在windows系统下使用nrf connect给nrf52840 dongle写入固件nRF52\_driver\_firmware.hex。

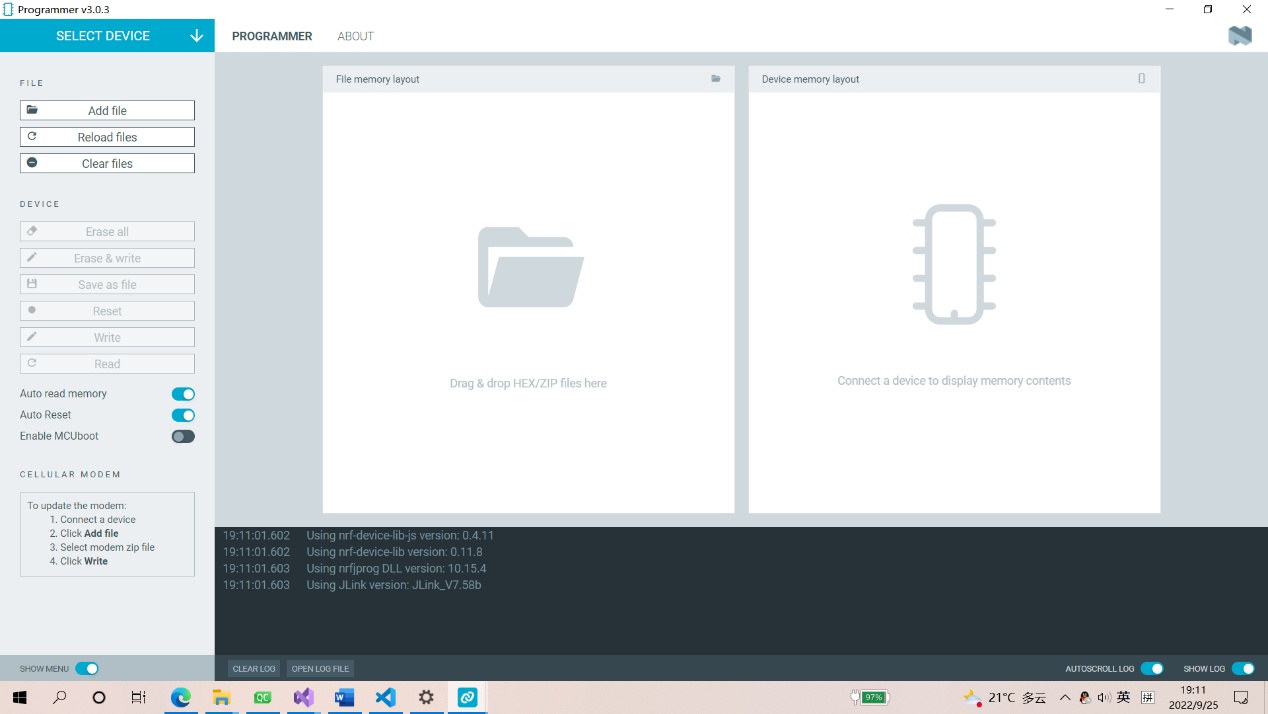


图1 刷固件

低功耗蓝牙的程序运行在kali环境下，使用python2.7，在使用前安装依赖，依赖部分在requirements.txt中，使用命令“sudo pip install -r requirements.txt”进行安装。requirements.txt中的依赖有pyserial, nrfutil, pycryptodome, six。

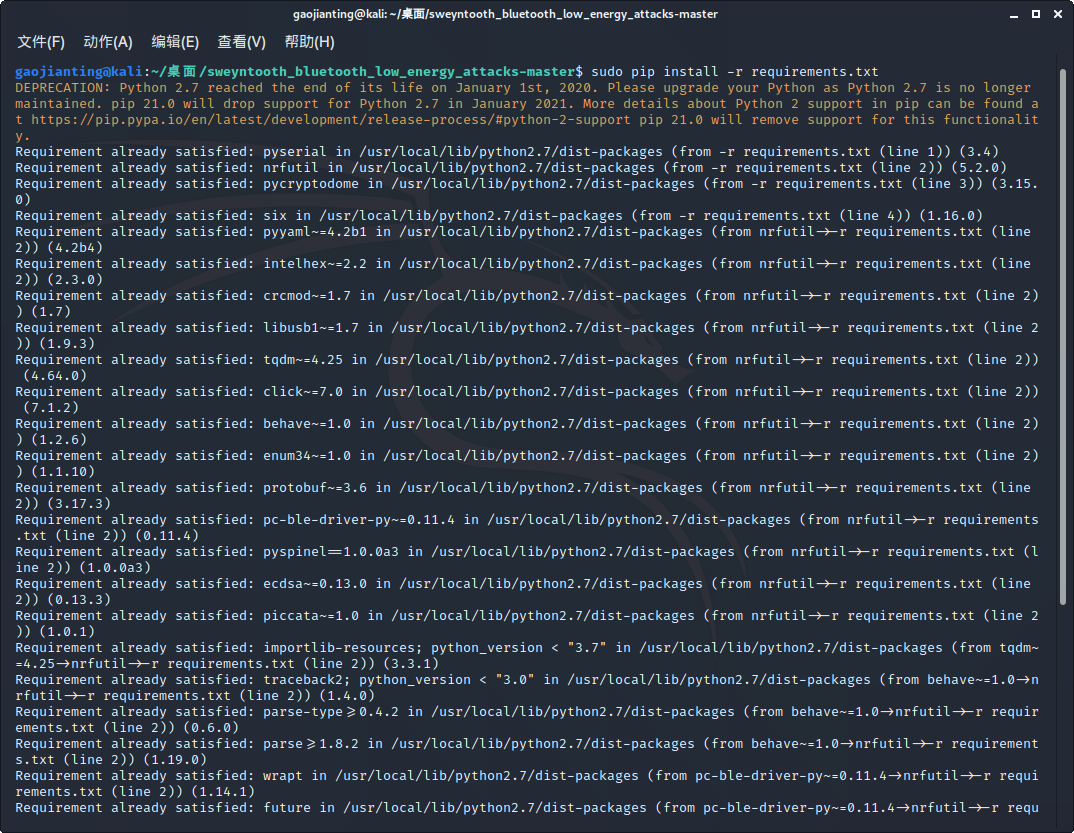


图2 安装依赖

运行程序需要使用写有固件nRF52\_driver\_firmware.hex的nrf52840 dongle设备。运行程序时使用指令“sudo python program.py port mac”。在kali环境下port一般为/dev/ttyACM0，mac为所测设备的mac地址。

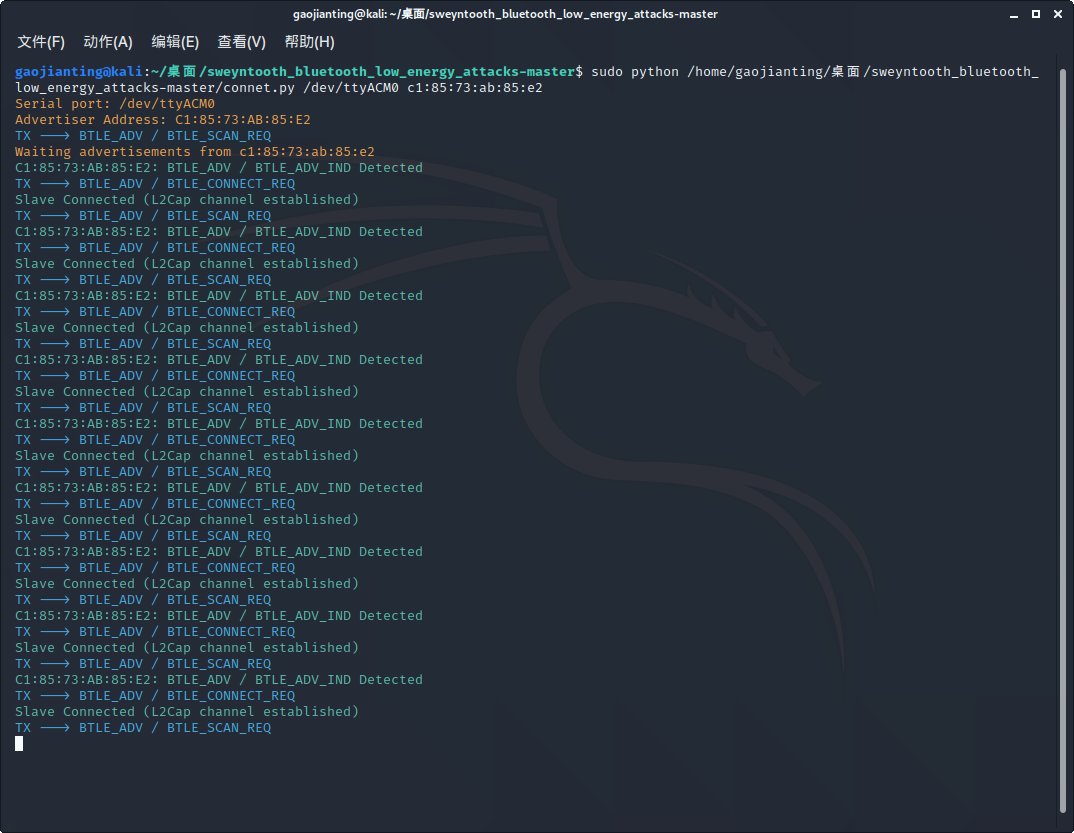


图3 运行connect程序

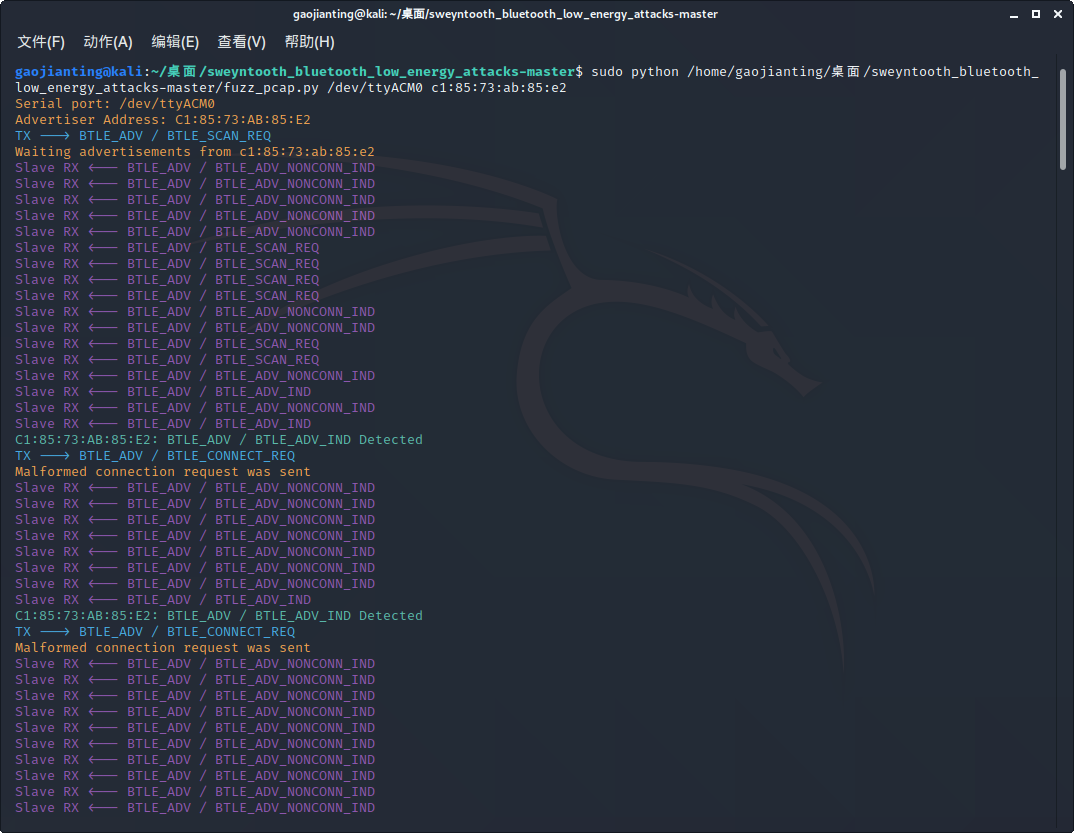


图4 运行fuzz程序