浙江大学

本科实验报告

课程名称：	计算机网络基础
姓　　名：	蔡佳伟
学　　院：	计算机科学与技术学院
系：	计算机科学与技术学系
专　　业：	软件工程
学　　号：	3220104519
指导教师：	高艺

2024 年 9 月 13 日

浙江大学实验报告

课程名称：计算机网络基础 实验类型：操作实验

实验项目名称：WireShark 软件初探和常见网络命令的使用

学生姓名：蔡佳伟 专业：软件工程 学号：3220104519

同组学生姓名： 指导老师：高艺

实验地点：计算机网络实验室 实验日期：2024 年 9 月 13 日

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>
```

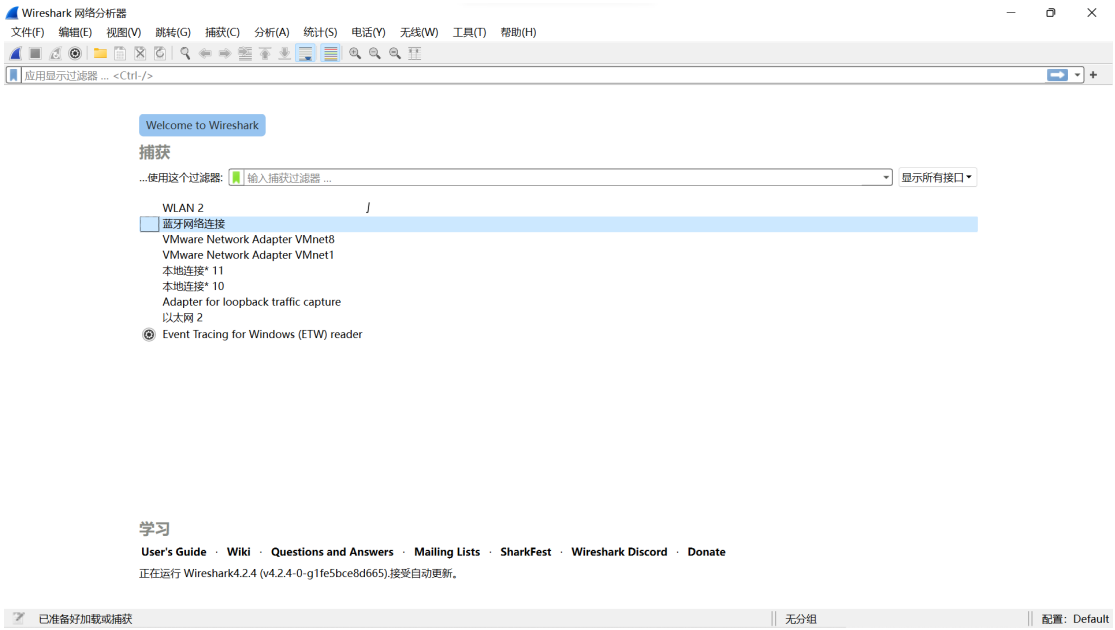
- 利用 WireShark 实时观察在执行上述命令时，哪些命令会额外产生数据包，并记录这些数据包的种类。

五、 实验数据记录和处理

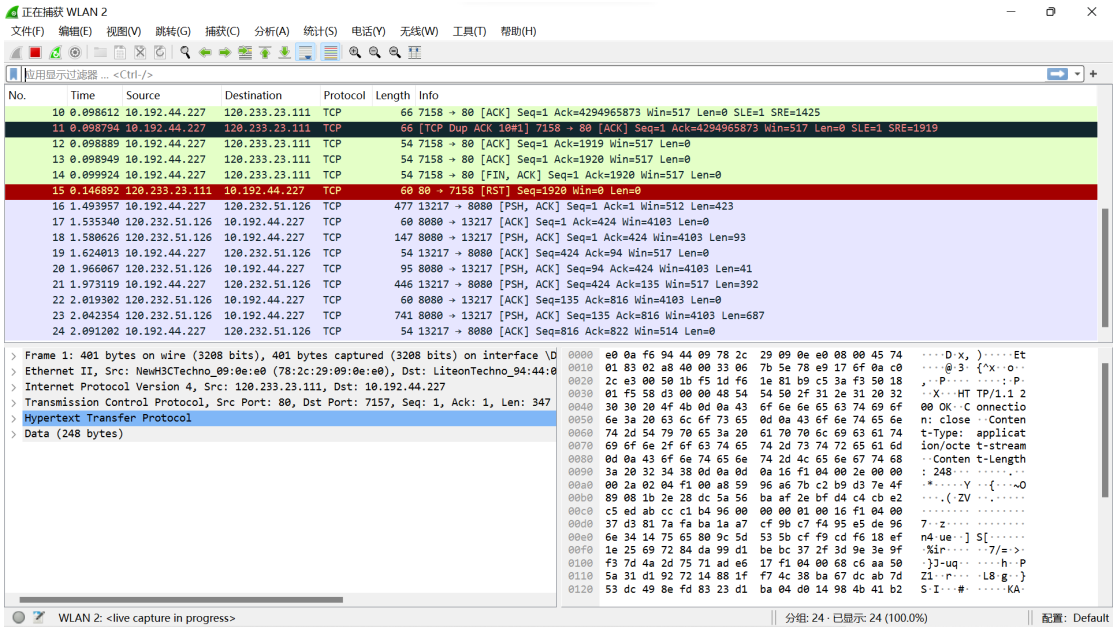
- **运行 Wireshark 软件，界面是由哪几个部分构成？各有什么作用？**

Wireshark 软件界面主要由下面几个部分构成：

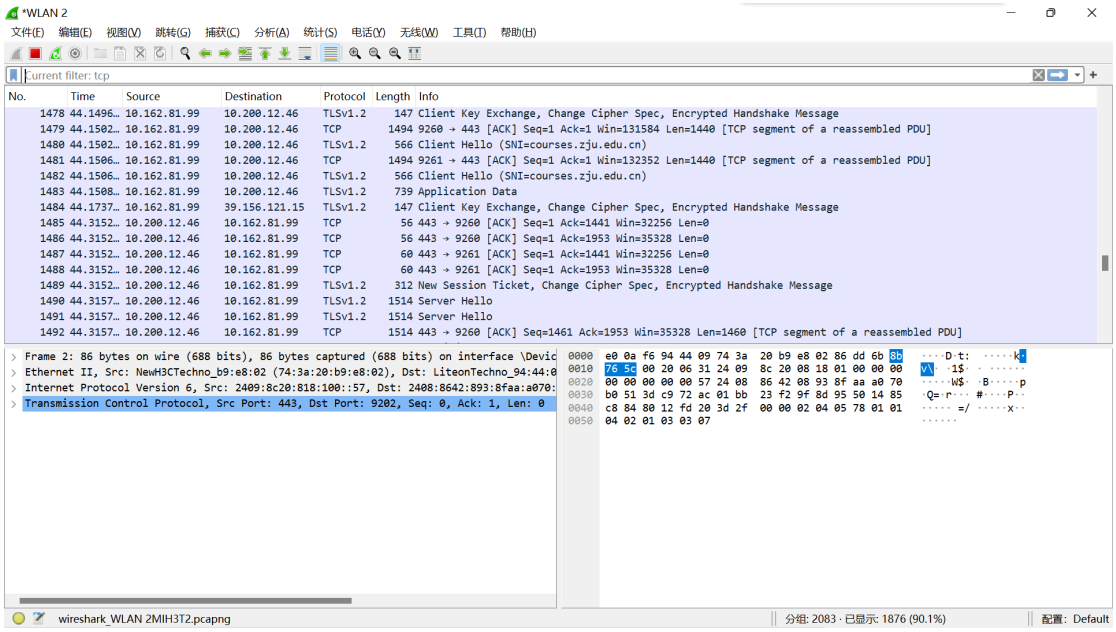
初始界面如下：主界面上有打开历史捕获流量文件和新建捕获两个部分。上方主工具栏有捕获、暂停、 重新开始、捕获选项、打开、保存、关闭、重新加载、查找、一系列跳转选项，工具栏 下面是过滤器工具栏，以及一些调整视图的选项。下面的大部分空白区域是主界面，可以选择筛选特定类型的数据包。（如 WIFI 相关的数据包）



开始捕获以后，界面如下：上方工具栏保持不变，但主界面显示捕获或加载的数据包列表和数据包的详细信息。主界面底部是详情，显示所选数据包的详细信息。整个窗口底部是状态栏，显示有关捕获进程，过滤器状态，数据报数量等信息。



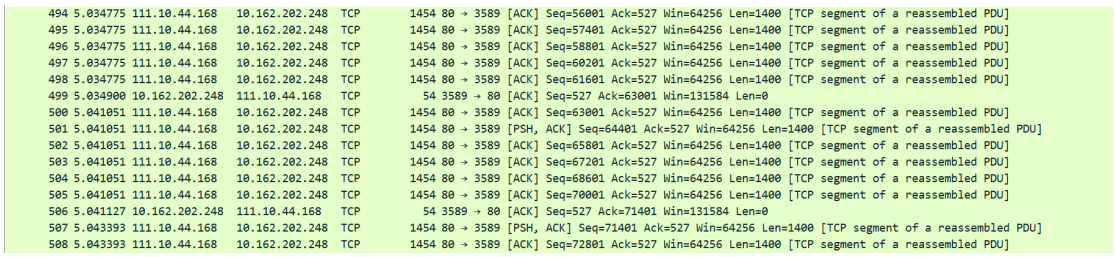
- 开始捕获网络数据包，你看到了什么？有哪些协议？



捕获到了很多数据包，包含了很多信息。包括：源地址和目标地址，协议，数据包大小，数据包信息等。

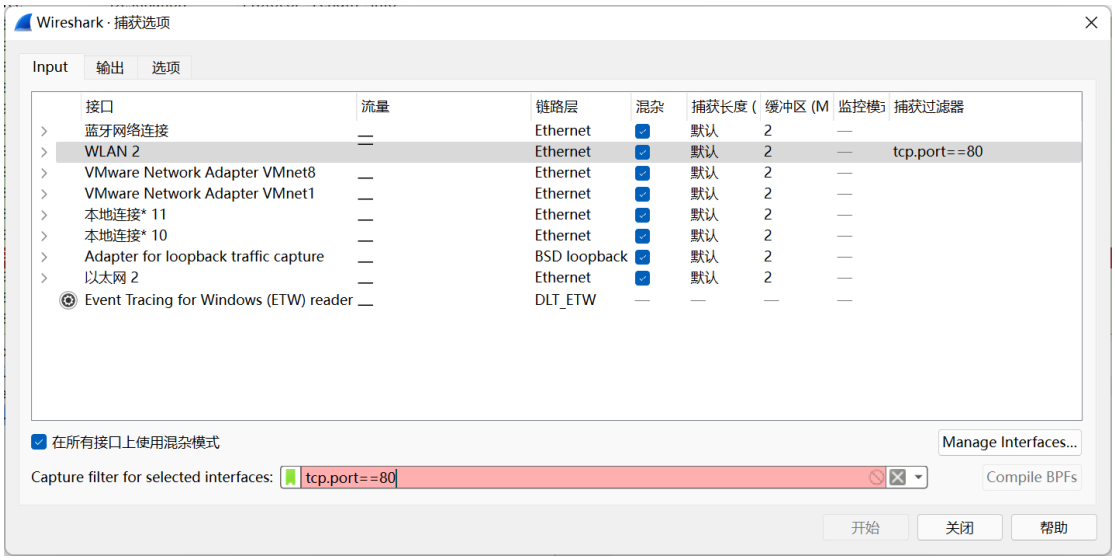
协议名：TCP、ICMP、TLSv1.2，DNS 等。

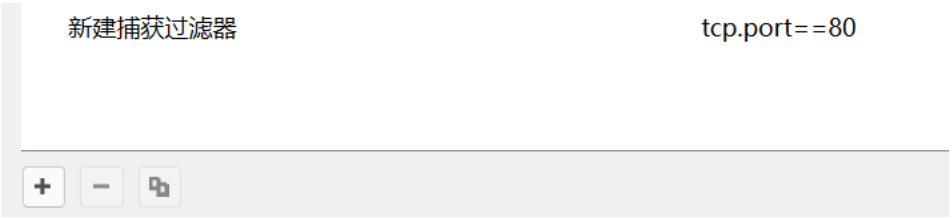
- 配置应用显示过滤器，让界面只显示某一协议类型的数据包。

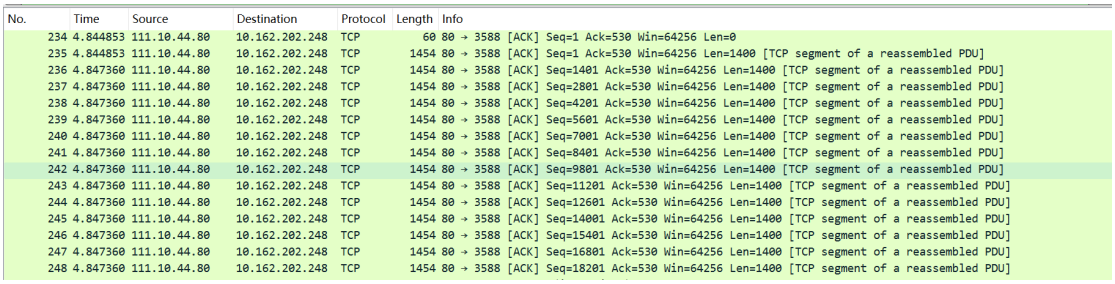


这里我设置显示过滤器为 TCP，可以看到此时显示的都是 TCP 协议类型的数据包。

- **配置捕获过滤器，只捕获某类协议的数据包。**







这里我设置捕获过滤器为 tcp.port==80,即可捕获到 TCP 协议类型的数据包。

- **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。**
- 1. 测试到特定地址的联通性、数据包延迟时间

```
C:\Users\Administrator>ping 10.12.86.210

正在 Ping 10.12.86.210 具有 32 字节的数据:
来自 10.12.86.210 的回复: 字节=32 时间=19ms TTL=59
来自 10.12.86.210 的回复: 字节=32 时间=12ms TTL=59
来自 10.12.86.210 的回复: 字节=32 时间=34ms TTL=59
来自 10.12.86.210 的回复: 字节=32 时间=23ms TTL=59

10.12.86.210 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 = 12ms, 最长 = 34ms, 平均 = 22ms
```

这里我们输入ping 10.12.86.210测试到这个地址的连通性和数据包延迟时间，结果如图。这里可以看到发送的 ICMP 包得到回复，说明联通。

- 2. 显示本机的网卡物理地址、IP 地址

```
C:\Users\Administrator>ipconfig/all
```

```
无线局域网适配器 WLAN 2:

   连接特定的 DNS 后缀 . . . . . . . :
   描述. . . . . . . . . . . . . . . : Realtek RTL8852BE WiFi 6 802.11ax PCIe Adapter
   物理地址. . . . . . . . . . . . . : E0-0A-F6-94-44-09
   DHCP 已启用 . . . . . . . . . . . : 是
   自动配置已启用. . . . . . . . . . : 是
   本地链接 IPv6 地址. . . . . . . . : fe80::fcc3:f17d:e22d:40ac%12(首选)
   IPv4 地址 . . . . . . . . . . . . : 10.192.44.227(首选)
   子网掩码 . . . . . . . . . . . . : 255.255.0.0
   获得租约的时间  . . . . . . . . . : 2024年9月19日 9:43:18
   租约过期的时间  . . . . . . . . . : 2024年9月19日 14:14:21
   默认网关. . . . . . . . . . . . . : 10.192.0.1
   DHCP 服务器 . . . . . . . . . . . : 10.192.0.1
   DHCPv6 IAID . . . . . . . . . . . : 383781622
   DHCPv6 客户端 DUID  . . . . . . . : 00-01-00-01-2D-F5-7F-F3-E0-0A-F6-94-44-09
   DNS 服务器  . . . . . . . . . . . : 10.10.0.21
                                       10.10.2.21
   TCPIP 上的 NetBIOS  . . . . . . . : 已启用
```

使用指令 ipconfig/all，可以看到物理地址是 E0-0A-F6-94-44-09，IPv4 地址是 10.192.44.227

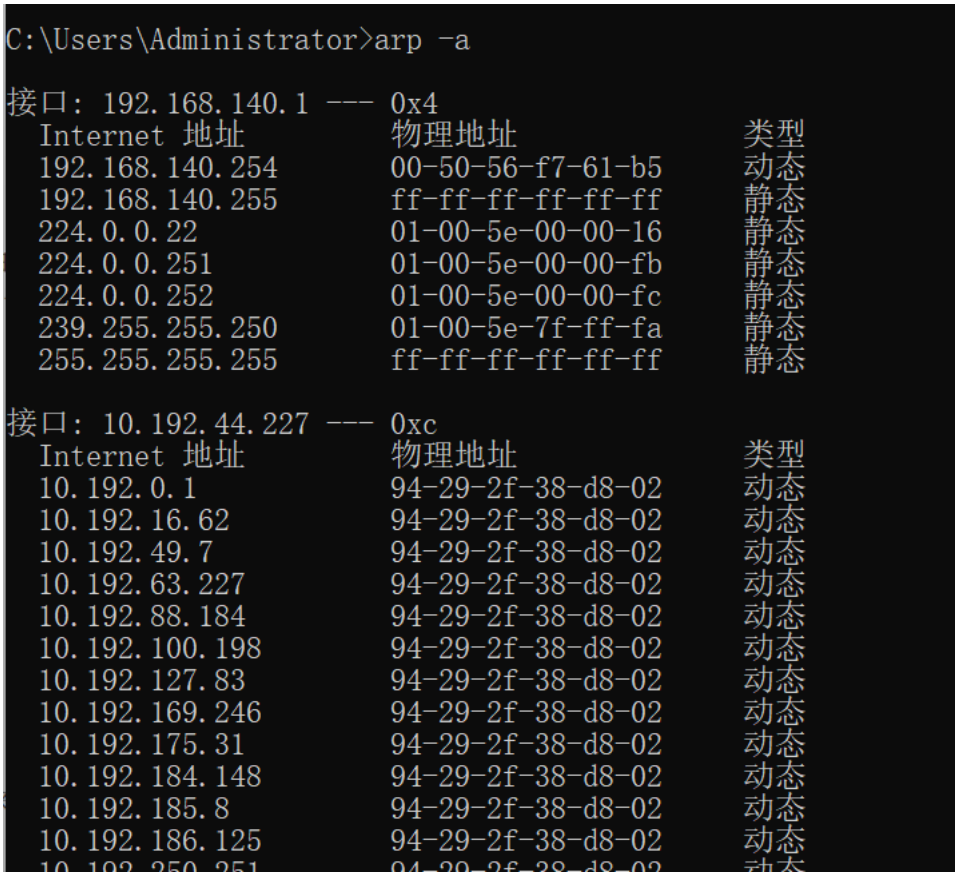
- 3. 显示本机的默认网关地址、DNS 服务器地址

```
无线局域网适配器 WLAN 2:

   连接特定的 DNS 后缀 . . . . . . . :
   描述. . . . . . . . . . . . . . . : Realtek RTL8852BE WiFi 6 802.11ax PCIe Adapter
   物理地址. . . . . . . . . . . . . : E0-0A-F6-94-44-09
   DHCP 已启用 . . . . . . . . . . . : 是
   自动配置已启用. . . . . . . . . . : 是
   本地链接 IPv6 地址. . . . . . . . : fe80::fcc3:f17d:e22d:40ac%12(首选)
   IPv4 地址 . . . . . . . . . . . . : 10.192.44.227(首选)
   子网掩码 . . . . . . . . . . . . : 255.255.0.0
   获得租约的时间  . . . . . . . . . : 2024年9月19日 9:43:18
   租约过期的时间  . . . . . . . . . : 2024年9月19日 14:14:21
   默认网关. . . . . . . . . . . . . : 10.192.0.1
   DHCP 服务器 . . . . . . . . . . . : 10.192.0.1
   DHCPv6 IAID . . . . . . . . . . . : 383781622
   DHCPv6 客户端 DUID  . . . . . . . : 00-01-00-01-2D-F5-7F-F3-E0-0A-F6-94-44-09
   DNS 服务器  . . . . . . . . . . . : 10.10.0.21
                                       10.10.2.21
   TCPIP 上的 NetBIOS  . . . . . . . : 已启用
```

指令同 2，可以看到默认网关是 10.192.0.1，DNS 服务器地址是 10.10.0.21，10.10.2.21

- 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

输入 arp –a 命令，即可查看本机记录的局域网内其他机器 IP 地址与其物理地址的对照表，如下图所示。

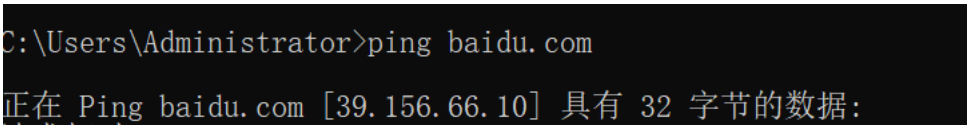


- 5. 显示从本机到达一个特定地址的路由

在终端输入 tracert xxx.com 即可查看本机到一个特定地址的路由。这里查看 baidu.com 的。

- 6. 显示某一个域名的 IP 地址

通过 ping 命令来显示域名的 IP 地址。这里我们通过 ping baidu.com 来查询百度的 ip 地址，如图。



可以看到地址是 39.156.66.10

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

非权威应答:
名称:    baidu.com
Addresses:  110.242.68.66
          39.156.66.10
```

- 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

在终端输入 netstat –an 命令，并通过管道传给 findstr “tcp” 和 findstr “ESTABILISHED” 即可看到已经与本机建立 TCP 连接的端口、IP 地址、连接状态等信息，如下图所示。

```
  TCP    10.192.44.227:5922     103.212.12.47:3000     ESTABLISHED
  TCP    10.192.44.227:5928     118.31.76.243:443      ESTABLISHED
  TCP    10.192.44.227:5933     10.10.98.98:443        ESTABLISHED
  TCP    10.192.44.227:5960     120.192.82.80:443      ESTABLISHED
  TCP    10.192.44.227:5974     111.0.39.81:443        ESTABLISHED
  TCP    10.192.44.227:5984     20.198.167.116:443     ESTABLISHED
  TCP    10.192.44.227:5985     111.0.39.81:443        ESTABLISHED
  TCP    10.192.44.227:5999     202.89.233.101:443     ESTABLISHED
  TCP    10.192.44.227:6000     112.13.92.196:443      ESTABLISHED
  TCP    10.192.44.227:13213    183.134.28.238:443     ESTABLISHED
  TCP    10.192.44.227:13217    120.232.51.126:8080    ESTABLISHED
  TCP    10.192.44.227:13227    104.18.39.102:443      ESTABLISHED
  TCP    10.192.44.227:13236    20.187.186.89:443      ESTABLISHED
  TCP    10.192.44.227:49415    20.197.71.89:443       ESTABLISHED
  TCP    127.0.0.1:1025         127.0.0.1:5354         ESTABLISHED
  TCP    127.0.0.1:1026         127.0.0.1:5354         ESTABLISHED
  TCP    127.0.0.1:1028         0.0.0.0:0              LISTENING
  TCP    127.0.0.1:1030         127.0.0.1:1031         ESTABLISHED
  TCP    127.0.0.1:1031         127.0.0.1:1030         ESTABLISHED
  TCP    127.0.0.1:1032         127.0.0.1:1033         ESTABLISHED
  TCP    127.0.0.1:1033         127.0.0.1:1032         ESTABLISHED
  TCP    127.0.0.1:1035         127.0.0.1:1036         ESTABLISHED
  TCP    127.0.0.1:1036         127.0.0.1:1035         ESTABLISHED
  TCP    127.0.0.1:1048         127.0.0.1:16308        ESTABLISHED
  TCP    127.0.0.1:1054         0.0.0.0:0              LISTENING
  TCP    127.0.0.1:1054         127.0.0.1:13197        ESTABLISHED
  TCP    127.0.0.1:1054         127.0.0.1:13220        ESTABLISHED
  TCP    127.0.0.1:5283         0.0.0.0:0              LISTENING
  TCP    127.0.0.1:5354         0.0.0.0:0              LISTENING
```

这里输入的是 netstat –an 命令，可以看到 ESTABLISHED 就是与本机建立了连接的信息。

输出顺序是：协议-本地地址-外部地址-状态

- 8. 显示本机的路由表信息，并手工添加一个路由

在终端中输入 route print 指令查看所有路由，结果如下图所示

```
C:\Users\Administrator>route print
===========================================================================
接口列表
 13...e2 0a f6 94 44 09 ......Microsoft Wi-Fi Direct Virtual Adapter #2
  8...f2 0a f6 94 44 09 ......Microsoft Wi-Fi Direct Virtual Adapter #3
  4...00 50 56 c0 00 01 ......VMware Virtual Ethernet Adapter for VMnet1
 17...00 50 56 c0 00 08 ......VMware Virtual Ethernet Adapter for VMnet8
 12...e0 0a f6 94 44 09 ......Realtek RTL8852BE WiFi 6 802.11ax PCIe Adapter
 10...00 ff 51 52 4b 32 ......Sangfor SSL VPN CS Support System VNIC
  2...e0 0a f6 94 44 0a ......Bluetooth Device (Personal Area Network)
  1...........................Software Loopback Interface 1
===========================================================================

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      10.192.0.1   10.192.44.227     35
       10.192.0.0      255.255.0.0         在链路上      10.192.44.227    291
    10.192.44.227  255.255.255.255         在链路上      10.192.44.227    291
   10.192.255.255  255.255.255.255         在链路上      10.192.44.227    291
        127.0.0.0        255.0.0.0         在链路上          127.0.0.1    331
        127.0.0.1  255.255.255.255         在链路上          127.0.0.1    331
  127.255.255.255  255.255.255.255         在链路上          127.0.0.1    331
    192.168.59.0    255.255.255.0         在链路上      192.168.59.1    291
    192.168.59.1  255.255.255.255         在链路上      192.168.59.1    291
  192.168.59.255  255.255.255.255         在链路上      192.168.59.1    291
  192.168.140.0    255.255.255.0         在链路上      192.168.140.1    291
```

```
  192.168.140.1  255.255.255.255         在链路上      192.168.140.1    291
192.168.140.255  255.255.255.255         在链路上      192.168.140.1    291
        224.0.0.0        240.0.0.0         在链路上          127.0.0.1    331
        224.0.0.0        240.0.0.0         在链路上      192.168.140.1    291
        224.0.0.0        240.0.0.0         在链路上       192.168.59.1    291
        224.0.0.0        240.0.0.0         在链路上      10.192.44.227    291
  255.255.255.255  255.255.255.255         在链路上          127.0.0.1    331
  255.255.255.255  255.255.255.255         在链路上      192.168.140.1    291
  255.255.255.255  255.255.255.255         在链路上       192.168.59.1    291
  255.255.255.255  255.255.255.255         在链路上      10.192.44.227    291
===========================================================================
永久路由:
  无

IPv6 路由表
===========================================================================
活动路由:
 接口跃点数网络目标                网关
  1    331 ::1/128                  在链路上
  4    291 fe80::/64                在链路上
 17    291 fe80::/64                在链路上
 12    291 fe80::/64                在链路上
  4    291 fe80::217c:6e0a:4a76:cfe3/128
                                    在链路上
 17    291 fe80::38d4:bfe2:daad:d131/128
                                    在链路上
 12    291 fe80::fcc3:f17d:e22d:40ac/128
                                    在链路上
```

```
                                    在链路上
  1    331 ff00::/8                 在链路上
  4    291 ff00::/8                 在链路上
 17    291 ff00::/8                 在链路上
 12    291 ff00::/8                 在链路上
===========================================================================
永久路由:
  无
```

我们通过 route add 10.253.251.0 mask 255.255.255.0 -p 192.254.1.1 命令手工添加路由，这 里 10.253.251.0 是源地址，255.255.255.0 是源地址掩码，192.254.1.1 是目标地址。我们通过 route print 查看路由，可以看到手工添加路由成功。

```
C:\Users\Administrator>route add 10.253.251.0 mask 255.255.255.0 -p 192.254.1.1
操作完成!
```

```
永久路由:
  网络地址          网络掩码  网关地址   跃点数
    10.253.251.0    255.255.255.0       192.254.1.1        1
===========================================================================
```

- 9. 显示本机的网络映射连接

在终端输入 net use 命令来显示本机的网络映射连接。

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

列表是空的。
```

后来我完成第十题后，再次输入 net use 命令，看到不同结果。

```
PS C:\Users\jin> net use \\MUZIBING\IPC$ "040517cc" /USER:"jin"
命令成功完成。

PS C:\Users\jin> net use
会记录新的网络连接。


状态       本地        远程                    网络

-------------------------------------------------------------------------------
OK                     \\MUZIBING\IPC$         Microsoft Windows Network
命令成功完成。

PS C:\Users\jin>
```

- 10. 显示局域网内某台机器的共享资源

这里我将自己（MUZIBING）和室友（jin）的电脑同时接入手机热点，并将自己电脑上的部分文件设为共享，创建实验环境。接着在室友电脑终端输入 net use \\[computername]\ipc$ “password” /user:”user name” 建立连接（computername 设共享的时候在第一个的就是） 随后 net view \\[computername]即可。这里可以看到成功建立了连接。


```
NET USE {devicename | *} [password | *] /HOME

NET USE [/PERSISTENT:{YES | NO}]


C:\Users\jin>net use \\MUZIBING\IPC$ "040517cc" /USER:"jin"
命令成功完成。


C:\Users\jin>net view \\MUZIBING
在 \\MUZIBING 的共享资源


共享名   类型   使用为   注释

-------------------------------------------------------------------------------
Users    Disk
命令成功完成。


C:\Users\jin>
```

- 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：

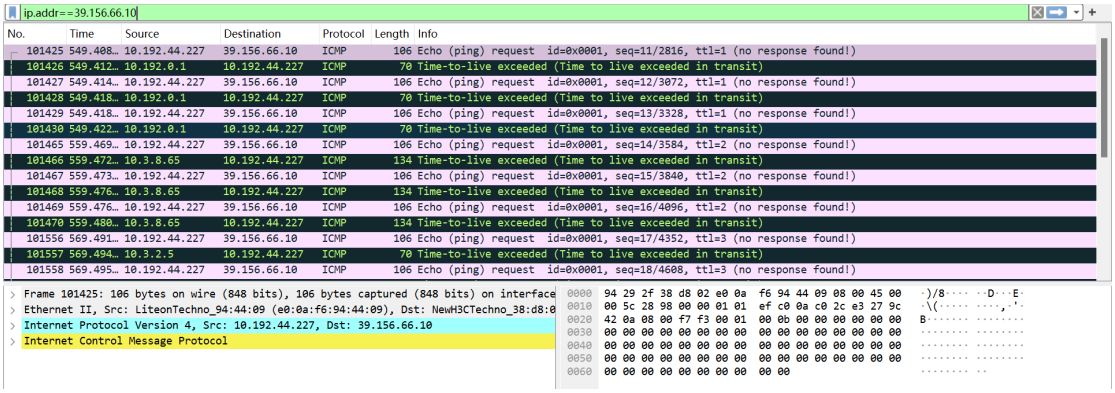
在终端输入 telnet www.baidu.com 80，随后敲入 ctrl+]，并敲击回车进入 telnet。随后输入 GET / HTTP/1.1 和 Host:www.baidu.com 两行命令，可以看到如下输出。

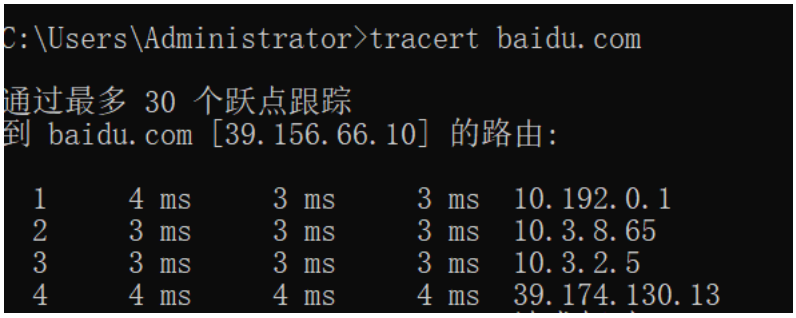
```
GET / HTTP/1.1
Host: www.baidu.com

HTTP/1.1 200 OK
Date: Sun, 01 Oct 2023 11:36:51 GMT
Server: Apache
Last-Modified: Tue, 12 Jan 2010 13:48:00 GMT
ETag: "51-47cf7e6ee8400"
Accept-Ranges: bytes
Content-Length: 81
Cache-Control: max-age=86400
Expires: Mon, 02 Oct 2023 11:36:51 GMT
Connection: Keep-Alive
Content-Type: text/html

<html>
      <meta http-equiv="refresh" content="0;url=http://www.baidu.com/">
                                                                    </html>
```

- **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？**

通过设置显示捕获器，我们捕获了执行 ping 10.12.86.210 时出现的数据包，可以看到这是 ICMP 协议的数据包。ICMP 用于在 IP 网络中传递控制消息和错误消息。Ping 命令实际上是 ICMP Echo 请求和响应的发送和接收过程。

- **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？**

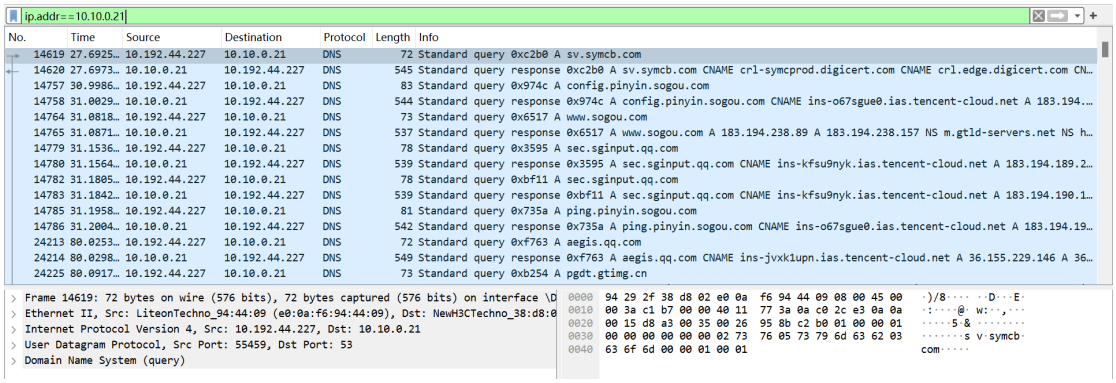


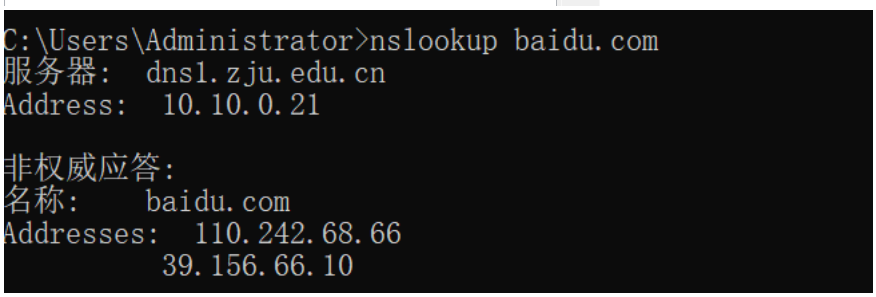


通过设置显示捕获器，我们捕获了执行 tracert baidu.com（IP 地址为 39.156.66.10） 时 出现的数据包。可以看到这也是 ICMP 协议的数据包。

当使用 Tracert（或 Traceroute）命令时，在 Wireshark 中出现的数据包属于 ICMP（Internet Control Message Protocol）协议。Tracert 是一种网络诊断工具，用于跟踪数据包在网络中的路径，并显示每个路由器或中间节点的延迟时间。

- **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？**





执行指令 nslookup baidu.com 时，可以看到 wireshark 中出现了 DNS 协议的数据包，且 info 里包含了 baidu.com。

DNS 是一种用于域名解析的协议，它将域名映射到 IP 地址，以便计算机能够在网络上找到其他设备。当你运行 nslookup 命令并指定要查询的域名时，计算机会向 DNS 服务器发送 DNS 查询请求，以获取该域名对应的 IP 地址

- **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？**

在执行上面的第十一个功能时，我们可以看到 wireshark 中捕获了 TCP 协议和 HTTP 协议的数据包。Wireshark 可以捕获并显示这些 Telnet 通信的 TCP 数据包，包括 TCP 连接的建立、HTTP 请求的发送以及从 Web 服务器返回的 HTTP 响应。

六、 实验结果与分析

- WireShark 的两种过滤器有什么不同？

1. 显示过滤器

显示过滤器用于在 Wireshark 的用户界面过滤和显示已经捕获到的数据包，它只会影响我们在 Wireshark 中看到的数据包，而不会影响包的捕获。它用于在已经捕获的数据包中筛选、搜索、过滤或突出显示特定类型的数据包，以帮助用户更容易地分析网络流量。

2. 捕获过滤器

捕获过滤器在数据包捕获开始之前定义要捕获的数据包类型，它实际影响包的捕获，可以用来减少捕获的数据量，来节省存储和分析时间，大量不必要的数据包不会被捕获记录。

- 哪些网络命令会产生在 WireShark 中产生数据包，为什么？

1. Ping 命令

当使用 ping 命令测试到特定主机的连接性时，它会发送 ICMP Echo 请求数据包到目标主机，并接收来自目标主机的 ICMP Echo 响应数据包。

2. Tracert 命令

使用 tracert 命令来跟踪数据包从源到目标的路径。它会发送一系列的 ICMP Echo 请求数据包。

3. Telnet 命令

当使用 Telne 等远程登录协议连接到远程主机时，会建立 TCP 连接，并在该连接上传输命令和响应

4. HTTP 或 HTTPS 请求

当使用 Web 浏览器或其他 HTTP 客户端发送 HTTP 或 HTTPS 请求时，会触发 TCP 连接并发送 HTTP 请求数据包到 Web 服务器。Web 服务器会返回 HTTP 响应数据包。这些数据包可见于 Wireshark，用于查看 Web 通信，包括请求和响应。

5. Nslookup 命令

使用 nslookup 查询域名时，通常会触发 DNS 查询，因此会生成 DNS 查询数据包。这些 DNS 查询数据包将用于获得域名的 IP 地址或其他相关信息。

6. Arp 命令

如果 ARP 缓存表中不存在对应的目标网络，源计算机就会发出 ARP 请求，QrP 请求就是将自己的 IP 地址和希望得到的 MAC 地址的目标计算机的 IP 地址包装成数据包，通过广播发出去，当目标计算机接收到这个数据包后会将源 IP 地址取出来，

将自己的 MAC 地址包装成数据包发送回去。

- 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 发送的是 ICMP 协议数据包。

2.ping 目标主机的 IP 地址，当本地计算机不知道目标主机的 MAC 地址时会出现 ARP 消息。这是为了构建要发送到目标主机的数据包。

3.ping 一个域名：首先会使用 DNS 解析该域名，将域名转换为 IP 地址。然后会发送 ICMP Echo 请求数据包到得到的 IP 地址。在整个过程中，会出现 DNS 请求和响应的数据包，以及 ICMP Echo 请求和响应的数据包。

Ping 一个 IP 地址：直接发送 ICMP Echo 请求数据包到这个 IP 地址。在整个过程中，没有 DNS 请求和响应的数据包，只有 ICMP Echo 请求和响应的数据包。

七、 讨论、心得

整个过程中，最大的困难在于对实验步骤和目的非常陌生。看上去理论和实验关系不大，同时我虽然上过《信息安全原理》，比较熟悉 Wireshark，但是对每个操作的目的也感到十分陌生。希望理论和实验的关系会大一点，不过第一个实验可能难以避免这种脱节的情况。整个过程中，对我帮助最大的是 GPT 和百度。不过也还是了解到了一些网络相关的知识。

求捞捞 o(╥﹏╥)o