《计算机网络第三次实验》

班级：信安2302班

学号：202308060227

姓名：石云博

目录

[一. 问题描述 2](#_Toc193022805)

[二. 问题分析 3](#_Toc193022806)

[三. 实验过程及代码 3](#_Toc193022807)

[四. 结论 14](#_Toc193022808)

[五. 参考文献 14](#_Toc193022809)

# 问题描述

Assignment 3: Measure the WiFi hotspot

1.Write a program that can probe and record the WiFi hotspots around Yuelu Mountain, visualize them in a map, as many as possible

2.Measure/eavesdrop/estimate their network performance: Loss, delay, bandwidth, find their home AS

3.Probe their security modes, find the proportion of different security settings Talk about your methods and results, any interesting point?

# 问题分析

问题中要求我们探测岳麓山附近的热点情况，我们首先要知道怎么将手机上的热点情况记录下来，即怎么获取手机网络状态，Android 可以使用软件TelephonyManager ，iOS可以使用软件 CoreTelephony 获取移动网络信息。

在 Linux 系统上，则可使用 nmcli 或 qmicli。

然后，我们要记录地址信息以在地图上显示化表述出来，这里首先想到的是gps，但是网上的资料表明wifi和蓝牙定位都是可行的。

最后，我们要绘制信息地图，可以使用Matplotlib或Foliu 在地图上绘制基站和网络模式。

对于这些网络的测试，测试丢包可以使用使用 ping 连续发送 ICMP 数据包，计算丢包，延时可以使用 ping 计算 RTT（Round Trip Time），带宽可以下载Speedtest来进行测试，要找到Wi-Fi热点IP的归属AS，需要获取其外网IP并查询ASN信息，我们可以使用网站<https://ipinfo.io/>来进行在线的查询。

最后，找出其安全模式，网上找资料，得到一般网络的安全模式有以下几种：

**WPA3-Personal**：家庭WiFi网络的最佳安全设置，**WPA3-企业**：企业的最佳安全设置，**WPA2 (AES)**：第二好的安全设置，在更多路由器上可用，**WPA/WPA2-PSK (TKIP/AES)**：对于旧设备网络的最佳安全设置，但在大多数路由器上不可用，**WPA2-PSK (TKIP)**：仍然可用，但仅提供最低限度的安全性。

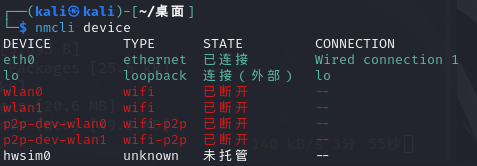
# 实验过程及代码

首先，我们要获取周围的wifi热点信息，可以使用linux中的nmcli也可以使用windows中自带的指令“netsh wlan show interfaces”。

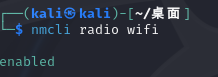
我们首先使用linux中的nmcli，使用kali打开：



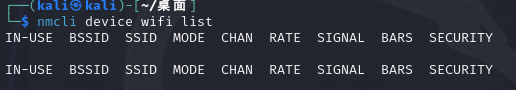
使用指令“nmcli device”查看当前设备的网络设施：

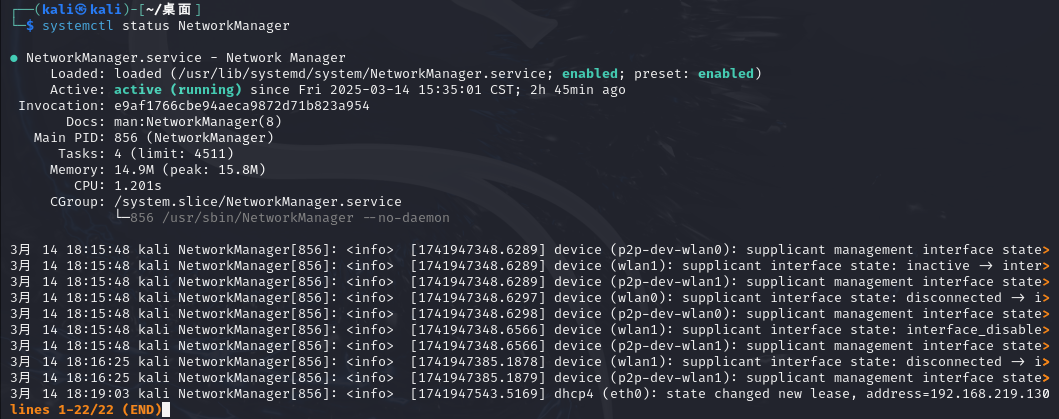


我们需要用到wlan0中的wifi，这里显示已断开，我们试着检查wifi状态，使用指令“nmcli radio wifi”来查看：

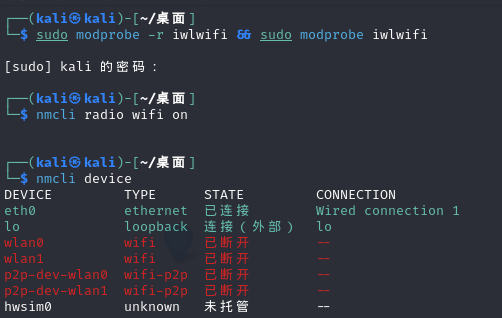


我们发现wifi是打开了的，我们尝试查找附近wifi，使用指令“nmcli device wifi list”：



可以看到还是没有结果。再检查 NetworkManager 是否运行：

可以看到处于运行状态，试着重新加载wifi驱动，再重新打开WiFi：

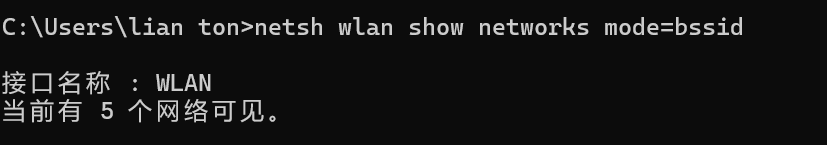


可以看到wifi还是处于断开状态。网上查原因，可能是当系统内无第三方网络管理工具（如 nm）时，系统默认使用 interfaces 文件内的参数进行网络配置。

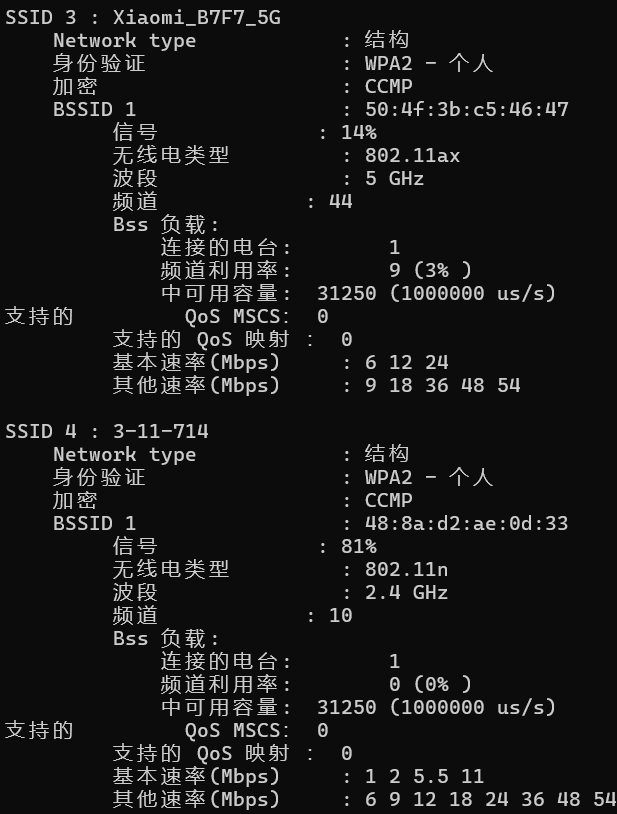
当系统内安装了 nm 之后，nm 默认接管了系统的网络配置，使用 nm 自己的网络配置参数来进行配置。

没有办法，我们转用windows系统下的工具来探测网络。

在windows终端中使用指令“netsh wlan show networks mode=bssid”：

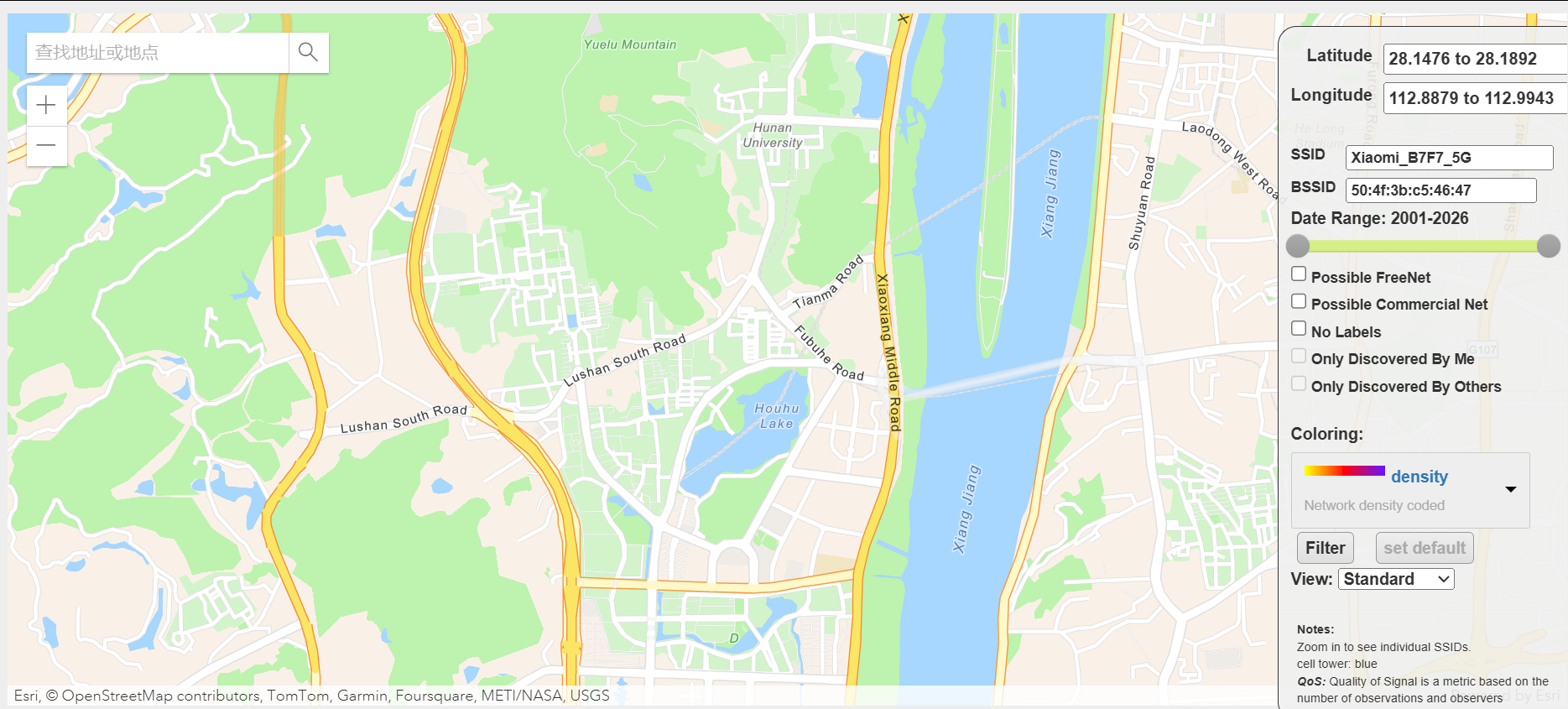


可以看到我们这里得到了五个结果，每个结果里面包含了该wifi的具体信息：



里面包含了ssid，bssid，类型，加密，速率等等。

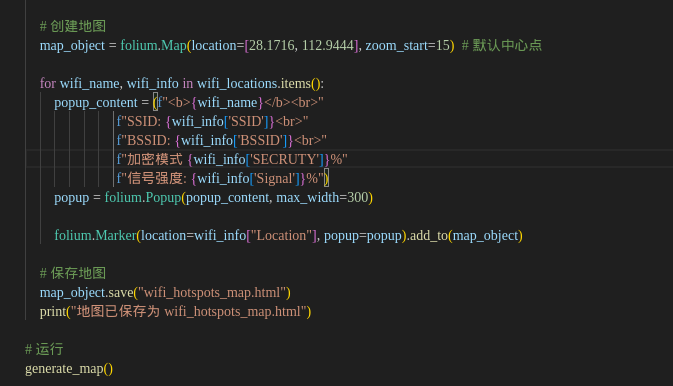
得到了这些信息之后，我们就要开始绘制信息地图了。这里我们可以用到一个地图网站<https://wigle.net/index>：





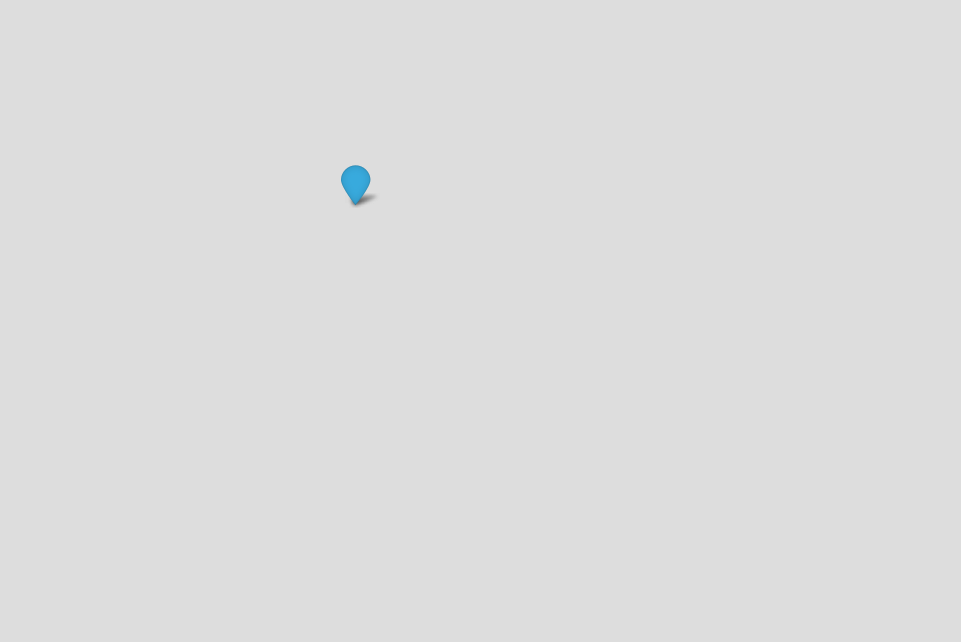
右边可以设置的信息中，我们可以输入ssid和bssid来获得其经纬度以及定位到大概的位置，可以看到图上大概就是岳麓山附近位置。

但是这里不好添加信息到地图中，而且最多只能使用五次，所以我转头使用folium画图。我们使用python来实现这个画图：

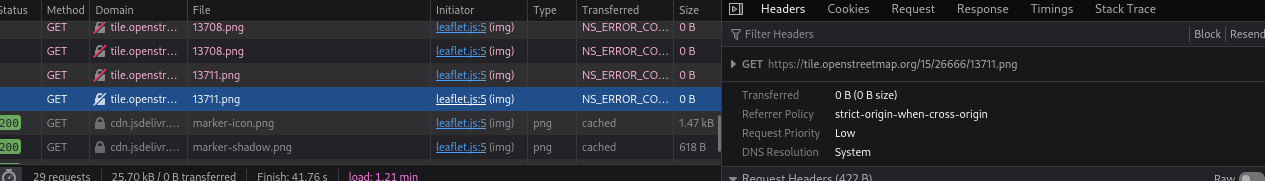


使用python3来运行该py文件，生成地图文件。

打开地图文件：



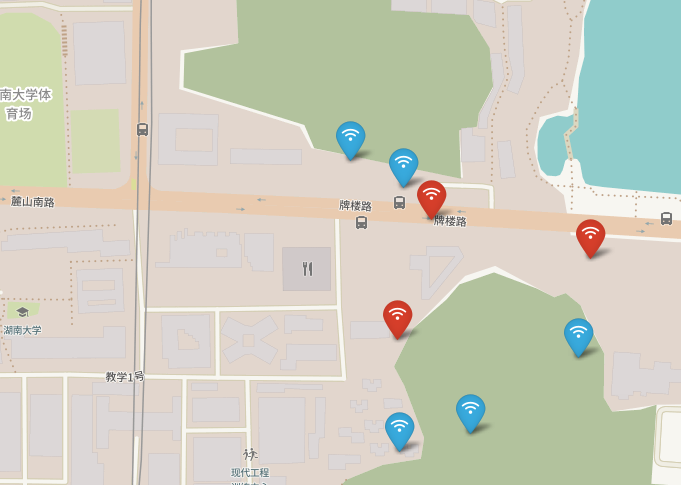
发现地图加载不出来，只有节点，查看浏览器的网络流量情况，发现有很多内容没有被正确地get到。



把这个问题反馈给chatgpt，得到答案“如果 tile.openstreetmap.org 速度慢或被屏蔽，可在 folium（或其他地图库）中更换为其他 Tile Provider。例如使用 openstreetmap.fr 镜像”，于是我们在原有代码中加上tiles="https://{s}.tile.openstreetmap.fr/hot/{z}/{x}/{y}.png",

attr="OpenStreetMap FR“

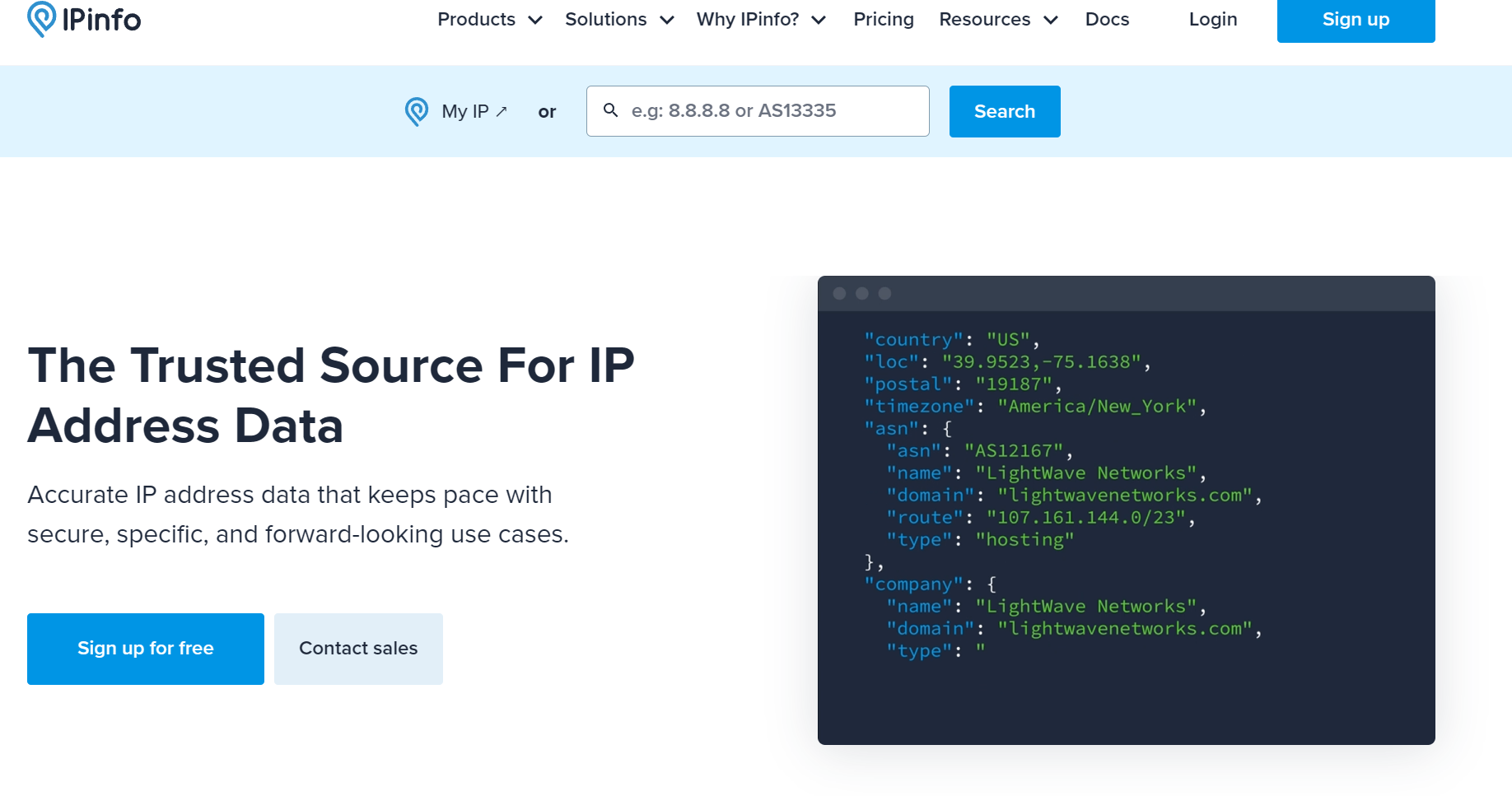
再次生成地图文件，打开：



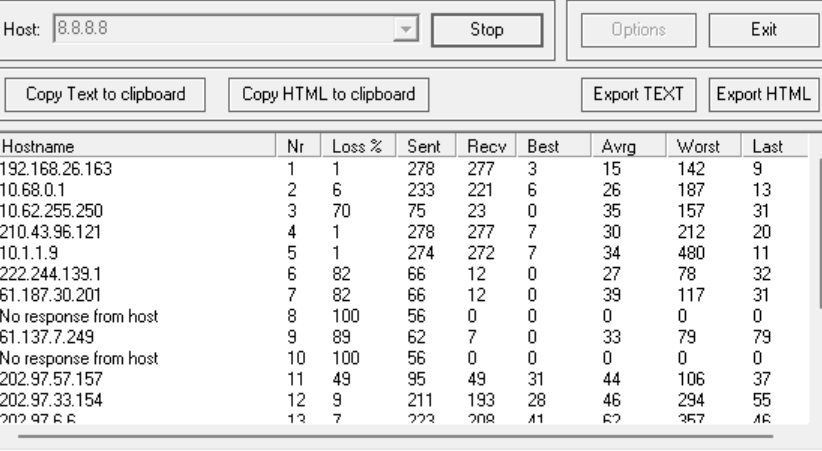


第二部分：测量/窃听/评估他们的网络性能：丢包、延迟、带宽、找到他们的归属 AS

测试丢包可以使用使用 ping 连续发送 ICMP 数据包，计算丢包，延时可以使用 ping 计算 RTT（Round Trip Time），带宽可以下载Speedtest来进行测试，要找到Wi-Fi热点IP的归属AS，需要获取其外网IP并查询ASN信息，我们可以使用网站<https://ipinfo.io/>来进行在线的查询：

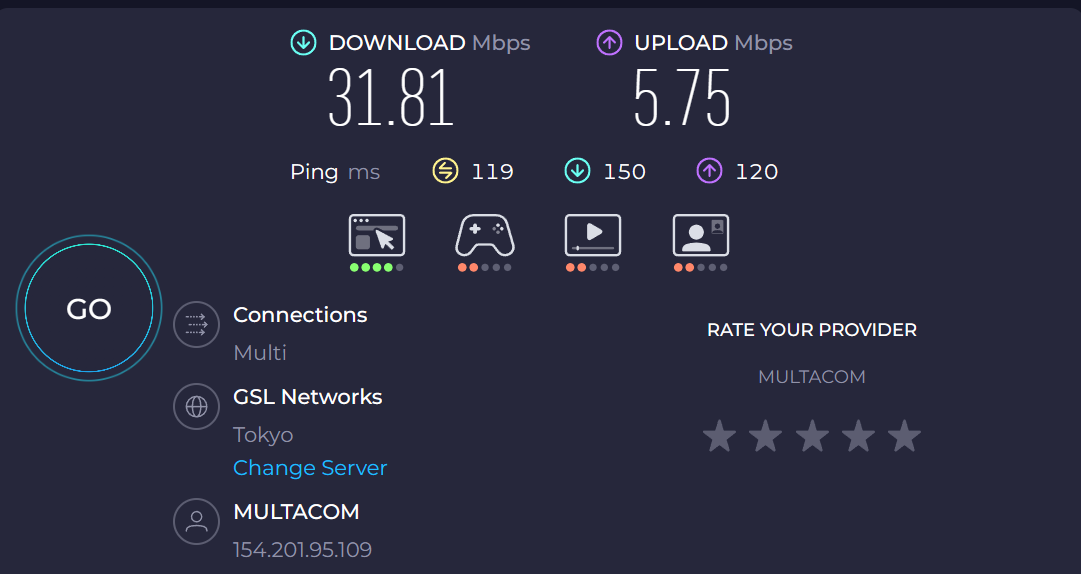


对于延迟和丢包，我选择了使用软件winMTR来进行测试。首先我们电脑连接要测试的对象，然后对于host：8.8.8.8来进行测试，得到如下结果：



我们可以看到对于只有一条的情况，也就是Nr=1，其丢包率为百分之一，最低延迟3，最高延迟143，平均延迟为15.

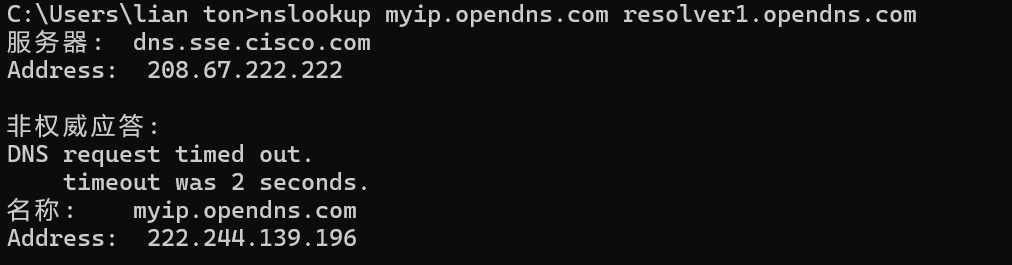
接下来测试带宽，我们选择在Speedtest网站上直接进行在线测速，得到结果：



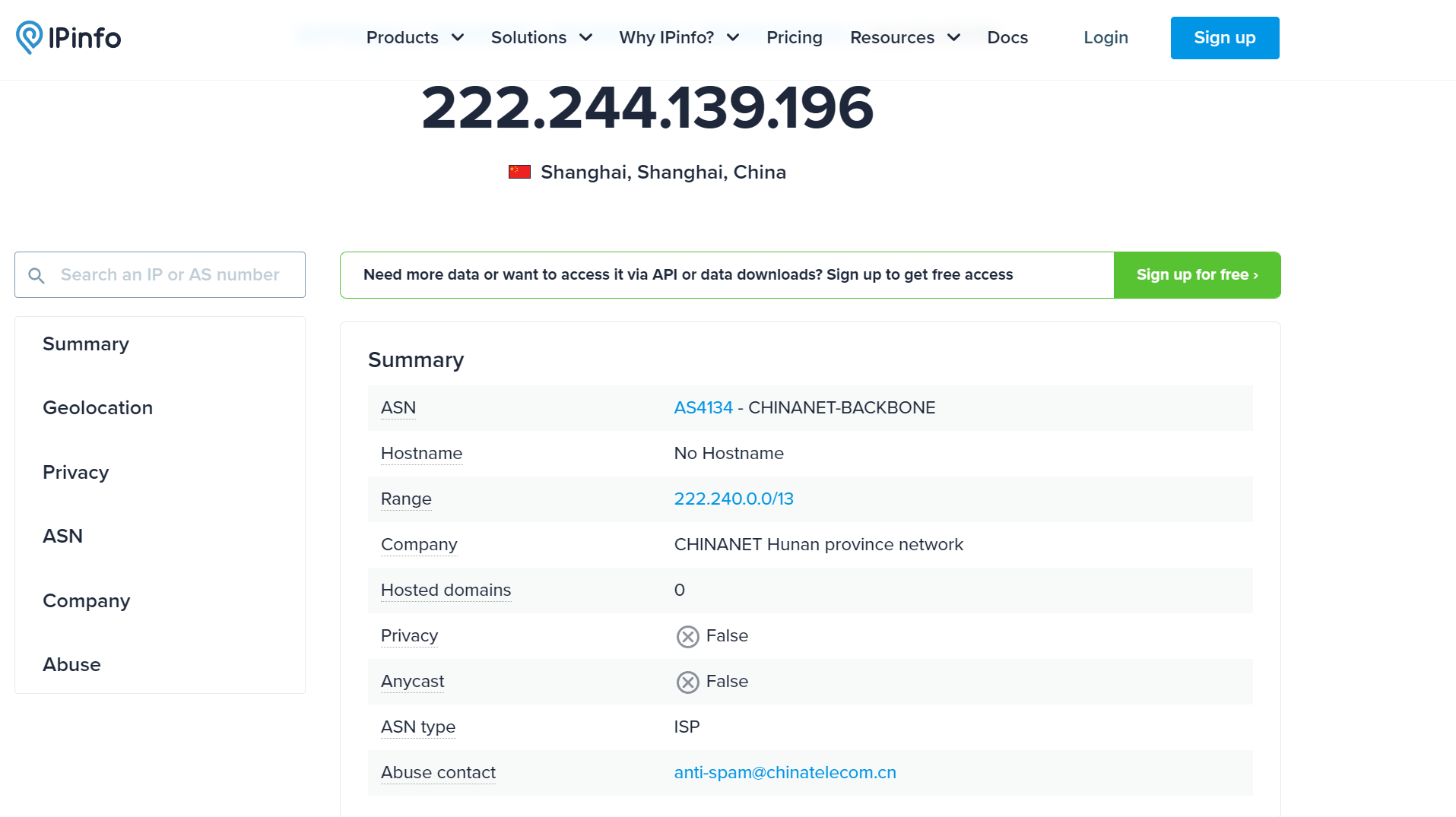
经该网站测试，下载带宽为31.81Mbps，上载带宽为5.75Mbps。

测试所属AS：

我们首先找到自己的公网ip，windows下可以使用指令“nslookup myip.opendns.com resolver1.opendns.com”来得到：



下面的address后面的数字就是我们的公网ip，将其复制之后到网站<https://ipinfo.io/>中进行查找：

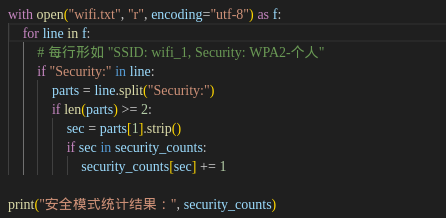


我们可以看到，ASN为AS4134-CHINANET-BACKBONE

Company是CHINANET Hunan province network。

最后一个部分：探究其网络模式，找出不同安全模式的比例。因为我们第一个任务中测试网络时，我们将测得的网络信息存在了“wifi.txt”文件中，所以我们可以直接从里面统计出不同安全模式的比例。

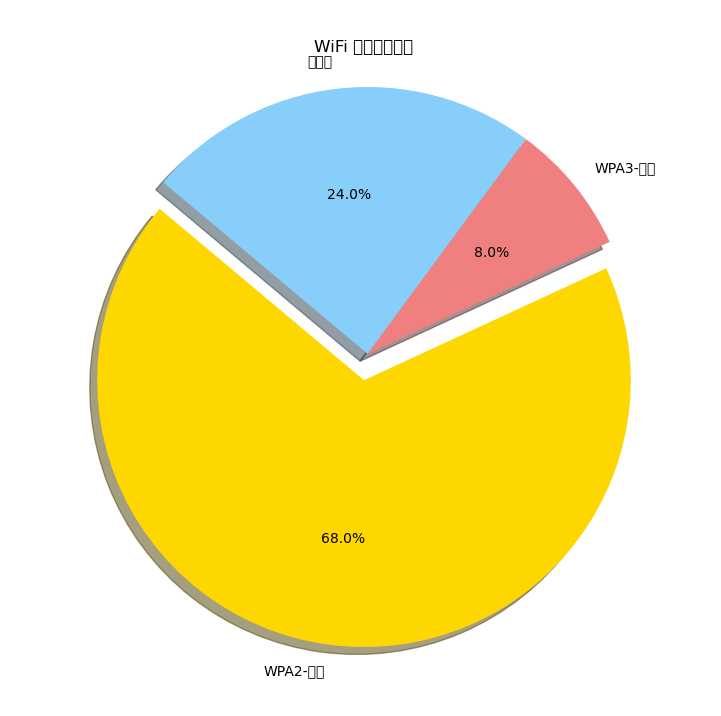
我们使用一个简单的python程序来进行统计：





刚开始生成的比例图中，没有办法显示中文，出现了错误“/usr/lib/python3.13/tkinter/\_\_init\_\_.py:865: UserWarning: Glyph 23433 (\N{CJK UNIFIED IDEOGRAPH-5B89}) missing from current font.

func(\*args)”表示Tkinter 正在尝试显示一个当前字体中没有的字符，即 Unicode 字符 “安”（CJK UNIFIED IDEOGRAPH-5B89）。这通常发生在使用默认字体时，该字体不支持某些中文字符。我找了很多攻略试了很多次都没有办法完全消除这个问题，故最终结果只能这样表示了：



蓝色的是开放式的网络，黄色是WPA2-个人，红色的是WPA3-个人。可以看到WPA2-个人最多，而WPA3-个人最少，开放式居中。

# 结论

我首先对所要解决的问题进行了分析，通过查阅资料和对题目中安全模式等方面的研究，提出了解决思路。具体而言，我在 Windows 环境下利用 Python 脚本调用 “netsh wlan show networks mode=bssid” 命令，收集了周边个WiFi 热点信息。随后，我查询了 WIGLE 数据库，并使用统计图呈现了本小区周边的 WiFi 热点分布情况。接着，通过 Python 脚本将这些 WiFi 热点的经纬度信息生成了一个 HTML 文件，能够直观展示各热点的地理位置。

在对这些 WiFi 热点进行分析后发现，除了主流的 WPA2 安全模式外，WPA3 和开放式网络也同时存在，并且它们的延迟和带宽特性各有不同。总体来看，所收集的中国电信 WiFi 热点主要采用 “WPA2-个人”、“WPA3-个人” 以及 “开放式” 三种安全模式。通过这些结果，我对热点分布和安全模式的规律进行了探讨。

# 参考文献

1 <https://blog.csdn.net/ccc61987/article/details/106068658>，Matlab2019 中文显示问题(乱码与方框). FJUR. 2020.5.26.

[2] https://www.cnblogs.com/surt/p/15601654.html. WLAN安全策略-WEP、WPA/WPA2、WPA3. 贪知猪. 2023.03.22.

[3] https://zhuanlan.zhihu.com/p/681806463. WiFi测试的核心思路和主要工具. Ankie Wan.2021.01.24.

[4] https://blog.csdn.net/HGJ515/article/details/115914249. 测试局域网或wifi实际最大带宽. 请叫我阿进.2023.8.15.

[5] https://blog.csdn.net/2409\_89014517/article/details/144028757. 使用WinMTR软件简单分析跟踪检测网络路由情况. 网硕互联的小客服.2022.3.24

[6] https://blog.csdn.net/python2021\_/article/details/123652555. Python绘制地图神器folium介绍及安装使用教程. python2021\_.2022.03.22.

[7] https://zhuanlan.zhihu.com/p/604459423. 彩云之南. 测试WiFi信号、选用WiFi信道的App：WiFi Analyzer. 2022.8.15.