

实验一：Wireshark 的使用以及分析 DNS 协议

学号：16307130194, 姓名：陈中钰

1 问题 1

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

1.1 用 nslookup 查询 Web 服务器的 IP 地址

使用 nslookup 查询 www.fudan.edu.cn 的 IP 地址，结果如 Figure 1 所示。其中，第一次查询没有指定 DNS 服务器，因此默认使用的是本地的 DNS 服务器，查询结果为“非权威应答”；而第二次查询时指定了 DNS 服务器为 ns.fudan.edu.cn，查询结果为“权威应答”。

```
C:\Users\ECHOES>nslookup www.fudan.edu.cn
服务器: ns-cx1.online.sh.cn
Address: 116.228.111.18

非权威应答:
名称: www.fudan.edu.cn
Addresses: 2001:da8:8001:2::115
           202.120.224.115

C:\Users\ECHOES>nslookup www.fudan.edu.cn ns.fudan.edu.cn
服务器: ns.fudan.edu.cn
Address: 202.120.224.26

名称: www.fudan.edu.cn
Addresses: 2001:da8:8001:2::115
           202.120.224.115
```

Figure 1: 用 nslookup 查询 Web 服务器的 IP 地址的结果

1.2 nslookup 查询原理

nslookup 指令可以输入两个参数，一个是想要查询的域名，另一个是 DNS 服务器，如果没有提供 DNS 服务器，则默认使用本地的 DNS 服务器。

nslookup 查询时，首先客户机先向 DNS 服务器发出连接查询请求，请求成功后，输出 DNS 服务器的域名和地址。第二步，客户机向 DNS 服务器请求获取目标域名的信息，如果 DNS 服务器没有实际存储目标域名的信息，该 DNS 服务器会通过迭代查询或递归查询的方式从实际存储该域名信息的 DNS 服务器中获取对应的域名信息，把结果反馈给客户机，这种回答属于“非权威应答”。同时，DNS 服务器会把目标域名的信息缓存一段时间，当又有客户

机从同一个 DNS 服务器请求该域名解析时，该 DNS 服务器直接从自身缓存中提取结果，并返回给客户机，这种回答也是“非权威应答”。如果接收请求的 DNS 服务器实际存储了目标域名的信息，则会把对应信息返回给客户机，这种回答是“权威应答”。

1.3 结果分析

如 Figure 1 所示，第一次查询时没有指定 DNS 服务器，因此默认使用的是本地 DNS 服务器 ns-cx1.online.sh.cn，其地址为 116.228.111.18，由于该 DNS 服务器并没有实际存储目标域名的信息，需要向其他 DNS 服务器查询，或者从自身缓存中获得域名信息，因此结果为“非权威应答”。

第二次查询时，指定了复旦大学的公开 DNS 服务器 ns.fudan.edu.cn，因此使用的是该 DNS 服务器，地址为 202.120.224.26，并向该 DNS 服务器查询目标域名信息。由于该 DNS 服务器实际存储了目标域名信息，直接返回结果，而且是“权威应答”。

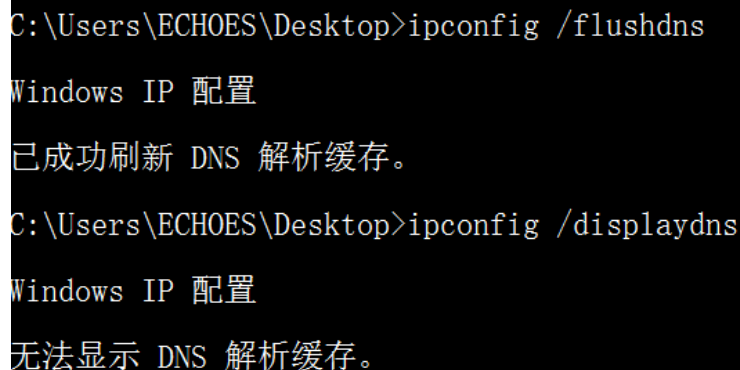
可以看到两次查询目标域名 www.fudan.edu.cn 的 IP 地址，结果都是 2001:da8:8001:2::115 和 202.120.224.115，前者为 IPv6 地址，后者为 IPv4 地址。

2 问题 2

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

2.1 清除本机 DNS 缓存

如 Figure 2 所示，输入 `ipconfig /flushdns` 清除本机的 DNS 缓存，接着用 `ipconfig /displaydns` 显示本机缓存的 DNS 记录，确认 DNS 缓存已被清空。



```
C:\Users\ECHOES\Desktop>ipconfig /flushdns

Windows IP 配置

已成功刷新 DNS 解析缓存。

C:\Users\ECHOES\Desktop>ipconfig /displaydns

Windows IP 配置

无法显示 DNS 解析缓存。
```

Figure 2: 清除本机 DNS 缓存

2.2 查看 WLAN 的 IP 地址

输入 `ipconfig`，查看 WLAN 信息，如 Figure 3 所示，可知 WLAN 的 IP 地址为 192.168.1.108，由于当前连接的网络为 WLAN，因此该 IP 地址就是本机 IP 地址。

2.3 捕获分组

打开 Wireshark，由于当前连接的网络为 WLAN，则选择要捕获的网络为 WLAN。在显示过滤器中输入 `ip.addr == 192.168.1.108`，该 IP 地址为上述查询获得的 WLAN 的 IP 地址。点击开始捕获分组按钮，打开 Edge 浏览器访问 www.baidu.com，在网页加载完后点击停止捕获分组按钮。

```
无线局域网适配器 WLAN:

连接特定的 DNS 后缀 . . . . . : DHCP HOST
本地链接 IPv6 地址. . . . . : fe80::b9e4:e950:ff39:a706%12
IPv4 地址 . . . . . : 192.168.1.108
子网掩码 . . . . . : 255.255.255.0
默认网关. . . . . : 192.168.1.1
```

Figure 3: 查看 WLAN 的 IP 地址

2.4 捕获结果

从封包列表中查找 Protocol 为 DNS、Source 为上述本机 IP 地址、Info 中含有 Standard query 以及 www.baidu.com 字段的封包。最终找到 No. 7 封包符合要求，如 Figure 4 所示，这就是 DNS query message。

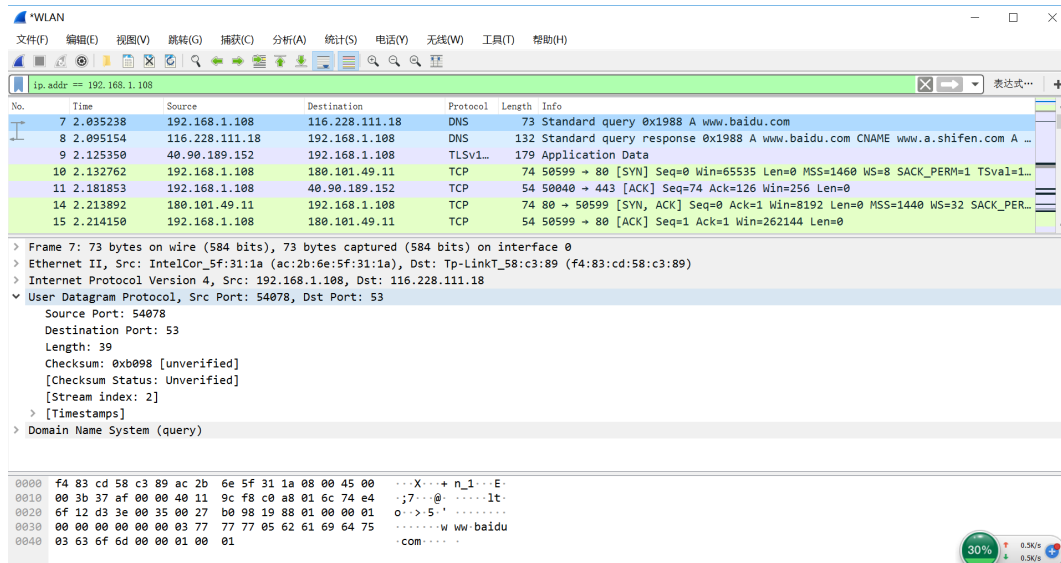


Figure 4: DNS query message

同样，从封包列表中查找 Protocol 为 DNS、Destination 为上述本机 IP 地址、Info 中含有 Standard query response 以及 www.baidu.com 字段的封包。最终找到 No. 8 封包符合要求，如 Figure 5 所示，这就是 DNS response message。

2.5 发送方式

查看找到的 DNS query message 的封包详细信息，如 Figure 4 所示，可以看到 User Datagram Protocol 字段，说明该 DNS query message 是通过 UDP 发送的。

同样，如 Figure 5 所示，DNS response message 的封包详细信息中也可以看到 User Datagram Protocol 字段，说明该 DNS response message 也是通过 UDP 发送的。

3 问题 3

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

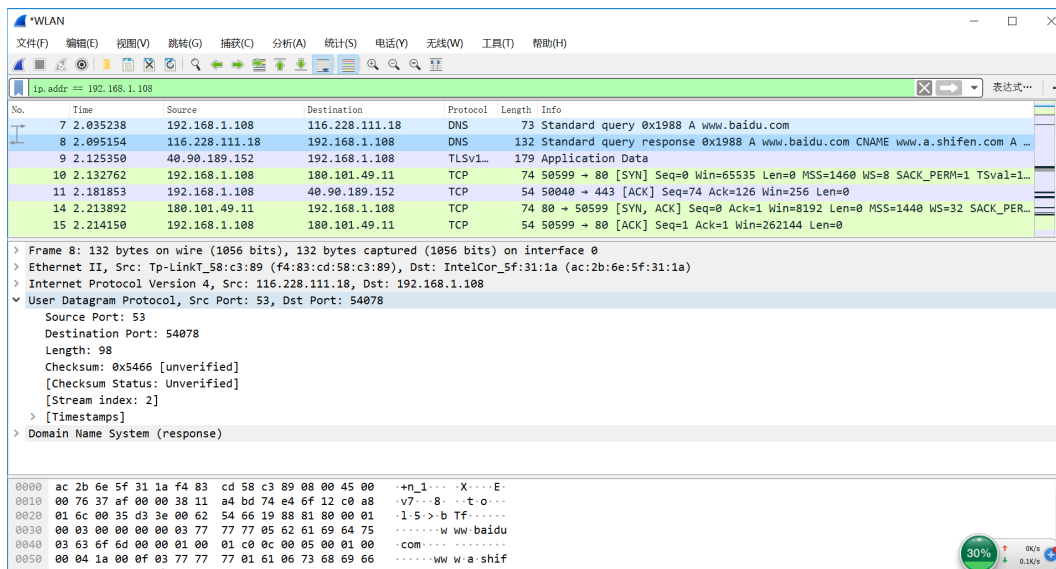


Figure 5: DNS response message

3.1 端口信息

查看 DNS query message 的封包详细信息，如 Figure 4 所示，在 User Datagram Protocol 字段旁边可以看到 Src Port 和 Dst Port。可以看到，DNS query message 的 destination port 为 53。

同样，查看 DNS response message 的封包详细信息，如 Figure 5 所示，在 User Datagram Protocol 字段旁边可以看到，DNS response message 的 source port 为 53。

分析可得，DNS query message 从 WLAN 发送到本地 DNS 服务器，而 DNS response message 刚好相反，是从本地 DNS 服务器发送到 WLAN。因此，DNS query message 的 source IP 和 port 跟 DNS response message 的 destination IP 和 port 是一样的，都是 WLAN 的 IP 和 port。同样，DNS query message 的 destination IP 和 port 跟 DNS response message 的 source IP 和 port 也是一样的，都是本地 DNS 服务器的 IP 和 port。

4 问题 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?

4.1 DNS query message 接收方的 IP 地址

查看 DNS query message 的封包，如 Figure 4 所示，可以看到封包的 destination 的 IP 地址为 116.228.111.18，这就是 DNS query message 被发送到的 IP 地址。

4.2 本地 DNS 服务器的 IP 地址

使用 ipconfig 查询不到本地 DNS 服务器的 IP 地址，但使用 ipconfig /all 就可以查到了，如 Figure 6 所示，本地 DNS 服务器的 IP 地址为 116.228.111.18。可以发现，上述两个 IP 地址是相同的。

5 问题 5

Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers” ?

```

无线局域网适配器 WLAN:

    连接特定的 DNS 后缀 . . . . . : DHCP HOST
    描述. . . . . : Intel(R) Dual Band Wireless-AC 3165
    物理地址. . . . . : AC-2B-6E-5F-31-1A
    DHCP 已启用 . . . . . : 是
    自动配置已启用. . . . . : 是
    本地链接 IPv6 地址. . . . . : fe80::b9e4:e950:ff39:a706%12(首选)
    IPv4 地址 . . . . . : 192.168.1.108(首选)
    子网掩码 . . . . . : 255.255.255.0
    获得租约的时间 . . . . . : 2019年10月11日 0:45:27
    租约过期的时间 . . . . . : 2019年10月11日 2:45:16
    默认网关. . . . . : 192.168.1.1
    DHCP 服务器 . . . . . : 192.168.1.1
    DHCPv6 IAID . . . . . : 44837742
    DHCPv6 客户端 DUID . . . . . : 00-01-00-01-20-12-6D-66-54-AB-3A-A0-D6-5C
    DNS 服务器 . . . . . : 116.228.111.18
                           180.168.255.118
    TCP/IP 上的 NetBIOS . . . . . : 已启用

```

Figure 6: 本地 DNS 服务器的 IP 地址

5.1 DNS query message 的 DNS 详细信息

浏览 DNS query message 的封包详细信息，其中包含了 DNS 的详细信息，如 Figure 7 所示。

```

▼ Domain Name System (query)
    Transaction ID: 0x1988
    > Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
    ▼ 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)
\[Response In: 8\]

```

Figure 7: DNS query message 的 DNS 详细信息

5.2 DNS query message 的 DNS 详细信息的分析

如 Figure 7 所示，在 Queries 栏中可以看到 www.baidu.com: type A 的字段，说明该 DNS query 是 type A 的。另外，Answer RRs: 0 说明该 query 不包含任何 answer。

6 问题 6

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

6.1 DNS response message 的 DNS 详细信息

同样，浏览 DNS response message 的封包详细信息，其中包含了 DNS 的详细信息，如 Figure 8 所示。

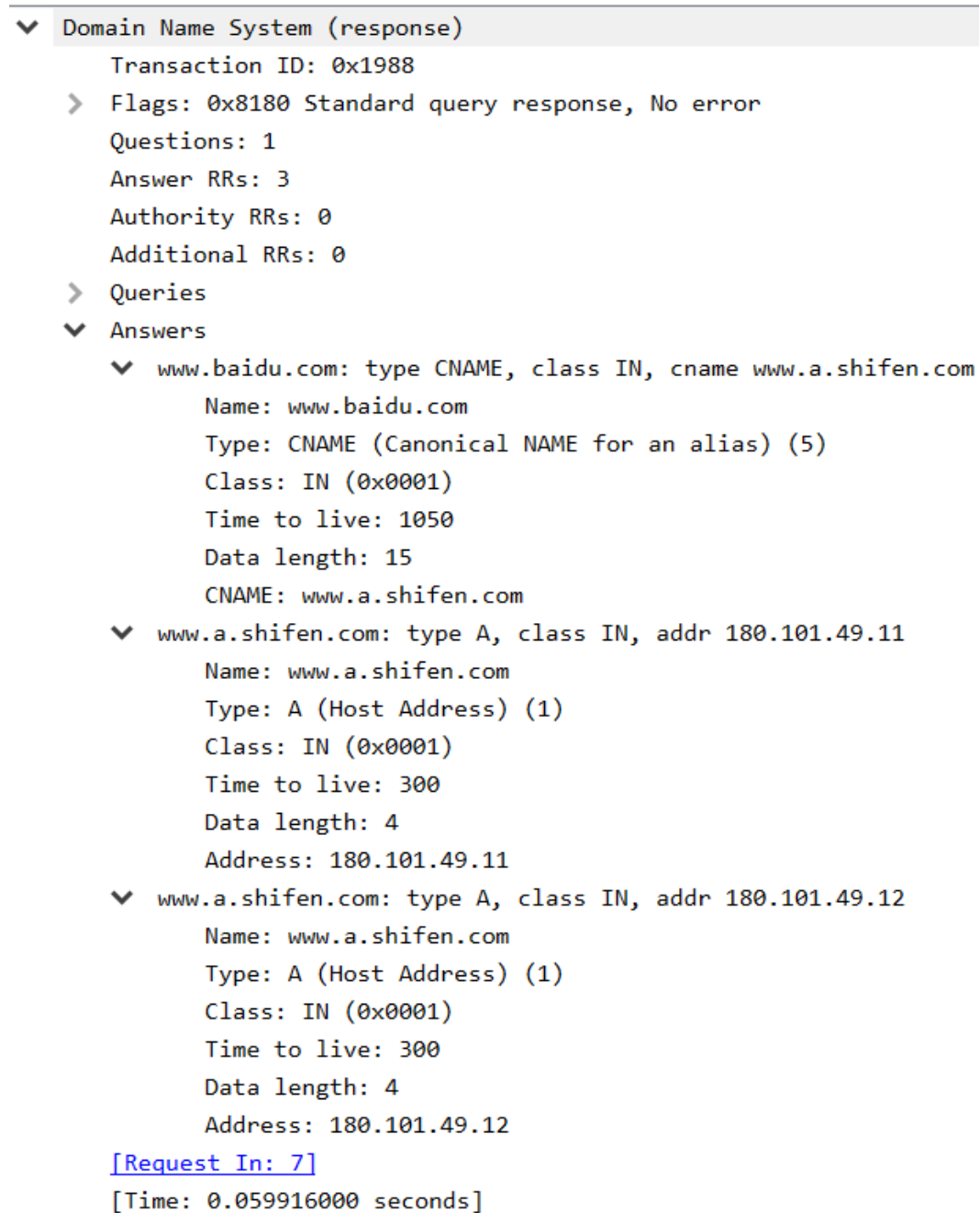


Figure 8: DNS response message 的 DNS 详细信息

6.2 DNS response message 的 DNS 详细信息的分析

其中，Answer RRs: 3 说明该 response 提供了 3 个 answer。查看 Answers 栏，展开里面的 3 个 answer，如 Figure 8 所示，可以发现，每个 answer 中都包含了：Name（域名）、Type（类型）、Class（类别）、Time to live（缓存时间）、Data length（数据长度）、Address（IP 地址）。