中山大學 SUN YAT-SEN UNIVERSITY 移动网络安全技术实验报告

警示

1. 实验报告如有雷同，雷同各方当次实验成绩均以 0 分计。
2. 当次小组成员成绩只计学号、姓名登录在下表中的。
3. 在规定时间内未上交实验报告的，不得以其他方式补交，当次成绩按 0 分计。
4. 实验报告文件以 PDF 格式提交。

院系	数据科学与计算机学院	班 级	周三下午 56 节	组长	韩硕轩
学号	15352102	15352174		15352071	
学生	韩硕轩	李南茜		戴斯铭	
实验分工					
韩硕轩		李南茜		戴斯铭	
完成实验，撰写报告。		完成实验，撰写报告。		完成实验，撰写报告。	

Wifi 热点实验

【实验图标】

中山大學 SUN YAT-SEN UNIVERSITY 移动网络安全技术实验报告

【实验内容】

下面实验时，请写明便用的手机品牌、型号。

实验 1：简述什么是 WiFi 热点。

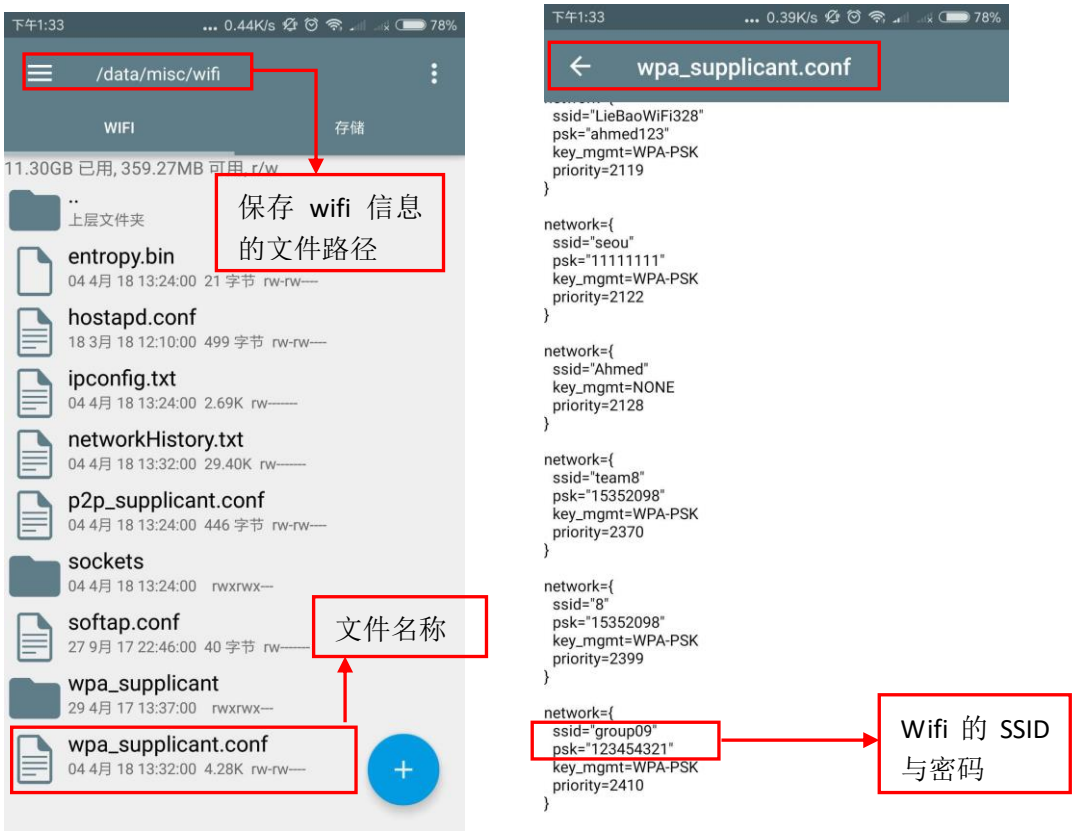
wifi 热点是指把手机的接收 GPRS、3G 或 4G 信号转化为 wifi 信号再发出去，这样手机就成了一个 wifi 热点。作为热点，手机必须具有无线 AP 功能。

实验 2：在手机上，会保留搜索到的 wifi 信息，当处在相应 wifi 环境下时能免密自动连接。请给出所保留 wifi 的 SSID、保存密码的文件夹及文件具体路径、内容（如果使用工具软件，简述此工具的功能），请通过一连接实例找出并给出截图（请描述实验时的环境，例如在什么地点、场合搜索到什么 wifi，而该 wifi 需要密码才能连接上网）。

使用“re 文件管理器”：其功能为，获取 Root 权限后对系统文件进行操作，可以新建文件夹，查看编辑文件，软件安装，支持查看和解压 RAR、zip 档案等。

使用红米 note3 连接在电脑上建立的”group09”wifi 热点。

WiFi 信息保存路径：data/misc/wifi/wpa_supplicant.conf：



实验 3：分别在下列设备上建立 wifi 热点（热点名：组号，指出采用什么身份认证，测试 PC 连接到手机热点、手机连接到 PC 热点的连通性。捕获热点的连接信息并加以分析。

（1）直接在手机建立。

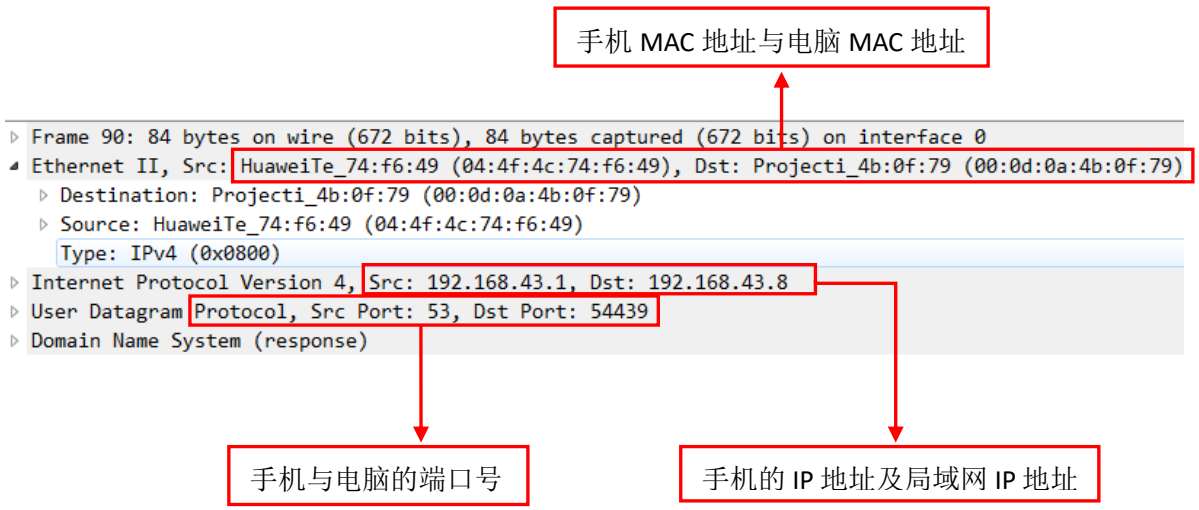
手机上建立 wifi 热点名称为：9

电脑连接手机建立的 wifi 热点：

身份认证方式：采用静态密码进行认证。即在网络登陆时输入正确的密码，就默认为合法用户。

热点信息捕获：wireshark 捕获

热点信息分析：



（2）在有无线网卡的 PC 上建立。

电脑建立 wifi 的命令：

```
C:\Users\Administrator>netsh wlan set hostednetwork mode=allow
承载网络模式已设置为允许。

C:\Users\Administrator>netsh wlan set hostednetwork ssid=group09
已成功更改承载网络的 SSID。

C:\Users\Administrator>netsh wlan set hostednetwork key=123454321
已成功更改托管网络的用户密钥密码。

C:\Users\Administrator>netsh wlan start hostednetwork
已启动承载网络。
```

对网络连接的设置：

手机连入”group09”wifi：

分析捕获的数据包，先在手机上查看手机的 ip 地址，然后在命令行里 ping 该地址：

```
正在 Ping 192.168.137.173 具有 32 字节的数据:
来自 192.168.137.173 的回复: 字节=32 时间=65ms TTL=64
来自 192.168.137.173 的回复: 字节=32 时间=599ms TTL=64
来自 192.168.137.173 的回复: 字节=32 时间=107ms TTL=64
来自 192.168.137.173 的回复: 字节=32 时间=433ms TTL=64
```

打开电脑上的 wireshark，选择对应网卡进行抓包，发现 tcp 的三次握手：

Source	Destination	Protocol	Length	Info
192.168.137.173	118.194.55.232	TCP	74	43776 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1360 SACK_PERM=1 TSval=3427354 TSecr=0 WS=64
118.194.55.232	192.168.137.173	TCP	58	443 → 43776 [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=0 MSS=1460
192.168.137.173	118.194.55.232	TCP	54	43776 → 443 [ACK] Seq=1 Ack=1 Win=65535 Len=0

（关键部分放大：

```
[SYN] Seq=0 Win=65535 Len=0
[SYN, ACK] Seq=0 Ack=1 Win=
[ACK] Seq=1 Ack=1 Win=6553
```

）

实验 4：在实验 3 基础上，查看建立的热点信息（例如，BSSID、无线电类型、频道、已连接用户的客户端数目和 mac 地址等）。如何判断 wifi 热点有没有被蹭网？请实验验证。

电脑建立的热点信息：

```
C:\Users\Administrator>netsh wlan show hostednetwork

承载网络设置
----------------------
    模式                   : 已启用
    SSID 名称              : “group09”
    最多客户端数  : 100
    身份验证           : WPA2 - 个人
    密码                   : CCMP

承载网络状态
----------------------
    状态                   : 已启动
    BSSID                  :00:0d:0a:4b:17:e1
    无线电类型             :802.11b
    频道                 : 1
    客户端数       : 1
        64:a6:51:a8:5c:ce          已经过身份验证
```

判断 wifi 热点被蹭网：

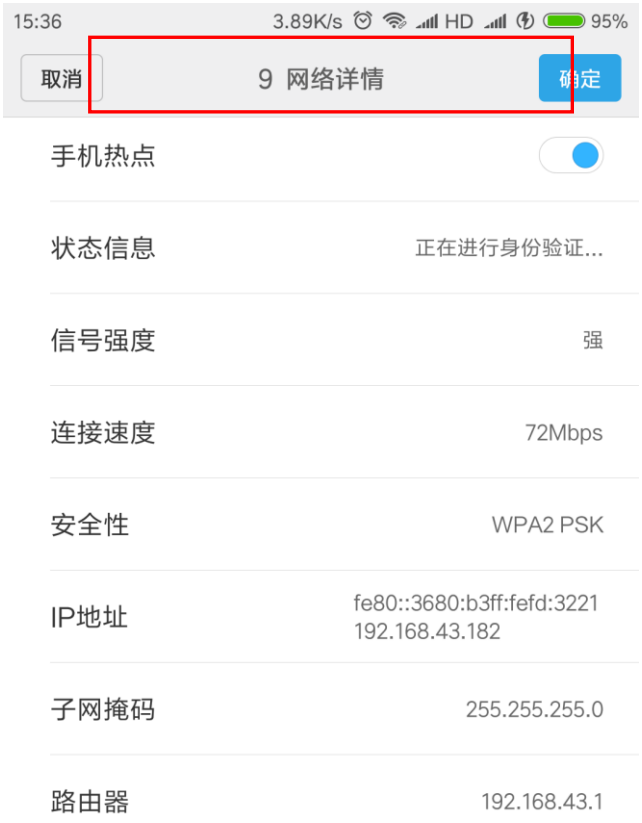
```
C:\Users\Administrator>netsh wlan show hostednetwork

承载网络设置
----------------------
    模式                   : 已启用
    SSID 名称              : “group09”
    最多客户端数  : 100
    身份验证           : WPA2 - 个人
    密码                   : CCMP

承载网络状态
----------------------
    状态                   : 已启动
    BSSID                  :00:0d:0a:4b:17:e1
    无线电类型             :802.11b
    频道                 : 1
    客户端数       : 2
        64:a6:51:a8:5c:ce          已经过身份验证
        34:80:b3:fd:32:21          已经过身份验证
```

蹭网用户的 MAC 地址

手机建立的热点信息：



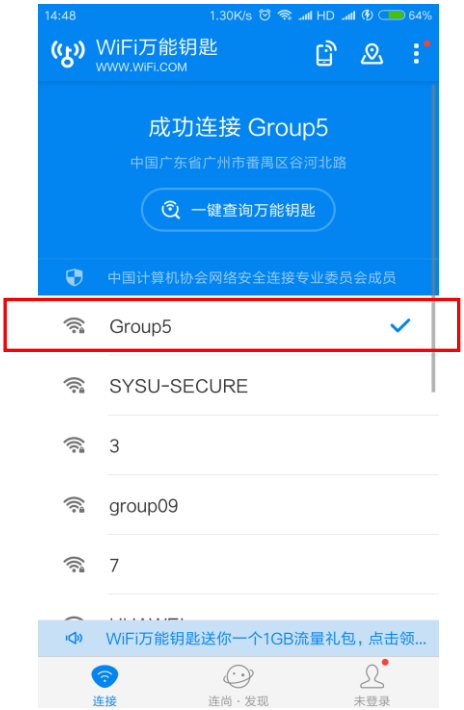
可以看到手机热点连接的设备有 2 台，被蹭网了：

中山大學 SUN YAT-SEN UNIVERSITY 移动网络安全技术实验报告

实验 5：如何对热点密码进行暴力破解攻击？写出思路、使用工具，并实例验证。（使用了什么破解工具、简述此工具的功能。蹭网是否成功？）

1) 使用 wifi 万能钥匙破解了”Group5”的 wifi 密码：

wifi 万能钥匙通过用户上传分享的热点（主动或“被动”）到后台服务器的方式收集、积累数据。后台服务器维护者一份热点数据库，其中包含着热点名称（或者用来唯一标识的 MAC 地址）以及与其对应的密码字符串。查询密码时，用户将周围扫描到的陌生热点信息上传，服务器后台查询到相对应的密码（如果分享过的话）后返回给 APP 供用户选择使用。



2) 使用幻影 wifi 进行暴力破解：

幻影 wifi 采取依次尝试所有弱密码等可能出现的组合直到成功连接的手段进行破解。原理为字典破解，用字典（密码结合）里面有的密码去注意尝试连接，即“密码库穷举暴力破解法”。

中山大學 SUN YAT-SEN UNIVERSITY 移动网络安全技术实验报告

实验 6：如何发现和判断流氓热点？写出思路、使用工具，并实例验证。

方法 1：BSSID 白名单

跟其他网络设备一样，每一个 WiFi 接入点都有自己的 MAC 地址，而 MAC 地址也是它会发送的数据的其中一部分。一种检测流氓热点的方法就是设置一个可信接入点白名单，然后用 MAC 地址做标识来进行热点匹配。但是问题就在于，攻击者仍然可以轻而易举地伪造 MAC 地址。

方法 2：非同步的 MAC 时间戳

生成相同网络的接入点都会拥有高度同步的内部时钟。因此，接入点会不断地交换时间戳以实现同步，这个时间是毫秒级的，同步增量为 25 微秒。大多数流氓热点在尝试进行时间戳同步时往往会出现各种各样的错误，你可以通过检测这种错误来发现流氓热点。

方法 3：错误的信道

你可以设置一个列表来存储所有受信任接入点的信道，如果信道不同，则说明该接入点有问题。但是对于攻击者来说，这种保护方式也是能够轻松绕过的。

方法 4：信号强度异常

我们还可以通过分析 WiFi 信号的强度来检测流氓热点。如果攻击者伪造了一个接入点的话，你会发现其 MAC 地址（BBSID）和信号强度会突然发生改变。

实验总结：根据以上实验，请对 wifi 热点的安全性做一个综述（如有引用文献资料，请标出）。

在上面使用破解软件进行“蹭网”的实验中会发现，wifi 热点是相对不安全的。

1. Wifi 热点有被进行暴力破解的风险，而对此的唯一防范方法时使用健壮的 wifi 密码，并且不要使用 WEP。
2. Wifi 热点也有可能被金属物体、障碍物阻碍，或是被人为因素、wifi 信号之间相互干扰。
3. 手机在自动连接到的 wifi 网络还有可能是流氓热点，会使不法分子有机可乘，黑客在公共场合伪造 wifi，盗取用户个人信息。由运营商提供的免费 WiFi 和其他商家提供的免费 WiFi 在使用过程和技术保障上都存在很大的区别，电信提供的免费 WiFi 均需要账号密码做身份认证，使用时会有专门的认证页面或者专用的客户端软件。而部分商家和黑客提供的免费 WiFi 基本都没有认证的措施，用户无需确认身份即可使用。

引用：

http://www.library.sh.cn/tsgc/tsfw/dzpx/2011/120610.pdf

【交实验报告】

上传实验报告：ftp://222.200.180.109/　　截止日期（不迟于）：三周之内完成

上传小组实验报告。上传文件名格式：小组号_ 实验名.pdf （由组长负责上传）

例如：文件名“6_ 网络攻击分析实验.pdf”表示第 6 组的网络攻击分析实验报告

注意：不要打包上传！