浙江大学

本科实验报告

课程名称：	计算机网络基础
姓　　名：	姚熙源
学　　院：	计算机学院
系：	计算机科学与技术
专　　业：	软件工程
学　　号：	3190300677
指导教师：	董玮

2022 年　　2 月　　24 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：姚熙源 专业：软件工程 学号：3190300677

同组学生姓名：- 指导老师：董玮

实验地点：计算机网络实验室 实验日期：2022 年 2 月 24 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

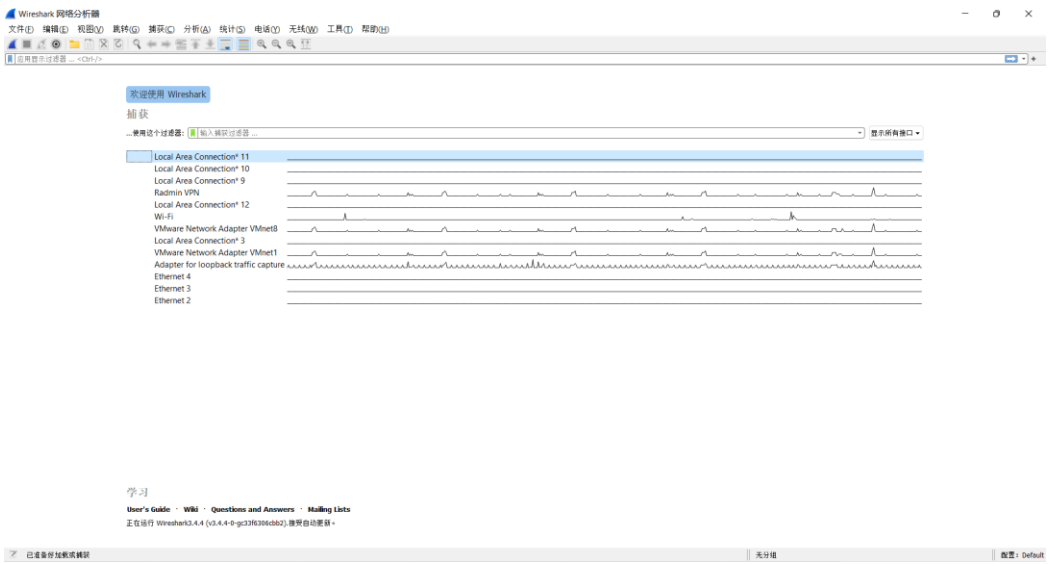
5. 显示从本机到达一个特定地址的路由
6. 显示某一个域名的 IP 地址
7. 显示已经与本机建立 TCP 连接的端口、IP 地址、连接状态等信息
8. 显示本机的路由表信息，并手工添加一个路由
9. 显示本机的网络映射连接
10. 显示局域网内某台机器的共享资源
11. 使用 telnet 连接 WEB 服务器的端口，输入（<cr>表示回车）获得该网站的主页内容：

```
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？**

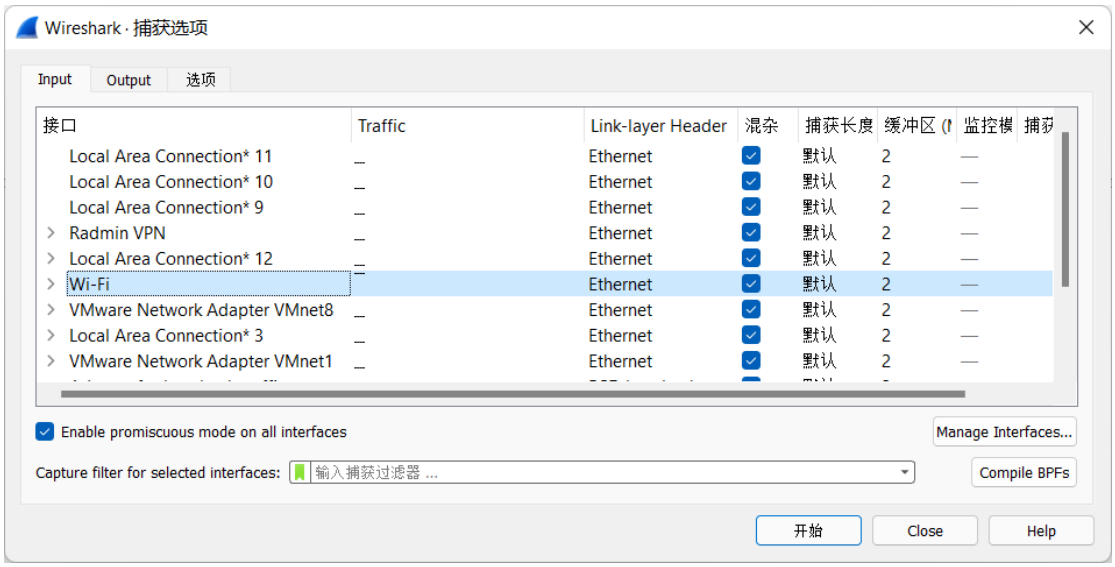


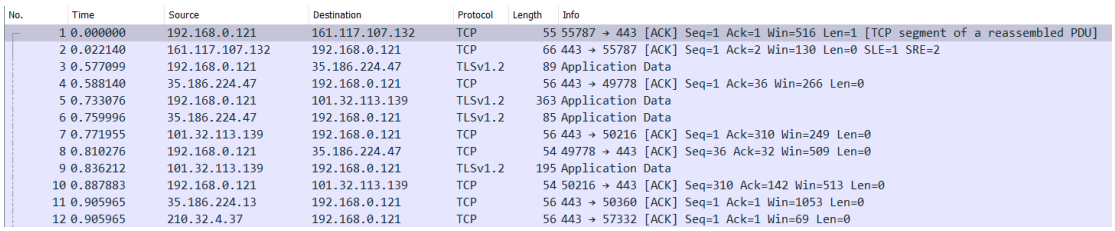
界面由以下六个部分组成：

- 菜单栏(Menu Bar)：包括文件、编辑、视图、跳转、捕获、分析、统计、电话、无线、工具、帮助等功能。
- 工具：捕获按钮、停止捕获按钮、重新捕获按钮、接口设置按钮等。
- 过滤栏：设置过滤词，用于应用显示过滤器。
- 网络接口栏：显示本地电脑的网络接口，通过观察图中显示的接口来看哪些是由流量传输的以及其分布情况。
- 学习与指导信息:给予新用户一些指导来使用 Wireshark 以及关于 Wireshark 的信息。
- 状态栏：显示 Wireshark 目前的状态。

- **开始捕获网络数据包，你看到了什么？有哪些协议？**

点击捕获按钮然后选择当前连接的网络。

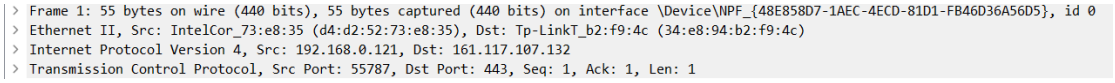




No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.0.121	161.117.107.132	TCP	55	55787 → 443 [ACK] Seq=1 Ack=1 Win=516 Len=1 [TCP segment of a reassembled PDU]
2	0.022140	161.117.107.132	192.168.0.121	TCP	66	443 → 55787 [ACK] Seq=1 Ack=2 Win=130 Len=0 SLE=1 SRE=2
3	0.577099	192.168.0.121	35.186.224.47	TLSv1.2	89	Application Data
4	0.588140	35.186.224.47	192.168.0.121	TCP	56	443 → 49778 [ACK] Seq=1 Ack=36 Win=266 Len=0
5	0.733076	192.168.0.121	101.32.113.139	TLSv1.2	363	Application Data
6	0.759996	35.186.224.47	192.168.0.121	TLSv1.2	85	Application Data
7	0.771955	101.32.113.139	192.168.0.121	TCP	56	443 → 50216 [ACK] Seq=1 Ack=310 Win=249 Len=0
8	0.810276	192.168.0.121	35.186.224.47	TCP	54	49778 → 443 [ACK] Seq=36 Ack=32 Win=509 Len=0
9	0.836212	101.32.113.139	192.168.0.121	TLSv1.2	195	Application Data
10	0.887883	192.168.0.121	101.32.113.139	TCP	54	50216 → 443 [ACK] Seq=310 Ack=142 Win=513 Len=0
11	0.905965	35.186.224.13	192.168.0.121	TCP	56	443 → 50360 [ACK] Seq=1 Ack=1 Win=1053 Len=0
12	0.905965	210.32.4.37	192.168.0.121	TCP	56	443 → 57332 [ACK] Seq=1 Ack=1 Win=69 Len=0

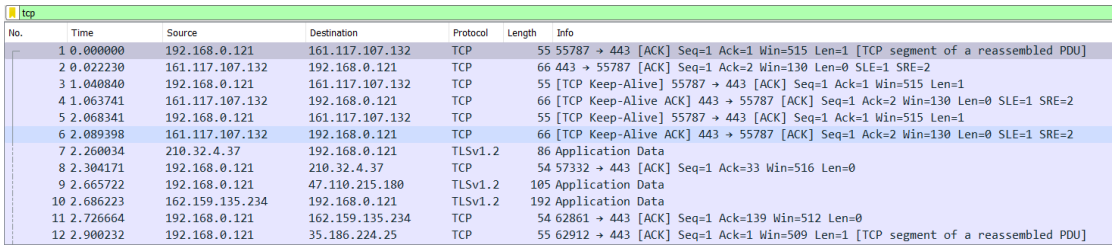
看到了很多的包和序列号在传输（ACK 包，Seq 等），每一条传输的包都包含协议，协议分别有 TCP、TLSv1.2、ARP、UDP、DNS、SSL、HTTP 等。

从中选择其中一条信息，可查看更详细的信息包括协议、端口 PORT、Source、Destination、网络类型（IPv4/IPv6）、Sequence 序列号、传输时间等各种信息，可展开分析。



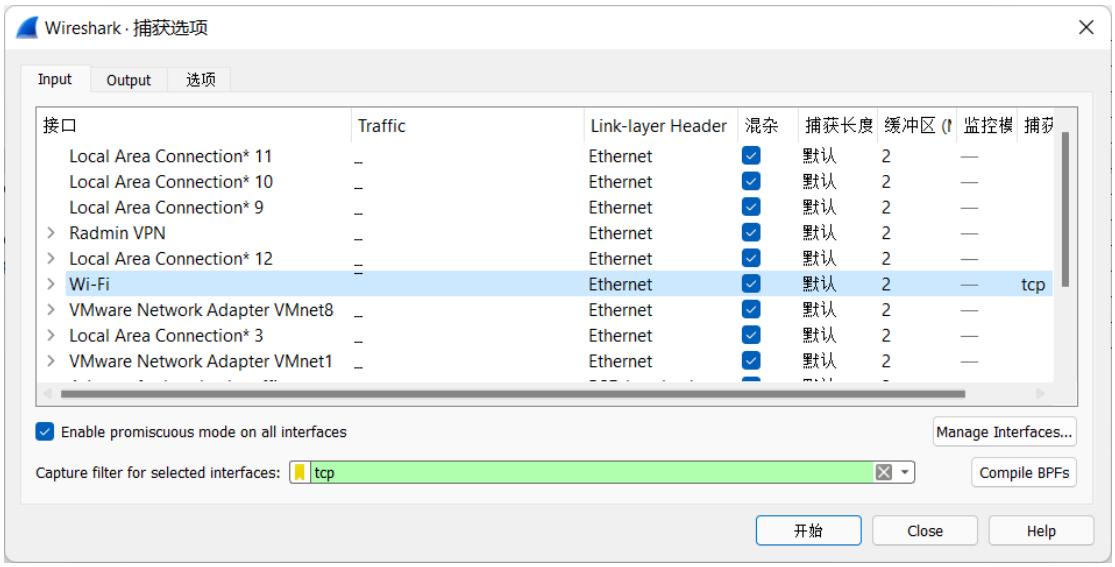
- **配置应用显示过滤器，让界面只显示某一协议类型的数据包。**

在过滤器输入 tcp，界面只会显示 TCP 协议类型的数据包。

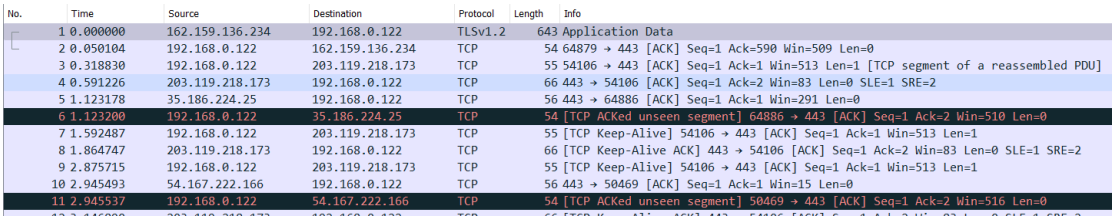


No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.0.121	161.117.107.132	TCP	55	55787 → 443 [ACK] Seq=1 Ack=1 Win=515 Len=1 [TCP segment of a reassembled PDU]
2	0.022230	161.117.107.132	192.168.0.121	TCP	66	443 → 55787 [ACK] Seq=1 Ack=2 Win=130 Len=0 SLE=1 SRE=2
3	1.040840	192.168.0.121	161.117.107.132	TCP	55	[TCP Keep-Alive] 55787 → 443 [ACK] Seq=1 Ack=1 Win=515 Len=1
4	1.063741	161.117.107.132	192.168.0.121	TCP	66	[TCP Keep-Alive ACK] 443 → 55787 [ACK] Seq=1 Ack=2 Win=130 Len=0 SLE=1 SRE=2
5	2.068341	192.168.0.121	161.117.107.132	TCP	55	[TCP Keep-Alive] 55787 → 443 [ACK] Seq=1 Ack=1 Win=515 Len=1
6	2.089398	161.117.107.132	192.168.0.121	TCP	66	[TCP Keep-Alive ACK] 443 → 55787 [ACK] Seq=1 Ack=2 Win=130 Len=0 SLE=1 SRE=2
7	2.260034	210.32.4.37	192.168.0.121	TLSv1.2	86	Application Data
8	2.304171	192.168.0.121	210.32.4.37	TCP	54	57332 → 443 [ACK] Seq=1 Ack=33 Win=516 Len=0
9	2.665722	192.168.0.121	47.110.215.180	TLSv1.2	105	Application Data
10	2.686223	162.159.135.234	192.168.0.121	TLSv1.2	192	Application Data
11	2.726664	192.168.0.121	162.159.135.234	TCP	54	62861 → 443 [ACK] Seq=1 Ack=139 Win=512 Len=0
12	2.900232	192.168.0.121	35.186.224.25	TCP	55	62912 → 443 [ACK] Seq=1 Ack=1 Win=509 Len=1 [TCP segment of a reassembled PDU]

- **配置捕获过滤器，只捕获某类协议的数据包。**



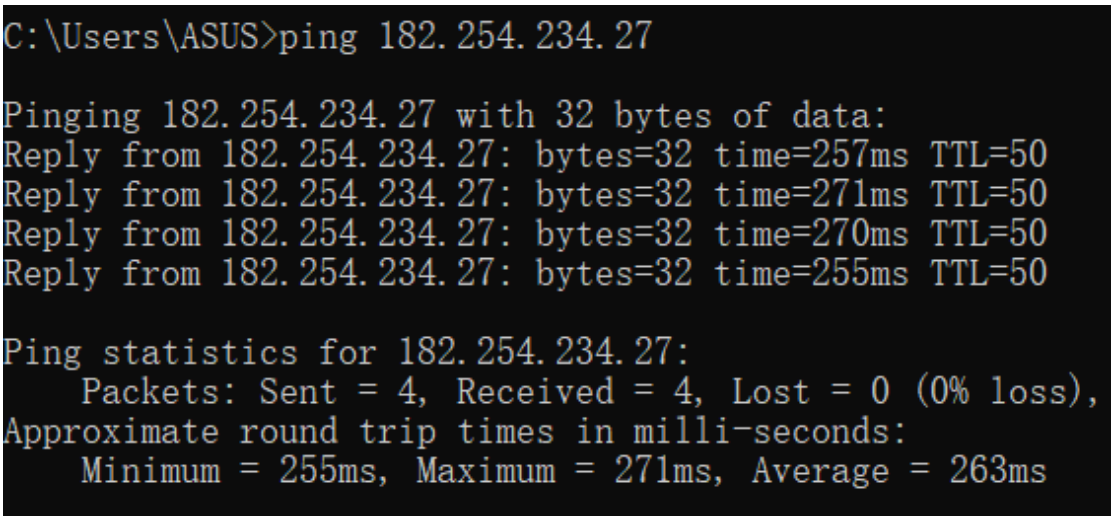
在点击捕获后，过滤捕获过滤器 tcp 协议，只会捕获 TCP 协议的数据包并显示每天捕获记录。



- **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。**

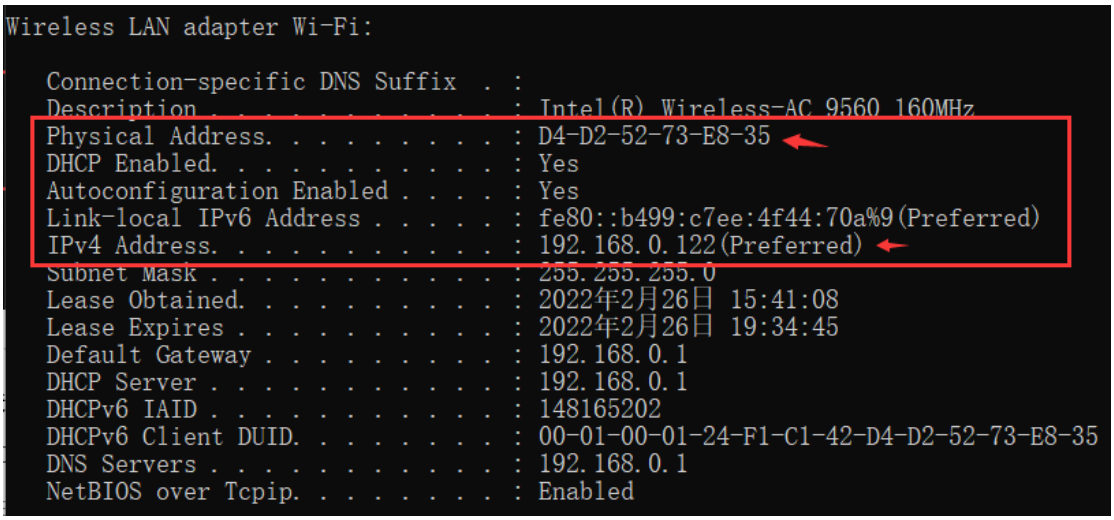
1. 测试到特定地址的联通性、数据包延迟时间

执行 ping 指令，测试特定地址



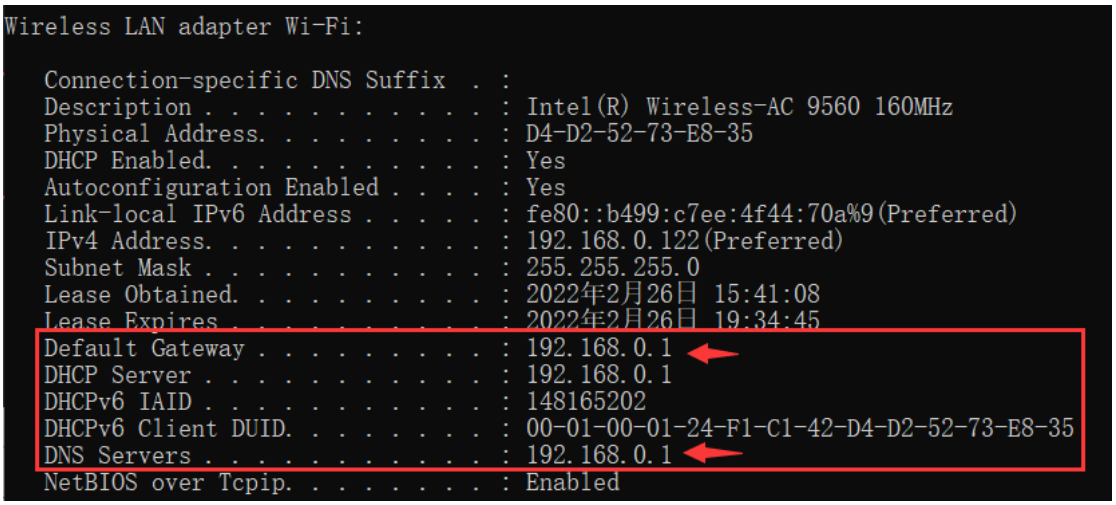
2. 显示本机的网卡物理地址、IP 地址

执行 ipconfig /all，获取本机网卡的物理地址、IP 地址（箭头）



3. 显示本机的默认网关地址、DNS 服务器地址

执行 ipconfig /all，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

执行命令 arp -a 可显示

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

Interface: 26.96.75.40 --- 0x6
  Internet Address      Physical Address      Type
  26.255.255.255        ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static

Interface: 192.168.208.1 --- 0x7
  Internet Address      Physical Address      Type
  192.168.208.255       ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static

Interface: 192.168.0.122 --- 0x9
  Internet Address      Physical Address      Type
  192.168.0.1           34-e8-94-b2-f9-4c     dynamic
  192.168.0.255         ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static

Interface: 192.168.47.1 --- 0xe
  Internet Address      Physical Address      Type
  192.168.47.255        ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
```

5. 显示从本机到达一个特定地址的路由

执行 tracert 命令，追踪浙江大学官网 IP

```
C:\Users\ASUS>tracert www.zju.edu.cn

Tracing route to www.zju.edu.cn.w.cdngslb.com [47.246.26.232]
over a maximum of 30 hops:

  1     1 ms    <1 ms    <1 ms  192.168.0.1
  2     5 ms     5 ms     3 ms  100.91.127.254
  3    36 ms     5 ms     3 ms  10.233.97.55
  4     9 ms     9 ms     8 ms  10.55.37.120
  5    17 ms    18 ms    11 ms  202.188.133.150
  6     7 ms    10 ms   124 ms  47.246.26.232

Trace complete.
```

6. 显示某一个域名的 IP 地址

执行 ping 指令，获取官网的 IP 地址

```
C:\Users\ASUS>ping www.zju.edu.cn

Pinging www.zju.edu.cn.w.cdngslb.com [47.246.26.229] with 32 bytes of data:
Reply from 47.246.26.229: bytes=32 time=8ms TTL=60
Reply from 47.246.26.229: bytes=32 time=6ms TTL=60
Reply from 47.246.26.229: bytes=32 time=8ms TTL=60
Reply from 47.246.26.229: bytes=32 time=7ms TTL=60

Ping statistics for 47.246.26.229:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 6ms, Maximum = 8ms, Average = 7ms
```

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

执行 netstat 指令

```
C:\Users\ASUS>netstat

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    127.0.0.1:49675        Peter:49676            ESTABLISHED
  TCP    127.0.0.1:49676        Peter:49675            ESTABLISHED
  TCP    127.0.0.1:49677        Peter:49678            ESTABLISHED
  TCP    127.0.0.1:49678        Peter:49677            ESTABLISHED
  TCP    127.0.0.1:50968        Peter:54530            TIME_WAIT
  TCP    127.0.0.1:50970        Peter:50969            TIME_WAIT
  TCP    127.0.0.1:52752        Peter:54530            ESTABLISHED
  TCP    127.0.0.1:52753        Peter:52754            ESTABLISHED
  TCP    127.0.0.1:52754        Peter:52753            ESTABLISHED
  TCP    127.0.0.1:54530        Peter:52752            ESTABLISHED
  TCP    192.168.0.122:49726    20.197.71.89:https     ESTABLISHED
  TCP    192.168.0.122:49788    20.197.71.89:https     ESTABLISHED
  TCP    192.168.0.122:50871    1.117.136.158:https    ESTABLISHED
  TCP    192.168.0.122:50895    52.98.90.2:https       ESTABLISHED
  TCP    192.168.0.122:50949    101.32.104.4:http      ESTABLISHED
  TCP    192.168.0.122:50956    20.197.71.89:https     ESTABLISHED
  TCP    192.168.0.122:50960    sa-in-f188:5228        ESTABLISHED
  TCP    192.168.0.122:50972    ec2-52-197-149-250:https  ESTABLISHED
  TCP    192.168.0.122:50976    25:https               ESTABLISHED
  TCP    192.168.0.122:50982    25:https               ESTABLISHED
  TCP    192.168.0.122:50984    13:https               ESTABLISHED
  TCP    192.168.0.122:51668    175.27.56.160:http     ESTABLISHED
  TCP    192.168.0.122:51775    203.205.219.229:https  CLOSE_WAIT
  TCP    192.168.0.122:51820    210.32.174.2:https     CLOSE_WAIT
```

8. 显示本机的路由表信息，并手工添加一个路由

执行 route print 指令显示本机的路由表信息

```
IPv4 Route Table
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0      192.168.0.1    192.168.0.122     35
         26.0.0.0        255.0.0.0         On-link       26.96.75.40    257
      26.96.75.40  255.255.255.255         On-link       26.96.75.40    257
   26.255.255.255  255.255.255.255         On-link       26.96.75.40    257
        127.0.0.0        255.0.0.0         On-link        127.0.0.1    331
        127.0.0.1  255.255.255.255         On-link        127.0.0.1    331
  127.255.255.255  255.255.255.255         On-link        127.0.0.1    331
      192.168.0.0    255.255.255.0         On-link      192.168.0.122    291
    192.168.0.122  255.255.255.255         On-link      192.168.0.122    291
    192.168.0.255  255.255.255.255         On-link      192.168.0.122    291
     192.168.47.0    255.255.255.0         On-link       192.168.47.1    291
     192.168.47.1  255.255.255.255         On-link       192.168.47.1    291
   192.168.47.255  255.255.255.255         On-link       192.168.47.1    291
    192.168.208.0    255.255.255.0         On-link      192.168.208.1    291
    192.168.208.1  255.255.255.255         On-link      192.168.208.1    291
  192.168.208.255  255.255.255.255         On-link      192.168.208.1    291
        224.0.0.0        240.0.0.0         On-link        127.0.0.1    331
        224.0.0.0        240.0.0.0         On-link       26.96.75.40    257
        224.0.0.0        240.0.0.0         On-link      192.168.208.1    291
        224.0.0.0        240.0.0.0         On-link       192.168.47.1    291
        224.0.0.0        240.0.0.0         On-link      192.168.0.122    291
  255.255.255.255  255.255.255.255         On-link        127.0.0.1    331
  255.255.255.255  255.255.255.255         On-link       26.96.75.40    257
  255.255.255.255  255.255.255.255         On-link      192.168.208.1    291
  255.255.255.255  255.255.255.255         On-link       192.168.47.1    291
  255.255.255.255  255.255.255.255         On-link      192.168.0.122    291
===========================================================================
Persistent Routes:
  None
```

（打开 cmd 时记得以管理员身份运行 Run as Administrator 不然会出错）执行 route add 192.168.10.0 mask 255.255.0.0 192.168.0.254 -p 添加一个路由，执行 route print 可再次查看路由表，可看到新增了一个永久的路由。然后也可删除，执行 route delete 192.168.10.0

```
IPv4 Route Table
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0      192.168.0.1    192.168.0.122     35
         26.0.0.0        255.0.0.0         On-link       26.96.75.40    257
      26.96.75.40  255.255.255.255         On-link       26.96.75.40    257
   26.255.255.255  255.255.255.255         On-link       26.96.75.40    257
        127.0.0.0        255.0.0.0         On-link        127.0.0.1    331
        127.0.0.1  255.255.255.255         On-link        127.0.0.1    331
  127.255.255.255  255.255.255.255         On-link        127.0.0.1    331
      192.168.0.0    255.255.255.0         On-link      192.168.0.122    291
    192.168.0.122  255.255.255.255         On-link      192.168.0.122    291
    192.168.0.255  255.255.255.255         On-link      192.168.0.122    291
     192.168.47.0    255.255.255.0         On-link       192.168.47.1    291
     192.168.47.1  255.255.255.255         On-link       192.168.47.1    291
   192.168.47.255  255.255.255.255         On-link       192.168.47.1    291
    192.168.208.0    255.255.255.0         On-link      192.168.208.1    291
    192.168.208.1  255.255.255.255         On-link      192.168.208.1    291
  192.168.208.255  255.255.255.255         On-link      192.168.208.1    291
        224.0.0.0        240.0.0.0         On-link        127.0.0.1    331
        224.0.0.0        240.0.0.0         On-link       26.96.75.40    257
        224.0.0.0        240.0.0.0         On-link      192.168.208.1    291
        224.0.0.0        240.0.0.0         On-link       192.168.47.1    291
        224.0.0.0        240.0.0.0         On-link      192.168.0.122    291
  255.255.255.255  255.255.255.255         On-link        127.0.0.1    331
  255.255.255.255  255.255.255.255         On-link       26.96.75.40    257
  255.255.255.255  255.255.255.255         On-link      192.168.208.1    291
  255.255.255.255  255.255.255.255         On-link       192.168.47.1    291
  255.255.255.255  255.255.255.255         On-link      192.168.0.122    291
===========================================================================
Persistent Routes:
  Network Address          Netmask  Gateway Address  Metric
    192.168.10.0    255.255.0.0    192.168.0.254       1
===========================================================================
```

9. 显示本机的网络映射连接

执行 net use 指令可查看列表。当前没有进行网络映射连接。若要映射可通过执行 net use z: \\IPv4 地址\c$ 密码 /user:用户名，验证后进行连接 net use z: \\IPv4 地址\c$，c$是默认的文件共享目录，z：映射后的驱动器盘，之后可以切换至 z 盘（执行 z:）。

```
C:\WINDOWS\system32>net use
New connections will be remembered.

There are no entries in the list.
```

10. 显示局域网内某台机器的共享资源

执行 net share 指令查看局域网内某台机器的共享资源

```
C:\WINDOWS\system32>net share

Share name   Resource                        Remark

-------------------------------------------------------------------------------
D$           D:\                             Default share
C$           C:\                             Default share
IPC$                                         Remote IPC
ADMIN$       C:\WINDOWS                      Remote Admin
C            C:\
D            D:\
The command completed successfully.
```

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：

执行 telnet www.google.com 80 命令连接上谷歌，按着 CTRL +]健可转换成显示模式。然后再按回车键，输入以下命令得到以下结果。

GET / HTTP/1.1<cr>

Host: www.google.com

<cr>

连接谷歌

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

HTTP/1.1 200 OK
Date: Sat, 26 Feb 2022 13:18:53 GMT
Expires: -1
Cache-Control: private, max-age=0
Content-Type: text/html; charset=ISO-8859-1
P3P: CP="This is not a P3P policy! See g.co/p3phelp for more info."
Server: gws
X-XSS-Protection: 0
X-Frame-Options: SAMEORIGIN
Set-Cookie: 1P_JAR=2022-02-26-13; expires=Mon, 28-Mar-2022 13:18:53 GMT; path=/; domain=.google.com; Secure
Set-Cookie: NID=511=b0-FakJsla2DoWAlSYIbSUL9_t15DrdGHY1NY10Rz4OGlvu6gVbn7KKUiBsUK8dRWSqfc5ic-iKb30V0EiXX59QSG2svHxZU-gl0
5HiCCGgL-eDY3zRbgqGL_9Lq0-ileprdtslhrMSASSm9ntkkou6eWLCOhYpePHxEAN5b8e0; expires=Sun, 28-Aug-2022 13:18:53 GMT; path=/;
domain=.google.com; HttpOnly
Accept-Ranges: none
Vary: Accept-Encoding
Transfer-Encoding: chunked
```

- **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？**

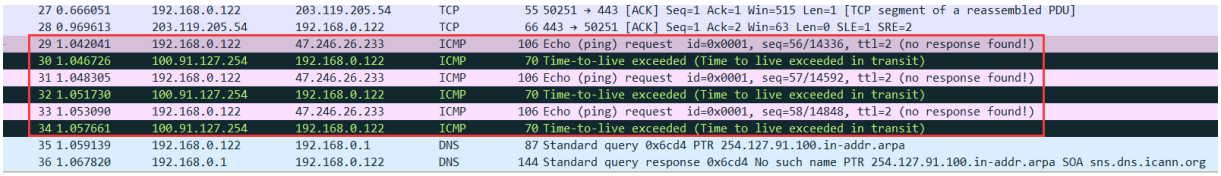
执行 ping www.zju.edu.cn

406	15.603495	192.168.0.122	47.246.26.230	ICMP	74 Echo (ping) request id=0x0001, seq=51/13056, ttl=128 (reply in 407)
407	15.631417	47.246.26.230	192.168.0.122	ICMP	74 Echo (ping) reply id=0x0001, seq=51/13056, ttl=60 (request in 406)
408	15.994654	192.168.0.122	35.186.224.25	TCP	55 [TCP Keep-Alive] [TCP ACKed unseen segment] 53965 → 443 [ACK] Seq=0 Ack=2 Win=513 Len=1
409	16.005297	35.186.224.25	192.168.0.122	TCP	66 [TCP Previous segment not captured] 443 → 53965 [ACK] Seq=2 Ack=1 Win=842 Len=0 SLE=0 SRE=1
410	16.367577	192.168.0.122	203.119.205.54	TCP	55 [TCP Keep-Alive] 50251 → 443 [ACK] Seq=0 Ack=1 Win=515 Len=1
411	16.617075	192.168.0.122	47.246.26.230	ICMP	74 Echo (ping) request id=0x0001, seq=52/13312, ttl=128 (reply in 412)
412	16.627282	47.246.26.230	192.168.0.122	ICMP	74 Echo (ping) reply id=0x0001, seq=52/13312, ttl=60 (request in 411)

这是 ICMP 协议

- **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？**

执行 tracert www.zju.edu.cn

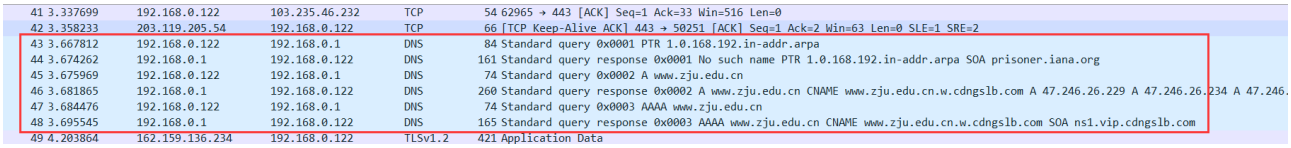


27	0.666051	192.168.0.122	203.119.205.54	TCP	55 50251 → 443 [ACK] Seq=1 Ack=1 Win=515 Len=1 [TCP segment of a reassembled PDU]
28	0.969613	203.119.205.54	192.168.0.122	TCP	66 443 → 50251 [ACK] Seq=1 Ack=2 Win=63 Len=0 SLE=1 SRE=2
29	1.042041	192.168.0.122	47.246.26.233	ICMP	106 Echo (ping) request id=0x0001, seq=56/14336, ttl=2 (no response found!)
30	1.046726	100.91.127.254	192.168.0.122	ICMP	70 Time-to-live exceeded (Time to live exceeded in transit)
31	1.048305	192.168.0.122	47.246.26.233	ICMP	106 Echo (ping) request id=0x0001, seq=57/14592, ttl=2 (no response found!)
32	1.051730	100.91.127.254	192.168.0.122	ICMP	70 Time-to-live exceeded (Time to live exceeded in transit)
33	1.053090	192.168.0.122	47.246.26.233	ICMP	106 Echo (ping) request id=0x0001, seq=58/14848, ttl=2 (no response found!)
34	1.057661	100.91.127.254	192.168.0.122	ICMP	70 Time-to-live exceeded (Time to live exceeded in transit)
35	1.059139	192.168.0.122	192.168.0.1	DNS	87 Standard query 0x6cd4 PTR 254.127.91.100.in-addr.arpa
36	1.067820	192.168.0.1	192.168.0.122	DNS	144 Standard query response 0x6cd4 No such name PTR 254.127.91.100.in-addr.arpa SOA sns.dns.icann.org

同样也是 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？**

执行 nslookup www.zju.edu.cn

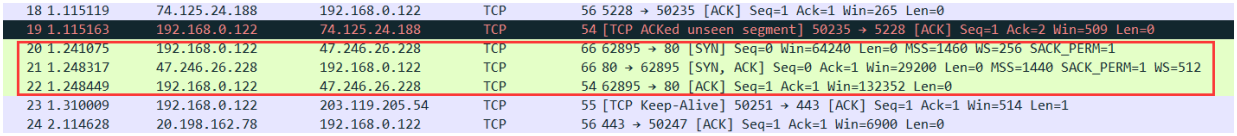


41	3.337699	192.168.0.122	103.235.46.232	TCP	54 62965 → 443 [ACK] Seq=1 Ack=33 Win=516 Len=0
42	3.358233	203.119.205.54	192.168.0.122	TCP	66 [TCP Keep-Alive ACK] 443 → 50251 [ACK] Seq=1 Ack=2 Win=63 Len=0 SLE=1 SRE=2
43	3.667812	192.168.0.122	192.168.0.1	DNS	84 Standard query 0x0001 PTR 1.0.168.192.in-addr.arpa
44	3.674262	192.168.0.1	192.168.0.122	DNS	161 Standard query response 0x0001 No such name PTR 1.0.168.192.in-addr.arpa SOA prisoner.iana.org
45	3.675969	192.168.0.122	192.168.0.1	DNS	74 Standard query 0x0002 A www.zju.edu.cn
46	3.681865	192.168.0.1	192.168.0.122	DNS	260 Standard query response 0x0002 A www.zju.edu.cn CNAME www.zju.edu.cn.w.cdngslb.com A 47.246.26.229 A 47.246.26.234 A 47.246.
47	3.684476	192.168.0.122	192.168.0.1	DNS	74 Standard query 0x0003 AAAA www.zju.edu.cn
48	3.695545	192.168.0.1	192.168.0.122	DNS	165 Standard query response 0x0003 AAAA www.zju.edu.cn CNAME www.zju.edu.cn.w.cdngslb.com SOA ns1.vip.cdngslb.com
49	4.203864	162.159.136.234	192.168.0.122	TLSv1.2	421 Application Data

这是 DNS 协议

- **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？**

执行 telnet www.zju.edu.cn 80



18	1.115119	74.125.24.188	192.168.0.122	TCP	56 5228 → 50235 [ACK] Seq=1 Ack=1 Win=265 Len=0
19	1.115163	192.168.0.122	74.125.24.188	TCP	54 [TCP ACKed unseen segment] 50235 → 5228 [ACK] Seq=1 Ack=2 Win=509 Len=0
20	1.241075	192.168.0.122	47.246.26.228	TCP	66 62895 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
21	1.248317	47.246.26.228	192.168.0.122	TCP	66 80 → 62895 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1440 SACK_PERM=1 WS=512
22	1.248449	192.168.0.122	47.246.26.228	TCP	54 62895 → 80 [ACK] Seq=1 Ack=1 Win=132352 Len=0
23	1.310009	192.168.0.122	203.119.205.54	TCP	55 [TCP Keep-Alive] 50251 → 443 [ACK] Seq=1 Ack=1 Win=514 Len=1
24	2.114628	20.198.162.78	192.168.0.122	TCP	56 443 → 50247 [ACK] Seq=1 Ack=1 Win=6900 Len=0

这是 TCP 协议。

六、 实验结果与分析

- WireShark 的两种过滤器有什么不同？

  使用捕获过滤器后，在捕获数据包的时候就已经根据过滤词去进行过滤了。

  使用显示过滤器则是在捕获数据包后显示时才再过滤。

- 哪些网络命令会产生在 WireShark 中产生数据包，为什么？

  Ping.exe、Telnet.exe、Tracert.exe、Nslookup.exe 会产生数据包。因为要根据协议去进行发送请求，所以就会产生数据包。

- 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？
  - Ping 发送的是 ICMP 类型的协议数据包。
  - 当我们向一个 IP 地址发送数据的时候就需要用到 ARP 缓存表，这个表记录着 IP 地址与 MAC 地址的映射关系，可查询 MAC 地址。但是当缓存表中没有这样的记录时，就会发送一个 ARP 请求给该 IP 所对应的 MAC 地址。
  - Ping 一个域名时还需要发送 DNS 协议请求数据来获得对应的 IP 地址。

七、 讨论、心得

在开始做这个实验前，我其实还不太了解一些指令来抓取数据包，所以现在网上学了指令的用法才开始进行实验的各项步骤（根据实验步骤一个个学习）。在根据实验要求抓取数据包时，我不太看得懂这些数据包的含义，协议的类型也不太了解，希望在以后的理论课中可以学到这些协议与信息代表什么。

我一直有个疑问，在访问一个域名时，那其中的数据包是怎么形成的？是从哪一层传到哪一层？而每个层的工作又是什么？这些的问题我都还不太明白，只能等上课后才能更深入地理解。

此次的实验算是给像我这种初学者一个很好的入门机会，了解计算机网络的基础知识，通过 Wireshark 这个工具捕获数据包来让我们实践以及观察请求和接收数据包的过程，体验计算机网络的具体实践过程。如果有一定的理论知识还可以更加深入地了解这些数据包的含义以及基础概念。