



本科实验报告

课程名称: 计算机网络基础

姓 名: 祖敬涵

学 院: 计算机学院

系: 计算机科学与技术

专 业: 信息安全

学 号: 3220102091

指导教师:

2024 年 9 月 19 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: 祖敬涵 专业: 信息安全 学号: 3220102091

同组学生姓名: _____ 指导老师: _____

实验地点: 计算机网络实验室 实验日期: 2024 年 9 月 11 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

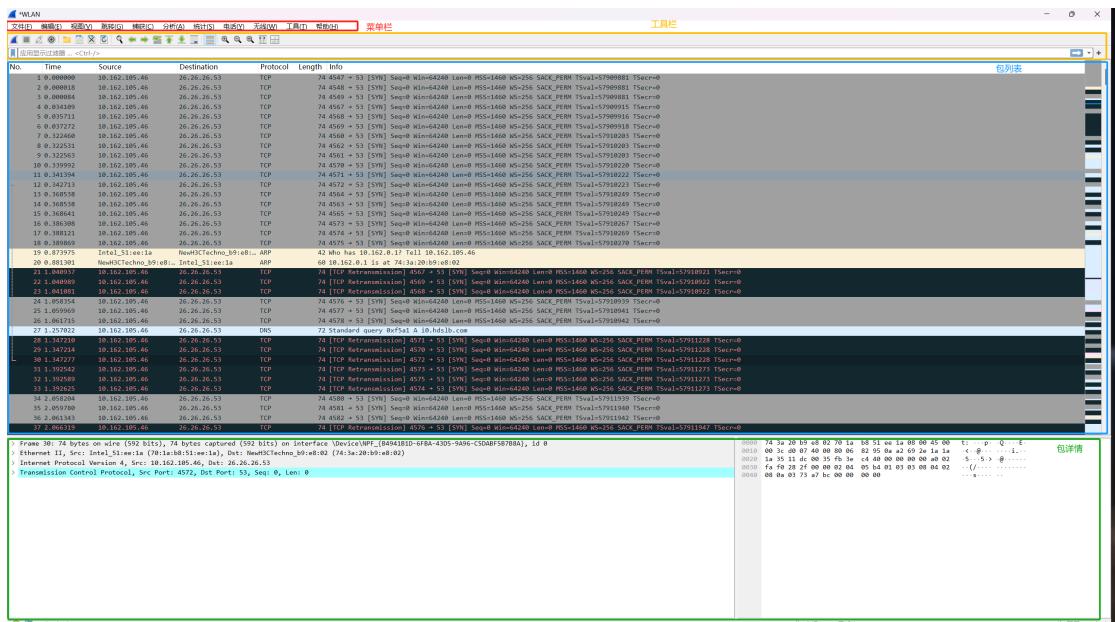
四、 操作方法与实验步骤

1. 安装网络包捕获软件 Wireshark
2. 配置网络包捕获软件, 捕获所有类型的数据包
3. 配置网络包捕获软件, 只捕获特定类型的包
4. 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):
 - a) 测试到特定地址的联通性、数据包延迟时间
 - b) 显示本机的网卡物理地址、IP 地址
 - c) 显示本机的默认网关地址、DNS 服务器地址
 - d) 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

- e) 显示从本机到达一个特定地址的路由
 - f) 显示某一个域名的 IP 地址
 - g) 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
 - h) 显示本机的路由表信息，并手工添加一个路由
 - i) 显示本机的网络映射连接
 - j) 显示局域网内某台机器的共享资源
 - k) 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：
 - i. GET / HTTP/1.1
 - ii. Host:www.baidu.com
5. 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。

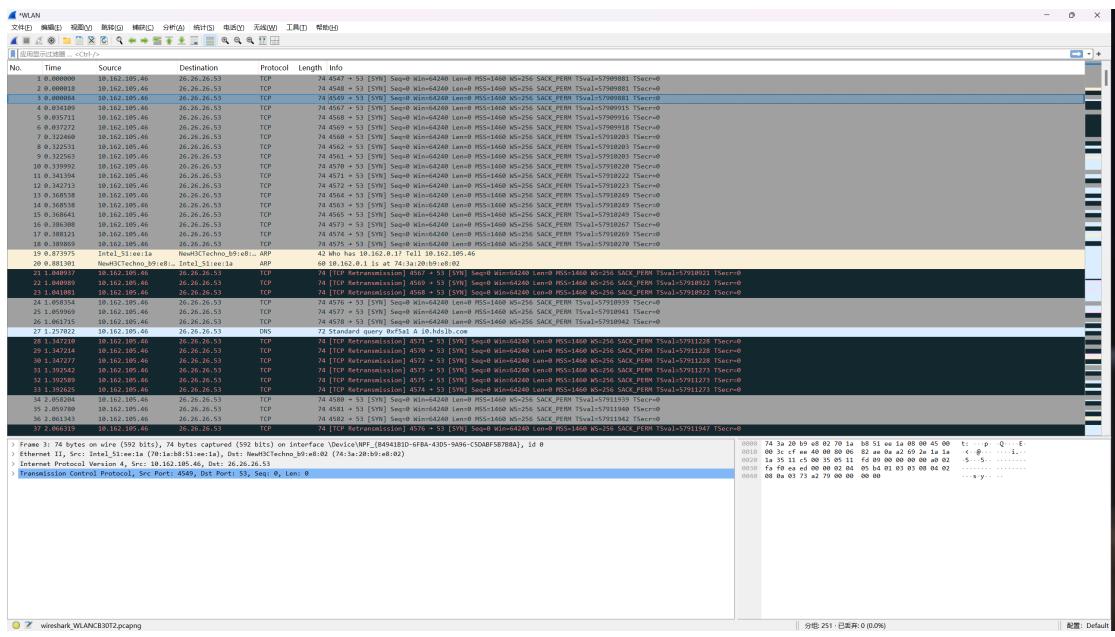
五、实验数据记录和处理

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

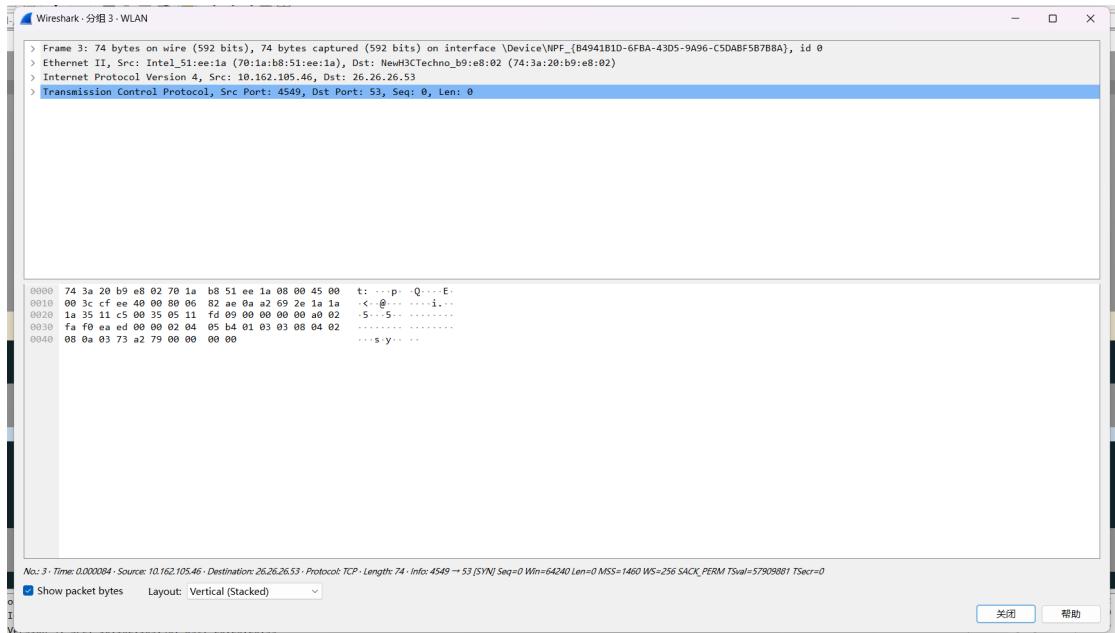


1. **菜单栏:** 包括文件、编辑、查看、捕获、分析、统计、帮助等选项，提供了丰富的功能。
2. **工具栏:** 包含了开始/停止捕获、保存、打开文件、过滤等常用操作按钮。
3. **包列表:** 显示捕获到的所有网络数据包的列表，可以根据需要进行排序和筛选。
4. **包详情:** 显示选中数据包的详细信息，包括各个网络层的字段和值。

● 开始捕获网络数据包，你看到了什么？有哪些协议？

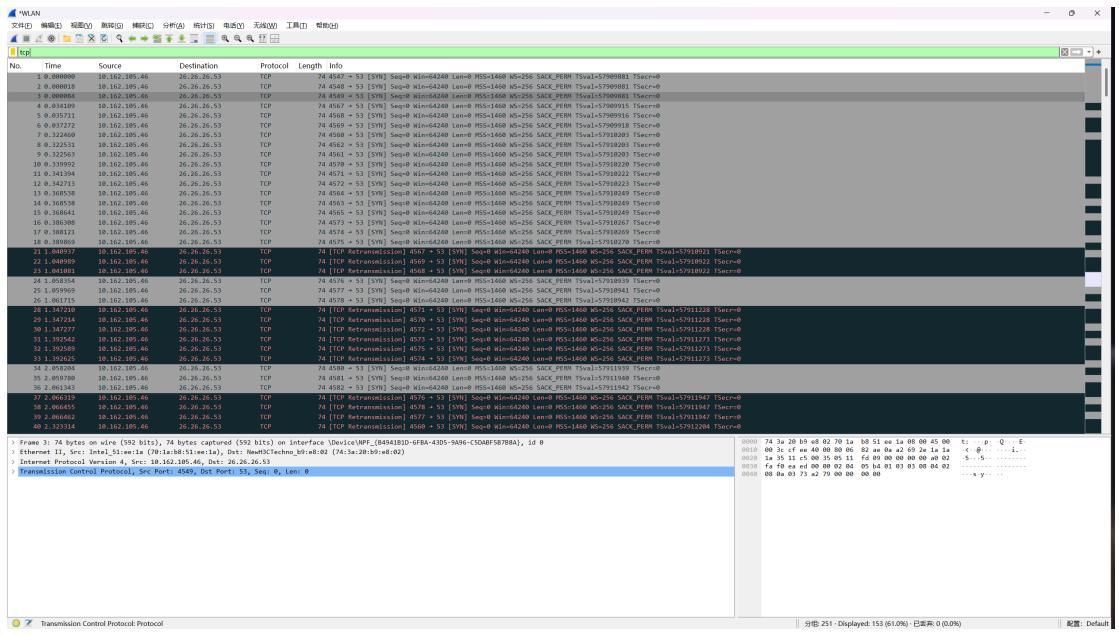


显示了抓取到的数据包，点开能够查看详细信息。



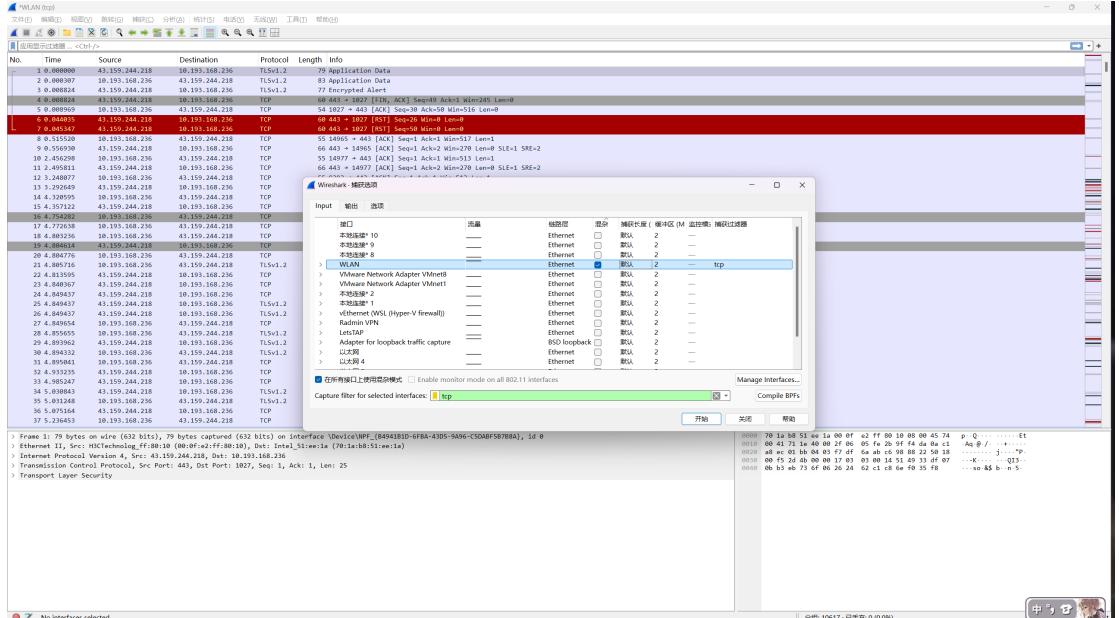
看到的协议有 TCP、ARP、DNS、UDP、TLSv1.2……

● 配置显示过滤器，让界面只显示某一协议类型的数据包。

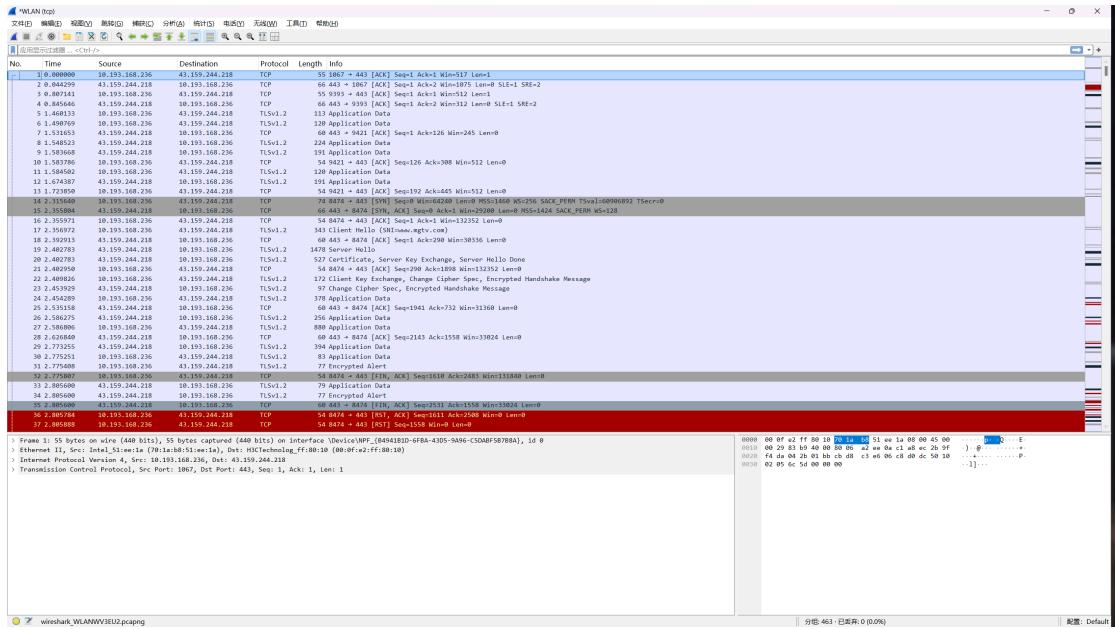


通过在上方的过滤器中添加想要的效果，如图所示，我填入 **tcp**，并回车，则下方将所有的 **tcp** 协议数据包单独显示。

● 配置捕获过滤器，只捕获某类协议的数据包。



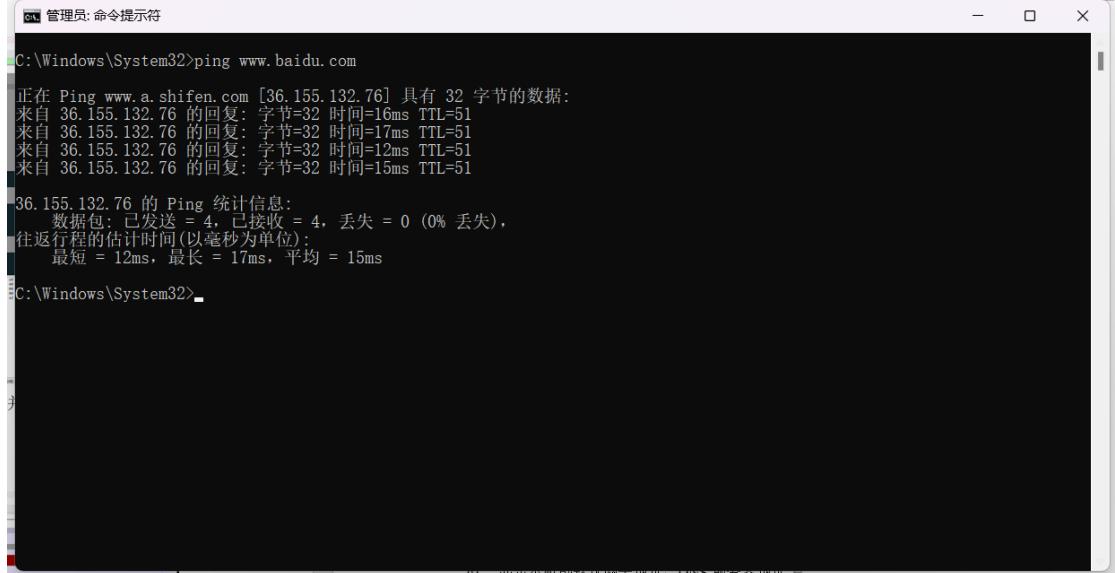
需要在捕获中点击选项，在这里输入捕获过滤器的内容，填入 **tcp** 点击开始，会开始新的捕获，效果如下。



一开始我还心思为啥有 TLSv1.2，后来查说 TLS 是建立在 TCP 上的，是其一部分，所以会显示出来。

- 利用 ping, ipconfig, arp, tracert, nslookup, nbstat, route, netstat, NET SHARE, telnet 命令完成在实验步骤 4 中列举的 11 个功能。

a) 测试到特定地址的联通性、数据包延迟时间



ping 了百度。

b) 显示本机的网卡物理地址、IP 地址

```
管理员: 命令提示符
C:\Windows\System32>ipconfig /all

Windows IP 配置

主机名 . . . . . : summitsoul
主 DNS 后缀 . . . . . :
节点类型 . . . . . : 混合
IP 路由已启用 . . . . . : 否
WINS 代理已启用 . . . . . : 否

以太网适配器 LetsTAP:

连接特定的 DNS 后缀 . . . . . :
描述 . . . . . : TAP-Windows Adapter V9
物理地址 . . . . . : 00-FF-EA-78-1D-41
DHCP 已启用 . . . . . : 否
自动配置已启用 . . . . . : 是
本地链接 IPv6 地址 . . . . . : fe80::77bf:1e01:138c:3fcf%25(首选)
IPv4 地址 . . . . . : 26.26.26.1(首选)
子网掩码 . . . . . : 255.255.255.248
默认网关 . . . . . :
DHCPv6 IAID . . . . . : 1426128874
DHCPv6 客户端 DUID . . . . . : 00-01-00-01-2A-34-E4-D7-58-11-22-DF-57-34
DNS 服务器 . . . . . : 26.26.26.53
TCPIP 上的 NetBIOS . . . . . : 已启用

以太网适配器 Radmin VPN:

连接特定的 DNS 后缀 . . . . . :
```

利用 ipconfig /all 指令，我们可以看到，物理地址是 70-1A-B8-51-EE-1A，IP 地址为 10.193.168.236。

c) 显示本机的默认网关地址、DNS 服务器地址

```
管理员: 命令提示符
物理地址 . . . . . : 00-FF-6B-6A-27-7E
DHCP 已启用 . . . . . : 是
自动配置已启用 . . . . . : 是

无线局域网适配器 WLAN:

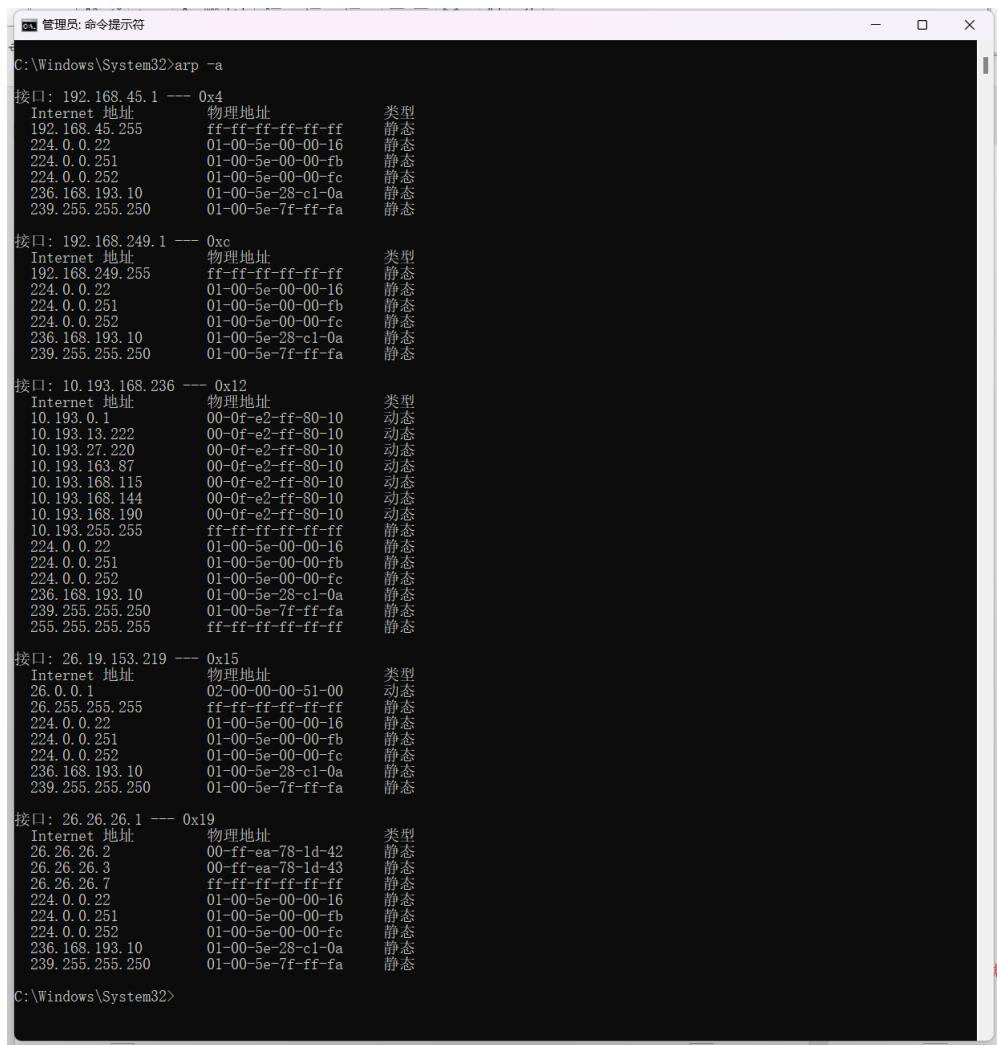
连接特定的 DNS 后缀 . . . . . :
描述 . . . . . : Intel(R) Wi-Fi 6E AX211 160MHz
物理地址 . . . . . : 70-1A-B8-51-EE-1A
DHCP 已启用 . . . . . : 是
自动配置已启用 . . . . . : 是
本地链接 IPv6 地址 . . . . . : fe80::86e0:6fe3:792f:6281%18(首选)
IPv4 地址 . . . . . : 10.193.168.236(首选)
子网掩码 . . . . . : 255.255.0.0
获得租约的时间 . . . . . : 2024年9月11日 15:36:38
租约过期的时间 . . . . . : 2024年9月11日 18:06:58
默认网关 . . . . . :
DHCP 服务器 . . . . . : 10.193.0.1
DHCPv6 IAID . . . . . : 141564600
DHCPv6 客户端 DUID . . . . . : 00-01-00-01-2A-34-E4-D7-58-11-22-DF-57-34
DNS 服务器 . . . . . : 26.26.26.53
TCPIP 上的 NetBIOS . . . . . : 已启用

以太网适配器 以太网 4:

媒体状态 . . . . . : 媒体已断开连接
连接特定的 DNS 后缀 . . . . . :
描述 . . . . . : Sangfor SSL VPN CS Support System VNIC
物理地址 . . . . . : 00-FF-3F-02-F3-6C
DHCP 已启用 . . . . . : 否
```

跟上一个一样，同样用 ipconfig /all 指令，默认网关地址是 10.193.0.1，DNS 服务器地址是 26.26.26.53。

d) 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



```
C:\Windows\System32>arp -a

接口: 192.168.45.1 --- 0x4
Internet 地址 物理地址 类型
192.168.45.255 ff-ff-ff-ff-ff-ff 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
236.168.193.10 01-00-5e-28-c1-0a 静态
239.255.255.250 01-00-5e-7f-ff-fa 静态

接口: 192.168.249.1 --- 0xc
Internet 地址 物理地址 类型
192.168.249.255 ff-ff-ff-ff-ff-ff 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
236.168.193.10 01-00-5e-28-c1-0a 静态
239.255.255.250 01-00-5e-7f-ff-fa 静态

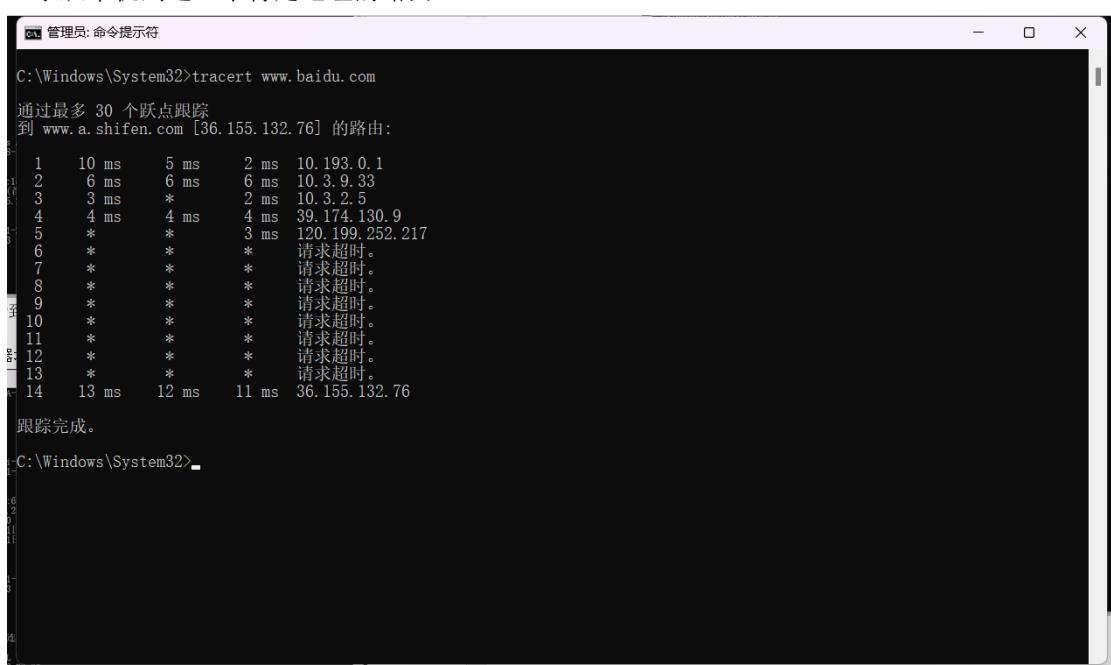
接口: 10.193.168.236 --- 0x12
Internet 地址 物理地址 类型
10.193.0.1 00-0f-e2-ff-80-10 动态
10.193.13.222 00-0f-e2-ff-80-10 动态
10.193.27.220 00-0f-e2-ff-80-10 动态
10.193.163.87 00-0f-e2-ff-80-10 动态
10.193.168.115 00-0f-e2-ff-80-10 动态
10.193.168.144 00-0f-e2-ff-80-10 动态
10.193.168.190 00-0f-e2-ff-80-10 动态
10.193.255.255 ff-ff-ff-ff-ff-ff 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
236.168.193.10 01-00-5e-28-c1-0a 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

接口: 26.19.153.219 --- 0x15
Internet 地址 物理地址 类型
26.0.0.1 02-00-00-00-51-00 动态
26.255.255.255 ff-ff-ff-ff-ff-ff 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
236.168.193.10 01-00-5e-28-c1-0a 静态
239.255.255.250 01-00-5e-7f-ff-fa 静态

接口: 26.26.26.1 --- 0x19
Internet 地址 物理地址 类型
26.26.26.2 00-ff-ea-78-1d-42 静态
26.26.26.3 00-ff-ea-78-1d-43 静态
26.26.26.7 ff-ff-ff-ff-ff-ff 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
236.168.193.10 01-00-5e-28-c1-0a 静态
239.255.255.250 01-00-5e-7f-ff-fa 静态
```

利用 arp 指令。

e) 显示从本机到达一个特定地址的路由



```
C:\Windows\System32>tracert www.baidu.com

通过最多 30 个跃点跟踪
到 www.a.shifen.com [36.155.132.76] 的路由:

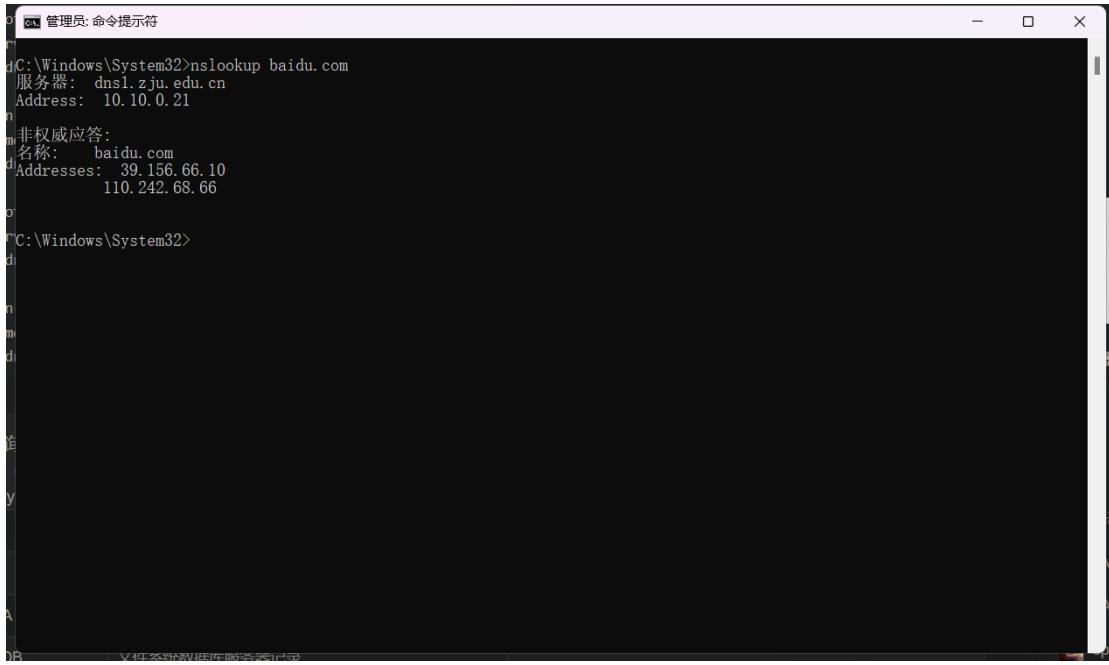
  1  10 ms   5 ms   2 ms  10.193.0.1
  2   6 ms   6 ms   6 ms  10.3.9.33
  3   3 ms   *       2 ms  10.3.2.5
  4   4 ms   4 ms   4 ms  39.174.130.9
  5   *       *       3 ms  120.199.252.217
  6   *       *       *       请求超时。
  7   *       *       *       请求超时。
  8   *       *       *       请求超时。
  9   *       *       *       请求超时。
至 10   *       *       *       请求超时。
  11  *       *       *       请求超时。
  12  *       *       *       请求超时。
  13  *       *       *       请求超时。
  14  13 ms   12 ms   11 ms  36.155.132.76

跟踪完成。

C:\Windows\System32>
```

利用 tracert 指令，跑的是到百度的。

- f) 显示某一个域名的 IP 地址



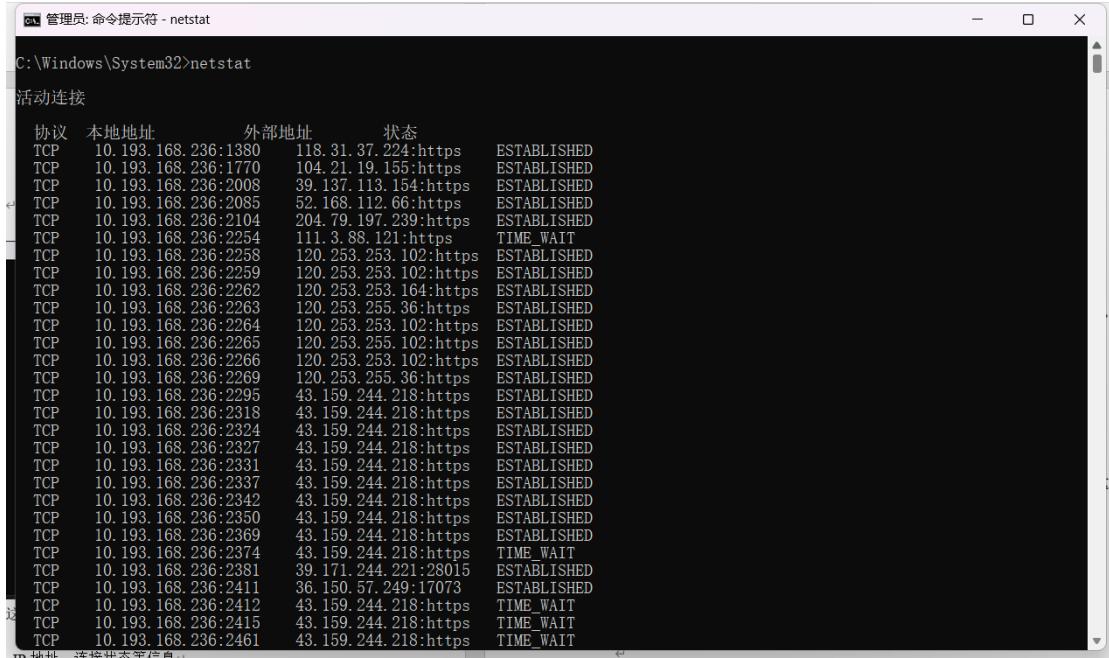
```
C:\Windows\System32>nslookup baidu.com
服务器: dns1.zju.edu.cn
Address: 10.10.0.21

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

C:\Windows\System32>
```

利用 nslookup 指令，可以看到，在这里百度的 IP 有两个，分别是 39.156.66.10 和 110.242.68.66。

- g) 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



```
C:\Windows\System32>netstat
活动连接

协议 本地地址          外部地址          状态
TCP   10.193.168.236:1380    118.31.37.224:https ESTABLISHED
TCP   10.193.168.236:1770    104.21.19.155:https ESTABLISHED
TCP   10.193.168.236:2008    39.137.113.154:https ESTABLISHED
TCP   10.193.168.236:2085    52.168.112.66:https ESTABLISHED
TCP   10.193.168.236:2104    204.79.197.239:https ESTABLISHED
TCP   10.193.168.236:2254    111.3.88.121:https TIME_WAIT
TCP   10.193.168.236:2258    120.253.253.102:https ESTABLISHED
TCP   10.193.168.236:2259    120.253.253.102:https ESTABLISHED
TCP   10.193.168.236:2262    120.253.253.164:https ESTABLISHED
TCP   10.193.168.236:2263    120.253.255.36:https ESTABLISHED
TCP   10.193.168.236:2264    120.253.253.102:https ESTABLISHED
TCP   10.193.168.236:2265    120.253.255.102:https ESTABLISHED
TCP   10.193.168.236:2266    120.253.253.102:https ESTABLISHED
TCP   10.193.168.236:2269    120.253.255.36:https ESTABLISHED
TCP   10.193.168.236:2295    43.159.244.218:https ESTABLISHED
TCP   10.193.168.236:2318    43.159.244.218:https ESTABLISHED
TCP   10.193.168.236:2324    43.159.244.218:https ESTABLISHED
TCP   10.193.168.236:2327    43.159.244.218:https ESTABLISHED
TCP   10.193.168.236:2331    43.159.244.218:https ESTABLISHED
TCP   10.193.168.236:2337    43.159.244.218:https ESTABLISHED
TCP   10.193.168.236:2342    43.159.244.218:https ESTABLISHED
TCP   10.193.168.236:2350    43.159.244.218:https ESTABLISHED
TCP   10.193.168.236:2369    43.159.244.218:https ESTABLISHED
TCP   10.193.168.236:2374    43.159.244.218:https TIME_WAIT
TCP   10.193.168.236:2381    39.171.244.221:28015 ESTABLISHED
TCP   10.193.168.236:2411    36.150.57.249:17073 ESTABLISHED
TCP   10.193.168.236:2412    43.159.244.218:https TIME_WAIT
TCP   10.193.168.236:2415    43.159.244.218:https TIME_WAIT
TCP   10.193.168.236:2461    43.159.244.218:https TIME_WAIT
```

利用 netstat 指令即可。

h) 显示本机的路由表信息，并手工添加一个路由

```
管理员: 命令提示符
C:\Windows\System32>route print
=====
接口列表
25...00 ff ea 78 1d 41 .....TAP-Windows Adapter V9
21...02 50 46 83 af 42 .....Pamatech Radmin VPN Ethernet Adapter
27...58 11 22 df 57 34 .....Realtek Gaming 2.5GbE Family Controller
2...70 1a b8 51 ee 1b .....Microsoft Wi-Fi Direct Virtual Adapter
19...72 1a b8 51 ee 1a .....Microsoft Wi-Fi Direct Virtual Adapter #2
24...00 ff e9 48 35 a5 .....VeryKuai TAP Adapter
4...00 50 56 c0 00 01 .....VMware Virtual Ethernet Adapter for VMnet1
12...00 50 56 c0 00 08 .....VMware Virtual Ethernet Adapter for VMnet8
14...00 ff 6b 6a 27 7e .....Netease UU TAP-Win32 Adapter V9.21
18...70 1a b8 51 ee 1a .....Intel(R) Wi-Fi 6E AX211 160MHz
10...00 ff 3f 02 f3 6c .....Sangfor SSL VPN CS Support System VNIC
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 跳点数
0.0.0.0 0.0.0.0 26.0.0.1 26.19.153.219 9257
0.0.0.0 0.0.0.0 10.193.0.1 10.193.168.236 35
0.0.0.0 128.0.0.0 26.26.26.3 26.26.26.1 1
10.193.0.0 255.255.0.0 在链路上 10.193.168.236 291
10.193.168.236 255.255.255.255 在链路上 10.193.168.236 291
10.193.255.255 255.255.255.255 在链路上 10.193.168.236 291
26.0.0.0 255.0.0.0 在链路上 26.19.153.219 257
26.19.153.219 255.255.255.255 在链路上 26.19.153.219 257
26.26.26.0 255.255.255.248 在链路上 26.26.26.1 257
26.26.26.1 255.255.255.255 在链路上 26.26.26.1 257
26.26.26.7 255.255.255.255 在链路上 26.26.26.1 257
26.255.255.255 255.255.255.255 在链路上 26.19.153.219 257
127.0.0.0 255.0.0.0 在链路上 127.0.0.1 331
=====
```

利用 route print 指令可以查看路由表信息。

```
管理员: 命令提示符
10...00 ff 3f 02 f3 6c .....Sangfor SSL VPN CS Support System VNIC
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 跳点数
0.0.0.0 0.0.0.0 26.0.0.1 26.19.153.219 9257
0.0.0.0 0.0.0.0 10.193.0.1 10.193.168.236 35
0.0.0.0 128.0.0.0 26.26.26.3 26.26.26.1 1
10.193.0.0 255.255.0.0 在链路上 10.193.168.236 291
10.193.168.236 255.255.255.255 在链路上 10.193.168.236 291
10.193.255.255 255.255.255.255 在链路上 10.193.168.236 291
26.0.0.0 255.0.0.0 在链路上 26.19.153.219 257
26.19.153.219 255.255.255.255 在链路上 26.19.153.219 257
26.26.26.0 255.255.255.248 在链路上 26.26.26.1 257
26.26.26.1 255.255.255.255 在链路上 26.26.26.1 257
26.26.26.7 255.255.255.255 在链路上 26.26.26.1 257
26.255.255.255 255.255.255.255 在链路上 26.19.153.219 257
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
127.0.0.1 255.255.255.255 在链路上 127.0.0.1 331
128.0.0.0 128.0.0.0 26.26.26.3 26.26.26.1 1
192.168.45.0 255.255.255.0 在链路上 192.168.45.1 291
192.168.45.1 255.255.255.255 在链路上 192.168.45.1 291
192.168.45.255 255.255.255.255 在链路上 192.168.45.1 291
192.168.249.0 255.255.255.0 在链路上 192.168.249.1 291
192.168.249.1 255.255.255.255 在链路上 192.168.249.1 291
192.168.249.255 255.255.255.255 在链路上 192.168.249.1 291
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 26.26.26.1 257
224.0.0.0 240.0.0.0 在链路上 26.19.153.219 257
224.0.0.0 240.0.0.0 在链路上 192.168.45.1 291
224.0.0.0 240.0.0.0 在链路上 192.168.249.1 291
224.0.0.0 240.0.0.0 在链路上 10.193.168.236 291
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 26.26.26.1 257
255.255.255.255 255.255.255.255 在链路上 26.19.153.219 257
255.255.255.255 255.255.255.255 在链路上 192.168.45.1 291
255.255.255.255 255.255.255.255 在链路上 192.168.249.1 291
255.255.255.255 255.255.255.255 在链路上 10.193.168.236 291
=====
```

这个是一开始的信息，我们运行如下指令：route add 192.168.1.0 mask 255.255.255.0 192.168.0.1。添加到 192.168.1.0/24 网络的路由，网关为 192.168.0.1。此时再查看，结果如下。

网络目标	网络掩码	网关	接口	跃点数
0.0.0.0	0.0.0.0	26.0.0.1	26.19.153.219	9257
0.0.0.0	0.0.0.0	10.193.0.1	10.193.168.236	35
0.0.0.0	128.0.0.0	26.26.26.3	26.26.26.1	1
10.193.0.0	255.255.0.0	在链路上	10.193.168.236	291
10.193.168.236	255.255.255.255	在链路上	10.193.168.236	291
10.193.255.255	255.255.255.255	在链路上	10.193.168.236	291
26.0.0.0	255.0.0.0	在链路上	26.19.153.219	257
26.19.153.219	255.255.255.255	在链路上	26.19.153.219	257
26.26.26.0	255.255.255.248	在链路上	26.26.26.1	257
26.26.26.1	255.255.255.255	在链路上	26.26.26.1	257
26.26.26.7	255.255.255.255	在链路上	26.26.26.1	257
26.255.255.255	255.255.255.255	在链路上	26.19.153.219	257
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
128.0.0.0	128.0.0.0	26.26.26.3	26.26.26.1	1
192.168.1.0	255.255.255.0	192.168.0.1	26.26.26.1	2
192.168.45.0	255.255.255.0	在链路上	192.168.45.1	291
192.168.45.1	255.255.255.255	在链路上	192.168.45.1	291
192.168.45.255	255.255.255.255	在链路上	192.168.45.1	291
192.168.249.0	255.255.255.0	在链路上	192.168.249.1	291
192.168.249.1	255.255.255.255	在链路上	192.168.249.1	291
192.168.249.255	255.255.255.255	在链路上	192.168.249.1	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	26.26.26.1	257
224.0.0.0	240.0.0.0	在链路上	26.19.153.219	257
224.0.0.0	240.0.0.0	在链路上	192.168.45.1	291
224.0.0.0	240.0.0.0	在链路上	192.168.249.1	291
224.0.0.0	240.0.0.0	在链路上	10.193.168.236	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	26.26.26.1	257
255.255.255.255	255.255.255.255	在链路上	26.19.153.219	257
255.255.255.255	255.255.255.255	在链路上	192.168.45.1	291
255.255.255.255	255.255.255.255	在链路上	192.168.249.1	291
255.255.255.255	255.255.255.255	在链路上	10.193.168.236	291
<hr/>				
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	26.0.0.1	9256	
<hr/>				
IPv6 路由表				
<hr/>				
活动路由:				

可以看到这一条之前是没有的，是通过上述指令添加进去的路由。

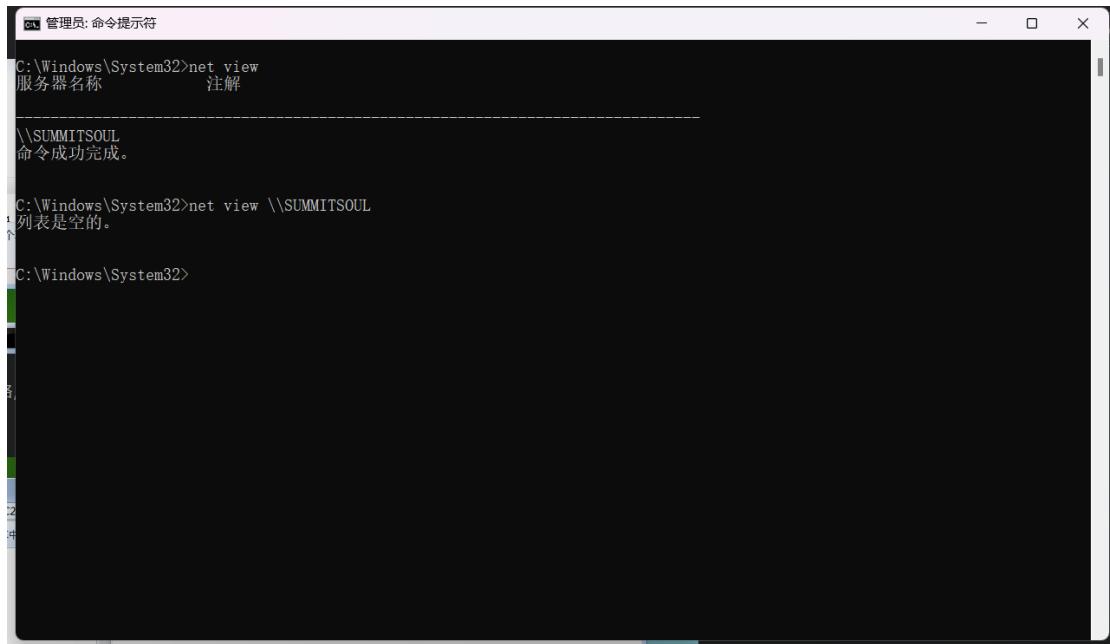
i) 显示本机的网络映射连接

```
C:\Windows\System32>net use
会记录新的网络连接。
列表是空的。

C:\Windows\System32>
```

利用 net use 指令，空的。

j) 显示局域网内某台机器的共享资源

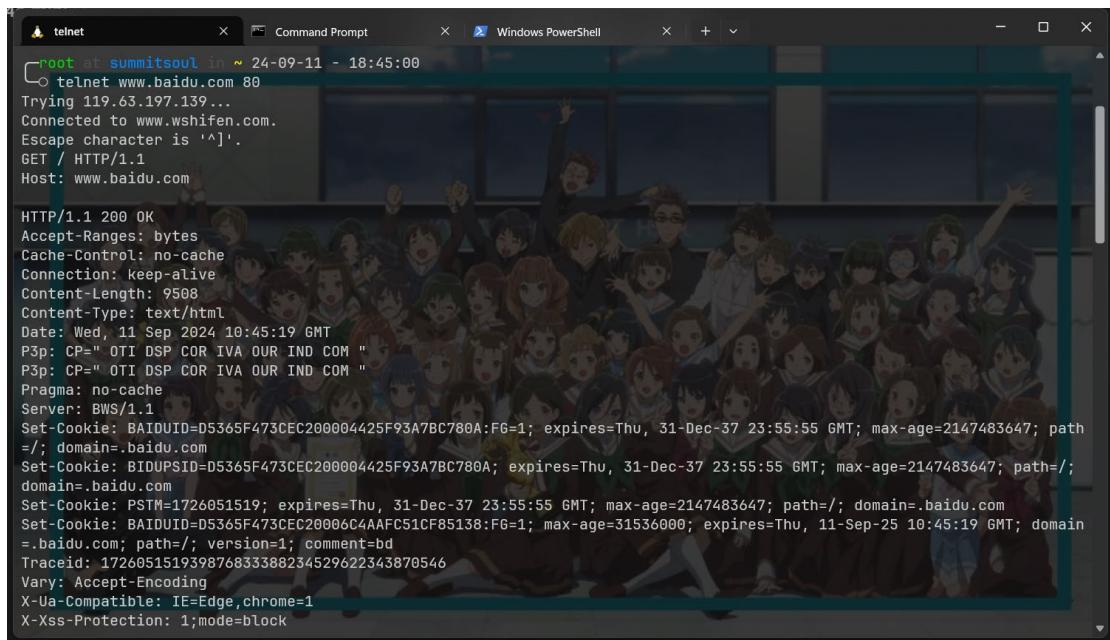


```
C:\Windows\System32>net view \\SUMMITSOUL
服务器名称      注解
\\SUMMITSOUL
命令成功完成。

C:\Windows\System32>net view \\SUMMITSOUL
列表是空的。
C:\Windows\System32>
```

因为只有一台机器，所以没有共享的资源

k) 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：

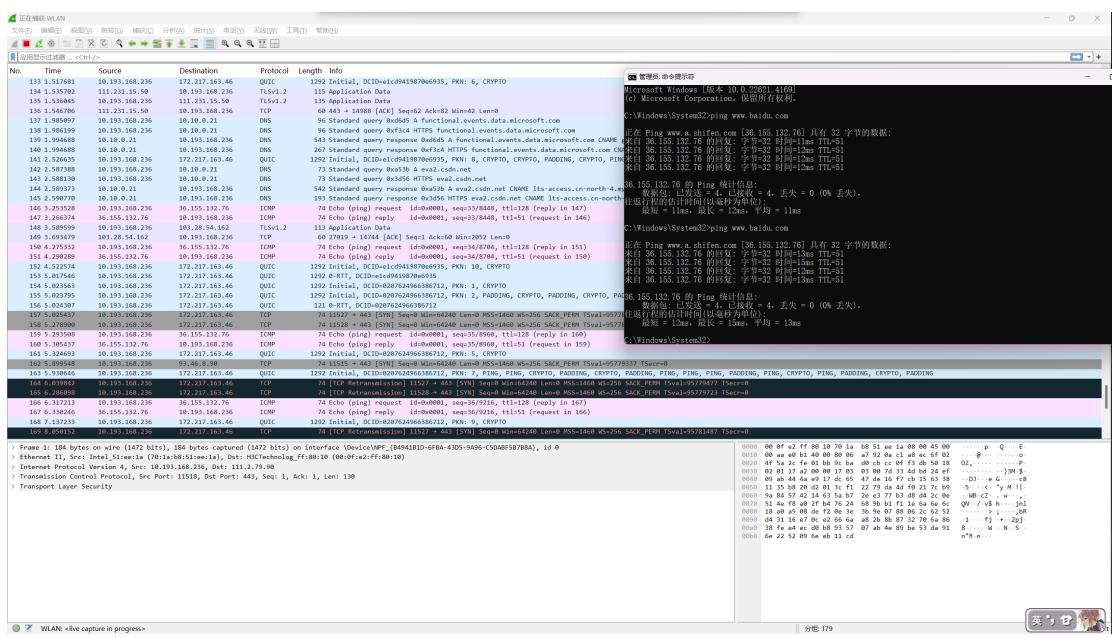


```
root at summitsoul in ~ 24-09-11 - 18:45:00
telnet www.baidu.com 80
Trying 119.63.197.139...
Connected to www.wshifen.com.
Escape character is '^].
GET / HTTP/1.1
Host: www.baidu.com

HTTP/1.1 200 OK
Accept-Ranges: bytes
Cache-Control: no-cache
Connection: keep-alive
Content-Length: 9508
Content-Type: text/html
Date: Wed, 11 Sep 2024 10:45:19 GMT
P3p: CP=" OTI DSP COR IVA OUR IND COM "
P3p: CP=" OTI DSP COR IVA OUR IND COM "
Pragma: no-cache
Server: BWS/1.1
Set-Cookie: BAIDUID=D5365F473CEC200004425F93A7BC780A;FG=1; expires=Thu, 31-Dec-37 23:55:55 GMT; max-age=2147483647; path=/; domain=.baidu.com
Set-Cookie: BTDUSID=D5365F473CEC200004425F93A7BC780A; expires=Thu, 31-Dec-37 23:55:55 GMT; max-age=2147483647; path=/; domain=.baidu.com
Set-Cookie: PSTM=1726051519; expires=Thu, 31-Dec-37 23:55:55 GMT; max-age=2147483647; path=/; domain=.baidu.com
Set-Cookie: BAIDUID=D5365F473CEC200006C4AAFC51CF85138:FG=1; max-age=31536000; expires=Thu, 11-Sep-25 10:45:19 GMT; domain=.baidu.com; path=/; version=1; comment=bd
Traceid: 172605151939876833388234529622343870546
Vary: Accept-Encoding
X-UA-Compatible: IE=Edge,chrome=1
X-Xss-Protection: 1;mode=block
```

cmd 不知道为啥，一直不好使，一直是 404，后来用 wsl 好使了。

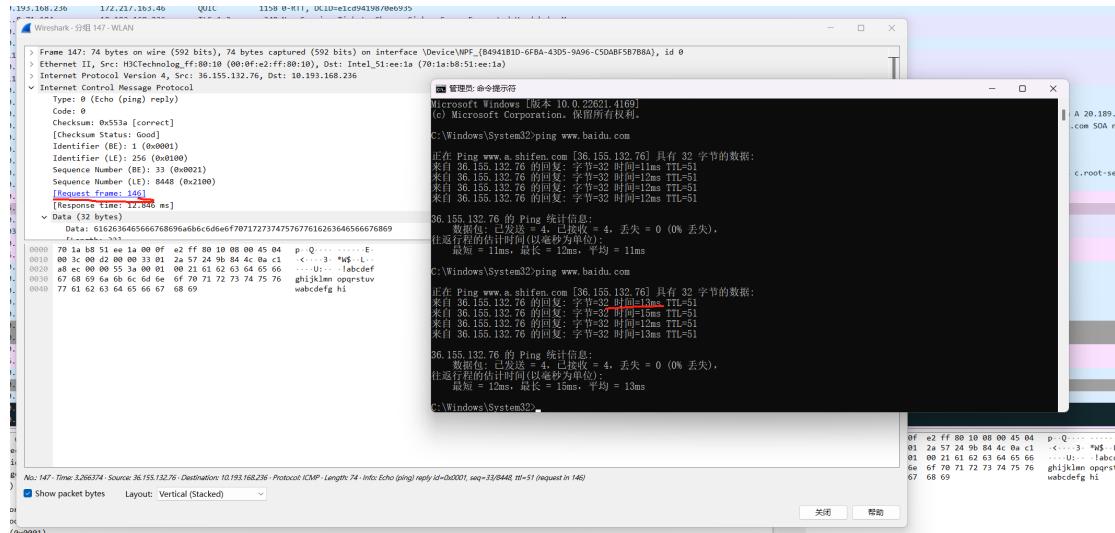
● 观察使用 ping 命令时在 Wireshark 中出现的数据包并捕获。这是什么协议？



在 ping 的同时观察 wireshark，可以看到，其中粉色的那几个字段里写了 Echo(ping)

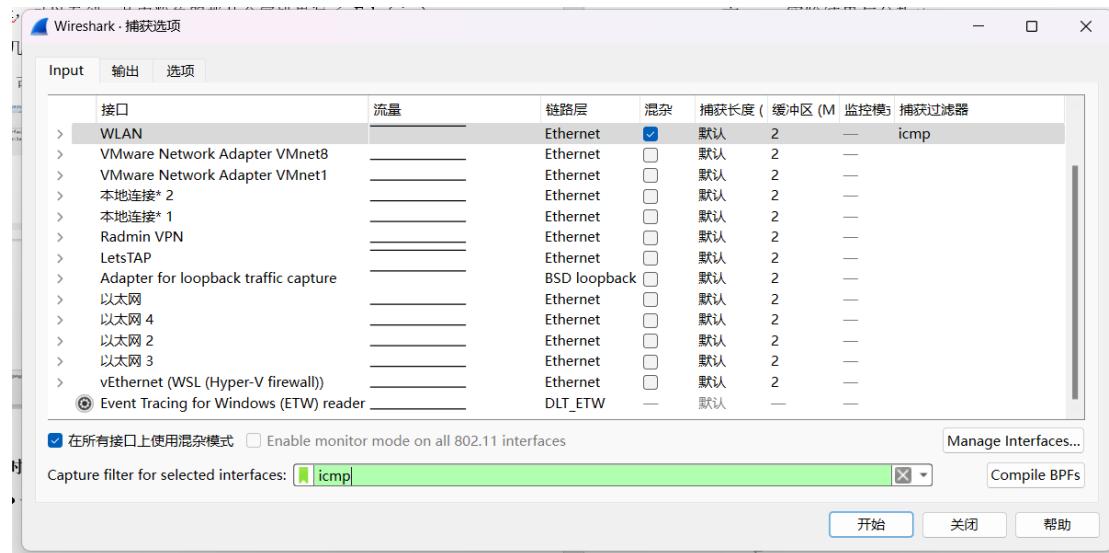
request/reply 因此，合理推测这几个是 ping 命令的数据包，我们可以看到这是 ICMP 协议。

同时我们点看查看具体的内容，可以看到时间也是对得上的。

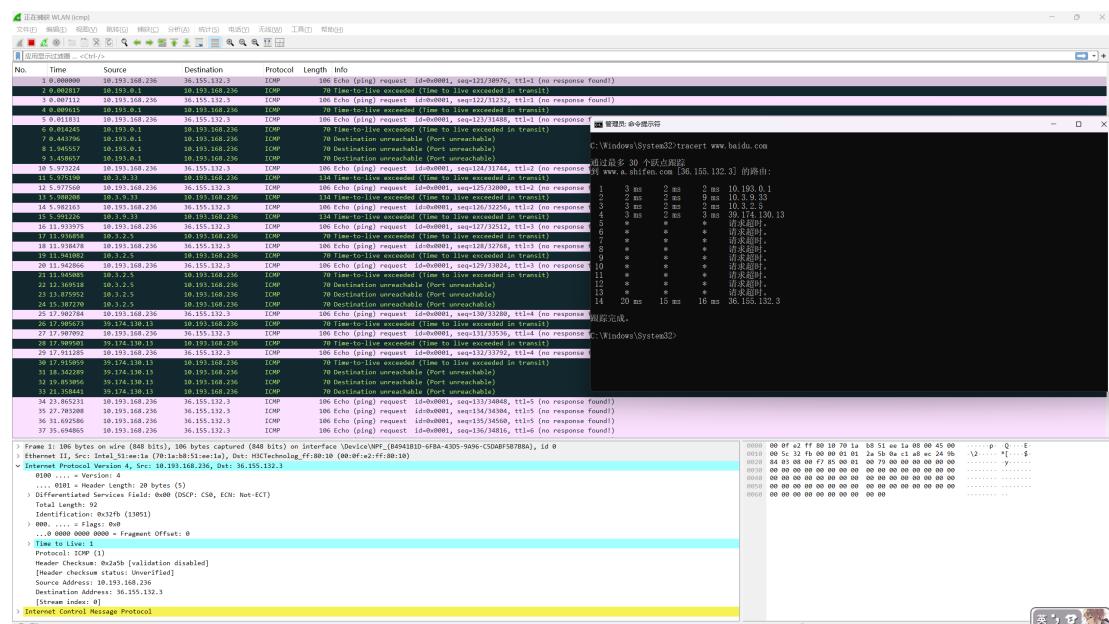


● 观察使用 tracert 命令时在 Wireshark 中出现的数据包并捕获。这是什么协议？

一开始其实猜了一下还是 ICMP 协议，感觉跟 ping 有点像，所以最开始设置了一下过滤器为 ICMP。

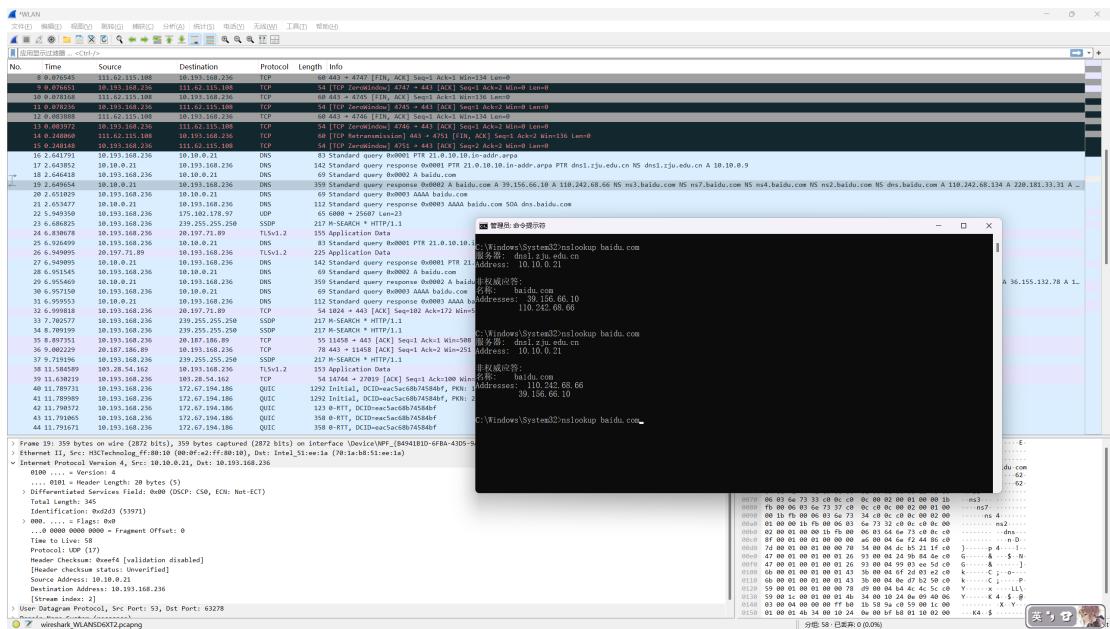


然后运行之后还是 tracert 百度。



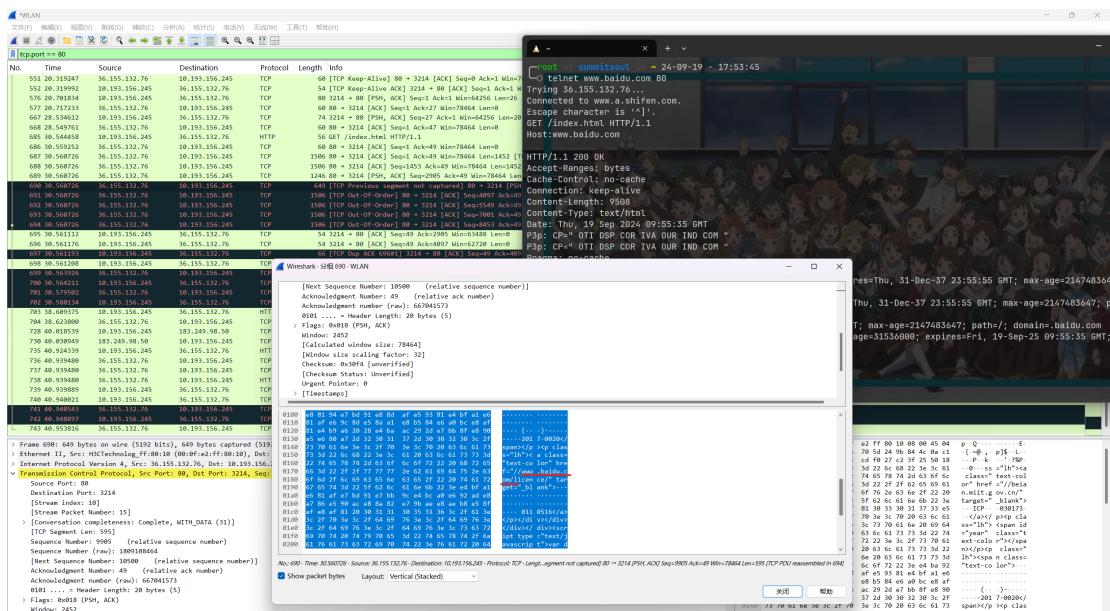
没有问题。

● 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？



这个感觉还挺好看的，在 info 中直接都有写出来 baidu.com，所以说这是 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？



因为我是 telnet 的 80 端口，所以这里设置了一下过滤器，然后查看包的详细信息里看到这里跟百度有关的内容，所以时候 TCP 协议，后面的几个包里的内容也符合抓取出来的内容，所以是 TCP 协议。

六、实验结果与分析

- Wireshark 的两种过滤器有什么不同？

捕捉过滤器是在抓包之前设置的，就直接不对其进行捕获；而显示过滤器是从捕获的数据包中进行过滤，将符合条件的进行显示出来。

- 哪些网络命令会产生在 Wireshark 中产生数据包，为什么？

感觉会产生数据包的命令都挺多的，前面说道的 ping、telnet、nslookup 这些都会产生数据包。产生的原因是它们涉及网络通信或数据交换的操作。在传输过程中数据会被打包成数据包发送到网络上，这些数据包在网络层次上被 wireshark 捕获。Wireshark 能捕捉到的所有数据包都是网络设备或操作系统在处理网络通信时生成的。

- 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？

ICMP。

ARP 消息会在需要解析 IP 地址对应的 MAC 地址时出现。

ping 域名会先有 DNS 查询，随后和 ping IP 地址一样发送 ICMP 包，而 ping IP 地址则直接进行 ICMP 通信。

七、讨论、心得

主要感觉还好，telnet 那里搞了一会，实在是不知道为啥在 cmd 上就是不好使，在 wsl 上就是可以。

补充，后来知道了，在 cmd 上他不好使是因为打字他不显示出来，真的离谱，其实也是好使的，但在 wsl 上能看到字，就一直在 wsl 上搞了。