实验一 常用网络命令及工具实验报告

组号： 7-1

姓名： 白佳兴 学号： 2204311549 班级： 计算机 2105w

一、 实验名称

常用网络命令及工具练习。

二、 实验目的

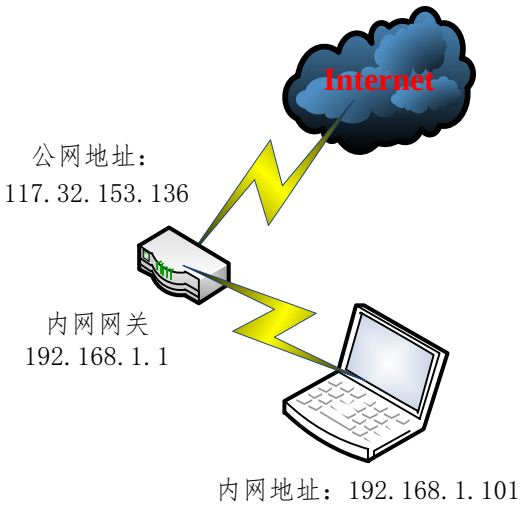
掌握常用网络命令（ping、tracert、ipconfig、route 等）的使用，掌握常用网络工具（如 Wireshark，putty 等）的使用。

三、 实验内容

1. 常用网络命令练习；
2. 网络分析软件练习。

四、 实验设备环境

按照实际网络情况绘制拓扑图，标注出内网、公网地址。【获取公网地址方式：Wireshark 抓包分析、查看路由器配置、访问 https://ip138.com/等网站和 HTTP File Server 软件等】。



五、 实验过程及结果分析

【过程记录应当详尽，截图并加以说明。以下过程和表格仅供参考。】

1. 常用网络命令练习

步骤 1：以命令行方式查看并记录本机的网络配置信息，查看本机共有几个网卡，哪些是物理网卡，哪些是虚拟网卡；【参考命令：ipconfig /all】

本机上网时用的是哪一个网卡，IP 地址、子网掩码、默认网关及 DNS 服务器地址分别是多少？

字段	配置值
上网网卡描述	Killer(R) Wi-Fi 6 AX1650i 160MHz Wireless Network Adapter (201NGW)
IP 地址	192.168.238.14
子网掩码	255.255.255.0
默认网关	192.168.238.100
DNS 服务器	192.168.238.100

步骤 2：用命令行修改本机 IP 地址和 DNS 服务器地址的获取方式（原来是自动获取方式则改为手动设置，原来为手动设置地址则改为自动获取）查看并记录网卡配置信息，与手动设置地址时的配置有什么不同（注意观察租约时间）？

【参考命令：

IP 地址手动设置命令：netsh interface ip set address name="本地连接" static 192.168.1.101 255.255.255.0 192.168.1.1；

DNS 服务器地址手动设置命令：netsh interface ip set dns name="本地连接" source=static add=202.117.1.20；

IP 地址自动获取命令：netsh interface ip set address name="本地连接" source=dhcp；

DNS 服务器地址自动获取设置命令：netsh interface ip set dns name="本地连接" source=dhcp。

（注意将 name、IP 地址等参数改为自己电脑网卡的实际参数）】


WLAN 属性
IP 分配: 手动
IPv4 地址: 192.168.238.14
IPv4 掩码: 255.255.255.0
IPv4 网关: 192.168.238.100
DNS 服务器分配: 手动
IPv4 DNS 服务器: 192.168.238.100 (未加密)
SSID: 奋斗是青春最美的底色
协议: Wi-Fi 4 (802.11n)
安全类型: WPA2-个人
制造商: Intel Corporation
描述: Killer(R) Wi-Fi 6 AX1650i 160MHz Wireless Network Adapter (201NGW)
驱动程序版本: 22.250.10.1
网络频带: 2.4 GHz
网络通道: 11
链接速度(接收/传输): 144/130 (Mbps)
IPv6 地址: 2409:8970:379:1b08:cad1:ffbf:607:969
本地链接 IPv6 地址: fe80::4059:fdca:b26e:dcf5%22
IPv4 地址: 192.168.238.14
IPv4 DNS 服务器: 192.168.238.100 (未加密)
物理地址(MAC): E4-5E-37-D2-86-3D


Internet 协议版本 4 (TCP/IPv4) 属性
常规
如果网络支持此功能，则可以获取自动指派的 IP 设置。否则，你需要从网络系统管理员处获得适当的 IP 设置。
自动获得 IP 地址(O)
使用下面的 IP 地址(S):
IP 地址(I): 192 . 168 . 238 . 14
子网掩码(U): 255 . 255 . 255 . 0
默认网关(D): 192 . 168 . 238 . 100
自动获得 DNS 服务器地址(B)
使用下面的 DNS 服务器地址(E):
首选 DNS 服务器(P): 192 . 168 . 238 . 100
备用 DNS 服务器(A): . . .
退出时验证设置(L)
高级(V)...
确定
取消

步骤 3：查看并记录本机的路由表，标记出默认路由。用命令行删除默认路由，看看本机还能否上网并分析原因（如果还能上网，查看是否开启了 IPv6，可禁用后再试）。查看网卡的默认网关配置是否还在？【参考命令：route print，route delete，ipconfig】

```
C:\Windows\System32>route delete 0.0.0.0
 操作完成!

C:\Windows\System32>route print
===========================================================================
接口列表
  6...00 ff 1c 11 2e 81 ......TAP-Windows Adapter V9
  8...e4 5e 37 d2 86 3e ......Microsoft Wi-Fi Direct Virtual Adapter
 10...e6 5e 37 d2 86 3d ......Microsoft Wi-Fi Direct Virtual Adapter #2
 20...00 ff dc 42 29 41 ......Netease UU TAP-Win32 Adapter V9.21
 16...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
 22...e4 5e 37 d2 86 3d ......Killer(R) Wi-Fi 6 AX1650i 160MHz Wireless Network Adapter (201NGW)
 11...70 b5 e8 9d 84 8a ......Killer E2500 Gigabit Ethernet Controller
  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
        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
    192.168.132.0    255.255.255.0         在链路上     192.168.132.1    291
    192.168.132.1  255.255.255.255         在链路上     192.168.132.1    291
  192.168.132.255  255.255.255.255         在链路上     192.168.132.1    291
    192.168.134.0    255.255.255.0         在链路上     192.168.134.1    291
    192.168.134.1  255.255.255.255         在链路上     192.168.134.1    291
  192.168.134.255  255.255.255.255         在链路上     192.168.134.1    291
    192.168.238.0    255.255.255.0         在链路上    192.168.238.14    306
   192.168.238.14  255.255.255.255         在链路上    192.168.238.14    306
  192.168.238.255  255.255.255.255         在链路上    192.168.238.14    306
```

删除默认路由之后无法上网的原因：删除默认路由可能导致设备无法将数据包传送到互联网。没有默认路由，设备不知道要将数据包发送到何处以便访问互联网上的主机或网络

步骤 4：分别用 route add 和 route add -p 增加一条默认路由，看看它们会出现在哪个路由表里，这两个路由表中的路由有什么不同？

```
C:\Windows\System32>route add 0.0.0.0 mask 0.0.0.0 192.168.238.101
 操作完成!

C:\Windows\System32>route add -p 0.0.0.0 mask 0.0.0.0 192.168.238.102
 操作完成!
```

```
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  192.168.238.100   192.168.238.14     50
          0.0.0.0          0.0.0.0  192.168.238.101   192.168.238.14     51
          0.0.0.0          0.0.0.0  192.168.238.102   192.168.238.14     51
     36.155.132.0    255.255.255.0  192.168.238.100   192.168.238.14     51
        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
    192.168.132.0    255.255.255.0         在链路上     192.168.132.1    291
    192.168.132.1  255.255.255.255         在链路上     192.168.132.1    291
  192.168.132.255  255.255.255.255         在链路上     192.168.132.1    291
    192.168.134.0    255.255.255.0         在链路上     192.168.134.1    291
    192.168.134.1  255.255.255.255         在链路上     192.168.134.1    291
  192.168.134.255  255.255.255.255         在链路上     192.168.134.1    291
    192.168.238.0    255.255.255.0         在链路上    192.168.238.14    306
   192.168.238.14  255.255.255.255         在链路上    192.168.238.14    306
  192.168.238.255  255.255.255.255         在链路上    192.168.238.14    306
        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     192.168.134.1    291
        224.0.0.0        240.0.0.0         在链路上     192.168.132.1    291
        224.0.0.0        240.0.0.0         在链路上    192.168.238.14    306
  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     192.168.134.1    291
  255.255.255.255  255.255.255.255         在链路上     192.168.132.1    291
  255.255.255.255  255.255.255.255         在链路上    192.168.238.14    306
===========================================================================
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  192.168.238.102        1
===========================================================================
```

Route add 添加的路由出现在活动路由之中，route add -p 添加的路由会出现在活动路由和永久路由之中。

二者的区别是前者是临时性质的，这些路由表项在系统重新启动后将会被删除。后者是永久性质的，这些路由表项将会在系统重新启动后保留下来。

步骤 5：在命令行运行 ipconfig /flushdns 清除本地 DNS 缓存，ping 通一个网址（如 www.xjtu.edu.cn）后，用 ipconfig /displaydns 查看本地 DNS 缓存，记录域名与 IP 地址。

```
C:\Windows\System32>ipconfig /flushdns

Windows IP 配置

已成功刷新 DNS 解析缓存。

C:\Windows\System32>ping www.xjtu.edu.cn

正在 Ping www.xjtu.edu.cn [2001:250:1001:1::ca75:10d] 具有 32 字节的数据:
来自 2001:250:1001:1::ca75:10d 的回复: 时间=84ms
来自 2001:250:1001:1::ca75:10d 的回复: 时间=84ms
来自 2001:250:1001:1::ca75:10d 的回复: 时间=93ms
来自 2001:250:1001:1::ca75:10d 的回复: 时间=84ms

2001:250:1001:1::ca75:10d 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 = 84ms，最长 = 93ms，平均 = 86ms

C:\Windows\System32>ipconfig /displaydns

Windows IP 配置

    tpstelemetry.tencent.com
    ----------------------------------------
    记录名称. . . . . : tpstelemetry.tencent.com
    记录类型. . . . . : 28
    生存时间. . . . . : 24
    数据长度. . . . . : 16
    部分. . . . . : 答案
    AAAA 记录 . . . . . : 240e:97c:2f:2::5c


    记录名称. . . . . : ns-cmn1.qq.com
    记录类型. . . . . : 28
    生存时间. . . . . : 24
    数据长度. . . . . : 16
    部分. . . . . : 其他
    AAAA 记录 . . . . . : 2402:4e00:111:ff4::3
```

```
www.xjtu.edu.cn
----------------------------------------
记录名称. . . . . : www.xjtu.edu.cn
记录类型. . . . . : 1
生存时间. . . . . : 675
数据长度. . . . . : 4
部分. . . . . : 答案
A (主机)记录 . . . . : 202.117.1.13

记录名称. . . . . : ns2.xjtu.edu.cn
记录类型. . . . . : 1
生存时间. . . . . : 675
数据长度. . . . . : 4
部分. . . . . : 其他
A (主机)记录 . . . . : 202.117.0.21

记录名称. . . . . : dec3000.xjtu.edu.cn
记录类型. . . . . : 1
生存时间. . . . . : 675
数据长度. . . . . : 4
部分. . . . . : 其他
A (主机)记录 . . . . : 202.117.0.20
```

步骤 6：把网卡的 DNS 服务器地址修改为无效 DNS 地址，分别 ping 域名和 IP 地址看能否 ping 通，查看本地 DNS 缓存，记录结果并分析原因。【参考命令：netsh interface ip set dns name="本地连接" source=static add=202.117.1.222】

```
C:\Windows\System32>netsh interface ip set dns name="WLAN" source=static add=202.117.1.222

配置的 DNS 服务器不正确或不存在。


C:\Windows\System32>ping www.xjtu.edu.cn
Ping 请求找不到主机 www.xjtu.edu.cn。请检查该名称，然后重试。

C:\Windows\System32>ping 202.117.1.13

正在 Ping 202.117.1.13 具有 32 字节的数据:
来自 202.117.1.13 的回复: 字节=32 时间=10ms TTL=60
来自 202.117.1.13 的回复: 字节=32 时间=4ms TTL=60
来自 202.117.1.13 的回复: 字节=32 时间=7ms TTL=60
来自 202.117.1.13 的回复: 字节=32 时间=7ms TTL=60

202.117.1.13 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 = 4ms，最长 = 10ms，平均 = 7ms
```

当 ping 一个域名的时候，计算机会将域名发送到相应的 DNS 服务器用来获取其 IP 地址，但是此时 DNS 服务器地址无效，DNS 解析失败，所以计算机也就不会得到域名的 IP 地址，故而 ping 失败。

如果直接 Ping 一个 IP 地址，而不需要进行 DNS 解析，Ping 命令会直接使用该 IP 地址进行 Ping。因此，即使 DNS 服务器地址无效，也可以通过直接 Ping IP 地址来进行通信。

2. 网络分析工具练习

步骤 1：将网卡禁用后再启用，打开 Wireshark 软件抓包，能够正常上网后（打开网页、登录微信成功等）停止抓包。查看捕获的数据包及涉及到的协议，选择 2 种协议（如 DHCP，ARP 等，利用协议过滤筛选出该协议报文），分析协议的功能及关键交互数据。

协议名	描述项	配置值
ARP	*协议功能*	*IP 地址对应 MAC 地址解析*
	源地址-目的地址	*192.168.238.14- Broadcast*
	请求/应答信息	*Who has 192.168.238.100? Tell 192.168.238.14*
ARP	协议功能	*IP 地址对应 MAC 地址解析*
	源地址-目的地址	*192.168.238.100- 192.168.238.14*
	请求/应答信息	192.168.238.100 is at 46:55:08:05:19:26
DHCP	协议功能	集中对用户 IP 地址进行动态管理和配置
	源地址-目的地址	0.0.0.0 - 255.255.255.255
	请求/应答信息	DHCP Request - Transaction ID 0xf495c6e1

步骤 2：清除本机的 DNS 缓存【参考命令：ipconfig /flushdns】，运行 Wireshark 截获报文，浏览器访问网站（如 http://github.com，浏览新闻，下载软件等），利用 IP 地址过滤筛选出访问该网站的报文，查看访问该网站时，都用到了哪些协议，主要作用是什么？【域名解析为 IP 地址方法：ping 域名，或 nslookup 域名】

协议名	描述项	配置值
TCP	*协议功能*	*传输控制协议,在不可靠的互联网络上提供可靠的端到端传输。*
	源地址-目的地址	*2409:8970:379:1b08:35ff:9cb7:a231:d8e5 - 2001:250:1001:1::ca75:10d*
	请求/应答信息	*12855 → 80 [SYN] Seq=0 Win=64800 Len=0 MSS=1350 WS=256 SACK_PERM*
ARP	协议功能	*IP 地址对应 MAC 地址解析*
	源地址-目的地址	46:55:08:05:19:26 - Intel_d2:86:3d
	请求/应答信息	Who has 192.168.238.14? Tell 192.168.238.100
DNS	协议功能	将域名解析成对应的 ip 地址
	源地址-目的地址	192.168.238.14 - 192.168.238.100
	请求/应答信息	Standard query 0x5d4a A www.google.com

步骤 3：运行 Wireshark 截获报文，登陆 QQ 或微信，和好友进行语音或者视频聊天。查看截获的报文，找出 QQ 或微信的服务器地址，分析语音或视频通信过程中双方的 IP 地址、协议及端口等信息。

106.119.179.191 IP 106.119.179.191 的地理位置

输入IP地址或域名进行查询 106.119.179.191 查询

您查询的IP地址: 106.119.179.191

IP : 106.119.179.191 的地理位置信息

准确归属地: 106.119.179.191 -> 河北省唐山市 电信

参考归属地: 106.119.179.191 -> 中国 河北 石家庄

No.	Time	Source	Destination	Protocol	Lengtl	Info
166	5.545795	106.119.179.191	10.164.255.107	UDP	108	8000 → 65179 Len=66
167	5.557343	106.119.179.191	10.164.255.107	UDP	101	8000 → 65179 Len=59
168	5.561354	10.164.255.107	106.119.179.191	UDP	84	65179 → 8000 Len=42
169	5.580098	106.119.179.191	10.164.255.107	UDP	112	8000 → 65179 Len=70
170	5.581362	10.164.255.107	106.119.179.191	UDP	86	65179 → 8000 Len=44
171	5.598177	106.119.179.191	10.164.255.107	UDP	103	8000 → 65179 Len=61
172	5.601343	10.164.255.107	106.119.179.191	UDP	84	65179 → 8000 Len=42
173	5.621387	10.164.255.107	106.119.179.191	UDP	86	65179 → 8000 Len=44
174	5.629751	106.119.179.191	10.164.255.107	UDP	97	8000 → 65179 Len=55
175	5.640719	106.119.179.191	10.164.255.107	UDP	108	8000 → 65179 Len=66

本机捕获信息

描述项	值
QQ/微信服务器地址	106.119.179.191
本机 IP 地址	10.164.255.107
本机自测公网地址	117.32.155.38
通信好友的 IP 地址	10.164.243.102
通信协议（Protocol）	UDP
通信源端口-目的端口	65179 - 8000

192	1.440016	106.119.172.17	10.164.243.102	UDP	82	8000 → 55326 Len=40
193	1.444339	10.164.243.102	106.119.172.17	UDP	108	55326 → 8000 Len=66
194	1.459456	106.119.172.17	10.164.243.102	UDP	82	8000 → 55326 Len=40
195	1.464418	10.164.243.102	106.119.172.17	UDP	106	55326 → 8000 Len=64
196	1.479268	106.119.172.17	10.164.243.102	UDP	82	8000 → 55326 Len=40
197	1.484589	10.164.243.102	106.119.172.17	UDP	99	55326 → 8000 Len=57
198	1.498993	106.119.172.17	10.164.243.102	UDP	82	8000 → 55326 Len=40
199	1.504593	10.164.243.102	106.119.172.17	UDP	94	55326 → 8000 Len=52
200	1.520981	106.119.172.17	10.164.243.102	UDP	82	8000 → 55326 Len=40
201	1.524542	10.164.243.102	106.119.172.17	UDP	92	55326 → 8000 Len=50
202	1.541891	106.119.172.17	10.164.243.102	UDP	82	8000 → 55326 Len=40
203	1.544554	10.164.243.102	106.119.172.17	UDP	92	55326 → 8000 Len=50
204	1.564570	10.164.243.102	106.119.172.17	UDP	92	55326 → 8000 Len=50

好友端捕获信息

描述项	值
QQ/微信服务器地址	106.119.172.17
本机 IP 地址	10.164.243.102
本机自测公网地址	117.32.155.38
通信好友的 IP 地址	10.164.255.107
通信协议（Protocol）	UDP
通信源端口-目的端口	55326 - 8000

3. 互动讨论主题

本地计算机接入网络之后，需要通过哪些设置、启用哪些协议之后才能上网（通过域名访问网站等）。

需要设置路由器和网卡。

对于路由器，首先需要连接网线和电源，然后需要设置路由器的连接方式。

对于网卡，需要设置 IP 地址、子网掩码、默认网关、DNS 服务器地址后才能访问互联网。

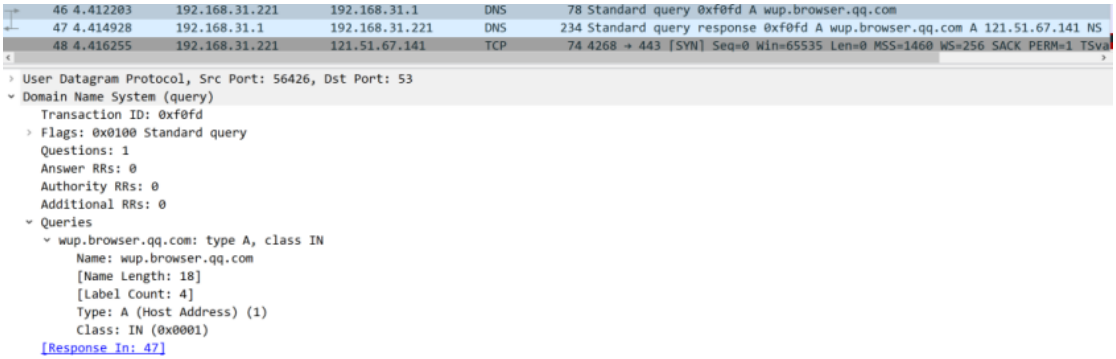
需要启用的协议有 DHCP 协议、IP 协议、DNS 协议、ARP 协议、TCP 协议、UDP 协议、HTTP 协议等

4. *进阶自设计

通过 Wireshark 抓包分析 QQ 的登陆认证、消息传输、语音/视频通话、退出等过程，分析各过程中涉及到的协议、服务器地址和数据包标识等。

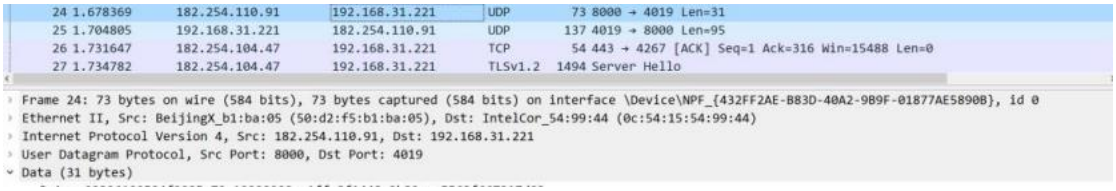
【OICQ 是 QQ 的专用协议类型，注意观察数据包中的标识，看看能找到多少种类型的 OICQ 数据包，可利用这些数据包区分各个功能段。综合利用 Wireshark 软件的协议过滤、IP 地址过滤、数据流追踪等功能，找出 QQ 各个过程对应的数据包段。】

DNS 协议



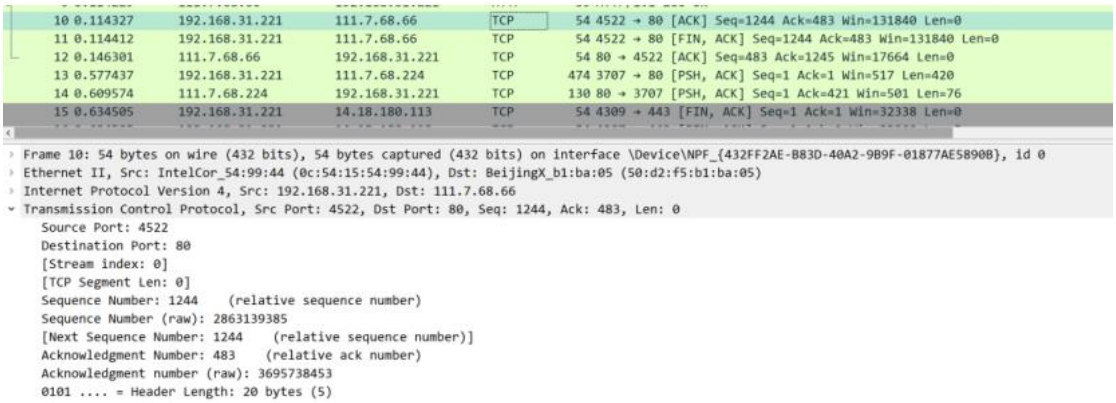
关键数据和标识：后缀带有 browser.qq.com。

UDP 协议



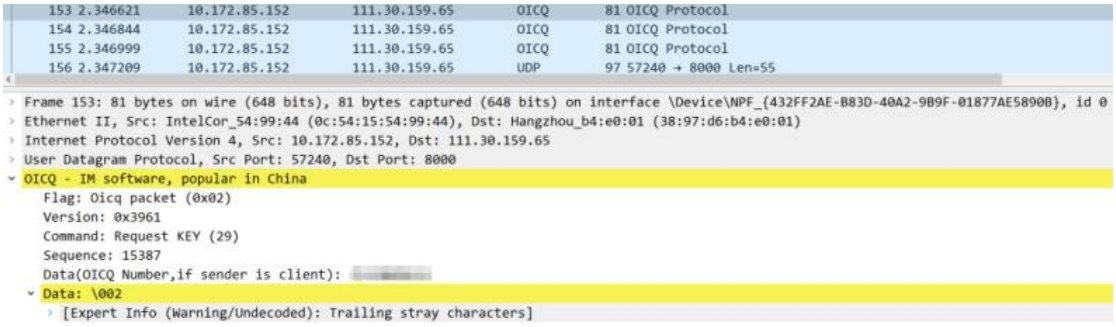
关键数据和标识：目的 ip 地址为 QQ 服务器地址，端口号为 8000。

TCP 协议



关键数据和标识：目的 ip 地址所在地为深圳市，并且端口号为 80。

OICQ 协议



关键数据和标识：Command 行的值为 Request KEY ，Data 行的值为正在 登陆的 QQ 号。

六、 总结及心得体会

这次实验共分为两部分，一是利用命令行命令查看、修改网络配置，二是学习如何抓包，并对报文进行分析。需要注意的是在手动设置主机 ip 地址、子网掩码、网关和 DNS 服务器地址时，不能盲目照抄参考书上的命令，因为每台主机所处的网络环境不同，故对应的地址都不一样,需要在当前主机能正常访问互联网时利用 ipconfig/all 查 看对应网卡的配置信息，然后再手动修改为和配置信息相同的地址。注意只有在以上几个地址均设置正确的情况下才能正常访问互联网。通过这次实验我学会了用 ipconfig/all 命令查看主机的网络配置信息，用 netsh 语句手动或自动配置 ip 地址和 dns 服务器地址，还学会了利用 route 语句打印路由表、增删路由表条目。同时通过使用 wireshark 软件抓取并对数据包进行分析，我还了解到了在访问网页和过程中涉及到的相关协议及其对应功能