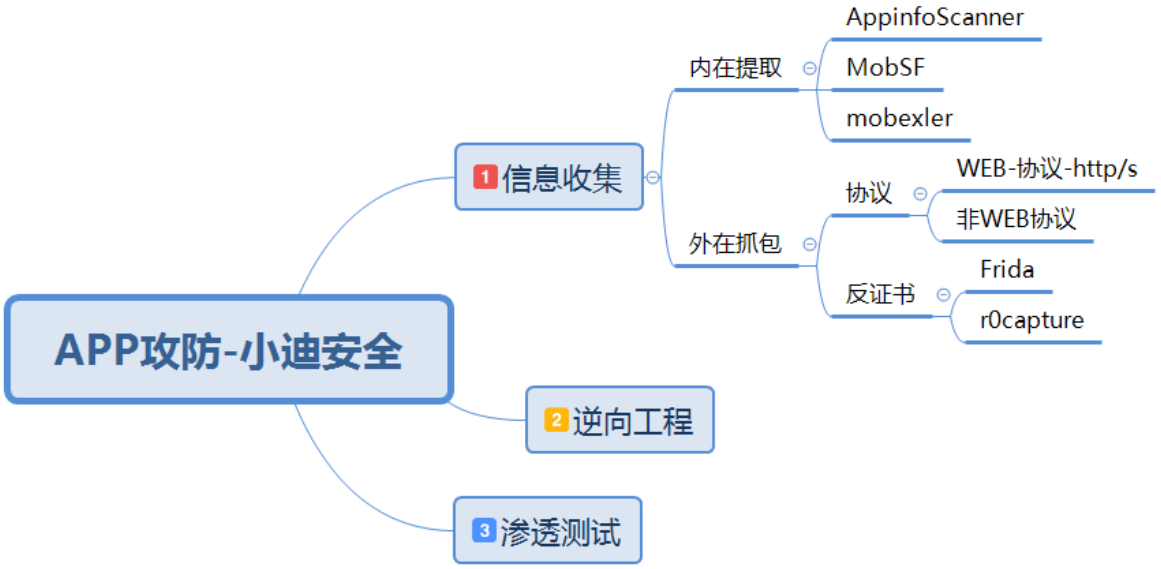
Day67　APP 攻防-Frida 反证书抓包&移动安全系统&资产提取&评估扫描



1.知识点

- 1、资产提权-AppinfoScanner
- 2、评估框架-MobSF&mobexler
- 3、抓包利器-Frida&r0capture

2.章节点

- 1、信息收集-应用&资产提取&权限等
- 2、漏洞发现-反编译&脱壳&代码审计
- 3、安全评估-组件&敏感密匙&恶意分析

3.核心点

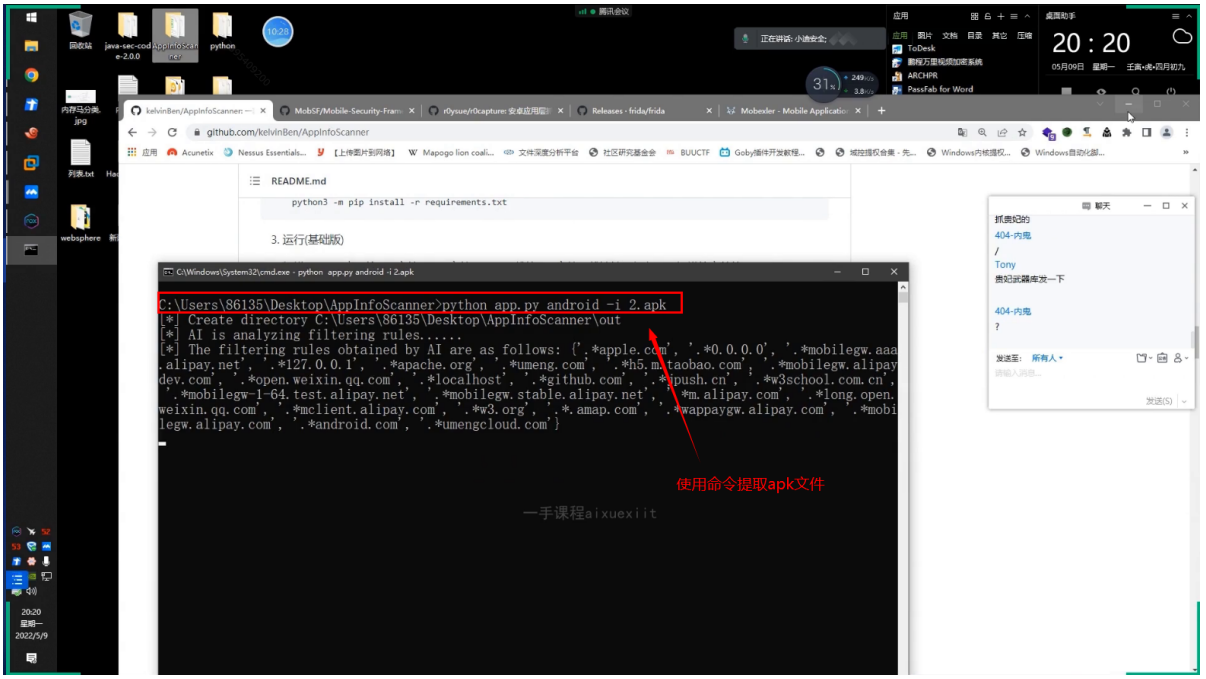
- 1、内在点-资产提取&版本&信息等
- 2、抓包点-反代理&反证书&协议等
- 3、逆向点-反编译&脱壳&重打包等
- 4、安全点-资产&接口&漏洞&审计等

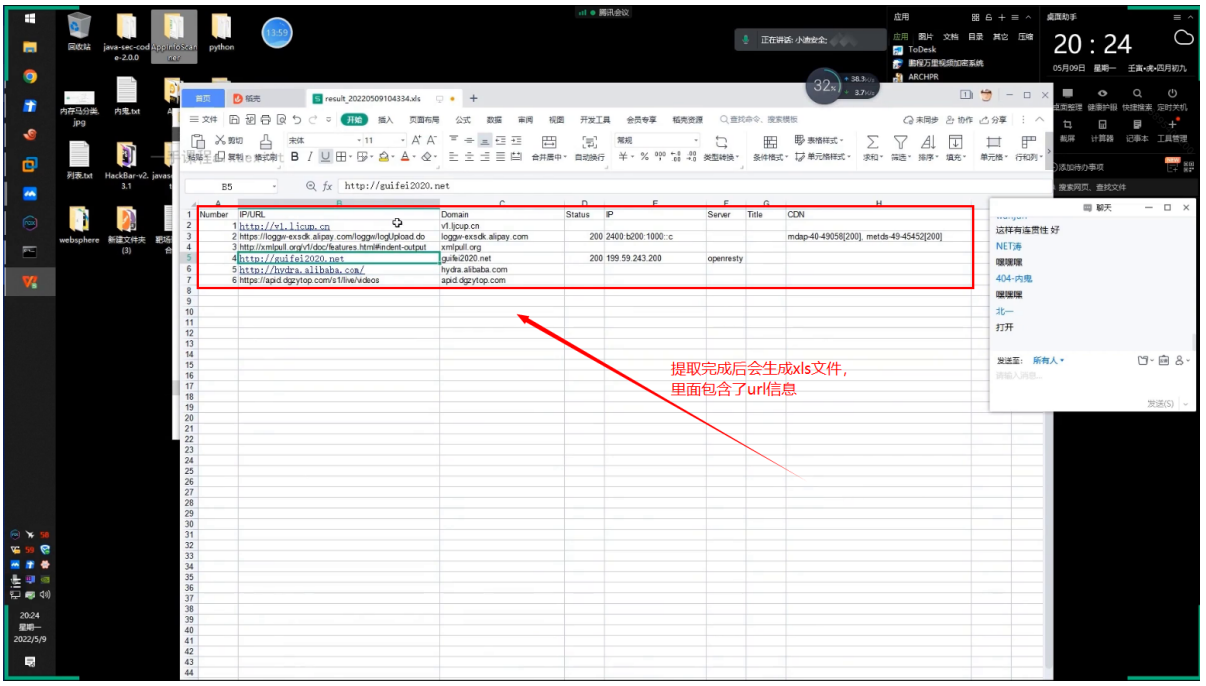
4.演示案例

4.1 内在-资产提取-AppinfoScanner

```
1  AppinfoScanner 一款适用于以 HW 行动/红队/渗透测试团队为场景的移动端(Android、iOS、WEB、H5、静态网站)信息收集扫描工具，可以帮助渗透测试工程师、攻击队成员、红队成员快速收集到移动端或者静态 WEB 站点中关键的资产信息并提供基本的信息输出,如：Title、Domain、CDN、指纹信息、状态信息等。
2  https://github.com/kelvinBen/AppInfoScanner
```

（1）使用工具对apk文件中的url地址进行提取即可：



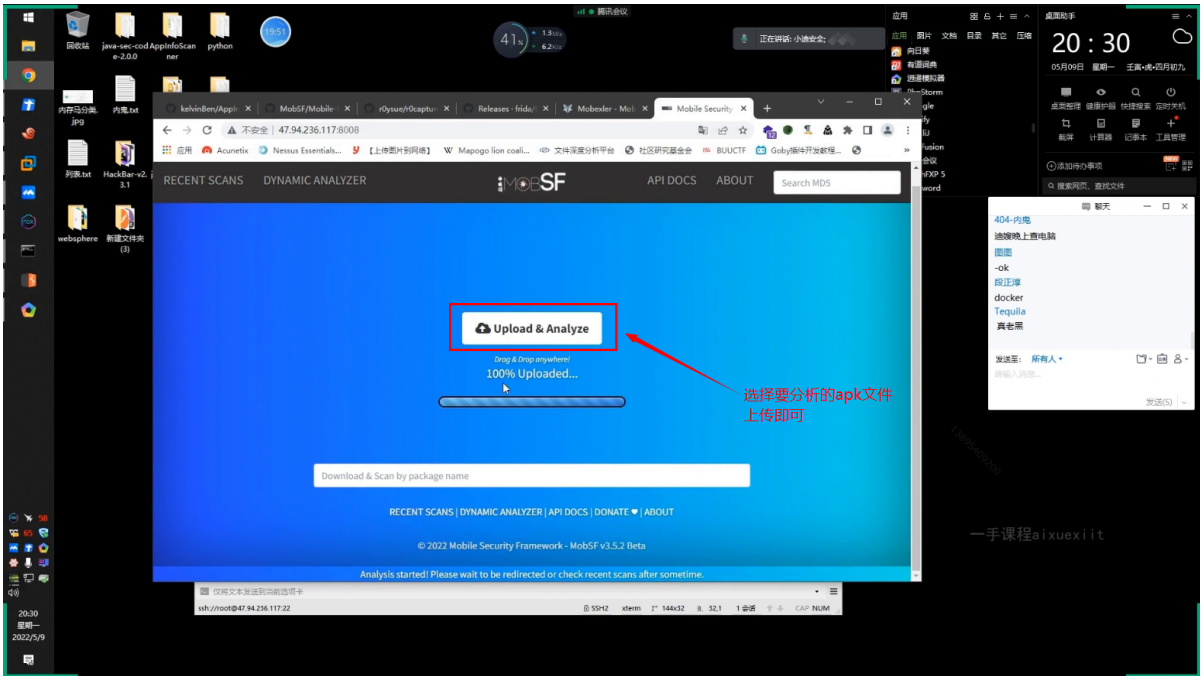


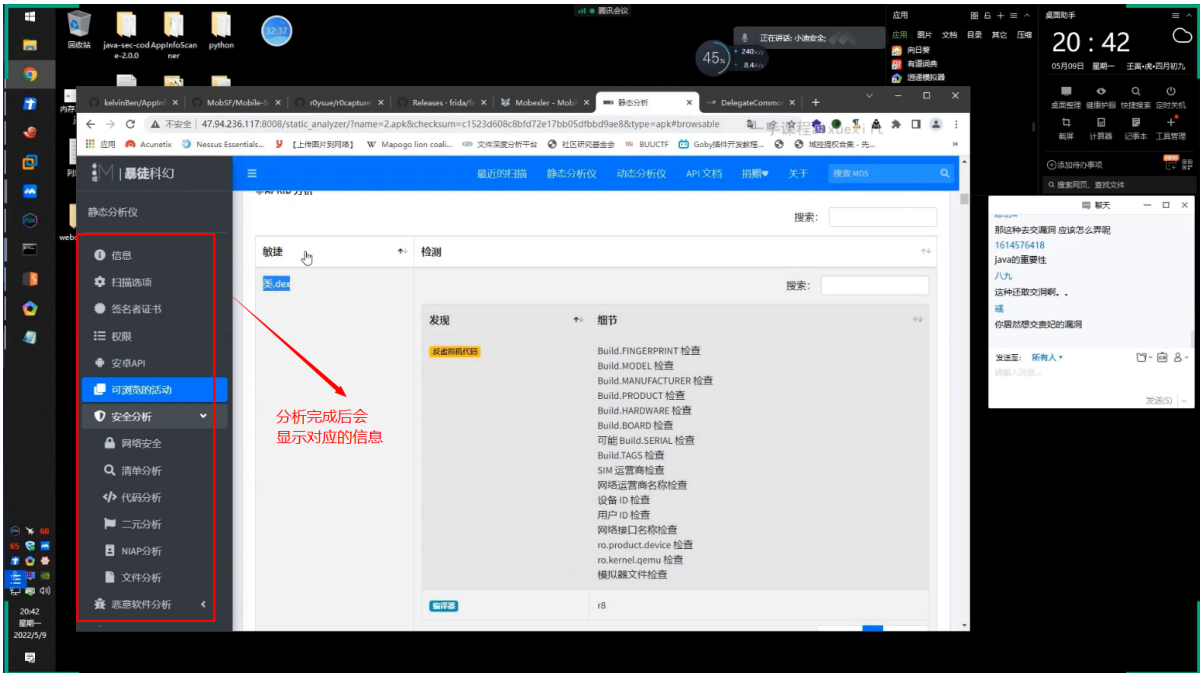
4.2 内在-安全评估-MobSF&mobexler

移动安全框架（MobSF）是一种自动化的一体化移动应用程序（Android/iOS/Windows）渗透测试、恶意软件分析和安全评估框架，能够执行静态和动态分析。MobSF 支持移动应用程序二进制文件（APK、XAPK、IPA 和 APPX）以及压缩源代码，并提供 REST API 以与您的 CI/CD 或 DevSecOps 管道无缝集成。动态分析器可帮助您执行运行时安全评估和交互式仪器测试。

```
Mobexler 是基于 Elementary OS 的定制虚拟机，旨在帮助进行 Android 和 iOS 应用程序的渗透测试。Mobexler 预装了各种开源工具，脚本，黑客必备软件等，这些都是安全测试 Android 和 iOS 应用程序所必需的。
https://mobexler.com/
https://github.com/MobSF/Mobile-Security-Framework-MobSF
docker pull opensecurity/mobile-security-framework-mobsf
docker run -it -p 8008:8000 opensecurity/mobile-securityframework-mobsf:latest
```

（1）靶场搭建完成后，上传apk分析即可：





4.3 外在-证书抓包-frida-server&r0capture

> 以探探APP为例。

```
-r0capture 仅限安卓平台，测试安卓 7、8、9、10、11 可用;无视所有证书校验或绑定，不用考虑任何证书的事情;通杀TCP/IP四层模型中的应用层中的全部协议;
通杀协议包括:Http,WebSocket,Ftp,Xmpp,Imap,Smtp,Protobuf 等、及它们的SSL 版本;
通杀所有应用层框架，包括 HttpUrlConnection、Okhttp1/3/4、Retrofit/Volley 等等； 无视加固，不管是整体壳还是二代壳或 VMP，不用考虑加固的事情;
```

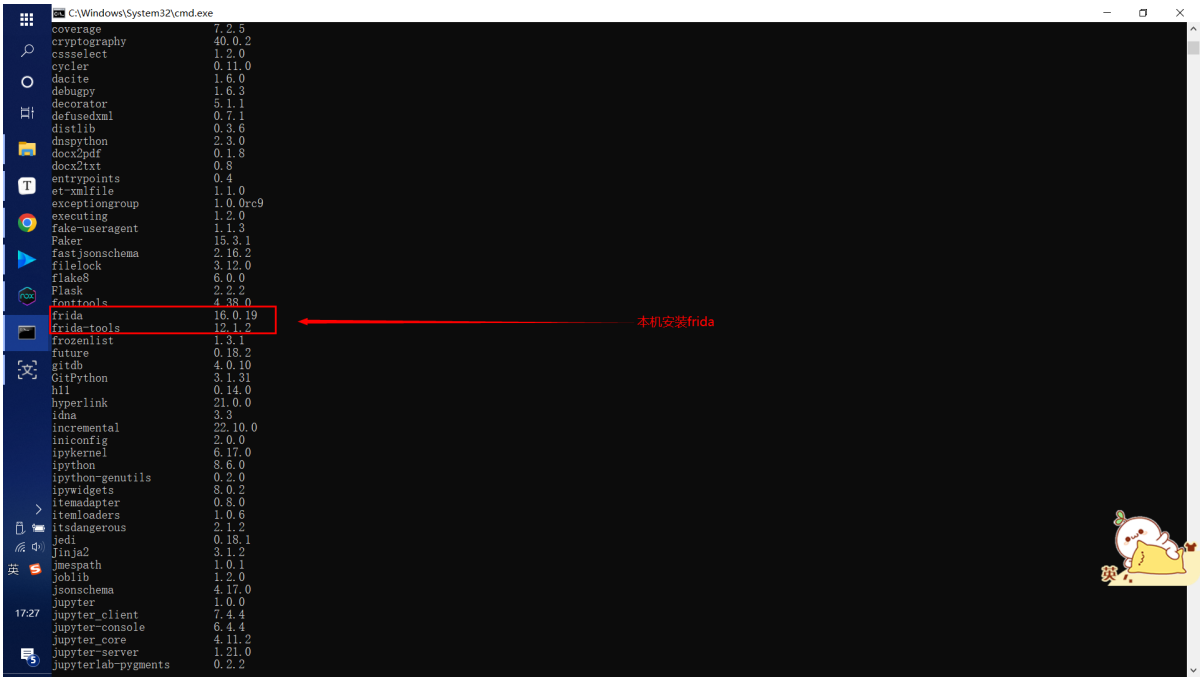
```
-Firda 是一款易用的跨平 Hook 工具， Java 层到 Native 层的 Hook 无所不能，是一种 动态 的插桩工具，可以插入代码到原生 App 的内存空间中，动态的去监视和修改行为，原生平台包括 Win、Mac、Linux、Android、iOS 全平台。
```

```
测试环境:
Windows10 Python3.7 夜神模拟器 r0capture frida-server wireshark
https://github.com/r0ysue/r0capture
https://github.com/frida/frida/releases
```

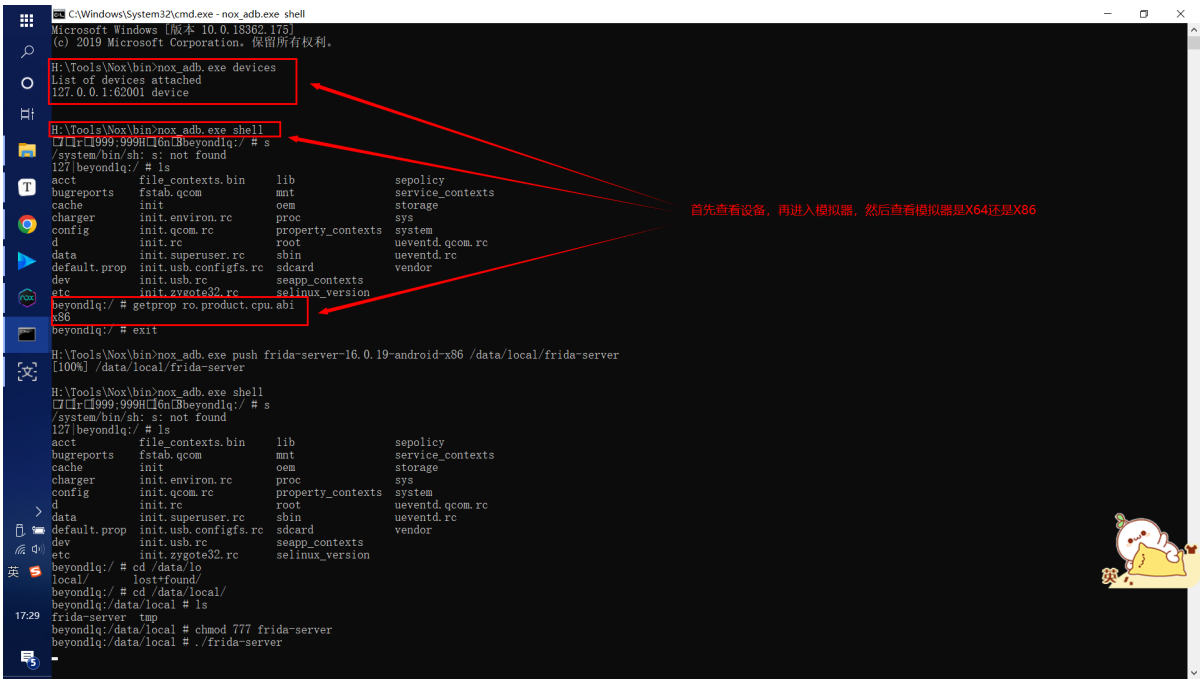
```
1、本地安装Frida
pip install frida
pin install firda-tools

2、模拟器安装Frida
注意:版本要与本地Frida一致
下载: https://github.com/frida/frida/releases
真机:ARM版本及位数模拟器:无ARM的位数
getprop ro.product.cpu.abi  #查看是X86还是X64
```

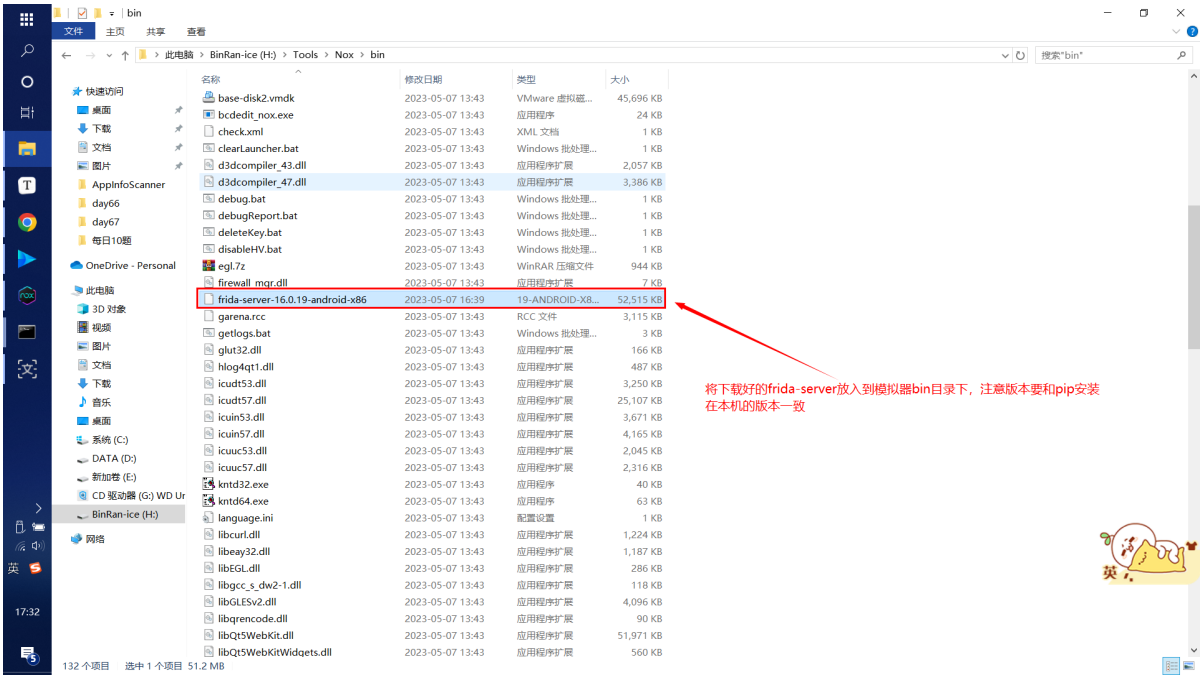
```
nox_adb.exe devices      #查看设备
nox_adb.exe shell        #进入模拟器
nox_adb.exe push frida-server-16.0.19-android-x86 /data/local/frida-server  #将frida-sever上传到模拟器
cd /data/local/      #切换到frida-sever目录
chmod 777 frida-server        #赋予执行权限
./frida-server                #运行
ps | grep frida               #查看进程是否运行成功

3、转发并启动Frida
nox_adb.exe forward tcp:27042 tcp:27042
连接判断:frida-ps -U frida-ps -R

4、获取包名并运行抓包
获取包名:/data/data或Apk-Messenger
python rOcapture.py -U -f com.p1.mobile.putong -p tantan.pcap
```

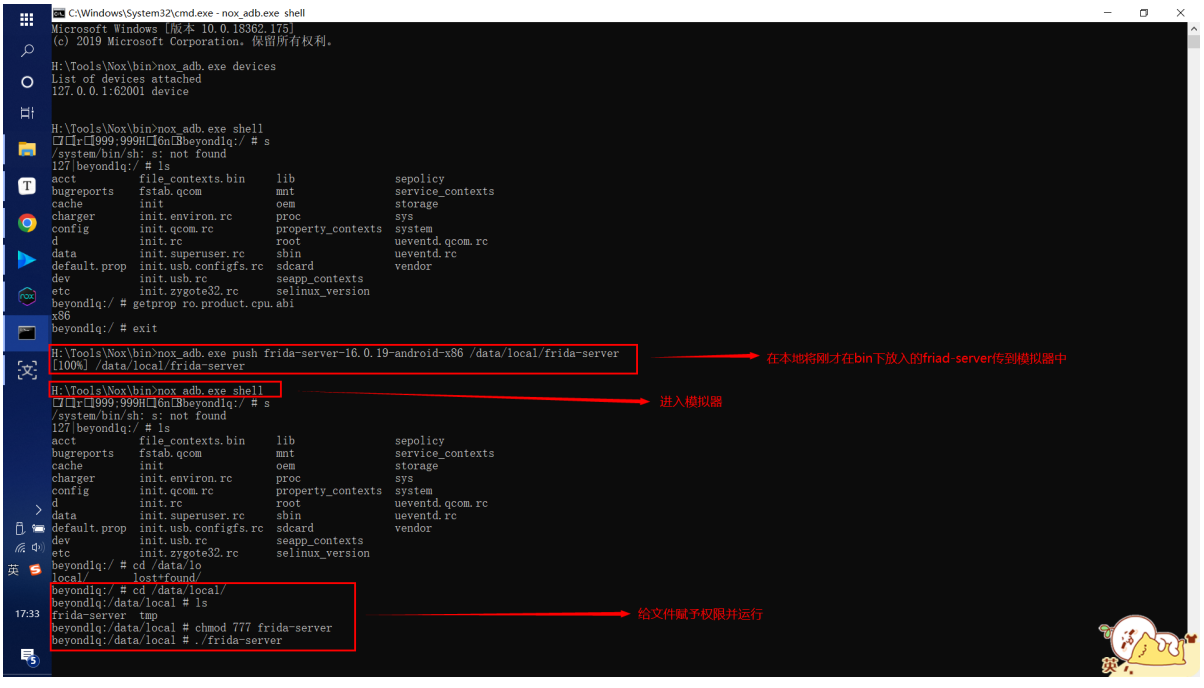
（1）本地安装Frida：



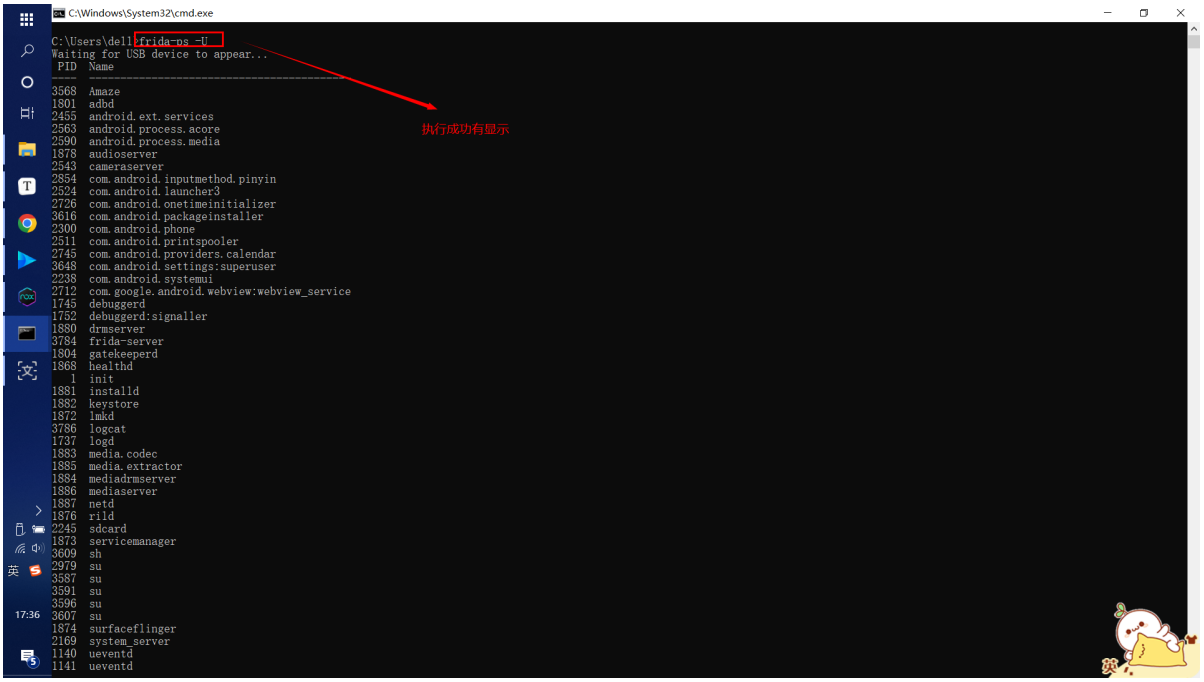
（2）模拟器安装Frida：

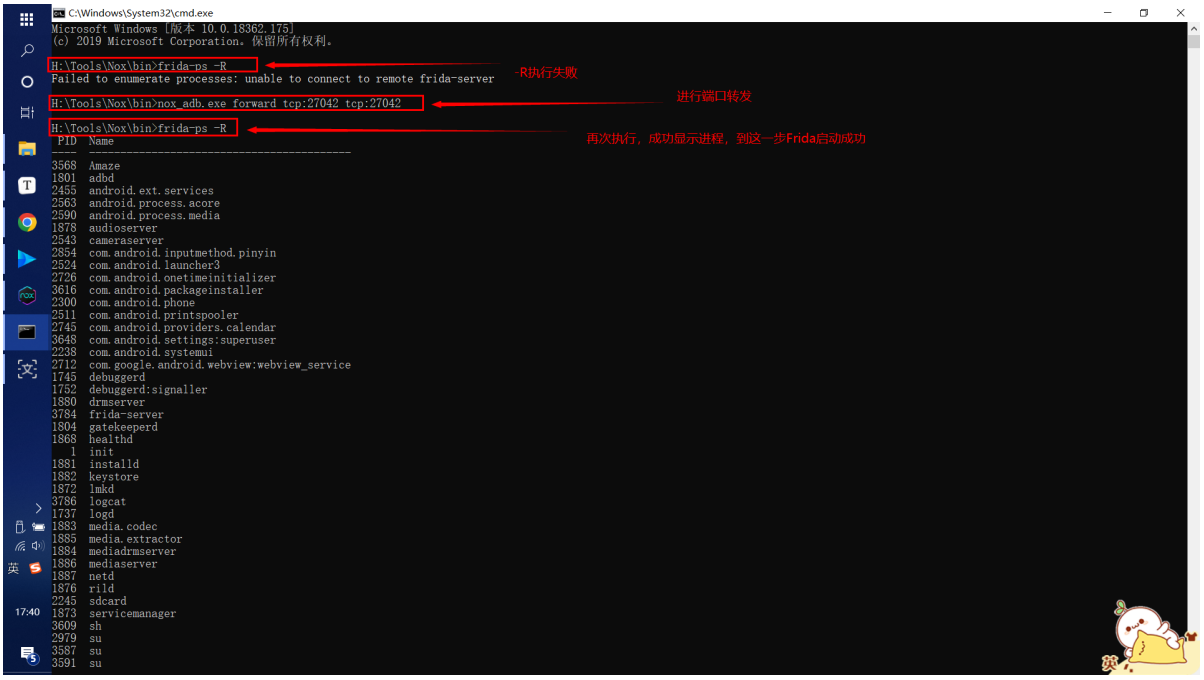

C:\Windows\System32\cmd.exe - nox_adb.exe shell
Microsoft Windows [版本 10.0.18362.175]
(c) 2019 Microsoft Corporation。保留所有权利。
H:\Tools\Nox\bin>nox_adb.exe devices
List of devices attached
127.0.0.1:62001 device
H:\Tools\Nox\bin>nox_adb.exe shell
/system/bin/sh: s: not found
127|beyondlq:/ # ls
beyondlq:/ # getprop ro.product.cpu.abi
x86
beyondlq:/ # exit
H:\Tools\Nox\bin>nox_adb.exe push frida-server-16.0.19-android-x86 /data/local/frida-server
[100%] /data/local/frida-server
beyondlq:/ # cd /data/lo
beyondlq:/ # cd /data/local/
beyondlq:/data/local # ls
frida-server tmp
beyondlq:/data/local # chmod 777 frida-server
beyondlq:/data/local # ./frida-server
首先查看设备，再进入模拟器，然后查看模拟器是X64还是X86


bin
frida-server-16.0.19-android-x86
将下载好的frida-server放入到模拟器bin目录下，注意版本要和pip安装在本机的版本一致


C:\Windows\System32\cmd.exe - nox_adb.exe shell
H:\Tools\Nox\bin>nox_adb.exe push frida-server-16.0.19-android-x86 /data/local/frida-server
在本地将刚才在bin下放入的friad-server传到模拟器中
H:\Tools\Nox\bin>nox_adb.exe shell
进入模拟器
beyondlq:/data/local # chmod 777 frida-server
beyondlq:/data/local # ./frida-server
给文件赋予权限并运行

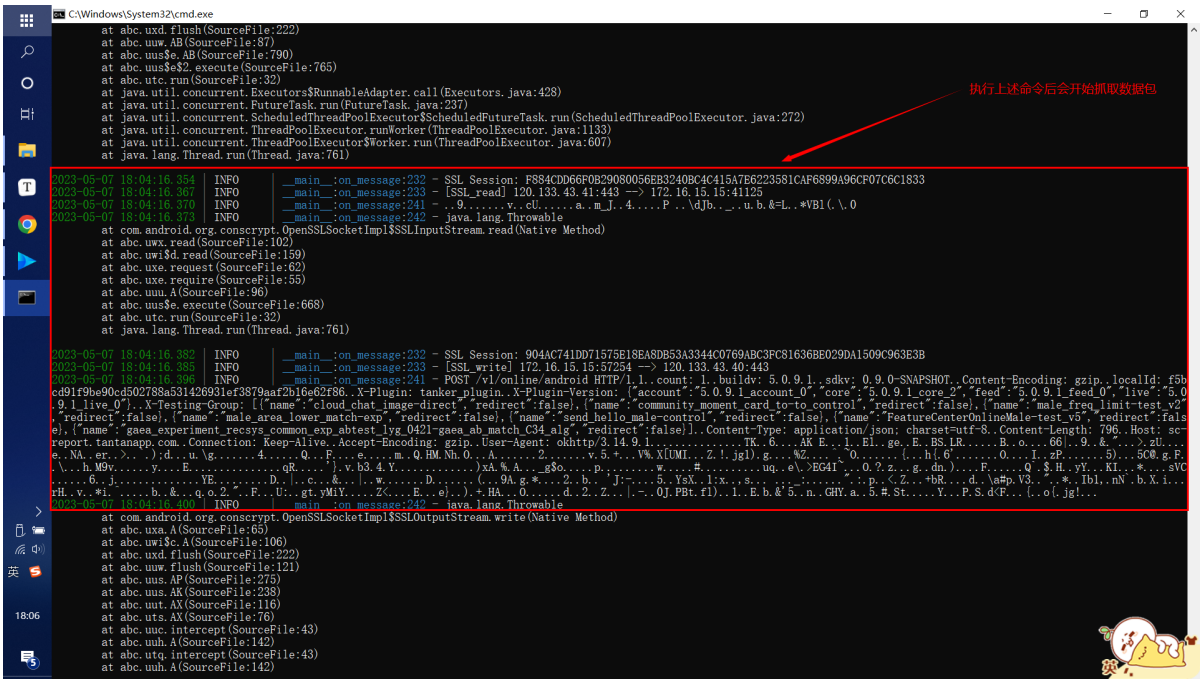
（3）连接判断，启动Frida：

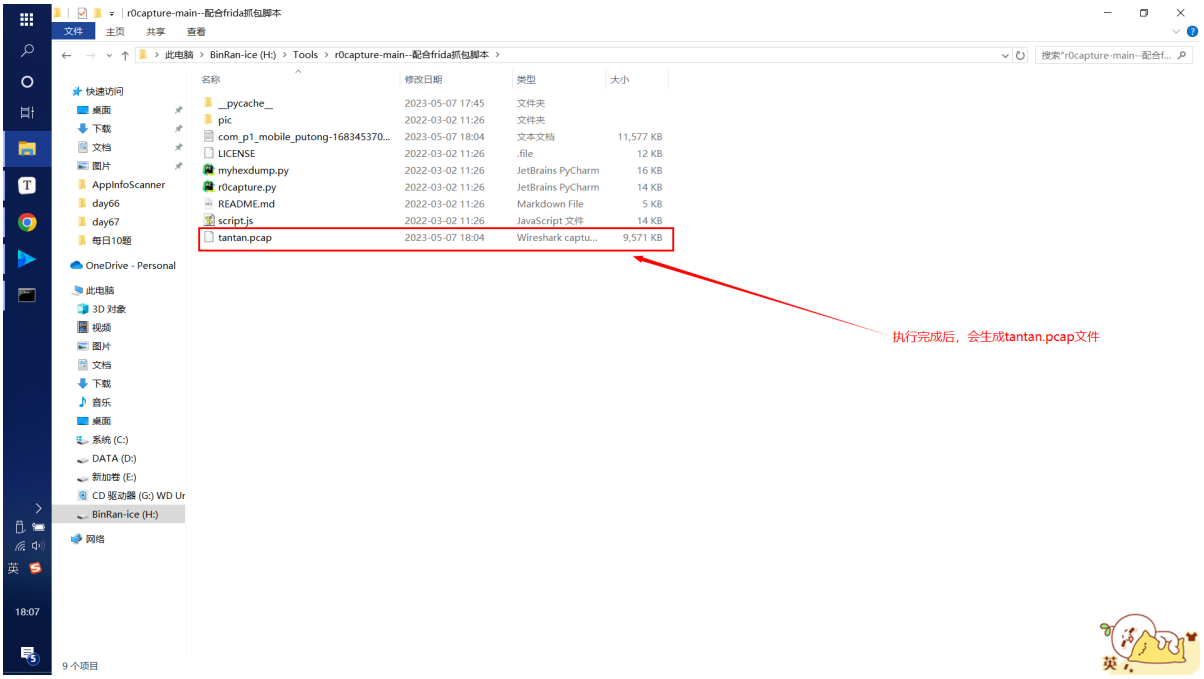




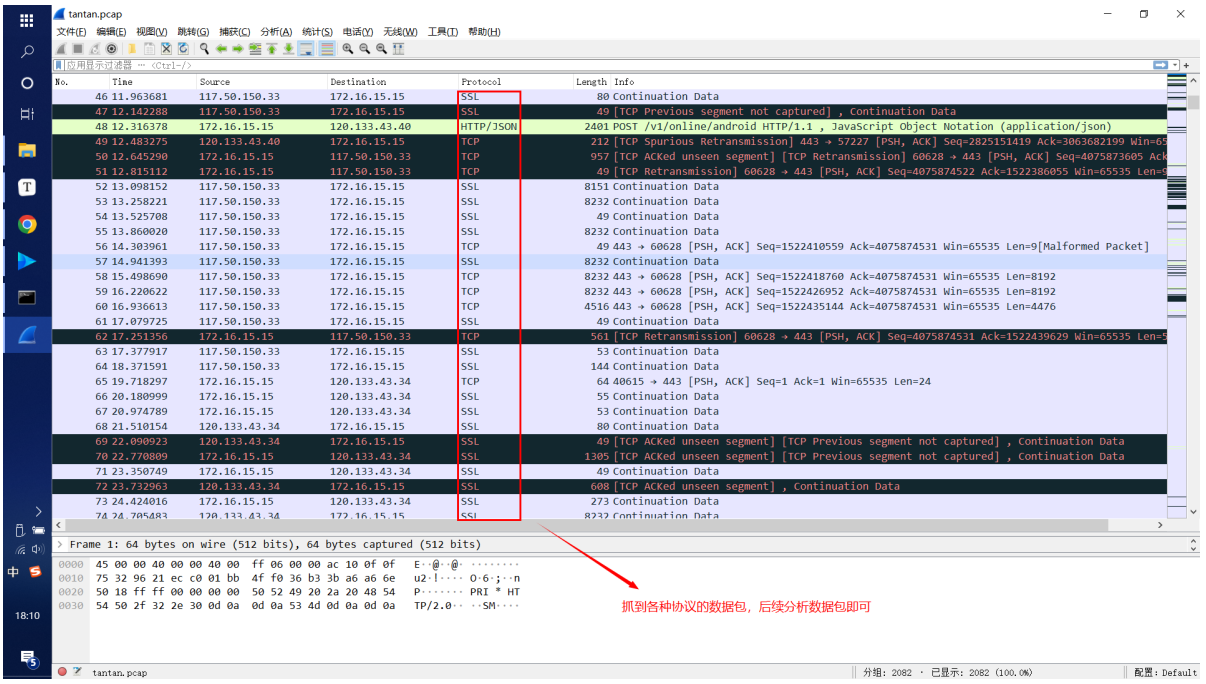
（4）获取包名并运行抓包：

```
python r0capture.py -U -f com.p1.mobile.putong -p tantan.pcap
```





（5）使用wireshark分析数据包即可：



资源：

```
AppInfoScanner：
https://github.com/kelvinBen/AppInfoScanner
mobexler：
https://mobexler.com/
MobSF：
https://github.com/MobSF/Mobile-Security-Framework-MobSF
rOcapture：
https://github.com/rOysue/rOcapture
frida：
https://github.com/frida/frida/releases
```