

# 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

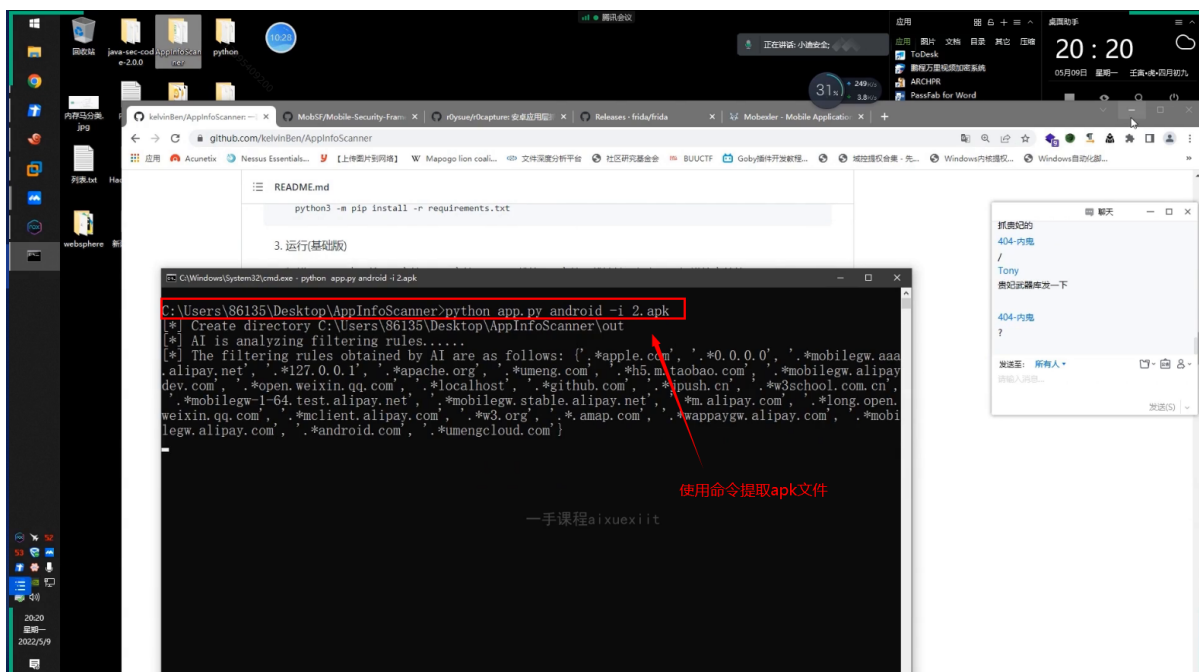
- 1、内在点-资产提取&版本&信息等
- 2、抓包点-反代理&反证书&协议等
- 3、逆向点-反编译&脱壳&重打包等
- 4、安全点-资产&接口&漏洞&审计等

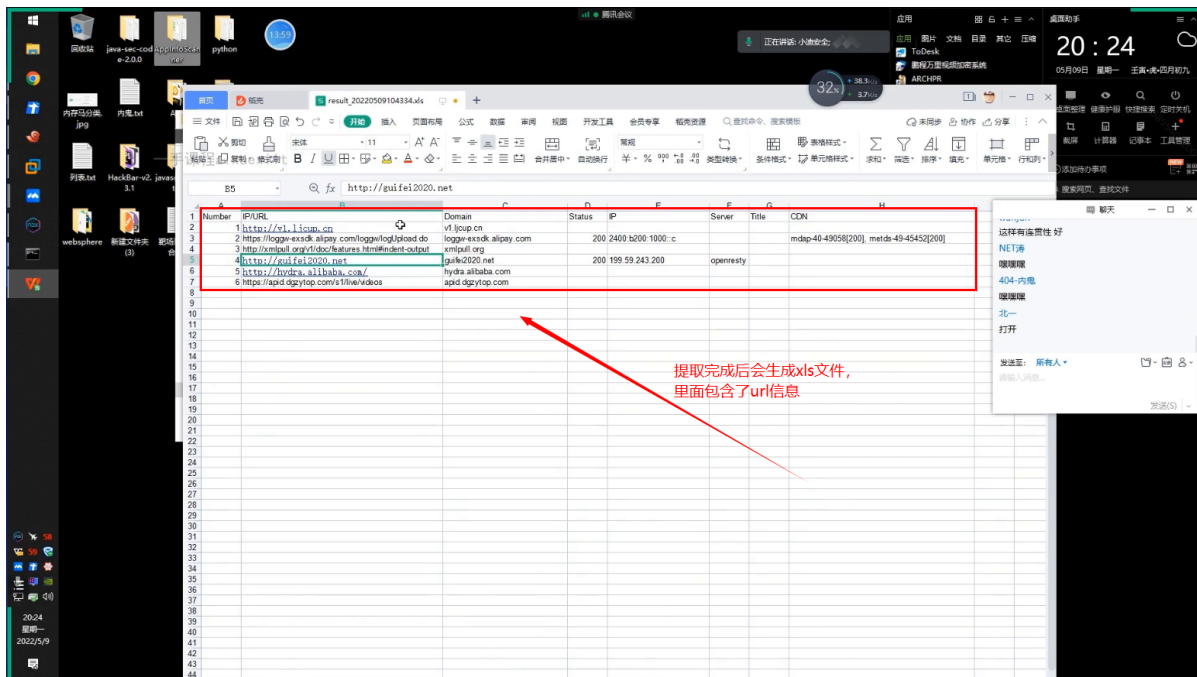
### 4.演示案例

#### 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

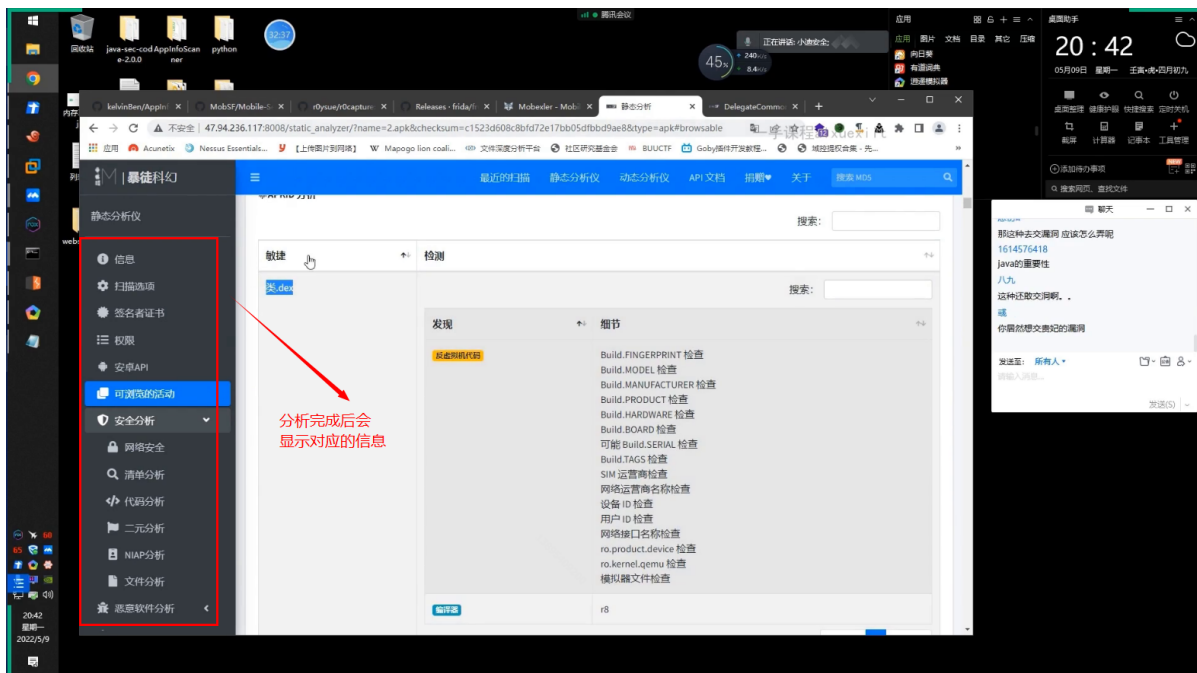
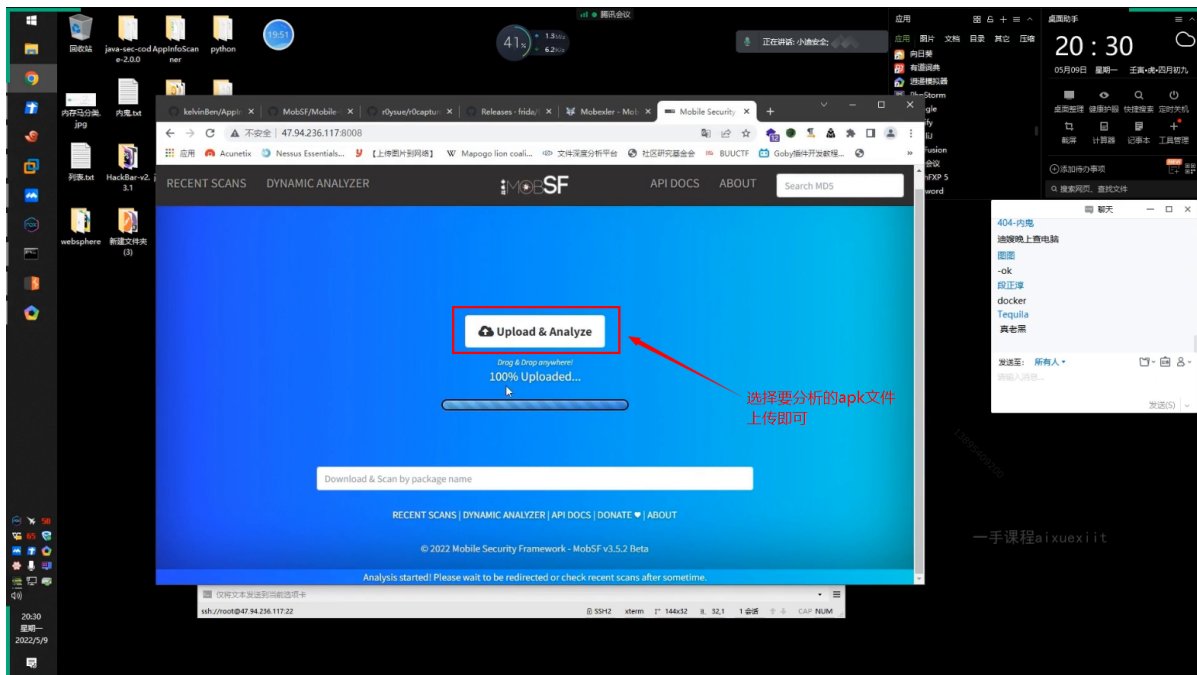


- 1 移动安全框架（MobSF）是一种自动化的一体化移动应用程序（Android/iOS/windows）渗透测试、恶意软件分析和安全评估框架，能够执行静态和动态分析。MobSF 支持移动应用程序二进制文件（APK、XAPK、IPA 和 APPX）以及压缩源代码，并提供 REST API 以与您的 CI/CD 或 DevSecOps 管道无缝集成。动态分析器可帮助您执行运行时安全评估和交互式仪器测试。



- 1 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。
- 2 <https://mobexler.com/>
- 3 <https://github.com/MobSF/Mobile-Security-Framework-MobSF>
- 4 `docker pull opensecurity/mobile-security-framework-mobsf`
- 5 `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。



- 1 `-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；
- 2 通杀协议包括：  
`Http,WebSocket,Ftp,Xmpp,Imap,Smtp,Protobuf` 等、及它们的SSL 版本；
- 3 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；



- 1 `-Frida` 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。



- 1 测试环境：
- 2 windows10 Python3.7 夜神模拟器 `r0capture frida-server wireshark`
- 3 <https://github.com/r0ysue/r0capture>
- 4 <https://github.com/frida/frida/releases>



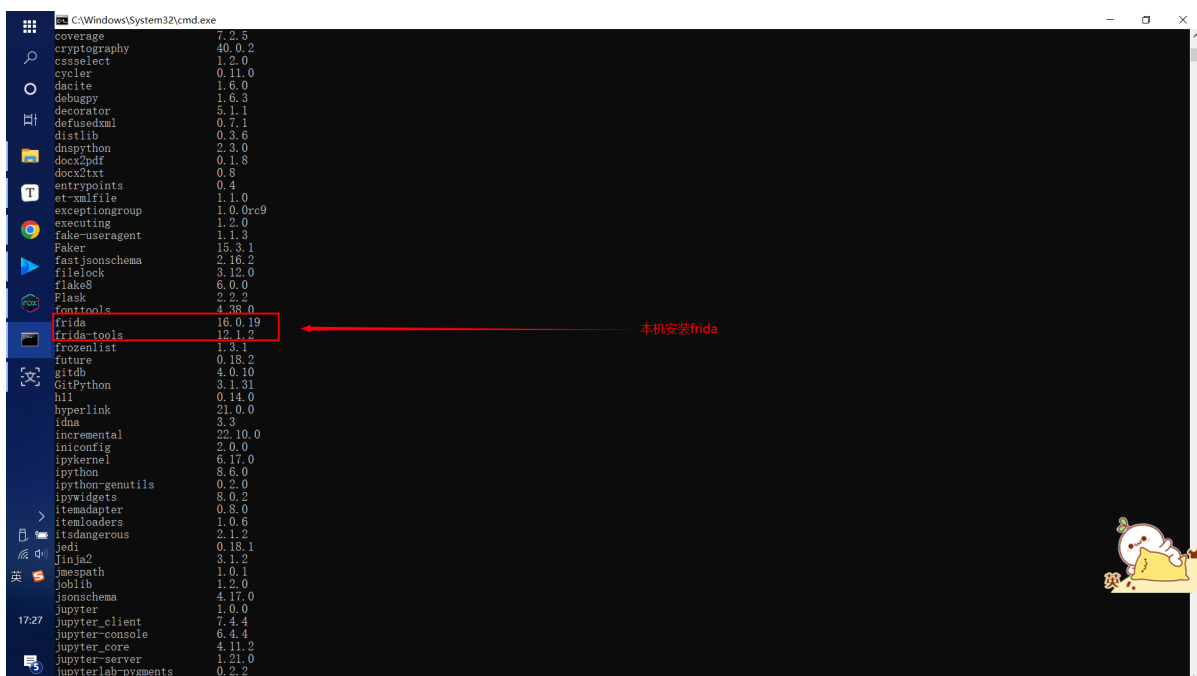
- 1 1、本地安装Frida
- 2 `pip install frida`
- 3 `pin install frida-tools`
- 4
- 5 2、模拟器安装Frida
- 6 注意：版本要与本地Frida一致
- 7 下载：<https://github.com/frida/frida/releases>
- 8 真机：ARM版本及位数模拟器：无ARM的位数
- 9 `getprop ro.product.cpu.abi` #查看是x86还是x64

```

10 nox_adb.exe devices      #查看设备
11 nox_adb.exe shell      #进入模拟器
12 nox_adb.exe push frida-server-16.0.19-android-
   x86 /data/local/frida-server #将frida-sever上传到
   模拟器
13 cd /data/local/        #切换到frida-sever目录
14 chmod 777 frida-server  #赋予执行权限
15 ./frida-server          #运行
16 ps | grep frida         #查看进程是否运行成功
17
18 3、转发并启动Frida
19 nox_adb.exe forward tcp:27042 tcp:27042
20 连接判断:frida-ps -U frida-ps -R
21
22 4、获取包名并运行抓包
23 获取包名:/data/data或Apk-Messenger
24 python r0capture.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
[1]r1999:999H[6nBbeyondiq:/ # s
/system/bin/sh: s: not found
127/beyondiq:/ # ls
acct      file_contexts.bin  lib          sepolICY
bugreports fstab.qcom        mnt          service_contexts
cache     init              oem          storage
charger   init.envIRON.rc   proc         sys
config    init.qcom.rc      property_contexts system
d         init.rc           root         ueventd.qcom.rc
data      init.superuser.rc/sbin         ueventd.rc
default.prop init.usb.configfs.rc sdcard       vendor
dev        init.usb.rc       seapp_contexts
etc        init.zygote32.rc  selinux_version

beyondiq:/ # getprop ro.product.cpu.abi
x86

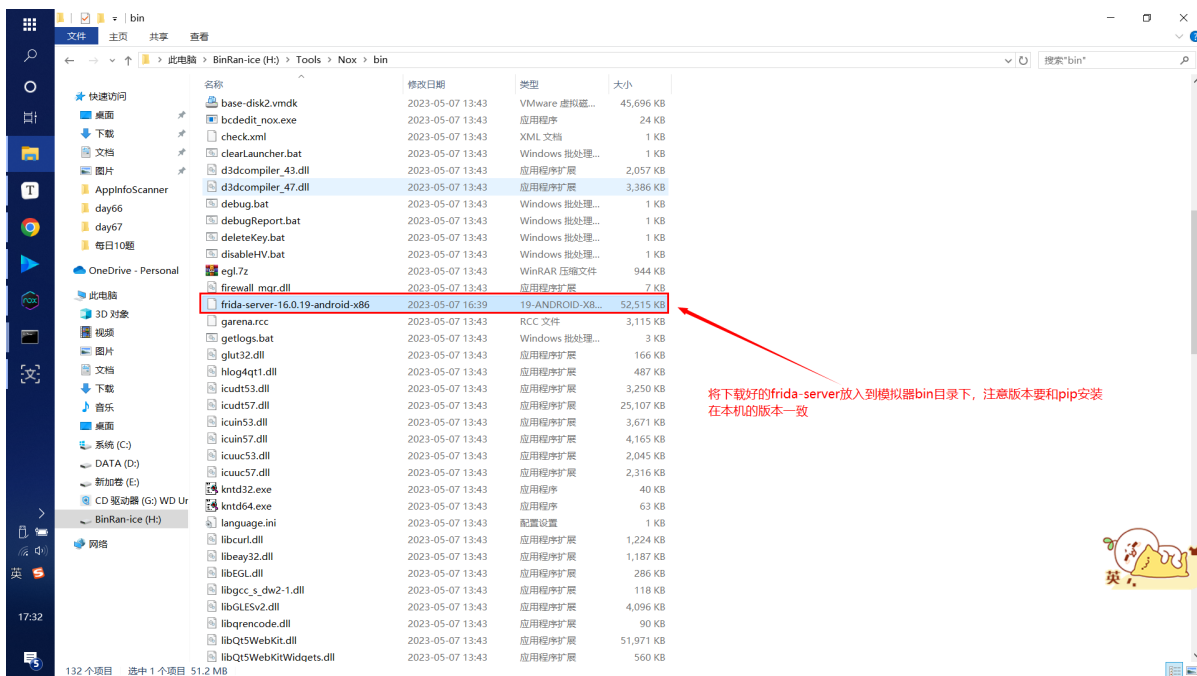
beyondiq:/ # exit

H:\Tools\Nox\bin>nox_adb.exe push frida-server-16.0.19-android-x86 /data/local/frida-server
[100%] /data/local/frida-server

H:\Tools\Nox\bin>nox_adb.exe shell
[1]r1999:999H[6nBbeyondiq:/ # s
/system/bin/sh: s: not found
127/beyondiq:/ # ls
acct      file_contexts.bin  lib          sepolICY
bugreports fstab.qcom        mnt          service_contexts
cache     init              oem          storage
charger   init.envIRON.rc   proc         sys
config    init.qcom.rc      property_contexts system
d         init.rc           root         ueventd.qcom.rc
data      init.superuser.rc/sbin         ueventd.rc
default.prop init.usb.configfs.rc sdcard       vendor
dev        init.usb.rc       seapp_contexts
etc        init.zygote32.rc  selinux_version

beyondiq:/ # cd /data/local/
lostfound/
beyondiq:/ # cd /data/local/
beyondiq:/data/local # ls
frida-server tmp
beyondiq:/data/local # chmod 777 frida-server
beyondiq:/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



C:\Windows\System32\cmd.exe - nox\_adb.exe shell

Microsoft Windows [版本 10.0.15368.1715]  
(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  
[1999:999H]onBbeyondiq:/ # s  
/system/bin/sh: s; not found  
127beyondiq:/ # ls

|              |                      |                   |                  |
|--------------|----------------------|-------------------|------------------|
| acct         | file_contexts.bin    | lib               | sepolicy         |
| bugreports   | fstab.qcom           | mnt               | service_contexts |
| cache        | init                 | oem               | storage          |
| charger      | init.envirom.rc      | proc              | sys              |
| config       | init.qcom.rc         | property_contexts | system           |
| d            | init.rc              | root              | ueventd.qcom.rc  |
| data         | init.superuser.rc    | sbin              | ueventd.rc       |
| default.prop | init.usb.configfs.rc | sdcard            | vendor           |
| dev          | init.usb.rc          | seapp_contexts    |                  |
| etc          | init.zygote32.rc     | selinux_version   |                  |

beyondiq:/ # getprop ro.product.cpu.abi  
x86  
beyondiq:/ # 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

H:\Tools\Nox\bin\nox\_adb.exe shell  
[1999:999H]onBbeyondiq:/ # s  
/system/bin/sh: s; not found  
127beyondiq:/ # ls

|              |                      |                   |                  |
|--------------|----------------------|-------------------|------------------|
| acct         | file_contexts.bin    | lib               | sepolicy         |
| bugreports   | fstab.qcom           | mnt               | service_contexts |
| cache        | init                 | oem               | storage          |
| charger      | init.envirom.rc      | proc              | sys              |
| config       | init.qcom.rc         | property_contexts | system           |
| d            | init.rc              | root              | ueventd.qcom.rc  |
| data         | init.superuser.rc    | sbin              | ueventd.rc       |
| default.prop | init.usb.configfs.rc | sdcard            | vendor           |
| dev          | init.usb.rc          | seapp_contexts    |                  |
| etc          | init.zygote32.rc     | selinux_version   |                  |

beyondiq:/ # cd /data/io  
local/  
lost+found/  
beyondiq:/ # cd /data/local/  
beyondiq:/data/local # ls  
frida-server tmp  
beyondiq:/data/local # chmod 777 frida-server  
beyondiq:/data/local # ./frida-server



### (3) 连接判断, 启动Frida:

```
C:\Windows\System32\cmd.exe
C:\Users\deli>frida-ps -U
Waiting for USB device to appear...
PID Name
-----
3568 Amaze
1801 adbd
2455 android.ext.services
2563 android.process.acore
2590 android.process.media
1878 audioserver
2543 cameracore
2854 com.android.inputmethod.pinyin
2524 com.android.launcher3
2726 com.android.onetimeinitializer
3616 com.android.packageinstaller
2300 com.android.phone
2511 com.android.printspooler
2745 com.android.providers.calendar
3648 com.android.settings.superuser
2238 com.android.systemui
2712 com.google.android.webview:webview_service
1745 debuggerd
1752 debuggerd:signaller
1880 drmservice
3784 frida-server
1804 gatekeeperd
1868 healthd
1 init
1881 install
1882 keystore
1872 lmkd
3786 logcat
1737 logd
1883 media.codec
1885 media.extractor
1884 mediadrmserver
1886 mediaserver
1887 netd
1876 ril
2245 sdcard
1873 servicemanager
3609 sh
2979 su
3587 su
3591 su
3596 su
3607 su
1874 surfaceflinger
2169 system_server
1140 ueventd
1141 ueventd
```

```
C:\Windows\System32\cmd.exe
Microsoft Windows [版本 10.0.18362.175]
(c) 2019 Microsoft Corporation. 保留所有权利。

H:\Tools\Nox\bin>frida-ps -R
Failed to enumerate processes: unable to connect to remote frida-server -R执行失败

H:\Tools\Nox\bin>nox adb.exe forward tcp:27042 tcp:27042 进行端口转发

H:\Tools\Nox\bin>frida-ps -R
PID Name
-----
3568 Amaze
1801 adbd
2455 android.ext.services
2563 android.process.acore
2590 android.process.media
1878 audioserver
2543 cameracore
2854 com.android.inputmethod.pinyin
2524 com.android.launcher3
2726 com.android.onetimeinitializer
3616 com.android.packageinstaller
2300 com.android.phone
2511 com.android.printspooler
2745 com.android.providers.calendar
3648 com.android.settings.superuser
2238 com.android.systemui
2712 com.google.android.webview:webview_service
1745 debuggerd
1752 debuggerd:signaller
1880 drmservice
3784 frida-server
1804 gatekeeperd
1868 healthd
1 init
1881 install
1882 keystore
1872 lmkd
3786 logcat
1737 logd
1883 media.codec
1885 media.extractor
1884 mediadrmserver
1886 mediaserver
1887 netd
1876 ril
2245 sdcard
1873 servicemanager
3609 sh
2979 su
3587 su
3591 su
```

### (4) 获取包名并运行抓包:

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

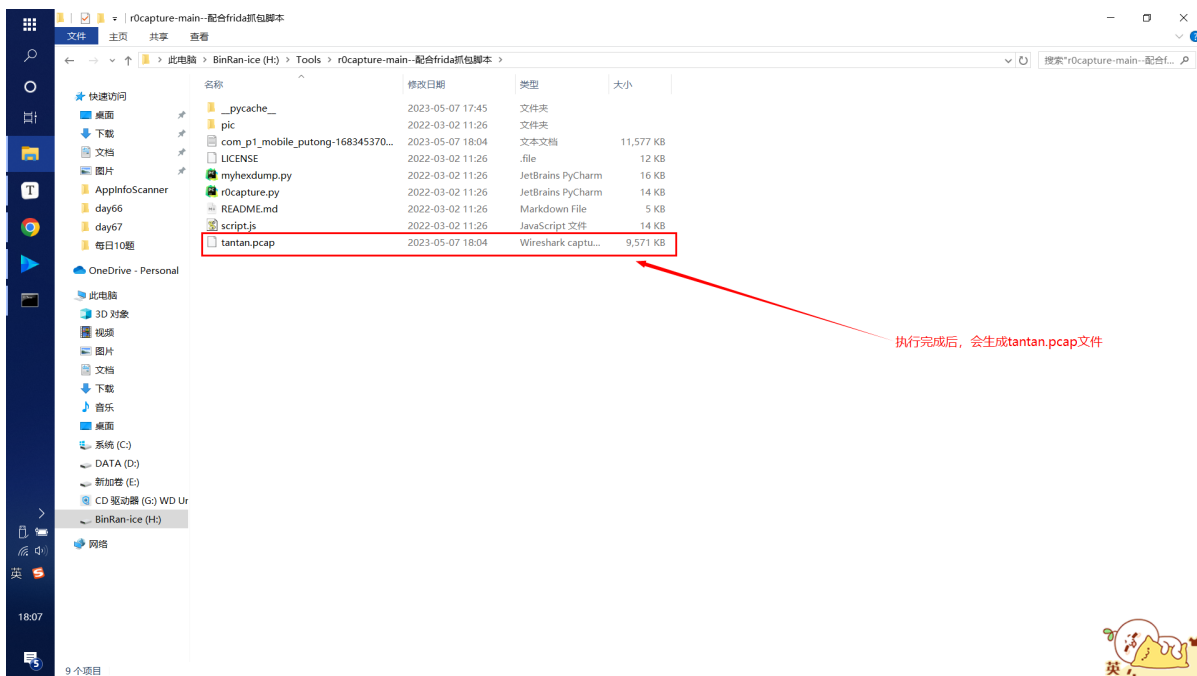


```
C:\Windows\System32\cmd.exe
at abc.uxd.flush(SourceFile:222)
at abc.uuw.AB(SourceFile:37)
at abc.uus$e.AB(SourceFile:790)
at abc.uus$e$2.execute(SourceFile:765)
at abc.uts.run(SourceFile:32)
at java.util.concurrent.ExecutorTask$RunnableAdapter.call(Executors.java:428)
at java.util.concurrent.FutureTask.run(FutureTask.java:237)
at java.util.concurrent.ScheduledThreadPoolExecutor$ScheduledFutureTask.run(ScheduledThreadPoolExecutor.java:272)
at java.util.concurrent.ThreadPoolExecutor.runWorker(ThreadPoolExecutor.java:1133)
at java.util.concurrent.ThreadPoolExecutor$Worker.run(ThreadPoolExecutor.java:607)
at java.lang.Thread.run(Thread.java:761)

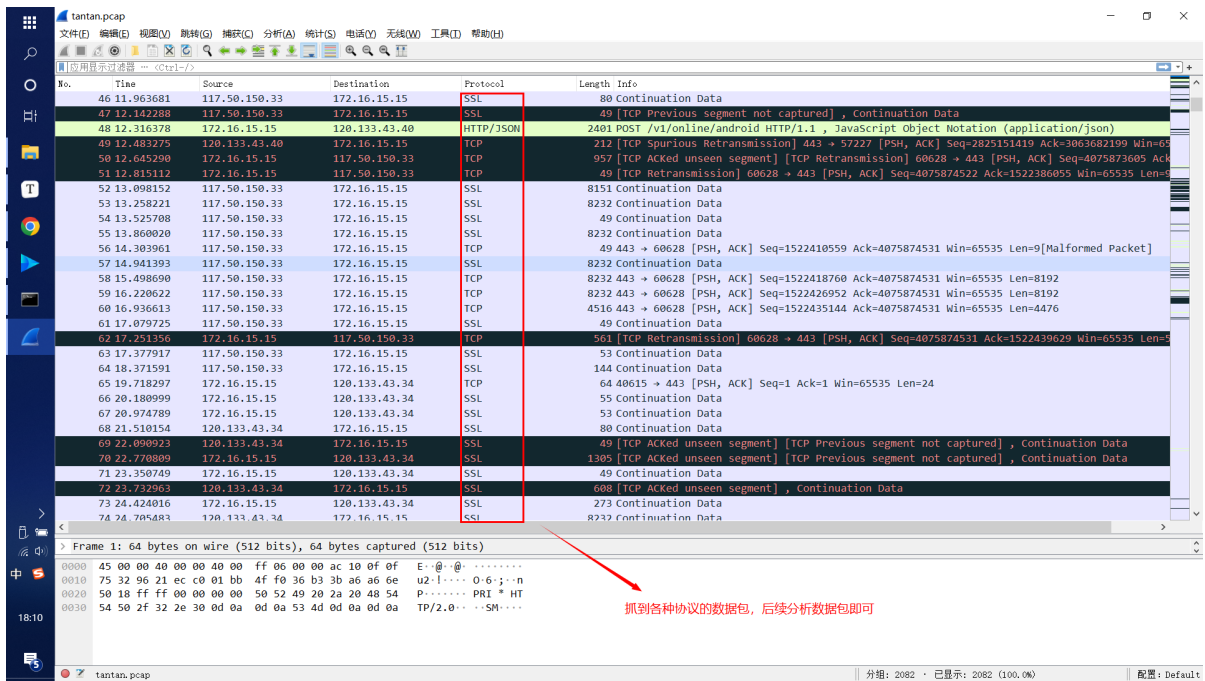
2023-05-07 18:04:16.354 INFO main :on_message:232 - SSL Session: F884CD66F0B29080056EB3240BC4C415A7E6223581CAF6899A96CF07C6C1833
2023-05-07 18:04:16.367 INFO main :on_message:233 - [SSL_read] 120.133.43.41:443 -> 172.16.15.15:41125
2023-05-07 18:04:16.370 INFO main :on_message:241 - ..9.....v.cL.....a.m.J..4....P...dJb...u.b.&=L.*VBI(. \ 0
2023-05-07 18:04:16.373 INFO main :on_message:242 - java.lang.Throwable
at com.android.org.conscrypt.OpenSSLSocketImpl$SSLInputStream.read(Native Method)
at abc.uwx.read(SourceFile:102)
at abc.wi$d.read(SourceFile:159)
at abc.uxe.request(SourceFile:62)
at abc.uxe.require(SourceFile:55)
at abc.uuu.A(SourceFile:96)
at abc.uus$e.execute(SourceFile:668)
at abc.uts.run(SourceFile:32)
at java.lang.Thread.run(Thread.java:761)

2023-05-07 18:04:16.382 INFO main :on_message:232 - SSL Session: 904AC741DD71575E18EA8DB53A3344C0769ABC3FC81636BE029DA1509C963E3B
2023-05-07 18:04:16.385 INFO main :on_message:233 - [SSL_write] 172.16.15.15:57254 -> 120.133.43.40:443
2023-05-07 18:04:16.386 INFO main :on_message:241 - POST /v1/online/android HTTP/1.1..count:1..buildv:5.0.9.1..sdkv:0.9.0-SNAPSHOT..Content-Encoding:gzip..localId:f5b
cd91f9be90c4502788a531426931ef3879aaf2b16e62f86..X-Plugin:tanker_plugin..X-Plugin-Version:{'account':'5.0.9.1..account:0'..'core':'5.0.9.1..core:2'..'feed':'5.0.9.1..feed:0'..'live':'5.0
.9.1..live:0'}.X-Testing-Group:[{'name':'cloud_chat_image_direct'..'redirect':false},{'name':'community_moment_card_to_to_control'..'redirect':false},{'name':'male_freq_limit-test_v2'
'..'redirect':false},{'name':'male_area_lower_match-exp'..'redirect':false},{'name':'send_hello_male-control'..'redirect':false},{'name':'FeatureCenterOnlineMale-test_v5'..'redirect':fals
e},{'name':'gaia_experiment_recsys_common_exp_adtest_v2'..'gaia_ab_match:C34..als'..'redirect':false}].Content-Type:application/json..charset=utf-8..Content-Length:796..Host:scr
report.tantanapp.com..Connection:Keep-Alive..Accept-Encoding:gzip..User-Agent:okhttp/3.14.9.....TK..6...AK.E...l..El..ga..E..BS.LR.....B..o...66)..9..&...>zH...
e..NA..er...>..>..d...u..g.....4.....Q..F...e...m..Q..HM..Nn..0..A.....2.....v..5..+...V%..X[UMI...Z..l..jgl)..g...%Z.....0.....{..h..6'.....0...I..zP.....5)...SCg..F..
{...h..M9v.....>..E.....gR.....}.v.b3.4.Y.....xA.%..A...g$so...p.....w.....#.....uq..e\..>EG41'...0..?..z...g..dn)...F.....Q'..$.H..yY..KI..*...sVC
{...G..j.....G..j.....TE.....D...G..&...l..w.....D...9A..g...&...2..b...J...5..YsX..l..x..s...p..<Z...>+R...d..>ap.V3...*.Ibl..nN..b.X.i...
rh..v..#1...b..E..&..q..0..F...U...gt..mYI...ZC...E...e)..>+Ha...0.....d..2..Z...|..>..0J..FBt..fl)...l..E..b..&..s..n..GH..a..S..R..St...Y...P..S..d(F...l..o{..jg...
2023-05-07 18:04:16.400 INFO main :on_message:242 - java.lang.Throwable
at com.android.org.conscrypt.OpenSSLSocketImpl$SSLOutputStream.write(Native Method)
at abc.uxa.A(SourceFile:65)
at abc.uxa.A(SourceFile:106)
at abc.uxd.flush(SourceFile:222)
at abc.uuw.AB(SourceFile:121)
at abc.uus.AP(SourceFile:275)
at abc.uus.AM(SourceFile:238)
at abc.uts.run(SourceFile:116)
at abc.uts.AX(SourceFile:76)
at abc.uuc.intercept(SourceFile:43)
at abc.uuh.A(SourceFile:142)
at abc.utq.intercept(SourceFile:43)
at abc.uuh.A(SourceFile:142)
```

执行上述命令后会开始抓取数据包



(5) 使用wireshark分析数据包即可：



## 资源：

- 1 AppInfoScanner:
- 2 <https://github.com/kelvinBen/AppInfoScanner>
- 3 mobexler:
- 4 <https://mobexler.com/>
- 5 MobSF:
- 6 <https://github.com/MobSF/Mobile-Security-Framework-MobSF>
- 7 r0capture:
- 8 <https://github.com/r0ysue/r0capture>
- 9 frida:
- 10 <https://github.com/frida/frida/releases>