实验项目名称：WireShark 软件初探和常见网络命令的使用

一、 实验目的和要求：

- 初步了解 WireShark 软件的界面和功能
- 熟悉各类常用网络命令的使用

二、 实验内容和原理

- Wireshark 是 PC 上使用最广泛的免费抓包工具，可以分析大多数常见的协议数据包。有 Windows 版本、Linux 版本和 Mac 版本，可以免费从网上下载
- 初步掌握网络协议分析软件 Wireshark 的使用，**学会配置过滤器**
- 根据要求配置 Wireshark，捕获某一类协议的数据包
- 在 PC 机上熟悉常用网络命令的功能和用法: **Ping.exe，Netstat.exe, Telnet.exe, Tracert.exe, Arp.exe, Ipconfig.exe, Net.exe, Route.exe, Nslookup.exe**
- 利用 WireShark 软件捕捉上述部分命令产生的数据包

三、 主要仪器设备

- 联网的 PC 机
- WireShark 协议分析软件

四、 操作方法与实验步骤

- 安装网络包捕获软件 Wireshark
- 配置网络包捕获软件，捕获所有机器的数据包
- 配置网络包捕获软件，只捕获特定类型的包
- 在 Windows 命令行方式下，执行适当的命令，完成以下功能(请以管理员身份打开命令行)：
    1. 测试到特定地址的联通性、数据包延迟时间
    2. 显示本机的网卡物理地址、IP 地址
    3. 显示本机的默认网关地址、DNS 服务器地址
    4. 显示本机记录的局域网内其它机器 IP 地址与其物理地址的对照表
    5. 显示从本机到达一个特定地址的路由
    6. 显示某一个域名的 IP 地址
    7. 显示已经与本机建立 TCP 连接的端口、IP 地址、连接状态等信息
    8. 显示本机的路由表信息，并手工添加一个路由
    9. 显示本机的网络映射连接
    10. 显示局域网内某台机器的共享资源
    11. 使用 telnet 连接 WEB 服务器的端口，输入（<cr>表示回车）获得该网站的主页内容：

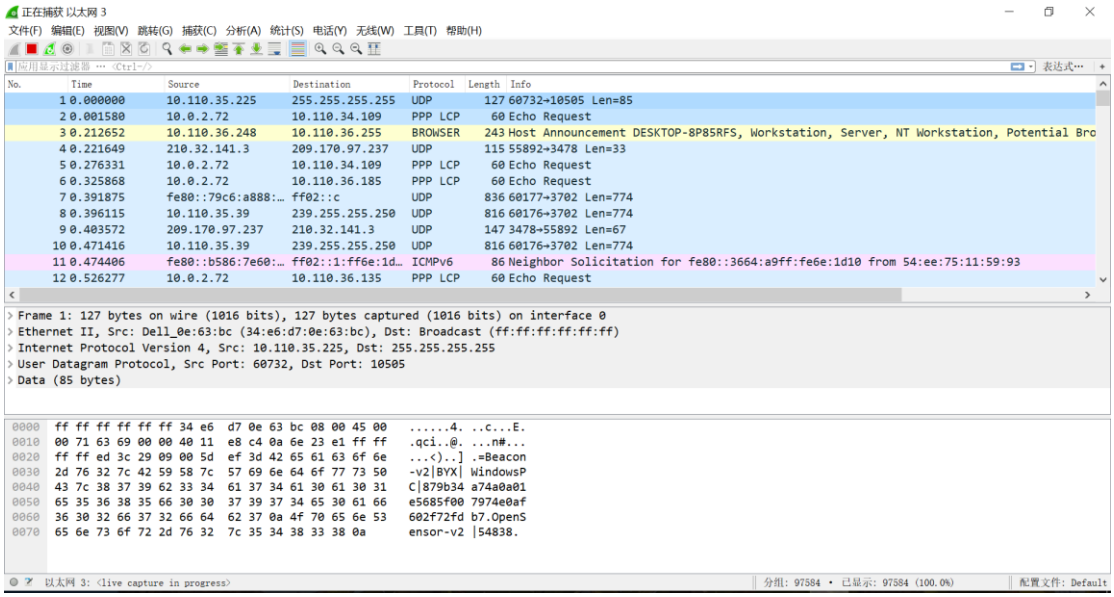
```
GET / HTTP/1.1<cr>
Host: 任意字符串<cr>
<cr>
```

- 利用 WireShark 实时观察在执行上述命令时，哪些命令会额外产生数据包，并记录

这些数据包的种类。

五、 实验数据记录和处理

- **运行 Wireshark 软件，界面是由哪几个部分构成？各有什么作用？**



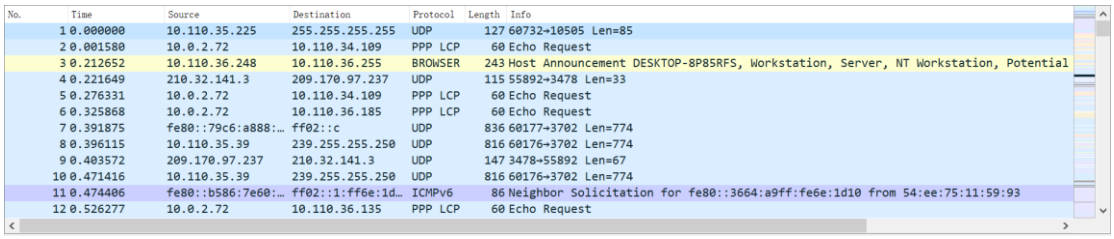
（主窗口界面）

1. **菜单：**用于开始操作。

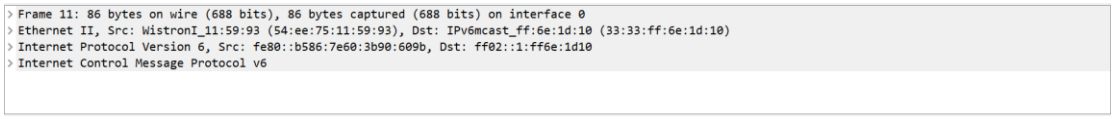
2. **主工具栏：**提供快速访问菜单中经常用到的项目的功能。

3. **Filter toolbar/过滤工具栏：**提供处理当前显示过滤得方法。

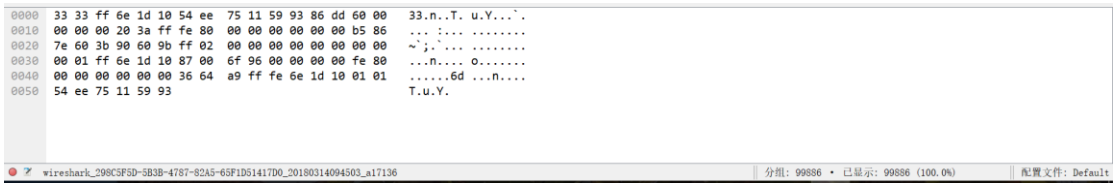
4. **Packet List 面板：**显示打开文件的每个包的摘要。点击面板中的单独条目，包的其他情况将会显示在另外两个面板中。



5. **Packet Detail 面板：**显示在 Packet List 面板中选择的包的更多详情。



6. **Packet bytes 面板：**显示在 Packet List 面板选择的包的数据，以及在 Packet details 面板高亮显示的字段。

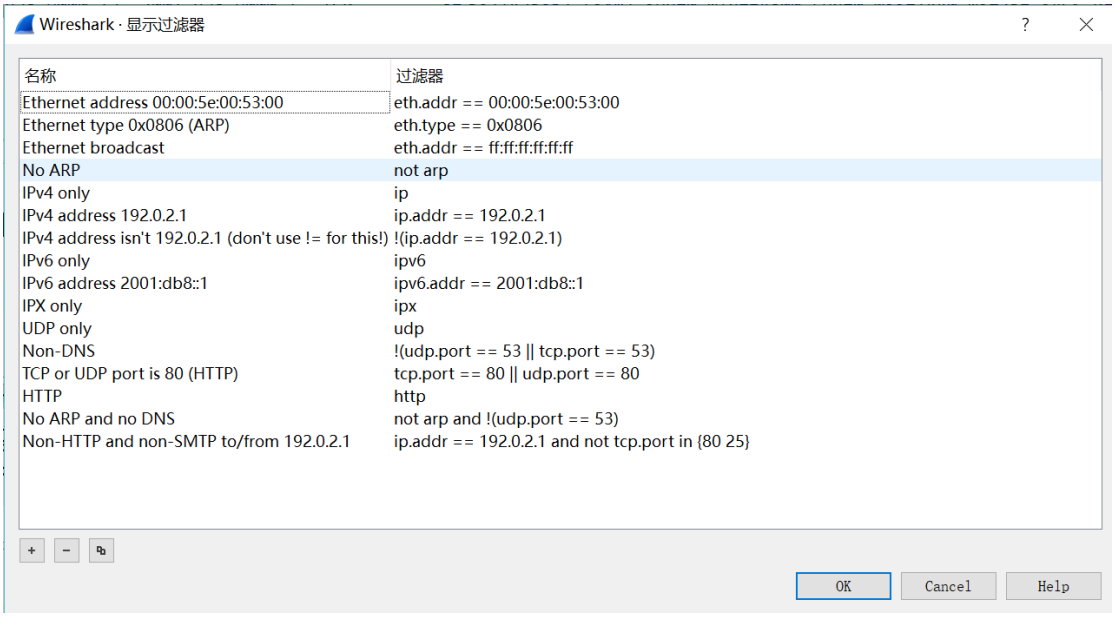


7.**状态栏：**显示当前程序状态以及捕捉数据的更多详情。

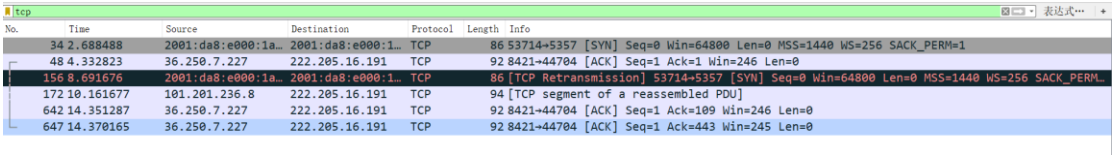
- **开始捕获网络数据包，你看到了什么？有哪些协议？**

在本次抓包中，出现了 PPP LCP，ARP，SSDP， L2TP，SSDP，OSPF，DHCPv6， TCP，ICMPv6， MBNS，UDP, TCP, MDNS, IGMPv3, IGMPv2 等协议。

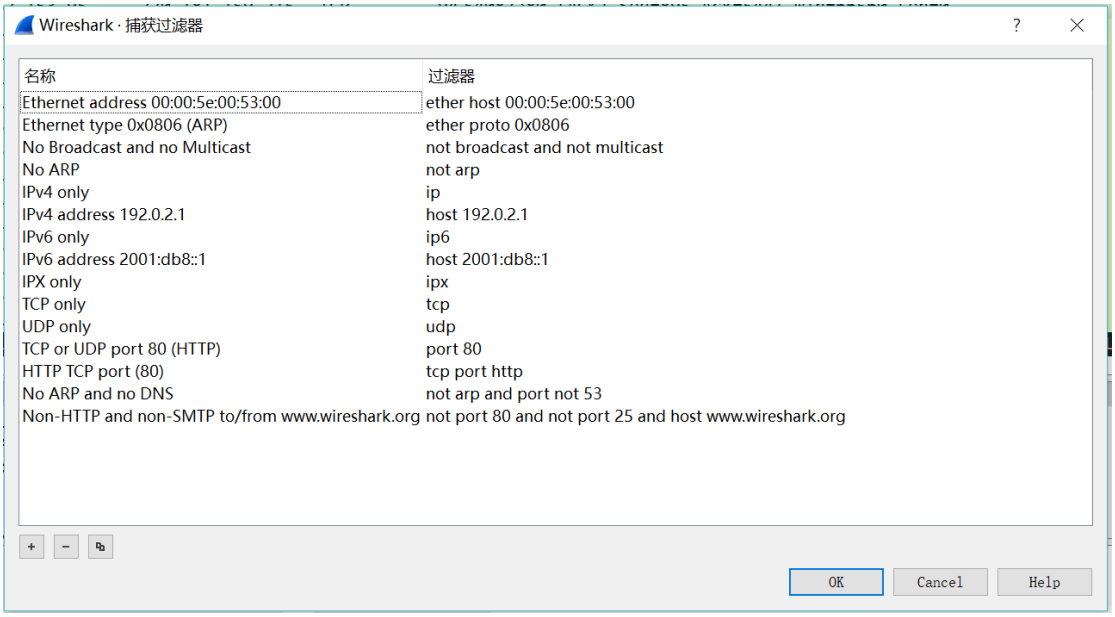
- **配置应用显示过滤器，让界面只显示某一协议类型的数据包。**



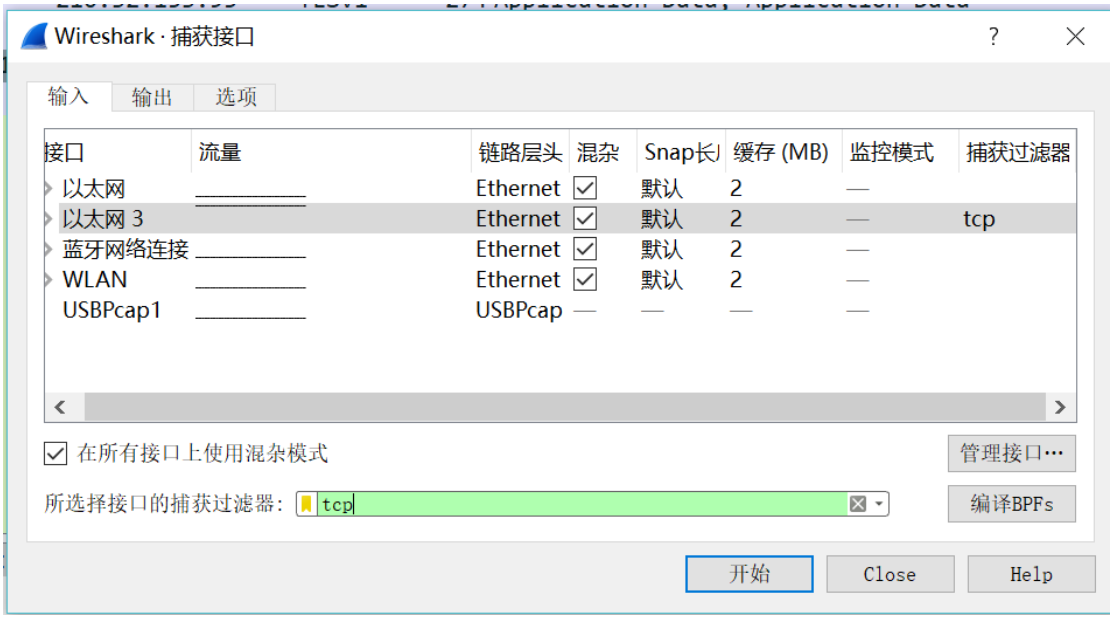
在本次实验中，采用了 tcp 来配置应用显示过滤器。

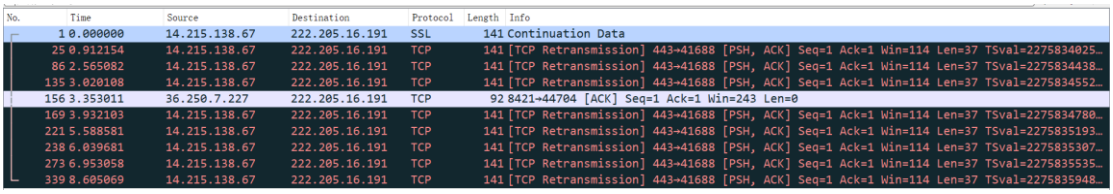


- **配置捕获过滤器，只捕获某类协议的数据包。**



在本次实验中使用捕获过滤器捕获 TCP 的信息。





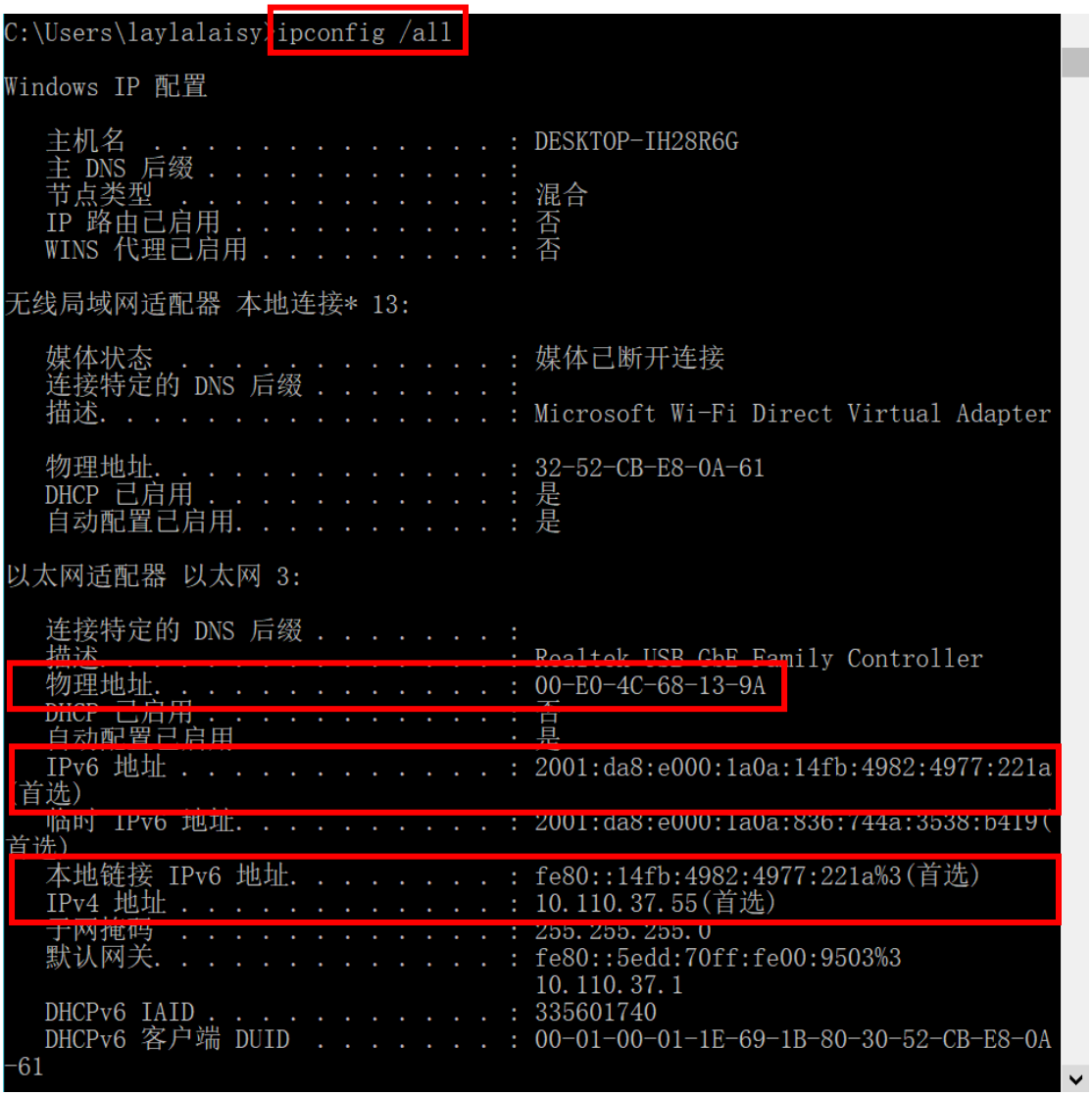
- **利用 Ping.exe，Netstat.exe， Telnet.exe, Tracert.exe, Arp.exe, Ipconfig.exe, Net.exe, Route.exe 命令完成在实验步骤中列举的 11 个功能。**

本次实验中 1-8 连接以太网 3， 9-11 连接 WLAN 完成。

1. 测试到特定地址的联通性、数据包延迟时间：**Ping.exe**

```
C:\Users\laylalaisy>ping 10.110.37.55

正在 Ping 10.110.37.55 具有 32 字节的数据:
来自 10.110.37.55 的回复: 字节=32 时间<1ms TTL=64
来自 10.110.37.55 的回复: 字节=32 时间<1ms TTL=64
来自 10.110.37.55 的回复: 字节=32 时间<1ms TTL=64
来自 10.110.37.55 的回复: 字节=32 时间<1ms TTL=64

10.110.37.55 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 = 0ms, 最长 = 0ms, 平均 = 0ms
```

2. 显示本机的网卡物理地址、IP 地址：**Ipconfig.exe**



3. 显示本机的默认网关地址、DNS 服务器地址：**Ipconfig.exe**

4. 显示本机记录的局域网内其它机器 IP 地址与其物理地址的对照表：**Arp.exe**

```
C:\Users\laylalaisy>arp -a

接口: 10.110.37.55 --- 0x3
  Internet 地址         物理地址              类型
  10.110.37.1           5c-dd-70-00-95-03     动态
  10.110.37.9           28-d2-44-7c-cb-da     动态
  10.110.37.20          00-0e-c6-d6-96-ed     动态
  10.110.37.30          08-9e-01-f4-95-d2     动态
  10.110.37.93          f8-a9-63-41-ef-da     动态
  10.110.37.126         34-17-eb-57-89-8e     动态
  10.110.37.152         c8-5b-76-72-aa-a8     动态
  10.110.37.222         28-d2-44-c1-6a-51     动态
  10.110.37.227         d4-81-d7-6b-e9-04     动态
  10.110.37.251         00-0e-c6-d4-42-de     动态
  10.110.37.255         ff-ff-ff-ff-ff-ff     静态
  224.0.0.2             01-00-5e-00-00-02     静态
  224.0.0.5             01-00-5e-00-00-05     静态
  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

接口: 210.32.153.95 --- 0x31
  Internet 地址         物理地址              类型
  0.0.0.0                                     静态
  2.16.162.10                                 静态
  2.16.162.12                                 静态
  2.16.162.16                                 静态
  2.16.162.21                                 静态
  2.17.34.29                                  静态
  10.10.0.21                                  静态
  10.10.2.21                                  静态
  10.202.102.20                               静态
  13.67.53.38                                 静态
  13.75.42.223                                静态
  13.78.94.7                                  静态
```

5. 显示从本机到达一个特定地址的路由：**Tracert.exe**

```
C:\Users\laylalaisy>tracert www.baidu.com

通过最多 30 个跃点跟踪
到 www.a.shifen.com [115.239.210.27] 的路由:

  1    <1 毫秒    <1 毫秒    <1 毫秒 10.0.2.72
  2     3 ms     1 ms     2 ms  10.3.7.86
  3     5 ms     1 ms     1 ms  10.3.7.89
  4   322 ms   330 ms   274 ms  10.3.7.129
  5    11 ms     3 ms     5 ms  115.236.179.225
  6    12 ms     3 ms     2 ms  220.191.134.177
  7     *        *        *     请求超时。
  8     *        *        *     请求超时。
  9     6 ms    10 ms     6 ms  115.239.209.10
 10     *        *        *     请求超时。
 11     *        *        *     请求超时。
 12     3 ms     3 ms     5 ms  115.239.210.27

跟踪完成。
```

6. 显示某一个域名的 IP 地址：**Ping.exe**

```
C:\Users\laylalaisy>ping www.baidu.com

正在 Ping www.a.shifen.com [115.239.210.27] 具有 32 字节的数据:
来自 115.239.210.27 的回复: 字节=32 时间=4ms TTL=53
来自 115.239.210.27 的回复: 字节=32 时间=2ms TTL=53
来自 115.239.210.27 的回复: 字节=32 时间=3ms TTL=53
来自 115.239.210.27 的回复: 字节=32 时间=3ms TTL=53

115.239.210.27 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 = 2ms, 最长 = 4ms, 平均 = 3ms
```

7. 显示已经与本机建立 TCP 连接的端口、IP 地址、连接状态等信息：**Netstat.exe**

```
C:\Users\laylalaisy>netstat -a

活动连接

  协议   本地地址          外部地址        状态
  TCP    0.0.0.0:22             DESKTOP-IH28R6G:0      LISTENING
  TCP    0.0.0.0:135            DESKTOP-IH28R6G:0      LISTENING
  TCP    0.0.0.0:445            DESKTOP-IH28R6G:0      LISTENING
  TCP    0.0.0.0:902            DESKTOP-IH28R6G:0      LISTENING
  TCP    0.0.0.0:912            DESKTOP-IH28R6G:0      LISTENING
  TCP    0.0.0.0:5357           DESKTOP-IH28R6G:0      LISTENING
  TCP    0.0.0.0:7779           DESKTOP-IH28R6G:0      LISTENING
  TCP    0.0.0.0:7998           DESKTOP-IH28R6G:0      LISTENING
  TCP    0.0.0.0:49664          DESKTOP-IH28R6G:0      LISTENING
  TCP    0.0.0.0:49665          DESKTOP-IH28R6G:0      LISTENING
  TCP    0.0.0.0:49666          DESKTOP-IH28R6G:0      LISTENING
  TCP    0.0.0.0:49667          DESKTOP-IH28R6G:0      LISTENING
  TCP    0.0.0.0:49668          DESKTOP-IH28R6G:0      LISTENING
  TCP    0.0.0.0:49670          DESKTOP-IH28R6G:0      LISTENING
  TCP    0.0.0.0:49671          DESKTOP-IH28R6G:0      LISTENING
  TCP    10.110.37.55:139       DESKTOP-IH28R6G:0      LISTENING
  TCP    127.0.0.1:4012         DESKTOP-IH28R6G:0      LISTENING
  TCP    127.0.0.1:4013         DESKTOP-IH28R6G:0      LISTENING
  TCP    127.0.0.1:7991         DESKTOP-IH28R6G:0      LISTENING
  TCP    127.0.0.1:7991         DESKTOP-IH28R6G:62140  ESTABLISHED
  TCP    127.0.0.1:7995         DESKTOP-IH28R6G:0      LISTENING
  TCP    127.0.0.1:7995         DESKTOP-IH28R6G:62145  ESTABLISHED
  TCP    127.0.0.1:9421         DESKTOP-IH28R6G:0      LISTENING
  TCP    127.0.0.1:10000        DESKTOP-IH28R6G:0      LISTENING
  TCP    127.0.0.1:27015        DESKTOP-IH28R6G:0      LISTENING
  TCP    127.0.0.1:27015        DESKTOP-IH28R6G:61722  ESTABLISHED
  TCP    127.0.0.1:54530        DESKTOP-IH28R6G:0      LISTENING
  TCP    127.0.0.1:54530        DESKTOP-IH28R6G:62519  ESTABLISHED
  TCP    127.0.0.1:61722        DESKTOP-IH28R6G:27015  ESTABLISHED
  TCP    127.0.0.1:62034        DESKTOP-IH28R6G:62035  ESTABLISHED
  TCP    127.0.0.1:62035        DESKTOP-IH28R6G:62034  ESTABLISHED
  TCP    127.0.0.1:62036        DESKTOP-IH28R6G:62037  ESTABLISHED
  TCP    127.0.0.1:62037        DESKTOP-IH28R6G:62036  ESTABLISHED
```

```
  TCP    127.0.0.1:62140        DESKTOP-IH28R6G:7991   ESTABLISHED
  TCP    127.0.0.1:62145        DESKTOP-IH28R6G:7995   ESTABLISHED
  TCP    127.0.0.1:62519        DESKTOP-IH28R6G:54530  ESTABLISHED
  TCP    127.0.0.1:62520        DESKTOP-IH28R6G:62521  ESTABLISHED
  TCP    127.0.0.1:62521        DESKTOP-IH28R6G:62520  ESTABLISHED
  TCP    210.32.153.95:139      DESKTOP-IH28R6G:0      LISTENING
  TCP    210.32.153.95:53293    180.163.238.163:https  ESTABLISHED
  TCP    210.32.153.95:53789    52.230.80.159:https    ESTABLISHED
  TCP    210.32.153.95:54369    115.231.31.133:https   CLOSE_WAIT
  TCP    210.32.153.95:54370    115.231.21.20:http     CLOSE_WAIT
  TCP    210.32.153.95:54371    115.231.21.20:http     CLOSE_WAIT
  TCP    210.32.153.95:54372    115.231.21.20:http     CLOSE_WAIT
  TCP    210.32.153.95:54373    115.231.21.20:http     CLOSE_WAIT
  TCP    210.32.153.95:54374    115.231.21.20:http     CLOSE_WAIT
  TCP    210.32.153.95:54545    125.88.200.229:http    ESTABLISHED
  TCP    210.32.153.95:62550    a-0011:https           TIME_WAIT
  TCP    210.32.153.95:62579    116.211.169.105:https  TIME_WAIT
```

8. 显示本机的路由表信息，并手工添加一个路由：**Route.exe**

```
C:\Users\laylalaisy>route print
===========================================================================
接口列表
 12...32 52 cb e8 0a 61 ......Microsoft Wi-Fi Direct Virtual Adapter
  3...00 e0 4c 68 13 9a ......Realtek USB GbE Family Controller
 49.....................SRun3K专用宽带拨号连接
  2...00 ff 1b 49 eb 4e ......Sangfor SSL VPN CS Support System VNIC
 18...30 52 cb e8 0a 61 ......Dell Wireless 1820A 802.11ac
 10...30 52 cb e8 0a 62 ......Bluetooth Device (Personal Area Network)
  1.....................Software Loopback Interface 1
  5...00 00 00 00 00 00 00 e0 Teredo Tunneling Pseudo-Interface
===========================================================================

IPv4 路由表
===========================================================================
活动路由:
网络目标        网络掩码          网关       接口   跃点数
          0.0.0.0          0.0.0.0      10.110.37.1     10.110.37.55   4516
          0.0.0.0          0.0.0.0            在链路上     210.32.153.95     36
         10.0.0.0        255.0.0.0      10.110.37.1     10.110.37.55   4561
       10.0.2.72  255.255.255.255      10.110.37.1     10.110.37.55   4261
     10.110.37.0    255.255.255.0            在链路上      10.110.37.55   4516
    10.110.37.55  255.255.255.255            在链路上      10.110.37.55   4516
   10.110.37.255  255.255.255.255            在链路上      10.110.37.55   4516
     58.196.64.0    255.255.255.0      10.110.37.1     10.110.37.55   4561
    58.196.224.0    255.255.240.0      10.110.37.1     10.110.37.55   4561
    58.196.224.0    255.255.255.0      10.110.37.1     10.110.37.55   4561
       127.0.0.0        255.0.0.0            在链路上        127.0.0.1   4556
       127.0.0.1  255.255.255.255            在链路上        127.0.0.1   4556
 127.255.255.255  255.255.255.255            在链路上        127.0.0.1   4556
     210.32.0.0    255.255.240.0      10.110.37.1     10.110.37.55   4561
     210.32.0.0    255.255.255.0      10.110.37.1     10.110.37.55   4561
   210.32.153.95  255.255.255.255            在链路上     210.32.153.95    291
    210.32.160.0    255.255.255.0      10.110.37.1     10.110.37.55   4561
    210.32.164.0    255.255.255.0      10.110.37.1     10.110.37.55   4561
    210.32.174.0    255.255.255.0      10.110.37.1     10.110.37.55   4561
    210.32.176.0    255.255.240.0      10.110.37.1     10.110.37.55   4561
    210.32.176.0    255.255.255.0      10.110.37.1     10.110.37.55   4561
```

```
    210.32.176.0    255.255.240.0      10.110.37.1     10.110.37.55    4561
    210.32.176.0    255.255.255.0      10.110.37.1     10.110.37.55    4561
     222.205.0.0    255.255.255.0      10.110.37.1     10.110.37.55    4561
       224.0.0.0        240.0.0.0            在链路上         127.0.0.1    4556
       224.0.0.0        240.0.0.0            在链路上      10.110.37.55    4516
       224.0.0.0        240.0.0.0            在链路上     210.32.153.95      36
 255.255.255.255  255.255.255.255            在链路上         127.0.0.1    4556
 255.255.255.255  255.255.255.255            在链路上      10.110.37.55    4516
 255.255.255.255  255.255.255.255            在链路上     210.32.153.95     291
===========================================================================
永久路由:
  网络地址          网络掩码   网关地址   跃点数
          0.0.0.0          0.0.0.0      10.110.37.1     默认
===========================================================================

IPv6 路由表
===========================================================================
活动路由:
 接口跃点数网络目标                  网关
  3    291 ::/0                     fe80::5edd:70ff:fe00:9503
  1    331 ::1/128                  在链路上
  5    331 2001::/32                在链路上
  5    331 2001:0:9d38:6ab8:57:1ce3:2ddf:66a0/128
                                    在链路上
  3    291 2001:da8:e000:1a0a::/64  在链路上
  3    291 2001:da8:e000:1a0a:836:744a:3538:b419/128
                                    在链路上
  3    291 2001:da8:e000:1a0a:14fb:4982:4977:221a/128
                                    在链路上
  3    291 fe80::/64                在链路上
  5    331 fe80::/64                在链路上
  5    331 fe80::57:1ce3:2ddf:66a0/128
                                    在链路上
  3    291 fe80::14fb:4982:4977:221a/128
                                    在链路上
  1    331 ff00::/8                 在链路上
  5    331 ff00::/8                 在链路上
  3    291 ff00::/8                 在链路上
===========================================================================
永久路由:
  无
```

在本次实验中，手动添加了所有到 10.0.0.5/24 网段的数据包通过本机接口。

```
C:\WINDOWS\system32>route add 10.0.0.5 mask 255.255.255.255 10.110.37.55
 操作完成!

C:\WINDOWS\system32>route print
===========================================================================
接口列表
 12...32 52 cb e8 0a 61 ......Microsoft Wi-Fi Direct Virtual Adapter
  3...00 e0 4c 68 13 9a ......Realtek USB GbE Family Controller
 49.....................SRun3K专用宽带拨号连接
  2...00 ff 1b 49 eb 4e ......Sangfor SSL VPN CS Support System VNIC
 18...30 52 cb e8 0a 61 ......Dell Wireless 1820A 802.11ac
 10...30 52 cb e8 0a 62 ......Bluetooth Device (Personal Area Network)
  1.....................Software Loopback Interface 1
  5...00 00 00 00 00 00 00 e0 Teredo Tunneling Pseudo-Interface
===========================================================================

IPv4 路由表
===========================================================================
活动路由:
网络目标        网络掩码          网关       接口   跃点数
          0.0.0.0          0.0.0.0      10.110.37.1    10.110.37.55   4516
          0.0.0.0          0.0.0.0         在链路上     210.32.153.95     36
         10.0.0.0        255.0.0.0      10.110.37.1    10.110.37.55   4561
         10.0.0.5  255.255.255.255         在链路上     10.110.37.55   4261
        10.0.2.72  255.255.255.255      10.110.37.1    10.110.37.55   4261
     10.110.37.0    255.255.255.0         在链路上     10.110.37.55   4516
    10.110.37.55  255.255.255.255         在链路上     10.110.37.55   4516
   10.110.37.255  255.255.255.255         在链路上     10.110.37.55   4516
     58.196.64.0    255.255.255.0      10.110.37.1    10.110.37.55   4561
    58.196.224.0    255.255.240.0      10.110.37.1    10.110.37.55   4561
    58.196.224.0    255.255.255.0      10.110.37.1    10.110.37.55   4561
       127.0.0.0        255.0.0.0         在链路上        127.0.0.1   4556
       127.0.0.1  255.255.255.255         在链路上        127.0.0.1   4556
  127.255.255.255  255.255.255.255         在链路上        127.0.0.1   4556
     210.32.0.0    255.255.240.0      10.110.37.1    10.110.37.55   4561
     210.32.0.0    255.255.255.0      10.110.37.1    10.110.37.55   4561
   210.32.153.95  255.255.255.255         在链路上     210.32.153.95    291
    210.32.160.0    255.255.255.0      10.110.37.1    10.110.37.55   4561
```

9. 显示本机的网络映射连接：**Net.exe**

```
C:\Users\laylalaisy>net use
会记录新的网络连接。

列表是空的。
```

10. 显示局域网内某台机器的共享资源：**Net.exe**

```
C:\Users\laylalaisy>net share

共享名       资源                            注解

-------------------------------------------------------------------------------
--
C$           C:\                             默认共享

IPC$                                         远程 IPC

ADMIN$       C:\WINDOWS                      远程管理

命令成功完成。
```

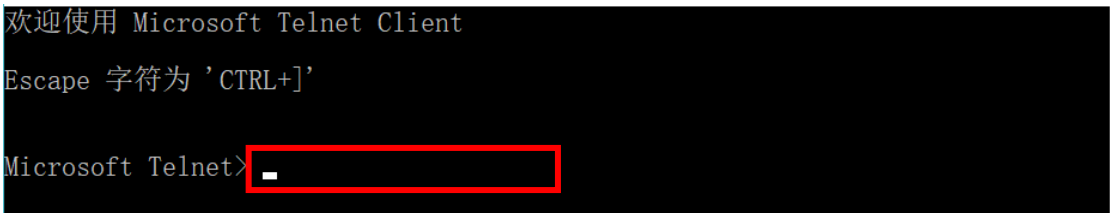
11. 使用 telnet 连接 WEB 服务器的端口，输入（<cr>表示回车）获得该网站的主

页内容：

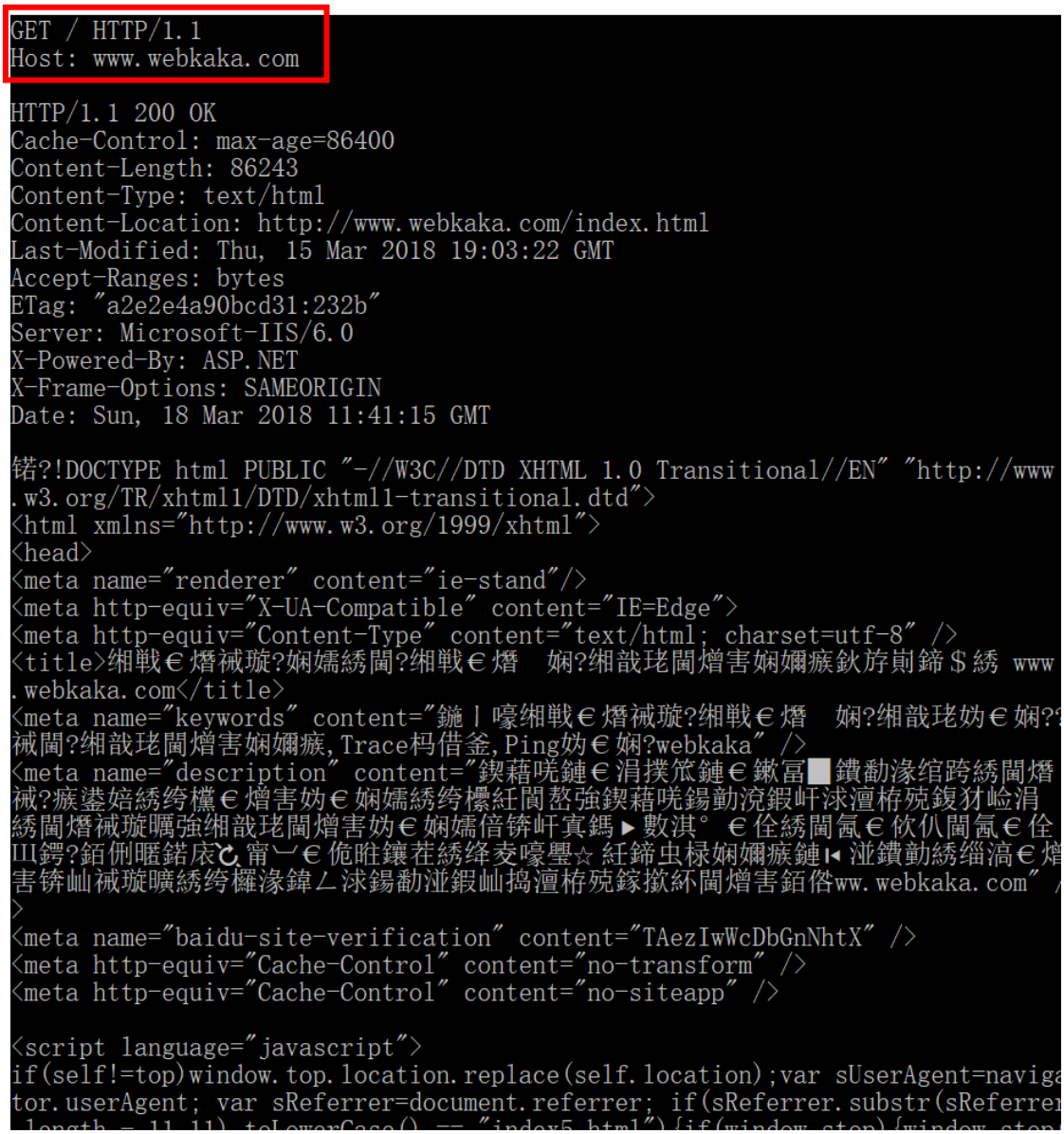
GET / HTTP/1.1<cr>
Host: 任意字符串<cr>
<cr>

（1）使用 telnet 连接 WEB 服务器的端口

（2）按组合键 ctrl +] 然后回车，此时再输入命令将出现在屏幕上。因为 windows 自带的 telnet 在输入内容的时候看不到输入的内容



（3）获得该网站的主页内容



（4）获得某一张网页 HTML 内容

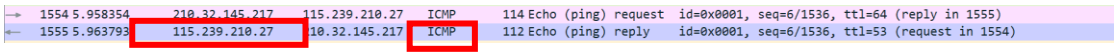
```
GET /demo/checkPC.html HTTP/1.1
Host: www.webkaka.com

HTTP/1.1 200 OK
Cache-Control: max-age=86400
Content-Length: 1108
Content-Type: text/html
Last-Modified: Thu, 18 May 2017 08:52:10 GMT
Accept-Ranges: bytes
ETag: "f2ac6d9b4cfd21:232b"
Server: Microsoft-IIS/6.0
X-Powered-By: ASP.NET
X-Frame-Options: SAMEORIGIN
Date: Sun, 18 Mar 2018 11:38:07 GMT

锘?!DOCTYPE html>
<head>
<meta http-equiv="X-UA-Compatible" content="IE=edge,chrome=1">
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
<title>閫氳繃UA妫€娴嬪櫒鎼风  璁惧  </title>
</head>
<body>
<script>
var os = function() {
     var ua = navigator.userAgent,
     isWindowsPhone = /(?:Windows Phone)/.test(ua),
     isSymbian = /(?:SymbianOS)/.test(ua) || isWindowsPhone,
     isAndroid = /(?:Android)/.test(ua),
     isFireFox = /(?:Firefox)/.test(ua),
     isChrome = /(?:Chrome|CriOS)/.test(ua),
     isTablet = /(?:iPad|PlayBook)/.test(ua) || (isAndroid && !/(?:Mobile)/.t
est(ua)) || (isFireFox && /(?:Tablet)/.test(ua)),
     isPhone = /(?:iPhone)/.test(ua) && !isTablet,
     isPc = !isPhone && !isAndroid && !isSymbian;
     return {
          isTablet: isTablet,
          isPhone: isPhone,
          isAndroid : isAndroid,
          isPc : isPc
     };
}().
```

- **观察使用 Ping 命令时在 WireShark 中出现的数据包并捕获。这是什么协议？**

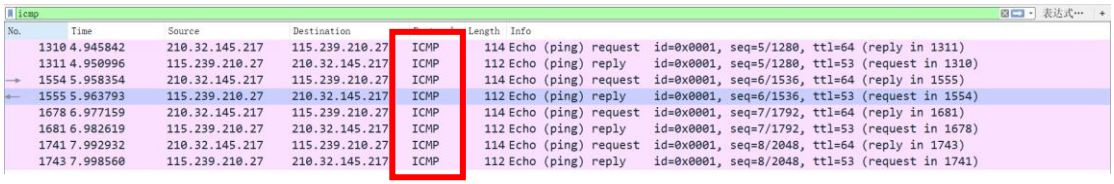
（1）在本实验中使用 ping www.baidu.com，其中 IP 地址为 115.239.210.27；

```
C:\Users\laylalaisy>ping www.baidu.com

正在 Ping www.a.shifen.com [115.239.210.27] 具有 32 字节的数据:
来自 115.239.210.27 的回复: 字节=32 时间=5ms TTL=53
来自 115.239.210.27 的回复: 字节=32 时间=6ms TTL=53
来自 115.239.210.27 的回复: 字节=32 时间=6ms TTL=53
来自 115.239.210.27 的回复: 字节=32 时间=6ms TTL=53

115.239.210.27 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 = 5ms，最长 = 6ms，平均 = 5ms
```

（2）找到对应 IP 地址的数据包，得出 ping 命令时采用的是 ICMP 协议：



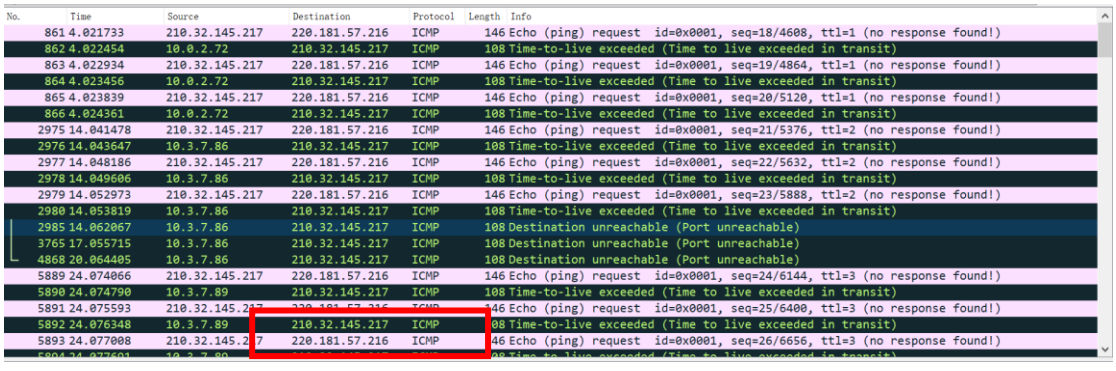
（3）应用显示过滤器，显示 ICMP 协议数据包；



- **观察使用 Tracert 命令时在 WireShark 中出现的数据包并捕获。这是什么协议？**

（1）在本实验中使用 tracert www.baidu.com，其中 IP 地址为 220.181.57.216；

（2）找到对应 IP 地址的数据包，得出 tracert 命令时采用的是 ICMP 协议：



- **观察使用 Nslookup 命令时在 WireShark 中出现的数据包并捕获。这是什么协议？**

（1）首先清空 DNS 的缓存记录；

```
C:\Users\laylalaisy>ipconfig /flushdns

Windows IP 配置

已成功刷新 DNS 解析缓存。
```

（2）在本实验中使用 nslookup www.baidu.com，其中 IP 地址为 10.10.0.21；

```
C:\Users\laylalaisy>nslookup www.baidu.com
服务器:  dns1.zju.edu.cn
Address:  10.10.0.21

非权威应答:
名称:    www.a.shifen.com
Addresses:  115.239.210.27
          115.239.211.112
Aliases:  www.baidu.com
```

（3）找到对应 IP 地址的数据包，得出 nslookup 命令时采用的是 DNS 协议：

No.	Time	Source	Destination	Protocol	Length	Info
1727	27.525441	10.110.37.55	10.10.0.21	DNS	83	Standard query 0x0001 PTR 21.0.10.10.in-addr.arpa

（4）应用显示过滤器，显示 DNS 协议数据包；

dns

No.	Time	Source	Destination	Protocol	Length	Info
1727	27.525441	10.110.37.55	10.10.0.21	DNS	83	Standard query 0x0001 PTR 21.0.10.10.in-addr.arpa
1728	27.526104	10.10.0.21	10.110.37.55	DNS	142	Standard query response 0x0001 PTR 21.0.10.10.in-addr.arpa PTR dns1.zju.edu.cn NS dns…
1729	27.526914	10.110.37.55	10.10.0.21	DNS	73	Standard query 0x0002 A www.baidu.com
1730	27.527823	10.10.0.21	10.110.37.55	DNS	302	Standard query response 0x0002 A www.baidu.com CNAME www.a.shifen.com A 115.239.211.1…
1731	27.528444	10.110.37.55	10.10.0.21	DNS	73	Standard query 0x0003 AAAA www.baidu.com
1732	27.529149	10.10.0.21	10.110.37.55	DNS	157	Standard query response 0x0003 AAAA www.baidu.com CNAME www.a.shifen.com SOA ns1.a.sh…
1733	27.532139	10.110.37.55	10.10.0.21	DNS	83	Standard query 0x30d4 A 21.0.10.10.in-addr.arpa
1734	27.532872	10.10.0.21	10.110.37.55	DNS	139	Standard query response 0x30d4 A 21.0.10.10.in-addr.arpa SOA dns1.zju.edu.cn

- **观察使用 Telnet 命令时在 WireShark 中出现的数据包并捕获。这是什么协议？**

（1）使用 telnet 连接 WEB 服务器的端口并获得主页内容

```
C:\Users\laylalaisy>telnet www.webkaka.com 80
```

```
GET / HTTP/1.1
Host: www.webkaka.com

HTTP/1.1 200 OK
Cache-Control: max-age=86400
Content-Length: 86243
Content-Type: text/html
Content-Location: http://www.webkaka.com/index.html
Last-Modified: Thu, 15 Mar 2018 19:03:22 GMT
Accept-Ranges: bytes
ETag: "a2e2e4a90bcd31:232b"
Server: Microsoft-IIS/6.0
X-Powered-By: ASP.NET
X-Frame-Options: SAMEORIGIN
Date: Sun, 18 Mar 2018 11:41:15 GMT

锘?!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www
.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<meta name="renderer" content="ie-stand"/>
<meta http-equiv="X-UA-Compatible" content="IE=Edge">
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
<title>细戦€熸祴璇?娴嬬綉閫?细戦€熸 娴?细戠珯閫熷害娴嬭瘯鈥斿崕鍗＄綉 www
.webkaka.com</title>
<meta name="keywords" content="鍦ㄧ嚎细戦€熸祴璇?细戦€熸 娴?细戠珯妫€娴?
祴閫?细戠珯閫熷害娴嬭瘯,Trace杩借釜,Ping妫€娴?webkaka" />
<meta name="description" content="鍥藉唴鏈€涓撲笟鏈€鍬冨█鐨勭綉绔欓熸
祴?瘯鍙婄綉绔欐€熷害妫€娴嬬綉绔欐紑閫熸強鍥藉唴鍚勫湴鍖哄埌鏂欓
綉閫熸祴璇曞細戠珯閫熷害妫€娴嬪伐鍏寓鏁版嵁...
...
ww.webkaka.com" /
>
<meta name="baidu-site-verification" content="TAezIwWcDbGnNhtX" />
<meta http-equiv="Cache-Control" content="no-transform" />
<meta http-equiv="Cache-Control" content="no-siteapp" />

<script language="javascript">
if(self!=top)window.top.location.replace(self.location);var sUserAgent=naviga
tor.userAgent; var sReferrer=document.referrer; if(sReferrer.substr(sReferre
```

（2）找到对应 IP 地址 211.149.163.240：

```
C:\Users\laylalaisy>ping www.webkaka.com

正在 Ping s-340253.abc188.com [211.149.163.240] 具有 32 字节的数据:
来自 211.149.163.240 的回复: 字节=32 时间=42ms TTL=118
来自 211.149.163.240 的回复: 字节=32 时间=42ms TTL=118
来自 211.149.163.240 的回复: 字节=32 时间=42ms TTL=118
来自 211.149.163.240 的回复: 字节=32 时间=42ms TTL=118

211.149.163.240 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 = 42ms，最长 = 42ms，平均 = 42ms
```

（3）找到对应 IP 地址的数据协议：

185	3.188596	10.180.86.0	211.149.163.240	TCP	74	49841→80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1 TSval=239402 TSe
186	3.233641	211.149.163.240	10.180.86.0	TCP	78	80→49841 [SYN, ACK] Seq=0 Ack=1 Win=16384 Len=0 MSS=1460 WS=1 TSval=0 TSecr=0 SAC
187	3.233777	10.180.86.0	211.149.163.240	TCP	66	49841→80 [ACK] Seq=1 Ack=1 Win=66560 Len=0 TSval=239447 TSecr=0

六、 实验结果与分析

- WireShark 的两种过滤器有什么不同？

（1） 捕获过滤器：进行包捕获时进行过滤，只捕获过滤规则之内的数据包；

（2） 显示过滤器：在捕获数据包之后，只显示过滤规则之内的数据包；

- 哪些网络命令会产生在 WireShark 中产生数据包，为什么？

综合本次实验可以得出：

（1） Ping 命令：ICMP 协议；

（2） Tracert 命令：ICMP 协议；

（3） Nslookup 命令：DNS 协议；

（4） Telnet 命令：TCP 协议；

其产生数据包的原因是这些命令会使数据报文进行交换，而 Wireshark 使用 WinPCAP 作为接口，直接与网卡进行数据报文交换，从而完成网络封包分析的功能。

- Ping 发送的是什么类型的协议数据包？什么时候会出现 ARP 消息？Ping 一个域名和 Ping 一个 IP 地址出现的数据包有什么不同？

（1）Ping 发送的数据包是 ICMP 类型。

（2）ARP 是消息解析协议，当需要根据 IP 地址获取物理地址且在 ARP 缓存中没有找到映射的时候就会产生 ARP 消息。

（3）首先域名和 IP 并不是一一对应的关系；因此当 ping 域名的时候可以得到一个 IP 为目标，也可能得到域名的多负载不同的 IP；但是 ping ip 的时候得到的是整个服务器，而不是某一个域名。

七、 讨论、心得

本次实验中总体来说，通过学习 WireShark 网上教程以及对有关指令进行搜索可以完成。在实验过程中遇到最大的困难来自于 telnet，由于是第一次在 windows 上使用 telnet，因此最开始的时候没有意识到 telnet 需要手动开启。在搜索了相关教程并开启 telnet 之后，发现经常出现 23 端口，连接失败的错误。后来发现是由于很多网站并不支持 telnet 远程连接而不是本机 telnet 的安装错误。同时由于 windows 自带的 telnet 在输入内容的时候看不到输入的内容，参考相关教程后按组合键 ctrl +] 然后回车，此时再

输入命令将出现在屏幕上。最后完成该部分有关 telnet 的实验要求，并且通过 GET 指定 html 可以获得非主页的其他网页的内容。