认服务器:  c.cn
Address:  192.168.1.1

> www.baidu.com
服务器:  c.cn
Address:  192.168.1.1

非权威应答:
名称:    www.a.shifen.com
Addresses:  182.61.200.6
          182.61.200.7
Aliases:  www.baidu.com

> 182.61.200.7
服务器:  c.cn
Address:  192.168.1.1

*** c.cn 找不到 182.61.200.7: Non-existent domain
> 182.61.200.6
服务器:  c.cn
Address:  192.168.1.1

*** c.cn 找不到 182.61.200.6: Non-existent domain
> quit
```

答疑：

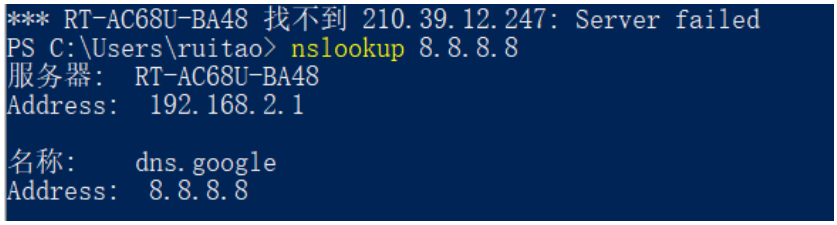
1. DNS 逆向查询实际上是通过发送一种特殊形式的 DNS 查询请求来实现的，这种查询类型是 PTR。例如运行 nslookup 210.39.12.247 的时候，会产生了如下的 DNS 查询请求。



在现在的网路里，大部分域是不会给主机创建 PTR 类型的条目。所以出现这种情况：你查不到深大 web 服务器 IP 地址对应的域名，如下图。



2. 为什么能通过 nslookup 8.8.8.8 查询到对应的域名呢？见下图



这是因为 Google 管理域的时候，创建了 PTR 条目，如下图红色部分。

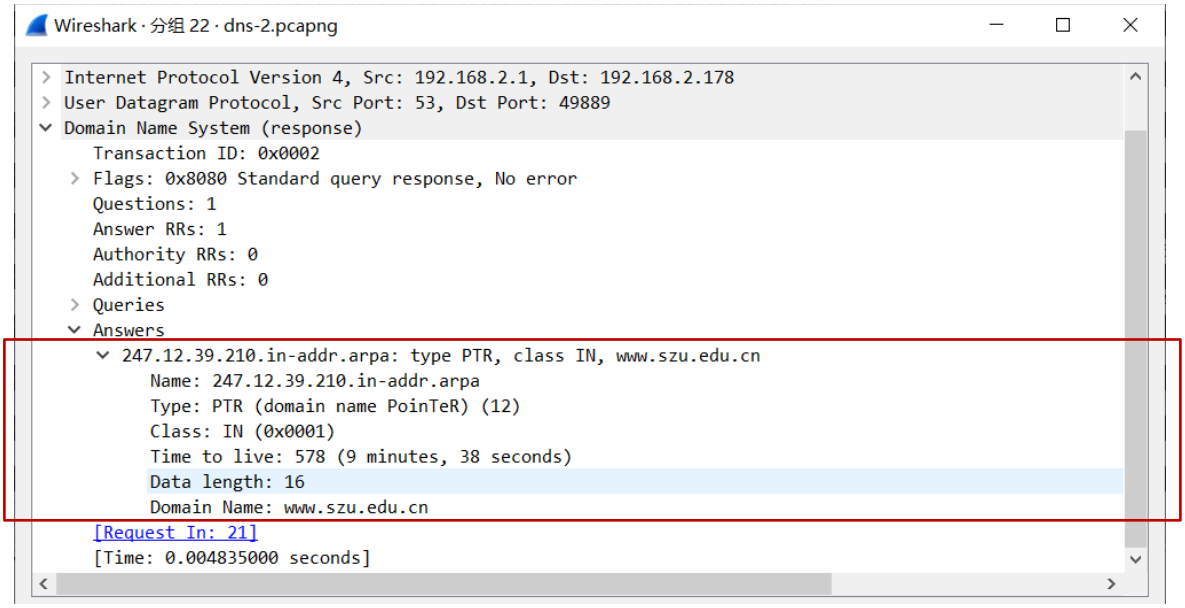
```
PS C:\Users\ruitao> dig PTR +search 8.8.8.8.in-addr.arpa

; <<>> DiG 9.14.0 <<>> PTR +search 8.8.8.8.in-addr.arpa
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 60485
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;8.8.8.8.in-addr.arpa.          IN      PTR

;; ANSWER SECTION:
8.8.8.8.in-addr.arpa.   35761   IN      PTR     dns.google.

;; Query time: 0 msec
;; SERVER: 192.168.2.1#53(192.168.2.1)
;; WHEN: Wed Apr 01 13:17:01 中国标准时间 2020
;; MSG SIZE  rcvd: 73
```

3. 为什么我有时候可以查询到深大 web 服务器 IP 的域名呢？

注意在我执行 nslookup www.szu.edu.cn 之后，我的 dns 服务器自己制造了一条 PTR 条目。所以当我之后执行 nslookup 210.39.12.247 时，得到了 www.szu.edu.cn。

```
PS C:\Users\ruitao> dig PTR +search 247.12.39.210.in-addr.arpa
;; Warning: Message parser reports malformed message packet.

; <<>> DiG 9.14.0 <<>> PTR +search 247.12.39.210.in-addr.arpa
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 55050
;; flags: qr ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: 131bda1af4cd0a8a (echoed)
;; QUESTION SECTION:
;247.12.39.210.in-addr.arpa.    IN      PTR

;; ADDITIONAL SECTION:
247.12.39.210.in-addr.arpa. 589 IN      PTR     www.szu.edu.cn.

;; Query time: 3 msec
;; SERVER: 192.168.2.1#53(192.168.2.1)
;; WHEN: Wed Apr 01 13:08:43 中国标准时间 2020
;; MSG SIZE  rcvd: 95
```

在这个过程中，产生了 DNS 应答，从中可以看到这条 PTR 条目的过期时间也就只有 10 分钟。10 分钟以后，再次执行 nslookup 210.39.12.247 就又找不到了。



4. 如果先执行 nslookup www.szu.edu.cn，再执行 nslookup 210.39.12.24，为什么你会查询不到呢？

这是因为你用的 DNS 服务器的设置是不配置 PTR 条目，所以你无法进行逆向查询。