

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

实验一：802.3 协议分析和以太网

一、实验目的

1. 分析 802.3 协议；
2. 熟悉以太网帧的格式；
3. 熟悉 ARP 报文的格式。

二、实验内容

通过练习使用分组分析器 Wireshark 来分析协议。

Wireshark 是一种可以运行在 Windows, UNIX, Linux 等操作系统上的分组分析器。

Wireshark 的界面主要有五个组成部分：

1. 命令菜单 (command menus)：命令菜单位于窗口的最顶部，是标准的下拉式菜单。最常用菜单命令有两个：File、Capture。File 菜单允许你保存捕获的分组数据或打开一个已被保存的捕获分组数据文件或退出 Wireshark 程序。Capture 菜单允许你开始捕获分组。
2. 捕获分组列表 (listing of captured packets)：按行显示已被捕获的分组内容，其中包括：Wireshark 赋予的分组序号、捕获时间、分组的源地址和目的地址、协议类型、分组中所包含的协议说明信息。单击某一列的列名，可以使分组按指定列进行排序。在该列表中，所显示的协议类型是发送或接收分组的最高层协议的类型。
3. 分组头部明细 (details of selected packet header)：显示捕获分组列表窗口中被选中分组的头部详细信息。包括：与以太网帧有关的信息，与包含在该分组中的 IP 数据报有关的信息。单击以太网帧或 IP 数据报所在行左边的向右或向下的箭头可以展开或最小化相关信息。另外，如果利用 TCP 或 UDP 承载分组，Wireshark 也会显示 TCP 或 UDP 协议头部信息。最后，分组最高层协议的头部字段也会显示在此窗口中。
4. 分组内容窗口 (packet content)：以 ASCII 码和十六进制两种格式显示被捕获帧的完整内容。
5. 显示筛选规则 (display filter specification)：在该字段中，可以填写协议的名称或其他信息，根据此内容可以对分组列表窗口中的分组进行过滤。

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:

以太网适配器 以太网:

连接特定的 DNS 后缀 : cqupt.edu.cn

本地链接 IPv6 地址. : fe80::2c7f:943c:931b:d417%22

IPv4 地址 : 172.18.109.83

子网掩码 : 255.255.252.0

默认网关. : 172.18.108.1

PPP 适配器 Netkeeper:

连接特定的 DNS 后缀 :

IPv4 地址 : 113.251.216.160

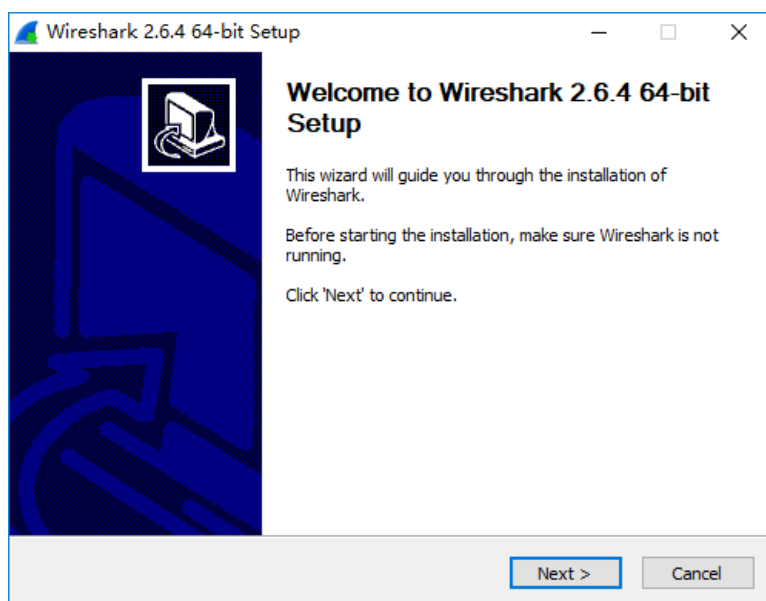
子网掩码 : 255.255.255.255

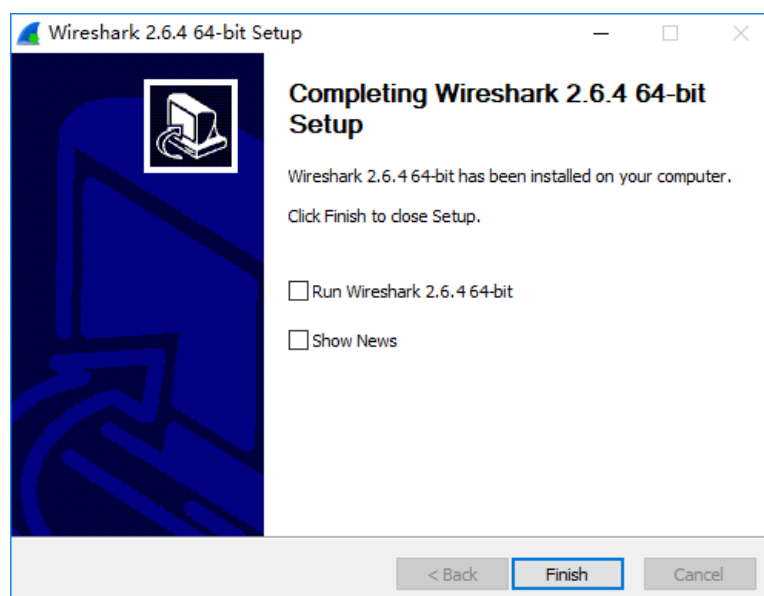
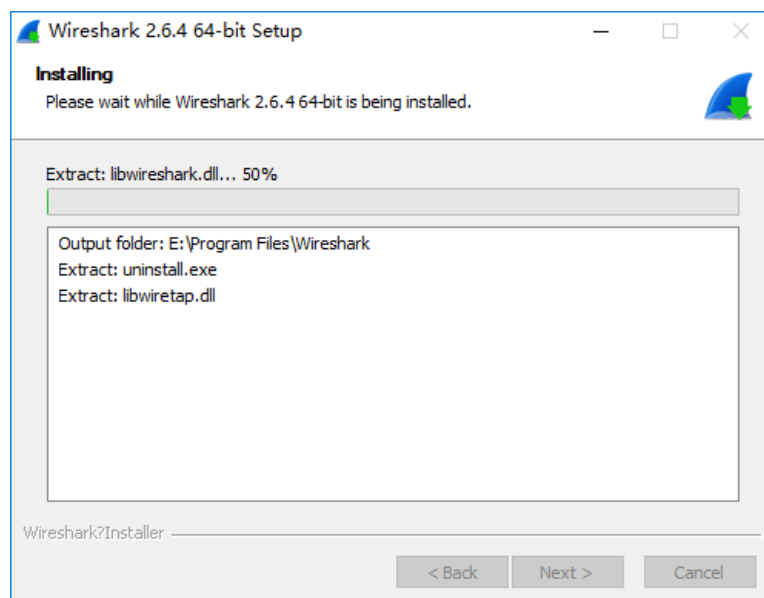
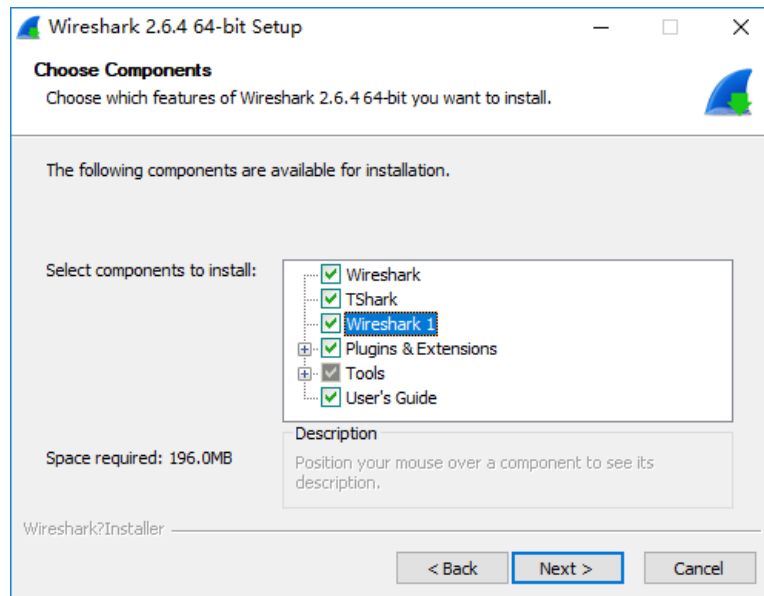
默认网关. : 0.0.0.0

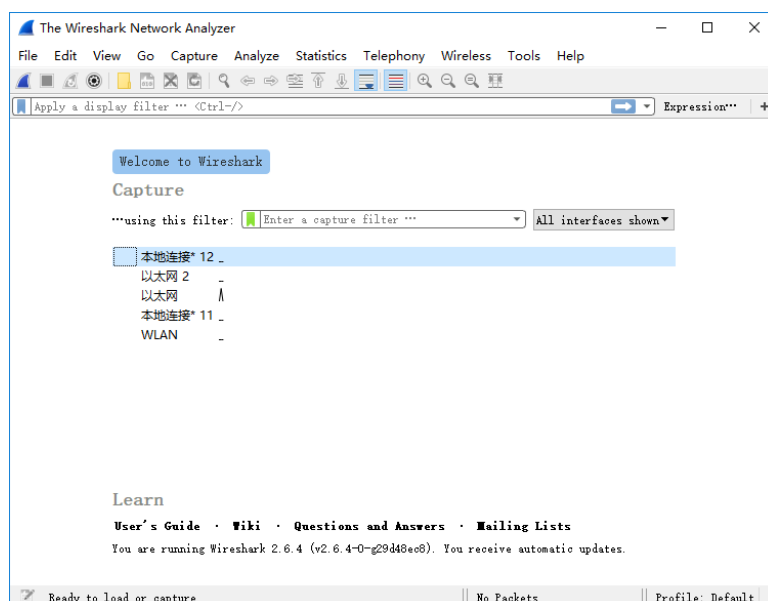
四、实验步骤

1. 安装 Wireshark

本次实验 Wireshark 使用的是 2.6.4 英文版本。安装过程及软件开始界面如下:

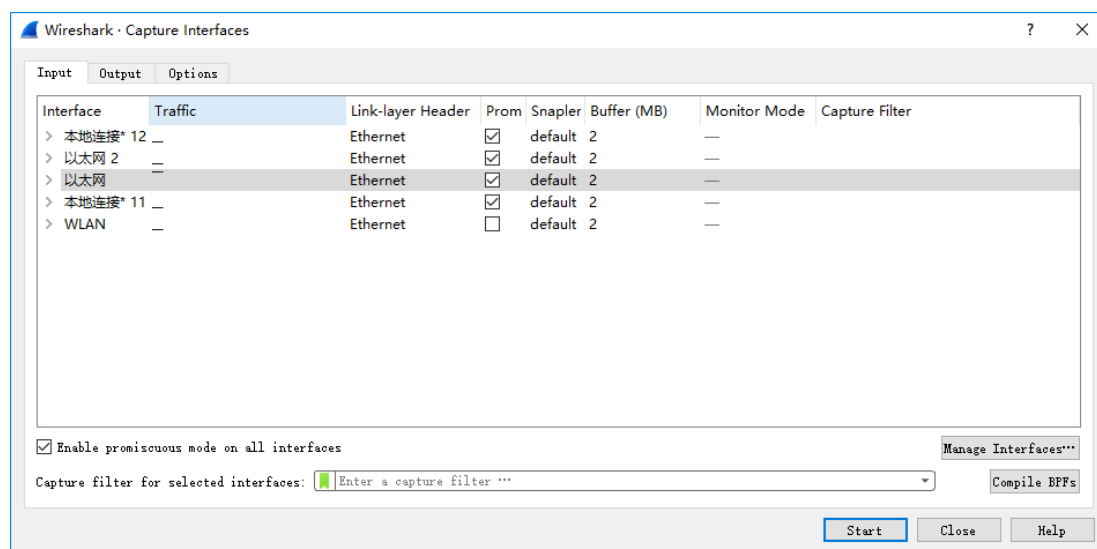






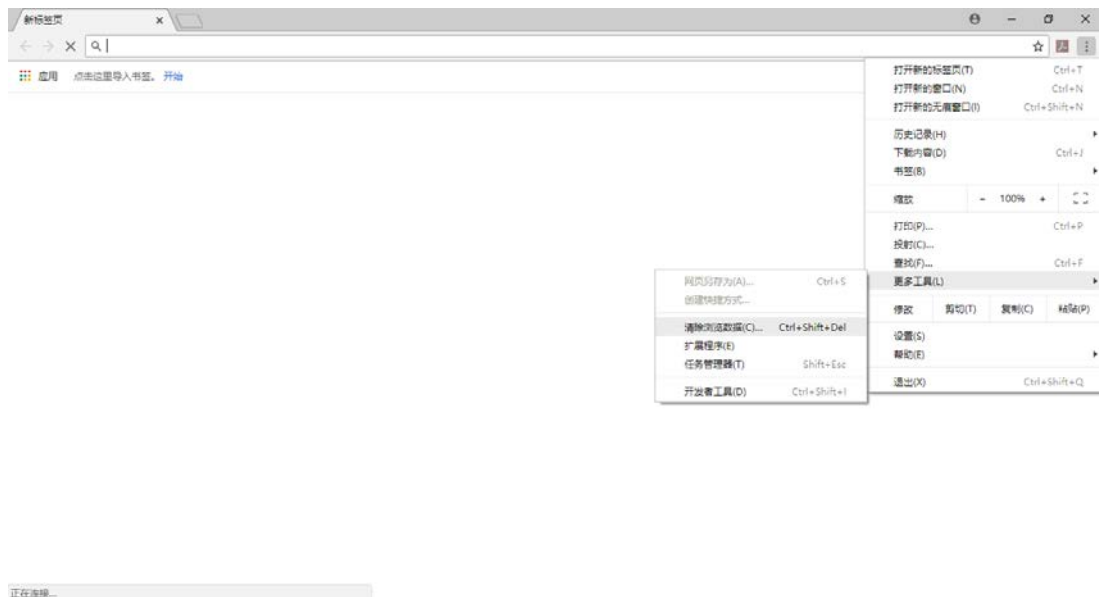
2. 使用 Wireshark

启动界面后，点击命令菜单中的“Options”命令，可进行分组捕获设置。设置完成后即可点击 Start 开始进行分组捕获。

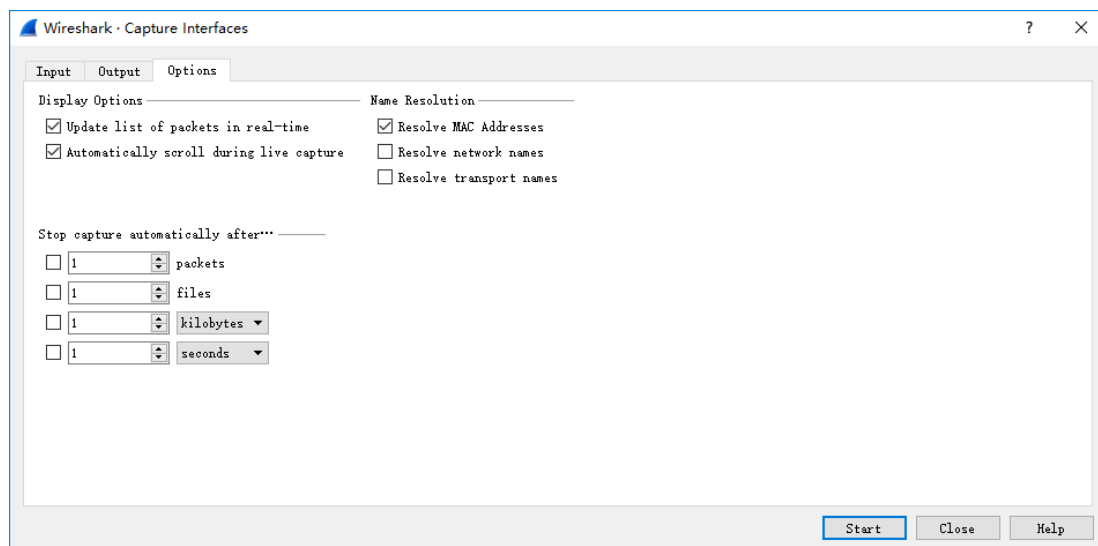


3. 使用 Wireshark 捕获并分析以太网帧

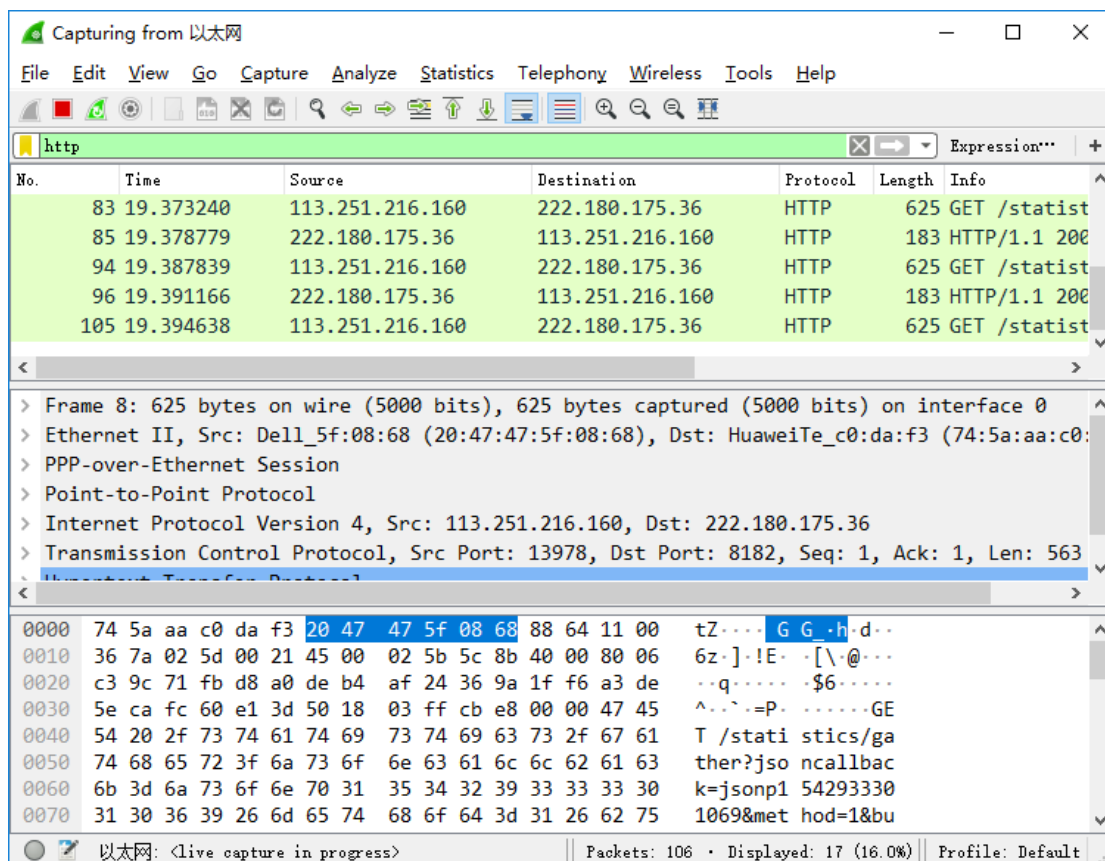
- (1) 清空浏览器缓存（在 IE 窗口中，选择“工具/Internet 选项/删除文件”命令）；



- (2) 启动 Wireshark，开始分组捕获；
- (3) 启动主机上的 Chrome 浏览器。
- (4) 启动 Wireshark。窗口中没有任何分组列表。
- (5) 开始分组捕获：选择“capture”下拉菜单中的“Options”命令，会出现如图所示的“Wireshark: Capture Options”窗口，可以设置分组捕获的选项。



- (6) 在实验中,可以使用窗口中显示的默认值。在“Wireshark: Capture Options”窗口的最上面有一个“interface”下拉菜单,其中显示计算机中所安装的网络接口(即网卡)。当计算机具有多个活动网卡(装有多块网卡,并且均正常工作)时,需要选择其中一个用来发送或接收分组的网络接口(如某个有线接口)。
- (7) 随后,单击“Start”开始进行分组捕获,所有由选定网卡发送和接收的分组都将被捕获。
- (8) 开始分组捕获后,会出现分组捕获统计窗口。该窗口统计显示各类已捕获分组的数量。在该窗口中有一个“stop”按钮,可以停止分组的捕获。
- (9) 在运行分组捕获的同时,在 Chrome 浏览器地址栏中输入某网页的 URL,如: www.baidu.com。为显示该网页,浏览器需要连接 www.baidu.com 的服务器,并与之交换 HTTP 消息,以下载该网页。包含这些 HTTP 消息的以太网帧(Frame)将被 Wireshark 捕获。



- (10) Wireshark 主窗口显示已捕获的你的计算机与其他网络实体交换的所有协议报文，其中一部分就是与 www.baidu.com 服务器交换的 HTTP 消息。
- (11) 在显示筛选编辑框中输入“http”，单击“apply”，分组列表窗口将只显示 HTTP 消息。
- (12) 选择分组列表窗口中的第一条 HTTP 消息。它应该是你的计算机发向 www.baidu.com 服务器的 HTTP GET（HTTP 定义的用于获取/查询资源信息的方法）消息。
- (13) 选择“Analyze->Enabled Protocols”，取消对 IP 复选框的选择，单击 OK。当你选择该消息后，以太网帧、IP 数据报、TCP 报文段、以及 HTTP 消息首部信息都将显示在分组首部子窗口中。单击分组首部详细信息子窗口中向右和向下箭头，可以最小化帧、以太网、IP、TCP 信息显示量，可以最大化 HTTP 协议相关信息的显示量。
- (14) 选择包含 HTTP GET 消息的以太网帧，在分组详细信息窗口中，展开 Ethernet II 部分。根据操作，回答“实验报告内容”中的 1-4 题；

以太网

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http

No.	Time	Source	Destination	Protocol	Length	Info
189	3.634495	113.251.216.160	222.180.175.36	HTTP	625	GET /stat
192	3.672987	222.180.175.36	113.251.216.160	HTTP	164	HTTP/1.1
194	3.718544	113.251.216.160	222.180.175.36	HTTP	625	GET /stat
195	3.720958	222.180.175.36	113.251.216.160	HTTP	183	HTTP/1.1
204	3.795824	113.251.216.160	222.180.175.36	HTTP	625	GET /stat

Frame 189: 625 bytes on wire (5000 bits), 625 bytes captured (5000 bits) on interface 0

Ethernet II, Src: Dell_5f:08:68 (20:47:47:5f:08:68), Dst: HuaweiTe_c0:da:f3 (74:5a:aa:c0:da:f3)

PPP-over-Ethernet Session

Point-to-Point Protocol

Internet Protocol Version 4, Src: 113.251.216.160, Dst: 222.180.175.36

Transmission Control Protocol, Src Port: 14097, Dst Port: 8182, Seq: 1, Ack: 1, Len: 563

HTTP Request Method, 3 bytes

Packets: 282 • Displayed: 19 (6.7%) • Dropped: 0 (0.0%) Profile: Default

以太网

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http

No.	Time	Source	Destination	Protocol	Length	Info
189	3.634495	113.251.216.160	222.180.175.36	HTTP	625	GET /stat
192	3.672987	222.180.175.36	113.251.216.160	HTTP	164	HTTP/1.1
194	3.718544	113.251.216.160	222.180.175.36	HTTP	625	GET /stat
195	3.720958	222.180.175.36	113.251.216.160	HTTP	183	HTTP/1.1
204	3.795824	113.251.216.160	222.180.175.36	HTTP	625	GET /stat

Ethernet II, Src: Dell_5f:08:68 (20:47:47:5f:08:68), Dst: HuaweiTe_c0:da:f3 (74:5a:aa:c0:da:f3)

Destination: HuaweiTe_c0:da:f3 (74:5a:aa:c0:da:f3)

Source: Dell_5f:08:68 (20:47:47:5f:08:68)

Type: PPPoE Session (0x8864)

PPP-over-Ethernet Session

Point-to-Point Protocol

Internet Protocol Version 4, Src: 113.251.216.160, Dst: 222.180.175.36

Type (eth.type), 2 bytes

Packets: 282 • Displayed: 19 (6.7%) • Dropped: 0 (0.0%) Profile: Default

(15) 选择包含 HTTP 响应消息第一个字节的以太网帧。

4. 查看主机 ARP 缓存

- (1) 利用 MS-DOS 命令：arp -a 查看主机上 ARP 缓存的内容。

```
命令提示符
220.165.138.61 静态
220.181.57.216 静态
220.181.57.232 静态
220.181.57.233 静态
220.181.90.52 静态
220.181.163.104 静态
220.181.172.34 静态
222.177.4.43 静态
222.177.4.166 静态
222.177.26.6 静态
222.177.26.12 静态
222.177.26.17 静态
222.177.26.61 静态
222.177.26.62 静态
222.180.166.245 静态
222.180.175.36 静态
222.180.175.37 静态
222.184.96.66 静态
222.184.96.68 静态
222.184.96.69 静态
222.184.96.71 静态
222.184.96.72 静态
222.184.96.73 静态
222.184.96.75 静态
222.192.186.85 静态
222.192.186.105 静态
222.192.186.110 静态
224.0.0.22 静态
C:\Users\Wenze>
```

- (2) 利用 MS-DOS 命令：arp -d * 以清除主机中 ARP 缓存的内容。

```
命令提示符
222.177.26.6 静态
222.177.26.12 静态
222.177.26.17 静态
222.177.26.61 静态
222.177.26.62 静态
222.180.166.245 静态
222.180.175.36 静态
222.180.175.37 静态
222.184.96.66 静态
222.184.96.68 静态
222.184.96.69 静态
222.184.96.71 静态
222.184.96.72 静态
222.184.96.73 静态
222.184.96.75 静态
222.192.186.85 静态
222.192.186.105 静态
222.192.186.110 静态
224.0.0.22 静态
C:\Users\Wenze>arp -d *
ARP 项删除失败：请求的操作需要提升。

C:\Users\Wenze>arp -d *
C:\Users\Wenze>arp -a
未找到 ARP 项。
C:\Users\Wenze>
```

5. 实验结果

- (1) 你的主机的 48 位以太网地址 (MAC 地址) 是多少？

20-47-47-5F-08-68

- (2) 目标 MAC 地址是 www.baidu.com 服务器的 MAC 地址吗？如果不是，该地址是什么设备的 MAC 地址？

该地址是连接该服务器的路由器的 MAC 地址 (HuaweiTe_c0:da:f3
(74:5a:aa:c0:da:f3))

(3) 给出 Frame 头部 Type 字段(2 字节)的十六进制值。

0x8864

(4) 在包含“HTTP GET”的以太网帧中,字符“G”的位置(是第几个字节,假设 Frame 头部第一个字节的顺序为 1)?

3F (16 进制) 63 (10 进制)

五、实验结论

收获 1. 在 Wireshark 的抓包细节中,具体字节排序序号是以 16 进制来显示的。
如下图所示。

问题 1. `arp -d *` 删除时报错 ARP 项删除失败: 请求的操作需要提升?

解决 1. 可以使用命令为 `arp -d *`, 也可使用管理员权限打开 cmd 进行执行。

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 *

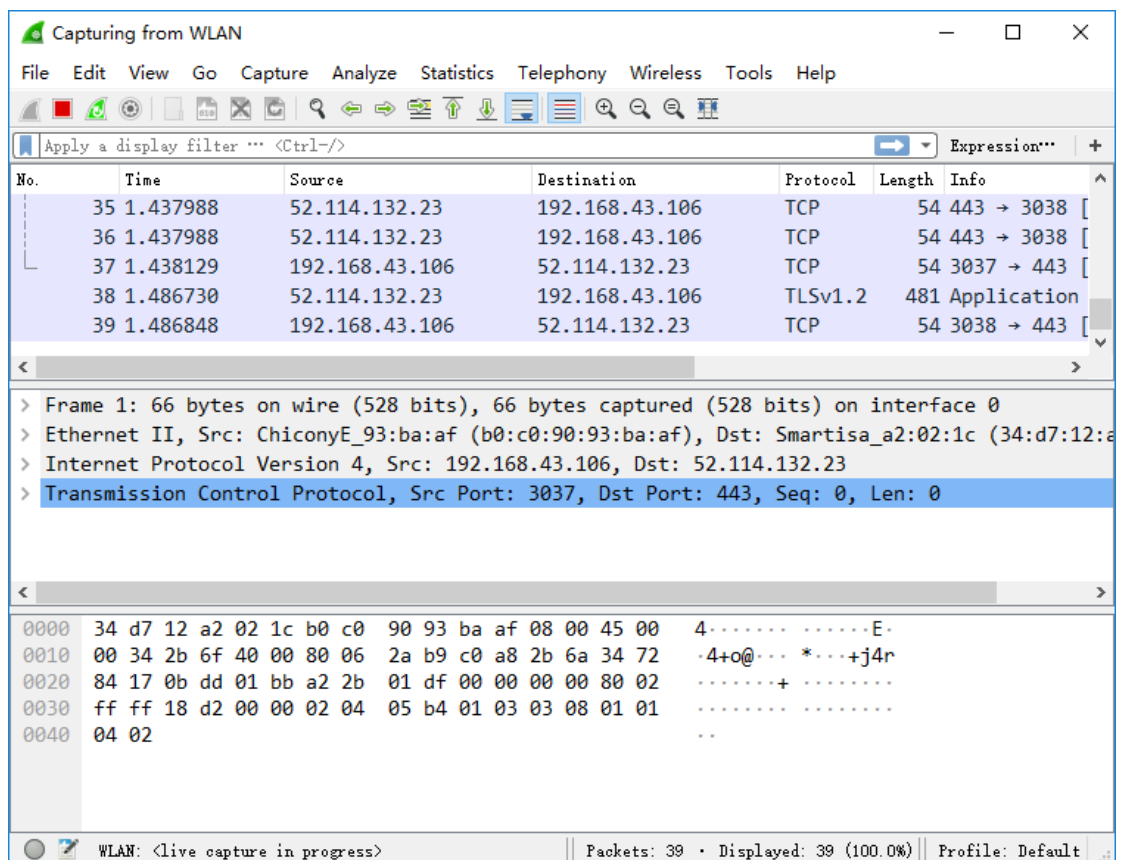
C:\Windows\system32>arp -a

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

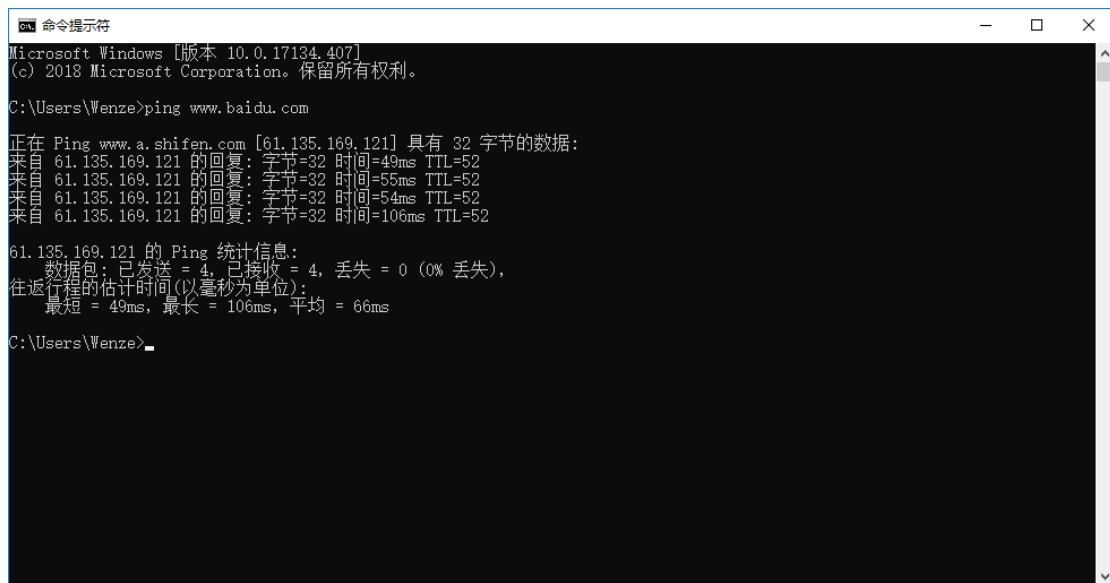
C:\Windows\system32>

```

(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。

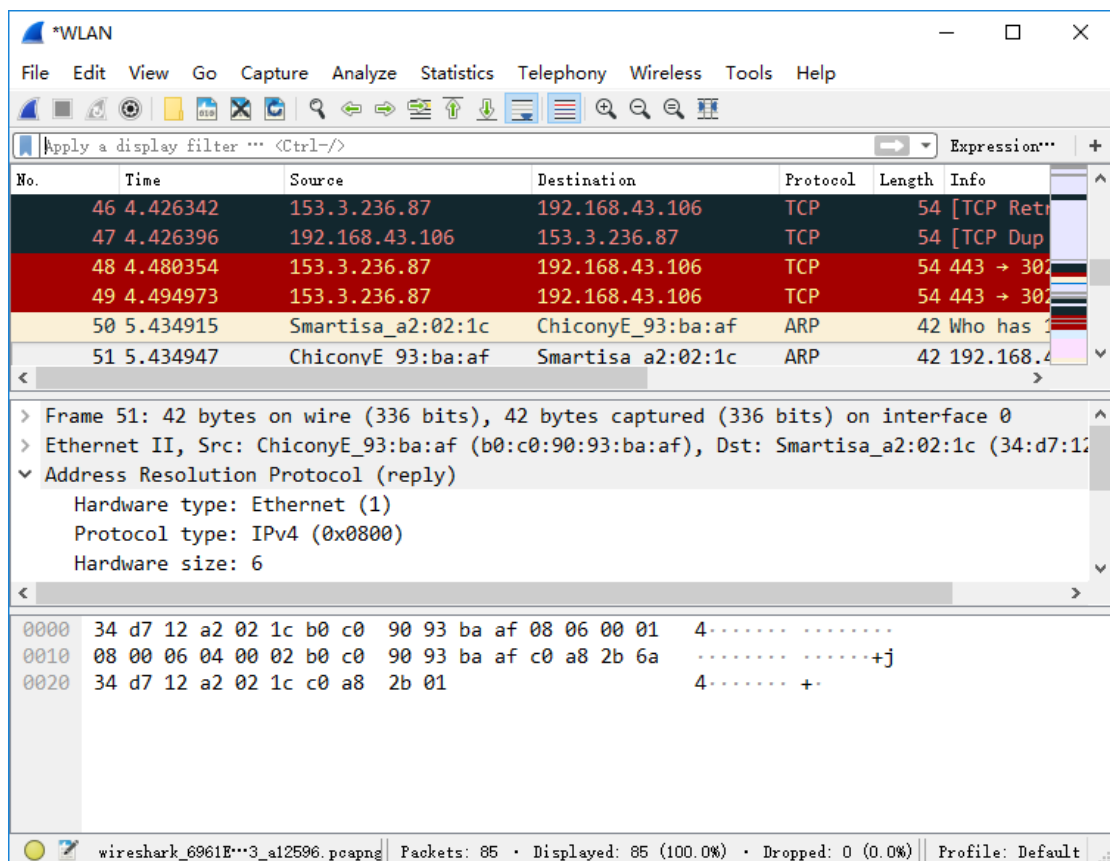
C:\Users\Wenze>ping www.baidu.com

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；

The image displays two screenshots from the Wireshark network protocol analyzer. The top screenshot shows a packet capture on the 'WLAN' interface with a filter set to 'arp'. It lists four packets: packets 50 and 84 are ARP requests from Smartisa_a2:02:1c to ChiconyE_93:ba:af; packets 51 and 85 are ARP replies from ChiconyE_93:ba:af to Smartisa_a2:02:1c. Packet 51 is selected, and its details pane shows it is an 'Address Resolution Protocol (reply)' with hardware type Ethernet, protocol type IPv4, and opcode reply. The packet bytes pane shows the raw data in hexadecimal and ASCII. The bottom screenshot is a zoomed-in view of the details pane for packet 51, highlighting the 'Hardware type: Ethernet (1)' field. The packet bytes pane also shows the raw data for packet 51.

Wireshark - WLAN

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

arp

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

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

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_6961E5...53_a12596.pcapng | Packets: 85 • Displayed: 4 (4.7%) • Dropped: 0 (0.0%) | Profile: Default

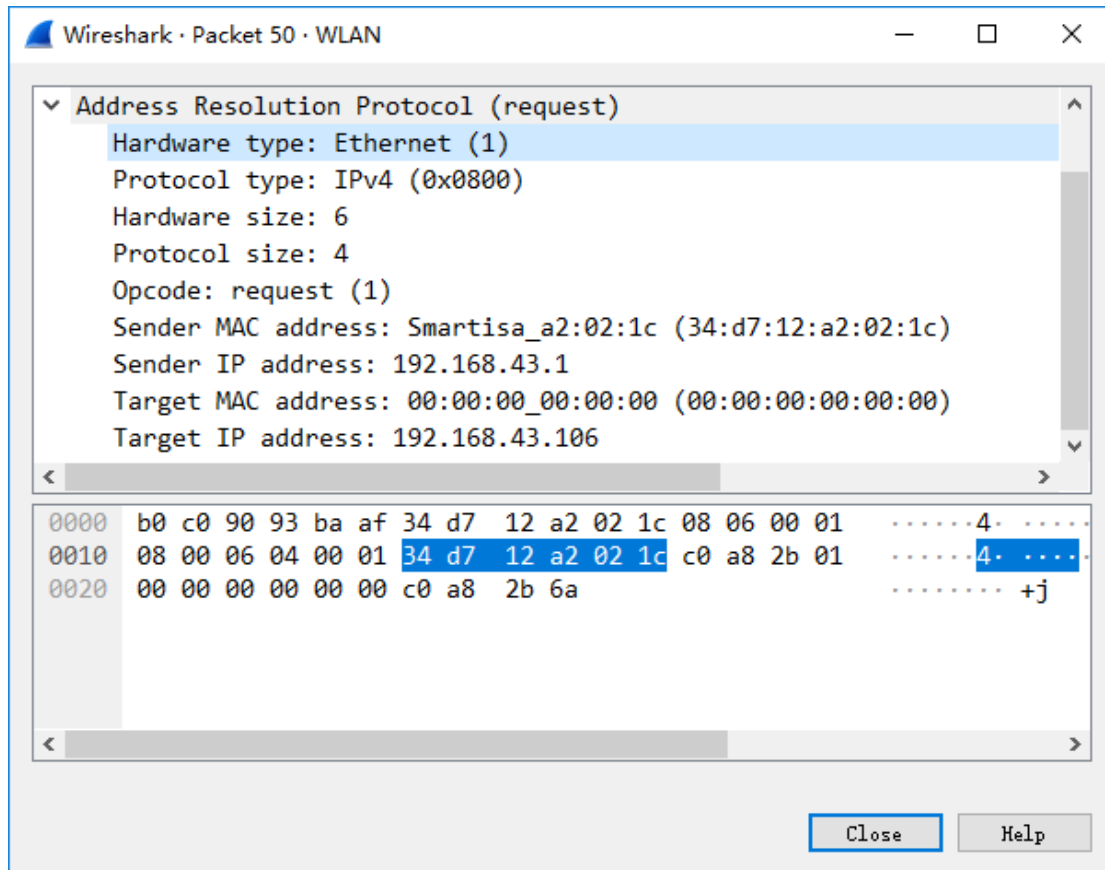
Wireshark - Packet 51 - WLAN

v 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

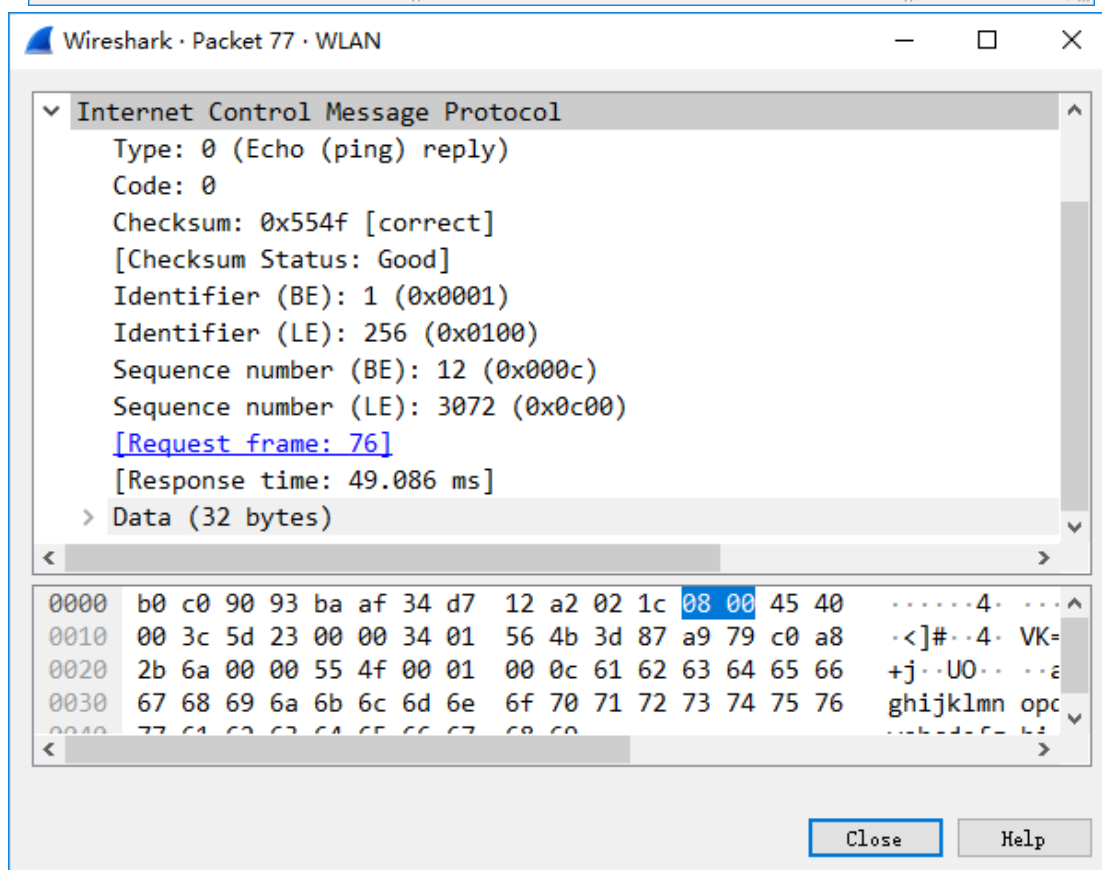
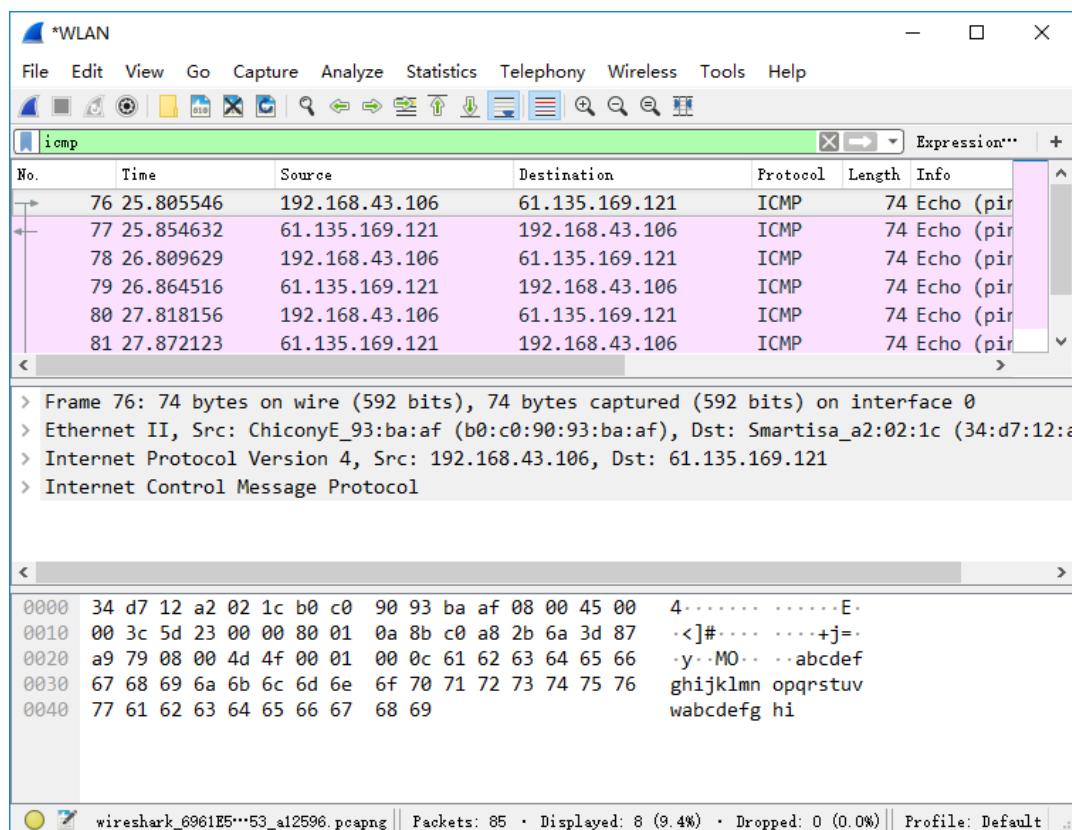
0000 34 d7 12 a2 02 1c b0 c0 90 93 ba af 08 06 00 01 4.....
0010 08 00 06 04 00 02 b0 c0 90 93 ba af c0 a8 2b 6a
0020 34 d7 12 a2 02 1c c0 a8 2b 01 4.....+

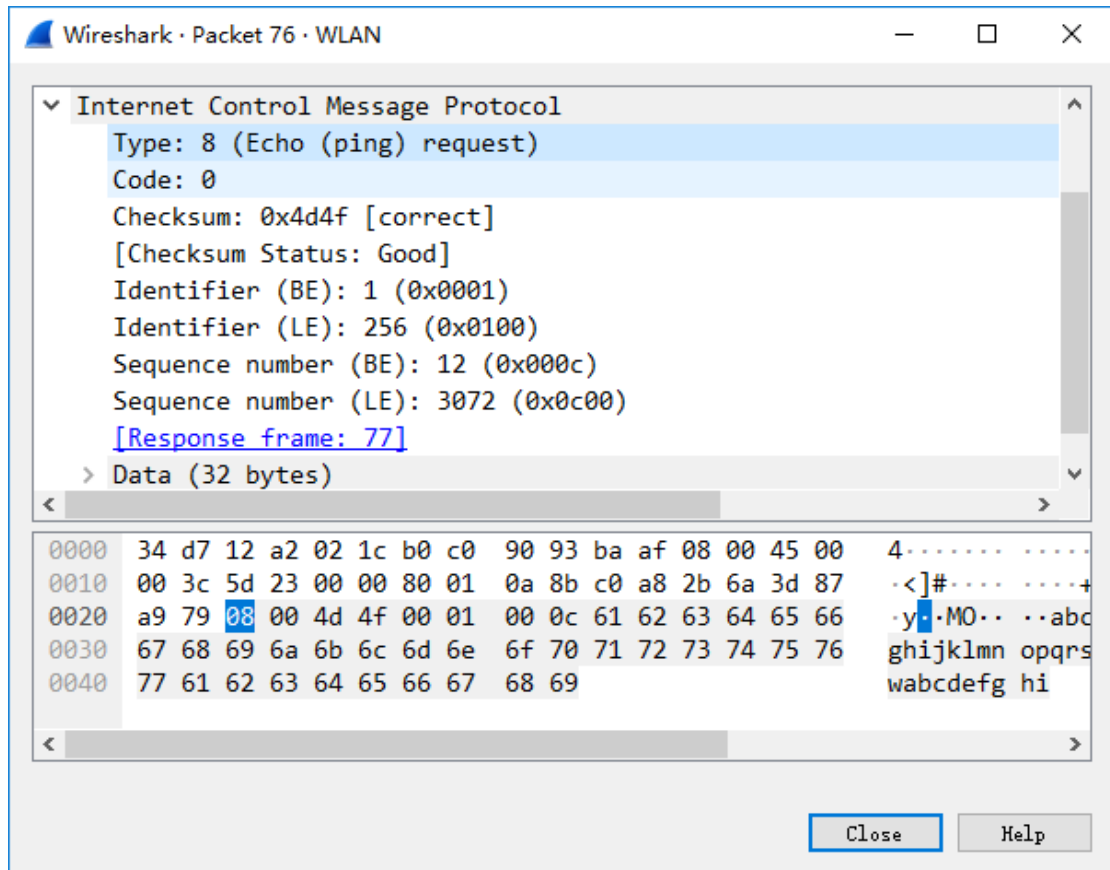
Close Help



- 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 地址时确定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。

实验三：TCP 协议分析

一、实验目的

1. 熟悉 TCP 协议的基本原理；
2. 学会使用 Wireshark 分析 TCP 协议。

二、实验内容

通过 Wireshark 抓包工具分析 TCP/IP 的三次握手。

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 : lan

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

IPv4 地址 : 192.168.199.175

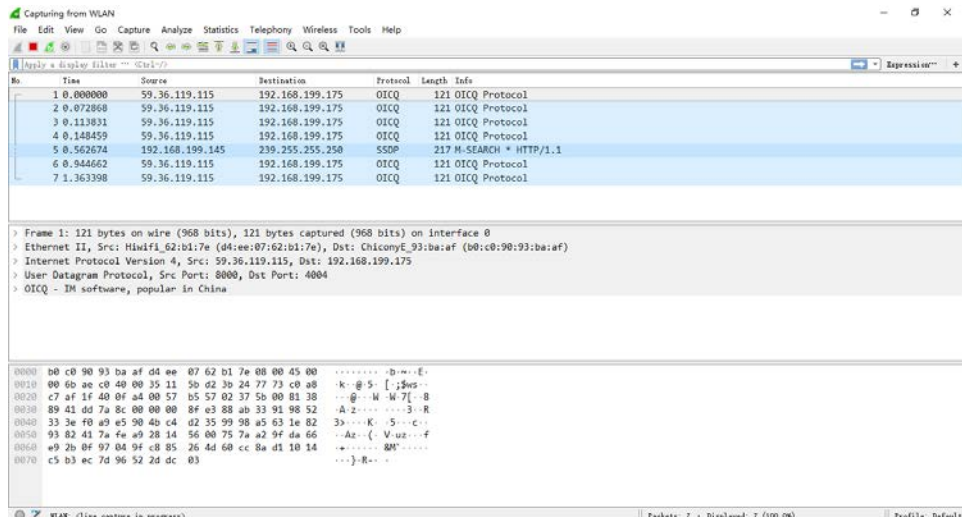
子网掩码 : 255.255.255.0

默认网关. : 192.168.199.1

四、实验步骤

1. 捕获大量的由本地主机到远程服务器的 TCP 分组

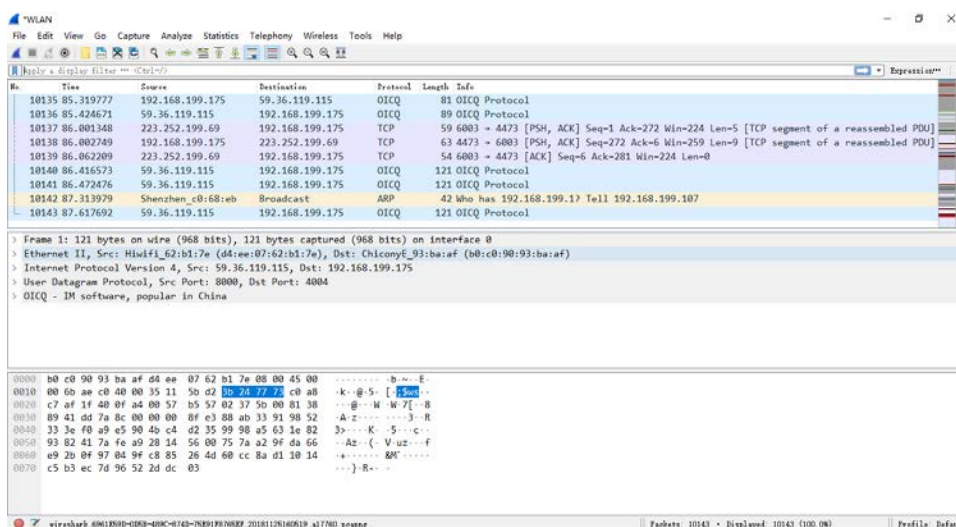
(1) 启动 Wireshark，开始进行；



(2) 启动 Chrome 浏览器，打开 <https://www.sina.com.cn/> 网页；

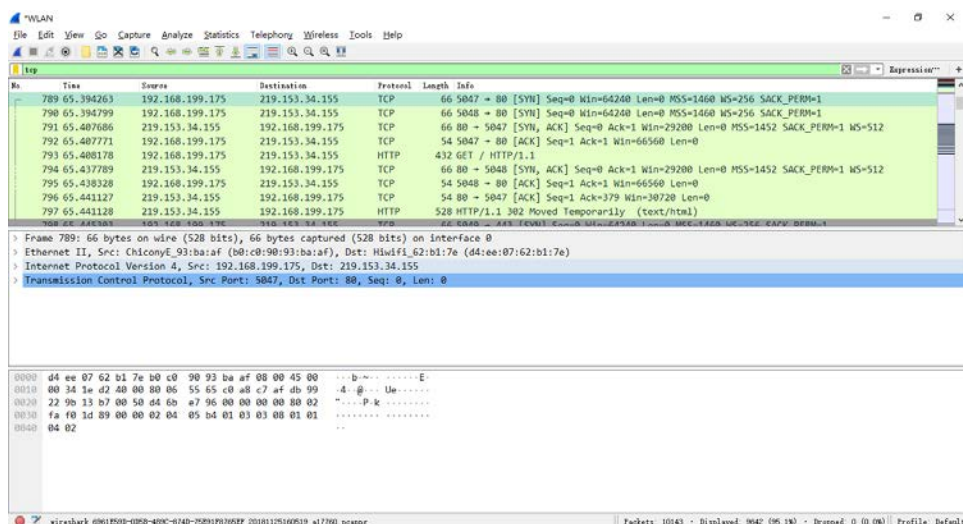


(3) 停止分组捕获。



2. 浏览追踪信息

(1) 在显示筛选规则编辑框中输入“tcp”，可以看到在本地主机和服务端之间传输的一系列 tcp 和 HTTP 消息，可以看到包含 SYN Segment 的三次握手。也可以看到有主机向服务器发送的一个 HTTP GET 消息和一系列的“http continuation”报文。



(2) 根据操作回答“实验报告内容”中的 1-2 题。

3. TCP 基础

根据操作回答“实验报告内容”中的 3-5 题；

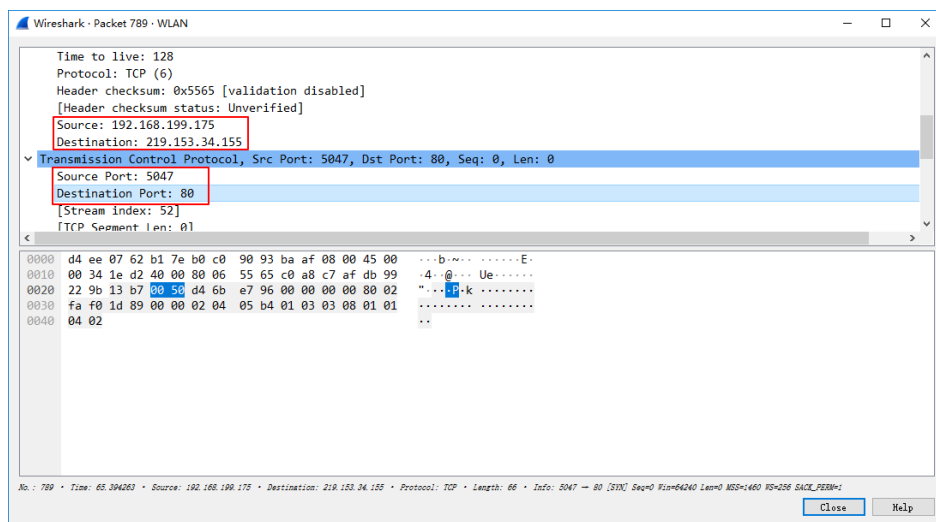
4. TCP 拥塞控制

(1) 在 Wireshark 已捕获分组列表窗口中选择一个 TCP 报文段；

(2) 选择菜单: Statistics->TCP Stream Graph->Time Sequence Graph (Stevens)。

5. 实验结果

(1) 向 www.sina.com.cn 服务器传送文件的客户端主机的 IP 地址和 TCP 端口号分别是多少？请截图并回答。

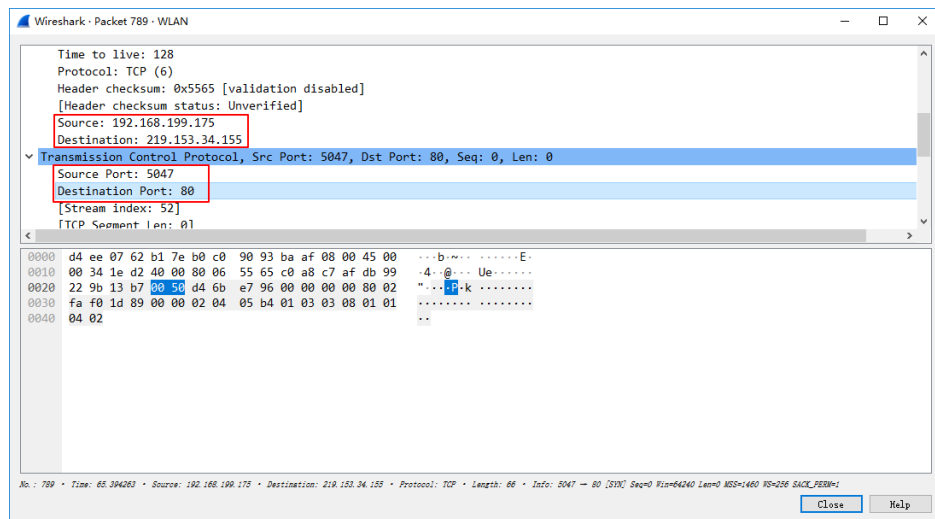


主机: 192.168.199.175

端口号: 5047

(2) www.sina.com.cn 服务器的 IP 地址是多少？对这一连接,它用来发送和接收

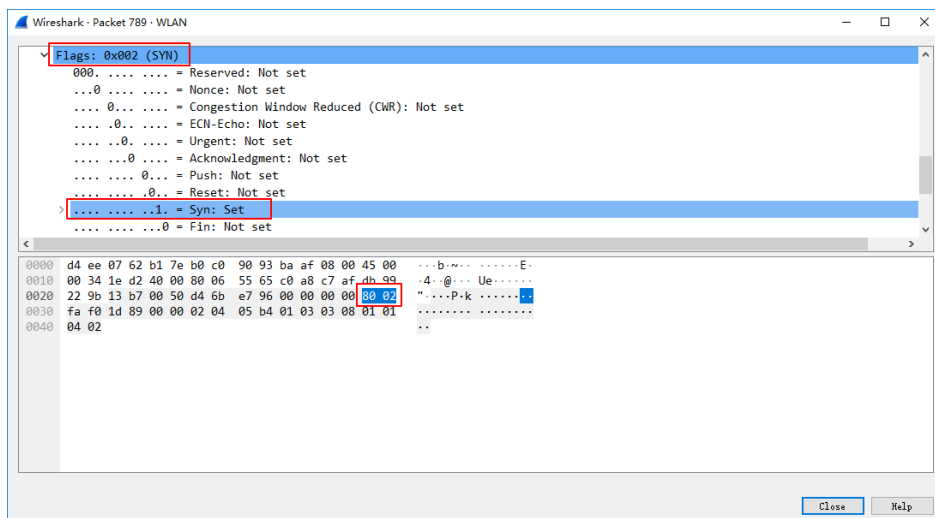
TCP 报文的端口号是多少？请截图并回答。



IP 地址：219.153.34.155

端口号：80

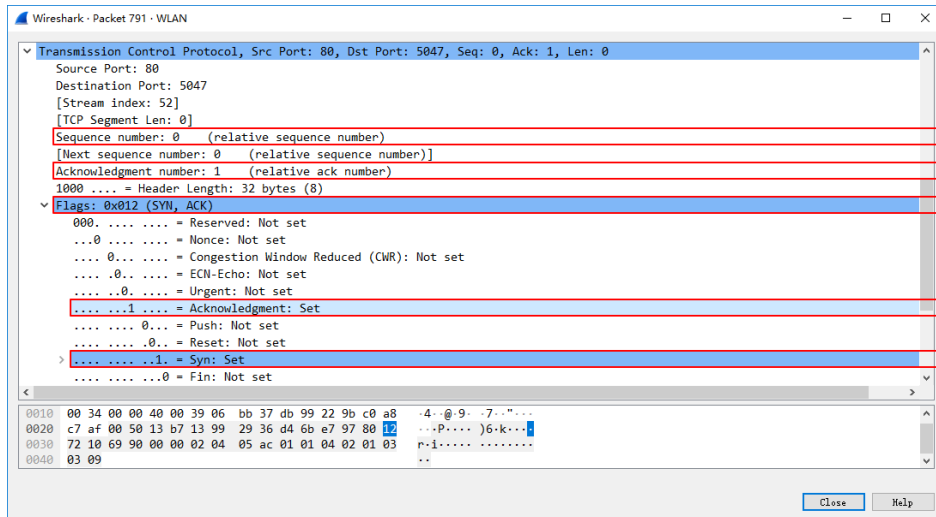
- (3) 客户服务器之间用于初始化 TCP 连接的 TCP SYN 报文段的序号 (sequence number) 是多少？在该报文段中, 是用什么来标示该报文段是 SYN 报文段的？



该报文段序号为 0；

在该报文段中, 含有一个 Flags 标志, 该标志总共可以设置 10 个标志, 当该报文段为 SYN 时, 该标志的第 2 位 (设该二进制的最低位为第 1 位) 置 1, 对应 16 进制的值为 0x002；

- (4) 服务器向客户端发送的 SYNACK 报文段序号是多少？该报文段中, Acknowledgement 字段的值是多少？www.sina.com.cn 服务器是如何决定此值的？在该报文段中, 是用什么来标识该报文段是 SYN ACK 报文段的？



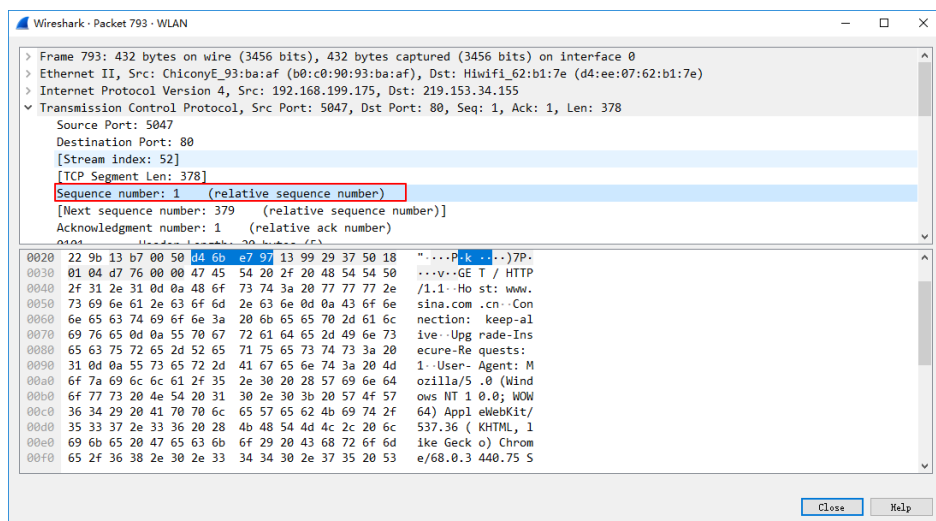
该报文段序号为0；

Acknowledgement 字段的值为1；

ACK 的值由服务器接收到的 SYN 的值+1 得到；

在该报文段中，含有一个 Flags 标志，该标志总共可以设置 10 个标志，当该报文段为 SYN ACK 报文段时，该标志的第 2 位和第 5 位（设该二进制的最小位为第 1 位）置 1，对应 16 进制的值为 0x012；

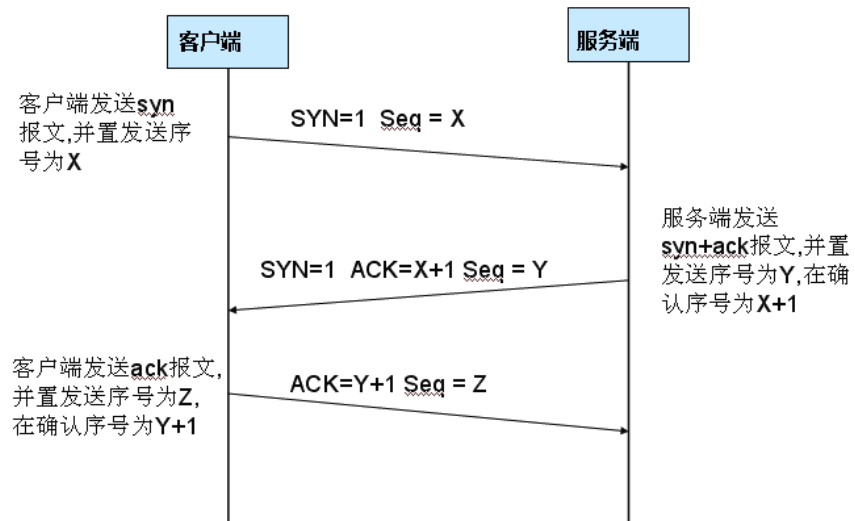
（5） 包含 HTTP GET 消息的 TCP 报文段的序号是多少？



五、实验结论

收获 1. Wireshark 捕获的数据过多时可以使用过滤规则 `ip.src == IP_ADDRESS` or `ip.dst == IP_ADDRESS` 来筛选数据。如本题，可以先使用 `ping` 命令获取 `www.sina.com.cn` 的 IP 地址，然后使用过滤规则过滤即可，即使用语句 `ip.src == 219.153.34.155` or `ip.dst == 219.153.34.155`

收获 2. TCP 三次握手图解：



实验四：HTTP 和 DNS 分析

一、实验目的

1. 熟悉并掌握 Wireshark 的基本操作，了解网络协议实体间的交互以及报文交换；
2. 分析 HTTP 和 DNS 协议。

二、实验内容

通过使用命令行中的 nslookup 命令和 Wireshark 抓包工具理解 HTTP 和 DNS 协议。

三、实验环境

操作系统：Windows 10 专业版 1809

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 : lan

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

IPv4 地址 : 192.168.199.175

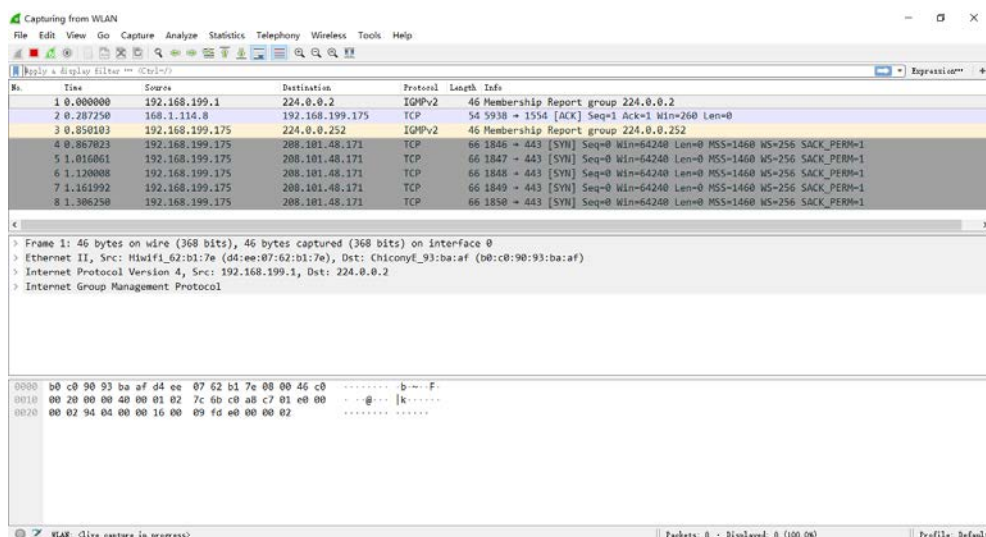
子网掩码 : 255.255.255.0

默认网关. : 192.168.199.1

四、实验步骤

1. HTTP 分析

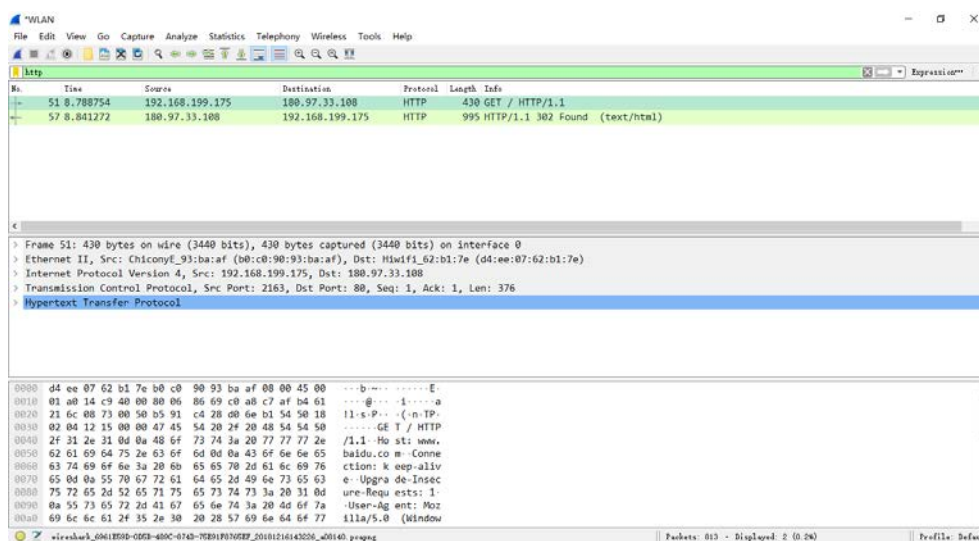
(1) 启动 Wireshark，开始分组捕获：



- (2) 启动主机上的 Chrome 浏览器，在浏览器的地址栏中输入：www.baidu.com；
- 浏览器将显示百度搜索网页；



- (3) 在窗口的显示过滤规则编辑框处输入“http”，分组列表子窗口中将只显示所捕获到的 HTTP 消息。选择分组列表窗口中的第一条 http 报文。它应该是你的计算机发向 www.baidu.com 服务器的 HTTP GET 报文；



- (4) 停止分组捕获，并根据捕获窗口内容，回答“实验报告内容”中的问题。

2. 跟踪并分析 DNS

nslookup 工具允许主机向指定的 DNS 服务器查询某个 DNS 记录。如果没有指明 DNS 服务器，nslookup 将把查询请求发向默认的 DNS 服务器。

```
命令提示符
Microsoft Windows [版本 10.0.17763.194]
(c) 2018 Microsoft Corporation. 保留所有权利。

C:\Users\Wenze>nslookup /?
用法:
nslookup [-opt ...]          # 使用默认服务器的交互模式
nslookup [-opt ...] - server # 使用 "server" 的交互模式
nslookup [-opt ...] host     # 仅查找使用默认服务器的 "host"
nslookup [-opt ...] host server # 仅查找使用 "server" 的 "host"

C:\Users\Wenze>
```

nslookup 的一般格式是: nslookup - option1 - option2 host-to-find
dns-server;

ipconfig 命令用来显示你当前的 TCP/IP 信息, 包括: 你的地址、DNS 服务器的地址、适配器的类型等信息。

如果要显示与主机相关的信息用命令: ipconfig/all;

```
命令提示符
C:\Users\Wenze>ipconfig /all

Windows IP 配置

   主机名 . . . . . : AZE-Windows
   主 DNS 后缀 . . . . . : 
   节与类型 . . . . . : 混合
   IP 路由已启用 . . . . . : 否
   WINS 代理已启用 . . . . . : 否
   DNS 后缀搜索列表 . . . . . : lan

以太网适配器 以太网:

   媒体状态 . . . . . : 媒体已断开连接
   连接特定的 DNS 后缀 . . . . . : 
   描述 . . . . . : Realtek PCIe FE Family Controller
   物理地址 . . . . . : 
   DHCP 已启用 . . . . . : 是
   自动配置已启用 . . . . . : 是

无线局域网适配器 本地连接* 1:

   媒体状态 . . . . . : 媒体已断开连接
   连接特定的 DNS 后缀 . . . . . : 
   描述 . . . . . : Microsoft Wi-Fi Direct Virtual Adapter
   物理地址 . . . . . : 
   DHCP 已启用 . . . . . : 是
   自动配置已启用 . . . . . : 是

无线局域网适配器 本地连接* 2:
```

如果要查看 DNS 缓存中的记录用命令: ipconfig/displaydns

```
命令提示符
C:\Users\Wenze>ipconfig /displaydns

Windows IP 配置

array704-prod.do.dsp.mp.microsoft.com
-----
记录名称 . . . . . : array704-prod.do.dsp.mp.microsoft.com
记录类型 . . . . . : 1
生存时间 . . . . . : 2926
数据长度 . . . . . : 4
部分 . . . . . : 答案
A (主机)记录 . . . . . : 52.229.168.53

accounts.google.com
-----
记录名称 . . . . . : accounts.google.com
记录类型 . . . . . : 1
生存时间 . . . . . : 190
数据长度 . . . . . : 4
部分 . . . . . : 答案
A (主机)记录 . . . . . : 216.58.200.77

ocsp2.digicert.com
-----
记录名称 . . . . . : ocsp2.digicert.com
记录类型 . . . . . : 5
生存时间 . . . . . : 995
数据长度 . . . . . : 8
```

如果要清空 DNS 缓存用命令: ipconfig /flushdns

```
生存时间. . . . . : 107
数据长度. . . . . : 4
部分. . . . . : 答案
A (主机)记录 . . . . : 203.208.40.65

记录名称. . . . . : redirector.gvt1.com
记录类型. . . . . : 1
生存时间. . . . . : 107
数据长度. . . . . : 4
部分. . . . . : 答案
A (主机)记录 . . . . : 203.208.40.72

记录名称. . . . . : redirector.gvt1.com
记录类型. . . . . : 1
生存时间. . . . . : 107
数据长度. . . . . : 4
部分. . . . . : 答案
A (主机)记录 . . . . : 203.208.40.71

C:\Users\Wenze>ipconfig /flushdns

Windows IP 配置

已成功刷新 DNS 解析缓存。

C:\Users\Wenze>
```

运行以上命令需要进入 MSDOS 环境。(开始菜单->运行->输入命令“cmd”)

- (1) 利用 ipconfig 命令清空主机上的 DNS 缓存。启动 Chrome 浏览器，并将浏览器的缓存清空：

```
生存时间. . . . . : 107
数据长度. . . . . : 4
部分. . . . . : 答案
A (主机)记录 . . . . : 203.208.40.65

记录名称. . . . . : redirector.gvt1.com
记录类型. . . . . : 1
生存时间. . . . . : 107
数据长度. . . . . : 4
部分. . . . . : 答案
A (主机)记录 . . . . : 203.208.40.72

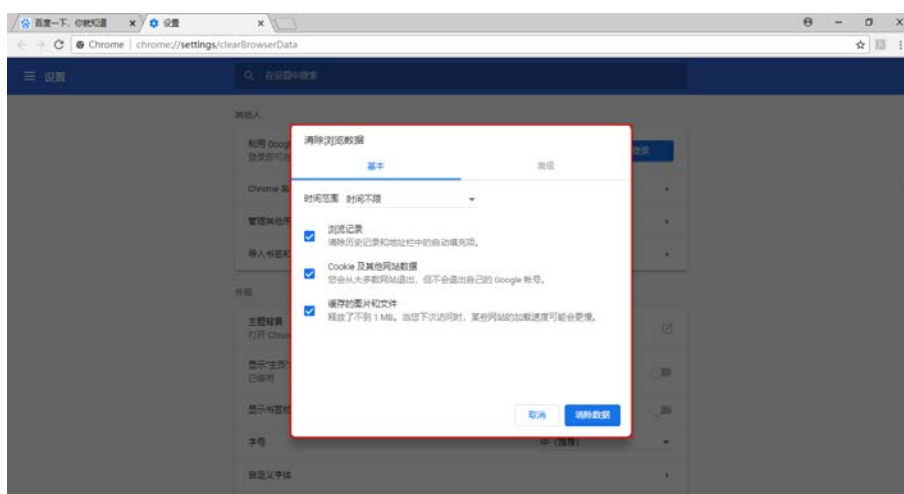
记录名称. . . . . : redirector.gvt1.com
记录类型. . . . . : 1
生存时间. . . . . : 107
数据长度. . . . . : 4
部分. . . . . : 答案
A (主机)记录 . . . . : 203.208.40.71

C:\Users\Wenze>ipconfig /flushdns

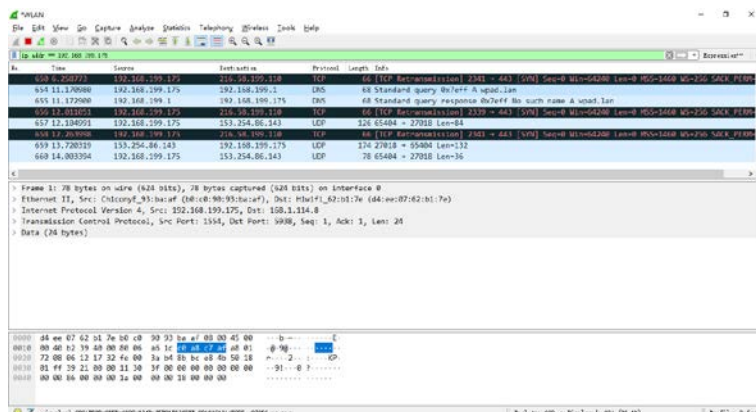
Windows IP 配置

已成功刷新 DNS 解析缓存。

C:\Users\Wenze>
```



- (2) 启动 Wireshark，在显示过滤筛选规则编辑框处输入：
- “ip.addr == your_IP_address” (如：ip.addr==10.17.7.23)；



- (3) 过滤器将会删除所有目的地址和源地址与指定 IP 地址都不同的分组；
- (4) 开始 Wireshark 分组捕获；
- (5) 在 Chrome 浏览器的地址栏中输入：www.baidu.com 后，回车；
- (6) 停止分组捕获；
- (7) 开始 Wireshark 分组捕获。
- (8) 在 www.baidu.com 上进行 nslookup 即执行命令：nslookup www.baidu.com；
- (9) 停止分组捕获。

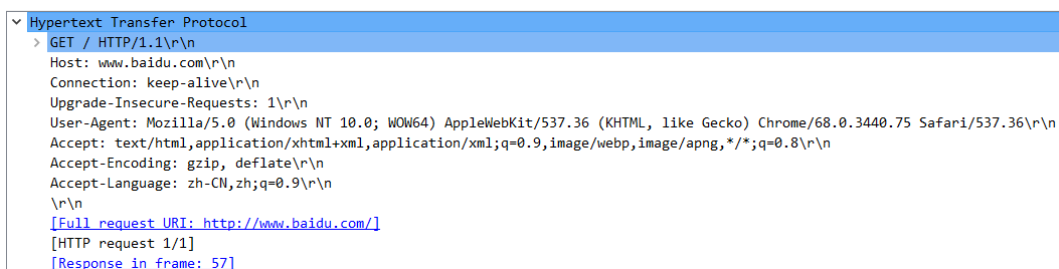
3. HTTP 分析实验结果

- (1) 从发出 HTTP GET 消息到接收到 HTTP OK 响应报文共需要多长时间？（在默认的情况下，分组列表窗口中 Time 列的值是从 Wireshark 开始追踪到分组被捕获时总的时间，以秒为单位。若要按 time-of-day 格式显示 Time 列的值，需选择 View 下拉菜单，再选择 Time Display Format，然后选择 Time-of-day。）

No.	Time	Source	Destination	Protocol	Length	Info
51	8.788754	192.168.199.175	180.97.33.108	HTTP	430	GET / HTTP/1.1
57	8.841272	180.97.33.108	192.168.199.175	HTTP	995	HTTP/1.1 302 Found (text/html)

接收到 HTTP Found: $T = 8.841272 - 8.788754s = 0.052518s = 52.518ms$

- (2) 写出第 3 步所显示的 HTTP 消息头部行信息并说明其含义？



GET 该消息类型以及具体协议

Host 发出请求的页面所在的域

Connection 浏览器与服务器之间连接的类型

Upgrade-Insecure-Requests 告知服务器，浏览器可以处理 https 协议，与服务器返回的 Content-Security-Policy 相对应，可以将该网址（http）升级为 https 协议。

User-Agent 浏览器的用户代理字符串

Accept 浏览器能够处理的内容类型

Accept-Encoding 浏览器能够处理的压缩编码

Accept-Language 浏览器当前设置的语言

等等

- (3) 你的浏览器使用的是 HTTP1.0，还是 HTTP1.1？你所访问的 Web 服务器所用 HTTP 协议的版本号是多少？

```
Info
GET / HTTP/1.1
HTTP/1.1 302 Found (text/html)
```

均为 HTTP 1.1

- (4) 从服务器向你的浏览器返回 response 消息的状态代码是多少？表示什么意思？

```
▼ Hypertext Transfer Protocol
  ▼ HTTP/1.1 302 Found\r\n
    > [Expert Info (Chat/Sequence): HTTP/1.1 302 Found\r\n]
      Response Version: HTTP/1.1
      Status Code: 302
      [Status Code Description: Found]
      Response Phrase: Found
```

302：请求的资源现在临时从不同的 URI 响应请求。由于这样的重定向是临时的，客户端应当继续向原有地址发送以后的请求。只有在 Cache-Control 或 Expires 中进行了指定的情况下，这个响应才是可缓存的。

4. 跟踪并分析 DNS 实验结果

- (1) 定位到 DNS 查询消息和查询响应报文，这两种报文的发送是基于 UDP 还是基于 TCP 的？

No.	Time	Source	Destination	Protocol	Length	Info
4	2.564828	192.168.199.175	192.168.199.1	DNS	73	Standard query 0xc4e4 A www.baidu.com
5	2.577552	192.168.199.1	192.168.199.175	DNS	132	Standard query response 0xc4e4 A www.baidu.com CNAME www.a.shifen.com A 188.97.33.1
43	2.696549	192.168.199.175	192.168.199.1	DNS	73	Standard query 0xd217 A sp0.baidu.com
76	2.720415	192.168.199.175	192.168.199.1	DNS	75	Standard query 0xd259 A b1.bstatic.com
77	2.720613	192.168.199.175	192.168.199.1	DNS	75	Standard query 0xe7b2 A s1.bstatic.com
78	2.721142	192.168.199.175	192.168.199.1	DNS	72	Standard query 0xd204 A t1.baidu.com
79	2.721258	192.168.199.175	192.168.199.1	DNS	76	Standard query 0xd151 A s11.bstatic.com
82	2.721593	192.168.199.1	192.168.199.175	DNS	132	Standard query response 0xd217 A sp0.baidu.com CNAME www.a.shifen.com A 188.97.33.1
86	2.730303	192.168.199.1	192.168.199.175	DNS	130	Standard query response 0xd217 A s1.bstatic.com CNAME www.a.shifen.com A 188.97.33.1

Internet Protocol Version 4, Src: 192.168.199.175, Dst: 192.168.199.1						
0180 = Version: 4						
... 0181 = Header Length: 20 bytes (5)						
Differential Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)						
Total Length: 59						
Identification: 0x2e2a (11002)						
Flags: 0x0000						
Time to live: 128						
Protocol: UDP (17)						
Header checksum: 0xfcf5 [validation disabled]						
[Header checksum status: Unverified]						
Source: 192.168.199.175						
Destination: 192.168.199.1						

这两种报文的发送是基于 UDP 的。

(2) DNS 查询消息的目的端口是多少？DNS 查询响应消息的端口号是多少？

No.	Time	Source	Destination	Protocol	Length	Info
4	2.564828	192.168.199.175	192.168.199.1	DNS	73	Standard query 0xc4e4 A www.baidu.com
5	2.577552	192.168.199.1	192.168.199.175	DNS	132	Standard query response 0xc4e4 A www.baidu.com CNAME www.a.shifen.com A 188.97.33.1
43	2.696549	192.168.199.175	192.168.199.1	DNS	73	Standard query 0xd217 A sp0.baidu.com
76	2.720415	192.168.199.175	192.168.199.1	DNS	75	Standard query 0xd259 A b1.bstatic.com
77	2.720613	192.168.199.175	192.168.199.1	DNS	75	Standard query 0xe7b2 A s1.bstatic.com
78	2.721142	192.168.199.175	192.168.199.1	DNS	72	Standard query 0xd204 A t1.baidu.com
79	2.721258	192.168.199.175	192.168.199.1	DNS	76	Standard query 0xd151 A s11.bstatic.com
82	2.721593	192.168.199.1	192.168.199.175	DNS	132	Standard query response 0xd217 A sp0.baidu.com CNAME www.a.shifen.com A 188.97.33.1
86	2.730303	192.168.199.1	192.168.199.175	DNS	130	Standard query response 0xd217 A s1.bstatic.com CNAME www.a.shifen.com A 188.97.33.1

Frame 4: 73 bytes on wire (584 bits), 73 bytes captured (584 bits) on interface 0						
Ethernet II, Src: Chicony_E93:ba:af (08:c0:90:93:ba:af), Dst: Huiwifl_62:bi:7e (04:ee:07:62:bi:7e)						
Internet Protocol Version 4, Src: 192.168.199.175, Dst: 192.168.199.1						
User Datagram Protocol, Src Port: 55077, Dst Port: 53						
Domain Name System (query)						

No.	Time	Source	Destination	Protocol	Length	Info
4	2.564828	192.168.199.175	192.168.199.1	DNS	73	Standard query 0xc4e4 A www.baidu.com
5	2.577552	192.168.199.1	192.168.199.175	DNS	132	Standard query response 0xc4e4 A www.baidu.com CNAME www.a.shifen.com A 188.97.33.1
43	2.696549	192.168.199.175	192.168.199.1	DNS	73	Standard query 0xd217 A sp0.baidu.com
76	2.720415	192.168.199.175	192.168.199.1	DNS	75	Standard query 0xd259 A b1.bstatic.com
77	2.720613	192.168.199.175	192.168.199.1	DNS	75	Standard query 0xe7b2 A s1.bstatic.com
78	2.721142	192.168.199.175	192.168.199.1	DNS	72	Standard query 0xd204 A t1.baidu.com
79	2.721258	192.168.199.175	192.168.199.1	DNS	76	Standard query 0xd151 A s11.bstatic.com
82	2.721593	192.168.199.1	192.168.199.175	DNS	132	Standard query response 0xd217 A sp0.baidu.com CNAME www.a.shifen.com A 188.97.33.1
86	2.730303	192.168.199.1	192.168.199.175	DNS	130	Standard query response 0xd217 A s1.bstatic.com CNAME www.a.shifen.com A 188.97.33.1

Frame 5: 132 bytes on wire (1056 bits), 132 bytes captured (1056 bits) on interface 0						
Ethernet II, Src: Huiwifl_62:bi:7e (04:ee:07:62:bi:7e), Dst: Chicony_E93:ba:af (08:c0:90:93:ba:af)						
Internet Protocol Version 4, Src: 192.168.199.1, Dst: 192.168.199.175						
User Datagram Protocol, Src Port: 53, Dst Port: 55077						
Domain Name System (response)						

查询消息的目的端口是 53；响应消息的目的端口号是 55077。

(3) DNS 查询消息发送的目的地址 IP 是多少？利用 ipconfig 命令(ipconfig/all)

查看你主机的本地 DNS 服务器的 IP 地址。这两个地址相同吗？

No.	Time	Source	Destination	Protocol	Length	Info
4	2.564828	192.168.199.175	192.168.199.1	DNS	73	Standard query 0xc4e4 A www.baidu.com
5	2.577552	192.168.199.1	192.168.199.175	DNS	132	Standard query response 0xc4e4 A www.baidu.com CNAME www.a.shifen.com A 188.97.33.1
43	2.696549	192.168.199.175	192.168.199.1	DNS	73	Standard query 0xd217 A sp0.baidu.com
76	2.720415	192.168.199.175	192.168.199.1	DNS	75	Standard query 0xd259 A b1.bstatic.com
77	2.720613	192.168.199.175	192.168.199.1	DNS	75	Standard query 0xe7b2 A s1.bstatic.com
78	2.721142	192.168.199.175	192.168.199.1	DNS	72	Standard query 0xd204 A t1.baidu.com
79	2.721258	192.168.199.175	192.168.199.1	DNS	76	Standard query 0xd151 A s11.bstatic.com
82	2.721593	192.168.199.1	192.168.199.175	DNS	132	Standard query response 0xd217 A sp0.baidu.com CNAME www.a.shifen.com A 188.97.33.1
86	2.730303	192.168.199.1	192.168.199.175	DNS	130	Standard query response 0xd217 A s1.bstatic.com CNAME www.a.shifen.com A 188.97.33.1

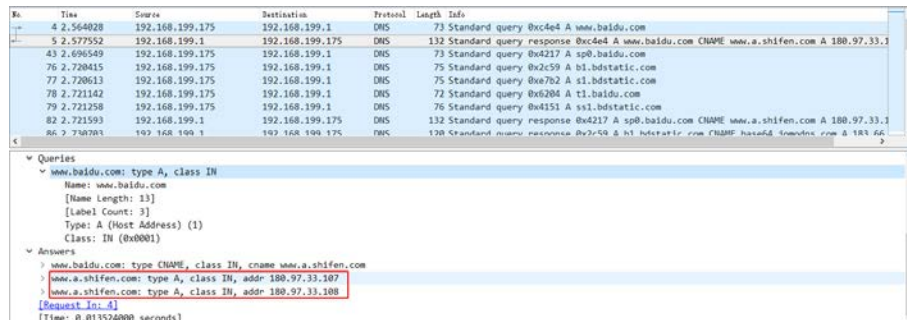
Frame 4: 73 bytes on wire (584 bits), 73 bytes captured (584 bits) on interface 0						
Ethernet II, Src: Chicony_E93:ba:af (08:c0:90:93:ba:af), Dst: Huiwifl_62:bi:7e (04:ee:07:62:bi:7e)						
Internet Protocol Version 4, Src: 192.168.199.175, Dst: 192.168.199.1						
User Datagram Protocol, Src Port: 55077, Dst Port: 53						
Domain Name System (query)						

命令提示符		
媒体状态	:	媒体已断开连接
连接特定的 DNS 后缀	:	
描述	:	TeamViewer VPN Adapter
物理地址	:	{8} {8} {8} {8} {8} {8}
DHCP 已启用	:	是
自动配置已启用	:	是
无线局域网适配器 WLAN:		
连接特定的 DNS 后缀	:	lan
描述	:	Dell Wireless 1705 802.11b/g/n (2.4GHz)
物理地址	:	E0-C0-90-93-BA-AF
DHCP 已启用	:	是
自动配置已启用	:	是
本地连接 IPv6 地址	:	fe80::3079:5439:d245:a240%9(首选)
IPv4 地址	:	192.168.199.175(首选)
子网掩码	:	255.255.255.0
获得租约的时间	:	2018-12-16 14:19:49
租约已过期时间	:	2018-12-17 2:19:50
默认网关	:	192.168.199.1
DHCP 服务器	:	192.168.199.1
DHCPv6 IAD	:	162578576
DHCPv6 客户端 DUID	:	00-01-00-01-23-80-52-F5-20-47-47-5F-08-68
DNS 服务器	:	192.168.199.1
TCPIP 上的 NetBIOS	:	已启用

DNS 查询消息发送的目的地址 IP 为：192.168.199.1

主机的本地 DNS 服务器的 IP 地址为：192.168.199.1，IP 地址相同。

- (4) 考虑一下你的主机随后发送 TCP SYN Segment，包含 SYN Segment 的 IP 分组头部中目的 IP 地址是否与在 DNS 查询响应消息中提供的某个 IP 地址相对应？



No.	Time	Source	Destination	Protocol	Length	Info
4	2.564028	192.168.199.175	192.168.199.1	DNS	73	Standard query 0xc4e4 A www.baidu.com
5	2.577552	192.168.199.1	192.168.199.175	DNS	132	Standard query response 0xc4e4 A www.baidu.com CHAME www.a.shifen.com A 180.97.33.107
43	2.696549	192.168.199.175	192.168.199.1	DNS	73	Standard query 0x4217 A sp0.baidu.com
76	2.720415	192.168.199.175	192.168.199.1	DNS	75	Standard query 0x2c59 A bl.bdstatic.com
77	2.720613	192.168.199.175	192.168.199.1	DNS	75	Standard query 0x67b2 A sl.bdstatic.com
78	2.721142	192.168.199.175	192.168.199.1	DNS	72	Standard query 0x6204 t1.baidu.com
79	2.721258	192.168.199.175	192.168.199.1	DNS	76	Standard query 0x4151 A ssl.bdstatic.com
82	2.721593	192.168.199.1	192.168.199.175	DNS	132	Standard query response 0x4217 A sp0.baidu.com CHAME www.a.shifen.com A 180.97.33.107
86	2.730701	192.168.199.1	192.168.199.175	DNS	128	Standard query response 0x2c59 A bl.bdstatic.com CHAME www.a.shifen.com A 180.97.33.107

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)

Answers

- www.baidu.com: type CHAME, class IN, cname www.a.shifen.com
- www.a.shifen.com: type A, class IN, addr: 180.97.33.107
- www.a.shifen.com: type A, class IN, addr: 180.97.33.108

[Request In: 4]
[Time: 0.013524000 seconds]

可能为 180.97.33.108 或 180.97.33.107

五、实验结论

收获 1. DNS 全称 Domain Name System，即域名系统，可以将域名解析为对应的 IP 地址。

收获 2. DNS 协议是基于 UDP 协议的，使用端口号为常用端口号 53。