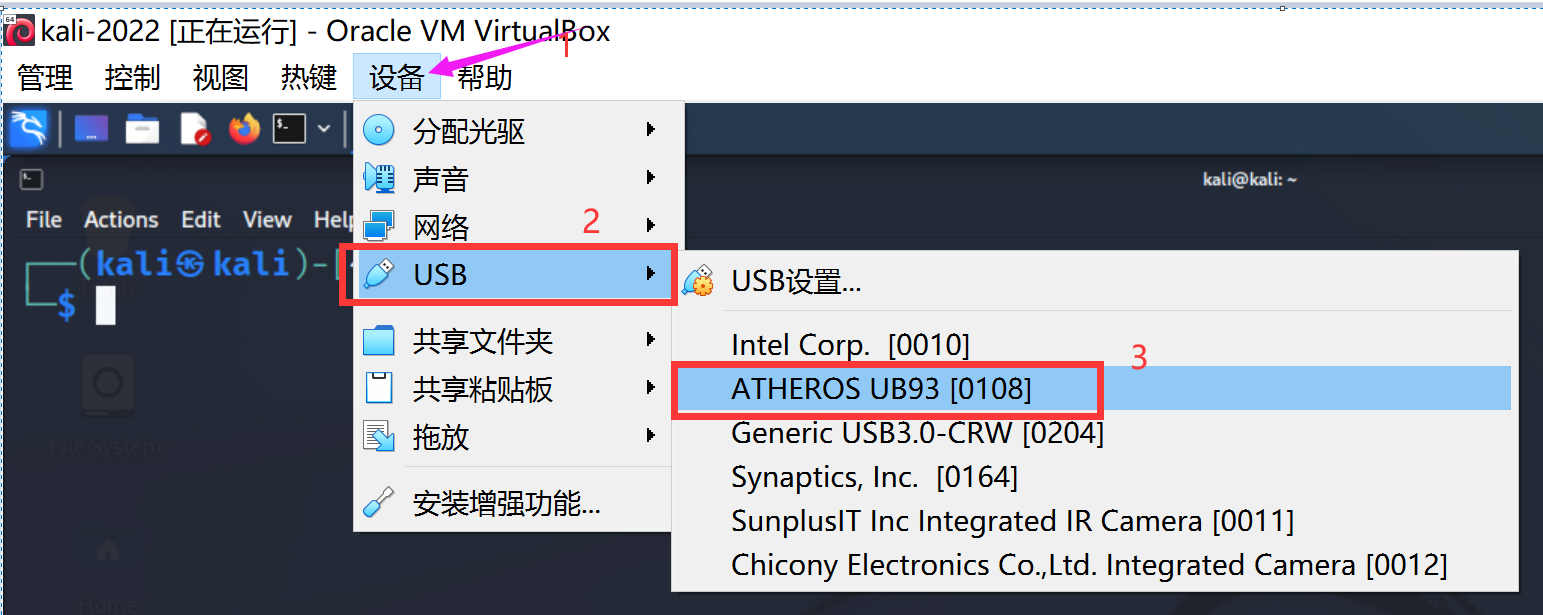
# WLAN流量获取

## 无线网卡配置

先启动操作系统，宿主机插入无线网卡，然后执行如下操作。可以在USB设备中看到无线网卡，选中，稍后网卡指示灯开始闪烁。



列举无线网卡，命令：

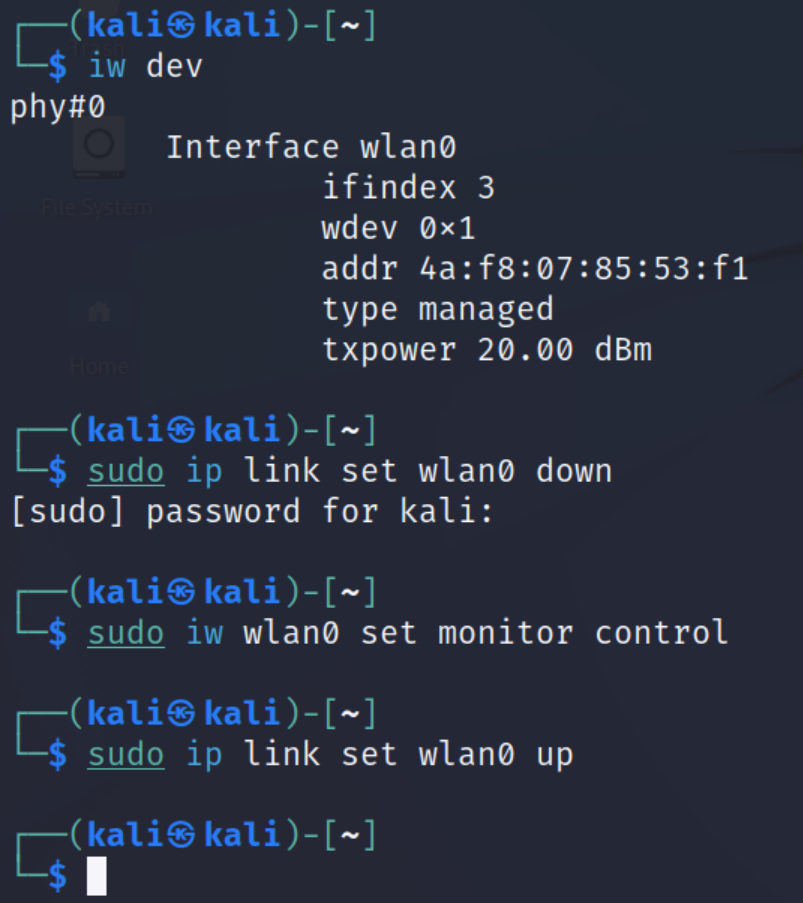
iw dev

设置为monitor模式：

sudo ip link set INTERFACE down

sudo iw INTERFACE set monitor control

sudo ip link set INTERFACE up



运行airodump-ng来抓无线帧：

sudo airodump-ng INTERFACE

抓包命令：

sudo airodump-ng INTERFACE --channel CHANNEL --write FILENAME

抓取特定channel的数据：

sudo ip link set INTERFACE down

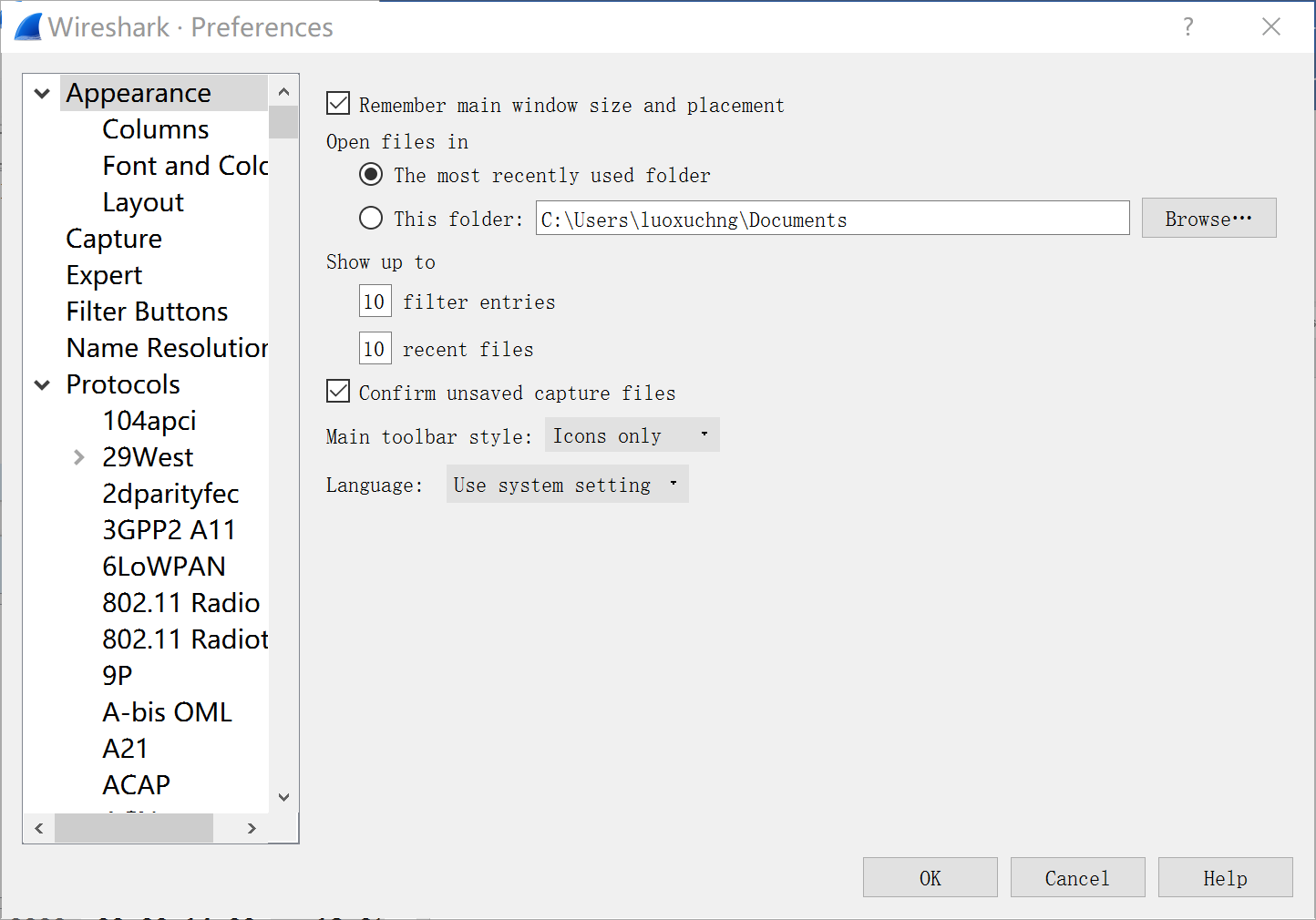
sudo iw INTERFACE set monitor control

sudo ip link set INTERFACE up

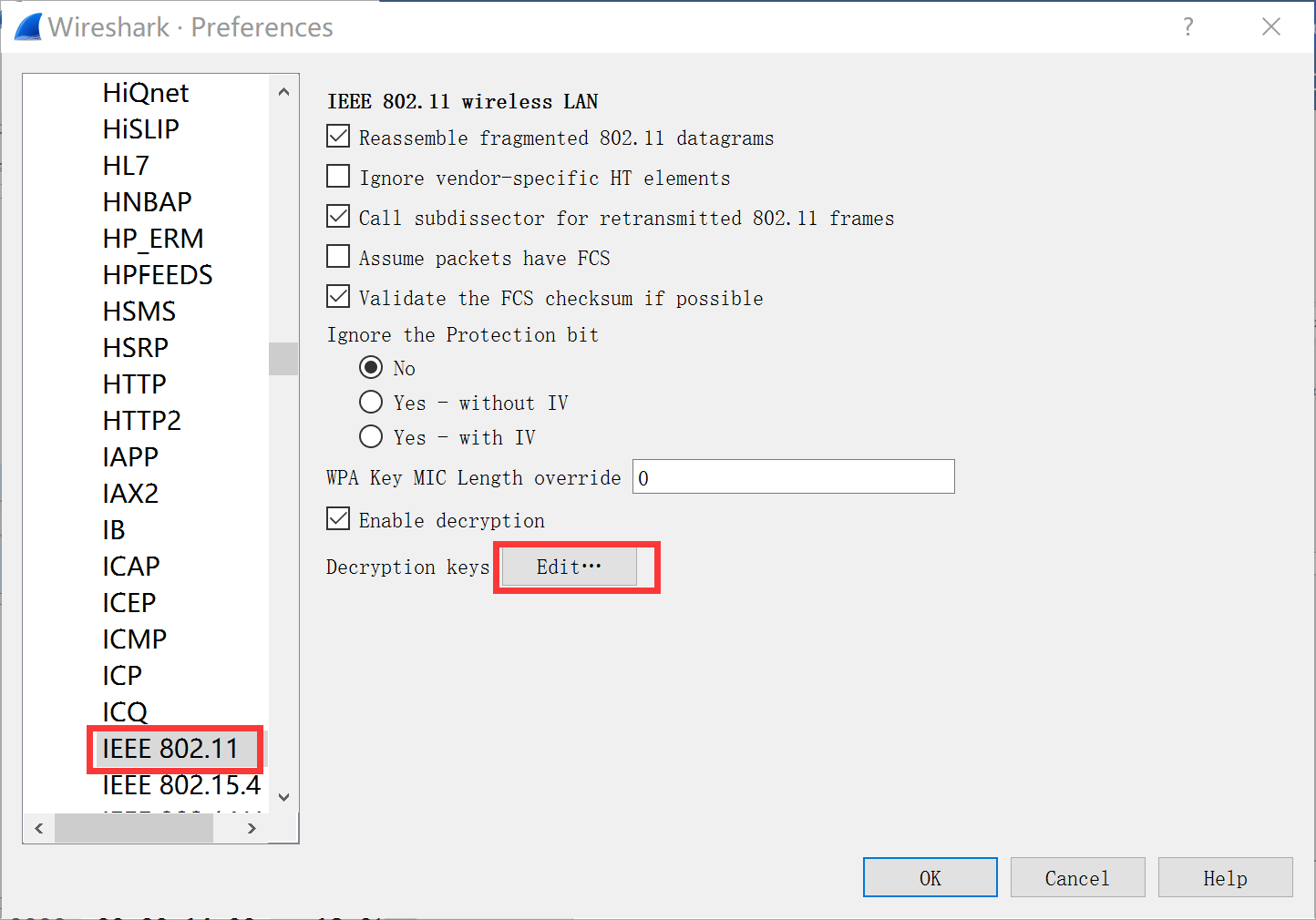
sudo iw dev INTERFACE set channel CHANNEL

# wireshark解密流量配置

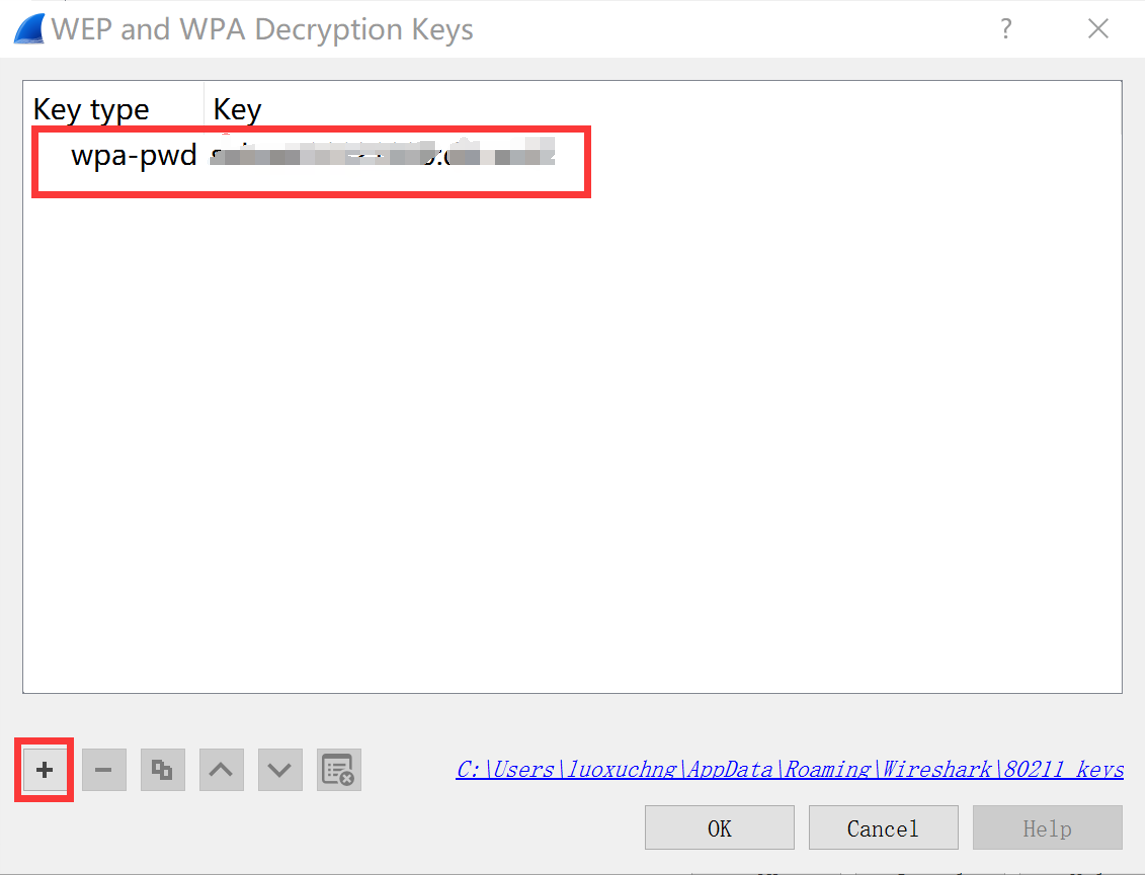
通过Edit菜单，打开Preferences，如下：



点开Protocols，然后选择IEEE 802.11(注意不是选择802.11radio等开头的那些协议)。



打开Edit对话框：

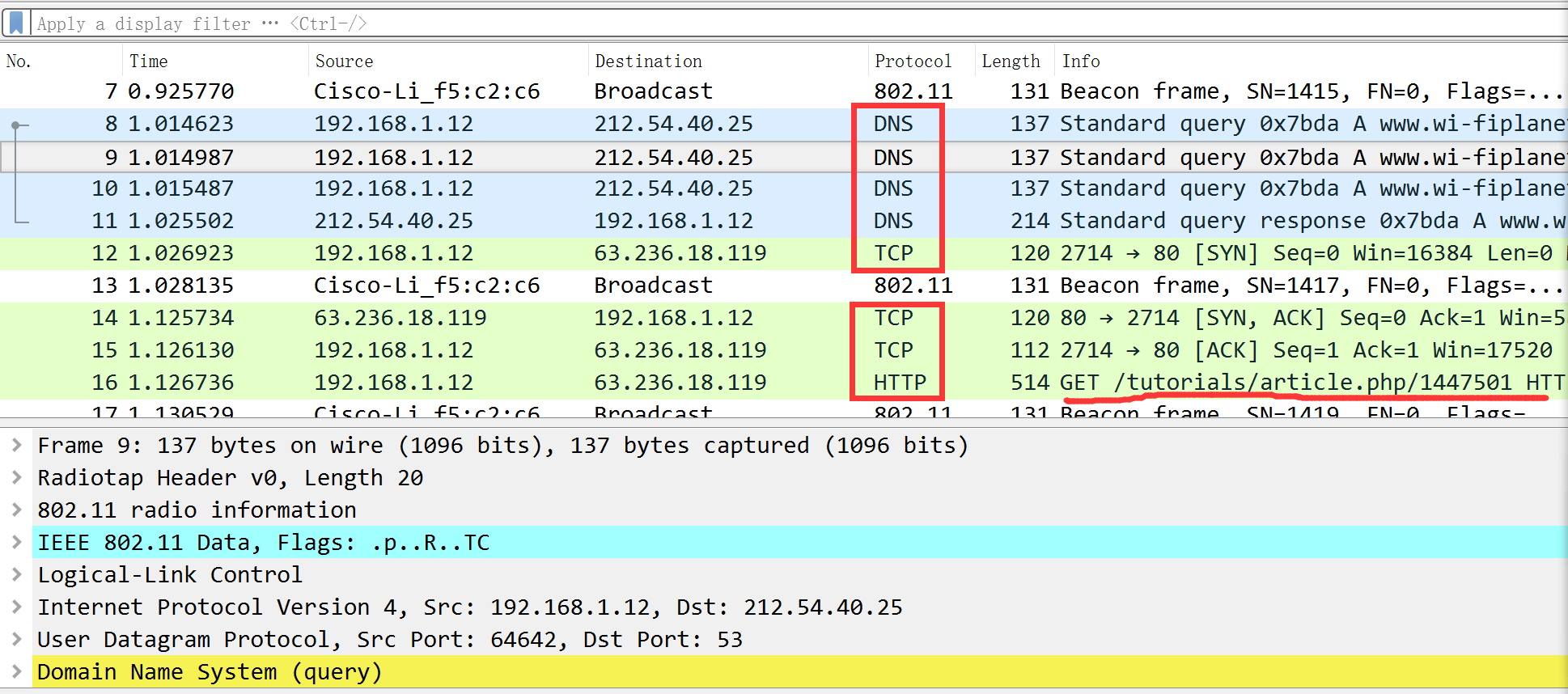


点击+按钮，可以添加表项。针对目前这个wifi流量，我们添加一个表项，选择key type为wpa-pwd，然后配置key为

MyPassword:MySSID

前面部分是口令，中间是冒号，之后是SSID。

OK之后，回到主界面：



从这里可以看到，上层协议可以解析了，比如DNS协议里面的域名，http协议里面GET命令的内容等，表明已经解密数据帧。

通过这种方式，我们可以进一步验证所破解的口令是否正确。