

# 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?

No.	Time	Source	Destination	Protocol	Length	Info
30	0.650922	10.222.193.82	202.120.224.26	DNS	73	Standard query 0xea66 A www.baidu.com
31	0.654519	202.120.224.26	10.222.193.82	DNS	302	Standard query response 0xea66 A www.baidu.com CNAME www.a.shifen.com A 182.61.200.7 A 182.61.200.6 NS ns4.a.s...
188	1.227789	10.222.193.82	202.120.224.26	DNS	73	Standard query 0xb844 A sp1.baidu.com
189	1.230689	202.120.224.26	10.222.193.82	DNS	302	Standard query response 0xb844 A sp1.baidu.com CNAME www.a.shifen.com A 182.61.200.6 A 182.61.200.7 NS ns2.a.s...
271	2.307799	10.222.193.82	202.120.224.26	DNS	73	Standard query 0xc2b5 A sp2.baidu.com
272	2.310811	202.120.224.26	10.222.193.82	DNS	302	Standard query response 0xc2b5 A sp2.baidu.com CNAME www.a.shifen.com A 182.61.200.6 A 182.61.200.7 NS ns1.a.s...

> Frame 30: 73 bytes on wire (584 bits), 73 bytes captured (584 bits) on interface 0  
> 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)

0000 c0 bf c0 b9 98 0d 7c 67 a2 b6 a9 d1 00 00 45 00 .....[g]-----E-  
0010 00 3b 70 91 00 00 40 11 93 5d 8a de c1 52 ca 78 ;p---[g]-]---R-x  
0020 e0 1a fd 2e 00 35 00 27 e4 90 ea e6 01 00 00 01 ....S'-----  
0030 00 00 00 00 00 00 03 77 77 77 05 62 61 69 64 75 .....a ww-baidu  
0040 03 63 6f 6d 00 00 01 00 01 .....com.....

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

No.	Time	Source	Destination	Protocol	Length	Info
30	0.650922	10.222.193.82	202.120.224.26	DNS	73	Standard query 0xea66 A www.baidu.com
31	0.654519	202.120.224.26	10.222.193.82	DNS	302	Standard query response 0xea66 A www.baidu.com CNAME www.a.shifen.com A 182.61.200.7 A 182.61.200.6 NS ns4.a.s...
188	1.227789	10.222.193.82	202.120.224.26	DNS	73	Standard query 0xb844 A sp1.baidu.com
189	1.230689	202.120.224.26	10.222.193.82	DNS	302	Standard query response 0xb844 A sp1.baidu.com CNAME www.a.shifen.com A 182.61.200.6 A 182.61.200.7 NS ns2.a.s...
271	2.307799	10.222.193.82	202.120.224.26	DNS	73	Standard query 0xc2b5 A sp2.baidu.com
272	2.310811	202.120.224.26	10.222.193.82	DNS	302	Standard query response 0xc2b5 A sp2.baidu.com CNAME www.a.shifen.com A 182.61.200.6 A 182.61.200.7 NS ns1.a.s...

> Frame 31: 302 bytes on wire (2416 bits), 302 bytes captured (2416 bits) on interface 0  
> Ethernet II, Src: HuaweiTe\_b9:98:0d (c0:bf:c0:b9:98:0d), Dst: IntelCor\_b6:a9:d1 (7c:67:a2:b6:a9:d1)  
> Internet Protocol Version 4, Src: 202.120.224.26, Dst: 10.222.193.82  
> User Datagram Protocol, Src Port: 53, Dst Port: 64814  
> Domain Name System (response)

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”?

```

  Queries
  www.baidu.com: type A, class IN
    Name: www.baidu.com
    [Name Length: 13]
    [Label Count: 3]
    Type: A (Host Address) (1)
    Class: IN (0x0001)
    [Response In: 31]

  Domain Name System (query)
    Transaction ID: 0xae6
    > Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0

```

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?

```

> Flags: 0x8180 Standard query response, No error
Questions: 1
Answer RRs: 3
Authority RRs: 5
Additional RRs: 5
Queries
Answers
  www.baidu.com: type CNAME, class IN, cname www.a.shifen.com
  www.a.shifen.com: type A, class IN, addr 182.61.200.7
  www.a.shifen.com: type A, class IN, addr 182.61.200.6

```

DNS response message 包含了 3 个 answers。

```

  www.baidu.com: type CNAME, class IN, cname www.a.shifen.com
    Name: www.baidu.com
    Type: CNAME (Canonical NAME for an alias) (5)
    Class: IN (0x0001)
    Time to live: 1091
    Data length: 15
    CNAME: www.a.shifen.com
  www.a.shifen.com: type A, class IN, addr 182.61.200.7
    Name: www.a.shifen.com
    Type: A (Host Address) (1)
    Class: IN (0x0001)
    Time to live: 106
    Data length: 4
    Address: 182.61.200.7
  www.a.shifen.com: type A, class IN, addr 182.61.200.6
    Name: www.a.shifen.com
    Type: A (Host Address) (1)
    Class: IN (0x0001)
    Time to live: 106
    Data length: 4
    Address: 182.61.200.6

```

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