# lab1 wireshark 以及 DNS

**17307130178 宁晨然**

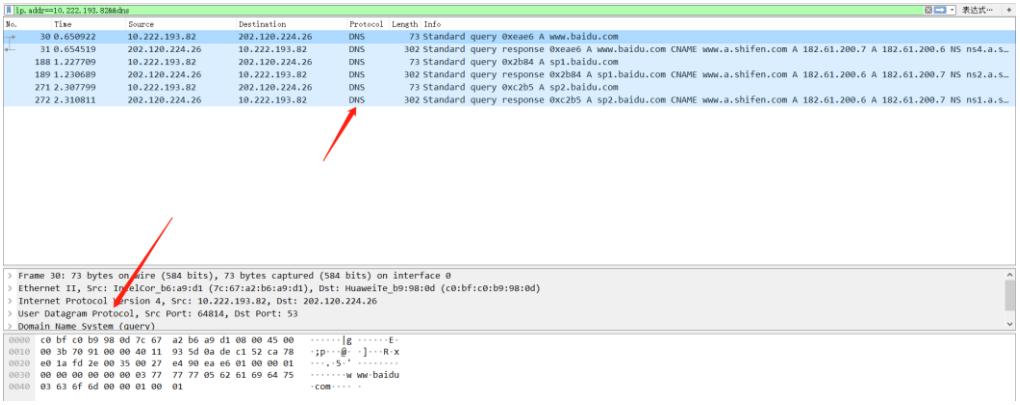
1. Run nslookup to obtain the IP address of a Web server in Asia. What is the IP address of that server?

ANS：我查询了百度的 IP 地址。www.baidu.com 的 IP 地址为 182.61.200.6 和 182.61.200.7

```
C:\Users\61082>nslookup www.baidu.com
服务器:  ns.fudan.edu.cn
Address:  202.120.224.26

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

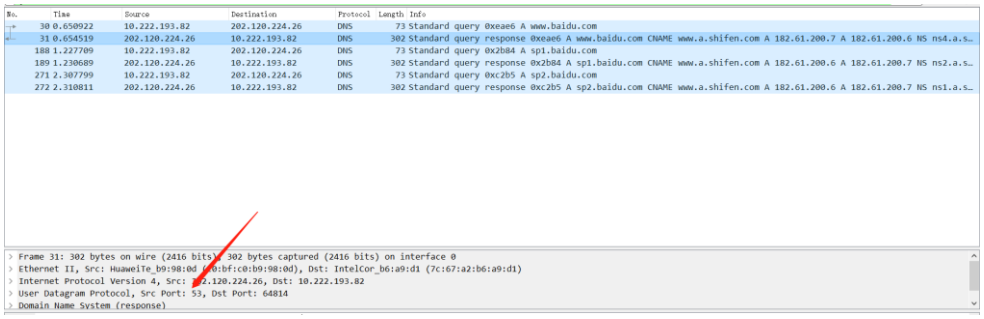
2. Locate the DNS query and response messages. Are then sent over UDP or TCP?




它们通过 UDP 发送。

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

DNS 查找的目标端口是 53，DNS 响应信息的资源端口是 53



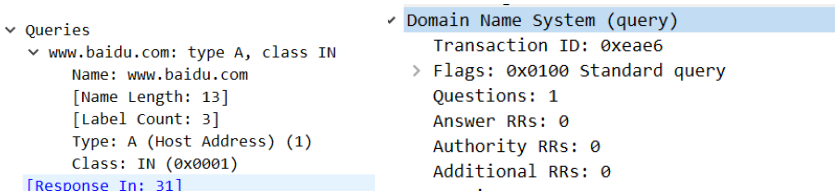

4. To what IP address is the DNS query message sent? Use ipconfig to determine the IP address of your local DNS server. Are these two IP addresses the same?

```
> Ethernet II, Src: IntelCor_b6:a9:d1 (7c:67:a2:b6:a9:d1), Dst: HuaweiTe_b9:98:0d (c0:bf:c0:b9:98:0d)
> Internet Protocol Version 4, Src: 10.222.193.82, Dst: 202.120.224.26
> User Datagram Protocol, Src Port: 64814, Dst Port: 53
> Domain Name System (query)
```

DNS query 的 IP 地址就是 10.222.193.82，这个与我本地 IP 地址相同。

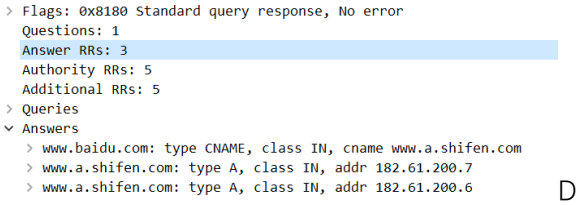
5. Examine the DNS query message. What “Type” of DNS query is it? Does the query

message contain any “answers”?

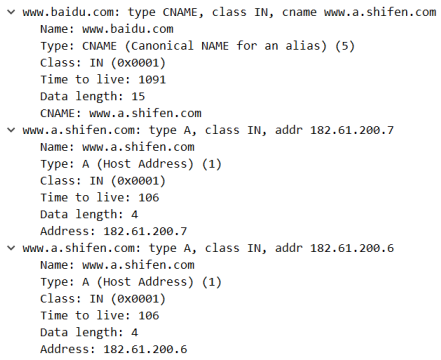



根据 DNS 信息，可知 query 的 type 是 type A；无 answer。

6. Examine the DNS response message. How many “answers” are provided? What do each of these answers contain?




DNS response message 包含了 3 个 answers。




每个 answer 包含了 name,type,class,time to live,data length,CNAME/address 等信息。