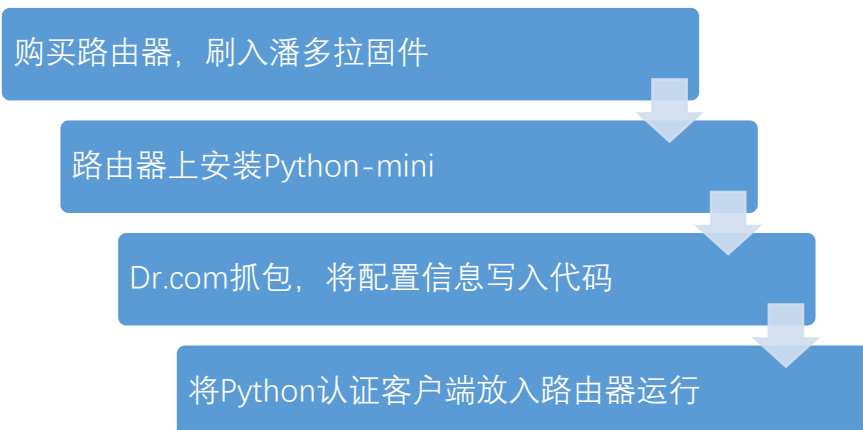


目前支持 K1/K2/小米 mini 和 NEWIFI-mini

🔧 基本原理:

首先需要刷入开源固件潘多拉，然后安装路由器专用 python-mini，在 Windows 上抓包 Dr.com，将你的账户和配置信息写入 Python 程序，将程序复制到路由器，模拟 Dr.com 的运行



引用资源: <https://github.com/drcoms/drcom-generic>

特别指出禁止任何个人或者公司将 **drcoms** 的代码投入商业使用，由此造成的后果和法律责任均与本人无关。

🔧 本文档以及相关文件下载链接:

链接: <http://pan.baidu.com/s/1eRGrbYM> 密码: rca6

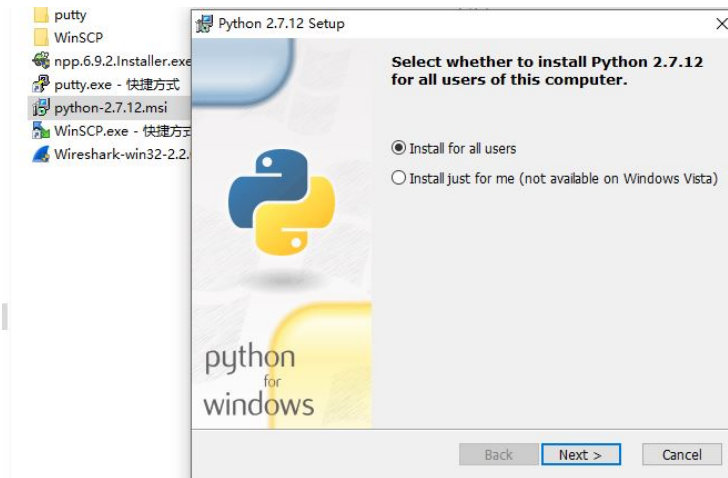
DocuSigned by:
luochenzhimu
FAEB62719A45435...

2016/10/20

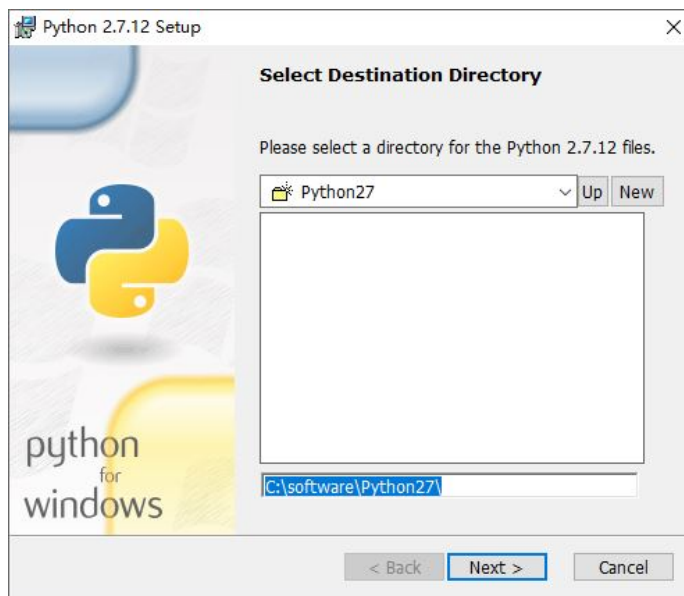
准备工作:

安装 Python2.7:

双击 python-2.7.12.msi



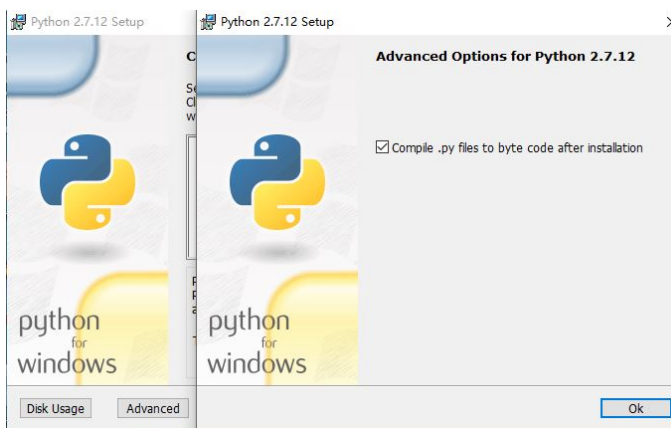
选择安装路径



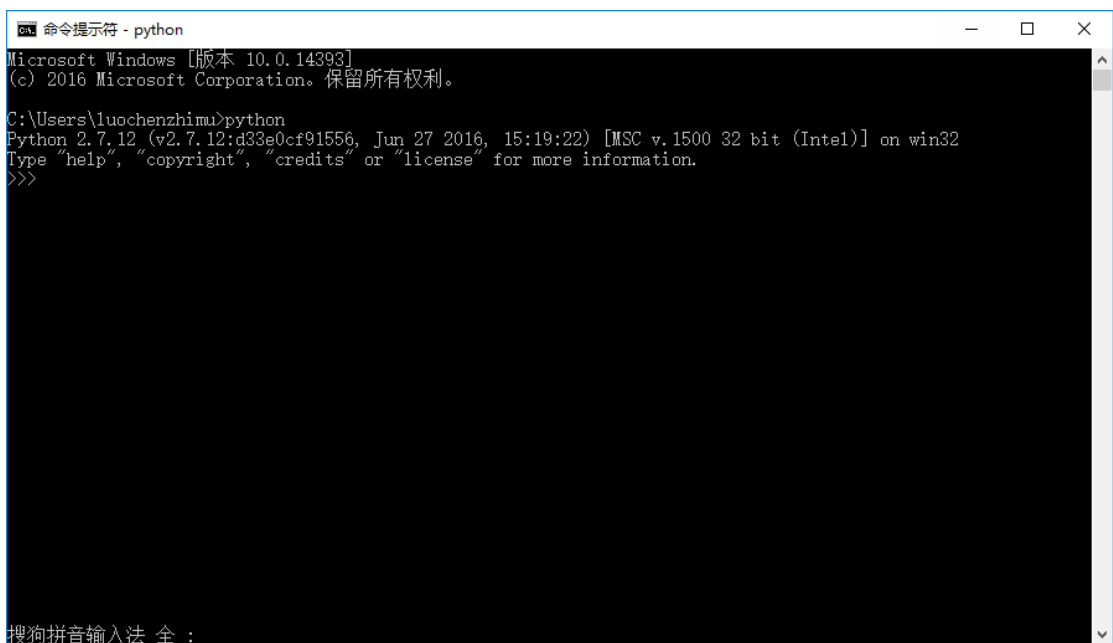
选择 Add python.exe to Path



在 Advanced 里勾选关联.py 文件



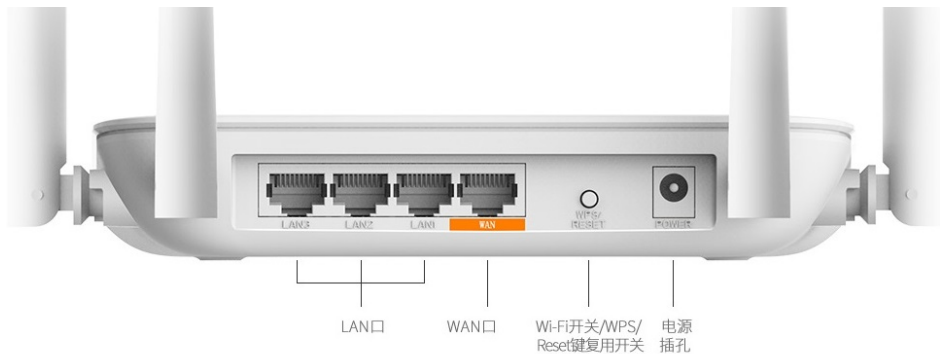
安装完成后 Win+X+C 打开命令提示符，输入 python 测试下能不能运行



接着安装 Wireshark 和 Notepad++，这个没有特殊要求，一直点下一步就可以安装完成，就不演示了，Putty 和 WinSCP 不需要安装，直接双击看快捷方式就可以使用

刷入固件

用网线连接路由器的 LAN 口和电脑网线接口



以管理员身份运行路由器刷 breed Web 助手通用版 v2.8.exe，如果你购买的是 K1/K2，则选择斐讯 k1,k1s,k2 全自动方案，如果是小米路由器 mini，则选择小米路由器方案(需要开启路由器 ssh 服务)，点击开始刷机，程序会自动运行，特别提醒，Breed 不支持小米路由器 3，不能用这个软件来刷，可能会变砖。



刷机完成后，等待一段时间，拔掉路由器电源，按住复位按钮，插上电源，等待约 10 秒，在浏览器中输入 192.168.1.1，打开 Breed 控制台

192.168.1.1/index.html

Breed Web 恢复控制台

系统信息

固件更新

固件备份

频率设置

恢复出厂设置

固件启动设置

MAC 地址修改

重启

关于

CPU	MediaTek MT7620A ver 2, eco 6
内存	64MB DDR2
Flash	GigaDevice GD25Q64 @ 24MHz (8MB)
以太网	MediaTek MT7620A built-in 5-port 10/100M switch
时钟频率	CPU: 580MHz, Bus: 193MHz
编译日期	2016-04-19 [git-3b445d3]
版本	1.0 (r849)

选择合适的固件，我给了四个固件：
推荐使用 K2-PandoraBox-160922-adbyby.bin，预装有广告屏蔽插件 Adbyby
K2-PandoraBox-160922-no-usb.bin 没有预装 Adbyby
PandoraBox-ralink-mt7620-xiaomi-mini-squashfs-sysupgrade-r1055-20150615_5.5M.bin
RT-AC54U-GPIO-1-PSG1208-64M_3.4.3.9-099.trx 华硕固件，非校园网用
若需要其他品牌路由器的潘多拉固件，可以访问 <http://downloads.openwrt.org.cn/PandoraBox>
在固件更新里选择合适的固件

Breed Web 恢复控制台

系统信息

固件更新

固件备份

频率设置

恢复出厂设置

固件启动设置

MAC 地址修改

重启

关于

常规固件

编程器固件

<input type="checkbox"/> Bootloader		浏览...
<input checked="" type="checkbox"/> 固件	D:\最终版本\1-刷潘多拉固件\PandoraBox-ralink-mt7620-xiaomi-mini	浏览...
<input type="checkbox"/> EEPROM		浏览...
闪存布局	公版 (0x50000) ▾	

☒ 自动重启

上传

点更新

Breed Web 恢复控制台

更新确认

文件已上传，请确认下方列出的信息

类型	固件
文件名	PandoraBox-ralink-mt7620-xiaomi-mini-squashfs-sysupgrade-r1055-20150615_5.5M.bin
大小	5.5MB (5767172B)
MD5 校验	ff0eba71c27c59cad1a7cda20adeefa8

更新

等待刷机完成

Breed Web 恢复控制台

操作正在进行

您选择的操作正在进行
正在更新固件，请耐心等待至进度条完成

12%

警告：在操作进行过程中请不要断开电源

稍等后浏览器打开 192.168.1.1，用户名为 root，密码 admin

192.168.1.1

PandoraBox_2077

需要授权

请输入用户名和密码。

用户名

root

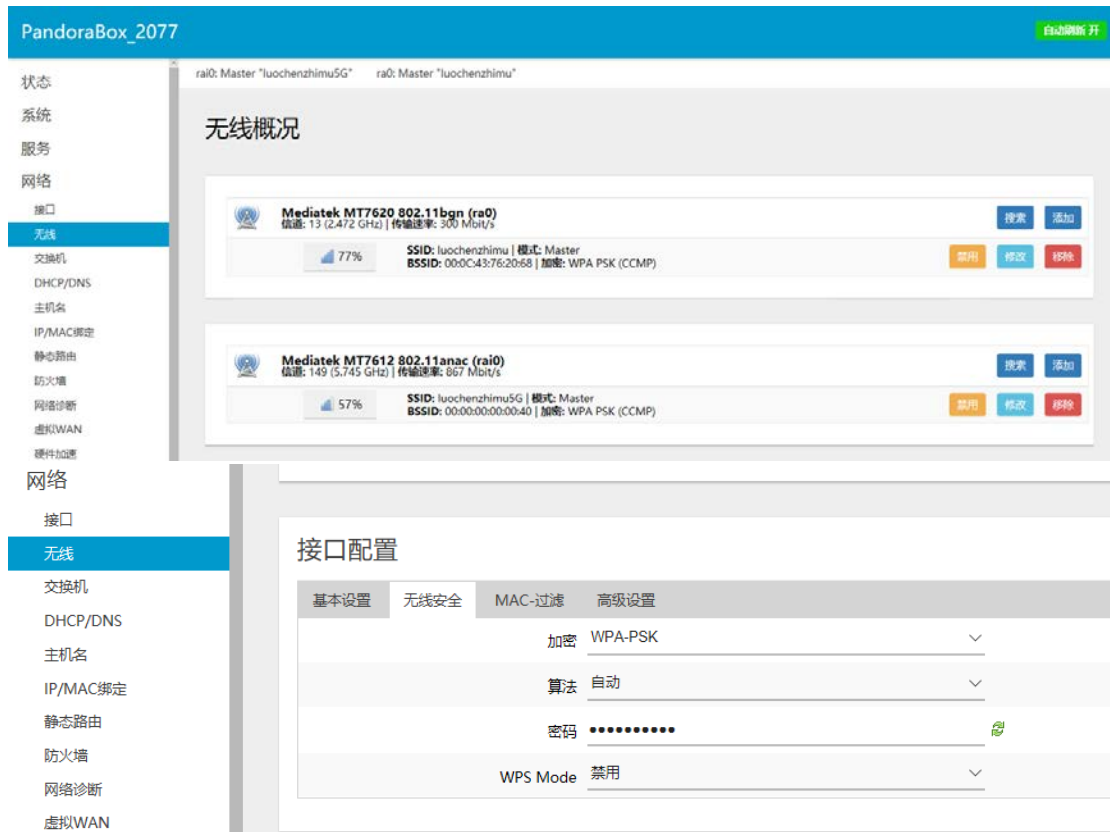
密码

登录

验证

Powered by LuCI Master (git-16.255.20859-251f41b) / PandoraBox 16.09 2016-09-22-git-3f0accd

点击网络→无线，修改你的 SSID 和无线密码，然后保存设置



配置 Dr.COM 脚本

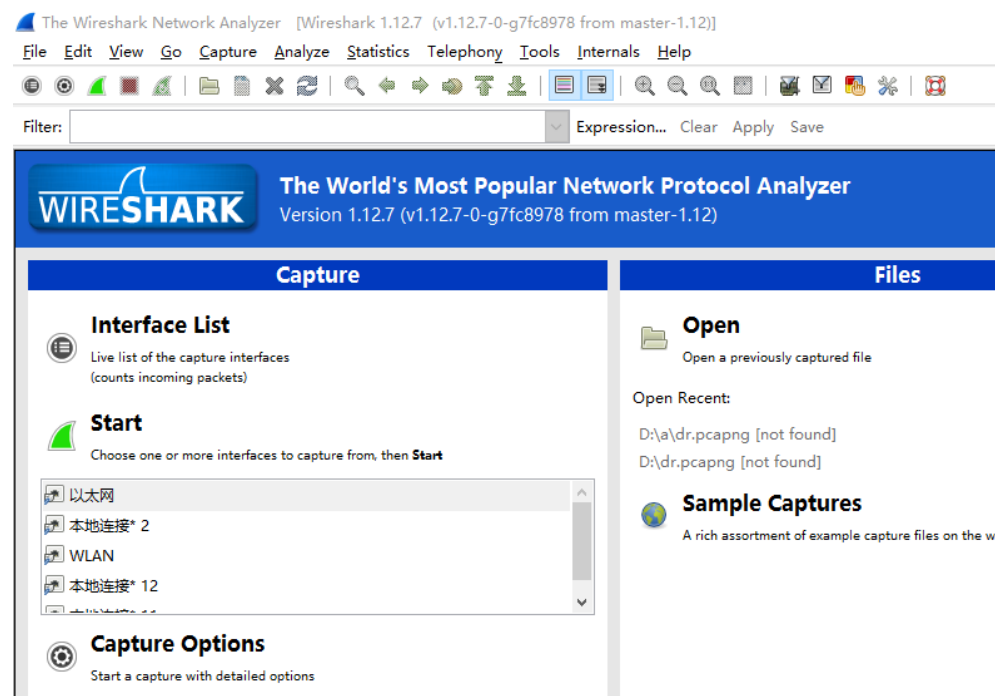
访问 <https://github.com/drcoms/drcom-generic> 下载适合你的 drcom 版本

接着抓包，需要提示的是，抓包的信息可以复用，只需要改下账号和密码，所以如果你已经有了配置文件，就不需要安装桌面版的 Python2.7 和 Wireshark，只需要修改你的登录脚本账号和密码即可。

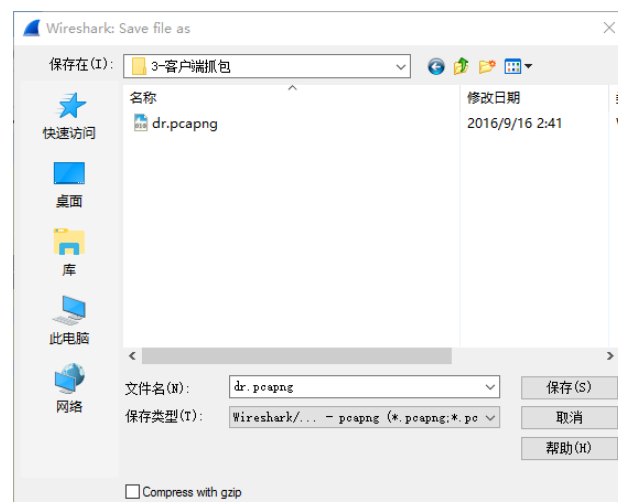
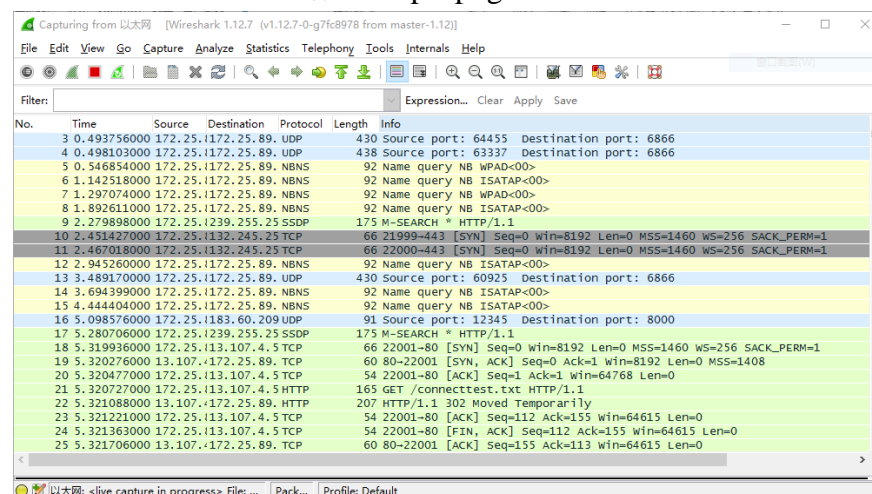
首先打开客户端，输入账户和密码，先不要登录



打开 Wireshark，点击以太网，再点击 Start



登录客户端，短暂时间后点击左上角红色按钮
点击 File→Save As 保存为 dr.pcapng



当前目录需要的三个文件，双击 Double_Click_to_Run.cmd，在当前目录会生成 config.txt 文件

名称	修改日期	类型	大小
Double_Click_to_Run.cmd	2016/9/17 17:16	Windows 命令脚本	1 KB
dr.pcapng	2016/9/16 2:41	Wireshark captu...	153 KB
drcom_d_config.py	2016/9/16 4:42	Python File	2 KB

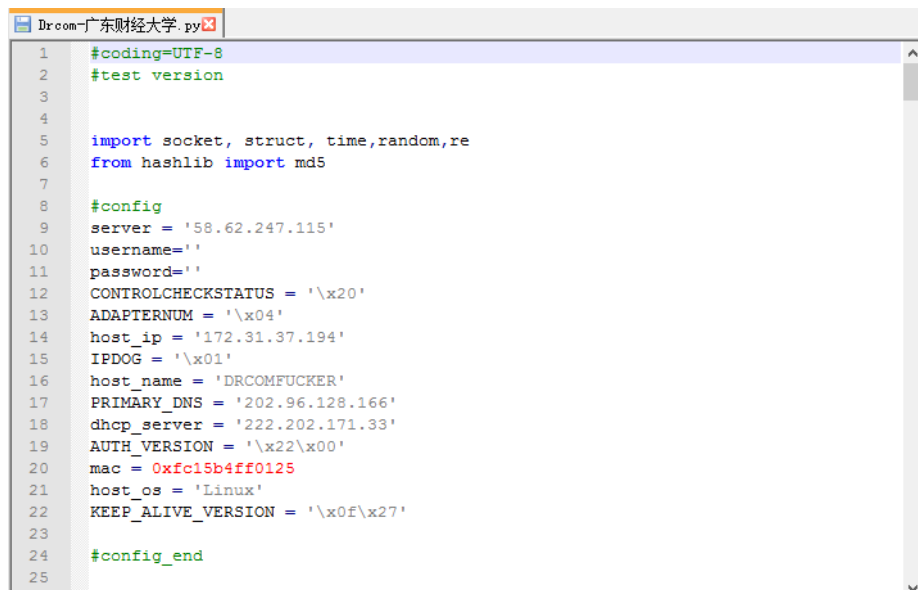
名称	修改日期	类型	大小
config.txt	2016/9/17 17:19	文本文档	1 KB
Double_Click_to_Run.cmd	2016/9/17 17:16	Windows 命令脚本	1 KB
dr.pcapng	2016/9/16 2:41	Wireshark captu...	153 KB
drcom_d_config.py	2016/9/16 4:42	Python File	2 KB

生成的 config.txt 内容如下，每台电脑抓包生成的文件都不一样：

```
pcapng file: dr.pcapng
copy following statements to drcom.conf or overwrite field between "# CONFIG" and "#
CONFIG_END" in latest-wired.py

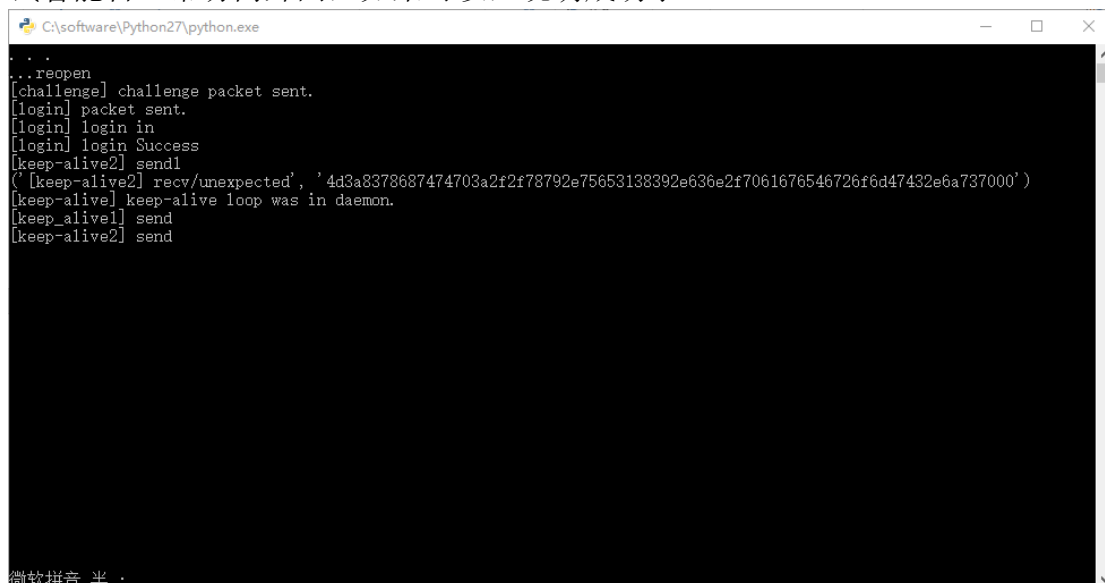
server = '*****'
username='*****'
password='*****'
CONTROLCHECKSTATUS = '\x20'
ADAPTERNUM = '\x01'
host_ip = '172.**.**.*'
IPDOG = '\x01'
host_name = 'DRCOMFUCKER'
PRIMARY_DNS = '*****'
dhcp_server = '*****'
AUTH_VERSION = '\x2b\x00'
mac = 0x*****
host_os = 'WINDIAOS'
KEEP_ALIVE_VERSION = '\xdc\x02'
```

使用 Notepad++打开 Drcom.py, 修改#config 和%config_end 之间的配置信息为你刚刚生成的, 同时在 password=”的引号里面输入你的密码



```
1 #coding=UTF-8
2 #test version
3
4
5 import socket, struct, time, random, re
6 from hashlib import md5
7
8 #config
9 server = '58.62.247.115'
10 username = ''
11 password = ''
12 CONTROLCHECKSTATUS = '\x20'
13 ADAPTERNUM = '\x04'
14 host_ip = '172.31.37.194'
15 IPDOG = '\x01'
16 host_name = 'DRCOMFUCKER'
17 PRIMARY_DNS = '202.96.128.166'
18 dhcp_server = '222.202.171.33'
19 AUTH_VERSION = '\x22\x00'
20 mac = 0xfc15b4ff0125
21 host_os = 'Linux'
22 KEEP_ALIVE_VERSION = '\x0f\x27'
23
24 #config_end
25
```

然后注销 Dr.com 客户端, 双击 Drcom.py 运行, 出现如下信息说明登录成功, 测试看能否正常访问外网, 如果可以, 说明成功了



```
C:\software\Python27\python.exe
...reopen
[challenge] challenge packet sent.
[login] packet sent.
[login] login in
[login] login Success
[keep-alive2] send1
(' [keep-alive2] rcv/unexpected', '4d3a8378687474703a2f2f78792e75653138392e636e2f7061676546726f6d47432e6a737000')
[keep-alive] keep-alive loop was in daemon.
[keep-alive1] send
[keep-alive2] send
```

微软拼音 半：

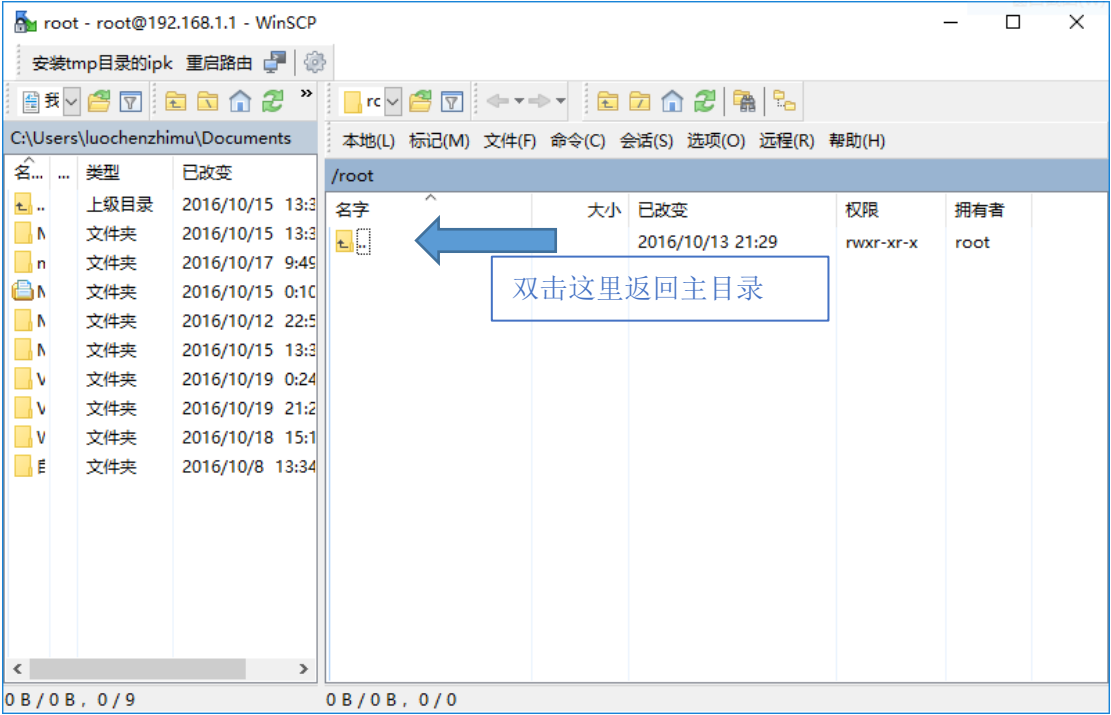
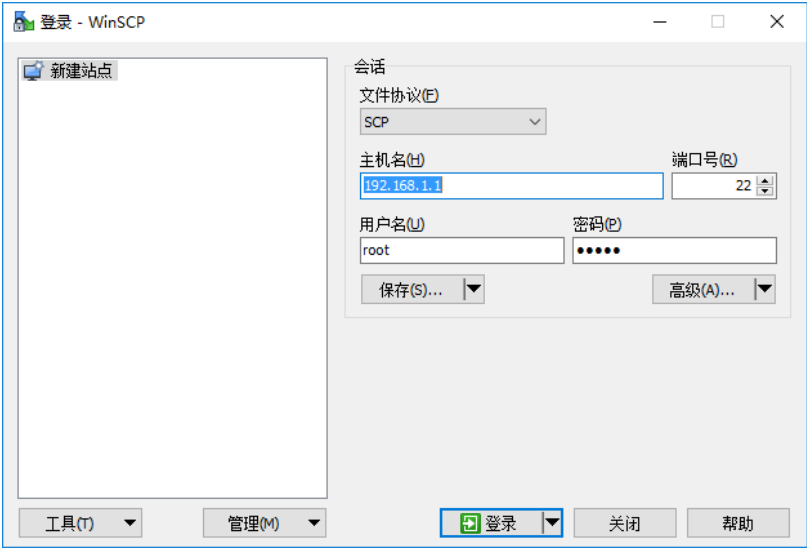
然后将 Drcom.py 修改为没有后缀名的 drcom

将 drcom 放在 \最终文件夹\usr\bin

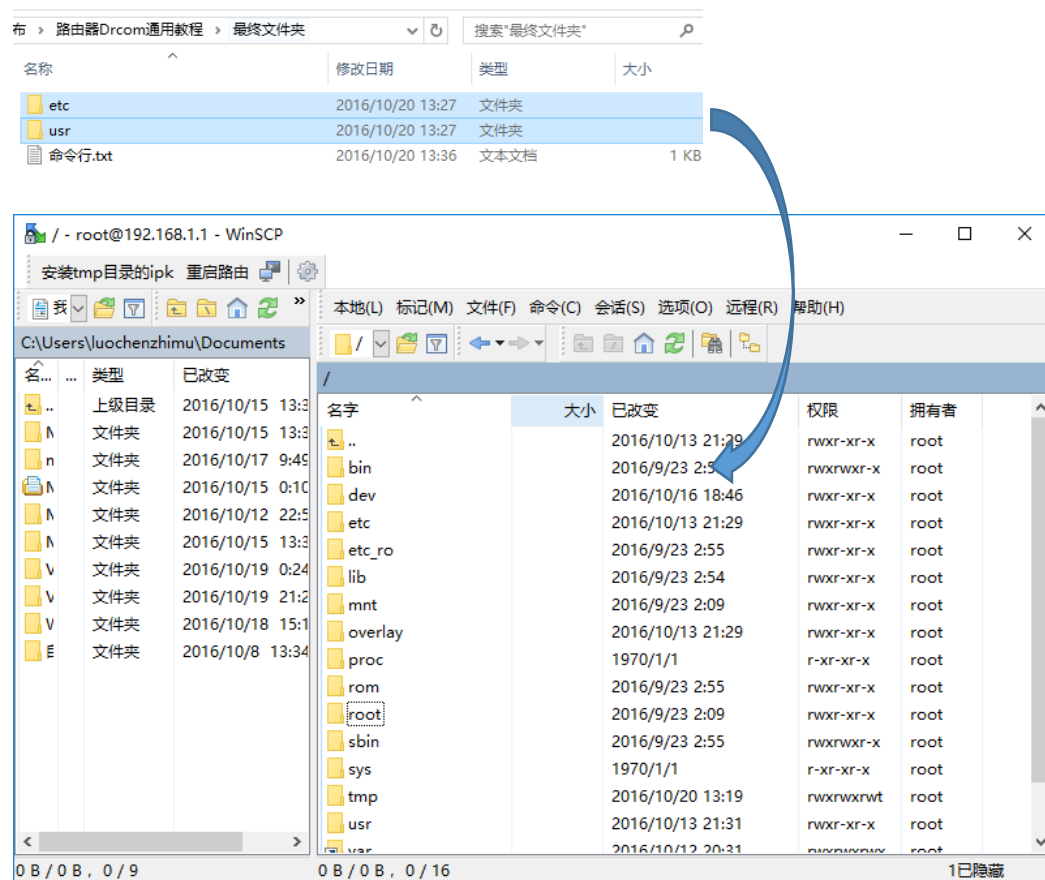


第二版通用教程 > 最终文件夹 > usr > bin				搜索"bin"
名称	修改日期	类型	大小	
drcom	2016/9/27 13:15	文件	101	

配置文件完成后打开 WinSCP 登录

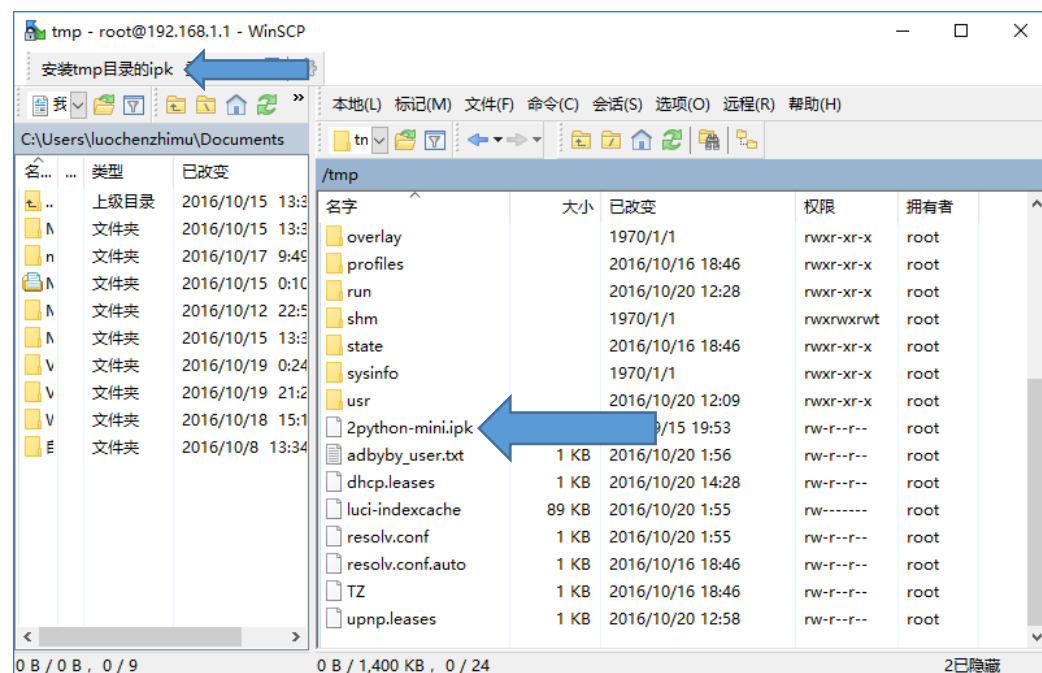


把最终文件夹里的 `etc` 和 `usr` 拖放到路由器主目录并替换，注意刚才配置好的 `drcom` 放在 `\usr\bin` 目录下

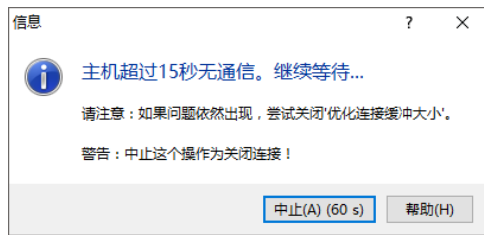


然后打开 `\tmp` 目录

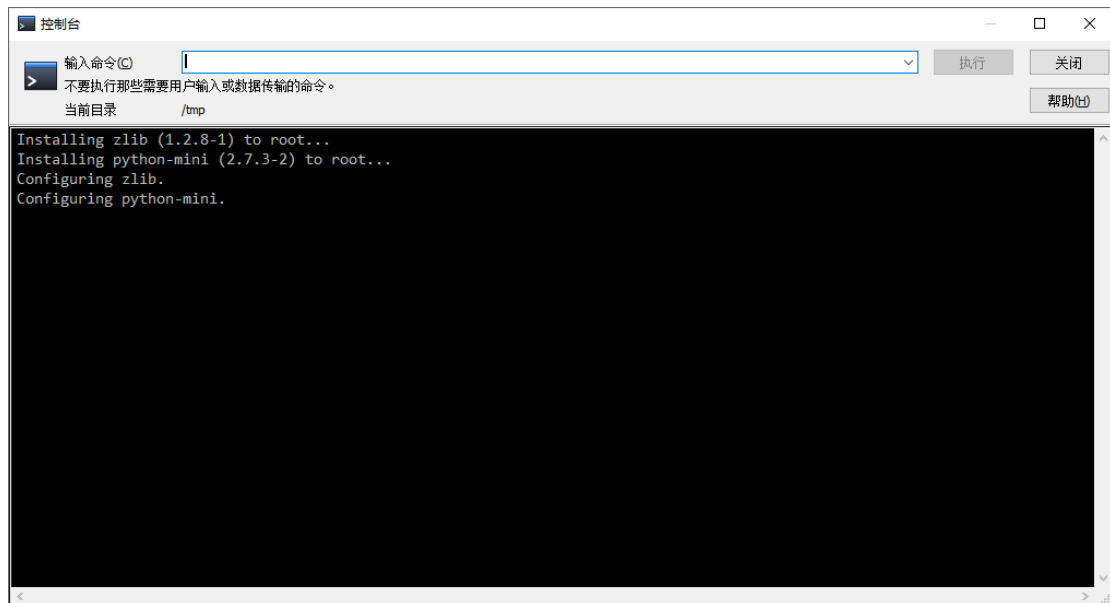
把 2-路由器 python 安装包目录下的 `2python-mini.ipk` 拖进去，然后点击左上角的安装 `\tmp` 目录的 `ipk`，等待接近 20s 时间，中间会提示无响应，不用理会



不用管这个

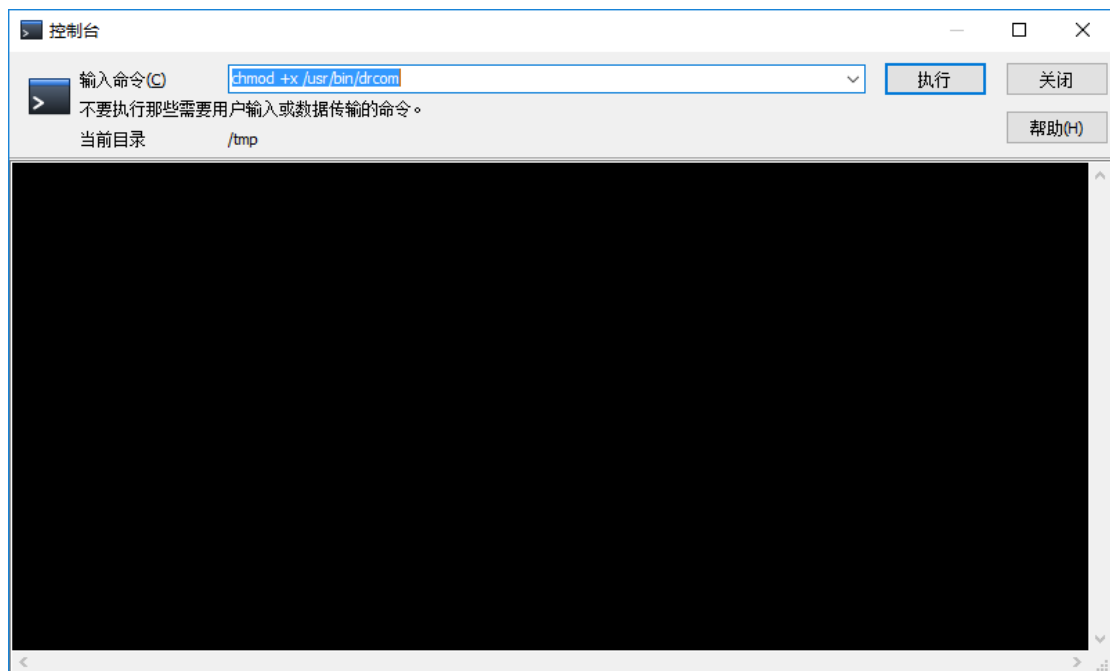


安装成功提示 Configuring python-mini.



最后在终端中输入以下命令并执行

chmod +x /usr/bin/drcom



重启路由器，享受无线网络吧