

重庆邮电大学

学生实验实习报告册

学年学期： 2018-2019 学年 ☐春☒秋学期

课程名称： 计算机网络

学生学院： 软件工程学院

专业班级： 13001603班

学生学号： 2016214052

学生姓名： 姜文泽

联系电话： 17783101834

重庆邮电大学教务处制

实验二：IP 层协议分析

一、实验目的

1. 了解 ICMP、IP 数据包的格式；
2. 理解 ARP 命令、PING 命令与 ARP、ICMP 协议的关系；
3. 熟悉 ARP 和 ICMP 协议包格式；
4. 了解 ARP、ICMP 会话过程。

二、实验内容

通过命令行中的 ARP 命令和 PING 命令理解 ARP 和 ICMP 协议。

三、实验环境

操作系统：Windows 10 专业版 1803

工具软件：Wireshark 2.6.4

浏览器软件：Google Chrome

网络环境：

无线局域网适配器 WLAN：

连接特定的 DNS 后缀 :

IPv6 地址 : 2408:84f6:8000:3e9b:3079:5439:d245:e240

临时 IPv6 地址. : 2408:84f6:8000:3e9b:6cb2:b358:2f6b:fa4c

本地链接 IPv6 地址. : fe80::3079:5439:d245:e240%9

IPv4 地址 : 192.168.43.106

子网掩码 : 255.255.255.0

默认网关. : fe80::36d7:12ff:fea2:21c%9

192.168.43.1

四、实验步骤

1. 实验过程

- (1) 以管理员身份启动命令提示符 (cmd)；
- (2) 输入 `arp -d *` 以清除自己电脑中 MAC 和 IP 映射表；

```
管理员: 命令提示符
Microsoft Windows [版本 10.0.17134.407]
(c) 2018 Microsoft Corporation. 保留所有权利。

C:\Windows\system32>arp -a

接口: 192.168.43.106 --- 0x9
Internet 地址      物理地址      类型
192.168.43.1      34-d7-12-a2-02-1c 动态
224.0.0.22        01-00-5e-00-00-16 静态
224.0.0.251       01-00-5e-00-00-fb 静态
224.0.0.252       01-00-5e-00-00-fc 静态
239.255.255.250   01-00-5e-7f-ff-fa 静态
255.255.255.255   ff-ff-ff-ff-ff-ff 静态

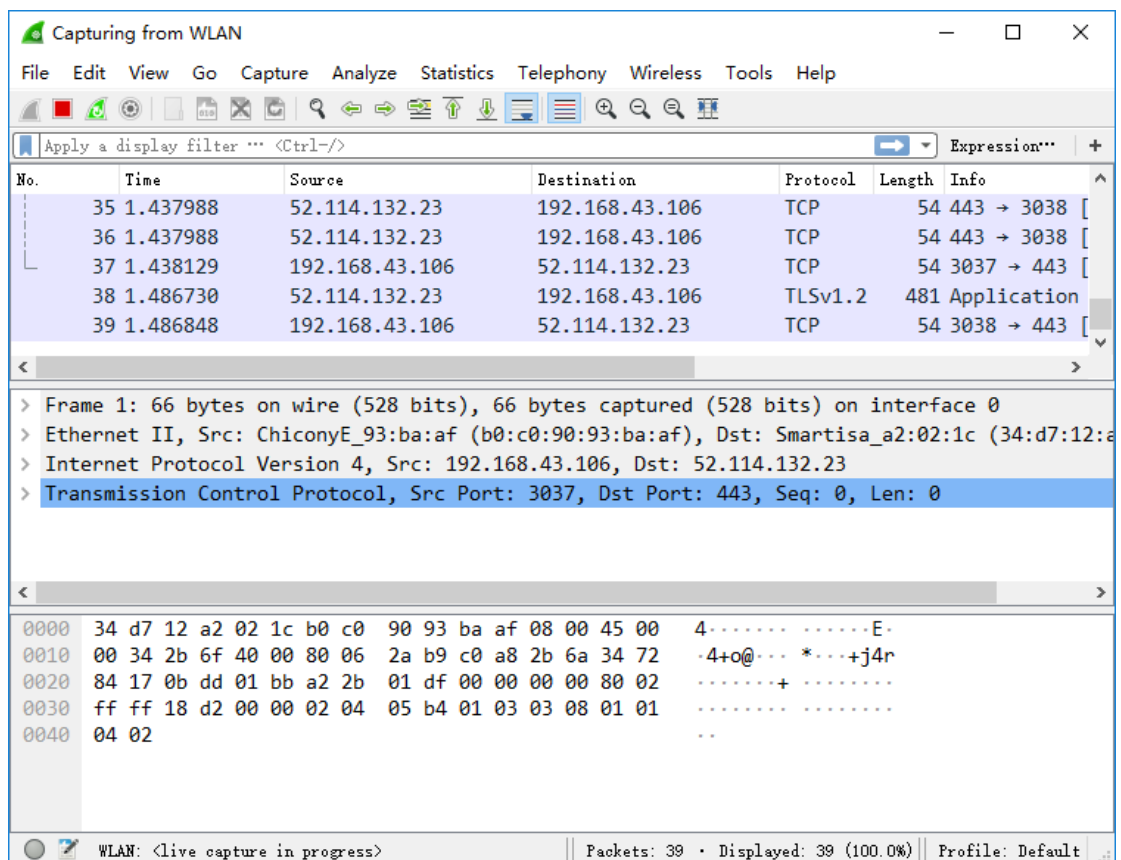
C:\Windows\system32>arp -d *

C:\Windows\system32>arp -a

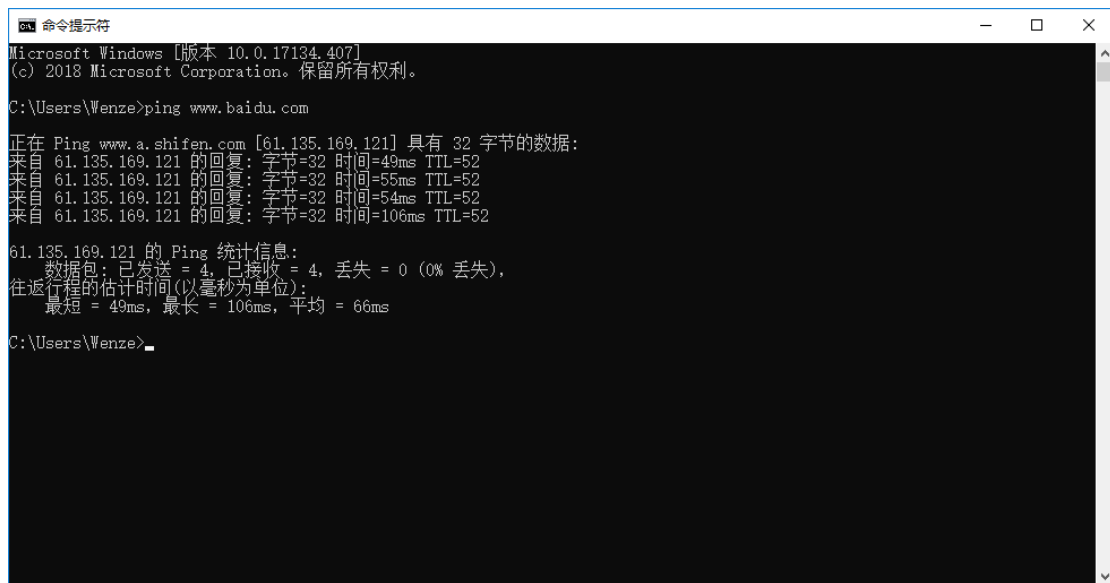
接口: 192.168.43.106 --- 0x9
Internet 地址      物理地址      类型
192.168.43.1      34-d7-12-a2-02-1c 动态
224.0.0.22        01-00-5e-00-00-16 静态
255.255.255.255   ff-ff-ff-ff-ff-ff 静态

C:\Windows\system32>
```

(3) 启动 Wireshark, 开始捕获分组;



(4) 在 MS DOS 下键入 ping www.baidu.com, 见图所示;



```
命令提示符
Microsoft Windows [版本 10.0.17134.407]
(c) 2018 Microsoft Corporation。保留所有权利。

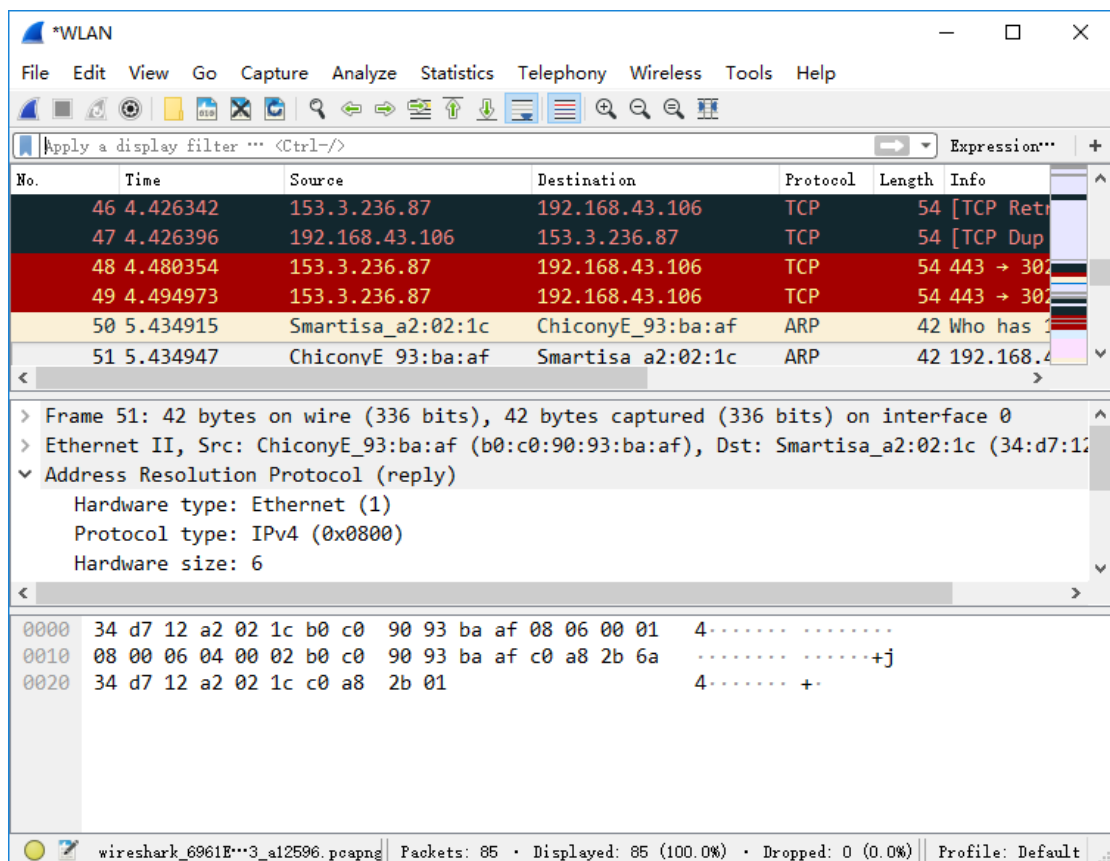
C:\Users\Wenze>ping www.baidu.com

正在 Ping www.a.shifen.com [61.135.169.121] 具有 32 字节的数据:
来自 61.135.169.121 的回复: 字节=32 时间=49ms TTL=52
来自 61.135.169.121 的回复: 字节=32 时间=55ms TTL=52
来自 61.135.169.121 的回复: 字节=32 时间=54ms TTL=52
来自 61.135.169.121 的回复: 字节=32 时间=106ms TTL=52

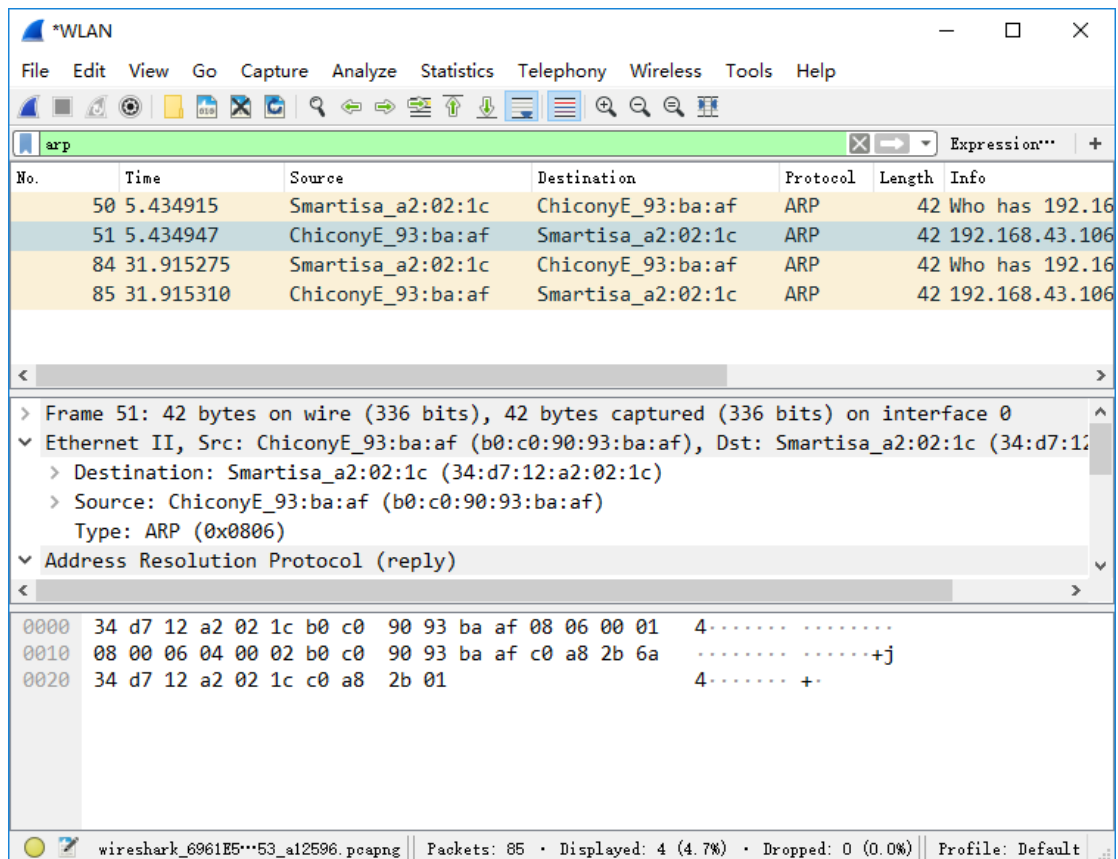
61.135.169.121 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
    往返行程的估计时间(以毫秒为单位):
        最短 = 49ms, 最长 = 106ms, 平均 = 66ms

C:\Users\Wenze>
```

(5) 回到 Wireshark 并停止抓包;



(6) 查找到 ARP 请求和应答数据包，回答实验报告内容中的 1-2 题；



Wireshark packet capture window showing ARP traffic. The filter is 'arp'. The packet list shows four packets:

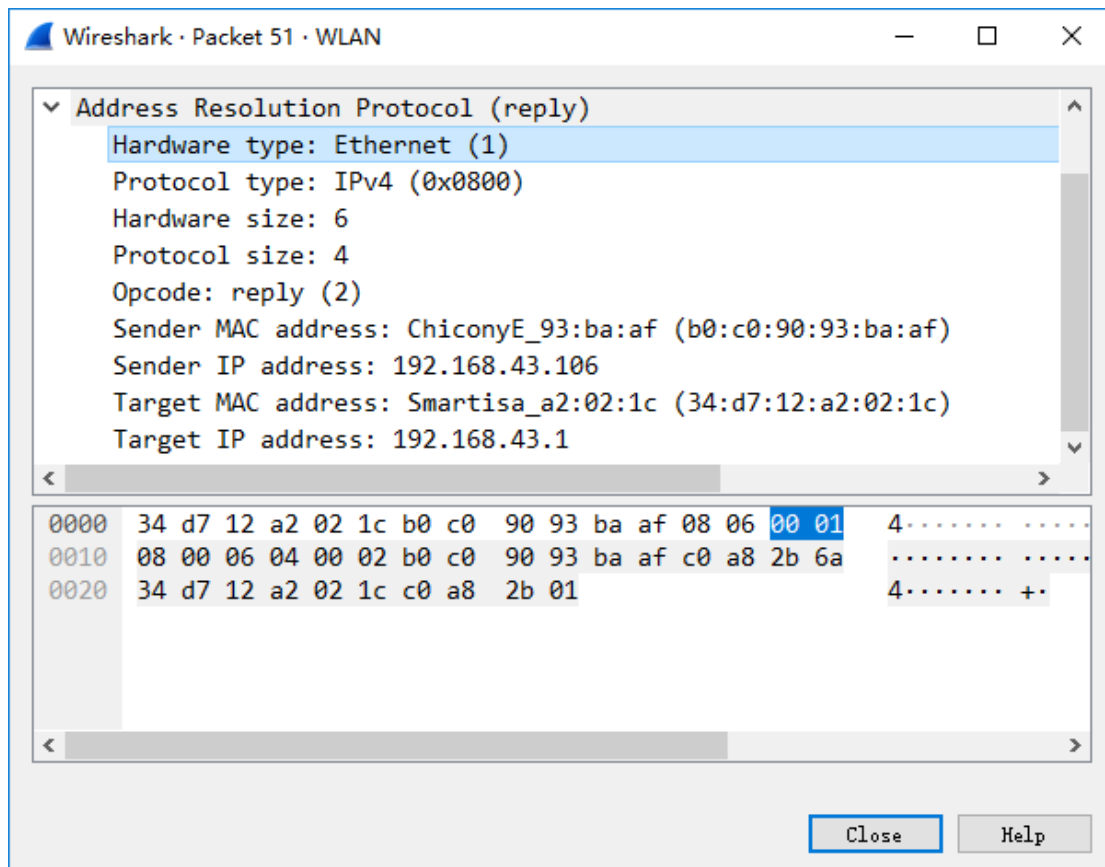
No.	Time	Source	Destination	Protocol	Length	Info
50	5.434915	Smartisa_a2:02:1c	ChiconyE_93:ba:af	ARP	42	Who has 192.168.43.106
51	5.434947	ChiconyE_93:ba:af	Smartisa_a2:02:1c	ARP	42	192.168.43.106
84	31.915275	Smartisa_a2:02:1c	ChiconyE_93:ba:af	ARP	42	Who has 192.168.43.106
85	31.915310	ChiconyE_93:ba:af	Smartisa_a2:02:1c	ARP	42	192.168.43.106

Packet 51 details:

- Frame 51: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface 0
- Ethernet II, Src: ChiconyE_93:ba:af (b0:c0:90:93:ba:af), Dst: Smartisa_a2:02:1c (34:d7:12:a2:02:1c)
 - Destination: Smartisa_a2:02:1c (34:d7:12:a2:02:1c)
 - Source: ChiconyE_93:ba:af (b0:c0:90:93:ba:af)
 - Type: ARP (0x0806)
- Address Resolution Protocol (reply)

Packet bytes:

```
0000 34 d7 12 a2 02 1c b0 c0 90 93 ba af 08 06 00 01 4.....
0010 08 00 06 04 00 02 b0 c0 90 93 ba af c0 a8 2b 6a .....+j
0020 34 d7 12 a2 02 1c c0 a8 2b 01 4.....+
```

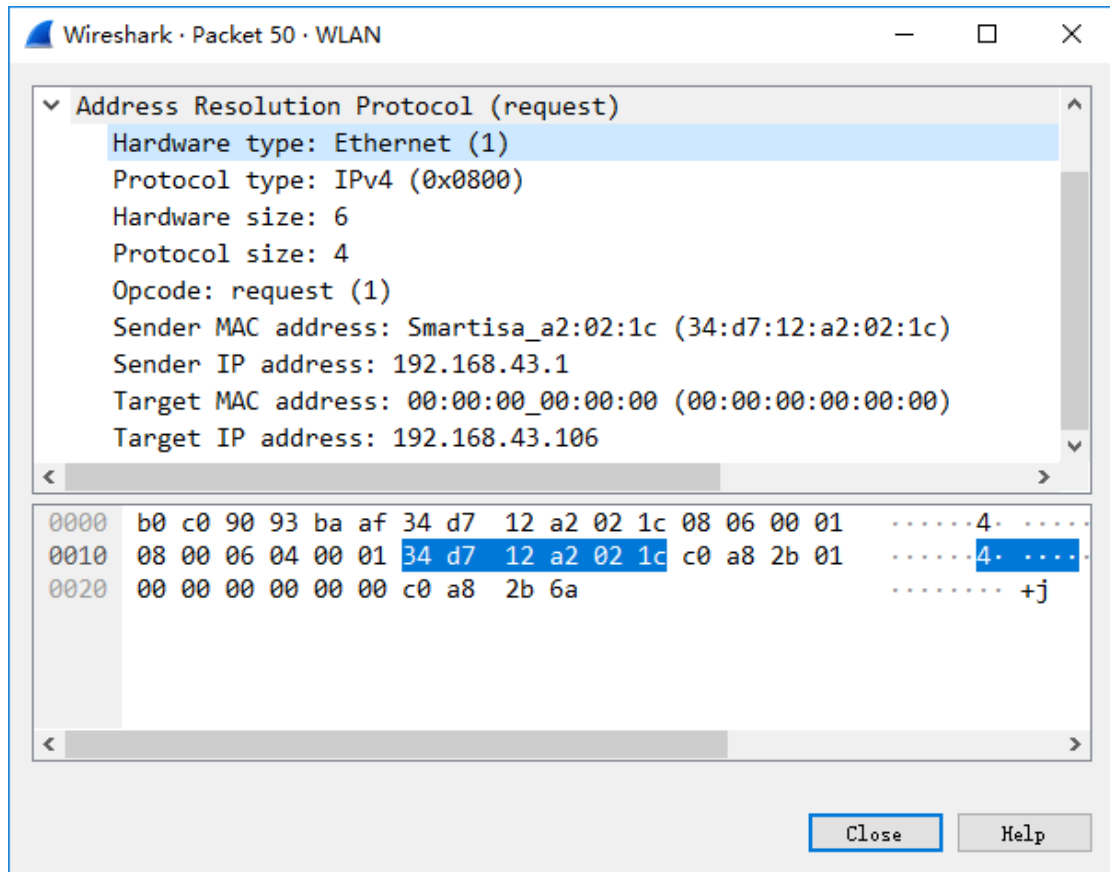


Wireshark packet details window for packet 51, showing the ARP (reply) details:

- Address Resolution Protocol (reply)
 - Hardware type: Ethernet (1)
 - Protocol type: IPv4 (0x0800)
 - Hardware size: 6
 - Protocol size: 4
 - Opcode: reply (2)
 - Sender MAC address: ChiconyE_93:ba:af (b0:c0:90:93:ba:af)
 - Sender IP address: 192.168.43.106
 - Target MAC address: Smartisa_a2:02:1c (34:d7:12:a2:02:1c)
 - Target IP address: 192.168.43.1

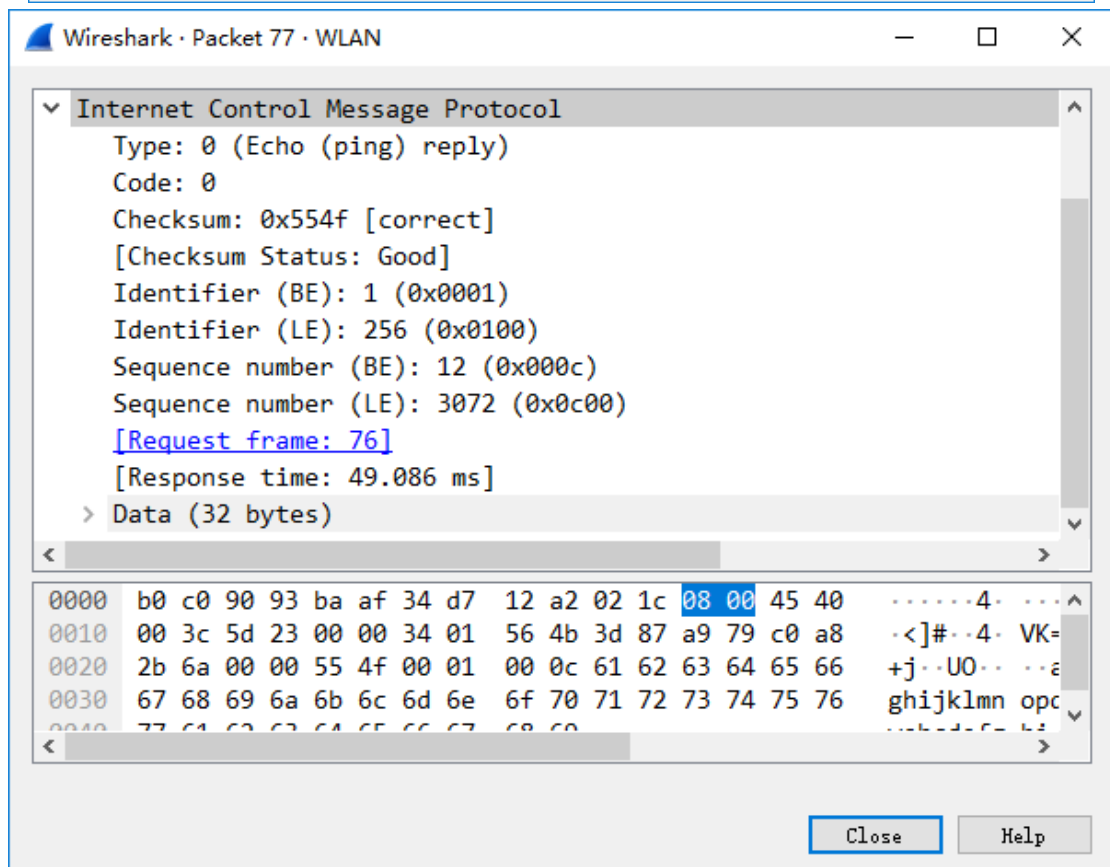
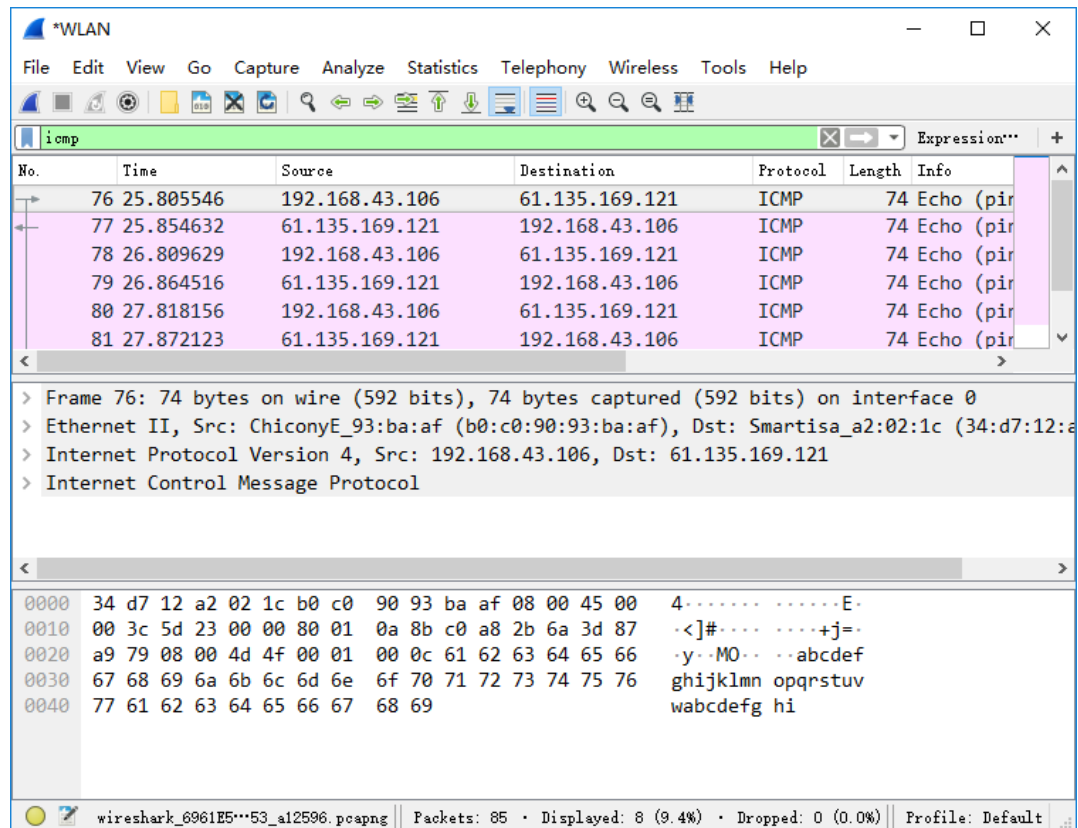
Packet bytes:

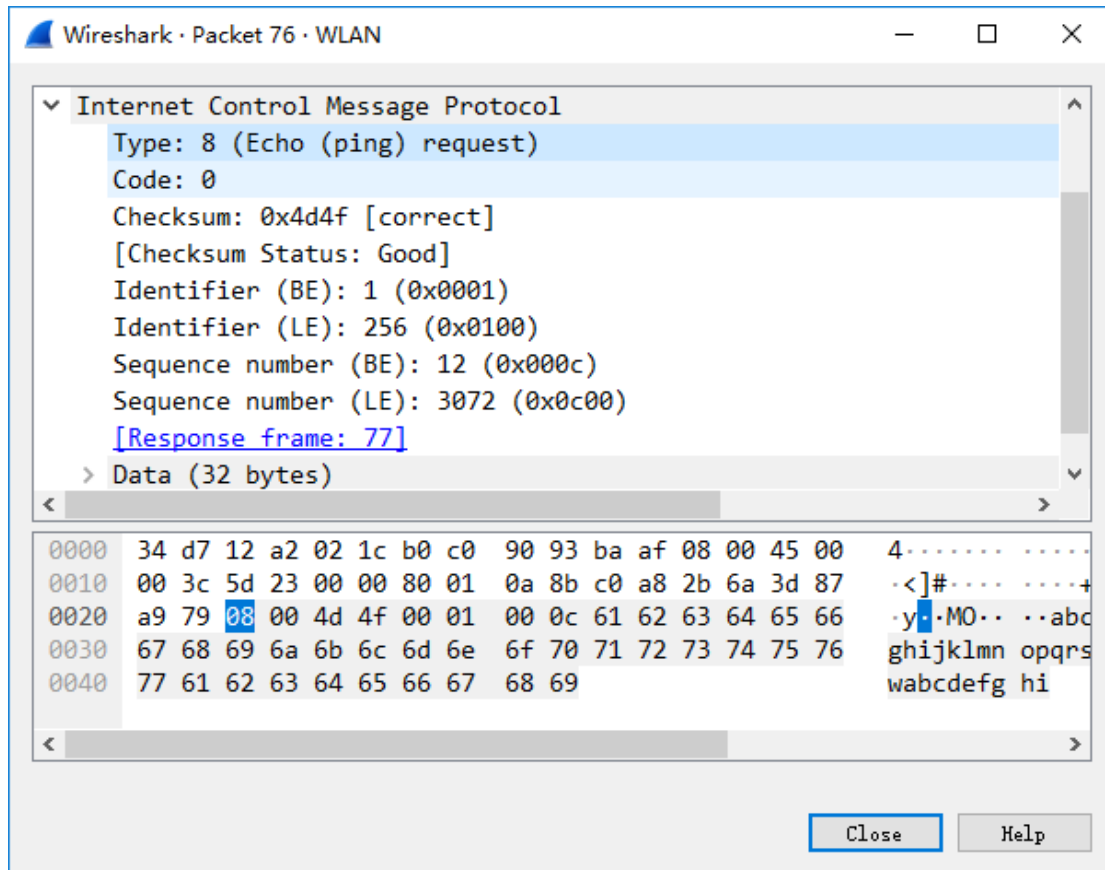
```
0000 34 d7 12 a2 02 1c b0 c0 90 93 ba af 08 06 00 01 4.....
0010 08 00 06 04 00 02 b0 c0 90 93 ba af c0 a8 2b 6a .....
0020 34 d7 12 a2 02 1c c0 a8 2b 01 4.....+
```



- 该部分第一张图为筛选过 arp 的数据包，共有 4 个，两个一组，构成请求和应答数据包；
- 第二张图为 arp 的 reply 包，其中数据部分为 Sender MAC/IP 和 Target MAC/IP，即发送方和接收方的 MAC 和 IP 地址；
- 第三张图为 arp 的 request 包，其中数据部分为 Sender MAC/IP 和 Target MAC/IP，即发送方和接收方的 MAC 和 IP 地址，发送方和接收方的对象和 reply 包中的相反，即 request 的发送方变为 reply 的接收方，request 的接收方变为 reply 的发送方。

- (7) 查到 PING 命令执行时, 产生的 ICMP 请求和应答报文, 回答实验报告内容中的 3 题。





- 该部分第一张图为筛选过 icmp 的数据包，两个一组，构成请求和应答数据包；

2. 实验结果

(1) 什么是 ARP? ARP 与 IP 的关系。

ARP 全称 Address Resolution Protocol，即地址解析协议，是在仅知道主机的 IP 地址时确地址解析协议定其物理地址的一种协议。

在 TCP/IP 协议中，A 给 B 发送 IP 包，在报头中需要填写 B 的 IP 为目标地址，但这个 IP 包在以太网上传输的时候，还需要进行一次以太包的封装，在这个以太包中，目标地址就是 B 的 MAC 地址。即本实验中的 reply 包的发送方和接收方。

计算机 A 是如何得知 B 的 MAC 地址的呢？解决问题的关键就在于 ARP 协议。

在 A 不知道 B 的 MAC 地址的情况下，A 就广播一个 ARP 请求包，（即该实验中 ARP 部分第一张图的 Who has...），请求包中填有 B 的 IP (192. 168. 43. 1)，

以太网中的所有计算机都会接收这个请求，而正常的情况下只有 B 会给出 ARP 应答包，包中就填充上了 B 的 MAC 地址，并回复给 A。（此为该实验的 request 包）

A 得到 ARP 应答后，将 B 的 MAC 地址放入本机缓存，便于下次使用。（可以通过 `arp -a` 查看）

本机 MAC 缓存是有生存期的，生存期结束后，将再次重复上面的过程。也可手动通过 `arp -d *` 来清除。

综上，ARP 协议可以实现任意网络层地址到任意物理地址的转换，例如 IP 地址转换为 MAC 地址。所以网络层知道了对方的 IP 地址，并且想要发送数据，那么就需要通过 ARP 请求找到对应的 MAC 地址。

(2) ARP 请求和应答数据包的数据部分的内容是什么？代表什么意思？

在本实验中，请求数据包中的数据部分为：

```
Sender MAC address: ChiconyE_93:ba:af (b0:c0:90:93:ba:af)
Sender IP address: 192.168.43.106
Target MAC address: Smartisa_a2:02:1c (34:d7:12:a2:02:1c)
Target IP address: 192.168.43.1
```

应答数据包中的数据部分为：

```
Sender MAC address: Smartisa_a2:02:1c (34:d7:12:a2:02:1c)
Sender IP address: 192.168.43.1
Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
Target IP address: 192.168.43.106
```

皆为发送端 IP 地址和 MAC 地址和目的 IP 地址和 MAC 地址

(3) 什么是 ICMP？ICMP 与 IP 的关系。

ICMP 是控制报文协议，他是 TCP/IP 协议族的一个子协议，用于在 IP 主机，路由器之间传递控制消息。当 ping 命令执行时，会向其服务器传递消息（4 次）。

五、实验结论

收获 1. ARP 协议可以实现任意网络层地址到任意物理地址的转换，例如 IP 地址转换为 MAC 地址。

收获 2. 本机 MAC 缓存是有生存期的，生存期结束后，将再次重复上面的过程。也可手动通过 `arp -d *` 来清除。