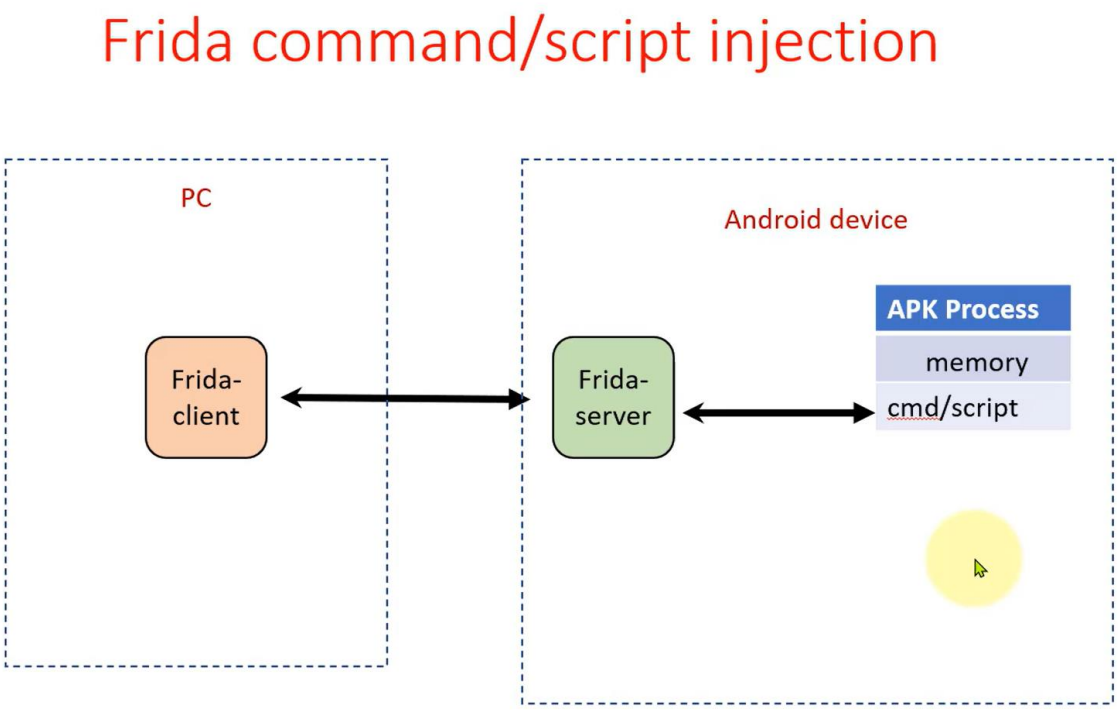
REVERSE ENGINEER: FRIDA FOR BEGINNERS

1 Section 1: Introduction

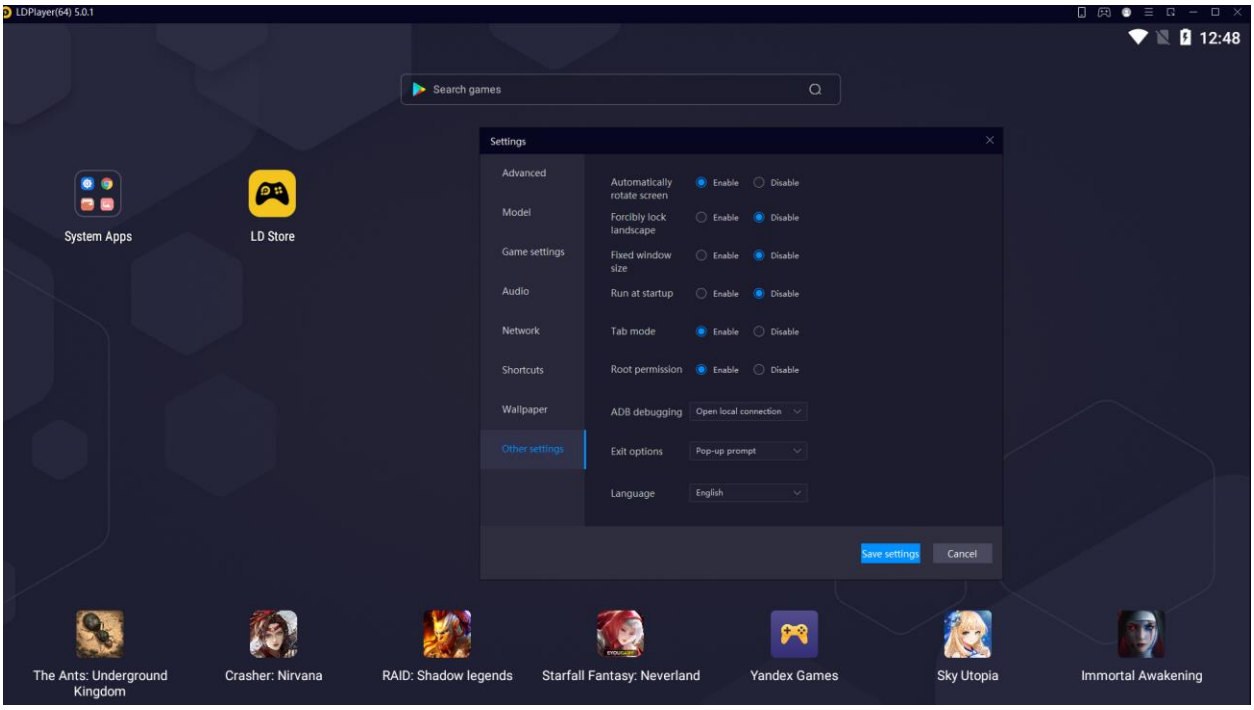
1.1 Intro to Frida

1.2 Intro to Frida Injection



2 Section 2: Setting up lab and rooted android emulator

2.1 Installing LD-player emulator



2.2 Installing platform tools

ABD viết tắt của cụm từ Android Debug Bridge, là một chương trình dạng dòng lệnh (cmd) cho phép tương tác với thiết bị android kết nối với máy tính. Các lệnh adb cho phép thi hành một số tác vụ, như cài đặt ứng dụng, gỡ rối (debug) ứng dụng, đồng thời nó cho phép bạn truy cập vào Unix shell để thi hành các lệnh nhân Unix trên thiết bị.

```
C:\Windows\System32>adb version
Android Debug Bridge version 1.0.41
Version 34.0.0-9570255
Installed as C:\frida-android\platform-tools\adb.exe

C:\Windows\System32>
```

Test → run LD-palyer

C:\Windows\System32>adb kill-server

C:\Windows\System32>adb start-server

```
C:\Windows\System32>adb kill-server

C:\Windows\System32>adb start-server
* daemon not running; starting now at tcp:5037
* daemon started successfully
```

C:\Windows\System32>adb devices

```
C:\Windows\System32>adb devices
List of devices attached
emulator-5554   device


C:\Windows\System32>
```

C:\Windows\System32>adb -s emulator-5554 shell

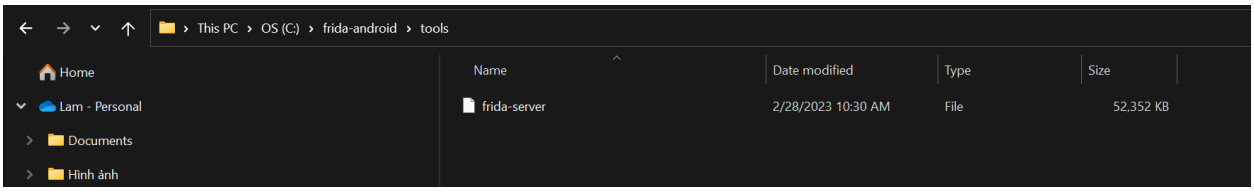
```
C:\Windows\System32>adb -s emulator-5554 shell
aosp:/ # id
uid=0(root) gid=0(root) groups=0(root),1004(input),1007(log),1011(adb),1015(sdcard_rw),1028(sdcard_r),3001(net_bt_admin),3002(net_bt),3003(inet),3006(net_bw_stats),3009(readproc)
```

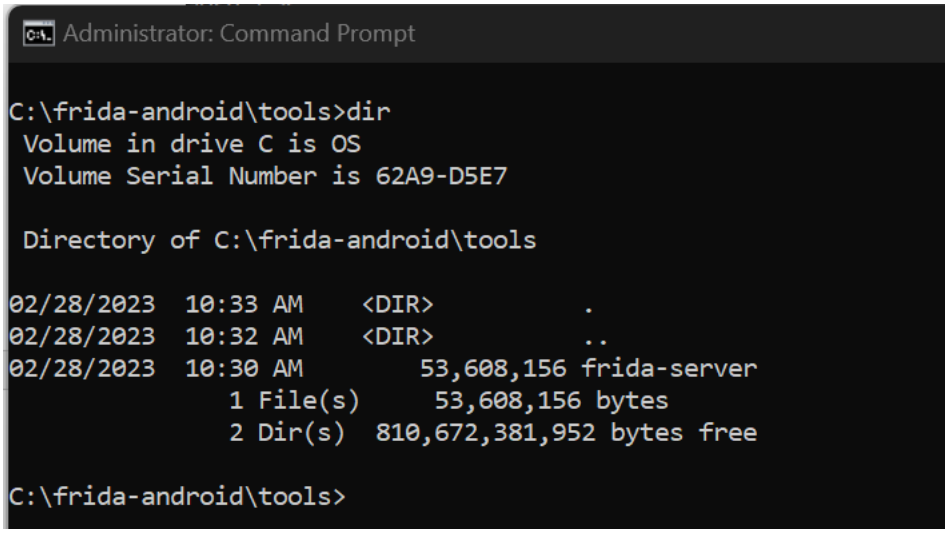
```
aosp:/ # ls -al
total 1876
drwxr-xr-x  16 root   root         0 2023-02-28 00:50 .
drwxr-xr-x  16 root   root         0 2023-02-28 00:50 ..
dr-xr-xr-x  24 root   root         0 2023-02-28 00:50 acct
lrwxrwxrwx   1 root   root        50 1970-01-01 01:00 bugreports -> /data/user_de/0/com.android.shell/files/bugreports
drwxrwx---   6 system cache      120 2023-02-28 00:50 cache
lrwxrwxrwx   1 root   root        13 1970-01-01 01:00 charger -> /sbin/healthd
drwxr-xr-x   3 root   root         0 2023-02-28 00:50 config
lrwxrwxrwx   1 root   root        17 1970-01-01 01:00 d -> /sys/kernel/debug
drwxrwx--x  34 system system    4096 2023-02-28 00:34 data
-rw-------   1 root   root      1361 1970-01-01 01:00 default.prop
drwxr-xr-x  14 root   root      1360 2023-02-28 00:50 dev
lrwxrwxrwx   1 root   root        11 1970-01-01 01:00 etc -> /system/etc
-rw-r--r--   1 root   root     73488 1970-01-01 01:00 file_contexts.bin
-rw-r-----   1 root   root       658 1970-01-01 01:00 fstab.android_x86_64
-rwxr-x---   1 root   root   1513640 1970-01-01 01:00 init
-rwxr-x---   1 root   root      6182 1970-01-01 01:00 init.android_x86_64.rc
-rwxr-x---   1 root   root       887 1970-01-01 01:00 init.environ.rc
-rwxr-x---   1 root   root     52942 1970-01-01 01:00 init.rc
-rwxr-x---   1 root   root      1214 1970-01-01 01:00 init.superuser.rc
-rwxr-x---   1 root   root      9283 1970-01-01 01:00 init.usb.configfs.rc
-rwxr-x---   1 root   root      5718 1970-01-01 01:00 init.usb.rc
-rwxr-x---   1 root   root       411 1970-01-01 01:00 init.zygote32.rc
-rwxr-x---   1 root   root       684 1970-01-01 01:00 init.zygote64_32.rc
lrwxrwxrwx   1 root   root        10 2023-02-28 00:50 lib -> system/lib
drwxr-xr-x  12 root   system     260 2023-02-28 00:50 mnt
drwxr-xr-x   2 root   root         0 1970-01-01 01:00 oem
dr-xr-xr-x 137 root   root         0 2023-02-28 00:50 proc
-rw-r--r--   1 root   root      4365 1970-01-01 01:00 property_contexts
drwx------   2 root   root         0 2023-01-12 07:02 root
drwxr-x---   2 root   root         0 1970-01-01 01:00 sbin
lrwxrwxrwx   1 root   root        21 1970-01-01 01:00 sdcard -> /storage/self/primary
-rw-r--r--   1 root   root       758 1970-01-01 01:00 seapp_contexts
drwxr-xr-x   2 root   root         0 2023-02-28 00:50 selinux
-rw-r--r--   1 root   root        73 1970-01-01 01:00 selinux_version
-rw-r--r--   1 root   root    169459 1970-01-01 01:00 sepolicy
-rw-r--r--   1 root   root     11181 1970-01-01 01:00 service_contexts
drwxr-xr-x   4 root   root        80 2023-02-28 00:50 storage
dr-xr-xr-x  12 root   root         0 2023-02-28 00:50 sys
drwxr-xr-x  17 root   root      4096 1970-01-01 01:00 system
-rw-r--r--   1 root   root       469 1970-01-01 01:00 ueventd.android_x86_64.rc
-rw-r--r--   1 root   root      9606 1970-01-01 01:00 ueventd.rc
lrwxrwxrwx   1 root   root        14 1970-01-01 01:00 vendor -> /system/vendor
aosp:/ #
```

2.3 Install Frida server on Android Emulator

2.3.1 Download Frida-server

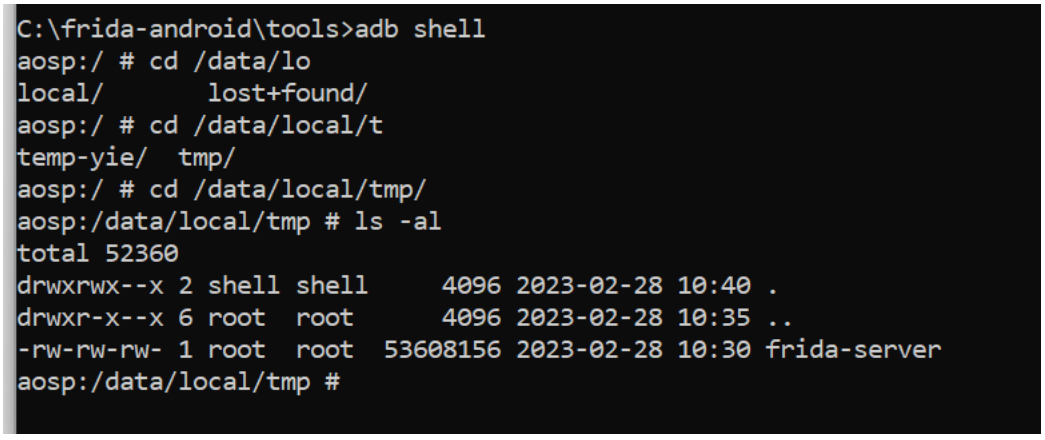
Version [frida-server-16.0.10-android-x86_64.xz]





2.3.2 Copy Frida-server to emulator

C:\frida-android\tools>adb push frida-server /data/local/tmp/



2.3.3 Run Frida server

```
aosp:/data/local/tmp # ls -al
total 52360
drwxrwx--x 2 shell shell     4096 2023-02-28 10:40 .
drwxr-x--x 6 root  root      4096 2023-02-28 10:35 ..
-rw-rw-rw- 1 root  root  53608156 2023-02-28 10:30 frida-server
aosp:/data/local/tmp # chmod -R 777 *
aosp:/data/local/tmp # ls -al
total 52360
drwxrwx--x 2 shell shell     4096 2023-02-28 10:40 .
drwxr-x--x 6 root  root      4096 2023-02-28 10:35 ..
-rwxrwxrwx 1 root  root  53608156 2023-02-28 10:30 frida-server
aosp:/data/local/tmp #
```

aosp:/data/local/tmp # ./frida-server &

```
Administrator: Command Prompt - adb  shell
aosp:/data/local/tmp # ./frida-server &
[1] 2787
aosp:/data/local/tmp # netstat -antlp
Active Internet connections (established and servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program Name
tcp        0      0 127.0.0.1:27042         0.0.0.0:*               LISTEN      2787/frida-server
tcp        0      0 127.0.0.1:5037          0.0.0.0:*               LISTEN      1123/adbd
tcp6       0      0 :::5555                 :::*                    LISTEN      1123/adbd
tcp6       0      0 ::ffff:172.16.1.1:50932 ::ffff:142.251.209.:443 ESTABLISHED 2149/com.android.vending
tcp6       0      0 ::ffff:172.16.1.1:49726 ::ffff:172.217.218:5228 ESTABLISHED 1599/com.google.android.gms.persistent
tcp6       1      0 ::ffff:172.16.1.1:33778 ::ffff:142.250.180.:443 CLOSE_WAIT  2149/com.android.vending
tcp6       0      0 ::ffff:172.16.1.1:35657 ::ffff:142.250.184.:443 ESTABLISHED 1599/com.google.android.gms.persistent
tcp6       0      0 ::ffff:172.16.1.1:53479 ::ffff:142.250.184.:443 ESTABLISHED 2149/com.android.vending
tcp6      32      0 ::ffff:172.16.1.1:56087 ::ffff:129.226.103.:443 CLOSE_WAIT  1830/com.ldmnq.launcher3
tcp6       0    382 ::ffff:172.16.1.15:5555 ::ffff:172.16.1.2:53295 ESTABLISHED 1123/adbd
tcp6       0      0 ::ffff:172.16.1.1:53481 ::ffff:142.250.184.:443 ESTABLISHED 2149/com.android.vending
tcp6     259      0 ::ffff:172.16.1.15:5555 ::ffff:172.16.1.2:53234 CLOSE_WAIT  1123/adbd
tcp6       1      0 ::ffff:172.16.1.1:60115 ::ffff:142.250.180.:443 CLOSE_WAIT  2149/com.android.vending
tcp6       1      0 ::ffff:172.16.1.1:60113 ::ffff:142.250.180.:443 CLOSE_WAIT  2149/com.android.vending
```

```
1|aosp:/data/local/tmp # ps | grep frida
root      2787  2740  61524  48748          0 00f7f1bd30 S ./frida-server
aosp:/data/local/tmp #
```

2.4 Installing objection and Frida tool on the PC

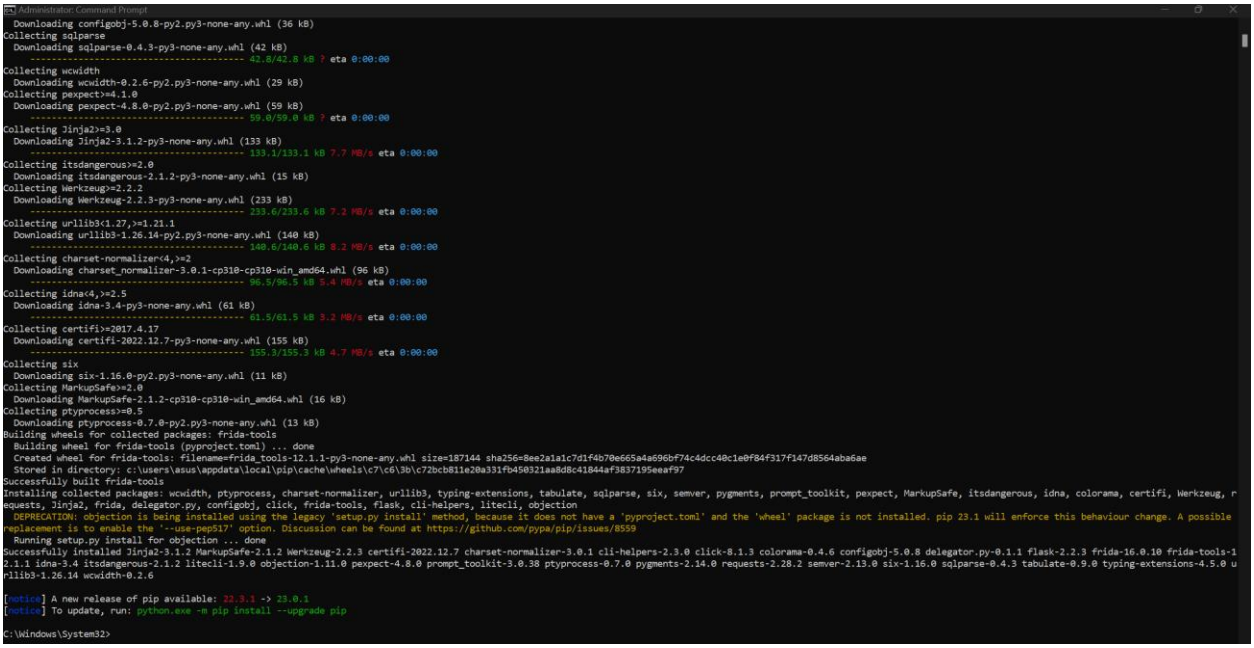
2.4.1 Install python > 3.4

```
C:\Windows\System32>python --version
Python 3.10.9

C:\Windows\System32>
```

```
C:\Windows\System32>pip --version
pip 22.3.1 from C:\Users\ASUS\AppData\Local\Programs\Python\Python310\lib\site-packages\pip (python 3.10)

C:\Windows\System32>
```

2.4.2 Install objection (Frida)

C:\Windows\System32>pip3 install -U objection



2.4.3 Test

2.5 Testing object and Frida

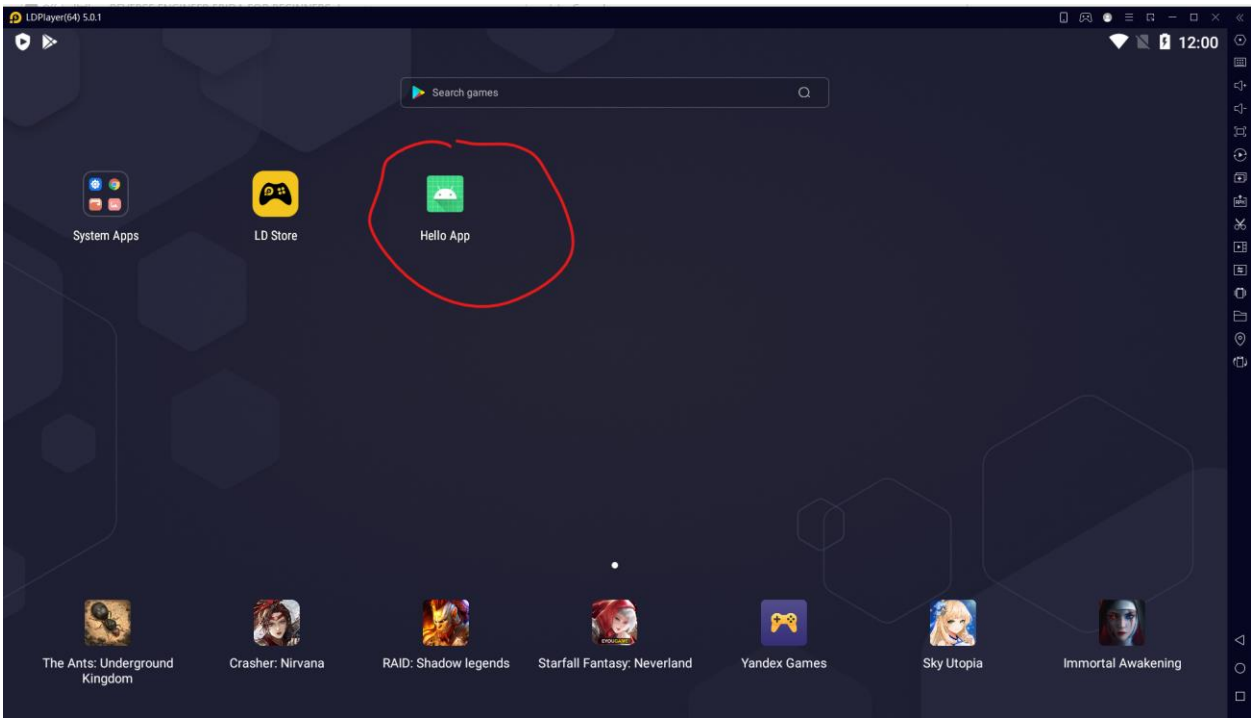
Start Frida server

```
aosp:/data/local/tmp # ./frida-server &
[1] 3477
aosp:/data/local/tmp # netstat -antlp
Active Internet connections (established and servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program Name
tcp        0      0 127.0.0.1:27042         0.0.0.0:*               LISTEN      3477/frida-server
tcp        0      0 127.0.0.1:5037          0.0.0.0:*               LISTEN      1123/adbd
tcp        0      0 172.16.1.15:38989       142.250.184.74:443      ESTABLISHED 1599/com.google.android.gms.persistent
tcp6       0      0 :::5555                 :::*                    LISTEN      1123/adbd
tcp6       0      0 ::ffff:172.16.1.1:49726 ::ffff:172.217.218:5228 ESTABLISHED 1599/com.google.android.gms.persistent
tcp6       0      0 ::ffff:172.16.1.1:38985 ::ffff:142.250.184.:443 ESTABLISHED 3189/com.android.vending:instant_app_installer
tcp6       0      0 ::ffff:172.16.1.1:38988 ::ffff:142.250.184.:443 ESTABLISHED 2149/com.android.vending
tcp6       0      0 ::ffff:172.16.1.15:5555 ::ffff:172.16.1.2:53295 ESTABLISHED 1123/adbd
tcp6       0      0 ::ffff:172.16.1.1:33795 ::ffff:142.250.180.:443 ESTABLISHED 3235/com.google.android.gms
tcp6       0      0 ::ffff:172.16.1.1:50951 ::ffff:142.251.209.:443 ESTABLISHED 2149/com.android.vending
tcp6       0      0 ::ffff:172.16.1.1:34900 ::ffff:142.251.209.:443 ESTABLISHED 3235/com.google.android.gms
tcp6     259      0 ::ffff:172.16.1.15:5555 ::ffff:172.16.1.2:53234 CLOSE_WAIT  1123/adbd
tcp6       0      0 ::ffff:172.16.1.1:53491 ::ffff:142.250.184.:443 ESTABLISHED 2149/com.android.vending
aosp:/data/local/tmp #
```

C:\frida-android\tools>frida-ps -Uai

```
C:\frida-android\tools>frida-ps -Uai
 PID  Name               Identifier
4  -----------------  ----------------------------
2149  Google Play Store  com.android.vending
1995  LD Store           com.android.ld.appstore
1830  Launcher3          com.ldmnq.launcher3
   -  Chrome             com.android.chrome
   -  Contacts           com.android.contacts
   -  File Manager       com.cyanogenmod.filemanager
   -  Files              com.android.documentsui
   -  Gallery            com.android.gallery3d
   -  Google Play Games  com.google.android.play.games
   -  Settings           com.android.settings

C:\frida-android\tools>
```

Drop hello-app.apk to emulator


LDPlayer(64) 5.0.1
12:00
Search games
System Apps
LD Store
Hello App
The Ants: Underground Kingdom
Crasher: Nirvana
RAID: Shadow legends
Starfall Fantasy: Neverland
Yandex Games
Sky Utopia
Immortal Awakening


LDPlayer(64)
Home
Hello App
12:01
Second Fragment

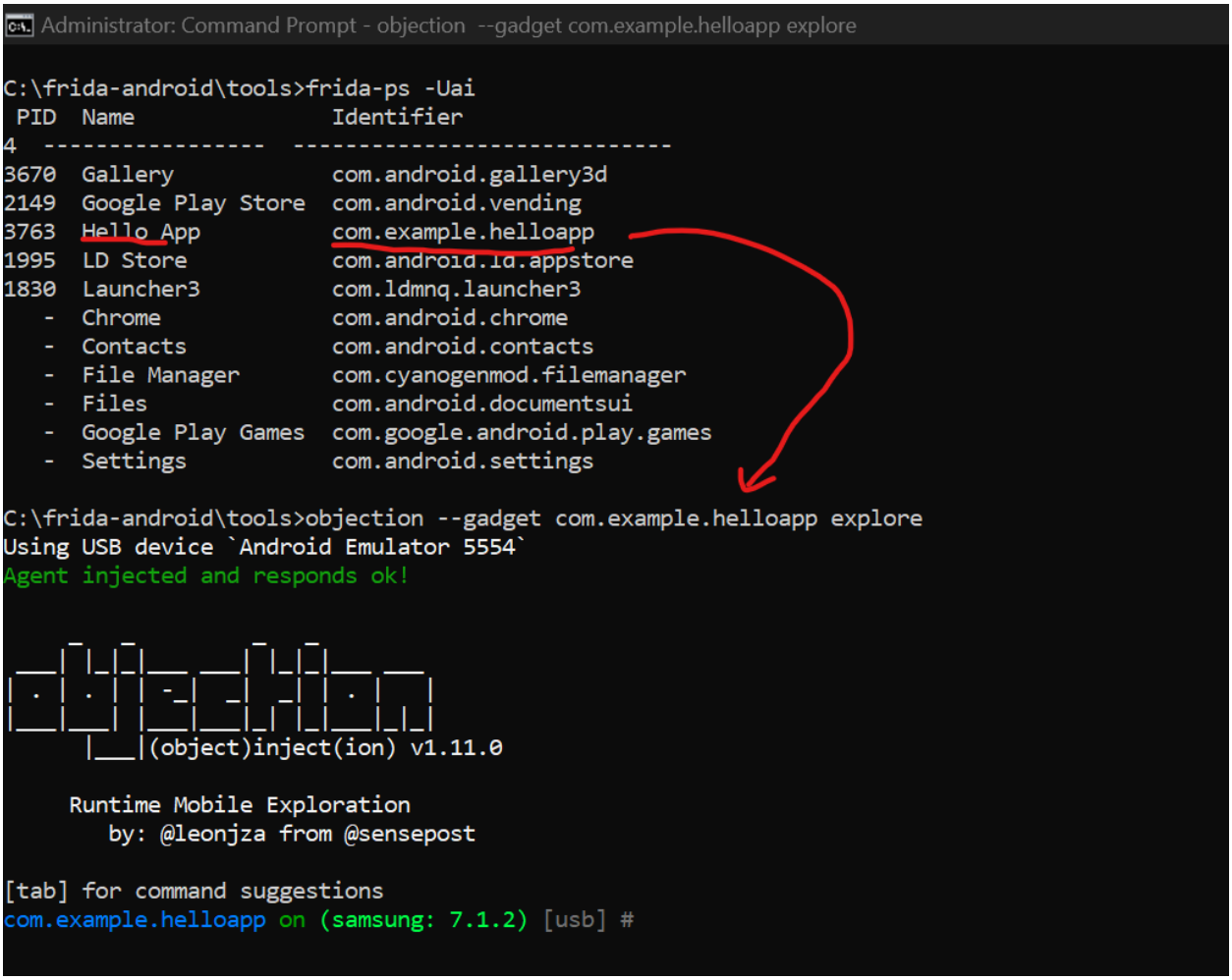
PREVIOUS

```
C:\frida-android\tools>frida-ps -Uai
 PID  Name               Identifier
4  ----------------  --------------------------
2149  Google Play Store  com.android.vending
1995  LD Store           com.android.ld.appstore
1830  Launcher3          com.ldmnq.launcher3
   -  Chrome             com.android.chrome
   -  Contacts           com.android.contacts
   -  File Manager       com.cyanogenmod.filemanager
   -  Files              com.android.documentsui
   -  Gallery            com.android.gallery3d
   -  Google Play Games  com.google.android.play.games
   -  Settings           com.android.settings

C:\frida-android\tools>frida-ps -Uai
 PID  Name               Identifier
4  ----------------  --------------------------
3670  Gallery            com.android.gallery3d
2149  Google Play Store  com.android.vending
3763  Hello App          com.example.helloapp
1995  LD Store           com.android.ld.appstore
1830  Launcher3          com.ldmnq.launcher3
   -  Chrome             com.android.chrome
   -  Contacts           com.android.contacts
   -  File Manager       com.cyanogenmod.filemanager
   -  Files              com.android.documentsui
   -  Google Play Games  com.google.android.play.games
   -  Settings           com.android.settings

C:\frida-android\tools>
```

C:\frida-android\tools>frida -U -n "Hello App"

```
C:\frida-android\tools>frida -U -n "Hello App"
     ____
    / _  |   Frida 16.0.10 - A world-class dynamic instrumentation toolkit
   | (_| |
    > _  |   Commands:
   /_/ |_|       help      -> Displays the help system
   . . . .       object?   -> Display information about 'object'
   . . . .       exit/quit -> Exit
   . . . .
   . . . .   More info at https://frida.re/docs/home/
   . . . .
   . . . .   Connected to Android Emulator 5554 (id=emulator-5554)

[Android Emulator 5554::Hello App ]-> exit

Thank you for using Frida!

C:\frida-android\tools>
```

C:\frida-android\tools>objection --gadget com.example.helloapp explore



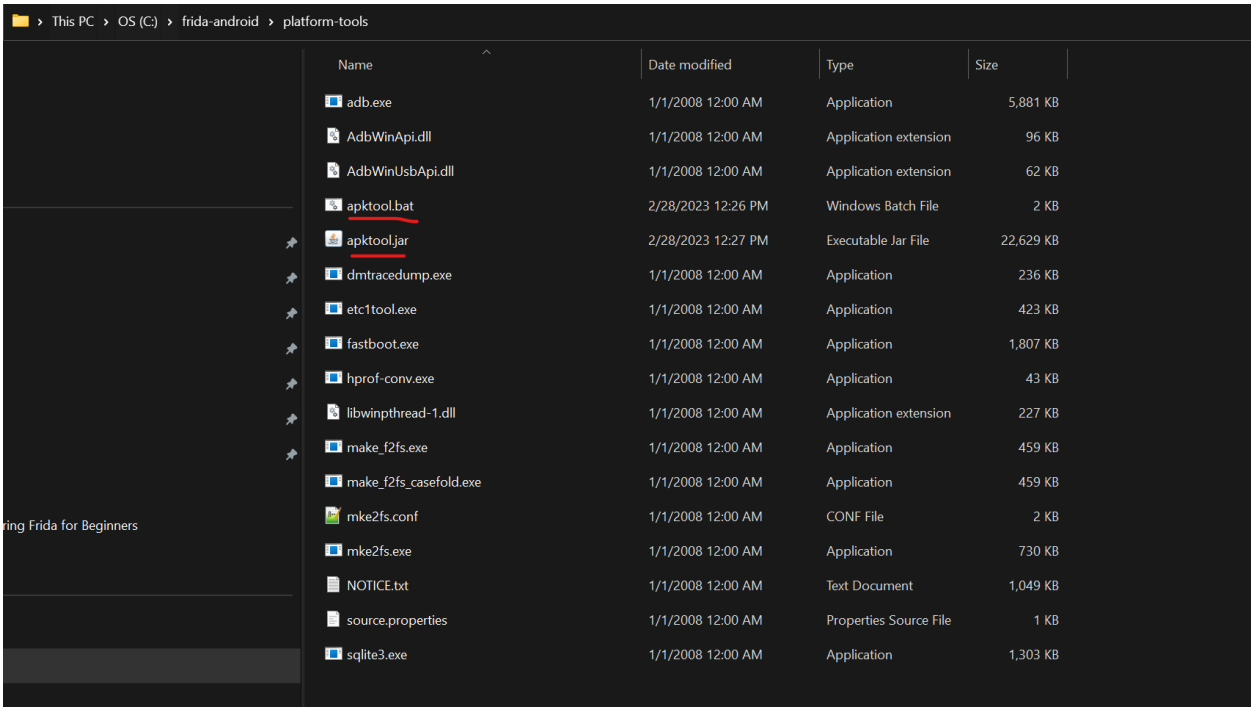
3 Section 3: Setting up lab for non-rooted android phone

3.1 Installing Android studio build-tools

3.2 Installing the apk tool

https://ibotpeaches.github.io/Apktool/install/

Out in platform-tools directory



Check

C:\frida-android\tools>apktool

```
C:\frida-android\tools>apktool
Apktool v2.7.0 - a tool for reengineering Android apk files
with smali v2.5.2-403e9037 and baksmali v2.5.2-403e9037
Copyright 2010 Ryszard Wiśniewski <brut.alll@gmail.com>
Copyright 2010 Connor Tumbleson <connor.tumbleson@gmail.com>

usage: apktool
 -advance,--advanced   prints advance information.
 -version,--version    prints the version then exits
usage: apktool if|install-framework [options] <framework.apk>
 -p,--frame-path <dir>   Stores framework files into <dir>.
 -t,--tag <tag>          Tag frameworks using <tag>.
usage: apktool d[ecode] [options] <file_apk>
 -f,--force              Force delete destination directory.
 -o,--output <dir>       The name of folder that gets written. Default is apk.out
 -p,--frame-path <dir>   Uses framework files located in <dir>.
 -r,--no-res             Do not decode resources.
 -s,--no-src             Do not decode sources.
 -t,--frame-tag <tag>    Uses framework files tagged by <tag>.
usage: apktool b[uild] [options] <app_path>
 -f,--force-all          Skip changes detection and build all files.
 -o,--output <dir>       The name of apk that gets written. Default is dist/name.apk
 -p,--frame-path <dir>   Uses framework files located in <dir>.

For additional info, see: https://ibotpeaches.github.io/Apktool/
For smali/baksmali info, see: https://github.com/JesusFreke/smali

C:\frida-android\tools>
```

3.3 Patching the target apk file with the frida-gadget (frida-server)

Connect with real android phone.

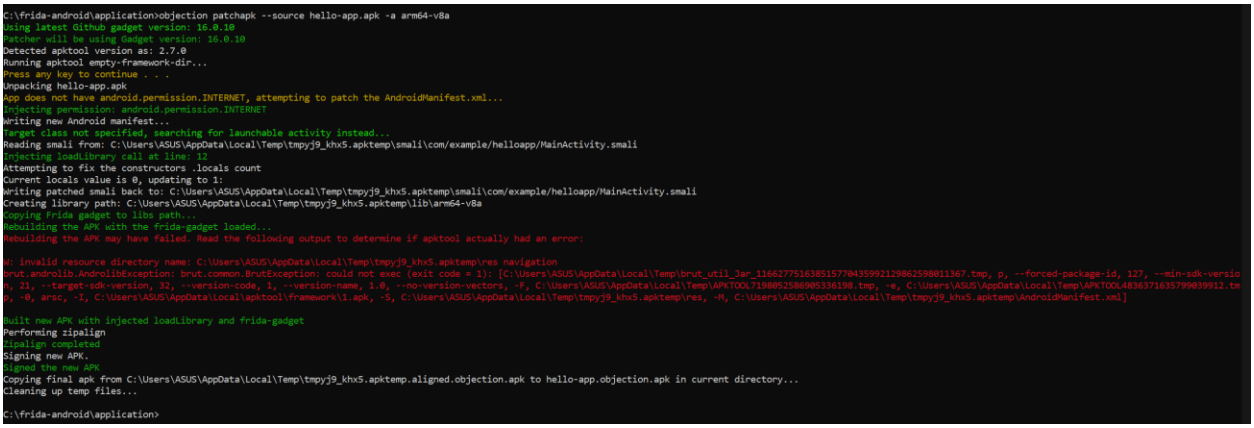
Get architecture

m51:/ # getprop ro.product.cpu.abi

arm64-v8a

```
m51:/ $ getprop ro.product.cpu.abi
arm64-v8a
m51:/ $
```

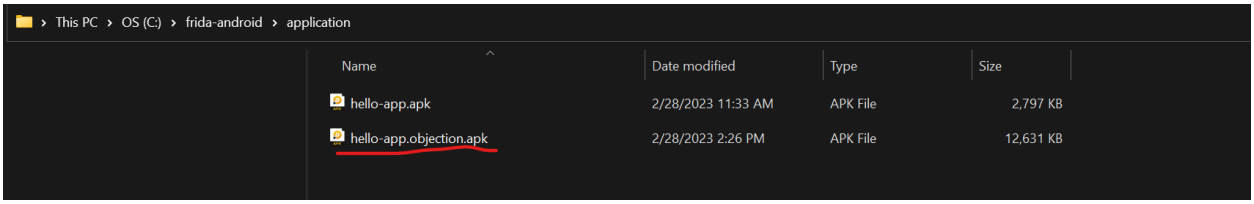
C:\frida-android\application>objection patchapk --source hello-app.apk -a arm64-v8a



Fix error

C:\frida-android\application>objection patchapk --source hello-app.apk -a arm64-v8a --use-aapt2

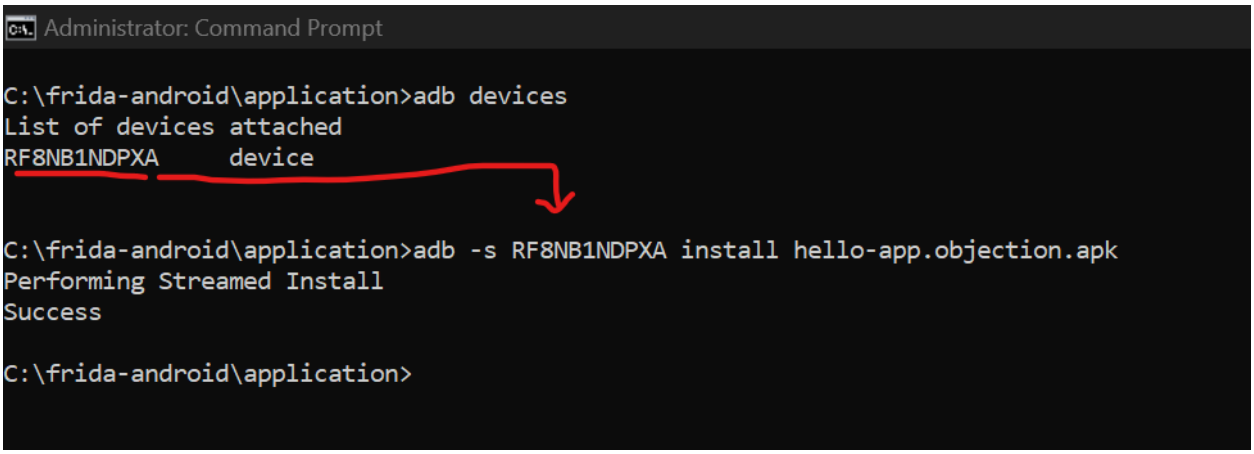
```
C:\frida-android\application>objection patchapk --source hello-app.apk -a arm64-v8a --use-aapt2
Using latest Github gadget version: 16.0.10
Patcher will be using Gadget version: 16.0.10
Detected apktool version as: 2.7.0
Running apktool empty-framework-dir...
I: Removing 1.apk framework file...
Press any key to continue . . .
Unpacking hello-app.apk
App does not have android.permission.INTERNET, attempting to patch the AndroidManifest.xml...
Injecting permission: android.permission.INTERNET
Writing new Android manifest...
Target class not specified, searching for launchable activity instead...
Reading smali from: C:\Users\ASUS\AppData\Local\Temp\tmp3ayor0xq.apktemp\smali\com/example/helloapp/MainActivity.smali
Injecting loadLibrary call at line: 12
Attempting to fix the constructors .locals count
Current locals value is 0, updating to 1:
Writing patched smali back to: C:\Users\ASUS\AppData\Local\Temp\tmp3ayor0xq.apktemp\smali\com/example/helloapp/MainActivity.smali
Creating library path: C:\Users\ASUS\AppData\Local\Temp\tmp3ayor0xq.apktemp\lib\arm64-v8a
Copying Frida gadget to libs path...
Rebuilding the APK with the frida-gadget loaded...
Built new APK with injected loadLibrary and frida-gadget
Performing zipalign
Zipalign completed
Signing new APK...
Signed the new APK
Copying final apk from C:\Users\ASUS\AppData\Local\Temp\tmp3ayor0xq.apktemp.aligned.objection.apk to hello-app.objection.apk in current directory...
Cleaning up temp files...

C:\frida-android\application>
```



3.4 Enabling developer mode on the android phone

3.5 Installing the patched-apk file to the android phone and testing it

C:\frida-android\application>adb -s RF8NB1NDPXA install hello-app.objection.apk



While open app, the app will in “Paused State” so we need perform next step.

C:\frida-android\application>frida-ps -Uai

```
C:\frida-android\application>frida-ps -Uai
  PID  Name                 Identifier
5  -------------------  ------------------------------------
16938  Calendar             com.samsung.android.calendar
13390  Chrome               com.android.chrome
17352  FPT Play             com.fplay.activity
17675  Facebook             com.facebook.katana
17612  Gadget               re.frida.Gadget
26735  Game Launcher        com.samsung.android.game.gamehome
26057  Gmail                com.google.android.gm
 2389  Google               com.google.android.googlequicksearchbox
32291  Google Play Store    com.android.vending
17612  Hello App            com.example.helloapp
13574  Messenger            com.facebook.orca
16622  Samsung Global Goals  com.samsung.sree
27817  Samsung Health       com.sec.android.app.shealth
16467  Samsung Internet     com.sec.android.app.sbrowser
16406  Samsung Notes        com.samsung.android.app.notes
12756  Shopee               com.shopee.vn
13252  Telegram             org.telegram.messenger
 3547  YouTube              com.google.android.youtube
    -  ABC News             android.AbcApplication
    -  APKCombo Installer   com.apkcombo.app
    -  AR Zone              com.samsung.android.arzone
    -  Calculator           com.sec.android.app.popupcalculator
    -  Camera               com.sec.android.app.camera
    -  Clock                com.sec.android.app.clockpackage
    -  Contacts             com.samsung.android.app.contacts
    -  Discord              com.discord
    -  Drive                com.google.android.apps.docs
```

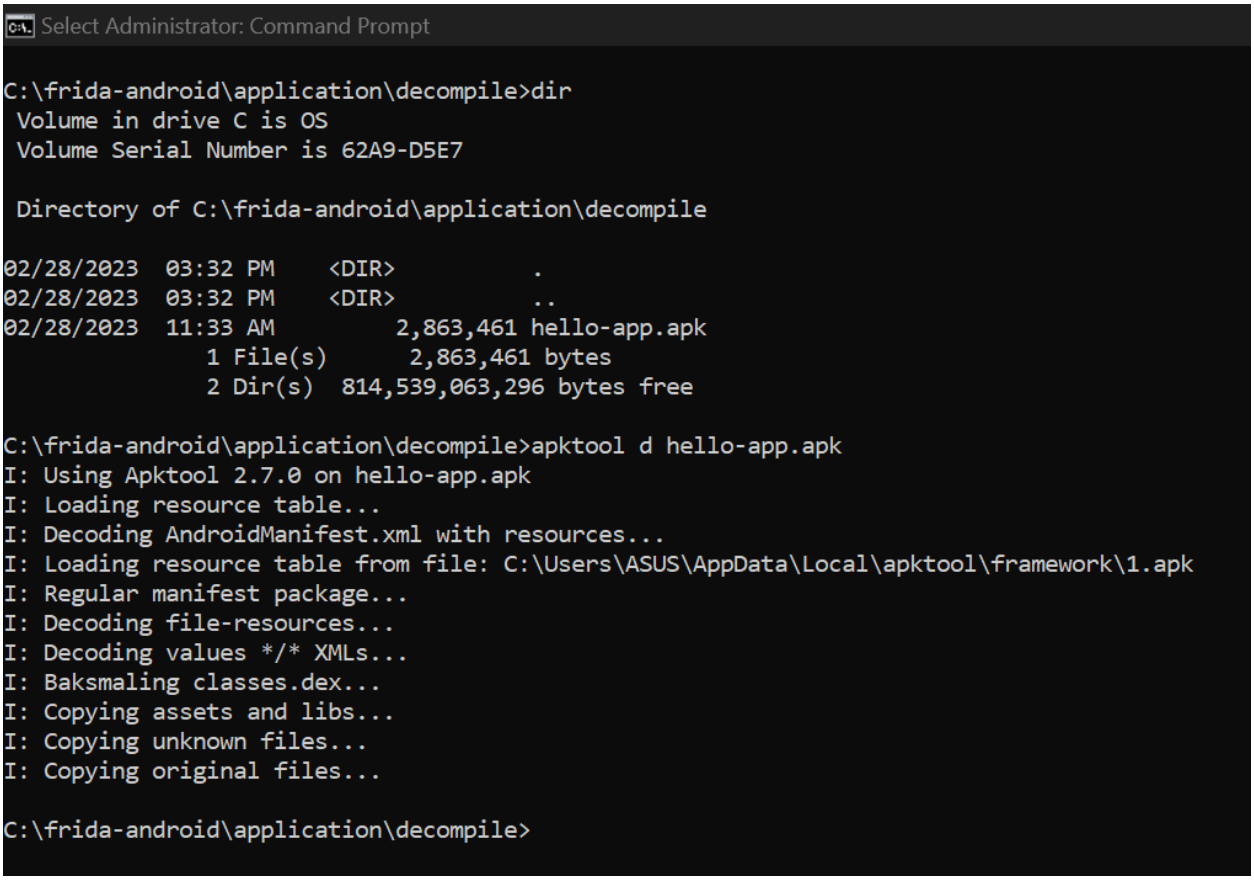
C:\frida-android\application>frida -U -n Gadget

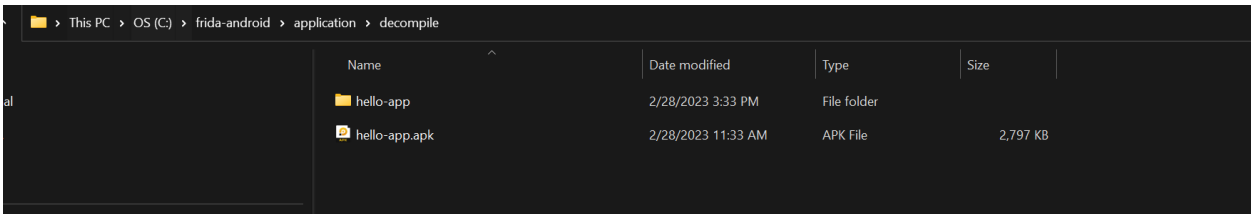
```
C:\frida-android\application>frida -U -n Gadget
     ____
    / _  |   Frida 16.0.10 - A world-class dynamic instrumentation toolkit
   | (_| |
    > _  |   Commands:
   /_/ |_|       help      -> Displays the help system
   . . . .       object?   -> Display information about 'object'
   . . . .       exit/quit -> Exit
   . . . .
   . . . .   More info at https://frida.re/docs/home/
   . . . .
   . . . .   Connected to SM M515F (id=RF8NB1NDPXA)

[SM M515F::Gadget ]->
```

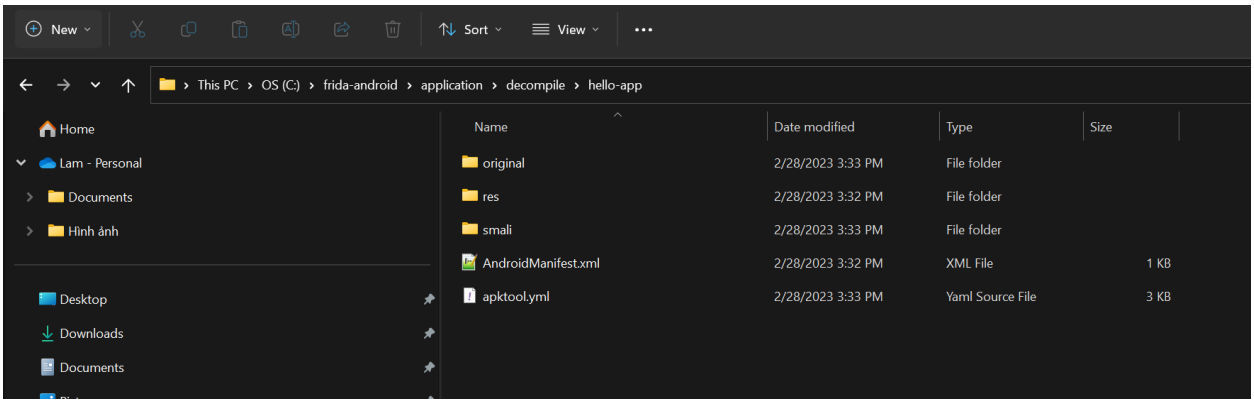
4 Section 4: Decompiling apk files

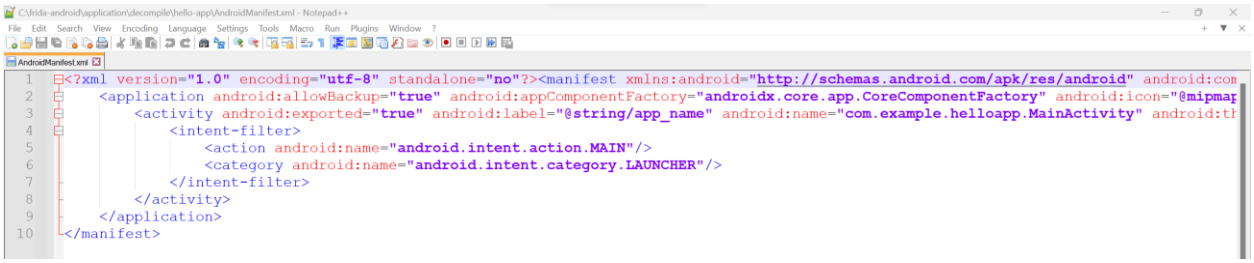
4.1 Reverse engineering using the apktool

C:\frida-android\application\decompile>apktool d hello-app.apk



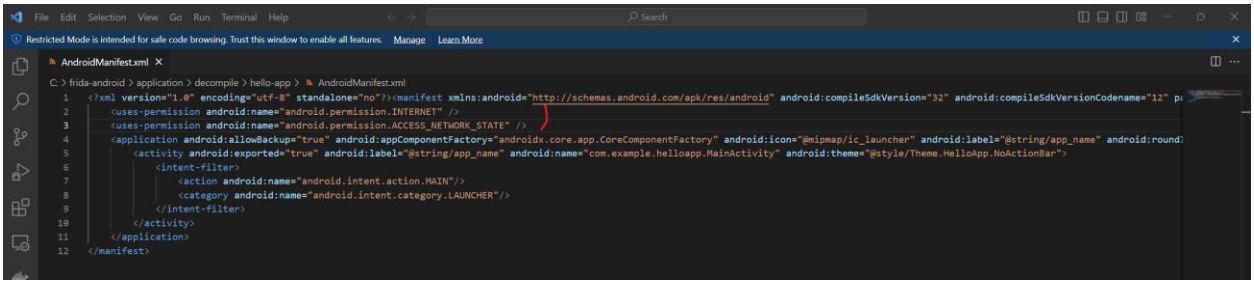






```
<?xml version="1.0" encoding="utf-8" standalone="no"?><manifest xmlns:android="http://schemas.android.com/apk/res/android" android:com
    <application android:allowBackup="true" android:appComponentFactory="androidx.core.app.CoreComponentFactory" android:icon="@mipmap
        <activity android:exported="true" android:label="@string/app_name" android:name="com.example.helloapp.MainActivity" android:th
            <intent-filter>
                <action android:name="android.intent.action.MAIN"/>
                <category android:name="android.intent.category.LAUNCHER"/>
            </intent-filter>
        </activity>
    </application>
</manifest>
```

Add two permissions



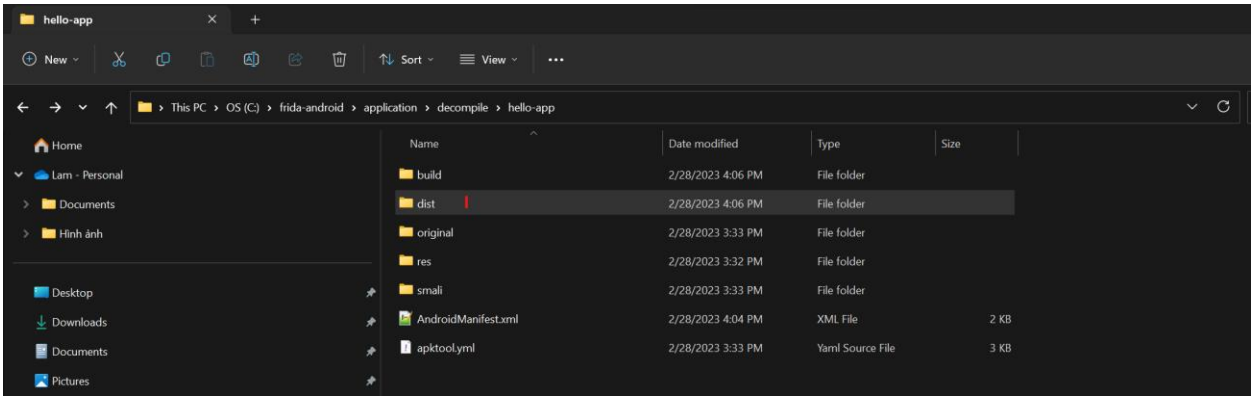
```
<?xml version="1.0" encoding="utf-8" standalone="no"?><manifest xmlns:android="http://schemas.android.com/apk/res/android" android:compileSdkVersion="32" android:compileSdkVersionCodename="12" p
    <uses-permission android:name="android.permission.INTERNET" />
    <uses-permission android:name="android.permission.ACCESS_NETWORK_STATE" />
    <application android:allowBackup="true" android:appComponentFactory="androidx.core.app.CoreComponentFactory" android:icon="@mipmap/ic_launcher" android:label="@string/app_name" android:round
        <activity android:exported="true" android:label="@string/app_name" android:name="com.example.helloapp.MainActivity" android:theme="@style/Theme.HelloApp.NoActionBar">
            <intent-filter>
                <action android:name="android.intent.action.MAIN"/>
                <category android:name="android.intent.category.LAUNCHER"/>
            </intent-filter>
        </activity>
    </application>
</manifest>
```

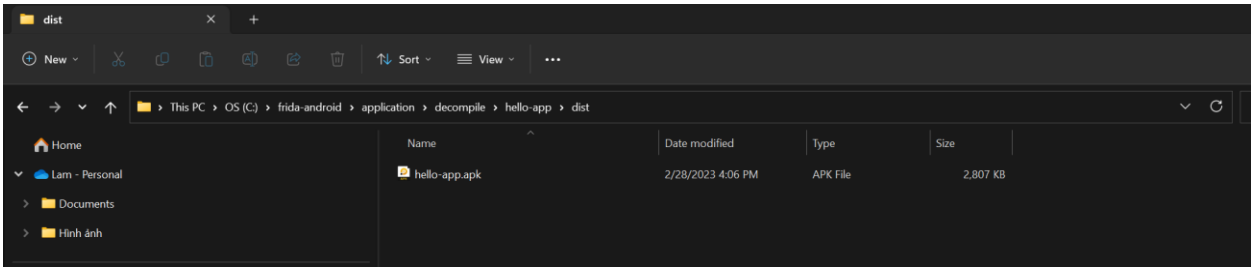
Re-compile

C:\frida-android\application\decompile>apktool b hello-app --use-aapt2

```
 Directory of C:\frida-android\application\decompile

02/28/2023  04:06 PM    <DIR>          .
02/28/2023  03:32 PM    <DIR>          ..
02/28/2023  03:33 PM    <DIR>          hello-app
               0 File(s)              0 bytes
               3 Dir(s)  814,449,254,400 bytes free

C:\frida-android\application\decompile>apktool b hello-app --use-aapt2
I: Using Apktool 2.7.0
I: Checking whether sources has changed...
I: Smaling smali folder into classes.dex...
I: Checking whether resources has changed...
I: Building resources...
I: Building apk file...
I: Copying unknown files/dir...
I: Built apk into: hello-app\dist\hello-app.apk

C:\frida-android\application\decompile>
```

New “dist” directory contains hello-app.apk



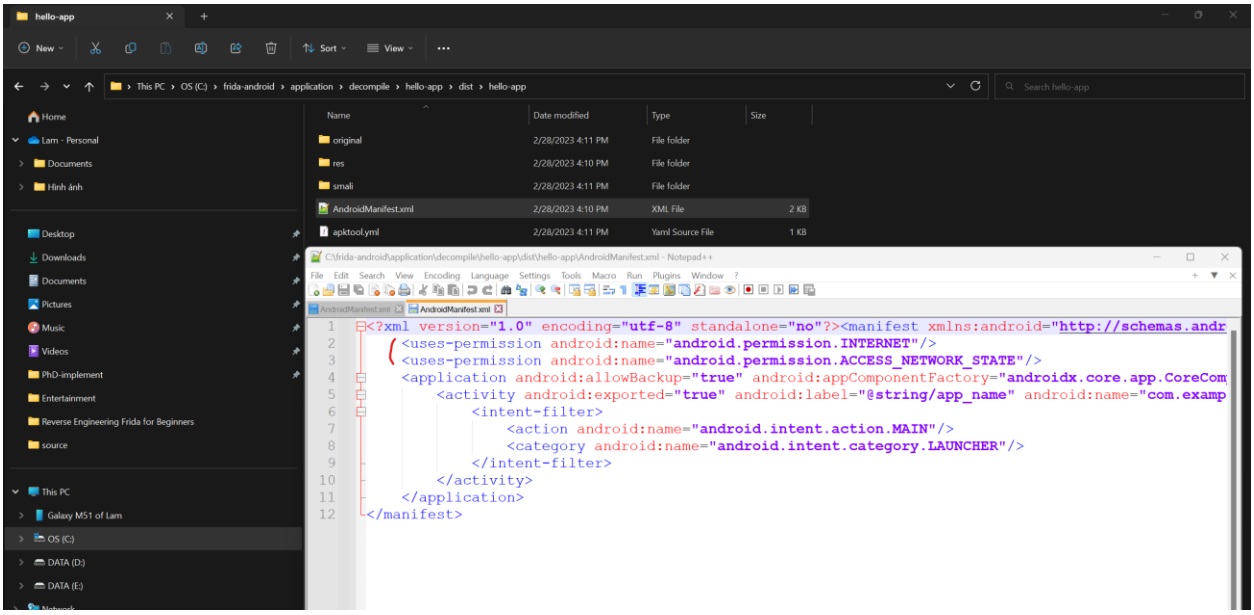


Decompiling for testing

```
C:\frida-android\application\decompile>cd hello-app

C:\frida-android\application\decompile\hello-app>cd dist

C:\frida-android\application\decompile\hello-app\dist>dir
 Volume in drive C is OS
 Volume Serial Number is 62A9-D5E7

 Directory of C:\frida-android\application\decompile\hello-app\dist

02/28/2023  04:06 PM    <DIR>          .
02/28/2023  04:06 PM    <DIR>          ..
02/28/2023  04:06 PM         2,873,925 hello-app.apk
               1 File(s)      2,873,925 bytes
               2 Dir(s)  814,449,537,024 bytes free

C:\frida-android\application\decompile\hello-app\dist>
```

```
C:\frida-android\application\decompile\hello-app\dist>apktool d hello-app.apk
I: Using Apktool 2.7.0 on hello-app.apk
I: Loading resource table...
I: Decoding AndroidManifest.xml with resources...
I: Loading resource table from file: C:\Users\ASUS\AppData\Local\apktool\framework\1.apk
I: Regular manifest package...
I: Decoding file-resources...
I: Decoding values */* XMLs...
I: Baksmaling classes.dex...
I: Copying assets and libs...
I: Copying unknown files...
I: Copying original files...

C:\frida-android\application\decompile\hello-app\dist>
```

We have two added permission



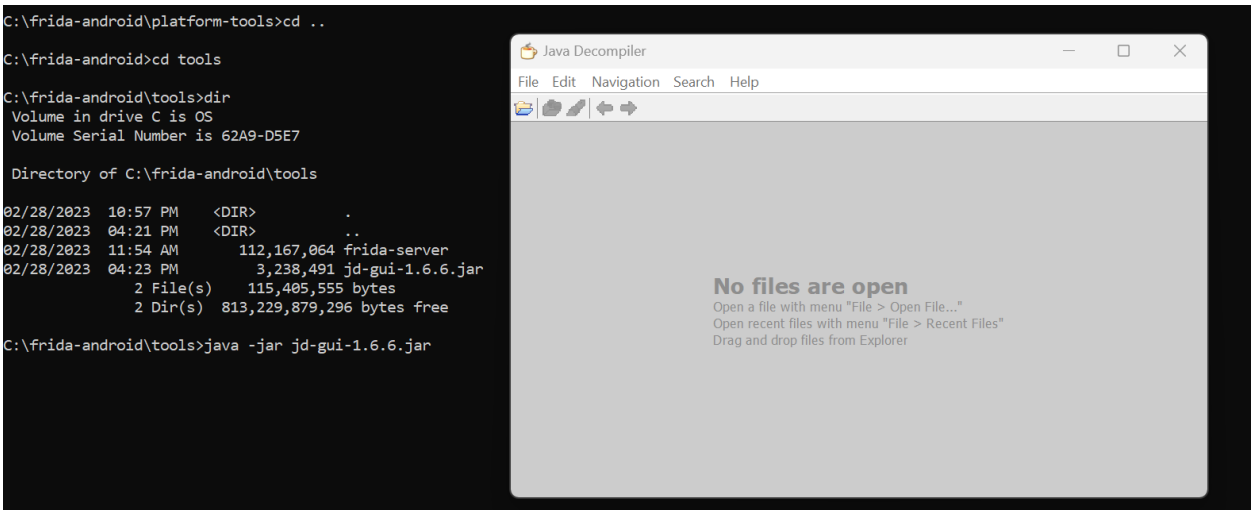
4.2 Installing dex2jar and jd-gui

```
Administrator: Command Prompt
(c) Microsoft Corporation. All rights reserved.

C:\Windows\System32>d2j-dex2jar
d2j-dex2jar -- convert dex to jar
usage: d2j-dex2jar [options] <file0> [file1 ... fileN]
options:
 --skip-exceptions            skip-exceptions
 -d,--debug-info              translate debug info
 -e,--exception-file <file>   detail exception file, default is $current_dir/[fi
                              le-name]-error.zip
 -f,--force                   force overwrite
 -h,--help                    Print this help message
 -n,--not-handle-exception    not handle any exceptions thrown by dex2jar
 -nc,--no-code
 -o,--output <out-jar-file>   output .jar file, default is $current_dir/[file-na
                              me]-dex2jar.jar
 -os,--optmize-synchronized   optimize-synchronized
 -p,--print-ir                print ir to System.out
 -r,--reuse-reg               reuse register while generate java .class file
 -s                           same with --topological-sort/-ts
 -ts,--topological-sort       sort block by topological, that will generate more
                               readable code, default enabled
version: reader-2.1, translator-2.1, ir-2.1

C:\Windows\System32>
```

```
C:\frida-android>cd tools

C:\frida-android\tools>dir
 Volume in drive C is OS
 Volume Serial Number is 62A9-D5E7

 Directory of C:\frida-android\tools

02/28/2023  10:57 PM    <DIR>          .
02/28/2023  04:21 PM    <DIR>          ..
02/28/2023  11:54 AM       112,167,064 frida-server
02/28/2023  04:23 PM         3,238,491 jd-gui-1.6.6.jar
               2 File(s)    115,405,555 bytes
               2 Dir(s)  813,229,879,296 bytes free

C:\frida-android\tools>
```

Run

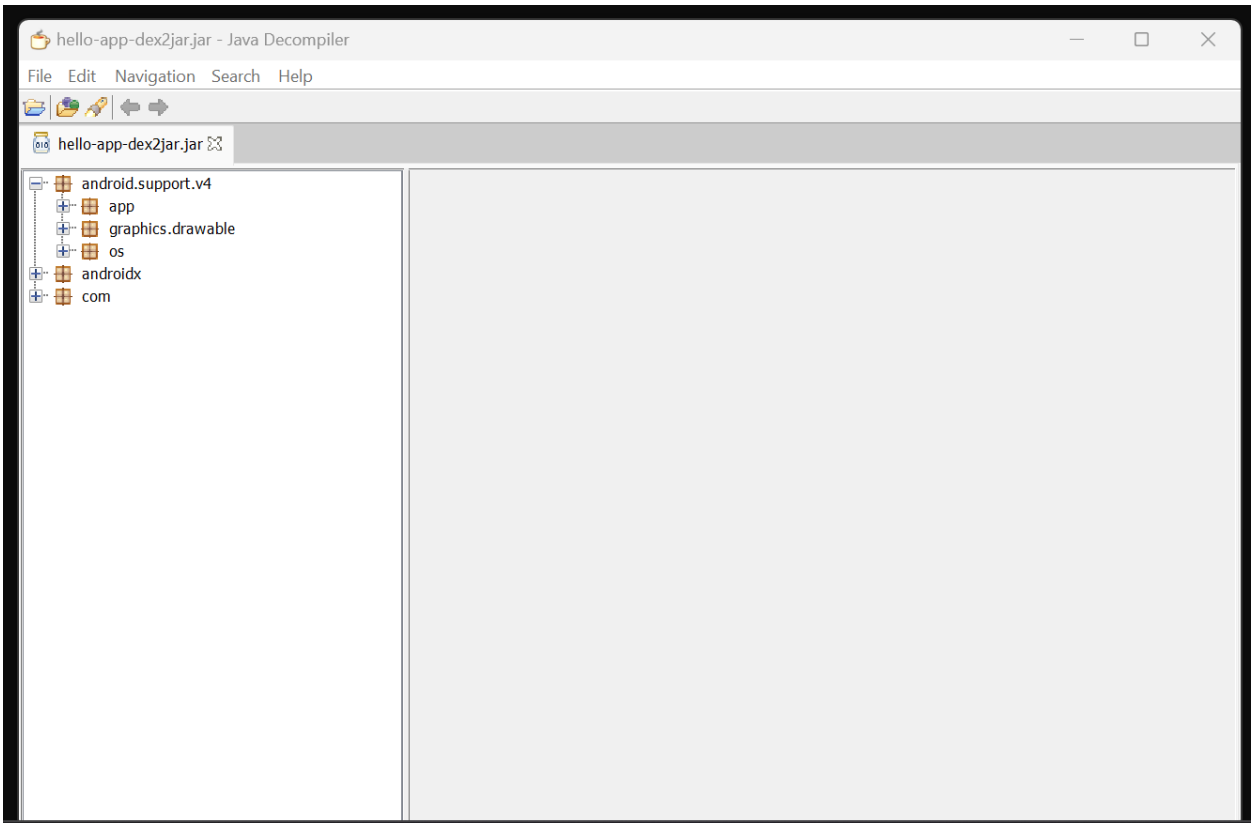
C:\frida-android\tools>java -jar jd-gui-1.6.6.jar

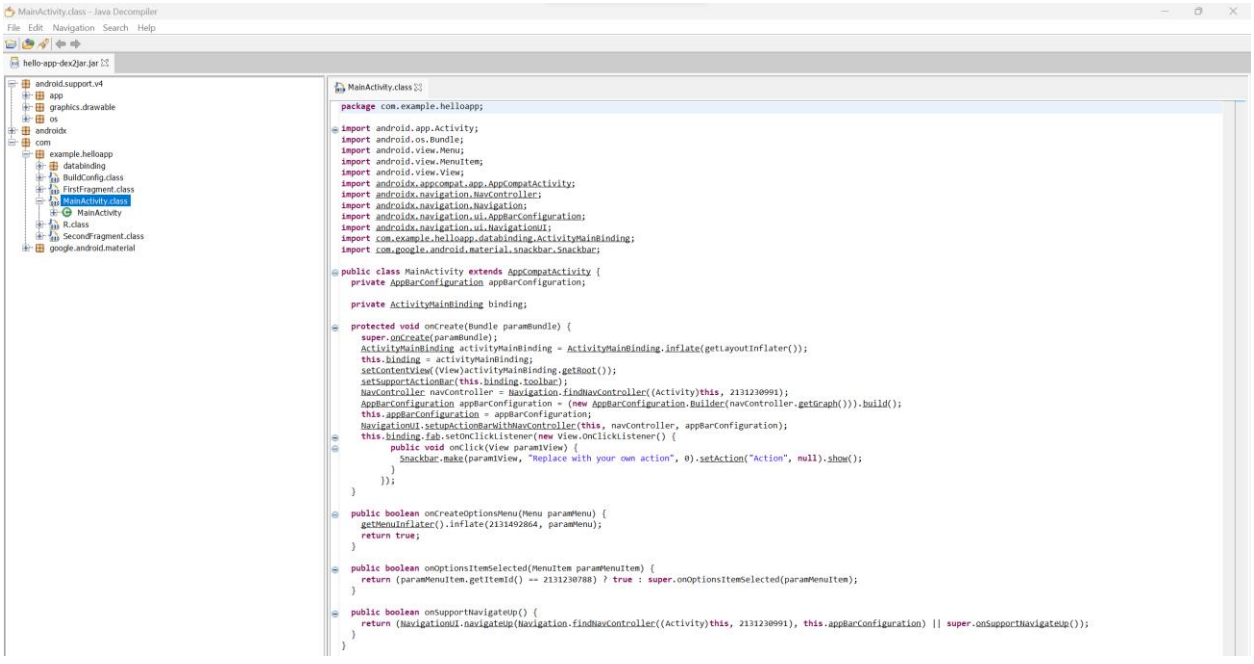


4.3 Decompling an apk file using dex2jar and jd-gui

C:\frida-android\application>d2j-dex2jar hello-app.apk

```
C:\frida-android>cd application

C:\frida-android\application>dir
 Volume in drive C is OS
 Volume Serial Number is 62A9-D5E7

 Directory of C:\frida-android\application

02/28/2023  03:32 PM    <DIR>          .
02/28/2023  04:21 PM    <DIR>          ..
02/28/2023  04:06 PM    <DIR>          decompile
02/28/2023  11:33 AM         2,863,461 hello-app.apk
02/28/2023  02:26 PM        12,933,711 hello-app.objection.apk
               2 File(s)     15,797,172 bytes
               3 Dir(s)  813,248,188,416 bytes free

C:\frida-android\application>d2j-dex2jar hello-app.apk
dex2jar hello-app.apk -> .\hello-app-dex2jar.jar

C:\frida-android\application>
```


hello-app-dex2jar.jar - Java Decompiler
File Edit Navigation Search Help
hello-app-dex2jar.jar
android.support.v4
app
graphics.drawable
os
androidx
com


MainActivity.class - Java Decompiler
File Edit Navigation Search Help
hello-app-dex2jar.jar
android.support.v4
app
graphics.drawable
os
androidx
com
example.helloapp
databinding
BuildConfig.class
FirstFragment.class
MainActivity.class
MainActivity
R.class
SecondFragment.class
google.android.material
MainActivity.class
package com.example.helloapp;
import android.app.Activity;
import android.os.Bundle;
import android.view.Menu;
import android.view.MenuItem;
import android.view.View;
import androidx.appcompat.app.AppCompatActivity;
import androidx.navigation.NavController;
import androidx.navigation.Navigation;
import androidx.navigation.ui.AppBarConfiguration;
import androidx.navigation.ui.NavigationUI;
import com.example.helloapp.databinding.ActivityMainBinding;
import com.google.android.material.snackbar.Snackbar;
public class MainActivity extends AppCompatActivity {
private AppBarConfiguration appBarConfiguration;
private ActivityMainBinding binding;
protected void onCreate(Bundle paramBundle) {
super.onCreate(paramBundle);
ActivityMainBinding activityMainBinding = ActivityMainBinding.inflate(getLayoutInflater());
this.binding = activityMainBinding;
setContentView((View)activityMainBinding.getRoot());
setSupportActionBar(this.binding.toolbar);
NavController navController = Navigation.findNavController((Activity)this, 2131230991);
AppBarConfiguration appBarConfiguration = (new AppBarConfiguration.Builder(navController.getGraph())).build();
this.appBarConfiguration = appBarConfiguration;
NavigationUI.setupActionBarWithNavController(this, navController, appBarConfiguration);
this.binding.fab.setOnClickListener(new View.OnClickListener() {
public void onClick(View param1View) {
Snackbar.make(param1View, "Replace with your own action", 0).setAction("Action", null).show();
}
});
}
public boolean onCreateOptionsMenu(Menu paramMenu) {
getMenuInflater().inflate(2131492864, paramMenu);
return true;
}
public boolean onOptionsItemSelected(MenuItem paramMenuItem) {
return (paramMenuItem.getItemId() == 2131230788) ? true : super.onOptionsItemSelected(paramMenuItem);
}
public boolean onSupportNavigateUp() {
return (NavigationUI.navigateUp(Navigation.findNavController((Activity)this, 2131230991), this.appBarConfiguration) || super.onSupportNavigateUp());
}
}

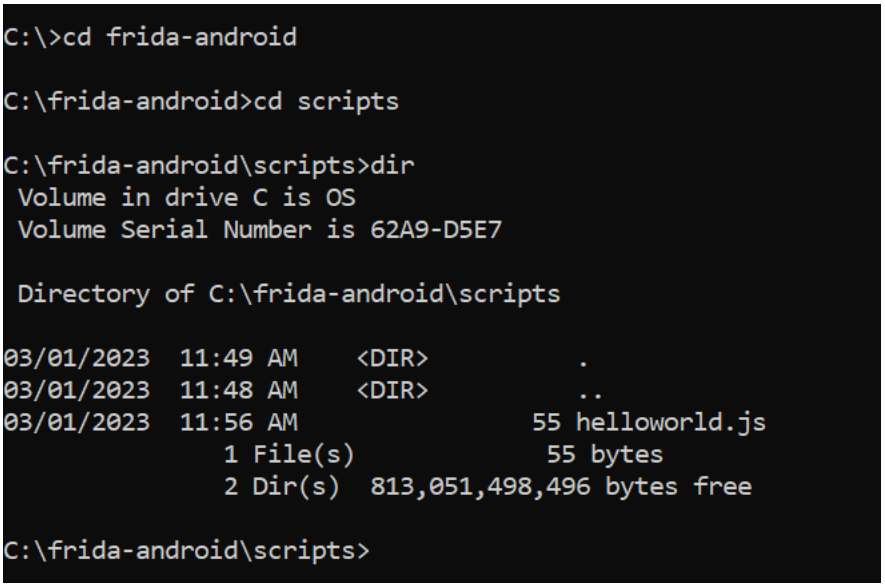
5 Section 5: Understanding the Frida CLI

Link: https://frida.re/docs/javascript-api/#java

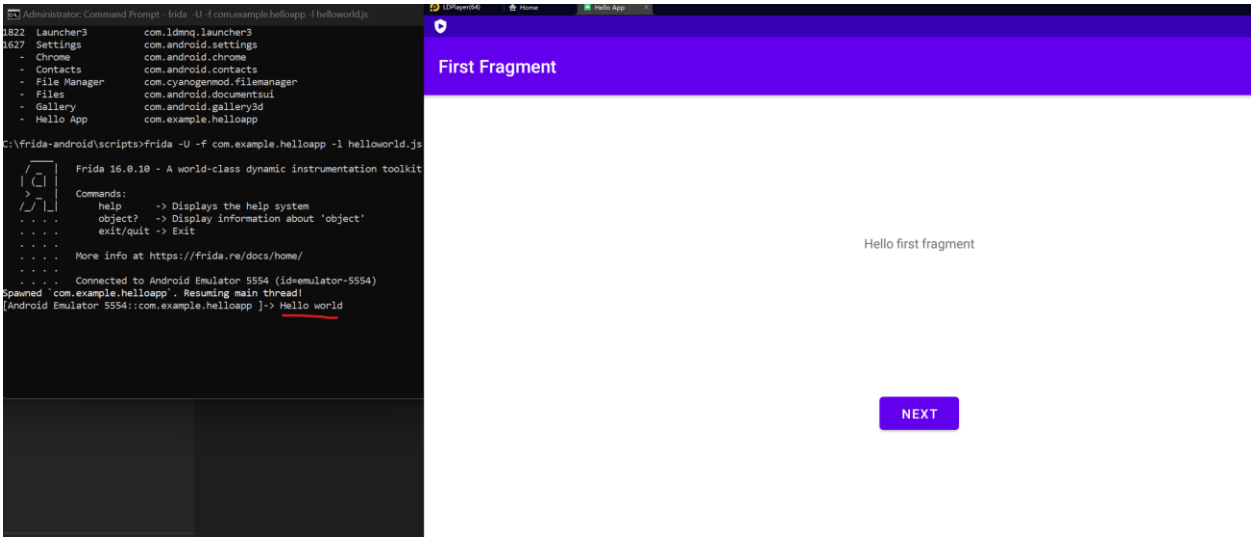
6 Section 6: Simple Frida hello-world script

Link: https://frida.re/docs/javascript-api/#java

```
Java.perform(()=>{
    console.log("Hello world")
});
```

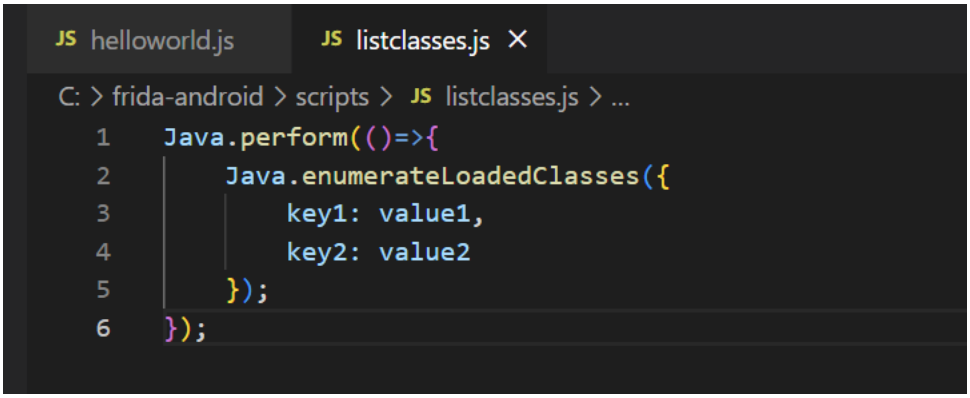


C:\frida-android\scripts>frida -U -f com.example.helloapp -l helloworld.js



7 Section 7: Frida scripts to list classes

7.1 Template




```
Java.perform(()=>{
    Java.enumerateLoadedClasses({
        key1: value1,
        key2: value2
    });
});
```

7.2 Implement

helloworld.js | listclasses.js

C: > frida-android > scripts > listclasses.js > ...

```
1   Java.perform(()=>{
2       Java.enumerateLoadedClasses({
3           onMatch: function(name,handle){
4
5           },
6           key2: value2
7       });
8   });
```

helloworld.js | listclasses.js

C: > frida-android > scripts > listclasses.js > ...

```
1   Java.perform(()=>{
2       Java.enumerateLoadedClasses({
3           onMatch: function(name,handle){
4                   console.log(name)
5           },
6           onComplete: function(){
7                   console.log("---DONE---")
8           },
9       });
10  });
```

7.3 Run

C:\frida-android\scripts>frida -U -f com.example.helloapp -l listclasses.js

```
C:\frida-android\scripts>frida -U -f com.example.helloapp -l listclasses.js
     ____
    / _  |   Frida 16.0.10 - A world-class dynamic instrumentation toolkit
   | (_| |
    > _  |   Commands:
   /_/ |_|       help      -> Displays the help system
   . . . .     object?   -> Display information about 'object'
   . . . .     exit/quit -> Exit
   . . . .
   . . . .   More info at https://frida.re/docs/home/
   . . . .
   . . . .   Connected to Android Emulator 5554 (id=emulator-5554)
Spawned `com.example.helloapp`. Resuming main thread!
[Android Emulator 5554::com.example.helloapp ]-> org.apache.http.HttpEntityEnclosingRequest
org.apache.http.ProtocolVersion
org.apache.http.HttpResponse
org.apache.http.impl.cookie.DateParseException
org.apache.http.HeaderIterator
org.apache.http.message.AbstractHttpMessage
org.apache.http.HttpHost
org.apache.http.params.AbstractHttpParams
org.apache.http.message.BasicHeader
org.apache.http.StatusLine
org.apache.http.client.methods.HttpUriRequest
org.apache.http.conn.ClientConnectionManager
org.apache.http.HttpEntity
org.apache.http.Header
```

```
android.media.MediaDrm$ProvisionRequest
android.hardware.camera2.params.MeteringRectangle
android.hardware.camera2.CameraCharacteristics$5
[Landroid.hardware.camera2.marshal.MarshalQueryable;
android.hardware.camera2.impl.CameraMetadataNative$7
android.hardware.camera2.impl.GetCommand
android.os.GraphicsEnvironment
android.hardware.camera2.impl.CameraMetadataNative$8
android.app.ProfilerInfo
libcore.reflect.WildcardTypeImpl
---DONE---
[Android Emulator 5554::com.example.helloapp ]->

Thank you for using Frida!

C:\frida-android\scripts>
```

7.4 Filter

```
Java.perform(()=>{
    Java.enumerateLoadedClasses({
        onMatch: function(name,handle){
            if(name.includes("com.example.helloapp")){
                console.log(name);
            }
        },
        onComplete: function(){
                console.log("---DONE---")
        },
    });
});
```

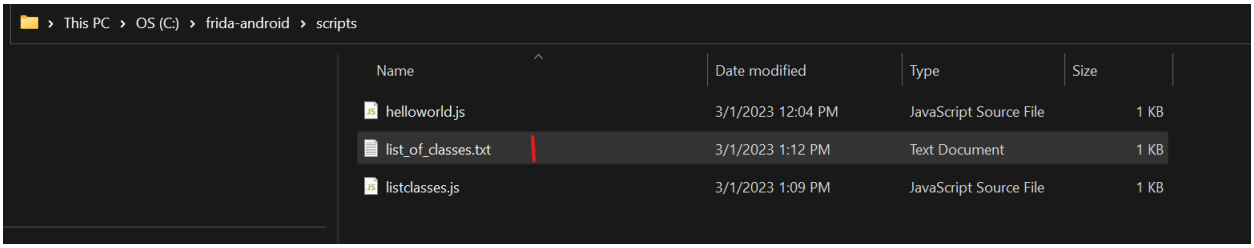
helloworld.js listclasses.js

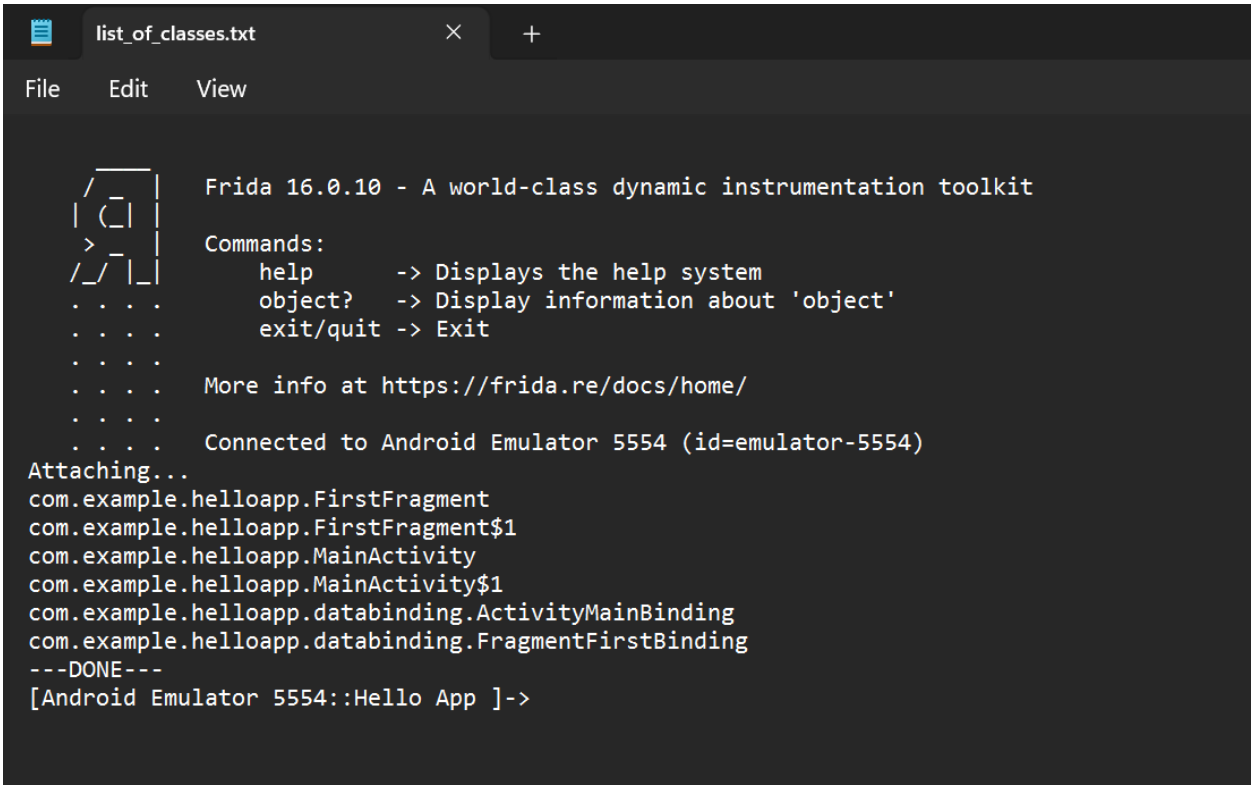
C: > frida-android > scripts > listclasses.js > ...

```
Java.perform(()=>{
    Java.enumerateLoadedClasses({
        onMatch: function(name,handle){
            if(name.includes("com.example.helloapp")){
                console.log(name);
            }
        },
        onComplete: function(){
                console.log("---DONE---")
        },
    });
});
```

```
C:\frida-android\scripts>frida -U -f com.example.helloapp -l listclasses.js
     ____
    / _  |   Frida 16.0.10 - A world-class dynamic instrumentation toolkit
   | (_| |
    > _  |   Commands:
   /_/ |_|       help      -> Displays the help system
   . . . .       object?   -> Display information about 'object'
   . . . .       exit/quit -> Exit
   . . . .
   . . . .   More info at https://frida.re/docs/home/
   . . . .
   . . . .   Connected to Android Emulator 5554 (id=emulator-5554)
Spawned `com.example.helloapp`. Resuming main thread!
[Android Emulator 5554::com.example.helloapp ]-> ---DONE---
com.example.helloapp.FirstFragment
com.example.helloapp.FirstFragment$1
com.example.helloapp.MainActivity
com.example.helloapp.MainActivity$1
com.example.helloapp.databinding.ActivityMainBinding
com.example.helloapp.databinding.FragmentFirstBinding
---DONE---
com.example.helloapp.FirstFragment
com.example.helloapp.FirstFragment$1
com.example.helloapp.MainActivity
com.example.helloapp.MainActivity$1
com.example.helloapp.databinding.ActivityMainBinding
com.example.helloapp.databinding.FragmentFirstBinding
---DONE---
```

C:\frida-android\scripts>frida -U -n "Hello App" -l listclasses.js > list_of_classes.txt

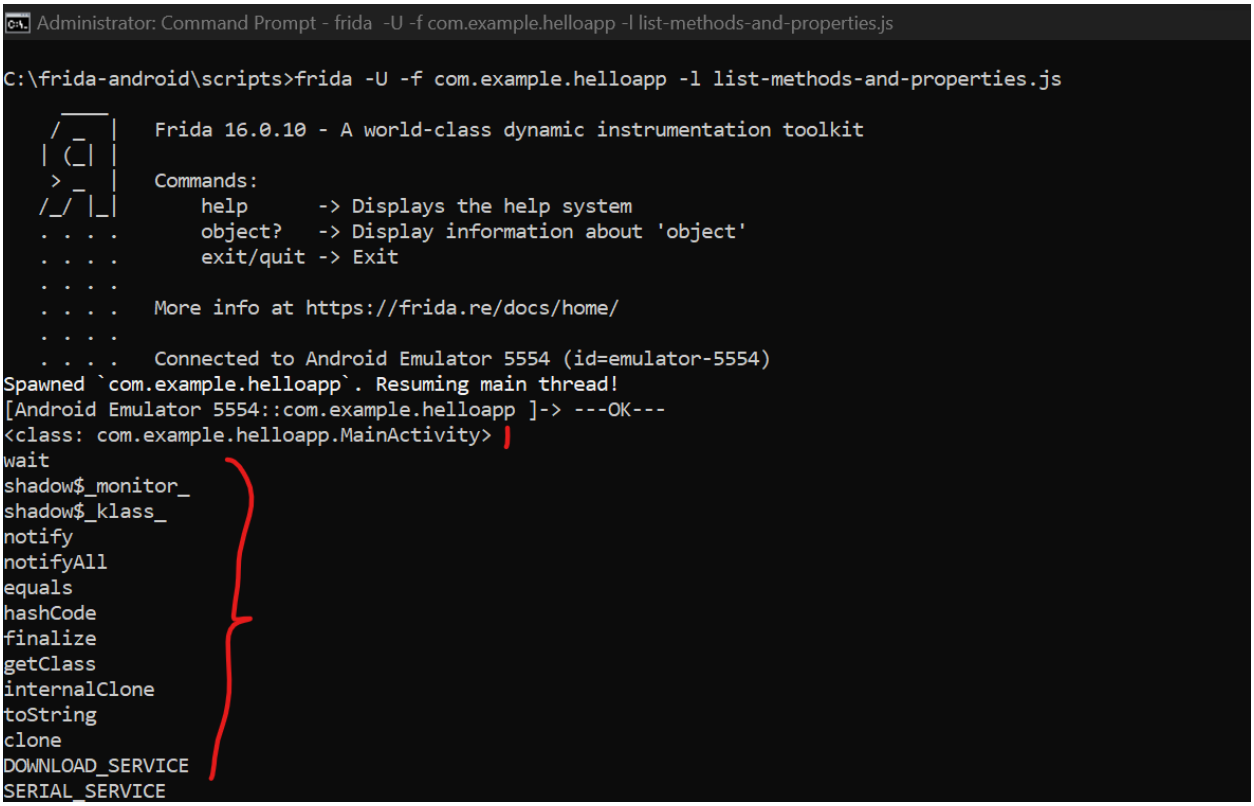


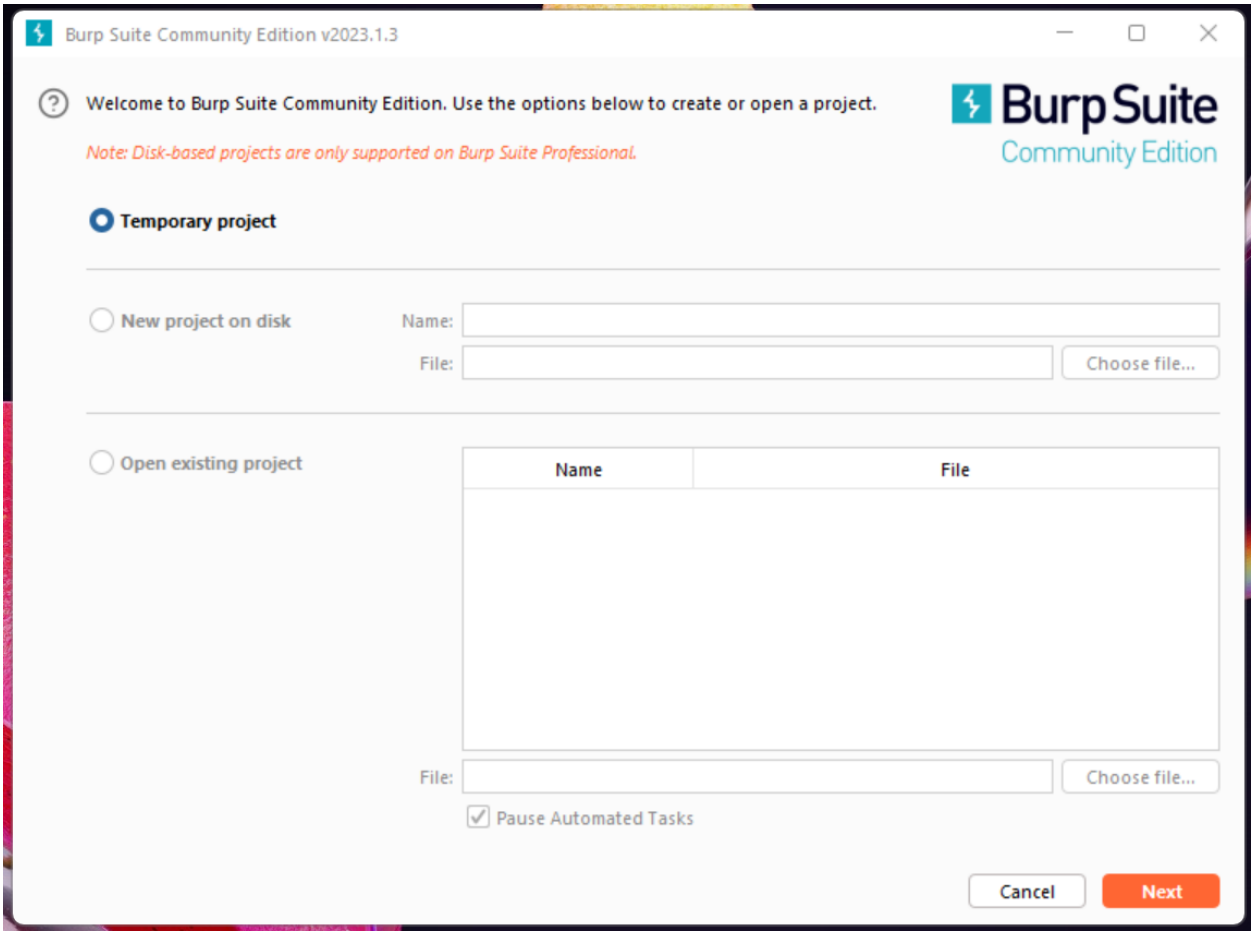


8 Section 8: Frida script to list method and properties

```
Java.perform(()=>{
    console.log("---OK---")
    const activityclass = Java.use("com.example.helloapp.MainActivity");
    console.log(activityclass)
    console.log(Object.getOwnPropertyNames(activityclass).join("\n"))
});
```

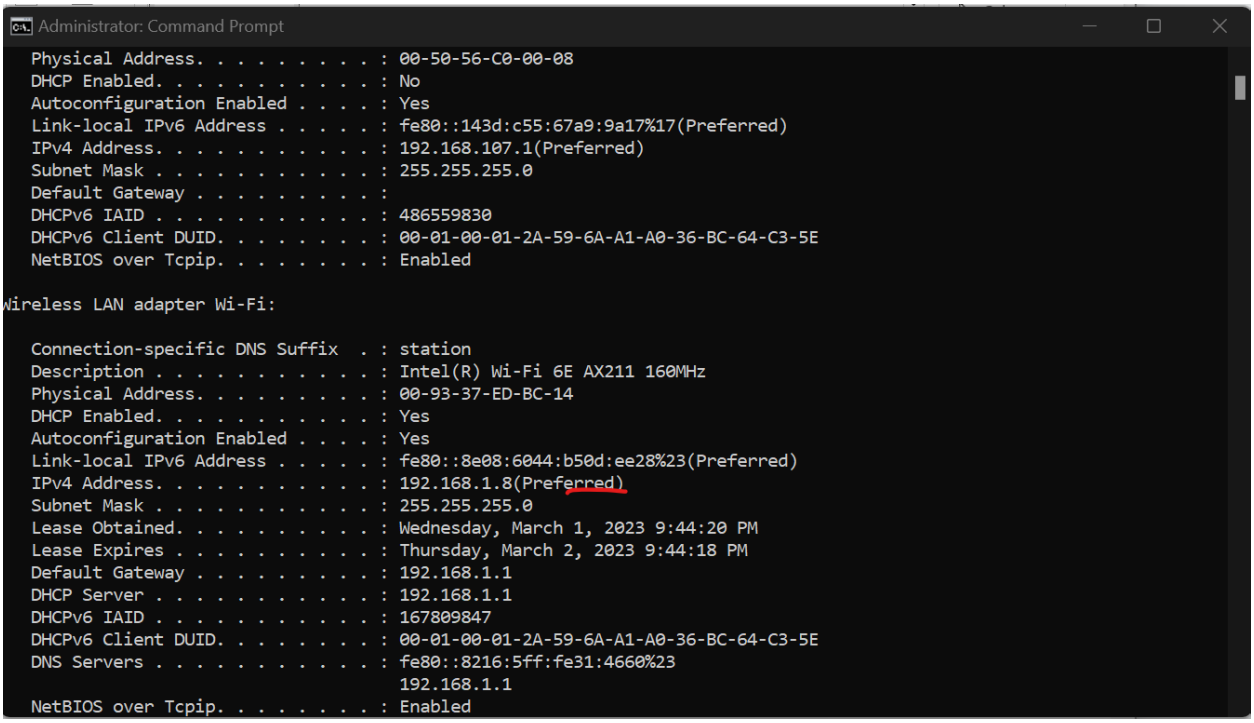
C:\frida-android\scripts>frida -U -f com.example.helloapp -l list-methods-and-properties.js


Administrator: Command Prompt - frida -U -f com.example.helloapp -l list-methods-and-properties.js
C:\frida-android\scripts>frida -U -f com.example.helloapp -l list-methods-and-properties.js
Frida 16.0.10 - A world-class dynamic instrumentation toolkit
Commands:
help -> Displays the help system
object? -> Display information about 'object'
exit/quit -> Exit
More info at https://frida.re/docs/home/
Connected to Android Emulator 5554 (id=emulator-5554)
Spawned `com.example.helloapp`. Resuming main thread!
[Android Emulator 5554::com.example.helloapp]-> ---OK---
<class: com.example.helloapp.MainActivity>
wait
shadow$_monitor_
shadow$_klass_
notify
notifyAll
equals
hashCode
finalize
getClass
internalClone
toString
clone
DOWNLOAD_SERVICE
SERIAL_SERVICE


Burp Suite Community Edition v2023.1.3
Welcome to Burp Suite Community Edition. Use the options below to create or open a project.
Note: Disk-based projects are only supported on Burp Suite Professional.
Burp Suite
Community Edition
Temporary project
New project on disk
Name:
File:
Choose file...
Open existing project
Name
File
File:
Choose file...
Pause Automated Tasks
Cancel
Next

19.2 Setting Burpsuite proxy for LDplayer emulator

19.2.1 Check IP laptop

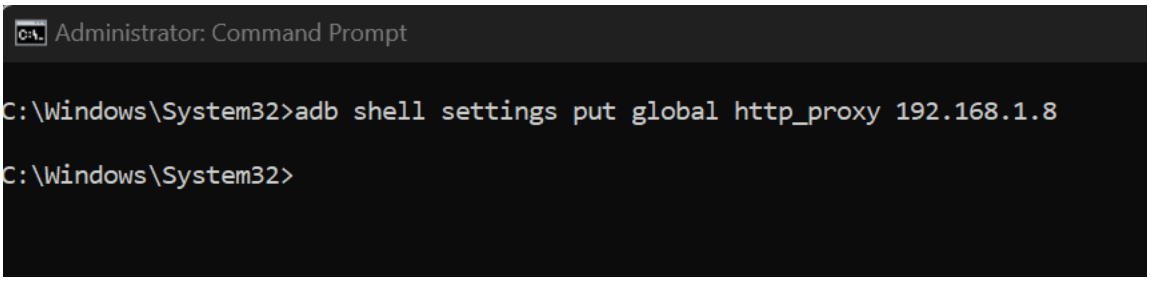


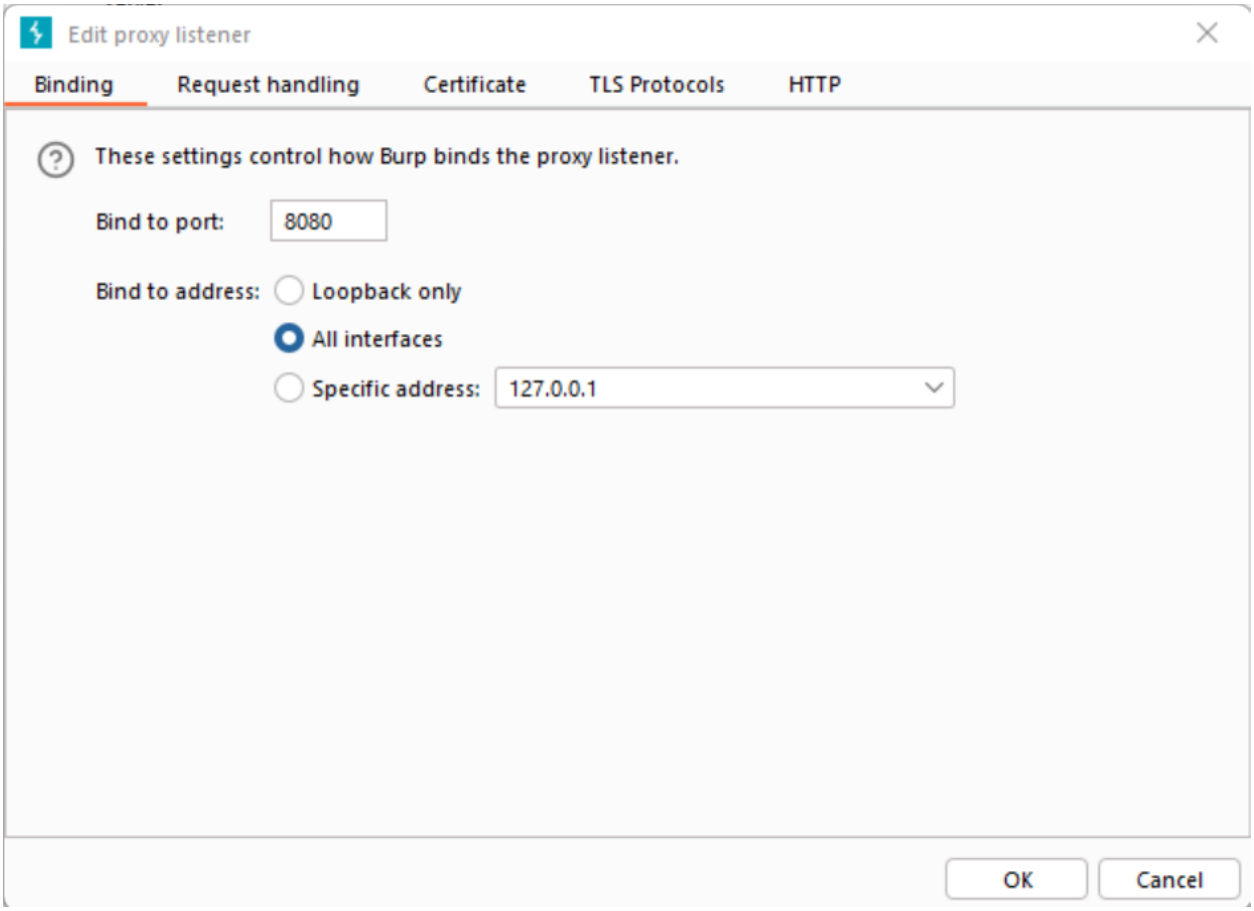
19.2.2 Check connection

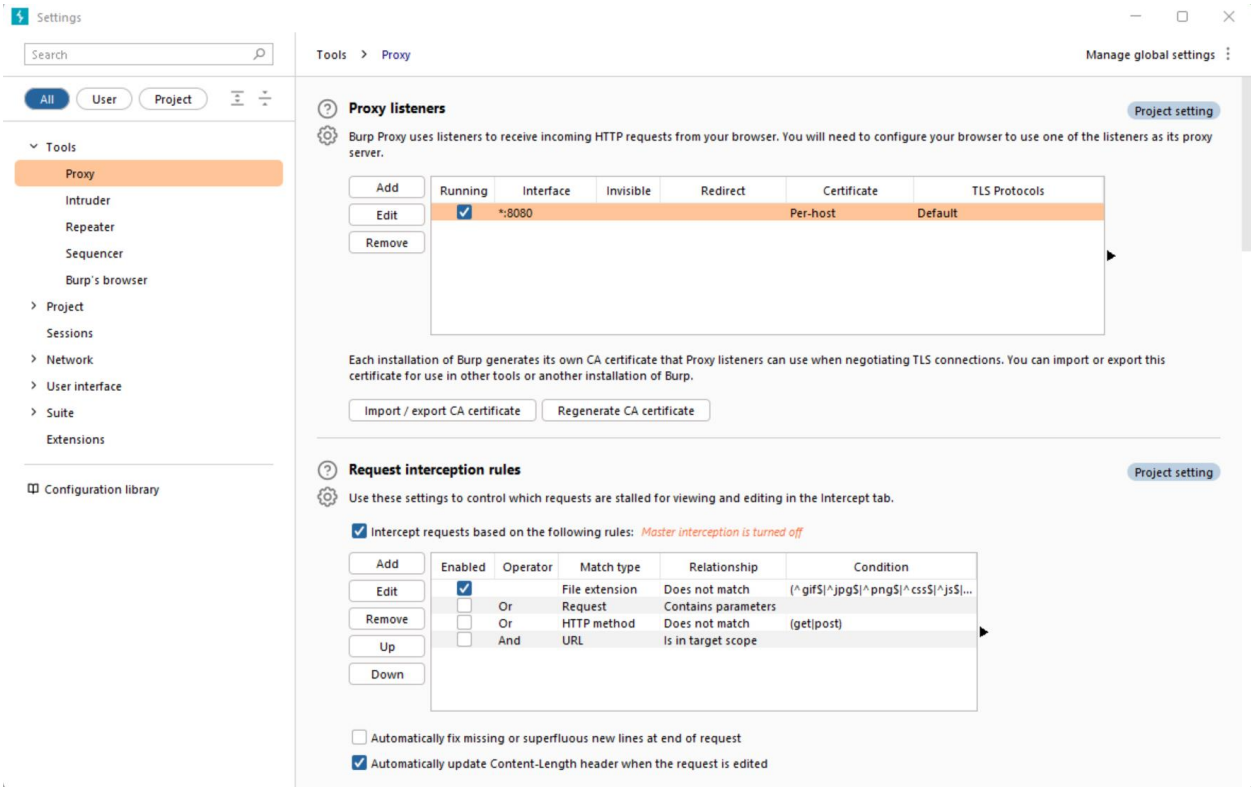
```
C:\Windows\System32>adb shell
aosp:/ # ping 192.168.1.8
PING 192.168.1.8 (192.168.1.8) 56(84) bytes of data.
64 bytes from 192.168.1.8: icmp_seq=1 ttl=127 time=1.11 ms
64 bytes from 192.168.1.8: icmp_seq=2 ttl=127 time=11.0 ms
64 bytes from 192.168.1.8: icmp_seq=3 ttl=127 time=1.32 ms
64 bytes from 192.168.1.8: icmp_seq=4 ttl=127 time=1.12 ms
^C
--- 192.168.1.8 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3015ms
rtt min/avg/max/mdev = 1.112/3.653/11.050/4.271 ms
aosp:/ #
```

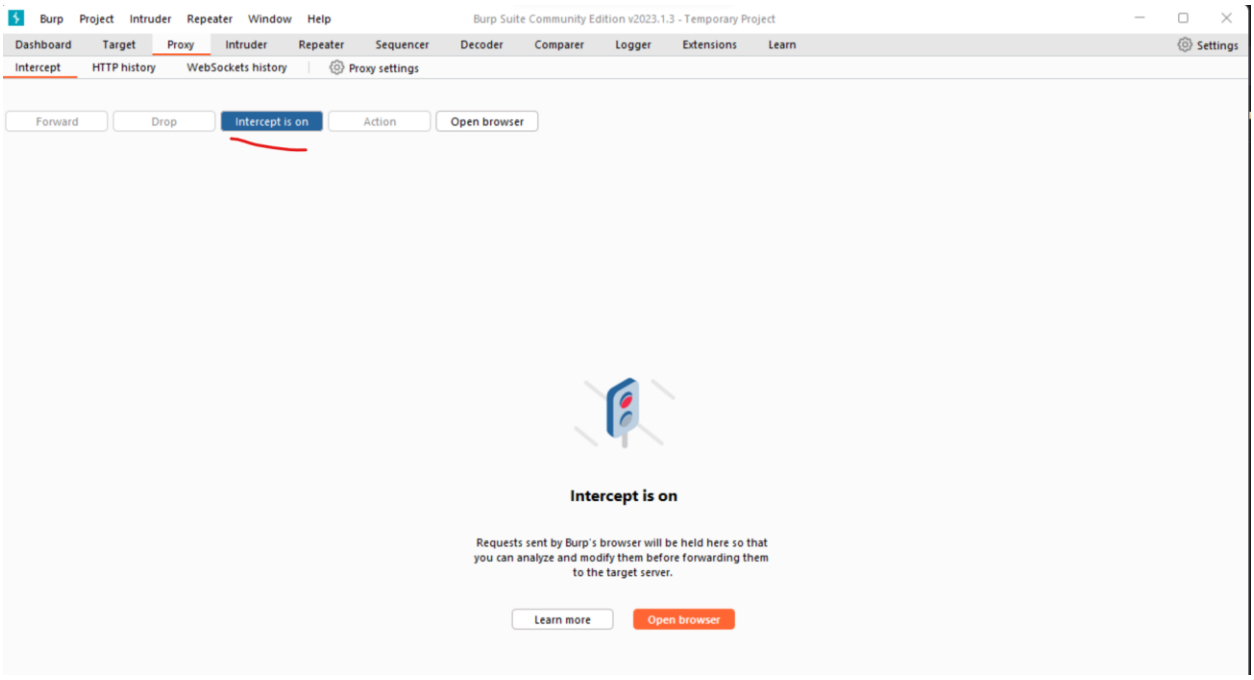
19.2.3 Setting up proxy

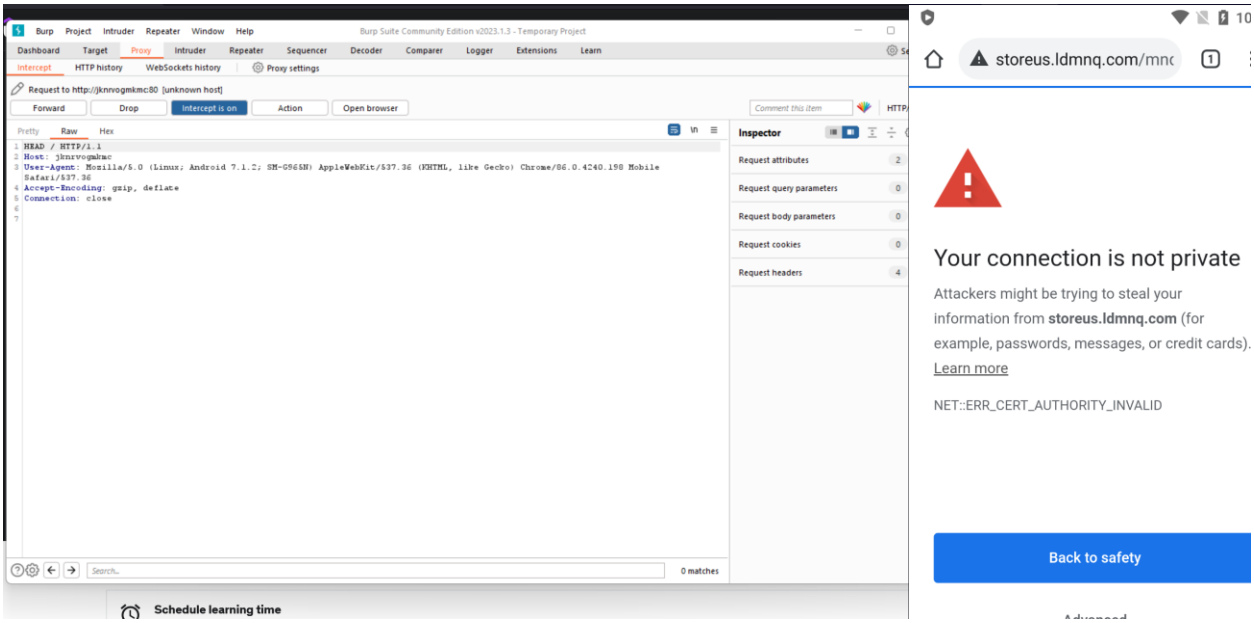
C:\Windows\System32>adb shell settings put global http_proxy 192.168.1.8

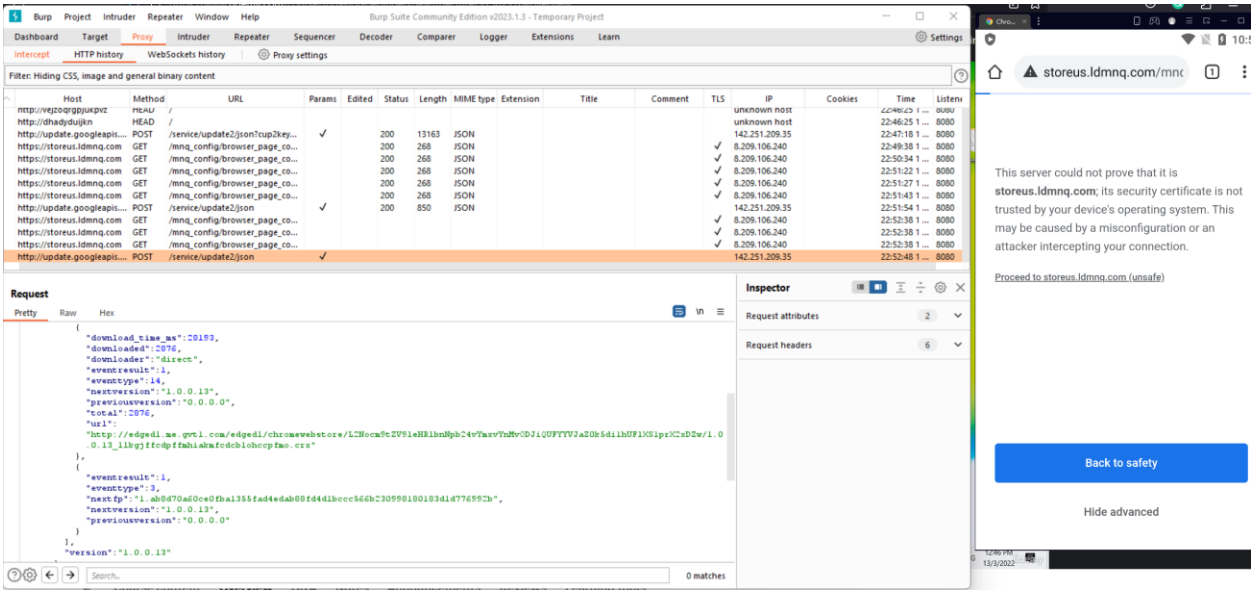

Administrator: Command Prompt
C:\Windows\System32>adb shell settings put global http_proxy 192.168.1.8
C:\Windows\System32>


Edit proxy listener
Binding
Request handling
Certificate
TLS Protocols
HTTP
These settings control how Burp binds the proxy listener.
Bind to port:
8080
Bind to address:
Loopback only
All interfaces
Specific address:
127.0.0.1
OK
Cancel


Settings
Search
All
User
Project
Tools
Proxy
Intruder
Repeater
Sequencer
Burp's browser
Project
Sessions
Network
User interface
Suite
Extensions
Configuration library
Tools > Proxy
Manage global settings
Proxy listeners
Project setting
Burp Proxy uses listeners to receive incoming HTTP requests from your browser. You will need to configure your browser to use one of the listeners as its proxy server.
Add
Edit
Remove
Running
Interface
Invisible
Redirect
Certificate
TLS Protocols
*:8080
Per-host
Default
Each installation of Burp generates its own CA certificate that Proxy listeners can use when negotiating TLS connections. You can import or export this certificate for use in other tools or another installation of Burp.
Import / export CA certificate
Regenerate CA certificate
Request interception rules
Project setting
Use these settings to control which requests are stalled for viewing and editing in the Intercept tab.
Intercept requests based on the following rules: Master interception is turned off
Add
Edit
Remove
Up
Down
Enabled
Operator
Match type
Relationship
Condition
File extension
Does not match
(^gif$|^jpg$|^png$|^css$|^js$|...
Or
Request
Contains parameters
Or
HTTP method
Does not match
(get|post)
And
URL
Is in target scope
Automatically fix missing or superfluous new lines at end of request
Automatically update Content-Length header when the request is edited

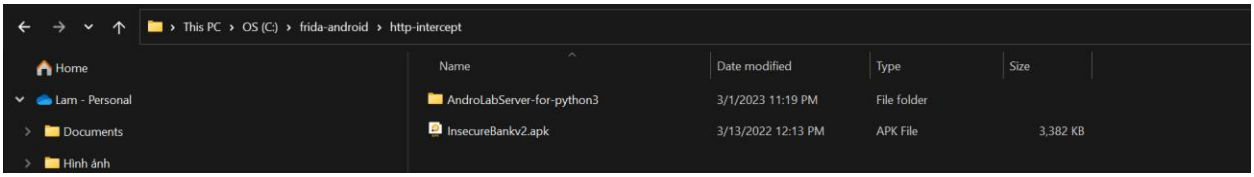

Burp
Project
Intruder
Repeater
Window
Help
Burp Suite Community Edition v2023.1.3 - Temporary Project
Dashboard
Target
Proxy
Intruder
Repeater
Sequencer
Decoder
Comparer
Logger
Extensions
Learn
Settings
Intercept
HTTP history
WebSockets history
Proxy settings
Forward
Drop
Intercept is on
Action
Open browser
Intercept is on
Requests sent by Burp's browser will be held here so that you can analyze and modify them before forwarding them to the target server.
Learn more
Open browser





19.3 Installing the Insecure Bank app

19.3.1 Start server



C:\frida-android\http-intercept\AndroLabServer-for-python3>pip install -r requirements.txt

```
C:\frida-android\http-intercept\AndroLabServer-for-python3>pip install -r requirements.txt
Requirement already satisfied: flask in c:\users\asus\appdata\local\programs\python\python310\lib\site-packages (from -r requirements.txt (line 1)) (2.2.3)
Collecting sqlalchemy
  Downloading SQLAlchemy-2.0.4-cp310-cp310-win_amd64.whl (2.0 MB)
     ---------------------------------------- 2.0/2.0 MB 5.0 MB/s eta 0:00:00
Collecting simplejson
  Downloading simplejson-3.18.3-cp310-cp310-win_amd64.whl (74 kB)
     ---------------------------------------- 74.9/74.9 kB 4.0 MB/s eta 0:00:00
Collecting web.py
  Downloading web.py-0.62.tar.gz (623 kB)
     ---------------------------------------- 623.2/623.2 kB 5.6 MB/s eta 0:00:00
  Installing build dependencies ... done
  Getting requirements to build wheel ... done
  Preparing metadata (pyproject.toml) ... done
Requirement already satisfied: Jinja2>=3.0 in c:\users\asus\appdata\local\programs\python\python310\lib\site-packages (from flask->-r requirements.txt (line 1)) (3.1.2)
Requirement already satisfied: Werkzeug>=2.2.2 in c:\users\asus\appdata\local\programs\python\python310\lib\site-packages (from flask->-r requirements.txt (line 1)) (2.2.3)
Requirement already satisfied: click>=8.0 in c:\users\asus\appdata\local\programs\python\python310\lib\site-packages (from flask->-r requirements.txt (line 1)) (8.1.3)
Requirement already satisfied: itsdangerous>=2.0 in c:\users\asus\appdata\local\programs\python\python310\lib\site-packages (from flask->-r requirements.txt (line 1)) (2.1.2)
Requirement already satisfied: typing-extensions>=4.2.0 in c:\users\asus\appdata\local\programs\python\python310\lib\site-packages (from sqlalchemy->-r requirements.txt (line 2)) (4.5.0)
Collecting greenlet!=0.4.17
  Downloading greenlet-2.0.2-cp310-cp310-win_amd64.whl (192 kB)
     ---------------------------------------- 192.2/192.2 kB 12.1 MB/s eta 0:00:00
Collecting cheroot
  Downloading cheroot-9.0.0-py2.py3-none-any.whl (100 kB)
     ---------------------------------------- 100.6/100.6 kB 6.0 MB/s eta 0:00:00
Requirement already satisfied: colorama in c:\users\asus\appdata\local\programs\python\python310\lib\site-packages (from click>=8.0->flask->-r requirements.txt (line 1)) (0.4.6)
Requirement already satisfied: MarkupSafe>=2.0 in c:\users\asus\appdata\local\programs\python\python310\lib\site-packages (from Jinja2>=3.0->flask->-r requirements.txt (line 1)) (2.1.2)
Requirement already satisfied: six>=1.11.0 in c:\users\asus\appdata\local\programs\python\python310\lib\site-packages (from cheroot->web.py->-r requirements.txt (line 4)) (1.16.0)
Collecting more-itertools>=2.6
  Downloading more_itertools-9.1.0-py3-none-any.whl (54 kB)
     ---------------------------------------- 54.2/54.2 kB 2.7 MB/s eta 0:00:00
Collecting jaraco.functools
  Downloading jaraco.functools-3.6.0-py3-none-any.whl (7.9 kB)
Building wheels for collected packages: web.py
  Building wheel for web.py (pyproject.toml) ... done
  Created wheel for web.py: filename=web.py-0.62-py3-none-any.whl size=78588 sha256=65382a607c51dff5f9a019252b1186fdffacdc74ee57ea17ecb564e7919e47d6
  Stored in directory: c:\users\asus\appdata\local\pip\cache\wheels\d7\26\ae\7365539ba096c7907194fa908f12ebb9549959752ae5c5036b
Successfully built web.py
Installing collected packages: simplejson, more-itertools, greenlet, sqlalchemy, jaraco.functools, cheroot, web.py
Successfully installed cheroot-9.0.0 greenlet-2.0.2 jaraco.functools-3.6.0 more-itertools-9.1.0 simplejson-3.18.3 sqlalchemy-2.0.4 web.py-0.62

[notice] A new release of pip available: 22.3.1 -> 23.0.1
[notice] To update, run: python.exe -m pip install --upgrade pip

C:\frida-android\http-intercept\AndroLabServer-for-python3>
```

Fix

app.py database.py

```python
from sqlalchemy import create_engine
from sqlalchemy.orm import scoped_session, sessionmaker
from sqlalchemy.ext.declarative import declarative_base

#engine = create_engine('sqlite:///mydb.db', convert_unicode=True)
engine = create_engine('sqlite:///mydb.db')
db_session = scoped_session(sessionmaker(autocommit=False,
                                         autoflush=False,
                                         bind=engine))
Base = declarative_base()
Base.query = db_session.query_property()

def init_db():
    # import all modules here that might define models so that
    # they will be registered properly on the metadata.  Otherwise
    # you will have to import them first before calling init_db()
    import models
    Base.metadata.create_all(bind=engine)

```

C:\frida-android\http-intercept\AndroLabServer-for-python3>python app.py --help

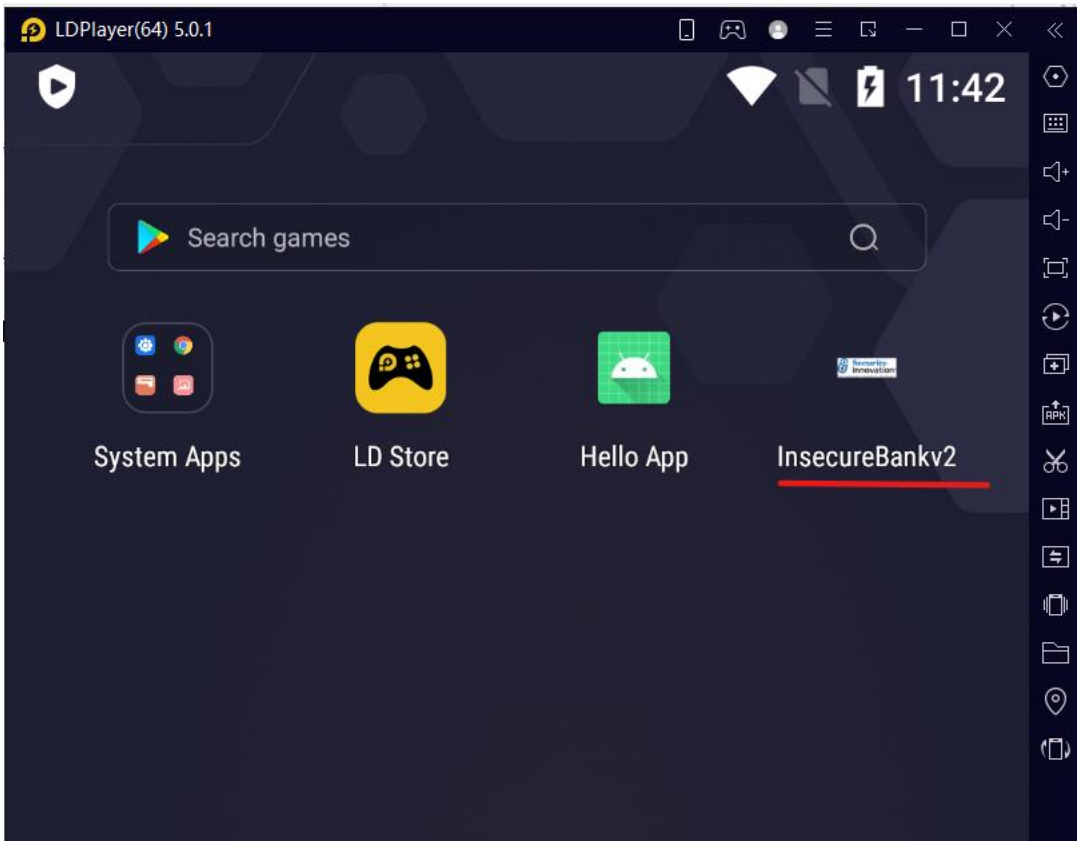
C:\frida-android\http-intercept\AndroLabServer-for-python3>python app.py

```
C:\frida-android\http-intercept\AndroLabServer-for-python3>python app.py --help
InsecureBankv2 Backend-Server
Options:
  --port p    serve on port p (default 8888)
  --help      print this message

C:\frida-android\http-intercept\AndroLabServer-for-python3>python app.py
The server is hosted on port: 8888
```

C:\Windows\System32>netstat -tna

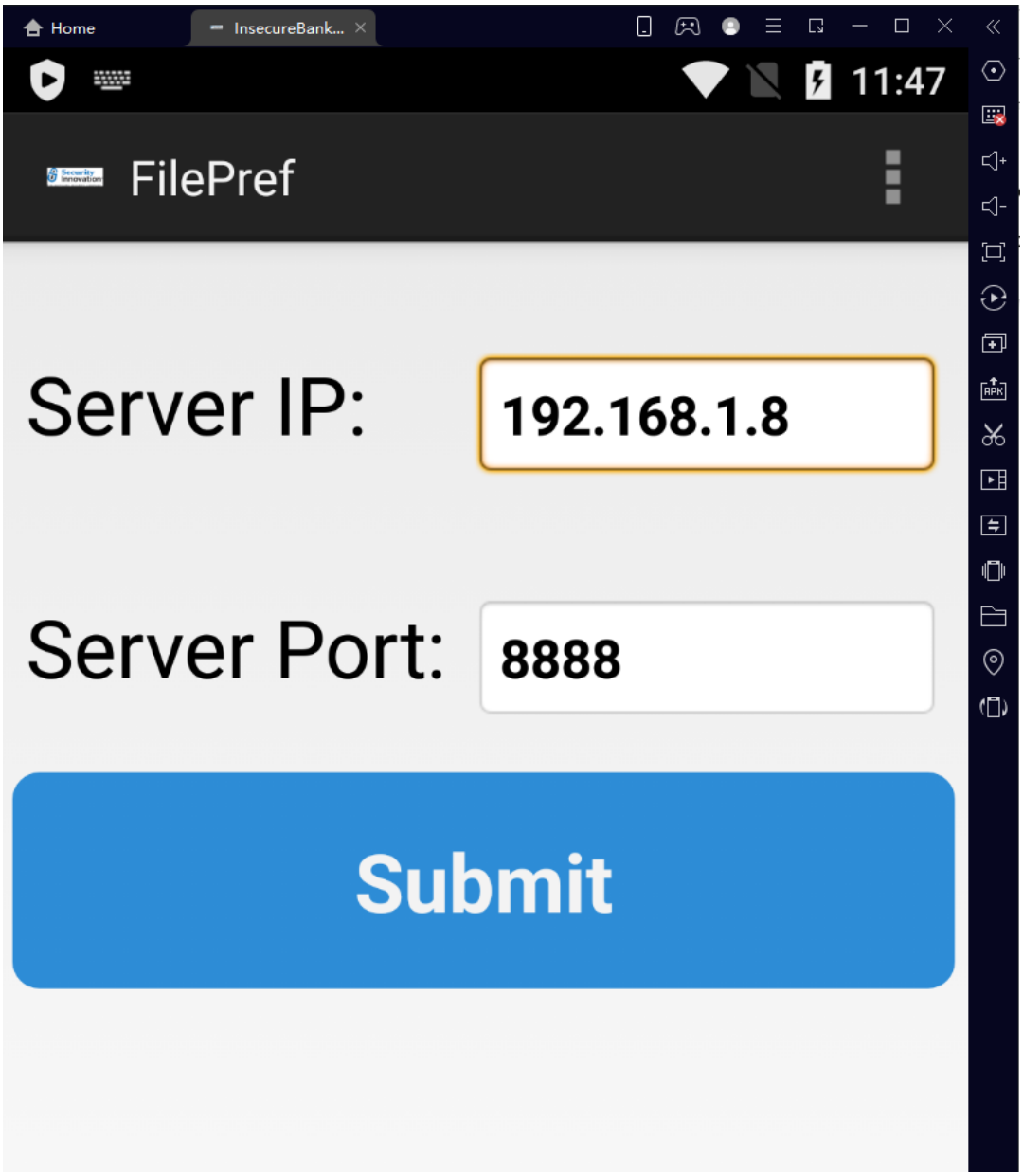
```
Select Administrator: Command Prompt
Microsoft Windows [Version 10.0.22621.1265]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\System32>netstat -tna

Active Connections

  Proto  Local Address          Foreign Address        State           Offload State

  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING       InHost
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING       InHost
  TCP    0.0.0.0:902            0.0.0.0:0              LISTENING       InHost
  TCP    0.0.0.0:912            0.0.0.0:0              LISTENING       InHost
  TCP    0.0.0.0:2222           0.0.0.0:0              LISTENING       InHost
  TCP    0.0.0.0:2869           0.0.0.0:0              LISTENING       InHost
  TCP    0.0.0.0:5040           0.0.0.0:0              LISTENING       InHost
  TCP    0.0.0.0:5555           0.0.0.0:0              LISTENING       InHost
  TCP    0.0.0.0:7680           0.0.0.0:0              LISTENING       InHost
  TCP    0.0.0.0:8080           0.0.0.0:0              LISTENING       InHost
  TCP    0.0.0.0:8888           0.0.0.0:0              LISTENING       InHost
  TCP    0.0.0.0:49664          0.0.0.0:0              LISTENING       InHost
  TCP    0.0.0.0:49665          0.0.0.0:0              LISTENING       InHost
  TCP    0.0.0.0:49668          0.0.0.0:0              LISTENING       InHost
  TCP    0.0.0.0:49669          0.0.0.0:0              LISTENING       InHost
  TCP    0.0.0.0:49678          0.0.0.0:0              LISTENING       InHost
  TCP    0.0.0.0:49686          0.0.0.0:0              LISTENING       InHost
```

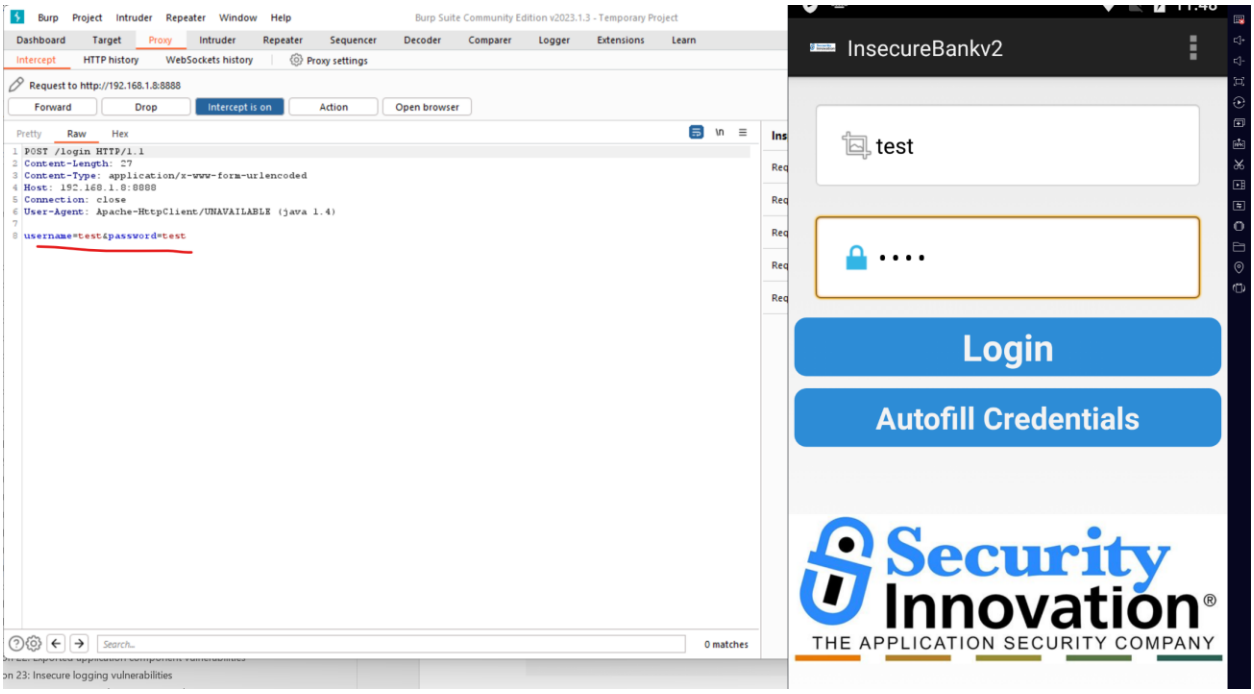
19.3.2 Install apk



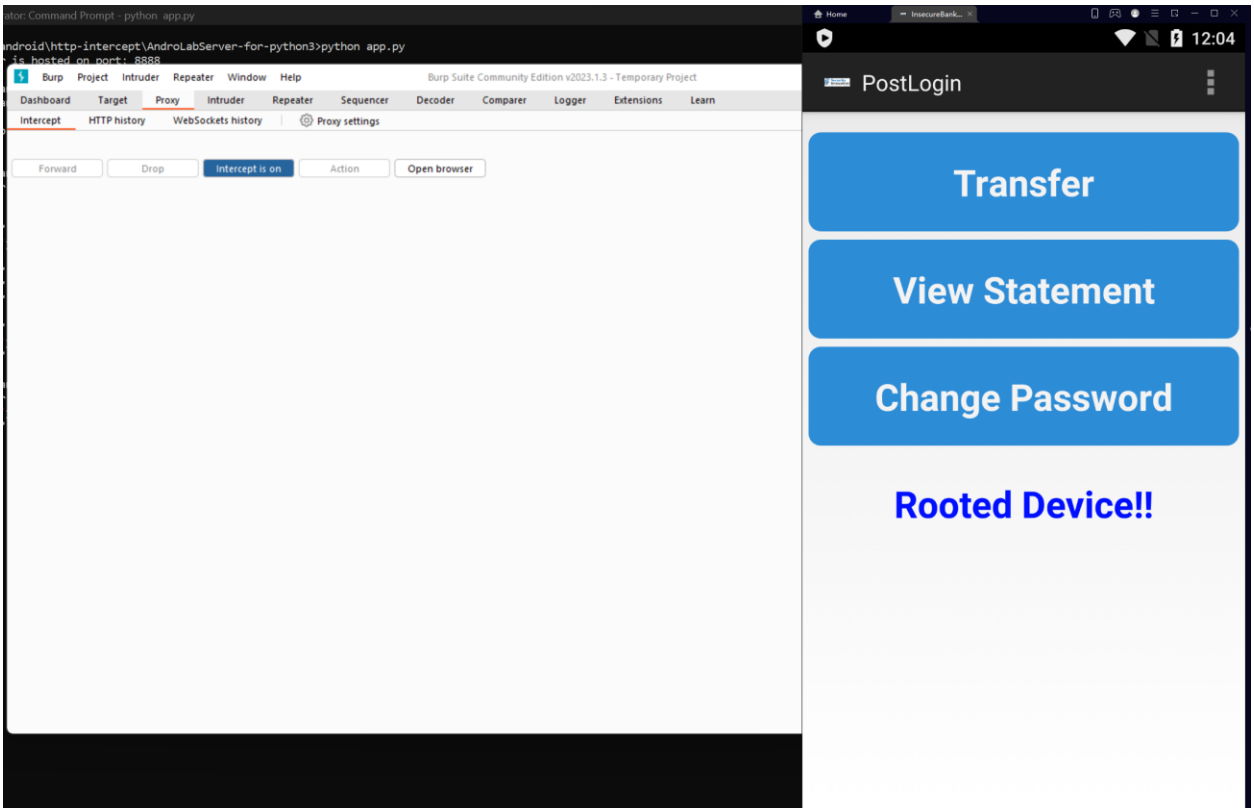
https://github.com/napoleon211092/Android-InsecureBankv2

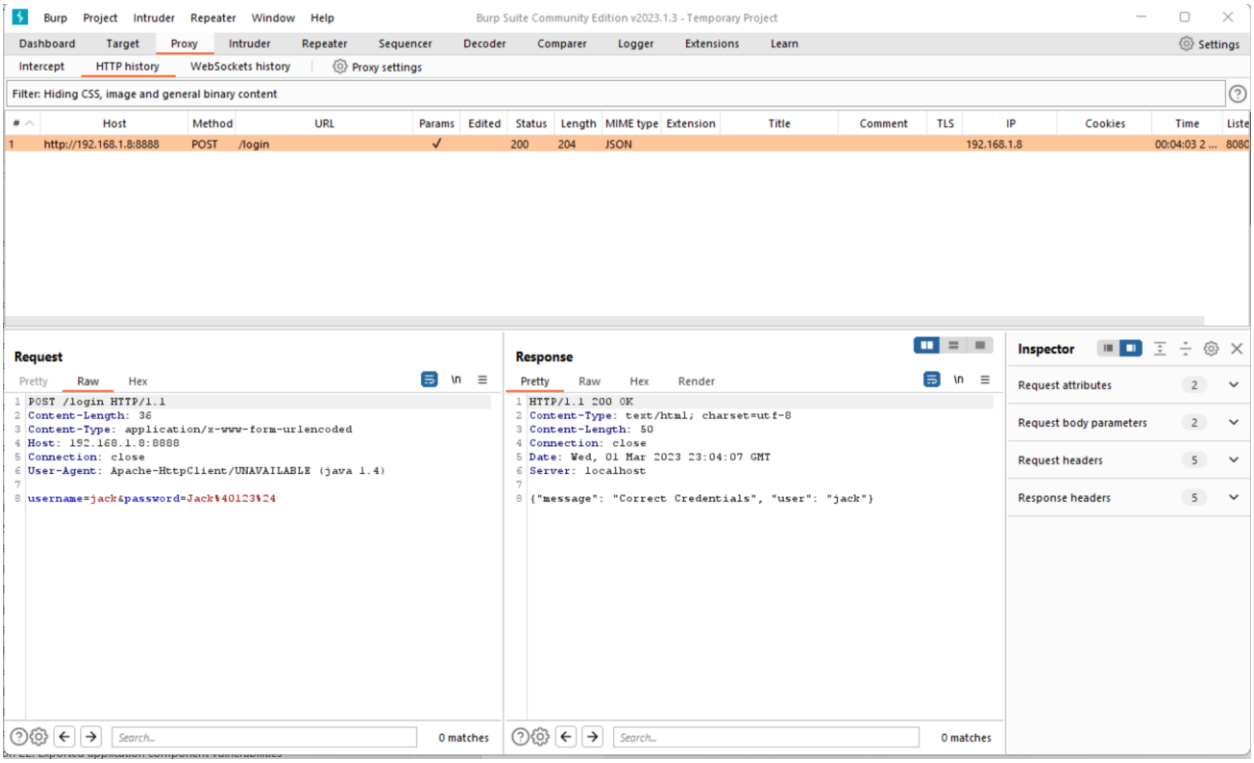
dinesh/Dinesh@123$ or jack/Jack@123$


Home
InsecureBank...
11:47
FilePref
Server IP:
192.168.1.8
Server Port:
8888
Submit



Correct username and pass





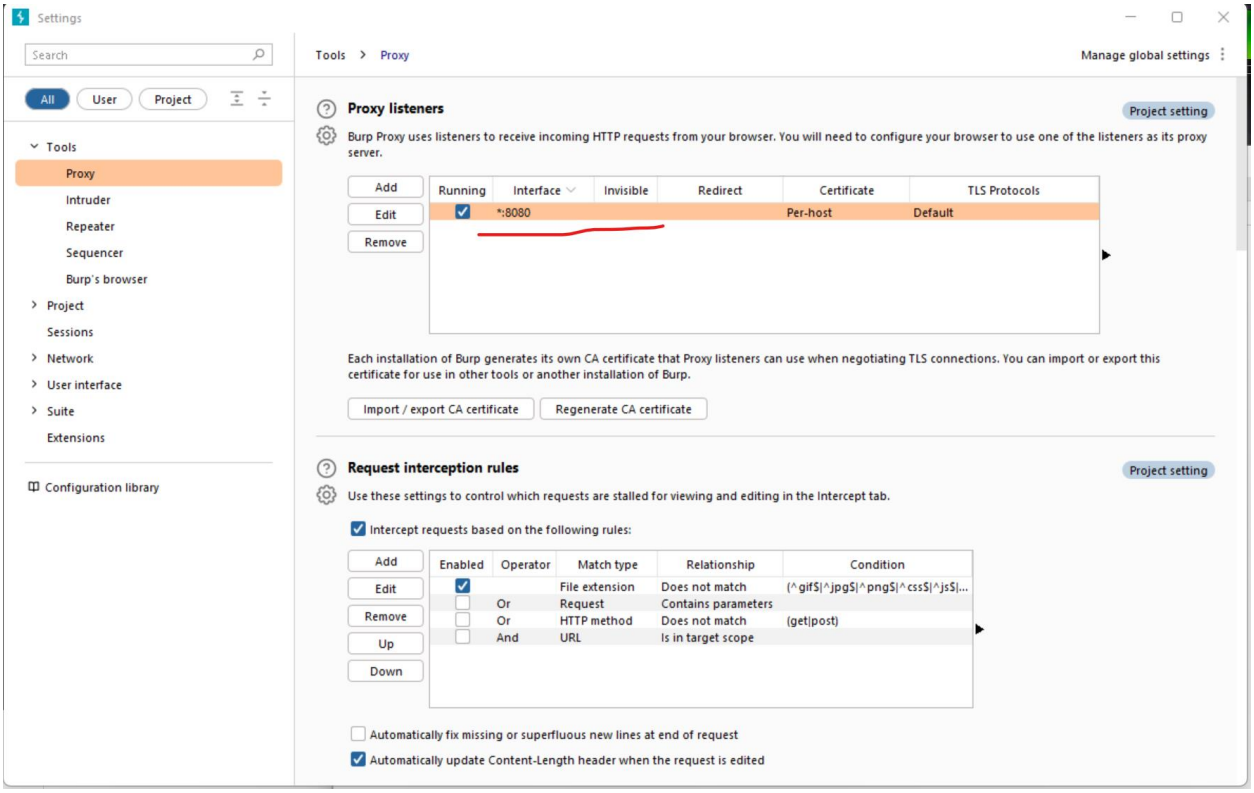
20 Section 20: Intercepting HTTPs traffic

20.1 Installing burpsuite CA cert

20.1.1 Setting up proxy

adb shell settings put global http_proxy 192.168.1.8

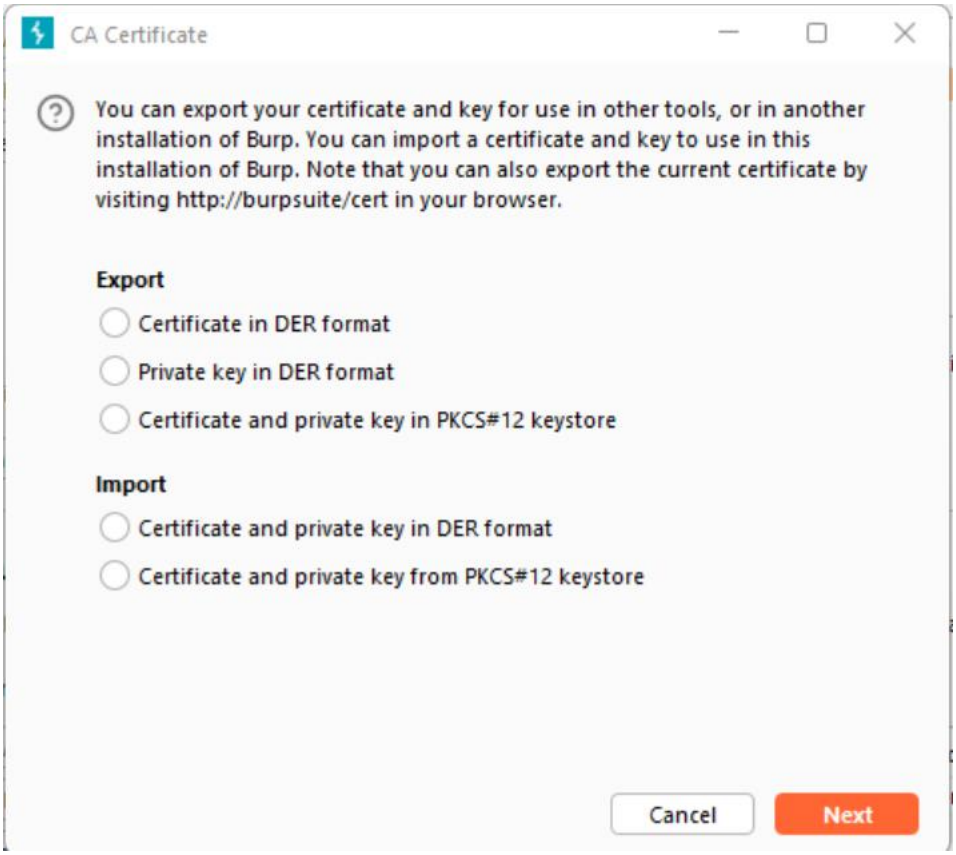
```
C:\>adb devices
List of devices attached
emulator-5554   device


C:\>adb shell settings put global http_proxy 10.23.11.244

C:\>
```



20.1.2 Export certificate

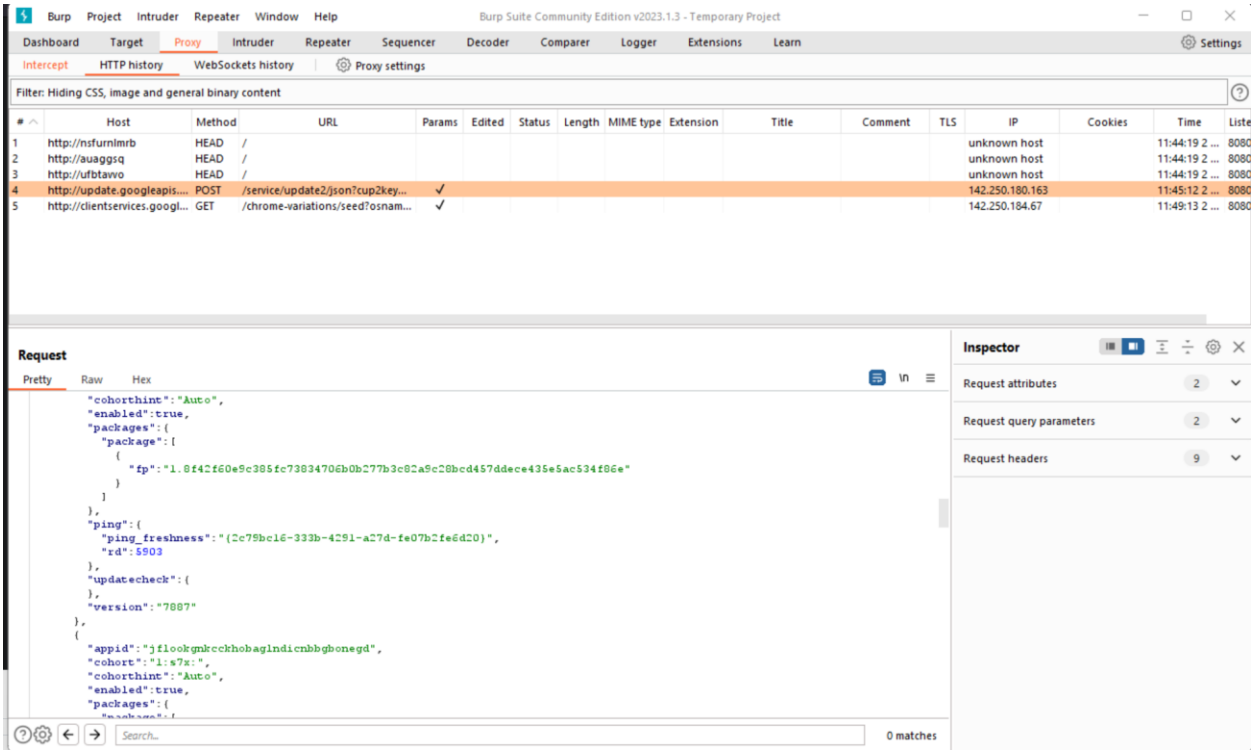
C:\Users\ASUS\Documents\XuanZhi64\Pictures

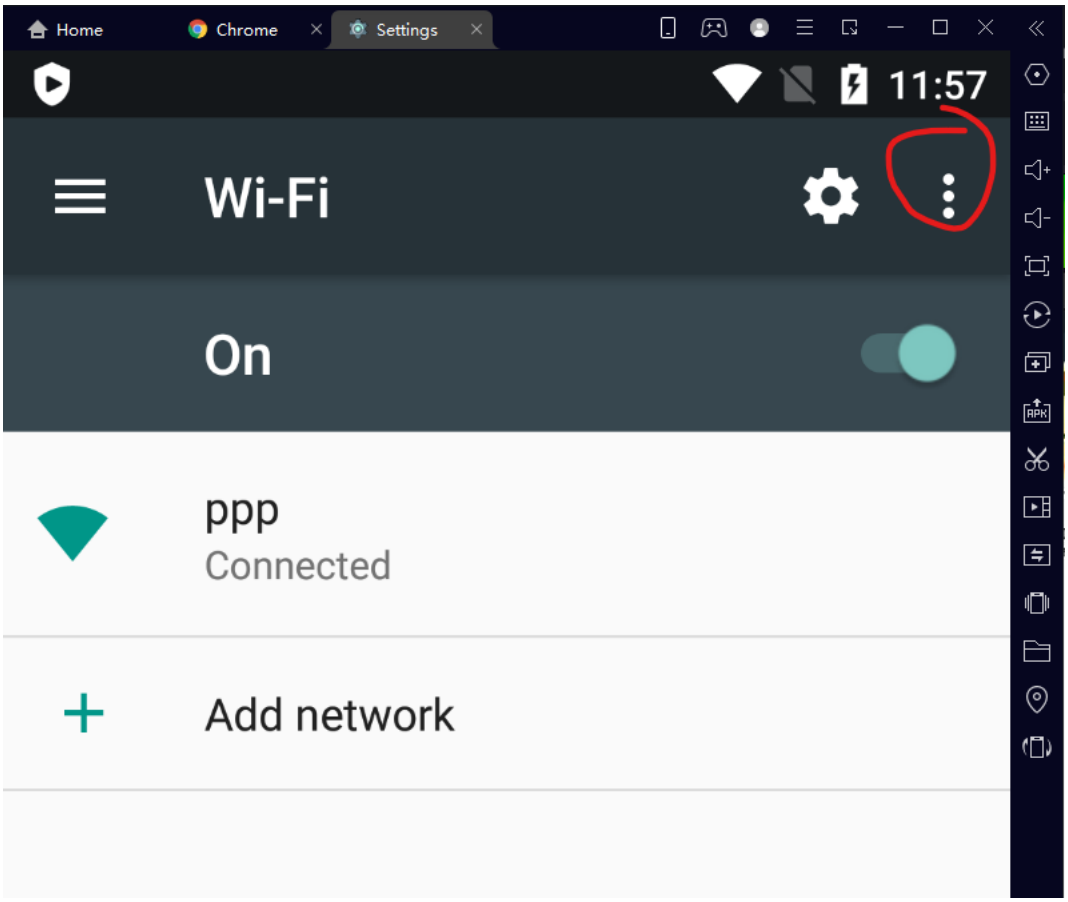
Rename → BurpCert.cer

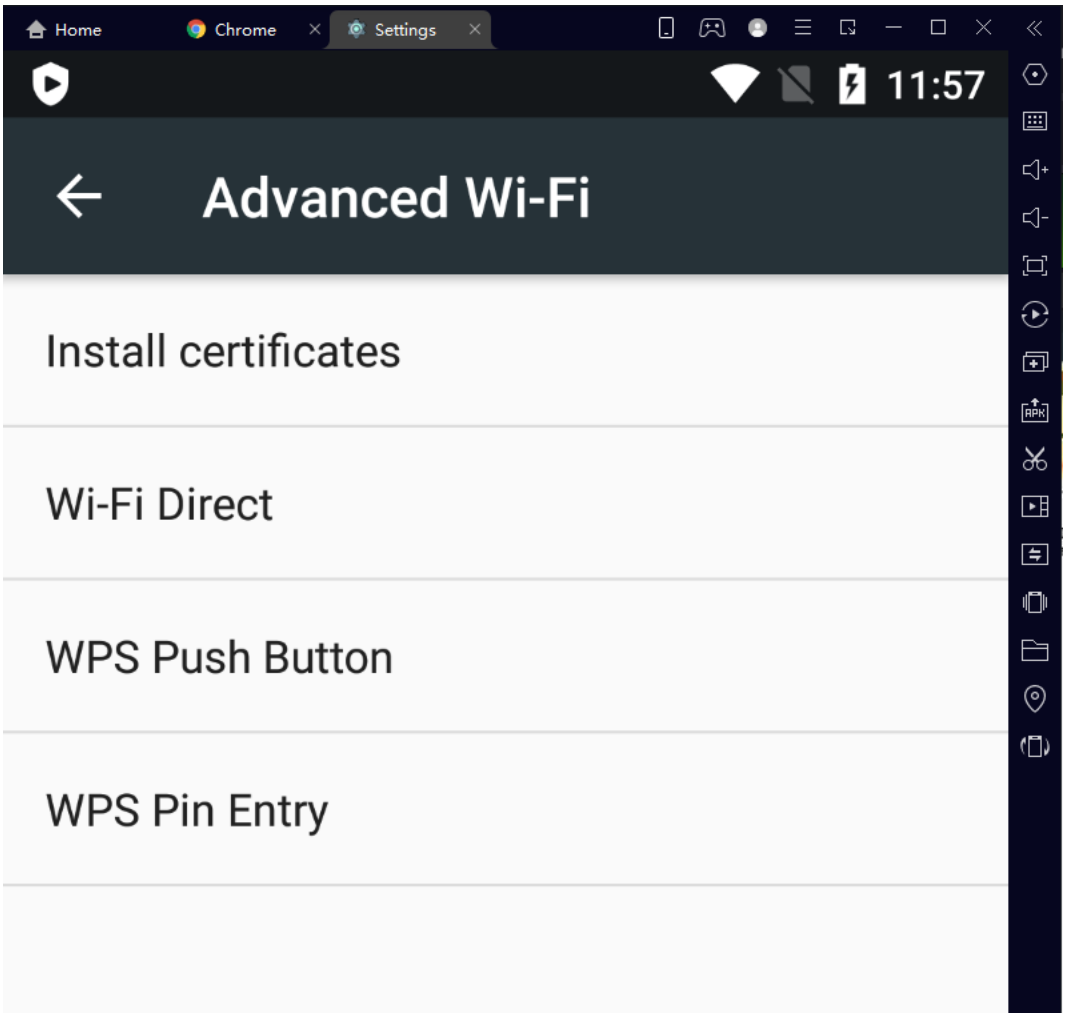


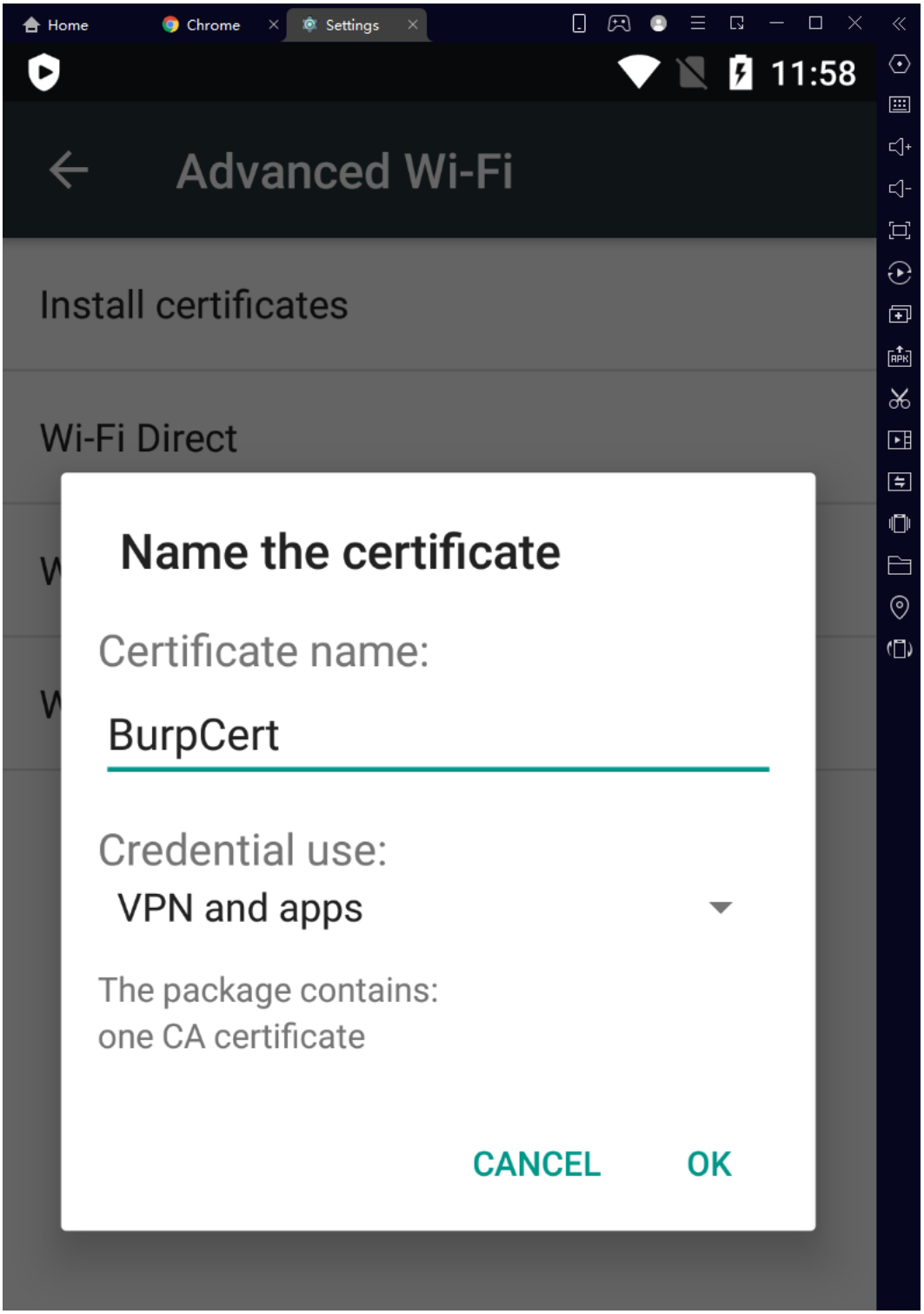
20.1.3 Install certificate

Before install certificate

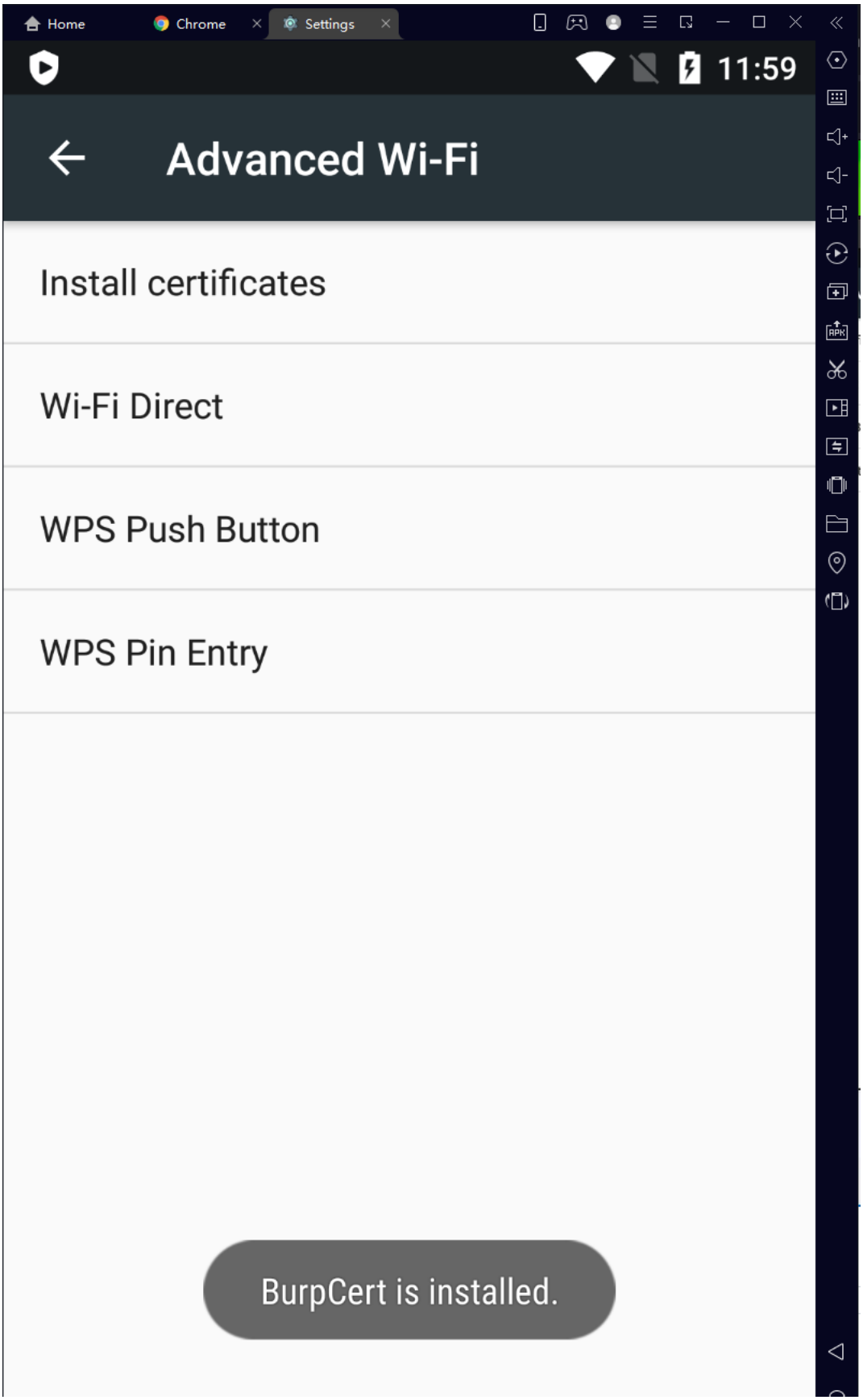

Burp Project Intruder Repeater Window Help
Burp Suite Community Edition v2023.1.3 - Temporary Project
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extensions Learn
Settings
Intercept HTTP history WebSockets history Proxy settings
Filter: Hiding CSS, image and general binary content
Host Method URL Params Edited Status Length MIME type Extension Title Comment TLS IP Cookies Time
1 http://nsfurnlmrb HEAD / unknown host 11:44:19 2 ... 8080
2 http://auaggsq HEAD / unknown host 11:44:19 2 ... 8080
3 http://ufbtawvo HEAD / unknown host 11:44:19 2 ... 8080
4 http://update.googleapis.... POST /service/update2/json?cup2key... ✓ 142.250.180.163 11:45:12 2 ... 8080
5 http://clientservices.googl... GET /chrome-variations/seed?osnam... ✓ 142.250.184.67 11:49:13 2 ... 8080
Request
Pretty Raw Hex
"cohorthint":"Auto",
"enabled":true,
"packages":{
"package":[
{
"fp":"1.8f42f60e9c385fc73834706b0b277b3c82a9c28bcd457ddece435e5ac534f86e"
}
]
},
"ping":{
"ping_freshness":"{2c75bc16-333b-4291-a27d-fe07b2fe6d20}",
"rd":5903
},
"updatecheck":{
},
"version":"7887"
},
{
"appid":"jflookgmkcckhobaglndicnbbgbonegd",
"cohort":"1:s7x:",
"cohorthint":"Auto",
"enabled":true,
"packages":{
Search...
0 matches
Inspector
Request attributes 2
Request query parameters 2
Request headers 9


Home
Chrome
Settings
11:57
Wi-Fi
On
ppp
Connected
Add network


Home
Chrome
Settings
11:57
Advanced Wi-Fi
Install certificates
Wi-Fi Direct
WPS Push Button
WPS Pin Entry

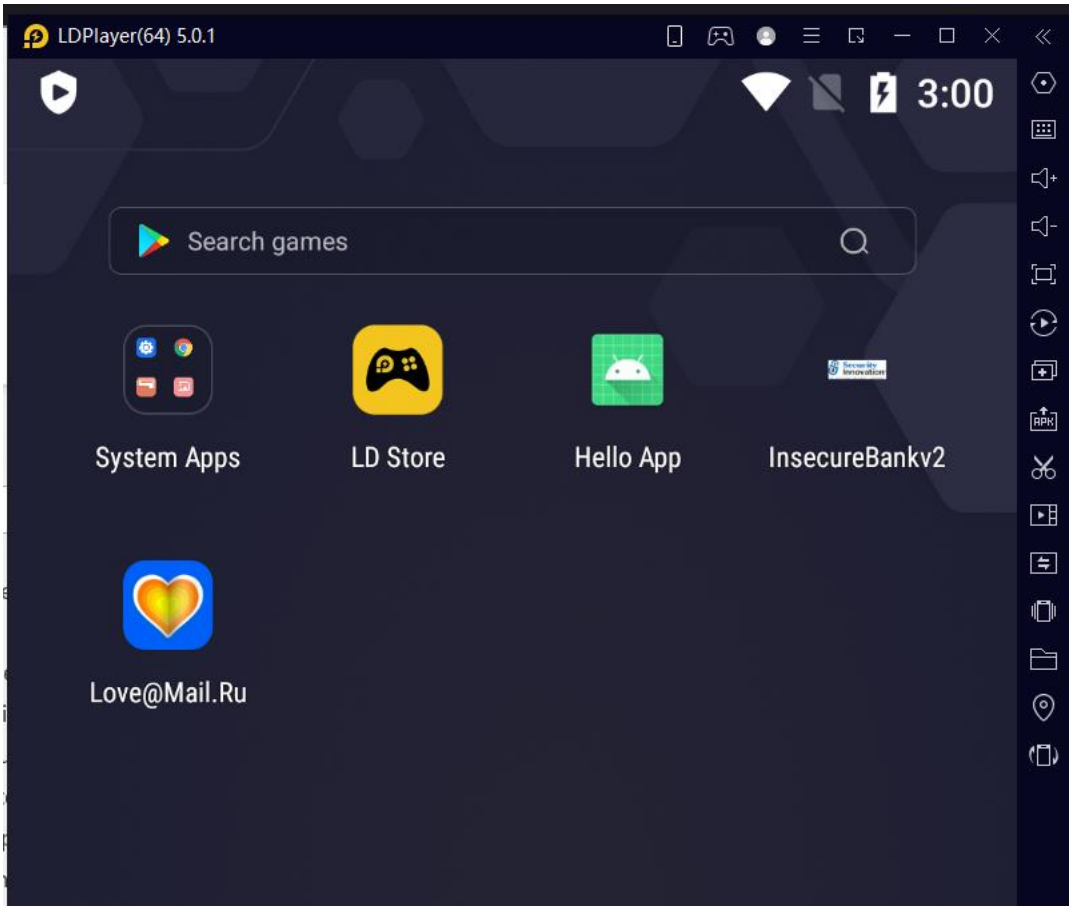

Home
Chrome
Settings
11:58
Advanced Wi-Fi
Install certificates
Wi-Fi Direct
Name the certificate
Certificate name:
BurpCert
Credential use:
VPN and apps
The package contains:
one CA certificate
CANCEL
OK

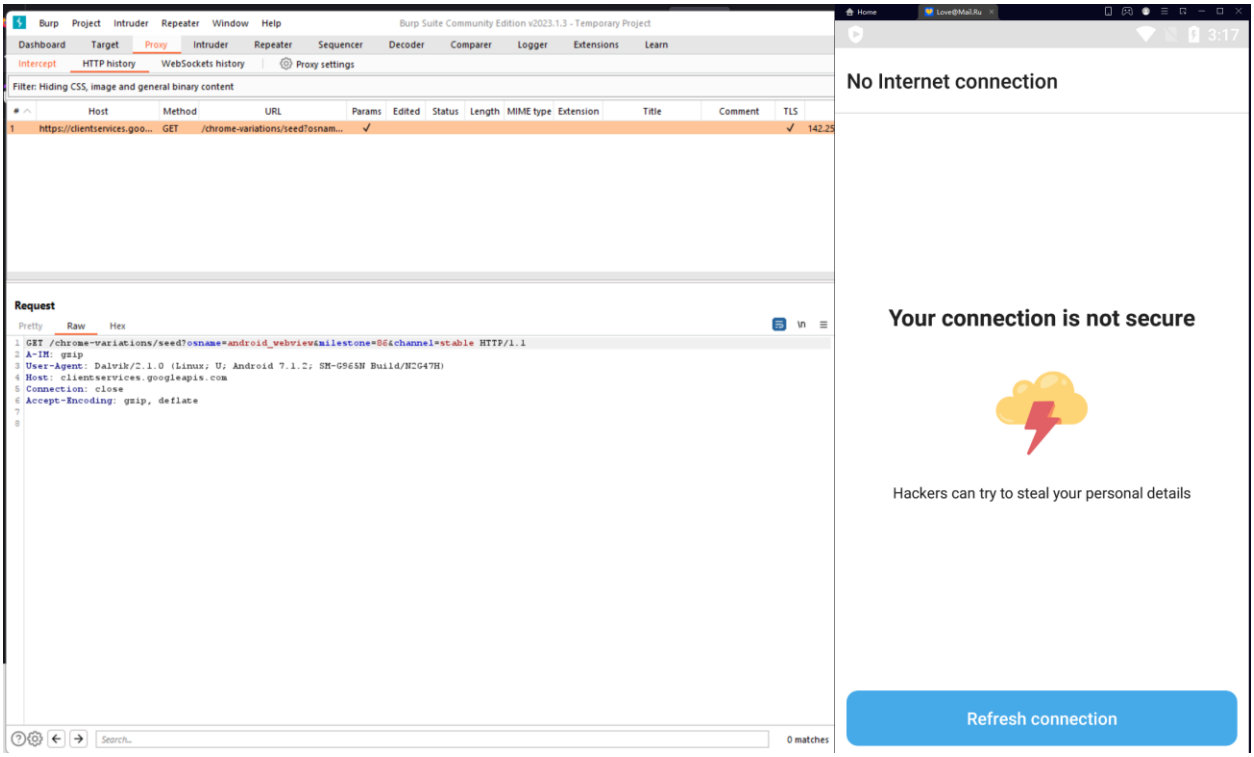
Pin = 1234


Home
Chrome
Settings
11:59
Advanced Wi-Fi
Install certificates
Wi-Fi Direct
WPS Push Button
WPS Pin Entry
BurpCert is installed.

20.2 Modifying network-security-config

20.2.1 Install dating app





We can’t move because this app has high-level security

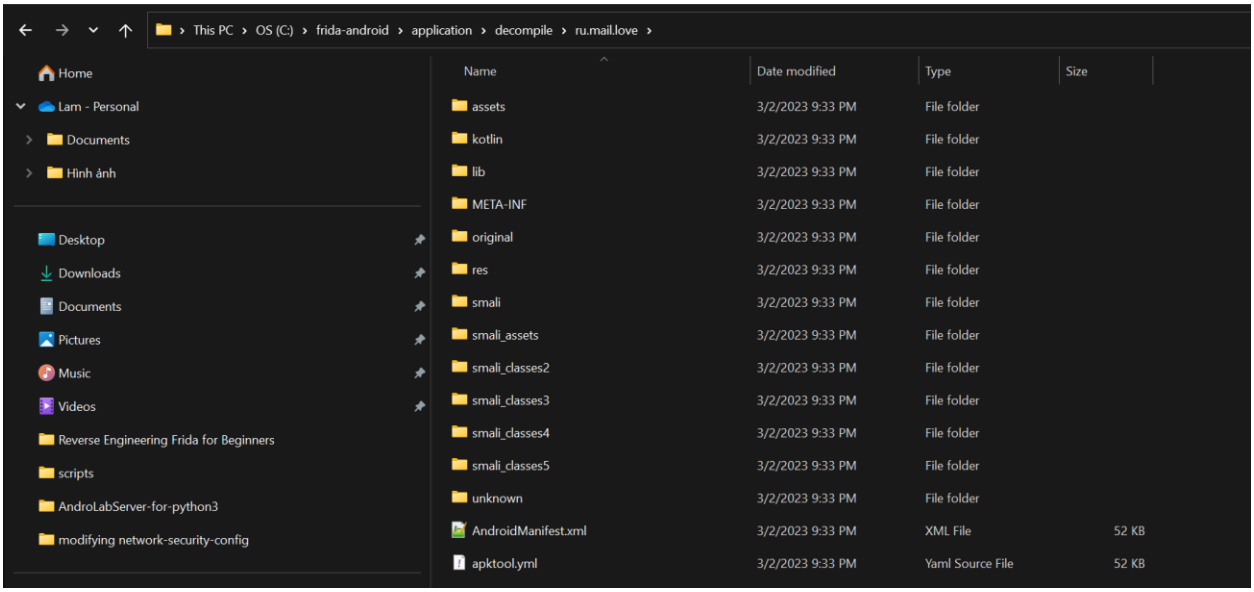
20.2.2 Fix

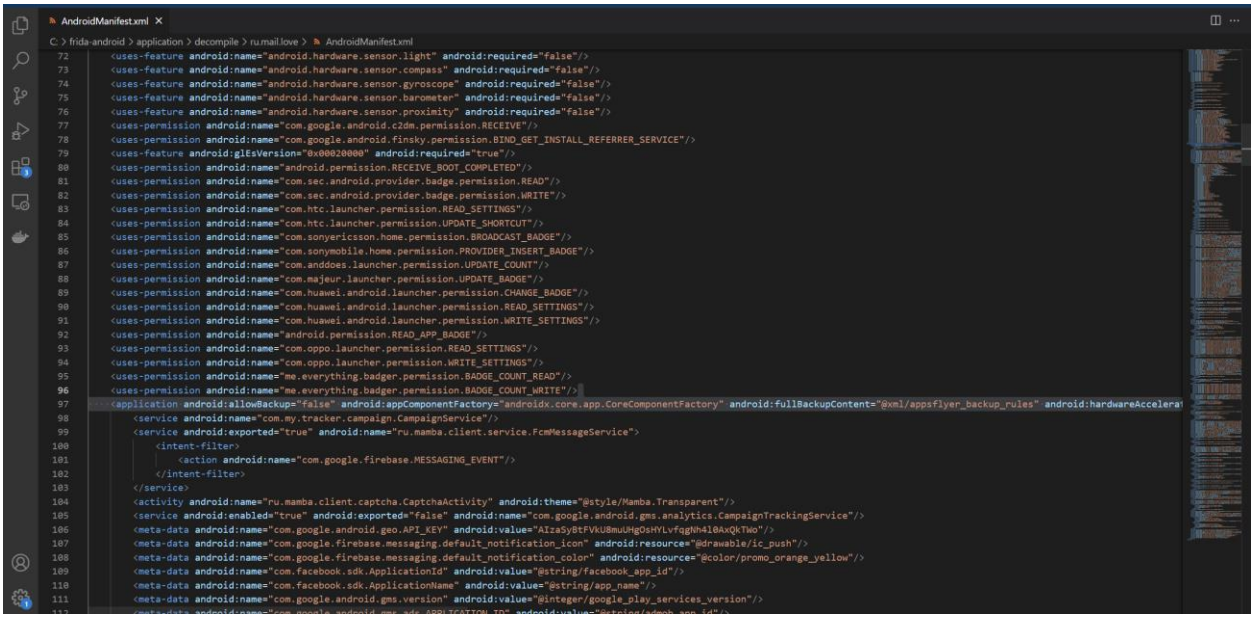
Uninstall app, close BurpSuite

Decompile

C:\frida-android\application\decompile>apktool d ru.mail.love.apk

```
C:\frida-android\application\decompile>apktool d ru.mail.love.apk
I: Using Apktool 2.7.0 on ru.mail.love.apk
I: Loading resource table...
I: Decoding AndroidManifest.xml with resources...
I: Loading resource table from file: C:\Users\ASUS\AppData\Local\apktool\framework\1.apk
I: Regular manifest package...
I: Decoding file-resources...
I: Decoding values */* XMLs...
I: Baksmaling classes.dex...
I: Baksmaling classes2.dex...
I: Baksmaling classes3.dex...
I: Baksmaling classes4.dex...
I: Baksmaling classes5.dex...
I: Baksmaling assets/audience_network.dex...
I: Copying assets and libs...
I: Copying unknown files...
I: Copying original files...
I: Copying META-INF/services directory

C:\frida-android\application\decompile>
```



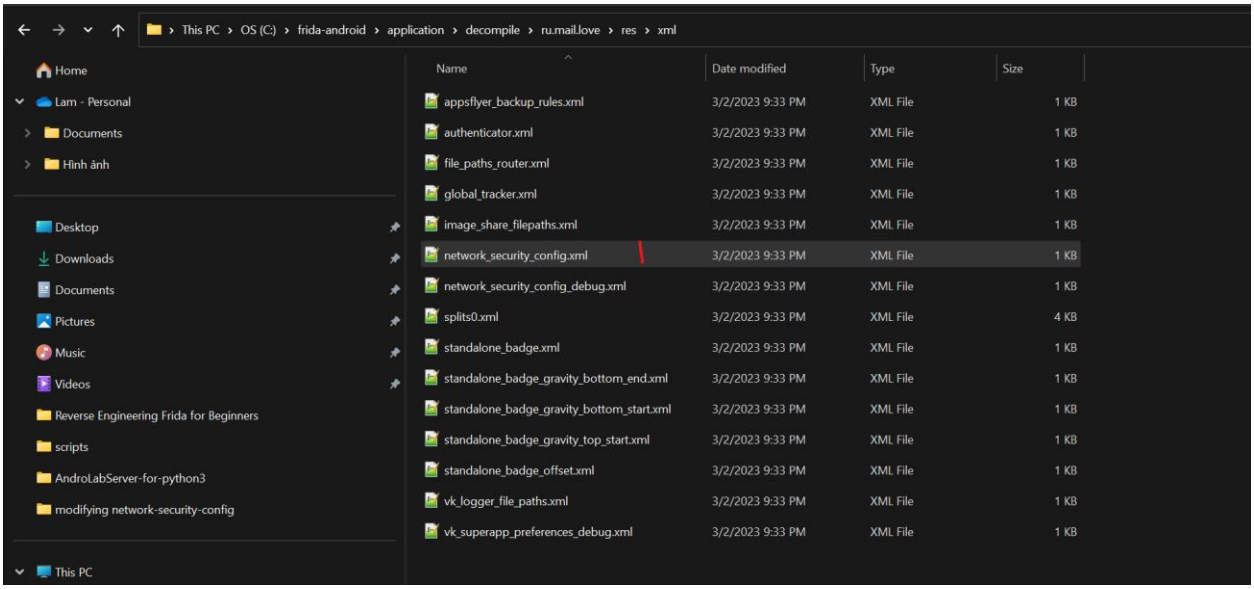


Change from

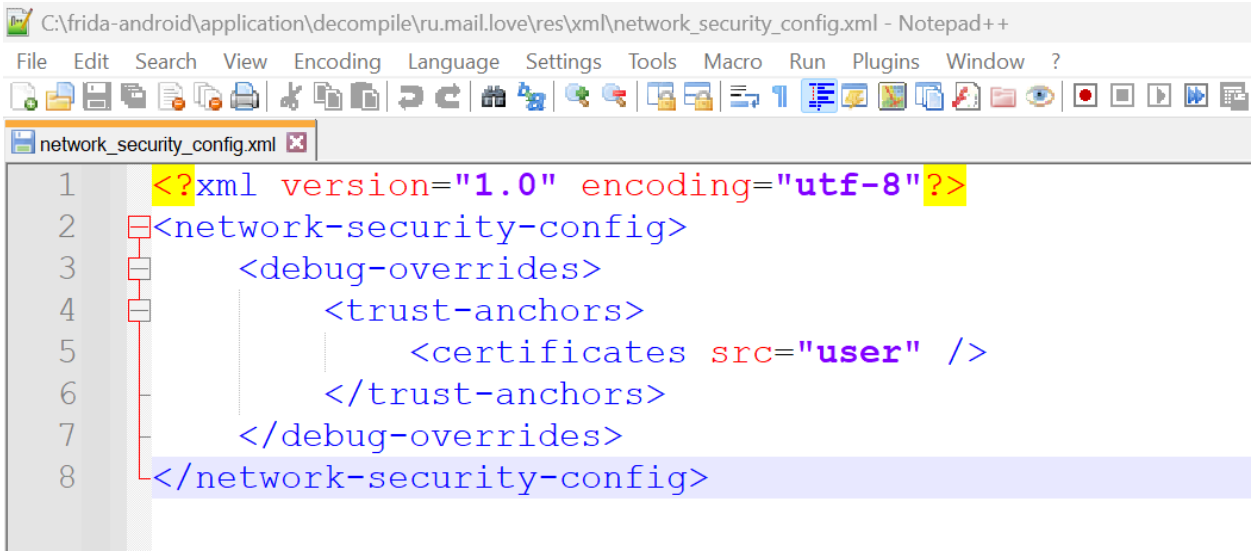
```
android:networkSecurityConfig="@xml/network_security_config_debug"
```

To

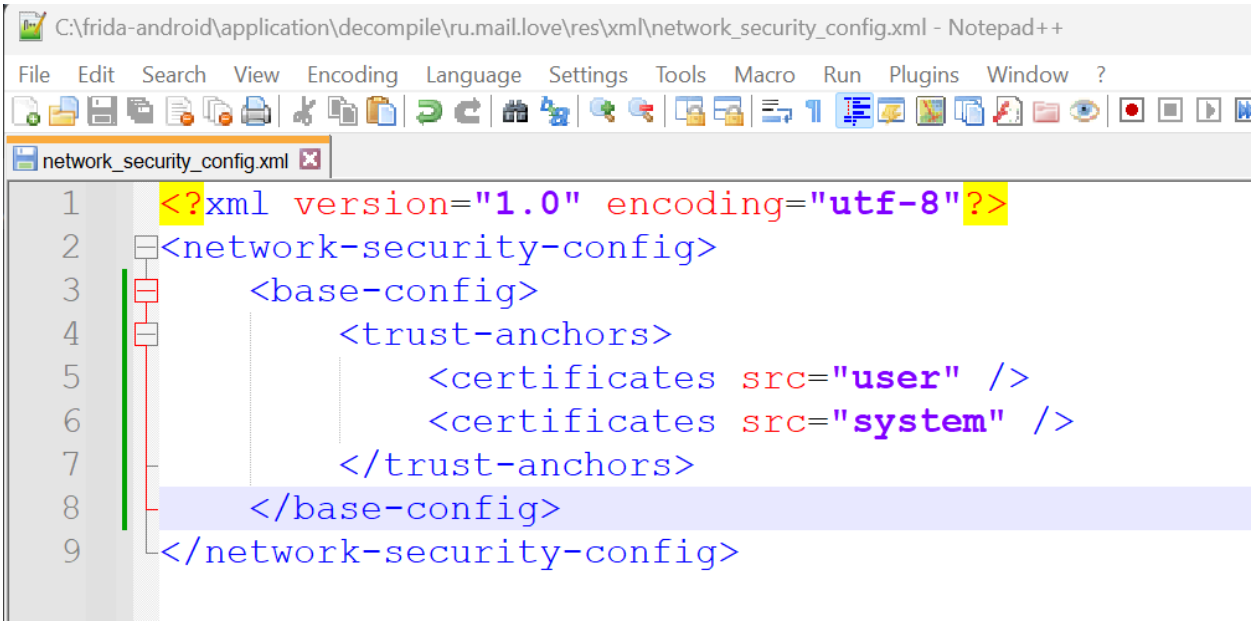
```
android:networkSecurityConfig="@xml/network_security_config"
```



Change from



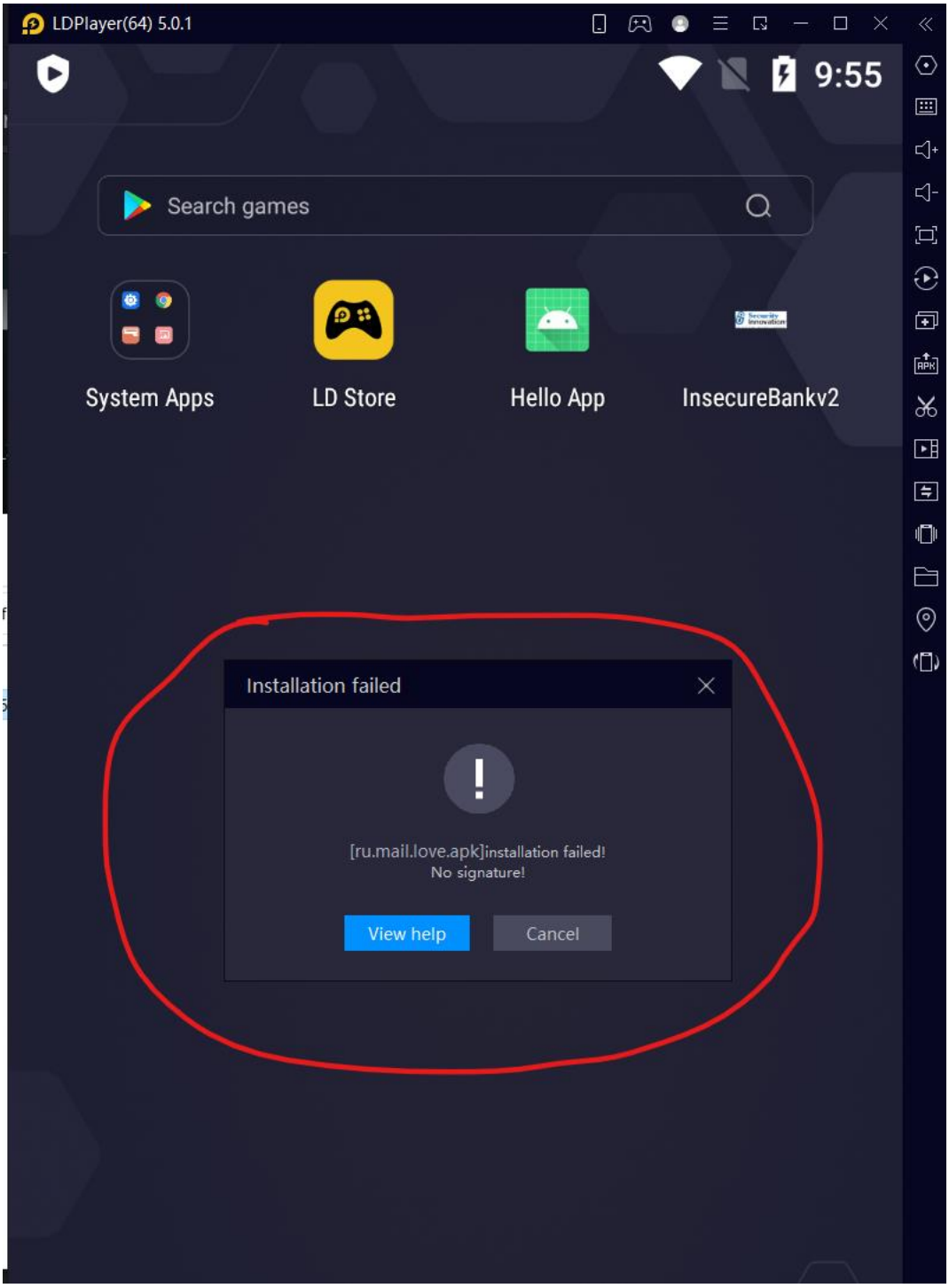
To



Build again

C:\frida-android\application\decompile>apktool b ru.mail.love --use-aapt2

```
C:\frida-android\application\decompile>apktool b ru.mail.love --use-aapt2
I: Using Apktool 2.7.0
I: Checking whether sources has changed...
I: Smaling smali folder into classes.dex...
I: Checking whether sources has changed...
I: Smaling smali_assets folder into assets.dex...
I: Checking whether sources has changed...
I: Smaling smali_classes2 folder into classes2.dex...
I: Checking whether sources has changed...
I: Smaling smali_classes3 folder into classes3.dex...
I: Checking whether sources has changed...
I: Smaling smali_classes4 folder into classes4.dex...
I: Checking whether sources has changed...
I: Smaling smali_classes5 folder into classes5.dex...
I: Checking whether resources has changed...
I: Building resources...
I: Copying libs... (/lib)
I: Copying libs... (/kotlin)
I: Copying libs... (/META-INF/services)
I: Building apk file...
I: Copying unknown files/dir...
I: Built apk into: ru.mail.love\dist\ru.mail.love.apk

C:\frida-android\application\decompile>
```



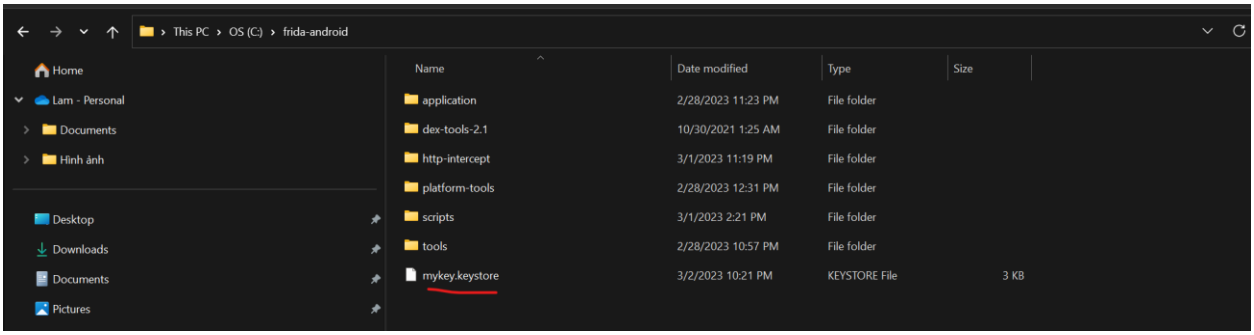
20.3 Creating keystore signing and intercepting https

20.3.1 Create keystore

C:\frida-android>keytool -genkey -v -keystore mykey.keystore -alias mykey -keyalg RSA -keysize 2048 -validity 10000

Pass = 123456

```
C:\frida-android>keytool -genkey -v -keystore mykey.keystore -alias mykey -keyalg RSA -keysize 2048 -validity 10000
Enter keystore password:
Re-enter new password:
What is your first and last name?
  [Unknown]:
What is the name of your organizational unit?
  [Unknown]:
What is the name of your organization?
  [Unknown]:
What is the name of your City or Locality?
  [Unknown]:
What is the name of your State or Province?
  [Unknown]:
What is the two-letter country code for this unit?
  [Unknown]:
Is CN=Unknown, OU=Unknown, O=Unknown, L=Unknown, ST=Unknown, C=Unknown correct?
  [no]:  yes

Generating 2,048 bit RSA key pair and self-signed certificate (SHA256withRSA) with a validity of 10,000 days
        for: CN=Unknown, OU=Unknown, O=Unknown, L=Unknown, ST=Unknown, C=Unknown
[Storing mykey.keystore]

C:\frida-android>
```



20.3.2 Signing

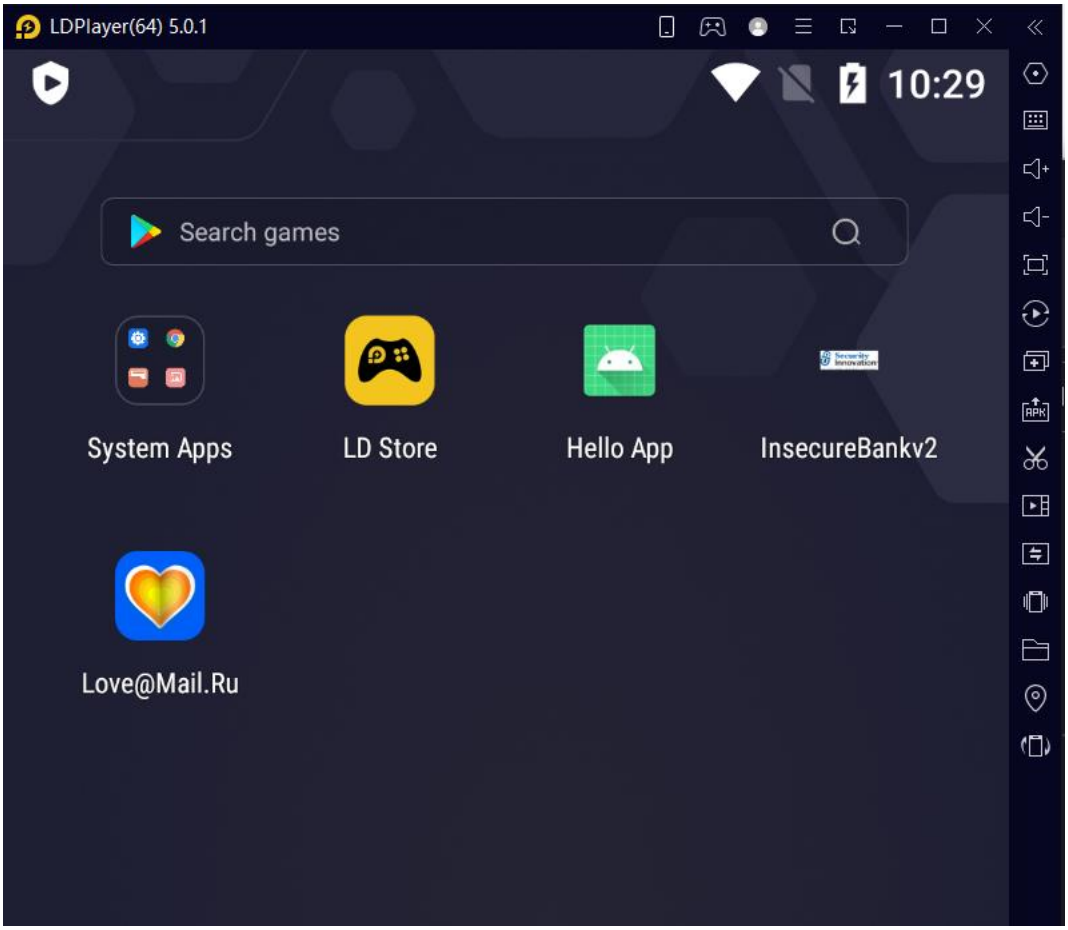
C:\frida-android\application\decompile\ru.mail.love\dist>jarsigner -verbose -sigalg SHA1withRSA -digestalg SHA1 -keystore mykey.keystore ru.mail.love.apk mykey

Pass = 123456

```
C:\frida-android\application\decompile\ru.mail.love\dist>jarsigner -verbose -sigalg SHA1withRSA -digestalg SHA1 -keystore mykey.keystore ru.mail.love.apk mykey
Enter Passphrase for keystore:
   adding: META-INF/MANIFEST.MF
   adding: META-INF/MYKEY.SF
   adding: META-INF/MYKEY.RSA
  signing: META-INF/services/kotlinx.coroutines.CoroutineExceptionHandler
  signing: META-INF/services/kotlinx.coroutines.internal.MainDispatcherFactory
  signing: AndroidManifest.xml
  signing: assets.dex
  signing: classes.dex
  signing: classes2.dex
  signing: classes3.dex
  signing: classes4.dex
  signing: classes5.dex
```

```
  signing: google/protobuf/timestamp.proto
  signing: google/protobuf/type.proto
  signing: google/protobuf/wrappers.proto
  signing: okhttp3/internal/publicsuffix/NOTICE
  signing: okhttp3/internal/publicsuffix/publicsuffixes.gz

>>> Signer
    X.509, CN=Unknown, OU=Unknown, O=Unknown, L=Unknown, ST=Unknown, C=Unknown
    Signature algorithm: SHA256withRSA, 2048-bit key
    [trusted certificate]

jar signed.

Warning:
The signer's certificate is self-signed.
The SHA1 algorithm specified for the -digestalg option is considered a security risk and is disabled.
The SHA1withRSA algorithm specified for the -sigalg option is considered a security risk and is disabled.

C:\frida-android\application\decompile\ru.mail.love\dist>
```

Install again



21 Section 21: Local data storage vulnerabilities

22 Section 22: Exported application component vulnerabilities

23 Section 23: Insecure logging vulnerabilities

24 Section 24: Bypassing root detection using objection

25 Section 25: Resources for further study

26 Bypass SSL pinning

26.1 Install tool

https://infosecwriteups.com/bypass-ssl-pinning-in-android-phones-part-2-cda0f6d3913f

(base) PS C:\Users\ASUS> pip install frida

```
(base) PS C:\Users\ASUS> pip install frida
Collecting frida
  Downloading frida-16.0.19-cp37-abi3-win_amd64.whl (29.9 MB)
     ---------------------------------------- 29.9/29.9 MB 5.0 MB/s eta 0:00:00
Requirement already satisfied: typing-extensions in c:\users\asus\anaconda3\lib\site-packages (from frida) (4.3.0)
Installing collected packages: frida
Successfully installed frida-16.0.19
(base) PS C:\Users\ASUS>
```

(base) PS C:\Users\ASUS> pip install frida-tools

```
(base) PS C:\Users\ASUS> pip install frida-tools
Collecting frida-tools
  Downloading frida-tools-12.1.2.tar.gz (177 kB)
     ---------------------------------------- 177.6/177.6 kB 3.6 MB/s eta 0:00:00
  Installing build dependencies ... done
  Getting requirements to build wheel ... done
  Preparing metadata (pyproject.toml) ... done
Requirement already satisfied: colorama<1.0.0,>=0.2.7 in c:\users\asus\anaconda3\lib\site-packages (from frida-tools) (0
.4.5)
Requirement already satisfied: frida<17.0.0,>=16.0.9 in c:\users\asus\anaconda3\lib\site-packages (from frida-tools) (16
.0.19)
Requirement already satisfied: prompt-toolkit<4.0.0,>=2.0.0 in c:\users\asus\anaconda3\lib\site-packages (from frida-too
ls) (3.0.20)
Requirement already satisfied: pygments<3.0.0,>=2.0.2 in c:\users\asus\anaconda3\lib\site-packages (from frida-tools) (2
.11.2)
Requirement already satisfied: typing-extensions in c:\users\asus\anaconda3\lib\site-packages (from frida<17.0.0,>=16.0.
9->frida-tools) (4.3.0)
Requirement already satisfied: wcwidth in c:\users\asus\anaconda3\lib\site-packages (from prompt-toolkit<4.0.0,>=2.0.0->
frida-tools) (0.2.5)
Building wheels for collected packages: frida-tools
  Building wheel for frida-tools (pyproject.toml) ... done
  Created wheel for frida-tools: filename=frida_tools-12.1.2-py3-none-any.whl size=187175 sha256=d6d879f3e38357b2db32ece
1b7f62eb0bf93f8f43310156a1ff0567bb2471246
  Stored in directory: c:\users\asus\appdata\local\pip\cache\wheels\34\dd\51\c93ce19121d037fb36dbef1e098c9fd5a613f22cf7d
55b33c7
Successfully built frida-tools
Installing collected packages: frida-tools
Successfully installed frida-tools-12.1.2
(base) PS C:\Users\ASUS>
```

26.2 Start Frida server

m51:/data/local/tmp # ./frida-server &

```
m51:/data/local/tmp # ./frida-server &
[1] 18892
m51:/data/local/tmp # netstat -antlp | grep frida
tcp        0      0 127.0.0.1:27042         0.0.0.0:*               LISTEN      18892/frida-server
m51:/data/local/tmp #
```

D:\PhD\PhD-implement\root_android_phone>adb push mitmproxy-ca-cert.cer /data/local/tmp

D:\PhD\PhD-implement\root_android_phone>adb push ssl-pinning.js /data/local/tmp

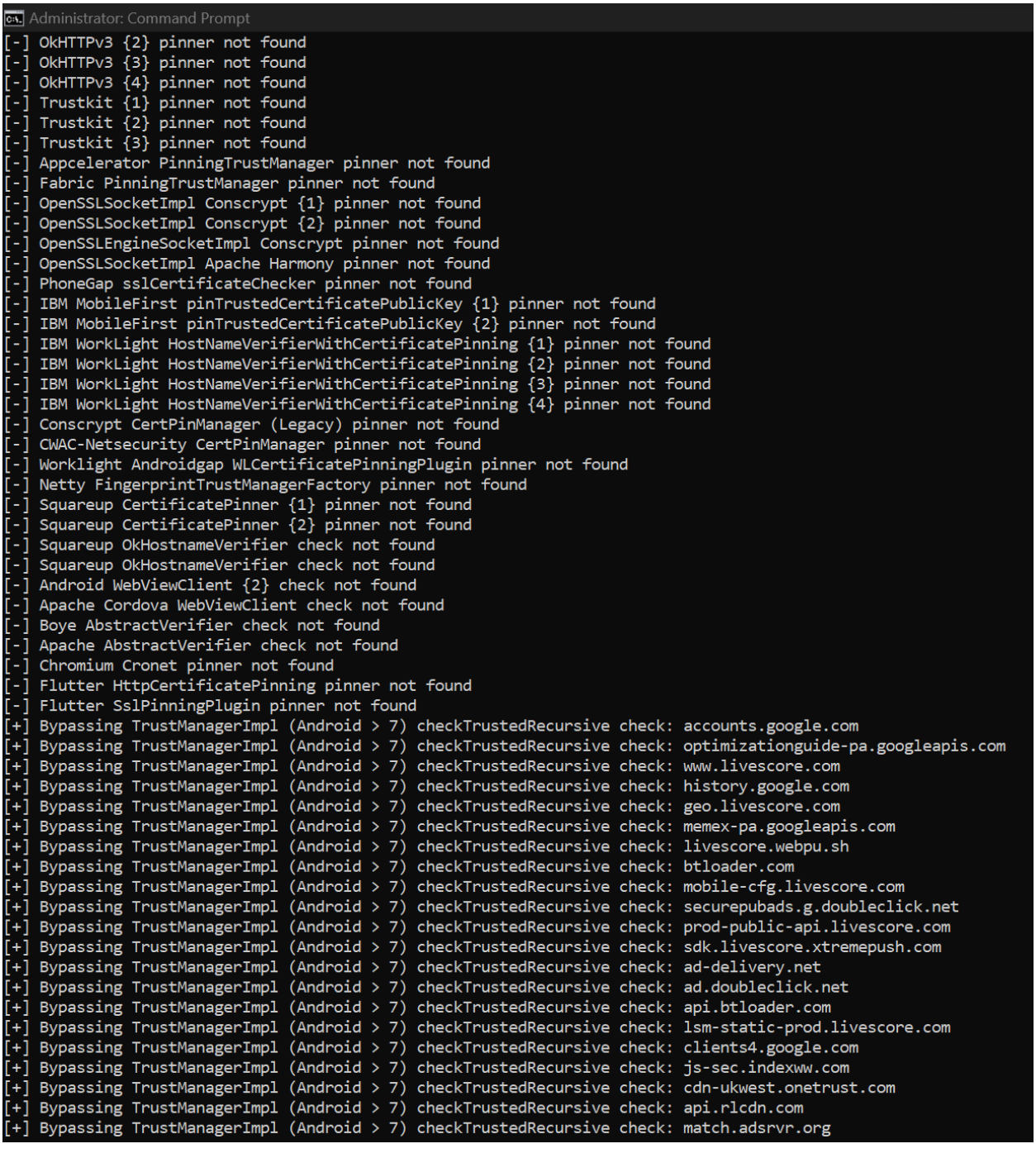
```
D:\PhD\PhD-implement\root_android_phone>adb push mitmproxy-ca-cert.cer /data/local/tmp
mitmproxy-ca-cert.cer: 1 file pushed, 0 skipped. 2.7 MB/s (1172 bytes in 0.000s)

D:\PhD\PhD-implement\root_android_phone>adb push ssl-pinning.js /data/local/tmp
ssl-pinning.js: 1 file pushed, 0 skipped. 13.5 MB/s (2945 bytes in 0.000s)

D:\PhD\PhD-implement\root_android_phone>
```

```
m51:/data/local/tmp # ls -al
total 51080
drwxrwx--x 4 shell shell     3488 2023-06-02 23:12 .
drwxr-x--x 6 root  root      3488 2018-04-15 23:47 ..
-rw-rw-rw- 1 shell shell     1172 2023-03-05 21:30 cert-der.crt
-rw-rw-rw- 1 shell shell      117 2023-04-26 12:58 chrome-command-line
-rwxrwxrwx 1 shell shell 52214528 2023-03-07 00:05 frida-server
-rw-rw-rw- 1 shell shell     1172 2023-03-07 10:49 mitmproxy-ca-cert.cer
-rw-rw-rw- 1 shell shell       22 2023-04-18 11:49 mock_apps.json
drwxr-xr-x 2 root  root      3488 2023-06-02 23:07 re.frida.server
-rwxrwxrwx 1 shell shell      153 2023-04-17 22:30 run-frida-server.sh
-rw-rw-rw- 1 shell shell     2945 2023-06-02 22:56 ssl-pinning.js
drwxr-xr-x 3 root  root      3488 2023-03-07 11:56 system
m51:/data/local/tmp #
```

26.3 SSL pinning

https://codeshare.frida.re/@akabe1/frida-multiple-unpinning/

D:\PhD\PhD-implement\root_android_phone>frida -U -f com.android.chrome -l "frida_multiple_unpinning.js"



27 Fix

27.1 Apply proxy

C:\>adb shell settings put global http_proxy 192.168.1.25:8080

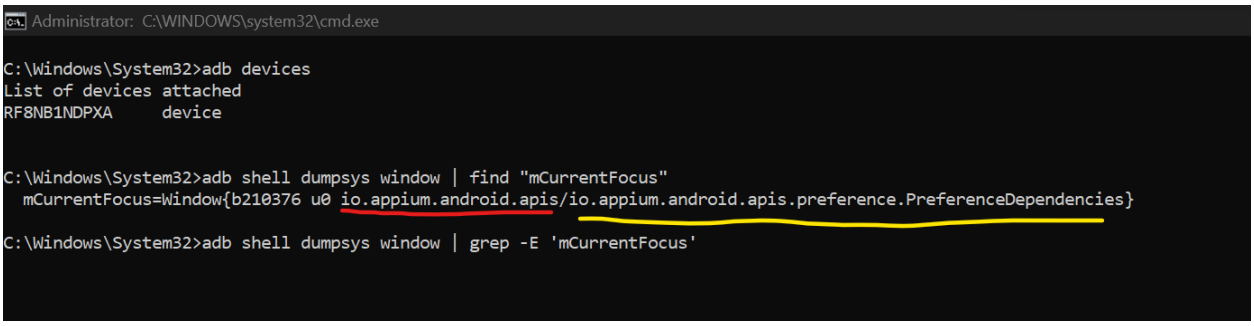
adb shell settings put global http_proxy 193.206.183.20:8080

27.2 Remove proxy

C:\>adb shell settings put global http_proxy :0

27.3 Determine package name and activities name

C:\Windows\System32>adb shell dumpsys window | find "mCurrentFocus"



Red: package name

Yellow: activity name

Note for MAC/Linux

adb shell dumpsys window | grep -E 'mCurrentFocus'

27.4 Start exactly activity

adb shell am start -n <package_name>/<activity_name>